User Guide

AIP-W525H

PowerMax 2

Rev: 1.1.0

FCC 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.

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

Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER’S AUTHORITY TO OPERATE THE EQUIPMENT.

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.

“To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

CE Mark Warning

CE ⓘ

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don’t use the product outdoors in France.

CONTENTS

Package Contents

The following items should be found in your package:

- AIP-W525H PowerMax 2 Router
- Power Adapter for AIP-W525H PowerMax 2 Router
- Quick Installation Guide
- Resource CD for AIP-W4525H PowerMax 2 Router, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Chapter 1. Introduction

Thank you for choosing the AIP-W525H PowerMax 2 Router.

1.1 Overview of the Router

The AIP-W525H PowerMax 2 Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. The AIP-W525H PowerMax 2 Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

Incredible Speed

The AIP-W525H PowreMax 2 provides up to 300M wireless connection with other 802.11n wireless clients. The speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128-bit WEP encryption, WiFi protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the AIP-W525H PowerMax 2 provides complete data privacy.

Flexible Access Control

The AIP-W525H PowerMax 2 Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the Router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the Router, please look through this guide to know all the Router’s functions.

1.2 Conventions

The Router or AIP-W525H mentioned in this guide stands for AIP-W525H PowerMax 2 Router without any explanation.

1.3 Main Features

- Make use of IEEE 802.11n wireless technology to provide a wireless data rate of up to 300Mbps.
- One 10/100M Auto-Negotiation RJ45 WAN port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet.
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports Stateful Packet Inspection.
- Supports VPN Passthrough.
- Supports Parental Control and Access Control.
- Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

1.4 Panel Layout

1.4.1 The Front Panel

Figure 1-1 Front Panel sketch

The Router's LEDs and the WPS/Reset Button are located on the front panel (View from left to right).

Name	Status	Indication
PWR	Off	Power is off.
	On	Power is on.
SYS	On	The Router is initializing.
	Flashing	The Router is working properly.
	Off	The Router has a system error.
WLAN	Off	The Wireless function is disabled.

	Flashing	The Wireless function is enabled.
WAN, 1,2,3,4 (LAN)	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an active device linked to the corresponding port.
WPS	Slow Flash	A wireless device is connecting to the network by WPS function. This process will last for about 2 minutes.
	On	A wireless device has been successfully added to the network by WPS function. The LED will keep on for about 5 minutes.
	Quick Flash	A wireless device failed to be added to the network by WPS function.

Table 1-1 The LEDs Description

☞ **Note:**

1. After a device is successfully added to the network by WPS function, the WPS LED will keep on for about 5 minutes and then turn off.

2. When press and hold the WPS/Reset Button for more than 5 seconds, you will reset the router.

1.4.2 The Rear Panel

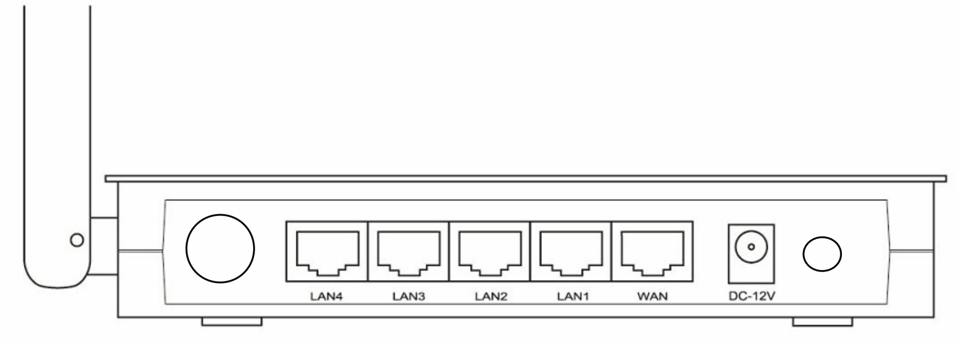


Figure 1-2 Rear Panel sketch

The following parts are located on the rear panel (View from left to right).

- **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this AIP-W525H PowerMax 2.
- **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet.
- **1,2,3,4 (LAN):** Those ports (1, 2, 3, 4) connect the Router to the local PC(s).
- **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the Router is connected directly to the Ethernet.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari

2.2 Installation Environment Requirements

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating Temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

Before installing the Router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the Router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC, Cable/DSL Modem, and the Router.
2. Locate an optimum location for the Router. The best place is usually at the center of your wireless network.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the Router, shown in Figure 2-1. (If you have the wireless NIC and want to use the wireless function, you can skip this step.)
5. Connect the DSL/Cable Modem to the WAN port on the Router, shown in Figure 2-1.

6. Connect the power adapter to the power socket on the Router, and the other end into an electrical outlet. Press the power switch, and then the router will start to work.

7. Power on your PC and Cable/DSL Modem.

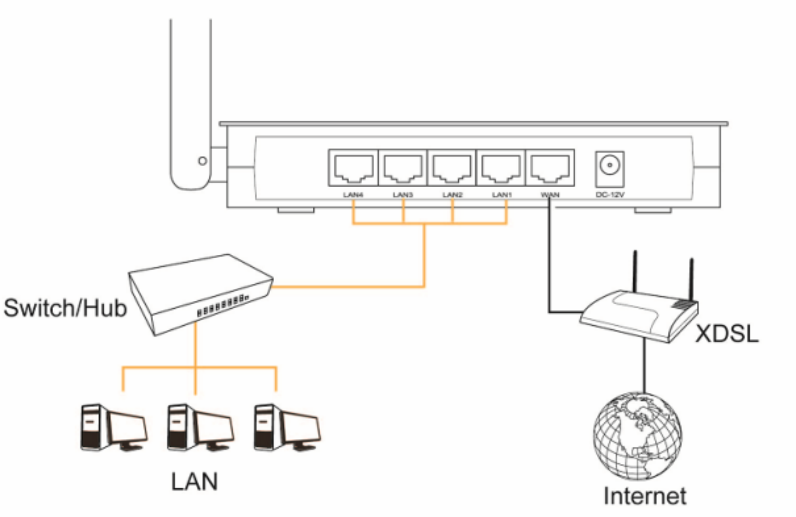


Figure 2-1 Hardware Installation of the AIP-W525H PowerMax 2 Router

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AIP-W525H PowerMax 2 Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the AIP-W525H PowreMax 2 Router is 192.168.2.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the local PC to the LAN ports of the Router. And then you can configure the IP address for your PC in the following two ways.

➢ Configure the IP address manually

1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to Appendix B: Configuring the PC.

2) Configure the network parameters. The IP address is 192.168.2.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.2.1 (The Router's default IP address).

➢ Obtain an IP address automatically

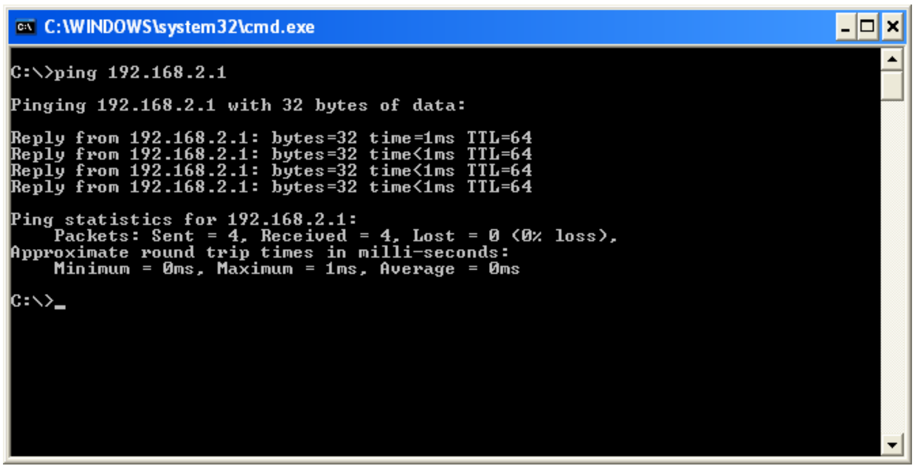
1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to Appendix B: Configuring the PC.

2) Then the built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the Router. The following example is in Windows XP OS.

Open a command prompt, and type *ping 192.168.2.1*, and then press **Enter**.

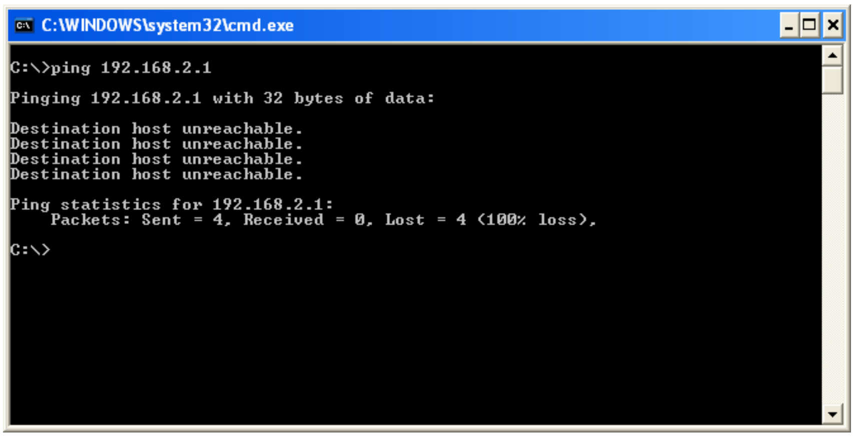
➢ If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the Router has been established well.



```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_
```

Figure 3-1 Success result of Ping command

- If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the Router is failed.



```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

1. Is the connection between your PC and the Router correct?

☞ **Note:**

The 1/2/3/4 LEDs of LAN ports which you link to on the Router and LEDs on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

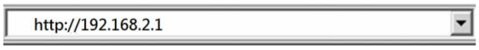
☞ **Note:**

If the Router's IP address is 192.168.2.1, your PC's IP address must be within the range of 192.168.2.2 ~ 192.168.2.254.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the AIP-W525H PowerMax 2 Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.2.1 in the address field of the browser.



http://192.168.2.1

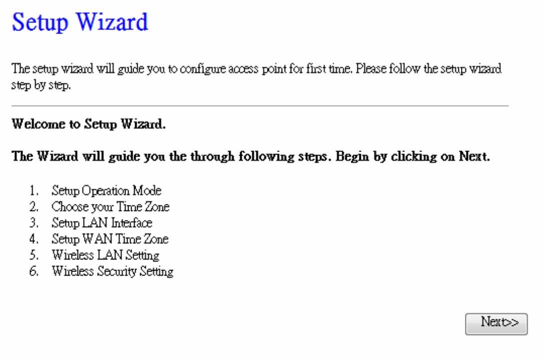
Figure 3-3 Log in the Router

After a moment if a login window pops up, leave blank for both **User Name** and **Password**. Then click **OK** or press **Enter**.

☞ **Note:**

If the above screen does not pop-up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

2. After successfully log in, you can click the **Quick Setup** menu to quickly configure your Router.



Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

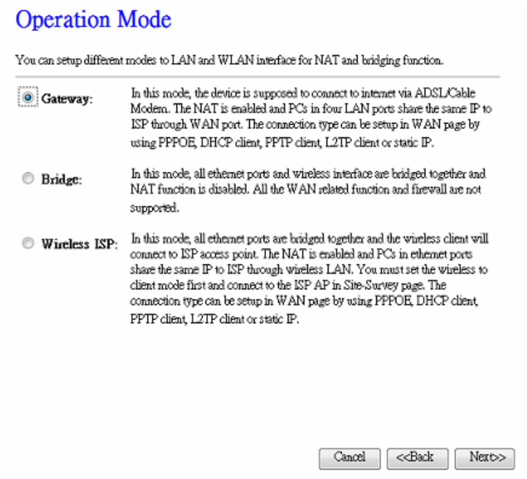
Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Time Zone
5. Wireless LAN Setting
6. Wireless Security Setting

Figure 3-4 Quick Setup

3. Click **Next**, and then **Operation Mode** page will appear, shown in Figure 3-5.



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 four 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, L2TP client or static IP.

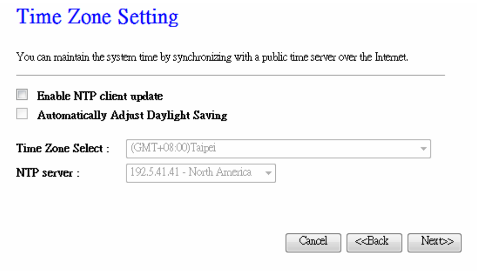
○ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Figure 3-5 Quick Setup - WAN Connection Type

The Router provides three popular ways **Gateway**, **Bridge** and **Wireless ISP** to connect to the Internet. It's recommended that you make use of the **Gateway** function. If you are sure of what kind of connection type your ISP provides, you can select the very type and click **Next** to go on configuring.

4. If you are sure of what kind of NTP server your Router, you can select the very type and click **Next** to go on configuring as shown in Figure 3-6.



Time Zone Setting

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

□ Enable NTP client update

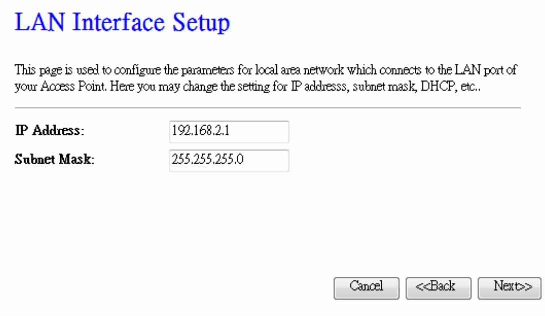
□ Automatically Adjust Daylight Saving

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

NTP server : 192.5.41.41 - North America

Figure 3-6 Quick Setup - Time Zone Setting

5. Confirm the IP address for your Router and click **Next** to go on configuring.



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..

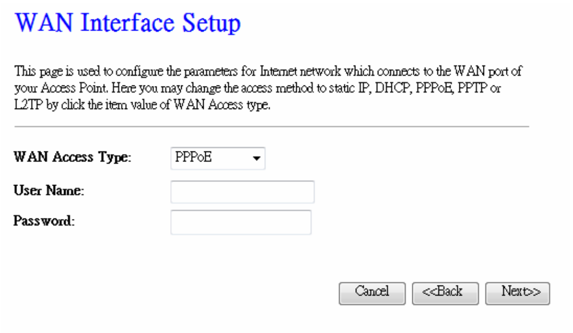
IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Figure 3-7 Quick Setup - LAN Interface Setting

6. If you select **Gateway**, the Router provides six connection types for your ISP provides. Make sure the cable is securely plugged into the WAN port before continue.

   a) If the connection type is **PPPoE**, then select it from drop down menu as shown below. Enter the **User Name** and **Password** provided by your ISP, and then click **Next**.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPPoE

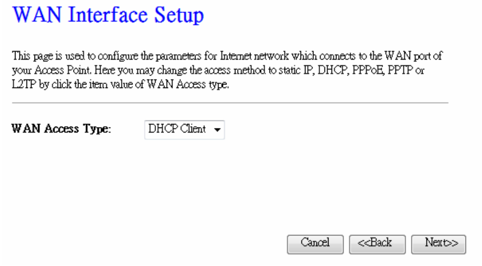
User Name:

Password:

Figure 3-8 Quick Setup - WAN Interface Setting

- **User Name/Password -** Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

b) If the connection type detected is **DHCP Client**, the next screen will appear as shown in Figure 3-9. Then you can go on with the wireless configuration.



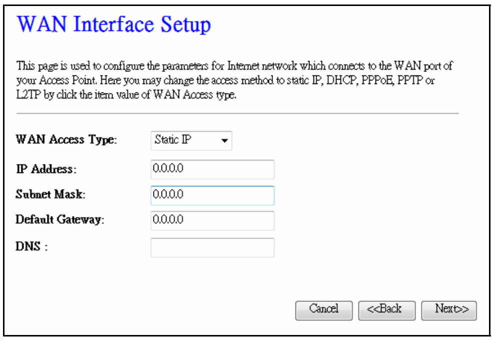
WAN Interface Setup

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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Figure 3-9 Quick Setup - DHCP

c) If the connection type detected is Static IP, the next screen will appear as shown in Figure 3-10.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

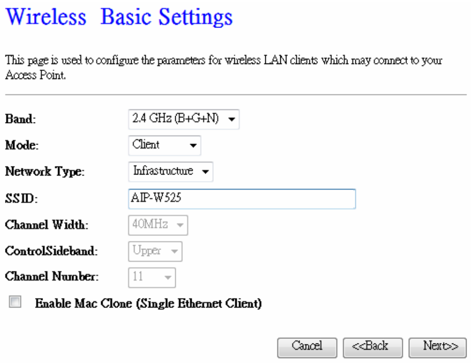
Default Gateway: 0.0.0.0

DNS :

Figure 3-10 Quick Setup - Static IP

- **IP Address -** This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask -** The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.
- **Default Gateway -** Enter the gateway IP address into the box if required.
- **Primary DNS -** Enter the DNS Server IP address into the box if required.

7. Click **Next** to continue, the Wireless settings page will appear as shown in Figure 3-11.



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 (B+G+N)

Mode: Client

Network Type: Infrastructure

SSID: AIP-W525

Channel Width: 40MHz

ControlSideband: Upper

Channel Number: 11

□ Enable Mac Clone (Single Ethernet Client)

Figure 3-11 Quick Setup – Wireless

- **Band**: Keep the default setting: **2.4GHz (B+G+N)**. If you just want to use specific protocol only, please use drop down menu to select it.
- **Mode**: This field determines the wireless mode which the Router works on.
- **Network Type**: Keep the default setting: **Infrastructure**. If you just want to use other operation mode, please use drop down menu to select it.
- **SSID**: Create a unique and easy to remember name for your wireless network. You can also keep default settings without the device being affected.
- **Channel Width -** Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.
- **Channel Number-** This field determines which operating frequency will be used. The default channel is set to Auto. so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

8. Set your security preference then click the **Finished** button.

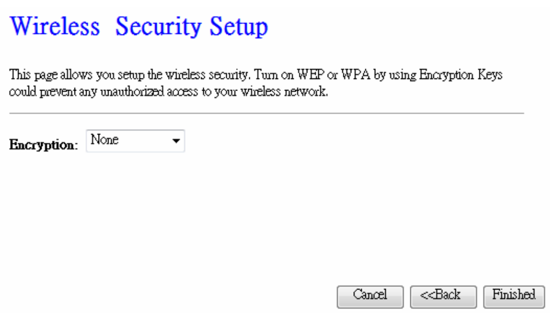
Wireless Security: Recommend to choose **WPA-PSK/WPA2-PSK** and enter a Security Key using ASCII characters between 8 and 63 characters or 64 hexadecimal characters in the **PSK Password** filed. For advanced settings, please refer to Section 4.6: "Wireless".

- **WPA-PSK/WPA2-PSK -** Select WPA based on pre-shared passphrase.
  - **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters.

    For **ASCII**, the key can be made up of any numbers 0 to 9 and any letters A to Z, the length should be between 8 and 63 characters.

    For **Hexadecimal**, the key can be made up of any numbers 0 to 9 and letters A to F, the length should be between 8 and 64 characters.

    Please also note the key is case sensitive, this means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings.



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

Figure 3-12 Quick Setup - Finish

Chapter 4. Configuring the Router

This chapter will show each Web page's key functions and the configuration way.

4.1 Login

After your successful login, you will see the seven main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

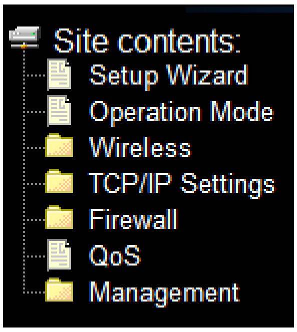
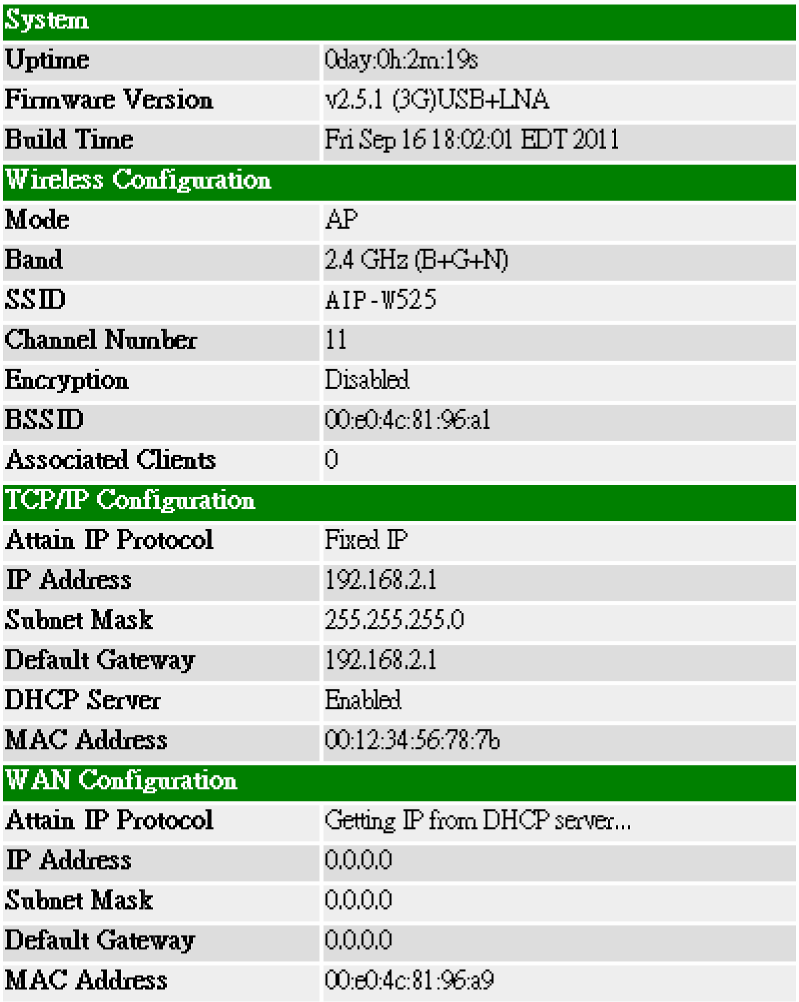


Figure 4-1 the main menu

The detailed explanations for each Web page’s key function are listed below.

4.2 Status

The Status page provides the current status information about the Router. All information is read-only.



System	
Uptime	0day:0h:2m:19s
Firmware Version	v2.5.1 (3G)USB+LNA
Build Time	Fri Sep 16 18:02:01 EDT 2011
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	AIP-W525
Channel Number	11
Encryption	Disabled
BSSID	00:e0:4c:81:96:a1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DHCP Server	Enabled
MAC Address	00:12:34:56:78:7b
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:a9

Figure 4-2 Router Status

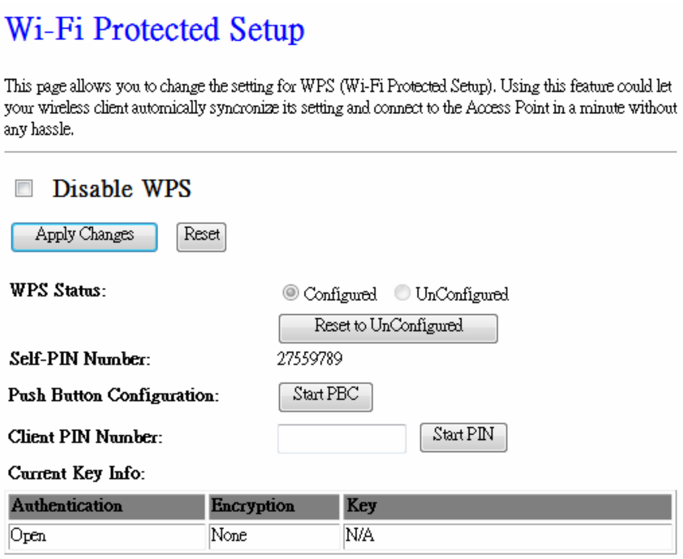
4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide".

4.4 WPS

This section will guide you to add a new wireless device to an existing network quickly by **WPS (Wi-Fi Protect Setup)** function.

a) Choose **WPS** from **Security** menu you will see the next screen (shown in Figure 4-3).



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ Disable WPS

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 27559789

Push Button Configuration:

Client PIN Number:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Figure 4-3 WPS

- **WPS Status -** Configure or Unconfigure the WPS function here.
- **Self-PIN Number -** The current value of the Router's PIN is displayed here.
- **Push Button Configuration –** Push this button to synchronize Router and your wifi adapter
- **Client PIN Number –** To synchronize wifi adapter by entering adapter’s PIN.

b) To add a new device:

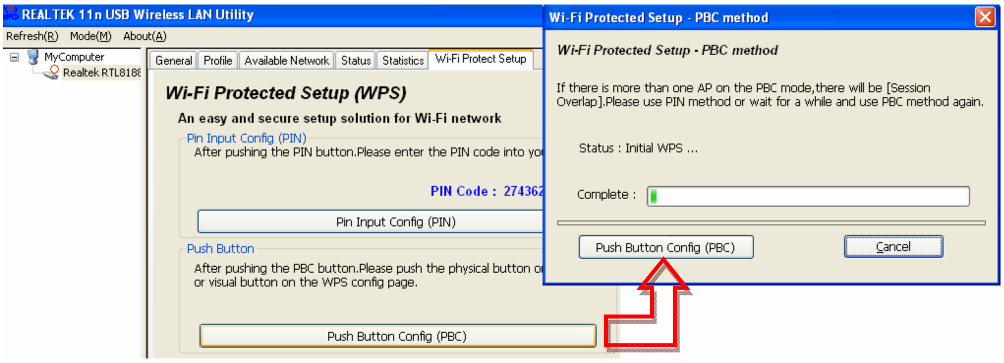
If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method.

☞ **Note:**

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function.

For the configuration of the new device, here takes AWUS036NHR for example.

Step 1: Press **PBC** button from the Wireless LAN Utility then **Wi-Fi Protected Setup – PBC method** pops up and waiting for authentication.



Wi-Fi Protected Setup (WPS)

An easy and secure setup solution for Wi-Fi network

Pin Input Config (PIN)

After pushing the PIN button.Please enter the PIN code into yo

PIN Code : 274362

Push Button

After pushing the PBC button.Please push the physical button o or visual button on the WPS config page.

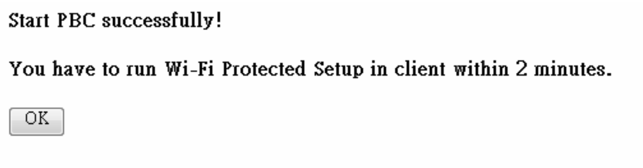
Wi-Fi Protected Setup - PBC method

If there is more than one AP on the PBC mode,there will be [Session Overlap].Please use PIN method or wait for a while and use PBC method again.

Status : Initial WPS ...

Complete :

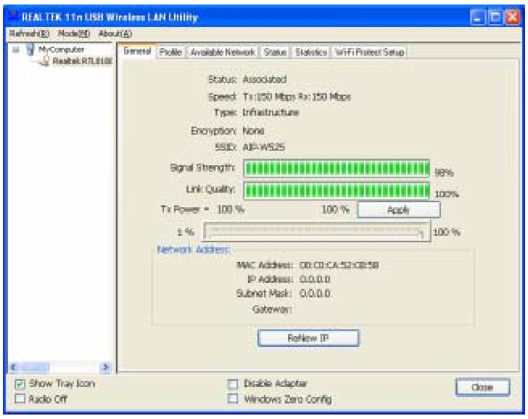
Step 2: Press **Start PBC** button on your Router for authentication.



Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

Step 3: Wait for a minute then you'll discovered your AWUS036NHR is connected to AIP-W525 automatically.



Status: Associated
Speed: Tx:150 Mbps Rx:150 Mbps
Type: Infrastructure
Encryption: None
SSID: AIP-W525
Signal Strength: 98%
Link Quality: 100%
Tx Power = 100 % 100 %
1 % 100 %

Network Address:
MAC Address: 00:C0:CA:52:C8:58
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway:

☑ Show Tray Icon
☐ Radio Off
☐ Disable Adapter
☐ Windows Zero Config

4.5 TCP/IP Settings

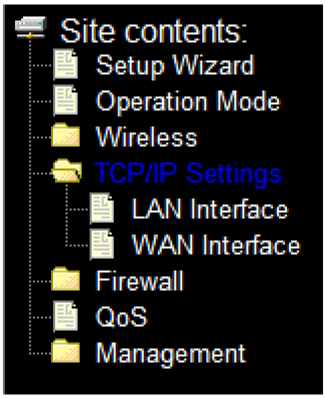
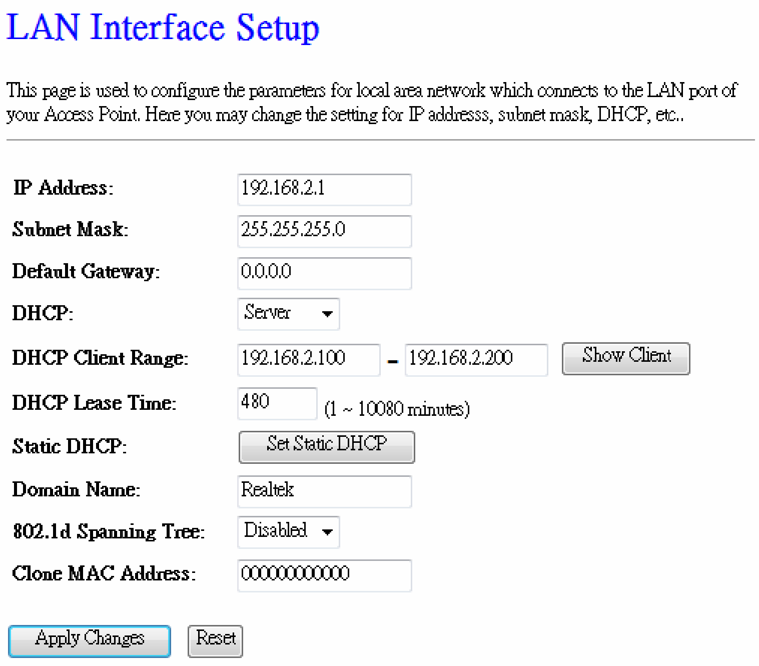


Figure 4-5 the Network menu

There are two submenus under the TCP/IP Settings menu (shown in Figure 4-5): **LAN Interface**, and **WAN** Interface**.** Click any of them, and you will be able to configure the corresponding function.

4.5.1 LAN

Choose menu "**TCP/IP Settings** → **LAN**", you can configure the IP parameters of the LAN on the screen as below.



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:	192.168.2.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.2.100 - 192.168.2.200
DHCP Lease Time:	480 (1 ~ 10080 minutes)
Static DHCP:	Set Static DHCP
Domain Name:	Realtek
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Figure 4-6 LAN Interface

- **IP Address -** Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.2.1).

- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

☞ **Note:**

1. If you change the IP Address of LAN, you must use the new IP Address to log in the Router.
2. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time， while the Virtual Server and DMZ Host will not take effect until they are re-configured.

- **Default Gateway -** Enter the gateway IP address in dotted-decimal notation provided by your system administrator.

- **DHCP** – Select Disabled, Client or Server in different operation mode for AIP-W525H

- **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 automatically.

- **Show Client** – Press button to open the active DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]

- **DHCP Lease Time** – Amount of time the IP address is leased for.

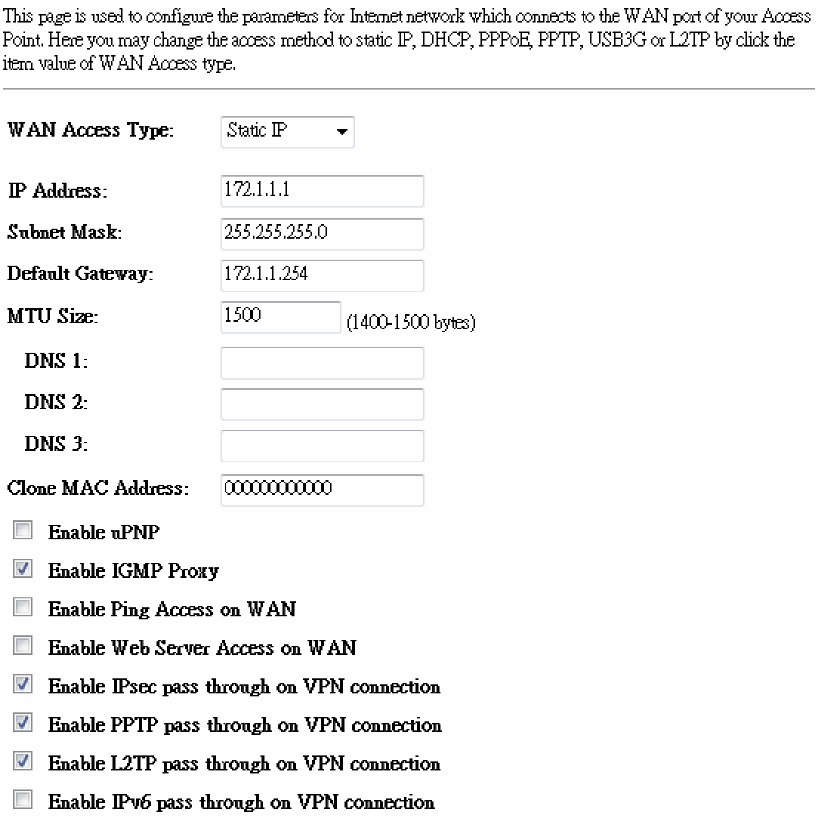
- **Set Static DHCP** - Manual setup Static DHCP IP address for specific MAC address. [Server mode only]

- **Domain Name -** Assign Domain Name and dispatch to DHCP clients [optional]

- **802.1d Spanning Tree** - 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.

4.5.2 WAN Interface

Choose menu “**TCP/IP Settings → WAN**”, you can configure the IP parameters of the WAN on the screen below.



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, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

MTU Size: 1500 (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☐ Enable uPNP

☑ Enable IGMP Proxy

☐ Enable Ping Access on WAN

☐ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

☐ Enable IPv6 pass through on VPN connection

Figure 4-7 WAN – Static IP

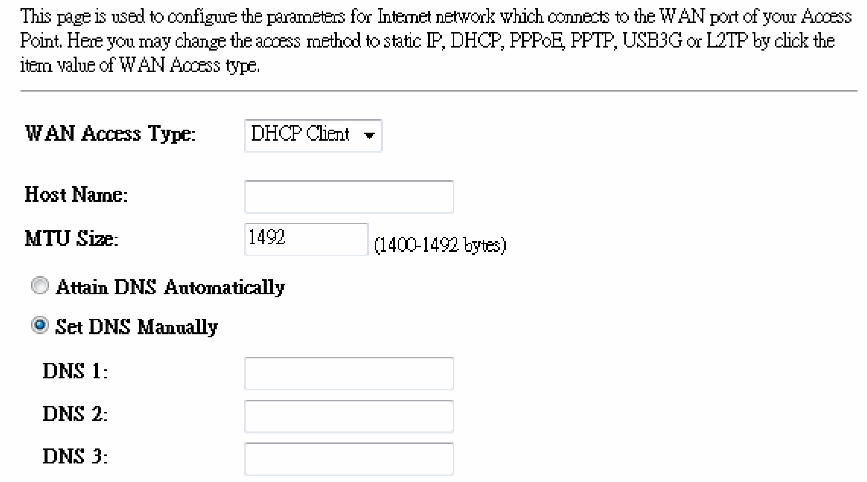
- **Clone MAC Address** - Fill in the MAC address that is the MAC address to be cloned
- **Enable uPNP** - Click the checkbox to enable uPNP function.
- **Enable IGMP Proxy** - Click the checkbox to enable IGMP proxy
- **Enable Ping Access on WAN** - Click the checkbox to enable WAN IGMP response.
- **Enable Web server Access on WAN** - Click the checkbox to enable web configuration from
- **Enable IPsec pass through on VPN connection** - Click the checkbox to enable IPSec packet pass through
- **Enable PPTP pass through on VPN connection** - Click the checkbox to enable PPTP packet pass through
- **Enable L2TP pass through on VPN connection** - Click the checkbox to enable L2TP packet pass through

1. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-7.

   - **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
   - **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
   - **Default Gateway -** (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
   - **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
   - **DNS 1 / DNS 2 / DNS 3 -** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

   Click the **Apply Changes** button to save your settings.

2. If your ISP provides the DHCP service, please choose **DHCP Client** type, and the Router will automatically get IP parameters from your ISP (shown in Figure 4-8).



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, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client ▾

Host Name:

MTU Size: 1492 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

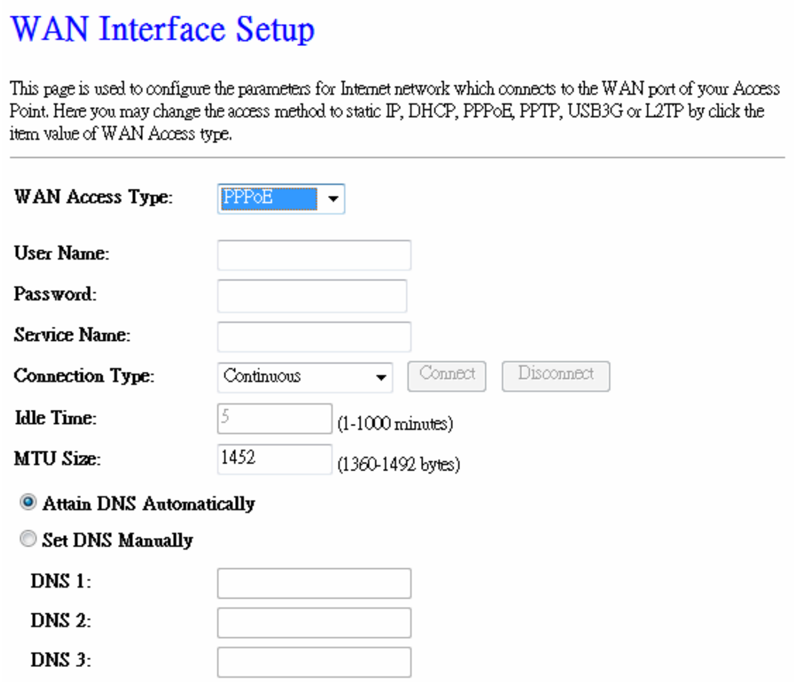
Figure 4-8 WAN – Dynamic IP

- **Host Name** – Enter the host name provided by your ISP, default value is blank.
- **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Attain DNS Automatically** – Receives DNS address automatically from the ISP.
- **Set DNS Manually -** If your ISP gives you one or two DNS addresses, select **Set DNS Manually** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

☞ **Note:**

If you find error when you go to a website after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

3. If your ISP provides a PPPoE connection, select **PPPoE** option. And you should enter the following parameters (Figure 4-9):



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, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:	PPPoE
User Name:	
Password:	
Service Name:	
Connection Type:	Continuous
Idle Time:	5 (1-1000 minutes)
MTU Size:	1452 (1360-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	

Figure 4-9 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Service Name -** The service name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **Connection Type**
  - **Continuous –** Continuous connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband Router is powered on.
  - **Connect on Demand –** In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again.
  - **Manual -** You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a

specified inactivity period and re-established when you attempt to access the Internet again.

Caution: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

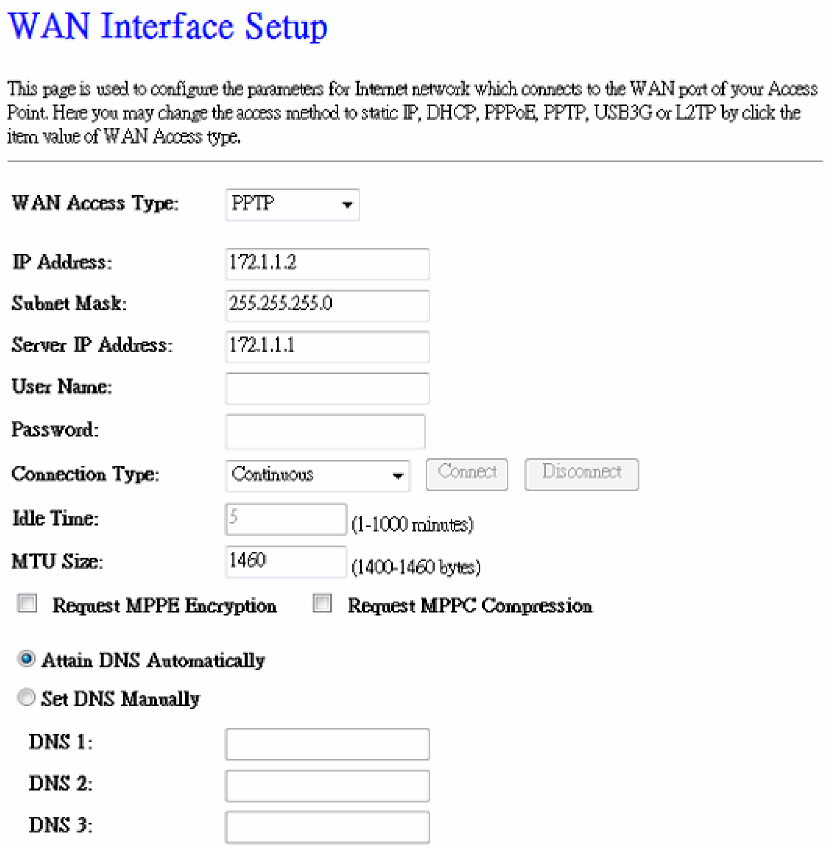
- **Idle Time -** If you want your Internet connection keeps active all the time, please enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **MTU Size -** The default MTU size is “1480” bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Attain DNS Automatically** – Receives DNS address automatically from the ISP.
- **Set DNS Manually -** If your ISP gives you one or two DNS addresses, select **Set DNS Manually** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

☞ **Note:**

If you find error when you go to a website after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Click the **Apply Changes** button to save your settings.

4. If your ISP provides PPTP connection, please select **PPTP** option. And you should enter the following parameters (Figure 4-11):



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, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:	PPTP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
Connection Type:	Continuous
Idle Time:	5 (1-1000 minutes)
MTU Size:	1460 (1400-1460 bytes)

□ Request MPPE Encryption □ Request MPPC Compression

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	

Figure 4-11 L2TP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

  If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

  Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand -** You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

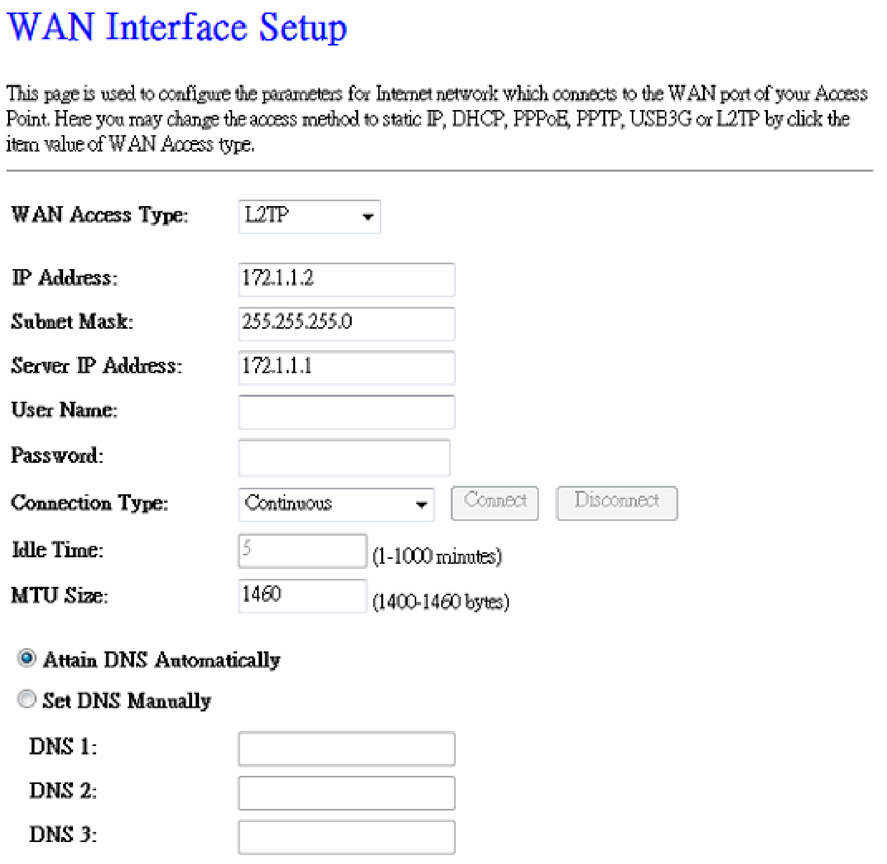
- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check the radio button.

- **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

5. If your ISP provides L2TP connection, please select **L2TP** option. And you should enter the following parameters (Figure 4-12):



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, PPTP, USB3G or L2TP by click the item value of WAN Access type.

WAN Access Type:	L2TP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
Connection Type:	Continuous [Connect] [Disconnect]
Idle Time:	5 (1-1000 minutes)
MTU Size:	1460 (1400-1460 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	

Figure 4-12 L2TP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand -** You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check the radio button.
- **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

☞ **Note:**

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE -** Connections which use PPPoE that requires a user name and password.
- **Dynamic IP -** Connections which use dynamic IP address assignment.
- **Static IP -** Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.6 Wireless

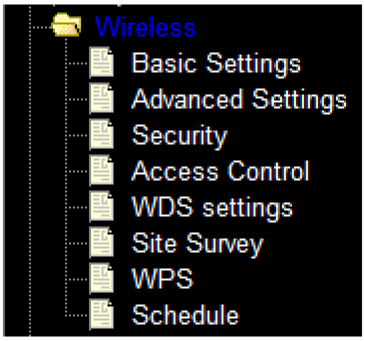
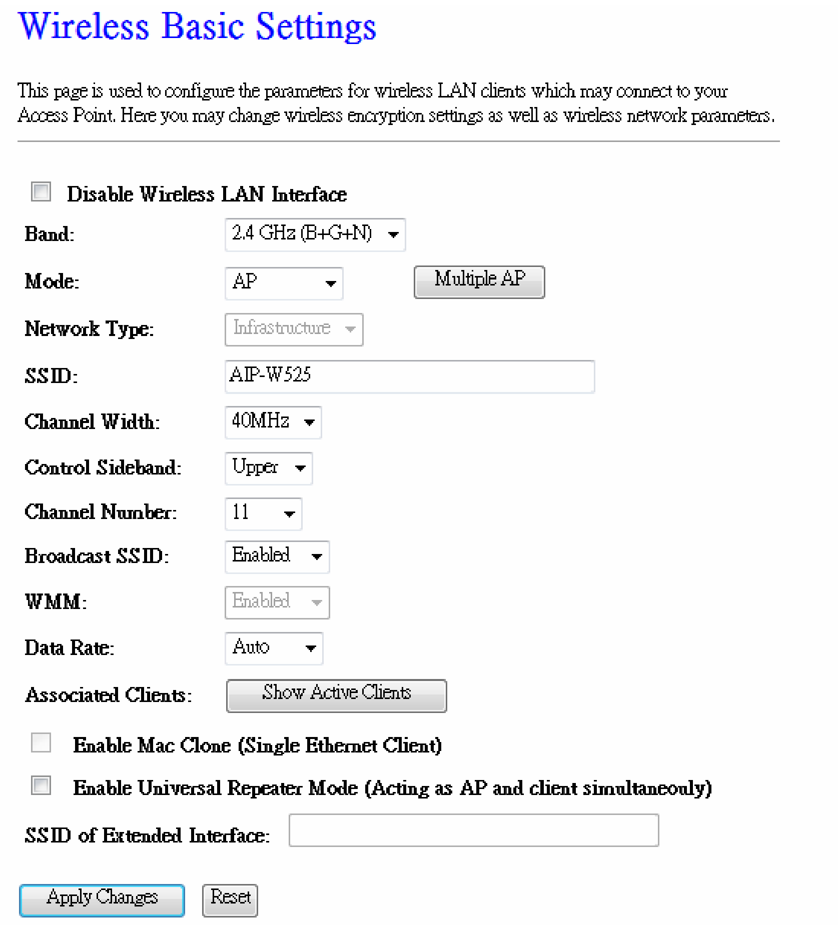


Figure 4-15 Wireless menu

There are eight submenus under the Wireless menu (shown in Figure 4-15): **Basic Settings**, **Advanced Settings**, **Security, Access Control, WDS Setting, Site Survey, WPS,** and **Schedule.** Click any of them, and you will be able to configure the corresponding function.

4.6.1 Basic Settings

Choose menu "**Wireless** → **Basic Settings**", you can configure the basic settings for the wireless network on this page.



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 (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	AIP-W525
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Figure 4-16 Wireless Settings

- **Band -** Select the desired protocol. The default setting is 2.4GHz (B+G+N).

  2.4GHz (B) - Select if all of your wireless clients are 802.11b.

  2.4GHZ (G) - Select if all of your wireless clients are 802.11g.

  2.4GHz (N) - Select only if all of your wireless clients are 802.11n.

  2.4GHz (B+G) - Select if you are using both 802.11b and 802.11g wireless clients.

  2.4GHz (G+N) - Select if you are using both 802.11g and 802.11n wireless clients.

  2.4GHz (B+G+N) – Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

- **Mode -** Select the desired wireless mode. AIP-W525H PowerMax 2 offers AP, Client, WDS, and AP + WDS. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to **2.4GHz (B+G+N)** and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

- **Network Type -** After network mode is selected to be "Client" then you need to set network type as infrastructure or Ad-Hoc.

- **SSID -** Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

- **Channel width -** Select the channel width from the pull-down list. The default setting is 40MHz.

  ☞ **Note:**

  If **2.4GHz (B)**, **2.4GHz (G)**, or **2.4GHz (B+G)** is selected in the **Mode** field, the **Channel Width** selecting field will be disappeared and the value will become 20M, which is unable to be changed.

- **Control Sideband –** Select the sideband with upper or lower for channel width 40MHz.

- **Channel Number-** This field determines which operating frequency will be used. The default channel is CH11. And you can set to Auto so the AP will choose the best channel automatically, it is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Broadcast SSID -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the **Enable** for **Broadcast SSID** then Router will broadcast its name (SSID) on the air.

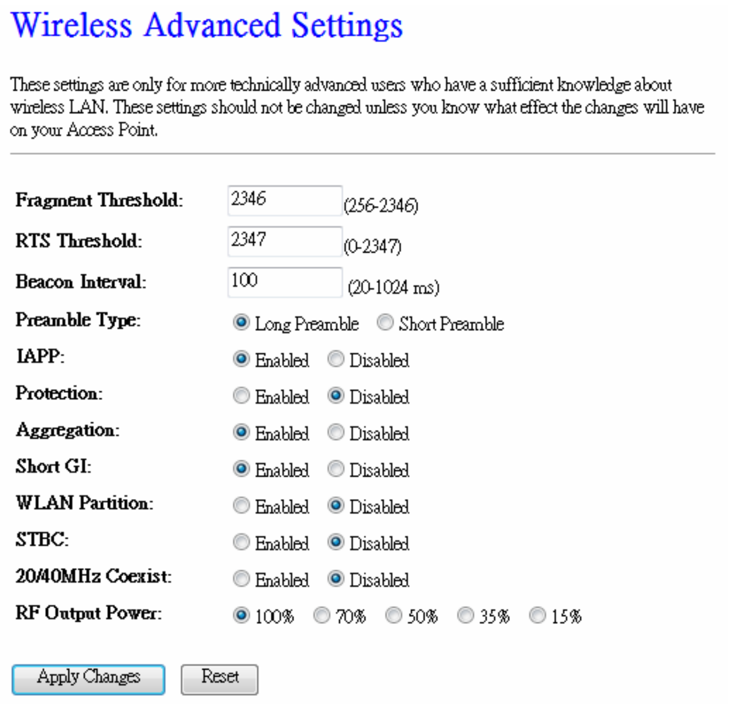
- **WMM –** Click on Enable or Disable Wireless Multimedia (WMM).

- **Data Rate -** Select transmission data rate from pull-down menu. Data rate can be auto select, 1M to 54Mbps or MCS. The default option is AUTO.

- **Associate Clients –** Click **Show Active Clients** 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) –** Copy your system's NIC MAC address as wireless client's MAC address and this function is only work if **Client** mode is selected.
- **Enable Universal Repeater Mode –** Check to enable Universal Repeater Mode where Router acting as AP and client simultaneously in this mode).
- **SSID for Extended Interface** – Assign a SSID when Universal Repeater Mode is enabled.

4.6.2 Advanced Settings

Choose menu "**Wireless → Security**", you can configure the security settings of your wireless network.



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.

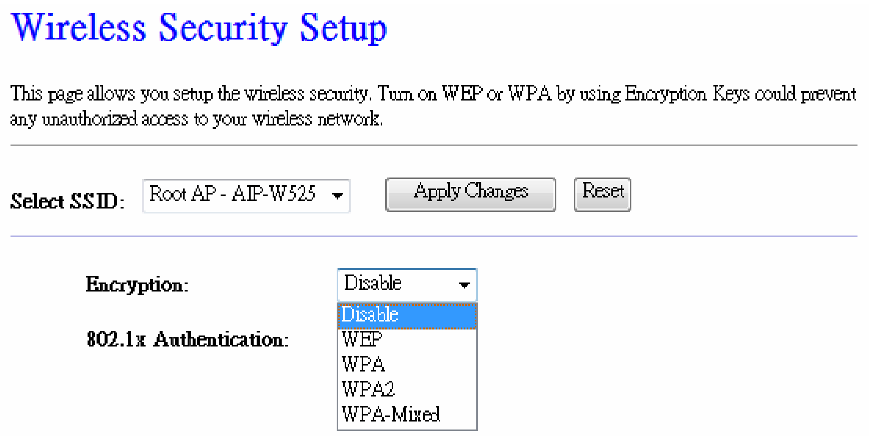
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Preamble Type:	● Long Preamble ○ Short Preamble
IAPP:	● Enabled ○ Disabled
Protection:	○ Enabled ● Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WLAN Partition:	○ Enabled ● Disabled
STBC:	○ Enabled ● Disabled
20/40MHz Coexist:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 70% ○ 50% ○ 35% ○ 15%

- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Beacon Interval -** Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.

4.6.3 Security

Choose menu "**Wireless → Security**", you can configure the security settings of your wireless network.

There are four wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA-Mixed (Pre-Shared Key or Enterprise).



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.

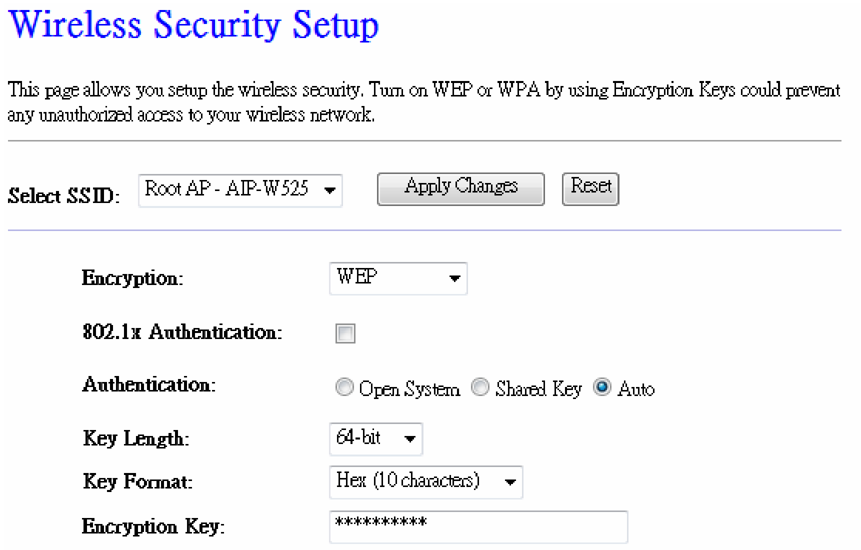
Select SSID: Root AP - AIP-W525

Encryption: Disable

802.1x Authentication:

Figure 4-18 Wireless Security

- **Disable -** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the following modes to enable security.
- **WEP -** It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as show in Figure 4-19.



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.

Select SSID: Root AP - AIP-W525

Encryption: WEP

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: **********

Figure 4-19

- **802.1x Authentication –** Check to enable 802.1x authentication via RADIUS server.

- **Authentication -** you can choose the type for the WEP security on the pull-down list. The default setting is **Auto**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **Key Length -** You can select the WEP key length (64-bit, or 128-bit) for encryption.

  64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

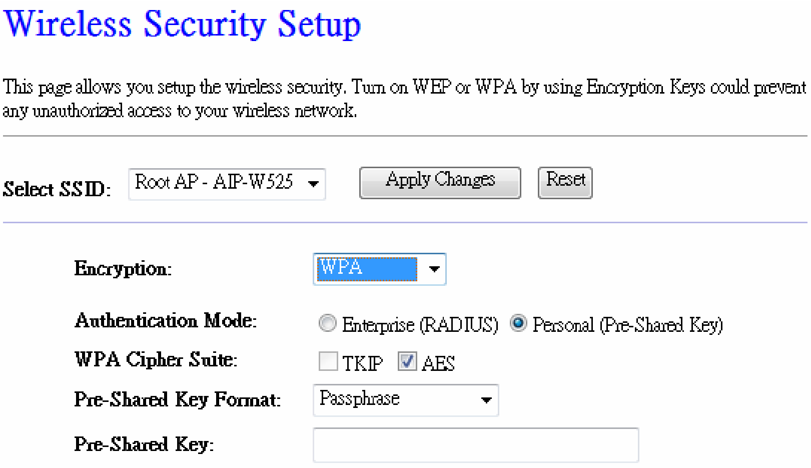
  128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

  ☞ **Note:**

  If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.
- **Key Format - Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **Encryption Key -** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Radius Server IP Address -** Enter the IP address of the Radius server, if **802.1x Authentication** is selected.
- **Radius Server Port -** Enter the port number of the Radius server, if **802.1x Authentication** is selected.
- **Radius Server Password -** Enter the password for the Radius server, if **802.1x Authentication** is selected.

Be sure to click the **Apply Changes** button to save your settings on this page

➢ **WPA -** It's the WPA authentication type based on pre-shared passphrase or RADIUS server.



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.

Select SSID: Root AP - AIP-W525 ▾ | Apply Changes | Reset

Encryption: WPA ▾

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

WPA Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase ▾

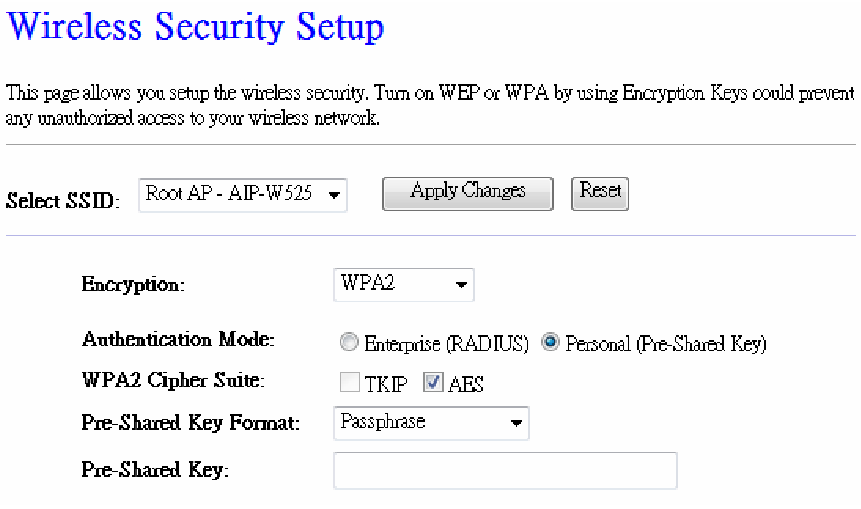
Pre-Shared Key:

Figure 4-20

- **Authentication Mode -** you can choose the either **Enterprise (RADIUS)** or **Personal (Pre-Shared Key)**. The default setting is **Personal (Pre-Share Key)**, it's a passphrase between 8 and 63 characters. **Enterprise (RADIUS),** it's an authentication via RADIUS server.
- **WPA Cipher Suite -** When **WPA** is set as the Authentication Type, you can select **TKIP** or **AES** or AUTO if both encryption is checked.
- **Pre-Shared Key Format -** You can enter chose either **Passphrase** (8 ~ 63 characters) or **HEX(64 Characters)**.
- **Pre-Shared Key -** Enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Radius Server IP Address -** Enter the IP address of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Port -** Enter the port number of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Password -** Enter the password for the Radius server, if **Enterprise (RADIUS)** is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

➢ **WPA2 -** It's the WPA2 authentication type based on pre-shared passphrase or RADIUS server.



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.

Select SSID: Root AP - AIP-W525

Encryption: WPA2

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

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

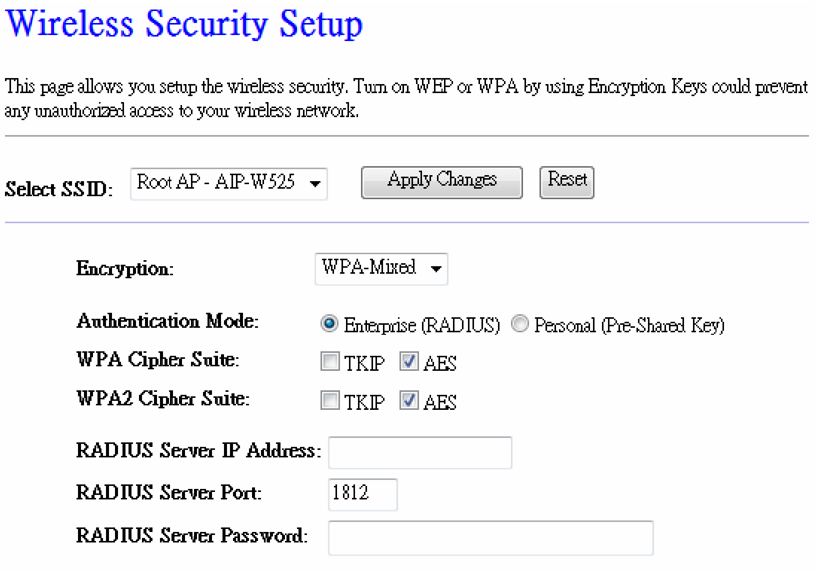
Figure 4-21

- **Authentication Mode -** you can choose the either **Enterprise (RADIUS)** or **Personal (Pre-Shared Key)**. The default setting is **Personal (Pre-Share Key)**, it's a passphrase between 8 and 63 characters. **Enterprise (RADIUS),** it's an authentication via RADIUS server.

- **WPA2 Cipher Suite -** When **WPA2** is set as the Authentication Type, you can select **TKIP** or **AES** or AUTO if both encryption is checked..
- **Pre-Shared Key Format -** You can enter chose either **Passphrase** (8 ~ 63 characters) or **HEX(64 Characters)**.
- **Pre-Shared Key -** Enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Radius Server IP Address -** Enter the IP address of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Port -** Enter the port number of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Password -** Enter the password for the Radius server, if **Enterprise (RADIUS)** is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

➢ **WPA-Mixed -** It's the WPA/WPA2 authentication type based on pre-shared passphrase or RADIUS server.



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.

Select SSID: Root AP - AIP-W525

Encryption: WPA-Mixed

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

WPA Cipher Suite: □ TKIP ☑ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

Figure 4-22

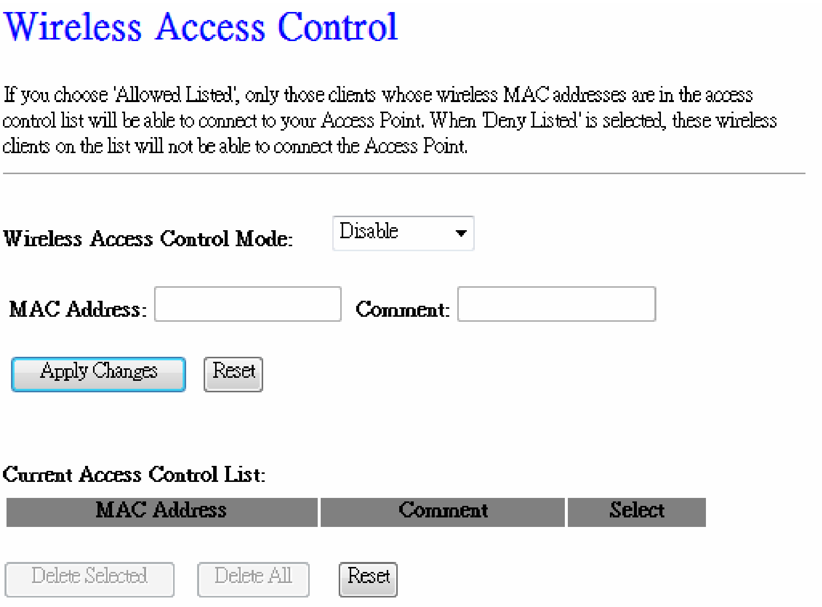
- **Authentication Mode -** you can choose the either **Enterprise (RADIUS)** or **Personal (Pre-Shared Key)**. The default setting is **Personal (Pre-Share Key)**, it's a passphrase between 8 and 63 characters. **Enterprise (RADIUS),** it's an authentication via RADIUS server.
- **WPA Cipher Suite -** When **WPA** is set as the Authentication Type, you can select either **TKIP** or **AES** as Encryption.
- **WPA2 Cipher Suite -** When **WPA2** is set as the Authentication Type, you can select either **TKIP** or **AES** as Encryption.

- **Pre-Shared Key Format -** You can enter chose either **Passphrase** (8 ~ 63 characters) or **HEX(64 Characters)**.
- **Pre-Shared Key -** Enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Radius Server IP Address -** Enter the IP address of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Port -** Enter the port number of the Radius server, if **Enterprise (RADIUS)** is selected.
- **Radius Server Password -** Enter the password for the Radius server, if **Enterprise (RADIUS)** is selected.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.6.4 Access Control

Choose menu "**Wireless → Access Control**", you can control the wireless access by configuring the **Wireless Access Control** function, shown in Figure 4-23.



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: Disable

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select

Figure 4-23 Wireless Access Control

To allow wireless users by MAC Address, click **Allow Listed,** or prohibited wireless users by MAC Address by click **Deny Listed**. The default setting is **Disable**.

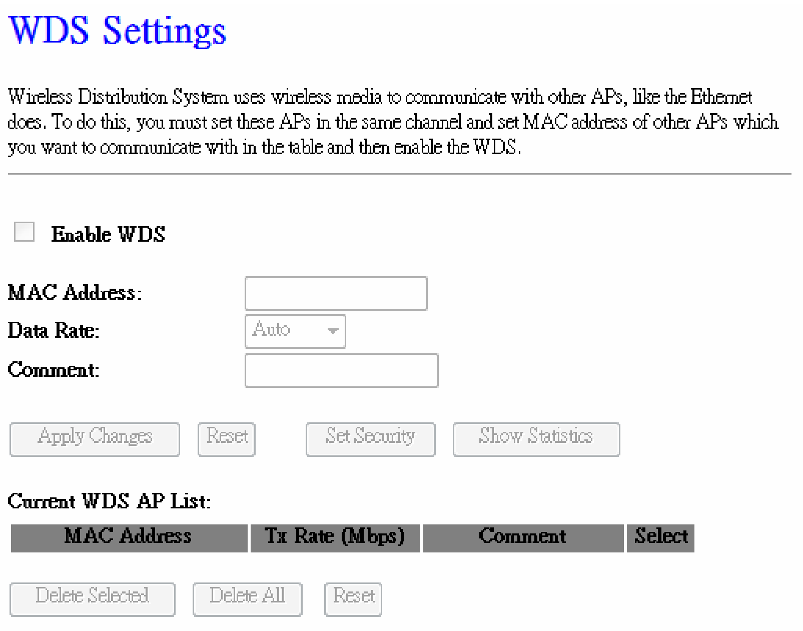
- **MAC Address -** The wireless station's MAC address that you want to filter.
- **Comment -** A simple description of the wireless station.

Be sure to click the **Apply Changes** button to save your settings on this page

- **Current Access Control List -** Displays the registered clients that are allowed to link to this WLAN Broadband Router.

4.6.5 WDS Settings

Choose menu “**Wireless → WDS Settings**”, you can configure the advanced settings of your wireless network.



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

MAC Address:	
Data Rate:	Auto
Comment:	

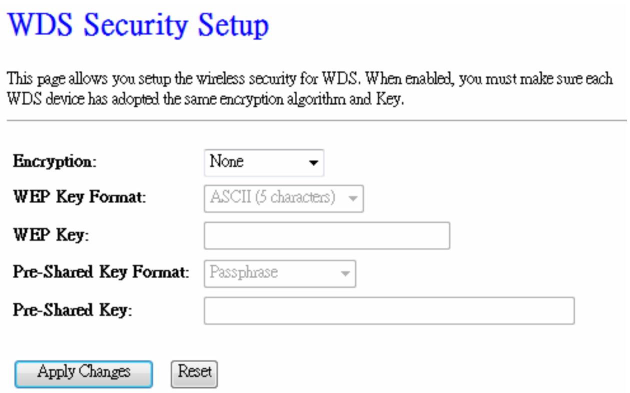
Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select

Figure 4-24 Wireless Advanced

To add wireless AP by MAC Address, click **Enable WDS**.

- **MAC Address -** The wireless station's MAC address that you want to add.
- **Data Rate -** Select transmission data rate from drop down menu. Data rate can be auto-selected, 1Mbps to 54Mbps or MCS.
- **Set Security** - There are two wireless security modes supported by the WDS: WEP (Wired Equivalent Privacy), and WPA2 (Wi-Fi Protected Access 2).



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:	None
WEP Key Format:	ASCII (5 characters)
WEP Key:	
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

- Encryption – Use drop down menu to configure WDS security, you can select it from **None**, **WEP 64-bits**, **WEP 128-bits**, or **WPA2 (AES)**.
- **WEP Key Format** – **Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length. **64-bit -** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters. **128-bit -** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.
- **Encryption Key -** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your WDS network
- **Pre-Shared Key Format -** You can enter chose either **Passphrase** (8 ~ 63 characters) or **HEX(64 Characters)**.
- **Pre-Shared Key -** Enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your WDS network

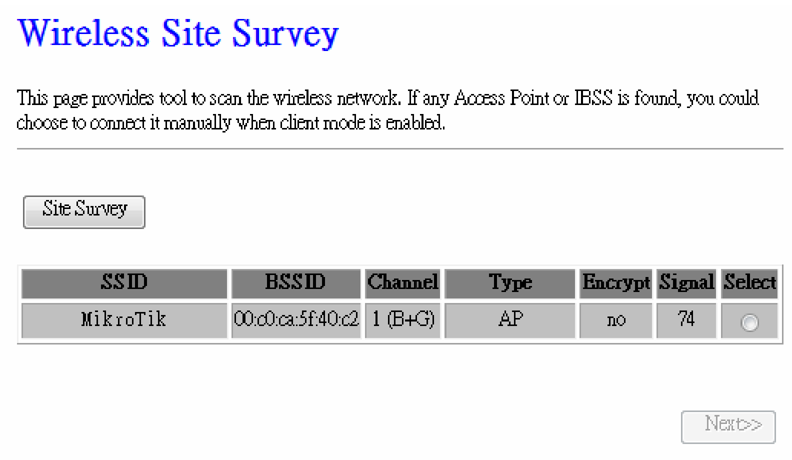
Comment - A simple description of the wireless station.

Be sure to click the **Apply Changes** button to save your settings on this page

Current WDS AP List - Displays the registered APs that are allowed to link to this WLAN Broadband Router.

4.6.6 Site Survey

Choose menu "**Wireless** → **Site Survey**", you scan and connect nearby APs when operate at client mode.



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.

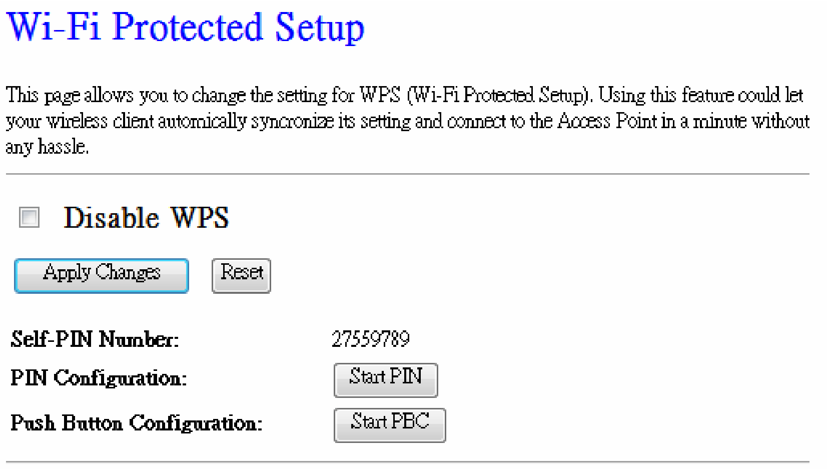
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
MikroTik	00:c0:ca:5f:40:c2	1 (B+G)	AP	no	74	○

- **SSID(to be WDS)** - The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.

- **BSSID(to be WDS)** - The BSSID of the AP your Router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Channel -** This field displayed operating frequency of the AP your Router is going to connect to as a client.
- **Type –** Type of the AP your Router is going to connect to as a client, AP or AD-HOC.
- **Encryption –** Shows encryption type of the AP your Router is going to connect to as a client.
- **Signal –** Shows the signal strength of the AP your Router is going to connect to as a client.

4.6.7 WPS

Choose menu "**Wireless** → **WPS**", where you to add a new wireless device to an existing network quickly.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

Self-PIN Number: 27559789

PIN Configuration: Start PIN

Push Button Configuration: Start PBC

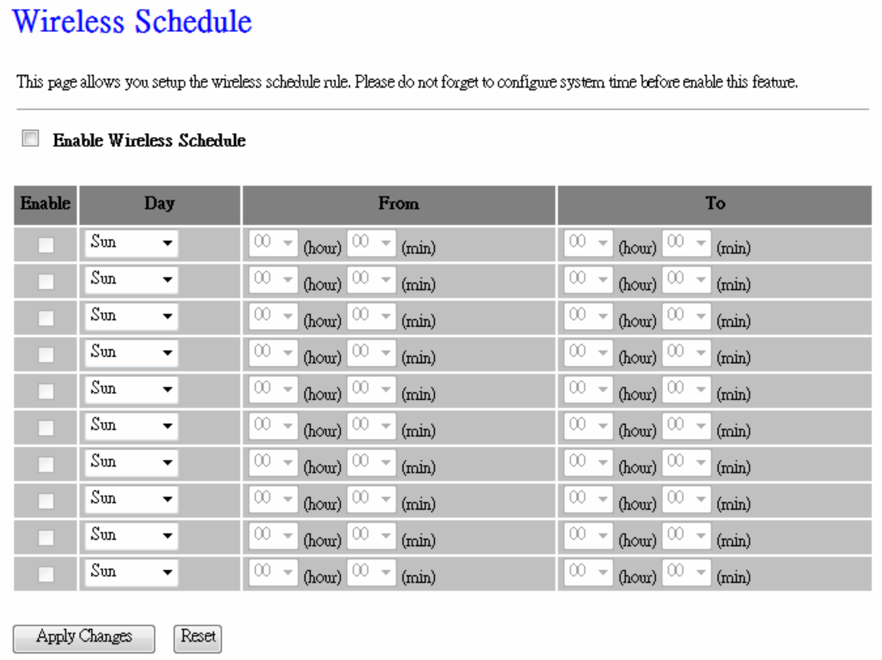
- **Self-PIN Number -** The current value of the Router's PIN is displayed here.
- **PIN Configuration -** You will need to enter **Self-PIN Number** into adapter's configuration utility or on the adapter itself. Press the **Start PIN** button on the router and on the adapter.

  Note: You will have two minutes to push the PIN button on the router and device(s) you want to connect.
- **Push Button Configuration -** You will need an adapter that supports it via a utility or on the adapter itself. Press the **Start PBC** button on the router and on the adapter.

  Note: You will have two minutes to push the PIN button on the router and device(s) you want to connect.

4.6.8 Schedule

Choose menu "**Wireless → Schedule**", time period allowed for the PC controlled to access the Internet.



Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

□ Enable Wireless Schedule

Enable	Day	From	To
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)

Figure 4-25 Schedule

4.7 Firewall

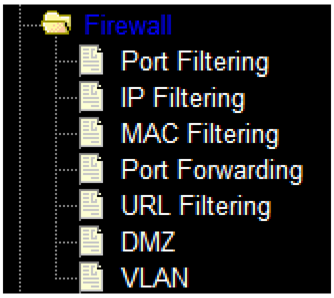
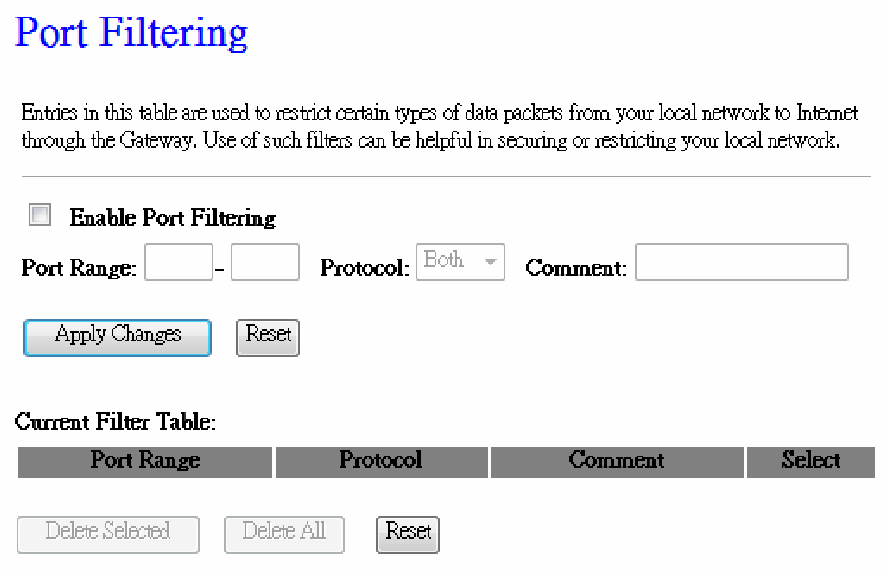


Figure 4-26 The Firewall menu

There are seven submenus under the Firewall menu (shown in Figure 4-26), **Port Filtering, IP Filtering, MAC Filtering, Port Forwarding, URL Filtering, DMZ, and VLAN.** Click any of them, and you will be able to configure the corresponding function.

4.7.1 Port Filtering

Choose menu "**Firewall → Port Filtering**", you can control the wireless access by configuring the **Port Filtering** function as shown in Figure 4-27.



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

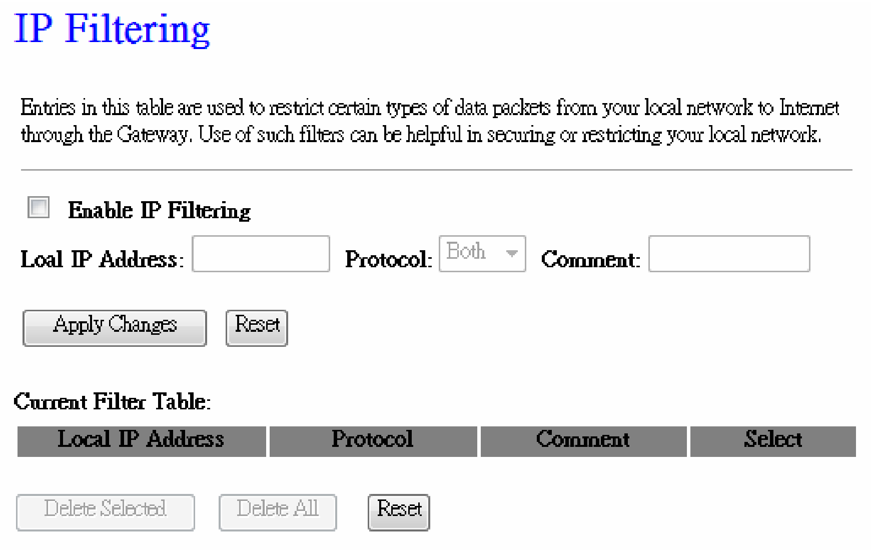
Figure 4-27 Port Filtering

- **Enable Port Filtering –** Check to **Enable** port filtering feature.
- **Port Range / Protocol / Comment -** Specify the port range from start-port to end-port and put your comment to remind you why you have restriction on these ports. You can restricted TCP, UDP, or both protocol.

Be sure to click the **Apply Changes** button to save your settings on this page

4.7.2 IP Filtering

Choose menu "**Firewall → IP Filtering**", you can control the wireless access by configuring the **IP Filtering** function as shown in Figure 4-28.



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

Loal IP Address: [ ] Protocol: Both Comment: [ ]

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Figure 4-28 IP Filtering

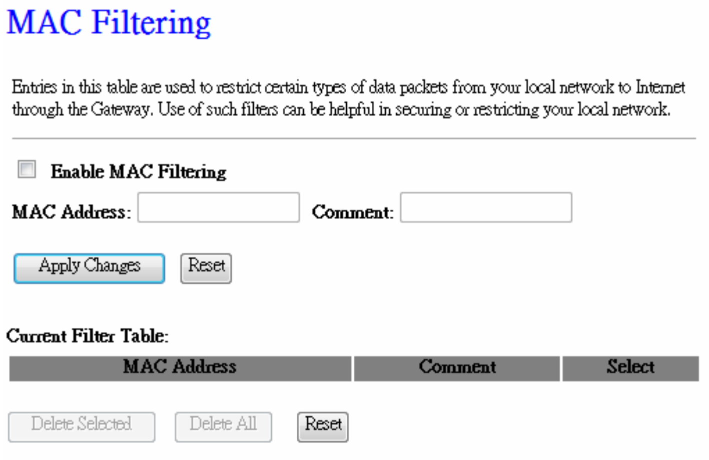
- **Enable IP Filtering –** Check to **Enable** IP filtering feature.

- **Local IP Address / Protocol / Comment -** Specify the local IP address that you wish to put restriction and mark your comment to remind you why you have restriction on this IP address. You can restrict the traffic from TCP, UDP, or both protocol.

Be sure to click the **Apply Changes** button to save your settings on this page

4.7.3 MAC Filtering

Choose menu "**Firewall → MAC Filtering**", you can control the wireless access by configuring the **MAC Filtering** function as shown in Figure 4-29.



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

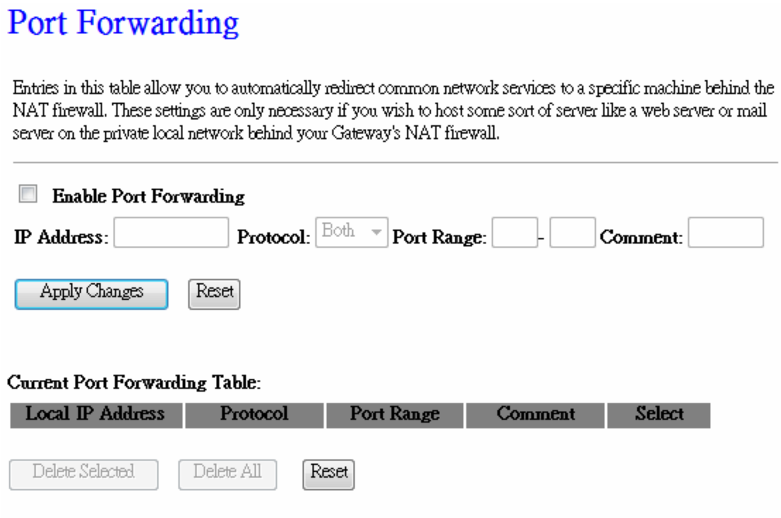
Figure 4-29 MAC Filtering

- **Enable MAC Filtering –** Check to **Enable** MAC filtering feature.
- **MAC Address -** The wireless station's MAC address that you want to filter.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.7.4 Port Forwarding

Choose menu "**Firewall → Port Forwarding**", you can redirect the network traffic by configuring the **Port Forwarding** function as shown in Figure 4-30.



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

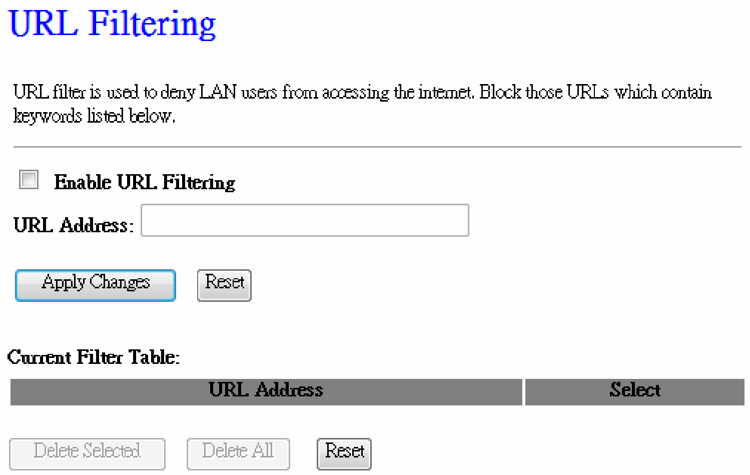
Figure 4-30 MAC Filtering

- **Enable Port Forwarding –** Check to **Enable** port forwarding feature.
- **IP Address –** Forward data packets to specific IP address in your local area network.
- **Protocol -** The protocol used for forwarding data packets, either **TCP** or **UDP**, or **BOTH**
- **Port Range -** The port range used by the remote system when it responds to the forwarding request. A response using one of these ports will be forwarded to the PC that triggered this rule.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.7.5 URL Filtering

Choose menu "**Firewall → URL Filtering**", you can restrict user to access specific web page by configuring the **URL Filtering** function as shown in Figure 4-31.



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

□ Enable URL Filtering

URL Address:

Current Filter Table:

URL Address	Select

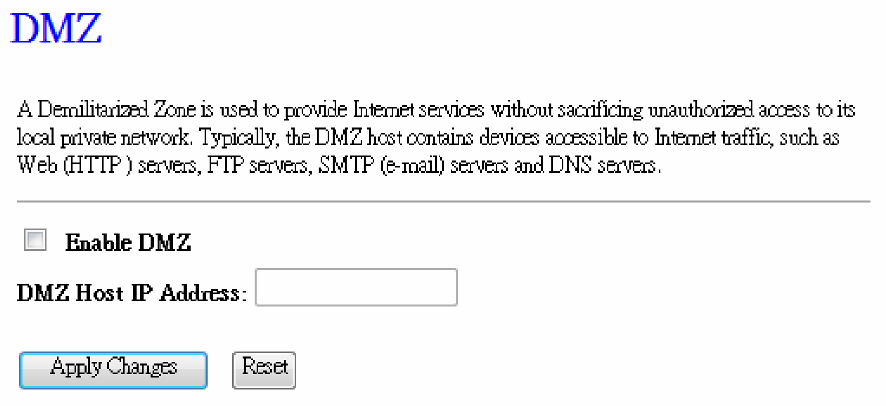
Figure 4-31 URL Filtering

- **Enable URL Filtering –** Check to **Enable** URL filtering feature.
- **URL Address -** The address that you want to restrict user to access.

Be sure to click the **Apply Changes** button to save your settings on this page.

4.7.6 DMZ

Choose menu "**Firewall** → **DMZ**", you can view and configure DMZ host in the screen as shown in Figure 4-32. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.



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.

□ Enable DMZ

DMZ Host IP Address:

Figure 4-32 DMZ

To assign a computer or server to be a DMZ server:

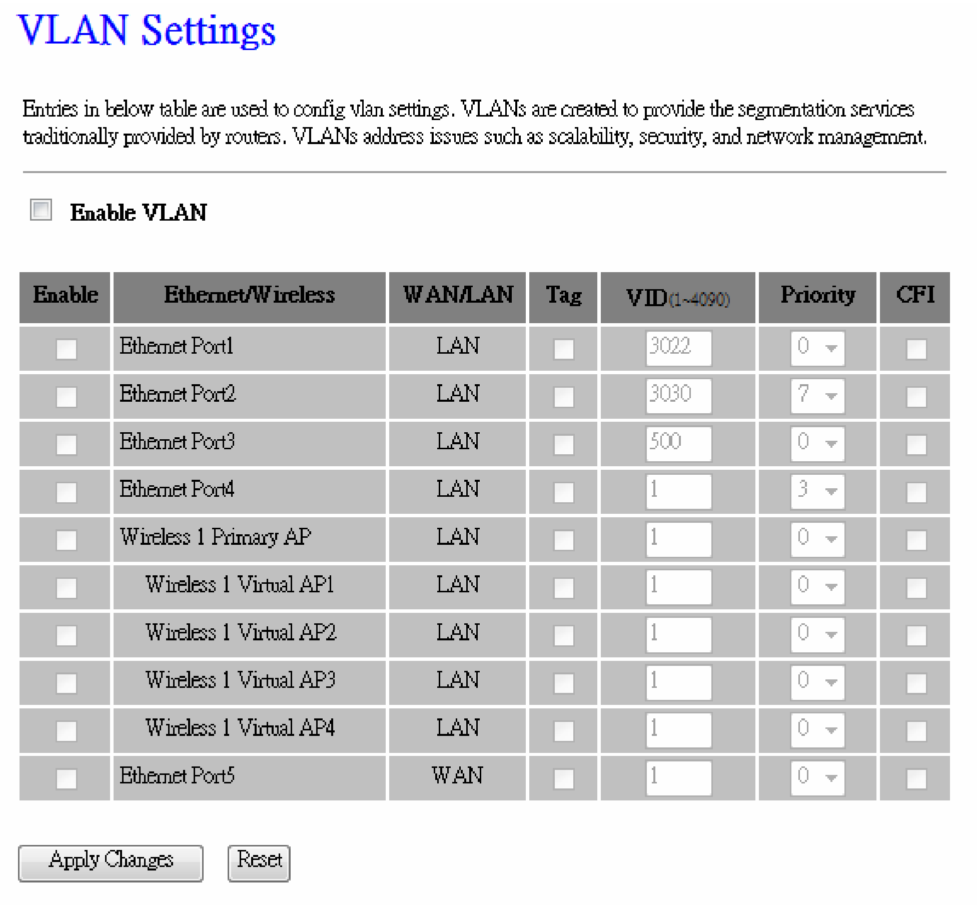
1. Check the **Enable DMZ** checkbox.
2. Enter the IP Address of a local host in the **DMZ Host IP Address** field.
3. Click the **Apply Changes** button.

☞ **Note:**

After you set the DMZ host, the firewall related to the host will not work.

4.7.7 VLAN

Choose menu "**Firewall** → **VLAN**", if you want to configure the Guest and Internal networks on VLAN, the switch you are using must support VLAN. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard, and enable this field as shown in Figure 4-33.



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

□ Enable VLAN

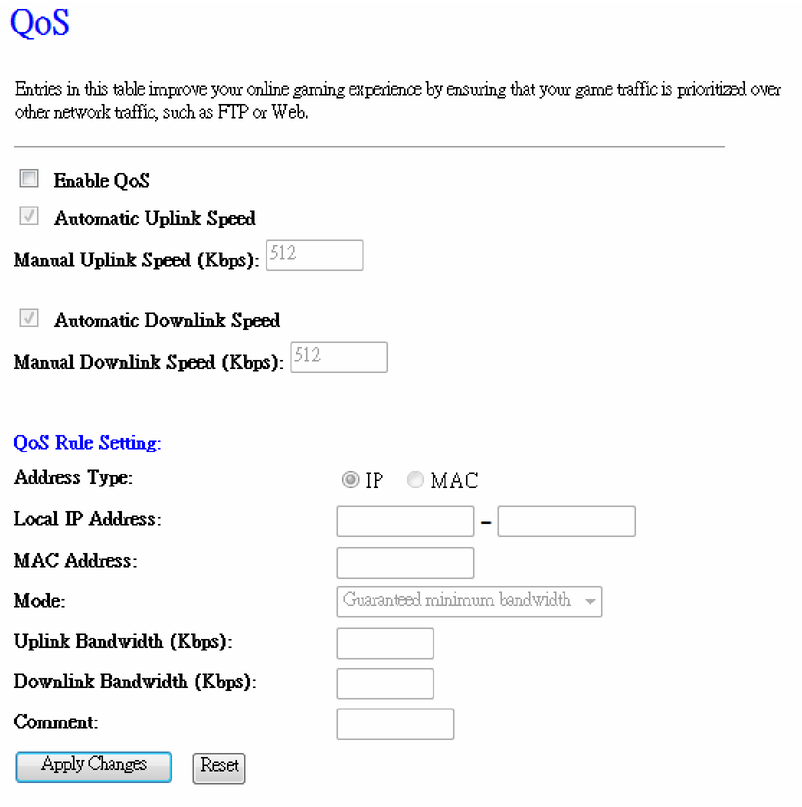
Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
□	Ethernet Port1	LAN	□	3022	0	□
□	Ethernet Port2	LAN	□	3030	7	□
□	Ethernet Port3	LAN	□	500	0	□
□	Ethernet Port4	LAN	□	1	3	□
□	Wireless 1 Primary AP	LAN	□	1	0	□
□	Wireless 1 Virtual AP1	LAN	□	1	0	□
□	Wireless 1 Virtual AP2	LAN	□	1	0	□
□	Wireless 1 Virtual AP3	LAN	□	1	0	□
□	Wireless 1 Virtual AP4	LAN	□	1	0	□
□	Ethernet Port5	WAN	□	1	0	□

Figure 4-33 VLAN

➢

Be sure to click the **Apply Changes** button to save your settings on this page.

4.8 QoS



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

☐ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 512

QoS Rule Setting:

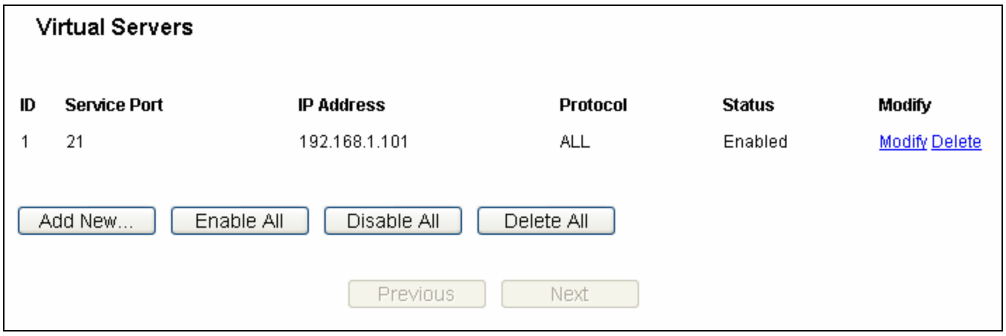
Address Type:	● IP ○ MAC
Local IP Address:	-
MAC Address:	
Mode:	Guaranteed minimum bandwidth
Uplink Bandwidth (Kbps):	
Downlink Bandwidth (Kbps):	
Comment:	

Figure 4-34 The QoS menu

There are four submenus under the Forwarding menu (shown in Figure 4-31): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Virtual Servers

Choose menu "**Forwarding** → **Virtual Servers**", you can view and add virtual servers in the screen as shown in Figure 4-32. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.



Virtual Servers

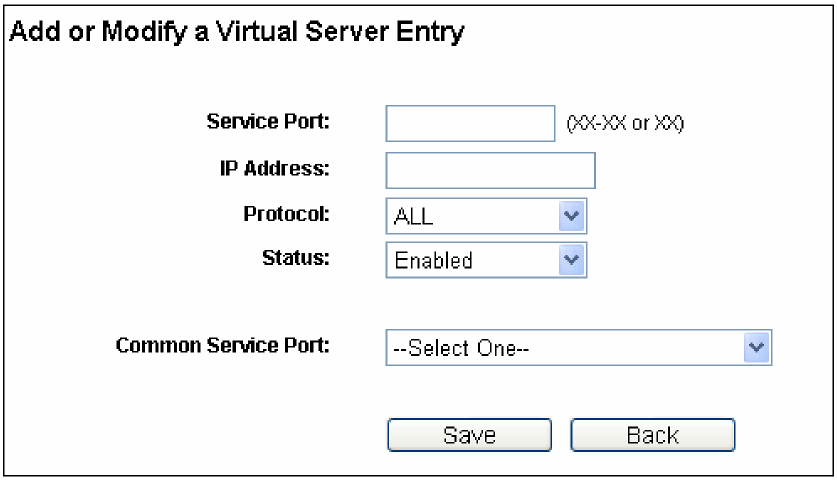
ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	ALL	Enabled	Modify Delete

Figure 4-32 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **IP Address -** The IP Address of the PC providing the service application.
- **Protocol -** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
- **Status -** The status of this entry, either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New…** button, the next screen will pop-up as shown in Figure 4-33.
2. Select the service port you want to use from the **Common Service Port** list. If the **Common Service Port** list does not have the service that you want to use, type the service port number or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **IP Address** box.
4. Select the protocol used for this application, either **TCP**, **UDP**, or **All**.
5. Select the **Enable** to enable the virtual server.
6. Click the **Save** button.



Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)

IP Address:

Protocol: ALL

Status: Enabled

Common Service Port: --Select One--

Figure 4-33 Add or Modify a Virtual Server Entry

☞ **Note:**

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disabled All** button to make all entries enabled/disabled.

Click the **Delete All** button to delete all entries.

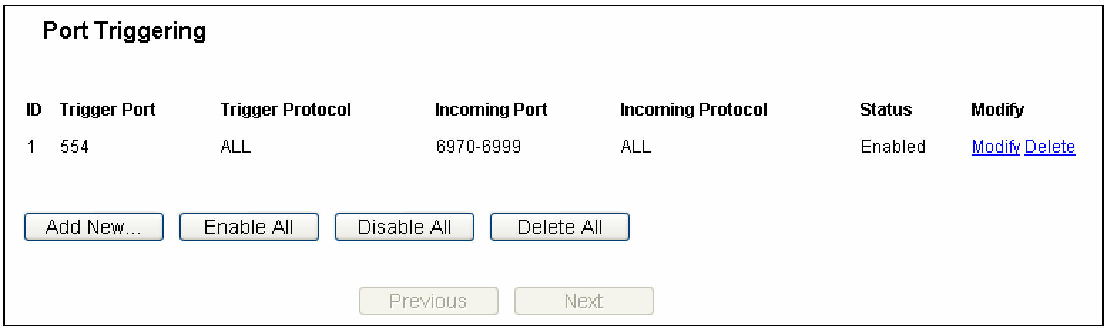
Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

☞ **Note:**

If you set the service port of the virtual server as 80, you must set the Web management port on "**Security → Remote Management**" page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.8.2 Port Triggering

Choose menu "**Forwarding → Port Triggering**", you can view and add port triggering in the screen as shown in Figure 4-34. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.



Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify
1	554	ALL	6970-6999	ALL	Enabled	Modify Delete

Figure 4-34 Port Triggering

Once the Router is configured, the operation is as follows:

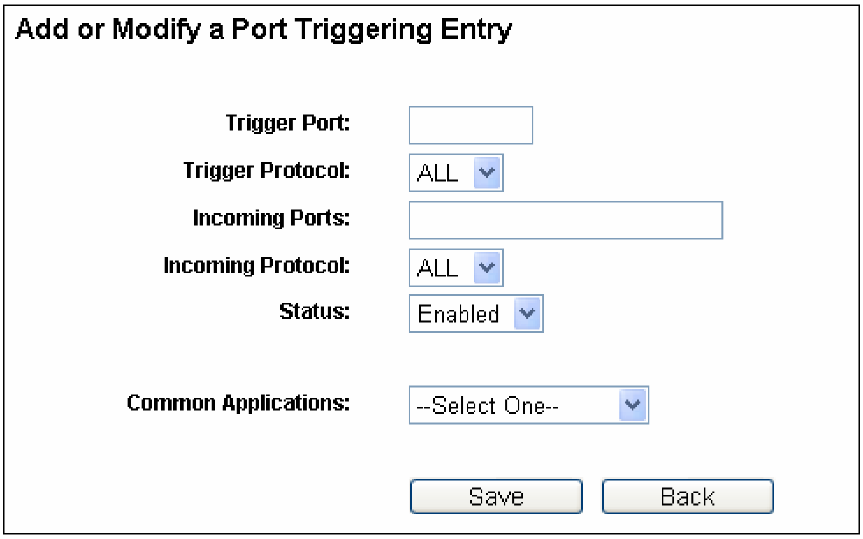
1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

3. When necessary， the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

- **Trigger Port -** The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Trigger Protocol -** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
- **Incoming Ports Range -** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** The protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **ALL** (all protocols supported by the Router).
- **Status -** The status of this entry, either **Enabled** or **Disabled**.

To add a new rule, follow the steps below.

1. Click the **Add New…** button, the next screen will pop-up as shown in Figure 4-35.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Incoming Ports** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Incoming Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All.**
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.



Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL

Incoming Ports:

Incoming Protocol: ALL

Status: Enabled

Common Applications: --Select One--

Figure 4-35 Add or Modify a Port Triggering Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

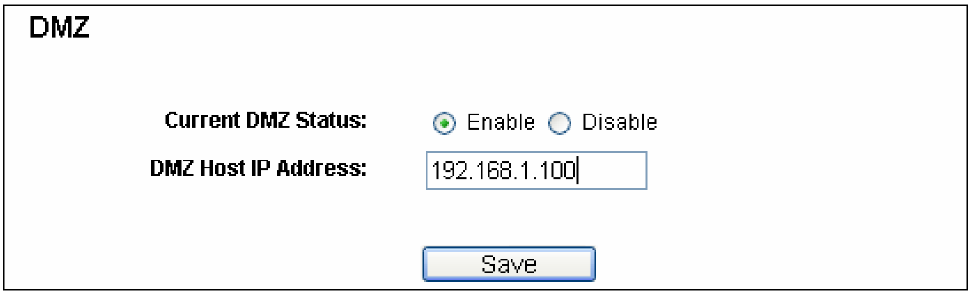
Click the **Delete All** button to delete all entries.

☞ **Note:**

1. When the trigger connection is released, the corresponding opening ports will be closed.
2. Each rule is allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

4.8.3 DMZ

Choose menu "**Forwarding** → **DMZ**", you can view and configure DMZ host in the screen as shown in Figure 4-36. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.



DMZ

Current DMZ Status: ● Enable ○ Disable

DMZ Host IP Address: 192.168.1.100

Figure 4-36 DMZ

To assign a computer or server to be a DMZ server:

4. Check the **Enable** radio button.

5. Enter the IP Address of a local host in the **DMZ Host IP Address** field.

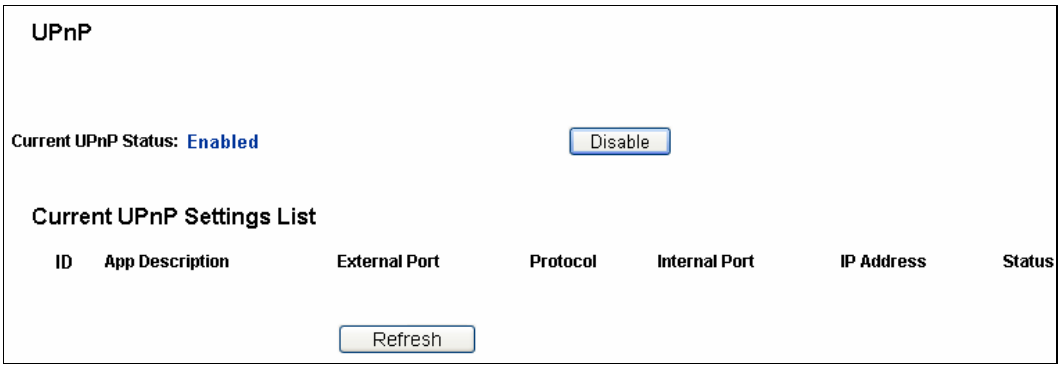
6. Click the **Save** button.

☞ **Note:**

After you set the DMZ host, the firewall related to the host will not work.

4.8.4 UPnP

Choose menu "**Forwarding** → **UPnP**", you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown in Figure 4-37. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



UPnP

Current UPnP Status: Enabled

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status

Figure 4-37 UPnP

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button.

- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description -** The description provided by the application in the UPnP request.
  - **External Port -** The external port the Router opens for the application.
  - **Protocol -** The type of protocol the Router opens for the application.
  - **Internal Port -** The Internal port the Router opens for local host.
  - **IP Address -** The IP address of the UPnP device that is currently accessing the Router.

- **Status -** The status of the port is displayed here. “Enabled” means that the port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

4.9 Management

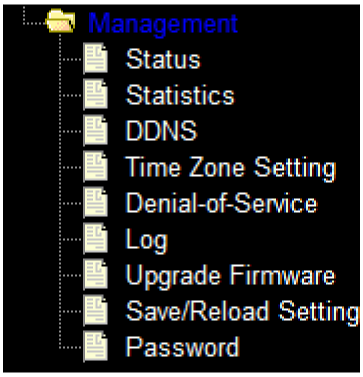
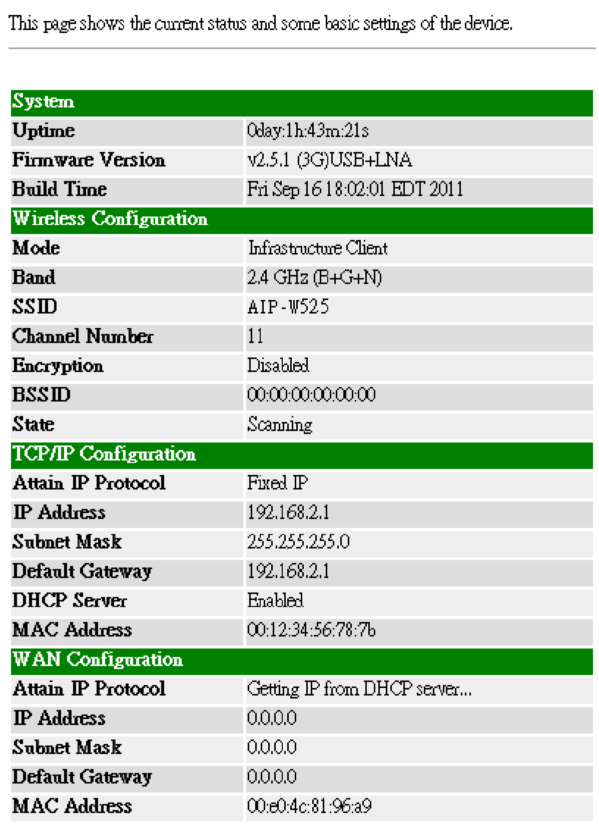


Figure 4-35 The Management menu

There are nine submenus under the Management menu as shown in Figure 4-35: **Status**, **Statists**, **DDNS, Time Zone Setting, Denial-of-Service, Log, Upgrade Firmware, Save/Reload Setting,** and **Password.** Click any of them, and you will be able to configure the corresponding function.

4.9.1 Status

Choose menu “**Management** → **Status**”, display the current status of AIP-W525H as shown in Figure 4-39.



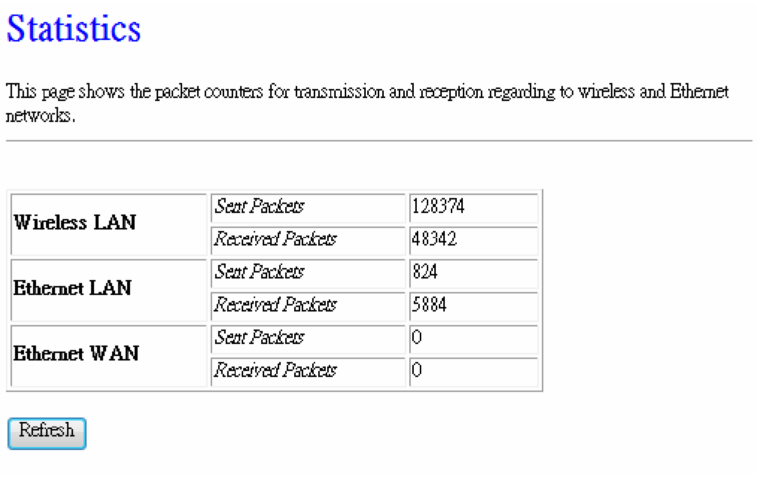
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:1h:43m:21s
Firmware Version	v2.5.1 (3G)USB+LNA
Build Time	Fri Sep 16 18:02:01 EDT 2011
Wireless Configuration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	AIP-W525
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DHCP Server	Enabled
MAC Address	00:12:34:56:78:7b
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:a9

Figure 4-35 Status

4.9.2 Statistics

Choose menu "**Management** → **Statistics**", you can view the network traffic on the Router as shown in Figure 4-36.



Statistics

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

Wireless LAN	*Sent Packets*	128374
	Received Packets	48342
Ethernet LAN	*Sent Packets*	824
	Received Packets	5884
Ethernet WAN	*Sent Packets*	0
	Received Packets	0

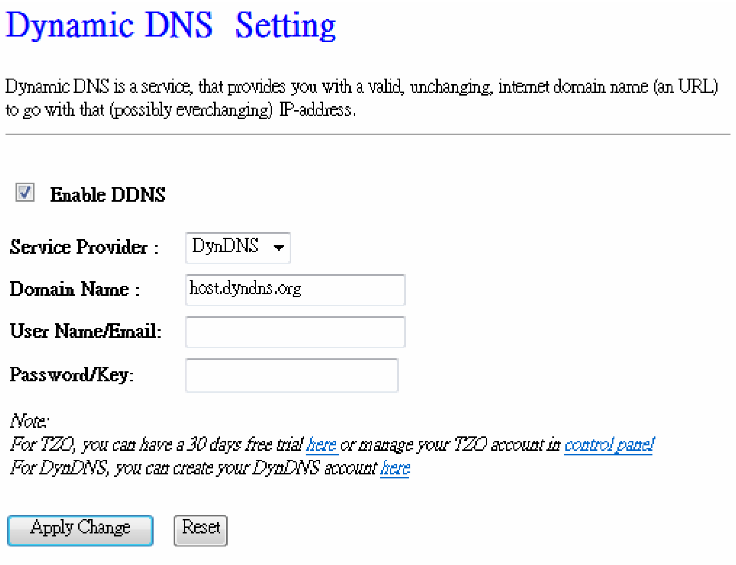
Figure 4-36 Advanced Security

4.9.3 DDNS

Choose menu “**Management -> DDNS**”, you can configure the Dynamic DNS function.

The Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, or TZO. The Dynamic DNS client service provider will give you a password or key.

If the dynamic DNS **Service Provider** your select is www.dyndns.org, the page will appear as shown in Figure 4-41.



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

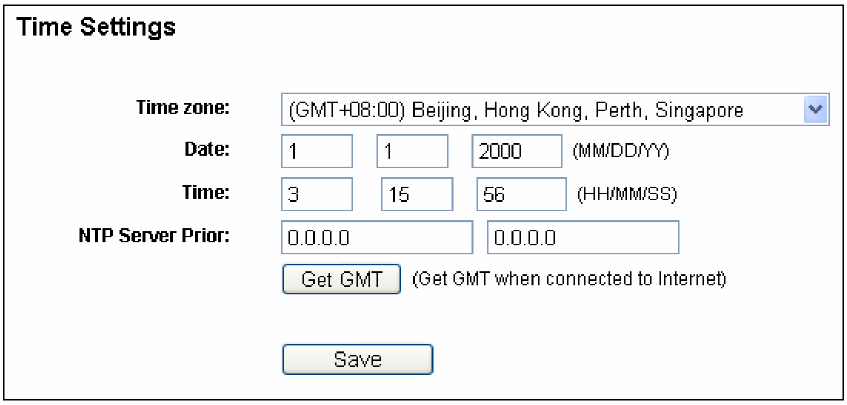
Figure 4-41 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain Name** you received from dynamic DNS service provider here.
4. Click the **Apply Change** button to log in to the DDNS service.

4.9.4 Time Zone Setting

Choose menu “**System Tools → Time Settings**”, you can configure the time on the following screen.



Time Settings

Time zone:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore			
Date:	1	1	2000	(MM/DD/YY)
Time:	3	15	56	(HH/MM/SS)
NTP Server Prior:	0.0.0.0	0.0.0.0		

Figure 4-42   Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior -** Enter the address for the NTP Server, then the Router will get the time from the NTP Server preferentially. In addition, for some built-in common NTP Servers, the Router can get time automatically once it connects the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.
3. Click **Save** to save the configuration.

To configure the system automatically:

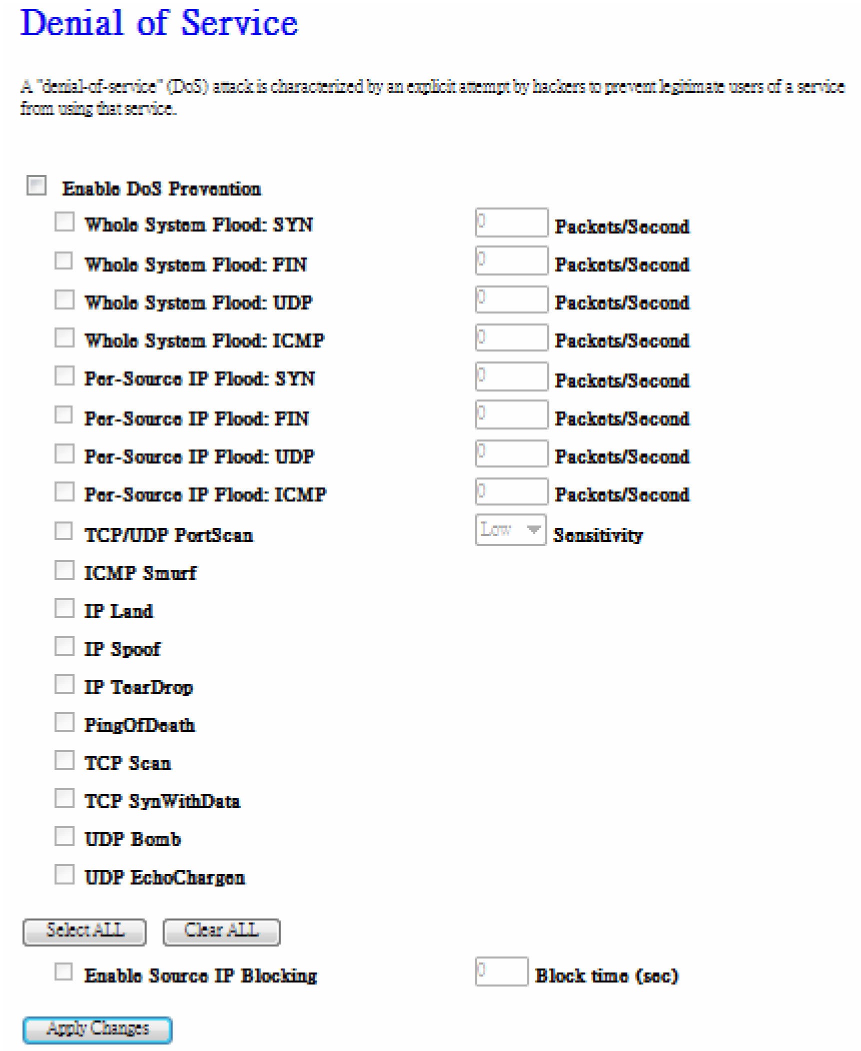
1. Select your local time zone.
2. Enter the IP address for **NTP Server Prior**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

☞ **Note:**

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the Router successfully, otherwise, these functions will not take effect.
2. The time will be lost if the Router is turned off.
3. The Router will obtain GMT automatically from Internet if it has already connected to Internet.

4.9.5 Denial-of-Service

DoS Protection will take effect only when the **Enable DoS Preventation** in "**Management → DoS**" is enabled as shown in Figure 4-43.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

- ☐ Enable DoS Prevention
  - ☐ Whole System Flood: SYN — 0 Packets/Second
  - ☐ Whole System Flood: FIN — 0 Packets/Second
  - ☐ Whole System Flood: UDP — 0 Packets/Second
  - ☐ Whole System Flood: ICMP — 0 Packets/Second
  - ☐ Per-Source IP Flood: SYN — 0 Packets/Second
  - ☐ Per-Source IP Flood: FIN — 0 Packets/Second
  - ☐ Per-Source IP Flood: UDP — 0 Packets/Second
  - ☐ Per-Source IP Flood: ICMP — 0 Packets/Second
  - ☐ TCP/UDP PortScan — Low Sensitivity
  - ☐ ICMP Smurf
  - ☐ IP Land
  - ☐ IP Spoof
  - ☐ IP TearDrop
  - ☐ PingOfDeath
  - ☐ TCP Scan
  - ☐ TCP SynWithData
  - ☐ UDP Bomb
  - ☐ UDP EchoChargen

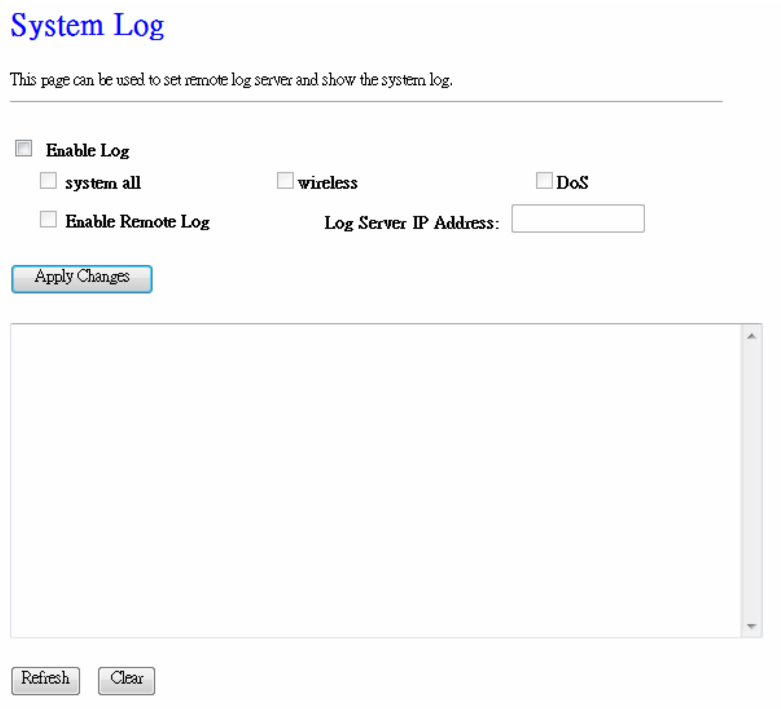
☐ Enable Source IP Blocking — 0 Block time (sec)

Figure 4-43 DoS

Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

4.9.6 Log

Choose menu "**Management →Log**", you can view the logs of the Router.



System Log

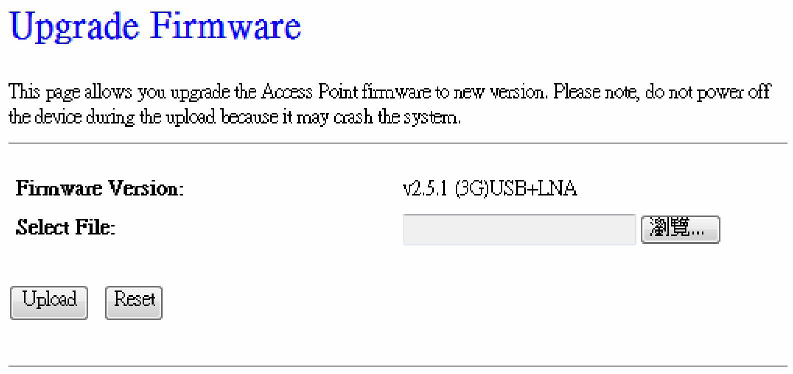
This page can be used to set remote log server and show the system log.

Figure 4-44 System Log

- **System all –** Display all the log file on the Router .
- **Wireless –** Display just the wireless log on the Router.
- **DoS –** Display just Denial-of-Service log on the Router.
- **Enable Remote Log -** Click to enable remote log service.
- **Log Server IP Address –** Please enter the IP address to store your log file when **Enable Remote Log** is enabled.

4.9.7 Upgrade Firmware

Choose menu "**Management → Upgrade Firmware**", you can update the latest version of firmware for the Router on the following screen.



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.

Firmware Version: v2.5.1 (3G)USB+LNA

Select File:

Figure 4-45 Firmware Upgrade

- **Firmware Version -** This displays the current firmware version.

To upgrade the Router's firmware, follow these instructions below:

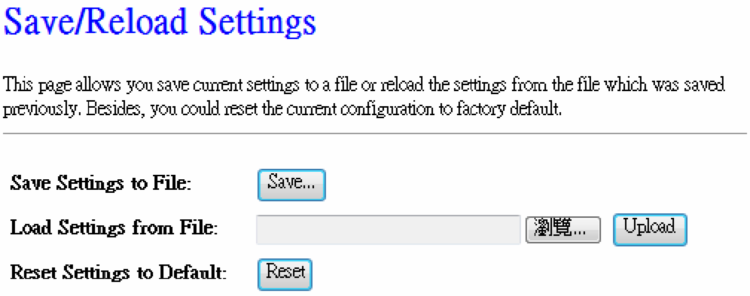
1. Download a more recent firmware upgrade file from our website.
2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

☞ **Note:**

1. New firmware versions are posted at our website and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
2. When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
3. Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
4. The Router will reboot after the upgrading has been finished.

4.9.8 Save/Reload Setting

Choose menu "**Management → Save/Reload Setting**", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 4-46.



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: Save...

Load Settings from File: 瀏覽... Upload

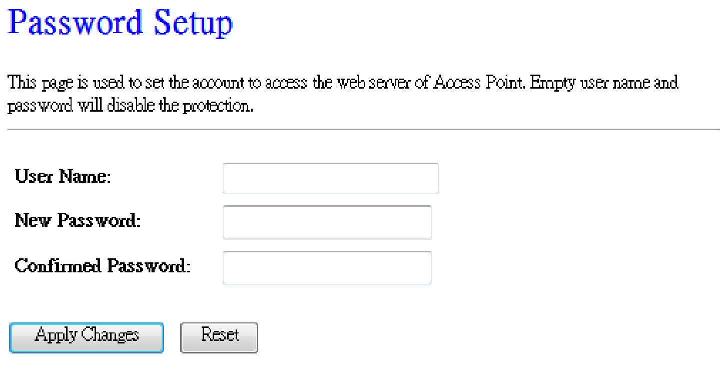
Reset Settings to Default: Reset

Figure 4-46 Backup & Restore Configuration

- Click the **Save** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse…** button to locate the update file for the Router, or enter the exact path to the Setting file in the text box.
  - Click the **Upload** button.
- Click the **Reset** button restore the configurations of the Router to factory defaults.

4.9.9 Password

Choose menu “**Management → Password**”, you can change the factory default user name and password of the Router in the next screen as shown in Figure 4-47.



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:

New Password:

Confirmed Password:

Figure 4-47 Password

It is strongly recommended that you should change the factory default user name and password of the Router, because all users who try to access the Router's Web-based utility or Quick Setup will be prompted for the Router's default user name and password.

Click the **Apply Change** button when finished.

Click the **Reset** button to clear all.

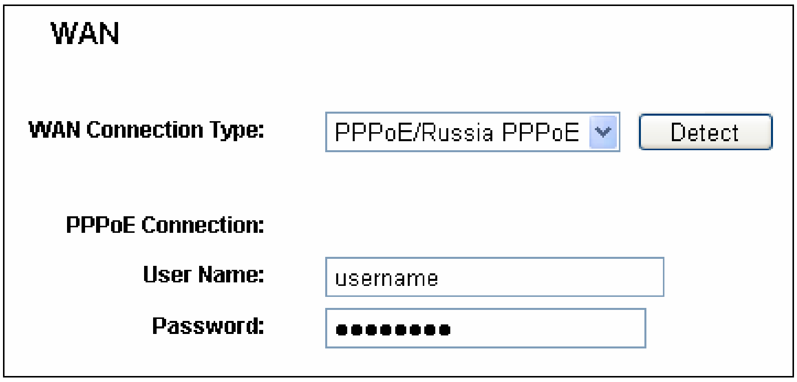
Appendix A: FAQ

1. How do I configure the Router to access the Internet by ADSL users?

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Log in to the Router, click the "**Network**" menu on the left of your browser, and click "**WAN**" submenu. On the **WAN** page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking **Connect**.



WAN

WAN Connection Type: PPPoE/Russia PPPoE Detect

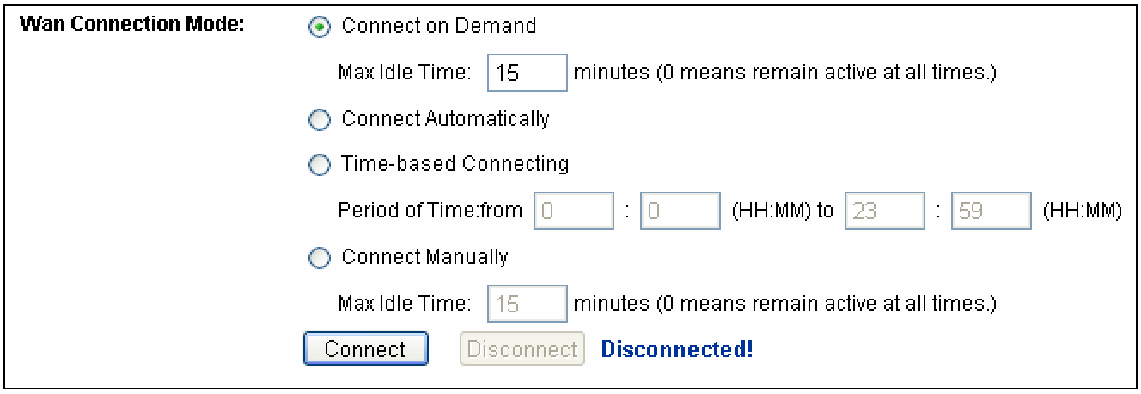
PPPoE Connection:

User Name: username

Password: ●●●●●●●●●

Figure A-1 PPPoE Connection Type

4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.



Wan Connection Mode: ● Connect on Demand

Max Idle Time: 15 minutes (0 means remain active at all times.)

○ Connect Automatically

○ Time-based Connecting

Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

○ Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

Connect Disconnect Disconnected!

Figure A-2 PPPoE Connection Mode

☞ **Note:**

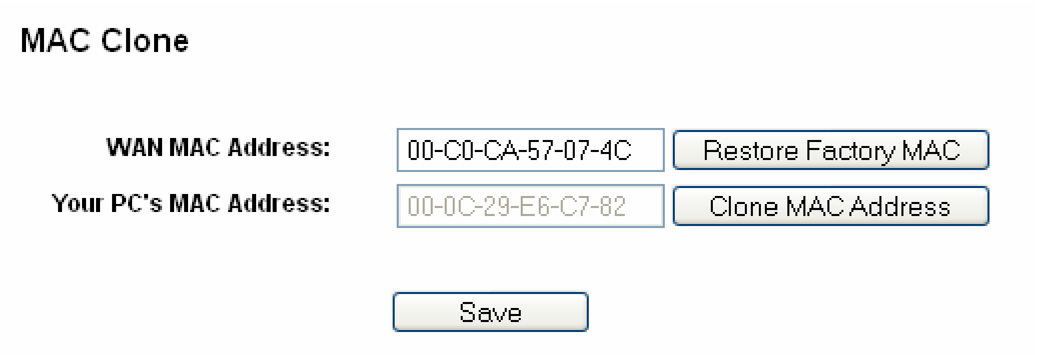
1. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

2. If you are a Cable user, please configure the Router following the above steps.

2. **How do I configure the Router to access the Internet by Ethernet users?**

1) Log in to the Router, click the “**Network**” menu on the left of your browser, and click "**WAN**" submenu. On the **WAN** page, select “Dynamic IP” for "WAN Connection Type", finish by clicking **Save**.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, log in to the Router and click the "**Network**" menu link on the left of your browser, and then click "**MAC Clone**" submenu link. On the "**MAC Clone**" page, if your PC’s MAC address is proper MAC address, click the **Clone MAC Address** button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the **Save** button. It will take effect after rebooting.


MAC Clone

WAN MAC Address: 00-C0-CA-57-07-4C

Your PC's MAC Address: 00-0C-29-E6-C7-82

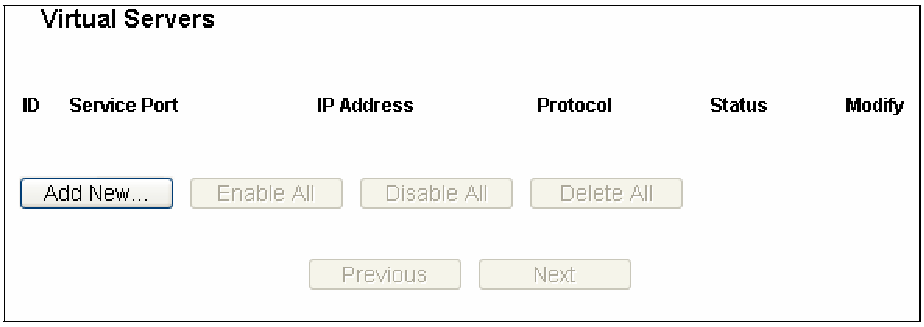
Figure A-3 MAC Clone

3. **I want to use NetMeeting, what do I need to do?**

1) If you start NetMeeting as a sponsor, you don’t need to do anything with the Router.

2) If you start as a response, you need to configure Virtual Server or DMZ Host and make sure the H323 ALG is enabled.

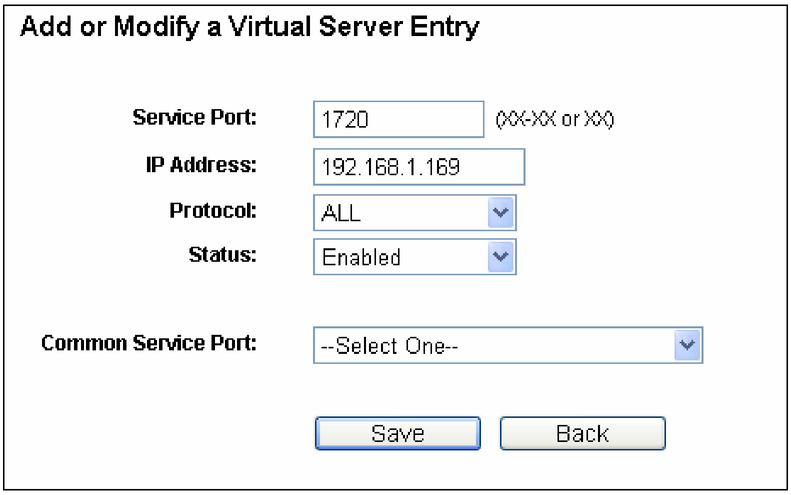
3) How to configure Virtual Server: Log in to the Router, click the “**Forwarding**” menu on the left of your browser, and click "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**. Then on the “**Add or Modify a Virtual Server Entry**” page, enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.1.169 for an example, remember to **Enable** and **Save**.



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure A-4 Virtual Servers



Add or Modify a Virtual Server Entry

Service Port: 1720 (XX-XX or XX)

IP Address: 192.168.1.169

Protocol: ALL

Status: Enabled

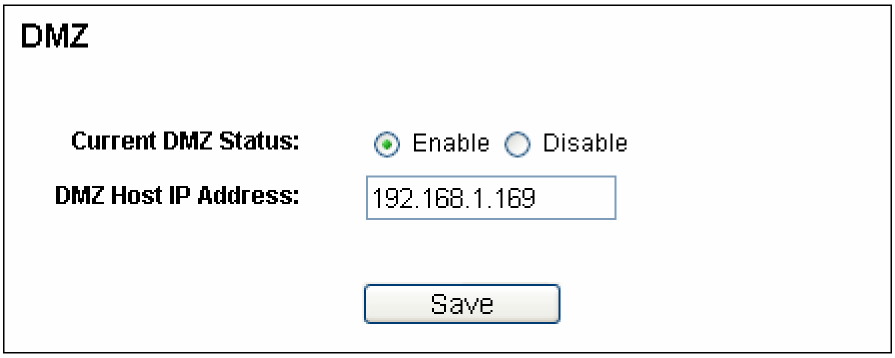
Common Service Port: --Select One--

Figure A-5 Add or Modify a Virtual server Entry

☞ **Note:**

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

4) How to enable DMZ Host: Log in to the Router, click the “**Forwarding**” menu on the left of your browser, and click "**DMZ**" submenu. On the "DMZ" page, click **Enable** radio button and type your IP address into the “DMZ Host IP Address” field, using 192.168.1.169 as an example, remember to click the **Save** button.



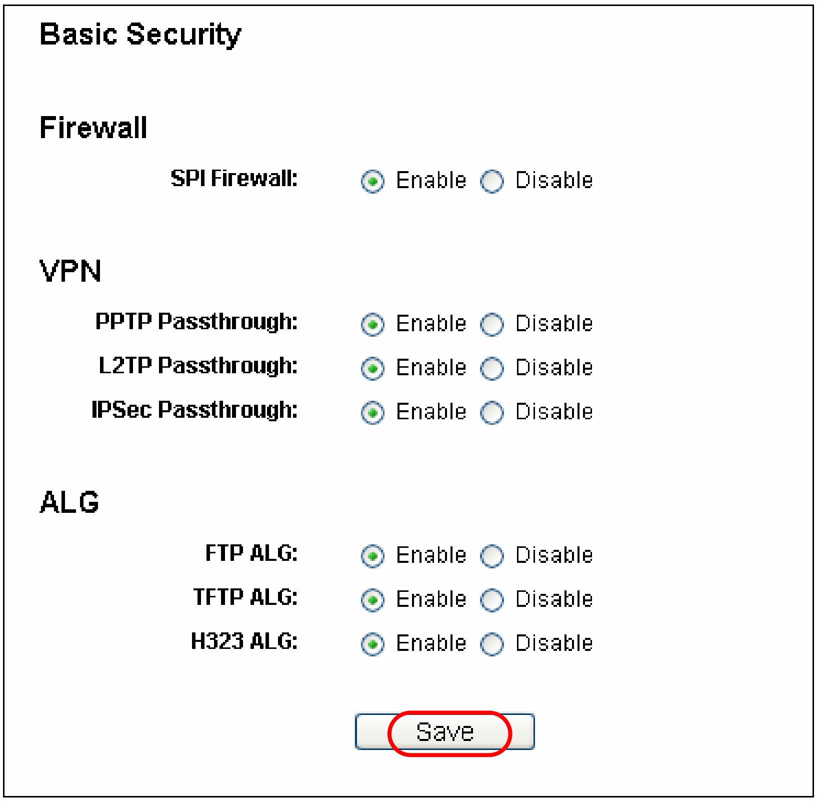
DMZ

Current DMZ Status: ● Enable ○ Disable

DMZ Host IP Address: 192.168.1.169

Figure A-6 DMZ

5) How to enable H323 ALG: Log in to the Router, click the “**Security**” menu on the left of your browser, and click “**Basic Security**” submenu. On the “**Basic Security**” page, check the **Enable** radio button next to **H323 ALG**. Remember to click the **Save** button.



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

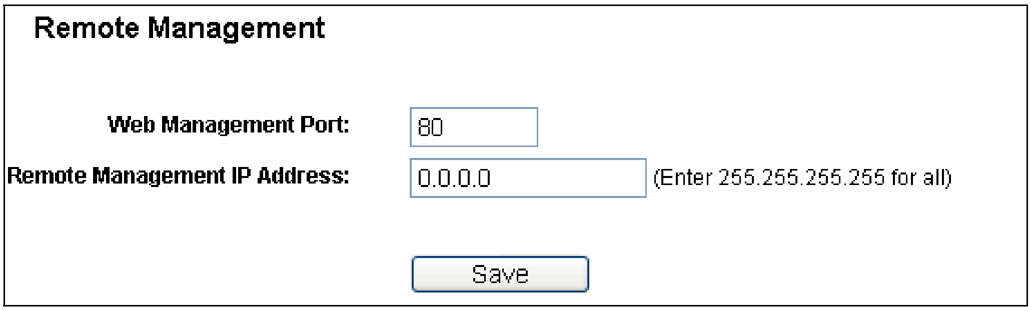
H323 ALG: ● Enable ○ Disable

Figure A-7 Basic Security

4. **I want to build a WEB Server on the LAN, what should I do?**

1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you must change the WEB management port number to avoid interference.

2) To change the WEB management port number: Log in to the Router, click the “**Security**” menu on the left of your browser, and click "**Remote Management**" submenu. On the "**Remote Management**" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click **Save** and reboot the Router.



Remote Management

Web Management Port: 80

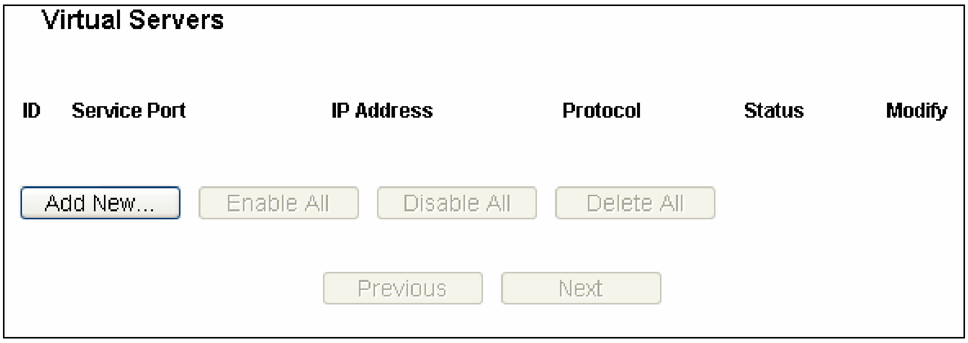
Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

Figure A-8 Remote Management

☞ **Note:**

If the above configuration takes effect, configure to the Router by typing 192.168.1.1:88 (the Router’s LAN IP address: Web Management Port) in the address field of the Web browser.

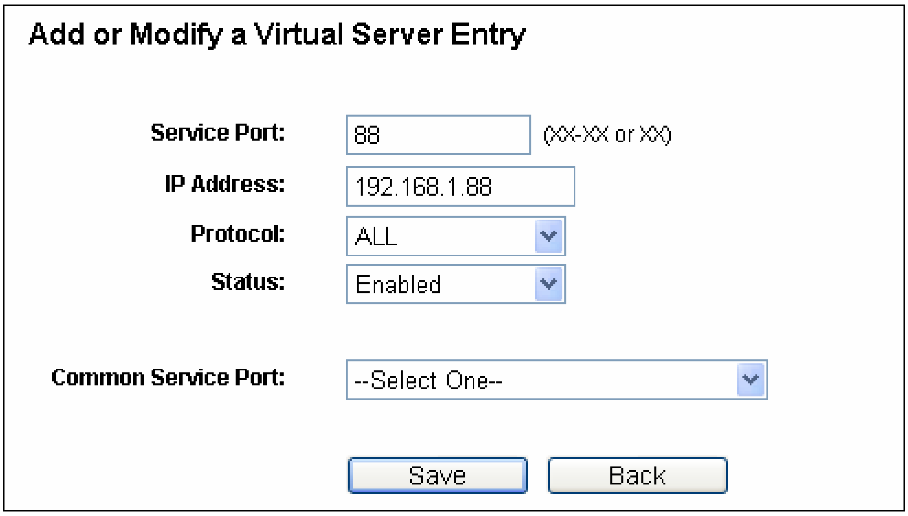
3) Log in to the Router, click the "**Forwarding**" menu on the left of your browser, and click the "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**, then on the "**Add or Modify a Virtual Server**" page, enter "80" into the blank next to the "**Service Port**", and your IP address next to the "**IP Address**", assuming 192.168.1.188 for an example, remember to **Enable** and **Save**.



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure A-9 Virtual Servers



Add or Modify a Virtual Server Entry

Service Port: 88 (XX-XX or XX)

IP Address: 192.168.1.88

Protocol: ALL

Status: Enabled

Common Service Port: --Select One--

Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the Router.

1) Make sure the "**Enable Wireless Router Radio**" is checked.

2) Make sure that the wireless stations' SSID accord with the Router's SSID.

3) Make sure the wireless stations have right KEY for encryption when the Router is encrypted.

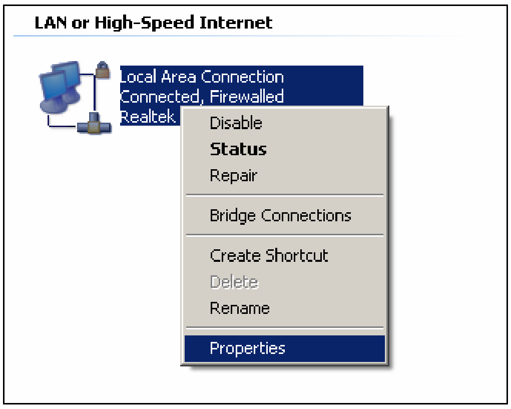
4) If the wireless connection is ready, but you can't access the Router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.
2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
3) Right click the icon that showed below, select Properties on the prompt page.

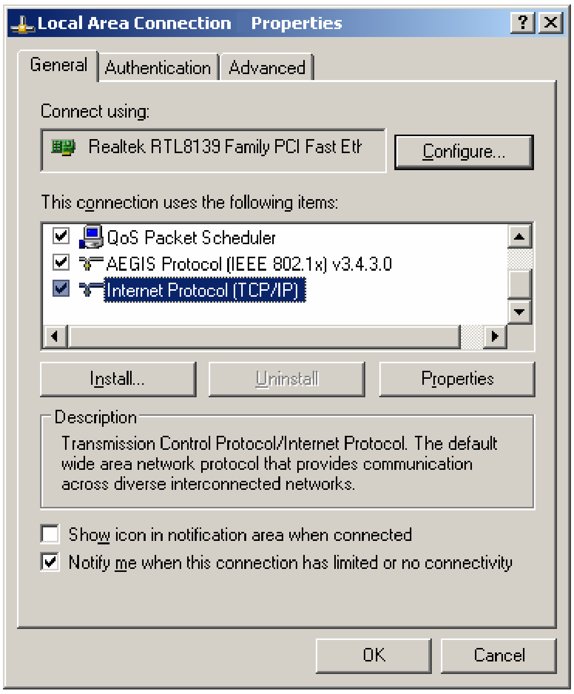


LAN or High-Speed Internet

Local Area Connection
Connected, Firewalled
Realtek

Figure B-1

4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.



Local Area Connection Properties

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.4.3.0
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

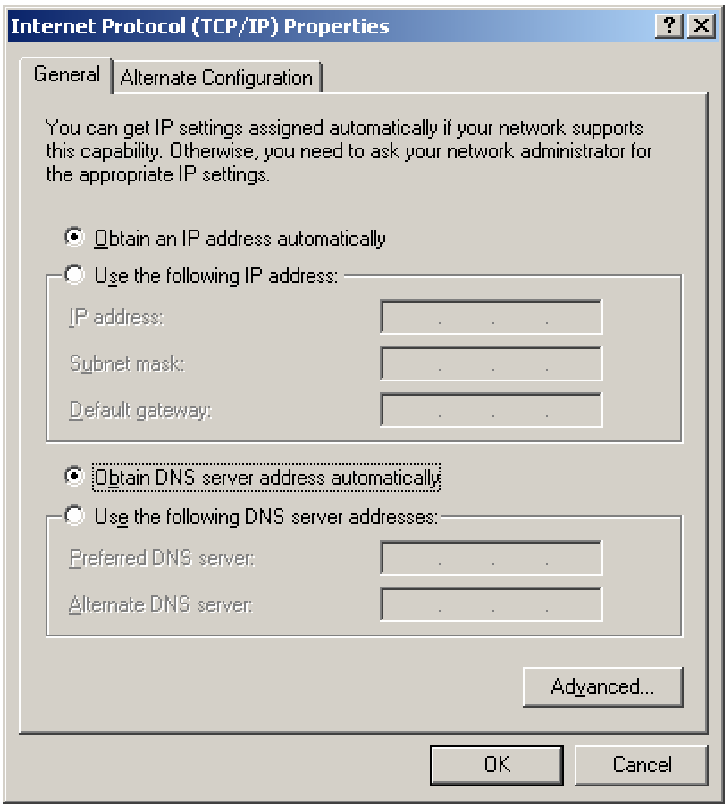
Figure B-2

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

➢ **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure B-3

☞ **Note:** For Windows 98 OS or before, the PC and Router may need to be restarted.

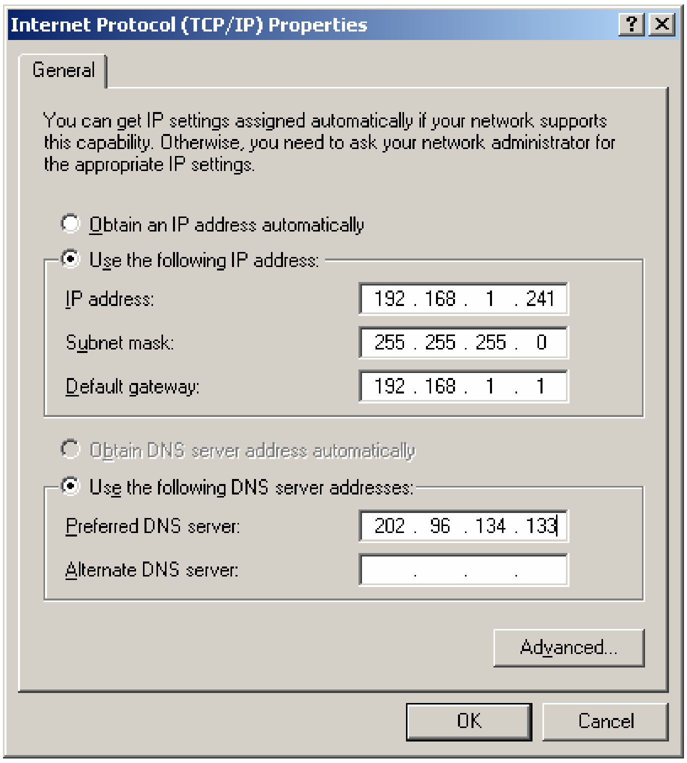
➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button. And the following items available.

2 If the Router's LAN IP address is 192.168.1.1, specify the **IP address** as 192.168.1.x (x is from 2 to 254), and the **Subnet mask** as 255.255.255.0.

3 Type the Router’s LAN IP address (the default IP is 192.168.1.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 241

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 202 . 96 . 134 . 133

Alternate DNS server: . . .

Figure B-4

Now, click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b, 802.11g Compatible with 802.11n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	PWR, SYS, WLAN, WAN, LAN (1-4), WPS
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n：up to 300Mbps（Automatic） 11g：54/48/36/24/18/12/9/6M（Automatic） 11b：11/5.5/2/1M（Automatic）
Channels	1~11
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	-1dBi
Environmental and Physical	
Temperature.	Operating : 0℃~40℃ (32℉~104℉)
	Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 90% RH, Non-condensing

Appendix D: Glossary

- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **–** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.