



LevelOne

User Manual

WGR-6013

300Mbps Wireless Gigabit Router

Ver. 1.0

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 product 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>



General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at <http://global.level1.com>.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US\$9.99 plus the cost of shipping.

Table of Contents

| | | |
|------------|---|----|
| Chapter 1 | Introduction | 5 |
| 1.1 | Packing List | 5 |
| 1.2 | Spec Summary Table | 5 |
| 1.3 | Hardware Configuration..... | 7 |
| 1.4 | LED indicators..... | 8 |
| 1.5 | Button Definition..... | 9 |
| 1.6 | Procedure for Hardware Installation | 9 |
| Chapter 2 | Getting Start..... | 11 |
| Chapter 3 | Making Configuration | 17 |
| 2.1 | Login to Configure from Wizard..... | 18 |
| 2.2 | System Status | 23 |
| 2.3 | Advanced | 24 |
| Appendix A | FAQ and Troubleshooting | 89 |
| | What can I do when I have some trouble at the first time? | 89 |
| | How do I connect router by using wireless? | 91 |

| | |
|-------------------|-------------|
| IP Address | 192.168.1.1 |
| Password | admin |
| Wireless Mode | Enable |
| Wireless SSID | LevelOne |
| Wireless Security | None |

Chapter 1 Introduction

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

1.1 Packing List

WGR-6013

Power Adapter

RJ-45 LAN Cable

Quick Installation Guide

CD Manual/QIG

Antenna

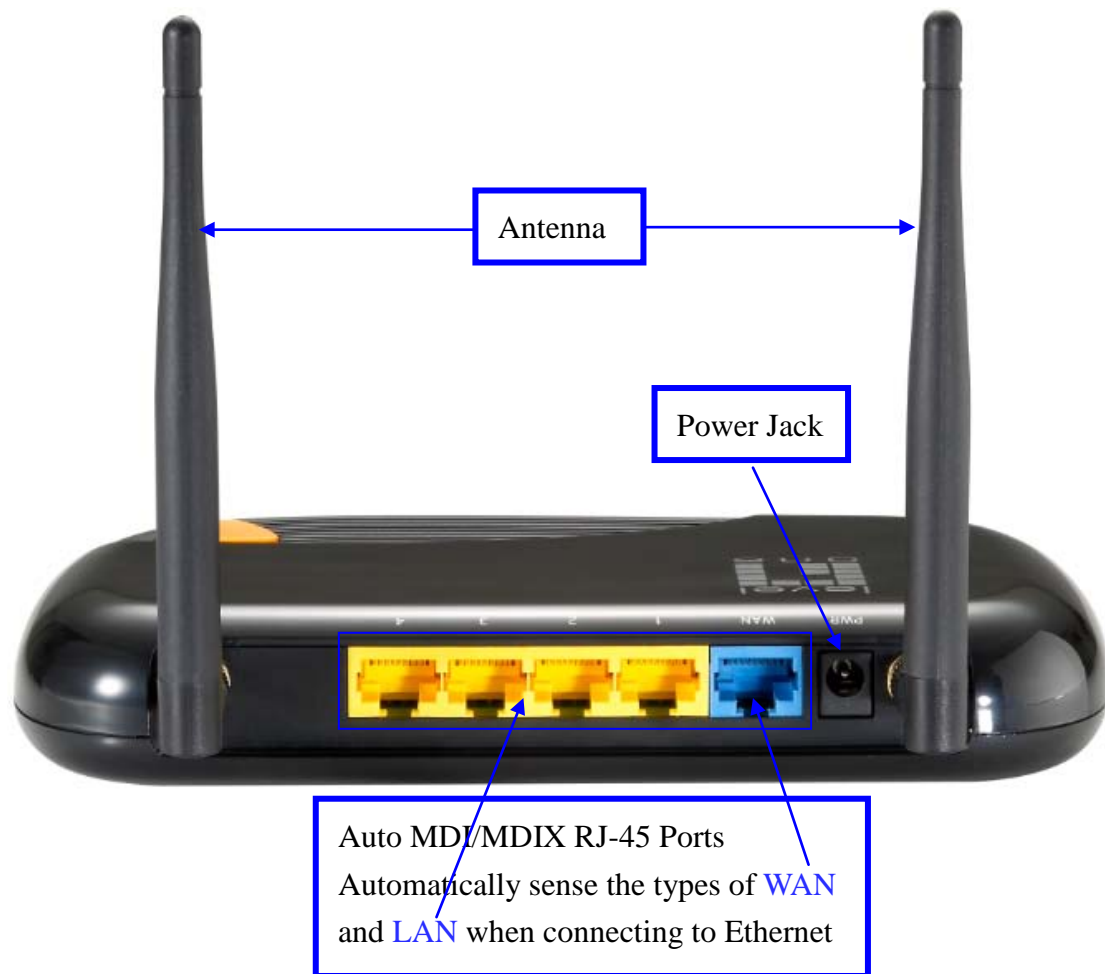
1.2 Spec Summary Table

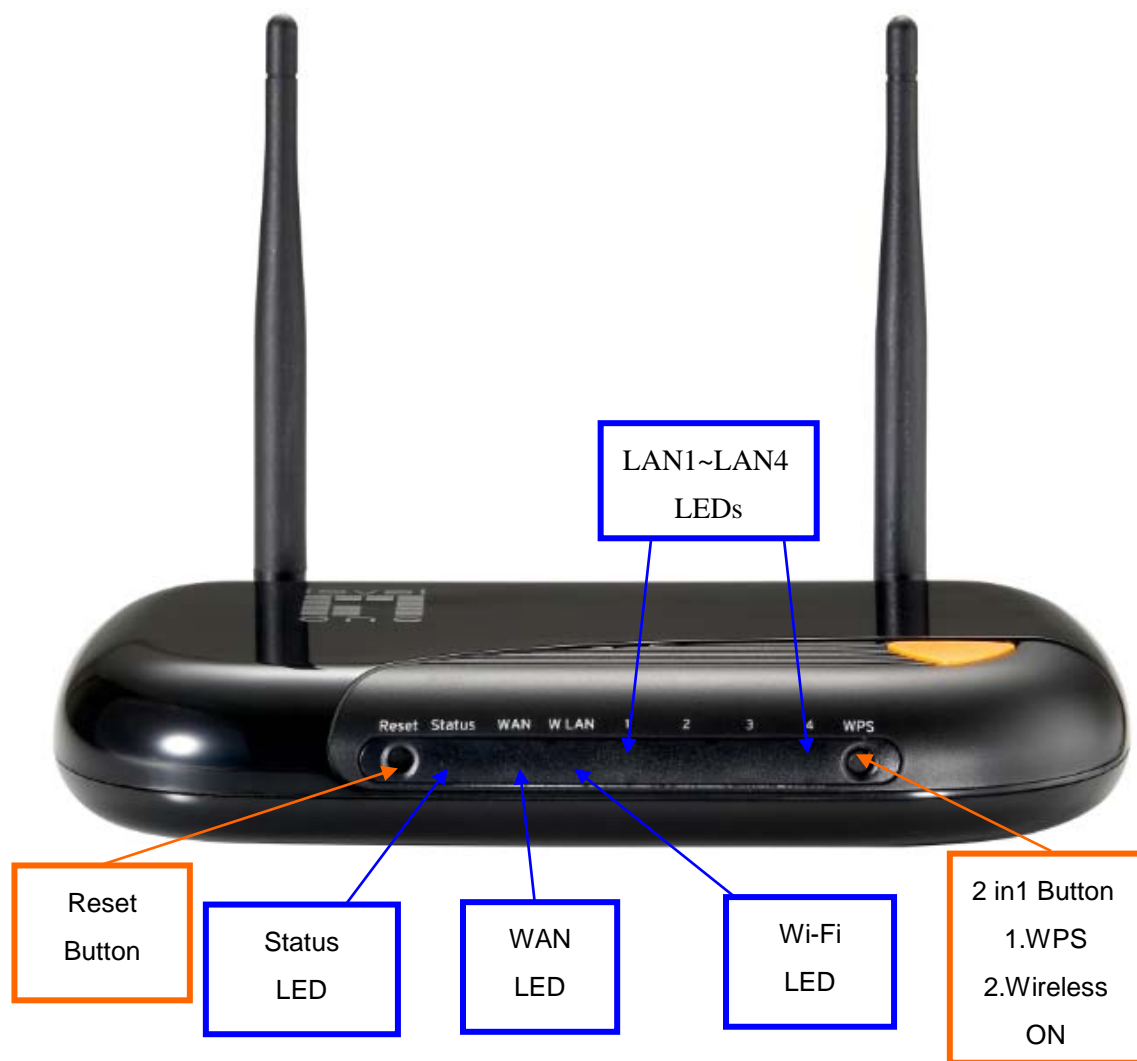
| Device Interface | |
|---------------------|--|
| Ethernet WAN | 1 x RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX |
| Ethernet LAN | 4 x RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX |
| Antenna | 2 dBi detachable antenna |
| WPS Button | For WPS connection |
| Reset Button | Reset router setting to factory default |
| LED Indication | Power/Status / WAN / LAN1 ~ LAN4/ WiFi |
| Power Jack | DC Power Jack, powered via external DC 5V/1.2A switching power adapter |
| Wireless LAN (WiFi) | |
| Standard | IEEE 802.11b/g/n compliance |
| SSID | SSID broadcast or in stealth mode |
| Channel | Auto-selection, manually |
| Security | WEP, WPA, WPA-PSK, WPA2, WPA2-PSK |
| WPS | WPS (Wi-Fi Protected Setup) |
| WMM | WMM (Wi-Fi Multimedia) |

| Functionality | |
|-----------------------------|--|
| Ethernet WAN | PPPoE, DHCP client, Static IP |
| WAN Connection | Auto-reconnect, dial-on-demand, manually |
| One-to-Many NAT | Virtual server, special application, DMZ, Super DMZ(IP pass-through) |
| NAT Session | Support NAT session(20000) |
| SPI Firewall | IP/Service filter, URL blocking, Internet Access Control |
| DoS Protection | DoS (Deny of Service) detection and protection |
| Routing Protocol | Static route, dynamic route (RIP v1/v2) |
| Management | SNMP, UPnP IGD, syslog, DDNS |
| Administration | Web-based UI, remote login, backup/restore setting |
| Performance | NAT up to 700Mbps and Wireless up to 150Mbps |
| Environment & Certification | |
| Package Information | Device dimension (mm) 185x119x32 |
| Operation Temp. | Temp.: 0~40°C, Humidity 10%~90% non-condensing |
| Storage Temp. | Temp.: -10~70°C, Humidity: 0~95% non-condensing |
| EMI Certification | CE/FCC compliance |
| RoHS | RoHS compliance |

*Specifications are subject to change without prior notice.

1.3 Hardware Configuration





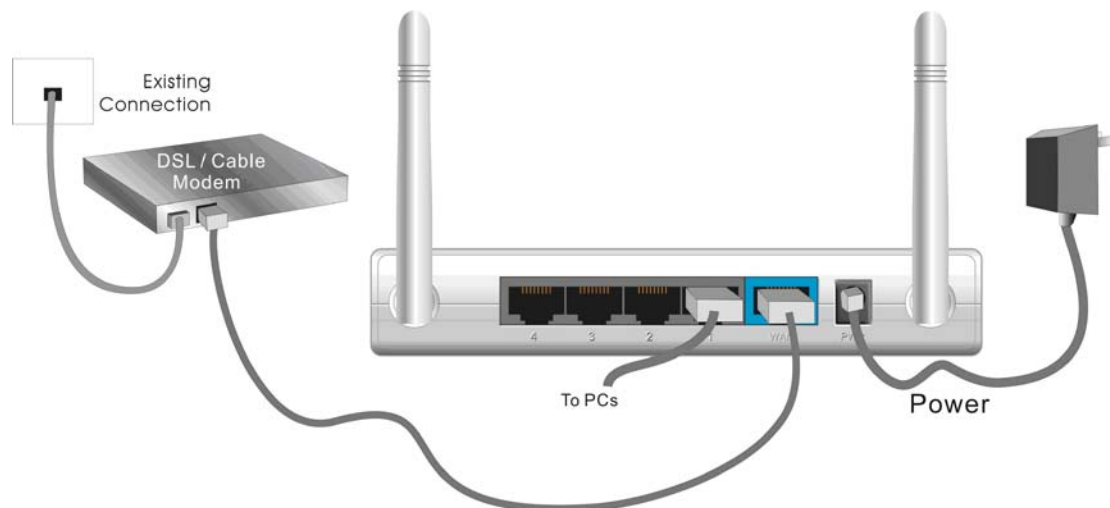
1.4 LED indicators

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

1.5 Button Definition

| | Description |
|-------------|--|
| WPS | When Wireless is On, press this button (about 1 sec) to execute WPS function. |
| Wireless On | When Wireless is off depend as Schedule Rule, Press this button(about 5 sec) to enable "Wireless Radio". |
| Reset | <ol style="list-style-type: none">1. Press this button then Power on the device2. Press about 6 second, the device will reset to default then Status LED flashes per sec in Normal status. Notice: If Status LED flashes very fast, it means to press this button too long and please try again. |

1.6 Procedure for Hardware Installation



Step 1 Insert the Ethernet cable into LAN

Port:

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



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

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



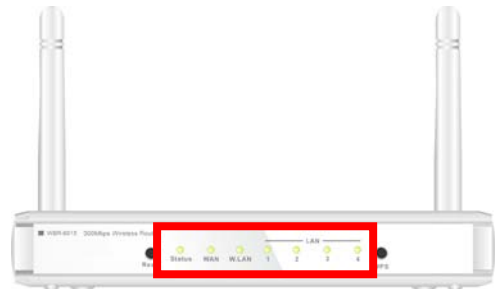
Step 3. Power on Router:

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



Step 4. Complete the setup.

When complete, the Status LED will flash.



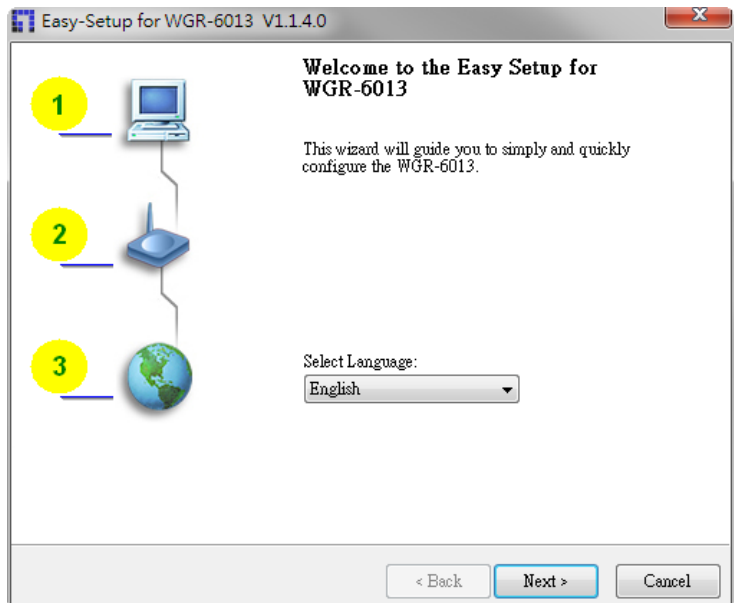
Chapter 2 Getting Start

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

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

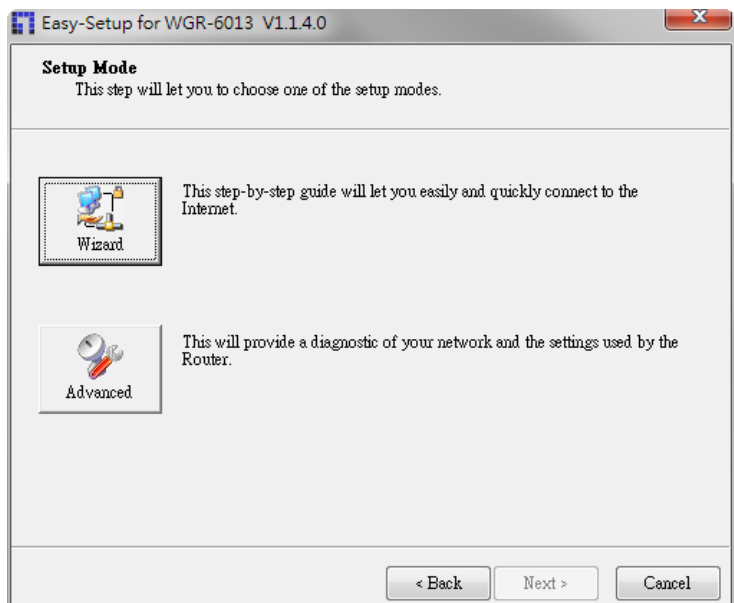
Configure the settings by the following steps.

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



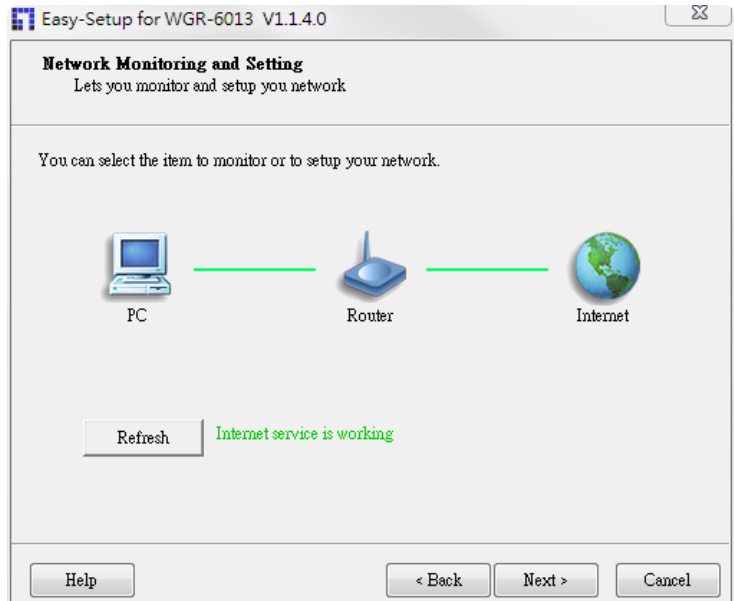
2.2 Setup mode

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



2.3 Advanced mode Setup.

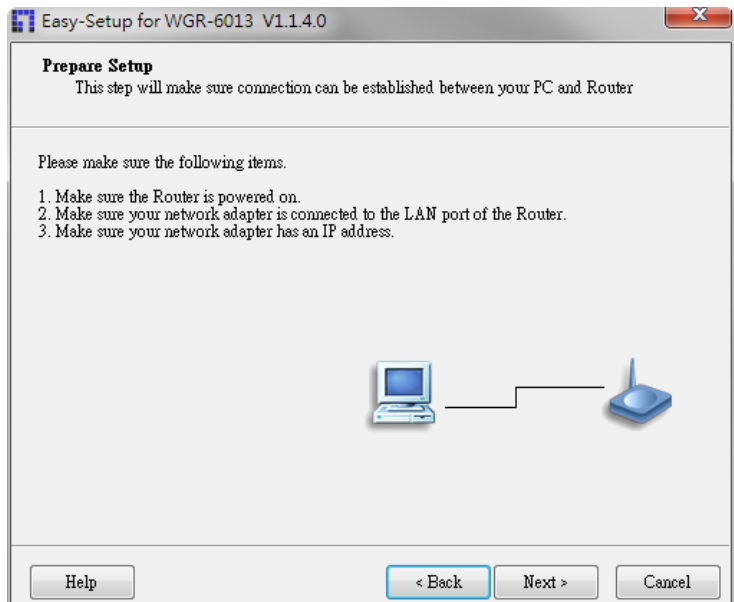
Check the PC, Router or Internet icons for the Status of PC, Router or Internet.



2.4 Quick Wizard Install mode Setup

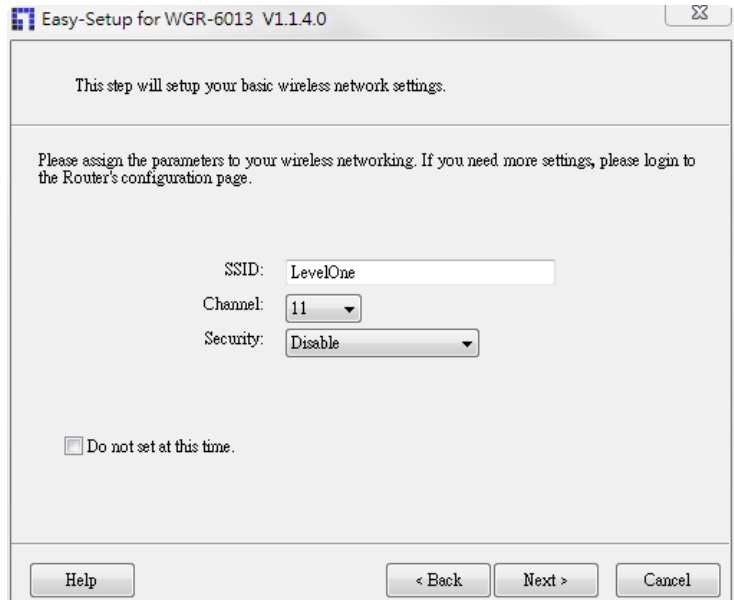
1. Make sure the router is powered on.
2. Make sure your network adapter is connected to the LAN port of the router
3. Make sure your network adapter has an IP address.

Click "Next" for continues



2.5. Wireless Setting.

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



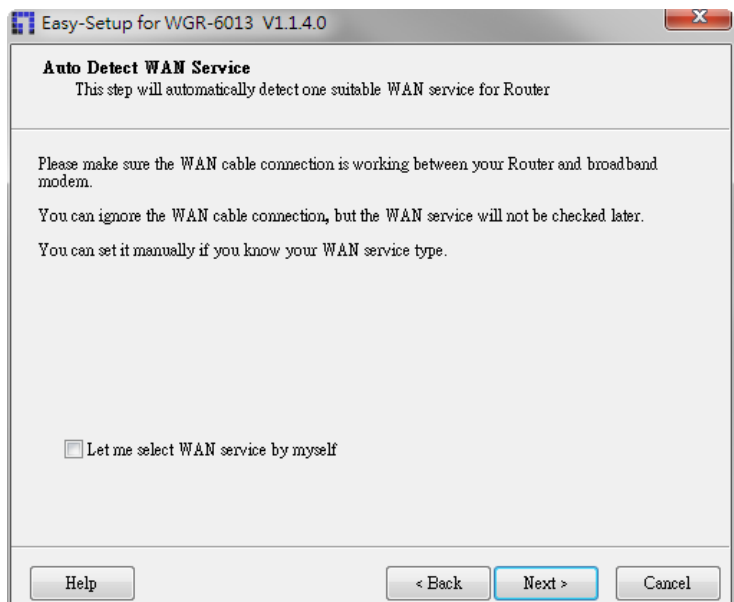
The screenshot shows a window titled "Easy-Setup for WGR-6013 V1.1.4.0". The main text says: "This step will setup your basic wireless network settings." Below this, it says: "Please assign the parameters to your wireless networking. If you need more settings, please login to the Router's configuration page." There are three input fields: "SSID:" with the value "LevelOne", "Channel:" with the value "11", and "Security:" with the value "Disable". At the bottom, there is a checkbox labeled "Do not set at this time." and three buttons: "Help", "< Back", and "Next >", and a "Cancel" button.

2.6 Auto Detect WAN Service.

Click “Next” for continue.

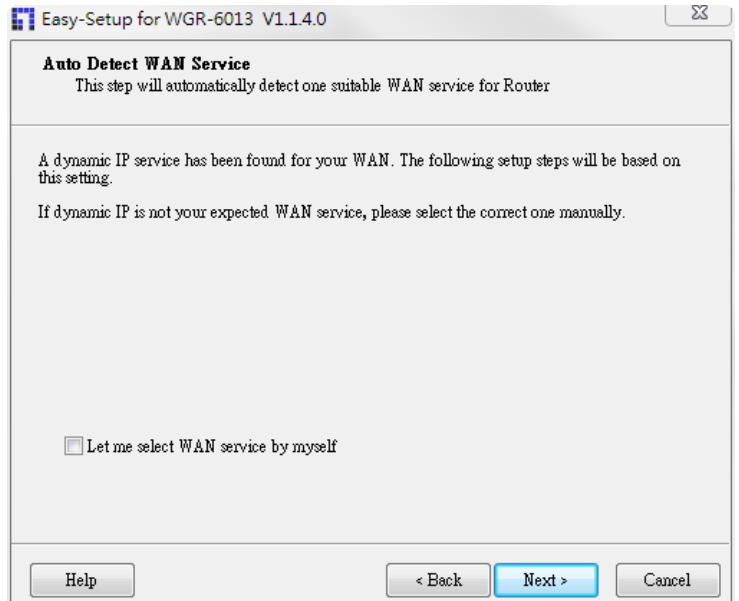
Click the button, “Let me select WAN service by myself”, to disable this function.

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



The screenshot shows a window titled "Easy-Setup for WGR-6013 V1.1.4.0". The main text says: "Auto Detect WAN Service" and "This step will automatically detect one suitable WAN service for Router". Below this, it says: "Please make sure the WAN cable connection is working between your Router and broadband modem." and "You can ignore the WAN cable connection, but the WAN service will not be checked later." and "You can set it manually if you know your WAN service type." At the bottom, there is a checkbox labeled "Let me select WAN service by myself" and three buttons: "Help", "< Back", and "Next >", and a "Cancel" button.

Example, the Dynamic WAN type is detected.

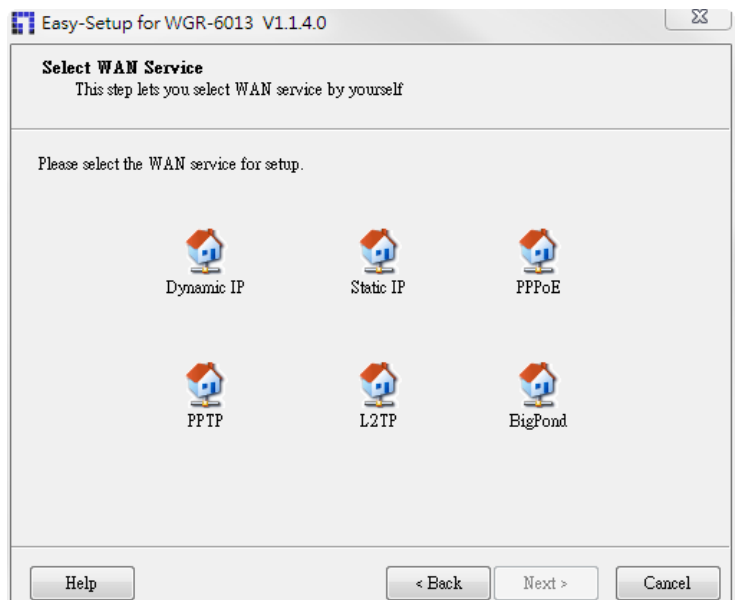


2.7. Manual select WAN Service

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

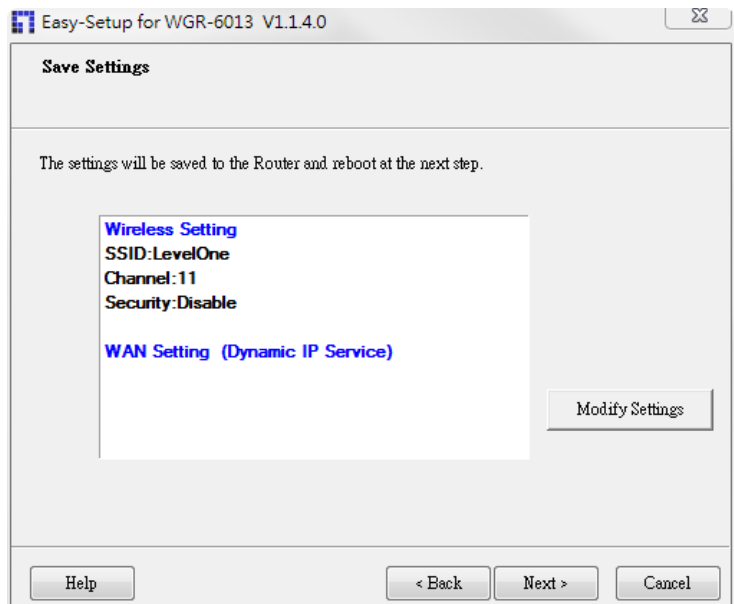
2.8 Summary of the settings and Next to “Reboot”

Click “Next” for continue.



2.9 Apply the Settings or Modify.

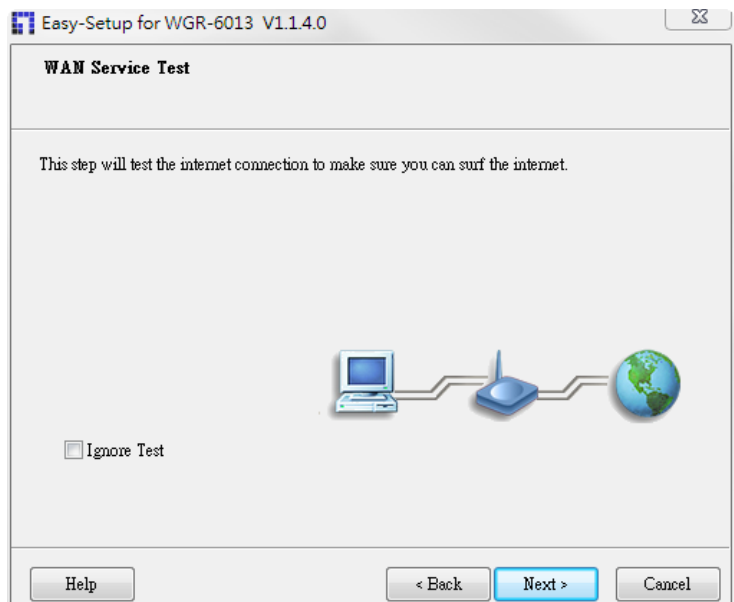
Click “Next” for continue.



2.10 Test the Internet connection.

Test WAN Networking service. Click “Next” for continue.

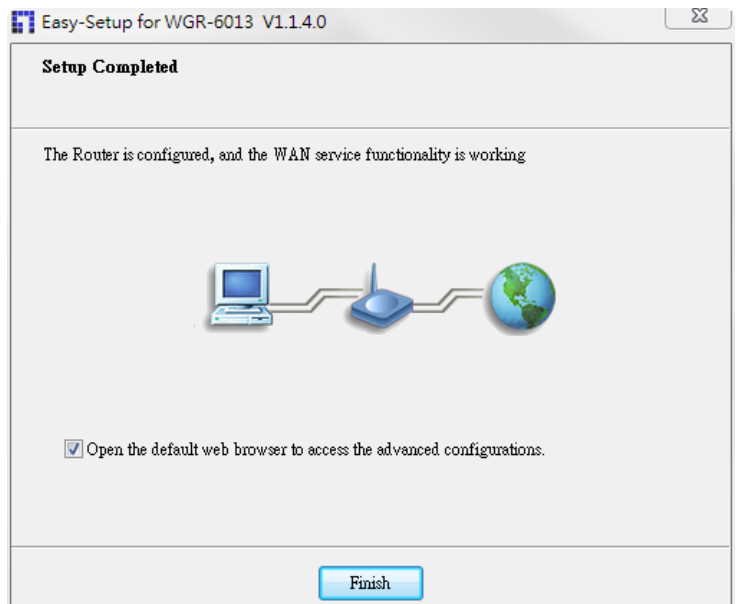
You can ignore the by select the “Ignore Test”.



2.11 Setup Completed.

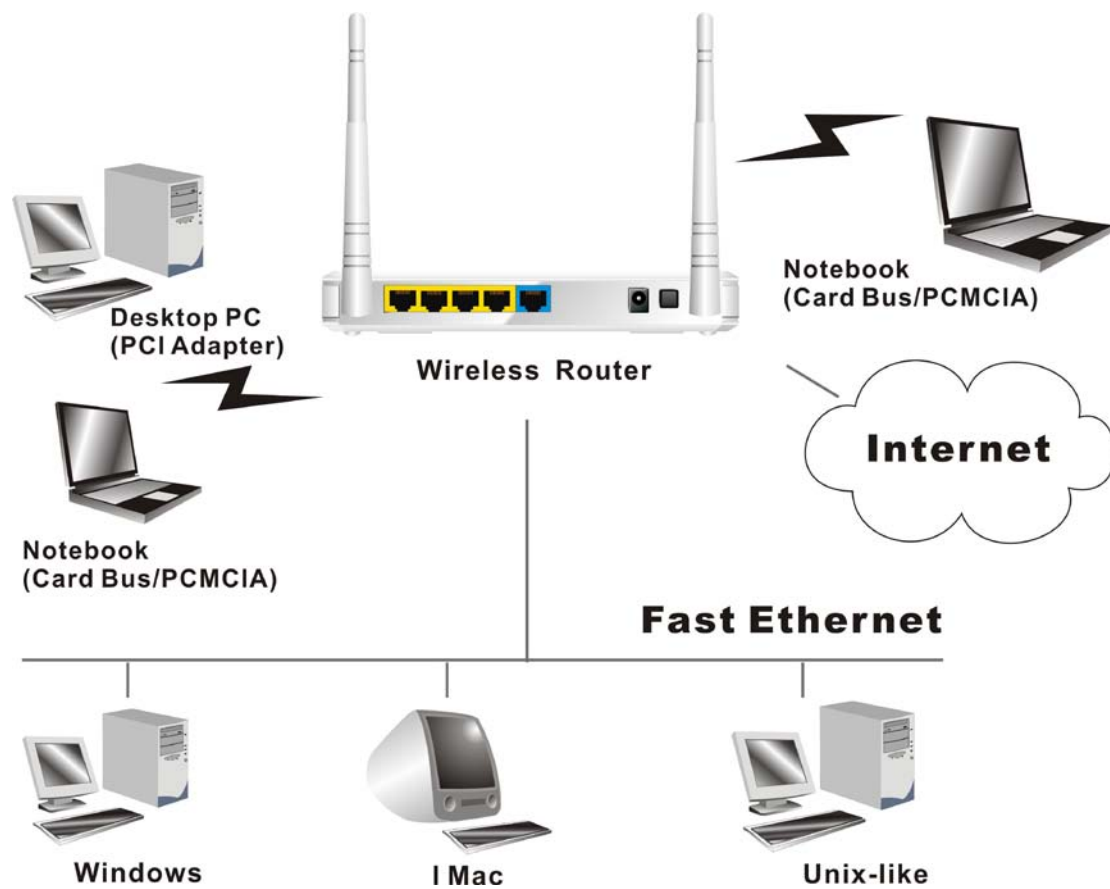
The EzSetup is finish, you can open the default web browser to configure advanced settings of the Router.

Click "Finish" to complete the installation.



Chapter 3 Making Configuration

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



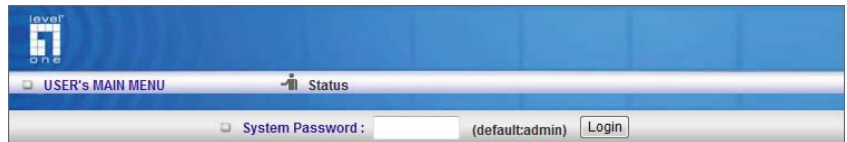
2.1 Login to Configure from Wizard

Type in the IP Address

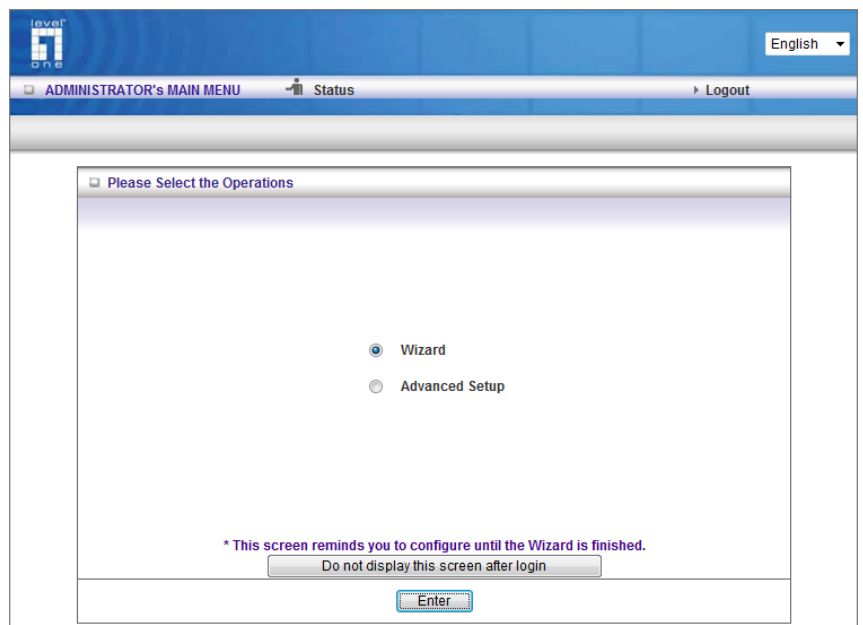
(<http://192.168.1.1>)



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



Press "Wizard" for basic
settings with simple way.



Press "Next" to start wizard.

The screenshot shows the LevelOne ONE Administrator's Main Menu. The top navigation bar includes "ADMINISTRATOR's MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A language dropdown is set to "English". The "Setup Wizard" window is open, displaying the following steps:

- ▶ Step 1. Setup Login Password.
- ▶ Step 2. WAN Setup.
- ▶ Step 3. Wireless Setup.
- ▶ Step 4. Summary.
- ▶ Step 5. Finish.

At the bottom, there is a "< Back" button, a breadcrumb trail "[Start > Password > WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 1:
Set up your system password.

The screenshot shows the "Setup Wizard - Setup Login Password" screen. It contains three input fields:

- ▶ Old Password
- ▶ New Password
- ▶ Reconfirm

At the bottom, there is a "< Back" button, a breadcrumb trail "[Start > Password > WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 2:
Select Wan Type.

Auto Detecting or
Setup Manually.

The screenshot shows the "Setup Wizard - WAN Type Setup" screen. It contains two radio button options:

- ☒ Auto Detecting WAN Type
- ☐ Setup WAN Type Manually

At the bottom, there is a "< Back" button, a breadcrumb trail "[Start > Password > WAN > Wireless > Summary > Finish!]", and a "Next >" button.

LevelOne ONE Administrator's Main Menu

English

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

Setup Wizard - Select WAN Type [EXIT]

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

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

Step 3:
Setup the LAN IP and WAN
Type.

LevelOne ONE Administrator's Main Menu

English

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

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

- ▶ LAN IP Address: 192.168.1.1
- ▶ Host Name: WGR-6013 (optional)
- ▶ WAN's MAC Address: 00-50-18-64-BF-8B [Clone MAC]

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

Example:

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

LevelOne ONE Administrator's Main Menu

English

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

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

- ▶ LAN IP Address: 192.168.1.1
- ▶ Account: []
- ▶ Password: []
- ▶ Primary DNS: 0.0.0.0
- ▶ Secondary DNS: 0.0.0.0
- ▶ PPPoE Service Name: [] (optional)
- ▶ Assigned IP Address: 0.0.0.0 (optional)

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

Step 5:

Set up your Wireless.

The screenshot shows the 'Setup Wizard - Wireless settings' page. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The page title is 'Setup Wizard - Wireless settings' with an '[EXIT]' link. The settings are as follows:

- Wireless function: ☒ Enable ☐ Disable
- Network ID(SSID): LevelOne
- Channel: Auto

At the bottom, there is a '< Back' button, a progress bar showing '[Start > Password > WAN > **Wireless** > Summary > Finish!]', and a 'Next >' button.

Set up your Authentication and Encryption.

The screenshot shows the 'Setup Wizard - Wireless Security' page. The top navigation bar is the same as the previous page. The page title is 'Setup Wizard - Wireless Security' with an '[EXIT]' link. The settings are as follows:

- Security: WEP
- 64 bits ☒ 128 bits ☐
- Key 1:
- Key 2:
- Key 3:
- Key 4:

Below the keys, there is a note: 'Please configure 26 for 128bits or 10 for 64 bits hexadecimal (0, 1, 2...8, 9, A, B...F) digits.'

At the bottom, there is a '< Back' button, a progress bar showing '[Start > Password > WAN > **Wireless** > Summary > Finish!]', and a 'Next >' button.

Step 6:

Then click Apply Setting.

And then the device will reboot.

The screenshot shows the 'Setup Wizard - Summary' page of a LevelOne device's web interface. The page has a blue header with the LevelOne logo and a language dropdown set to 'English'. Below the header is a navigation bar with links: 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Summary' and contains a confirmation message: 'Please confirm the information below.' Below this, there are two sections: '[WAN Setting]' and '[Wireless Setting]'. The WAN settings include: WAN Type (Dynamic IP Address), Host Name (WGR-6013), and WAN's MAC Address (00-50-18-64-BF-8B). The Wireless settings include: Wireless (Enable), SSID (LevelOne), Channel (Auto), and Security (None). At the bottom of the settings, there is a checkbox labeled 'Do you want to proceed the network testing?' which is checked. Below the checkbox are two buttons: '< Back' and 'Apply Settings'. A breadcrumb trail at the bottom reads: '[Start > Password > WAN > Wireless > Summary > Finish!]'.

| [WAN Setting] | |
|-------------------|--------------------|
| WAN Type | Dynamic IP Address |
| Host Name | WGR-6013 |
| WAN's MAC Address | 00-50-18-64-BF-8B |

| [Wireless Setting] | |
|----------------------|----------|
| Wireless | Enable |
| SSID | LevelOne |
| Channel | Auto |
| Security | None |

☒ Do you want to proceed the network testing?

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

Step 7:


Click Finish to complete it.

The screenshot shows the 'Setup Wizard - WAN Connection Test' page of a LevelOne device's web interface. The page has the same blue header and navigation bar as the previous screen. The main content area is titled 'Setup Wizard - WAN Connection Test' and contains a message: 'System is applying the settings. Please wait a moment...'. At the bottom, there are two buttons: '< Back' and 'Next >'. A breadcrumb trail at the bottom reads: '[Start > Password > WAN > Wireless > Summary > Finish!]'.

System is applying the settings. Please wait a moment...

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

2.2 System Status



English ▾

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

System Status [HELP]

| Item | WAN Status | Sidenote |
|----------------------|-------------------------|--------------------------|
| Remaining Lease Time | 47:59:40 | <button>Renew</button> |
| IP Address | 192.168.50.125 | <button>Release</button> |
| Subnet Mask | 255.255.255.0 | |
| Gateway | 192.168.50.1 | |
| Domain Name Server | 168.95.1.1, 61.31.233.1 | |
| MAC Address | 00-50-18-64-BF-8B | |

IPv6 System Status

| Item | WAN Status | Sidenote |
|-----------------------------|------------|----------|
| ipv6 | Disable | |
| WAN Link Local Address | - | |
| LAN IPv6 Address | - | |
| LAN IPv6 Link-Local Address | - | |

Wireless Status

| Item | WLAN Status | Sidenote |
|---------------|--------------------|------------|
| Wireless mode | Enable | |
| SSID | LevelOne | |
| Channel | Auto | |
| Security | WPA-PSK / WPA2-PSK | (TKIP+AES) |
| MAC Address | 00-50-18-64-BF-8C | |

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

WAN Status.

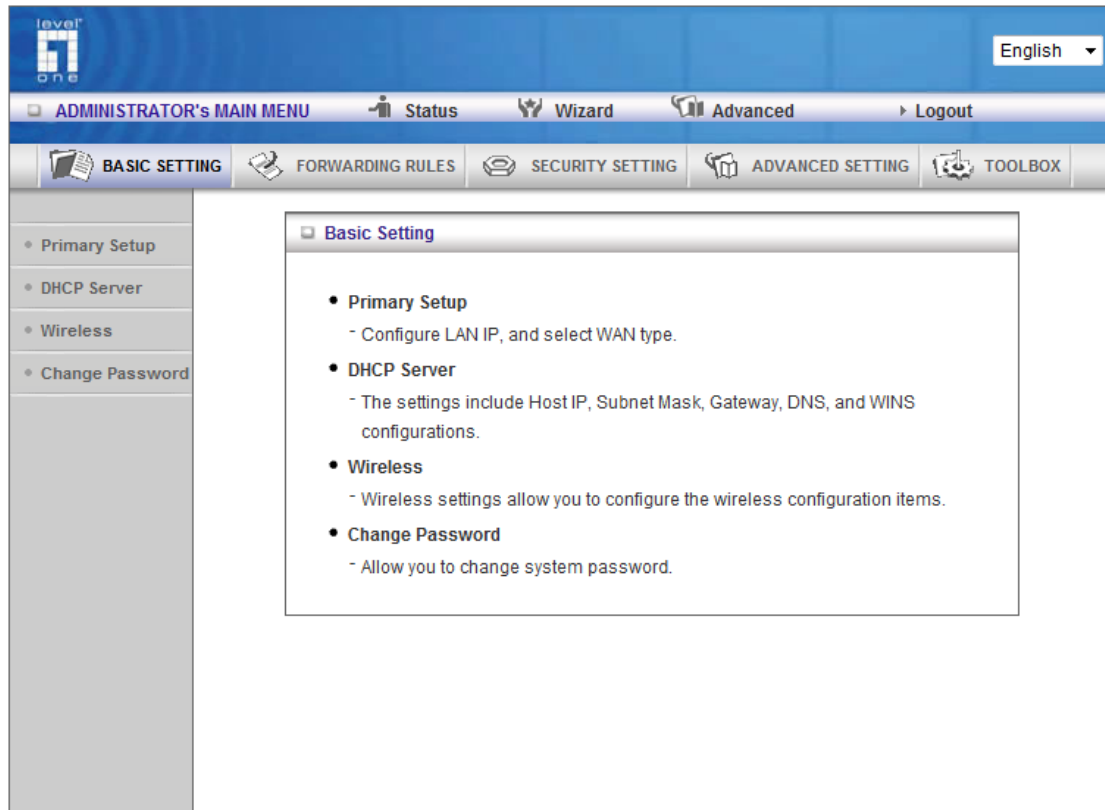
If the WAN port is assigned a dynamic IP, there may appear a **“Renew”** or **“Release”** button on the Sidenote column. You can click this button to renew or release IP manually.

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

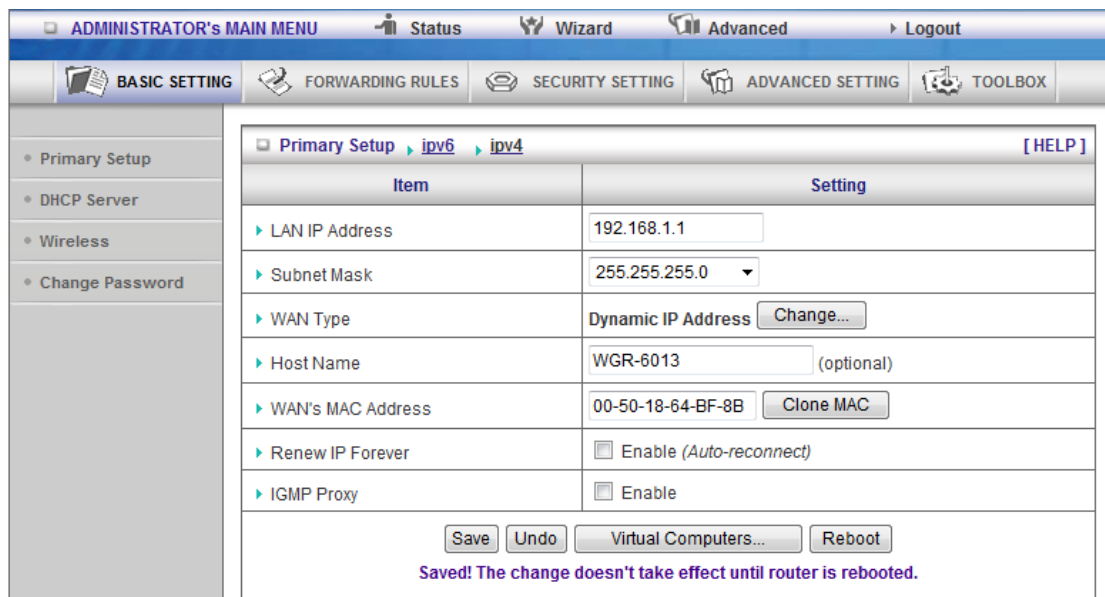
2.3 Advanced

2.3.1 Basic Setting

Please Select "Advanced Setup" to Setup



2.3.1.1 Primary Setup – WAN Type, Virtual Computers



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

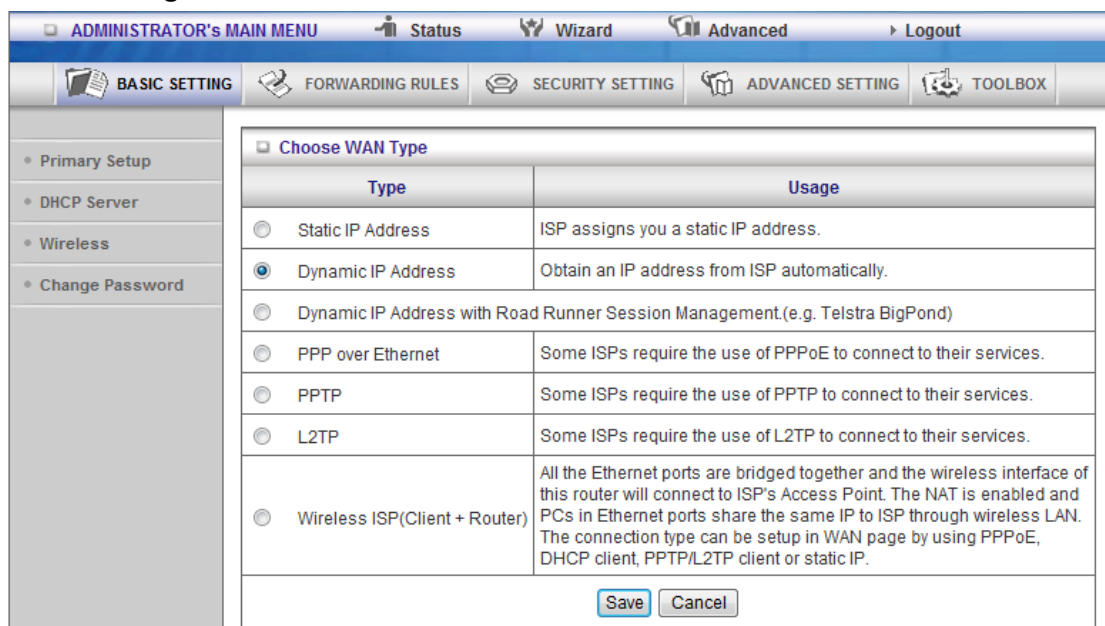
Primary Setup > ipv6 > ipv4 [HELP]

| Item | Setting |
|-------------------|--|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | Dynamic IP Address Change... |
| Host Name | WGR-6013 (optional) |
| WAN's MAC Address | 00-50-18-64-BF-8B Clone MAC |
| Renew IP Forever | <input type="checkbox"/> Enable (Auto-reconnect) |
| IGMP Proxy | <input type="checkbox"/> Enable |

[Save](#) [Undo](#) [Virtual Computers...](#) [Reboot](#)

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

Press “Change”



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

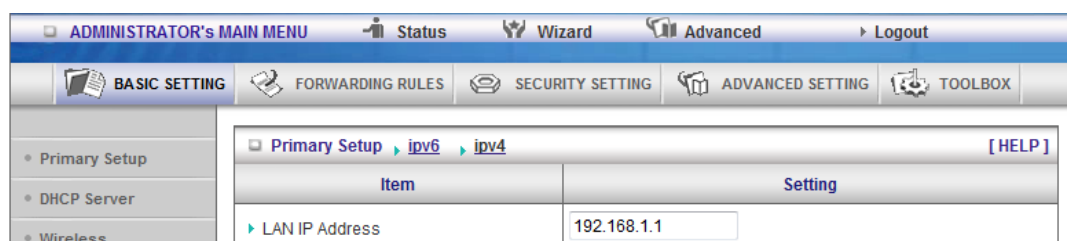
Choose WAN Type

| Type | Usage |
|---|--|
| <input type="radio"/> Static IP Address | ISP assigns you a static IP address. |
| <input checked="" type="radio"/> Dynamic IP Address | Obtain an IP address from ISP automatically. |
| <input type="radio"/> Dynamic IP Address with Road Runner Session Management (e.g. Telstra BigPond) | |
| <input type="radio"/> PPP over Ethernet | Some ISPs require the use of PPPoE to connect to their services. |
| <input type="radio"/> PPTP | Some ISPs require the use of PPTP to connect to their services. |
| <input type="radio"/> L2TP | Some ISPs require the use of L2TP to connect to their services. |
| <input type="radio"/> Wireless ISP (Client + Router) | All the Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP. |

[Save](#) [Cancel](#)

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.



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless

Primary Setup > ipv6 > ipv4 [HELP]

| Item | Setting |
|----------------|-------------|
| LAN IP Address | 192.168.1.1 |

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

| Choose WAN Type | |
|---|--|
| Type | Usage |
| <input type="radio"/> Static IP Address | ISP assigns you a static IP address. |
| <input 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. |
| <input checked="" type="radio"/> Wireless ISP(Client + Router) | All the Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP. |
| <div>Save Cancel</div> | |

- A. Static IP Address: ISP assigns you a static IP address.
- B. Dynamic IP Address: Obtain an IP address from ISP automatically.
- C. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
- D. PPTP: Some ISPs require the use of PPTP to connect to their services.
- E. L2TP: Some ISPs require the use of L2TP to connect to their services
- F. WISP: All the Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client or static IP.

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

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

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Primary Setup > ipv6 > ipv4 [HELP]

| Item | Setting |
|-----------------|---|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | Static IP Address Change... |
| WAN IP Address | 0.0.0.0 |
| WAN Subnet Mask | 255.255.255.0 |
| WAN Gateway | 0.0.0.0 |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| IGMP Proxy | <input type="checkbox"/> Enable |

[Save](#) [Undo](#) [Virtual Computers...](#) [Reboot](#)

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

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

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

Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Primary Setup > ipv6 > ipv4 [HELP]

| Item | Setting |
|-------------------|--|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | Dynamic IP Address Change... |
| Host Name | WGR-6013 (optional) |
| WAN's MAC Address | 00-50-18-64-BF-8B Clone MAC |
| Renew IP Forever | <input type="checkbox"/> Enable (Auto-reconnect) |
| IGMP Proxy | <input type="checkbox"/> Enable |

[Save](#) [Undo](#) [Virtual Computers...](#) [Reboot](#)

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

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

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Primary Setup DHCP Server Wireless Change Password

It is the IP address of this device. Beware that it always the default gateway of the computers.

Primary Setup ipv6 ipv4 [HELP]

| Item | Setting |
|-----------------------|---|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | PPP over Ethernet Change... |
| PPPoE Account | |
| PPPoE Password | |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Maximum Idle Time | 300 seconds |
| Authentication method | Auto |
| Connection Control | Connect-on-demand |
| PPPoE Service Name | (optional) |
| Assigned IP Address | 0.0.0.0 (optional) |
| MTU | 1492 |
| IGMP Proxy | <input type="checkbox"/> Enable |

Save Undo Reboot

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

PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.

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

Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.

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

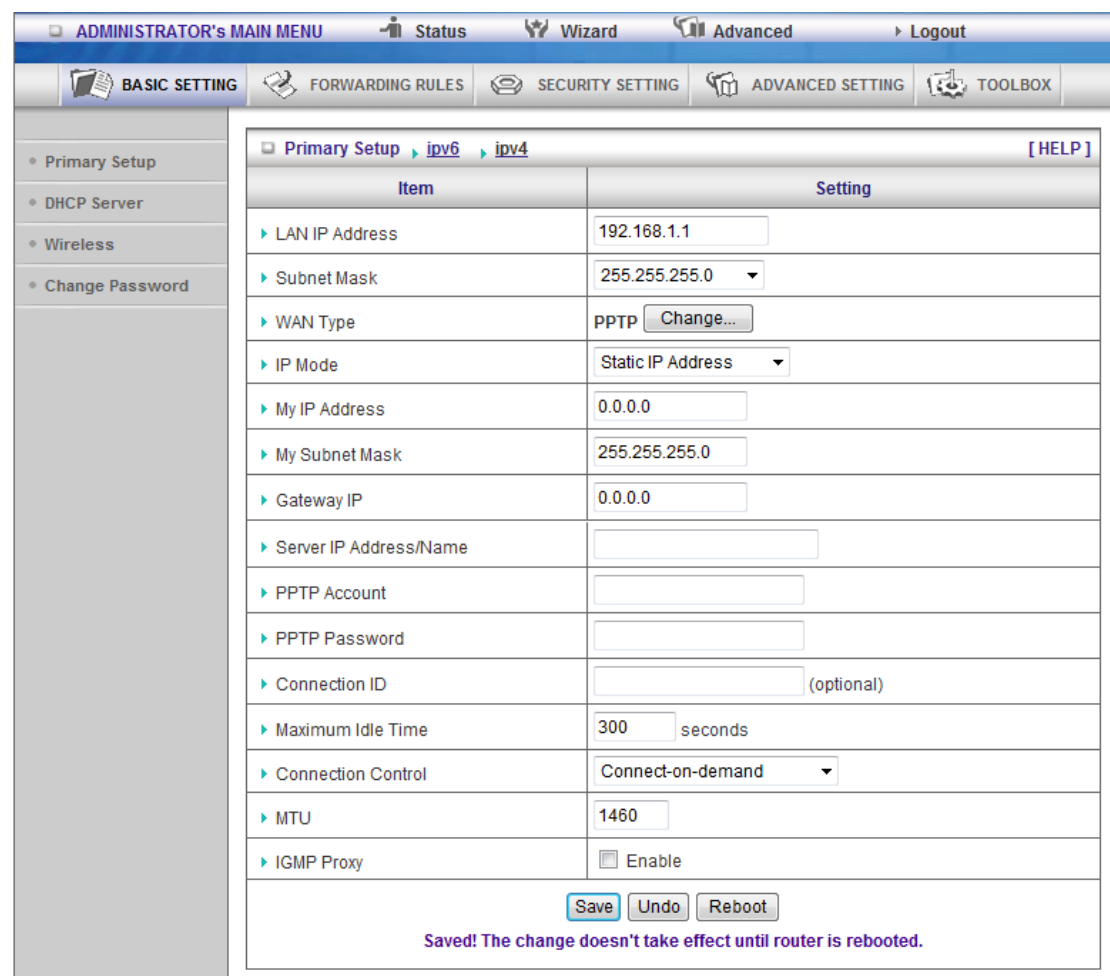
Connection Control: There are 3 modes to select:

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

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

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

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



| Item | Setting |
|------------------------|---------------------------------|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | PPTP Change... |
| IP Mode | Static IP Address |
| My IP Address | 0.0.0.0 |
| My Subnet Mask | 255.255.255.0 |
| Gateway IP | 0.0.0.0 |
| Server IP Address/Name | |
| PPTP Account | |
| PPTP Password | |
| Connection ID | (optional) |
| Maximum Idle Time | 300 seconds |
| Connection Control | Connect-on-demand |
| MTU | 1460 |
| IGMP Proxy | <input type="checkbox"/> Enable |

[Save](#) [Undo](#) [Reboot](#)

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

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.

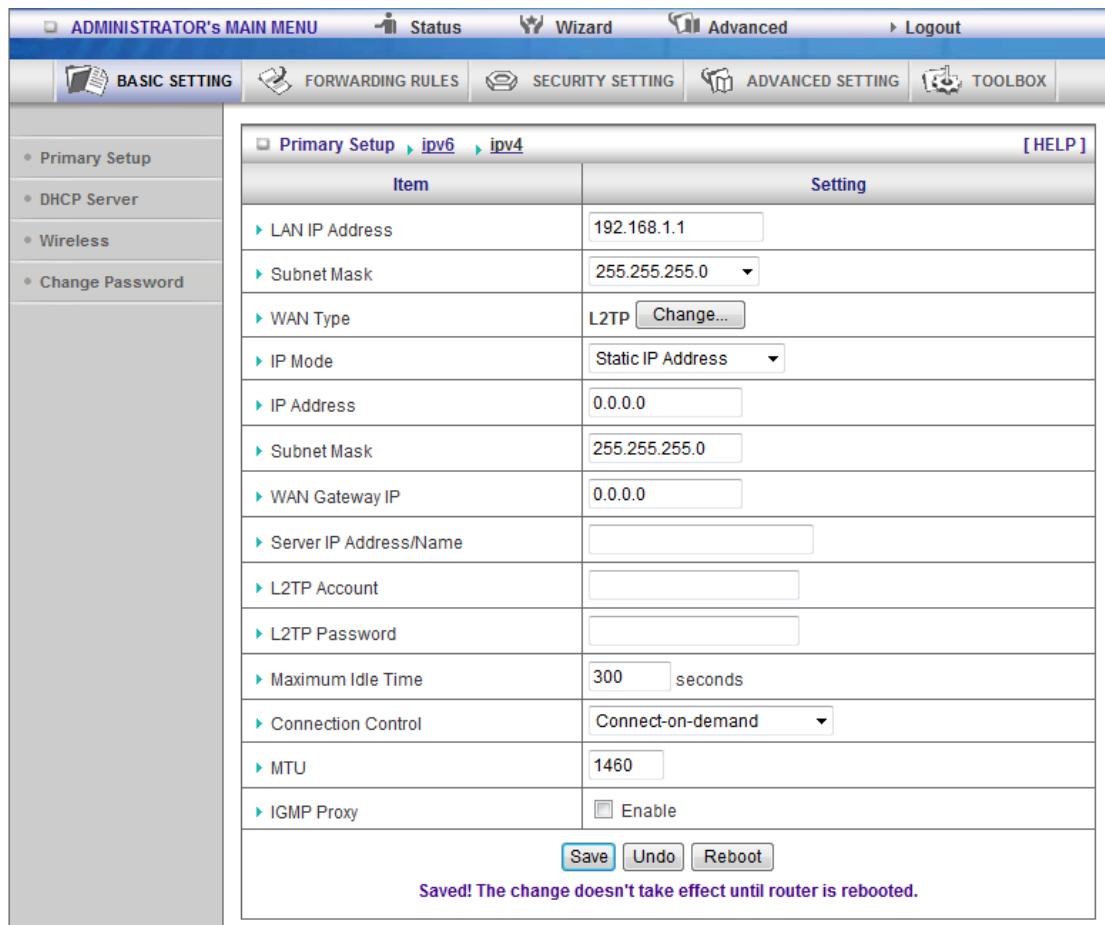
Connection Control: There are 3 modes to select:

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



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 ipv6 ipv4 [HELP]

| Item | Setting |
|------------------------|---------------------------------|
| LAN IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| WAN Type | L2TP Change... |
| IP Mode | Static IP Address |
| IP Address | 0.0.0.0 |
| Subnet Mask | 255.255.255.0 |
| WAN Gateway IP | 0.0.0.0 |
| Server IP Address/Name | |
| L2TP Account | |
| L2TP Password | |
| Maximum Idle Time | 300 seconds |
| Connection Control | Connect-on-demand |
| MTU | 1460 |
| IGMP Proxy | <input type="checkbox"/> Enable |

[Save](#) [Undo](#) [Reboot](#)

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

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

For example: Use Static

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

Connection Control: There are 3 modes to select:

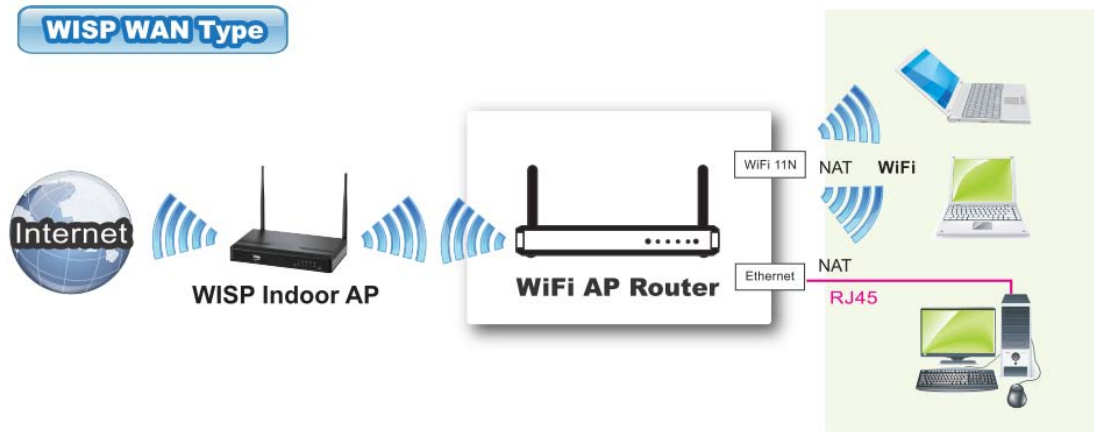
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

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

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

WISP: Wireless ISP(Client + Router)

In this mode, the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card, and then provide IP sharing capability all at the same time!



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 | 192.168.1.1 |
| WAN Type | WISP Change... |
| WISP WAN Type | <input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP <input type="radio"/> PPPoE |
| SSID | |
| MAC | 00-00-00-00-00-00 |
| Channel | 1 |
| Security | None |
| Scanned AP's MAC | --- Select one --- Copy |

[Save](#) [Undo](#) [Scan AP](#)

First, Select WISP WAN Type and please follow Dynamic IP, Static IP and PPPoE to configure. Regarding with Wireless setting, like SSID,MAC Channel, Security and Scanned AP'S MAC. Please refer to "[2.3.1.3 Wireless Setting](#)"

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

The screenshot shows the 'Virtual Computers' configuration page. At the top, there is a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Virtual Computers' and includes a '[HELP]' link. Below the title, there is a 'DHCP clients' dropdown menu set to '--- Select one ---', a 'Copy to' button, and an 'ID' dropdown. A table with 4 columns (ID, Global IP, Local IP, Enable) contains 5 rows. The 'Global IP' column has empty input fields. The 'Local IP' column shows '192.168.1.' followed by empty input fields. The 'Enable' column has checkboxes. At the bottom of the table are 'Save' and 'Undo' buttons. A text box on the left sidebar states: 'Allow you to setup the one-to-one mapping of multiple global IP address and local IP address.'

| ID | Global IP | Local IP | Enable |
|----|----------------------|---------------------------------|--------------------------|
| 1 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> |
| 2 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> |
| 3 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> |
| 4 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> |
| 5 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> |

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

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

2.3.1.2 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This router supports 6 types of IPv6 connection (Static IPv6/ DHCPv6/ PPPoE/ 6 to 4 / IPv6 in IPv4 tunnel/ / PPPoA). Please ask your ISP of what types of IPv6 are supported before you proceed with IPv6 setup.

■ Coexistence (Ether or PPPoE Dual Stack)

[Primary Setup](#)
[▶ ipv6](#)
[▶ ipv4](#)

| Coexistence | |
|-----------------|--|
| Item | Setting |
| ▶ WAN Type | <input checked="" type="radio"/> Ether <input type="radio"/> PPPoE (go ipv4 PPPoE) |
| ▶ Primary DNS | <input type="text"/> |
| ▶ Secondary DNS | <input type="text"/> |

[Current LAN Address](#)

| Item | Setting |
|--------------------------|---|
| ▶ IPv6 SPI | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| ▶ Link Local Address | <input type="text"/> |
| ▶ Autoconfiguration Type | Stateless ▼ |

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

- Select WAN type Ether or PPPoE: Almost ISPs follow the setting of IPv4 to connect IPv6 , for example, use the same account and Password in the PPPoE of IPv4 Page.
- IPv6 DNS (WAN IPv6 address) settings: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
- IPv6 SPI: The firewall settings section is an advance feature used to allow or deny traffic from passing through the device.
- LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
- Address auto configuration settings:
 - Auto-configuration: Disable or enable this auto configuration setting.
 - Auto-configuration type: You may set stateless or stateful (Dynamic IPv6).

■ Static IPv6

☐ Primary Setup
 [▶ ipv6](#)
[▶ ipv4](#)

| Static v6 | |
|-----------------------------|-----------------------------------|
| Item | Setting |
| ▶ Link Local IP Address | <input type="text"/> |
| ▶ Global IP Address | <input type="text"/> |
| ▶ Gateway Global IP Address | <input type="text"/> |
| ▶ Prefix Length | <input type="text" value="64"/> |
| ▶ MTU | <input type="text" value="1500"/> |
| ▶ Primary DNS | <input type="text"/> |
| ▶ Secondary DNS | <input type="text"/> |

☐ Current LAN Address

| Item | Setting |
|--------------------------|---|
| ▶ IPv6 SPI | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| ▶ Link Local Address | <input type="text"/> |
| ▶ Autoconfiguration Type | Stateless <input type="button" value="v"/> |
| ▶ Global Address | <input type="text"/> |

- IPv6 address: Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
- Prefix Length: enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.
- Gateway Global IP Address: Enter the Default Gateway address here; A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table.
- IPv6 DNS (WAN IPv6 address) settings: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
- IPv6 SPI: The firewall settings section is an advance feature used to allow or deny traffic from passing through the device.
- LAN IPv6 address settings: Please enter "LAN IPv6 address" and ignore the "LAN IPv6 Link-Local address".

- Address auto configuration settings:

Auto-configuration: Disable or enable this auto configuration setting.

Auto-configuration type: You may set stateless or stateful (Dynamic IPv6).

■ 6RD

| Primary Setup > ipv6 > ipv4 | |
|---|---|
| 6RD | |
| Item | Setting |
| ▶ Remote IPv4 Address | <input type="text" value="0.0.0.0"/> |
| ▶ Remote IPv6 Address/Prefix | <input type="text"/> |
| ▶ Primary DNS | <input type="text"/> |
| ▶ Secondary DNS | <input type="text"/> |
| Current LAN Address | |
| Item | Setting |
| ▶ IPv6 SPI | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| ▶ Link Local Address | <input type="text"/> |
| ▶ Autoconfiguration Type | Stateless ▼ |
| <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Reboot"/> | |
| Saved! The change doesn't take effect until router is rebooted. | |

- Remote IPv4 address: Enter Remote IP Address
- Remote IPv6 Address/Prefix Length: Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is "2001:0db8:85a3:0000:0000:8a2e:0370:7334". Then enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.
- IPv6 DNS (WAN IPv6 address) settings: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
- IPv6 SPI: The firewall settings section is an advance feature used to allow or deny

traffic from passing through the device.

- LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
- Address auto configuration settings:

Auto-configuration: Disable or enable this auto configuration setting.

Auto-configuration type: You may set stateless or stateful (Dynamic IPv6).

■ 6in4

| <input type="checkbox"/> Primary Setup ▶ ipv6 ▶ ipv4 | |
|--|---|
| 6 in 4 Relay Router Address item | |
| Item | Setting |
| ▶ Remote IPv4 Address | <input type="text" value="0.0.0.0"/> |
| ▶ Remote IPv6 Address/Prefix | <input type="text"/> |
| ▶ Primary DNS | <input type="text"/> |
| ▶ Secondary DNS | <input type="text"/> |
| <input type="checkbox"/> Current LAN Address | |
| Item | Setting |
| ▶ IPv6 SPI | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| ▶ Link Local Address | <input type="text"/> |
| ▶ Autoconfiguration Type | <input type="text" value="Stateless"/> ▼ |
| <div>Save Undo Reboot</div> <p>Saved! The change doesn't take effect until router is rebooted.</p> | |

- Remote IPv4 address: Enter Remote IP Address
- Remote IPv6 Address/Prefix Length: Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is “2001:0db8:85a3:0000:0000:8a2e:0370:7334”. Then enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.
- IPv6 DNS (WAN IPv6 address) settings: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS

address and secondary DNS address.

- IPv6 SPI: The firewall settings section is an advance feature used to allow or deny traffic from passing through the device.
- LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
- Address auto configuration settings:

Auto-configuration: Disable or enable this auto configuration setting.

Auto-configuration type: You may set stateless or stateful (Dynamic IPv6).

■ 6to4

| <input type="checkbox"/> Primary Setup ▶ <input type="checkbox"/> ipv6 ▶ <input type="checkbox"/> ipv4 | |
|--|---|
| 6 to 4 Relay Router Address item | |
| Item | Setting |
| ▶ Primary DNS | <input type="text"/> |
| ▶ Secondary DNS | <input type="text"/> |
| <input type="checkbox"/> Current LAN Address | |
| Item | Setting |
| ▶ IPv6 SPI | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| ▶ Link Local Address | <input type="text"/> |
| ▶ Autoconfiguration Type | Stateless ▼ |
| <div>Save Undo Reboot</div> <p>Saved! The change doesn't take effect until router is rebooted.</p> | |

- IPv6 DNS (WAN IPv6 address) settings: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
- IPv6 SPI: The firewall settings section is an advance feature used to allow or deny traffic from passing through the device.
- LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
- Address auto configuration settings:

Auto-configuration: Disable or enable this auto configuration setting.

Auto-configuration type: You may set stateless or stateful (Dynamic IPv6).

2.3.1.3 DHCP Server

| Item | Setting |
|----------------------------|---|
| ▶ DHCP Server | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| ▶ Lease Time | 0 Minutes |
| ▶ IP Pool Starting Address | 50 |
| ▶ IP Pool Ending Address | 200 |
| ▶ Domain Name | |
| ▶ Primary DNS | 0.0.0.0 |
| ▶ Secondary DNS | 0.0.0.0 |
| ▶ Primary WINS | 0.0.0.0 |
| ▶ Secondary WINS | 0.0.0.0 |
| ▶ Gateway | 0.0.0.0 (optional) |

Save Undo Clients List...

Press “More>>”

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

| ADMINISTRATOR's MAIN MENU | | | | Status | Wizard | Advanced | Logout | | | | | | | | |
|---|-----------|--|--------------------------|------------------|---------|----------|--------|------------|-----------|-------------|--------|--------------|--------|-------------------|--------------------------|
| BASIC SETTING | | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX | | | | | | | | | | |
| <ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password | | DHCP Clients List <table border="1"> <thead> <tr> <th>IP Address</th> <th>Host Name</th> <th>MAC Address</th> <th>Select</th> </tr> </thead> <tbody> <tr> <td>192.168.1.62</td> <td>@IP062</td> <td>0C-74-C2-D2-B9-16</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <div> Wake up Delete Back Refresh </div> | | | | | | IP Address | Host Name | MAC Address | Select | 192.168.1.62 | @IP062 | 0C-74-C2-D2-B9-16 | <input type="checkbox"/> |
| IP Address | Host Name | MAC Address | Select | | | | | | | | | | | | |
| 192.168.1.62 | @IP062 | 0C-74-C2-D2-B9-16 | <input type="checkbox"/> | | | | | | | | | | | | |

2.3.1.3 Wireless Setting

| Wireless Setting | | [HELP] |
|--|--|----------|
| Item | Setting | |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Wireless Operation Mode | AP Router Mode | |
| Wireless Off Schedule | (00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| Network ID(SSID) | LevelOne | |
| Wireless Mode | 11b/g/n Mixed mode | |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Channel | Auto | |
| Security | None | |
| Save Undo WPS Enter... Wireless Client List... | | |

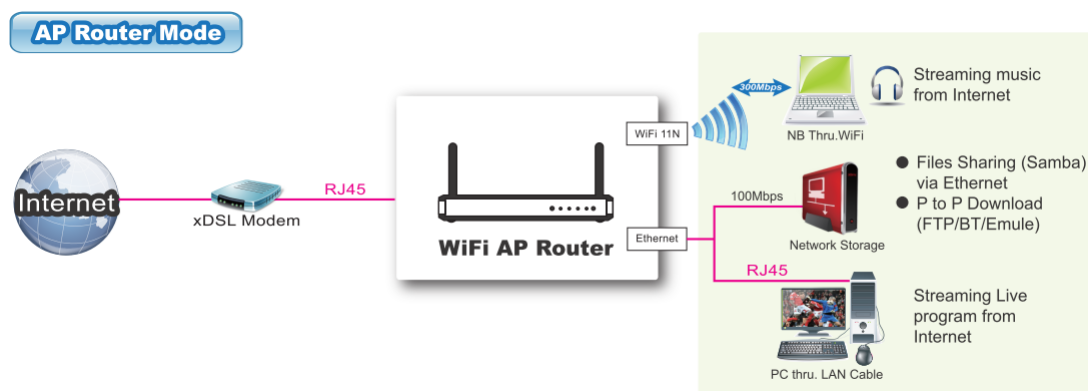
Wireless settings allow you to set the wireless configuration items.

Wireless Radio: The user can turn on or off Wireless Service.

Wireless Operation Mode

AP Router Mode:

This Mode can allow you Get your wired and wireless devices connected with NAT.



| Wireless Setting [HELP] | |
|---------------------------|--|
| Item | Setting |
| ▶ Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ▶ Wireless Operation Mode | AP Router Mode ▼ |
| ▶ Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| ▶ Network ID(SSID) | LevelOne |
| ▶ Wireless Mode | 11b/g/n Mixed mode ▼ |
| ▶ SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ▶ Channel | Auto ▼ |
| ▶ Security | None ▼ |

Wireless Off Schedule: Before turning Off Wireless Radio, the device will detect if Wireless station is online, then depend as Schedule " 01:00~08:30" to disable WiFi service.

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

SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that

The wireless clients can know how many ap devices by scanning function in the network. Therefore, This function is disabled, the wireless clients can not find the device from beacons.

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

WPS (WiFi Protection Setup)

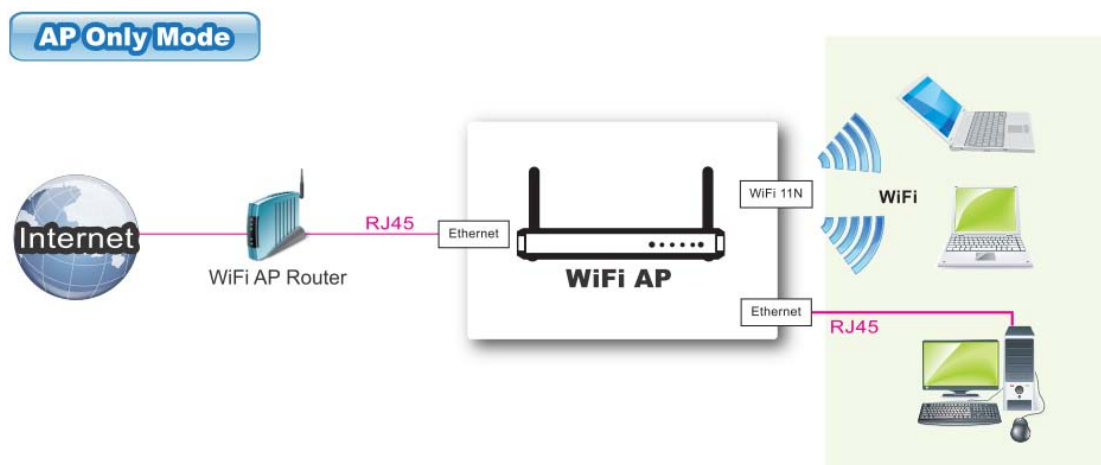
WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

| ADMINISTRATOR'S MAIN MENU | | Status | Wizard | Advanced | Logout | | | | | | | | | | | | |
|---|---|---|------------------|------------------|---------|------|---------|-----|---|-------|---|---------------------------|--|-----------|------|------------|---|
| BASIC SETTING | | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX | | | | | | | | | | | | |
| <ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password | | <div>Wi-Fi Protected Setup</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>WPS</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Setup</td> <td><input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station</td> </tr> <tr> <td>Current PIN of the device</td> <td> <input type="text" value="11968818"/> <input type="button" value="Generate New PIN"/> </td> </tr> <tr> <td>WPS state</td> <td>Idle</td> </tr> <tr> <td>WPS status</td> <td>Configured <input type="button" value="Release"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/> </div> | | | | Item | Setting | WPS | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | Setup | <input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station | Current PIN of the device | <input type="text" value="11968818"/> <input type="button" value="Generate New PIN"/> | WPS state | Idle | WPS status | Configured <input type="button" value="Release"/> |
| Item | Setting | | | | | | | | | | | | | | | | |
| WPS | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | | | | | | | | | | | | | | |
| Setup | <input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station | | | | | | | | | | | | | | | | |
| Current PIN of the device | <input type="text" value="11968818"/> <input type="button" value="Generate New PIN"/> | | | | | | | | | | | | | | | | |
| WPS state | Idle | | | | | | | | | | | | | | | | |
| WPS status | Configured <input type="button" value="Release"/> | | | | | | | | | | | | | | | | |

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

AP only Mode:

When acting as an access point, this device connects all the stations to a wired network and WAN Port is disabled. See the sample application below.



| Wireless Setting [HELP] | |
|--|--|
| Item | Setting |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Wireless Operation Mode | AP Only Mode ▼ |
| Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Network ID(SSID) | LevelOne |
| Wireless Mode | 11b/g/n Mixed mode ▼ |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto ▼ |
| Security | None ▼ |
| <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WPS Enter..."/> <input type="button" value="Wireless Client List..."/> | |

Wireless Off Schedule: Before turning Off Wireless Radio, the device will detect if Wireless station is online, then depend as Schedule " 01:00~08:30" to disable WiFi service.

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

SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that

The wireless clients can know how many ap devices by scanning function in the network. Therefore, This function is disabled, the wireless clients can not find the device from beacons.

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

WPS (WiFi Protection Setup)

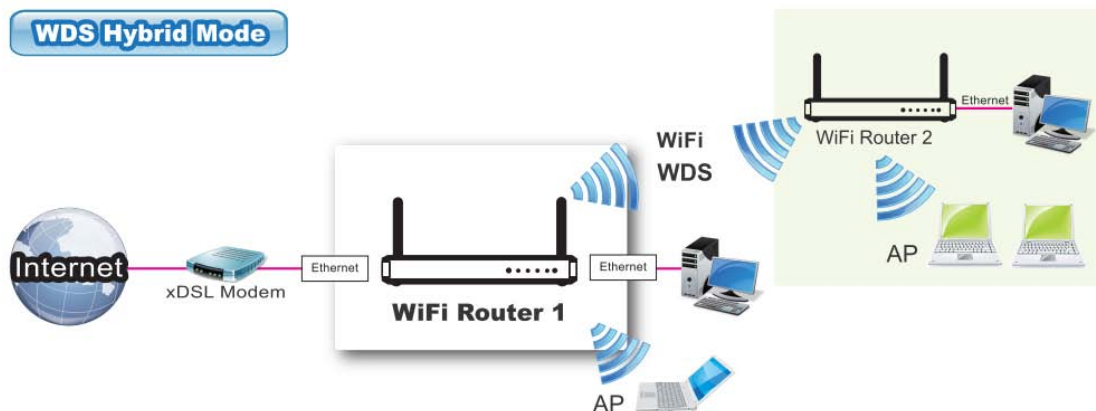
WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

| ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout | |
|--|---|
| BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX | |
| • Primary Setup • DHCP Server • Wireless • Change Password | |
| Wi-Fi Protected Setup | |
| Item | Setting |
| ▶ WPS | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ▶ Setup | <input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station |
| ▶ Current PIN of the device | <input type="text" value="11968818"/> <input type="button" value="Generate New PIN"/> |
| ▶ WPS state | Idle |
| ▶ WPS status | Configured <input type="button" value="Release"/> |
| <input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/> | |

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

WDS Hybrid Mode:

While acting as Bridges, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection



| WDS Setting | | [HELP] |
|--|--|----------------------|
| Item | Setting | |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Wireless Operation Mode | WDS Hybrid Mode ▼ | |
| Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| Network ID(SSID) | LevelOne | |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Channel | 1 ▼ | |
| Security | None ▼ | |
| Remote AP MAC | MAC 1 | <input type="text"/> |
| | MAC 2 | <input type="text"/> |
| | MAC 3 | <input type="text"/> |
| | MAC 4 | <input type="text"/> |
| Scanned AP's MAC --- Select one --- ▼ <input type="button" value="Copy to"/> Remote AP MAC -- ▼ | | |
| SSID | Channel | MAC Address |
| <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Scan AP"/> <input type="button" value="Back"/> | | |

Wireless Off Schedule: Before turning Off Wireless Radio, the device will detect if Wireless station is online, then depend as Schedule " 01:00~08:30" to disable WiFi service.

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.

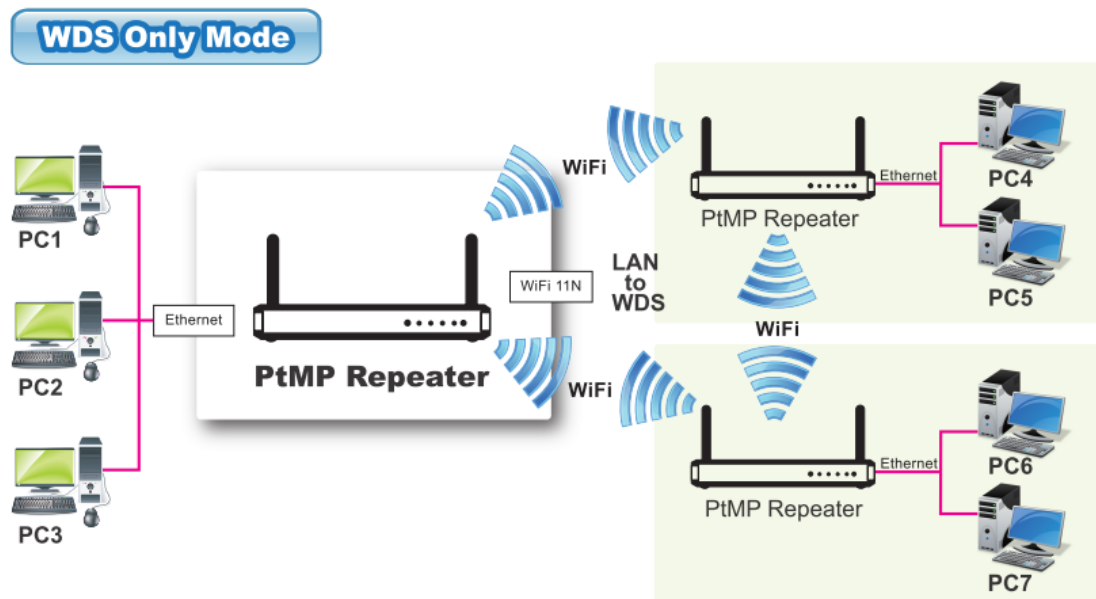
Channel: The radio channel number. The permissible channels depend on the Regulatory Domain.

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

Remote AP MAC : Choose "Manual" or scan one AP to copy to item1~4.

WDS(Wireless Distribution System)

The WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools ...etc.



| WDS Setting | | [HELP] |
|---|---|----------------------|
| Item | Setting | |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Wireless Operation Mode | WDS Only Mode | |
| Network ID(SSID) | LevelOne | |
| Channel | 1 | |
| Security | None | |
| Remote AP MAC | MAC 1 | <input type="text"/> |
| | MAC 2 | <input type="text"/> |
| | MAC 3 | <input type="text"/> |
| | MAC 4 | <input type="text"/> |
| Scanned AP's MAC --- Select one --- Copy to Remote AP MAC -- | | |
| SSID | Channel | MAC Address |
| <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Scan AP"/> <input type="button" value="Back"/> </div> | | |

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.

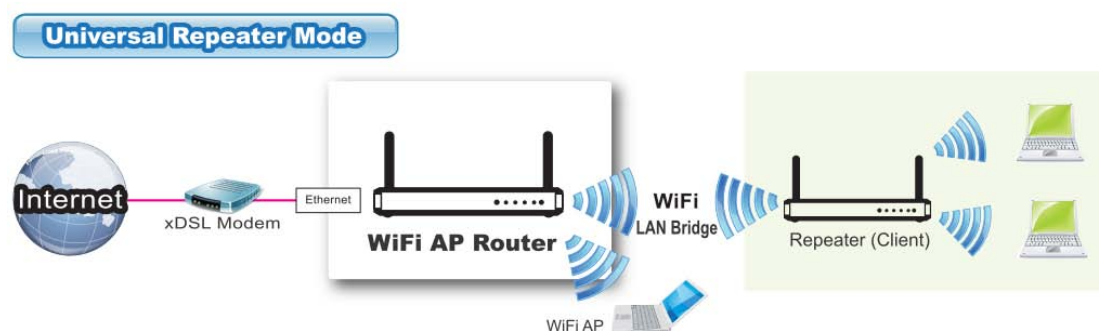
Security: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

Remote AP MAC : Choose “Manual” or scan one AP to copy to item1~4.

Universal Repeater Mode

Universal Repeater is a technology used to extend wireless coverage.

It provides the function to act as Adapter (client) and AP at the same time and can use this function to connect to a Root AP and use AP(SSID name is same with Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.



| Universal Repeater Mode | | | | | |
|------------------------------|-------------|---|-----------------|---------------------------------------|-------------------|
| Item | | Setting | | | |
| Wireless Radio | | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | |
| Wireless Operation Mode | | Universal Repeater ▼ | | | |
| SSID (Wireless Network Name) | | <input type="text"/> | | <input type="button" value="Manual"/> | |
| Security | | None ▼ | | | |
| Select | SSID | Channel | Signal Strength | Security | MAC Address |
| <input type="radio"/> | WBR-6012TSD | 1 | 5 | WPA2-PSK | 00-11-6B-2F-B5-A6 |

SSID (Wireless Network Name): Select “AP” or entry SSID manually to connect.

Security “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.

| Wireless Setting [HELP] | |
|---|--|
| Item | Setting |
| ▶ Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ▶ Wireless Operation Mode | AP Router Mode ▼ |
| ▶ Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| ▶ Network ID(SSID) | LevelOne |
| ▶ Wireless Mode | 11b/g/n Mixed mode ▼ |
| ▶ SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ▶ Channel | Auto ▼ |
| ▶ 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 | |
| <div> Save Undo WPS Enter... Wireless Client List... </div> | |

WPA-PSK

1. Select Encryption and Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

| Wireless Setting [HELP] | |
|---------------------------|--|
| Item | Setting |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Wireless Operation Mode | AP Router Mode ▼ |
| Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Network ID(SSID) | LevelOne |
| Wireless Mode | 11b/g/n Mixed mode ▼ |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto ▼ |
| Security | WPA-PSK ▼ |
| Encryption | <input checked="" type="radio"/> TKIP <input type="radio"/> AES |
| Preshare Key Mode | ASCII ▼ |
| Preshare Key | |

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

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

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

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

WPA2-PSK(AES)

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

WPA2(AES)

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

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

Select RADIUS Shared Key

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

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

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

WPA-PSK /WPA2-PSK

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

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

| Wireless Setting [HELP] | |
|---|--|
| Item | Setting |
| Wireless Radio | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Wireless Operation Mode | AP Router Mode ▼ |
| Wireless Off Schedule | (00)Always ▼ <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Network ID(SSID) | LevelOne |
| Wireless Mode | 11b/g/n Mixed mode ▼ |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto ▼ |
| Security | WPA-PSK / WPA2-PSK ▼ |
| Encryption | TKIP + AES |
| Preshare Key Mode | ASCII ▼ |
| Preshare Key | |
| <div>Save Undo WPS Enter... Wireless Client List...</div> | |

WPA/WPA2

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

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

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

Select RADIUS Shared Key

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

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

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

Wireless Client List

The screenshot shows the 'Wireless Client List' page. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area has a title 'Wireless Client List' and a table with two columns: 'Connected Time1' and 'MAC Address'. The table contains one entry: 'Sun May 31 23:11:14 2009' and '48-5D-60-9B-C0-A3'. Below the table are 'Back' and 'Refresh' buttons.

| Connected Time1 | MAC Address |
|--------------------------|-------------------|
| Sun May 31 23:11:14 2009 | 48-5D-60-9B-C0-A3 |

2.3.1.4 Change Password

The screenshot shows the 'Change Password' page. The top navigation bar is identical to the previous page. The sidebar lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area has a title 'Change Password' and a table with two columns: 'Item' and 'Setting'. The table contains three rows: 'Old Password', 'New Password', and 'Reconfirm', each with an adjacent text input field. Below the table are 'Save' and 'Undo' buttons.

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

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

2.3.2 Forwarding Rules

The screenshot displays the Level One router's web-based configuration interface. At the top, there is a blue header bar with the 'level one' logo on the left and a language dropdown menu set to 'English' on the right. Below the header 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 highlighted), 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left side of the main content area, 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 configuration options:

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

2.3.2.1 Virtual Server

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Virtual Server
- Special AP
- Miscellaneous

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 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 2 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 3 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 4 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 5 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 6 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 7 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 8 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 9 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 10 | 192.168.1. | | | 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**.

2.3.2.2 Special AP

The screenshot shows a web-based configuration interface for a firewall. 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 'Virtual Server', 'Special AP' (selected), and 'Miscellaneous'. The main content area is titled 'Special Applications' and includes a '[HELP]' link. It features a 'Popular applications' dropdown menu set to '-- Select one --', 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 'ID' column contains numbers 1 through 8. The 'Trigger' column contains empty text boxes. The 'Incoming Ports' column contains empty text boxes. The 'Enable' column contains checkboxes, all of which are currently unchecked. 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.

2.3.2.3 Miscellaneous Items

| Miscellaneous Items | | |
|---|---|-------------------------------------|
| Item | Setting | Enable |
| ▶ IP Address of DMZ Host | <input checked="" type="radio"/> 192.168.1. <input type="text"/> | <input type="checkbox"/> |
| ▶ Super DMZ(IP Passthrough) | <input type="radio"/> <input type="text" value="-- Select one --"/> <input type="button" value="Copy"/> <input type="text"/> | <input type="checkbox"/> |
| ▶ Hardware DMZ Port | <input type="text" value="Port1"/> | <input type="checkbox"/> |
| ▶ Non-standard FTP port | <input type="text"/> | |
| ▶ UPnP setting | | <input checked="" type="checkbox"/> |
| ▶ Xbox Support | | <input checked="" type="checkbox"/> |
| <input type="button" value="Save"/> <input type="button" value="Undo"/> | | |

IP Address of DMZ Host

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

NOTE: This feature should be used only when needed.

Super DMZ(IP Passthrough)

The client be set in Super DMZ and dhcp server assigns a global IP which is the same with Wan IP of this device. This client also can access the local client.This client behind NAT can use various applications without limitation.

Non-standard FTP port

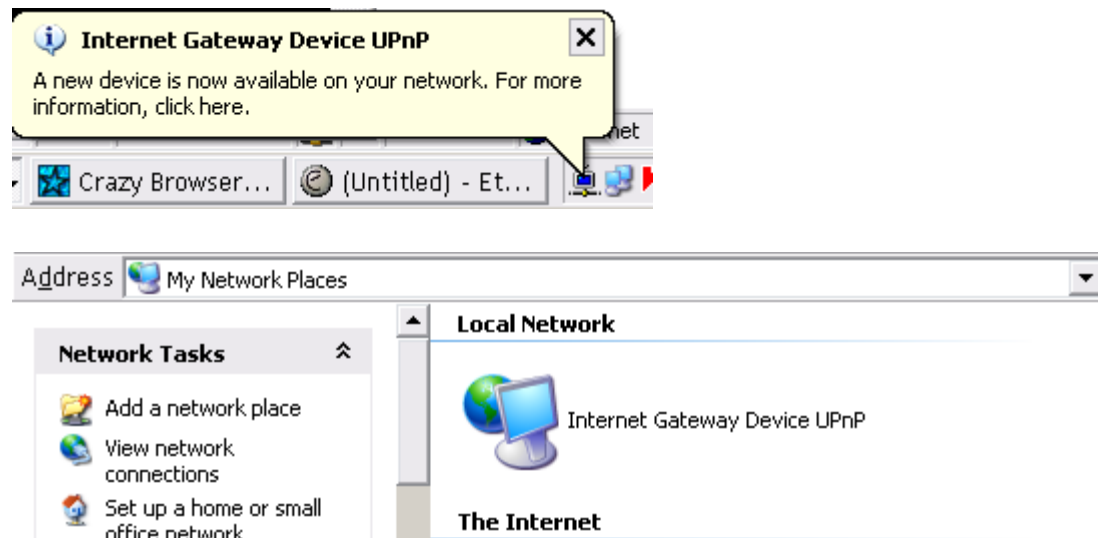
You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

Xbox Support

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

UpnP Setting

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



2.3.3 Security Settings

The screenshot displays the LevelOne network device administrator interface. At the top, there is a blue header bar with the LevelOne logo on the left and a language dropdown menu set to 'English' on the right. Below the header 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', 'SECURITY SETTING' (which is highlighted), 'ADVANCED SETTING', and 'TOOLBOX'. On the left side of the main content area, there is a vertical sidebar menu with the following items: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Access Control', and 'Miscellaneous'. The main content area is titled 'Security Setting' and contains a list of security features with their descriptions:

- **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 behind this device from accessing specific URLs.
- **URL Blocking**
 - URL Blocking will block LAN computers to connect to pre-defined websites.
- **Internet Address Control**
 - The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.
- **Miscellaneous**
 - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
 - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
 - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

2.3.3.1 Packet Filters

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

• Packet Filters
• Domain Filters
• URL Blocking
• MAC Access Control
• Miscellaneous

Outbound Packet Filter [HELP]

| Item | Setting |
|--|---------------------------------|
| Outbound Filter | <input type="checkbox"/> Enable |
| <input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules. | |
| Block List -- select one -- Schedule rule (00)Always Copy to ID -- | |

| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
|----|-------------------|------------------------|--------------------------|----------------|
| 1 | | 20-21 | <input type="checkbox"/> | 0 |
| 2 | | 80 | <input type="checkbox"/> | 0 |
| 3 | | 443 | <input type="checkbox"/> | 0 |
| 4 | | 53 | <input type="checkbox"/> | 0 |
| 5 | | 25 | <input type="checkbox"/> | 0 |
| 6 | | 110 | <input type="checkbox"/> | 0 |
| 7 | | 23 | <input type="checkbox"/> | 0 |
| 8 | | | <input type="checkbox"/> | 0 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

<< Previous Next >> Save Undo Inbound Filter...

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

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

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

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

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

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

Each rule can be enabled or disabled individually.

Inbound Filter:

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

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

Example 1:

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

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

Inbound Packet Filter [HELP]

| Item | Setting |
|--|--|
| Inbound Filter | <input checked="" type="checkbox"/> Enable |
| <input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules. | |
| Virtual Server Rule -- IP address : Port (Service) -- Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- | |

| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
|----|---------------------|------------------------|-------------------------------------|----------------|
| 1 | 1.2.3.100-1.2.3.149 | 25-100 | <input checked="" type="checkbox"/> | 0 |
| 2 | 1.2.3.10-1.2.3.20 | | <input checked="" type="checkbox"/> | 0 |
| 3 | | | <input type="checkbox"/> | 0 |
| 4 | | | <input type="checkbox"/> | 0 |
| 5 | | | <input type="checkbox"/> | 0 |
| 6 | | | <input type="checkbox"/> | 0 |
| 7 | | | <input type="checkbox"/> | 0 |
| 8 | | | <input type="checkbox"/> | 0 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

<< Previous | Next >> | Save | Undo | Outbound Filter...

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

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

Others are all blocked.

Example 2:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

Packet Filters
Domain Filters
URL Blocking
MAC Access Control
Miscellaneous

Inbound Packet Filter [HELP]

Item Setting

► Inbound Filter ☒ Enable

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

Virtual Server Rule -- IP address : Port (Service) --
Schedule rule (00)Always Copy to ID --

| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
|----|---------------------|------------------------|-------------------------------------|----------------|
| 1 | 1.2.3.100-1.2.3.199 | 21 | <input checked="" type="checkbox"/> | 0 |
| 2 | 1.2.3.100-1.2.3.199 | 199 | <input checked="" type="checkbox"/> | 0 |
| 3 | | | <input type="checkbox"/> | 0 |
| 4 | | | <input type="checkbox"/> | 0 |
| 5 | | | <input type="checkbox"/> | 0 |
| 6 | | | <input type="checkbox"/> | 0 |
| 7 | | | <input type="checkbox"/> | 0 |
| 8 | | | <input type="checkbox"/> | 0 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

<< Previous Next >> Save Undo Outbound Filter...

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

Others are all allowed.

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

Outbound Filter:

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

Example 1:

Router LAN IP is 192.168.12.254

The screenshot shows the Mikrotik WinBox interface for configuring the Inbound Packet Filter. The left sidebar lists navigation options: Packet Filters, Domain Filters, URL Blocking, MAC Access Control, and Miscellaneous. The main panel is titled 'Inbound Packet Filter' and includes a '[HELP]' link. It features a table with columns for ID, Source IP : Ports, Destination IP : Ports, Enable, and Schedule Rule#. Two rules are configured: Rule 1 allows traffic from 100-192.168.12.149 to 21-100, and Rule 2 allows traffic from 2.10-192.168.12.20. Rules 3 through 10 are disabled. The bottom of the panel contains navigation buttons: '<< Previous', 'Next >>', 'Save', 'Undo', and 'Outbound Filter...'.

| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
|----|--------------------|------------------------|-------------------------------------|----------------|
| 1 | 100-192.168.12.149 | 21-100 | <input checked="" type="checkbox"/> | 0 |
| 2 | 2.10-192.168.12.20 | | <input checked="" type="checkbox"/> | 0 |
| 3 | | | <input type="checkbox"/> | 0 |
| 4 | | | <input type="checkbox"/> | 0 |
| 5 | | | <input type="checkbox"/> | 0 |
| 6 | | | <input type="checkbox"/> | 0 |
| 7 | | | <input type="checkbox"/> | 0 |
| 8 | | | <input type="checkbox"/> | 0 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

(192.168.12.100-192.168.12.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing)

Others are all blocked.

Example 2:

Router LAN IP is 192.168.12.254

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

Packet Filters
Domain Filters
URL Blocking
MAC Access Control
Miscellaneous

Inbound Packet Filter [HELP]

| Item | Setting | | | |
|--|--|------------------------|-------------------------------------|----------------|
| Inbound Filter | <input checked="" type="checkbox"/> Enable | | | |
| <input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules. | | | | |
| Virtual Server Rule -- IP address : Port (Service) -- Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- | | | | |
| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
| 1 | 192.168.12.100 | : 21 | <input checked="" type="checkbox"/> | 0 |
| 2 | 192.168.12.119 | : 119 | <input checked="" type="checkbox"/> | 0 |
| 3 | | | <input type="checkbox"/> | 0 |
| 4 | | | <input type="checkbox"/> | 0 |
| 5 | | | <input type="checkbox"/> | 0 |
| 6 | | | <input type="checkbox"/> | 0 |
| 7 | | | <input type="checkbox"/> | 0 |
| 8 | | | <input type="checkbox"/> | 0 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

<< Previous Next >> Save Undo Outbound Filter...

(192.168.12.100 and 192.168.12.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

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

2.3.3.2 Domain filters

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

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

Enable it and show actions when someone accesses the specific URLs in syslog page.

Domain Filter
[HELP]

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

| ID | Domain Suffix | Action | Enable | Schedule Rule# |
|----|----------------------|--|--------------------------|--------------------------------|
| 1 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 2 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 3 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 4 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 5 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 6 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 7 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 8 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 9 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 10 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 11 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 12 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 13 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 14 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 15 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 16 | <input type="text"/> | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | <input type="text" value="0"/> |
| 17 | *(all others) | <input type="checkbox"/> Drop <input type="checkbox"/> Log | - | <input type="text" value="0"/> |

Save
Undo

Domain Filter

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

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

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

Privilege IP Addresses Range

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

Domain Suffix

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

Action

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

Enable

Check to enable each rule.

Example:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

• Packet Filters
• Domain Filters
• URL Blocking
• MAC Access Control
• Miscellaneous

Domain Filter [HELP]

| Item | | Setting | | |
|------------------------------|----------------|--|-------------------------------------|----------------|
| Domain Filter | | <input checked="" type="checkbox"/> Enable | | |
| Log DNS Query | | <input checked="" type="checkbox"/> Enable | | |
| Privilege IP Addresses Range | | From 0 To 0 | | |
| ID | Domain Suffix | Action | Enable | Schedule Rule# |
| 1 | www.msn.com | <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log | <input checked="" type="checkbox"/> | 0 |
| 2 | www.sina.com | <input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log | <input checked="" type="checkbox"/> | 0 |
| 3 | ww.baidu.com | <input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log | <input checked="" type="checkbox"/> | 0 |
| 4 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 5 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 6 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 7 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 8 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 9 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 10 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 11 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 12 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 13 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 14 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 15 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 16 | | <input type="checkbox"/> Drop <input type="checkbox"/> Log | <input type="checkbox"/> | 0 |
| 17 | * (all others) | <input type="checkbox"/> Drop <input type="checkbox"/> Log | - | 0 |

Save Undo

In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.
2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.

3. URL include “www.baidu.com” will be blocked, but the action will not be record in log-file.
4. IP address x.x.x.1~x.x.x.99 can access Internet without restriction.

2.3.3.3 URL Blocking

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

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

URL Blocking [HELP]

| Item | | Setting | |
|----------------|----------------------|---------------------------------|--------------------------------|
| ▶ URL Blocking | | <input type="checkbox"/> Enable | |
| ID | URL | Enable | Schedule Rule# |
| 1 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 2 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 3 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 4 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 5 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 6 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 7 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 8 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 9 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 10 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 11 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 12 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 13 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 14 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 15 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 16 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 17 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 18 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 19 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 20 | <input type="text"/> | <input type="checkbox"/> | <input type="text" value="0"/> |

Save Undo

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

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

URL Blocking Enable

Checked if you want to enable URL Blocking.

URL

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

Enable

Checked to enable each rule.

| ADMINISTRATOR's MAIN MENU | | | |
|--|------|-------------------------------------|----------------|
| Status Wizard Advanced Logout | | | |
| BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX | | | |
| URL Blocking [HELP] | | | |
| Item | | Setting | |
| URL Blocking | | <input type="checkbox"/> Enable | |
| ID | URL | Enable | Schedule Rule# |
| 1 | msn | <input checked="" type="checkbox"/> | 0 |
| 2 | sina | <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 |
| 9 | | <input type="checkbox"/> | 0 |
| 10 | | <input type="checkbox"/> | 0 |
| 11 | | <input type="checkbox"/> | 0 |
| 12 | | <input type="checkbox"/> | 0 |
| 13 | | <input type="checkbox"/> | 0 |
| 14 | | <input type="checkbox"/> | 0 |
| 15 | | <input type="checkbox"/> | 0 |
| 16 | | <input type="checkbox"/> | 0 |
| 17 | | <input type="checkbox"/> | 0 |
| 18 | | <input type="checkbox"/> | 0 |
| 19 | | <input type="checkbox"/> | 0 |
| 20 | | <input type="checkbox"/> | 0 |
| Save Undo | | | |

In this example:

1. URL include "msn" will be blocked, and the action will be record in log-file.
2. URL include "sina" will be blocked, but the action will be record in log-file

3.3.3.4 Internet Access Control

The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.

Administrator MAC Control

Regardless the MAC access configuration of administrator, specific MAC can access the device.

The screenshot shows the 'Administrator MAC Control' configuration page. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (selected), 'ADVANCED SETTING', and 'TOOLBOX'. A left sidebar lists 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Access Control' (selected), and 'Miscellaneous'. The main content area is titled 'Administrator MAC Control' with a '[HELP]' link. It features a 'DHCP clients' dropdown menu set to '--- Select one ---', a 'Copy to' button, and an 'ID' dropdown. Below this is a table with three columns: 'ID', 'MAC Address', and 'Enable'. The table contains three rows with IDs 1, 2, and 3. Each row has a text input field for the MAC Address and a checkbox in the 'Enable' column. At the bottom of the table are 'Save' and 'Undo' buttons.

| ID | MAC Address | Enable |
|----|----------------------|--------------------------|
| 1 | <input type="text"/> | <input type="checkbox"/> |
| 2 | <input type="text"/> | <input type="checkbox"/> |
| 3 | <input type="text"/> | <input type="checkbox"/> |

This device can record 3 sets. When the host(should be admin) logs Web management, the device will record MAC address of this host. Before this host configures Internet Access Control, Suggest end-user to enable this feature, first.

The screenshot shows the 'Internet Access Control' configuration page. It has a table with two columns: 'Item' and 'Setting'. The first row has 'Access Control Type' in the 'Item' column and three radio button options in the 'Setting' column: 'MAC Access Control', 'Group MAC Access Control', and 'Interface Access Control'. At the bottom of the page is a 'Next >>' button.

| Item | Setting |
|-----------------------|--|
| ► Access Control Type | <input type="radio"/> MAC Access Control <input type="radio"/> Group MAC Access Control <input type="radio"/> Interface Access Control |

1. MAC control

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

• Packet Filters
• Domain Filters
• URL Blocking
• MAC Access Control
• Miscellaneous

Allow you to allow or deny the wired and wireless clients to connect to this device and the Internet.

MAC Address Control [HELP]

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

DHCP clients:

Schedule Rule: ID:

| ID | MAC Address | IP Address | C | A | Schedule Rule |
|----|----------------------|---------------------------------|--------------------------|--------------------------|--------------------------------|
| 1 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 2 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 3 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 4 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |

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 | Schedule Rule |
|----|----------------------|---------------------------------|--------------------------|--------------------------|--------------------------------|
| 1 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 2 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 3 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 4 | <input type="text"/> | 192.168.1. <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |

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

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

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

DHCP clients

Copy to ID

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

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

Example:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

• Packet Filters
• Domain Filters
• URL Blocking
• MAC Access Control
• Miscellaneous

MAC Address Control [HELP]

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

DHCP clients ID

Schedule Rule ID

| ID | MAC Address | IP Address | C | A | Schedule Rule |
|----|-------------------|---------------|-------------------------------------|-------------------------------------|--------------------------------|
| 1 | 48-5D-60-9B-C0-A3 | 192.168.1.146 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| 2 | 0C-74-C2-D2-B9-17 | 192.168.1. | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| 3 | 0C-74-C2-D2-B9-16 | 192.168.1.62 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |
| 4 | | 192.168.1. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="0"/> |

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

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

ID 1 - " 48-5D-60-9B-C0-A3" --> 192.168.1.146

ID 3 - " 0C-74-C2-D2-B9-16" --> 192.168.1.62

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 (192.168.1.62), 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.

2. Group MAC Access Control

Administrator can define hosts in which Group to allow Internet. For example, Father and Mother are in Group1 without limitation and hosts Brother and Sister are in Group2 to access according to Schedule Rule2.

For example,

Schedule Rule 1 sets “always” everyday with limitation.

Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

The screenshot shows the 'Group MAC Access Control' configuration page. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (selected), 'ADVANCED SETTING', and 'TOOLBOX'. A left sidebar lists 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Access Control' (selected), and 'Miscellaneous'. The main content area is titled 'Group MAC Access Control' with a '[HELP]' link. It contains a table with 'Item' and 'Setting' columns, showing 'Group MAC Access Control' with an 'Enable' checkbox. Below this are 'Save' and 'Undo' buttons. The 'Add Member to Group List' section includes a form to add a MAC address to a group and apply a schedule rule. A confirmation message states: 'Add MAC : 48-5D-60-9B-C0-A3 to Group 2 !'. There are two group lists: 'Group List 1 - Always active.' and 'Group List 2 - Always active.'. Each list has a table with columns for 'MAC Address', 'Host Name', 'IP Address', and 'Action'. Group List 1 contains one entry with MAC '0C-74-C2-D2-B9-16', Host Name '@IP062', IP Address '192.168.1.62', and a 'Delete' button. Group List 2 contains one entry with MAC '48-5D-60-9B-C0-A3', Host Name 'Ray-NB', IP Address '192.168.1.146', and a 'Delete' button.

| Item | Setting |
|--------------------------|---------------------------------|
| Group MAC Access Control | <input type="checkbox"/> Enable |

Save Undo

Add Member to Group List

Add MAC Address - << Copy --- Select one ---
to Group 1 and apply schedule rule (00)Always Add

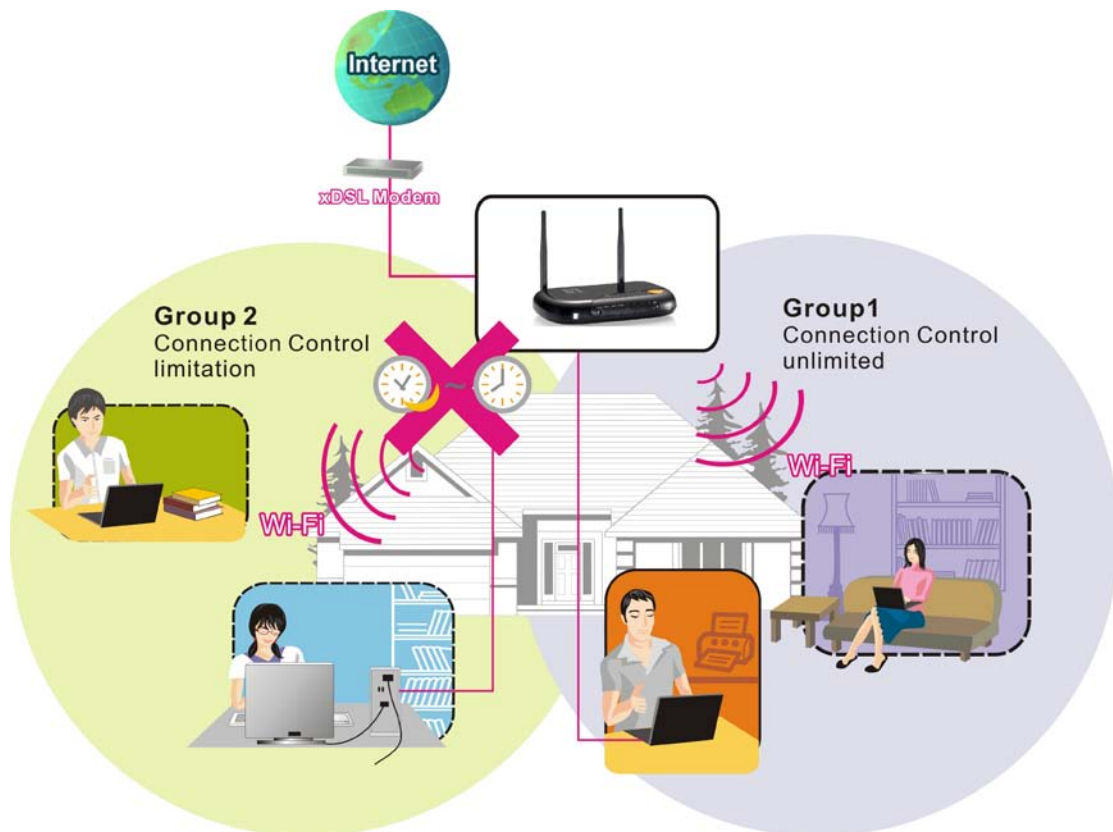
Add MAC : 48-5D-60-9B-C0-A3 to Group 2 !

Group List 1 - Always active.

| MAC Address | Host Name | IP Address | Action |
|-------------------|-----------|--------------|--------|
| 0C-74-C2-D2-B9-16 | @IP062 | 192.168.1.62 | Delete |

Group List 2 - Always active.

| MAC Address | Host Name | IP Address | Action |
|-------------------|-----------|---------------|--------|
| 48-5D-60-9B-C0-A3 | Ray-NB | 192.168.1.146 | Delete |



3. Interface Access Control

The device defines 5 Interfaces as Lan1,Lan2, Lan3,Lan4 and WiFi. The device allows different interface to access Internet by time schedule

For example,

Schedule Rule 1 sets “always” everyday with limitation.

Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

Administrator can set guests in Lan3 and Lan4 to access Internet according as Schedule Rule

2. Set Friends in Lan1 ,Lan2 and WiFi according as Schedule Rule 1.

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

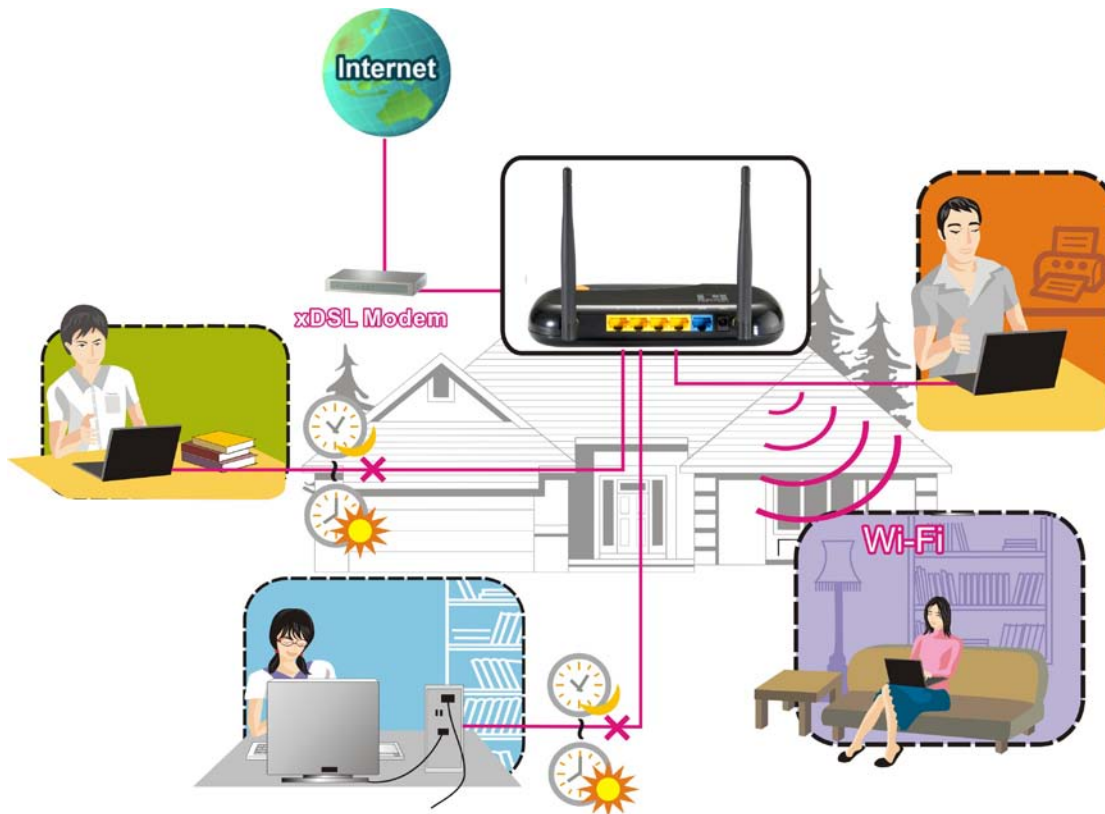
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

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

Interface Access Control
[HELP]

| Item | Setting | |
|--------------------------|--|-------------------------------------|
| Interface Access Control | <input checked="" type="checkbox"/> Enable | |
| Interface | Schedule Rule | Deny |
| Port 1 | (00)Always | <input checked="" type="checkbox"/> |
| Port 2 | (00)Always | <input checked="" type="checkbox"/> |
| Port 3 | (00)Always | <input checked="" type="checkbox"/> |
| Port 4 | (00)Always | <input checked="" type="checkbox"/> |
| Wireless | (00)Always | <input checked="" type="checkbox"/> |

Save
Undo



2.3.3.5 Miscellaneous Items

| Miscellaneous Items | | [HELP] |
|------------------------------------|----------------------------|-------------------------------------|
| Item | Setting | Enable |
| ▶ Remote Administrator Host / Port | 0.0.0.0 / 8080 | <input type="checkbox"/> |
| ▶ Administrator Time-out | 600 seconds (0 to disable) | |
| ▶ Discard PING from WAN side | | <input type="checkbox"/> |
| ▶ SPI mode | | <input type="checkbox"/> |
| ▶ DoS Attack Detection | | <input type="checkbox"/> |
| ▶ VPN PPTP Pass-Through | | <input checked="" type="checkbox"/> |
| ▶ VPN IPSec Pass-Through | | <input checked="" type="checkbox"/> |
| <div>Save Undo</div> | | |

Remote Administrator Host/Port

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

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

Administrator Time-out

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

Discard PING from WAN side

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

SPI Mode

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

DoS Attack Detection

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

VPN PPTP and IPSec Pass-Through

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

2.3.4 Advanced Settings

The screenshot displays the LevelOne Administrator's Main Menu. The top navigation bar includes the LevelOne logo, a language dropdown set to 'English', and links for 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (which is highlighted), and 'TOOLBOX'. On the left side, a vertical sidebar lists several settings: 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing', and 'Schedule Rule'. The main content area, titled 'Advanced Setting', contains a bulleted list of settings with brief descriptions:

- **System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- **System Log**
 - Send system log to a dedicated host or email to specific recipients.
- **Dynamic DNS**
 - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- **QoS Rule**
 - Quality of Service provides different priority to different users or data types, or guarantee a certain level of performance.
- **SNMP**
 - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- **Routing**
 - If you have more than one router and subnet, you can use a routing table to allow packets to follow the proper paths and allow different subnets to communicate with each other.
- **Schedule Rule**
 - Apply schedule rules to Packet Filters and Virtual Server.

2.3.4.1 System Time

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

System Time System Log Dynamic DNS SNMP Routing Schedule Rule

System Time [HELP]

| Item | Setting |
|--|---|
| System Time | 2009年6月1日 上午 01:43:55 |
| <input checked="" type="radio"/> Get Date and Time by NTP Protocol | <input type="button" value="Sync Now !"/> |
| Time Server | time.nist.gov |
| Time Zone | (GMT-08:00) Pacific Time (US & Canada) |
| <input type="radio"/> Set Date and Time using PC's Date and Time | |
| PC Date and Time | 2012年7月2日 下午 03:47:24 |
| <input type="radio"/> Set Date and Time manually | |
| Date | Year: 2009 Month: Jun Day: 01 |
| Time | Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59) |
| Daylight Saving | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Start | Month: Jan Day: 01 Hour: 00 |
| End | Month: Jan Day: 01 Hour: 00 |

Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

Daylight Saving: Set up where the location is.

2.3.4.2 System Log

| Item | Setting | Enable |
|-----------------------------|--|--------------------------|
| IP Address of Syslog Server | 192.168.1. | <input type="checkbox"/> |
| E-mail Alert | <input type="button" value="Send Mail Now"/> | <input type="checkbox"/> |
| SMTP Server IP/Port | <input type="text"/> | |
| E-mail addresses | <input type="text"/> | |
| E-mail Subject | <input type="text"/> | |
| User name | <input type="text"/> | |
| Password | <input type="text"/> | |
| Log Type | <input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice | |

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

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

E-mail Alert Enable

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

SMTP Server IP and Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

Send E-mail alert to

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

2.3.4.3 Dynamic DNS

The screenshot shows a web interface for configuring Dynamic DNS. At the top, there is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a tabbed interface with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (selected), and 'TOOLBOX'. On the left, a sidebar lists 'System Time', 'System Log', 'Dynamic DNS' (selected), 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' with a '[HELP]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has five rows: 'DDNS' with radio buttons for 'Disable' (selected) and 'Enable'; 'Provider' with a dropdown menu showing 'DynDNS.org(Dynamic)' and a 'Provider website' button; 'Host Name' with a text input field; 'Username / E-mail' with a text input field; and 'Password / Key' with a text input field. At the bottom of the table are 'Save' and 'Undo' buttons.

| Item | Setting |
|-------------------|---|
| DDNS | <input 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"/> |

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.

2.3.4.4 SNMP

The screenshot shows the 'ADMINISTRATOR'S MAIN MENU' at the top with links for Status, Wizard, Advanced, and Logout. Below this is a navigation bar with icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING (which is highlighted), and TOOLBOX. On the left side, there is a sidebar menu with options: System Time, System Log, Dynamic DNS, SNMP (highlighted), Routing, and Schedule Rule. The main content area is titled 'SNMP Setting' with a '[HELP]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has the following rows: 'Enable SNMP' with checkboxes for 'Local' (checked) and 'Remote'; 'Get Community' with a text input field containing 'public'; 'Set Community' with a text input field containing 'private'; 'IP 1' through 'IP 4' each with a text input field; and 'SNMP Version' with radio buttons for 'V1' and 'V2c' (selected). At the bottom of the table are 'Save' and 'Undo' buttons.

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

Save Undo

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

Enable SNMP

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

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

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

SNMP Version

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

WAN Access IP Address

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

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

2.3.4.5 Routing

The screenshot shows a web-based configuration interface for a network device. 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' (which is highlighted), and 'TOOLBOX'. On the left side, there is a sidebar menu with options: 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing' (which is selected), and 'Schedule Rule'. The main content area is titled 'Routing Table' with a '[HELP]' link. It contains two sections: 'Dynamic Routing' with radio buttons for 'Disable' (selected), 'RIPv1', and 'RIPv2'; and 'Static Routing' with radio buttons for 'Disable' (selected) and 'Enable'. Below these is a table with 6 columns: 'ID', 'Destination', 'Subnet Mask', 'Gateway', 'Hop', and 'Enable'. The table has 8 rows, each with input fields for the first five columns and a checkbox for the 'Enable' column. At the bottom of the table are 'Save' and 'Undo' buttons.

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

Save Undo

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

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

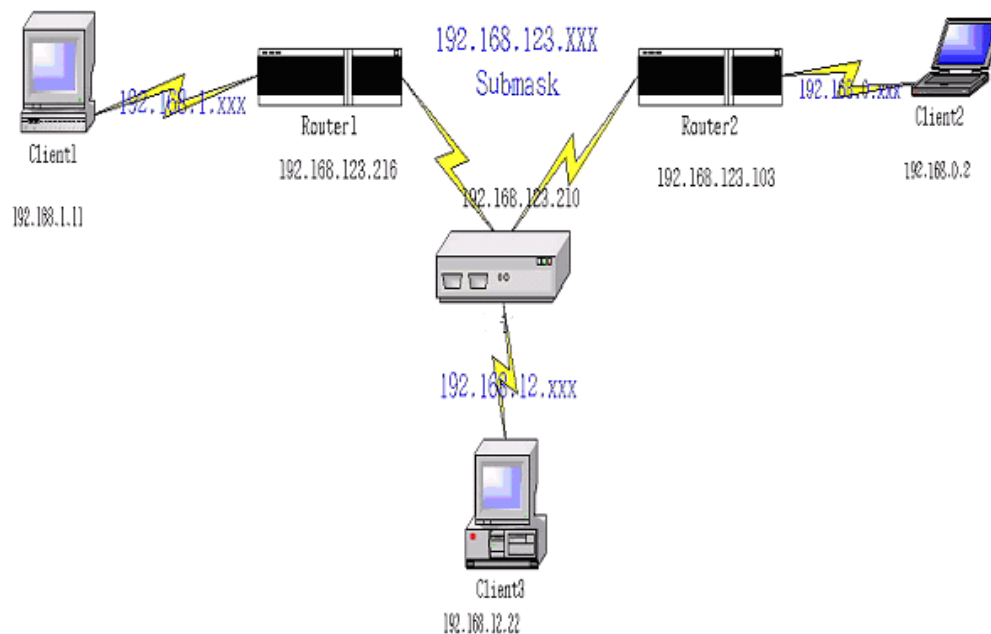
Dynamic Routing

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

Otherwise, please select RIPv1 if you need this protocol.

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

Example:



Configuration on NAT Router

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

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

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

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

2.3.4.6 Schedule Rule

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

• System Time
• System Log
• Dynamic DNS
• SNMP
• Routing
• **Schedule Rule**

Schedule Rule [HELP]

| Item | Setting | |
|------------|---------------------------------|--------|
| ▶ Schedule | <input type="checkbox"/> Enable | |
| Rule# | Rule Name | Action |

Save 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

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

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

• System Time
• System Log
• Dynamic DNS
• SNMP
• Routing
• **Schedule Rule**

Schedule Rule Setting [HELP]

| Item | Setting | |
|------------------|-----------------------|------------------|
| ▶ Name of Rule 1 | | |
| ▶ System Time | 2009年6月1日 上午 01:46:39 | |
| Week Day | Start Time (hh:mm) | End Time (hh:mm) |
| Sunday | : | : |
| Monday | : | : |
| Tuesday | : | : |
| Wednesday | : | : |
| Thursday | : | : |
| Friday | : | : |
| Saturday | : | : |
| Every Day | : | : |

Save Undo Back

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

To edit the schedule rule.

Delete

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

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Example1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:20 to 16:30)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

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

Virtual Server Special AP Miscellaneous

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 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 2 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 3 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 4 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 5 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 6 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 7 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 8 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 9 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |
| 10 | 192.168.1. | | | Both | <input type="checkbox"/> | 0 |

Next >> Save Undo

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

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

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

Outbound Packet Filter
[HELP]

| Item | Setting | | | |
|--|--|------------------------|-------------------------------------|----------------|
| Outbound Filter | <input checked="" type="checkbox"/> Enable | | | |
| <input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules. | | | | |
| Block List -- select one -- Schedule rule (00)Always Copy to ID -- | | | | |
| ID | Source IP : Ports | Destination IP : Ports | Enable | Schedule Rule# |
| 1 | | : 21 | <input checked="" type="checkbox"/> | 1 |
| 2 | | | <input 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 |
| 9 | | | <input type="checkbox"/> | 0 |
| 10 | | | <input type="checkbox"/> | 0 |

2.3.5 Toolbox

The screenshot displays the LevelOne administrator web interface. At the top, there is a blue header with the LevelOne logo on the left and a language dropdown menu set to 'English' on the right. Below the header is a navigation bar with several tabs: 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains icons and labels for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The 'TOOLBOX' tab is currently selected. On the left side of the main content area, there is a vertical sidebar with a list of links: 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area features a window titled 'Toolbox' which contains a bulleted list of the same six items, each followed by a brief description of its function.

levelone
English

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

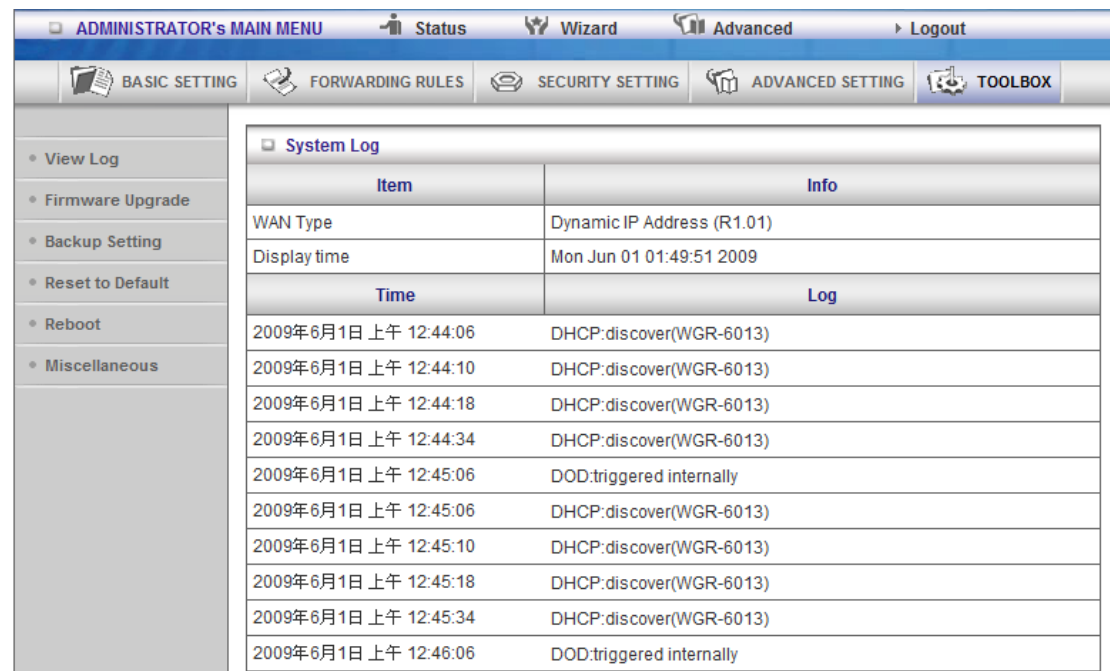
BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING **TOOLBOX**

• View Log
• Firmware Upgrade
• Backup Setting
• Reset to Default
• Reboot
• Miscellaneous

Toolbox

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

2.3.5.1 View Log



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

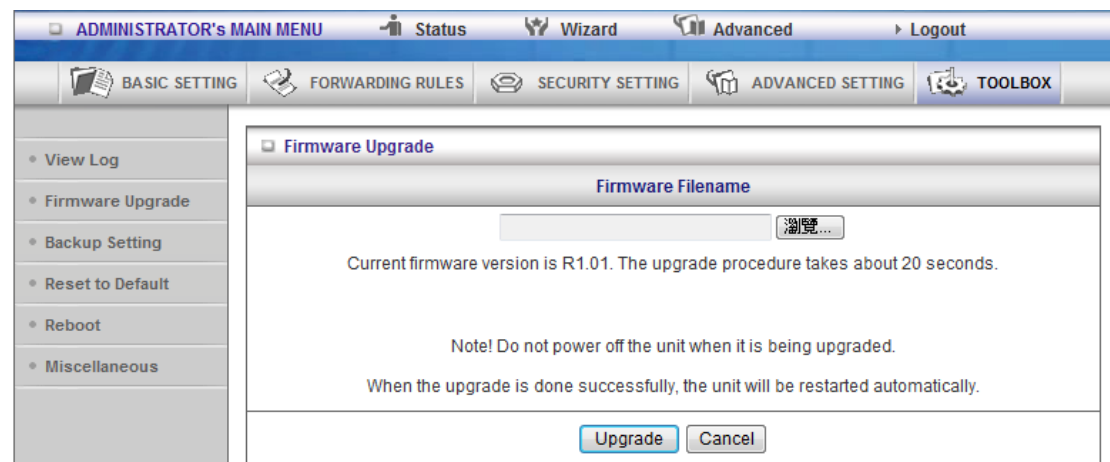
- View Log
- Firmware Upgrade
- Backup Setting
- Reset to Default
- Reboot
- Miscellaneous

System Log

| Item | Info |
|-----------------------|----------------------------|
| WAN Type | Dynamic IP Address (R1.01) |
| Display time | Mon Jun 01 01:49:51 2009 |
| Time | Log |
| 2009年6月1日 上午 12:44:06 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:44:10 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:44:18 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:44:34 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:45:06 | DOD:triggered internally |
| 2009年6月1日 上午 12:45:06 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:45:10 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:45:18 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:45:34 | DHCP:discover(WGR-6013) |
| 2009年6月1日 上午 12:46:06 | DOD:triggered internally |

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

2.3.5.2 Firmware Upgrade



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- View Log
- Firmware Upgrade
- Backup Setting
- Reset to Default
- Reboot
- Miscellaneous

Firmware Upgrade

Firmware Filename

Current firmware version is R1.01. The upgrade procedure takes about 20 seconds.

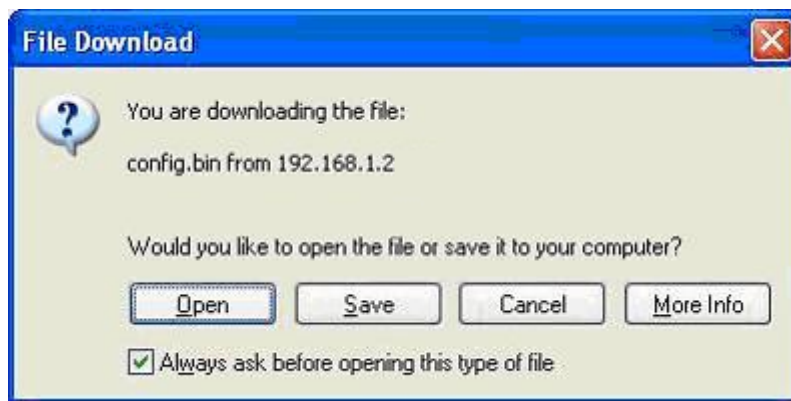
Note! Do not power off the unit when it is being upgraded.

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

Upgrade Cancel

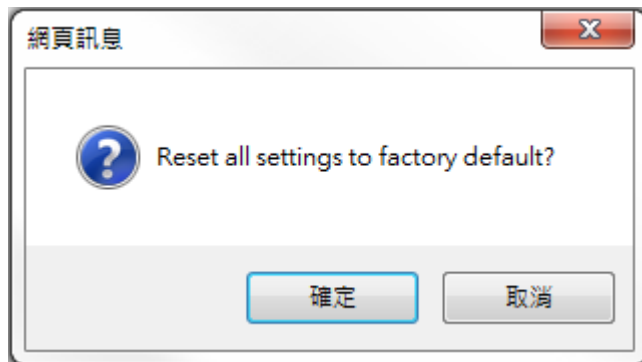
You can upgrade firmware by clicking **Firmware Upgrade** button.

2.3.5.3 Backup Setting



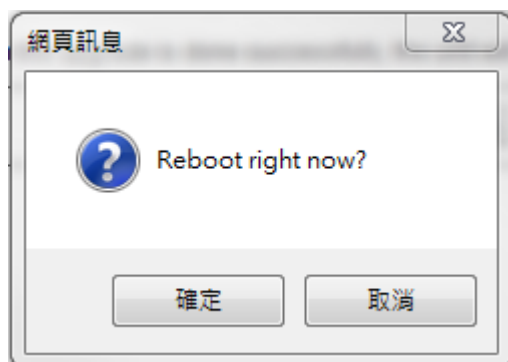
You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

2.3.5.4 Reset to default



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

2.3.5.5 Reboot



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

2.3.5.6 Miscellaneous Items

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

MAC Address for Wake-on-LAN

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

Domain Name or IP Address for Test

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

Appendix A FAQ and Troubleshooting

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

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

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



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

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

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

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

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

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

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

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

If not, please check How blinking Status led shows.

There are many abnormal symptoms as below:

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

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

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

3. How to reset to factory default?

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

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

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

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

| Choose WAN Type | |
|---|--|
| Type | Usage |
| <input type="radio"/> Static IP Address | ISP assigns you a static IP address. |
| <input checked="" type="radio"/> Dynamic IP Address | Obtain an IP address from ISP automatically. |
| <input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond) | |
| <input type="radio"/> PPP over Ethernet | Some ISPs require the use of PPPoE to connect to their services. |
| <input type="radio"/> PPTP | Some ISPs require the use of PPTP to connect to their services. |
| <input type="radio"/> L2TP | Some ISPs require the use of L2TP to connect to their services. |

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

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

How do I connect router by using wireless?

1. How to start to use wireless?

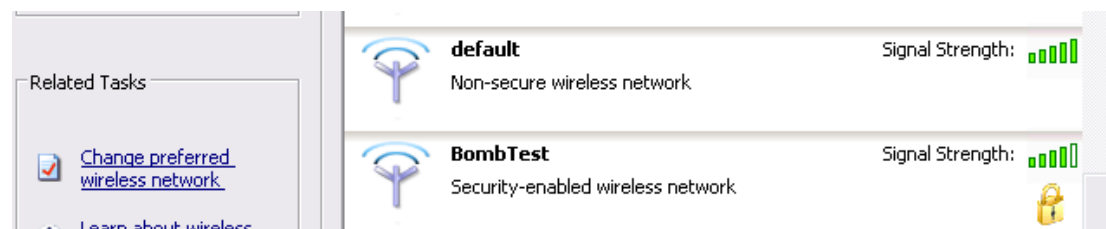
A: First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

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

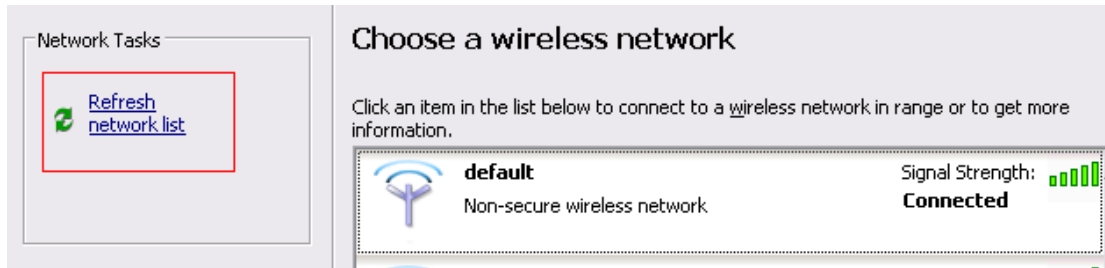
About wireless client, you will see wireless icon:



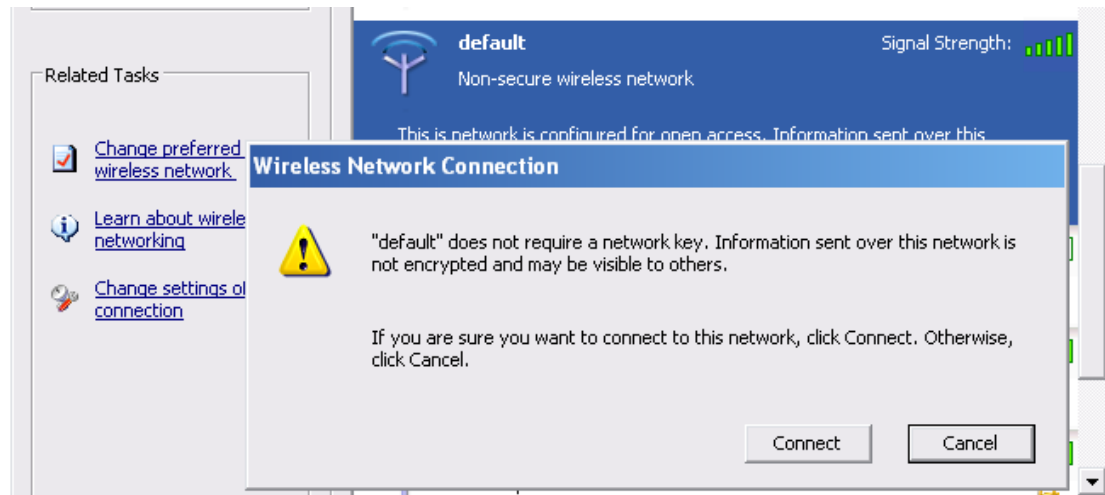
Then click and will see the ap list that wireless client can be accessed:



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



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



If successfully, the computer will show



and get ip from router:

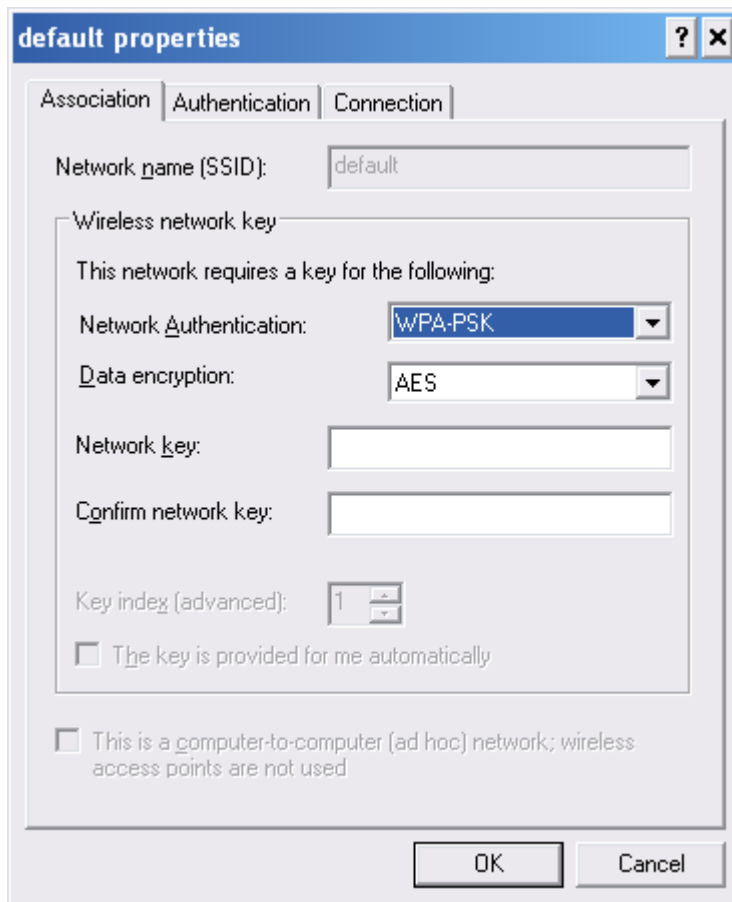


2. When I use AES encryption of WPA-PSK to connect even if I input the correct pre-share key?

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.