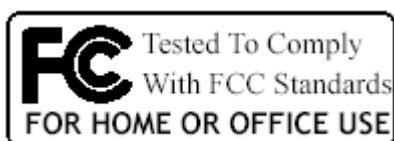


# User's Manual

Version: 1.1

**WLAN 11g Router**

WA-2204A



## **Trademarks**

Copyright ©2005

Contents are subject to change without notice.

All trademarks belong to their respective proprietors.

## **Copyright Statement**

THIS DOCUMENT CONTAINS OF PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THIS COMPANY. AND NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRICAL OR MECHANICAL, BY PHOTOCOPYING, RECORDING, OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF THIS COMPANY.

## INFORMATION TO USER

### **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

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

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

Installation and use of this **WLAN 11g Router** must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

**FCC RF Radiation Exposure Statement: This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.**

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance **20cm** between the radiator and your body.

Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

“CC&C Technologies, Inc. declare that WA-2204A , (FCC ID: PANWA2204A) is limited in CH1~CH 11 by specified firmware controller in USA. ”

The users manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

特別警示：

根據交通部低功率電波輻射性電機管理辦法第十二條及第十四條規定：

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

## REGULATORY INFORMATION

WLAN 11g Router must be installed and used in strict accordance with the instructions. This device complies with the following radio frequency and safety standards.

### **USA - Federal Communications Commission (FCC)**

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

### **Europe- R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

### **CE Declaration of Conformity**

For the following equipment:

**WLAN 11g Router**

---

(Product Name)

**WA-2204A**

---

(Model Designation)

is herewith confirmed to comply with the requirements set out in the Council (European parliament) Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility of Radio and Telecom device (1999/5/EC). For the evaluation regarding this Directive, the following standards were applied:

EN 300 328 V1.6.1 (2004-11)

---

EN 301 489-1 V1.4.1 (2002-08), EN 301 489-17 V1.2.1 (2002-08)

---

EN 60950-1: 2001

---

## EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

## EU Countries Not intended for use

None.

## Potential restrictive use

France: Only channels 10,11,12, and 13

The channel identifiers, channel center frequencies, and regulatory domains of each 22-MHz-wide channel are shown in following Table.

| Channel Identifier | Center Frequency (MHZ) | Regulatory Domains |      |               |        |        |        |
|--------------------|------------------------|--------------------|------|---------------|--------|--------|--------|
|                    |                        | Japan              | ETSI | North America | Israel | France | Mexico |
| 1                  | 2412                   | ✓                  | ✓    | ✓             |        |        |        |
| 2                  | 2417                   | ✓                  | ✓    | ✓             |        |        |        |
| 3                  | 2422                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 4                  | 2427                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 5                  | 2432                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 6                  | 2437                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 7                  | 2442                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 8                  | 2447                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 9                  | 2452                   | ✓                  | ✓    | ✓             | ✓      |        |        |
| 10                 | 2457                   | ✓                  | ✓    | ✓             |        | ✓      | ✓      |
| 11                 | 2462                   | ✓                  | ✓    | ✓             |        | ✓      | ✓      |
| 12                 | 2467                   | ✓                  | ✓    |               |        | ✓      |        |
| 13                 | 2472                   | ✓                  | ✓    |               |        | ✓      |        |
| 14                 | 2484                   | ✓                  |      |               |        |        |        |

# Table of Contents

**REVISION HISTORY ..... I**

**TERMINOLOGY ..... II**

**1 INTRODUCTION..... 1**

    1.1 PACKAGE CONTENTS ..... 1

    1.2 PRODUCT SPECIFICATIONS ..... 1

    1.3 PRODUCT FEATURES ..... 2

    1.4 FRONT PANEL DESCRIPTION..... 3

    1.5 REAR PANEL DESCRIPTION..... 4

**2 INSTALLATION ..... 6**

    2.1 HARDWARE INSTALLATION ..... 6

    2.2 SOFTWARE INSTALLATION..... 6

**3 SOFTWARE CONFIGURATION ..... 7**

    3.1 PREPARE YOUR PC TO CONFIGURE THE WLAN 11G ROUTER ..... 7

    3.2 CONNECT TO THE WLAN 11G ROUTER ..... 9

    3.3 MANAGEMENT AND CONFIGURATION ON THE WLAN 11G ROUTER..... 9

        3.3.1 Status..... 9

        3.3.2 Setup Wizard..... 11

            I Operation Mode ..... 11

            II Time Zone Setting..... 12

            III LAN Interface Setup ..... 12

            IV WAN Interface Setup ..... 13

            V Wireless Basic Settings..... 13

            VI Wireless Security Setup ..... 14

        3.3.3 Operation Mode ..... 14

        3.3.4 Wireless - Basic Settings..... 15

        3.3.5 Wireless - Advanced Settings ..... 16

        3.3.6 Wireless - Security Setup..... 18

            I WEP Key Setup ..... 20

        3.3.7 Wireless - Access Control..... 21

        3.3.8 WDS Settings..... 22

|          |  |           |
|----------|--|-----------|
| I        | WDS Security Setup .....                                       | 23        |
| II       | WDS AP Table .....   | 24        |
| 3.3.9    | Site Survey .....  | 25        |
| 3.3.10   | LAN Interface Setup .....                                      | 25        |
| 3.3.11   | WAN Interface Setup .....                                      | 27        |
| I        | Static IP .....  | 27        |
| II       | DHCP Client .....  | 28        |
| III      | PPPoE .....  | 30        |
| IV       | PPTP .....   | 32        |
| 3.3.12   | Firewall - Port Filtering .....                                | 33        |
| 3.3.13   | Firewall - IP Filtering .....                                  | 34        |
| 3.3.14   | Firewall - MAC Filtering .....                                 | 35        |
| 3.3.15   | Firewall - Port Forwarding .....                               | 36        |
| 3.3.16   | Firewall - DMZ .....   | 38        |
| 3.3.17   | VPN Setting .....  | 38        |
| I        | VPN Setup - Edit Tunnel .....                                  | 40        |
| II       | Advanced IKE Setup.....  | 42        |
| 3.3.18   | Management - Statistics .....                                  | 43        |
| 3.3.19   | Management - DDNS .....  | 44        |
| 3.3.20   | Management - Time Zone Setting.....                            | 45        |
| 3.3.21   | Management - Log .....   | 45        |
| 3.3.22   | Management - Upgrade Firmware .....                            | 46        |
| 3.3.23   | Management Save/ Reload Settings.....                          | 47        |
| 3.3.24   | Management - Password Setup .....                              | 48        |
| 3.3.25   | Logout .....   | 48        |
| <b>4</b> | <b>FREQUENTLY ASKED QUESTIONS (FAQ).....</b>                   | <b>50</b> |
| 4.1      | WHAT AND HOW TO FIND MY PC'S IP AND MAC ADDRESS? .....         | 50        |
| 4.2      | WHAT IS WIRELESS LAN? .....                                    | 50        |
| 4.3      | WHAT ARE ISM BANDS? .....                                      | 50        |
| 4.4      | HOW DOES WIRELESS NETWORKING WORK?.....                        | 50        |
| 4.5      | WHAT IS BSSID? .....   | 51        |
| 4.6      | WHAT IS ESSID? .....   | 51        |
| 4.7      | WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE? ..... | 52        |
| 4.8      | WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS? ..... | 52        |
| 4.9      | WHAT IS WEP? .....   | 52        |
| 4.10     | WHAT IS FRAGMENT THRESHOLD?.....                               | 52        |



4.11 WHAT IS RTS (REQUEST TO SEND) THRESHOLD? ..... 53

4.12 WHAT IS BEACON INTERVAL? ..... 53

4.13 WHAT IS PREAMBLE TYPE? ..... 54

4.14 WHAT IS SSID BROADCAST? ..... 54

4.15 WHAT IS WI-FI PROTECTED ACCESS (WPA)? ..... 54

4.16 WHAT IS WPA2? ..... 55

4.17 WHAT IS 802.1X AUTHENTICATION? ..... 55

4.18 WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)? ..... 55

4.19 WHAT IS ADVANCED ENCRYPTION STANDARD (AES)? ..... 55

4.20 WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)? ..... 55

4.21 WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)? ..... 56

4.22 WHAT IS UNIVERSAL PLUG AND PLAY (UPNP)? ..... 56

4.23 WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE? ..... 56

4.24 WHAT IS CLONE MAC ADDRESS? ..... 56

4.25 WHAT IS DDNS? ..... 56

4.26 WHAT IS NTP CLIENT? ..... 56

4.27 WHAT IS VPN? ..... 56

4.28 WHAT IS IPSEC? ..... 57

5.1 EXAMPLE ONE – PPPoE ON THE WAN ..... 58

5.2 EXAMPLE TWO – FIXED IP ON THE WAN ..... 60

## Revision History

| <b>DATE</b> | <b>REVISION OF USER'S MANUAL</b>  | <b>FIRMWARE</b> |
|-------------|-----------------------------------|-----------------|
| 2005/4/7    | First release (Version 1.0)       | V1.2.0          |
| 2005/6/15   | Add product with SMA Antenna info | V1.2.x          |

## Terminology

|         |  |
|---------|--|
| 3DES    | Triple Data Encryption Standard                    |
| AES     | Advanced Encryption Standard                       |
| ANSI    | American National Standards Institute              |
| AP      | Access Point                                       |
| CCK     | Complementary Code Keying                          |
| CSMA/CA | Carrier Sense Multiple Access/ Collision Avoidance |
| CSMA/CD | Carrier Sense Multiple Access/ Collision Detection |
| DDNS    | Dynamic Domain Name Server                         |
| DH      | Diffie-Hellman Algorithm                           |
| DHCP    | Dynamic Host Configuration Protocol                |
| DSSS    | Direct Sequence Spread Spectrum                    |
| EAP     | Extensible Authentication Protocol                 |
| ESP     | Encapsulating Security Payload                     |
| FCC     | Federal Communications Commission                  |
| FTP     | File Transfer Protocol                             |
| IEEE    | Institute of Electrical and Electronic Engineers   |
| IKE     | Internet Key Exchange                              |
| IP      | Internet Protocol                                  |
| ISM     | Industrial, Scientific and Medical                 |
| LAN     | Local Area Network                                 |
| MAC     | Media Access Control                               |
| MD5     | Message Digest 5                                   |
| NAT     | Network Address Translation                        |
| NT      | Network Termination                                |
| NTP     | Network Time Protocol                              |
| PPTP    | Point to Point Tunneling Protocol                  |
| PSD     | Power Spectral Density                             |
| RF      | Radio Frequency                                    |
| SHA1    | Secure Hash Algorithm                              |
| SNR     | Signal to Noise Ratio                              |
| SSID    | Service Set Identification                         |
| TCP     | Transmission Control Protocol                      |
| TFTP    | Trivial File Transfer Protocol                     |

---

|      |                                 |
|------|---------------------------------|
| TKIP | Temporal Key Integrity Protocol |
| UPNP | Universal Plug and Play         |
| VPN  | Virtual Private Network         |
| WDS  | Wireless Distribution System    |
| WEP  | Wired Equivalent Privacy        |
| WLAN | Wireless Local Area Network     |
| WPA  | Wi-Fi Protected Access          |

## 1 Introduction

The Wireless LAN 11g Router is an affordable IEEE 802.11b/g wireless LAN broadband router solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN.

This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

### 1.1 Package contents

The package of the WLAN 11g Router includes the following items,

- ✓ The WLAN 11g Router
- ✓ The AC to DC power adapter
- ✓ The Documentation CD
- ✓ 1.8M RJ-45 Cable Line

### 1.2 Product Specifications

|                       |  |
|-----------------------|--|
| Product Name          | WLAN 11g Router  |
| Standard              | 802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT)  |
| Data Transfer Rate    | 54Mbps(Wireless), 100Mbps(Ethernet)  |
| Modulation Method     | CCK(802.11b), OFDM(802.11g)  |
| Frequency Band        | 2.4GHz – 2.4835GHz ISM Band, DSSS  |
| RF Output Power       | CCK:22.9 dBm, OFDM:17.71 dBm   |
| Receiver Sensitivity  | 802.11b -80 dBm@8%, 802.11g -68 dBm@5%   |
| Operation Range       | 30 to 280 meters (depend on surrounding)   |
| Antenna               | External Antenna   |
| LED                   | Power, Active (WLAN), Act/Link (Ethernet)  |
| Security              | 64 bit/ 128 bit WEP, WPA, WPA2, port filtering, IP filtering, MAC filtering, port forwarding and DMZ hosting |
| LAN interface         | One 10/100BaseT with RJ45 connector (WAN)<br>Four 10/100BaseT with RJ45 connectors (LAN)                     |
| Power Consumption     | 7.5V DC Power Adapter  |
| Operating Temperature | 0 ~ 50°C ambient temperature   |
| Storage Temperature   | -20 ~ 70°C ambient temperature   |
| Humidity              | 5 to 90 % maximum (non-condensing)   |
| Dimension             | 137 x 96 x 35 mm   |

### 1.3 Product Features

- Complies with IEEE 802.11b/g standard for 2.4GHz Wireless LAN.
- Supports bridging, routing, VPN, WISP functions between wireless and wired Ethernet interfaces.
- Supports 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- Supports Inter-Access Point Protocol (IAPP).
- Supports Wireless Distribution System (WDS).
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client for Ethernet WAN interface auto IP address assignment.
- Supports static and dynamic IP routing.
- Supports PPPoE on Ethernet WAN interface.
- Supports clone MAC address function.
- Supports firewall security with port filtering, IP filtering, MAC filtering, port forwarding, trigger port and DMZ hosting functions.
- Supports WEB based management and configuration.
- Supports PPTP Client on Ethernet WAN interface.
- Supports UPnP for automatic Internet access.
- Supports Dynamic DNS service.
- Supports NTP client service.
- Supports Log table and remote Log service.
- Support Setup Wizard mode.
- Supports Virtual Private Network (VPN) connection.
- Supports IPSEC tunnel encryption(3DES/AES128) and authentication(MD5/SHA1)
- Supports WISP (Wireless ISP).

### 1.4 Front Panel Description

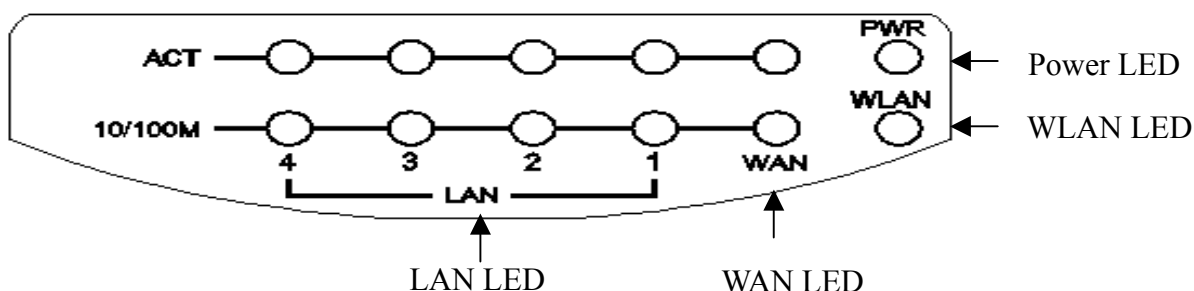


Figure 1 –WLAN 11g Router Front Panel

| LED Indicator | State    | Description  |  |
|---------------|----------|--|--|
| 1. Power LED  | On       | The WLAN11g Router is powered on.                    |  |
|               | Off      | The WLAN 11g Router is powered off.                  |  |
| 2. WLAN LED   | Flashing | Data is transmitting or receiving on the antenna.    |  |
|               | Off      | No data is transmitting or receiving on the antenna. |  |
| 3. WAN LED    | ACT      | Flashing   | Data is transmitting or receiving on the WAN interface.    |
|               |          | Off  | No data is transmitting or receiving on the WAN interface. |
| 10/100M       | On       | Connection speed is 100Mbps on WAN interface.        |  |
|               | Off      | Connection speed is 10Mbps on WAN interface.         |  |
| 4. LAN LED    | ACT      | Flashing   | Data is transmitting or receiving on the LAN interface.    |
|               |          | Off  | No data is transmitting or receiving on the LAN interface. |
| 10/100M       | On       | Connection speed is 100Mbps on LAN interface.        |  |
|               | Off      | Connection speed is 10Mbps on LAN interface.         |  |

### 1.5 Rear Panel Description

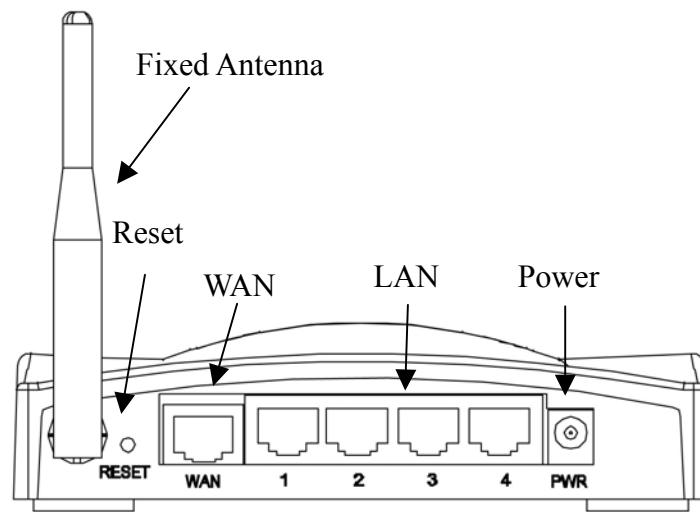


Figure 2 – WLAN 11g Router Rear Panel (Fixed Antenna)



| <b>Interfaces</b>     | <b>Description</b>   |
|-----------------------|--|
| 1. Antenna<br>(Fixed) | The Wireless LAN Antenna.<br>(Figure 2)  |
| 2. Reset              | Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.  |
| 3. WAN                | The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively. |
| 4. LAN                | The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.  |
| 5. Power              | The power jack allows an external DC +7.5 V power supply connection.<br>The external AC to DC adaptor provide adaptive power requirement to the WLAN 11g Router.             |

## 2 Installation

### 2.1 Hardware Installation

Step 1: Place the Wireless LAN 11g Router to the best optimum transmission location.

The best transmission location for your WLAN 11g Router is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

Step 2: Connect the WLAN 11g Router to your wired network. Connect the Ethernet WAN interface of WLAN 11g Router by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the WLAN 11g Router. Use only the AC/DC power adapter supplied with the WLAN 11g Router; it may occur damage by using a different type of power adapter.

The hardware installation finished.

### 2.2 Software Installation

- There are no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

**Notice: It will take about 55 seconds to complete the boot up sequence after powered on the WLAN 11g Router; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.**

### 3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The WLAN 11g Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.1.254**

Default IP subnet mask: **255.255.255.0**

WEB login User Name: *<empty>*

WEB login Password: *<empty>*

#### 3.1 Prepare your PC to configure the WLAN 11g Router

##### **For OS of Microsoft Windows 95/ 98/ Me:**

1. Click the **Start** button and select **Settings**, then click **Control Panel**. The **Control Panel** window will appear.  
**Note:** Windows Me users may not see the Network control panel. If so, **select View all Control Panel options** on the left side of the window
2. Move mouse and double-click the right button on **Network** icon. The **Network** window will appear.
3. Check the installed list of **Network Components**. If TCP/IP is not installed, click the **Add** button to install it; otherwise go to step 6.
4. Select **Protocol** in the **Network Component Type** dialog box and click **Add** button.
5. Select **TCP/IP** in **Microsoft** of **Select Network Protocol** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to **Network** dialog box after the TCP/IP installation.
6. Select **TCP/IP** and click the **properties** button on the **Network** dialog box.
7. Select **Specify an IP address** and type in values as following example.
  - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
  - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK and reboot your PC after completes the IP parameters setting.

##### **For OS of Microsoft Windows 2000, XP:**

1. Click the **Start** button and select **Settings**, then click **Control Panel**. The **Control**

- Panel* window will appear.
2. Move mouse and double-click the right button on *Network and Dial-up Connections* icon. Move mouse and double-click the *Local Area Connection* icon. The *Local Area Connection* window will appear. Click *Properties* button in the *Local Area Connection* window.
  3. Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
  4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
  5. Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
  6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
  7. Select *Specify an IP address* and type in values as following example.
    - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
    - ✓ IP Subnet Mask: **255.255.255.0**
  8. Click OK to completes the IP parameters setting.

#### **For OS of Microsoft Windows NT:**

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear. Click *Protocol* tab from the *Network* window.
3. Check the installed list of *Network Protocol* window. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
5. Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
7. Select *Specify an IP address* and type in values as following example.
  - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
  - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

### 3.2 Connect to the WLAN 11g Router

Open a WEB browser, i.e. Microsoft Internet Explore, then enter 192.168.1.254 on the URL to connect the WLAN 11g Router.

### 3.3 Management and configuration on the WLAN 11g Router

#### 3.3.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.

| <b>Broadband Router Status</b>  |                   |
|---|-------------------|
| This page shows the current status and some basic settings of the device. |                   |
| <b>System</b>   |                   |
| Uptime  | 0day:0h:2m:21s    |
| Firmware Version  | v1.2.0            |
| <b>Wireless Configuration</b>   |                   |
| Mode  | AP                |
| Band  | 2.4 GHz (B+G)     |
| SSID  | MyWLAN            |
| Channel Number  | 11                |
| Encryption  | Disabled          |
| BSSID   | 00:02:72:00:81:86 |
| Associated Clients  | 1                 |
| <b>TCP/IP Configuration</b>   |                   |
| Attain IP Protocol  | Fixed IP          |
| IP Address  | 192.168.1.254     |
| Subnet Mask   | 255.255.255.0     |
| Default Gateway   | 192.168.1.254     |
| DHCP Server   | Enabled           |
| MAC Address   | 00:02:72:00:81:86 |
| <b>WAN Configuration</b>  |                   |
| Attain IP Protocol  | DHCP              |
| IP Address  | 192.168.0.107     |
| Subnet Mask   | 255.255.255.0     |
| Default Gateway   | 192.168.0.10      |
| MAC Address   | 00:02:72:00:81:87 |

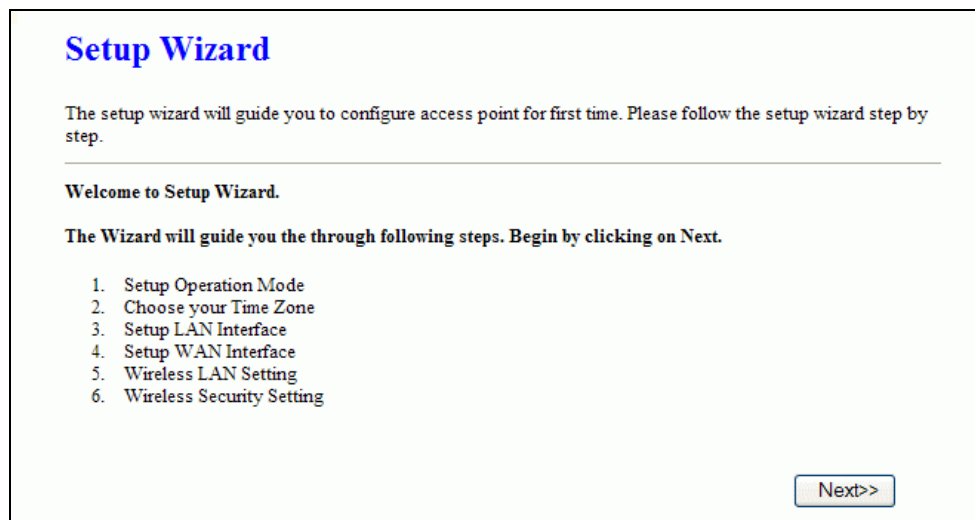
Screen snapshot – Status

| Item                   | Description  |
|------------------------|--|
| System                 |  |
| Uptime                 | It shows the duration since WLAN 11g Router is powered on. |
| Firmware version       | It shows the firmware version of WLAN 11g Router.          |
| Wireless configuration |  |

|                    |  |
|--------------------|--|
| Mode               | It shows wireless operation mode   |
| Band               | It shows the current wireless operating frequency.   |
| SSID               | It shows the SSID of this WLAN 11g Router.<br>The SSID is the unique name of WLAN 11g Router and shared among its service area, so all devices attempts to join the same wireless network can identify it. |
| Channel Number     | It shows the wireless channel connected currently.   |
| Encryption         | It shows the status of encryption function.  |
| Associated Clients | It shows the number of connected clients (or stations, PCs).   |
| BSSID              | It shows the BSSID address of the WLAN 11g Router.<br>BSSID is a six-byte address.   |
| LAN configuration  |  |
| IP Address         | It shows the IP address of LAN interfaces of WLAN 11g Router.  |
| Subnet Mask        | It shows the IP subnet mask of LAN interfaces of WLAN 11g Router.  |
| Default Gateway    | It shows the default gateway setting for LAN interfaces outgoing data packets.   |
| DHCP Server        | It shows the DHCP server is enabled or not.  |
| MAC Address        | It shows the MAC address of LAN interfaces of WLAN 11g Router.   |
| WAN configuration  |  |
| Attain IP Protocol | It shows how the WLAN 11g Router gets the IP address.<br>The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.                      |
| IP Address         | It shows the IP address of WAN interface of WLAN 11g Router.   |
| Subnet Mask        | It shows the IP subnet mask of WAN interface of WLAN 11g Router.   |
| Default Gateway    | It shows the default gateway setting for WAN interface outgoing data packets.  |
| MAC Address        | It shows the MAC address of WAN interface of WLAN 11g Router.  |

### 3.3.2 Setup Wizard

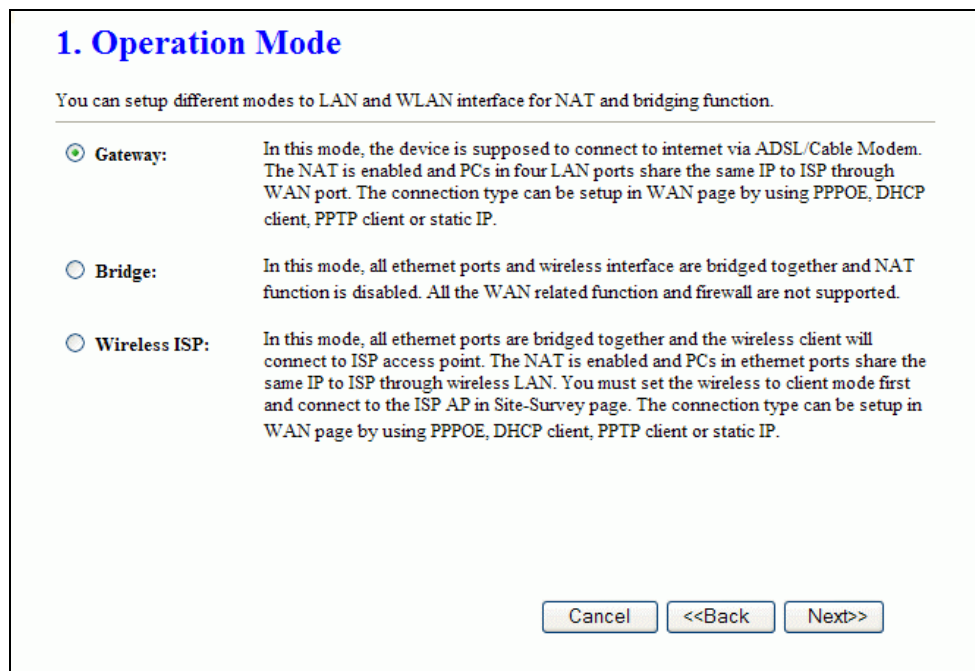
This page guides you to configure wireless broadband router for first time



Screen snapshot – Setup Wizard

### I Operation Mode

This page followed by Setup Wizard page to define the operation mode.



Screen snapshot – Operation Mode

## II Time Zone Setting

This page is used to enable and configure NTP client

### 2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

---

**Enable NTP client update**

**Time Zone Select :** (GMT+08:00)Taipei

**NTP server :** 192.5.41.41 - North America

Cancel <<Back Next>>

Screen snapshot – Time Zone Settings

## III LAN Interface Setup

This page is used to configure local area network IP address and subnet mask

### 3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

---

**IP Address:** 192.168.1.254

**Subnet Mask:** 255.255.255.0

Cancel <<Back Next>>

Screen snapshot – LAN Interface Setup



#### IV WAN Interface Setup

This page is used to configure WAN access type

### 4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

WAN Access Type: DHCP Client ▾

Cancel
<<Back
Next>>

Screen snapshot – WAN Interface Setup

#### V Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone(Single Ethernet Client)

### 5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

---

Band: 2.4 GHz (G) ▾

Mode: AP ▾

Network Type: Infrastructure ▾

SSID: MyWLAN

Channel Number: 11 ▾

Enable Mac Clone (Single Ethernet Client)

Cancel
<<Back
Next>>

Screen snapshot – Wireless Basic Settings

## VI Wireless Security Setup

This page is used to configure wireless security

Screen snapshot – Wireless Security Setup

### 3.3.3 Operation Mode

This page is used to configure which mode wireless broadband router acts

Screen snapshot – Operation Mode

| Item    | Description   |
|---------|---|
| Gateway | Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN |

|               |   |
|---------------|---|
|               | interface, Wireless interface, NAT and Firewall modules are applied to this mode  |
| Bridge        | Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router's functions are not supported          |
| Wireless ISP  | Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all router's functions |
| Apply Changes | Click the <b>Apply Changes</b> button to complete the new configuration setting.  |
| Reset         | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.                                 |

### 3.3.4 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Broadband Router. Here you may change wireless encryption settings as well as wireless network parameters.

#### Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

---

**Disable Wireless LAN Interface**

Band: 2.4 GHz (G) ▼

Mode: AP ▼ Site Survey

Network Type: Infrastructure ▼

SSID: MyWLAN

Channel Number: 11 ▼

Associated Clients: Show Active Clients

**Enable Mac Clone (Single Ethernet Client)**

Apply Changes
Reset

Screen snapshot – Wireless Basic Settings

| Item                           | Description   |
|--------------------------------|---|
| Disable Wireless LAN Interface | Click on to disable the wireless LAN data transmission. |
| Band                           | Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G)     |

---

|   |   |
|---|---|
| Mode                                      | Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode.  |
| Site Survey                               | The <b>Site Survey</b> button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. Refer to <a href="#">3.3.9 Site Survey</a> . |
| SSID                                      | It is the wireless network name. The SSID can be 32 bytes long.   |
| Channel Number                            | Select the wireless communication channel from pull-down menu.  |
| Associated Clients                        | Click the <b>Show Active Clients</b> button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for each associated wireless client.                           |
| Enable Mac Clone (Single Ethernet Client) | Take Laptop NIC MAC address as wireless client MAC address. <b>[Client Mode only]</b>   |
| Apply Changes                             | Click the <b>Apply Changes</b> button to complete the new configuration setting.  |
| Reset                                     | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.   |

---

### 3.3.5 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your WLAN 11g Router.

### Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

---

**Authentication Type:**       Open System    Shared Key    Auto

**Fragment Threshold:**       (256-2346)

**RTS Threshold:**             (0-2347)

**Beacon Interval:**           (20-1024 ms)

**Data Rate:**                   

**Preamble Type:**             Long Preamble    Short Preamble

**Broadcast SSID:**             Enabled    Disabled

**IAPP:**                             Enabled    Disabled

**802.11g Protection:**        Enabled    Disabled

Screen snapshot – Wireless Advanced Settings

| Item                | Description   |
|---------------------|---|
| Authentication Type | Click to select the authentication type in <i>Open System</i> , <i>Shared Key</i> or <i>Auto</i> selection.   |
| Fragment Threshold  | Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes.<br>Refer to <a href="#">4.10 What is Fragment Threshold?</a>                  |
| RTS Threshold       | Set the RTS Threshold, value can be written between 0 and 2347 bytes.<br>Refer to <a href="#">4.11 What is RTS(Request To Send) Threshold?</a>                              |
| Beacon Interval     | Set the Beacon Interval, value can be written between 20 and 1024 ms.<br>Refer to <a href="#">4.12 What is Beacon Interval?</a>   |
| Data Rate           | Select the transmission data rate from pull-down menu.<br>Data rate can be auto-select, 11M, 5.5M, 2M or 1Mbps.   |
| Preamble Type       | Click to select the <i>Long Preamble</i> or <i>Short Preamble</i> support on the wireless data packet transmission.<br>Refer to <a href="#">4.13 What is Preamble Type?</a> |
| Broadcast SSID      | Click to enable or disable the SSID broadcast function.<br>Refer to <a href="#">4.14 What is SSID Broadcast?</a>  |
| IAPP                | Click to enable or disable the IAPP function.<br>Refer to <a href="#">4.20 What is Inter-Access Point Protocol(IAPP)?</a>   |

|                    |   |
|--------------------|---|
| 802.11g Protection | Protect 802.11b user.   |
| Apply Changes      | Click the <b>Apply Changes</b> button to complete the new configuration setting.              |
| Reset              | Click the <b>Reset</b> button to abort change and recover the previous configuration setting. |

### 3.3.6 Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

#### Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

---

Encryption: None Set WEP Key

Use 802.1x Authentication       WEP 64bits    WEP 128bits

WPA Authentication Mode:       Enterprise (RADIUS)    Personal (Pre-Shared Key)

Pre-Shared Key Format:      Passphrase

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server:    Port 1812    IP address     Password

*Note: When encryption WEP is selected, you must set WEP key value.*

Apply Changes
Reset

Screen snapshot – Wireless Security Setup

| Item       | Description  |
|------------|--|
| Encryption | Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed<br>Refer to <a href="#">4.9 What is WEP?</a><br><a href="#">4.15 What is Wi-Fi Protected Access (WPA)?</a><br><a href="#">4.16 What is WPA2(AES)?</a><br><a href="#">4.17 What is 802.1X Authentication?</a><br><a href="#">4.18 What is Temporal Key Integrity Protocol (TKIP)?</a><br><a href="#">4.19 What is Advanced Encryption Standard (AES)?</a> |

|                              |   |
|------------------------------|---|
| Use 802.1x Authentication    | <p>While Encryption is selected to be WEP.</p> <p>Click the check box to enable IEEE 802.1x authentication function.</p> <p>Refer to <a href="#">4.16 What is 802.1x Authentication?</a></p>  |
| WPA Authentication Mode      | <p>While Encryption is selected to be WPA.</p> <p>Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).</p> <p>Refer to <a href="#">4.15 What is Wi-Fi Protected Access (WPA)?</a></p> |
| Pre-Shared Key Format        | <p>While Encryption is selected to be WPA.</p> <p>Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). <b>[WPA, Personal(Pre-Shared Key) only]</b></p>                    |
| Pre-Shared Key               | <p>Fill in the key value. <b>[WPA, Personal(Pre-Shared Key) only]</b></p>   |
| Enable Pre-Authentication    | <p>Click to enable Pre-Authentication. <b>[WPA2/WPA2 Mixed only, Enterprise only]</b></p>   |
| Authentication RADIUS Server | <p>Set the IP address, port and login password information of authentication RADIUS sever.</p>  |
| Apply Changes                | <p>Click the <b><i>Apply Changes</i></b> button to complete the new configuration setting.</p>  |
| Reset                        | <p>Click the <b><i>Reset</i></b> button to abort change and recover the previous configuration setting.</p>   |

## I WEP Key Setup

### Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

---

**Key Length:** 64-bit ▾

**Key Format:** Hex (10 characters) ▾

**Default Tx Key:** Key 1 ▾

**Encryption Key 1:**

**Encryption Key 2:**

**Encryption Key 3:**

**Encryption Key 4:**

Apply Changes
Close
Reset

Screen snapshot – WEP Key Setup

| Item             | Description   |
|------------------|---|
| Key Length       | Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys.<br>The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit). |
| Key Format       | Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.   |
| Default Tx Key   | Set the default secret key for WEP security function.<br>Value can be chose between 1 and 4.  |
| Encryption Key 1 | Secret key 1 of WEP security encryption function.   |
| Encryption Key 2 | Secret key 2 of WEP security encryption function.   |
| Encryption Key 3 | Secret key 3 of WEP security encryption function.   |
| Encryption Key 4 | Secret key 4 of WEP security encryption function.   |
| Apply Changes    | Click the <i>Apply Changes</i> button to complete the new configuration setting.  |
| Close            | Click to close this WEP Key setup window.   |
| Reset            | Click the <i>Reset</i> button to abort change and recover the   |



previous configuration setting.

WEP encryption key (secret key) length:

|        |        |                      |                      |
|--------|--------|----------------------|----------------------|
|        | Length | 64-bit               | 128-bit              |
| Format | ASCII  | 5 characters         | 13 characters        |
|        | HEX    | 10 hexadecimal codes | 26 hexadecimal codes |

### 3.3.7 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

**Wireless Access Control**

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

---

Wireless Access Control Mode:  ▾

MAC Address:  Comment:

Current Access Control List:

| MAC Address       | Comment | Select                   |
|-------------------|---------|--------------------------|
| 00:02:72:81:86:01 | ST-1    | <input type="checkbox"/> |
| 00:00:55:66:66:50 | ST-2    | <input type="checkbox"/> |

Screen snapshot – Wireless Access Control

| Item                         | Description  |
|------------------------------|--|
| Wireless Access Control Mode | Click the <i>Disabled</i> , <i>Allow Listed</i> or <i>Deny Listed</i> of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN 11g Router. |
| MAC Address                  | Fill in the MAC address of client to register this WLAN  |

|                             |   |
|-----------------------------|---|
|                             | 11g Router access capability.   |
| Comment                     | Fill in the comment tag for the registered client.  |
| Apply Changes               | Click the <b>Apply Changes</b> button to register the client to new configuration setting.        |
| Reset                       | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.     |
| Current Access Control List | It shows the registered clients that are allowed to link to this WLAN 11g Router.                 |
| Delete Selected             | Click to delete the selected clients that will be access right removed from this WLAN 11g Router. |
| Delete All                  | Click to delete all the registered clients from the access allowed list.                          |
| Reset                       | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.     |

### 3.3.8 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.

#### WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

---

**Enable WDS**

Add WDS AP:    MAC Address     Comment

**Current WDS AP List:**

| MAC Address       | Comment | Select                   |
|-------------------|---------|--------------------------|
| 00:02:72:81:86:0a | AP-1    | <input type="checkbox"/> |
| 00:02:72:81:86:0b | AP-2    | <input type="checkbox"/> |

Screen snapshot – WDS Setup

| Item            | Description   |
|-----------------|---|
| Enable WDS      | Click the check box to enable wireless distribution system. Refer to <a href="#">4.21 What is Wireless Distribution System (WDS)?</a> |
| MAC Address     | Fill in the MAC address of AP to register the wireless distribution system access capability.   |
| Comment         | Fill in the comment tag for the registered AP.  |
| Apply Changes   | Click the <b>Apply Changes</b> button to register the AP to new configuration setting.  |
| Reset           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.   |
| Set Security    | Click button to configure wireless security like <b>WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES)</b> or <b>None</b>                |
| Show Statistics | It shows the TX, RX packets, rate statistics  |
| Delete Selected | Click to delete the selected clients that will be removed from the wireless distribution system.                                      |
| Delete All      | Click to delete all the registered APs from the wireless distribution system allowed list.  |
| Reset           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.   |

### I WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs. Refer to [3.3.6 Wireless Security Setup](#).

### WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

---

Encryption:

WEP Key Format:

WEP Key:

Pre-Shared Key Format:

Pre-Shared Key:

Screen snapshot – WDS Security Setup

## II WDS AP Table

This page is used to show WDS statistics

### WDS AP Table

This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.

---

| MAC Address       | Tx Packets | Tx Errors | Rx Packets | Tx Rate (Mbps) |
|-------------------|------------|-----------|------------|----------------|
| 00:02:72:81:86:0a | 22         | 0         | 0          | 1              |
| 00:02:72:81:86:0b | 22         | 14        | 0          | 1              |

Screen snapshot – WDS AP Table

| Item        | Description   |
|-------------|---|
| MAC Address | It shows the MAC Address within WDS.  |
| Tx Packets  | It shows the statistic count of sent packets on the wireless LAN interface.       |
| Tx Errors   | It shows the statistic count of error sent packets on the Wireless LAN interface. |
| Rx Packets  | It shows the statistic count of received packets on the wireless LAN interface.   |

|                |  |
|----------------|--|
| Tx Rare (Mbps) | It shows the wireless link rate within WDS.            |
| Refresh        | Click to refresh the statistic counters on the screen. |
| Close          | Click to close the current window.                     |

### 3.3.9 Site Survey

This page is used to view or configure other APs near yours.

#### Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

| SSID           | BSSID             | Channel  | Type   | Encrypt | Signal | Select                |
|----------------|-------------------|----------|--------|---------|--------|-----------------------|
| MyWLAN         | 00:02:72:00:81:86 | 11 (B+G) | AP     | no      | 90     | <input type="radio"/> |
| linux-wlan     | 00:02:72:f1:02:ad | 6 (B)    | AP     | no      | 76     | <input type="radio"/> |
| RTL8186-VPN-GW | 00:e0:4c:81:86:23 | 11 (B+G) | AP     | no      | 66     | <input type="radio"/> |
| Sales          | 00:02:72:04:68:92 | 11 (B)   | AP     | yes     | 53     | <input type="radio"/> |
| Tekom_Office   | 00:02:72:00:93:fb | 9 (B)    | AP     | yes     | 35     | <input type="radio"/> |
| alex           | d6:4c:fc:0d:2a:d4 | 1 (B)    | Ad hoc | no      | 32     | <input type="radio"/> |
| MyWLAN         | 00:02:72:85:15:99 | 11 (B+G) | AP     | no      | 32     | <input type="radio"/> |

Screen snapshot – Wireless Site Survey

| Item    | Description   |
|---------|---|
| SSID    | It shows the SSID of AP.  |
| BSSID   | It shows BSSID of AP.   |
| Channel | It show the current channel of AP occupied.                           |
| Type    | It show which type AP acts.   |
| Encrypt | It shows the encryption status.                                       |
| Signal  | It shows the power level of current AP.                               |
| Select  | Click to select AP or client you'd like to connect.                   |
| Refresh | Click the <b>Refresh</b> button to re-scan site survey on the screen. |
| Connect | Click the <b>Connect</b> button to establish connection.              |

### 3.3.10 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN 11g Router. Here you may change

the setting for IP address, subnet mask, DHCP, etc.

### LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

---

IP Address:

Subnet Mask:

Default Gateway:

DHCP:  ▾

DHCP Client Range:  -

802.1d Spanning Tree:  ▾

Clone MAC Address:

Screen snapshot – LAN Interface Setup

| Item                 | Description  |
|----------------------|--|
| IP Address           | Fill in the IP address of LAN interfaces of this WLAN 11g Router.  |
| Subnet Mask          | Fill in the subnet mask of LAN interfaces of this WLAN 11g Router.   |
| Default Gateway      | Fill in the default gateway for LAN interfaces out going data packets.   |
| DHCP Server          | Click to select <b>Disabled</b> , <b>Client</b> or <b>Server</b> in different operation mode of wireless broadband router.   |
| DHCP Client Range    | Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.                          |
| Show Client          | Click to open the <b>Active DHCP Client Table</b> window that shows the active clients with their assigned IP address, MAC address and time expired information. <b>[Server mode only]</b> |
| 802.1d Spanning Tree | Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.  |
| Clone MAC Address    | Fill in the MAC address that is the MAC address to be cloned. Refer to <a href="#">4.24 What is Clone MAC Address?</a>   |

|               |   |
|---------------|---|
| Apply Changes | Click the <i>Apply Changes</i> button to complete the new configuration setting.              |
| Reset         | Click the <i>Reset</i> button to abort change and recover the previous configuration setting. |

### 3.3.11 WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your WLAN 11g Router. Here you may change the access method to *Static IP*, *DHCP*, *PPPoE* or *PPTP* by click the item value of **WAN Access Type**.

#### I Static IP

Screen snapshot – WAN Interface Setup – Static IP

| Item        | Description   |
|-------------|---|
| Static IP   | Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done. |
| IP Address  | If you select the Static IP support on WAN interface, fill in the IP address for it.  |
| Subnet Mask | If you select the Static IP support on WAN interface, fill  |

|                                 |   |
|---------------------------------|---|
|                                 | in the subnet mask for it.  |
| Default Gateway                 | If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets. |
| DNS 1                           | Fill in the IP address of Domain Name Server 1.   |
| DNS 2                           | Fill in the IP address of Domain Name Server 2.   |
| DNS 3                           | Fill in the IP address of Domain Name Server 3.   |
| Clone MAC Address               | Fill in the MAC address that is the MAC address to be cloned. Refer to <a href="#">4.24 What is Clone MAC Address?</a>      |
| Enable uPNP                     | Click the checkbox to enable uPNP function.<br>Refer to <a href="#">4.22 What is Universal Plug and Play (uPNP)?</a>        |
| Enable Web Server Access on WAN | Click the checkbox to enable web configuration from WAN side.   |
| Enable WAN Echo Reply           | Click the checkbox to enable WAN ICMP response.   |
| Apply Changes                   | Click the <b>Apply Changes</b> button to complete the new configuration setting.  |
| Reset                           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.                               |

## II DHCP Client

### WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

WAN Access Type: DHCP Client ▼

Attain DNS Automatically  
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP  
 Enable Web Server Access on WAN  
 Enable WAN Echo Reply

Apply Changes
Reset

Screen snapshot – WAN Interface Setup – DHCP Client



| Item                            | Description  |
|---------------------------------|--|
| DHCP Client                     | Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.                                    |
| Attain DNS Automatically        | Click to select getting DNS address for <b>DHCP</b> support. Please select <b>Set DNS Manually</b> if the <b>DHCP</b> support is selected. |
| Set DNS Manually                | Click to select getting DNS address for <b>DHCP</b> support.   |
| DNS 1                           | Fill in the IP address of Domain Name Server 1.  |
| DNS 2                           | Fill in the IP address of Domain Name Server 2.  |
| DNS 3                           | Fill in the IP address of Domain Name Server 3.  |
| Clone MAC Address               | Fill in the MAC address that is the MAC address to be cloned. Refer to <a href="#">4.24 What is Clone MAC Address?</a>                     |
| Enable uPNP                     | Click the checkbox to enable uPNP function. Refer to <a href="#">4.22 What is Universal Plug and Play (uPNP)?</a>                          |
| Enable Web Server Access on WAN | Click the checkbox to enable web configuration from WAN side.  |
| Enable WAN Echo Reply           | Click the checkbox to enable WAN ICMP response.  |
| Apply Changes                   | Click the <b>Apply Changes</b> button to complete the new configuration setting.   |
| Reset                           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.  |

### III PPPoE

#### WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

**WAN Access Type:** PPPoE

**User Name:**

**Password:**

**Connection Type:** Continuous

**Idle Time:**  (1-1000 minutes)

**MTU Size:**  (1400-1492 bytes)

**Attain DNS Automatically**  
 **Set DNS Manually**

**DNS 1:**

**DNS 2:**

**DNS 3:**

**Clone MAC Address:**

**Enable uPNP**  
 **Enable Web Server Access on WAN**  
 **Enable WAN Echo Reply**

Screen snapshot – WAN Interface Setup – PPPoE

| Item            | Description   |
|-----------------|---|
| PPPoE           | Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.  |
| User Name       | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.   |
| Password        | If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.   |
| Connection Type | Select the connection type from pull-down menu. There are <b>Continuous</b> , <b>Connect on Demand</b> and <b>Manual</b> three types to select.<br><br><b>Continuous</b> connection type means to setup the connection through PPPoE protocol whenever this WLAN 11g Router is powered on.<br><br><b>Connect on Demand</b> connection type means to setup the |

connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set.

**Manual** connection type means to setup the connection through the PPPoE protocol by clicking the **Connect** button manually, and clicking the **Disconnect** button manually.

|                                 |   |
|---------------------------------|---|
| Idle Time                       | If you select the <b>PPPoE</b> and <b>Connect on Demand</b> connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes. |
| MTU Size                        | Fill in the mtu size of MTU Size. The default value is 1400. Refer to <a href="#">4.23 What is Maximum Transmission Unit (MTU) Size?</a>                                  |
| Attain DNS Automatically        | Click to select getting DNS address for <b>PPPoE</b> support. Please select <b>Set DNS Manually</b> if the <b>PPPoE</b> support is selected.                              |
| Set DNS Manually                | Click to select getting DNS address for <b>Static IP</b> support.   |
| DNS 1                           | Fill in the IP address of Domain Name Server 1.   |
| DNS 2                           | Fill in the IP address of Domain Name Server 2.   |
| DNS 3                           | Fill in the IP address of Domain Name Server 3.   |
| Clone MAC Address               | Fill in the MAC address that is the MAC address to be cloned. Refer to <a href="#">4.24 What is Clone MAC Address?</a>  |
| Enable uPNP                     | Click the checkbox to enable uPNP function.<br>Refer to <a href="#">4.22 What is Universal Plug and Play (uPNP)?</a>  |
| Enable Web Server Access on WAN | Click the checkbox to enable web configuration from WAN side.   |
| Enable WAN Echo Reply           | Click the checkbox to enable WAN ICMP response.   |
| Apply Changes                   | Click the <b>Apply Changes</b> button to complete the new configuration setting.  |
| Reset                           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.   |

## IV PPTP

### WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

---

WAN Access Type: PPTP ▼

IP Address:

Subnet Mask:

Server IP Address:

User Name:

Password:

MTU Size:  (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable uPNP

Enable Web Server Access on WAN

Enable WAN Echo Reply

Screen snapshot – WAN Interface Setup – PPTP

| Item              | Description  |
|-------------------|--|
| PPTP              | Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection. |
| IP Address        | If you select the PPTP support on WAN interface, fill in the IP address for it.  |
| Subnet Mask       | If you select the PPTP support on WAN interface, fill in the subnet mask for it.   |
| Server IP Address | Enter the IP address of the PPTP Server.   |
| User Name         | If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.  |

|                                 |  |
|---------------------------------|--|
| Password                        | If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.                              |
| MTU Size                        | Fill in the mtu size of MTU Size. The default value is 1400. Refer to <a href="#">4.23 What is Maximum Transmission Unit (MTU) Size?</a>   |
| Attain DNS Automatically        | Click to select getting DNS address for <b>PPTP</b> support. Please select <b>Set DNS Manually</b> if the <b>PPTP</b> support is selected. |
| Set DNS Manually                | Click to select getting DNS address for <b>PPTP</b> support.   |
| DNS 1                           | Fill in the IP address of Domain Name Server 1.  |
| DNS 2                           | Fill in the IP address of Domain Name Server 2.  |
| DNS 3                           | Fill in the IP address of Domain Name Server 3.  |
| Clone MAC Address               | Fill in the MAC address that is the MAC address to be cloned. Refer to <a href="#">4.24 What is Clone MAC Address?</a>                     |
| Enable uPNP                     | Click the checkbox to enable uPNP function. Refer to <a href="#">4.22 What is Universal Plug and Play (uPNP)?</a>                          |
| Enable Web Server Access on WAN | Click the checkbox to enable web configuration from WAN side.  |
| Enable WAN Echo Reply           | Click the checkbox to enable WAN ICMP response.  |
| Apply Changes                   | Click the <b>Apply Changes</b> button to complete the new configuration setting.   |
| Reset                           | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.  |

### 3.3.12 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

**Enable Port Filtering**  
 Port Range:  -  Protocol: Both Comment:

**Current Filter Table:**

| Port Range | Protocol | Comment | Select                   |
|------------|----------|---------|--------------------------|
| 20-21      | TCP-UDP  | FTP     | <input type="checkbox"/> |

Screen snapshot – Firewall - Port Filtering

| Item                  | Description  |
|-----------------------|--|
| Enable Port Filtering | Click to enable the port filtering security function.  |
| Port Range            | To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. |
| Protocol              | The <i>Protocol</i> can be TCP, UDP or Both.   |
| Comments              | <i>Comments</i> let you know about whys to restrict data from the ports.   |
| Apply Changes         | Click the <i>Apply Changes</i> button to register the ports to port filtering list.  |
| Reset                 | Click the <i>Reset</i> button to abort change and recover the previous configuration setting.  |
| Delete Selected       | Click to delete the selected port range that will be removed from the port-filtering list.   |
| Delete All            | Click to delete all the registered entries from the port-filtering list.   |
| Reset                 | Click the <i>Reset</i> button to abort change and recover the previous configuration setting.  |

### 3.3.13 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**IP Filtering**

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Enable IP Filtering**

Local IP Address:  Protocol:  Comment:

**Current Filter Table:**

| Local IP Address | Protocol | Comment | Select                   |
|------------------|----------|---------|--------------------------|
| 192.168.1.201    | TCP-UDP  | ST-1    | <input type="checkbox"/> |
| 192.168.1.202    | TCP      | ST-2    | <input type="checkbox"/> |

Screen snapshot – Firewall - IP Filtering

| Item                | Description   |
|---------------------|---|
| Enable IP Filtering | Click to enable the IP filtering security function.   |
| Local IP Address    | To restrict data transmission from local network on certain IP addresses, fill in the IP address and the                      |
| Protocol            | protocol, also put your comments on it.   |
| Comments            | The <b>Protocol</b> can be TCP, UDP or Both.<br><b>Comments</b> let you know about whys to restrict data from the IP address. |
| Apply Changes       | Click the <b>Apply Changes</b> button to register the IP address to IP filtering list.  |
| Reset               | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.                                 |
| Delete Selected     | Click to delete the selected IP address that will be removed from the IP-filtering list.                                      |
| Delete All          | Click to delete all the registered entries from the IP-filtering list.  |
| Reset               | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.                                 |

### 3.3.14 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be

helpful in securing or restricting your local network.

### MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

**Enable MAC Filtering**

MAC Address:  Comment:

**Current Filter Table:**

| MAC Address       | Comment | Select                   |
|-------------------|---------|--------------------------|
| 00-02:72:00:81:90 | ST-1    | <input type="checkbox"/> |
| 00-02:72:00:81:91 | ST-2    | <input type="checkbox"/> |

Screen snapshot – Firewall - MAC Filtering

| Item                 | Description   |
|----------------------|---|
| Enable MAC Filtering | Click to enable the MAC filtering security function.  |
| MAC Address          | To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your |
| Comments             | comments on it.<br><br><b>Comments</b> let you know about whys to restrict data from the MAC address.       |
| Apply Changes        | Click the <b>Apply Changes</b> button to register the MAC address to MAC filtering list.                    |
| Reset                | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.               |
| Delete Selected      | Click to delete the selected MAC address that will be removed from the MAC-filtering list.                  |
| Delete All           | Click to delete all the registered entries from the MAC-filtering list.                                     |
| Reset                | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.               |

### 3.3.15 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only



necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

### Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

---

**Enable Port Forwarding**

IP Address:  Protocol: Both Port Range:  -  Comment:

**Current Port Forwarding Table:**

| Local IP Address | Protocol | Port Range | Comment | Select                   |
|------------------|----------|------------|---------|--------------------------|
| 192.168.1.201    | TCP+UDP  | 20-21      | FTP     | <input type="checkbox"/> |

Screen snapshot – Firewall - Port Forwarding

| Item                   | Description  |
|------------------------|--|
| Enable Port Forwarding | Click to enable the Port Forwarding security function.   |
| IP Address             | To forward data packets coming from WAN to a specific  |
| Protocol               | IP address that hosted in local network behind the NAT   |
| Port Range             | firewall, fill in the IP address, protocol, port range and   |
| Comment                | your comments.<br>The <b>Protocol</b> can be TCP, UDP or Both.<br>The <b>Port Range</b> for data transmission.<br><b>Comments</b> let you know about whys to allow data packets forward to the IP address and port number. |
| Apply Changes          | Click the <b>Apply Changes</b> button to register the IP address and port number to Port forwarding list.  |
| Reset                  | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.  |
| Delete Selected        | Click to delete the selected IP address and port number that will be removed from the port-forwarding list.  |
| Delete All             | Click to delete all the registered entries from the port-forwarding list.  |

Reset Click the **Reset** button to abort change and recover the previous configuration setting.

---

### 3.3.16 Firewall - DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



Screen snapshot – Firewall - DMZ

| Item                | Description   |
|---------------------|---|
| Enable DMZ          | Click to enable the DMZ function.   |
| DMZ Host IP Address | To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface. |
| Apply Changes       | Click the <b>Apply Changes</b> button to register the IP address of DMZ host.   |
| Reset               | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.                         |

### 3.3.17 VPN Setting

This page is used to show VPN connection table, configure IPSEC VPN, NAT Traversal, Generate RSA Key, Show RSA Public Key.

### VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

**Enable IPSEC VPN**     
  **Enable NAT Traversal**     

**Current VPN Connection Table: WAN IP:192.168.3.254**

| #  | Name  | Active | Local Address  | Remote Address | Remote Gateway | Status    |
|----|-------|--------|----------------|----------------|----------------|-----------|
| 1  | site5 | Y      | 192.168.1.0/24 | 192.168.4.0/24 | 192.168.3.1    | Connected |
| 2  | -     | -      | -              | -              | -              | -         |
| 3  | -     | -      | -              | -              | -              | -         |
| 4  | -     | -      | -              | -              | -              | -         |
| 5  | -     | -      | -              | -              | -              | -         |
| 6  | -     | -      | -              | -              | -              | -         |
| 7  | -     | -      | -              | -              | -              | -         |
| 8  | -     | -      | -              | -              | -              | -         |
| 9  | -     | -      | -              | -              | -              | -         |
| 10 | -     | -      | -              | -              | -              | -         |

Screen snapshot – VPN Setup

| Item                         | Description  |
|------------------------------|--|
| Enable IPSEC VPN             | Click to enable IPSEC VPN function. Refer to <a href="#">4.27 What is VPN?</a> and <a href="#">4.28 What is IPSEC?</a> |
| Enable NAT Traversal         | Click to enable NAT Traversal function.  |
| Generate RSA Key             | Click to generate RSA key.   |
| Show RSA Public Key          | Click to show RSA public key that we generate.   |
| Apply Changes                | Click the <b>Apply Changes</b> button to enable IPSEC VPN, NAT Traversal settings.                                     |
| Current VPN Connection Table | It shows current WAN interface information and VPN connection table.   |
| Edit                         | Click to enter the current VPN tunnel configuration page.  |
| Delete                       | Click to delete the current VPN tunnel that radio button stay.   |
| Refresh                      | Click to refresh the current VPN connection table.   |

## I VPN Setup - Edit Tunnel

**VPN Setup**

---

**Enable Tunnel 1**

**Connection Name:**

**Auth Type:**

**Local Site:**

Local IP Address/Network:

Local Subnet Mask:

**Remote Site:**

Remote Secure Gateway:

Remote IP Address/Network:

Remote Subnet Mask:

**Local/Peer ID:**

Local ID Type:

Local ID:

Remote ID Type:

Remote ID:

Screen snapshot – VPN Setup-Edit-1

| Item                             | Description   |
|----------------------------------|---|
| Enable Tunnel #                  | Click to enable the IPSEC VPN current tunnel.   |
| Connection Name                  | Assign the connection name tag.   |
| Auth Type                        | Click to select <b>PSK</b> or <b>RSA</b> .  |
| Local Site                       | Click to select <b>Single Address</b> or <b>Subnet Address</b> VPN connection.  |
| <b>Local IP Address/Network</b>  | Fill in IP address or subnet address depends on which Local Site option you choose.   |
| <b>Local Subnet Mask</b>         | Fill in the local subnet mask.  |
| Remote Site                      | Click to select <b>Single Address</b> , <b>Subnet Address</b> , <b>Any Address</b> or <b>NAT-T Any Address</b> VPN remote connection. |
| <b>Remote Secure Gateway</b>     | Fill in remote gateway IP address   |
| <b>Remote IP Address/Network</b> | Fill in IP address or subnet address depends on which Remote Site option you choose.  |
| <b>Remote Subnet Mask</b>        | Fill in remote subnet mask  |
| Local/Peer ID                    | Define IKE exchange information type  |
| <b>Local ID Type</b>             | Click to select <b>IP</b> , <b>DNS</b> or <b>E-mail</b> as local exchange type  |
| <b>Local ID</b>                  | Fill in local ID except IP selected   |
| <b>Remote ID Type</b>            | Click to select <b>IP</b> , <b>DNS</b> or <b>E-mail</b> as remote exchange  |

type

**Remote ID**

Fill in remote ID except IP selected

Screen snapshot – VPN Setup-Edit-2

| Item               | Description   |
|--------------------|---|
| Key Management     | Click to select <i>IKE</i> or <i>Manual</i> mode.   |
| Advanced           | Click <i>Advanced</i> button to configure more IKE settings.  |
| Connection Type    | Click to select <i>Initiator</i> or <i>Responder</i> mode.  |
| Connect            | Click to connect manually. [ <b>Responder mode only</b> ]   |
| Disconnect         | Click to disconnect manually. [ <b>Responder mode only</b> ].   |
| ESP                | Click to configure <i>3DES</i> , <i>AES128</i> or <i>NULL</i> encryption.<br>Click to configure <i>MD5</i> or <i>SHA1</i> authentication. |
| PreShared Key      | Fill in the key value. [ <b>IKE mode only</b> ]   |
| Remote RSA Key     | Fill in the remote gateway RSA key. [ <b>IKE mode only</b> ]  |
| Status             | It shows connection status. [ <b>IKE mode only</b> ]  |
| SPI                | Fill in Security Parameter Index value. [ <b>Manual mode only</b> ]   |
| Encryption Key     | Fill in encryption key. [ <b>Manual mode only</b> ]   |
| Authentication Key | Fill in authentication key. [ <b>Manual mode only</b> ]   |
| Apply Change       | Click the <i>Apply Changes</i> button to save current tunnel settings.  |
| Reset              | Click the <i>Reset</i> button to abort change and recover the previous configuration setting.   |
| Refresh            | It shows the current connection status. [ <b>Manual mode only</b> ]   |
| Back               | It returns back to VPN Setup page.  |

## II Advanced IKE Setup

### Advanced VPN Setting for IKE

This page is used to provide advanced setting for IKE mode

---

**Tunnel 1**

**Phase 1:**

|                          |   |
|--------------------------|---|
| Negotiation Mode         | Main mode   |
| Encryption Algorithm     | 3DES <input type="button" value="v"/>                 |
| Authenticaiton Algorithm | MD5 <input type="button" value="v"/>                  |
| Key Group                | DH2(modp1024) <input type="button" value="v"/>        |
| Key Life Time            | <input style="width: 80%;" type="text" value="3600"/> |

**Phase 2:**

|                               |  |
|-------------------------------|--|
| Active Protocol               | ESP  |
| Encryption Algorithm          | 3DES <input type="button" value="v"/>                  |
| Authenticaiton Algorithm      | MD5 <input type="button" value="v"/>                   |
| Key Life Time                 | <input style="width: 80%;" type="text" value="28800"/> |
| Encapsulation                 | Tunnel mode  |
| Perfect Forward Secrecy (PFS) | ON <input type="button" value="v"/>                    |

Screen snapshot – Advanced VPN Settings for IKE

| Item                     | Description  |
|--------------------------|--|
| Phase 1                  |  |
| Negotiation Mode         | Main mode.   |
| Encryption Algorithm     | Click to select <b>3DES</b> or <b>AES128</b> encryption.   |
| Authentication Algorithm | Click to select <b>MD5</b> or <b>SHA1</b> authentication.  |
| Key Group                | Click to select <b>DH1(modp768)</b> , <b>DH2(modp1024)</b> or <b>DH5(modp1536)</b> key group. Default value is DH2 |
| Key Life Time            | Fill in the key life time value by seconds.  |
| Phase 2                  |  |

|                               |   |
|-------------------------------|---|
| Active Protocol               | ESP.  |
| Encryption Algorithm          | Click to select <i>3DES</i> , <i>AES128</i> or <i>NULL</i> encryption.      |
| Authentication Algorithm      | Click to select <i>MD5</i> or <i>SHA1</i> authentication.                   |
| Key Life Time                 | Fill in the key life time value by seconds.                                 |
| Encapsulation                 | Tunnel mode.  |
| Perfect Forward Secrecy (PFS) | Click to select <i>ON</i> or <i>NONE</i> .                                  |
| Ok                            | Click the <i>Ok</i> button to save current tunnel settings.                 |
| Cancel                        | Click the <i>Cancel</i> button to close current window without any changes. |

### 3.3.18 Management - Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.

**Statistics**

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

|              |                         |       |
|--------------|-------------------------|-------|
| Wireless LAN | <i>Sent Packets</i>     | 1361  |
|              | <i>Received Packets</i> | 25883 |
| Ethernet LAN | <i>Sent Packets</i>     | 1529  |
|              | <i>Received Packets</i> | 1269  |
| Ethernet WAN | <i>Sent Packets</i>     | 597   |
|              | <i>Received Packets</i> | 30386 |

Screen snapshot – Management - Statistics

| Item                                    | Description   |
|---|---|
| Wireless LAN<br><i>Sent Packets</i>     | It shows the statistic count of sent packets on the wireless LAN interface.     |
| Wireless LAN<br><i>Received Packets</i> | It shows the statistic count of received packets on the wireless LAN interface. |
| Ethernet LAN<br><i>Sent Packets</i>     | It shows the statistic count of sent packets on the Ethernet LAN interface.     |
| Ethernet LAN                            | It shows the statistic count of received packets on the                         |

|                         |   |
|-------------------------|---|
| <b>Received Packets</b> | Ethernet LAN interface.                                 |
| Ethernet WAN            | It shows the statistic count of sent packets on the     |
| <b>Sent Packets</b>     | Ethernet WAN interface.                                 |
| Ethernet WAN            | It shows the statistic count of received packets on the |
| <b>Received Packets</b> | Ethernet WAN interface.                                 |
| Refresh                 | Click the refresh the statistic counters on the screen. |

### 3.3.19 Management - DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.

#### Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

---

Enable DDNS

Service Provider : DynDNS ▼

Domain Name : host.dyndns.org

User Name/Email:  

Password/Key:  

Note:  
 For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)  
 For DynDNS, you can create your DynDNS account [here](#)

Apply Change
Reset

Screen snapshot – Management – DDNS

| Item             | Description   |
|------------------|---|
| Enable DDNS      | Click the checkbox to enable <b>DDNS</b> service. Refer to <a href="#">4.25 What is DDNS?</a> |
| Service Provider | Click the drop down menu to pickup the right provider.  |
| Domain Name      | To configure the Domain Name.   |
| User Name/Email  | Configure User Name, Email.   |
| Password/Key     | Configure Password, Key.  |
| Apply Change     | Click the <b>Apply Changes</b> button to save the enable DDNS service.                        |
| Reset            | Click the <b>Reset</b> button to abort change and recover the previous configuration setting. |



### 3.3.20 Management - Time Zone Setting

This page is used to configure NTP client to get current time.

#### Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

---

Current Time : Yr  Mon  Day  Hr  Mn  Sec

Time Zone Select :

Enable NTP client update

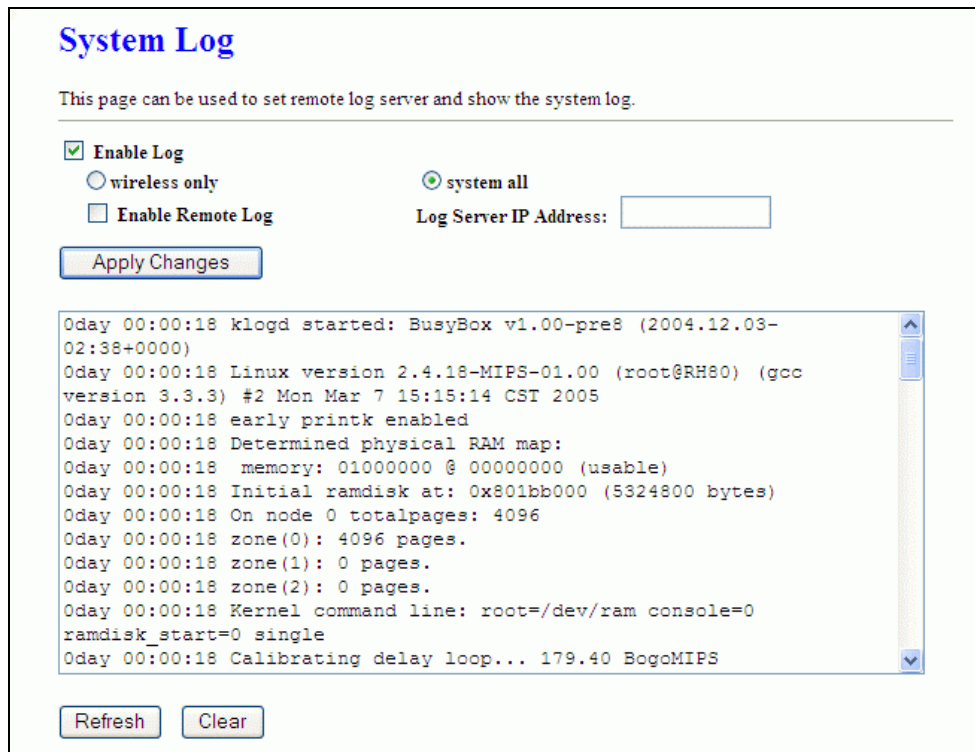
NTP server :     
  (Manual IP Setting)

Screen snapshot – Management – Time Zone Settings

| Item                     | Description   |
|--------------------------|---|
| Current Time             | It shows the current time.  |
| Time Zone Select         | Click the time zone in your country.  |
| Enable NTP client update | Click the checkbox to enable NTP client update. Refer to <a href="#">4.26 What is NTP Client?</a> |
| NTP Server               | Click select default or input NTP server IP address.  |
| Apply Change             | Click the <b>Apply Changes</b> button to save and enable NTP client service.                      |
| Reset                    | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.     |
| Refresh                  | Click the refresh the current time shown on the screen.   |

### 3.3.21 Management - Log

This page is used to configure the remote log server and shown the current log.

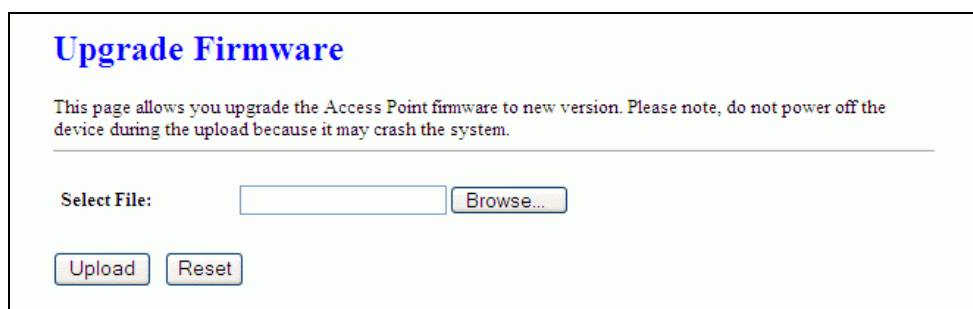


Screen snapshot – Management – Log

| Item                         | Description   |
|------------------------------|---|
| Enable Log                   | Click the checkbox to enable log.                             |
| <i>Wireless only</i>         | Only show wireless log  |
| <i>System all</i>            | Show all log of wireless broadband router                     |
| <i>Enable Remote Log</i>     | Click the checkbox to enable remote log service.              |
| <i>Log Server IP Address</i> | Input the remote log IP address                               |
| Apply Changes                | Click the <i>Apply Changes</i> button to save above settings. |
| Refresh                      | Click the refresh the log shown on the screen.                |
| Clear                        | Clear log display screen                                      |

### 3.3.22 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

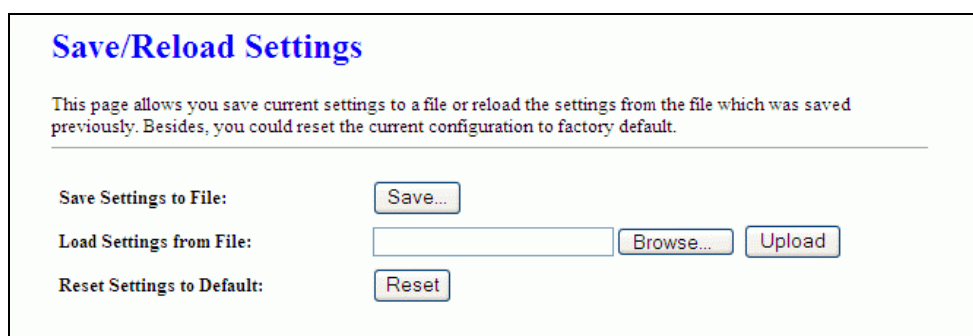


Screen snapshot – Management - Upgrade Firmware

| Item        | Description  |
|-------------|--|
| Select File | Click the <b>Browse</b> button to select the new version of web firmware image file.             |
| Upload      | Click the <b>Upload</b> button to update the selected web firmware image to the WLAN 11g Router. |
| Reset       | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.    |

### 3.3.23 Management Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.



Screen snapshot – Management - Save/Reload Settings

| Item                    | Description   |
|-------------------------|---|
| Save Settings to File   | Click the <b>Save</b> button to download the configuration parameters to your personal computer.                            |
| Load Settings from File | Click the <b>Browse</b> button to select the configuration files then click the <b>Upload</b> button to update the selected |

|                           |   |
|---------------------------|---|
|                           | configuration to the WLAN 11g Router.   |
| Reset Settings to Default | Click the <b>Reset</b> button to reset the configuration parameter to factory defaults. |

### 3.3.24 Management - Password Setup

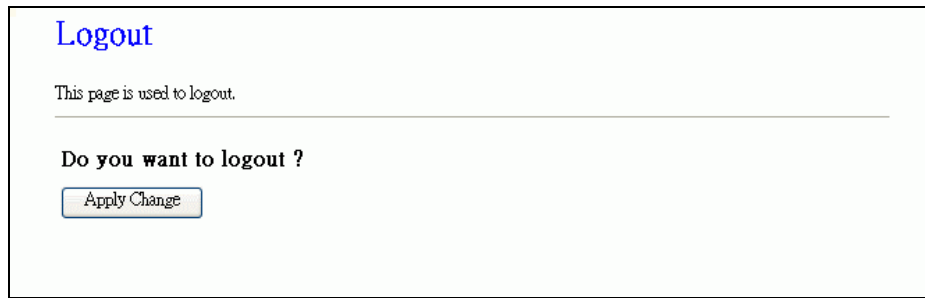
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Screen snapshot – Management - Password Setup

| Item               | Description  |
|--------------------|--|
| User Name          | Fill in the user name for web management login control.  |
| New Password       | Fill in the password for web management login control.   |
| Confirmed Password | Because the password input is invisible, so please fill in the password again for confirmation purpose.  |
| Apply Changes      | Clear the <b>User Name</b> and <b>Password</b> fields to empty, means to apply no web management login control. Click the <b>Apply Changes</b> button to complete the new configuration setting. |
| Reset              | Click the <b>Reset</b> button to abort change and recover the previous configuration setting.  |

### 3.3.25 Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.



Screen snapshot – Logout



Screen snapshot – Logout - OK

| Item         | Description  |
|--------------|--|
| Apply Change | Click the <i>Apply Change</i> button, Then click <b>OK</b> button to logout. |

## 4 Frequently Asked Questions (FAQ)

### 4.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
- ✓ Type in *ipconfig /all* then press the *Enter* button.
  
- Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

### 4.2 What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

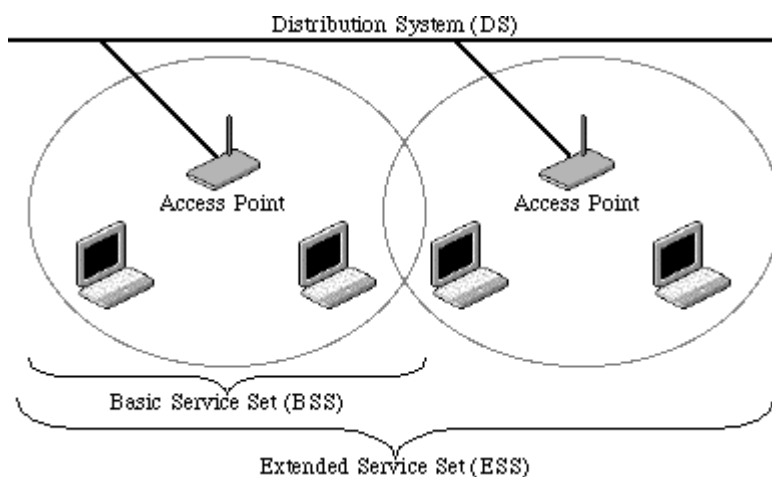
### 4.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

### 4.4 How does wireless networking work?

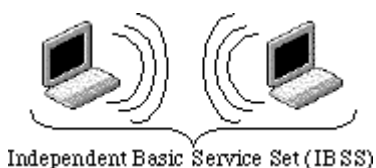
The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access

to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

#### 4.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

#### 4.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

#### 4.7 What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture... etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, ... etc.
- ✓ Add additional WLAN Access Points if necessary.

#### 4.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

#### 4.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

#### 4.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several



fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

#### 4.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

#### 4.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling

stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

#### 4.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

#### 4.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

#### 4.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an

authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

#### 4.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

#### 4.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

#### 4.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

#### 4.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

#### 4.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

#### 4.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

#### 4.22 What is Universal Plug and Play (uPnP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

#### 4.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default is value 1400.

#### 4.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.

Since that all the clients will communicate outside world through the WLAN 11g Router, so have the cloned MAC address set on the WLAN 11g Router will solve the issue.

#### 4.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

#### 4.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

#### 4.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to-point private link via shared or public network.

#### 4.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

## 5 Configuration Examples

### 5.1 Example One – PPPoE on the WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the WLAN 11g Router implementation by the following configuration.

*WAN configuration:*

*PPPoE*

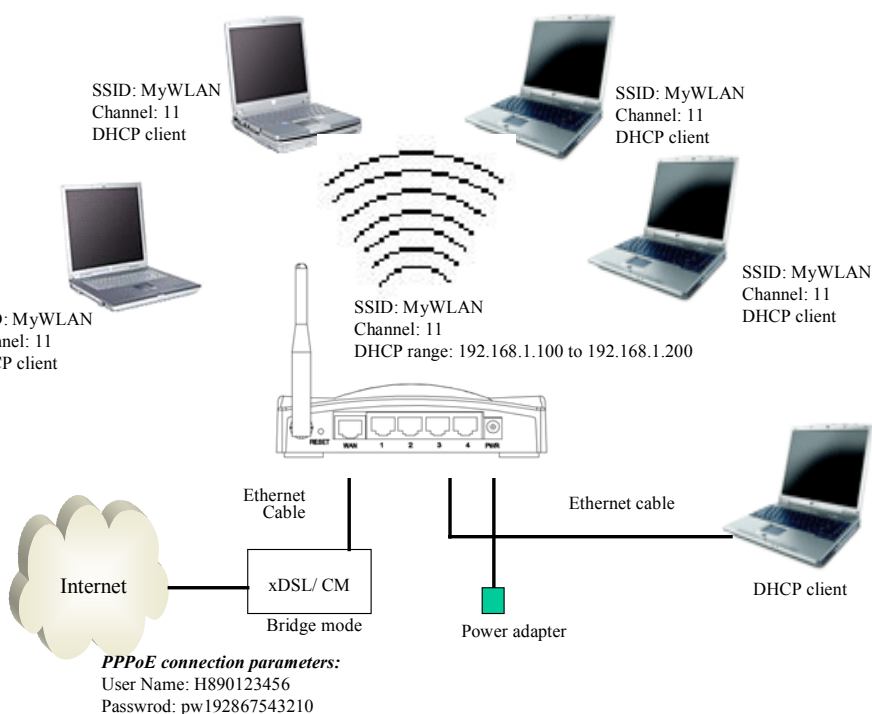
|                  |                       |
|------------------|-----------------------|
| <i>User Name</i> | <b>H890123456</b>     |
| <i>Password</i>  | <b>PW192867543210</b> |

*LAN configuration*

|                          |                                      |
|--------------------------|--------------------------------------|
| <i>IP Address</i>        | <b>192.168.1.254</b>                 |
| <i>Subnet Mask</i>       | <b>255.255.255.0</b>                 |
| <i>Default Gateway</i>   | <b>0.0.0.0</b>                       |
| <i>DHCP Client Range</i> | <b>192.168.1.100 – 192.168.1.200</b> |

*WLAN configuration*

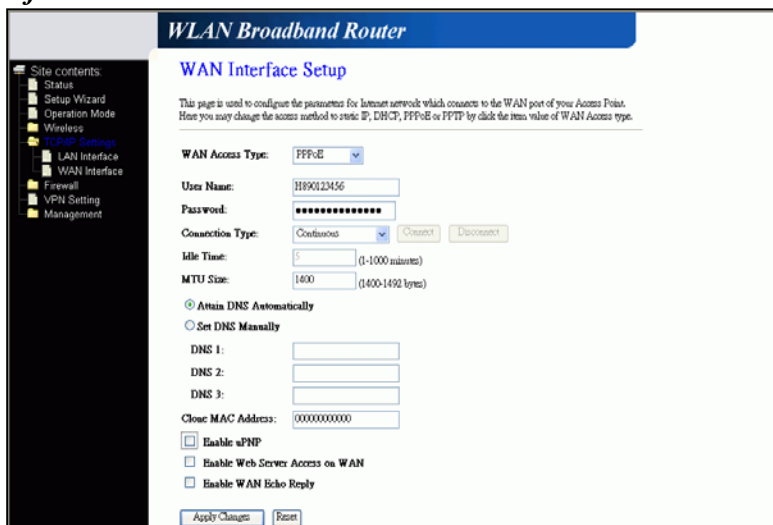
|                       |               |
|-----------------------|---------------|
| <i>SSID</i>           | <b>MyWLAN</b> |
| <i>Channel Number</i> | <b>11</b>     |

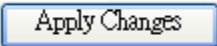


**Figure 3 – Configuration Example One – PPPoE on the WAN**

**Configure the WAN interface:**

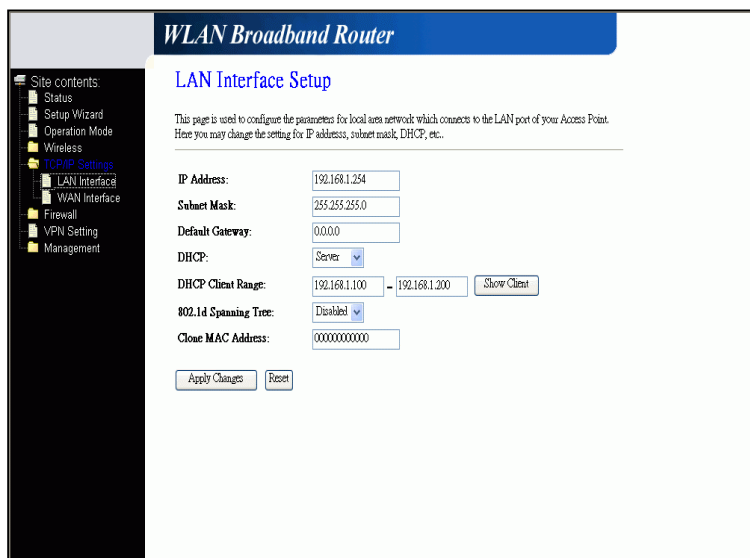
Open WAN Interface Setup page, select PPPoE then enter the User Name “H890123456” and Password “PW192867543210”, the password is encrypted to display on the screen.

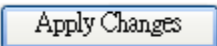


Press  button to confirm the configuration setting.

**Configure the LAN interface:**

Open LAN Interface Setup page, enter the IP Address “192.168.1.254”, Subnet Mask “255.255.255.0”, Default Gateway “0.0.0.0”, enable DHCP Server, DHCP client range “192.168.1.100” to “192.168.1.200”.

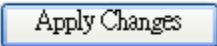


Press  button to confirm the configuration setting.

**Configure the WLAN interface:**

Open WLAN Interface Setup page, enter the SSID “MyWLAN”, Channel Number “11”.



Press  button to confirm the configuration setting.

**5.2 Example Two – Fixed IP on the WAN**

Company ABC likes to establish a WLAN network to support mobile communication on all employees’ Notebook PCs. MIS engineer collects information and plans the WLAN 11g Router implementation by the following configuration.

*WAN configuration:*

*Fixed IP*

|                        |                      |
|------------------------|----------------------|
| <i>IP Address</i>      | <b>192.168.2.254</b> |
| <i>Subnet Mask</i>     | <b>255.255.255.0</b> |
| <i>Default Gateway</i> | <b>192.168.2.10</b>  |
| <i>DNS Address</i>     | <b>168.95.1.1</b>    |

*LAN configuration*

|                          |                                      |
|--------------------------|--------------------------------------|
| <i>IP Address</i>        | <b>192.168.1.254</b>                 |
| <i>Subnet Mask</i>       | <b>255.255.255.0</b>                 |
| <i>Default Gateway</i>   | <b>192.168.2.254</b>                 |
| <i>DHCP Client Range</i> | <b>192.168.1.100 – 192.168.1.200</b> |

*WLAN configuration*

|                       |               |
|-----------------------|---------------|
| <i>SSID</i>           | <b>MyWLAN</b> |
| <i>Channel Number</i> | <b>11</b>     |



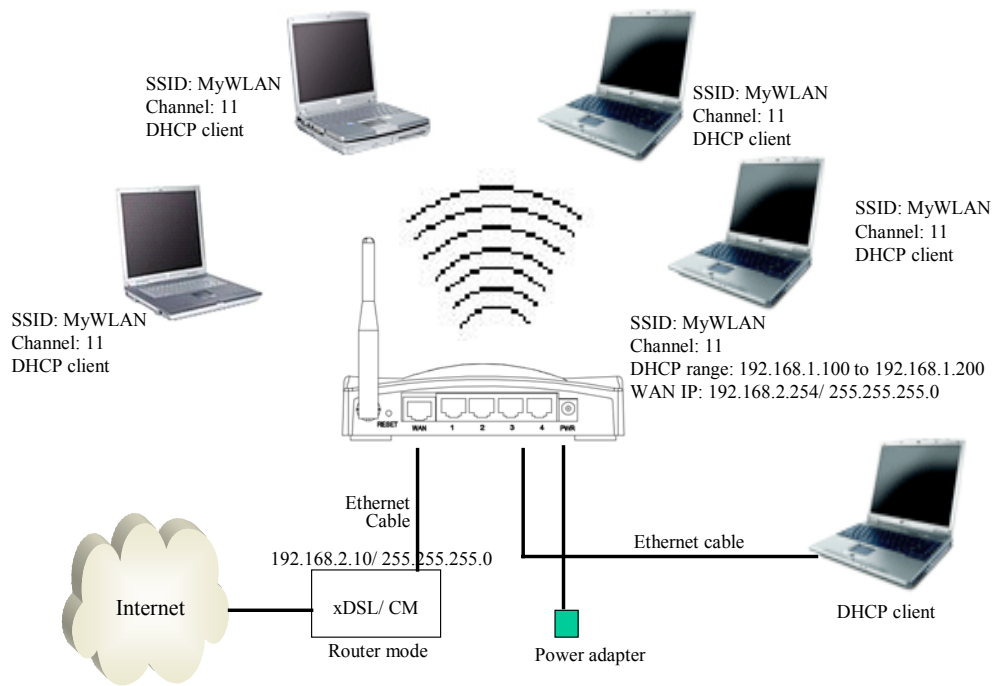
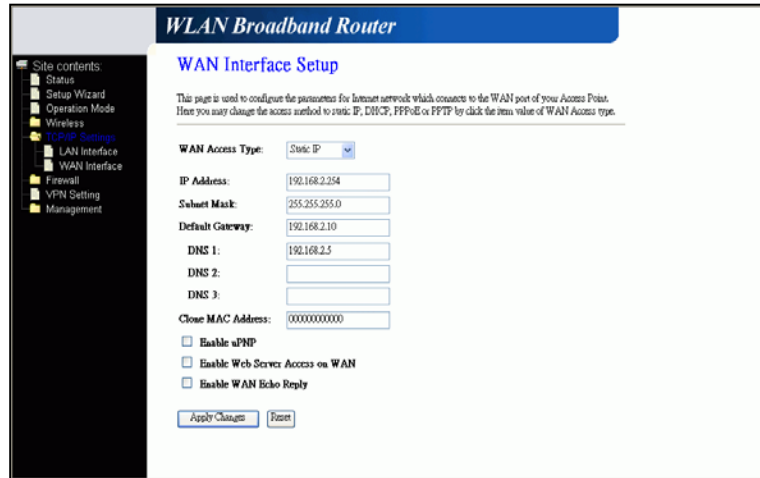
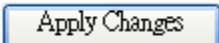


Figure 4 – Configuration Example Two – Fixed IP on the WAN

**Configure the WAN interface:**

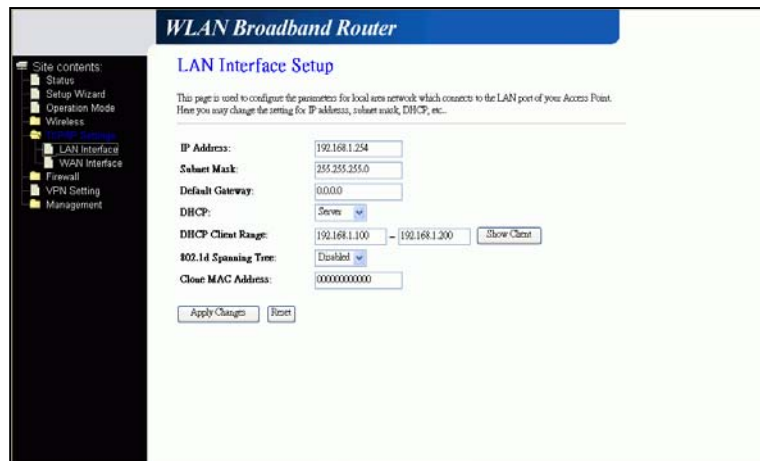
Open WAN Interface Setup page, select Fixed IP then enter IP Address  
 “192.168.2.254”, subnet mask  
 “255.255.255.0”, Default gateway  
 “192.168.2.10”.

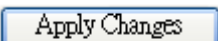


Press  button to confirm the configuration setting.

**Configure the LAN interface:**

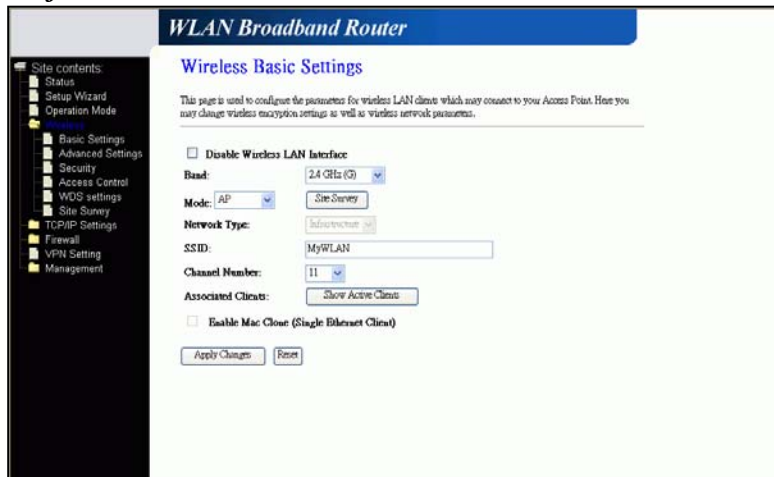
Open LAN Interface Setup page, enter the IP Address  
 “192.168.1.254”, Subnet Mask  
 “255.255.255.0”, enable DHCP Server, DHCP client range  
 “192.168.1.100” to “192.168.1.200”.

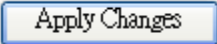


Press  button to confirm the configuration setting.

**Configure the WLAN interface:**

Open WLAN Interface Setup page, enter the SSID “MyWLAN”, Channel Number “11”.



Press  button to confirm the configuration setting.