Handlink AP-100 AP/CPE Configuration Manual

Version 1.0
Date: 10-Sep-2013

Handlink Technologies Inc.
4F, No. 3, Prosperity Rd. 1, Science-Based Industrial Park, Hsinchu 300, Taiwan, R.O.C.

Telephone: +886-3-564-5166
Fax: +886-3-564-3922
Web: www.handlink.com.tw

Customer Support Centre:
Email: handlinksupport@handlink.com.tw

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures

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.

Warning

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.

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

Please install a lightning arrestor to protect the base station from lightning dissipation during rainstorms. Lightning arrestors are mounted outside the structure and must be grounded by means of a ground wire to the nearest ground rod or item that is grounded.

Disclaimer

All specifications are subject to changes without prior notice. Handlink Technologies Inc. assumes no responsibilities for any inaccuracies in this document or for any obligation to update information in this document. This document is provided for information purposes only. Handlink Technologies Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Content Table

Manual Conventions

Bold	Bold type within paragraph text indicates commands, files names, directory names, paths, output, or returned values.
Italic	Within commands, italics indicate a variable that the user must specify. Titles of manuals or other published documents are also set in italics.
_____	Underline means that you have to pay attention to the words.
`Courier`	The courier font indicates output or display.
[ ]	Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit.
{ }	Within commands, item enclosed in braces are options which the user must choose from.
|	Within commands, the vertical bar separates options.
…	An ellipsis indicates a repetition of preceding parameter.
>	The right angle bracket separates successive menu selection.

NOTE: This message denotes neutral or positive information that calls out important points to the text. A note provides information that applies only in special cases.

⚠ **Caution:** Cautions call special attention to hazards that can cause system damage or data corruption, to a lesser degree than warnings.

⚠ **Warnings:** Warnings call special attention to hazards that can cause system damage, data corruption, personal injury, or death.

1. Introduction

This manual is to summarize how to perform basic configuration for the Handlink AP-100 AP/CPE through web-admin interface.

2. AP-100 Model and Firmware Version

This manual is applicable for the following models, hardware and firmware versions:

Product name : **AP-100 AP/CPE**

Hardware Platform	Firmware Version
V1.0	*1.2.4.701*

Table 1 AP-100 Model

3. New Functions Introduction

This table is the new functions description：

No.	**New functions description**	**Property**	**Module**	**Chapter**
1				
2				
3				
4				
5				
6				
7				

Table 2 New Function Introduction

4. Getting Started

4.1. Setup Local Area Connection on Your PC

AP-100 AP/CPE can be connected to your PC in wired mode or in wireless mode. In the following, wired mode will be introduced. This is because the configurations are similar in wireless mode, except SSID has to be configured in both AP-100 AP/CPE and PC.

- AP-100 AP/CPE can be connected to your PC directly or by a switch or a hub.

Start Network Configuration on your PC.

For Windows XP user,

1. Click the "**Start**" menu and choose "**Control Panel**".
2. Click "**Network Connections**".

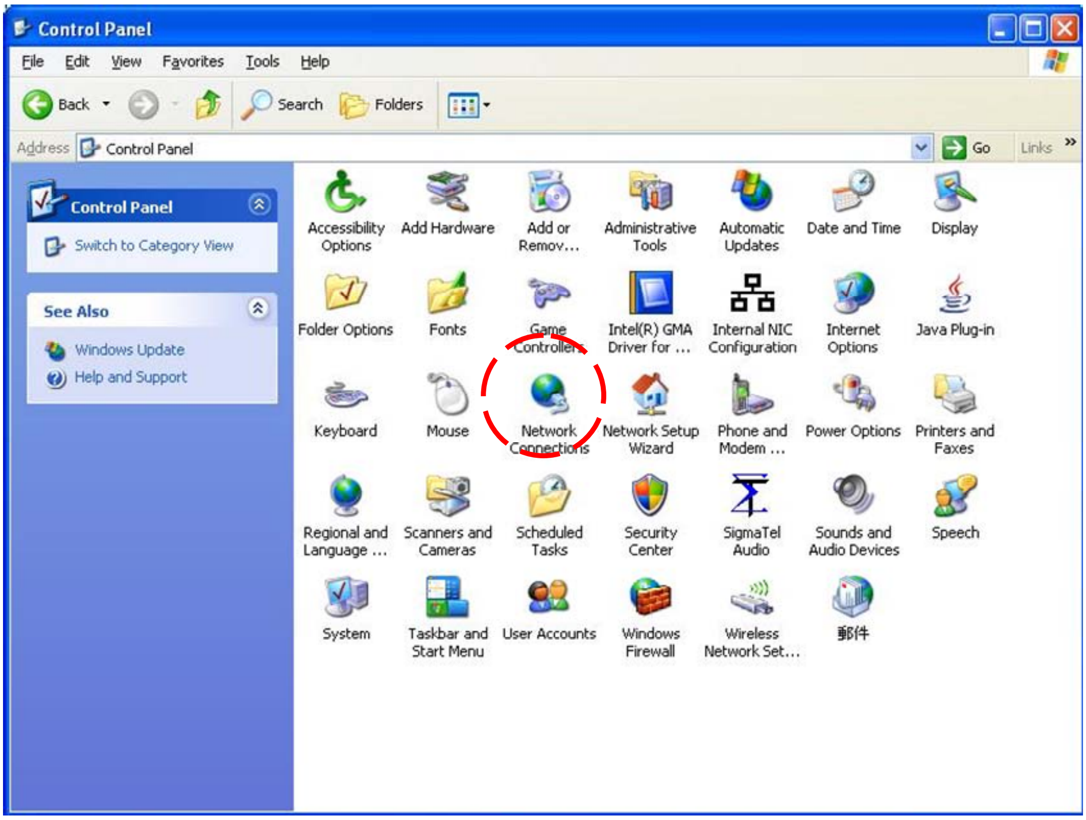


Figure 4-1 Control Panel in Windows XP

3. Right-click the “**Local Area Connection**” and select “**Properties**”.

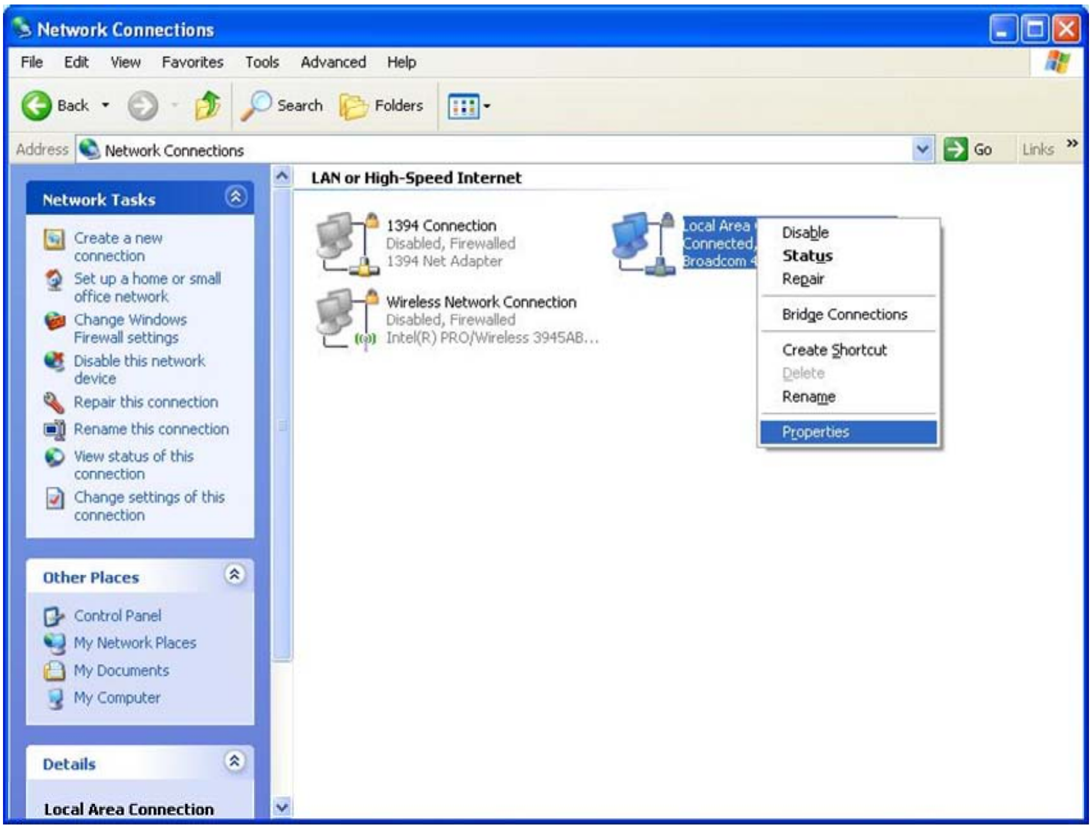
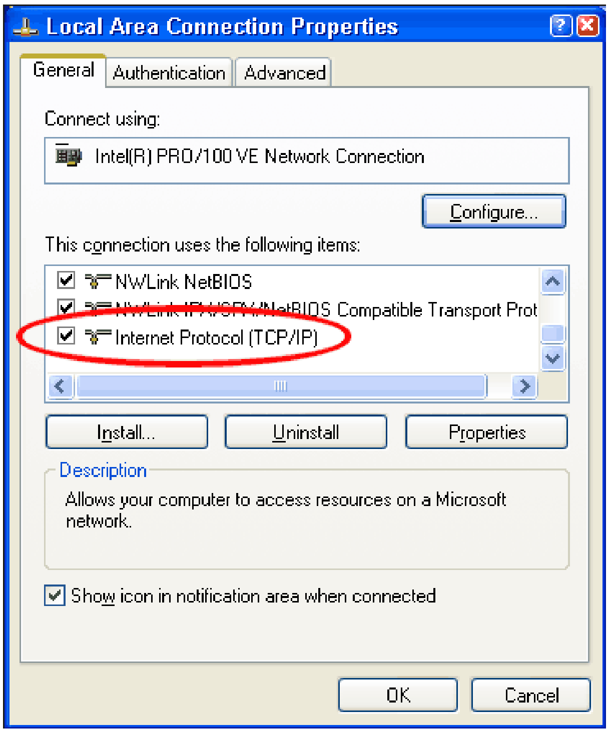


Figure 4-2 Network Connection in Windows XP

4. After clicking “**Properties**”, you will see the diagram as below.



Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ NWLink NetBIOS

☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot

☑ Internet Protocol (TCP/IP)

Description

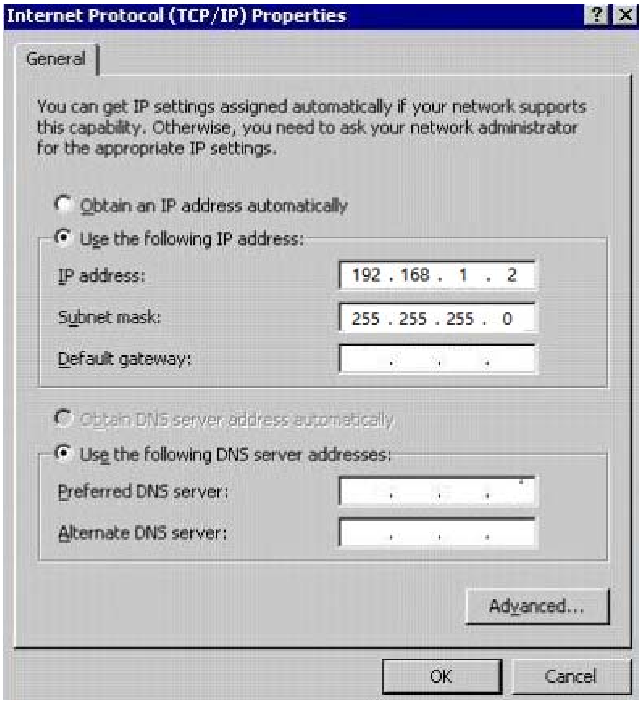
Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

Figure 4-3 Local Area Connection Properties in Windows XP

5. Mark the “Internet Protocol (TCP/IP)” and click “**Properties**”.

6. Type in an "**IP address**", for example, 192.168.1.2, which is under the same subnet as the Default IP Address of AP-100 AP/CPE (10.59.100.1).
7. Using the default "**Subnet mask**" (default: 255.255.255.0) setting in the first time.
8. Keep the "**Default gateway**" as "Blank".
9. Keep the "**Preferred DNS server**" and "**Alternate DNS server**" as "Blank" also.
10. Click "**OK**" when you finish setting and close the Window.



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

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: . . .

Figure 4-4 Internet Protocol (TCP/IP) Properties in Windows XP

4.2. Check Access

"ping" utility of Command Prompt is a handy tool to check the access to the AP-100 AP/CPE.

1. Go to the Command Prompt by typing "cmd" in "**Run**".
2. Type command:

```
ping 10.59.100.1
```

The AP-100 AP/CPE shall respond to your ping request if AP-100 AP/CPE and your PC have a correct connection.

NOTE: Using the same PC to ping different AP-100 AP/CPE may cause ping failure. This is because AP-100 AP/CPE has the same default IP address but different MAC addresses. You need to type command "arp –d" in Command Prompt to clear ARP table on PC before each ping.

4.3. Configuration with Web-Admin

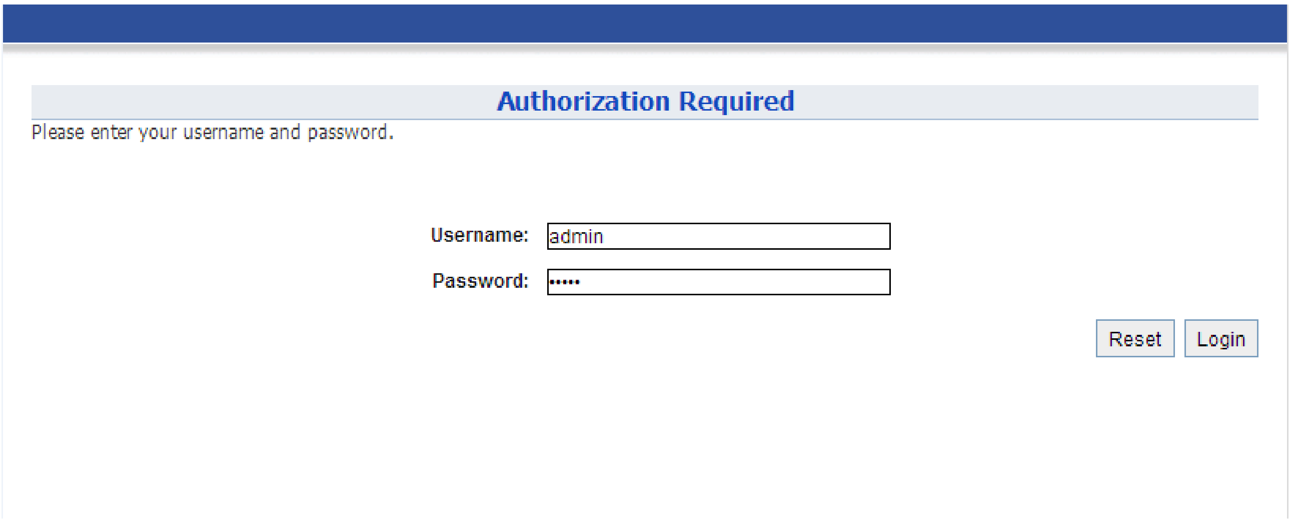
The AP-100 can be accessed through a Web Browser, for example, Internet Explorer (IE).

1. Open an IE session and type the IP address of the AP-100 AP/CPE. Example: http://10.59.100.1 or https://10.59.100.1, where 10.59.100.1 is the AP-100's IP address. The ***default IP Address*** is ***10.59.100.1***.

2. A window will pop up, as shown in figure 4-5. Enter the user name and password in the corresponding fields, which are the same as for the CLI. The ***default User Name*** and ***Password*** are shown in Table 3. They are **case sensitive**.

Firmware version	Default User Name	Default Password
1.2.4.701	***admin***	***admin***

Table 3 AP-100 default User Name and Password



Authorization Required

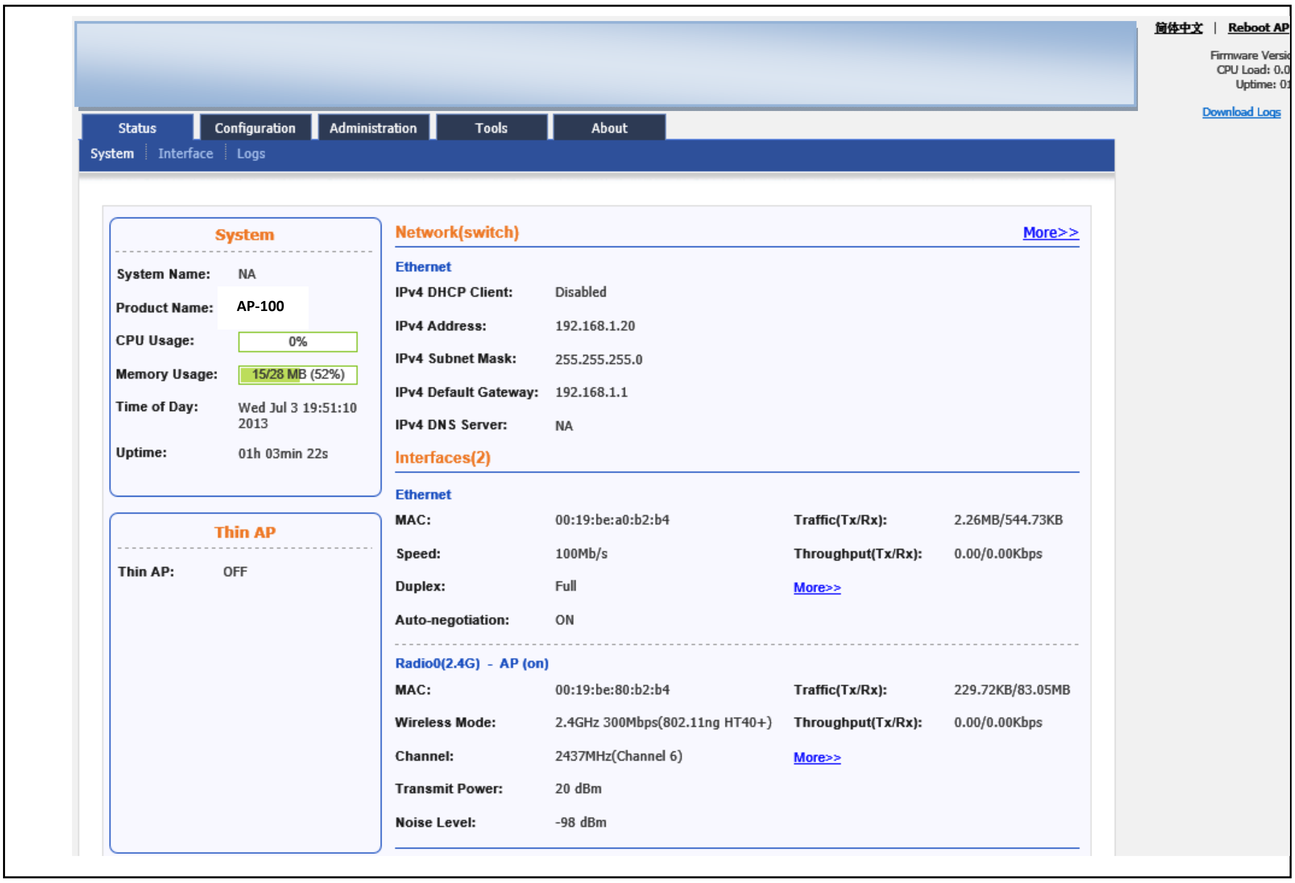
Please enter your username and password.

Username: admin

Password: •••••

Figure 4-5 Enter User Name and Password

3. A login page in IE appears, as shown in figure 4-6. A **Menu Bar** is located on the top of the IE window. Different functions can be accessed through the menu bar.



Firmware Versi
CPU Load: 0.0
Uptime: 01
Download Logs

System

System Name:	NA
Product Name:	AP-100
CPU Usage:	0%
Memory Usage:	15/28 MB (52%)
Time of Day:	Wed Jul 3 19:51:10 2013
Uptime:	01h 03min 22s

Thin AP

Thin AP: OFF

Network(switch) More>>

Ethernet

IPv4 DHCP Client:	Disabled
IPv4 Address:	192.168.1.20
IPv4 Subnet Mask:	255.255.255.0
IPv4 Default Gateway:	192.168.1.1
IPv4 DNS Server:	NA

Interfaces(2)

Ethernet

MAC:	00:19:be:a0:b2:b4	Traffic(Tx/Rx):	2.26MB/544.73KB
Speed:	100Mb/s	Throughput(Tx/Rx):	0.00/0.00Kbps
Duplex:	Full	More>>	
Auto-negotiation:	ON		

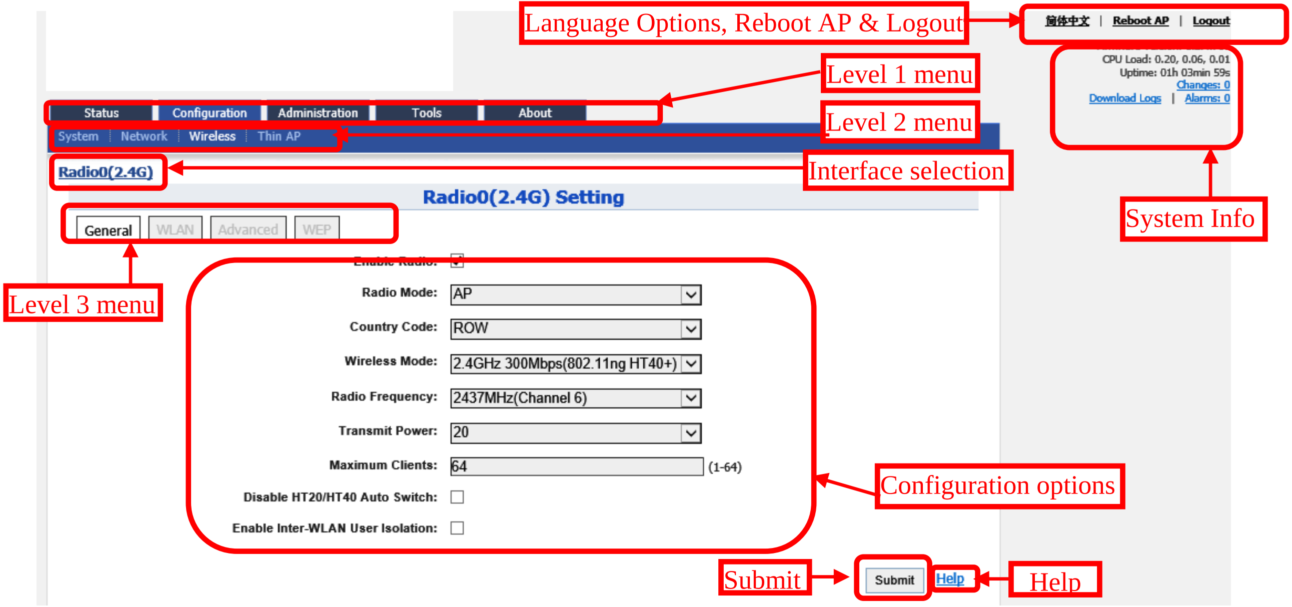
Radio0(2.4G) - AP (on)

MAC:	00:19:be:80:b2:b4	Traffic(Tx/Rx):	229.72KB/83.05MB
Wireless Mode:	2.4GHz 300Mbps(802.11ng HT40+)	Throughput(Tx/Rx):	0.00/0.00Kbps
Channel:	2437MHz(Channel 6)	More>>	
Transmit Power:	20 dBm		
Noise Level:	-98 dBm		

Figure 4-6 Web-admin Login Page

4.4. Interface Introduction

AP-100 interface is separated to 5 levels: Level 1 menu, Level 2 menu, Interface selection, Level 3 menu and Configuration options



Language Options, Reboot AP & Logout

Level 1 menu

Level 2 menu

Interface selection

System Info

Level 3 menu

Configuration options

Submit

Help

CPU Load: 0.20, 0.06, 0.01
Uptime: 01h 03min 59s
Changes: 0
Download Logs | Alarms: 0

Radio0(2.4G) Setting

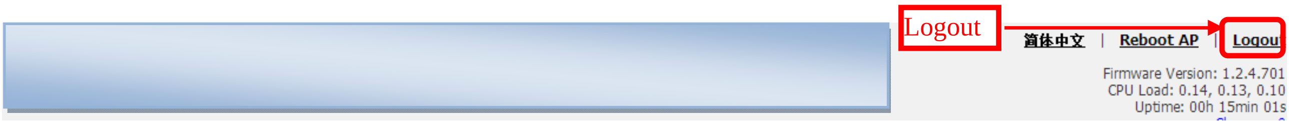
Enable Radio:	☑
Radio Mode:	AP
Country Code:	ROW
Wireless Mode:	2.4GHz 300Mbps(802.11ng HT40+)
Radio Frequency:	2437MHz(Channel 6)
Transmit Power:	20
Maximum Clients:	64 (1-64)
Disable HT20/HT40 Auto Switch:	☐
Enable Inter-WLAN User Isolation:	☐

Figure 4-7 AP-100 Webpage

4.5. Logout from AP-100 Interface

On the right top corner of AP-100 Web interface, click “Logout” button to logout from AP-100.

On the other side, you can directly close AP-100 webpage to logout from AP-100.



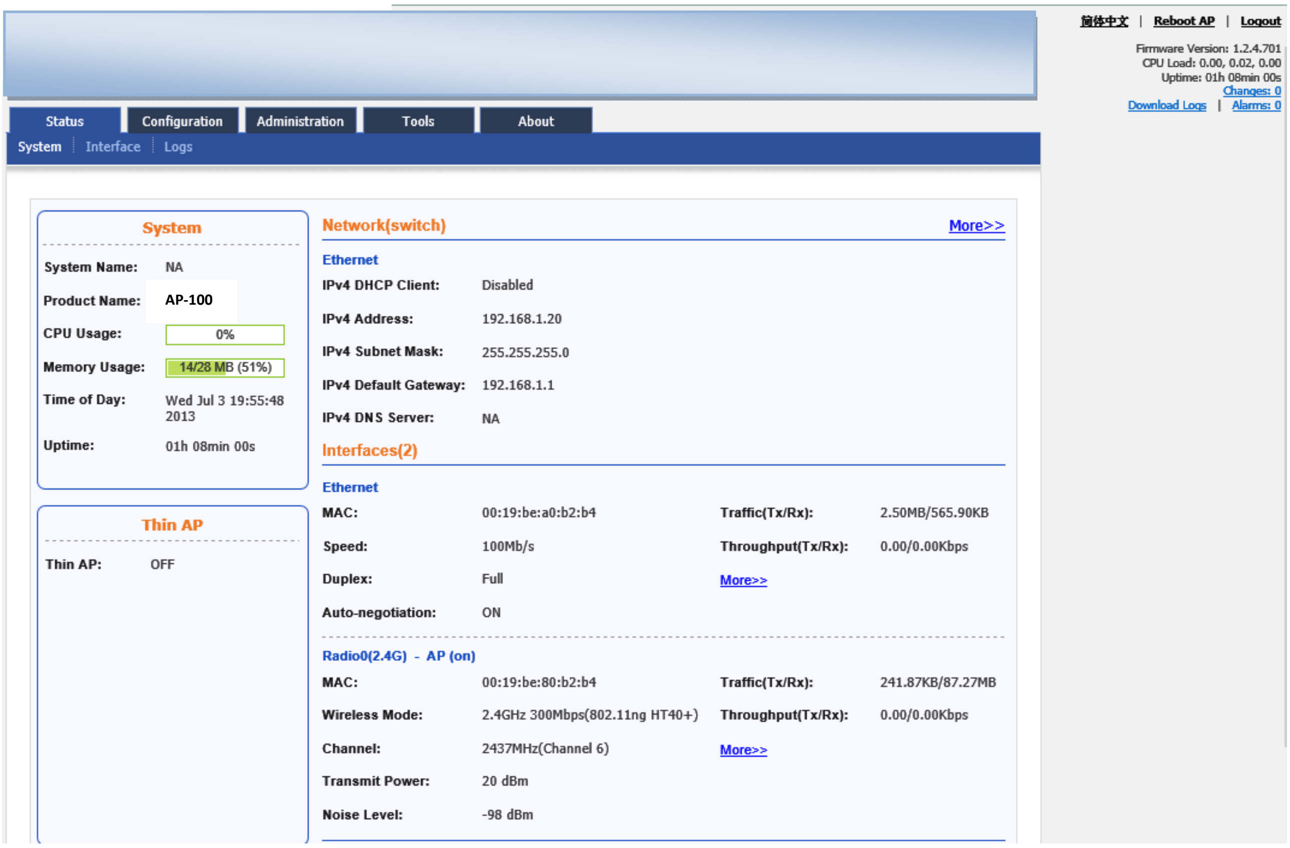
Firmware Version: 1.2.4.701
CPU Load: 0.14, 0.13, 0.10
Uptime: 00h 15min 01s

Figure 4-8 Logout

5. System Status

AP-100 Status function gives System information, interface information, Log.

You can select **Status** -> **System** to check AP-100 basic information and real-time status.



Firmware Version: 1.2.4.701
CPU Load: 0.00, 0.02, 0.00
Uptime: 01h 08min 00s

System

System Name: NA
Product Name: AP-100
CPU Usage: 0%
Memory Usage: 14/28 MB (51%)
Time of Day: Wed Jul 3 19:55:48 2013
Uptime: 01h 08min 00s

Thin AP

Thin AP: OFF

Network(switch)

Ethernet
IPv4 DHCP Client: Disabled
IPv4 Address: 192.168.1.20
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 192.168.1.1
IPv4 DNS Server: NA

Interfaces(2)

Ethernet
MAC: 00:19:be:a0:b2:b4
Traffic(Tx/Rx): 2.50MB/565.90KB
Speed: 100Mb/s
Throughput(Tx/Rx): 0.00/0.00Kbps
Duplex: Full
Auto-negotiation: ON

Radio0(2.4G) - AP (on)
MAC: 00:19:be:80:b2:b4
Traffic(Tx/Rx): 241.87KB/87.27MB
Wireless Mode: 2.4GHz 300Mbps(802.11ng HT40+)
Throughput(Tx/Rx): 0.00/0.00Kbps
Channel: 2437MHz(Channel 6)
Transmit Power: 20 dBm
Noise Level: -98 dBm

Figure 5-1 System Information

Following information can be found from “System” function:

System

System Name： System name for AP-100, it can be customized by customer.

Product Name： AP-100.

CPU Loading： AP-100 CPU Loading.

CPU Usage： AP-100 CPU Usage (%).

Memory Usage：AP-100 memory Usage (Byte).

Thin AP

Show the status of thin AP function (On/Off).

Network (Switch/Gateway)

It shows the status and information of network. It is switch mode as default.

IPv4 DHCP Client：Enable/disable IPv4 DHCP Client.

IPv4 Address：AP-100 current IPv4 address

IPv4 Subnet Mask：AP-100 IPv4 subnet mask

IPv4 Default Gateway Address：AP-100 IPv4 gateway address

Interfaces (2)

Ethernet

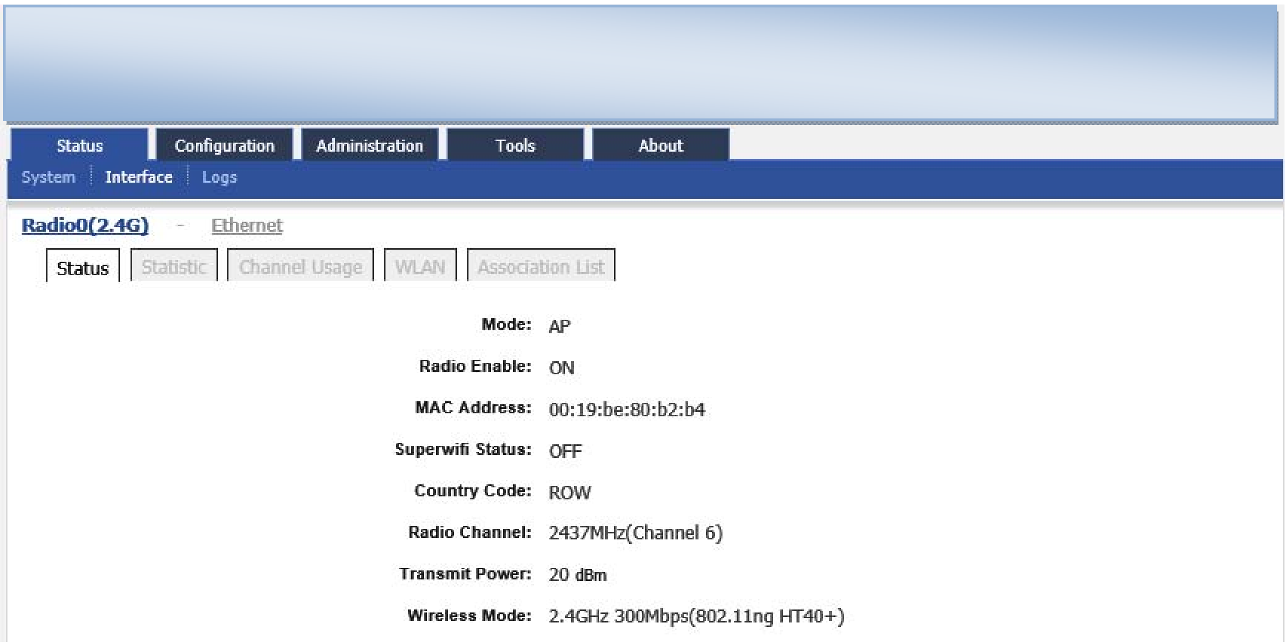
It shows the status and information of Ethernet including Mac address, Traffic (Tx/Rx), Speed, Throughput (Tx/Rx), Duplex and Auto-negotiation. If click the "**More>>**", more detail information will be shown.

Radio (2.4G)

It shows AP-100 Radio0 interface information including Mac address, Traffic (Tx/Rx), Wireless Mode, Throughput (Tx/Rx), Channel, Transmit Power and Noise Level. If click the "**More>>**", more detail information will be shown. As default, the 2.4G radio is on.

5.1. Interface

You can select **Status** -> **Interface** to check interface information which includes radio0 (2.4GHz) and Ethernet information.



Mode: AP

Radio Enable: ON

MAC Address: 00:19:be:80:b2:b4

Superwifi Status: OFF

Country Code: ROW

Radio Channel: 2437MHz(Channel 6)

Transmit Power: 20 dBm

Wireless Mode: 2.4GHz 300Mbps(802.11ng HT40+)

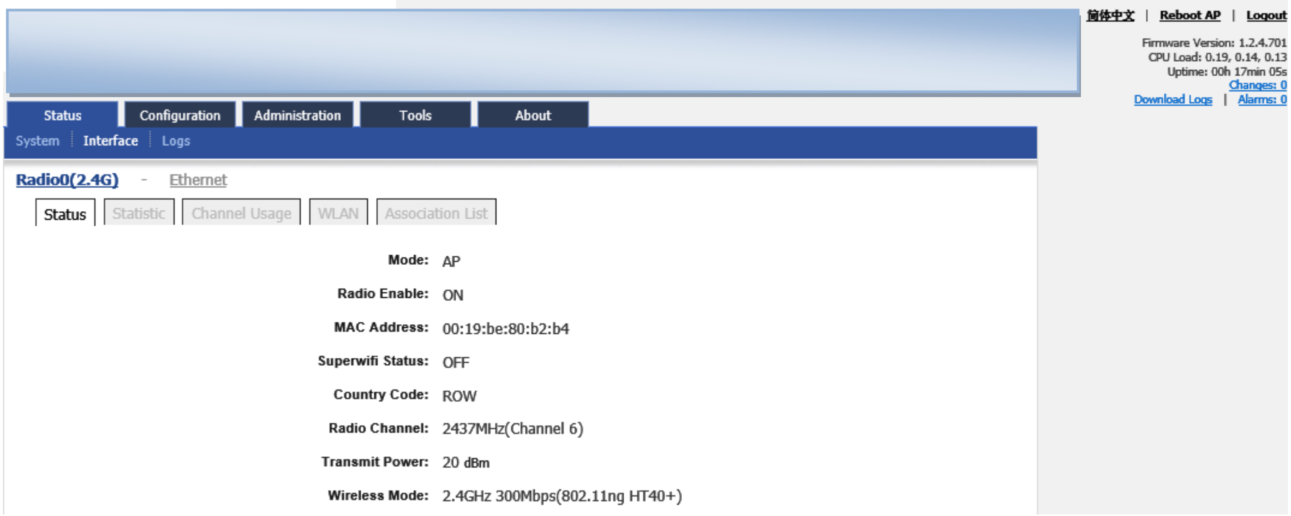
Figure 5-2 Interface Status

5.1.1. 2.4G Interface Status

By selecting **Status** -> **Interface**-> **Radio0(2.4G)** you can find 2.4G interface (radio0) information which includes following 5 parts: Status, Statistic, Channel Usage, WLAN and Association List.

5.1.1.1. Status

Please select **Status** -> **Interface**-> **Radio0(2.4G)** -> **Status** to check radio0 status, the webpage provides radio0 Mode, Radio Enable/Disable, MAC Address, Superwifi Status, Country Code, Radio Channel, Transmit Power and Wireless Mode.



Firmware Version: 1.2.4.701
CPU Load: 0.19, 0.14, 0.13
Uptime: 00h 17min 05s

Mode: AP

Radio Enable: ON

MAC Address: 00:19:be:80:b2:b4

Superwifi Status: OFF

Country Code: ROW

Radio Channel: 2437MHz(Channel 6)

Transmit Power: 20 dBm

Wireless Mode: 2.4GHz 300Mbps(802.11ng HT40+)

Figure 5-3 Interface Status

Mode： Operation mode

Radio Enable：Radio0 (2.4G) status (ON/OFF)

MAC Address：Radio0 (2.4G) MAC address.

Superwifi Status：Superwifi Status (ON/OFF), as default, it is on.

Country Code：Country Code.

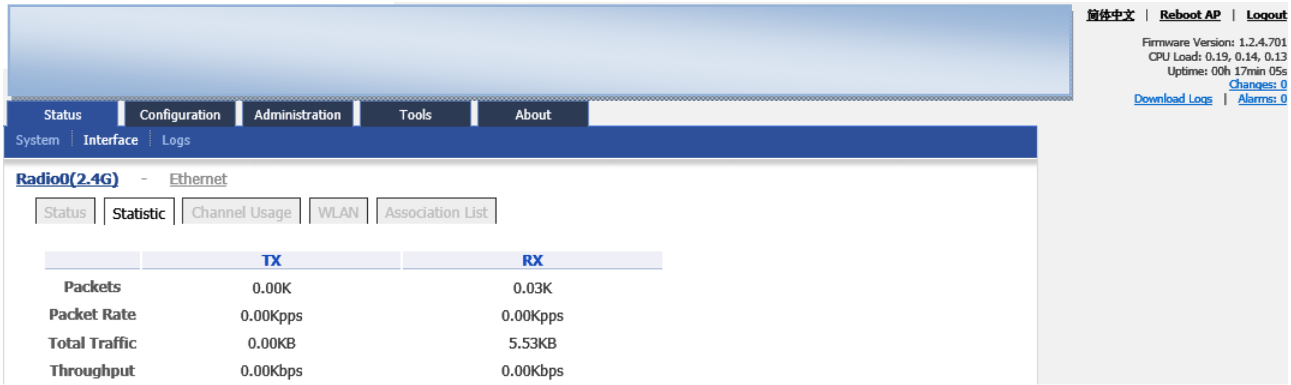
Radio Channel：Radio0 (2.4G) current channel

Transmit Power：Radio0 (2.4G) transmit power

Wireless Mode：Radio0 (2.4G) wireless mode

5.1.1.2. Statistic

Please select **Status** -> **Interface**-> **radio0(2.4G)** -> **Statistic** to check radio0 statistics information which includes radio0 Tx and Rx Packets, Tx and Rx Packet Rate, Total traffic, Throughput.



Firmware Version: 1.2.4.701
CPU Load: 0.19, 0.14, 0.13
Uptime: 00h 17min 05s
Changes: 0
Download Logs | Alarms: 0

	TX	RX
Packets	0.00K	0.03K
Packet Rate	0.00Kpps	0.00Kpps
Total Traffic	0.00KB	5.53KB
Throughput	0.00Kbps	0.00Kbps

Figure 5-4 Interface Statistic

Packets： Radio0 (2.4G) received and sent packets.

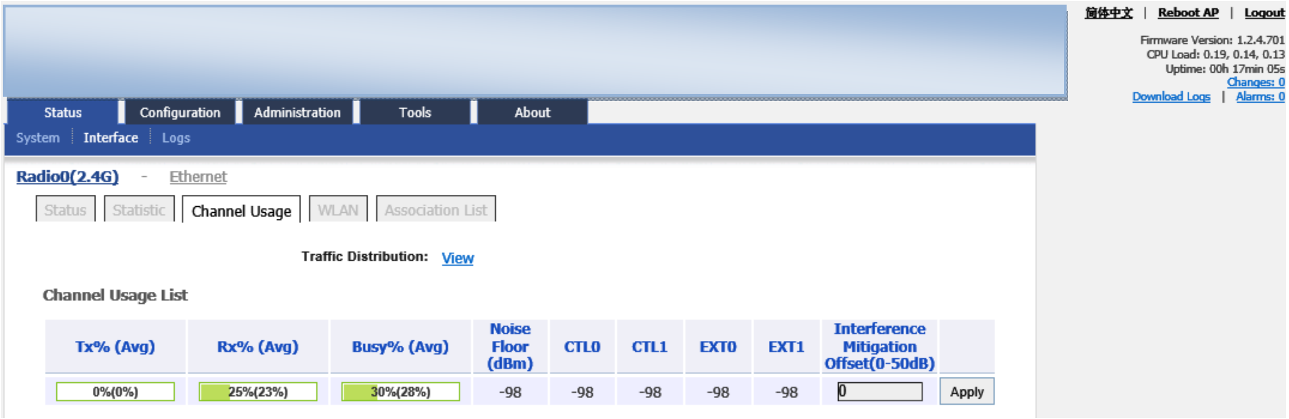
Packet Rate： Radio0 (2.4G) packet rate.

Total Traffic： Radio0 (2.4G) received and sent total traffic.

Throughput： Radio0 (2.4G) throughput.

5.1.1.3. Channel Usage

Please select **Status** -> **Interface**-> **Radio0(2.4G)** -> **Channel Usage** to check radio0 channel usage information including: state, Tx Frame（%）, Rx Frame（%）, Busy State（%）, Noise Floor（dBm）, CTL0, CTL1, EXT0, EXT1, Interference Mitigation Offset(0-50dB) and Traffic Distribution.



Firmware Version: 1.2.4.701
CPU Load: 0.19, 0.14, 0.13
Uptime: 00h 17min 05s
Changes: 0
Download Logs | Alarms: 0

Traffic Distribution: View

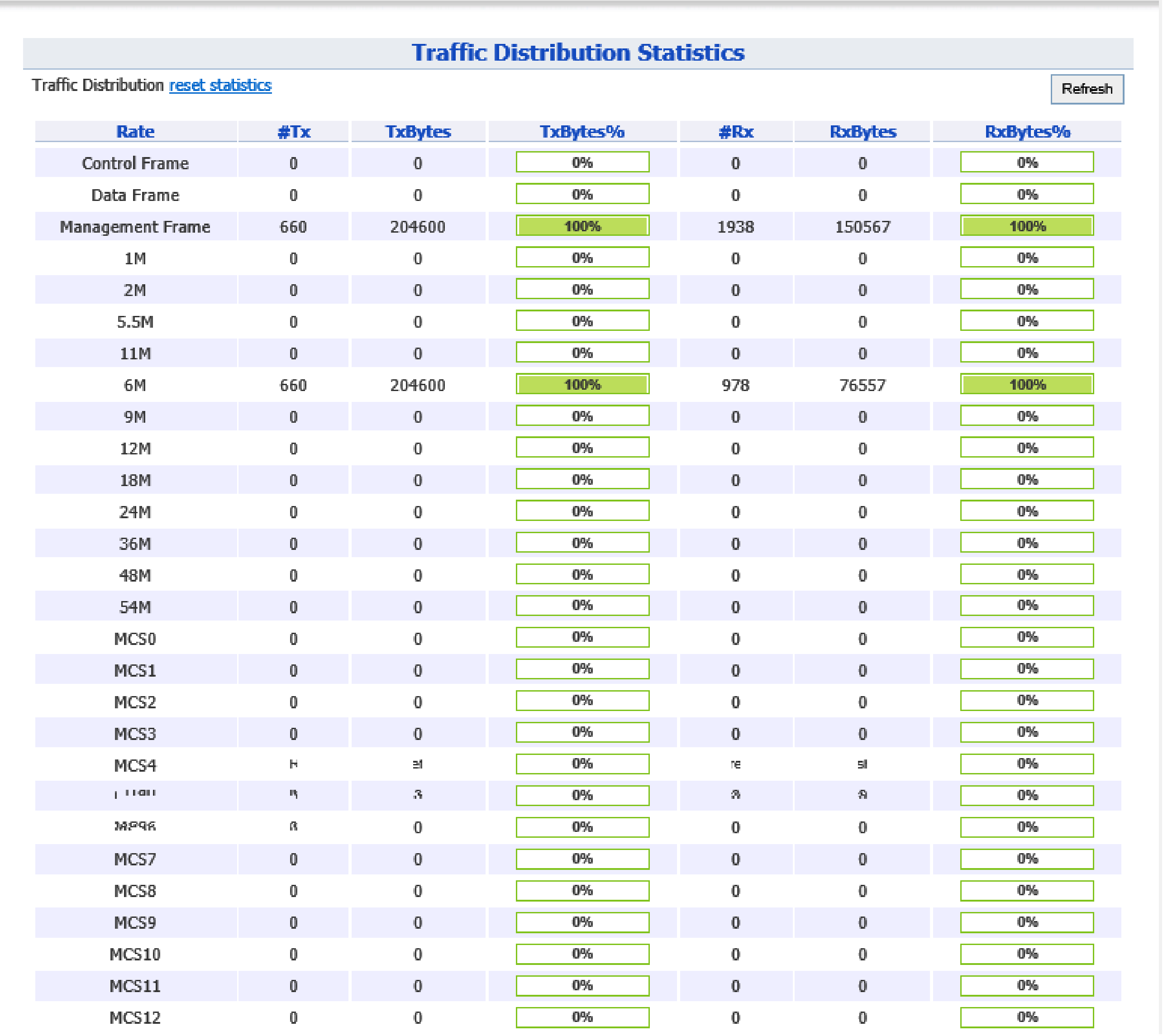
Channel Usage List

Tx% (Avg)	Rx% (Avg)	Busy% (Avg)	Noise Floor (dBm)	CTL0	CTL1	EXT0	EXT1	Interference Mitigation Offset(0-50dB)	
0%(0%)	25%(23%)	30%(28%)	-98	-98	-98	-98	-98	0	Apply

Figure 5-5 Channel Usage

Interference Mitigation Offset(0-50dB)：This option will mask all noise / valid signal below "0-50" dB.

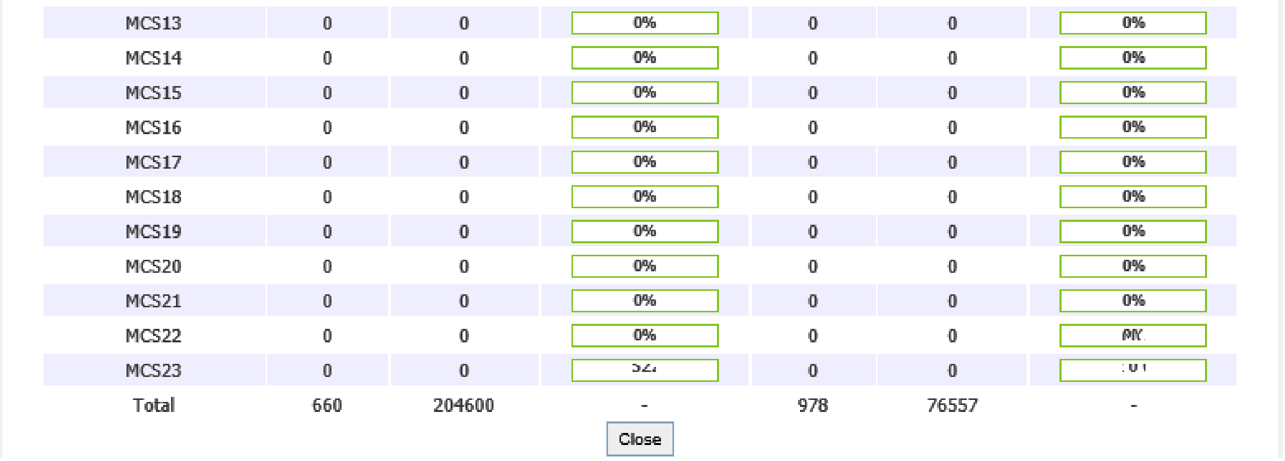
The traffic distribution statistics will be shown by clicking "**View**" on the channel usage page.



Traffic Distribution Statistics

Traffic Distribution reset statistics

Rate	#Tx	TxBytes	TxBytes%	#Rx	RxBytes	RxBytes%
Control Frame	0	0	0%	0	0	0%
Data Frame	0	0	0%	0	0	0%
Management Frame	660	204600	100%	1938	150567	100%
1M	0	0	0%	0	0	0%
2M	0	0	0%	0	0	0%
5.5M	0	0	0%	0	0	0%
11M	0	0	0%	0	0	0%
6M	660	204600	100%	978	76557	100%
9M	0	0	0%	0	0	0%
12M	0	0	0%	0	0	0%
18M	0	0	0%	0	0	0%
24M	0	0	0%	0	0	0%
36M	0	0	0%	0	0	0%
48M	0	0	0%	0	0	0%
54M	0	0	0%	0	0	0%
MCS0	0	0	0%	0	0	0%
MCS1	0	0	0%	0	0	0%
MCS2	0	0	0%	0	0	0%
MCS3	0	0	0%	0	0	0%
MCS4	[illegible]	[illegible]	0%	[illegible]	[illegible]	0%
[illegible]	[illegible]	[illegible]	0%	[illegible]	[illegible]	0%
[illegible]	[illegible]	0	0%	0	0	0%
MCS7	0	0	0%	0	0	0%
MCS8	0	0	0%	0	0	0%
MCS9	0	0	0%	0	0	0%
MCS10	0	0	0%	0	0	0%
MCS11	0	0	0%	0	0	0%
MCS12	0	0	0%	0	0	0%



MCS13	0	0	0%	0	0	0%
MCS14	0	0	0%	0	0	0%
MCS15	0	0	0%	0	0	0%
MCS16	0	0	0%	0	0	0%
MCS17	0	0	0%	0	0	0%
MCS18	0	0	0%	0	0	0%
MCS19	0	0	0%	0	0	0%
MCS20	0	0	0%	0	0	0%
MCS21	0	0	0%	0	0	0%
MCS22	0	0	0%	0	0	[illegible]
MCS23	0	0	[illegible]	0	0	[illegible]
Total	660	204600	-	978	76557	-

Figure 5-6 Traffic Distribution Statistics

Tx **Frame**(%)(**Avg**)： Average transmit frames percentage

Rx **Frame**(%)(**Avg**)： Average receive frames percentage

Busy State(%)(**Avg**)：Average busy state percentage

Noise Floor(**dBm**) ：Noise floor

CTL0：Chain 0 Noise Floor of the Control Channel (i.e the operating channel for HT20 case)

CTL1：Chain 1 Noise Floor of the Control Channel (i.e the operating channel for HT20 case)

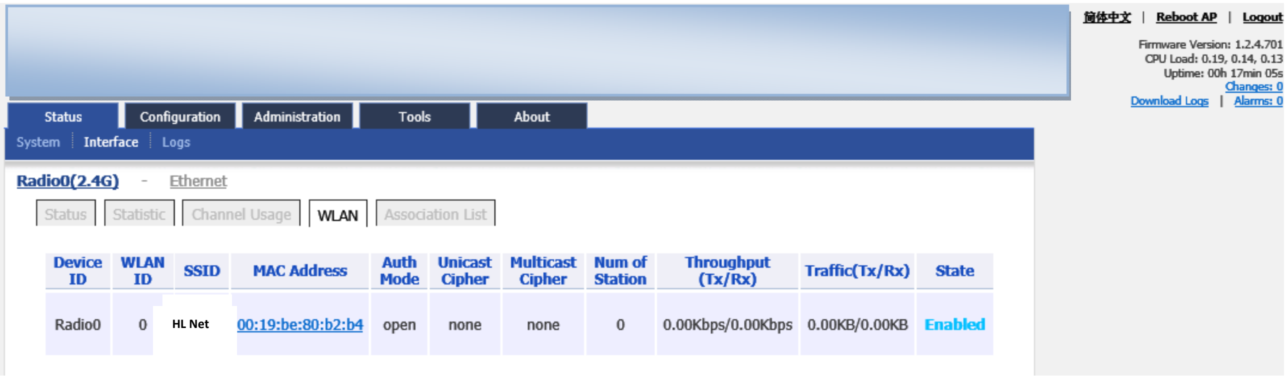
EXT0：Chain 0 Noise Floor of the Extension Channel (i.e the +/- channel of the HT40 case)

EXT1：Chain 1 Noise Floor of the Extension Channel (i.e the +/- channel of the HT40 case)

5.1.1.4. WLAN

Please select **Status** -> **Interface**-> Radio0(2.4G) -> **WLAN** to check radio0 wireless network information including: Device ID WLAN ID, SSID, MAC Address, Auth Mode, Unicast Cipher, Multicast Cipher, Num of Station, Throughput（TX/RX）, Download/Upload Byte, State.

When you enable a WLAN, you can find its relevant information in “State”.



Firmware Version: 1.2.4.701
CPU Load: 0.19, 0.14, 0.13
Uptime: 00h 17min 05s

Device ID	WLAN ID	SSID	MAC Address	Auth Mode	Unicast Cipher	Multicast Cipher	Num of Station	Throughput (Tx/Rx)	Traffic(Tx/Rx)	State
Radio0	0	HL Net	00:19:be:80:b2:b4	open	none	none	0	0.00Kbps/0.00Kbps	0.00KB/0.00KB	Enabled

Figure 5-7 WLAN Information

Device Id：2.4G interface ID

WLAN：Wireless network number

SSID： AP-100 default SSID is Superwifi Network x (x is from 0 to 7)

MAC Address： 2.4G wireless network MAC address (BSSID)

Auth Mode： Authentication mode for each wireless network

Unicast Cipher ：Unicast cipher mode for each wireless network

Multicast Cipher ： Multicast cipher mode for each wireless network

Num of Station： Associated client number

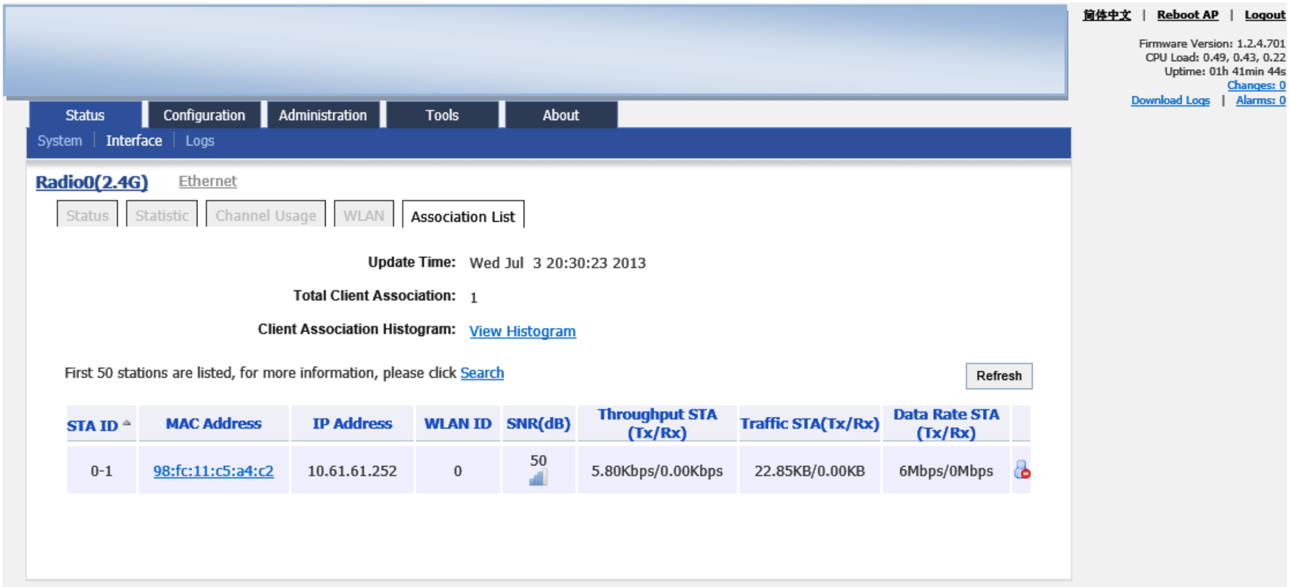
Throughput（TX/RX）：Real Throughput of transmitted and received packets for each wireless network

Download/Upload Byte：Download and Upload packets for each wireless network

State：Wireless network state

5.1.1.5. Association List

Please select **Status** -> **Interface**-> **radio0** -> **Association List** to get associated client information including: Total Client Association, Client Association Histogram, STA ID, Mac Address, WLAN ID, SNR, Download/Bytes, Upload/Bytes, Download Rate/kbps, Upload Rate/kbps.



Firmware Version: 1.2.4.701
CPU Load: 0.49, 0.43, 0.22
Uptime: 01h 41min 44s

Update Time: Wed Jul 3 20:30:23 2013

Total Client Association: 1

Client Association Histogram: View Histogram

First 50 stations are listed, for more information, please click Search

STA ID	MAC Address	IP Address	WLAN ID	SNR(dB)	Throughput STA (Tx/Rx)	Traffic STA(Tx/Rx)	Data Rate STA (Tx/Rx)	
0-1	98:fc:11:c5:a4:c2	10.61.61.252	0	50	5.80Kbps/0.00Kbps	22.85KB/0.00KB	6Mbps/0Mbps	

Figure 5-8 Association List

Total Client Association：Total associated clients

Client Association Histogram：Association client history records

STA ID： Wireless client ID

Mac Address：Wireless client MAC address

Wlan ID：Client associated WLAN ID

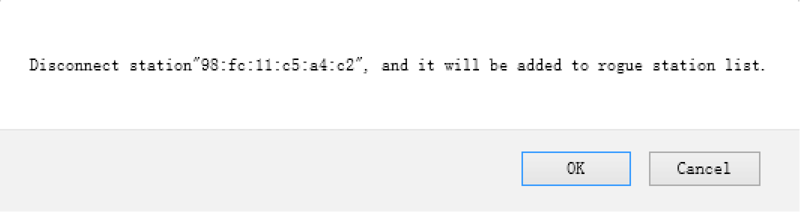
SNR：Wireless client SNR

Throughput (Rx/Tx) ：Wireless client real throughput received and transmitted traffic (kbps)

Download/Upload Byte ：Wireless client download and upload traffic (Bytes)

Download/Upload Rate ：Wireless client download and upload rate (kbps)

Click this icon, below prompt will pop up. If choice the yes, the associated client will be disconnected and added into rogue station list.



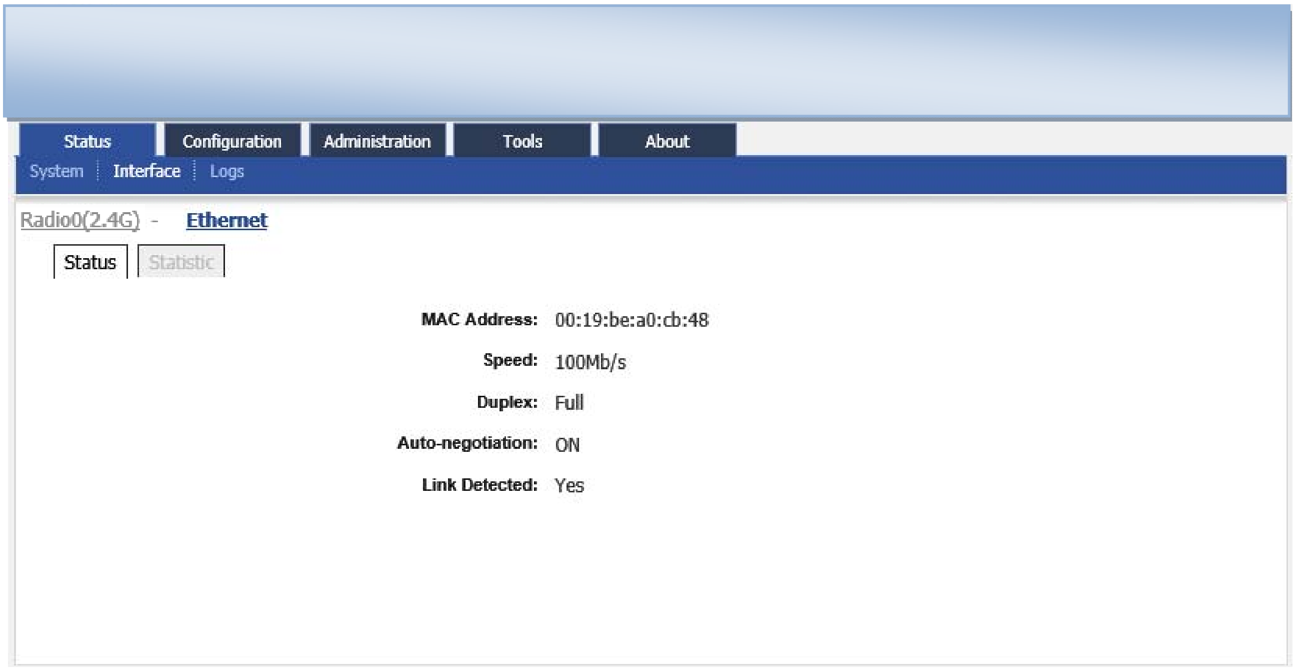
Disconnect station"98:fc:11:c5:a4:c2", and it will be added to rogue station list.

5.1.2. Ethernet Interface

Please select **Status** -> **Interface-**> **Ethernet** to check Ethernet interface information including Status and Statistic.

5.1.2.1. Status

Please select **Status** -> **Interface**-> **Ethernet** -> **Status** to check Ethernet interface status which includes Ethernet MAC Address, Speed, Duplex, Auto-negotiation and Link Detected.



MAC Address: 00:19:be:a0:cb:48
Speed: 100Mb/s
Duplex: Full
Auto-negotiation: ON
Link Detected: Yes

Figure 5-9 Ethernet Interface State

MAC Address： AP-100 Ethernet MAC address

Speed： AP-100 Ethernet speed

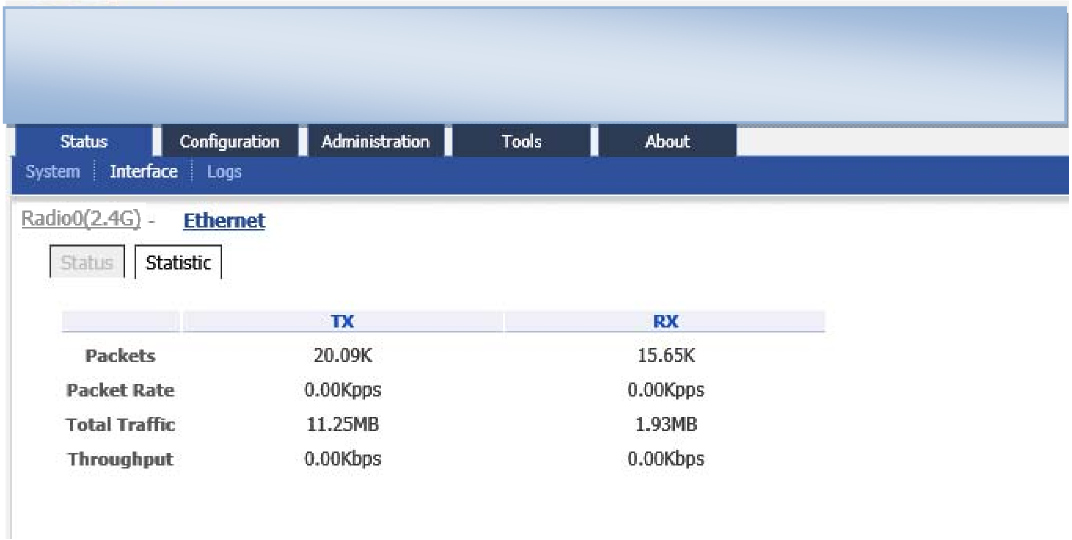
Duplex：AP-100 Ethernet duplex mode (Full/Half)

Auto-negotiation：AP-100 Ethernet auto-negotiation mode ON or OFF, by default it is “ON”.

Link Detected：Whether AP-100 Ethernet do link detection, by default it is “yes”.

5.1.2.2. Statistic

Please select **Status** -> **Interface**-> **Ethernet** -> **Statistic** to check Ethernet statistic information including Ethernet Tx & Rx Packets, Tx & Rx Packet Rate, Total Traffic and Throughput.



	TX	RX
Packets	20.09K	15.65K
Packet Rate	0.00Kpps	0.00Kpps
Total Traffic	11.25MB	1.93MB
Throughput	0.00Kbps	0.00Kbps

Figure 5-10 Ethernet Interface Statistic

Packets：Ethernet transmitted and received packets

Octets：Ethernet transmitted and received octets

Packet Rate：Ethernet interface packet rate

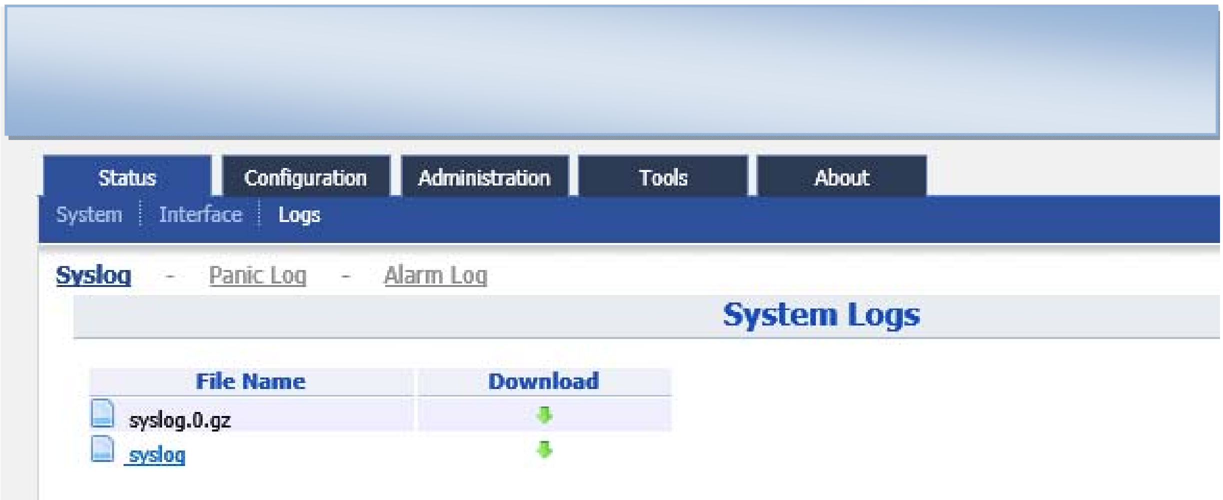
Throughput：Ethernet interface throughput

5.1.3. Logs

In order to realize easier monitoring and diagnosis, AP-100 provides log function. Selecting **Status** -> **Logs**, you will find 3 sub-items below: SysLog, Panic Log, and Alarm Logs.

5.1.3.1. System Log

The system log gives AP-100 system information like: software, hardware, system configuration, and self-checking result. Please select **Status** -> **Logs** -> **Syslog** to check system log:



System Logs

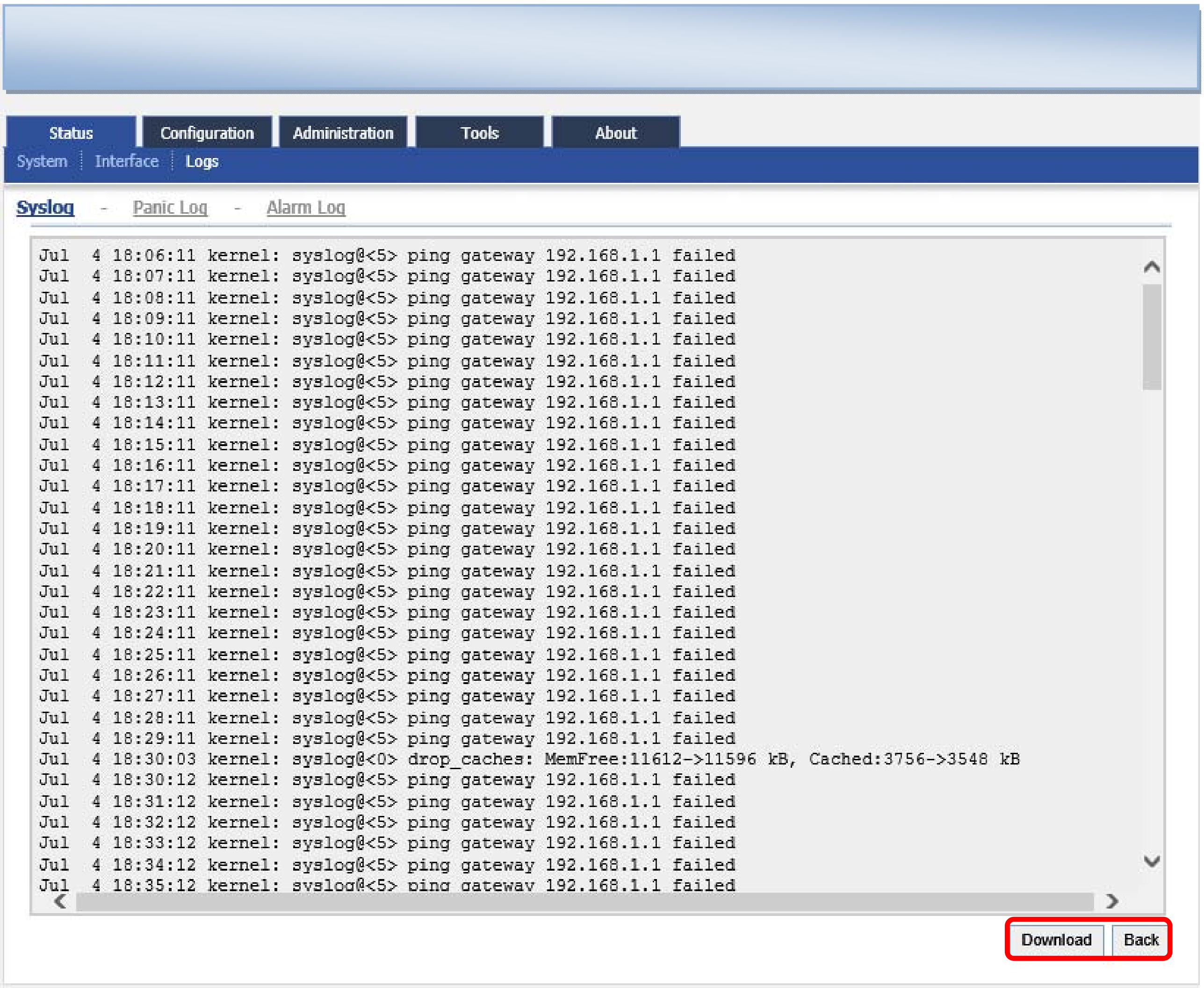
File Name	Download
syslog.0.gz	↓
syslog	↓

Figure 5-11 System Log

File Name：The name of log files, you can click it to open the log file.

Download：Download log file. Please click the green downward arrow to download the log file.

Click **File Name**-> **Syslog**, and you will find the log page below:



```
Jul  4 18:06:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:07:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:08:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:09:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:10:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:11:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:12:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:13:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:14:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:15:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:16:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:17:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:18:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:19:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:20:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:21:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:22:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:23:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:24:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:25:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:26:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:27:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:28:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:29:11 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:30:03 kernel: syslog@<0> drop_caches: MemFree:11612->11596 kB, Cached:3756->3548 kB
Jul  4 18:30:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:31:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:32:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:33:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:34:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
Jul  4 18:35:12 kernel: syslog@<5> ping gateway 192.168.1.1 failed
```

Figure 5-12 System Log “Download and Back” Button

Please click **Download** to download the system log file and click **Back** at the end of log to come back the previous page:

5.1.3.2. Panic Log

Panic Log is a self-generated log when the system finds some internal errors and need to reboot itself.

Please select **Status** -> **Logs** -> **Panic Log** to go to Panic log page:

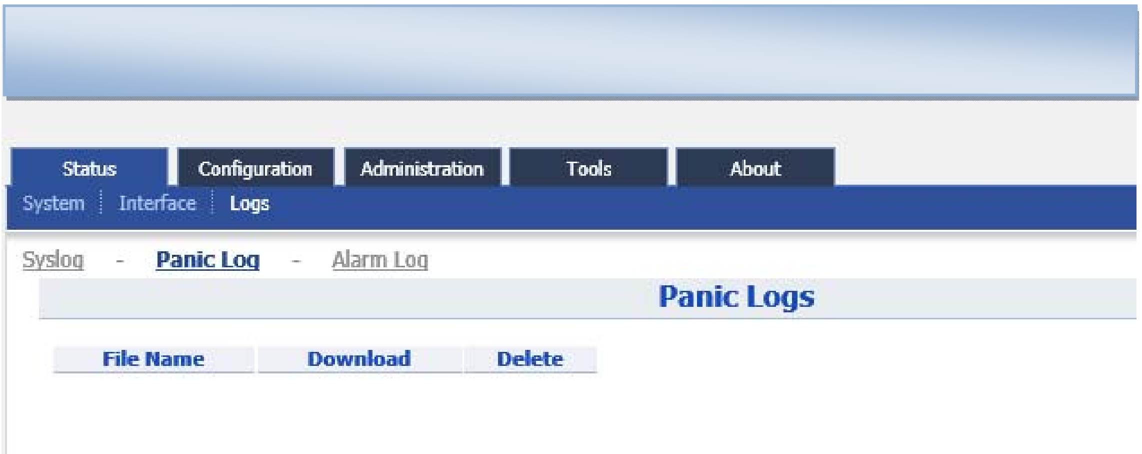


Figure 5-13 Panic Logs

File Name：The name of Panic log files, you can click it to open the log file.

Download：Download Panic log file. Please click the green downward arrow to download the log file.

Delete：Delete Panic log file.

5.1.3.3. Alarm Log

Please select **Status** -> **Logs** -> **Alarm Log** to go to alarm log page.

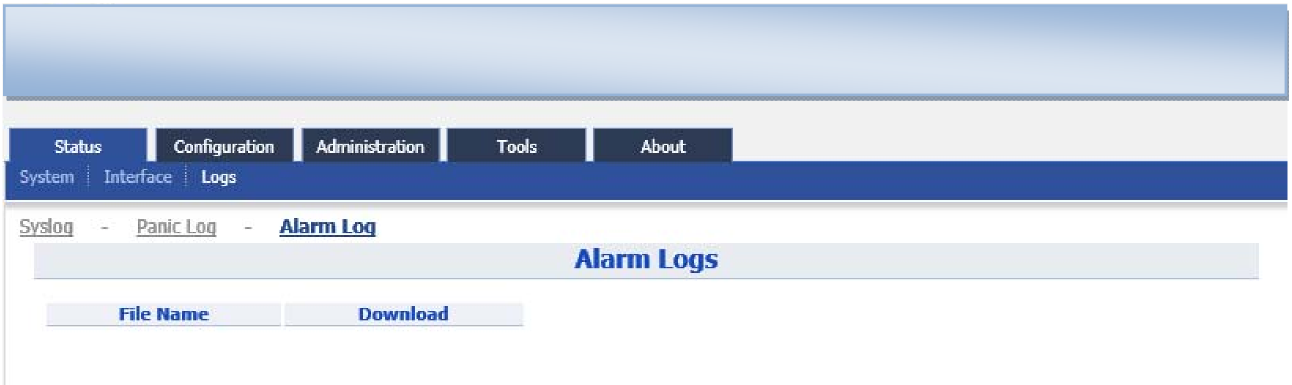


Figure 5-14 Alarm Logs

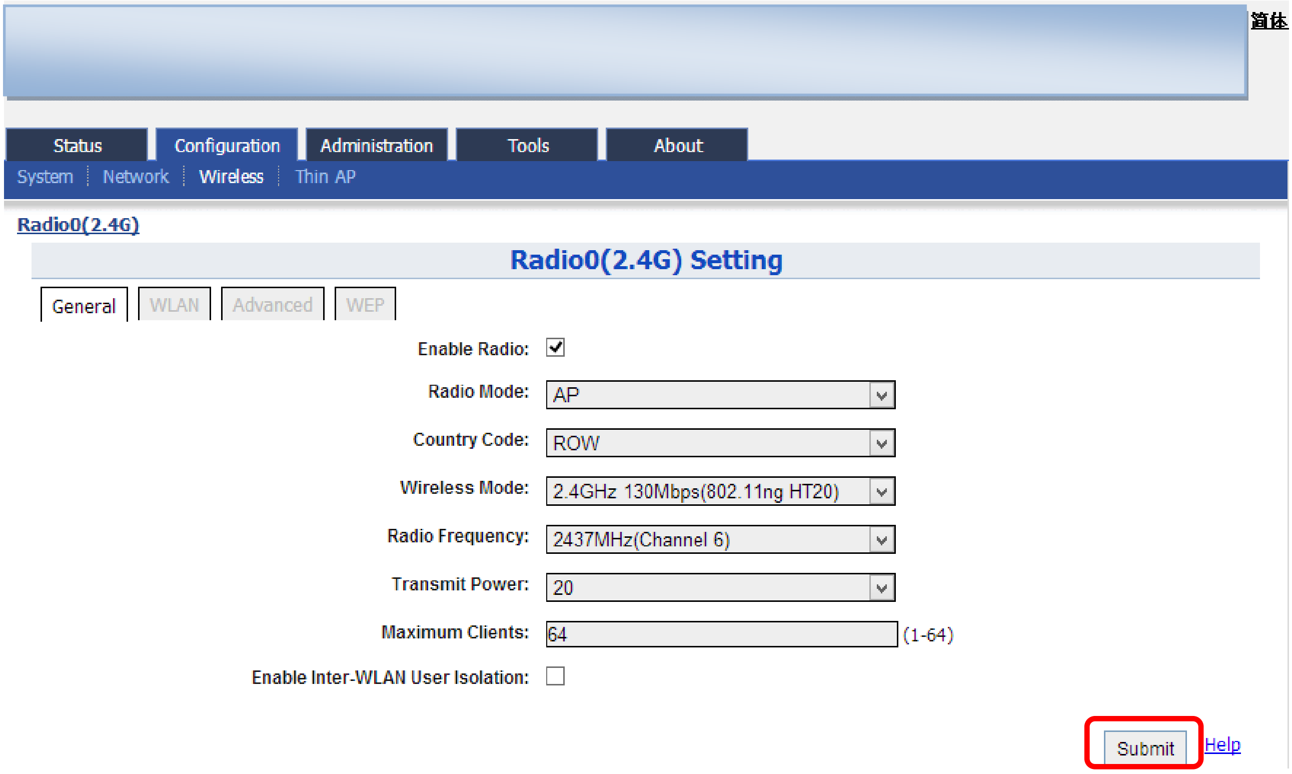
File Name：The name of log files, you can click it to open the log file.

Download：Download log file. Please click the green downward arrow to download the log file.

6. System Configuration

6.1. AP-100 Configuration Procedures

1 Users need to click **Submit** button to store the changed settings.



Radio0(2.4G) Setting

Enable Radio: ☑

Radio Mode: AP

Country Code: ROW

Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Radio Frequency: 2437MHz(Channel 6)

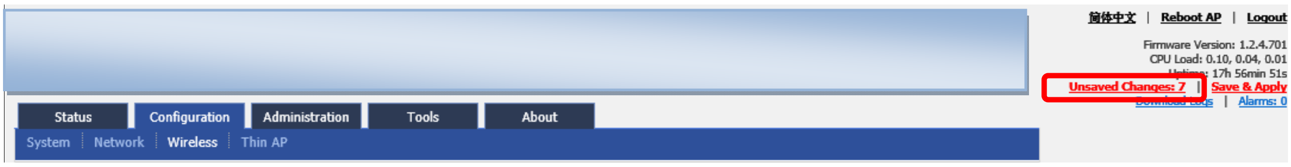
Transmit Power: 20

Maximum Clients: 64 (1-64)

Enable Inter-WLAN User Isolation: □

Figure 6-1 Submit Change

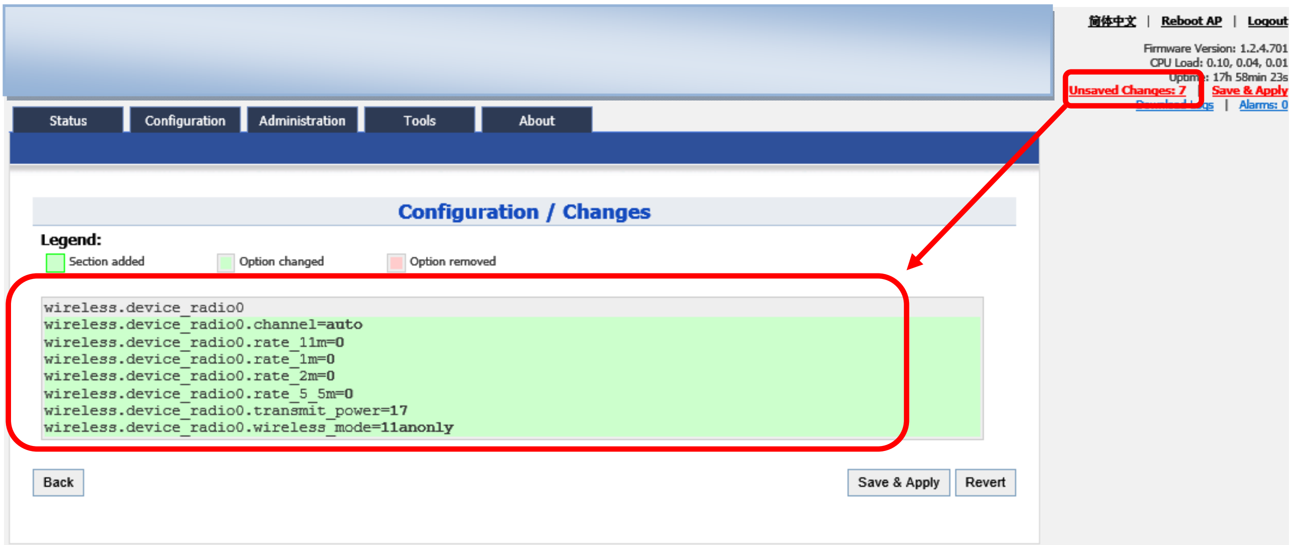
2 On the right top corner, there is an **Unsaved Changes** button; you can click it to check submitted items.


简体中文 | Reboot AP | Logout
Status
Configuration
Administration
Tools
About
System
Network
Wireless
Thin AP
Unsaved Changes: 7 | Save & Apply
Download Logs | Alarms: 0

Firmware Version: 1.2.4.701
CPU Load: 0.10, 0.04, 0.01
Uptime: 17h 56min 51s

Figure 6-2 Unsaved Change

3 Please click **Unsaved Changes** button to check changed setting detail information.


简体中文 | Reboot AP | Logout
Unsaved Changes: 7 | Save & Apply
Download Logs | Alarms: 0
Status
Configuration
Administration
Tools
About
Back
Save & Apply
Revert

Firmware Version: 1.2.4.701
CPU Load: 0.10, 0.04, 0.01
Uptime: 17h 58min 23s

Configuration / Changes

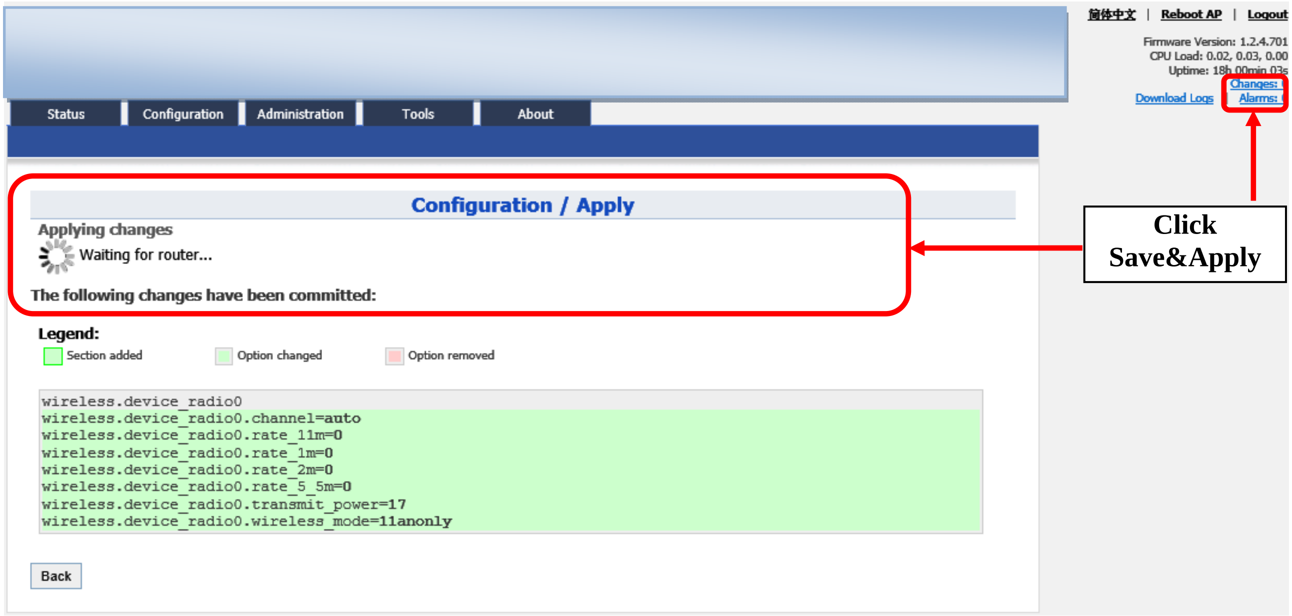
Legend:

🟩 Section added ▨ Option changed 🟥 Option removed

```
wireless.device_radio0
wireless.device_radio0.channel=auto
wireless.device_radio0.rate_11m=0
wireless.device_radio0.rate_1m=0
wireless.device_radio0.rate_2m=0
wireless.device_radio0.rate_5_5m=0
wireless.device_radio0.transmit_power=17
wireless.device_radio0.wireless_mode=11anonly
```

Figure 6-3 Unsaved Change Detail

4 Click **Save&Apply** button to perform all submitted changes:



Firmware Version: 1.2.4.701
CPU Load: 0.02, 0.03, 0.00
Uptime: 18h 00min 03s

Configuration / Apply

Applying changes

Waiting for router...

The following changes have been committed:

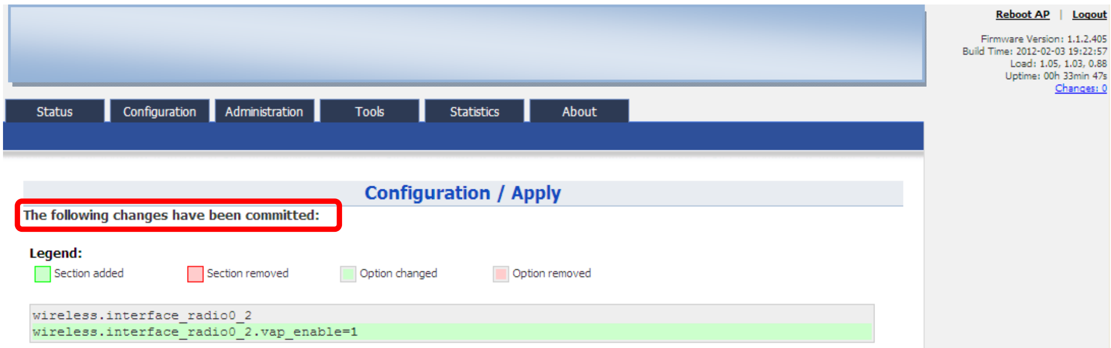
Legend:

🟩 Section added ▨ Option changed 🟥 Option removed

```
wireless.device_radio0
wireless.device_radio0.channel=auto
wireless.device_radio0.rate_11m=0
wireless.device_radio0.rate_1m=0
wireless.device_radio0.rate_2m=0
wireless.device_radio0.rate_5_5m=0
wireless.device_radio0.transmit_power=17
wireless.device_radio0.wireless_mode=11anonly
```

Figure 6-4 Save and Apply Changes

5 You will find “The following changes have been committed”



Firmware Version: 1.1.2.405
Build Time: 2012-02-03 19:22:57
Load: 1.05, 1.03, 0.88
Uptime: 00h 33min 47s

Configuration / Apply

The following changes have been committed:

Legend:

🟩 Section added 🟥 Section removed ▨ Option changed ▨ Option removed

```
wireless.interface_radio0_2
wireless.interface_radio0_2.vap_enable=1
```

Figure 6-5 Changes have been committed

6 The whole committing changes progress, it is no need to reboot AP-100.

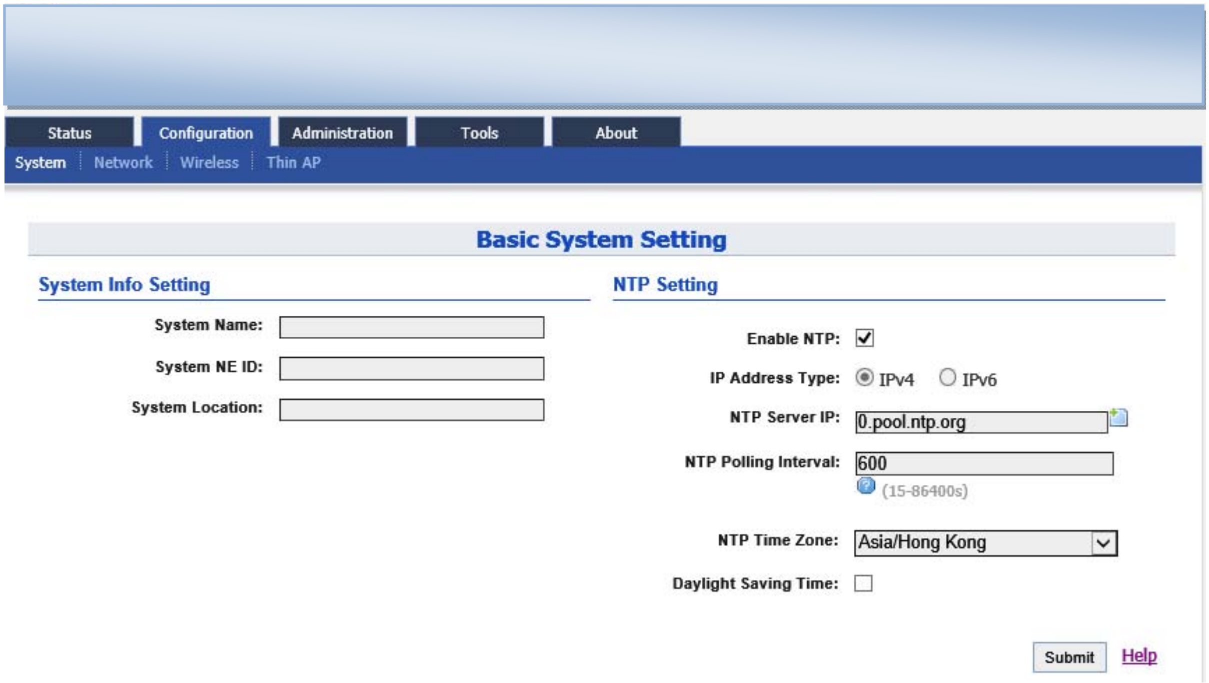
6.2. Basic Configuration

6.2.1. Basic System Configuration

System configuration web includes two parts: System Info setting and NTP Setting.

NTP is a network time protocol for the AP-100 to synchronize the system time. NTP is Enable by default. If NTP is needed, IP address of the NTP server must be added and AP-100 will synchronize with the NTP server. It is useful to maintain the network and make sure all APs are using the same system time by setting the same NTP server.

Please select **Configuration** -> **System** to configure System Info Setting and NTP setting.



Basic System Setting

System Info Setting

System Name:

System NE ID:

System Location:

NTP Setting

Enable NTP: ☑

IP Address Type: ● IPv4 ○ IPv6

NTP Server IP: 0.pool.ntp.org

NTP Polling Interval: 600 (15-86400s)

NTP Time Zone: Asia/Hong Kong

Daylight Saving Time: □

Figure 6-6 NTP Setting

System Name：Set system name of the device, the system name can be up to 255 characters long.

System NE ID：Set system NE ID, the system NE ID can be up to 64 characters long.

System Location：Set system location, the system location can be up to 255 characters long.

Enable NTP： Enable or disable NTP function, by default it is selected.

IP Address Type：IPv4 or IPv6. (Please note that IPv6 is available to be select after enable IPv6 in Network setting web page, refer to section 6.3).

NTP Server IP： NTP server IP address, please click “” to add new NTP server IP address.

NTP Polling Interval： By default, it is 600s

NTP Time Zone： Time Zone setting, by default it is Asia/Hong Kong.

Daylight Saving Time： By default, it is not selected.

Procedures：

1 Select **Configuration**->**System**， to go to system setting page.

2 Type in the system information if it is needed.

3 Add NTP IP address in **NTP Server IP**.

4 Set **NTP Polling Interval**

5 Choose local NTP **Time** Zone

6 Set **Daylight Saving Time**（Optional）

7 Click **Submit**

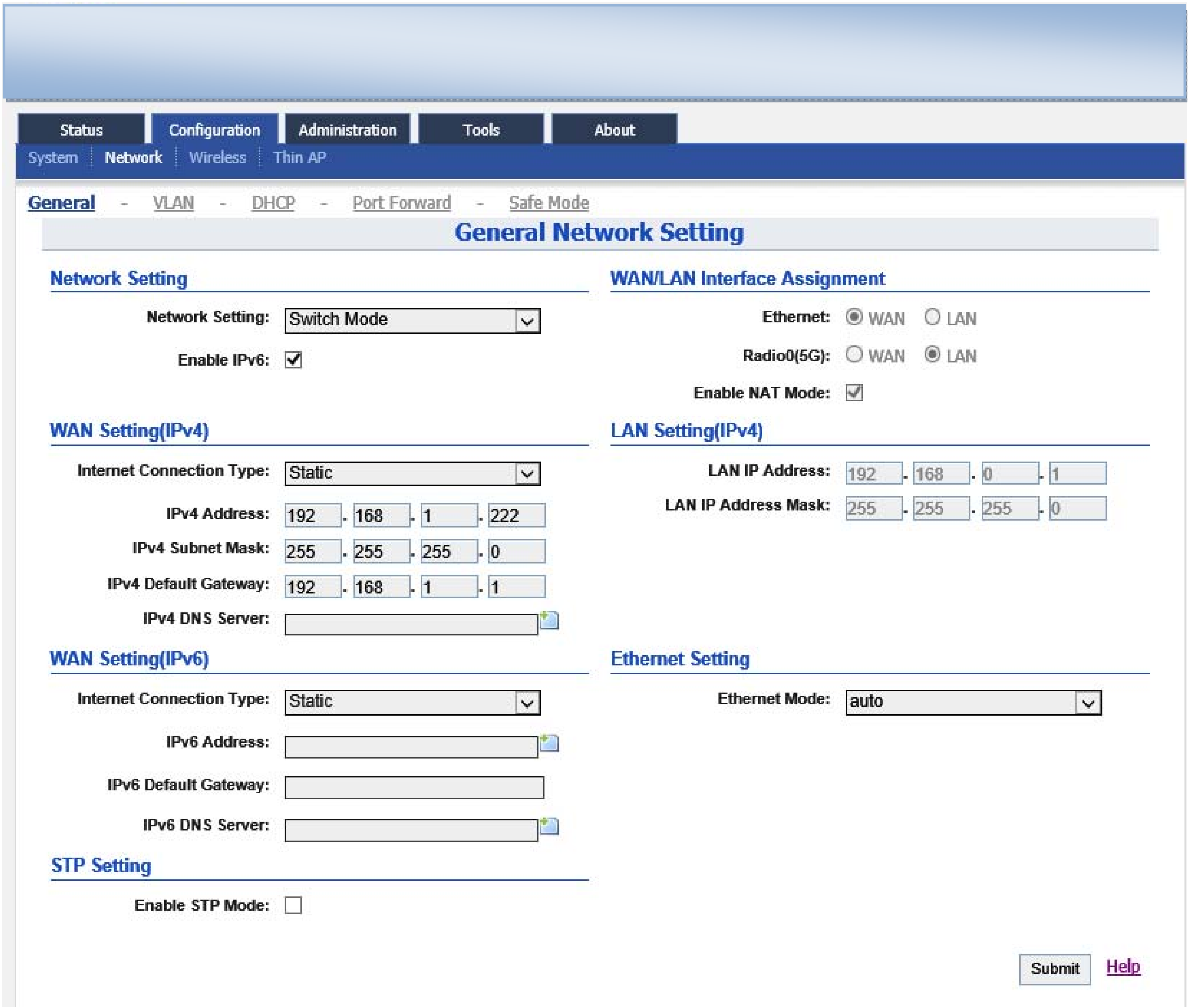
8 Click **Save&Apply** to commit changes.

6.2.2. Network Configuration

Please select **Configuration** -> **Network** to go to Network configuration page.

6.2.2.1. General Network Configuration

Please select **Configuration** -> **Network** -> **General** and start to configure general settings.



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: ☑

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(5G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

IPv6 Address:

IPv6 Default Gateway:

IPv6 DNS Server:

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-7 Network Setting

Network Setting：There are Switch Mode and Gateway Mode being selected.

Enable IPv6：IPv6 is disable by default.

Internet Connection Type： Static IP or DHCP client

IPv4 Address： If AP-100 uses static IP, please give it a fixed IP

IPv4 Subnet Mask：If AP-100 uses static IP, please give it a subnet mask

IPv4 Default Gateway：If AP-100 uses static IP, please give it a Gateway address

IPv4 DNS Server：If AP-100 uses static IP, please set DNS IP address

Internet Connection Type： Static IP or DHCP client

IPv6 Address： If AP-100 uses static IP, please give it a fixed IP

IPv6 Default Gateway：If AP-100 uses static IP, please give it a Gateway address

IPv6 DNS Server：If AP-100 uses static IP, please set DNS IP address

Enable STP Mode：Enable or disable the STP service.

Ethernet/Radio0(2.4G)：LAN interface or WAN interface, only work in gateway mode.

Enable NAT Mode：If NAT Mode is set to "Disabled" then the AP will not perform any network address translations and all IP traffic will be passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio) without any modification. If NAT Mode is set to "Enabled" then the AP will perform network address translations on all traffic being passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio). The NAT will translate IP traffic address's between the wireless client subnet and the DS subnet.

LAN IP Address：IP address of local area network.

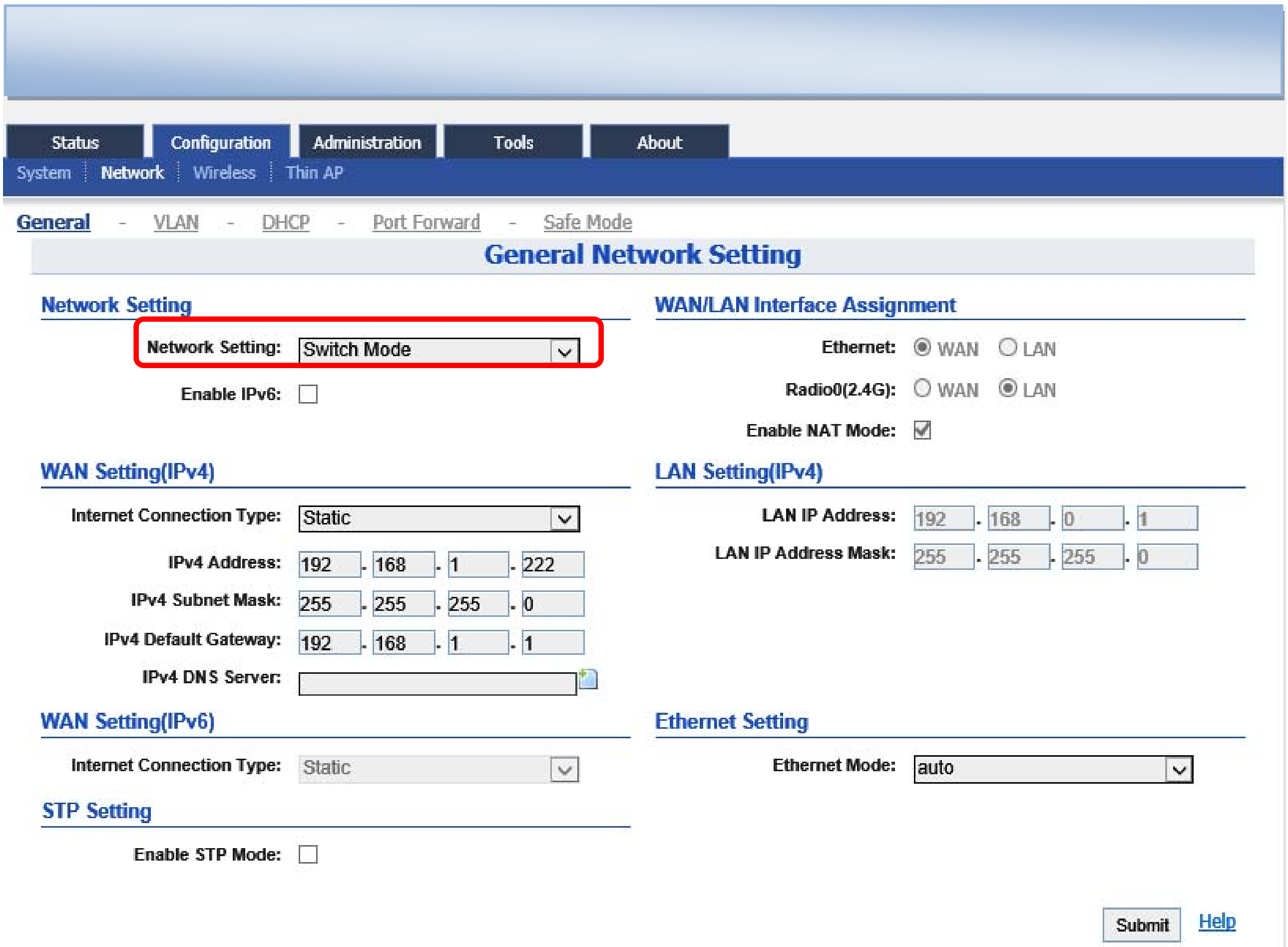
LAN IP Address Mask：IP address mask of local area network.

Ethernet Mode：Auto/manual mode.

Ethernet Duplex：AP Ethernet duplex mode (Full/Half).

6.2.1.1.1. Network Setting

- Switch Mode



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-8 Network Mode

In switch mode, AP-100 works as a switch to deliver data between Ethernet interface and wireless interfaces.

Configuration procedures：

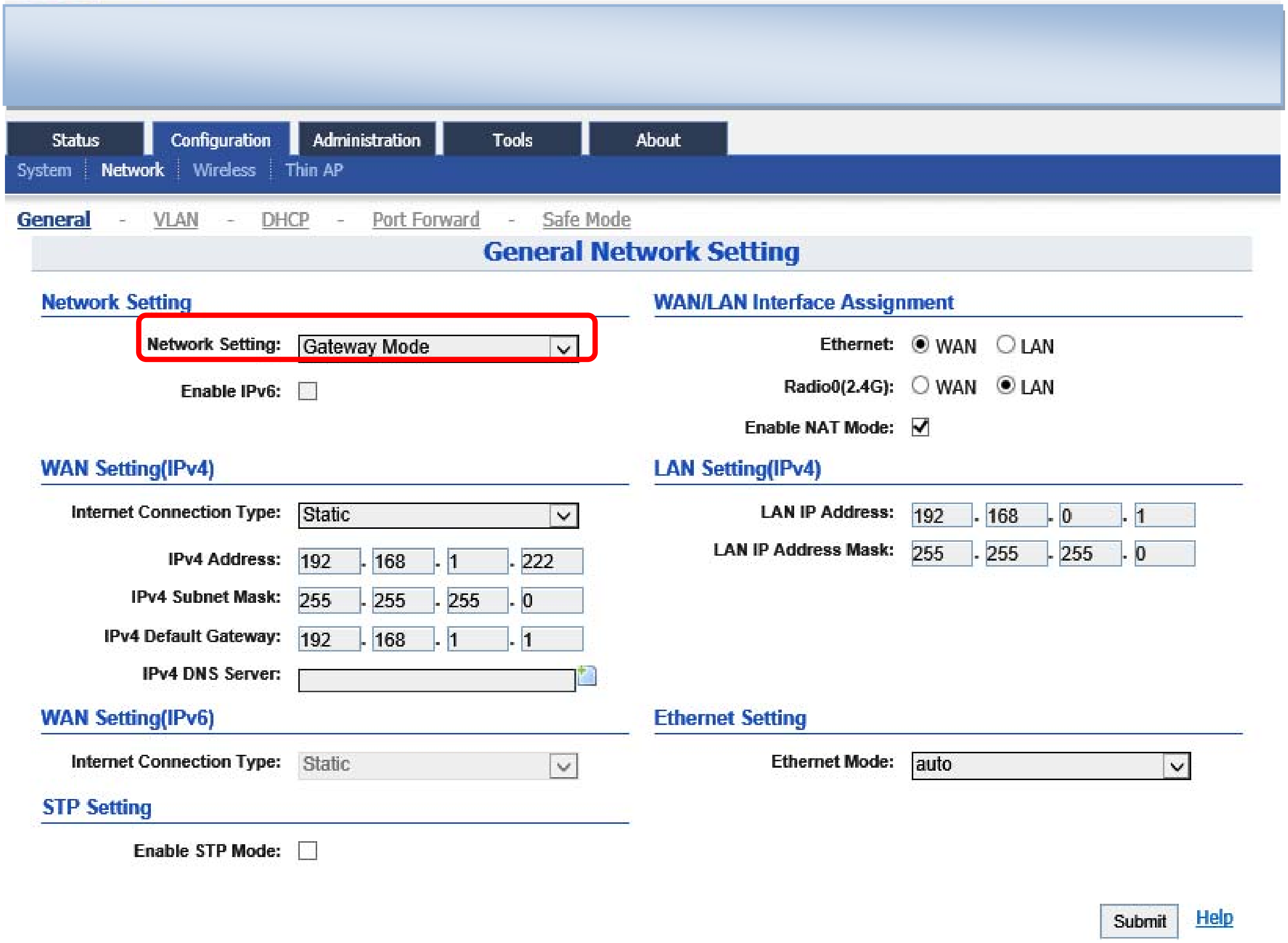
1 Select **Configuration**->**Network**->**General** to go to configuration page.

2 **Network Setting**: Switch Mode.

3 Click **Submit**.

4 Click **Save&Apply** to apply changes.

- Gateway Mode



General Network Setting

Network Setting

Network Setting: Gateway Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-9 Network Mode

In Gateway mode, the AP-100 acts as a gateway. The Local IP Address and Local IP Address Mask information must be provided to specify the IP address used to communicate to the wireless client locally (i.e. IP address for 2.4GHz radio interface). The AP-100 would use another IP address to communicate to the outside network (i.e. IP address for Ethernet interface). If a wireless client sends a packet to the outside network, the packet would send to the AP-100 with its local IP address in the local network. Then, the AP-100 will pass this packet to the outside network (Ethernet) using its remote IP address.

Configuration procedures：

1 Select **Configuration**->**Network**->**General** to go to configuration page.

2 **Network Setting**: Gateway Mode.

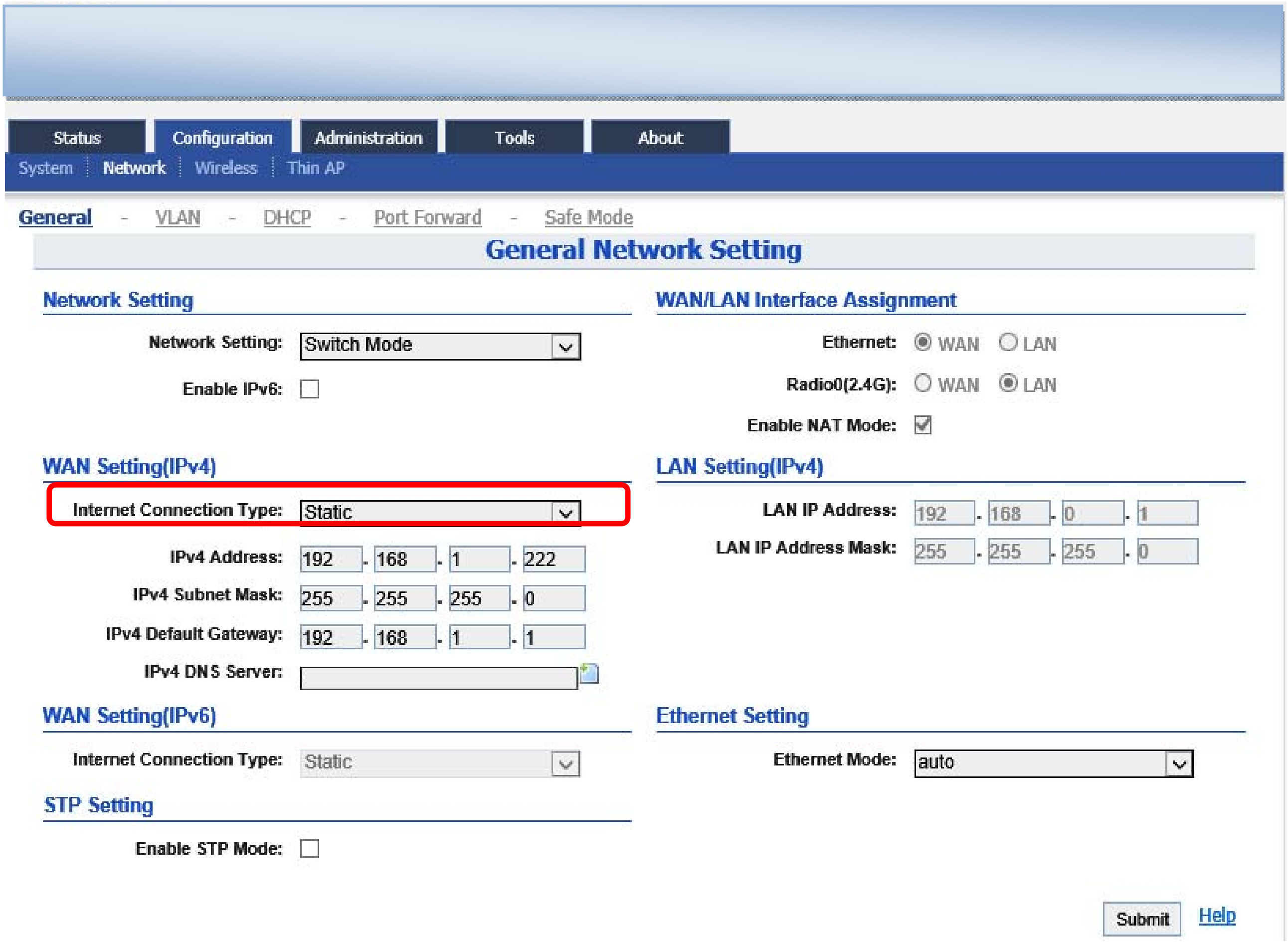
3 Click **Submit**.

4 Click **Save&Apply** to apply changes.

Warnings ：***When the Network mode as Gateway mode the VLAN will not be used and it would not be used for the 2.4G Radio.***

6.2.1.1.2. WAN Setting (IPv4)

In switch mode and Gateway mode, there are 2 types: Static IP or DHCP client



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-10 Internet Connection Type

Procedures：

1 Select **Configuration**->**Network**->**General**

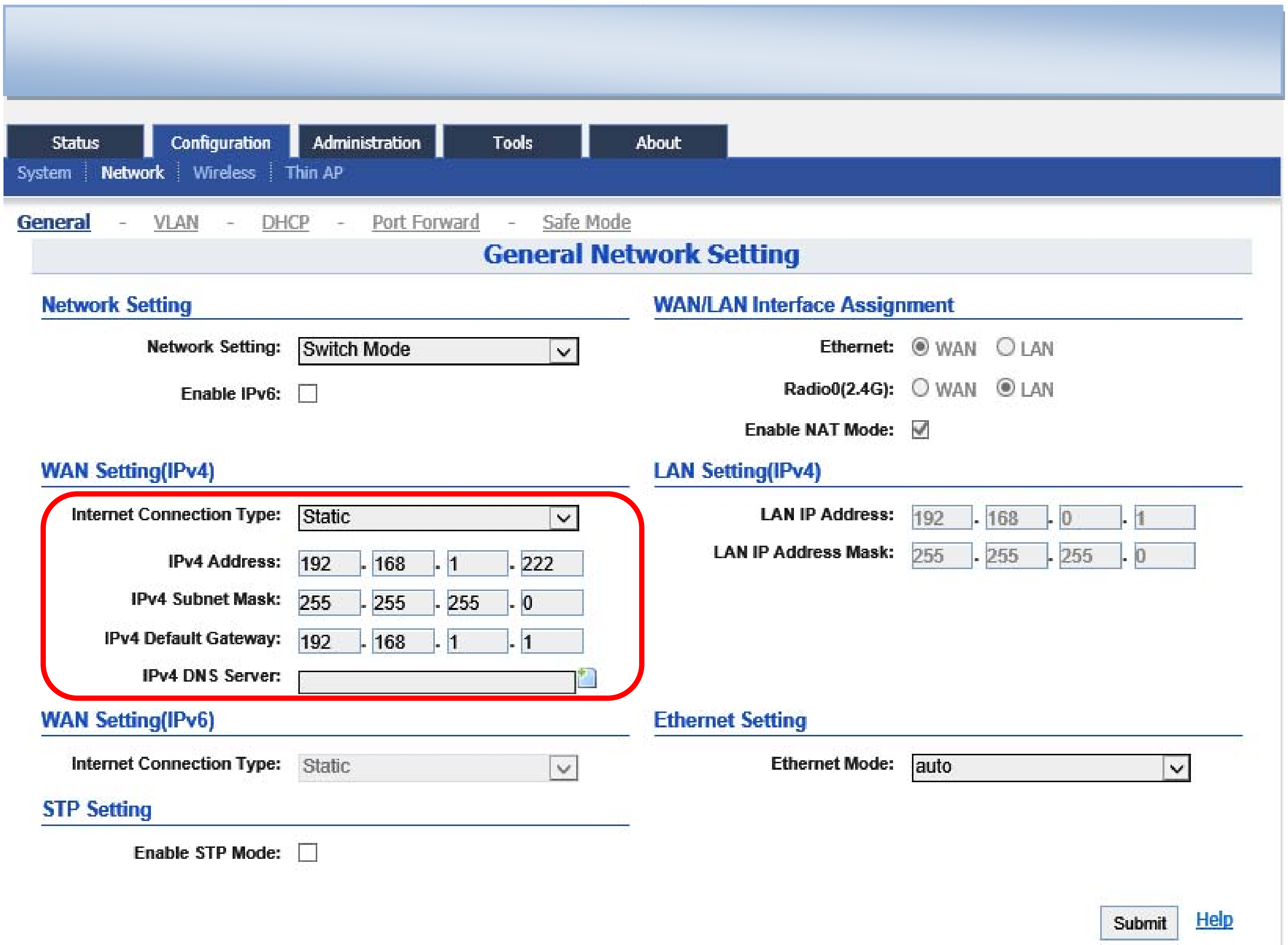
2 **Internet Connection Type**：choose Static or DHCP

3 Click **Submit**

4 Click **Save&Apply** to apply.

- Static IP (IPv4)

Users need manually configure AP-100 IP address, subnet mask, gateway address and DNS server IP address:



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-11 Static IP

Procedures：

1 Select **Configuration**->**Network**->**General**

2 **Internet Connection Type** : choose "Static"

3 **IP Address** : input IP address

4 **Subnet Mask** : input subnet mask

5 **Default Gateway Address** : input gateway address

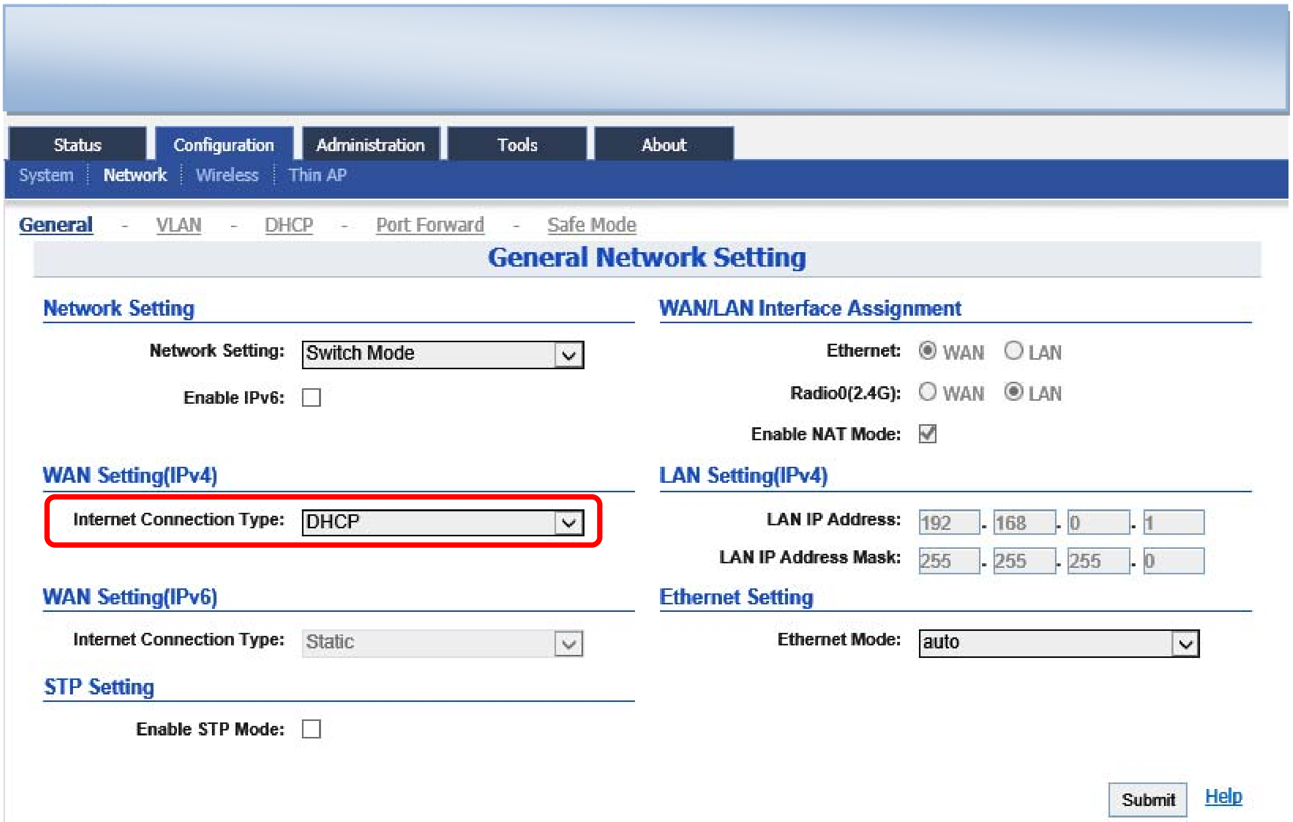
6 **DNS Server** IP **Address**: input DNS address

7 Click **Submit**

8 Click **Save&Apply** to apply

- DHCP (IPv4)

AP-100 will get IP from DHCP server



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN Setting(IPv4)

Internet Connection Type: DHCP

WAN Setting(IPv6)

Internet Connection Type: Static

STP Setting

Enable STP Mode: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

Ethernet Setting

Ethernet Mode: auto

Figure 6-12 DHCP Client

Procedures：

1 Select **Configuration**->**Network**->**General**

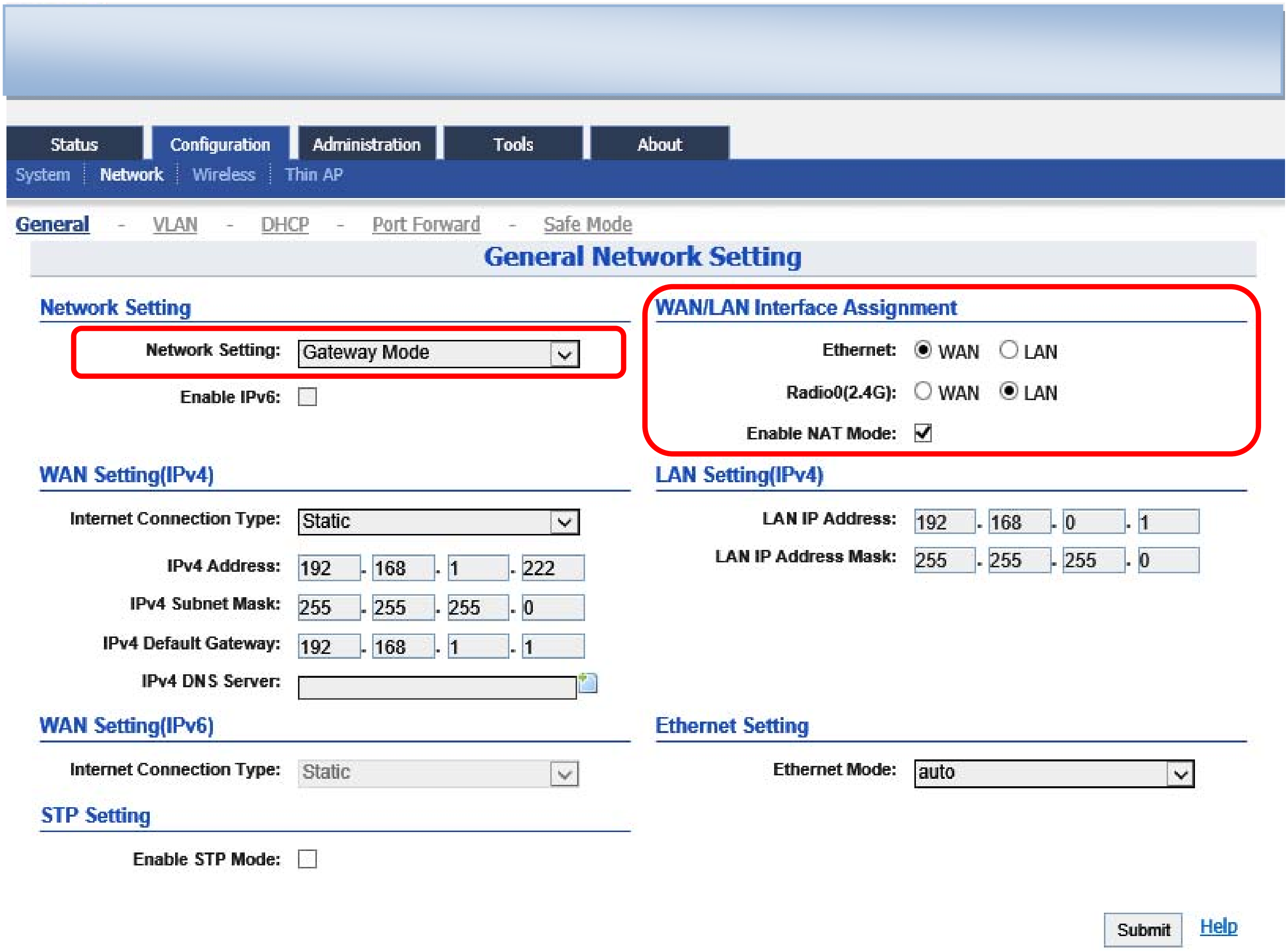
2 **Internet Connection Type** : choose DHCP;

3 Click **Submit**

4 Click **Save&Apply** to apply

6.2.1.1.3. WAN/LAN Interface Assignment

This option will be available to be edit while the Gateway mode is selected in the network setting.



General Network Setting

Network Setting

Network Setting: Gateway Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(2.4G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

STP Setting

Enable STP Mode: □

Figure 6-13 WAN/LAN Interface Assignment

Ethernet/Radio (2.4G): LAN interface or WAN interface, only work in gateway mode.

Enable NAT Mode: If NAT Mode is set to "Disabled" then the AP will not perform any network address translations and all IP traffic will be passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio) without any modification. If NAT Mode is set to "Enabled" then the AP will perform network address translations on all traffic being passed from the wireless clients to the DS (Ethernet) port or wireless bridge (802.11a radio). The NAT will translate IP traffic address's between the wireless client subnet and the DS subnet

6.2.1.1.4. LAN Setting (IPv4)

LAN IP Address: IP address of local area network.

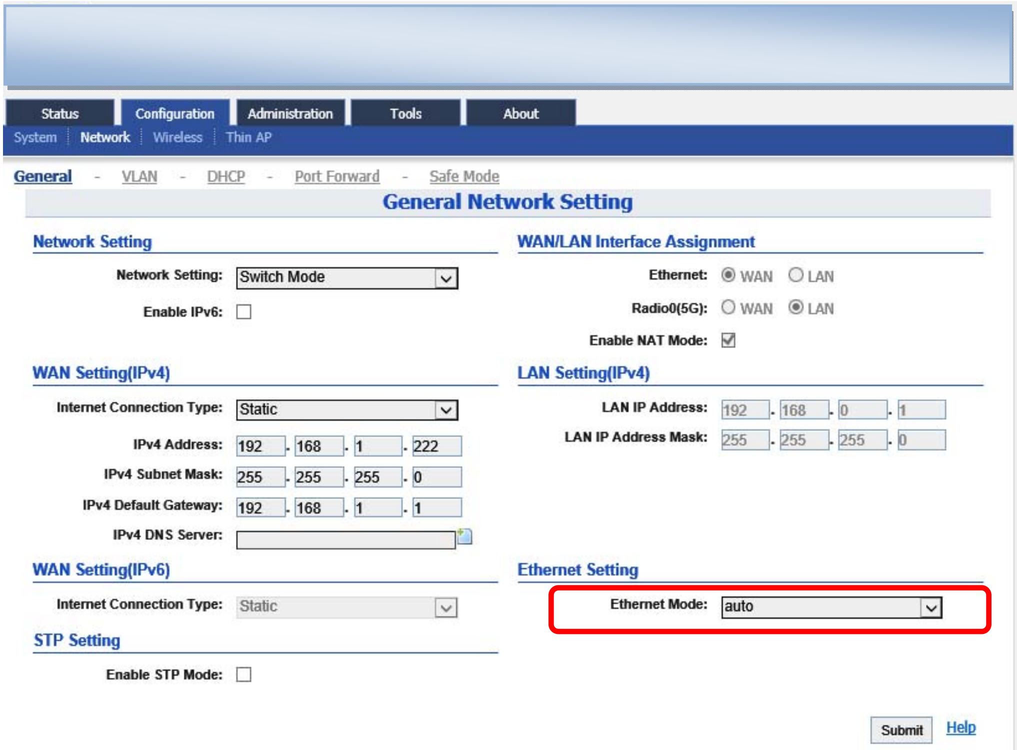
LAN IP Address Mask: IP address mask of local area network

6.2.1.1.5. Ethernet Mode

In switch mode and Gateway mode, there are 2 types: Auto and Manual

1） Auto

AP-100 Ethernet port duplex and speed will be auto



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(5G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: auto

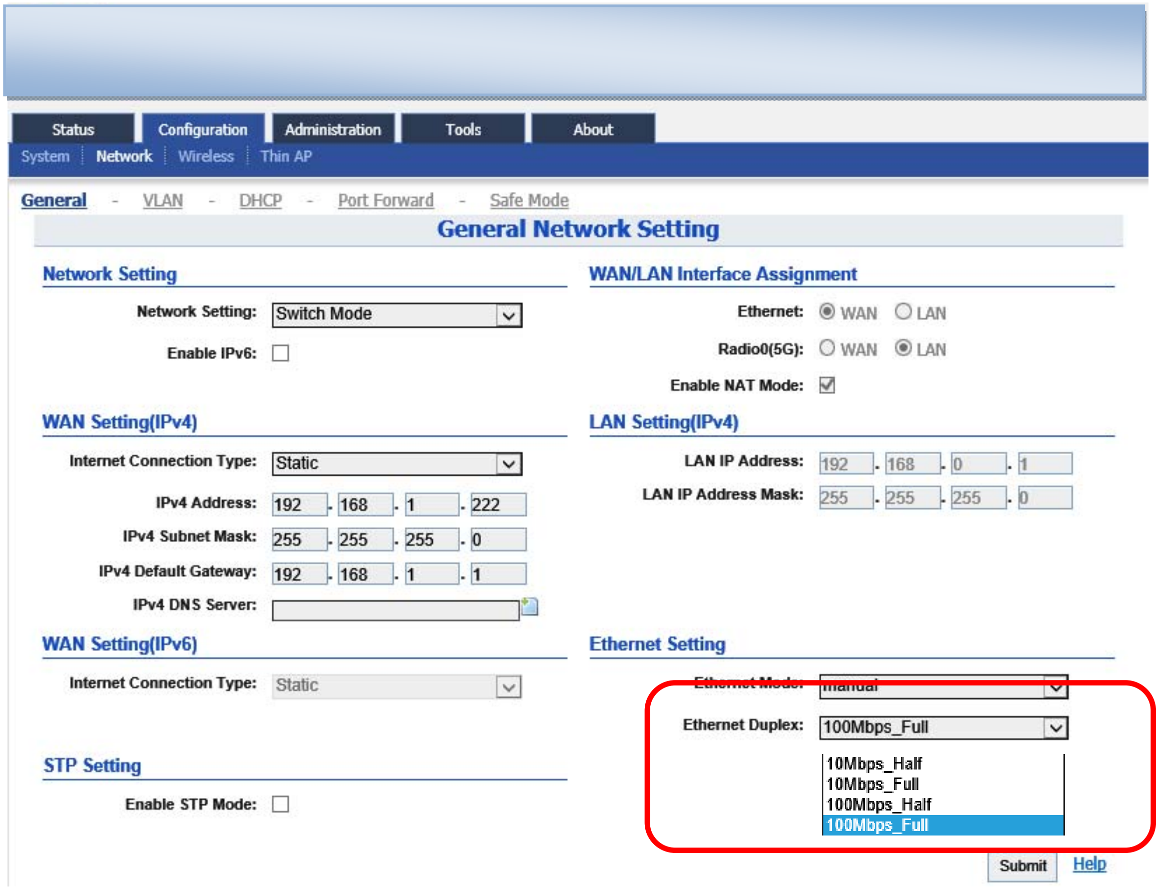
STP Setting

Enable STP Mode: □

Figure 6-14 Ethernet Mode

2） Manual

AP-100 Ethernet port will be manual, and the Ethernet Duplex and Speed will be selected by Full/Half, 100Mbps/10Mbps.



General Network Setting

Network Setting

Network Setting: Switch Mode

Enable IPv6: □

WAN/LAN Interface Assignment

Ethernet: ● WAN ○ LAN

Radio0(5G): ○ WAN ● LAN

Enable NAT Mode: ☑

WAN Setting(IPv4)

Internet Connection Type: Static

IPv4 Address: 192 . 168 . 1 . 222

IPv4 Subnet Mask: 255 . 255 . 255 . 0

IPv4 Default Gateway: 192 . 168 . 1 . 1

IPv4 DNS Server:

LAN Setting(IPv4)

LAN IP Address: 192 . 168 . 0 . 1

LAN IP Address Mask: 255 . 255 . 255 . 0

WAN Setting(IPv6)

Internet Connection Type: Static

Ethernet Setting

Ethernet Mode: manual

Ethernet Duplex: 100Mbps_Full

10Mbps_Half
10Mbps_Full
100Mbps_Half
100Mbps_Full

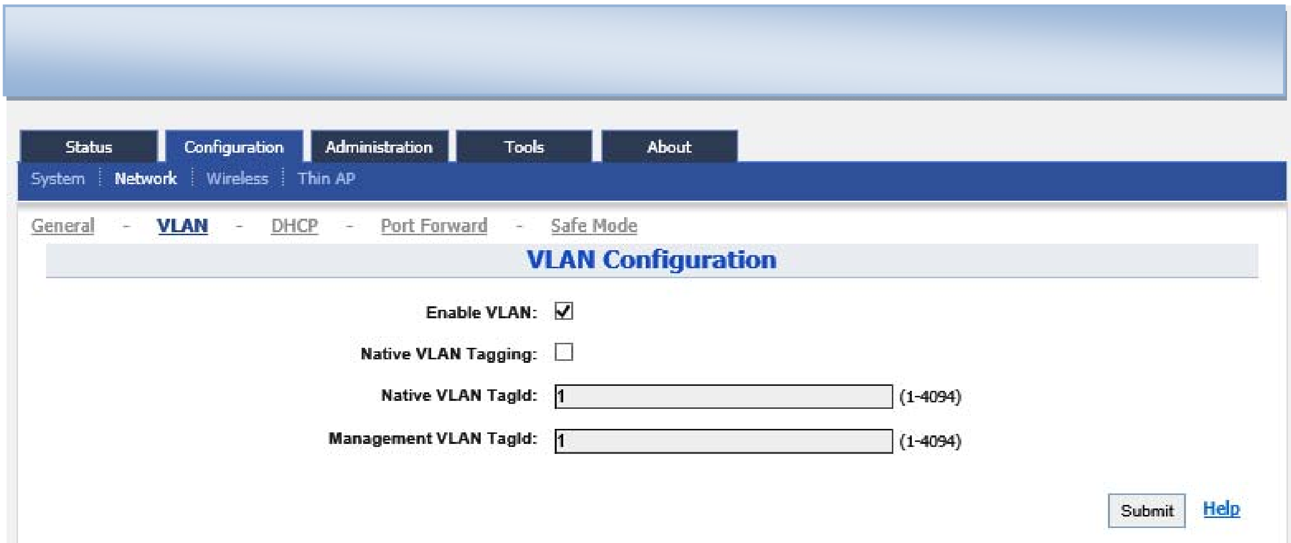
STP Setting

Enable STP Mode: □

Figure 6-15 Ethernet Mode

6.2.2.2. VLAN

Select **Configuration** -> **Network** -> **VLAN** to access to VLAN configuration page.



VLAN Configuration

Enable VLAN: ☑

Native VLAN Tagging: □

Native VLAN TagId: 1 (1-4094)

Management VLAN TagId: 1 (1-4094)

Figure 6-16 VLAN Setting

By default, AP-100 VLAN setting is disabled.

Enable VLAN：Enable or Disable VLAN function

Native VLAN Tagging：By default, it is not selected.

Native VLAN TagId：Native VLAN ID

Management VLAN TagId：Management VLAN ID

Procedures：

1 Select **Configuration**->**Network**->**VLAN**

2 **Enable VLAN** Enable or disable VLAN

3 **Native VLAN Tagging** : Enable or disable native VLAN tagging

4 **Native VLAN TagId**: input Native VLAN ID

5 **Management VLAN TagId**: input management VLAN ID

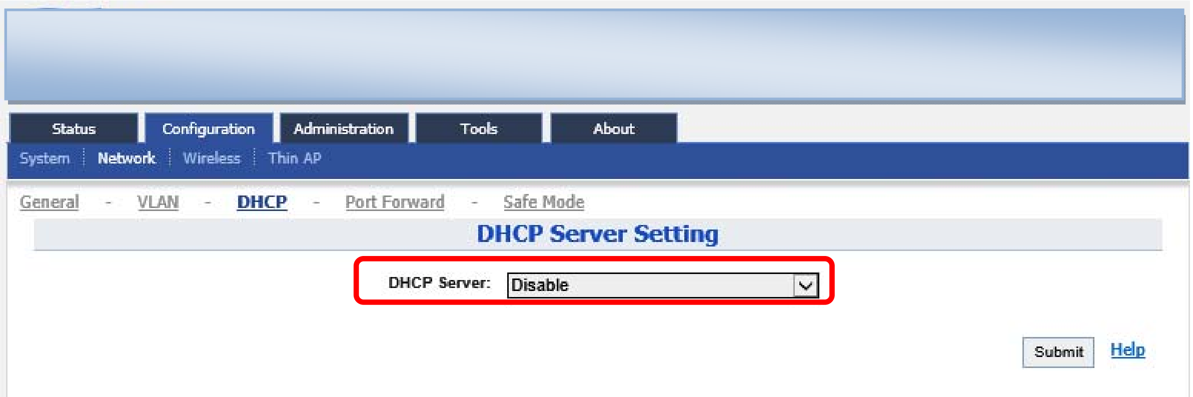
6 **VLAN TagId** : input VLAN ID

7 Click **Submit**

8 Click **Save&Apply** to apply

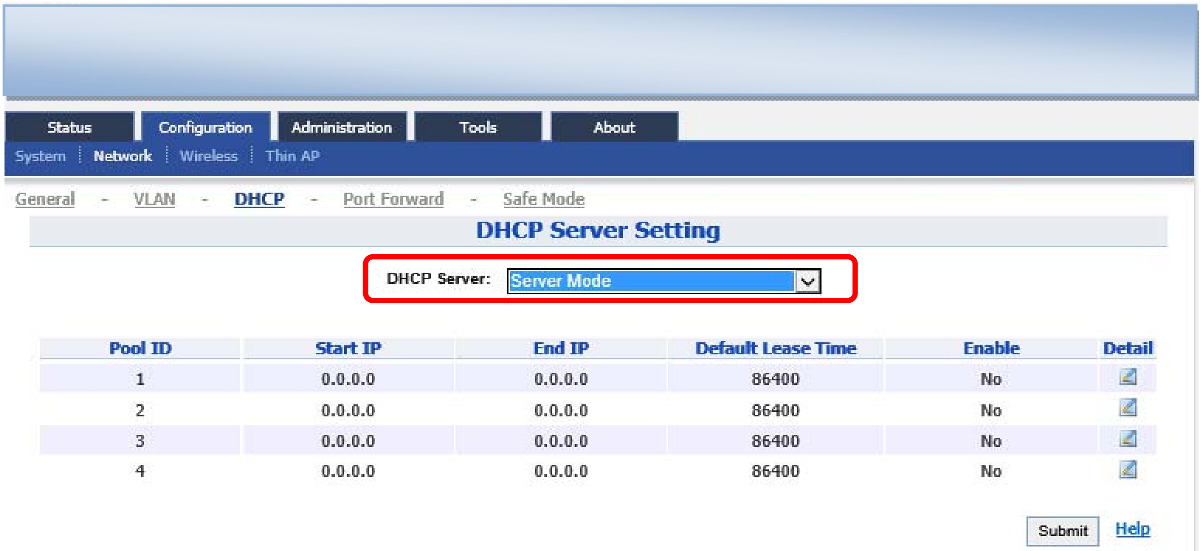
6.2.2.3. DHCP Server

Select **Configuration** -> **Network** -> **DHCP Server** to access to DHCP configuration page. And there are two options, Disable and DHCP Server.



DHCP Server Setting

DHCP Server: Disable



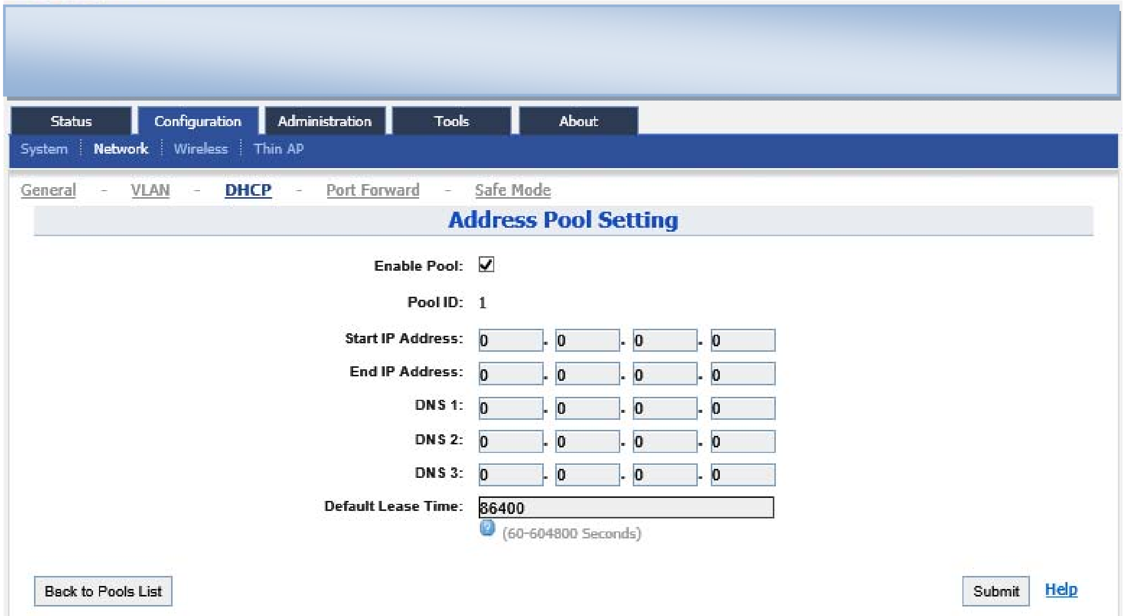
DHCP Server Setting

DHCP Server: Server Mode

Pool ID	Start IP	End IP	Default Lease Time	Enable	Detail
1	0.0.0.0	0.0.0.0	86400	No	✎
2	0.0.0.0	0.0.0.0	86400	No	✎
3	0.0.0.0	0.0.0.0	86400	No	✎
4	0.0.0.0	0.0.0.0	86400	No	✎

Figure 6-17 DHCP Server

If the DHCP Server Mode is set to Server, then the AP-100 will act as a DHCP server for allocation of IP address to the wireless client associated. The following procedures show the allocation of the IP address, subnets mask, gateway and DNS information. And edit the Pool ID 1.



Address Pool Setting

Enable Pool: ☑

Pool ID: 1

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

DNS 1: 0 . 0 . 0 . 0

DNS 2: 0 . 0 . 0 . 0

DNS 3: 0 . 0 . 0 . 0

Default Lease Time: 86400 (60-604800 Seconds)

Figure 6-18 DHCP Server

Enable Pool：Enable or Disable Pool

Pool ID：ID of the IP Pool

Start IP Address：Start IP address of the Pool

End IP Address：End IP address of the Pool

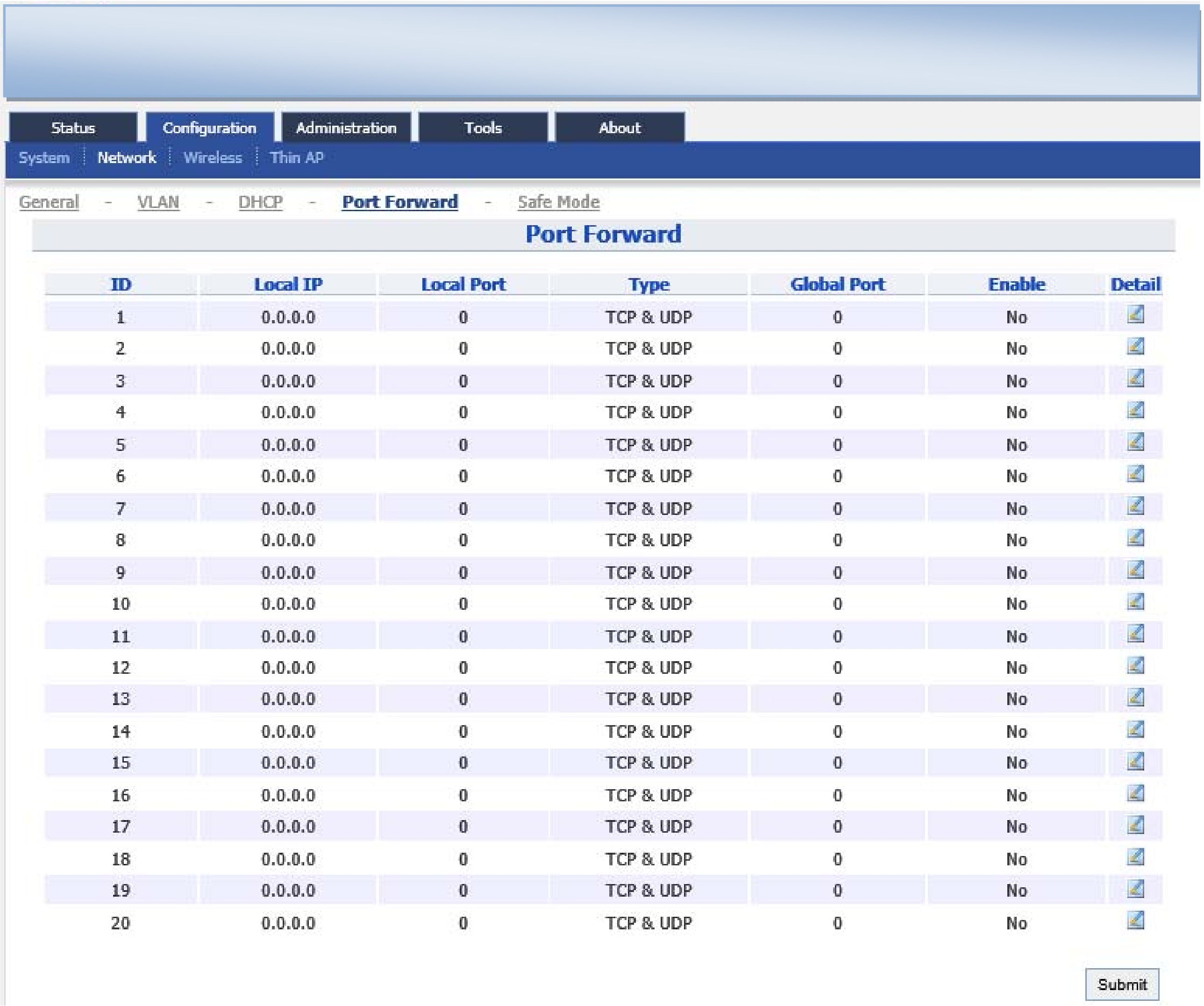
DNS1,2,3：DNS IP address of the Pool

Default Lease Time：Time to release the IP address to the clients

6.2.2.4. Port Forwarding

Select **Configuration** -> **Network** -> **Port Forwarding** to access Port forwarding configuration page to set the mapping relation for local IP, Local Port and Global Port.

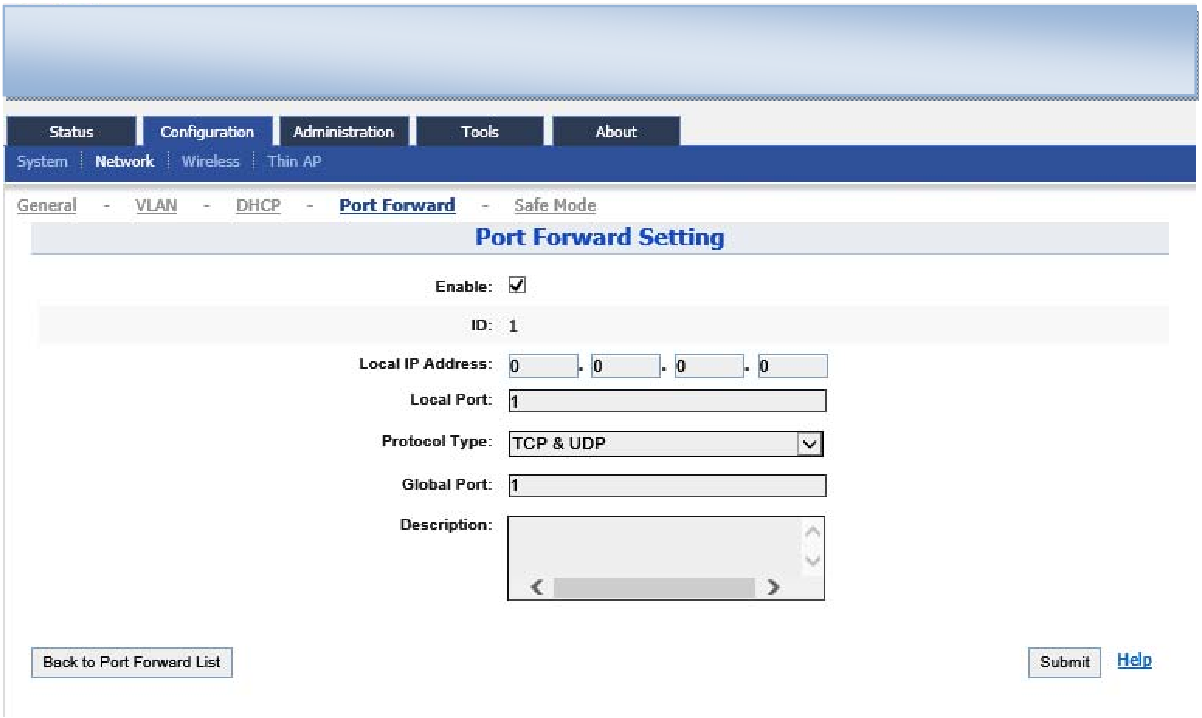
Please note that Port forwarding service only works at gateway mode.



Port Forward

ID	Local IP	Local Port	Type	Global Port	Enable	Detail
1	0.0.0.0	0	TCP & UDP	0	No	✎
2	0.0.0.0	0	TCP & UDP	0	No	✎
3	0.0.0.0	0	TCP & UDP	0	No	✎
4	0.0.0.0	0	TCP & UDP	0	No	✎
5	0.0.0.0	0	TCP & UDP	0	No	✎
6	0.0.0.0	0	TCP & UDP	0	No	✎
7	0.0.0.0	0	TCP & UDP	0	No	✎
8	0.0.0.0	0	TCP & UDP	0	No	✎
9	0.0.0.0	0	TCP & UDP	0	No	✎
10	0.0.0.0	0	TCP & UDP	0	No	✎
11	0.0.0.0	0	TCP & UDP	0	No	✎
12	0.0.0.0	0	TCP & UDP	0	No	✎
13	0.0.0.0	0	TCP & UDP	0	No	✎
14	0.0.0.0	0	TCP & UDP	0	No	✎
15	0.0.0.0	0	TCP & UDP	0	No	✎
16	0.0.0.0	0	TCP & UDP	0	No	✎
17	0.0.0.0	0	TCP & UDP	0	No	✎
18	0.0.0.0	0	TCP & UDP	0	No	✎
19	0.0.0.0	0	TCP & UDP	0	No	✎
20	0.0.0.0	0	TCP & UDP	0	No	✎

Figure 6-19 Port Forwarding-01



Port Forward Setting

Enable: ☑

ID: 1

Local IP Address: 0 . 0 . 0 . 0

Local Port: 1

Protocol Type: TCP & UDP

Global Port: 1

Description:

Figure 6-20 Port Forwarding-02

Enable Flag ：Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in system configuration file and only the enabled port forwarding entries will be active.

Local IP Address ： This control is used to specify the host which is connected to the internal network and needs to be accessible from the external network.

Local Port :This control is used to specify the TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network.

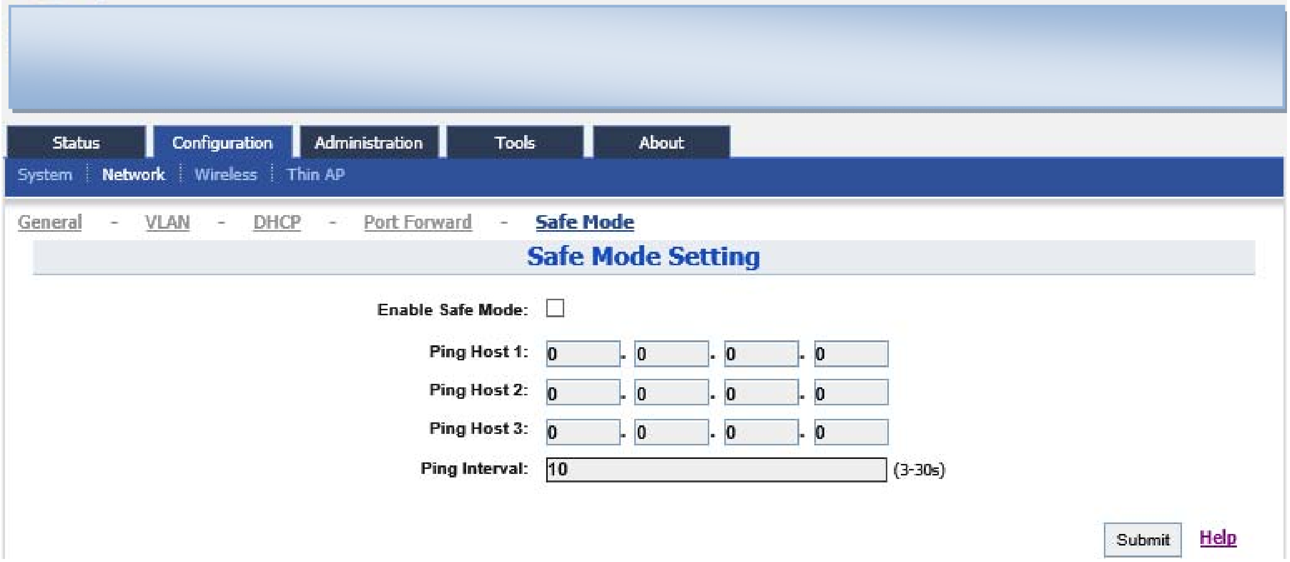
Protocol Type ： This control is used to specify the L3 protocol (IP) type which need to be forwarded from the internal network.

Global Port ： This control is used to specify the TCP/UDP port of the AP-100 Wi-Fi Access Point/Bridge based device which will accept and forward the connections from the external network to the host connected to the internal network.

Description ： This control is used to specify informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually.

6.2.2.5. Safe Mode

Select **Configuration** -> **Network** -> **Safe Mode** to access Safe Mode configuration page.



Safe Mode Setting

Enable Safe Mode: □

Ping Host 1: 0 . 0 . 0 . 0

Ping Host 2: 0 . 0 . 0 . 0

Ping Host 3: 0 . 0 . 0 . 0

Ping Interval: 10 (3-30s)

Figure 6-21 STP Setting

Enable Safe Mode：By default, it is disabled.

Ping Host：Three ping hosts can be entered. AP will ping these hosts periodically at the ping interval configured through its current backhaul link.

Ping Interval：Default setting is 10 seconds.

Procedures:

1 Select Configuration->Network->**Sate Mode**

2 **Enable Safe Mode**: Select it to enable safe mode function. By default, it is disabled.

3 **Ping Host**: at least input one host

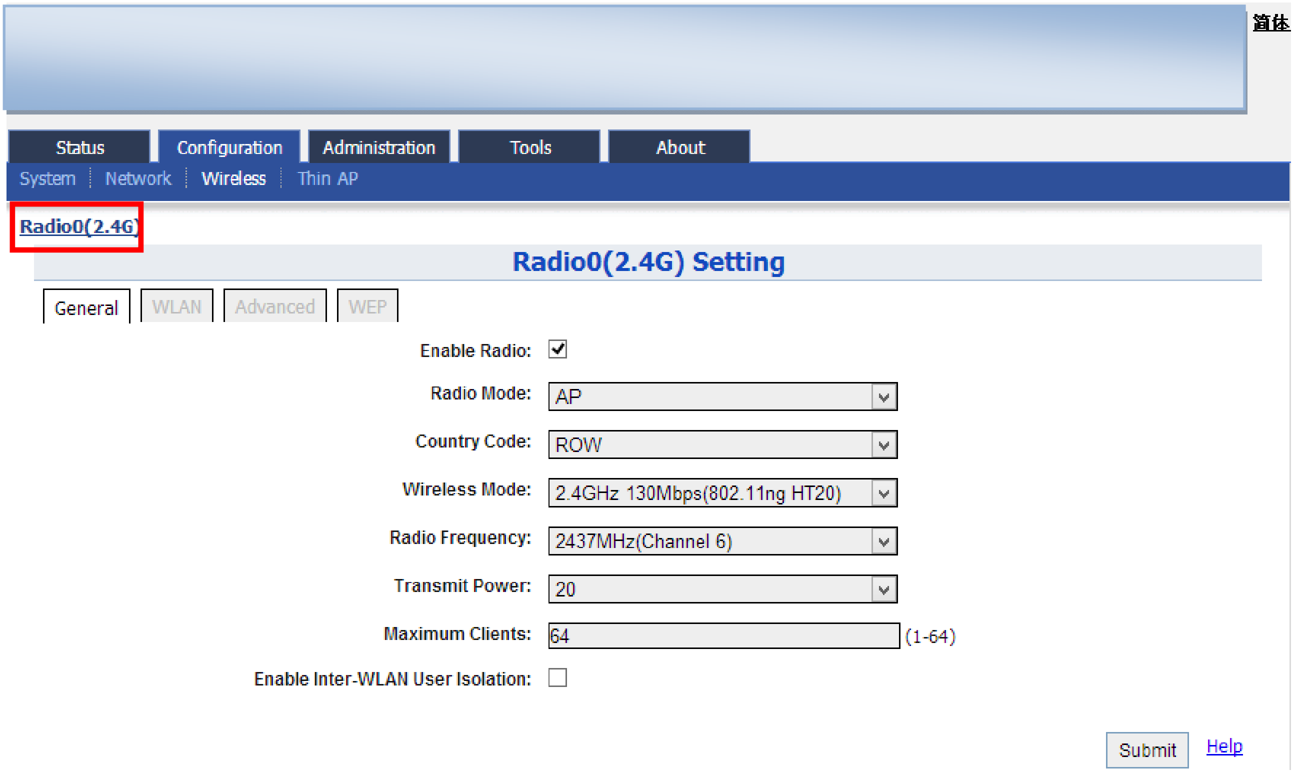
4 **Ping Interval:** input the interval of ping

5 Click **Submit**

6 Click **Save&Apply** to apply

6.2.3. Wireless

Select **Configuration** -> **Wireless** to access wireless network configuration page. There is 1 interfaces, Radio0 (2.4G).



Radio0(2.4G) Setting

Enable Radio: ☑

Radio Mode: AP

Country Code: ROW

Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Radio Frequency: 2437MHz(Channel 6)

Transmit Power: 20

Maximum Clients: 64 (1-64)

Enable Inter-WLAN User Isolation: □

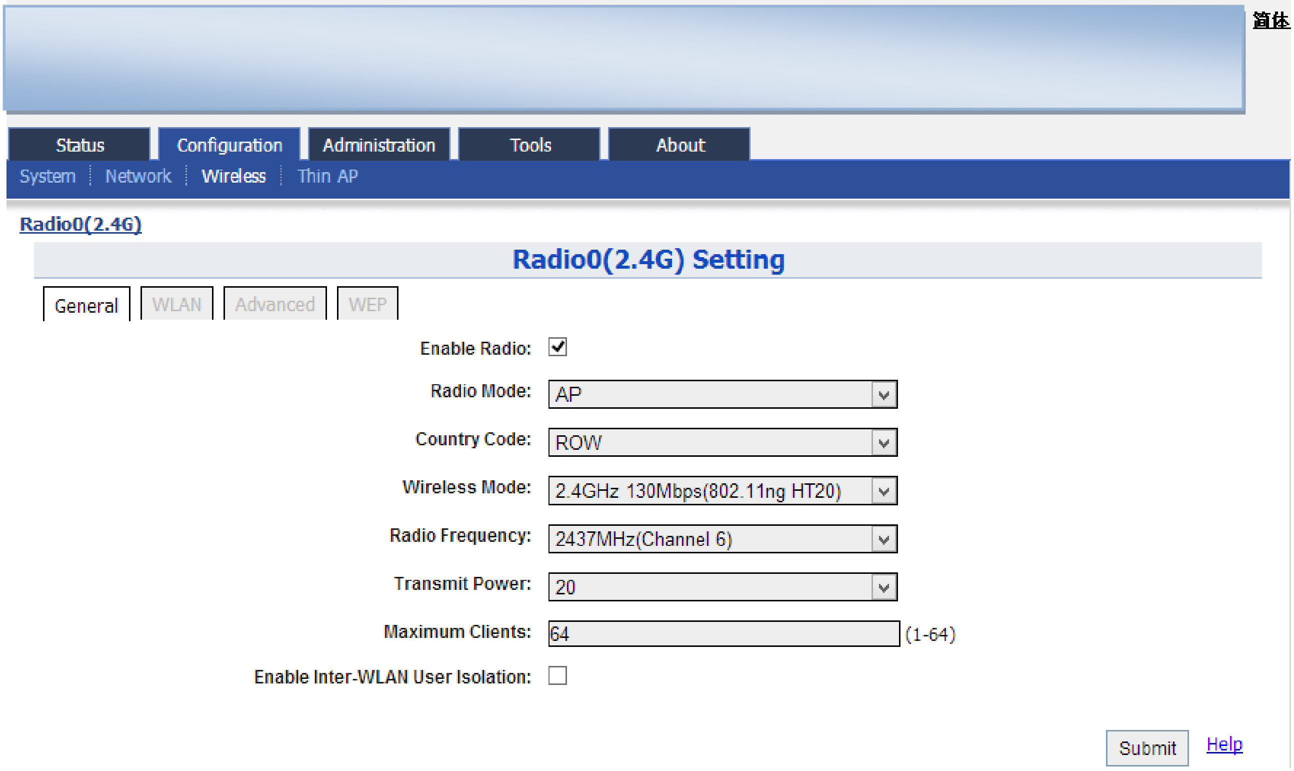
Figure 6-22 2.4G Radio Setting

6.2.3.1. 2.4G Radio

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** to change 2.4G radio setting. You can configure the items below: General, WLAN, Advanced, QoS, and WEP.

6.2.3.1.1. 2.4G General Configuration

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **General** to access 2.4G general configuration page:



Radio0(2.4G) Setting

Enable Radio: ☑

Radio Mode: AP

Country Code: ROW

Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Radio Frequency: 2437MHz(Channel 6)

Transmit Power: 20

Maximum Clients: 64 (1-64)

Enable Inter-WLAN User Isolation: □

Figure 6-23 2.4G Radio Parameters

Enable Radio: Enable or disable 2.4G radio, by default it is enabled.

Radio Mode: AP or Station or Repeater.

Country Code: ROW is default setting.

Wireless Mode: By default, it is 2.4GHz 300Mbps (802.11ng HT40+). 2.4GHz 130Mbps (802.11ng HT20) is recommended.

Radio Frequency: By default, it is 2437MHz (Channel 6).

Transmit Power：By default, it is 20.

Maximum Clients：By default, it is 64.

Enable Inter-WLAN User Isolation：By default, it is disable.

Disable HT20/HT40 Auto Switch：In HT40 mode, enable or disable auto switch between HT40 and HT20.

Procedures:

Select Configuration->Wireless ->Radio0 (2.4G)->General

1 **Enable Radio :** Select to enable 2.4G Radio

2 **Radio Mode:** Select to AP mode

3 **Country Code:** Select your country code

4 **Wireless Mode** Select wireless mode

5 **Transmit Power** Set transmit power

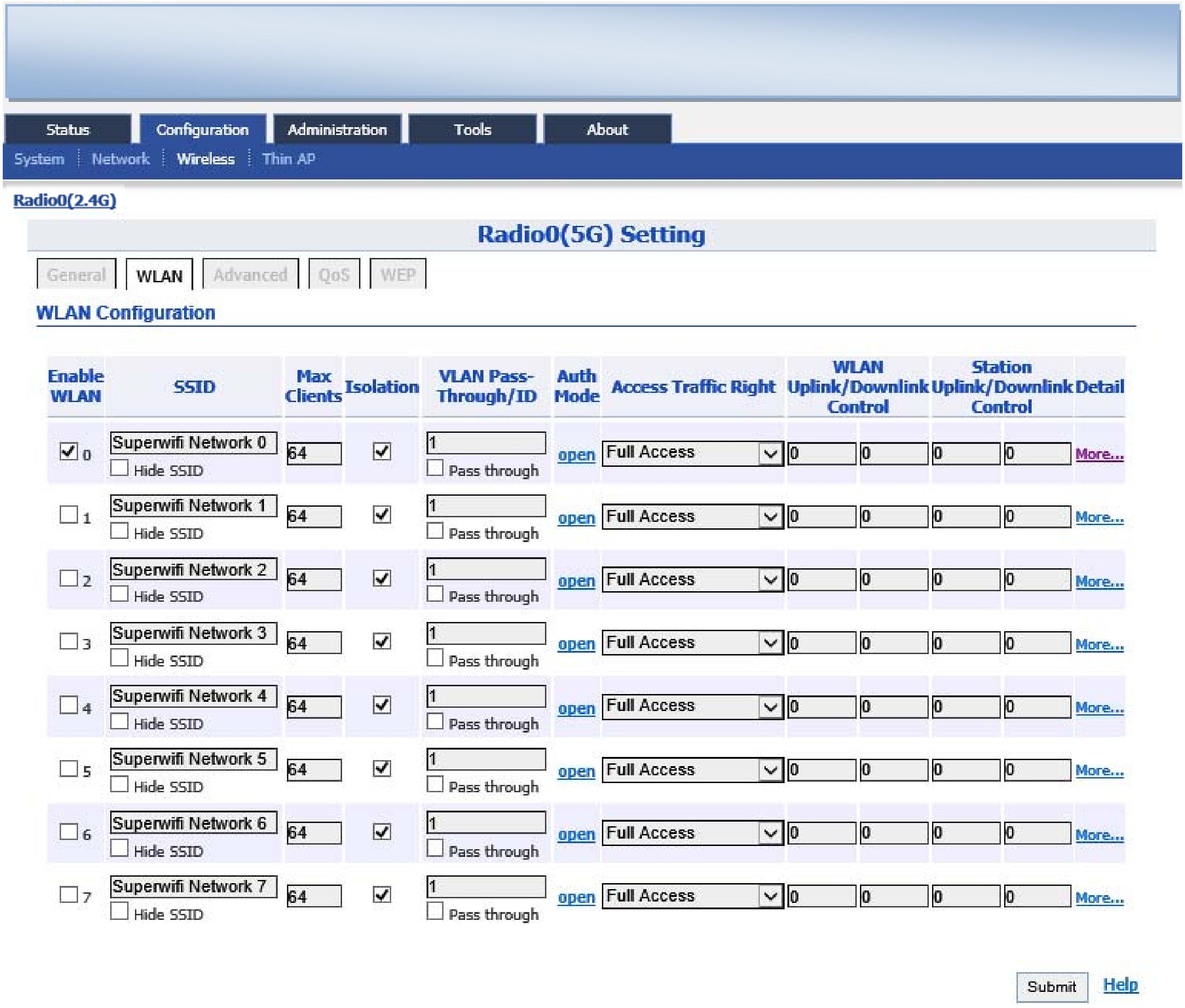
6 **Maximum Clients** Set 2.4G maximum clients

7 Click **Submit**

8 Click **Save&Apply** to apply

6.2.3.1.2. 2.4G WLAN

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to access to 2.4G radio WLAN setting page:



Radio0(5G) Setting

WLAN Configuration

Enable WLAN	SSID	Max Clients	Isolation	VLAN Pass-Through/ID	Auth Mode	Access Traffic Right	WLAN Uplink/Downlink Control		Station Uplink/Downlink Control		Detail
☑ 0	Superwifi Network 0 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 1	Superwifi Network 1 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 2	Superwifi Network 2 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 3	Superwifi Network 3 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 4	Superwifi Network 4 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 5	Superwifi Network 5 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 6	Superwifi Network 6 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...
□ 7	Superwifi Network 7 □ Hide SSID	64	☑	1 □ Pass through	open	Full Access	0	0	0	0	More...

Figure 6-24 WLAN Setting

AP-100 2.4G radio supports maximum 8 WLANs, and they can be configured separately.

Enable WLAN ： Enable or Disable WLAN from 0-7.

SSID：Support maximum 32 characters, default SSID is：Superwifi Network X, X is WLAN number.

Max Clients：Max. Associated clients

Isolation： Enable or Disable inter-WLAN communication isolation. By default, it is enable.

VLAN Pass-Through/ID： Set VLAN pass through or VLAN TagID this WLAN

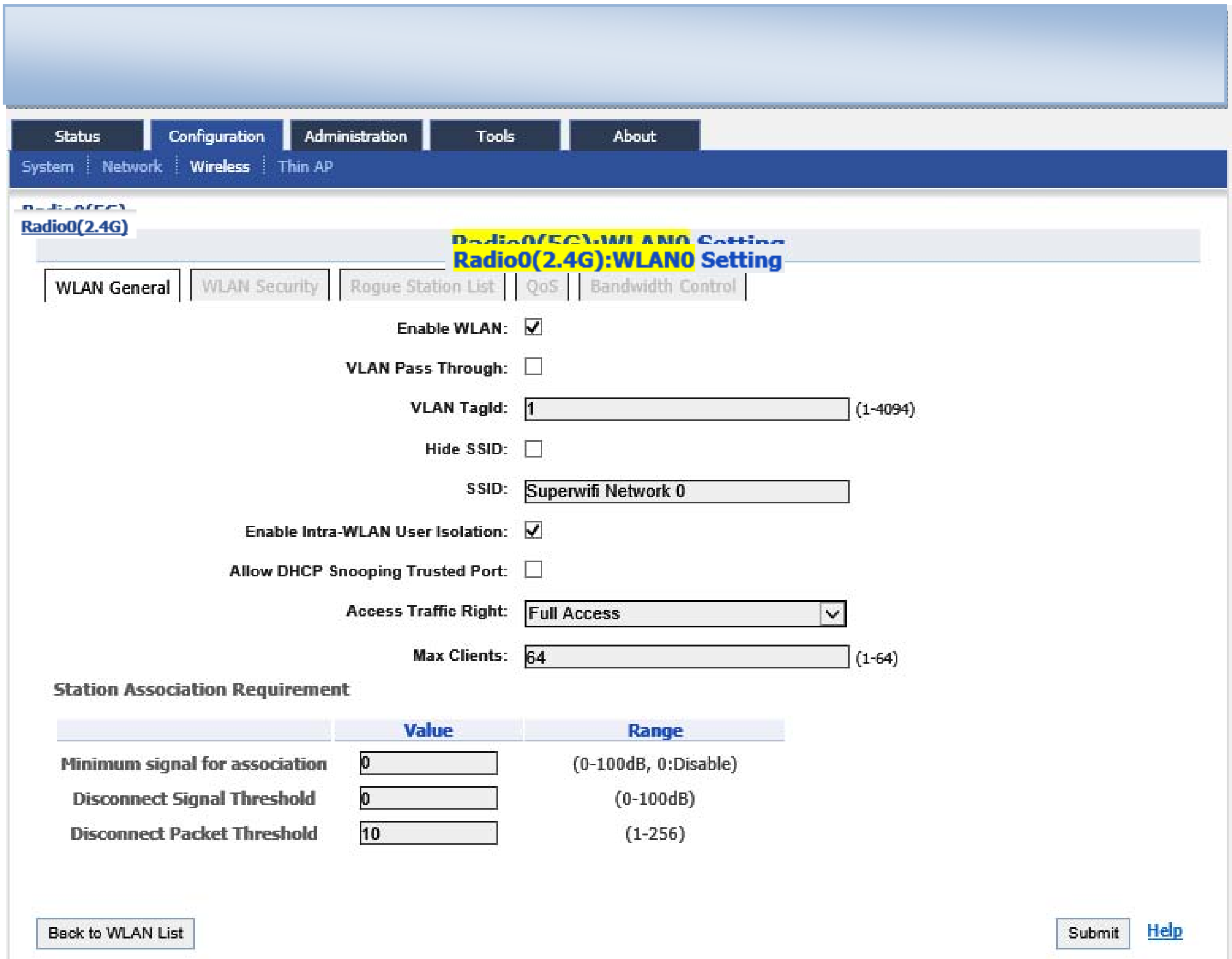
Access Traffic Right：Access traffic right controls associated stations the ability to permit or deny AP management.

WLAN Uplink/Downlink Control： This option control the uplink and downlink speed for this WLAN.

Station Uplink/Downlink Control： This option control the uplink and downlink speed for the stations which associate to this WLAN.

1. WLAN X (0-7) WLAN Setting

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to click "**More…**" behind the WLAN, and then select **WLAN General**.



Radio0(2.4G):WLAN0 Setting

Enable WLAN:	☑	
VLAN Pass Through:	□	
VLAN TagId:	1	(1-4094)
Hide SSID:	□	
SSID:	Superwifi Network 0	
Enable Intra-WLAN User Isolation:	☑	
Allow DHCP Snooping Trusted Port:	□	
Access Traffic Right:	Full Access	
Max Clients:	64	(1-64)

Station Association Requirement

	Value	Range
Minimum signal for association	0	(0-100dB, 0:Disable)
Disconnect Signal Threshold	0	(0-100dB)
Disconnect Packet Threshold	10	(1-256)

Figure 6-25 WLAN General Setting

Enable WLAN：Enable or disable this WLAN.

VLAN Pass Through：VLAN pass through for this WLAN.

Enable WLAN：Set VLAN TagId for this WLAN.

Hide SSID：Hide this SSID or not.

SSID：Set SSID name.

Allow Intra-WLAN User Isolation :Allow or block intra-WLAN user communication. By default, it is enable.

Allow DHCP Snooping Trusted Port：DHCP snooping prevents illegal DHCP servers from offering IP address on untrusted wireless port.

Access Traffic Right：Access traffic right controls associated stations the ability to permit or deny AP management.

Max Clients：Maximum value is 64.

Station Association Requirement

Minimum signal for association: Set the minimum signal value (SNR) for client can associate to this WLAN. The range is 0~100dB, and 0 means disable.

Disconnect Signal Threshold： Set the signal threshold value (SNR) for client to disconnect to this WLAN.

Disconnect Packet Threshold :Set the packet threshold value (SNR) for client to disconnect to this WLAN.

Back to WLAN List： Go back to previous page

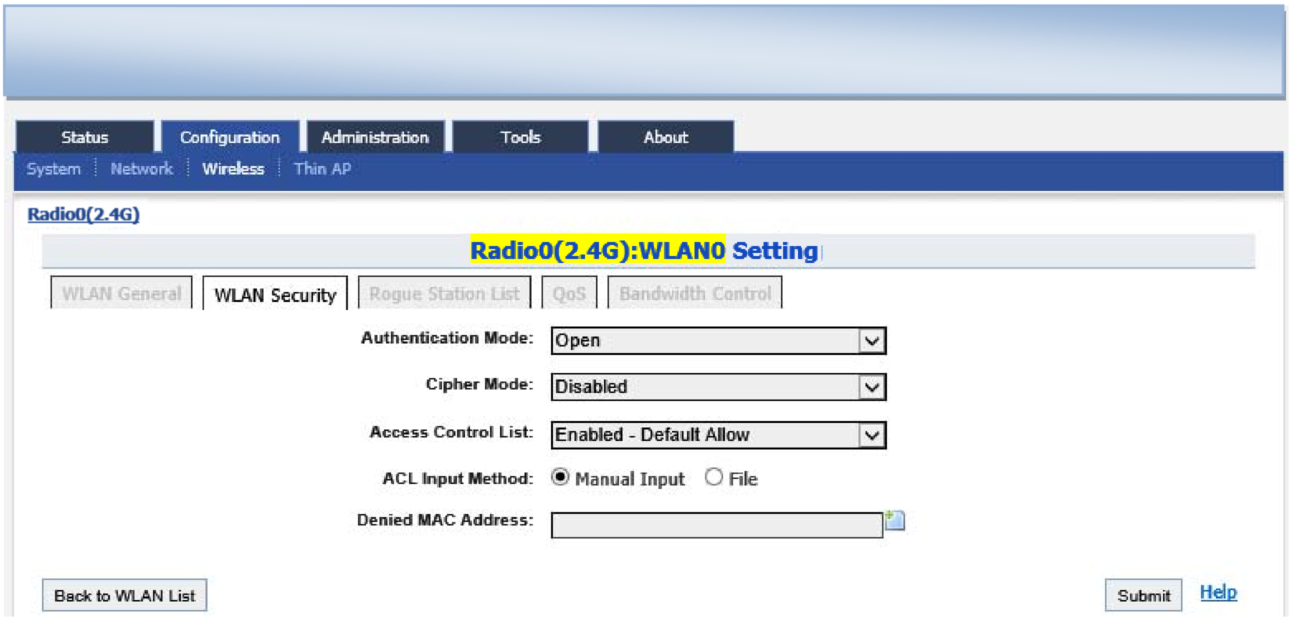
Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to click "**More…**" behind the WLAN, and then select **WLAN General**.
2. **Enable WLAN** select to enable this WLAN
3. **VLAN Pass Through** allow or don't allow VLAN pass through
4. **VLAN TagId** Set VLAN ID
5. **SSID** set SSID
6. **Allow Intra-WLAN User Isolation**: Allow or block intra-WLAN User communication.
7. **Max Clients** Maximum is 64
8. Click **Submit**
9. Click **Save&Apply** to apply

2. WLAN X (0-7) Security

AP-100 2.4GHz supports Open, Shared Key, WPA, WPA-PSK, WPA2, WPA2-PSK, WAPI, WAPI-PSK authentication mode, and Disabled, WEP, AES, TKIP, SMS4 cipher mode.

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)**-> **WLAN** to edit "More…" WLAN, and then select **WLAN Security** to access to security configuration page.



Authentication Mode: Open

Cipher Mode: Disabled

Access Control List: Enabled - Default Allow

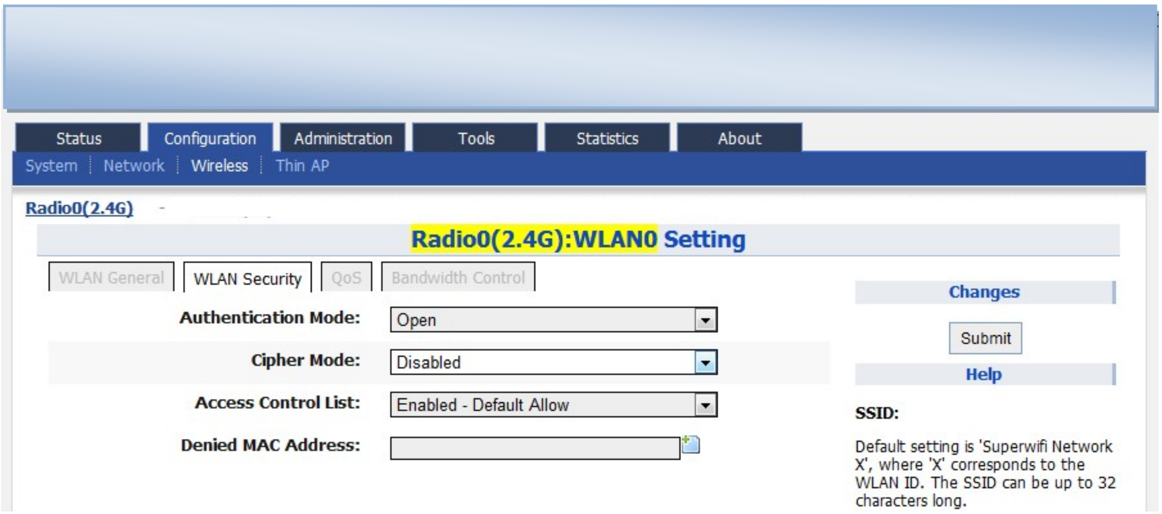
ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

Figure 6-26 WLAN Security Setting

1) Open

After selecting Open, you can select Disabled or WEP:



Authentication Mode: Open

Cipher Mode: Disabled

Access Control List: Enabled - Default Allow

Denied MAC Address:

SSID:

Default setting is 'Superwifi Network X', where 'X' corresponds to the WLAN ID. The SSID can be up to 32 characters long.

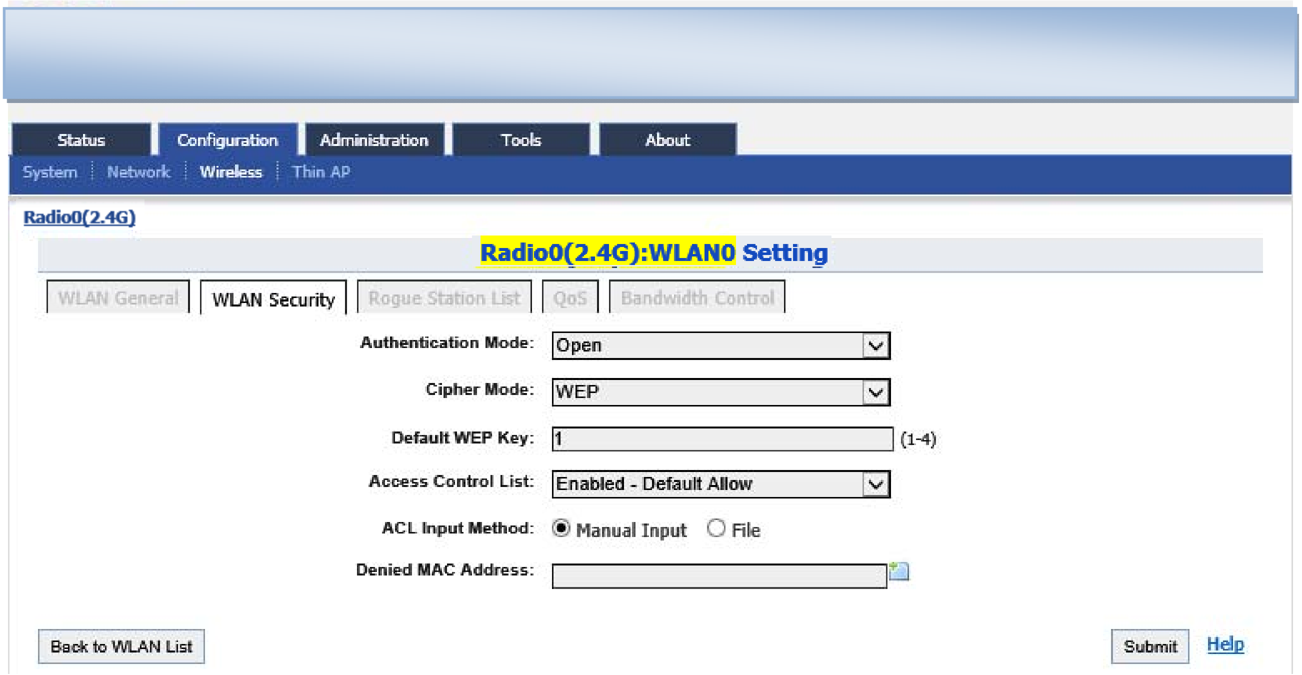
Figure 6-27 Open & No Security

Open & No security procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)**-> **WLAN** to edit “More…” WLAN, and then select **WLAN Security** to access to security configuration page
2. **Authentication Mode** choose Open
3. **Cipher Mode** choose Disabled
4. Click **Submit**
5. Click **Save&Apply** to apply

Open – WEP Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)**-> **WLAN** to edit "More…" WLAN, and then select **WLAN Security** to access to security configuration page
2. **Authentication Mode** choose Open
3. **Cipher Mode** choose WEP
4. **Default WEP Key** set the password
5. Click **Submit**
6. Click **Save&Apply** to apply



Authentication Mode: Open

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

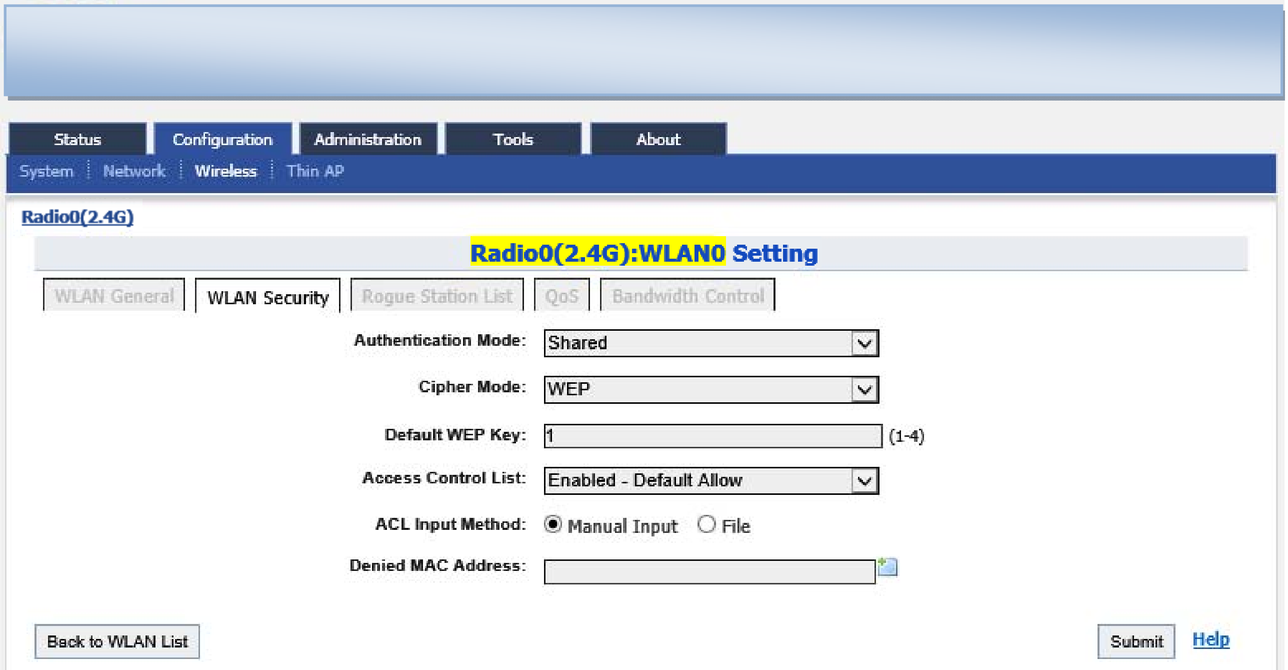
Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

Figure 6-28 Open & WEP

2) Shared Key



Authentication Mode: Shared

Cipher Mode: WEP

Default WEP Key: 1 (1-4)

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

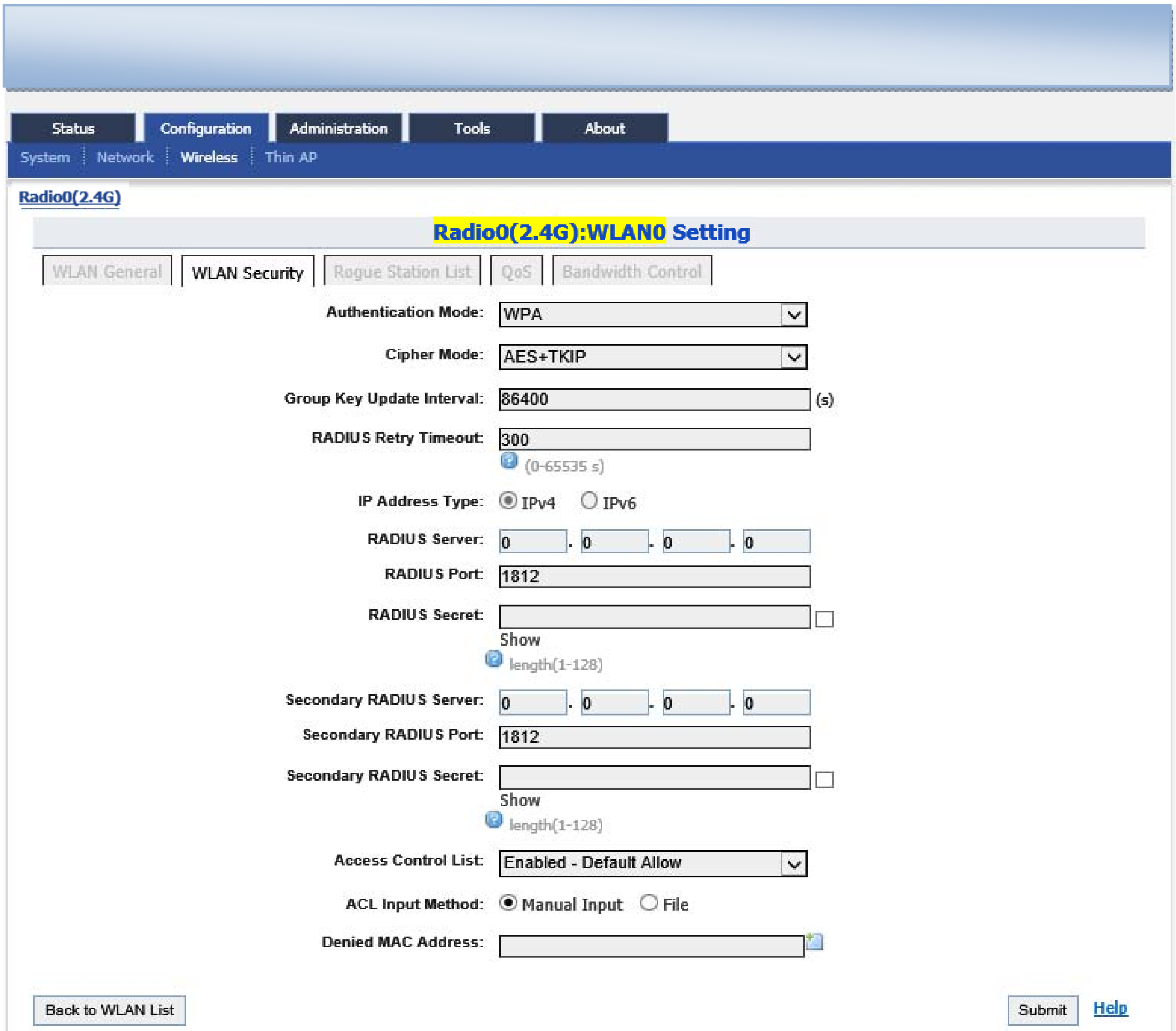
Figure 6-29 Shared Key

Shared key Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)**-> **WLAN** to edit “More…” WLAN, and then select **WLAN Security** to access to security configuration page
2. **Authentication Mode** choose Shared
3. **Cipher Mode** choose WEP
4. **Default WEP Key** set the password
5. Click **Submit**
6. Click **Save&Apply** to apply

3) WPA/WPA2

WPA/WPA2 can be enabled by selecting WPA, WPA2 for Authentication Mode. The AES and TKIP are the two available options for Ciper mode.



Radio0(2.4G):WLAN0 Setting

Authentication Mode: WPA

Cipher Mode: AES+TKIP

Group Key Update Interval: 86400 (s)

RADIUS Retry Timeout: 300 (0-65535 s)

IP Address Type: ● IPv4 ○ IPv6

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

RADIUS Secret: □ Show length(1-128)

Secondary RADIUS Server: 0 . 0 . 0 . 0

Secondary RADIUS Port: 1812

Secondary RADIUS Secret: □ Show length(1-128)

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

Figure 6-30 WPA/WPA2

Authentication Mode：WPA or WPA2

Cipher Mode： AES and TKIP can be choice.

Radius Server：Set Radius server IP address

Radius Port：set Radius server port

Radius Secret：Set Radius secret

Secondary Radius Server：Set Secondary Radius server IP address

Secondary Radius Port：Set Secondary Radius server port

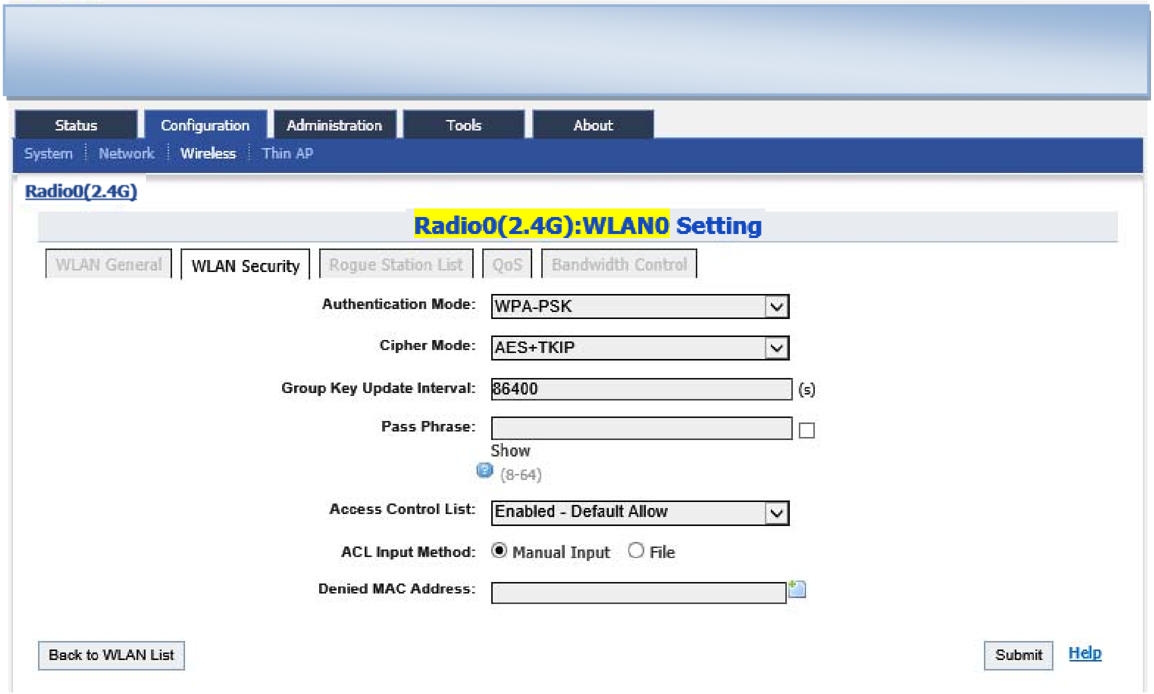
Secondary Radius Secret：Set Secondary Radius server secret

WPA/WPA2 Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)**-> **WLAN** to edit "More…" WLAN, and then select **WLAN Security** to access to security configuration page
2. **Authentication Mode** choose WPA or WPA2
3. **Cipher Mode** choose AES+TKIP
4. **Radius Server** set Radius server IP address
5. **Radius Port** set Radius server port
6. **Radius Secret** set Radius password
7. **Secondary Radius Server** set Secondary Radius server IP address (optional)
8. **Secondary Radius Port** set Secondary Radius server port (optional)
9. **Secondary Radius Secret** set Secondary Radius server secret (optional)
10. Click **Submit**
11. Click **Save&Apply** to apply

4) WPA-PSK/WPA2-PSK

WPA-PSK can be enabled by selecting ***WPA-PSK, WPA2-PSK*** for Authentication Mode. The ***AES*** and ***TKIP*** are the two available options for Cipher Mode.



Radio0(2.4G):WLAN0 Setting

Authentication Mode: WPA-PSK

Cipher Mode: AES+TKIP

Group Key Update Interval: 86400 (s)

Pass Phrase: □ Show (8-64)

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

Figure 6-31 WPA-PSK/WPA2-PSK

Authentication Mode：WPA or WPA2

Cipher Mode： AES and TKIP can be selected.

Group Key Update Interval：By default, it is 3600

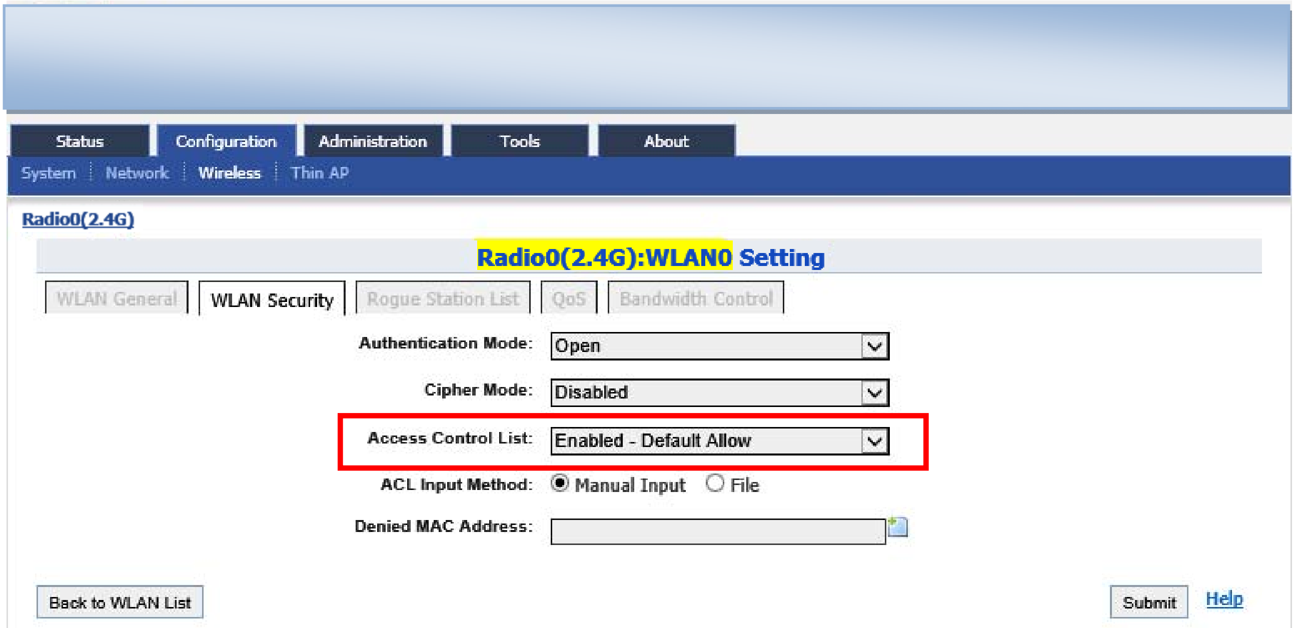
Pass Phrase：From 8-64 bits

WPA-PSK/WPA2-PSK Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…" WLAN, and then select **WLAN Security** to access to security configuration page
2. **Authentication Mode** choose WPA-PSK or WPA2-PSK
3. **Cipher Mode** choose AES+TKIP
4. **Group Key Update Interval**: set interval
5. **Pass Phrase** set the password
6. Click **Submit**
7. Click **Save&Apply** to apply

5) ACL Configurations

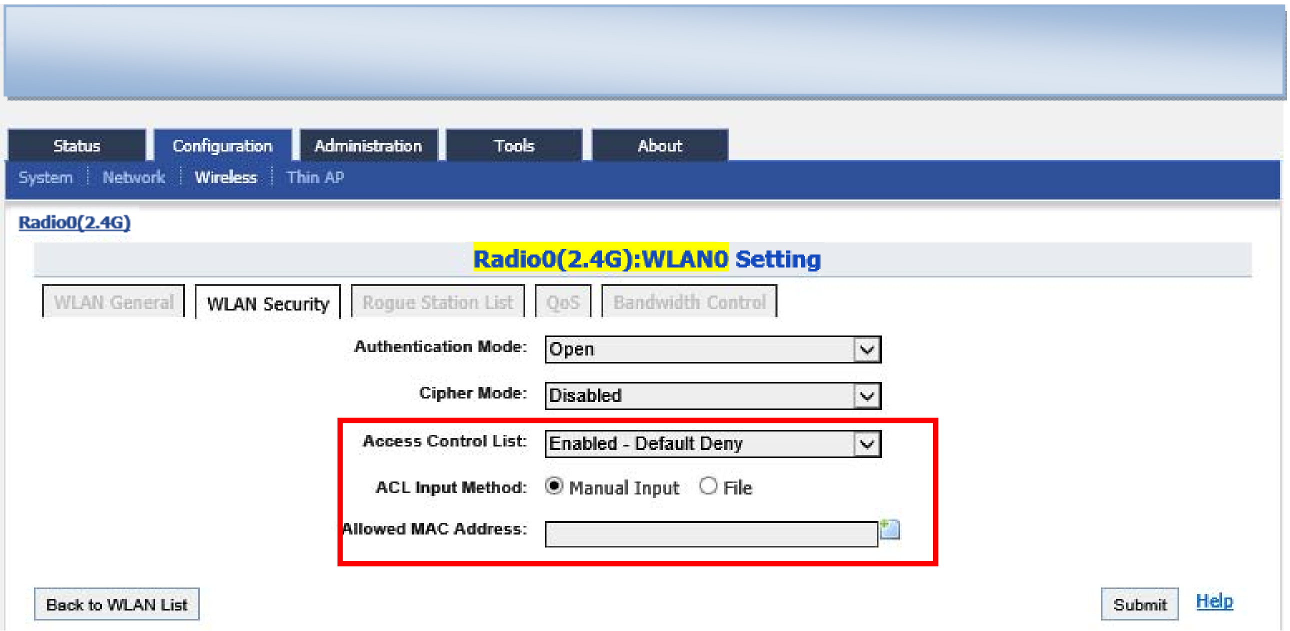
AP-100 supports ACL（Access Control List）, it bases on MAC address filter.



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open
Cipher Mode: Disabled
Access Control List: Enabled - Default Allow
ACL Input Method: ● Manual Input ○ File
Denied MAC Address:

Figure 6-32 ACL-Disable



Authentication Mode: Open

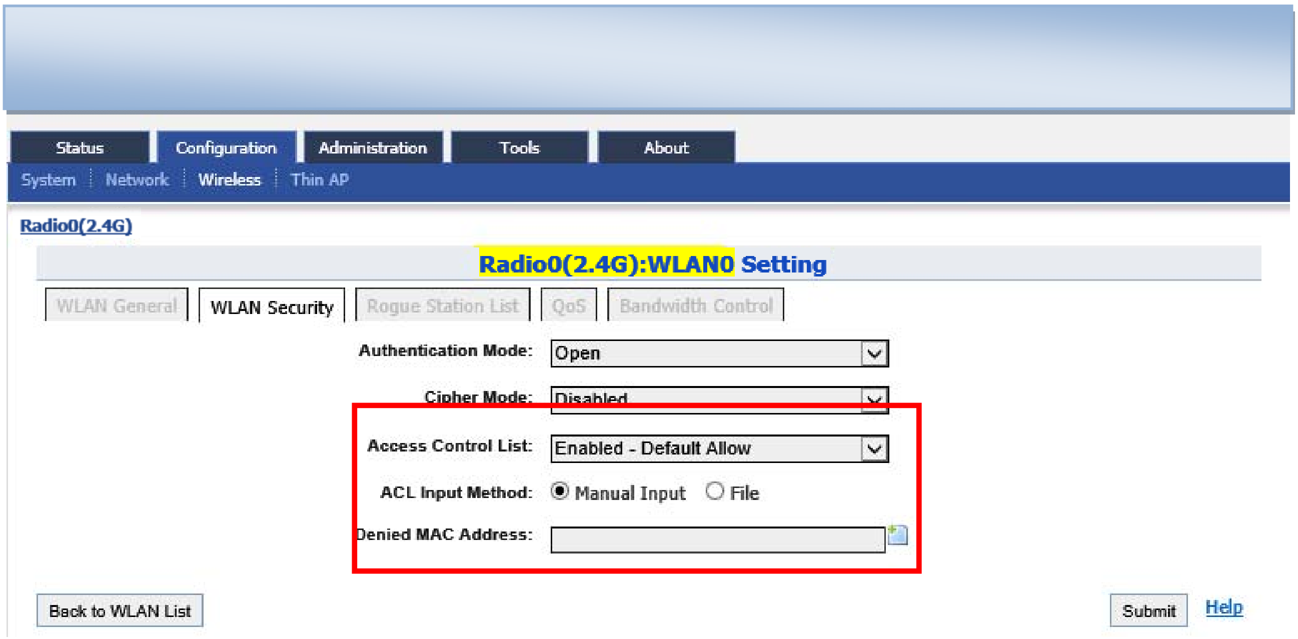
Cipher Mode: Disabled

Access Control List: Enabled - Default Deny

ACL Input Method: ● Manual Input ○ File

Allowed MAC Address:

Figure 6-33 ACL-Deny MAC Address



Authentication Mode: Open

Cipher Mode: Disabled

Access Control List: Enabled - Default Allow

ACL Input Method: ● Manual Input ○ File

Denied MAC Address:

Figure 6-34 ACL-Allow MAC Address

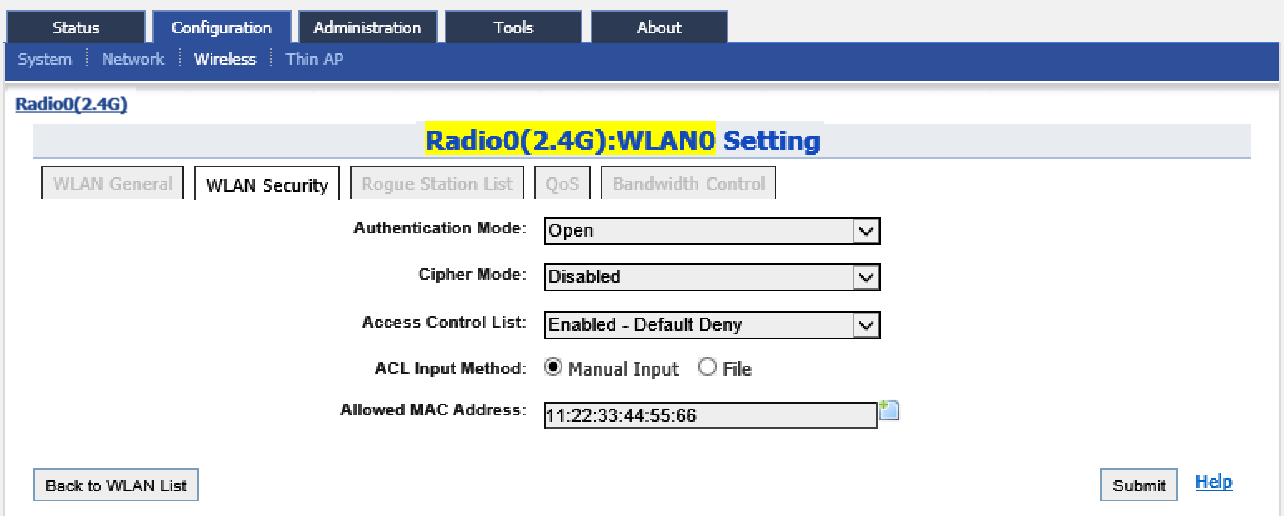
Access Control List：There are 3 modes: Disabled, Enabled-Default Allow, and Enable-Default Deny.

Denied MAC Address：All MAC address in the list will be blocked.

Allowed MAC Address：Only MAC address in the list can access.

ACL Procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…" WLAN, and then select **WLAN Security** to access to security configuration page
2. **Access Control List** choose the control mode.
3. **Denied MAC Address** input MAC address
4. **Allowed MAC Address** input MAC address
5. Click **Submit**
6. Click **Save&Apply** to apply



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

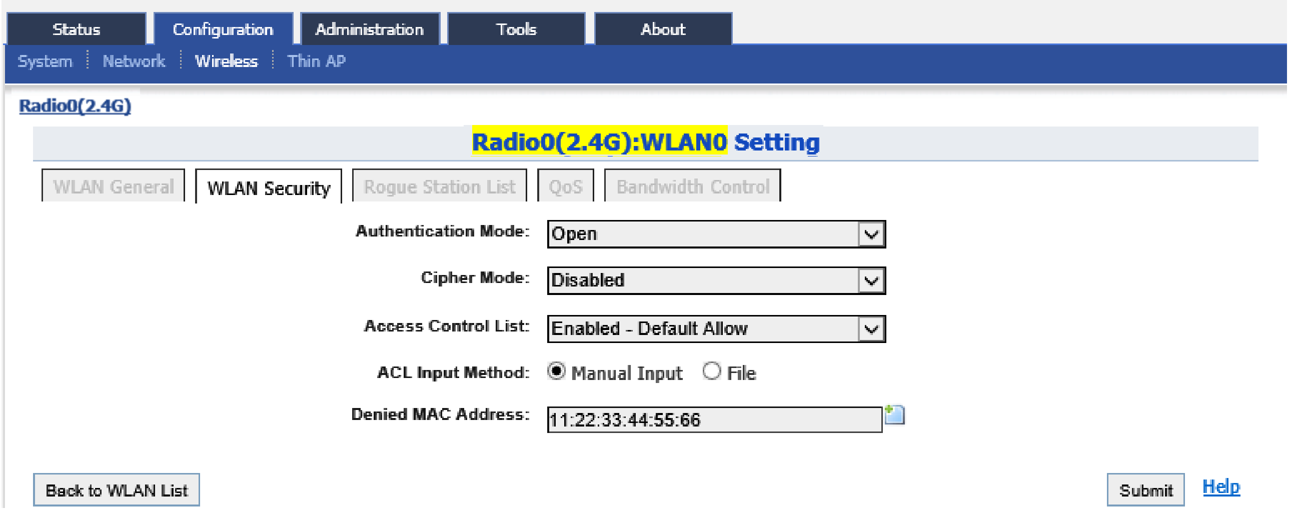
Cipher Mode: Disabled

Access Control List: Enabled - Default Deny

ACL Input Method: ● Manual Input ○ File

Allowed MAC Address: 11:22:33:44:55:66

Figure 6-35 ACL-Add Denied MAC Address



Radio0(2.4G):WLAN0 Setting

Authentication Mode: Open

Cipher Mode: Disabled

Access Control List: Enabled - Default Allow

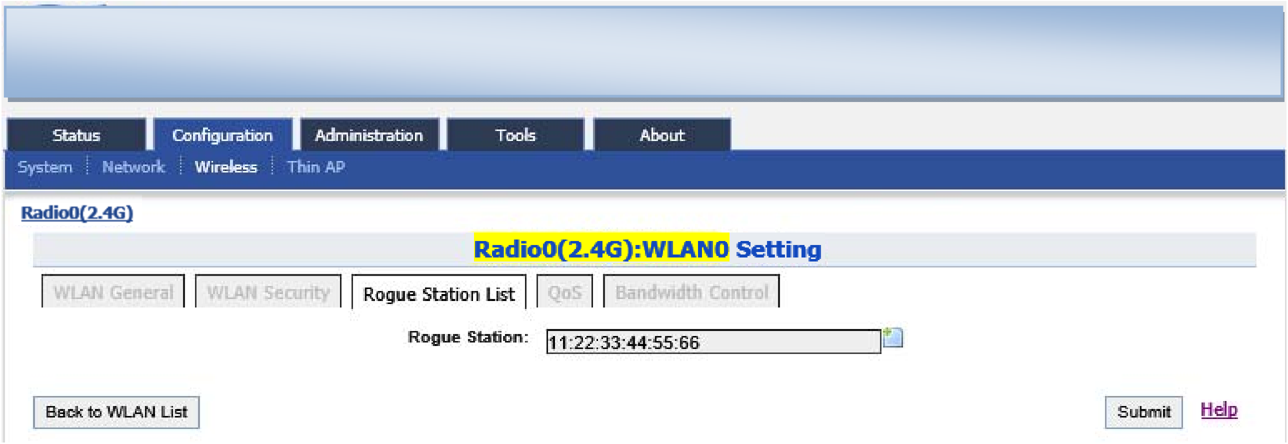
ACL Input Method: ● Manual Input ○ File

Denied MAC Address: 11:22:33:44:55:66

Figure 6-36 ACL-Add Allowed MAC Address

3. WLAN X (0-7) Rogue Station List

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…" WLAN, and then select **Rogue Station List** to access to Rogue Station List configuration page



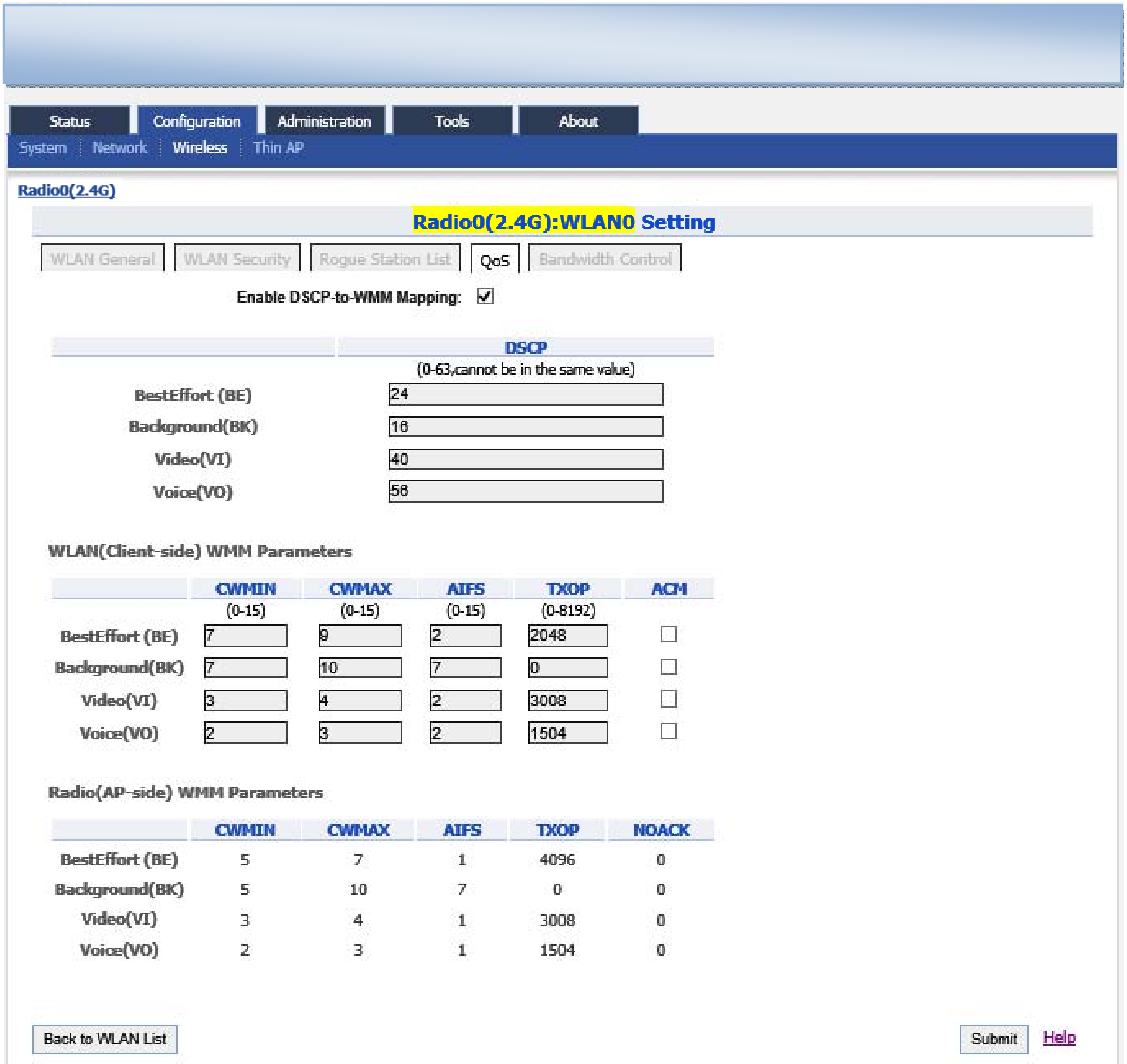
Rogue Station: 11:22:33:44:55:66

Figure 6-37 Rogue Station List

Rogue Station： Type in the MAC address of rogue station.

4. WLAN X (0-7) QoS

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…" WLAN, and then select **QoS** to access to QoS configuration page



Radio0(2.4G):WLAN0 Setting

Enable DSCP-to-WMM Mapping: ☑

	DSCP (0-63,cannot be in the same value)
BestEffort (BE)	24
Background(BK)	16
Video(VI)	40
Voice(VO)	56

WLAN(Client-side) WMM Parameters

	CWMIN (0-15)	CWMAX (0-15)	AIFS (0-15)	TXOP (0-8192)	ACM
BestEffort (BE)	7	9	2	2048	□
Background(BK)	7	10	7	0	□
Video(VI)	3	4	2	3008	□
Voice(VO)	2	3	2	1504	□

Radio(AP-side) WMM Parameters

	CWMIN	CWMAX	AIFS	TXOP	NOACK
BestEffort (BE)	5	7	1	4096	0
Background(BK)	5	10	7	0	0
Video(VI)	3	4	1	3008	0
Voice(VO)	2	3	1	1504	0

Figure 6-38 WLAN QoS

Enable DSCP-to-WMM Mapping：Enable mapping from DSCP to WMM.

DSCP：4 priorities: BestEffort、Background、Video、Voice

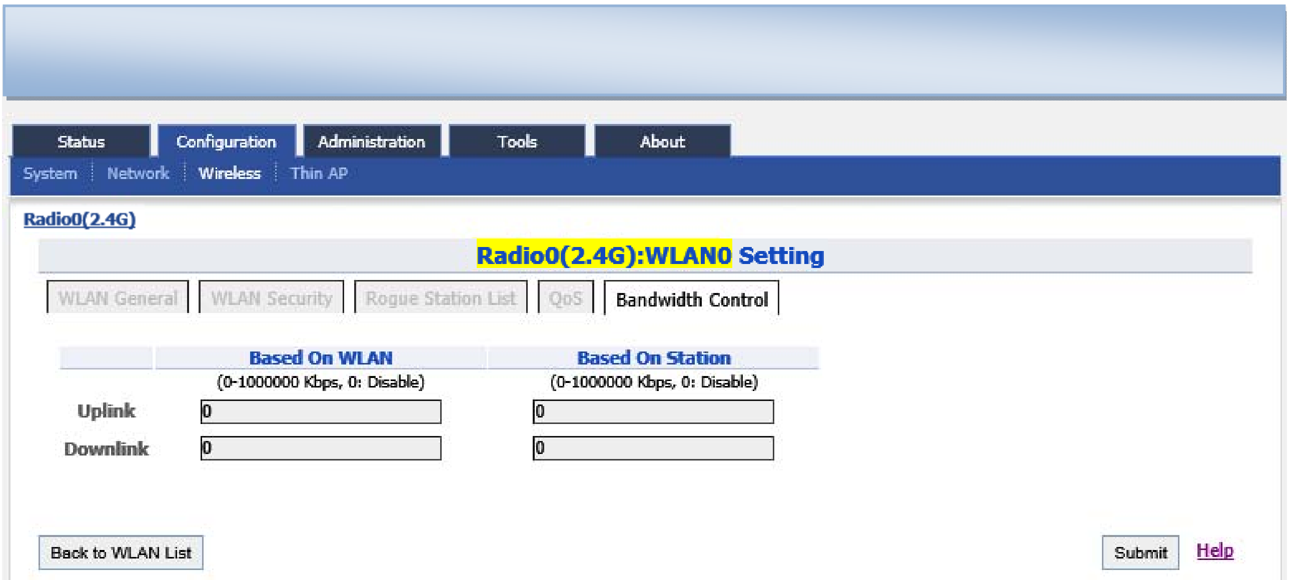
WLAN（Client-side）WMM Parameters：Set CWMIN、CWMAX、AIFS、TXOP value

Radio(AP-side) WMM Parameters：List WMM parameters

WLAN X QoS configuration procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…" WLAN, and then select **QoS** to access to QoS configuration page
2. **Enable DSCP-to-WMM Mapping** (optional)
3. **DSCP** choose one of priorities
4. **WLAN（Client-side）WMM Parameters** Set CWMIN、CWMAX、AIFS、TXOP value
5. Click **Submit**
6. Click **Save&Apply** to apply

5. WLAN X (0-7) Bandwidth Control



Radio0(2.4G):WLAN0 Setting

	Based On WLAN (0-1000000 Kbps, 0: Disable)	Based On Station (0-1000000 Kbps, 0: Disable)
Uplink	0	0
Downlink	0	0

Figure 6-39 WLAN Bandwidth Control

Uplink：Uplink bandwidth control, from 0-1000000Kbps

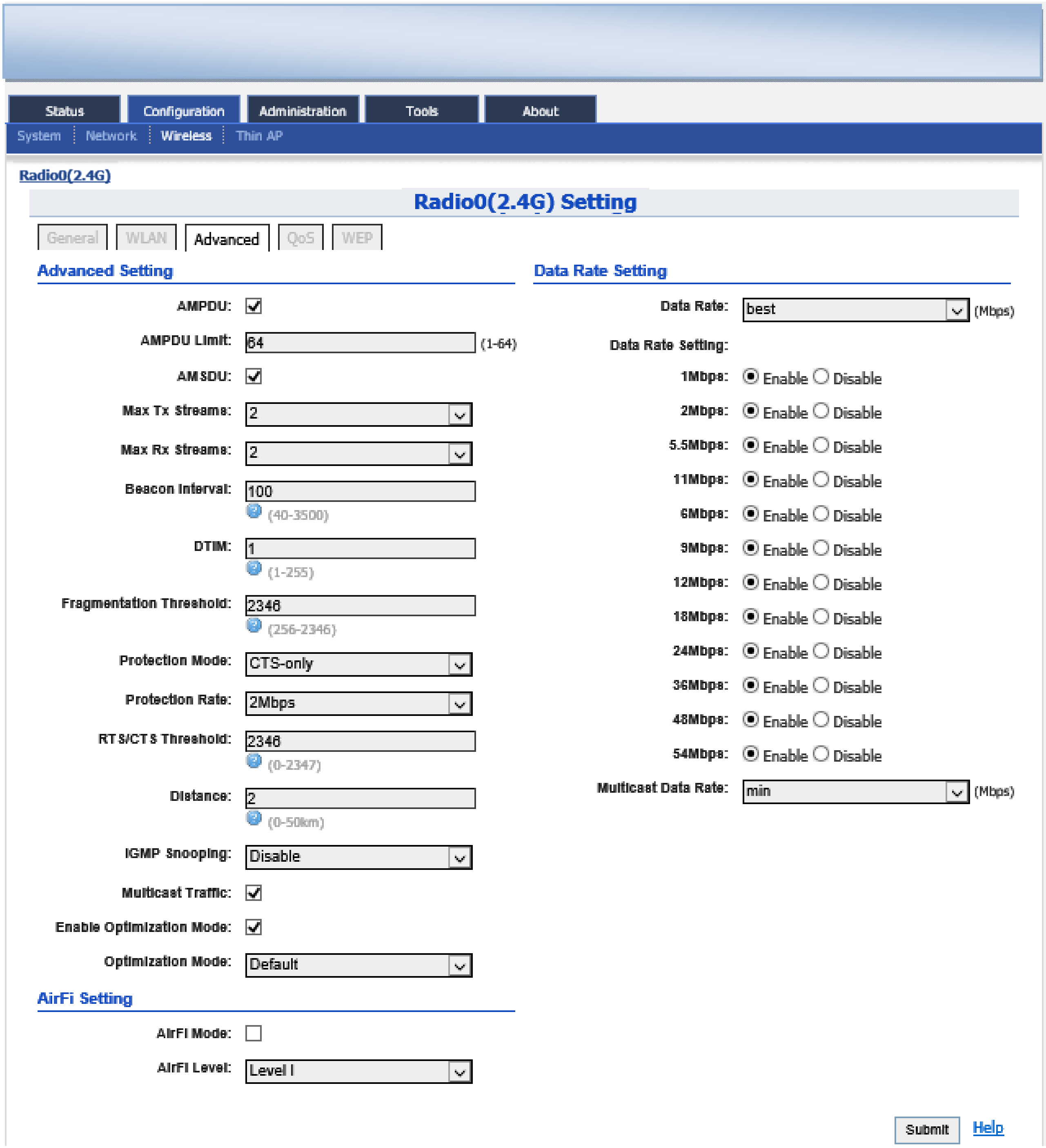
Downlink：Downlink bandwidth control, from 0-1000000Kbps

WLAN X bandwidth control procedures：

1. Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **WLAN** to edit "More…"WLAN, and then select **Bandwidth Control** to access to Bandwidth Control configuration page
2. **Uplink** set uplink bandwidth limitation
3. **Downlink** set downlink bandwidth limitation
4. Click **Submit**
5. Click **Save&Apply** to apply

6.2.3.1.3. 2.4G Advanced Configuration

Select **Configuration** -> **Wireless** -> **Radio0 (2.4G)** -> **Advanced** to access to Advanced configuration page



Radio0(2.4G) Setting

Advanced Setting

AMPDU:	☑
AMPDU Limit:	64 (1-64)
AMSDU:	☑
Max Tx Streams:	2
Max Rx Streams:	2
Beacon Interval:	100 (40-3500)
DTIM:	1 (1-255)
Fragmentation Threshold:	2346 (256-2346)
Protection Mode:	CTS-only
Protection Rate:	2Mbps
RTS/CTS Threshold:	2346 (0-2347)
Distance:	2 (0-50km)
IGMP Snooping:	Disable
Multicast Traffic:	☑
Enable Optimization Mode:	☑
Optimization Mode:	Default

AirFi Setting

AirFi Mode:	□
AirFi Level:	Level I

Data Rate Setting

Data Rate:	best (Mbps)
Data Rate Setting:	
1Mbps:	● Enable ○ Disable
2Mbps:	● Enable ○ Disable
5.5Mbps:	● Enable ○ Disable
11Mbps:	● Enable ○ Disable
6Mbps:	● Enable ○ Disable
9Mbps:	● Enable ○ Disable
12Mbps:	● Enable ○ Disable
18Mbps:	● Enable ○ Disable
24Mbps:	● Enable ○ Disable
36Mbps:	● Enable ○ Disable
48Mbps:	● Enable ○ Disable
54Mbps:	● Enable ○ Disable
Multicast Data Rate:	min (Mbps)

Figure 6-40 Radio Advanced Setting

AP-100 provides advanced parameter setting, it would change AP-100 performance. ***Default setting is recommended.***

Advance Setting

AMPDU：IEEE802.11n aggregation of MAC protocol data unit.

AMPDU Limit：Maximum number frames in 11n frame aggregation.

AMSDU：IEEE802.11n aggregation of MAC service data unit.

Max Tx/Rx Streams：Maximum number of transmit streams/receive streams in 11n MIMO.

Beacon Interval：Default setting is 100 ms (equivalent to 10 beacons per second). The amount of time between AP-100 BTS beacon transmissions for each supported BSS, with each BSS using the same beacon interval. The beacon interval can be configured between 20 and 1000 ms.

DTIM：Default setting is 1. DTIM Interval, always a multiple of the beacon period, determines how often the beacon contains a traffic indicator map (TIM). The TIM alerts clients in sleep state to stay awake long enough to receive their data frames. The value range is from 1 to 255.

Fragmentation Threshold :Default setting is 2346 bytes. The fragmentation threshold, specified in bytes, determines whether data packets will be fragmented and at what size. Frames that are smaller than the specified fragmentation threshold value will not be fragmented. Frames that are larger than the fragmentation threshold will be fragmented into smaller packets and transmitted a piece at a time instead of all at once. The setting must be within the range of 256 to 2346 bytes. It is recommended to use the default value or only minor reductions of this default value.

Protection Mode：Default setting is "None". If set to "CTS-Only" then when protection is turned on and prior to the transmission of an 802.11g frame, the AP sends out a CTS frame (also known as CTS-to-Self) to set the NAV in all the clients so that they will not transmit during the time period of the subsequent data packet from the AP. If set to "RTS-CTS" then the AP sends a RTS frame, waits for the clients CTS frame and then sends the data packet. Setting "RTS-CTS" will allow more robust operation, but at the expense of additional overheads.

RTS/CTS Threshold：If a frame is smaller than the RTS/CTS threshold, it will be sent by the AP without modification. If a frame is larger than the RTS/CTS threshold, then two frames will be sent by the AP. The first frame is an RTS (request to send) frame. After the RTS frame is sent, the AP listens for the corresponding CTS from the target client. Upon reception of the CTS, the AP then sends the data frame. There are trade-offs when considering what value you should set for the RTS/CTS threshold. Smaller values will cause RTS to be sent more often, increasing overheads. However, the more often RTS packets are sent, the sooner the system can recover from collisions. It is recommended to use the default value or only minor reductions of this default value. The value range is from 0 to 2347.

Distance：Target area distance.

IGMP Snooping：AP is a Layer 2 device when it is configured as Switch mode. However, IGMP Snooping implementation on AP is a little bit different than that of standard Layer 2 Switch.

Each Virtual AP (VAP) port is similar to a Layer 2 switch port. With IGMP Snooping enabled in the AP, clients associated to a VAP will only receive multicast packets if there is at least one client joined the multicast group in that VAP. Unlike ordinary IGMP Snooping implementation, where Layer 2 switch converts multicast to unicast and delivers them to devices registered with the multicast group, AP should simply send out the multicast packets from the VAP which has at least one client joined the multicast group. This is done because the wireless media is a broadcast media. It does not need to be sent multiple times when there are more than one registered clients.

When IGMP Snooping is turned on, multicast packets should be dropped at the VAP exit if there is no client from the VAP who has joined the corresponding multicast group.

The IGMP snooping forwarding table (port and multicast MAC address mapping table) should support aging mechanism to age out the entry which has no multicast traffic for a period of time (120 seconds in AP-100).

The default setting of the IGMP Snooping is “Disabled”.

Multicast Traffic：Default setting is "**Enabled** ". If set to "**Enabled**", the system allows multicast traffic in all VAPs. If set to "**Disabled**", all multicast traffic in all VAPs will be dropped.

Enable Optimization Mode：Set the Optimization mode to optimize the performance depending on different deployment environment.

Optimization Mode：There are three modes, default, optimized for throughput and optimized for capacity.

Data Rate Setting

Data Rate：Default setting is “***best***”. The transmission data rate that appears on the drop-down

AP-100 supports “***Multicast Traffic Data Rate Setting***” to transmit all multicast traffic of the 2.4G interface at the configured multicast data rate. The multicast data rate must be set to any of the basic data rates. Default setting is 1 Mbps.

AirFi Setting

AirFi Mode：Enable AirFi mode to get enhanced throughput experience.

AirFi Level：There are four options for AirFi level: Level I, Level II, Level III and Custom. AirFi level I is recommended.

Advanced configuration procedures：

1. Select **Configuration**->**Wireless**->**Radio0(2.4G)**->**Advanced**
2. **AMPDU** selected by default
3. **AMSDU** selected by default
4. **Data Rate** by default it is “best”

5. **Beacon Interval** set beacon interval

6. **Distance** set target area distance

7. **IGMP Snooping** choose IGMP snooping mode if need

8. **Multicast Traffic** allow or block multicast traffic

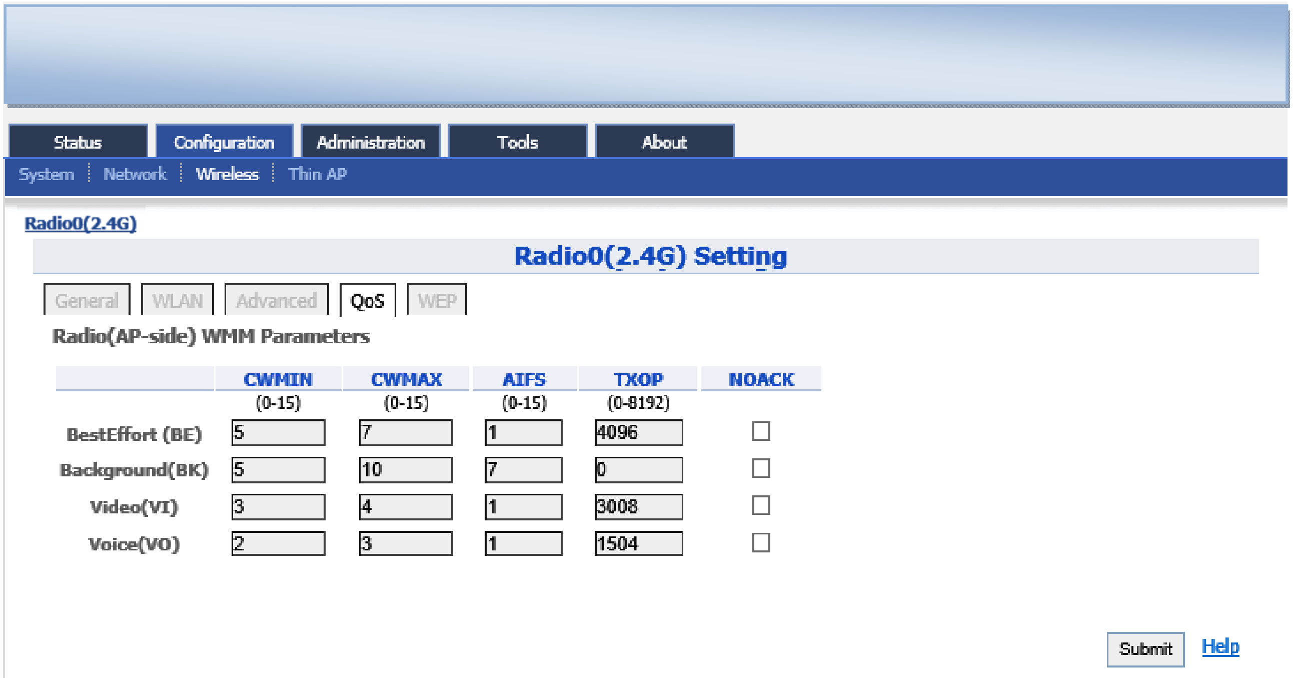
9. **Multicast Data Rate** set multicast data rate

10. Click **Submit**

11. Click **Save&Apply** to apply

Warnings ：*The default setting for advance is recommended.*

6.2.3.1.4. 2.4G Wireless QoS Configuration



Radio(AP-side) WMM Parameters

	CWMIN (0-15)	CWMAX (0-15)	AIFS (0-15)	TXOP (0-8192)	NOACK
BestEffort (BE)	5	7	1	4096	□
Background(BK)	5	10	7	0	□
Video(VI)	3	4	1	3008	□
Voice(VO)	2	3	1	1504	□

Figure 6-41 2.4G Radio QoS Parameters

QoS parameters configuration procedures：

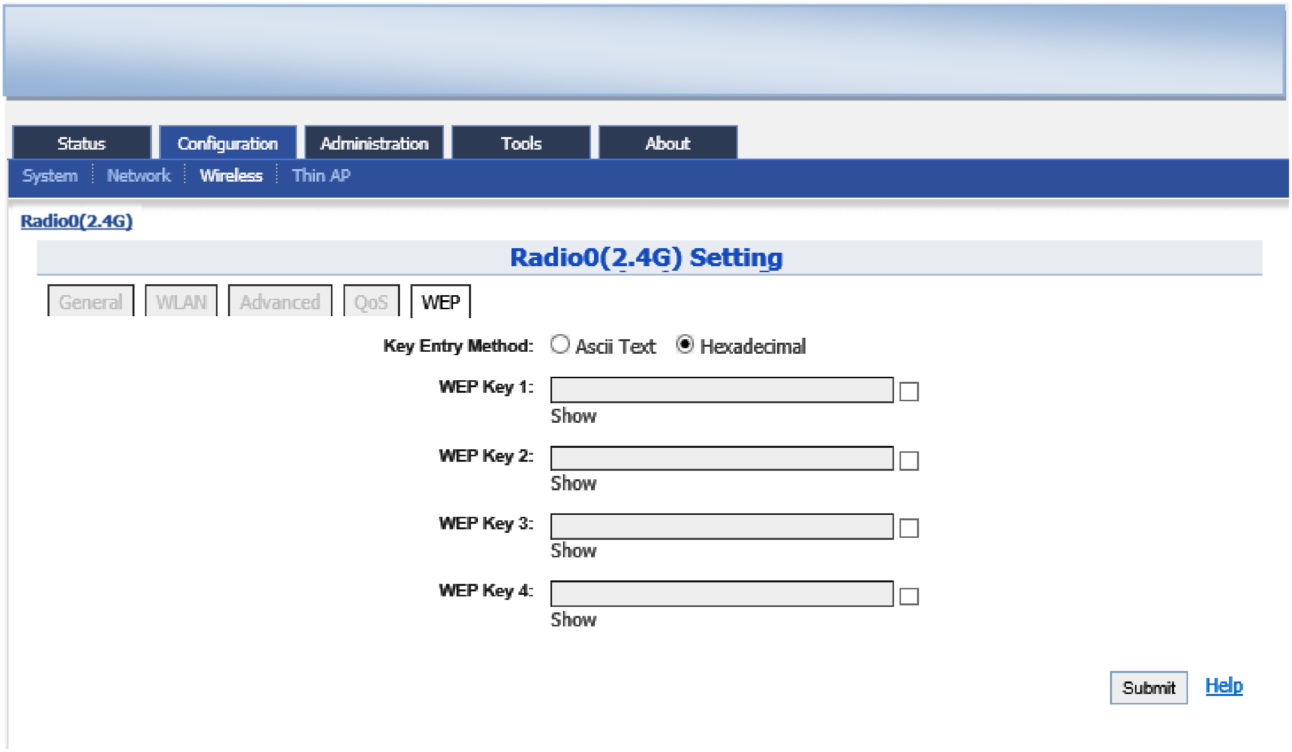
1. Select **Configuration**->**Wireless**->**Radio0(2.4G)**->**QoS**

2. Set values for this Priority-WMM table

3. Click **Submit**

4. Click **Save&Apply** to apply

6.2.3.1.5. 2.4G WEP Key



Key Entry Method: ○ Ascii Text ● Hexadecimal

WEP Key 1: □ Show

WEP Key 2: □ Show

WEP Key 3: □ Show

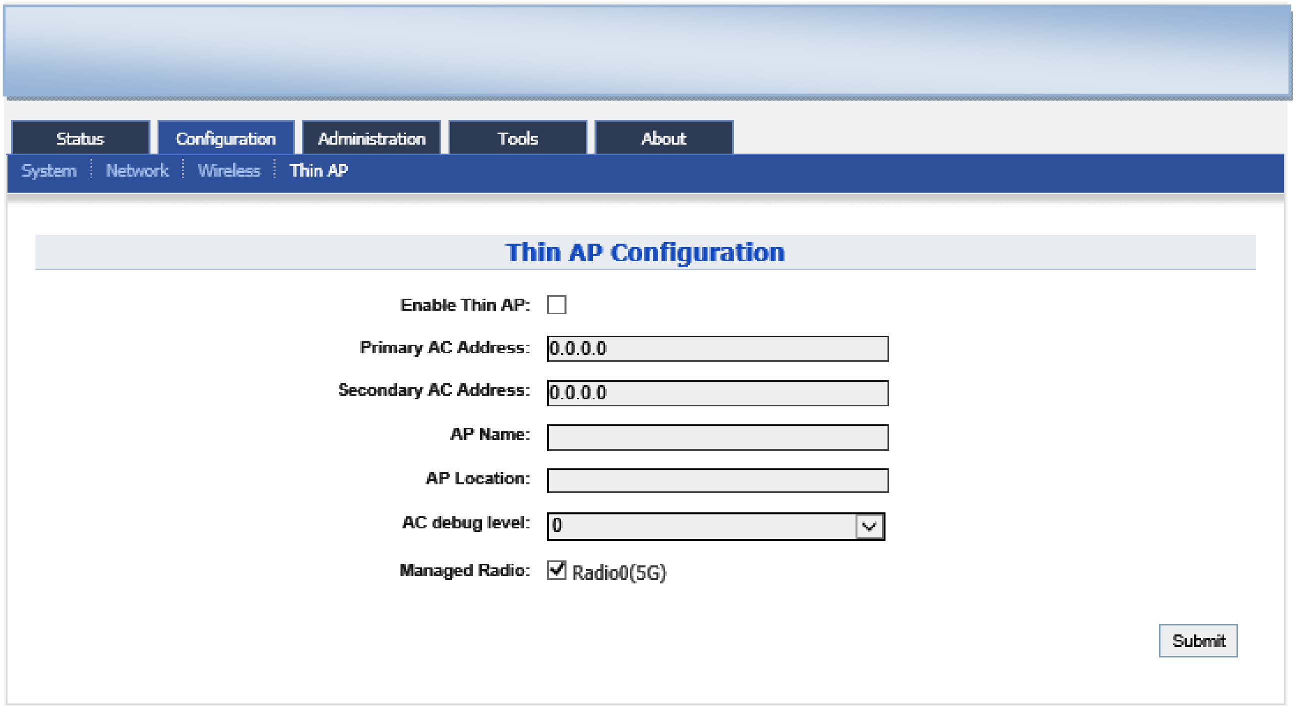
WEP Key 4: □ Show

Figure 6-42 2.4G Radio WEP Key

Procedures：

1. Select **Configuration**->**Wireless**->**Radio0(2.4G)**->**WEP**
2. **Key Entry Method** select the key format
3. Input key phrase in related WEP Key
4. Click **Submit**
5. Click **Save&Apply** to apply

6.2.4. Thin AP Configuration



Thin AP Configuration

Enable Thin AP: □

Primary AC Address: 0.0.0.0

Secondary AC Address: 0.0.0.0

AP Name:

AP Location:

AC debug level: 0

Managed Radio: ☑ Radio0(5G)

Figure 6-43 Thin AP Configurations

Thin AP ：Enable or disable Thin AP mode

AC IP Address： Set static IP address or automatically get AC IP address

AP Name： Thin AP name

AP Location：Thin AP location information

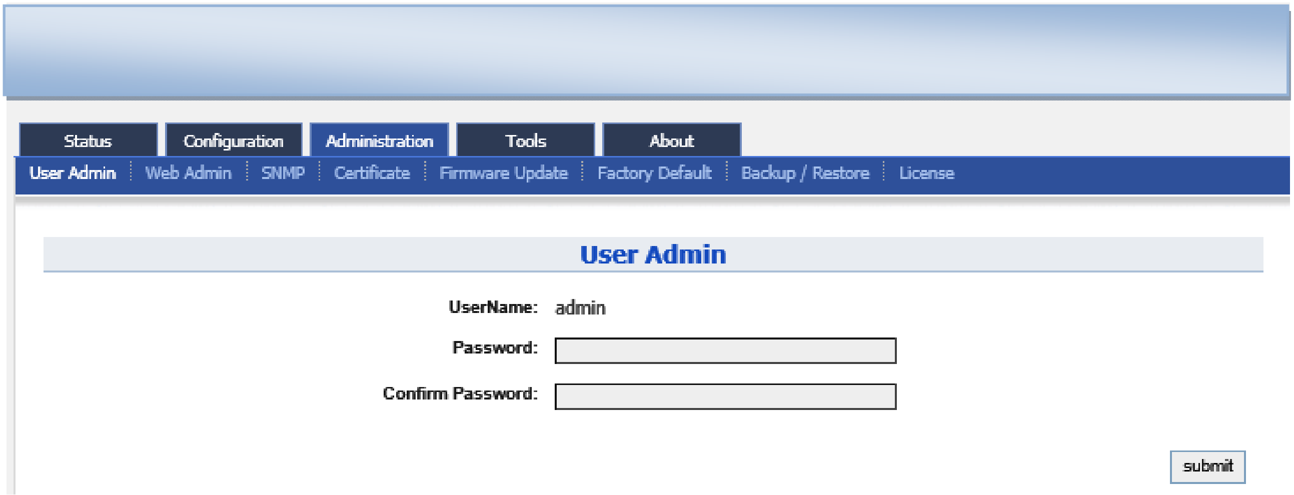
AC debug level：AC debug level, from 0-10

7. Administration Configuration

7.1. Administration General Setting

Please select **Administration** -> User Admin to change login and password.

The user account：admin. Default username is ：**admin**, default password is ：**admin.**



UserName: admin

Password:

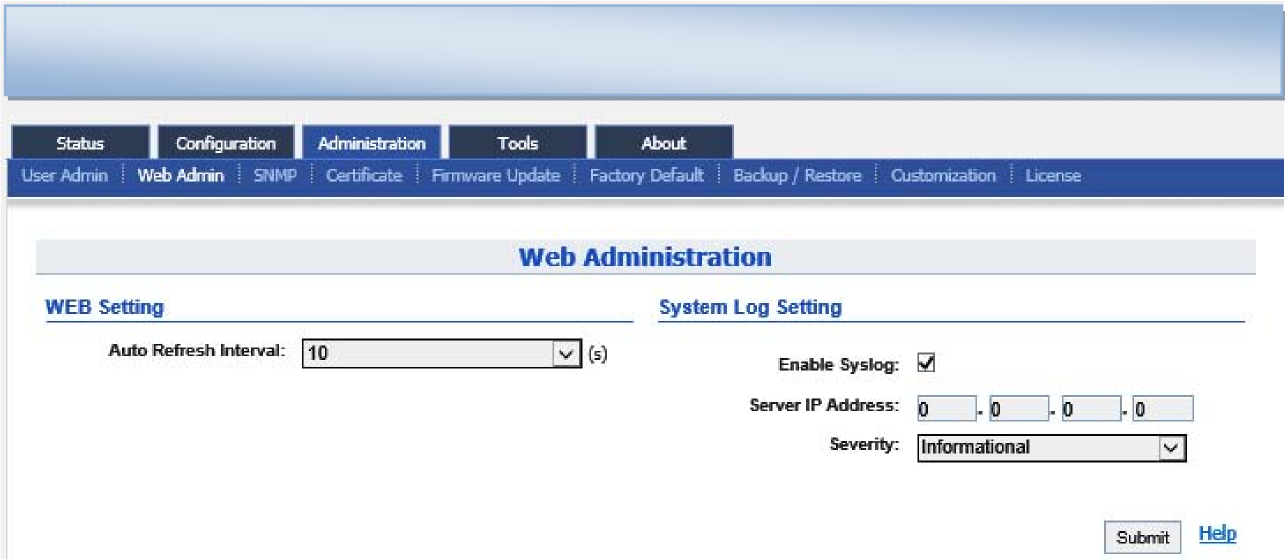
Confirm Password:

Figure 7-1 General Administration

Procedures：

1. Select **Administration** -> **General**,
2. **Password** set password
3. **Confirm Password** input password again to confirm
4. Click **Submit**
5. Click **Save&Apply** to apply

7.2.Web Admin



Web Administration

WEB Setting

Auto Refresh Interval: 10 (s)

System Log Setting

Enable Syslog: ☑

Server IP Address: 0 . 0 . 0 . 0

Severity: Informational

Figure 7-2 WEB Administration

WEB Setting

Auto Refresh Interval：Set auto refresh interval

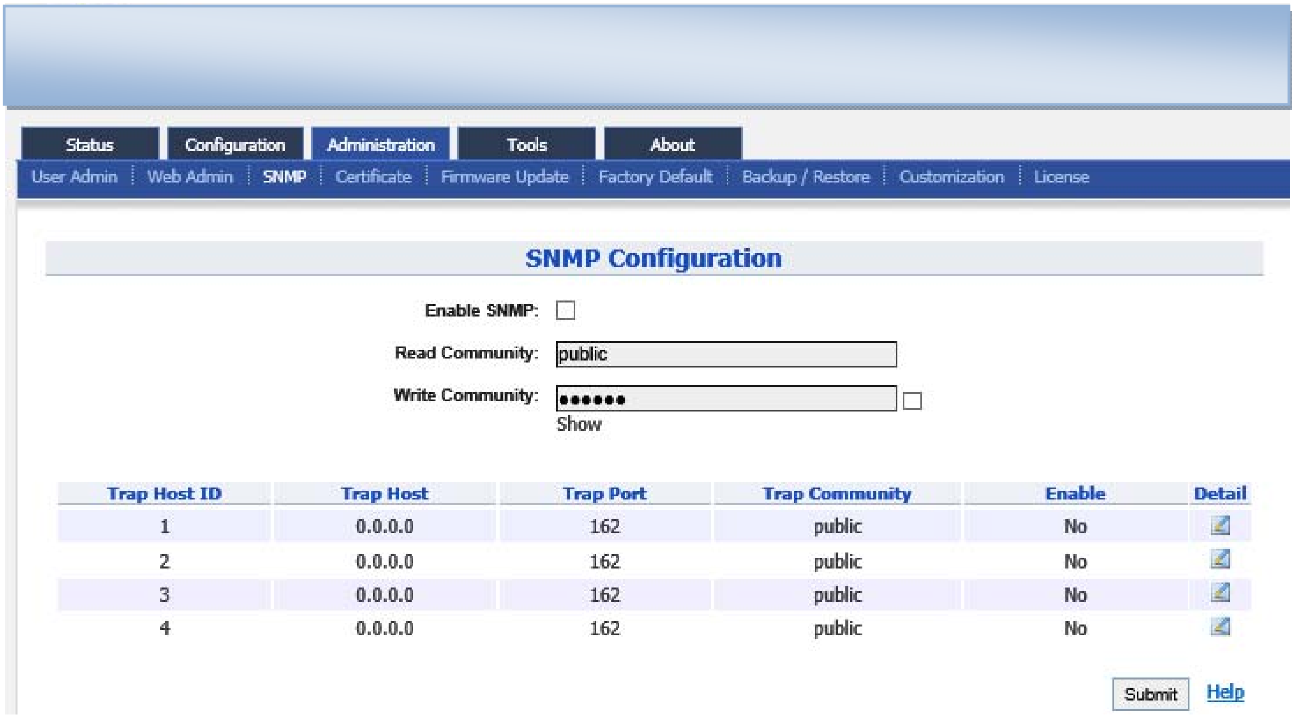
System Log Setting

Enable Syslog：Enable or disable Syslog.

Server IP Address：Type in the IP address of syslog server.

Severity：There are eight kinds of severities: Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug.

7.3. SNMP Setting



SNMP Configuration

Enable SNMP: □

Read Community: public

Write Community: ●●●●●● □ Show

Trap Host ID	Trap Host	Trap Port	Trap Community	Enable	Detail
1	0.0.0.0	162	public	No	✎
2	0.0.0.0	162	public	No	✎
3	0.0.0.0	162	public	No	✎
4	0.0.0.0	162	public	No	✎

Figure 7-3 SNMP Configuration

Enable SNMP: Enable or disable SNMP.

Read Community：SNMP protocol read community; by default it is “public”

Write Community：SNMP protocol write community, by default it is “write”

Show：Show write community phrase

Trap Host ID： SNMP Trap host ID, it supports Max. 4 Trap Host

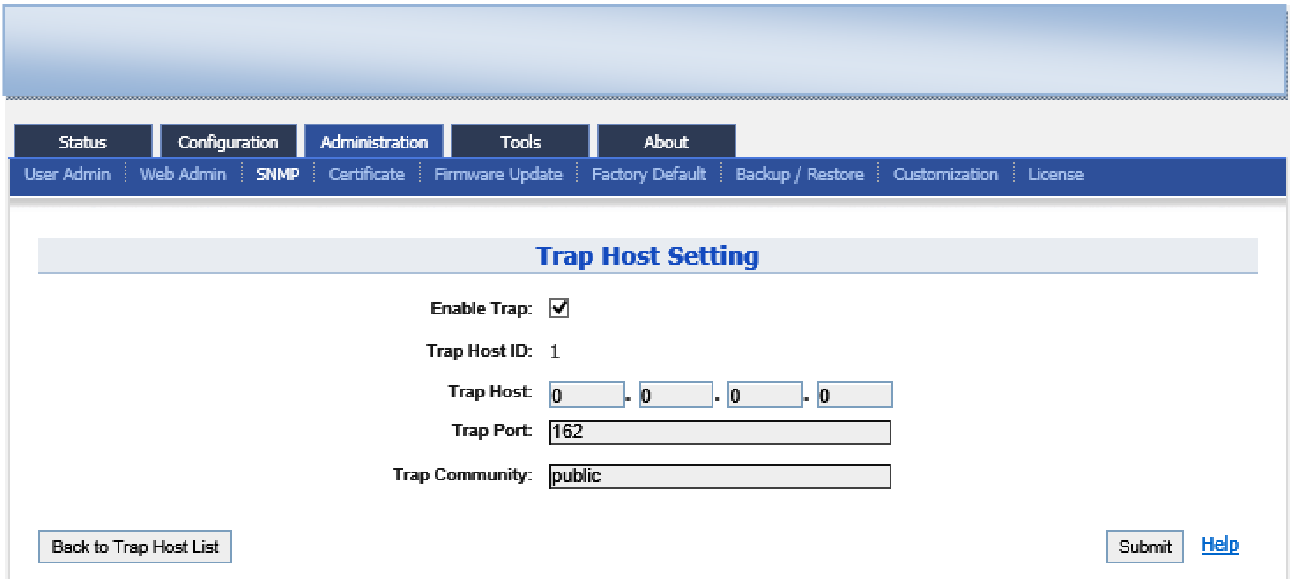
Trap Host： Trap Host IP address

Trap Port： Trap port, by default it is 162

Trap Community：Trap community information

Enable：Trap Host state (enabled or disabled)

Press ✎：To edit Trap Host



Trap Host Setting

Enable Trap: ☑

Trap Host ID: 1

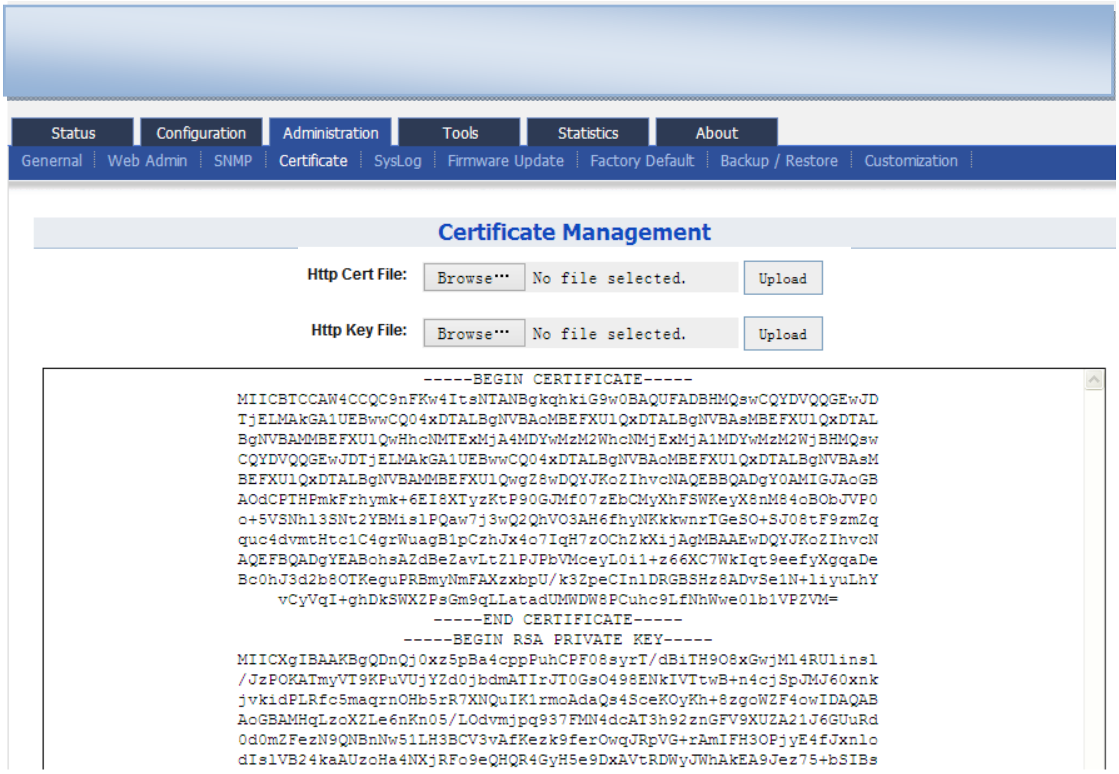
Trap Host: 0 . 0 . 0 . 0

Trap Port: 162

Trap Community: public

Figure 7-4 SNMP Trap Host

7.4. Certificate Management



Certificate Management

Http Cert File: No file selected.

Http Key File: No file selected.

```
-----BEGIN CERTIFICATE-----
MIICBTCCAW4CCQC9nFKw4ItsNTANBgkqhkiG9w0BAQUFADBHMQswCQYDVQQGEwJD
TjELMAkGA1UEBwwCQ04xDTALBgNVBAoMBEFXU1QxDTALBgNVBAsMBEFXU1QxDTAL
BgNVBAMMBEFXU1QwHhcNMTExMjA4MDYwMzM2WhcNMjExMjA1MDYwMzM2WjBHMQsw
CQYDVQQGEwJDTjELMAkGA1UEBwwCQ04xDTALBgNVBAoMBEFXU1QxDTALBgNVBAsM
BEFXU1QxDTALBgNVBAMMBEFXU1QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AOdCPTHPmkFrhymk+6EI8XTyzKtP90GJMf07zEbCMyXhFSWKeyX8nM84oBObJVP0
o+5VSNhl3SNt2YBMislPQaw7j3wQ2QhVO3AH6fhyNKkkwnrTGeSO+SJ08tF9zmZq
quc4dvmtHtc1C4grWuagB1pCzhJx4o7IqH7zOChZkXijAgMBAAEwDQYJKoZIhvcN
AQEFBQADgYEABohsAZdBeZavLtZlPJPbVMceyL0i1+z66XC7WkIqt9eefyXgqaDe
Bc0hJ3d2b8OTKeguPRBmyNmFAXzxbpU/k3ZpeCInlDRGBSHz8ADvSe1N+liyuLhY
    vCyVqI+ghDkSWXZPsGm9qLLatadUMWDW8PCuhc9LfNhWwe0lb1VPZVM=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDnQj0xz5pBa4cppPuhCPF08syrT/dBiTH9O8xGwjMl4RUlinsl
/JzPOKATmyVT9KPuVUjYZd0jbdmATIrJT0GsO498ENkIVTtwB+n4cjSpJMJ60xnk
jvkidPLRfc5maqrnOHb5rR7XNQuIK1rmoAdaQs4SceKOyKh+8zgoWZF4owIDAQAB
AoGBAMHqLzoXZLe6nKn05/LOdvmjpq937FMN4dcAT3h92znGFV9XUZA21J6GUuRd
0d0mZFezN9QNBnNw51LH3BCV3vAfKezk9ferOwqJRpVG+rAmIFH3OPjyE4fJxnlo
dIslVB24kaAUzoHa4NXjRFo9eQHQR4GyH5e9DxAVtRDWyJWhAkEA9Jez75+bSIBs
```

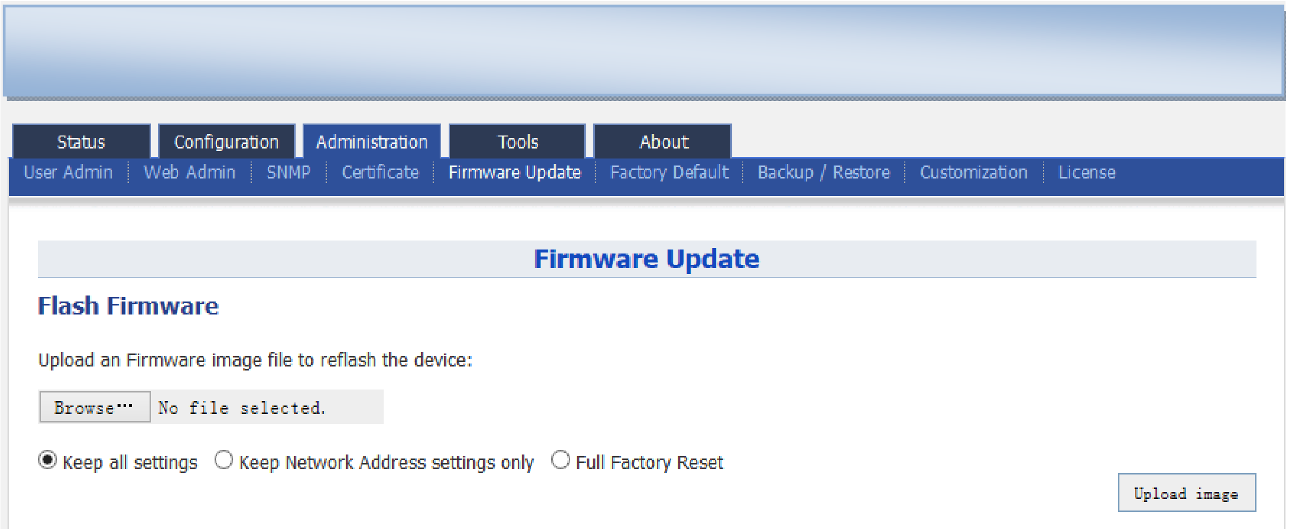
Figure 7-5 Certificate Management

Procedures：

1. Press **Administration** -> **Certificate**
2. **Http Cert File** Click “Browse” to choose Http Certificate file, and then click **Upload**.
3. **Http Key File** click “browse” to choose Http Key file, and then click **Upload**.

7.5. Firmware Update

Go to **Administration** -> **Firmware Update** to update the firmware of AP-100：



Firmware Update

Flash Firmware

Upload an Firmware image file to reflash the device:

No file selected.

● Keep all settings ○ Keep Network Address settings only ○ Full Factory Reset

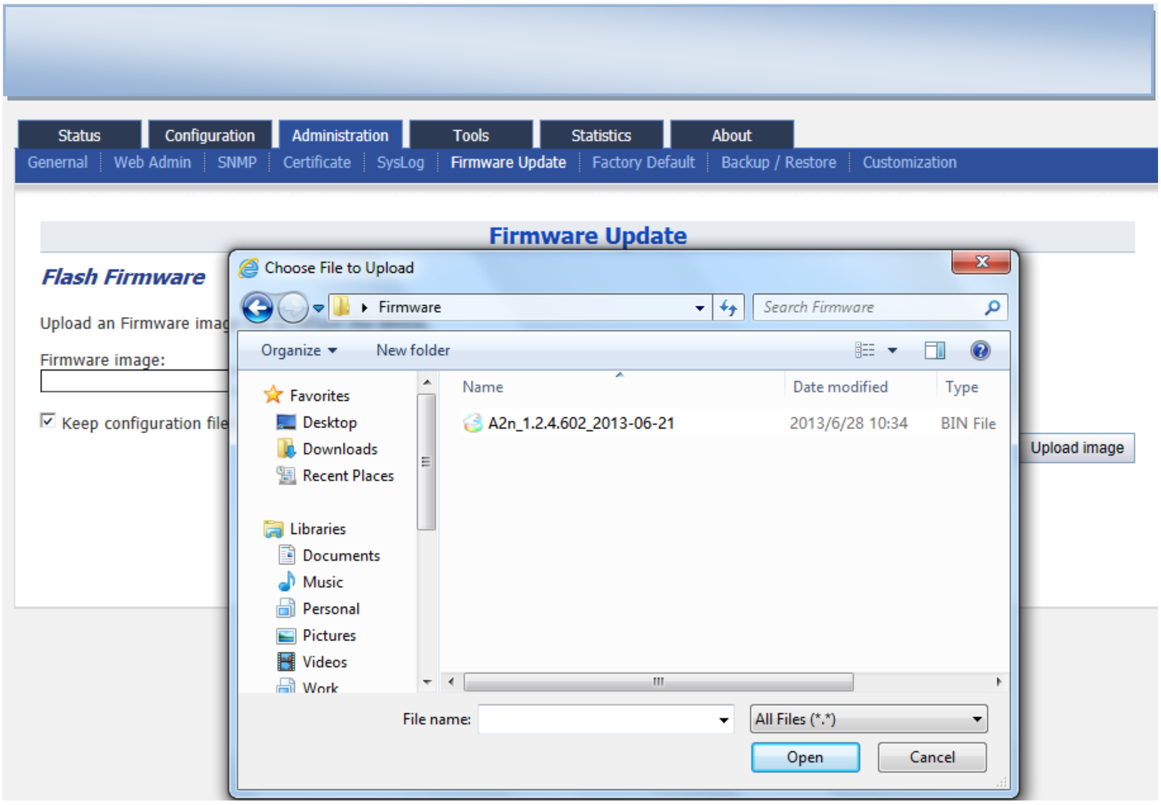
Figure 7-6 Firmware Upgrade

Caution: Do not interrupt the process of firmware update. Please maintain network connection and power supply. AP-100 will not function properly if interruption happened during firmware update.

Procedures:

1. Go to **Aministration** -> **Firmware Update**,

2. Press **Browse**， select the firmware.



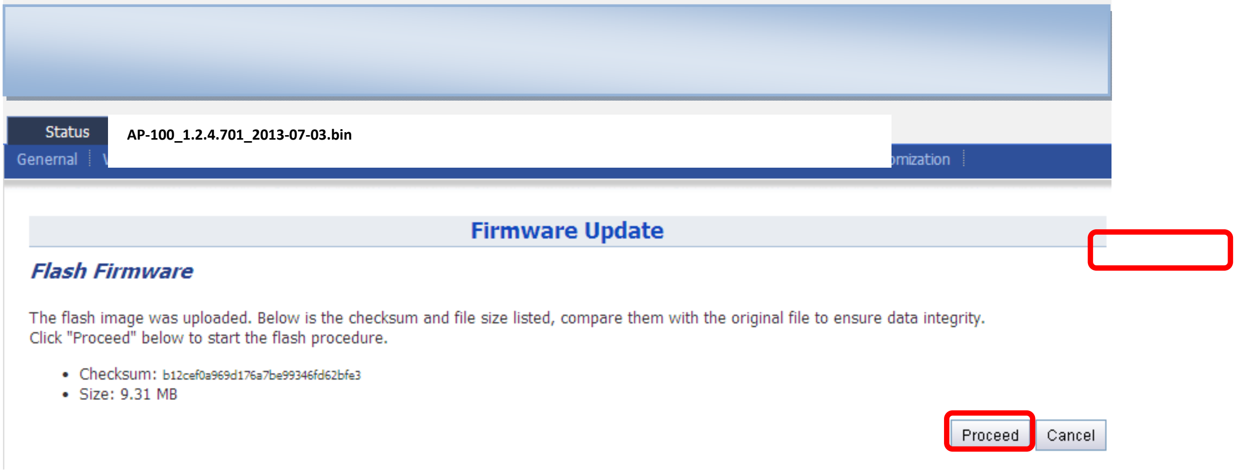
Name	Date modified	Type
A2n_1.2.4.602_2013-06-21	2013/6/28 10:34	BIN File

Figure 7-7 Select Firmware File

4. Press **Upload image** to begin the update， the **keep configuration files** allow user to keep the current configuration after update.

Upload Image to start firmware update

4. AP-100 will run the checksum on the firmware, once it validate the firmware, press proceed to continue,



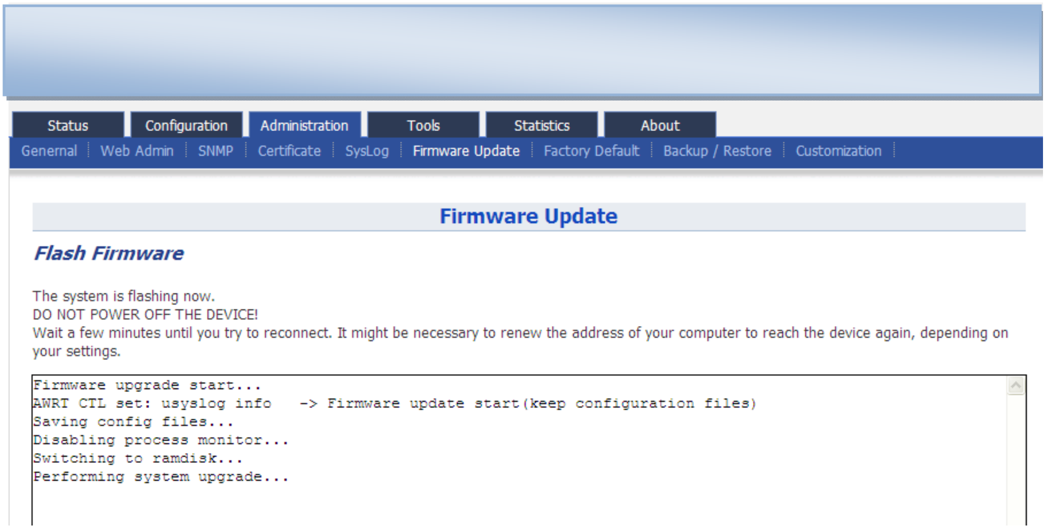
AP-100_1.2.4.701_2013-07-03.bin

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum: b12cef0a969d176a7be99346fd62bfe3
- Size: 9.31 MB

Figure 7-9 Press “Proceed”

5. You will find following notification:



Firmware Update

Flash Firmware

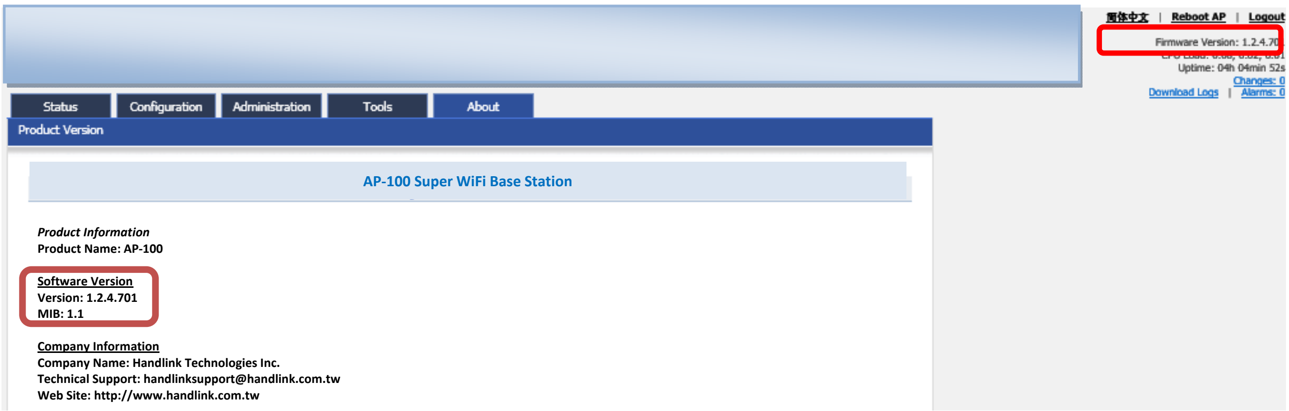
The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

```
Firmware upgrade start...
AWRT CTL set: usyslog info   -> Firmware update start(keep configuration files)
Saving config files...
Disabling process monitor...
Switching to ramdisk...
Performing system upgrade...
```

Figure 7-10 Progress of firmware update

6. AP-100 will reboot and load the Main page after firmware update.

7. Login with username and password， check the firmware version on the top right corner or go to the “About” page.



Firmware Version: 1.2.4.70
Uptime: 04h 04min 52s

AP-100 Super WiFi Base Station

Product Information
Product Name: AP-100

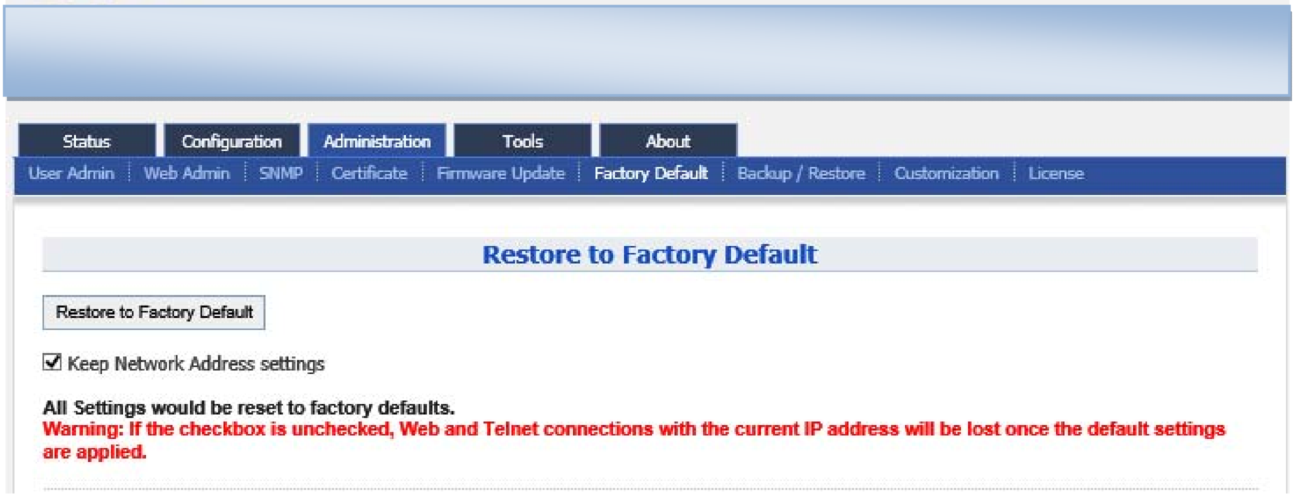
Software Version
Version: 1.2.4.701
MIB: 1.1

Company Information
Company Name: Handlink Technologies Inc.
Technical Support: handlinksupport@handlink.com.tw
Web Site: http://www.handlink.com.tw

Figure 7-11 Information after firmware update

7.6. Reset Back to Factory Default Via User Interface

Under **Administration** -> **Factory Default**, user can reset the AP-100 back to Factory Default Configuration.



☑ Keep Network Address settings

All Settings would be reset to factory defaults.
Warning: If the checkbox is unchecked, Web and Telnet connections with the current IP address will be lost once the default settings are applied.

Figure 7-12 Restore to Factory Default

Procedures:

Reset to Factory Default：Press this button to reset AP-100 to Factory Default Configuration.

Keep Network Address Settings: Select this if user doesn’t wish to reset the IP address configuration to factory default. If this option is not selected, the IP address of AP-100 will be set back to default IP address: 10.59.100.1.

Once restore to factory default configuration, user can login to the AP-100 with the following information:

AP-100 default IP address：10.59.100.1

Username：**admin**

Password：**admin**

7.7. Backup/Restore

AP-100 supports Backup/Restore，Press **Administration** -> **Backup/Restore** to open the configuration interface

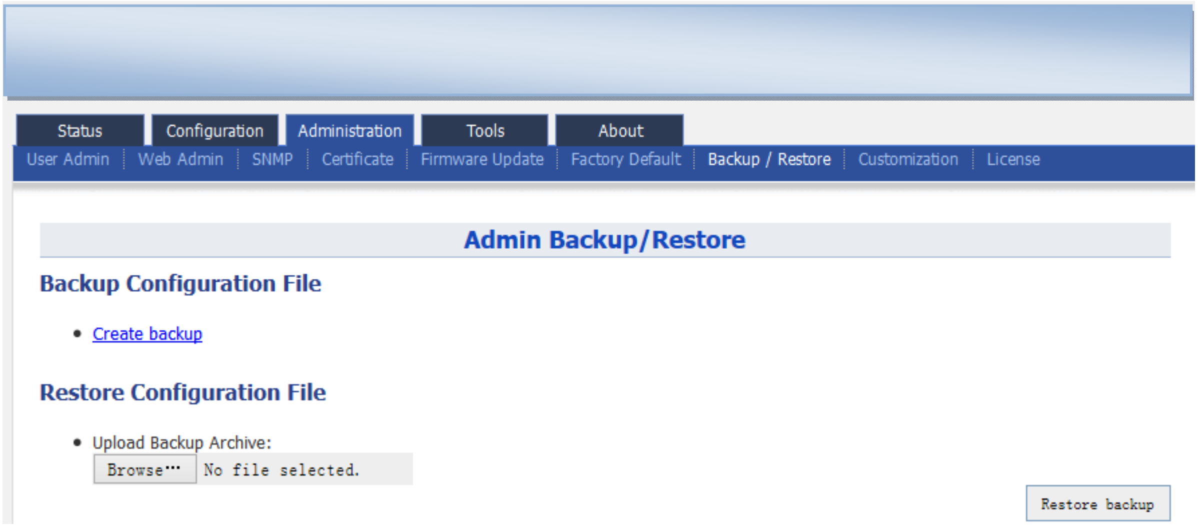


Figure 7-13 AP-100 Backup/Restore

Procedures：

1. Select **Administration**->**Backup/Restore**

2. Press **Create backup** and save it.

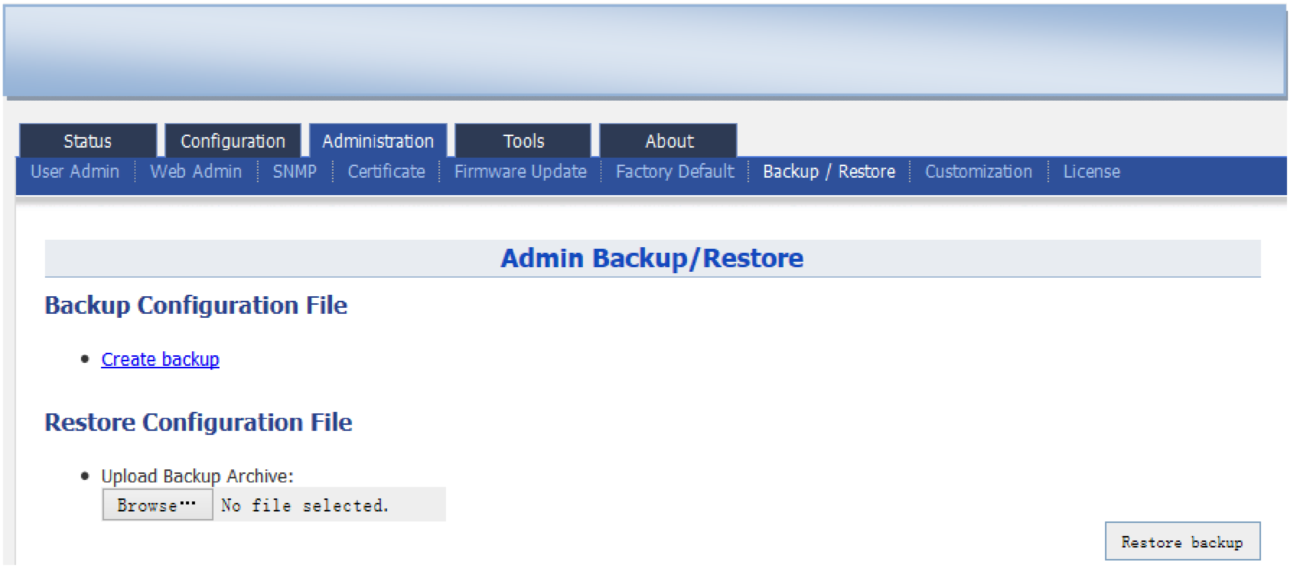
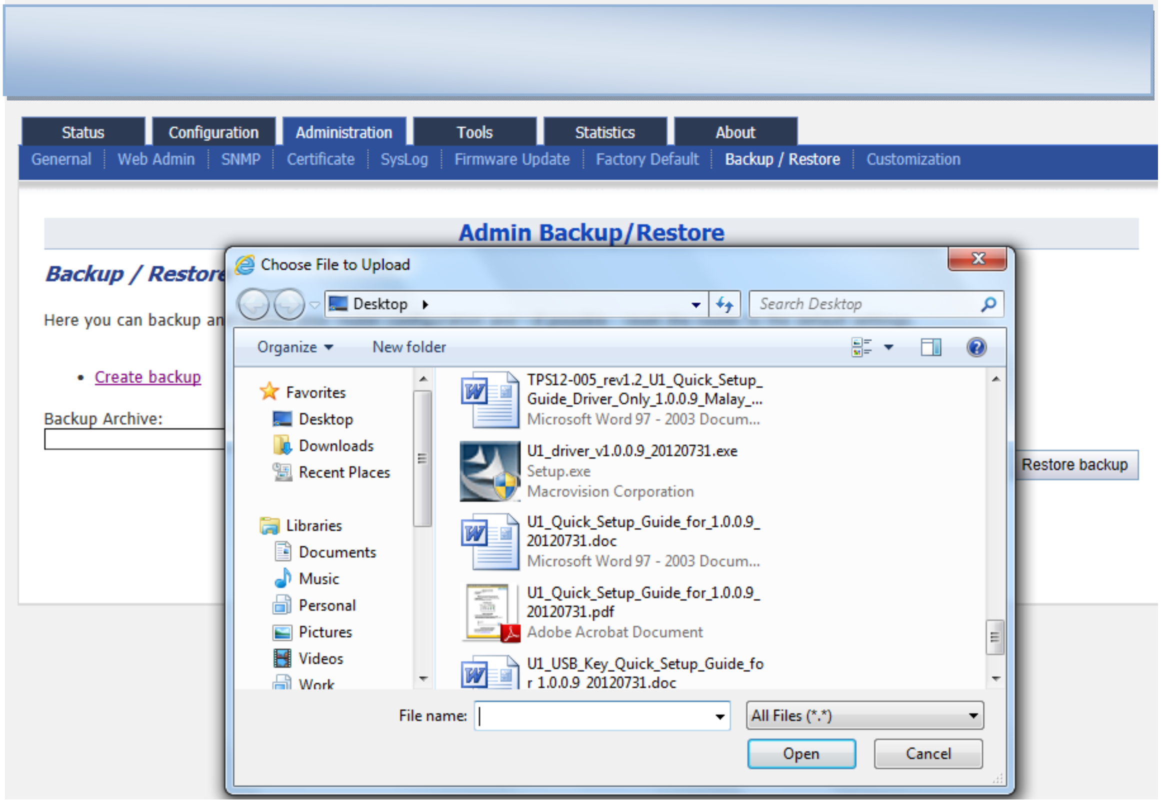


Figure 7-14 AP-100 Backup

3. To restore configuration，Under **Backup Archive**, press **Browse…**，and select the backup file，press **Restore backup** to start restore.



Admin Backup/Restore

Backup / Restore

Here you can backup an

- Create backup

Backup Archive:

TPS12-005_rev1.2_U1_Quick_Setup_Guide_Driver_Only_1.0.0.9_Malay_...
Microsoft Word 97 - 2003 Docum...

U1_driver_v1.0.0.9_20120731.exe
Setup.exe
Macrovision Corporation

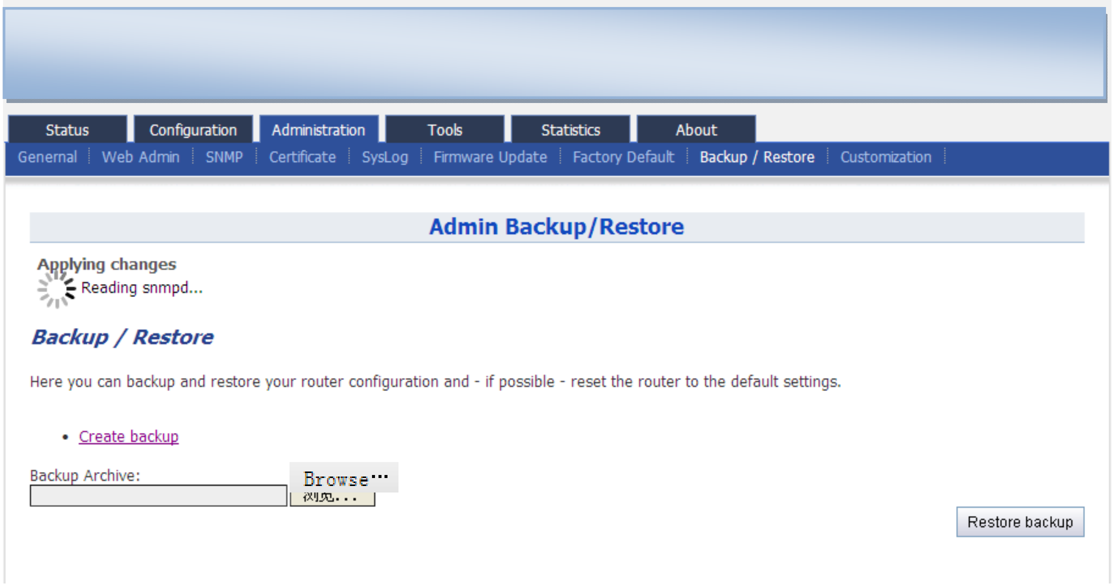
U1_Quick_Setup_Guide_for_1.0.0.9_20120731.doc
Microsoft Word 97 - 2003 Docum...

U1_Quick_Setup_Guide_for_1.0.0.9_20120731.pdf
Adobe Acrobat Document

U1_USB_Key_Quick_Setup_Guide_for 1.0.0.9 20120731.doc

File name:

Figure 7-15 Select the Backup File



Admin Backup/Restore

Applying changes
Reading snmpd...

Backup / Restore

Here you can backup and restore your router configuration and - if possible - reset the router to the default settings.

- Create backup

Backup Archive:

Figure 7-16 Press "Restore backup" to start restore

8. Tools

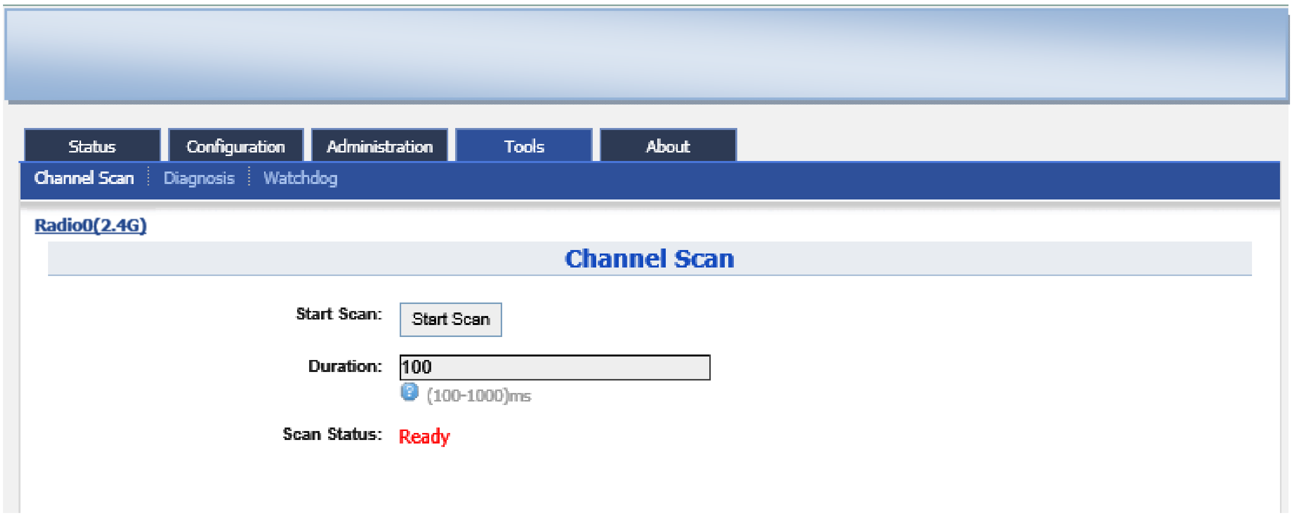
AP-100 provides useful tools，this enable the user to have better radio planning.

8.1. Channel Scan

Through the channel scan tool of AP-100，user is able to know the status of 2.4GHz channels around the AP-100, this provides useful information to the user on how to configure AP-100 and radio planning.

Press on **Tools** -> **Channel Scan** to open the channel scan.

Press **Tools** -> **Channel Scan** to start the channel scan.



Start Scan: Start Scan

Duration: 100

(100-1000)ms

Scan Status: Ready

Figure 8-1 Channel Scan

Details of 2.4G channel scan：

Start Scan ：Press **Start Scan** to start channel scan.

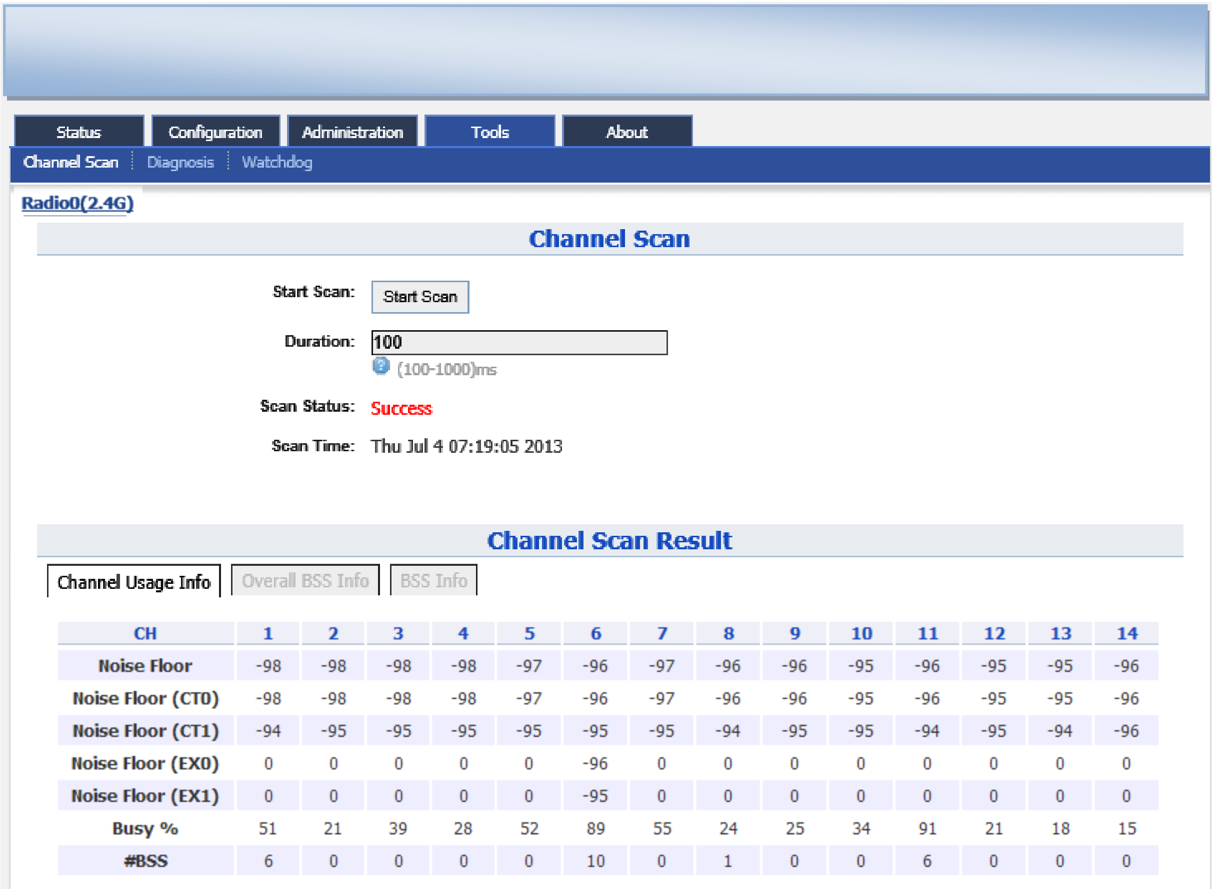
Duration：The switching time of the channel scanning interval，setting range is 100-1000ms，default is 100ms.

Scan Status：AP-100 Base station channel scan status，"Ready" means it can start scan. "Success" means scan finished.

Procedures：

1. In the main menu, select **Tools** -> **Channel Scan**
2. Press **Start Scan**

3. Wait until the scan status change to “**Success**”. The scanning will take approximately 20 seconds



Channel Scan

Start Scan: Start Scan

Duration: 100
(100-1000)ms

Scan Status: Success

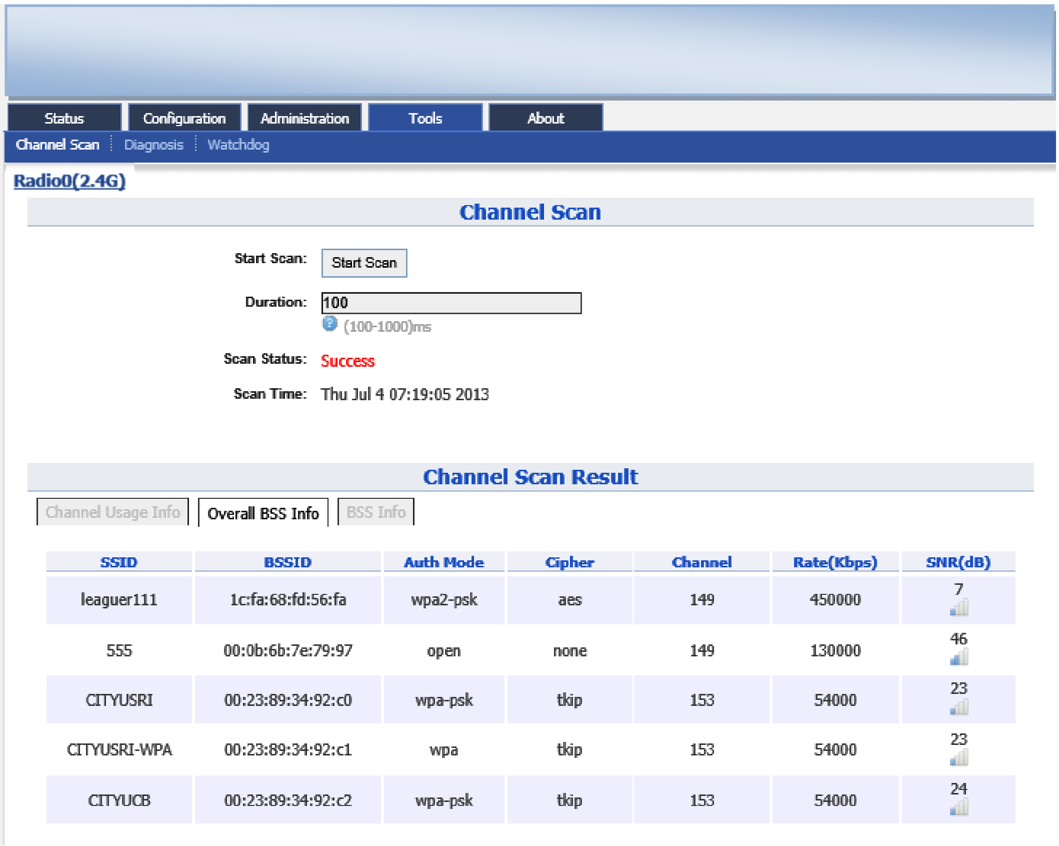
Scan Time: Thu Jul 4 07:19:05 2013

Channel Scan Result

CH	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Noise Floor	-98	-98	-98	-98	-97	-96	-97	-96	-96	-95	-96	-95	-95	-96
Noise Floor (CT0)	-98	-98	-98	-98	-97	-96	-97	-96	-96	-95	-96	-95	-95	-96
Noise Floor (CT1)	-94	-95	-95	-95	-95	-95	-95	-94	-95	-95	-94	-95	-94	-96
Noise Floor (EX0)	0	0	0	0	0	-96	0	0	0	0	0	0	0	0
Noise Floor (EX1)	0	0	0	0	0	-95	0	0	0	0	0	0	0	0
Busy %	51	21	39	28	52	89	55	24	25	34	91	21	18	15
#BSS	6	0	0	0	0	10	0	1	0	0	6	0	0	0

Figure 8-2 2.4G Channel Usage

From the Channel Scan Result，press on **Channel Usage Info** user will see the condition of 2.4G channel around AP-100.Overall BBS Info：



Channel Scan

Start Scan: Start Scan

Duration: 100

Scan Status: Success

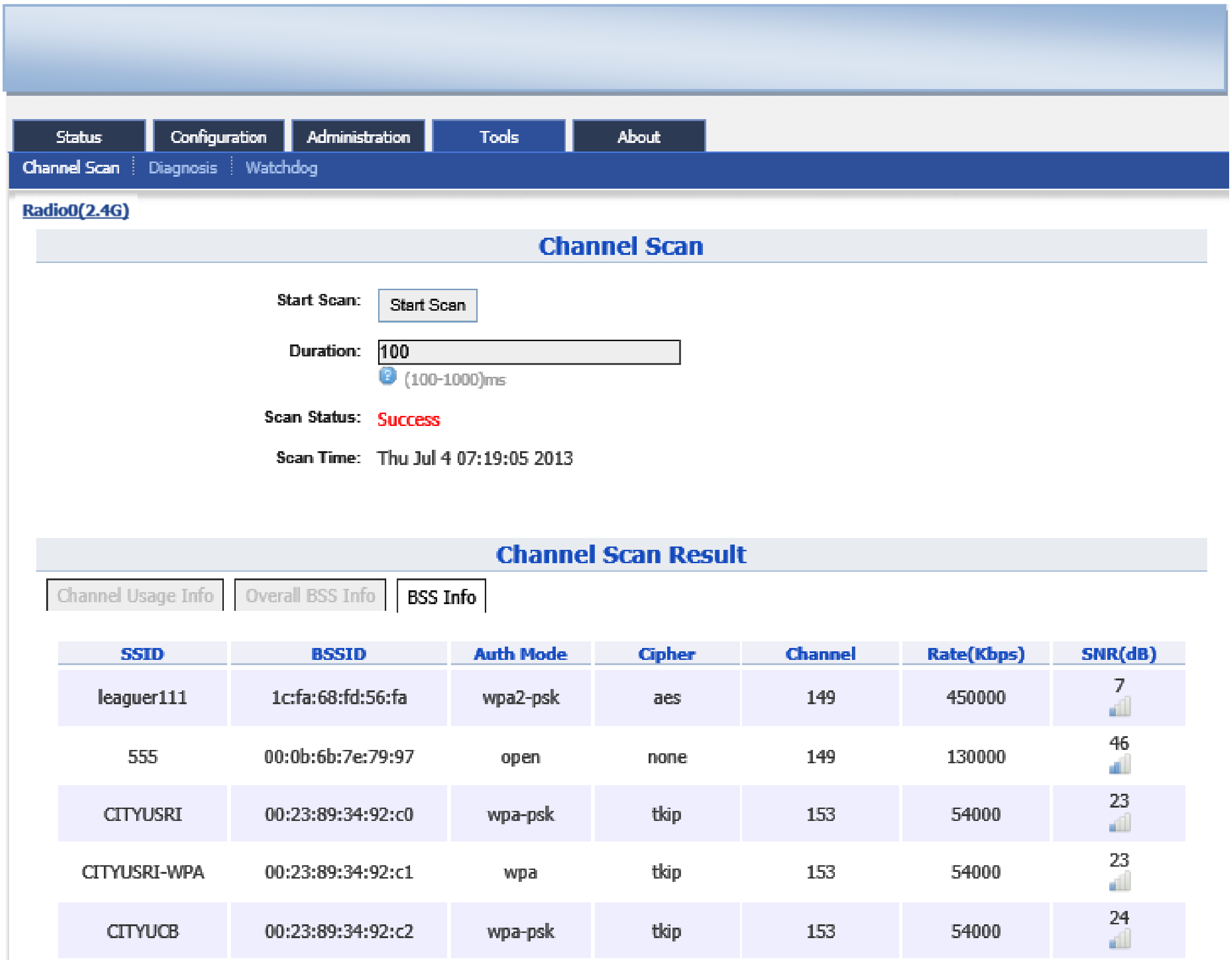
Scan Time: Thu Jul 4 07:19:05 2013

Channel Scan Result

SSID	BSSID	Auth Mode	Cipher	Channel	Rate(Kbps)	SNR(dB)
leaguer111	1c:fa:68:fd:56:fa	wpa2-psk	aes	149	450000	7
555	00:0b:6b:7e:79:97	open	none	149	130000	46
CITYUSRI	00:23:89:34:92:c0	wpa-psk	tkip	153	54000	23
CITYUSRI-WPA	00:23:89:34:92:c1	wpa	tkip	153	54000	23
CITYUCB	00:23:89:34:92:c2	wpa-psk	tkip	153	54000	24

Figure 8-3 2.4G BSS Info

In Channel Scan Result, press **Overall BSS Info** for 2.4G BSS Info, it shows information of BSSID around AP-100. BSS Info：



Channel Scan

Start Scan: Start Scan

Duration: 100

(100-1000)ms

Scan Status: Success

Scan Time: Thu Jul 4 07:19:05 2013

Channel Scan Result

SSID	BSSID	Auth Mode	Cipher	Channel	Rate(Kbps)	SNR(dB)
leaguer111	1c:fa:68:fd:56:fa	wpa2-psk	aes	149	450000	7
555	00:0b:6b:7e:79:97	open	none	149	130000	46
CITYUSRI	00:23:89:34:92:c0	wpa-psk	tkip	153	54000	23
CITYUSRI-WPA	00:23:89:34:92:c1	wpa	tkip	153	54000	23
CITYUCB	00:23:89:34:92:c2	wpa-psk	tkip	153	54000	24

Figure 8-4 BSS information

In Channel Scan Result, press **BSS Info** and it shows information of BSSID from AP-100.

Base on AP-100 2.4G Channel Scan Result，user can select 2.4G channel with lower noise floor, less busy and less SSID as the channel for AP-100’s SSID.

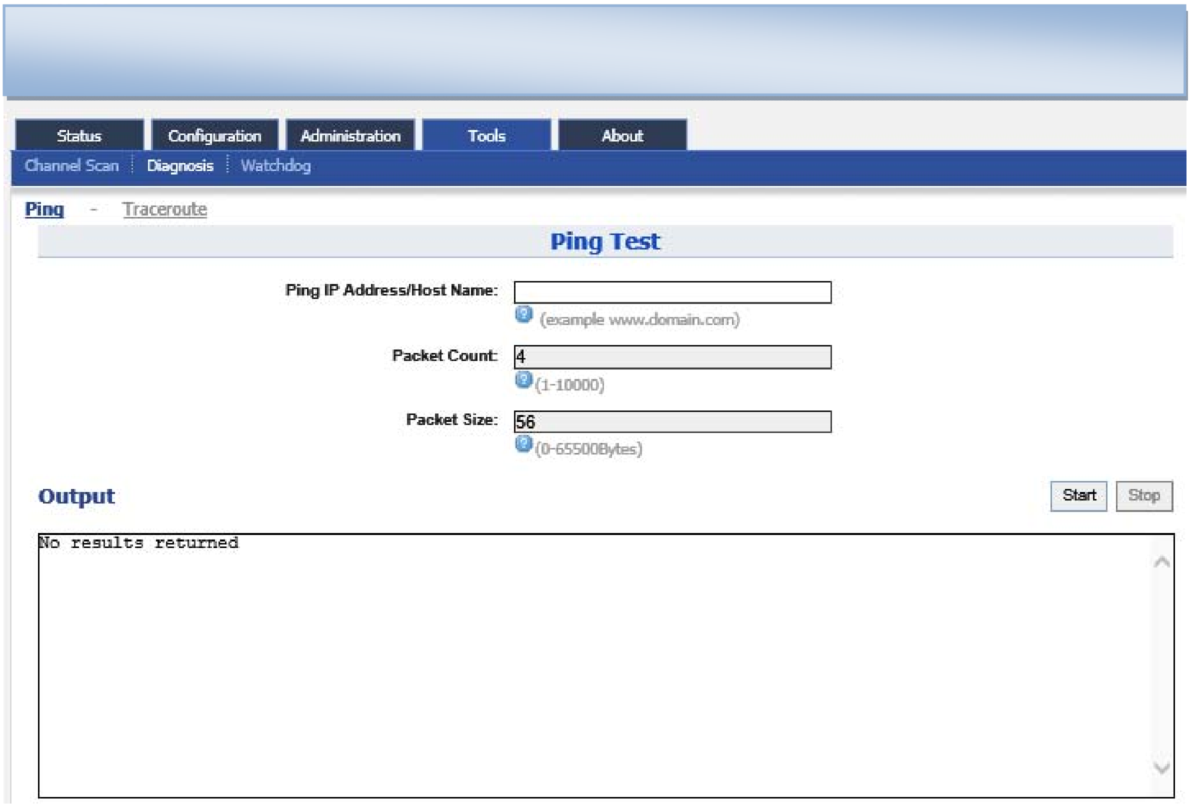
⚠***Caution ：During the process of channel scan, all WiFi clients associated to AP-100 via 2.4G channel will be drop for approximately 15-20 seconds.***

8.2. Diagnosis

Press **Tools** -> **Diagnosis** to start the diagnosis.

8.2.1. Ping to Host

Press **Tools** -> **Diagnosis** -> **Ping** to start the ping.



Ping IP Address/Host Name:
(example www.domain.com)

Packet Count: 4
(1-10000)

Packet Size: 56
(0-65500Bytes)

```
No results returned
```

Figure 8-5 Ping to Host

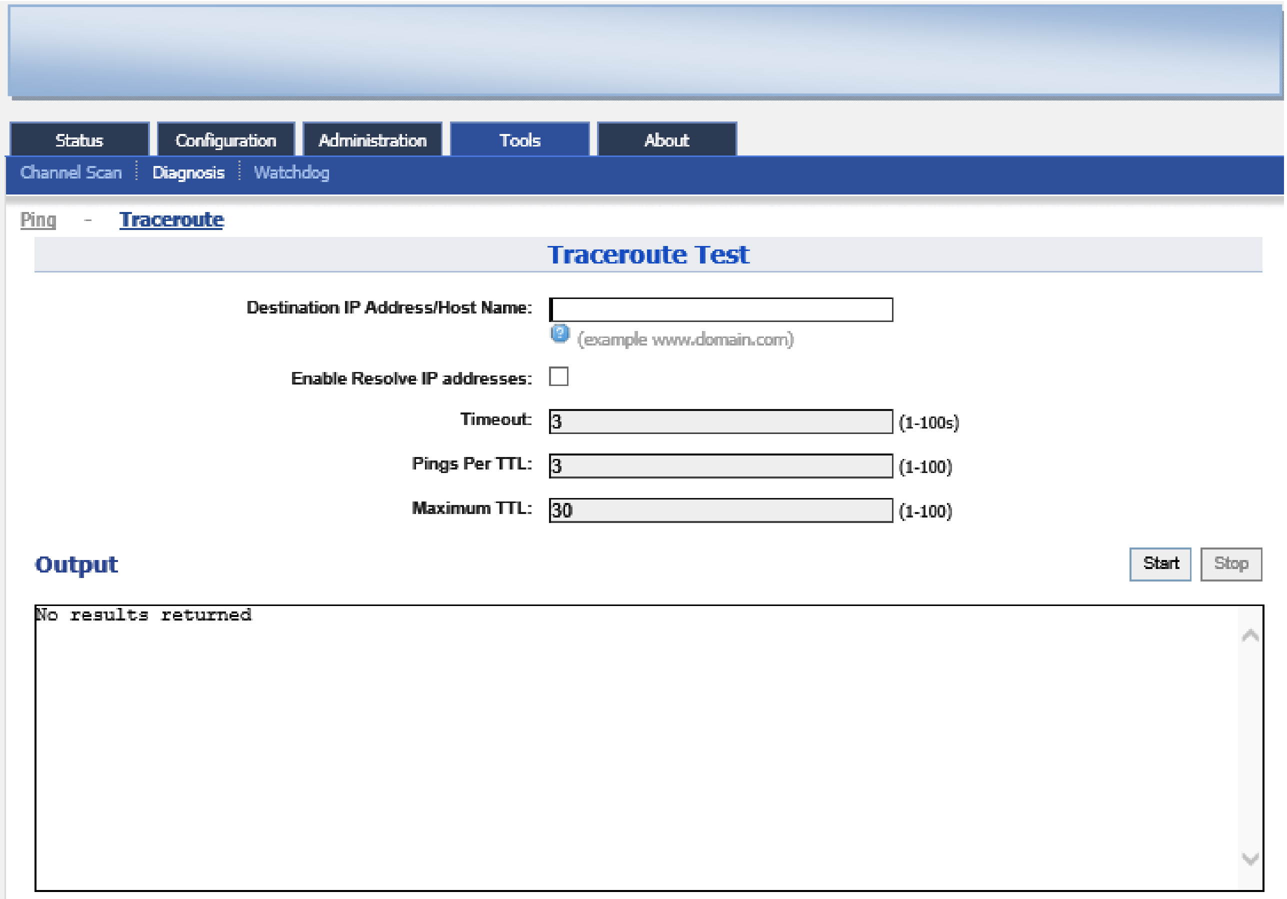
Ping IP Address/Host Name ： Type in the target IP address or target Host name.

Packet Count： The range for Packet count is 1-10000.

Packet Size： Type in the packet size for ping.

8.2.2. Traceroute to Host

Press **Tools** -> **Diagnosis** -> **Traceroute** to start the trace.



Traceroute Test

Destination IP Address/Host Name:
(example www.domain.com)

Enable Resolve IP addresses: □

Timeout: 3 (1-100s)

Pings Per TTL: 3 (1-100)

Maximum TTL: 30 (1-100)

Output

```
No results returned
```

Figure 8-6 Traceroute

Destination IP Address/Host Name ：Type in the target IP address or target Host name.

Enable Resolve IP Address：Enable or disable IP address resolve.

Timeout：Type in the timeout value.

Ping Per TTL：Type in the TTL value for ping.

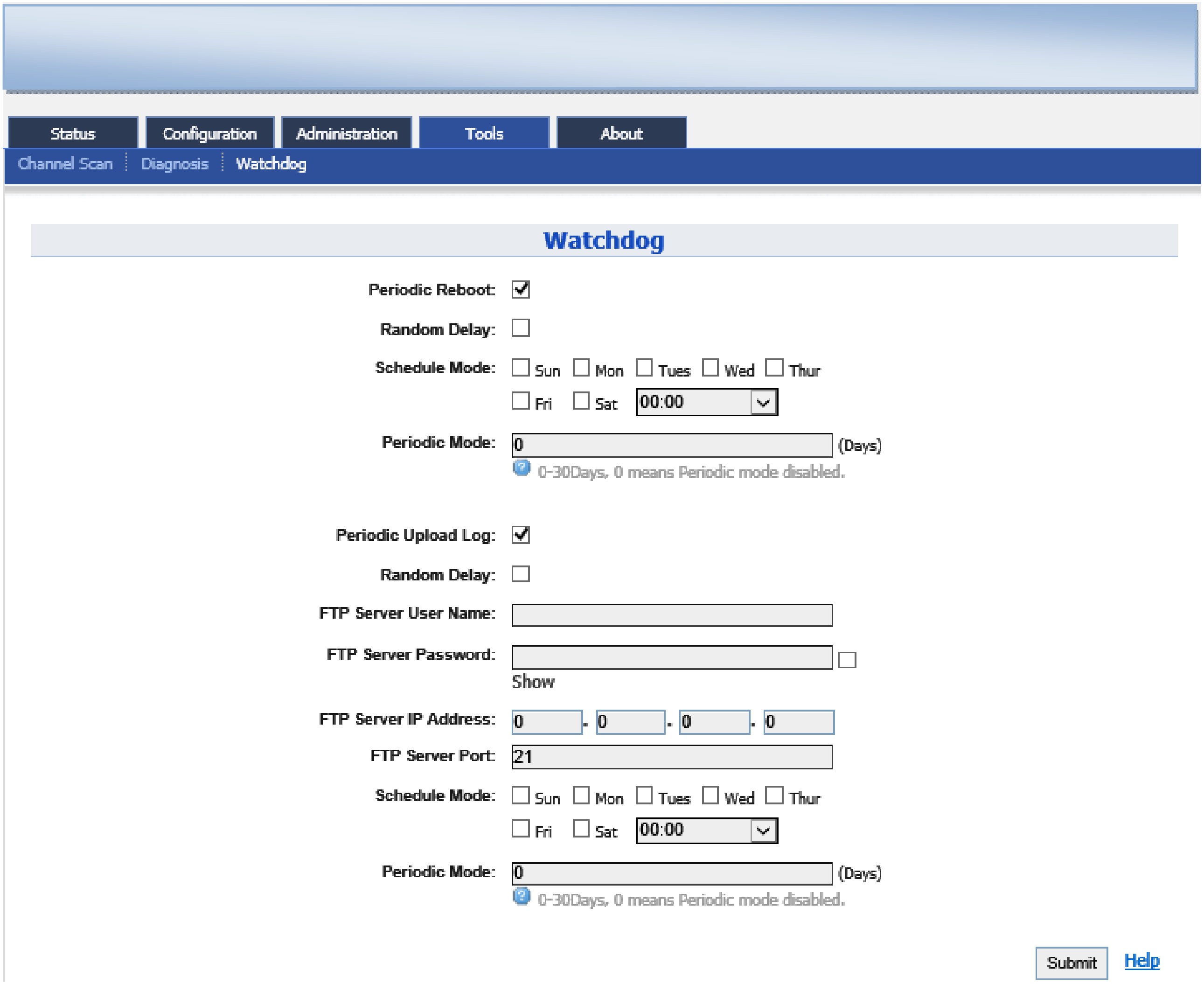
Maximum TTL：Type in the maximum TTL value for ping.

8.3. Watchdog

Press **Tools** -> **Watchdog** to start the watchdog. Watchdog is for periodic reboot setting and periodic upload log setting.

Periodic reboot function can make the unit reboot in the specified time while it is enabled.

Periodic upload log function can make the unit upload the log to the ftp server in the specified time while it is enabled.



Watchdog

Periodic Reboot: ☑

Random Delay: □

Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Days)
0-30Days, 0 means Periodic mode disabled.

Periodic Upload Log: ☑

Random Delay: □

FTP Server User Name:

FTP Server Password: □ Show

FTP Server IP Address: 0 . 0 . 0 . 0

FTP Server Port: 21

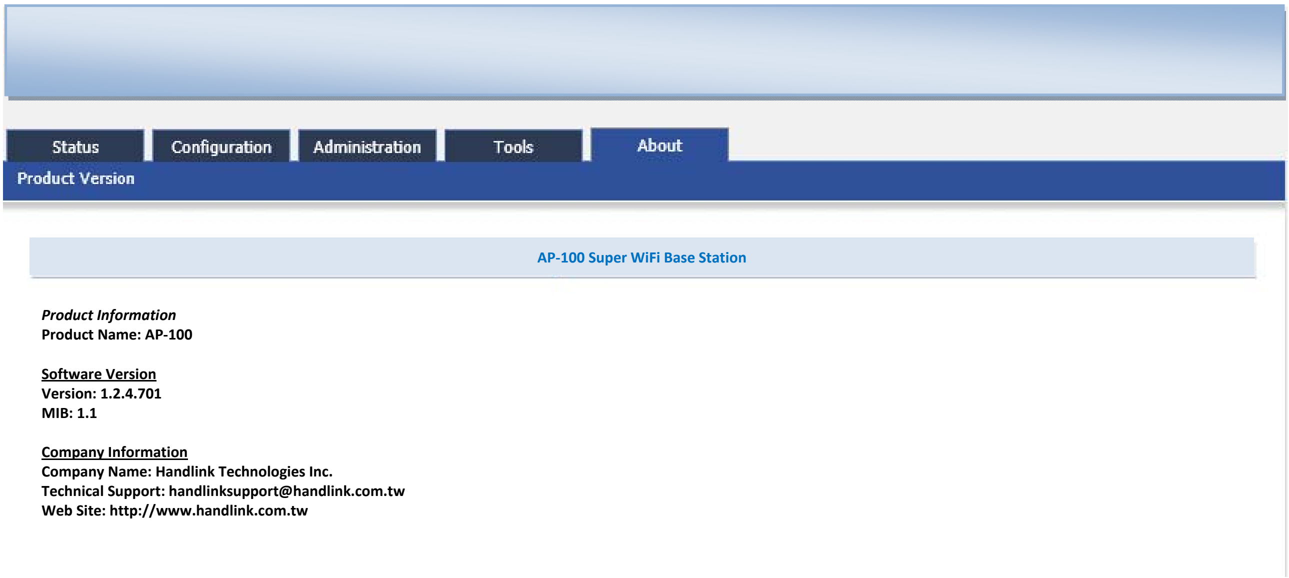
Schedule Mode: □ Sun □ Mon □ Tues □ Wed □ Thur □ Fri □ Sat 00:00

Periodic Mode: 0 (Days)
0-30Days, 0 means Periodic mode disabled.

Figure 8-7 Watchdog Setting

9. AP-100 Information

The “About” in the web layout shows product information



AP-100 Super WiFi Base Station

Product Information
Product Name: AP-100

Software Version
Version: 1.2.4.701
MIB: 1.1

Company Information
Company Name: Handlink Technologies Inc.
Technical Support: handlinksupport@handlink.com.tw
Web Site: http://www.handlink.com.tw

Figure 9-1 AP-100“About”

Details of AP-100 Information：

Production Information: This shows the name, code, serial number, product mode, supported power supply and etc.

Software Version: Display the version of firmware and MIB.

Company Information： Display information of Handlink