ZXV10 W615 Outdoor Wireless Access Point User Manual

Verson: V3.0

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

LEGAL INFORMATION

Copyright © 2010 ZTE CORPORATION.

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without the prior written permission of ZTE Corporation.

The manual is published by ZTE Corporation. We reserve the right to make modifications on print errors or update specifications without prior notice.

Version No. : RVerson: V3.0 Edition Time : 2012-08-20(R1.0) Manual No. : SJ-20120820095015-001

<u>Chapter</u> 1

Product Introduction

Product Overview

The ZTE ZXV10 W615 broadband wireless access product operates at 2.4 GHz, 5.2 GHz and 5.8 GHz frequency bands and complies with IEEE 802.11a, 802.11b, 802.11g, and 802.11n protocols. The device adopts the Orthogonal Frequency Division Multiplexing (OFDM) technology. Featuring a transmission speed of up to 300 Mbps, high receiving sensitivity, and long transmission distance, it provides a powerful wireless access solution for telecommunication operators, Internet Service Provider (ISP) and other enterprises.

By supporting multiple encryption mechanisms and authority management functions, the ZXV10 W615 provides a highly secure system for Wireless Local Area Network (WLAN).

By supporting Power over Ethernet (PoE), ZXV10 W615 acquires convenient power supply.

Typical Application

The device is typically used in the following scenarios:

• Small and medium-sized enterprises

To realize wireless coverage and meet mobile office requirements.

• Remote access to the company network.

To receive and send E-mails, transmit files, emulate terminals, and others. The device supports various wireless network connection modes, such as point-to-point connection, single access point connection, multiple access point connection, and roaming. It can apply to various application environments, such as connection within an Intranet and between different networks.

• An environment where it is difficult to establish a connection through network cables

To be used in places where cabling is difficult, such as an old building and



an asbestos building structure.

Mobile office system

To be used by retailers, manufacturers and in the working site which needs to be changed frequently.

• Temporary LAN establishment for a special project

To be used when a LAN needs to be established temporarily in places such as commercial exhibitions, exhibition halls and construction sites; when the capacity needs to be expanded during peak hours in places such as retailing shops, airports and airlines; or when the financial auditor needs to establish a client work group.

• Access to the database by mobile workers

To enable doctors, nurses and retailers to share information through mobile access to the database.

Family office users

To meet the requirement for installing a small computer network easily and quickly.

Interface and Button Description

For a description of the interfaces and buttons of the ZXV10 W615, refer to the following table:

Name	Description
Ethernet	LAN interface/PoE (supports 10/100/1000 Mbps), connected by an RJ-45 network cable.
2.4G-A	2.4G antenna interface, used to connect an antenna.
2.4G-B	2.4G antenna interface, used to connect an antenna.
5G-A	5G antenna interface, used to connect an antenna.
5G-B	5G antenna interface, used to connect an antenna.
WAN/PoE	RJ-45 interface, used for uplink connection and supplying power.
GND	Grounding terminal.

Technical Specifications

Physical Specification

- Size: 210 mm×210 mm×69 mm (Length × Width × Height)
- Weight: 4 kg

Electric Parameters

• Power supply: 802.3at PoE+

- Voltage: -48 VDC
- Maximum power consumption: 18 W

Environment Requirement

- Working temperature: -40 $^{\circ}$ C to 65 $^{\circ}$ C
- Working humidity: 5 % RH to 100 % RH

IP Protection Class

IP protection class: IP66

Passed Certifications

CCCi、Wi-Fi、RoHS

ZTE Corporation reserves the right to modify technical parameters with this manual without notice.

Antenna Requirement

Antenna Type: N-type Dipole Antenna

Frequency (MHz)	Gain(dBi)
2400	1.0
2410	1.2
2420	1.1
2430	1.2
2440	0.9
2450	1.0
2460	1.1
2470	1.0
2480	1.2
2490	1.4
2500	1.1
5220	2.98
5765	3.43

<u>Chapter</u> 2

Configuration Preparation

Login

The ZXV10 W615 supports configuration based on Web pages. You can configure and manage the ZXV10 W615 through a Web browser.

Open the Internet Explorer, type http://192.168.0.228 on the address bar, and then press **Enter**. The login dialog box is displayed, see the following figure.

Please login to c	ontinue	⇔中文
Username		
Password		Login

Enter a valid user name and a password, and then click **Login**. The Web configuration page of the ZXV10 W615 device is displayed.

NOTE Notes:

The initial user name and password of a common user are both user. This user has only the authority to view the related Status information of this device. The initial user name and password of the administrator are both admin. This user has the authority to configure and manage the device through the Web browser.

For the factory defaults of ZXV10 W615, refer to the following table:

Item	Default Value
IP Address/Mask of Ethernet interface	IP address: 192.168.0.228 Subnet mask: 255.255.255.0
User name/Password	Initial user name/password for common user: user/user Initial user name/password for administrator: admin/admin



Item	Default Value
AP mode	Fit AP
AP name	APxxxxxxxxxx, where xxxxxxxxx means the Medium Access Control (MAC) address of the device
AC discovery mode	Dynamic Host Configuration Protocol (DHCP), applicable for fit AP only.
WAN mode	DHCP
Wireless mode	 Network card 1: Mixed (802.11b+802.11g) Network card 2: Mixed (802.11a+802.11n)
SSID	SSID1 is enabled.

Introduction to the GUI for Software Setup

After log in, the software interface is displayed as *Figure 1*.

Figure 1 Software Interface

ZTE中兴					Z)	<v10 th="" w<=""><th>615 V3</th></v10>	615 V3
ф ф х	1 Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management System Management Log Management Diagnosis WAN Type 2 2 _{Help}		E Tra Trap Read Write	nable SNMP ap Server IP o Server2 IP Server Port Community Community	 ✓ 10.62.32.211 162 public private 	(1 ~ 65535)	3	
	7					Submit	Cancel
1. Main menu 2. Submenu 3. Parameter	Copyrig	ht © 2012 Z1	E Corporatio	on. All ríghts re	served.		

Select items on the main menu for software setup.

Select sub-items to set parameters on the left submenu.



NOTE Notes:

- Click Logout at the upper-right corner of the current Web page. Then, the system log outs and returns to the Login page.
- Click Help at the bottom of the navigation pane 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.
- Click • * at the top of the current web page to change the language to chinese.



Device Status

Checking Device Information

This section describes how to check the device information.

Steps

Select **Status > Device Information** to open the **Device Information** page. Device information is displayed on the **Device Information** page as *Figure* 2.

Figure 2 Device Information

Model	ZXV10 W615 V3
Serial Number	ZTENW36C1108090
batch number	07dchS300102cd
Hardware Version	V3.0
Software Version	V2.0
Boot Loader Version	V2.0
AP Name	AP384608D63944

NOTE Notes:

This page includes the information of model, serial no, batch number, hardware version, software version, boot loader version and AP name.

-END OF STEPS-



Checking Information of Network Interfaces

Checking Ethernet Interface Information

This section describes how to check Ethernet interface information.

Steps

Select **Status > Network Interface > Ethernet**, the following page with Ethernet interface information is displayed.

Ethernet Port	WAN	
MAC Address	38:46:08:d6:39:44	
Status	Up	
Mode	1000M/FULL DUPLEX	
Packets Received/Bytes Received	2745/279586	
Packets Sent/Bytes Sent	2447/1901869	
		Pofrod

Figure 3 Ethernet Interface Information

NOTE Notes:

- ► This page includes Ethernet port, MAC address, status, mode, packets received/bytes received, and packets sent/bytes sent information.
- ▶ You can click Refresh to view the latest Ethernet interface information.

-END OF STEPS-

Checking WAN Connection

This section describes how to check the network connection information.

Steps

Select **Status > Network Interface > WAN Connection**., the following page with the established connection information is displayed.



Figure 4 WAN Connection Information

NAT Disabled IP 90.90.90.40/255.255.255.0 DNS 0.0.0.0/0.0.0/0.0.00 Gateway 90.90.90.1 Connection Status Connected	NAT Disabled IP 90.90.90.40/255.255.255 DNS 0.0.0.0/0.0.0/0.0.0 Gateway 90.90.90.1
IP 90.90.90.40/255.255.255.0 DNS 0.0.0.0/0.0.0/0.0.0 Gateway 90.90.90.1 Connection Status Connected	IP 90.90.90.40/255.255.255 DNS 0.0.0.0/0.0.0.0/0.0.0 Gateway 90.90.90.1
DNS 0.0.0.0/0.0.0/0.0.0 Gateway 90.90.90.1 Connection Status Connected	DNS 0.0.0/0.0.0/0.0.0 Gateway 90.90.90.1
Gateway 90.90.90.1 Connection Status Connected	Gateway 90.90.90.1
Connection Status Connected	
	Connection Status Connected
emaining Lease Time 498 sec	maining Lease Time 498 sec

Notes:

- ► This page includes DHCP, WAN MAC, NAT(Network Address Translation), IP, DNS (Domain Name Server), Gateway, Connection status, remaining lease time.
- ▶ You can click Refresh to view the latest WAN connection information.

-END OF STEPS-

Checking WLAN Interface Information

This section describes how to check the WLAN interface information.

Steps

Select **Status > User Interface > WLAN**, the following page is displayed. In the right pane, view the WLAN interface information.



Enable Wireless RF1	Enabled
Channel	11
WDS Mode	Disabled
SSID1 Enable	Enabled
SSID1 Name	W615V3-100d
Authoptication Tuno	Onen Custom

Figure 5 WLAN Interface Information

WDS Mode	Disabled
SSID1 Enable	Enabled
SSID1 Name	W615V3-100d
Authentication Type	Open System
Encryption Type	None
MAC Address	38:46:08:d6:39:44
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	359/80965
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	174

NOTE Notes:

- ► This page includes the wireless switch state, the channel, the WDS mode (if the WDS is enabled, the MAC address of the WDS interface, the MAC address of the relay/the root AP and the connection state is displayed) and the SSID enabled state.
- ▶ You can click Refresh below the drop-down scroll bar (It isn't displayed in the above figure for the limitation on the figure size) to view the latest device information.

-END OF STEPS-



Network Configuration

Broadband Connection Configuration

Configuring a Broadband Connection (Fit AP)

The ZXV10 W615 has two operational modes: fat AP and fit AP. The default operational mode is fit AP.

Context

For instructions on how to change the AP mode for the ZXV10 W615, refer to "Setting the AP Mode".

NOTE Notes:

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

Steps

1. Select Network > WAN > WAN Connection. The following page is displayed.



ф Ф X	Status	Network	Security	Application	Administration	Help	Logout
-WAN WAN Connection WLAN LAN Partice	٨	The devi page is s	ce will be aut submitted.	omatically reb	ooted after the s	ettings in th	is
Kouling			IP Version	Pv4	v		
? Help		AC Disco	ivery Mode [OHCP	V		
• Hold			AC Type 🛛	Adapter	v		
			AC Name				
	Ena	ble CAPWAP	Encryption [
			WAN Type [)HCP	V		
		Enabl	e Verify AC 🛛	7			
		Er	nable VLAN 🛛				
			VLAN ID				
			802.1p 🛛) 7			
		Er	iable DSCP				
			DSCP				
			MTU 1	448			
	/					Submit	Cancel

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

Parameter	Description
IP Version	Supported protocol versions include Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), and IPv4/v6. The default setting is IPv4.
AC Discovery Mode	Includes DHCP, Static, DNS, and Broadcast. The default setting is DHCP.
АС Туре	Set AC Type. When AC Type is set to Adapter , the AP selects the uplink AC automatically.
AC Name	This parameter is configurable when AC Discovery Mode is DHCP or DNS .
Enable CAPWAP Encryption	Enables or disables CAPWAP encryption.
WAN Type	When IP Version is IPv4 , the supported modes are DHCP, Static, and PPPoE. When IP version is IPv6 or IPv4/v6 , the supported modes are DHCP and PPPoE. The default mode is DHCP. When AC Discovery Mode is DHCP , the WAN mode is set to DHCP.

Parameter	Description
Enable Verify AC	Enables or disables the AC verification function when WAN Type is DHCP .
Enable VLAN	Enables or disables the VLAN configuration function. Virtual Local Area Network (VLAN) Identification/Identity/Identifier (ID) and 802.1p are used to set the VLAN and priority for the selected device.
VLAN ID	Indicates the VLAN ID of packets through the WAN interface. The value range is 0-4094.
802.1p	Specifies the processing priority. It only applies to multiple WAN connections. The range is 0-7 and the default value is 0, which means no priority. A greater value indicates a higher priority.
Enable DSCP	Enables or disables the Differential Services Code Point (DSCP) function for data flow.
DSCP	Specifies the DSCP value. The value range is 0-63.
MTU	Specifies the Maximum Transmission Unit (MTU) value. The default value is 1448.

3. Click Submit.

NOTE Notes:

The configuration on this page takes effect after the device is restarted.

-END OF STEPS-

Configuring a Broadband Connection (Fat AP)

This section describes how to configure a broadband connection for fat AP.

Steps

The AP mode of the device is **Fat**.

1. Select Network > WAN > WAN Connection. The following page is displayed.



¢ФÌ	Status	Network	Security	Application	Administration	Help	Logout
-WAN WAN Connection WLAN LAN	٨	The devi page is s	ce will be aut submitted.	omatically reb	ooted after the s	ettings in th	is
Routing ? Helo		Wo	IP Version I king Mode E WAN Type C	Pv4 Iridae IHCP	V V V		
			VLAN ID 802.1p	<u>v</u>			
		Er	DSCP	400			
						Submit	Cancel

- 2. Configure the parameters. For details, refer to "Configuring a Broadband Connection (Fit AP)".
 - Working Mode: supports Bridge mode and Route mode. The default is Bridge mode.
 - WAN Type: When **IP Version** is **IPv4**, the supported modes are DHCP, Static, and PPPoE. When **IP version** is **IPv6** or **IPv4/v6**, the supported modes are DHCP and PPPoE. The default mode is DHCP.
- 3. Click Submit.

```
NOTE Notes:
```

The configuration on this page takes effect after the device is restarted.

-END OF STEPS-

WLAN Configuration

Setting Basic Information

This section describes how to set WLAN information for the ZXV10 W615.

Context

Two network cards are available. You can set the cards respectively.

¹⁴ Confidential and Proprietary Information of ZTE CORPORATION

ZTE中兴

- Network card 1: works at 2.4 GHz, and supports 802.11b, 802.11g, and 802.11n.
- Network card 2: works at 5.8 GHz, and supports 802.11a and 802.11n.

Steps

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

-WLAN	A If AP allow s association	ns from the IEEE 802.11n mode STAs, please
•Basic	make sure SSID securit	y without TKIP or WEP Encryption Algorithm
SSID Settings	The device will be auto	matically rebooted after the settings of "Low er
Security	Density Enable" from se	elected to unselected in this page is submitted.
Rate Limit		
Access Control List	Network Card	Network Card1 🗸
Associated Devices	Enable Wireless RF	
AP Scanning	Fachle Teclesian	
SSID Real-time scanning	Enable Isoladon	
spectrum scan	Mode	Mixed(802.11b+802.11q+802.11n) ∨
WMM	Country/Region	United States of America 🗸
Channel Auto-Switch	Band	2.4G
Wireless Mode	Band Width	20MHz V
Mesh Configuration	MINO	a*a ¥
Mesh topology query	MIND	2.2.*
Ferria Service	11N Rate	Auto 🗸
Auto Changel Swtich	Downstream Rate(Check All 🗌)	1 2 5.5 11 ⊻ 6 ⊻ 9 ⊻ 12 ⊻ 18
LAN	_	24 236 248 254
Routing	Downstream MCS(Check All 🗹)	V 0 V 1 V 2 V 3 V 4 V 5 V 6 V 7
Advanced WLAN		
	Upstream Rate(Check All ∟)	1 2 5.5 11 №6 №9 №12 №18
(9 Help		
	Upstream MCS(Check All 🗹)	
	đ	
	Channel	Auto
	Total Maximum Clients	128 (1 -: 512)
	FGT Enable	(1~ 312)
	Beacon Interval	100 (20 ~ 1000) ms
	Power Type	mafia by percent
	Transmitting Power	
	OpS Type	WMM Y
	RTS Threshold	2347
	DTIM Interval	1
	W IDS Mode	Access V
	WIDS Scan Period	120
	W IDS Scan Mode	Current Channel 💙

2. Confiture the basic parameters of WLAN.

If **Network Card 1** is selected, see the previous figure for the configuration page. For a description of the parameters, refer to the following table.

Parameter	Description
Network Card	Select network card 1.
Enable Wireless RF	Enables or disables the wireless RF function
Enable Isolation	Enables or disables the SSID isolation function.
Mode	Supports IEEE 802.11b Only, IEEE 802.11g Only, IEEE 802.11n Only, Mixed(802.11b+802.11g), Mixed(802.11g+802.11n), and Mixed(802.11b+802.11g+802.11n).



Parameter	Description		
Country/Region	United States of America.		
Band	2.4 G		
Band Width	The options are 20 MHz, 40 MHz, and automatic.		
MIMO	The options are 1*1, 1*2, 2*1, and 2*2.		
11N Rate	Specifies the transmission rate of 802.11n. 17 rates are available and the default is Auto.		
Transmit Rate	Supports various kinds of transmitting rates including1 Mbps、 2 Mbps、 5.5 Mbps、 11 Mbps、 6 Mbps、 9 Mbps、 12 Mbps、 18 Mbps、 24 Mbps、 36 Mbps、 48 Mbpsand 54 Mbps		
Channel	Proper channel can be selected according to country code. It can be selected as Auto or any value in the range of 1-11. The default is Auto. The channel used to accomplish communication between AP and wireless station is determined by local policy. All wireless stations which communicate with the ZXV10 W615 must use the same channel.		
Only Select Channel 1/6/11	Determines whether to select channel 1/6/11 or select all channels.		
Total Maximum Clients	Specifies the maximum number of connected users. The range is 1-512.		
SGI Enable	Enables or disables the SGI function.		
A-MPDU Enable	Enables or disables the A-MPDU function.		
Beacon Interval	Specifies the beacon interval.		
Power Type	Supports configuration by percent, configuration based on actual power value (unit: dBm), and configuration based on actual power value (unit: mW)		
Transmitting Power	Supports automatic, 100%, 90%, 80%, 70%, 60%, 50%, 40%, 30%, 20%, 12.5%, and 10%. The default is 100%. The power class refers to the percentage of output power to maximum power. A higher power indicates a farther transmission distance.		
QoS Type	The options are disabled, WMM, and SSID.		
RTS Threshold	Specifies the upper limit of transmission request.		
DTIM Interval	Specifies the DTIM time patch.		
WIDS Mode	The options are Access, Monitor, and Mixed.		
WIDS Scan Period	Specifies the value of WIDS scan interval.		
WIDS Scan Mode	The options are Current Channel and All Channel.		
Protection Mode	The options are None, CTS Only, and RTS/CTS.		
Application Scenarios	Support three kinds of application scenarios: low density, high density, user configuration.		
5G Access First	Enables or disables 5G access in precedence.		

ZTE中兴

Parameter	Description
TxBF Enable	Enables or disables beam forming technology.

If **Network card 2** is selected, see the figure below for the configuration page. For a description of the parameters, refer to the following table.

-WLAN •Basic SSID Settings Security Rate Limit	If AP allows association make sure SSID securit mode configured. The device will be auto Density Enable" from se	is from the IEEE 802.11n mode STAs, please y without TKIP or WEP Encryption Algorithm matically rebooted after the settings of "Low er elected to unselected in this page is submitted.
Access Control List	Network Card	Network Card2
Associated Devices	Enable Wireless RF	
AP Scanning	Eachle Tealation	
SSID Real-time scanning	Enable Isolation	
spectrum scan	Mode	Mbked(802.11a+802.11n)
WMM Channel Auto Switch	Country/Region	United States of America 🗸
Wiseless Mede	Band	5G
Mark Configuration	Band Width	20MHz V
Mesh topology query	MIMO	2*2
Mesh topology list	11N Pate	Auto
ServAc		
Auto Channel Swtich	Downstream Rate(Check AI 🖭)	
LAN	Downstream MCS(Check All ⊻)	
Routing Advanced WI AN	Libertree Rote (Charle All [4])	
	upstream Rate(Check AI 🗹)	
0	Upstream MCS(Check All ⊻)	
Help	Channel	
	Total Maximum Clients	128 (1 ~ 512)
	SGI Enable	
	A-MPDU Enable	3
	A-MSDU Enable	
	Beacon Interval	100 (20 ~ 1000) ms
	Power Type	config by percent V
	Transmitting Power	100%
	QoS Type	WMM 🗸
	RTS Threshold	2347
	DTIM Interval	1
	W IDS Mode	Access 🗸
	W IDS Scan Period	120
	W IDS Scan Mode	Current Channel 🗸
	Protection Mode	None
	TxBF Enable	

Parameter	Description
Network Card	Select network card 2.
Enable Wireless RF	Enables or disables the WLAN RF function.
Enable Isolation	Enables or disables the SSID isolation function.
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	United States of America.
Band	5G
Band Width	The options are 20 MHz, 40 MHz, and automatic.

Confidential and Proprietary Information of ZTE CORPORATION 17



Parameter	Description
MIMO	The options are 1×1 , 1×2 , 2×1 , and 2×2 .
11N Rate	Specifies the transmission rate of 802.11n, supporting seven rate types.
Channel	Proper channel can be selected according to country code. It can be selected as Auto, 149, 153, 157, 161, or 165. The default is Auto. The channel used to accomplish communication between AP and wireless station is determined by local policy. All wireless stations which communicate with the ZXV10 W615 must use the same channel.
Total Maximum Clients	Specifies the maximum number of connected users. The range is 1-512.
SGI Enable	Enables or disables the SGI function.
A-MPDU Enable	Enables or disables the A-MPDU function.
Beacon Interval	Specifies the beacon interval.
Power Type	Supports configuration by percent, configuration based on actual power value (unit: dBm), and configuration based on actual power value (unit: mW)
Transmitting Power	Supports automatic, 100%, 90%, 80%, 70%, 60%, 50%, 40%, 30%, 20%, 12.5%, and 10%. The default is 100%. The power class refers to the percentage of output power to maximum power. A higher power indicates a farther transmission distance.
QoS Type	The options are Disabled, WMM, and SSID.
RTS Threshold	Specifies the upper limit of transmission request.
DTIM Interval	Specifies the DTIM time patch.
WIDS Mode	The options are Access, Monitor, and Mixed. The default is Access.
WIDS Scan Period	Specifies the value of WIDS scan interval.
WIDS Scan Mode	The options are Current Channel and All Channel.
Protection Mode	The options are None, CTS Only, and RTS/CTS.
Application Scenarios	Support three kinds of application scenarios: Low density, High density, User configuration.
5G Access First	Enables or disables 5 G access in precedence.
TxBF Enable	Enables or disables beam forming technology.

3. Click Submit.

-END OF STEPS-

Setting SSID

This section describes how to set SSID.

ZTE中兴

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

¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout	
WAN								
-WLAN								
Basic		-1	T		_			
SSID Settings		Ch	oose SSID	SSID1	•			
Security		Net	work Card	letwork Card1	V			
Rate Limit			Hide SSID 🖡	1				
Access Control List		Fi	nable SSID - [
Associated Devices		E-able con	n teeletien I					
AP Scanning		Enable SSID Isolation						
WDS		Isolation Mode ALL						
WMM		Maximum Clients 32 (1 ~ 512)						
Channel Auto-Switch		SSID Name SSID1 (1 ~ 32 characters)						
Wireless Mode		Dulaiha						
LAN								
Routing		VLAN ID 0						
			802.1p)	V			
() Help		As Manage	ment SSID 🖡					
		-						
						Submit	Cancel	

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

Parameter	Description
Choose SSID	Specifies the SSID to be configured. The range is from SSID1 to SSID32.
Network Card	Displays the wireless network card of the current SSID. SSID1–SSID16 correspond to network card 1. SSID17–SSID32 correspond to network card 2.
Hide SSID	Determines whether to hide this SSID.
Enable SSID	Enables or disables this SSID.
Enable SSID Isolation	Enables or disables the isolation within this SSID.
Isolation Mode	Specifies an appropriate isolation mode from four modes, which are Unicast, Broadcast, Multicast, and ALL. The default setting is ALL.
Maximum Clients	Specifies the maximum number of clients allowed for this SSID. The value range is 1–512. The default is 32.
SSID Name	Specifies the name of this SSID. The number of characters is in a range of 1–32.



Parameter	Description
Priority	Specifies the SSID priority. The range is 0–7. The default value is 0, which means no priority. A greater value indicates a higher priority.
VLAN ID	VLAN tag of data packets. VLAN ID can be set in a range of 0-4094.
802.1p	Specifies the processing priority. The range is 0–7. The default value is 0, which means no priority. A greater value indicates a higher priority.
As Management SSID	Disabled by default. When this function is enabled, the user associated with the SSID can manage the device.

3. Click Submit.

-END OF STEPS-

Setting Security Information

This section describes how to set WLAN security information.

Steps

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

¢ 中 X	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN	A	With TK1	P or WEP End	ryption Algorit	hm configured. A	.P does not	
Basic	-	allow as	sociations fro	m the IEEE 80	2.11n mode STA	s.	
SSID Settings							
• Security			Choose SS	ID SSID1	V		
Rate Limit		Δut	nentication Tv			7	
Access Control List		Aut	rendeddorr ry	PS WEATON			
Associated Devices		V	VPA Passphra	se •••••••	• (8 ~ 63 chara	acters)	
AP Scanning	Er	nable WPA Gr	oup Key Upda	ite 🔽			
WDS	WF	A Group Kev	Update Inter	val 600	sec		
WMM		WDA F	united stands				
Channel Auto-Switch		WPA ENC	yption Algoriti	IM IKIP	T		
Wireless Mode							
LAN							
Routing							
2 Haln							
	J						
						Submit	Cancel

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



Parameter	Description
Choose SSID	Specifies the SSID to be configured. The range is SSID1-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	Specifies the WPA encryption key. The range is 8-63 characters.
Enable WPA Group Key Update	Enables or disables WPA group key updating function. It is enabled by default.
WPA Group Key Update Interval	Specifies the key updating interval. The default is 600 seconds.
WPA Encryption Algorithm	Supports TKIP, AES, and TKIP+AES.

Authentication Type is divided into non-encryption, WPA-PSK encryption, WPA-EAP encryption, WEP encryption, WAPI-PSK encryption and WAPI-CERT encryption.

▶ non-encryption

Authentication Type selects Open System, meaning non-encryption.

▶ WPA-PSK encryption

WPA encryption means Wi-Fi protected access. It has three modes: WPA-PSK, WPA2-PSK, and WPA/WPA2-PSK.

- i. In the Authentication Type drop-down 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 drop-down list, select WPA-EAP, WPA2-EAP, or WPA/WPA2-EAP to enable WPA-EAP encryption.





¢ Ф Ў	Status	Network	Security	Application	Administration	Help	Logout			
WAN										
-WI AN										
Basic		With TKI	IP or WEP End	ryption Algorit	hm configured, A	AP does not				
SSID Settings		dirow associations from the feet 602.11ft mode STAS.								
● Security			Change SS							
Rate Limit			CHOOSE 53	נטופפן טוי		_				
Access Control List		Aut	hentication Ty	pe WPA-EAP		•				
Associated Devices			Server Ty	pe Master Au	th Server	•				
AP Scanning		Se	erver IP Addre	ss 192.168.1	.1					
WDS			Server Pr	nrt 1812	(0 ~ 65535)					
WMM			bervern							
Channel Auto-Switch			Sec	ret ••••••	(1 ~ 64 char	acters)				
Wireless Mode			Reauth Peri	od 3600	sec					
LAN			Enable Preau	ith 🗌						
Routing	Er	nable WPA Gr	oup Kev Upda	te 🔽						
		N. Carrie Karr								
? Help	WH	A Group Key	update Inter		sec					
		WPA Encr	yption Algoritl	nm TKIP	V					
	7					Submit	Cancel			

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 1-64 characters.
Reauth Period	The default is 3600 seconds.
Enable Preauth	Enables or disables the pre-authentication function. The function is disabled by default.
Enable WPA Group Key Update	Enables or disables WPA group key updating 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. Three options



Parameter	Description
	are available: AES, TKIP, and TKIP+AES. The default is TKIP.

▶ WEP encryption

Wired Equivalent Privacy (WEP) is a commonly used WLAN security protocol.

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

¢ ₱ ኟ	Status	Network	Security	Application	Administration	Help	Logout
WAN •WLAN Basic SSID Settings	4	With TKI allow as	P or WEP End sociations fro	ryption Algorit m the IEEE 80	thm configured,)2.11n mode ST/	AP does not As.	
SSID Settings SSID Settings Rate Limit Access Control List Associated Devices AP Scanning WDS WMM Channel Auto-Switch Wireless Mode LAN Routing		Aut WEP I	Choose SS nentication Ty WEP Encryption Encryption Le WEP Key Inc WEP Ke WEP Ke WEP Ke	SID SSID1 pe Shared Ki on Enable vel 64bit lex 1 y1 ••••• y2 ••••• y3 •••••	ey	Y	
🖁 Helo	5	13 ASCII d ASCII chars c	hars or 26 he	xadecimal digi Encryption imal digits can Key.	ts can be entere Key. I be entered for	ed for 128-bi 64-bit WEP I	t WEP Encryption

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

Parameter	Description
WEP Encryption	Enables or disables WEP encryption function. The function is enabled by default.
WEP Encryption Level	There are two types of WEP key, namely 64bit and 128bit.
WEP Key Index	Specifies corresponding key value.



Parameter	Description
WEP Key 1–4	Specifies WEP encryption key value. 64-bit WEP key corresponds to five ASCII characters or ten hexadecimal characters. 128-bit WEP key corresponds to 13 ASCII characters or 26 hexadecimal characters.

► WAPI-PSK encryption

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

ф Ф X	Status	Network	Security	Application	Administration	Help	Logout
WAN -WLAN Basic SSID Settings	۵	With TKI allow as	P or WEP End sociations fro	ryption Algorit m the IEEE 80	thm configured, Al 12.11n mode STAs	P does not	
Security Rate Limit Access Control List Associated Devices AP Scanning WDS WMM Channel Auto-Switch Wireless Mode LAN Routing Help		Aut	Choose SS nentication Ty WAPI Key Mo WAPI K	ID SSID1 pe WAPI-PSP de ASCII ev •••••••	((8 ~ 64 chara] acters)	
	/					Submit	Cancel

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

Parameter	Description
WAPI Key Mode	Supports two modes: ASCII and HEX. The default is ASCII.
WAPI Key	Specifies WAPI key value. The range is 8-64 characters.

▶ WAPI-CERT encryption

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

ZTE中兴

¢ † X	Status	Network	Security	Application	Administration	Help	Logout
WAN -WLAN Basic SSID Settings	٨	With TKI allow as	P or WEP Enc sociations fro	ryption Algorit m the IEEE 80	thm configured, A 2.11n mode STA	IP does not s.	:
Security Rate Limit Access Control List Associated Devices AP Scanning WDS WMM Channel Auto-Switch Wireless Mode LAN Routing		Auth Cert Certific	Choose SS nentication Ty ificate Server cate Server Pi te Manageme	ID SSID1 Pe WAPI-CEI IP Ort O ent Certifica	▼ (0 ~ 65535) te Uploading		
	/					Submit	Cancel

- ii. Enter the certificate server IP address and certificate server port.
- iii. Click the **Certificate Uploading** button, select the proper type of certificate file in the displayed dialog box, and then click **Upload**.

NOTE Notes:

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

▶ WEP-EAP encryption

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



¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN	A	WEL TH					
Basic	-	allow as	P or WEP End sociations fro	nyption Algorit m the IEEE 80	nm configurea, A 12.11n mode STA	AP does not S.	
SSID Settings							
● Security			Choose SS	ID SSID1	•		
Rate Limit		Auth	ontication Tv			7	
Access Control List		Auu	ienucauon ry	PC WEP-EAP		-	
Associated Devices		Server Type Master Auth Server 💌					
AP Scanning	Server IP Address 192.168.1.1						
WDS		Server Port 1812 (0 ~ 65535)					
WMM			0		(* *****	t \	
Channel Auto-Switch			560	et ••••••	(1 ~ 64 char)	acters)	
Wireless Mode			Reauth Peri	od 3600	Sec		
LAN	Enable Preauth 🗍						
Routing							
? Help							
					_	Submit	Cancel
4	7						

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 1-64 characters.				
Reauth Period	The default is 3600 s.				
Enable Preauth	Enables or disables the pre-authentication function. The function is disabled by default.				
WEP Encryption	Enables or disables WEP encryption. It is disabled by default.				
WEP Encryption Level	Specifies the WEP key length. The options are 128bit and 64bit. The default is 128 bit.				

3. Click **Submit**.



-END OF STEPS-

Setting Rate Limit

This section describes how to set rate limit for WLAN services.

Steps

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

♀ 申 艾	Status	Network	Security	Application	Administration	Help	Logout		
WAN									
·WLAN	A	Control	Tuna awitah ti	less affact imr	nadistaly and th	a aattinaa ai	¢		
Basic	-	the old (Control Type 1	vill be lost.	es errect immediately and the settings of I be lost.				
SSID Settings		The item	's Rate Limit (iunction will no	ot take effect if it	s value is "O	".		
Security									
•Rate Limit			Control	Type SSID/ST	Δ				
Access Control List				.,					
Associated Devices									
AP Scanning			Choose	SSID SSID1	V				
WDS		SSID Downlin	k Rate Guara	ntee O	(0 ~ 25000	10 kbps)			
WMM		SSID D	ownlink Rate	Limit 0	(0 ~ 25000	10 khns)			
Channel Auto-Switch					(0 20000				
Wireless Mode		STA D	ownlink Rate	Limit U	(0 ~ 25000	IO KDPS)			
LAN		SSID Uplin	k Rate Guara	ntee O	(0 ~ 25000	10 kbps)			
Routing		SSIE) Uplink Rate	Limit 0	(0 ~ 25000	10 kbps)			
		ST/	Uplink Rate	Limit 0	(0 ~ 25000	10 kbps)			
😗 Help									
	/					Submit	Cancel		

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

Parameter	Description
Control Type	Supports SSID/STA and MAC.
Choose SSID	Specifies the SSID to be configured. The range is SSID1-SSID16.
SSID Downlink Rate Guarantee	The configuration range is 0-250000 kbps. The default is 0, which means no rate guarantee.
SSID Downlink Rate Limit	The configuration range is 0-250000 kbps. The default is 0, which means no rate limit.
STA Downlink Rate Limit	The configuration range is 0-250000 kbps. The default is 0, which means no rate limit.
SSID Uplink Rate Guarantee	The configuration range is 0-250000 kbps. The default is 0, which means no rate guarantee.



Parameter	Description
SSID Uplink Rate Limit	The configuration range is 0-250000 kbps. The default is 0, which means no rate limit.
STA Uplink Rate Limite	The configuration range is 0-250000 kbps. The default is 0, which means no rate limit.

3. Click Submit.

-END OF STEPS-

Setting Access Control List

The access control list is used to guarantee the device security in networks.

Steps

1. Select **Network > WLAN > Access Control List**. The following page is displayed.



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

Parameter	Description
Choose SSID	Specifies the SSID to be configured. The range is SSID1-SSID32.
Mode	The supported modes are:

28 Confidential and Proprietary Information of ZTE CORPORATION



Parameter	Description			
	 Disabled: no SSID access is controlled. It is the default setting. 			
	• Block: prohibits the access of devices with specified MAC addresses.			
	► Permit: permits the access of devices with specified MAC addresses.			
MAC Address	Specifies the MAC address of the equipment to be controlled.			
Delete	Click to delete the corresponding item of control channel.			

3. Click Add.

-END OF STEPS-

Checking Associated Devices

This section describes how to check the detailed information of the devices associated with the SSID.

Steps

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



ZXV10 W615 User Manual

⇔中文	Status	Network	Security	Applica	ition Administrat	ion Help	Logout
WAN							
-WLAN							
Basic							
SSID Settings		C	hoose SSID	SSID1	•		
Security	MA	C Address	Associating S	tatus	Packets Sent	QoS	
Rate Limit		SSID P	ower Saving	Status I	Packets Received	RSSI(dBm)	
Access Control List			The	re is no d	lata.		
Associated Devices							
AP Scanning							
WDS							
WMM							
Channel Auto-Switch							
Wireless Mode							
LAN							
Routing							
🕐 _{Heln}							
	/						Refresh

2. In the **Choose SSID** drop-down list, select the required SSID. View the detailed information of the associated device corresponding to the SSID. By default, the system displays the device information associated with SSID1.

NOTE Notes:

You can click Refresh to view the latest information.

-END OF STEPS-

Scanning an AP

This section describes how to scan an AP.

Steps

1. Select Network > WLAN > AP Scanning. The following page is displayed.

ZTE中兴

¢ 中 文	Status	Network	Security	Application	Administration	Help	Logout
WAN •WLAN	A	There do	oesn't exist er	nabled SSID, t	his page cannot	be configur	ed.
Basic SSID Settings			_			-	
Security		Ne	twork Card 🛛	letwork Card	1		
Rate Limit			Channel	Current Channe	v		
Access Control List	SS	SID Chan	nel Se	curity	Beacon Inte	rval	
Associated Devices	M	AC SNI	R RSS	il(dBm)	NSI(dBm)	
•AP Scanning			The	e is no data.			
WDS							
WMM							
Channel Auto-Switch							
Wireless Mode							
LAN							
Routing							
2 Help							
						_	
	/						Scan

2. In the **Network Card** and **Channel** drop-down lists, select the network card and channel to be scanned respectively.



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

3. Click **Scan**. The scan result is displayed on the refreshed page.

-END OF STEPS-

Setting WDS

This section describes how to set WDS.

Steps

1. Select Network > WLAN > WDS. The following page is displayed.



ZXV10 W615 User Manual

¢¢≵	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN							
Basic			_				
SSID Settings		Ne	twork Card 🛛	Network Card	1 🔻		
Security			WDS Mode	Disabled	•		
Rate Limit			L				
Access Control List							
Associated Devices							
AP Scanning							
●WDS							
WMM							
Channel Auto-Switch							
Wireless Mode							
LAN							
Routing							
? Help							
	/						

2. Select the network card. Configure the parameters based on the selected WDS mode.

If WDS Mode is set to Disabled, no parameter needs to be configured.

If **WDS Mode** is set to **WDS+Root**, the configuration page changes to:

ZTE中兴

¢ ₱ X	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN Basic							
SSID Settings			'ha channal a	nd cocurity co	ttings of the rea	aator must h	10
Solution Security		the sam	e as the root.	iu security se	tungs of the rep	caler must L	
Security							
Kate Limit							
Access Control List		Ne	twork Card	Network Card	1 💌		
Associated Devices			WDS Mode	WDS+Root	•		
AP Scanning							
● WDS		o 1-1 (14	VO Address of	0.00.00.00.0	0.00		
WMM	WD	S Interface M	AC Address U		0:00		
Channel Auto-Switch		Repeater M	AC Address	: : :			
Wireless Mode				Submit			
LAN							
Routing							
🕐 Heln							
- Ticib							
_							

Configure the parameters. Refer to the following table.

Parameter	Description
WDS Interface MAC Address	Displays the MAC address of the WDS interface.
Repeater MAC Address	Specifies the MAC address of the repeater.

If **WDS Mode** is set to **WDS+Repeater**, the configuration page changes to:

ZXV10 W615 User Manual



7TF击兴

Configure the parameters. Refer to the following table.

Parameter	Description
WDS Interface MAC Address	Displays the MAC address of the WDS interface.
Root MAC Address	Specifies the MAC address of the root AP.

3. Click Submit.

-END OF STEPS-

Setting STA WMM

This section describes how to set STA WMM.

Steps

1. Select **Network > WLAN > STA WMM**. The following page is displayed.
<u>ZTE中兴</u>

\$ ₱ X	Status	Network	Security	Applicatior	Administration	Help	Logout
WAN							
WLAN							
Basic							
SSID Settings		Net	twork Card [Network Card	1 💌		
Security			Choose AC	BE	•		
Rate Limit			AIFSN 3	}	(0 ~ 15)		
Access Control List			ECWMin		(0 ~ 15)		
Associated Devices					(0 - 15)		
AP Scanning			ECWMax ()	(0 ~ 15)		
WDS			TXOP ()	(0 ~ 255)		
STA WMM			Qlength 2	256	(0 ~ 1000)		
●AP WMM			SRL 7	,	(0 ~ 255)		
Channel Auto-Switch					(0 or 255)		
Wireless Mode			LIVE [(0 ** 200)		
Mesh Configuration							
LAN							
Routing							
2 usta							
• пец							

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

Parameter	Description
Network Card	Select the network card for which WMM is to be configured.
Choose AC	The available options are VO, VI, BE, and BK.
AIFSN	The available range is 0–15.
ECWMin	The available range is 0–15.
ECWMax	The available range is 0–15.
ТХОР	The available range is 0–255.
Qlength	The available range is 0–1000.
SRL	The available range is 0–255.



Parameter	Description
LRL	The available range is 0–255.

3. Click Submit.

-END OF STEPS-

Setting AP WMM

This section describes how to set AP WMM.

Steps

1. Select Network > WLAN > AP WMM. The following page is displayed.

LILYA	/				ZX	(V10 W6	615 V3
¢ 中 ≵	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN							
Basic							
SSID Settings		Ne	twork Card [Vetwork Card:	1 🔻		
Security			Choose AC	BE	•		
Rate Limit			AIFSN 3	(0 ~ 15)		
Access Control List	CUM			(0~15)		
Associated Devices	ECWMIN						
AP Scanning	ECWMax			(6(0 ~ 15)			
WDS	ТХОР			0 (0 ~ 255)			
STA WMM			Qlength 2	56 ((0 ~ 1000)		
●AP WMM			SRL 7	(0 ~ 255)		
Channel Auto-Switch					0 ~ 255)		
Wireless Mode					0 ~ 200)		
Mesh Configuration							
LAN							
Routing							
2							
• Негр	J						
						Submit	Cancel
			3	1123129	60		

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

Parameter	Description
-----------	-------------



Parameter	Description
Network Card	Select the network card for which WMM is to be configured.
Choose AC	The available options are VO, VI, BE, and BK.
AIFSN	The available range is 0–15.
ECWMin	The available range is 0–15.
ECWMax	The available range is 0–15.
ТХОР	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.

3. Click Submit.

-END OF STEPS-

Setting Automatic Channel Switching

This section describes how to set automatic channel switching.

Steps

1. Select **Network > WLAN > Channel Auto-Switch**. The following page is displayed.

ZXV10 W615 User Manual



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

Parameter	Description
Network Card	Select the network card for which automatic channel adjustment is to be configured.
Enable Channel Auto-Switch	Enables or disables the automatic frequency adjustment function.
Adjustment Type	Supports two types: Adjust On Startup and Adjust Periodically.
RSSI Threshold	Specifies the signal strength threshold. The value range is -90 dBm to 10 dBm. The default value is -30 dBm.
Cycle Period	Specifies the interval of channel adjustment. The value range is 1 to 1440 minutes. The default value is 30 minutes.
Duration	Specifies the duration of channel adjustment. The value range is 0 to 3600 seconds.

3. Click Submit.

-END OF STEPS-

Setting Wireless Mode

This section describes how to set wireless modes for the two network cards of



the ZXV10 W615.

Steps

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

¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout
WAN							
-WLAN Basic SSID Settings Security Rate Limit Access Control List Associated Devices AP Scanning WDS	The device will be automatically rebooted after the settings of Wireless Mode and Node Type in this page is submitted. Network Card Network Card Vetwork Card Ve						
Channel Auto-Switch							
●Wireless Mode LAN Routing ? Helo							
	/					Submit	Cancel

- 2. Select the network card to be configured. Select **Wireless Mode** to be **Only Coverage** or **Only Backhaul**.
- 3. Click Submit.

-END OF STEPS-

Setting the Network Configuration

This section describes how to configure the network.

Steps

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



Figure 6 Network Configuration

7TF由兴							\leq
	_				ZX	V10 W6	15 V3
ф Ф X	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN Basic SSID Settings Security Rate Limit Access Control List Associated Devices AP Scanning WDS STA WMM Channel Auto-Switch Wireless Mode Mesh Configuration LAN Routing	Enal	Network Die Wireless I Mesh Node	Card Networ Aesh h ID Type Normal	k Card1 💌 (1 Node 🔍	~ 32 characters)		
	7				_	Culumit	Cancel
	C	h @ 2012 77	T. Comora	All sinkles		SUDMIT	Cancel
	Copyrig	nt © 2012 ZT	E Corporation	i. All rights res	served.		

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

Parameter	Description
Network Card	Select the network card 1 or the network card 2 as mesh returning network card.
Enable Wireless Mesh	Enables or disables the mesh function.
Mesh ID	Set the mesh identity.
Mesh Node Type	Supports two types: normal node, gateway node. The default value is normal node.

3. Click **Submit**.

-END OF STEPS-

Addresses Management

Managing Addresses

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

Steps

1. Select Nework > LAN > Address Management. The following page is displayed.

\$\\$ ₱ 文	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN -LAN • Address Management DHCP Conditional Serving Pool IPv6 Address Management Routing Helb		NOTE: 1. should be LAN IP Add Subnet N Enable DHCP Se	The DHCP Sta in the same s ress 192.168 4ask 255.255 STP stp	IT IP Address subnet as the 1.1.1 1.255.0	and DHCP End II LAN IP.	P address	
	DHCF DHC DNS SA DNS SA DNS SA Alloc MAC	P Start IP Add P End IP Add erver1 IP Add erver2 IP Add erver3 IP Add Default Gate Lease ated Address Address IP	ress 192.168 ress	1.1.2 1.1.254 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.1 1.1.2 1.1.2 1.1.254	se Time Host Na	ame Port	
	/					Submit	Cancel

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

Parameter	Description
LAN IP Address	IP address of LAN group (interface subnet). The default IP address is 192.168.1.1.



Parameter	Description
Subnet Mask	Subnet mask of LAN group.
Enable STP	Enables or disables the STP function.
DHCP Service	 When the AP mode is Fit, the supported states are DHCP Server and OFF. The default state is DHCP Server. When the AP mode is Fat, the supported states are DHCP Server, DHCP Relay, and OFF. The default state is DHCP Server.
DHCP Start IP Address	The start IP address allocated by the DHCP Server. Before modifying the start or end IP address, ensure that this IP address is in the same network segment with that of ZXV10 W615.
DHCP End IP Address	The end IP address allocated by the DHCP Server. Before modifying the start or end IP address, ensure that this IP address is in the same network segment with that of ZXV10 W615.
DNS Server 1–3 IP Address	IP address of the DNS server. There are three available addresses.
Default Gateway	The value is 192.168.1.1 by default.
Lease Time	Lease time stands for the duration when an IP address can be leased from the IP pool by the client dynamically. The default value is 86400 seconds. 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.
Allocated Address	Refers to the allocated IP address. The page displays the allocated IP address and the basic information of devices that use the IP addresses.

3. Click Submit.

-END OF STEPS-

Setting DHCP Conditional Serving Pool

This section describes how to set the DHCP conditional serving pool in the fat AP mode.

Steps

1. Select Network > LAN > DHCP Conditional Serving Pool. The following page is displayed.

ZTE中兴

☆中文	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN -LAN Address Management	NOTE: DHCP Conditional Serving Pool's Start IP Address and End IP Address should be in the same subnet as the LAN IP.						
DHCP Conditional Serving Pool IPv6 Address Management Routing		Start IP Add End IP Add	ress				
💔 Helo	P	ort St	art IP Addres	s End	IP Address	Modify	
	S	SID1	0.0.0.0		0.0.0.0	2	
	SS	ID16	0.0.0.0		0.0.0.0	2	
	SS	ID17	0.0.0.0		0.0.0.0	2	
	/	, , , , , , , , , , , , , , , , , , ,		·			

Notes:

The DHCP Conditional Serving Pool page is unavailable in the fit AP mode..

- 2. Enter the start IP address and end IP address.
- 3. Click **Modify**.
- -END OF STEPS-

Managing an IPv6 Address

This section describes how to manage an IPv6 address.

Steps

1. Select **Network > LAN > IPv6 Address**. The following page is displayed.





¢ ₱ X	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN -LAN Address Management DHCP Conditional Serving Paol		LAN IP1	v6 Address fe	80::1			
IPv6 Address Management Routing Help							
	/					Submit	Cancel

- 2. On this page, re-configure the IPv6 address of this terminal.
- 3. Click Submit.
- -END OF STEPS-

Routing Management

Setting an IPv4 Static Route

This section describes how to set an IPv4 static route.

Steps

1. Select **Network > Routing > Static Routing (IPv4)**. The following page is displayed.

ZTE中兴

ZTE¢%				~	ZX	(V10 W6	15 V3
\$ 中 文	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN LAN •Routing •Static Routing(IPv4) Static Routing(IPv6) Dynamic Routing		WAN Conner Network Add Subnet I Gate	ction IGD.WD Iress Mask eway Add)1.WCD1.WCI	P1 v		
😗 Help	Network Address	Subnet Mask There is	Gateway s no data, ple	WAN Connection ase add one f	Status ModifyDele irst.	ete	
	/						
	Copyrig	ht © 2012 ZT	'E Corporation	n. All rights res	served.		

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

Parameter	Description
WAN Connection	Specifies the required interface.
Network Address	Refers to the address of the destination network.
Subnet Mask	Refers to the subnet mask of the destination network.
Gateway	Refers to the IP address of the gateway (next hop).
Modify	Click <i>C</i> to edit the corresponding static route rule.
Delete	Click ut to delete the corresponding static route rule.

3. Click Add.

-END OF STEPS-

Setting an IPv6 Static Route

This section describes how to configure an IPv6 static route.

Steps

1. Select **Network > Routing > Static Routing (IPv6)**. The following page is displayed.



ZXV10 W615 User Manual

ф Ф X	Status	Network	Security	Application	Administration	Help	Logout
WAN WLAN LAN -Routing Static Routing(IPv4) •Static Routing(IPv6)		WAN Conner P Gate	refix way Add	/ /			
Dynamic Routing	WAN Connectio	n Pi	refix	Gateway	StatusModifyDele	ete	
? Help		There is	no data, ple	ase add one	first.		

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

Parameter	Description
WAN Connection	Select the related interface as needed.
Prefix	Fill in the front blank with the IPv6 address. Fill in the back blank with the length of the subnetwork prefix.
Gateway	The Gateway IP address (Next hop)
Modify	Click <i>C</i> to edit the corresponding static route rule.
Delete	Click u to delete the corresponding static route rule.

-END OF STEPS-

Setting a Dynamic Route

This section describes how to set a dynamic route.

Steps

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

ZTE中兴

		INCLIMULK	Security	Application	Administration	Help	Logout
WAN WLAN LAN Routing Static Routing(IPv4) Static Routing(IPv6)		Enable Ver Authentica	RIP sion RIP v2 ation Simple	▼ Password ▼			
Dynamic Routing Help	j	uthentication	Key]	0.442	Caral

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

Parameter	Description
Enable RIP	Enables or disables RIP.
Version	Supports RIP v1, RIP v2, and RIP v1 Compatible.
Authentication	Supports No Authentication, Simple Password, and MD5 Authentication.
Authentication Key	Refers to the authentication key.

3. Click Submit.

-END OF STEPS-

<u>Chapter 5</u>

Security Configuration

Setting a Firewall

This section describes how to set a firewall.

Steps

1. Select **Security > Firewall**. The following page is displayed.



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

Parameter	Description
Enable Anti-Hacking Protection	Enables or disables the anti-hacking protection function.
Firewall Level	The firewall levels are as follows:



Parameter	Description
	 High: allows legal WAN side access, but prohibits PING from the WAN side.
	 Middle: allows legal WAN side access, but resists certain types of dangerous data flow traveling over Internet.
	► Low: allows legal WAN side access and PING from the WAN side.
	► Off: Not recommended to use this configuration. When the firewall is closed, the network is vulnerable to attacks and normal Internet access may be affected.

3. Click **Submit**.

-END OF STEPS-

Setting IP Filter (Fat AP)

This section describes how to filter the addresses in a certain range or used by a specified port.

Steps

The AP mode of the device is **Fat**.

1. Select **Security > IP Filter**. The following page is displayed.







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

Parameter	Description
Enable	Enables or disables the IP filter function.
Protocol	The available options are ANY, TCP, User Datagram Protocol (UDP), TCP AND UDP, and Internet Control Message Protocol (ICMP). ANY refers to any protocol.
Name	Refers to the IP filter name. The length is 1 to 256 characters.
Source IP Address	Start IP address of the source (LAN side).
End Source IP Address	End IP address of the source (LAN side).
Start Destination IP	Start IP address of the destination.



Parameter	Description
Address	
End Destination IP Address	End IP address of the destination.
Start source port	Port number of the start source (LAN side) address.
End source port	Port number of the end source (LAN side) address.
Start Destination port	Port number of the start destination source (LAN side) address.
End Destination port	Port number of the end destination source (LAN side) address.
Ingress	The availbable options are LAN, IGD.WD1.WCD1.WCIP1, or blank. It is blank by default, which refers to any mode.
Egress	The availbable options are LAN, IGD.WD1.WCD1.WCIP1 or blank. It is blank by default, which refers to any mode.
Mode	Select a filtering mode: Discard or Permit.
Modify	Click 🖉 to modify the corresponding IP filter rule.
Delete	Click to delete the corresponding IP filter rule.

3. Click Add.

-END OF STEPS-

Setting MAC Filter

This section describes how to filter the prohibited MAC addresses.

Steps

1. Select **Security > MAC Filter**. The following page is displayed.





¢¢≵	Status	Network	Security	Application	Administration	Help	Logout					
Firewall MAC Filter Service List	٨	If you choose the Permit mode, please add the MAC address of your PC first, otherwise web access is not allowed.										
😗 Help			Enable									
			Mode	Discard	V							
		Type Bridge										
			Protocol [IP .	V							
		Source M	AC Address	:[:[:	::::							
	[Destination M	AC Address	: : : : :	::::							
				Add								
	Type Protocol Source MAC Address Destination MAC Address Modify Delete											
	There is no data, please add one first.											
	7											
	/											

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

Parameter	Description
Enable	Enables or disables the MAC filter function. This function is disabled by default.
Mode	Select a filtering mode: Discard or Permit.
Туре	Specifies the type: Bridge, Route, or Bridge+Route.
Protocol	Specifies the protocol: IP, Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), PPPoE, or ALL.
Source MAC Address	MAC address of the device on the LAN side.
Destination MAC Address	MAC address of the device on the WAN side.
Modify	Click <i>C</i> to modify the corresponding MAC filter rule.
Delete	Click to delete the corresponding MAC filter rule.

ZTE中兴

Notes:

If the Permit mode is selected, the MAC address of the local computer must be entered to ensure network connection.

```
3. Click Add.
```

-END OF STEPS-

Checking the Service List

The service list shows the enabled service ports.

Steps

1. Select **Security > Service List**. The following page is displayed.

¢ † Ž	Status	Network	Security	Applicati	on Administration	Help	Logou		
Firewall MAC Filter	List	of Services a	nd Ports						
Service List	Servi	e Name	Por		Enable				
•	ŀ	TP	21		0				
V Help	TELNET		23		1				
	HTTP		80		1				
	HTTPS		443		1				
	List of Service Connection								
	Service Name Client IP Address AP device IP Address								
NOTE Notes:									

- In the lists of services and ports, Enable is O: indicates Stop;Enable is 1: indicates Start.
- Under normal condition, List of Service Connection recorded Client IP Address and AP device IP Address after log on HTTP.

2. Check the detailed information about the service ports and connections. —**END OF STEPS**—

Setting Service Control (Fat AP)

This section describes how to prevent specified IP addresses from accessing the network.



Steps

The AP mode of the device is **Fat**.

1. Select **Security > Service Control**. The following page is displayed.



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

Parameter	Description
Enable	Enables or disables the service control function.
Ingress	Supports LAN, WAN or empty The default value is empty, meaning any values.
Start Source IP Address	Start IP address of the source.
End Source IP Address	End IP address of the source.
Mode	The options are Permit and Discard.
Service List	The available options are Web, File Transfer Protocol (FTP), and TELNET. Select one or more options.
Modify	Click 🖉 to edit the corresponding access control rule.
Delete	Click to delete the corresponding access control rule.

3. Click Add.

-END OF STEPS-



Setting the ALG Switch (Fat AP)

This section describes how to configure the ALG switch.

Steps

The AP mode of the device is **Fat**.

1. Select **Security > ALG**. The following page is displayed.

¢	Status	Network	Security	Application	Administration	Help	Logout	
¢ 中 文 Firewall IP Filter MAC Filter Service List Service Control ALG ? _{Help}	Status	Network Enable	Security ALG ☑ FTP ☑ SIP ☑ L2TF ☑ H32 ☑ RTSI	Application ALG ALG ALG ALG 3 ALG 2 ALG	Administration	Help	Logout	
	IPSEC ALG							
	Submit Cancel							

2. Refer to the following table to confirm the protocol name for NAT conversion. Open/close the related ALG switches.

Parameter	Description
FTP ALG	Open/close the NAT conversion switch for the FTP protocol.
TFTP ALG	Open/close the NAT conversion switch for the TFTP protocol.
SIP ALG	Open/close the NAT conversion switch for the SIP protocol.
L2TP ALG	Open/close the NAT conversion switch for the L2TP protocol.
H323 ALG	Open/close the NAT conversion switch for the H323 protocol.
RTSP ALG	Open/close the NAT conversion switch for the RTSP protocol.
PPTP ALG	Open/close the NAT conversion switch for the PPTP protocol.
IPSEC ALG	Open/close the NAT conversion switch for the PSEC protocol.

3. Click Submit.

-END OF STEPS-

<u>Chapter</u> 6

Application Configuration

Configuring UPnP (Fat AP)

This section describes how to configure UPnP.

Context

The AP mode of the device is **Fat**.

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

A devices supporting UPnP can access the network dynamically, obtain the IP address, and send its performance information. If there are DHCP and DNS servers, the device can obtain the DHCP and DNS services automatically.

A devices supporting UPnP can be disconnected from the network automatically without affecting the device itself or other devices in the network.

Steps

1. Select **Application > UPnP**. The following page is displayed.

¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout
UPnP DNS Service QoS SNTP IGMP MLD Snooping LED Control	Adverti Advertise	En WAN Conner sement Perio minu ment Time To (in h	able tion d (in 30 Live 4 ops)		X		
	/					Submit	Cancel

Confidential and Proprietary Information of ZTE CORPORATION 56

Parameter	Description
Enable	Enable or disable the UPnP function. It is disabled by default.
WAN Connection	Select IGD.WD1.WCD1.WCIP1 or empty. The default value is empty, meaning any values.
Advertisement Period (in minutes)	Set the corresponding advertisement time as required. The unit is minute.
Advertisement Time to Live (in hops)	Set the corresponding time to live (hop count) as required.

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

3. Click Submit.

-END OF STEPS-

Setting a Device Name (Fat AP)

This section describes how to set a device name.

Steps

The AP mode of the device is **Fat**.

- 1. Set the domain name.
 - i. Select **Application > DNS Service > Domain Name**. The following page is displayed.

¢ † X	Status	Network	Security	Application	Administration	Help	Logout
UPnP							
-DNS Service		Domain N	ame				
Domain Name							
Hosts							
QoS							
SNTP							
IGMP							
MLD Snooping							
LED Control							
? Help							
	/					Submit	Cancel

- ii. In the **Domain Name** text box, enter the corresponding domain name, such as **ZTE**.
- iii. Click Submit.



- 2. Set the host name.
 - i. Select **Application** > **DNS Service** > **Hosts**. The following page is displayed.

¢ ₱ X	Status	Network	Security	Application	Administration	Help	Logout					
UPnP												
-DNS Service		Host N	amo									
Domain Name												
●Hosts		IP Address										
QoS			Add									
SNTP												
IGMP	_	5 51 B										
MLD Snooping	The	items with dis do't be energy	sabled button	is are allocate	d from a DHCP se	erver, which						
LED Control	coul	unt be opera	teo.									
		Host Nam	e	IP Addre	ss Modi	fy Delete						
2 Hala		There is no data, please add one first.										
	7											

ii. In the **Host Name** and **IP Address** text boxes, enter the host name and corresponding IP address respectively.

iii. Click Add.

NUIE Notes:

The items with dimmed buttons are allocated from a DHCP server and cannot be operated.

- Click \blacksquare to edit the corresponding host information.
- Click iii to delete the corresponding host information.

-END OF STEPS-

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.

The concept of Class of Service is introduced to QoS frame. By using QoS, ZXV10 W615 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 (such as ToS and priority) to queue. For the outgoing data packet, it is required to convert its queue to field mapping.



Configuring Basic QoS Parameters

This section describes how to set basic QoS parameters.

Steps

1. Select **Application > QoS > Basic**. The following page is displayed.

¢¢≵	Status	Network	Security	Application	Administration	Help	Logout
•QoS ●Basic Classification			Enable QoS				
Queue Management SNTP IGMP MLD Snooping LED Control	I	Total Upstrei Enable Queue Sched Enable DSC Enable 802.1	am Bandwidth Managemeni uler Algorithm CP Re-markin <u>c</u> Lp Re-markin <u>c</u>	0 : 	bps		
	/					Submit	Cancel

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

Parameter	Description
Enable QoS	Enables or disables the QoS function.
Total Upstream Bandwidth	Specifies the total upstream bandwidth.
Enable Queue Management	Enables or disables the function of congestion management. It is disabled by default.
Scheduler Algorithm	The available algorithms are SP, DWRR and SP_DWRR. SP: Sends 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 in turn. SP_DWRR: Adopts SP and DWRR. The queue 0 adopts the SP algorithm. The queue 1 to the queue 7 adopt the DWRR algorithm. That is, using the DWRR scheduler algorithm in priority on the queue 1 to queue 7, and then using the SP scheduler algorithm on the queue 0.
Enable DSCP Re-marking	Enables or disables DSCP re-marking. It is disabled by default.
Enable 802.1p Re-marking	Enables or disables 802.1p processing priorities re-marking. It is disabled by default.



3. Click Submit.

-END OF STEPS-

Setting a Classification Rule

This section describes how to set a classification rule.

Steps

1. Select **Application** > **QoS** > **Classification**. The following page is displayed.

Basic	Enable		
• Classification	DevIn	•	
Queue Management	L2Protocol		
IGMP	L 3Protocol		
MLD Snooping	Course MAG Address		
LED Control	Source MAC Address		
	802.1p	(0 ~ 7)	
😗 Help	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)	
	802.1n Re-marking	(0 ~ 7)	
	DSCP Re-marking	(0 ~ 63)	
	Duce Kernanking		
	Queue Index		
		Add	
	Rule Description	Modify Delete	
	There is no data, p	lease add one first.	

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

Parameter	Description



Parameter	Description
Enable	Enables or disables the function of QoS classification configuration.
DevIn	The ingress of packets. Select a LAN interface or the configured SSID. Only one interface type can be selected at a time.
L2Protocol	Specifies the layer-2 protocol for packets. The options are IPv4, IPv6, ARP, and PPPoE.
L3Protocol	Specifies the layer-3 protocol for packets. The options are 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). A greater value indicates a higher priority.
Destination Port MIN/MAX	Specifies the destination port number (minimum value and maximum value) of packets. The range is 0 to 65535.
Modify	Click 🖉 to modify the corresponding rule.
Delete	Click under the corresponding rule.
Modify	Click <i>low</i> to modify the corresponding rule.
Delete	Click under the corresponding rule.
Modify	Click 🖉 to modify the corresponding rule.
Delete	Click ut to delete the corresponding rule.
DSCP	Specifies the DSCP value of packets. The value range is 0 to 63.
Modify	Click 🖉 to modify the corresponding rule.
Delete	Click ut to delete the corresponding rule.
Proprietary configuration for	IPv4
Source IP Address MIN/MAX	Specifies the minimum and maximum values of packet source IP address.
Destination IP Address MIN/MAX	Specifies the minimum and maximum values of packet destination IP address.
TOS	Specifies the service type field of data packets. The range is 0 to 255.
IP Precedence	IP priority that ranges from 0 to 7 (0 indicates priority unavailable). A greater value indicates a higher priority.
Proprietary configuration for	IPv6
Source IPv6 Address MIN/MAX	Specifies the minimum and maximum values of packet source IPv6 address.
Destination IPv6 Address MIN/MAX	Specifies the minimum and maximum values of packet destination IPv6 address.

Parameter	Description
Traffic Class	Specifies the traffic type ranging from 0 to 255.
Flow Label	Specifies the flow flag ranging from 0 to 1048575.
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). A greater value indicates a higher priority.
DSCP Re-marking	Specifies the re-marking value of DSCP. The value range is 0 to 63.
Queue Index	Specifies the corresponding management queue number that ranges from 1 to 8.

3. Click Submit.

-END OF STEPS-

Configuring Congestion Management

This section describes how to configure congestion management.

Context

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

Steps

1. Select **Application** > **QoS** > **Queue Management**. The following page is displayed.

ZTE中兴

¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout
-QoS							
Basic	A	Current Sc	neduler Algori	thm is SP.			
Classification	-	Queue 8 is the default queue which is enabled by default.					
•Queue Management			Enab	le 🗖			
SNTP							
IGMP			Queue Ind	ex			
MLD Snooping							
LED Control		Queue I	ıdex	E	nable	Modify	
•		1			X	2	
U Help		2			X	2	
		3			X	2	
		4			X	2	
		5			X	2	
		6			X	2	
		7			X	2	
		0			1		

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

Parameter	Description
Enable	Enables or disables the configuration function of QoS queues.
Queue Index	Includes Queue 1- Queue 8. Queue 8 is enabled by default.

- 3. Click the *local* icon of the queue to be modified. Select or clear the **Enable** check box.
- 4. Click Modify.
- -END OF STEPS-

Configuring SNTP

This section describes how to configure time management to achieve time synchronization with the time server.

Steps

1. Select **Application > SNTP**. The following page is displayed.

ZXV10 W615 User Manual



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

Parameter	Description
Current Date and Time	Displays the current date and time of the device.
Time Zone	Specifies the time zone where the device is located.
Primary NTP Server Address	Specifies the address or domain name of the primary Network Time Protocol (NTP) server.
Secondary NTP Server Address	Specifies the address or domain name of the secondary NTP server.
Poll Interval	The interval of server time synchronization. It is 86400 seconds by default.
Enable Daylight Saving Time	Enables or disables the daylight saving time function. It is disabled by default.
DSCP	Specifies the DSCP value. The value range is 0-63.

3. Click Submit.

-END OF STEPS-

IGMP Configuration

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

The IP host uses the 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.

Configuring WAN Connection (Fat AP)

This section describes how to configure WAN connection.

Steps

The AP mode of the device is Fat.

1. Select **Application** > **IGMP** > **WAN Proxy**. The following page is displayed.



- 2. Select **IGD.WD1.WCD1.WCIP1** or **WANBRIDGE1** as the WAN connection.
- 3. Click Add.
- -END OF STEPS-

Configuring IGMP Snooping

This section describes how to configure IGMP snooping.

Steps

1. Select **Application** > **IGMP** > **IGMP** Snooping. The following page is displayed.



¢ 中 文	Status	Network	Security	Application	Administration	Help	Logout
QoS SNTP							
-IGMP					Enable IGMP P	roxy 🗌	
●IGMP Snooping				Er	nable IGMP Snoo	ping 🗹	
MLD Snooping LED Control			En	able IGMP Sno	ooping Enhancen	nent 🗹	
? Helo							
	/					Submit	Cancel

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

Parameter	Description
Enable IGMP Proxy	Enables or disables the IGMP proxy function. It is disabled by default.
Enable IGMP Snooping	Enables or disables the IGMP snooping function. It is enabled by default.
Enable IGMP Snooping Enhancement	Enables or disables the IGMP snooping enhancement function. It is enabled by default.

3. Click Submit.

-END OF STEPS-

Configuring MLD Snooping

This section describes how to configure Multicast Listener Discovery (MLD) snooping.

Steps

1. Select **Application > MLD Snooping**. The following page is displayed.

ZTE中兴

ф Ф X	Status	Network	Security	Application	Administration	Help	Logout
QoS SNTP IGMP MLD Snooping LED Control HelD	Enat	Ena ole MLD Snooj	ble MLD Snoo	ping 🗹 nent 🗹			
	/					Submit	Cancel

- 2. Based on the actual requirement, select or clear **Enable MLD Snooping** and **Enable MLD Snooping Enhancement**. Two parameters are all enabled by default.
- 3. Click Submit.

-END OF STEPS-

Configuring LED Control

This section describes how to configure LED control.

Steps

1. Select **Application > LED Control**. The following page is displayed.



- 2. Enable or disable the LED function.
- 3. Click **Submit**.
- -END OF STEPS-

<u>Chapter</u> 7

Management Configuration

Managing SNMPv1/v2c

This section describes how to configure SNMPv1/v2c management.

Steps

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

¢ † X	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM)		E	nable SNMP	V 102 169 1 1			
User Management System Management Log Management AP Manaoement		Trap Trap	Server 1P [Server2 IP [Server Port [162 (1 ~ 65535)		
Diagnosis 7 _{Heln}		Read Write	Community [Community [public private			
	/					Submit	Cancel

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

Parameter	Description
Enable SNMP	Enables or disables the SNMP function. The default value is enabled.
Trap Server IP	Enter the IP address of the Trap server, for example, 192.168.1.1.
Trap Server2 IP	Enter the IP address of the standby Trap server.



Parameter	Description
Trap Server Port	Enter the port number of the Trap server within the range 1–65535. The default value is 162.
Read Community	The default password is public.
Write Community	The default password is private.

3. Click Submit.

-END OF STEPS-

SNMPv3 Security Management (USM)

Managing SNMPv3 Users

This section describes how to manage SNMPv3 users.

Steps

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

¢	Status	Network	Security	Application	Administratio	n Help	Logout
SNMPv1/v2c							
-SNMPv3 Security(USM)		Sec	curity Name				
SNMPv3 Users		Authentienti	ion Drotocol				
SNMPv1/v2c Users		Authentication Protocol none					
SNMPv3 Access Control (VACM)	1	Authentication	n Password		_		
User Management		Priva	acy Protocol	none	•		
System Management		Privacy Password					
Log Management							
AP Management				Add			
Diagnosis							
2 Hala	S	ecurity Name	Authentica Protocc	tion I I	Privacy Protocol Mo	difyDelete	
- neib	na	anpuser			(
	а	npuser	MD5		(/	
	i	apuser	MD5		DES	/	

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

Parameter	Description		
Security Name	User name.		
Authentication Protocol	The options are None, MD5, and SHA.		



Parameter	Description		
Authentication Password	Authentication password.		
Privacy Protocol	The options are None and DES.		
Privacy Password	Encryption password.		
Modify	Click <i>C</i> to modify the corresponding SNMPv3 user information.		
Delete	Click to delete the corresponding SNMPv3 user information.		

3. Click Add.

-END OF STEPS-

Managing SNMPv1/v2c Users

This section describes how to manage SNMPv1/v2c users.

Steps

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

¢ ₱ ┇	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c -SNMPv3 Security(USM) SNMPv3 Users •SNMPv1/v2c Users		Sec	curity Name (Source IP (
SNMPv3 Access Control (VACM)				Add			
User Management System Management	S	ecurity Name		Source IP	Modify	Delete	
Log Management AP Management		public		0.0.0.0	2	İ	
Diagnosis							
? Helo							
	/						

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

Parameter	Description		
Security Name	User name.		
Source IP	Start IP address of the source.		
Modify	Click 🖉 to modify the corresponding SNMPv1/v2c user		


Parameter	Description
	information.
Delete	Click to delete the corresponding SNMPv1/v2c user information.

3. Click Add.

-END OF STEPS-

SNMPv3 Access Control Management (VACM)

Managing Context

This section describes how to manage the context.

Steps

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



- 2. Enter the context information. The default is "".
- 3. Click **Submit**.
- -END OF STEPS-

Managing Security Groups

This section describes how to manage security groups.



Steps

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

¢¢Ì	Status	Network	Security	Application	Administration	Help	Logout	
SNMPv1/v2c SNMPv3 Security(USM) -SNMPv3 Access Control (VACM) Context • Security To Group View Tree Family Access Table	Security Model USM Security Name nanpuser Group Name Add							
User Management System Management Log Management AP Management Diagnosis	Sec	USM USM USM USM	Security Na nanpuse anpuser apuser	me Grou r read write write	p Name Modi Igroup 2 2group 2 2group 2	y Delete		
• Help	/							

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

Parameter	Description
Security Model	Supports USM, SNMPv1, and SNMPv2c.
Security Name	Supports nanpuser, anpuser, apuser.
Group Name	Specifies the group name.
Modify	Click <i>low</i> to modify the corresponding security group information.
Delete	Click to delete the corresponding security group information.

- 3. Click Add.
- -END OF STEPS-

Managing View Subtree

This section describes how to configure the view subtree.

Steps

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

¢ ₱ ┇	Status	Network	Security	Application	Administratio	n Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) -SNMPv3 Access Control (VACM) Context Security To Group •View Tree Family Access Table			View Name [SubTree [Mask [Type]	included Add	(Optional)		
System Management	11		Culture	March	T 11-	l'6 palata	
Log Management AP Management Diagnosis	VI	ew Name all	SubTree .1	Mask	included	dity Delete	
P _{Help}							

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

Parameter	Description
View Name	View name.
SubTree	Subtree name.
Mask	(Optional) Subnet mask.
Туре	The options are included and excluded.
Modify	Click <i>low</i> to modify the corresponding view information.
Delete	Click to delete the corresponding view information.

3. Click Add.

-END OF STEPS-

Managing the Access Table

This section describes how to manage the access table.

Steps

1. Select Adminstration > SNMPv3 Access Control (VACM) > Access Table. The following page is displayed.



ZXV10 W615 User Manual

\$ † Ì	Status	Network	Security	y Application	Administration	Help	Logo			
SNMPv1/v2c										
SNMPv3 Access Control		Group Name readgroup 🔽								
VACM)		Context Prefix								
Context										
Security To Group		58	curity mode	ei jusm	<u> </u>					
View Tree Family		Se	ecurity Leve	el noAuthNoPriv	•					
•Access Table		Co	ntext Match	h exact	v					
User Management		Read	View Name	e none	•					
System Management					-					
bystem Hundgement		Maita	Minus Manas		-					
Log Management		Write	View Name	e none	<u> </u>					
Log Management AP Management Diagnosis		Write Notify	View Name View Name	e none e none	<u>·</u>					
Log Management AP Management Diagnosis		Write Notify	View Name View Name	e none e none	•					
Log Management AP Management Diagnosis		Write Notify	View Name	e none e none Add	•					
Log Management AP Management Diagnosis ? Help		Write Notify	View Name	e Inone e Inone Add Authentication	2					
Log Management AP Management Diagnosis Helo	Group Nan	Write Notify	View Name View Name xt Prefix	e none e none Add Authentication Protocol	Security Le	vel	/Dalata			
Log Management AP Management Diagnosis ? Help	Group Nan Context Mal	Write Notify e Contex ch Rear	View Name View Name xt Prefix d View ame	e Inone e Inone Add Authentication Protocol Write View Nam	Security Le e Notify Vie Name	vel Modify w	/Delete			
Log Management AP Management Diagnosis Helo	Group Nam Context Mat readgroup	Write Notify Ie Conte: Ich Read Ni	View Name View Name xt Prefix d View ame	e Inone Add Authentication Protocol Write View Nam	Security Le Between the security Le Notify Vie Name noAuthNoP	vel W Modify	/Delete			
Log Management AP Management Diagnosis Helo	Group Nam Context Mai readgroup exact	Write Notify e Conte: ch Rea(N)	View Name View Name xt Prefix d View ame "" all	e Inone Add Authentication Protocol Write View Nan USM none	Security Le Security Vie Name noAuthNoP none	vel w Modify riv 2	/Delete			
Log Management AP Management Diagnosis Helo	Group Nan Context Ma readgroup exact writegroup	Write Notify ch Rea(N)	View Name View Name xt Prefix d View ame "" all	e Inone Add Authentication Protocol Write View Nam USM None USM		vel Modify	/Delete			

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

Parameter	Description
Group Name	Group name.
Context Prefix	Information on the context prefix.
Security Model	Supports USM, SNMPv1, SNMPv2c, and any.
Security Level	Supports noAuthNoPriv, authNoPriv, and authPriv.
Context Match	The options are exact and prefix.
Read View Name	The options are none and all.
Write View Name	The options are none and all.
Notify View Name	The options are none and all.
Modify	Click <i>Click</i> to modify the corresponding access table information.
Delete	Click i to delete the corresponding access table information.

3. Click Add.

-END OF STEPS-

User Management

Managing Users

This section describes how to manage users. You can modify the admin password and create a common account.

Steps

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

¢¢≵	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) -User Management		User Privil	ege: ⊙ Adm O User	inistrator			
User Management Auto Logout Management System Management		Usern Old Passa	ame admin				
Log Management AP Management Diagnosis		New Passy	vord				
Help	Col	nfirmed Passv	vord				
	\square					Submit	Cancel

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

Parameter	Description
User Privilege	Determines 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.
Confirmed Password	To make a confirmation, enter the new password again.

3. Click **Submit**.



-END OF STEPS-

Managing Automatic Logout

This section describes how to configure automatic logout.

Steps

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

¢ 中 文	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c							
SNMPv3 Security(USM)							
SNMPv3 Access Control (VACM)			limeout		5 ~ 60 min)		
-User Management							
User Management							
•Auto Logout Management							
System Management							
Log Management							
AP Management							
Diagnosis							
? Help							
	/					Submit	Cancel

- 2. Set the timeout period within the range of 5 to 60 minutes. The default is 5 minutes.
- 3. Click Submit.

-END OF STEPS-

Device Management

Configuring System Management

This section describes how to configure system management.

Steps

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

¢	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management -System Management	٨	Click this b	utton to warn Warm Re	n reboot the d	evice.		
System Management Software Upgrade User Configuration Management Default Configuration Management Log Management	۵	Click this b	utton to cold I Cold Rel	reboot the der poot	vice.		
AP Management Diagnosis PHelp	٨	Click this b settings. T	utton to resto he device will <u>Restore D</u>	re the configu reboot after o efault	ration to factory operating.	default	
	/						

- 2. You can restart the device or restore default settings.
 - Click Warm Reboot for a warm restart of the device.
 - Click **Cold Reboot** for a cold restart of the device.
 - Click **Restore Default** to restore the factory settings.

-END OF STEPS-

Setting Version Upgrade

This section describes how to upgrade the ZXV10 W615 system through a Web page.

Steps

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



4	The device	will reboot a	tar unara dina			
			ter upgrading			
Please s	elect a new s	oftware/firmv	vare image		浏览	
			Upgrade			
				Upgrade	Upgrade	Upgrade

Notes:

You need to wait patiently when the software of the device is being upgraded, and pay attention to the prompt in the page. To prevent the device from being damaged, do not turn off the power or restart the device.

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

-END OF STEPS-

Managing User Configuration

This section describes how to manage user configuration.

Steps

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

9 4 X	Status	Network	Security	Application	Administration	Help	Logout		
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management		Bac	kup user con Back	figuration file l up Configurat	from the device				
-System Management System Management Software Upgrade	Δ	The device	will reboot al	ter operating.					
Management Default Configuration Management	Plea	Please select a user configuration file							
AP Management Diagnosis					_				

- 2. Choose backup operation or configuration import based on the actual requirement.
 - To export a configuration file, do as follow:

Click **Backup Configuration**. Then, the system backs up the current configuration file of the device.

- ► To import a configuration file, do as follow:
 - i. Click **Browse** and select the configuration file to be imported.
 - ii. Click **Restore Configuration**. Then, the specified configuration file is imported.

NOTE Notes:

The device automatically restarts after the operation is completed.

-END OF STEPS-

Managing the Default Configuration

This section describes how to manage the default configuration.

Steps

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



¢ 中 文	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management		Back	up default co	nfiguration file up Configurat	from the device		
-System Management System Management Software Upgrade User Configuration Management	٨	The device	will reboot a	iter operating.			
Default Configuration	Pleas	e select a dei	fault configur	ation file		浏览	
Management Log Management			Rest	ore Configurat	ion		
AP Management							
Diagnosis							

- 2. Choose backup operation or configuration import based on the actual requirement.
 - ▶ To export a configuration file, do as follow:

Click **Backup Configuration**. Then, the system backs up the default configuration file of the device.

- To import the default configuration file, do as follows:
 - 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 Notes:

The device automatically restarts after the operation is completed.

-END OF STEPS-

Configuring Log Management

This section describes how to configure log management.

Steps

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

¢ † X	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management System Management Log Management Diagnosis PHelo	Er Lo ProductCla SerialNuml IP: 192.16(HWVer:V3 SWVer:V2. P0000-00- because Iţ P0000-00- because Iţ P0000-00-	Enable Save Log L nable Remote g Server Add rer:ZTE; ss:ZXV10 W0 ber:ZTENW36 3.0.228; .0; .0; .00T00:00:28 pv4 Wan Eth .00T002:12:42 pv4 Wan Eth .00T02:12:42 pv4 Wan Eth .00T02:12:42	Log V evel Notice Log ress 515 V3; 511100035; 515 V3; 511100035; 515 V3; 511100035; 515 V3; 515 V3;	I log! Wanc D ct! WAND is I log! Wanc D	isconnect GD.WD1 isconnect GD.WD1 isconnect GD.WD1 isconnect acconnect		
	/					Submit	Cancel

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

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

- 3. Click the corresponding button as needed.
 - 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 disk.
 - Click Submit to display the log information of the corresponding log level



in the square box on the page.

-END OF STEPS-

Access Point Management

Setting the AP Mode

This section describes to set the AP mode.

Steps

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

	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management	٨	The device Mode is cha	will be automa nged.	tically reboot	ed after the AP		
System Management Log Management -AP Management		AP N	lode Fit	V			
AP Name Diagnosis							
😗 Helo							
	/					Submit	Cancel

2. Set the AP mode, Fat or Fit, based on the actual requirement.

NOTE Notes:

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

3. Click Submit.

-END OF STEPS-

Setting an AP Name

This section describes how to set an AP name.

Steps

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

82 Confidential and Proprietary Information of ZTE CORPORATION

♀ 申 文	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c							
SNMPv3 Security(USM)							
SNMPv3 Access Control (VACM)							
User Management		AP N	ame AP4CAC	0A4FAD96			
System Management							
Log Management							
-AP Management							
AP Mode							
●AP Name							
Diagnosis							
2 Help							
	_						
	7					Submit	Cancel

- 2. In the **AP Name** text box, set the corresponding name.
- 3. Click Submit.
- -END OF STEPS-

Diagnosis Configuration

Performing Ping Diagnosis

This section describes how to configure Ping diagnosis to detect device faults.

Steps

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



今中文	Status	Network	Security	Application	Administration	Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control VACM) User Management Log Management AP Management •Ping Diagnosis Trace Route Diagnosis WAN Type ?Help	IP Ad	dress or Host Name Ping num g packet size Egress	3	(1~40	96)	Ā	
	7					Submit	Cancel

- 2. In the **IP Address or Host Name** text box, type the host IP address or host name.
- 3. In the **Ping num** text box, type the Ping times.
- 4. In the **Ping packet size** text box, type the suitable Ping packet size. The value range is 1–4096.
- 5. In Engress drop-down box, select the egress to be diagnosed.

```
NOTE Notes:
```

Engress supports LAN, WAN and empty. The default value is empty, meaning any values.

6. Click **Submit**. The Ping result is displayed in the text box below.

-END OF STEPS-

Configuring Trace Route Diagnosis

Disconnected network nodes can be determined through Trace Route, which helps locate faults.

Steps

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

¢ ₱ ⋭	Status	Network	Security	Application Administrat	ion Help	Logout
SNMPv1/v2c SNMPv3 Security(USM) SNMPv3 Access Control (VACM) User Management System Management Log Management AP Management •Diagnosis Ping Diagnosis •Trace Route Diagnosis •Trace Route Diagnosis	IP Addr	ess or Host N WAN Conne Maximum H Wait	lame trion lops 30 Time 5	(2 ~ 64) (2 ~ 10 sec)		
	/				Submit	Cancel

- 2. In the **IP Address or Host Name** text box, type the host IP address or host name.
- 3. In the **WAN Connection** text box, select the WAN connection to be diagnosed
- 4. In the **Maximum Hops** text box, select the maximum number of hops to be diagnosed.
- 5. In the **Wait Time** text box, select the timeout period.
- 6. Click **Submit**. The Trace Route result is displayed in the area in the lower part.
- -END OF STEPS-



FCC Regulations:

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

This device 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 radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

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

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

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure Information

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation. The antenna of this device must be fixed-mounted on outdoor permanent structures to satisfy RF exposure requirements.

Glossary

ARP - Address Resolution Protocol, Allocation Retension priority **DHCP - Dynamic Host Configuration Protocol** DNS - Domain Name System, Domain Name Server **DSCP - Differentiated Services Code Point** FTP - File Transfer Protocol, Foiled Twisted Pair, Floating Termination **Point ICMP - Internet Control Message Protocol** ID - Identification, Identity, Identifier **IGMP - Internet Group Management Protocol IPv4 - Internet Protocol version 4 IPv6 - Internet Protocol Version 6 ISP - Internet Service Provider** MAC - Medium Access Control, Message Authentication Code MTU - Maximum Transfer Unit, Multi-Tenant Unit, Maximum **Transmission Unit NAT - Network Address Translation NTP - Network Time Protocol PoE - Power over Ethernet QoS - Quality of Service RARP - Reverse Address Resolution Protocol SNMP - Simple Network Management Protocol** STP - Signaling Trace Part, Signaling Transfer Point, Spanning Tree Protocol, Shielded Twisted Pair, SATA Tunneling Protocol **UDP - User Datagram Protocol** VLAN - Virtual Local Area Network **WEP - Wired Equivalent Privacy**

WLAN - Wireless Local Area Network

WPA - Wi-Fi Protected Access