KWA-6960

Portable Smart Bridge

User Manual

Copyright

About this manual

The purpose to use this manual is for install the device. This manual is including disposing course and method and helping the customer to solve the unpredictable problem.

The following typographical conventions are used in this purpose:

Notice:

- This indicates an important Note.

Caution:

- This indicates a warning or caution

Bold Type：Indicates the function, important words, and so on.

Index

Chapter 1 Introduction

Introduction

Thank you for choosing the KWA-6960. The KWA-6960 work on 5GHz, and it based on powerful Wi-Fi technology that provides higher throughput.

Appearance of Product

Figure 1 **KWA-6960**

Features and Benefits

- ✓ Easy to install and friendly to user, just plug and play.
- ✓ Provides Web-based configuration utility.
- ✓ Support 12V 1A DC Power Supply
- ✓ IP67 class of enclosure

Chapter 2 Hardware Installation

System Requirement

Two PCs with automatic speed control connector NIC supporting the transfer rate of 10/100Mbps data.

- ✓ The IP address of NIC should be the same subnet with the AP, the default IP address of AP is 192.168.1.1
- ✓ Microsoft Internet Explorer 6 or above.

Produce Kit

1. KWA-6960 x 1
2. 12V 1A DC Adapter x 1
3. PoE injector guide x 1
4. Wall Mount Kit x 1 set
5. Check list of components x 1
6. Disc for user manual x 1

Hardware Installation

The following steps will help you while installing KWA-6960.

LED Descriptions

LED	Status	Description
Power	Blue	Power ON
Link Status	Blue	Remote Device Connects with KWA-6960

Figure 2 **LED Definition**

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the KWA-6960 factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Item	Factory Default
Login Information	
User Name	admin
Password	password
Basic Settings	
Device Name	DEVICExxxxxx (xxxxxx Represent the last 6 digitals of the MAC address)
Ethernet Data Rate	Automatic
Spanning Tree Protocol	Enable
VLAN (802.1Q)	Disable
IP Settings	IP Type：Manual
	IP Address：192.168.1.1
	IP Subnet Mask：255.255.255.0
	Default Gateway：0.0.0.0
	Primary DNS Server：0.0.0.0
	Secondary DNS Server: 0.0.0.0
Time Settings	Time Server: [spare]
	Time Sever Port: 123
	Time Zone: (GMT-08:00)Pacific Time(US & Canada);Tijuana
Wireless Setup	
Radio Frequency (RF)	Enable
Network ID	Wireless
RF Bandwidth	20MHz
Channel / Frequency	5260MHz
Data Rate	BPSK 1/2 – 64QAM 3/4
Output Power	Full
Fragmentation length	2346

Figure 3 **Default Settings**

Using the Web Management

The KWA-6960 provides you with user-friendly Web-based management tool.

Open IE and enter the default IP address (Default: 192.168.1.1) and Login as below：

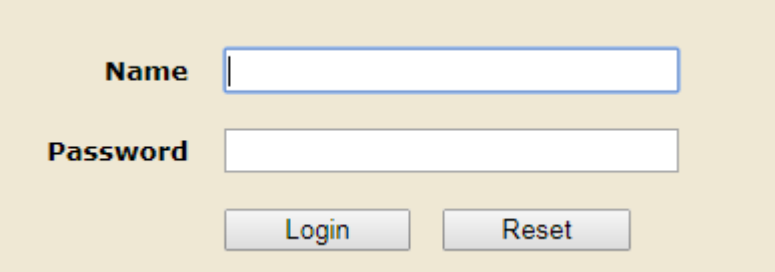


Figure 4 **Login Interface**

Enter the username (Default: **admin**) and password (Default: **password**) and click “Login”

Caution：

- IP address of your PC must be the same subnet of device

After login, you can check basic information of device, such as MAC address off device, Firmware version, etc.

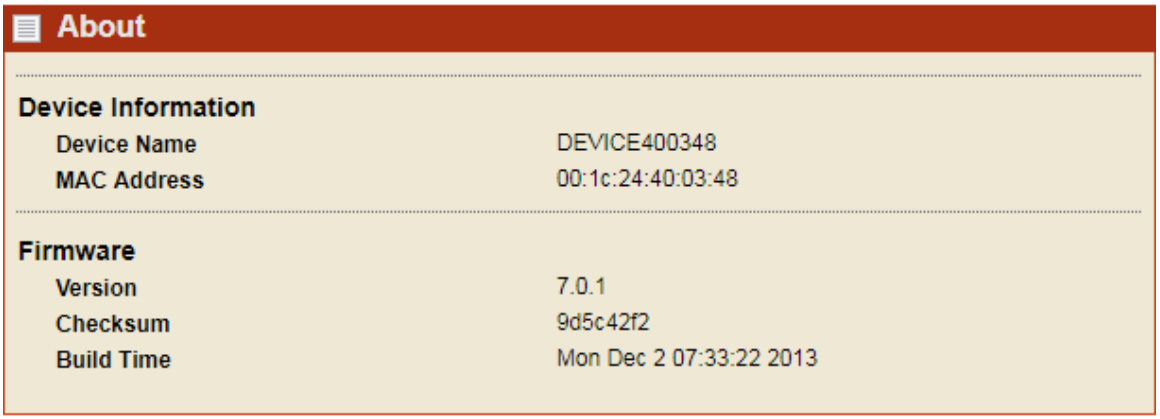


Figure 5 **Device Information**

Basic System Setup

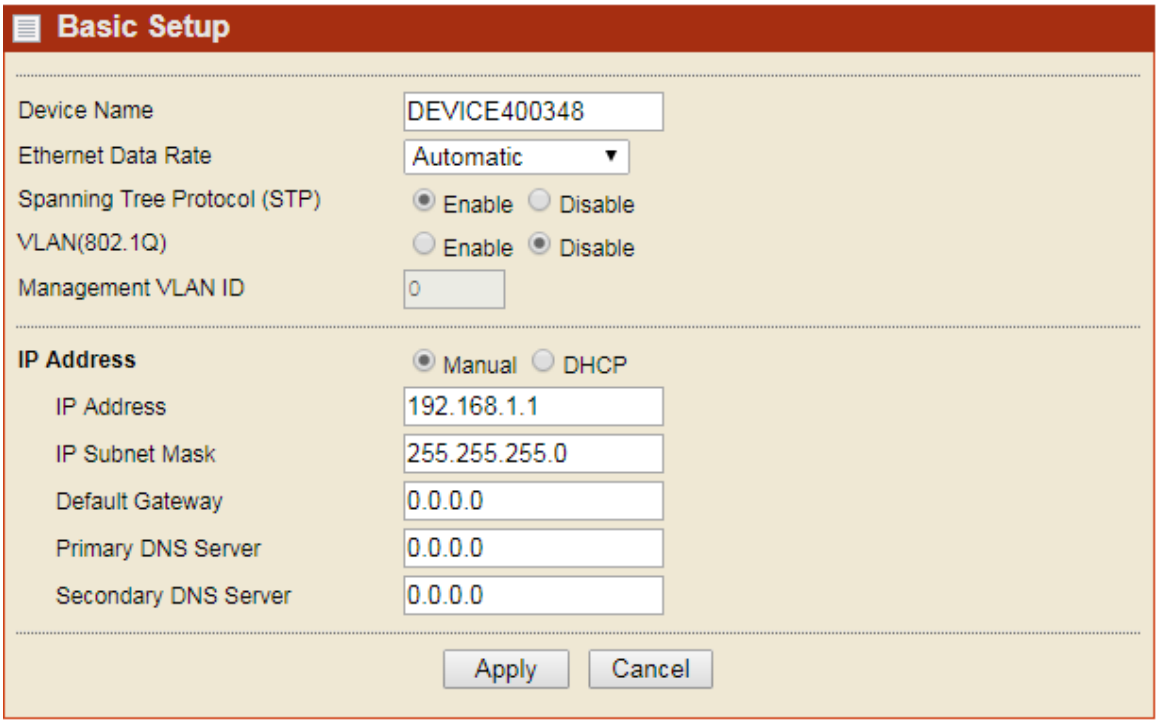


Figure 6 **Basic Settings**

Device Name

Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Due to support WINS, You can use “Device Name” instead of IP address to access device via WEB interface. For instance, device named as DEVICE400348, you can enter “DEVICE400348” in the IE, then click “ENTER” and WEB page; or use “ping” command to check settings is active or not, such as ping DEVEICE400348.

Ethernet Data Rate

Specify the transmission rate of data, default is Automatic.

Automatic / T-base10Mbps / T-Base100Mbps

Spanning Tree Protocol (STP):

Enabling spanning tree can prevent undesirable loops in the network, ensuring a smooth running network. By default, the function is enabled.

VLAN (802.1Q)

Virtual local network can promote network security. By default, the function is disabled.

Management VLAN ID

To be able to access the web page of the managed Base Station in the VLAN network, you have to assign the VLAN management ID for the managed Base Station. Note that the ID on the switch must be identical of the Base Station's VLAN ID. Check Enable VLAN(802.1Q) checkbox to activate it.

IP Address

Manual is for specifying the IP Address manually.

DHCP is for allocating IP Address by DHCP server automatically.

IP Address

This IP in your network must be unique, the default is 192.168.1.1.

IP Subnet Mask

Use subnet mask to ensure two devices in the same network, default is 255.255.255.0

Default Gateway

Default gateway and DNS server for your local area network which connects to LAN port.

Primary DNS Sever

First choice of domain name server

Secondary DNS Sever

Second choice of domain name server

Statistics

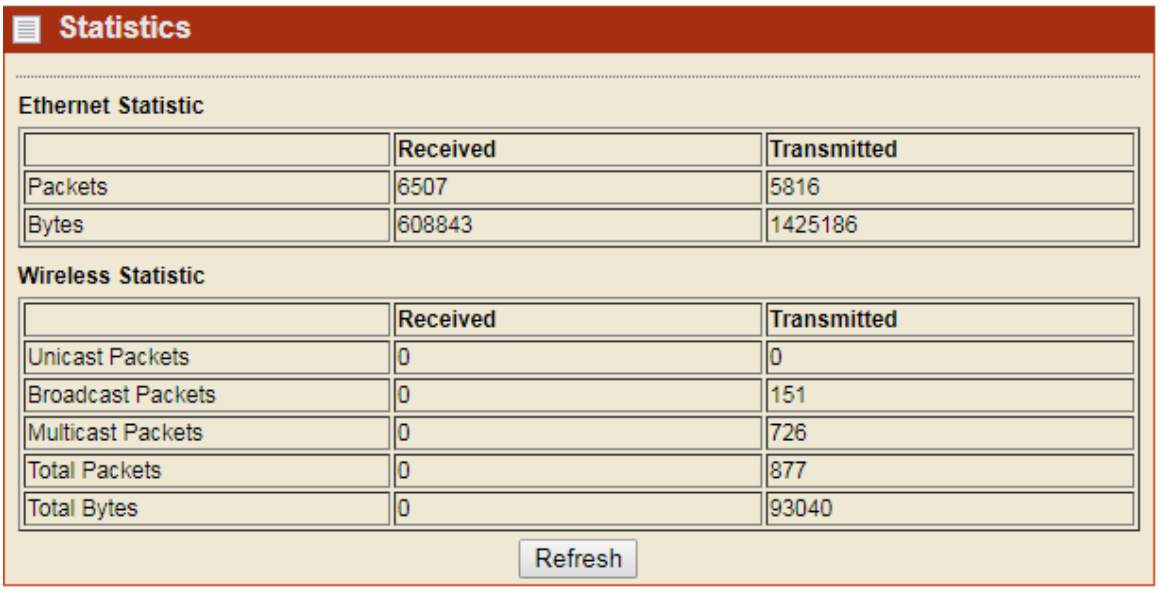


Figure 7 **Statistics**

Display wired and wireless statistics of packets including transmitted and received packets, Uncast, Broadcast, Multicast and total Packets. Click “Refresh” can get instant information.

Chapter 4 Wireless Settings

Basic Wireless Settings

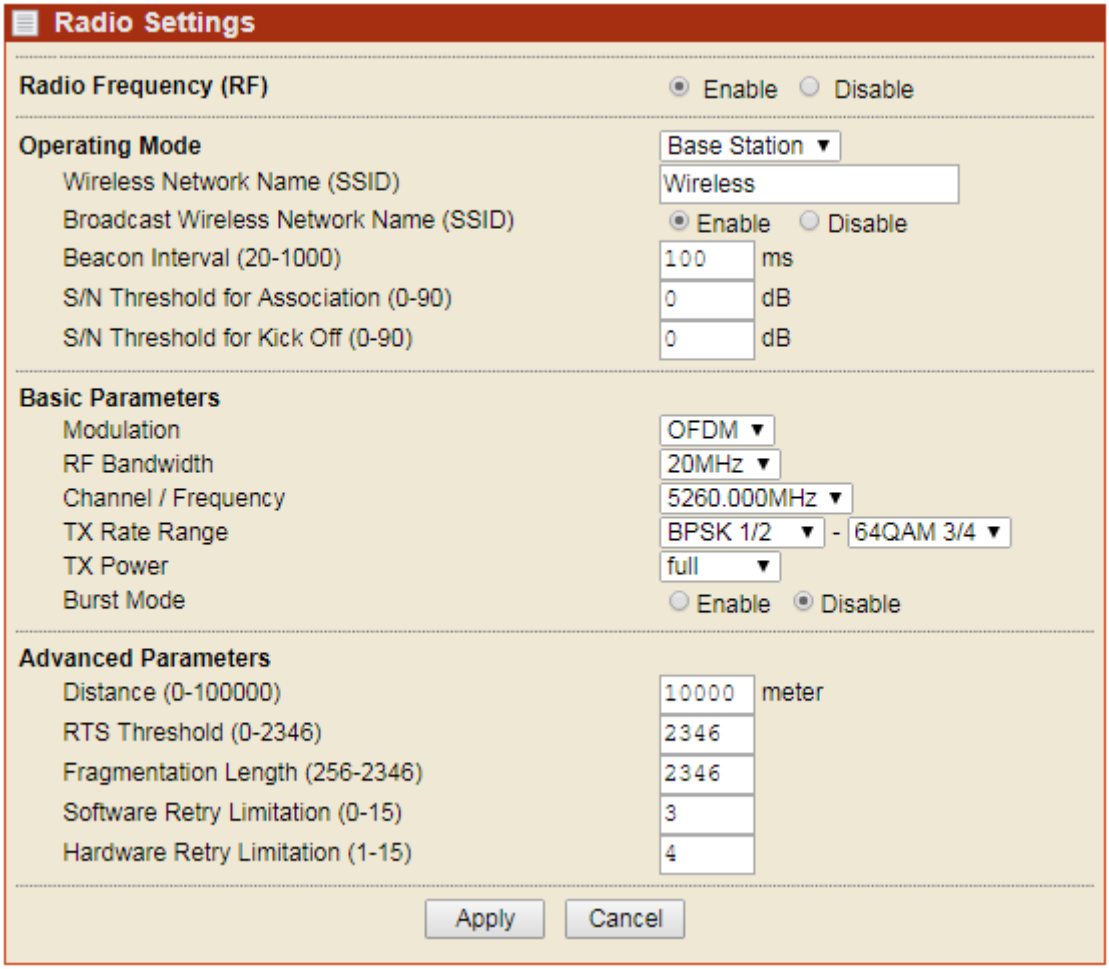


Figure 8 **Radio Settings**

Radio Frequency (RF)

RF-Wireless, default is enabled.

Operating Mode

Base Station：Establishing a wireless coverage and receives connectivity from other wireless devices. The default mode is Base Station.

CPE：Perform as a client station associated to other Bridges. In CPE Mode, CPE can only connect to a specified Base Station with Wireless Network Name(SSID).

Peer-to-Peer: It adopts the WDS protocol to make the connection. The device establishes wireless connectivity

with another by keying in remote MAC address.

Wireless Network Name (SSID)

The SSID is a unique ID used by Access Points and Stations to identify a wireless LAN. Wireless clients associating to any Access Point must have the same SSID. The default ESSID is "**Wireless**". The ESSID can up to 32 characters

Broadcast Wireless Network Name (SSID)

Enabled to broadcast wireless network name, disable to disabled it.

The Wireless Network Name broadcasting is used in the first place is to make it easy for CPE to see and connect to the network. Otherwise, they have to know the name beforehand and set up a manual connection to it. However, with the Wireless Network Name enabled, not only do your neighbors see your network any time they browse for nearby wireless, it makes it easier for potential hackers to see that you have a wireless network within range.

Beacon Interval Time (20~1000)

Specify the frequency interval to broadcast packets. Default is 100ms.

Basic Parameters

Modulation

Specify the modulation of connection. Options are OFDM and DSSS.

RF Bandwidth

Decide bandwidth of Radio Frequency. Including 5 / 10 / 20 / 40 MHz, default is 20MHz.

Channel / Frequency

Using different frequency to be applied.

TX Rate Range

Specify the TX rate range of operating. There are 64QAM 3/4, 64QAM 2/3, 16QAM 3/4, 16QAM 1/2, QPSK 3/4, QPSK 1/2, BPSK 3/4 and BPSK 1/2.

TX Power

Setting power of TX, default is full.

Half: -3 dB

Quarter: -6 dB

Eighth: -9 dB

Min: -12 dB

Robust Mode

It helps the wireless stability when working on the complicated wireless environment. The default is disable

Advanced Parameters

Distance

Specify the distance between both wireless devices. The default is 10000m.

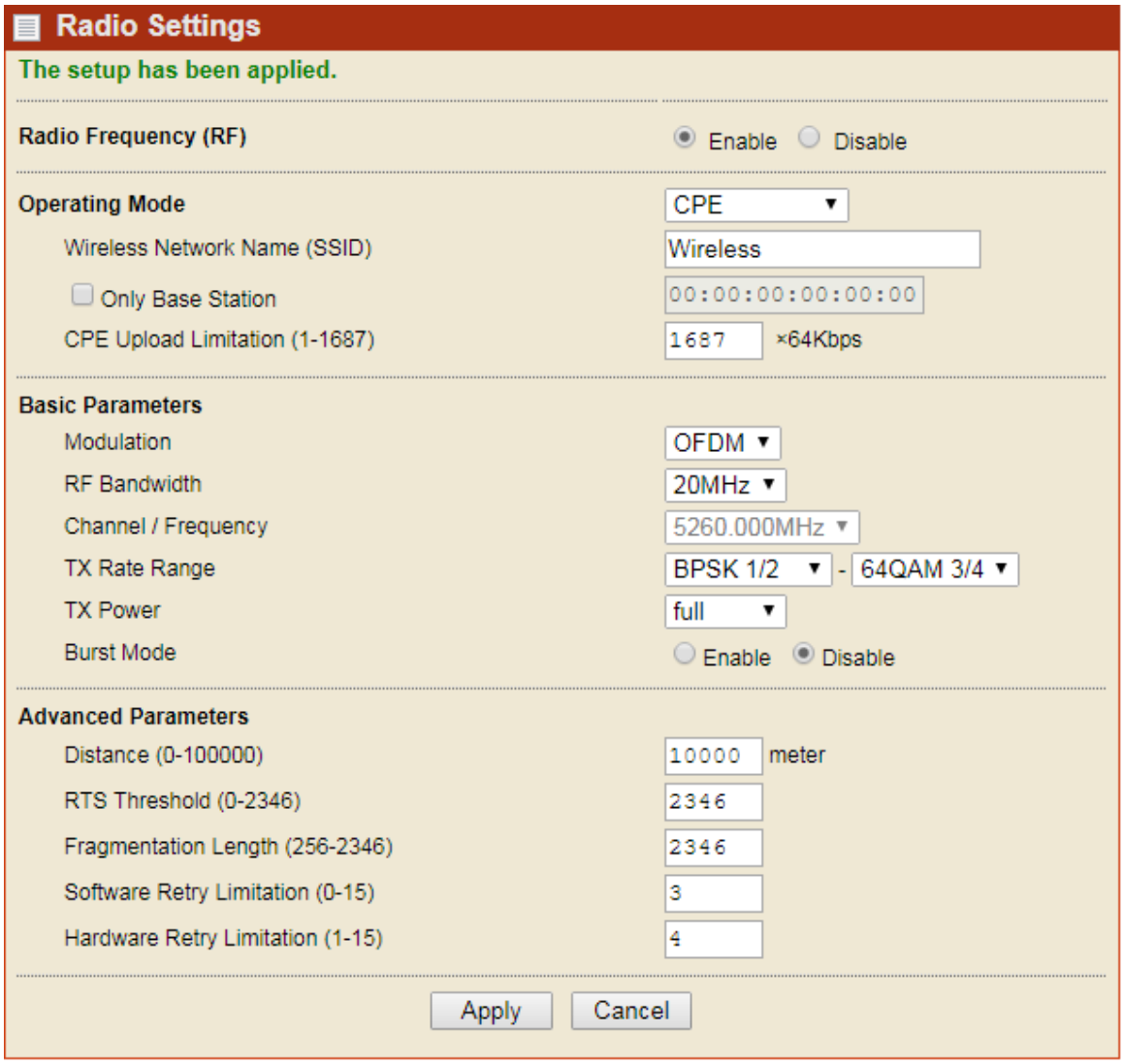
RTS Threshold

The device sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Fragmentation Length

Specify the length of the maximum fragmentation packet. When packet is large than setting, it would divide to smaller segment package. By default, it will divide the length of segment packet automatically.

Operating Mode - CPE



Wireless Network Name (SSID)

Specify the SSID for the CPE to be connected. The default SSID is “Wireless” and the “SSID” characters are up to 32.

Only Base Station

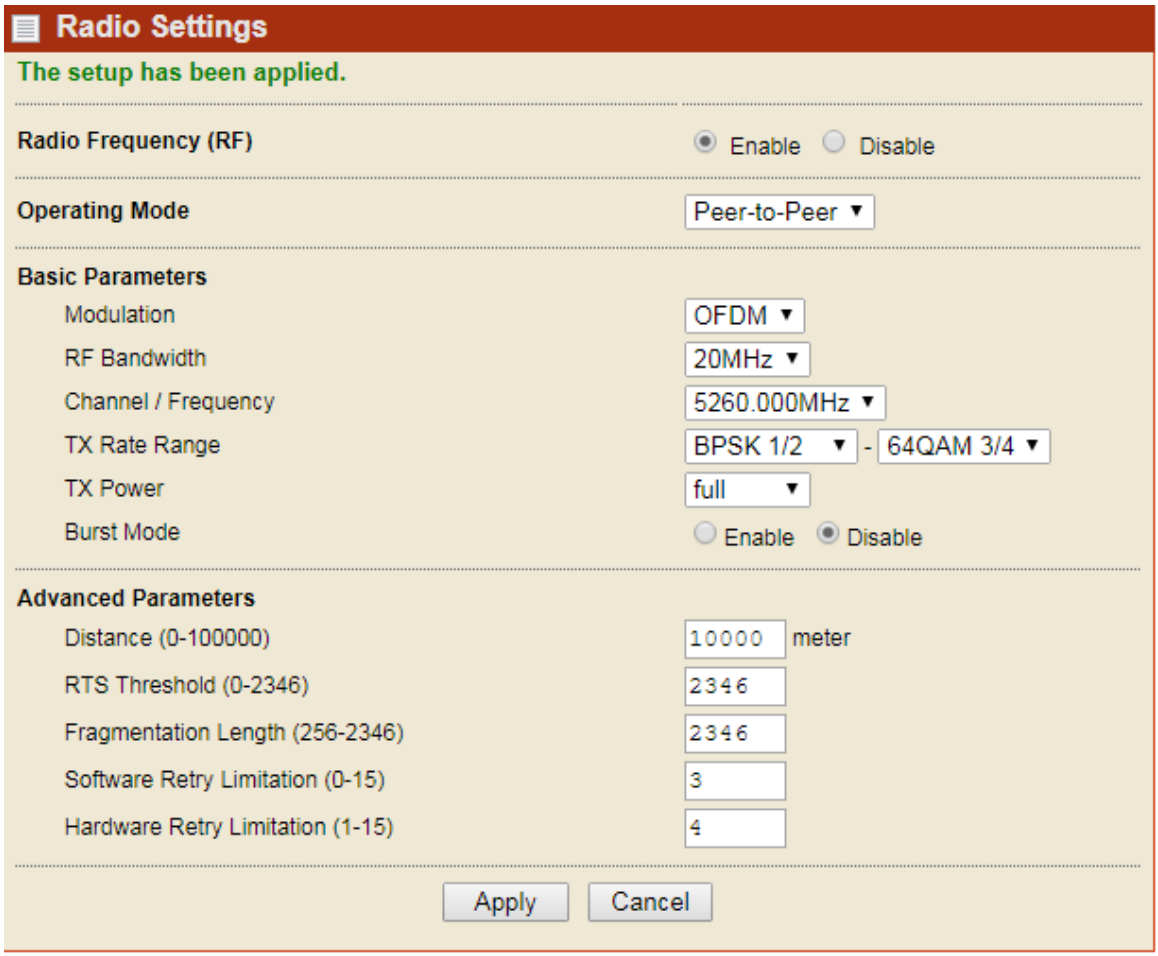
Specify the dedicated base station to avoid connecting another BS with same SSID.

CPE Upload Limitation

Limiting the CPE’s upload capability, the default is 1687 and unlimited.

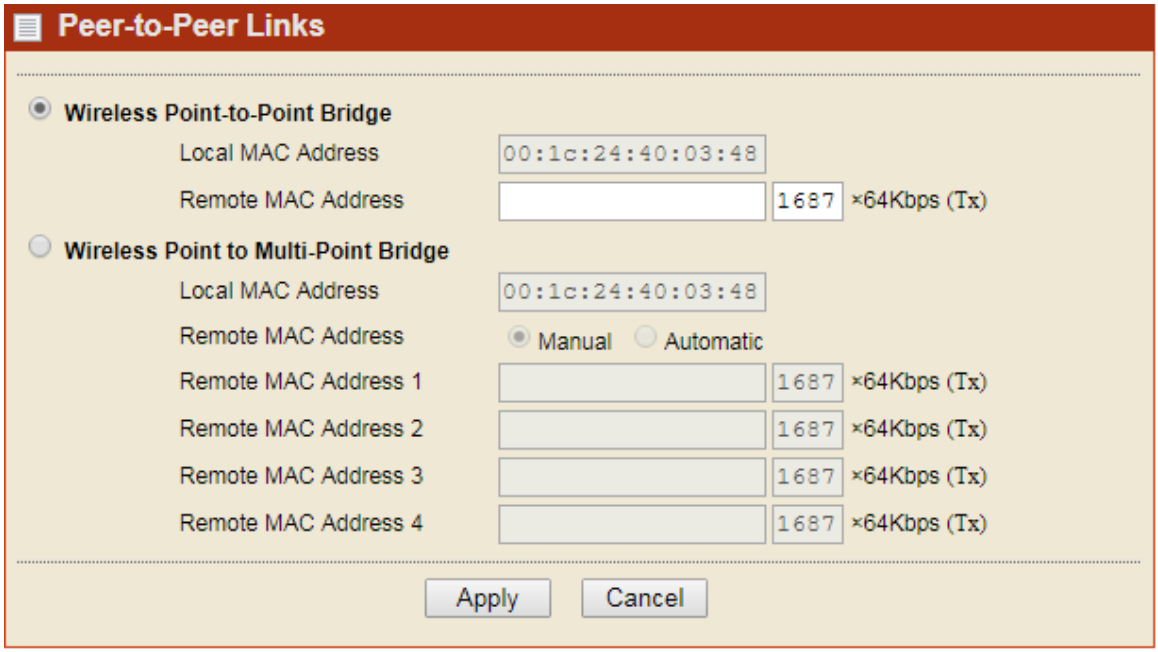
- **Basic Parameters and Advanced Parameters description can be found at page 12&13**

Operating Mode – Peer-to-Peer



- **Basic Parameters and Advanced Parameters description can be found at page 12&13.**
- **Peer-to-Peer Link settings are at page 16.**

Peer-to-Peer Links



- **Operation Mode set to Peer-to-Peer**
- **Selecting Wireless Point-to-Point Bridge or Wireless Point to Multi-Point Bridge**

1. **Wireless Point-to-Point Bridge**
   (1) Filling in the remote mac address at the field.
   (2) Apply to active it

2. **Wireless Point to Multi-Point Bridge**
   Remote MAC Address
   Select Manual for manually input the mac address or Automatic for accepting the remote connect automatically.

   (1) Filling in the remote mac address 1~4 at the field, it can support max. 4 bridge connections at the same time.
   (2) Apply to active it

Security

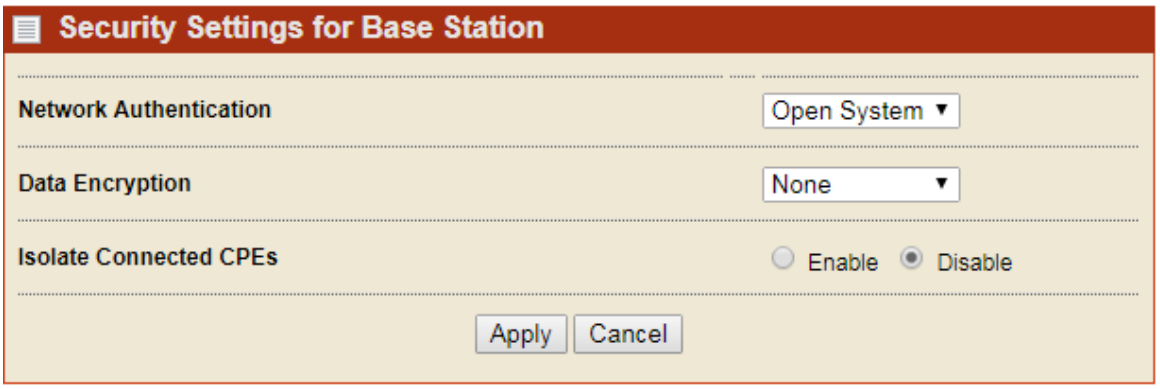


Figure 9 **Security Settings**

Network Authentication

There are Open System/ Shared Key/ WPA PSK/ WPA2 PSK to set, default is Open System.

Open System

It allows any device to join the network without performing any security check.

Shared Key

Data encryption and key are required for wireless authentication

WPA PSK: Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is a security mechanism used to authenticate and validate users on a wireless LAN (WLAN) or Wi-Fi connection. It is a variation of the WPA security protocol. The key should be 8-63 characters.

WPA2 PSK

As a new version of WPA, only all the clients support WPA2 PSK to be connected. Once selected, the data encryption can only be AES and the Pre-shared key is required.

Data Encryption

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.

Isolate Connected CPEs

Enable to active “isolate connected CPEs”, or to disable it.

When disabled it, the CPEs could be connected and transmitted the packets each other. Default is enabled.

Access Control

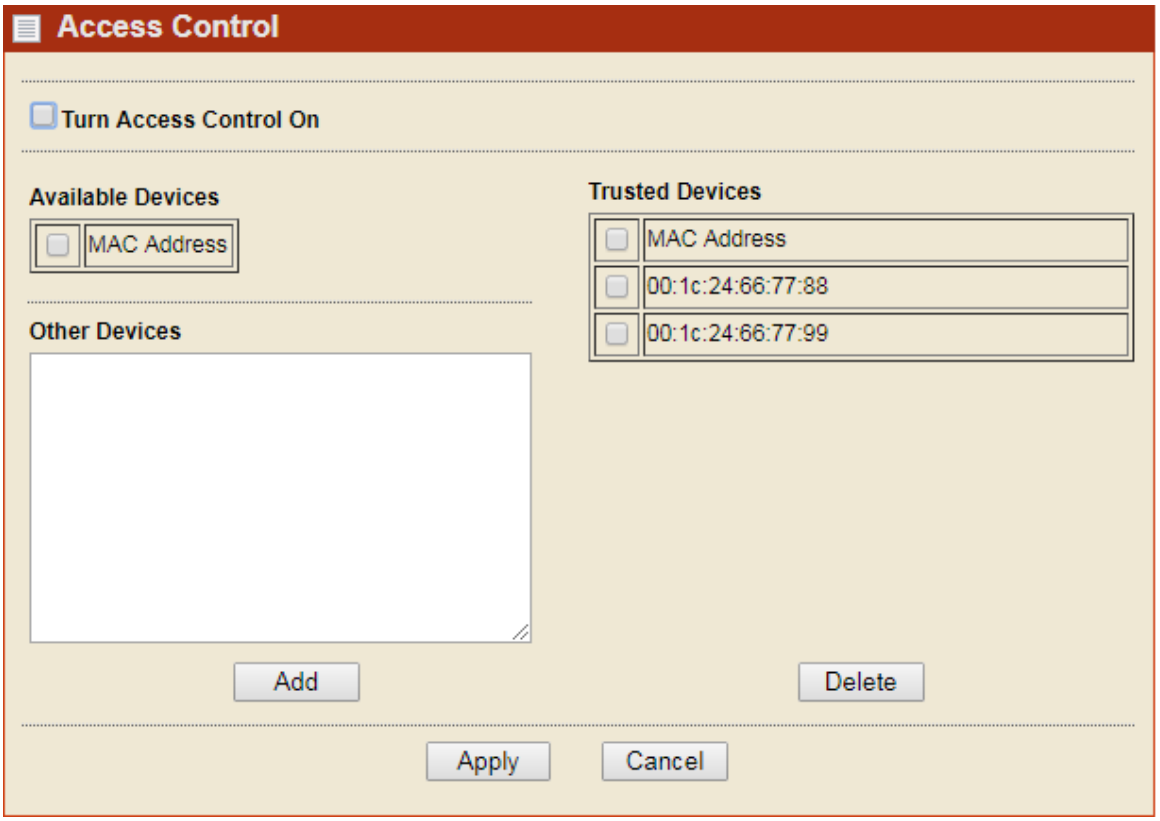


Figure 10 **Security Settings**

The optional Access Control window lets you permit the network to access privilege of the specified stations through the BS. This provides an additional layer of security.

Input the MAC address in the field of Other Devices, then to click Add button and Apply it next.

Those trusted devices MAC are listed. Turn Access Control on to enable the function.

Status

In connection status, you can have those information which includes CPE MAC address, IP address, Modulation/Data rate, RSSI(dBm) and Status.

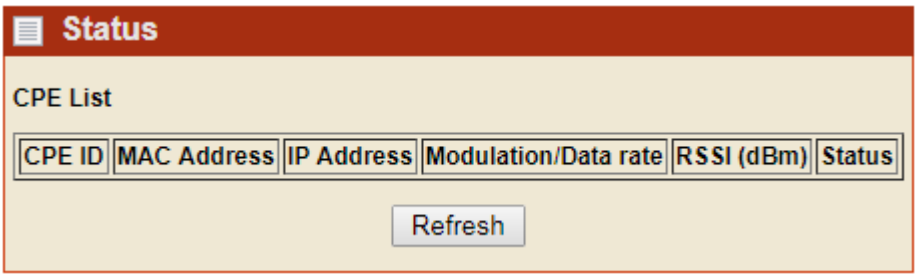


Figure 11 **Status**

Throughput

Wireless Throughput shows graphs which continuously represents the current data traffic on the Wireless interface. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the throughput value. Throughput statistics is updated automatically.

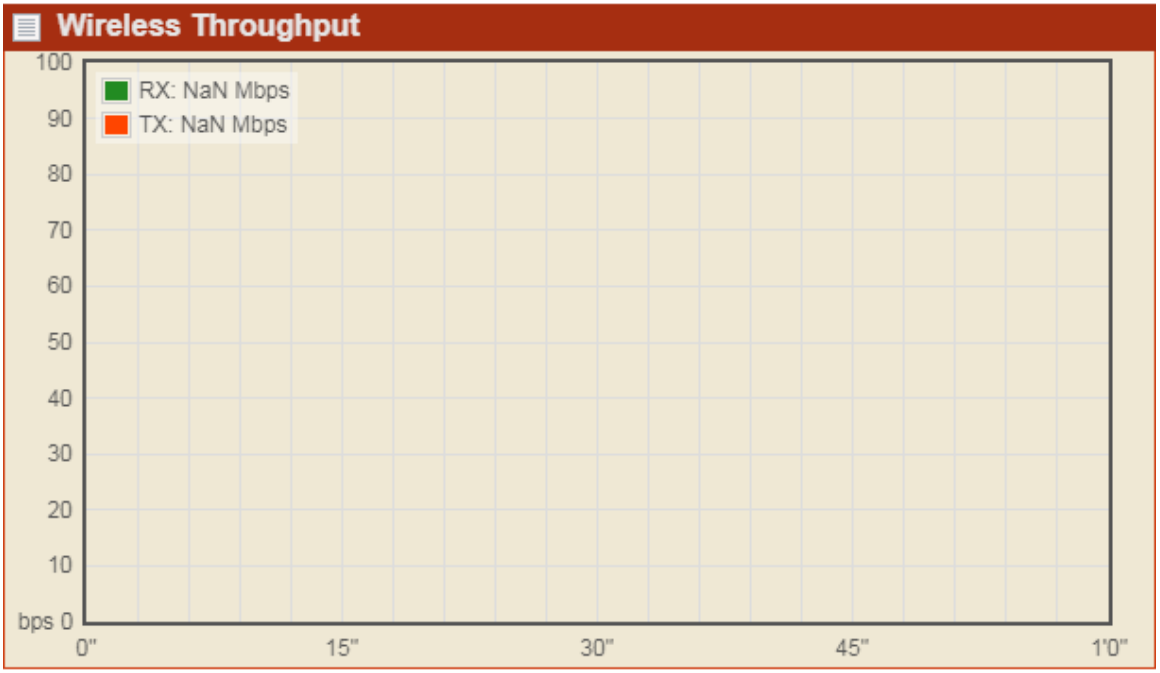


Figure 12 **Wireless Throughput**

Chapter 5 Management

Change Password

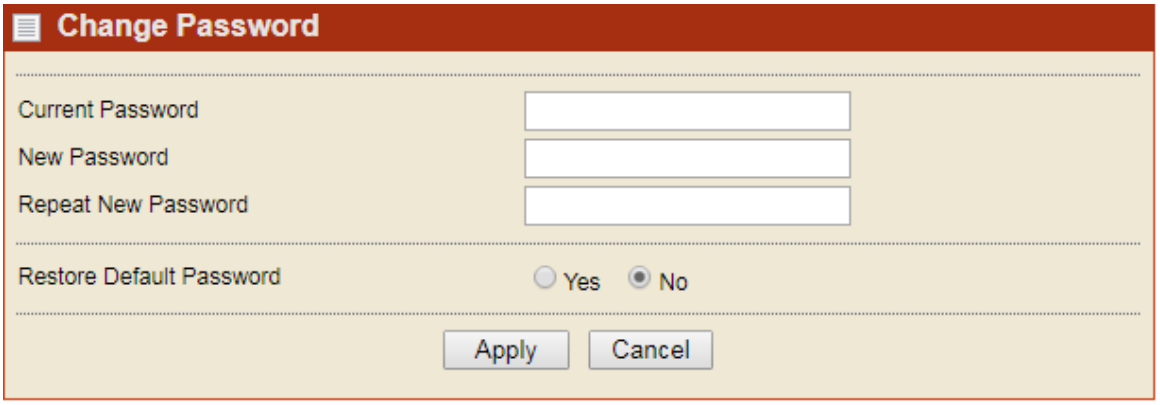


Figure 13 **Change Password**

You can use the Change Password page to change the Access Point administrator's password to access the Settings pages.

To change the password, Type the old password. The default password is “password”. Type a new password and type it again in the Repeat New Password box to confirm it.

Click Apply to have the password changed or click Cancel to keep the current password.

Remote Management

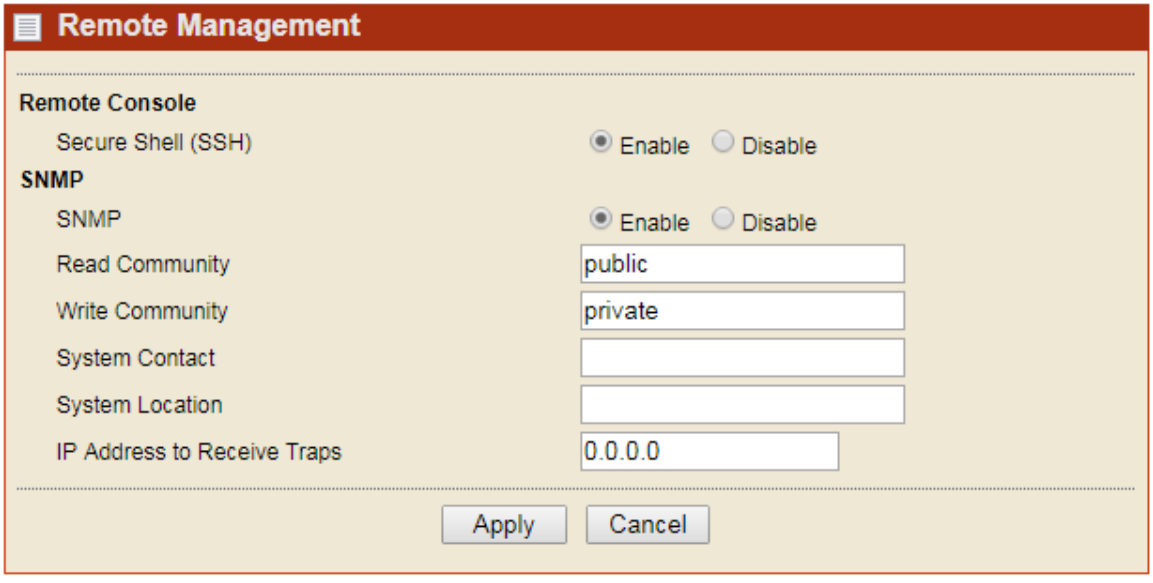


Figure 14 **Remote Management**

Bridge supports SNMP. If you use SNMP to control bridge. At first you should set SNMP settings Active SNMP, and control bridge by SNMP network system.

- Set Read Community password；Default is public

- Set Write Community password；Default is private
- Setting Trap Sever IP address

When bridge is under abnormal condition like bridge power failure or reset is usual.

Administrator can easy control device by exception log in Trap Server.

Upgrade Firmware

Via WEB interface to upgrade firmware：

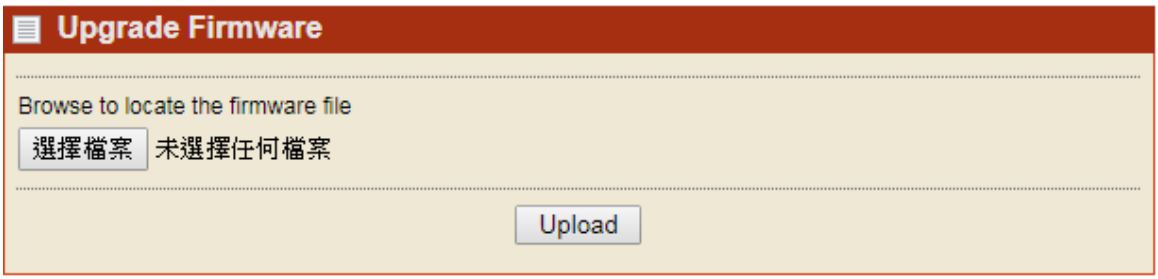


Figure 15 **Upgrade Firmware**

1. Open Upgrade Firmware page
2. Click browser button and select the firmware file in local hard disk.
3. Click Upload button.
4. After upgrade, login again and check the software version.

Backup/Restore

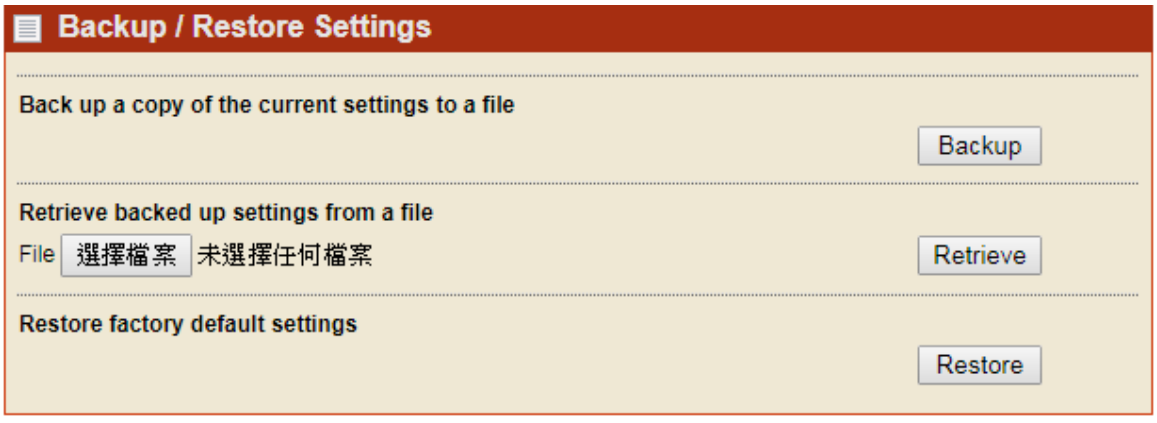


Figure 16 **Backup / Restore**

It would be better to backup settings of device after it work fine, so that you can recover settings quickly when something go wrong.

1. Open"Backup/Restore" page, click "**Backup**", it will pop up a dialog for input path and filename such as F:\device.cfg, and it will save "device.cfg" in the local disk after that.
2. Open "Backup/Restore" page, click "Browser", It will pop up a dialog to choice what file you want to restore, such as "F:\device.cfg", then click "**Retrieve**", the settings of the file will be restored back to device,

and it will active for the device after auto reboot.

3. Open “Backup/Restore” page, click “**Restore**”, It will pop up a dialog to do Restore factory default settings. After applying it, the all settings reset to default.

Time Setting

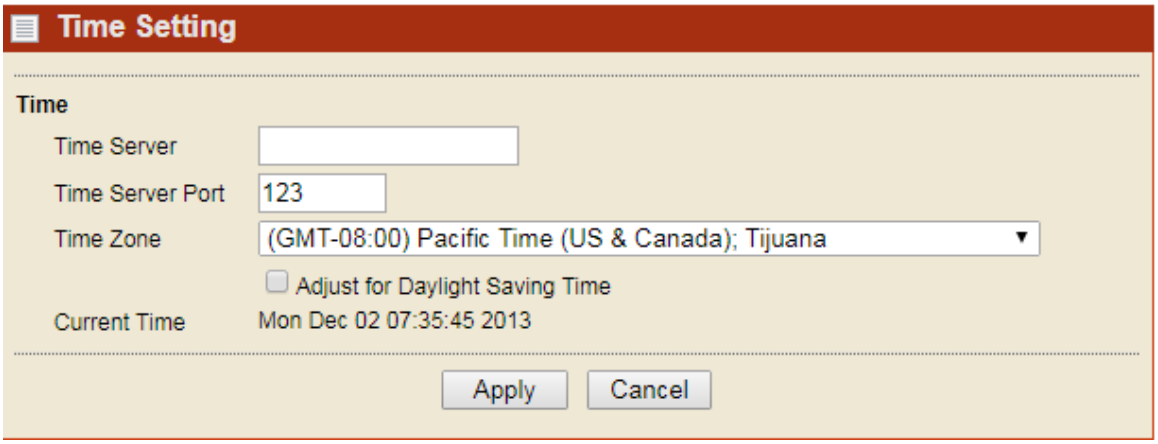


Figure 17 **Time Setting**

Time Server

Specify the time server’s IP

Time Server Port

This field identifies the time server port like 123.

Time Zone

Select the time zone location for your setting.

Current Time

This field identifies the current time in your specific time zone.

Event Log

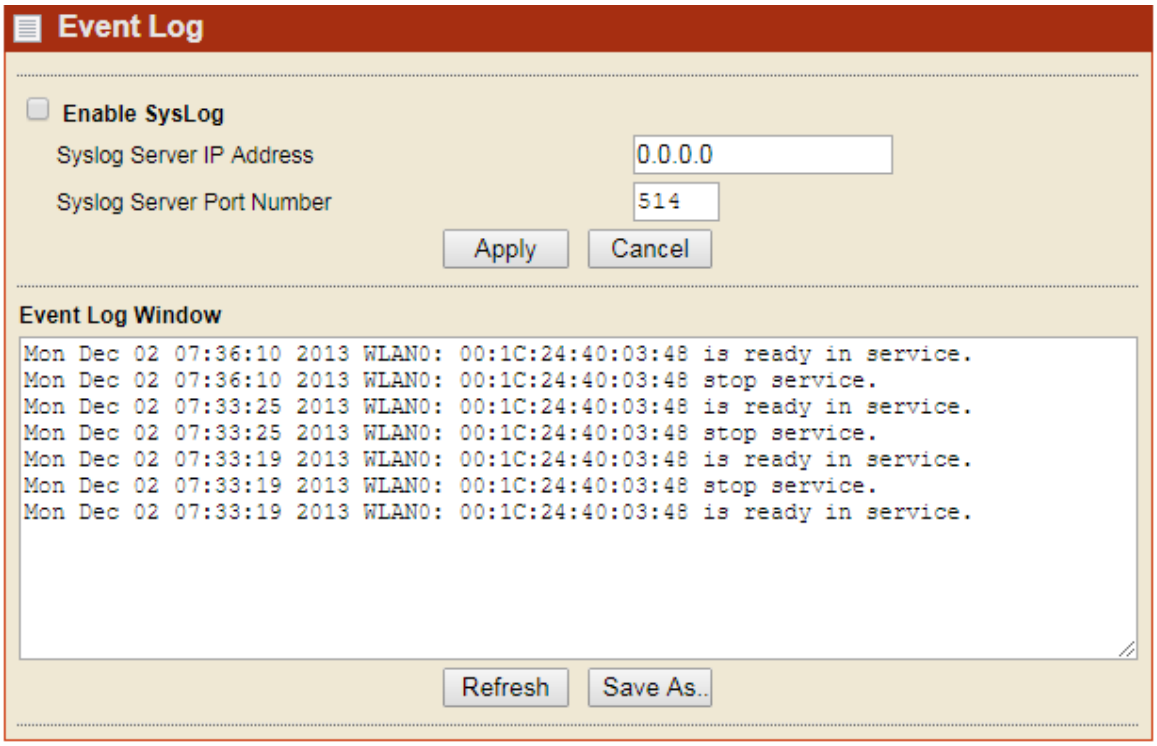


Figure 18 **Event Log**

Event log can show you the event of device, for example, connect, disconnect, reboot of Base station, or something change about settings. If you need long time observational notes, you can active Syslog. Enter Log Sever IP address, the port number configured in the SysLog server on your network. By default, it is514

SysLog Server IP address

The access point will send all the SysLog to the specified IP address if SysLog option is enabled.

Default: 0.0.0.0

Port

The port number was configured in the SysLog server on your network. By default, it is 514

Reboot

When you need to reboot the device, you can click the “yes” button and the click “Apply” it will reboot.

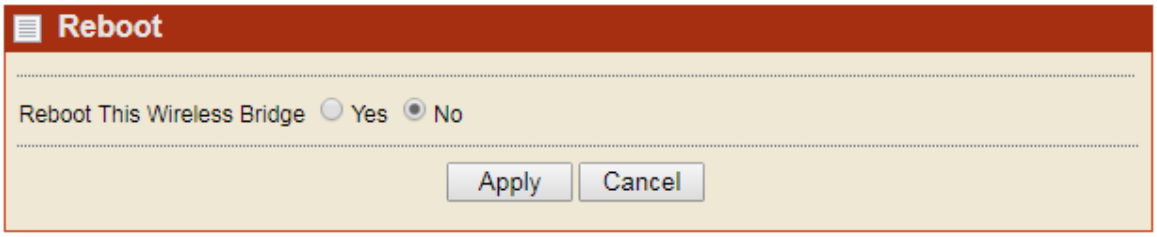


Figure 19 **Reboot**