



# LevelOne

## User Manual

WBR-6001

***N\_Max* Wireless Broadband Router**

Ver. 1.0.0-0801

# Safety

## FCC WARNING

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

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 or more of the following measures:

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

## CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

## CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WBR-6001) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

<http://www.levelone.eu/support.php>



# Table of Content

---

|  |           |
|--|-----------|
| <b>TABLE OF CONTENT</b> .....  | <b>V</b>  |
| <b>1. INTRODUCTION</b> .....   | <b>1</b>  |
| USER MANUAL OVERVIEW.....  | 1         |
| <b>2. UNPACKING AND SETUP</b> .....  | <b>3</b>  |
| FEATURES .....   | 3         |
| PACKAGE CONTENTS.....  | 3         |
| <b>3. HARDWARE INSTALLATION</b> .....  | <b>5</b>  |
| PRODUCT LAYOUT – FRONT VIEW.....   | 5         |
| PRODUCT LAYOUT – REAR VIEW .....   | 6         |
| HARDWARE INSTALLATION STEPS .....  | 6         |
| NETWORK CHECK.....   | 8         |
| <b>4. CONFIGURING WIRELESS ROUTER</b> .....  | <b>10</b> |
| LED INDICATOR FOR <i>N_MAX</i> WIRELESS ROUTER .....                               | 10        |
| LOGIN TO CONFIGURE FROM WIZARD .....   | 7         |
| BASIC SETTING .....  | 10        |
| <i>Primary Setup – WAN Type, Virtual Computers</i> .....                           | 10        |
| Static IP Address.....   | 12        |
| Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)..... | 13        |
| PPP over Ethernet .....  | 13        |
| PPTP .....   | 13        |
| L2TP .....   | 14        |
| Virtual Computers (Only for Static and dynamic IP address Wan type) .....          | 15        |
| <i>DHCP Server</i> .....   | 16        |
| <i>Wireless setting, 802.1X setting and WDS</i> .....                              | 17        |
| <i>Change Password</i> .....   | 25        |
| FORWARDING RULES .....   | 26        |
| <i>Virtual Server</i> .....  | 27        |
| <i>Special AP</i> .....  | 28        |
| <i>Miscellaneous Items</i> .....   | 29        |
| SECURITY SETTINGS.....   | 30        |
| <i>Packet Filter</i> .....   | 31        |
| <i>Domain Filter</i> .....   | 36        |

|   |    |
|---|----|
| <i>URL Blocking</i> .....                       | 38 |
| <i>MAC Address Control</i> .....                | 40 |
| <i>Miscellaneous Items</i> .....                | 43 |
| <b>ADVANCED SETTINGS</b> .....                  | 44 |
| <i>System Time</i> .....                        | 45 |
| <i>System Log</i> .....                         | 46 |
| <i>Dynamic DNS</i> .....                        | 47 |
| <i>SNMP Setting</i> .....                       | 49 |
| <i>Routing</i> .....                            | 50 |
| <i>Schedule Rule</i> .....                      | 52 |
| <i>Qos Rule</i> .....                           | 54 |
| <b>TOOLBOX</b> .....                            | 55 |
| <i>System Log</i> .....                         | 55 |
| <i>Firmware Upgrade</i> .....                   | 55 |
| <i>Backup Setting</i> .....                     | 55 |
| <i>Reset to default</i> .....                   | 56 |
| <i>Reboot</i> .....                             | 56 |
| <b>APPENDIX A 802.1X SETTING</b> .....          | 57 |
| <b>APPENDIX B WPA-PSK AND WPA</b> .....         | 62 |
| <b>APPENDIX C FAQ AND TROUBLESHOOTING</b> ..... | 73 |
| <b>TECHNICAL SPECIFICATIONS</b> .....           | 78 |

# 1. Introduction

---

Congratulations on your purchase of LevelOne *N\_Max* 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 the manual carefully for fully exploiting the functions of this product.

## User Manual Overview

|                                 |   |
|---------------------------------|---|
| <b>Introduction</b>             | Describes <i>N_Max</i> Wireless Broadband Router.   |
| <b>Unpacking and Setup</b>      | Helps user to get started with the basic installation of the <i>N_Max</i> Wireless Broadband Router.                    |
| <b>Hardware Installation</b>    | Describes the LED indicators of the <i>N_Max</i> Wireless Broadband Router.   |
| <b>Configuration</b>            | Describes the functionalities and its settings.   |
| <b>Technical Specifications</b> | Lists the technical (general, physical and environmental) specifications of the <i>N_Max</i> Wireless Broadband Router. |



## 2. Unpacking and Setup

---

This chapter provides the package contents and setup information for the *N\_Max* Wireless Broadband Router.

### Features

- Extended and high-speed wireless connectivity with wireless *N* technology
- Advanced QoS Services for Intelligent Internet
- Backward compliant with IEEE802.11g and 11b standards
- Operates on the 2.4GHz frequency band
- Stay Protected with Advanced Network Security
- WEP and WPA/WPA2-PSK encryption supported along with Wi-Fi Protected Setup
- Integrate 4-Port Fast Ethernet Switch with 10/100Mbps MDI-MDI-X auto-sensing
- Built-in NAT function allows multiple PCs and devices to share Internet connection
- Browser-based interface configuration and management
- Quick Setup Wizard provides alternative way to manage device

### Package Contents

Open the box of the *N\_Max* Wireless Broadband Router and carefully unpack it. The box should contain the following items:

- WBR-6001 *N\_Max* Wireless Broadband Router
- Power Adapter
- Cat.5 Cable
- Antenna
- CD Manual/Utility
- Quick Installation Guide

If any item is found missing or damaged, please contact your local reseller for replacement.



## 3. Hardware Installation

---

### Product Layout – Front View



#### 1) Reset

Press the Reset button to reboot device or restores factory default setting.

#### 2) Status

A blinking light indicates the device is ready

#### 3) WAN

A solid light indicates the WAN port is connected.

#### 4) WLAN

A solid light indicates the Wireless segment is ready. LED blinks during wireless data transmission.

#### 5) LAN LEDs

A solid light indicates to an Ethernet enable computer on ports 1~4.  
LED blinks during data transmission.

#### 6) WPS

Wi-Fi Protected Setup push button

## Product Layout – Rear View



### 1) Power Jack

Receptor for the supplied power adapter

### 2) LAN Ports (1~4)

Connect Ethernet devices such as computers, switches or hubs.

### 3) WAN Port

The WAN port is the connection for the Ethernet cable to the Cable or DSL Modem.

### 4) Antenna

Detachable antenna allows users to change antenna if necessary.

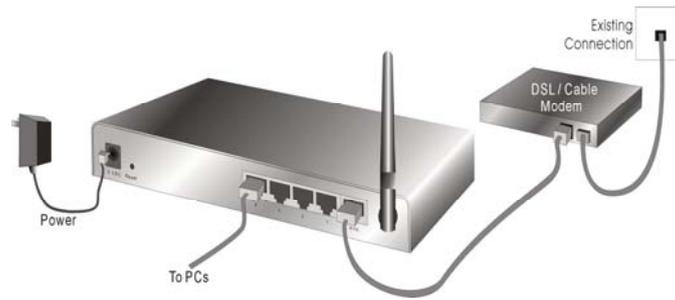
## Hardware installation steps

### Decide where to place your Wireless Broadband Router

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

### Setup LAN connection

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



### 3. Setup WAN connection

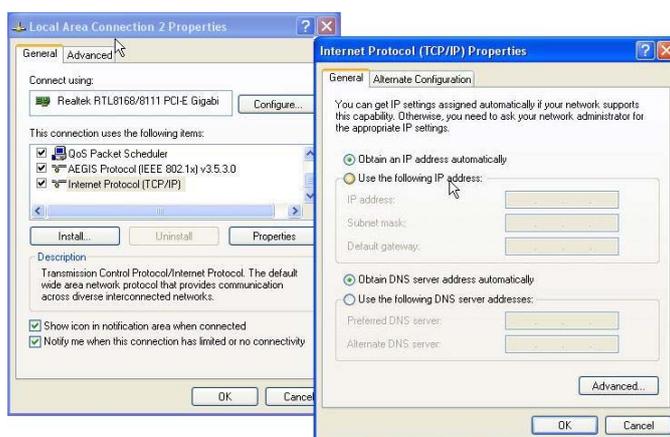
Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone.

### 4. Power on

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

# Network Check

1. Please make sure your PC can get IP address automatically so the WBR-6001 can communicate with your PC during configuration.
  - Select “Control Panel” > “Network Connections”.
  - Right click the “Local Area Connection” and choose “Properties”.
  - Select the TCP/IP protocol for your network card.
  - Click on the Properties button. You should then see the following screen and make sure you have selected “Obtain IP address automatically”



2. Reboot computer to make sure you have received the IP address correctly.
3. Start your Web browser. In the Address box, enter WBR-6001's default IP Address:

**http://192.168.0.1**

4. When prompted, use the following default password to login.



Password: **password**

## Default Settings

|               |             |
|---------------|-------------|
| IP Address    | 192.168.0.1 |
| Password      | password    |
| Wireless Mode | Enable      |
| SSID          | WBR-6001    |
| Security      | None        |



Please enter the default system password in lowercase only.

## 4. Configuring Wireless Router

---

### LED Indicator for *N\_Max* Wireless Router

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

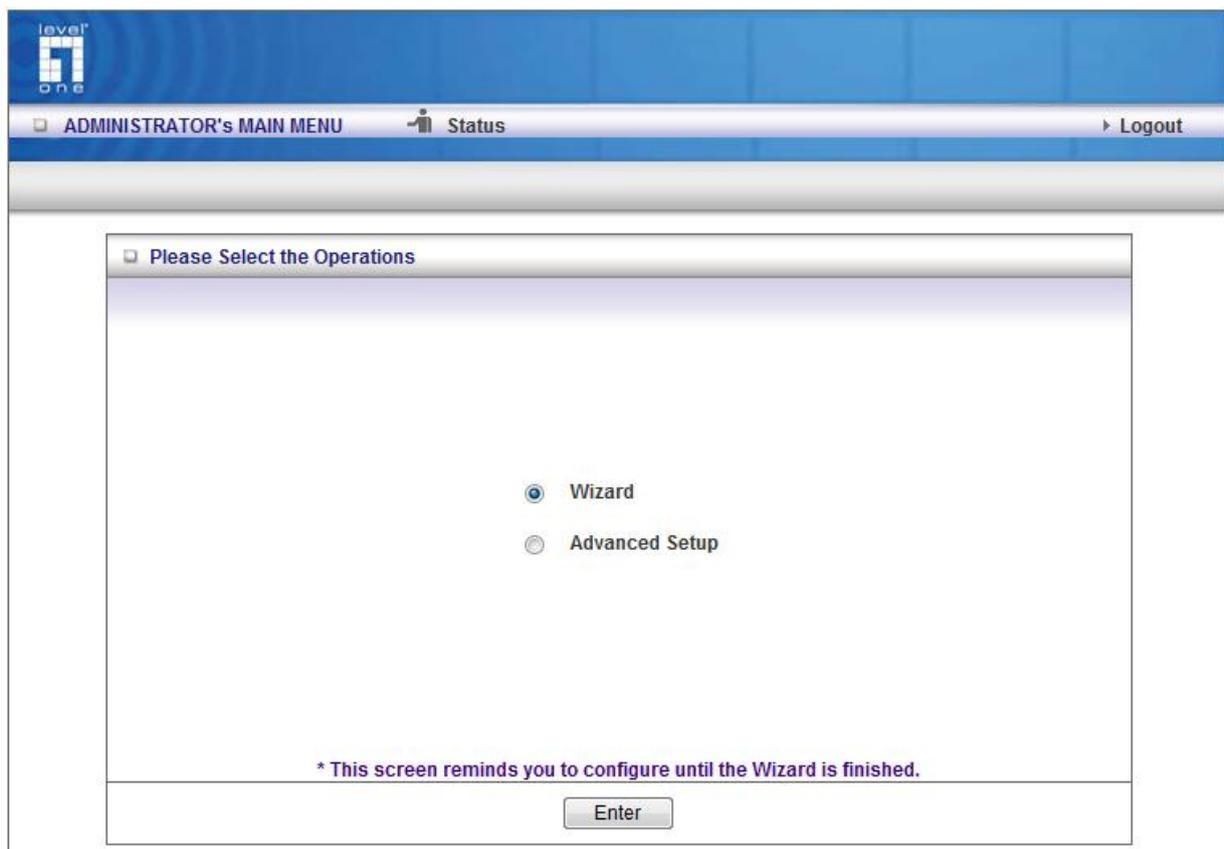
## Login to Configure from Wizard

Activate your browser, and disable the proxy or add the IP address of this product into the exceptions. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: http://192.168.0.1

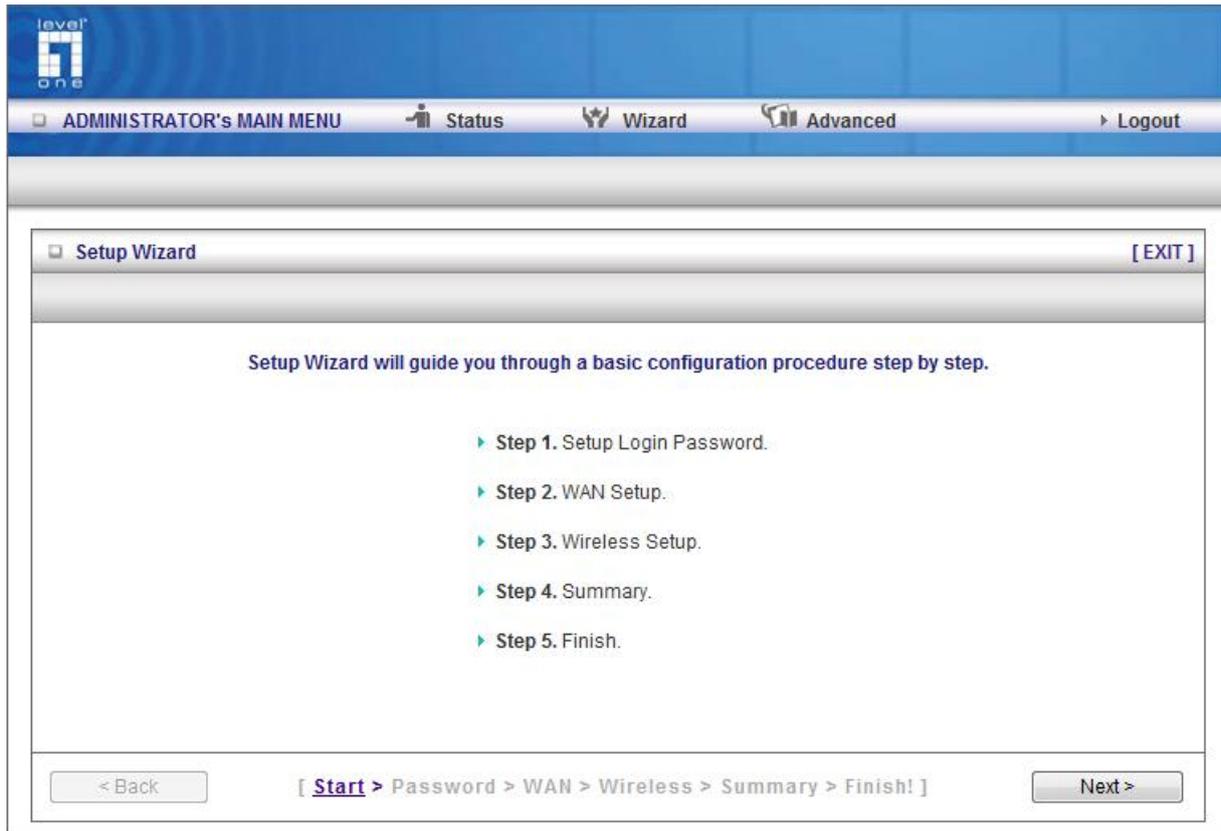
After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

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

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



Setup Wizard will guide you through a basic configuration procedure step by step. Press **”Next ”**



Once the user finishes those steps and the router screen displayed as below. It means that the Internet connection is now established.



Setup Wizard - WAN Connection Test

[EXIT]

## Congratulations!!

The Internet connection is established.

Connection information is

|                    |                          |
|--------------------|--------------------------|
| WAN Type           | Dynamic IP Address       |
| IP Address         | 192.168.50.102           |
| Subnet Mask        | 255.255.255.0            |
| Gateway            | 192.168.50.1             |
| Domain Name Server | 168.95.192.1, 168.95.1.1 |

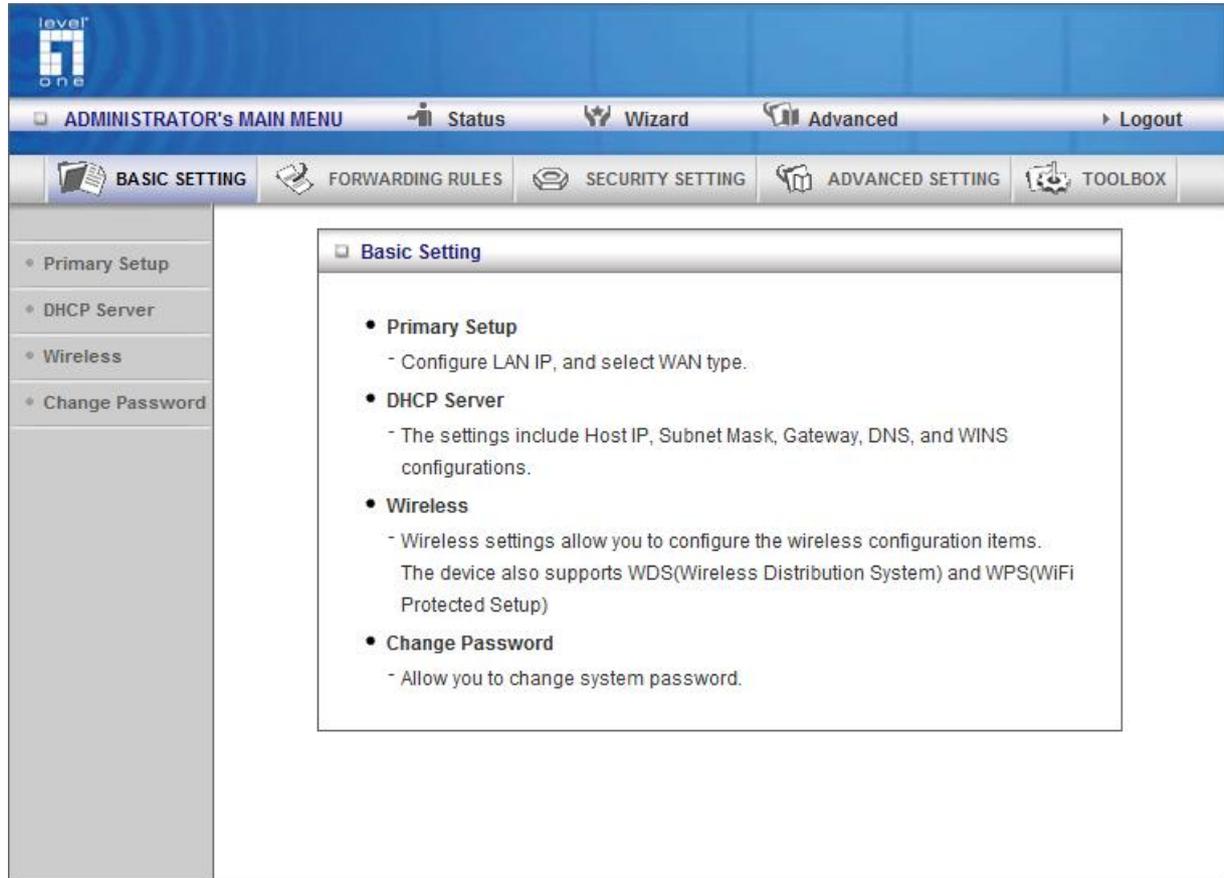
< Back

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

Finish

# Basic Setting

Please Select “Advanced Setup” to Setup



## Primary Setup – WAN Type, Virtual Computers

level one

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

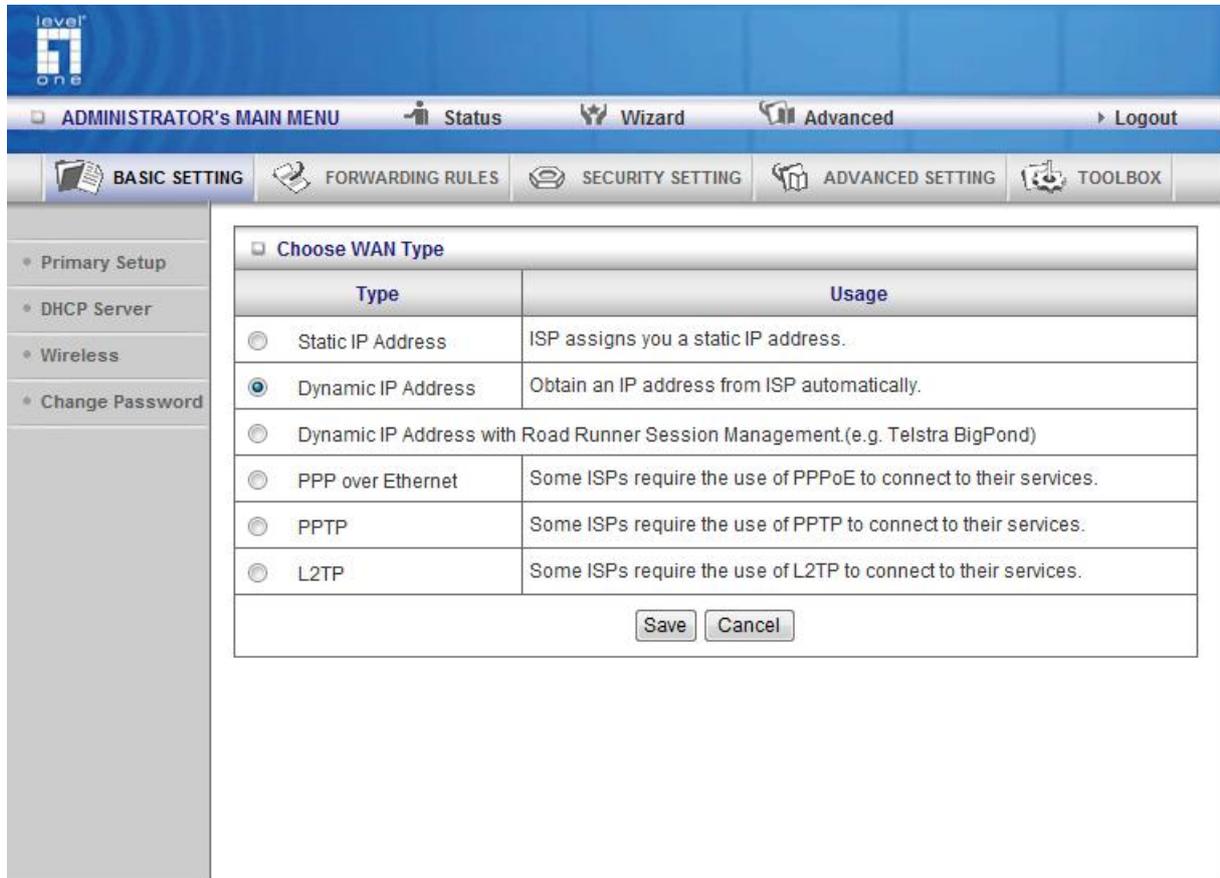
BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Primary Setup [HELP]

| Item                | Setting   |
|---------------------|---|
| ▶ LAN IP Address    | 192.168.0.1   |
| ▶ WAN Type          | Dynamic IP Address <input type="button" value="Change..."/> |
| ▶ Host Name         | <input type="text"/> (optional)                             |
| ▶ WAN's MAC Address | 00-50-18-21-C4-4C <input type="button" value="Clone MAC"/>  |
| ▶ Renew IP Forever  | <input type="checkbox"/> Enable (Auto-reconnect)            |

Press **“Change”**



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

1. LAN IP Address: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

2. WAN Type: WAN connection type of your ISP. You can click Change button to choose a correct one from the following four options:

- A. Static IP Address: ISP assigns you a static IP address.
- B. Dynamic IP Address: Obtain an IP address from ISP automatically.
- C. Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)
- D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
- E. PPTP: Some ISPs require the use of PPTP to connect to their services.
- F. L2TP: Some ISPs require the use of L2TP to connect to their services

### Static IP Address

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

## **Dynamic IP Address**

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

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

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

## **PPP over Ethernet**

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
4. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.
5. Connection Control: There are 3 modes to select:  
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.  
Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.  
Manually : The device will not make the link until someone clicks the connect-button in the Staus-page.

## **PPTP**

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

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

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

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

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

## **L2TP**

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

For example: Use Static

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

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

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

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

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

The screenshot shows the Level One Administrator's interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains links for 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Virtual Computers' and includes a '[ HELP ]' link. At the top of the main area, there is a 'DHCP clients' dropdown menu set to '--- Select one ---', a 'Copy to' button, and an 'ID' dropdown menu. Below this is a table with the following structure:

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

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

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.

## DHCP Server

| Item                       | Setting   |
|----------------------------|---|
| ▶ DHCP Server              | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| ▶ Lease Time               | 60 Minutes  |
| ▶ IP Pool Starting Address | 100   |
| ▶ IP Pool Ending Address   | 199   |
| ▶ Domain Name              |   |

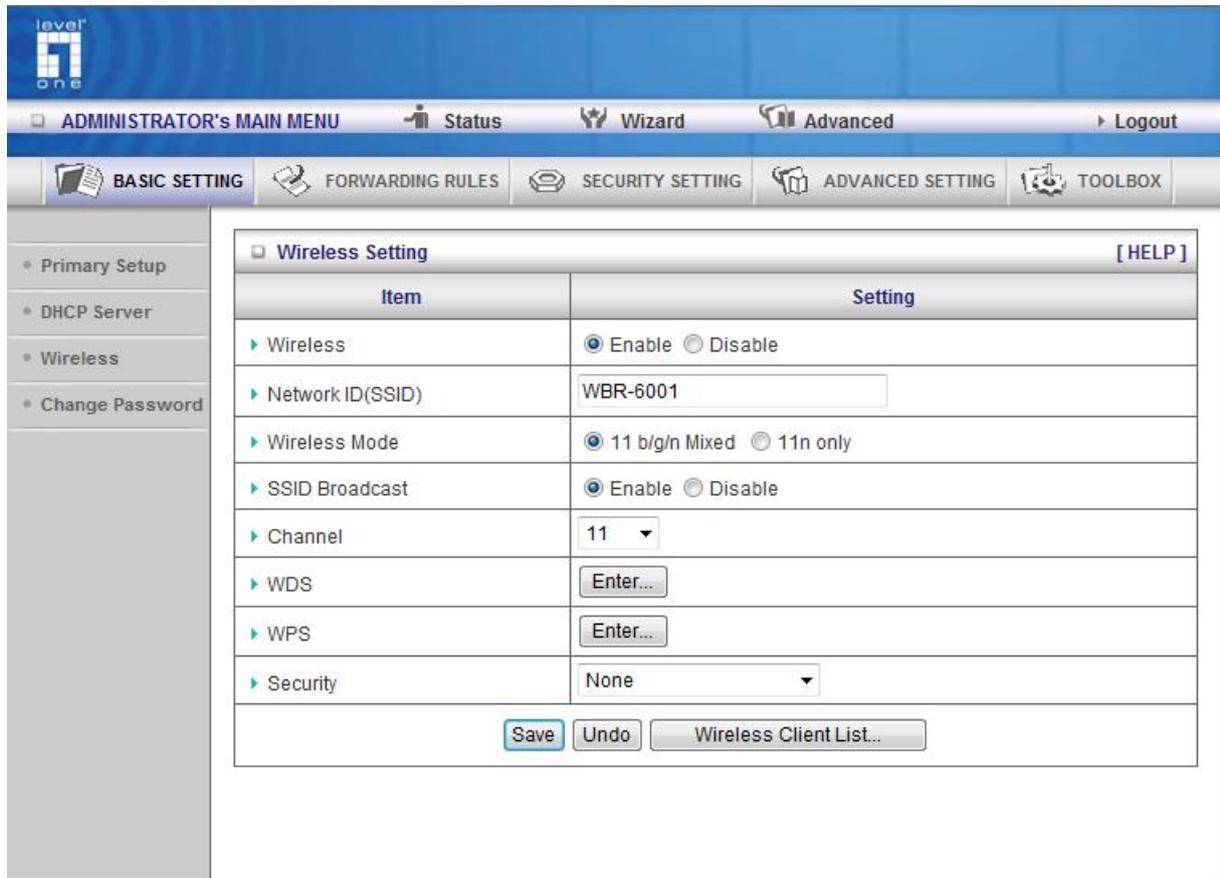
Save Undo More>> Clients List... Fixed Mapping...

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.

## Wireless setting, 802.1X setting and WDS



The screenshot shows the Level One router configuration interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', '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) | WBR-6001   |
| Wireless Mode    | <input checked="" type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only |
| SSID Broadcast   | <input checked="" type="radio"/> Enable <input type="radio"/> Disable          |
| Channel          | 11   |
| WDS              | Enter...   |
| WPS              | Enter...   |
| Security         | None   |

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

Wireless settings allow you to set the wireless configuration items.

Wireless: The user can enable or disable wireless function.

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

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

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

Security: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

There are several security types to use:

WEP:

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

802.1X

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

RADIUS Server

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

RADIUS Shared Key

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

| Item                  | Setting  |
|-----------------------|--|
| Wireless              | <input checked="" type="radio"/> Enable <input type="radio"/> Disable          |
| Network ID(SSID)      | WBR-6001   |
| Wireless Mode         | <input checked="" type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only |
| SSID Broadcast        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable          |
| Channel               | 11   |
| WDS                   | Enter...   |
| WPS                   | Enter...   |
| Security              | 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     |  |

Save Undo Wireless Client List..

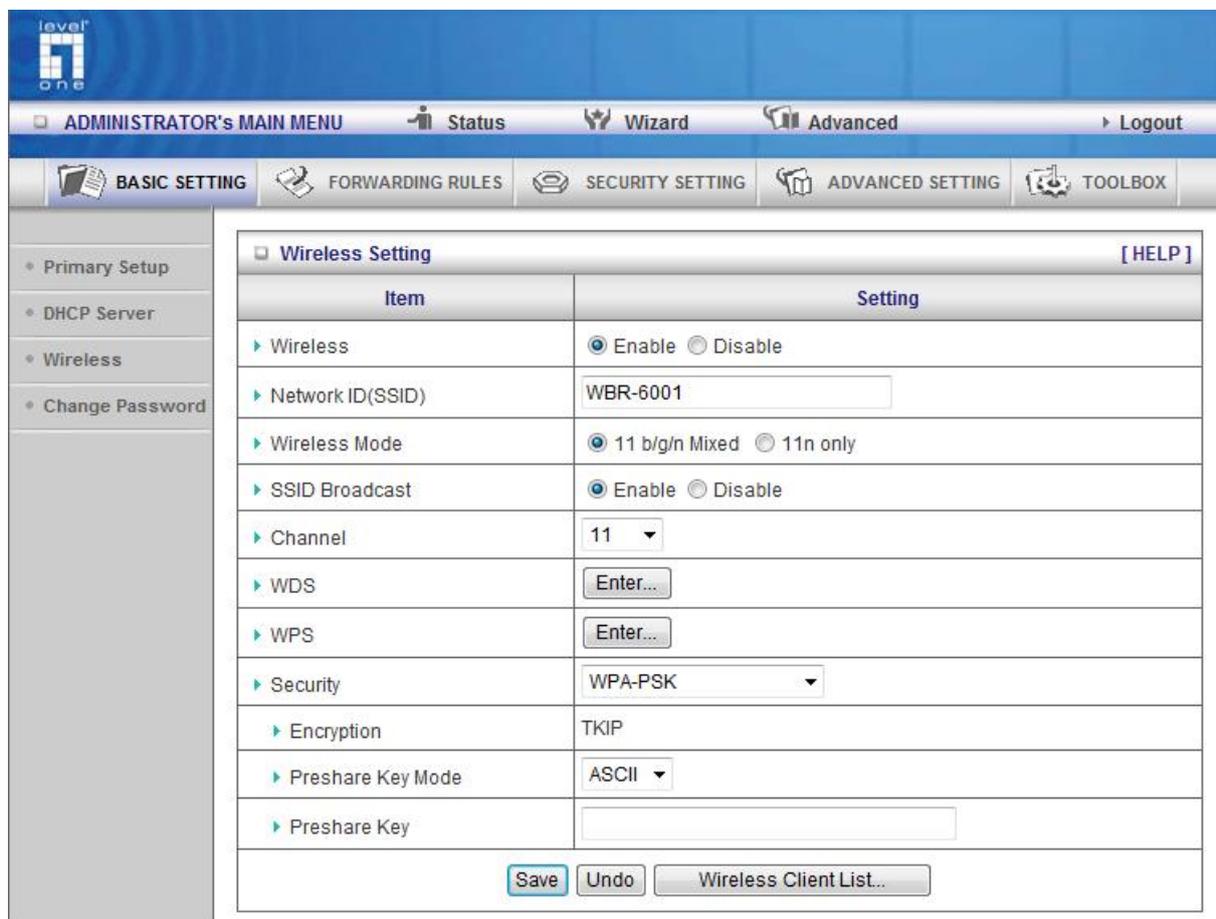
## WPA-PSK

### 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 user selects 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 user elects 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 user selects 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 user selects 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

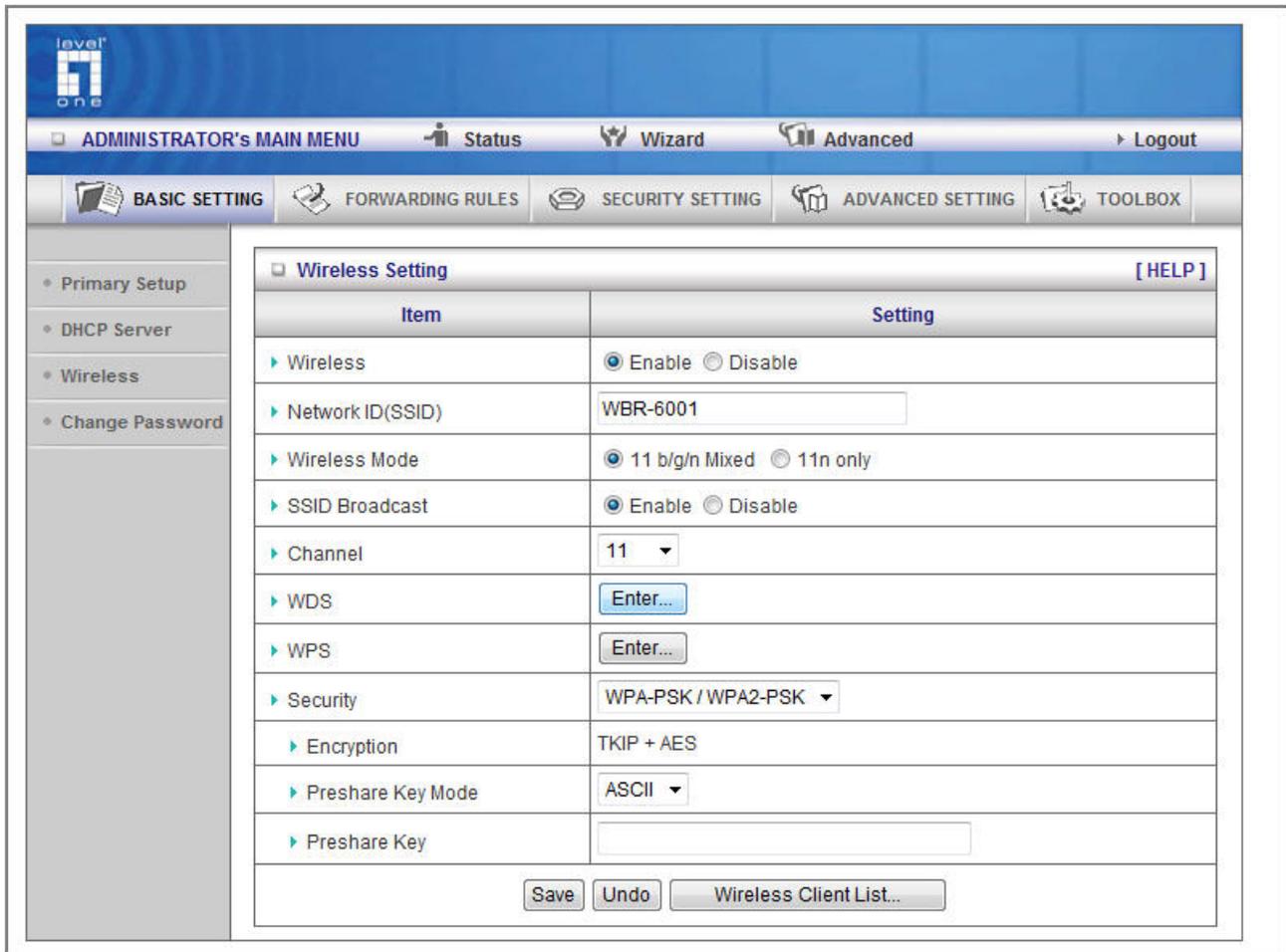
The router will detect automatically which Security type the client uses to encrypt.

### 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 user selects ASCII, the length of Pre-share key is from 8 to 63.

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



## WPA/WPA2

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server The router will detect automatically which Security type(Wpa-psk version 1 or 2) the client uses to encrypt.

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

Select RADIUS Shared Key

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

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

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

## WPS (WiFi Protection Setup)

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

The screenshot shows the Level One router's web interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wi-Fi Protected Setup' and contains a table with the following items and settings:

| Item         | Setting   |
|--------------|---|
| ▶ WPS        | <input checked="" type="radio"/> Enable <input type="radio"/> Disable   |
| ▶ Setup      | <input type="radio"/> Current AP PIN<br><input checked="" type="radio"/> Configure Wireless Station                 |
| ▶ Method     | <input type="radio"/> Enrollee PIN : <input type="text" value="00000000"/><br><input type="radio"/> Software button |
| ▶ WPS state  | <b>WPS is invalid!</b>  |
| ▶ WPS status | Configured <input type="button" value="Release"/>   |

At the bottom of the table, there are buttons for 'Save', 'Trigger', 'Back', and 'Reboot'. Below the buttons, a message states: '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.



- Primary Setup
- DHCP Server
- Wireless
- Change Password

WDS Setting [HELP]

| Item                   | Setting   |
|------------------------|---|
| Wireless Bridging      | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| Remote AP MAC    MAC 1 | <input type="text"/>  |
| MAC 2                  | <input type="text"/>  |
| MAC 3                  | <input type="text"/>  |

Scanned AP's MAC --- Select one ---        Remote AP MAC --

| SSID          | Channel | MAC Address       |
|---------------|---------|-------------------|
| WAP-0003      | 6       | 00-11-6B-60-6A-C5 |
| MeetingRoom   | 7       | 00-11-6B-B0-87-9C |
| WLAN-PS       | 6       | 6E-4F-11-D8-6C-81 |
| camera        | 6       | 00-19-5B-43-29-8E |
| camera        | 7       | 00-18-E7-1B-EE-58 |
| ts3406        | 11      | 00-11-6B-22-51-50 |
| WBR 6000v3    | 11      | 00-C0-02-00-00-10 |
| Danny_wbr3405 | 11      | 00-11-6B-B0-6A-01 |

# Change Password

The screenshot displays the Level One Administrator's Main Menu. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu shows 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists configuration categories: 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Change Password' and contains a table with the following structure:

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

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

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

# Forwarding Rules

The screenshot displays the Level One router administration web interface. At the top left is the Level One logo. Below it is a navigation bar with the following items: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. A secondary navigation bar contains icons and labels for BASIC SETTING, FORWARDING RULES (which is currently selected), SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, there is a sidebar menu with three items: Virtual Server, Special AP, and Miscellaneous. The main content area is titled "Forwarding Rules" and contains a list of three categories:

- **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.

## Virtual Server

level  
ONE

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Virtual Server [HELP]

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

| ID | Server IP  | Public Port | Private Port | Protocol | Enable                   | Schedule Rule# |
|----|------------|-------------|--------------|----------|--------------------------|----------------|
| 1  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 2  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 3  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 4  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 5  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 6  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 7  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 8  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 9  | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |
| 10 | 192.168.0. |             |              | Both     | <input type="checkbox"/> | 0              |

Next >>   Save   Undo

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

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

For example, if you have an FTP server (port 21) at 192.168.0.2, a Web server (port 80) at 192.168.0.3, and a VPN server at 192.168.0.6, then you need to specify the following virtual server mapping table:

| Service Port | Server IP   | Enable |
|--------------|-------------|--------|
| 21           | 192.168.0.2 | V      |
| 80           | 192.168.0.3 | V      |
| 1723         | 192.168.0.6 | V      |

## Special AP

The screenshot shows a web interface for configuring Special Applications. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar has a tree view with 'Virtual Server', 'Special AP', and 'Miscellaneous'. The main content area is titled 'Special Applications' and includes a '[ HELP ]' link. It features a 'Popular applications' dropdown menu, a 'Copy to' button, and an 'ID' dropdown. Below this is a table with 8 rows, each with columns for 'ID', 'Trigger', 'Incoming Ports', and 'Enable'. The 'Enable' column contains checkboxes. At the bottom of the table are 'Save' and 'Undo' buttons.

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

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

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

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

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

## Miscellaneous Items

The screenshot shows the LevelOne administrator interface. At the top, there is a navigation bar with the LevelOne logo and menu items: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary navigation bar with icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, there is a sidebar menu with options: Virtual Server, Special AP, and Miscellaneous. The main content area is titled 'Miscellaneous Items' and contains a table with the following data:

| Item                     | Setting                         | Enable                   |
|--------------------------|---------------------------------|--------------------------|
| ▶ IP Address of DMZ Host | 192.168.0. <input type="text"/> | <input type="checkbox"/> |
| ▶ Non-standard FTP port  | <input type="text" value="0"/>  |                          |
| ▶ UPnP setting           |                                 | <input type="checkbox"/> |
| ▶ Xbox Support           |                                 | <input type="checkbox"/> |

At the bottom of the table, there are 'Save' and 'Undo' buttons. A '[ HELP ]' link is located in the top right corner of the table area.

### 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.

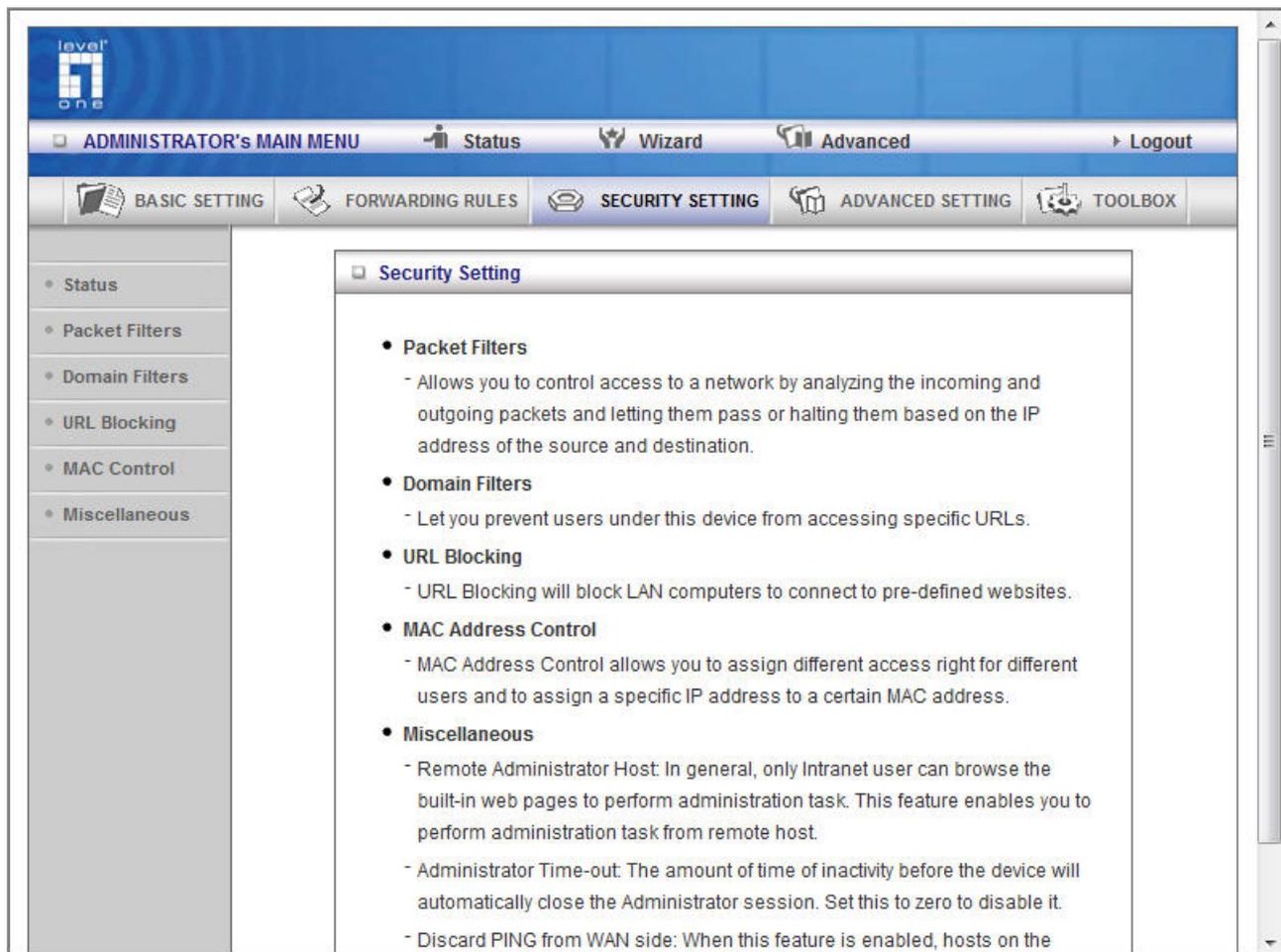
### Xbox Support

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.

## Security Settings



The screenshot displays the LevelOne administrator interface. At the top, there is a blue header with the LevelOne logo and navigation links: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary navigation bar with icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING (which is highlighted), ADVANCED SETTING, and TOOLBOX. On the left side, there is a vertical sidebar menu with options: Status, Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area is titled "Security Setting" and contains a list of security features:

- **Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- **Domain Filters**
  - Let you prevent users under this device from accessing specific URLs.
- **URL Blocking**
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- **MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- **Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the

## Packet Filter

level  
ONE

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Outbound Packet Filter [HELP]

Item Setting

Outbound Filter  Enable

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

Schedule rule (00)Always Copy to ID --

| ID | Source IP            | Destination IP : Ports                      | Enable                   | Schedule Rule# |
|----|----------------------|---|--------------------------|----------------|
| 1  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 2  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 3  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 4  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 5  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 6  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 7  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <input type="checkbox"/> | 0              |
| 8  | <input type="text"/> | <input type="text"/> : <input type="text"/> | <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**.

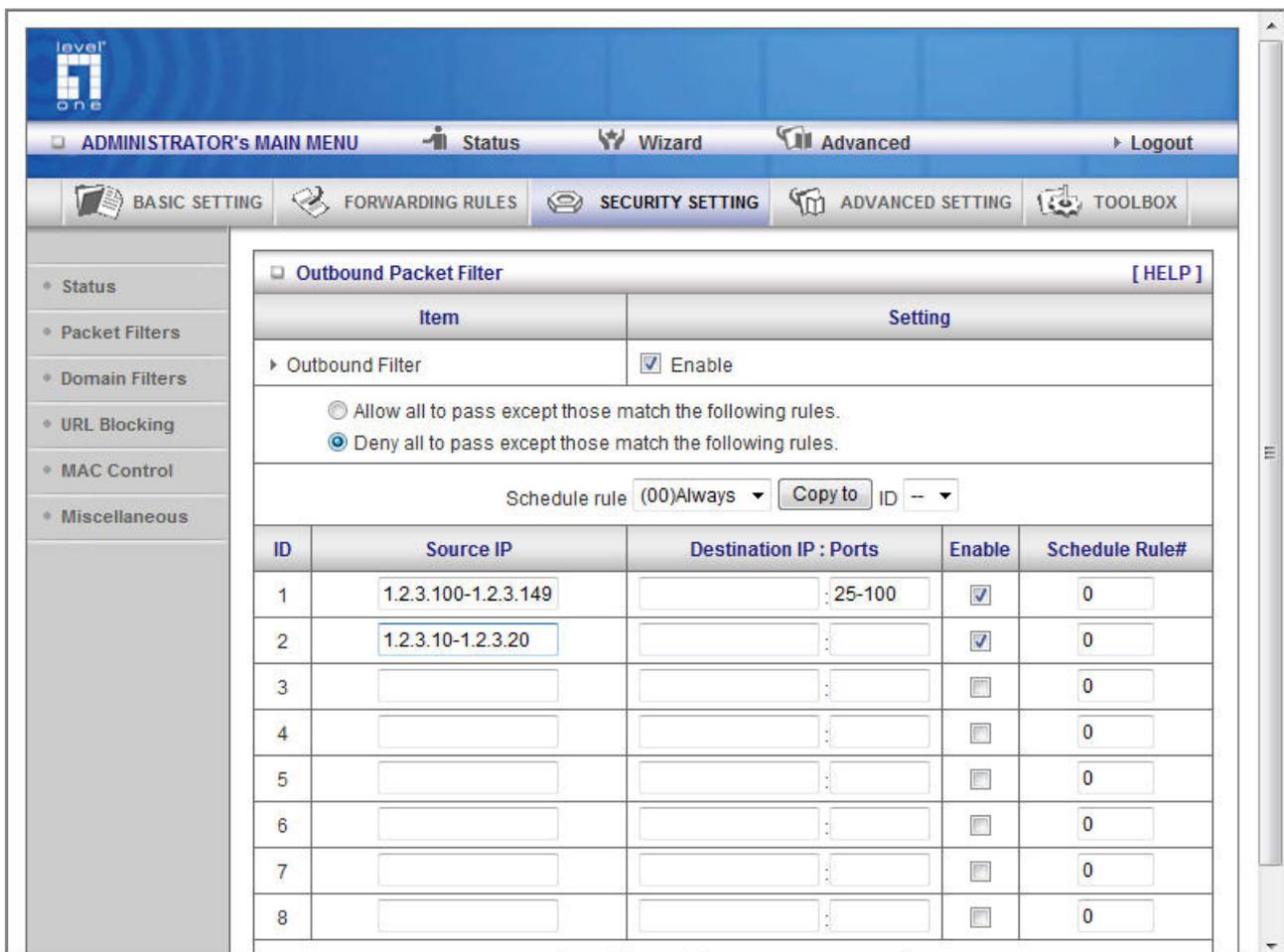
Each rule can be enabled or disabled individually.

Inbound Filter:

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

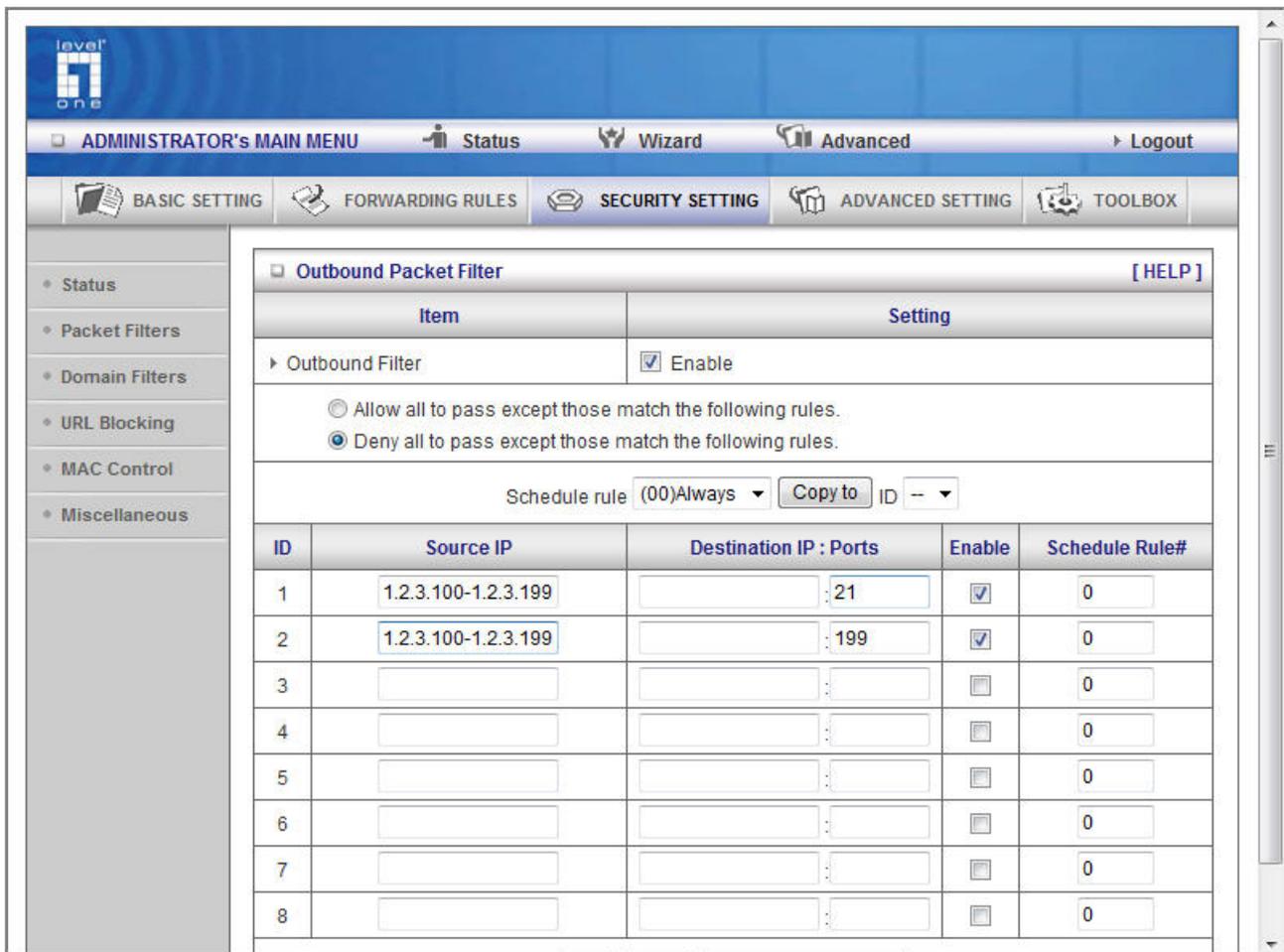
Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

**Example 1:**



(1.2.3.100-1.2.3.149) they are allow to send mail (port 25), and browse the Internet (port 80)  
 (1.2.3.10-1.2.3.20) they can do everything (block nothing)  
 Others are all blocked.

**Example 2:**



(1.2.3.100-1.2.3.119) they can do everything except read net news (port 119) and transfer files via FTP (port 21)  
 Others are all allowed.

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

Outbound Filter:

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

**Example 1:**

level ONE

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Outbound Packet Filter [HELP]

Item   Setting

Outbound Filter    Enable

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

Schedule rule (00)Always   Copy to ID 1

| ID | Source IP          | Destination IP : Ports | Enable                              | Schedule Rule# |
|----|--------------------|------------------------|-------------------------------------|----------------|
| 1  | 00-149.161.123.149 | : 25-100               | <input checked="" type="checkbox"/> | 0              |
| 2  | .10-149.161.123.20 | :                      | <input checked="" type="checkbox"/> | 0              |
| 3  |                    | :                      | <input type="checkbox"/>            | 0              |
| 4  |                    | :                      | <input type="checkbox"/>            | 0              |
| 5  |                    | :                      | <input type="checkbox"/>            | 0              |
| 6  |                    | :                      | <input type="checkbox"/>            | 0              |
| 7  |                    | :                      | <input type="checkbox"/>            | 0              |
| 8  |                    | :                      | <input type="checkbox"/>            | 0              |

(149.161.123.100-149.161.123.149) they are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(149.161.123.10-149.161.123.20) they can do everything (block nothing)  
Others are all blocked.

### Example 2:

The screenshot shows the 'Outbound Packet Filter' configuration page in the Level One interface. The page is titled 'Outbound Packet Filter' and includes a '[HELP]' link. The configuration is as follows:

- Outbound Filter:**  Enable
- Policy:**  Allow all to pass except those match the following rules.  Deny all to pass except those match the following rules.
- Schedule rule:** (00)Always  ID 1

| ID | Source IP       | Destination IP : Ports | Enable                              | Schedule Rule# |
|----|-----------------|------------------------|-------------------------------------|----------------|
| 1  | 149.161.123.100 | : 21                   | <input checked="" type="checkbox"/> | 0              |
| 2  | 149.161.123.119 | : 119                  | <input checked="" type="checkbox"/> | 0              |
| 3  |                 |                        | <input type="checkbox"/>            | 0              |
| 4  |                 |                        | <input type="checkbox"/>            | 0              |
| 5  |                 |                        | <input type="checkbox"/>            | 0              |
| 6  |                 |                        | <input type="checkbox"/>            | 0              |
| 7  |                 |                        | <input type="checkbox"/>            | 0              |
| 8  |                 |                        | <input type="checkbox"/>            | 0              |

(149.161.123.100 and 149.161.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

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

## Domain Filter

The screenshot shows the 'Domain Filter' configuration page in the Level One Administrator's interface. The page has a blue header with the Level One logo and navigation tabs: ADMINISTRATOR's MAIN MENU, Status, Wizard, and Advanced. Below this is a secondary navigation bar with icons for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left, a sidebar menu lists various settings categories. The main content area is titled 'Domain Filter' and contains a table with the following data:

| Item                         |  | Setting   |                          |
|------------------------------|--|---|--------------------------|
| Domain Filter                |  | <input type="checkbox"/> Enable   |                          |
| Log DNS Query                |  | <input 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 type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 2                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 3                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 4                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 5                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 6                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 7                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 8                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |
| 9                            | <input type="text"/>                     | <input type="checkbox"/> Drop <input type="checkbox"/> Log                | <input type="checkbox"/> |

### Domain Filter

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

### Domain Filter Enable

Check if you want to enable Domain Filter.

### Log DNS Query

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

### Privilege IP Addresses Range

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

### Domain Suffix

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

### Action

When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check log to log these accesses.

### Enable

Check to enable each rule.

## Example:

The screenshot shows the LevelOne administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Domain Filter' and includes a '[ HELP ]' link. It contains a table with columns 'Item' and 'Setting'. Below this is a table with columns 'ID', 'Domain Suffix', 'Action', and 'Enable'.

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

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

In this example:

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

## URL Blocking

The screenshot shows the Level One administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar has expandable sections: 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'URL Blocking' and includes a '[ HELP ]' link. It features a table with columns 'ID', 'URL', and 'Enable'. The 'Enable' column contains checkboxes. Below the table are 'Save' and 'Undo' buttons.

| URL Blocking |                                 |                          |
|--------------|---------------------------------|--------------------------|
| 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-define 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

Check 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

Check to enable each rule.

The screenshot shows the Level One administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists filter categories: Status, Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area is titled 'URL Blocking' and contains a table with the following data:

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

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

In this example:

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

## MAC Address Control

The screenshot shows the Level One network management interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists categories: Status, Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area is titled 'MAC Address Control' and includes a '[ HELP ]' link. It features three main settings:

- Enable:** A checkbox to enable MAC Address Control.
- Connection control:** A checkbox to enable controlling which wired and wireless clients can connect. The setting is 'allow' for unspecified MAC addresses to connect.
- Association control:** A checkbox to enable controlling which wireless client can associate to the wireless LAN. The setting is 'deny' for unspecified MAC addresses to associate. A note states: 'Note: Association control has no effect on wired clients.'

Below these settings is a 'DHCP clients' dropdown menu set to '--- Select one ---' and a 'Copy to ID --' dropdown. At the bottom is a table with the following structure:

| ID | MAC Address          | IP Address                      | C                        | A                        |
|----|----------------------|---------------------------------|--------------------------|--------------------------|
| 1  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Navigation buttons at the bottom include '<< 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"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4  | <input type="text"/> | 192.168.0. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |

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

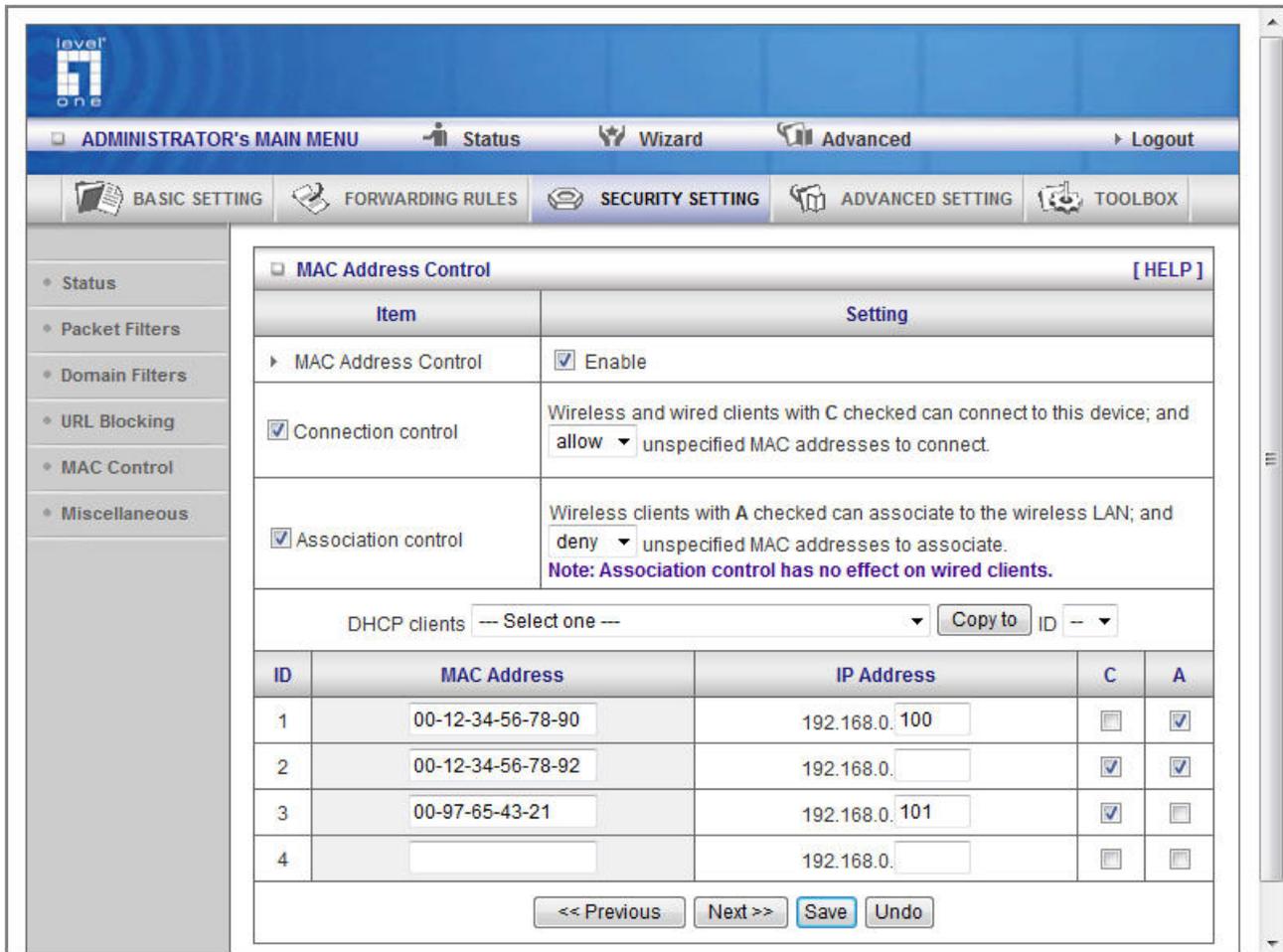
|                    |  |
|--------------------|--|
| <b>MAC Address</b> | MAC address indicates a specific client.   |
| <b>IP Address</b>  | Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.   |
| <b>C</b>           | When " <b>Connection control</b> "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

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

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

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

**Example:**

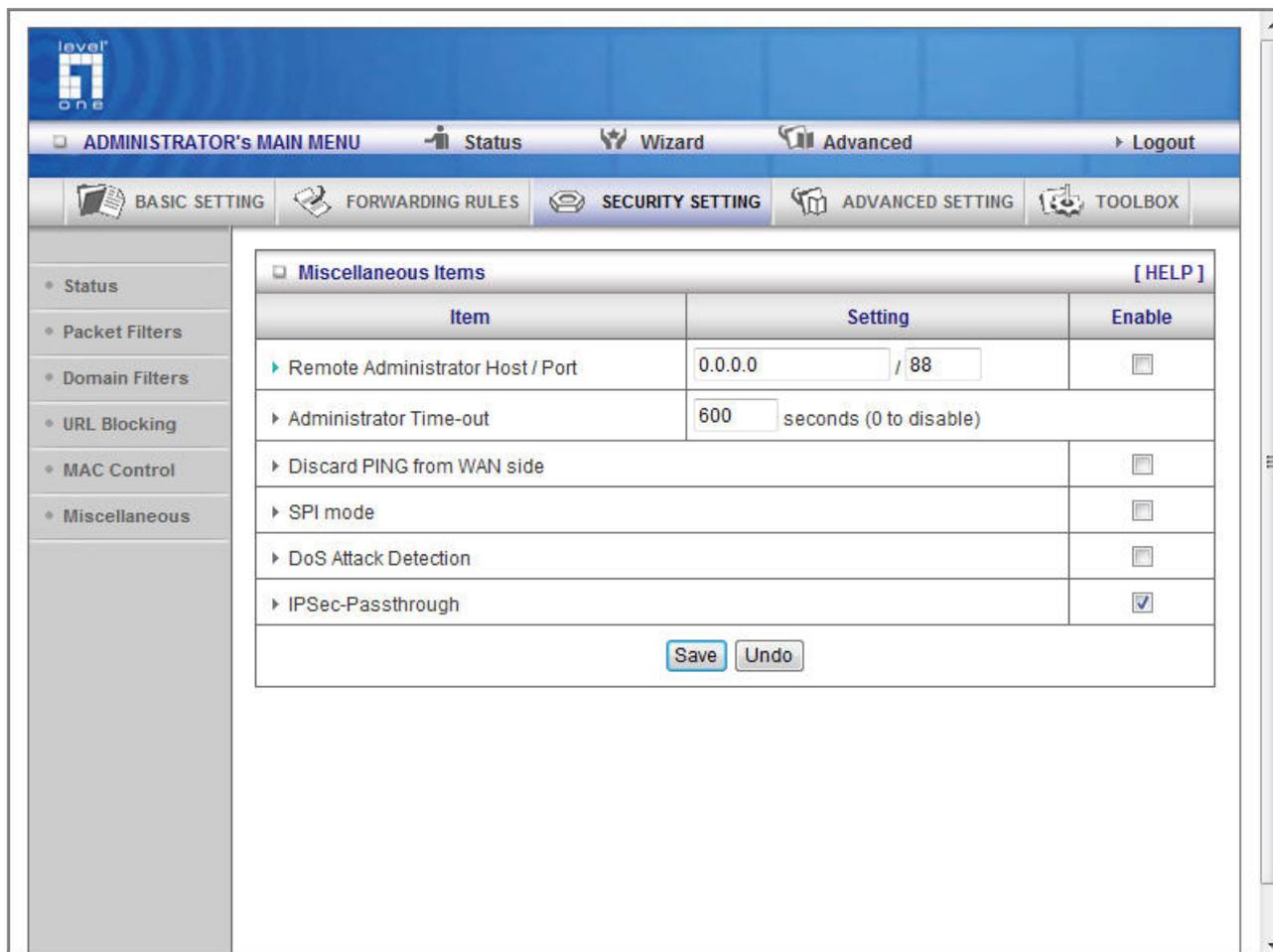


In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

1. The "MAC Address Control" function is enabled.
2. "Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.
3. "Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.
4. Clients 1 and 3 have fixed IP address 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.

## 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"/>            |
| ▶ IPsec-Passthrough                |                            | <input checked="" type="checkbox"/> |

Save Undo

### Remote Administrator Host/Port

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



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 elapses 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.

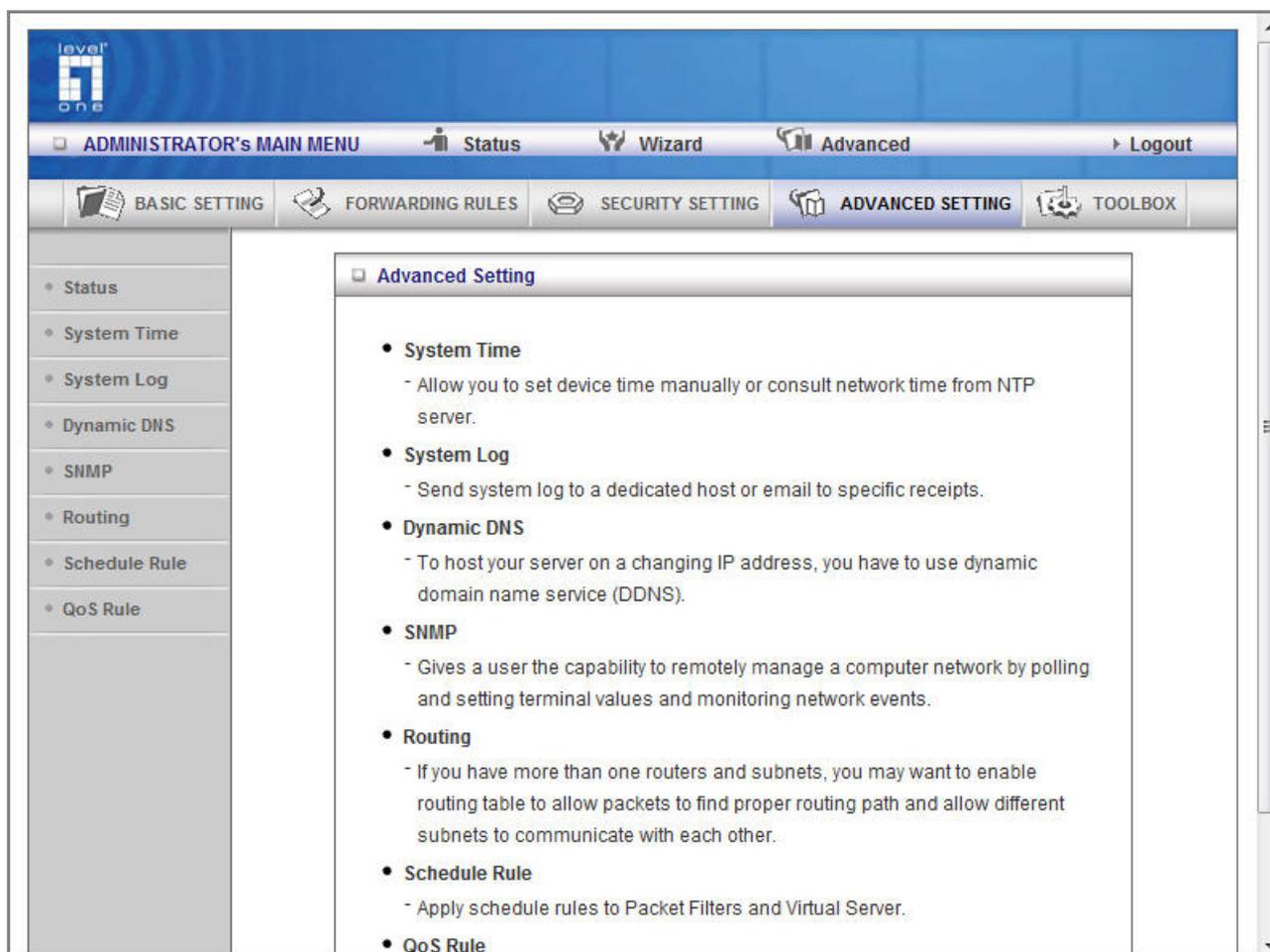
## SPI Mode

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.

## Advanced Settings



# System Time

The screenshot shows a web interface for configuring system time. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists various system settings: Status, System Time, System Log, Dynamic DNS, SNMP, Routing, Schedule Rule, and QoS Rule. The main content area is titled 'System Time' and contains a table with two columns: 'Item' and 'Setting'. The table lists several configuration options, including NTP protocol settings, PC date and time, and manual date and time settings.

| Item   | Setting   |
|--|---|
| System Time  | 2007年11月1日 上午 01:57:50  |
| <input type="radio"/> Get Date and Time by NTP Protocol          | <input type="button" value="Sync Now !"/>                             |
| Time Server  | time.nist.gov   |
| Time Zone  | (GMT-08:00) Pacific Time (US & Canada)                                |
| <input type="radio"/> Set Date and Time using PC's Date and Time |   |
| PC Date and Time   | 2008年1月5日 下午 06:01:09   |
| <input checked="" type="radio"/> Set Date and Time manually      |   |
| Date   | Year: 2007 Month: Nov Day: 01   |
| Time   | Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)                      |
| <input type="radio"/> 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   |

## Get Date and Time by NTP Protocol

Select it 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

Select it if you want to Set Date and Time manually.

## Set Date and Time manually

Select it 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.

## System Log

| Item                                 | Setting  | Enable                   |
|--------------------------------------|--|--------------------------|
| ▶ IP Address for Syslogd             | 192.168.0. <input type="text"/>  | <input type="checkbox"/> |
| ▶ IP Address of Outgoing Mail Server | <input type="text"/> <input type="button" value="Send Mail Now"/>  | <input type="checkbox"/> |
| • SMTP Server IP/Port                | <input type="text"/>   |                          |
| • E-mail addresses                   | <input type="text"/>   |                          |
| • E-mail Subject                     | <input type="text"/>   |                          |
| • User name                          | <input type="text"/>   |                          |
| • Password                           | <input type="text"/>   |                          |
| ▶ Log Type                           | <input checked="" type="checkbox"/> System Activity<br><input checked="" type="checkbox"/> Debug Information<br><input checked="" type="checkbox"/> Attacks<br><input checked="" type="checkbox"/> Dropped Packets<br><input checked="" type="checkbox"/> Notice |                          |

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

### IP Address for Syslog

Host IP of destination where syslogs will be sent to. Check **Enable** to enable this function.

### E-mail Alert Enable

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

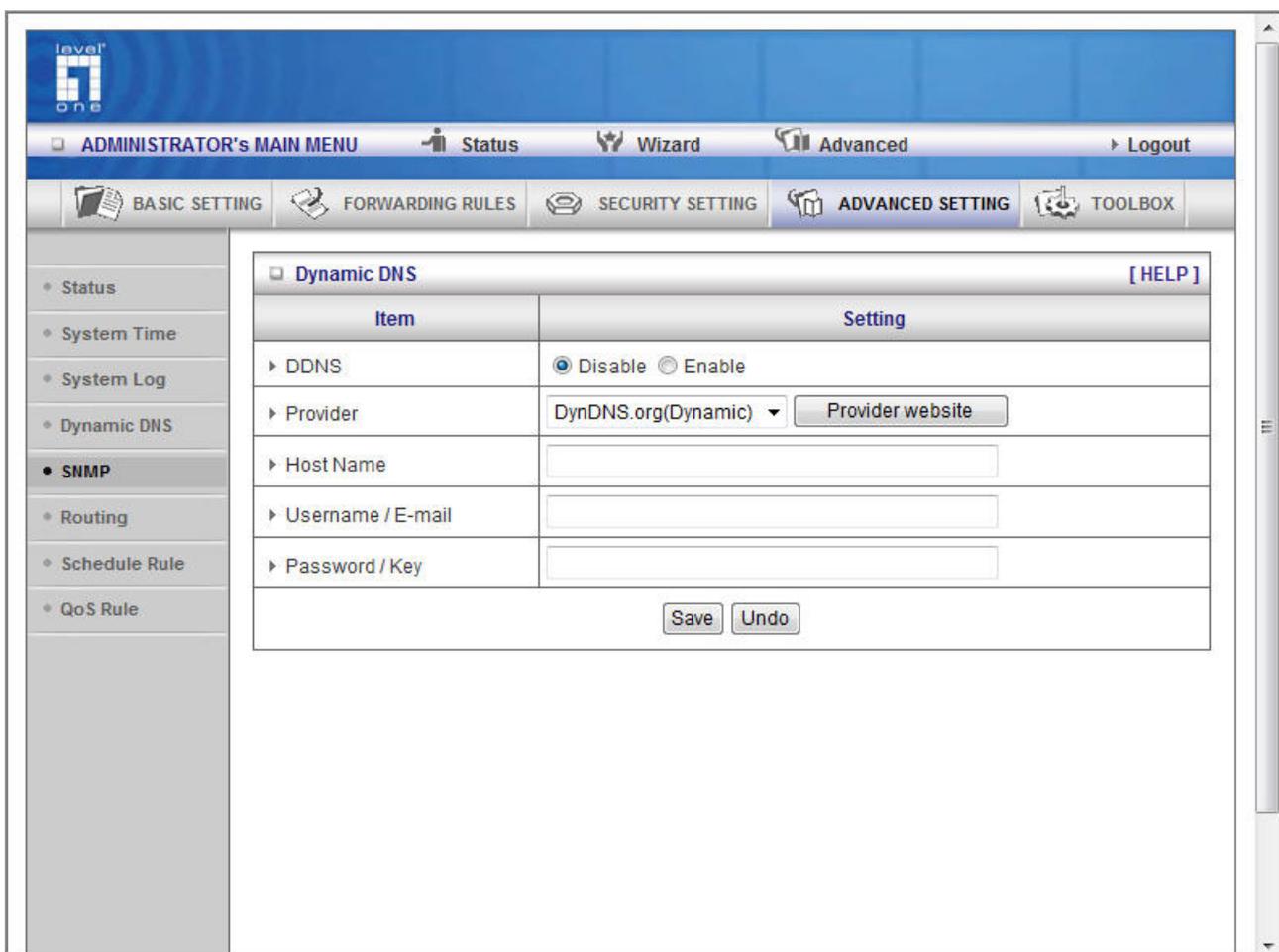
### SMTP Server IP and Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25. For example, "mail.your\_url.com" or "192.168.1.100:26".

## Send E-mail alert to

Send e-mail alert to the recipient who will receive these logs. You can assign more than 1 recipient by using ';' or ',' to separate these email addresses.

## Dynamic DNS



The screenshot shows the Level One administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: Status, System Time, System Log, Dynamic DNS, SNMP (selected), Routing, Schedule Rule, and QoS Rule. The main content area is titled 'Dynamic DNS' and features a table with two columns: 'Item' and 'Setting'. The table contains the following rows:

| 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="text"/>  |

At the bottom of the table are 'Save' and 'Undo' buttons. A '[ HELP ]' link is located in the top right corner of the table area.

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

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

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

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

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

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

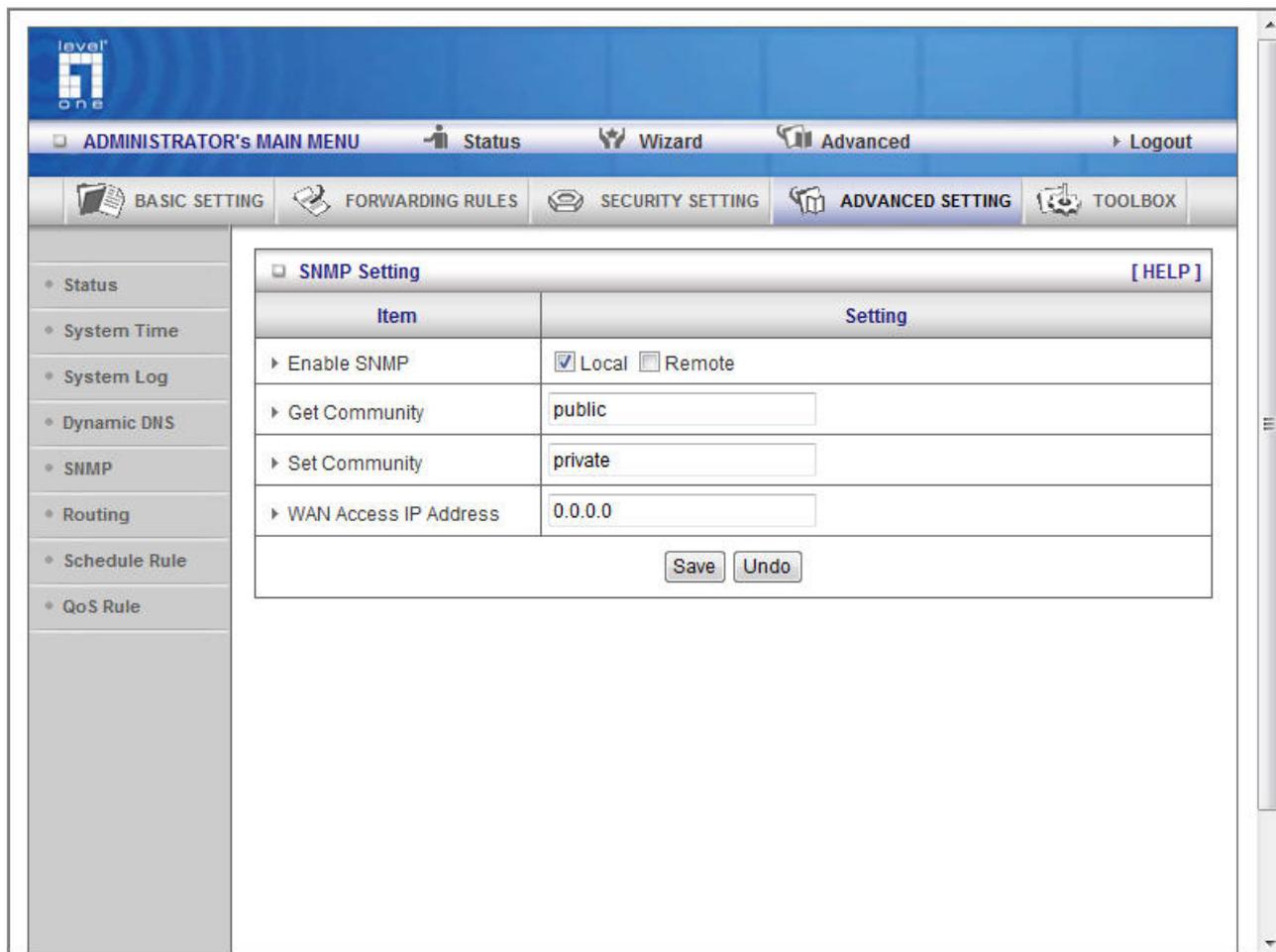
You will get this information when you register an account on a Dynamic DNS server.

**Example:**

| Dynamic DNS [ HELP ]  |   |
|---|---|
| Item  | Setting   |
| ▶ DDNS  | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| ▶ Provider  | DynDNS.org(Dynamic) <input type="button" value="Provider website"/>   |
| ▶ Host Name   | <input type="text" value="levelone.dyndns.org"/>                      |
| ▶ Username / E-mail   | <input type="text" value="service@level1.com"/>                       |
| ▶ Password / Key  | <input type="password" value="....."/>                                |
| <input type="button" value="Save"/> <input type="button" value="Undo"/> |   |

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

## SNMP Setting



The screenshot shows the LevelOne network device configuration interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of settings: Status, System Time, System Log, Dynamic DNS, SNMP, Routing, Schedule Rule, and QoS Rule. The main content area is titled 'SNMP Setting' and contains a table with the following items:

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

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

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

### Enable SNMP

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

### Get Community

Setting the community of Get Request your device will response.

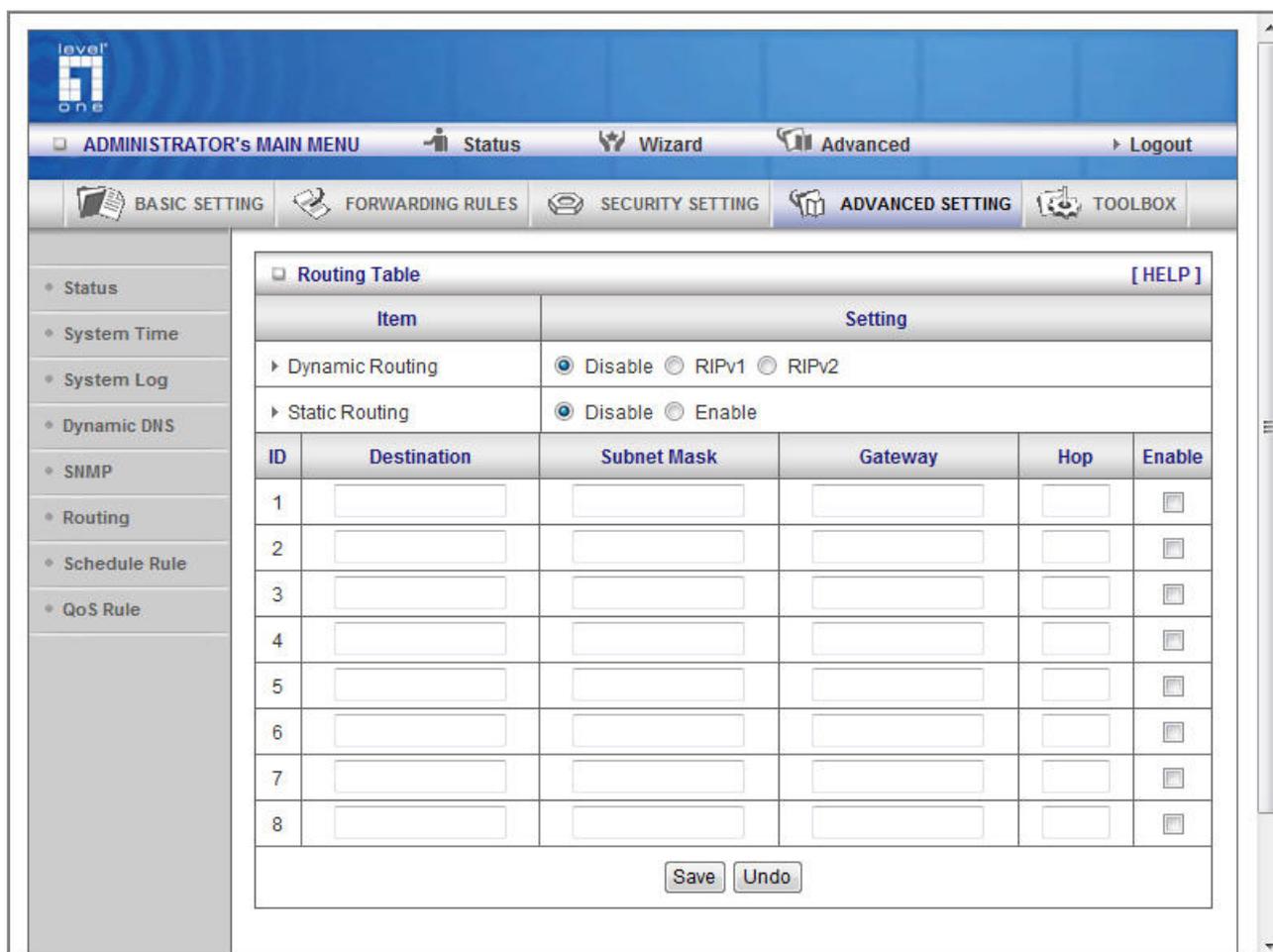
### Set Community

Setting the community of Set Request your device will accept.

### WAN Access IP Address

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

# Routing



**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.

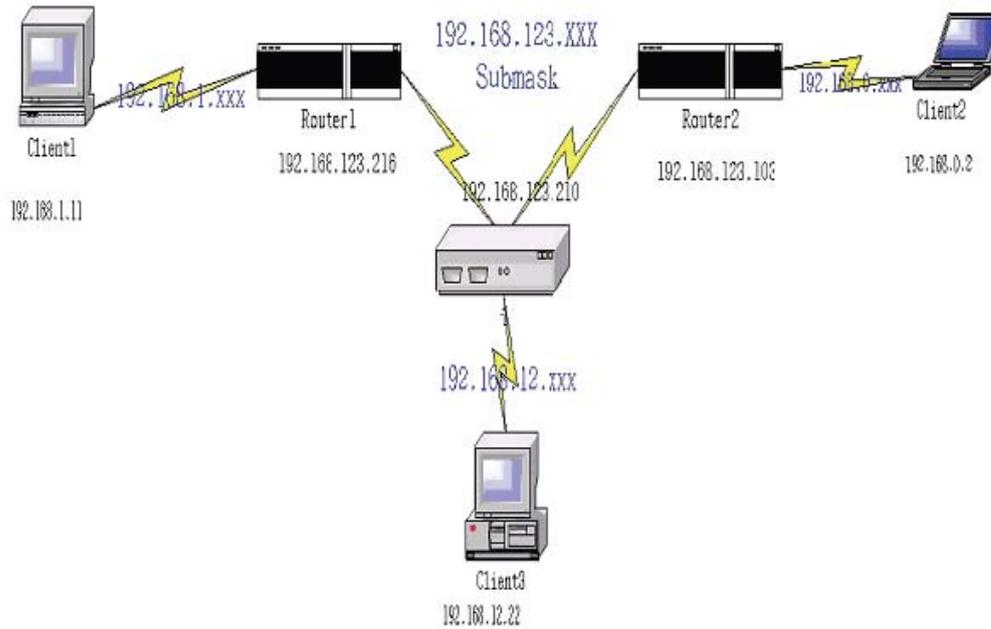
Routing Table settings are settings used to setup the functions of static.

## 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, and hop for each routing rule, and then enable or disable the rule by checking or un-checking 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.

## Schedule Rule

The screenshot shows the LevelOne administrator interface. At the top, there is a navigation bar with the LevelOne logo and the text "ADMINISTRATOR's MAIN MENU". Below this, there are several menu items: "Status", "Wizard", "Advanced", and "Logout". A secondary navigation bar contains "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". On the left side, there is a sidebar menu with the following items: "Status", "System Time", "System Log", "Dynamic DNS", "SNMP", "Routing", "Schedule Rule", and "QoS Rule". The main content area is titled "Schedule Rule" and includes a "[ HELP ]" link. It features a table with two columns: "Item" and "Setting". The "Item" column contains a "Schedule" entry, and the "Setting" column contains an "Enable" checkbox. Below the table, there is a table with three columns: "Rule#", "Rule Name", and "Action". At the bottom of the main content area, there are two buttons: "Save" and "Add New 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

level ONE

ADMINISTRATOR's MAIN MENU   Status   Wizard   Advanced   Logout

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

◦ Status  
◦ System Time  
◦ System Log  
◦ Dynamic DNS  
◦ SNMP  
◦ Routing  
◦ **Schedule Rule**  
◦ QoS Rule

▣ **Schedule Rule Setting** [HELP]

| Item             | Setting                                     |   |
|------------------|---|---|
| ▶ Name of Rule 1 | time-limit                                  |   |
| ▶ System Time    | 2007年11月1日 上午 02:01:34                      |   |
| Week Day         | Start Time (hh:mm)                          | End Time (hh:mm)                            |
| Sunday           | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Monday           | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Tuesday          | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Wednesday        | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Thursday         | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Friday           | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Saturday         | <input type="text"/> : <input type="text"/> | <input type="text"/> : <input type="text"/> |
| Every Day        | 14 : 20                                     | 16 : 30                                     |

Save   Undo   Back

## Schedule Enable

Selected if you want to Enable the Scheduler press **“Edit”**

To edit the schedule rule, press **“Delete”**

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

Schedule Rule can be applied to Virtual server and Packet Filter.

# Qos Rule

The screenshot shows the Level One network management interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of system settings: Status, System Time, System Log, Dynamic DNS, SNMP, Routing, Schedule Rule, and QoS Rule. The main content area is titled 'QoS Rule' and contains a configuration form. At the top of the form, there is a 'QoS Control' section with an 'Enable' checkbox checked. Below this, there are dropdown menus for 'Well known services' (set to '-- select one --') and 'Schedule rule' (set to '(00)Always'). A 'Copy to ID' button and another dropdown are also present. The main part of the form is a table with 8 rows and 6 columns: ID, Local IP, Remote IP : Ports, QoS Priority, Enable, and Schedule Rule#. Each row contains input fields for the first five columns and a '0' in the 'Schedule Rule#' column.

| ID | Local IP             | Remote IP : Ports                           | QoS Priority | Enable                   | Schedule Rule# |
|----|----------------------|---|--------------|--------------------------|----------------|
| 1  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 2  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 3  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 4  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 5  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 6  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 7  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |
| 8  | <input type="text"/> | <input type="text"/> : <input type="text"/> | Normal ▼     | <input type="checkbox"/> | 0              |

## Local IP:

Please input Client IP, Example: 192.168.12.33.

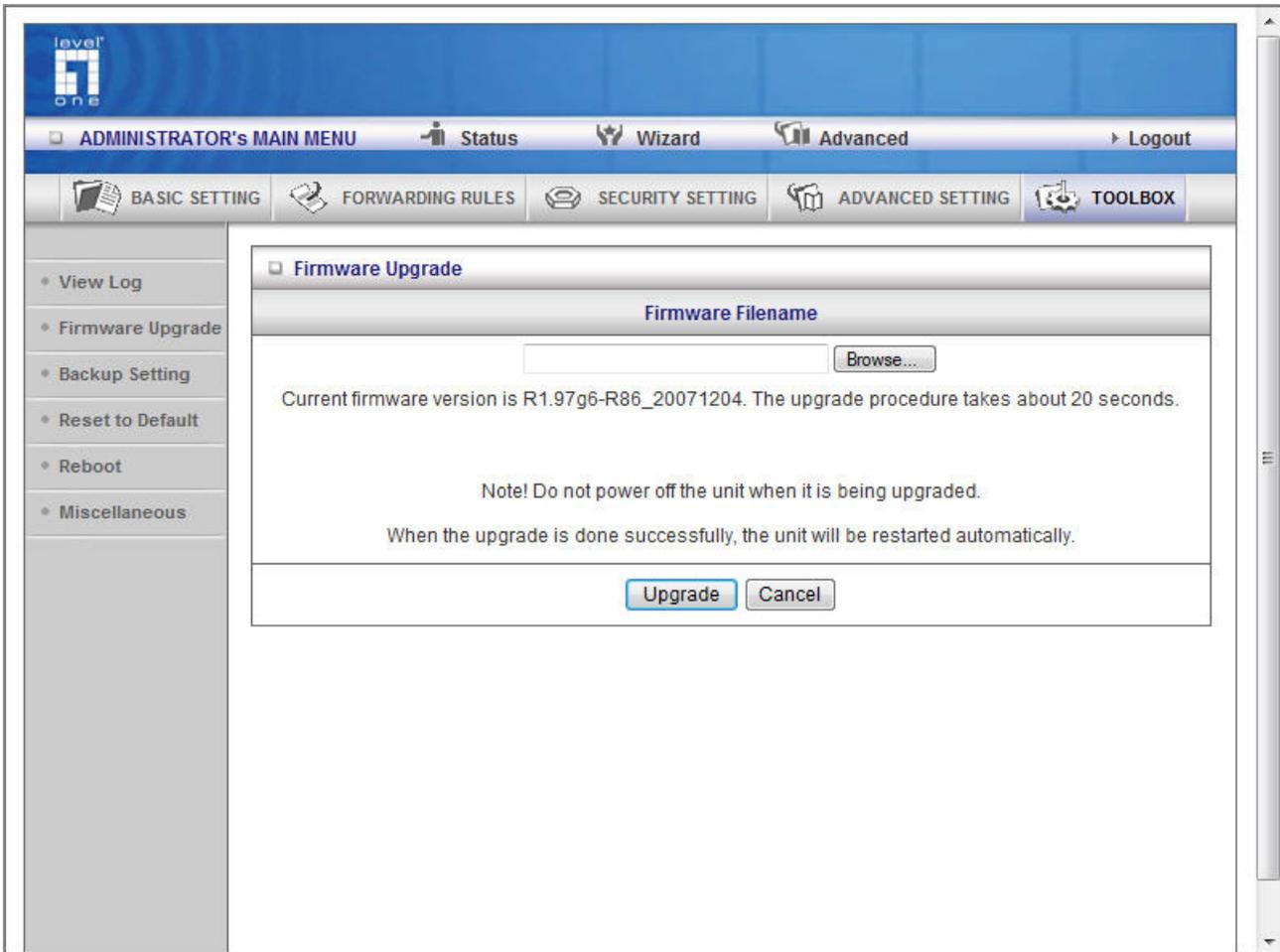
## Remote Priority:

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

# Toolbox

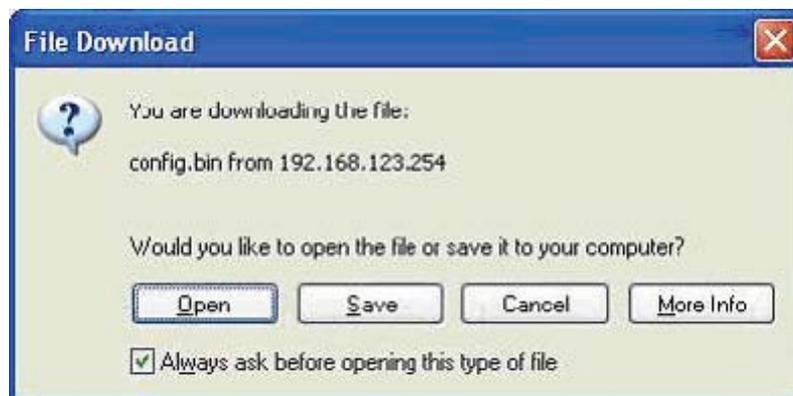
## System Log

## Firmware Upgrade



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

## 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.

## Reset to default



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

## Reboot



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

## Miscellaneous Items

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

### MAC Address for Wake-on-LAN

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

### Domain Name or IP Address for Test

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

# Appendix A 802.1x Setting

---

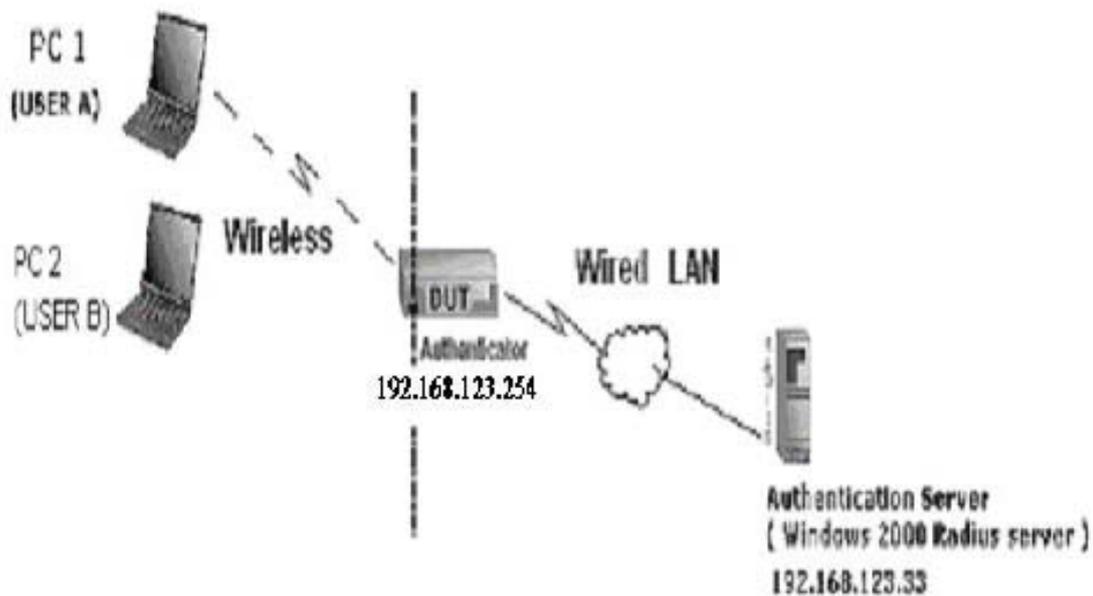


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

## Equipment Details

**PC1:** Microsoft Windows XP Professional without Service Pack 1 and LevelOne Wireless PCI Card

**PC2:** Microsoft Windows XP Professional with Service Pack 1a or latter and LevelOne Wireless PCI Card.

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



Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 (You can get more information from

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

## DUT Configuration:

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

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

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

Setup Windows 2000 RADIUS Server

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

### **Setup DUT**

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

### **Setup Network adapter on PC**

1. Choose the IEEE802.1X as the authentication method. (Fig 2)
2. Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
3. If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer.
4. We will change EAP type to fit the variable test condition.



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



Figure 2: Enable IEEE 802.1X access control / Smart card or certificate properties

### Windows 2000 RADIUS server Authentication testing:

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

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

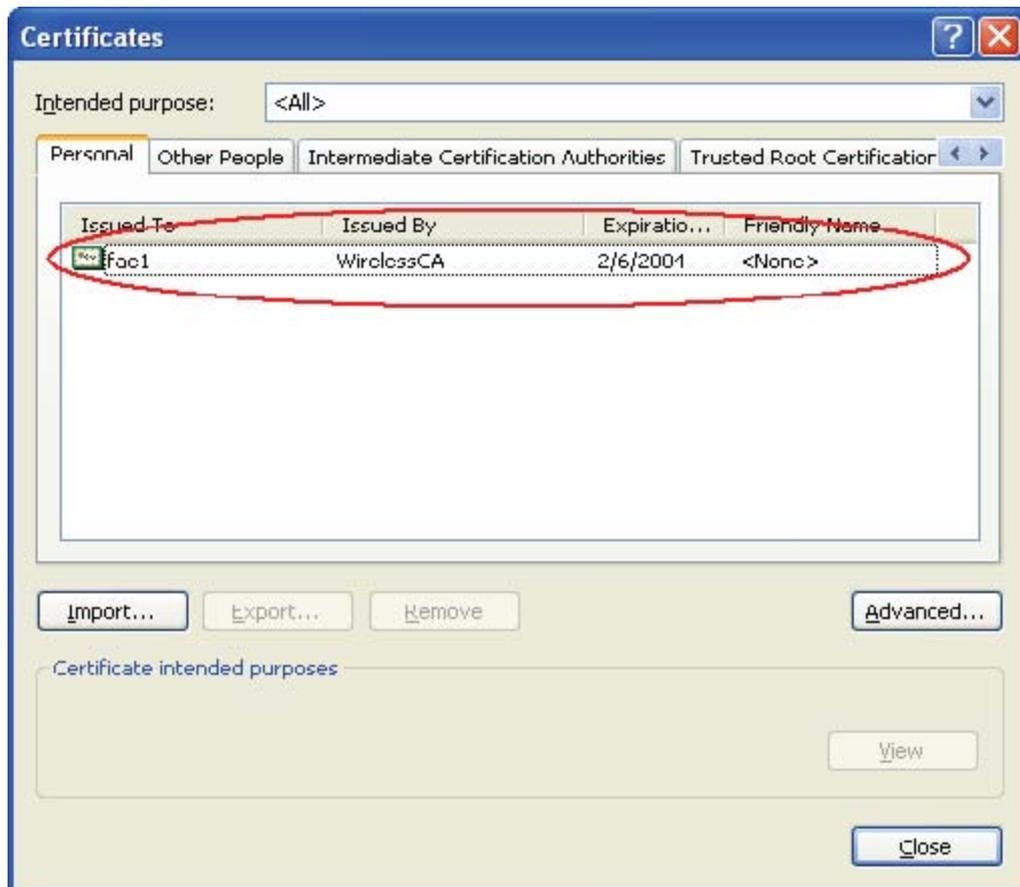


Figure 4: Certificate information on PC1

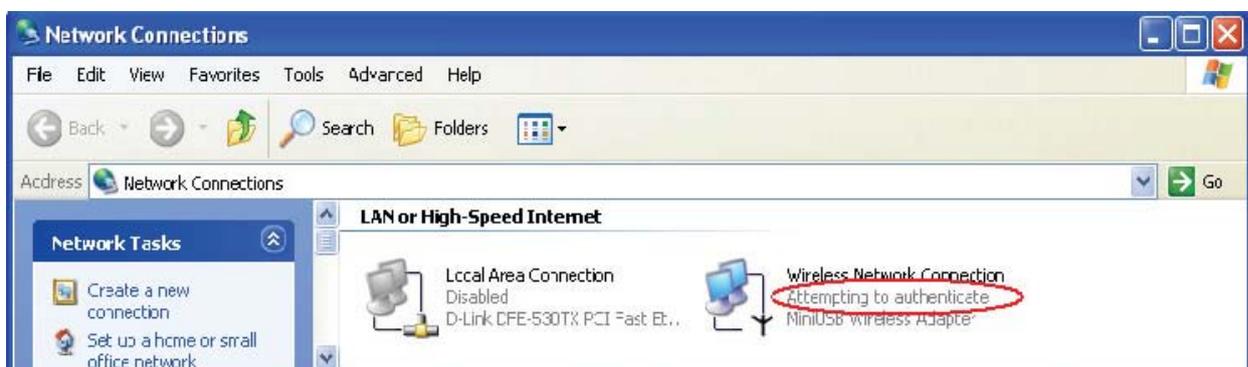


Figure 5: Authenticating

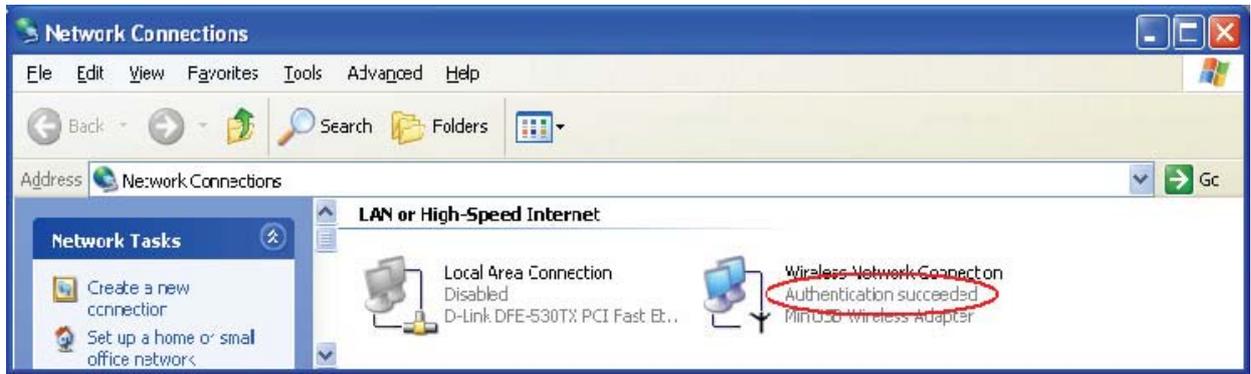


Figure 6: Authentication success

DUT authenticate PC2 using PEAP-TLS.

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

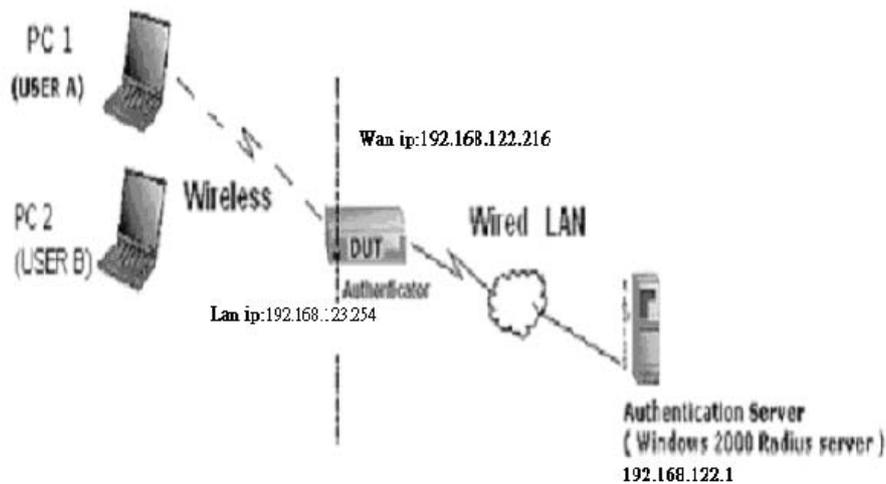
**Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.**



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

## Appendix B WPA-PSK and WPA

---



Wireless Router: LAN IP: 192.168.123.254

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

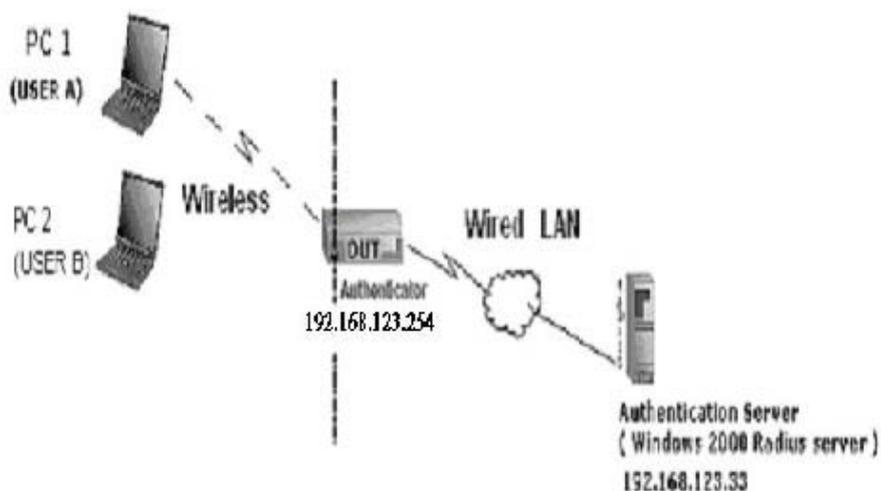
User A: XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

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

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

Or Another Configuration:



### WPA-PSK

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

Method1:

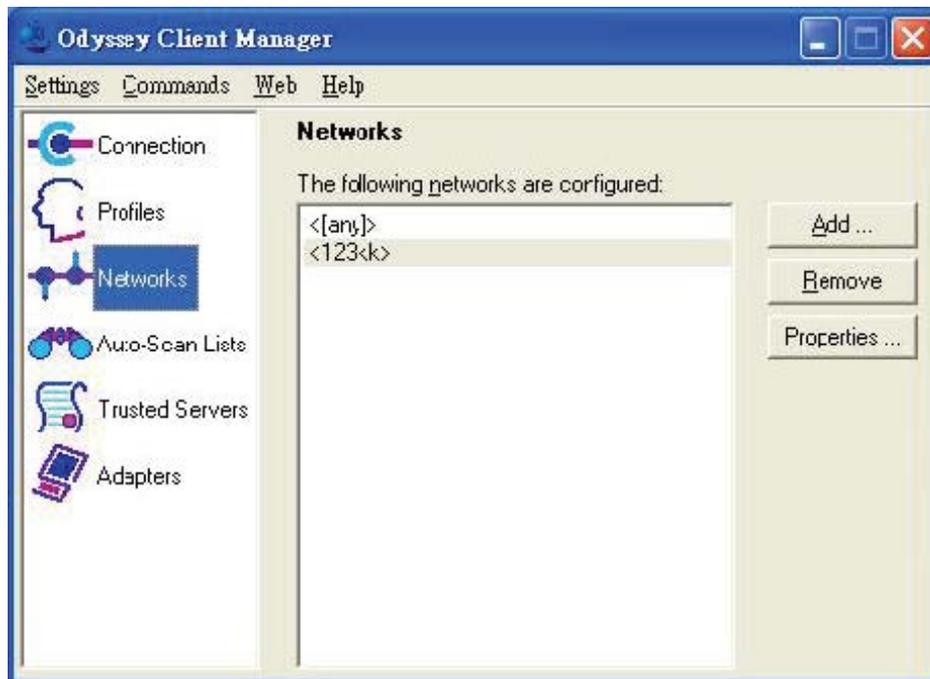
1. Go to the Web manager of Wireless Router to configure, like below:

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

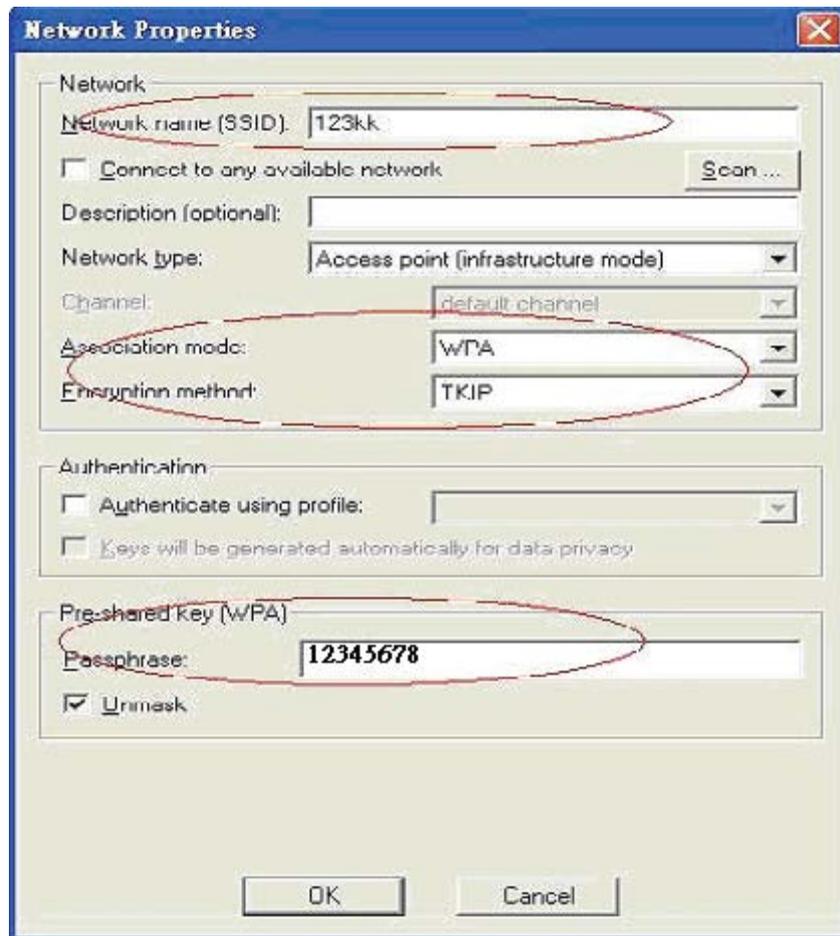
2. Go to Odyssey Client Manager, first choose "Network"

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

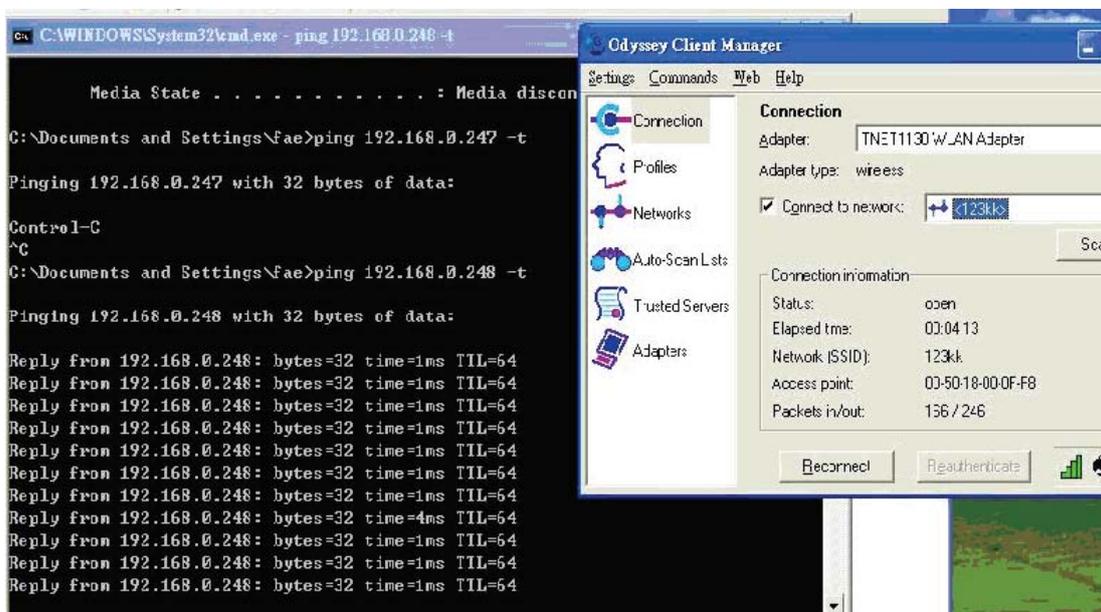
Open "Adapters"



3. Add and edit some settings:



4. Back to Connection:  
Then Select "Connect to network" You will see:



Method2:

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

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

2. Then reboot.

3. Setting on the router and client:

Router:

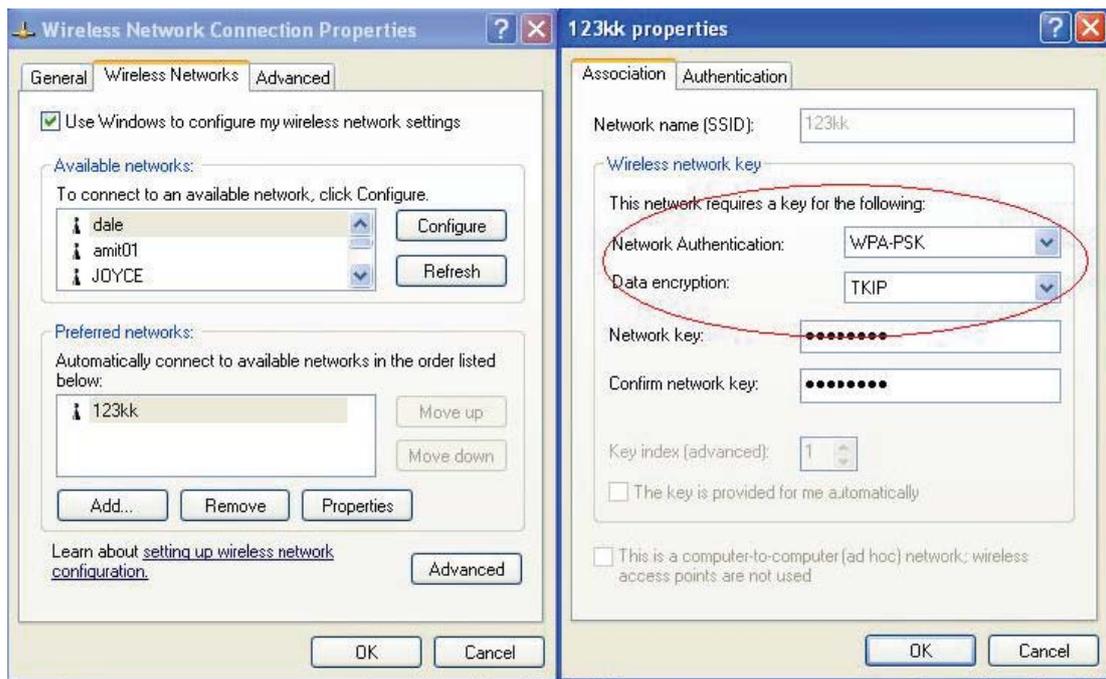
|                  |          |
|------------------|----------|
| Network ID(SSID) | 123kk    |
| Channel          | 8        |
| Security         | WPA-PSK  |
| Key Mode         | ASCII    |
| Preshare Key     | 12345678 |

Client:

Go to “Network Connection” and select wireless adapter.

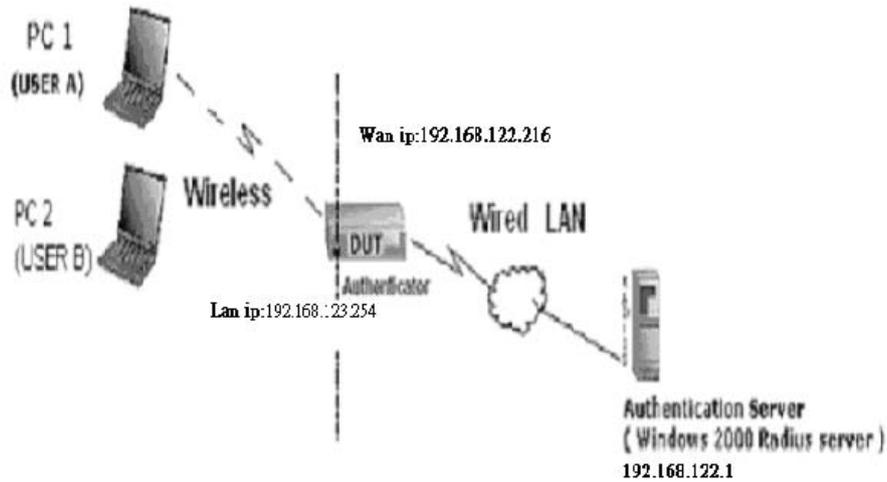
Choose “View available Wireless Networks” like below:

Advanced choose “123kk”



**WPA:**

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



The above is our environment:

Method 1:

1. The User A or User B have to get certificate from Radius, first.

<http://192.168.122.1/certsrv>

Account: fae1

Password: fae1



2. Then, Install this certificate and finish.

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

|                  |       |
|------------------|-------|
| Network ID(SSID) | 123kk |
| Channel          | 8     |
| Security         | WPA   |

#### 802.1X Settings

|                   |               |
|-------------------|---------------|
| RADIUS Server IP  | 192.168.122.1 |
| RADIUS port       | 1812          |
| RADIUS Shared Key | costra        |

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

**Add Profile**

Profile name: 1

User Info | **Authentication** | ITLS Settings | PEAP Settings

Login name: fae1

Password

Permit login using password

use Windows password

prompt for password

use the following password:

fae1

Unmask

Certificate

Permit login using my certificate:

fae1

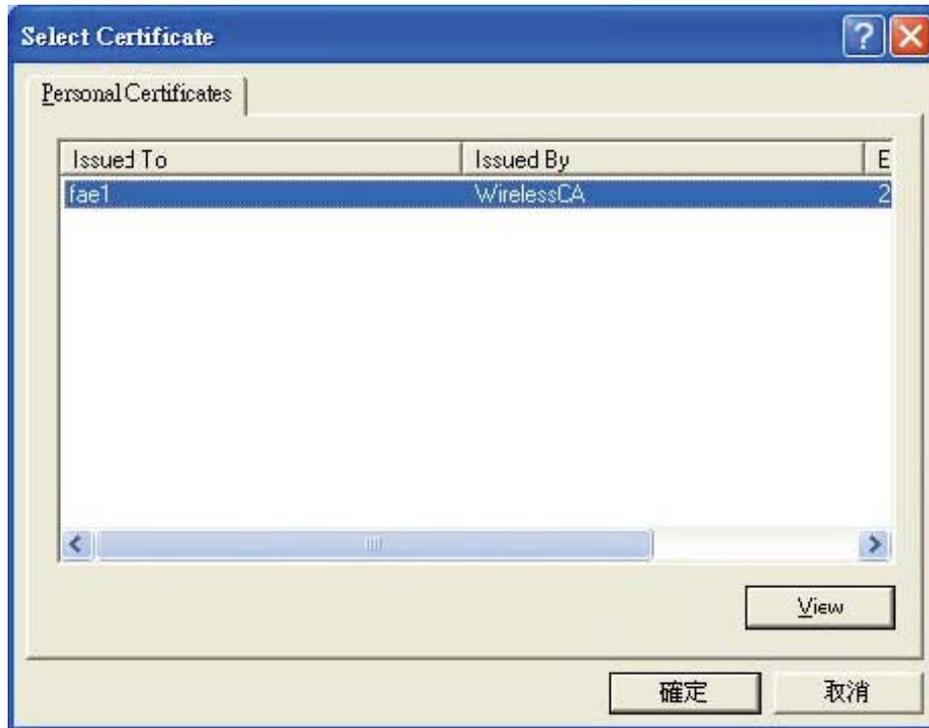
View ... Browse ...

OK Cancel

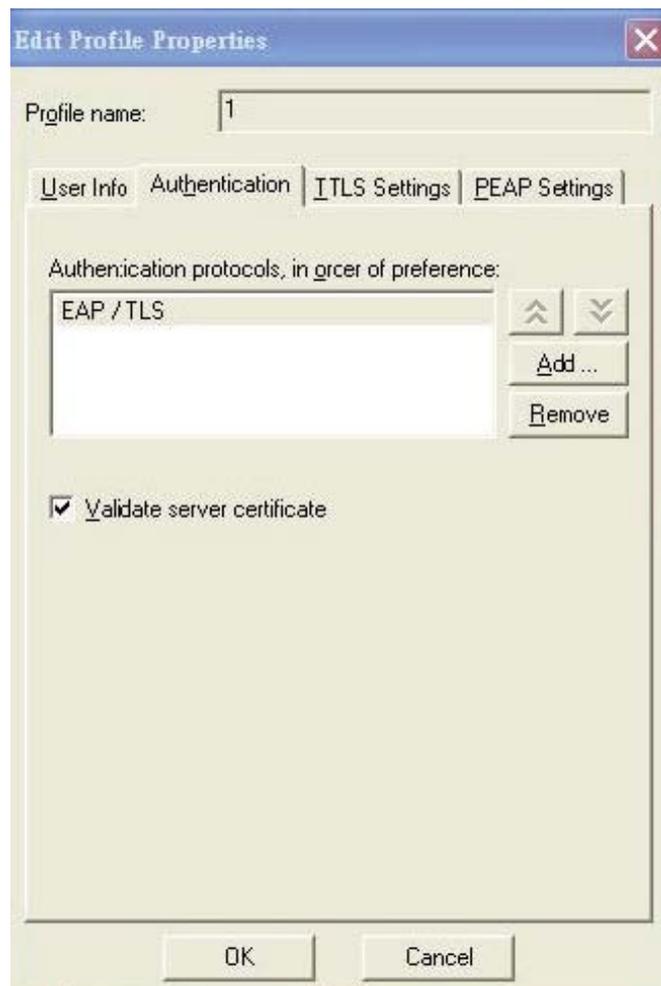
Login name and passwd are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

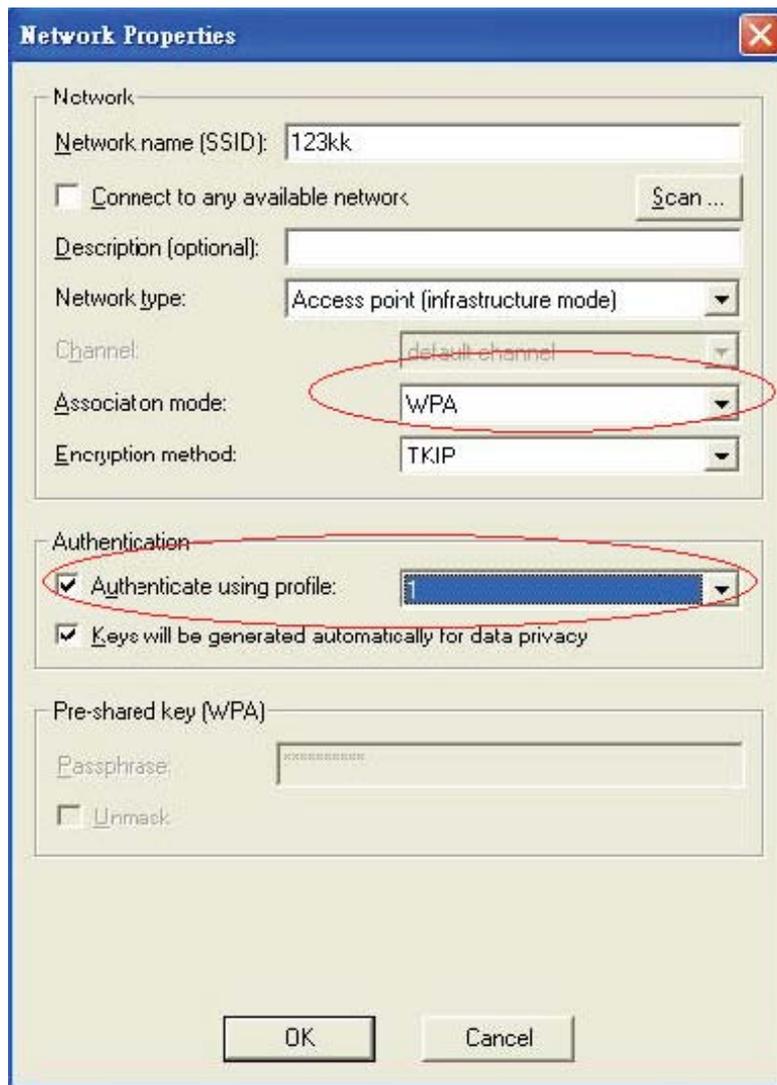
5. Then Choose "certificate" like above.



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

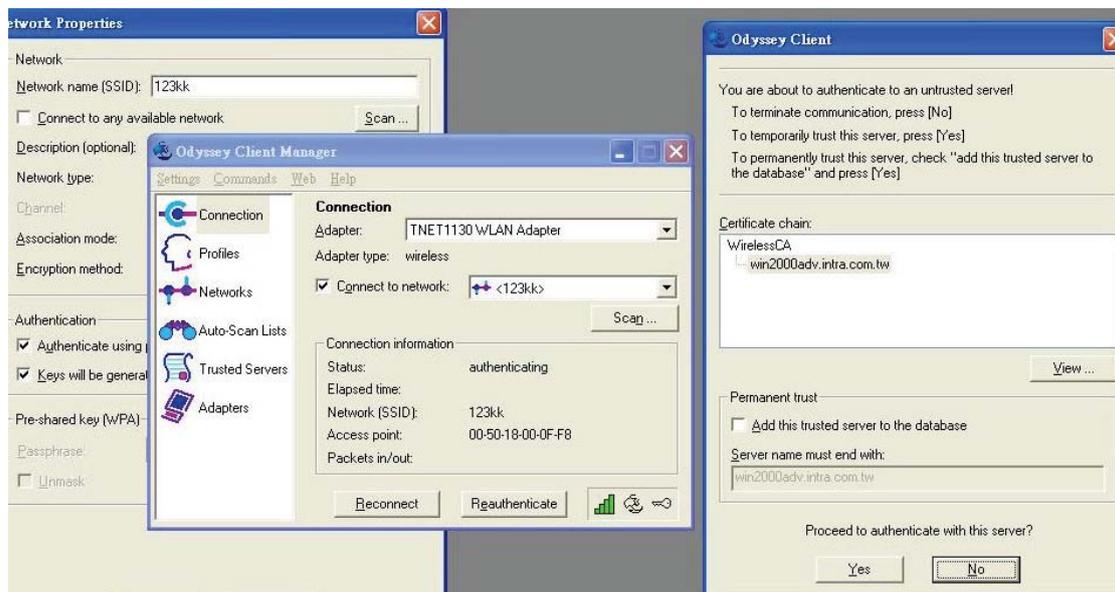


7. Go "Network" and Select "1" and ok

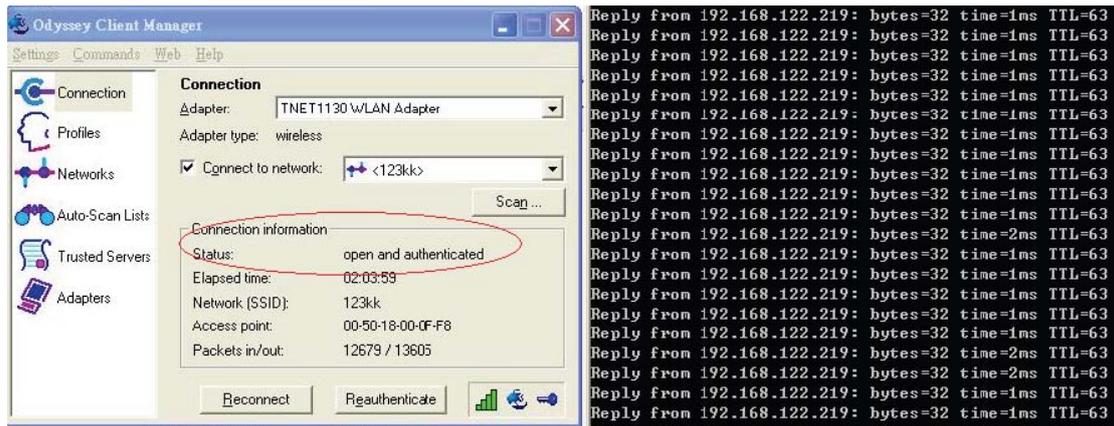


8. Back to Connection and Select "123kk."

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



## 9.Result:



## Method 2:

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

<http://192.168.122.1/certsrv>

Account: fae1

Password: fae1



2. Then Install this certificate and finish.

3. Setting on the router and client:

Router:

|                   |       |
|-------------------|-------|
| Network ID (SSID) | 123kk |
| Channel           | 8     |
| Security          | WPA   |

#### 802.1X Settings

|                   |               |
|-------------------|---------------|
| RADIUS Server IP  | 192.168.122.1 |
| RADIUS port       | 1812          |
| RADIUS Shared Key | costra        |

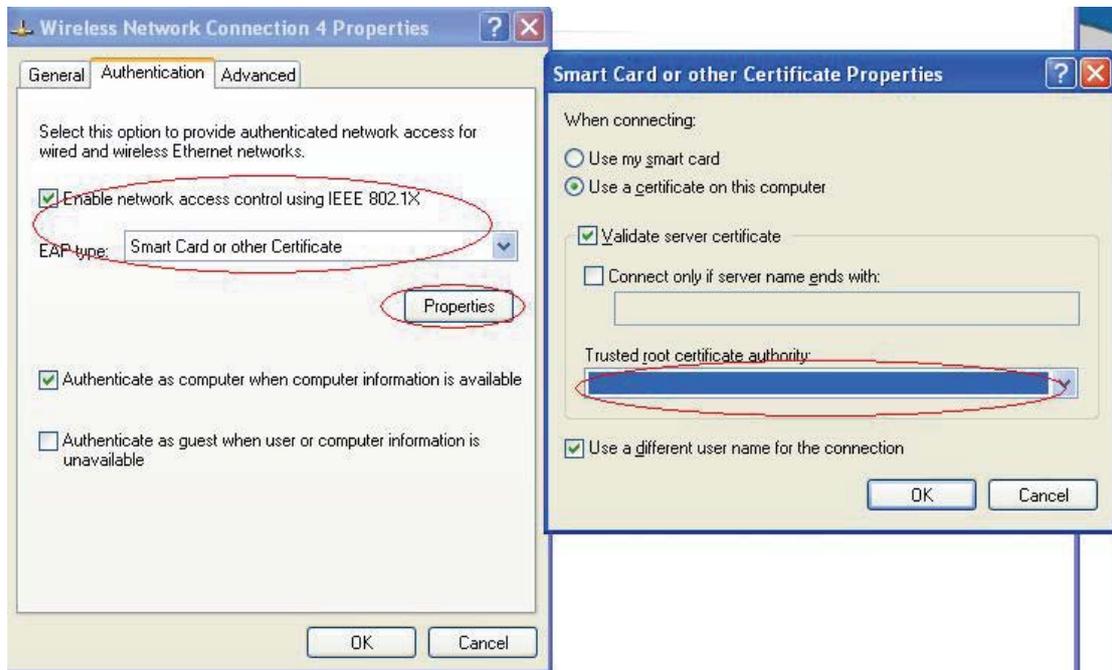
Client:

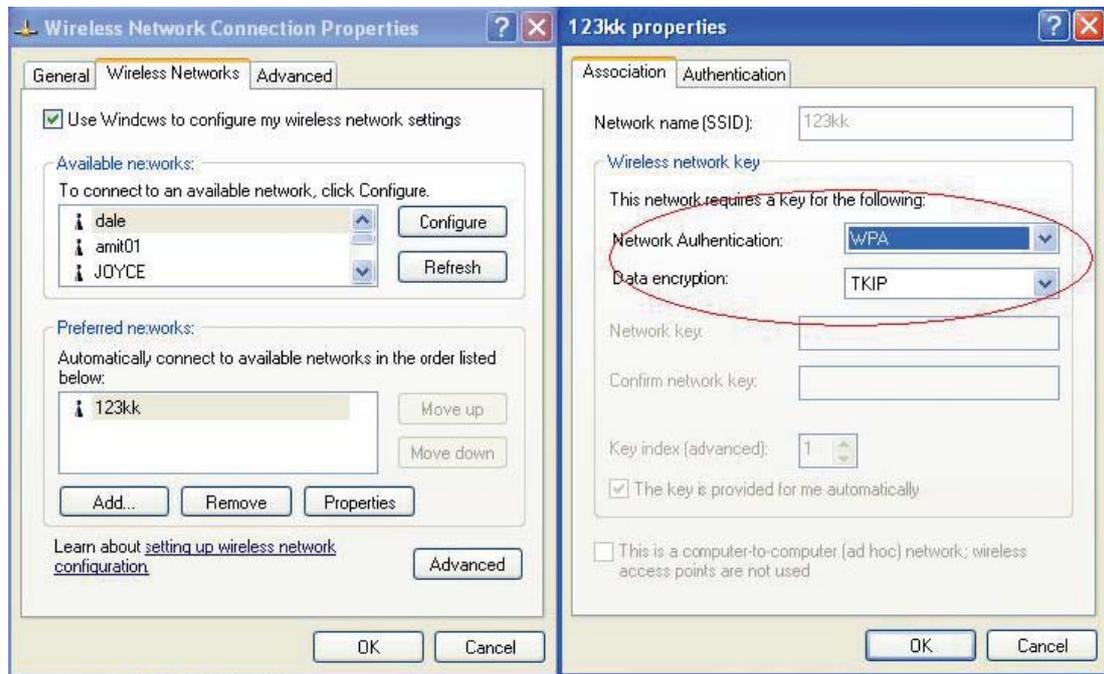
Go to "Network Connection" and select wireless adapter.

Choose "View available Wireless Networks" like below:

Advanced choose "123kk"

Select "WirelessCA and Enable" in Trusted root certificate authority:





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

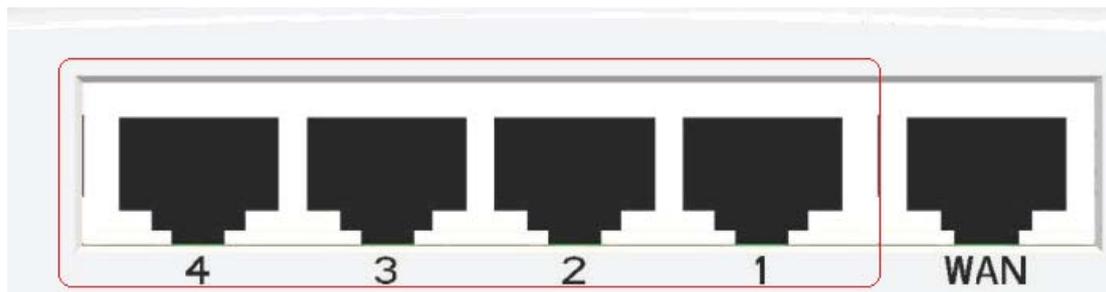
# Appendix C FAQ and Troubleshooting

---

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

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

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



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

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

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

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

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

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

## **2. Why can I not connect the router even if the cable is plugged in LAN port and the led is light?**

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

If not, please check the blinking Status led shows.

There are many abnormal symptoms as below:

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

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

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

## **3. How to reset to factory default?**

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

### **Method 1) Restore with RESET button**

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

### **Method 2) Restore directly when the router power on**

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

## **4. 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 of 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?

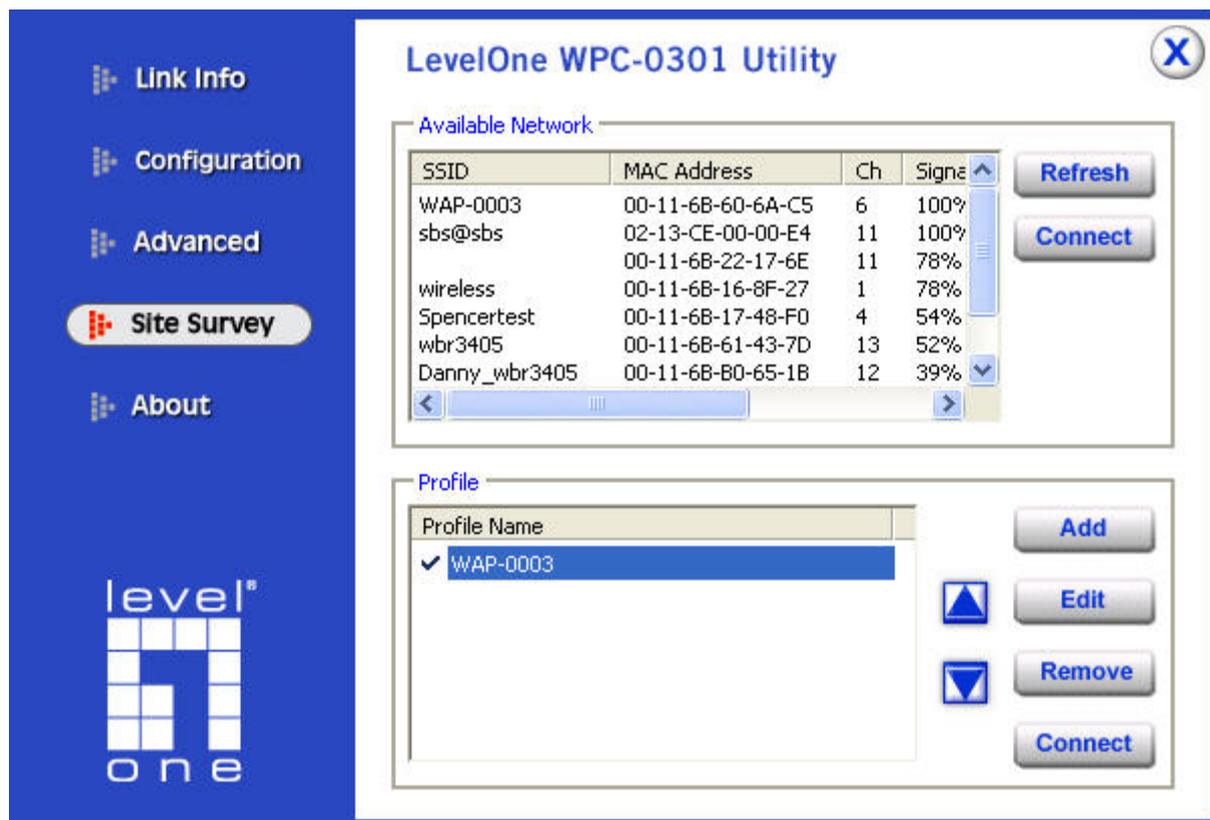
**A:** First, make sure that you already installed wireless client device in your computer. Then check the configuration of wireless router. The default is as below:

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

About wireless client, you will see wireless icon:



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



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

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

If successfully, the computer will show



User will also retrieve IP from router:

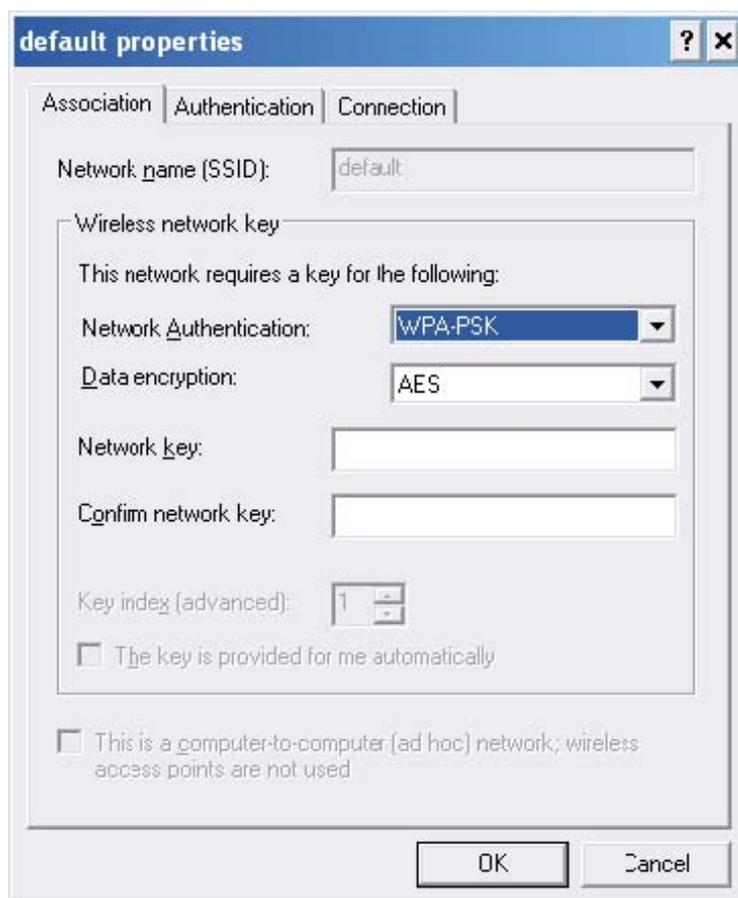
```
Ethernet adapter Wireless Network Connection 5:  
Connection-specific DNS Suffix . :  
IP Address . . . . . : 192.168.123.165  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.123.254
```

## 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.

# Technical Specifications

## General

|                    |   |
|--------------------|---|
| Model              | WBR-6001 <i>N_Max</i> Wireless Broadband Router   |
| Data Transfer Rate | 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps<br>Max physical rate up to 300 Mbps in 802.11n mode |
| Transmit Power     | 802.11b: 17±2dBm<br>802.11g: 15±2dBm<br>802.11n: 14±2dBm  |
| Frequency Range    | America/ FCC: 2.412~2.462GHz (11 Channels)<br>Europe/ ETSI: 2.412~2.472GHz (13 Channels)            |
| Modulation Schemes | DBPSK/DQPSK/CCK/OFDM  |
| Channels           | 1~11 channels (FCC), 1~13 channels (ETSI),<br>1~14 channels (MCK-Japan)                             |
| Security           | 64/128-bits WEP Encryption, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.x                                     |
| Diagnostic LED     | <b>Reset</b><br><b>Status</b><br><b>WAN</b><br><b>WLAN</b><br>LAN LEDs                              |
| Antenna            | 1.8dBi dipole antenna * 2   |

## Physical and Environmental

|                |  |
|----------------|--|
| Driver Support | Windows 2000, Windows XP, Windows Vista      |
| Temperature    | Operating: 0° ~ 40° C, Storage: -10° ~ 70° C |
| Humidity       | 10% ~ 95% RH, no condensation                |
| Dimensions     | 170mm (W) x 30(H) x 110 (D)                  |
| Certifications | FCC, CE                                      |