Long Range Multi-Function Access Point

M35

User Manual

V1.0

Table of Contents

1 Product Overview

Thank you for using M35. It is a powerful, enhanced, enterprise scale product with 7+1 multi-functions Access Point, Access Point with WDS function, Client Bridge, WDS Bridge, Repeater, AP Router, Client Router, and Mesh.

M35 is easily to install almost anywhere with Power over Ethernet for quick indoor installation and regular Power by Adapter. External N-type antenna provides better wireless signal quality and the antenna is upgradeable.

M35 can manage power level control, Narrow bandwidth selection, Traffic shaping and Real-time RSSI indicator. M35 is fully support of security encryption including WI-Fi Protected Access (WPA-PSK/WPA2-PSK), 64/128/152-bit WEP Encryption and IEEE 802.1x with RADIUS Accounting.

1.1 Benefits

The following list describes the design of the M35 made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**

Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **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.

Benefits	
High Speed Data Rate Up to 108Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power up to 28 dBm	Extended excellent Range and Coverage
IEEE 802.11b/g Compliant	Fully Interoperable with IEEE 802.11b/IEEE 802.11g compliant devices
Detachable antenna support (N-Type)	Collocate with any antenna for user's environment
7+1 Multi-Function	Users can use different mode in various environment
Point-to-point, Point-to-multipoint Wireless Connectivity	Let users transfer data between two buildings or multiple buildings
Channel Bandwidth Selection	Using different bandwidth to reach varied distance
Support RSSI Indicator (CB mode)	Users can select the best signal to connect with AP easily
Power-over-Ethernet	Flexible Access Point locations and cost savings. M35 must uses the adapter provided in the package.
Support Multi-SSID function (4 SSID) in AP mode	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID by manager
WPA2/WPA/ WEP/ IEEE 802.1x support	Fully support all types of security types.
MAC address filtering in AP mode	Ensures secure network connection
PPPoE/PPTP function support (AP Router/CR mode)	Easy to access internet via ISP service authentication
SNMP Remote Configuration Management	Help administrators to remotely configure or manage the Access Point easily.
QoS (WMM) support	Enhance user performance and density

High Speed Data Rate Up to 108Mbps	Capable of handling heavy data payloads such as MPEG video streaming

1.2 Feature

Access Point Mode	Use this feature to setup the access point's configuration information. It has support adjusting transmit power and channel. Client can access the network with different regulatory settings and automatically change to the local regulations.
Client Bridge Mode	Use this feature to connect to an Access Point and enjoy the great speed of surfing internet.
WDS Mode	Use this feature to link multiple APs in a network, All clients associated with any APs can communicate each other like an ad-hoc mode.
Repeater Mode	Use this feature to extend the wireless signal coverage area.
AP Router Mode	This feature provides ability to connect to internet and has a DHCP server build inside that allows client easily to retrieve automatically.
Client Router Mode	This feature functions completely opposite but similarly with AP Router Mode. Client Router connected to an AP wirelessly and transmit internet connection protocol through AP to access the internet.
Mesh Mode	Use this feature to establish a NET type of network. Mesh can reduce the cost of the T1 and xDSL wired network. If one path of the network is broken or blocked, the transmission is automatically find the best path to the destination.
Multiple SSIDs	M35 supports up to 4 SSIDs on your access point. The following options can be set to each SS to each SSID: - SSID for public or private network - Authentication is fully supported - VLAN identifier - Radius accounting identifier - Profile isolation for infrastructure network
VLAN	Specify a VLAN number for each SSID to separate the services among clients.
QoS	Use this feature to limit the incoming or outgoing throughput.
Wi-Fi Protect Access	Wi-Fi Protect Access is a standard-based interoperable security enhancement that increases the level of data protection and access control for existing and future wireless LAN system. It is compatible with IEEE 802.11i standard WPA leverages TKIP and 802.1X for

	authenticated key management.

1.3 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* Long Range Multi-Function AP (M35)
- 1* 12V/1A Power Adapter
- 1* 50cm Ethernet Cable
- 1* QIG
- 1* CD (User Manual)
- 2* 5dBi 2.4GHz Dipole Antennas

Auction: Using other Power Adapter than the one included with M35 may cause damage of the device.

1.4 System Requirement

The following conditions are the minimum system requirement.

- A computer with an Ethernet interface and operating under Windows XP, Vista, 7 or Linux.
- Internet Browser that supports HTTP and JavaScript.

1.5 Hardware Overview

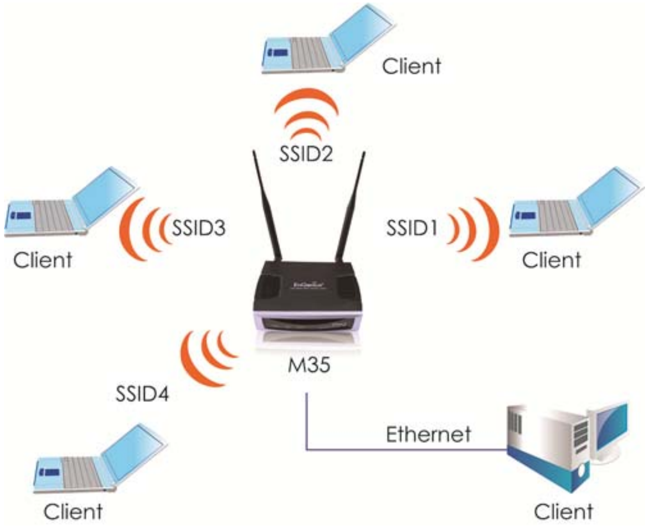
MCU	Atheros SoC, 180MHz
Memory	32MB SDRAM
Flash	8MB
Physical Interface	● LAN: One 10/100 Fast Ethernet RJ-45 ● Reset Button ● Power Jack
LEDs Status	● Power/ Status ● LAN (10/100Mbps) ● WLAN (Wireless Connection)

Power Requirements	● Power Supply: 90 to 240 VDC ± 10％, 50/60 Hz (depends on different countries) ● Active Ethernet (Power over Ethernet, IEEE802.3af)- 48 VDC/0.375A ● Device: 12V/1A
Regulation Certifications	● FCC Part 15, CE

2 M35 Multi-Function Instruction Guide

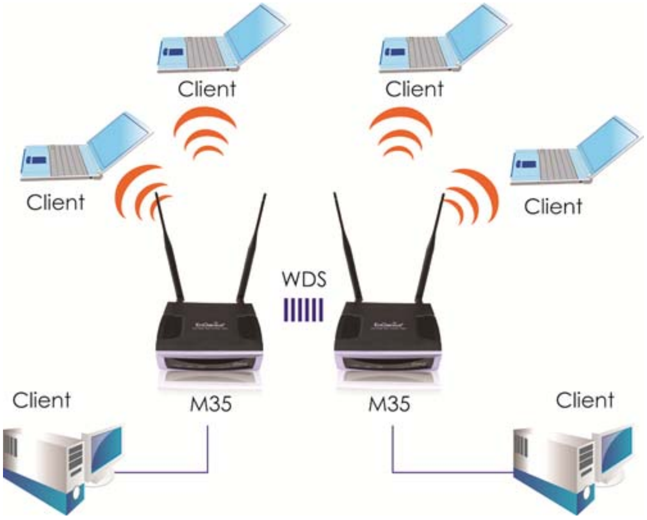
2.1 Access Point

In the Access Point Mode with WDS Function, M35 function likes a central connection for any stations or clients that support IEEE 802.11b/g and SuperG network. Stations and Client must configure the same SSID and Security Password to associate within the range. M35 supports 4 different SSIDs to separate different clients at the same time.



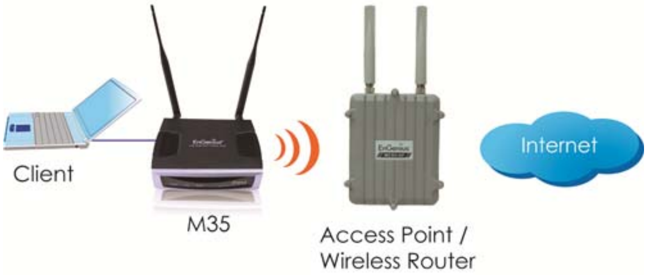
2.2 Access Point with WDS Function

M35 also supports WDS function in Access Point Mode without losing AP's capabilities. Configure others Access Point's Wireless MAC Address in both Access Point devices to enlarge the wireless area by enabling WDS Link Settings. WDS function can support up to 8 different AP's MAC addresses. Auction: Not every Access Point device has support WDS in Access Point Mode. It is recommended using M35 if you would like to use this service.



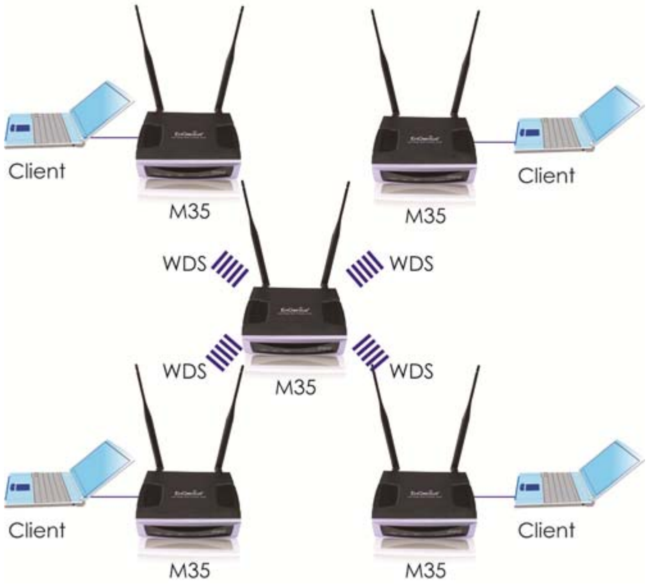
2.3 Client Bridge

In the Client Bridge Mode, the M35 function likes a wireless dongle. Connected to an Access Point wirelessly and surf internet whenever you want. Using Site Survey to scan all the Access Point within the range and configure its SSID and Security Password to associate with it. Connect you station to the LAN port of the M35 via Ethernet.



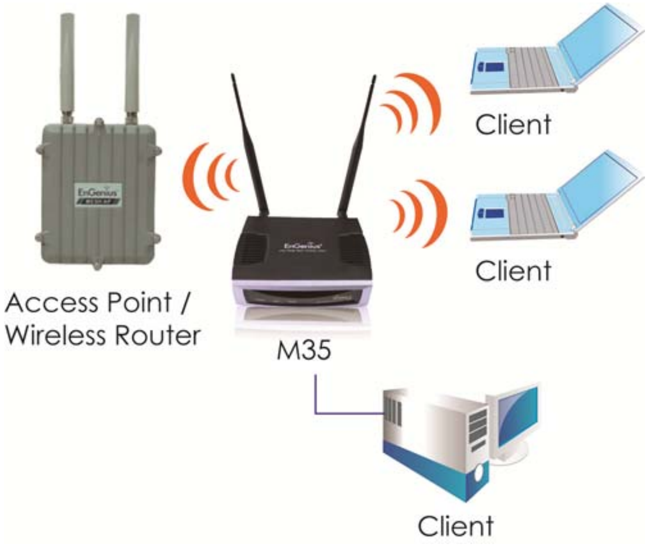
2.4 WDS Bridge

In the WDS Bridge Mode, the M35 can wirelessly connect different LANs by just simply configure each other's MAC Address and Security Settings. This mode is used when two wired LANs locate in small distance and want to communicate each other. The best solution is using M35 wirelessly connect two wired LANs. WDS Bridge Mode can establish 16 WDS links, the connection diagram is like a Star.
Auction: WDS Bridge Mode is not function like Access Point. APs linked by WDS are using the same frequency channel, more APs connected together may lower throughput. Please be aware to avoid loop connection diagram, otherwise enable Spanning Tree Function.



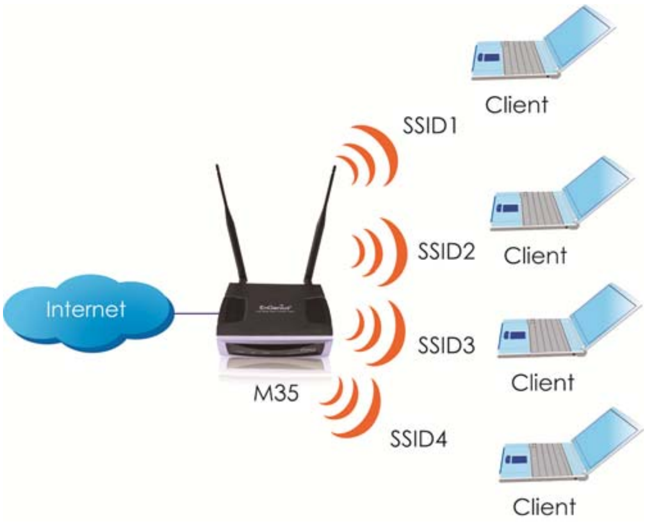
2.5 Repeater

In the Repeater Mode, the M35 can extend the wireless coverage area of another Access Point or Wireless Router. Access Point or Wireless Router must within the range and M35 must use the same SSID, Security Password and Channel.



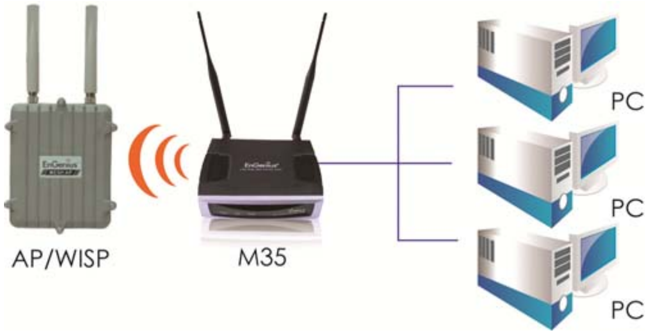
2.6 AP Router

In the AP Router Mode, the M35 has DHCP server build inside that allows you to configure easily via wireless. AP Router Mode can also support four different SSIDs. Use wireless device to associate with M35, connect an Ethernet through the WAN port. You can surf internet whenever you want within the range.



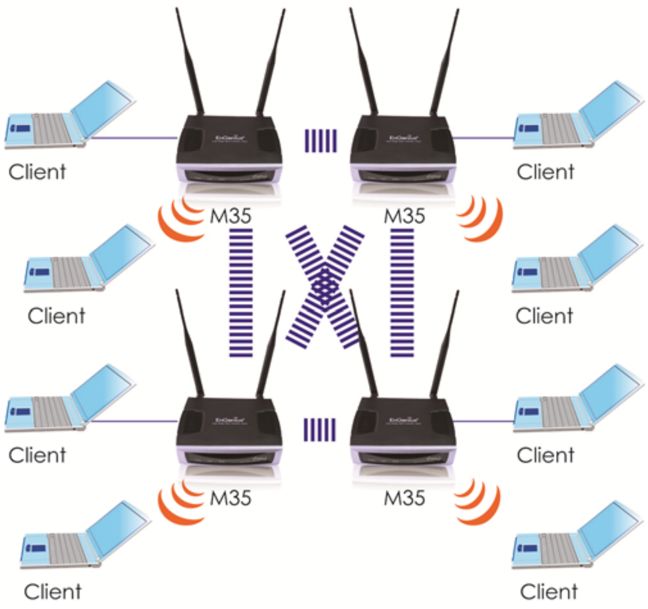
2.7 Client Router

In the Client Router Mode, the M35 has DHCP Server build inside that allows many LANs automatically generate an IP address to share the same Internet. Connect an AP/WISP Wirelessly and connect to LANs via wired. Client Router Mode is act completely opposite to the AP Router Mode.



2.8 Mesh

In the Mesh Mode, the M35 is act like an independent node and each node is allowed connecting to another network. If one node is lost, the continuous connection through around the broken or blocked by hopping from node to node until the destination is reached. Each node is connected to every other node. Mesh network is similarly to the ad hoc network.



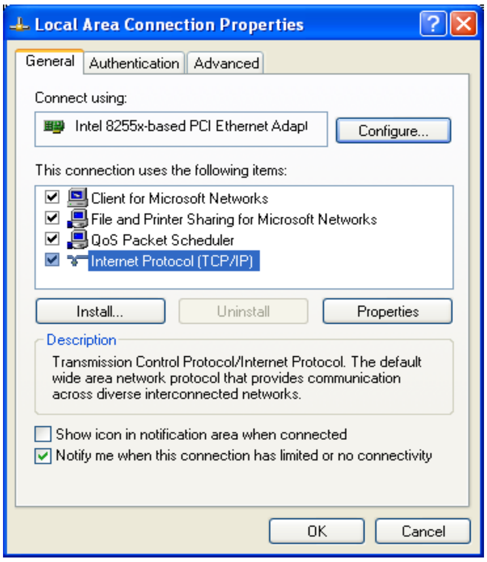
In Mesh Mode, recommended 1 Gateway with 4 Relay Linear and radiative deployment scenario.

3 Computer Configuration Instruction

3.1 Assign a Static IP

In order to configure M35, please follow the instruction below:

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.



Connect using:
Intel 8255x-based PCI Ethernet Adapl

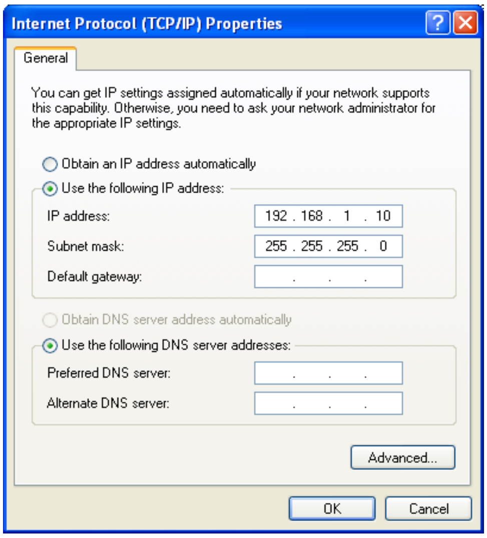
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

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

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.



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: . . .

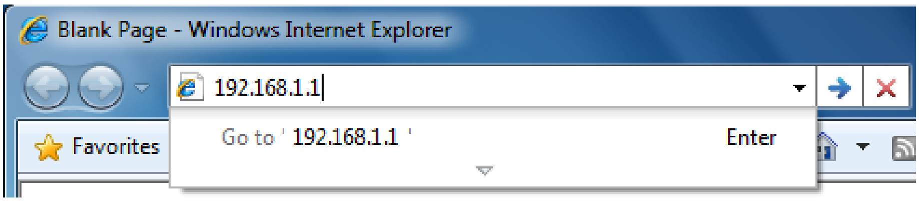
4. Click on the **OK** button to close this window, and then close LAN properties window.

Auction: IP Address entered in the TCP/IP Properties needs to be at the same subnet of the M35 IP Address. For example: M35’s default IP Address is **192.168.1.1** so the IP Address in the TCP/IP settings could be **192.168.1.10**.

3.2 Logging Method

After complete the IP settings from last section, you can now access the web-based configuration menu.

1. Open web browser

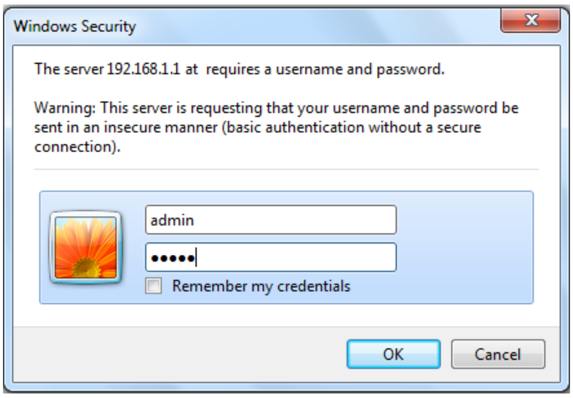


192.168.1.1

Go to ' 192.168.1.1 '

2. Enter IP **192.168.1.1** into you address filter.

Auction: If you have changed the M35 LAN IP address, make sure you enter the correct IP Address.



The server 192.168.1.1 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

•••••

□ Remember my credentials

3. After connected to the M35 successfully, browser will pop out a Windows Security window. Please enter the correct **Username** and **Password**.

4. The default Username and Password are both **admin**.

Auction: If you have changed the Username and Password, please enter your own Username and Password.

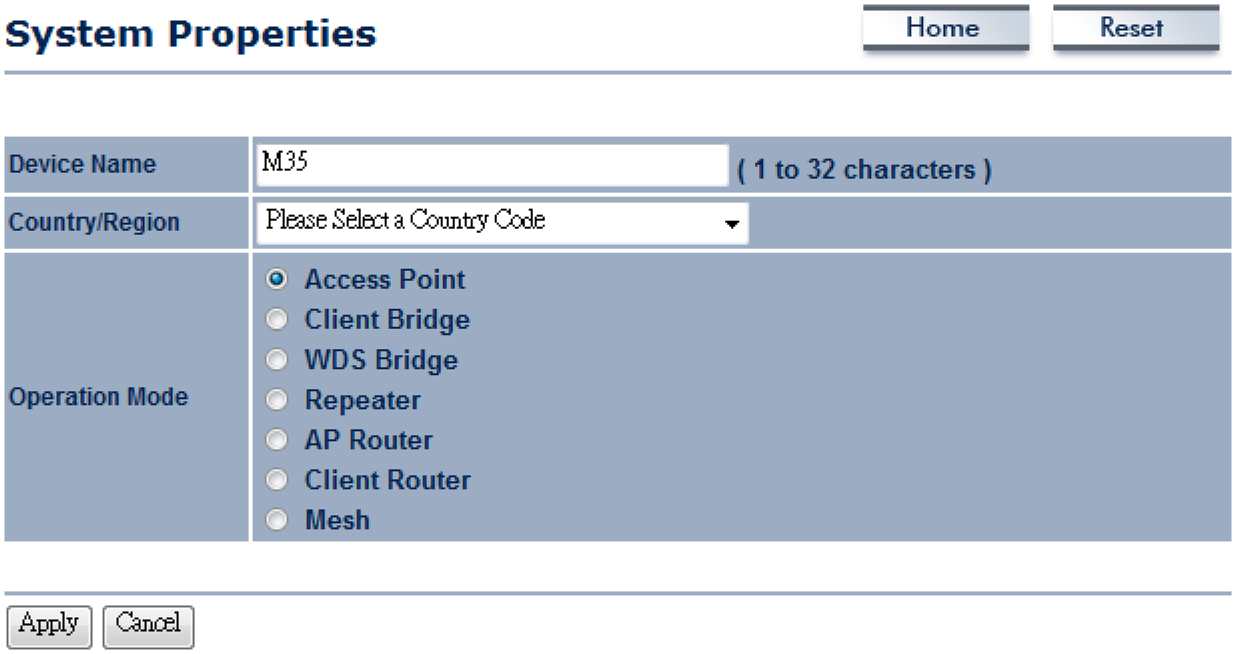
4 Wireless Configuration

4.1 Switching Operation Mode

The M35 supports 6 different operation modes: Access Point, Client Bridge, WDS Bridge, Repeater, AP Router, and Client Router.

Click **System Properties** under System Section to begin.

.



System Properties

Device Name	M35 (1 to 32 characters)
Country/Region	Please Select a Country Code
Operation Mode	● Access Point ○ Client Bridge ○ WDS Bridge ○ Repeater ○ AP Router ○ Client Router ○ Mesh

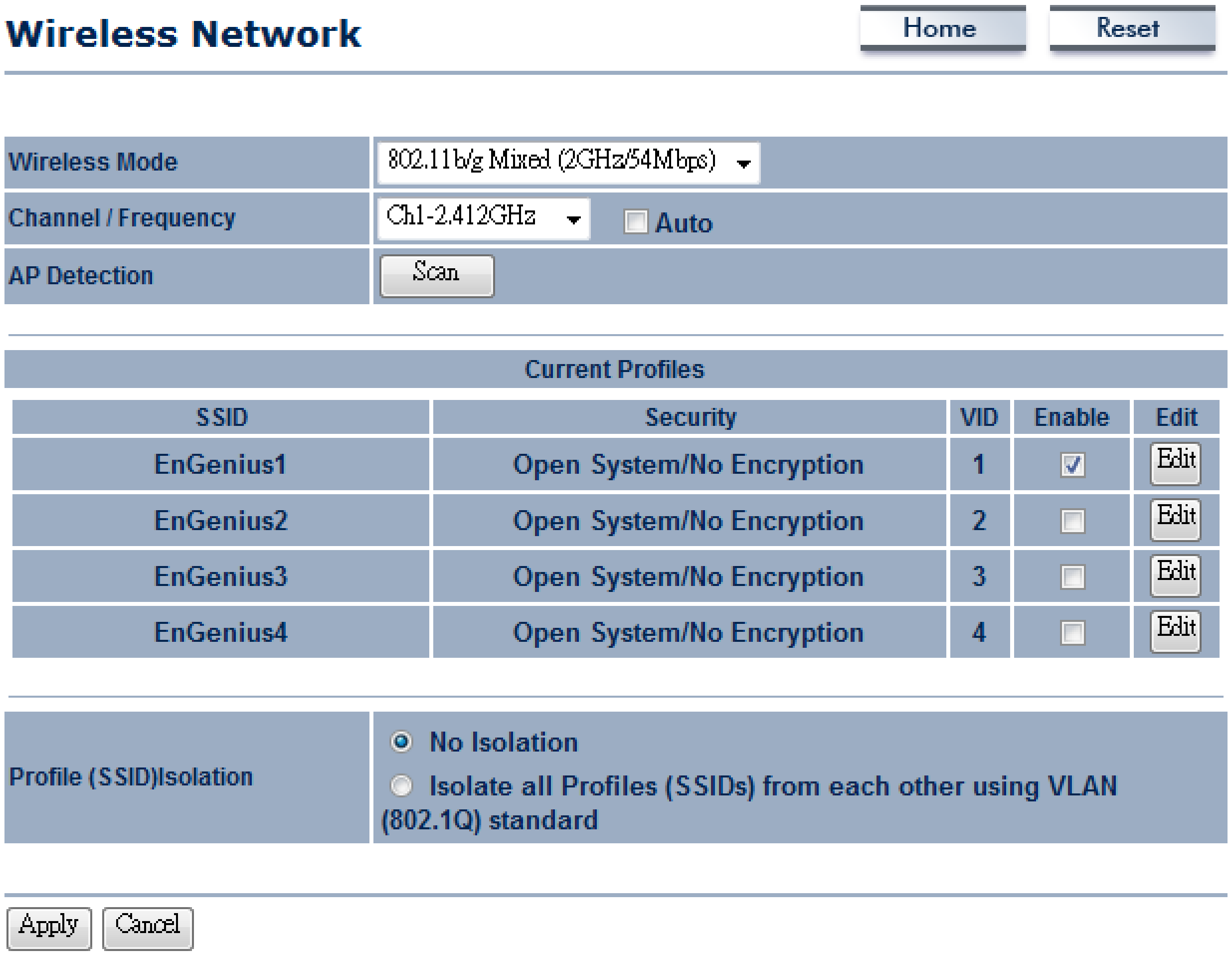
Device Name: Specify a name for the device, but it is not the broadcast SSID. It will be shown in SNMP management.
Country/Region: Select a Country/Region to conform local regulation.
Operation Mode: Select an operation mode via **Radio Button**.

Click **Apply** to save the changed.

Note: If you would like to use Access Point with WDS Function mode, please select Access Point Mode and then enable WDS Link Settings function.

4.2 Wireless Settings

4.2.1 Access Point Mode



Wireless Network

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

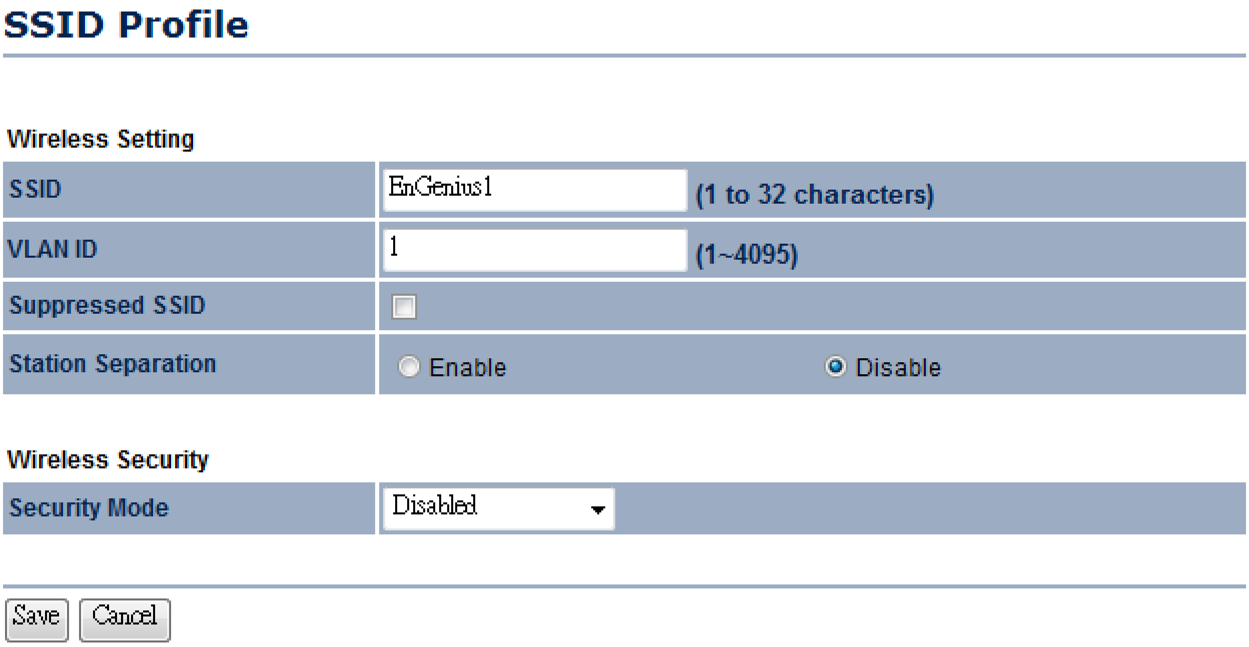
Current Profiles

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	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11b, 802.11g Only, 802.11 b/g mixed and SuperG.
Channel / Frequency	The channel availability is based on the country's regulation.
Auto	Place a **Check** to enable Auto channel selection.
AP Detection	AP Detection can help to select a best channel by scan nearby area.
Current Profile	Configure up to four different SSIDs, it can help to divide group of clients to access the network. Press **Edit** to configure the profile and place a **Check** to enable extra SSID.
Profile Isolation	Restricted Client to communicate with different VID by Selecting the Radio button.

Auction: SuperG is a special feature in M35. If the client does not support SuperG, it cannot establish a wireless connection successfully.



SSID Profile

Wireless Setting

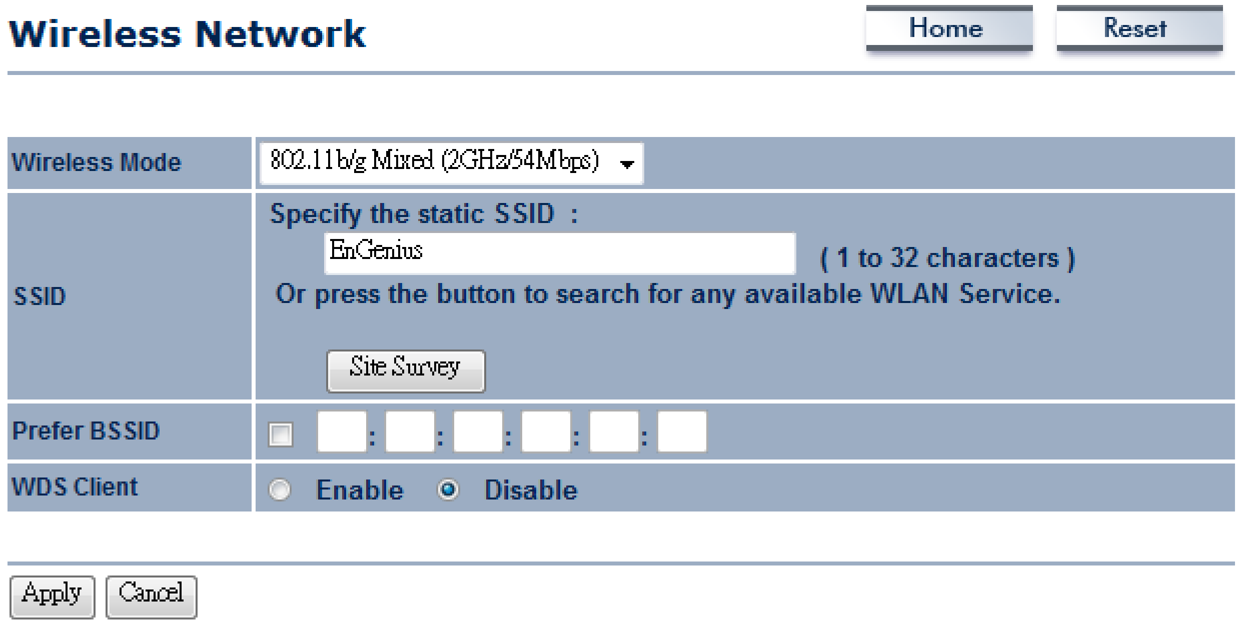
SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	☐
Station Separation	○ Enable ● Disable

Wireless Security

Security Mode	Disabled ▾

SSID	Specify the SSID for current profile.
VLAN ID	Specify the VLAN tag for current profile.
Suppressed SSID	Place a **Check** to hide the SSID. Client will not be able to see the broadcast SSID in Site Survey.
Station Separation	Select the Radio Button to allow / deny client to communicate each other.
Wireless Security	Please refer to the Wireless Security section.
Save / Cancel	Press **Save** to save the changes or **Cancel** to return previous settings.

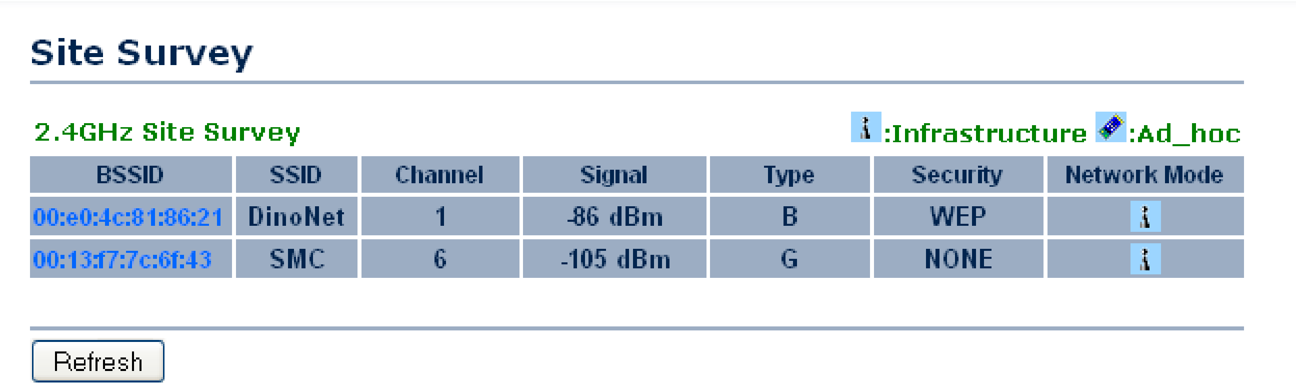
4.2.2 Client Bridge Mode



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.
Prefer BSSID	□ _ : _ : _ : _ : _ : _
WDS Client	○ Enable ● Disable

Wireless Mode	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11b, 802.11g Only, 802.11 b/g mixed and SuperG.
SSID	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
Site Survey	Using Site Survey to scan nearby APs and then select the AP to establish the connection.
Prefer BSSID	Specify the MAC address if known. Prefer BSSID text box will be automatically fill in when select an AP in the Site Survey.
WDS Client	Place a Radio button to Enable / Disable WDS Client.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.



Site Survey

2.4GHz Site Survey

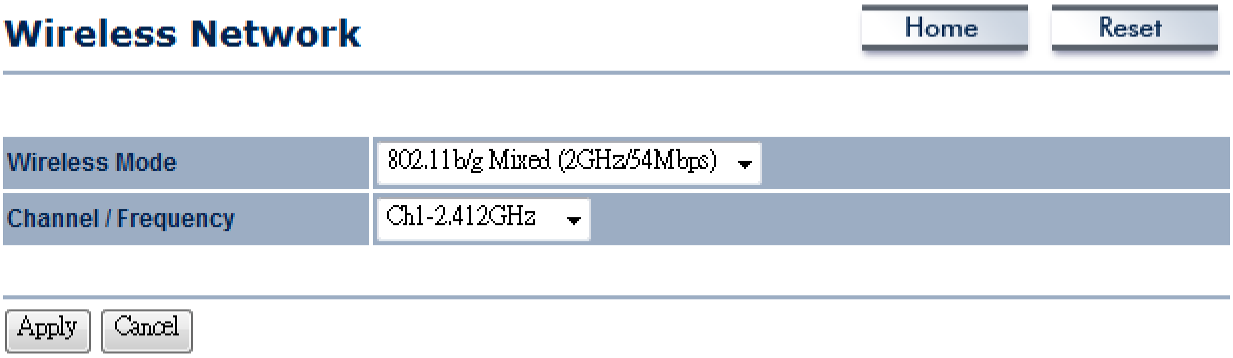
BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	i
00:13:f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	i

Profile	After Site Survey, webpage will display all nearby area's Access Point. Click the BSSID if you would like to connect with it.

Wireless Security	Please refer to the Wireless Security section.
Refresh	Press Refresh to scan again.

Auction: If the Access Point is suppressed its own SSID, SSID section will be blank, the SSID must be filled in manually.

4.2.3 WDS Bridge Mode



Wireless Network

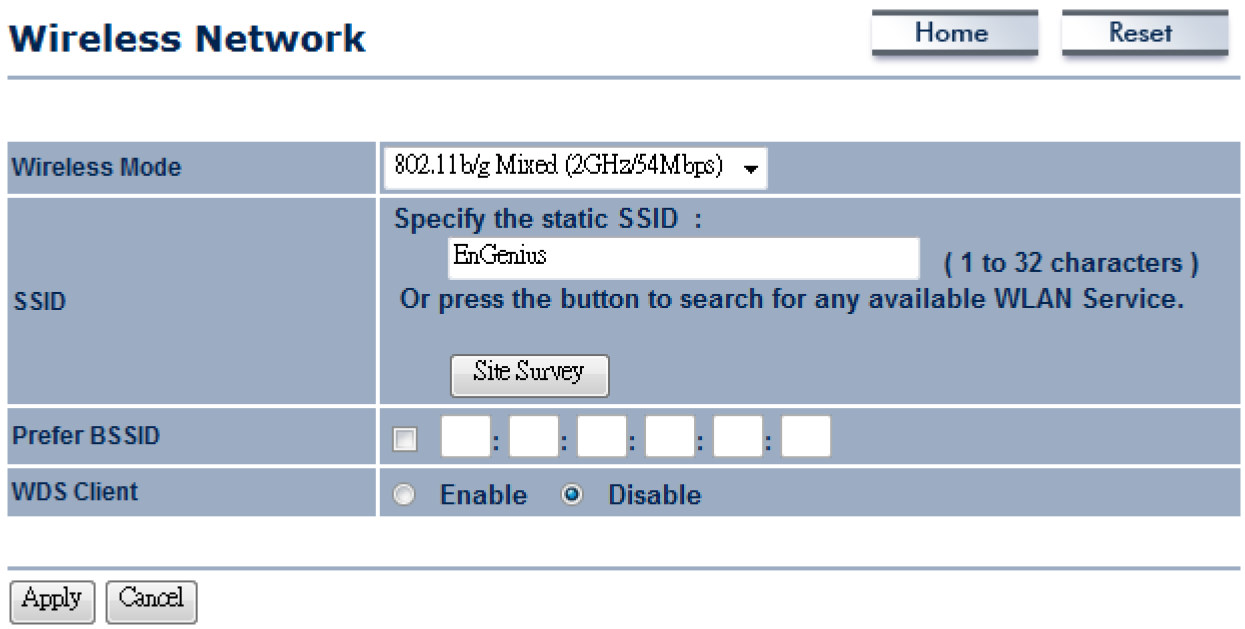
Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
Channel / Frequency	Ch1-2.412GHz

Wireless Mode	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11b, 802.11g Only, 802.11 b/g mixed and SuperG.
Channel / Frequency	The channel availability is based on the country's regulation.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

MAC Address	Enter the Access Point's MAC address that you would like to extend the wireless area into the MAC address filter.
Mode	Select Disable or Enable from the drop down list.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: The Access Point that you would like to extend the wireless area must enter your Access Point's MAC address. Not all Access Point supports this feature.

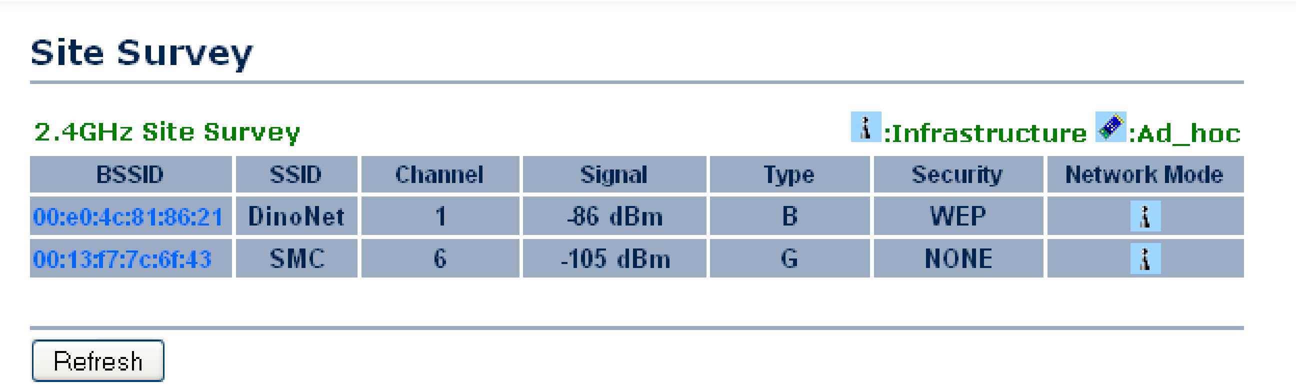
4.2.4 Repeater Mode



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	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11g Only, 802.11 b/g mixed and SuperG.
SSID	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
Site Survey	Using Site Survey to scan nearby APs and then select the AP to establish the connection.
Prefer BSSID	Specify the MAC address if known. Prefer BSSID text box will be automatically fill in when select an AP in the Site Survey.
WDS Client	Place a Radio button to Enable / Disable WDS Client.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.



Site Survey

2.4GHz Site Survey

:Infrastructure :Ad_hoc

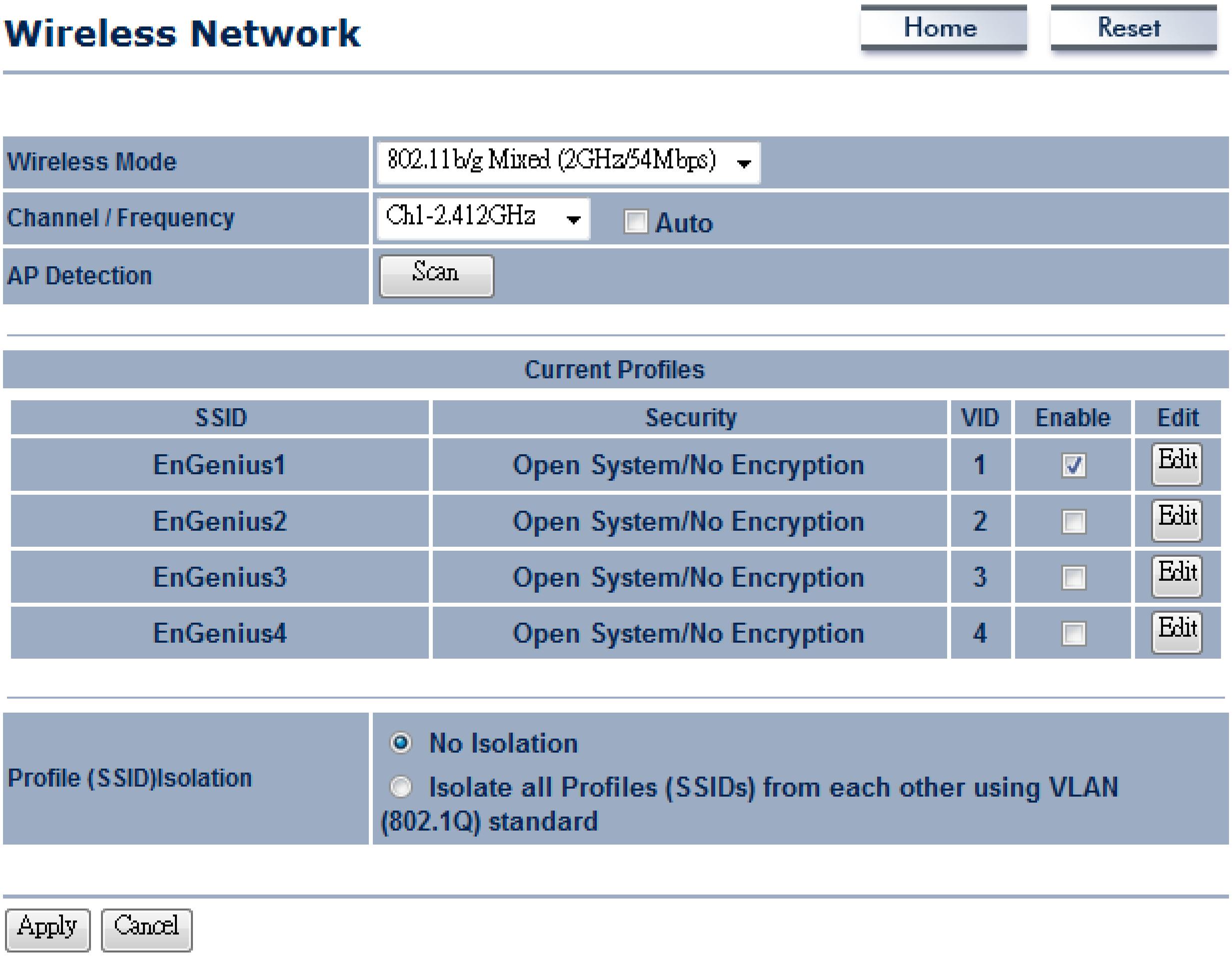
BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	
00:13:f7:7c:6f:43	SMC	6	-105 dBm	G	NONE	

Profile	After Site Survey, webpage will display all nearby area's Access Point. Click the BSSID if you would like to connect with it.

Wireless Security	Please refer to the Wireless Security section.
Refresh	Press Refresh to scan again.

Auction: If the Access Point is suppressed its own SSID, SSID section will be blank, the SSID must be filled in manually.

4.2.5 AP Router Mode



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

Current Profiles

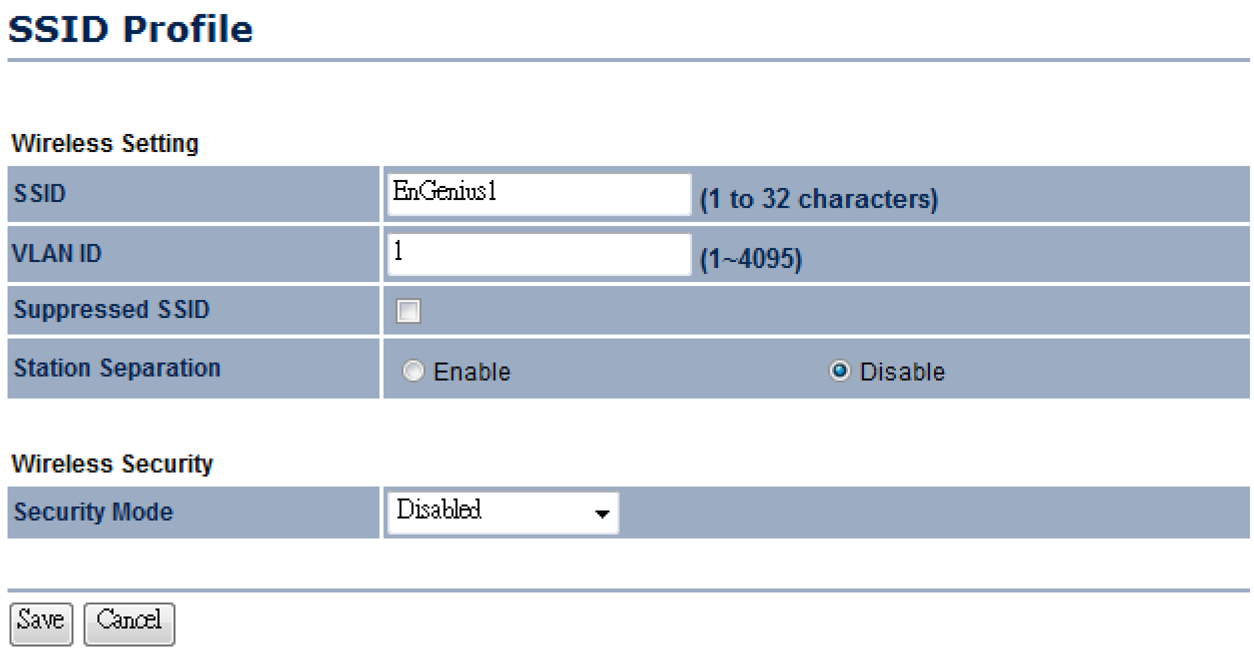
SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	☑	Edit
EnGenius2	Open System/No Encryption	2	□	Edit
EnGenius3	Open System/No Encryption	3	□	Edit
EnGenius4	Open System/No Encryption	4	□	Edit

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

Wireless Mode	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11b, 802.11g Only, 802.11 b/g mixed and SuperG.
Channel / Frequency	The channel availability is based on the country's regulation.
Auto	Place a **Check** to enable Auto channel selection.
AP Detection	AP Detection can help to select a best channel by scan nearby area.
Current Profile	Configure up to four different SSIDs, it can help to divide group of clients to access the network. Press **Edit** to configure the profile and place a **Check** to enable extra

	SSID.
Profile Isolation	Restricted Client to communicate with different VID by Selecting the Radio button.

Auction: SuperG is a special feature in M35. If the client does not support SuperG, it cannot establish a wireless connection successfully.



SSID Profile

Wireless Setting

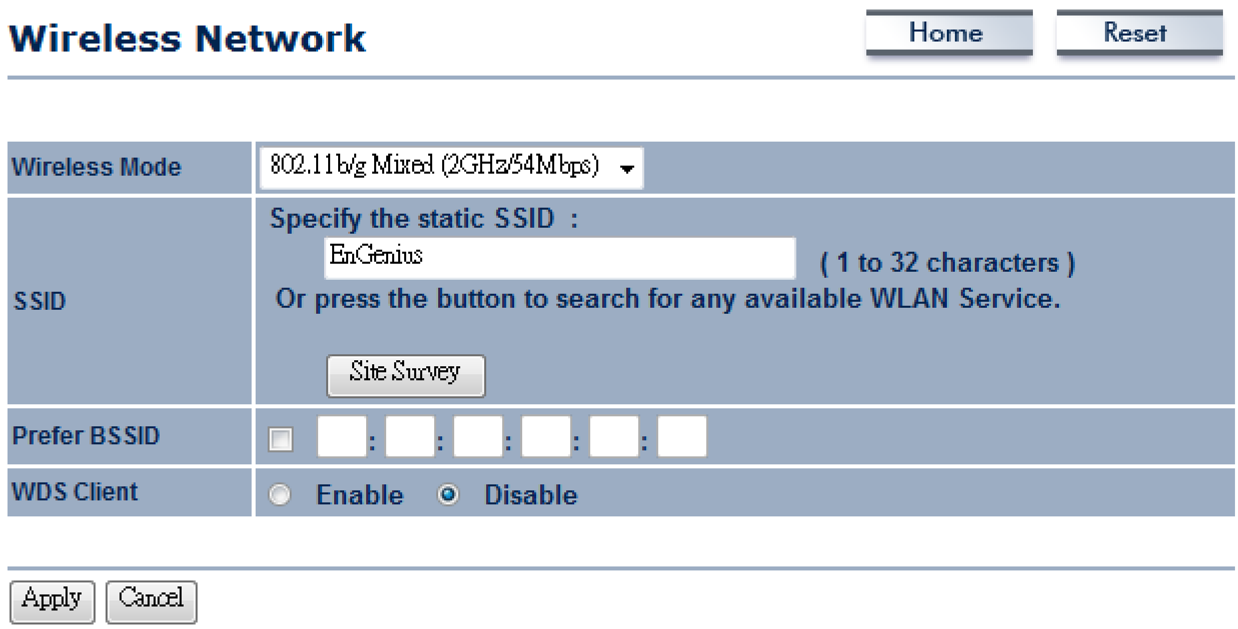
SSID	EnGenius1	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	□	
Station Separation	○ Enable	● Disable

Wireless Security

Security Mode	Disabled

SSID	Specify the SSID for current profile.
VLAN ID	Specify the VLAN tag for current profile.
Suppressed SSID	Place a **Check** to hide the SSID. Client will not be able to see the broadcast SSID in Site Survey.
Station Separation	Select the Radio Button to allow / deny client to communicate each other.
Wireless Security	Please refer to the Wireless Security section.
Save / Cancel	Press **Save** to save the changes or **Cancel** to return previous settings.

4.2.6 Client Router Mode



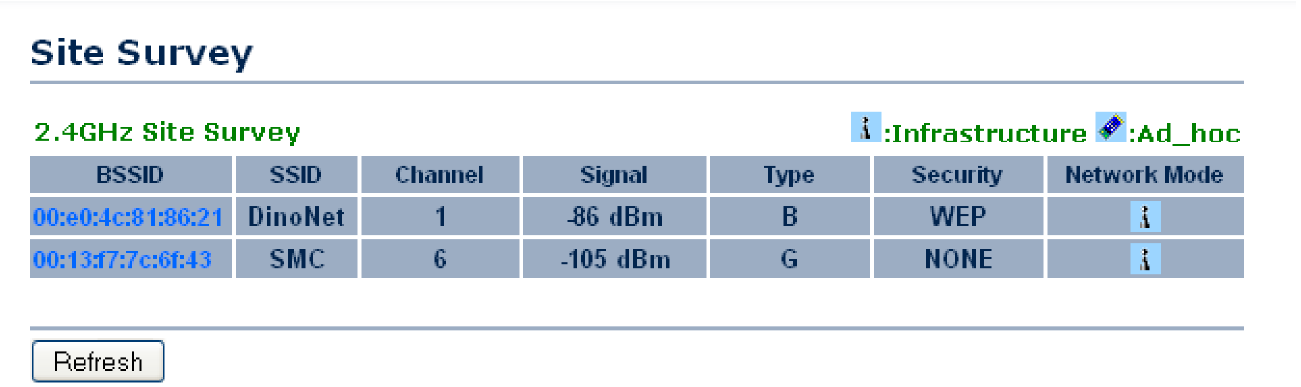
Wireless Network

Home | Reset

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

Apply | Cancel

Wireless Mode	Select the desired 802.11 standard modes or SuperG mode. There are four different modes and they are 802.11b, 802.11g Only, 802.11 b/g mixed and SuperG.
SSID	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
Site Survey	Using Site Survey to scan nearby APs and then select the AP to establish the connection.
Prefer BSSID	Specify the MAC address if known. Prefer BSSID text box will be automatically fill in when select an AP in the Site Survey.
WDS Client	Place a Radio button to Enable / Disable WDS Client.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.



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

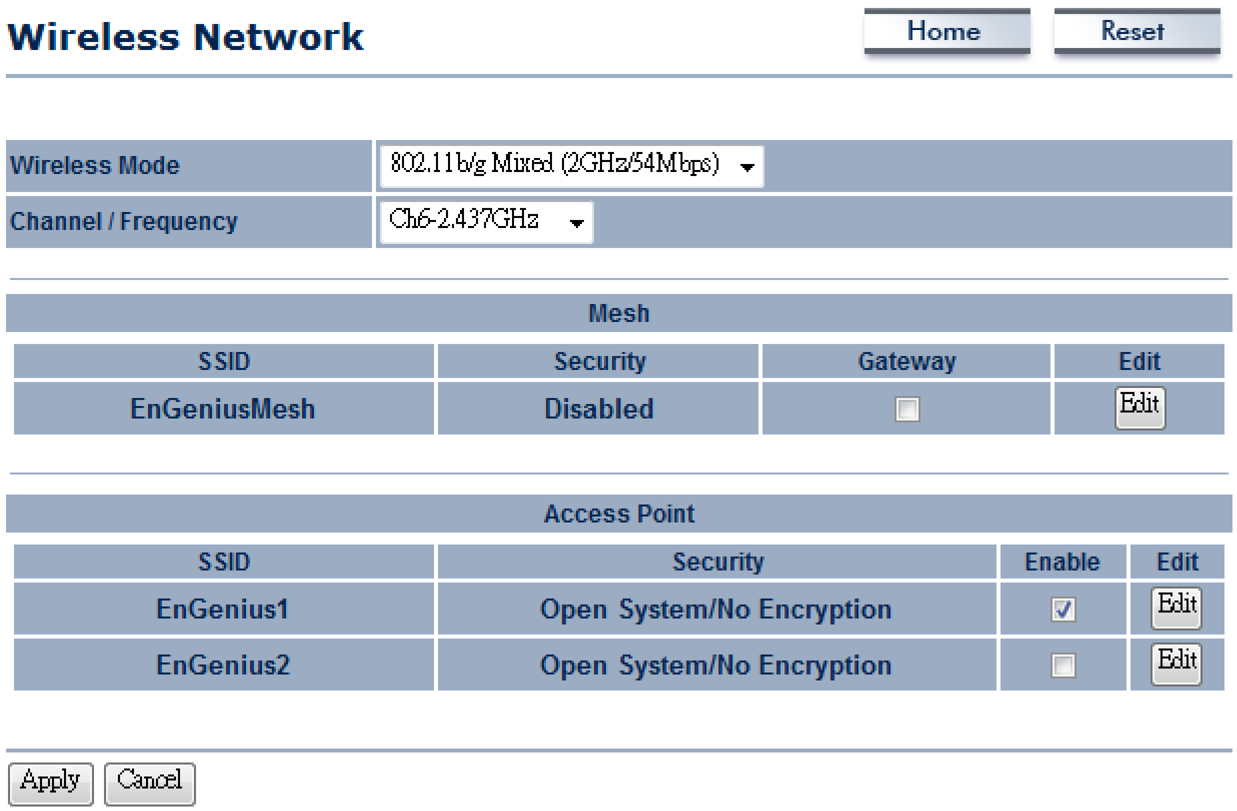
Refresh

Profile	After Site Survey, webpage will display all nearby area's Access Point. Click the BSSID if you would like to connect with it.

Wireless Security	Please refer to the Wireless Security section.
Refresh	Press Refresh to scan again.

Auction: If the Access Point is suppressed its own SSID, SSID section will be blank, the SSID must be filled in manually.

4.2.7 Mesh Mode



Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
Channel / Frequency	Ch6-2.437GHz

Mesh

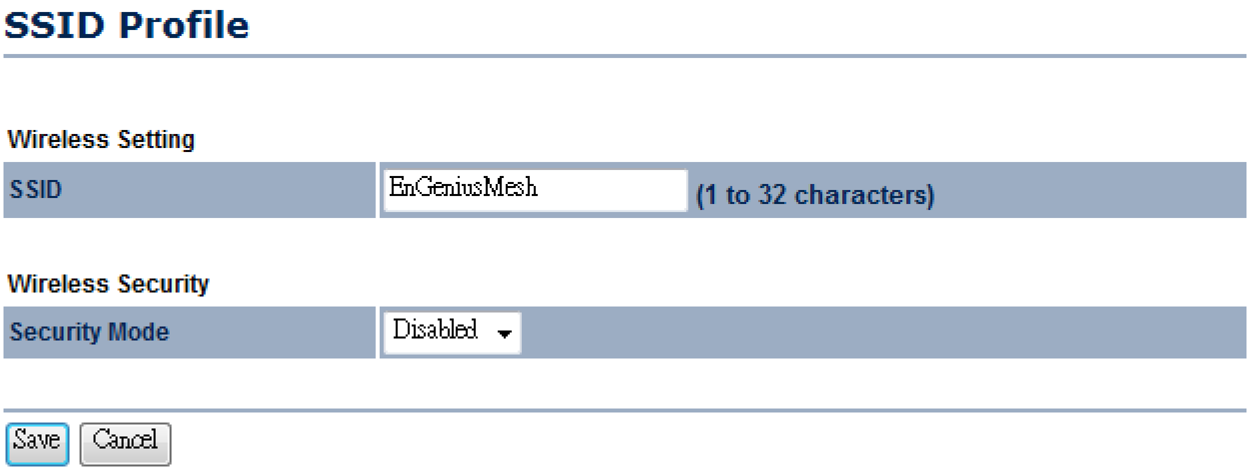
SSID	Security	Gateway	Edit
EnGeniusMesh	Disabled	□	Edit

Access Point

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

Wireless Mode	Select the desired 802.11 standard modes. There are three different modes and they are 802.11b, 802.11g Only, and 802.11 b/g mixed.
SSID	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
Channel / Frequency	The channel availability is based on the country's regulation.
Mesh Profile	Place a **Check** to act like gateway. Press **Edit** to configure the mesh profile and place a **Check** to enable extra SSID.
Access Point Profile	Configure up to two different SSIDs, it can help to divide group of clients to access the network. Press **Edit** to configure the profile and place a **Check** to enable extra SSID.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Mesh Profile


SSID Profile

Wireless Setting

SSID	EnGeniusMesh (1 to 32 characters)

Wireless Security

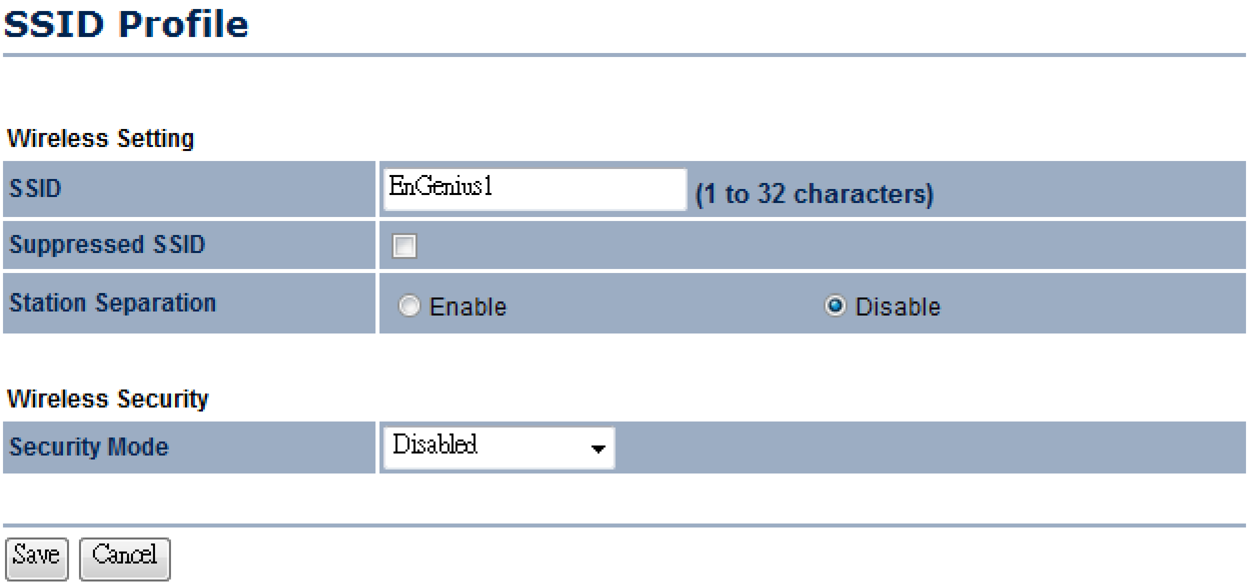
Security Mode	Disabled

SSID	Specify the name of the Mesh networking.
Wireless Security	Please refer to the Wireless Security section.
Save / Cancel	Press **Save** to save the changes or **Cancel** to return previous settings.

Note: Mesh Mode's Wireless Security only supports WEP encryption.

Auction: The SSID and security mode must be the same to the Mesh Network otherwise it cannot join the mesh network

Access Point Profile


SSID Profile

Wireless Setting

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

Wireless Security

Security Mode	Disabled

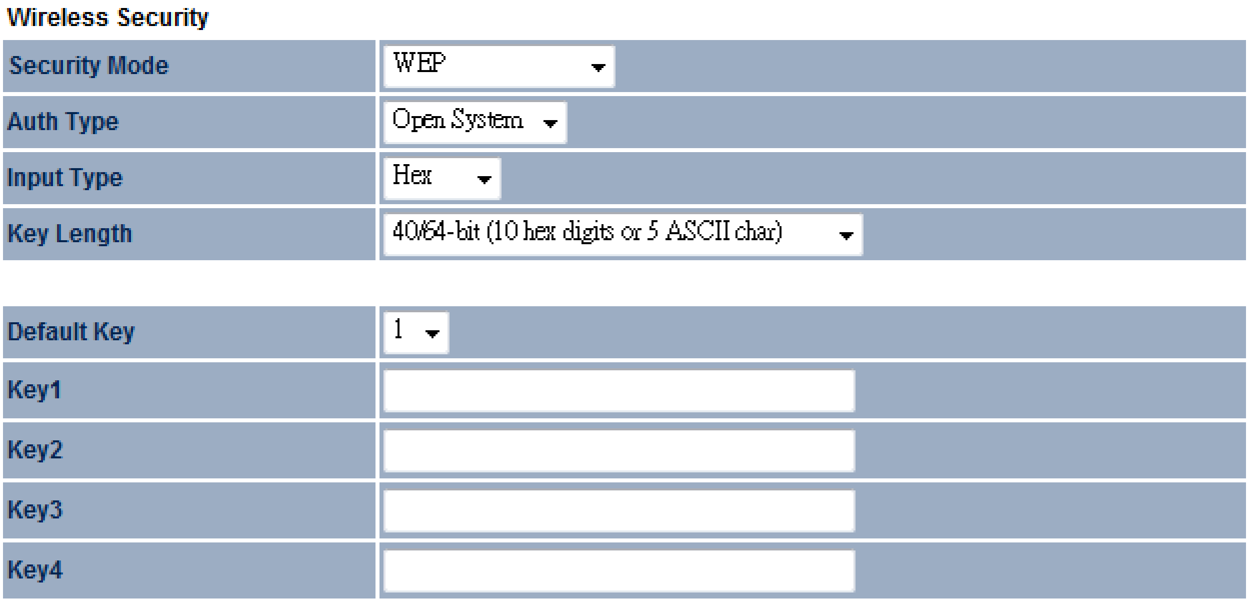
SSID	Specify the SSID for current profile.
Suppressed SSID	Place a **Check** to hide the SSID. Client will not be able to see the broadcast SSID in Site Survey.

Station Separation	Select the Radio Button to allow / deny client to communicate each other.
Wireless Security	Please refer to the Wireless Security section.
Save / Cancel	Press **Save** to save the changes or **Cancel** to return previous settings.

4.3 Wireless Security Settings

Wireless Security Settings section will guide you to the entire Security modes configuration: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed.
We strongly recommend that uses WPA2-PSK as your security settings.

4.3.1 WEP

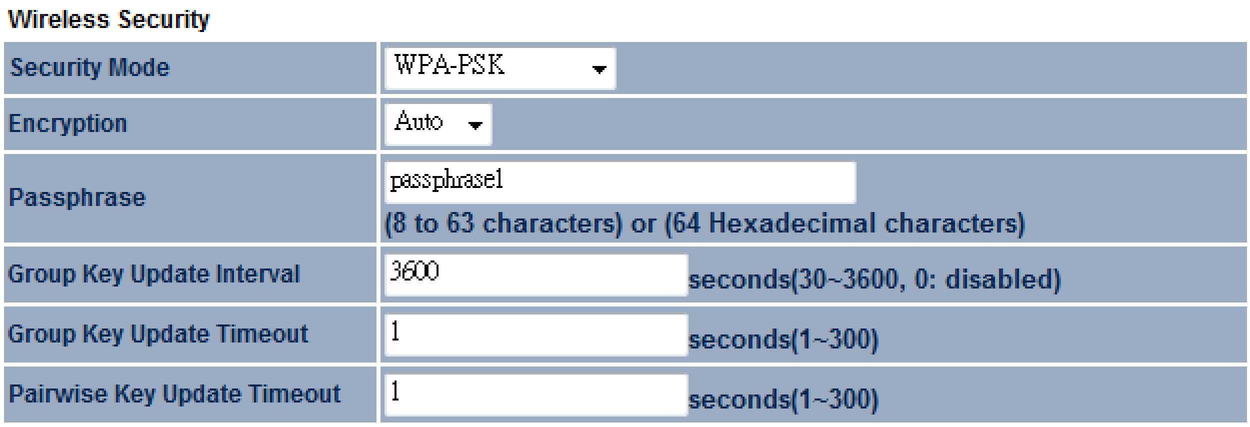


Wireless Security

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	

Security Mode	Select **WEP** from the drop down list to begin the configuration.
Auth Type	Select Auth Type in **Open System** or **Shared**.
Input Type	Select Input Type in **Hex** or **ASCII**.
Key Length	Select Key Length in 64/128/152 bit password length.
Default Key	Select the default index key for wireless security.
Key1	Specify password for security key index No.1.
Key2	Specify password for security key index No.2.
Key3	Specify password for security key index No.3.
Key4	Specify password for security key index No.4.

4.3.2 WPA-PSK

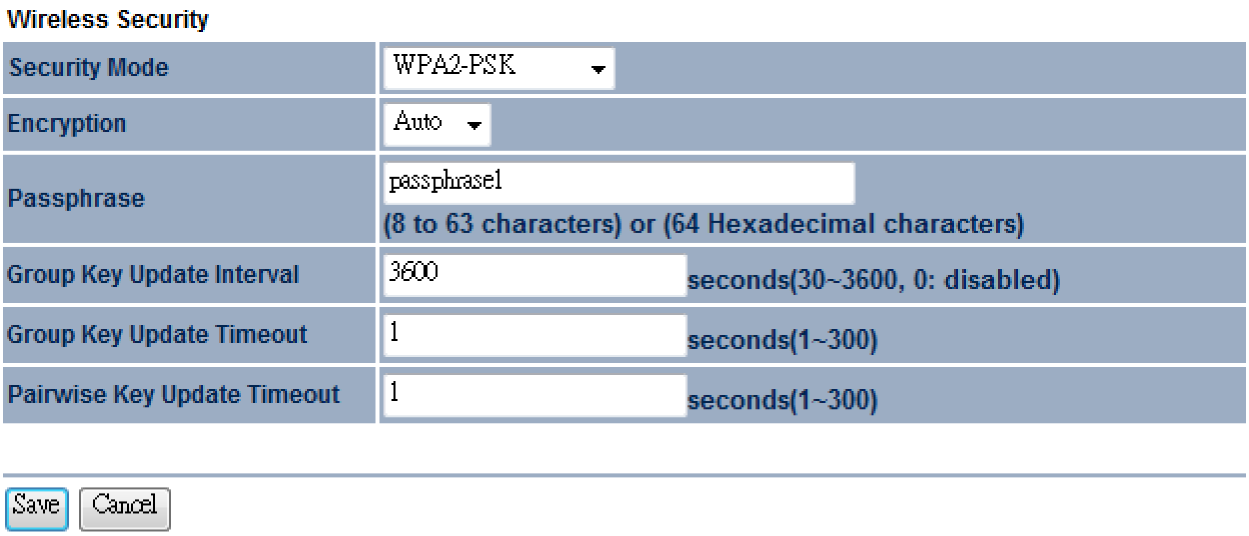


Wireless Security

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)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)

Security Mode	Select **WPA-PSK** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Passphrase	Specify the security password.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.

4.3.3 WPA2-PSK

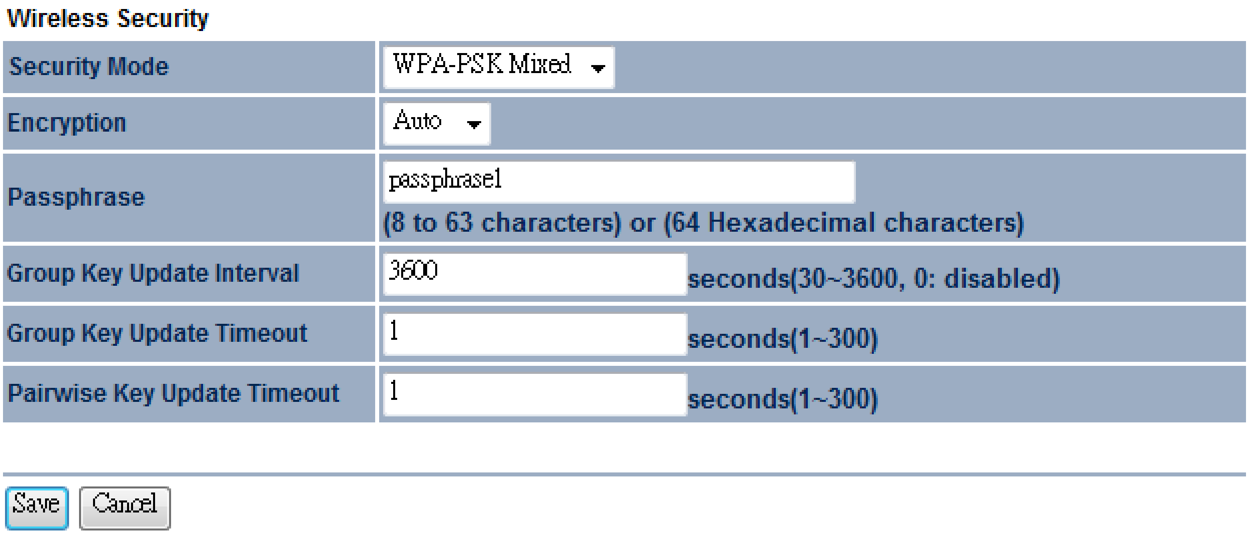


Wireless Security

Security Mode	WPA2-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)

Security Mode	Select **WPA2-PSK** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Passphrase	Specify the security password.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.

4.3.4 WPA-PSK Mixed



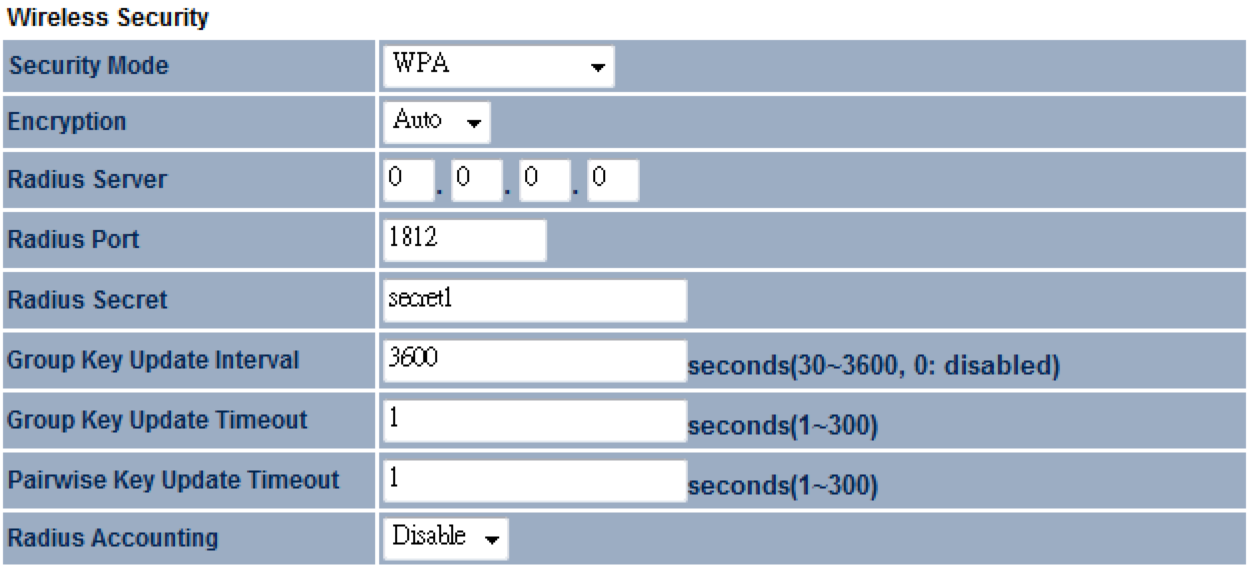
Wireless Security

Security Mode	WPA-PSK Mixed
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)

Security Mode	Select **WPA-PSK Mixed** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Passphrase	Specify the security password.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.

Auction: WPA-PSK Mixed means it allow both WPA-PSK and WPA2-PSK security types to establish wireless connection.

4.3.5 WPA

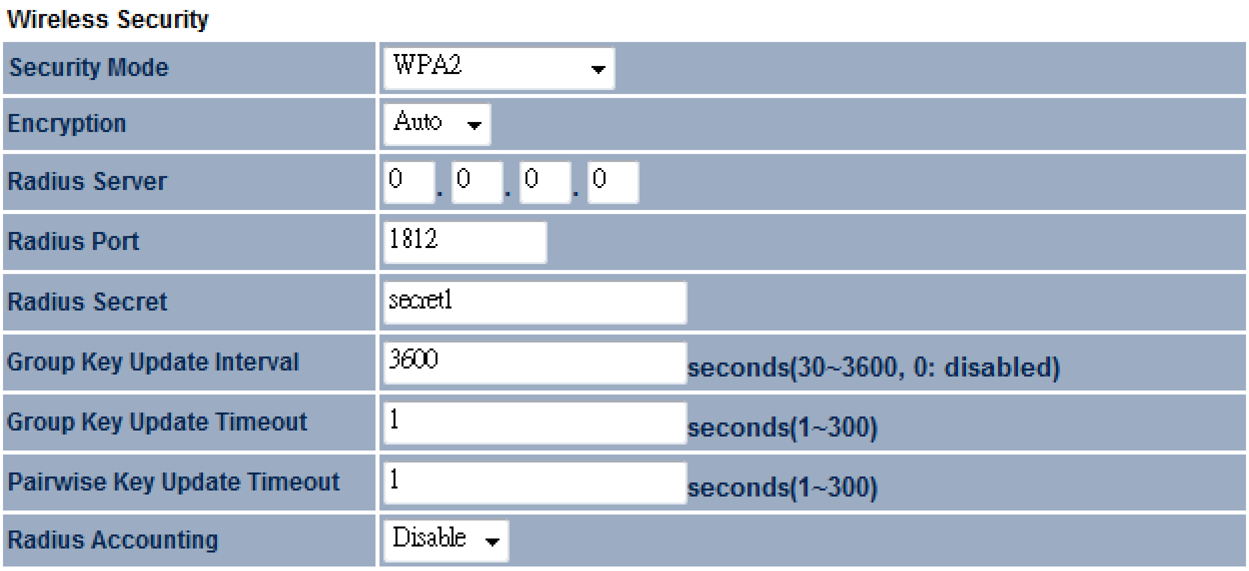


Wireless Security

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)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable

Security Mode	Select **WPA** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Radius Server	Specify Radius Server IP Address.
Radius Port	Specify Radius Port number, the default port is 1812.
Radius Secret	Specify Radius Secret that is given by the Radius Server.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.
Radius Accounting	Select **Enable** or **Disable** Radius Accounting. The detail of Radius Accounting is at next section.

4.3.6 WPA2

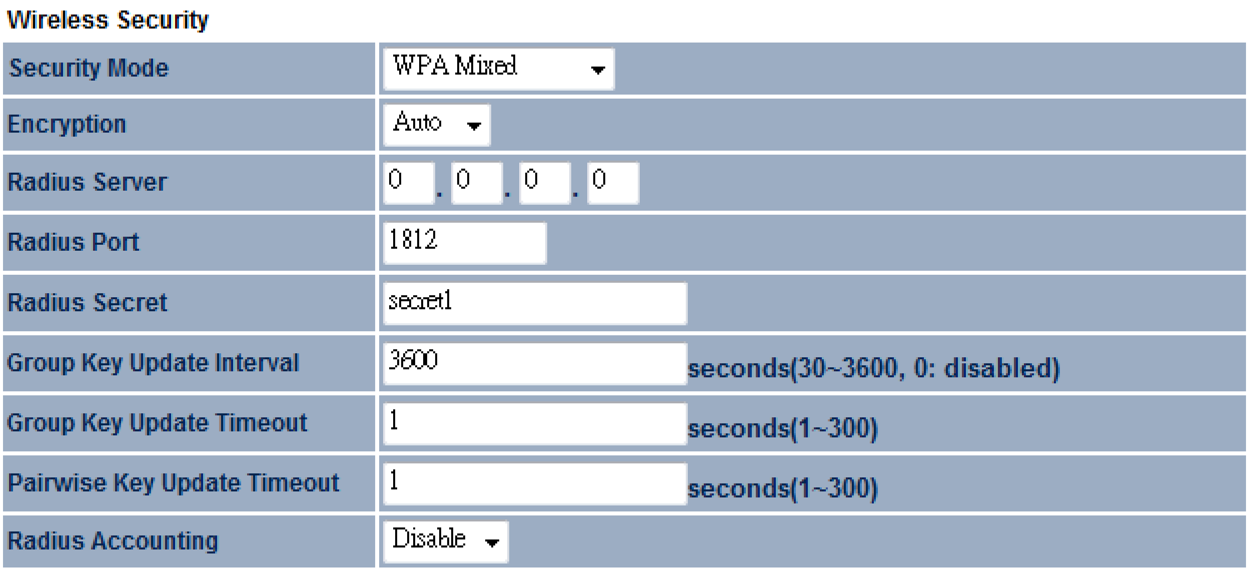


Wireless Security

Security Mode	WPA2
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable

Security Mode	Select **WPA2** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Radius Server	Specify Radius Server IP Address.
Radius Port	Specify Radius Port number, the default port is 1812.
Radius Secret	Specify Radius Secret that is given by the Radius Server.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.
Radius Accounting	Select **Enable** or **Disable** Radius Accounting. The detail of Radius Accounting is at next section.

4.3.7 WPA Mixed



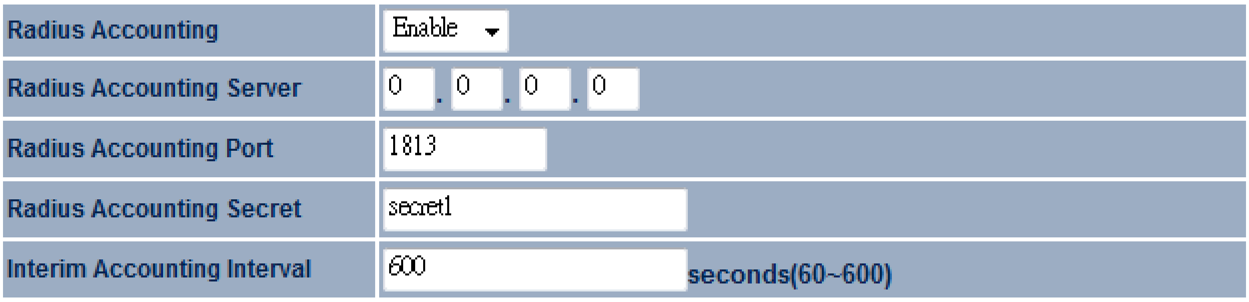
Wireless Security

Security Mode	WPA Mixed
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable

Security Mode	Select **WPA Mixed** from the drop down list to begin the configuration.
Encryption	Select **Auto**, **TKIP** or **AES** for Encryption type.
Radius Server	Specify Radius Server IP Address.
Radius Port	Specify Radius Port number, the default port is 1812.
Radius Secret	Specify Radius Secret that is given by the Radius Server.
Group Key Update Interval	Specify Group Key Update Interval time.
Group Key Update Timeout	Specify Group Key Update Timeout time.
Pairwise Key Update Interval	Specify Pairwise Key Update Timeout time.
Radius Accounting	Select **Enable** or **Disable** Radius Accounting. The detail of Radius Accounting is at next section.

Auction: WPA Mixed means it allow both WPA and WPA2 security types to establish wireless connection.

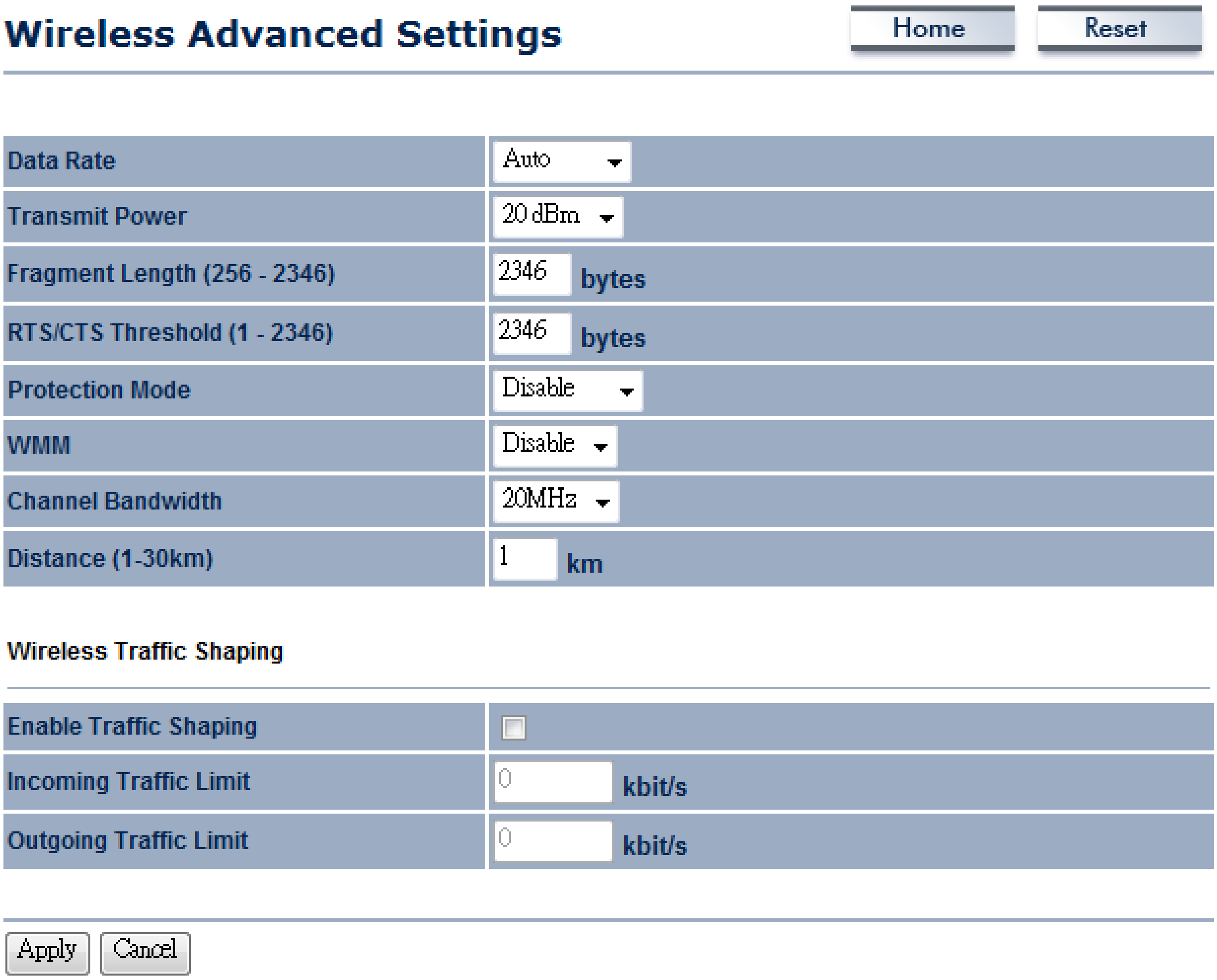
4.3.8 Radius Accounting



Radius Accounting	Enable
Radius Accounting Server	0 . 0 . 0 . 0
Radius Accounting Port	1813
Radius Accounting Secret	secret1
Interim Accounting Interval	600 seconds(60~600)

Radius Accounting	Select **Enable** to begin configuration of Radius Accounting.
Radius Accounting Server	Specify Radius Accounting Server IP.
Radius Accounting Port	Specify Radius Accounting Server IP. The default port is 1813.
Radius Accounting Secret	Specify Radius Accounting Server Secret that is given by the Radius Accounting Server.
Radius Accounting Interval	Specify Radius Accounting Interval for updating information.

4.4 Wireless Advanced Settings



Wireless Advanced Settings

Data Rate	Auto
Transmit Power	20 dBm
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

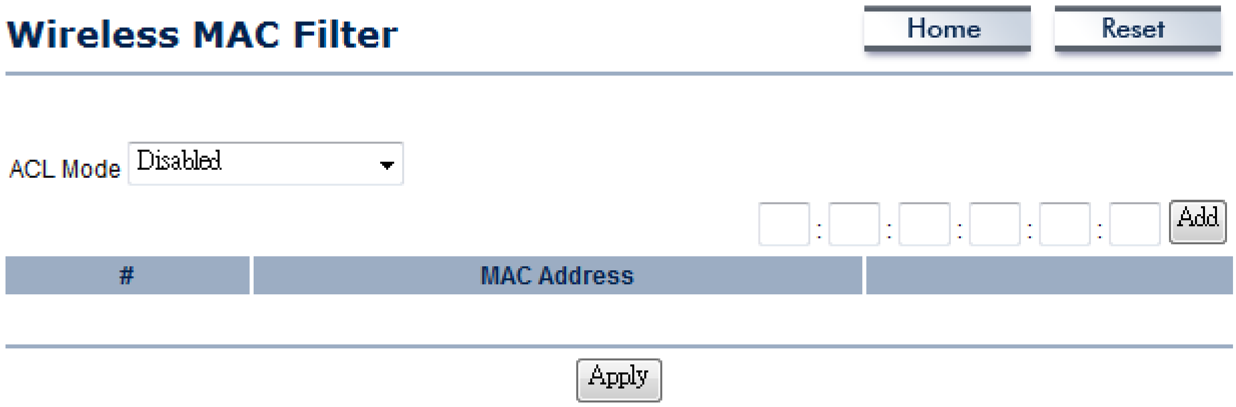
Data Rate	Select Data Rate from the drop down list. Data rate will affect the efficiency of the throughput. If the data rate is set to a small number, the lower through will get but it can transmit to longer distance.
Transmit Power	Select Transmit Power to increase or decrease Transmit Power. Higher transmit power will sometimes cause unable to connect to the network. On the other hand, the lower transmit power will cause client unable to connect to the device.
Fragment Length	Specify package size during transmission. If large amount of client are accessing to the network, specify small number of the fragment length in order to avoid collision.
RTS/CTS Threshold	Specify Threshold package size for RTC/CTS. Using small number of the threshold will cause RTS/CTS packets to be sent more often to consuming more of the available bandwidth. In addition, if the heavy load traffic occurs, the wireless network can be recovered easily from interferences or collisions.
Protection Mode	Select **Disable** or **Enable** Protection Mode. If there are large amount of error occur during the transmission, please enable the protect mode otherwise protect mode should remain disable.

WMM	Select **Disable** or **Enable** WMM function. WMM is based on the four Access Categories: voice, video, best effort and background. WMM function is not used to guarantee transmission speed.
Channel Bandwidth	Select Channel Bandwidth from the drop down list. Decrease channel bandwidth may cause lower throughput but less collision.
Distance	Specify distance rage between AP and Clients. Longer distance may lose high connection speed.
Wireless Traffic Shaping	Place a **Check** to enable Wireless Traffic Shaping function.
Incoming Traffic Limit	Specify the wireless transmission speed for downloading.
Outgoing Traffic Limit	Specify the wireless transmission speed for uploading.

Auction: Changing Wireless Advanced Settings may cause insufficient wireless connection quality. Please remain all settings as default unless you have acknowledged all changing that you have made.

4.5 Wireless MAC Filter

Wireless MAC Filters is used to Allow or Deny wireless clients, by their MAC addresses, accessing the Network. You can manually add a MAC address to restrict the permission to access M35. The default setting is Disable Wireless MAC Filters.



ACL Mode: Disabled

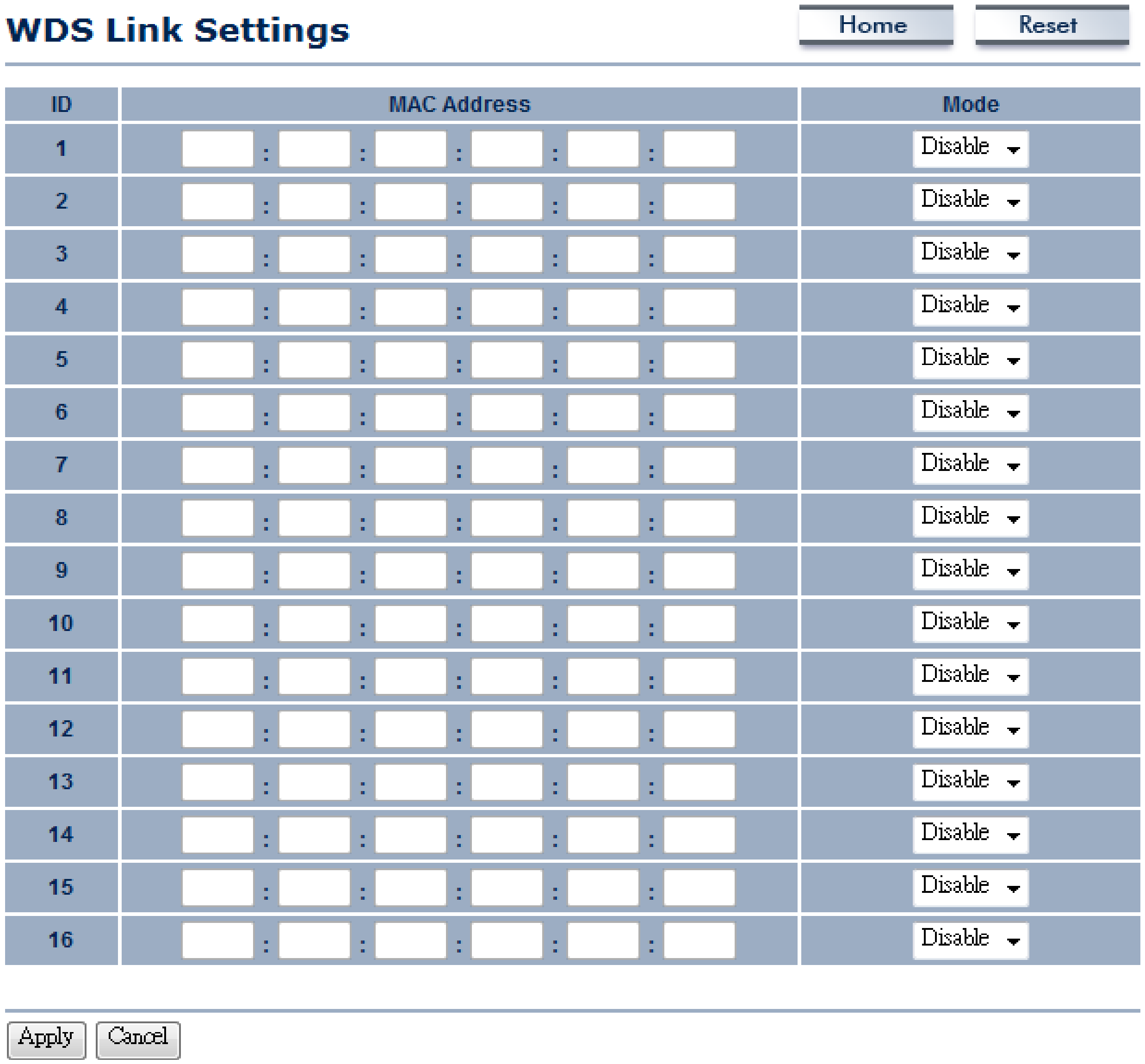
#	MAC Address	

0.

ACL Mode	ACL Mode can help to deny or allow certain Client to access the network. Select Disable, Deny MAC in the list or Allow MAC in the list from the drop down list.
MAC Address Filter	Specify the MAC address manually.
Add	Press **Add** to add the MAC address in the table.
Apply	Press **Apply** to apply the changes.

4.6 WDS Link Settings

WDS Link Settings is used to establish a connection between Access Points but the device is not losing Access Point function. AP has WDS function can extend the wireless coverage and allow LANs to communicate each other.



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	Enter the Access Point's MAC address that you would like to extend the wireless area.
Mode	Select Disable or Enable from the drop down list.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: The Access Point that you would like to extend the wireless area must enter your Access Point's MAC address. Not all Access Point supports this feature.

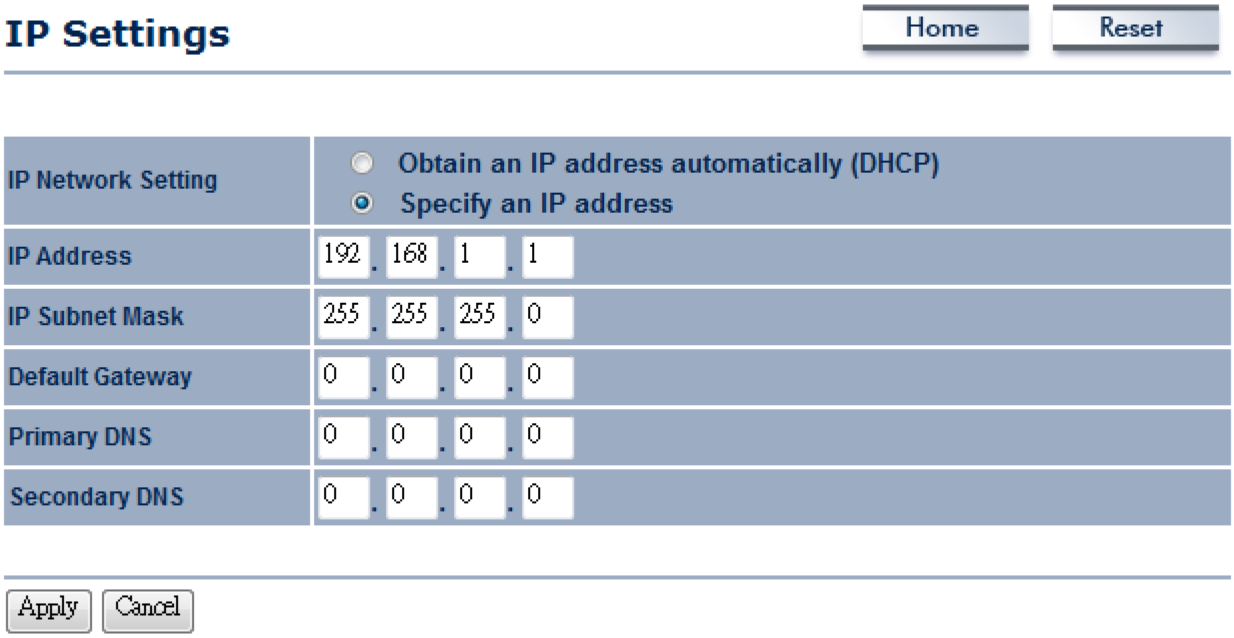
5 LAN Setup

This section will guide you to the Local Area Network (LAN) settings

5.1 IP Settings

This section is only available for **Non-Router Mode**. IP Settings allows you to LAN port IP address of the M35.

Auction: Changing LAN IP Address will change LAN Interface IP address. Webpage will automatically redirect to the new IP address after Apply.

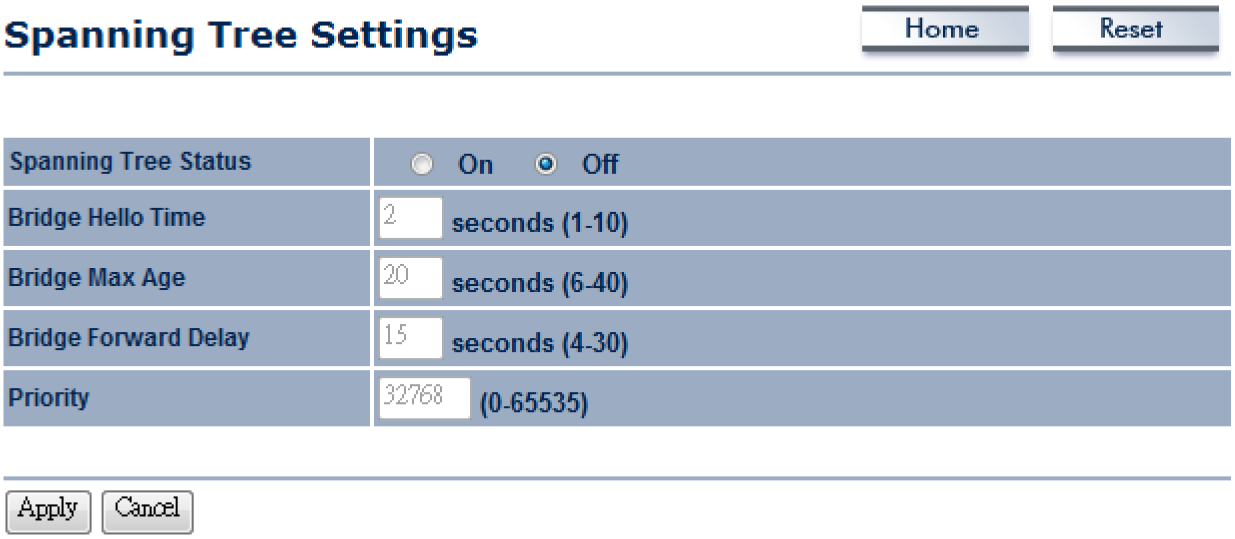


IP Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

IP Network Setting	Select Radio button for **Obtain an IP address automatically** or **Specify an IP address**.
IP Address	Specify LAN port IP address.
IP Suet Mask	Specify Subnet Mask.
Default Gateway	Specify Default Gateway
Primary DNS	Specify Primary DNS
Secondary DNS	Specify Secondary DNS
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: Obtain an IP address automatically is not a DHCP server. It means automatically get IP address when device connected to a device which has DHCP server.

5.2 Spanning Tree Settings



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	Select the Radio button to On or Off Spanning Tree function.
Bridge Hello Time	Specify Bridge Hello Time in second.
Bridge Max Age	Specify Bridge Max Age in second.
Bridge Forward Delay	Specify Bridge Forward Delay in second.
Priority	Specify the Priority number. Smaller number has greater priority.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

6 Router Settings

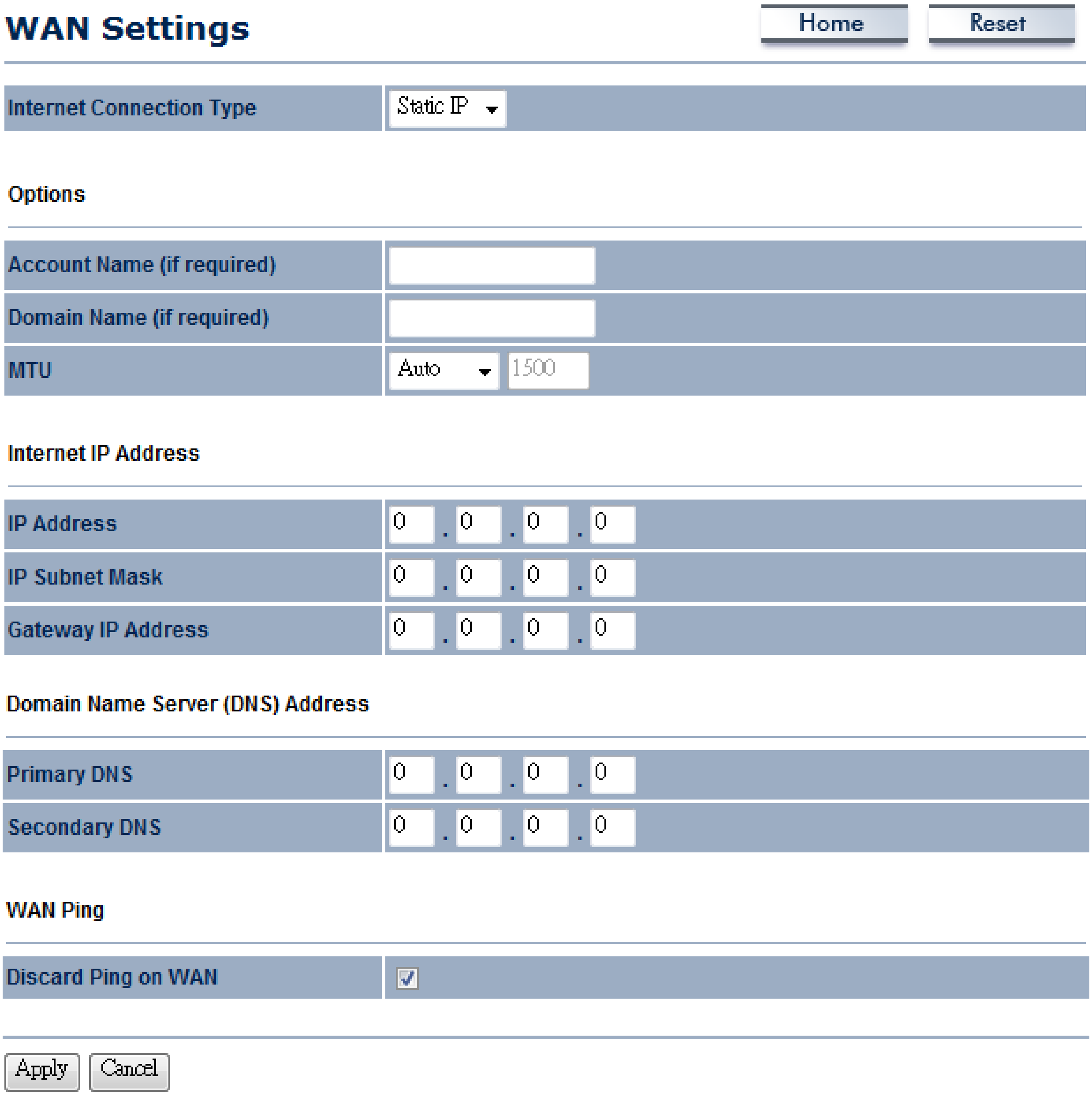
This section is only available for **AP Router Mode** and **Client Router Mode**.

6.1 WAN Settings

There are four different types of WAN connection: Static IP, DHCP, PPPoE and PPTP. Please contact your ISP to select the connection type.

6.1.1 Static IP

Select Static IP in WAN connection if your ISP gives all the information about IP address, Subnet Mask, Default Gateway, Primary DNS and Secondary DNS.



WAN Settings

Internet Connection Type	Static IP

Options

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

Internet IP Address

IP Address	0 . 0 . 0 . 0
IP Subnet Mask	0 . 0 . 0 . 0
Gateway IP Address	0 . 0 . 0 . 0

Domain Name Server (DNS) Address

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

WAN Ping

Discard Ping on WAN	☑

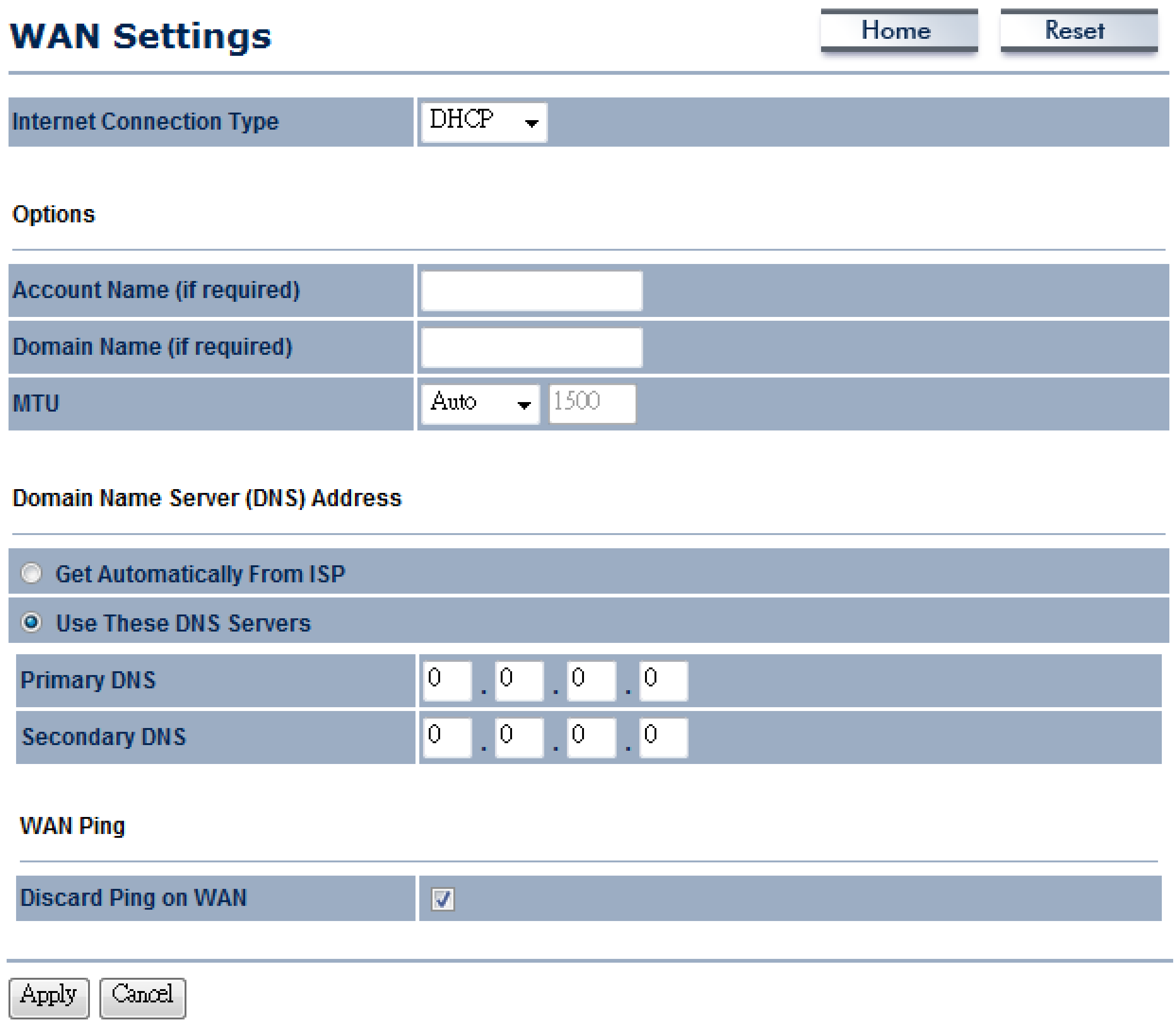
Internet Connection Type	Select **Static IP** to begin configuration of the Static IP connection.
Account Name	Specify Account Name that is provided by ISP.
Domain Name	Specify Domain Name that is provided by ISP.
MTU	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
IP Address	Specify WAN port IP address.
IP Subnet Mask	Specify WAN IP Subnet Mask.
Gateway IP Address	Specify WAN Gateway IP address.
Primary DNS	Specify Primary DNS IP.
Secondary DNS	Specify Secondary DNS IP.
Discard Ping on WAN	Place a Check to Enable or Disable ping from WAN.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: 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.

6.1.2 DHCP (Dynamic IP)

Select DHCP as your WAN connection type to obtain your IP address automatically. You will need to enter Account Name as your hostname and DNS (Optional).



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

WAN Ping

Discard Ping on WAN	☑

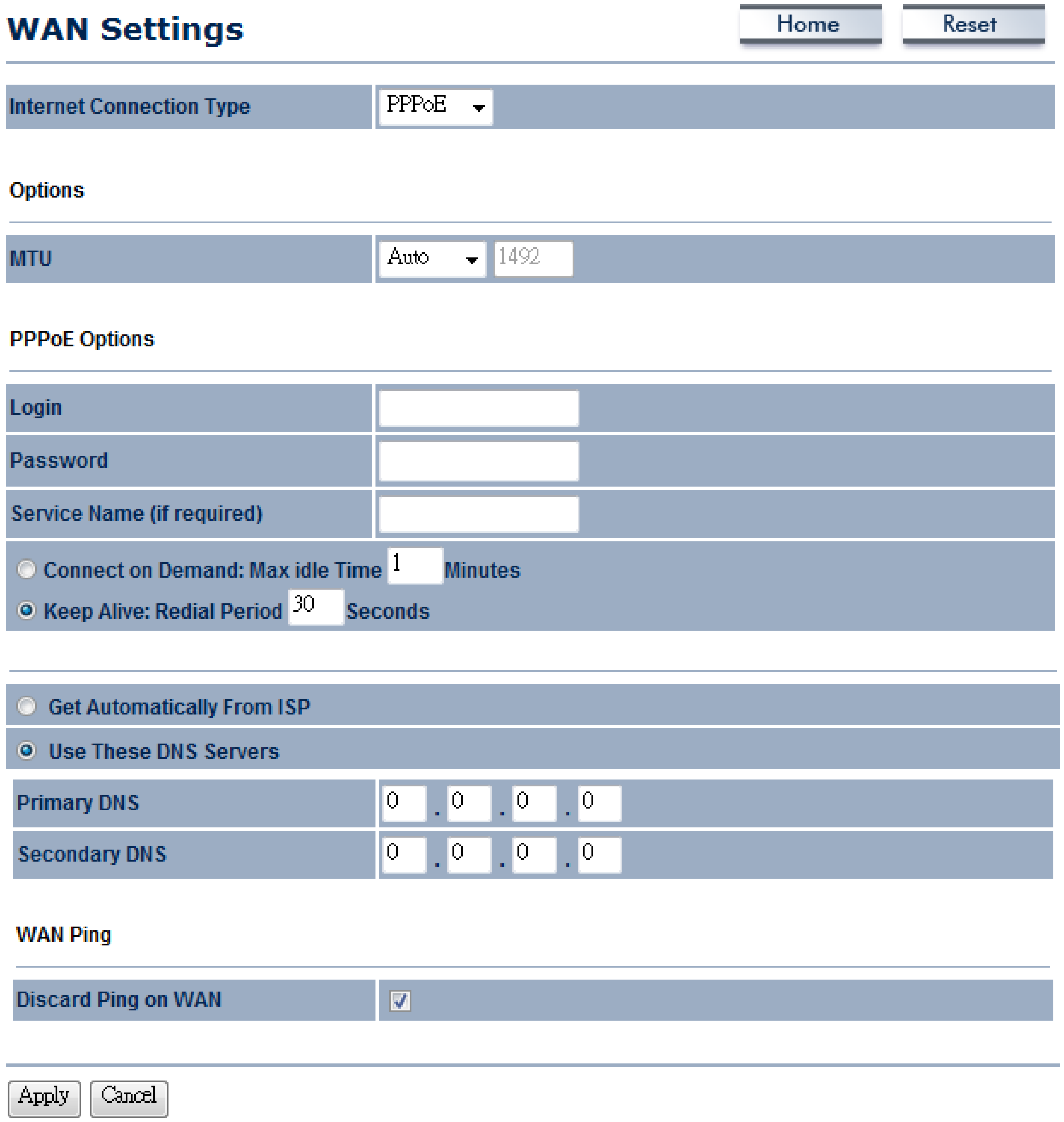
Internet Connection Type	Select **DHCP** to begin configuration of the DHCP connection.
Account Name	Specify Account Name that is provided by ISP.
Domain Name	Specify Domain Name that is provided by ISP.
MTU	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
Get Automatically From ISP	Select the Radio button for get the DNS automatically from DHCP server.
Use These DNS Servers	Select the Radio button for setup the **Primary DNS** and **Secondary DNS** servers

	manually.
Discard Ping on WAN	Place a Check to Enable or Disable ping from WAN.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: 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.

6.1.3 PPPoE (Point-to-Point Protocol over Ethernet)

Select PPPoE as your WAN connection type if your ISP provides Username and Password. PPPoE is a DSL service and please remove your PPPoE software from your computer, the software is not worked in M35.



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

○ Get Automatically From ISP
● Use These DNS Servers

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

WAN Ping

Discard Ping on WAN	☑

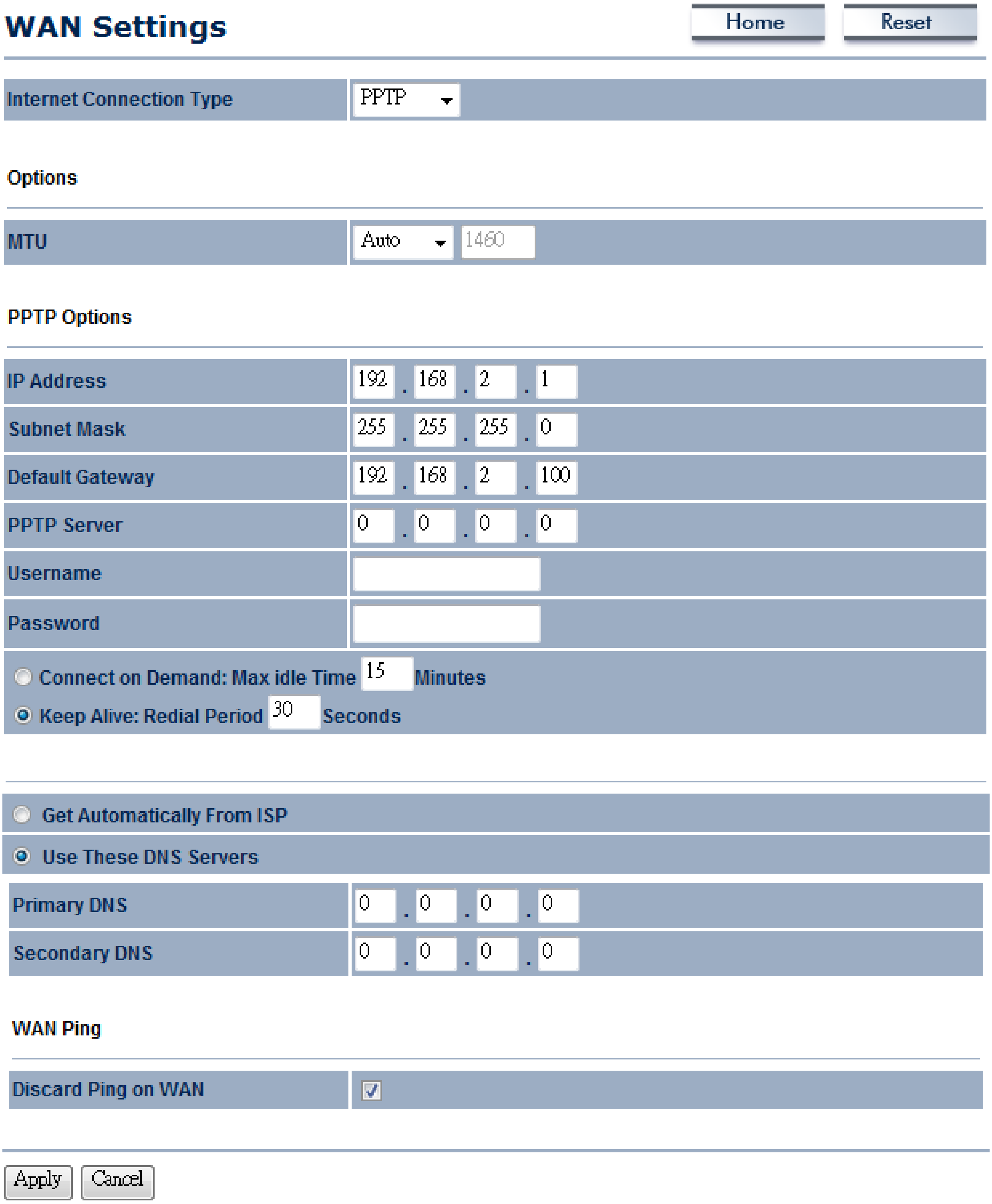
Internet Connection Type	Select **PPPoE** to begin configuration of the PPPoE connection.
MTU	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
Login	Specify the **Username** that is given by your ISP.
Password	Specify the **Password** that is given by your ISP.
Service Name	Specify the **Service Name** that is given by your ISP.

Connect on Demand	Select the Radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
Keep Alive	Select the Radio button to keep internet connection always on. Specify the redial period once the internet lose connection.
Get Automatically From ISP	Select the Radio button for get the DNS automatically from DHCP server.
Use These DNS Servers	Select the Radio button for setup the **Primary DNS** and **Secondary DNS** servers manually.
Discard Ping on WAN	Place a Check to Enable or Disable ping from WAN.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: 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.

6.1.4 PPTP (Point-to-Point Tunneling Protocol)

Select PPTP as your WAN connection type if your ISP provides information about IP Address, Subnet Mask, Default Gateway (Optional), DNS (Optional), Server IP, Username, and Password.



Internet Connection Type	PPTP

Options

MTU	Auto 1460

PPTP Options

IP Address	192 . 168 . 2 . 1
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 2 . 100
PPTP Server	0 . 0 . 0 . 0
Username	
Password	

○ Connect on Demand: Max idle Time 15 Minutes

● Keep Alive: Redial Period 30 Seconds

○ Get Automatically From ISP

● Use These DNS Servers

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

WAN Ping

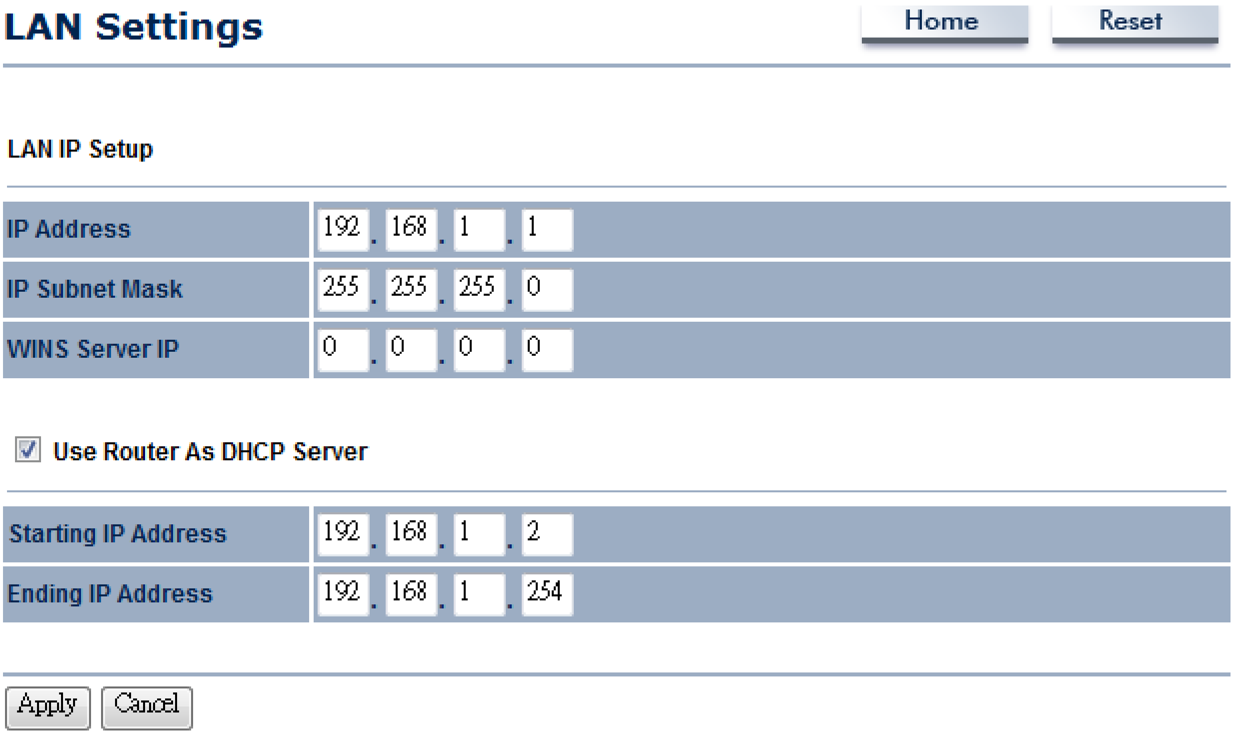
Discard Ping on WAN	☑

Internet Connection Type	Select **PPTP** to begin configuration of the PPTP connection.

MTU	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
IP Address	Specify WAN port IP address.
IP Subnet Mask	Specify WAN IP Subnet Mask.
Gateway IP Address	Specify WAN Gateway IP address.
PPTP Server	Specify PPTP Server IP address.
Username	Specify the **Username** that is given by your ISP.
Password	Specify the **Password** that is given by your ISP.
Connect on Demand	Select the Radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
Keep Alive	Select the Radio button to keep internet connection always on. Specify the redial period once the internet lose connection.
Get Automatically From ISP	Select the Radio button for get the DNS automatically from DHCP server.
Use These DNS Servers	Select the Radio button for setup the **Primary DNS** and **Secondary DNS** servers manually.
Discard Ping on WAN	Place a Check to Enable or Disable ping from WAN.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: 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.

6.2 LAN Settings (Router Mode)



LAN Settings

Home Reset

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

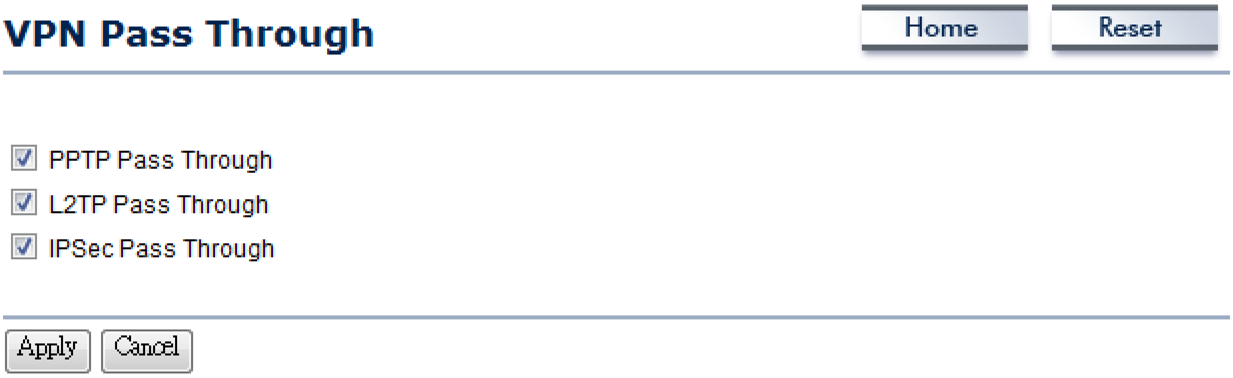
Starting IP Address	192 . 168 . 1 . 2
Ending IP Address	192 . 168 . 1 . 254

Apply Cancel

IP Address	Specify LAN port IP address.
IP Subnet Mask	Specify LAN IP Subnet Mask.
WINS Server IP	Specify WINS Server IP.
Use Router As DHCP Server	Place a **Check** to enable DHCP server.
Starting IP Address	Specify DHCP server starting IP address.
Ending IP Address	Specify DHCP server ending IP address.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

6.3 VPN Pass Through

VPN Pass Through is on top of an existing network by passing or restricting certain protocol. This function can help to provide a secure private network.

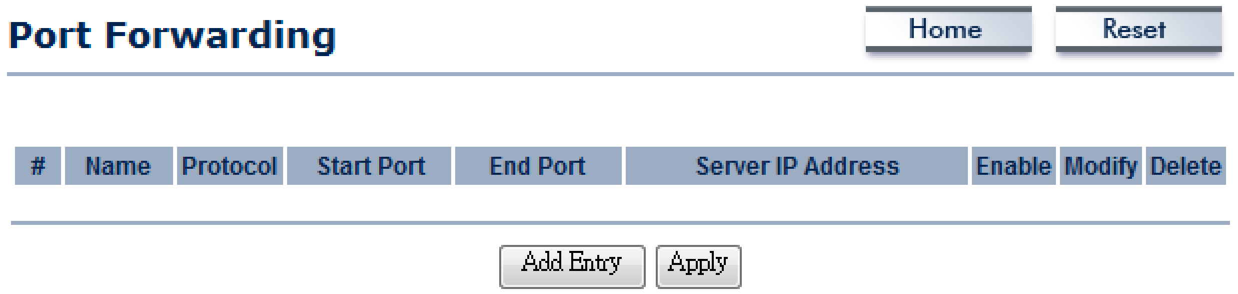


☑ PPTP Pass Through
☑ L2TP Pass Through
☑ IPSec Pass Through

PPTP Pass Through	Place a **Check** to enable PPTP protocol passes through WAN.
L2TP Pass Through	Place a **Check** to enable L2TP protocol passes through WAN.
IPSec Pass Through	Place a **Check** to enable IPSec protocol passes through WAN.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

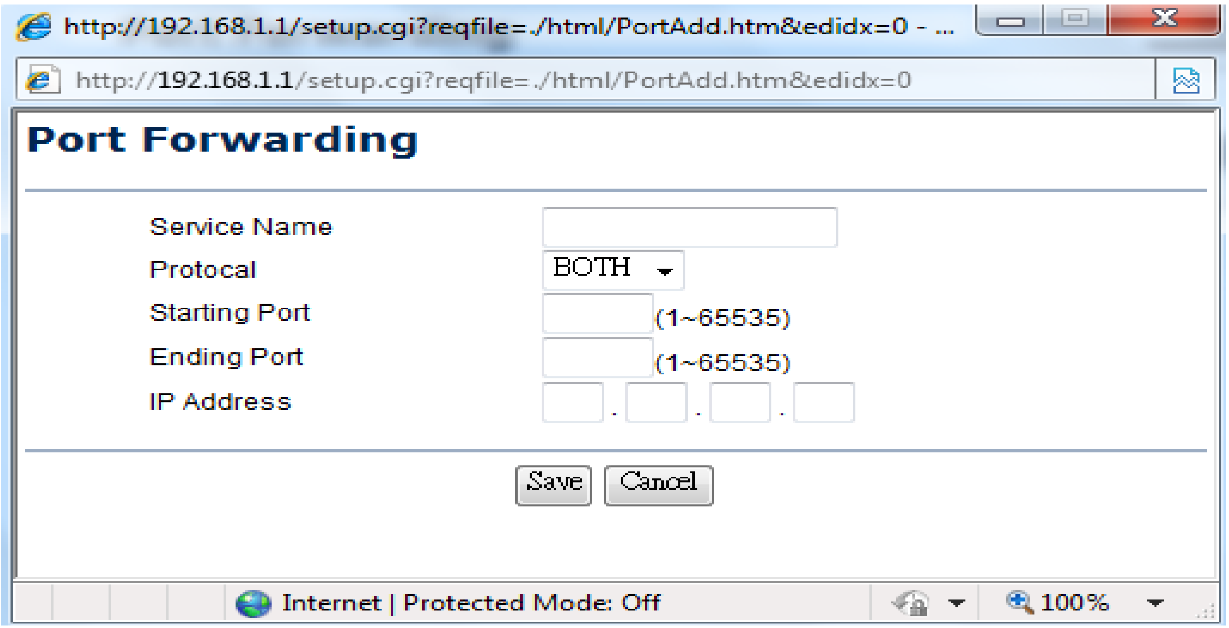
6.4 Port Forwarding

Port Forwarding is used to forward a TCP/IP packet in a NAT to a specific network port.



#	Name	Protocol	Start Port	End Port	Server IP Address	Enable	Modify	Delete

Add Entry	Press Add Entry to add a rule of Port Forwarding.
Apply	Press **Apply** to apply the changes.

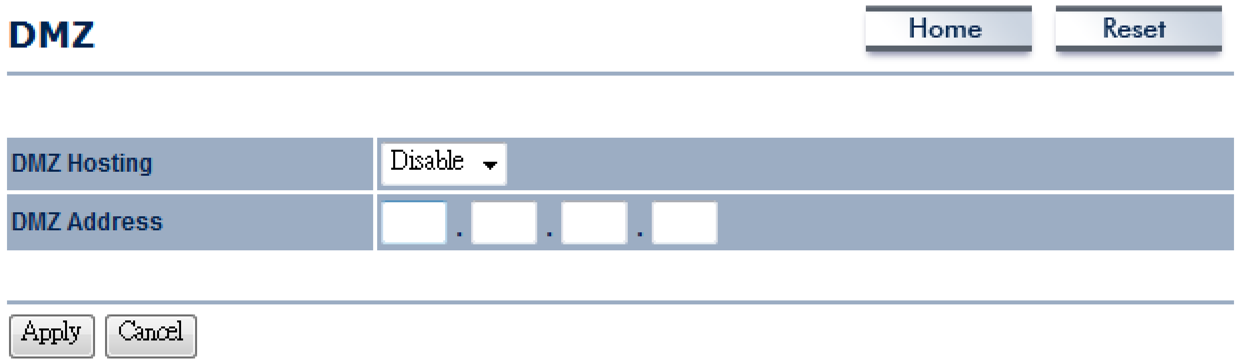

http://192.168.1.1/setup.cgi?reqfile=./html/PortAdd.htm&edidx=0 - ...
http://192.168.1.1/setup.cgi?reqfile=./html/PortAdd.htm&edidx=0
Port Forwarding
Save
Cancel
Internet | Protected Mode: Off
100%

Service Name	
Protocal	BOTH
Starting Port	(1~65535)
Ending Port	(1~65535)
IP Address	. . .

Service Name	Specify a name for current Port Forwarding rule.
Protocol	Select a protocol from drop down list: Both, TCP and UDP.
Starting Port	Specify Starting Port number.
Ending Port	Specify Ending Port number.
IP Address	Specify IP address.
Save / Cancel	Press **Save** to apply the changes or **Cancel** to return previous settings.

6.5 DMZ

DMZ (Demilitarized) is a physical or logical subnetwork that exposed LAN to an unknown network. This function allows you to add an additional entry to an IP address.



DMZ Hosting	Disable
DMZ Address	. . .

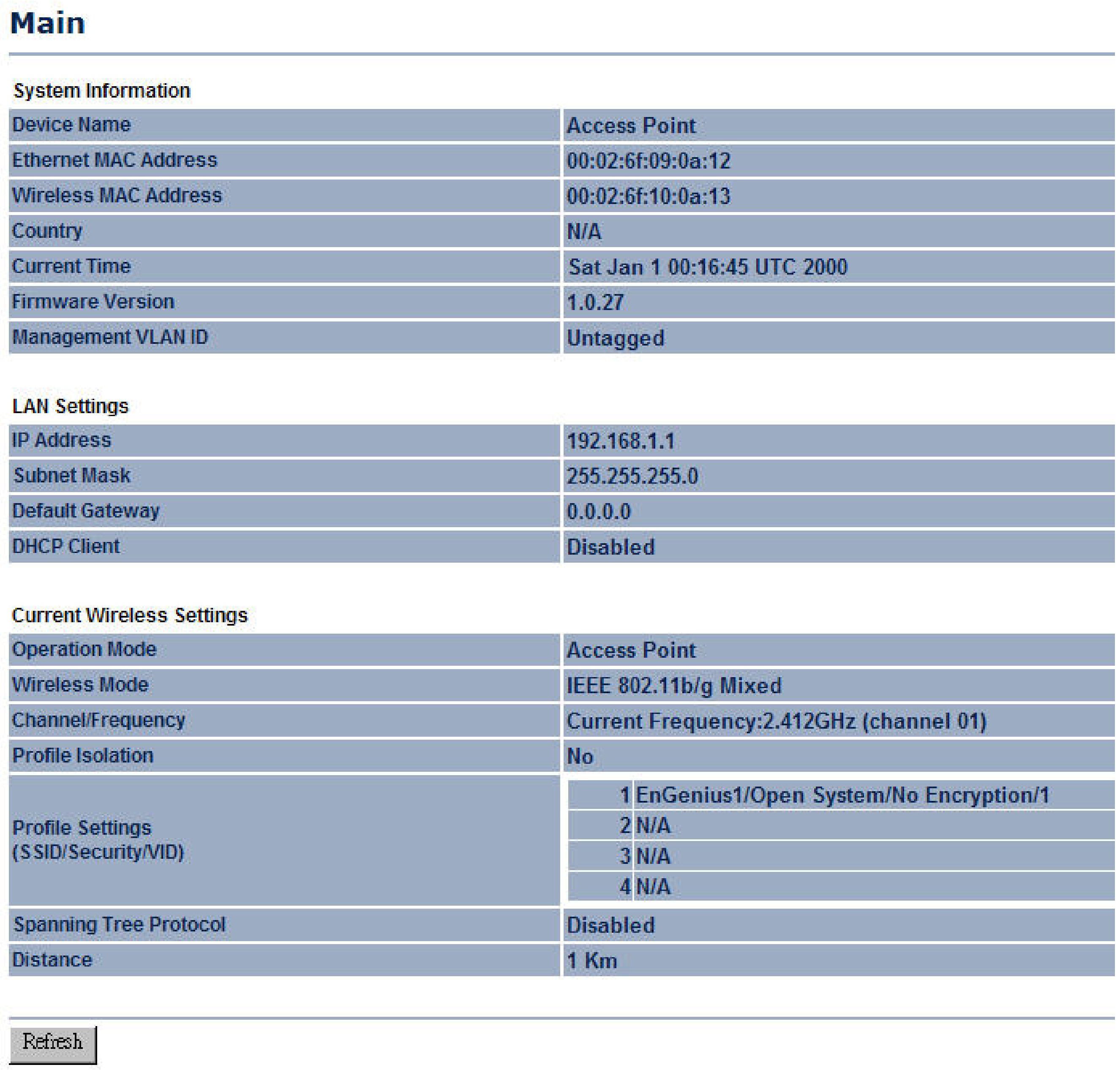
DMZ Hosting	Select **Enable** or **Disable** DMZ from drop down list.
DMZ Address	Specify an IP address of DMZ.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

7 Information Status

Status section is on the navigation drop-down menu. You will then see three options: Main, Wireless Client List, System Log, WDS Link Status, Connection Status, and DHCP Client Table. Each option is described in detail below.

7.1 Main

Click on the **Main** link under the **Status** drop-down menu or click **Home** from the top-right of the webpage. The status that is displayed corresponds with the operating mode that is selected. Information such as operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the ‘System’ section. LAN IP address, subnet mask, and MAC address are displayed in the ‘LAN’ section. In the ‘Wireless section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.



Main

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 00:16:45 UTC 2000
Firmware Version	1.0.27
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

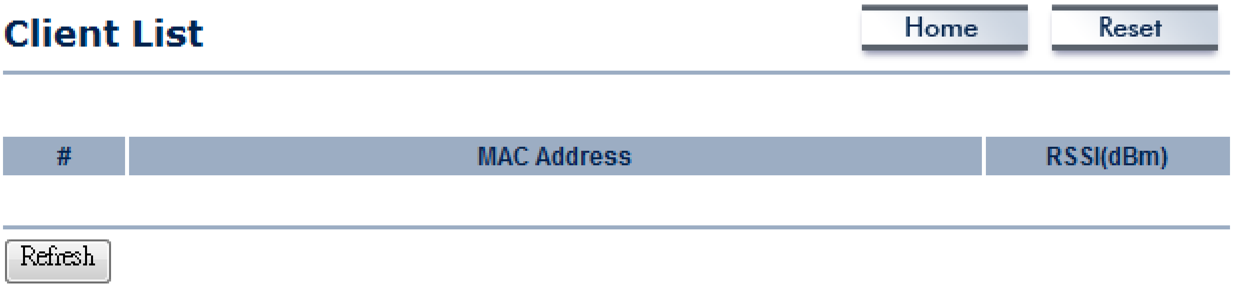
Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current 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

7.2 Wireless Client List

Click on the **Wireless Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the M35.

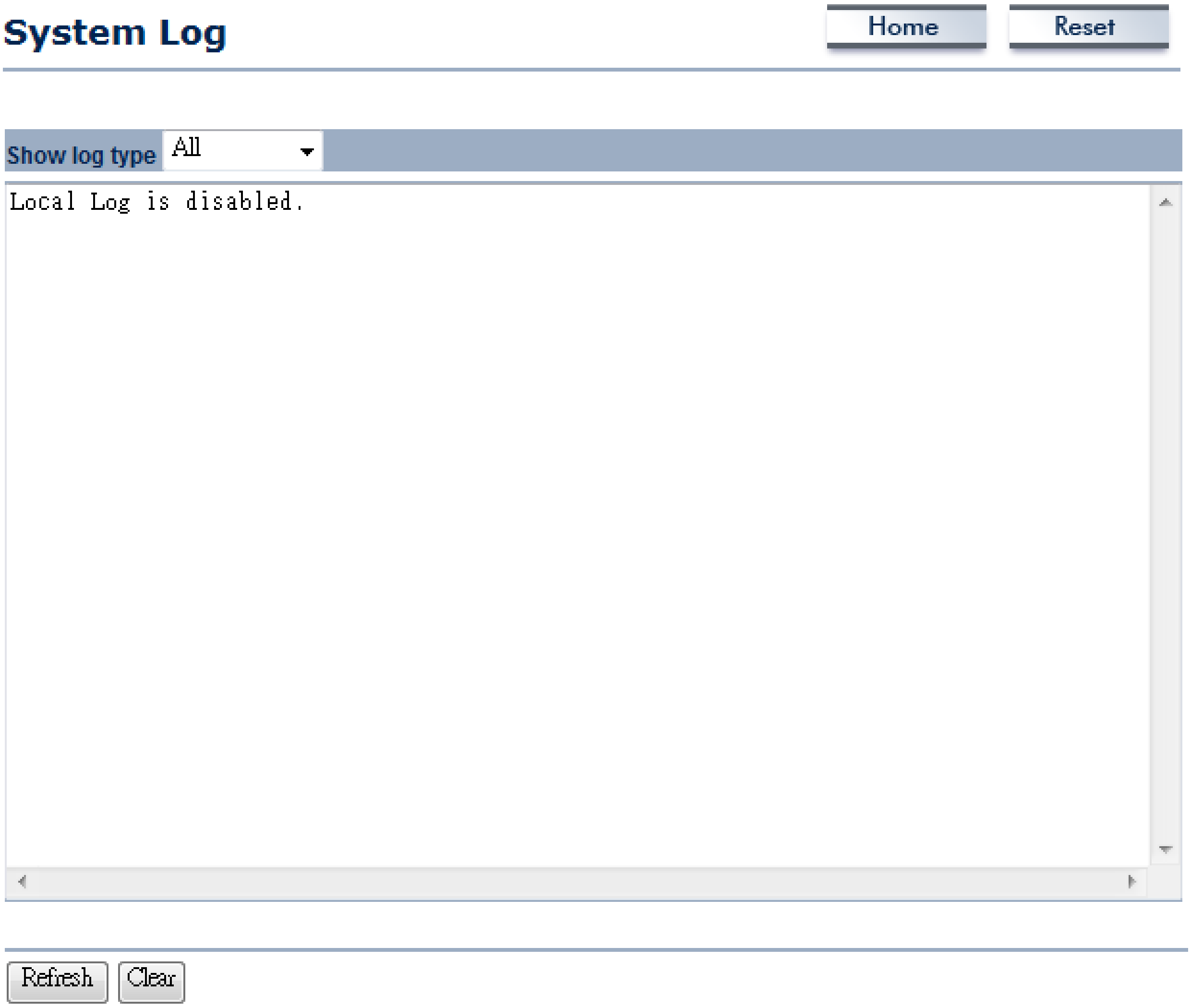
The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list



#	MAC Address	RSSI(dBm)

7.3 System Log

Click on the **System Log** link under the **Status** drop-down menu. 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.

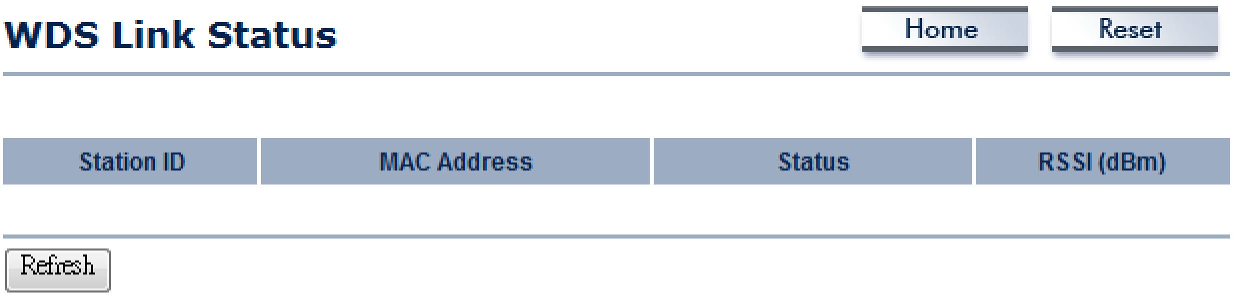


Show log type: All

```
Local Log is disabled.
```

7.4 WDS Link Status

The WDS Link Status will only show in WDS Bridge Mode. Click on the **WDS Link Status** link under the **Status** drop-down menu. This page displays the current status of WDS link, including station ID, MAC address, status and RSSI.

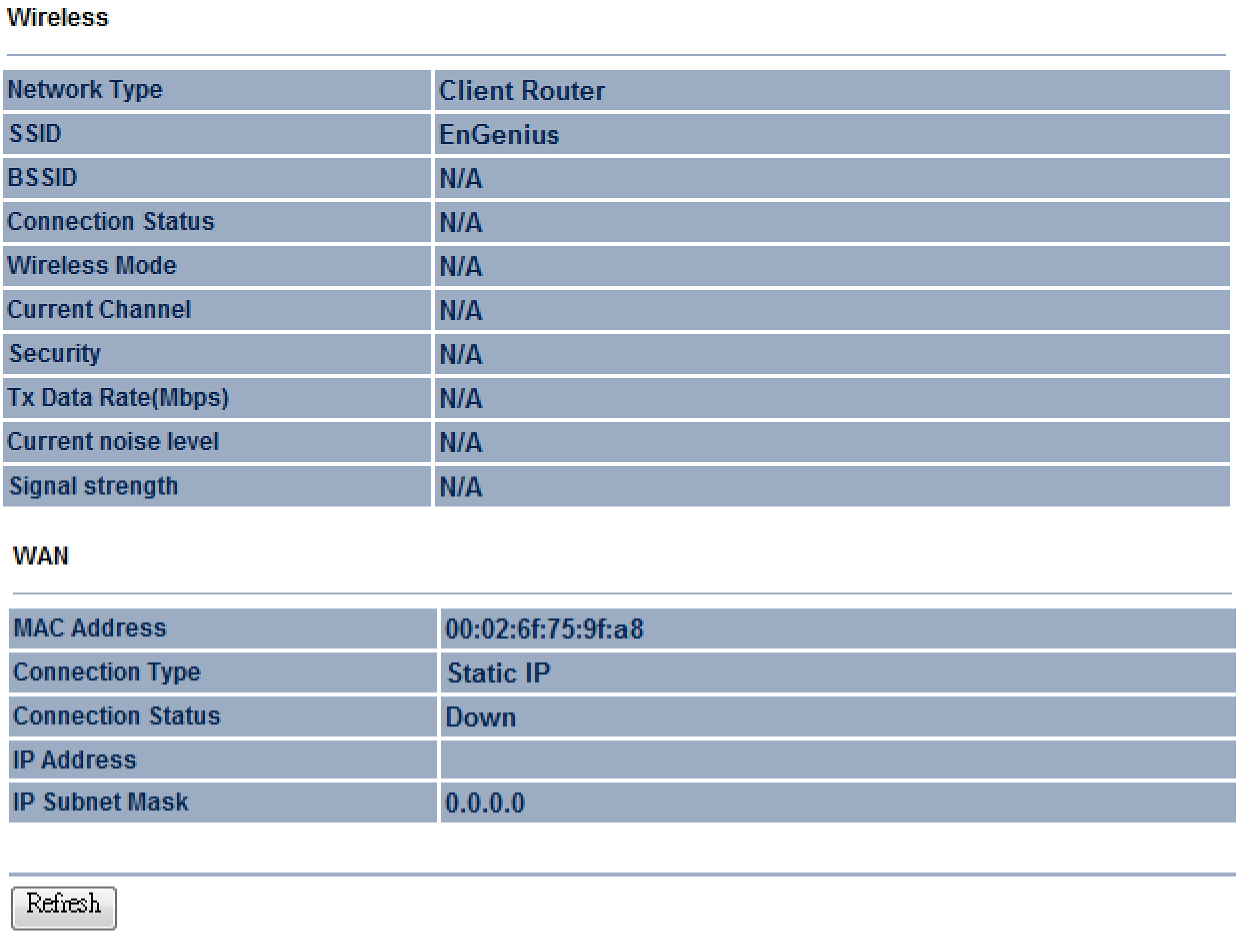


WDS Link Status

Station ID	MAC Address	Status	RSSI (dBm)

7.5 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.



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

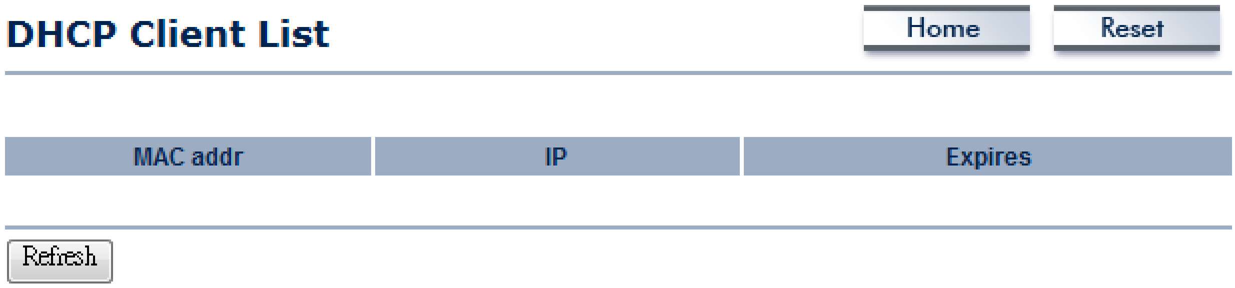
WAN

MAC Address	00:02:6f:75:9f:a8
Connection Type	Static IP
Connection Status	Down
IP Address	
IP Subnet Mask	0.0.0.0

7.6 DHCP Client Table

Click on the **DHCP Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the M35 through DHCP.

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



DHCP Client List

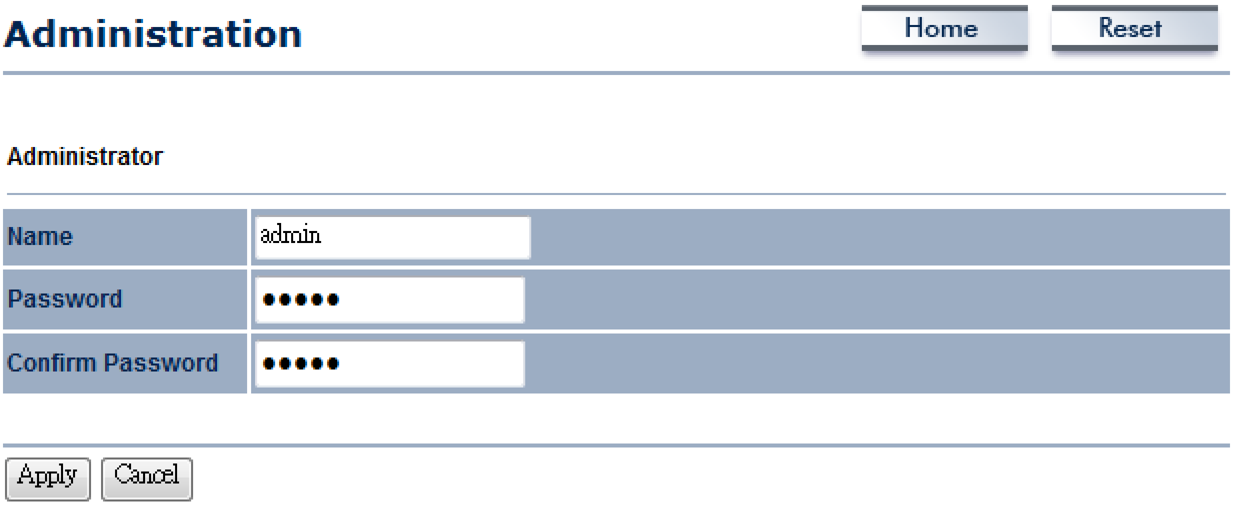
MAC addr	IP	Expires

8 Management Settings

Management section is on the navigation drop-down menu. You will then see seven options: administration, management VLAN, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

8.1 Administration

Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured with a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.

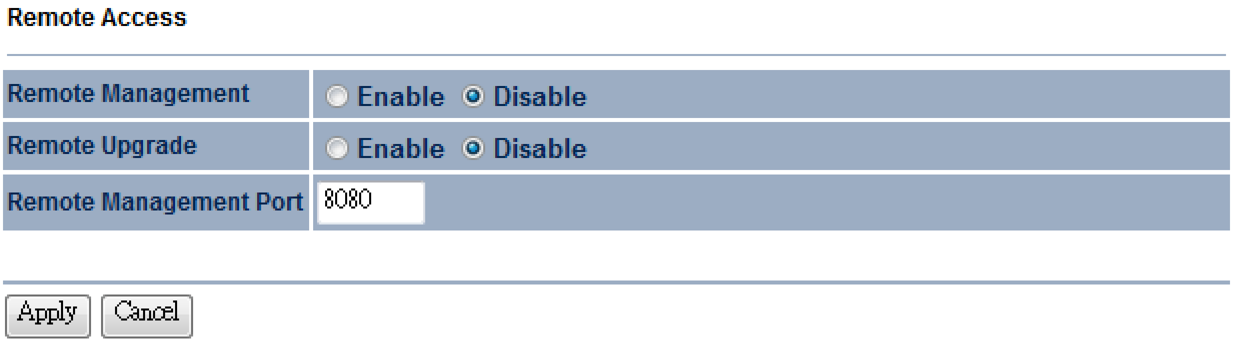


Administration

Administrator

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

Name	Specify Username for login.
Password	Specify a Password for login
Confirm Password	Re-enter the Password for confirmation.



Remote Access

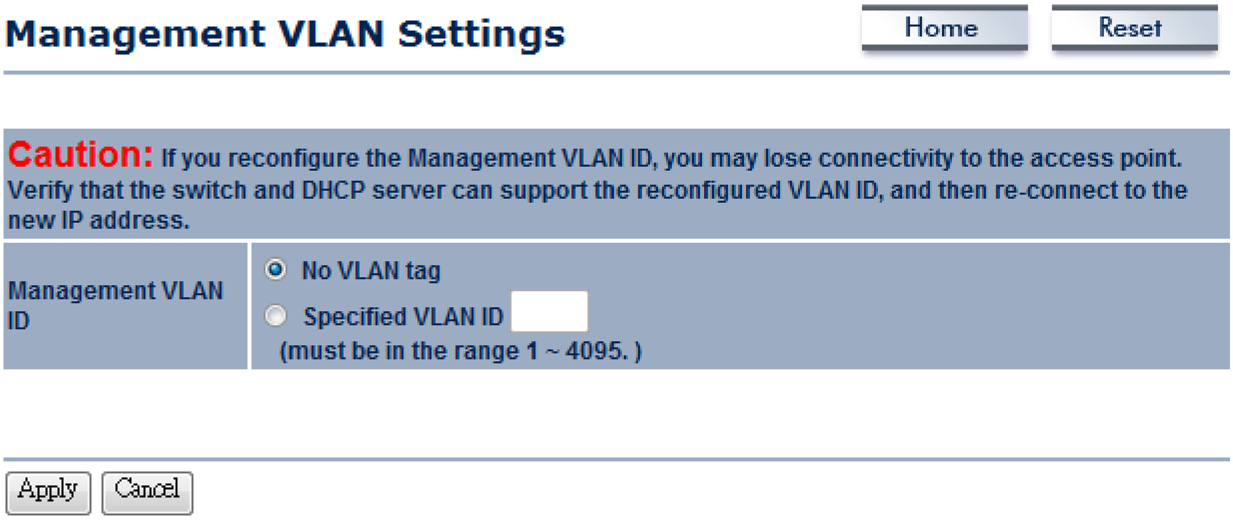
Remote Management	○ Enable ● Disable
Remote Upgrade	○ Enable ● Disable
Remote Management Port	8080

Remote Management	Select the Radio button to Enable or Disable Remote Management.
Remote Upgrade	Select the Radio button to Enable or Disable Remote Upgrade.
Remote Management	Specify the Port number for Remote Management. For example: If you specify the

Port	Port number is 8080, then you will need to enter following http://<IP address>:8080 to access the web interface.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

8.2 Management VLAN

Click on the **Management VLAN** link under the **Management** menu. This option allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN


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.

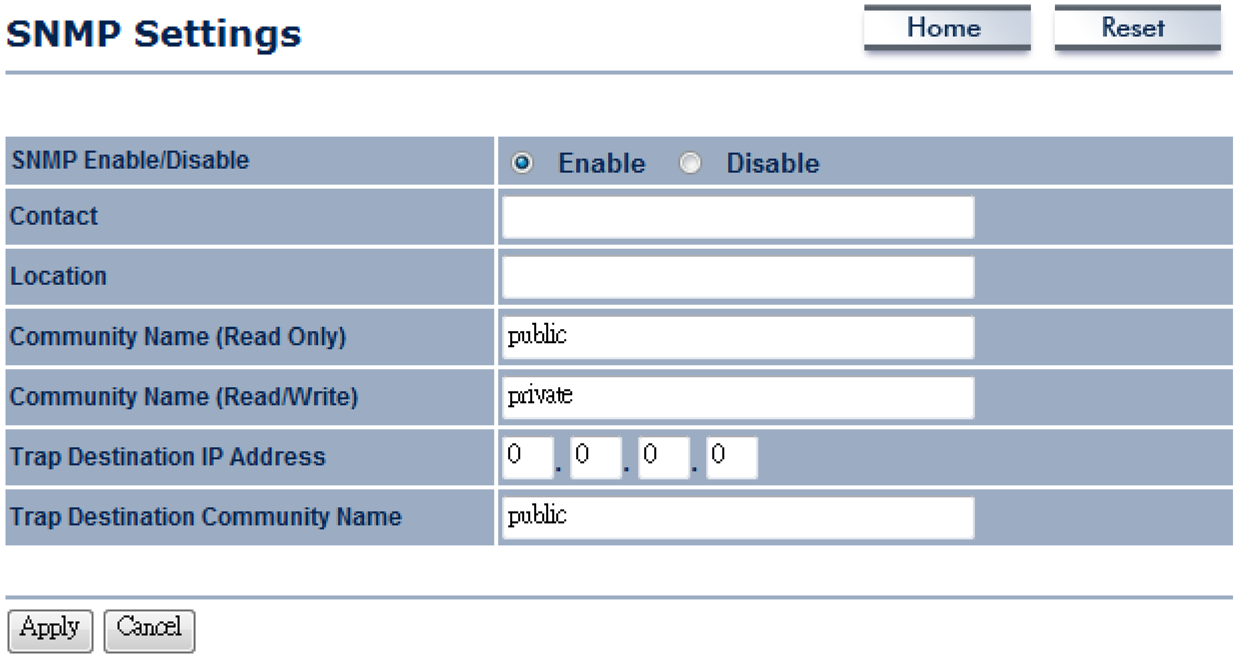
Management VLAN ID	● No VLAN tag ○ Specified VLAN ID (must be in the range 1 ~ 4095.)

Management VLAN ID	If your network includes VLANs and if tagged packets need to pass through the Access Point, specify the VLAN ID into this field. If not, select the **No VLAN tag** radio button.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: If you reconfigure the Management VLAN ID, you may lose connection to the M35. Verify DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

8.3 SNMP Settings

Click on the **SNMP Settings** link under the **Management** menu. 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.

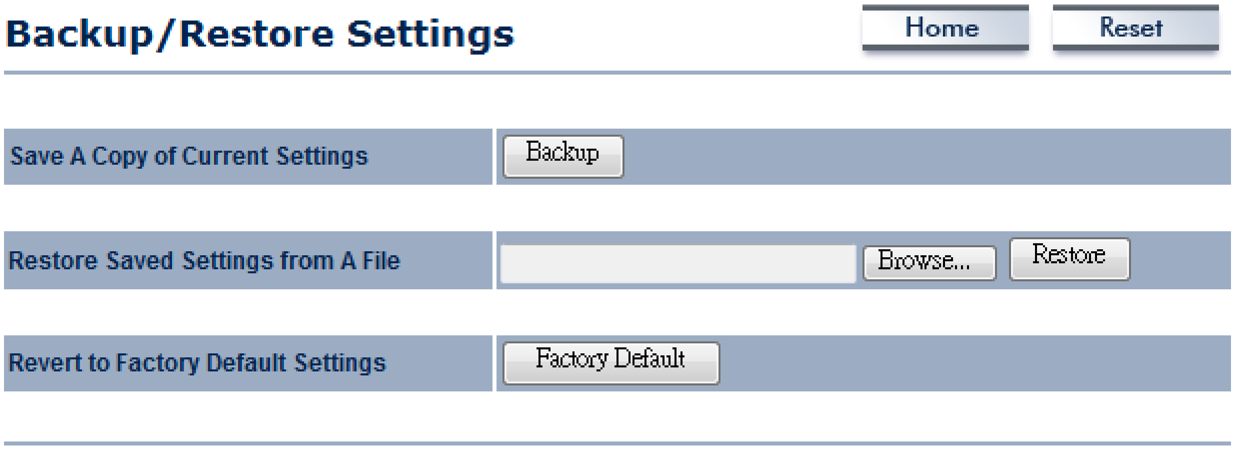


SNMP Enable/Disable	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

SNMP Enable/Disable	Select the Radio button to Enable or Disable SNMP function.
Contact	Specify the contact details of the device.
Location	Specify the location of the device.
Community Name	Specify the password for access the SNMP community for read only access.
Community Name	Specify the password for access the SNMP community for read and write access.
Trap Destination IP Address	Specify the IP address that will receive the SNMP trap.
Trap Destination Community Name	Specify the password of the SNMP trap community.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

8.4 Backup/Restore Settings

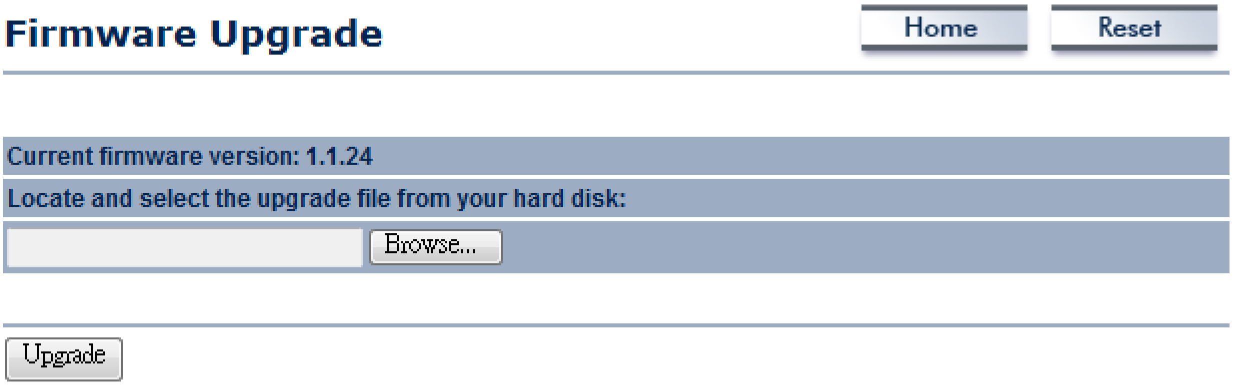
Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need 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 Current Settings	Click on **Backup** to save current configured settings.
Restore Saved Settings from a File	M35 can restore a previous setting that has been saved. Click on Browse to select the file and Restore.
Revert to Factory Default Settings	Click on Factory Default button to reset all the settings to the default values.

8.5 Firmware Upgrade

Click on the **Firmware Upgrade** link under the **Management** menu. This page is used to upgrade the firmware of the device. Make sure that downloaded the appropriate firmware from your vendor.

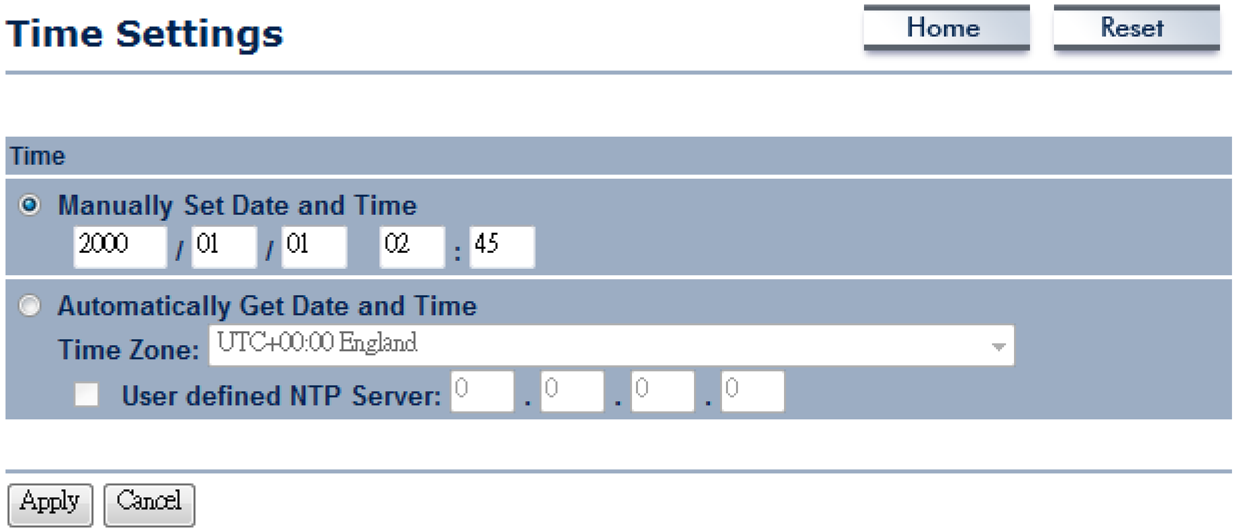

Current firmware version: 1.1.24

Locate and select the upgrade file from your hard disk:

Auction: Upgrade process may take few minutes, please do not power off the device and it may cause the device crashed or unusable. M35 will restart automatically once the upgrade is completed.

8.6 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 : 45

○ Automatically Get Date and Time

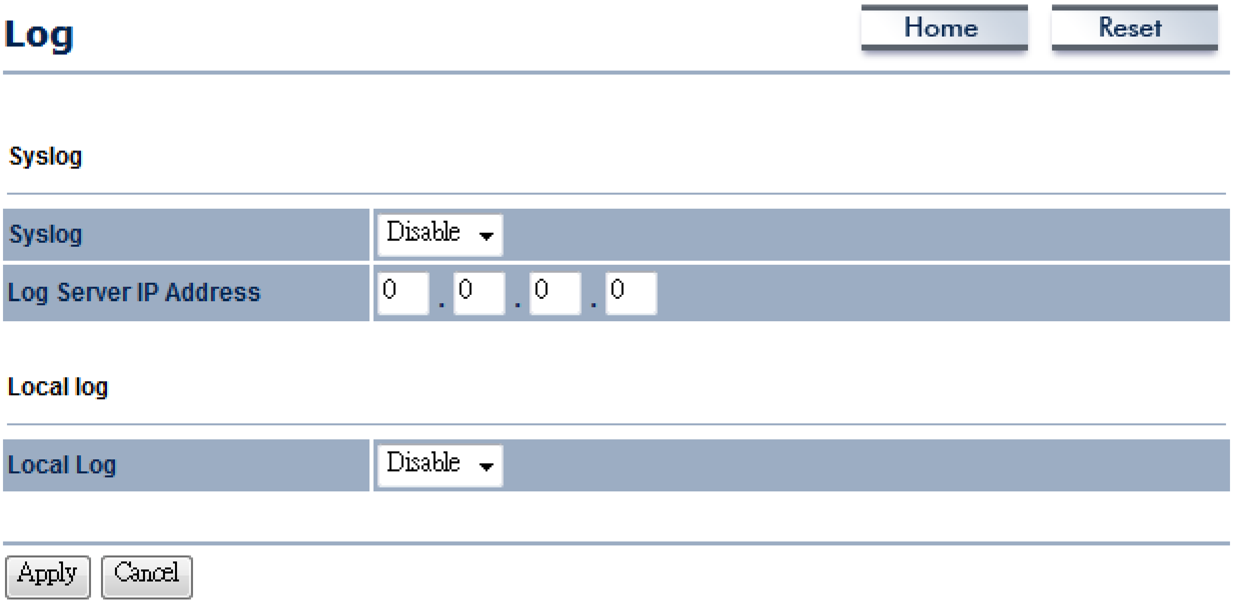
Time Zone: UTC+00:00 England

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

Manually Set Date and Time	Manually setup the date and time.
Automatically Get Date and Time	Specify the Time Zone from the drop down list and Place a **Check** to specify the IP address of the NTP Server manually or uses default NTP Server.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

8.7 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

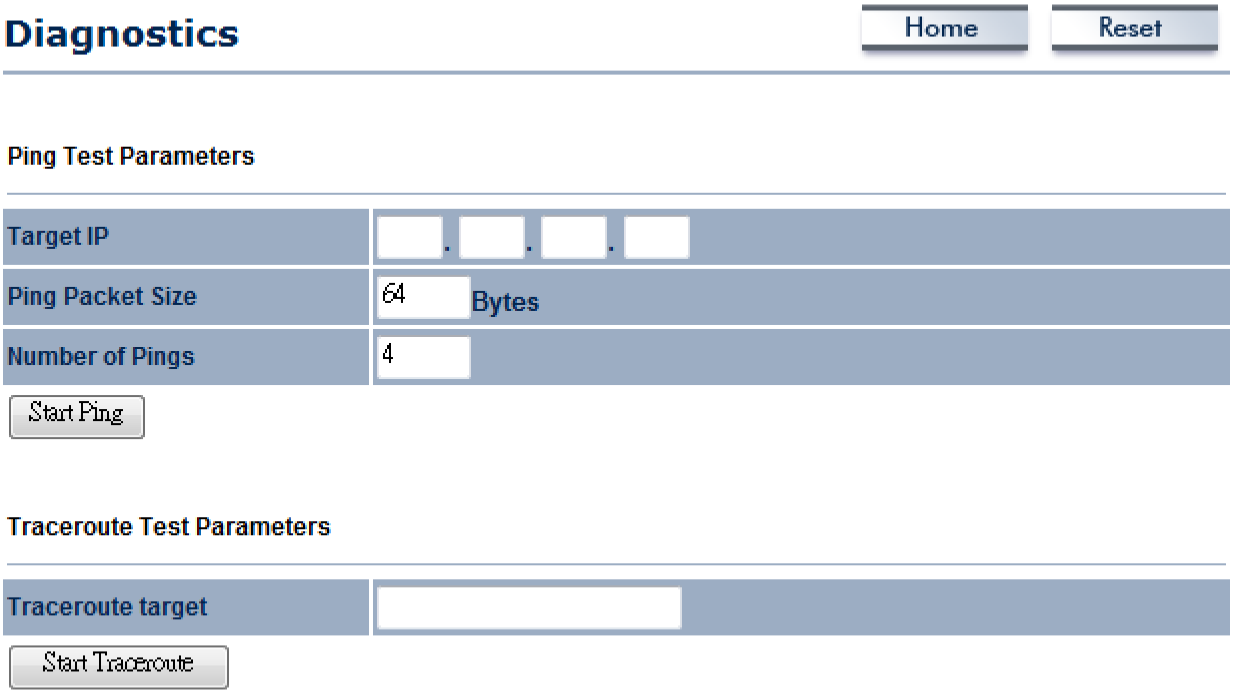
Local log

Local Log	Disable

Syslog	Select Enable or Disable Syslog function from the drop down list.
Log Server IP Address	Specify the Log Server IP address.
Local Log	Select Enable or Disable Local Log service.
Apply / Cancel	Press **Apply** to apply the changes or **Cancel** to return previous settings.

8.8 Diagnostics

Click on the **Diagnostics** link under the **Management** menu. This function allows you to detect connection quality and trace the routing table to the target.



Diagnostics

Ping Test Parameters

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

Traceroute Test Parameters

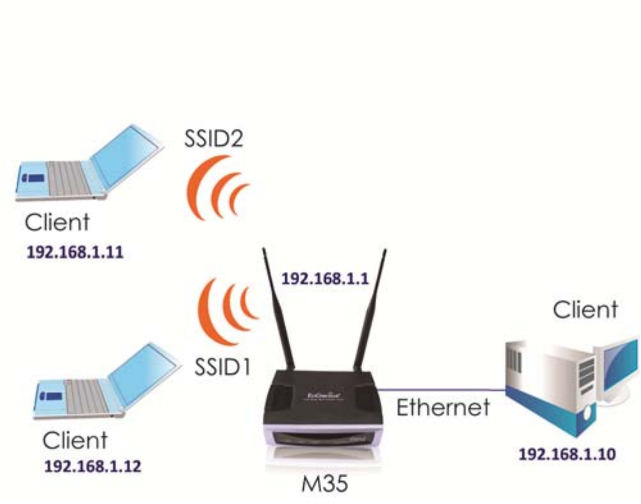
Traceroute target	

Target IP	Specify the IP address you would like to search.
Ping Packet Size	Specify the packet size of each ping.
Number of Pings	Specify how many times of ping.
Start Ping	Press Start Ping to begin.
Traceroute Target	Specify an IP address or Domain name you would like to trace.
Start Traceroute	Press Start Traceroute to begin.

9 Network Configuration Example

This chapter describes the role of the M35 with three different modes. The Access Point mode's default configuration is a central unit of the wireless network or as a root device of the wired environment. Repeater mode and Mesh network mode need future configuration.

9.1 Access Point



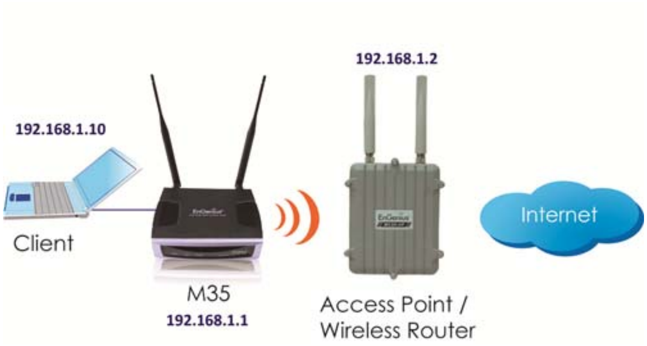
Access Point	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region's regulation.
Step3	Select 802.11b, 802.11g, 802.11b/g mixed or SuperG as your wireless mode.
Step4	Use site survey to scan channels that have been used in nearby area.
Step5	Select channel with less interferences.
Step6	Specify the SSID for your broadcast SSID and you can also configure multiple SSID at the same time.
Step7	Verify VLAN identifier to separate services among clients
Step8	Setup the authentication settings.
Step9	Press Apply to save all changes.
Note: For more advanced settings, please refer to the previous chapters.	
Wireless Client	
Step1	Select wireless mode you would like to associate with.
Step2	Use site survey to scan nearby Access Point and select the certain AP you would like

	to connect with or enter SSID manually.
Step3	Configure VLAN ID in your wireless device if available.
Step4	Select correct authentication type and password.

Auction: M35's Access Point Mode does not provide DHCP server so the Wireless Client IP address must configure manually at the same subnet in Local Area Network.

9.2 Client Bridge Mode

Client Bridge Mode functions like a wireless dongle. It must connect to an Access Point/AP Router to join the network.



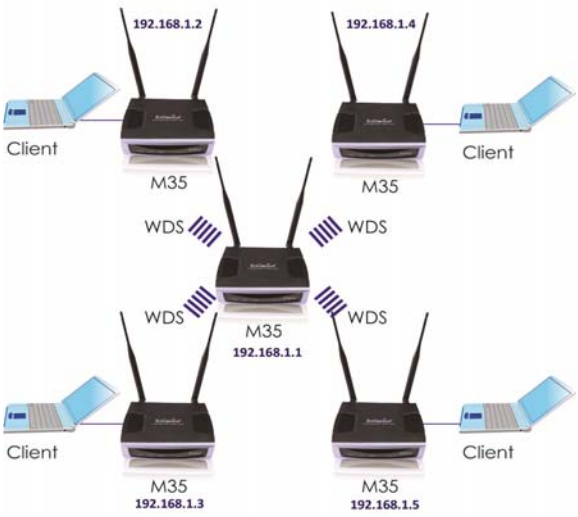
Please refer to the last section to check Access point's configuration.

Client Bridge	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region's regulation.
Step3	Select **Operation Mode** to **Client Bridge** from **System Properties**.
Step4	Select 802.11b, 802.11g, or 802.11b/g mixed as your wireless mode.
Step5	Use site survey to scan Access Points that are available in nearby area.
Step6	Select the AP you would like to associate with.
Step7	Setup the authentication settings that match to the Access Point's setting.
Step8	Press Apply to process all the configurations.

Auction: Client Bridge's IP setting must match to the Access Point's subnet.

9.3 WDS Bridge Mode

Use this feature to link multiple APs in a network, All clients associated with any APs can communicate each other like an ad-hoc mode.

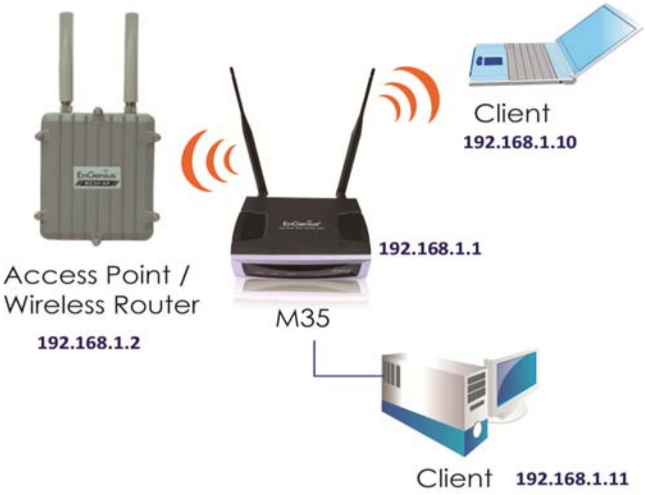


WDS Bridge	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region's regulation.
Step3	Select **Operation Mode** to **WDS Bridge** from **System Properties**.
Step4	Select 802.11b, 802.11g or 802.11b/g mixed as your wireless mode.
Step5	Select channel you would like to use.
Step6	Setup the authentication settings
Step7	Setup WDS Link Settings.
Step8	Specify the AP's MAC address you would like to connect with.
Step9	Press Apply to process all the configurations.

Auction: Each WDS bridge's device must use the same **Subnet**, **Wireless Mode**, **Wireless Channel**, and **Security Setting**.

9.4 Repeater Mode

AP Repeater is used to extend the wireless coverage area of the Access Point. Please refer to the previous section to configure the Access Point.



Repeater	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region’s regulation.
Step3	Change operation mode to **Repeater** from **System Properties**.
Step4	Select wireless mode you would like to associate with.
Step5	Select channel/frequency you would like to associate with.
Step6	Use site survey to scan nearby Access Point and select the certain AP you would like to connect with or enter SSID manually.
Step7	Select correct authentication type and password the same as Access Point.
Step8	Enable Prefer BSSID for automatically reconnected.

Note(1): For more advanced settings, please refer to the previous chapters.

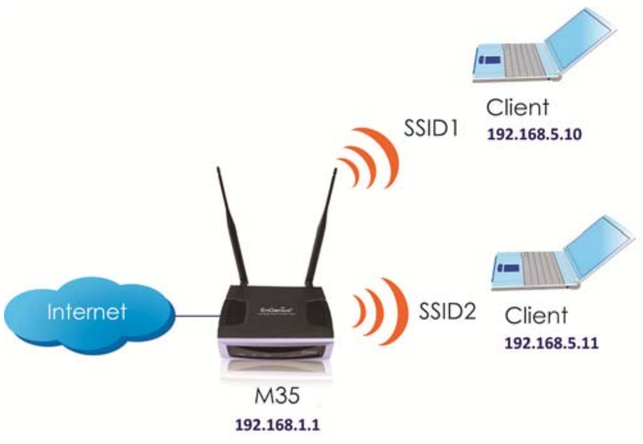
Note(2): Repeater IP subnet must the same as the Access Point, please refer to the **IP Settings** section for details.

Wireless Client	
Step1	Select wireless mode you would like to associate with.
Step2	Use site survey to scan nearby Access Point and select the certain AP you would like to connect with or enter SSID manually.
Step3	Configure VLAN ID in your wireless device if available.
Step4	Select correct authentication type and password.

Auction: Wireless Client IP address must configure manually at the same subnet in Local Area Network or enable DHCP server of M35 to retrieve IP automatically.

9.5 AP Router Mode

The M35 has DHCP server build inside that allows you to configure easily via wireless. AP Router Mode can also support four different SSIDs. Use wireless device to associate with M35, connect an Ethernet through the WAN port.

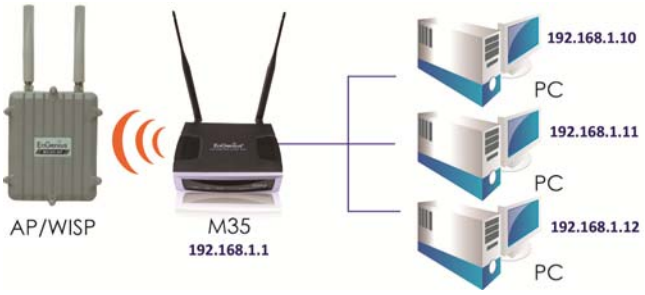


AP Router	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region's regulation.
Step3	Change operation mode to **AP Router** from **System Properties**.
Step4	Setup your wireless client's **Wireless Local Area Network** to **Obtain an IP Address Automatically**.
Step5	Login to the web-based configuration interface with default IP 192.168.1.1 via wireless.
Step6	Select 802.11b, 802.11g, 802.11b/g mixed or SuperG as your wireless mode.
Step7	Use site survey to scan channels that have been used in nearby area.
Step8	Select channel with less interferences.
Step9	Specify the SSID for your broadcast SSID and you can also configure multiple SSID at the same time.
Step10	Verify VLAN identifier to separate services among clients
Step11	Setup the authentication settings.
Step12	Setup your WAN connection type given by your **Internet Service Provider** from **WAN Settings**.
Step13	Press Apply to save all changes.

Auction: Once you have successfully connected to internet, you may not be able to access the device. Please try to disconnect your internet connection from WAN port.

9.6 Client Router

In the Client Router Mode, the M35 has DHCP Server build inside that allows many LANs automatically generate an IP address to share the same Internet. Connect an AP/WISP Wirelessly and connect to LANs via wired. Client Router Mode is act completely opposite to the AP Router Mode.



Please refer to the last section to check Access point's configuration.

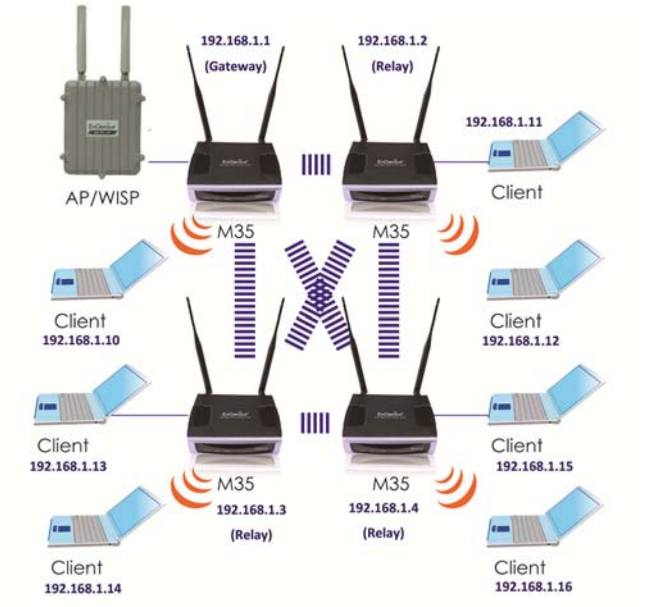
Client Router	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1

Step2	Select your country or region’s regulation.
Step3	Select **Operation Mode** to **Client Router** from **System Properties**.
Step4	Change your **Local Area Network** setting to **Obtain an IP Address Automatically**.
Step5	Select 802.11b, 802.11g, or 802.11b/g mixed as your wireless mode.
Step6	Use site survey to scan Access Points that are available in nearby area.
Step7	Select the AP you would like to associate with.
Step8	Setup the authentication settings that match to the Access Point’s setting.
Step9	Setup your WAN connection type given by your **Internet Service Provider** from **WAN Settings**.
Step10	Press Apply to process all the configurations.

Auction: Client Router’s IP setting must match to the Access Point’s subnet.

9.7 Mesh

In order to construct the Mesh Network, the following configuration must be the same.



Mesh	
Step1	Login to the web-based configuration interface with default IP 192.168.1.1
Step2	Select your country or region’s regulation.
Step3	Change device mode to **Mesh** from **System Properties**.
Step4	Select wireless mode you would like to associate with.
Step5	Select channel/frequency you would like to associate with.
Step6	Specify SSID for the Mesh Network.
Step7	Setup the authentication settings.

Step8	Specify current device is a gateway or relay.
Step9	Press Apply to save all changes.

Note(1): Non-M35 product may find difficulty of configuration.

Note(2): **In Mesh Mode, recommended 1 Gateway with 4 Relay Linear and radiative deployment scenario.**

Access Point	
Step1	Specify the SSID for your broadcast SSID and you can also configure multiple SSID at the same time.
Step2	Setup the authentication settings.
Step3	Press Apply to save all changes.

Note: For more advanced settings, please refer to the previous chapters.

Wireless Client	
Step1	Select wireless mode you would like to associate with.
Step2	Use site survey to scan nearby Access Point and select the certain AP you would like to connect with or enter SSID manually.
Step3	Configure VLAN ID in your wireless device if available.
Step4	Select correct authentication type and password.

Auction: Wireless Client IP address must configure manually at the same subnet in Local Area Network. Once a Gateway is connected to a WISP, all wireless clients and Mesh can retrieve IP address automatically.

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.