ZA-4000

User's Manual

V1.2.17

Copyright

About the manual

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

The following typographical conventions are used in this purpose:

Notice:

λ This indicates an important Note.

Warning:

λ This indicates a warning or caution.

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

Content

Content of Figure

Content of Table

Chapter 1 Introduction

Product Introduction

ZA4000 works at 5GHz, compatible with 802.11a standard designed as CPE and WDS. With the high throughput and long-distance transmission, it is the appropriate solution for Carriers, Service Providers and Enterprises. As outdoor remote client, ZA4000 can make users easily build up broadband access system.

The new features and benefits are: support POE (power over Ethernet), support test-link, use this utility, you can place the antenna in the best place. Fully compliant with IEEE802.11a standard, The CPE provides powerful features.

Appearance of Product

Figure 1 ZA4000

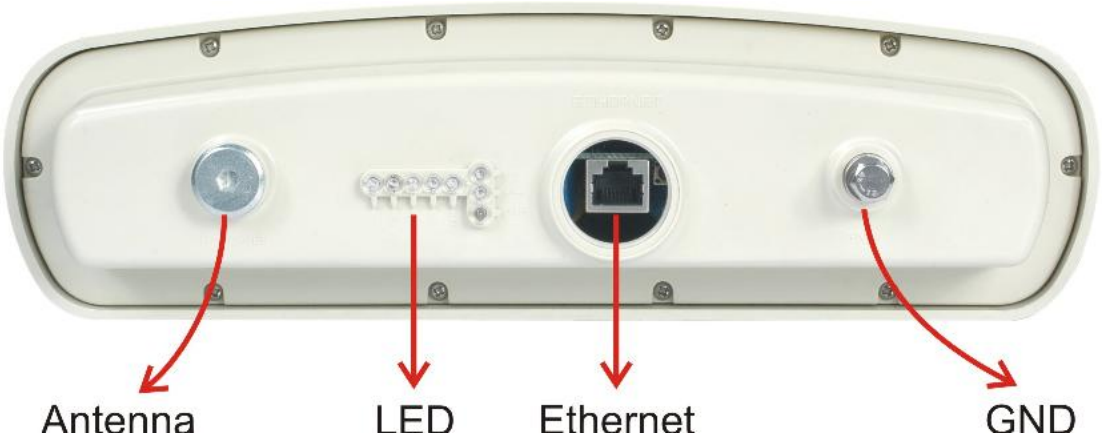


Figure 2 ZA4000 ports

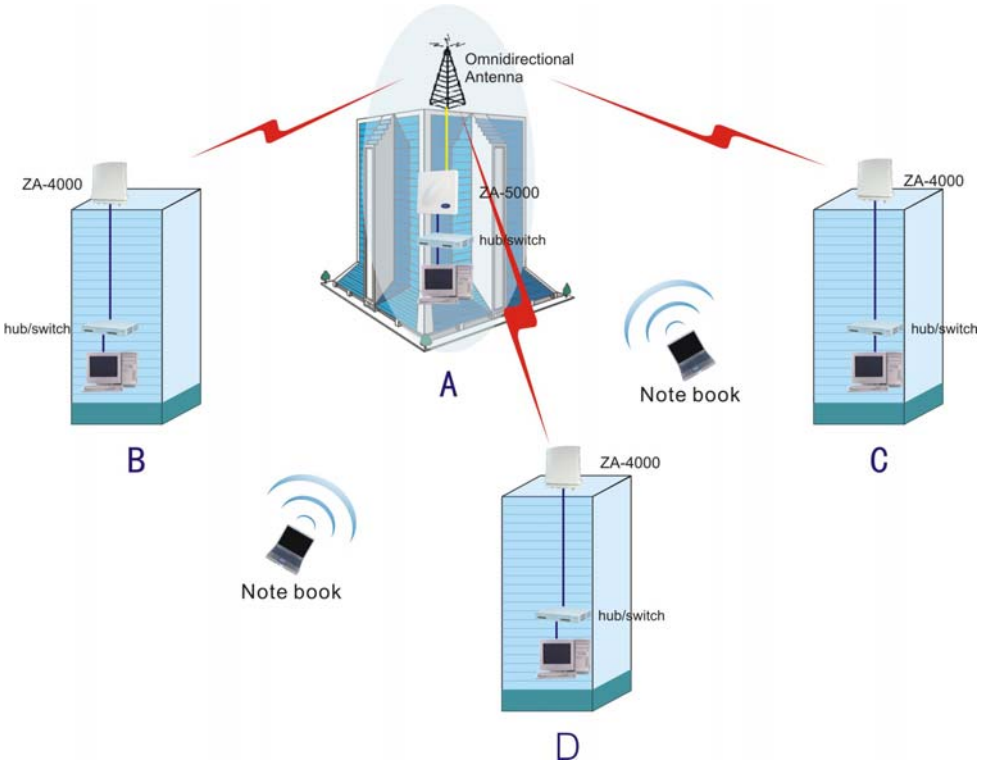
Features and Benefits

- λ Features 54Mbps data rate by incorporating OFDM technology
- λ Fully IEEE 802.11a compatible
- λ Technique operating in 5GHz band
- λ MAC address control (CPE)
- λ Easy to install and friendly to user, just plug and play
- λ Provides Web-based configuration utility
- λ Tight design with lightweight, compact size, and low power consumption
- λ Support PoE(Power over Ethernet)
- λ Waterproof and can place into outdoor directly
- λ Test-link utility, help you place your antenna at the best place
- λ LED function: The LED has two types: signal light and indicator light. The signal light is used to show the intensity of the signal. It has five lights and it lights from left to right. The number of the lighted lights is as following:

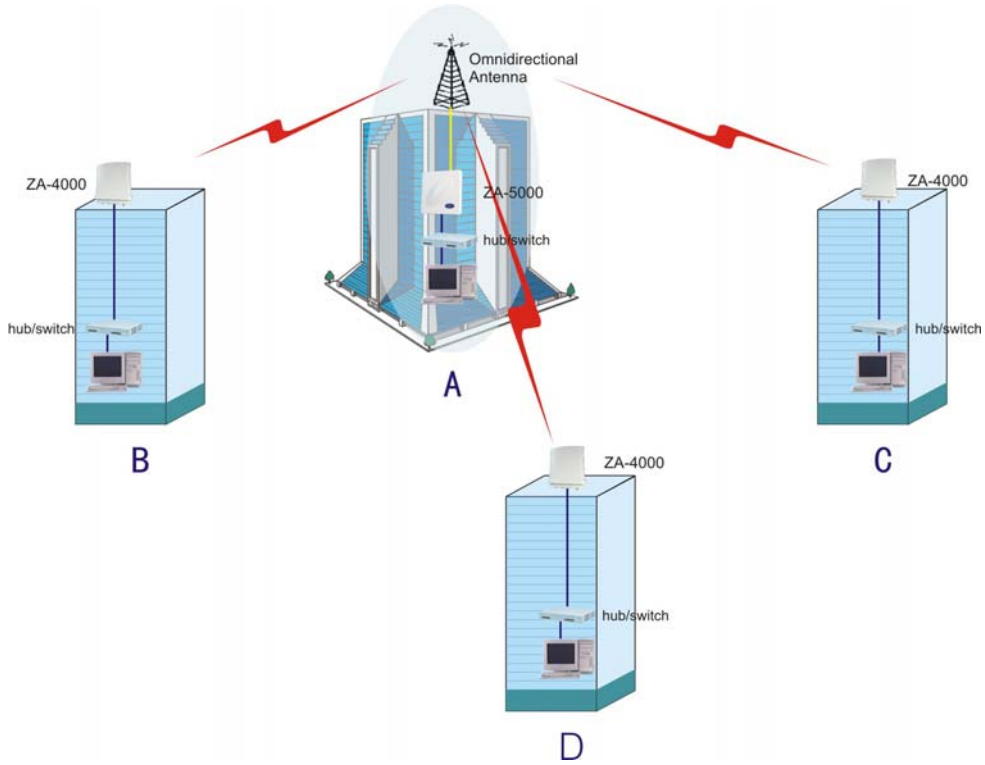
The number of LED	Signal intensity
0	-92 <= dBm < -87
1	-87 <= dBm < -67
2	-67 <= dBm < -52
3	-52 <= dBm < -47
4	-47 <= dBm < -45
5	-45 <= dBm <= 10

The indicator light is used to show the status of power, wireless and wired information. The power light is always lighted. The wireless and wired light will twinkle when there is data flowing.

Network Construct



Point to Multi-point Overcast Application



Point to Multi-point Application

Application

- λ Remote Access to Corporate Network Information
- λ E-mail, file transfer and terminal emulation.
- λ Difficult-to-Wire Environments
- λ Historical or old buildings, asbestos installations, and open area where wiring is difficult to deploy.
- λ Frequently Changing Environments
- λ Retailers, manufacturers and those who frequently rearrange the workplace and change location.
- λ Temporary LANs for Special Projects or Peak Time
- λ Trade shows, exhibitions and construction sites where a temporary network will be practical; Retailers, airline and shipping companies need additional workstations during peak period; Auditors requiring workgroups at customer sites.
- λ Access to Database for Mobile Workers
- λ Doctors, nurses, retailers, accessing their database while being mobile in the hospital, retail store or office campus.
- λ High Security Connection
- λ The secure wireless network can be installed quickly and provide flexibility

Chapter 2 Hardware Installation

System Requirement

Installation of the Outdoor CPE requires:

- A RJ-45 connector supports the transfer rate of 10/100Mbps data.
- A PC of install the following WEB browsers, Microsoft Internet Explorer 6 and fix Service Pack 1 or the newer patch and wrapped up Q323308.
- One 48V, 1A Power Adapter, in order to power supply of the CPE.

Product Kit

Before installation, make sure that you the following items:

- ZA-4000 ×1
- Product CD ×1
- Power Adapter ×1
- DC Injector ×1
- Power Cable ×1
- Fixed settings ×1
- Installation Guide ×1

If any of the above items are not included or damaged, please contact your local dealer for support.

Hardware Installation

Take the following steps to set up the CPE:

1. Hardware equipment

2. Make the RJ-45 connector:

white orange｜orange　white green｜blue　white blue｜green　white brown｜brown

3. Plug water-joint into the CPE

4. Close the water-joint

Warning：

- Please confirm ground connection of the CPE.
- Please don't insert and pull out the Ethernet cable with electricity.

Chapter 3 Basic configuration

Default Settings

When use this product for the first time, the default settings as the below diagram will be seen, or restore it refer to **Restore to Factory**.

Diagram 1Default Settings

Options	Default Value
User Name	admin
password	password
System Name	STAxxxxxx（xxxxxx indicates the last 6 of MAC address of STA）
Country/Region	China
Configure Device as a	Bridge
Spanning Tree	Enable
IP Address	192.168.0.228
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary/Secondary DNS Server	0.0.0.0
Time Server	N/A
Time Server Port	123
Time Zone	(GMT): Dublin, Edinburgh, Lisbon, London
Adjust for Daylight Saving Time	OFF
Operation Mode	CPE
Wireless Network Name	Wireless
BSSID	00:00:00:00:00:00
Data Rate	Best
Output Power	Full
RTS Threshold	2346
Fragmentation	2346
Space from AP	10000
Enable Super-A Mode	No
Enable TDM	No
Authentication Type	Open System
Encryption Strength	None
SSH	Enable

SNMP	Enable
Trap Server IP	0.0.0.0
Read Community	public
Write Community	private
IP and MAC Access Control	Disable
SysLog	OFF

Using the Web Management

Follow the steps below to configure an CPE operating setting using the WEB interface.

1. Open a web browser on a network computer. The WEB interface supports the following browser. Microsoft Internet Explore 6 with Service Pack 1 or later. Netscape 6.1 or later
2. Enter the device's IP address **http://192.168.0.228** in the browser's Address field and press Enter, After press Enter key then pop up a security alarm page, the page will show up. Click yes button, the login page will show up.

Figure 3Security Alert

3. Choose **YES** and a login window will be seen as below:

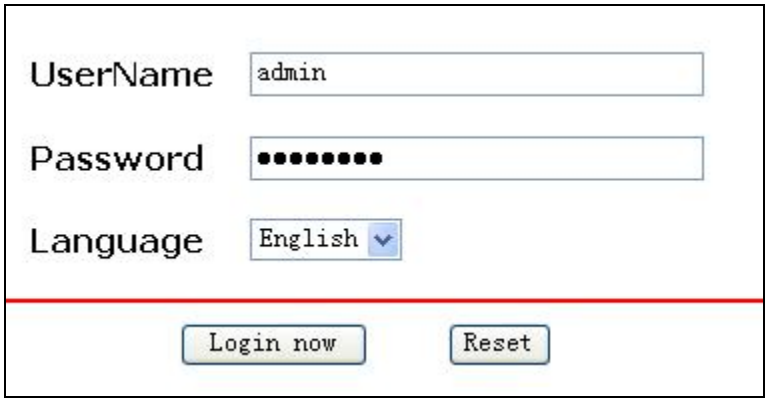


Figure 4Login

Notice:

λ The PC and device must be in the same subnet

4. Enter default User Name (**admin**) in the user name field. Enter default Password (**password**) in the password field. Click **Login**, and a web-based management homepage will appear on your screen as shown below. Result: You can configure the device using WEB interface.

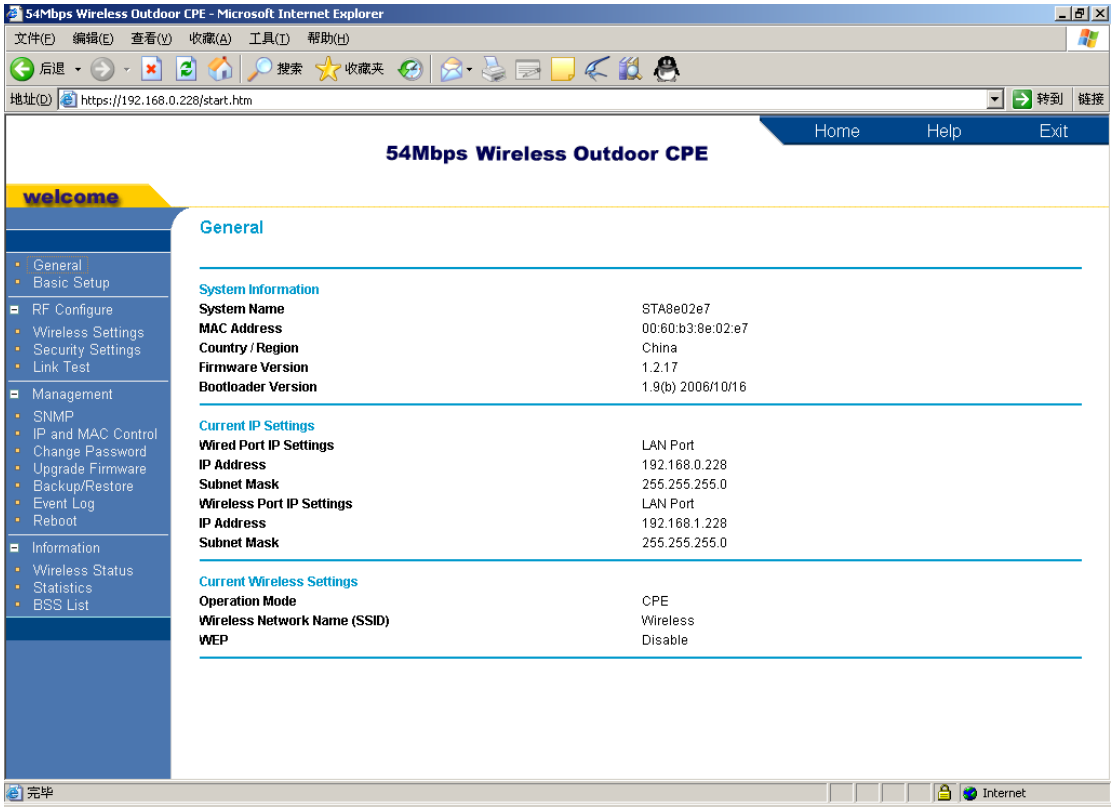


Figure 5General Page

Set the Basic Configuration

In the Basic Setup page, the basic configuration can be set.

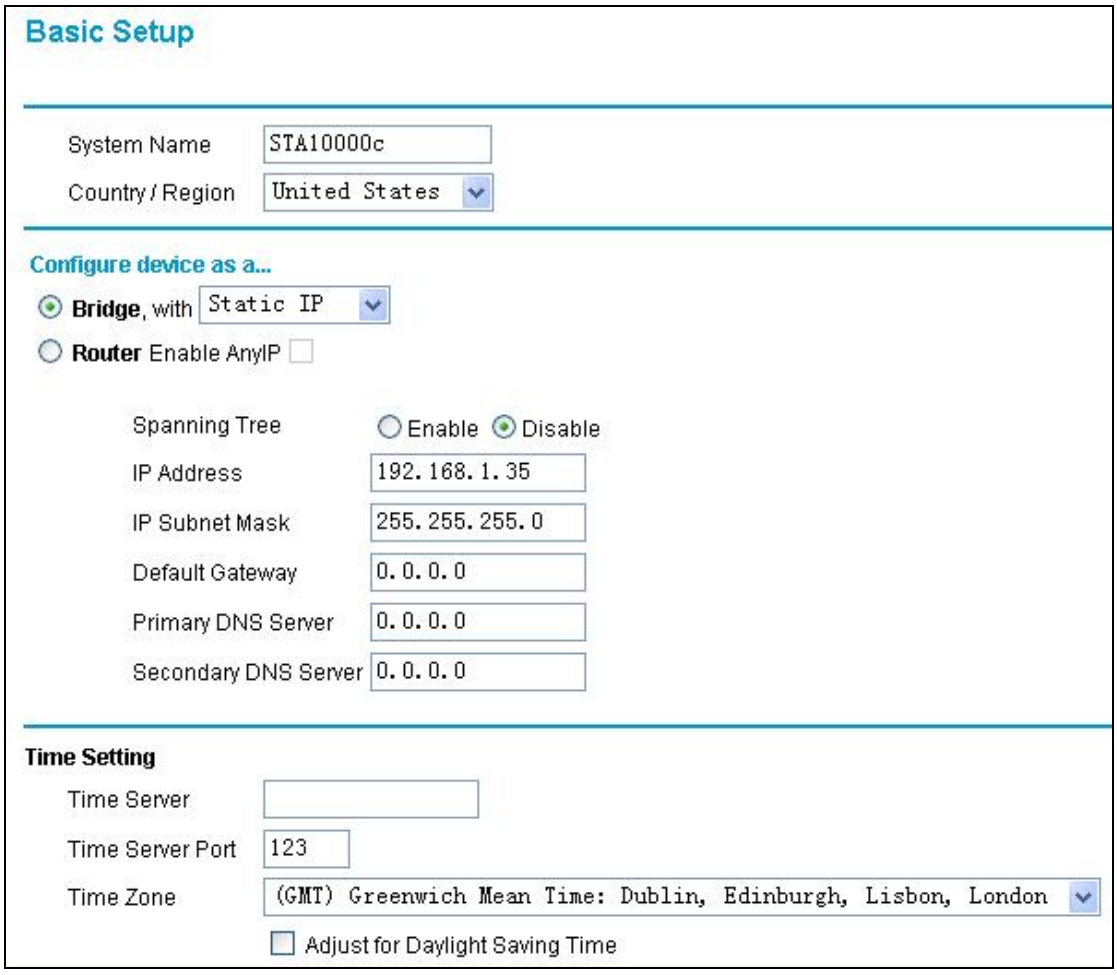


Figure 6Basic Setup

- **System Name**

  This is the NetBIOS name, Device in up to 15 characters, represented by numbers, 0-9, alphabet, A-Z or a-z and "-". device's name can replace IP address in the address field. For example, enter device's name, "sta030201" in the address field; Click Enter, a page will appear on your screen. As device's name support WINS, use "ping" command to check whether the configuration is ineffective.

✎ **Notice:**

- λ The device's default name is: STAxxxxxx xxxxxx representing the last 6 digits of MAC address.
- λ The first character of device 's Name cannot be represented by a figure.
- λ Your host must have a TCP/IP address in your host and IP address have to be in the same subnet while operating WINS.

- **Country/Region:**

The frequency bands determine the available channels depending on the regulatory domain or country. Select your country or region in the table below, the frequencies band in 5GHz. If your country or region is not available, please contact the local reseller or log in our web for more related information.

Diagram 2Channel within 5GHz Frequency Band

Country/Region	Channel
Australia	36-64,149-165
Austria	36-48
Canada	36-64,149-165
China	149-165
Denmark	36-64,100-140
Finland	36-64,100-140
France	36-64
Germany	36-64,100-140
Hong Kong	36-64,149-165
Iceland	36-64,100-140
Ireland	36-64,100-140
Italy	36-64,100-140
Japan	34-46
Liechtenstein	36-64
Luxemburg	36-64,100-140
Netherlands	36-64,100-140
New Zealand	36-64,149-165
Norway	36-64,100-140
Portugal	36-64,100-140
Singapore	36-64,149-165
Spain	36-64,100-140
Sweden	36-64,100-140

Switzerland	36-64
Taiwan	56-64,149-161
United Kingdom	36-64,100-140
United States	149-161

- **Configure Device as a：**

  Configure device, enabling it as a Bridge or a Router. AS a bridge, you can configure IP address, subnet mask, gateway, Primary DNS Server and Secondary DNS Server. As a Route, Please consult **Configure device as a Router**.

- **IP Address：**

  Two types of IP address in the bridge mode described below.

  λ Static IP: Manually configure IP address, subnet mask, gateway, Primary DNS Server and Secondary DNS Server. The Device will automatically understand the subnet mask based on the assigned IP address. Otherwise, you can use 255.255.255.0 as the subnet mask.

  λ DHCP Client: device will obtain IP's settings from DHCP Server automatically during boot-up.

- **Spanning Tree：**

  If enable this function, Spanning Tree Protocol can detect the network loop link and avoid broadcast storm.

- **Time Server：**

  You can input your Time Server IP Address. Default: Null.

- **Time Server Port**

  Input your Time Server Port, Default: 123.

- **Time Zone**

  You may select appropriate Time Zone.

- **Current Time**

  You can get current time from your Time Server.

Set the Basic Wireless Parameters

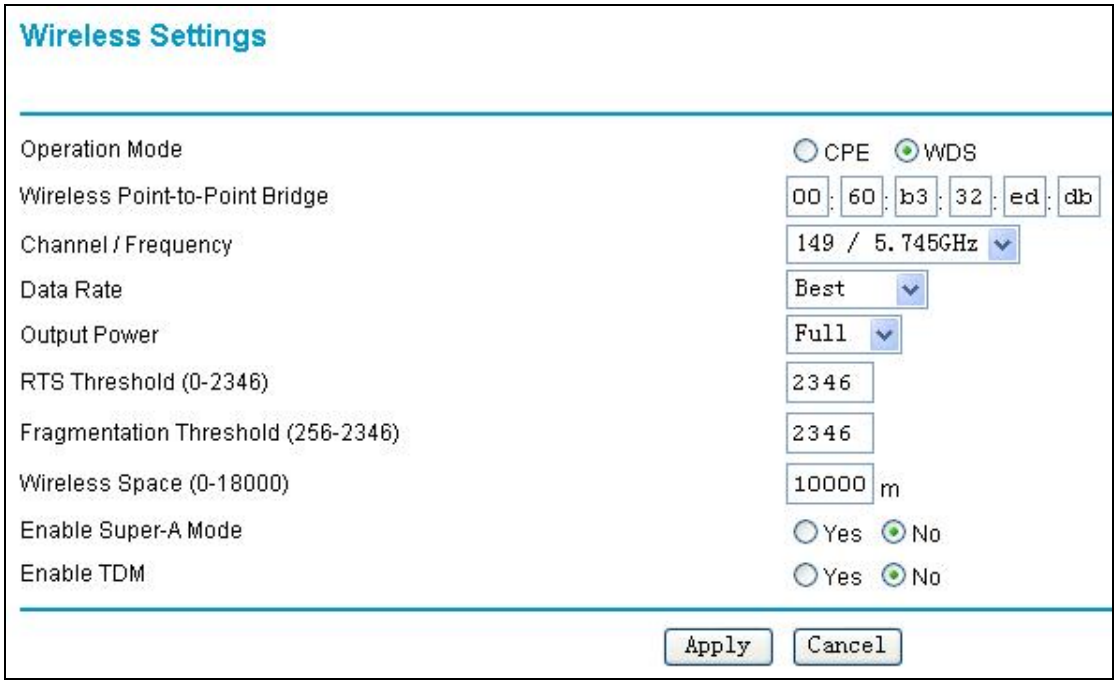


Figure 7Wireless Settings

- **Operation Mode**

  The Device can work as CPE or WDS, choose the right mode depend your need. Default: CPE.

- **Wireless Network Name**

  Enter a 32-character (maximum) Service Set ID in this field; the characters are case sensitive. When in infrastructure mode, this field defines the Service Set ID (SSID). The SSID assigned to the wireless node is required to match the SSID in order for the wireless node to communicate with the remote Device.

  Default: Wireless

- **BSSID**

  Enter a Basic Service Set ID in this field. When in infrastructure mode, this field defines the Basic Service Set ID (BSSID). The BSSID assigned to the wireless node is required to match the BSSID in order for the wireless node to communicate with the remote Device.

  Default: 00:00:00:00:00:00

✎ **Notice:**

λ BSSID priority is higher than SSID, but CPE that only set BSSID can not connect a hidden AP, you must set SSID.

- **Wireless Point-to-Point Bridge**

  The BSSID of the remote device, only be seen under WDS mode

- **Channel / Frequency**

  In WDS Mode, The frequency bands determine the available channels depending on the regulatory domain or country. Frequency and channel are described as follows.

Diagram 3Channel/Frequency within 5GHz

Channel	Centre Frequency （MHz）
34	5170
36	5180
38	5190
40	5200
42	5210
44	5220
46	5230
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
149	5745
153	5765

157	5785
161	5805
165	5825

- **Data Rate**

  Select the available transmit data rate of the wireless network. The possible data rates supported are: Best, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps and 54 Mbps.

  Default: Best

- **Output Power**

  Select the available transmit power of the CPE. The possible Tx power options are: Full, 50%, 25%, 12.5%, Min .The transmit power may varies depends on the local regulatory regulations.

  Default: Full

- **RTS Threshold**

  Request to Send Threshold. The size of packet is up to using CSMA/CD or CSMA/CD mechanism to transmit data packages. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

  Default: 2346

- **Fragmentation Threshold**

  This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

  Default: 2346

✎ **Notice:**

λ The Fragmentation Threshold must be larger than RTS or RTS Threshold is set to 0, then the RTS/CTS will function.

- **Space from AP**

  Input the value of Space from remote AP.

  Default: 10000m

✎ **Notice:**

λ The value of Space from AP should close to the real distance. The distance must be input.

λ If you experience interference (shown by lost connections and/or slow data transfers) you may need to change the channel of the remote AP to see which the best is.

- **Enable TDM**

  Enable when need, detail information refer to **TDM** in Advanced Configuration. Default: OFF

Chapter 4 Advanced Configuration

Security Setup

To enhance the security of the device, Security Setup can be used to gain the more safe wireless transmission. WEP、WPA-PSK and WPA2-PSK will be supported at present

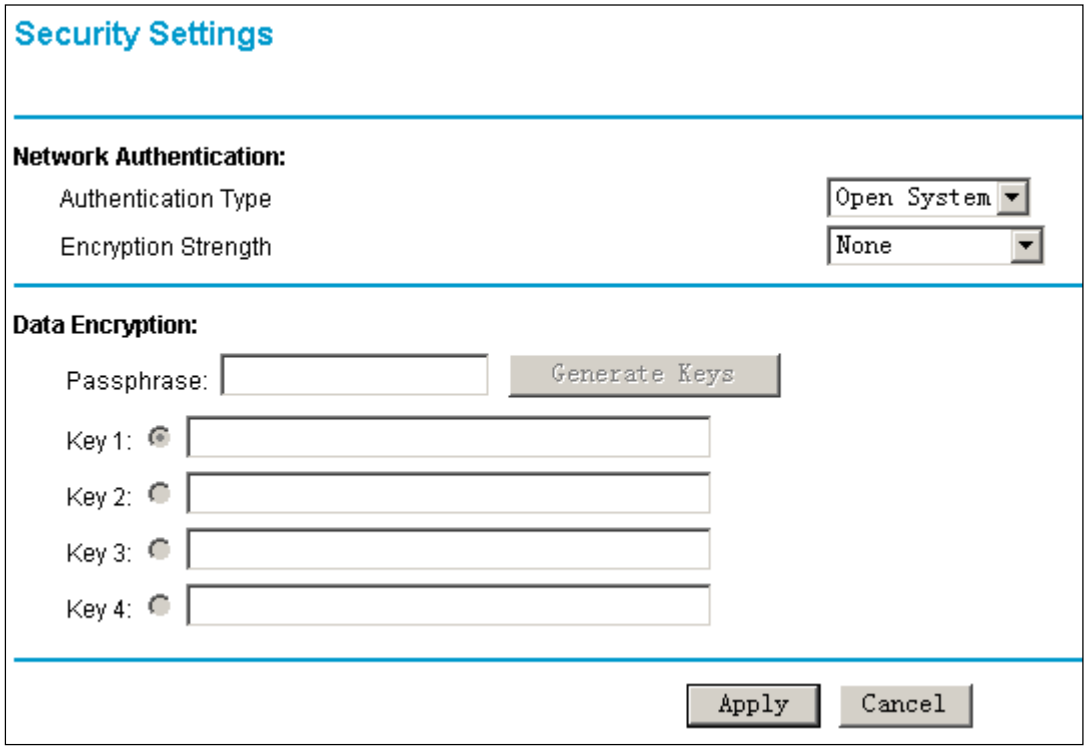


Figure 8 Security Setup

- **Authentication Type**

  Choose the following Authentication type.

  λ Open System: Allow any AP or wireless bridge to connect

  λ Shared Key: If Shared Key is selected, you must enable WEP and enter at least one shared key.

  λ Use WPA (2)-PSK if you have WPA (2)-PSK wireless clients but no RADIUS server.

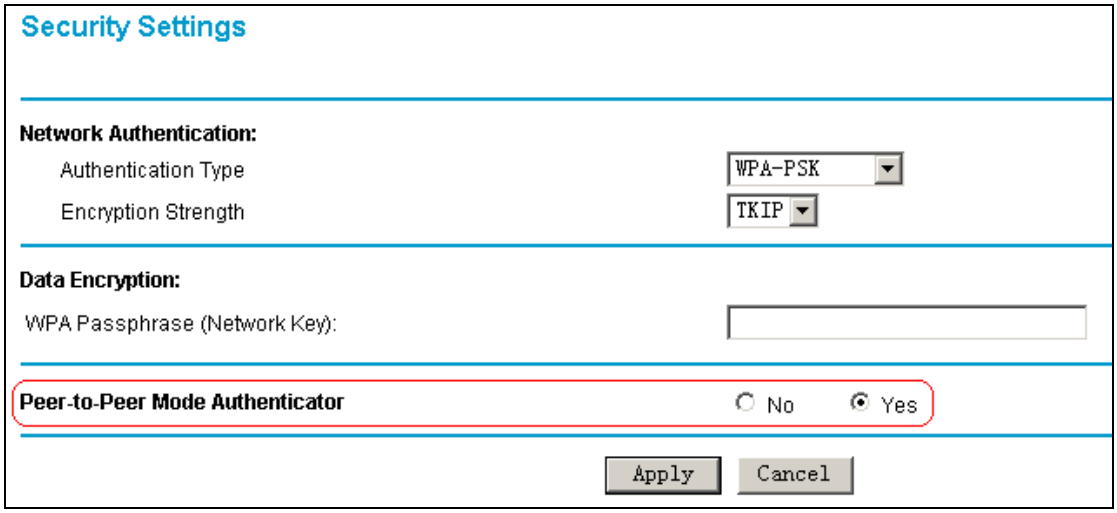
- **Encryption Strength**

  Select the option. If data encryption is enabled, keys must be entered and wireless stations or bridge must use the same keys to connect with the AP.

  λ None

- λ WEP 64 bit: 10 Hex digits (any combination of 0-9, a-f, or A-F)
- λ WEP 128 bit: 26 Hex digits (any combination of 0-9, a-f, or A-F)
- λ WEP 152 bit: 32 Hex digits (any combination of 0-9, a-f, or A-F)
- λ TKIP：you may input 8-63 characters or 64 hex (A-F or 0-9).
- λ AES：you may input 8-63 characters or 64 hex (A-F or 0-9).

- **Security Encryption (WEP) Keys**
  - λ Passphrase: To use the generated keys from passphrase, please enter a passphrase and click Generate Keys button. You can also enter the keys directly. Only 8 to 63 characters are allowed to be entered. Wireless stations or bridge must use the same keys to connect with the AP.
  - λ Key1~Key4: Select the key used as the default key. Data transmissions are always encrypted by the default key. Other keys can only be used to decrypt received data. The four entries will be disabled if WPA with Radius authentication option is selected.
- **Pear-to-Peer Mode Authenticator**



When set device WDS Mode and choose Authentication Type is WPA-PSK or WPA2-PSK.You should set one device is Authenticator and the other is Authenticated.

✎ **Notice:**

- λ The device and the APs must have the same Authentication Type, Data Encryption and Key; otherwise they cannot connect with each other.

IP and MAC Access Control

IP and MAC Access Control provides an additional layer of security when device work as CPE. It is used to ensure that only the specified PCs in the network can access the network which the remote AP is in.

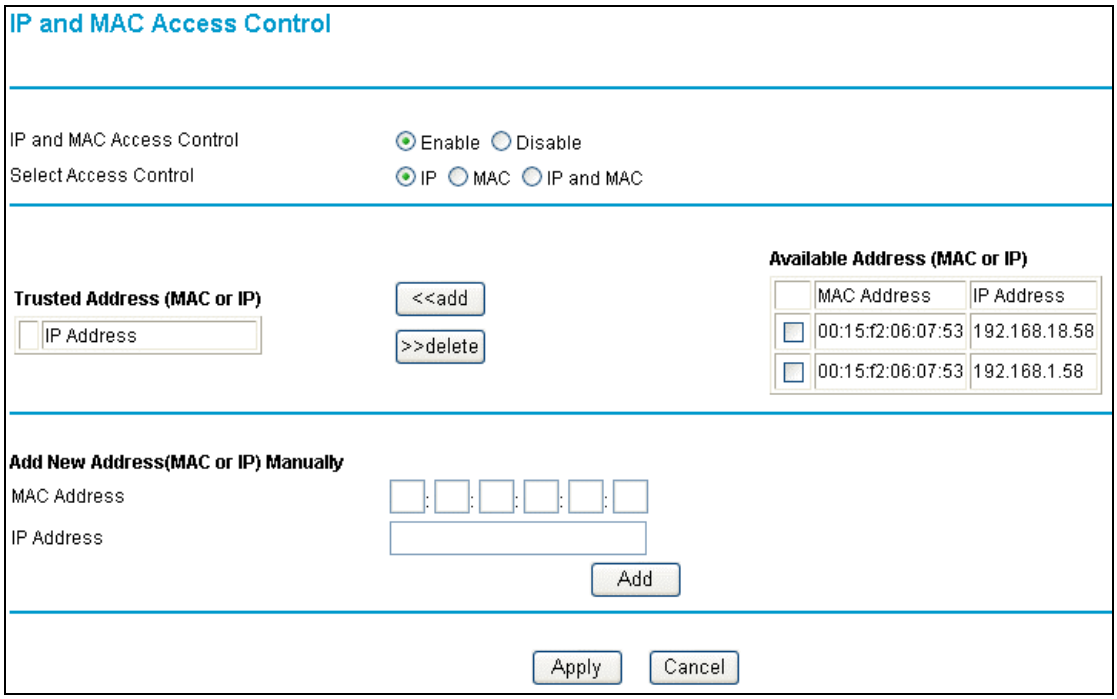


Figure 9IP and MAC Access Control

Enable the **IP and MAC Access Control** in the page. Only the PCs in the "Trusted Address" list can access the network wireless connected remote AP. What you should do is to maintenance the "Trusted Address" list.

Three options are available, IP Address Isolation, MAC Isolation and both IP Address and MAC Isolation, to authorize PCs access into the network wirelessly connected to remote AP.

We'll elaborate the three approaches below.

- λ IP Address Isolation: Specify certain of IP addresses and authorize them to access the network wireless connected remote AP.
- λ MAC Isolation: Specify certain of MACs and authorize them to access the network wireless connected remote AP.
- λ both IP Address and MAC Isolation: Specify a certain of MACs and IP addresses and authorize them to access the network wireless connected remote AP

- **Add trusted PCs**

  λ Add new Addresses Manually: Fill the Address in the textbox and click **Add** button. Then click **Apply** button to make the configuration take effect.

  λ Add by Available Address list: Select the Address from the Available Address list and click **Add** button to add the station to the Trusted Address list. Then click **Apply** button to make the configuration take effect.

- **Delete trusted PCs**

  Choose the Address in the Trusted Address list and click **delete** button. Then click **Apply** button to make the configuration take effect.

TDM

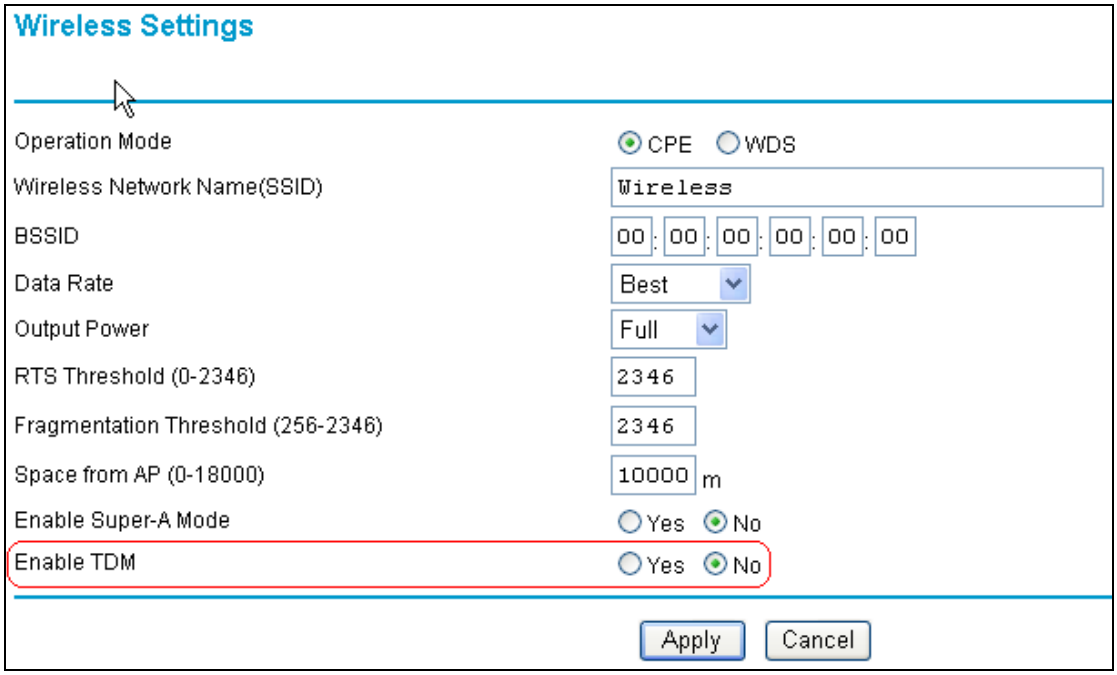


Figure 10Enable TDM

In AP-Station mode, if there are many stations, the throughput of wireless network will reduce; the TDM function can solve this problem. When there are more than 4 stations, we suggest this function should be enabled.

- λ To avoid interference among the hidden nodes.
- λ Limit the wireless clients against occupying too much bandwidth
- λ Ensure the specific wireless clients a spacious bandwidth.

In Bridge mode, if the throughput of some one node is very low, you may also enable TDM function.

Configure as a Router

The simple Router function can connect two different subnets.

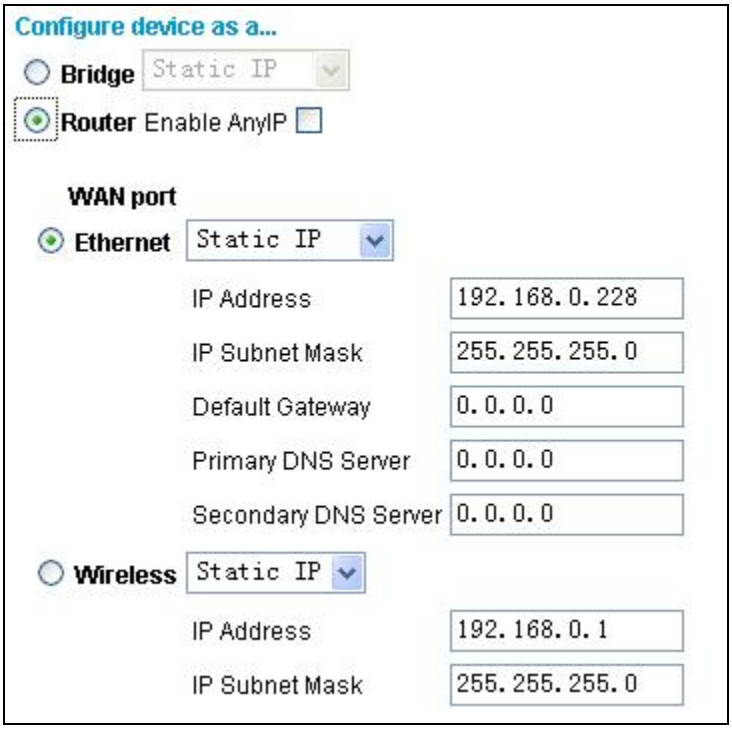


Figure 11Router

There two kinds of Router mode.

- **WAN on Ethernet**
- **WAN on Wireless**

  You can choose one mode according to your need. Then set the IP address of WAN and LAN (Their IP address should be in different subnet.). The following figure shows the two modes.

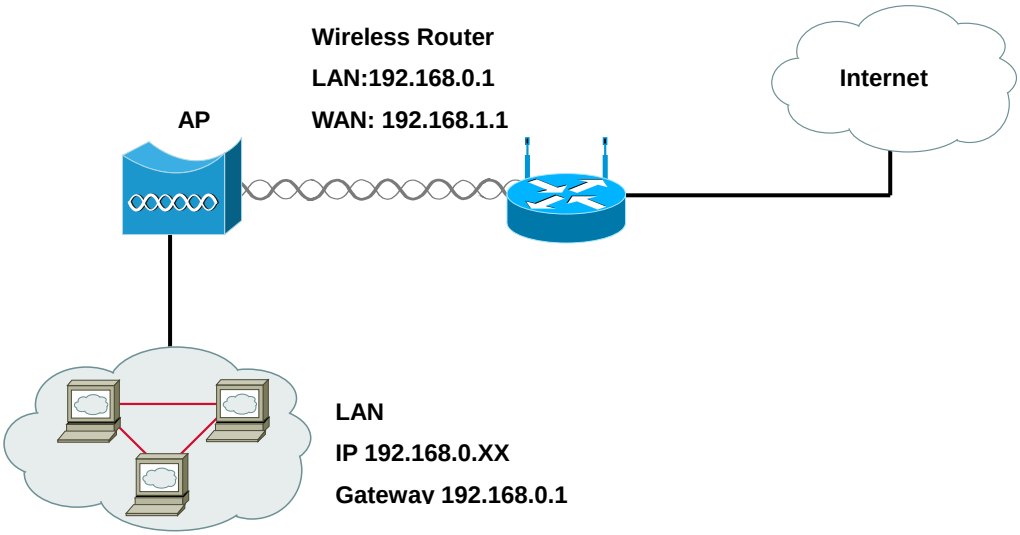


Figure 12Wireless Router—WAN on Ethernet

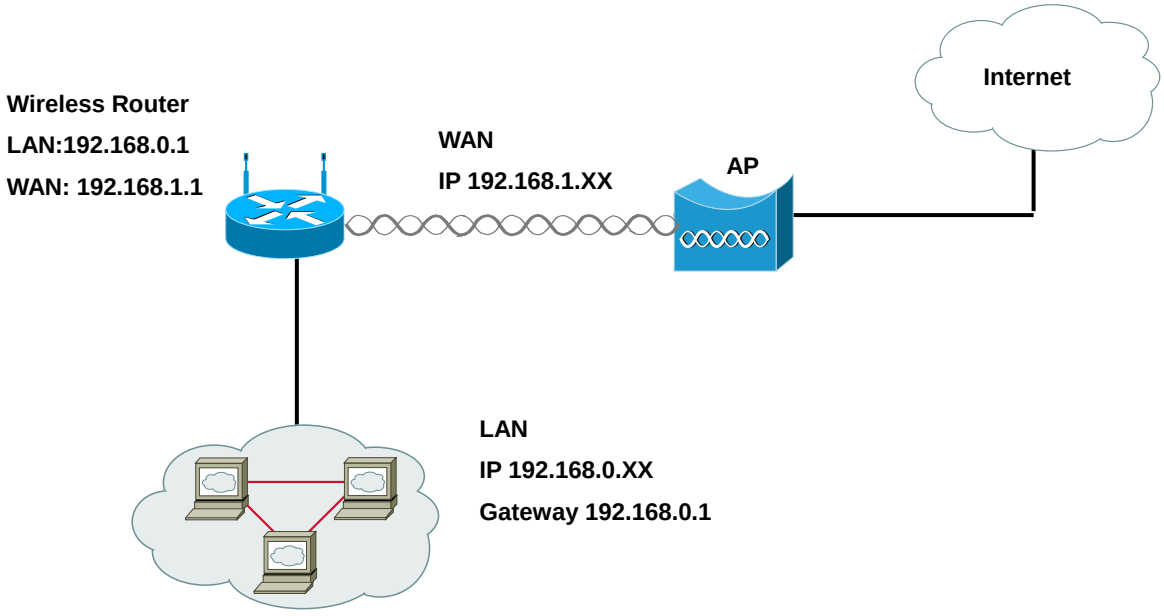


Figure 13Wireless Router—WAN on Wireless

AnyIP

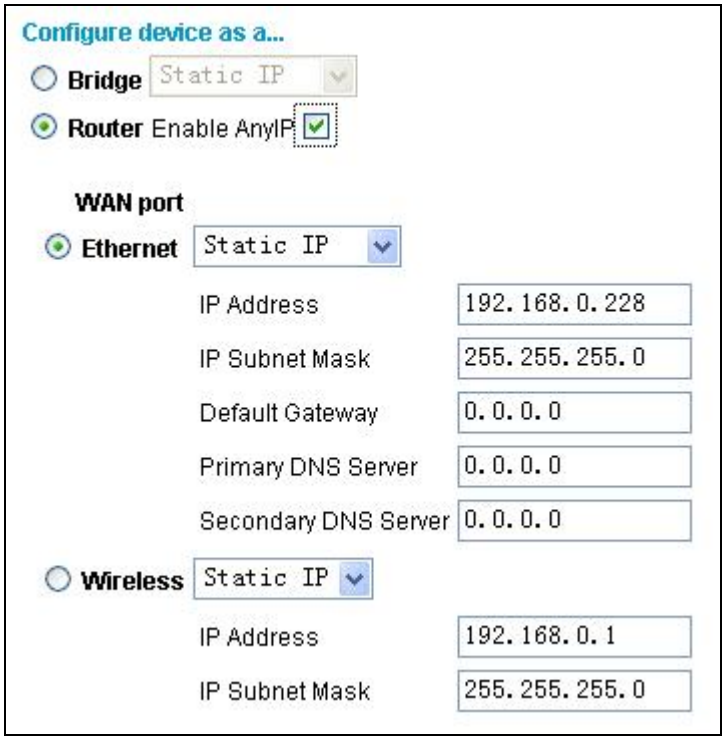


Figure 14AnyIP

The AnyIP, sparing you the trouble of setting IP address can be functioned in Router mode only. You have to set the correct IP Address, Gateway and DNS, but you could set the client's IP Address, Gateway and DNS with your like.

WDS Mode

The device can connect to the remote AP with the WDS function.

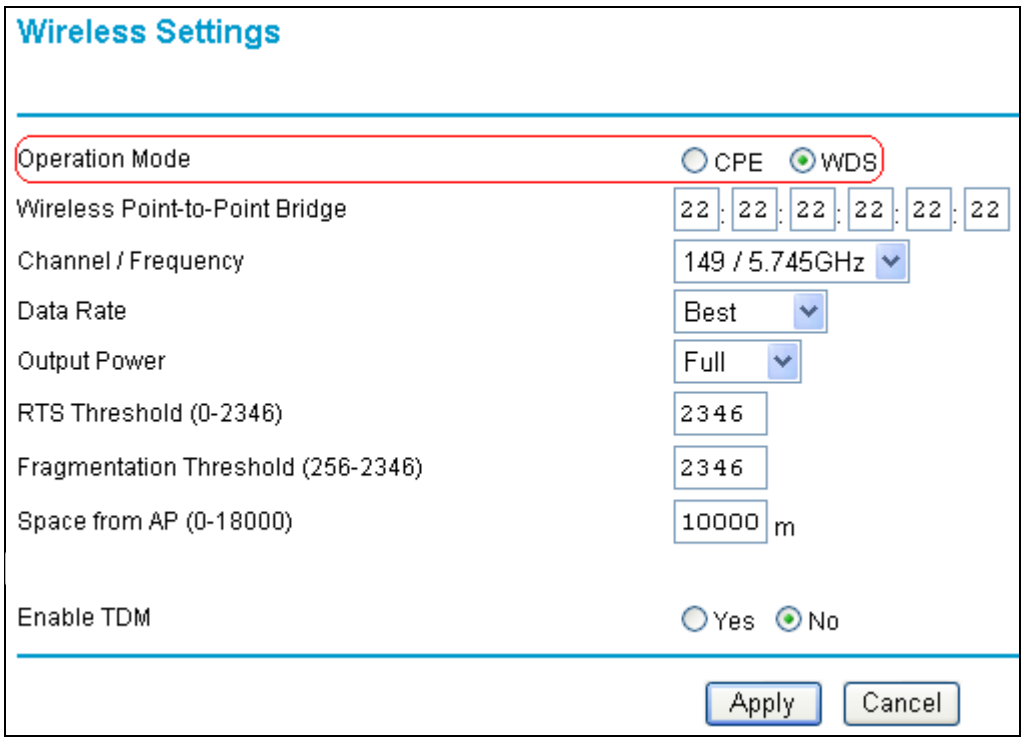


Figure 15WDS Mode

WDS connection can be configured refer to the following steps:

1. Change the **Operation Mode** to **WDS**
2. Input the MAC Address of the remote AP
3. Select the right Channel/Frequency
4. Click **Apply** to make the configure work. Now the two devices have normally worked. You can change settings account to your need. The detail about changing settings refer to **Set the Basic Wireless Parameters**, **Security Setup**.

✎ **Notice:**

λ The both Access Points settings of Country/Region, Channel/Frequency and Security should be the same.

λ The WDS Mode can't be used between two ZA-4000 or with other CPE with WDS function.

5. Use "Link Test" to test the signal strengthens of wireless network. At first, open "WDS Settings" page, input the real space between Bridges. Then open "Link Test" page, check those settings whether is right. If right.

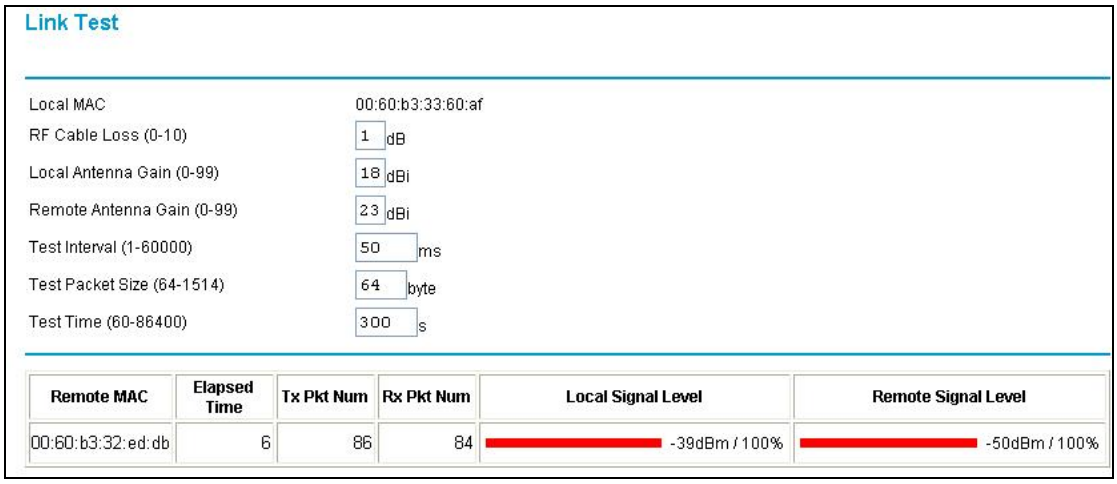


Figure 16Link Test

✎ **Notice:**

λ For the accuracy of test result, you should make sure that the Link Test settings are right.

Click start button to begin test. The result will show bellow.

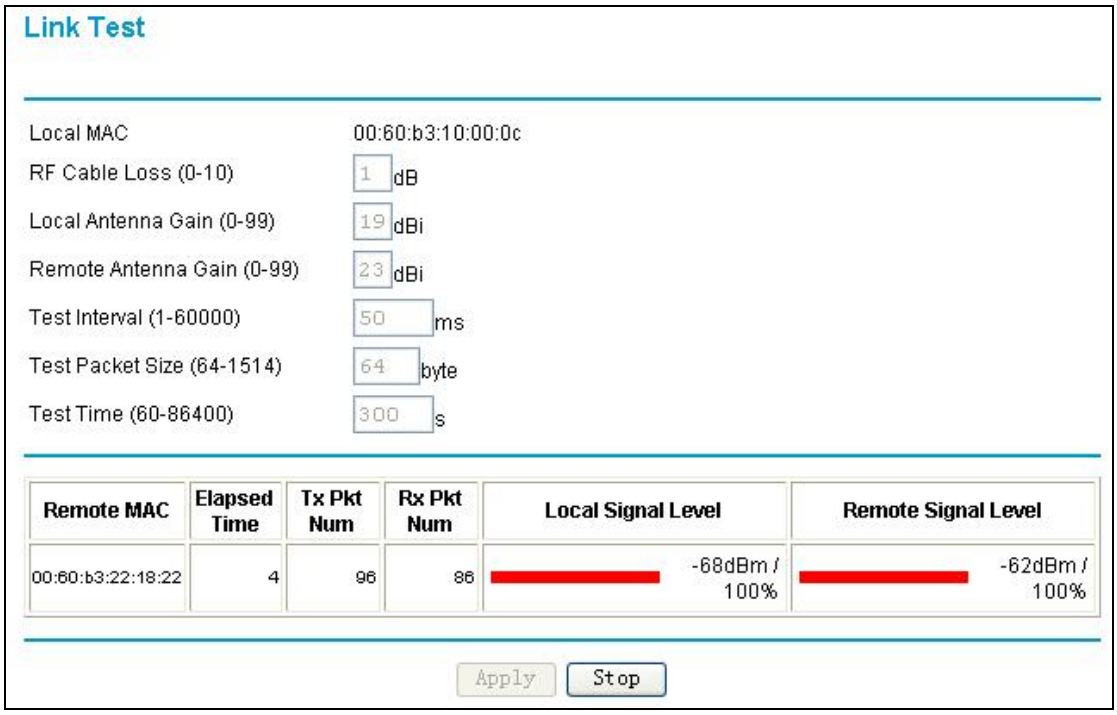


Figure 17Link Test Signal

Form the test result table you can get:

Local Signal Level (dBm): shows the received signal strengthen of local Access Point

Remote Signal Level (dBm): shows the received signal strengthen of remote Access Point.

View the intensity of signal, and adjust the positions and angles of the antenna according to the intensity of signal. Adjust the antenna, and observe the value of dBm at the same time. When the number value of dBm is the greatest, the antenna is in the best positions and angles.

Diagram 4Signal Strengthen and Throughput List

Signal Strengthen (dBm)	Transmit Data Rate(Mbps)	Real Throughput(Mbps)
－65	54	24
－66	48	22
－70	36	17
－74	24	12
－77	18	10
－79	12	8
－81	9	6

✎ **Notice:**

λ The signal strengthens (dBm) is negative value, the more little the absolute value of it, the better the signal strengthens. For the better throughput of wireless network, you should better adjust the signal strengthen as better as possible.

λ The signal strengthens (Percent) is just a reference value. It lies on not only the real signal strengthen but also the academic signal strengthen which lies on the Link Test settings. So you should take the signal strengthens (dBm) as reference while adjusting antenna.

Diagram 5Distance and Signal Strengthen

Distance(km)	Best Signal Strengthen (dBm)
3	－64 ~ －56dBm
6	－72 ~ －62dBm
10	－75 ~ －67dBm
18	－80 ~ －72dBm

－64～－56dBm, data rate can reaches 54Mbps, So you should adjust antenna to get at least

Example: If the space between wireless bridges is 3km then the best signal strengthen can reach －60dBm.If get any other trouble outdoor while set up AP. please see **Troubleshooting**

Chapter 5 Management

View the General Information

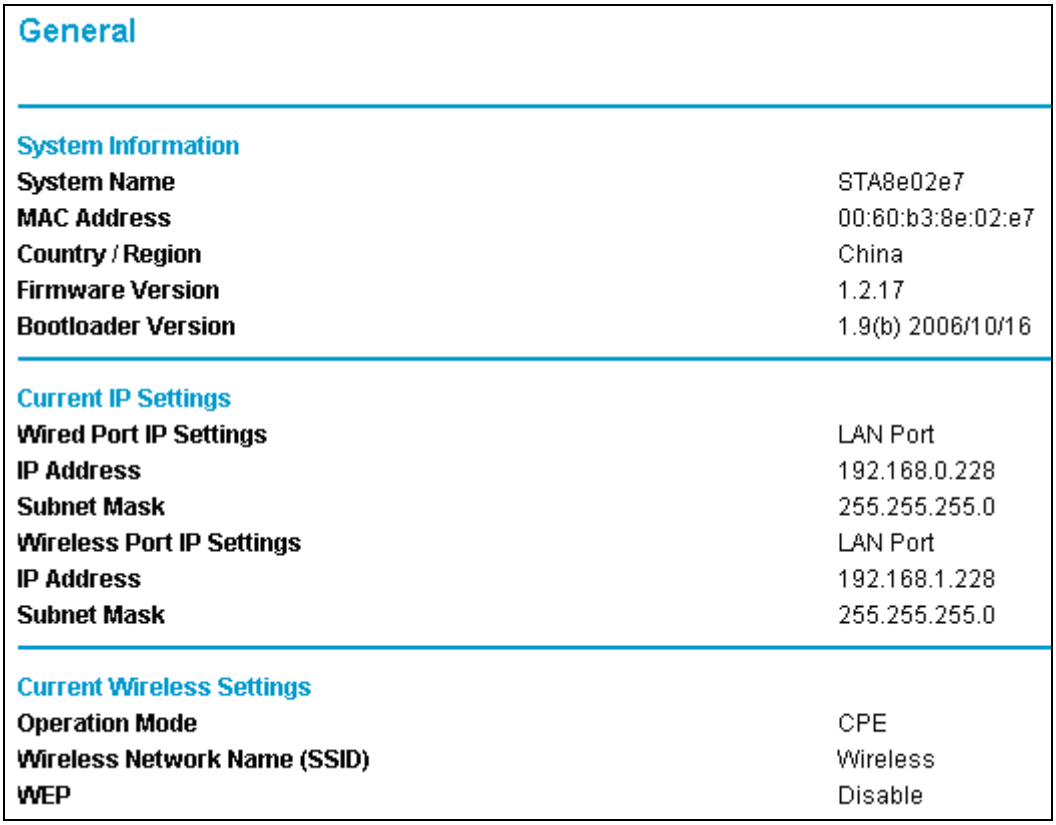


Figure 18General

The General Read-only Information page displays current settings and statistics of your Access Point and any change of settings must be indicated on other pages.

Wireless Status

This page displays both Wireless Status and Signal Level. Click Refresh to update the current statistics.

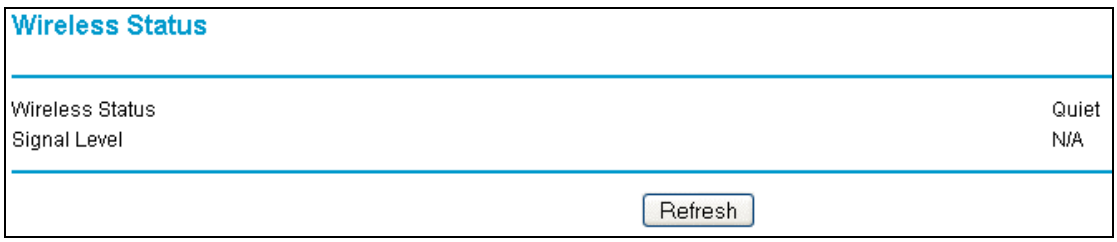


Figure 19Wireless Status

It shows the status between ZA4000 and AP. It has these status: Quiet，Joined，Auth，Assoc，Connected and Unknown. Quiet means the product hasn't connected an AP. Joined means the product is connecting an AP. Auth means the product and AP is authenticating. Assoc means they has authenticated and begin to associate. Connected means the product has connected an AP. Unknown means error between connections. The connection process is that: Joined-Auth-Assoc-Connected.

- **Signal Level**

It shows the signal level of the ZA4000.You can see the value only when ZA4000 has connected an AP. Otherwise, it is N/A.

View the intensity of signal, and adjust the positions and angles of the antenna according to the intensity of signal. Adjust the antenna from side to side from head to foot, observe the number value of dBm in no time, when the adjustable value of dBm is the greatest, the antenna is in the best positions and angles promptly in the locale.

Statistics

This page displays both wired and wireless interface network traffic. Click Refresh to update the current statistics.

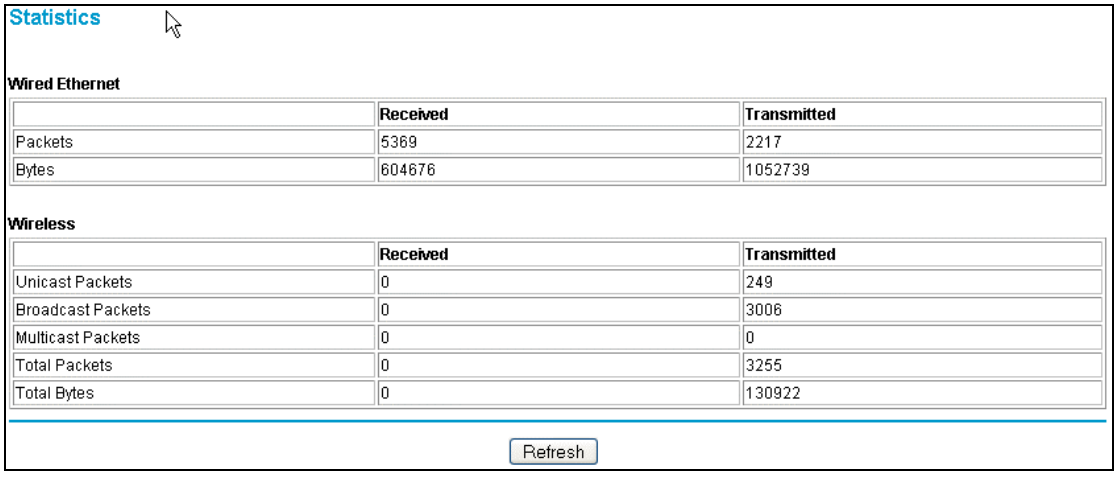


Figure 20Statistics

- **Wired Ethernet**

This section displays traffic statistics for the wired Ethernet interface.

- **Wireless**

This section displays traffic statistics for the Wireless interface.

BSS List

This page shows the Channel, Wireless Mode, Security, BSSID, and SSID for each available wireless Access Point in wireless network.

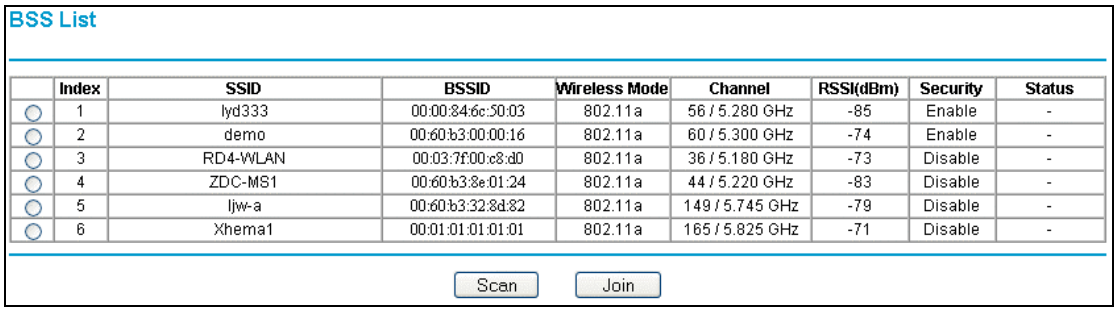


Figure 21BSS List

Change Login Password

You can use the Change Password page to change the CPE administrator's password for accessing the Settings pages.

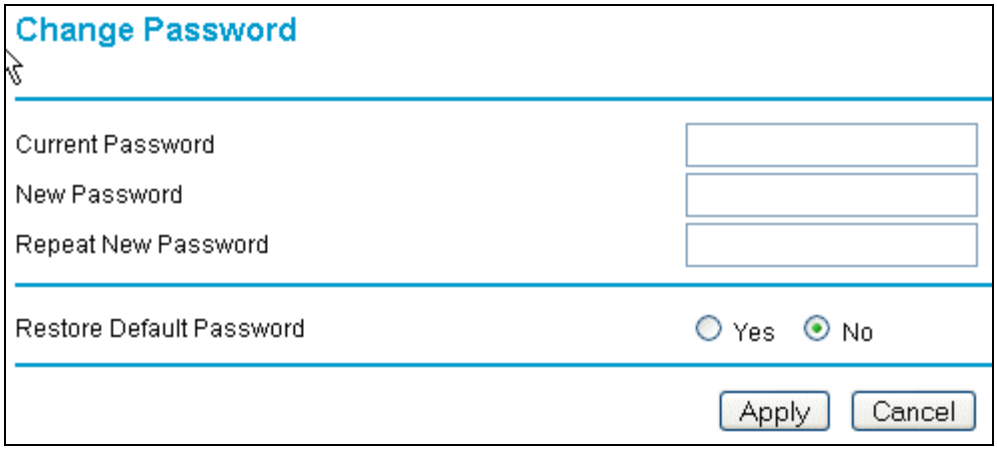


Figure 22Change Password

You can change the password to control access the device or not in Change Password page.

To change the password, type the original password, the default one is "password". Type a new password and re-type it in the Repeat New Password box to confirm it.

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

Be sure to write it down in a secure location and the maximal length of the password is 19 characters.

Firmware Upgrade

There are two ways to upgrade Access Point software.

- **By WEB**

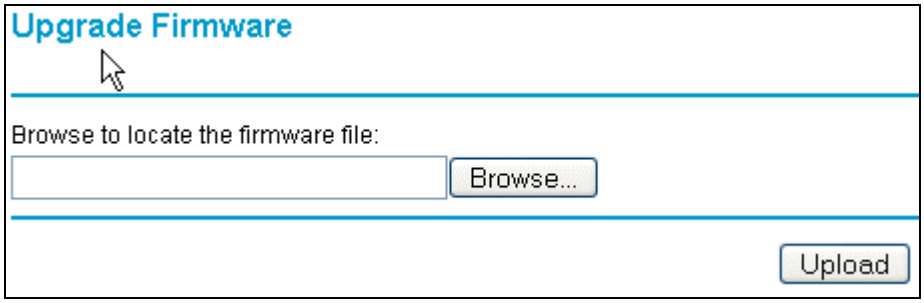


Figure 23Firmware Upgrade

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

- **By FTP**

1. ftp 192.168.0.228, the device IP address, input user name (admin) and password (password).
2. After loginning in, input command "bin" and "put za4000.rmt". The upgrading is launched automatically.

```
C:\>ftp 192.168.0.228
Connected to 192.168.0.228.
220 (vsFTPd 1.1.3)
User (192.168.0.228:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files.  Login successful. Have fun.
ftp> put za4000.rmt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
ftp: 发送 4014088 字节，用时 2.58Seconds 1553.44Kbytes/sec.
ftp> by
221 Goodbye.
```

3. Waiting for some seconds ,the device will reboot.

Warning:

λ The software must be za4000.rmt when upgrading by FTP

λ Do not try to turn off the Access Point, shutdown the computer or do anything else to the Access Point until the Access Point finishes restarting!

✎ **Notice:**

λ In some cases, such as a major upgrade, you may need to erase the configuration and manually reconfigure your CPE after upgrading it. Refer to the Guide included with the software to find out if you need to reconfigure the CPE.

Backup/Restore Settings

There are two kinds way to backup or restore Access Point.

- **WEB**

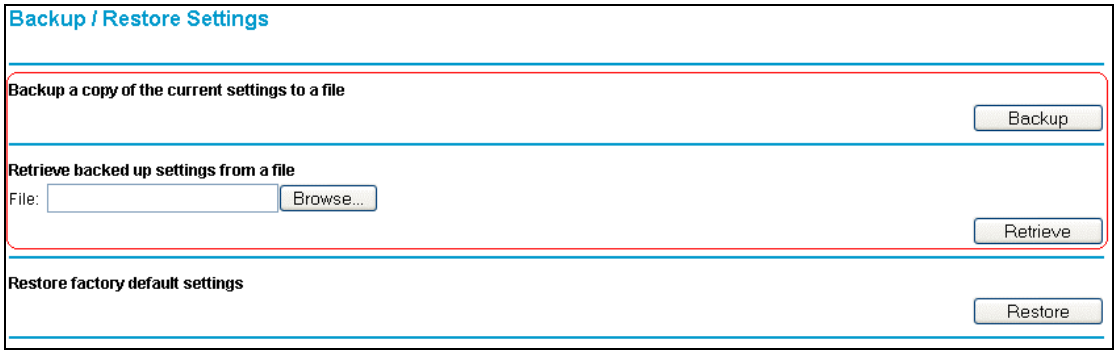


Figure 24Backup/Restore Settings

1. Click button to save backup file to hard disk.
2. Click Browser button to locate the backup file you want to retrieve and click retrieve button, then the device will restart.

- **FTP**

1. Login device by ftp.
2. Input command get za4000.cfg, it will be saved in current directory.

```
C:\>ftp 192.168.0.228
Connected to 192.168.0.228.
220 (vsFTPd 1.1.3)
User (192.168.0.228:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files.  Login successful. Have fun.
ftp> get za4000.cfg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for /mnt/ramd/za4000.cfg (12176 bytes).
226 File send OK.
ftp: 收到 12176 字节，用时 0.03Seconds 405.87Kbytes/sec.
ftp> quit
221 Goodbye.
```

3. Input command put za4000.cfg, it will retrieve it to device. and device will restart.

Notice:

λ The config file must be za4000.cfg when restore by FTP

λ Do not try to turn off the device, shutdown the computer or do anything else to the device until it finishes restarting!

Restore to Factory

There are two kinds way to restore Access Point to factory.

- **WEB**

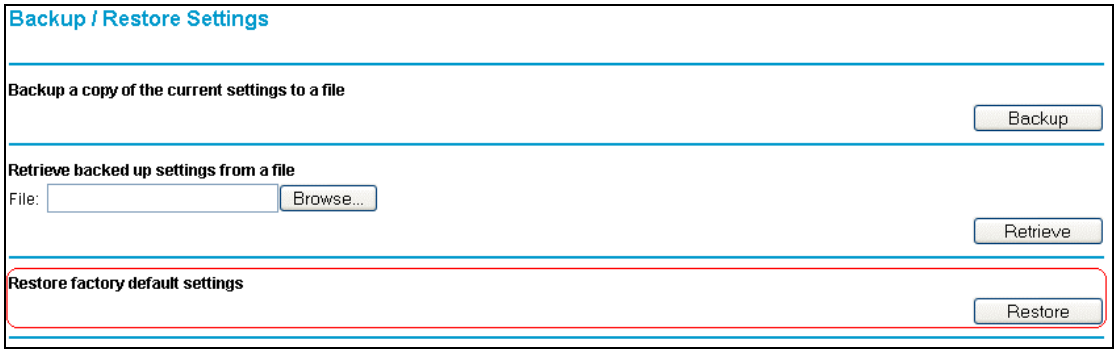


Figure 25Restore to Factory

Click **Restore** button then the device will restart to factory.

- **Hardware Default Button**

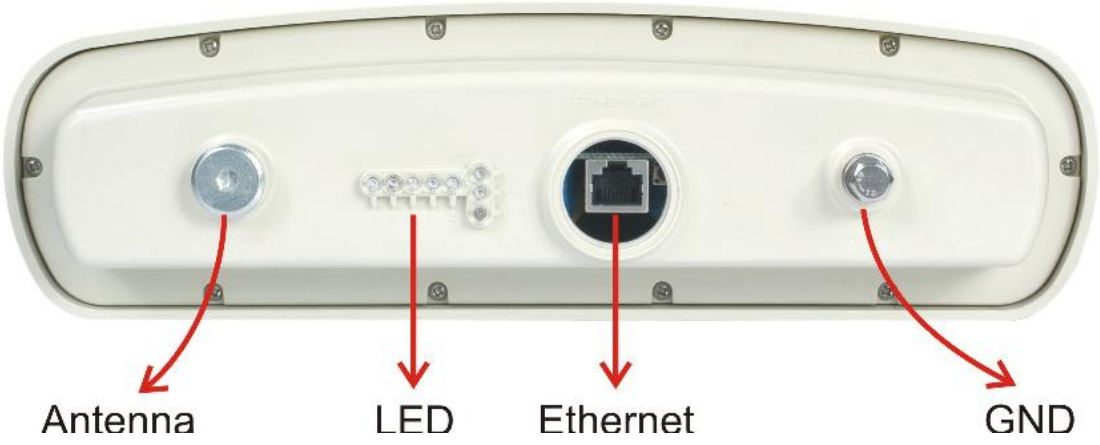


Figure 26Default Button

Press the default button for more than ten seconds while power on the device.

Warning:

λ Don't turn off the device during restoring to factory.

Event Log

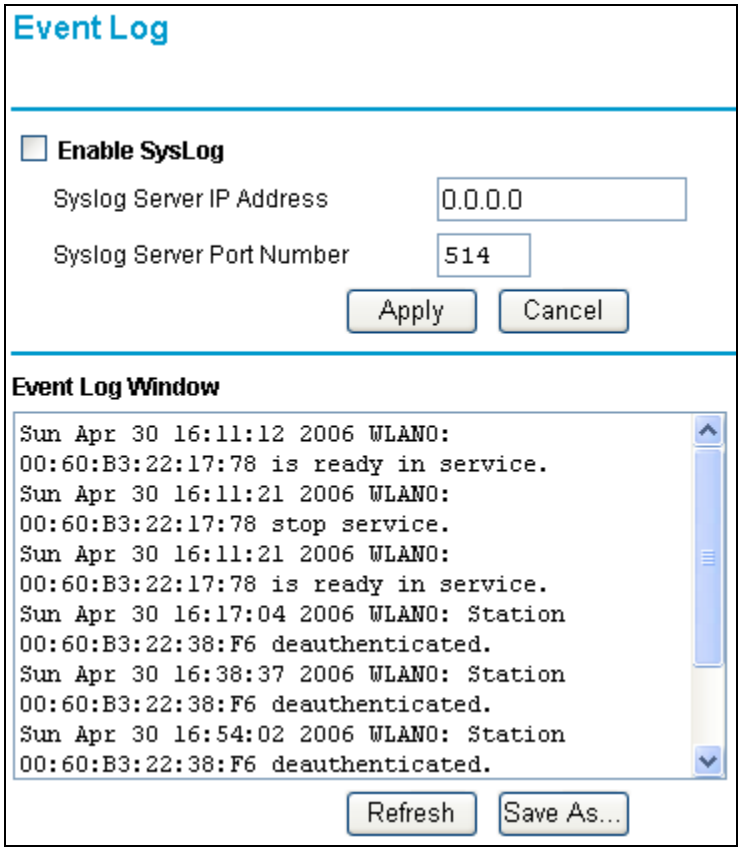


Figure 27Event Log

- **Enable SysLog**

Enable or Disable SysLog function.

Default: Disable

- **Syslog Server IP Address**

Input your Syslog Server IP Address.

Default: 0.0.0.0

- **Syslog Server Port Number**

Input your Syslog Server Port Number.

Default: 514

- **Event Log Window**

You can see log information in Event Log Window. You may click Refresh button for updating Event log, and you may click Save As button for saving Event Log to your hard disk

Reboot System

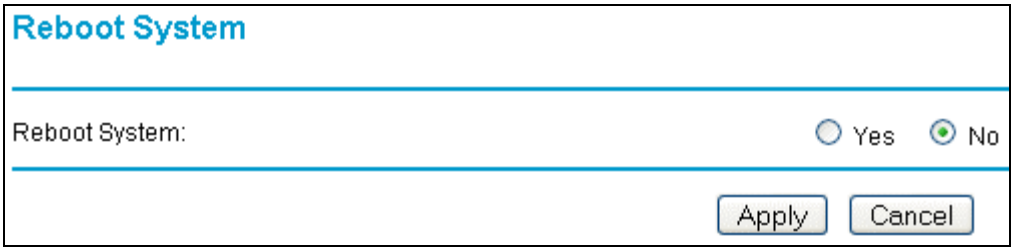


Figure 28Reboot System

You may select Yes on "Reboot System" page and then click on apply button to reboot the device.

SNMP Management

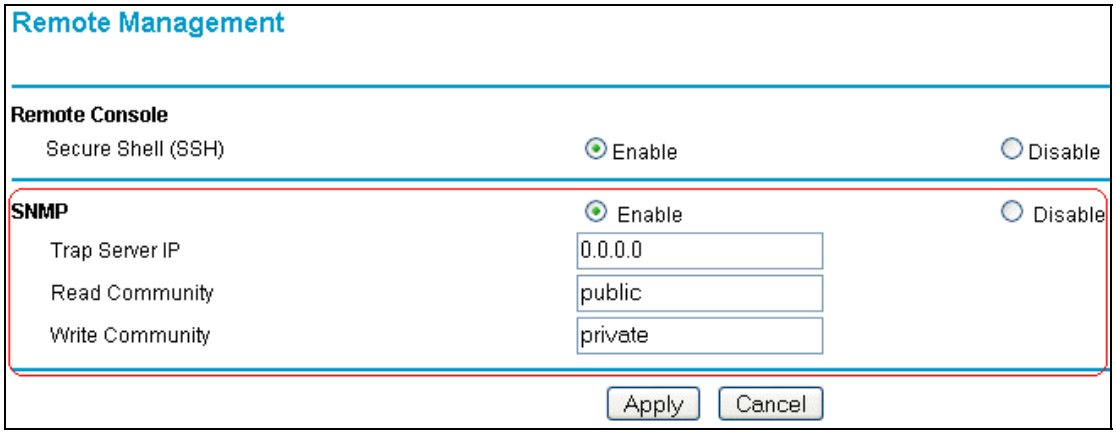


Figure 29SNMP

Device supports SNMP. At first you should set SNMP settings and get MIB file from device by ftp.

1. SNMP Settings.

a) Set the Trap Server Address;

You can find the unusual log on the Trap Server.

b) Set the Read-only Community;

c) Set the Read-write Community;

d) Click the "Apply" button to save setting.

2. Get MIB file by ftp

a) Login device by ftp.

b) Input command "get za4000.mib", you will find the mib file in current directory.

```
C:\>ftp 192.168.0.228
Connected to 192.168.0.228.
220 (vsFTPd 1.1.3)
User (192.168.0.228:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files.  Login successful. Have fun.
ftp> get za4000.mib
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for /mnt/ramd/za4000.mib (38178 bytes).
226 File send OK.
ftp: 收到 38178 字节，用时 0.02Seconds 1908.90Kbytes/sec.
ftp> by
221 Goodbye.
```

✎ **Notice:**

λ The file name must be za4000.mib.

SSH Management

ZA-4000 support telnet management and access by SSH, suggest that you use Putty software to login.

1. Open the Remote Management page，enable SSH.

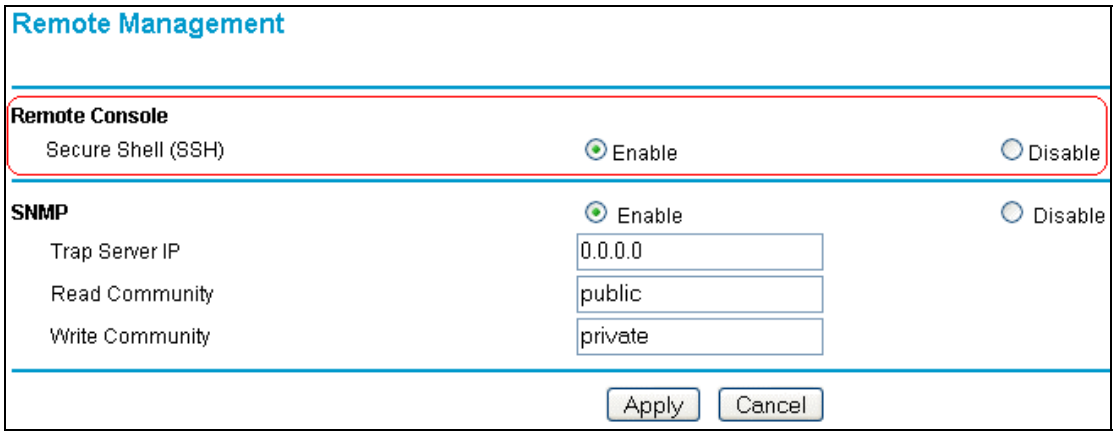


Figure 30Enable SSH

2. open Putty

3. Input device address, choose SSH protocol.

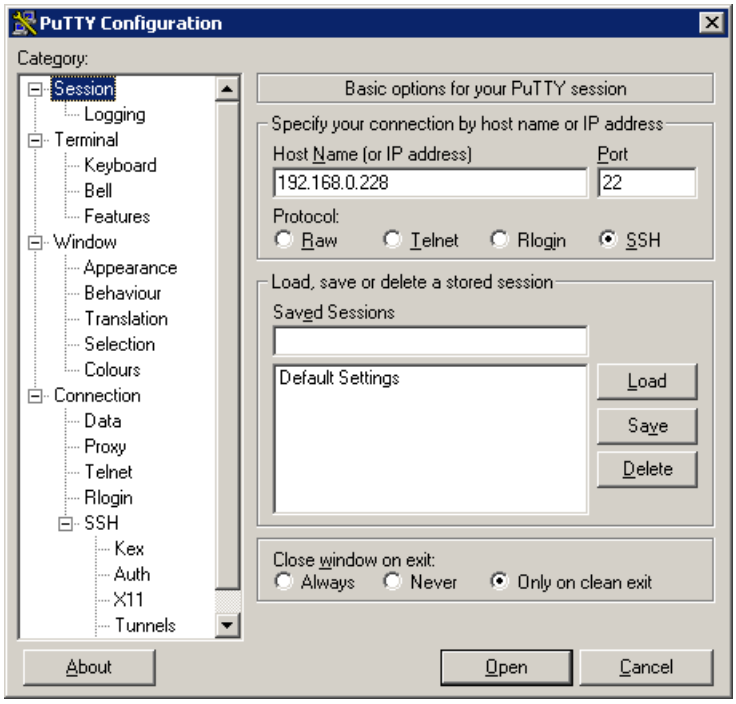


Figure 31Putty1

4. Open it. You will see as following figure.

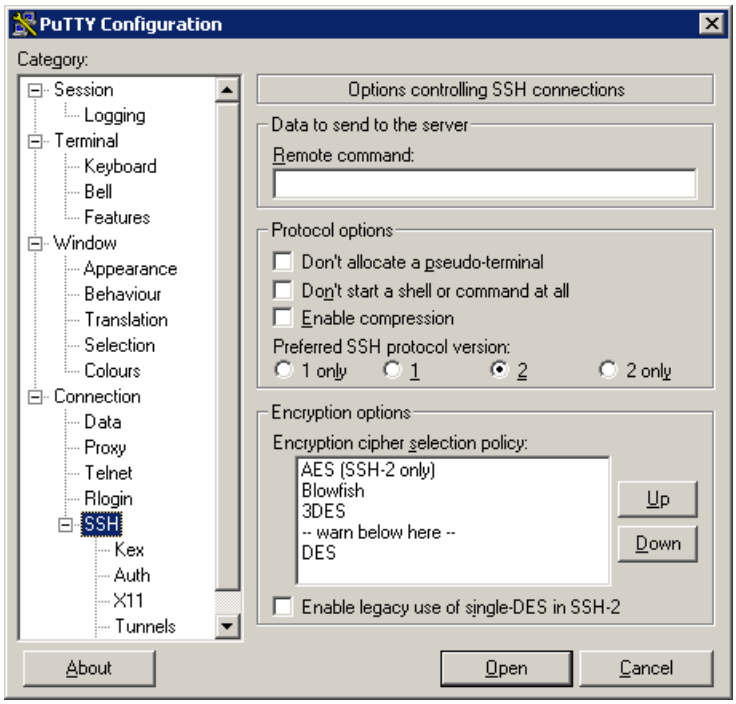


Figure 32Putty2

5. Click Open，the window show as below

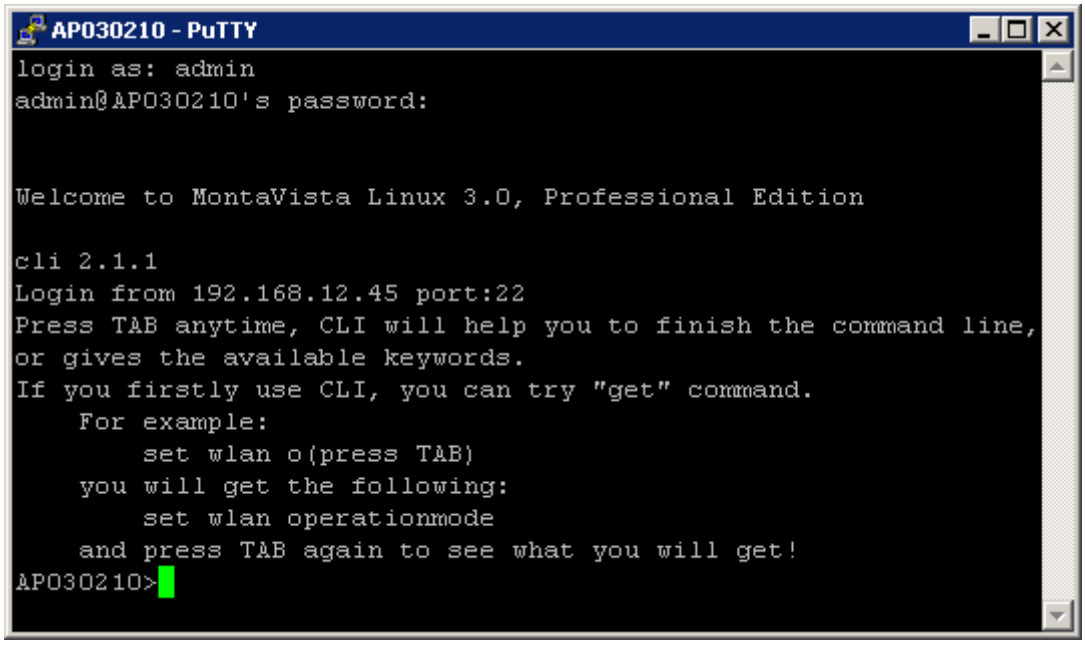


Figure 33SSH Terminal

6. The user name is admin and password is password, after login you can use command line to

set device. you can input command "help" to get help.

All the command supported is in **Appendix D. SSH**.

Chapter 6 Troubleshooting

FAQ

Q 1. How to know the MAC address of the Access Point?

- The MAC address is written in a label which is in the bottom of Access Point.

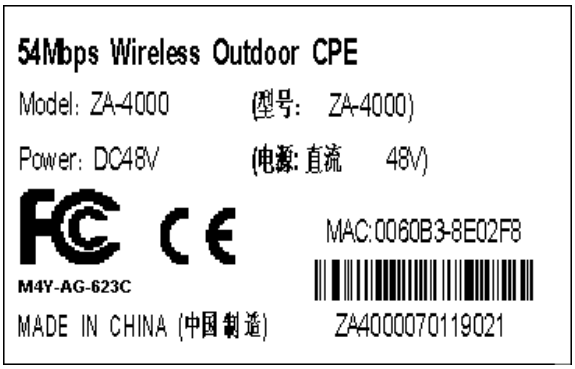


Figure 34MAC Address

- From the General page of WEB configuration, you also can get the MAC address of device.

Q 2. Why STA can not build connection after setting?

- Check the "SSID" or "ESSID" whether is same.
- Check the "Data Encryption" and "Key" whether is same.
- Check the "Wireless Space" whether is real space. The Wireless Space should be the distance between AP and the farthest CPE.

Q 3. How to calculate the academic signal strengthens?

Local receive signal strengthens (dBm)= remote AP Tx Power -Cable1 Loss+ Antenna1 Gain -Path Loss + Antenna2 Gain-Cable2 Loss

Diagram 6RF Path Loss

M(Meter)	5GHz（dBm）
1	46
2	52
5	60
7	63

10	66
20	72
30	75.6
40	78
50	80
60	81.2
70	83
80	84
90	85
100	86
200	92
300	95.6
500	100
1000	106
3000	116
5000	120
10000	126
15000	130
20000	132
25000	134
30000	136

Example: one pairs of ZA-5000-MS ,another is ZA-4000, the space between bridges is 3km.

Tx Power ＝ 15dBm

Cable loss ＝ 1dBi

Antenna Gain ＝ 18dBi

Path loss ＝ 116dBm

Local receive signal strengthens（dBm）＝ 15－1.5＋18－116＋16－1 ＝ －69（dBm）

Q 4. Why the throughput is not high?

You should adjust antenna to get highest signal strengthens by Link Test. You can refer to **Diagram 5Signal Strengthen and Throughput List** If can not get higher signal strengthens, please check the following steps:

- Wireless Channel/Frequency

Try to change other channel

- Wireless disturbance

Check whether there are other wireless equipments nearby AP; make sure they do not disturb AP.

Q 5. The wireless becomes unstable such as ping timed out and lose packet after a period of well work?

This situation may the wireless network is disturbed by something, what you can do is following steps:

(1). check whether every joint point of network is well（such as Ethernet port, antenna connection）

(2). Restart device.

(3). Default device and restore last settings.

(4). Please call the sales if can not solve problem after all.

Q 6. How to adjust output power?

In the Wireless Settings page, you can do it.

Diagram 7Output Power

	Full	1/2	1/4	1/8	Min
Output Power	18dbm	15dbm	12dbm	9dbm	6dbm

Q 7. Why device need ground?

If device need not ground, ETH port may reboot continuous or PING timed out and lost most packets. In order to avoid the harmful, the device needs ground. While you should do:

1) Electrical source ground

2) Ground port of device ground

Appendix A. Technical Specifications

Diagram 8 ZA-4000 Spec

802.11a Wireless Outdoor CPE	
	Main Features as follows: ♦ RoHS. ♦ Signal Status Display In Web. ♦ Signal Status Display by Led Line. ♦ TDM-QoS. ♦ PoE.
Model	**ZA-4000**
Description	ZA-4000 works at 5GHz, compatible with 802.11a standard designed as CPE. With the high throughput and long-distance transmission, it is the appropriate solution for Carriers, Service Providers and Enterprises. As outdoor remote client, ZA-4000 can make users easily build up broadband access system.
Feature	
Compliant Standards	IEEE 802.11a IEEE 802.3u IEEE 802.3af
Support Network Protocol	TCP/IP IPX NetBEUI
Data Transfer Rate	Best / 54 / 48 / 36 / 24 / 18 / 12 / 9 / 6 Mbps
Working Mode	Station, WDS(Client)
Signal Status Display In Web	Support
Signal Indicators	-92 <= dBm < -87 0LED ON -87 <= dBm < -67 1LED ON -67 <= dBm < -52 2LED ON -52 <= dBm < -47 3LED ON -47 <= dBm < -45 4LED ON -45 <= dBm <= 10 5LED ON

Firmware Upgrade	WEB,TFTP,FTP
Super Mode	Support
TDM-QoS(Client)	Support
NAT	Support
Linktest	Support
IP and MAC Access Control	Support
Interface	
LAN	One 10/100-BaseTX RJ-45 Ethernet Port
Antenna Type（Built-in）	built-in 18dBi antenna (12°×16°) (optional)
Antenna Type（External）	One N type(Female) interface(optional)
Default Button	Support
Ground Interface	Support
Led	1-POWER,1-WLAN,1-LAN,5-Signal Indicator
Electricity	
POE (Power over Ethernet)	Yes
Output Power	48V DC/0.83A, Compatible with IEEE 802.3af(optional)
Power Consumption	200mA@48V
Radio	
Modulation Type	America: 5.725GHz～5.825GHz Europe: 5.47GHz～5.725GHz China: 5.725GHz～5.850GHz Japan: 5.15GHz～5.25GHz
RF Output Power	16dBm (±1dBm)
Sensitivity	54 Mbps:≦-72dBm 48 Mbps:≦-73dBm 36 Mbps:≦-77dBm 24 Mbps:≦-81dBm 18 Mbps:≦-84dBm 12 Mbps:≦-86dBm

	9 Mbps: ≦-88dBm 6 Mbps: ≦-90dBm
Management	
Secure Web Management	Support
SNMP MIB	Support
SSH	Support
CLI	Support
BWA Viewer	Support
Security	
WEP Encryption	64 / 128 / 152 bits
WPA-PSK/WPA2-PSK	Support
Appearance	
Dimensions	292mm×288mm×84mm
Unite Weight	1.4kg
Specifications	
Working Temperature	-20～65℃
Store Temperature	-20～80℃
Waterproof Grade	IP65

Appendix B. Glossary

Diagram 9Glossary

Glossary	Expiation
802.11a	IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 5GHz. 802.11a provides specifications for wireless ATM systems and is used in access hubs. Networks using 802.11a operate at radio frequencies between 5.180 GHz and 5.825 GHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. In 802.11a, data speeds as high as 54 Mbps are possible.
Access Point	In a wireless local area network (WLAN), an Access Point is a station that transmits and receives data (sometimes referred to as a transceiver). An Access Point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each Access Point can serve multiple users within a defined network area; as people move beyond the range of one Access Point, they are automatically handed over to the next one. A small WLAN may only require a single Access Point; the number required increases as a function of the number of network users and the physical size of the network.
Infrastructure	In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless

	clients can freely roam from one Access Point domain to another and still maintain seamless network connection.
ESS	Short for the extended service set, One BSS or more builds one ESS. A station can connect or roaming ESS by ESSID of AP.
WEP	Wired Equivalent Privacy is a data encryption protocol for 802.11 wireless networks. All wireless nodes and access points on the network are configured with a 64-bit, 128-bit or 152-bit Shared Key for data encryption.
Access Control	This function is only valid under AP mode, invalid under the mode of bridge graft. Used in MAC address to filter.
Bridge	Bridge is the device that connects and transmits data packets with two subnets by the same protocol and it works in the LLC layer of OSI.
DHCP ， DHCP Client、DHCP Server	DHCP stands for "Dynamic Host Configuration Protocol". DHCP's purpose is to enable individual computers (DHCP Client) on an IP network to extract their configurations from a server (the DHCP server) or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.
Encryption	For the security of transmit data in network, the data should be encrypted before transmit and decrypt received data.
IP Address	Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP. A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.
LAN&WAN	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many

	technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
MAC Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.
NetBIOS	Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.
Ping	A command line program in Windows, use it to check the connection whether is reachable.
Router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Web-based Graphical User Interface (GUI)	In this kind of user interface, user can use Microsoft Internet Explorer or other browser to control, guard and manage the device.
WINS Server	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

Appendix C. ASCII

You can dispose hexadecimal number system counting or ACSII one yard of keys encrypted as WEP. Hexadecimal number system is made up by 0-9 and A-F (letter does not distinguish capital and small letter); ACSII yard is by 0-9 figures, A-F, a-f (letter distinguishes capital and small letter), and the punctuation mark makes up. Each ACSII yard can is it says to count by one hexadecimal number system of two. One-one ASCII yard of all and hexadecimal number system are counted to make forms and list all.

Diagram 10ASCII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Appendix D. SSH

Diagram 11 SSH

get	set	del	keyword				descriptions
√	√		system				--- system setting
√			version				--- system firmware version
√	√		apname				--- system name
√			macaddress				--- system MAC address
√	√		country				--- country/region
√	√		routemode				--- system route mode
√	√		anyiponroute				---system any ip on route mode
√	√		bridge				--- system bridge port
√	√			iptype			--- system dhcp client
√	√			ipaddr			--- system IP address
√	√			netmask			--- system network mask
√	√			gateway			--- system gateway
√	√			dns primary			--- system primary DNS
√	√			dns secondary			--- system secondary DNS
√	√		ethernet				--- system ethernet port
√	√			iptype			--- system dhcp client
√	√			ipaddr			--- system IP address
√	√			netmask			--- system network mask
√	√			gateway			--- system gateway
√	√			dns primary			--- system primary DNS
√	√			dns secondary			--- system secondary DNS
√	√			IP start			--- IP range start
√	√			IP End			--- IP range end
√	√			IP Range Netmask			--- IP range netmask
√	√		wireless				--- system wireless port
√	√			iptype			--- system dhcp client
√	√			ipaddr			--- system IP address
√	√			netmask			--- system network mask
√	√			gateway			--- system gateway
√	√			dns primary			--- system primary DNS
√	√			dns secondary			--- system secondary DNS
√	√			IP start			--- IP range start

√	√			IP End			--- IP range end
√	√			IPRange Netmask			--- IP range netmask
√	√		stp				--- enable spanning tree protocol
√			ethstats				--- ethernet statistics
√	√		radius				---radius setting
√	√			auth			---authentication radius setting
√	√				primary		---primary
√	√					ipaddr	---radius IP address
√	√					port	---radius port number
√	√					secret	---radius secret string
√	√				secondary		
√	√					ipaddr	---radius IP address
√	√					port	---radius port number
√	√					secret	---radius secret string
√	√			account			
√	√				primary		---primary
√	√					ipaddr	---radius IP address
√	√					port	---radius port number
√	√					secret	---radius secret string
√	√				secondary		
√	√					ipaddr	---radius IP address
√	√					port	---radius port number
√	√					secret	---radius secret string
√	√		ssh				--- enable remote SSH access
√	√		snmp				--- SNMP setting
√	√			server			--- enable SNMP agent
√	√			trap server			--- SNMP TrapServer IP address
√	√			read community			--- SNMP Readcommunity
√	√			write community			--- SNMP Writecommunity
√	√			description			--- SNMP System Description
√	√	√	wlan				--- wireless setting
√	√			radio			--- enable wireless radio
√	√			wirelessmode			--- wireless mode
√	√			channel			--- wireless channel(depends on country and wireless

							mode)
√	√			rate			--- wireless transmission data rate
√	√			ssid			--- wireless network name(1-32chars)
√	√			power			--- wireless transmit power
√	√			tdm			---enable TDM mode or not
√	√			antenna			---wireless antenna selection
√	√			fragmentationthreshold			--- wireless fragmentation threshold (even only)
√	√			rtsthreshold			--- wireless RTS/CTS threshold
√	√			super			--- enable Super-A/G mode
√	√			beaconinterval			--- wireless beacon period in TU(1024us)
√	√			dtim			--- wireless DTIM period in beacon interval
√	√			preamble			--- wireless preamble(only effect on 802.11b rates)
√	√			wirelessisolate			--- wireless isolate communication between clients
√	√			oprationmode			--- wireless operation mode
√	√	√		remoteap			--- wireless remote AP(s) (depends on oprationmode)
√	√	√			p2p(+ap)		--- remote ap address for p2p mode
√	√	√			p2mp(+ap)		--- remote ap address for p2mp mode
√	√	√				1	--- 1st remote ap address for p2mp mode
√	√	√				2	--- 2nd remote ap address for p2mp mode
√	√	√				3	--- 3rd remote ap address for p2mp mode
√	√	√				4	--- 4th remote ap address for p2mp mode
√	√	√				5	--- 5th remote ap address for p2mp mode
√	√	√				6	--- 6th remote ap address for p2mp mode
√	√	√				7	--- 7th remote ap address for

							p2mp mode
√	√	√				8	--- 8th remote ap address for p2mp mode
√	√	√	acl				--- wireless access control
√	√			mode			--- enable wireless access control (ACL)
√	√	√		list			---
		√			all		--- (delete only) all local ACL address
√	√	√			null		--- edit local ACL address
√			association				--- list of associated wireless clients
√			wlanstats				--- wlan statistics
√	√		authentication				--- wireless authentication type
√	√		encryption				--- wireless data encryption
√	√	√	key				--- wireless wep key setting
√	√			type			--- wireless wep key type
√	√			default			--- wireless wep default key index
√	√	√		passphrase			--- wireless wep passphrase key
√	√	√		1			--- wireless wep key 1
√	√	√		2			--- wireless wep key 2
√	√	√		3			--- wireless wep key 3
√	√	√		4			--- wireless wep key 4
√	√	√	wpa				--- wireless WPA setting
√	√	√		psk			--- wireless pre-shared key (PSK) for WPA-PSK
√	√			reauthtime			--- wireless WPA re-auth period (in seconds)
√	√			keyupdate			--- enable wireless WPA global key update
√	√				mode		--- wireless WPA global key update condition
√	√				interval		--- wireless WPA global key

							update interval
√	√					sec	--- wireless WPA global key update interval (in seconds)
√	√					pkt	--- wireless WPA global key update interval (in packets)
√	√		SmartWDS				--- SmartWDS settings
√	√			ID			--- Auto WDS ID
√				remotes			--- Auto WDS remote AP list
√				status			--- Auto WDS status
√	√		spaceinmeter				--- wireless space in meter
√	√		maxrssi				--- wireless max rssi
√	√		RFlinewaste				--- RF line waste
√	√		localplus				--- local plus
√	√		remoteplus				--- remote plus
√	√		testremotemac				--- remote test mac
√	√		linktime				--- MIB_WLAN_LINK_TIME
√	√		linkpktsize				--- MIB_WLAN_LINK_PKT_SIZE
√	√		linkpktinterval				--- MIB_WLAN_LINK_TEST_INTERVAL
√	√		linkaction				--- MIB_WLAN_LINK_ACTION
	√		password				--- system password
	√		reboot				--- reboot system
	√		exit				--- logout from CLI
	√		quit				--- quit CLI

Warning:

Statement:

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.

Note:

Class B:

FEDERAL COMMUNICATIONS 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 or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

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

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

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could

void the user's authority to operate the equipment.

RF exposure warning

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.