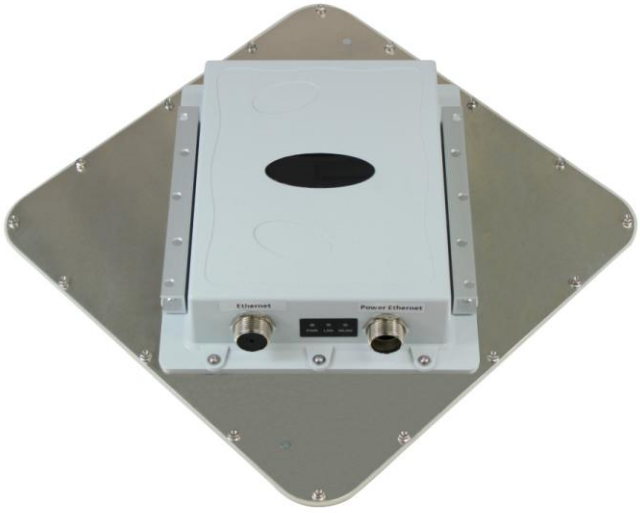
802.11a/n Wireless
High Power Outdoor
Access Point / Client / Pt(M)P



User Manual

Revision 1.0

Revision History

Version	Date	Notes
1.0	Jan. 05, 2013	Initial Version

Introduction

The 802.11a/n wireless outdoor unit (referred as **the unit** afterward) is a long range outdoor wireless Access Point / Client / Pt(M)P that operates in 5GHz frequency. The unit extends radio coverage, avoids unnecessary roaming between Access Points and ensures a stable wireless connection while reduces the number of required equipments.

The unit provides user friendly interface including user friendly distance control ranges from 1KM up to 30KM. It comes with PoE adapter for convenient outdoor installation.

The unit enforces transmission security with full support of latest encryption mechanism including 64/128/152-bit WEP, WPA and WPA2. With (5GHz) external antenna connector or integrated 23dBi flat panel antenna and superior performance, the unit makes an optimal wireless solution for both small and large scale projects.

Features & Benefits

Features	Benefits
High Speed Data Rate Up to 54Mbps HT20, HT40(+)/HT40(-)	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power up to 26 dBm and ACK timeout for Distance Control	Extended excellent Range and Coverage (fewer APs)
IEEE 802.11a Compliant	Fully Interoperable with IEEE 802.11a compliant devices
Multifunction application	Access Point/Wireless Client /Pt(M)P mode
Support Multi-SSID function (4 SSIDs) in AP mode	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID by manager
WPA2/WPA/ IEEE 802.1x support	Powerful data security
MAC address filtering in AP mode(up to 50)	Ensures secure network connection
User isolation support (AP mode)	Protect the private network between client users
Keep personal setting	Keep the latest setting when firmware upgrade
SNMP Remote Configuration Management	Help administrators to remotely configure or manage the Access Point easily.
QoS (WMM) support	Enhance user performance and density

System Requirements

The following are the minimum system requirements in order to configure the unit:

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

Applications

The wireless LAN system is easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
   There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
b) **Temporary workgroups**
   Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
c) **The ability to access real-time information**
   Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
d) **Frequently changed environments**
   Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
e) **Small Office and Home Office (SOHO) networks**
   SOHO users need a cost-effective, easy and quick installation of a small network.
f) **Wireless extensions to Ethernet networks**
   Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
g) **Wired LAN backup**
   Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
h) **Training/Educational facilities**
   Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

FCC Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/ TV technician for help.

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

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

The Wireless Technology

Standard

The Wireless Access Point utilizes the 802.11a/n standards. It increases the data rate up to 54 Mbps within the 5GHz band, utilizing OFDM technology. This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format in your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of cross talk (interference) in signal transmissions. The unit will automatically sense the best possible connection speed to ensure the greatest speed and range possible. 802.11a/n offers the most advanced network security features available today, including: WPA, WPA2, TKIP, AES and Pre-Shared Key mode.

Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network. The wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router. An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the unit will pick up the wireless PC's signal, providing that they both share the same channel and

SSID. Before enabling you consider roaming, choose a feasible radio channel and optimum position. Proper positioning combined with a clear radio signal will greatly enhance performance.

Network Layout

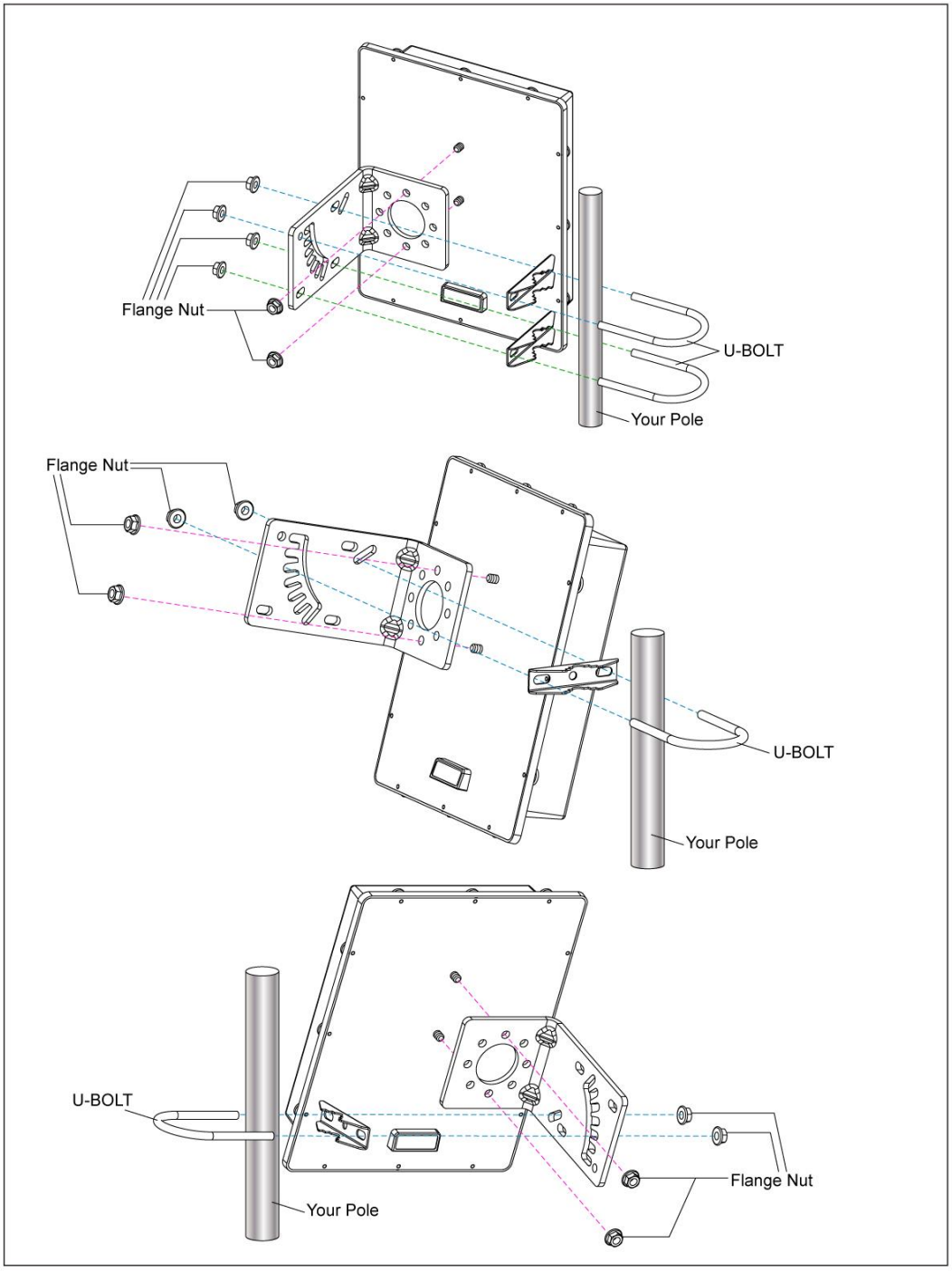
The unit has been designed for use with 802.11a products. With 802.11n products communicating with the 802.11a standard, products using these standards can communicate with each other. The unit is compatible with 802.11a adapters, such at the PC Cards for your laptop computers, PCI Card for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with an 802.11a wireless Print Server. When you wish to connect your wired network with your wireless network, the unit's network port can be used to connect to any of switches or routers.

Installation Considerations

The unit lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

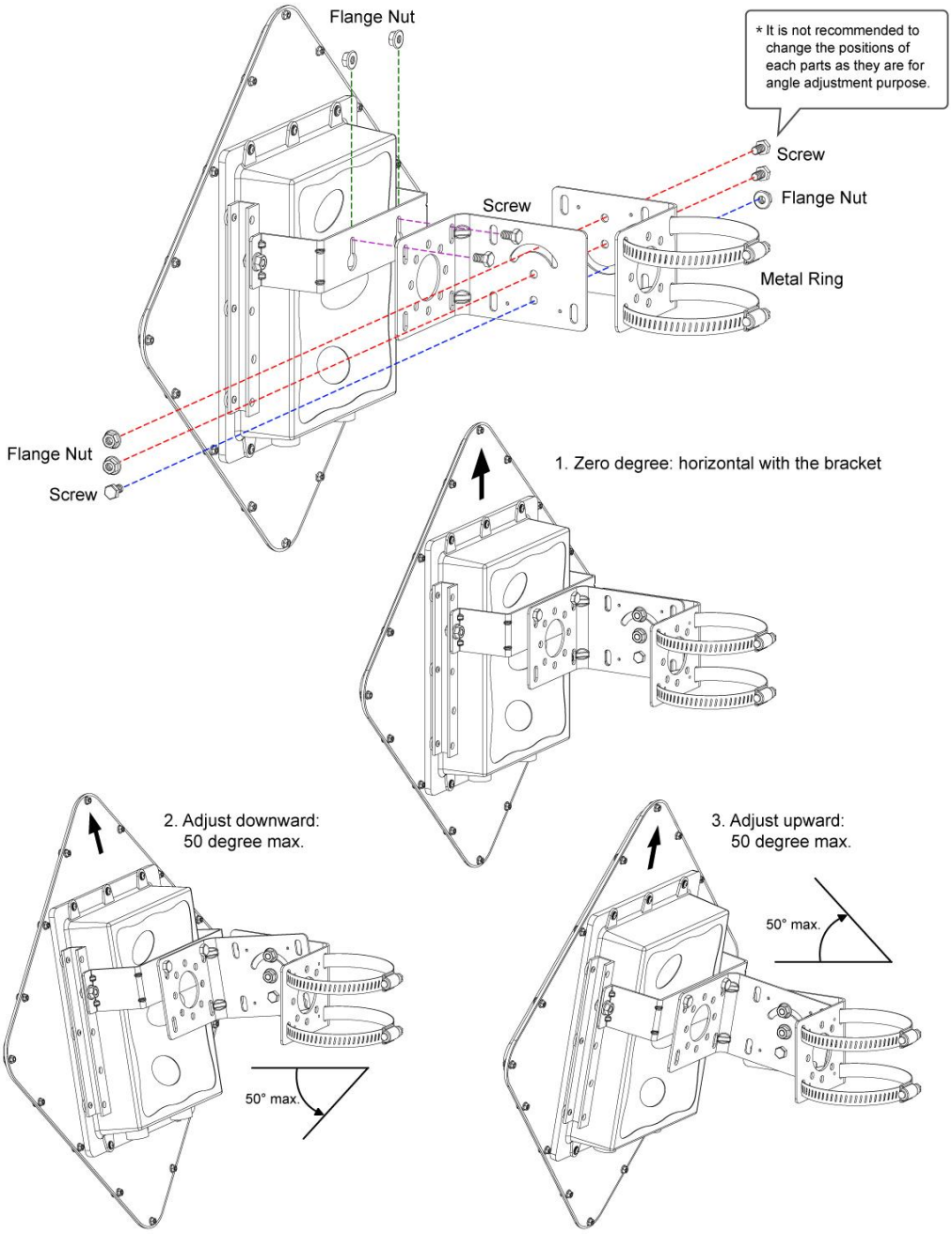
- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
- Keep the number of walls and ceilings between the unit and other network devices to a minimum - each wall or ceiling can reduce the unit's range from 3-90 feet (1-30 meters.) Position the unit so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position the unit so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position the unit and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

Installation Diagram



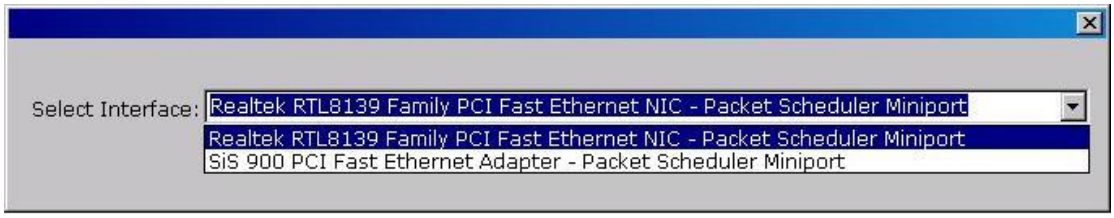
Installation Guide

5G Wireless Solution with 23dBi Flat Panel Antenna



AP Configuration Using Locator

While entering the Locator utility, the Locator will automatically search the available unit in the same network. Locator will show the Device Name, Device Type, IP Address, Ethernet MAC Address and Firmware Version in first page. Before start using Locator, make sure you disable personal firewall installed in your PC (Ex. Windows XP personal firewall).



If you have 2 Fast Ethernet Adapters or more, you can choose enable one Fast Ethernet Adapter for enter with Locator utility.

AP Configuration Using Web User Interface

Before Setup…

❖ Verify the IP address setting

You need to configure your PC's network settings to obtain an IP address. Computer use IP addresses to communicate with each other across a network, such as the Internet.

1. From the taskbar, click **Start**, select **Settings** > **Control Panel**. From there, double-click **the Network connections** icon.
2. Right click on the **Local Area Connection** icon, **Properties**; and select **TCP/IP** for the applicable Ethernet adapter. Then, click **Properties**.
3. Click the **IP Address** tab page, select **USE the following IP address**, enter **192.168.1.254** (but, **192.168.1.1** for the device use) in the **IP Address** field and **255.255.255.0** in the **Subnet Mask** field, then click **OK**.

Start Setup by Browser...

1. After getting the correct connection, start the web browser (make sure you disable the proxy) and type **192.168.1.1 (is outdoor unit IP Address)** in the **Address** field. Press **Enter**. 

2. Enter the factory default ***User name*** and ***Password*** fields:
   User Name: **Admin**

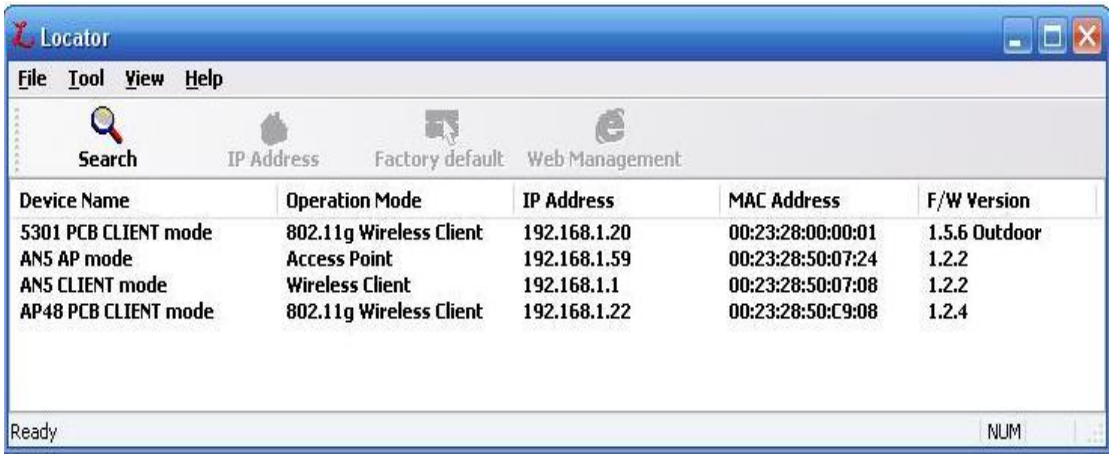
Password: **(leave blank)**

then click **OK**.

3. You will enter the Utility homepage.

Start Setup by Locator...

1. You just need to click on the **Web** icon in the Locator main page. The Locator will launch a default browser for you and lead you into web UI directly

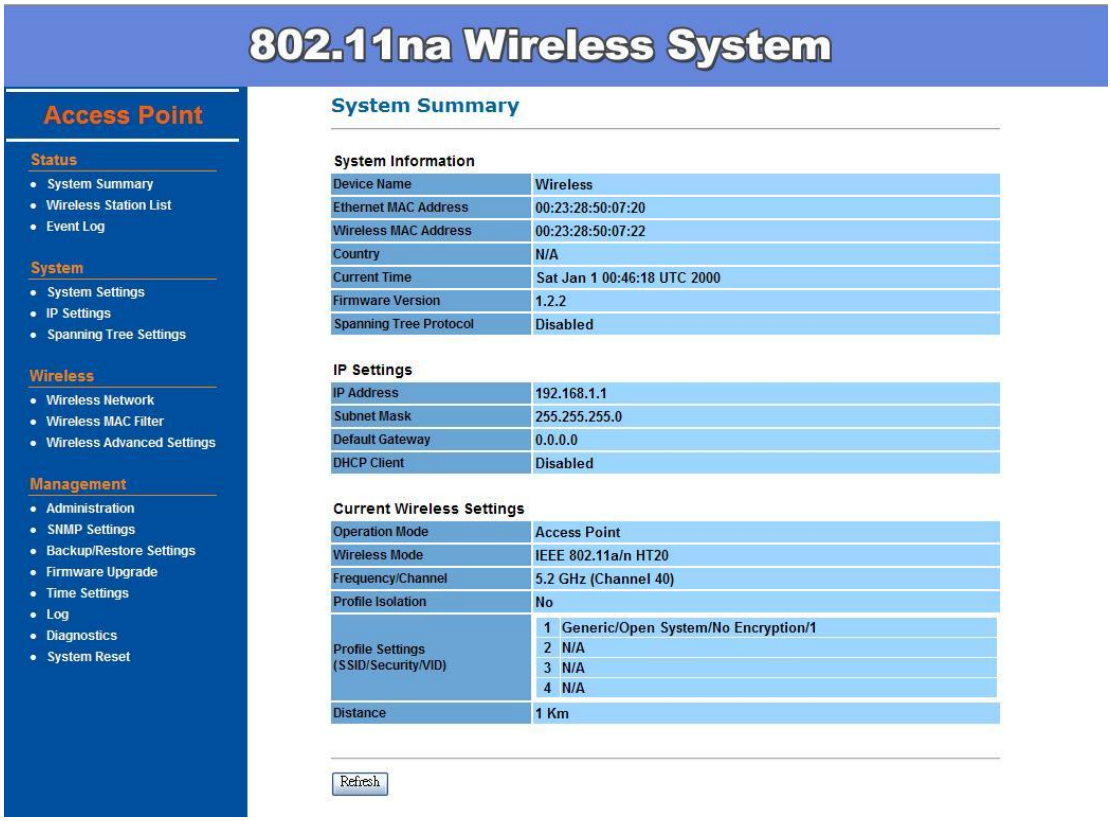


Wireless Configuration - AP Mode

System Status –

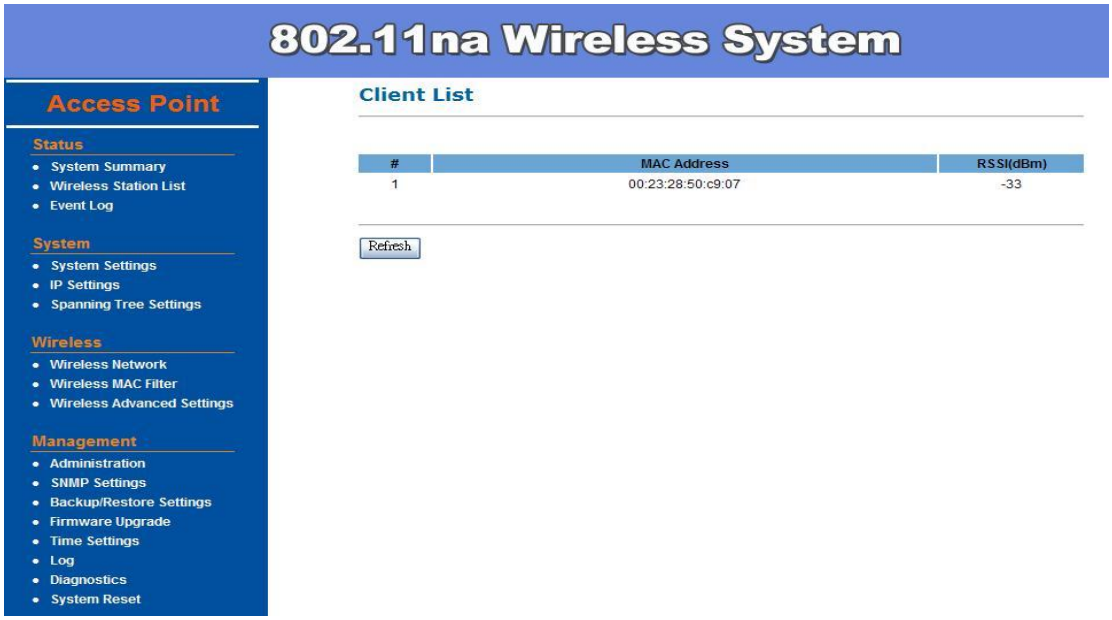
The first page appears in main page will show **System Status** -> **System Summary** automatically, you can find detail system configuration in this page including:

- **System Information –** This will display system name and both Ethernet MAC address and Wireless MAC address. Current country setting and Current time. Firmware version and Management VLAN ID.
- **Current IP Settings –** This section show current IP address setting including IP address, Subnet Mask, Default Gateway and DHCP status.
- **Current Wireless Settings** – This area shows current wireless setting including operation mode, wireless mode, Channel/Frequency, profile isolation, profile settings (SSID/Security/VID), Spanning Tree Protocol etc.



The first page appears can help user to identify current devices that already associated to the AP.

The MAC addresses and signal strength for each client are displayed. Click on **Refresh** to refresh the client list.



System Log –

Click on **System Log** under the **Status** drop-down menu. The device automatically records all events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

System Configuration –

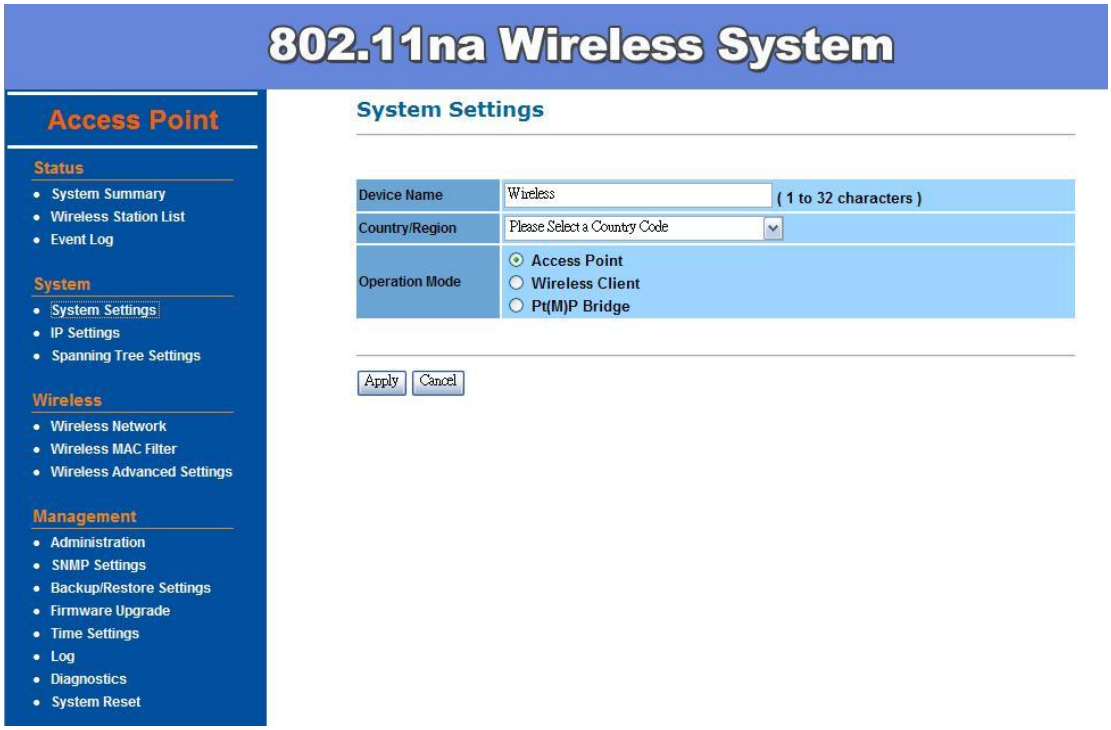
Now you can start to configure the system. In **System Properties** page, you can configure:

- **Device Name –** You may assign any name to the unit. Memorable, Unique names are helpful especially if you are deploying multiple access points on the same network. The device name needs to be less than 32 characters. After verify the name you input and click **Apply** to save the settings.
- **Country/Region** – Here you can set the unit to follow different country and region regulation.
- **Operation Mode** - The default operation mode is Wireless Client.

  In most cases, no change is necessary. Pt(M)P Bridge (WDS) allows Bridge point to point or point to multi-point network architecture. In order to establish the wireless link between bridge radios, the MAC address of remotes bridge(s) need to be registered in the address table. Enter the MAC address with format xx:xx:xx:xx:xx:xx (x is the hexadecimal digit) and use **Add** and **Delete** button to edit the address table. A Master Bridge Radio may accommodate up to **8** remote MAC addresses.

  Make sure you click **Apply** to save the changes before move to next page.

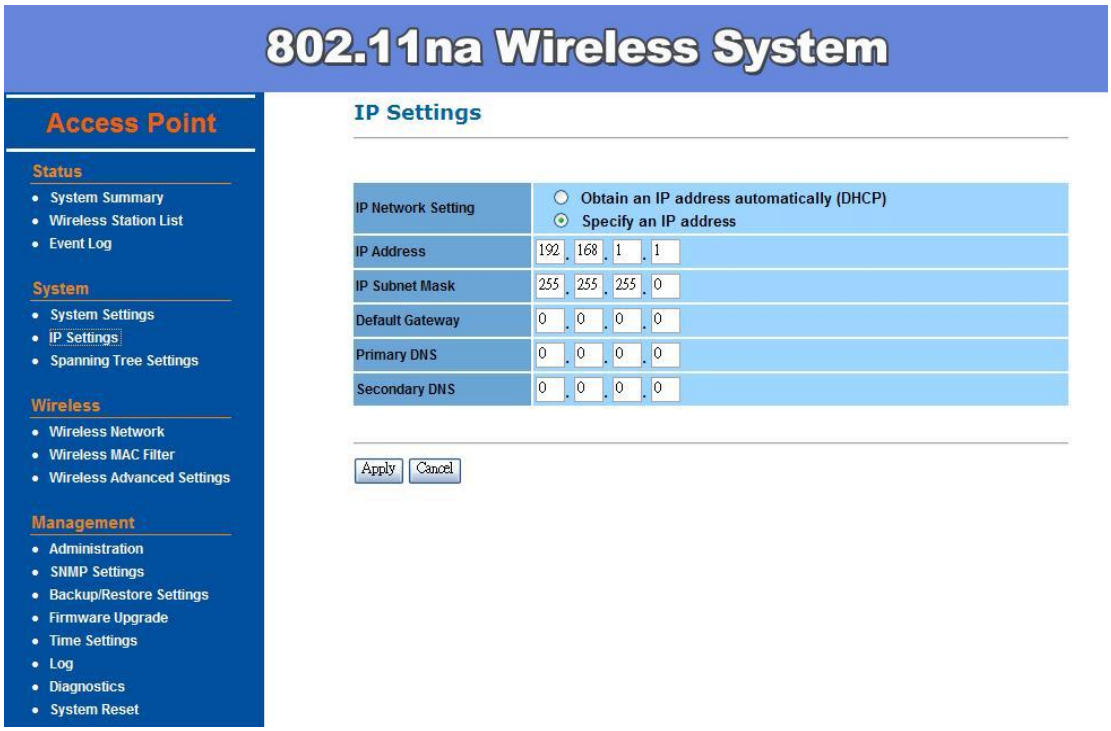
Note: There's another firmware which supports all channels between 5.0GHz to 6.0GHz. However, it does NOT have country/Region selections.



IP Settings –

IP Setting page can configure system IP address. Default IP address is **192.168.1.1** and Subnet Mask is **255.255.255.0**. You can manually enter the IP address or get an IP from a DHCP server.

- **IP Network Setting –** Here you can choose to get IP from a DHCP server or specify IP address manually. Choose to obtain an IP address from DHCP server if your environment or ISP provides DHCP server. Otherwise, you can manually setup IP address.
- **IP Address –** The IP address needs to be unique to your network. We would like to recommend you stay with default IP address 192.168.x.x. This is private address and should work well with your original environment.
- **IP Subnet Mask –** The Subnet Mask must be the same as that set on your Ethernet network.
- **Default Gateway –** If you have assigned a static IP address to the unit, then enter the IP address of your network's Gateway, such as a router, in the Gateway field. If your network does not have a Gateway, then leave this field blank.
- **Primary DNS –**
- **Secondary DNS –**



Spanning Tree Settings –

Click **Spanning Tree** under the **System Configuration** drop-down menu. Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

- **Spanning Tree Status**: Choose to enable (**On**) or disable (**Off**) the spanning tree function.
- **Bridge Hello Time**: Specify the number of seconds for the hello time.
- **Bridge Max Age**: Specify the number of seconds for the max age.
- **Bridge Forward Delay**: Specify the number of seconds for the bridge forward delay.
- **Priority**: Specify the number of seconds for the priority.

  Click **Apply** to save the changes.

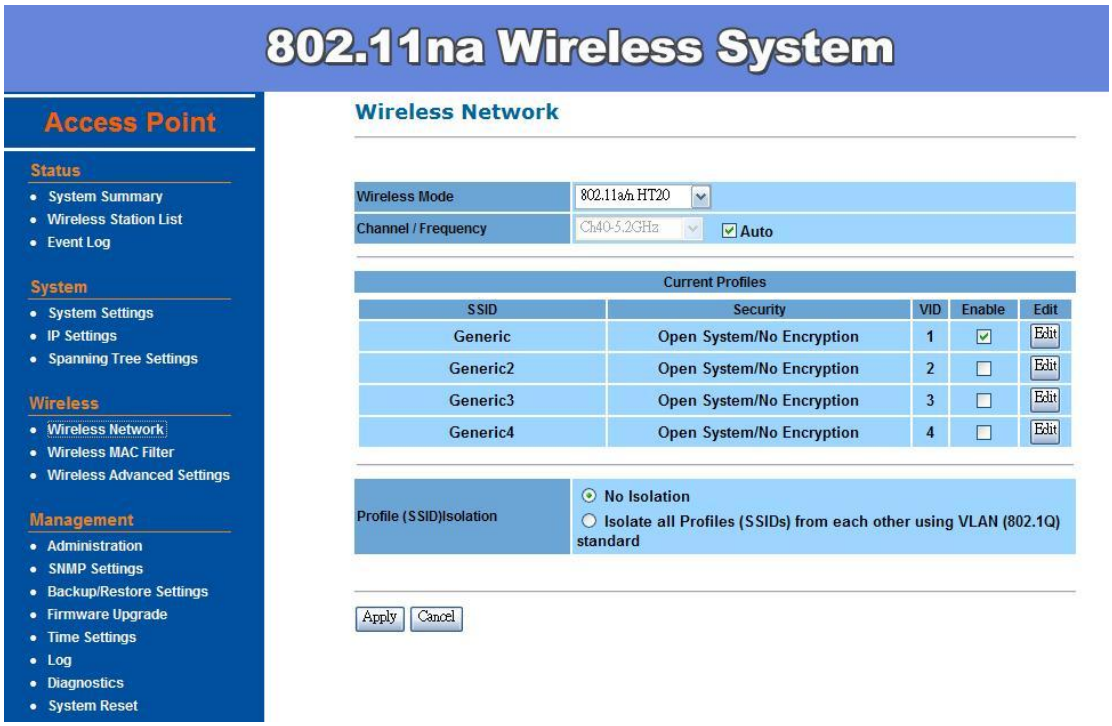
Wireless Network -

At Wireless Network page, it allows you to configure the **Wireless Mode**, **Channel/Frequency**, **SSID** and **Security**.

- **Wireless Mode –** Default setting is **802.11a/n HT20**.
  HT40(+) is using upper extension channel as its secondary channel.
  HT40(-) is using lower extension channel as its secondary channel.
- **Channel / Frequency –**The channels available are based on the country's regulation and select the appropriate channel from the list provided to correspond with your network settings.

  Note: There's another firmware which supports all channels between 5.0GHz to 6.0GHz. However, it does NOT have country/Region selections.

- **Current Profiles –** You may configure up to four different wireless profiles. Click **Edit** to modify the profile and place a check in the **Enable** box to activate the profile.
- **Profile (SSID) Isolation –** Stations connected to different profiles cannot access each other. Choose **No Isolation** (Full access), or **Isolate all profiles (SSIDs) from each other using VLAN (802.1Q) standard**.
- **SSID –** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. For added security, you should change the SSID from the default name **Generic1**, to a unique name.
- **VLAN ID –** If you have enabled VLAN tagging on your network, specify the VLAN tag ID 1 to 4095. You can assign an SSID to a VLAN. Client devices using the SSID are grouped in that VLAN.
- **Suppressed SSID –** This option can hide the SSID not available from site survey tool. Enable this function only if you do not want the unit to be found by others.
- **Stations Separation –** Default setting is **Disable**. This option disallows the client devices connected to this unit could not access each other.
- **Security Mode**: By default, the security is disabled. Refer to the next section to configure the security features such as **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK Mixed**, **WPA**, **WPA2** and **WPA-Mixed**.
  Click **Apply** to save the changes.



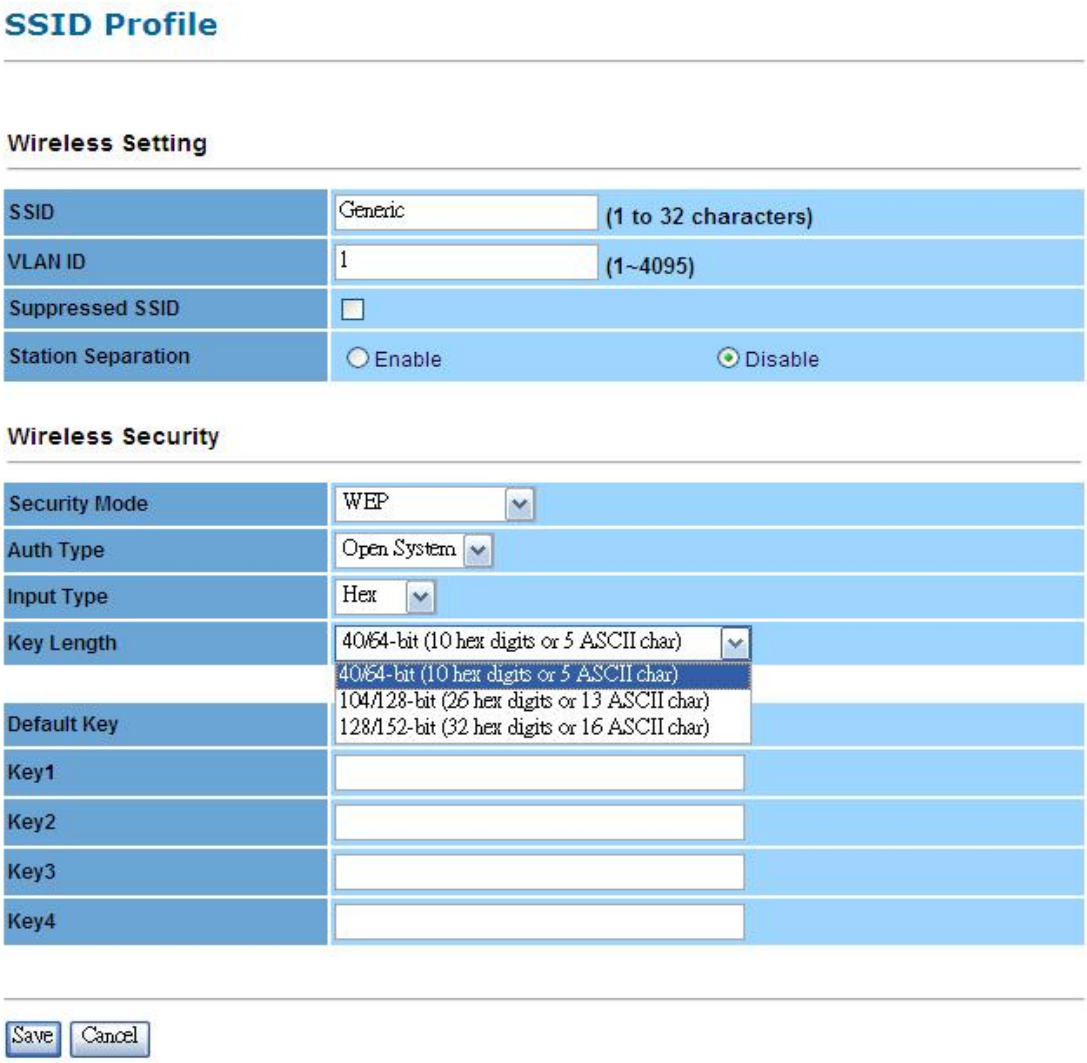
Wireless Security -

The wireless security settings configure the security of your wireless network. There are three major wireless security mode options (WEP, WPA & WPA2) which supported by the unit: **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK Mixed**, **WPA**, **WPA2** and **WPA-Mixed** (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy. WPA-PSK/WPA2-PSK stands for Wi-Fi Protected Access – Pre-Shared Key. WPA-PSK/WPA2-PSK is design for home users who do not have RADIUS server in their network environment. WPA/WPA2 can provide better security level than WEP without difficult setting procedure.

In Wireless Security page, you can configure the unit to work with **Disabled** (no Security), **WEP**, **WPA-PSK, WPA2-PSK, WPA-PSK Mixed**, **WPA, WPA2** and **WPA-Mixed** security mode. Once you setup the unit to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is **Disabled**.

WEP is a basic encryption method, which is not as secure as WPA. To use WEP, you will need to select a default transmit key and a level of WEP encryption:

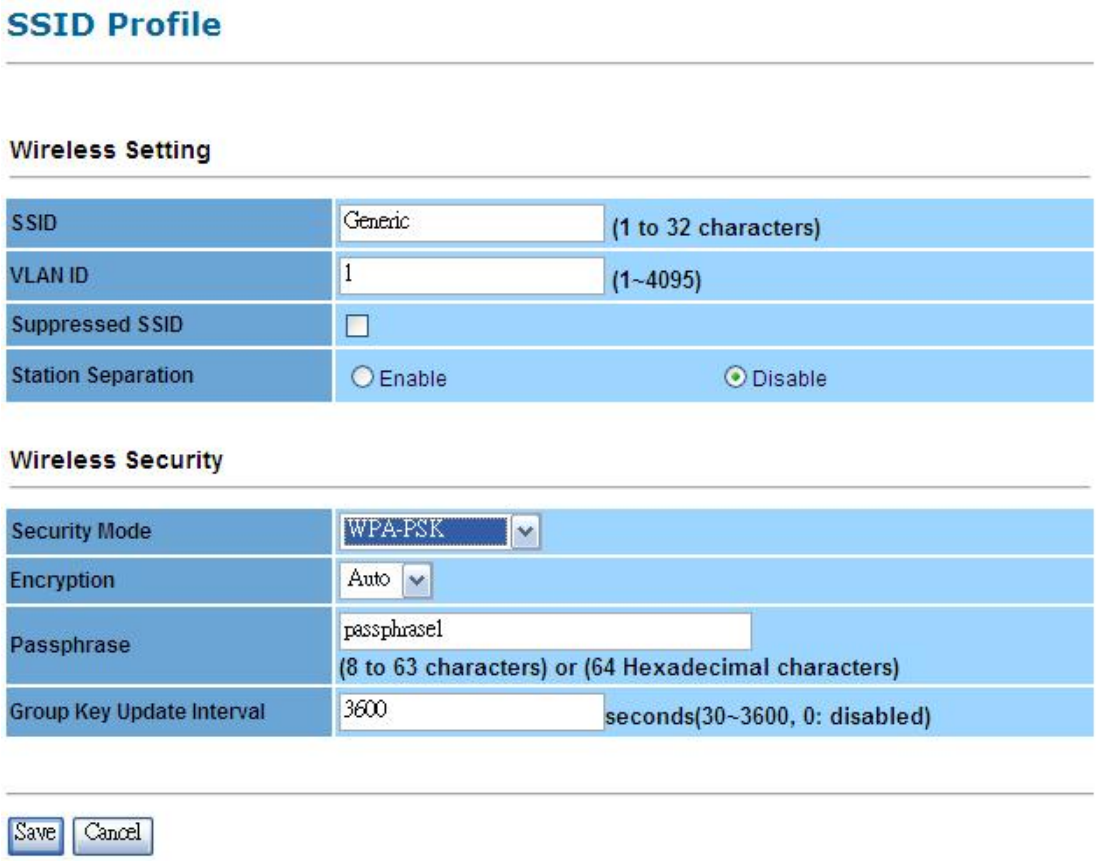
- **Authentication Type:** Select an authentication method. Available options are: **Open System**, **Shared Key** or **Auto**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the unit. The device requesting authentication encrypts the challenge text and sends it back to the unit. If the challenge text is encrypted correctly, the unit allows the requesting device to authenticate. It is recommended to select **Auto** if you are not sure which authentication type is used.
- **Input Type**: Select **Hex** or **ASCII** from the drop-down list.
- **Key Length**: Select a key format from the drop-down list. 40/64bit-hex keys require 10 characters or ASCII keys require 5 characters, where as 104/128-bit-hex keys require 26 characters or ASCII keys require 13 characters, as 128/152-bit-hex keys require 32 characters or ASCII keys require 16 characters. A hex key is defined as a number between 0 through 9 and letter between A through F.
- **Default Key**: You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key table –** You can input 4 different WEP encryption keys into the table and by choosing the radio button to decide which one is valid now. The unit supports 64, 128 and 152bit key length. The longer key we choose usually means the encryption is stronger.



After all changes are made, click **Save** to make sure all changes are saved into system.

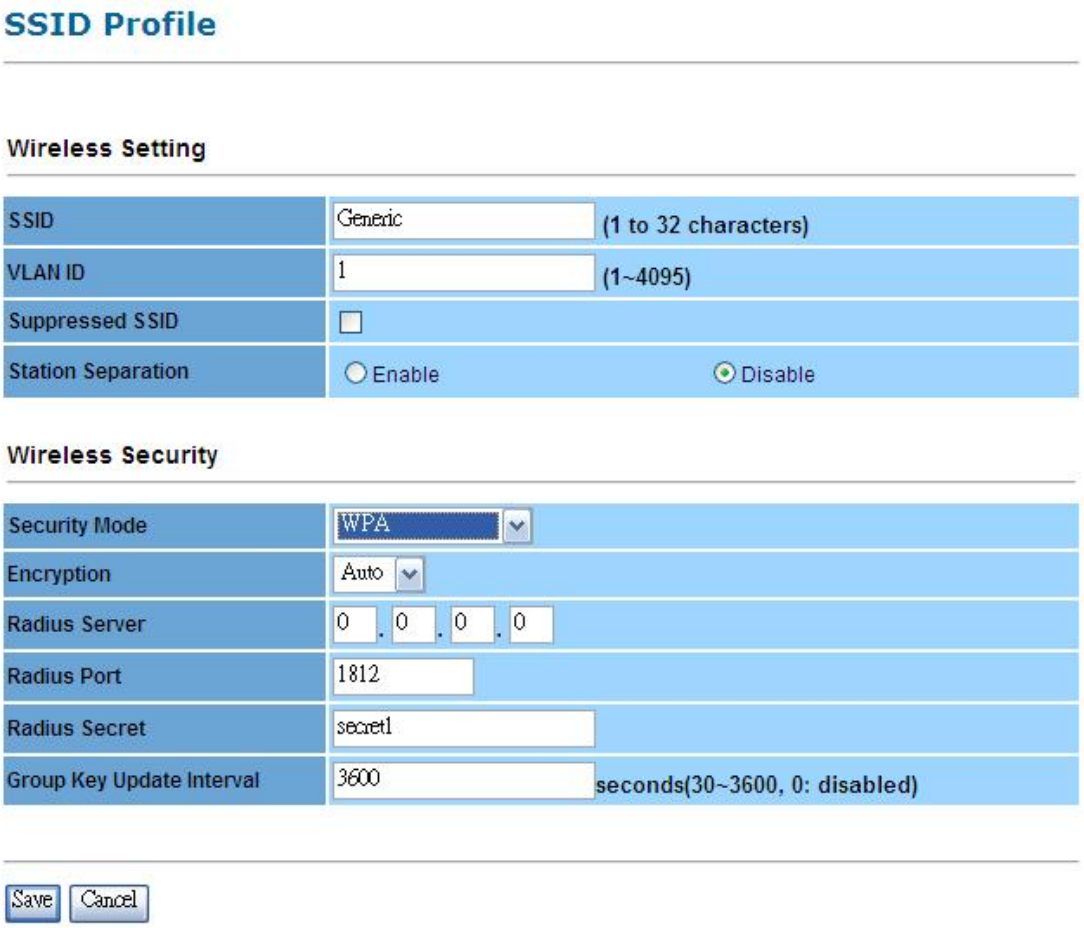
- **PassPhrase -** Enter a WPA Shared Key of 8-63 characters. The Shared Key should be also applying the clients work in the same wireless network.
- **Encryption -** WPA gives you two encryption methods: **TKIP** and **AES** with dynamic encryption keys. Select the type of algorithm **TKIP** or **AES**.
- **Group Key Update Interval -** Enter a number of seconds which instructs the unit how often it should change the encryption keys. Usually the security level will be higher if you set the period shorter to change encryption keys more often. Default value is **3600** seconds, set 0 in Group Key Update Interval to disable key renewal.

Click **Save** to make sure all changes are made before leaving this page.



WPA/WPA2 option features WPA/WPA2 used in coordination with a RADIUS server (This should only be used when a RADIUS server is connected to the unit).

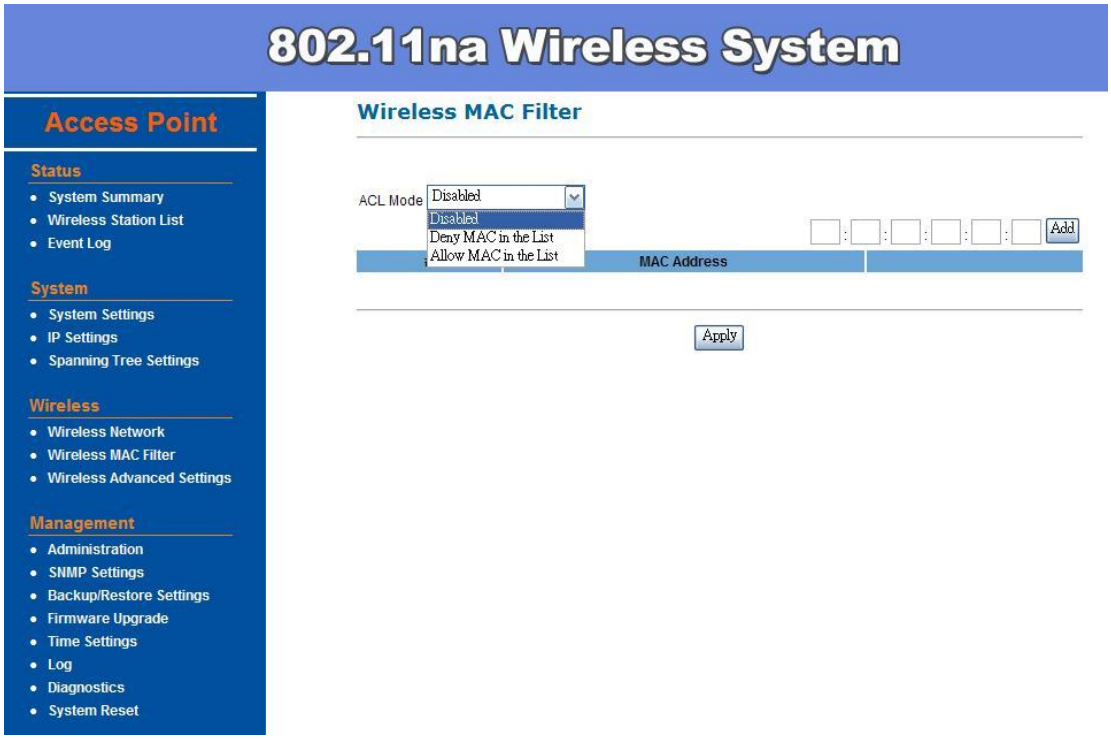
- **RADIUS Server –** Here enter the IP address of your RADIUS server.
- **RADIUS Port –** Port number for RADIUS service, default value is **1812**.
- **RADIUS Secret –** RADIUS secret is the key shared between the unit and RADIUS server.
- **Encryption –** WPA/WPA2 gives you two encryption methods: **TKIP** and **AES** with dynamic encryption keys. Select **Auto** if you are not sure which encryption is used.
- **Group Key Update Interval –** This column indicate how often should the Access Point change the encryption key. Default value is **3600** seconds, set 0 in Group Key Update Interval to disable key renewal.



Wireless MAC Filter –

On this page you can filter the MAC address by allowing or blocking access the network:

- **ACL (Access Control) Mode:** You may choose to **Disabled**, **Deny MAC in the List,** or **Allow MAC in the List**. By selecting **Allow MAC in the List**, only the address listed in the table will have access to the network; all other clients will be blocked. On the other hand, selected **Deny MAC in the List**, only the listed MAC addresses will be blocked from accessing the network; all other clients will have access to the network.
- **MAC Address:** Enter the MAC address.
- This table lists the blocked or allowed MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking **Delete**.
  Click **Apply** to save the changes.



Wireless Advance Settings -

The page below can help users to configure advanced wireless setting. Before making any changes at this page, please check your wireless settings on other system as well, as these changes will alter the effectiveness of the unit. In most cases, these settings do not need to be changed:

- **Data Rate –**This defines the data rate (in Mbps) which the unit should transmit wireless packets. Higher data rates will get higher throughput but with a shorter distances. You can fix a specific data rate (MCS0 to MCS6.5) or select **Auto** to get the best data rate dynamically according to link quality condition. It is recommended to use **Auto**, especially if you are having trouble getting connected or losing data at higher data rate.
- **Transmit Power –** You can reduce the RF output power by selecting adjustable transmit power by 1dBm step from 26 to 10dBm. To change transmit power may decrease your wireless signal coverage. This feature can be helpful in restricting the coverage area of the wireless network.

- **Aggregation-**A part of 802.11n standard. It creates the larger frame by combing smaller frames with same physical source and destination and QoS into one large frame with a common MAC header.

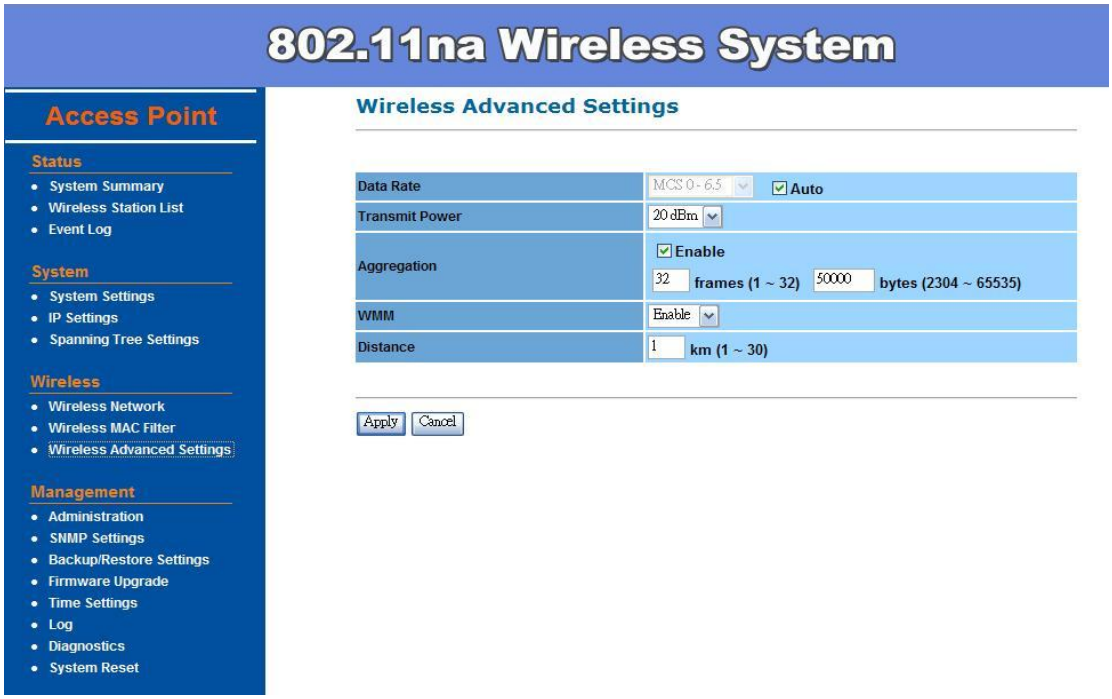
  frames: the number of frames combined on the new large frame.

  bytes: the size of the large frame.

- **WMM –**Part of the 802.11e QoS enhancement to the Wi-Fi standard. It is recommended to enable this setting for 802.11n wireless mode to enhance traffic throughput.

- **Distance (1-30km) –** Enter a number which is according to the longest link distance between the point to point or point to multi-point in the network. The number needs to be greater than or equal to the real distance. The range can be from **1km** to **30km**.

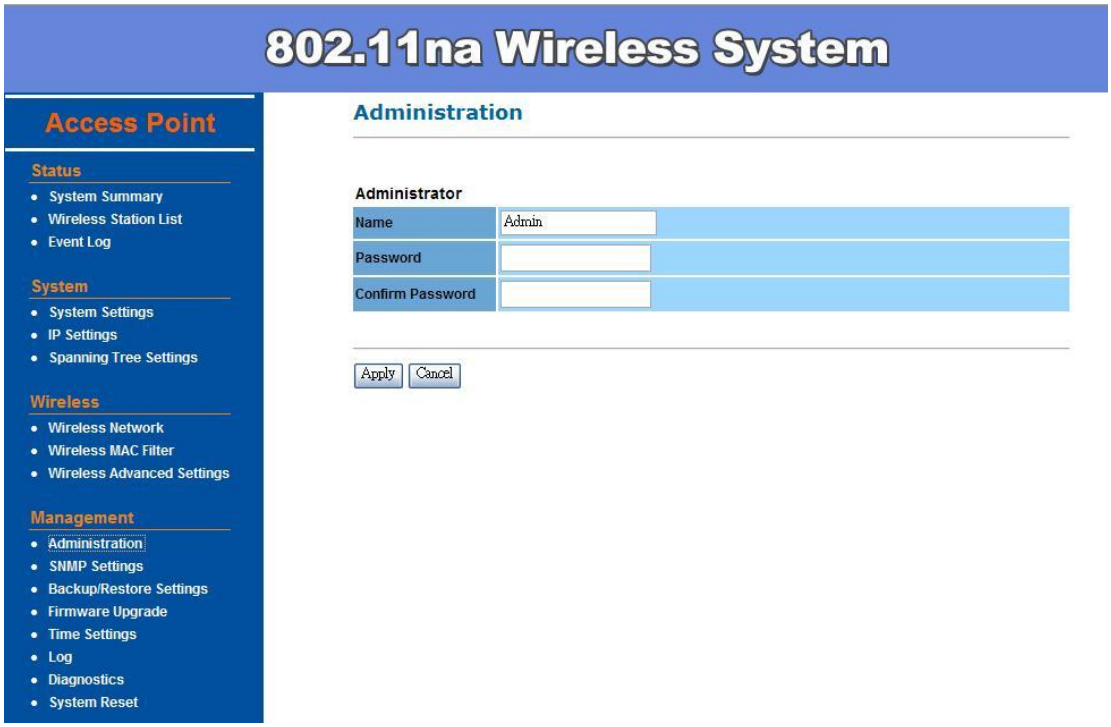
Click **Apply** to make sure all changes are made before leaving this page.



Management

Administration –

In the administration page, you can modify **Name** and **Password**. Changing the user name and password are as easy as just entering the string you wish in the column. Then, enter the password again into the second column to confirm. This option allows you to create a user name and password for the unit. By default, this unit is configured with a user name **Admin** and password (**leave blank**). For security reasons, it is highly recommended that you create a new user name and password. Click **Apply** to finish the procedure. Be sure you noted the modification before apply all changes.

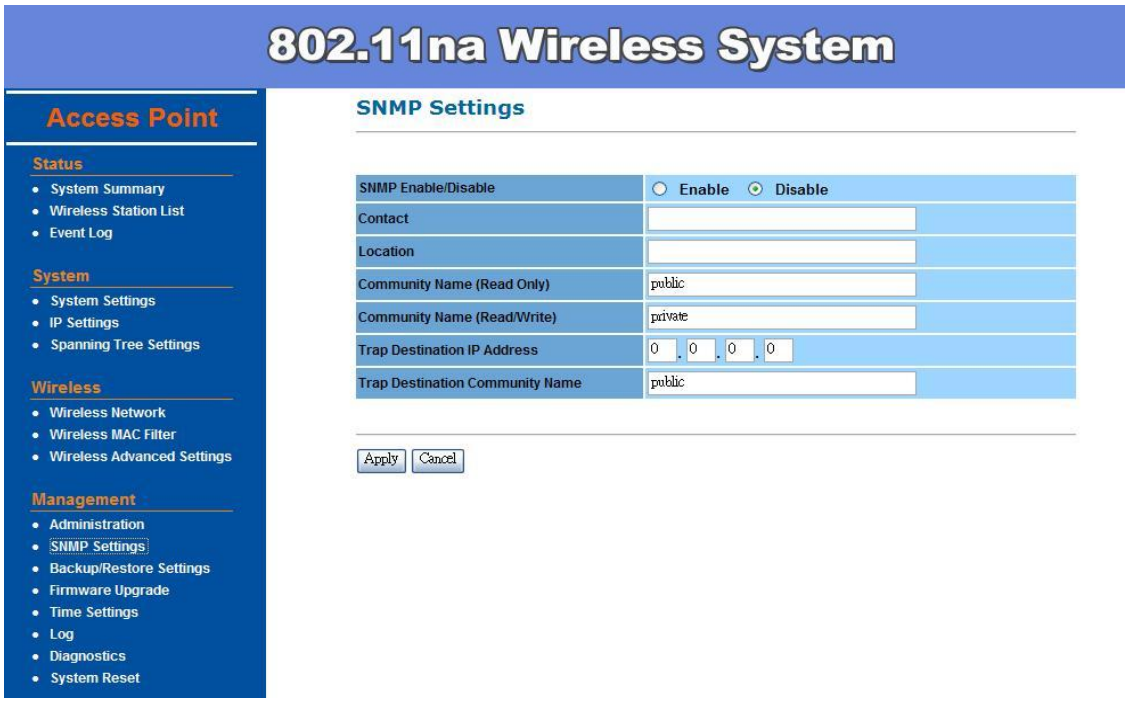


SNMP Settings–

Under System Configuration, click **SNMP** to display and change settings for the Simple Network Management Protocol.

To communicate with the unit, the **SNMP** agent must first be enabled and the Network Management Station must submit a valid community string for authentication. Select **SNMP** Enable and enter data into the fields as described below. Click **Apply** when finished.

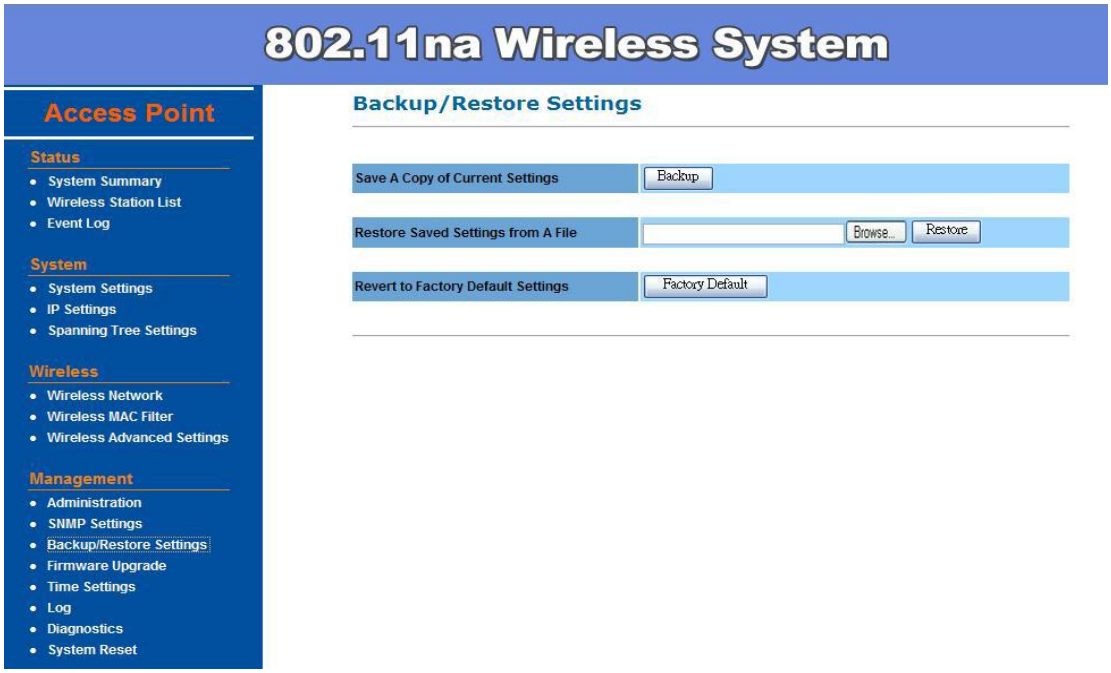
Setting	Description
SNMP	Enables or disables SNMP.
Contact Location	Sets the location string that describes the system location. Maximum length is 255 characters.
Community Name (Read Only)	Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. Maximum length is 32 characters. Default is **public**.
Community Name (Read/Write)	Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Maximum length is 32 characters. Default is **private**.
Trap Destination IP Address	Enter the IP address of the trap manager that will receive these messages.
Trap Destination Community Name	Enter the community name of the trap manager that will receive these messages. Default is **public**.



Backup/Restore and Reset to factory default Settings–

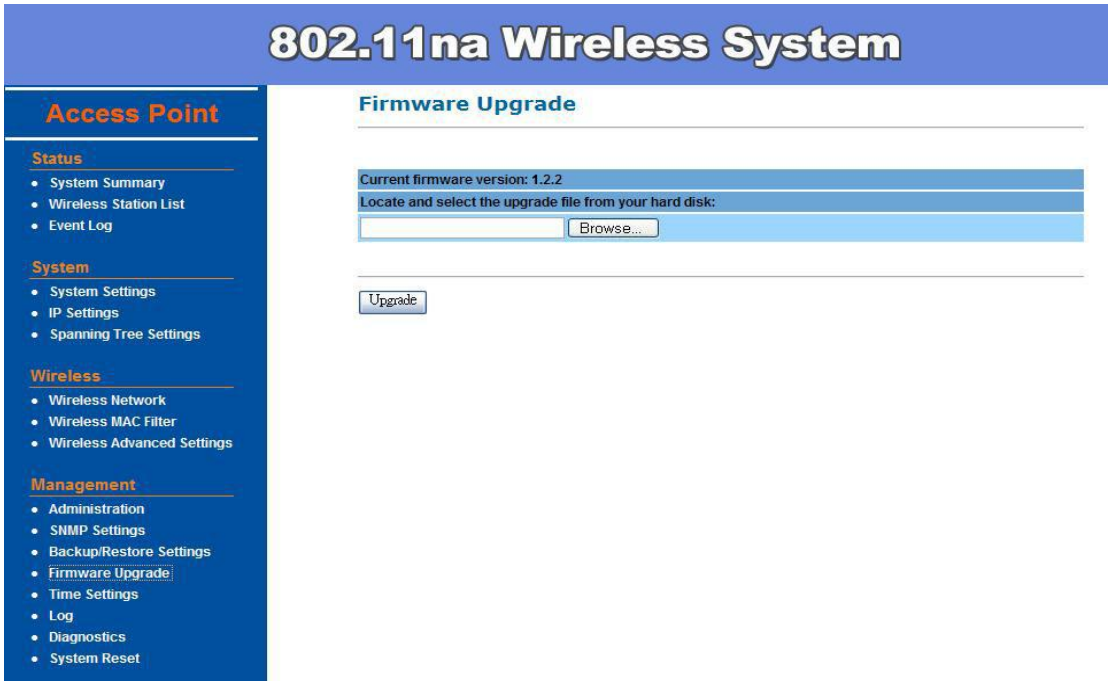
In Management section, you can **Backup/Restore Setting** and **Revert to Factory Default Settings** in following pages:

- **Backup the current settings to a file –** Click **Backup** and the system will prompt you where to save the backup file. You can choose the directory to save your configuration file.
- **Restore settings from a backup file –** Here you can restore the configuration file from where you previous saved.
- **Revert to factory default settings –** Be very carefully before restore system back to default since you will lose all current settings immediately.
  The IP address will restore to default values as:
  192.168.1.1 in the **IP Address** field and **255.255.255.0** in the **Subnet Mask** field



Firmware Upgrade –

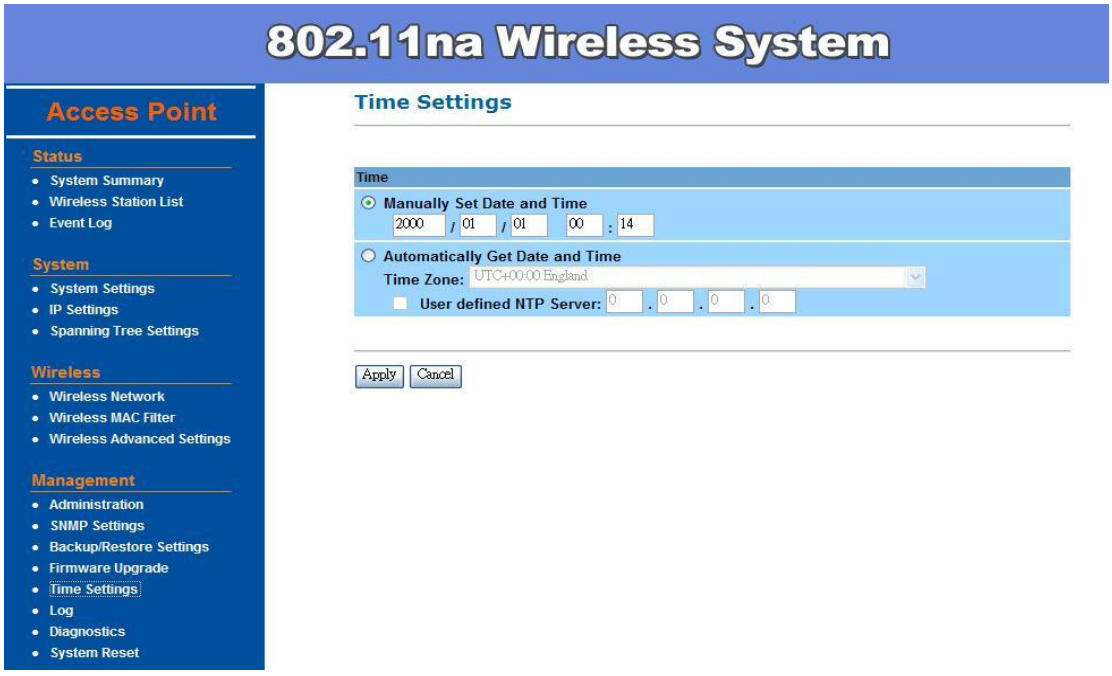
Enter the location of the firmware upgrade file in the file path field, or click **Browse** to find the firmware upgrade file. Then click **Upgrade** and follow the instructions. The whole firmware upgrade process will take around 90 seconds. Before upgrade, make sure you are using correct version. Please check with your technical support service if new firmware available.



Time Settings –

This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server:

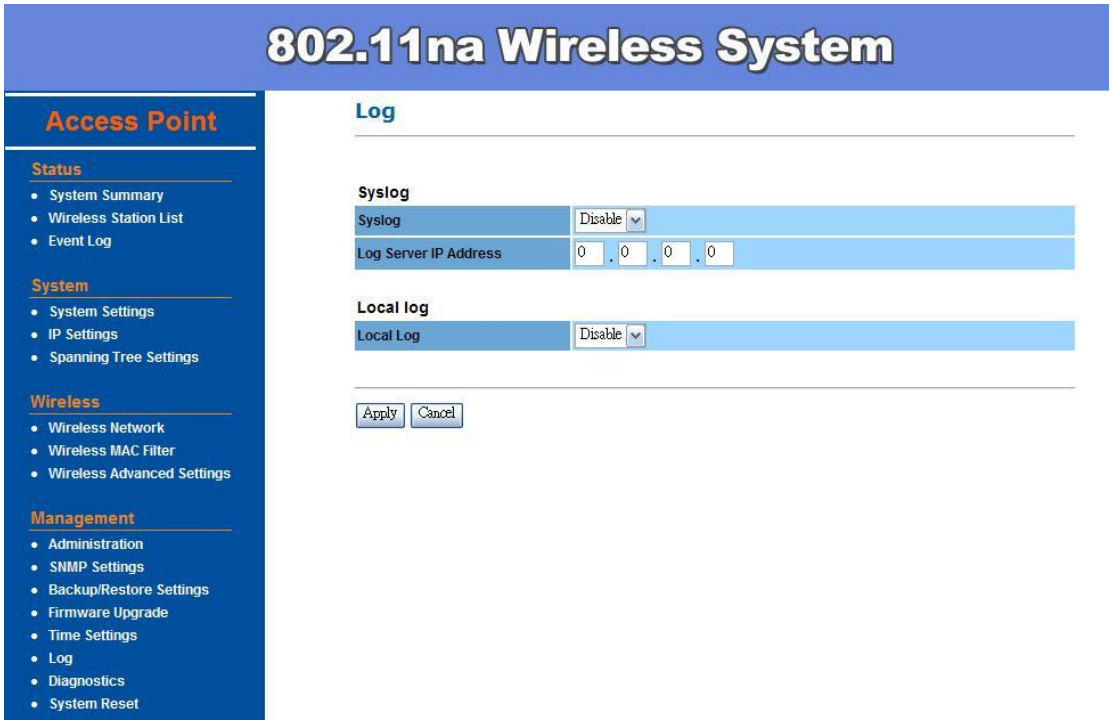
- **Manually Set Date and Time**: Specify the date and time
- **Automatically Get Date and Time**: Select the time zone from the drop-down list and then specify the IP address of the NTP server.
  Click **Apply** to save the changes.



Log –

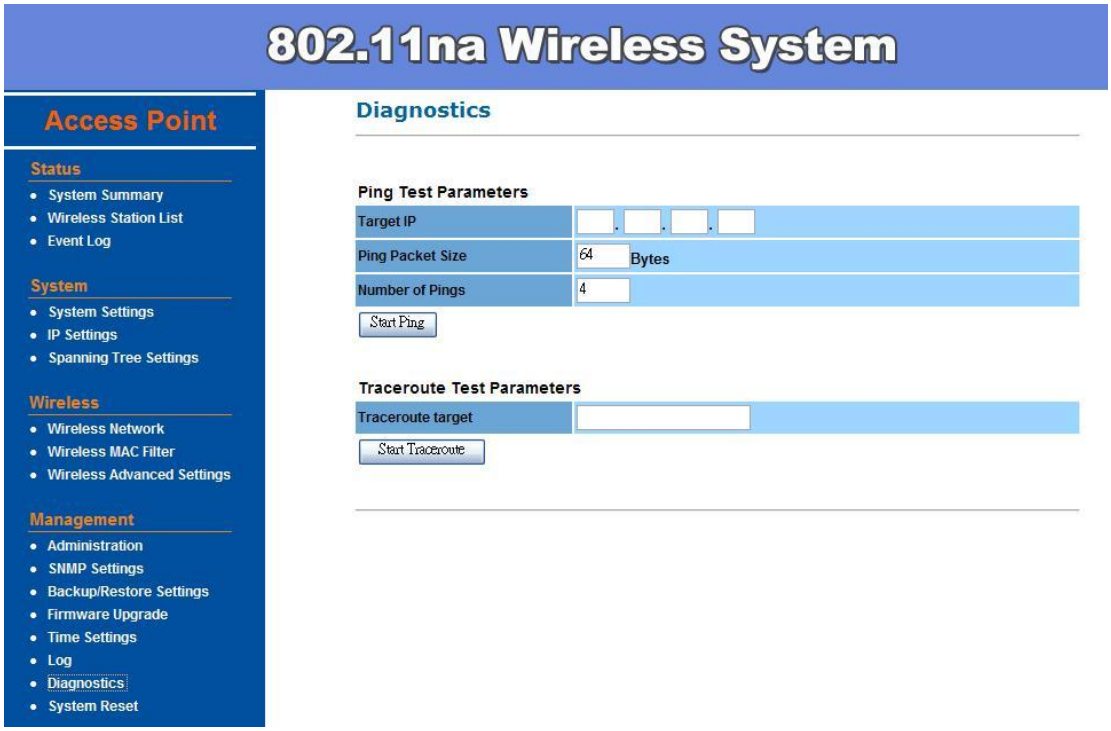
This page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes:

- **Syslog**: Choose to enable or disable the system log.
- **Log Server IP Address**: Specify the IP address of the server that will receive the system log.
- **Local Log**: Choose to enable or disable the local log.
  Click **Apply** to save the changes.



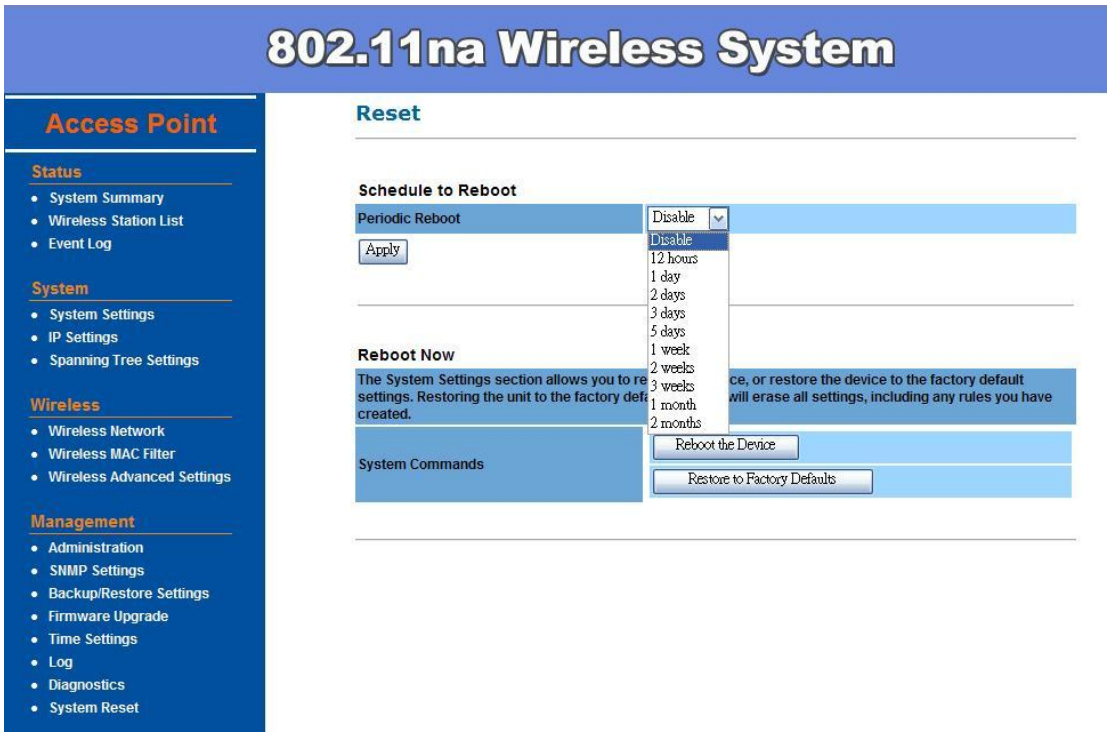
Diagnostics –

The Diagnostics is to provide tools to understand the network connecting status. The Ping utility is used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets. The Traceroute utility is used for tracing the hops route from the device across the network to a selected outgoing IP address.

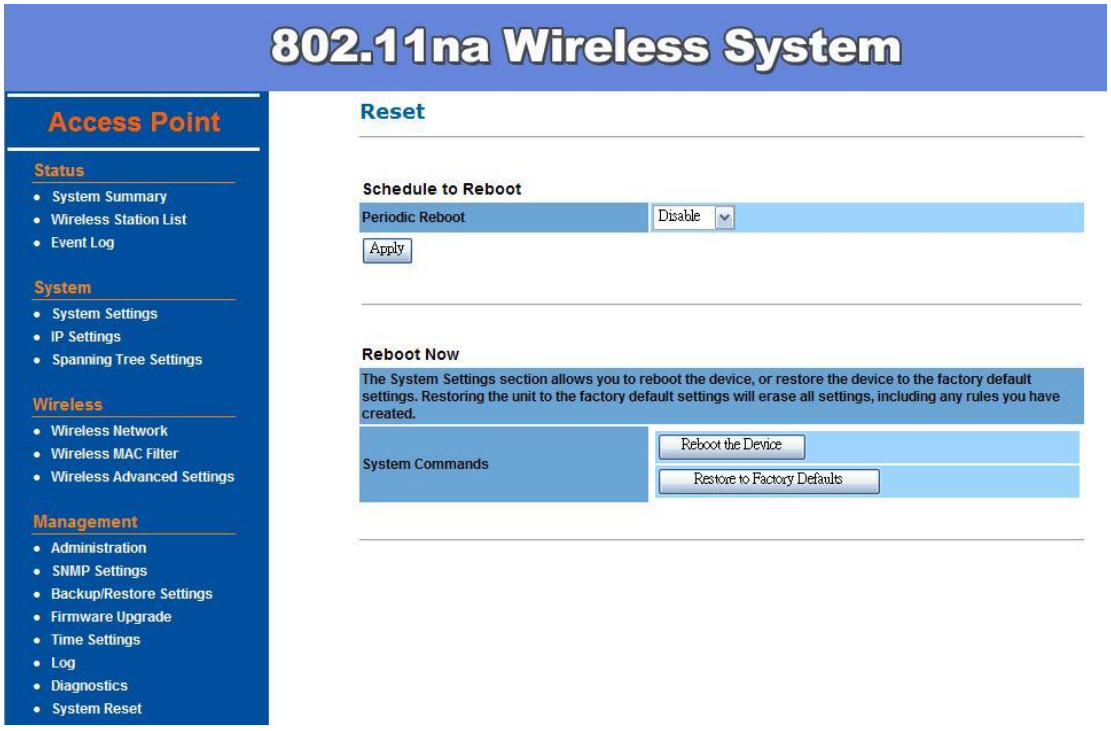


System Reset –

- **Periodic Reboot**: This function allows user to set up a time to reboot the unit without changing any current settings. This function is designed for solving the problem of flash memory running out by large or long period data transmitting. By doing this, the unit will automatically reboot as scheduled and release the flash memory.

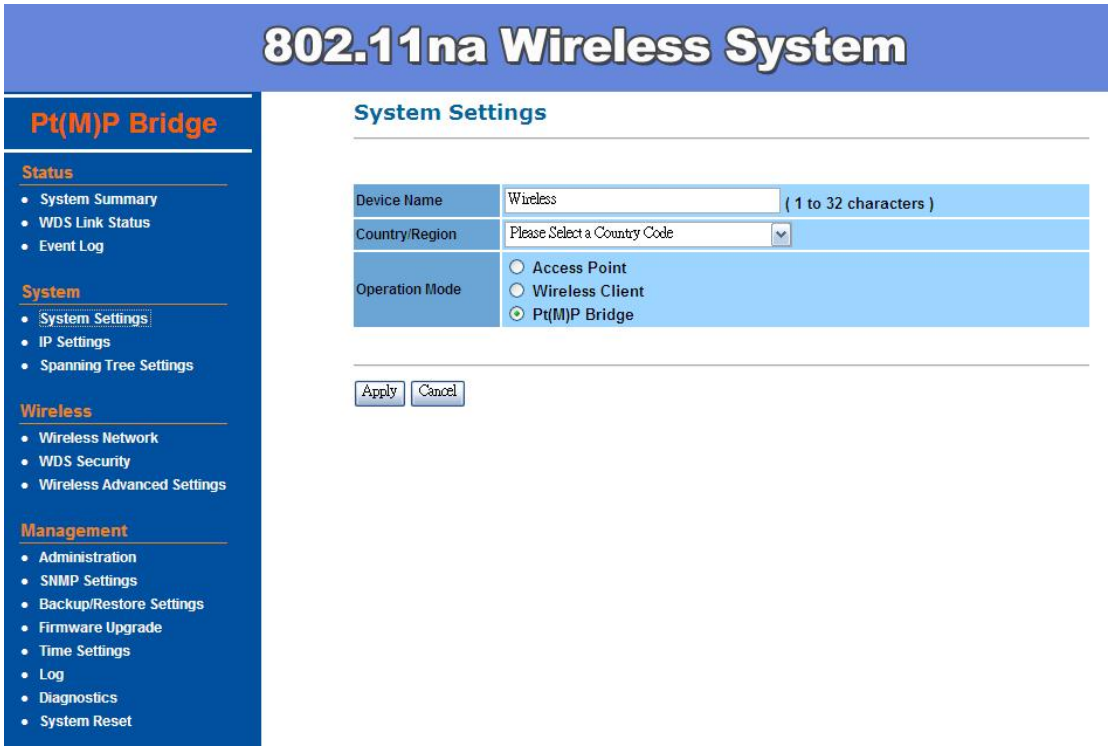


Click **Apply** to save the changes.

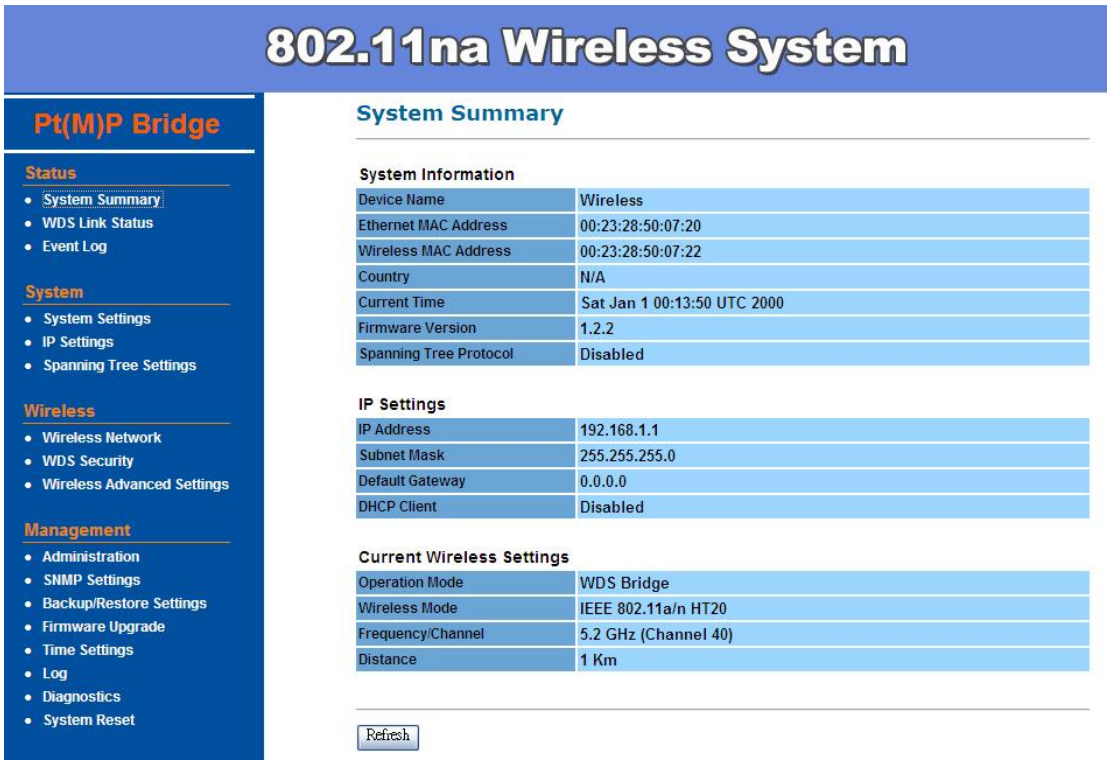


Wireless Configuration – Pt(M)P Bridge Mode

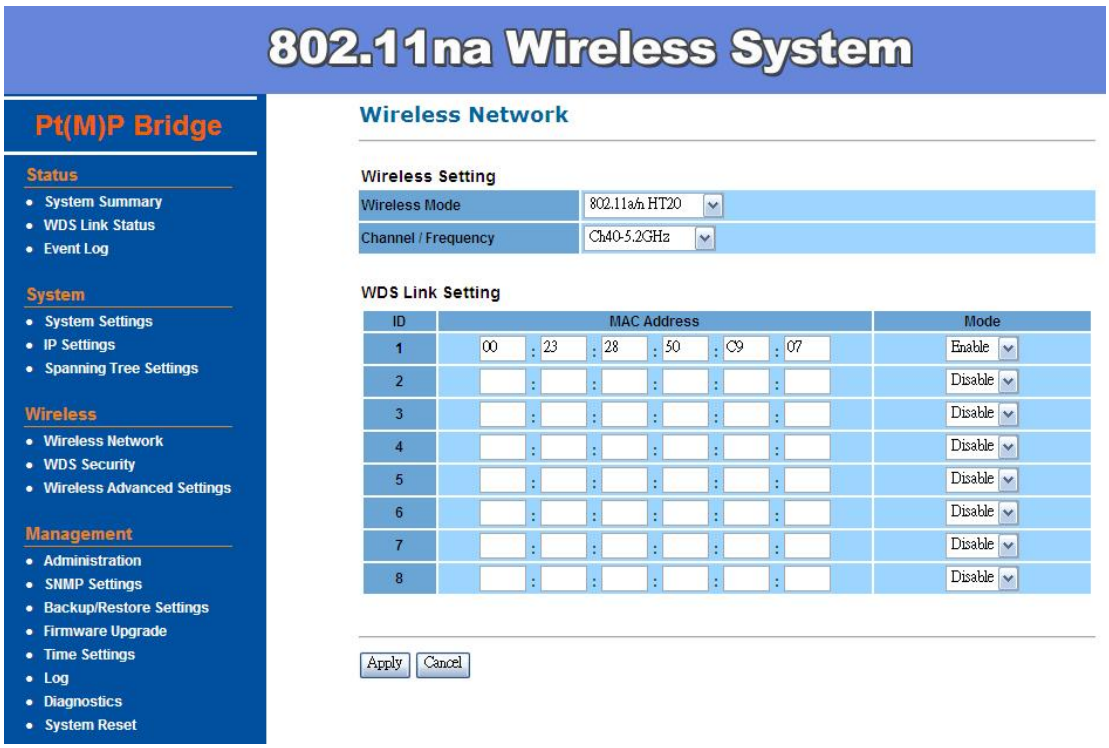
Pt(M)P Bridge means Point to Point or Point to Multi-Point Distribution System which defined by the IEEE802.11 standard. In IEEE 802.11 terminology a Distribution System is a system that Interconnects, so-called, Basic Service Sets (BSS). A BSS is best compared to a **Cell**, driven by a single Access Point (one of those circles in the diagram below). So a **Distribution System** connects cells in order to build a premise wide network which allows users of mobile equipment to roam and stay connected to the available network resources.



Pt(M)P is used for wirelessly connect Access Points, and in doing so to extend a wired infrastructure to locations where cabling is not possible or inefficient to implement (Be sure you understand the purpose of Pt(M)P before proceed configuration).

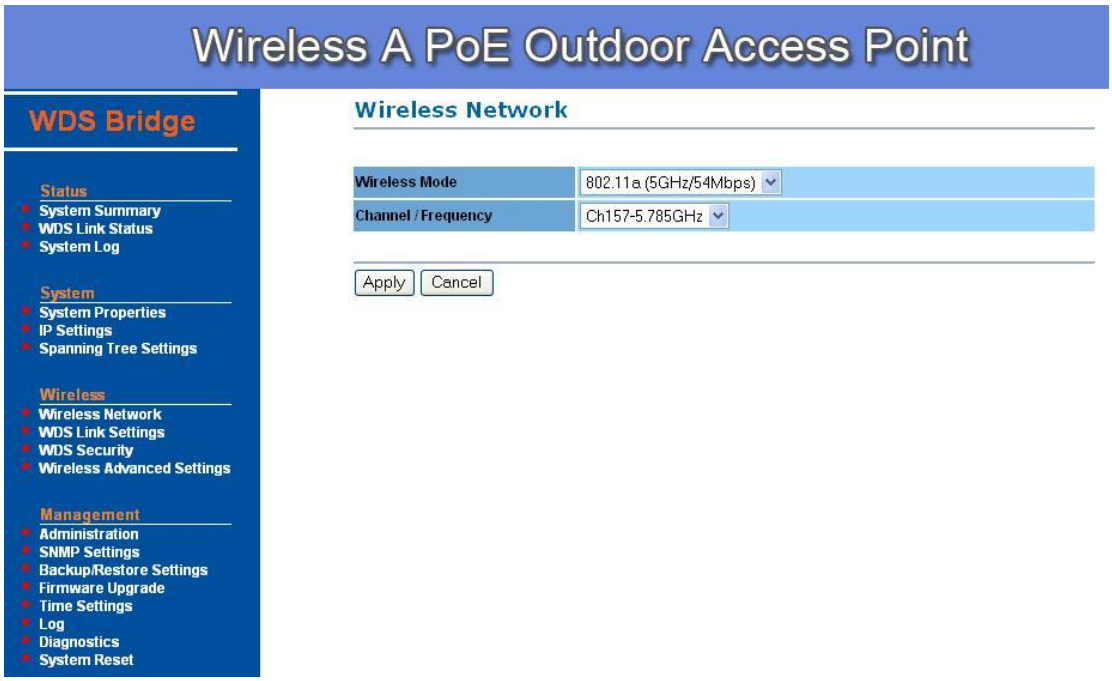


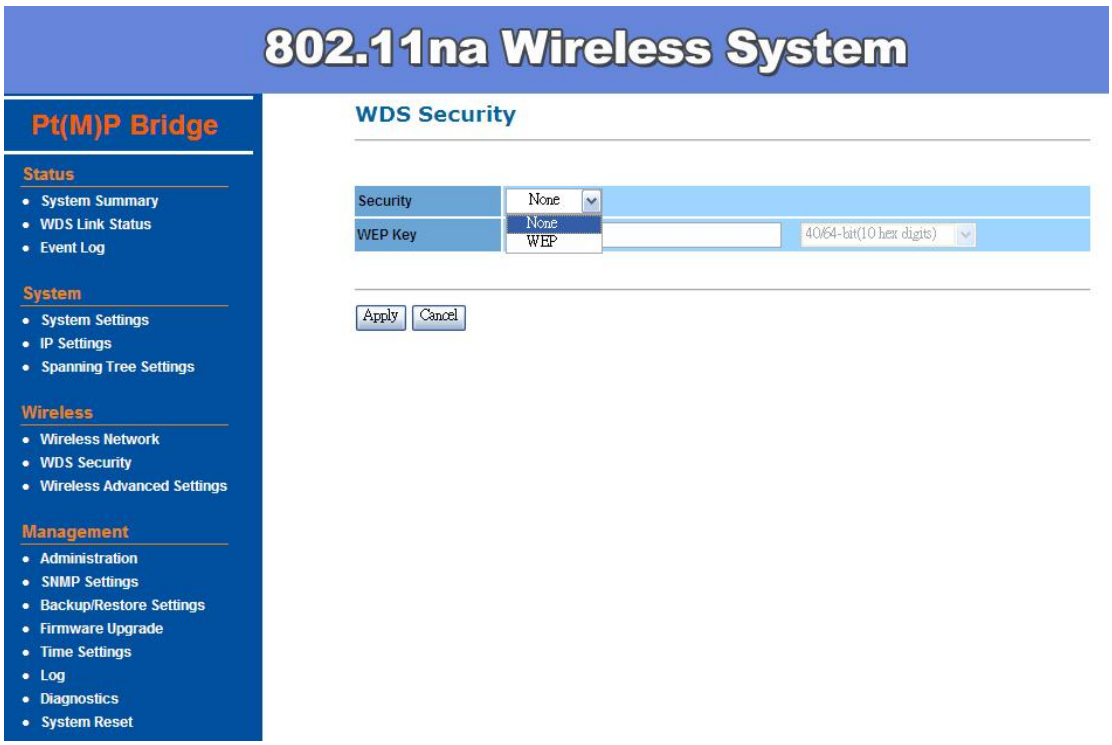
The WDS Link Settings coexist with Wireless WDS Link in this unit. Therefore, you can support regular wireless stations or WDS link. In the **WDS Link Settings**, check box and switch the mode to **Enable**. Then you are able to fill in MAC Address of each WDS link Settings.



Considerations before installation –

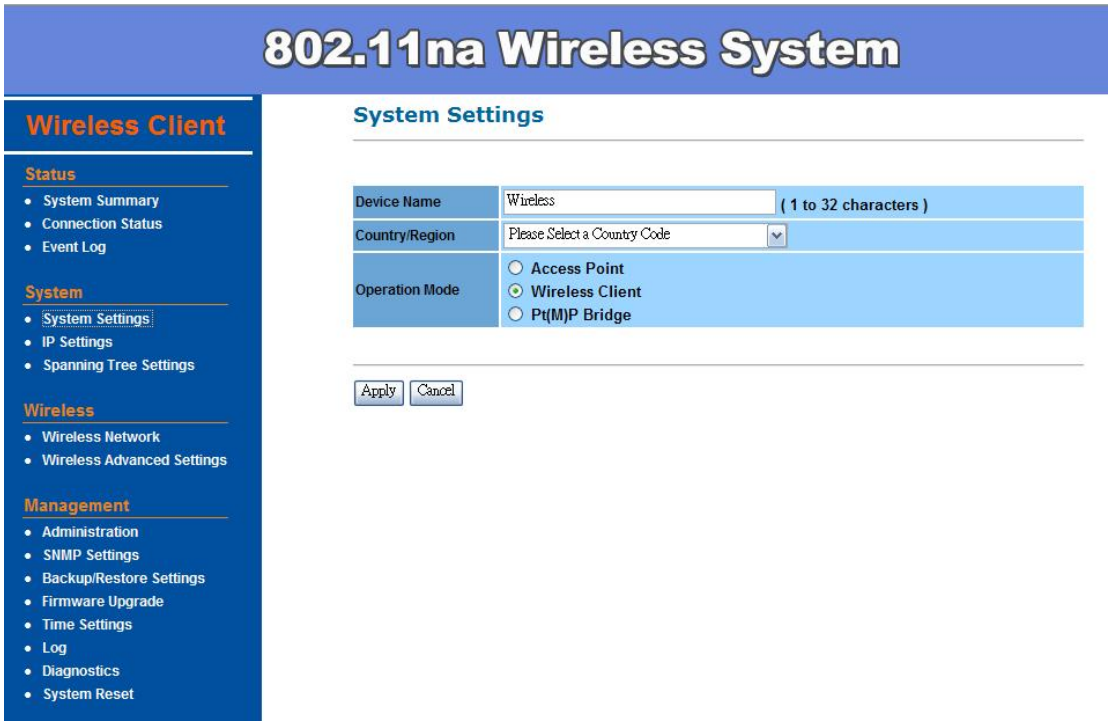
- **Loop Prevention –** Be careful to plan you WDS Link connections, prevent your wireless network topology to have loop. Once loop shows up, you network traffic will become unstable.
- **Performance –** The system can support up to 8 WDS links. But all links and wireless stations that operate at the same time will all share single radio bandwidth (Ex. 11a have 54Mbps bandwidth).
- **Latency –** In the chain topology configuration, if the chain becomes very long, end-to-end latency issue may come in play. We suggest the WDS link topology planning should not exceed 2 hops in chain configuration.




802.11na Wireless System
Pt(M)P Bridge
Status
System Summary
WDS Link Status
Event Log
System
System Settings
IP Settings
Spanning Tree Settings
Wireless
Wireless Network
WDS Security
Wireless Advanced Settings
Management
Administration
SNMP Settings
Backup/Restore Settings
Firmware Upgrade
Time Settings
Log
Diagnostics
System Reset
WDS Security
Security
None
WEP Key
None
WEP
40/64-bit(10 hex digits)
Apply
Cancel

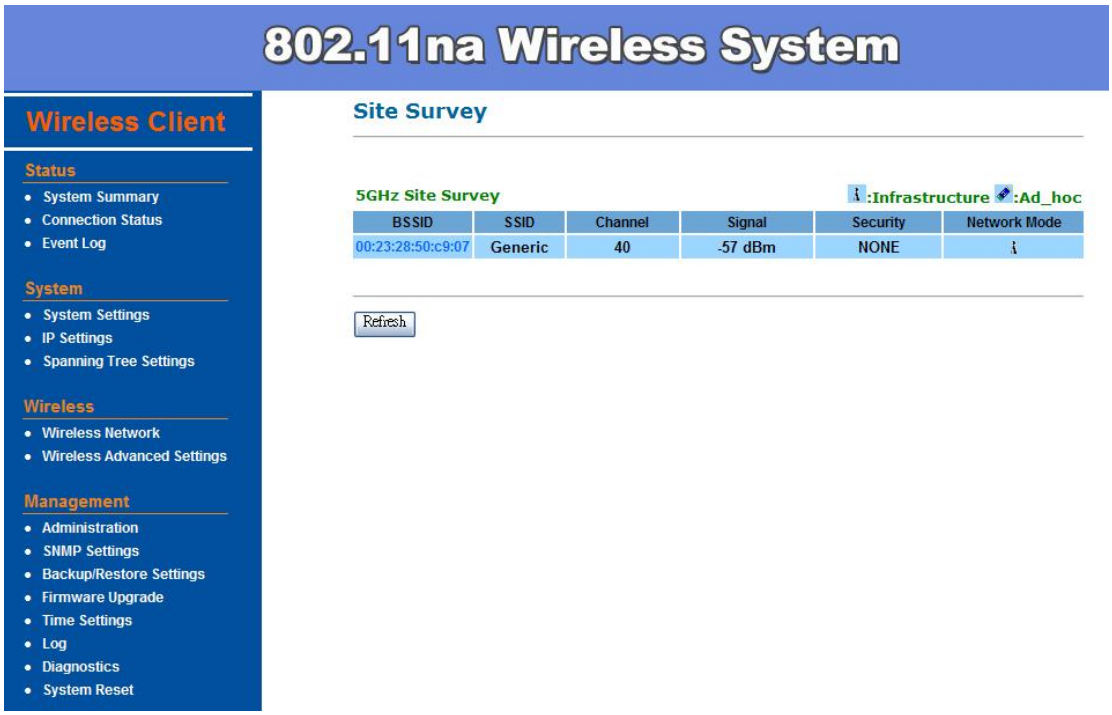
Wireless Configuration – Wireless Client Mode

When set the unit as **Wireless Client**, the unit is able to talk with one remote access point within its range and retransmit its signal.



You can click **Wireless Network** -> **Site Survey** to pick one of the SSIDs you would like to retransmit its signal.

- **Wireless Client Type**: **Universal Client** is to configure the unit to act as general wireless station, while connecting to Access Point with specified SSID, and forward the packets between Ethernet interface and wireless interface.
  WDS Client is to configure the unit to act as the transparent bridge between Ethernet interface and wireless interface, while connecting Access Point with WDS protocol support.
- **Wireless Mode**: Support 802.11a and 802.11a/n HT20 and HT20/HT40 (auto) modes. If you choose HT20/HT40 (auto) mode, the channel bandwidth is using 20 MHz or 40 MHz depended on associated Access Point.
- **SSID**: You can connect to a specific Access Point by entering its SSID directly, or use site survey feature to select the specified Access Point.
- **Prefer BSSID**: This setting is to let the wireless client always connect to the Access Point with specific MAC address, and will not roam to other Access Point with the same SSID.
  Click **Apply** to save the changes.



After clicking **Site Survey**, you can choose the Access Point you need to extend its range by clicking the **BSSID**. Then click **Apply** to make sure system working properly with new setting.

After all the changes are made, you can check **Connect Status** to check current SSID and link quality / signal strength. Some more information are all available at this page.

Appendix A: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 5GHz.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

Download - To receive a file transmitted over a network.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops

networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node - A network junction or connection point, typically a computer or work station.

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 Linksys products.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires

acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

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

WEP (**W**ired **E**quivalent **P**rivacy) - An optional cryptographic confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix B: Notice

Please refer to the following system grounding diagram for your installation reference.

When in doubt, refer to the NEC code to determine proper grounding techniques.

For detailed information regarding grounding the outdoor wireless system.