

# **802.11g Wireless Broadband Router**

**User's Manual**

## FCC Certifications



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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

## **CE Mark Warning**



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

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

### **Trademarks:**

All trade names and trademarks are the properties of their respective companies.

Copyright © 2006, All Rights Reserved.

---

## **Table of Contents**

---

Unpacking Information .....	1
Introduction To Wireless Router .....	2
General Description .....	2
Key Features .....	3
The Front Panel .....	4
System LEDs .....	4
Port LEDs (Wireless) .....	4
Port LEDs (WAN) .....	4
Port LEDs (LAN) .....	5
The Rear Panel .....	5
Power Connection .....	5
Placement (Optional) .....	5
Restore Default Button .....	6
Installing And Using Wireless Router .....	7
Network configuration setup .....	7
Computer configuration setup .....	8
Management .....	10
Wireless Router configuration setup .....	10
Setup Wizard .....	12
Operation Mode .....	16
Wireless .....	17
Basic Settings .....	17
Advanced Settings .....	20
Security .....	22
Access Control .....	24
WDS Setting .....	25
TCP/IP Setting .....	26

LAN Interface Setup .....	26
WAN Interface Setup .....	27
Static IP Mode .....	27
Firewall Configuration .....	31
Port Filtering .....	31
IP filtering .....	32
MAC filtering .....	33
Port forwarding .....	34
URL Filtering .....	35
Virtual DMZ .....	36
Management .....	37
Status .....	37
Statistics .....	39
DDNS .....	39
Time Zone Setting .....	40
System Log .....	40
Upgrade Firmware .....	41
Save and Reload Settings .....	42
Password .....	42
Product Specifications .....	43

## **Unpacking Information**

---

Thank you for purchasing the product. Before you start, please check all the contents of this package.

The product package should include the following:

- 1. One Wireless Router**
- 2. One power adapter**
- 3. One User Manual (CD)**
- 4. One detachable antenna**

## **Introduction To Wireless Router**

---

### **General Description**

The Wireless Router built-in with 4-port 10/100Mbps Fast Ethernet Switch is the latest generation of Wireless router product for Home/Office and SOHO users. This full-feature and self-contained compact Wireless Router will be fully for broadband access in both of LAN and Wireless environment. This device has been specifically designed to provide LAN and Wireless users the most cost-effective method with multiple accesses to the Internet at the cost of a single public IP address (IP Sharing) and enjoy the true Plug-and-Play installation. Moreover, the built-in 4-port 10/100Mbps switch lets users plug the network cable into the device without buying additional switch.

This device is also an Access Point. It has a built-in wireless LAN. Users can connect to Internet using wireless network interfaces anywhere within the range of its radio transmission. It's ideal for SOHO users who require instant and convenient access to Internet without the restriction of connecting cables.

The friendly WEB-based graphics interface for setup makes any inexperienced users soon enter plug-and-play operation. Embedded DHCP server simplified IP address management and no MIS people needed for daily technical services. What is more, NAT/firewall is also implemented on this compact Router Box for protecting whole LAN from outside attack.

### **Key Features**

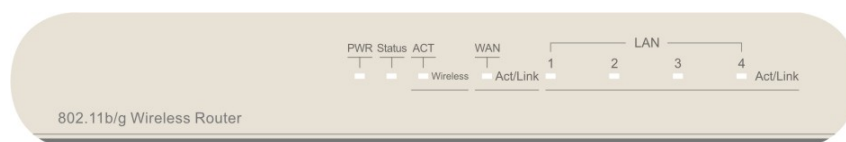
The switch provides the following key features:

- Complies with IEEE 802.11b/g wireless standards
- Provides one 802.11b/g wireless Reverse SMA detachable antenna
- High speed transfer data rate up to 54Mbps
- Supports turbo mode for 72Mbps data transfer
- Supports wireless data encryption with 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 and AES functions
- Supports system log
- Supports authentication for wireless connectivity based on ESSID
- Provides MAC access control and hidden SSID function
- WDS supported with WEP, TKIP and AES encryption
- Channel : USA 11, Europe 13
- Supports NAT/NAPT IP Sharing
- Supports Static IP, PPPoE, PPTP, & DHCP client
- SPI Anti-DoS Firewall; Virtual DMZ; DNS relay; UPnP
- Provides DHCP server
- Supports ALG for FTP, NetMeeting, DDNS (DynDNS, TZO)
- Supports firmware upgrade function via Web
- Compliant with FCC Part 15.247 for US, ETS 300 328 for Europe
- Flash : 2MB NOR type, SDRAM : 8MB
- Certifications : FCC Class B, CE Mark



## **The Front Panel**

The front panel of the Wireless Router is shown below.



### **System LEDs**

System LED indicators locate on the front panel for showing the operating status of the whole device.

- **PWR (Power) LED**  
This indicator lights green when the Wireless Router is receiving power; otherwise, it is off.
- **Status LED**  
The LED will be dark for a few seconds when the system is started. After that, the LED will blink periodically to show the Wireless Router is working normally. If the LED stays green/dark that means the system failed, you need to contact your agent or try to reboot the system.

### **Port LEDs (Wireless)**

- **ACT LED**
  - I. When Wireless AP is ready for data transmitting and receiving, it is steady green.
  - II. When the data is transmitting or receiving, it is blinking green.

### **Port LEDs (WAN)**

Port LED (WAN) indicators locate on the front panel for showing the operating status of WAN port.

- **Act/Link LED**  
The LED stays light (green) means the port has good linkage to its associated devices.  
The LED will blink green when there is traffic transverse the port.

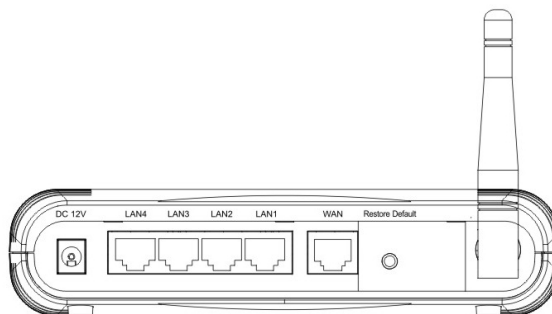
### **Port LEDs (LAN)**

Port LEDs (LAN) indicators locate on the front panel for showing the operating status of 10/100Mbps Fast Ethernet switching ports.

- **Act/Link LED**  
Every port has a Act/Link LED. Steady green (link state) indicates that the port has good linkage to its associated devices. Flashing green indicates that the port is receiving or transmitting data between its associated devices.

### **The Rear Panel**

The rear panel of the Wireless Router is shown below



### **Power Connection**

Plug the circle end of the power adapter firmly into the rear panel of the Wireless Router, and the other end put into an electric service outlet then the system is ready.

### **Placement (Optional)**

There are three ways to place the Router. The first way is to place the Router horizontally on a surface. The second way is to attach the router to the wall. The third way is to stand the Router vertically on a surface. These options are explained in further detail below.

#### **Desktop Option**

1. The Router has one plastic stand that can be divided into two parts.
2. Combine one part of stand with the side of router.
3. Do the same with the second part.
4. Place the Router

### **Wall-mount option**

Before attach this router on the wall, you have to finish the desktop option steps first.

1. Select a location with access for cables and a power outlet.
2. Unplug the unit. Place it upside down on a flat surface and mark the two holes for anchors.
3. Installing the Wall mount anchor (plastic) into the wall with tools such as drill or hammer.
4. Insert the provided screws in each hole of the stand parts.
5. Attaches the unit to the anchors on the wall.

### **Stand Option**

1. The Router includes two stand parts.
2. Combine two parts into one stand. Combine it with the side of router near the power port. Push the stand up to snap it into place.
3. Place the Router.

### **Restore Default Button**

1. Push the button for more than 5 seconds and then release it, the system will return to factory default setting. In the meantime, system rewrites flash to default value and Status LED halts for a while. Approximately 60 seconds later, the Status LED blinks green periodically, now the whole system parameters have returned to factory default value. If the process has been interrupted by any reason (power off...), the system will fail. Before performing the process, ensure a safe operating environment please !
2. To reboot the Router, Press the button for 2-5 seconds and then release it, and all the setting won't be erased. Wait for the Router to complete the reboot, and then you can start to use it.

---

**Warning :** Incomplete factory setting recovery procedure will cause the Wireless Router malfunction ! If you are unfortunately in this situation, do not try to repair it by yourself. Consult your local distributor for help !

---

## **Installing And Using Wireless Router**

This Chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. We suggest you go over the whole chapter and then do more advanced operation.

### ***Network configuration setup***

---

Steps to build up the network:

- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.
- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer's Ethernet card to an 10/100Mbps Ethernet port on the back of the Wireless Router.
- Plug-in the power adapter to the Router and the other side to the wall outlet.

## ***Computer configuration setup***

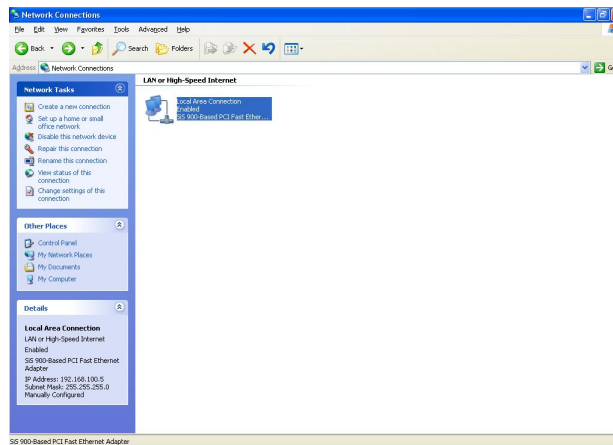
In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to be compatible with the device. The router supports DHCP server and it is enabled as default. Users that configure your IP address as “**Obtain an IP address automatically**” may skip the following IP configuration instruction.

### **Note:**

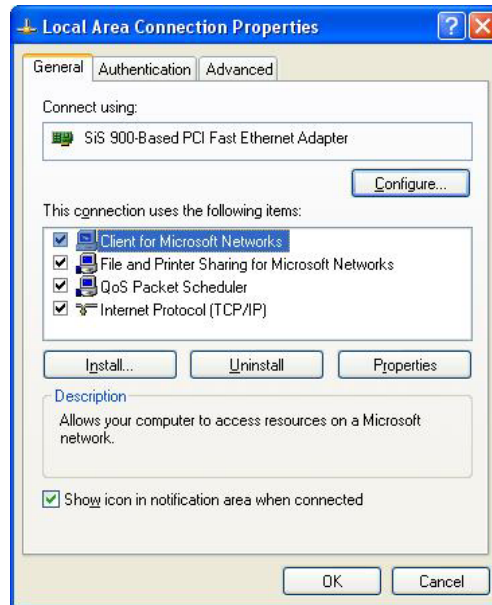
1. The default network setting of the device:  
**IP address:** 192.168.1.1  
**Subnet Mask:** 255.255.255.0  
**DHCP Server:** enabled
2. In the following TCP/IP configuration guide, the IP address “192.168.1.2 ” is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose 192.168.1.1 for the IP address (192.168.1.1) has been set as the default IP for this device.
3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

### **Procedures to configure IP addresses for your computer**

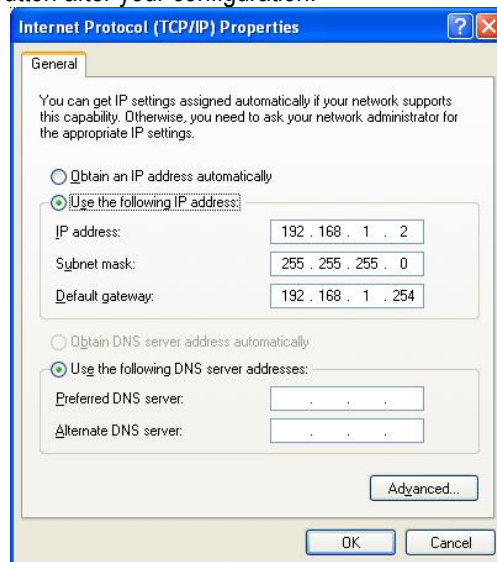
1. If you are in Classic Start menu view, click **Start→Settings→Control Panel→Network Connections**.  
If you are in Start menu view, click **Start→Control Panel→ Network Connections**.
2. Double click “**Local Area Connection**”



3. Choose **Internet Protocol (TCP/IP)** and click **Properties**.



4. You may choose "Obtain an IP address automatically" (recommended) to get IP address automatically or choose "Use the following IP address" to specify IP addresses manually. Please click the OK button after your configuration.



## Management

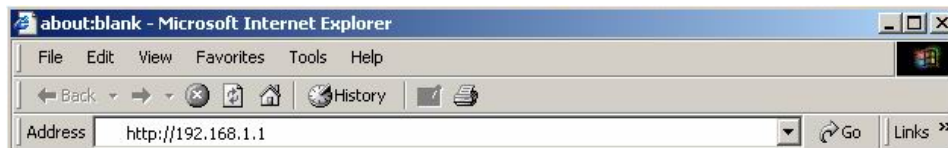
---

### ***Wireless Router configuration setup***

---

In order to make the whole network operate successfully, it is necessary to configure the Wireless Router through your computer has a WEB browser installed. Please follow up the steps listed below.

1. Double click the Internet WEB browser icon on your desktop screen (Netscape Communicator 4.0 and Internet Explorer 3.0 or update version)
2. Type 192.168.1.1 into the URL WEB address location and press Enter.



3. The Username and Password Required window appears.
  - Enter **admin** in the User Name location (default value).
  - Enter **admin** in the Password location (default value).
  - Click "**OK**" button



#### 4. The Graphic User Interface

After the password authorization, the Setup Wizard shows up as the home page of the Graphic User interface. You may click on each folder on left column of each page to get access to each configuration page.





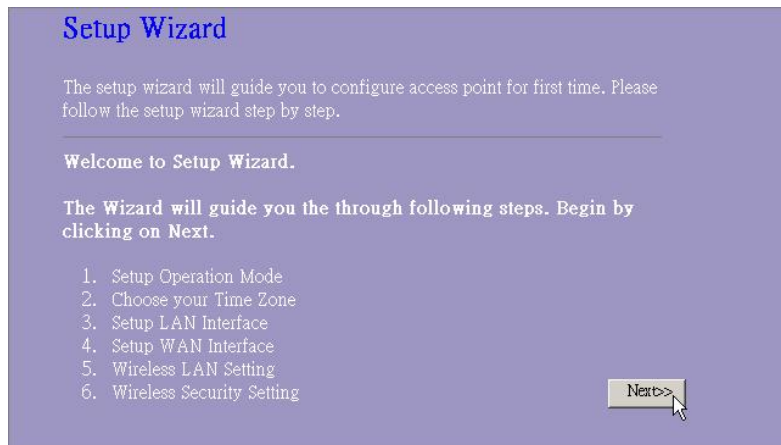
## Setup Wizard

---

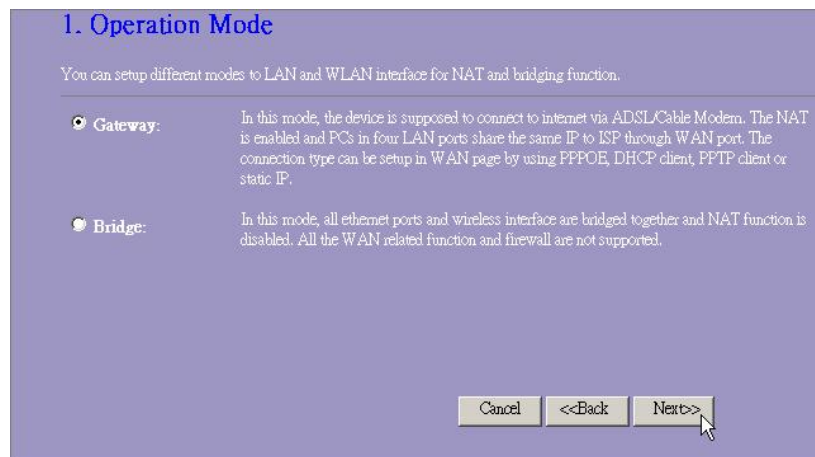
If you are using the router for the first time, you may follow the procedures of the setup wizard to do a step-by-step configuration.

**Note:** The following instruction does an overall introduction to the Setup Wizard. For detail information to each item, please refer to instruction of each page.

1. To start the Setup Wizard, click the “Next” button to proceed.



2. Select your demanding operation mode and click “Next”.



3. Mark the check box to enable synchronizing time by NTP server. Select the religion you live and a NTP server by clicking the drop list then click "Next".

**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>>

4. Specify an IP address and subnet mask for connecting to the router in LAN.

**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 address, subnet mask, DHCP, etc..

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Cancel <<Back Next>>

5. Select a WAN access type for the router to connect to Internet. Fill in the parameters that required in each blank, and then click the “Next” button. You may get those parameters from your ISP.

**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:

IP Address:

Subnet Mask:

Default Gateway:

DNS :

6. Select the wireless parameters that are used for associating with this router and click “Next”

**5. Wireless Basic Settings**

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

---

Band:

Mode:

SSID:

Country:

Channel Number:

7. Click the drop list to select the encryption type for your wireless network. Fill in the parameters for the encryption type you select and click finish to complete configuration.

## 6. 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:

Cancel

<<Back

Finished

## ***Operation Mode***

---

To select an operation mode for this router, click on the mode that you want to perform and click the  button to execute.

### Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.
- Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

## Wireless

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE802.11b/g wireless network adaptor connect to your Intranet. It supports WEP encryption and MAC address filter to enhance the security of your wireless network.

### Basic Settings

You can set up the configuration of your Wireless and monitor the Wireless Clients associate with your AP.

#### 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:

Mode:

SSID:

Country:

Channel Number:

Associated Clients:

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

### Configuration

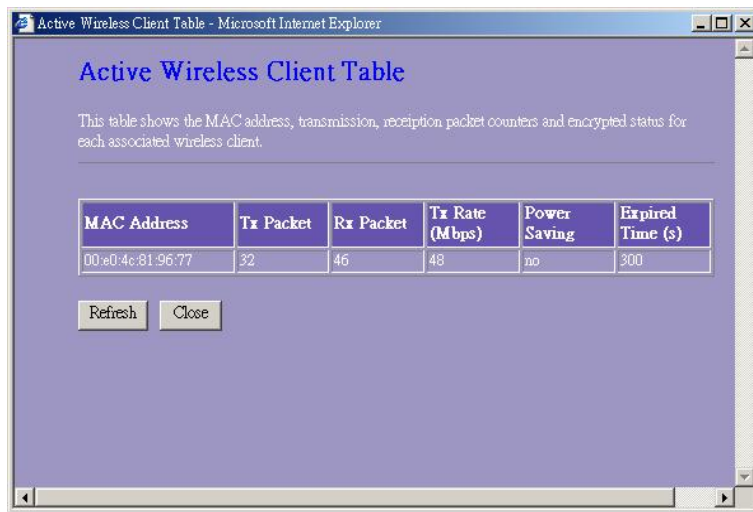
<b>Disable Wireless LAN Interface</b>	To Disable interface of Wireless LAN
<b>Band</b>	To select a band for this device to match 802.11b, 802.11g or both.
<b>Mode</b>	Configure this device as AP, WDS or both.
<b>SSID</b>	The name of the wireless network
<b>Country</b>	Select the region you live.
<b>Channel Number</b>	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
<b>Associated Clients</b>	Click "Show Active Clients" button, then an "Active

	Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
<b>Enable Universal Repeater Mode</b>	Mark this checkbox to enable Universal Repeater Mode which acts this device as an AP and client simultaneously.
<b>SSID of Extended Interface</b>	While you enable the Universal Repeater Mode, you have to specify an SSID for the extended interface.

Click **<Apply changes>** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

- **Active Wireless Client Table**

This is the window that pops up after clicking the **"Show Active Clients"** button.



<b>MAC Address</b>	MAC address of this active wireless station.
<b>Tx Packet</b>	The number of transmitted packets that are sent out from this active wireless station.
<b>Rx Packet</b>	The number of received packets that are received by this active wireless station.

<b>TX Rate</b>	The transmission rate
<b>Power Saving</b>	Shows if the wireless client is in Power Saving mode
<b>Expired Time</b>	This is the time in second before dissociation. If the wireless keeps idle longer than the expired time, this wireless router will dissociate it. The wireless client station has to associate again when it is active.
<b>Refresh</b>	Refresh the "Active Wireless Client Table".
<b>Close</b>	Close the "Active Wireless Client Table".



## Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Data Rate, Preamble Type, Broadcast SSID, IAPP and 802.11g Protection. We recommend not changing these parameters unless you know what changes will be there on this 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

RF Output Power:     100%     50%     25%     10%     5%

Turbo Mode:     Auto     Always     Off

## Configuration

<b>Authentication Type</b>	<b>Open System mode</b>	Wireless AP can associate with this wireless router without WEP encryption.
	<b>Shared Key mode</b>	You should also setup WEP key in the "Security" page and wireless AP associating with this wireless router should use WEP encryption in the authentication phase.
	<b>Auto</b>	The wireless client can associate with this wireless router by using any one of these two Modes.
<b>Fragment Threshold</b>	To specifies the maximum size of packet during the data transition. The lower values you set, the worst performance it will be.	
<b>RTS</b>	If the packet size is smaller the RTS threshold, the	

<b>Threshold</b>	wireless router will not send this packet by using the RTS/CTS mechanism.
<b>Beacon Interval</b>	The period of time how long a beacon is broadcasted.
<b>Data Rate</b>	The "Data Rate" is the data packets limitation this wireless router can transmit. The wireless router will use the highest possible selected transmission rate to transmit the data packets.
<b>Preamble Type</b>	It defines the length of CRC block in the frames during the wireless communication. "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability
<b>Broadcast SSID</b>	If you enable "Broadcast SSID", every wireless station located within the coverage of this wireless router can discover this wireless router easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast SSID" can provide better security.
<b>IAPP</b>	To enables multiple AP to communicate and pass information regarding the location of associated Stations.
<b>802.11g Protection</b>	Some 802.11g wireless adapters support 802.11g protection, which allows the adapters searches for 802.11g singles only. Select the "Disabled" to disable supporting 802.11g protection or select "enable" to support this function.
<b>RF Output power</b>	Select the RF (Radio Frequency) power. The RF output power has positive correlation with signal strength.
<b>Turbo Mode</b>	Some of our wireless adapters supports turbo mode, which provides a better connection quality. Select "Always" to support turbo mode or select "off" to turn it off . Select "Auto" turns it on or off automatically.

Click the <Apply Changes> button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

## Security

At the page, you can set up the WEP, WPA Encryption to ensure the security of your Wireless.

### 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:

Use 802.1x Authentication  WEP 64bits  WEP 128bits

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

WPA Cipher Suite:  TKIP  AES

WPA2 Cipher Suite:  TKIP  AES

Pre-Shared Key Format:

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server: Port  IP address  Password

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

## Configuration

<b>Encryption</b>	To enable WEP, WPA, WPA2 and WPA2 Mixed encryption modes, select the option in the drop list. If you select none, any data will be transmitted without Encryption and any station can access the router.
<b>Use 802.1x Authentication</b>	To enable the 802.1x, Click the check box of the item.
<b>WPA Authentication Mode</b>	There are two items, "Enterprise (WPA-Radius)" and "Personal (Pre-Shared Key)". You can select the mode by clicking the item.
<b>WPA Cipher Suite</b>	Select the WPA Cipher Suite to be TKIP or AES

<b>WPA2 Cipher Suite</b>	Select the WPA2 Cipher Suite to be TKIP or AES
<b>Pre-Shared key Format</b>	To decide the format, select what you need in the drop list.
<b>Pre-shared Key</b>	Enter the Pre-shared Key according to the pre-shared key format you select.
<b>Enable Pre-Authentication</b>	You can mark this checkbox to enable Pre-authentication after selecting Enterprise (RADIUS) WPA 2 authentication mode
<b>Authentication RADIUS Sever</b>	If you use RADIUS Sever to ensure your security, you have to set up the parameters in the item. To set up the Port, IP address and Password of your RADIUS, Enter the Port Number, IP and Password.

Click <**Apply Change**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

## Access Control

To restrict the Number of Access authentication of Stations, Set up the control list in this page.

### 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
-------------	---------	--------

## Configuration

<b>Wireless Access Control Mode</b>	Click on the drop list to choose the access control mode. You may select "Allow listed" to allow those allowed MAC addresses or select "Deny Listed" to ban those MAC addresses from accessing to this device.
<b>MAC Address &amp; Comment</b>	To set up the Value of MAC Address & Comment; enter the MAC Address and Comment of station and click Apply Changes to save.
<b>Current Access Control list</b>	To Delete the station on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all stations on the list, click "Delete All" to remove all of them.

Click <Apply Change> button to save the above configurations. You can now configure other advance sections or start using the router.



## TCP/IP Setting

### LAN Interface Setup

To set up the configuration of LAN interface, Private IP of you router LAN Port and Subnet mask for your LAN segment.

#### 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 address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
DHCP Server:	<input type="text" value="Enabled"/>
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
802.1d Spanning Tree:	<input type="text" value="Disabled"/>
<input type="checkbox"/> Enable UPnP	
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

#### Configuration

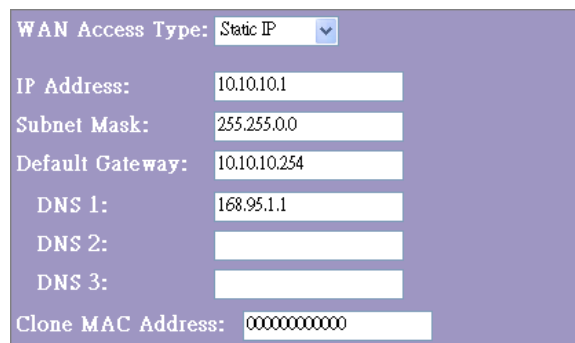
<b>IP address</b>	The IP of your Router LAN port (Default 192.168.1.1)
<b>Subnet Mask</b>	Subnet Mask of you LAN (Default 255.255.255.0)
<b>DHCP Server</b>	To give your LAN Client an IP, you have to enable "DHCP Server". If not, manual setting up your client IP is necessary when you want to use the router as your client's default gateway.
<b>DHCP Client Range</b>	Specify the DHCP Client IP address range. You can also click the "Show Client" button to listed those connected DHCP clients.
<b>802.1d Spanning tree</b>	To prevent from network loops and preserve the quality of bridged network
<b>Enable UPnP</b>	Mark this checkbox to allow this router to be recognized by uPnP.

## WAN Interface Setup

---

This page allows users to configure those parameters for connecting to Internet. You may select the WAN Access Type from the drop list and configure parameters for each mode.

### Static IP Mode



The screenshot shows a configuration form for Static IP Mode. The 'WAN Access Type' is set to 'Static IP'. The fields are: IP Address: 10.10.10.1, Subnet Mask: 255.255.0.0, Default Gateway: 10.10.10.254, DNS 1: 168.95.1.1, DNS 2: (empty), DNS 3: (empty), and Clone MAC Address: 000000000000.

---

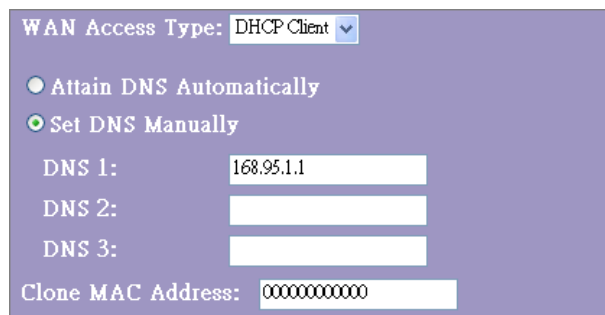
**IP Address, Subnet Mask and Default Gateway** Fill in the IP address, Subnet Mask and Default Gateway that provided by your ISP.

---

**DNS 1, 2 and 3** To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

---

### DHCP Client Mode



The screenshot shows a configuration form for DHCP Client Mode. The 'WAN Access Type' is set to 'DHCP Client'. There are two radio buttons: 'Attain DNS Automatically' (selected) and 'Set DNS Manually'. Below the radio buttons are fields for DNS 1: 168.95.1.1, DNS 2: (empty), and DNS 3: (empty). The Clone MAC Address field contains 000000000000.

---

**Attain DNS automatically:** If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"

---

**Set DNS Manually** To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

---



## PPPoE Mode

WAN Access Type: PPPoE

User Name:

Password:

Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1452 (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1: 168.95.1.1

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

<b>User Name, password and service name</b>	Fill in the User Name, password and service name that provided by your ISP.
<b>Connection Type</b>	<p>“<b>Continuous</b>” is for Always keep connection</p> <p>“<b>Connect on demand</b>” is for bill by connection time. You can set up the Idle time for the value specifies the number of time that elapses before the system automatically disconnects the PPPoE session.</p> <p>“<b>Manual</b>” To connect to ISP, click “Connect” manually from the WEB user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.</p>
<b>Idle Time:</b>	The value specifies the number of idle time that elapses before the system automatically disconnects the PPPoE session.
<b>MTU Size</b>	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation.
<b>Attain DNS automatically:</b>	If your DNS provide by ISP is dynamic, choose “Attain DNS automatically
<b>Set DNS Manually</b>	To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

## PPTP Mode

WAN Access Type:	<input type="text" value="PPTP"/>
IP Address:	<input type="text" value="172.16.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Server IP Address:	<input type="text" value="172.16.1.1"/>
User Name:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
MTU Size:	<input type="text" value="1452"/> (1400-1492 bytes)
<input type="radio"/> Attain DNS Automatically	
<input checked="" type="radio"/> Set DNS Manually	
DNS 1:	<input type="text" value="168.95.1.1"/>
DNS 2:	<input type="text"/>
DNS 3:	<input type="text"/>

---

**IP Address, Subnet Mask, Server IP Address, User Name and Password** Fill in the IP address, Subnet Mask, Server IP Address, User Name and password that provided by your ISP.

---

**MTU Size** To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation.

---

**Attain DNS automatically:** If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"

---

**Set DNS Manually** To specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

---

## Common configurations for WAN interface

There are some settings are able to be configured on each WAN access types:



The screenshot shows a configuration window with a purple background. At the top, there is a text box labeled 'Clone MAC Address:' containing the value '000000000000'. Below this are four checkboxes, each followed by a label and a text box: 'Enable Web Server Access on WAN from port:' with '8080', 'Enable IPsec pass through on VPN connection', 'Enable PPTP pass through on VPN connection', and 'Enable L2TP pass through on VPN connection'. At the bottom, there are two buttons: 'Apply Changes' and 'Reset'.

---

<b>Enable Web Server Access on WAN from port</b>	To Enable the user to access this Router through Internet, Enter the specific IP and the port number
<b>Enable IPsec pass through on VPN connection</b>	Mark the check box to enable IPsec pass through on VPN connection and clear the checkbox to disable.
<b>Enable PPTP pass through on VPN connection</b>	Mark the check box to enable PPTP pass through on VPN connection and clear the checkbox to disable.
<b>Enable L2TP pass through on VPN connection</b>	Mark the check box to enable L2TP pass through on VPN connection and clear the checkbox to disable.
<b>Clone MAC Address</b>	When ISP use MAC address authentication (with DHCP), then the MAC address of the Ethernet card attached to your Cable modem must be registered with the ISP before connecting to the WAN (Internet). If the Ethernet card is changed, the new MAC address must be registered with the ISP. MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.

---

## Firewall Configuration

---

### Port Filtering

---

The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users.

Port Filtering To restrict certain type of data packets from your LAN to Internet through the Router, add them on the Current Filtering Table.

**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

Local Port Range:  -  Protocol: Both ▾

Comment:

Apply Changes Reset

Current Filter Table:

Local Port Range	Protocol	Comment	Select
------------------	----------	---------	--------

Delete Selected Delete All Reset

### Configuration

---

- |              |   |
|--------------|---|
| <b>STEPS</b> | 1. Click the check box of "Enable Port Filtering" to enable the function.   |
|              | 2. Enter the Port range (EX 25-110), Protocol (UDP/TCP), and comment (EX. E-Mail)   |
|              | 3. To Delete the Port range on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them. |

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

## IP filtering

---

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet.

The screenshot shows the 'IP Filtering' configuration page. At the top, there is a title 'IP Filtering' in blue. Below it, a paragraph explains that entries in the table are used to restrict data packets from the local network to the Internet through the Gateway. The main configuration area includes a checkbox for 'Enable IP Filtering', a text input for 'Local IP Address', a dropdown menu for 'Protocol' (set to 'Both'), and a text input for 'Comment'. Below these are 'Apply Changes' and 'Reset' buttons. A section titled 'Current Filter Table:' contains a table with four columns: 'Local IP Address', 'Protocol', 'Comment', and 'Select'. Below the table are 'Delete Selected', 'Delete All', and 'Reset' buttons.

## Configuration

---

- | STEPS |   |
|-------|---|
|       | 1. Click the check box of "Enable IP Filtering" to enable the function.   |
|       | 2. Enter the specific Local IP address (EX 10.10.3.9), Protocol (UDP/TCP), and comment (EX. Peter)  |
|       | 3. To Delete the IP address on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them. |

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

## MAC filtering

---

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the MAC addresses to block specific internal users from accessing the Internet.

The screenshot shows the 'MAC Filtering' configuration page. At the top, there is a title 'MAC Filtering' and a descriptive paragraph: '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.' Below this, there is a checkbox labeled 'Enable MAC Filtering'. Underneath, there are two input fields: 'Local MAC Address:' and 'Comment:'. At the bottom of this section are two buttons: 'Apply Changes' and 'Reset'. Below the input fields, there is a section titled 'Current Filter Table:' which contains a table with three columns: 'Local MAC Address', 'Comment', and 'Select'. Below the table are three buttons: 'Delete Selected', 'Delete All', and 'Reset'.

## Configuration

---

- | STEPS |   |
|-------|---|
| 1.    | Click the check box of "Enable MAC Filtering" to enable the function.   |
| 2.    | Enter the specific MAC address (EX 00:0e:b6:a8:72), and comment (EX. Peter)   |
| 3.    | To Delete the MAC address on the list, Click the check box in the select item and click the "Delete Selected". If you want to delete all Entries on the list, click "Delete All" to remove all of them. |

Click <Apply Change> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

## Port forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router 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

Local IP Address:  Protocol:  Port Range:  -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

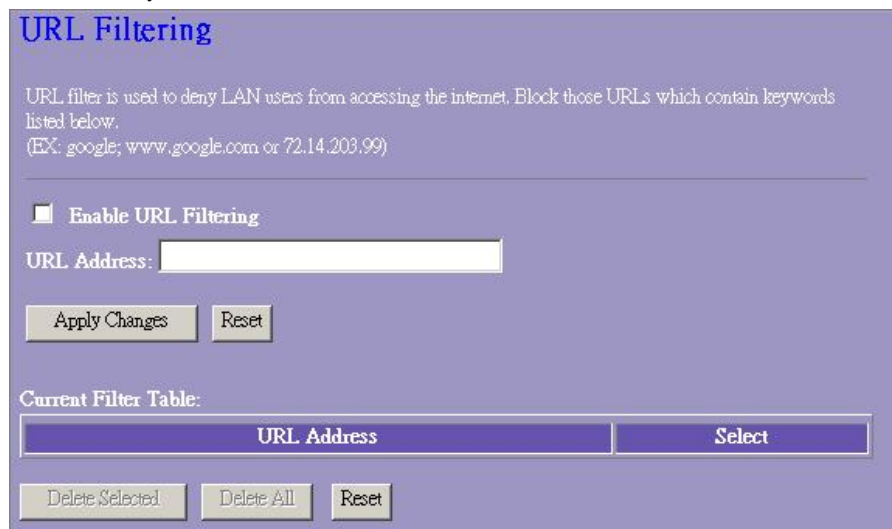
## Configuration

- |              |   |
|--------------|---|
| <b>STEPS</b> | 1. Click the check box of "Enable port forwarding" to enable the function.  |
|              | 2. Enter the specific IP address (EX 10.10.10.10), Protocol (UDP/TCP), Port range (EX 25-110), and comment (EX. E-Mail)   |
|              | 3. To Delete the IP address on the table, Click the check box in the select item and click the "Delete Selected". If you want to delete all Entries on the table, click "Delete All" to remove all of them. |

Click <Apply Change> at the bottom of the screen to save the above configurations.

## URL Filtering

The URL Filter allows users to prevent certain URL from accessing by users in LAN. This filter will block those URLs that contain certain keywords.



The screenshot shows a web-based configuration page for URL filtering. At the top, the title "URL Filtering" is displayed in blue. Below the title, a descriptive paragraph explains that the filter is used to deny LAN users from accessing the internet by blocking URLs containing specific keywords, with examples like "google" or "72.14.203.99". A checkbox labeled "Enable URL Filtering" is currently unchecked. Below this is a text input field for "URL Address". Two buttons, "Apply Changes" and "Reset", are positioned below the input field. A section titled "Current Filter Table" contains a table with two columns: "URL Address" and "Select". Below the table are three buttons: "Delete Selected", "Delete All", and "Reset".

## Configuration

- |              |   |
|--------------|---|
| <b>STEPS</b> | 1. Click the check box of "Enable URL Filtering" to enable the function.  |
|              | 2. Enter the URL that is going to be banned.  |
|              | 3. To Delete the URL on the table, Click the check box in the select item and click the "Delete Selected". If you want to delete all URLs on the table, click "Delete All" to remove all of them. |

Click <Apply Change> at the bottom of the screen to save the above configurations.



## Virtual DMZ

---

The virtual DMZ is used to enable protocols, which need to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this page.

### Virtual DMZ

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

Enable Virtual DMZ

Virtual DMZ Host IP Address:

To configure it, enter the Host IP (private IP address) and Click “Apply changes” to enact the setting.

## Management

### Status

In the home page of the Wireless Router, the left navigation bar shows the options to configure the system. In the right navigation screen is the summary of system status for viewing the configurations.

This page shows the current status and some basic settings of the device.

SYSTEM	
Uptime	0day:0h:2m:54s
Firmware Version	v1.0
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	WLAN-11g-GW
Channel Number	11
Encryption	Disabled
BSSID	00:e0:7d:c0:c7:d1
Associated Clients	0
LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:e0:7d:c0:c7:d1
WAN Configuration	
Attain IP Protocol	Static IP
IP Address	10.10.10.1
Subnet Mask	255.255.0.0
Default Gateway	10.10.10.254
MAC Address	00:e0:7d:c0:c7:d3

- **System**

<b>Uptime</b>	The period that you power the device on.
<b>Firmware Version</b>	The version of the firmware applied on this device.

- **Wireless Configuration**

<b>Mode</b>	The operation mode of the wireless router
<b>Band</b>	The performing band of this wireless router
<b>SSID</b>	The name of this wireless network

<b>Channel Number</b>	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel
<b>Encryption</b>	The security encryption status of this wireless network
<b>BSSID</b>	The Basic Service Set Identity of this router. (This parameter is the same as the MAC address of LAN port)
<b>Associated Clients</b>	The number of associated clients.

- LAN Configuration

<b>IP Address</b>	IP Address of router
<b>Subnet Mask</b>	Subnet Mask of the router
<b>DHCP Server</b>	Enabled or Disable of DHCP
<b>MAC Address</b>	MAC Address of LAN-port

- WAN Configuration

<b>Attain IP Protocol</b>	Static IP address
<b>IP Address</b>	IP address of WAN-port
<b>Subnet Mask</b>	Subnet Mask of WAN-port
<b>Default Gateway</b>	Default Gateway of WAN-port
<b>MAC Address</b>	MAC Address of WAN-port

## Statistics

On this page, you can monitor the sent & received packets counters of wireless, Ethernet LAN, and Ethernet WAN. To see the latest report, click refresh button.

### Statistics

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

Wireless LAN	<i>Sent Packets</i>	145357
	<i>Received Packets</i>	1121
Ethernet LAN	<i>Sent Packets</i>	6845
	<i>Received Packets</i>	858102
Ethernet WAN	<i>Sent Packets</i>	8285
	<i>Received Packets</i>	0

## DDNS

This page allows users to connect to DDNS. To enable DDNS, Mark the “Enable DDNS” checkbox. Select the service provider from the drop list. Fill in domain name, username, and password. Click the “Apply Change” button after configuration.

### 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 :

Domain Name :

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](#)

## Time Zone Setting

---

This page allows users to configure the time of the router. To specify manually, fill in the blanks in “Current Time” and click the “Apply Change” button. To synchronize time from a timeserver, please mark the “Enable NTP client update” checkbox, select a NTP server from the drop list or manually enter a NTP server. Click the “Apply Change” button after your configuration.

**Time Zone Setting**

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

Current Time : Yr 2000 Mon 1 Day 3 Hr 8 Mn 38 Sec 11

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

Enable NTP client update

NTP server :  192.5.41.41 - North America  (Manual IP Setting)

Apply Change Reset Refresh

## System Log

---

This System Log page shows the information of the current activities on the router.

To enable system log function:

1. Mark the “Enable Log” checkbox.
2. To see all information of the system, select the “system all” checkbox.  
To see wireless information only, select the “wireless” checkbox.  
To sent the log information to a certain note, select the “Enable Remote Log” checkbox and fill in the IP address in the “Log Server IP Address” box.
3. Click the “Apply Changes” button to activate

You could also click the “Refresh” button to refresh the log information or click the “clear” button to clean the log table.

**System Log**

This page can be used to set remote log server and show the system log.

Enable Log  
 system all       wireless  
 Enable Remote Log      Log Server IP Address:   
    Server Port: 514

Apply Changes

Refresh   Clear

## Upgrade Firmware

---

To Upgrade Firmware,

- |              |  |
|--------------|--|
| <b>STEPS</b> | <ol style="list-style-type: none"> <li>1. Click "browse..." button to select the firmware you want to upgrade.</li> </ol> <hr style="border-top: 1px dashed black;"/> <ol style="list-style-type: none"> <li>2. Click Upload to start the upgrade process. Please don't close the WEB-browser and wait for process to complete. When Upgrade is completed, you can start to use the router.</li> </ol> |
|--------------|--|

**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.

Select File:

## Save and Reload Settings

---

To save setting to file, click "Save..." button.

To load setting from file,

1. Click "Browse..." on the to select the file
2. Click upload to start the process and wait for it to complete

To reset setting to Default, click reset to start the process and it will be completed till the status LED start blinking.

### Save/Reload Settings

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

Save Settings to File:	<input type="button" value="Save..."/>
Load Settings from File:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Reset Settings to Default:	<input type="button" value="Reset"/>

## Password

---

To set up the Administrator Account information, enter the Username, New password, and reenter the password on the text box. Don't forget to click the "Apply Changes" to save the configuration.

### 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.

User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>
<input type="button" value="Apply Changes"/>	<input type="button" value="Reset"/>

## Product Specifications

<b>Standard</b>	IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX IEEE802.3x full duplex operation and flow control IEEE802.11b wireless LAN infrastructure IEEE802.11g wireless LAN infrastructure
<b>Interface</b>	1 * WAN port 4 * 10/100 RJ-45 Fast Ethernet switching ports Antenna: 802.11b/g wireless reverse SMA detachable
<b>WAN Connection</b>	Ethernet 10/100 Mbps
<b>Cable Connections</b>	RJ-45 (10BASE-T): Category 3,4,5 UTP RJ-45 (100BASE-TX): Category 5 UTP
<b>Network Data Rate</b>	802.11b: 1, 2, 5.5 and 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps
<b>Transmission Mode</b>	Auto-Negotiation (Full-duplex, Half-duplex)
<b>LED indications</b>	System: Power, Status Port (WAN): ACT/LINK Port (LAN): ACT/LINK Port(Wireless): ACT
<b>Security</b>	64/128-bit WEP, WPA(TKIP with IEEE 802.1x), WPA2, AES
<b>Receiver Sensitivity</b>	54Mbps OFDM, 10%PER, -71dBm 11Mbps CCK, 10%PER, -81dBm 1Mbps BPSK, 10%PER, -92dBm
<b>Memory</b>	Flash : 2MB NOR type, SDRAM : 8MB
<b>Transmit Power</b>	16dBm~18dBm
<b>Range Coverage</b>	Indoor 35~100 meters Outdoor 100~300meters.
<b>Emission</b>	FCC CLASS B, CE
<b>Operating Temperature</b>	0° ~ 40°C (32° ~ 104°F)
<b>Operating Humidity</b>	10% - 90%
<b>Power Supply</b>	External Power Adapter, 12VDC/ 1A