# ZA-5000 Series

# (ZA-5000-I/ZA-5000-E)

# User's Manual

V2.2.5

## 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:**

- This indicates an important Note.

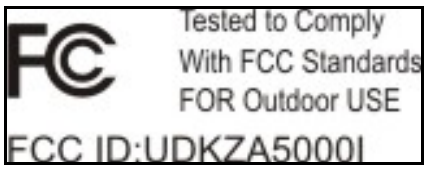
**Warning:**

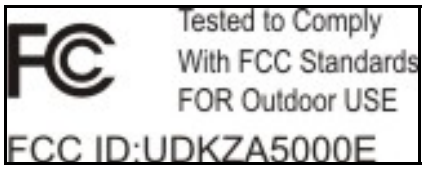
- This indicates a warning or caution.

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

## Federal Communications Commission (FCC) Compliance Notice:

## Radio Frequency Notice




**This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:**

- **This device may not cause harmful interference.**
- **This device must accept any interference received, including interference that may cause undesired operation.**

# 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.**

**Use only shielded cables to connect I/O device to this equipment. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.**

## 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.**

# FCC DECLARATION OF CONFORMITY

## DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2.1077(a)

The following equipment:

| | | |
|---|---|---|
| Product Name | : | 54Mbps Wireless Outdoor Bridge |
| Model Number | : | ZA-5000-I |
| Trade Name | : | ZDC |

It's herewith confirmed to comply with the requirements of FCC Part 15 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.

The result of electromagnetic emission has been evaluated by QuieTek EMC laboratory (NVLAP Lab. Code : 200743-0)

It is understood that each unit marketed is identical to the device as tested, and any changes to the device that could adversely affect the emission characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:

| | | | |
|---|---|---|---|
| Company Name | Nanjing Z-Com Wireless Co., Ltd. | | |
| Company Address | 168 Long Pan Zhong Road, Jiangsu Software Park, Suite 118, Nanjing 210002, China | | |
| Telephone | +86-25-84661314 | Facsimile | +86-25-84661313 |

Person is responsible for marking this declaration:

| | |
|---|---|
| Jason Wang | Product Manager |
| Name (Full name) | Position / Title |
| 2006/06/30 | Jason Wang |
| Date | Legal Signature |

# DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2.1077(a)

The following equipment:

| | | |
|---|---|---|
| Product Name | : | 54Mbps Wireless Outdoor Bridge |
| Model Number | : | ZA-5000-E |
| Trade Name | : | ZDC |

It's herewith confirmed to comply with the requirements of FCC Part 15 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.

The result of electromagnetic emission has been evaluated by QuieTek EMC laboratory (NVLAP Lab. Code : 200743-0)

It is understood that each unit marketed is identical to the device as tested, and any changes to the device that could adversely affect the emission characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:

| | |
|---|---|
| Company Name | Nanjing Z-Com Wireless Co., Ltd. |
| Company Address | 168 Long Pan Zhong Road, Jiangsu Software Park, Suite 118, Nanjing 210002, China |
| Telephone | +86-25-84661314 Facsimile +86-25-84661313 |

Person is responsible for marking this declaration:

| | |
|---|---|
| Jason Wang | Product Manager |
| Name (Full name) | Position / Title |
| 2006/06/30 | Jason Wang |
| Date | Legal Signature |

**Europe – EU Declaration of Conformity** CE 0678①

# Declaration of Conformity

The following product is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the laws of the Member States relating to R&TTE Directive(1999/5/EC)· Low Voltage Directive 73/23/EEC, The listed standards as below were applied:

The following Equipment:

| | | |
|---|---|---|
| Product | : | 54Mbps Wireless Outdoor Bridge |
| Model Number | : | ZA-5000-D / ZA-5000-E / ZA-5000-I |
| Trade Name | : | ZDC |

This product is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the laws of the Member States relating to R&TTE Directive(1999/5/EC)· Low Voltage Directive 73/23/EEC,the following standards were applied:

| | |
|---|---|
| **ETSI EN 301 489-1:V1.6.1 (2005-09)** | **EN 55022:1998+A1: 2000+A2: 2003** |
| **ETSI EN 301 489-17:V1.2.1 (2002-08)** | **EN 61000-3-2:2000+A1: 2001** |
| **ETSI EN 300 328:V1.6.1 (2004-11)** | **EN 61000-3-3:1995+A1: 2001** |
| **ETSI EN 301 893:V1.2.1(2002-07)** | **EN 61000-4-3:2002+A1: 2002** |
| **EN 60950(2001)** | **EN 61000-4-4:1995+A1: 2001+A2: 2001** |
| | **EN 61000-4-5:1995+A1+ 2001** |
| | **EN 61000-4-6:1996 +A1: 2001** |
| | **EN 61000-4-11:1994+A1: 2001** |

The following importer/manufacturer is responsible for this declaration:

| | | |
|---|---|---|
| Company Name | : | Nanjing Z-Com Wireless Co., Ltd. |
| Company Address | : | 168 Long Pan Zhong Road, Jiangsu Software Park, Suite 118<br>Nanjing 210002, China |
| Telephone | : | +86-25-84661314 Facsimile: +86-25-84661313 |

Person is responsible for marking this declaration:

| | |
|---|---|
| Jason Wang | Product Manager |
| Name (Full Name) | Position/ Title |
| 2006/06/30 | Jason Wang |
| Date | Legal Signature |

# Content

**Chapter 1 Introduction.....1**

Introduction.....1

Appearance of Product.....1

Features and Benefits.....2

Network Construct.....2

Representative Application.....4

**Chapter 2 Hardware Installation.....6**

System Requirement.....6

Product Kit.....6

Hardware Installation.....6

Antenna Installation.....8

**Chapter 3 Basic configuration.....10**

Default Settings.....10

Using the Web Management.....11

Set the Basic Configuration.....12

Set the Basic Wireless Parameters.....15

Outdoor Point to Point Bridge Application.....17

**Chapter 4 Advanced Configuration.....18**

RADIUS.....18

Security Setup.....18

Access Control List Setup.....18

Hidden SSID Setup.....18

Wireless Isolation.....18

Configure as a Router.....18

AnyIP.....18

SuperA Application.....18

SmartWDS Application.....18

Outdoor Point to Multi-Point Bridge Application....18

Outdoor Wireless Cover Application....18

"AP + Bridge" Mode Application....18

**Chapter 5 Management....18**

View the General Information....18

View the STA List....18

View the Device's Link Status....18

Change Login Password....18

Firmware Upgrade....18

Backup/Restore Settings....18

Restore to Factory....18

Reboot AP....18

SNMP Management....18

SSH Management....18

**Chapter 6 Troubleshooting....18**

FAQ....18

Technology Support....18

**Appendix A. Technical Specifications....18**

**Appendix B. Glossary....18**

**Appendix C. ASCII....18**

**Appendix D. SSH....18**

# Content of Figure

Figure 1 ZA-5000-I....1

Figure 2 ZA-5000-E....2

Figure 3 Point to Point....3

Figure 4 Point to Multi Point....3

Figure 5 Wireless Repeater....4

Figure 6 Access Point....4

Figure 7 Security Alarm ..... 11
Figure 8 login ..... 11
Figure 9 General Page ..... 12
Figure 10 Basic Setup ..... 12
Figure 11 Wireless Settings ..... 15
Figure 12 Point to Point Connection ..... 18
Figure 13 Link Test ..... 18
Figure 14 Link Test Signal ..... 18
Figure 15 RADIUS ..... 18
Figure 16 Security Settings ..... 18
Figure 17 Access Control List ..... 18
Figure 18 RADIUS MAC Access Control ..... 18
Figure 19 Hidden SSID Setup ..... 18
Figure 20 Wireless Client Security Separator ..... 18
Figure 21 Wireless Separator ..... 18
Figure 22 Router ..... 18
Figure 23 Wireless Router (Bridge Mode)—WAN on Ethernet ..... 18
Figure 24 Wireless Router (Bridge Mode)—WAN on Wireless ..... 18
Figure 25 AP Router ..... 18
Figure 26 “AP + Bridge” Router ..... 18
Figure 27 AnyIP ..... 18
Figure 28 Super A ..... 18
Figure 29 SmartWDS ..... 18
Figure 30 Outdoor Wireless Cover Application ..... 18
Figure 31 AP Settings ..... 18
Figure 32 “AP + Bridge” Mode Application ..... 18
Figure 33 General ..... 18
Figure 34 STA List ..... 18
Figure 35 Link Statistics ..... 18
Figure 36 Change Login Password ..... 18

Figure 37 Firmware Upgrade ..... 18
Figure 38 Backup/Restore Settings ..... 18
Figure 39 Restore to Factory ..... 18
Figure 40 Default Button ..... 18
Figure 41 Reboot AP ..... 18
Figure 42 SNMP ..... 18
Figure 43 Putty Settings 1 ..... 18
Figure 44 Putty Settings 2 ..... 18
Figure 45 SSH ..... 18
Figure 46 MAC Address ..... 18

# Content of Table

Diagram 1 Default Settings ..... 10
Diagram 2 Country/Region frequency list (5GHz frequency band） ..... 14
Diagram 3 Channel/Frequency List（5GHz） ..... 16
Diagram 4 Signal Strengthen and buzzer sound list ..... 18
Diagram 5 Signal Strengthen and Throughput List ..... 18
Diagram 6 Distance and Signal Strengthen ..... 18
Diagram 7 Super A Function and Throughput ..... 18
Diagram 8 RF Path Loss ..... 18
Diagram 9 Output Power ..... 18
Diagram 10 ZA-5000-I Spec ..... 18
Diagram 11 ZA-5000-E Spec ..... 18
Diagram 12 Glossary ..... 18
Diagram 13 ASCII ..... 18
Diagram 14 SSH ..... 18

# Chapter 1 Introduction

## Introduction

The next-generation Broadband Wireless Access device－ZA-5000－a new high-speed wireless bridge aimed at last-mile broadband wireless access (BWA) links and campus data networks that need to send large amounts of data over the air. By enabling corporations and ISPs to bridge the gap between multiple buildings without incurring the expense of leased lines or fiber runs, ZA-5000 offers fast return on investment while providing optimal network performance. ZA-5000-I build in 5GHz antenna, ZA-5000-E with external antenna.

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

## Appearance of Product

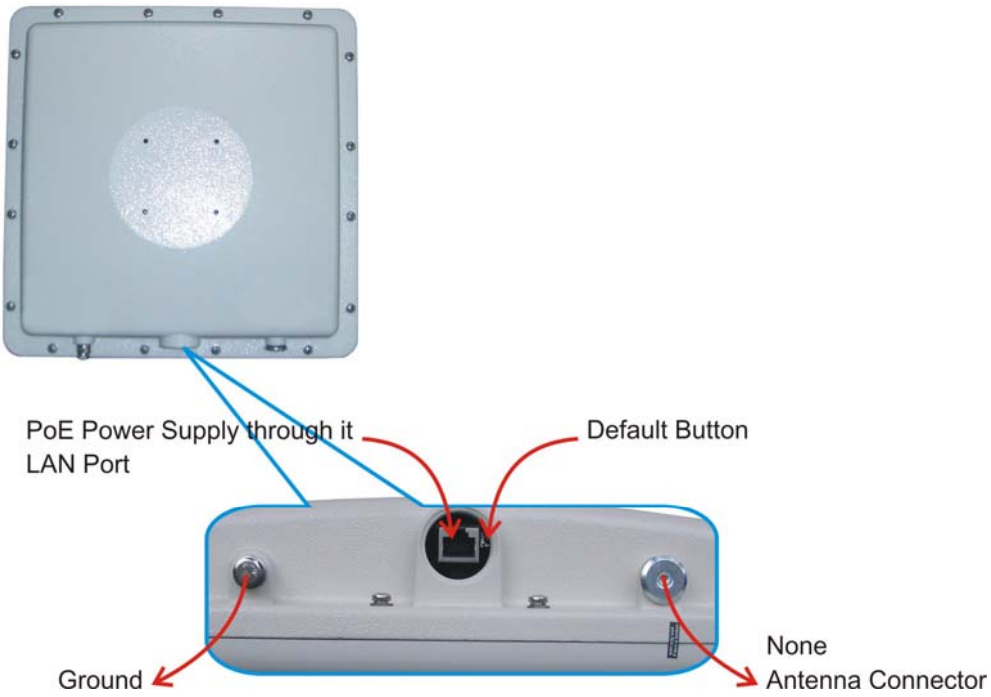



**Figure 1 ZA-5000-I**

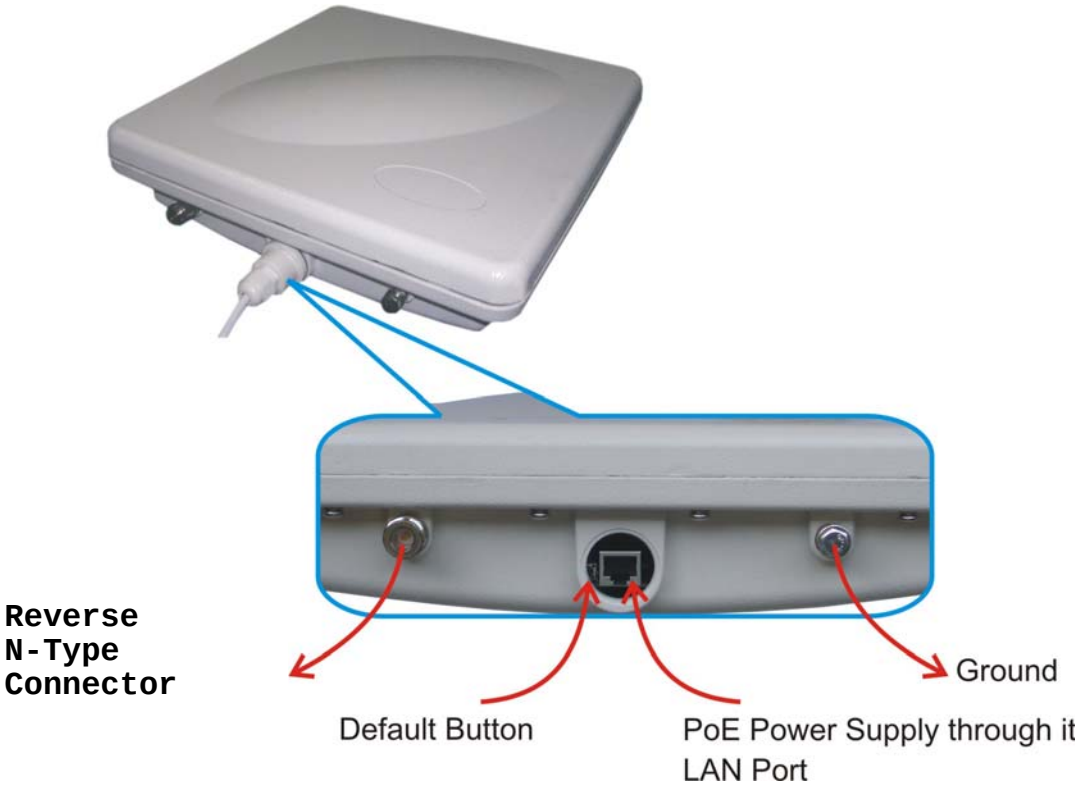



**Figure 2 ZA-5000-E**

# Features and Benefits

- Support power over Ethernet
- Waterproof and can place into outdoor directly
- Test-link utility helps you to place your antenna in the best position
- MAC address control
- Provides Web-based configuration utility
- Special SmartWDS Function is easy to build network

# Network Construct

- Outdoor Point to Point

  Application condition: This solution is used in connecting two networks in different places, such as headquarter and branch, network center and residential area.

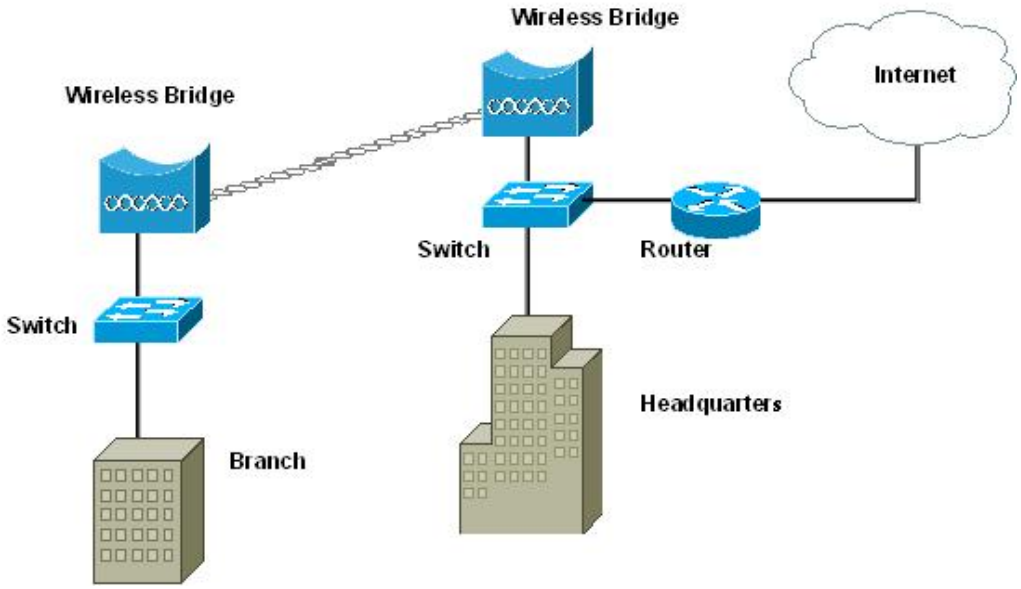



**Figure 3 Point to Point**

- Outdoor Point to Multi Point

  Application condition: In this solution, there is always a network center point connecting with several remote points to build wireless bridge. It will provide broad band service for several enterprises and its cost is low, construction period is short. It is the better choice for ISP.

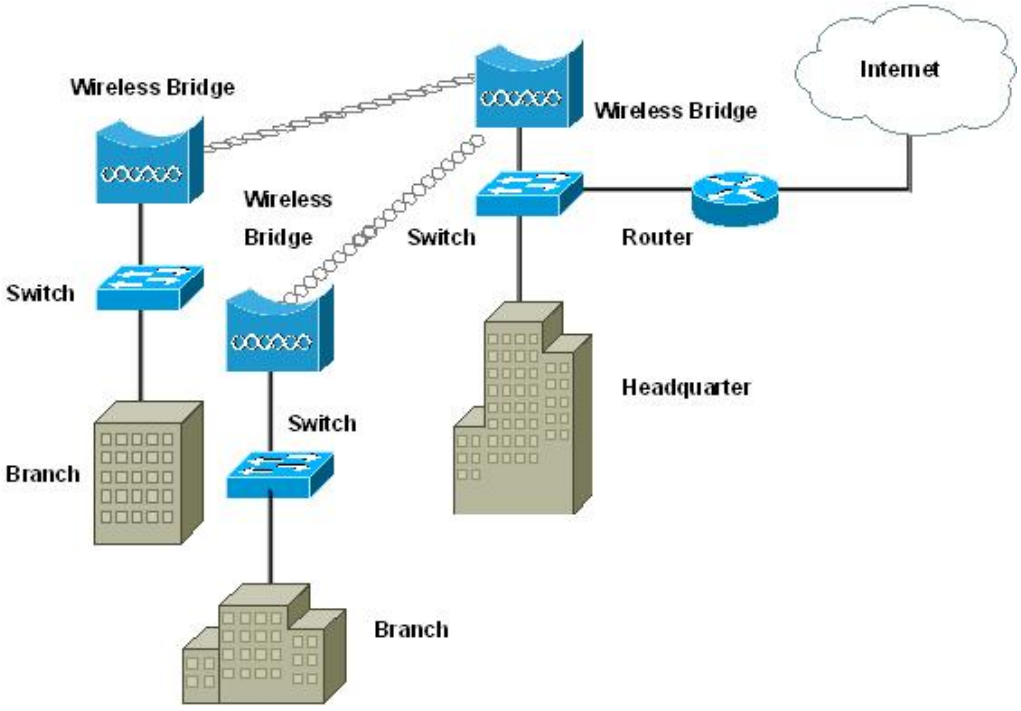



**Figure 4 Point to Multi Point**

- Wireless Repeater

  Application condition: This solution is used for builds wireless repeater bridge between two

places which there are long distance and can not be visual.

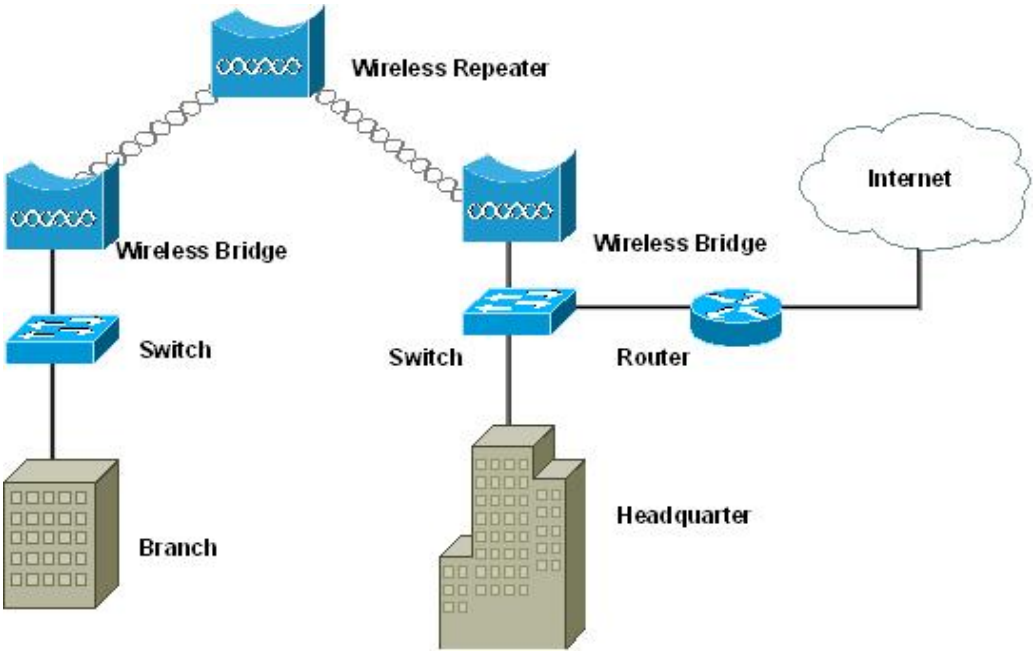



**Figure 5 Wireless Repeater**

- Access Point

Application condition: This solution is used for mobile office places.

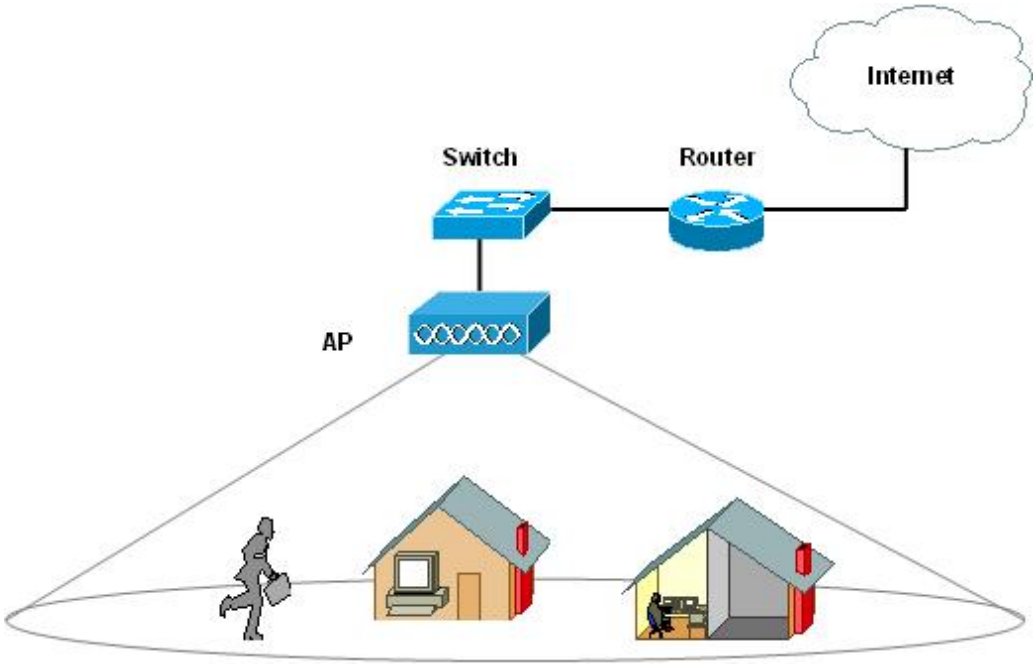



**Figure 6 Access Point**

# Representative Application

The Access Point offers a fast, reliable, cost-effective solution for wireless client access to the

network in applications like these:

- Remote Access to Corporate Network Information

  E-mail, file transfer and terminal emulation.

- Difficult-to-Wire Environments

  Historical or old buildings, asbestos installations, and open area where wiring is difficult to deploy.

- Frequently Changing Environments

  Retailers, Manufacturers and those who frequently rearrange the workplace and change location.

- Temporary LANs for Special Projects or Peak Time

  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.

- Access to Database for Mobile Workers

  Doctors, nurses, retailers, accessing their database while being mobile in the hospital, retail store or office campus.

- SOHO (Small Office and Home Office) Users

  SOHO users need easy and quick installation of a small computer network.

- High Security Connection

  The secure wireless network can be installed quickly and provide flexibility.

# Chapter 2 Hardware Installation

## System Requirement

- Two PCs with RJ-45 connector NIC supporting the transfer rate of 10/100Mbps data.
- The IP address of NIC should be the same subnet with the AP, the default IP address of AP is 192.168.0.228.
- Microsoft Internet Explorer 6 updated with Service Pack 1 or the newer patch Q323308.

## Product Kit

- Wireless Device×1
- Power Module×1
- Fixed settings×1
- Product CD×1

## Hardware Installation

Take the following steps to set up the ZA-5000-E (the different of hardware installation between ZA-5000-E and ZA-5000-I is antenna.).

1. All the parts of product are shown as following picture.

2. You should fix the Access Point, the following figure shows it.
3. Put a Cat-5e STP (Shielded twisted pair) cable with RJ-45 connector through the water-joint. If there no such cable, Make the RJ-45 connector as the following rules:

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

4. Attach STP cable to the RJ-45 connector on the Access Point. Then connect another end of the RJ-45 cable to a hub or a terminal.

5. Plug water-joint into the Access Point and tighten it.

6. Attach the external antenna to Access Point. ( There is an inner antenna inside ZA-5000-I which no need of external antenna)

7. Connect the Access Point to the ground via ground connection which is beside the RJ-45 port.


Thus all, the hardware installation is completed.

**Notice:**

- While there is build-in buzzer inside ZA-5000, users can adjust antenna by the buzzer. Before adjusting antenna, please do not tighten waterproof joint, otherwise you can possibly not hear sound of buzzer.
- There is a plastic film covering the build-in antenna. Please tear this film while using ZA-5000.

**Warning:**

- Please confirm ground connection of the Access Point.
- Please confirm ground connection of the STP cable, and traverse an EMI suppression ferrite ring core.

# Antenna Installation

There is an inner antenna inside ZA-5000-I which no need of external antenna

The ZA-5000-E needs an external antenna.

**You just can use the antenna offered by manufacturer.**

**Warning:**

- Please do not put Access Point near these places: electric power line, electric light, electricity or any places nearby strong electric power, otherwise it may make damage to Access Point.
- The inner Antenna Lightning Protection is in base level. You should add advanced Antenna Lightning Protection if condition possible.

**Note:**

**ZA-5000-D will automatically discontinue transmissions when ether absence information to transmit or operational failure, ZA-5000-D use the module AG-621, FCC ID:M4Y-0AG621**

# Chapter 3 Basic configuration

## Default Settings

**Diagram 1 Default Settings**

| Options | Default Value |
|---|---|
| User Name | admin |
| password | password |
| Access Point Name | APxxxxxx（xxxxxx indicate the last 6 MAC address of AP） |
| Country/Region | China |
| Spanning Tree | Enable |
| IP Address | IP Type: STATIC<br>IP Address :192.168.0.228<br>Mask ： 255.255.255.0<br>Gateway：0.0.0.0<br>DNS Server：0.0.0.0 |
| Bridge Mode | Bridge |
| Operating Mode | 802.11a |
| Channel/Frequency | 149/5.745GHz |
| Data rate | Best |
| Output Power | Full |
| RTS Threshold | 2346 |
| Fragment Threshold | 2346 |
| Super A | OFF |
| SSID | Wireless |
| Beacon Interval | 100 |
| DTIM Interval | 1 |
| Broadcast SSID | Yes |
| Enable Wireless Client Security Separator | No |
| Wireless Separator | No |
| Space between Bridge | 5000 |
| Buzzer Switch | OFF |
| WEP | Disable |
| Access Control | Disable |
| Link Test | RF Cable Loss: 2 |
| | Local Antenna Gain: 6 |
| | Remote Antenna Gain: 6 |
| | Test Interval: 50 |

| | |
|---|---|
| | Test Packet Size: 64 |
| | Test Time: 300 |
| SNMP | SNMP：Enable<br>Trap Server：192.168.0.254<br>Read Community：public<br>Write Community：private |

# Using the Web Management

The Web Management provides you with a user-friendly graphical user interface. The Access Point allows you via web browser (MS Internet Explorer 6.0) to monitor and configure the device.

1. Run Web Explorer, Enter default IP Address: **http://192.168.0.228** in the Address field. After press Enter key then pop up a security alarm page, the page will show up:


**Figure 7 Security Alarm**

2. Click yes button, the login page will show up.

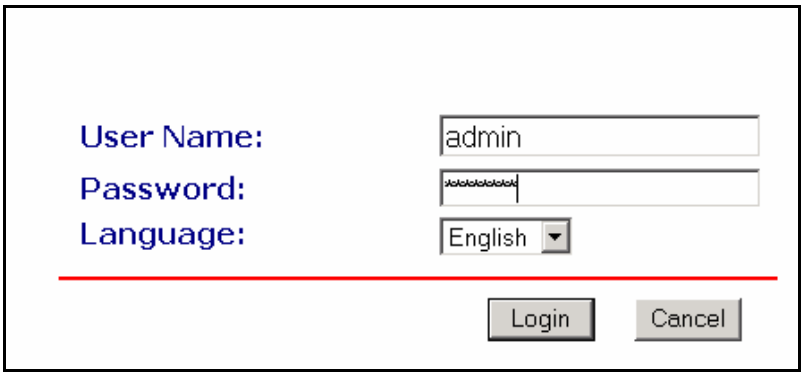



**Figure 8 login**

3. Enter default User Name (admin) and default Password (password), Click Login. The home

page will show up.

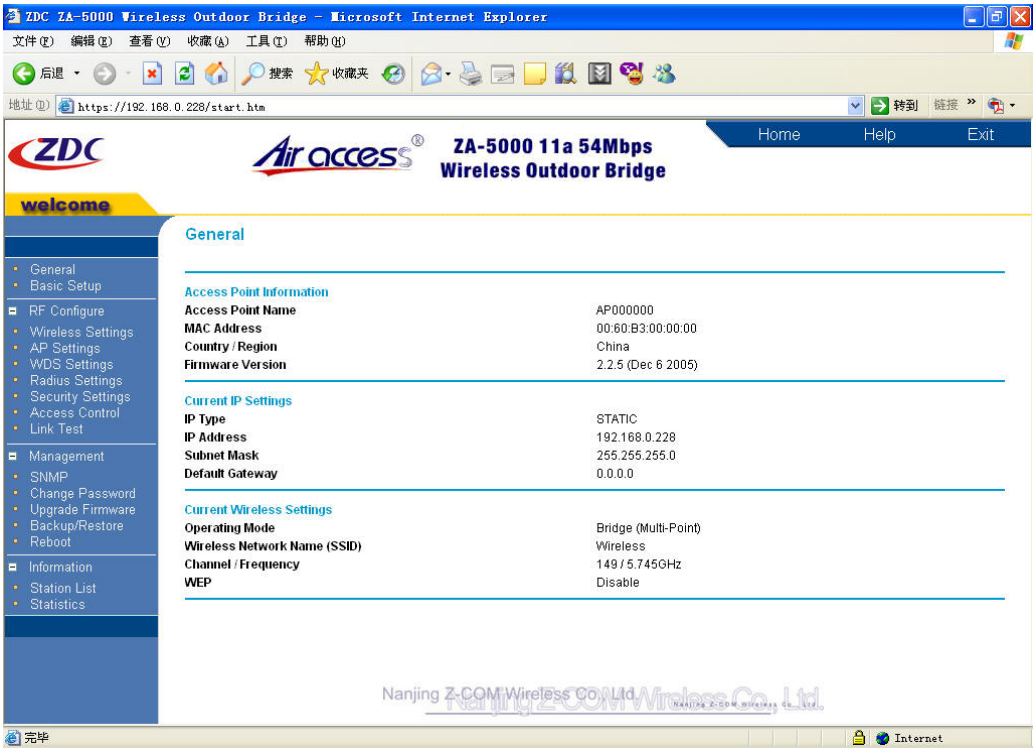



**Figure 9 General Page**

# Set the Basic Configuration

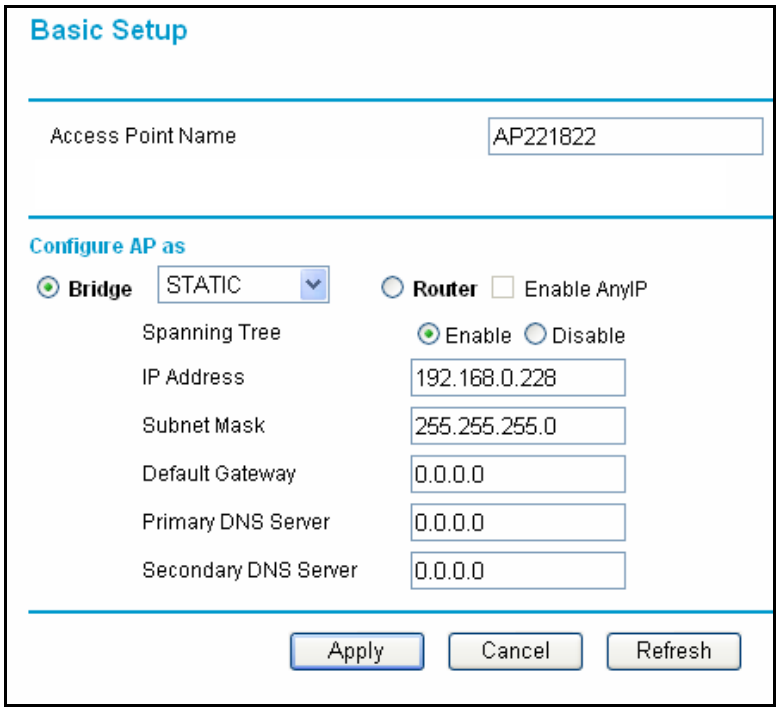



**Figure 10 Basic Setup**

- **Access Point Name**

  This is the NetBIOS name of Access Point; you may modify the default name with a unique name up to 15 characters long including numbers from 0 to 9, letters (A-Z; a-z) and digraphs (-), the name supports WINS so you can ping Access Point using “ping Access Point Name” or use web browser to open web utility by inputting Access Point Name in the IE address.

**Notice:**

- The default Access Point Name is: APxxxxxx (xxxxxx represents the last 6 digits of MAC address.
- The first character of Access Point Name cannot be digits.
- Your host must have a TCP/IP address with the same subnet as the Access Point while using WINS.

- **Country/Region**

  **USA use only.**

- **Configure AP as**

  Configure AP as Bridge or Router, in Bridge mode; you can configure IP address, subnet mask, gateway, Primary DNS Server and Secondary DNS Server. The configuration of Router mode is in Chapter **Configure AP as a Router**.

- **IP Address**

  There two type in Bridge mode:

  - Static IP: You should manually configure IP address, subnet mask, gateway, Primary DNS Server and Secondary DNS Server. The Access Point will automatically calculate the subnet mask based on the assigned IP address. Otherwise, you can use 255.255.255.0

as the subnet mask.

- DHCP Client: AP can get IP settings from DHCP Server.

- **Spanning Tree**

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

# Set the Basic Wireless Parameters

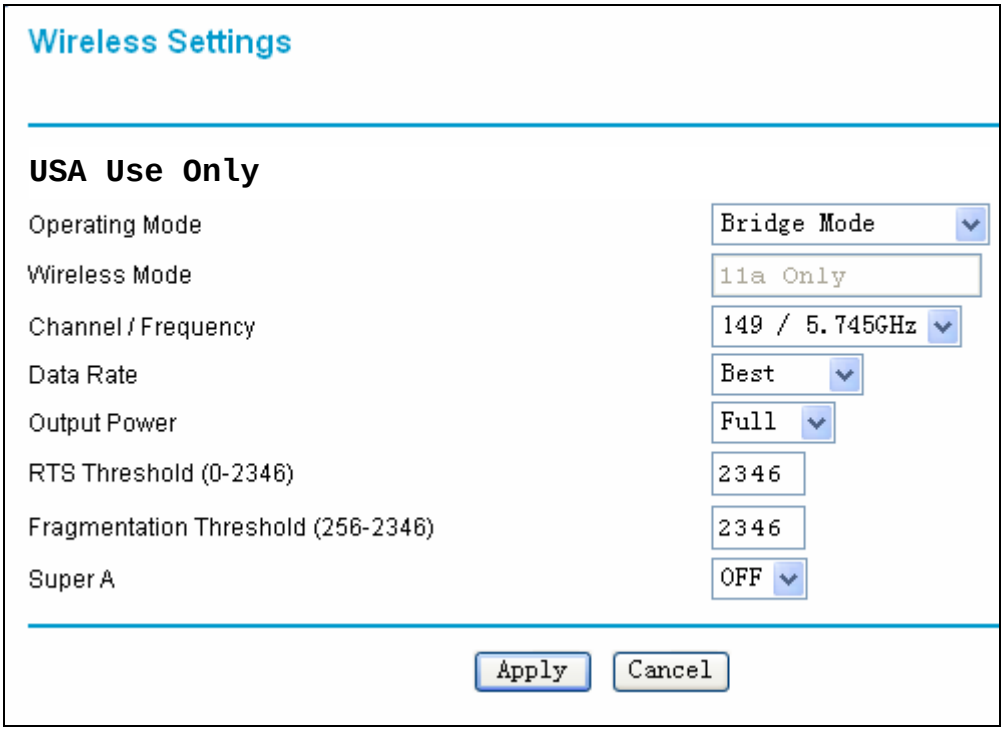



**Figure 11 Wireless Settings**

- **Operating Mode**
  - AP mode: This mode is used to build infrastructure network which allowing station connection.
  - Bridge mode: This mode is used to build WDS network which allowing other wireless bridge connection.
  - AP + Bridge Mode: This mode allows both station and wireless bridge connection.

- **Channel/Frequency**

  Select the channel that you plan to use.

**Diagram 3 Channel/Frequency List（5GHz）**

| Channel | Centre Frequency（MHz） |
|---|---|
| 149 | 5745 |
| 153 | 5765 |
| 157 | 5785 |
| 161 | 5805 |

- **Data Rate**

  The available transmit data rate of the wireless network. The AP will choose the highest data rate to transmit data in Best mode. You also can choose lower data rate in order to transmit data in longer distance.

- **Output Power**

  **You can't adjust the output power.**

- **RTS Threshold**

Request to Send Threshold. Its value is from 0 to 2346 bytes, RTS is designed to solve Network collision. It will make signals lose if two stations send data to AP at the same time. When the transmitted data size is larger than RTS threshold, the RTS mechanism will be active. 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. The other station which have listen the CTS will waits for a time before send data. The default value is 2346 and not active. If set it to zero, this function will be active always.

- **Fragmentation Threshold**

  This is the maximum packet size used for fragmentation and can only be set as even number. Packets larger than the size programmed in this field will be fragmented. The little packet data can reduce loses and raises the quality of transmission.

✎ **Notice:**

- The Fragment Threshold value should be larger than the RTS Threshold value or the RTS Threshold is zero, otherwise the RTS function will not work.

# Outdoor Point to Point Bridge Application

The wireless bridge between outdoor two places is the main application condition, here we will introduce you how to build such network quickly

We suggest you should first builds networks between two wireless bridges indoor and the connection is normal then take them outdoor.

Access Points builds connection by WDS (Wireless Distribution System) mode. The main setting is remote MAC address. The following steps are the way. Step from 1 to 5 is taken indoor; step 6 should take Access Points outdoor.

**1.** After power on two Access Points, use two notebook computers to connect each of them by network cable. As the following figure. Sets the IP address.

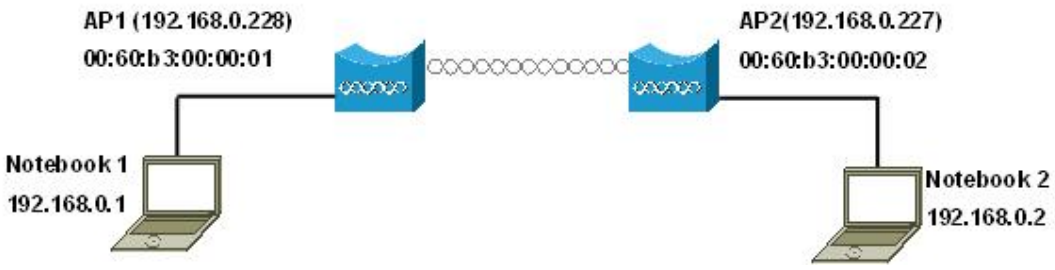



**Figure 12 Point to Point Connection**

**2.** Open the AP web configuration by using IE with IP of 192.168.0.228, user name of admin and password of password. Open "WDS Settings" page, choose "Wireless Point-to-Point Bridge" and add MAC address of remote wireless bridge. As following figure.

✎ **Notice:**

- You should set the two Access Points different IP addresses in order to expediently manage them.

**3.** After above configuration, open buzzer switch and you will hear the sound of buzzer switch. The times of continuous sound indicate the signals strengthen between two Access Points.

**Diagram 4 Signal Strengthen and buzzer sound list**

| Signal Strengthen Percent | Times of continuous Buzzer Switch sound |
|---|---|
| 0%<= P <=10% | 0 |
| 10%< P <=50% | 1 |
| 50%< P <=60% | 2 |
| 60%< P <=80% | 3 |
| 80%< P <=90% | 4 |
| 90%< P <=100% | 5 |

To confirm the right connection of wireless network, you can use "ping" program. At the local notebook computer (192.168.0.1), ping 192.168.0.228, ping 192.168.0.227, ping 192.168.0.2.

If the buzzer switch does not work or the ping is timed out, please take a reference to chapter "**Troubleshooting**".

**4.** Now the two Access Points have normally worked. You can change settings account to your need. The detail about changing settings is in above chapter. After all, you should make sure than notebook1 and notebook2 are connecting well.

**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.

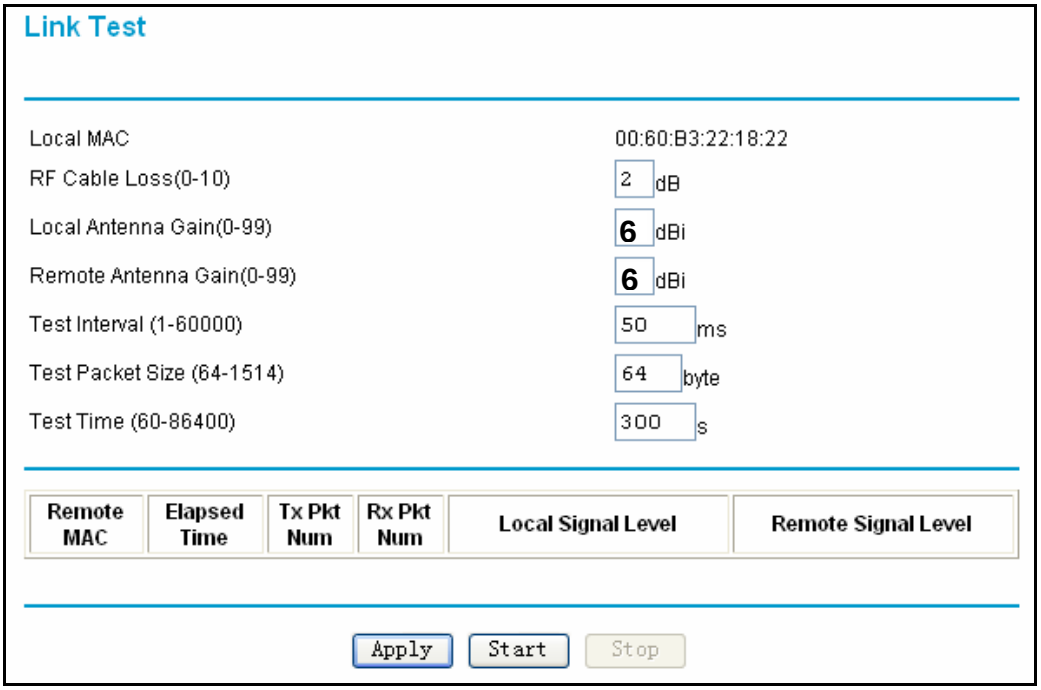



**Figure 13 Link Test**

**Notice:**

- 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.

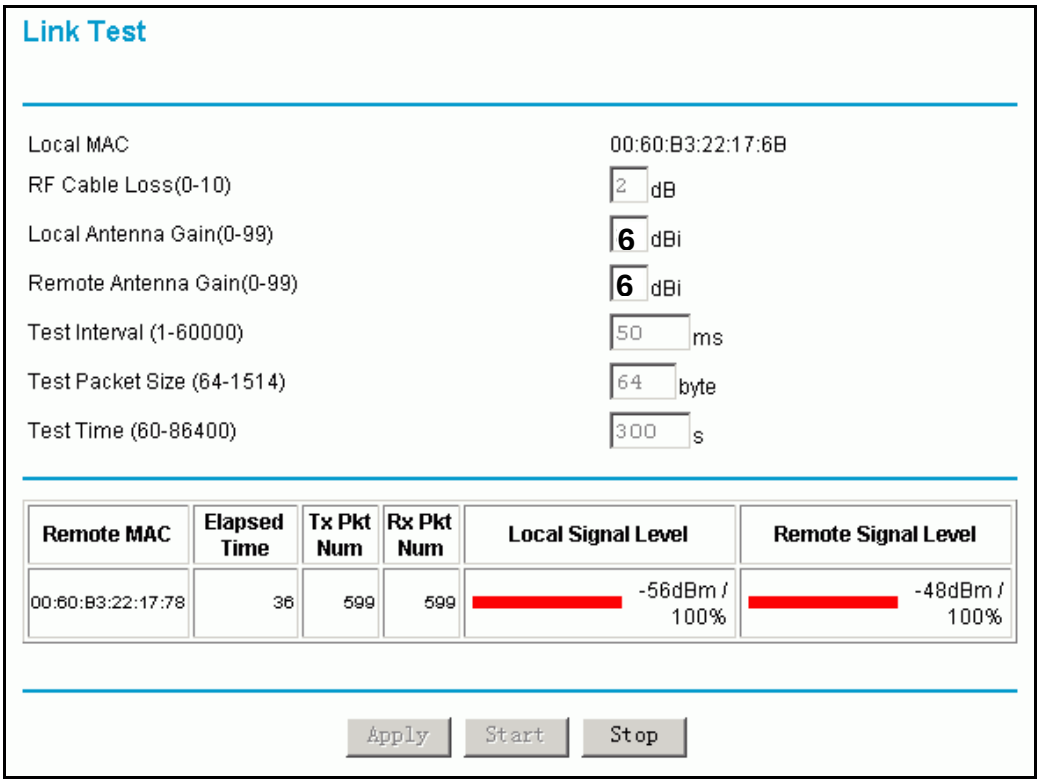



**Figure 14 Link Test Signal**

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 5 Signal 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:**

- 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.
- 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.

**6.** Take the Access Points outdoor and do “Link Test”.

Normally, after the step from 1 to 5, move the Access Points outdoor, they can work well only make sure that there are direct visual space between them. The only thing you should do is to adjust the antenna to best angel to get the best signal strengthen. The following table shows those values.

**Diagram 6 Distance 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.

# Chapter 4 Advanced Configuration

## RADIUS

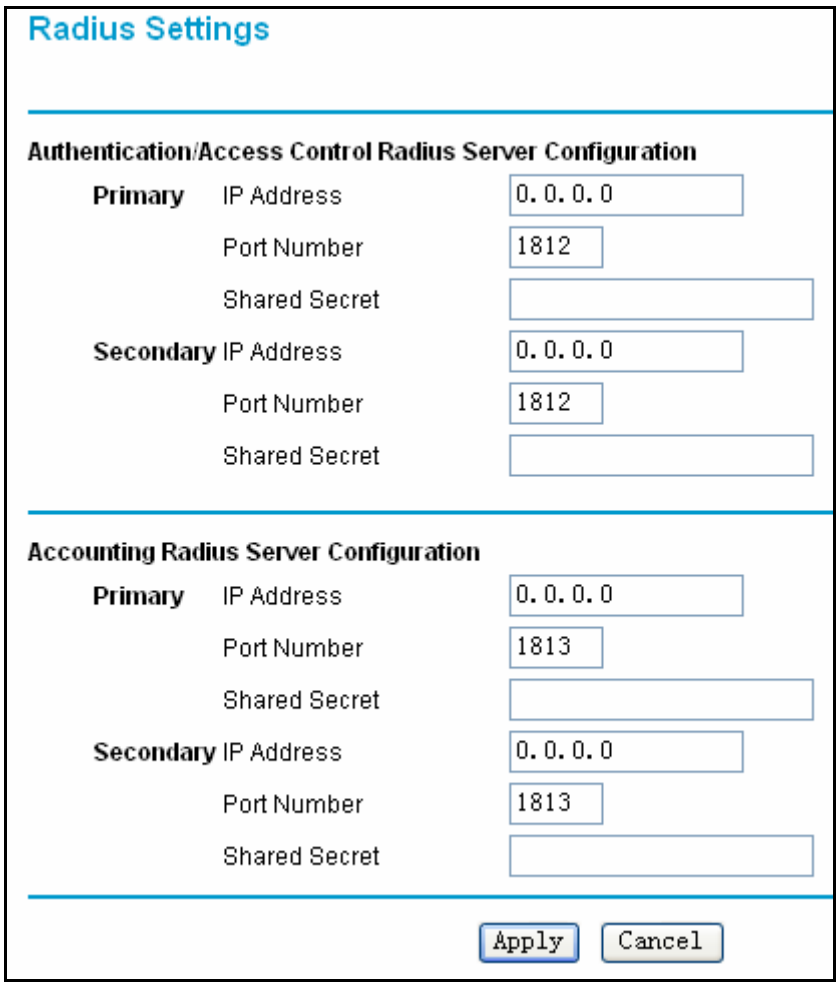



**Figure 15 RADIUS**

RADIUS (Remote Authentication Dial-In User Service) plays a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing and alarming…etc and allows an organization to maintain user profiles in a central database that all remote servers can share. Since RADIUS is relatively complex to explain, we will focus here on how it acts as an 802.1x authentication server (EAP-aware RADIUS) and assists in enhancing security.

RADIUS performs the authentication function required to check the credentials of users and intermediate Access Points and indicates whether the users are authorized to access the Access Points. Enabling RADIUS is therefore the first step toward building up an 802.1x-capable

environment. Even more, it is also a must-do to accommodate the recently introduced Wi-Fi protected access (WPA-EAP) to wireless networks.

- **Authentication/Access Control Radius Server Configuration**

  This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.

  - IP Address: IP address of the Radius Server. The default is 0.0.0.0
  - Port Number: Port number of the Radius Server. The default is 1812.
  - Shared Secret: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

- **Accounting Radius Server Configuration:**

  This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.

  - IP Address: The IP address of the Radius Server. The default is 0.0.0.0
  - Port Number: Port number of the Radius Server. The default is 1813.
  - Shared Secret: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

# Security Setup

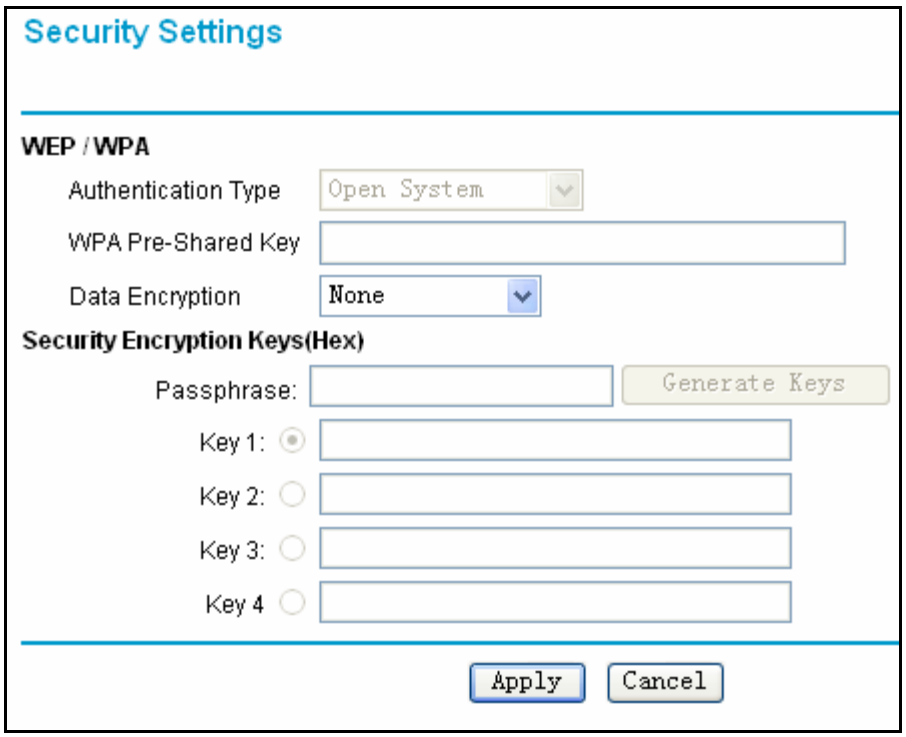



**Figure 16 Security Settings**

- **Authentication Type**

  Choose the following type.

  - Open System: Allow any wireless NIC or wireless bridge connect
  - Shared Key: If Shared Key is selected, you need to enabled WEP and enter at least one shared key.
  - 802.1x: IEEE 802.1x is a standard for network access control (port based), which was introduced especially for distributing encryption keys in a wireless network. The Access Point supports 802.1x for keeping out unauthorized users and for verifying the credentials of users with RADIUS so that authorized users can access the network and services. To use 802.1x, you will need at least one common Extensible Authentication Protocol (EAP) method on your authentication server, Access Points (authenticator) and stations (supplicant). 802.1x is also used to perform generation and distribution of encryption keys with enabling Data Encryption as WEP from AP to the station as part of or after the authentication process.
  - WPA + RADIUS: In cooperation with RADIUS, systems with WPA-EAP will be used

with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.

- WPA+ PSK: Instead of using RADIUS for authentication, systems with WPA-PSK will be configured with a secret password phrase. Enter your password phrase and press "Generate". You can now create a pre-shared key in the Access Point and copy the characters you input to the station's WPA-PSK entry. A shared secret is only secure as long as no third party knows about it.

**Notice:**

- You must configure Radius Server Settings with either Legacy 802.1x or WPA with Radius option.

- **WPA Pre-Shared Key:**

  Enter your password phrase and press "Generate" button, the key will be generated.

- **Data Encryption**

  Select the desired option, if enabled the keys must be entered, and other wireless stations or bridge must use the same keys. The default is None.

  - None
  - WEP 64 bit: 10 Hexadecimal digits (any combination of 0-9, a-f, or A-F)
  - WEP 128 bit: 26 Hexadecimal digits (any combination of 0-9, a-f, or A-F)
  - WEP 152 bit: 32 Hexadecimal digits (any combination of 0-9, a-f, or A-F)
  - TKIP: The TKIP option is automatically enabled when either WPA with Radius or WPA-PSK authentication type is selected.

- **Security Encryption Keys (Hex)**

  - Passphrase: To use the passphrase to generate the keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations or bridges. Only 8 to 63 characters can be entered.
  - Key1~~Key4: Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data. The four entries will be disabled if WPA with Radius authentication option is selected.

**Notice:**

- The Access Point and the stations must have the same Authentication Type, Data Encryption and Key, otherwise they can not connect.

# Access Control List Setup

The optional Access Control window lets you block the network access privilege of the specified stations through the Access Point. This provides an additional layer of security. There are two kinds of ACL.

- **Local MAC Address Database**

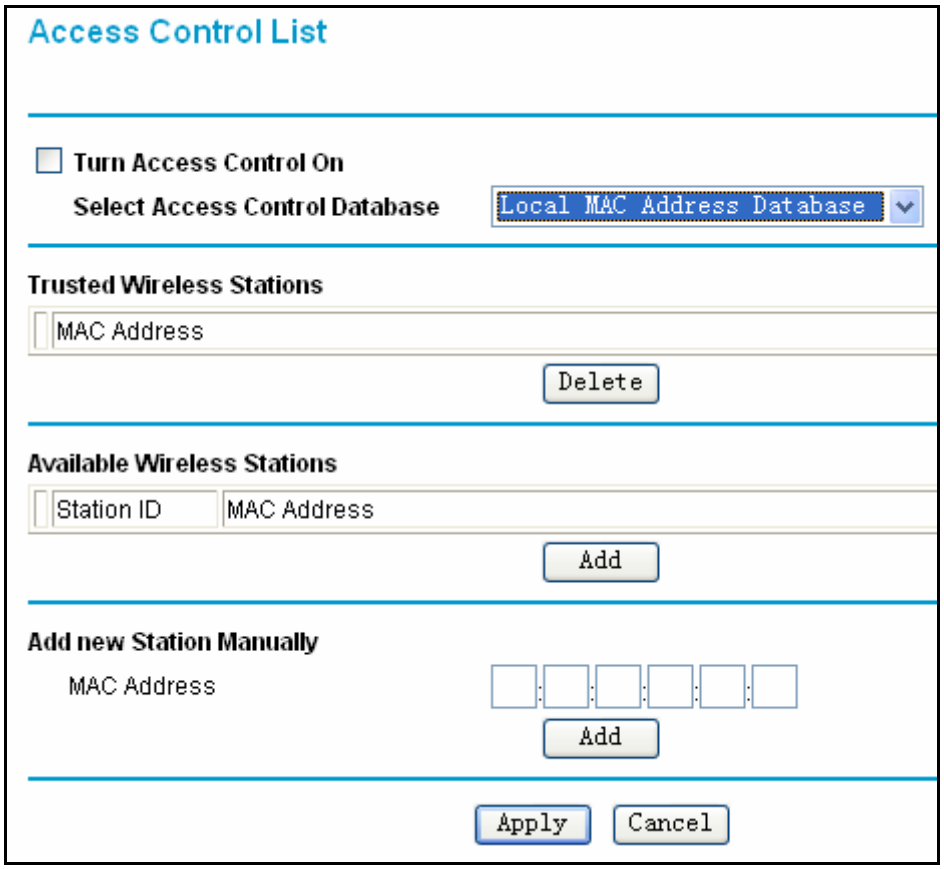



**Figure 17 Access Control List**

Choose the Turn Access Control On to enable Access Control feature and click Apply button. Only the station in the Trusted Wireless Stations can connect AP. What you should do is to maintenance the Available Wireless Stations list

- **Add Trusted Wireless Stations**
  - Add new Station Manually: add the MAC address in the MAC Address textbox and click

Add button and Apply button.

- Add Available Wireless Stations: Select the stations from the wireless station list and click Add button to add to the Trusted Wireless Stations list and click Add button and Apply button.
- Delete Trusted Wireless Stations: Choose the station in the Trusted Wireless Stations list, click Delete button and Apply button.

- **RADIUS MAC Address Database**

This function only can use after enable Authentication/Access Control Radius Server configuration.

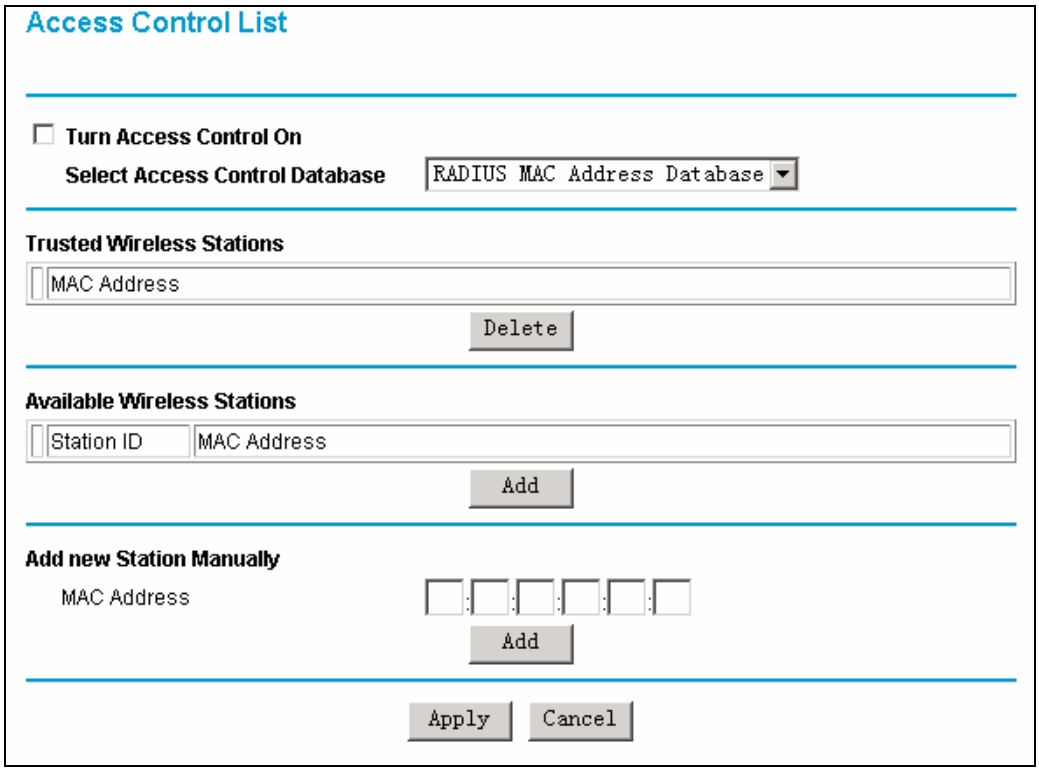



**Figure 18 RADIUS MAC Access Control**

The Access Point will use the MAC address table located on the external Radius Server on the LAN for Access Control.

# Hidden SSID Setup

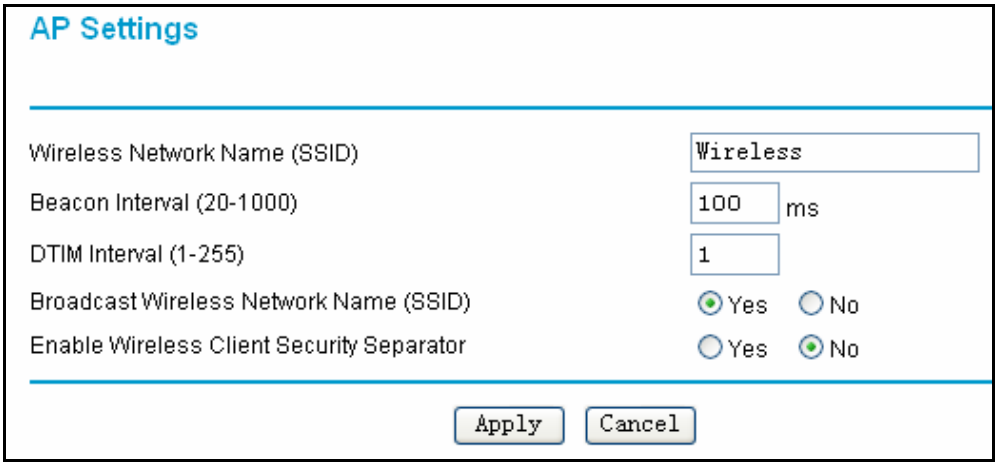



**Figure 19 Hidden SSID Setup**

If set to Yes, the Access Point will broadcast its SSID, allowing Wireless Stations which have a "null" (blank) SSID to adopt the correct SSID. If set to No, the SSID is not broadcast then station can not scan the AP in order to avoid illegal attack.

# Wireless Isolation

The wireless isolation can give the wireless network more security. There two kinds of wireless isolation: wireless client security separator in AP mode and wireless separator in bridge mode.

- **wireless client security separator**

  The associated wireless clients will not be able to communicate with each other if this feature is enabled.

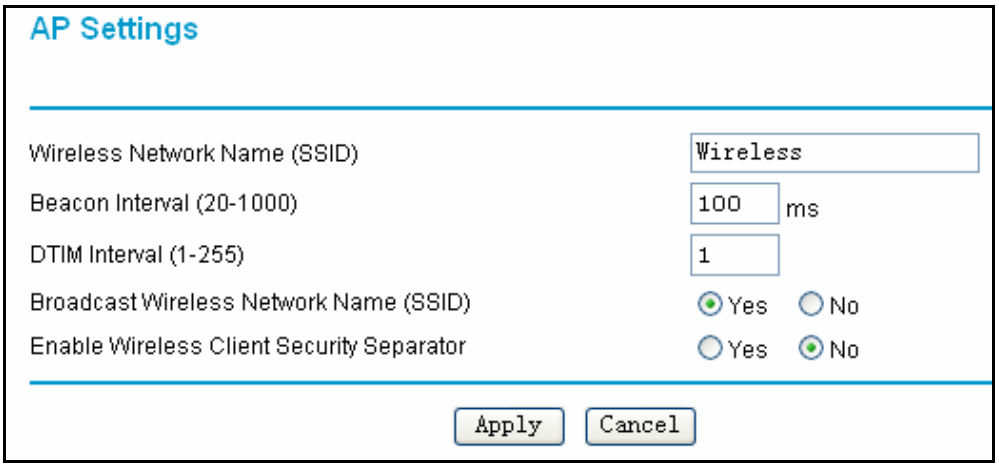



**Figure 20 Wireless Client Security Separator**

- **Wireless Separator**

The remote Bridges will not be able to communicate with each other if this feature is enabled.

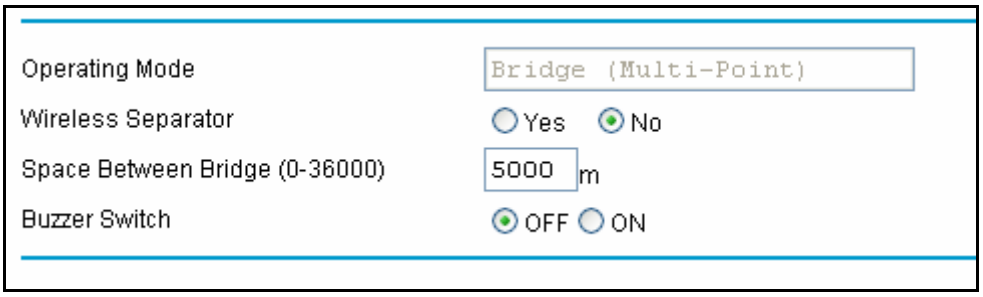



**Figure 21 Wireless Separator**

# Configure as a Router

The simple Router function can connect two different subnets.

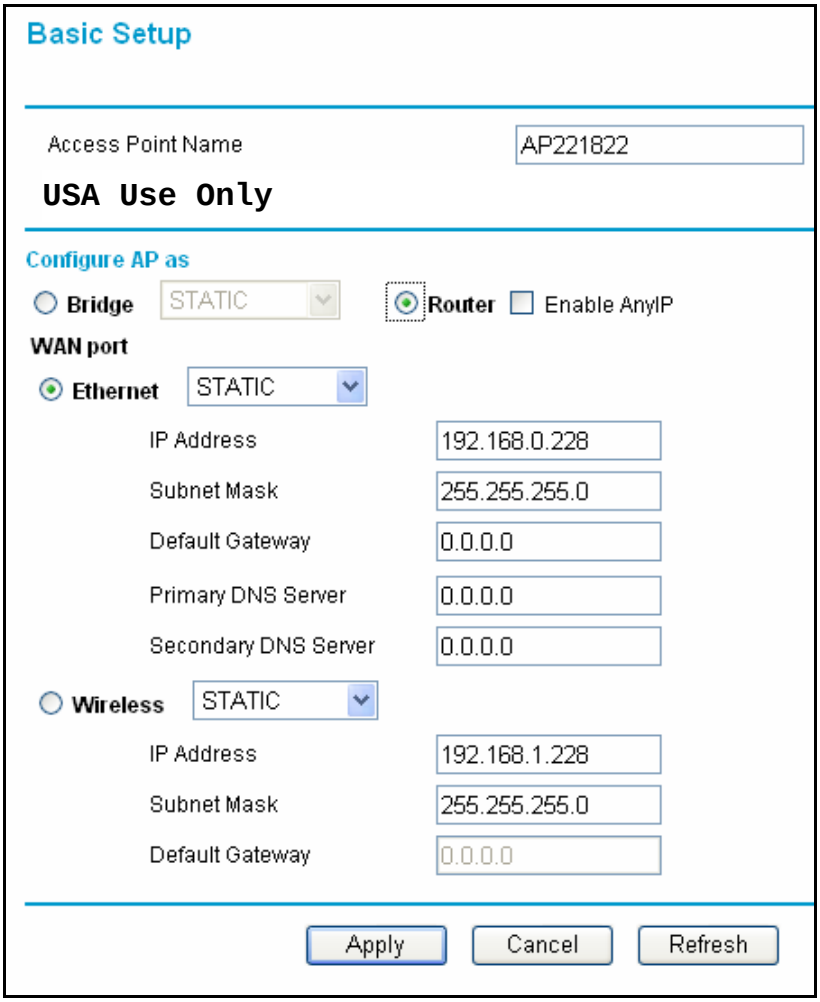



**Figure 22 Router**

There two kinds of Router mode.

- **WAN on Ethernet**

- **WAN on Wireless**

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

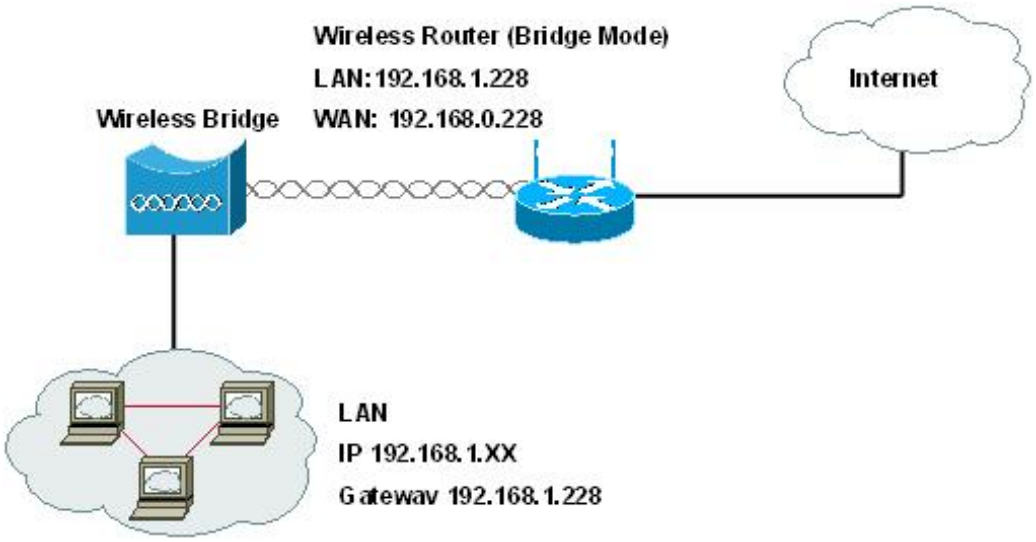



**Figure 23 Wireless Router (Bridge Mode)—WAN on Ethernet**

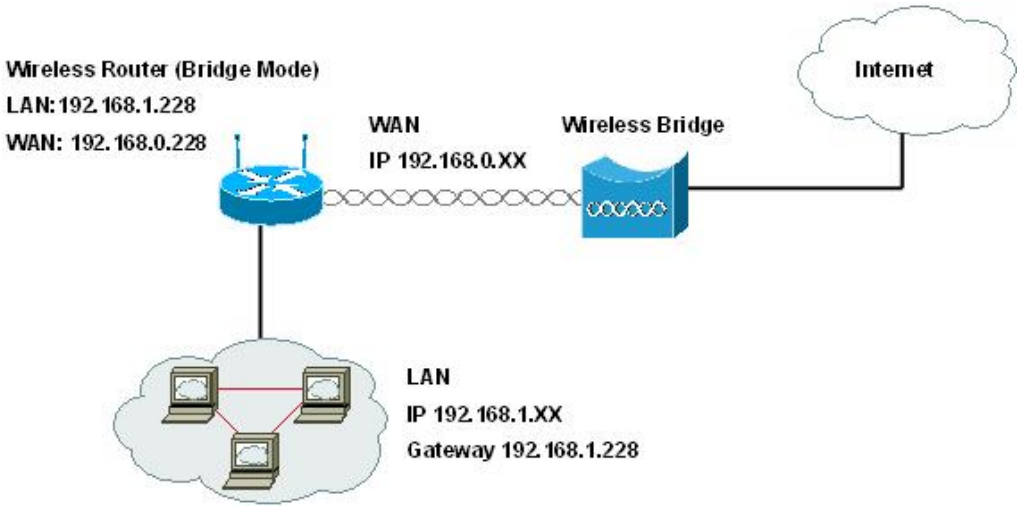



**Figure 24 Wireless Router (Bridge Mode)—WAN on Wireless**

In AP mode, the normal Router settings is following figure:

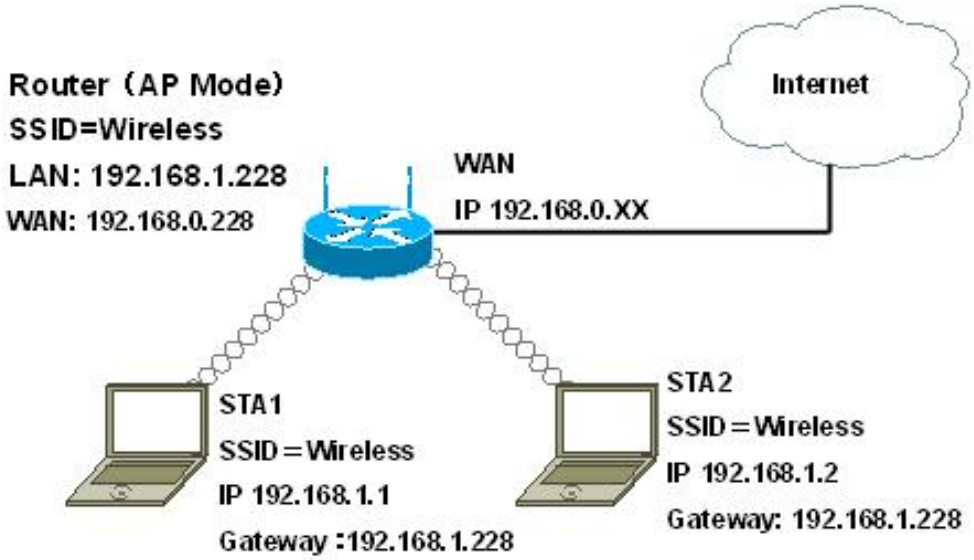



**Figure 25 AP Router**

In AP +Bridge mode, the normal Router settings is following figure:

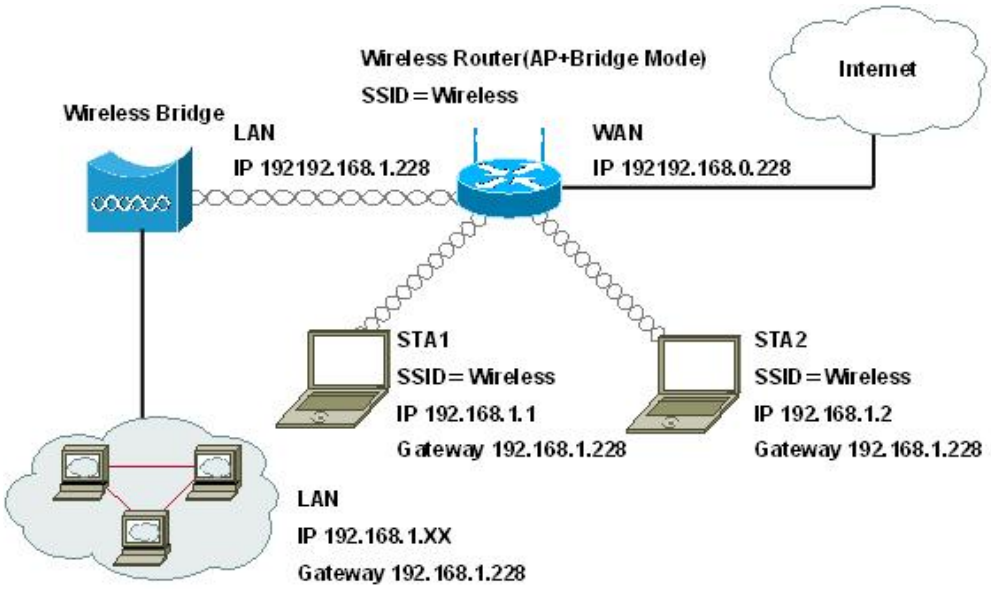



**Figure 26 "AP + Bridge" Router**

# AnyIP

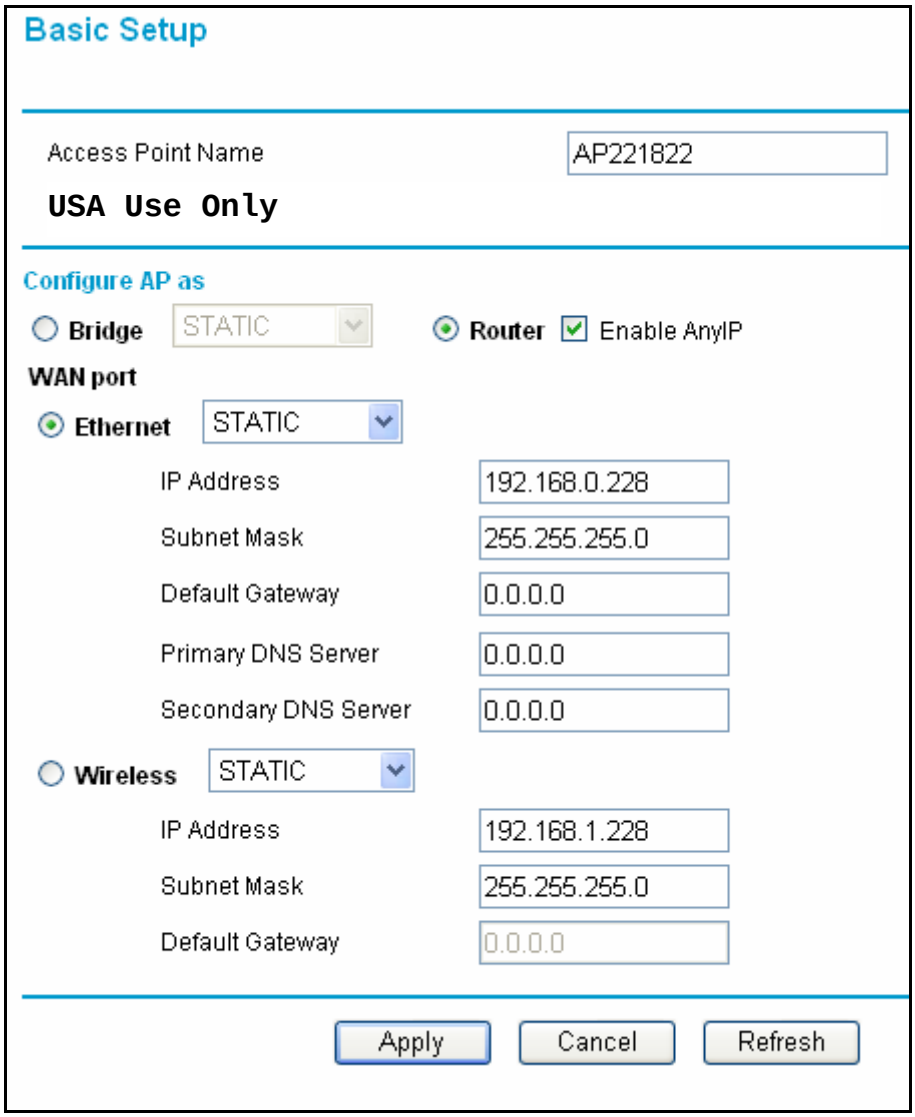



**Figure 27 AnyIP**

The AnyIP function can only be active in Router mode, the IP address, subnet mask, gateway and DNS Server of stations or PCs in LAN can be set as any value.

# SmartWDS Application

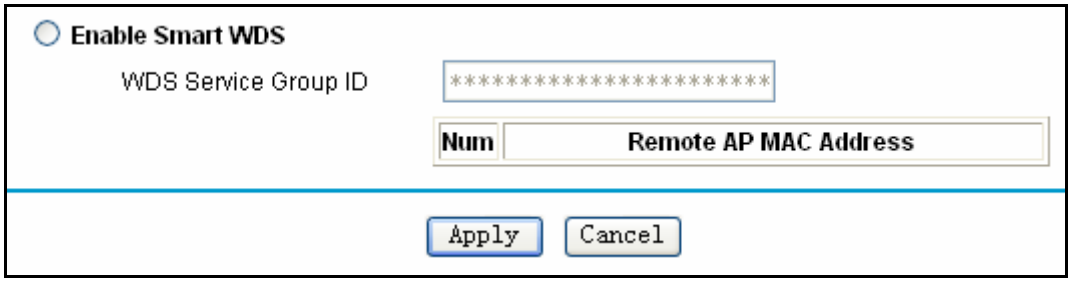



**Figure 29 SmartWDS**

SmartWDS mode is a private connection protocol. All wireless bridges can automatically connect just by the same SmartWDS group ID. There no needs of setting MAC address.

In the WDS Settings page, choose enable SmartWDS function, input an ID(no more than 32 characters) to indicate one WDS group. Such as “Bridge 123”.

The wireless bridge with the same ID will automatically choose one channel to builds connection and use private data encryption to communicate. At the same time, the “Channel” and “Security Settings” is disabled.

The largest number of one SmartWDS group is nine. The tenth or more wireless bridge with the same ID of other first nine bridges will builds another wireless network which can not connect with the first one.

✎ **Notice:**

- All the bridges want to join SmartWDS must support SmarWDS function.

# Outdoor Point to Multi-Point Bridge Application

In some application structure, there is a wireless bridge as centre point, other bridge access network by connecting it. We can this structure “Point to Multi-Point Bridge” just like “Point to Point Bridge”, we also suggest you should make all wireless bridge build a network and make sure than each bridge work well indoor, then take them outdoor for use. The following should be noticed:

- **The settings of centre point:**

  Set it as “Wireless Point-to-Multi-Point Bridge” mode, add all remote bridges MAC address in the remote MAC address textbox.

- **The settings of remote point:**

  Set it as “Wireless Point-to-Point Bridge” mode, add centre bridge MAC address in the remote MAC address textbox; because all the remote points share the throughput of centre point, the throughput between two remote points is half of that of one remote with centre point.

- **Link Test of multi points**

  In centre point, input the real space between centre point and the furthest remote point in Space between Bridge textbox. In each remote point, input the real space between centre point and it in Space between Bridge textbox.

  In the Link Test page of centre point, you can test signal strengthen of each remote point.

- **Down Flow Band Control**

  You can control the throughput between centre and remote by set the value (Mbps) in the textbox after the remote MAC address textbox.

# Outdoor Wireless Cover Application

In the AP mode, it can be set as wireless cover spot.

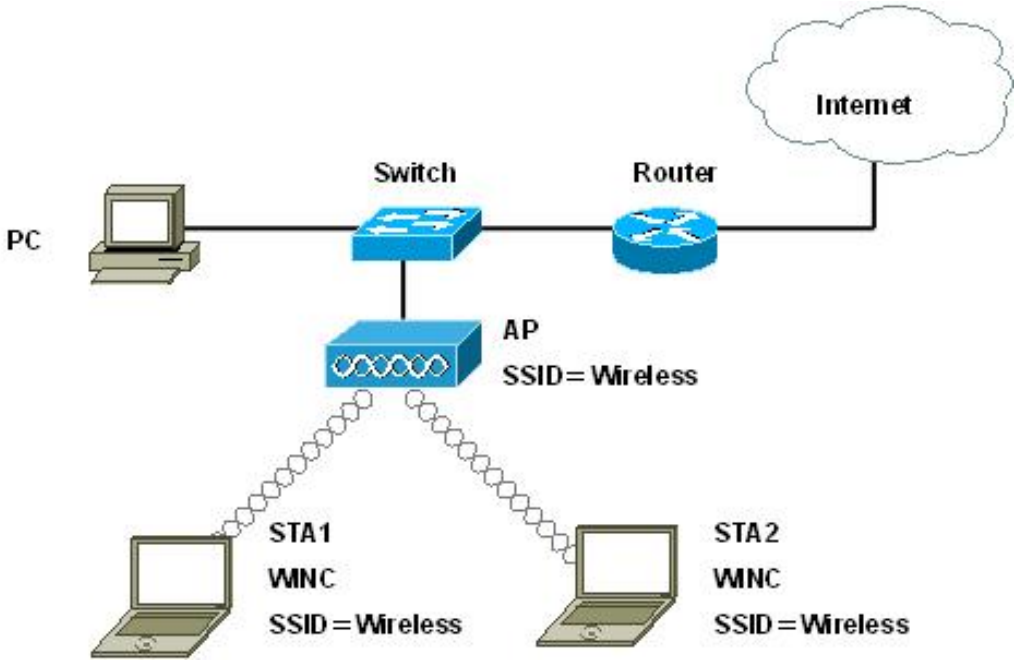



**Figure 30 Outdoor Wireless Cover Application**

STA1 and STA2 connect AP by SSID, and then they can access PC in Ethernet and internet. Do steps as following:

1. Set Operating Mode as AP mode in Wireless Settings page.

2. Open AP Settings page, set basic information.

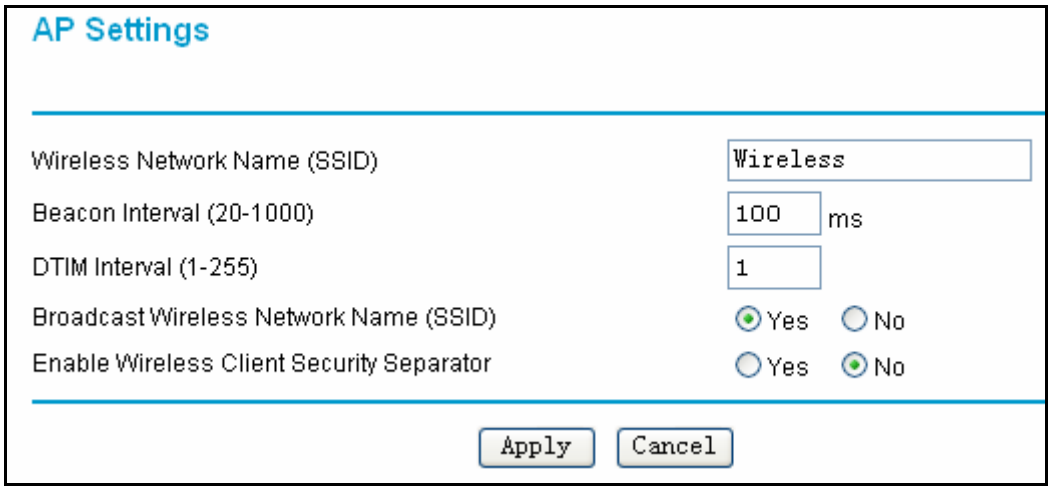



**Figure 31 AP Settings**

- **Wireless Network Name (SSID)**

  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 Access Point.

- **Beacon Interval**

  Specifies the interval time (20~~1000ms) for each beacon transmission.

- **DTIM Interval**

  The Delivery Traffic Indication Message, Specifies the data beacon rate between 1 and 255.

**Notice**

- Because the limitation of wireless network, you can realize security by authentication, data encryption and access control. At the same time, you can use wireless client security separator to protect client. The detail is list in **Wireless Security Settings**, **Wireless Access Control** and **Wireless Isolation**.

# "AP + Bridge" Mode Application

In "AP + Bridge" mode, you can use it both wireless bridge connection and wireless hotspot cover.

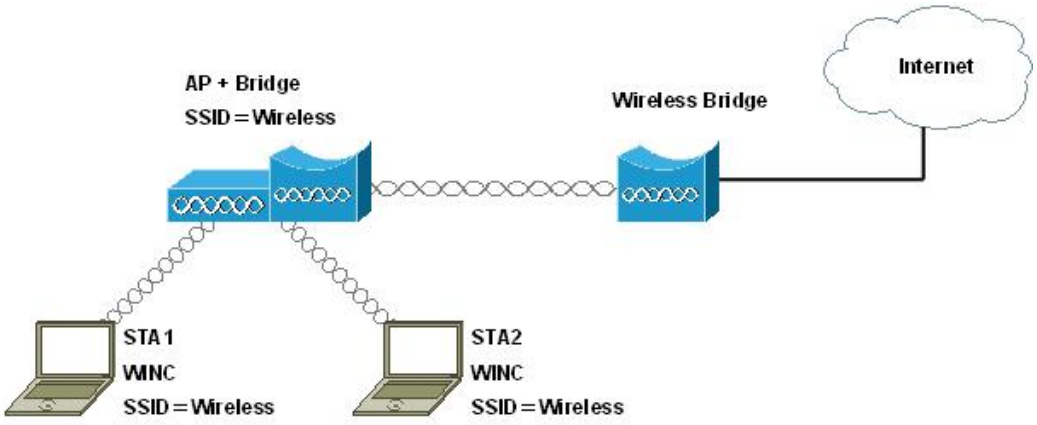



**Figure 32 "AP + Bridge" Mode Application**

Set Operating Mode as "AP + Bridge" mode in Wireless Settings page.

The settings of AP mode are list in **Outdoor Wireless Cover Application** .

The settings of Bridge mode are list in **Outdoor Point to Point Bridge Application** and **Outdoor Point to Multi-Point Bridge Application** chapter.

# Chapter 5 Management

## View the General Information

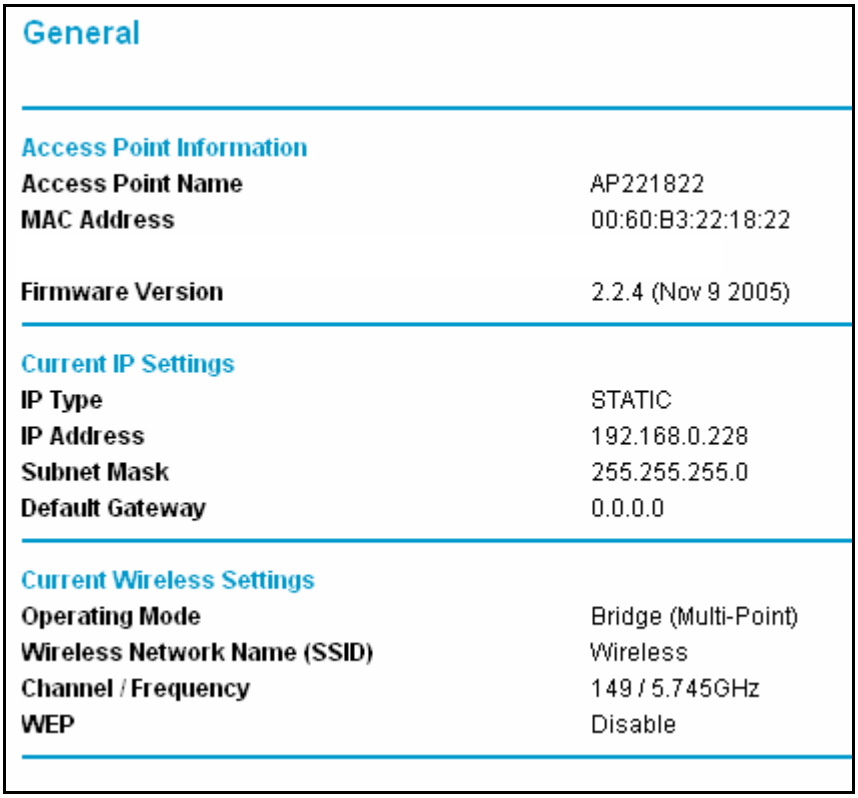



**Figure 33 General**

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

## View the STA List

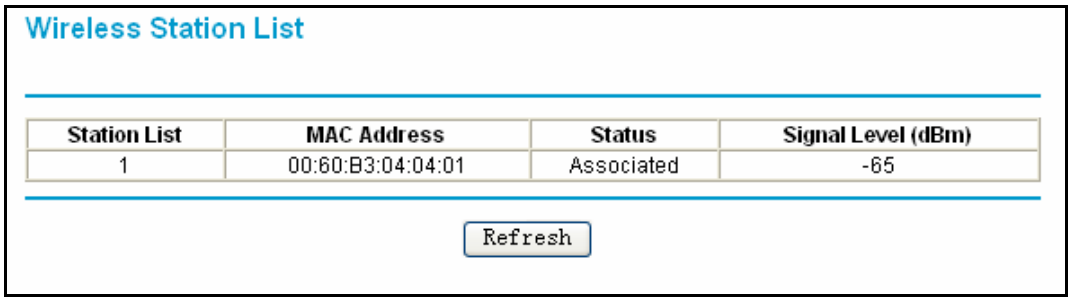



**Figure 34 STA List**

This page shows the Station ID, MAC address, Status and Signal Level for each wireless access

point or client node associated with the Access Point.

# View the Device's Link Status

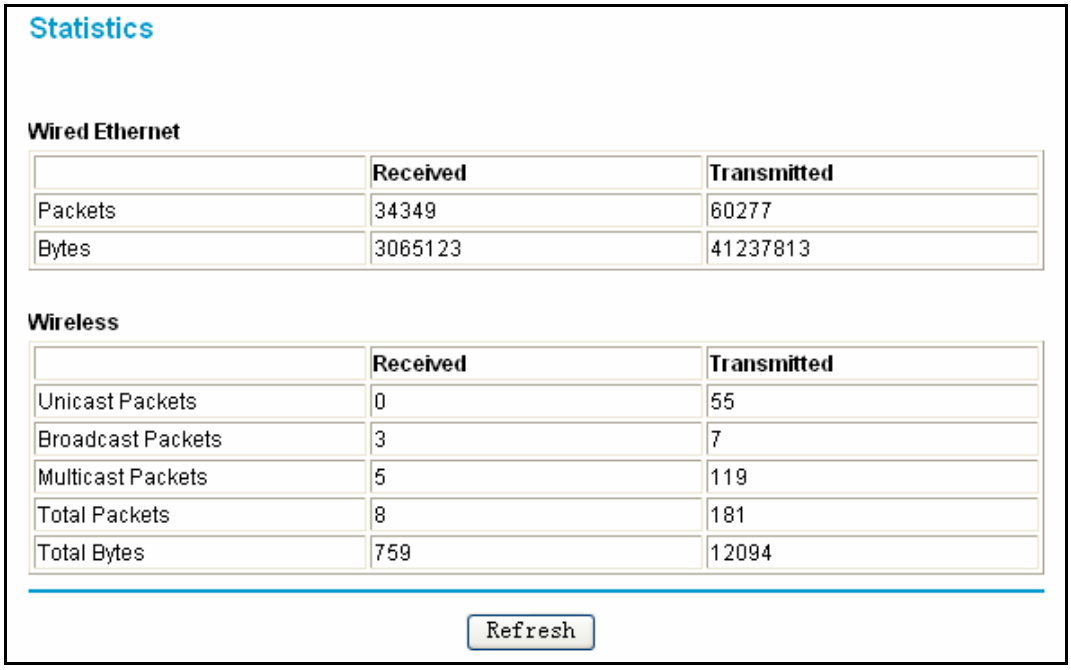



**Figure 35 Link Statistics**

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

# Change Login Password

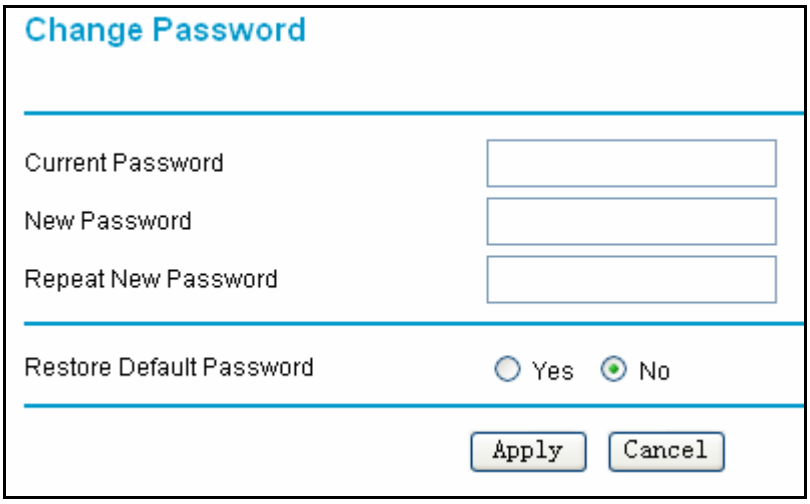



**Figure 36 Change Login Password**

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

To change the password, Type the old password. The default password for the Access Point is: password. Type a new password and type it again in the Repeat New Password box to confirm it. Click Apply to have the password changed or click Cancel to keep the current password.

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

# Firmware Upgrade

**User can't modify anything about firmware.**

# Backup/Restore Settings

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

- **WEB**

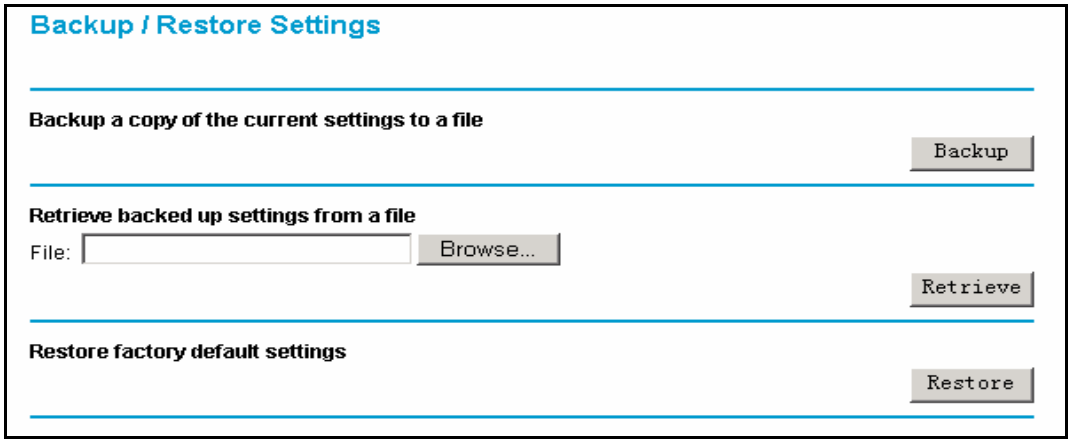



**Figure 38 Backup/Restore Settings**

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 AP will restart.

- **FTP**

1. Login AP by ftp.
2. Input command get zag5000.cfg, it will be saved in current directory.
3. Input command put zag5000.cfg, it will retrieve it to AP. and AP will restart.

```
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 zag5000.cfg
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
ftp: 3973128 bytes sent in 0.55Seconds 7263.49Kbytes/sec.
ftp> quit
221 Goodbye.
```

✎ **Notice:**

- The config file must be zag5000.cfg or ZAG5000.cfg
- 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!

# Restore to Factory

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

- **WEB**

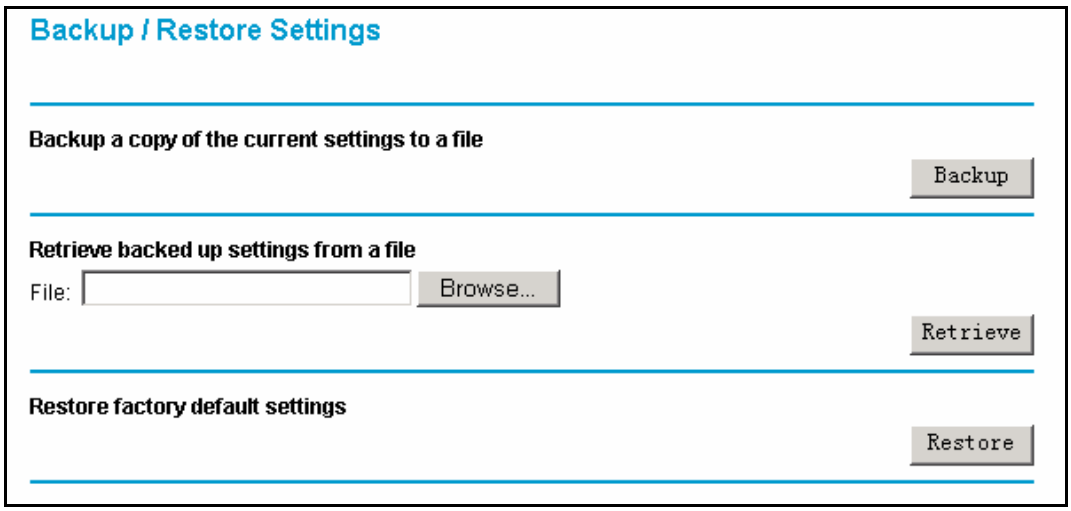



**Figure 39 Restore to Factory**

Click Restore button then the AP will restart to factory.

- **Hardware Default Button**


**Figure 40 Default Button**

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

# Reboot AP

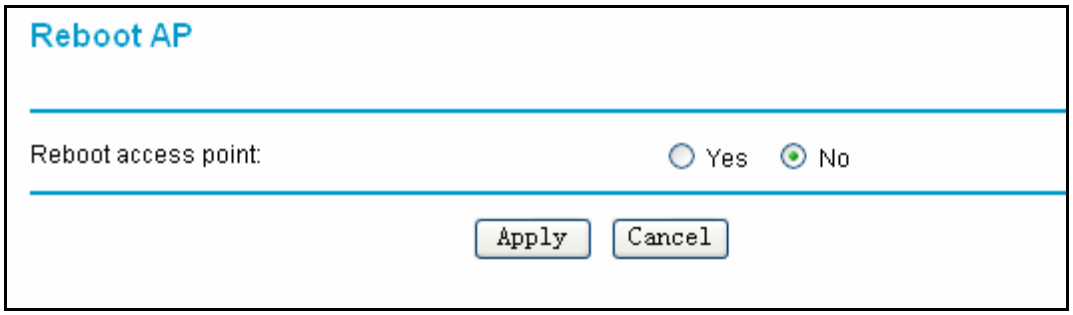



**Figure 41 Reboot AP**

You may select Yes on “Reboot AP” page and then click on APPLY button to reboot the access point.

# SNMP Management

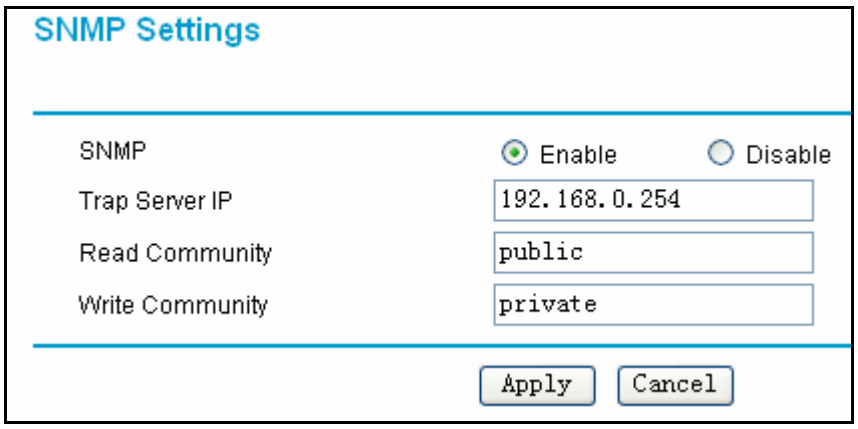



**Figure 42 SNMP**

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

b) Input command “get zag5000.mib”,you will find the mib file in the 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 zag5000.mib
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for /mnt/ramd/zag5000.mib (35518 bytes).
226 File send OK.
ftp: 35518 bytes received in 0.03Seconds 1183.93Kbytes/sec.
ftp> quit
221 Goodbye.
```

# SSH Management

1. Open putty.exe file


2. Input AP address, choose SSH protocol.

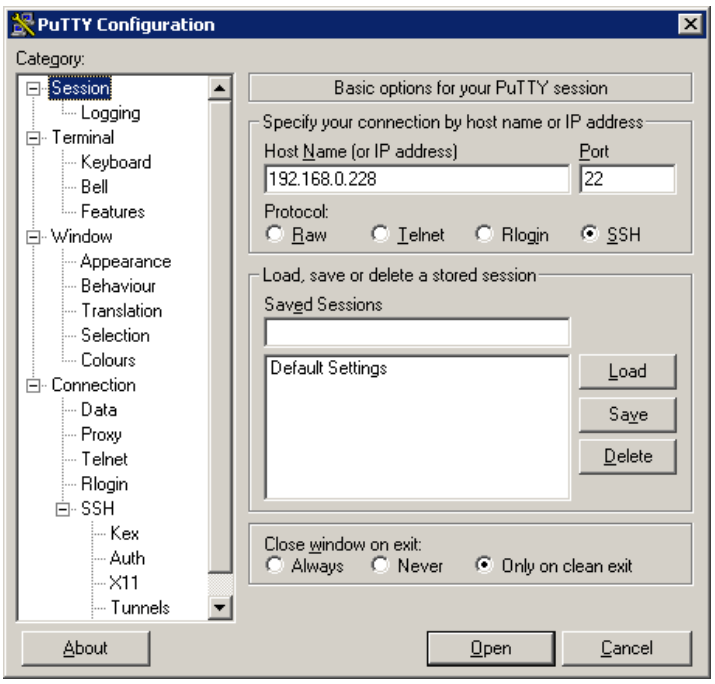



**Figure 43 Putty Settings 1**

3. The “3DES” should be in first in “Encryption cipher selection policy”.

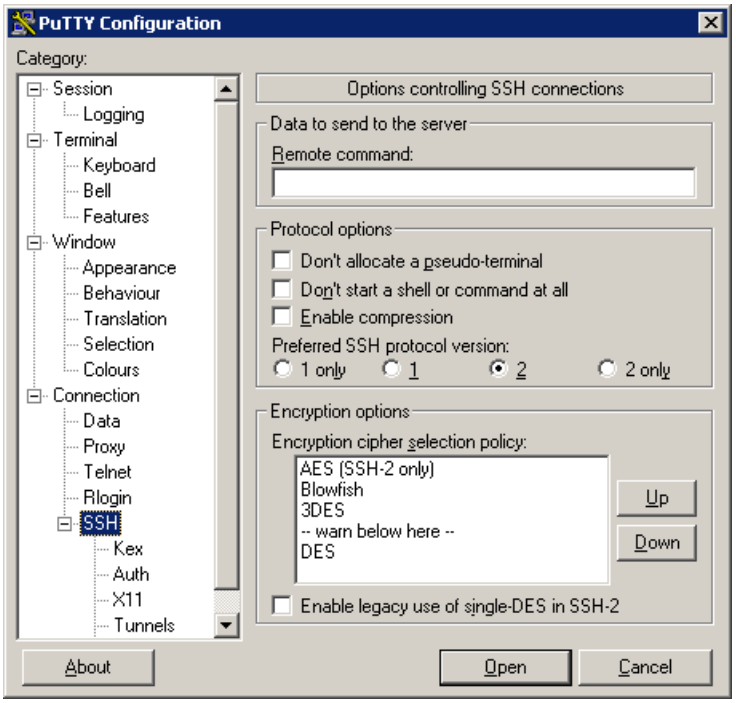



**Figure 44 Putty Settings 2**

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

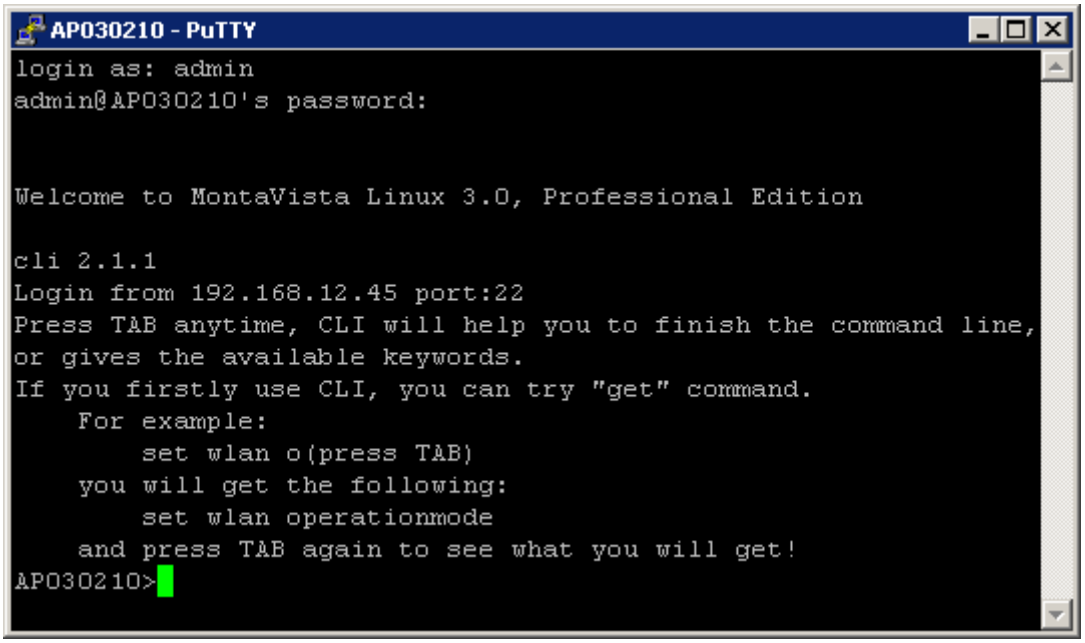



**Figure 45 SSH**

5. The user name is admin and password is password, after login you can use command line to set AP. you can input command “help” to get help. All the command supported is in Appendix DSSH.

# 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.

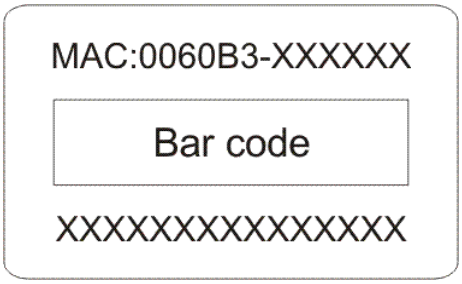



**Figure 46 MAC Address**

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

**Q 2. Why two Access Points can not build connection after setting?**

- Check the “Operating Mode” whether is “Bridge Mode”.
- Check the “remote MAC address” whether is right.

- Check the “Channel/Frequency” whether is same.
- Check the “Data Encryption” and “Key” whether is same.
- Check the “Space between Bridge” whether is real space.

**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 8 RF 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-I, the space between bridges is 3km.**

Tx Power ＝ 18dBm

Cable loss ＝ 1dBi

Antenna Gain ＝**6** dBi

Path loss ＝ 116dBm

Local receive signal strengthens（dBm）＝ 18－1＋23－116＋**6** －1 ＝ **–71**（dBm）

**Q 4. Why the throughput is not high?**

You should adjust antenna to get highest signal strengthens. 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). Change the channel if the Link Test value is not high，excluding other wireless equipments disturb AP.

(3). Restart AP.

(4). Default AP and restore last settings.

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

**Q 6. How to adjust output power?**

**Fixed power level.**

**Q 7. Why the buzzer stops work after a period of time, and how to close buzzer manually?**

As design the buzzer will automatically stop ringing after working one hour.

You can choose buzzer switch to OFF to close buzzer in WDS Settings page.

**Q 8. Why can not open WEB page of remote wireless bridge in local network?**

Because this kind of settings will slow the response of remote AP WEB Server, just waiting for several minutes or restarting remote wireless bridge is a way to solve problem. We suggest you set AP in local wired Ethernet network.

# Technology Support

You can access the web page: **http://www.zcom.com.cn/english/support/downloads.asp** to download and upgrade latest software. If you meet any problem in the course of installing and using the Access Point, please contact local suppliers.

Homepage: **http://www.zcom.com.cn**

E-Mail: **support@zcom.com.cn**

Tel: 86-25-84661320

# Appendix A. Technical Specifications

**Diagram 10 ZA-5000-I Spec**

| ZA-5000-I IEEE 802.11a 54Mbps Wireless Outdoor Bridge | |
|---|---|
|  | ZA-5000-I a new high-speed wireless bridge aimed at last-mile broadband wireless access (BWA) links and campus data networks that need to send large amounts of data over the air. By enabling corporations and ISPs to bridge the gap between multiple buildings without incurring the expense of leased lines or fiber runs, ZA-5000-I offers fast return on investment while providing optimal network performance. |
| **Feature** | |
| Description | ZA-5000-I IEEE 802.11a 54Mbps<br>Wireless Outdoor Bridge |
| Standard | IEEE 802.11a IEEE 802.3u IEEE 802.3af |
| Support Protocol | TCP/IP IPX NetBEUI |
| Rate Select | Best / 54 / 48 / 36 / 24 / 18 / 12 / 9 / 6 Mbps |
| AP Mode | Yes |
| Bridge Mode | Point-to-Point, Point-to-Multipoint, Repeater |
| WDS Mode | AP + Bridge |
| IP Routing | Yes |
| Any IP | Yes |
| DHCP | DHCP Server、DHCP Client |
| Super A | No |
| Smart WDS | WDS Service Group ID |
| Spanning Tree | Yes |
| Power Control | No |
| Link Test | Yes |
| Wireless Station List | Yes |
| **Interface** | |
| LAN | One 10/100-BaseTX RJ-45 Ethernet Port |
| Antenna | One Integrated Panel Antenna (9°×9°) |
| Default Button | Yes |
| Ground Interface | Yes |
| **Electrical** | |
| POE (Power over Ethernet) | Yes |
| Power Supply | 48V DC/1A, Compatible with IEEE 802.3af |
| Power Consumption | 200mA@48V |
| Buzzer | Yes (Signal Level) |
| **Radio** | |
| Channel / Frequency | America: |

| | |
|---|---|
| | 5.725GHz～5.825GHz |
| RF Output Power | **15.5dBm** |
| Sensitivity | －65dBm@54Mbps<br>－66dBm@48Mbps<br>－70dBm@36Mbps<br>－74dBm@24Mbps<br>－77dBm@18Mbps<br>－79dBm@12Mps<br>－81dBm@9Mps<br>－82dBm@6Mbps |
| **Management** | |
| Web Management | Yes |
| SNMP MIB | Yes |
| Telnet | SSH |
| Bandwidth Control | Yes |
| W Upgrade | Web / TFTP |
| Backup Settings | Web / FTP |
| **Security** | |
| WEP Encryption | 64 / 128 / 152 bits |
| Radius | Yes |
| 802.1x | Yes |
| WPA | Yes |
| Access Control | Yes |
| SSID Broadcast | Hidden AP |
| Wireless Client Separator | Yes |
| Wireless Separator | Yes |
| **Physical** | |
| Dimension | 305mm(L)×305mm(W)×88mm(H) |
| Weight | 3.4 Kg |
| **Environment** | |
| Operating Temperature | －20～65℃ |
| Storage Temperature | －20～80℃ |
| Humidity | 5～95％ |

**Diagram 11 ZA-5000-E Spec**

| ZA-5000-E IEEE 802.11a 54Mbps Wireless Outdoor Bridge | |
|---|---|
|  | ZA-5000-E a new high-speed wireless bridge aimed at last-mile broadband wireless access (BWA) links and campus data networks that need to send large amounts of data over the air. By enabling corporations and ISPs to bridge the gap between multiple buildings without incurring the expense of leased lines or fiber runs, ZA-5000-E offers fast return on investment while providing optimal network performance. |
| **Feature** | |
| Description | ZA-5000-E IEEE 802.11a 54Mbps<br>Wireless Outdoor Bridge |
| Standard | IEEE 802.11a IEEE 802.3u IEEE 802.3af |
| Support Protocol | TCP/IP IPX NetBEUI |
| Rate Select | Best / 54 / 48 / 36 / 24 / 18 / 12 / 9 / 6 Mbps |
| AP Mode | Yes |
| Bridge Mode | Point-to-Point, Point-to-Multipoint, Repeater |
| WDS Mode | AP + Bridge |
| IP Routing | Yes |
| Any IP | Yes |
| DHCP | DHCP Server、DHCP Client |
| Super A | No |
| Smart WDS | WDS Service Group ID |
| Spanning Tree | Yes |
| Power Control | No |
| Link Test | Yes |
| Wireless Station List | Yes |
| **Interface** | |
| LAN | One 10/100-BaseTX RJ-45 Ethernet Port |
| Antenna | Reverse N-Type connector |
| Default Button | Yes |
| Ground Interface | Yes |
| **Electrical** | |
| POE (Power over Ethernet) | Yes |
| Power Supply | 48V DC/1A, Compatible with IEEE 802.3af |
| Power Consumption | 200mA@48V |
| Buzzer | Yes (Signal Level) |
| **Radio** | |

| | |
|---|---|
| Channel / Frequency | America:<br>5.725GHz～5.825GHz |
| RF Output Power | **15.5dBm** |
| Sensitivity | －65dBm@54Mbps<br>－66dBm@48Mbps<br>－70dBm@36Mbps<br>－74dBm@24Mbps<br>－77dBm@18Mbps<br>－79dBm@12Mps<br>－81dBm@9Mps<br>－82dBm@6Mbps |
| **Management** | |
| Web Management | Yes |
| SNMP MIB | Yes |
| Telnet | SSH |
| Bandwidth Control | Yes |
| W Upgrade | Web / TFTP |
| Backup Settings | Web / FTP |
| **Security** | |
| WEP Encryption | 64 / 128 / 152 bits |
| Radius | Yes |
| 802.1x | Yes |
| WPA | Yes |
| Access Control | Yes |
| SSID Broadcast | Hidden AP |
| Wireless Client Separator | Yes |
| Wireless Separator | Yes |
| **Physical** | |
| Dimension | 310mm(L)×305mm(W)×94mm(H) |
| Weight | 3.6 Kg |
| **Environment** | |
| Operating Temperature | －20～65℃ |
| Storage Temperature | －20～80℃ |
| Humidity | 5～95％ |

# Appendix B. Glossary

**Diagram 12 Glossary**

| 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.<br>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".<br>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. |
| LAN&WAN | LAN. A communications network serving users within a limited area, such as one floor of a building.<br>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.<br>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 13 ASCII**

| 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 14 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 |
| √ | √ | | | 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 |
| √ | √ | | authenticati on | | | | --- 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 |
| √ | √ | | downflowwidth | | | | --- wireless down flow width |
| √ | √ | | RFlinewaste | | | | --- RF line waste |
| √ | √ | | localplus | | | | --- local plus |
| √ | √ | | remoteplus | | | | --- remote plus |
| √ | √ | | testremotemac | | | | --- remote test mac |
| √ | √ | | linkrx | | | | --- MIB_WLAN_LINK_RX |
| √ | √ | | linktx | | | | --- MIB_WLAN_LINK_TX |
| √ | √ | | linktime | | | | --- MIB_WLAN_LINK_TIME |
| √ | √ | | linkpktsize | | | | --- MIB_WLAN_LINK_PKT_SIZE |
| √ | √ | | linkpktinterval | | | | --- MIB_WLAN_LINK_TEST_INTERVAL |
| √ | √ | | linklocalrssi | | | | --- MIB_WLAN_LINK_LOCAL_RSSI |
| √ | √ | | linkremotersi | | | | --- MIB_WLAN_LINK_REMOTE_RSSI |
| √ | √ | | linkaction | | | | --- MIB_WLAN_LINK_ACTION |
| | √ | | password | | | | --- system password |
| | √ | | reboot | | | | --- reboot system |
| | √ | | exit | | | | --- logout from CLI |
| | √ | | quit | | | | --- quit CLI |

Nan Jing Z-Com Wireless Co.,Ltd.

Address: 168 Long Pan Zhong Road Jiang Su SoftwarePark, 118

Nan Jing China

Postalcode: 210002

TEL: +86-25-84661320

FAX: +86-25-84661313

Homepage: **www.zcom.com.cn**

E-Mail: **support@zcom.com.cn**