



ZXHN F670

GPON ONU

## Maintenance Management Guide

---

Version: V1.0

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

## **LEGAL INFORMATION**

Copyright © 2015 ZTE CORPORATION.

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

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

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

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

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the ZTE technical support website <http://support.zte.com.cn> to inquire for related information.

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

## **Revision History**

Serial Number: SJ-20151016170048-003

Publishing Date: 2015-11-10 (R1.0)

# Contents

---

<b>Safety Precautions .....</b>	<b>I</b>
<b>Chapter 1 Product Overview .....</b>	<b>1-1</b>
1.1 Package Content.....	1-1
1.2 Indicator .....	1-2
1.3 Interface .....	1-3
1.4 Product Features.....	1-4
1.5 Technical Specification .....	1-5
1.6 Cable Connection.....	1-5
<b>Chapter 2 Configuration Preparation .....</b>	<b>2-1</b>
2.1 Configure TCP/IP .....	2-1
2.2 Login to the System.....	2-2
<b>Chapter 3 Status .....</b>	<b>3-1</b>
3.1 Check the Device Information .....	3-1
3.2 Check the Network Interface .....	3-2
3.2.1 Check the WAN Connection Information .....	3-2
3.2.2 Check the 3G Connection Information .....	3-4
3.2.3 Check the 4in6 Tunnel Connection Information.....	3-5
3.2.4 Check the PON Information .....	3-6
3.2.5 Check the Mobile Network Information.....	3-6
3.3 Check the User Interface .....	3-7
3.3.1 Check the WLAN Radio 2.4G Information .....	3-7
3.3.2 Check the Ethernet Information .....	3-9
3.3.3 Check the USB Information.....	3-10
3.4 Check the VoIP Information.....	3-10
<b>Chapter 4 Network Configuration .....</b>	<b>4-1</b>
4.1 WAN Configuration.....	4-1
4.1.1 Configure the WAN Connection .....	4-1
4.1.2 Configure the 3G WAN Connection .....	4-5
4.1.3 Create a 4in6 Tunnel Connection .....	4-7
4.1.4 Create a 6in4 Tunnel Connection .....	4-9
4.1.5 Configure the Port Binding .....	4-10
4.1.6 Configure the DHCP Release.....	4-12
4.2 WLAN Common Setting.....	4-12

4.2.1 Configure the WiFi Restrictions .....	4-12
4.2.2 Configure the Setting Deleting.....	4-14
4.3 WLAN Radio 2.4G(Online) Configuration .....	4-15
4.3.1 Configure the WLAN Basic Configuration(2.4G) .....	4-15
4.3.2 Configure the SSID(2.4G).....	4-17
4.3.3 Configure the WLAN Security(2.4G) .....	4-19
4.3.4 Access the Control List(2.4G).....	4-21
4.3.5 Check the Associated Devices(2.4G).....	4-22
4.3.6 Configure the WMM(2.4G) .....	4-23
4.3.7 Configure the WPS(2.4G) .....	4-25
4.4 WLAN Radio 5G Configuration.....	4-27
4.4.1 Configure the Basic Parameters(5G) .....	4-27
4.4.2 Configure the SSID(5G).....	4-30
4.4.3 Configure the WLAN Security(5G).....	4-31
4.4.4 Access the Control List(5G) .....	4-33
4.4.5 Check the Associated Devices(5G) .....	4-34
4.4.6 Configure the WMM(5G).....	4-35
4.4.7 Configure the WPS(5G) .....	4-37
4.5 LAN Configuration .....	4-38
4.5.1 Configure the DHCP Server .....	4-38
4.5.2 Configure the DHCP Server(IPv6) .....	4-40
4.5.3 Configure the DHCP Binding.....	4-42
4.5.4 Configure the DHCP Port Service.....	4-42
4.5.5 Configure the Static Prefix .....	4-44
4.5.6 Configure the DHCP Port Service (IPv6).....	4-45
4.5.7 Configure the RA Service.....	4-47
4.6 Register.....	4-49
4.7 Route Management(IPv4).....	4-52
4.7.1 Configure the Default Gateway(IPv4).....	4-52
4.7.2 Configure the Static Routing(IPv4).....	4-52
4.7.3 Configure the Policy Routing(IPv4) .....	4-53
4.7.4 Check the Routing Table(IPv4) .....	4-55
4.8 Route Management(IPv6) .....	4-56
4.8.1 Configure the Default Gateway(IPv6).....	4-56
4.8.2 Configure the Static Routing(IPv6) .....	4-56
4.8.3 Configure the Policy Routing(IPv6) .....	4-57
4.8.4 Check the Routing Table(IPv6) .....	4-59

4.9 Configure the Port Locating.....	4-59
<b>Chapter 5 Security Configuration .....</b>	<b>5-1</b>
5.1 Configure the Firewall.....	5-1
5.2 Configure the IPv4 Filter .....	5-3
5.3 Configure the MAC Filter .....	5-5
5.4 Configure the URL Filter .....	5-6
5.5 Configure the Service Control Filter .....	5-6
5.6 Configure the ALG Feature .....	5-8
<b>Chapter 6 Application Configuration.....</b>	<b>6-1</b>
6.1 VoIP (H248) Configuration .....	6-1
6.1.1 Configure the WAN Connection(H248).....	6-1
6.1.2 Configure the Advanced Parameters(H248).....	6-2
6.1.3 Configure the Fax Feature(H248) .....	6-4
6.1.4 Configure the VoIP Service(H248).....	6-4
6.1.5 Configure the Basic H248 Parameters .....	6-6
6.1.6 Configure the H248 Terminations .....	6-8
6.1.7 Configure the H248 Authentication .....	6-9
6.1.8 Configure the H248 Timers .....	6-11
6.1.9 Configure the Media Codec Type(H248) .....	6-12
6.1.10 Configure the CID Feature(H248).....	6-14
6.1.11 Configure the SLIC(H248).....	6-15
6.2 VoIP (SIP) Configuration .....	6-17
6.2.1 Configure the WAN Connection(SIP) .....	6-17
6.2.2 Configure the Advanced Parameters(SIP).....	6-17
6.2.3 Configure the Fax Feature(SIP).....	6-17
6.2.4 Configure the SIP Protocol.....	6-17
6.2.5 Configure the SIP Account.....	6-19
6.2.6 Configure the VoIP Service(SIP).....	6-20
6.2.7 Configure the Digital Map.....	6-22
6.2.8 Configure the Media Codec Type(SIP).....	6-23
6.2.9 Configure the CID Feature(SIP) .....	6-25
6.2.10 Configure the SLIC(SIP) .....	6-26
6.3 Configure the DDNS.....	6-26
6.4 Configure the DMZ .....	6-27
6.5 Configure the UPnP .....	6-29
6.6 Check the UPnP Port Mapping.....	6-30
6.7 Configure the Port Forwarding .....	6-31

6.8 DNS Service .....	6-33
6.8.1 Configure the Domain Name .....	6-33
6.8.2 Configure the Hosts .....	6-34
6.8.3 Configure the DNS Servers .....	6-35
6.9 Configure the Time Parameters .....	6-36
6.10 Multicast Configuration .....	6-37
6.10.1 Configure the IGMP WAN Connection .....	6-37
6.10.2 Configure the Multicast Mode .....	6-38
6.10.3 Configure the MLD WAN Connection .....	6-39
6.10.4 Configure the Basic Parameters of Multicast .....	6-40
6.10.5 Configure the VLAN .....	6-41
6.10.6 Configure the Maximum Number of Addresses .....	6-42
6.11 Configure the BPDU .....	6-43
6.12 Check the USB Storage Information .....	6-44
6.13 Configure the DMS .....	6-45
6.14 Configure the FTP Server Feature .....	6-47
6.15 Configure the Port Triggering .....	6-48
6.16 Configure the Port Forwarding(Application List) .....	6-50
6.17 Configure the Application List .....	6-51
6.18 Configure the Samba Service .....	6-52
6.19 Configure the USB Print Server .....	6-54
<b>Chapter 7 Administration Management.....</b>	<b>7-1</b>
7.1 Remote Management .....	7-1
7.1.1 Configure the Basic Parameters of TR-069 .....	7-1
7.1.2 Configure the Certificate .....	7-3
7.2 Configure the Web User Management .....	7-4
7.3 Configure the Login Timeout .....	7-5
7.4 Device Management.....	7-6
7.4.1 Configure the System Management.....	7-6
7.4.2 Configure the Software Upgrade .....	7-6
7.4.3 Configure the User Configuration Management .....	7-7
7.4.4 Configure the Default Configuration Management .....	7-8
7.4.5 Configure the Remote Upgrade .....	7-9
7.4.6 Configure the USB Backup .....	7-10
7.4.7 Configure the USB Restoration .....	7-11
7.5 Configure the Log Management .....	7-12
7.6 Diagnosis and Maintenance .....	7-14

7.6.1 Configure the Ping Diagnosis .....	7-14
7.6.2 Configure the Trace Route Diagnosis .....	7-15
7.6.3 Configure the Simulation.....	7-17
7.6.4 Configure the AT Diagnosis.....	7-18
7.6.5 Configure the Port Mirror .....	7-19
7.6.6 Configure the PPPoE Diagnosis .....	7-20
7.6.7 Configure the DNS Diagnosis.....	7-21
7.6.8 Configure the IP Diagnosis .....	7-22
7.6.9 Configure the Voice Diagnosis .....	7-23
7.6.10 Check the ARP Table.....	7-24
7.6.11 Check the MAC Table .....	7-25
7.7 Loopback Detection.....	7-26
7.7.1 Configure the Basic Parameters of Loopback Detection.....	7-26
7.7.2 Configure the Loopback Detection.....	7-28
7.7.3 Configure the VLAN of Loopback Detection .....	7-29
7.8 Configure the IPv6 Switch.....	7-30
7.9 Configure the VoIP Protocol .....	7-31
7.10 Configure the 3G Switch .....	7-32
<b>Appendix A Troubleshooting .....</b>	<b>A-1</b>

# Safety Precautions

---

## Usage Cautions

- Read all the safety cautions carefully before using the device.
- Only use the accessories included in the package, such as power supply adapter.
- Do not extend the power cord, otherwise the device will not work.
- The power supply voltage must meet the requirements of the device input voltage (The voltage fluctuation range is less than 10%).
- Keep the power plug clean and dry to prevent any risk of electric shock or other dangers.
- Disconnect all the cables during a lightning storm to prevent the device from damage.
- Power off and unplug the power plug when the device is not in use for a long time.
- Do not attempt to open the covers of the device. It is dangerous to do so when the device is powered ON.
- Do not directly stare at the optical interface to prevent any eye injuries.
- Power off and stop using the device under the conditions such as, abnormal sound, smoke, and strange smell. Contact the service provider for maintenance if the device is faulty.



### Note:

The users should read the usage cautions above carefully and will be responsible for any incident resulting from the violation of the above cautions.

---

## Environment Requirements

- Ensure proper ventilation to the device. Place the device away from direct sunlight and never spill any liquid on the device.
- Do not place any object on the device to prevent any deformation or damage to the device.
- Do not place the device near any source of heat or water.
- Keep the device away from any household appliances with strong magnetic or electric fields, such as microwave oven and refrigerator.

## Cleaning Requirements

- Before cleaning, power off the device, and unplug all the cables connected to the device, such as power cable, optical fiber, and Ethernet cable.
- Do not use any liquid or spray to clean the device. Use a soft dry cloth.



## Environment Protection

- Do not dispose the device or battery improperly.
- Observe the local regulations about the equipment disposal or treatment.

RF exposure information: The Maximum Permissible Exposure (MPE) level has been calculated based on a distance of  $d=20$  cm between the device and the human body. To maintain compliance with RF exposure requirement, a separation distance of 20 cm between the device and the human should be maintained.

# Chapter 1

# Product Overview

---




## Table of Contents

Package Content.....	1-1
Indicator .....	1-2
Interface .....	1-3
Product Features.....	1-4
Technical Specification .....	1-5
Cable Connection.....	1-5

## 1.1 Package Content

Please make sure the ZXHN F670 package contains the items, refer to [Table 1-1](#).

Table 1-1 Package Contents

Item	Name	Quantity
	ZXHN F670 unit (built-in antenna/external antenna)	One
	AC-DC power supply adapter	One
	RJ-45 Ethernet cable	One



**Note:**

This manual uses a external antenna product as an example to describe product features. Refer to the object for the actual external view. This document is for reference only. For the actual product, refer to the object provided by operator.

One *ZXHN F670 GPON ONT User Manual* is delivered with the product.

If any of the items included in the package is incorrect, lost or damaged, please contact your service provider. If you need to replace the product, please keep the package and all the items in good condition.



Indicator	Status	Description
2.4GHz	Off	The device is not powered on or the wireless interface is disabled.
	Solid green	The wireless interface is enabled.
	Flashing green	Data is being transmitted.
5GHz	Off	The device is not powered on or the wireless interface is disabled.
	Solid green	The wireless interface is enabled.
	Flashing green	Data is being transmitted.
WPS	Yellow	Negotiation is in progress.
	Green	Negotiation is successful.
	Red	Session overlapping detection is being implemented or negotiation fails.
USB	Off	The device is not powered on or the USB interface is not connected.
	Solid green	The USB interface is connected and operating in host mode, but no data is being transmitted.
	Flashing green	Data is being transmitted on the interface.
BBU(optional)	Off	There is no standby power supply or the standby power supply fails.
	Solid green	The standby power supply is used and operates properly.
	Flashing green	The standby power supply is used but operates improperly. For example, undervoltage occurs.

## 1.3 Interface

Figure 1-2 shows the interfaces and buttons of the ZXHN F670 unit.

**Figure 1-2 Interfaces and Buttons on the Side Panel**



Table 1-3 describes the interfaces and buttons on the back panel of the ZXHN F670 unit.

**Table 1-3 Descriptions of the Interfaces and Buttons on the Side Panel**

Interface/Button	Description
WPS	Wi-Fi protection button. To enable the Wi-Fi protection function, press this button, so that users can access the network without entering their passwords.
Reset	Reset button, when the power is on, use a needle to press the button for over 5 seconds to restore the default settings.
Wi-Fi	WLAN button for enabling or disabling the WLAN function.

Figure 1-3 shows the interfaces and buttons of the ZXHN F670 unit.

**Figure 1-3 Interfaces and Buttons on the Back Panel**

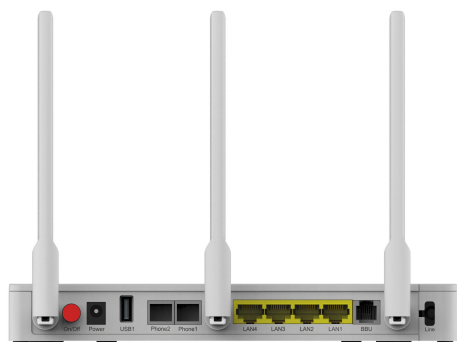


Table 1-4 describes the interfaces and buttons on the back panel of the ZXHN F670 unit.

**Table 1-4 Descriptions of the Interfaces and Buttons on the Back Panel**

Interface/Button	Description
On/Off	Power switch.
Power	12 V DC power connector.
USB1	Standard USB 2.0 interface, connected to a USB storage device for file sharing, fast backup, and data restoration.
Phone1、Phone2	RJ-11 telephone interface, connected to the telephone with RJ-11 telephone cable.
LAN1–LAN4	RJ-45 Ethernet interface.
BBU(optional)	Standby power supply interface, connected to a standby power supply through a dedicated cable.
Line	PON interface.

## 1.4 Product Features

### Interfaces

- GPON interface: GPON standard, SC/APC, comply with ITU G.984.1–G.984.5 standards.
- Ethernet interface: auto-sensing RJ-45 interface in compliance with IEEE 802.3 and IEEE 802.3u.
- Phone interface: RJ-11.
- WLAN interface: complies with IEEE 802.11ac, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n.
- USB interface: standard USB 2.0 interface.

### Technical Features

- Broadband service access: Connected to Internet through the GPON access method.
- Ethernet service access: Provides Ethernet interfaces, connected to the Ethernet devices, such as the user PC. Provides the Internet access and IPTV services.

- Phone service access: Supports SIP, H.248 and MGCP protocol.
- WLAN: Users can connect to the ZXHN F670 through WLAN.
- Data sharing, backup, and restoration: provides the USB 2.0 interface connected to a USB storage device for file sharing, fast backup, and data restoration.
- Security: Provides multi-level authentication based on the device, user and service, and provides the data channel encryption for safety.
- QoS: Provides QoS services meeting the requirements of various services for the local devices and network.
- Network management: Provides multi-mode network management.

## 1.5 Technical Specification

For the technical specifications of the ZXHN F670 , refer to [Table 1-5](#).

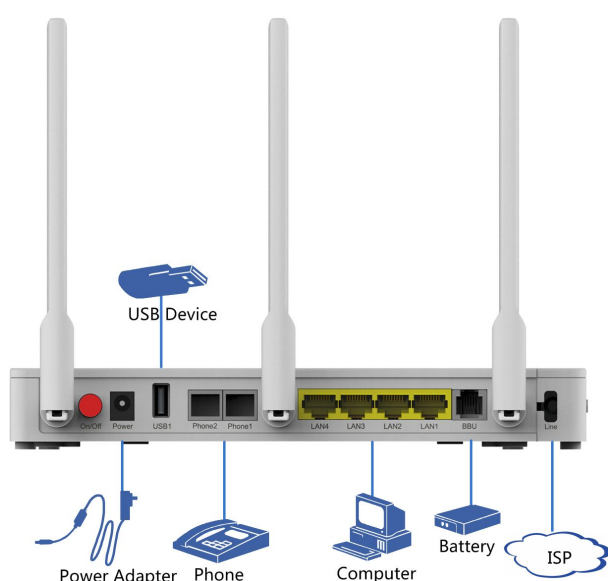
**Table 1-5 Technical Specifications**

Item	Specification
Dimension	220 mm (W) × 160 mm (D) × 28 mm (H)(antenna unincluded)
Rated current	1.5 A
Rated voltage	12 V DC
Operation temperature	0°C ~ 40°C
Operation humidity	5% ~ 95%

## 1.6 Cable Connection

[Figure 1-4](#) shows the devices that are connected to the ZXHN F670 devices.

**Figure 1-4 Entire Connection**



---

After the devices are connected to the ZXHN F670 device, press the power button. When the corresponding indicators on the front panel are ON, you can enjoy various services provided by the service provider.

# Chapter 2

## Configuration Preparation

---

This manual uses the Windows operating system as an example for describing how to configure the ZXHN F670. Before configuring the ZXHN F670, you need to perform the following operations:

- Ensure that a crossover or straight-through Ethernet cable connects a computer to the device.
- Ensure that the [TCP/IP](#) configuration on the computer is correct.
- Stop any firewall or other security software operating on the computer.
- Disable the proxy setting of Internet Explorer.

### Table of Contents

Configure TCP/IP .....	2-1
Login to the System.....	2-2

## 2.1 Configure TCP/IP

To log in to the ZXHN F670 on a computer, you need to set the IP address of the computer to ensure that the IP address of the computer and the maintenance IP address of the ZXHN F670 are in the same network segment.

### Context

The default maintenance IP address of the ZXHN F670 is as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

### Steps

1. Use an Ethernet cable to connect a local computer to the LAN interface of the ZXHN F670.
2. On the local computer, double-click **Local Area Connection** and click **Properties**. The **Local Area Connection Properties** dialog box is displayed.
3. Double-click **Internet Protocol (TCP/IP)**. The **Internet Protocol (TCP/IP) Properties** dialog box is displayed. Set the IP address to 192.168.1.200, subnet mask to 255.255.255.0, and default gateway to 192.168.1.1.
4. Click **OK**.



**Note:**

After the IP address of the computer is set, you can run the **Ping** command to ping the IP address 192.168.1.1. If the ping operation is successful, it indicates that the TCP/IP configuration is correct and the computer is properly connected to the ZXHN F670.

– End of Steps –

## 2.2 Login to the System

The ZXHN F670 provides a Web-based configuration and management system. You can enter a specified IP address in the address bar of Internet Explorer to access the system.

### Prerequisite

A computer is directly connected to the ZXHN F670, and their IP addresses are in the same network segment.

### Steps

1. Open Internet Explorer, and enter `http://192.168.1.1` (default maintenance IP address of the ZXHN F670) in the address field. Press the **Enter** key. The login page is displayed, as shown in [Figure 2-1](#).

**Figure 2-1 Login Page**

Please login to continue... 中文

Username

Password

2. Enter your username and password (the default username and password of the administrator are admin) and click **Login**. The configuration page is displayed, as shown in [Figure 2-2](#).

Figure 2-2 Configuration Page

The screenshot displays the ZTE F670 configuration interface. The top header features the ZTE logo and the model number F670. A left sidebar contains a navigation menu with options: -Status, Device Information, +Network Interface, +User Interface, VoIP Status, +Network, +Security, +Application, +Administration, and +Help. The main content area shows the path 'Path:Status-Device Information' and a table of device details. The table includes fields for Model, Serial Number, Hardware Version, Software Version, Boot Loader Version, PON Serial Number, Password, and Batch Number. The footer contains the copyright notice '©2008-2015 ZTE Corporation. All rights reserved.'

Model	F670
Serial Number	-C1027A63
Hardware Version	V1.0
Software Version	V1.0.10C4
Boot Loader Version	V1.0.10C1
PON Serial Number	ZTEGC1027A62
Password	GC12345678
Batch Number	07dfC403f8

– End of Steps –

# Chapter 3

## Status

### Table of Contents

Check the Device Information.....	3-1
Check the Network Interface .....	3-2
Check the User Interface .....	3-7
Check the VoIP Information .....	3-10

### 3.1 Check the Device Information

In the left navigation tree, click **Status > Device Information**. The **Device Information** page is displayed, as shown in [Figure 3-1](#). The device model, serial number, batch number, hardware version, software version, and so on are displayed on the page.

Figure 3-1 Device Information Page

Path:Status-Device Information

[中文](#)[Logout](#)

Model	F670
Serial Number	-C1027A63
Hardware Version	V1.0
Software Version	V1.0.10C4
Boot Loader Version	V1.0.10C1
PON Serial Number	ZTEGC1027A62
Password	GC12345678
Batch Number	07dfC403f8



**Note:**

The information displayed on the **Device Information** page in the above figure is provided for reference only.

## 3.2 Check the Network Interface

### 3.2.1 Check the WAN Connection Information

Through the **WAN Connection** menu item, you can check the status of WAN connection, including IP address, connection name and so on.

#### Steps

1. In the left navigation tree, click **Status > Network Interface**. The **WAN connection** page is displayed, as shown in [Figure 3-2](#).

Figure 3-2 WAN Connection Page

Path:Status-Network Interface-WAN Connection		<a href="#">中文</a>	<a href="#">Logout</a>
--	--	--------------------	------------------------

Type	PPPoE
Connection Name	omci_ipv4_pppoe_1
IP Version	IPv4
NAT	Enabled
IP	10.46.55.84
Subnet Mask	255.255.255.255
Gateway	10.46.55.65
DNS	10.30.1.9/10.30.1.10/0.0.0.0
IPv4 Connection Status	Connected
IPv4 Online Duration	880 sec
Disconnect Reason	None
WAN MAC	c8:9b:3a:0c:32:11

Type	DHCP
Connection Name	omci_ipv4_dhcp_2
IP Version	IPv4
NAT	Disabled
IP	10.46.32.254/255.255.255.128
Subnet Mask	255.255.255.128
Gateway	10.46.32.129
DNS	10.46.56.246/10.30.1.9/0.0.0.0
IPv4 Gateway	10.46.32.129
IPv4 Connection Status	Connected
IPv4 Disconnect Reason	None
IPv4 Online Duration	884 sec
Remaining Lease Time	166 sec
WAN MAC	c8:9b:3a:0c:32:12

- Click **Refresh** to check the latest information.

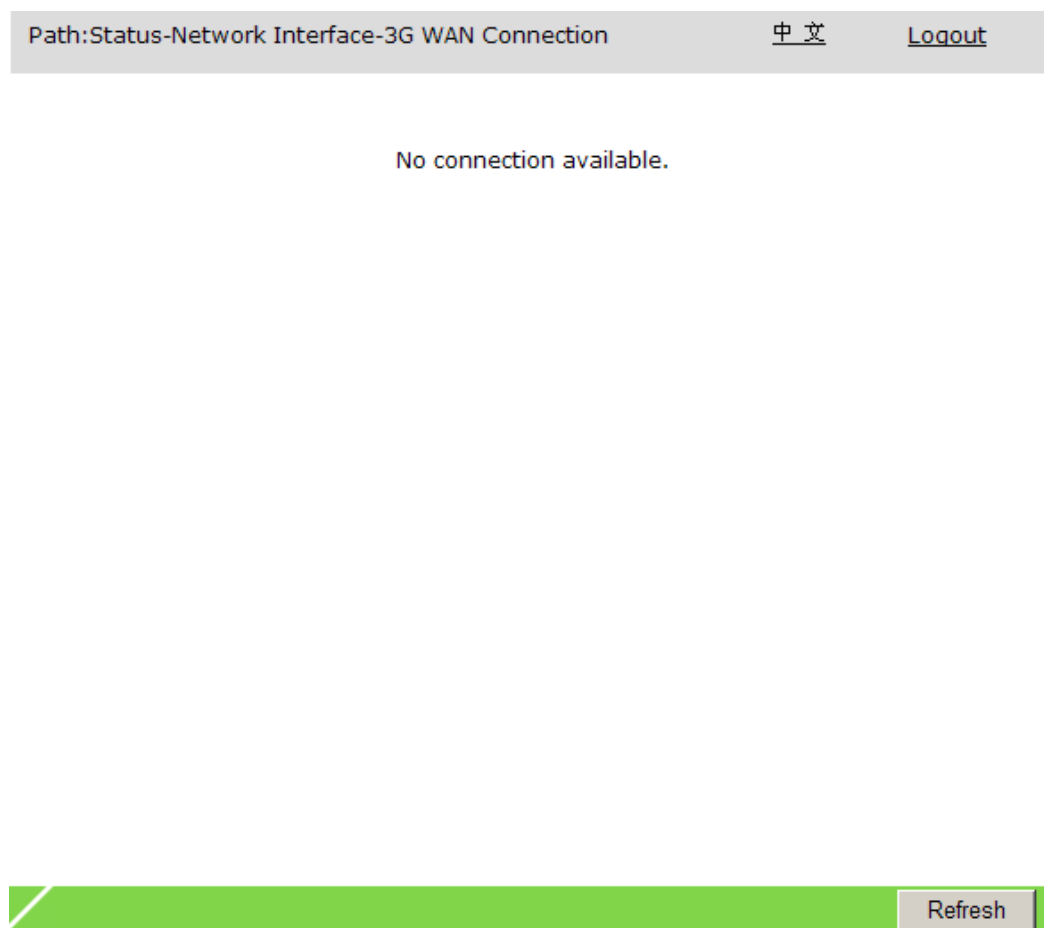
– End of Steps –

## 3.2.2 Check the 3G Connection Information

### Steps

1. In the left navigation tree, click **Status > Network Interface > 3G WAN Connection**. The **3G WAN Connection** page is displayed, as shown in [Figure 3-3](#).

**Figure 3-3 3G WAN Connection Page**



2. Click **Refresh** to check the latest information.



#### Note:

The 3G network information is displayed only if a 3G network connection is created and the ZXHN F670 is using the network connection. To create a 3G network connection, select **Network > WAN > 3G WAN Connection**.

– End of Steps –

### 3.2.3 Check the 4in6 Tunnel Connection Information

#### Steps

1. In the left navigation tree, click **Status > Network Interface > 4in6 Tunnel Connection**. The tunnel connection information is displayed, as shown in [Figure 3-4](#).

**Figure 3-4 4in6 Tunnel Connection Page**

Path:Status-Network Interface-4in6 Tunnel Connection		中文 <a href="#">Logout</a>
Tunnel Name	NET223	
Tunnel Type	ds-lite	
WAN Connection	NEW3	
Interface IPv4 Address	192.0.0.3	
AFTR	::	
Connection Status	Offline	

Refresh



#### Note:

- Click **Status > Network Interface > 6in4 Tunnel Connection** to check the 6in4 tunnel connection information.
- The tunnel information is displayed only if a tunnel is created. To create a tunnel, select **Network > WAN > 4in6 Tunnel Connection** or **6in4 Tunnel Connection**.

2. Click **Refresh** to check the latest information.

– End of Steps –

## 3.2.4 Check the PON Information

The optical module information of the ZXHN F670 includes GPON state, input power, output power, operating temperature, operating voltage, and operating current.

### Steps

1. In the left navigation tree, click **Status > Network Interface > PON Inform**. The **PON Inform** page is displayed, as shown in [Figure 3-5](#).

Figure 3-5 PON Inform Page

Path:Status-Network Interface-PON information		中文	Logout
GPON State		Operation State(o5)	
Optical Module Input Power(dBm)		-27.4	
Optical Module Output Power(dBm)		2.5	
Optical Module Supply Voltage(uV)		3295000	
Optical Transmitter Bias Current (uA)		15360	
Operating Temperature of the Optical Module(°C)		55	
		Refresh	

2. Click **Refresh** to check the latest information.

– End of Steps –

## 3.2.5 Check the Mobile Network Information

You can check the information on the 3G network connected to the ZXHN F670, including the service provider, network system (for example, GSM, WCDMA, or CDMA2000), signal strength, and **IMEI** of the card for accessing the Internet.

### Steps

1. In the left navigation tree, click **Status > User Interface > Mobile Network**. The **Mobile Network** page is displayed, as shown in [Figure 3-6](#).



Figure 3-6 Mobile Network Page

Path:Status-Network Interface-Mobile Network 中文 [Logout](#)

Service Provider(MCC/MNC)	
Network Mode	
Signal Strength	-----
IMEI	

Refresh

NOTE

**Note:**

The 3G network information is displayed only if a 3G network connection is created and the ZXHN F670 is using the network connection. To create a 3G network connection, select **Network > WAN > 3G WAN Connection**.

2. Click **Refresh** to check the latest information.

– End of Steps –

## 3.3 Check the User Interface

### 3.3.1 Check the WLAN Radio 2.4G Information

Through the **WLAN** menu item, you can check the status of the WLAN , including SSID switch status, SSID name, MAC address, packets received, packets sent and so on.

Steps

1. In the left navigation tree, click **Status > User Interface > WLAN Radio 2.4G**. The **WLAN Radio 2.4G** page is displayed, as shown in [Figure 3-7](#).

Figure 3-7 WLAN Page

Path:Status-User Interface-WLAN Radio2.4G 中文 [Logout](#)

Enable Wireless RF	Enabled
Channel	1

SSID1 Enable	Enabled
SSID1 Name	SSID1
Authentication Type	WPA/WPA2-PSK
Encryption Type	TKIP+AES
MAC Address	c8:9b:3a:0c:32:11
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	0/0
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	2754

SSID2 Enable	Disabled
--------------	----------

SSID3 Enable	Disabled
--------------	----------

SSID4 Enable	Disabled
--------------	----------

Refresh

2. Click **Refresh** to check the latest information.

**Note:**

Click **Status > User Interface > WLAN Radio 5G** to check WLAN Radio 5G information.

– End of Steps –

### 3.3.2 Check the Ethernet Information

Through the **Ethernet** menu item, you can check the operation of the LAN interfaces , including Ethernet port, the numbers of sent and received packets and error frames.

#### Steps

1. In the left navigation tree, click **Status > User Interface > Ethernet**. The **Ethernet** page is displayed, as shown in [Figure 3-8](#).

**Figure 3-8 Ethernet Page**

Path:Status-User Interface-Ethernet [中文](#) [Logout](#)

Ethernet Port	LAN1
Status	Linkup
Speed	1000M
Mode	full-duplex
Packets Received/Bytes Received	842/81742
Packets Sent/Bytes Sent	1188/1165590
Error Frames	8296006

Ethernet Port	LAN2
Status	Linkup
Speed	1000M
Mode	full-duplex
Packets Received/Bytes Received	38486/4280747352
Packets Sent/Bytes Sent	141/11485
Error Frames	0

2. Click **Refresh** to check the latest information.

– End of Steps –

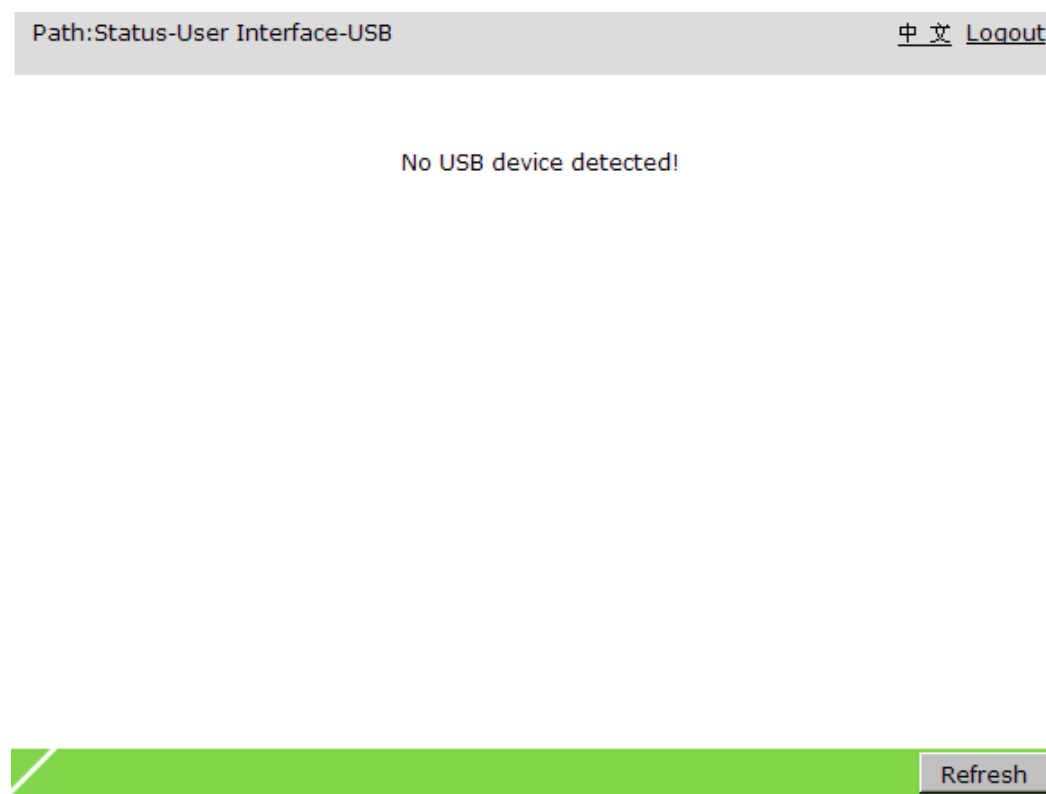
### 3.3.3 Check the USB Information

The USB information is displayed only if a USB storage device is connected to ZXHN F670 through a USB interface.

#### Steps

1. Select **Status > User Interface > USB**. The **USB** page is displayed, as shown in [Figure 3-9](#). The USB interface status is displayed on this page.

Figure 3-9 USB Page



2. Click **Refresh** to check the latest information.

– End of Steps –

## 3.4 Check the VoIP Information

The ZXHN F670 provides two Phone interfaces. If the VoIP service is configured in **WAN Connection**, you can check the VoIP operation.

## Steps

1. In the left navigation tree, click **Status > VoIP Status**. The **VoIP Status** page is displayed, as shown in [Figure 3-10](#).

**Figure 3-10 VoIP Status Page**

Path:Status-VoIP Status		<a href="#">中文</a>	<a href="#">Logout</a>
Phone	Phone1		
Register Status	Idle		
Phone	Phone2		
Register Status	Idle		

Refresh

2. Click **Refresh** to check the latest information.

– End of Steps –

# Chapter 4

## Network Configuration

---

### Table of Contents

WAN Configuration.....	4-1
WLAN Common Setting .....	4-12
WLAN Radio 2.4G(Online) Configuration .....	4-15
WLAN Radio 5G Configuration.....	4-27
LAN Configuration .....	4-38
Register .....	4-49
Route Management(IPv4) .....	4-52
Route Management(IPv6) .....	4-56
Configure the Port Locating .....	4-59

## 4.1 WAN Configuration

### 4.1.1 Configure the WAN Connection

This procedure describes how to configure a broadband connection (WAN connection) on the network side, so that user services (including the data, and video services) can be connected to the external network.

The ZXHN F670 supports PPP connection and IP connection.

#### Prerequisite

Be sure that the registration is completed successfully.

Be sure that the configuration in upper-layer OLT is completed.

#### Configuration Process

In the left navigation tree, click **Network > WAN > WAN Connection**. The **WAN Connection** page is displayed. as shown in [Figure 4-1](#).

Figure 4-1 WAN Connection Page

Path:Network-WAN-WAN Connection

中文

Logout

Connection Name

Create WAN Conn

New Connection Name

Enable VLAN

☐

Type

Route

Service List

INTERNET

MTU

1492

Link Type

PPP

PPP

Username

Password

Authentication Type

Auto

Connection Trigger

Always On

IP Version

IPv4

PPP TransType

PPPoE

IPv4

Enable NAT

☒

Create

Cancel

Table 4-1 lists the PPPoE(IPv4) process of configuring the WAN connection.

Table 4-1 PPPoE(IPv4) Configuration Process

Steps	Operations	Instructions
1	Create a new connection name.	Enter the name of the WAN connection in <b>New Connection Name</b> .
2	Enable VLAN.	The <b>VLAN ID</b> provided by carriers must be set.
3	Service List	This parameter must be consistent with service configuration.
4	Configure the <b>Link Type</b> .	Select <b>PPP</b> .
5	Configure the <b>Username</b> and <b>Password</b> .	The username and password are provided by carriers.
6	Configure the <b>IP Version</b> .	Select <b>IPv4</b> .

7	Click <b>Create</b> .	While the default settings to remaining parameters should perform well in most cases, some tuning might be required to get the best performance according to the carriers.
8	Check the configuration.	The IP address getting from carries can verify that the WAN Connection based on IPv4 was completed successfully.

Table 4-2 lists the DHCP IPv4 process of configuring the WAN connection.

**Table 4-2 DHCP IPv4 Configuration Process**

Steps	Operations	Instructions
1	Create a new connection name.	Enter the name of the WAN connection in <b>New Connection Name</b> .
2	Enable VLAN.	The <b>VLAN ID</b> provided by carriers must be set.
3	Service List	This parameter must be consistent with service configuration.
4	Configure the <b>Link Type</b> .	Select <b>IP</b> .
5	Configure the <b>IP Type</b> .	Select <b>DHCP</b> .
6	Configure the <b>IP Version</b> .	Select <b>IPv4</b> .
7	Click <b>Create</b> .	While the default settings to remaining parameters should perform well in most cases, some reconfigurations might be required to get the best performance.
8	Check the configuration.	The IP address getting from carries can verify that the WAN Connection based on IPv4 was completed successfully.

Table 4-3 lists the static IPv4 process of configuring the WAN connection.

**Table 4-3 Static IPv4 Configuration Process**

Steps	Operations	Instructions
1	Create a new connection name.	Enter the name of the WAN connection in <b>New Connection Name</b> .
2	Enable VLAN.	The <b>VLAN ID</b> provided by carriers must be set.
3	Configure the <b>Service List</b> .	This parameter must be consistent with service configuration.
4	Configure the <b>Link Type</b> .	Select <b>IP</b> .
5	Configure the <b>IP Version</b> .	Select <b>IPv4</b> .
6	Configure the <b>IP Type</b> .	Select <b>Static</b> .



7	Configure the IPv4 relevant parameters.	The mistakes of omission or commission would cause service failure. Perform the configurations according to the carriers with care.  The parameters needs to be configured, including <b>IP Address</b> , <b>Subnet Mask</b> , <b>Gateway</b> and <b>DNS Server1 IP Address</b> . <b>DNS Server2 IP Address</b> and <b>DNS Server3 IP Address</b> are optional.
8	Click <b>Create</b> .	While the default settings to remaining parameters should perform well in most cases, some reconfigurations might be required to get the best performance.

**Note:**

- WAN(IPv6) configuration process refers to WAN(IPv4) configuration process.

**Example**

This example describes how to configure static IPv4 connection.

**Steps**

1. Create a new connection name, for example "omci\_ipv4\_static\_1".
2. To enable VLAN, select this check box. Then set **VLAN ID** as '3032'.
3. Select **Route** from the **Type** drop-down list.
4. Select **INTERNET VoIP TR069** from the **Service List** drop-down list.
5. Select **IP** from the **Link Type** drop-down list.
6. Select **IPv4** from the **IP Version** drop-down list.
7. Select **Static** from the **IP Type** drop-down list. The parameters needs to be configured, including **IP Address**, **Subnet Mask** and **Gateway**.
8. Click **Create**. The **WAN Connection** page is displayed, as shown in [Figure 4-2](#).

Figure 4-2 WAN Connection Page

Path:Network-WAN-WAN Connection

[中文](#)
[Logout](#)

Connection Name
omci ipv4 static

New Connection Name
omci\_ipv4\_static\_1

Enable VLAN
☒

VLAN ID
3023

802.1p
0

Type
Route

Service List
INTERNET VoIP TR069

MTU
1500

Link Type
IP

IP Version
IPv4

IP Type
Static

IPv4

Enable NAT

☐

IP Address
10.46.42.126

Subnet Mask
255.255.255.0

Gateway
10.46.42.1

DNS Server1 IP Address

DNS Server2 IP Address

DNS Server3 IP Address

Modify

Delete

– End of Steps –

## 4.1.2 Configure the 3G WAN Connection

The ZXHN F670 supports dial-up Internet access through a 3G WAN card. You need to install the 3G WAN card on the USB interface of the ZXHN F670 and set the dial-up parameters on the **3G WAN Connection** page.

### Steps

1. In the left navigation tree, click **Network > WAN > 3G WAN Connection**. The **3G WAN Connection** page is displayed, as shown in [Figure 4-3](#).

Figure 4-3 3G WAN Connection Page

Path:Network-WAN-3G WAN Connection

[中文](#)
[Logout](#)

Connection Name

Service List

INTERNET

PDP Type

IP

APN

Dial Number

MTU

1500

Username

Password

Authentication Type

Auto

Connection Trigger

Always On

Idle Timeout

1200

sec

Create

Cancel

- Set the parameters. For a description of the parameters, refer to [Table 4-4](#).

Table 4-4 Parameter Descriptions for the 3G WAN Connection

Parameter	Description
Connection Name	To create a 3G WAN connection, enter the connection name. To query or modify an existing connection, select the corresponding connection.
Service List	Service that the device supports. Default: INTERNET.
PDP Type	The PDP protocol provides a packet data connection between a terminal and the network for IP packets switching. The PDP connections can be divided into PPP connections and IP connections. <ul style="list-style-type: none"> <li>PPP: Packet data connection is initiated through PPPoE dial-up.</li> <li>IP: A static or dynamic IP address link is used for accessing a 3G network.</li> </ul>
APN	Identifies the network of the carrier. For example, the APN for 3G WAN cards of China Unicom is 3GNET, CMNET for those of China Mobile, and CTNET for those of China Telecom.
Dial Number	Number of the 3G WAN card to be used.
MTU	Maximum Transfer Unit (MTU) of the 3G WAN connection. Default: 1500.

Parameter	Description
Username	Username of the PPPoE account. The username must be the same as that set on the peer server for authentication.
Password	Password of the PPPoE account. The password must be the same as that set on the peer server for authentication.
Authentication Type	It must be the same as that set on the peer server. Normally, it is set to <b>Auto</b> . <ul style="list-style-type: none"> <li>● <b>Auto</b>: The device automatically selects an authentication type based on the authentication types that the peer server supports.</li> <li>● <b>PAP</b>: Only the PAP type is used.</li> <li>● <b>CHAP</b>: Only the CHAP type is used.</li> </ul>
Connection Trigger	Normally, select <b>Always On</b> . Options: <ul style="list-style-type: none"> <li>● <b>Always On</b>: After the device is powered on or becomes offline, the system automatically initiates PPPoE dial-up.</li> <li>● <b>On Demand</b>: A PPPoE channel is automatically established as requested for data transmission. If the channel is idle for a particular period, it is automatically released.</li> <li>● <b>Manual</b>: You manually initiate PPPoE dial-up to establish a channel.</li> </ul>
Idle Timeout	Timeout time for dial-up access. If no connection is established within this period, a timeout message is displayed.

3. Click **Create**.

– End of Steps –

### 4.1.3 Create a 4in6 Tunnel Connection

The tunneling mechanism enables IPv4 packets to be transferred in an IPv6 tunnel, or IPv6 packets to be transferred in an IPv4 tunnel through packet encapsulation.

In the 4in6 tunneling mechanism, the ZXHN F670 supports IPv6 and the network architecture is built based on IPv6. IPv4 service traffic is borne over IPv6.

#### Steps

1. In the left navigation tree, click **Network > WAN > 4in6 Tunnel Connection**. The **4in6 Tunnel Connection** page is displayed, as shown in [Figure 4-4](#).

Figure 4-4 4in6 Tunnel Connection Page

Path:Network-WAN-4in6 Tunnel Connection

[中文](#)[Logout](#)

Tunnel Name

Create Tunnel

New Tunnel Name

Tunnel Type

ds-lite

WAN Connection

Interface IPv4 Address

Manual AFTR

☐

Create

Cancel

2. Set the parameters and click **Create**. For a description of the parameters, refer to Table 4-5.

Table 4-5 Parameter Descriptions for the 4in6 Tunnel Connection

Parameter	Description
Tunnel Name	To create a new channel, select <b>Create Tunnel</b> . To query or modify an existing tunnel, select the corresponding tunnel.
New Tunnel Name	To create a new channel, enter the channel name in the text box. If the <b>Tunnel Name</b> parameter is set to an existing tunnel, the tunnel name is displayed in the text box.
Tunnel Type	Default: ds-lite. The ds-lite option is a IPv4 to IPv6 transition technology. With ds-lite, the ZXHN F670 automatically converts IPv4 packets sent by LAN devices into IPv6 packets and then forwards them to the carrier's network.

Parameter	Description
WAN Connection	Name of the WAN connection bound with the tunnel. The IP version of the WAN connection must be IPv6.
Interface IPv4 Address	IPv4 address of an interface, range: 192.0.0.2–192.0.0.6.
Manual AFTR	Whether to obtain the fixed IPv6 address or host name of the peer end. If this check box is selected, you need to enter the corresponding IP address or host name in <b>AFTR</b> .

– End of Steps –

## 4.1.4 Create a 6in4 Tunnel Connection

The 6in4 tunnel mechanism keeps the existing network architecture that supports IPv4, and IPv6 traffic is borne over IPv4. This mechanism is applicable to a small network. An IPv6 gateway needs to be located at the core of the network, and IPv6 traffic converges at the gateway through tunnels.

### Steps

1. In the left navigation tree, click **Network > WAN > 6in4 Tunnel Connection**. The **6in4 Tunnel Connection** page is displayed, as shown in [Figure 4-5](#).

Figure 4-5 6in4 Tunnel Connection Page

Path:Network-WAN-6in4 Tunnel Connection 中文 [Logout](#)

Tunnel Name

Create Tunnel

New Tunnel Name

WAN Connection

omci ipv4 dhcp 2

MTU

1380

6in4 Tunnel Type

Manual Tunnel

Tunnel Remote Address

CreateCancel

2. Set the parameters and click **Create**. For a description of the parameters, refer to [Table 4-6](#).

**Table 4-6 Parameter Descriptions for the 6in4 Tunnel Connection**

Parameter	Description
Tunnel Name	To create a new channel, select <b>Create Tunnel</b> . To query or modify an existing tunnel, select the corresponding tunnel.
New Tunnel Name	To create a new channel, enter the channel name in the text box. If the <b>Tunnel Name</b> parameter is set to an existing tunnel, the tunnel name is displayed in the text box.
WAN Connection	Name of the WAN connection bound with the tunnel. The IP version of the WAN connection must be IPv4.
MTU	Maximum transfer unit, default: 1380.
6in4 Tunnel Type	Options include <b>Manual Tunnel</b> and <b>6rd</b> .
Tunnel Remote Address	IP address of the peer end.

– End of Steps –

## 4.1.5 Configure the Port Binding

This procedure introduces how to configure port binding. The port binding function is used to bind the LAN-side port with the WAN connection.

### Steps

1. In the left navigation tree, click **Network > WAN > Port Binding**. The **Port Binding** page is displayed, as shown in [Figure 4-6](#).

Figure 4-6 Port Binding Page

Path:Network-WAN-Port Binding

中文Logout

WAN Connectionomci ipv4 pppoe 1

☐ LAN1

☐ LAN2

☐ LAN3

☐ LAN4

☐ SSID1

☐ SSID2

☐ SSID3

☐ SSID4

☐ SSID5

☐ SSID6

☐ SSID7

☐ SSID8

Submit

Cancel

2. Select the check box to bind ports, and click **Submit**. For a description of the parameters, refer to [Table 4-7](#).

Table 4-7 Port Binding Parameter Descriptions

Parameter	Description
WAN Connection	Select a WAN connection.
LAN	Select one or more LANs. Options: LAN1~LAN4.
SSID	Select one or more SSIDs. Options: SSID1~SSID4.
WDS	Select one or more WDSs. Options: WDS1~WDS4.

– End of Steps –



## 4.1.6 Configure the DHCP Release

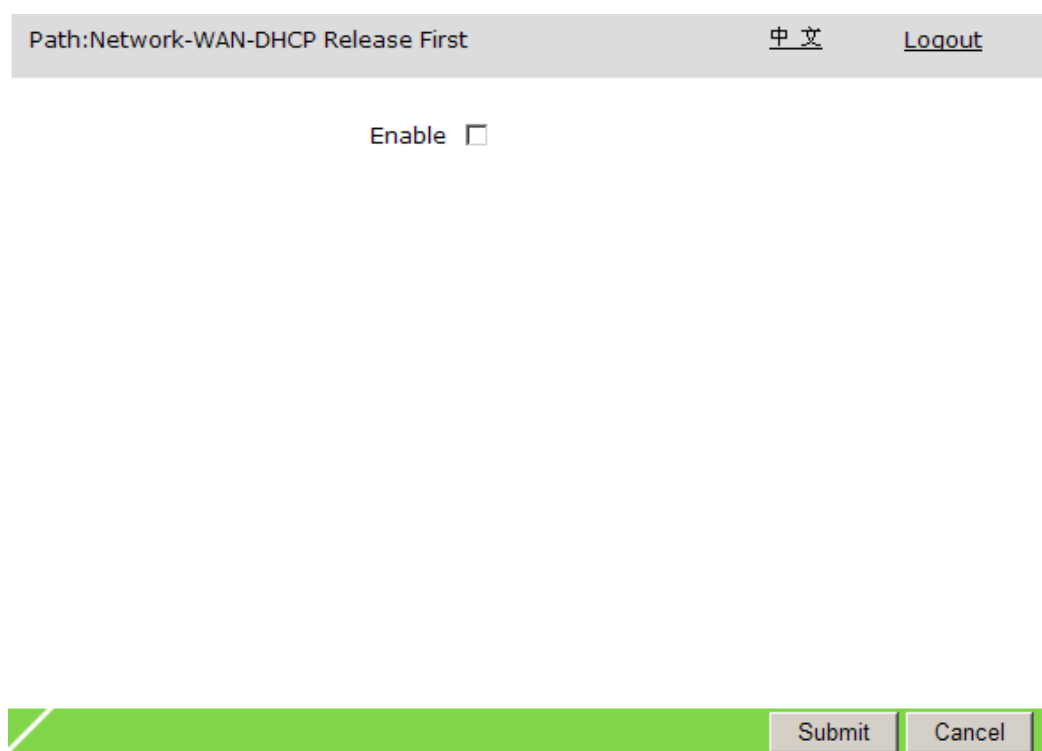
The DHCP release function takes effect only after the ZXHN F670 is restarted.

After the ZXHN F670 is started up, it initiates a Release packet to release the IP address obtained from the DHCP server the last time. Then, the ZXHN F670 starts the flow of obtaining its address in DHCP mode and obtains a new IP address.

### Steps

1. In the left navigation tree, click **Network > WAN > DHCP Release First**. The **DHCP Release First** page is displayed, as shown in [Figure 4-7](#).

Figure 4-7 DHCP Release First Page



2. To enable the DHCP release function, select **Enable** and click **Submit**.

– End of Steps –

## 4.2 WLAN Common Setting

### 4.2.1 Configure the WiFi Restrictions

#### Steps

1. In the left navigation tree, click **Network > WLAN Common Settings**. The **WiFi Restrictions** page is displayed by default, as shown in [Figure 4-8](#).

Figure 4-8 WiFi Restrictions Page

Path:Network-WLAN Common Setting-WiFi Restrictions

中文Logout

NOTE:  
If scheduled RF control is enabled, all WLAN Radios will be controlled, and when network time synchronization fails, all WLAN Radios will be enabled by default.

Enable Scheduled RF Control☐

Off Time00:00(hh:mm)  
On Time06:00(hh:mm)

SubmitCancel

2. Set the parameters and click **Submit**. For a description of the parameters, refer to Table 4-8.

Table 4-8 WiFi Restrictions Parameter Descriptions

Parameter	Description
Scheduled RF Mode	Only if the "Wireless RF Mode" is "Scheduled", the WiFi restrictions function works.
Off Time	This feature will be turned off since this time.
On time	This feature will be turned on since this time.



**Note:**

- If scheduled RF control is enabled, all WLAN Radios will be controlled, and when network time synchronization fails, all WLAN Radios will be enabled by default.

– End of Steps –

## 4.2.2 Configure the Setting Deleting

### Steps

1. In the left navigation tree, click **Network > WLAN Common Settings > Setting Deleting**. The **Setting Deleting** page is displayed by default, as shown in [Figure 4-9](#).

**Figure 4-9 Setting Deleting Page**

Path:Network-WLAN Common Setting-Setting Deleting 中文 [Logout](#)

There doesn't exist offline settings.

Card Selectable Wireless Mode	
Current Wireless Mode	
Band Surpported	
Auto Channel Selection	
Transmitting Power	

Delete

Refresh

2. Click **Refresh** to check the latest information.

3. (Optional) To delete a offline setting, click **Delete**.

– End of Steps –

## 4.3 WLAN Radio 2.4G(Online) Configuration

### 4.3.1 Configure the WLAN Basic Configuration(2.4G)

This procedure describes how to configure the WLAN operation conditions.

#### Steps

1. In the left navigation tree, click **Network > WLAN Radio2.4G > Basic**. The **Basic** page is displayed, as shown in [Figure 4-10](#).

**Figure 4-10 Basic Page**

Path:Network-WLAN Radio2.4G-Basic 中文 [Logout](#)

Enable Wireless RF ☐

Enable Isolation ☐

Mode

Band Width

Channel

SIG Enable ☐

Beacon Interval  ms

Transmitting Power

QoS Type

RTS Threshold

DTIM Interval

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-9](#).

**Table 4-9 Parameter Descriptions for WLAN Basic Configuration**

Parameter	Description
Enable Wireless RF	If this check box is selected, the wireless RF feature is enabled.
Enable Isolation	If this check box is selected, the <a href="#">SSID</a> isolation feature is enabled, so that users under different SSIDs cannot connect with each other.
Mode	Options: <ul style="list-style-type: none"> <li>● IEEE 802.11b Only</li> <li>● IEEE 802.11g Only</li> <li>● IEEE 802.11n Only</li> <li>● Mixed(802.11b+802.11g)</li> <li>● Mixed(802.11g+802.11n)</li> <li>● Mixed(802.11b+802.11g+802.11n)</li> </ul>
Band Width	Radio frequency bandwidth, including Auto, 20Mhz and 40Mhz. Default: 20MHz.
Channel	Channel of the wireless network. A proper channel can be selected in accordance with the country code. Options: Auto, 1–13, default: Auto. Specifies the channel used for communication between the AP and the wireless site, depending on the local circumstance.
SGI Enable	Enable or disable <a href="#">SGI</a> .
Beacon Interval	Interval for transmitting beacon frames, default: 100 ms. Beacon frames are used for communicating with other AP devices or network control devices to announce the WLAN presence.
Transmitting Power	Level of radio signal transmitting power. A larger value indicates wider coverage. Options: <ul style="list-style-type: none"> <li>● 100%</li> <li>● 80%</li> <li>● 60%</li> <li>● 40%</li> <li>● 20%</li> </ul>
QoS Type	Options: <ul style="list-style-type: none"> <li>● Disabled Disables QoS.</li> <li>● <a href="#">WMM</a> QoS control in compliance with the WMM standard. The voice service has the highest priority, followed by the IPTV service, Internet service, and other services.</li> <li>● SSID QoS is implemented in accordance with the SSID priority. If SSID is selected, the priority of each SSID must be specified.</li> </ul>

Parameter	Description
RTS Threshold	The Request To Send ( <a href="#">RTS</a> ) threshold is used in a wireless network to avoid data transmission failure. A smaller RTS threshold means a higher frequency of RTS packet transmission, where the system can be recovered more quickly. However, larger bandwidth is required.
DTIM Interval	Interval of <a href="#">DTIM</a> transmission.

3. Click **Submit**.

– End of Steps –

## 4.3.2 Configure the SSID(2.4G)


An [SSID](#) identifies a wireless network. The ZXHN F670 supports a maximum of four SSIDs. You can set the name for each SSID and specify whether to enable the SSID.

### Steps

1. In the left navigation tree, click **Network > WLAN Radio2.4G > SSID Settings**. The **SSID Settings** page is displayed, as shown in [Figure 4-11](#).

Figure 4-11 SSID Settings Page

Path:Network-WLAN Radio2.4G-SSID Settings 中文 [Logout](#)

 This page can not be configured while WLAN is off.

Choose SSID

Hide SSID ☐

Enable SSID ☒

Enable SSID Isolation ☐

Maximum Clients  (1 ~ 32)

SSID Name  (1 ~ 32 characters)

Priority

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-10](#).

Table 4-10 SSID Parameter Descriptions

Parameter	Description
Choose SSID	Select an SSID to be configured. Options: SSID1–SSID4.
Hide SSID	If this check box is selected, it indicates that the SSID broadcast feature is disabled. If an SSID is hidden, wireless terminals cannot view the network through search. To access the network, terminals must send requests.
Enable SSID	Select the check box to enable the corresponding wireless network. Clear the check box to disable the corresponding wireless network.

Parameter	Description
Enable SSID Isolation	If this check box is selected, the SSID isolation feature is enabled, so that users under the same SSID cannot connect with each other.
Maximum Clients	Maximum number of wireless terminals that can connect to the SSID, range: 1–32.
SSID Name	Name of the SSID, range: 1–32 characters. Space and tab are not allowed.
Priority	Priority of the SSID, range: 0–7. Default: 0, which means that no priority is specified. The larger the value, the higher the priority.

3. Click **Submit** to apply the changes.

**Note:**

This page can not be configured while WLAN is off.

– End of Steps –

### 4.3.3 Configure the WLAN Security(2.4G)


#### Steps

1. In the left navigation tree, click **Network > WLAN Radio2.4G > Security**. The **Security** page is displayed, as shown in [Figure 4-12](#).



Figure 4-12 WLAN Security Page

Path:Network-WLAN Radio2.4G-Security 中文 [Logout](#)

 This page can not be configured while WLAN is off.

Choose SSID

SSID1

Authentication Type

WPA/WPA2-PSK

WPA Passphrase

!@#\$%12345 (8 ~ 63 characters)

WPA Encryption Algorithm

TKIP+AES

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-11](#).

Table 4-11 WLAN Security Parameter Descriptions

Parameter	Description
Choose SSID	Select an SSID to be configured. Options: SSID1–SSID4.
Authentication Type	Each SSID supports multiple authentication methods, including Open System, Shared Key, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK.
WPA Passphrase	Authentication password for wireless terminals to access the wireless network, range: 8–63 characters.
WPA Encryption Algorithm	Options: <a href="#">AES</a> , <a href="#">TKIP</a> , and AES+TKIP.

- Click **Submit** to apply the changes.

**Note:**

This page can not be configured while WLAN is off.

– End of Steps –

### 4.3.4 Access the Control List(2.4G)

By enabling the WLAN access control feature and configuring access control list, you can control the WLAN access. If the **Mode** parameter is set to **Block** for an ACL, terminals not specified in the ACL can access the SSID. If the **Mode** parameter is set to **Permit**, only the terminals specified in the ACL can access the SSID.

#### Steps

- In the left navigation tree, click **Network > WLAN Radio2.4G > Access Control List**. The **Access Control List** page is displayed, as shown in [Figure 4-13](#).

**Figure 4-13 Access Control List Page**

- Set the parameters. For a description of the parameters, refer to [Table 4-12](#).

**Table 4-12 Access Control List Parameter Descriptions**

Parameter	Description
Choose SSID	Select an SSID to be configured. Options: SSID1–SSID4.

Parameter	Description
Mode	Options: <ul style="list-style-type: none"><li>● Disabled (default): SSID access control is disabled.</li><li>● Block: Terminals with specified MAC addresses cannot access the network.</li><li>● Permit: Only the terminals with specified MAC addresses can access the network.</li></ul>
MAC Address	MAC address of a terminal that accesses the WLAN. You can click <b>Add</b> to set multiple MAC addresses.

**Note:**

This page can not be configured while WLAN is off.

– End of Steps –

### 4.3.5 Check the Associated Devices(2.4G)

You can check the IP addresses and MAC addresses of devices that are associated with each SSID.

#### Steps


1. In the left navigation tree, click **Network > WLAN Radio2.4G > Associated Devices**. The **Associated Devices** page is displayed, as shown in [Figure 4-14](#).

Figure 4-14 Associated Devices Page

Path:Network-WLAN-Associated Devices

中文

Logout



This page can not be configured while WLAN is off.

Choose SSID

SSID1

MAC Address	IP Address	MCS	RSSI	TxRate (kbps)	RxRate (kbps)	STA Mode
There is no data.						

Refresh

- 2. Select an SSID from the **SSID** list, and click **Refresh**. The IP addresses and MAC addresses of the associated devices are displayed.

NOTE

**Note:**  
This page can not be configured while WLAN is off.

– End of Steps –

### 4.3.6 Configure the WMM(2.4G)

The section describes how to configure the WMM.


Steps

- 1. On the main page of the ZXHN F670, select **Network > WLAN Radio2.4G > WMM** to go to the **WMM**( page, as shown in [Figure 4-15](#).

Figure 4-15 WMM Configuration Page

Path:Network-WLAN-WMM

中文Logout

 This page can not be configured while WLAN is off.

Choose AC

BE

AIFSN

3

(2 ~ 15)

ECWMin

4

(0 ~ 15)

ECWMax

10

(0 ~ 15)

TXOP

0

(0 ~ 255)

Qlength

256

(0 ~ 1000)

SRL

7

(0 ~ 255)

LRL

4

(0 ~ 255)

Submit

Cancel

- 2. Set the parameters. For a description of the parameters, refer to[Table 4-13](#).

Table 4-13 WMM Parameter Descriptions

Parameter	Description
Choose AC	AC the device supporting, including: VO, VI, BE and BK.
AIFSN	Arbitration Inter Frame Space Number.
ECWMin/ECWMax	Exponent of Contention Window.
TXOP	Transmission Opportunity.

---

Parameter	Description
Qlength	The queue size value.
SRL	A short retry counter.
LRL	A long retry counter.

3. Click **Submit** button to apply the changes.



**Note:**

This page can not be configured while WLAN is off.

---

– End of Steps –

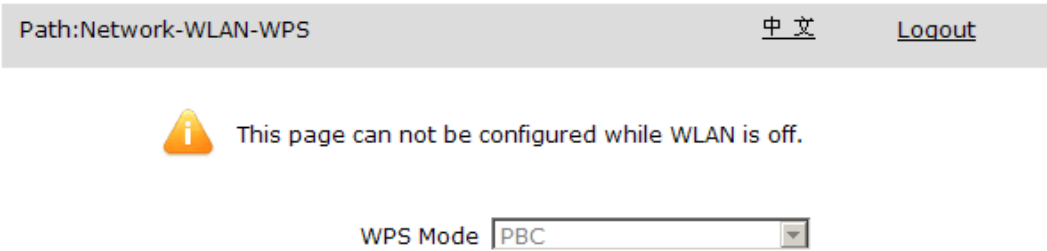
### 4.3.7 Configure the WPS(2.4G)

This procedure describes how to configure [WPS](#) parameters. Normally, the WPS parameters do not need to be modified. If the WPS feature is enabled, terminals such as PCs and handsets can access a WLAN by negotiating with the ONU. Users do not need to search for SSIDs or enter passwords.

#### Steps

1. In the left navigation tree, click **Network > WLAN Radio2.4G > WPS**. The **WPS** page is displayed, as shown in [Figure 4-16](#).

Figure 4-16 WPS Page



2. Set the parameter. For a description of the parameter, refer to [Table 4-14](#).

Table 4-14 WPS Parameter Description

Parameter	Description
WPS Mode	<p>This parameter takes effect immediately after an option is selected.</p> <p>Options:</p> <ul style="list-style-type: none"><li>● PBC: To enable the WPS feature, you must press the <b>WPS</b> button on the ZXHN F670.</li><li>● Disabled: disables the WPS feature.</li></ul>

**Note:**

The WPS mode switching takes effect immediately after an option is selected.

---

– End of Steps –

## 4.4 WLAN Radio 5G Configuration

### 4.4.1 Configure the Basic Parameters(5G)

This procedure introduces how to configure basic parameters of the WLAN radio 5G(Online).

**Steps**

1. Select **Network > WLAN Radio5G > Basic**. The **Basic** page is displayed, as shown in [Figure 4-17](#).



Figure 4-17 Basic Parameters Configuration(5G) Page

Path:Network-WLAN Radio5G-Basic

中文Logout

Enable Wireless RF☒

Enable Isolation☐

ModeMixed(802.11a+802.11n+802.11ac)

Band Width80MHz

ChannelAuto

SIG Enable☒

Beacon Interval100ms

Transmitting Power100%

QoS TypeWMM

RTS Threshold2347

DTIM Interval1

SubmitCancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-15](#).

Table 4-15 Basic Configuration(5G) Parameter Descriptions

Parameter	Description
Enable Wireless RF	To enable the wireless feature, select this check box <sup>RF</sup> .
Enable Isolation	If this check box is selected, the SSID isolation feature is enabled, so that users under different SSIDs cannot connect with each other.
Mode	Options: <ul style="list-style-type: none"><li>IEEE 802.11a Only</li><li>IEEE 802.11n Only</li><li>Mixed(802.11a+802.11n)</li><li>Mixed(802.11a+802.11n+802.11ac)</li></ul>

Parameter	Description
Country/Region	Country or region where the device is located.
Band Width	Radio frequency bandwidth, default: 80MHz. including: Auto, 20MHz, 40MHz, 80MHz.
Channel	Channel of the wireless network. A proper channel can be selected in accordance with the country code. Default: Auto. Specifies the channel used for communication between the AP and the wireless site, depending on the local circumstance.
SGI Enable	To enable the <a href="#">SGI</a> feature, select this check box.
Beacon Interval	Interval for transmitting beacon frames, default: 100 ms. Beacon frames are used for communicating with other AP devices or network control devices to announce the WLAN presence.
Transmitting Power	Level of radio signal transmitting power. A larger value indicates wider coverage. Options: <ul style="list-style-type: none"> <li>● 100%</li> <li>● 80%</li> <li>● 60%</li> <li>● 40%</li> <li>● 20%</li> </ul>
QoS Type	Options: <ul style="list-style-type: none"> <li>● Disabled Disables QoS.</li> <li>● <a href="#">WMM</a> QoS control in compliance with the WMM standard. The voice service has the highest priority, followed by the IPTV service, Internet service, and other services.</li> <li>● SSID QoS is implemented in accordance with the SSID priority. If SSID is selected, the priority of each SSID must be specified.</li> </ul>
RTS Threshold	The request to send ( <a href="#">RTS</a> ) threshold is used in a wireless network to avoid data transmission failure. A smaller RTS threshold means a higher frequency of RTS packet transmission, where the system can be recovered more quickly. However, larger bandwidth is required.
DTIM Interval	Interval of <a href="#">DTIM</a> transmission.

3. Click **Submit**.

– End of Steps –

## 4.4.2 Configure the SSID(5G)

A [SSID](#)(5G) identifies a wireless network. The ZXHN F670 supports a maximum of four SSIDs(5G). You can set the name for each SSID(5G) and specify whether to enable the SSID(5G).

### Steps

1. Select **Network > WLAN Radio 5G > SSID Settings**. The **SSID Settings**( page is displayed, as shown in [Figure 4-18](#).

**Figure 4-18 SSID Settings(5G) Page**

Path:Network-WLAN Radio5G-SSID Settings [中文](#) [Logout](#)

Choose SSID SSID5

Hide SSID ☐

Enable SSID ☒

Enable SSID Isolation ☐

Maximum Clients  (1 ~ 32)

SSID Name  (1 ~ 32 characters)

Priority 0

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-16](#).

**Table 4-16 SSID Settings(5G) Parameter Descriptions**

Parameter	Description
Choose SSID	Select an SSID to be configured. Options: SSID5~SSID8.
Hide SSID	If this check box is selected, it indicates that the SSID broadcast feature is disabled. If an SSID is hidden, wireless terminals cannot view the network through search. To access the network, terminals must send requests.
Enable SSID	To enable the SSID feature, select this check box.
Enable SSID Isolation	If this check box is selected, the SSID isolation feature is enabled, so that users under the same SSID cannot connect with each other.
Maximum Clients	Maximum number of wireless terminals that can connect to the SSID, range: 1~32.
SSID Name	Name of the SSID, range: 1~32 characters. Space and tab are not allowed.
Priority	Priority of the SSID, range: 0~7. Default: 0, which means that no priority is specified. A higher number indicates a higher priority.

3. Click **Submit**.

– End of Steps –

### 4.4.3 Configure the WLAN Security(5G)

The section describes how to configure the security(5G).

#### Steps

1. Select **Network > WLAN Radio 5G > Security**. The **Security** page is displayed, as shown in [Figure 4-19](#).

Figure 4-19 Security(5G) Page

Path:Network-WLAN Radio5G-Security 中文 [Logout](#)

Choose SSID

SSID5

Authentication Type

WPA/WPA2-PSK

WPA Passphrase

!@#\$%12345 (8 ~ 63 characters)

WPA Encryption Algorithm

TKIP+AES

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-17](#).

Table 4-17 Security(5G) Parameter Descriptions

Parameter	Description
Choose SSID	Select a SSID to be configured. Options: SSID5~SSID8.
Authentication Type	Options: Open System, Shared Key, WPA-PSK, WPA2-PSK and WPA/WPA2-PSK.
WPA Passphrase	Authentication password for wireless terminals to access the wireless network, range: 8~63 characters.
WPA Encryption Algorithm	Options: AES, TKIP and TKIP+AES.

3. Click **Submit**.
- End of Steps –

4.4.4 Access the Control List(5G)

By enabling the WLAN access control feature and configuring ACLs, you can control the WLAN access. If the **Mode** parameter is set to **Block** for an ACL, terminals not specified in the ACL can access the SSID. If the **Mode** parameter is set to **Permit**, only the terminals specified in the ACL can access the SSID.


Steps

1. Select **Network > WLAN Radio 5G > Access Control List**. The **Access Control List** page is displayed, as shown in [Figure 4-20](#).

Figure 4-20 Access Control List(5G) Page

Path:Network-WLAN Radio5G-Access Control List

[中文](#)[Logout](#)

 Mode switching will take effect immediately.

Choose SSID

SSID5

Mode

Disabled

MAC Address

:

:

:

:

:

:

Add

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

2. Set the parameters and click **Add** . For a description of the parameters, refer to [Table 4-18](#).

Table 4-18 Access Control List(5G) Parameter Descriptions

Parameter	Description
Choose SSID	Select an SSID to be configured. Options: SSID5–SSID8.
Mode	Options: <ul style="list-style-type: none"><li>● <b>Disabled</b> (default): SSID access control is disabled.</li><li>● <b>Block</b>: Terminals with specified MAC addresses cannot access the network.</li><li>● <b>Permit</b>: Only the terminals with specified MAC addresses can access the network.</li></ul>

4-33

SJ-20151016170048-003|2015-11-10 (R1.0)

ZTE Proprietary and Confidential

---

Parameter	Description
MAC Address	MAC address of a terminal that accesses the WLAN.

– End of Steps –

## 4.4.5 Check the Associated Devices(5G)

You can check the IP addresses and MAC addresses of devices that are associated with each SSID.

### Steps

1. Select **Network > WLAN Radio 5G > Associated Devices**. The **Associated Devices** page is displayed, as shown in [Figure 4-21](#).

Figure 4-21 Associated Devices(5G) Page

Path:Network-WLAN Radio5G-Associated Devices 中文 [Logout](#)

Choose SSID SSID5

MAC Address	IP Address	MCS	RSSI	TxRate (kbps)	RxRate (kbps)	STA Mode
There is no data.						

Refresh

- 2. Select an SSID from the **SSID** list, and click **Refresh**. The IP addresses and MAC addresses of the associated devices( 5G) are displayed.

– End of Steps –

### 4.4.6 Configure the WMM(5G)

The section describes how to configure WMM.

#### Steps

- 1. On the main page of the ZXHN F670, select **Network > WLAN Radio 5G > WMM** to go to the **WMM(5G)** page, as shown in [Figure 4-22](#).



### Figure 4-22 WMM Configuration Page

Path:Network-WLAN Radio5G-WMM

中文Logout

Choose AC

BE

AIFSN

3

(2 ~ 15)

ECWMin

4

(0 ~ 15)

ECWMax

10

(0 ~ 15)

TXOP

0

(0 ~ 255)

Qlength

256

(0 ~ 1000)

SRL

7

(0 ~ 255)

LRL

4

(0 ~ 255)

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-19](#).

### Table 4-19 WMM Parameter Descriptions

Parameter	Description
Choose AC	AC the device supporting, including: VO, VI, BE and BK.
AIFSN	Arbitration Inter Frame Space Number.
ECWMin/ECWMax	Exponent of Contention Window.
TXOP	Transmission Opportunity.
Qlength	The queue size value.
SRL	A short retry counter.
LRL	A long retry counter.

3. Click **Submit** button to apply the changes.

– End of Steps –

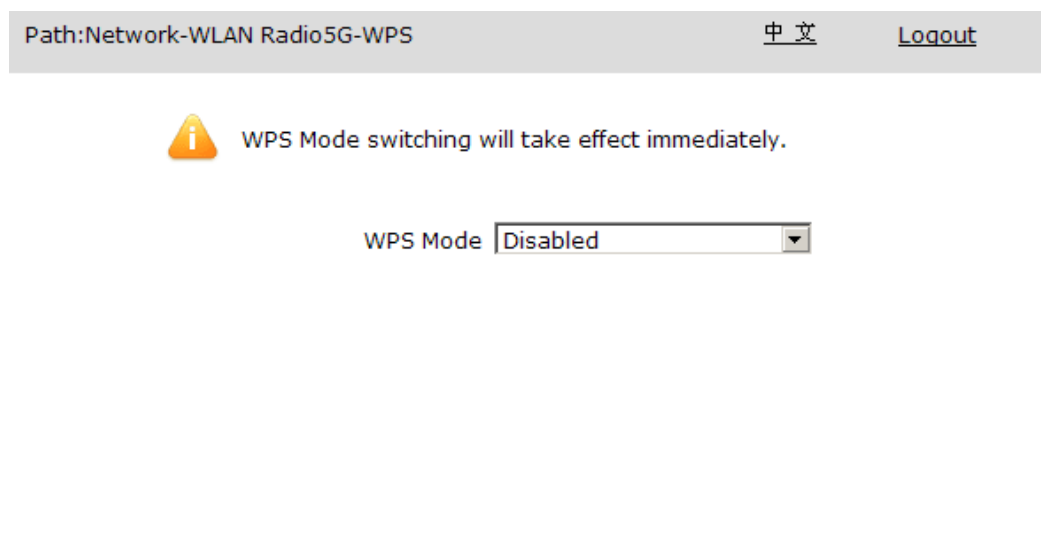
## 4.4.7 Configure the WPS(5G)

This procedure describes how to configure [WPS\(5G\)](#) parameters. Normally, the WPS(5G) parameters do not need to be modified. If the WPS(5G) feature is enabled, terminals such as PCs and handsets can access a WLAN by negotiating with the ONU. Users do not need to search for SSIDs or enter passwords.


### Steps

1. Select **Network > WLAN Radio 5G > WPS**. The **WPS** page is displayed, as shown in [Figure 4-23](#).

**Figure 4-23 WPS Page**



Path:Network-WLAN Radio5G-WPS [中文](#) [Logout](#)

 WPS Mode switching will take effect immediately.

WPS Mode

2. Set the parameters. For a description of the parameters, refer to [Table 4-20](#).

**Table 4-20 WPS Parameter Descriptions**

Parameter	Description
WPS Mode	<ul style="list-style-type: none"><li>● PBC : Press the WPS button on the panel to enable the WPS function.</li><li>● Disable: Disable the WPS function.</li></ul>

**Note:**

The WPS mode switching takes effect immediately after an option is selected.

– End of Steps –

## 4.5 LAN Configuration

### 4.5.1 Configure the DHCP Server

This procedure describes how to configure the IP address and subnet mask of the ZXHN F670 and enable the DHCP server feature, so that the ZXHN F670 can allocate dynamic IPv4 addresses to devices connected to the system.

#### Steps

1. In the left navigation tree, click **Network > LAN > DHCP Server**. The **DHCP Server** page is displayed, as shown in [Figure 4-24](#).

Figure 4-24 DHCP Server Page

Path:Network-LAN-DHCP Server

中文

Logout

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

LAN IP Address

192.168.1.1

Subnet Mask

255.255.255.0

Enable DHCP Server

☒

DHCP Start IP Address

192.168.1.2

DHCP End IP Address

192.168.1.254

Assign IspDNS

☐

DNS Server1 IP Address

192.168.1.1

DNS Server2 IP Address

DNS Server3 IP Address

Default Gateway

192.168.1.1

Lease Time

86400

sec

Allocated Address

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

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-21](#).

Table 4-21 DHCP Server Parameter Descriptions

Parameter	Description
LAN IP Address/Subnet Mask	IP address/subnet mask of the ZXHN F670. The device IP address should be in the same network segment as the DHCP address pool.
Enable DHCP Server	Select the <b>Enable DHCP Server</b> check box to let the device work as a DHCP server and assign IP addresses to the client PCs.
DHCP Start IP Address/DHCP End IP Address	Start/end IP address in the DHCP server address pool, which must be in the same network segment as the IP address of the ZXHN F670.
Assign DNS	Select this option to let the <a href="#">DNS</a> provided by the ISP to assign IP addresses to the client PCs.

Parameter	Description
DNS Server1 IP Address	IP address of the default DNS server, which means the IP address of the ZXHN F670.
DNS Server2 IP Address	IP address of a DNS server provided by the service provider.
DNS Server3 IP Address	IP address of a DNS server provided by the service provider.
Default Gateway	IP address of the ZXHN F670.
Lease Time	The time during which the client PCs use the IP addresses assigned by the DHCP server. After the lease time expires, the private IP address will be available for assigning to other network devices. Default: 86400 seconds

**Note:**

IP addresses are automatically assigned to the user-side PCs and wireless devices that are connected to the ZXHN F670.

3. Click **Submit**.

– End of Steps –

## 4.5.2 Configure the DHCP Server(IPv6)

This procedure describes how to configure the dynamic IPv6 address of the ZXHN F670 and enable the DHCP feature. For a family gateway, the IP address is also the gateway address of the subnet on the LAN side.

### Steps

1. In the left navigation tree, click **Network > LAN > DHCP Server(IPv6)**. The **DHCP Server(IPv6)** page is displayed, as shown in [Figure 4-25](#).

Figure 4-25 DHCP Server(IPv6) Page

Path:Network-LAN-DHCP Server(IPv6) 中文 [Logout](#)

LAN IP Address  /

Enable DHCP Server ☒

DNS Refresh Time  sec

Allocated Address

DUID	IP Address	Remaining Lease Time
There is no data.		

SubmitCancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-22](#).

Table 4-22 DHCP Server(IPv6) Parameter Descriptions

Parameter	Description
LAN IP Address	IPv6 address of the ZXHN F670.
Enable DHCP Server	To enable the DHCP server feature, select this check box.
DNS Refresh Time	<a href="#">DNS</a> update time, range: 60–864000, default: 86400, unit: seconds.

3. Click **Submit**.
- End of Steps –

### 4.5.3 Configure the DHCP Binding

This procedure describes how to configure a static IP address for a device connected to the system and bind the IP address with the MAC address to prevent access of illegal users.

#### Steps

1. In the left navigation tree, click **Network > LAN > DHCP Binding**. The **DHCP Binding** page is displayed, as shown in [Figure 4-26](#).

**Figure 4-26 DHCP Binding Page**

Path: Network-LAN-DHCP Binding      中文      Logout

IP Address

MAC Address  :  :  :  :  :

Add

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

2. Set the **IP Address** and **MAC Address** text boxes, and click **Add**.



#### Note:

Only IPv4 addresses are supported.

3. (Optional) To modify a configuration record, click next to the record.
4. (Optional) To delete a configuration record, click next to the record.

– End of Steps –

### 4.5.4 Configure the DHCP Port Service

#### Steps


1. In the left navigation tree, click **Network > LAN > DHCP Port Service**. The **DHCP Port Service** page is displayed, as shown in [Figure 4-27](#).

Figure 4-27 DHCP Port Service Page

Path:Network-LAN-DHCP Port Service

中文

Logout



DEFAULT is not to control DHCP mode.LAN is only get address from onu.WAN is only get address from internet.

Port	Dhcp Mode
LAN1	Default
LAN2	Default
LAN3	Default
LAN4	Default
SSID1	Default
SSID2	Default
SSID3	Default
SSID4	Default
SSID5	Default
SSID6	Default
SSID7	Default
SSID8	Default

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-23](#).

Table 4-23 DHCP Port Service Parameter Descriptions

Parameter	Description
DHCP Mode	DHCP mode includes: <ul style="list-style-type: none"><li>● Default: not to control DHCP mode.</li><li>● LAN : get address from ZXHN F670.</li><li>● WAN: get address from internet.</li></ul>

3. Click **Submit**.

– End of Steps –



## 4.5.5 Configure the Static Prefix

This procedure describes how to configure a static prefix and set the type of the server (RA or DHCPv6) that delegates the IPv6 prefix to devices on the LAN side.

### Steps

1. In the left navigation tree, click **Network > LAN > Prefix Management**. The **Prefix Management** page is displayed, as shown in Figure 4-28.

Figure 4-28 Prefix Management Page

Path:Network-LAN-Prefix Management

中文
Logout

WAN Connection
Prefix Source
Prefix
Preferred Lifetime
Valid Lifetime
Prefix Delegation
☐ RA
☐ DHCPv6

WAN Connection	Prefix Source	Prefix	Preferred/Valid Lifetime	Prefix Delegation	Modify
There is no data.					

2. For a description of the parameters, refer to Table 4-24.

Table 4-24 Prefix Management Parameter Descriptions

Parameter	Description
WAN Connection	If the prefix delegation function of the IPv6 WAN connection is enabled, the WAN connection name is displayed in the text box.
Prefix Source	Prefix source corresponds to the parameter <b>Prefix Delegation From</b> in <b>Network &gt; WAN &gt; WAN Connection</b> .
Prefix	IPv6 address and prefix length. Only a GUA prefix is supported. Prefix length range: 48–64.
Preferred Lifetime	Preferred lifetime of the prefix.
Valid Lifetime	Valid period of the prefix. This parameter must be equal to or greater than the <b>Preferred Lifetime</b> parameter.

Parameter	Description
Prefix Delegation	Only <b>Prefix Delegation</b> can be configured, after IPv6 WAN connection is available. <ul style="list-style-type: none"><li>● RA: The IPv6 prefix is delegated by an RA server.</li><li>● DHCPv6: The IPv6 prefix is delegated by a DHCPv6 server.</li></ul>

3. (Optional) To modify a configuration record, click  next to the record.

– End of Steps –

## 4.5.6 Configure the DHCP Port Service (IPv6)


This procedure describes how to disable the DHCPv6 and RA services for each LAN interface and SSID port on the user side.

### Steps

1. In the left navigation tree, click **Network > LAN > DHCP Port Service(IPv6)**. The **DHCP Port Service(IPv6)** page is displayed, as shown in [Figure 4-29](#).

Figure 4-29 DHCP Port Service(IPv6) Page

Path:Network-LAN-DHCP Port Service(IPv6) 中文 [Logout](#)

 The IPv6 address assign service will be opened on the port which is checked.The Router Advertisement will be opened on the port which is checked.

LAN1	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
LAN2	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
LAN3	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
LAN4	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID1	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID2	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID3	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID4	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID5	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID6	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID7	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA
SSID8	<input checked="" type="checkbox"/> DHCPv6	<input checked="" type="checkbox"/> RA

Submit

Cancel

2. Configure the port control parameters. [Table 4-25](#) lists the port control parameters.

Table 4-25 DHCP Port Service(IPv6) parameters

Parameter	Description
DHCPv6	A board assigns GUA, DNS, PD and so on to the LAN side through dhcpv6 messages.
RA	A board assigns DNS, PD and so on to the LAN side through icmpv6 messages.

**Note:**

- Click **All On** to select all IPv6 Service-Port control types.
- Click **All Off** to cancel all IPv6 Service-Port Control types.

3. Click **Submit**.

– End of Steps –

## 4.5.7 Configure the RA Service

This procedure describes how to configure RA service parameters. In [SLAAC](#), an IPv6 client or host retrieves the global route prefix of its IPv6 address through an RS message. After receiving the RS message, the router returns an [RA](#) message to specify the global route prefix.

### Steps

1. In the left navigation tree, click **Network > LAN > RA Service**. The **RA Service** page is displayed, as shown in [Figure 4-30](#).

Figure 4-30 RA Service Page

Path:Network-LAN-RA Service

中文

Logout

Minimum Wait Time

198

(3 ~ 1350)sec

Maximum Wait Time

600

(4 ~ 1800)sec

M

☐

O

☒

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 4-26](#).

Table 4-26 RA Service Parameter Descriptions

Parameter	Description
Minimum Wait Time	Minimum time for waiting for the RA message, range: 3–1350, unit: seconds.
Maximum Wait Time	Maximum time for waiting for the RA message, range: 4–1800, unit: seconds.

Parameter	Description
M, O	<p>M: managed address configuration.  O: other stateful configuration.  If a check box is selected, the value is 1. If not, the value is 0.</p> <ul style="list-style-type: none"> <li>● M = 0 and O = 0: SLAAC is used for acquiring information. It is applicable to a network without the DHCPv6 architecture.</li> <li>● M = 1 and O = 1: DHCPv6 is used for acquiring the address and other configuration information.</li> <li>● M = 0 and O = 1: SLAAC is used for acquiring address information. DHCPv6 is used only for acquiring network parameter settings except the IP address.</li> <li>● M = 1 and O = 0: DHCPv6 is used only for acquiring the address information.</li> </ul>

3. Click **Submit**.

– End of Steps –

## 4.6 Register

This procedure describes how to register the device through the combination modes.

There are manifold combination modes:

- **LOID**;
- **LOID + Password(LOID)**;
- **SN**;
- **Password(PON)** ;

Each of the modes above can complete the registration process.

The parameters are all provided by the network operators.

Only registered, other pages can be configured successfully.

### Prerequisite

Be sure the registration parameters are supplied by your carrier.

Be sure the device is power on and the GPON link is established.

### Steps

#### LOID + Password(LOID)

1. In the left navigation tree, click **Network > PON > LOID**. The **LOID** page is displayed, as shown in [Figure 4-31](#).

Figure 4-31 LOID Page

Path:Network-PON-LOID 中文 [Logout](#)

LOID

Password

2. Modify the **LOID** and **Password** parameters.

**Note:**

- In the LOID mode, the **Password** can be deleted or remains unchanged.


3. Click **Submit**.

**Password(SN)**

4. In the left navigation tree, click **Network > PON > SN**. The **SN** page is displayed, as shown in [Figure 4-32](#).

Figure 4-32 Password(SN) Page

Path:Network-PON-SN 中文 [Logout](#)

 Configure password take effect after rebooting the device.

SN

Password

5. Modify the **Password** parameters.

**Note:**

- The **SN** registration method will complete automatically.
- After setting the password, you must restart the device.

6. Click **Submit**.

**Note:**

- The parameter **ONU State(Status > Network Interface > PON Status)** verifies that the register was completed successfully.

– End of Steps –



## 4.7 Route Management(IPv4)

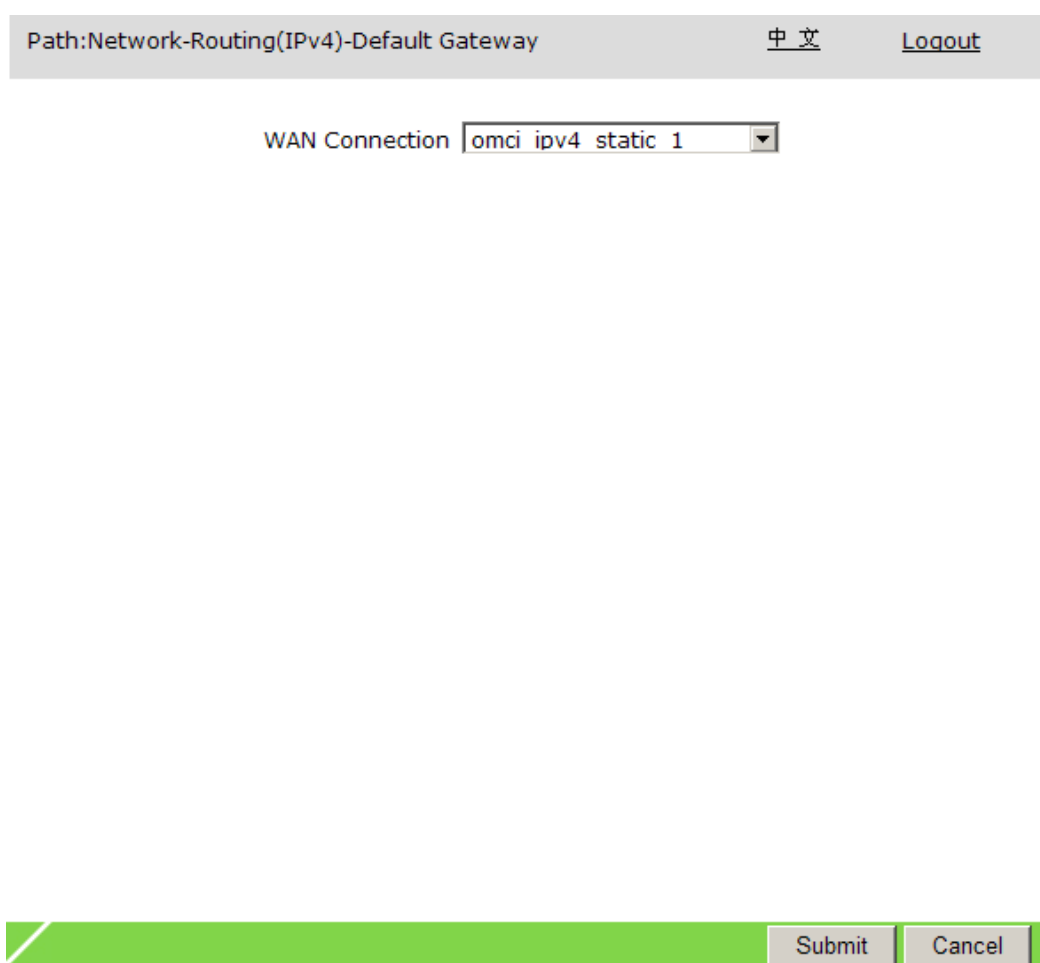
### 4.7.1 Configure the Default Gateway(IPv4)

This procedure describes how to select a [WAN](#) connection as the default route for the broadband access service.

#### Steps

1. In the left navigation tree, click **Network > Routing(IPv4)**. The **Default Gateway** page is displayed by default, as shown in [Figure 4-33](#).

**Figure 4-33 Default Gateway Page**



Path:Network-Routing(IPv4)-Default Gateway [中文](#) [Logout](#)

WAN Connection omci ipv4 static 1

Submit Cancel

2. Select a WAN connection from the **WAN Connection** list, and click **Submit**.

– End of Steps –

### 4.7.2 Configure the Static Routing(IPv4)

This procedure describes how to configure the next hop address for the destination network segment to implement static routing.

Steps

- 1. In the left navigation tree, click **Network > Routing(IPv4) > Static Routing**. The **Static Routing** page is displayed, as shown in [Figure 4-34](#).

Figure 4-34 Static Routing(IPv4) Page

Path:Network-Routing(IPv4)-Static Routing 中文 [Logout](#)

WAN Connection 

omci ipv4 static 1

Network Address

Subnet Mask

Gateway



Add

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

- 2. Set the parameters. For a description of the parameters, refer to [Table 4-27](#). Click **Add**.

Table 4-27 Static Routing(IPv4) Parameter Descriptions

Parameter	Description
WAN Connection	WAN connection that supports IPv4.
Network Address	IP address of the destination network. If network address and subnet mask are both 0.0.0.0, this configuration will be a default routing, which is effective for any destination address.
Subnet Mask	Subnet mask of the destination network.
Gateway	Gateway of the network segment which the network interface belongs to. If WAN connection and gateway are both configured, please ensure that the gateway can be reached through this WAN connection.

- 3. (Optional) To modify a routing entry, click  next to the routing entry.
- 4. (Optional) To delete a routing entry, click  next to the routing entry.

– End of Steps –

4.7.3 Configure the Policy Routing(IPv4)

Policy-based routing is a more flexible routing mechanism than destination-based routing, and packets can be forwarded in accordance with a specified policy. If a routing policy is applied to a WAN interface, the device checks packets received on the interface. The packets meeting the routing policy conditions are processed in accordance with the policy.

### Steps

1. In the left navigation tree, click **Network > Routing(IPv4) > Policy Routing**. The **Policy Routing** page is displayed, as shown in [Figure 4-35](#).

**Figure 4-35 Policy Routing(IPv4) Page**

Path:Network-Routing(IPv4)-Policy Routing
中文
[Logout](#)

Destination Interface omci ipv4 static 1

DSCP

Source IP

Source Mask

Destination IP

Destination Mask

Protocol ANY

Source Port

Destination Port

Source MAC  : : : : :

Add



Destination Interface	Source IP	Source Mask	Source Port	Protocol	
DSCP	Destination IP	Destination Mask	Destination Port	Source MAC	Delete
There is no data, please add one first.					

2. Set the parameters. For a description of the parameters, refer to [Table 4-28](#). Click **Add**.

**Table 4-28 Policy Routing(IPv4) Parameter Descriptions**

Parameter	Description
Destination Interface	WAN interface to which a routing policy is applied.
DSCP	QoS classification criterion. A DSCP is specified for the TOS byte in the IP header of each packet to indicate the priority. Range: 0–63.
Source IP	Source IP address of the matching packets.
Source Mask	Source subnet mask of the matching packets.
Destination IP	Destination IP address of the matching packets.
Destination Mask	Destination subnet mask of the matching packets.

Parameter	Description
Protocol	The protocol includes the following: <a href="#">TCP</a> , <a href="#">UDP</a> , <a href="#">ICMP</a> , ANY. The ANY option means any IP protocol.
Source Port	Source port number of the matching packets.
Destination Port	Destination port number of the matching packets.
Source MAC	MAC address of the source device that sends the matching packets.

3. (Optional) To modify a routing entry, click  next to the routing entry.
4. (Optional) To delete a routing entry, click  next to the routing entry.

– End of Steps –

## 4.7.4 Check the Routing Table(IPv4)

### Steps

1. In the left navigation tree, click **Network > Routing(IPv4) > Routing Table**. The **Routing Table** page is displayed, as shown in [Figure 4-36](#).

Figure 4-36 Routing Table(IPv4) Page

Path:Network-Routing(IPv4)-Routing Table			<a href="#">中文</a>	<a href="#">Logout</a>
Network Address	Subnet Mask	Gateway	Interface	
0.0.0.0	0.0.0.0	10.46.42.1	omci_ipv4_static_	
10.46.42.0	255.255.255.0		omci_ipv4_static_	
192.168.1.0	255.255.255.0		LAN	

				<a href="#">Refresh</a>
--	--	--	--	-------------------------

- Click **Refresh** to get the latest information.

– End of Steps –

## 4.8 Route Management(IPv6)

### 4.8.1 Configure the Default Gateway(IPv6)

Configure the default gateway(IPv6), referring to [4.7.1 Configure the Default Gateway\(IPv4\)](#).

### 4.8.2 Configure the Static Routing(IPv6)

This procedure describes how to configure the next-hop address for the destination network segment to implement static routing.

#### Steps

- In the left navigation tree, click **Network > Routing(IPv6) > Static Routing**. The **Static Routing** page is displayed, as shown in [Figure 4-37](#).

Figure 4-37 Static Routing(IPv6) Page

Path:Network-Routing(IPv6)-Static Routing

中文

Logout

WAN Connection

Prefix

/

Gateway



Add

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

2. Set the parameters. For a description of the parameters, refer to Table 4-29. Click **Add**.

Table 4-29 Static Routing(IPv6) Parameter Descriptions

Parameter	Description
WAN Connection	WAN connection that supports IPv6.
Prefix	IPv6 address and prefix length, range: 48–64.
Gateway	Gateway of the network segment which the network interface belongs to.

3. (Optional) To modify a routing entry, click  next to the routing entry.
4. (Optional) To delete a routing entry, click  next to the routing entry.

– End of Steps –

### 4.8.3 Configure the Policy Routing(IPv6)

Policy-based routing is a more flexible routing mechanism than destination-based routing, and packets can be forwarded in accordance with a specified policy. If a routing policy is applied to a WAN interface, the device checks packets received on the interface. The packets meeting the routing policy conditions are processed in accordance with the policy.

#### Steps

1. In the left navigation tree, click **Network > Routing(IPv6) > Policy Routing**. The **Policy Routing** page is displayed, as shown in Figure 4-38.

Figure 4-38 Policy Routing(IPv6) Page

Path:Network-Routing(IPv6)-Policy Routing

中文

Logout

Destination Interface

Source IP

Destination IP

Protocol

Source Port

Destination Port

Source MAC



Add

Destination Interface	Source IP	Source Port	Source MAC	Delete
Protocol	Destination IP	Destination Port		
There is no data, please add one first.				

2. Set the parameters. For a description of the parameters, refer to Table 4-30. Click **Add**.

Table 4-30 Policy Routing(IPv6) Parameter Descriptions

Parameter	Description
Destination Interface	WAN interface to which a routing policy is applied.
Source IP	Source IP address of the matching packets.
Destination IP	Destination IP address of the matching packets.
Protocol	The protocol includes the following: TCP, UDP, ANY. The ANY option means any IP protocol.
Source Port	Source port number of the matching packets.
Destination Port	Destination port number of the matching packets.
Source MAC	MAC address of the source device that sends the matching packets.

3. (Optional) To modify a routing entry, click  next to the routing entry.
4. (Optional) To delete a routing entry, click  next to the routing entry.

– End of Steps –

## 4.8.4 Check the Routing Table(IPv6)

### Steps

1. In the left navigation tree, click **Network > Routing > Routing Table**. The **Routing Table** page is displayed, as shown in [Figure 4-39](#).

**Figure 4-39 Routing Table(IPv6) Page**

Path:Network-Routing(IPv6)-Routing Table		<a href="#">中文</a>	<a href="#">Logout</a>
Prefix	Gateway	Interface	Type
fe80::/64	::	LAN	unicast

Refresh

2. Click **Refresh** to get the latest information.

– End of Steps –

## 4.9 Configure the Port Locating

The port locating feature can be enabled to prevent illegal use of user accounts. A field is added to PPPoE and DHCP messages. This field is used to describe the port.

### Steps

1. In the left navigation tree, click **Network > Port Locating**. The **Port Locating** page is displayed, as shown in [Figure 4-40](#).



Figure 4-40 Port Locating Page

Path:Network-Port Locating 中文 [Logout](#)

Enable DHCP Port Locating ☐

Enable PPPOE Port Locating ☐

Port Locating Format Custom

Custom Port Locating Format  (1 ~ 60 characters)

Submit Cancel

2. To enable the port locating, click the check box. And then click **Submit**.

– End of Steps –

# Chapter 5

## Security Configuration

---

### Table of Contents

Configure the Firewall .....	5-1
Configure the IPv4 Filter .....	5-3
Configure the MAC Filter .....	5-5
Configure the URL Filter .....	5-6
Configure the Service Control Filter .....	5-6
Configure the ALG Feature .....	5-8

## 5.1 Configure the Firewall

This procedure describes how to configure the firewall to enhance device security and avoid illegal access from external networks.

### Steps

1. In the left navigation tree, click **Security > Firewall**. The **Firewall** page is displayed, as shown in [Figure 5-1](#).

Figure 5-1 Firewall Page

Path:Security-Firewall

中文

Logout

Enable Anti-Hacking Protection ☐

Firewall Level

☐ Off

☒ Low

☐ Middle

☐ High

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 5-1](#).

Table 5-1 Firewall Parameter Descriptions

Parameter	Description
Enable Anti-Hacking Protection	To enable anti-hacking protection and prevent device shutdown due to Internet attacks, select this check box. This feature can prevent ping flood, ping to death, and SYN flood attacks.
Firewall Level	<ul style="list-style-type: none"><li>● Off: disables the firewall.</li><li>● Low: allows legal access from the WAN and allows Internet devices to send ping packets to the WAN interface of the ZXHN F670.</li><li>● Middle: allows legal access from the WAN and blocks dangerous data from the Internet.</li><li>● High: allows legal access from the WAN but forbids Internet devices from sending ping packets to the WAN interface of the ZXHN F670.</li></ul>

3. Click **Submit**.
- End of Steps –

## 5.2 Configure the IPv4 Filter

This procedure describes how to configure an IPv4 filter to allow or deny the access of devices with specific IPv4 addresses to the ZXHN F670.

### Steps

1. In the left navigation tree, click **Security > IP Filter**. The **IP Filter** page is displayed, as shown in [Figure 5-2](#).

Figure 5-2 IP Filter Page

Path:Security-IP Filter 中文 [Logout](#)

Enable ☐

Protocol 

TCP

Name

Start Source IP Address

End Source IP Address

Start Destination IP Address

End Destination IP Address

Start Source Port

End Source Port

Start Destination Port

End Destination Port

Ingress

Egress

Mode 

Discard

Add



Enable	Name	Start Source IP Address	Start Source Port	Start Destination IP Address	Start Destination Port	Ingress		Modify	Delete
Protocol	Mode	End Source IP Address	End Source Port	End Destination IP Address	End Destination Port	Egress			
There is no data, please add one first.									

2. Set the parameters. For a description of the parameters, refer to [Table 5-2](#). Click **Add**.

Table 5-2 IPv4 Filter Parameter Descriptions

Parameter	Description
Enable	To enable the IPv4 filter to be configured, select this check box.

Parameter	Description
Protocol	<p>Protocol of the packets to be filtered. Options:</p> <ul style="list-style-type: none"> <li>● TCP (default)</li> <li>● UDP</li> <li>● TCP AND UDP</li> <li>● ICMP</li> <li>● ANY</li> </ul> <p>Indicates that all the above protocols are selected.</p>
Start Source IP Address/End Source IP Address	Filter criteria, which can be set as required. Optional.
Start Destination IP Address/End Destination IP Address	Filter criteria, which can be set as required. Optional.
Start Source Port/End Source Port	Filter criteria, which can be set as required. Optional.
Start Destination Port/End Destination Port	Filter criteria, which can be set as required. Optional.
Ingress	<p>Specify the data traffic direction. The ingress option and egress option cannot be the same.</p> <ul style="list-style-type: none"> <li>● If the ingress is LAN, the egress should be a WAN or 3G connection. The data traffic direction is upstream.</li> <li>● If the ingress is a WAN or 3G connection, the egress should be the LAN. The data traffic direction is downstream.</li> </ul>
Egress	<p>Specify the data traffic direction. The ingress option and egress option cannot be the same.</p> <ul style="list-style-type: none"> <li>● If the ingress is LAN, the egress should be a WAN or 3G connection. The data traffic direction is upstream.</li> <li>● If the ingress is a WAN or 3G connection, the egress should be the LAN. The data traffic direction is downstream.</li> </ul>
Mode	<p>Action taken on the packets meeting the filter criteria. Options:</p> <ul style="list-style-type: none"> <li>● Discard</li> <li>● Permit</li> </ul>

- (Optional) To modify a configuration record, click  next to the record.
- (Optional) To delete a configuration record, click  next to the record.

– End of Steps –

## 5.3 Configure the MAC Filter

A list of [MAC](#) addresses that access the ZXHN F670 are stored on the ZXHN F670. You can restrict the access of some hosts by configuring a MAC filter. One host may have multiple IP addresses, but its MAC address is unique. The access rights of hosts can be controlled through MAC filters.

### Steps

1. In the left navigation tree, click **Security > MAC Filter**. The **MAC Filter** page is displayed, as shown in [Figure 5-3](#).

Figure 5-3 MAC Filter Page

Path:Security-MAC Filter

中文Logout

Enable☐

ModeDiscard

TypeBridge

ProtocolIP

Source MAC Address

:

:

:

:

:

:

Destination MAC Address

:

:

:

:

:

:

Add

2. Set the parameters. For a description of the parameters, refer to [Table 5-3](#). Click **Add**.

Table 5-3 MAC Filter Parameter Descriptions

Parameter	Description
Enable	Specifies whether to enable the MAC filter.
Mode	Action taken on the data meeting the filter criteria.
Type	Operation mode.
Protocol	Protocol of data streams. Options: IP, ARP, RARP, PPPoE and ALL.
Source MAC Address	Source MAC address to be filtered, which must be specified.
Destination MAC Address	Destination MAC address to be filtered, which must be specified.

3. (Optional) To modify a configuration record, click  next to the record.

4. (Optional) To delete a configuration record, click  next to the record.

– End of Steps –

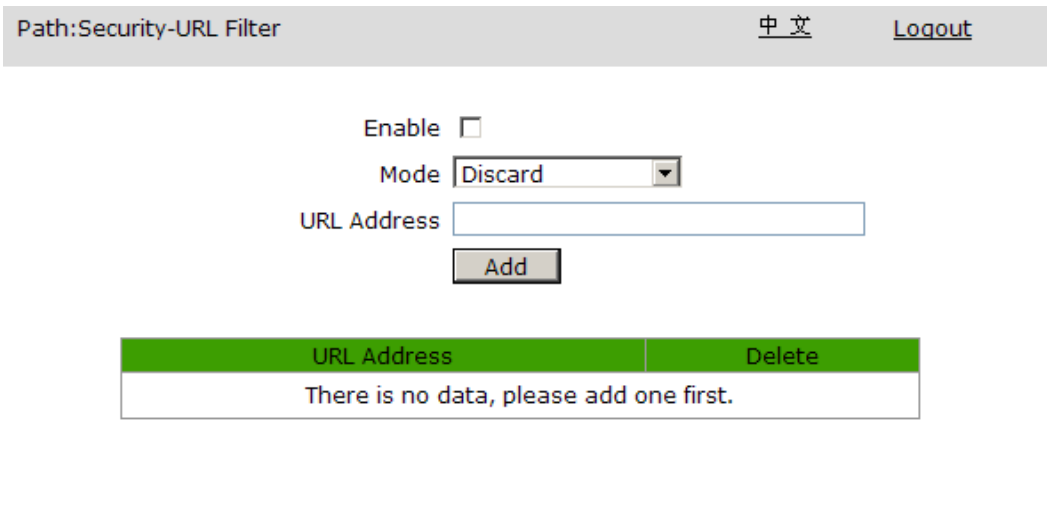
# 5.4 Configure the URL Filter

This procedure introduces how to configure the URL filter.

## Steps

1. In the left navigation tree, click **Security > Parental Control > URL Filter**. The **URL Filter** page is displayed by default, as shown in [Figure 5-4](#).

**Figure 5-4 URL Filter Page**



2. Set the parameters. For a description of the parameters, refer to [Table 5-4](#). Click **Add**.

**Table 5-4 URL Filter Parameter Descriptions**

Parameter	Description
Enable	To enable the URL filter, select this check box.
Mode	Action taken on the packets meeting the filter criteria. Options: <ul style="list-style-type: none"> <li>● Discard</li> <li>● Permit</li> </ul>
URL Address	The URL address that is allowed to be accessed or denied.

– End of Steps –

# 5.5 Configure the Service Control Filter

This procedure describes how to configure a service control filter to allow or deny the access of a specific service to the ZXHN F670.

Steps

- 1. In the left navigation tree, click **Security > Service Control**. The **Service Control** page is displayed, as shown in [Figure 5-5](#).

Figure 5-5 Service Control Page

Path:Security-Service Control 中文 [Logout](#)

IP Version 

IPv4

Enable ☐

Ingress

Start Source IP Address

End Source IP Address

Mode 

Discard

☐ HTTP

☐ FTP

Service List ☐ SSH

☐ TELNET

☐ HTTPS

Add

Enable	Ingress	Start Source IP Address	End Source IP Address	Mode	Service List	Modify	Delete
<input checked="" type="checkbox"/>	WAN			Permit	HTTP		

Note: If you need to configure the above remote access ports, please click on the hyperlinks below.  
[Modify Remote Access Port](#)



- 2. Set the parameters. For a description of the parameters, refer to [Table 5-5](#). Click **Add**.

Table 5-5 Service Control Parameter Descriptions

Parameter	Description
IP Version	Supported IP version. Options: IPv4 and IPv6.
Enable	To enable the service control filter to be configured, select this check box.
Ingress	<div>Specify the data stream inbound direction, and this parameter must be specified.</div> <ul style="list-style-type: none"><li>● If the Ingress is WAN, all the WAN connection can access ZXHN F670.</li><li>● If the Ingress is LAN, the LAN side can access ZXHN F670.</li><li>● If the Ingress is a WAN or Route_3G connection, the connection selected can access ZXHN F670.</li></ul>



Parameter	Description
Start Source IP Address/ End Source IP Address	IP address segment for which service control is implemented.
Mode	Action taken on the IP address segment meeting the filter criteria. Options: <ul style="list-style-type: none"> <li>● Discard</li> <li>● Permit</li> </ul>
Service List	Service to be controlled. Options: HTTP, FTP,SSH, TELNET, HTTPS
Modify Remote Access Port	To modify the service access port, click this link.

3. (Optional) To modify a configuration record, click  next to the record.
4. (Optional) To delete a configuration record, click  next to the record.

– End of Steps –

## 5.6 Configure the ALG Feature

This procedure describes how to enable the [ALG](#) feature, so that the ZXHN F670 can translate private IP addresses in layer-4 packets into public IP addresses to enhance security.

### Steps

1. In the left navigation tree, click **Security > ALG**. The **ALG** page is displayed, as shown in [Figure 5-6](#).

Figure 5-6 ALG Page

Path:Security-ALG [中文](#) [Logout](#)

Enable ALG

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

[Submit](#) [Cancel](#)

2. Select the protocols for which ALG is to be enabled, and click **Submit**.

– End of Steps –

# Chapter 6

## Application Configuration

---

### Table of Contents

VoIP (H248) Configuration.....	6-1
VoIP (SIP) Configuration .....	6-17
Configure the DDNS.....	6-26
Configure the DMZ .....	6-27
Configure the UPnP .....	6-29
Check the UPnP Port Mapping.....	6-30
Configure the Port Forwarding.....	6-31
DNS Service .....	6-33
Configure the Time Parameters.....	6-36
Multicast Configuration .....	6-37
Configure the BPDU .....	6-43
Check the USB Storage Information.....	6-44
Configure the DMS.....	6-45
Configure the FTP Server Feature.....	6-47
Configure the Port Triggering .....	6-48
Configure the Port Forwarding(Application List).....	6-50
Configure the Application List.....	6-51
Configure the Samba Service.....	6-52
Configure the USB Print Server.....	6-54

## 6.1 VoIP (H248) Configuration

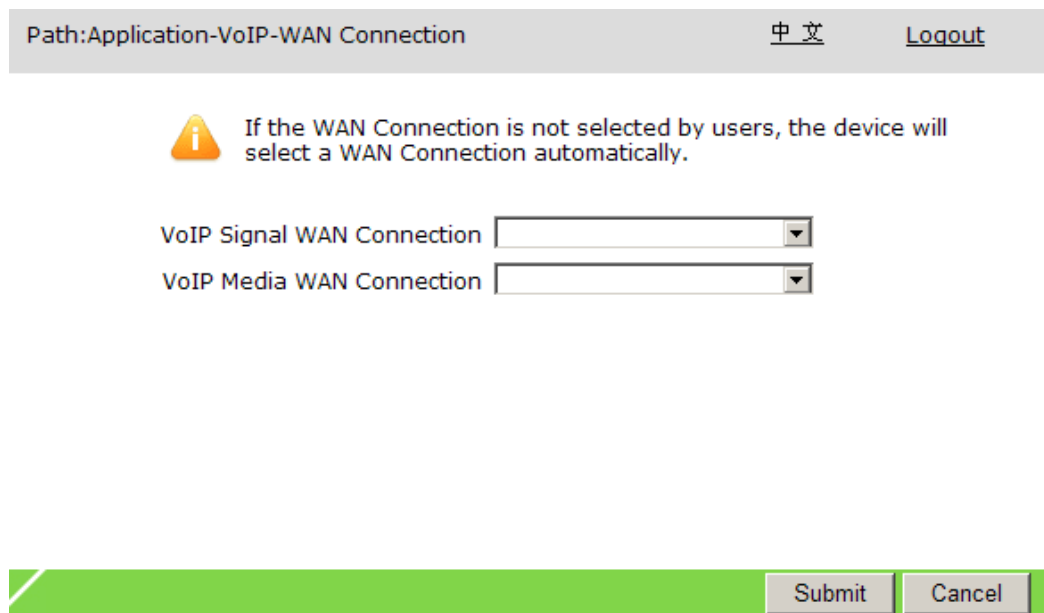
### 6.1.1 Configure the WAN Connection(H248)

This procedure describes how to configure WAN connections for the VoIP service. The signaling and media traffic can use the same or different WAN connections for connecting to the external network.


#### Steps

1. In the left navigation tree, click **Application > VoIP > WAN Connection**. The **WAN Connection** page is displayed, as shown in [Figure 6-1](#).

Figure 6-1 WAN Connection Page



Path:Application-VoIP-WAN Connection      中文      Logout

 If the WAN Connection is not selected by users, the device will select a WAN Connection automatically.

VoIP Signal WAN Connection

VoIP Media WAN Connection

Submit Cancel

2. Set the **VoIP Signal WAN Connection** and **VoIP Media WAN Connection** parameters.

**Note:**

If no option exists in the drop-down list, create a WAN connection whose **Service List** parameter is set to a value including the **VoIP** service (**Network > WAN > WAN Connection**).

3. Click **Submit**.

– End of Steps –

## 6.1.2 Configure the Advanced Parameters(H248)

This procedure describes how to configure advanced parameters of the VoIP service, including echo cancellation, jitter buffer, and [DTMF](#).

### Steps

1. In the left navigation tree, click **Application > VoIP > Advanced**. The **Advanced** page is displayed, as shown in [Figure 6-2](#).

Figure 6-2 Advanced Page

Path:Application-VoIP-Advanced

中文

Logout

DTMF

Dtmf in Voice

Jitter Buffer

Adaptive

Min Value

20

ms

Max Value

200

ms

Phone1

Echo Cancellation

Enabled

Exhaled gain

0

(-14~6)

Incoming gain

0

(-14~6)

Phone2

Echo Cancellation

Enabled

Exhaled gain

0

(-14~6)

Incoming gain

0

(-14~6)

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to Table 6-1.

Table 6-1 Advanced Parameter Descriptions for the VoIP Service

Parameter	Description
DTMF	DTMF mode. Options: <ul style="list-style-type: none"><li>● <b>RFC2833</b>: DTMF digits are carried by RTP streams.</li><li>● <b>Dtmf in Voice</b>: DTMF digits are not processed.</li></ul>
Jitter Buffer	The variation in packet delay is called jitter. Jitter buffer refers to intentional delay of packets. Options: <ul style="list-style-type: none"><li>● <b>Fixed</b>: A fixed buffer time must be specified.</li><li>● <b>Adaptive</b>: A jitter range must be specified.</li></ul>
Min Value	Minimum value of the jitter range, default: 20 ms.
Max Value	Maximum value of the jitter range, default: 200 ms.
Echo Cancellation	Whether to disable the echo cancellation feature.
Exhaled gain	Line transmit gain, range: -14 to 6 dBd.
Incoming gain	Line receive gain, range: -14 to 6 dBd.

3. Click **Submit**.

– End of Steps –

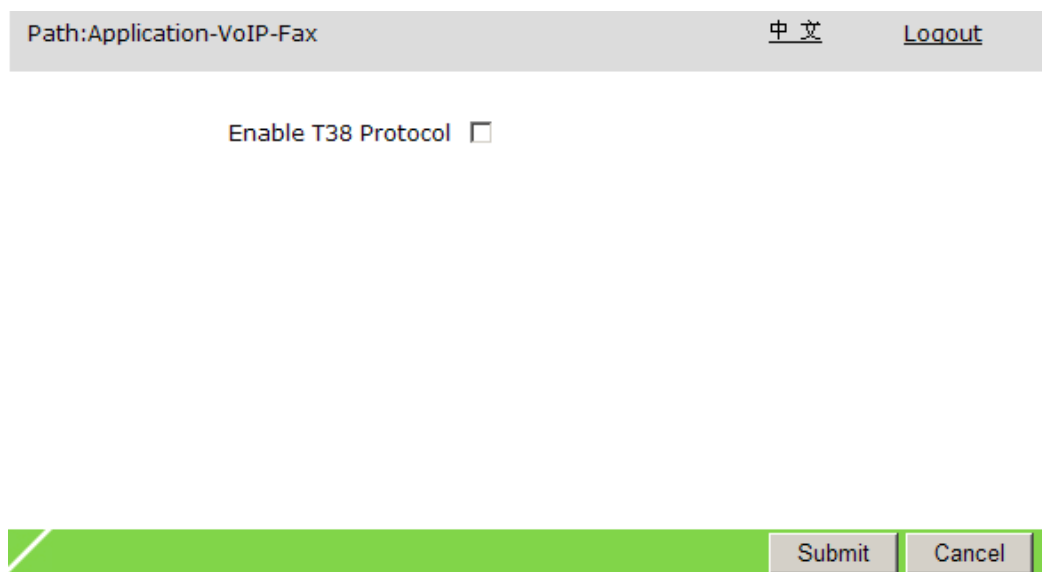
### 6.1.3 Configure the Fax Feature(H248)

This procedure describes how to switch from T30 protocol to T38 protocol.

#### Steps

1. In the left navigation tree, click **Application > VoIP > Fax**. The **Fax** page is displayed, as shown in [Figure 6-3](#).

**Figure 6-3 Fax Page**



Path:Application-VoIP-Fax [中文](#) [Logout](#)

Enable T38 Protocol ☐

[Submit](#) [Cancel](#)

2. Set the parameters. For a description of the parameters, refer to [Table 6-2](#).

**Table 6-2 Fax Parameter Descriptions**

Parameter	Description
Enable T38 Protocol	Whether to enable the T38 protocol. If this check box is not selected, the T30 protocol is used.

3. Click **Submit**.

– End of Steps –

### 6.1.4 Configure the VoIP Service(H248)

This procedure describes how to configure the basic parameters for the VoIP service on the ZXHN F670.

#### Steps

1. Select **Application > VoIP > VoIP Services**. The **VoIP Services** page is displayed, as shown in [Figure 6-4](#).

Figure 6-4 VoIP Services Page

Path:Application-VoIP-VoIP Services

中文

Logout

TestLink Flag

Notify

RTP Link Detection Flag

☐

Number Match Flag

Intelligent Match

DigitMap L Timer

2000

10 ms

DigitMap S Timer

500

10 ms

DigitMap T Timer

1000

10 ms

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to Table 6-3.

Table 6-3 VoIP Service Parameter Descriptions

Parameter	Description
TestLink Flag	Specifies whether the ZXHN F670 regularly sends heartbeat packets to the SS system to verify the link status. Options: <ul style="list-style-type: none"><li>● <b>Disable</b>: Heartbeat detection is disabled.</li><li>● <b>Service Change</b>: As a client, the ZXHN F670 sends Service Change messages (which are used as heartbeat detection messages) to the SS system.</li><li>● <b>Notify</b>: As a client, the ZXHN F670 sends Notify messages (which are used as heartbeat detection messages) to the SS system.</li></ul>
RTP Link Detection Flag	Specifies whether to enable RTP link detection.
Number Match Flag	Number matching mode. Options: <ul style="list-style-type: none"><li>● Intelligent Match</li><li>● Long Match</li><li>● Short Match</li></ul>
DigitMap L Timer	Long timer duration, unit: 10 ms, default: 20000 ms.
DigitMap S Timer	Short timer duration, unit: 10 ms, default: 5000 ms.
DigitMap T Timer	First digit timer duration, unit: 10 ms, default: 10000 ms.

3. Click **Submit**.

– End of Steps –

## 6.1.5 Configure the Basic H248 Parameters

In the SS system, the H248 protocol separates call logic control from the media gateway, so that the media gateway implements only media format conversion.

This procedure describes how to configure basic H248 parameters for normal connection between the ZXHN F670 and the SS system, including the address and port.

### Steps

1. In the left navigation tree, click **Application > VoIP > H248 Basic**. The **H248 Basic** page is displayed, as shown in [Figure 6-5](#).



Figure 6-5 H248 Basic Page

Path:Application-VoIP-H248 Basic

中文

Logout

Local Port

2944

(1024 ~ 65535)

Preferred CA Identifier

0.0.0.0

(0 ~ 63 characters)

Preferred Port

2944

(1024 ~ 65535)

Alternate CA Identifier

0.0.0.0

(0 ~ 63 characters)

Alternate Port

2944

(1024 ~ 65535)

MID Flag

IPv4

MID

(0 ~ 64 characters)

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-4](#).

Table 6-4 H248 Basic Parameter Descriptions

Parameter	Description
Local Port	Local port that the H248 protocol uses, default: 2944.
Preferred CA Identifier	IP address or domain name of the active H248 proxy server.
Preferred Port	H248 port of the active proxy server, which must be the same as that configured on the SS side.
Alternate CA Identifier	IP address or domain name of the standby H248 proxy server.

Parameter	Description
Alternate Port	H248 port of the standby proxy server, which must be the same as that configured on the SS side.
MID Flag	MID type. The options include IPv4, Domain Name, and Equipment Name. <ul style="list-style-type: none"><li>● <b>IPv4</b> :If it is set to <b>IPv4</b>, the VoIP WAN connection address must be the same as the IP address set in the SS system.</li><li>● <b>Domain Name</b>: globally unique domain name that the ONT registers in the SS system.</li><li>● <b>Equipment Name</b></li></ul>
MID	If <b>MID Flag</b> is set to <b>Domain Name</b> or <b>Equipment Name</b> , enter the domain name or device name that must be the same as that configured in the SS system.

3. Click **Submit**.

– End of Steps –

## 6.1.6 Configure the H248 Terminations

A H248 termination is a logical entity on the SS media gateway that is used for sending or receiving media streams and control packets.

This procedure describes how to configure H248 terminations.

### Steps

1. In the left navigation tree, click **Application > VoIP > H248 Termination**. The **H248 Termination** page is displayed, as shown in [Figure 6-6](#).

Figure 6-6 H248 Termination Page

Path:Application-VoIP-H248 Termination

中文

Logout

Physical Termination Setting

Group By Group

TID PrefixAG589

Extension Length2

Temporary TID PrefixRTP/

Extension Length5

Start Value0

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-5](#).

Table 6-5 H248 Termination Parameter Descriptions

Parameter	Description
Physical Termination Setting	Physical termination setting mode. Options: <ul style="list-style-type: none"><li>● Group by Group: A group of physical terminations are configured by setting the terminal ID prefix and extension length.</li><li>● One by One: Termination IDs are configured one by one.</li></ul>
TID Prefix	Prefix of termination IDs, which must be the same as that configured on SS.
Extension Length	Length of the extension name.
Temporary TID Prefix	A group of physical terminations are configured by setting the terminal ID prefix and extension length.
Start Value	Start value.

3. Click **Submit**.
- End of Steps –

### 6.1.7 Configure the H248 Authentication

This procedure describes how to configure H248 authentication parameters, including those required for connecting to the SS system.

### Steps

1. In the left navigation tree, click **Application > VoIP > H248 Auth**. The **H248 Auth** page is displayed, as shown in [Figure 6-7](#).

**Figure 6-7 H248 Auth Page**

Path:Application-VoIP-H248 Auth

中文
Logout

Access Flag

0

MID Flag

MAC

MID

(0 ~ 63 characters)

KI

0123456789ABCDE

(0 ~ 63 characters)

P

1

G

0

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-6](#).

**Table 6-6 H248 Authentication Parameter Descriptions**

Parameter	Description
Access Flag	Authentication flag. Options: 0, 1, and 100.
MID Flag	MID type if <b>Access Flag</b> is set to <b>100</b> . Options: <ul style="list-style-type: none"> <li>● <b>MAC</b>: The <b>MID</b> parameter is non-configurable and is set to ZTE-(WAN connection's MAC address).</li> <li>● <b>IP</b>: The <b>MID</b> parameter is non-configurable and is set to the IP address.</li> <li>● <b>Manual</b>: The <b>MID</b> parameter is configurable.</li> </ul>
MID	Gateway ID, which must be the same as that configured in the SS system.
KI	Initial key of the gateway, which must be the same as that configured in the SS system.
P	Default modulo. Options: <ul style="list-style-type: none"> <li>● <b>1</b>: 96-bit default modulo in the SS system.</li> <li>● <b>2</b>: 128-bit default modulo in the SS system.</li> </ul>
G	Bottom number G. Options: 0, 1, 2, 3, and 4, corresponding to the bottom numbers 2, 3, 5, 7, and 9 respectively in the SS system.

- Click **Submit**.

– End of Steps –

## 6.1.8 Configure the H248 Timers

This procedure describes how to configure H248 timers.

### Steps

- In the left navigation tree, click **Application > VoIP > H248 Timer**. The **H248 Timer** page is displayed, as shown in [Figure 6-8](#).

**Figure 6-8 H248 Timer Page**

Path:Application-VoIP-H248 Timer

中文

Logout

Min Restart Interval

1000

(0-50000)\*10ms

Max Restart Interval

6000

(0-50000)\*10ms

Min Register Interval

100

(0-50000)\*10ms

Max Register Interval

30000

(0-50000)\*10ms

TestLink Flag

Passive

Max Failed TestLink

1

(1-10)

Register Retransmit Type

1

Register Retransmit Times

6

(0-20)

Register Retransmit Timer

400

(10-5000)\*10ms

Total Register Retransmit Time

2500

(10-50000)\*10ms

Submit

Cancel

- Set the parameters. For a description of the parameters, refer to [Table 6-7](#).

**Table 6-7 H248 Timer Parameter Descriptions**

Parameter	Description
Min Restart Interval	Minimum value of the restart timer, unit: 10 ms, default: 1000.
Max Restart Interval	Maximum value of the restart timer, unit: 10 ms, default: 6000.
Min Register Interval	Minimum value of the re-registration timer, unit: 10 ms, default: 100.

Parameter	Description
Max Register Interval	Maximum value of the re-registration timer, unit: 10 ms, default: 30000.
TestLink Flag	Heartbeat mode. Options: Active and Passive.
Max Failed TestLink	Maximum number of heartbeat detection failures.
Register Retransmit Type	Retransmission mode. Options: 0 and 1.
Register Retransmit Times	Number of registration message retransmission times.
Register Retransmit Timer	Registration message retransmission timer, unit: 10 ms, default: 400.
Total Register Retransmit Time	Total retransmission time, unit: 10 ms, default: 2500.

3. Click **Submit**.

– End of Steps –

## 6.1.9 Configure the Media Codec Type(H248)

This procedure describes how to configure the media codec type.

### Steps

1. In the left navigation tree, click **Application > VoIP > Media**. The **Media** page is displayed, as shown in [Figure 6-9](#).

Figure 6-9 Media Page

Path:Application-VoIP-Media

中文

Logout

Media Negotiation Remote Priority

Phone1

☐ G711U VAD

☐ G711A VAD

☐ G729 VAD

☐ G722 VAD

Phone2

☐ G711U VAD

☐ G711A VAD

☐ G729 VAD

☐ G722 VAD

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-8](#).

Table 6-8 Media Parameter Descriptions

Parameter	Description
Media Negotiation	Media negotiation mode. Options: Remote Priority and Local Priority. <ul style="list-style-type: none"><li>Local Priority: The ONU performs voice media negotiation in accordance with its own coding and decoding priority.</li><li>Remote Priority: The ONU performs voice media negotiation in accordance with the coding and decoding priority of the peer end.</li></ul>

Parameter	Description
G711U VAD	Select a codec.
G711A VAD	
G729 VAD	
G722 VAD	

3. Click **Submit**.

– End of Steps –

### 6.1.10 Configure the CID Feature(H248)

The ZXHN F670 supports the caller identification feature in FSK and DTMF modes.

- FSK mode

During a call, the caller ID is transmitted in FSK mode between the first and second rings.

- DTMF mode

During a call, the caller ID is transmitted in DTMF mode before the first ring.

#### Steps

1. Select **Application > VoIP > Caller ID**. The **Caller ID** page is displayed, as shown in [Figure 6-10](#).



Figure 6-10 Caller ID Page

Path:Application-VoIP-Caller ID

中文

Logout

Caller ID Mode

FSK

ETSI CID Standard ☐

Submit

Cancel

2. Set the parameter. For a description of the parameter, refer to [Table 6-9](#).

Table 6-9 CID Parameter Description

Parameter	Description
Caller ID Mode	Caller ID transmission mode. Options: <a href="#">FSK</a> , <a href="#">DTMF</a> , and FSK&DTMF.
ETSI CID Standard	Select the check box to follow the standard.

3. Click **Submit**.
- End of Steps –

### 6.1.11 Configure the SLIC(H248)

This procedure describes how to configure [SLIC](#) parameters.

#### Steps

1. In the left navigation tree, click **Application > VoIP > SLIC configuration**. The **SLIC configuration** page is displayed, as shown in [Figure 6-11](#).

Figure 6-11 SLIC Parameter Descriptions

Path:Application-VoIP-SLIC configuration

中文

Logout

Phone1

ring voltage vpk70Vpk

loop current24mA

open circuit voltage52V

Phone2

ring voltage vpk70Vpk

loop current24mA

open circuit voltage52V

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to Table 6-10.

Table 6-10 SLIC Parameter Descriptions

Parameter	Description
ring voltage vpk	Ring voltage of the VoIP line, unit: vpk, default: 75.
loop current	Loop current of the VoIP line, unit: mA, default: 25.
open circuit voltage	Open circuit voltage of the VoIP line, unit: V, default: 48.

3. Click **Submit**.

– End of Steps –

## 6.2 VoIP (SIP) Configuration

### 6.2.1 Configure the WAN Connection(SIP)

The WAN connection configuration for the SIP-based VoIP service is the same as that for the H248-based VoIP service. For details, refer to [6.1.1 Configure the WAN Connection\(H248\)](#).

### 6.2.2 Configure the Advanced Parameters(SIP)

The advanced parameter configuration for the SIP-based VoIP service is the same as that for the H248-based VoIP service. For details, refer to [6.1.2 Configure the Advanced Parameters\(H248\)](#).

### 6.2.3 Configure the Fax Feature(SIP)

The fax feature configuration for the SIP-based VoIP service is the same as that for the H248-based VoIP service. For details, refer to [6.1.3 Configure the Fax Feature\(H248\)](#).

### 6.2.4 Configure the SIP Protocol

[SIP](#) is a network communication protocol for controlling the [VoIP](#) service. It supports voice, video, data, E-mail, chat, and game applications. This procedure describes how to configure the basic parameters for the SIP-based VoIP service on the ZXHN F670.

#### Steps

1. In the left navigation tree, click **Application > VoIP > SIP**. The **SIP** page is displayed, as shown in [Figure 6-12](#).

Figure 6-12 SIP Parameter Descriptions

Path:Application-VoIP-SIP

中文
Logout

Option 120 ☐

Local Port  (1024 ~ 65535)

Register Server

Primary Proxy Server

Primary Outbound Proxy Server

Primary Proxy Port  (1024 ~ 65535)

Secondary Proxy Server

Secondary Outbound Proxy Server

Secondary Proxy Port  (1024 ~ 65535)

Register Expires  sec

Unregister On Reboot ☐

Enable Link Test ☐

Link Test Interval  sec

Submit

Cancel

- Set the parameters. For a description of the parameters, refer to [Table 6-11](#).

Table 6-11 SIP Parameter Descriptions

Parameter	Description
Option 120	If the Option 120 is enabled, the message with field of Option 120 will be send to the DHCP server.
Local Port	Local port that the SIP protocol uses, default: 5060.
Register Server	IP address of the SIP register server that the ISP provides, which must be the same as that configured on the SIP server.
Primary Proxy Server	IP address of the active SIP proxy server that the ISP provides, which must be the same as that configured on the SIP server.
Primary Outbound Proxy Server	IP address of the active outbound proxy server that the ISP provides, which must be the same as that configured on the SIP server.
Primary Proxy Port	Port number that the ISP provides for communication between the active server and VoIP terminals, which must be the same as that configured on the SIP server, default: 5060.
Secondary Proxy Server	IP address of the standby SIP proxy server that the ISP provides, which must be the same as that configured on the SIP server.

Parameter	Description
Secondary Outbound Proxy Server	IP address of the standby outbound proxy server that the ISP provides, which must be the same as that configured on the SIP server.
Secondary Proxy Port	Port number that the ISP provides for communication between the standby server and VoIP terminals, which must be the same as that configured on the SIP server, default: 5060.
Register Expires	Registered lifecycle, unit: seconds, default: 3600.
Unregister On Reboot	Whether to deregister VoIP terminals after the server is restarted.
Enable Link Test	Whether to enable link tests.
Link Test Interval	Interval of link tests, default: 20 seconds.

3. Click **Submit**.

– End of Steps –

## 6.2.5 Configure the SIP Account

This procedure describes how to configure a SIP account.

### Steps

1. In the left navigation tree, click **Application > VoIP > SIP Accounts**. The **SIP Accounts** page is displayed, as shown in [Figure 6-13](#).

**Figure 6-13 SIP Accounts Page**



Path:Application-VoIP-SIP Accounts

[中文](#)
[Logout](#)

SIP Account

Authorization Username


Password

SIP Account	Authorization Username	Modify
		
		

2. Set the parameters. For a description of the parameters, refer to [Table 6-12](#).

**Table 6-12 SIP Account Parameter Descriptions**

Parameter	Description
SIP Account	Registered name of a SIP subscriber. Normally, it is the phone number of the subscriber.
Authorization Username	Username for authentication by the SS system, which must be the same as that configured in the SS system.
Password	Password for VoIP service authentication by the SS system, which must be the same as that configured in the SS system.

3. Click  next to an account to modify the information, and click **Modify**.

– End of Steps –

## 6.2.6 Configure the VoIP Service(SIP)


This procedure describes how to configure additional services for the SIP-based VoIP service on the ZXHN F670.

### Steps

1. In the left navigation tree, click **Application > VoIP > VoIP Services**. The **VoIP Services** page is displayed, as shown in [Figure 6-14](#).

Figure 6-14 VoIP Services Page

Path:Application-VoIP-VoIP Services中文[Logout](#)

 Configure VoIP Services, need to configure the SIP Accounts.

Phone

Phone1

SIP Account

Authorization Username

Unconditional Call Forwarding ☐

Forward to

Busy Call Forwarding ☐

Forward to

No Answer Call Forwarding ☐

Forward to

No Answer Timer200010ms

Call Waiting ☐

Call Transfer ☐

Call Hold ☐

Hook Delay ☐

INFO Procedure ☐

Three-Way Talking ☐

Conference URI

HotLine OptionsUnused

Destination Number

Delay Hot Line Timer100010ms

AntiPole☒

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-13](#).

Table 6-13 VoIP Services Parameter Descriptions

Parameter	Description
Phone	Line that is bound with the VoIP service, default: Phone1.
Unconditional Call Forwarding	Enables or disables unconditional call forwarding.
Forwarded to	Number to which a call is unconditionally forwarded.
Busy Call Forwarding	Enables or disables busy call forwarding.

Parameter	Description
Forwarded to	Number to which a call is forwarded when the called number is busy.
No Answer Call Forwarding	Enables or disables no answer call forwarding.
Forwarded to	Number to which a call is forwarded when the called number does not answer.
No Answer Timer	A call is forwarded when the called number does not answer exceeding time.
Call Waiting	Enables or disables call waiting.
Call Transfer	Enables or disables call transfer.
Call Hold	Enables or disables call hold.
Hook Delay	Enables or disables hook delay.
INFO Procedure	Enables or disables the INFO procedure function.
Three-Way Talking	Enables or disables the three-Way conference function.
Conference URI	Access number for a teleconference, configurable after the three-party conference function is enabled.
HotLine Options	Enables or disables the hotline function, including immediate hotline and delayed hotline.
Destination Number	Hotline number, configurable after the immediate or delayed hotline function is enabled.
Delay Hot Line Timer	Delay timer duration for the delayed hotline function, unit: 10 ms.
AntiPole	Enables or disables the polarity reversed signal function.

3. Click **Submit**.

– End of Steps –

## 6.2.7 Configure the Digital Map

A digital map defines dialing rules that must be followed when you dial a number.

### Steps

1. In the left navigation tree, click **Application > VoIP > Digital Map**. The **Digital Map** page is displayed, as shown in [Figure 6-15](#).



Figure 6-15 Digital Map Page

Path:Application-VoIP-Digital Map 中文 [Logout](#)

Please enter the Digital Map

X\*.X.#|#X.\*.X.##|#X.\*.X.T|#X.\*.X.#T|X\*.X.T|\*\*X.\*.X.\*.X.##|\*\*X.  
\*.X.\*.X.#T

Submit Cancel

In a digital map, **X** means digits, **\*** means the asterisk key, **#** means the pound key, and **.** means any length.

2. Click **Submit**.

– End of Steps –

## 6.2.8 Configure the Media Codec Type(SIP)

This procedure describes how to configure the media codec type.

### Steps

1. In the left navigation tree, click **Application > VoIP > Media**. The **Media** page is displayed, as shown in [Figure 6-16](#).

Figure 6-16 Media Page

Path:Application-VoIP-Media

中文Logout

Phone1

Codec Selection

☒ G711U

☐ VAD

☒ G711A

☐ VAD

☒ G729

☐ VAD

☒ G722

☐ VAD

Codec Priority 1~16

G711U2

G711A1

G7293

G7224

Phone2

Codec Selection

☒ G711U

☐ VAD

☒ G711A

☐ VAD

☒ G729

☐ VAD

☒ G722

☐ VAD

Codec Priority 1~16

G711U2

G711A1

G7293

G7224

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-14](#).

Table 6-14 Media Parameter Descriptions

Parameter	Description
Codec Selection	Select a codec, which must be the same as that configured in the SS system.
Codec Priority 1~16	You can modify priority through this parameter. A lower number indicates a higher priority.

3. Click **Submit**.

– End of Steps –

## 6.2.9 Configure the CID Feature(SIP)

The ZXHN F670 supports FSK-based and DTMF-based caller ID and call time display.

### Steps

1. In the left navigation tree, click **Application > VoIP > Caller ID**. The **Caller ID** page is displayed, as shown in [Figure 6-17](#).

**Figure 6-17 Caller ID Page**

Path:Application-VoIP-Caller ID      中文      Logout

Caller ID Mode

ETSI CID Standard ☐

Caller ID Time

CID Obtain

Preferred Username ☐

2. Set the parameters. For a description of the parameters, refer to [Table 6-15](#).

**Table 6-15 Call ID Parameter Descriptions**

Parameter	Description
Caller ID Mode	Caller ID transmission mode. Options: <a href="#">FSK</a> , <a href="#">DTMF</a> , and FSK&DTMF.
ETSI CID Standard	Select the check box to follow the standard.
Caller ID Time	Whether to display incoming call time. Options: Disable, Enable, and Auto.
CID Obtain	Source of caller ID. Options: FROM Obtain Only and Priority From PAI.
Preferred Username	Specifies whether to display the username preferably.

3. Click **Submit**.

**– End of Steps –**

### 6.2.10 Configure the SLIC(SIP)

The SLIC parameter configuration for the SIP-based VoIP service is the same as that for the H248-based VoIP service. For details, refer to [6.1.11 Configure the SLIC\(H248\)](#).

## 6.3 Configure the DDNS

The [DDNS](#) feature binds a static domain name with dynamic IP addresses, so that dynamic IP addresses can be mapped into a fixed domain name resolution server. When a user tries to access the network, the client sends the dynamic IP address to the specified server, and the server provides the DNS service and implements dynamic domain name resolution.

### Steps

1. In the left navigation tree, click **Application > DDNS**. The **DDNS** page is displayed, as shown in [Figure 6-18](#).

Figure 6-18 DDNS Page

Path:Application-DDNS 中文 [Logout](#)

Enable ☐

Service Type 

dipc

Server 

http://ns.eagleeyes.com.cn/cgi-bin/g

Username

Password 

•••••

WAN Connection

Domain

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-16](#).

Table 6-16 DDNS Parameter Descriptions

Parameter	Description
Enable	To enable the DDNS feature, select this check box.
Service Type	Options: dipc, dyndns, and DtDNS.
Server	URL of the domain name resolution server.

Parameter	Description
Username	Username for accessing the domain name resolution server, which must be the same as that configured on the server.
Password	Password for accessing the domain name resolution server, which must be the same as that configured on the server.
WAN Connection	WAN connection on which the DDNS feature is enabled.
Domain	Fixed domain name assigned for the WAN connection.

3. Click **Submit**.

– End of Steps –

## 6.4 Configure the DMZ

The section describes how to configure [DMZ](#). The CPE translates the destination IP address and port number from an outside-network address (network side) to an inside-network address (user side) so that an inside-network server can be accessed.

### Steps

1. In the left navigation tree, click **Internet > Security > DMZ** to the **DMZ** page, as shown in [Figure 6-19](#).

Figure 6-19 DMZ

Path:Application-DMZ Host

中文

Logout

Enable ☐

IPv4

WAN Connection

Enable MAC Mapping

☐

DMZ Host IP Address

IPv6

The Maximum of LAN IPv6 Addresses is 8.

Add

LAN IPv6 Address

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-17](#).

Table 6-17 DMZ Parameter Descriptions

Parameter	Description
Enable	To enable the DMZ feature, select this check box.
WAN Connection	WAN connection for a host on the LAN side to provide external services.
Enable MAC Mapping	To enable MAC mapping, select this check box. <ul style="list-style-type: none"><li>If MAC mapping is enabled, you need to configure the MAC address on the LAN side.</li><li>If MAC mapping is not enabled, the system uses IP address mapping by default.</li></ul>
DMZ Host MAC Address	Mapped MAC address of a host on the LAN side for providing external services.
DMZ Host IP Address	Mapped IP address of a host on the LAN side for providing external services.
LAN IPv6 Address	IPv6 address of a host on the LAN side for providing external services. A maximum of eight IPv6 addresses is supported. To add an IPv6 address, click <b>Add</b> .

- 3. Click **Submit** button to apply the changes.
- End of Steps –

## 6.5 Configure the UPnP

This page provides the parameters of **UPnP** configuration features.

### Steps

- 1. In the left navigation tree, click **Local Network > UPnP** to the **UPnP** page, as shown in [Figure 6-20](#).

Figure 6-20 UPnP

Path:Application-UPnP 中文 [Logout](#)

Enable ☐

-IPv4-

IPv4 WAN Connection

Advertisement Period (in minutes) 

30

Advertisement Time To Live (in hops) 

4

-IPv6-

IPv6 WAN Connection

Submit

Cancel

- 2. Set the parameters. For a description of the parameters, refer to [Table 6-18](#).

Table 6-18 UPnP parameters

Parameter	Description
UPnP Switch	Click <b>On</b> to enable the UPnP function.
IPv4 WAN Connection	IPv4 WAN connection for UPnP.

Parameter	Description
Advertisement Period	Time period that the UPnP device sends an announcement packet. If the UPnP device does not send any announcement packets during this period, it indicates that the device is invalid. By default, the period is 30 minutes.
Advertisement Time To Live	The TTL for the advertisement. The advertisement will be abandoned after it has been transferred for the specified times by the routers. The default value is 4.
IPv6 WAN Connection	IPv6 WAN connection for UPnP.

3. Click **Submit** button to apply the changes.

– End of Steps –

## 6.6 Check the UPnP Port Mapping

This procedure describes how to check port mapping information of UPnP devices, including the active/standby status, protocol, internal and external ports, and IP address.

### Steps






1. In the left navigation tree, click **Application > UPnP Port Mapping**. The **UPnP Port Mapping** page is displayed, as shown in [Figure 6-21](#).





Figure 6-21 UPnP Port Mapping Page

Path:Application-UPnP Port Mapping 中文 [Logout](#)

JPNP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address	Delete
✓	TCP	843	843	192.168.1.4	
✓	TCP	16000	3643	192.168.1.4	
✓	UDP	5041	3391	192.168.1.4	
✓	TCP	9393	9393	192.168.1.4	
✓	UDP	14471	9393	192.168.1.4	

 [Refresh](#)

- Click **Refresh** to update the UPnP port mapping information.
- (Optional) To delete a mapping item, click  next to the item.

– End of Steps –

## 6.7 Configure the Port Forwarding

This procedure describes how to configure the virtual host feature, so that a host on the WAN side can serve as a client to access a server on the LAN side.

### Steps

- In the left navigation tree, click **Application > Port Forwarding**. The **Port Forwarding** page is displayed, as shown in [Figure 6-22](#).

Figure 6-22 Port Forwarding Page

Path:Application-Port Forwarding

中文

Logout

Enable☐

Name

Protocol

TCP

WAN Host Start IP Address

WAN Host End IP Address

WAN Connection

omci ipv4 static 1

WAN Start Port

(1 ~ 65535)

WAN End Port

(1 ~ 65535)

Enable MAC Mapping☐

LAN Host IP Address

LAN Host Start Port

(1 ~ 65535)

LAN Host End Port

(1 ~ 65535)

Add



Enable	Name	WAN Host Start IP Address	WAN Start Port	LAN Host Start Port	WAN Connection	Modify	Delete
	Protocol	WAN Host End IP Address	WAN End Port	LAN Host End Port	LAN Host Address		
There is no data, please add one first.							

2. Set the parameters. For a description of the parameters, refer to [Table 6-19](#). Click **Add**.

Table 6-19 Port Forwarding Parameter Descriptions

Parameter	Description
Enable	To enable the virtual host feature, select this check box.
Name	Virtual host name.
Protocol	Protocol used for access. Options: <ul style="list-style-type: none"><li>TCP (default)</li><li>UDP</li><li>TCP AND UDP</li></ul>
WAN Host Start IP Address	Start IP address of the IP range for hosts on the WAN side.

Parameter	Description
WAN Host End IP Address	End IP address of the IP range for hosts on the WAN side.
WAN Connection	WAN connection for accessing the virtual host on the LAN side.
WAN Start Port	Start port number used on the WAN side.
WAN End Port	End port number used on the WAN side.
Enable MAC Mapping	To enable the MAC mapping feature, select this check box.
LAN Host MAC Address	MAC address of the virtual host on the LAN side, valid only if MAC mapping is enabled.
LAN Host IP Address	IP address of the virtual host on the LAN side.
LAN Host Start Port	Start port number of the virtual host on the LAN side.
LAN Host End Port	End port number of the virtual host on the LAN side.

3. (Optional) To modify a virtual host, click  next to the virtual host.
4. (Optional) To delete a virtual host, click  next to the virtual host.

– End of Steps –

## 6.8 DNS Service

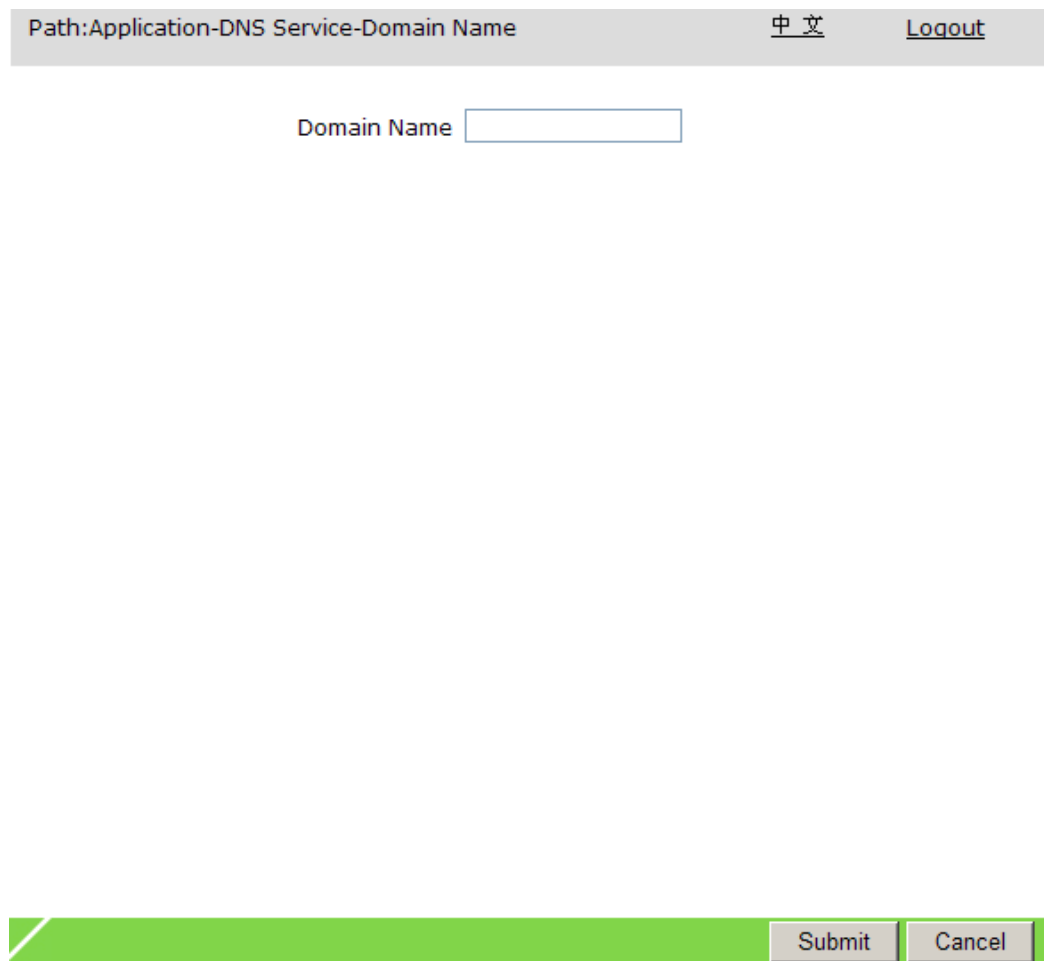
### 6.8.1 Configure the Domain Name

This procedure describes how to configure the domain name to add the ZXHN F670 into a network domain.

#### Steps

1. In the left navigation tree, click **Application > DNS Service > Domain Name**. The **Domain Name** page is displayed, as shown in [Figure 6-23](#).

Figure 6-23 Domain Name Page



Path:Application-DNS Service-Domain Name [中文](#) [Logout](#)

Domain Name

2. Enter a domain name and click **Submit**.

– End of Steps –

## 6.8.2 Configure the Hosts

This procedure describes how to establish a mapping relationship between a host name on the user side and an [IP](#) address.

### Steps

1. In the left navigation tree, click **Application > DNS Service > Hosts**. The **Hosts** page is displayed, as shown in [Figure 6-24](#).

Figure 6-24 Hosts Page

Path:Application-DNS Service-Hosts

中文

Logout

Host Name

IP Address

Add

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

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

2. Enter a host name and an IP address, and click **Add**. A configuration record is displayed after you establish a mapping relationship. You can modify or delete the configuration record as required.

– End of Steps –

### 6.8.3 Configure the DNS Servers

This procedure describes how to configure global [DNS](#) servers, so that features without specified WAN connections can use these global DNS servers for data transmission.

#### Steps

1. In the left navigation tree, click **Application > DNS Service > DNS**. The **DNS** page is displayed, as shown in [Figure 6-25](#).

Figure 6-25 DNS Page

Path:Application-DNS Service-DNS 中文 Logout

IPv4 DNSServer1

IPv4 DNSServer2

IPv6 DNSServer1

IPv6 DNSServer2

2. Enter the IPv4 and IPv6 addresses of DNS servers, and click **Submit**.

– End of Steps –

## 6.9 Configure the Time Parameters

This procedure describes how to configure time parameters for the ZXHN F670.

### Steps

1. In the left navigation tree, click **Application > SNTP**. The **SNTP** page is displayed, as shown in [Figure 6-26](#).

Figure 6-26 SNTP Page

Path:Application-SNTP

中文Logout

Current Date and Time 1970-01-04 23:21:55

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

Primary NTP Server Address

Secondary NTP Server Address

Poll Interval 86400sec

SubmitCancel

2. Set the parameters. For a description of the parameters, refer to Table 6-20.

Table 6-20 Time Parameter Descriptions

Parameter	Description
Time Zone	Time zone where the ZXHN F670 is located .
Primary NTP Server Address	IP address or domain name of the active NTP server .
Secondary NTP Server Address	IP address or domain name of the standby NTP server .
Poll Interval	Interval at which the ZXHN F670 sends a synchronization request to the NTP server, range: 3600~86400, default: 86400, unit: seconds.

3. Click **Submit**.
- End of Steps –

## 6.10 Multicast Configuration

### 6.10.1 Configure the IGMP WAN Connection

This procedure describes how to configure an IGMP WAN connection for the ZXHN F670.

### Steps

1. In the left navigation tree, click **Application > MultiCast > IGMP WAN Connection**. The **IGMP WAN Connection** page is displayed, as shown in [Figure 6-27](#).

**Figure 6-27 IGMP WAN Connection Page**

2. Select a WAN connection from the **WAN Connection** list, and click **Add**. You can delete an existing IGMP WAN connection as required.

– End of Steps –

## 6.10.2 Configure the Multicast Mode

This procedure describes how to configure the multicast mode.

### Steps

1. In the left navigation tree, click **Application > MultiCast > MultiCast Mode**. The **MultiCast Mode** page is displayed, as shown in [Figure 6-28](#).



Figure 6-28 MultiCast Mode Page

Path:Application-MultiCast-MultiCast Mode 中文 [Logout](#)

MultiCast Mode

- Set the parameter. For a description of the parameter, refer to [Table 6-21](#).

Table 6-21 MultiCast Mode Parameter Description

Parameter	Description
MultiCast Mode	IGMP mode that the ZXHN F670 supports. Options: <ul style="list-style-type: none"><li>● <b>Disable</b>: The ZXHN F670 does not process IGMP packets.</li><li>● <b>Snooping</b>: The device transparently transmits the multicast protocol messages and records the information of the multicast group.</li><li>● <b>Proxy</b>: The device intercepts multicast protocol messages, transmits the messages after processing them in accordance with the multicast protocol, and records the information of the multicast group. The <b>IGMP WAN Connection</b> configuration is effective only if this parameter is set to <b>Proxy</b>.</li></ul>

- Click **Submit**.

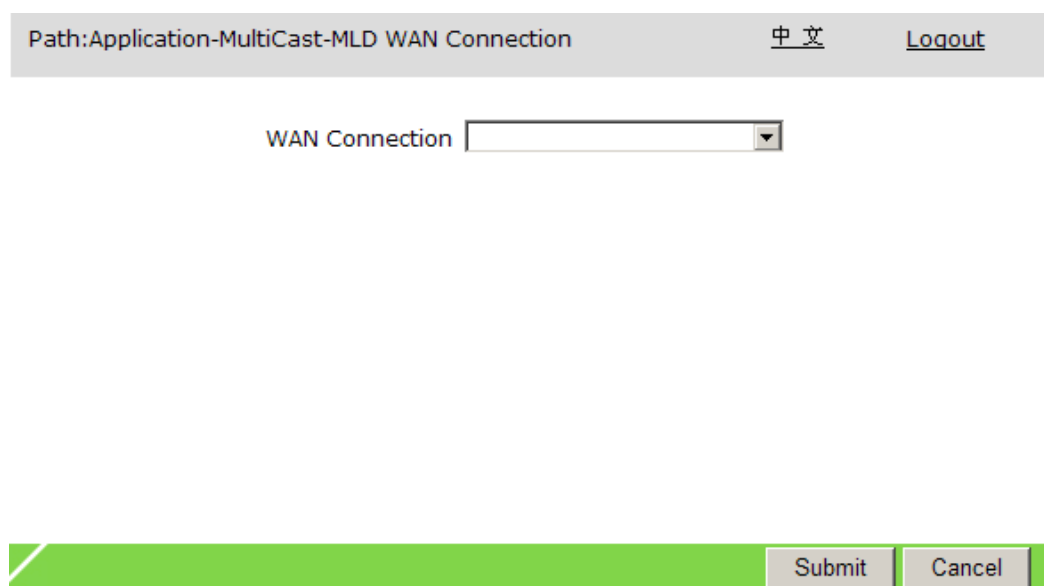
– End of Steps –

### 6.10.3 Configure the MLD WAN Connection

**MLD** is the IPv6 version of IGMP. This procedure describes how to configure an MLD WAN connection.

#### Steps

- In the left navigation tree, click **Application > MultiCast > MLD WAN Connection**. The **MLD WAN Connection** page is displayed, as shown in [Figure 6-29](#).

**Figure 6-29 MLD WAN Connection Page**

Path:Application-MultiCast-MLD WAN Connection      中文      [Logout](#)

WAN Connection

2. Select a WAN connection, and click **Submit**.

– End of Steps –

## 6.10.4 Configure the Basic Parameters of Multicast

**MLD** is the IPv6 version of IGMP. This procedure describes how to configure an MLD WAN connection.

### Steps

1. In the left navigation tree, click **Application > MultiCast > Basic Configuration**. The **Basic Configuration** page is displayed, as shown in [Figure 6-30](#).

Figure 6-30 Basic Configuration Page

Path:Application-MultiCast-Basic Configuration

中文Logout

Aging Time

300

(1-604800) sec

Non-fast Leave

☐

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 6-22](#).

Table 6-22 Basic Parameters of Multicast Description

Parameter	Description
Aging Time	Delay time for multicast records to be deleted from the ONU. Unit: seconds.
Non-fast Leave	<ul style="list-style-type: none"><li>If this option is selected: When receiving a leave message, the ONU sends a multicast query message, and then proceeds in accordance with the response.</li><li>If this option is not selected: When receiving a leave message, the ONU immediately deletes the multicast group and disconnects the multicast stream.</li></ul>

3. Click **Submit**.
- End of Steps –

### 6.10.5 Configure the VLAN

This procedure describes how to configure the VLAN.


### Steps

1. In the left navigation tree, click **Application > MultiCast > VLAN Configuration**. The **VLAN Configuration** page is displayed, as shown in [Figure 6-31](#).

**Figure 6-31 VLAN Configuration Page**

Path:Application-MultiCast-VLAN Configuration

[中文](#)
[Logout](#)


VLAN Configuration only takes effect in IGMP Snooping,IGMP Proxy,MLD Snooping and MLD Proxy modes.

Port

SSID1

MultiCast VLAN
(1-4094)

Add

Port	MultiCast VLAN	Delete
There is no data, please add one first.		

2. Set the parameters. For a description of the parameters, refer to [Table 6-23](#).

**Table 6-23 VLAN Parameter Descriptions**

Parameter	Description
Port	Port number of the ZXHN F670 on the user side. The options include LAN1~LAN4 and SSID1~SSID8.
MultiCast VLAN	VLAN of devices on the OLT side.

3. Click **Add**. A configuration record is displayed after you complete a configuration operation. You can delete an existing configuration record as required.

– End of Steps –

## 6.10.6 Configure the Maximum Number of Addresses


This procedure describes how to configure the maximum number of addresses for each port.

### Steps


1. In the left navigation tree, click **Application > MultiCast > Maximum Address Configuration**. The **Maximum Address Configuration** page is displayed, as shown in [Figure 6-32](#).

Figure 6-32 Maximum Address Configuration Page

Path: Application-MultiCast-Maximum Address Configuration      [中文](#)      [Logout](#)

 The Maximum Number of Addresses is 1024.

Port	Maximum Number of Addresses
LAN1	<input type="text" value="1024"/>
LAN2	<input type="text" value="1024"/>
LAN3	<input type="text" value="1024"/>
LAN4	<input type="text" value="1024"/>
SSID1	<input type="text" value="1024"/>
SSID2	<input type="text" value="1024"/>
SSID3	<input type="text" value="1024"/>
SSID4	<input type="text" value="1024"/>
SSID5	<input type="text" value="1024"/>
SSID6	<input type="text" value="1024"/>
SSID7	<input type="text" value="1024"/>
SSID8	<input type="text" value="1024"/>



2. Set the maximum number of addresses for each port, and click **Submit**.

– End of Steps –

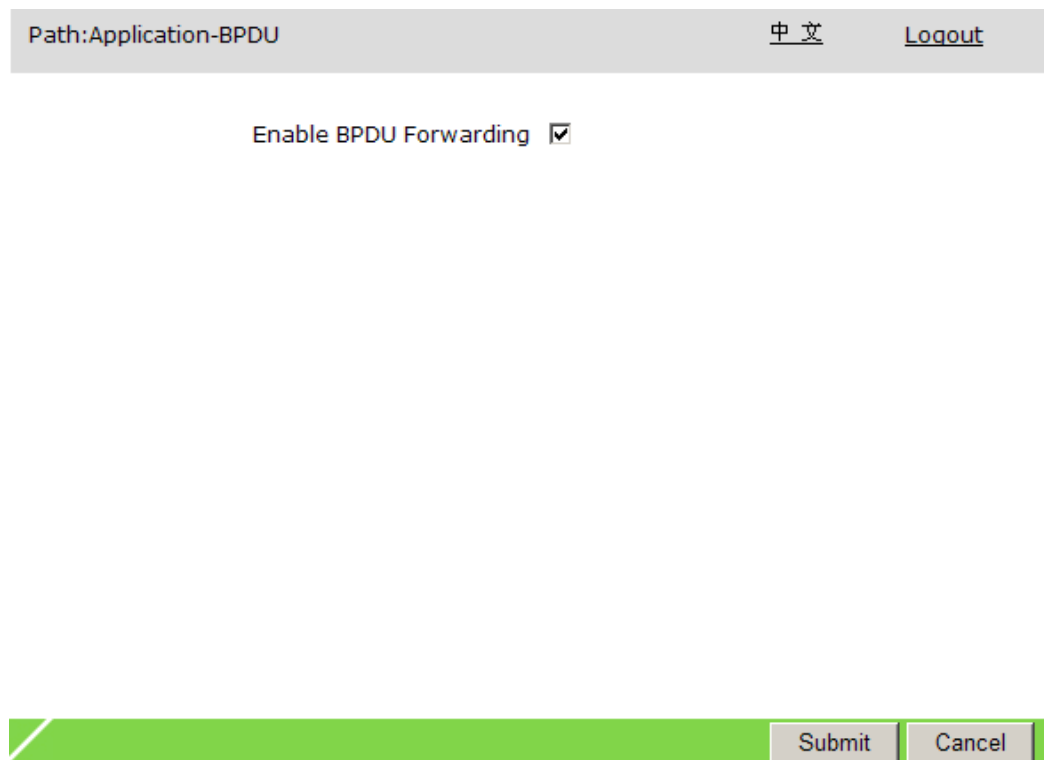
## 6.11 Configure the BPDU

If the [BPDU](#) feature is enabled, the ZXHN F670 can transparently transfer BPDU packets as required by ONT in some applications.

### Steps

1. In the left navigation tree, click **Application > BPDU**. The **BPDU** page is displayed, as shown in [Figure 6-33](#).

Figure 6-33 BPDU Page



2. To enable the BPDU feature, select the **Enable BPDU Forwarding** check box. Click **Submit**.

– End of Steps –

## 6.12 Check the USB Storage Information

If a storage device is connected to the USB interface, you can check the storage device information, including the disk name, partitions, and capacity.

### Steps

1. In the left navigation tree, click **Application > USB Storage**. The **USB Storage** page is displayed, as shown in [Figure 6-34](#).

Figure 6-34 USB Storage Page

Path:Application-USB Storage		<a href="#">中文</a>	<a href="#">Logout</a>
Disk Name	<input type="text" value="Kingston"/>		
Status	<input type="text" value="Mounted"/>		
File System	<input type="text" value="FAT"/>		
Total Size	<input type="text" value="1956224 KB"/>		
Free Size	<input type="text" value="1016192 KB ( 48% used )"/>		
Path	<input type="text" value="/mnt/usb1_1"/>		

Refresh

2. (Optional) Click **Refresh** to refresh the page.

– End of Steps –

## 6.13 Configure the DMS

The section describes how to configure [DMS](#). **DMS** provides the parameters of DMS configuration features.

DMS is a multimedia server defined in [DLNA](#) protocol, which uses [UPnP](#) protocol to search and categorize the local media files or photos, and provide [VOD](#) services for the DMP.

If the [DMS](#) function is enabled on the ZXHN F670 device, any client that supports UPnP function can use the specified DMP (for example, windows media player) to watch the media files or photos stored in the USB storage device.

The version of the windows media player used for DMS function must be 11 or later, or the OS must be vista or Win 7. To enable the DMP function in OS of earlier version, special tools, such as Intel(R) Tool for UPnP(TM) Technology or Twonky Media Manager must be installed.

### Steps

1. In the left navigation tree, click **Application > DMS** to go to the **DMS** page, as shown in [Figure 6-35](#).

Figure 6-35 DMS page

Path:Application-DMS

中文

Logout

Enable ☐

DMS Name

Library Rescan Method 

Auto

Media Source 1

Browse

Media Source 2

Browse

Media Source 3

Browse

Media Source 4

Browse

Submit

Cancel

2. Enable the DMS function, and specify the path storing the media files. For a description of the parameters, refer to [Table 6-24](#).

Table 6-24 Parameter Descriptions for the DMS

Parameter	Description
Enable	Select the check box to enable the DMS function.
DMS Name	To create a DMS, enter the name of the DMS.
Library Rescan Method	Library rescan method that the device supports. Normally, it is set to Auto.
Media Source1–Media Source4	By default, the media source is <code>/mnt</code> , that is the root directory of the USB device. You can change the root directory to other directory of the USB storage device.



**Note:**

By default, the media source is `/mnt`, that is the root directory of the USB device. You can change the root directory to other directory of the USB storage device.

3. Click **Submit** button to apply the changes.

– End of Steps –

## 6.14 Configure the FTP Server Feature

This procedure describes how to enable the [FTP](#) feature of the ZXHN F670 by configuring FTP parameters, including the username and password.

### Steps

1. In the left navigation tree, click **Application > FTP Application**. The **FTP Application** page is displayed, as shown in [Figure 6-36](#).

**Figure 6-36 FTP Application Page**

Path:Application-FTP Application      中文      [Logout](#)

Enable FTP Server ☒

FTP Username

FTP Password

[Refresh](#)

2. Set the parameters. For a description of the parameters, refer to [Table 6-25](#).

**Table 6-25 FTP Server Parameter Descriptions**

Parameter	Description
Enable FTP Server	To enable the FTP server feature, select this check box.
FTP Username/FTP Password	Valid only if FTP security control is enabled.

3. Click **Submit**.

– End of Steps –

## 6.15 Configure the Port Triggering

This procedure describes how to specify a triggering port. If an application uses a triggering port to establish a connection with an external network, the router connected to the system forwards application data to an internal forwarding port.

Port triggering ensures port security. The system does not need to open triggering ports, unless they is triggered.

### Steps

1. In the left navigation tree, click **Application > Port Trigger**. The **Port Trigger** page is displayed, as shown in [Figure 6-37](#).

Figure 6-37 Port Trigger Page

Path:Application-Port Trigger

中文

Logout

Enable Port Triggering☐

Application

Triggering IP Address

Service Type

TCP

Triggering Port

Connection Type

TCP

WAN Start Port

WAN End Port

Timeout

1200

(60 ~ 1800 sec)

Add



Application	Enable Port Triggering	Service Type	Triggering IP Address	WAN Start Port	Modify	Delete
	Timeout	Connection Type	Triggering Port	WAN End Port		
There is no data, please add one first.						

2. Set the parameters. For a description of the parameters, refer to Table 6-26. Click **Add**.

Table 6-26 Port Triggering Parameter Descriptions

Parameter	Description
Enable Port Triggering	To enable port triggering, select this check box.
Application	Name of the port triggering configuration record.
Triggering IP Address	IP address that the device needs to access.
Service Type	Application service type. Options: TCP, UDP, and TCP AND UDP. Default: TCP.
Triggering Port	Protocol port that the device needs to access. This parameter must be specified.
Connection Type	Type of connection to an external router. Options: <ul style="list-style-type: none"><li>TCP (default)</li><li>UDP</li><li>TCP AND UDP</li></ul>

Parameter	Description
WAN Start Port/WAN End Port	Range of the protocol ports that trigger port mapping (layer-4 port numbers). Once the device accesses the triggering port, the services corresponding to the ports within the port range are started. This parameter must be specified. The differences between the start port and the end port ranges from 1 to 9.
Timeout	If there is no traffic on the triggering port within a particular period, timeout occurs.

- (Optional) To modify a configuration record, click  next to the configuration record.
- (Optional) To delete a configuration record, click  next to the configuration record.

– End of Steps –

## 6.16 Configure the Port Forwarding(Application List)

This procedure describes how to configure a virtual host, which allows a client on the WAN side to access the server on the LAN side.


### Steps

- In the left navigation tree, click **Application > Port Forwarding(Application List)**. The **Port Forwarding (Application List)** page is displayed, as shown in [Figure 6-38](#).

**Figure 6-38 Port Forwarding (Application List) Page**

Path:Application-Port Forwarding ( Application List )

[中文](#)
[Logout](#)


If the number of the applications applied to virtual server exceed virtual server's maximum, the applications exceeding the maximum will be ineffective.

WAN Connection 
LAN Host IP Address 
AppName

WAN Connection	LAN Host IP Address	AppName	Delete
There is no data, please add one first.			

- Set the parameters and click **Add**. For a description of the parameters, refer to [Table 6-27](#).

Table 6-27 Port Forwarding Parameter Descriptions

Parameter	Description
WAN Connection	WAN connection of the virtual host on the user side.
LAN Host IP Address	IP address of the host on the LAN side.
AppName	It must be already configured in <b>Application &gt; Application List</b> .

3. (Optional) To delete a configuration record, click  next to the configuration record.

– End of Steps –

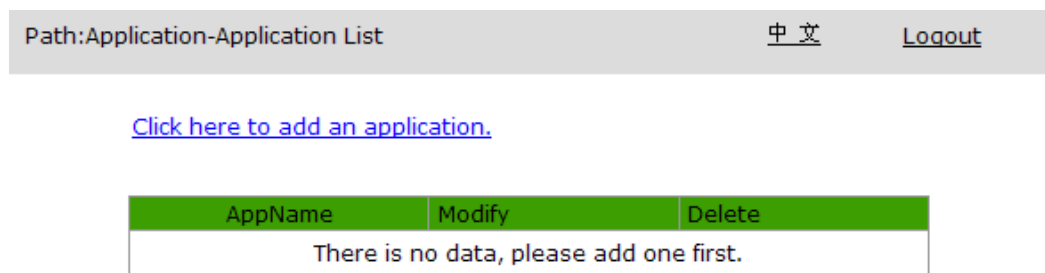
## 6.17 Configure the Application List

This procedure introduces how to configure the application list function.

### Steps

1. In the left navigation tree, click **Application > Application List**. The **Application List** page is displayed, as shown in Figure 6-39.

Figure 6-39 Application List Page





2. (Optional) To modify a configuration record, click  next to the configuration record.
3. (Optional) To delete a configuration record, click  next to the configuration record.
4. Click **Click here to add an application**. The application list adding page is displayed, as shown in Figure 6-40.

Figure 6-40 Application List Adding Page

Path:Application-Application List

中文

Logout

Application Name

App1

(1 ~ 256 characters)

Save

Protocol

TCP

WAN Start Port

(1 ~ 65535)

WAN End Port

(1 ~ 65535)

Start Mapping Port

(1 ~ 65535)

End Mapping Port

(1 ~ 65535)

Add

Protocol	WAN Start Port	WAN End Port	Map Start Port	Map End Port	Modify	Delete
There is no data, please add one first.						

5. Set the parameters and click **Add**. For a description of the parameters, refer to [Table 6-28](#).

Table 6-28 Application List Parameter Descriptions

Parameter	Description
Application Name	Create an application name.
Protocol	Protocol of the permitted packet including TCP, UDP , TCP AND UDP.
WAN Start Port / WAN End Port	Port number range of the WAN-side hosts.
Start Mapping Port/End Mapping Port	Port number range of the mapping-side hosts.

– End of Steps –

## 6.18 Configure the Samba Service

Samba is a software program used for the [SMB](#) feature. By enabling the Samba server for the ZXHN F670, files can be transferred between the Linux system and the Windows system. The SMB protocol is a file and printer sharing protocol operating over a LAN. It provides the file system and printing services or other information for other hosts with Windows and Linux systems within the same LAN.

## Steps

1. In the left navigation tree, click **Application > Samba Service**. The **Samba Service** page is displayed, as shown in [Figure 6-41](#).

**Figure 6-41 Samba Service Page**

Path:Application-Samba Service 中文 [Logout](#)

Enable Samba Server ☐

Auto Run Samba Server ☐

Host Name  (2 ~ 15 characters)

Anonymous ☐

Samba Username  (1 ~ 32 characters)

Samba Password  (0 ~ 32 characters)

2. Set the parameters. For a description of the parameters, refer to [Table 6-29](#).

**Table 6-29 Samba Server Parameter Descriptions**

Parameter	Description
Enable Samba Server	To enable the Samba server feature, select this check box. By default, the Samba server feature is disabled, and is mutually exclusive to the <b>Auto Run Samba Server</b> parameter.
Auto Run Samba Server	If this check box is selected, when a USB storage device is connected to the USB interface of the ONU, the Samba server feature is automatically enabled. After the USB storage device is removed, the Samba server feature is automatically disabled. By default, this parameter is not selected, and is mutually exclusive to the <b>Enable Samba Server</b> parameter.
Host Name	Samba server name, range: 2–15 characters.
Samba Username	Username for logging in to the Samba server, which must be the same as that configured on the server.
Samba Password	Password for logging in to the Samba server, which must be the same as that configured on the server.

3. Click **Submit**.

**Note:**

After the Samba server feature is enabled, a PC on the LAN side can access the Samba server by entering the \\Samba server name in the address bar of a browser, for example, \\smbshare.

– End of Steps –

## 6.19 Configure the USB Print Server

This procedure describes how to enable the USB print server feature for the ZXHN F670. If this feature is enabled, users connected to the ZXHN F670 can use the printing service.

### Steps

1. In the left navigation tree, click **Application > USB print server**. The **USB print server** page is displayed, as shown in [Figure 6-42](#).

**Figure 6-42 USB Print Server Page**

Path:Application-USB print server 中文 [Logout](#)

Enable USB print server ☐

[Submit](#) [Cancel](#)



2. To enable the USB print server feature, select the **Enable USB print server** check box.

**– End of Steps –**

# Chapter 7

## Administration Management

---

### Table of Contents

Remote Management.....	7-1
Configure the Web User Management.....	7-4
Configure the Login Timeout .....	7-5
Device Management .....	7-6
Configure the Log Management .....	7-12
Diagnosis and Maintenance .....	7-14
Loopback Detection.....	7-26
Configure the IPv6 Switch .....	7-30
Configure the VoIP Protocol .....	7-31
Configure the 3G Switch .....	7-32

## 7.1 Remote Management

### 7.1.1 Configure the Basic Parameters of TR-069

This procedure describes how to configure basic parameters for remote management, including the WAN connection and URL of the management server.

#### Steps

1. In the left navigation tree, click **Administration > TR-069 > Basic**. The **Basic** page is displayed, as shown in [Figure 7-1](#).

Figure 7-1 TR-069 Basic Page

Path:Administration-TR-069-Basic

中文

Logout

WAN Connection

ACS URL

Username

Password

Connection Request URL

Connection Request Username

Connection Request Password

Enable Periodic Inform

Periodic Inform Interval

sec

Enable Certificate

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 7-1](#).

Table 7-1 Basic Parameter Descriptions for Remote Management

Parameter	Description
WAN Connection	Select a WAN connection created in <b>Network &gt; WAN</b> . The <b>Service List</b> parameter of the WAN connection must be set to <b>TR069</b> .
ACS URL	IP address or domain name of the remote management server.
Username	Username that the ZXHN F670 uses for accessing the management server, which must be the same as that configured on the management server.
Password	Password that the ZXHN F670 uses for accessing the management server, which must be the same as that configured on the management server.
Connection Request URL	Local address of the ZXHN F670 for communicating with the management server.
Connection Request Username	Username that the management server uses for accessing the ZXHN F670.

Parameter	Description
Connection Request Password	Password that the management server uses for accessing the ZXHN F670.
Enable Periodic Inform	Specifies whether to enable the periodic message reporting feature. The ZXHN F670 sends messages to the management server for link detection.
Periodic Inform Interval	Interval for sending link detection messages.
Enable Certificate	Specifies whether to enable the CA feature. If this check box is selected, you must load a CA certificate in <b>Administration &gt; TR-069 &gt; Certificate</b> .

- Click **Submit**.

– End of Steps –

## 7.1.2 Configure the Certificate


The ZXHN F670 supports security control for the management server and clients through CA. This procedure describes how to upload certificates for authentication.

### Steps

- In the left navigation tree, click **Administration > TR-069 > Certificate**. The **Certificate** page is displayed, as shown in [Figure 7-2](#).

**Figure 7-2 Certificate Page**

Path:Administration-TR-069-Certificate
[中文](#)
[Logout](#)


The uploaded certificate will take effect only after the device reboot.

ACS Interactive Certificate

Please select an ACS CA Certificate

Please select a Client Certificate

- Click **Browse** to select a certificate.
- Click **Import Certificate**.

**Note:**

The uploaded certificates take effective only after the device is restarted.

– End of Steps –

## 7.2 Configure the Web User Management

The ZXHN F670 provides the user management function. Through the page, you can manage your account and create common user accounts.

### Steps

1. In the left navigation tree, click **Administration > User Management**. The **WEB User Management** page is displayed, as shown in [Figure 7-3](#).

**Figure 7-3 WEB User Management Page**

Path:Administration-User Management-WEB User Management      中文      [Logout](#)

User Privilege: ☒ Administrator  
☐ User

Username

Old Password

New Password

Confirmed Password

2. Modify your password as required, and click **Submit**.

**Note:**

Users include the administrator and common users. The administrator username cannot be modified, and common users can manage their own account information only.

– End of Steps –

## 7.3 Configure the Login Timeout

This procedure describes how to configure the ZXHN F670 login timeout time.

### Steps


1. In the left navigation tree, click **Administration > Login Timeout**. The **Login Timeout** page is displayed, as shown in [Figure 7-4](#).

**Figure 7-4 Login Timeout Page**

Path:Administration-Login Timeout

中文

Logout



1.Any value between 1 minute and 30 minutes is allowed.

2.The changes of Timeout take effect after re-login.

Timeout

minute(s)

Submit

Cancel

2. Set the timeout time, and click **Submit**.

**Note:**

The timeout configuration takes effect after you re-log in to the system.

– End of Steps –

## 7.4 Device Management

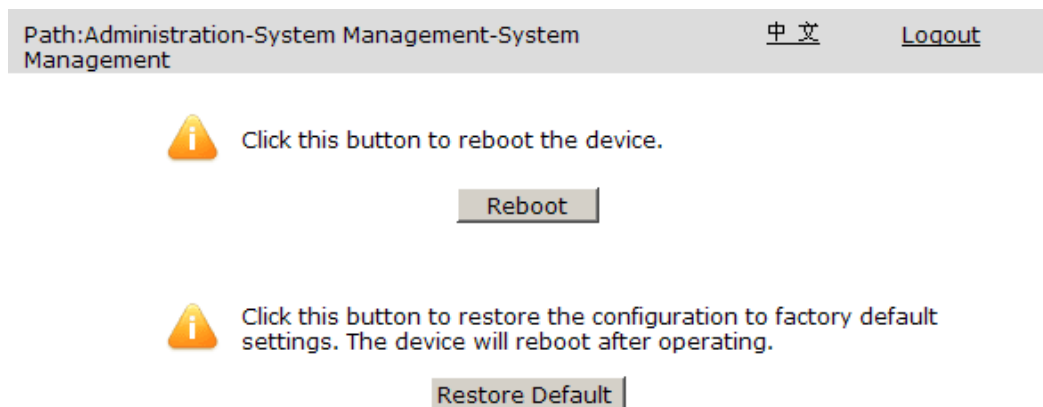
### 7.4.1 Configure the System Management

This procedure describes how to restart or reset the device.

#### Steps

1. In the left navigation tree, click **Administration > System Management**. The **System Management** page is displayed by default, as shown in [Figure 7-5](#).

**Figure 7-5 System Management Page**



2. To restart the device, click **Reboot**.
3. To restore the default configuration, click **Restore Default**.

– End of Steps –

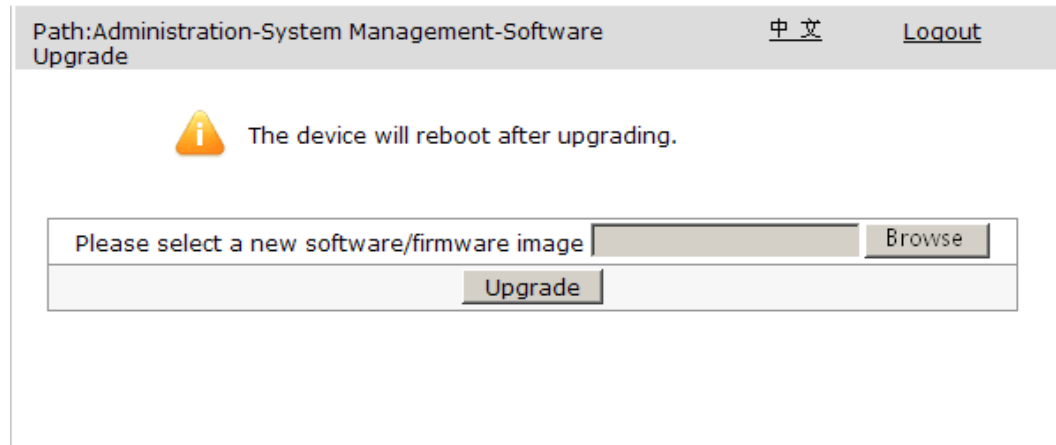
### 7.4.2 Configure the Software Upgrade

The ZXHN F670 supports local upgrade by uploading an upgrade file. Before upgrade, prepare the upgrade file, store the file on the local disk, and back up user data. The device is automatically restarted after upgrade is completed.


### Steps

1. In the left navigation tree, click **Administration > System Management > Software Upgrade**. The **Software Upgrade** page is displayed, as shown in [Figure 7-6](#).

**Figure 7-6 Software Upgrade Page**



Path:Administration-System Management-Software Upgrade      [中文](#)      [Logout](#)

 The device will reboot after upgrading.

Please select a new software/firmware image

2. Click **Browse** to select an upgrade file.
3. Click **Upgrade**. After the upgrade is completed, a message box is displayed.

– End of Steps –

## 7.4.3 Configure the User Configuration Management


This procedure describes how to back up or restore your user configuration file. The backup operation is used for routine maintenance, and the restoration operation is used for troubleshooting.

### Steps

1. In the left navigation tree, click **Administration > System Management > User Configuration Management**. The **User Configuration Management** page is displayed, as shown in [Figure 7-7](#).



**Figure 7-7 User Configuration Management Page**

Path:Administration-System Management-User Configuration Management	中文	Logout
Backup user configuration file from the device		
<input type="button" value="Backup Configuration"/>		
 The device will reboot after operating.		
Please select a user configuration file <input type="text"/>		
<input type="button" value="Browse"/>		
<input type="button" value="Restore Configuration"/>		

2. Backing up your user configuration file
  - a. Click **Backup Configuration**. The **File Download** dialog box is displayed.
  - b. Click **Save** and select a storage path.
3. Restoring your backup user configuration file
  - a. Click **Browse** to select a backup file to be restored.
  - b. Click **Restore Configuration**.

**Note:**

After the restoration operation is completed, the device is automatically restarted, causing temporary service interruption, so perform this operation with care.

– End of Steps –

## 7.4.4 Configure the Default Configuration Management

This procedure describes how to manage the default configuration file for the ZXHN F670.

### Steps


1. In the left navigation tree, click **Administration > System Management > Default Configuration Management**. The **Default Configuration Management** page is displayed, as shown in [Figure 7-8](#).

**Figure 7-8 Default Configuration Management Page**

Path:Administration-System Management-User Configuration Management	<a href="#">中文</a>	<a href="#">Logout</a>
---	--------------------	------------------------

Backup user configuration file from the device

Backup Configuration

 The device will reboot after operating.

Please select a user configuration file

Browse

Restore Configuration

2. Backing up the default configuration file
  - a. Click **Backup Configuration**. The **File Download** dialog box is displayed.
  - b. Click **Save** and select a storage path.
3. Restoring the default configuration file
  - a. Click **Browse** to select the backup default configuration file to be restored.
  - b. Click **Restore Configuration**.

– End of Steps –

## 7.4.5 Configure the Remote Upgrade


The ZXHN F670 provides the remote upgrade function. This procedure describes how to configure the URLs for remotely upgrading the configuration file and version file.

### Steps

1. In the left navigation tree, click **Administration > System Management > Remote Upgrade**. The Remote Upgrade page is displayed, as shown in [Figure 7-9](#).

Figure 7-9 Remote Upgrade Page

Path:Administration-System Management-Remote Upgrade [中文](#) [Logout](#)

 The device will reboot after upgrading.

The URL should be formatted as  
`http://ipaddress_or_domainname[:port]/pathname/filename`  
or  
`ftp://username:password@ipaddress_or_domainname[:port]/pathname/filename`

Configuration File URL

Firmware URL

2. Remotely upgrade the version file or configuration file.
    - a. Enter the root directory of the configuration file in **Configuration File URL**, and click **Upgrade**.
    - b. Enter the root directory of the version file in **Firmware URL**, and click **Upgrade**.
- End of Steps –

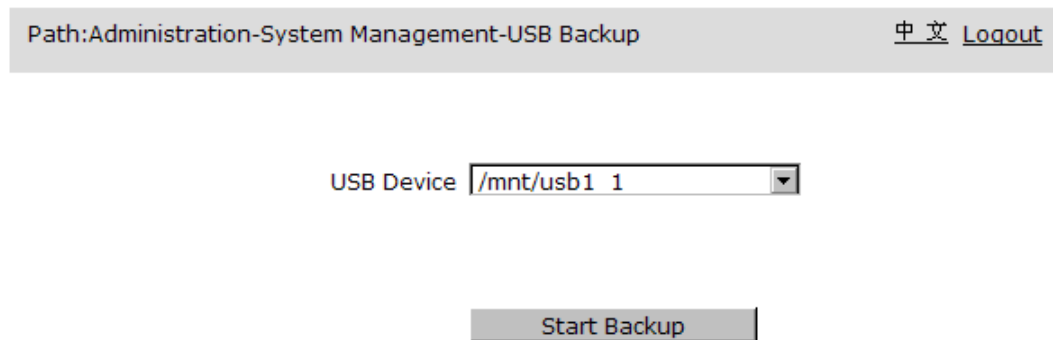
## 7.4.6 Configure the USB Backup

With the USB backup function, the ZXHN F670 can back up your configuration file and store it on a USB storage device through the USB interface.

### Steps

1. In the left navigation tree, click **Administration > System Management > USB Backup**. The **USB Backup** page is displayed, as shown in [Figure 7-10](#).

Figure 7-10 USB Backup Page



Path:Administration-System Management-USB Backup [中文](#) [Logout](#)

USB Device

Start Backup

2. Select a USB device from the **USB Device** list, and click **Start Backup**.

– End of Steps –

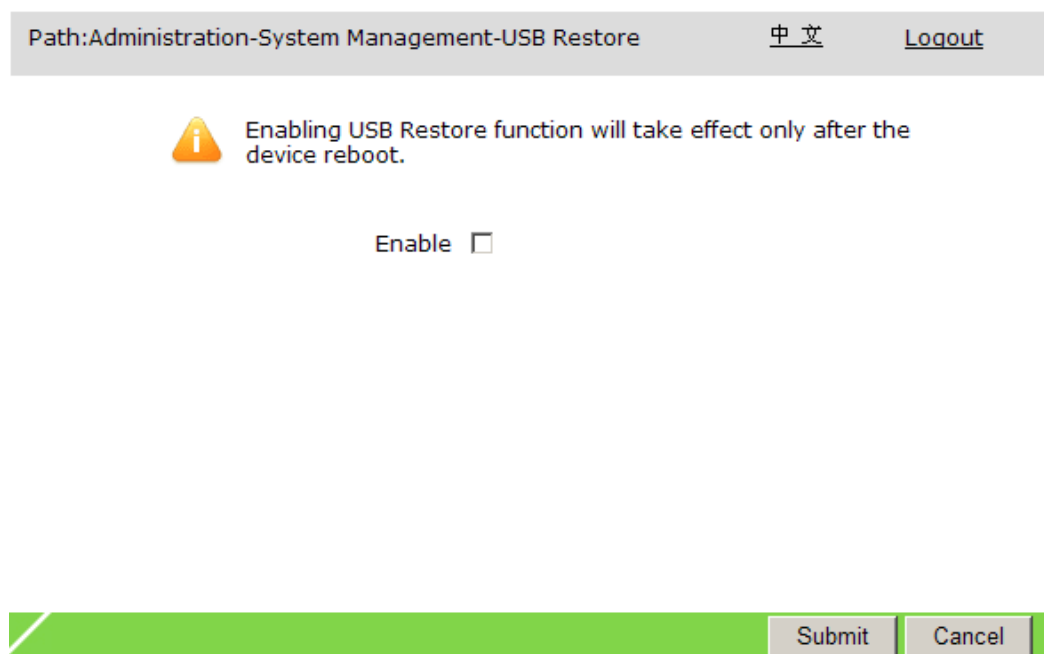
## 7.4.7 Configure the USB Restoration

The ZXHN F670 can restore your backup configuration file on a USB storage device through the USB interface.


### Steps

1. In the left navigation tree, click **Administration > System Management > USB Restore**. The **USB Restore** page is displayed, as shown in [Figure 7-11](#).

Figure 7-11 USB Restore Page



Path:Administration-System Management-USB Restore      中文      [Logout](#)

 Enabling USB Restore function will take effect only after the device reboot.

Enable ☐

[Submit](#) [Cancel](#)

2. To enable the USB restoration function, select the **Enable** check box, and click **Submit**.

– End of Steps –

## 7.5 Configure the Log Management

This procedure describes how to configure the log management function of the ZXHN F670.

### Steps

1. In the left navigation tree, click **Administration > Log Management**. The **Log Management** page is displayed, as shown in [Figure 7-12](#).

Figure 7-12 Log Management Page

Path:Administration-Log Management中文[Logout](#)

Enable Save Log ☐

Log Level 

Error

Refresh

Clear Log

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 7-2](#).

Table 7-2 Log Management Parameter Descriptions

Parameter	Description
Enable Save Log	Specifies whether to enable the log file storage function.
Log Level	<div>Options (ranked from low to high):<ul style="list-style-type: none"><li>● Debug</li><li>● Informational</li><li>● Notice</li><li>● Warning</li><li>● Error</li><li>● Critical</li><li>● Alert</li><li>● Emergency</li></ul>The system stores only the logs of the selected level and above levels.</div>

3. Click **Refresh** to show the latest logs.

4. Click **Clear Log** to clear the current logs.
5. Click **Download Log** to store log files on the local disk.
6. Click **Submit**.

– End of Steps –

## 7.6 Diagnosis and Maintenance

### 7.6.1 Configure the Ping Diagnosis

This procedure describes how to configure ping diagnosis for link detection.

#### Steps

1. In the left navigation tree, click **Administration > Diagnosis**. The **Ping Diagnosis** page is displayed by default, as shown in [Figure 7-13](#).

**Figure 7-13 Ping Diagnosis Page**

Path:Administration-Diagnosis-Ping Diagnosis      中文      Logout

IP Address or Host Name

Egress

2. Set the parameters. For a description of the parameters, refer to [Table 7-3](#).

**Table 7-3 Ping Diagnosis Parameter Descriptions**

Parameter	Description
IP Address or Host Name	Destination IP address or host name to be ping.
Egress	To detect the connection with an external address, select a WAN connection.

3. Click **Submit**. The system starts pinging the specified address. The system performs ping operations for four times by default, and the operation results are displayed in the bottom box.

– End of Steps –

## 7.6.2 Configure the Trace Route Diagnosis

Trace Route can detect the complete path from the source to the destination, including all the nodes that packets pass through. If a ping operation fails, Trace Route can detect the failed node.

### Steps

1. In the left navigation tree, click **Administration > Diagnosis > Trace Route Diagnosis**. The **Trace Route Diagnosis** page is displayed, as shown in [Figure 7-14](#).



Figure 7-14 Trace Route Diagnosis Page

Path:Administration-Diagnosis-Trace Route Diagnosis 中文 [Logout](#)

IP Address or Host Name

WAN Connection

Maximum Hops  (1 ~ 64)

Wait Time  (2000 ~ 10000 ms)

Protocol 

UDP

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 7-4](#).

Table 7-4 Parameter Descriptions for Trace Route Diagnosis

Parameter	Description
IP Address or Host Name	Destination IP address or host name for the Trace Route operation.
WAN Connection	To detect the connection with an external address, select a WAN connection.
Maximum Hops	Maximum number of hops that the Trace Route packets require for arriving at the destination, default: 30.
Wait Time	Time allowed for receiving a response in ms. If no response is received during this period, an asterisk is displayed. If multiple asterisks are displayed, it indicates that the corresponding node fails.
Protocol	Options: <a href="#">UDP</a> and <a href="#">ICMP</a> .

3. Click **Submit**. The result is displayed in the bottom box.

– End of Steps –

### 7.6.3 Configure the Simulation

The system can simulate scenarios where terminals such as PCs and set-top boxes initiate PPPoE dial-up or IPoE services, so that link detection can be implemented.

#### Steps

1. In the left navigation tree, click **Administration > Diagnosis > Simulation**. The **Simulation** page is displayed, as shown in [Figure 7-15](#).

Figure 7-15 Simulation Page

Path:Administration-Diagnosis-Simulation

中文

Logout

Simulation Type

PPPoE

Port

LAN1

Enable VLAN

☐

VLAN ID

(1 ~ 4094)

802.1p

0

Username

Password

Authentication Type

Auto

Retry Times

Simulation Result

Start

Stop

2. Set the parameters. For a description of the parameters, refer to [Table 7-5](#).

Table 7-5 Simulation Parameter Descriptions

Parameter	Description
Simulation Type	Simulated service type. Options: PPPoE and IPoE.

Parameter	Description
Port	Port on the user side that the simulation uses.
Enable VLAN	Specifies whether to carry a VLAN tag in the packets sent over the WAN connection. By default, this check box is not selected. If it is selected, a VLAN tag is carried in the packets sent over the WAN connection, and the <b>VLAN ID</b> must be set.
VLAN ID.	Identifies a VLAN. Range: 1–4094. To ensure normal service operation, the VLAN ID must be the same as that set in upper-layer OLT configuration.
802.1p	If VLAN is enabled, you can modify service priority through this parameter. Range: 0–7. A higher number indicates a higher priority.
Username	Username of the PPPoE account. The username must be the same as that set on the peer server for authentication.
Password	Password of the PPPoE account. The username must be the same as that set on the peer server for authentication.
Authentication Type	It must be the same as that set on the peer server. Normally, it is set to <b>Auto</b> . <ul style="list-style-type: none"> <li>● <b>Auto</b>: The device automatically selects an authentication type based on the authentication types that the peer server supports.</li> <li>● <b>PAP</b>: Only the PAP type is used.</li> <li>● <b>CHAP</b>: Only the CHAP type is used.</li> </ul>
Retry Times	Number of retries.

3. Click **Start**. The system starts simulation. The result is displayed in the bottom box.

– End of Steps –

## 7.6.4 Configure the AT Diagnosis

This procedure describes how to configure AT diagnosis to detect SIMs.

### Steps

1. In the left navigation tree, click **Administration > Diagnosis > AT Diagnosis**. The **AT Diagnosis** page is displayed, as shown in [Figure 7-16](#).

Figure 7-16 AT Diagnosis Page

Path:Administration-Diagnosis-AT Diagnosis      中文      Logout

AT Command

2. Enter an AT command and press the **Submit** key. The result is displayed in the bottom box.

– End of Steps –

## 7.6.5 Configure the Port Mirror


This procedure describes how to configure port mirroring, so that packets passing through a WAN connection of the ZXHN F670 can be mirrored to a LAN interface of the ZXHN F670. If service failure occurs, you can monitor the packets on the LAN interface for locating the failure cause quickly.

### Steps

1. In the left navigation tree, click **Administration > Diagnosis > Mirror Configuration**. The **Mirror Configuration** page is displayed, as shown in [Figure 7-17](#).

Figure 7-17 Mirror Configuration Page

Path:Administration-Diagnosis-Mirror Configuration 中文 [Logout](#)

 Source port cannot correspond to multiple destination ports.

Source

Destination

Add

Source	Destination	Delete
There is no data, please add one first.		

2. Set the parameters. For a description of the parameters, refer to [Table 7-6](#). Click **Add**.

Table 7-6 Port Mirroring Parameter Descriptions

Parameter	Description
Source	WAN connection on the network side
Destination	LAN interface on the user side

3. (Optional) To delete a configuration record, click the icon next to the record.

– End of Steps –

### 7.6.6 Configure the PPPoE Diagnosis


The PPPoE diagnosis function is used to check the communication status of PPPoE connections.

#### Steps

1. In the left navigation tree, click **Administration > Diagnosis > PPPoE Diagnosis**. The **PPPoE Diagnosis** page is displayed, as shown in [Figure 7-18](#).

Figure 7-18 PPPoE Diagnosis Page

Path:Administration-Diagnosis-PPPoE Diagnosis 中文 [Logout](#)



1.Current WAN connection may be dropped down during diagnosing.  
2.Only support "always-on" PPPoE connection.

PPPoE Check

This test checks the PPPoE connection and traffic.

PPPoE Connection

Check PPPoE server connectivity	
Check PPPoE server session	
Check authentication with PPPoE server	
Validate WAN assigned IP address	
Validate WAN assigned DNS IP address	
Validate WAN default gateway address	

Diagnose

2. Select the PPPoE connection to be tested. For a description of the parameters, refer to [Table 7-7](#).

Table 7-7 PPPoE Diagnosis Parameter Descriptions

Parameter	Description
PPPoE connection	Select a PPPoE connection that has been configured in <b>Network &gt; WAN &gt; WAN Connection</b> .

3. Click **Diagnosis**. If the test is successful, all test items are displayed as **pass**. Otherwise, the test result is **fail**.

– End of Steps –

### 7.6.7 Configure the DNS Diagnosis

The DNS diagnosis function is used to check the availability of the DNS server.

#### Steps

1. In the left navigation tree, click **Administration > Diagnosis > DNS Diagnosis**. The **DNS Diagnosis** page is displayed, as shown in [Figure 7-19](#).

Figure 7-19 DNS Diagnosis Page

Path:Administration-Diagnosis-DNS Diagnosis

中文Logout

DNS Check

This test checks the availability of the domain name servers.

Query DNS for a well known host

Domain Name

Diagnose

2. Set the parameters. For a description of the parameters, refer to [Table 7-8](#).

Table 7-8 DNS Diagnosis Parameter Descriptions

Parameter	Description
Domain Name	Enter a domain name that has been configured in <b>Application &gt; DNS Service &gt; Domain Name</b> .

3. Click **Diagnosis**. If the test is successful, the **Query DNS for a well known host** field is displayed as **pass**. Otherwise, it is displayed as **fail**.

– End of Steps –

### 7.6.8 Configure the IP Diagnosis

The IP diagnosis function is used to check IP connections.

#### Prerequisite


The DHCP WAN connection is created.

#### Steps

1. In the left navigation tree, click **Administration > Diagnosis > IP Diagnosis**. The **IP Diagnosis** page is displayed, as shown in [Figure 7-20](#).

Figure 7-20 IP Diagnosis Page

Path:Administration-Diagnosis-IP Diagnosis [中文](#) [Logout](#)

 Current WAN connection may be dropped down during diagnosing.

### IP Check

This test checks the IP connection and traffic.

DHCP Connection

Check DHCP server connectivity	
Validate WAN assigned IP address	
Validate WAN assigned DNS IP address	
Validate WAN default gateway address	

2. Select a WAN connection from the DHCP Connection drop-down list, and then click **Diagnose** to diagnose and display the status of the IP connectivity.

– End of Steps –

## 7.6.9 Configure the Voice Diagnosis

The voice diagnosis function is used to check voice connections.

### Prerequisite

The VoIP connection is created.

### Steps

1. In the left navigation tree, click **Administration > Diagnosis > Voice Diagnosis**. The **Voice Diagnosis** page is displayed, as shown in [Figure 7-21](#).



Figure 7-21 Voice Diagnosis Page

Path:Administration-Diagnosis-Voice Diagnosis 中文 [Logout](#)

**Voice Check**

This test checks the availability of voice service.

VoIP Account

Query DNS for server	
Check user registration	

Diagnose

2. Select a voip account from the drop-down list, and then click **Diagnose** to diagnose and display the status of the voice connectivity.

– End of Steps –

## 7.6.10 Check the ARP Table

This procedure describes how to check the [ARP](#) table, where the corresponding relationships between peer IP addresses and MAC addresses are displayed.

### Steps

1. In the left navigation tree, click **Administration > Diagnosis > ARP Table**. The **ARP Table** page is displayed, as shown in [Figure 7-22](#).

Figure 7-22 ARP Table Page

Path:Administration-Diagnosis-ARP Table		<a href="#">中文</a>	<a href="#">Logout</a>
Network Address	MAC Address	Status	Interface
10.46.42.1	00:22:93:54:d2:9d	Available	omci_ipv4_static_1

Refresh

- Click **Refresh** to refresh the ARP table.

– End of Steps –

### 7.6.11 Check the MAC Table


The MAC table displays the effective time of ports and MAC addresses.

#### Steps

- In the left navigation tree, click **Administration > Diagnosis > MAC Table**. The **MAC Table** page is displayed, as shown in [Figure 7-23](#).

Figure 7-23 MAC Table Page

Path:Administration-Diagnosis-MAC Table		<a href="#">中文</a>	<a href="#">Logout</a>
Port	MAC Address	Active Time(s)	
DEFAULT_BRIDGE	00:10:18:26:e3:cc	2.94	
DEFAULT_BRIDGE	00:18:71:eb:94:0c	69.59	
DEFAULT_BRIDGE	00:22:93:4e:4e:7d	281.22	
DEFAULT_BRIDGE	00:22:93:54:d2:9d	295.79	
DEFAULT_BRIDGE	44:8a:5b:51:1f:09	295.93	
DEFAULT_BRIDGE	44:a8:42:0f:08:3b	66.93	
DEFAULT_BRIDGE	46:0a:64:42:af:01	234.15	
DEFAULT_BRIDGE	78:ac:c0:f9:1a:7a	295.79	
DEFAULT_BRIDGE	9c:8e:99:fb:6c:7a	281.97	
DEFAULT_BRIDGE	9c:8e:99:fc:a0:7c	295.79	
DEFAULT_BRIDGE	b0:83:fe:ec:36:c2	209.31	
DEFAULT_BRIDGE	b8:2a:72:d1:8d:15	263.97	
DEFAULT_BRIDGE	b8:2a:72:d1:a5:e9	288.86	
DEFAULT_BRIDGE	b8:2a:72:d1:ab:eb	284.41	
DEFAULT_BRIDGE	b8:2a:72:d1:b2:dd	25.09	
DEFAULT_BRIDGE	c8:1f:66:f3:24:96	292.71	
DEFAULT_BRIDGE	c8:1f:66:f3:24:9e	295.79	
DEFAULT_BRIDGE	f8:bc:12:46:e7:50	209.32	



- Click **Refresh** to refresh the MAC table.

– End of Steps –

## 7.7 Loopback Detection

### 7.7.1 Configure the Basic Parameters of Loopback Detection

#### Steps

- In the left navigation tree, click **Administration > Loopback Detection**. The **Basic Configuration** page is displayed by default, as shown in [Figure 7-24](#).

Figure 7-24 Basic Configuration Page

Path:Administration-Loopback Detection-Basic Configuration 中文 [Logout](#)

Destination MAC: ☒ Broadcast Address ☐ BPDU Address

Ethernet Type  (hex 0000 - ffff)

Send Interval  (100 - 1000) ms

Port Closing Time  (60 - 300)sec

Loopback Recovery Time  (5 - 300)sec

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 7-9](#).

Table 7-9 Basic Parameter Descriptions for Loopback Detection

Parameter	Description
Destination MAC	Options: Broadcast Address and <a href="#">BPDU</a> Address.
Ethernet Type	Type of Ethernet packets for port loopback detection.
Send Interval	Interval for sending loopback detection packets.
Port Closing Time	Time allowed for closing a port after loopback is detected on the port.
Loopback Recovery Time	Time used for determining whether loopback detection has completed. If no detection packet is received within this period, loopback detection is considered to have completed.

3. Click **Submit**.

– End of Steps –

## 7.7.2 Configure the Loopback Detection

This procedure describes how to enable the loopback detection, alarm, and automatic loopback cancellation functions on the ports.

### Steps

1. In the left navigation tree, click **Administration > Loopback Detection > Enable Configuration**. The **Enable Configuration** page is displayed, as shown in [Figure 7-25](#).

**Figure 7-25 Enable Configuration Page**

Path:Administration-Loopback Detection-Enable Configuration

[中文](#)[Logout](#)

Port	Loopback Enable	Alarm Enable	Portdislooped Enable
LAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LAN2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LAN3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LAN4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SubmitCancel

2. Select the check boxes as required, and click **Submit**.

**Note:**

By default, the ZXHN F670 enables the alarm and automatic loopback cancellation functions.

- Each **Alarm Enable** check box specifies whether to report an alarm when loopback is detected.
- Each **Portdislooped Enable** check box specifies whether to automatically cancel loopback detection after loopback is detected on the corresponding port.

– End of Steps –

## 7.7.3 Configure the VLAN of Loopback Detection

This procedure describes how to enable VLAN-based loopback detection for a port.

### Steps

1. In the left navigation tree, click **Administration > Loopback Detection > VLAN Configuration**. The **VLAN Configuration** page is displayed, as shown in [Figure 7-26](#).

**Figure 7-26 VLAN Configuration Page**

Path:Administration-Loopback Detection-VLAN Configuration      中文      [Logout](#)

Port

VLAN  (1 - 4094)

Port	VLAN	Modify	Delete
There is no data, please add one first.			

2. Select a port for loopback detection, enter a VLAN ID, and click **Add**.
3. (Optional) To modify a configuration record, click next to the configuration record.
4. (Optional) To delete a configuration record, click next to the record.

– End of Steps –

## 7.8 Configure the IPv6 Switch


This procedure describes how to enable or disable IPv6 support for the ZXHN F670.

### Steps

1. In the left navigation tree, click **Administration > IPv6 Switch**. The **IPv6 Switch** page is displayed, as shown in [Figure 7-27](#).

**Figure 7-27 IPv6 Switch Page**

Path:Administration-IPv6 Switch 中文 [Logout](#)



1. IPv6 Switch change will take effect after reboot.
2. Before switching off IPv6 function, please ensure that all related configuration parameters are set appropriately, such as IP Address, WAN Connection, etc.

IPv6 Function

IPv6 Function Status: Enabled

2. To disable IPv6 support, set **IPv6 Function** to **Off**, and click **Submit**.



**Note:**

The configuration takes effective after the device is restarted.

– End of Steps –

## 7.9 Configure the VoIP Protocol


This procedure describes how to configure the VoIP protocol for the ZXHN F670.

### Steps

1. In the left navigation tree, click **Administration > VoIP Protocol Switch**. The **VoIP Protocol Switch** page is displayed, as shown in [Figure 7-28](#).

**Figure 7-28 VoIP Protocol Switch Page**

Path:Administration-VoIP Protocol Switch 中文 [Logout](#)

 The device will reboot after the VoIP Protocol is changed.

VoIP Protocol

2. Select a protocol from the **VoIP Protocol** list, and click **Submit**.



**Note:**

After the VoIP protocol is changed, the device is automatically restarted. Perform this operation with care.

– End of Steps –



# 7.10 Configure the 3G Switch

This procedure describes how to configure the 3G Switch for the ZXHN F670.

## Steps

1. In the left navigation tree, click **Administration > 3G Basic Configuration**. The **3G Basic Configuration** page is displayed, as shown in [Figure 7-29](#).

Figure 7-29 3G Basic Configuration Page

Path:Administration-3G Basic Configuration

[中文](#)[Logout](#)

3G Enable ☒

Auto Switch Time sec

Submit

Cancel

2. Set the parameters. For a description of the parameters, refer to [Table 7-10](#).

Table 7-10 Basic Parameter Descriptions for 3G

Parameter	Description
3G Enable	Select the check box to enable the 3G function.
Auto Switch Time	If the default route is interrupted, the device switches to 3G mode automatically.

3. Click **Submit**.

– End of Steps –

# Appendix A

## Troubleshooting

---

**The Power indicator on the front panel is off after the power button is pressed.**

The power adapter is not correctly connected to the device. Be sure to use the power adapter supplied with the device.

**The LOS indicator is flashing red or solid red after the device is powered on.**

- The optical fiber is not correctly connected to the ONT PON interface.
- The optical fiber is broken or damaged.
- If the indicator is solid red or keeps flashing, please contact the service provider for maintenance.

**The PON indicator on the front panel is off or flashing green after the device is powered on.**

- The GPON link is not established.
- The ONT is not registered.
- Please contact the service provider for help.

**The green LAN indicator on the front panel is off after the device is powered on.**

- The corresponding LAN link is not established.
- The Ethernet cable is not correctly connected to the LAN interface.
- The network device connected to the LAN interface is not powered on.

**The Phone indicator on the front panel is off after the device is powered on.**

The telephone function is abnormal. Please contact the service provider for help.