



# ZXV10 W812N V2

## Indoor Wireless Access Point

### User Manual

---

ZTE CORPORATION  
NO. 55, Hi-tech Road South, ShenZhen, P.R.China  
Postcode: 518057  
Tel: +86-755-26771900  
Fax: +86-755-26770801  
URL: <http://ensupport.zte.com.cn>  
E-mail: [support@zte.com.cn](mailto:support@zte.com.cn)

## **LEGAL INFORMATION**

Copyright © 2012 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided “as is”, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice. Users may visit ZTE technical support website <http://ensupport.zte.com.cn> to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

## **Revision History**

<b>Revision.</b>	<b>Revision Date</b>	<b>Revision Reason</b>
R1.0	2012-11-26	First Edition

Serial Number: SJ-20121126100147-001

Publishing Date: 2012-11-26 ( R1.0 )

# Contents

---

<b>Chapter 1 Safety Precautions.....</b>	<b>1-1</b>
<b>Chapter 2 Product Introduction .....</b>	<b>2-1</b>
2.1 Product Introduction .....	2-1
2.2 Typical Application.....	2-1
2.3 Indicators Status Description.....	2-2
2.4 Interface Description.....	2-3
<b>Chapter 3 Product Installation .....</b>	<b>3-1</b>
3.1 Installation Requirements.....	3-1
3.2 Hardware Installation .....	3-1
3.3 Computer Configuration.....	3-2
3.3.1 Checking Computer Configuration .....	3-2
3.3.2 Setting TCP/IP .....	3-3
<b>Chapter 4 Configuration Preparation .....</b>	<b>4-1</b>
4.1 Default Settings.....	4-1
4.2 Requirements Before Configuration .....	4-1
4.3 Logging in to the System .....	4-2
<b>Chapter 5 Device Status .....</b>	<b>5-1</b>
5.1 Checking Device Information.....	5-1
5.2 Checking Information of Network Interfaces .....	5-1
5.2.1 Checking Ethernet Interface Information .....	5-1
5.2.2 Checking Network Connection Information.....	5-2
5.3 Checking WLAN Interface Information .....	5-3
<b>Chapter 6 Network Configuration .....</b>	<b>6-1</b>
6.1 Broadband Connection Configuration .....	6-1
6.1.1 Configuring Broadband Connection (Fit AP).....	6-1
6.1.2 Configuring Broadband Connection (Fat AP).....	6-3
6.2 WLAN Configuration.....	6-4
6.2.1 Setting Basic Information .....	6-4
6.2.2 Configuring SSID .....	6-9
6.2.3 Setting Security Information .....	6-10
6.2.4 Setting Rate Limits .....	6-16
6.2.5 Setting an Access Control List.....	6-17
6.2.6 Checking Associated Devices .....	6-18

6.2.7 Scanning an Access Point .....	6-18
6.2.8 Configuring WDS .....	6-19
6.2.9 Configuring STA WMM .....	6-20
6.2.10 Configuring AP WMM .....	6-21
6.2.11 Setting Channel Auto-Switch .....	6-22
6.2.12 Setting Wireless Mode .....	6-23
6.2.13 Setting Mesh Configuration .....	6-23
6.3 LAN Management .....	6-24
6.3.1 Managing Addresses .....	6-24
6.3.2 Managing DHCP Conditional Serving Pool .....	6-25
6.3.3 Managing an IPv6 Address .....	6-26
6.4 Routing Management .....	6-26
6.4.1 Configuring a Static Route ( IPV4 ) .....	6-26
6.4.2 Configuring a Static Route(IPV6) .....	6-27
6.4.3 Setting a Dynamic Route .....	6-28
<b>Chapter 7 Security Configuration .....</b>	<b>7-1</b>
7.1 Configuring a Firewall .....	7-1
7.2 Configuring IP Filter .....	7-2
7.3 Configuring MAC Filter .....	7-4
7.4 Viewing a Service List .....	7-5
7.5 Configuring the ALG Switch .....	7-5
<b>Chapter 8 Application Configuration .....</b>	<b>8-1</b>
8.1 Configuring UPnP .....	8-1
8.2 Setting a Device Name .....	8-2
8.3 QoS Configuration .....	8-3
8.3.1 Configuring QoS Basic Parameters .....	8-3
8.3.2 Configuring a Classification Rule .....	8-4
8.3.3 Configuring Congestion Management .....	8-6
8.4 Configuring SNTP .....	8-7
8.5 IGMP Configuration .....	8-8
8.5.1 Setting IGMP Proxy .....	8-8
8.5.2 Configuring IGMP Snooping .....	8-8
8.6 Configuring MLD Listening .....	8-9
8.7 LED Control .....	8-9
<b>Chapter 9 Management Configuration .....</b>	<b>9-1</b>
9.1 Managing SNMPv1/v2c .....	9-1
9.2 SNMPv3 Security Management (USM) .....	9-2

9.2.1	Managing SNMPv3 Users .....	9-2
9.2.2	Managing SNMPv1/v2c Users .....	9-3
9.3	SNMPv3 Access Control Management (VACM) .....	9-3
9.3.1	Managing Context .....	9-3
9.3.2	Managing Security Groups .....	9-4
9.3.3	Managing View Subtree .....	9-4
9.3.4	Managing Access Table .....	9-5
9.4	User Management .....	9-6
9.4.1	Managing Users .....	9-6
9.4.2	Setting Automatic Logout .....	9-7
9.5	Device Management .....	9-8
9.5.1	Setting System Management .....	9-8
9.5.2	Setting Version Upgrade .....	9-8
9.5.3	Managing User Configuration .....	9-9
9.5.4	Managing the Default Configuration .....	9-9
9.6	Configuring Log Management .....	9-10
9.7	Access Point Management .....	9-11
9.7.1	Setting an AP Mode .....	9-11
9.7.2	Setting an Access Point Name .....	9-12
9.8	Diagnosis and Maintenance .....	9-12
9.8.1	Performing Ping Diagnosis .....	9-12
9.8.2	Configuring Trace Route Diagnosis .....	9-13
	<b>Appendix A Troubleshooting .....</b>	<b>A-1</b>
	<b>Appendix B Technical Specifications .....</b>	<b>B-1</b>
	<b>Appendix C Computer WLAN Configuration .....</b>	<b>C-1</b>
	<b>Appendix D CE and FCC Compliance Statement .....</b>	<b>D-1</b>
	<b>Glossary .....</b>	<b>I</b>



# Chapter 1

# Safety Precautions

---

## Installation

- Use the power adapter provided. If you use other power adapters, the device may be damaged or fails to operate properly.
- Make sure that the electric load of a power socket or a power cable meets the requirements. Overloading of power sockets or broken power cables may cause an electric shock or a fire. Check the cables periodically. Replace the damaged cables immediately.
- Appropriate space for heat dissipation is required to prevent the device from overheating. Avoid covering any heat dissipation hole to prevent the device from overheating.
- Keep the device from heat sources and high temperature. Do not expose the device to sunshine.
- Do not expose the device to any moisture environment.
- Do not place the device on an unstable desktop.

## Usage

- When this device is not in use or needs to be cleaned, switch off the power and disconnect the power cables. Note that the surface temperature of the power adapter may be quite high.
- After power off the device, wait at least 15 seconds between this power-off and next power-on.
- When this device is not in use for a period of time, disconnect power cables so as to ensure that this device will not be damaged by current or voltage increase due to lightning.

## Service

Do not disassemble the device, otherwise you will lose your warranty. Contact your service provider when one of the following problems occurs:

- The power cable or power socket is damaged.
- There is liquid entering the device.
- The device is wet because of rain or other liquid.
- The device fails to run normally although you have followed the instruction.
- The device is fallen off or is damaged by mishandling.
- The running indicators on this device are abnormal.

This page intentionally left blank.



# Chapter 2

## Product Introduction

---

### Table of Contents

Product Introduction .....	2-1
Typical Application.....	2-1
Indicators Status Description .....	2-2
Interface Description .....	2-3

## 2.1 Product Introduction

The ZXV10 W812N V2 broadband wireless access point operates at the 2.4 GHz (supported frequency range is from 2412 MHz to 2472 MHz) and 5.8 GHz (supported frequency range is from 5150 MHz to 5250 MHz, from 5250 MHz to 5350 MHz, from 5470 MHz to 5725 MHz, and from 5725 MHz to 5850 MHz) frequency band which is configurable according to frequency requirements of different countries, meeting the standards of IEEE 802.11a, 802.11b, 802.11g and 802.11n. With orthogonal frequency multiplex division (OFDM) technology, the device can provide a maximum data transmission rate of 300 Mbps. The product has advanced features such as high transmission rate, high receiving sensitivity, long-distance transmission, which provides an effective solution for basic telecommunication carriers, ISPs and industry enterprises. Furthermore, the ZXV10 W812N V2 product supports the function of multiple security encryption mechanisms and authorization management, which provides a highly secure system for WLAN. In addition, it also supports powering a device through the PoE mode.

## 2.2 Typical Application

- The small and medium-sized enterprises can realize wireless coverage to meet mobile office requirements.
- Access the company network remotely.

Receiving and sending e-mails, files transmission, terminal simulation and others. Support various wireless network connection modes such as point-to-point connection, single access point connection, multiple access point connection and roaming. The product can be applied to various application environment flexibly such as the connection between an intranet and different networks.

- The environment in which establishing a connection with network cables is difficult.  
The place where cabling is difficult such as an old building and an asbestos building structure.
- Mobile office system.

Retailers, manufacturers and the working site needs to be changed frequently.

- It is necessary to establish a LAN temporarily for a special project.

The place that needs to establish a LAN temporarily such as commercial exhibitions, exhibition halls and construction sites; situations when the space needs to be expanded during the working peak hours such as retailers, airports and airlines; The condition when the financial approver needs to establish a client work group.

- Mobile workers access the database.

Doctors, nurses and retailers need to implement information sharing by mobile access to the database.

- Home office users.

The device is suitable for home office users needing a small computer network with easy and quick installation.

## 2.3 Indicators Status Description

The indicators on the ZXV10 W812N V2 are described in the following table.

Indicator	Status	Description
Status	Flashing slowly	The device is operating properly or upgraded.
	Flashing quickly	The software is being started.
	Off	The device self-test fails.
	On	The AP has been registered in AC.
Power	On	The device is powered on.
	Off	The device is powered off or a fault occurs to the device.
RF1 (2.4 GHz)	On	The device normally enables the function through which WLAN can transmit data at 2.4 G frequency band.
	Flashing	The WLAN at 2.4 G frequency band is transmitting data.
	Off	The WLAN transmission function at 2.4 GHz frequency band is disabled or fails to be enabled.
RF2 (5.8 GHz)	On	The device normally enables the function through which WLAN can transmit data at 5.8 G frequency band.
	Flashing	The WLAN at 5.8 G frequency band is transmitting data.
	Off	The WLAN transmission function at 5.8 GHz frequency band is disabled or fails to be enabled.
Eth	On	The Ethernet port is properly connected.
	Flashing	Data is being transmitted through the Ethernet port.
	Off	The Ethernet port is disabled or faulty.

## 2.4 Interface Description

The following table shows the description of various interfaces and buttons on the ZXV10 W812N V2.

Name	Description
DC 12 V	The power interface is to connect to the associated power adapter.
WAN/PoE	The Ethernet interface to connect the Network Interface Card (NIC) on a PC or other network devices through the RJ-45 network cable.
Reset	During the switch-on period, press and hold this button for more than 5 seconds to reset the current settings to the default ones. Then the system restarts automatically.

This page intentionally left blank.

# Chapter 3

## Product Installation

---

### Table of Contents

Installation Requirements .....	3-1
Hardware Installation.....	3-1
Computer Configuration .....	3-2

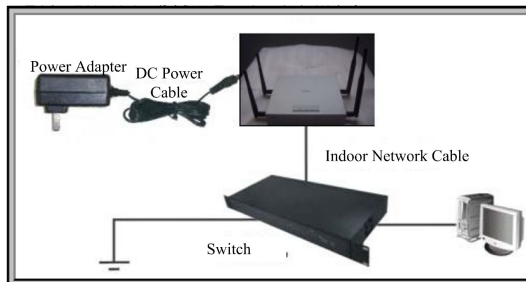
## 3.1 Installation Requirements

Before you begin to install the device, make sure the following conditions are met:

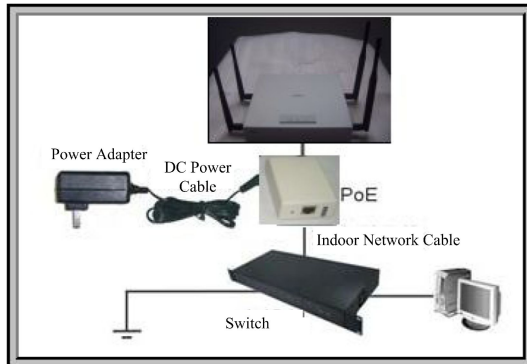
- A computer with the 10/100/1000 M Base-TX adaptive Ethernet NIC.
- The IP addresses of the Ethernet NIC and the device are in the same network segment (the default IP address of this device is 192.168.0.228), for example 192.168.0.1.
- An Internet Explorer 6.0 or a later version is recommended. Disable the proxy server setting of the Internet Explorer.
- Two network cables used to connect a device to a computer.

## 3.2 Hardware Installation

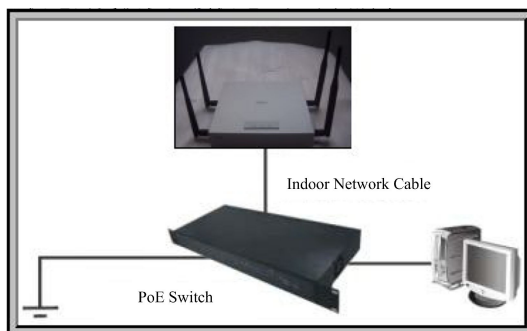
- The external power adapter can be a power supply through standard configuration, as shown in the following figure.



- When a switch does not support PoE power supply, the device can be powered by the 48 V Ethernet remote power supply through the PoE module of standard configuration, as shown in the following figure.



- The device can be powered directly through the switch supporting the standard PoE power supply, as shown in the following figure.



The wall mounting installation description of ZXV10 W812N V2 in the actual environment is described as follows.

1. Place the positioning cardboard on the wall required to be mounted with a device.
2. Hammer nails on the round holes of the positioning cardboard (It is recommend to use expansion screws in the accessories).
3. Remove the positioning cardboard and then place the device.

## 3.3 Computer Configuration

### 3.3.1 Checking Computer Configuration

#### Context

Disable the proxy service. Close the VPN software on the current computer and disable any running firewall or security software. This section provides an example of Microsoft Internet Explorer.

#### Steps

1. In a browser window, select **Tools > Internet Options** to open the **Internet Options** window.

2. In the **Internet Options** window, click the **Connections** tab and then click **LAN Settings**.
3. In the pop-up window, clear **Use a proxy server for your LAN** check box and then click **OK**.

– End of Steps –

## 3.3.2 Setting TCP/IP

### Context

This section takes the Windows XP operating system as an example to introduce TCP/IP configuration.

### Steps

1. In Windows task bar, select **Start > Control Panel**.
2. In **Control Panel**, double-click **Network Connections**.
3. In the **Network Connection** window, right-click **Local Area Connection** and then select **Properties**. The **Local Connection Properties** dialog box appears.
4. Select **Internet Protocol (TCP/IP)** and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.
5. In the **Internet Protocol (TCP/IP) Properties** dialog box, select **Use the following IP address** and then specify the IP address of the local computer and the IP address of the ZXV10 W812N V2 in the same network segment, that is, 192.168.0.x (in which, x is a decimal integer between 1 and 227 or between 229 and 254).
6. Click **OK** to save the configuration.

– End of Steps –

This page intentionally left blank.



# Chapter 4

## Configuration Preparation

---

### Table of Contents

Default Settings.....	4-1
Requirements Before Configuration.....	4-1
Logging in to the System.....	4-2

## 4.1 Default Settings

The default settings of the ZXV10 W812N V2 are described as follows.

Item	Default Setting
IP address/Subnet Mask of the Ethernet interface	The IP address is 192.168.0.228. The subnet mask is 255.255.255.0.
User name/Password	The initial user name/password of an ordinary user is username/username. The initial user name/password of the administrator is admin/admin.
Access point mode	Fit AP mode
Access point name	APxxxxxxxxxxx, where xxxxxxxxxxxx represents the device MAC address.
Country/Region	Uses the default value.
AC Discovery Mode	DHCP
WAN Mode	DHCP

## 4.2 Requirements Before Configuration

Before configuration, check and confirm the following items:

- An Ethernet cable (either cross-over or straight-through) is used to connect a computer to any Ethernet interface of the W812N device. Make sure that the corresponding LAN interface indicator is solid on or flashing. If wireless connection is adopted, make sure that WLAN configuration is working normally and the corresponding WLAN interface indicator is on or flashing.
- The **Internet Protocol (TCP/IP) Properties** attribute on this computer has been set correctly.
- It is required to disable the proxy server setting of the Web browser (Internet Explorer).

- Ask the service provider for necessary configuration data. Consult the service provider for the specific information.

## 4.3 Logging in to the System

### Context

The ZXV10 W812N V2 provides the configuration function based on a WEB page. Perform the configuration and management for the ZXV10 W812N V2 through the WEB browser.

The default language of ZXV10 W812N V2 Web pages is English.

### Steps

1. Open Internet Explorer, and type `http://192.168.0.228` (the default IP address of ZXV10 W812N V2 Ethernet interface) in the address bar and then press **Enter** to open the **Login** page as shown below.



#### Note:

Type the desired IP address and then press **Enter**. A dialog box appears indicating Internet Explorer will access to an unsafe network. Then, click **Yes** to open the **Login** page.

Please login to continue... 中文

Username

Password


2. Type a valid user name and password, and then click **Login** to open the WEB configuration page of the ZXV10 W812N V2 device.



#### Note:

The initial user name/password of an ordinary user is user/user. This user only has the authority to view the related **Status** information of this device. The initial user name/password of the administrator is admin/admin. This user has the authority to configure and manage the device through the WEB browser.

- Click **Logout** at the upper-right corner of the current WEB page and then the system will log out and return to the **Login** page.

- Click  Help to view the related help information on the current page.
- Click the **Help** tab to open the **Help** page to view the related help information.

– End of Steps –

This page intentionally left blank.

# Chapter 5

## Device Status

---

### Table of Contents

Checking Device Information.....	5-1
Checking Information of Network Interfaces .....	5-1
Checking WLAN Interface Information.....	5-3

## 5.1 Checking Device Information

### Steps

1. Click the **Status** tab and then select **Device Information** in the left pane. The **Device Information** page is displayed.

Model	ZXV10 W812N V2
Serial Number	ZTENW35B6C00002
batch number	07dcoS20020406
Hardware Version	V3.0
Software Version	V2.0
Boot Loader Version	V2.0
AP Name	AP384608C4DBD5

2. On the **Device Information** page, view the information such as **Model**, **Serial Number**, **batch number**, **Hardware Version**, **Software Version**, **Boot Loader Version**, and **AP Name**.

– End of Steps –

## 5.2 Checking Information of Network Interfaces

### 5.2.1 Checking Ethernet Interface Information

### Steps

1. Click the **Status** tab and then select **Network Interface > Ethernet** in the left pane. The **Ethernet** page is displayed.

Ethernet Port	WAN
MAC Address	d0:15:4a:f4:66:02
Status	Up
Mode	1000M/FULL DUPLEX
Packets Received/Bytes Received	27539/2325288
Packets Sent/Bytes Sent	25161/14478362

2. On the **Ethernet** page, check the Ethernet interface information such as **Ethernet Port**, **MAC Address**, **Status**, **Mode**, and **Packets Sent/Bytes Sent**.

**Note:**

Click **Refresh** on this page to refresh the related information of the current device.

– End of Steps –

## 5.2.2 Checking Network Connection Information

### Steps

1. Click the **Status** tab and then select **Network Interface > WAN Connection**. The **WAN Connection** page is displayed.

DHCP	WAN
WAN MAC	d0:15:4a:f4:66:02
NAT	Disabled
IP	12.10.10.6/255.255.255.0
DNS	12.10.10.66/0.0.0.0/0.0.0.0
Gateway	12.10.10.1
Connection Status	Connected
Remaining Lease Time	351 sec

2. On the **WAN Connection** page, check the established connection information such as **DHCP**, **WAN MAC**, **NAT**, **IP**, **DNS**, **Gateway**, **Connection Status**, and **Remaining Lease Time**.

**Note:**

Click **Refresh** on this page to refresh the related information of the current device.

– End of Steps –

## 5.3 Checking WLAN Interface Information

### Steps

1. Click the **Status** tab and then select **User Interface > WLAN**. The **WLAN** page is displayed.

Enable Wireless RF1	Enabled
Channel	1
WDS Mode	Disabled
SSID1 Enable	Enabled
SSID1 Name	wireless
Authentication Type	Open System
Encryption Type	None
MAC Address	4c:ac:0a:26:ab:4a
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	0/0
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	5109

2. On the **WLAN** page, check the WLAN interface information such as **Enable Wireless RF1**, **Channel**, **WDS Mode**, **SSID1 Enable**, **SSID1 Name**, **Authentication Type**, **Encryption Type**, **MAC Address**, **Packets Received/Bytes Received**, **Packets Sent /Bytes Sent**, **Error Packets Received**, **Error Packets Sent**, **Discarded Receiving Packets**, and **Discarded Sending Packets**.



**Note:**

Click **Refresh** on this page to refresh the related information of the current device.

---

**– End of Steps –**



# Chapter 6

## Network Configuration

---

### Table of Contents

Broadband Connection Configuration .....	6-1
WLAN Configuration.....	6-4
LAN Management .....	6-24
Routing Management .....	6-26

## 6.1 Broadband Connection Configuration

### 6.1.1 Configuring Broadband Connection (Fit AP)

#### Context

For ZXV10 W812N V2, there are two working modes of wireless access point: fat AP mode and fit AP mode. The default system working mode is the fit AP mode.

If it is required to change the access point mode of ZXV10 W812N V2, refer to **Setting an AP Mode**.



#### Note:

After the access point mode is switched, the device restarts.

---

#### Steps

1. Click the **Network** tab and then select **WAN > WAN Connection**. The following page is displayed.



The device will be automatically rebooted after the settings in this page is submitted.

IP Version 
  
 AC Discovery Mode 
  
 AC Type 
  
 AC Name 
  
 Enable CAPWAP Encryption 
  
 WAN Type 
  
 Enable Verify AC 
  
 Enable VLAN 
  
 VLAN ID 
  
 802.1p 
  
 Enable DSCP 
  
 DSCP 
  
 MTU 
  
 ARP BaseReach Time  (20~1200)
   
 ARP Retrans Time  (1~3)
   
 ARP DelayProbe Time  (1~60)

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
IP Version	Supported protocol versions include IPv4, IPv6 and IPv4/v6. The default setting is IPv4.
AC Discovery Mode	Include DHCP, Static, DNS and Broadcast. The default setting is DHCP.
AP Type	Adapter
AC Name	Configurable when <b>AC Discovery Mode</b> is <b>DNS</b> .
Enable CAPWAP Encryption	Enable/Disable CAPWAP encryption.
WAN Type	If <b>IP Version</b> is <b>IPv4</b> , the supported modes include DHCP, Static and PPPoE. If <b>IP Version</b> is <b>IPv6</b> or <b>IPv4/v6</b> , the supported modes include DHCP and PPPoE. The default mode is DHCP, the WAN mode is set as DHCP.
Enable Verify AC	Enable/Disable AC verification function when <b>WAN Type</b> is <b>DHCP</b> .
Enable VLAN	Enable/Disable the VLAN configuration function. VLAN ID and 802.1p are used to set the VLAN and priority for the selected device.
VLAN ID	VLAN ID of the WAN interface data packet. The value range is 0 to 4094.

Parameter	Description
802.1p	Specify the processing priority. It only applies to multiple WAN connections, the range is 0 to 7. The default value is 0, which means no priority. A bigger value indicates a higher priority.
Enable DSCP	Enable/Disable the Differential Services Code Point (DSCP) function of data flow.
DSCP	Specify the DSCP value. The value range is 0 to 63.
MTU	Specify the Maximum Transmission Unit (MTU) value. The default value is 1448.
ARP BaseReach Time	Specify ARP basic reachable time
ARP Retrans Time	Specify ARP retransmission time
ARP DelayProbe Time	Specify ARP probe time delay

3. Click **Submit**.

**Note:**

The configuration modification on this page only takes effect after the device restarts.

– End of Steps –

## 6.1.2 Configuring Broadband Connection (Fat AP)

### Prerequisite

The access point mode of the device is **Fat**.

### Steps

1. Click the **Network** tab and then select **WAN > WAN Connection** in the left pane. The following page is displayed.



The device will be automatically rebooted after the settings in this page is submitted.

IP Version	<input type="text" value="IPv4"/>	
Working Mode	<input type="text" value="Bridge"/>	
WAN Type	<input type="text" value="DHCP"/>	
Enable VLAN	<input type="checkbox"/>	
VLAN ID	<input type="text"/>	
802.1p	<input type="text" value="0"/>	
Enable DSCP	<input type="checkbox"/>	
DSCP	<input type="text"/>	
MTU	<input type="text" value="1400"/>	
ARP BaseReach Time	<input type="text" value="600"/>	(20~1200)
ARP Retrans Time	<input type="text" value="1"/>	(1~3)
ARP DelayProbe Time	<input type="text" value="15"/>	(1~60)

- Configure the parameters. For detailed information, refer to **Configuring Broadband Connection (Fit AP)**.
  - Working mode: supports bridge mode and route mode. By default, it is the bridge mode.
  - WAN mode: When **IP Version** is **IPv4**, DHCP, Static and PPPoE are all supported while when **IP Version** is **IPv6** or **IPv4/v6**, DHCP and PPPoE are supported. By default, it is DHCP.
- Click **Submit**.

**Note:**

The configuration modification on this page only takes effect after the device restarts.

– End of Steps –

## 6.2 WLAN Configuration

### 6.2.1 Setting Basic Information

#### Context

The system provides two wireless NICs. Users can configure these two wireless NICs respectively.

- NIC1: 2.4 GHz frequency band, supports 802.11b、802.11g、802.11n.
- NIC2: 5 GHz frequency band, supports 802.11a、802.11n.

### Steps

1. Select **Network > WLAN > Basic**. The following page is displayed.

2. Configure the parameters.


- When **Network Card1** is selected, the WEB page is as shown above. Refer to the parameter descriptions in the table below to configure parameters.

Parameter	Description
Network Card	Use Network Card1.
Enable Wireless RF	Enable/Disable the WLAN RF function.
Enable Isolation	Enable/Disable the SSID isolation function. It is disabled by default.
Mode	The supported modes include IEEE 802.11b Only, IEEE 802.11g Only, IEEE 802.11n Only, Mixed(802.11b+802.11g) and Mixed(802.11b+802.11g+802.11n). The default is Mixed(802.11b+802.11g).
Country/Region	Specify a country or region. The default is China.

Parameter	Description
Band	If <b>Network Card</b> is <b>Network Card1</b> , the frequency band is 2.4 G.
MIMO	The options are 1*1, 1*2, 2*1 and 2*2. The default is 2*2.
11N Rate	Specify the wireless transmission rate. The default is <b>Auto</b> .
Channel	Specify a channel according to the country code. The available options are Auto or 1–13. The default channel is set as Auto. The wireless channel used for the communication between the wireless access point and wireless station is determined by the local administration. All stations communicating with ZXV10 W812N V2 must use the same channel.
Only Select Channel 1/6/11	Determine whether to select only channel 1/6/11 or select all channels.
Total Maximum Clients	Specify the maximum number of users that are allowed to access. The range is from 1 to 512. The default is 128.
SGI Enable	Enable/Disable the SGI function.
A-MPDU Enable	Enable/Disable the A-MPDU function.
Beacon Interval	It is 100 ms by default.
Power Type	Support configuration by percent, configuration by actual power value (unit: dBm), and configuration by actual power value (unit: mW).
Transmitting Power	The available options are Auto, 100 %, 90 %, 80 %, 70 %, 60 %, 50 %, 40 %, 30 %, 20 %, 12.5 % or 10 %. The default value is 100 %. The power level is the ratio of the output power to the maximum power. A greater power indicates a longer transmitting distance.
QoS Type	The available options are Disabled, WMM and SSID. The default option is WMM.
RTS Threshold	Upper limit of sending requests
DTIM Interval	DTIM interval
Fragment Threshold	The size of the wireless fragment used to specify the size of a data packet. The data packet will be divided into fragments if the size of a data packet is greater than the fragment threshold. The data packet will be divided and transmitted in a small size.
WIDS Mode	The supported modes include Access, Monitor and Mixed. The default option is Access.
WIDS Scan Period	Specify the scan period of WIDS. The default value is 120 ms.
WIDS Scan Mode	The options are current channel and all channels.

Parameter	Description
Protection Mode	Support None, CTS Only, and RTS/CTS.
5G Access First	Enable/Disable the 5G access first function.

- When **Network Card2** is selected, the WEB page is as shown in the following figure. Configure the parameters. Refer to the following table.

 If AP allows associations from the IEEE 802.11n mode STAs, please make sure SSID security without TKIP or WEP Encryption Algorithm mode configured.

Network Card: Network Card2

Enable Wireless RF:

Enable Isolation:

Mode: Mixed(802.11a+802.11n)

Country/Region: China

Band: 5G

Band Width: 20MHz

MIMO: 2\*2

11N Rate: Auto

Support Rate:  6Mbps  9Mbps  12Mbps  
 18Mbps  24Mbps  36Mbps  
 48Mbps  54Mbps

Channel: Auto

Only Select Channel 1/6/11:

Total Maximum Clients: 128 (1 ~ 512)

SIG Enable:

A-MPDU Enable:

Beacon Interval: 100 ms

Power Type: config by percent

Transmitting Power: 100%

QoS Type: WMM

RTS Threshold: 2347

DTIM Interval: 1

WIDS Mode: Access

WIDS Scan Period: 120

WIDS Scan Mode: Current Channel

Protection Mode: None

Application Scenarios: User configuratio

5G Access First:

Parameter	Description
Network Card	Uses Network Card2.
Enable Wireless RF	Enables or disables the WLAN RF function.
Enable Isolation	Enables or disables the SSID isolation function. The default is disabled.
Mode	Supports IEEE 802.11a Only, IEEE 802.11n Only and Mixed(802.11a+802.11n). The default is Mixed(802.11a+802.11n).
Country/Region	Select a country or region according to the actual situation. The default is China.

Parameter	Description
Band	If <b>Network Card</b> is <b>Network Card2</b> , the frequency band is 5 G.
Band Width	The available options are 20 MHz, 40 MHz and automatic. The default is 20 MHz.
MIMO	The options are 1*1, 1*2, 2*1 and 2*2. The default is 2*2.
11N Rate	Specifies the transmission rate of 802.11n. There are 17 rates and the default value is auto.
Channel	Proper channel can be selected according to country code. The available options are Auto, 149, 153, 157, 161 or 165. The default is Auto. The channel used for the communication between the wireless access point and wireless station is determined by local policy. All wireless stations which communicate with ZXV10 W812N V2 must use the same channel.
Total Maximum Clients	Specifies the maximum number of connected users. The range is 1 to 512. The default is 128.
SIG Enable	Enables or disables the SIG function.
A-MPDU Enable	Enables or disables the A-MPDU function.
Beacon Interval	The beacon interval is 100 ms by default.
Transmitting Power	Supports automatic, 100 %, 90 %, 80 %, 70 %, 60 %, 50 %, 40 %, 30 %, 20 %, 12.5 % or 10 %. The default is 100 %. The power class refers to percentage of output power to maximum power. A higher power indicates a farther transmission distance.
QoS Type	The options are disabled, WMM and SSID. The default is WMM.
RTS Threshold	The upper limit of transmission request.
DTIM Interval	DTIM time patch.
Fragment Threshold	Refers to the size of the wireless patch. It is used to limit the size of data packet. If the size is greater than the threshold value, the data packet will be fragmented and transmitted as multiple packets.
WIDS Mode	Includes three modes such as Access, Monitor and Mixed. The default is Access.
WIDS Scan Period	Specifies the value of WIDS scan interval. The default is 120 ms.
WIDS Scan Mode	The available options are current channel and all channels.



Parameter	Description
Protection Mode	Supports None, CTS Only, and RTS/CTS.
5G Access First	Enables or disables the 5G access first function.

3. Click **Submit**.

– End of Steps –

## 6.2.2 Configuring SSID

### Steps

1. Select **Network > WLAN > SSID Settings** . The following page is displayed.

Choose SSID

Network Card

Hide SSID

Enable SSID

Enable SSID Isolation

Isolation Mode

Maximum Clients  (1 ~ 512)

SSID Name  (1 ~ 32 characters)

Priority

VLAN ID

802.1p

Probe Response Mode

As Management SSID

Manager Frame Rate

2. Configure the parameters. Refer to the following table.

Parameter	Description
Choose SSID	Select the SSID required to be configured. The available options are from SSID1 to SSID32.
Network Card	Display the wireless NIC corresponding to current SSID. SSID1–SSID16 corresponds to the NIC 1 while SSID17–SSID32 corresponds to NIC 2.
Hide SSID	Hide this SSID.
Enable SSID	Enable/Disable this SSID.
Enable SSID Isolation	Enables or disables the internal isolation function of this SSID.

Parameter	Description
Isolation Mode	Select the corresponding isolation mode. The available options are Unicast, Broadcast, Multicast and ALL. The default option is ALL.
Maximum Clients	Set the maximum number of users that are allowed to connect to the SSID. The default value is 32. The range is from 1 to 512.
SSID Name	Set a name for this SSID. A name is composed of 1–32 characters.
Priority	Set the SSID priority ranging from 0 to 7. The default value is 0, indicating no priority is set. A greater value indicates a higher priority.
VLAN ID	The VLAN label of an interface data package. The ID ranges from 0 to 4094.
802.1p	Set the priority ranging from 0 to 7. The default value is 0, indicating no priority is set. A greater value indicates a higher priority.
As Management SSID	This function is disabled by default. If you select <b>As Management SSID</b> , the user associated with this SSID can manage this device.
Manager Frame Rate	Support various rates including 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 12 Mbps.

3. Click **Submit**.

– End of Steps –

## 6.2.3 Setting Security Information

### Steps

1. Select **Network > WLAN > Security**. The following page is displayed.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

WPA Passphrase  (8 ~ 63 characters)

Enable WPA Group Key Update

WPA Group Key Update Interval  sec

WPA Encryption Algorithm

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Choose SSID	Specifies the SSID to be configured. The range is SSID1 to SSID15.
Authentication Type	Supports Open System, Shared Key, Open System & Shared Key, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, WPA-EAP, WPA2-EAP, WPA/WPA2-EAP, WAPI-PSK, WAPI-CERT and WEP-EAP.
WPA Passphrase	WPA encryption key setting. The range is 8–63 characters.
Enable WPA Group Key Update	Enables or disables WPA group key updating function. The default is enabled.
WPA Group Key Update Interval	Key updating interval. The default value is 600 s.
WPA Encryption Algorithm	WPA encryption algorithm, supporting TKIP, AES and TKIP+AES.

**Authentication Type** may be selected among Open system, WPA-PSK encryption, WPA-EAP encryption, WEP encryption, WAPI-PSK encryption and WAPI-CERT encryption.

- **Open System** means no encryption.
- WPA-PSK encryption
  - WPA encryption means Wi-Fi Protected Access, including three modes, namely WPA-PSK, WPA2-PSK and WPA/WPA2-PSK.
  - i. In the **Authentication Type** list, select **WPA-PSK** , **WPA2-PSK** , or **WPA/WPA2-PSK** to enable WPA-PSK encryption.
  - ii. Set the parameters as required by referring to the parameter description in the previous table.
- WPA-EAP encryption
  - i. In the **Authentication Type** list, select **WPA-EAP** , **WPA2-EAP** or **WPA/WPA2-EAP** to enable the WPA-EAP encryption, as shown in the following figure.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

Server Type

Server IP Address

Server Port  (0 ~ 65535)

Secret  (1 ~ 64 characters)

Reauth Period  sec

Enable Preauth

Enable WPA Group Key Update

WPA Group Key Update Interval  sec

WPA Encryption Algorithm

ii. Configure the parameters. Refer to the following table.

Parameter	Description
Server Type	Specifies the server type. The options are Master Auth Server, Master Acct Server, Backup Auth Server, and Backup Acct Server. The default is Master Auth Server.
Server IP Address	Specifies the IP address of the authentication server, for example 192.168.1.1.
Server Port	Specifies the port of the authentication server, for example, 1812. The range is 0 to 65535.
Secret	Specifies the WPA-EAP encryption key. The range is 1 to 64 characters.
Reauth Period	The default is 3600 seconds.
Enable Preauth	Enables/Disables the pre-authentication function. The function is disabled by default.
Enable WPA Group Key Update	Enables/Disables the WPA group key update function. The function is enabled by default.
WPA Group Key Update Interval	Specifies the interval of WPA group key update. The default is 600 seconds.
WPA Encryption Algorithm	Specifies the WPA encryption algorithm. There are three options, AES, TKIP and TKIP+AES. The default is TKIP.

- WEP encryption

WEP, abbreviated from Wired Equivalent Privacy, is a commonly used WLAN security protocol.

- i. Select **Shared Key** or **Open System & Shared Key** for **Authentication Type**. The following page is displayed.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

WEP Encryption

WEP Encryption Level

WEP Key Index

WEP Key1

WEP Key2

WEP Key3

WEP Key4

13 ASCII chars or 26 hexadecimal digits can be entered for 128-bit WEP Encryption Key.  
 5 ASCII chars or 10 hexadecimal digits can be entered for 64-bit WEP Encryption Key.

- ii. Configure the parameters according to the parameter description in the table below.

Parameter	Description
WEP Encryption	Enables or disables the WEP encryption function. The default is enabled.
WEP Encryption Level	There are two types of WEP key, namely 64 bit and 128 bit.
WEP Key Index	Specifies corresponding key value.
WEP Key1/2/3/4	Specifies WEP encryption key value. 64-bit WEP key corresponds with 5 ASCII characters or 10 hexadecimal characters. 128-bit WEP key corresponds with 13 ASCII characters or 26 hexadecimal characters.

- WAPI-PSK encryption

- i. Select **WAPI-PSK** as the **Authentication Type**. The following page is displayed.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

WAPI Key Mode

WAPI Key  (8 ~ 64 characters)

- ii. Configure the parameters. Refer to the following table.

Parameter	Description
WAPI Key Mode	Supports two modes, namely ASCII and HEX. The default is ASCII.
WAPI Key	Specifies WAPI key value. The length is 8 to 64 characters.

- WAPI-CERT encryption

- Select **WAPI-CERT** as the **Authentication Type**. The following page is displayed.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

Certificate Server IP

Certificate Server Port  (0 ~ 65535)

Certificate Management

- Fill in **Certificate Server IP** and **Certificate Server Port**.
- Click the **Certificate Uploading** button, and then select the proper type of certificate file in the dialog box that appears. Click **Upload**.



**Note:**

Certificate files include AS certificate, AP certificate and CA certificate. If only AP and CA certificates are necessary, upload AP certificate first and then AS certificate.

- WEP-EAP encryption

- Select **WEP-EAP** as the **Authentication Type**. The following page is displayed.



With TKIP or WEP Encryption Algorithm configured, AP does not allow associations from the IEEE 802.11n mode STAs.

Choose SSID

Authentication Type

Server Type

Server IP Address

Server Port  (0 ~ 65535)

Secret  (1 ~ 64 characters)

Reauth Period  sec

Enable Preauth

WEP Encryption

- ii. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Server Type	Specify the server type. The options are Master Auth Server, Master Acct Server, Backup Auth Server and Backup Acct Server. The default is Master Auth Server.
Server IP Address	Specify the IP address of the authentication server, for example 192.168.1.1.
Server Port	Specify the port of the authentication server, for example 1812. The range is 0 to 65535.
Secret	Specify the WPA-EAP encryption key. The range is 1–64 characters.
Reauth Period	The default is 3600 seconds.
Enable Preauth	Enable/Disable the pre-authentication function. The function is disabled by default.
WEP Encryption	Enable/Disable WEP encryption. The default is disabled.

3. Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.4 Setting Rate Limits

### Context



**Note:**

The value of the rate limit is 0, which represents there is no rate limit.

### Steps

1. Select **Network > WLAN > Rate Limit** from the menu bar. The following page is displayed.



Control Type switch takes effect immediately and the settings of the old Control Type will be lost.

The item's Rate Limit function will not take effect if its value is "0".

Control Type

Choose SSID

SSID Downlink Rate Guarantee  (0 ~ 250000 kbps)

SSID Downlink Rate Limit  (0 ~ 250000 kbps)

STA Downlink Rate Limit  (0 ~ 250000 kbps)

SSID Uplink Rate Guarantee  (0 ~ 250000 kbps)

SSID Uplink Rate Limit  (0 ~ 250000 kbps)

STA Uplink Rate Limit  (0 ~ 250000 kbps)

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Control Type	Support SSID/STA and MAC.
Choose SSID	Specify the SSID to be configured. The range is SSID1 to SSID16.
SSID Downlink Rate Guarantee	The available range is from 0 kbps to 250000 kbps. It is 0 by default, which represents there is no rate limit.
SSID Downlink Rate Limit	The available range is from 0 kbps to 100000 kbps. It is 0 by default, which represents there is no rate limit.
STA Downlink Rate Limit	The available range is from 0 kbps to 100000 kbps. It is 0 by default, which represents there is no rate limit.
SSID Uplink Rate Limit	The available range is from 0 kbps to 100000 kbps. It is 0 by default, which represents there is no rate limit.



Parameter	Description
STA Uplink Rate Limit	The available range is from 0 kbps to 100000 kbps. It is 0 by default, which represents there is no rate limit.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.5 Setting an Access Control List

### Steps

- Select **Network > WLAN > Access Control List** from the menu bar to open the **Access Control List** page as shown below.


Choose SSID

Mode

MAC Address  :  :  :  :  :

SSID	MAC Address	Delete
There is no data, please add one first.		

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Choose SSID	Select the SSID required to be configured. The available options are from SSID1 to SSID32.
Mode	The available options are Disabled, Block, and Permit, which indicates no SSID channel control, block and permit a device connection of the corresponding MAC address respectively. The default option is Disabled.
MAC Address	Type the MAC address of the device to be controlled.
Delete	Click  to delete the corresponding control channel item.

- Click **Add** to submit the current configuration.

– End of Steps –

## 6.2.6 Checking Associated Devices

### Steps

1. Select **Network > WLAN > Associated Devices** from the menu bar to open the **Associated Devices** page as shown below.

Choose SSID

MAC Address	Associating Status	Packets Sent	QoS
SSID	Power Saving Status	Packets Received	RSSI(dBm)
There is no data.			

2. In **Choose SSID**, select the SSID interface required to be viewed. The user can view the detailed information of the associated device corresponding to the SSID interface. By default, the system displays the device information associating with SSID1 interface.



**Note:**

Click **Refresh** on this page to refresh the related information of the current device.

– End of Steps –

## 6.2.7 Scanning an Access Point

### Prerequisite

The corresponding SSID needs to be enabled.

### Steps

1. Select **Network > WLAN > AP Scanning** from the menu bar to open the **AP Scanning** page as shown below.



WIDS Mode is Access, this page cannot be configured.

Network Card

Channel

SSID	Channel	Security	Beacon Interval
MAC	SNR	RSSI(dBm)	NSI(dBm)
There is no data.			

2. In the **Network Card** and **Channel** drop-down list box, select the channel required to be scanned as required.

**Caution!**

When the SSID is disabled or the WDS mode is Access, this page cannot be configured.

- Click **Scan** and then the corresponding scan result will be displayed on the refreshed page.

– End of Steps –

## 6.2.8 Configuring WDS

### Steps

- Select **Network > WLAN > WDS** from the menu bar to open the **WDS** page as shown below.

Network Card

WDS Mode

- Select the NIC required to be configured and then configure the parameters according to the WDS mode.
  - When **WDS Mode** is **Disabled**, the configuration page is as shown above and there is no need to configure the parameters.
  - When **WDS Mode** is **WDS+Root**, the configuration page is as shown below and then configure the parameters according to the parameter descriptions in the table below.

NOTE: The channel and security settings of the repeater must be the same as the root.

Network Card

WDS Mode

WDS Interface MAC Address 4c:ac:0a:26:ab:4a

Repeater MAC Address  :  :  :  :  :

Parameter	Description
WDS Interface MAC Address	Display the MAC address information of the WDS interface.
Repeater MAC Address	Set the MAC address of the relay device.

- When **WDS Mode** is **WDS+Repeater**, the configuration page is as shown below. Configure the parameters according to the parameter description in the table below.

NOTE: The channel and security settings of the repeater must be the same as the root.

Network Card

WDS Mode

WDS Interface MAC Address: 4c:ac:0a:26:ab:4a

Root MAC Address  :  :  :  :  :

Parameter	Description
WDS Interface MAC Address	Display the MAC address information of the WDS interface.
Root MAC Address	Set the MAC address of the root AP.

3. Click **Submit** to submit the current configuration.
- End of Steps –

## 6.2.9 Configuring STA WMM

### Steps

1. Select **Network > WLAN > STA WMM** from the menu bar to open the **STA WMM** page as shown below.

Network Card

Choose AC

AIFSN  (0 ~ 15)

ECWMin  (0 ~ 15)

ECWMax  (0 ~ 15)

TXOP  (0 ~ 255)

Qlength  (0 ~ 1000)

SRL  (0 ~ 255)

LRL  (0 ~ 255)

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Network Card	Select the WMM NIC required to be configured.

Parameter	Description
Choose AC	The available options are VO, VI, BE or BK.
AIFSN	The available range is 2-15.
ECWMin	The available range is 0-15.
ECWMax	The available range is 0-15.
TXOP	The available range is 0-255.
Qlength	The available range is 0-1000.
SRL	The available range is 0-255.
LRL	The available range is 0-255.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.10 Configuring AP WMM

### Steps

- Select **Network > WLAN > AP WMM** from the menu bar to open the **AP WMM** page as shown below.

Network Card

Choose AC

AIFSN  (0 ~ 15)

ECWMin  (0 ~ 15)

ECWMax  (0 ~ 15)

TXOP  (0 ~ 255)

Qlength  (0 ~ 1000)

SRL  (0 ~ 255)

LRL  (0 ~ 255)

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Network Card	Select the WMM NIC required to be configured.
Choose AC	The available options are VO, VI, BE or BK.
AIFSN	The available range is 2-15.
ECWMin	The available range is 0-15.
ECWMax	The available range is 0-15.
TXOP	The available range is 0-255.

Parameter	Description
Qlength	The available range is 0-1000.
SRL	The available range is 0-255.
LRL	The available range is 0-255.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.11 Setting Channel Auto-Switch

### Steps

- Select **Network > WLAN > Channel Auto-Switch** from the menu bar. The following page is displayed.

Network Card  ▼

Enable Channel Auto-Switch

Adjustment Type  ▼

RSSI Threshold  (-90 ~ 10 dBm)

Cycle Period  (1 ~ 1440 min)

Duration  (0 ~ 3600 s)

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Network Card	Select network card that needs automatic channel adjustment
Enable Channel Auto-Switch	Enable/Disable frequency auto-switch function
Adjustment Type	Support two types, including adjust on startup, adjust cyclically
RSSI Threshold	Specify the threshold of signal intensity. The range is from -90 dBm ~ 10 dBm. The default is -30 dBm
Cycle Period	Specify the cycle period of channel adjustment. The range is from 1 min to 1440 min. The default is 30 min
Duration	Specify the duration of channel adjustment. The range is from 0 s to 3600 s

- Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.12 Setting Wireless Mode

### Steps

1. Select **Network > WLAN > Wireless Mode** from the menu bar. The following page is displayed.



The device will be automatically rebooted after the settings of Wireless Mode and Node Type in this page is submitted.

Network Card    
 Wireless Mode

2. Select the network card to be configured. Specify **Wireless Mode** to be **Only Coverage** or **Only Backhaul**.
3. Click **Submit** to submit the current configuration.

– End of Steps –

## 6.2.13 Setting Mesh Configuration

### Steps

1. Select **Network > WLAN > Mesh Configuration** from the menu bar. The following page is displayed.

Network Card    
 Enable Wireless Mesh   
 Mesh ID  (1 ~ 32 characters)  
 Mesh NodeType

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Network Card	Select network card1 or network card2 as the mesh backhaul network card
Enable Wireless Mesh	Enable/Disable mesh function
Mesh ID	Specify mesh network identification
Mesh Node Type	Support two types, including normal node and gateway node. The default is normal node

3. Click **Submit** to submit the current configuration.

– End of Steps –

## 6.3 LAN Management

### 6.3.1 Managing Addresses

#### Context

The DHCP start IP address and the DHCP end IP address should be inside the subnet of LAN IP.

#### Steps

1. Select **Network > LAN > Address Management** from the menu bar to open the **Address Management** page as shown below.

NOTE: 1. The DHCP Start IP Address and DHCP End IP address should be in the same subnet as the LAN IP.

LAN IP Address

Subnet Mask

Enable STP

DHCP Service

DHCP Start IP Address

DHCP End IP Address

DNS Server1 IP Address

DNS Server2 IP Address

DNS Server3 IP Address

Default Gateway

Lease Time  sec

Allocated Address

MAC Address	IP Address	Remaining Lease Time	Host Name	Port
There is no data.				

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
LAN IP Address	IP address of LAN group (interface subnet). The default IP address is 192.168.1.1.
Subnet Mask	Subnet mask of LAN group
Enable STP	Enable/Disable the STP function.



Parameter	Description
DHCP Service	<ul style="list-style-type: none"> <li>When the access point mode of the device is <b>fit</b>, the supported status includes DHCP Server and OFF. It is DHCP Server by default.</li> <li>When the access point mode of the device is <b>fat</b>, the supported status includes DHCP Server, DHCP Relay and OFF. It is DHCP Server by default.</li> </ul>
DHCP Start IP Address	The start IP address allocated by the DHCP Server. Make sure that this IP address is in the same network segment with that of ZXV10 W812N V2 before the start or end IP address is required to be modified.
DHCP End IP Address	The end IP address allocated by the DHCP Server. Make sure that this IP address is in the same network segment with that of ZXV10 W812N V2 before the start or end IP address is required to be modified.
DNS Server1/2/3 IP Address	IP addresses of the DNS server. There are three available addresses.
Default Gateway	It is 192.168.1.1 by default.
Lease Time	<p>Lease time is the duration for which the DHCP server leases the IP address, with seconds as its unit. The default value is 86400 seconds.</p> <p>Lease time stands for the duration when an IP address can be leased from the IP pool by the client dynamically. When the lease time expires, the DHCP server can lease this IP address to this client again or assign a new IP address for this client.</p>
Allocated Address	IP address allocated. The page displays IP addresses allocated and the basic information of devices that uses the IP addresses.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 6.3.2 Managing DHCP Conditional Serving Pool

### Prerequisite

The access point mode of the device is **fat**.




### Steps

- Select **Network > LAN > DHCP Conditional Serving Pool** from the menu bar to open the **DHCP Conditional Serving Pool** page as shown below.

NOTE: DHCP Conditional Serving Pool's Start IP Address and End IP Address should be in the same subnet as the LAN IP.

Start IP Address

End IP Address

Port	Start IP Address	End IP Address	Modify
SSID1	0.0.0.0	0.0.0.0	
SSID16	0.0.0.0	0.0.0.0	
SSID17	0.0.0.0	0.0.0.0	

2. Type **Start IP Address** and **End IP Address**, Click **Modify**.

– End of Steps –

## 6.3.3 Managing an IPv6 Address

### Steps

1. Select **Network > LAN > IPv6 Address Management** from the menu bar to open the **IPv6 Address Management** page as shown below.

LAN IPv6 Address

2. On this page, you can re-configure the IPv6 address of this terminal.
3. Click **Submit** to submit the current configuration.

– End of Steps –

## 6.4 Routing Management

### 6.4.1 Configuring a Static Route ( IPV4 )

#### Steps

1. Select **Network > Routing > Static Routing(IPV4)** from the menu bar to open the **Static Routing(IPV4)** page as shown below.

WAN Connection



Network Address

Subnet Mask

Gateway

Network Address	Subnet Mask	Gateway	WAN Connection	Status	Modify	Delete
There is no data, please add one first.						

- Configure the parameters according to the descriptions in the table below.

Parameter	Description
WAN Connection	Select the corresponding interface as required.
Network Address	Network address of the destination network
Subnet Mask	Subnet mask of the destination network
Gateway	IP address of the gateway (next hop)
Modify	Click  to edit the corresponding static route rule.
Delete	Click  to delete the corresponding static route rule.

- Click **Add** to submit the current configuration.

– End of Steps –

## 6.4.2 Configuring a Static Route(IPV6)

### Steps

- Select **Network > Routing > Static Routing(IPV6)** from the menu bar to open the **Static Routing(IPV6)** page as shown below.

WAN Connection



Prefix  /

Gateway

WAN Connection	Prefix	Gateway	Status	Modify	Delete
There is no data, please add one first.					

- Configure the parameters according to the descriptions in the table below.

Parameter	Description
WAN Connection	Select corresponding interface as needed

Parameter	Description
prefix	Type IPV6 address in the former space, and type subnetwork prefix length in the later space
Gateway	Gateway (next hop) IP address
Modify	Click  to edit the corresponding static route rule.
Delete	Click  to delete the corresponding static route rule.

- Click **Add** to submit the current configuration.

– End of Steps –

## 6.4.3 Setting a Dynamic Route

### Context

This section describes how to set a dynamic route.

### Steps

- Select **Network > Routing > Dynamic Routing**. The following page is displayed.

Enable RIP

Version

Authentication

Authentication Key

- Configure the parameters. Refer to the following table.

Parameter	Description
Enable RIP	Enable/Disable RIP.
Version	Support RIP v1, RIP v2, and RIP v1 Compatible.
Authentication	Support No Authentication, Simple Password, and MD5 Authentication.
Authentication Key	Refer to the authentication key.

- Click **Submit** to submit the current configuration.

– End of Steps –

# Chapter 7

## Security Configuration

---

### Table of Contents

Configuring a Firewall.....	7-1
Configuring IP Filter.....	7-2
Configuring MAC Filter .....	7-4
Viewing a Service List .....	7-5
Configuring the ALG Switch.....	7-5

## 7.1 Configuring a Firewall

### Steps

1. Select **Security > Firewall** from the menu bar to open the **Firewall** page as shown below.

Enable Anti-Hacking Protection

Firewall Level

Enable DNS Anti-Hacking Protection

Instruction of firewall level:

High: Allow legal WAN side access, but prohibit Ping from WAN side.

Middle: Allow legal WAN side access and resist certain types of dangerous data travelling over the Internet.

Low: Allow legal WAN side access and Ping from WAN side.

Off: **This option is not recommended.** If the firewall is disabled, the device will be open to the hacking and danger from the internet.

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable Anti-Hacking Protection	Enable/Disable the function of preventing unauthorized access.

Parameter	Description
Firewall Level	<p>Select high, middle, low or off as required.</p> <p>Firewall level description</p> <ul style="list-style-type: none"> <li>● High: Allow legal WAN side access, but prohibit PING from the WAN side.</li> <li>● Middle: Allow legal WAN side access and resist certain types of dangerous data traveling over Internet.</li> <li>● Low: Allow legal WAN side access and PING from the WAN side.</li> <li>● Off: <b>This option is not recommended.</b> if the firewall is disabled, the device will be open to the hacking and danger from the Internet.</li> </ul>
Enable DNS Anti-Hacking Protection	Enable/Disable the DNS anti-hacking protection

3. Click **Submit** to submit the current configuration.

– End of Steps –

## 7.2 Configuring IP Filter

### Prerequisite

The access point mode of the device is **fat**.

### Steps



1. Select **Security > IP Filter** from the menu bar to open the **IP Filter** page as shown below.

Enable   
 Protocol   
 Name   
 Start Source IP Address   
 End Source IP Address   
 Start Destination IP Address   
 End Destination IP Address   
 Start Source port   
 End Source port   
 Start Destination port   
 End Destination port   
 Ingress   
 Egress   
 mode

Enable	Name	Start Source IP Address	Start Source port	Start Destination IP Address	Start Destination port	Ingress	Egress	mode	Modify	Delete
There is no data, please add one first.										

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable	Enable/Disable the IP filter function.
Protocol	Specify a protocol (including ANY, TCP, UDP, TCP AND UDP and ICMP. Where, ANY refers to any protocol).
Name	IP filter name. The length is 1 to 256 characters.
Start Source IP Address	The start source (LAN side) IP address.
End Source IP Address	The end source (LAN side) IP address.
Start Destination IP Address	The start destination IP address
End Destination IP Address	The end destination IP address
Start Source port	Start source (LAN side) address port number
End Source port	End source (LAN side) address port number
Start Destination port	Start destination (LAN side) address port number
End Destination port	End destination (LAN side) address port number
Ingress	The available options are LAN, established WAN connections or leave blank. It is blank by default, which refers to any mode.
Egress	The available options are LAN, established WAN connections or leave blank. It is blank by default, which refers to any mode.
mode	Select a filtering mode: Discard and Permit.

Parameter	Description
Modify	Click  to modify the corresponding IP filter rule.
Delete	Click  to delete the corresponding IP filter rule.

- Click **Add** to submit the current configuration.
- End of Steps –

## 7.3 Configuring MAC Filter

### Context



**Note:**

In the **Permit** mode, please type the local MAC address, otherwise the network cannot be accessed.

### Steps

- Select **Security > MAC Filter** from the menu bar to open the **MAC Filter** page as shown below.





If you choose the Permit mode, please add the MAC address of your PC first, otherwise web access is not allowed.

Enable   
 Mode   
 Type   
 Protocol   
 Source MAC Address   
 Destination MAC Address

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable	Enable/Disable the MAC filter function.
Mode	Select the filtering mode: Discard and Permit.
Type	Select the type: Bridge, Route, Bridge+Route.
Protocol	Select a protocol: IP, ARP, RARP, PPPoE and ALL.



Parameter	Description
Source MAC Address	The device MAC address on the LAN side
Destination MAC Address	The device MAC address on the WAN side
Modify	Click  to modify the corresponding MAC filter rule.
Delete	Click  to delete the corresponding MAC filter rule.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 7.4 Viewing a Service List

### Steps

- Select **Security > Service List** from the menu bar to open the **Service List** page as shown below.

List of Services and Ports

Service Name	Port	Enable
FTP	21	0
TELNET	23	1
HTTP	80	1
HTTPS	443	1

List of Service Connection

Service Name	Client IP Address	AP device IP Address
HTTP	12.10.10.27	12.10.10.6

- You can view the detailed information of service ports and service connections on this page.

– End of Steps –

## 7.5 Configuring the ALG Switch

### Prerequisite

The access point mode of the device is **fat**.

### Steps

- Select **Security > ALG** from the menu bar to open the **ALG** page as shown below.

Enable ALG

- FTP ALG
- TFTP ALG
- SIP ALG
- L2TP ALG
- H323 ALG
- RTSP ALG
- PPTP ALG
- IPSEC ALG

2. Select the corresponding ALG switches to be enabled as required.
3. Click **Submit** to submit the current configuration.

– End of Steps –

# Chapter 8

## Application Configuration

---

### Table of Contents

Configuring UPnP .....	8-1
Setting a Device Name .....	8-2
QoS Configuration .....	8-3
Configuring SNTP .....	8-7
IGMP Configuration .....	8-8
Configuring MLD Listening .....	8-9
LED Control .....	8-9

## 8.1 Configuring UPnP

### Prerequisite

The access point mode of the device is **fat**.

### Context

The Universal Plug and Play (UPnP) function supports zero-configuration connection. This function helps to discover various networking devices automatically.

The devices supporting UPnP can access the network dynamically, obtaining IP addresses and sending its performance information. If there are DHCP and DNS servers, the device can obtain the DHCP and DNS services automatically.

The device supporting UPnP function can exit the network automatically without affecting the device itself or other devices in the network.

### Steps

1. Select **Application > UPnP** from the menu bar to open the **UPnP** page as shown below.

Enable

WAN Connection

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable	Enable/Disable the UPnP function. It is disabled by default.
WAN Connection	Select the corresponding WAN connection as required.
Advertisement Period (in minutes)	Set the corresponding time as required. Unit: minute.
Advertisement Time To Live (in hops)	Set the corresponding time to live (hop count) as required, for example 4.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 8.2 Setting a Device Name

### Prerequisite

The access point mode of the device is **fat**.

### Steps

- Domain name setting
  - Select **Application > DNS Service > Domain Name** from the menu bar to open the **Domain Name** page as shown below.

Domain Name

- In **Domain Name**, type the corresponding domain name, such as **ZTE**.
  - Click **Submit** to submit the current configuration.
- Host name setting
    - Select **Application > DNS Service > Hosts** from the menu bar to open the **Hosts** page as shown below.

Host Name   
 IP Address



The items with disabled buttons are allocated from a DHCP server, which couldn't be operated.

Host Name	IP Address	Modify	Delete
There is no data, please add one first.			

- Fill the corresponding host name and the IP address corresponding to this host in the **Host Name** and **IP Address** text box.
- Click **Add** to submit the current configuration.

**Note:**

The items with the dimmed button are allocated from a DHCP server, which are inoperable.

- Click  to edit the corresponding host information.
- Click  to delete the corresponding host information.

– End of Steps –

## 8.3 QoS Configuration

Quality of Service (QoS) defines the quality agreement on the information transmission and sharing between network users. For example, the allowed transmission delay time, the degree of distortion, and the synchronization of audio and video, etc.

The concept of Class of Service is introduced to QoS frame. By using QoS, ZXV10 W812N V2 can completely control the incoming and outgoing data packets of this device. For the incoming data packet, it is required to convert its field mapping (for example ToS, priority and so on) to queue. For the outgoing data packet, it is required to convert its queue to field mapping.

### 8.3.1 Configuring QoS Basic Parameters

#### Steps

1. Select **Application > QoS > Basic** from the menu bar to open the **Basic** page as shown below.

Enable QoS

Total Upstream Bandwidth  bps

Enable Queue Management

Scheduler Algorithm

Enable DSCP Re-marking

Enable 802.1p Re-marking

2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable QoS	Enable/Disable the QoS function.
Total Upstream Bandwidth	Set the total upstream bandwidth.

Parameter	Description
Enable Queue Management	Enable/Disable the function of congestion management. It is disabled by default.
Scheduler Algorithm	The available algorithms are SP, DWRR and SP_DWRR. SP: Send the group in a queue with higher priority in descending order of priorities. When the queue with higher priority is empty, the device will send the group in a queue with lower priority. DWRR: the priority cycle by weighting. Each queue is served by turn.
Enable DSCP Re-marking	Enable/Disable DSCP re-marking. It is disabled by default.
Enable 802.1p Re-marking	Enable/Disable 802.1p processing priorities re-marking. It is disabled by default.

3. Click **Submit** to submit the current configuration.

– End of Steps –



### 8.3.2 Configuring a Classification Rule

#### Steps

1. Select **Application > QoS > Classification** from the menu bar to open the **Classification** page as shown below.

Enable  
 DevIn   
 L2Protocol   
 L3Protocol   
 Source MAC Address  :  :  :  :  :   
 802.1p  (0 ~ 7)  
 Destination Port MIN:  MAX:  (0 ~ 65535)  
 DSCP  (0 ~ 63)  
 Proprietary configuration for IPv4  
 Source IP Address MIN:  MAX:   
 Destination IP Address MIN:  MAX:   
 TOS  (0 ~ 255)  
 IP Precedence  (0 ~ 7)  
 Proprietary configuration for IPv6  
 Source IPv6 Address MIN:  MAX:   
 Destination IPv6 Address MIN:  MAX:   
 Traffic Class  (0 ~ 255)  
 Flow Label  (0 ~ 1048575)  
 802.1p Re-marking  (0 ~ 7)  
 DSCP Re-marking  (0 ~ 63)  
 Queue Index  1

## 2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable	Enable/Disable the function of QoS classification configuration.
DevIn	The entrance of packets. Select a LAN interface or the SSID having been configured. You can only select one interface at a time.
L2Protocol	Select the layer-2 protocol for packets including IPV4, IPV6, ARP and PPPoE.
L3Protocol	Select the layer-3 protocol for packets including TCP, UDP and ICMP.
Source MAC Address	Source MAC address of packets
802.1p	The flag value of VLAN packets used for setting user priority that ranges between 0 and 7 (0 means that the priority is not set). The greater the value, the higher the priority is.
Destination Port MIN/MAX	Type the destination port number (minimum value and maximum value) of packets. The value range is 0 to 65535.
DSCP	Type the DSCP value of packets. The value range is 0 to 63.
802.1p Re-marking	The re-marking value of 802.1p processing priority. The value range is 0 to 7 (0 means that the priority is not set). The greater the value, the higher the priority is.
DSCP Re-marking	Type the re-marking value of DSCP. The value range is 0 to 63.
Queue Index	Select the corresponding management queue number that ranges from 1 to 8.
Modify	Click  to modify the corresponding rule.
Delete	Click  to delete the corresponding rule.
Proprietary configuration for IPv4	
Source IP Address MIN/MAX	Fill in the minimum value and maximum value of packet source IP address.
Destination IP Address MIN/MAX	Fill in the minimum value and maximum value of packet destination IP address.
TOS	Type the service type field of data packets. It ranges from 0 to 255.
IP Precedence	IP priority that ranges from 0 to 7 (0 indicates priority unavailable). The greater the value, the higher the priority is.
Proprietary configuration for IPv6	
Source IPv6 Address MIN/MAX	Fill in the minimum value and maximum value of packet source IPv6 address.

Parameter	Description
Destination IPv6 Address MIN/MAX	Fill in the minimum value and maximum value of packet destination IPv6 address.
Traffic Class	Traffic type ranging from 0 to 255.
Flow Label	Set the flow flag ranging from 0 to 1048575.

- Click **Add** to submit the current configuration.

– End of Steps –


### 8.3.3 Configuring Congestion Management

#### Context







The default congestion management algorithm is SP. The default queue is Queue 8. It is enabled by default.

#### Steps

- Select **Application > QoS > Queue Management** from the menu bar to open the **Queue Management** page as shown below.


 Current Scheduler Algorithm is SP.  
Queue 8 is the default queue which is enabled by default.

Enable   
Queue Index

Queue Index	Enable	Modify
1		
2		
3		
4		
5		
6		
7		
8		

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable	Enable/Disable the configuration function of QoS queues.
Queue Index	Include Queue 1- Queue 8. The Queue 8 is enabled by default.

- Click  to modify the queue number required to be modified. In **Enable**, select whether to enable this queue.



- Click **Modify** to submit the current configuration.

– End of Steps –

## 8.4 Configuring SNTP

### Context

Configure the related information of SNTP on the device to realize the time synchronization with the time server.

### Steps

- Select **Application > SNTP** from the menu bar to open the **SNTP** page as shown below.

Current Date and Time 2012-11-08T23:59:52

Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, I ▼

Primary NTP Server Address 12.10.10.56

Secondary NTP Server Address 12.10.10.56

Poll Interval 600 sec

Enable Daylight Saving Time

DSCP (0 ~ 63)

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Current Date and Time	Display the current date and time of the device.
Time Zone	Select the time zone where the device locates as required.
Primary NTP Server Address	Fill in the address or domain name of the primary NTP server.
Secondary NTP Server Address	Fill in the address or domain name of the secondary NTP server.
Poll Interval	The interval of server time synchronization. It is 86400s by default.
Enable Daylight Saving Time	Enable/Disable the daylight saving time function. It is disabled by default.
DSCP	Configure the DSCP value ranging from 0 to 63.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 8.5 IGMP Configuration

The multicast function supports sending the same data to several devices.

The IP host uses an Internet Group Management Protocol (IGMP) to report the qualifications of multicast group members to the neighboring router by sending data. At the same time, the multicast router uses the IGMP to find which hosts belong to the same multicast group.

The device supports processing IGMP packets through the IGMP proxy. When the IGMP proxy is enabled, the LAN host can request to join in or leave the multicast group. The multicast router can send multicast packets to the multicast group at the WAN side and serve as the proxy.

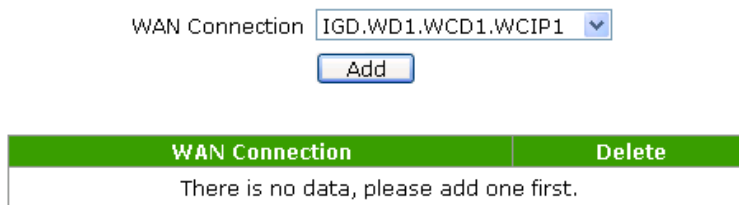
### 8.5.1 Setting IGMP Proxy

#### Prerequisite

The access point mode of the device is **fat**.

#### Steps

1. Select **Application > IGMP > IGMP Proxy** from the menu bar to open the **IGMP Proxy** page as shown below.



2. Configure the parameters according to the parameter description in the table below.

Parameter	Description
WAN Connection	There are two types for WAN connection, including IGD.WD1.WCD1.WCIP1, and WANBRIDGE1

3. Click **Add**.

– End of Steps –

### 8.5.2 Configuring IGMP Snooping

#### Steps

1. Select **Application > IGMP > IGMP Snooping** from the menu bar to open the **IGMP Snooping** page as shown below.

Enable IGMP Proxy   
 Enable IGMP Snooping   
 Enable IGMP Snooping Enhancement

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable IGMP Proxy	Enable/Disable the IGMP function.
Enable IGMP Snooping	Enable/Disable the IGMP listening function.
Enable IGMP Snooping Enhancement	Enable/Disable IGMP Snooping Enhancement function.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 8.6 Configuring MLD Listening

### Steps

- Select **Application > MLD Snooping** from the menu bar to open the **MLD Snooping** page as shown below.

Enable MLD Snooping   
 Enable MLD Snooping Enhancement

- Configure the parameters according to the parameter description in the table below.

Parameter	Description
Enable MLD Snooping	Enable/Disable the MLD ( Multicast Listener Discovery) Snooping function.
Enable MLD Snooping Enhancement	Enable/Disable the MLD Snooping Enhancement function.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 8.7 LED Control

### Steps

- Select **Application > LED Control** from the menu bar to open the **LED Control** page.
- Check whether **Enable LED** or not.

3. Click **Submit** to submit the current configuration.
- End of Steps –

# Chapter 9

## Management Configuration

### Table of Contents

Managing SNMPv1/v2c.....	9-1
SNMPv3 Security Management (USM).....	9-2
SNMPv3 Access Control Management (VACM).....	9-3
User Management.....	9-6
Device Management .....	9-8
Configuring Log Management .....	9-10
Access Point Management.....	9-11
Diagnosis and Maintenance .....	9-12

## 9.1 Managing SNMPv1/v2c

### Steps

1. Select **Administration > SNMPv1/v2c** . The following page is displayed.

Enable SNMP

Trap Server IP

Trap Server2 IP

Trap Server Port  (1 ~ 65535)

Read Community

Write Community

2. Configure the parameters. Refer to the following table.

Parameter	Description
Enable SNMP	Enable/Disable the SNMP function.
Trap Server IP	Specify the IP address of the alarm server, for example 192.168.1.1.
Trap Server2 IP	Specify the IP address of the standby alarm server.
Trap Server Port	Specify the port of the alarm server, ranging from 1 to 65535.
Read Community	The default read permission password is public.
Write Community	The default write permission password is private.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 9.2 SNMPv3 Security Management (USM)

### 9.2.1 Managing SNMPv3 Users

#### Steps

- Select **Administration > SNMPv3 Security (USM) > SNMPv3 Users**. The following page is displayed.

Security Name

Authentication Protocol

Authentication Password

Privacy Protocol

Privacy Password

Security Name	Authentication Protocol	Privacy Protocol	Modify	Delete
nanpuser				
anpuser	MD5			
apuser	MD5	DES		

- Configure the parameters. Refer to the following table.

Parameter	Description
Security name	User name
Authentication Protocol	Support none, MD5, and SHA
Authentication Password	Authentication password
Privacy Protocol	Support none and DES
Privacy Password	Encryption password
Modify	Click  to modify the corresponding SNMPv3 user information
Delete	Click  to delete the corresponding SNMPv3 user information

- Click **Add**.

– End of Steps –

## 9.2.2 Managing SNMPv1/v2c Users

### Steps

1. Select **Administration > SNMPv3 Security(USM) > SNMPv1/v2c Users**. The following page is displayed.

Security Name

Source IP

Security Name	Source IP	Modify	Delete
public	0.0.0.0		

2. Configure the parameters. Refer to the following table.

Parameter	Description
Security Name	User Name
Source IP	IP address of the source
Modify	Click  to modify the corresponding SNMPv1/v2c user information
Delete	Click  to delete the corresponding SNMPv1/v2c user information

3. Click **Add**.

– End of Steps –

## 9.3 SNMPv3 Access Control Management (VACM)

### 9.3.1 Managing Context

#### Steps

1. Select **Administration > SNMPv3 Access Control (VACM) > Context**. The following page is displayed.

Context  (Default: "")


2. Enter the context information. The default is "".
3. Click **Submit**.


– End of Steps –

## 9.3.2 Managing Security Groups







### Steps

1. Select **Administration > SNMPv3 Access Control (VACM) > Security To Group**. The following page is displayed.



Security Model  

Security Name  

Group Name

Security Model	Security Name	Group Name	Modify	Delete
USM	nanpuser	readgroup		
USM	anpuser	writgroup		
USM	apuser	writgroup		

2. Configure the parameters. Refer to the following table.

Parameter	Description
Security Model	Support USM, SNMPv1, and SNMPv2c.
Security Name	Specify the security user name.
Group Name	Specify the group name.
Modify	Click  to modify the corresponding security group information.
Delete	Click  to delete the corresponding security group information.

3. Click **Add**.

– End of Steps –

## 9.3.3 Managing View Subtree

### Steps

1. Select **Administration > SNMPv3 Access Control (VACM) > View Tree Family**. The following page is displayed.



View Name



SubTree

Mask  (Optional)

Type  ▼

View Name	SubTree	Mask	Type	Modify	Delete
all	.1		included		

- Configure the parameters. Refer to the following table.

Parameter	Description
View Name	View name.
Subtree	Subtree name.
Mask	(Optional) Subnet mask.
Type	The options are included and excluded.
Modify	Click  to modify the corresponding view information.
Delete	Click  to delete the corresponding view information.

- Click **Add**.

– End of Steps –

## 9.3.4 Managing Access Table

### Steps

- Select **Administration > SNMPv3 Access Control (VACM) > Access Table**. The following page is displayed.

Group Name

Context Prefix

Security Model

Security Level

Context Match

Read View Name

Write View Name

Notify View Name

Group Name	Context Prefix	Authentication Protocol	Security Level	Modify	Delete
Context Match	Read View Name	Write View Name	Notify View Name		
readgroup	""	USM	noAuthNoPriv		
exact	all	none	none		
writegroup	""	USM	authNoPriv		
exact	all	all	all		

2. Configure the parameters. Refer to the following table.

Parameter	Description
Group Name	Group name.
Context Prefix	Information of the context prefix.
Security Model	Support USM, SNMPv1, SNMPv2c, and any.
Security Level	Support noAuthNoPriv, autoNoPriv, and authPriv.
Context Match	Support exact and prefix.
Read View Name	Support none and all.
Write View Name	Support none and all.
Notify View Name	Support none and all.
Modify	Click  to modify the corresponding access table information.
Delete	Click  to delete the corresponding access table information.

3. Click **Add**.

– End of Steps –

## 9.4 User Management

### 9.4.1 Managing Users

#### Steps

1. Select **Administration > User Management > User Management**. The following page is displayed.

User Privilege:  Administrator  
 User

Username

Old Password

New Password

Confirmed Password

- Configure the parameters. Refer to the following table.

Parameter	Description
User Privilege	Determine whether to modify the management maintenance account or common account.
Username	The management maintenance account is admin and it cannot be modified. The common account is user and it can be modified.
Old Password	To modify the password of the management maintenance account, enter the original login password.
New Password	New password of the corresponding user.
Confirm Password	To make a confirmation, enter the new password of the corresponding user again.

- Click **Submit** to submit the current configuration.

– End of Steps –

## 9.4.2 Setting Automatic Logout

### Steps

- Select **Administration > User Management > Auto Logout Management**. The following page is displayed.

Timeout  (5 ~ 60 min)

- Set the timeout period within the range of 5 to 60 minutes. The default is 5 minutes.
- Click **Submit** to submit the current configuration.

– End of Steps –

## 9.5 Device Management

### 9.5.1 Setting System Management

#### Steps

1. Select **Administration > System Management > System Management**. The following page is displayed.



Click this button to warm reboot the device.

Reboot



Click this button to restore the configuration to factory default settings. The device will reboot after operating.

Restore Default

2. The user can restart the device and restore default settings.
  - Click **Reboot** to restart the device.
  - Click **Restore Default** to restore the factory settings.

– End of Steps –

### 9.5.2 Setting Version Upgrade

#### Context



#### Note:

Please wait when the software of the device is being upgraded, and pay attention to the prompt in the page. To prevent damage to the device, do not switch off the power or restart the device.

#### Steps

1. Select **Administration > System Management > Software Upgrade**. The following page is displayed.



The device will reboot after upgrading.

Please select a new software/firmware image

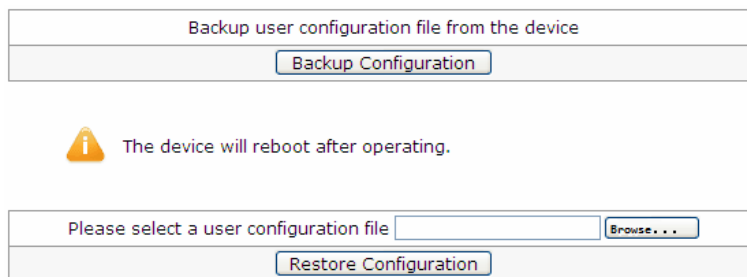
2. Click **Browse** to select the desired software version file.
3. Click **Upgrade** to upgrade the software version.

– End of Steps –

## 9.5.3 Managing User Configuration


### Steps

1. Select **Administration > System Management > User Configuration Management**. The following page is displayed.



Backup user configuration file from the device

Backup Configuration

 The device will reboot after operating.

Please select a user configuration file  Browse...

Restore Configuration

2. Choose backup operation or configuration import based on the actual requirement.
  - Export a configuration file
  - Click **Backup Configuration** to back up the current configuration file of the device.
  - Import a configuration file
    - i. Click **Browse** and select the configuration file to be imported.
    - ii. Click **Restore Configuration**. Then, the specified configuration file is imported.



#### Note:

The device automatically restarts after this operation is completed.

– End of Steps –


## 9.5.4 Managing the Default Configuration

### Steps

1. Select **Administration > System Management > Default Configuration Management**. The following page is displayed.

---

Backup default configuration file from the device
<input type="button" value="Backup Configuration"/>

 The device will reboot after operating.

Please select a default configuration file <input type="text"/> <input type="button" value="Browse . . ."/>
<input type="button" value="Restore Configuration"/>

2. Choose backup operation or configuration import based on the actual requirement.
  - Export the default configuration file  
Click **Backup Configuration** to back up the current configuration file of the device.
  - Import the default configuration file
    - i. Click **Browse** and select the default configuration file to be imported.
    - ii. Click **Restore Configuration**. Then, the specified default configuration file is imported.



**Note:**

The device automatically restarts after this operation is completed.

---

– End of Steps –

## 9.6 Configuring Log Management

### Steps

1. Select **Administration > Log Management**. The following page is displayed.

Enable Save Log  
 Log Level   
 Enable Remote Log  
 Log Server Address

```

Manufacturer:ZTE;
ProductClass:ZXV10 W812N V2;
SerialNumber:ZTENW35B6C00002;
IP:12.10.10.6;
HWVer:V3.0;
SWVer:V2.0;

P0000-00-00T00:00:16 Critical log! Lan Up!PHY_SPEC_STATUS
register value bc50
P0000-00-00T00:00:25 Critical log! Tunnel Setup Success!Tunnel
Device Create Success
2012-11-08T13:47:08Z Critical log! Tunnel Config Change!Tunnel
Time Configuration Change TUNNEL_KERNEL Success
2012-11-08T13:47:08Z Critical log! Tunnel Config Change!Tunnel
    
```

Download log file from the device

2. Configure the parameters according to the descriptions in the table below.

Parameter	Description
Enable Save Log	Enable/Disable the function of log server management. It is disabled by default.
Log Level	Log levels are Debug, Informational, Notice, Warning, Error, Critical, Alert, and Emergency in the ascending priority order. After a log level is selected, only logs of the selected level and with higher levels will be recorded.
Enable Remote Log	Enable/Disable the function of the log server remote login. It is disabled by default.
Log Server Address	Specify the IP address of remote log server.

3. Click **Submit**. Then, the logs of the corresponding level are displayed on the page.
- Click **Refresh** to view the latest log records.
  - Click **Clear Log** to clear the current log records.
  - Click **Download Log** to save the log information to a local file.

– End of Steps –

## 9.7 Access Point Management

### 9.7.1 Setting an AP Mode

#### Steps

1. Select **Administration > AP Management > AP Mode**. The following page is displayed.



The device will be automatically rebooted after the AP Mode is changed.

AP Mode

2. Set AP mode, Fat or Fit, based on the actual requirement. The default AP mode is **Fit**.



**Note:**

After the AP mode is switched, the device restarts automatically.

3. Click **Submit**.

– End of Steps –

## 9.7.2 Setting an Access Point Name

### Steps

1. Select **Administration > AP Management > AP Name**. The following page is displayed.

AP Name

2. In **AP Name** field, set the corresponding name as required.
3. Click **Submit** to submit the current configuration.

– End of Steps –

## 9.8 Diagnosis and Maintenance

### 9.8.1 Performing Ping Diagnosis

#### Steps

1. Select **Administration > Diagnosis > Ping Diagnosis**. The following page is displayed.



IP Address or Host Name

Ping num

Ping packet size  (1~4096)

Egress

- Configure the parameters. Refer to the following table.

Parameter	Description
IP Address or Host Name	The host IP address or host name
Ping num	Specify the ping number
Ping packet size	Specify the size of the ping packet. The range is from 1 to 4096
Egress	Select the egress to be diagnosed

- Click **Submit**. The PING result is displayed in the text box in the lower part.

– End of Steps –

## 9.8.2 Configuring Trace Route Diagnosis

### Steps

- Select **Administration>Diagnosis>Trace Route Diagnosis**. The following page is displayed.

IP Address or Host Name

WAN Connection

Maximum Hops  (2 ~ 64)

Wait Time  (2 ~ 10 sec)

2. Configure the parameters. Refer to the following table.

Parameter	Description
IP Address or Host Name	The host IP address or host name.
WAN Connection	Select the WAN connection to be diagnosed.
Maximum Hops	Select the maximum number of hops to be diagnosed.
Wait Time	Select the time-out period.

3. Click **Submit**. The Trace Route result is displayed in the text box in the lower part.

– End of Steps –

# Appendix A

## Troubleshooting

The solutions for the common problems during the installation and operation of the ZXV10 W812N V2 are provided in this section. For any unresolved problems, contact the service provider for help.

Problem	Solution
How to know the MAC address of the device?	<p>A MAC address is the unique identifier of a network device. This problem can be resolved in the following two ways:</p> <ul style="list-style-type: none"> <li>● Check the MAC address of this device on the little label at the bottom of each device.</li> <li>● Log in to the WEB management page of the device to view <b>Basic information of the device</b> so as to know the MAC address of the wireless access point.</li> </ul>
The STA cannot connect to an AP.	<p>Usually, the connection between an STA and an AP is established through the following steps such as finding an available AP, authenticating and connection. Therefore, if an STA cannot connect to an AP, the probable reasons are as follows:</p> <ul style="list-style-type: none"> <li>● The channel supported by an STA is different from that of an AP. If the AP uses the channel that the STA cannot support, the STA cannot find the AP. In this case, change the channel of the AP.</li> <li>● The authentication and encryption mode used by the STA are different from that of the AP. If their authentication and encryption modes are inconsistent, the STA cannot pass the authentication, which prevents the connection from being established.</li> <li>● The interference from the same device. Check whether there is a wireless device around the device. If there is a wireless device, switch off the device and then check whether the problem has been solved. Shield the device generating interference or change its location.</li> <li>● The interference from other devices. Check whether there are other interference sources around this device, for example microwaves and other 2.4 GHz high-power devices. These devices will affect normal working of the device. Try to switch off other devices if possible to check whether the problem has been solved.</li> <li>● There is the compatibility problem between an STA and an AP. The STA may not comply with the 802.11 protocol specification. As a result, the STA cannot connect with an AP.</li> </ul>

Problem	Solution
<p>Why the bandwidth is not high after the wireless network connection is established?</p>	<p>The bandwidth of a device is not high due to environment interference in most cases. However, sometimes, an ageing device may be causing the low transmission power. You can try the following methods to solve this problem:</p> <ul style="list-style-type: none"> <li>● Wireless channels. You can try to select other channels to check whether the rate can be improved dramatically.</li> <li>● Wireless interference. Check whether there is a wireless device around the device. If there is a wireless device, switch off the device and then check whether the problem has been solved. Shield the device generating interference or change its location.</li> <li>● View the signal strength. Check the signal strength between an STA and an AP. If the signal strength is quite low, the antenna may not to be connected reliably, or the output power is quite low due to the ageing problem.</li> <li>● Check an NIC. The power of the NIC may be quite low. Position the NIC close to an AP to test its bandwidth.</li> </ul>
<p>Why the connection cannot be established after the bridge configuration between the two devices has been completed?</p>	<p>Check the parameter configuration of the two devices:</p> <ul style="list-style-type: none"> <li>● Whether <b>Working Mode</b> is <b>Bridge</b>.</li> <li>● Whether the MAC address of the added remote end is correct.</li> <li>● Whether the configuration of <b>Country/Region</b> is the same.</li> <li>● Whether the configuration of <b>Channel /Frequency</b> is the same.</li> <li>● Whether the configuration of <b>Encryption Mode</b> is the same.</li> </ul>
<p>The system works normally after the wireless network is constructed. However, after a period, the problem in which links are not stable occurs, for example delay time increases and packet loss occurs.</p>	<p>Probably because the wireless environment in which the device works is influenced, the problem above occurs. Check whether the problem has been solved through the following steps:</p> <ul style="list-style-type: none"> <li>● Check whether the connection between various parts of a device is reliable (for example the connection of network cables and antenna connection).</li> <li>● Power off the device and then restart it.</li> <li>● Restore the device configuration to be the default value and then re-configure the device.</li> <li>● Check whether there is any virus intrusion in the wired and wireless device of an AP.</li> </ul>
<p>For the two devices whose bridging has been established, why the WEB page of the remote device cannot be opened if the remote device is configured through the wireless link on the near-end.</p>	<p>The WEB Server of the remote device responds quite slowly because the device is configured through WLAN. Wait for three minutes or restart the remote device to solve this problem. We recommend that configure the device through the connection of network cables.</p>

# Appendix B

## Technical Specifications

---

### Physical Specifications

- Size (Length × Width × Height): 7.075 inch (180 mm) × 6.486 inch (165 mm) × 1.789 inch (45.5 mm)
- Weight (excluding the power adapter): 1.764 lbs (800 g)

### Electric Standards

- Power adapter: Input 100 VAC to 240 VAC 50/60Hz; output 12 VDC/1500 mA
- POE power supply

### Power Consumption

Power consumption of the equipment is less than 12.5 W.

### Environment Requirement

- Working temperature: 14°F (−10°C) to 131°F (55°C)
- Working humidity: 5 % to 95 %

### IP Protection Classe

- IP protection class: IP31

### Passed Certifications

- CE
- CCCi
- Wi-Fi
- Wireless Transmission Equipment Type Approval

ZTE CORPORATION reserves the right to modify technical parameters in this manual without prior notice.

This page intentionally left blank.

# Appendix C

## Computer WLAN Configuration

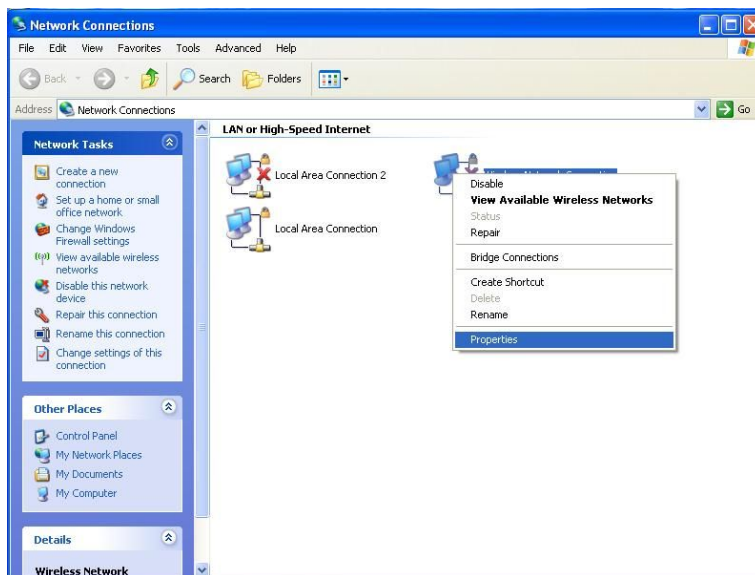
---

### Context

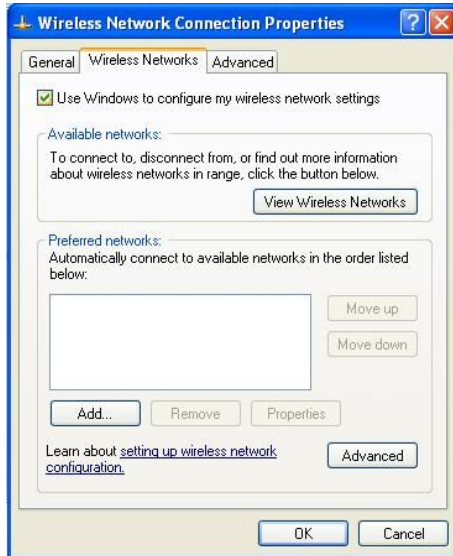
To access WLAN (Wi-Fi) from the user's computer, it is required to configure WLAN settings of the computer. The following example assumes that a laptop computer with a built-in network interface card (NIC) is used and the operating system is Windows XP.

### Steps

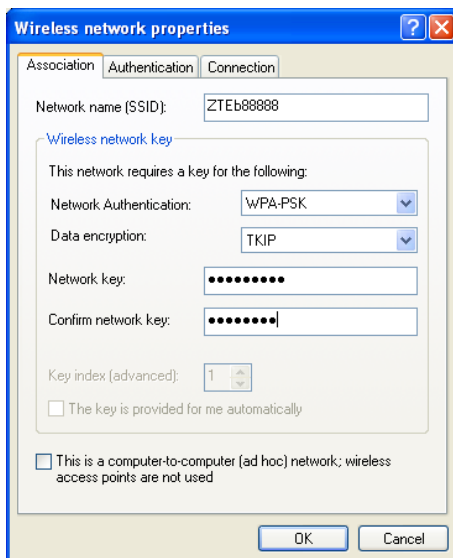
1. In Windows taskbar, select **Start > Control Panel**.
2. Double-click **Network Connection** and right-click **Wireless Network Connection**. Then click **Properties**, as shown in the following figure.



3. On the **Wireless Network Connection Properties** page, click the **General** tab. Set the IP address and the **DNS** server address of the NIC on the computer or obtain an IP address and a DNS server address by the DHCP mode from a terminal.
4. On the **Wireless Network Connection Properties** page, click the **Wireless Networks** tab. Select **Use Windows to configure my wireless network settings** and check whether the desired WLAN SSID is included in the Preferred networks area, as shown below.

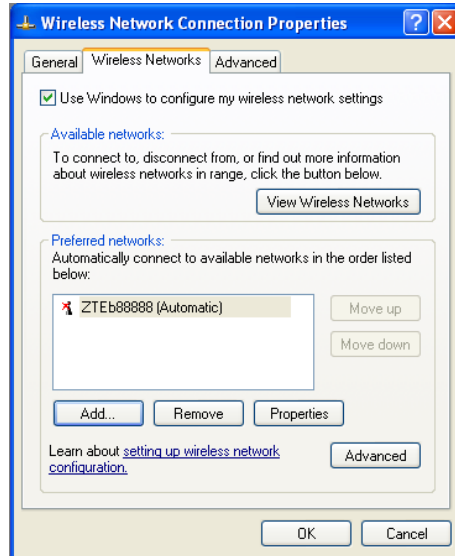


If there is no desired SSID, click the **Add** button. Then the **Association** page appears.

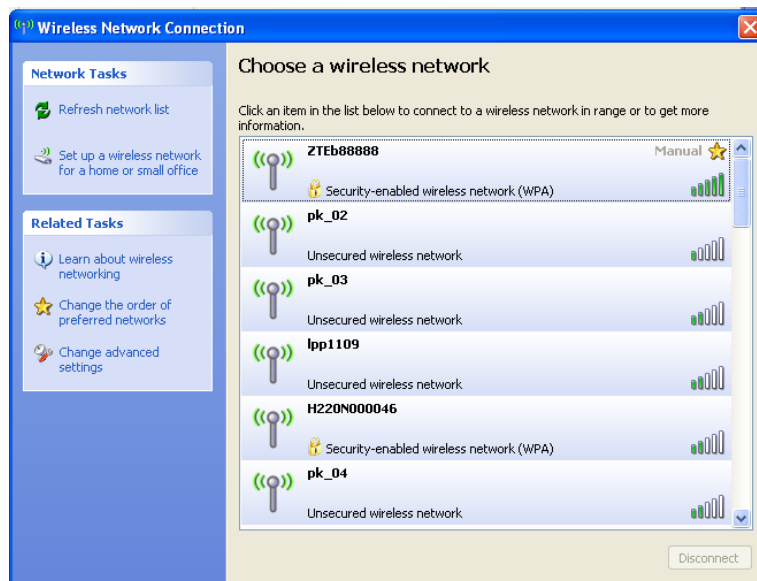


- On the **Association** page, type an SSID (it should be the same as the one set in the terminal and is case sensitive) in the network name text box. Supposing that the terminal adopts WPA-PSK for Network Authentication and 12345678 for the Data encryption, perform the following procedure in the computer: **Network Authentication** is selected as **WPA-PSK** while **Data encryption** is selected as **TKIP**. Clear **The key is provided for me automatically**. In the **Network key** field, type 12345678 (the same as the encryption key set on the terminal). Click **OK** to return to the following page.

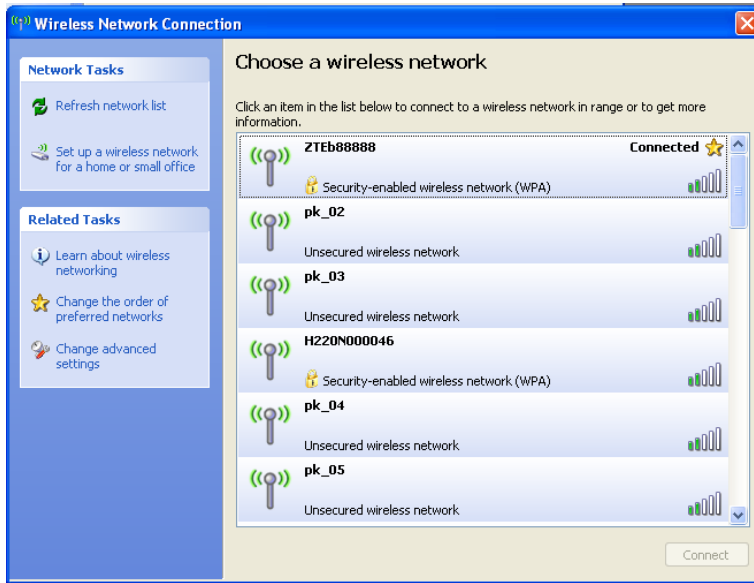




6. Click **View Wireless Networks** to view the wireless network list in the figure above. Check the wireless network list to see if the newly added wireless network connection exists. If not, click **Refresh network list** on the left pane of the page. If the wireless network is found, select it and then click **Connect**, as shown below.



7. Type the encryption key again and click **Connect**.
8. After the wireless network is connected successfully, the following page appears.



– End of Steps –

# Appendix D

## CE and FCC Compliance Statement

ZXV10 W812N V2 is compliant with the requirements of [CE](#) and [FCC](#).

### CE Compliance Statement

Country	CE Compliance Statement
Bulgarian Български	С настоящето, ZTE corporation декларира, че това безжично устройство е в съответствие със съществените изисквания и другите приложими разпоредби на Директива 1999/5/EC.
Czech Česky	ZTE corporation tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish Dansk	Undertegnede ZTE corporation erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Dutch Nederlands	Hierbij verklaart ZTE corporation dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze ZTE corporation dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, ZTE corporation declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian Eesti	Käesolevaga kinnitab ZTE corporation seadme Radio LAN device vastavust direktiivi 1999/ 5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish Suomi	Valmistaja ZTE corporation vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French Français	Par la présente ZTE corporation déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Country	CE Compliance Statement
German Deutsch	Hiermit erklärt ZTE corporation dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW) Hiermit erklärt ZTE corporation die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek Ελληνική	με την παρούσα ZTE corporation δηλώνει ότι radio LAN device συμμορφώνεται προς τις ουσιώδεις απαιτήσεις και τις λοιπές ζητητικές διατάξεις της οδηγίας 1999/5/ΕΚ.
Hungarian Magyar	Alulírott, ZTE corporation nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Italian Italiano	Con la presente ZTE corporation dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian Latviski	Ar šo deklarē ZTE corporation ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo ZTE corporation deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Maltese Malti	Hawnhekk, ZTE corporation jiddikjara li dan Radio LAN device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Polish Polski	Niniejszym ZTE corporation oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	ZTE corporation declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Romanian Romană	declară că acest dispozitiv fără fir respectă cerințele esențiale și alte dispoziții relevante ale Directivei 1999/5/EC.
Slovak Slovensky	týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	izjavlja, da je ta radio LAN device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Spanish Español	Por medio de la presente ZTE corporation declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Swedish Svenska	Härmed intygar ZTE corporation att denna Radio LAN device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Country	CE Compliance Statement
Turkish Turk	ZTE corporation bu kablosuz cihazın temel gereksinimleri ve 1999/5/EC yonergesindeki ilgili koşulları karşıladığını beyan eder.

### FCC Compliance 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.

### FCC Radiation Exposure Compliance Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This equipment 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.



**Caution!**

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.

This page intentionally left blank.

# Glossary

---

**CE**

- CONFORMITE EUROPEENDE

**DHCP**

- Dynamic Host Configuration Protocol

**DNS**

- Domain Name Server

**FCC**

- Federal Communication Commission

**IP**

- Internet Protocol

**LAN**

- Local Area Network

**MAC**

- Medium Access Control

**NAT**

- Network Address Translation

**OFDM**

- Orthogonal Frequency Division Multiplexing

**PoE**

- Power over Ethernet

**WAN**

- Wide Area Network

**WLAN**

- Wireless Local Area Network