Air Live®
Powered by OvisLink Corp.

N.TOP

802.11n Ceiling Mount
Long Range PoE AP

User's Manual

www.airlive.com

Copyright & Disclaimer

FCC Statement

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. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Table of Contents

1 Introduction

1.1 Overview

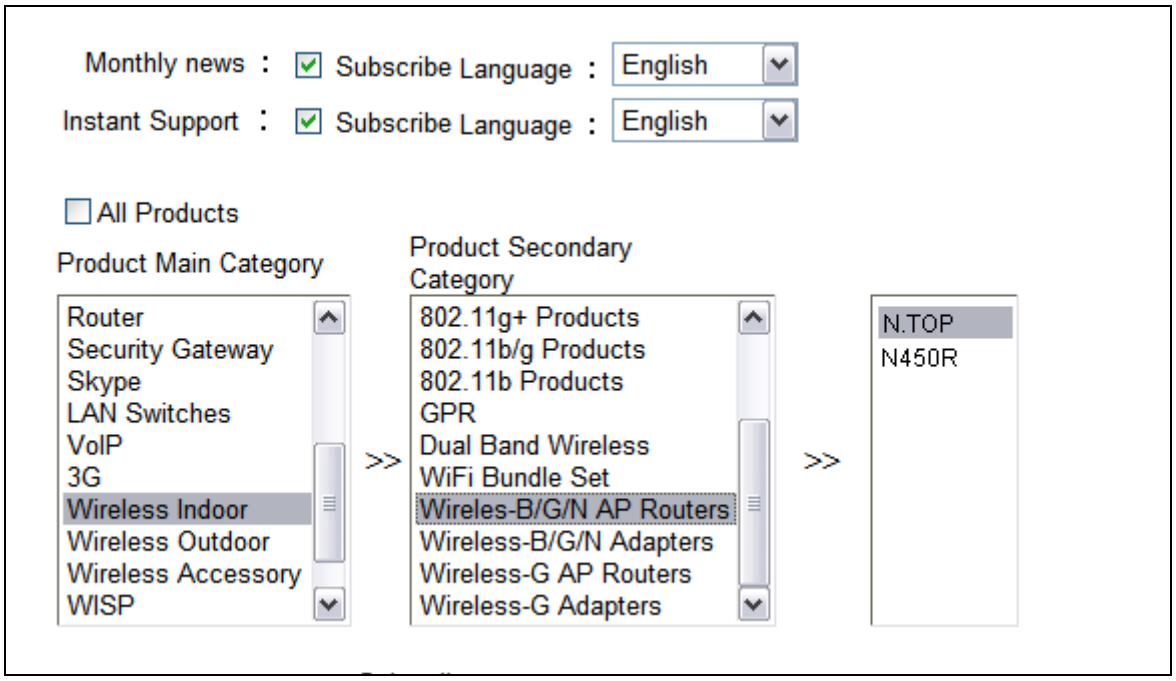
The N.TOP is a ceiling mount wireless multi-function AP based on 300Mbps 2T2R Wireless b/g/n MIMO standard radio technologies. The Wireless Access Point is equipped with one 10/100 Mbps Auto-sensing Ethernet ports for connecting to LAN and also for cascading to next Wireless Access Point. It has built-in 802.3af PoE port for installation up to 100 meter away from the power source.

1.2 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmware that either increase software functions or provide bug fixes for N.TOP. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



AirLive Newsletter Suppport System

1.3 Features

- 300Mbps 802.11b/g/n Standard
- Built-in MIMO Antennas
- 4MB Flash and 32MB SDRAM
- 5 wireless multi-function modes: AP, Client, WDS Bridge, WDS Repeater and Universal Repeater.
- R-SMA connector antenna.
- 1 x 10/100 Ethernet Port with IEEE 802.3af PoE support
- Web management
- Easy Setup Wizard
- Wireless Access Control ,Multiple SSID and Virtual AP
- Wireless Client Limit, Client Isolation and Watchdog

- IP Finder Management Utility
- Optional 802.2af POE Injector (AirLive POE-48PB) or PoE switch is required for PoE installation.
- Green WLAN for Power Saving

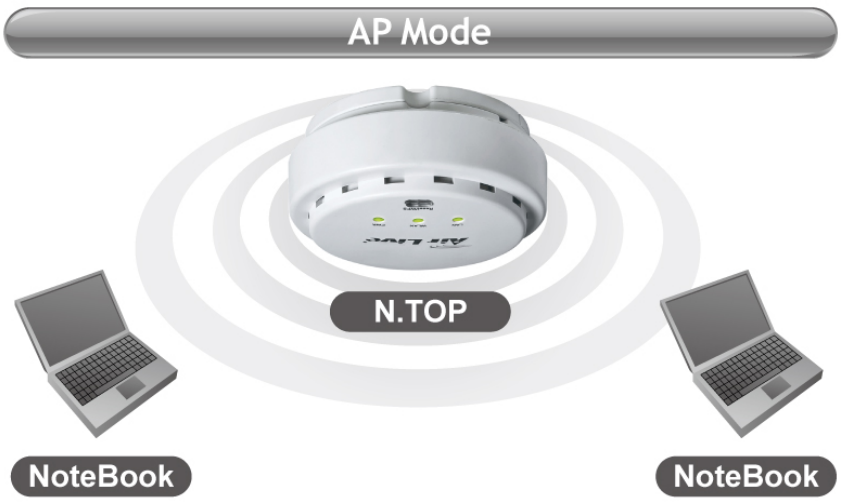
1.4 Wireless Operation Modes

The N.TOP can perform as a Multi-Function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the N.TOP to perform.

N.TOP Wireless Operation Mode			
Wireless Mode	**Radio**	**WAN**	**Application**
Access Point	AP	None	Hotspot (Indoor and Outdoor)
Client	Client	None	WISP Client
Bridge	Bridge	None	Building to Building network
WDS Repeater	AP + Client	None	Extend distance of another WDS AP/Router
Universal Repeater	AP + Client	None	Extend distance of any AP Router

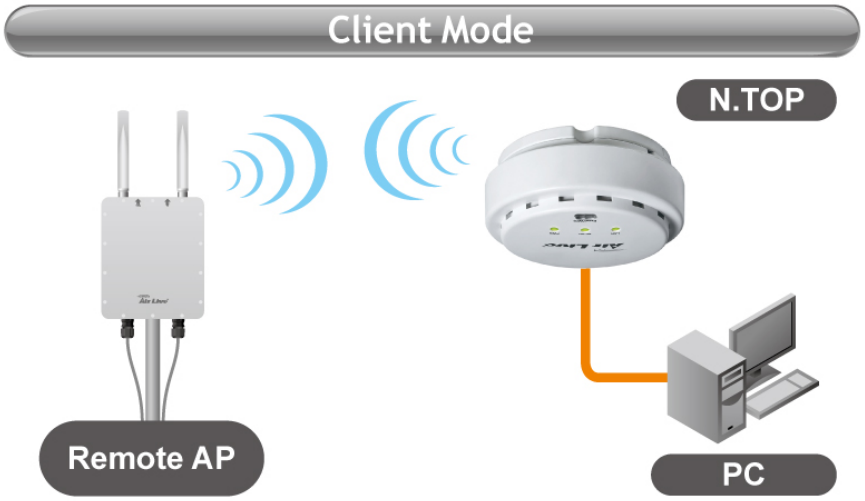
1.4.1 Access Point Mode

When operating in the Access Point mode, the N.TOP becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through N.TOP. This type of network is known as "**Infrastructure Network**". Other N.TOP or 802.11b/g/n device can connect to AP mode through "**Client Mode**".



1.4.2 Client Mode

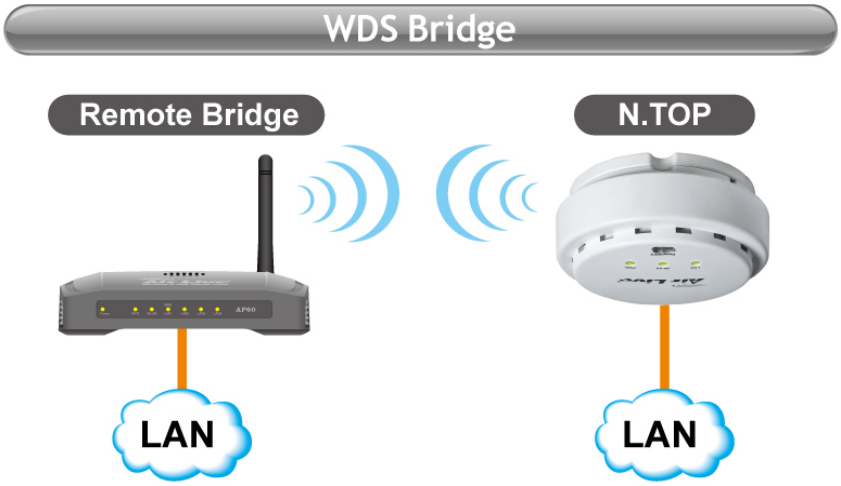
This mode is also known as "**Client**" mode. For N.TOP, there are 2 types of Client modes: Infrastructure and Adhoc mode. In Infrastructure mode, the N.TOP acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of N.TOP to get network access. This mode is often used by WISP on the subscriber's side.



In Client Ad Hoc mode, N.TOP can connect to other wireless adapters without access point. Users can attach a computer or a router to the LAN port of N.TOP to get network access.

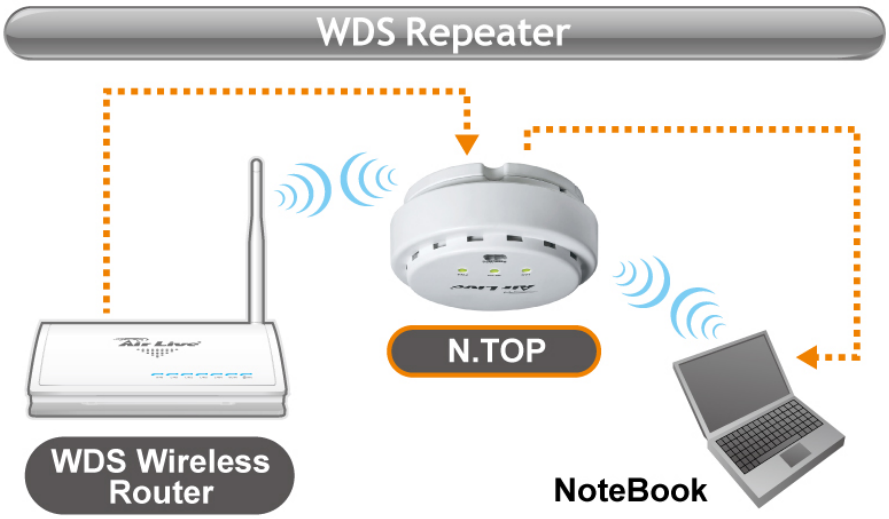
1.4.3 Bridge Mode

This mode is also known as "WDS Pure MAC Bridge mode". When configured to operate in the Wireless Distribution System (WDS) Mode, the N.TOP provides bridging functions with remote LAN networks in the WDS system. The system will support up to total of 8 bridges in a WDS network (by daisy chain). However, each bridge can only associate with maximum of 4 other bridges in the WDS configuration. This mode is best used when you want to connect LAN networks together wirelessly (for example, between office and warehouse). If you have more than 2 AP in WDS Bridges mode, please remember to turn on the "802.1d Spanning Tree" or "STP" option on to avoid network loop. This mode usually delivers faster performance than infrastructure mode.



1.4.4 WDS Repeater Mode

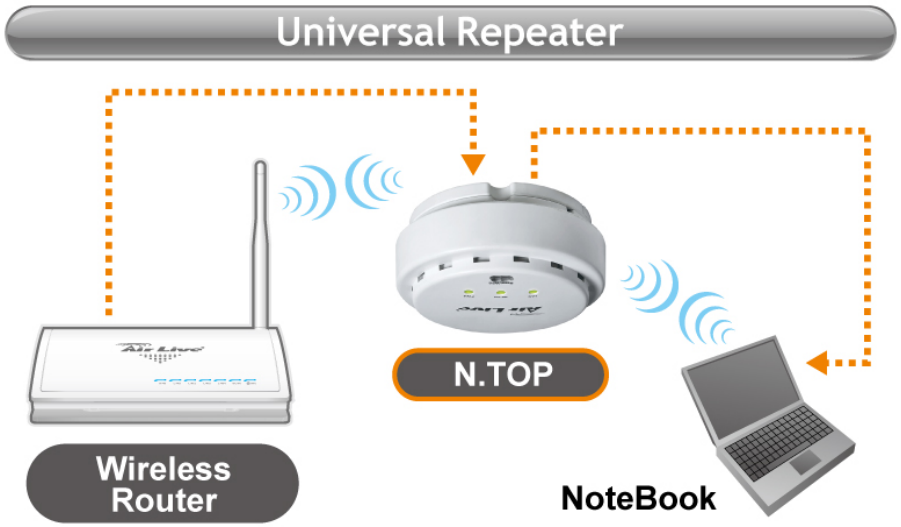
In WDS Repeater mode, the N.TOP functions as a repeater that extends the range of remote wireless LAN. In this mode, the remote Access Point must have WDS (Wireless Distribution System) capability. If you require the PC's MAC addresses to be preserved when the data pass through the Repeater, it is necessary to use the WDS Repeater mode. Because the radio is divided into WDS + AP mode, the Repeater mode will have less performance and distance.



1.4.5 Universal Repeater Mode

In Universal Repeater mode, the N.TOP functions as a repeater that extends the range of remote wireless LAN. This mode can repeat the signal of any remote AP/Router, even if they do not have WDS capability. However, the MAC addresses of any wireless traffic going through Universal Repeater are “translated” into the Repeater’s MAC address. As a result, any applications that require identification by MAC address (such as hotspot or firewall) can not use this mode. It is also recommended to use “DHCP” Relay function to get IP address from remote DHCP server.

Because the radio is divided into Client + AP mode, the Repeater mode will have less performance and distance.



2 Installing the N.TOP

This section describes the installation procedure for the N.TOP. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the N.TOP. Finally, this section explains how to configure a Windows PC to communicate with the N.TOP.

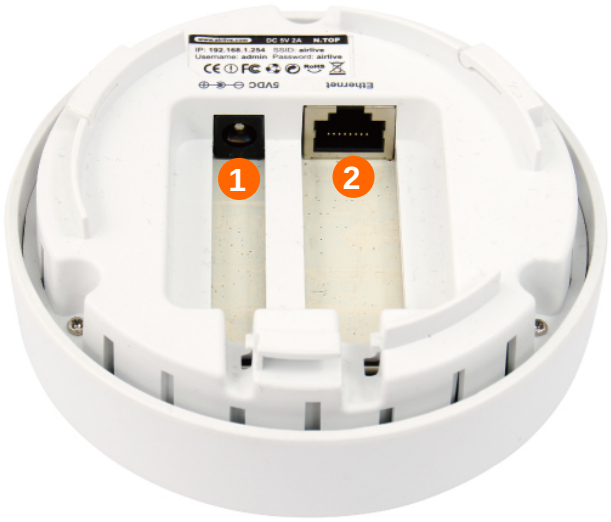
2.1 Package Content

The N.TOP package contains the following items:

- One N.TOP main unit
- One 5V DC power adapter
- One CD of the N.TOP
- Quick Start Guide

2.2 Knowing your N.TOP

Below are descriptions and diagrams of the product:

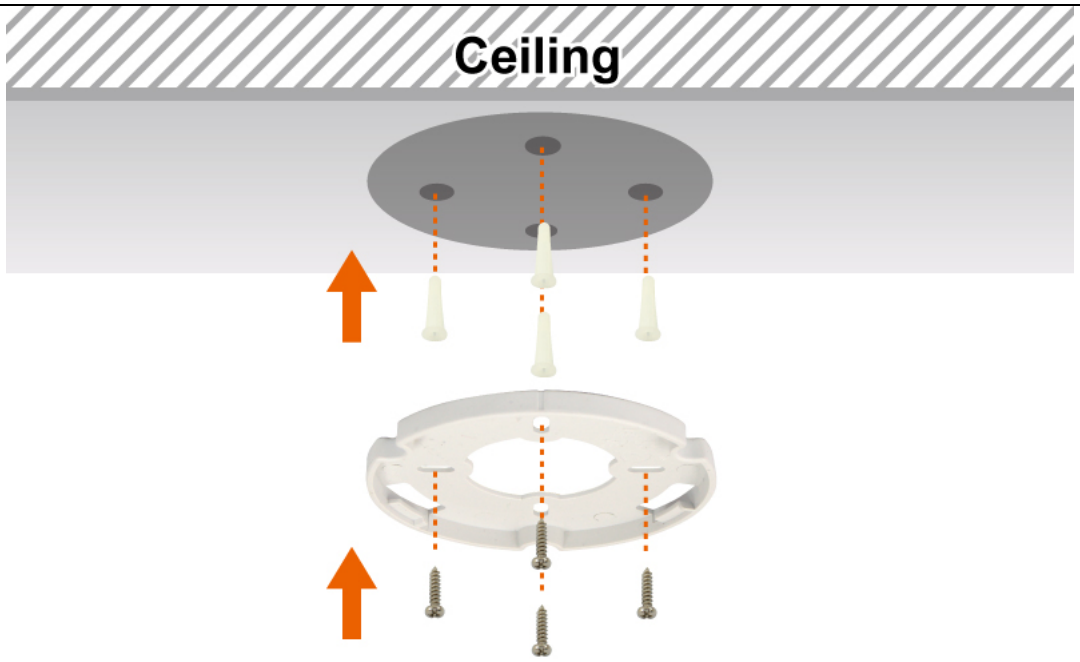


1. Power Adapter Connector
2. LAN Port, PoE Port

2.3 Hardware Installation

※Note	Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations.

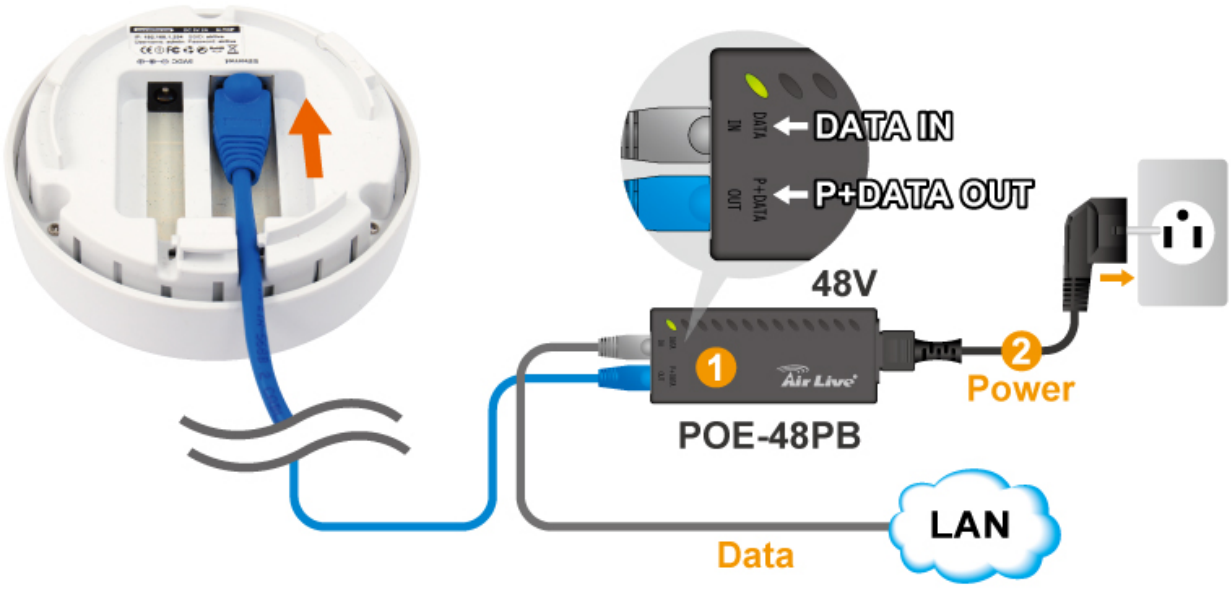
1. Screw the bottom case into the wall.



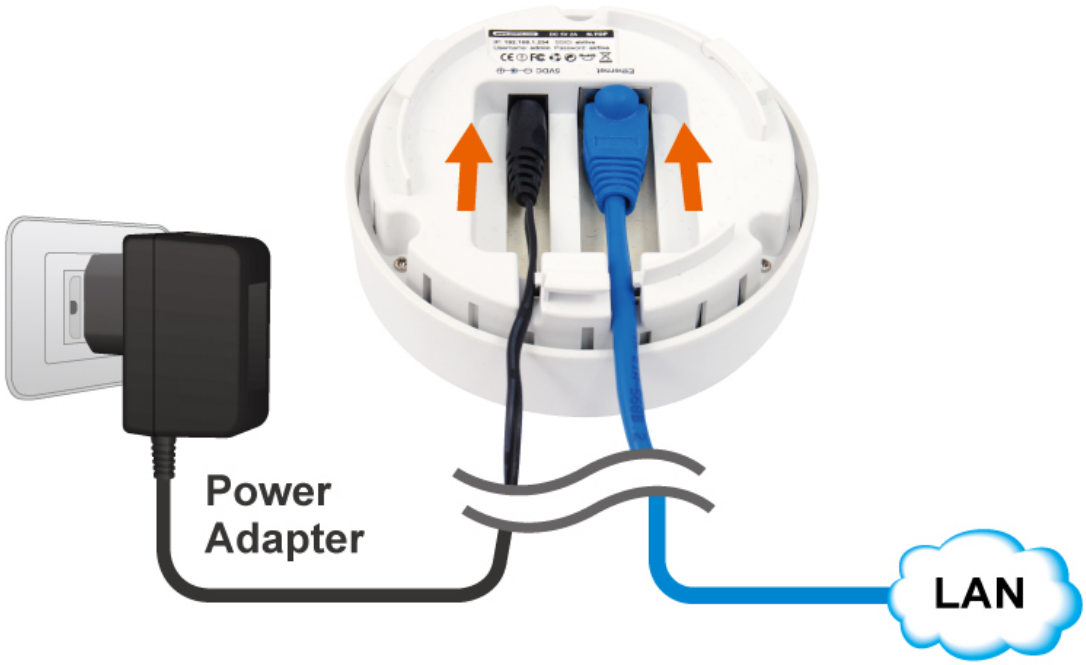
2. There are two ways to connect N.TOP,

(1) Via PoE

N.TOP is equipped with 802.3af compliant PoE port. You can select AirLive PoE-48PB for the deployment of the PoE network environment. The POE-48PB is an optional accessory that must be purchased separately. ***You must use Cat.5E or better graded Ethernet Cable for PoE Installation.***



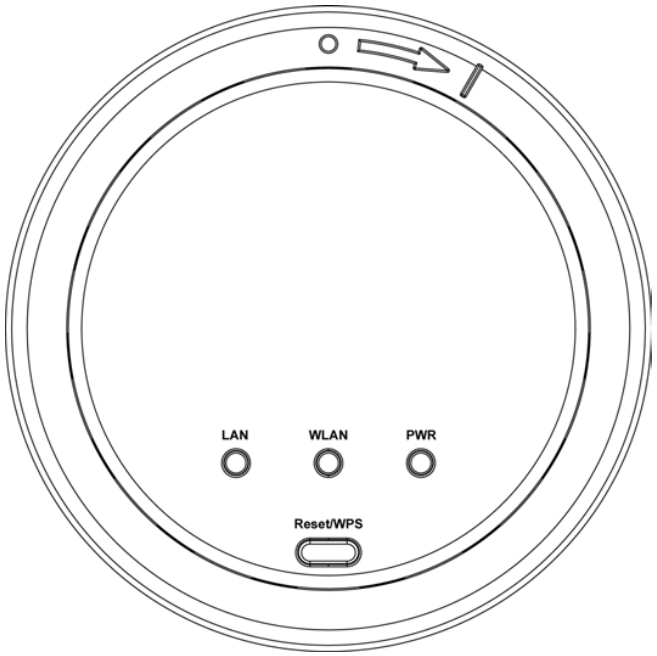
(2) Via power adapter



3. Put the case screws back.

2.4 LED Indicators

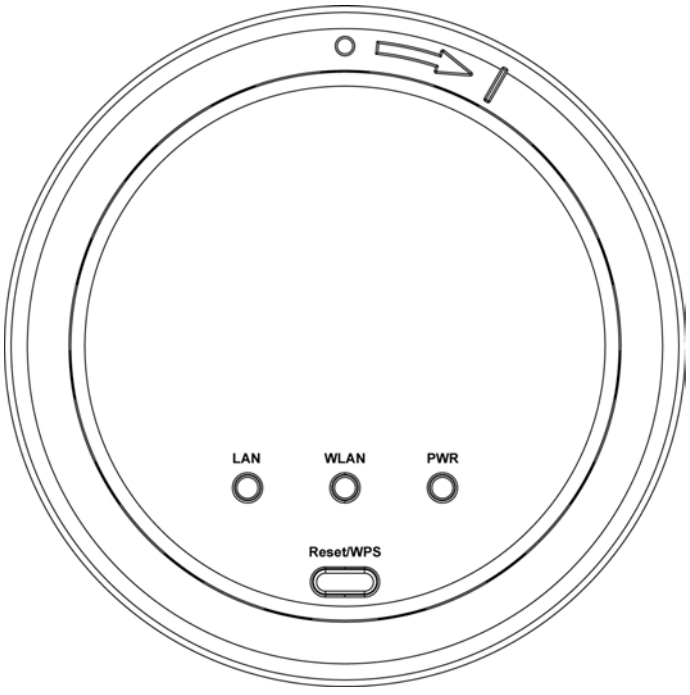
This section describes the LED behavior of N.TOP.
You can find the LED in front of the N.TOP.



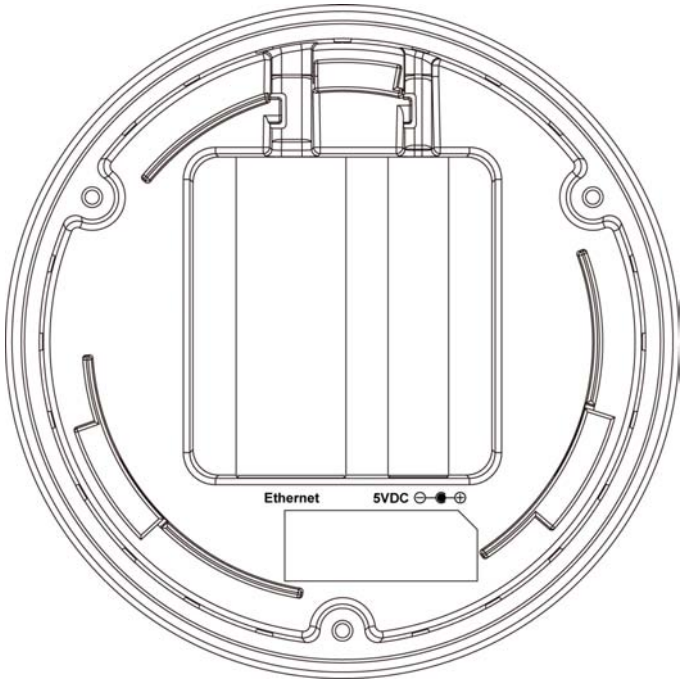
LED	Display	Status	Description
1	PWR	On	The access point is switched on and correctly powered.
		Slow Blinking	System is reset to factory default, at the same time WLAN LED is on.
		Off	The access point is switched off.
2	WLAN	On	Wireless WPS mode is enabled.
		Off	Wireless network is switched off.
		Flashing	Wireless LAN activity (transferring or receiving data).
3	LAN	On	LAN port is connected
		Off	LAN port is not connected
		Flashing	LAN activity (transferring or receiving data)

2.5 Button and Connector Definition

This section describes the button behavior of N.TOP.
You can find the Button in front of the N.TOP.



Button	Description
Reset / WPS	Reset the router to factory default settings (clear all settings) or start WPS function. • **Reset:** Press this button and hold for 10 seconds to restore all settings to factory defaults. • **WPS:** Press this button for less than 5 seconds to start WPS function.



Connector	Description
Power	Power connector, connects to A/C power adapter.
Ethernet	Local Area Network (LAN) port.

3 Configuring the N.TOP

The N.TOP offers web browser (http) as management interface. In this chapter, we will explain N.TOP's web management interface and how to get into them.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the password and SSID are case sensitive.

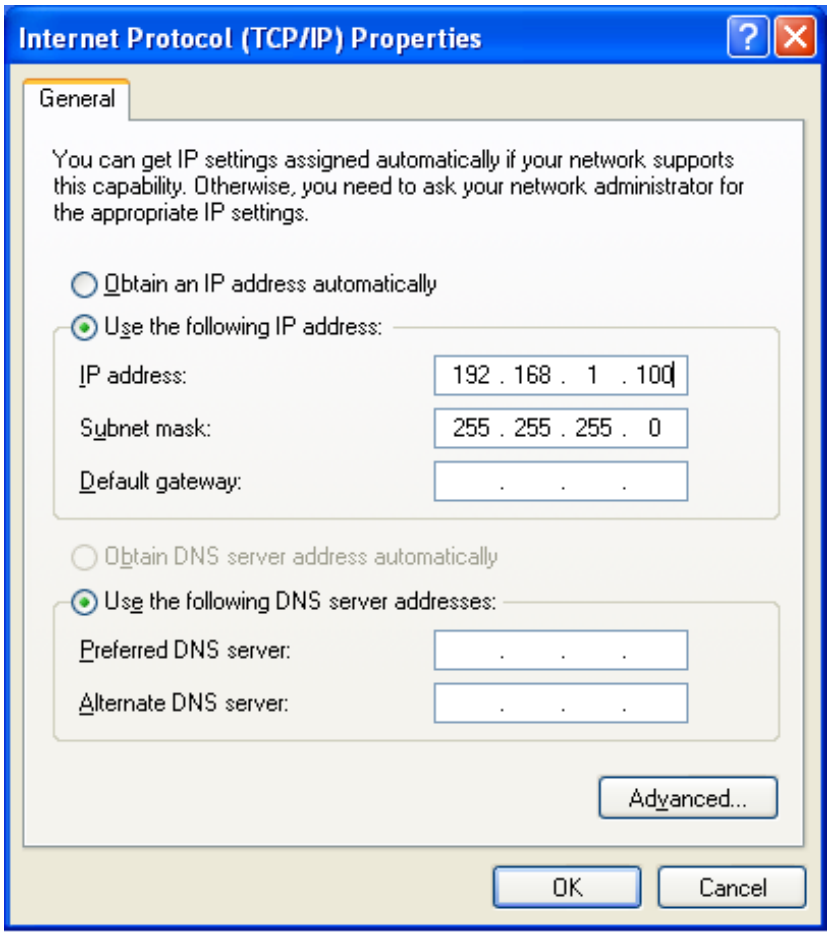
- The default IP address is: **192.168.1.254** Subnet Mask: **255.255.255.0**
- The default user's name is: **admin**
- The default password is: **airlive**
- The default SSID is: **airlive**
- The default wireless mode is : **AP mode**
- After power on, please wait for 1 minutes for N.TOP to finish boot up
- Please remember to click on "**Apply**" for new settings to take effect
- **You must reboot the N.TOP after you finish all the settings for changes to take effect**
- By Default, the DHCP server is turned off, please to configure your PC's IP address manually.

3.2 Prepare your PC

The N.TOP can be managed remotely by a PC through either the wired or wireless network. The default IP address of the N.TOP is **192.168.1.254** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the same subnet of the N.TOP..

To prepare your PC for management with the N.TOP, please do the following:

1. Connect your PC directly to the LAN port of N.TOP
2. Set your PC's IP address manually to 192.168.1.100 (or other address in the same subnet)



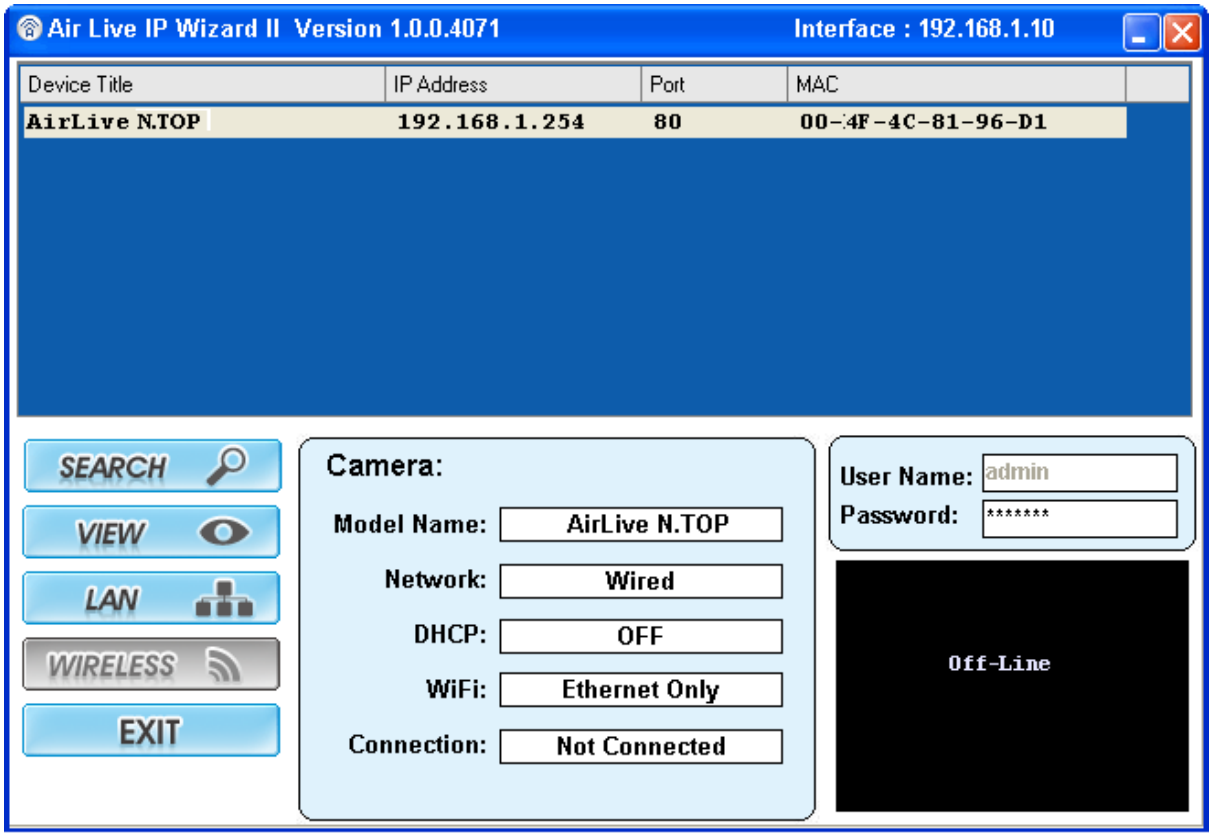
You are ready now to configure the N.TOP using your PC.

3.3 Introduction to IP Finder

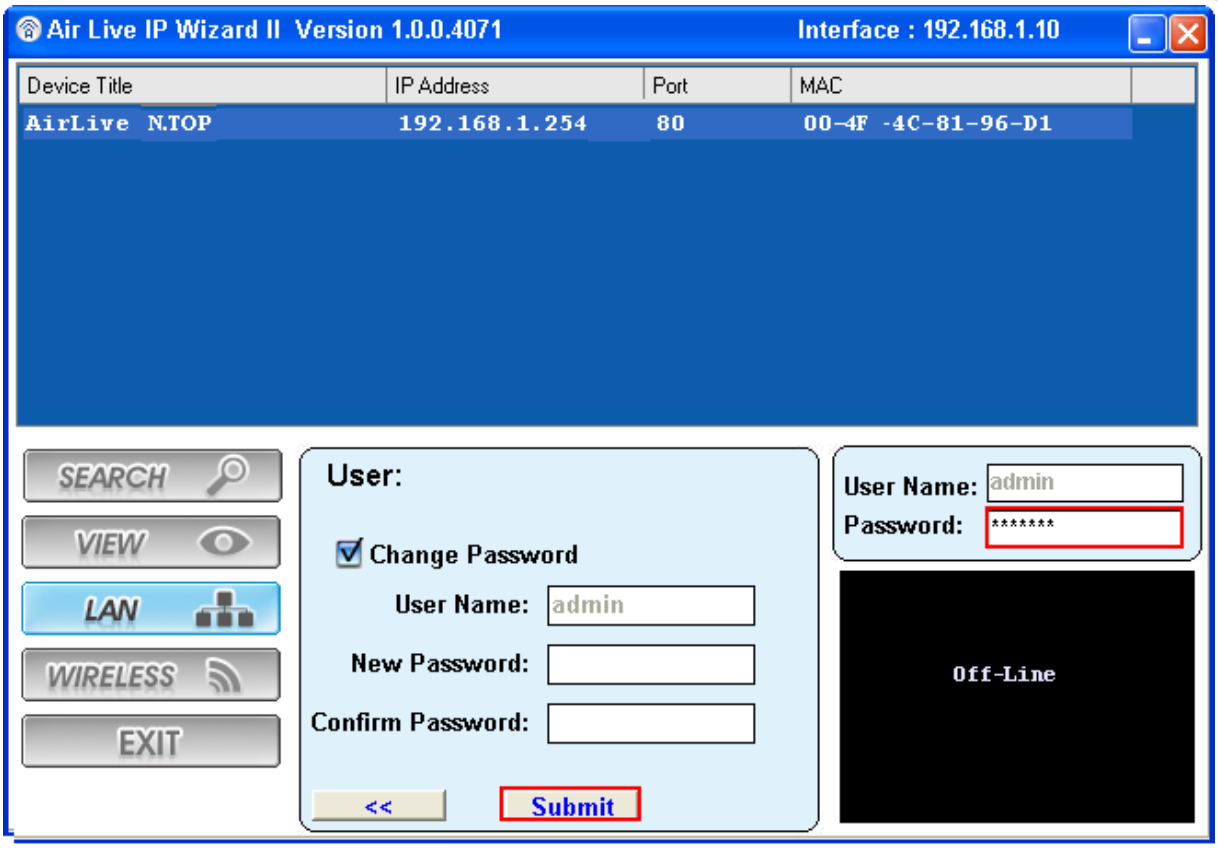
The N.TOP provides IP Finder utility and you can get into web management easily. IP Finder is included in the CD. Just click and follow the step by step instruction to install.

While entering the IP Finder utility, the IP Finder will automatically search the AP available on the network. IP Finder will show the Device Name, IP Address, HTTP Port, and Ethernet MAC Address.

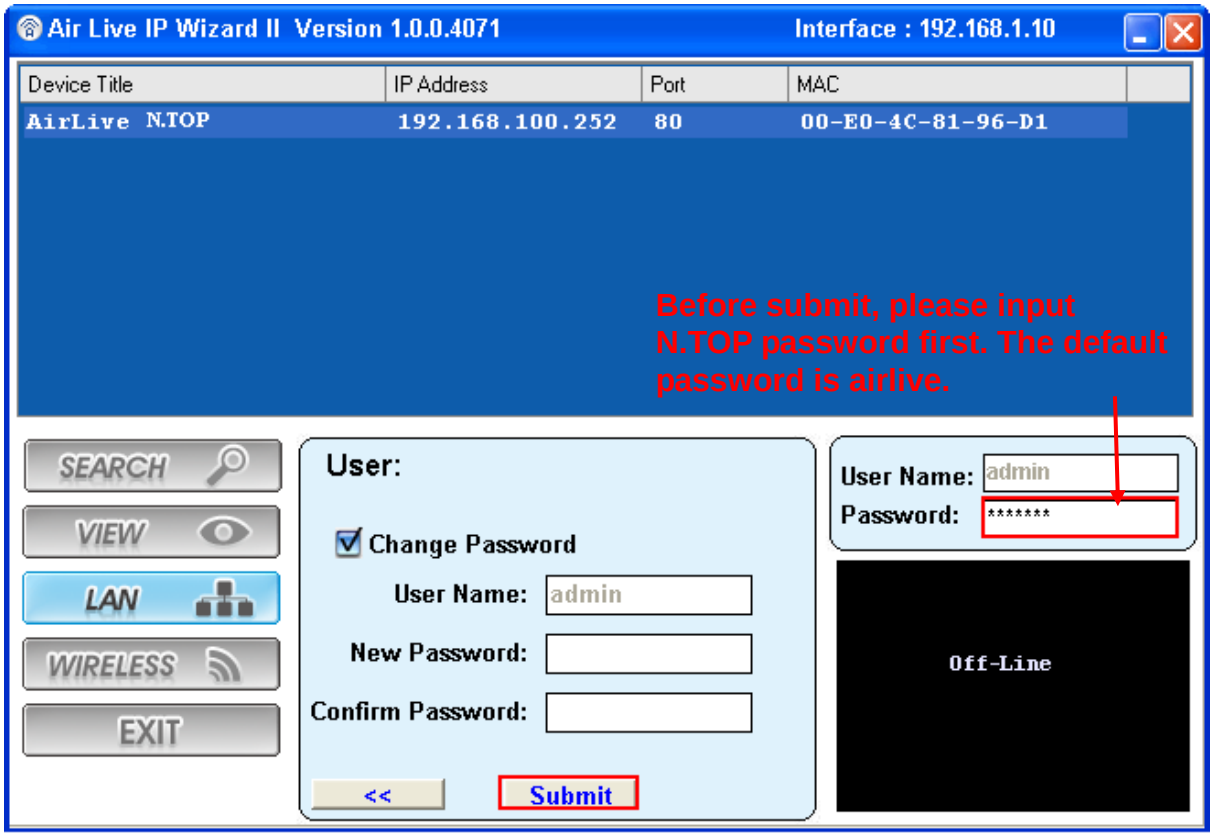
Before start using IP Finder, make sure you disable personal firewall installed in you PC. (Ex. Windows XP personal firewall)



- **Search:** By clicking Search, IP Finder will try to discover the N.TOP on the network.
- **View:** The function is for IP Camera only. It does not work for PC.
- **LAN:** You can configure the N.TOP LAN IP address here. After enter the IP Address, press >> to the next page. If you would like to change the N.TOP login password, please check the box and enter the new password. Please note that the password should be filled before clicks submit.
- **Exit:** Click to close IP Finder.



Click to the next page



Click Submit to save the configuration.

3.4 Introduction to Web Management

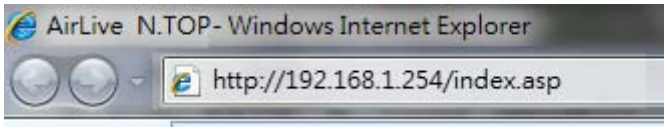
The N.TOP can be configured using the Web management interfaces by simply typing its IP address in the web browser. Most functions of N.TOP can be accessed by it.

If you are placing the N.TOP behind router or firewall, you might need to open the port 80 at virtual server on your firewall/router. This procedure is not necessary in most cases unless there is a router/firewall between your PC and N.TOP.

3.4.1 Getting into Web Management

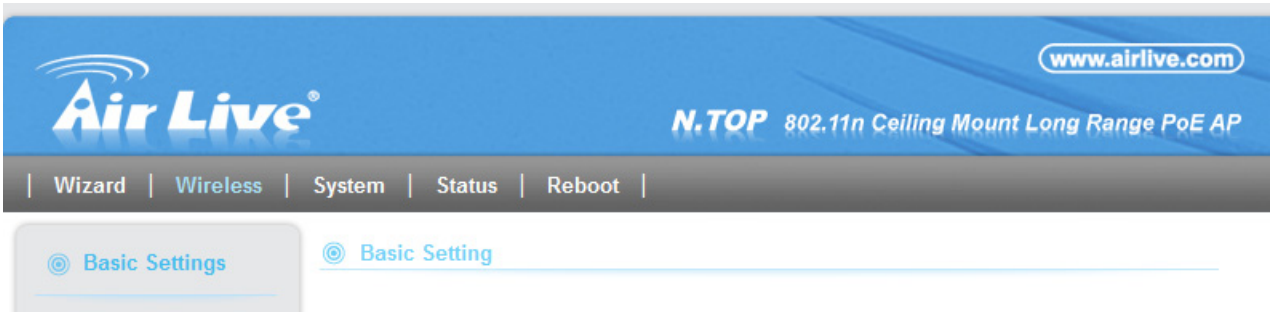
You can enter the web management by entering IP address into the web browser's address field.

- To get into the Normal Web Management, simply type in the N.TOP's IP address (default IP is **192.168.1.254**) into the web browser's address field.



3.4.2 Main Menu

After key in the correct username and password, you will enter the main Web management screen.



- **Wizard**:
  The wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.
- **Wireless**:
  You will find all the settings for wireless settings in this page. The N.TOP's wireless settings are different between wireless modes.
- **System:**
  All non-wireless and router mode settings are in this category. The system

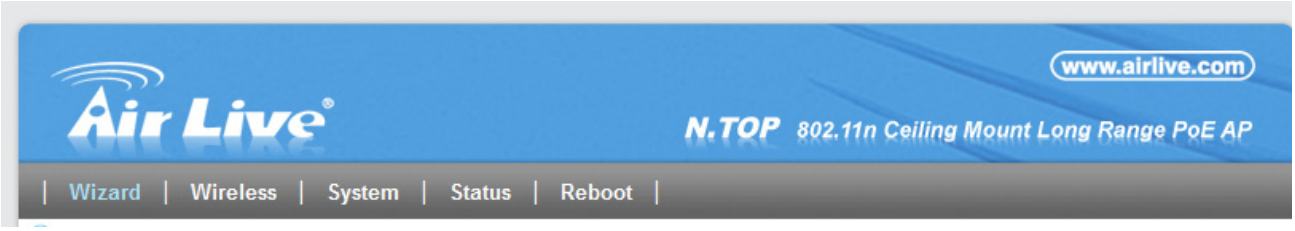
configurations including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management.

- **Status**:
  This section for monitoring the status of N.TOP. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Reboot:**
  Please remember to save changes and reboot after you finish all settings. The changes will take effect only after reboot.

3.5 Configuring with Setup Wizard

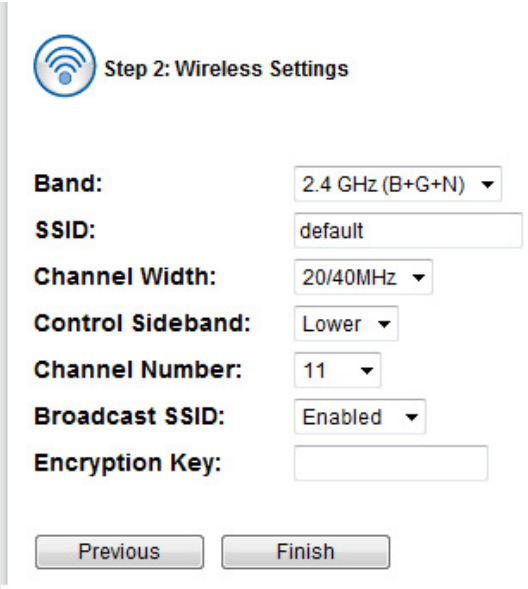
You can browse to activate the Setup Wizard

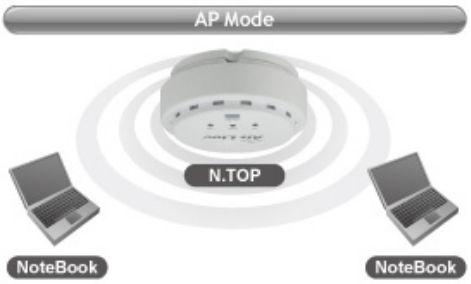
Step1: Login the Web UI of N.TOP, select "**Wizard**" for basic settings with simple way.



Step2: Select wireless mode that you deserved, and click "**Next**" to continue.

Step3: Setup your wireless settings such as **SSID**, **Wireless Channel** and **Encryption Key**…etc, and click "**Finish**" to apply the setting or click on "**Previous**" to the previous settings.





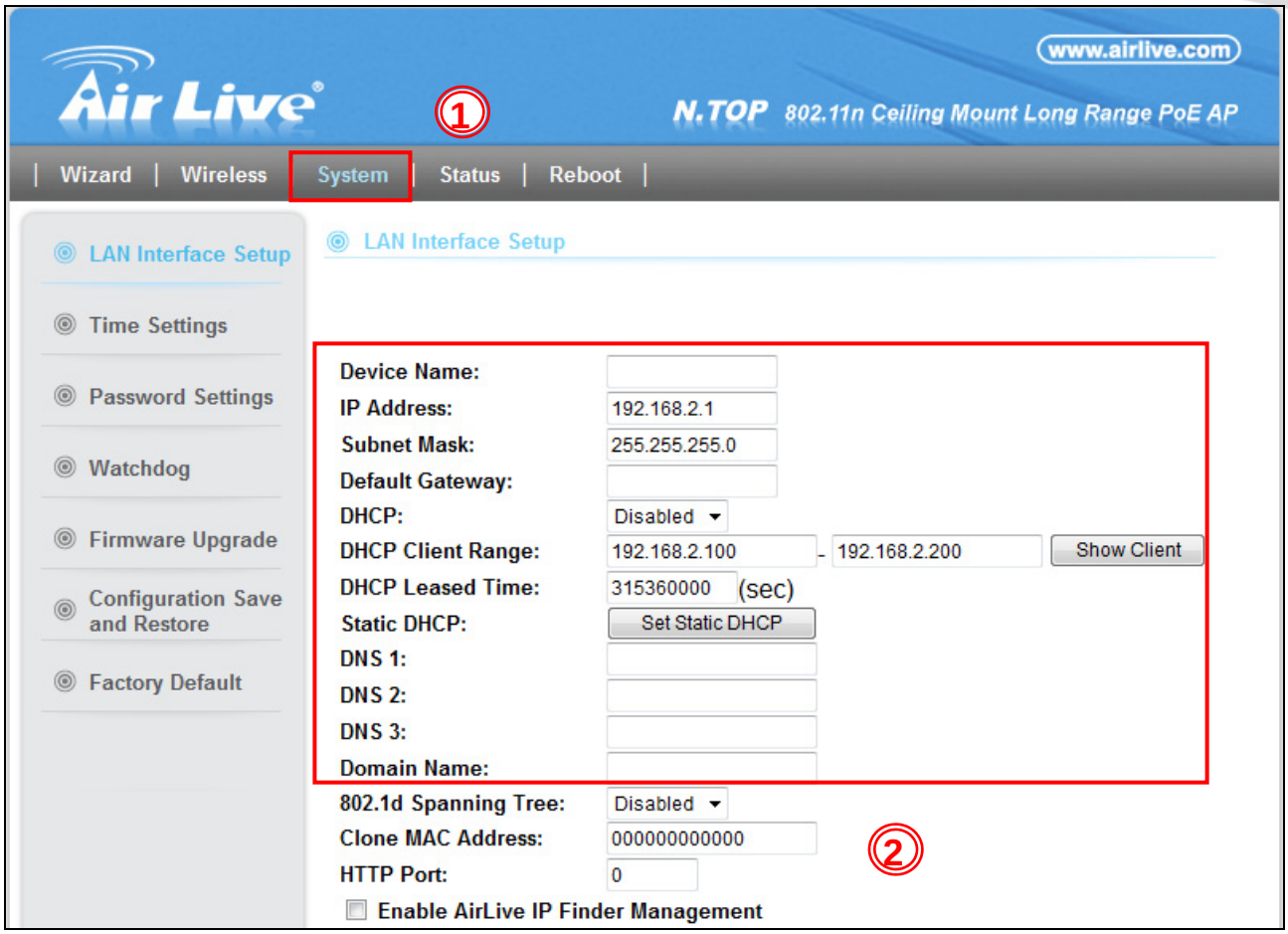
3.6 Initial Configurations

We recommend users to browse through N.TOP's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

3.6.1 Change the Device's IP Address

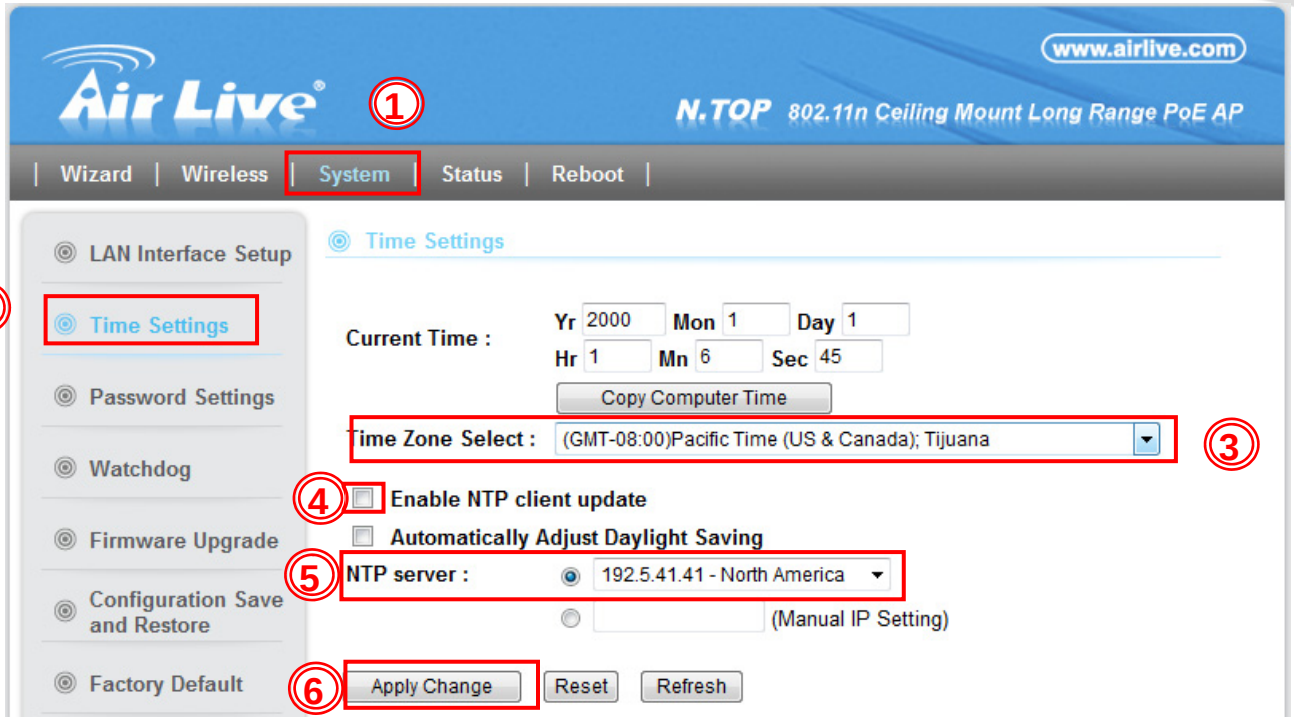
The default IP address is at **192.168.1.254**. You should change it to the same subnet as your network. Also, if you want to manage N.TOP remotely, you have to set the Gateway and DNS server information.

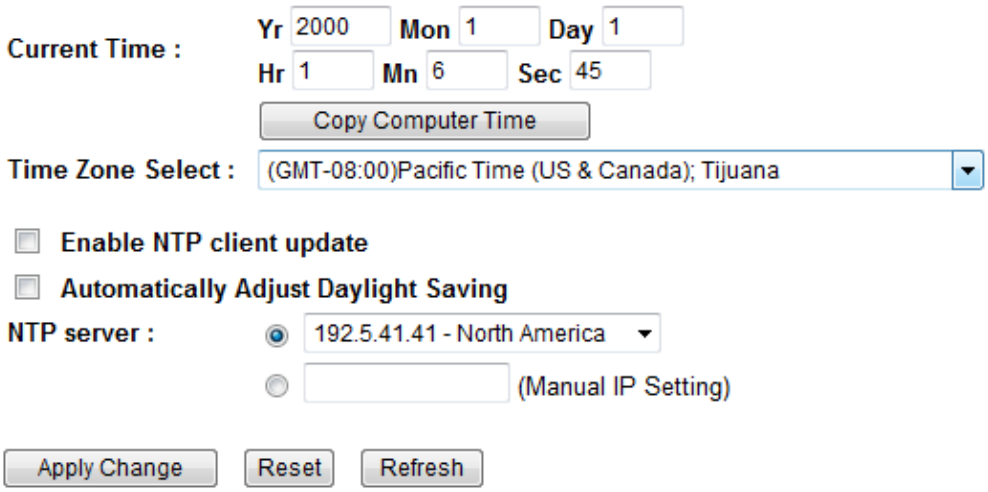
To setup the IP settings for N.TOP, please select "System Configuration" -> LAN Interface Setup". After entering the IP information, click on "Apply Changes" to finish.



3.6.2 Set the Time and Date

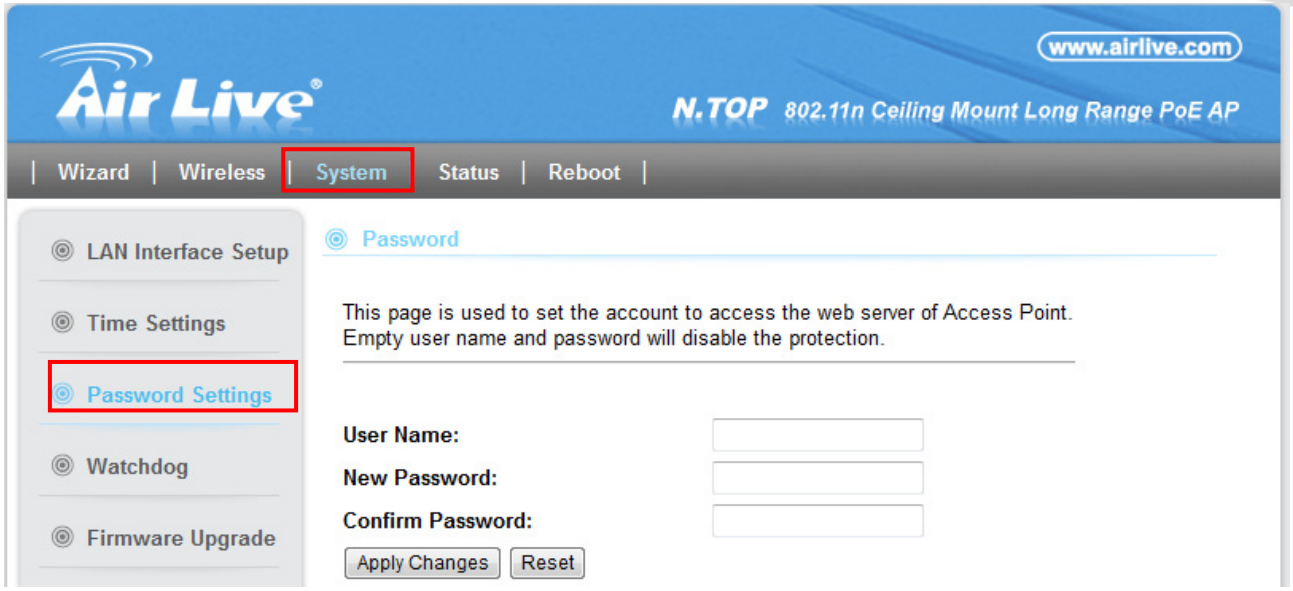
It is important that you set the date and time for your N.TOP so that the system log will record the correct date and time information. Please go to "*System Configuration" ->Time Settings*. We recommend you choose "Enable NTP" so the time will be keep even after reboot. If your N.TOP is not connected to Internet, please enter the time manually. Please remember to select your local time zone and click "Apply" to finish.





3.6.3 Change Password

You should change the password for N.TOP at the first login. To change password, please go to "***System***" -> "***Password Settings***" menu.


www.airlive.com
N.TOP 802.11n Ceiling Mount Long Range PoE AP
Wizard
Wireless
System
Status
Reboot
LAN Interface Setup
Time Settings
Password Settings
Watchdog
Firmware Upgrade
Password
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:
Confirm Password:
Apply Changes
Reset


User Name:
New Password:
Confirm Password:
Apply Changes
Reset

4 Wireless Settings

In this chapter, we will explain about the wireless settings in web management interface. Please be sure to read through Chapter1's Wireless Operation Mode and Chapter 3's "*Introduction to Web Management"* and *"Initial Configurations"* first.

Although router mode settings (WAN port, Virtual Server…etc) are part of the wireless settings menu, they will be explained in Chapter 5.

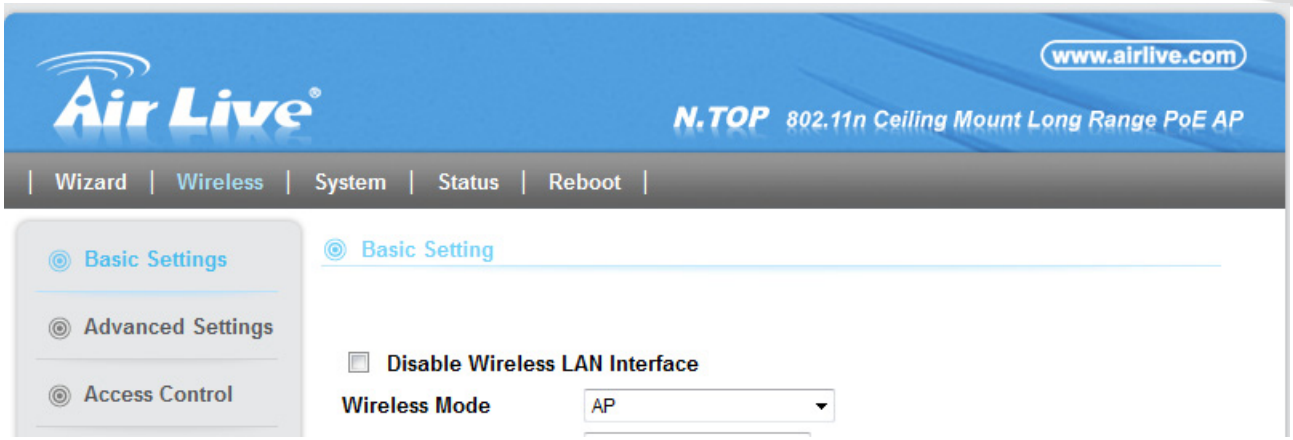
4.1 About Wireless Modes

The N.TOP has total of 5 operation modes to suit different application requirements. In this section, we will explain how to change between wireless operation modes. For explanation on each different operation mode, please read Chapter 1 section 1.4 first.

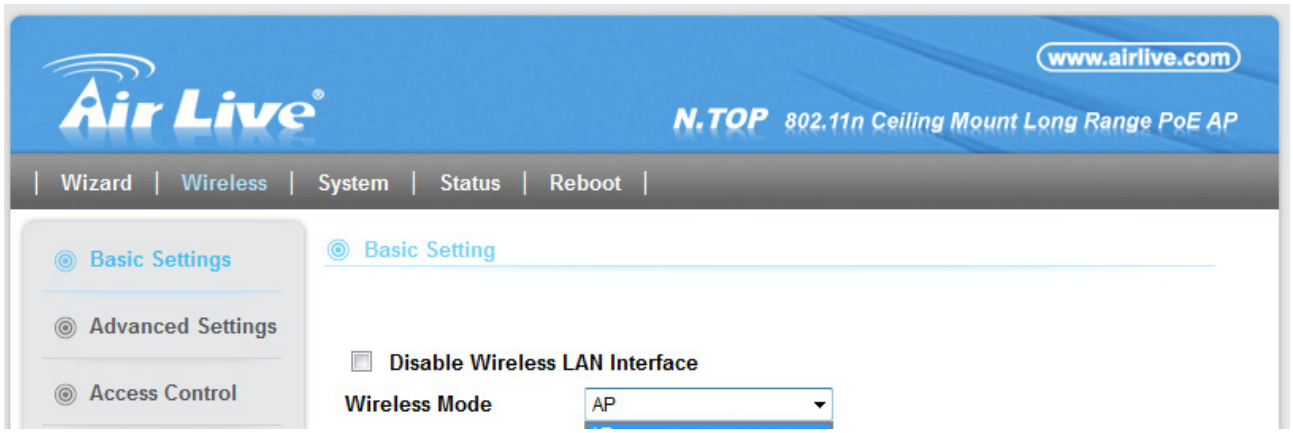
Below is the summary table for different wireless modes:

N.TOP Wireless Operation Mode			
Wireless Mode	**Radio**	**WAN**	**Application**
Access Point	AP	None	Hotspot (Indoor and Outdoor)
Client	Client	None	WISP Client
Bridge	Bridge	None	Building to Building network
WDS Repeater	AP + Client	None	Extend distance of another WDS AP/Router
Universal Repeater	AP + Client	None	Extend distance of any AP Router

To change between different wireless modes, please to go the "**Wireless**" menu, on the left hand side bar, you will see the "**Wireless Mode**" pull down menu which displays the current operation mode.



To change wireless mode, please select the new wireless mode from the pull-down menu. The N.TOP will ask you to confirm about the mode change. After your confirmation, the AP will reboot itself to the new mode.



4.2 Basic Wireless Functions

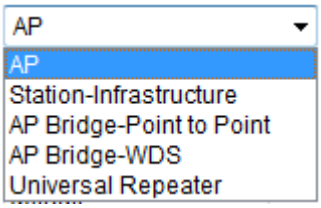
This section will explain the general wireless functions. Not all functions are available in every wireless mode. Please refer to the web interface what is available of each mode.

When you select "***Wireless*"** on the top menu; the following screen will appear:

4.2.1 Wireless Mode

Wireless -> Wireless

There are 5 wireless modes such as AP, Bridge, Client, Repeater and more for you can work in different application environments



4.2.2 Band

Wireless -> Band

N.TOP has 6 different options for WLAN transmission. All devices in the same network should use the same WLAN mode.

- **2.4 GHz (B):** The radio will only connect at 11b mode.
- **2.4 GHz (G):** The radio will only connect at 11g mode.
- **2.4 GHz (N):** The radio will only connect at 11n mode.
- **2.4 GHz (B+G):** The radio will auto adjust between 11g and 11b mode.
- **2.4 GHz (G+N):** The radio will auto adjust between 11n and 11g mode.
- **2.4 GHz (B+G+N):** The radio will auto adjust between 11n, 11g and 11b mode. It is recommended to use this mode.

4.2.3 Network Name (SSID)

Wireless -> Network Name (SSID)

The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the same wireless network. The SSID length is up to 32 characters. The default SSID is "**airlive**".

4.2.4 Broadcast SSID

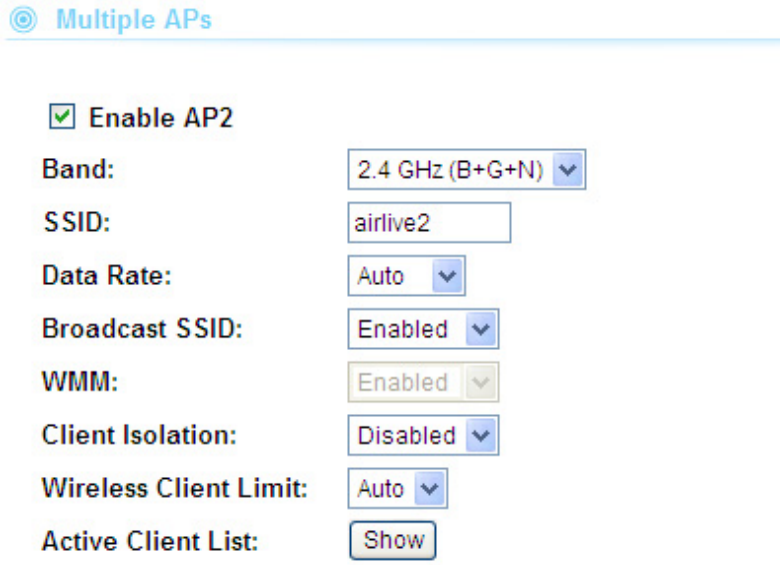
Wireless Settings -> Broadcast SSID

When this function is disabled, the wireless network will become invisible. Only people who know the SSID name can join the network. It is recommended to use this feature to protect the network from intruders. However, once this function is disabled, it might be necessary to configure the wireless connection manually. This option is available in AP mode, AP Router mode, and Repeater modes only.

4.2.5 Multiple SSID

Wireless -> Multiple SSID

Multiple SSID allows Air3G to create up to **4** different wireless networks (SSID). It is also known as "**Virtual AP**" function. Each SSID can have its Encryption policy. The SSID1 is the main SSID under Wireless Setting page.



4.2.6 Channel

Wireless -> Channel

The channel is the frequency range used by radio. In 802.11n/g/b standard, there are maximum of 14 Channels. However, the available channels in each country are dependant on the local regulation. If you are living in Europe, you can use channel 1 to 13. If you are living in the United States, you can use channel 1 to 11.

Each wireless channel takes between 22 to 25MHz of frequency width. But the channels are only 5MHz apart. Therefore, only every 5 channels can be free of interference with each other. It is recommended that you can do a site survey to find about what channels are used by surrounding AP and choose a channel that is not used by other APs.

Channel	Frequency (MHz)	U.S.A.	Europe
1	2412	O	O
2	2417	O	O
3	2422	O	O
4	2427	O	O
5	2432	O	O
6	2437	O	O
7	2442	O	O
8	2447	O	O

9	2452	O	O
10	2457	O	O
11	2462	O	O
12	2467	-	O
13	2472	-	O
14	2484	-	-

4.2.7 Channel Width

Wireless -> Channel Width

You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

4.2.8 Wireless Client Limit

Wireless -> Wireless Client Limit

This limitation applies to number of wireless clients the device can associate. If you need to serve wireless connection to large number of users in one location. You can deploy many APs and limit the number of wireless clients, so any additional wireless connection attempt will be rejected (therefore, redirect to other AP). The range of user limitation is from 1 to 31.

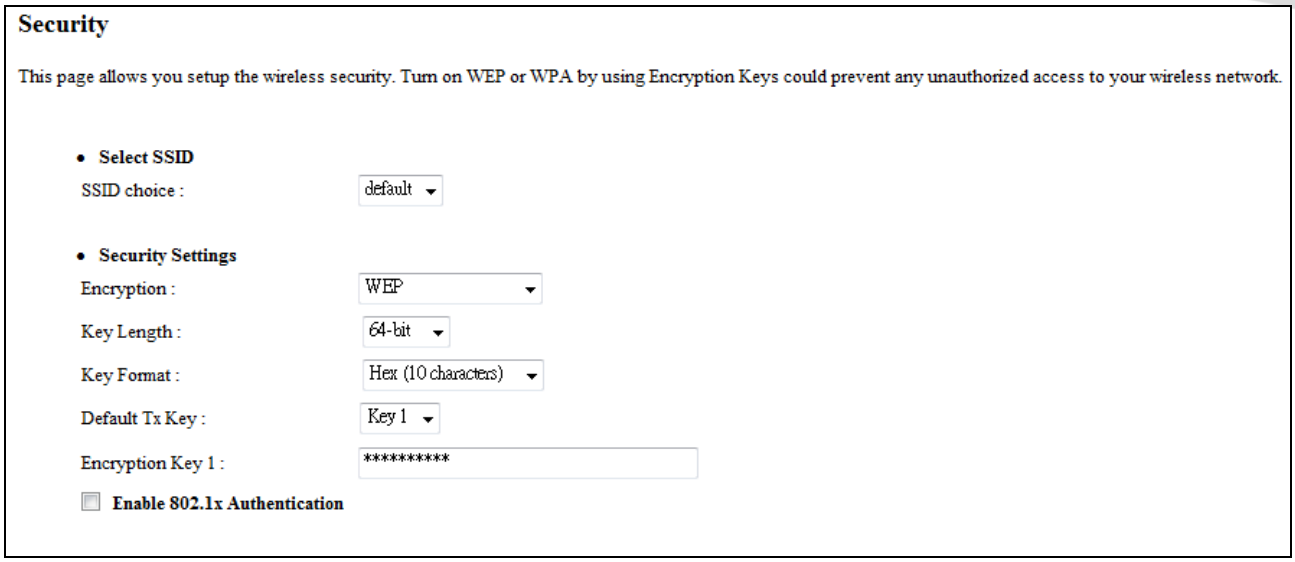
4.2.9 Security

Wireless -> Security

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The N.TOP features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal.

WEP

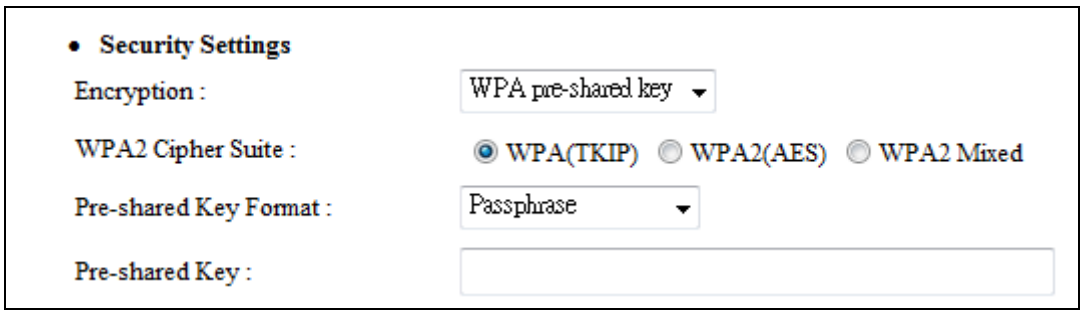
WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



- **Key Length:** The N.TOP offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
- **Key Format:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. “airlivepass12”). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.

WPA(TKIP), WPA(AES), WPA Mixed

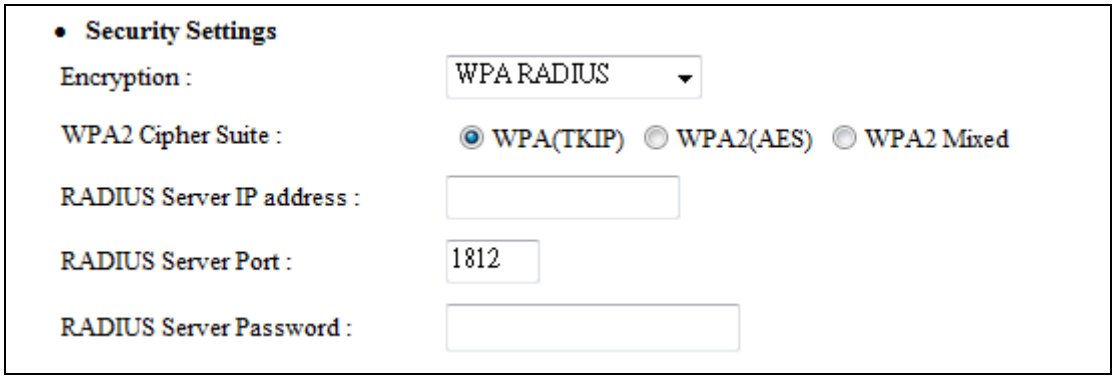
Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA Mixed tries to authenticate wireless clients using both WPA-PSK and WPA2-PSK.



- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

WPA Radius

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using either WPA or WPA2.



4.2.10 WMM

Wireless -> WMM

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

The Wi-Fi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and it is enabled under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.

4.2.11 Data Rate

Wireless -> Data Rate

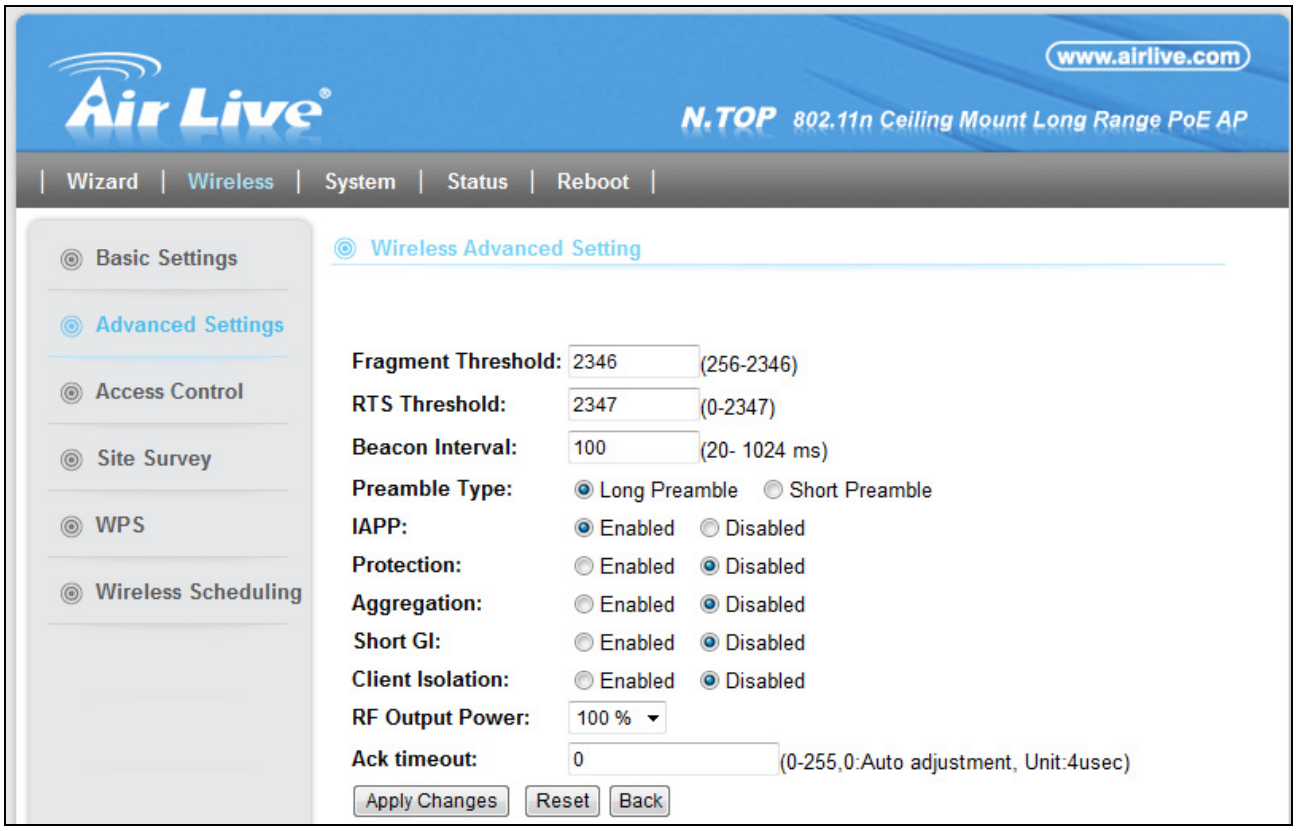
Data Rate is the physical speed of transmission. The default setting is Auto. In “Auto” mode, the data rate will adjust according to the connection condition. It is advised to put the data rate in Auto.

4.2.12 N Data Rate

Wireless -> N Data Rate

N Data Rate is the physical speed of transmission for 802.11n. The default setting is Auto. In “Auto” mode, the data rate will adjust according to the connection condition. It is advised to put the data rate in Auto. However, you can also force the radio to operate at specific data rate. The highest for 11n is MCS15.

4.3 Advance Settings



- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "**noisy**" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **IAPP:** IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.

- **Protection:** Select Enabled or Disabled to execute the security function.

- **Aggregation:** Select Enabled or Disabled to execute this function.

- **Short GI:** Select Enabled or Disabled to execute this function.

- **Client Isolation:** The default setting is "**Disable**". When enabled, the wireless clients will not be able to communicate with each other. This feature is useful for public WiFi, WISP operators, and Hotspot operators.

- **RF Output Power**: You can adjust the transmit output power of the N.TOP's radio. The higher the output power, the more distance N.TOP can deliver. However, it is advised that you use just enough output power so it will not create excessive interference for the environment. Also, using too much power at close distance can create serious performance drop due to signal distortion.

  If you are not getting good signal, you can try to increase the output power. However; if your signal appear to be strong but the performance is low, it is advised to reduce the output power.
  Please make sure not to exceed the legal limit of output power in your country. For EU, it is limited to 20dBm. For U.S.A., the limit is 23dBm.

- **Ack timeout**: Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the

remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput.
If the ACK setting is too high then throughput will be lost due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The N.TOP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the N.TOP will automatically calculate the correct ACK timeout value, it should have a value of 0-255 sec.

4.4 Access Control

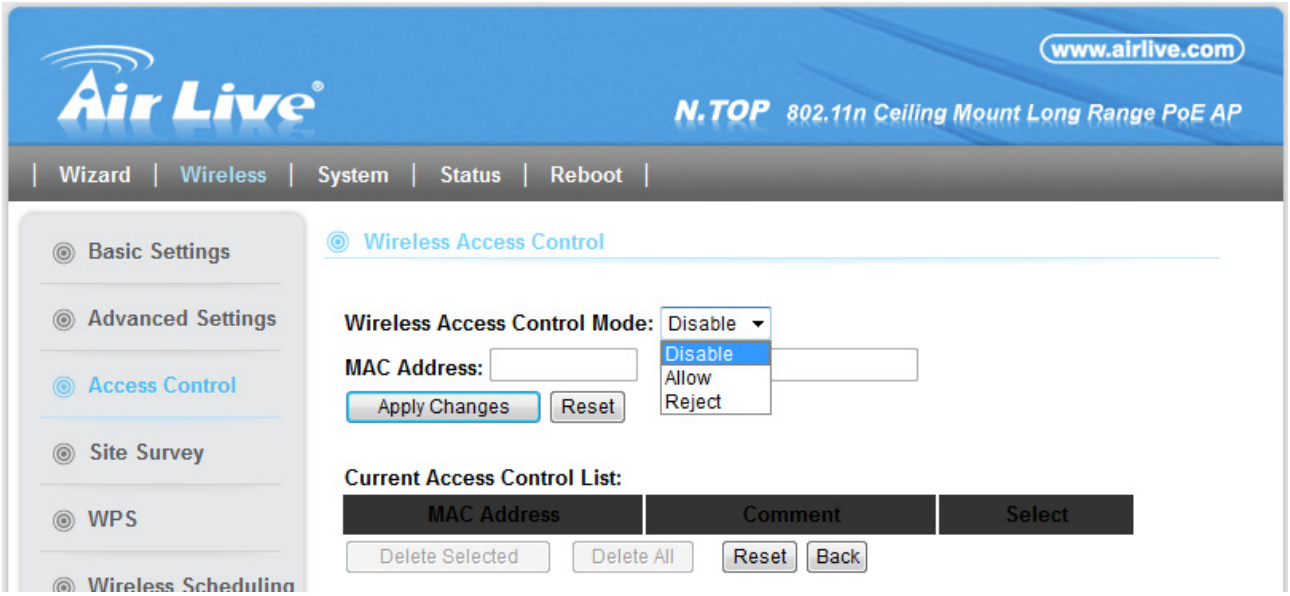
Wireless -> Access Control

The N.TOP allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and AP Router modes. This function is available only for Access Point and Gateway modes.

- **Disable:** When selected, no MAC address filtering will be performed.
- **Allow list:** When selected, data traffic from only the specified devices in the table

will be allowed in the network.

- **Reject list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

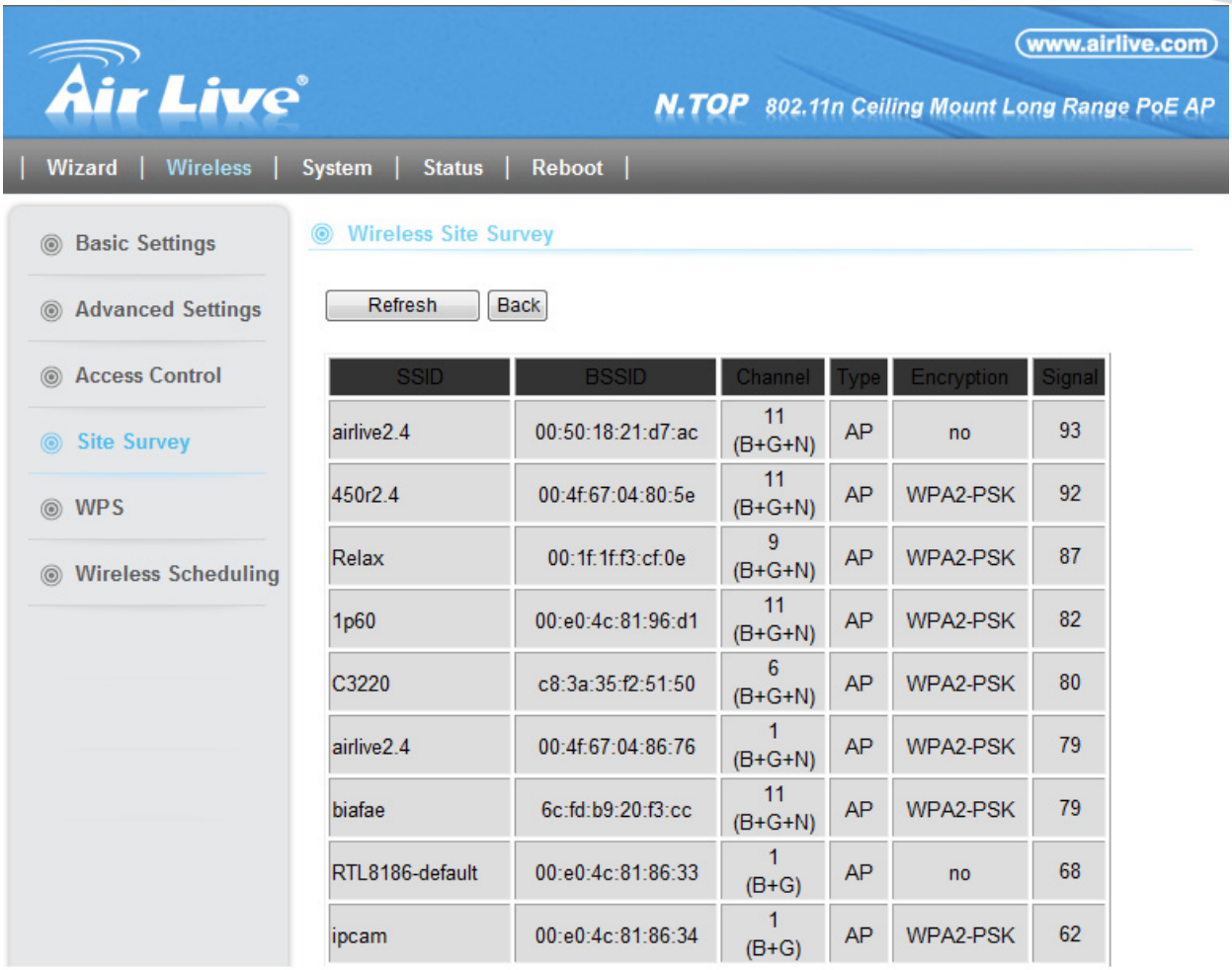


4.5 Site Survey

Wireless -> Site Survey

You can scan for wireless networks around your location using the Site Survey function. From the site survey function, you can also perform antenna alignment and establish wireless connection

When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area.

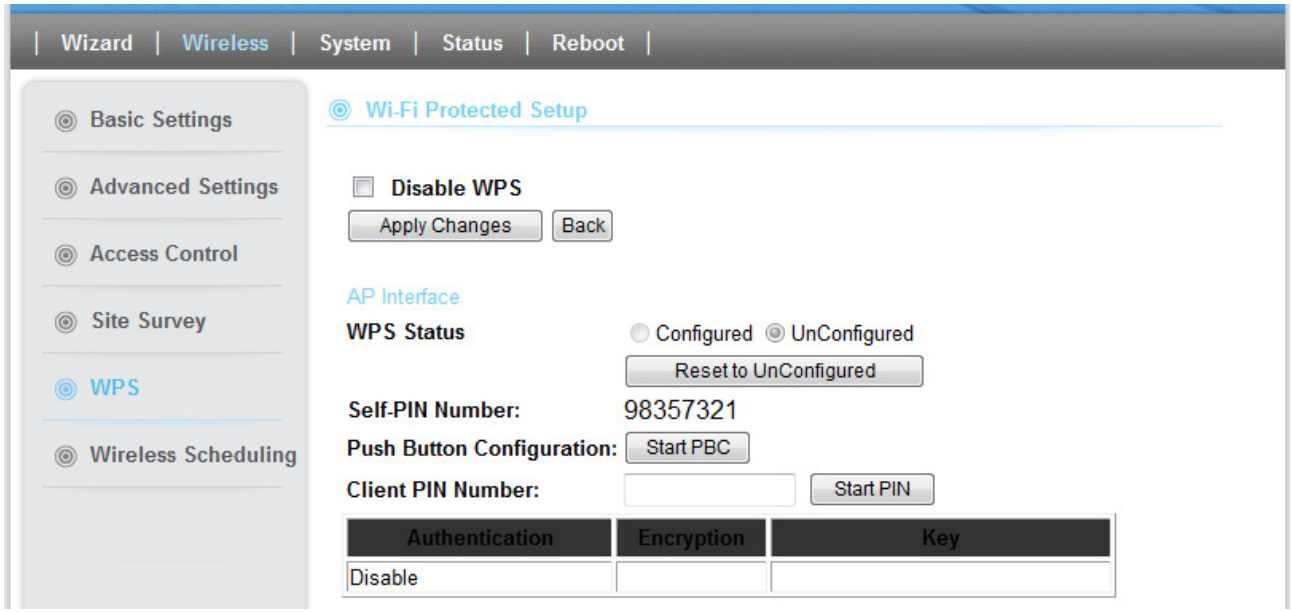


SSID	BSSID	Channel	Type	Encryption	Signal
airlive2.4	00:50:18:21:d7:ac	11 (B+G+N)	AP	no	93
450r2.4	00:4f:67:04:80:5e	11 (B+G+N)	AP	WPA2-PSK	92
Relax	00:1f:1f:f3:cf:0e	9 (B+G+N)	AP	WPA2-PSK	87
1p60	00:e0:4c:81:96:d1	11 (B+G+N)	AP	WPA2-PSK	82
C3220	c8:3a:35:f2:51:50	6 (B+G+N)	AP	WPA2-PSK	80
airlive2.4	00:4f:67:04:86:76	1 (B+G+N)	AP	WPA2-PSK	79
biafae	6c:fd:b9:20:f3:cc	11 (B+G+N)	AP	WPA2-PSK	79
RTL8186-default	00:e0:4c:81:86:33	1 (B+G)	AP	no	68
ipcam	00:e0:4c:81:86:34	1 (B+G)	AP	WPA2-PSK	62

- **SSID**: This is the remote AP's SSID.
- **MAC**: This is the remote's AP's MAC address.
- **Channel**: The current scanned channel
- **Type**: The wireless type of remote AP.
- **Encryption**: The wireless encryption of remote AP.
- **Signal**: This is signal strength number in percentage in 0 to 100 scales. The higher the number, the better signal.

4.6 WPS

Wireless Settings -> WPS

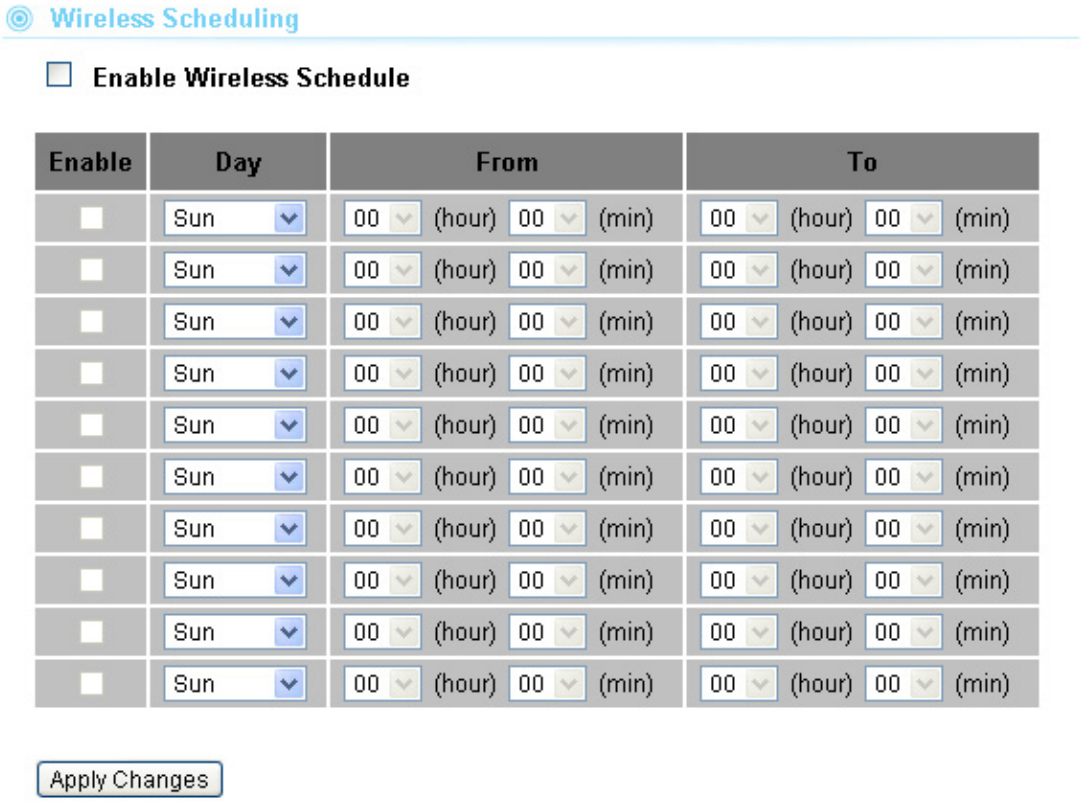


- **Disable WPS**: Check the box to disable the WPS function, default setting is enabled.
- **WPS Status**: Here shows the current status of the WPS function. Default setting is configured; click **Reset to UnConfigured** to re-configure the WPS connection.
- **Self-PIN Number**: Here shows the 8-digit numbers PIN code of the router itself. Enter the Self-PIN Number to client (Registrar) end and click the PIN button at the client end to make a WPS connection. It will connect with the wireless router within two minutes and get IP address.
- **Push Button Configuration**: Click **Start PBC** button (or press the physical WPS button on the Wireless Router once), meanwhile, the client should also click the PBC button simultaneously within 2 minutes.
- **Client PIN Number**: Enter the client (Enrollee) PIN code into the blank field then click the **Start PIN** button to make a WPS connection with client. Then, the wireless router will connect to client within 2 minutes and get IP address

4.7 Wireless Scheduling

Wireless -> Wireless Scheduling

Check the box to enable the schedule function. Set up the time to schedule the wireless access rule. Select the day and time you want to enable the wireless function.

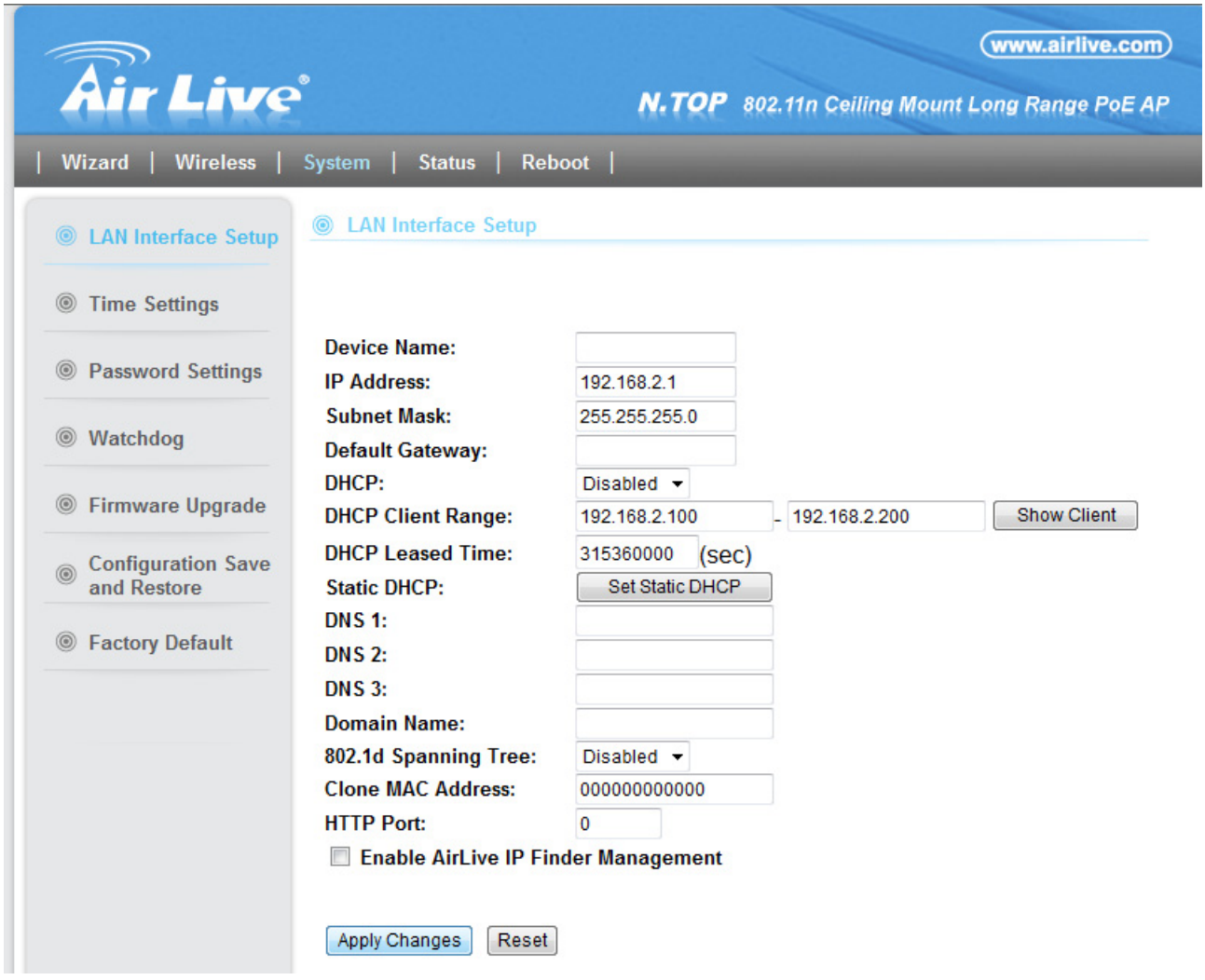


5 System Configurations

In this chapter, we will explain about *System Configurations* in web management interface. Please be sure to read through Chapter 3's "***Introduction to Web Management***" and "***Initial Configurations***" first. .

5.1 Menu Structure

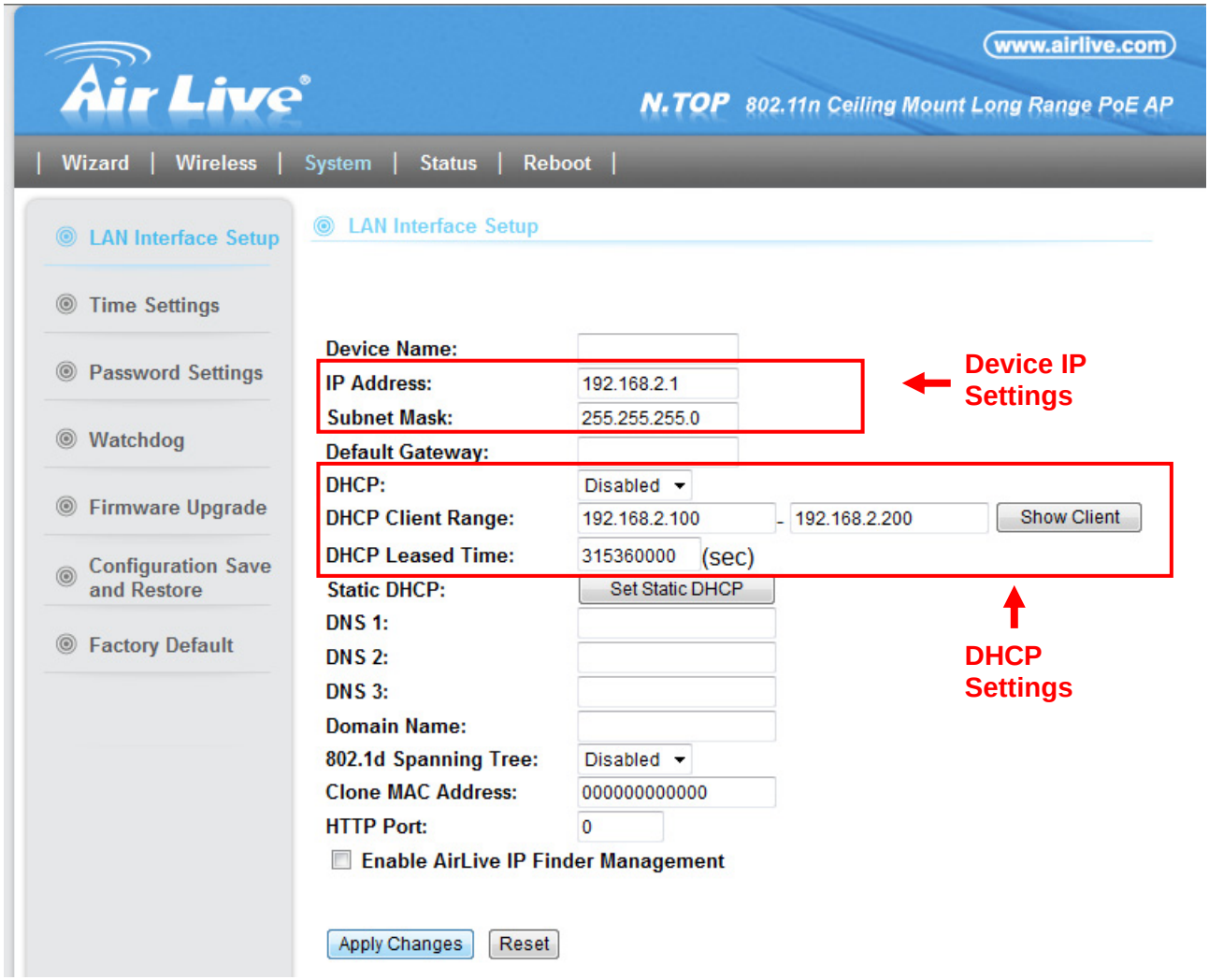
When you click on the "**System**" menu on the top menu bar, the following screen will appear. The system configuration includes all non-wireless settings. We will explain their functions here.



5.2 LAN Interface Setup

System >> LAN Interface Setup

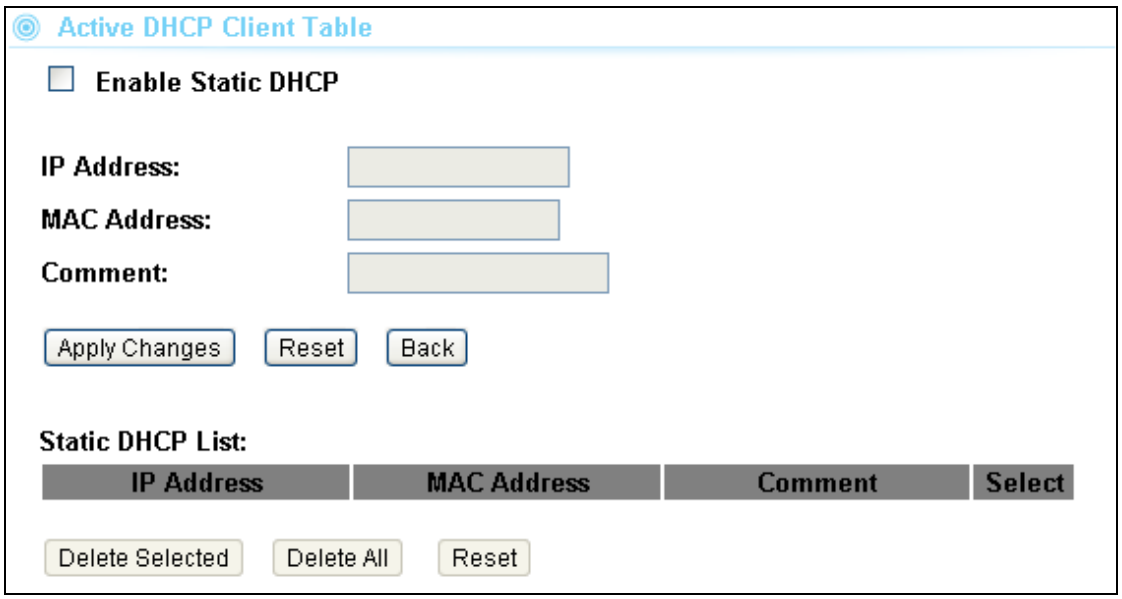
This menu is where you can configuration all the aspect about LAN interface including IP address, DHCP server settings etc.



5.2.1 DHCP Settings

- **DHCP Service:** You can enable or disable DHCP server here.
  - **Disable(default)**: Disable DHCP server
  - **Enable:** The N.TOP will act as DHCP server to provide IP addresses to the clients on the LAN/Wireless interface. By default, the DHCP server is on.
- **DHCP Client Range**: You can define the IP pool from which the DHCP clients can get IP address.. Click on "**Show Client"** to see the current DHCP client table.
- **DHCP Release Time:** You can define how long the N.TOP will reserve IP address for a particular PC or Device here.

5.2.2 Set Static DHCP



If you want to lock IP address to a MAC address, you should add DHCP clients to the "**Static DHCP List**". Up to 40 entries can be entered. Below is the procedure for adding an entry:

1. Enter the MAC address of the device
2. Enter the IP address of the device
3. Click on the "**Apply Changes**" button

5.2.3 Domain Name

You can enter the network area name here.

5.2.4 802.11d Spanning Tree

Select Disabled or Enabled form the pull-down list.

5.2.5 Clone MAC Address

You can change the MAC address of your LAN port to other value here.

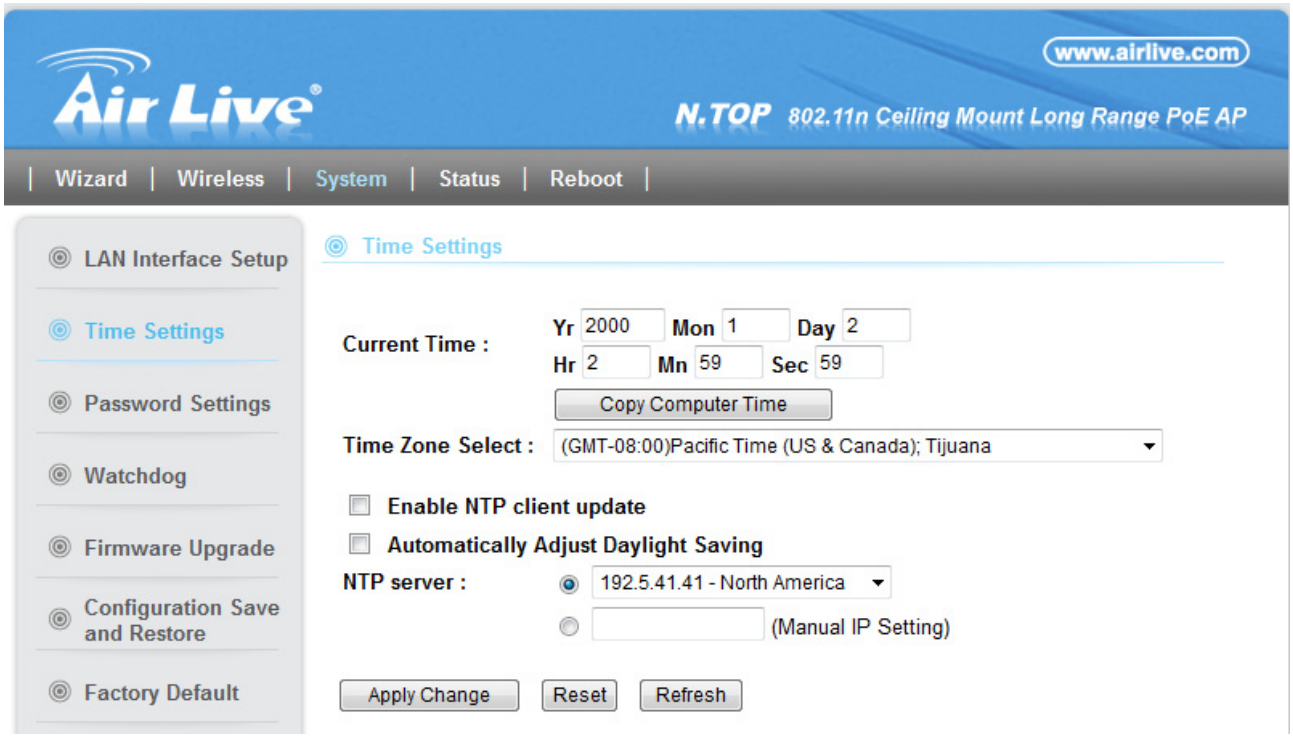
5.2.6 Enable AirLive IP Finder Management

By enabling the function, IP Finder could discover the N.TOP in the LAN.

5.3 Time Settings

System ->Time Settings

You can set the NTP Time Server for your N.TOP's internal clock here. You can use NTP server function so your N.TOP will check with NTP to set time automatically upon each startup. Thus, it prevents the clock losing track of time during reboot or power outage.



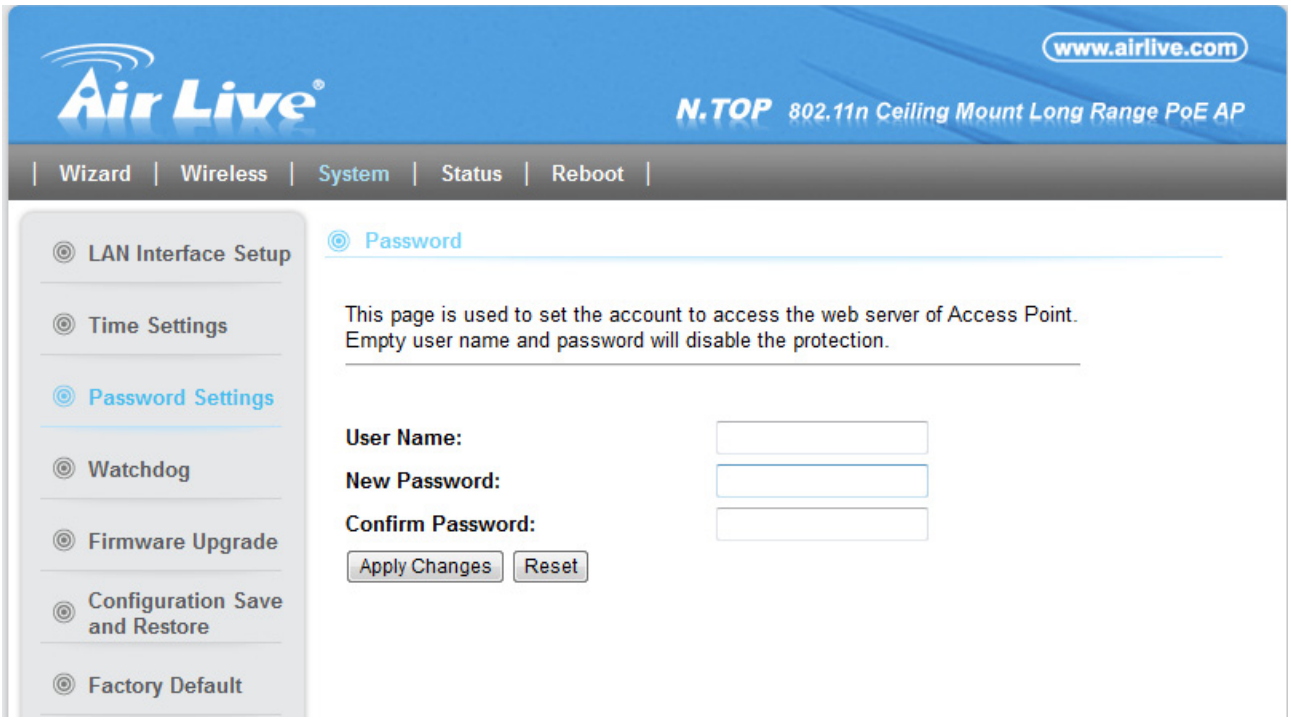
Below is the procedure to set your NTP server

1. Check the "**Enable NTP Client Update**"
2. Select your time Zone
3. Select your NTP server
4. Click on "**Apply Change**"

5.4 Password Settings

System -> Password Settings

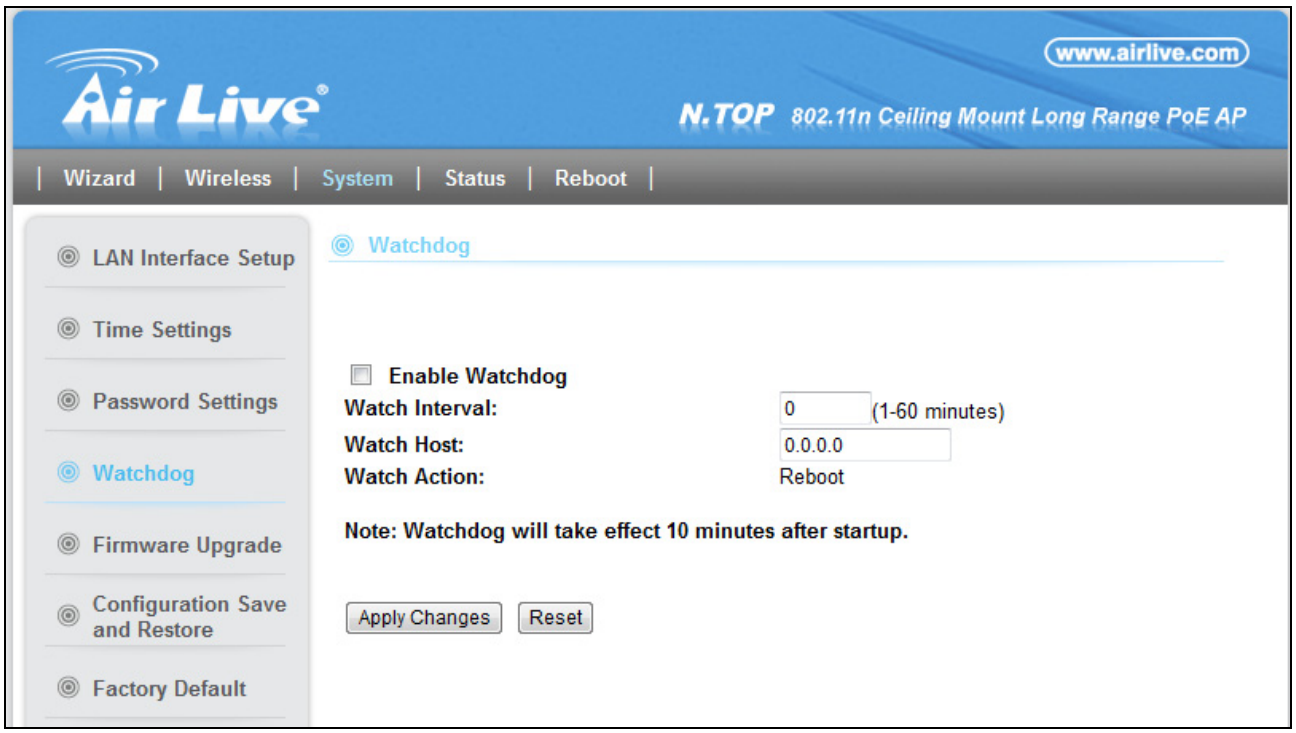
The N.TOP's password protection is turned off by default. To enable password protection or change password, just enter your username and password, and click on "**Apply Change**" button.



5.5 Watchdog

System -> Watchdog

The Ping Watchdog will ping remote IP addresses to make sure the wireless connection is active, if not, it will reboot. To prevent the AP from power recycling, the PING watchdog will start 10 minutes after power up to prevent power recycle problem.

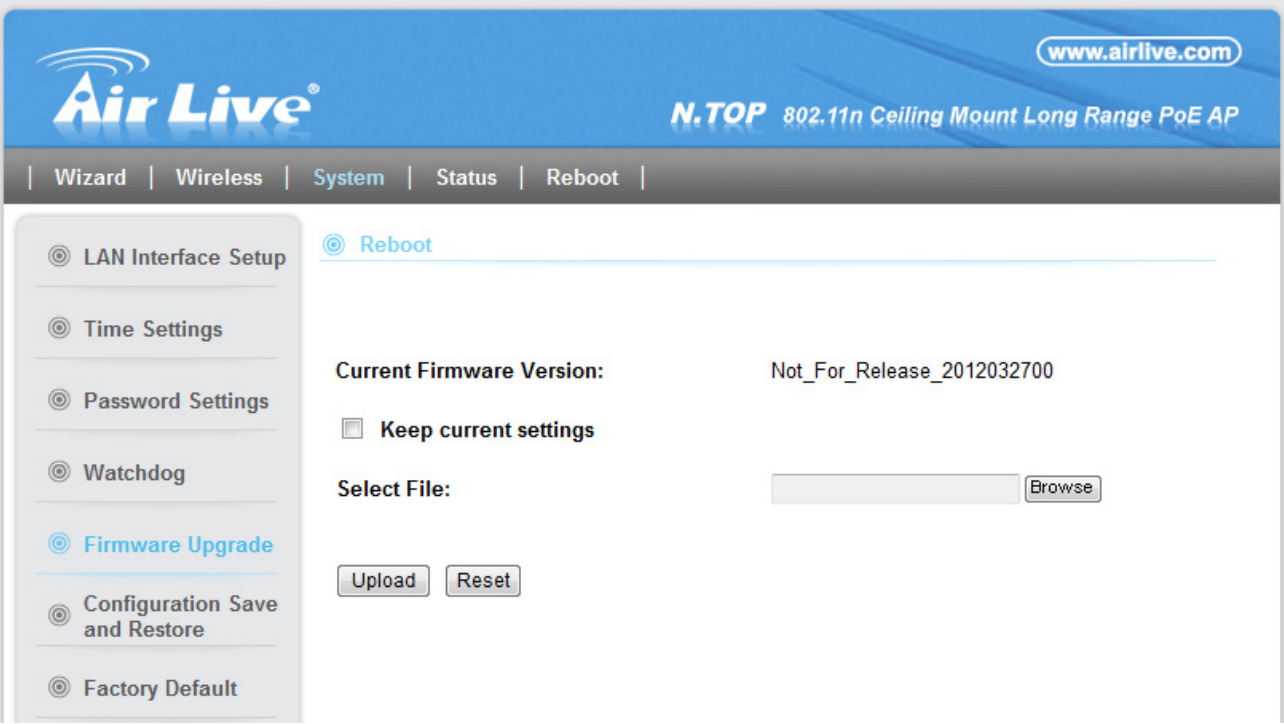


- **Watch Interval:** means: "How often the N.TOP will PING". For example, it will PING once every "1" minute.
- **Watch Host:** This is the IP address for which the Watchdog will ping.
- **Watch Actions:** Reboo,the N.TOP will do a power recycle.

5.6 Firmware Upgrade

System -> Firmware Upgrade

You can upgrade the firmware of your N.TOP (the software that controls your N.TOP's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version.



- **Upgrade Firmware:**

  To update the N.TOP firmware, first download the firmware from AirLive web site to your local disk. Then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

  Please make sure to check the "Keep Settings" box if you want the settings to be kept after firmware upgrade.

  The new firmware will be loaded to your N.TOP. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

Do not power off the device while upgrading the firmware.
It is recommended that you do not upgrade your N.TOP unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

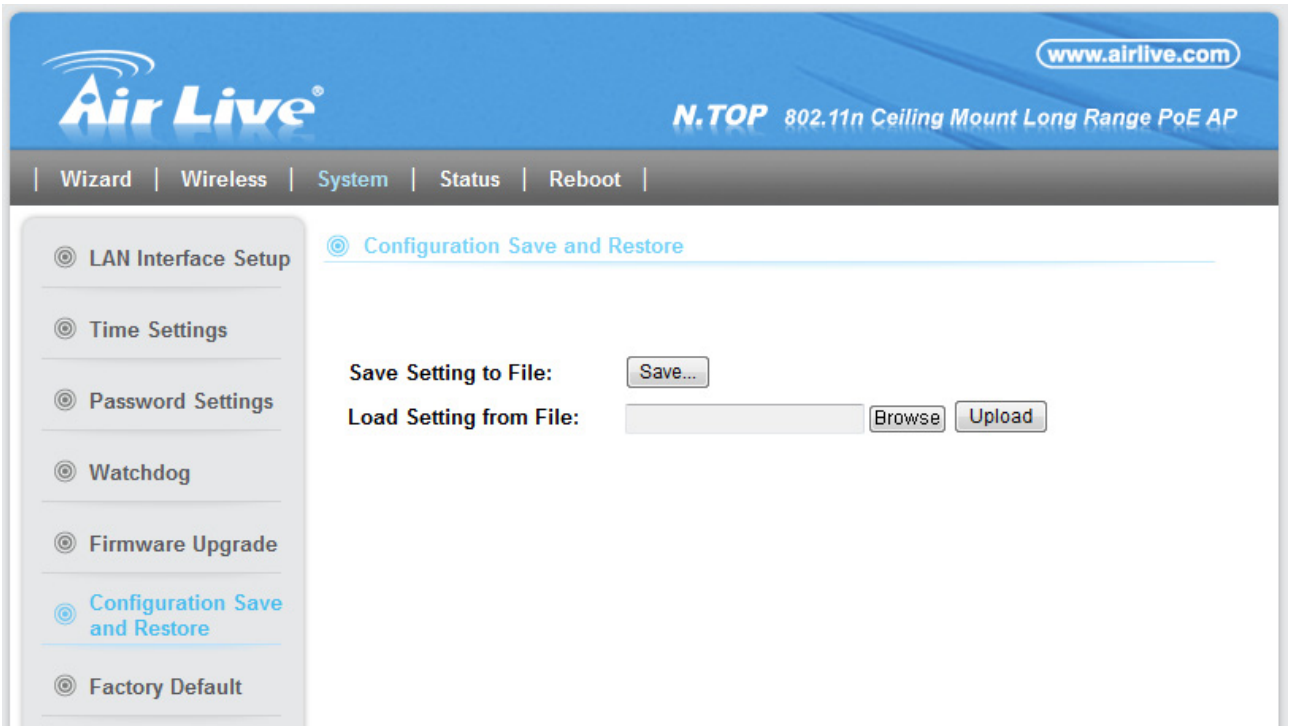
5.7 Configuration Save and Restore

System -> Configuration Save and Restore

The N.TOP can save and restore the settings to a file. In addition, it has the unique capability to restore only the network or wireless settings. This makes changes of wireless settings across the entire network of AP much easier.

You can save system configuration settings to a file, and later download it back to the N.TOP by following the steps.

Step 1 Select ***Configuration Save and Restore*** from the ***System*** menu.



Step 2 Click on "**Save Setting to File"** and enter the path of the configuration file to save-to.

Restore Setting:

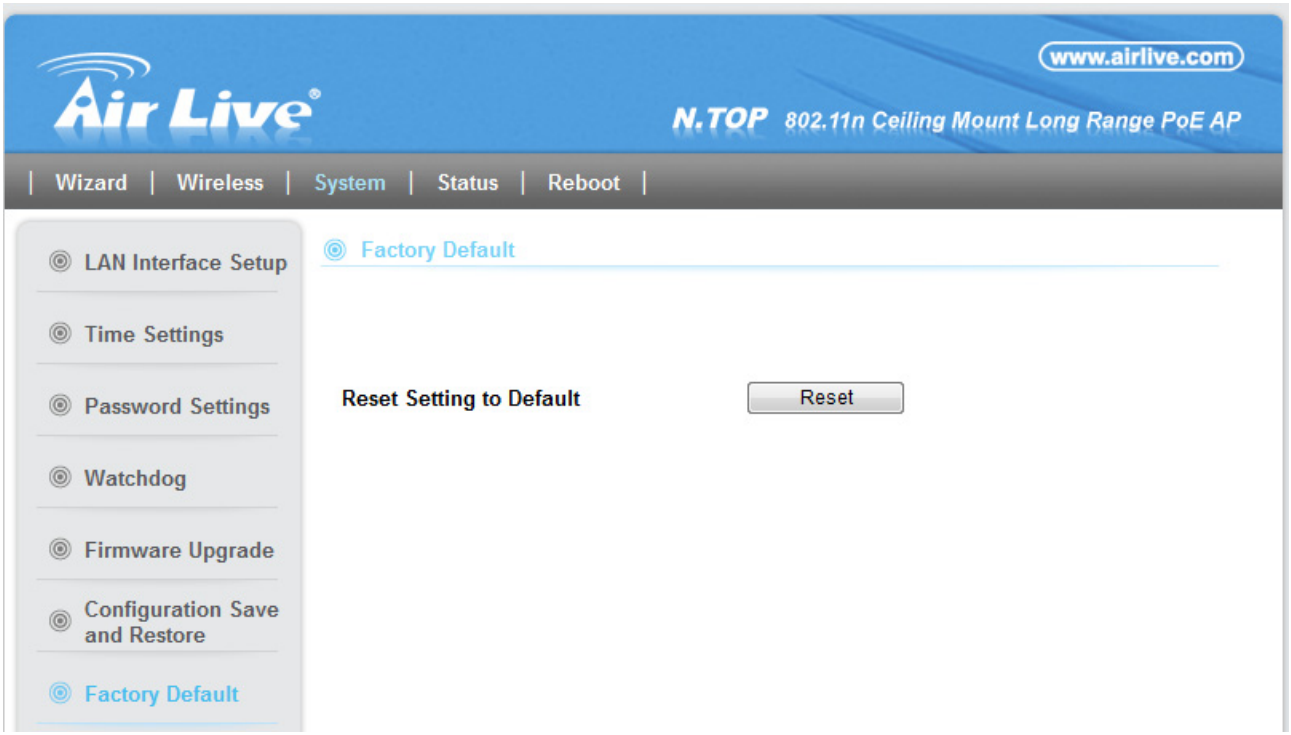
Step1: Enter the file name in the "**Load Settings from File**" field. Or click on "**Browse**" button to location the location of the file.

Step2: Click on "**Upload**" button to restore settings.

5.8 Factory Default

System Configuration -> Factory Default

You can reset the configuration of your N.TOP to the factory default settings.

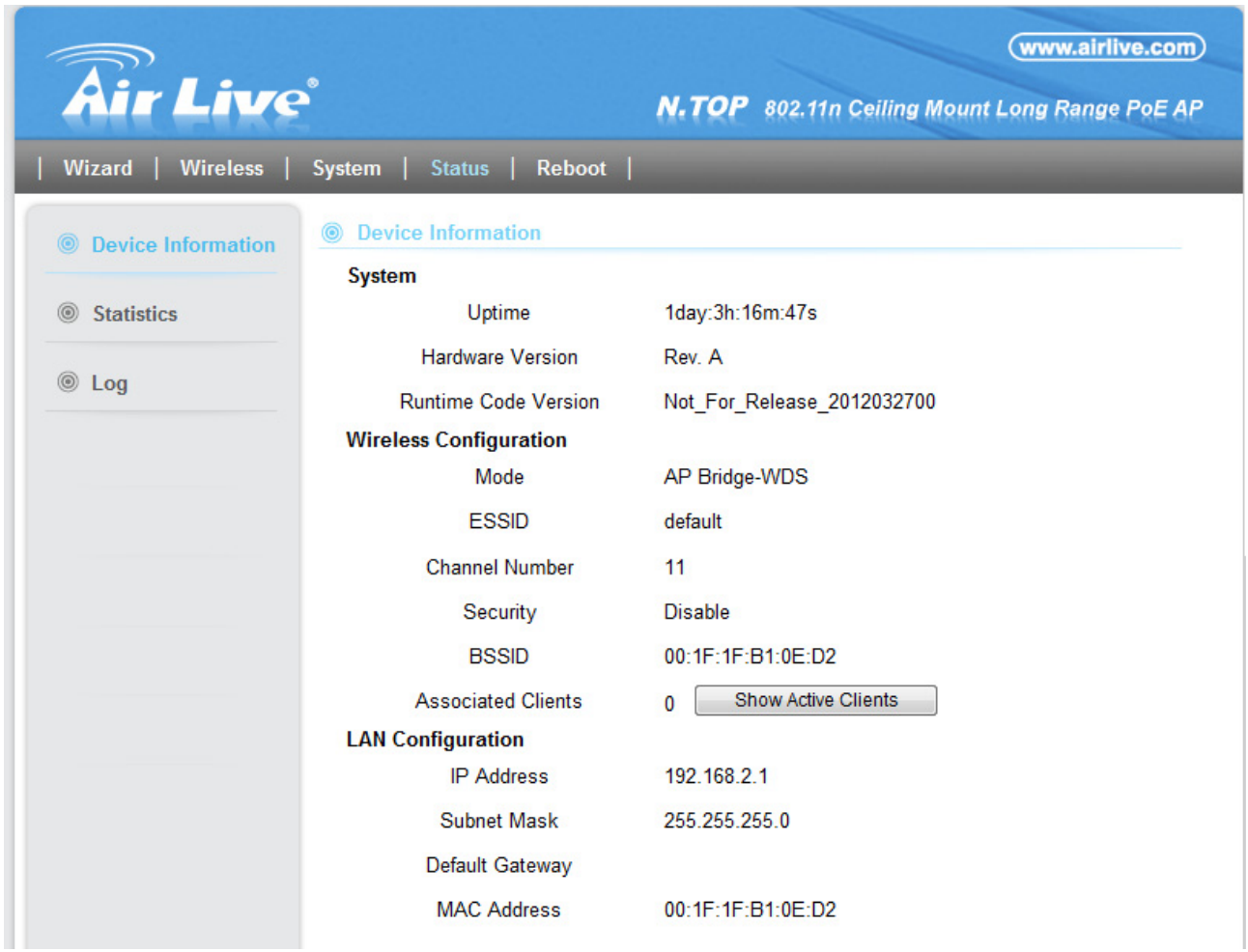


6 Status Menu

In this chapter, we will explain the "**Status**" menu in the web management interface. Before you read this chapter, please make sure to read through chapter 3 on "Introduction to Web Management Interface.

6.1 Menu Structure

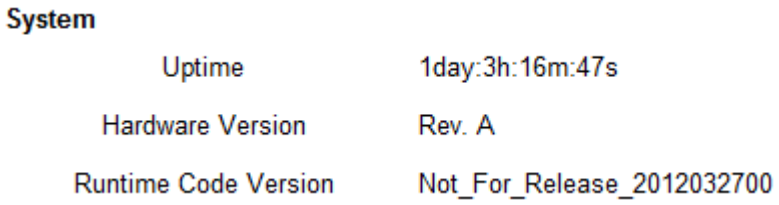
When you click on the "**Status**" on the top menu bar, the sub menu for device status will appear.



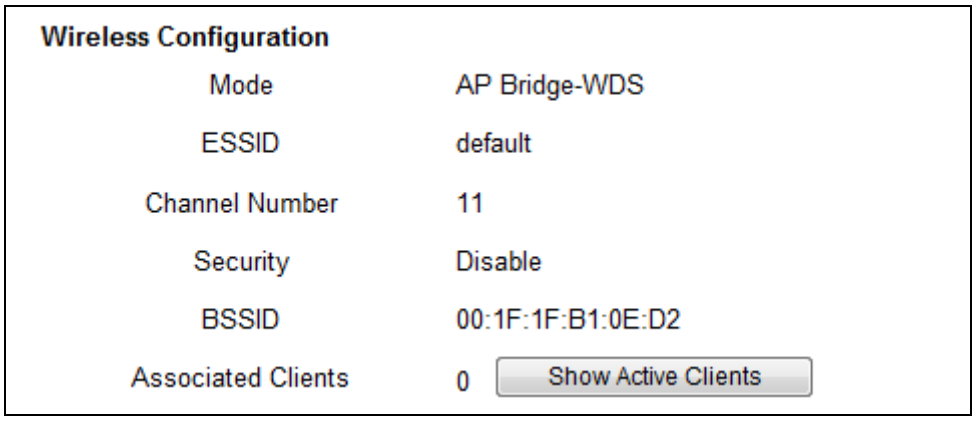
6.2 Device Information

This page shows the general information about N.TOP such as Uptime, Firmware version, Wireless Interface…etc. Below are some additional explanations on some status information of this page:

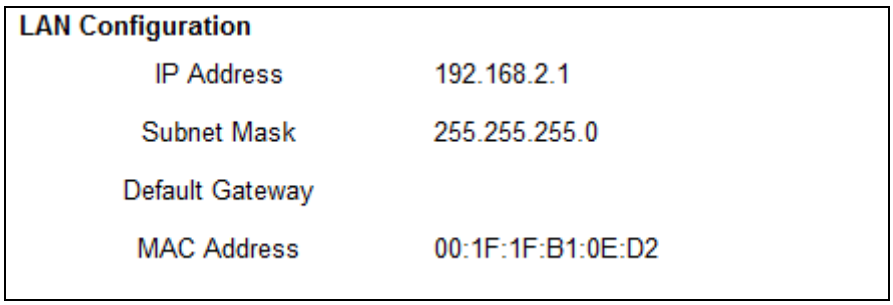
- **Uptime:** This displays the time since system last boot up. This is a good indication for how long the system has been alive.
- **Hardware Version**: It displays the hardware version.
- **Runtime Code Version**: This place will display the current firmware version.



- **Wireless:** This page displays the current settings and status of the radio. It includes the BSSID and connection status. The BSSID is also the wireless MAC address that is needed for the WDS entry.

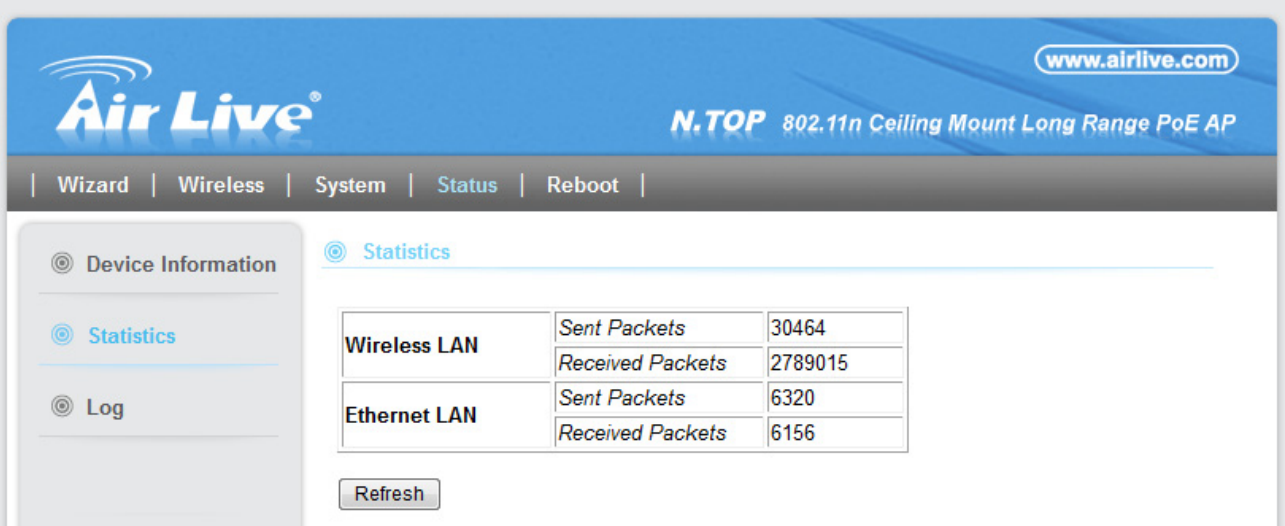


- **LAN Configuration:** This page displays the status of the LAN port such as MAC address, DHCP status.



6.3 Statistic

This page shows the sent and received packet information for Radio1, Radio2, LAN, and WAN interface.

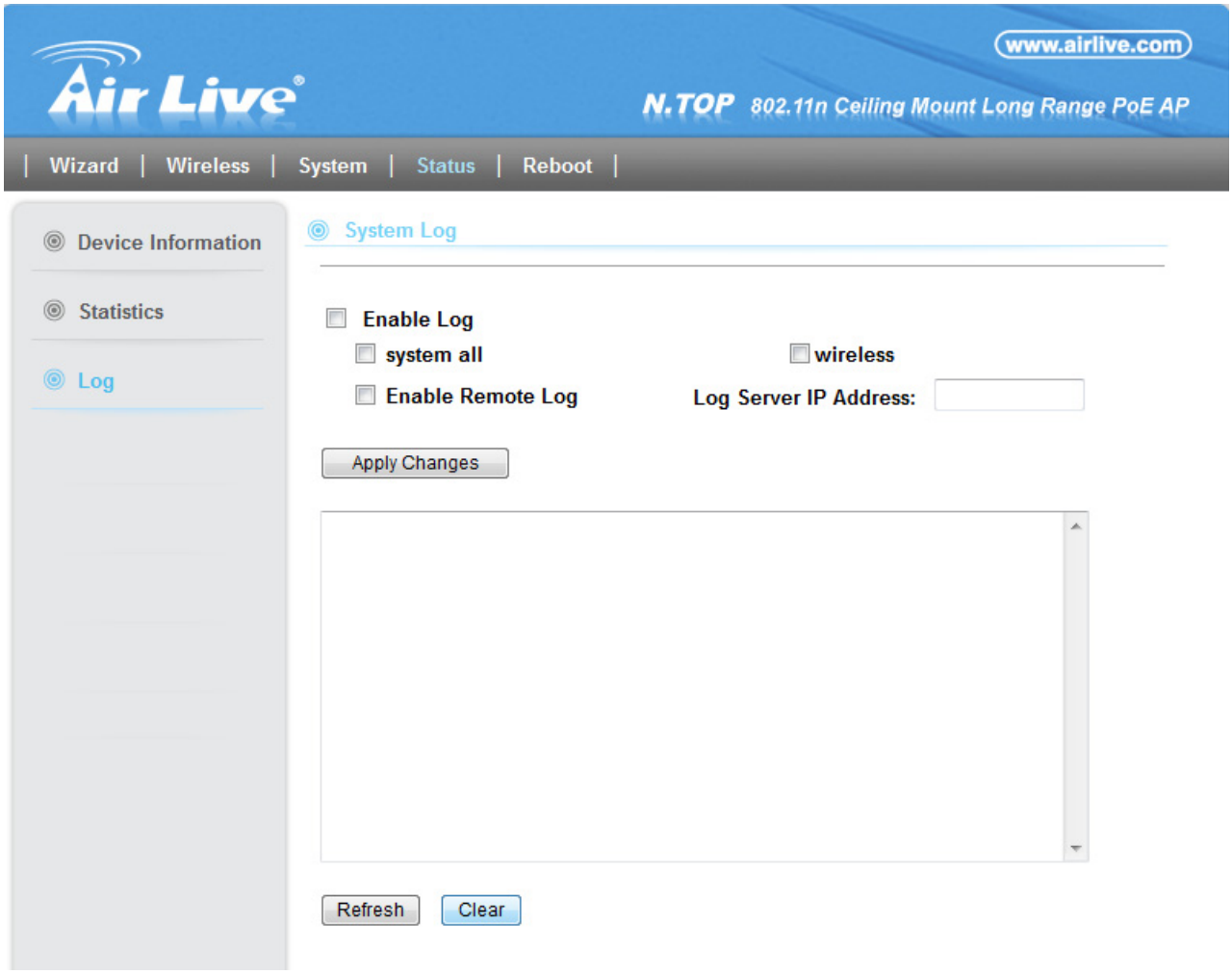


6.4 Log

The log function is where you can check for error messages for diagnostic purpose.

- **Enable Log: Check this box to enable log function.**
- **System All**: Activates all logging functions
- **Wireless**: Only logs related to the wireless LAN will be recorded
- **Enable Remote Log**: Only logs related to the Remote control will be recorded.
- **Log Server IP Address**: Only logs related to the server will be recorded.

.



7 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about N.TOP

Q: I forgot my password or the IP address of N.TOP.

A:

Please restore your settings to default by press the reset button for more than 5 seconds. You should be able to find your N.TOP at 192.168.1.254 with default username "**admin**" and password "**airlive**".

Q: N.TOP is not responding to me when I want to access it by web browser

A:

a. Please check the connection of power cord and network cable of this access point. All cords and cables should be correctly and firmly inserted to N.TOP.
b. If all LEDs on this access point are out, please check the status of A/C power adapter, and make sure it's correctly powered.
c. You must use the same IP address section which N.TOP uses.
d. Are you using MAC or IP address filter?
   Try to connect the access point by another computer and see if it works; if not, please perform a hard reset (pressing '**reset'** button).
e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.

f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help.
g. If all above solutions don't work, contact the dealer of purchase for help.

Q: Can't get connected to N.TOP.

A:

a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client.
b. Try to move closer to N.TOP.
c. Unplug the power plug of N.TOP and plug it back again after 10 seconds.
d. If all LEDs on this N.TOP are out, please check the status of A/C power adapter, and make sure it's correctly powered.

Q: I can't locate my access point by my wireless client

A:

a. '**Broadcast ESSID**' set to off?
b. Is Antenna properly installed and secured?
c. Are you too far from your N.TOP? Try to get closer.
d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.

Q: File download is very slow or breaks frequently

A:

a. Try to reset the N.TOP and see if it's better after that.
b. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow.
c. Change channel number and see if this works.

Q: I can't log onto web management interface: password is wrong

A:

a. Make sure you're connecting to the correct IP address of the N.TOP!
b. Password is case-sensitive. Make sure the '**Caps Lock**' light is not illuminated.
c. If you really forget the password, do a hard reset.

Q: N.TOP become hot

A:

a. This is not a malfunction, if you can keep your hand on the N.TOP's case.
b. If you smell something wrong or see the smoke coming out from access point or A/C power adapter, please disconnect the access point and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

8 Specifications

The specification of N.TOP is subject to change without notice. Please use the information with caution.

8.1 Hardware Features

8.1.1 General Hardware Feature

- 1 x 10/100 Mbps Ethernet Port with Auto MDI/MDI-X Support
- 802.3af PoE Port (LAN) LAN, WLAN, PWR, Reset/WPS LED Indicators
- Reversed SMA Female Antenna Port
- LAN, WLAN, PWR, Reset/WPS LED Indicators
- 300N 2T2R 11b/g/n Radio
- 2MB Flash, 16MB SDRAM
- Reset/WPS Button

8.1.2 Antenna

PiFa Antenna x 2 (2T2R MIMO Technology)

8.1.3 Power Supply

- 5VDC, 2A Switching Power Adapter

8.1.4 Dimension and Weight

- Product Weight: 143 g
- Product Size (L x W x H): 105 x 105 x 46 mm

8.1.5 EMI

- FCC, CE

8.2 Radio Specifications

8.2.1 Frequency Band

- 2.4000~2.4835GHz (Industrial Scientific Medical Band)

8.2.2 Rate and Modulation

- Data Rate:
  - 802.11n (40MHz): MCS0-7, up to 300Mbps
  - 802.11n (20MHz): MCS0-7, up to 144Mbps
  - 802.11g: 6, 9, 12, 24, 36, 48,54Mbps
  - 802.11b: 1, 2, 5.5, 11Mbps

- Modulation
  - 802.11b: DSSS (DBPSK, DQPSK, CCK)
  - 802.11g: OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
  - 802.11n: OFDM(BPSK, QPSK, 16-QAM, 64-QAM)

- Receiver Sensitivity
  - 802.11b 11Mbps ≦ -88dBm +/- 1
  - 802.11g 54Mbps ≦ -75dBm +/- 1
  - 802.11n HT20 MCS7 ≦ -72dBm +/- 1
  - 802.11n HT40 MCS7 ≦ -68dBm +/- 1

8.2.3 Supported WLAN Mode

- 2.4 GHz (B + G + N)
- 2.4 GHz (B)
- 2.4 GHz (B + G)
- 2.4 GHz (G)

8.2.4 Supported WLAN Encryption

- 64/128-bit WEP
- WPA/WPA2-PSK support
- 802.1x Radius Support

8.3 Software Feature

8.3.1 Operation Mode

- Access Point Mode (AP mode)
- Client Mode (Station-Infrastructure)
- AP Bridge-Point to Point Mode
- AP Bridge-WDS Mode
- Universal Repeater Mode

8.3.2 Management Interface

- Web HTTP

8.3.3 Advance Functions

- Setup Wizard
- Support WPS Button for Easy Setup
- Multiple SSID, Virtual AP, Watchdog, Hidden SSID
- ACK Timeout Adjustment
- WMM, MAC Access Control, Wireless Client Isolation, Channel, RTS Threshold
- Green AP Energy Saving Feature TX Output Power Adjustment
- Wireless Mode: AP, Client, WDS Bridge, WDS Repeater and Universal Repeater
- Wireless Security: WEP- 64/128bit, WPA, WPA2 and IEEE 802.1x
- Restore to Factory Default
- Configuration Backup and Restore

8.4 Environmental

8.4.6 Environmental

- Operating temperature: 0~40 Degree C
- Operating humidity (non-condensing): 10~90%
- Storage temperature: -20~60 Degree C
- Storage humidity: 95% Max

9 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.3ad
802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af
This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b
International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP
Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advice to turn on this option for multi-link bridge network.

802.11d
Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e
The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g
A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11i

The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc

A Peer-to-Peer wireless network. An Adhoc wireless network does not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The N.TOP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the N.TOP will automatically calculate the correct ACK timeout value.

Bandwidth Management (Bandwidth Control)
Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader
Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge
A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client
Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices
CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receives wireless broadband access from the WISP. The opposite of CPE is CO.

CTS
Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS
Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP
Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ
Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS
A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name
The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the domain name.

DoS Attack
Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption
Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)

The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware

The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold

Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Gateway

In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot

A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping
Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode
A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address
IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec
IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking
The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both devices must set the trunking feature to work.

MAC
Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps
Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH
Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO
Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT
Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP; the IP assigned to PC under the NAT environment is called Private IP.

Node
A network connection end point, typically a computer.

Packet
A unit of data sent over a network.

Passphrase
Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE
Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power source. A POE system typically composes of 2 main component: DC Injector (Base Unit) and Splitter (Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity
Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45
Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router
An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

SIGNAL STRENGTH
Receiver Sensitivity Index. SIGNAL STRENGTH is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher SIGNAL STRENGTH values. For SIGNAL STRENGTH value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS
Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold
RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP
Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH
Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL
Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask
An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet
Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

TCP
A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

UDP
User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade
To replace existing software or firmware with a newer version.

Upload
To send a file to the Internet or network device.

URL
Uniform Resource Locator. The address of a file located on the Internet.

VPN
Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

WAN
Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP
Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi
Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX
Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The original 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 GHz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 MHz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS
Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN

Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS

Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA

Wi-Fi Protected Access. It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2

Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.