CANYON

CNP-WF514A

Wireless Broadband Router

User Manual

Table of Contents

Thank you for purchasing **CANYON CNP-WF514A**. We sincerely wish you to enjoy the wireless broadband router. It provides user an easy and stable high speed internet connection. It is also equipped with built-in NAT technology that acts as a firewall to protect the network from outside intrusions. Ultimately, the device is implemented with an IEEE 802.11b/g access point which is capable of wireless LAN network. To fully utilize the functions and features of **CANYON CNP-WF514A**, please read through the user manual before you get started.

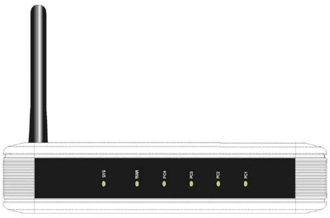
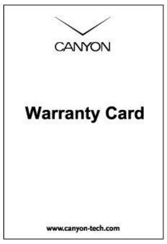
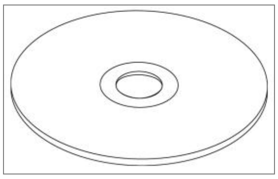
Introduction

Safety Precautions

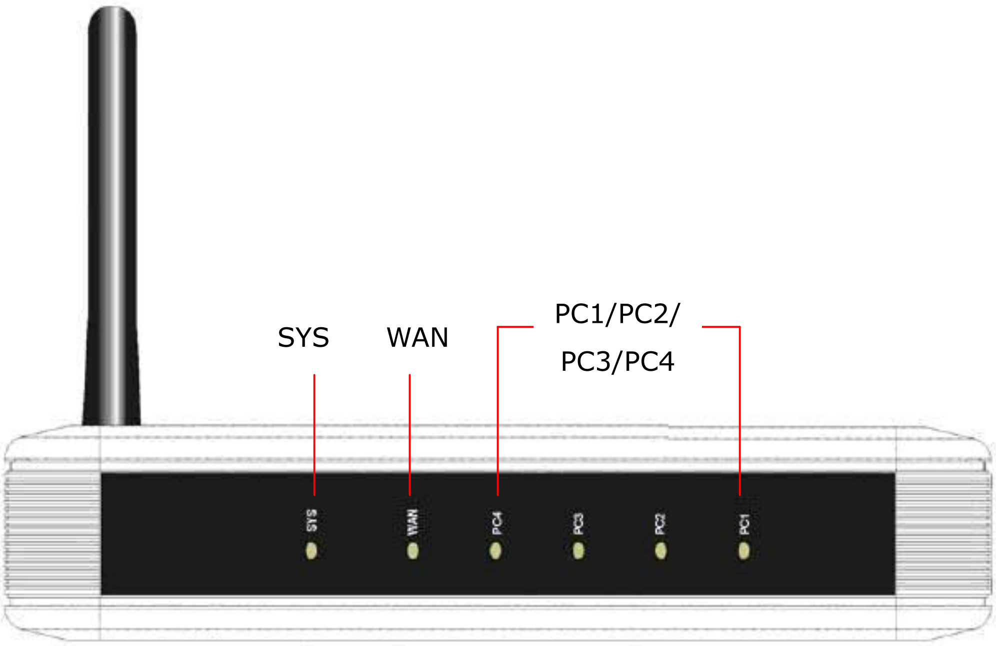
Please observe all safety precautions before using the device. Please follow all procedures outlined in this manual to properly operate the device.

- Do NOT attempt to disassemble or alter any part of the device that is not described in this guide.
- Do NOT place the device in contact with water or any other liquids. The device is NOT designed to be liquid proof of any sort.
- In the event of liquid entry into device interior, immediately disconnect the device from the computer. Continuing use of the device may result in fire or electrical shock. Please consult your product distributor or the closest support center.
- To avoid risk of electrical shock, do not connect or disconnect the device with wet hands.
- Do NOT place the device near a heat source or directly expose it to flame.
- Never place the device in vicinity of equipments generating strong electromagnetic fields. Exposure to strong magnetic fields may cause malfunctions or data corruption and loss.
- All images in the user manual are for user reference only. Actual products might differ slightly than images shown here.

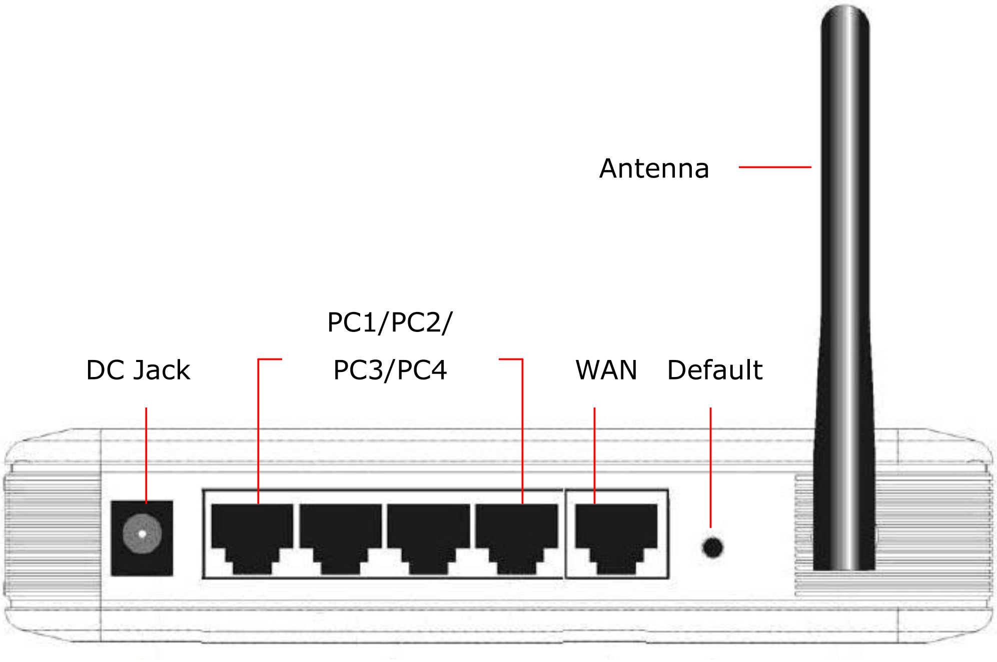
Package Contents

Product Image	Item Name
	**CNP-WF514A** Main Unit
	Standing Base
	Power Adapter
	Warranty Card
	Quick Guide
	Documentation CD

Hardware Overview



SYS	Power status indicator
WAN	WAN interface status indicator
PC1/PC2/PC3/PC4	LAN interface status indicator



DC Jack	Connects to power adapter
WAN	Connects to cable/DSL modem or other Ethernet devices
PC1/PC2/PC3/PC4	Connects to LAN port on PC or other Ethernet devices
Default	Reset device to factory default settings
Antenna	Transmits signals

Getting Started

Connecting to Device

Please follow the steps below to connect the modem and PC(s) with **CANYON CNP-WF514A**:

1. Begin by searching for an appropriate location to setup device. Please keep in mind to keep the device in the center of working area as the signal strength and data transfer rate falls off with distance.

2. It is also recommended to place device at a higher position to ensure minimum obstacle interference.

3. Make sure that all network devices are powered off, including the device itself, PCs, switches, cable or DSL modem, and other peripherals.

4. Connect the modem to WAN port of the device by one CAT 5 Ethernet cable.

5. Connect PC(s) with the LAN ports (PC1/PC2/PC3/PC4) of the device by CAT 5 Ethernet cables. One PC connects to only one port using one cable.

6. Power on the cable or DSL modem.

7. Plug in the power of the device. The Power status indicator at the front panel of device will light up as soon as the power adapter is connected properly.

8. Power on PC(s).

Windows XP Setup

1. Click on Start → Settings → Control Panel.
2. Click on Network and Internet Connections icon.
3. Click on Network Connections
4. Right click on Local Area Connection icon and click on Properties.
5. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.
6. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
7. Click Ok to confirm modifications.

Windows Vista Setup

1. Click on Start → Settings → Network Connections.
2. Right click on Local Area Connection icon and click on Properties.
3. Click on Continue in User Account Control dialog box.
4. Select TCP/IPv4 option and click on Properties. The Properties dialog box will be displayed.
5. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
6. Click Ok to confirm modifications.

Windows 2000 Setup

1. Click on Start → Settings → Control Panel.
2. Double click on Network and Dial-up Connections icon. The Network dialog box will be displayed.
3. Right click on Local Area Connection icon and click on Properties.
4. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.
5. Check "Obtain an IP address automatically" and "Obtain DNS server address automatically" options.
6. Click Ok to confirm modifications.

Windows 98/ME Setup

1. Click on Start → Settings → Control Panel.
2. Double click on Network icon. The Network dialog box will be displayed.
3. Please make sure that appropriate network card is installed before proceeding. Click on the Configuration label.
4. Select TCP/IP option and click on Properties. The Properties dialog box will be displayed.

NOTE:
Select the TCP/IP item with an arrow "→" pointing to the network card if more than one TCP/IP options is present.

5. Make sure that the option "Obtain IP address automatically" is checked.
6. Make sure that the "WINS Resolution" option is checked under WINS Configuration dialog box.

7. From Gateway dialog box, remove all entries from the Installed gateways by selecting them and clicking on Remove.
8. From DNS Configuration dialog box, remove all entries from DNS server search order box and Domain suffix search order box by selecting them and clicking on Remove. Click on Disable DNS.
9. Click Ok to confirm modifications.

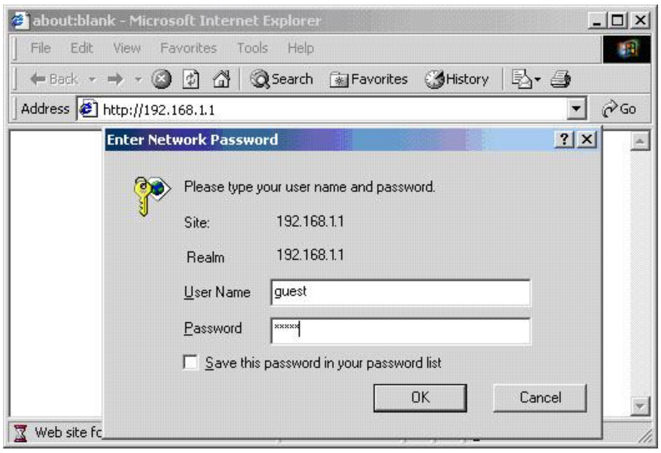
NOTE:

To access the device via a wireless connection, PC must be equipped with 802.11b or 802.11g wireless adapter/PCI card. The configuration should be set as below:

- Operation Mode: Infrastructure
- SSID: Default
- Authentication: Disabled
- Encryption: Off

Device Configuration

Before setting up the device, please make sure that the host PC(s) is set on the IP sub-network accessible by **CANYON CNP-WF514A** device. The default network address of the device is set as 192.168.1.1. Please configure IP address of host PC at 192.168.1.XXX where XXX is a number between 002 and 254. The subnet mask should be 255.255.255.0. Please follow below steps to enter web browser management mode.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Web site fc

http://192.168.1.1

Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

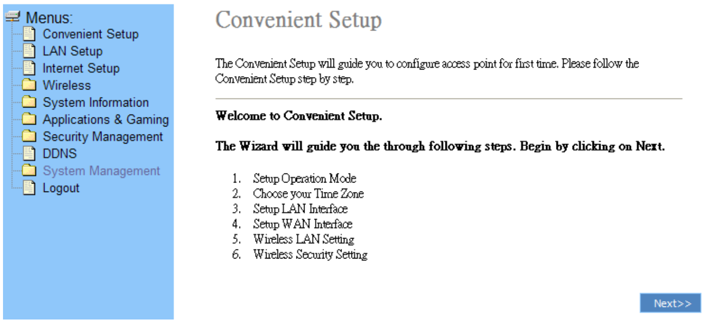
Realm 192.168.1.1

User Name guest

Password *****

□ Save this password in your password list

1. Open a browser (**Internet Explorer browser only**) and type in "192.168.1.1" at the address bar and press Enter.
2. Type "guest" at the user name text box and "guest" again at the password text box.



Convenient Setup

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

Welcome to Convenient Setup.

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

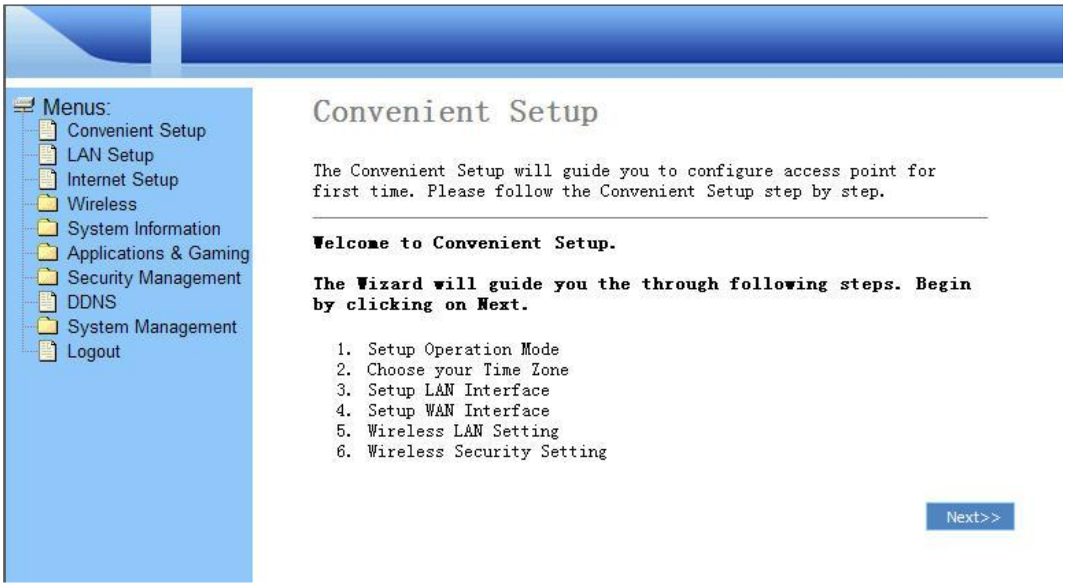
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

3. The home page of web browser management mode will be displayed.
4. Click on 10 different functions on the main router menu on the left. The corresponding information will be displayed at right.
5. Click on Help at any time to bring up help menu.

NOTE:

The factory settings of user name and the password are by default "guest". It is recommended that user change that information to better maintain network security.

Convenient Setup



Convenient Setup

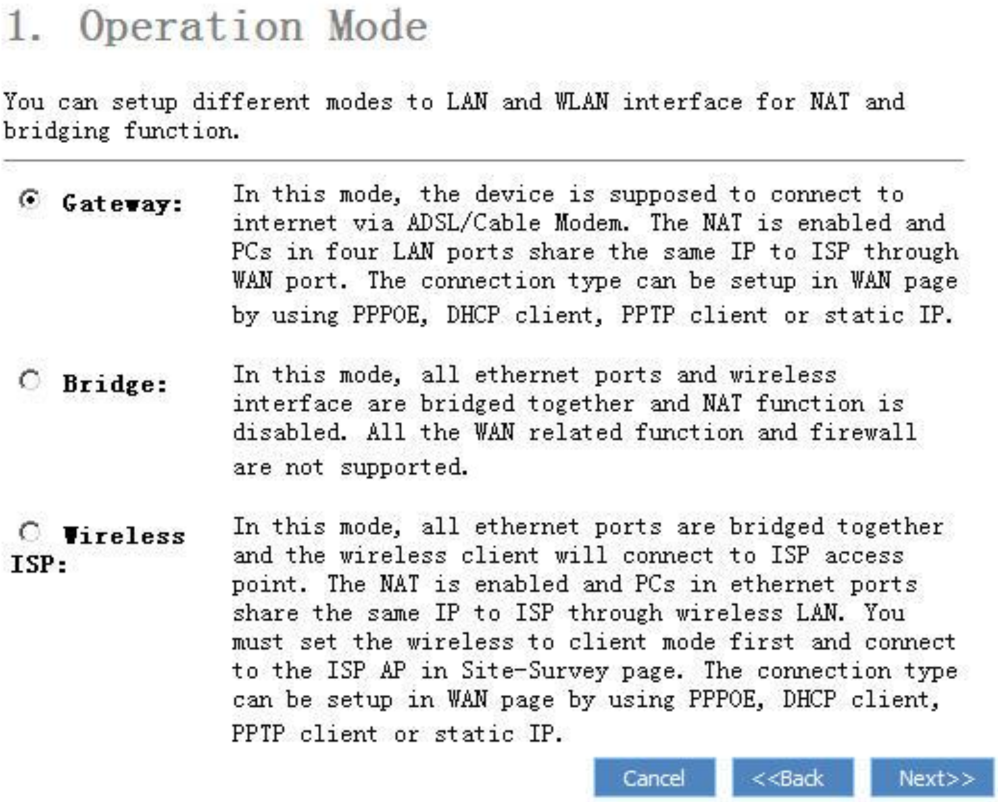
The Convenient Setup will guide you to configure access point for first time. Please follow the Convenient Setup step by step.

Welcome to Convenient Setup.

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 Interface
5. Wireless LAN Setting
6. Wireless Security Setting

1. Click on **Convenient Setup** function at the main router menu on the left.
2. Click on **Next>>** to continue **Convenient Setup** process.



1. 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 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.

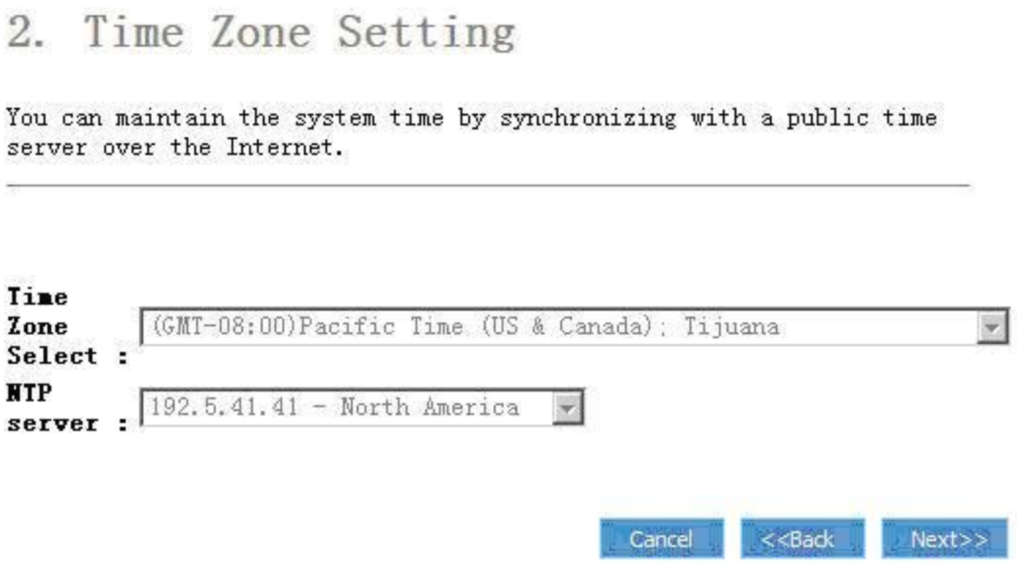
○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey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

1. Select and click on different connection mode options to adapt to desired function.

NOTE:

Please consult IT professionals to select best connection mode.

2. Click on **Next>>** to continue or **<<Back** to go back to previous page.
3. Click on **Cancel** to exit.



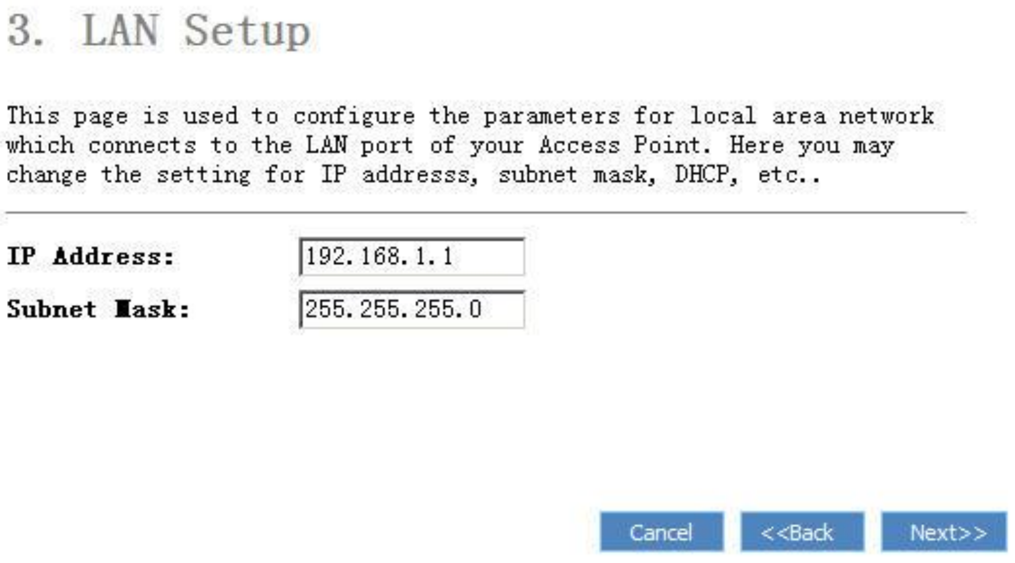
2. Time Zone Setting

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

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

NTP server : 192.5.41.41 - North America

1. Select desired time zone from **Time Zone Select** drop down text box.
2. Select time server from **NTP server** drop down text box to synchronize time setting.
3. Click on **Next>>** to continue or **<<Back** to go back to previous page.
4. Click on **Cancel** to exit.



3. LAN Setup

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

IP Address: 192.168.1.1

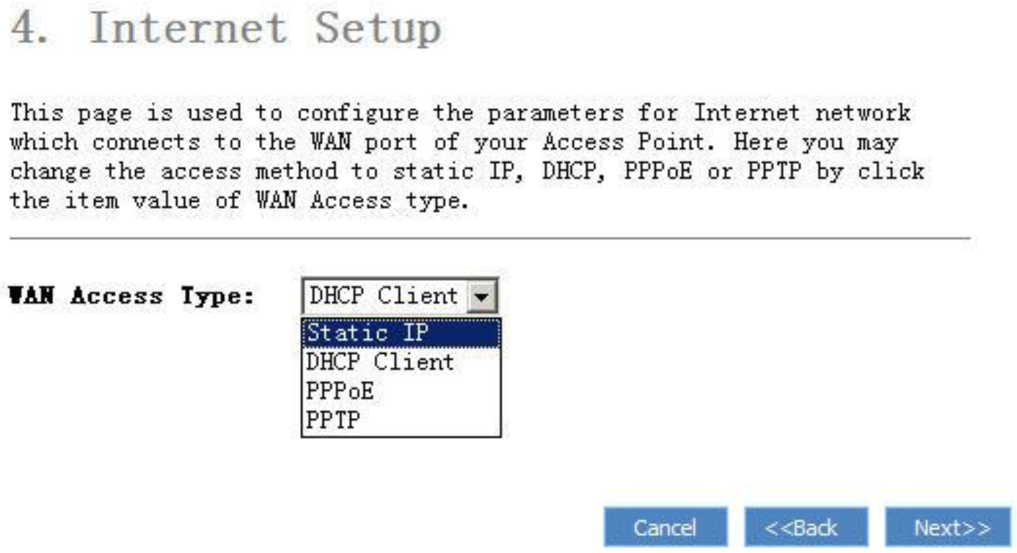
Subnet Mask: 255.255.255.0

1. Type in device **IP address** and **Subnet Mask** in the corresponding textbox.

NOTE:

The default settings are **192.168.1.1** and **255.255.255.0**.

2. Click on **Next>>** to continue or **<<Back** to go back to previous page.
3. Click on **Cancel** to exit.



4. Internet Setup

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

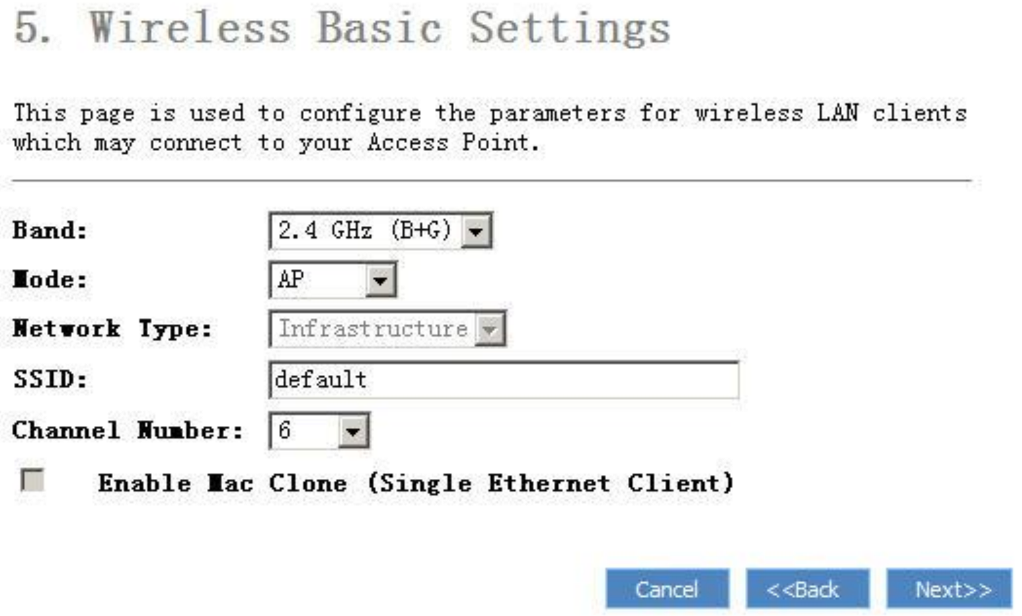
WAN Access Type: DHCP Client

1. Select desired Internet connection method (**Static IP**, **DHCP Client**, **PPPoE**, and **PPTP**) from **WAN Access Type** drop down text box.
2. Type in required parameters if necessary.

NOTE:

Please consult IT professionals and/ or ISP provider to obtain necessary information.

3. Click on **Next>>** to continue or **<<Back** to go back to previous page.
4. Click on **Cancel** to exit.



5. Wireless Basic Settings

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

Band: 2.4 GHz (B+G)

Mode: AP

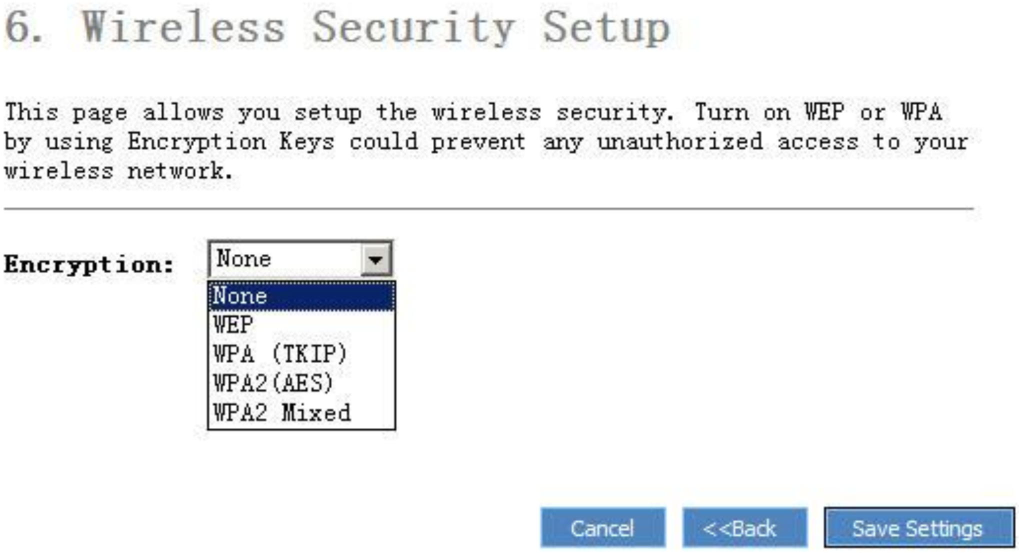
Network Type: Infrastructure

SSID: default

Channel Number: 6

□ Enable Mac Clone (Single Ethernet Client)

1. Select network band from **Band** drop down text box.
2. Select network band, function **Mode** (**AP**, **Client**, **WDS**, and **AP+WPS**), **Network Type** (**Infrastructure** or **Ad-Hoc**), **Channel Number** from their corresponding drop down text box.
3. Type in desired **SSID** in the **SSID** text box.
4. Check on **Enable MAC Clone** option if necessary.
5. Click on **Next>>** to continue or **<<Back** to go back to previous page.
6. Click on **Cancel** to exit.

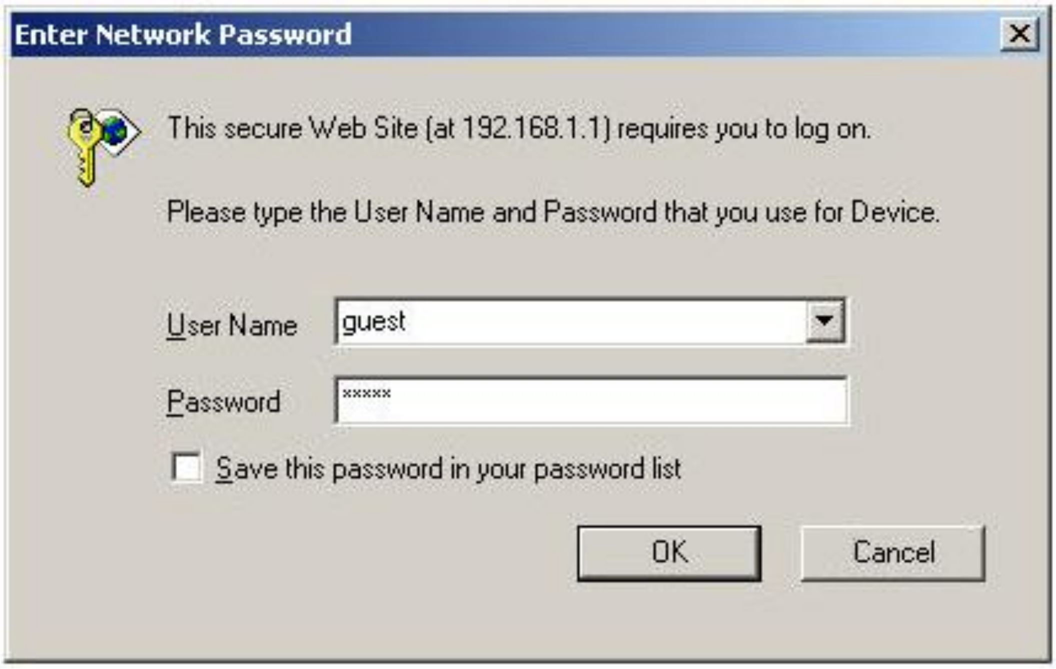


6. Wireless Security Setup

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

Encryption: None

1. Select data encryption type (**None**, **WEP**, **WPA(TKIP)**, **WPA2(AES)**, and **WPA2 Mixed**) from **Encryption** drop down text box.
2. Type in or select required parameters if necessary.
3. Click on **Save Settings** to save adjustment or **<<Back** to go back to previous page.
4. Click on **Cancel** to exit.



Enter Network Password

This secure Web Site (at 192.168.1.1) requires you to log on.

Please type the User Name and Password that you use for Device.

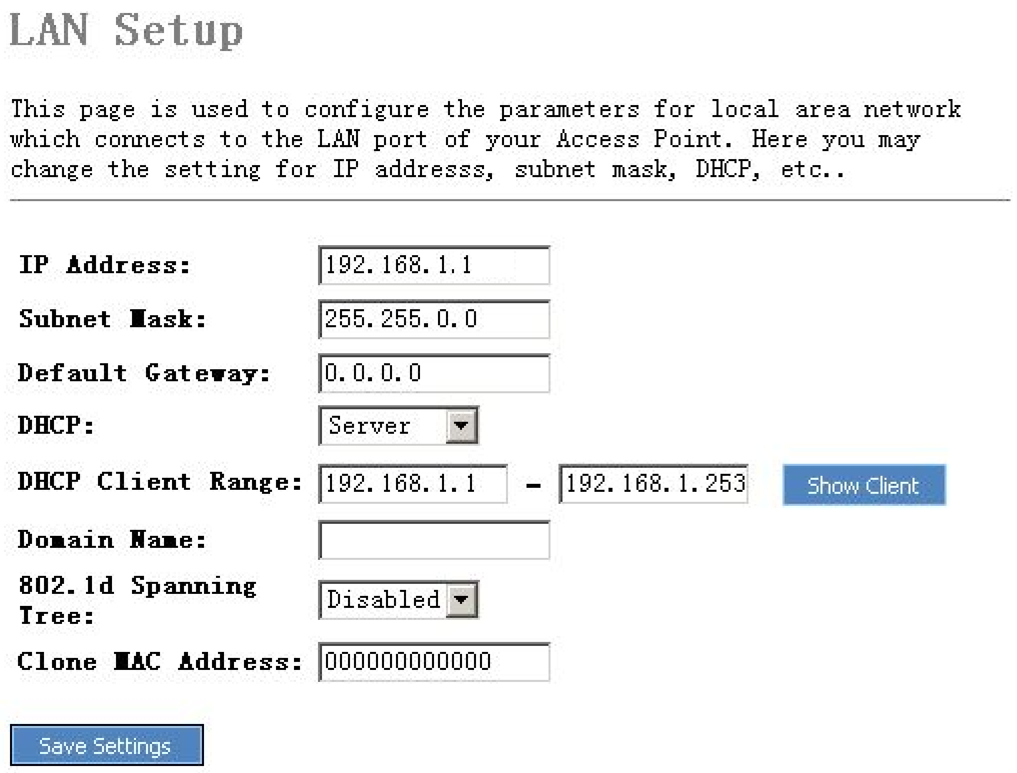
User Name: guest

Password: *****

□ Save this password in your password list

1. Upon completion, type in User **Name** and **Password** as indicated. Click on **OK** to continue or **Cancel** to exit.
2. Click on **OK** again to confirm setting adjustment.
3. The device is now ready for use.

LAN Setup



LAN Setup

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

IP Address:	192.168.1.1
Subnet Mask:	255.255.0.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.1.1 - 192.168.1.253
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

This section allows user specification of private IP address for the device LAN ports and subnet mask for LAN segment.

IP Address

Type in desired IP address for the device at the appropriate text box.

Subnet Mask

Type in desired Subnet Mask for device LAN segment at the appropriate text box.

Default Gateway

Type in Default Gateway as receiving Internet connection at the appropriate text box. The field should be left blank if not connected to Internet.

DHCP

Select **Disabled** to disable DHCP server function. Select **Client** to received IP address from source DHCP server and **Server** to automatically assign IP address to all client devices connected at device LAN ports.

DHCP Client Range

Specify the range of IP addresses allotted for DHCP to assign to clients connected to device. Click on **Show Client** to display all connected client device(s) with attributes such as assigned IP address, MAC Address of client device, and Time expired. Click on **Refresh** to update the table or **Close** to exit.

Domain Name

Type in a Domain Name of DHCP server for the device at the appropriate text box.

802.1 Spanning Tree

Select **Disabled** or **Enable** to disable/enable Spanning tree function.

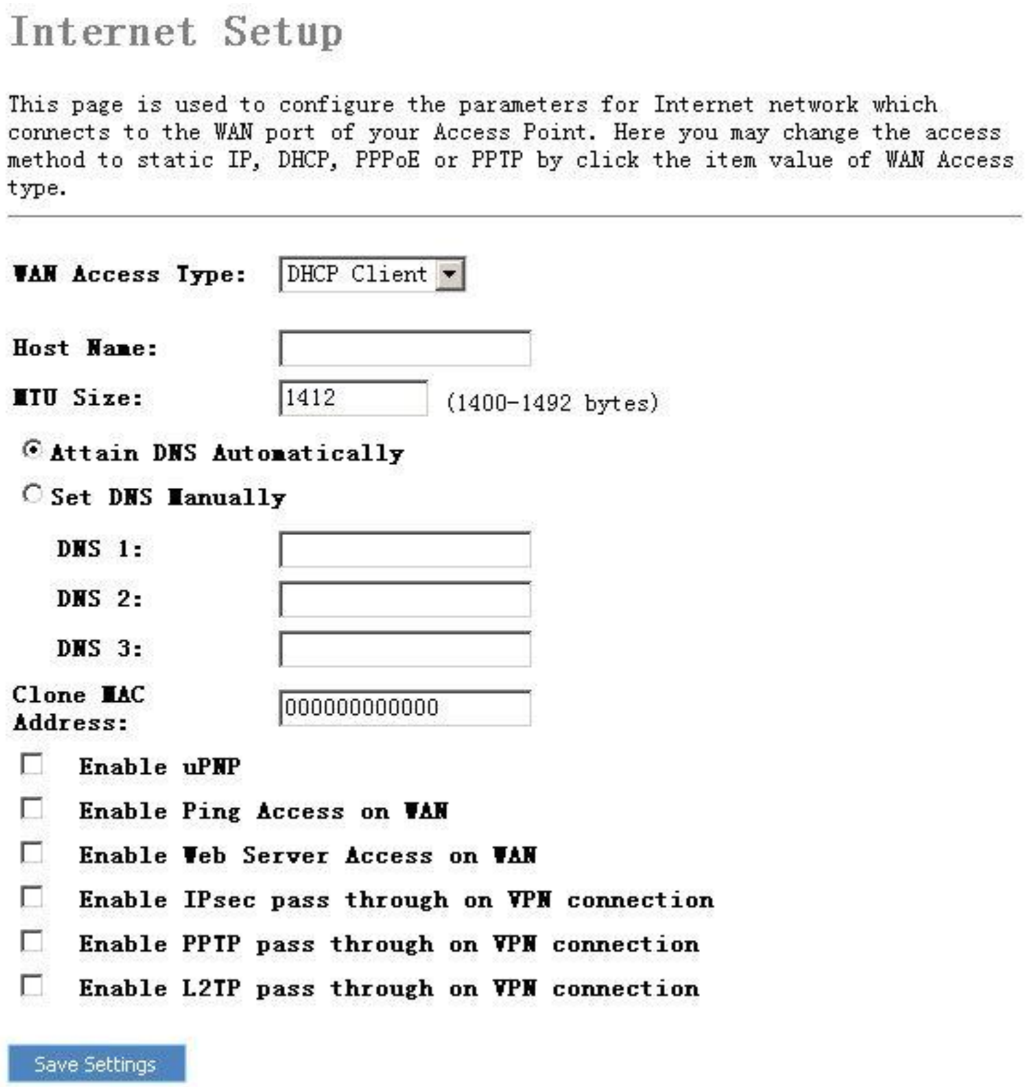
Clone MAC Address

Type in MAC address to replace factory default MAC address.

Save Settings

Click on **Save Settings** to save modifications.

Internet Setup



Internet Setup

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

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1412 (1400-1492 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

□ 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

This section allows adjustment of Internet network connected to device WAN port.

WAN Access Type

Select Internet connection type of **Static IP**, **DHCP Client**, **PPPoP**, and **PPTP**.

NOTE:

Please consult IT professionals and/ or ISP provider to obtain necessary information.

- **Static IP** option:

  Type in **IP address**, **Subnet Mask**, and **Default Gateway** obtained from service provider in the appropriate text box.

- **DCHP Client** option:

  Type in **Host Name** in the text box if required.

- **PPPoE** option:

  Type in **User Name**, **Password**, **Service Name** (Name of service provider) obtained from service provider. Select Connection Type of **Continuous** (non-stop connection), **Connect on Demand** (Connection activated only when associated application is launched), and **Manual** (Manual connection activation/deactivation by clicking on **Connect** or **Disconnect**) from the drop down text box. Type in **Idle Time** (only available in Connect on Demand mode) from 1 to 1000 minutes if necessary.

- **PPTP** option:

Type in **IP address**, **Subnet Mask**, **Server IP Address**, **User Name**, and **Password** obtained from service provider in the appropriate text box.

MTU Size

Enter **MTU** value if required. The default value is set at 1492. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. It is recommended to use the default value of 1492. The value should be set in range of 1200 and 1500 if manual overrides are required. Failure to comply may result in problems such as unable to send Email, or fail to browse website. Please consult ISP for more information.

DNS Server Settings

Select **Attain DNS Automatically** option to automatically extract DNS server address from source. Alternatively, Select **Set DNS Manually** option and type in up to 3 DNS server address.

Clone MAC Address

Type in MAC address to replace factory default MAC address.

Other Options

Click on desired option(s) to enable/disable function. The functions are intended for advanced users only. Please consult with IT Professional before making adjustments.

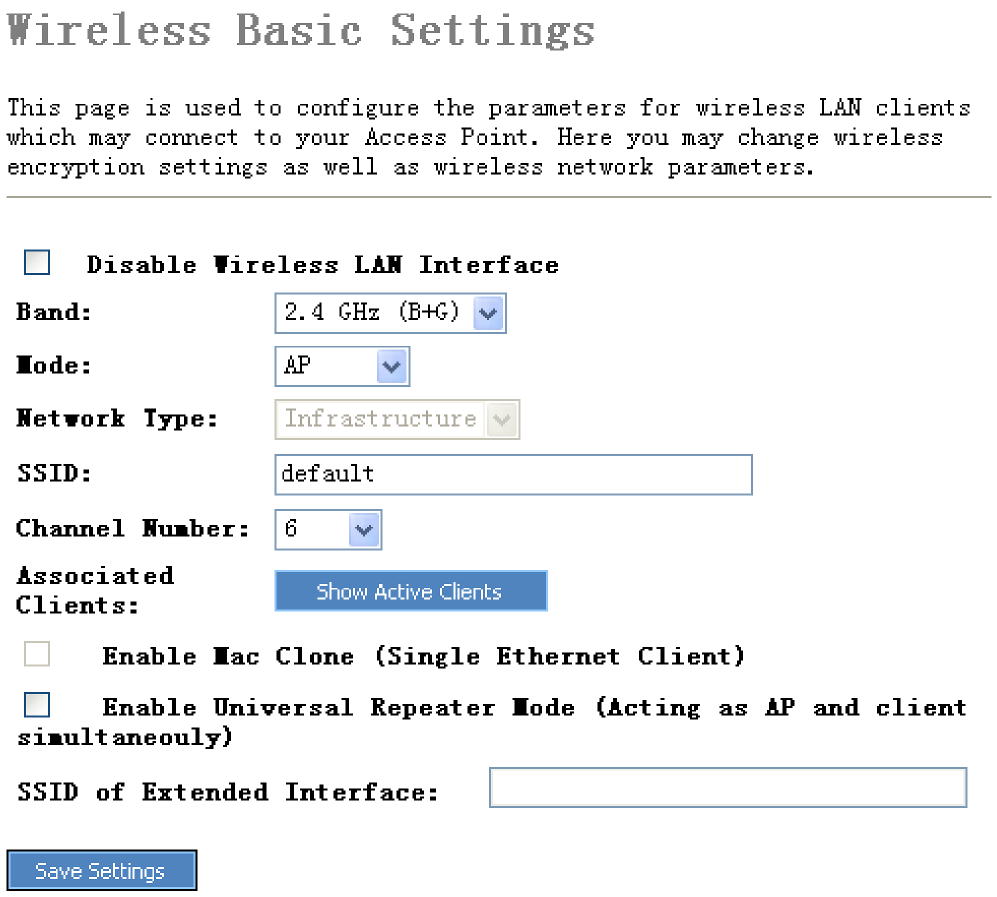
Save Settings

Click on **Save Settings** to save modifications.

Wireless

This section assists user to create a network environment that connects wireless client device(s) to a wired LAN. It also allows wireless stations to access network resources and share the broadband Internet connection. The section is divided into 7 categories as illustrated below.

Basic Setting



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)
Mode:	AP
Network Type:	Infrastructure
SSID:	default
Channel Number:	6
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:

Disable Wireless LAN Interface

Click on the option to disable wireless function. Uncheck to restore.

Band

Select network **Band** of **2.4GHz (B)**, **2.4GHz (G)**, and **2.4GHz (B+G)** from the drop down text box. It is recommended to maintain **2.4GHz (B+G)** network band to accommodate both types of connection.

Mode

Select network **Mode** of **AP**, **Client**, **WDS**, and **AP+WDS** from the drop down text box. **AP** option is set as factory default setting.

Network Type

Select **Network Type** of **Infrastructure** and **Ad hoc** from the drop down text box. **Infrastructure** option is set as factory default setting. This option is only available under **Client Mode**.

SSID

Type in SSID in the appropriate text box. SSID is the handle name that all wireless devices in the network should adapt to. SSID **Default** is set as factory default setting.

NOTE:

It is recommended to change default **SSID** (default) to a unique name for better security.

Channel Number

Select a **Channel Number** (Auto, 1-14) from the drop down text box. All wireless devices in the same network should share the same channel number.

Associated Clients

Click on **Show Active Clients** to display all connected wireless client device(s) with attributes such as MAC Address of client device, TX Packet, RX Packet, TX Rate(Mbps), Power Saving, and Expired Time(s). Click on **Refresh** to update the table or **Close** to exit.

Enable MAC Clone (Single Ethernet Client

Click on **Enable MAC Clone** to copy MAC address of current PC used to configure device to device MAC address. This option is only available under **Client Mode**.

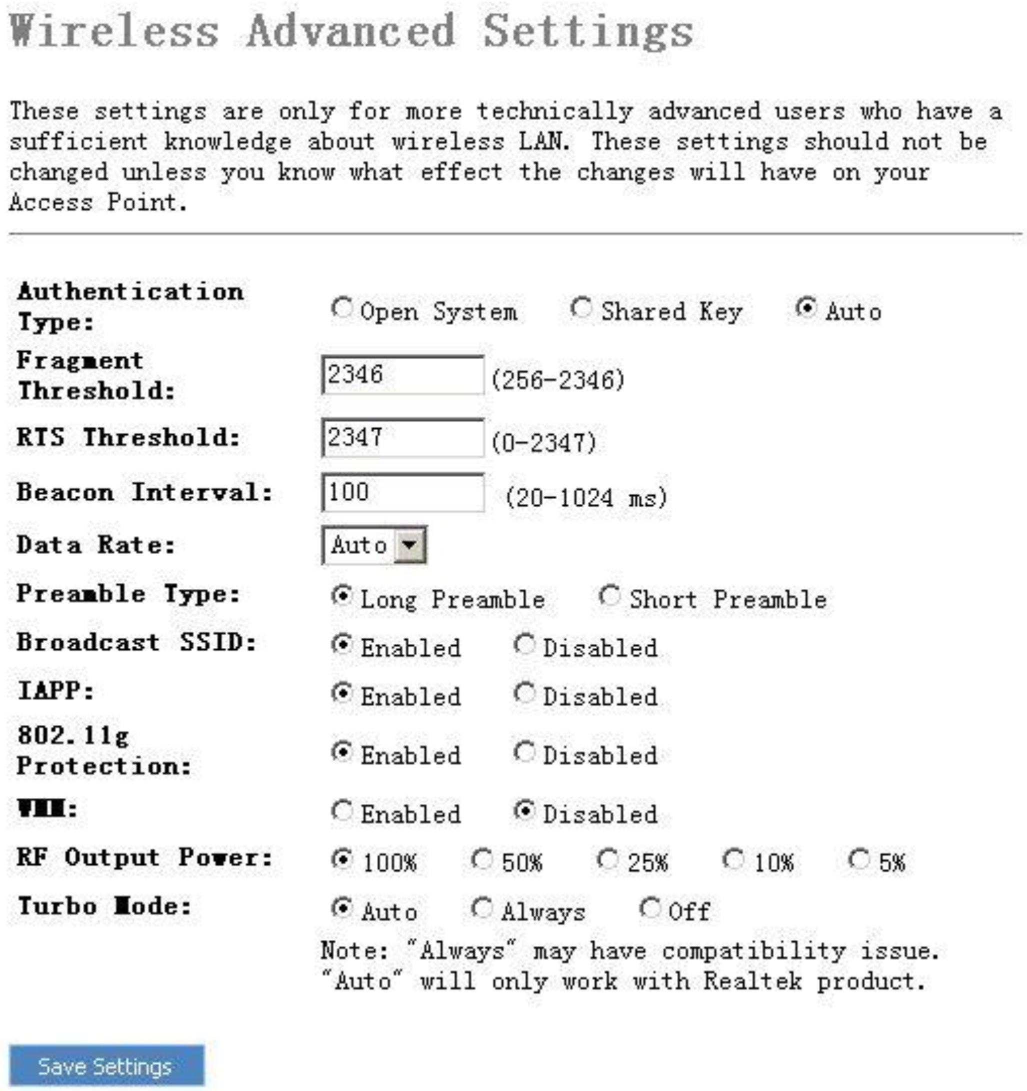
Enable Universal Repeater Mode (Acting as AP and client simultaneously

Click on the option to enable/disable **Universal Repeater Mode**. The device is now able to perform functions in **AP** and **Client Mode** simultaneously. This option is only available under **AP**, **Client**, and **AP+WDS Mode**.

Save Settings

Click on **Save Settings** to save modifications.

Advanced Setting



Wireless Advanced Settings

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

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
IAPP:	● Enabled ○ Disabled
802.11g Protection:	● Enabled ○ Disabled
WMM:	○ Enabled ● Disabled
RF Output Power:	● 100% ○ 50% ○ 25% ○ 10% ○ 5%
Turbo Mode:	● Auto ○ Always ○ Off Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

Authentication Type

Click on **Authentication Type** of **Open System**, **Shared Key**, and **Auto** to designated security type of wireless connection. **Open System** does not provide security measures to wireless device(s) connecting to the device while **Shared Key** offers **WEP** encryption during authentication phase to associate with client device(s). **Auto** allows device to automatically adjust authentication type when associating with client device(s).

Fragment Threshold

Type in **Fragment Threshold** value from 256 to 2346 in the appropriate text box. **Fragment Threshold** value determines the maximum size of packet during the fragmentation of transmitted date.

RTS Threshold

Type in **RTS Threshold** value from 0 to 2347 in the appropriate text box. Device will not use RTS/CTS mechanism to transmit data packets when the packet size is smaller than **RTS Threshold** value.

Beacon Interval

Type in **Beacon Interval** value from 20 to 1024 (ms) in the appropriate text box. Beacon is a signal used to synchronize the wireless network. Device broadcasts beacon signal at a interval defined by the value.

Data Rate

Select **Data Rate** value from 1 to 54 (Mbit/s) from the drop down text box. The device always uses the highest possible data transmission rate to transmit data packets.

Preamble Type

Click on **Preamble Type** (**Long Preamble** or **Short Preamble**) options to determine wireless connection stability. **Long Preamble** option allows better device wireless connection compatibility while **Short Preamble** option offers wireless connection performance.

Broadcast SSID

Click on **Broadcast SSID** options to enable/disable the function. SSID will be broadcasted in the device signal coverage with function enabled.

IAPP

Click on **IAPP** to enable/disable the function. SSID will be broadcasted in the device signal coverage with function enabled.

802.11g Protection

Click on **802.11g Protection** options to enable/disable the function. It is recommended to enable the function to reduce the rate of data collision between 802.11b and 802.11g wireless devices.

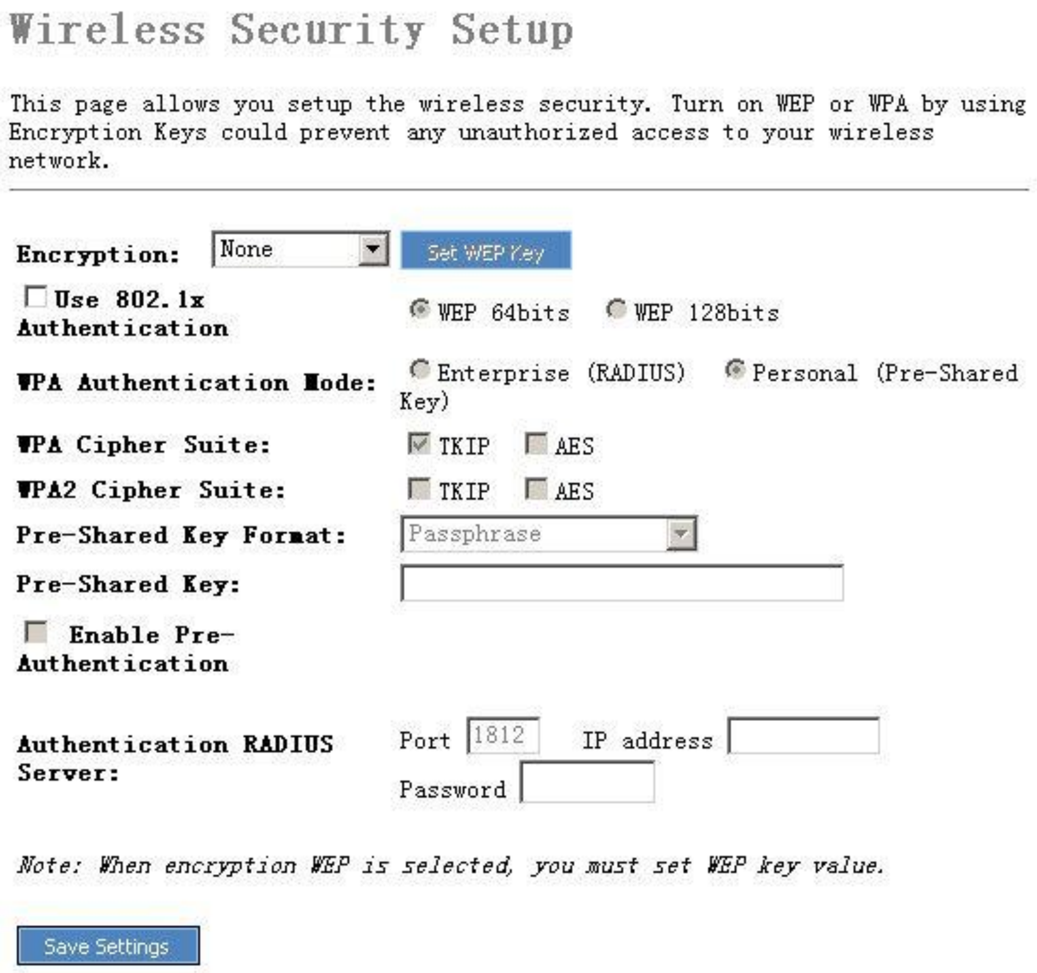
Other Options

Click on desired option(s) to enable/disable function. The functions are intended for advanced users only. Please consult with IT Professional before making adjustments.

Save Settings

Click on **Save Settings** to save modifications.

Security



Wireless Security Setup

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

Encryption:	None ▾ Set WEP Key
□ **Use 802.1x Authentication**	● WEP 64bits ○ WEP 128bits
WPA Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
WPA Cipher Suite:	☑ TKIP □ AES
WPA2 Cipher Suite:	□ TKIP □ AES
Pre-Shared Key Format:	Passphrase ▾
Pre-Shared Key:	
□ **Enable Pre-Authentication**	
Authentication RADIUS Server:	Port 1812 IP address Password

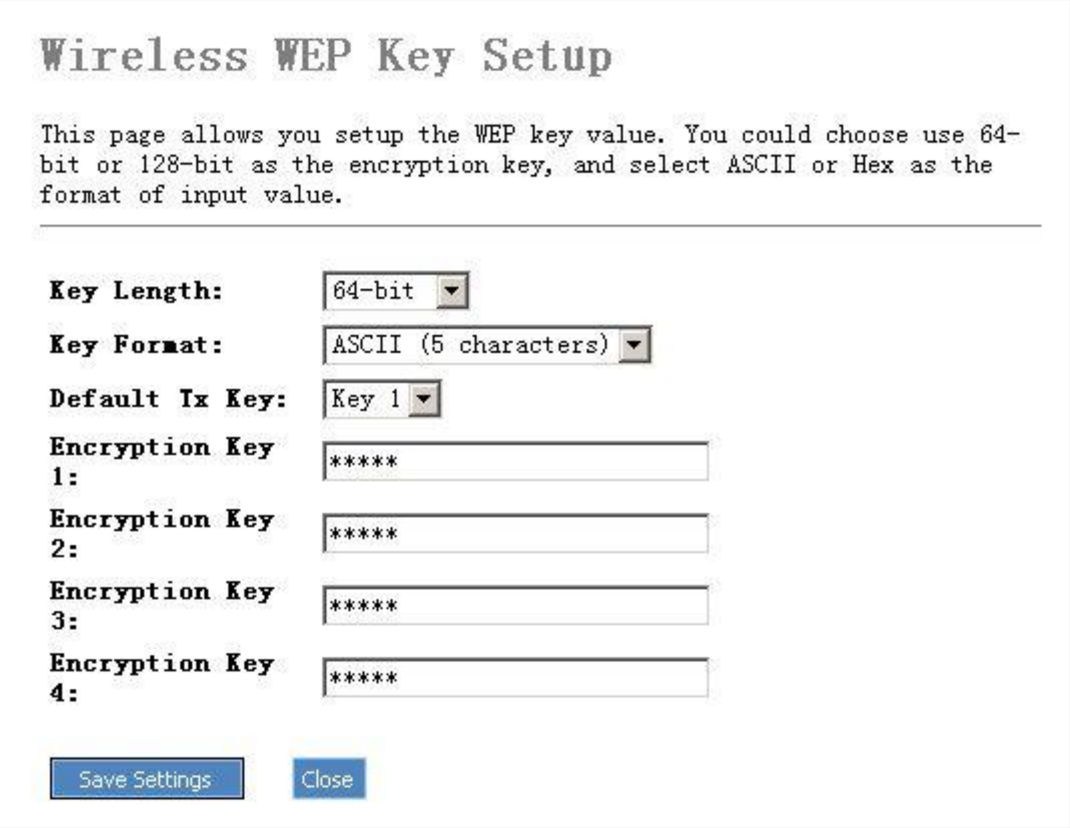
Note: When encryption WEP is selected, you must set WEP key value.

Save Settings

Encryption

Click on **Encryption** (**None**, **WEP**, **WPA**, **WPA2**, and **WPA2 Mixed**) to designated encryption type of wireless connection.

- **WEP** option generates encryption key to enhance wireless connection security. Please click on **Set WEP Key** and refer to below instructions for detailed setup procedure:



Wireless WEP Key Setup

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

Key Length: 64-bit

Key Format: ASCII (5 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

1. Select **Key Length** from the drop down text box. **64-bit** option provide higher throughput while **128-bit** offer higher level of security.
2. Select **Key Format** from the drop down text box. **ASCII** option accepts alphanumeric characters as encryption key while **Hex** option accepts hexadecimal characters as encryption key only.
3. Select **Default TX Key** (**Key1**, **Key2**, **Key3**, and **Key4**) to set default key. Only the selected key number will be accepted during authentication phase.
4. Type in **Encryption Key** value in the appropriate text box. Encryption key should be entered according to its corresponding key format as indicated in the **Key Format** option.

Key Length	HEX Format	ASCII Format
64 bit	10 hexadecimal digits	5 ASCII characters
128 bit	26 hexadecimal digits	13 ASCII characters

5. Click on **Save Settings** to confirm or **Close** to cancel.

Use 802.1x Authentication

Click on the option to replace original WEP Encryption key with 802.1x Authentication protocol. The authentication protocol is monitored and processed by a RADIUS server. Please proceed to **Authentication RADIUS Server** section to complete **802.1x Authentication** settings.

WPA Authentication Mode

Select **WPA Authentication Mode**. **Enterprise (RADIUS)** option utilizes RADIUS server to grant access to wireless connection. Please refer to **Authentication RADIUS Server** section to complete settings. **Personal (Pre-Shared Key)** option utilizes a set of alphanumerical or hexadecimal characters (**Passphrase**) to enhance wireless network security.

WPA Cipher Suite

Select **WPA** encryption method. **TKIP** option constantly changes the encryption key to further enhance wireless network security. **AES** option uses CCMP protocol to constantly change the encryption key.

WPA2 Cipher Suite

Select **WPA2** encryption method. **TKIP** option constantly changes the encryption key to further enhance wireless network security. **AES** option uses CCMP protocol to constantly change the encryption key.

NOTE:

TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption algorithm and includes Message Integrity Code while **AES** (Advanced Encryption System) utilizes a symmetric 128 bit block data encryption, the strongest encryption currently available.

Pre-Shared Key Format

Select **Pre-shared Key Format** (**Passphrase** and **Hex (64 characters)**) from the drop down text box.

Pre-Shared Key

Type in desired **Pre-Shared Key** in the appropriate text box. The key should be entered according to its corresponding key format as indicated in the **Pre-Shared Key Format** option.

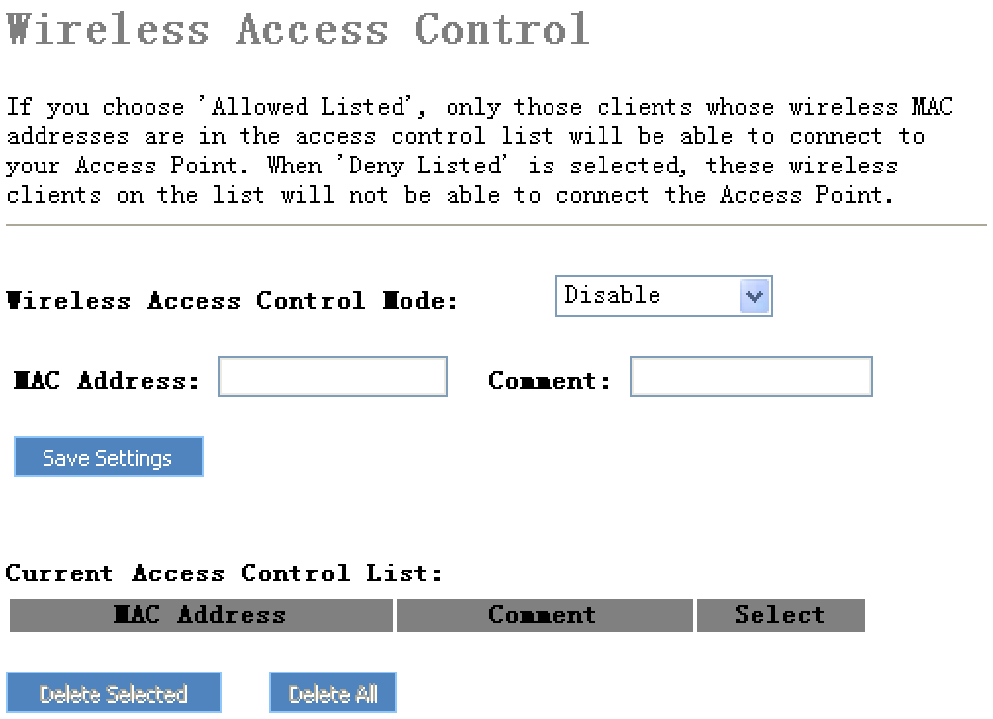
Authentication RADIUS Server

The option is only available when WEP encryption with **Use 802.1x Authentication** option, **WPA** encryption, **WPA2** encryption, or **WPA2 Mixed** Encryption is enabled. Type in RADIUS server **Port** number, **IP address**, and **Password** provided by network administrator.

Save Settings

Click on **Save Settings** to save modifications.

Access Control



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

Wireless Access Control Mode

Select **Wireless Access Control Mode**. **Disable** option disable access control. **Allow Listed** option allows wireless network access only to client device(s) listed while **Deny Listed** option prohibits access only to client device(s) listed.

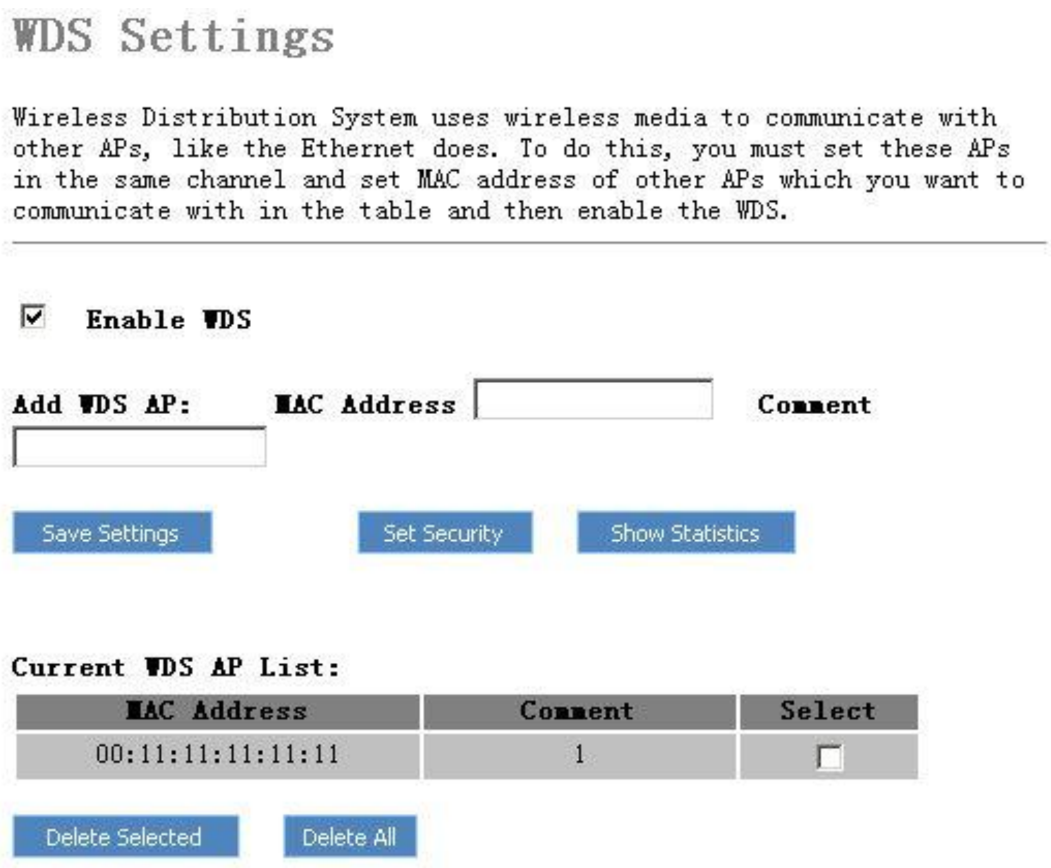
MAC Address and **Comment**

Type in **MAC Address** desired to be listed and **Comment** if necessary in the appropriate text box. Click on **Save Settings** to confirm input and display the client device(s) on the list.

Current Access Control List

Review allowed/denied client device of wireless network access. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

WDS Settings



WDS Settings

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

☑ Enable WDS

Add WDS AP: MAC Address ▭ Comment ▭

Current WDS AP List:

MAC Address	Comment	Select
00:11:11:11:11:11	1	□

Enable WDS

Select the option to enable WDS function.

Add WDS AP

Type in **MAC Address** desired to connect to and **Comment** if necessary in the appropriate text box. Click on **Save Settings** to confirm input and display the client device(s) on the list. Click on **Set Security** to adjust security settings and **Show Statistics** to review detailed information.

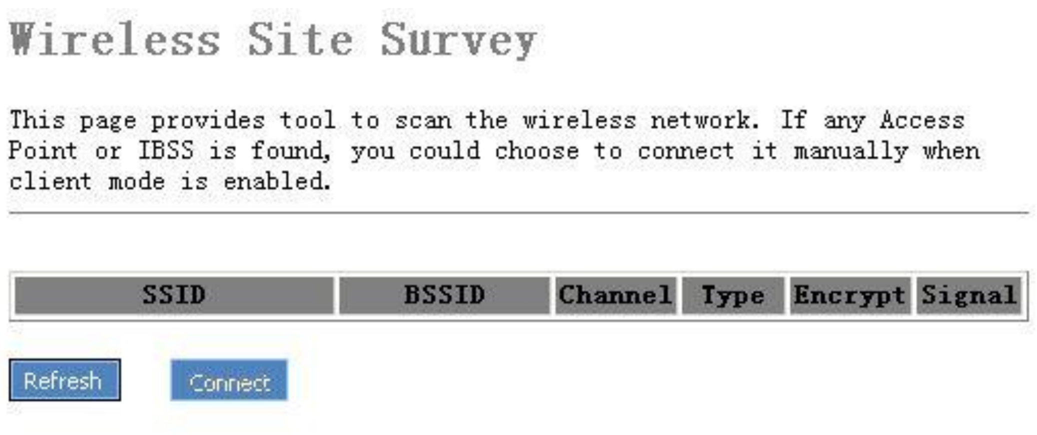
Current WDS AP List

Review all connected AP device within the same wireless network. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

NOTE:

The function is only available when device is configured as an Access Point (**AP Mode**) in the same channel.

Site Survey



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

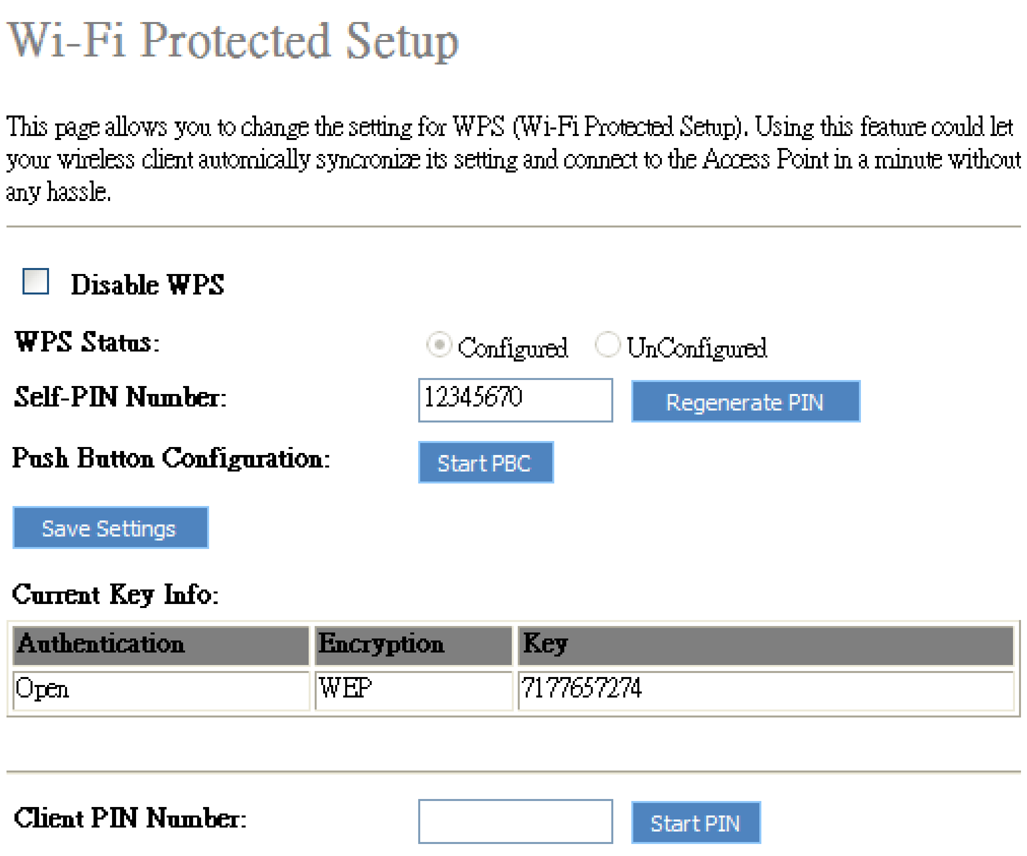
Refresh and **Connect**

Review all available AP device(s) within the range. Click on **Select** option and click on **Connect** to selected AP device. Click on **Refresh** to update the list.

NOTE:

The function is only available when device is configured in **Client Mode**.

WPS



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: 12345670

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	WEP	7177657274

Client PIN Number:

Disable WPS

Click on the option to disable WPS function.

WPS Status

The option displays WPS status of **Configured** or **UnConfigured**. The device must be configured before WPS function becomes available.

Self-PIN Number

Click on **Regenerate PIN** to generate new PIN number. PIN number must be entered at client device to facilitate PBC connection.

Push Button Configuration

Click on **Start PBC** to initiate Push Button Configuration sequence. The device will be enabled of PBC activity in the next 120 seconds.

Save Settings

Click on **Start PBC** to initiate Push Button Configuration sequence. The device will be enabled of PBC activity in the next 120 seconds.

Current Key Info

Review PBC related information such as **Authentication** type, **Encryption** type, and **Key** value.

Client PIN Number

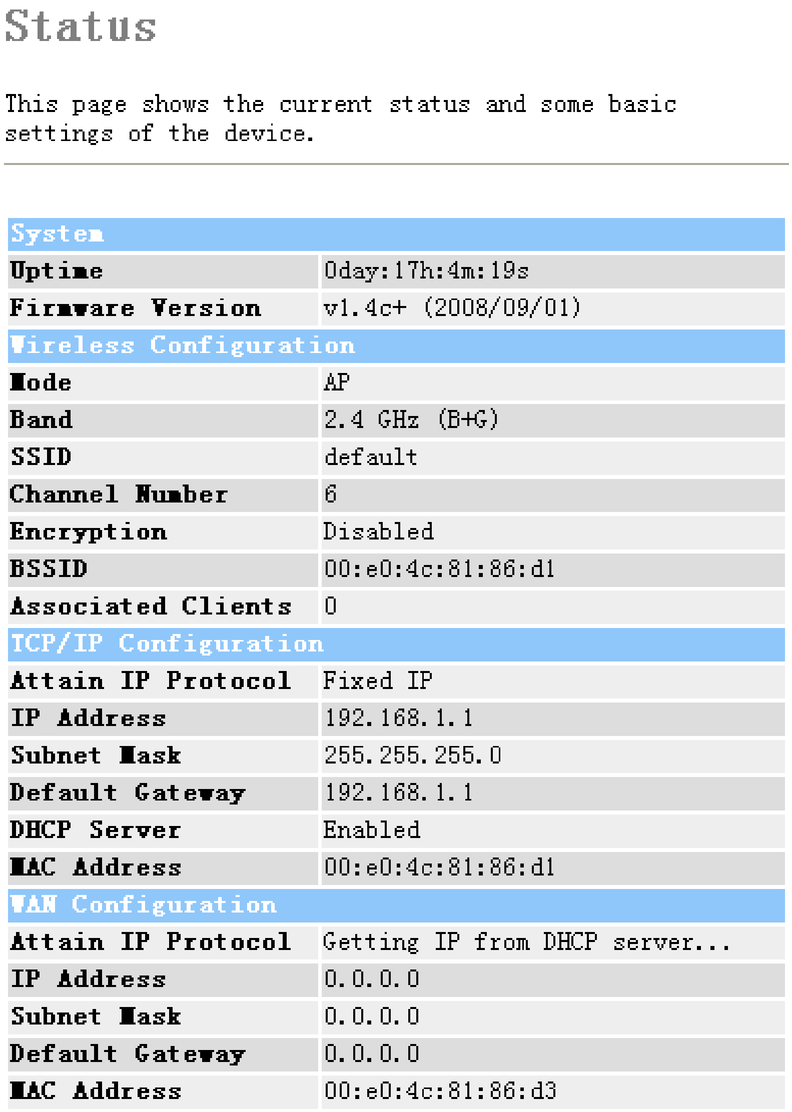
Type in PIN number generated by client device and click on **Start PIN** to activate Push Button Configuration process.

Save Settings

Click on **Save Settings** to save modifications.

System Information

Status



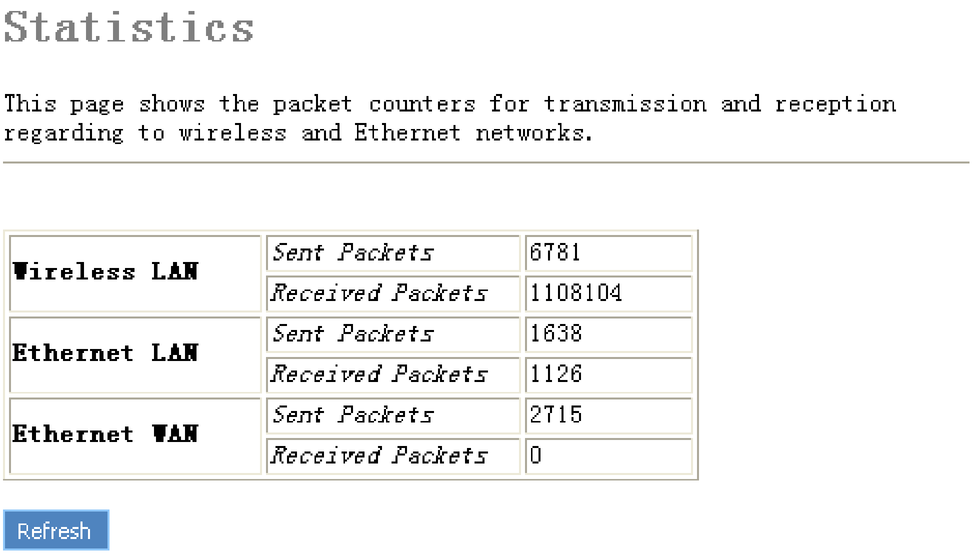
Status

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

System	
Uptime	0day:17h:4m:19s
Firmware Version	v1.4c+ (2008/09/01)
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	default
Channel Number	6
Encryption	Disabled
BSSID	00:e0:4c:81:86:d1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:d1
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:81:86:d3

The **Status** section monitors the current status of the device including information such as **System**, **Wireless Configuration**, **TCP/IP Configuration**, and **WAN Configuration**.

Statistics



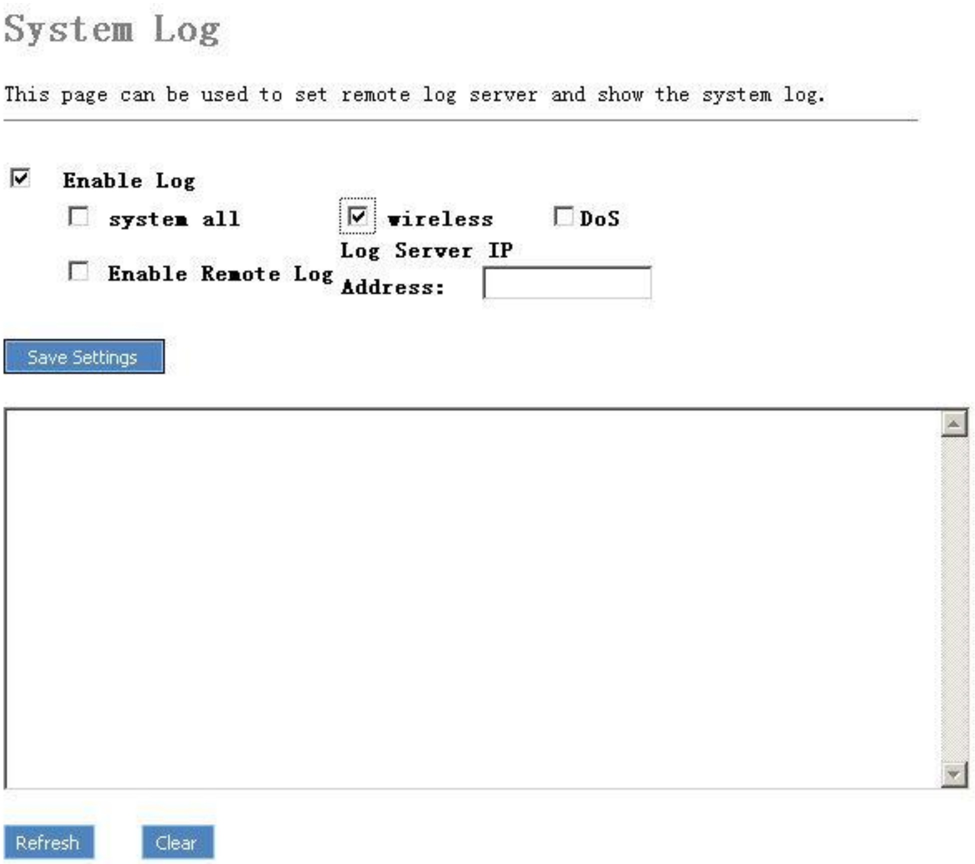
Statistics

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

Wireless LAN	*Sent Packets*	6781
	Received Packets	1108104
Ethernet LAN	*Sent Packets*	1638
	Received Packets	1126
Ethernet WAN	*Sent Packets*	2715
	Received Packets	0

The **Statistics** section displays packet counters from transmission and reception on wireless and Ethernet network. Click on **Refresh** to update data.

System Log



System Log

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

☑ Enable Log

☐ system all ☑ wireless ☐ DoS

☐ Enable Remote Log Log Server IP Address:

The **System Log** section displays current system log of the device after system boot.

Enable Log

Click on the option to enable automatic update of system log. Click on **System all** option to record all system entries. Click on **wireless** option to record wireless network entries only and **DoS** option to record Denial of Service entries only. Click on **Refresh** to refresh log status or **Clear** to remove all previous entries.

Enable Remote Log

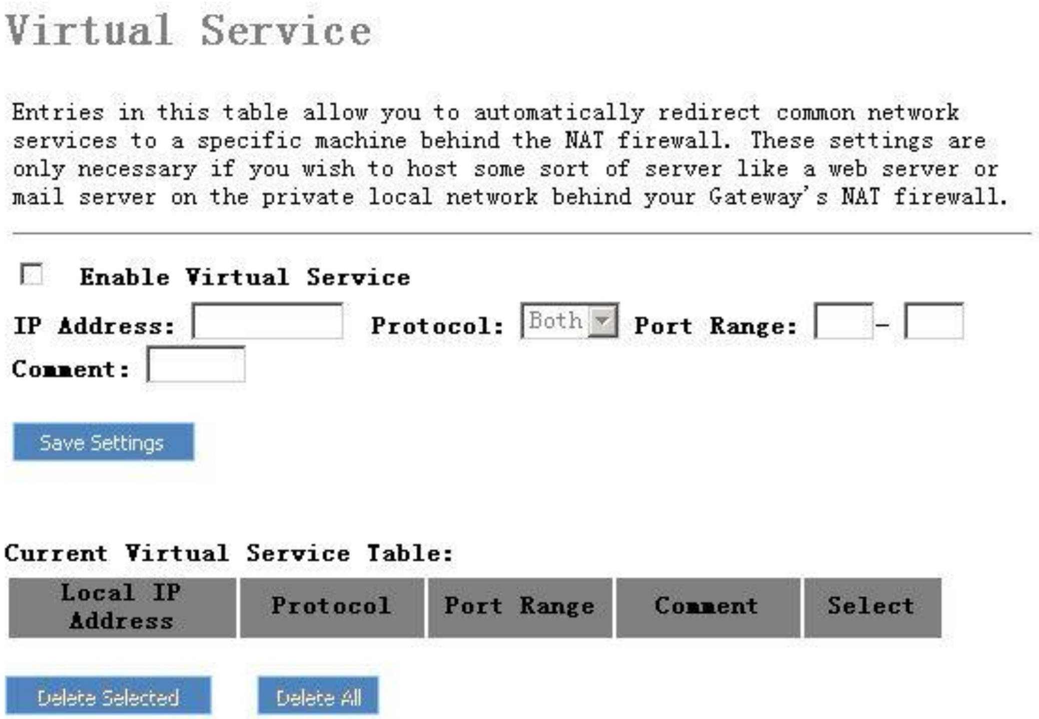
Click on the option to enable remote monitoring and data logging of the device. Type in **Log Server IP Address** in the appropriate text box to allow remote access.

Save Settings

Click on **Save Settings** to save modifications.

Applications & Gaming

Virtual Service



Virtual Service

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 Virtual Service

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

Current Virtual Service Table:

Local IP Address	Protocol	Port Range	Comment	Select

Enable Virtual Service

Click on the option to enable **Virtual Service** function. Type in **IP address** of connected client device that the data will be delivered to in the appropriate text box.

NOTE:

Client device must be assigned with a fixed IP address for proper connection for virtual server to be established.

Select **Protocol** type (**TCP**, **UDP**, and **Both**) from the drop down text box and type in values of **Port Range** from the client device in the appropriate text box.

Type in **Comment** in the appropriate text box if necessary.

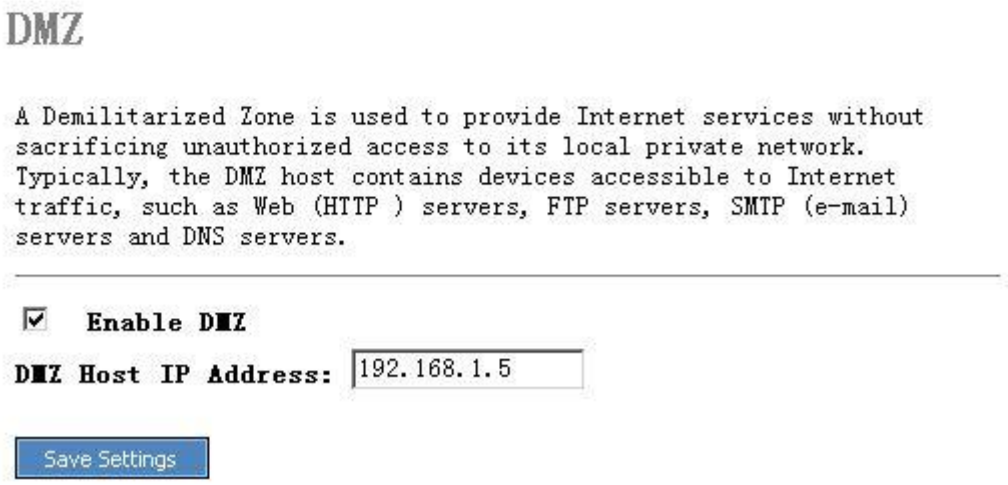
Save Settings

Click on **Save Settings** to save modifications.

Current Virtual Service Table

Review all virtual services and their related attributes such as **Local IP Address**, **Protocol**, **Port Range**, and **Comment**. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

DMZ



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: 192.168.1.5

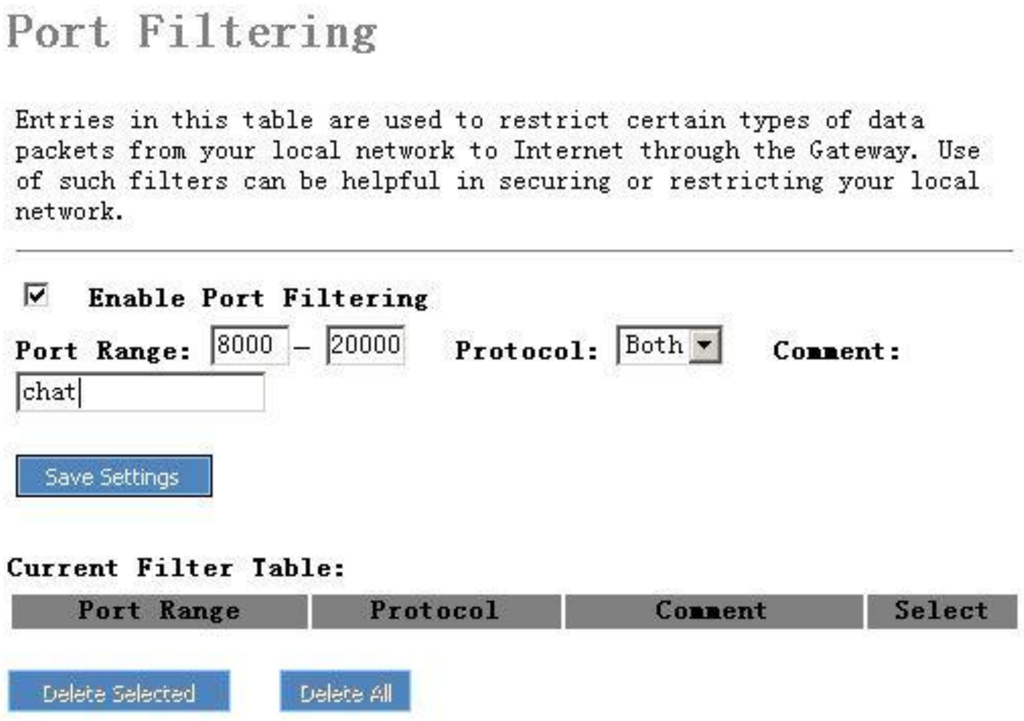
Enable DMZ

Click on the option to enable **DMZ** (Demilitarized Zone) function. Type in **IP address** of client device desired of all network traffic re-route in the appropriate text box.

Save Settings

Click on **Save Settings** to save modifications.

Port Filtering



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: 8000 – 20000 Protocol: Both Comment: chat

Current Filter Table:

Port Range	Protocol	Comment	Select

Enable Port Filtering

Click on the option to enable **Port Filtering** function. Type in values of **Port Range** of client device in the appropriate text box to restrict specific client network traffic to outside network. Select **Protocol** type (**TCP**, **UDP**, and **Both**) from the drop down text box. Type in **Comment** in the appropriate text box if necessary.

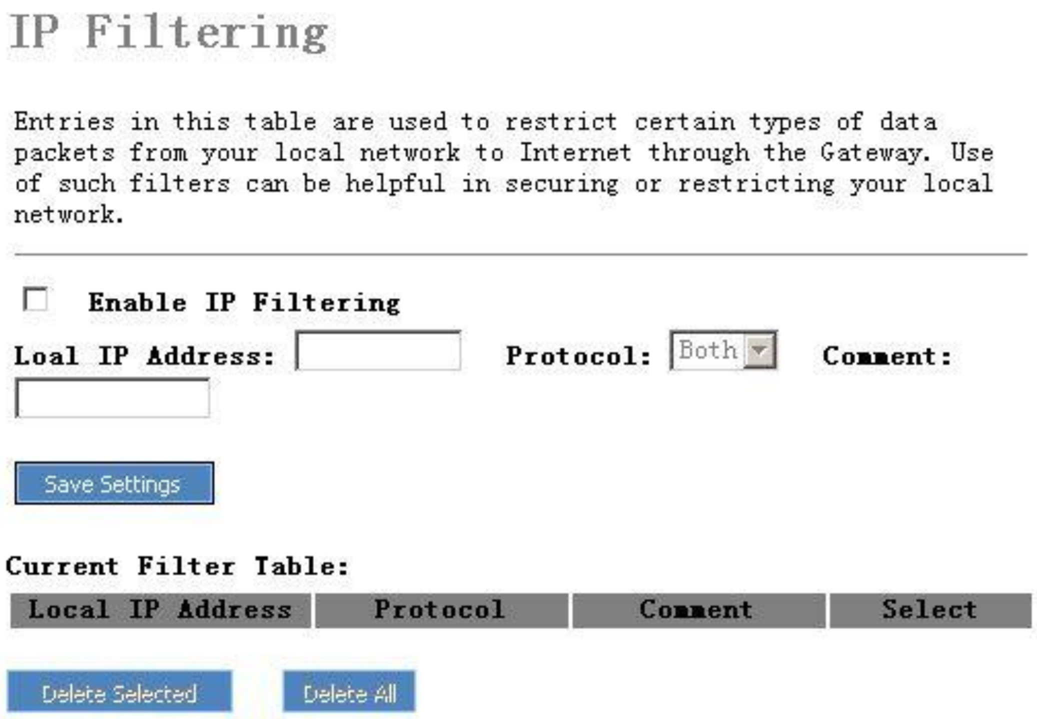
Save Settings

Click on **Save Settings** to save modifications.

Current Filter Table

Review all restricted **Ports** and their related attributes such as **Protocol** and **Comment**. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

IP Filtering



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

Enable IP Filtering

Click on the option to enable **IP Filtering** function. Type in **IP Address** of client device in the appropriate text box to prohibit client network traffic. Select **Protocol** type (**TCP**, **UDP**, and **Both**) from the drop down text box. Type in **Comment** in the appropriate text box if necessary.

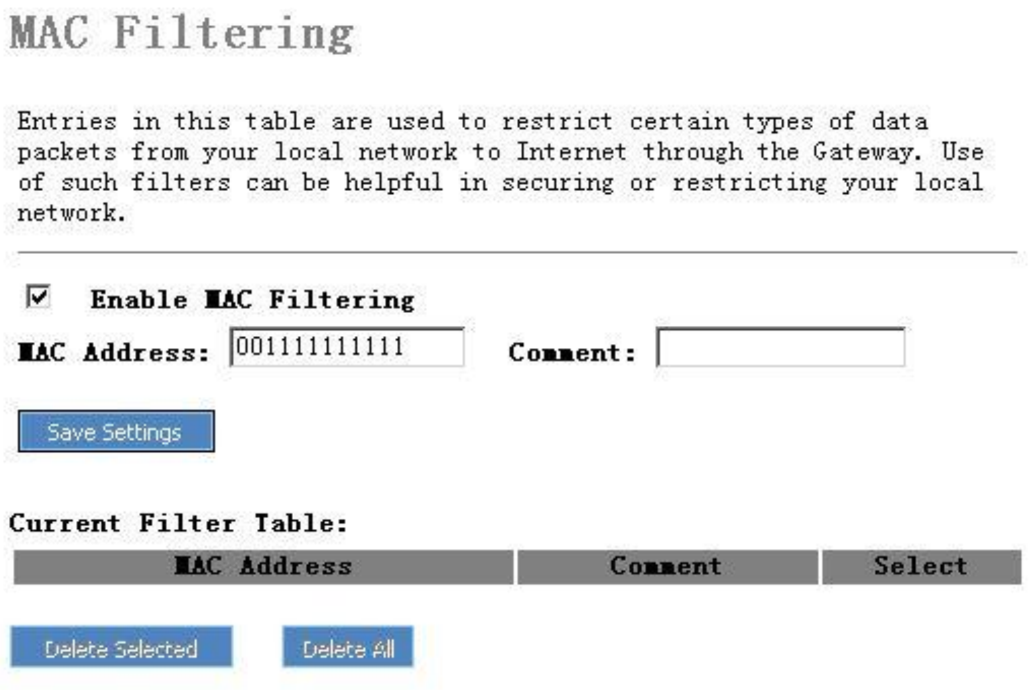
Save Settings

Click on **Save Settings** to save modifications.

Current Filter Table

Review all restricted **IP Addresses** and their related attributes such as **Protocol** and **Comment**. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

MAC Filtering



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: 001111111111 Comment:

Current Filter Table:

MAC Address	Comment	Select

Enable MAC Filtering

Click on the option to enable **MAC Filtering** function. Type in **MAC Address** of client device in the appropriate text box to prohibit client network traffic. Type in **Comment** in the appropriate text box if necessary.

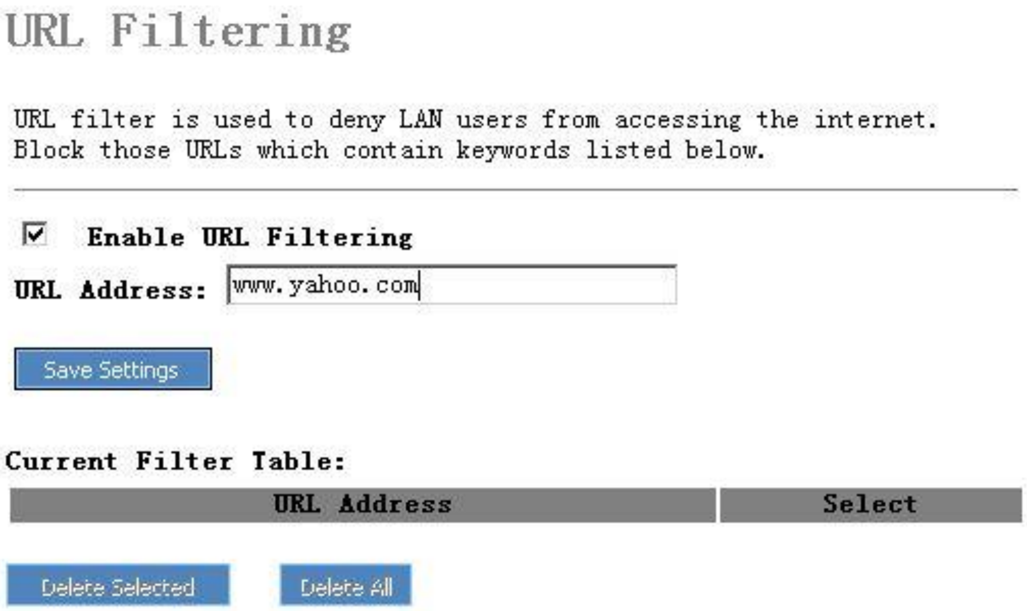
Save Settings

Click on **Save Settings** to save modifications.

Current Filter Table

Review all restricted **MAC Addresses** and their related attribute such as **Comment**. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

URL Filtering



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: www.yahoo.com

Current Filter Table:

URL Address	Select

Enable MAC Filtering

Click on the option to enable **URL Filtering** function. Type in **URL Address** of websites in the appropriate text box to prohibit client device from accessing.

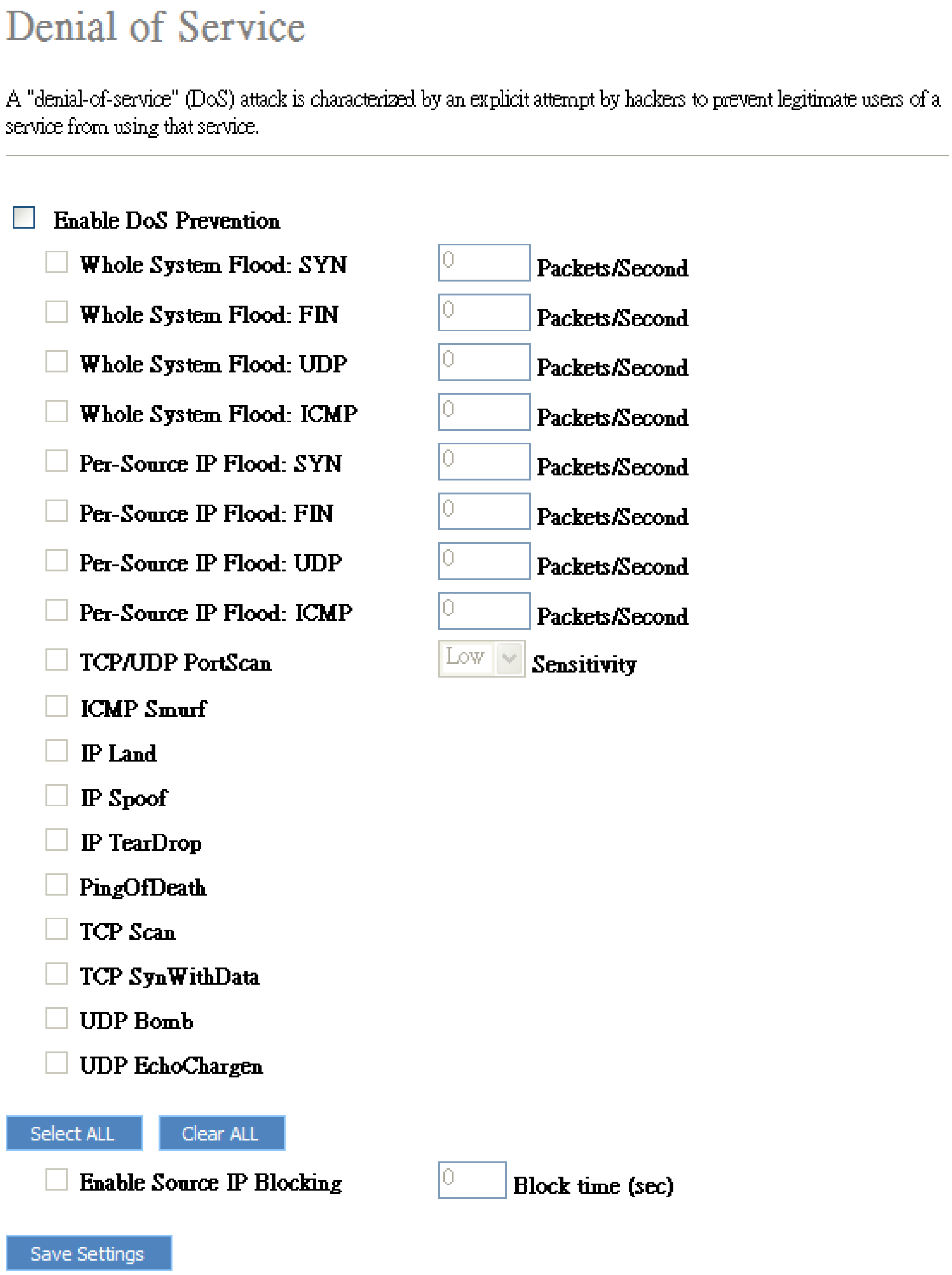
Save Settings

Click on **Save Settings** to save modifications.

Current Filter Table

Review all restricted **URL**. Click on **Select** option and click on **Delete Selected** to remove the selected entity from the list. Click on **Delete All** to remove all entities.

URL Filtering



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)

Enable DoS Prevention

Click on the option to enable **DoS Prevention** function. Click on various prevention measures and specify values if necessary. Click on **Select All** to select all prevention options or **Clear All** to disable all prevention options.

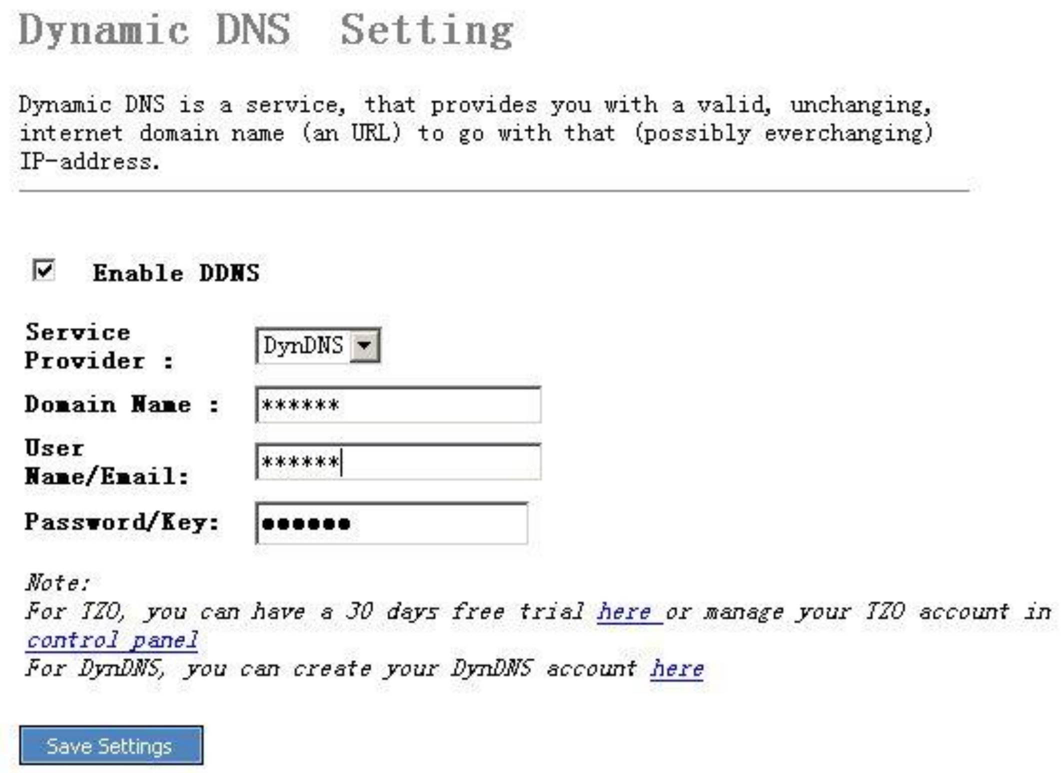
Enable Source IP Blocking

Click on the option to block attacks from **Source IP**. Type in **Block time** value in the appropriate text box.

Save Settings

Click on **Save Settings** to save modifications.

DDNS



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 :	******
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

Enable DDNS

Click on the option to enable **DDNS** function and to map the static domain name to a dynamic IP address. Select **Service Provider** (**DynDNS** and **TZO**) from the drop down text box. Type in **Domain Name**, **User Name/Email**, and **Password/Key** as required by service provider.

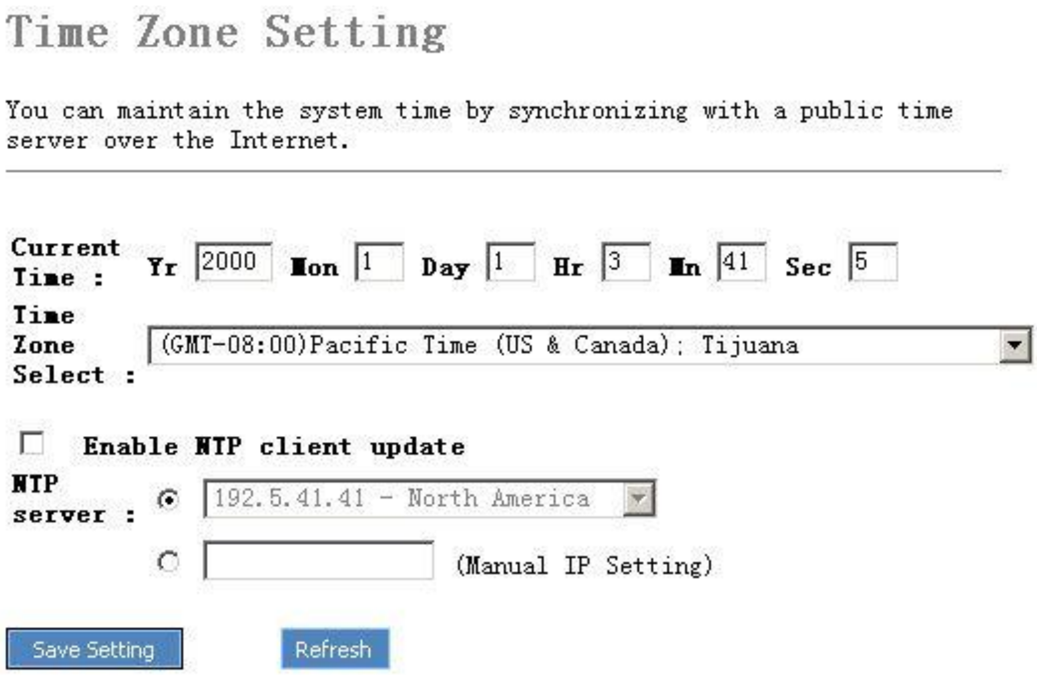
NOTE:

Please consult with IT professional on how to obtain a static domain from DDNS service provider.

Save Settings

Click on **Save Settings** to save modifications.

Time Zone Setting



Time Zone Setting

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

Current Time : Yr 2000 Mon 1 Day 1 Hr 3 Mn 41 Sec 5

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

□ Enable NTP client update

NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

Current Time

Type in current date and time values in the appropriate text box.

Time Zone Select

Select **Time Zone** from the drop down text box.

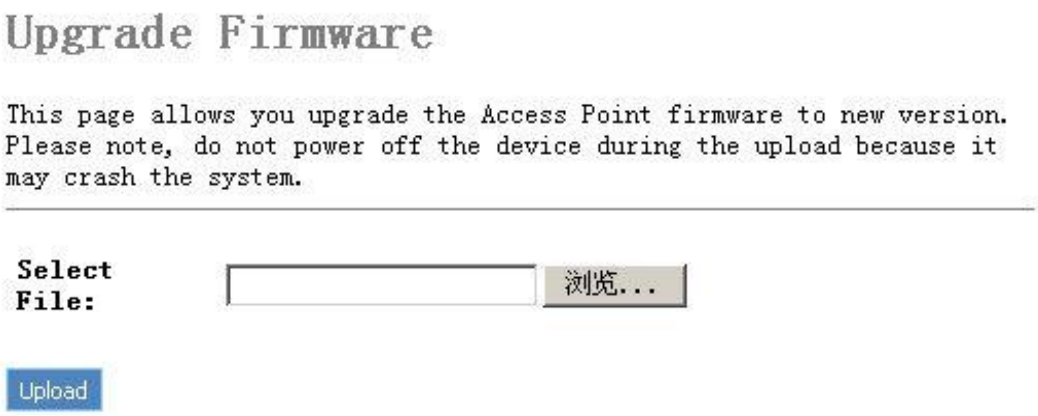
Enable NTP client update

Click on the option to enable **NTP client update** function. Select **NTP Server** from the drop down text box or type in **NTP Server** IP address if necessary.

Save Settings

Click on **Save Settings** to save modifications and Refresh to update current time.

Upgrade Firmware



Upgrade Firmware

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

Select File:

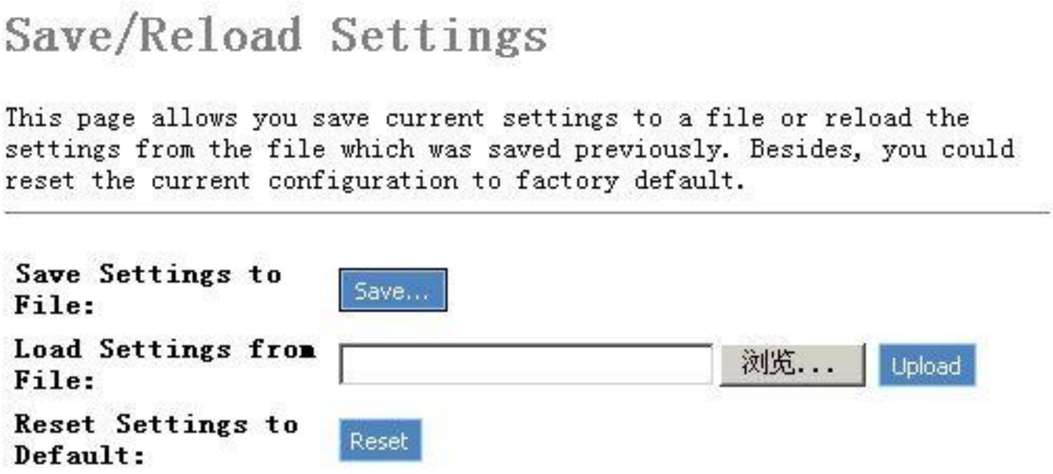
Select File

Type in path or click on **Browse** to locate firmware file in the connected client device. Click on **Upload** to initiate firmware upgrade process.

NOTE:

- Please do **NOT** power off the device while firmware upgrade is in process.
- Firmware upgrade will completely erase all user defined settings and restore device to factory default settings.

Save/Reload Settings



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:

Load Settings from File:

Reset Settings to Default:

Save Settings to File

Click on the option to save device configuration to a file stored in client device.

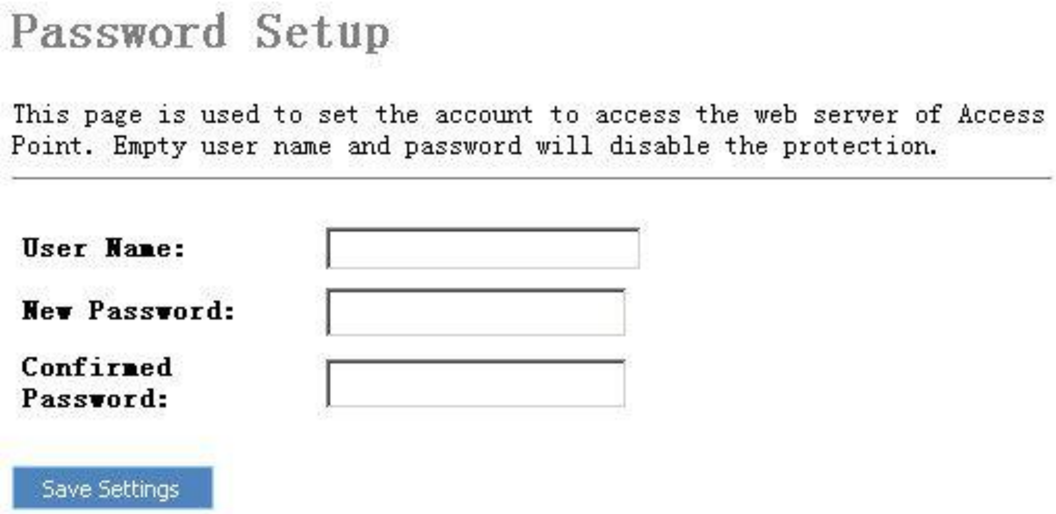
Load Settings from File

Type in path or click on **Browse** to locate saved device configuration file in the connected client device. Click on **Upload** to reload the settings from saved file.

Reset Settings to Default

Click on the option to restore all configuration to factory default settings.

Password



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

Type in desired **User Name** in the appropriate text box.

New Password

Type in desired **New Password** in the appropriate text box.

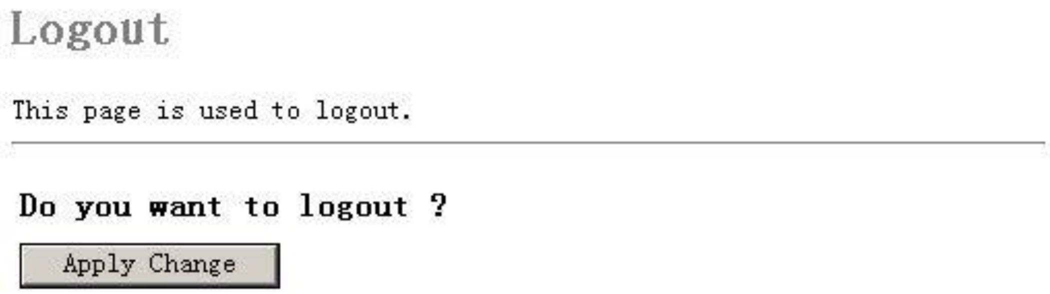
Confirm Password

Type in new password again in the appropriate text box to confirm.

Save Settings

Click on **Save Settings** to save modifications.

Logout



Logout

This page is used to logout.

Do you want to logout ?

Click on **Save Settings** to logout from device.

Troubleshooting

Please refer to the following procedures if **CNP-WF514A** does not function as it should be. Be advised that the following instructions are only intended for simply troubleshooting purpose. Please contact your local authorized shops for further troubleshooting and technical support.

- **Can not access the web-based configuration utility from Client device**
  1. Verify if the LAN LED is on or if the connection cable is firmly connected.
  2. Check whether client device resides on the same subnet with device LAN IP address.
  3. If client device is configured as a DHCP client, check whether the client device is assigned an IP address from other DHCP server. Renew the IP address of client device if necessary.
  4. Make sure browser on client device is not configured to use a proxy server.
  5. Verify device IP address. It might be different from device default LAN IP address (192.168.1.1)
- **Do not remember password.**
  1. Press and hold the reset button on the front panel of device for more than 5 seconds.
  2. Unplug power adapter and wait for 5 seconds before plugging it in again.
- **Device malfunctioning with cable/DSL modem connection.**
  1. Please check signal stability from cable/DSL modem. There should be a signal indicator on the modem displaying its connection status. Contact ISP if the signal is bad.
  2. Please check status indicators on the front panel of device. When working properly, the SYS indicator should be solid and the WAN indicator should be blinking. The LAN indicator(s) should also be blinking with corresponding client device(s) connect to the device.
  3. Please verify that the network cables are working properly.
  4. Enable DHCP server function. Please refer to LAN setup section
  5. Reset the device as described at above section if all else failed.
- **Setup PC(s) to obtain IP address manually.**

  The below instructions only refer to Windows XP verison OS only. Please refer to OS manufacturer for other OS

  1. Click on Start → Settings → Control Panel.
  2. Click on Network and Internet Connections and then Network

Connections.

3. Right click on Local Area Connection icon and select Properties.
4. Highlight Internet Protocol (TCP/IP) item and click on Properties.
5. Type in the following information on the corresponding properites:
   - IP address: 192.168.1.XXX where XXX is a number between 2 and 253.
   - Subnet mask: 255.255.255.0
   - Default gateway: 192.168.1.1
   - Preferred DNS server: 192.168.1.1
   - Alternate DNS server: leave this property blank.
6. Click on OK to confirm modifications.

Appendix

Technical Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE802.11b
Channels	13 Channels
Management Interface	Web Based
Network Ports	WAN: 1 X 10/100 RJ-45 Port LAN: 4 X 10/100 RJ-45 Ports (with switching function)
Cabling Type	Cat 5 Ethernet Network Cable
RF Power Output	15 ± 2dBm
Wireless Security	WPA/WPA2, WEP 64/128bit, Wireless MAC Filtering
LED Indicators	SYS, WLAN, LAN Link/Activity, WAN
Temperature	Operating: 0° to 40° C Storage: -20° to 70° C
Humidity	Operating: 10% to 85 % non-condensing Storage: 5% to 90 % non-condensing
Dimensions	135mm(L) X 95.4mm(W) X 28mm(H)
Weight	210g
Power	DC 9V, 700mA