User Manual

Model No. : AL-AP48H-15SO, AL-AP48H-23SO

Edition V.01

Power By Rick Wen

rickwen@emitech.com.tw

TABLE OF CONTENTESSCOPE

The Access Point has two basic operating modes that can be set through the web management interface:

- Router Mode – Normal gateway mode that connects a wired LAN and wireless clients to an internet access device, such as a cable or DSL modem. This is the factory set default mode.
- Bridge mode – An access point mode that extends a wired LAN to wireless clients.

In addition to these basic operating modes, each wireless interface supports a Wireless Distribution System (WDS) link to another AP, and a wireless client mode.

In a basic configuration, how the AP is connected depends on the operating mode. The following sections describe connections for basic Router Mode and Bridge Mode operation.

ROUTER MODE

In its default Router Mode, the AP48 forwards traffic between an internet connected cable or ADSL modem, and wired or wireless PCs or notebooks.

To connect the AP48 in Router Mode for use as an Internet gateway, follow these steps below:

1. Connect an Ethernet cable from the AP48's WAN port to your Internet connected cable or ADSL modem.
2. Connect an Ethernet cable from the AP48's LAN port to your PC. Alternatively, you can connect to a workgroup switch to support a multiple users. The AP48 can support up to 253 wired or wireless users.
3. Power on the AP48 by connecting the AC power adapter and plugging it into a power source.

Caution: Use ONLY the power adapter supplied with the AP48. Otherwise, the product maybe damaged.

BRIDGE MODE

In Bridge Mode, the AP48 operates as a wireless access point, extending a local wired network to associated wireless clients (PCs or notebooks with wireless capability). From any nearby location, you can then make a wireless connection to the AP48 and access the wired network resources, including local servers and the Internet.

INITIAL CONFIGURATION

The AP48 offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer.

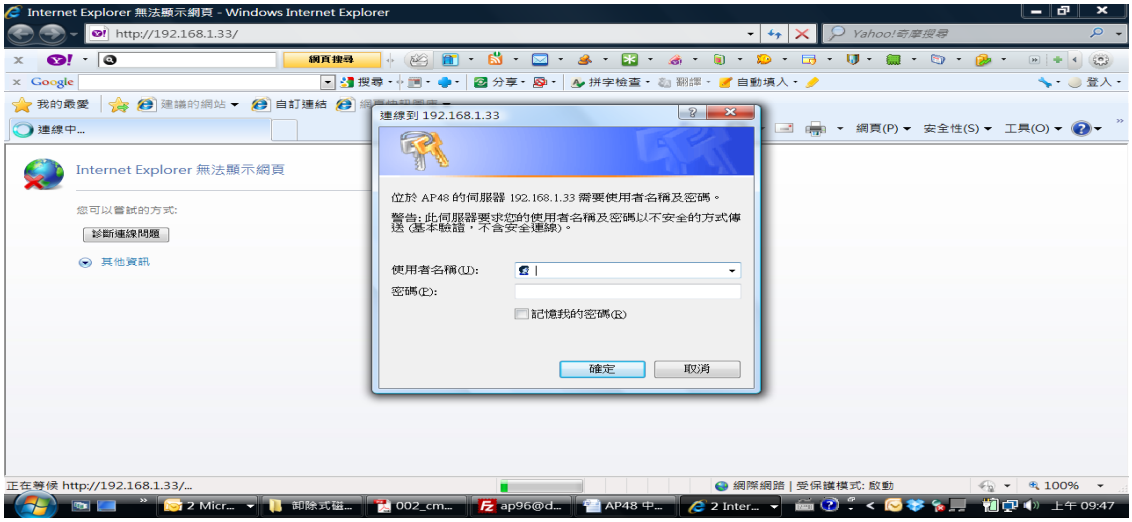
The Initial Configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to the AP before installing it in its intended location.

The AP has a default IP address of 192.168.1.33 and a subnet mask of 255.255.255.0. If your PC is set to "Obtain an IP address automatically" (that is, set as a DHCP client), you can connect immediately to the web interface. Otherwise, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start 192.168.1.x).

LOGGING INTO THE WEB INTERFACE

In the web browser's address bar, type the default IP address: http://192.168.1.33The web browser displays the home page.

The default Username is "admin" with a default Password of "admin" Click OK to access the web management interface.



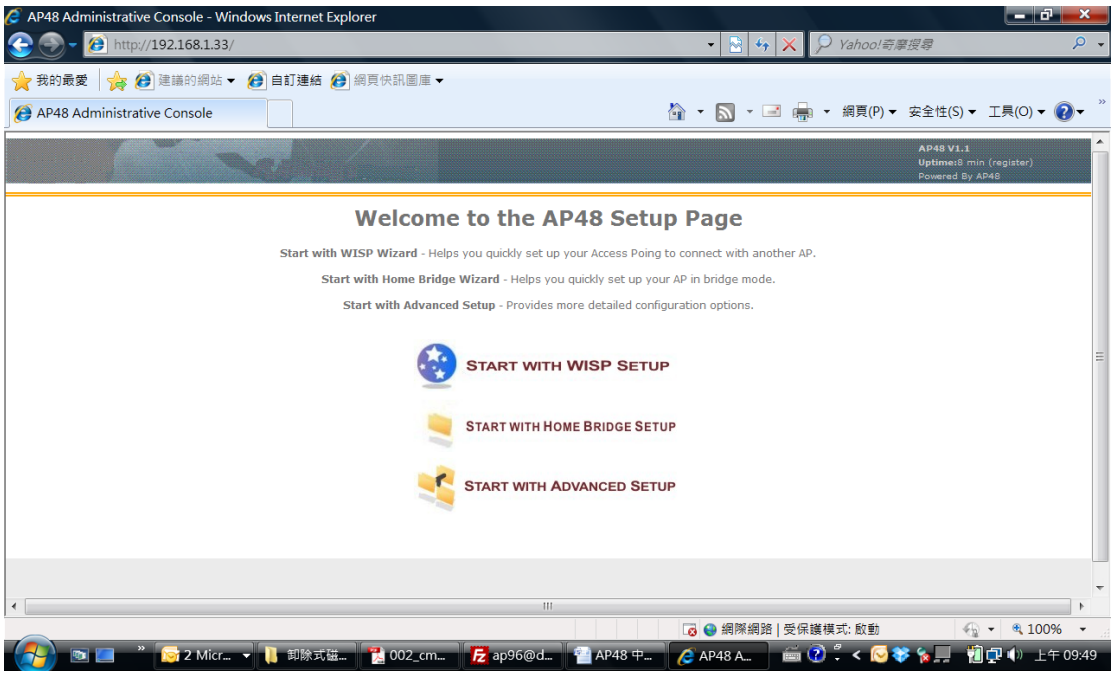
USING THE SETUP WIZARD

There are only a few basic steps you need to set up the AP and provide a connection for network access for other wireless stations.

The Setup Wizard takes you though configuration procedure for the general network settings, such as IP configuration, wireless network name (Service Set Identifier), and wireless security.

There are four types of wizards:

- Start with WISP Setup – Helps you quickly set up your AP to connect with another AP.
- Start with Home Bridge Setup – Helps you quickly set up your AP in Bridge Mode.
- Start with Advanced Setup – Provides more detailed configuration options.



For each type of setup the following sections cover the various pages of each setup scenario.

1.1 START WITH WISP SETUP

1.1.1 WAN SETTINGS

SSID Name of Parent AP: The name of the wireless network service. Clients that want to connect to the network must set their SSID to the same as the parent AP. (Default: “AP48H or AP8L”; Range: 1-32 characters)

The scan AP button opens a new window and scans all the APs in the area that maybe selected as the SSID. Clicking an entry will paste its SSID string to the Wireless Settings and close the window.

Radio Mode: Defines the radio mode.

AP48 only support 11a mode

Security Mode: Defines the security mode of the AP.

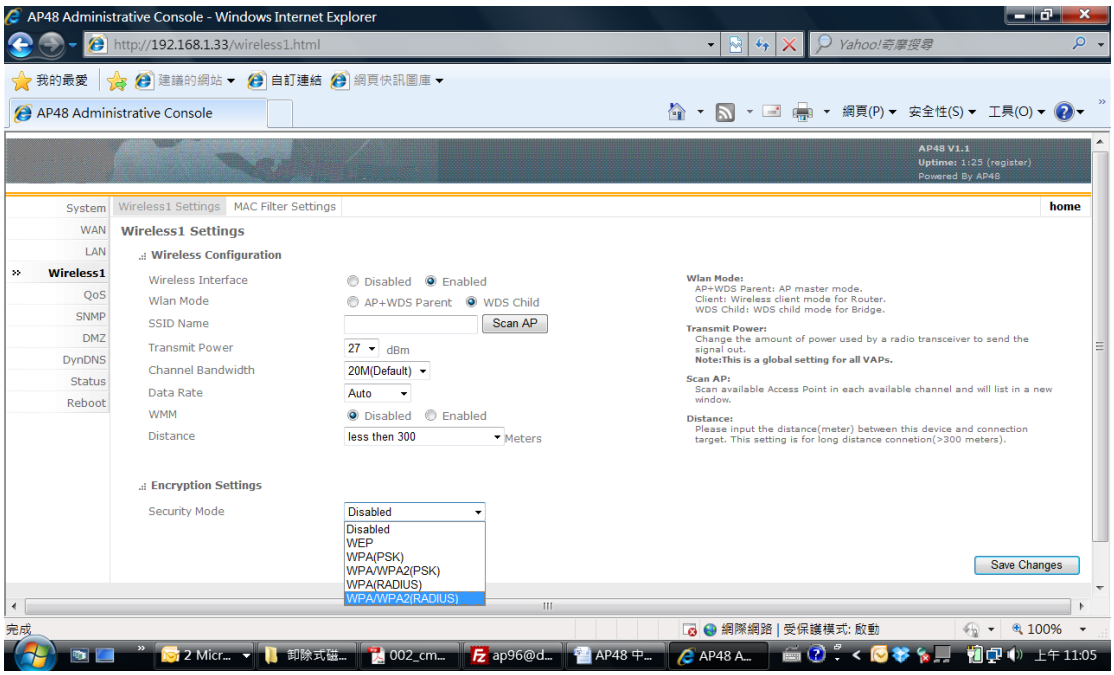
- **Disabled:** No security mode.
- **WEP:** Enable the AP to use WEP shared keys. If enabled, you must configure at least one key for the VAP interface and all its clients. Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the AP.
  - ✧ **Authentication Mode:** The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key”. Open-system authentication accepts any client attempting to connect to

the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.

- ✧ **Default Key:** Set WEP key values. At least one key must be specified. Each WEP key has an index number. The selected default key is used for authentication and encryption on the VAP interface. Enter key values that match the key type and length settings. Standard key values that match the key type and length settings. Standard keys are either 5 or 13 alphanumeric characters; or 10 or 26 hexadecimal digits.

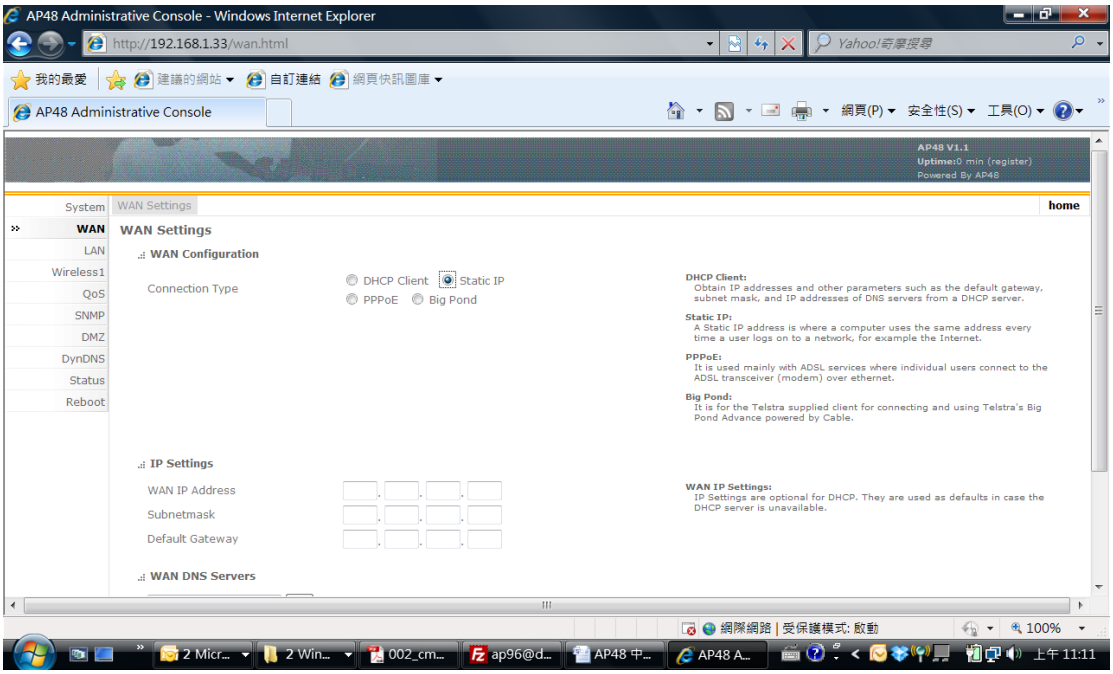
- **WPA(PSK) or WPA/ WPA2(PSK):** Enable WPA(PSK) or WPA/ WPA2(PSK) security on the VAP interface. Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small network uses a common password phrase that must be manually distributed to all clients that want to connect to the network. WPA/ WAP2(PSK) security on the VAP interface. WPA2 is a further security enhancement that includes the now ratified IEEE 802.11i wireless security standards.
  - ✧ **Pre-Shared Key:** Enter a key as to easy-to-remember form of letters and numbers. They key must be from 8 to 64 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface.
  - ✧ **Confirm Pre-Shared Key:** Enter the key for verification.

- **WPA(RADIUS) or WPA/ WPA2(RADIUS):** Enables WPA(RADIUS) or WPA2(RADIUS) security on the VAP interface. Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network. A RADIUS server must be specified for the AP to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.
  - ✧ **User Name:** A user name used by the RADIUS server.
  - ✧ **Password:** A shared text string used to encrypt messages between the Mini AP Router and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string.
  - ✧ **Confirm Password:** Enter the password for verification.

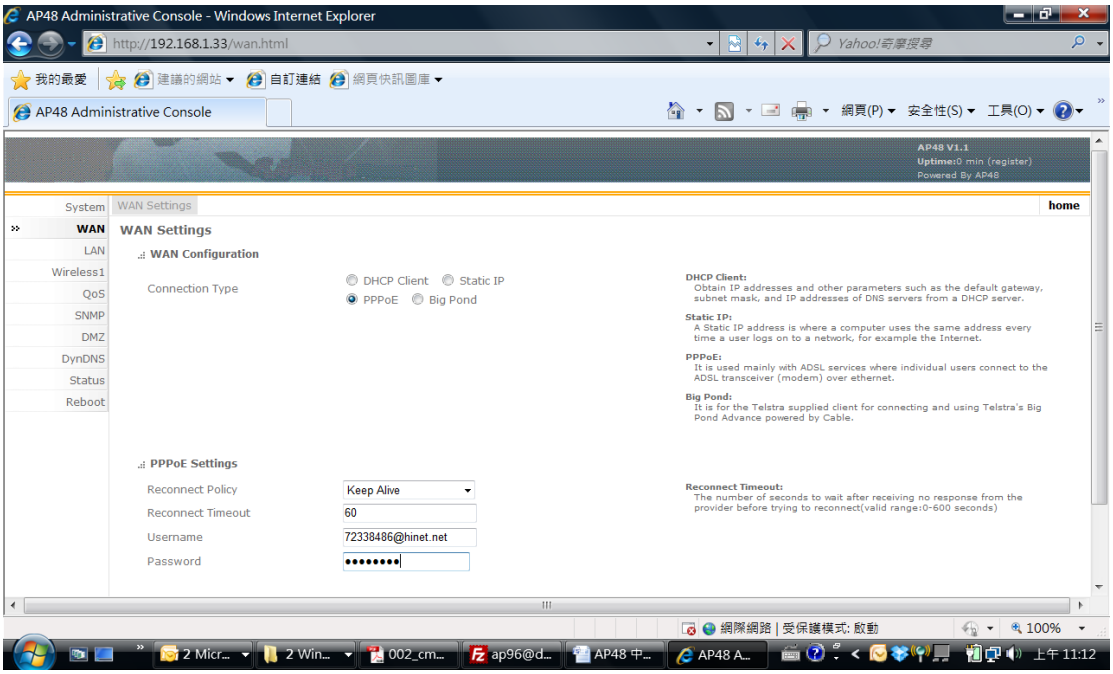


Connection Type:

- **DHCP Client:** Enables the AP to automatically obtain an IP address from a DHCP server normally operated by the Internet Service Provider (ISP).
- **Static IP:** Select configuration for a fixed IP address xDSL Internet connection.
  - ✧ **WAN IP Address:** The IP address of the AP. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
  - ✧ **Subnet Mask:** The mask that identifies the host address bits for routing to specific subnets.
  - ✧ **Default Gateway:** The IP address of the gateway router that is used if the requested destination address is not on the local subnet.



- **PPPoE:** Enable the AP IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using PPPoE.
  - ✧ **Reconnect Policy:** Select a procedure for the reconnect policy.
  - ✧ **Keep Alive:** Every few seconds the connection is verified by a keep-alive frame.
  - ✧ **Connect On Demand:** The connection attempt occurs on demand only.
  - ✧ **Username:** If your ISP has provided you with a PPPoE user name, enter it in the corresponding text box.
  - ✧ **Password:** If your ISP has provided you with a PPPoE password, enter it in the corresponding text box.



1.2 LAN SETTINGS (FOR ALL SETUPS)

Configures the AP's IP address and sets the DHCP server parameters for assigning IP addresses to wireless and LAN clients:

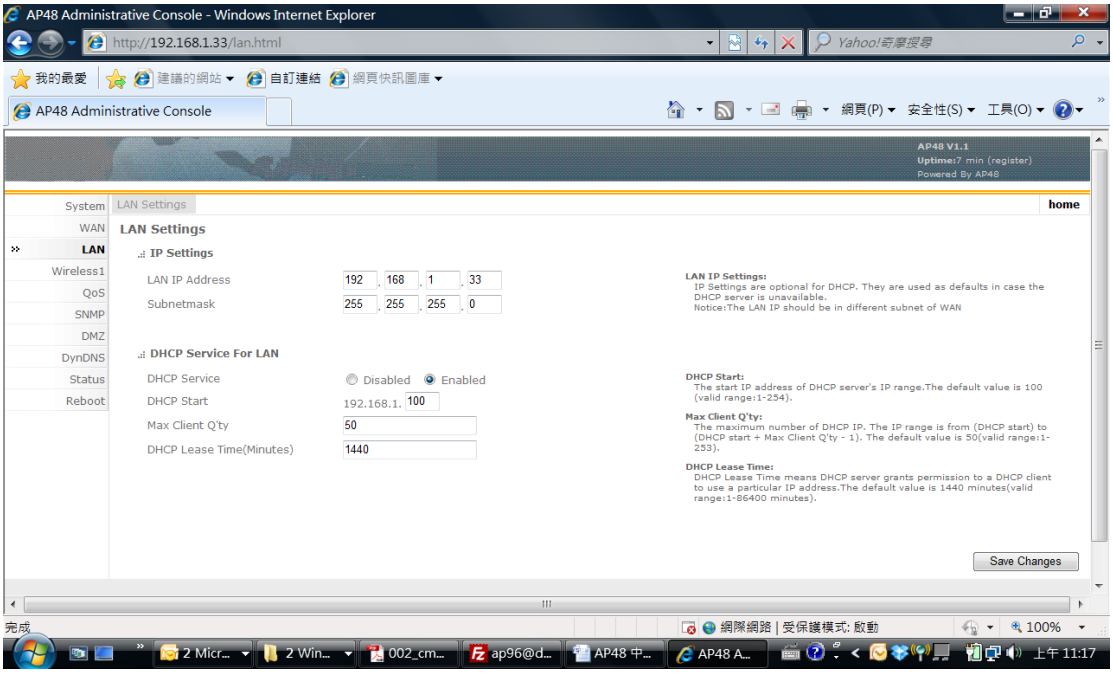
The displayed items on this page can be described as follows:

IP Settings: Set the IP address configuration of the AP.

- **LAN IP Address:** Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.1.33
- **Subnet mask:** Indicate the local subnet mask is fixed as 255.255.255.0.
- **Default Gateway (Home Bridge Setup only):** Normally, for wireless clients and stations in the attached LAN, the gateway address is the same as the LAN IP address. For a larger LAN with stations located on other subnets, type the IP address of the default gateway router in the text field provided.

DHCP Service for LAN: Set the DHCP service configuration of the Mini AP Router.

- **DHCP Service:** Enable or Disable the DHCP server.
- **DHCP Start:** Specify the start IP address of a range that the DHCP server can allocate to DHCP clients. Note that the address pool range is always in the same subnet as the unit's IP setting.
- **Max Client Q'ty:** Specify the maximum number of IP addresses to allocate to clients.
- **DHCP Lease Time (Minutes):** Select a time limit for the use of an IP address from the IP pool. When the time limit expires, the client has to request a new IP address.



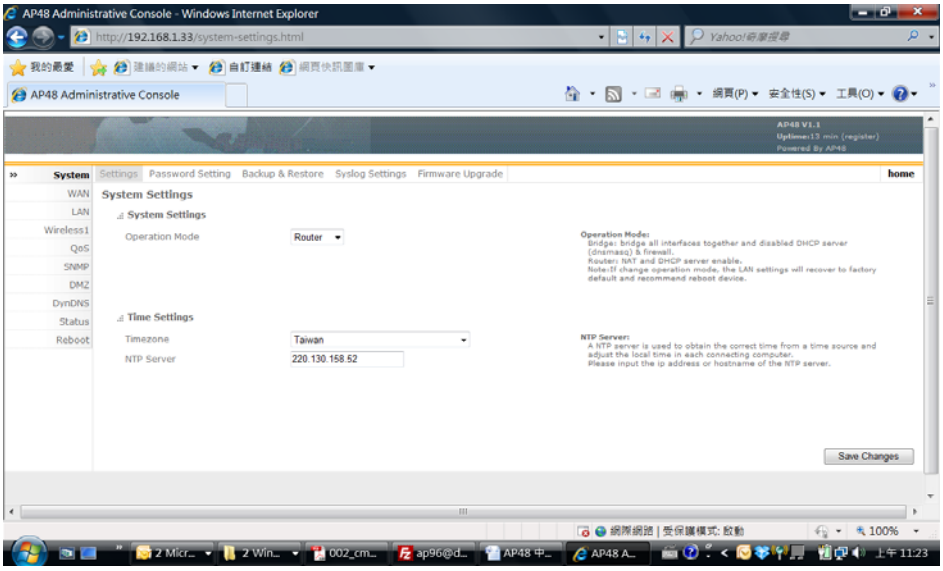
1.3 START WITH ADVANCED SETUP

1.3.1 SYSTEM

System Settings:

- **Operation Mode:**
  - ✧ Bridge: bridge all interfaces together and disabled DHCP server (dnsmasq) & firewall.
  - ✧ Router: NAT and DHCP server enable.

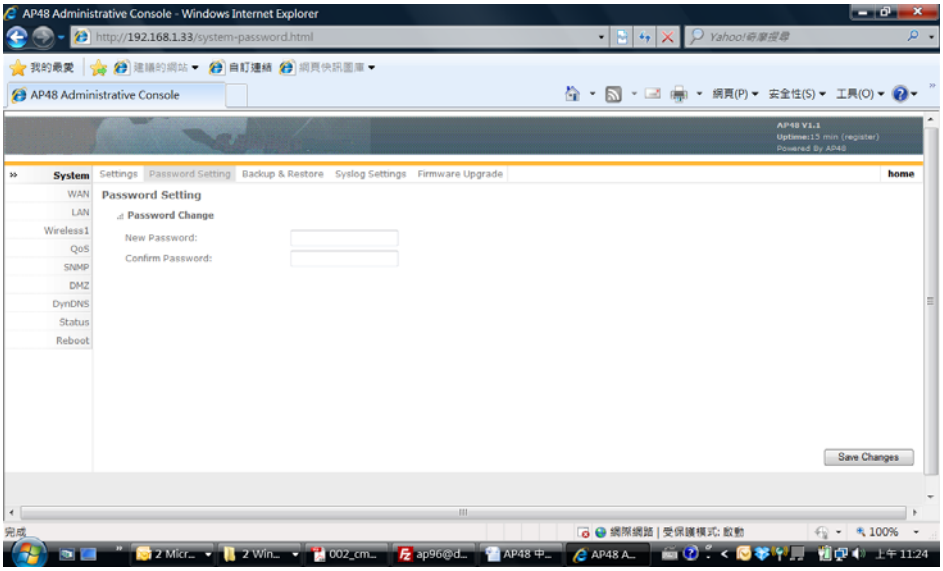
Note: If the operation mode is changed, the LAN settings will recover to factory default and recommend reboot service.



The password page allows you to change the password for access to the management interface.

Note: Pressing the reset button on the back of the AP for more than ten seconds resets the default password “admin”.

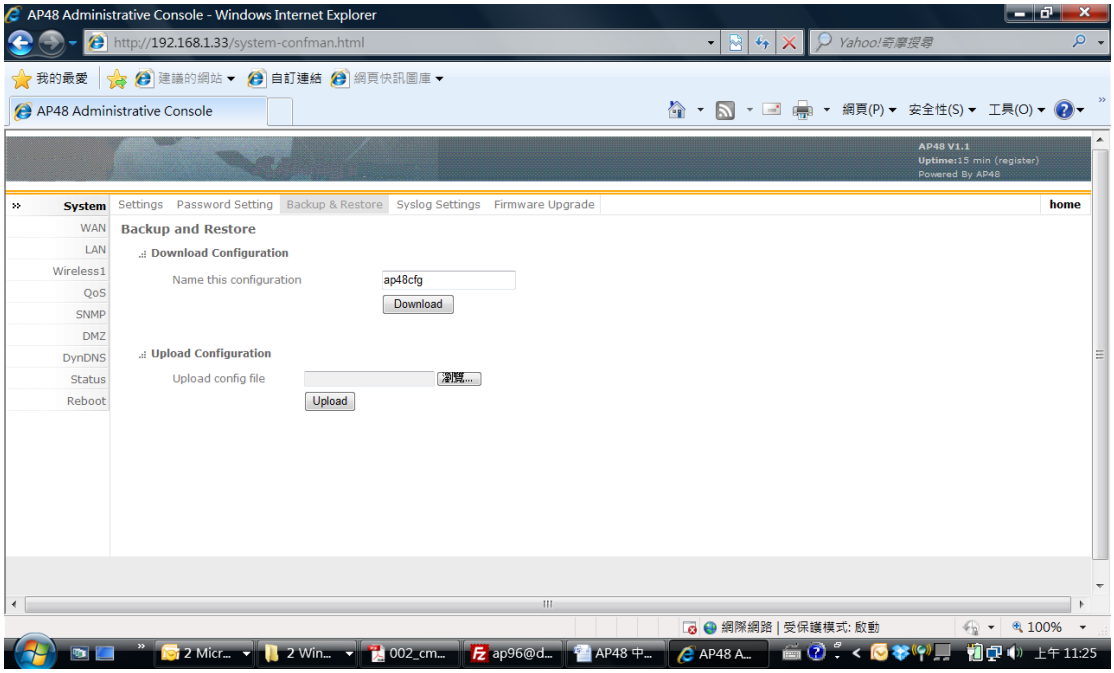
- **New Password:** The new password for management access.
- **Confirm Password:** Enter the password again for verification.



The Backup & Restore page allows you to save the AP’s current configuration or restore a previously saved configuration back to the device.

Download Configuration (Name this configuration): Saves the current configuration to a file on the web management station. Configuration file names file are given the extension “.tgz” on the management station.

Upload Configuration (Upload config file): Restore a previously saved configuration. Click the Browse button to locate the saved configuration file. The click the ***Upload*** button to restore the configuration to the AP.

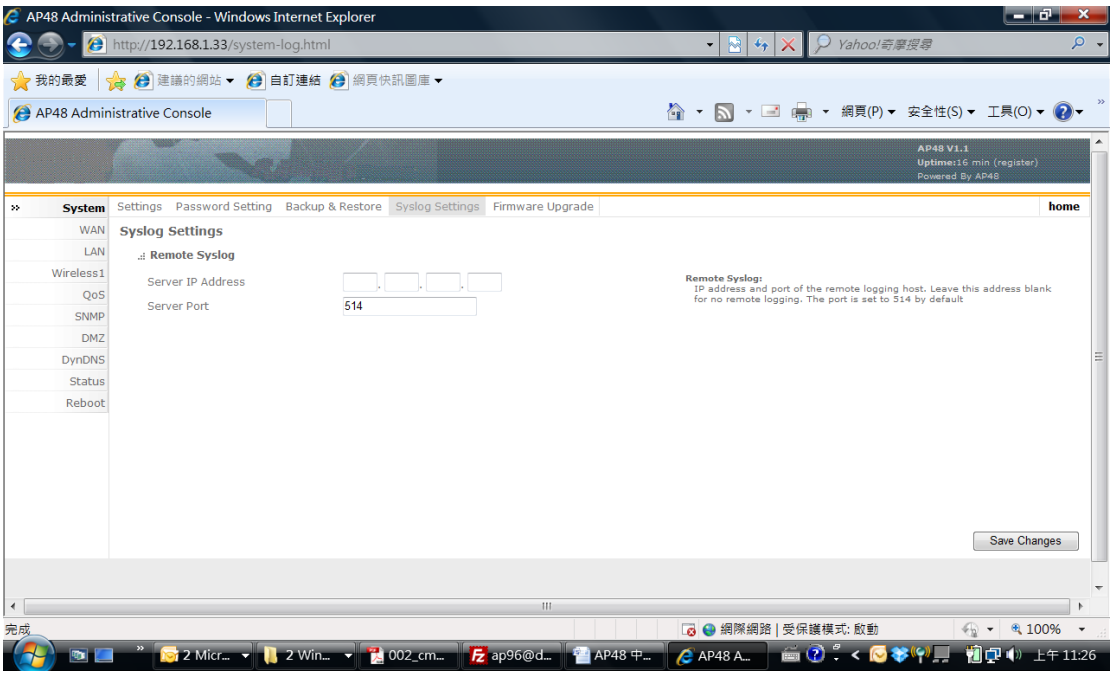


6.4.1.4 SYSTEM – SYSLOG SETTINGS

The AP supports a logging process that controls error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating AP and network problem.

Remote Syslog: Enable the logging process when a server IP address is configured.

- **Server IP Address:** The IP address of a Syslog server.
- **Server Port:** By default, the port used to listen for UDP syslog messages is 514. If you specify another port, it must be in the range of 1024 to 65535.



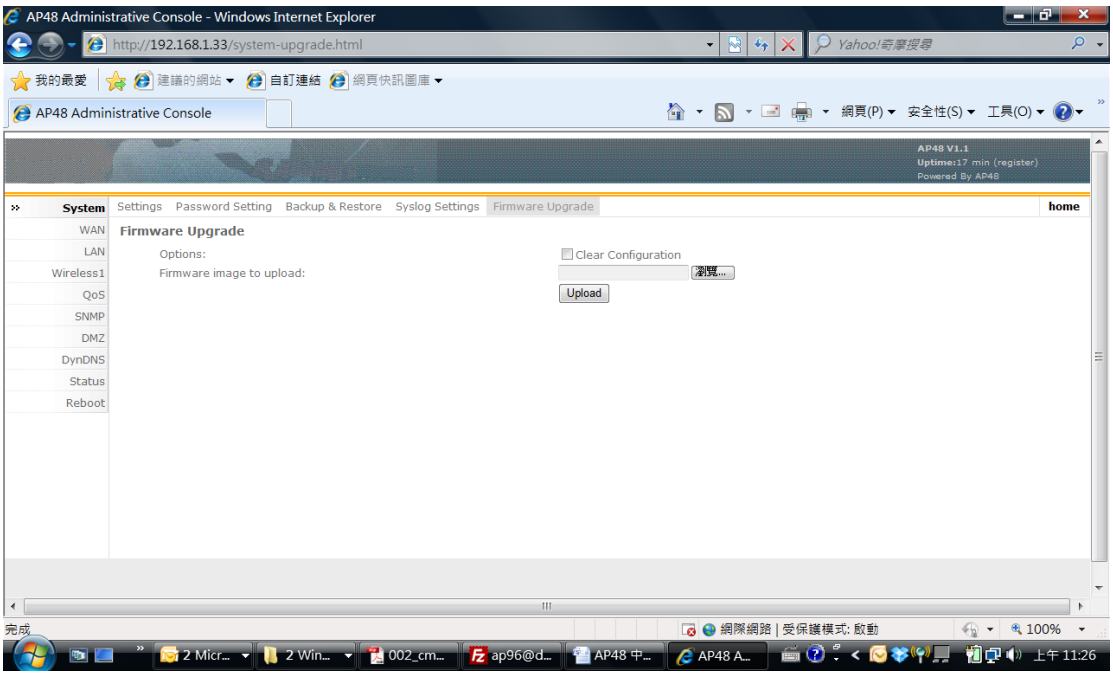
The firmware upgrade page allows you to download a new software code file from the local web management station to the AP using HTTP.

After upgrading to new software, the unit reboots automatically.

The displayed items on this page can be described as follows:

Clear Configuration: Check the box to clear the current configuration and return to factory default when uploading new firmware.

- **Firmware Image to upload:** Specify the name of the code file on the local web management station. You can use the ***Browse*** button to locate the image file locally on the management station. Click the ***Upload*** button to start the download process. Be sure to allow enough time for the download to complete before rebooting the AP.



QOS

QOS SETTINGS

Wireless networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia applications (with audio and video) are particularly sensitive to the delay and throughput variations that result from this equal opportunity wireless access method.

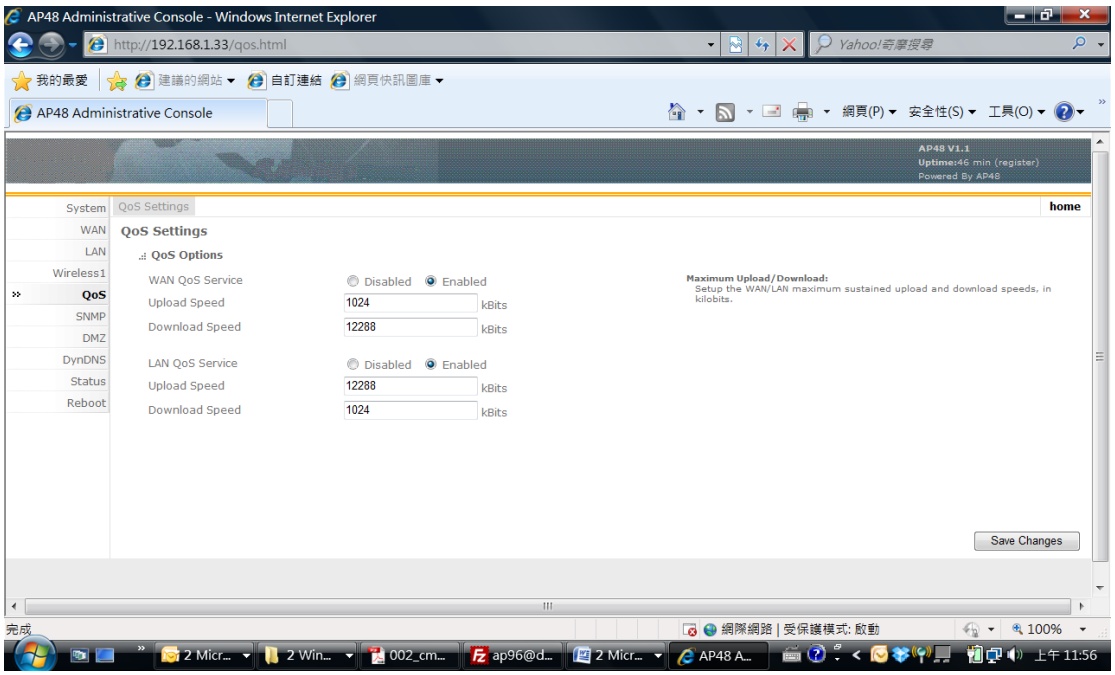
For multimedia applications to run well over a wireless network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an “enhanced opportunity” wireless access method.

The AP51 implements QoS using the Wi-Fi multimedia (WMM) standard. Using WMM, the min router is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the IEEE 802.11e QoS standard and it enables the AP51 to interoperate with both WMM-enabled clients and other devices that may lack any WMM functionality.

The QoS settings page allows you to enable the QoS settings and specify the WAN upload and download speeds.

- **WAN QoS Service:** Enables QoS settings of the AP51. (Default: disabled).

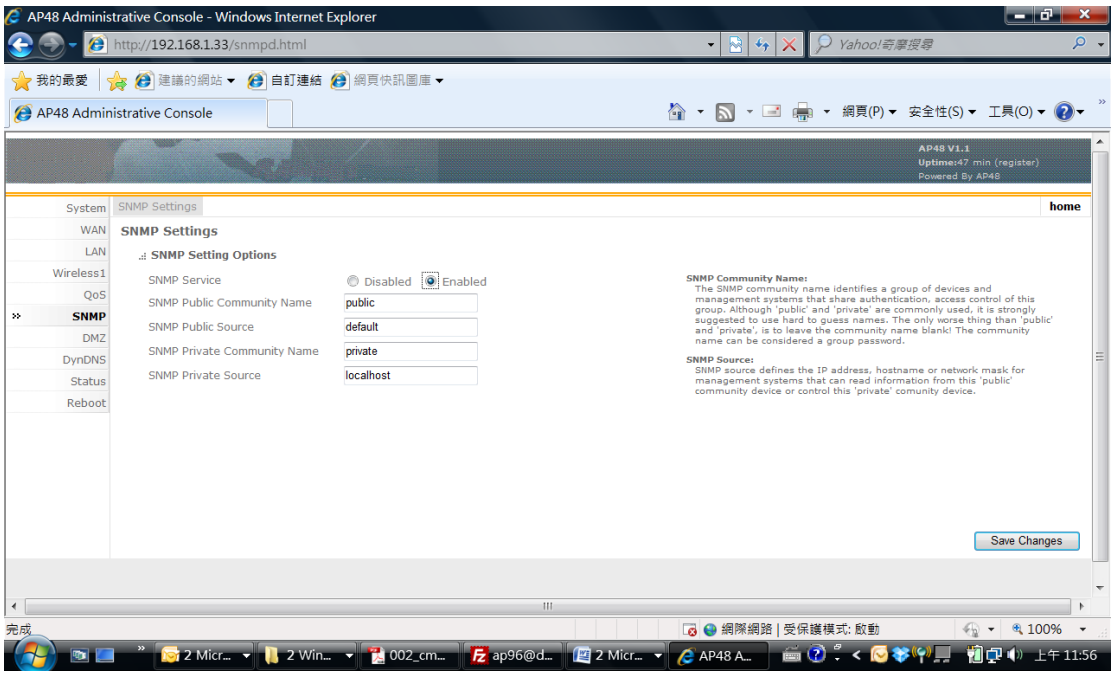
- **WAN Upload Speed / Download Speed:** The maximum upload and download speeds of the internet connection on the WAN port. It is recommended that you set these values at between 85-90% of your true speeds. (Used in kilobits)
- **LAN QoS Service:** Enables WAN QoS settings of the AP51. (Default: Disabled)
- **LAN Upload Speed / Download Speed:** The maximum upload and download speeds of the LAN port. It is recommended that you set these values at between 85-90% of your true speeds. (Used in kilobits)



SNMP

SNMP – SETTINGS

- **SNMP Service:** Enable or disable the SNMP service.
- **SNMP Public / Private Community Name:** SNMP community name identifies a group of advices and management systems that share authentication, access control of this group. Although ‘public’ and ‘private’ are commonly used, it is strongly suggested to use hard to guess names. The only worse thing than ‘public’ and ‘private’, is to leave the community name blank! The community name can be considered a group password.
- **SNMP Public / Private Source:** SNMP source defines the IP address, hostname or network mask for management systems that can read information from this ‘public’ community device or control this ‘private’ community device.



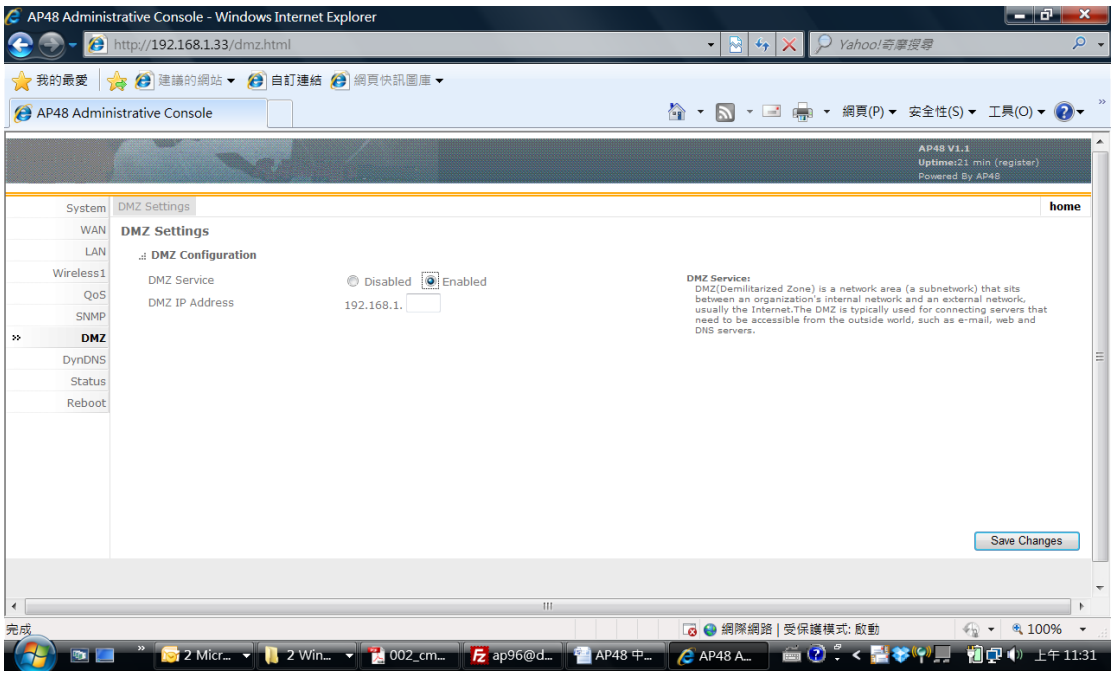
1.3.2 DMZ

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way internet access by defining a virtual-DMZ (virtual-demilitarized-zone) host.

DMZ (Demilitarized Zone) is a network area, (a sub network) that sits between an organization's internal network and an external network, usually the Internet. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.

- **DMZ Service:** Enables the DMZ feature. (Default: Disabled)
- **DMZ IP Address:** Specifies the IP address of the virtual DMZ host.

Note: Adding a host to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.



1.3.3 DYNDNS

Dynamic DNS (DDNS) provides users on the Internet with a method to tie a specific domain name to the unit's dynamically assigned IP address. DDNS allows your domain name to follow your IP address automatically by changing your DNS records when your IP address changes.

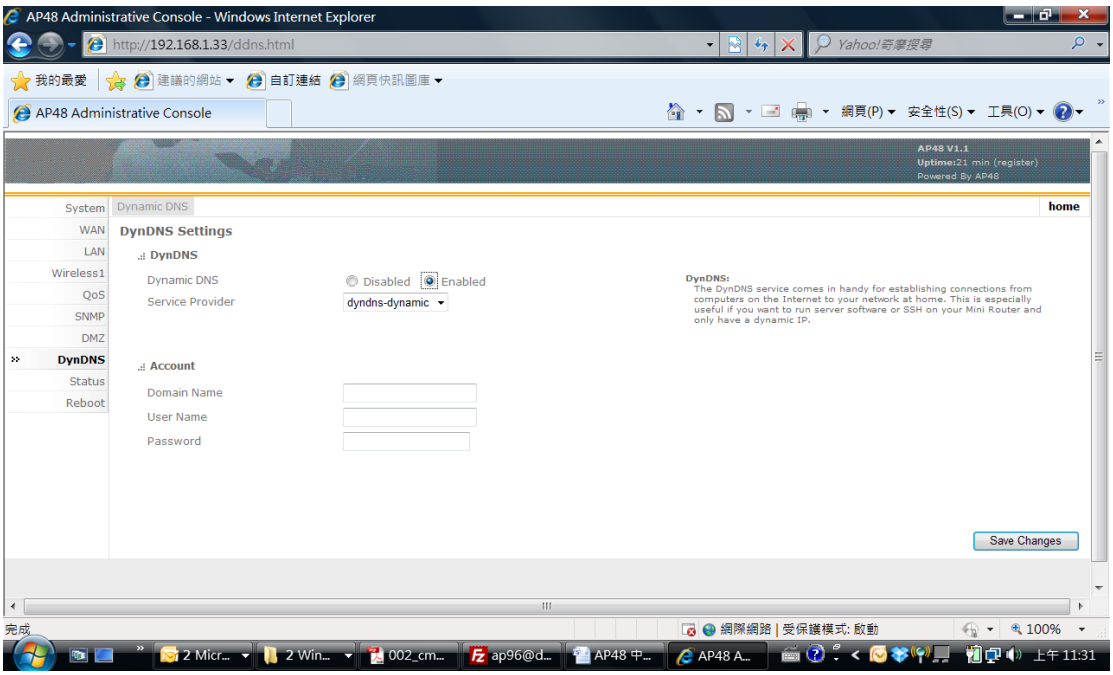
The DynDNS service comes in handy for establishing connection from computers on the Internet to your network at home. This is especially useful if you want to run server software or SSH on your Mini Router and only have a dynamic IP.

DynDNS:

- **Dynamic DNS:** Enable the Dynamic DNS of the AP.
- **Service Provider:** Specify the DDNS service provider.

Account:

- **Domain Name:** Specify the prefix to identify your presence on the DDNS server.
- **User Name:** Specify your username for the DDNS service.
- **Password:** Specify your password for the DDNS service.



1.3.4 STATUS

The status pages display details on the current configuration and status of the Mini AP Router, including associated wireless stations and event log messages.

System: Display the basic device information:

- ✧ **Device Name:** The device name and model number.
- ✧ **Firmware Version:** The version number of the current AP firmware.
- ✧ **Wire Interface:** The MAC address of the wired interface.
- ✧ **Wireless Interface:** The MAC address of the wireless interface.

WAN: Displays the basic WAN status.

- ✧ **Gateway:** Display the gateway IP.
- ✧ **IP Address:** The IP address specified or assigned by the Internet Service Provider.
- ✧ **DNS Server 1:** Address of the ISP's DNS server.

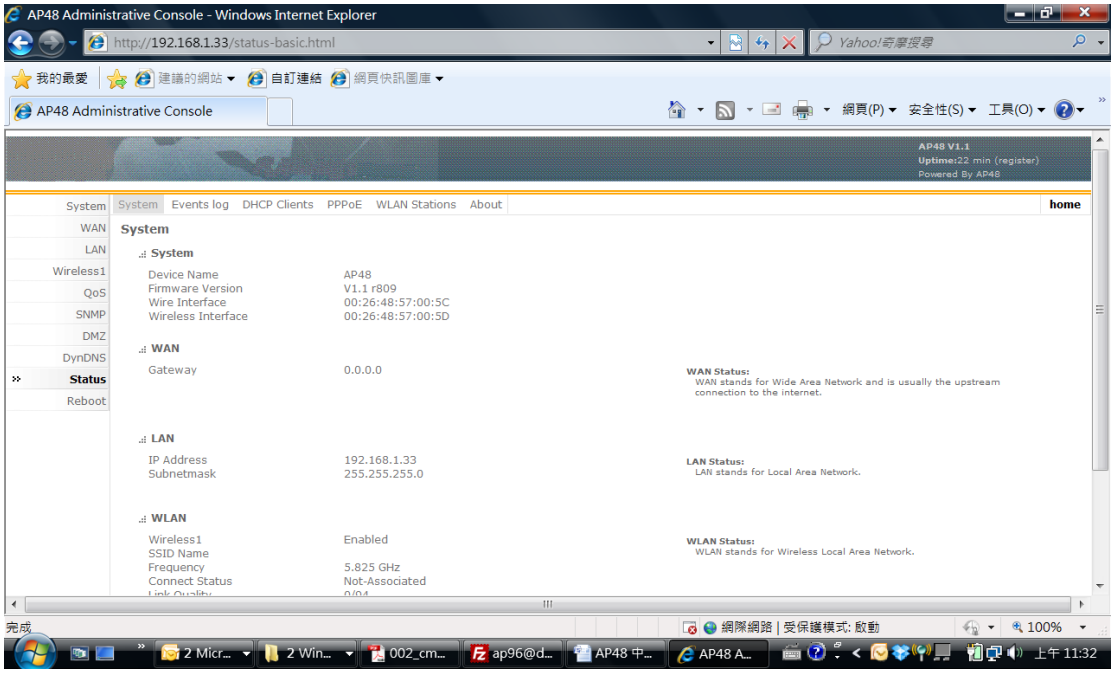
LAN: Displays the basic LAN status.

- ✧ **IP Address:** The IP address configured on the AP.
- ✧ **Subnet mask:** The subnet mask configured on the AP.

WLAN: Displays the basic WLAN information:

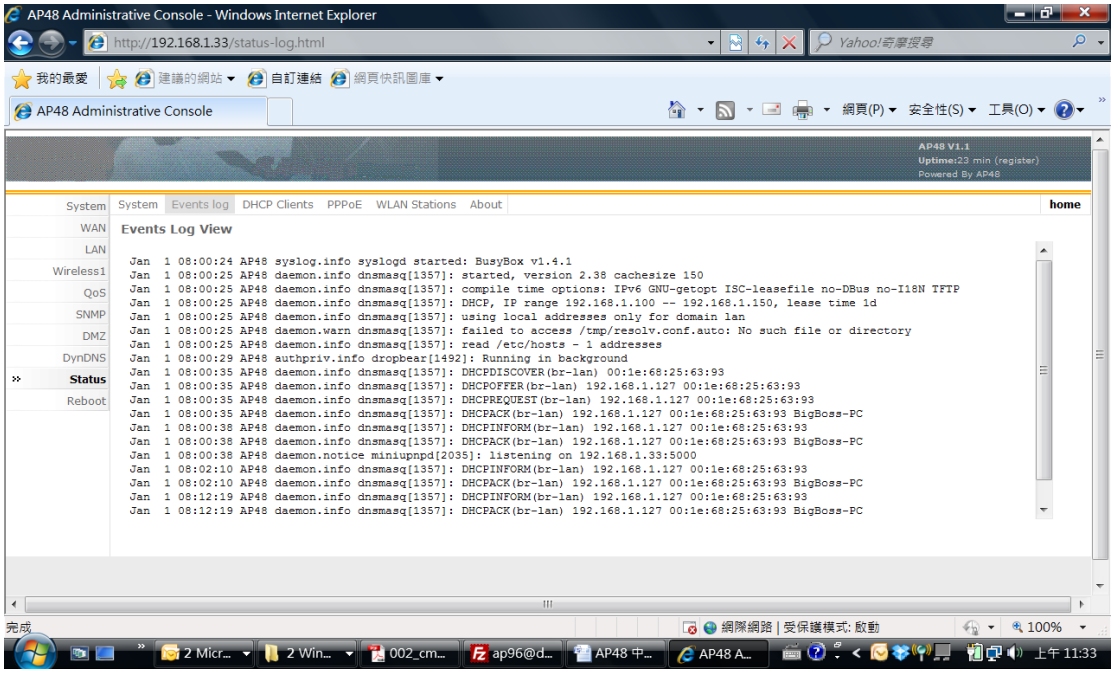
- ✧ **Wireless:** The status of the wireless interface. (enabled / disabled).
- ✧ **SSID Name:** The service set identifier for this wireless group.
- ✧ **Frequency:** The channel frequency being used by the radio.

- **MAC Address:** The MAC address of the WLAN interface.
- **Encryption:** The encryption used by the VAP interface.

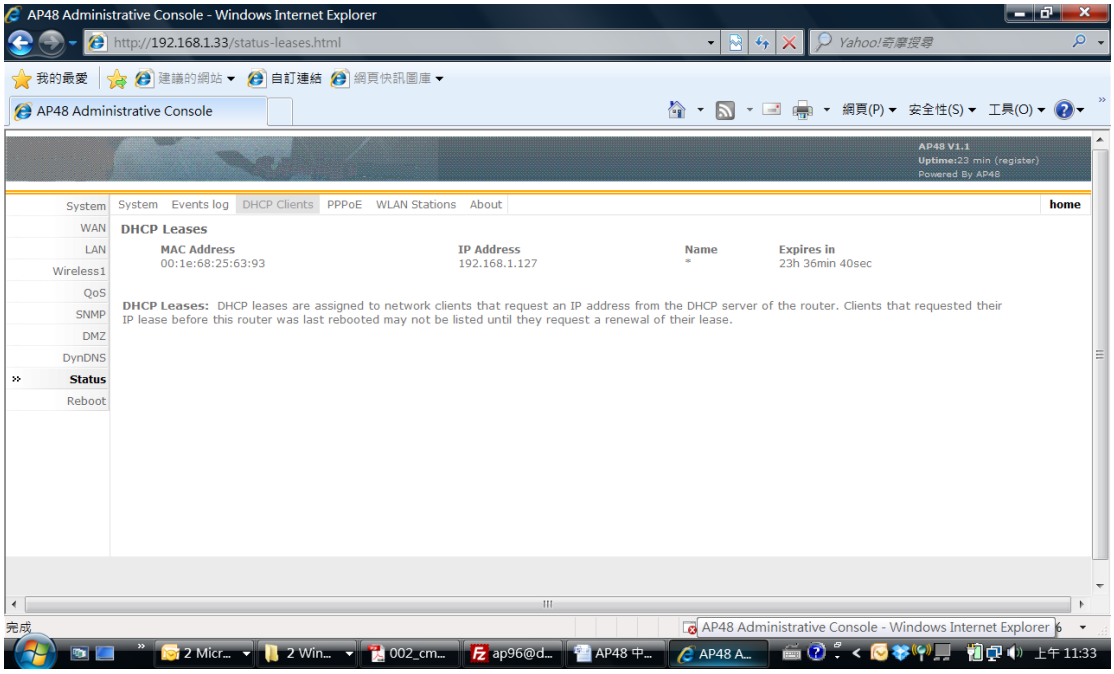


The Event Log page displays system messages generated during system operation. The logged messages can serve as a valuable tool for isolating AP and network problems.

The Event Log page displays the latest messages logged in chronological order, from the newest to the oldest. Log messages saved in the AP's memory are erased when the device is rebooted.



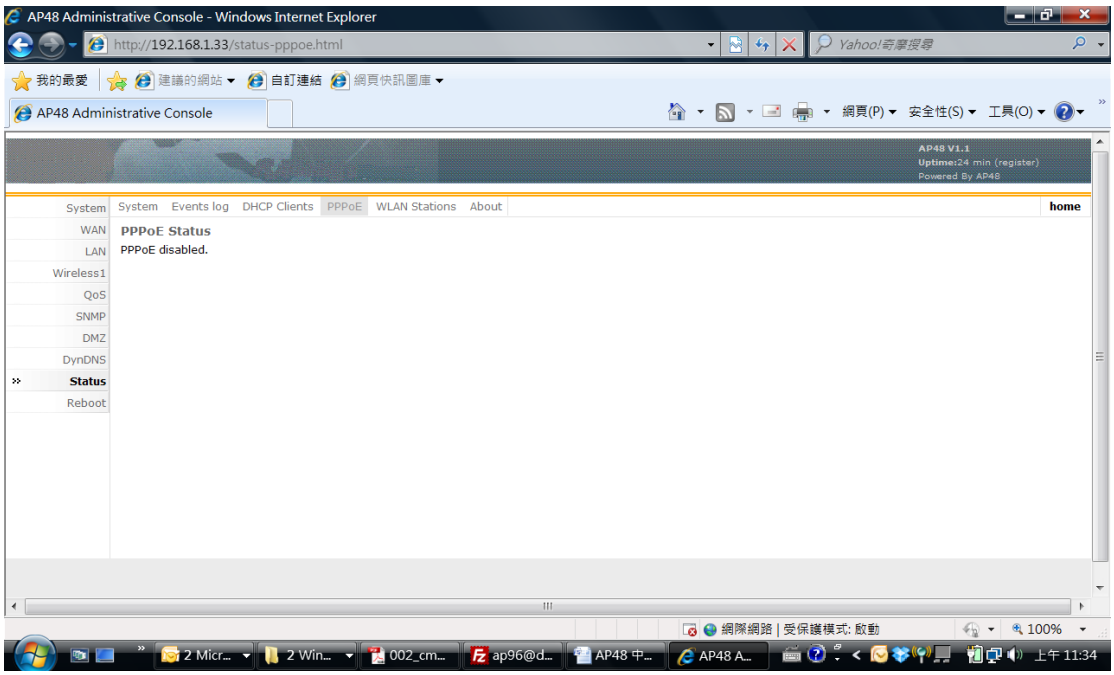
The network information page displays the current Dynamic Host Configuration Protocol (DHCP) client's status. The displayed settings are for status information only and are not configurable on this page.



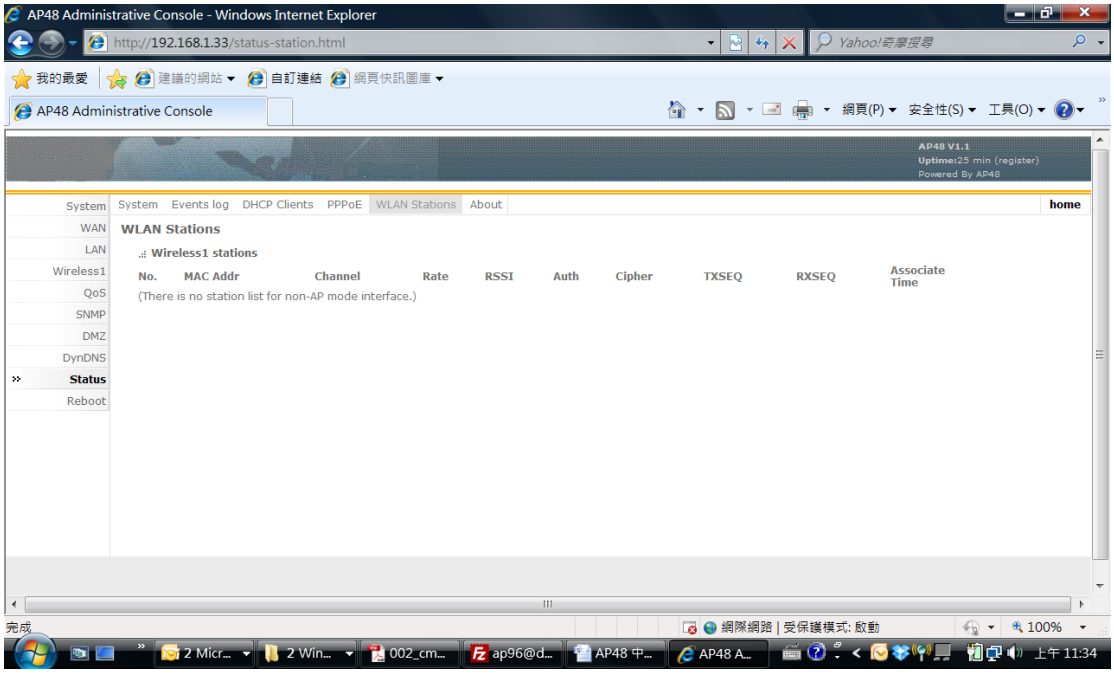
The PPPoE Status page displays the current Point-to-Point Protocol over Ethernet (PPPoE) status. The displayed settings are for status information only and are not configurable on this page.

It is possible to reconnect by pressing the ***Reconnect*** button.

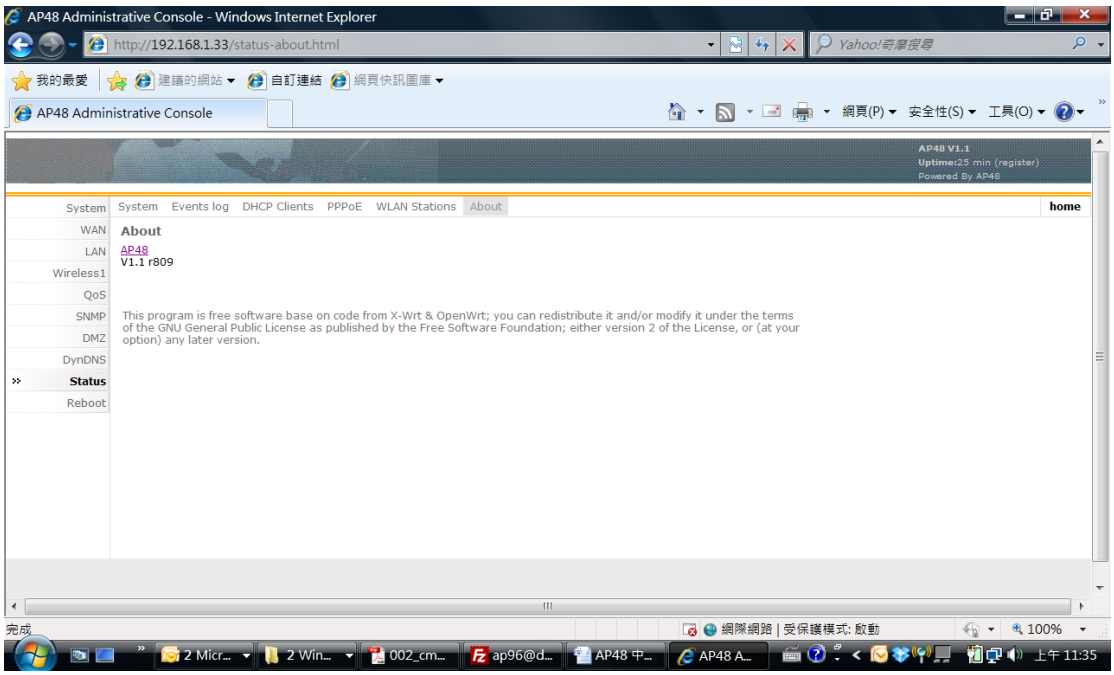
It is possible to Disconnect and Connect manually by pressing the ***Disconnect*** and ***Connect*** buttons.



The WLAN Stations page displays the wireless station status. The displayed settings are for status information only and are not configurable on this page.



The ‘About’ page displays the software version and status installed in the AP.



1.3.5 REBOOT

The Reboot page allows you to restart the AP software and restore factory default settings.

Reboot AP: Click the ‘Reboot device now’ button to reboot the system.

Restore Factory Settings: Click the ‘***Reset to factory default now***’ button to reset the configuration setting for the AP to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to use the default IP address to re-gain management access to the AP.

Note: If you have upgraded the system software, then you must reboot the AP to implement the new code.

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 50cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Professional installation instruction

Please be advised that due to the unique function supplied by this product, the device is intended for use with our interactive entertainment software and licensed third-party only. The product will be distributed through controlled distribution channel and installed by trained professional and will not be sold directly to the general public

through retail store.

1. Installation personal

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location

The product shall be installed at a location where the radiating antenna can be kept 50cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna

Use only the antennas which have been approved by Emitech. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.

4. Installation procedure

Please refer to user's manual for the detail.

5. Warning

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.