EnGenius M2000

Wireless Outdoor
Access Point / Client Bridge / Mesh

User Manual

Version: 1.0

Table of Contents

Revision History

Version	Date	Remark
1.0	Nov 30, 2009	Initial Version

1 Introduction

M2000 is a long range outdoor wireless Access Point / Client Bridge that operates in the **2.4GHz** frequency. It provides high bandwidth up to 54Mbps and features high transmitted output power as well as superior sensitivity. M2000 extends radio coverage, avoids unnecessary roaming between Access Points and ensures a stable wireless connection while reduces the number of required equipments. With mesh function implemented, it can be used to establish mesh network, reduces the expense of equipment and risk of disconnection.

M2000 provides user friendly interface including flexible distance control with ranges from 1KM up to 30KM and RSSI LED indicator offering real time signal status. It comes with a PoE injector for convenient outdoor installation.

M2000 enforces transmission security with full support of latest encryption mechanism including 64/128-bit WEP, WPA and WPA2. With a 10dBi Dual Polarization internal antenna and superior performance, M5000 makes an optimal wireless solution for both small and large scale projects.

1.1 Features

Wireless

- ***MESH*** *Easily create a Mesh network of interconnected APs with best link reliability under harsh outdoor environment*
- ***High output power*** *Transmit high output power programmable for different country selections*
- ***10dBi Internal Antenna*** *Built-in 10dBi Dual Polarization Antenna for superior performance*
- ***External Antenna*** *SMA connector to attach higher gain antenna*
- ***High Data Rate*** *High speed transmitting rate up to 54Mbps, support large payload*
- ***Multifunction application*** *Access Point/Client Bridge/Client Router/WDS/MESH Function*
- ***Long range transmitting*** *Transmit power control and distance control (ACK timeout)*
- ***Narrow Bandwidth*** *Provides 5MHz/10MHz/20MHz bandwidth selection*
- ***Signal Strength Display*** *RF signal strength status shown with 3 color LEDs for easy deployment to find the best signal reception.*
- ***Multiple SSID*** *4 SSID supported. Each SSID can set itself wireless or WAN access setting*
- ***AP Detection*** *Scan all neighboring APs with their channels and signal strengths*
- ***QoS(WMM)*** *Enhance performance and density*

Networking

- ***PPPoE*** *Point-to-Point Protocol over Ethernet in Client Router mode.*
- ***PPTP*** *Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks*
- ***VPN Pass Through***

Security

- ***802.11i*** *WEP, WPA, WPA2 (Encryption support TKIP/AES)*
- ***MAC address functions*** *MAC address filter (AP mode)*
- ***802.1x*** *IEEE802.1x Authentication*
- ***Station isolation***

Management

- ***Firmware Upgrade*** *Upgrading firmware via web browser, setting are kept after upgrade*
- ***Reset & Backup*** *Reset to factory default. User can export all setting into a file via WEB Interface.*
- ***Ping & Trace Route*** *Built-in PING function & Trace Route function in Web GUI*
- ***MIB*** *MIB I, MIB II(RFC1213), Private MIB*
- ***SNMP*** *V1, V2c*

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- 1* M2000
- 1* PoE injector (EPE-1212)
- 1* Power Adaptor (24V/0.6A)
- 1* CD with User's Manual
- 1* Quick Installation Guide (QIG)
- 1* Metal Strap
- 2* Special Screw Set

1.3 System Requirements

The following are the minimum system requirements in order to configure the device.

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

1.4 Applications

The wireless LAN products are 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 changing environments***
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) ***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.

f) ***Wired LAN backup***
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

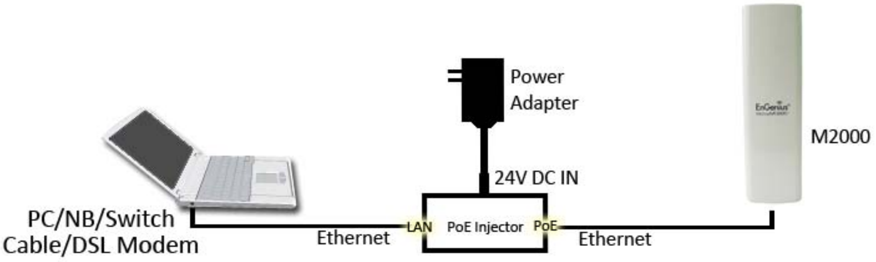
g) ***Training/Educational facilities***
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2 Understanding the Hardware

2.1 Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Network port of the PoE injector and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to AP/Bridge port of the PoE injector and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the 24V port of the PoE injector and the other end into the power socket on the wall.

This diagram depicts the hardware configuration



2.2 Hardware Description

The images below depict the front and rear panel of the unit.

Front Panel

Rear Panel

2.3 Mounting Kits

The images below depict the standard mounting kits.

Pole Mount

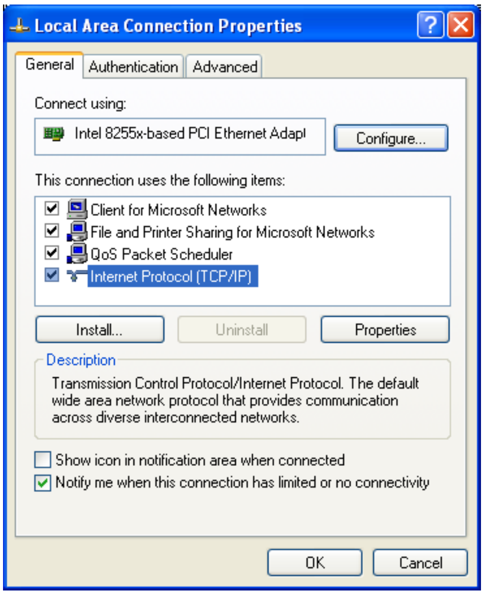
Wall Mount

Window Mount

2.4 IP Address Configuration

This device can be configured as a **Access Point** / **Client Bridge** / **WDS Bridge** / **Client Router / MESH**. The default IP address of the device is **192.168.1.1**. And in order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Intel 8255x-based PCI Ethernet Adapl

This connection uses the following items:

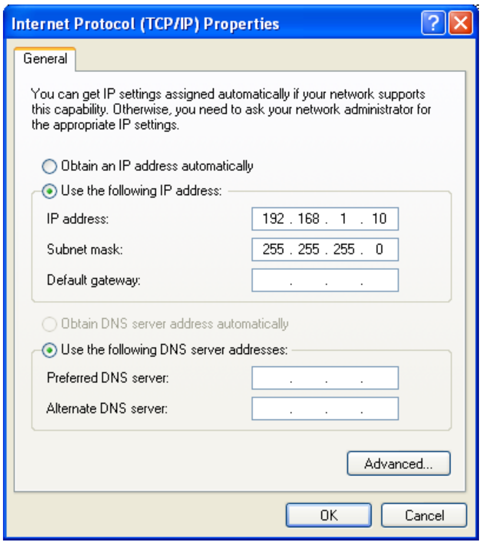
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

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

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

2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.
   For Example:

   PC IP address: 192.168.1.10
   PC subnet mask: 255.255.255.0

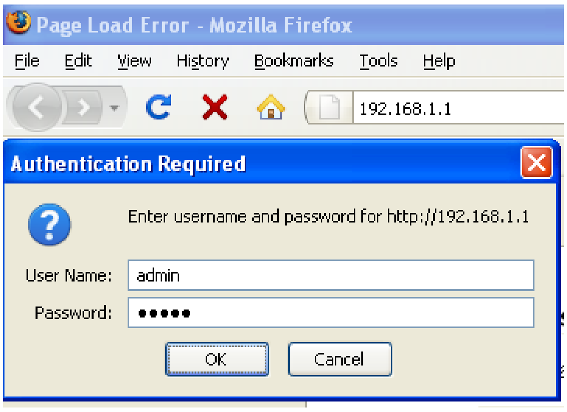
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

3 Switching Between Operating Modes

This device can operate in three modes: Access Point, Client Bridge, WDS Bridge, Client Router and Mesh modes. This chapter will describe how to switch between operating modes.

3.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computer are configured on the same subnet. (Refer to **Chapter 2** in order to configure the IP address of your computer)
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.

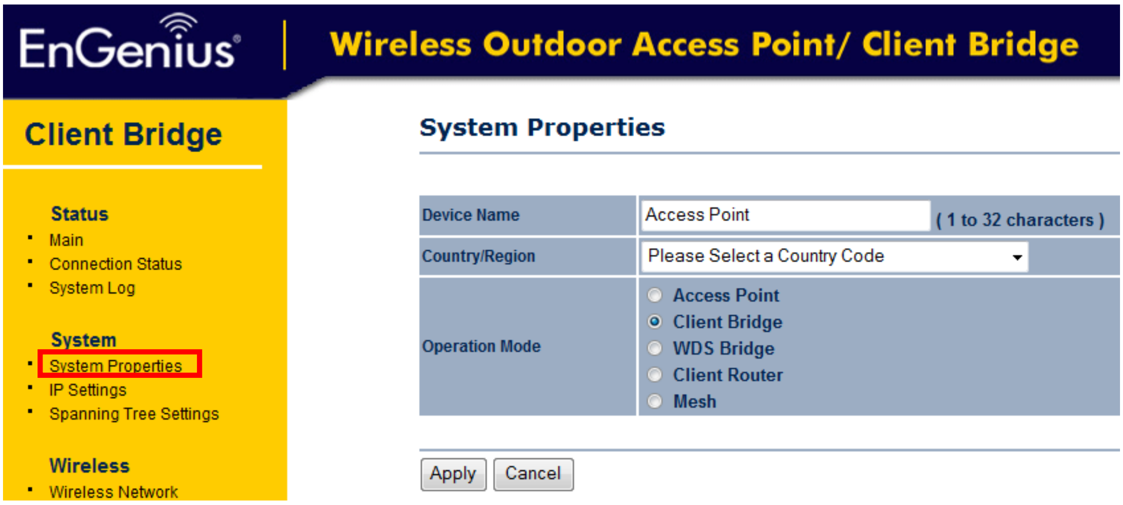

Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1
Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: •••••

- After logging in, you will see the graphical user interface of the device. Click on the **System Properties** link under the **System** section of the left menu.



Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	○ Access Point ● Client Bridge ○ WDS Bridge ○ Client Router ○ Mesh

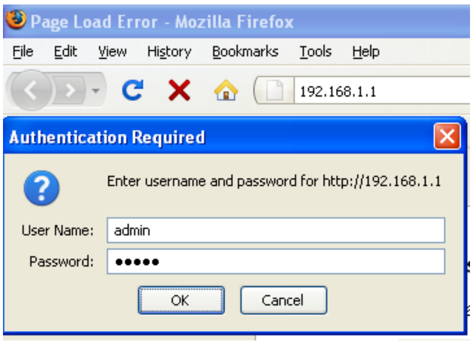
- Select operating mode you want from the list (Access Point, Client Bridge, WDS Bridge, Client Router or Mesh) and then click on the **Apply** button.

4 Access Point Operating Mode

4.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password (Default settings)
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:

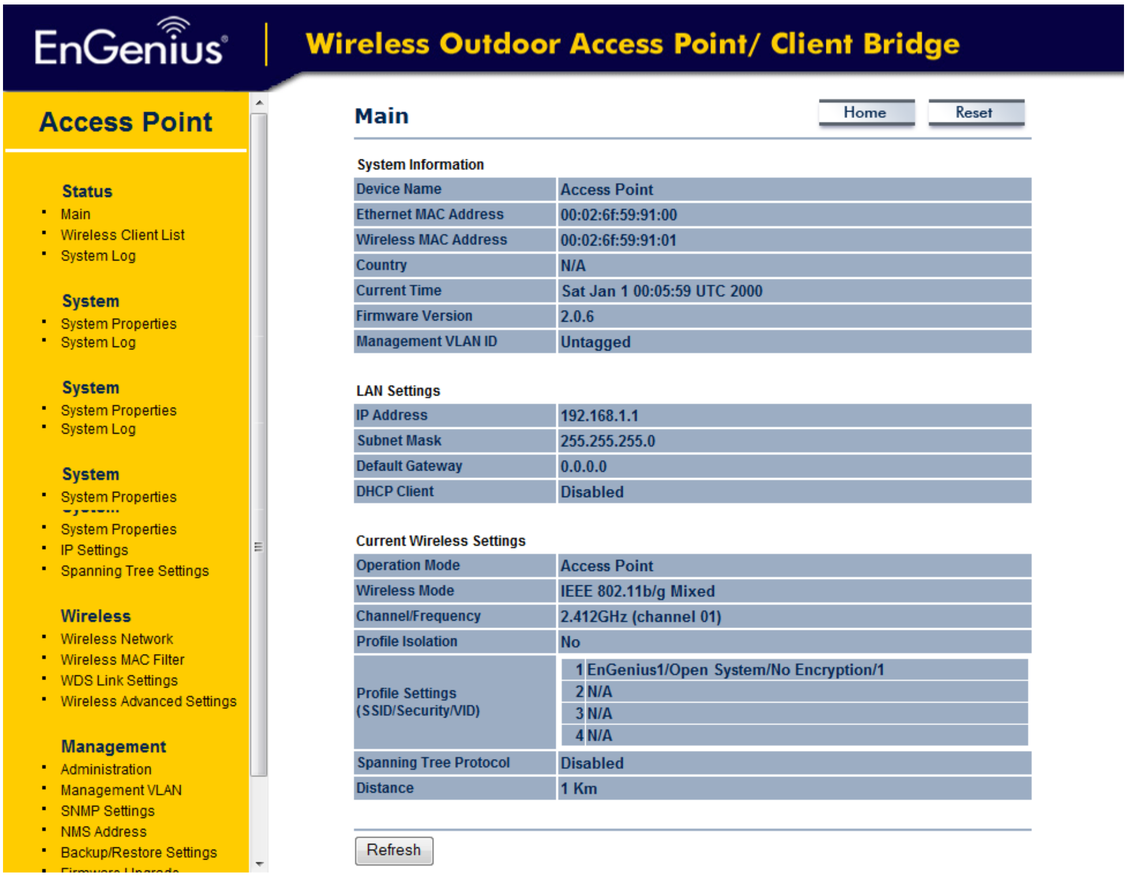
1. **Status**: Displays the overall status, connection status, and event log.
2. **System**: This menu includes the system properties, IP and Spanning Tree settings.
3. **Wireless**: This menu includes network setting, MAC filter, WDS link, advanced, and security.
4. **Management**: This menu includes the admin setup, SNMP, firmware upgrade, diagnostics, time setting and save/restore backup.


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1
Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: ●●●●●



System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:05:59 UTC 2000
Firmware Version	2.0.6
Management VLAN ID	Untagged

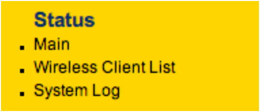
LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1 2 N/A 3 N/A 4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

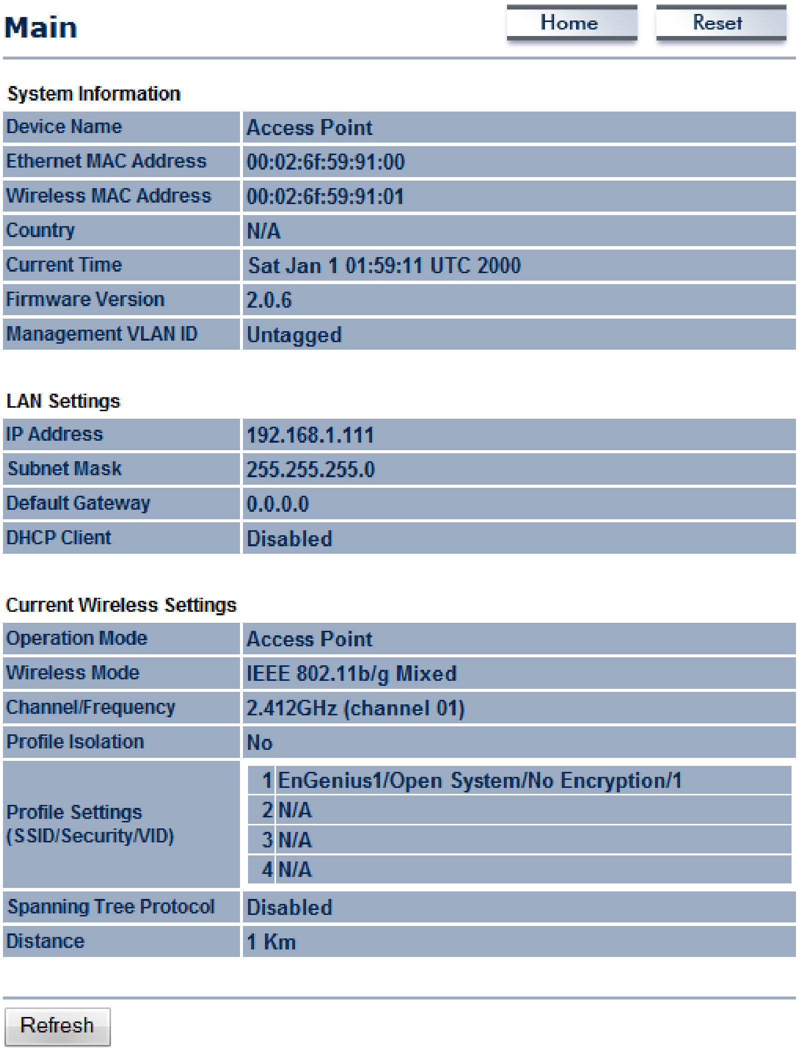
4.2 Status



- There are three options under the **Status** section of the left menu: **Main, Wireless Client List**, and **System Log**. Each option is described in detail below.

4.2.1 Main

- The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, MAC Address, Country, Current Time and Firmware Version are displayed in the 'System Information' section. IP address, Subnet Mask, and Default Gateway are displayed in the 'LAN Setting' section. In the 'Wireless Settings' section, Operation Mode, Wireless Mode, Channel/Frequency, MSSID with security, Spanning Tree and Distance setting are displayed.



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 01:59:11 UTC 2000
Firmware Version	2.0.6
Management VLAN ID	Untagged

LAN Settings

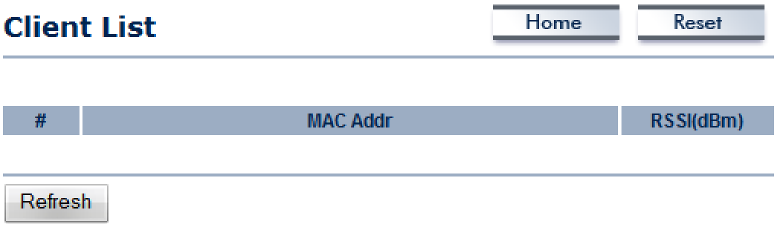
IP Address	192.168.1.111
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1 2 N/A 3 N/A 4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

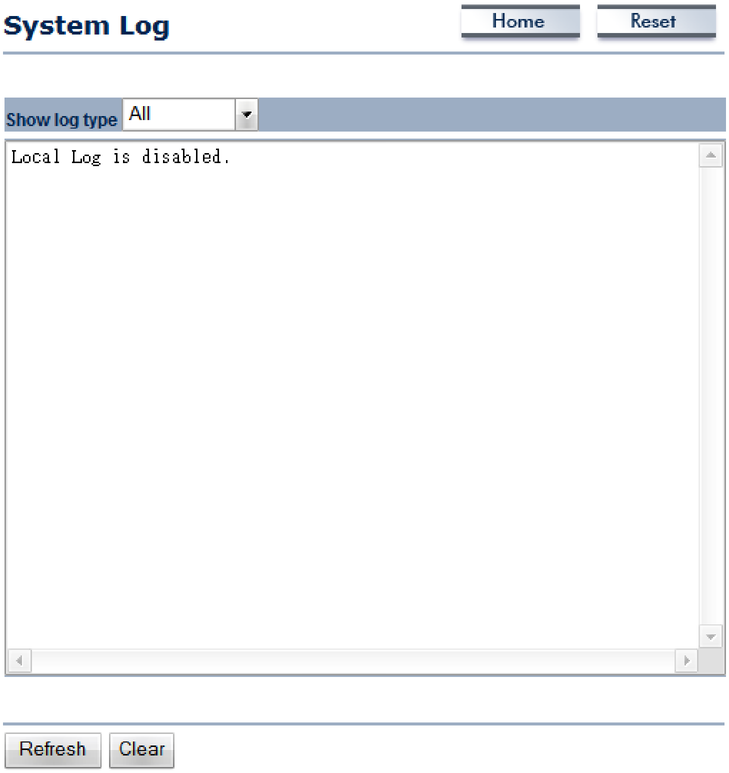
4.2.2 Wireless Client List

- This page displays the list of Clients that are associated to the Access Point.
- The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list.



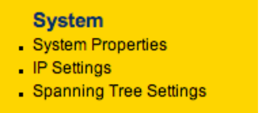
4.2.3 System Log

- The device automatically logs (records) 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.



```
Local Log is disabled.
```

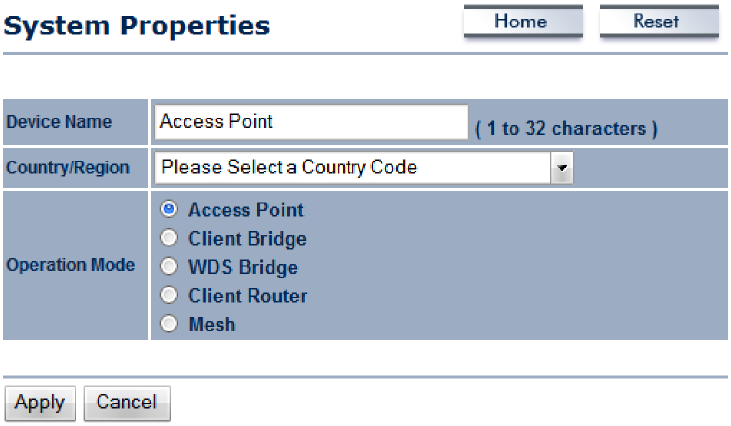
4.3 System



- Under the **System** section of the left menu, you will see the following options: **System Properties, IP Settings,** and **Spanning Tree Settings**. Each option is described in detail below.

4.3.1 System Properties

- This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

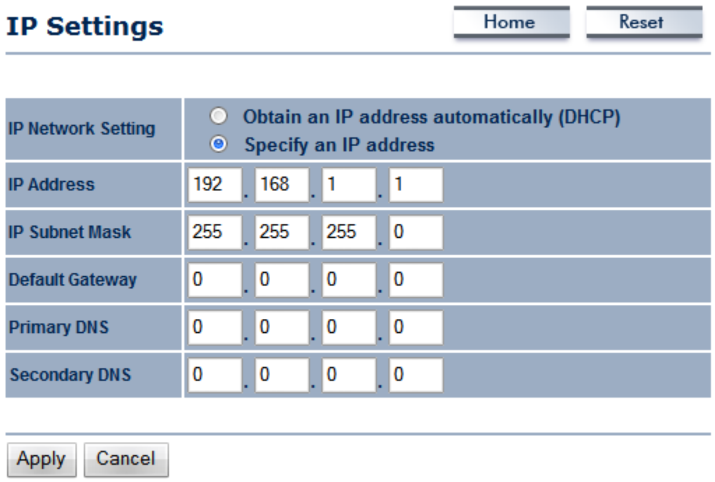


Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	● Access Point ○ Client Bridge ○ WDS Bridge ○ Client Router ○ Mesh

- **Device Name**: Specify a name for the device (this is not the SSID),
- **Country/Region**: Select a country from the drop-down list.
- **Operating Mode**: Select an Operating Mode. Configuration for each Operating Mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

4.3.2 IP Settings

- This page allows you to configure the device with a static IP address or a DHCP client.



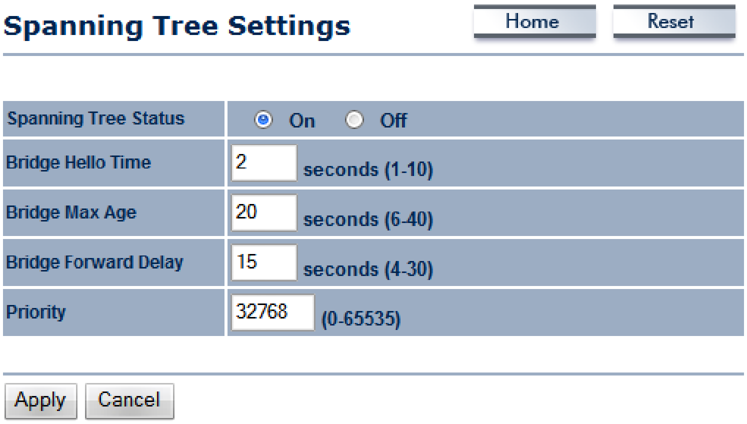
IP Settings

IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **IP Network Setting**: Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address**: Specify an IP address
- **IP Subnet Mask**: Specify the subnet mask for the IP address
- **Default Gateway**: Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

4.3.3 Spanning Tree Settings

- Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

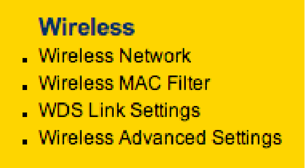


Spanning Tree Settings

Spanning Tree Status	● On ○ Off
Bridge Hello Time	2 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	15 seconds (4-30)
Priority	32768 (0-65535)

- **Spanning Tree Status**: Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time**: Specify the Bridge Hello Time in seconds.
- **Bridge Max Age**: Specify the Bridge Max Age in seconds.
- **Bridge Forward Delay**: Specify the Bridge Forward Delay in seconds.
- **Priority**: Specify the priority number.
- Click on the **Apply** button to save the changes.

4.4 Wireless

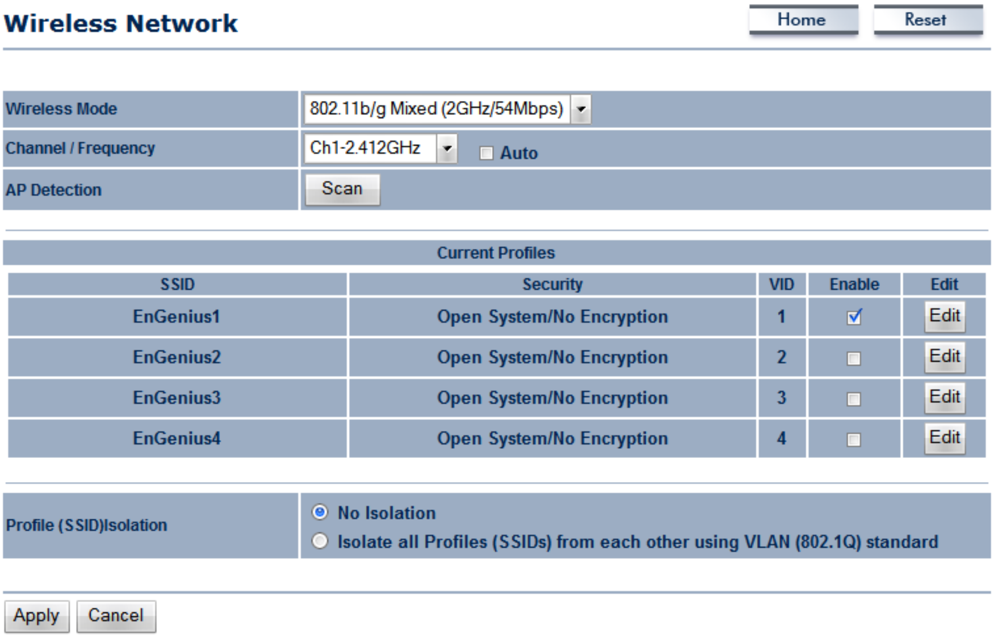


Wireless
- Wireless Network
- Wireless MAC Filter
- WDS Link Settings
- Wireless Advanced Settings

- The **Wireless** section of the left menu has the following options: **Wireless Network, Wireless MAC Filter, WDS Link Settings**, and **Wireless Advanced Settings**. Each option is described below.

4.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.



Wireless Network

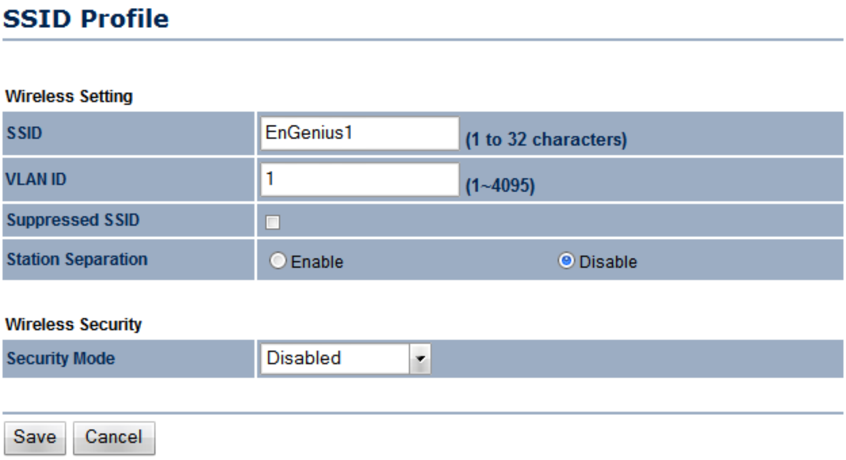
Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
Channel / Frequency	Ch1-2.412GHz □ Auto
AP Detection	Scan

Current Profiles

SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	☑	Edit
EnGenius2	Open System/No Encryption	2	□	Edit
EnGenius3	Open System/No Encryption	3	□	Edit
EnGenius4	Open System/No Encryption	4	□	Edit

Profile (SSID)Isolation	● No Isolation ○ Isolate all Profiles (SSIDs) from each other using VLAN (802.1Q) standard

- **Wireless Mode**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G or B/G-mixed or Super-G**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **Channel / Frequency**: Select a channel from the drop-down list. The channels available are based on the country's regulation.
- **Auto**: The M2000 will scan nearby wireless signals and choose the channel with the least interference.
- **AP Detection:** Press the **Scan** button to find nearby wireless signals.
- **Current Profiles**: User can setup SSID configuration in this item. M2000 supports 4 SSIDs, user can decide to use how many SSID via "Enable" or not. When click "Edit" button, you can setup detail, include SSID, VLAN ID and Security Mode.
- **Profile (SSID) Isolation**: When you select this function to enable, unit can isolate all profiles(SSIDs) from each other using VLAN standard.



SSID Profile

Wireless Setting

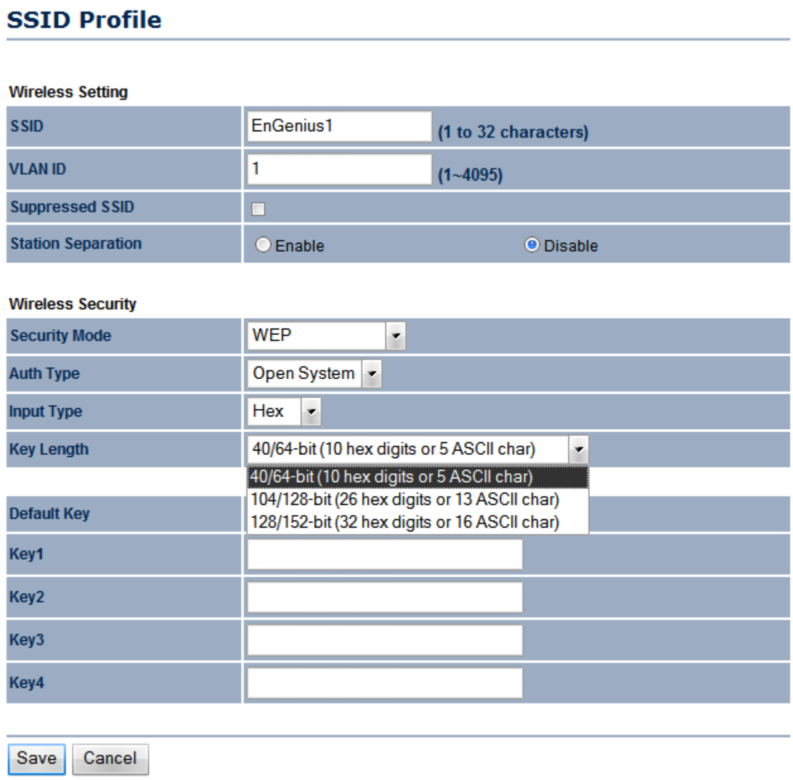
SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	Disabled

- **SSID**: Type in your SSID
- **VLAN ID:** Specify the VLAN ID to be applied to this SSID.
- **Suppressed SSID:** When enabled, the SSID will be hidden.
- **Station Separation:** When enabled, wireless clients on different SSID's cannot connect with each other.

▶ Wireless Security – Security Mode : WEP



SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char) 40/64-bit (10 hex digits or 5 ASCII char) 104/128-bit (26 hex digits or 13 ASCII char) 128/152-bit (32 hex digits or 16 ASCII char)
Default Key	
Key1	
Key2	
Key3	
Key4	

▶▶ **Security Mode**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

▶▶ **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. 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 Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point allows the requesting device to authenticate.

▶▶ **Input Type**: Select Hex or ASCII from the drop-down list

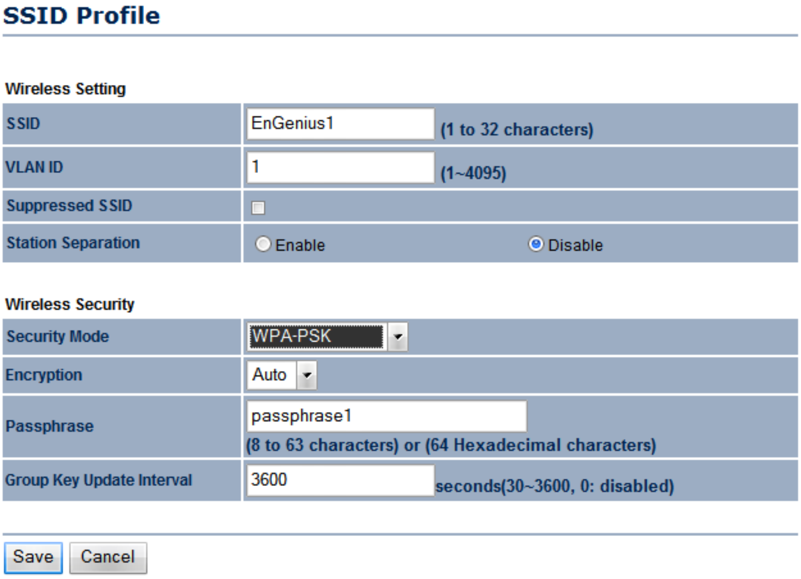
▶▶ **Key Length**: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters and 152-bit keys require 32 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.

▶▶ **Default Key**: You may use up to four different keys for four different networks. Select the current key that will be used.

▶▶ **Key 1-4**: You may enter four different WEP keys.

▶▶ Click on the **Save** button to save the changes.

▶ Wireless Security – Security Mode : WPA-PSK, WPA2-PSK, WPA-PSK Mixed



SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	WPA-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

▶▶ **Security Mode**: Select **WPA-PSK, WPA2-PSK, or WPA-PSK Mixed** from the drop-down list if your wireless network uses WPA pre-shared key.

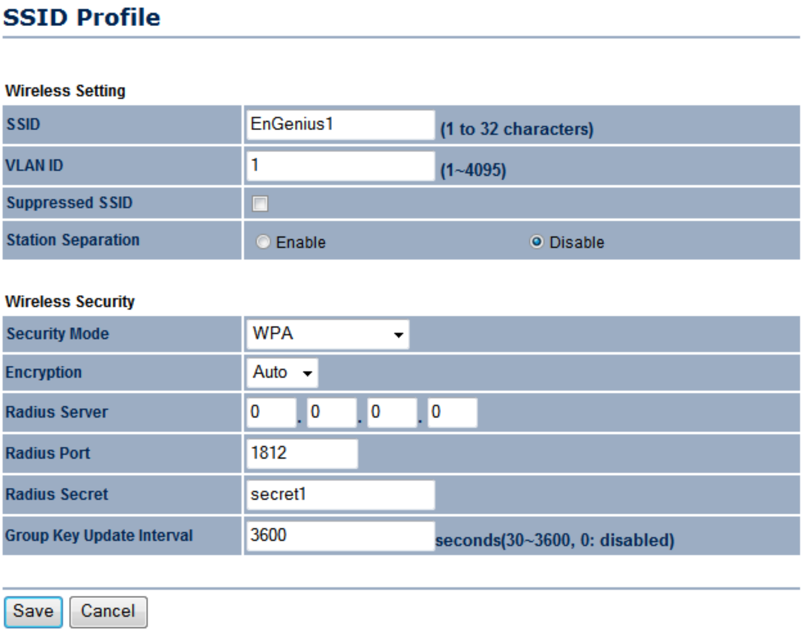
▶▶ **Encryption**: Select **TKIP**, **AES** or **Auto** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with. AES is an even more advanced method of encryption which offers the highest level of WPA/WPA2 security.

▶▶ **Passphrase**: Specify a passphrase that is shared amongst the Access Points and clients.

▶▶ **Group Key Update Interval**: Specify the number of seconds after which the Access Point will probe the client for the passphrase.

▶▶ Click on the **Save** button to save the changes.

▶ Wireless Security – Security Mode : WPA, WPA2, WPA Mixed



SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	WPA
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

▶▶ **Security Mode**: Select **WPA, WPA2 or WPA Mixed** from the drop-down list if your wireless network uses WPA. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

▶▶ **Encryption**: Select **TKIP**, **AES** or **Auto** from the drop-down list if your wireless network uses this encryption.

▶▶ **RADIUS Server:** Enter the IP address of the RADIUS server.

▶▶ **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.

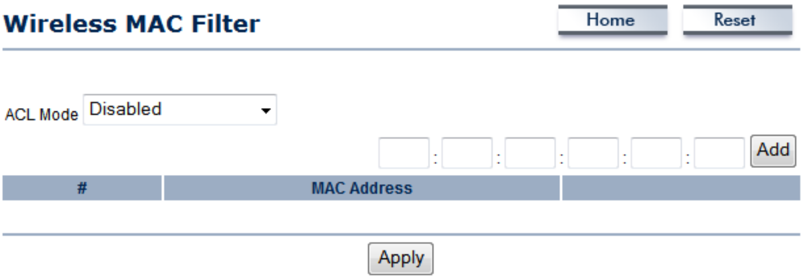
▶▶ **RADIUS Secret:** Enter the shared password of the RADIUS server.

▶▶ **Group Key Update Interval**: Specify the number of seconds after which the Access Point will probe the client for the secret.

▶▶ Click on the **Save** button to save the changes.

4.4.2 Wireless MAC Filter

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



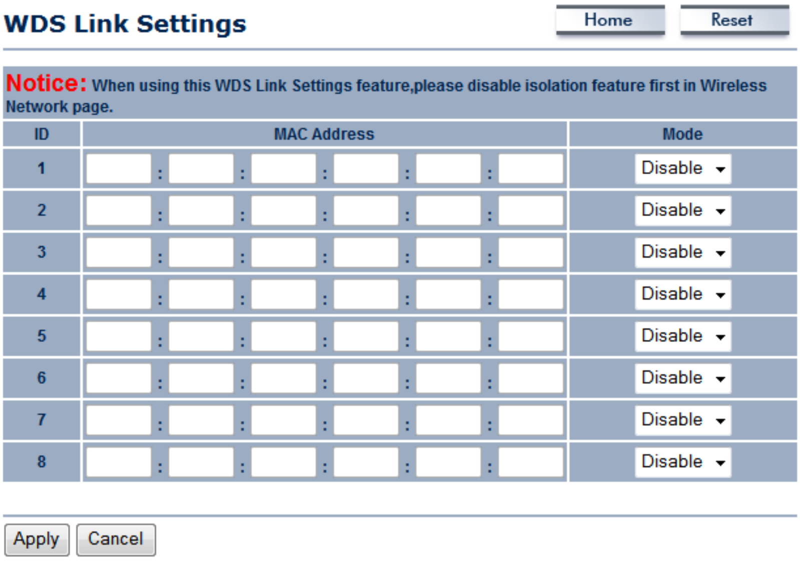
ACL Mode: Disabled

- **ACL (Access Control) Mode:** You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC addresses from associating with the network. 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 on the **Delete** button.
- Click on the **Apply** button to save the changes.

4.4.3 WDS Link Settings

On this page you can set the WDS link to connect to another WDS AP or WDS Bridge. The Maximum connection is up to 8 units.

Please enter the MAC Addresses of the other Access Points in your WDS network.



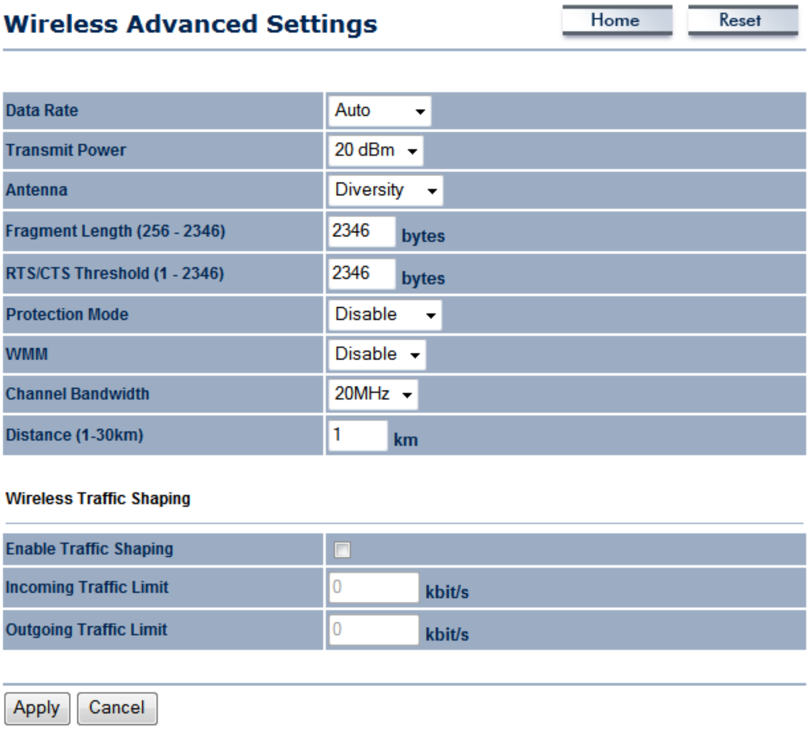
WDS Link Settings

Notice: When using this WDS Link Settings feature,please disable isolation feature first in Wireless Network page.

ID	MAC Address	Mode
1	: : : : :	Disable
2	: : : : :	Disable
3	: : : : :	Disable
4	: : : : :	Disable
5	: : : : :	Disable
6	: : : : :	Disable
7	: : : : :	Disable
8	: : : : :	Disable

4.4.4 Wireless Advanced Settings

- On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: **Data Rate, Transmit Power, Fragment Length, RTS Threshold, Protection Mode** and **Distance**.



Wireless Advanced Settings

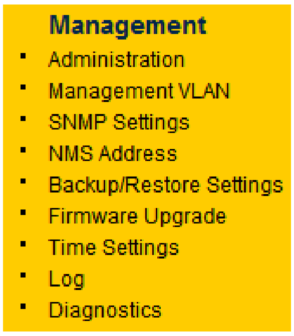
Data Rate	Auto
Transmit Power	20 dBm
Antenna	Diversity
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

Wireless Traffic Shaping

Enable Traffic Shaping	□
Incoming Traffic Limit	0 kbit/s
Outgoing Traffic Limit	0 kbit/s

- **Data Rate**: If you would like to have a fixed data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Antenna**: You can select the antenna polarization to Diversity, Horizontal or Vertical.
- **Fragment Length**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS/CTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode**: If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM**: Enable wireless Quality of Service
- **Distance (1-30km)**: Specify a distance between 1 and 30Km.
- **Channel Bandwidth**: For different application, you can select 20MHz, 10MHz or 5MHz channel bandwidth.
- **Wireless Traffic Shaping:** Specify the maximum bandwidth allocated to Incoming and Outgoing traffic.
- Click on the **Apply** button to save the changes.

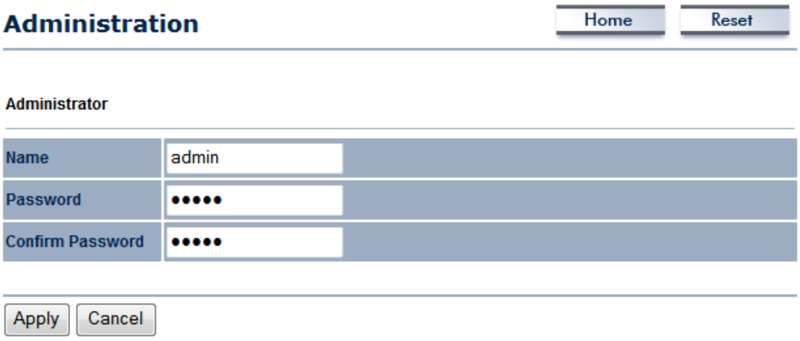
4.5 Management



- The following options are under the **Management** section of the left menu: **Administration, SNMP Settings, Backup/Restore Settings, Firmware Upgrade, Time Settings**, **Log** and **Diagnostics**. Each option is described below.

4.5.1 Administration

- This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



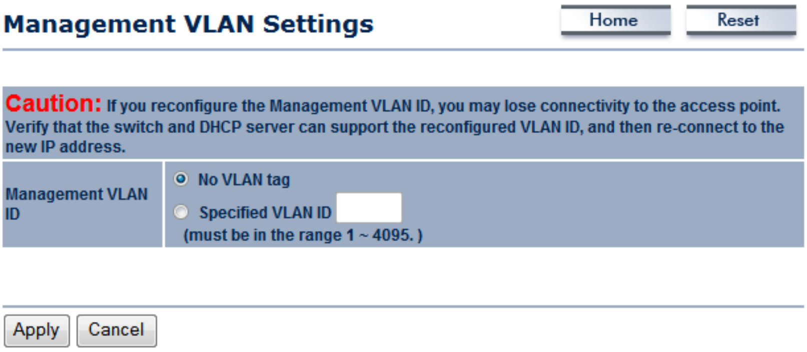
Name	admin
Password	•••••
Confirm Password	•••••

- **Name**: Specify a user name into the first field.
- **Password**: Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

4.5.2 Management VLAN

- This option allows you to specify VLAN ID (From 1 to 4095).

  Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify the switch and DHCP server can support the reconfigured VLAN ID, and then reconnect to new IP address.



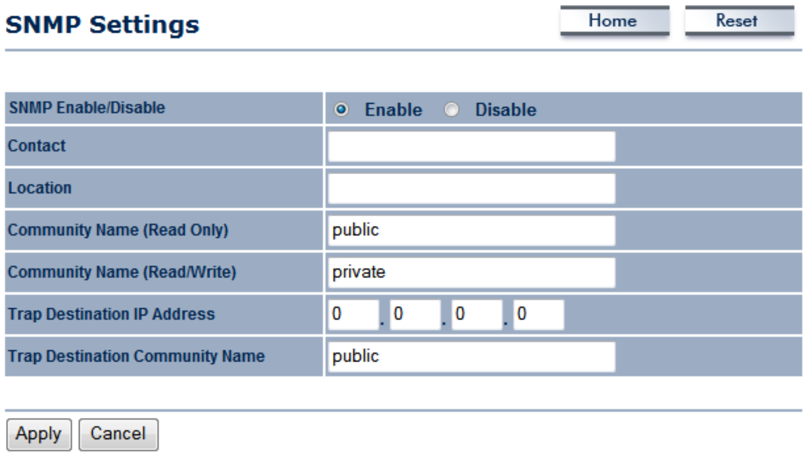
Management VLAN Settings

Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID	● No VLAN tag ○ Specified VLAN ID (must be in the range 1 ~ 4095.)

4.5.3 SNMP Settings

- This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

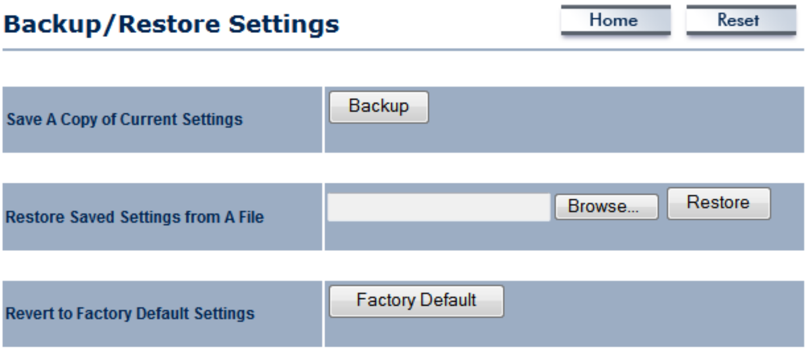


SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

- **SNMP Enable/Disable**: Choose to **enable** or **disable** the SNMP feature.
- **Contact**: Specify the contact details of the device.
- **Location**: Specify the location of the device.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name**: Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

4.5.4 Backup/Restore settings, Reset to factory default settings

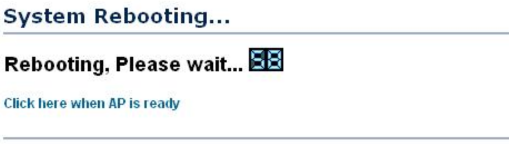
- This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.



Backup/Restore Settings

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	Browse... Restore
Revert to Factory Default Settings	Factory Default

- **Save a copy of the current settings**: Click on the Backup button to save the current configuration.
- **Restore saved settings from a file**: Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings**: Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: **192.168.1.1**



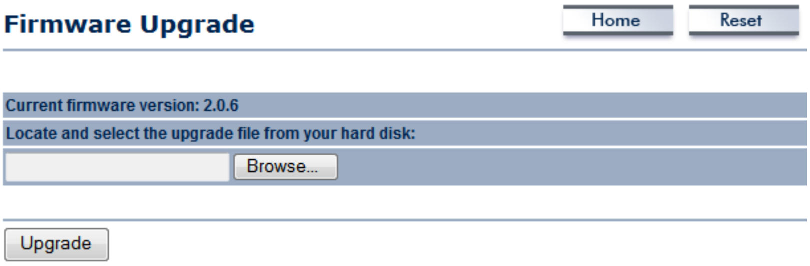
System Rebooting...

Rebooting, Please wait... 88

Click here when AP is ready

4.5.5 Firmware Upgrade

- This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



Firmware Upgrade

Current firmware version: 2.0.6

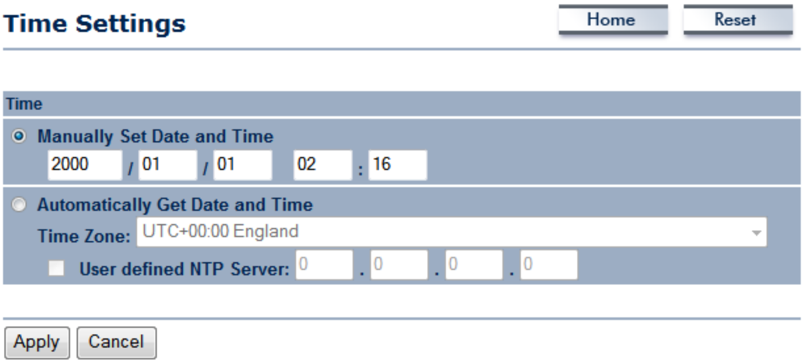
Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.

  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

4.5.6 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.



Time Settings

Time

● Manually Set Date and Time

2000 / 01 / 01 02 : 16

○ Automatically Get Date and Time

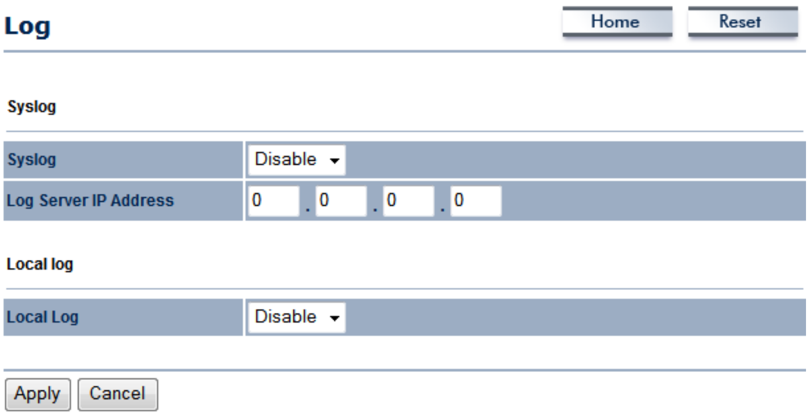
Time Zone: UTC+00:00 England

□ User defined NTP Server: 0 . 0 . 0 . 0

- **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 on the **Apply** button to save the changes.

4.5.7 Log

- The **Log** 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

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

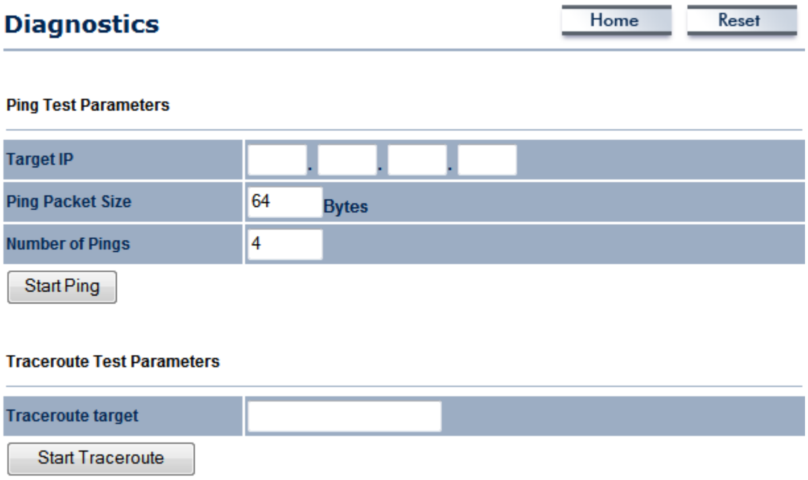
Local log

Local Log	Disable

- **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 on the **Apply** button to save the changes.

4.5.8 Diagnostics

- In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



Ping Test Parameters

Target IP	. . .
Ping Packet Size	64 Bytes
Number of Pings	4

Traceroute Test Parameters

Traceroute target	

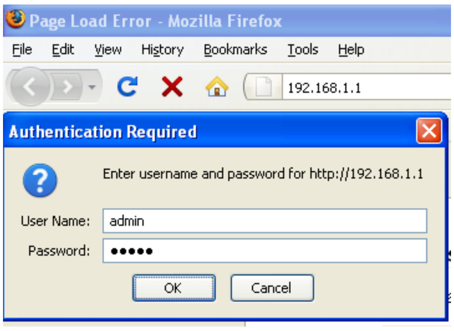
- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click Start Ping.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

5 Client Bridge Operating Mode

5.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:

1. **Status**: Displays the overall status, connection status, and system log.
2. **System**: This menu includes the system properties, IP and Spanning Tree settings.
3. **Wireless**: This menu includes network, security and advanced settings.
4. **Management**: This menu includes the admin setup, SNMP, firmware upgrade, time settings, diagnostics and save/restore backup.


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1

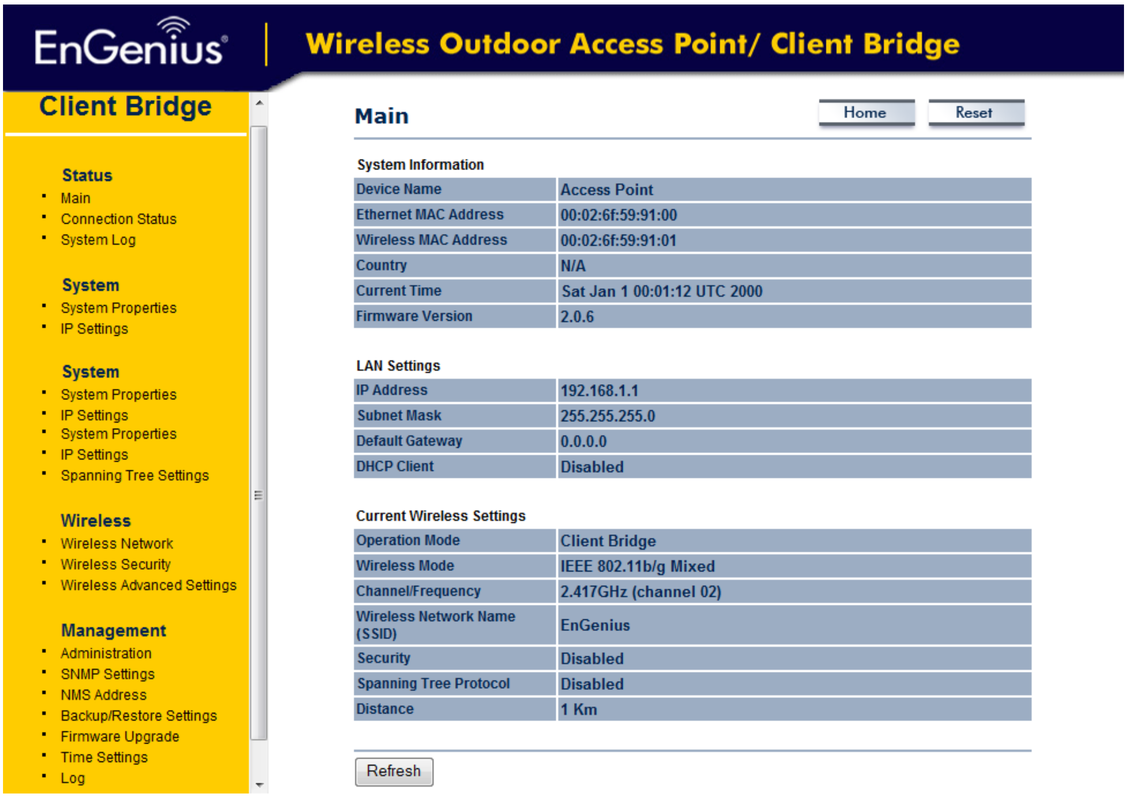
Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: •••••

OK Cancel



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:01:12 UTC 2000
Firmware Version	2.0.6

LAN Settings

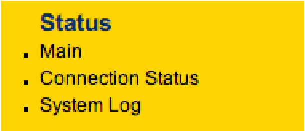
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.417GHz (channel 02)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Spanning Tree Protocol	Disabled
Distance	1 Km

Refresh

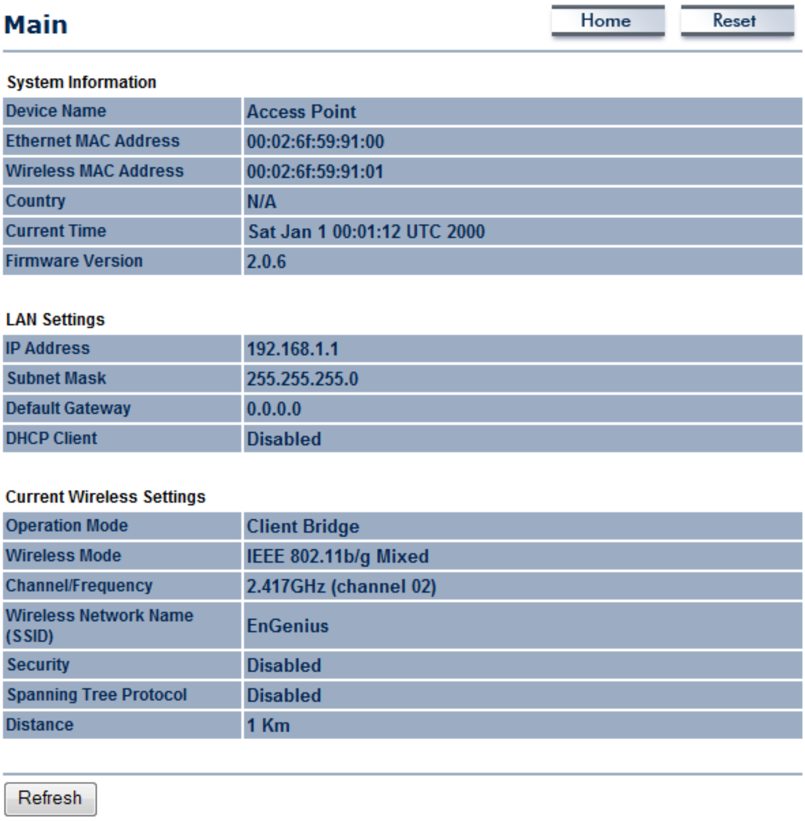
5.2 Status



- There are three options under the **Status** section of the left menu: **Main, Connection Status,** and **System Log**. Each option is described in detail below.

5.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as device name, firmware version, MAC address, country and current time are displayed in the 'System Information' section. IP address, subnet mask, default gateway and DHCP client are displayed in the 'LAN Settings' section. In the 'Current Wireless Settings' section, the operation mode, wireless mode, channel/frequency, SSID, security and distance are displayed.
-



System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:01:12 UTC 2000
Firmware Version	2.0.6

LAN Settings

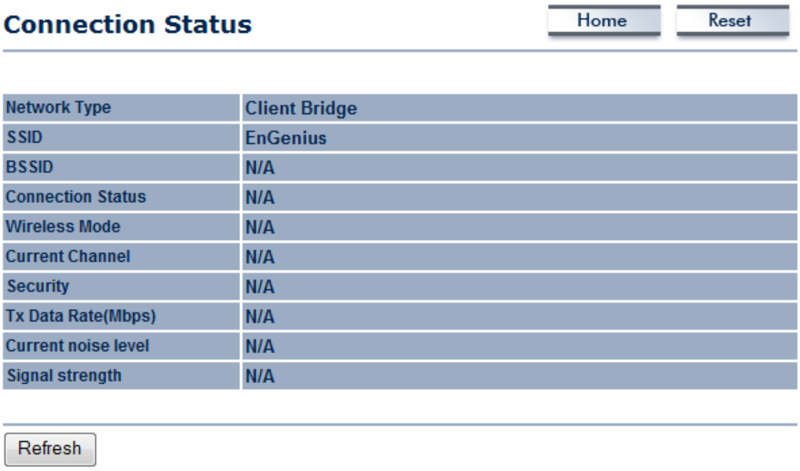
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.417GHz (channel 02)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Spanning Tree Protocol	Disabled
Distance	1 Km

5.2.2 Connection Status

- Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

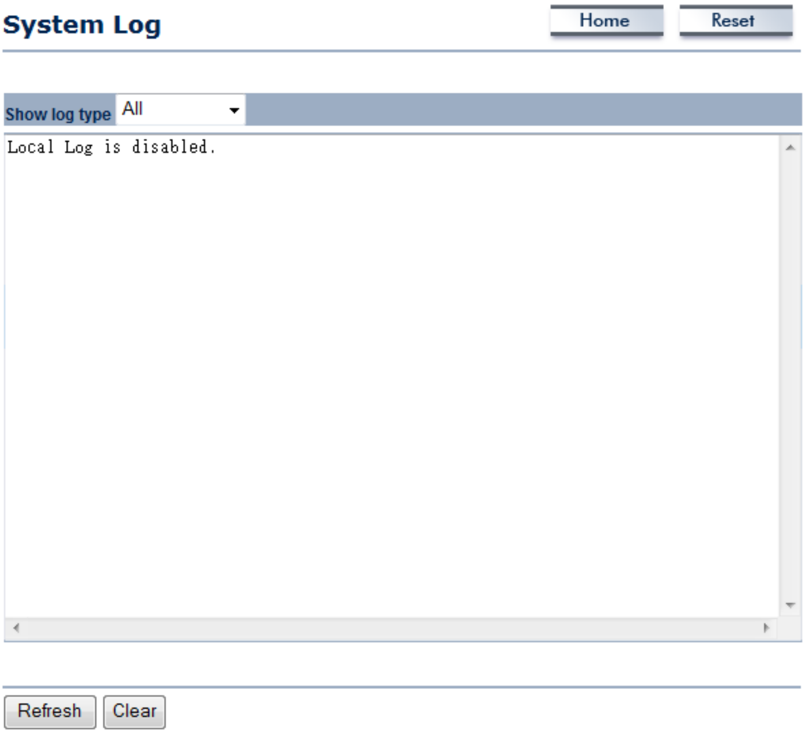


Connection Status

Network Type	Client Bridge
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

5.2.3 System Log

- The device automatically logs (records) 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.

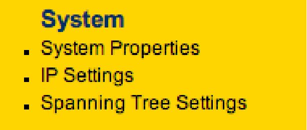


System Log

Show log type: All

```
Local Log is disabled.
```

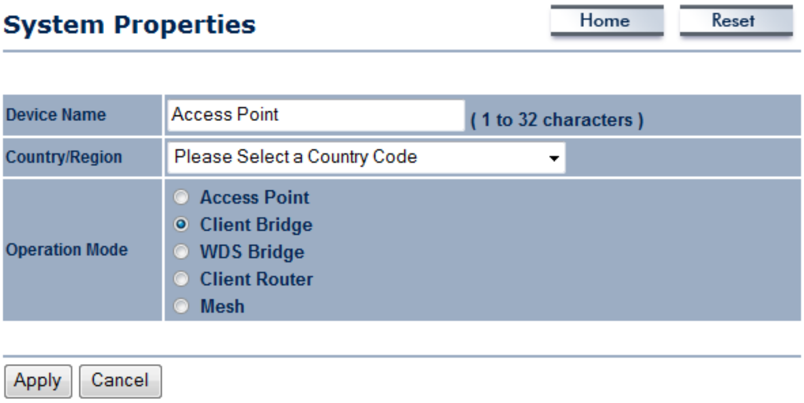
5.3 System



- Under the **System** section of the left menu, you will see the following options: **System Properties, IP Settings**, and **Spanning Tree Settings**. Each option is described in detail below.

5.3.1 System Properties

- This page allows you to switch the Operating Mode of the device, as well as specify a name and select the operating region.



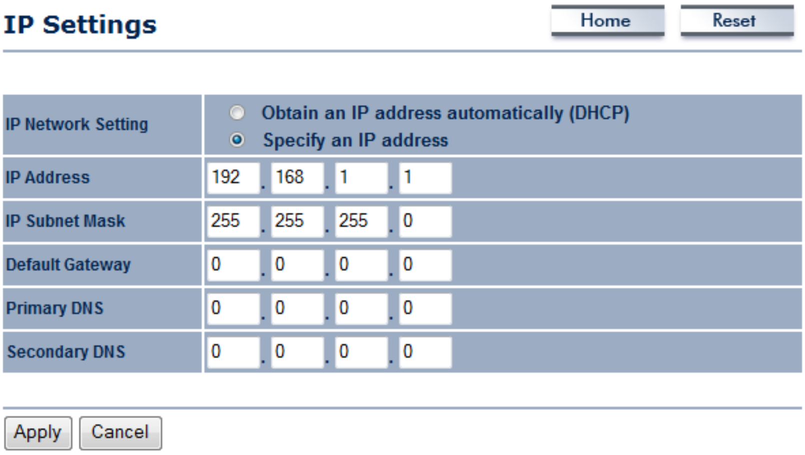
System Properties

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	○ Access Point ● Client Bridge ○ WDS Bridge ○ Client Router ○ Mesh

- **Device Name**: Specify a name for the device (this is not the SSID),
- **Country/Region**: Select a country from the drop-down list.
- **Operating Mode**: Select an Operating Mode. Configuration for each Operating Mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

5.3.2 IP Settings

- This page allows you to configure the device with a static IP address or a DHCP client.

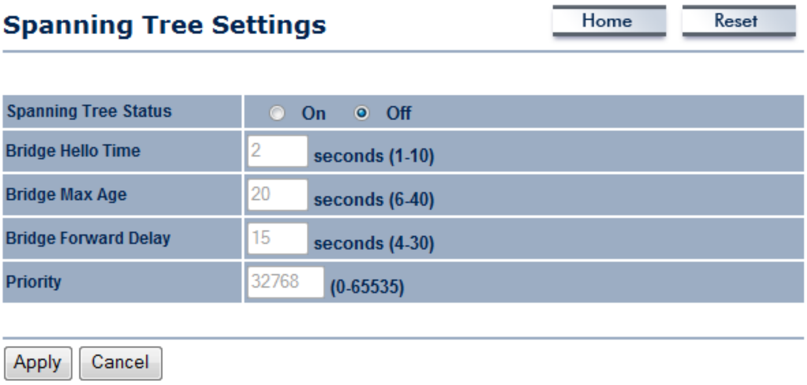


IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **IP Network Setting**: Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address**: Specify an IP address
- **IP Subnet Mask**: Specify the subnet mask for the IP address
- **Default Gateway**: Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

5.3.3 Spanning Tree Settings

- Click on the **Spanning Tree** link under the **System** 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	○ On ● Off
Bridge Hello Time	2 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	15 seconds (4-30)
Priority	32768 (0-65535)

- **Spanning Tree Status**: Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time**: Specify the Bridge Hello Time in seconds.
- **Bridge Max Age**: Specify the Bridge Max Age in seconds.
- **Bridge Forward Delay**: Specify the Bridge Forward Delay in seconds.
- **Priority**: Specify the Priority number.
- Click on the **Apply** button to save the changes.

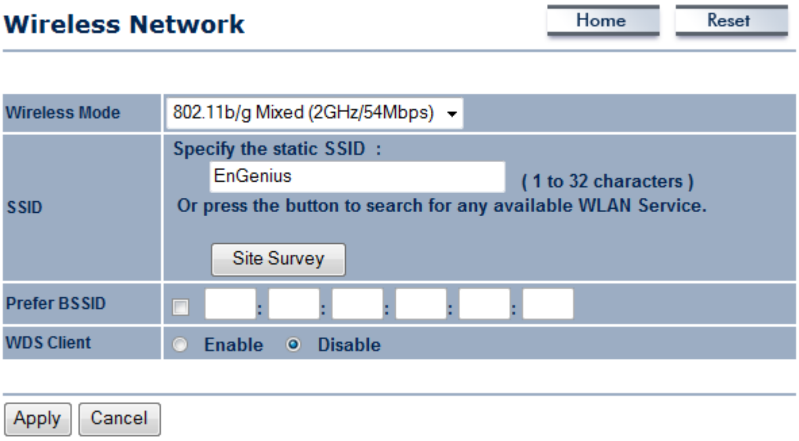
5.4 Wireless

Wireless
- Wireless Network
- Wireless Security
- Wireless Advanced Settings

- The **Wireless** section of the left menu has the following options: **Wireless Network, Wireless Security,** and **Wireless Advanced Settings**. Each option is described below.

5.4.1 Wireless Network

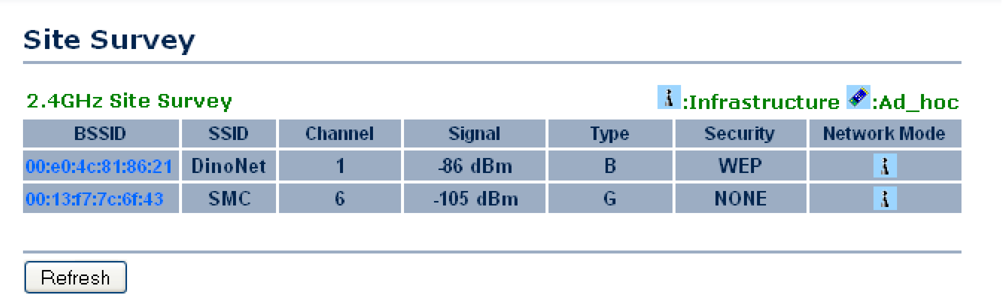
- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.



Wireless Network

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Prefer BSSID	□ __ : __ : __ : __ : __ : __
WDS Client	○ Enable ● Disable

- **Wireless Mode**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, **B/G-mixed or Super-G**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **SSID**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey**: Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.



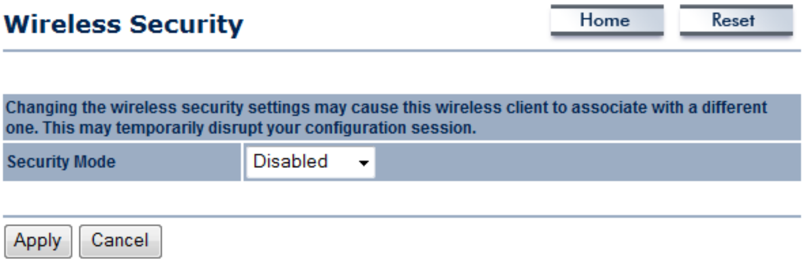
Site Survey

2.4GHz Site Survey ℹ:Infrastructure ✎:Ad_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	ℹ
00:13:f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	ℹ

5.4.2 Wireless Security

- You can change the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.



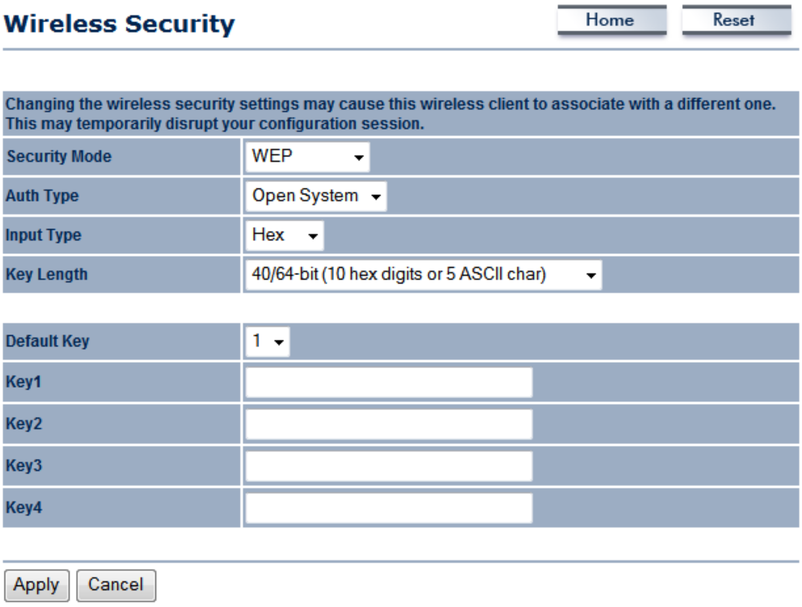
Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode: Disabled

Wireless Security : WEP

- **Security Mode**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.



Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

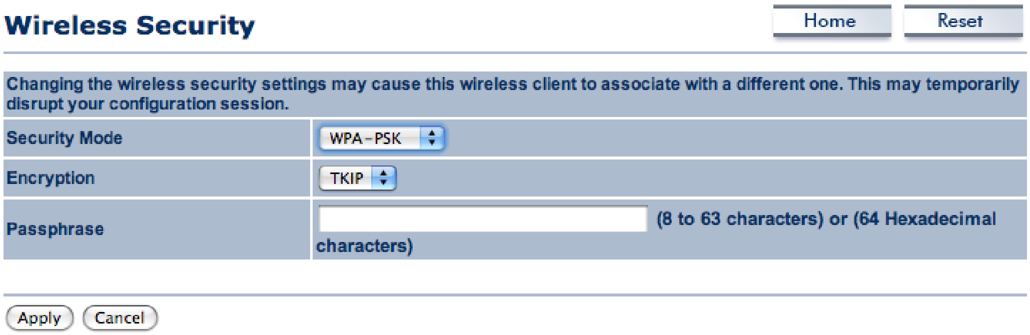
Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)

Default Key	1
Key1	
Key2	
Key3	
Key4	

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. 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 Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point 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. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters and 152-bit keys require 32 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and 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 1-4**: You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

Wireless Security : WPA-PSK

- **Security Mode**: Select **WPA-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.



Wireless Security

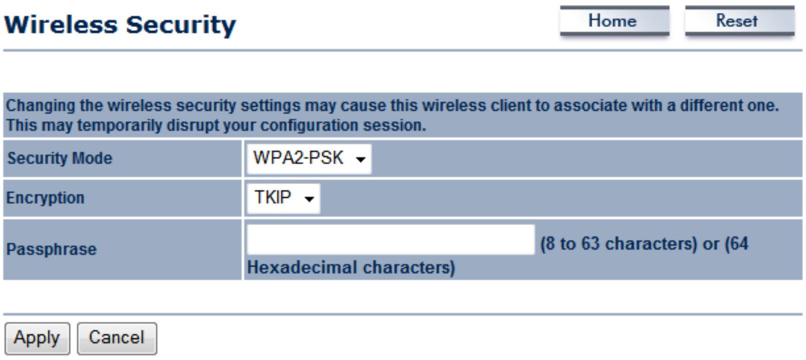
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)

- **Encryption**: Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with. AES is an even more advanced method of encryption which offers the highest level of WPA/WPA2 security.
- **Passphrase**: Specify a passphrase that is shared amongst the Access Points and clients.
  Click on the **Apply** button to save the changes.

Wireless Security : WPA2-PSK

- **Security Mode**: Select **WPA2-PSK** from the drop-down list if your wireless network uses WPA2 pre-shared key.



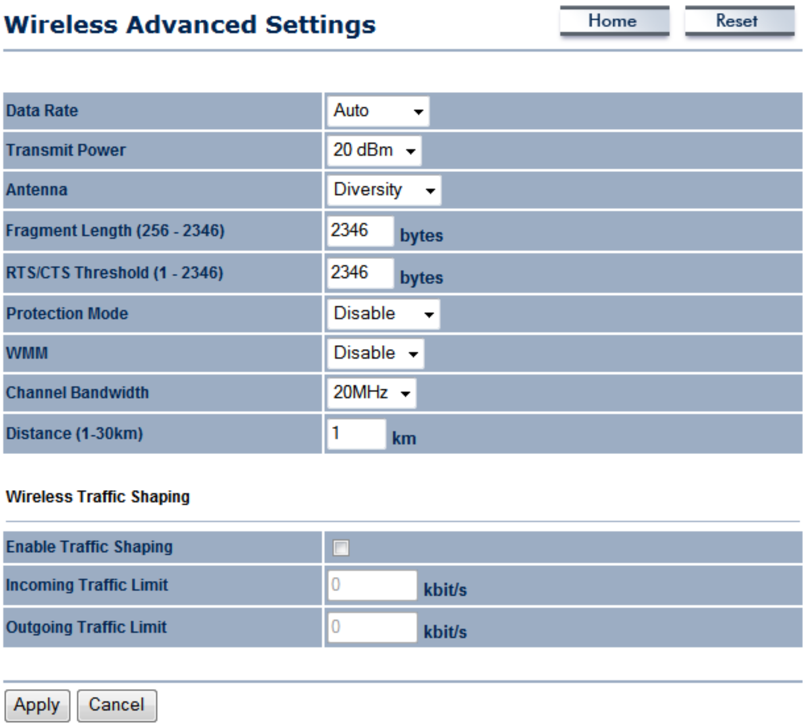
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)

- **Encryption**: Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with. AES is an even more advanced method of encryption which offers the highest level of WPA/WPA2 security.
- **Passphrase**: Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

5.4.3 Wireless Advanced Settings

- On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.



Wireless Advanced Settings

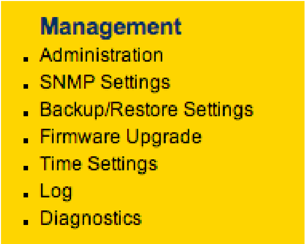
Data Rate	Auto
Transmit Power	20 dBm
Antenna	Diversity
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

Wireless Traffic Shaping

Enable Traffic Shaping	☐
Incoming Traffic Limit	0 kbit/s
Outgoing Traffic Limit	0 kbit/s

- **Data Rate**: If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Antenna**: You can select the antenna polarization to Diversity, Horizontal or Vertical.
- **Fragment**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode**: If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **Distance (1-30km)**: Specify a distance between 1 and 30Km.
- **Wireless Traffic Shaping:** Specify the maximum bandwidth allocated to Incoming and Outgoing traffic.
- Click on the **Apply** button to save the changes.

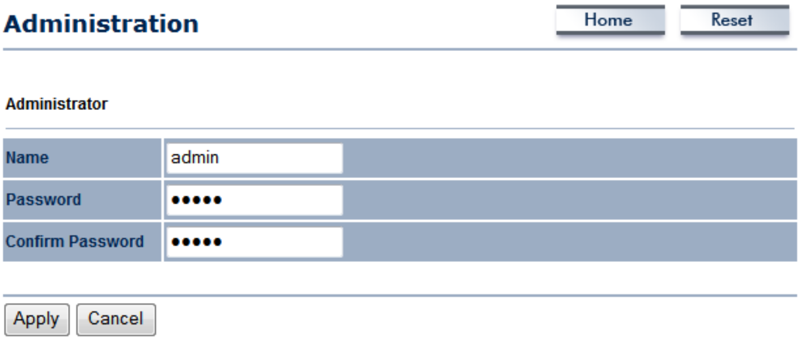
5.5 Management



- The following options are under the Management section of the left menu: **Administration, SNMP Settings, Backup/Restore Settings, Firmware Upgrade, Time Settings, Log** and **Diagnostics**. Each option is described below.

5.5.1 Administration

- This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



Administration

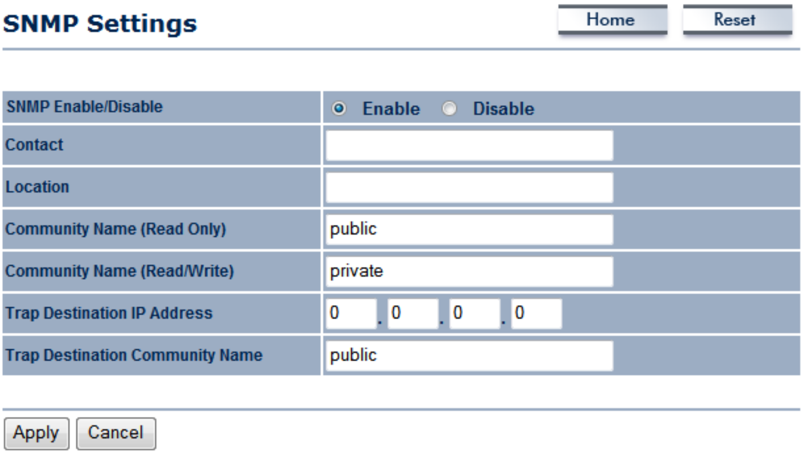
Administrator

Name	admin
Password	●●●●●
Confirm Password	●●●●●

- **Name**: Specify a user name into the first field.
- **Password**: Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

5.5.2 SNMP Settings

- This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.



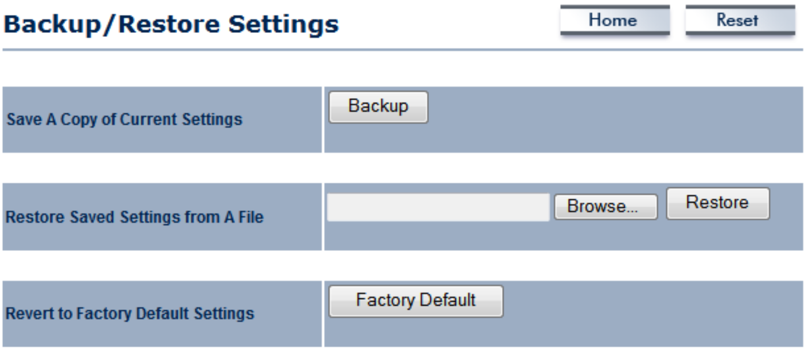
SNMP Settings

SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

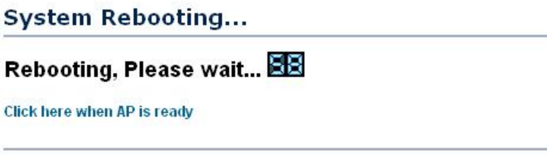
- **SNMP Enable/Disable**: Choose to **enable** or **disable** the SNMP feature.
- **Contact**: Specify the contact details of the device.
- **Location**: Specify the location of the device.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap**: Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name**: Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

5.5.3 Backup/Restore settings, Reset to factory default settings

- This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.


Backup/Restore Settings
Home
Reset
Save A Copy of Current Settings
Backup
Restore Saved Settings from A File
Browse...
Restore
Revert to Factory Default Settings
Factory Default

- **Save a copy of the current settings**: Click on the Backup button to save the current configuration.
- **Restore saved settings from a file**: Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings**: Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: **192.168.1.1**

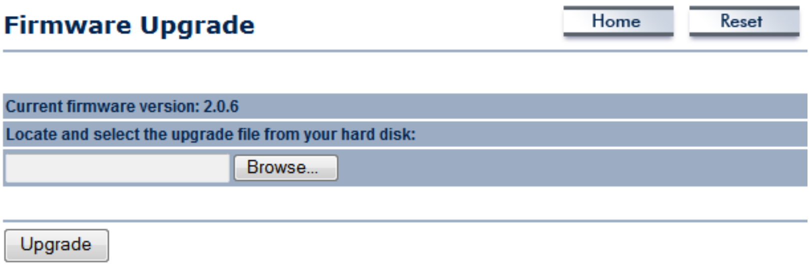

System Rebooting...

Rebooting, Please wait... 88

Click here when AP is ready

5.5.4 Firmware Upgrade

- This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



Firmware Upgrade

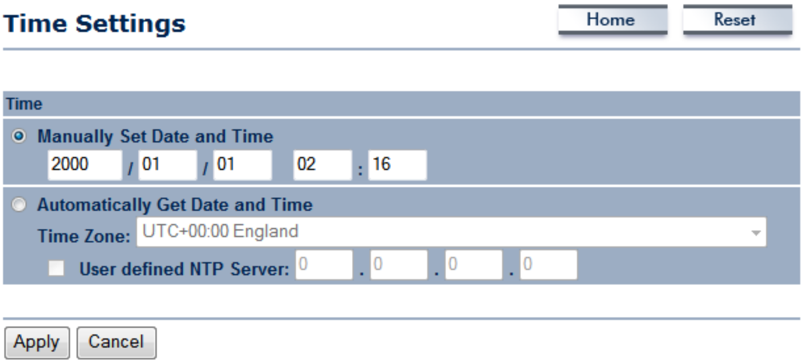
Current firmware version: 2.0.6

Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

5.5.5 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.



Time

● Manually Set Date and Time: 2000 / 01 / 01 02 : 16

○ Automatically Get Date and Time

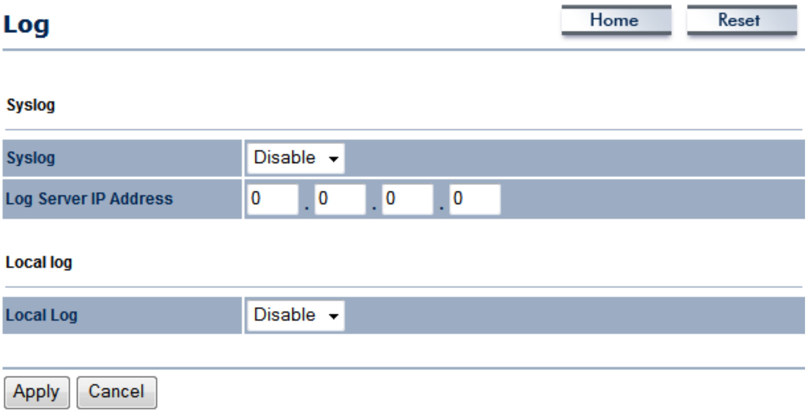
Time Zone: UTC+00:00 England

□ User defined NTP Server: 0 . 0 . 0 . 0

- **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 on the **Apply** button to save the changes.

5.5.6 Log

- Click on the **Log** link under the **Management** menu. The **Log** 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

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

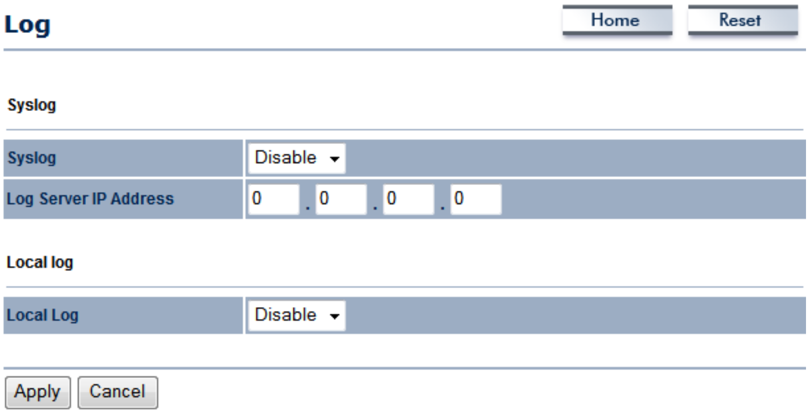
Local log

Local Log	Disable

- **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 on the **Apply** button to save the changes.

5.5.7 Diagnostics

- Click on the **Diagnostics** link under the **Management** menu. In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



Log

Syslog

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

Local log

Local Log	Disable

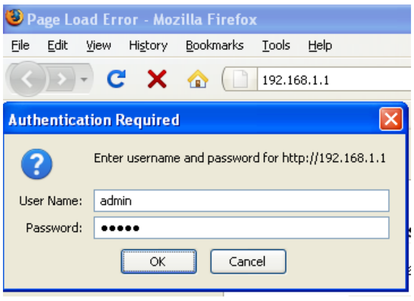
- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click Start Ping.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

6 WDS Bridge Operating Mode

6.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:

1. **Status**: Displays the overall status, WDS link status and system log.
2. **System**: This menu includes the system properties, IP and Spanning Tree settings.
3. **Wireless**: This menu includes network setting, WDS link setting, WDS security and advanced setting.
4. **Management**: This menu includes the admin setup, SNMP, firmware upgrade, time setting, diagnostics and save/restore backup.


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1

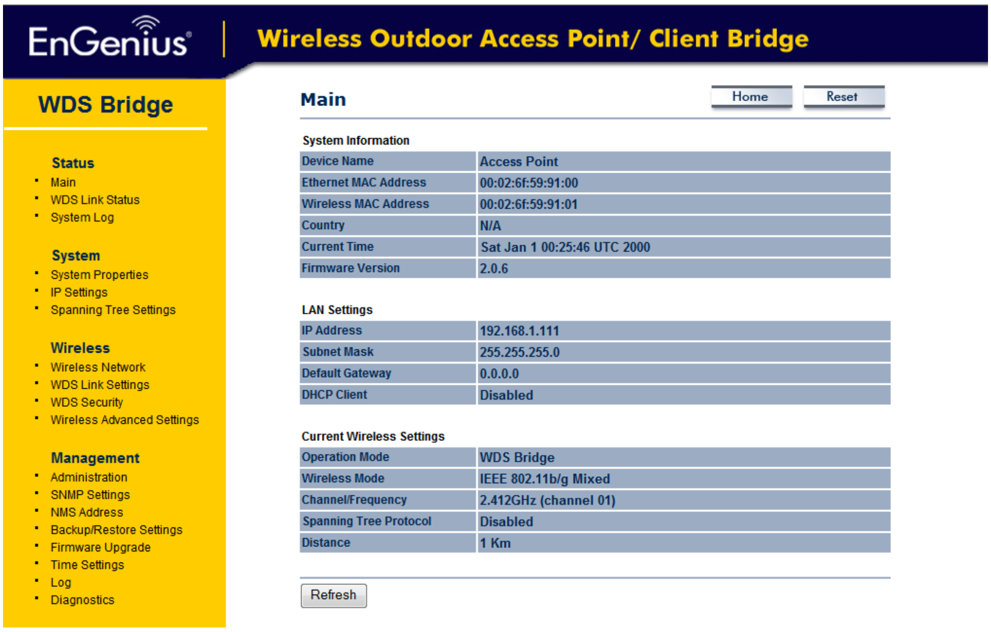
Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: •••••

OK Cancel



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:25:46 UTC 2000
Firmware Version	2.0.6

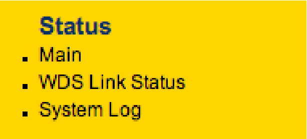
LAN Settings

IP Address	192.168.1.111
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	WDS Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Spanning Tree Protocol	Disabled
Distance	1 Km

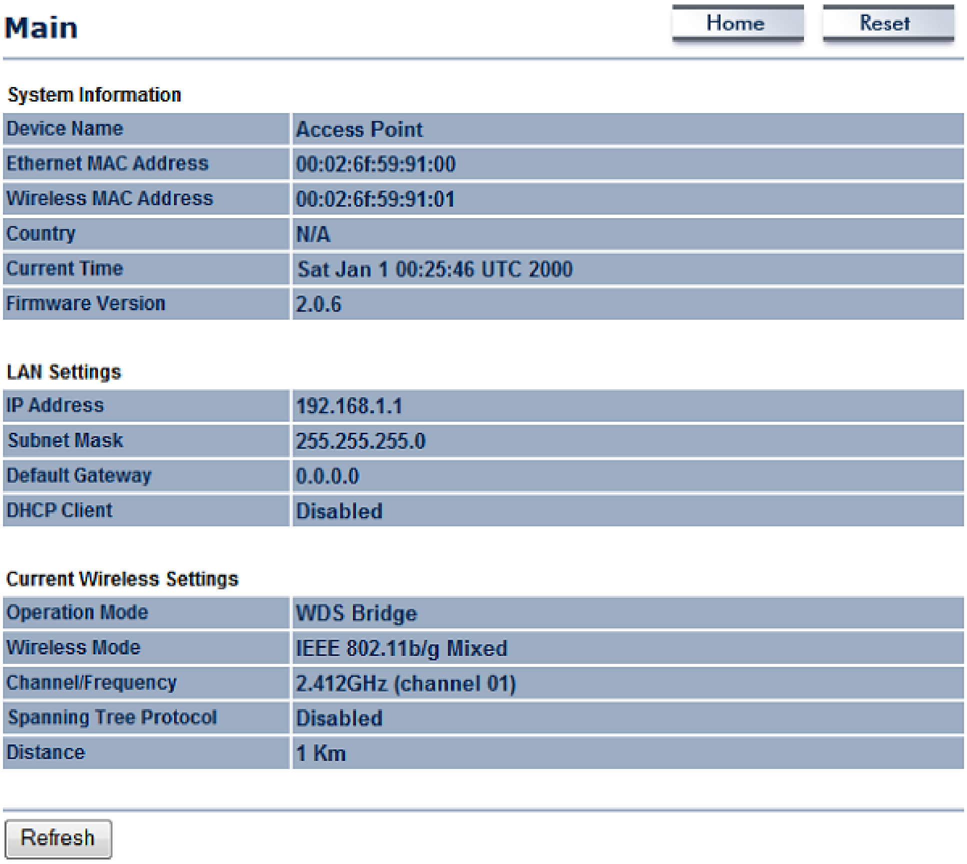
6.2 Status



- There are three options under the **Status** section of the left menu **Main, WDS Link Status**, and **System Log**. Each option is described in detail below.

6.2.1 Main

- The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, Ethernet MAC Address, Wireless MAC Address, Country, Current Time and Firmware are displayed in the 'System Information' section. IP address, Subnet Mask, Default Gateway and DHCP Client are displayed in the 'LAN Settings' section. In the 'Current Wireless Settings' section, the Operation Mode, Wireless Mode, Channel/Frequency, Spanning Tree Protocol and Distance are displayed.



System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:25:46 UTC 2000
Firmware Version	2.0.6

LAN Settings

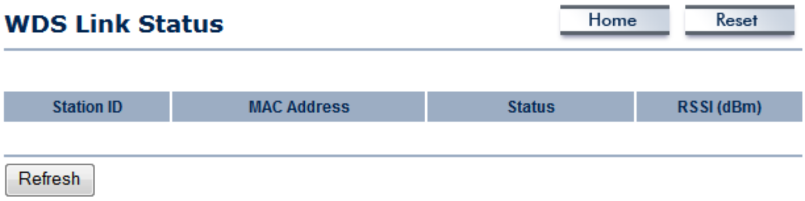
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	WDS Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Spanning Tree Protocol	Disabled
Distance	1 Km

6.2.2 WDS Link Status

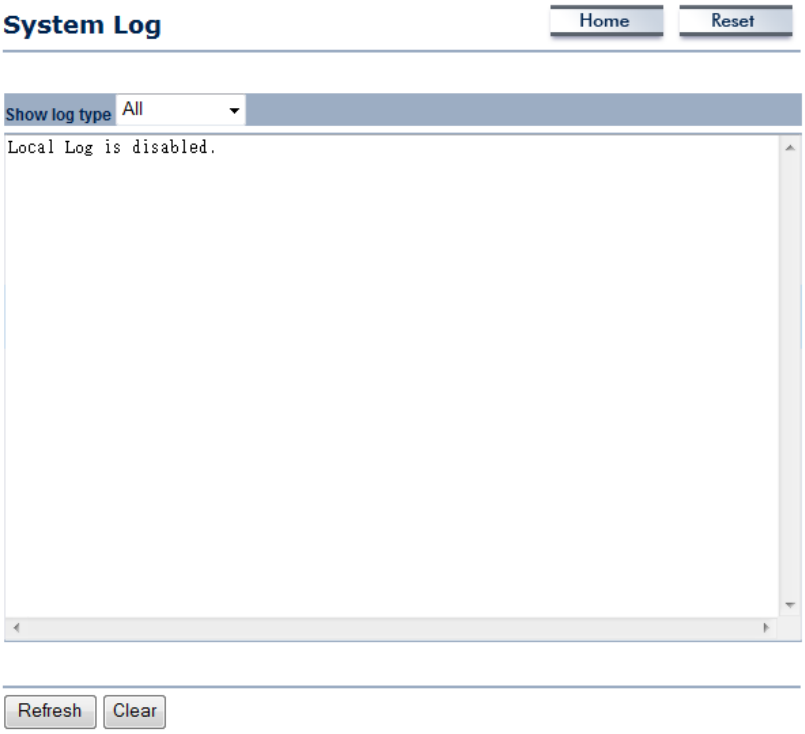
- This page displays the current status of the WDS Link, including Station ID, MAC address, Status, RSSI (Received Signal Strength Indicator).



Station ID	MAC Address	Status	RSSI (dBm)

6.2.3 System Log

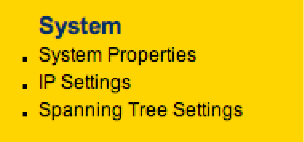
- The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.



Show log type: All

```
Local Log is disabled.
```

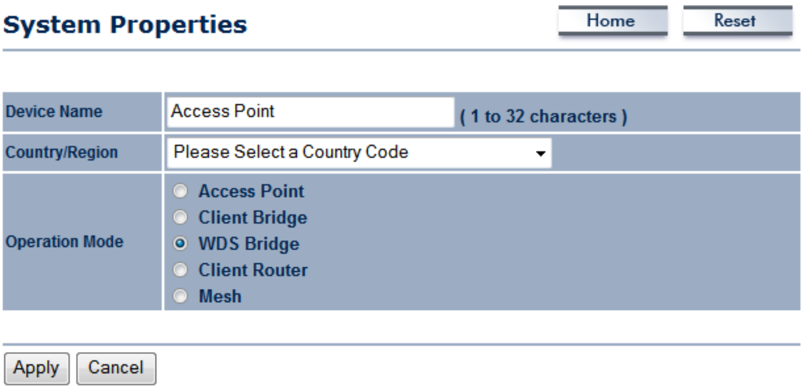
6.3 System



- Under the **System** section of the left menu, you will see the following options: **System Properties, IP Settings** and **Spanning Tree Settings**.

6.3.1 System Properties

- This page allows you to switch the Operating Mode of the device, as well as specify a name and select the operating region.



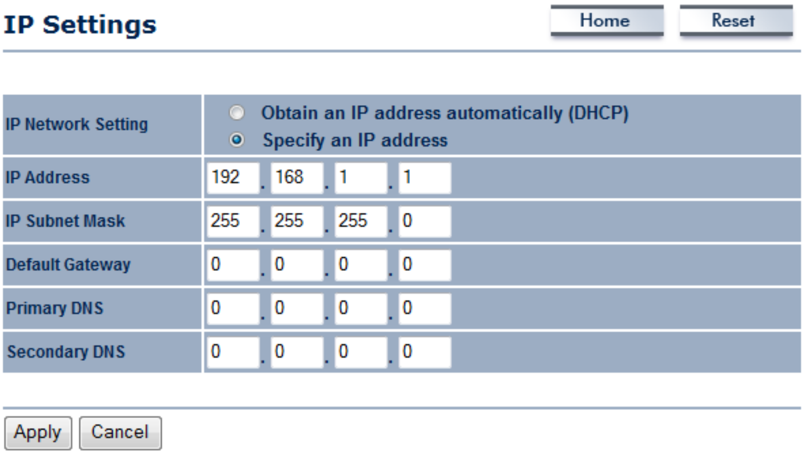
System Properties

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	○ Access Point ○ Client Bridge ● WDS Bridge ○ Client Router ○ Mesh

- **Device Name**: Specify a name for the device (this is not the SSID),
- **Country/Region**: Select a country from the drop-down list.
- **Operating Mode**: Select an Operating Mode. Configuration for each Operating Mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

6.3.2 IP Settings

This page allows you to configure the device with a static IP address or a DHCP client.



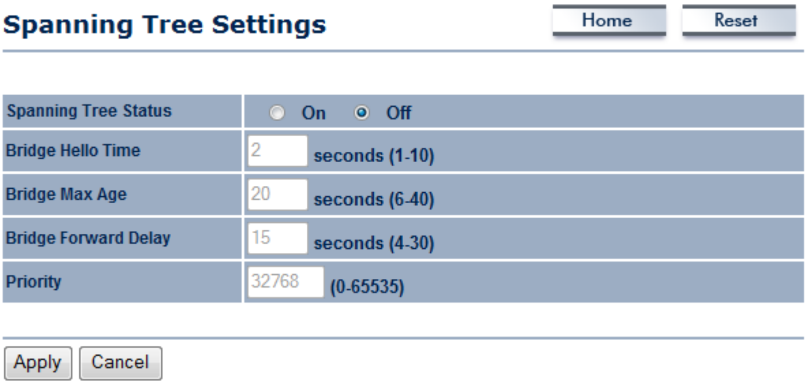
IP Settings

IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **IP Network Setting**: Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address**: Specify an IP address
- **IP Subnet Mask**: Specify the subnet mask for the IP address
- **Default Gateway**: Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

6.3.3 Spanning Tree Settings

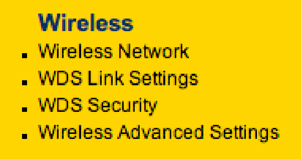
Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.



Spanning Tree Status	○ On ● Off
Bridge Hello Time	2 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	15 seconds (4-30)
Priority	32768 (0-65535)

- **Spanning Tree Status**: Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time**: Specify the Bridge Hello Time in seconds.
- **Bridge Max Age**: Specify the Bridge Max Age in seconds.
- **Bridge Forward Delay**: Specify the Bridge Forward Delay in seconds.
- **Priority**: Specify the Priority number.
- Click on the **Apply** button to save the changes.

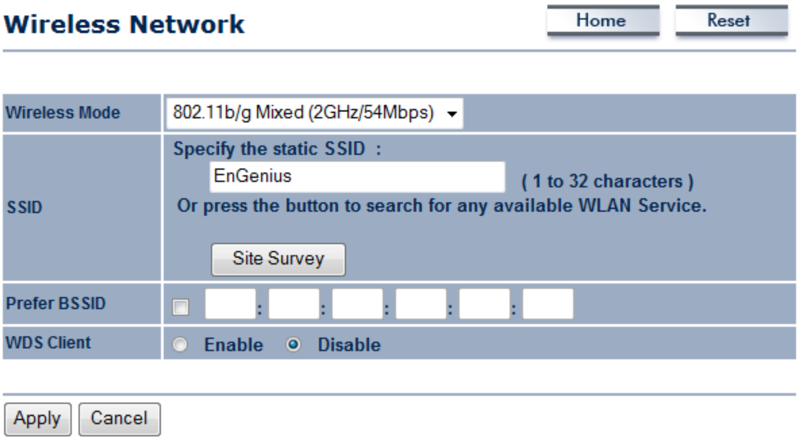
6.4 Wireless



- The **Wireless** section of the left menu has the following options: **Wireless Network, WDS Link Settings, WDS Security** and **Wireless Advanced Settings**. Each section is described in detail below.

6.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

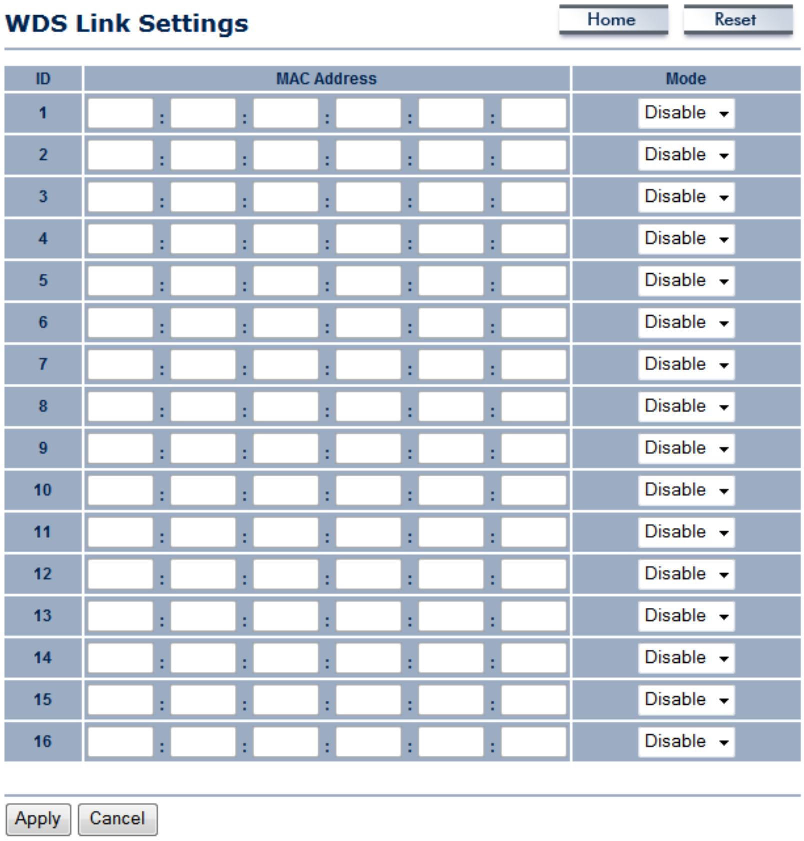


Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service.
Prefer BSSID	□ : : : : :
WDS Client	○ Enable ● Disable

- **Wireless Mode**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G, B/G-mixed or Super-G**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **Channel/Frequency**: Select a channel from the drop-down list. The channels available are based on the country's regulation.

6.4.2 WDS Link Settings

- This page allows you to setting your WDS device link up to 16 units.

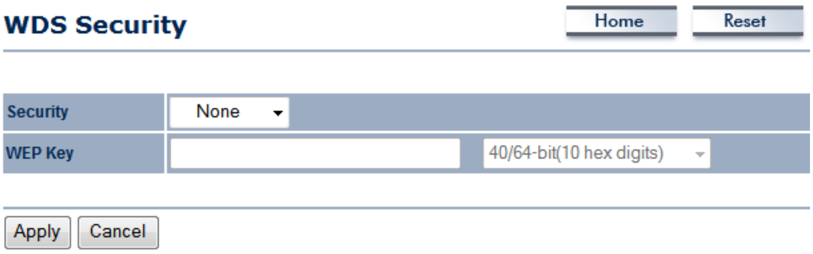


WDS Link Settings

ID	MAC Address	Mode
1	: : : : :	Disable
2	: : : : :	Disable
3	: : : : :	Disable
4	: : : : :	Disable
5	: : : : :	Disable
6	: : : : :	Disable
7	: : : : :	Disable
8	: : : : :	Disable
9	: : : : :	Disable
10	: : : : :	Disable
11	: : : : :	Disable
12	: : : : :	Disable
13	: : : : :	Disable
14	: : : : :	Disable
15	: : : : :	Disable
16	: : : : :	Disable

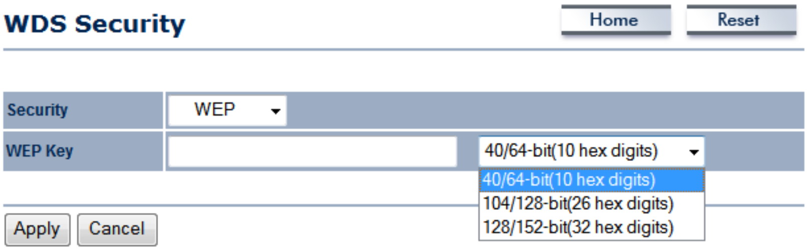
- **MAC Address**: you can input the MAC address of WDS device, which you want to link.
- **Mode**: Enable to connect, and Disable to disconnect.
- Click on the **Apply** button to save the changes.

6.4.3 WDS Security


WDS Security

Security	None	
WEP Key		40/64-bit(10 hex digits)

- **Security Mode**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

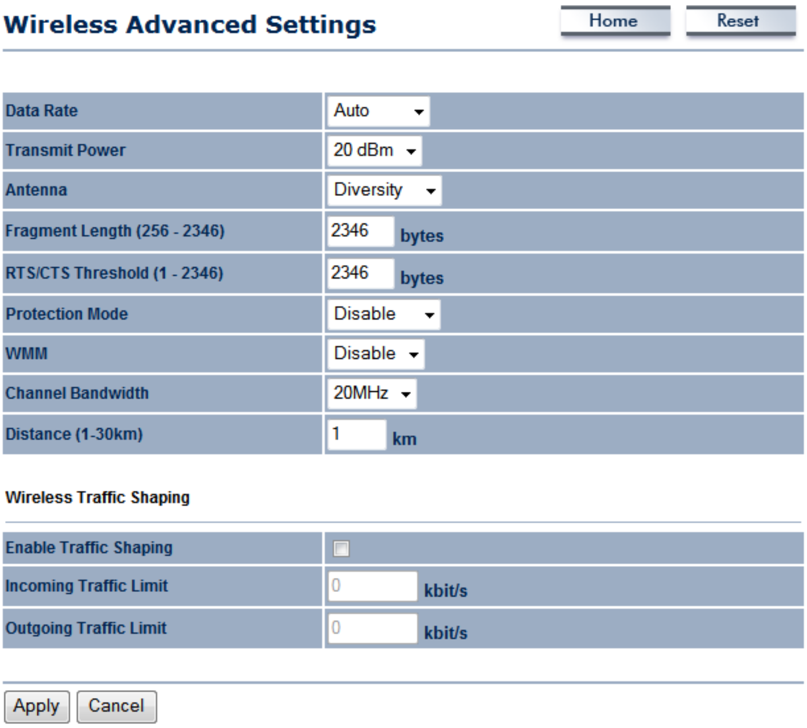

WDS Security

Security	WEP	
WEP Key		40/64-bit(10 hex digits)

- **WEP Key**: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters and 152-bits keys require 32 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.
- Click on the **Apply** button to save the changes.

6.4.4 Wireless Advanced Settings

On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: Data Rate, Transmit Power, Fragment Length, RTS Threshold, Protection Mode and Distance.



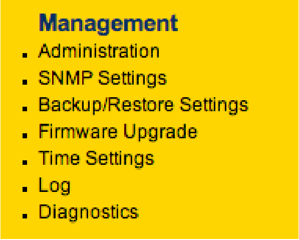
Data Rate	Auto
Transmit Power	20 dBm
Antenna	Diversity
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

Wireless Traffic Shaping

Enable Traffic Shaping	□
Incoming Traffic Limit	0 kbit/s
Outgoing Traffic Limit	0 kbit/s

- **Data Rate**: If you would like to have a fixed data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Antenna**: You can select the antenna polarization to Diversity, Horizontal or Vertical.
- **Fragment Length**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS/CTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode**: If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM**: Enable wireless Quality of Service
- **Distance (1-30km)**: Specify a distance between 1 and 30Km.
- **Wireless Traffic Shaping:** Specify the maximum bandwidth allocated to Incoming and Outgoing traffic.
- Click on the **Apply** button to save the changes.

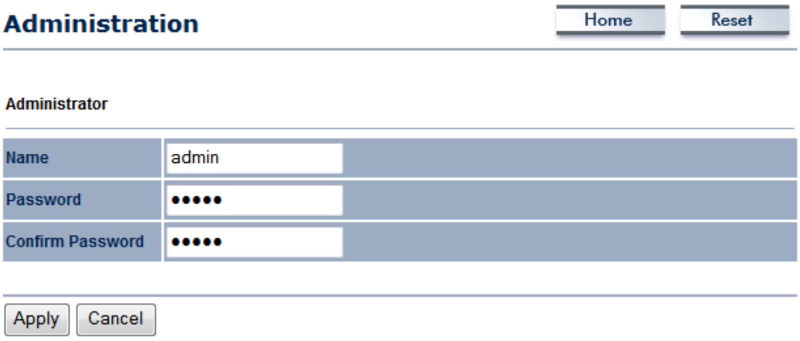
6.5 Management



- The following options are under the **Management** section of the left menu: **Administration, SNMP Settings, Backup/Restore Settings, Firmware Upgrade, Time Settings, Log** and **Diagnostics**. Each option is described below.

6.5.1 Administration

- This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



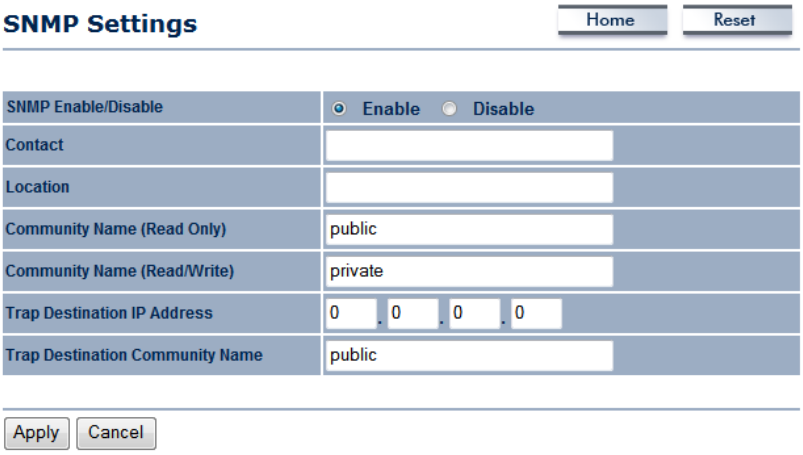
Administrator

Name	admin
Password	•••••
Confirm Password	•••••

- **Name**: Specify a user name into the first field.
- **Password**: Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

6.5.2 SNMP Settings

- This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases. .

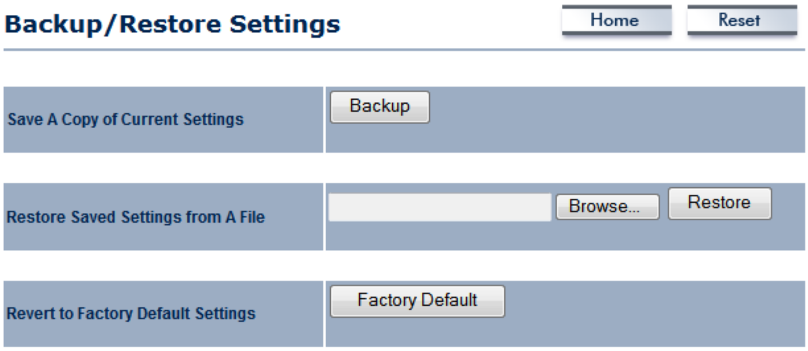


SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

- **SNMP Enable/Disable**: Choose to **enable** or **disable** the SNMP feature.
- **Contact**: Specify the contact details of the device.
- **Location**: Specify the location of the device.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Trap Destination IP Address**: Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name**: Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

6.5.3 Backup/Restore settings, Reset to factory default settings

- This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

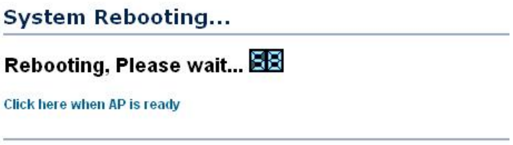

Backup/Restore Settings

Save A Copy of Current Settings

Restore Saved Settings from A File

Revert to Factory Default Settings

- **Save a copy of the current settings**: Click on the Backup button to save the current configuration.
- **Restore saved settings from a file**: Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings**: Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: **192.168.1.1**

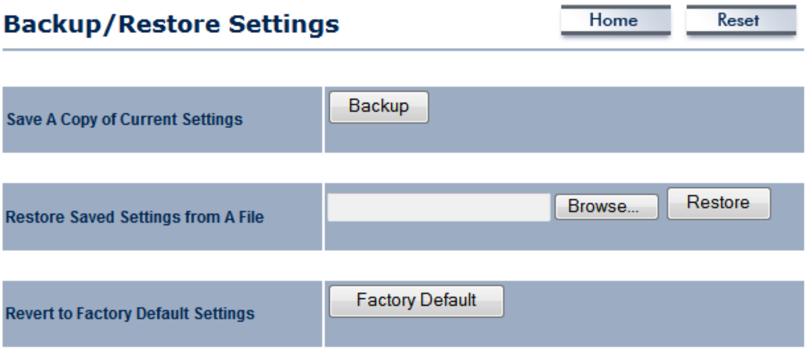

System Rebooting...

Rebooting, Please wait...

Click here when AP is ready

6.5.4 Firmware Upgrade

- This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



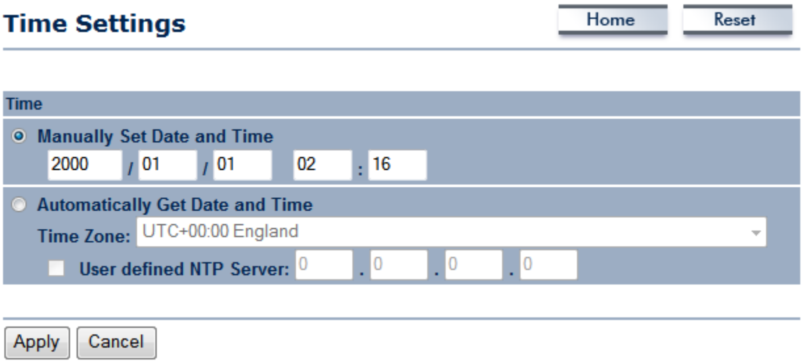
Backup/Restore Settings

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	Browse... Restore
Revert to Factory Default Settings	Factory Default

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

6.5.5 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.



Time Settings

Time

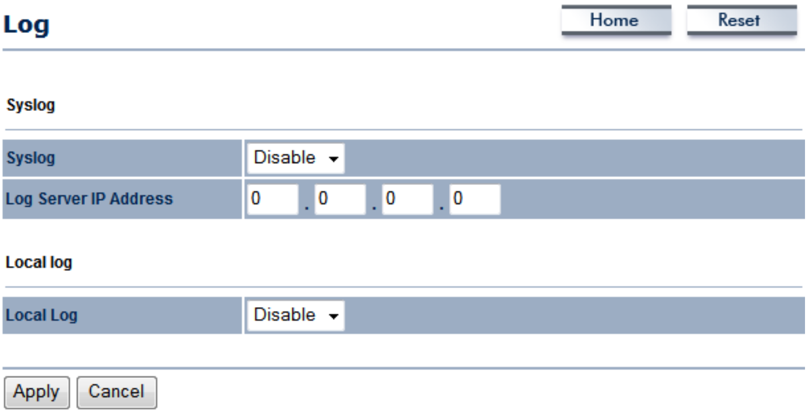
● Manually Set Date and Time
2000 / 01 / 01 02 : 16

○ Automatically Get Date and Time
Time Zone: UTC+00:00 England
□ User defined NTP Server: 0 . 0 . 0 . 0

- **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 on the **Apply** button to save the changes.

6.5.6 Log

- **Log** 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

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

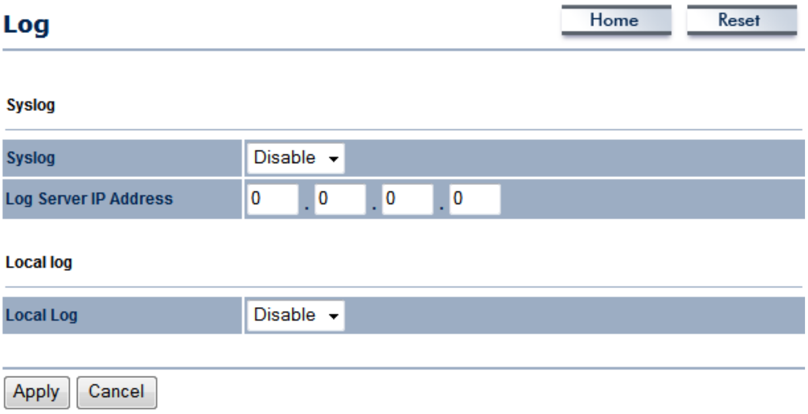
Local log

Local Log	Disable

- **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 on the **Apply** button to save the changes.

6.5.7 Diagnostics

- In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



Syslog

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

Local log

Local Log	Disable

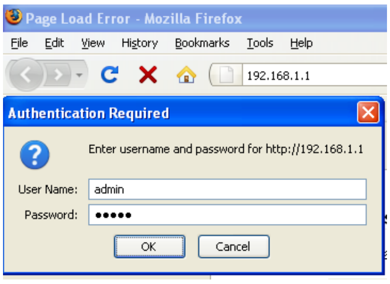
- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click **Start Ping**.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

7 Client Router Operating Mode

7.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:

1. **Status**: Displays the overall status, DHCP client table, connection status and system log.
2. **System**: This menu includes the system properties.
3. **Router**: This includes WAN, LAN, and VPN settings.
4. **Wireless**: This menu includes wireless network, security and advanced settings.
5. **Management**: This menu includes the admin setup, SNMP settings, firmware upgrade, save/restore backup, time setting and diagnostics.

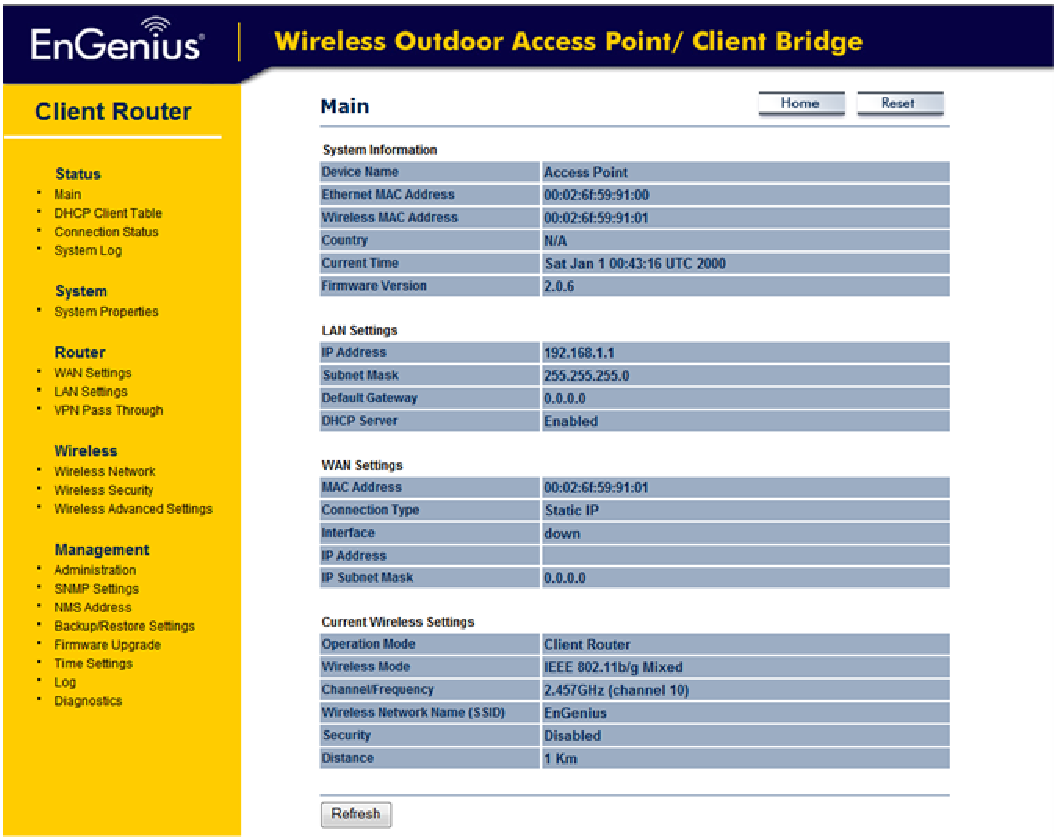


Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: ●●●●●



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:43:16 UTC 2000
Firmware Version	2.0.6

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled

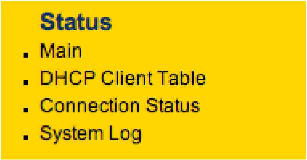
WAN Settings

MAC Address	00:02:6f:59:91:01
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

Current Wireless Settings

Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.457GHz (channel 10)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Distance	1 Km

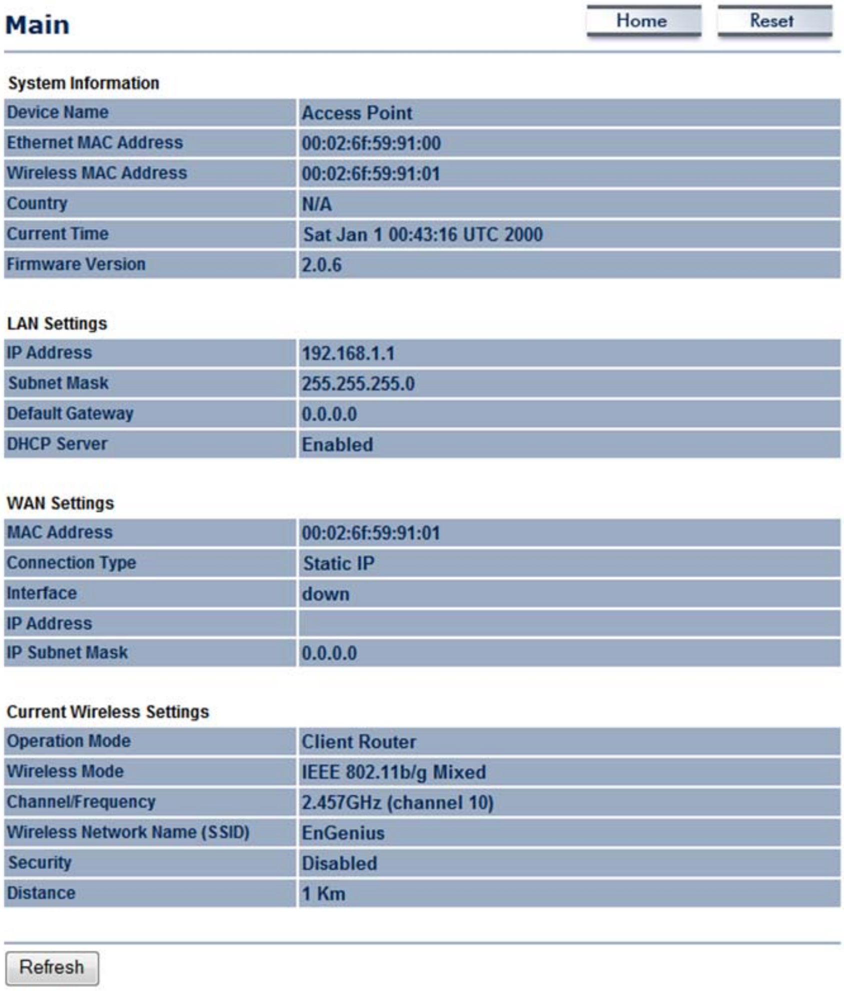
7.2 Status



- Under the **Status** section of the left menu, you will see the following options: **Main, DHCP Client Table, Connection Status** and **System Log**. Each option is described in detail below.

7.2.1 Main

- The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, MAC Address, Country, Current and Firmware Version are displayed in the 'System Information' section. IP Address, Subnet Mask, Default Gateway and DHCP Server condition are displayed in the 'LAN Settings' section. In the 'WAN Settings', MAC Address, Connection Type, Interface and IP Address/Subnet Mask are displayed. The 'Current Wireless Settings' section displays Operation Mode, Wireless Mode, Channel/Frequency, SSID, Security and Distance control.



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:43:16 UTC 2000
Firmware Version	2.0.6

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled

WAN Settings

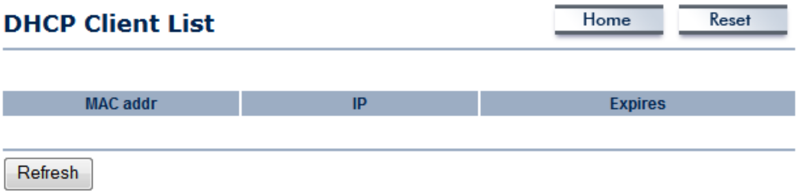
MAC Address	00:02:6f:59:91:01
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

Current Wireless Settings

Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.457GHz (channel 10)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Distance	1 Km

7.2.2 DHCP Client Table

- This page displays the current status of all DHCP clients, including MAC address, IP and Expires information.

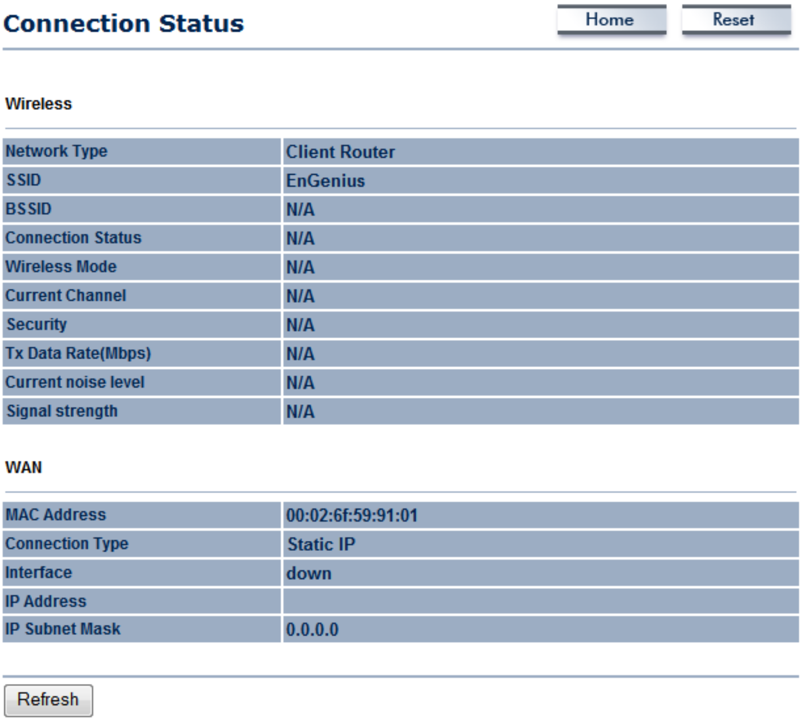


DHCP Client List

MAC addr	IP	Expires

7.2.3 Connection Status

This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.



Connection Status

Wireless

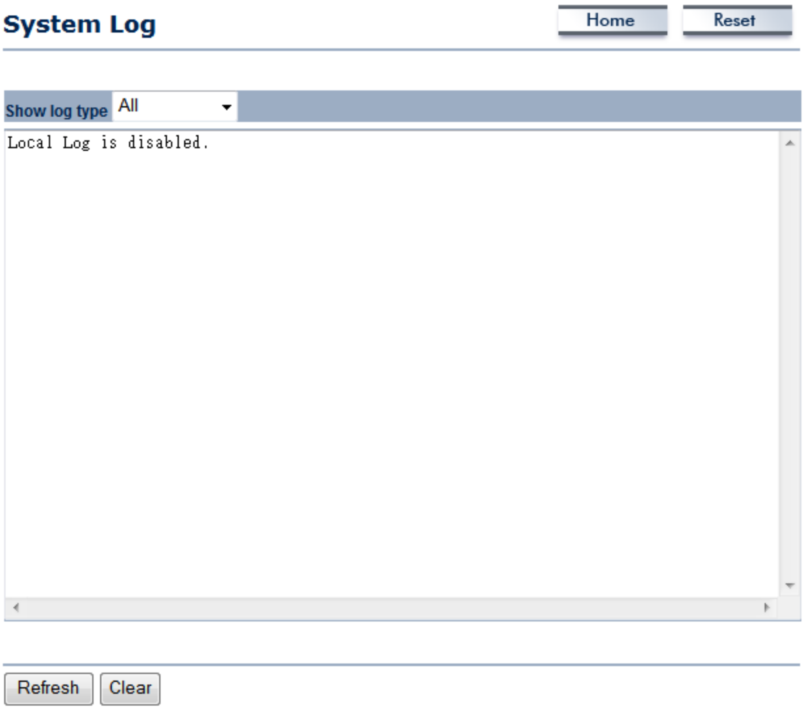
Network Type	Client Router
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

WAN

MAC Address	00:02:6f:59:91:01
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

7.2.4 System Log

The device automatically logs (records) 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.



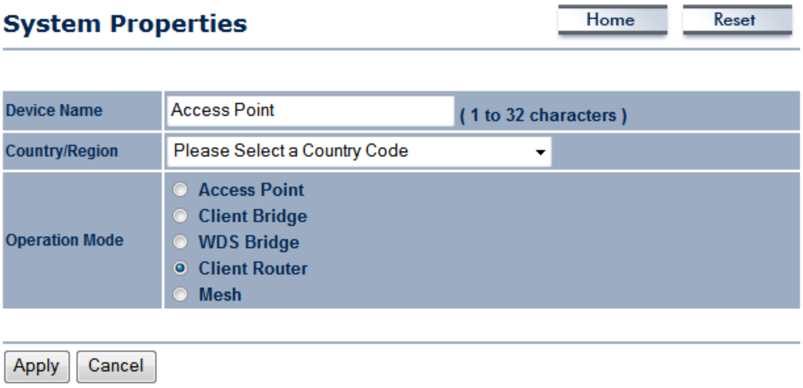
```
Local Log is disabled.
```

7.3 System

- Under the **System** section of the left menu, you will see the following options: **System Properties**, which is described below.

7.3.1 System Properties

- This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

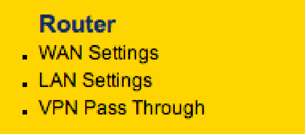


System Properties

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	○ Access Point ○ Client Bridge ○ WDS Bridge ● Client Router ○ Mesh

- **Device Name**: Specify a name for the device (this is not the SSID),
- **Country/Region**: Select a country from the drop-down list.
- **Operating Mode**: Select operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

7.4 Router



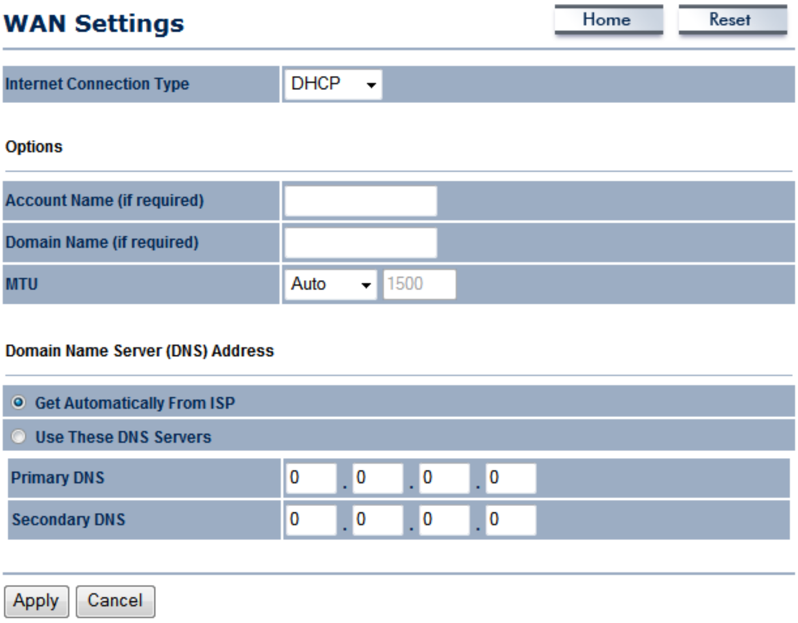
- Under the **Router** section of the left menu, you will see the following options: **WAN Settings, LAN Settings**, and **VPN Pass Through**. Each section is described in detail below.

7.4.1 WAN Settings

- This page allows you to configure the WAN interface as DHCP, Static IP, PPPoE or PPTP.

7.4.1.1 WAN – DHCP

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.



WAN Settings

Internet Connection Type	DHCP

Options

Account Name (if required)	
Domain Name (if required)	
MTU	Auto 1500

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

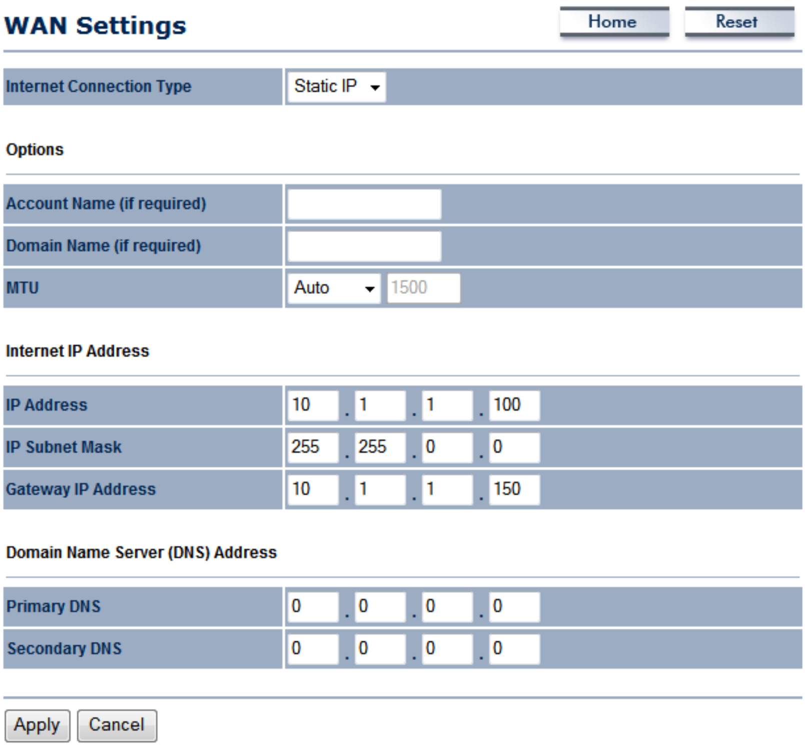
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **Internet Connection Type**: Select the **DHCP** from the drop-down list.
- **Account Name**: Specify an account name if your ISP has provided you with one.
- **Domain Name**: Specify a domain name if the ISP has provided you with one.
- **MTU**: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical value is 1500 bytes for an Ethernet connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

- **Domain Name Service**: Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

7.4.1.2 WAN – Static IP

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address (which does not change as DHCP).



Internet Connection Type	Static IP

Options

Account Name (if required)	
Domain Name (if required)	
MTU	Auto 1500

Internet IP Address

IP Address	10 . 1 . 1 . 100
IP Subnet Mask	255 . 255 . 0 . 0
Gateway IP Address	10 . 1 . 1 . 150

Domain Name Server (DNS) Address

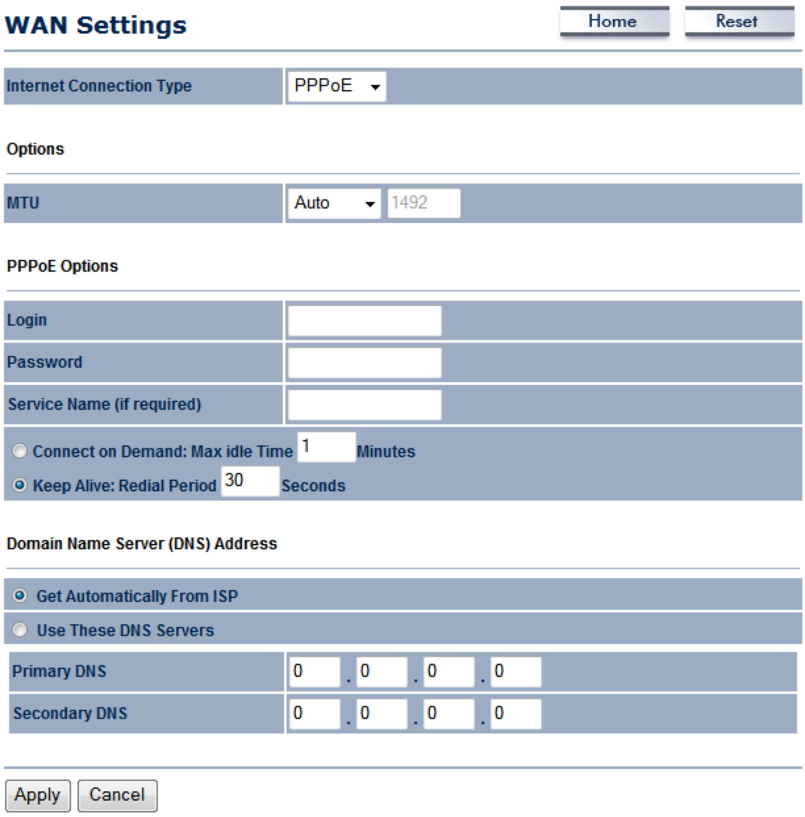
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **Internet Connection Type**: Select the **Static IP** from the drop-down list.
- **Account Name**: Specify an account name if your ISP has provided you with one.
- **Domain Name**: Specify a domain name if the ISP has provided you with one.
- **MTU**: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical value is 1500 bytes for an Ethernet connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.

- **Gateway IP Address:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Domain Name Service**: Specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

7.4.1.3 WAN – PPPoE

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.



WAN Settings

Internet Connection Type	PPPoE

Options

MTU	Auto 1492

PPPoE Options

Login	
Password	
Service Name (if required)	

○ Connect on Demand: Max idle Time 1 Minutes

● Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

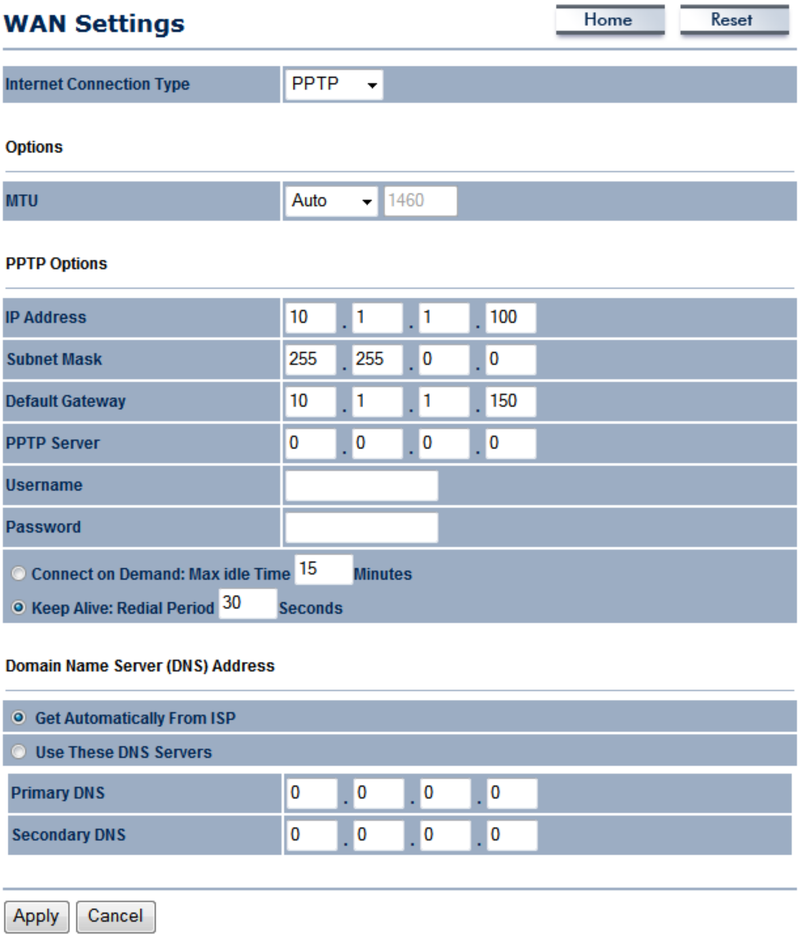
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **Internet Connection Type**: Select **PPPoE** from the drop-down list.
- **MTU**: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **Login**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Service Name**: Specify the name of the ISP.

- **Type**: Select a reconnection type: **Keep Alive** (A connection to the Internet is always maintained), **Connect on Demand**: You have to open up the Web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.
- **Domain Name Service**: Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

7.4.1.4 WAN – PPTP

- The WAN interface can be configured as PPTP. This type of connection is usually used for a DSL service and requires a username and password to connect.



Internet Connection Type	PPTP

Options

MTU	Auto 1460

PPTP Options

IP Address	10 . 1 . 1 . 100
Subnet Mask	255 . 255 . 0 . 0
Default Gateway	10 . 1 . 1 . 150
PPTP Server	0 . 0 . 0 . 0
Username	
Password	

○ Connect on Demand: Max idle Time 15 Minutes
● Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

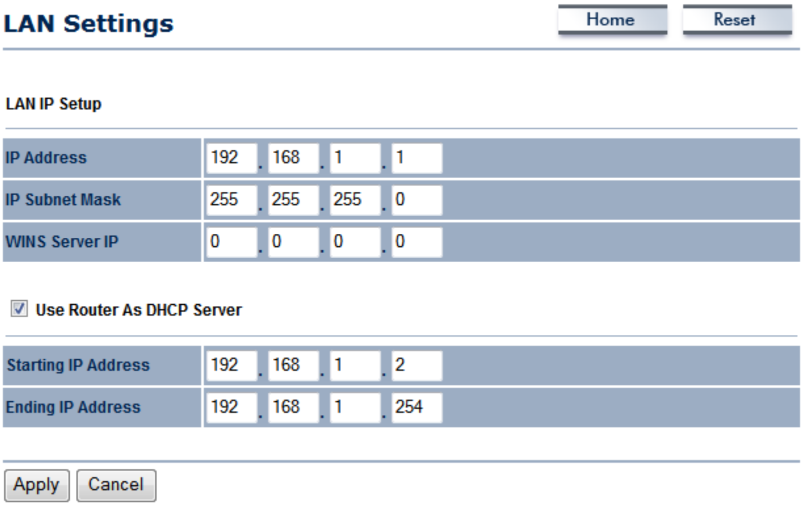
- **Internet Connection Type**: Select **PPPoE** from the drop-down list.
- **MTU**: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger

packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical value is 1500 bytes for an Ethernet connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

- **PPTP Options**: Specify IP address, subnet mask, default gateway and PPTP server.
- **Username**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Type**: Select a reconnection type: **Keep Alive** (A connection to the Internet is always maintained), **Connect on Demand**: You have to open up the Web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.
- **Domain Name Service**: Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

7.4.2 LAN Settings

This page allows you to configure the LAN interface as IP address, IP subnet mask and WINS server IP. When you enable 'Use Router As DHCP Server', specify the IP address from starting to ending.



LAN IP Setup

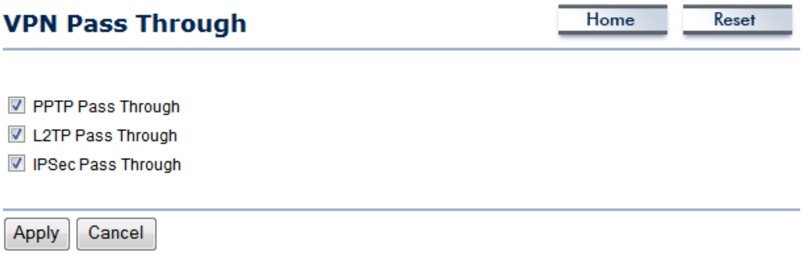
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
WINS Server IP	0 . 0 . 0 . 0

☑ Use Router As DHCP Server

Starting IP Address	192 . 168 . 1 . 2
Ending IP Address	192 . 168 . 1 . 254

7.4.3 VPN Pass Through

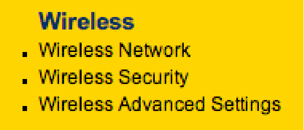
- This page allows you to enable the pass through feature.



☑ PPTP Pass Through
☑ L2TP Pass Through
☑ IPSec Pass Through

- **PPTP Pass Through**: Place a check in this box if you would like to enable this pass through. PPTP is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels"
- **L2TP Pass Through**: Place a check in this box if you would like to enable this pass through. Layer 2 Tunneling Protocol is a transport protocol that enables tunneling through the Internet for the establishment of virtual private networks.
- **IPSec Pass Through**: Place a check in this box if you would like to enable this pass through. IPSec is a VPN protocol used to implement secure exchange of packets at the IP layer.
- Click on the **Apply** button to save the changes.

7.5 Wireless



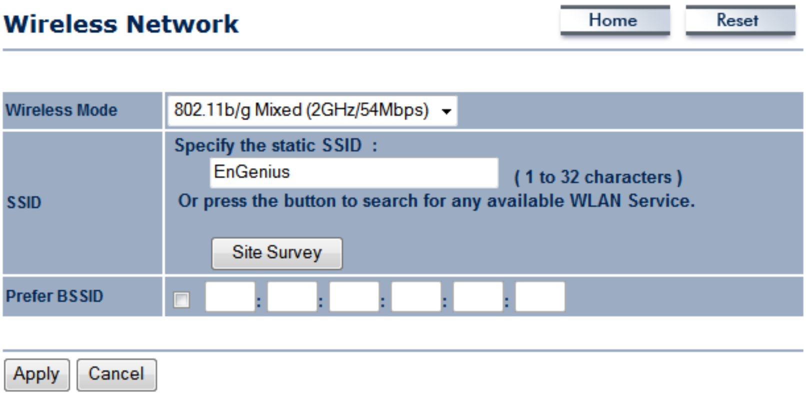
Wireless

- Wireless Network
- Wireless Security
- Wireless Advanced Settings

- Under the **Wireless** section of the left menu, you will see the following options: **Wireless Network, Wireless Security,** and **Wireless Advanced Settings**. Each option is described below.

7.5.1 Wireless Network

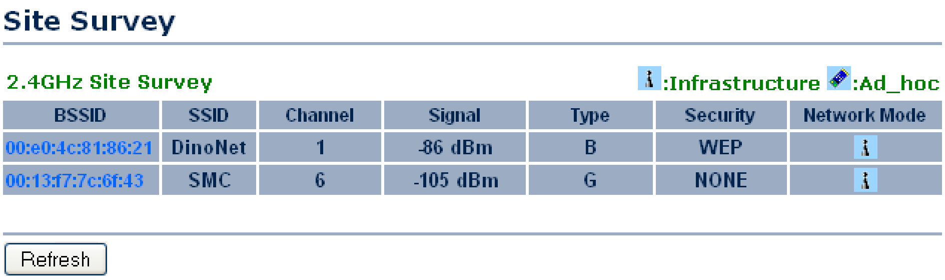
- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.



Wireless Network

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : EnGenius (1 to 32 characters) Or press the button to search for any available WLAN Service. Site Survey
Prefer BSSID	□ __ : __ : __ : __ : __ : __

- **Wireless Mode**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, **B/G-mixed or Super-G**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **SSID**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey**: Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.

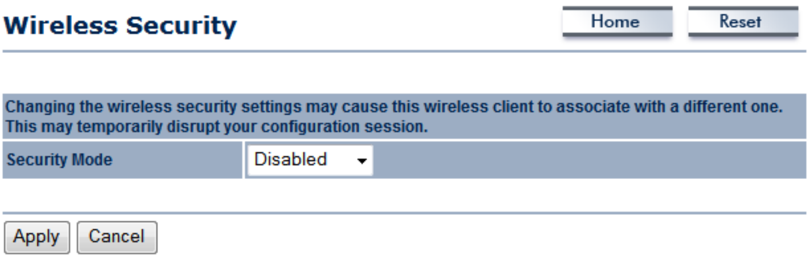


Site Survey

2.4GHz Site Survey ℹ:Infrastructure ✎:Ad_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	ℹ
00:13:f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	ℹ

7.5.2 Wireless Security



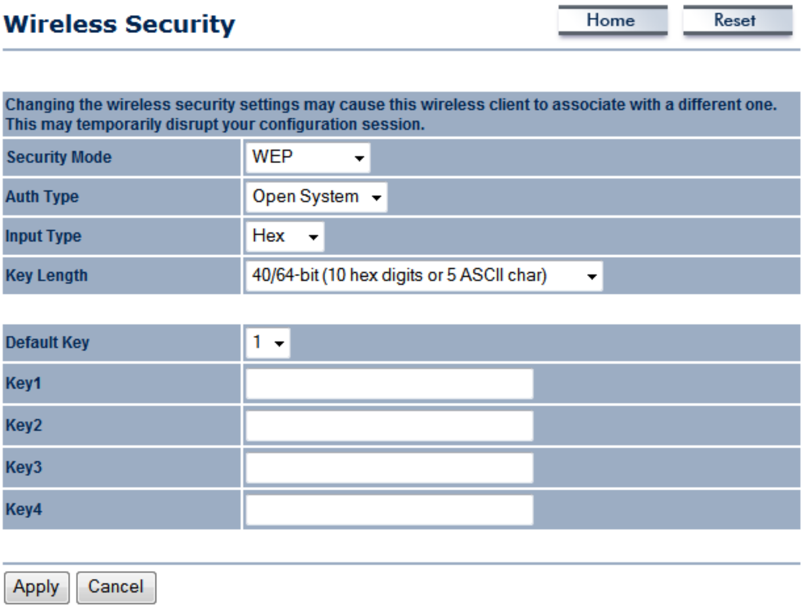
Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode: Disabled

7.5.2.1 Wireless Security : WEP

- **Security Mode**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.



Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

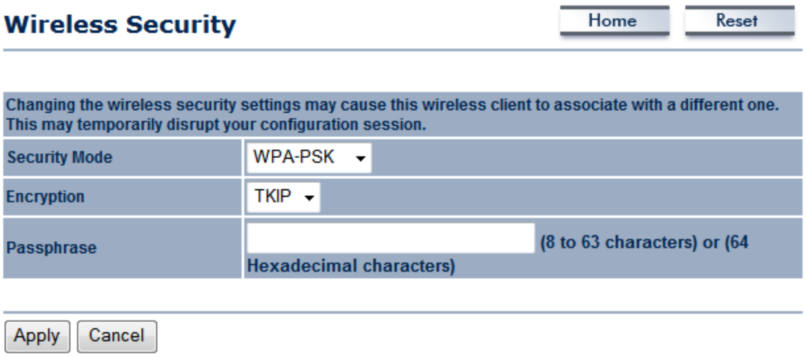
Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. 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 Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point 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. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and 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 1-4**: You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

7.5.2.2 Wireless Security : WPA-PSK, WPA2-PSK,

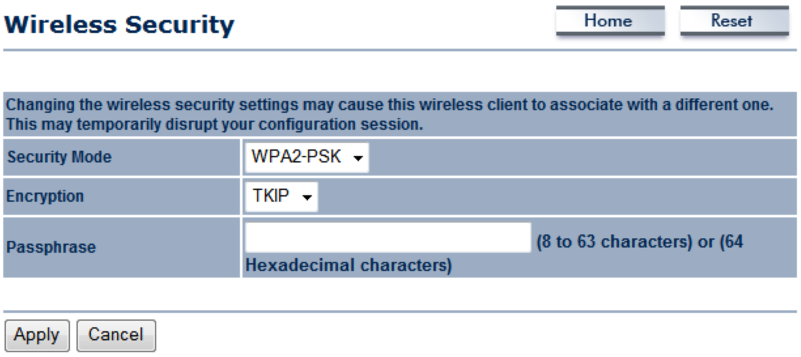
- **Security Mode**: Select **WPA-PSK or WPA2-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.



Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)



Wireless Security

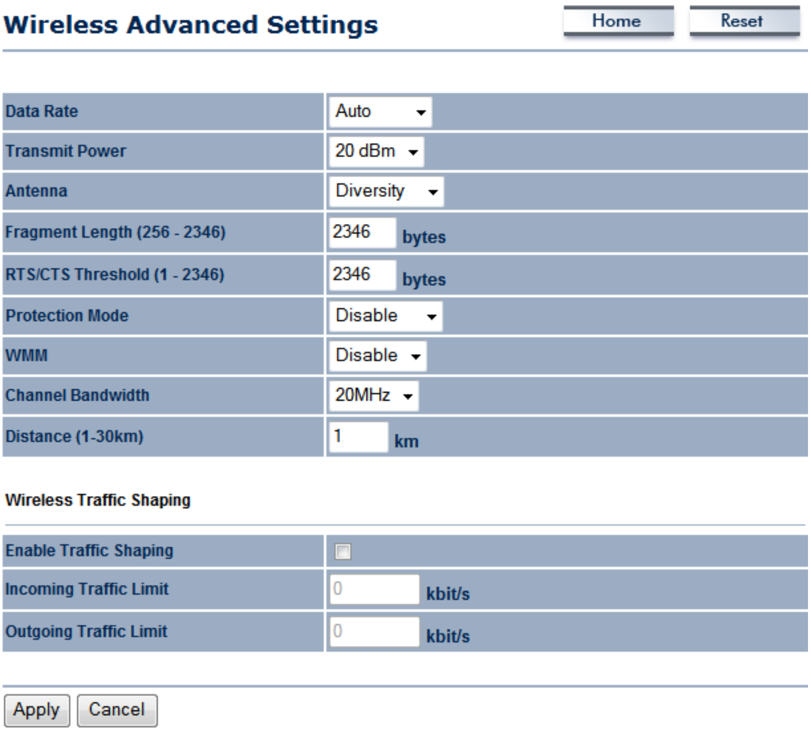
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	TKIP
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)

- **Encryption**: Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **Passphrase**: Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

7.5.3 Wireless Advanced Settings

- On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.



Wireless Advanced Settings

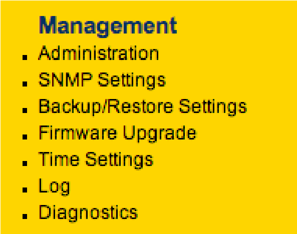
Data Rate	Auto
Transmit Power	20 dBm
Antenna	Diversity
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

Wireless Traffic Shaping

Enable Traffic Shaping	□
Incoming Traffic Limit	0 kbit/s
Outgoing Traffic Limit	0 kbit/s

- **Data Rate**: If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Antenna**: You can select the antenna polarization to Diversity, Horizontal or Vertical.
- **Fragment**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode**: If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM**: Enable wireless Quality of Service
- **Distance (1-30km)**: Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

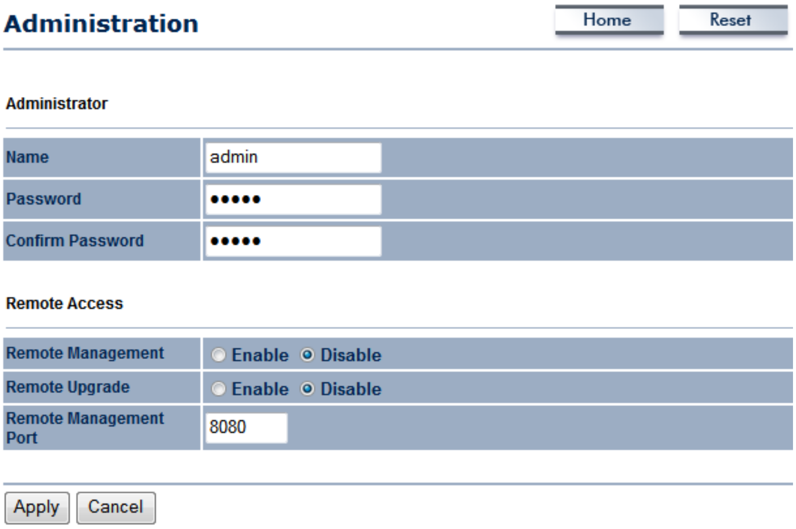
7.6 Management



- Under the **Management** section of the left menu, you will find the following options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, log and Diagnostics. Each option is described below.

7.6.1 Administration

- This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



Administrator

Name	admin
Password	●●●●●
Confirm Password	●●●●●

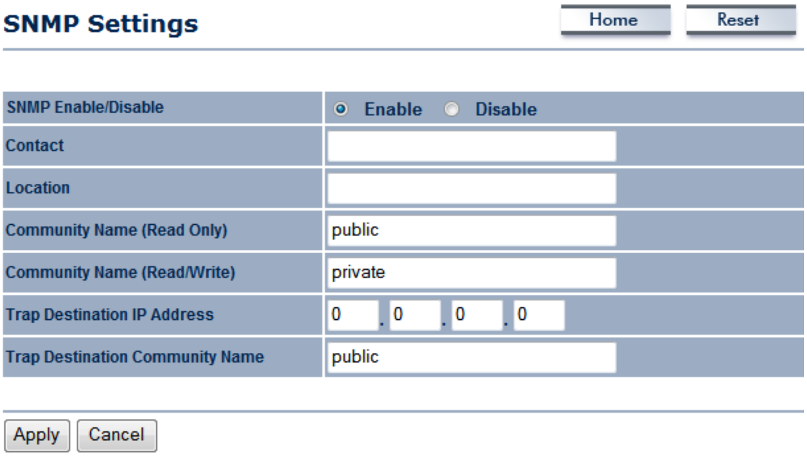
Remote Access

Remote Management	○ Enable ● Disable
Remote Upgrade	○ Enable ● Disable
Remote Management Port	8080

- **Name**: Specify a user name into the first field.
- **Password**: Specify a password into this field and then re-type the password into the **Confirm Password** field.
- **Remote Management**: Choose to enable or disable remote management.
- **Remote Upgrade**: Choose to enable or disable remote firmware upgrade.
- **Remote Management Port**: Specify a port for remote management. For example, if you specify 8080, then you will need to specify *<IP address>:<port>* 192.168.1.1:8080 to connect to the web interface of the device.
- Click on the **Apply** button to save the changes.

7.6.2 SNMP Settings

- This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.



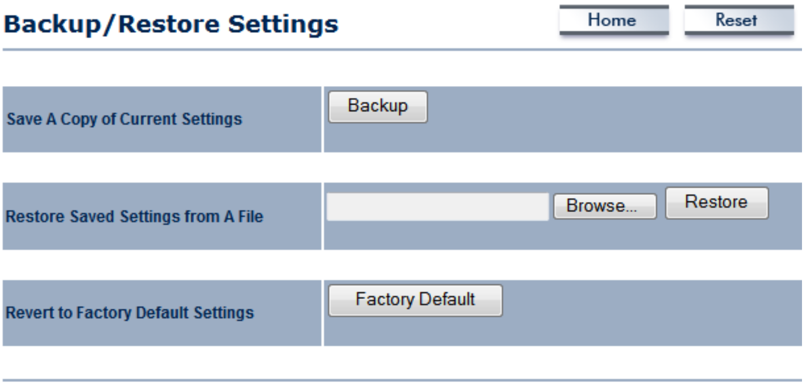
SNMP Settings

SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

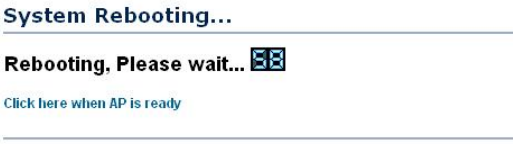
- **SNMP Enable/Disable**: Choose to **enable** or **disable** the SNMP feature.
- **Contact**: Specify the contact details of the device.
- **Location**: Specify the location of the device.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Trap Destination IP Address**: Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name**: Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

7.6.3 Backup/Restore settings, Reset to factory default settings

- This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.


Backup/Restore Settings
Home
Reset
Save A Copy of Current Settings
Backup
Restore Saved Settings from A File
Browse...
Restore
Revert to Factory Default Settings
Factory Default

- **Save a copy of the current settings**: Click on the Backup button to save the current configuration.
- **Restore saved settings from a file**: Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings**: Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1



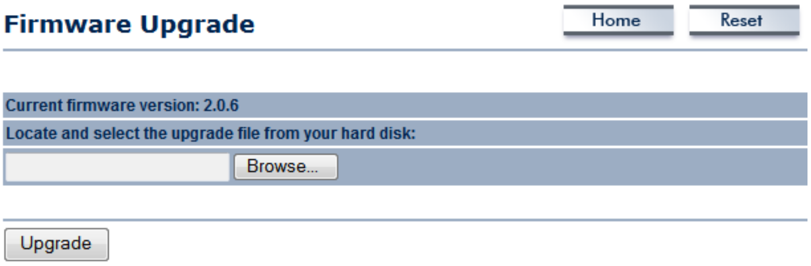
System Rebooting...

Rebooting, Please wait... 88

Click here when AP is ready

7.6.4 Firmware Upgrade

- This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



Firmware Upgrade

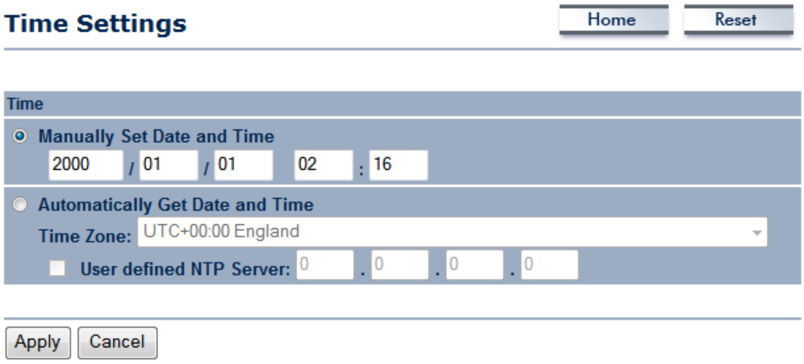
Current firmware version: 2.0.6

Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

7.6.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.



Time Settings

Time

● Manually Set Date and Time

2000 / 01 / 01 02 : 16

○ Automatically Get Date and Time

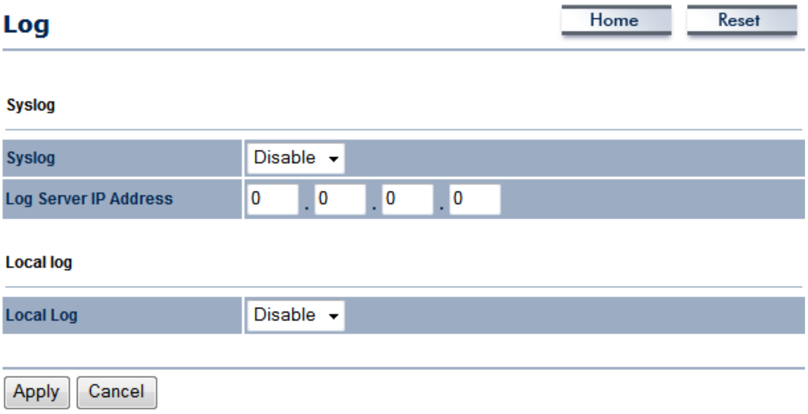
Time Zone: UTC+00:00 England

□ User defined NTP Server: 0 . 0 . 0 . 0

- **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 on the **Apply** button to save the changes.

7.6.6 Log

- Click on the **Log** link under the **Management** menu. The **Log** 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

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

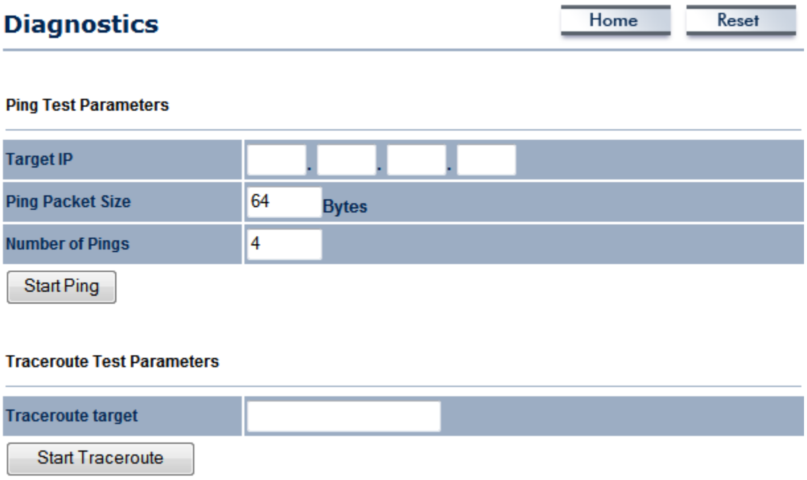
Local log

Local Log	Disable

- **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 on the **Apply** button to save the changes.

7.6.7 Diagnostics

- In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



Diagnostics

Ping Test Parameters

Target IP	. . .
Ping Packet Size	64 Bytes
Number of Pings	4

Traceroute Test Parameters

Traceroute target	

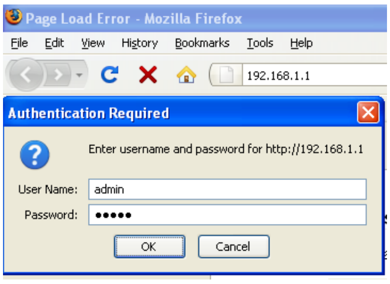
- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click **Start Ping**.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

8 Mesh Operating Mode

8.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:

6. **Status**: Displays the overall status, Wireless client list and system log.
7. **System**: This menu includes the system properties.
8. **Wireless**: This menu includes wireless network, security and advanced settings.
9. **Management**: This menu includes the admin setup, SNMP settings, firmware upgrade, save/restore backup, time setting and diagnostics.

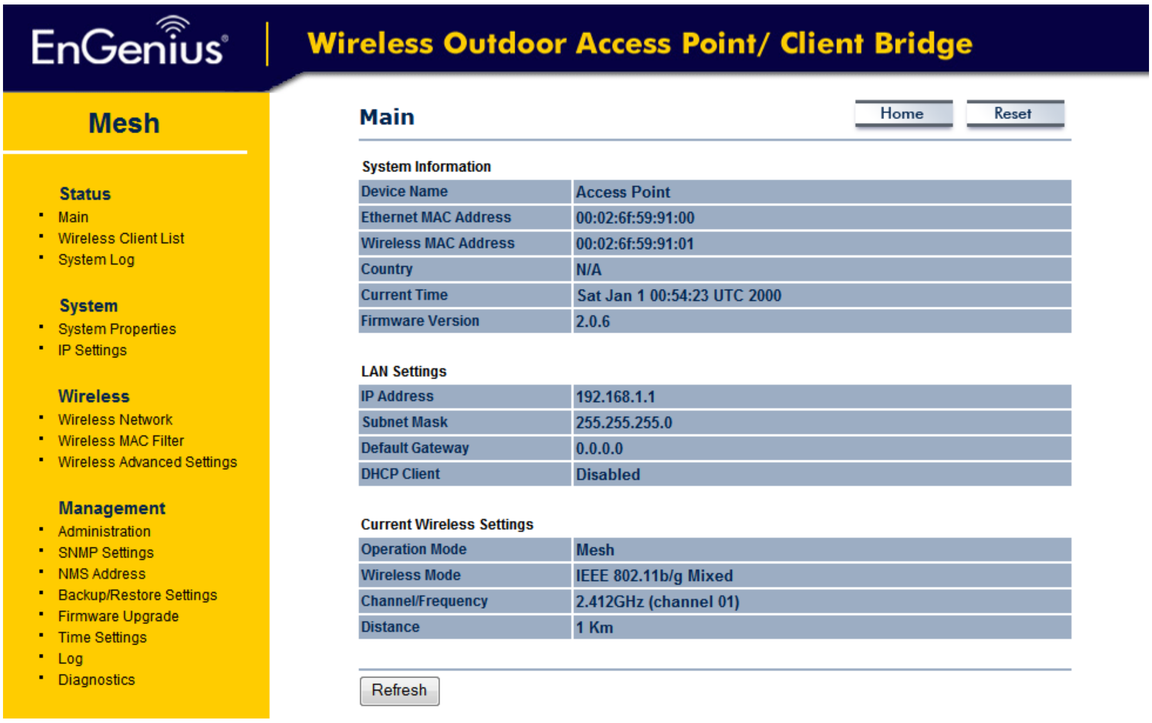

Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.1

Authentication Required

Enter username and password for http://192.168.1.1

User Name: admin

Password: •••••



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:54:23 UTC 2000
Firmware Version	2.0.6

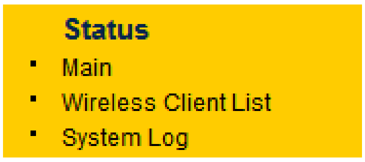
LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Mesh
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Distance	1 Km

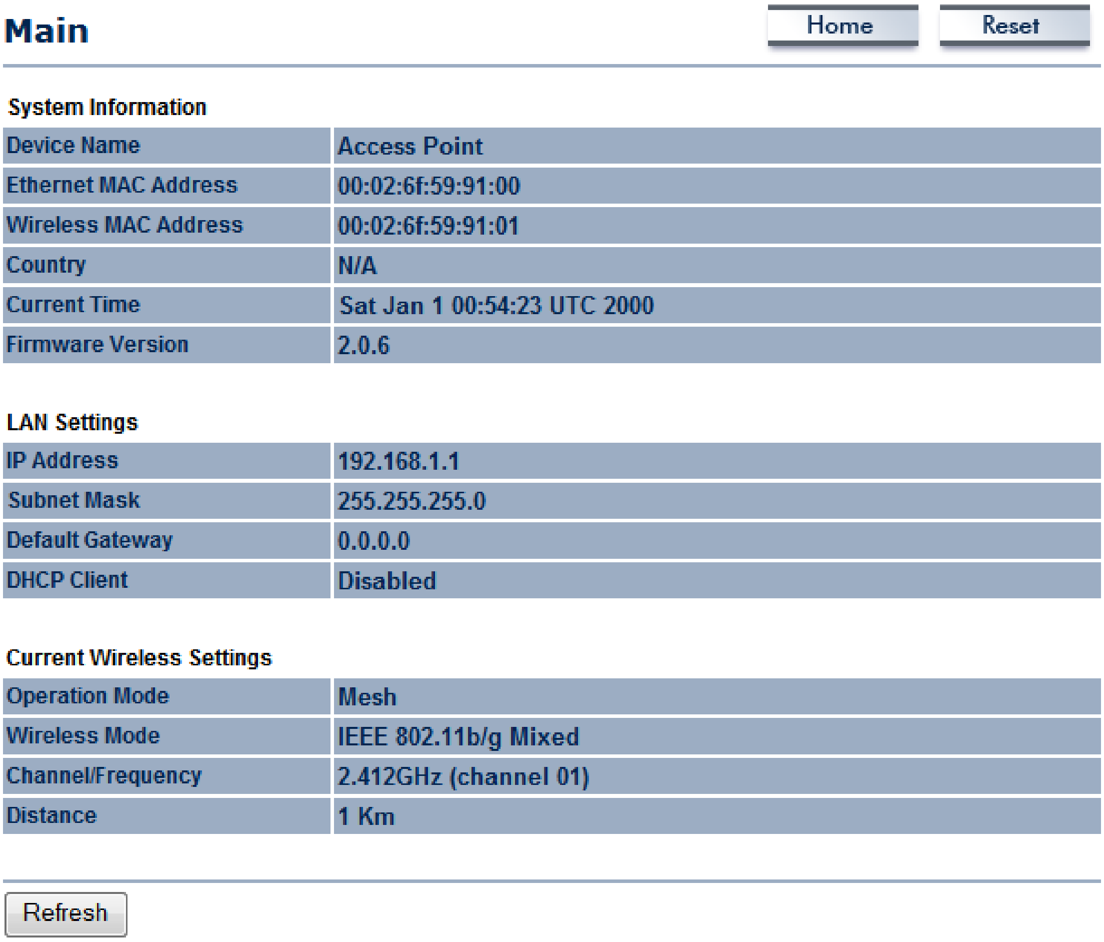
8.2 Status



- Under the **Status** section of the left menu, you will see the following options: **Main, Wireless Client List** and **System Log**. Each option is described in detail below.

8.2.1 Main

- The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, MAC Address, Country, Current and Firmware Version are displayed in the 'System Information' section. IP Address, Subnet Mask, Default Gateway and DHCP Server condition are displayed in the 'LAN Settings' section. The 'Current Wireless Settings' section displays Operation Mode, Wireless Mode, Channel/Frequency and Distance control.



System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:59:91:00
Wireless MAC Address	00:02:6f:59:91:01
Country	N/A
Current Time	Sat Jan 1 00:54:23 UTC 2000
Firmware Version	2.0.6

LAN Settings

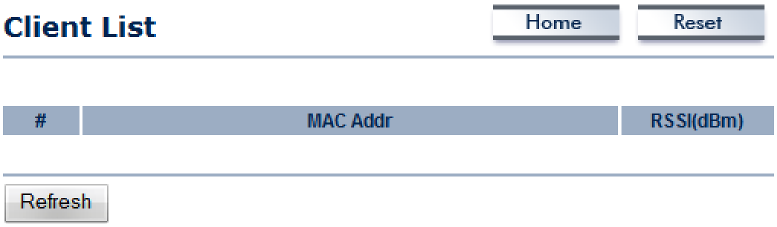
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Mesh
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Distance	1 Km

8.2.2 Wireless Client List

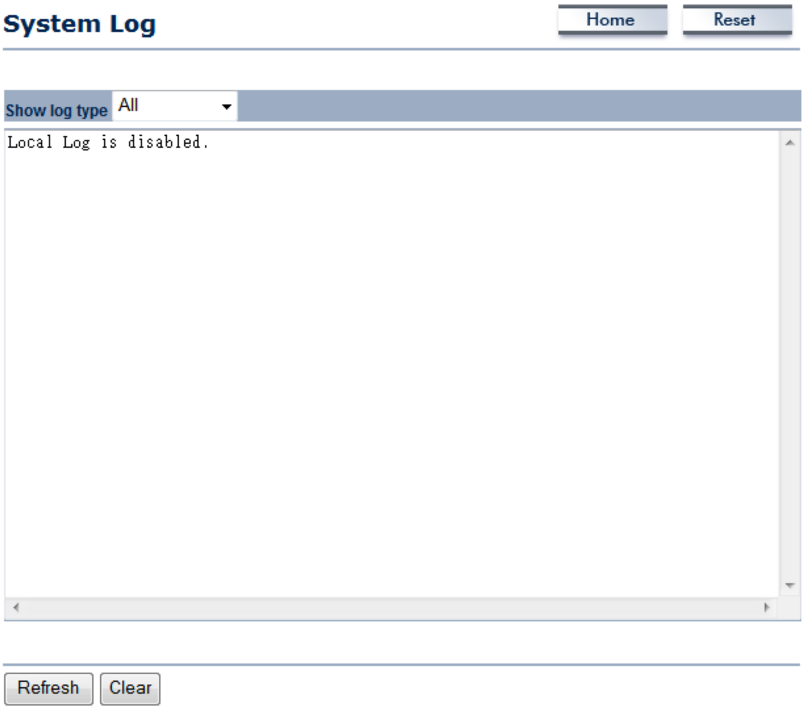
- This page displays the list of Clients that are associated to the Access Point.
- The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list.



#	MAC Addr	RSSI(dBm)

8.2.3 System Log

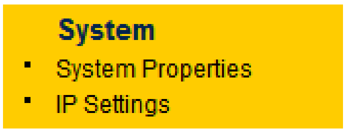
The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.



Show log type All

```
Local Log is disabled.
```

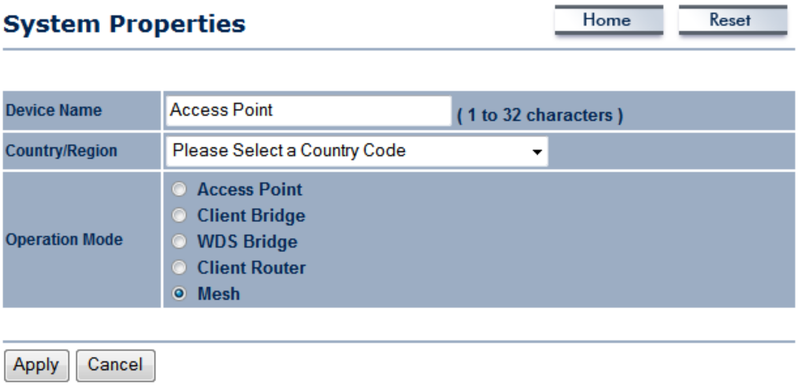
8.3 System



- Under the **System** section of the left menu, you will see the following options: **System Properties setting** and **IP Setting**, which are described below.

8.3.1 System Properties

- This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.



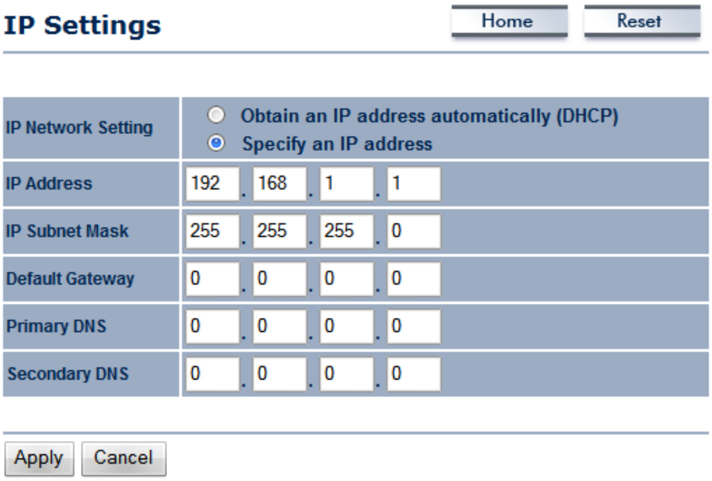
System Properties

Device Name	Access Point (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	○ Access Point ○ Client Bridge ○ WDS Bridge ○ Client Router ● Mesh

- **Device Name**: Specify a name for the device (this is not the SSID),
- **Country/Region**: Select a country from the drop-down list.
- **Operating Mode**: Select an Operating Mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

8.3.2 IP Settings

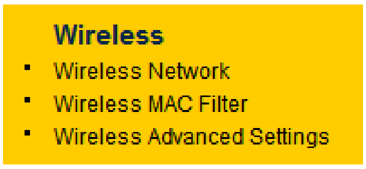
- This page allows you to configure the device with a static IP address or a DHCP client.



IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

- **IP Network Setting**: Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address**: Specify an IP address
- **IP Subnet Mask**: Specify the subnet mask for the IP address
- **Default Gateway**: Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

8.4 Wireless



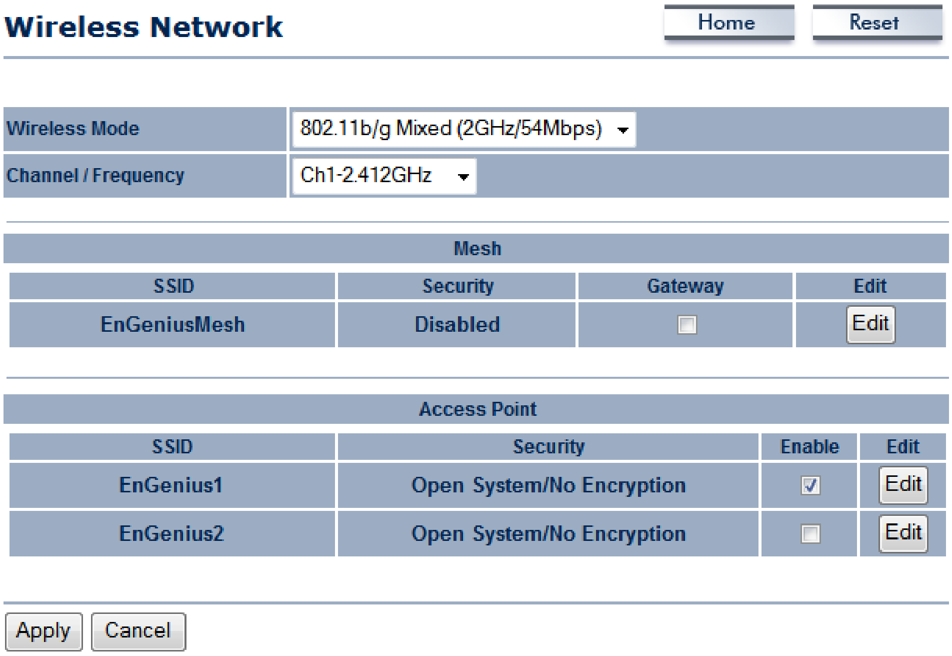
Wireless

- Wireless Network
- Wireless MAC Filter
- Wireless Advanced Settings

- Under the **Wireless** section of the left menu, you will see the following options: **Wireless Network, Wireless Security**, and **Wireless Advanced Settings**. Each option is described below.

8.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.



Wireless Network

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
Channel / Frequency	Ch1-2.412GHz

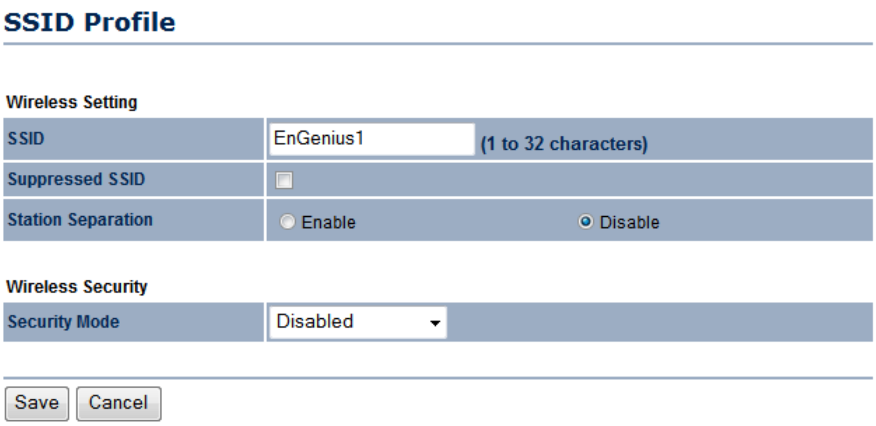
Mesh

SSID	Security	Gateway	Edit
EnGeniusMesh	Disabled	□	Edit

Access Point

SSID	Security	Enable	Edit
EnGenius1	Open System/No Encryption	☑	Edit
EnGenius2	Open System/No Encryption	□	Edit

- **Wireless Mode**: Depending on the type of wireless clients that are connected to the network, you may select **B**, **G or B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **Channel / Frequency**: Select a channel from the drop-down list. The channels available are based on the country’s regulation.
- **Mesh**: User can setup the SSID configuration and WEP security setting of the Mesh network.
- **Current Profiles**: User can setup SSID configuration in this item. In Mesh mode, the M2000 supports 2 SSIDs, the user can decide whether to “Enable” the SSID. Click the “Edit” button to configure the settings for the SSID.



SSID Profile

Wireless Setting

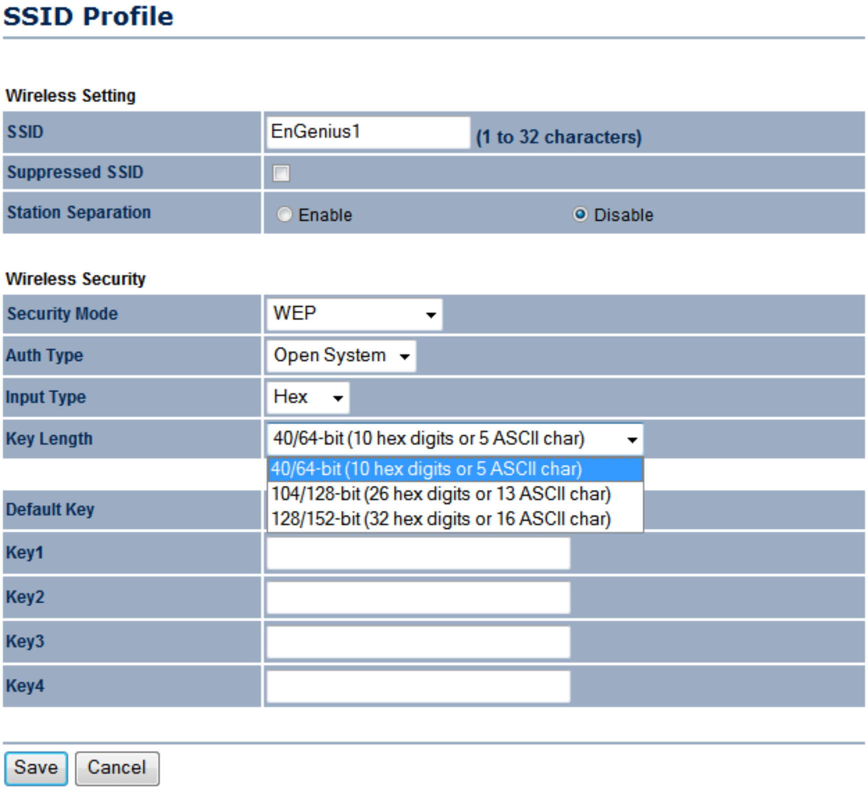
SSID	EnGenius1 (1 to 32 characters)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	Disabled

- **SSID**: Type in your SSID
- **Suppressed SSID:** When enabled, the SSID will be hidden.
- **Station Separation:** When enabled, wireless clients on different SSID's cannot connect with each other.

▶ Wireless Security – Security Mode : WEP



SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char) 40/64-bit (10 hex digits or 5 ASCII char) 104/128-bit (26 hex digits or 13 ASCII char) 128/152-bit (32 hex digits or 16 ASCII char)
Default Key	
Key1	
Key2	
Key3	
Key4	

▶▶ **Security Mode**: Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

▶▶ **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. 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 Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point 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

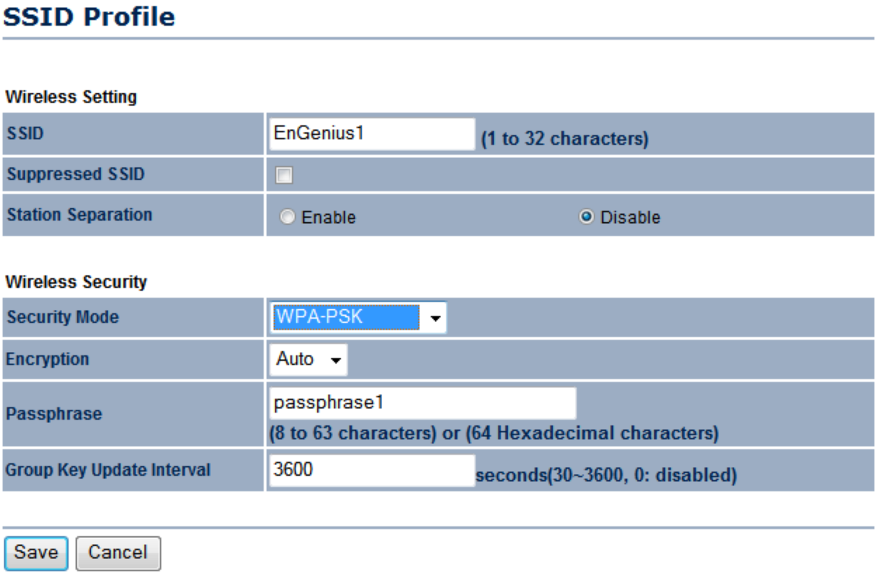
▶▶ **Key Length**: Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.

▶▶ **Default Key**: You may use up to four different keys for four different networks. Select the current key that will be used.

▶▶ **Key 1-4**: You may enter four different WEP keys.

▶▶ Click on the **Save** button to save the changes.

▶ Wireless Security – Security Mode : WPA-PSK, WPA2-PSK, WPA-PSK Mixed



SSID Profile

Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
Suppressed SSID	□
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	WPA-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

▶▶ **Security Mode**: Select **WPA-PSK, WPA2-PSK, or WPA-PSK Mixed** from the drop-down list if your wireless network uses WPA pre-shared key.

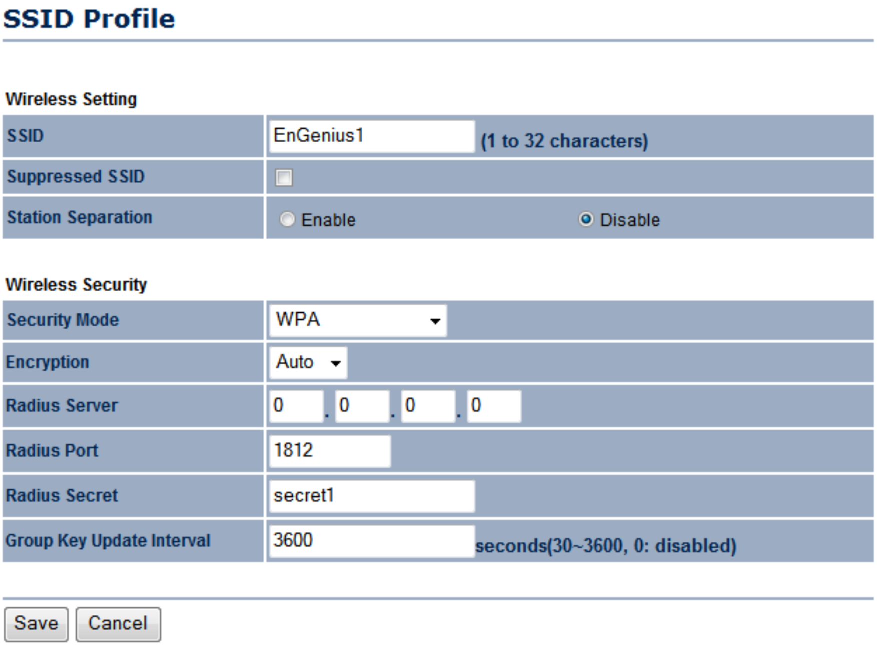
▶▶ **Encryption**: Select **TKIP**, **AES or Auto** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with. AES is an even more advanced method of encryption which offers the highest level of WPA/WPA2 security.

▶▶ **Passphrase**: Specify a passphrase that is shared amongst the Access Points and clients.

▶▶ **Group Key Update Interval**: Specify the number of seconds after which the Access Point will probe the client for the passphrase.

▶▶ Click on the **Save** button to save the changes.

▶ Wireless Security – Security Mode : WPA, WPA2, WPA Mixed



SSID Profile

Wireless Setting

SSID	EnGenius1	(1 to 32 characters)
Suppressed SSID	□	
Station Separation	○ Enable	● Disable

Wireless Security

Security Mode	WPA	
Encryption	Auto	
Radius Server	0 . 0 . 0 . 0	
Radius Port	1812	
Radius Secret	secret1	
Group Key Update Interval	3600	seconds(30~3600, 0: disabled)

▶▶ **Security Mode**: Select **WPA**, **WPA2 or WPA Mixed** from the drop-down list if your wireless network uses WPA. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

▶▶ **Encryption**: Select **TKIP**, **AES or Auto** from the drop-down list if your wireless network uses this encryption.

▶▶ **RADIUS Server:** Enter the IP address of the RADIUS server.

▶▶ **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.

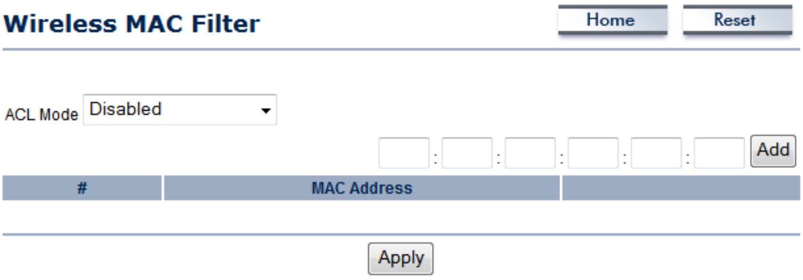
▶▶ **RADIUS Secret:** Enter the shared password of the RADIUS server.

▶▶ **Group Key Update Interval**: Specify the number of seconds after which the Access Point will probe the client for the secret.

▶▶ Click on the **Save** button to save the changes.

8.4.2 Wireless MAC Filter

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



Wireless MAC Filter

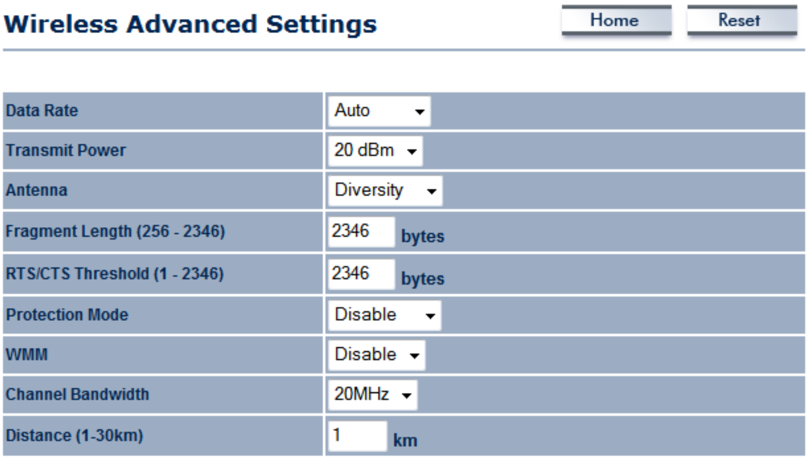
ACL Mode Disabled

#	MAC Address	

- **ACL (Access Control) Mode:** You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC addresses from associating with the network. 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 on the **Delete** button.
- Click on the **Apply** button to save the changes.

8.4.3 Wireless Advanced Settings

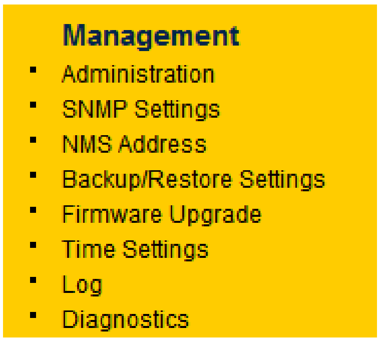
- On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.



Data Rate	Auto
Transmit Power	20 dBm
Antenna	Diversity
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

- **Data Rate**: If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power**: You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Antenna**: You can select the antenna polarization to Diversity, Horizontal or Vertical.
- **Fragment Length**: Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS/CTS Threshold**: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode**: If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM**: Enable wireless Quality of Service
- **Distance (1-30km)**: Specify a distance between 1 and 30Km.
- **Channel Bandwidth**: For different application, you can select 20MHz, 10MHz or 5MHz channel bandwidth.
- Click on the **Apply** button to save the changes.

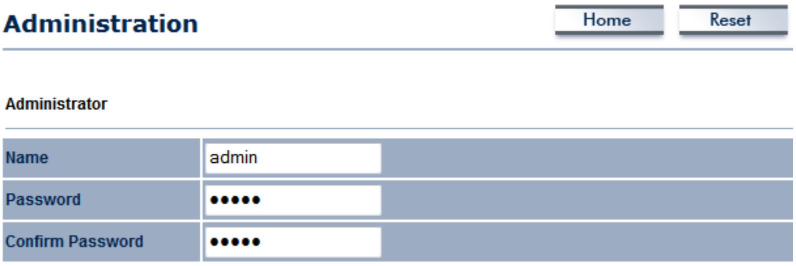
8.5 Management



- Under the **Management** section of the left menu, you will find the following options: **Administration, SNMP Settings, Backup/Restore Settings, Firmware Upgrade, Time Settings, Log** and **Diagnostics**. Each option is described below.

8.5.1 Administration

- This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



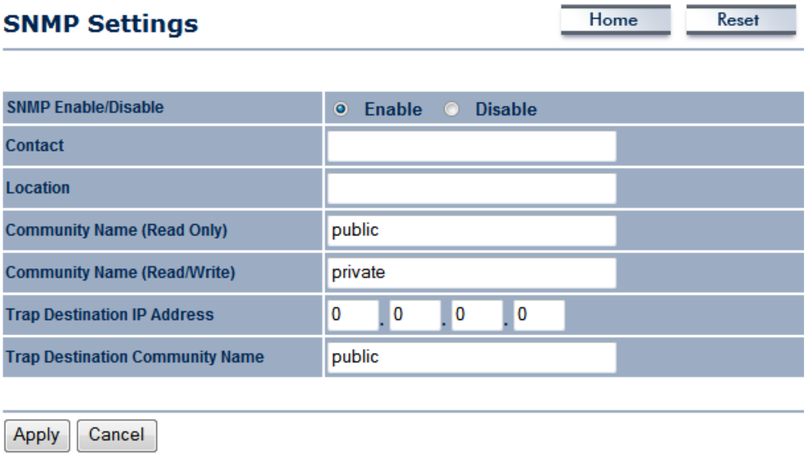
Administrator

Name	admin
Password	•••••
Confirm Password	•••••

- **Name**: Specify a user name into the first field.
- **Password**: Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

8.5.2 SNMP Settings

- This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

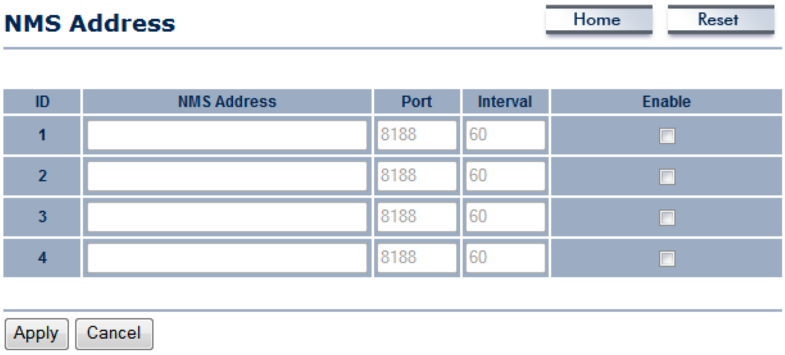


SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

- **SNMP Enable/Disable**: Choose to **enable** or **disable** the SNMP feature.
- **Contact**: Specify the contact details of the device.
- **Location**: Specify the location of the device.
- **Read-Only Community Name**: Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name**: Specify the password for access to the SNMP community with read/write access.
- **Trap Destination IP Address**: Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name**: Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

8.5.3 NMS Settings

- This option allows you to specify the address of the NMS server.



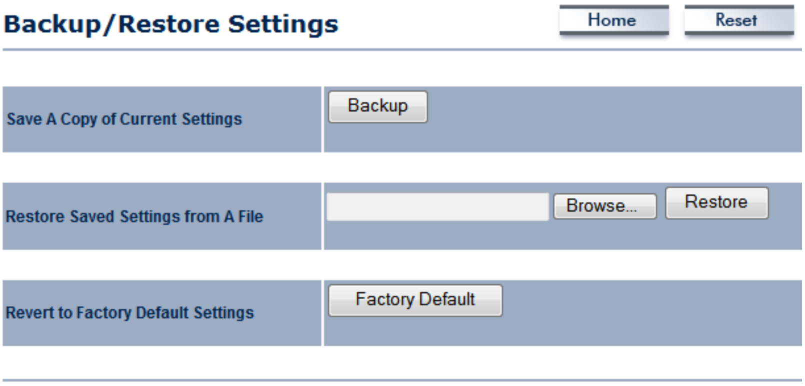
NMS Address

ID	NMS Address	Port	Interval	Enable
1		8188	60	☐
2		8188	60	☐
3		8188	60	☐
4		8188	60	☐

- **NMS Address**: Specify the address of the NMS server.
- **Port:** Specify the port of the NMS server.
- **Interval:** Specify how often the M2000 requests an update from the NMS server.
- **Enable:** Allow the M2000 to connect to the specified NMS server.

8.5.4 Backup/Restore settings, Reset to factory default settings

- This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.



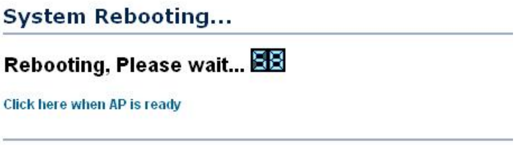
Backup/Restore Settings

Save A Copy of Current Settings

Restore Saved Settings from A File

Revert to Factory Default Settings

- **Save a copy of the current settings**: Click on the Backup button to save the current configuration.
- **Restore saved settings from a file**: Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings**: Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1



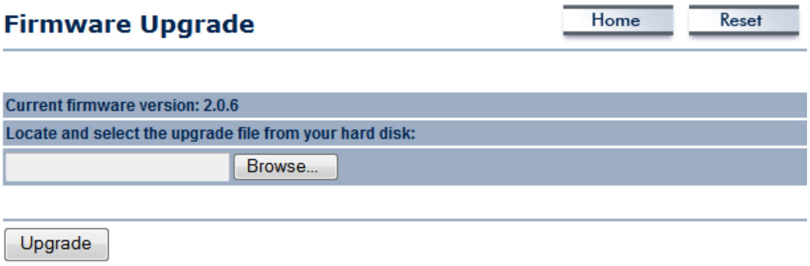
System Rebooting...

Rebooting, Please wait... 88

Click here when AP is ready

8.5.5 Firmware Upgrade

- This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.



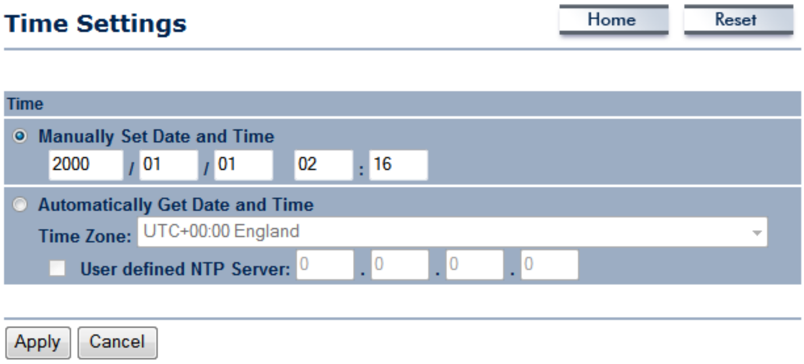
Current firmware version: 2.0.6

Locate and select the upgrade file from your hard disk:

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.
  Note: The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

8.5.6 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.



Time

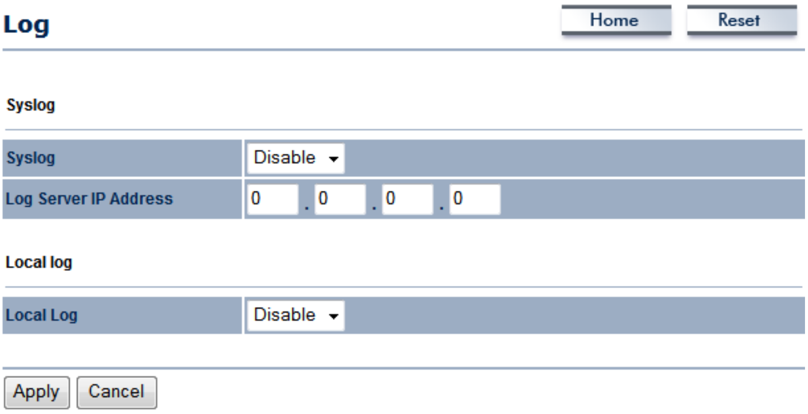
● Manually Set Date and Time
2000 / 01 / 01 02 : 16

○ Automatically Get Date and Time
Time Zone: UTC+00:00 England
□ User defined NTP Server: 0 . 0 . 0 . 0

- **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 on the **Apply** button to save the changes.

8.5.7 Log

- Click on the **Log** link under the **Management** menu. The **Log** 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

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

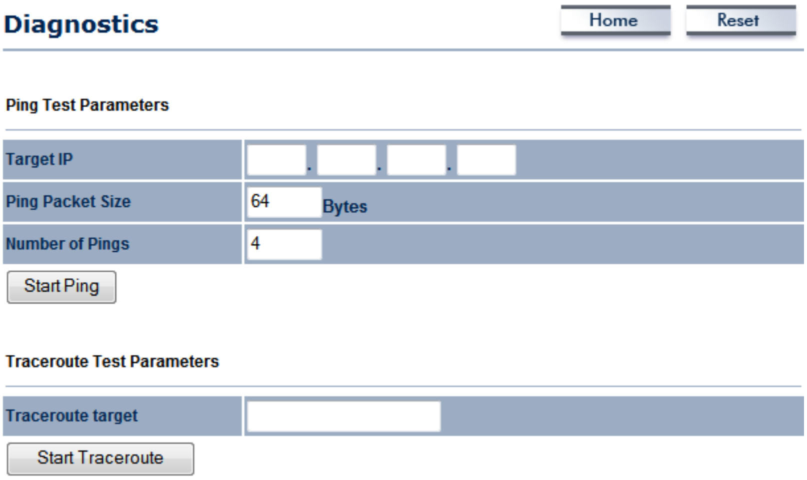
Local log

Local Log	Disable

- **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 on the **Apply** button to save the changes.

8.5.8 Diagnostics

- In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



Diagnostics

Ping Test Parameters

Target IP	. . .
Ping Packet Size	64 Bytes
Number of Pings	4

Traceroute Test Parameters

Traceroute target	

- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click **Start Ping**.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

Appendix A – FCC Interference 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.

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.

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

Appendix B – IC Statement

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
Radiation Exposure Statement:

This equipment complies with IC 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.

This device has been designed to operate with an antenna having a maximum gain of 5 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.