ZXA10 F660
GPON ONT
User Manual

Version: V1.0
LEGAL INFORMATION

Copyright © 2011 ZTE CORPORATION.
The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

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

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

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

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

Revision History

<table>
<thead>
<tr>
<th>Revision No.</th>
<th>Revision Date</th>
<th>Revision Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1.0</td>
<td>2011–07–18</td>
<td>First Edition</td>
</tr>
</tbody>
</table>

Serial Number: SJ-20110718111034-001

Publishing Date: 2011-07-18 (R1.0)
Contents

Preface ................................................................................................................................. I

Chapter 1 Overview ........................................................................................................... 1-1
  1.1 Product Introduction ................................................................................................. 1-1
  1.2 Packing List ............................................................................................................... 1-2
  1.3 Features and Specifications ..................................................................................... 1-2
  1.4 Product Appearance ............................................................................................... 1-3
  1.5 System Requirements ............................................................................................ 1-6
  1.6 System Application Environment ............................................................................ 1-6

Chapter 2 Configuration Preparation ............................................................................... 2-1
  2.1 Preliminary Setup ..................................................................................................... 2-1
  2.2 Configuring TCP/IP ................................................................................................. 2-1
  2.3 Logging In to the Device ......................................................................................... 2-6

Chapter 3 Device Status ................................................................................................... 3-1
  3.1 Device Information .................................................................................................. 3-1
  3.2 Network Connection Information .......................................................................... 3-2
  3.3 User Interface Information ..................................................................................... 3-3
    3.3.1 WLAN Interface Information ............................................................................ 3-3
    3.3.2 Ethernet Interface Information ....................................................................... 3-4
    3.3.3 VoIP Status Information .................................................................................. 3-5

Chapter 4 Network Configuration .................................................................................... 4-1
  4.1 Configuring WAN Connection ............................................................................... 4-1
  4.2 WLAN Configuration .............................................................................................. 4-5
    4.2.1 Configuring Basic WLAN Parameters ............................................................. 4-5
    4.2.2 Configuring Multi-SSID Parameters ............................................................... 4-7
    4.2.3 Configuring Security Properties ...................................................................... 4-8
    4.2.4 Viewing Associated Devices .......................................................................... 4-12
  4.3 Address Management Configuration ....................................................................... 4-13
    4.3.1 Configuring DHCP Server .............................................................................. 4-13
    4.3.2 Configuring DHCP Binding .......................................................................... 4-15
    4.3.3 Configuring Specific Address Range .............................................................. 4-16
  4.4 Route Management Configuration .......................................................................... 4-17
    4.4.1 Configuring Default Gateway ....................................................................... 4-17
    4.4.2 Configuring Static Routing ............................................................................ 4-18
Chapter 5 Security Configuration ......................................................... 5-1
5.1 Configuring Firewall ........................................................................... 5-1
5.2 Configuring IP Filter ............................................................................ 5-2
5.3 Configuring URL Filter .......................................................................... 5-5
5.4 Configuring DMZ Host .......................................................................... 5-7
5.5 Configuring Port Forwarding ................................................................. 5-9

Chapter 6 Service Configuration ............................................................. 6-1
6.1 SIP VoIP Service Configuration .......................................................... 6-1
   6.1.1 Configuring VoIP WAN Connection .............................................. 6-1
   6.1.2 Configuring SIP ............................................................................ 6-2
   6.1.3 Configuring SIP Accounts ........................................................... 6-4
   6.1.4 Configuring VoIP Advanced Parameters ...................................... 6-5
   6.1.5 Configuring VoIP Media Parameters ............................................ 6-7
   6.1.6 Configuring Fax .......................................................................... 6-8
6.2 Configuring DDNS .............................................................................. 6-10
6.3 Configuring UPnP ............................................................................... 6-11
6.4 DNS Configuration ............................................................................. 6-13
   6.4.1 Configuring Domain Name .......................................................... 6-13
   6.4.2 Configuring Host Name ............................................................... 6-14
6.5 QoS Configuration ............................................................................. 6-16
   6.5.1 Configuring Basic QoS Parameters .............................................. 6-16
   6.5.2 Configuring QoS Rule .................................................................. 6-19
   6.5.3 Configuring QoS Rule Type .......................................................... 6-20
   6.5.4 Configuring QoS Local Application ............................................. 6-22
   6.5.5 Configuring QoS Queue Management ......................................... 6-23
   6.5.6 Configuring QoS Ingress Rate Limit ............................................ 6-25
6.6 Configuring SNTP Client .................................................................... 6-26
6.7 IGMP Configuration ........................................................................... 6-28
   6.7.1 Configuring Basic IGMP Parameters ............................................ 6-28
   6.7.2 Configuring Multicast VLAN ..................................................... 6-31
   6.7.3 Configuring Multicast MAC Limit .............................................. 6-32
   6.7.4 Configuring MVLAN Tag Strip ................................................... 6-34
6.8 Configuring FTP Application .............................................................. 6-36

Chapter 7 Device Management ............................................................... 7-1
7.1 TR069 Configuration ........................................................................... 7-1
    7.1.1 Configuring Basic TR069 Parameters ........................................ 7-1
    7.1.2 Importing TRO69 Certificate ..................................................... 7-3
Preface

Purpose
This manual provides procedures and guidelines that support the operation on the ZXA10 F660 Optical Network Terminal (ZXA10 F660 for short).

Intended Audience
This manual is intended for engineers and technicians who perform operation activities on ZXA10 F660.

Prerequisite Skill and Knowledge
To use this manual effectively, users should have a general understanding of wireless telecommunications technology. Familiarity with the following is helpful:

- ZXA10 system and its various components
- Local operating procedures

What Is in This Manual
This manual contains the following chapters:

Chapter Summary

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, Overview</td>
<td>Provides an overview of the product, including the packing list, product features, appearance, and system requirements, and system application environment.</td>
</tr>
<tr>
<td>Chapter 2, Configuration Preparation</td>
<td>Describes the procedures for configuring TCP/IP, and logging in to the device.</td>
</tr>
<tr>
<td>Chapter 3, Device Status</td>
<td>Describes the device information, network connection information, and user interface information.</td>
</tr>
<tr>
<td>Chapter 4, Network Configuration</td>
<td>Describes the configuration of WAN connection, WLAN, address management, and route management.</td>
</tr>
<tr>
<td>Chapter 5, Security Configuration</td>
<td>Describes the procedures for configuring the firewall, IP filter, URL filter, DMZ, and port forwarding.</td>
</tr>
<tr>
<td>Chapter</td>
<td>Summary</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chapter 6, Service Configuration</td>
<td>Describes the configuration of VoIP, DDNS, UPnP, DNS server, QoS, SNTP client, IGMP, and FTP application.</td>
</tr>
<tr>
<td>Chapter 7, Device Management</td>
<td>Describes TRO69 configuration, user management, device management, log management, and ping diagnosis.</td>
</tr>
<tr>
<td>Chapter 8, FAQ</td>
<td>Provides the FAQs and solutions.</td>
</tr>
</tbody>
</table>

**Related Documentation**

None

**Conventions**

ZTE documents employ the following typographical conventions.

**Typographical Conventions**

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>References to other Manuals and documents.</td>
</tr>
<tr>
<td>“Quotes”</td>
<td>Links on screens.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus, menu options, function names, input fields, radio button names, check boxes, drop-down lists, dialog box names, window names.</td>
</tr>
<tr>
<td><strong>CAPS</strong></td>
<td>Keys on the keyboard and buttons on screens and company name.</td>
</tr>
<tr>
<td>Constant width</td>
<td>Text that you type, program code, files and directory names, and function names.</td>
</tr>
<tr>
<td>[]</td>
<td>Optional parameters</td>
</tr>
<tr>
<td>{}</td>
<td>Mandatory parameters</td>
</tr>
<tr>
<td>I</td>
<td>Select one of the parameters that are delimited by it.</td>
</tr>
</tbody>
</table>

**Note:** Provides additional information about a certain topic.

**Checkpoint:** Indicates that a particular step needs to be checked before proceeding further.
Mouse Operation Conventions are as follows:

**Mouse Operation Conventions**

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click</td>
<td>Refers to clicking the primary mouse button (usually the left mouse button) once.</td>
</tr>
<tr>
<td>Double-click</td>
<td>Refers to quickly clicking the primary mouse button (usually the left mouse button) twice.</td>
</tr>
<tr>
<td>Right-click</td>
<td>Refers to clicking the secondary mouse button (usually the right mouse button) once.</td>
</tr>
<tr>
<td>Drag</td>
<td>Refers to pressing and holding a mouse button and moving the mouse.</td>
</tr>
</tbody>
</table>

**How to Get in Touch**

The following sections provide information on how to obtain support for the documentation and the software.

**Customer Support**

If you have problems, questions, comments, or suggestions regarding your product, contact us by e-mail at support@zte.com.cn. You can also call our customer support center at (86) 755 26771900 and (86) 800-9830-9830.

**Documentation Support**

ZTE welcomes your comments and suggestions on the quality and usefulness of this document. For further questions, comments, or suggestions on the documentation, you can contact us by e-mail at doc@zte.com.cn; or you can fax your comments and suggestions to (86) 755 26772236. You can also browse our website at [http://ensupport.zte.com.cn](http://ensupport.zte.com.cn), which contains various interesting subjects like documentation, knowledge base, forum and service request.

**Declaration of RoHS Compliance**

To minimize the environmental impact and take more responsibility to the earth we live, this document shall serve as formal declaration that ZXA10 F660 manufactured by ZTE CORPORATION is in compliance with the Directive 2002/95/EC of the European
Parliament - RoHS (Restriction of Hazardous Substances) with respect to the following substances:

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent Chromium (Cr (VI))
- PolyBrominated Biphenyls (PBB's)
- PolyBrominated Diphenyl Ethers (PBDE's)

This declaration is issued based on our current level of knowledge. Since conditions of use are outside our control, ZTE CORPORATION makes no warranties, express or implied, and assumes no liability in connection with the use of this information.
Chapter 1
Overview

1.1 Product Introduction

ZXA10 F660 is a user-side access device module. It uses the computer network technology and broadband optical network technology to establish a home network center for the access of network devices. It provides users with various services.

Table 1-1 lists the ports and functions of ZXA10 F660 series products.

Table 1-1 ZXA10 F660 Ports and Functions

<table>
<thead>
<tr>
<th>Product</th>
<th>Port</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZXA10 F660</td>
<td>Four GE ports, two POTS ports, one Wi-Fi port, and two USB 2.0 ports</td>
<td>Supports Internet access, IPTV, VoIP, and Wi-Fi. It can be used as a home gateway.</td>
</tr>
<tr>
<td>ZXA10 F668</td>
<td>Four GE ports, two POTS ports, one Wi-Fi port, two USB 2.0 ports, and one CATV port</td>
<td>Supports Internet access, IPTV, VoIP, Wi-Fi, and CATV. It can be used as a home gateway.</td>
</tr>
<tr>
<td>ZXA10 F600G</td>
<td>Four GE ports and two USB 2.0 ports</td>
<td>Supports Internet access and IPTV.</td>
</tr>
<tr>
<td>ZXA10 F627</td>
<td>Four GE ports, two POTS ports, and one Wi-Fi port</td>
<td>Supports Internet access, IPTV, VoIP, and Wi-Fi. It can be used as a home gateway.</td>
</tr>
<tr>
<td>ZXA10 F625G</td>
<td>Four GE ports, two POTS port and one CATV port</td>
<td>Supports Internet access, IPTV, VoIP, and CATV. It can be used as a home gateway.</td>
</tr>
<tr>
<td>ZXA10 F607</td>
<td>Four GE ports and one Wi-Fi port</td>
<td>Supports Internet access, IPTV, and Wi-Fi. It can be used as a home gateway.</td>
</tr>
</tbody>
</table>
1.2 Packing List

Make sure that ZXA10 F660 package contains the following:

- One ZXA10 F660 host
- One AC-DC adaptor
- One RJ-45 straight-through cable
- Two RJ-11 telephone cables
- One ZXA10 F660 Optical Network Terminal User Manual

If any of the above contents is missing or damaged, please contact your dealer. Keep the packing box and components for the replacement purpose.

1.3 Features and Specifications

System Features

ZXA10 F660 has the following features:

- **MAC cache**: 4K
- **Multicast services**: 1024 multicast groups
- **VLAN range**: 1 - 4095
- **GEM ports**: 256
- **T-CONTs**: 40

Interface Features

The interface features are as follows:

- **GPON interface**: complies with the PON standard and SC/APC, in compliance with ITU G.984.1 - G.984.5 standards
- **Ethernet interface**: 10/100/1000 Mbps GE interfaces (RJ-45), in compliance with IEEE 802.3 and IEEE 802.3u standards
- **POTS interface**: RJ-11
- **WLAN interface**: complying with the IEEE 802.11n standard with built-in antenna

Technical Features

ZXA10 F660 implements data access and IP voice access.

- For data access, ZXA10 F660 implement L2 data switching and forwarding.
  
  By working with relevant network devices through signaling protocols such as H.248 and SIP, ZXA10 F660 implements IP voice function.

- ZXA10 F660 provides the security, QoS, and network management functions, such as multi-level authentication based on devices, users, and services.

  It supports data channel encryption, implementation of QoS requirements matching the local devices and network according to services with different requirements, and network management based on various management modes.
Certification Features

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

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

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, use product that maintain a 20cm distance between the device and human body.

Note:
Changes or modifications made to this equipment not expressly approved by (ZTE Corporation) may void the FCC authorization to operate this equipment.

Product Specifications

ZXA10 F660 specifications are as follows:

- Rated current: 1.3 A
- Rated voltage: 12 V DC
- Operating temperature: -5°C - 50°C
- Operating humidity: 5% - 95%
- Dimensions: 260 mm x 50 mm x 185 mm (Width x Height x Depth)

1.4 Product Appearance

Front Panel

Figure 1-1 shows the front panel of ZXA10 F660.

Figure 1-1 Front Panel

Table 1-2 lists LEDs on the front panel.
### Table 1-2 Front Panel LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PON</td>
<td>Green, ON</td>
<td>The ONT GPON is registered and the link is activated.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The ONT is not discovered and registered.</td>
</tr>
<tr>
<td></td>
<td>Flashing</td>
<td>The ONT is trying to be registered or set up the connection.</td>
</tr>
<tr>
<td>LOS</td>
<td>Red, ON</td>
<td>The ONU receives the optical power abnormally.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The ONU receives the optical power normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The IP address for the WAN connection is obtained.</td>
</tr>
<tr>
<td></td>
<td>Flashing</td>
<td>Fails to obtain the IP address for the WAN connection.</td>
</tr>
<tr>
<td>WLAN</td>
<td>Green, ON</td>
<td>The WLAN function is enabled.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The device is not powered ON or the wireless interface is disabled.</td>
</tr>
<tr>
<td>POTS1 POTS2</td>
<td>Green, ON</td>
<td>The device is registered on the SS, but no data is being transmitted.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The device is not powered ON or fails to be registered on the SS.</td>
</tr>
<tr>
<td></td>
<td>Flashing</td>
<td>Data is being transmitted.</td>
</tr>
<tr>
<td>Power indicator</td>
<td>Blue, ON</td>
<td>The device is powered ON normally.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The device is not powered ON.</td>
</tr>
<tr>
<td>LAN1 - LAN4</td>
<td>Green, ON</td>
<td>The network interface is connected, but no data is being transmitted.</td>
</tr>
<tr>
<td></td>
<td>OFF</td>
<td>The device is not powered ON or the network interface is not connected with a network device.</td>
</tr>
<tr>
<td></td>
<td>Flashing</td>
<td>Data is being transmitted.</td>
</tr>
</tbody>
</table>
Chapter 1 Overview

Back Panel

Figure 1-2 shows the back panel.

Figure 1-2 Back Panel

Table 1-3 lists the interfaces and buttons on the back panel.

Table 1-3 Interfaces and Buttons on the Back Panel

<table>
<thead>
<tr>
<th>Interface/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN1 - LAN4</td>
<td>RJ-45 LAN interface, connects to the local network through the RJ-45 network cable</td>
</tr>
<tr>
<td>POTS1 POTS2</td>
<td>RJ-11 telephone interface, connects to the telephone through the RJ-11 telephone cable</td>
</tr>
<tr>
<td>USB</td>
<td>USB interface, connects to a storage device or printer that has a USB interface</td>
</tr>
<tr>
<td>UPS</td>
<td>Secondary power monitoring interface</td>
</tr>
<tr>
<td>POWER</td>
<td>Power socket, connects to the power adapter, 12 V DC</td>
</tr>
<tr>
<td>WPS</td>
<td>WPS access switch</td>
</tr>
<tr>
<td>WLAN</td>
<td>WLAN button, to enable or disable WLAN</td>
</tr>
<tr>
<td>RESET</td>
<td>When the device is powered ON, press the button for more than 5 seconds to restore the factory default settings.</td>
</tr>
</tbody>
</table>

Side Panel

The side panel has an SC/APC single-mode fiber interface, implementing the services provided by the ISP in PON access mode. It connects to the GPON interface of ZXA10 F660 through an SC/APC single-mode fiber. Figure 1-3 shows the side panel.
1.5 System Requirements

The ZXA10 F660 system requirements are as follows:

- An ISP is needed so that the device can access the services provided by the ISP through the PON access mode.
- A computer that is installed with a 10 Mbps/100 Mbps/1000 Mbps Ethernet card is needed.
- If necessary, create a medium and small LAN by adding Ethernet hubs and cables.
- To use wireless access, an 802.11g/b wireless network card or a built-in 802.11g/b wireless network card is required.
- The computer that accesses the network should be installed with Windows 98/Me/2000/NT/XP/Vista/7 or Linux, network card driver program, and TCP/IP protocol, and its network settings are correct.
- A computer in the LAN is installed with a Web browser, such as Microsoft Internet Explorer 6.0 or higher, Netscape Communicator 4.0 or higher.

1.6 System Application Environment

ZXA10 F660 is an indoor device of ZTE series optical network terminal equipment. It works with the PON device to implement the FTTH application.

With the use of multiple user interfaces, hub, or Ethernet switch, ZXA10 F660 can implement the FTTO/B application.

Figure 1-4 shows the ZXA10 F660 application environment.
As an indoor device, ZXA10 F660 can be put on the desk with the base or hung on the wall without the base.

Figure 1-5 shows the ZXA10 F660 on a wall.

Figure 1-5 F66x Wall-Mount
This page intentionally left blank.
Chapter 2
Configuration Preparation

2.1 Preliminary Setup

Generally, the ISP has already configured the device. The user can directly use it after hardware connection. However, the user may need to configure the device in some special situations. The user must confirm the following preliminary setups:

- Use one crossover or straight-through Ethernet cable to connect a computer to the device.
- Check the TCP/IP settings of the computer.
- Disable any running firewall or security software.
- Disable the proxy server of the Internet Explorer.
- Consult the ISP if some data from the ISP is needed.

2.2 Configuring TCP/IP

Short Description

Perform this procedure to configure TCP/IP of a computer connected to the ZXA10 F660.

Context

This instance takes Windows XP as an example.

The default network settings for the ZXA10 F660 are as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1

To configure TCP/IP, perform the following steps:

Steps

1. Choose Start > Settings > Network Connections to open the Network Connections window.
2. Double-click **Local Area Connection** to open the **Local Area Connection Status** dialog box, as shown in **Figure 2-1**.

**Figure 2-1 Local Area Connection Status**

3. Click **Properties** in the **General** tab to open the **Local Area Connection Properties** dialog box.

4. Select **Internet Protocol (TCP/IP)**, as shown in **Figure 2-2**.
5. Click **Properties** to open the **Internet Protocol (TCP/IP) Properties** dialog box. Select **Use the following IP address** and specify the IP address, Subnet mask, and **Default gateway**. For example, you can set the **IP address** to 192.168.1.7, **Subnet mask** to 255.255.255.0, and **Default gateway** to 192.168.1.1, as shown in **Figure 2-3**.
Figure 2-3 Specifying the IP address in the Internet Protocol (TCP/IP) Properties

Note:
The IP address shall be in the same network segment as LAN port address of the device, which means the IP address you type in should be “192.168.1.x” (x can be any value from 2 to 254).

6. Click **OK** to save your settings.

Note:
If you are accessing the WEB page of the device for the first time, please configure the device as you are told.

--- End of Steps ---
Follow-Up Action

1. Choose Start > Run to open the Run dialog box.
2. Type CMD in the Open text box, and click OK.
3. Type ping 192.168.1.1 in the pop-up window and press Enter to carry out the ping command.
   - If the command window displays the messages, as shown in Figure 2-4, it indicates that the communication between your PC and the device is normal and you are able to access the Internet now.

Figure 2-4 Successful Ping Message

If the command window displays the messages, as shown in Figure 2-5, it indicates that the communication between your PC and the device fails.

Figure 2-5 Failed Ping Message

If the communication between your PC and the device fails, ensure the following items:
The Ethernet cable between the device and your PC has been connected properly.
The driver of your network adapter has been installed properly.
The TCP/IP setting has been configured correctly on your PC.
If the ZXA10 F660 IP address is 192.168.1.1, the IP address of the computer must be from 192.168.1.2 to 192.168.1.254. The subnet mask must be 255.255.255.0 and the default gateway must be 192.168.1.1.

2.3 Logging In to the Device

Short Description
Perform this procedure to log in to the device.

Prerequisites
The device is properly connected and the computer is correctly configured.

Context
To log in to the device, perform the following steps:

Steps
1. Open the Internet Explorer. Enter http://192.168.1.1 (default IP address of the device) on the address bar and press Enter. The login dialog box is displayed, as shown in Figure 2-6.

Figure 2-6 Login

2. Enter the Username and Password (by default, both are admin). Click Login.

– End of Steps –

Result
Logging in to the device is successful.
Chapter 3
Device Status

Table of Contents
Device Information ................................................................. 3-1
Network Connection Information ............................................... 3-2
User Interface Information ...................................................... 3-3

3.1 Device Information

On the Web interface of the device, click the Status tab. By default, the Device Information is selected. The right pane displays the device type, serial number, and version information, and registration password, as shown in Figure 3-1.

Figure 3-1 Device Information

Table 3-1 lists the parameters for the device information.

Table 3-1 Device Information Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Device type</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Device serial number</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Hardware version number</td>
</tr>
<tr>
<td>Software Version</td>
<td>Software version number</td>
</tr>
<tr>
<td>Boot Loader Version</td>
<td>Boot version number</td>
</tr>
<tr>
<td>PON Serial Number</td>
<td>PON serial number</td>
</tr>
</tbody>
</table>
3.2 Network Connection Information

On the Status tab, select Network Interface. By default, the WAN Connection sub-node is selected. The right pane displays the WAN connection information, as shown in Figure 3-2.

Click Refresh to view the latest information.

Figure 3-2 WAN Connection

Table 3-2 lists the parameters for the network connection information.

Table 3-2 Parameters for the Network Connection Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>omci1</td>
<td>WAN connection type</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID used by the WAN interface to send and receive data</td>
</tr>
<tr>
<td>NAT</td>
<td>Whether to enable the NAT function</td>
</tr>
<tr>
<td>IP</td>
<td>IP address used by ZXA10 F660</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS used by ZXA10 F660</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Gateway used by ZXA10 F660</td>
</tr>
<tr>
<td>Connection Status</td>
<td>WAN connection status</td>
</tr>
</tbody>
</table>
Note:

OMCI1 is the WAN connection name, which is created by the OMCI interface remotely.

3.3 User Interface Information

This topic includes the following:

- WLAN Interface Information
- Ethernet Interface Information
- VoIP Status Information

3.3.1 WLAN Interface Information

On the Status tab, select User Interface. By default, WLAN is selected. The right pane displays the WLAN switch information, packet receiving and sending information, and authentication information, as shown in Figure 3-3.

Click Refresh to view the latest information.

**Figure 3-3 WLAN Interface Information**

Table 3-3 lists the parameters for the WLAN interface information.
### Table 3-3 Parameters for the WLAN Interface Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wireless RF</td>
<td>Whether to enable the wireless RF</td>
</tr>
<tr>
<td>Channel</td>
<td>Channel</td>
</tr>
<tr>
<td>SSID1 Enable</td>
<td>Whether to enable the wireless network SSID1</td>
</tr>
<tr>
<td>SSID1 Name</td>
<td>SSID1 name, which identifies the wireless network service area</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Authentication mode</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Encryption mode</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address</td>
</tr>
<tr>
<td>Packets Received/Bytes Received</td>
<td>Number of received packets or bytes</td>
</tr>
<tr>
<td>Packets Sent/Bytes Sent</td>
<td>Number of sent packets or bytes</td>
</tr>
<tr>
<td>Error Packets Received</td>
<td>Error packets received</td>
</tr>
<tr>
<td>Error Packets Sent</td>
<td>Error packets sent</td>
</tr>
<tr>
<td>Discarded Receiving Packets</td>
<td>Discarded receiving packets</td>
</tr>
<tr>
<td>Discarded Sending Packets</td>
<td>Discarded sending packets</td>
</tr>
</tbody>
</table>

### 3.3.2 Ethernet Interface Information

On the **Status** tab, select **User Interface**. Select **Ethernet**. The right pane displays the packet receiving and sending information on the Ethernet interface, as shown in **Figure 3-4**.

Click **Refresh** to view the latest information.
Table 3-4 lists the parameters for the Ethernet interface information.

**Table 3-4 Parameters for the Ethernet Interface Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Port</td>
<td>Port name</td>
</tr>
<tr>
<td>Packets Received/Bytes Received</td>
<td>Number of received packets or bytes</td>
</tr>
<tr>
<td>Packets Sent/Bytes Sent</td>
<td>Number of sent packets or bytes</td>
</tr>
<tr>
<td>Error Frames</td>
<td>Ethernet error frames</td>
</tr>
</tbody>
</table>

### 3.3.3 VoIP Status Information

On the **Status** tab, select **User Interface**. Select **VoIP Status**. The right pane displays the VoIP status information, as shown in **Figure 3-5**.

Click **Refresh** to view the latest information.
Table 3-5 lists the parameters for the VoIP status information.

### Parameters for the VoIP Status Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Account Username</td>
<td>Telephone number</td>
</tr>
<tr>
<td>SIP Register Status</td>
<td>Registration status of the voice service</td>
</tr>
</tbody>
</table>
Chapter 4
Network Configuration

Table of Contents
Configuring WAN Connection ................................................................. 4-1
WLAN Configuration .............................................................................. 4-5
Address Management Configuration ......................................................... 4-13
Route Management Configuration ............................................................. 4-17

4.1 Configuring WAN Connection

Short Description
Perform this procedure to configure the WAN connection.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the WAN connection, perform the following steps:

Steps
1. On the Web interface of the device, click the Network tab. By default, WAN Connection is selected, as shown in Figure 4-1.

Figure 4-1 WAN Connection

![Figure 4-1 WAN Connection](image-url)
2. The connection type can be **PPPoE**, **Static**, or **DHCP**.

   a. Configure the **PPPoE** mode.

   Select **PPPoE** for **Type**, as shown in **Figure 4-2**.

   **Figure 4-2 PPPoE Mode Configuration**

   ![PPPoE Mode Configuration](image)

   **Table 4-1** lists the parameters for the **PPPoE** mode configuration.

   **Table 4-1 Parameters for PPPoE Mode Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Connection mode</td>
</tr>
<tr>
<td><strong>Connection Name</strong></td>
<td>PPPoE connection name, automatically generated by the system</td>
</tr>
<tr>
<td><strong>Enable NAT</strong></td>
<td>Whether to enable the NAT function</td>
</tr>
<tr>
<td><strong>Service List</strong></td>
<td>Service modes supported by the system:</td>
</tr>
<tr>
<td></td>
<td>● TR069 service mode</td>
</tr>
<tr>
<td></td>
<td>Remote maintenance and management mode</td>
</tr>
<tr>
<td></td>
<td>● Internet service mode</td>
</tr>
<tr>
<td></td>
<td>Broadband and IPTV service mode</td>
</tr>
<tr>
<td></td>
<td>● VoIP service mode</td>
</tr>
<tr>
<td></td>
<td>Voice service mode</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td><strong>VLAN ID</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>User name, used by the device authentication on interworking</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password, used by the device authentication on interworking</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Authentication type, the same as the authentication type for the upper-layer device</td>
</tr>
</tbody>
</table>
Chapter 4 Network Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Trigger</td>
<td>Dial-up connection mode:</td>
</tr>
<tr>
<td></td>
<td>● Always On</td>
</tr>
<tr>
<td></td>
<td>● On Demand</td>
</tr>
<tr>
<td></td>
<td>● Manual</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Idle time before the dial-up auto disconnection, available only in On Demand mode</td>
</tr>
</tbody>
</table>

b. Configure the static mode.

Select **Static** for **Type**, as shown in **Figure 4-3**.

**Figure 4-3 Static Mode Configuration**

![Static Mode Configuration](image)

Table 4-2 lists the parameters for the static mode configuration.

**Table 4-2 Static Mode Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Connection mode</td>
</tr>
<tr>
<td>Connection Name</td>
<td>Static connection name, automatically generated by the system</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Whether to enable the NAT function</td>
</tr>
<tr>
<td>Service List</td>
<td>Service modes supported by the system:</td>
</tr>
<tr>
<td></td>
<td>● TR069 service mode</td>
</tr>
<tr>
<td></td>
<td>Remote maintenance and management mode</td>
</tr>
<tr>
<td></td>
<td>● Internet service mode</td>
</tr>
<tr>
<td></td>
<td>Broadband and IPTV service mode</td>
</tr>
<tr>
<td></td>
<td>● VoIP service mode</td>
</tr>
<tr>
<td></td>
<td>Voice service mode</td>
</tr>
</tbody>
</table>
c. Configure the **DHCP** mode.

Select **DHCP** for **Type**, as shown in **Figure 4-4**.

**Figure 4-4 DHCP Mode Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address used by ZXA10 F660</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used by ZXA10 F660</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Gateway used by ZXA10 F660</td>
</tr>
<tr>
<td>DNS Server1 IP Address</td>
<td>IP address of DNS1 used by ZXA10 F660</td>
</tr>
<tr>
<td>DNS Server2 IP Address</td>
<td>IP address of DNS2 used by ZXA10 F660</td>
</tr>
<tr>
<td>DNS Server3 IP Address</td>
<td>IP address of DNS3 used by ZXA10 F660</td>
</tr>
</tbody>
</table>

**Table 4-3** lists the parameters for the **DHCP** mode configuration.

**Table 4-3 DHCP Mode Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Connection mode</td>
</tr>
<tr>
<td>Connection Name</td>
<td>DHCP connection name, automatically generated by the system</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Whether to enable the NAT function</td>
</tr>
<tr>
<td>Service List</td>
<td>Service modes supported by the system:</td>
</tr>
<tr>
<td></td>
<td>- TR069 service mode</td>
</tr>
<tr>
<td></td>
<td>- Remote maintenance and management mode</td>
</tr>
<tr>
<td></td>
<td>- Internet service mode</td>
</tr>
<tr>
<td></td>
<td>- Broadband and <strong>IPTV</strong> service mode</td>
</tr>
<tr>
<td></td>
<td>- <strong>VoIP</strong> service mode</td>
</tr>
<tr>
<td></td>
<td>- Voice service mode</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID</td>
</tr>
</tbody>
</table>
3. Click Create to finish the configuration. Click Cancel to cancel the configuration.

   – End of Steps –

Result
WAN connection configuration is complete.

4.2 WLAN Configuration

This topic includes the following:
- Configuring Basic WLAN Parameters
- Configuring Multi-SSID Parameters
- Configuring Security Properties
- Viewing Associated Devices

4.2.1 Configuring Basic WLAN Parameters

Short Description
Perform this procedure to configure the basic WLAN parameters.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the basic WLAN parameters, perform the following steps:

Steps
1. On the Network tab, select WLAN on the left pane. By default, the Basic sub-node is selected, as shown in Figure 4-5.
2. Configure the basic WLAN parameters, as listed in Table 4-4.

Table 4-4 Basic WLAN Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wireless RF</td>
<td>Whether to enable wireless RF</td>
</tr>
<tr>
<td>Mode</td>
<td>Wireless communication mode</td>
</tr>
<tr>
<td>Country/Region</td>
<td>Country or region name</td>
</tr>
<tr>
<td>Channel</td>
<td>Wireless channel number</td>
</tr>
<tr>
<td></td>
<td>Select a proper channel according to the country code</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>Beacon interval</td>
</tr>
<tr>
<td>Tx Rate</td>
<td>Data transmission rate</td>
</tr>
<tr>
<td></td>
<td>A low data transmission rate can enlarge the wireless communication area.</td>
</tr>
<tr>
<td>Transmitting Power</td>
<td>Transmission power</td>
</tr>
<tr>
<td>QoS Type</td>
<td>QoS priority type</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>RTS threshold</td>
</tr>
<tr>
<td>DTIM Interval</td>
<td>DTIM interval</td>
</tr>
<tr>
<td>Fragment Threshold</td>
<td>Fragment threshold</td>
</tr>
<tr>
<td></td>
<td>If a packet size exceeds this threshold, the packet is divided into several</td>
</tr>
<tr>
<td></td>
<td>fragments for transmission.</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –
Chapter 4 Network Configuration

Result
The basic WLAN parameters are configured.

4.2.2 Configuring Multi-SSID Parameters

Short Description
Perform this procedure to configure multi-SSID parameters.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure multi-SSID parameters, perform the following steps:

Steps
1. On the Network tab, click WLAN on the left pane. Select Multi-SSID Settings, as shown in Figure 4-6.

   Figure 4-6 Multi-SSID Settings
   ![Multi-SSID Settings](image)

2. Configure the multi-SSID parameters as shown in Table 4-5.

   Table 4-5 Multi-SSID Parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose SSID</td>
<td>Choose the SSID that needs to be configured.</td>
</tr>
<tr>
<td>Hide SSID</td>
<td>Disable or enable SSID broadcast.</td>
</tr>
<tr>
<td>Enable SSID</td>
<td>Enable the SSID.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSID Name</td>
<td>SSID name. It cannot exceed 32 characters and is case sensitive. It is used to control the WLAN access. The SSID name must match all the SSIDs of the related access nodes; otherwise, the device cannot be accessed. Up to four WLAN sub-ports are supported.</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

**Result**

The multi-SSID parameters are configured.

### 4.2.3 Configuring Security Properties

**Short Description**

Perform this procedure to configure the security properties.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the security properties, perform the following steps:

**Steps**

1. On the **Network** tab, select **WLAN**, and then select **Security**, as shown in **Figure 4-7**.

**Figure 4-7 Security Properties**

SSID supports four authentication modes: **Open System**, **Shared Key**, **WPA-PSK**, and **WPA2-PSK**.
2. From the **Choose SSID** drop-down list, select an SSID.

   a. In **Authentication Type**, select **Open System**, and then enable **WEP Encryption** (by default, it is disabled). The **Open System** configuration information is displayed, as shown in **Figure 4-8**.

   **Figure 4-8 Open System Configuration**

   ![](image)

   **Table 4-6 lists the parameters for the **Open System** authentication mode.**

   **Table 4-6 Parameters for Open System Authentication Mode**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose SSID</td>
<td>Current SSID</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Current SSID authentication mode</td>
</tr>
<tr>
<td>WEP Encryption</td>
<td>To enable or disable <strong>WEP</strong> encryption</td>
</tr>
<tr>
<td>WEP Encryption Level</td>
<td>WEP encryption length</td>
</tr>
<tr>
<td></td>
<td>● The 128–bit encryption can be a 13–bit ASCII codes or a 26–bit hexadecimal number.</td>
</tr>
<tr>
<td></td>
<td>● The 64–bit encryption can be a 5–bit ASCII code or a 10–bit hexadecimal number.</td>
</tr>
<tr>
<td></td>
<td>Generally, the 64–bit encryption can meet the user requirements. To enhance security, use the 128–bit encryption.</td>
</tr>
<tr>
<td>WEP Key Index</td>
<td>Current encryption value</td>
</tr>
<tr>
<td>WEP Key1</td>
<td>WEP encryption value</td>
</tr>
<tr>
<td></td>
<td>Range: 5–bit ASCII code or 10–bit hexadecimal number</td>
</tr>
<tr>
<td>WEP Key2</td>
<td>WEP encryption value</td>
</tr>
<tr>
<td></td>
<td>Range: 5–bit ASCII code or 10–bit hexadecimal number</td>
</tr>
</tbody>
</table>
b. In Authentication Type, select Shared Key. By default, WEP Encryption is enabled. The Shared Key configuration information is displayed, as shown in Figure 4-9.

**Figure 4-9 Shared Key Configuration**

![Shared Key Configuration](image)

**Table 4-7 Parameters for Shared Key Authentication Mode**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose SSID</td>
<td>Current SSID</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Current SSID authentication mode</td>
</tr>
<tr>
<td>WEP Encryption</td>
<td>To enable or disable WEP encryption</td>
</tr>
<tr>
<td>WEP Encryption Level</td>
<td>WEP encryption length</td>
</tr>
<tr>
<td></td>
<td>- The 128-bit encryption can be a 13-bit ASCII codes or a 26-bit hexadecimal number.</td>
</tr>
<tr>
<td></td>
<td>- The 64-bit encryption can be a 5-bit ASCII code or a 10-bit hexadecimal number.</td>
</tr>
<tr>
<td></td>
<td>Generally, the 64-bit encryption can meet the user requirements. To enhance security, use the 128-bit encryption.</td>
</tr>
<tr>
<td>WEP Key Index</td>
<td>Current encryption value</td>
</tr>
</tbody>
</table>
### Table 4-8: Parameters for WPA-PSK Authentication Mode

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose SSID</td>
<td>Current SSID</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Current SSID authentication mode</td>
</tr>
<tr>
<td>WPA Passphrase</td>
<td>WPA pre-shared key</td>
</tr>
<tr>
<td></td>
<td>Range: 8 – 63 characters</td>
</tr>
<tr>
<td>WPA Group Key Update Interval</td>
<td>Update interval of the WPA group key</td>
</tr>
<tr>
<td>WPA Encryption Algorithm</td>
<td>WPA encryption algorithm</td>
</tr>
</tbody>
</table>
3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result
The security properties are configured.

### 4.2.4 Viewing Associated Devices

**Short Description**
Perform this procedure to view the associated devices.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
To view the associated devices, perform the following steps:

**Steps**
1. On the **Network** tab, select **WLAN**, and then select **Associated Device**, as shown in Figure 4-11.

**Figure 4-11 Associated Device**
2. Select **SSID**, and then click **Refresh** to view the **MAC** addresses of the associated devices.

   – End of Steps –

**Result**

The associated devices are listed.

### 4.3 Address Management Configuration

This topic includes the following:

- Configuring DHCP Server
- Configuring DHCP Binding
- Configuring Specific Address Range

#### 4.3.1 Configuring DHCP Server

**Short Description**

Perform this procedure to configure the DHCP server.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the **DHCP** server, perform the following steps:

**Steps**

1. On the **Network** tab, select **Address Management**. By default, **DHCP Server** is selected, as shown in **Figure 4-12**.
2. On the **DHCP Server** tab, configure the parameters, as listed in Table 4-9.

### Table 4-9 Parameters for DHCP Server Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN IP Address</td>
<td>IP address of the LAN group (interface subnet)</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask of the LAN group</td>
</tr>
<tr>
<td>Enable DHCP Server</td>
<td>To enable or disable the DHCP server</td>
</tr>
<tr>
<td>DHCP Start IP Address</td>
<td>Starting IP address allocated by the DHCP server</td>
</tr>
<tr>
<td>DHCP End IP Address</td>
<td>Ending IP address allocated by the DHCP server</td>
</tr>
<tr>
<td>DNS Server1 IP Address</td>
<td>IP address of the DNS server</td>
</tr>
<tr>
<td>DNS Server2 IP Address</td>
<td>IP address of the DNS server</td>
</tr>
<tr>
<td>DNS Server3 IP Address</td>
<td>IP address of the DNS server</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>IP address of the default gateway</td>
</tr>
<tr>
<td>Lease Time</td>
<td>Lease time of the IP address by the DHCP server</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

Result

The DHCP server is configured.
4.3.2 Configuring DHCP Binding

Short Description
Perform this procedure to configure the DHCP binding.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the DHCP binding, perform the following steps:

Steps
1. On the Network tab, select Address Management, and then select DHCP Binding, as shown in Figure 4-13.

Figure 4-13 DHCP Binding

2. Configure binding between the MAC address and IP address. Create a DHCP binding table to map the client MAC address to the IP address.

   The DHCP server allocates IP addresses according to the binding relations, and the binding relations do not expire.

   For example, if the MAC address is set to 00-0a-e2-c6-48-ba and the IP address is set to 192.168.1.113, it indicates that the DHCP server allocates the IP address 192.168.1.113 to the host which the MAC address corresponds to.

   **Note:**
   The IP address belongs to the address pool that is provided by the DHCP server in the LAN group.
3. Click **Add** to finish the configuration. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

   – End of Steps –

**Result**

DHCP binding is configured.

### 4.3.3 Configuring Specific Address Range

**Short Description**

Perform this procedure to configure the specific address range.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the special address range, perform the following steps:

**Steps**

1. On the **Network** tab, select **Address Management**, and then select **Specific Address Range**, as shown in **Figure 4-14**.

**Figure 4-14 Specific Address Range**

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Start IP Address</th>
<th>End IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>STB</td>
<td>192.168.1.41</td>
<td>192.160.1.50</td>
<td></td>
</tr>
<tr>
<td>Camera</td>
<td>192.168.1.41</td>
<td>192.160.1.60</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td>192.168.1.71</td>
<td>192.168.1.80</td>
<td></td>
</tr>
<tr>
<td>PC</td>
<td>192.168.1.10</td>
<td>192.160.1.40</td>
<td></td>
</tr>
</tbody>
</table>

   The device is not in the scope of the following device pool, computer equipment belonging to the default.

2. Click **Modify** to modify the parameters, as shown in **Figure 4-15**.
3. In **Start IP Address** and **End IP Address**, enter the IP addresses, and then click **Modify**.

   – End of Steps –

**Result**

The specific address range is configured.

### 4.4 Route Management Configuration

This topic includes the following:

- Configuring Default Gateway
- Configuring Static Routing

#### 4.4.1 Configuring Default Gateway

**Short Description**

Perform this procedure to configure the default gateway.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the default gateway, perform the following steps:

**Steps**

1. On the **Network** tab, select **Routing Management**. By default, **Default Gateway** is selected, as shown in **Figure 4-16**.
2. From **WAN Connection**, select the connection interface at the **WAN** side.

**Note:**
This interface is available when configured on **WAN Connection**.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

**Result**
The default gateway is configured.

### 4.4.2 Configuring Static Routing

**Short Description**
Perform this procedure to configure the static routing.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
To configure the static routing, perform the following steps:

**Steps**
1. On the **Network** tab, select **Routing Management**, and then select **Static Routing**, as shown in Figure 4-17.
Table 4-10 lists the parameters for static routing configuration.

Table 4-10 Parameters for Static Routing Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Connection</td>
<td>Network-side interface type</td>
</tr>
<tr>
<td>Network Address</td>
<td>Network address</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Gateway</td>
</tr>
</tbody>
</table>

2. From the **WAN Connection** drop-down list, select the network-side interface.

3. Configure **Network Address**, **Subnet Mask**, and **Default Gateway**, as shown in Figure 4-18.

4. Click **Add** to finish the configuration, as shown in Figure 4-19. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.
Figure 4-19 Static Routing Configuration Completed

Result

The static routing is configured.
Chapter 5
Security Configuration

Table of Contents
Configuring Firewall................................................................. 5-1
Configuring IP Filter.................................................................. 5-2
Configuring URL Filter............................................................... 5-5
Configuring DMZ Host................................................................. 5-7
Configuring Port Forwarding...................................................... 5-9

5.1 Configuring Firewall

Short Description
Perform this procedure to configure the firewall.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the firewall, perform the following steps:

Steps
1. On the Web interface, click the Security tab. By default, Firewall is selected, as shown in Figure 5-1.

Figure 5-1 Firewall Configuration

2. Set the firewall parameters, as listed in Table 5-1.
### Table 5-1 Firewall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Anti-Hacking Protection</td>
<td>To enable or disable anti-hacking protection</td>
</tr>
</tbody>
</table>
| Firewall Level             | Firewall level  
  - **High**: Allow legal WAN-side access but prohibit WAN-side ping.  
  - **Low**: Allow legal WAN-side access and WAN-side ping.              |

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

- **End of Steps** -

**Result**

The firewall is configured.

### 5.2 Configuring IP Filter

**Short Description**

Perform this procedure to configure IP filter.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure IP filter, perform the following steps:

**Steps**

1. On the **Security** tab, select **IP Filter**, as shown in Figure 5-2.
Table 5-2 lists the parameters for IP filter configuration.

**Table 5-2 Parameters for IP Filter Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable the IP filter function</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol</td>
</tr>
<tr>
<td>Name</td>
<td>Name</td>
</tr>
<tr>
<td>Start Source IP Address</td>
<td>Starting source IP address</td>
</tr>
<tr>
<td>End Source IP Address</td>
<td>Ending source IP address</td>
</tr>
<tr>
<td>Start Destination IP Address</td>
<td>Starting destination IP address</td>
</tr>
<tr>
<td>End Destination IP Address</td>
<td>Ending destination IP address</td>
</tr>
<tr>
<td>Start Source Port</td>
<td>Starting source port number</td>
</tr>
<tr>
<td>End Source Port</td>
<td>Ending source port number</td>
</tr>
<tr>
<td>Start Destination Port</td>
<td>Starting destination port number</td>
</tr>
<tr>
<td>End Destination Port</td>
<td>Ending destination port number</td>
</tr>
<tr>
<td>Ingress</td>
<td>Ingress interface</td>
</tr>
<tr>
<td>Egress</td>
<td>Egress interface</td>
</tr>
<tr>
<td>Mode Discard Permit</td>
<td>Mode, including discard and permit</td>
</tr>
</tbody>
</table>
2. On the **IP Filter** tab, set the filter parameters, as shown in **Figure 5-3**.

**Figure 5-3 IP Filter Configuration**

3. Click **Add** to finish the configuration, as shown in **Figure 5-4**. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.
Chapter 5 Security Configuration

5.3 Configuring URL Filter

Short Description
Perform this procedure to configure the URL filter.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the URL filter, perform the following steps:

Steps
1. On the Security tab, select URL Filter, as shown in Figure 5-5.
Figure 5-5 URL Filter

Table 5-3 lists the parameters for URL filter configuration.

Table 5-3 Parameters for URL Filter Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable the URL filter function</td>
</tr>
<tr>
<td>Mode</td>
<td>Mode, including discard and permit</td>
</tr>
<tr>
<td>URL Address</td>
<td>URL address</td>
</tr>
</tbody>
</table>

2. On the URL Filter tab, set the filter parameters, as shown in Figure 5-6.

Figure 5-6 URL Filter Configuration

3. Click Add to finish the configuration, as shown in Figure 5-7. Click Delete to delete the configuration.
5.4 Configuring DMZ Host

Short Description
Perform this procedure to configure the DMZ host.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the DMZ host, perform the following steps:

Steps
1. On the Security tab, select DMZ Host, as shown in Figure 5-8.
2. Configure the DMZ host parameters, as shown in Figure 5-9.

![DMZ Host Configuration](image)

**Figure 5-9 DMZ Host Configuration**

Table 5-4 lists the parameters for DMZ host configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable the DMZ host</td>
</tr>
<tr>
<td>WAN Connection</td>
<td>WAN-side connection interface</td>
</tr>
<tr>
<td>DMZ Host IP Address</td>
<td>IP address of the DMZ host</td>
</tr>
</tbody>
</table>

**Note:**

After the DMZ full port mapping function is enabled, all the ports are enabled by default. The LAN-side host provides services through **DNAT**.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

5-8
Result
The DMZ host is configured.

5.5 Configuring Port Forwarding

Short Description
Perform this procedure to configure port forwarding.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure port forwarding, perform the following steps:

Steps
1. On the Security tab, select Port Forwarding, as shown in Figure 5-10.

   Figure 5-10 Port Forwarding

   ![Port Forwarding](image)

   2. Configure the port forwarding parameters, as shown in Figure 5-11.
Table 5-5 lists the parameters for port forwarding configuration.

### Table 5-5 Parameters for Port Forwarding Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable the port forwarding function</td>
</tr>
<tr>
<td>Name</td>
<td>Host name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol name, including TCP, UDP, as well as TCP and UDP protocols</td>
</tr>
<tr>
<td>WAN Host IP Address</td>
<td>Starting IP address of the WAN-side host</td>
</tr>
<tr>
<td>WAN Connection</td>
<td>WAN connection</td>
</tr>
<tr>
<td>WAN Start Port</td>
<td>Starting port number of the WAN-side host</td>
</tr>
<tr>
<td>WAN End Port</td>
<td>Ending port number of the WAN-side host</td>
</tr>
<tr>
<td>LAN Host IP Address</td>
<td>IP address of the LAN-side host</td>
</tr>
<tr>
<td>LAN Host Port</td>
<td>Port number of the LAN-side host</td>
</tr>
</tbody>
</table>

**Note:**

If a redirection policy of port access with the source address of the WAN-side IP address and the destination address of the LAN-side IP address is configured, it is used in the scenario where the WAN-side client accesses the LAN-side server.
3. Click **Add** to finish the configuration, as shown in Figure 5-12. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

**Figure 5-12 Port Forwarding Configuration Completed**

![Port Forwarding Configuration](image)

---

**Result**

Port forwarding is configured.
This page intentionally left blank.
Chapter 6
Service Configuration

Table of Contents
SIP VoIP Service Configuration ......................................................... 6-1
Configuring DDNS ................................................................. 6-10
Configuring UPnP ................................................................. 6-11
DNS Configuration ................................................................. 6-13
QoS Configuration ................................................................. 6-16
Configuring SNTP Client ......................................................... 6-26
IGMP Configuration ................................................................. 6-28
Configuring FTP Application ....................................................... 6-36

6.1 SIP VoIP Service Configuration

This topic includes the following:

● Configuring VoIP WAN Connection
● Configuring SIP
● Configuring SIP Accounts
● Configuring VoIP Advanced Parameters
● Configuring VoIP Media Parameters
● Configuring Fax

6.1.1 Configuring VoIP WAN Connection

Short Description
Perform this procedure to configure the VoIP WAN connection.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the VoIP WAN connection, perform the following steps:

Steps
1. On the Web interface, click the Application tab. Select VoIP. By default, WAN Connection is selected, as shown in Figure 6-1.
2. Select a connection interface from **WAN Connection**.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

--- **End of Steps** ---

**Result**

The VoIP WAN connection is configured.

### 6.1.2 Configuring SIP

**Short Description**

Perform this procedure to configure SIP.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure **SIP**, perform the following steps:

**Steps**

1. On the **Application** tab, select **VoIP**, and then select **SIP Protocol**, as shown in Figure 6-2.
2. Configure the SIP protocol parameters, as listed in Table 6-1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Port</td>
<td>Local port number used by the VoIP protocol</td>
</tr>
<tr>
<td>Primary Proxy Server</td>
<td>IP address of the primary proxy server</td>
</tr>
<tr>
<td>Primary Outbound Proxy Server</td>
<td>IP address of the primary outbound proxy server</td>
</tr>
<tr>
<td>Primary Proxy Port</td>
<td>Port number of the primary proxy server</td>
</tr>
<tr>
<td>Secondary Proxy Server</td>
<td>IP address of the secondary proxy server</td>
</tr>
<tr>
<td>Secondary Outbound Proxy Server</td>
<td>IP address of the secondary outbound proxy server</td>
</tr>
<tr>
<td>Secondary Proxy Port</td>
<td>Port number of the secondary proxy server</td>
</tr>
<tr>
<td>Register Expires</td>
<td>Registration expiration time</td>
</tr>
<tr>
<td></td>
<td>Unit: second</td>
</tr>
</tbody>
</table>

3. Click Submit to finish the configuration. Click Cancel to cancel the configuration.

– End of Steps –

Result

SIP is configured.
6.1.3 Configuring SIP Accounts

Short Description
Perform this procedure to configure SIP accounts.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure SIP accounts, perform the following steps:

Steps
1. On the Application tab, select VoIP, and then select SIP Accounts, as shown in Figure 6-3.

Figure 6-3 SIP Accounts

2. Click Modify to modify the account parameters, as shown in Figure 6-4.
Table 6-2 lists the parameters for SIP account configuration.

Table 6-2 Parameters for SIP Account Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Name of the SIP authentication user</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the SIP authentication user</td>
</tr>
<tr>
<td>URI</td>
<td>User registration identification, that is, the user SIP call number</td>
</tr>
</tbody>
</table>

3. Click **Modify**.

   – End of Steps –

Result

The SIP accounts are configured.

6.1.4 Configuring VoIP Advanced Parameters

Short Description

Perform this procedure to configure the VoIP advanced parameters.

Prerequisites

The user has logged in to the Web interface of the device.
Context

To configure the VoIP advanced parameters, perform the following steps:

Steps

1. On the Application tab, select VoIP, and then select Advanced, as shown in Figure 6-5.

Figure 6-5 Advanced Parameters

2. Configure the advanced parameters, as shown in Table 6-3.

Table 6-3 Advanced Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Cancellation</td>
<td>To enable or disable echo cancellation</td>
</tr>
<tr>
<td>VAD&amp;CNG</td>
<td>To enable or disable VAD and CNG</td>
</tr>
<tr>
<td>DTMF</td>
<td>DTMF mode, including RFC2833, RFC2198, and DTMF in Voice</td>
</tr>
<tr>
<td>Jitter Buffer</td>
<td>Jitter buffer, including fixed and adaptive</td>
</tr>
<tr>
<td>Min Value</td>
<td>Minimum jitter buffer value</td>
</tr>
<tr>
<td></td>
<td>Unit: ms</td>
</tr>
<tr>
<td>Max Value</td>
<td>Maximum jitter buffer value</td>
</tr>
<tr>
<td></td>
<td>Unit: ms</td>
</tr>
</tbody>
</table>

3. Click Submit to finish the configuration. Click Cancel to cancel the configuration.

– End of Steps –
Chapter 6 Service Configuration

Result
The VoIP advanced parameters are configured.

6.1.5 Configuring VoIP Media Parameters

Short Description
Perform this procedure to configure the VoIP media parameters.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure VoIP media parameters, perform the following steps:

Steps
1. On the Application tab, select VoIP, and then select Media, as shown in Figure 6-6.

   Figure 6-6 Media Parameters

![Media Parameters](image)

2. Configure the media parameters, as shown in Figure 6-7.
Figure 6-7 Media Parameter Configuration

Table 6-4 lists the media parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec Selection</td>
<td>Code type</td>
</tr>
<tr>
<td>Codec Priority</td>
<td>Code priority</td>
</tr>
<tr>
<td></td>
<td>The smaller the value is, the higher the priority is.</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

-- End of Steps --

Result

The VoIP media parameters are configured.

6.1.6 Configuring Fax

Short Description

Perform this procedure to configure fax.

Prerequisites

The user has logged in to the Web interface of the device.
Context
To configure fax, perform the following steps:

Steps
1. On the **Application** tab, select **VoIP**, and then select **Fax**, as shown in **Figure 6-8**.

**Figure 6-8 Fax Configuration**

![Fax Configuration]

2. Select **Enable T38**.

**NOTE**
To disable T38 fax mode, clear the check box.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result
Fax is configured.
6.2 Configuring DDNS

**Short Description**
Perform this procedure to configure DDNS.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
After DDNS is applied, the host that has the dynamic IP address can also provide the domain name service. For example, when the host obtains an IP address through xDSL dial-up or DHCP server dynamic allocation, and the host provides the domain name service, by using DDNS, the effect on the domain name access when the IP address changes is eliminated.

To configure DDNS, perform the following steps:

**Steps**
1. On the Application tab, select DDNS, as shown in Figure 6-9.

   ![Figure 6-9 DDNS](image)

   **Figure 6-9 DDNS**

2. Configure the DDNS parameters, as shown in Figure 6-10.
Table 6-5 lists the parameters for DDNS configuration.

### Table 6-5 Parameters for DDNS Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable the DDNS function</td>
</tr>
<tr>
<td>Server</td>
<td>Server address&lt;br&gt;If the GNUDIP HTTP protocol is used, the server address is a URL address. By default, it is <a href="http://ns.eagleeyes.com.cn/cgi-bin/gdipupdt.cgi">http://ns.eagleeyes.com.cn/cgi-bin/gdipupdt.cgi</a>.</td>
</tr>
<tr>
<td>Username</td>
<td>DDNS server user name</td>
</tr>
<tr>
<td>Password</td>
<td>DDNS server password</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain name corresponding to the user, valid only when the GNUDIP protocol is used</td>
</tr>
<tr>
<td>WAN Connection</td>
<td>WAN-side connection interface</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

**Result**

DDNS is configured.

### 6.3 Configuring UPnP

**Short Description**

Perform this procedure to configure UPnP.
Prerequisites
The user has logged in to the Web interface of the device.

Context
The UPnP function supports zero configuration and device auto-discovery. After this function is configured, the device can be dynamically added to a network to obtain the IP address, announce the function, and know the functions of other devices.

To configure UPnP, perform the following steps:

Steps
1. On the Application tab, select UPnP, as shown in Figure 6-11.

![Figure 6-11 UPnP](image1)

2. Configure the UPnP parameters, as shown in Figure 6-12.

![Figure 6-12 UPnP Configuration](image2)
Table 6-6 lists the UPnP parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>To enable UPnP</td>
</tr>
<tr>
<td>WAN Connection omci1</td>
<td>WAN-side connection interface</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

Result

UPnP is configured.

### 6.4 DNS Configuration

This topic includes the following:

- Configuring Domain Name
- Configuring Host Name

#### 6.4.1 Configuring Domain Name

**Short Description**

Perform this procedure to configure the domain name.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the domain name, perform the following steps:

**Steps**

1. On the **Application** tab, select **DNS Service**. By default, **Domain Name** is selected, as shown in Figure 6-13.
2. Set Domain Name.
3. Click Submit to finish the configuration. Click Cancel to cancel the configuration.

– End of Steps –

Result
The domain name is configured.

6.4.2 Configuring Host Name

Short Description
Perform this procedure to configure the host name.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the host name, perform the following steps:

Steps
1. On the Application tab, select DNS Service, and then select Hosts, as shown in Figure 6-14.
2. Set **Host Name** and **IP Address**, as shown in Figure 6-15.

3. Click **Add** to finish the configuration, as shown in Figure 6-16. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.
6.5 QoS Configuration

This topic includes the following:

- Configuring Basic QoS Parameters
- Configuring QoS Rule
- Configuring QoS Rule Type
- Configuring QoS Local Application
- Configuring QoS Queue Management
- Configuring QoS Ingress Rate Limit

6.5.1 Configuring Basic QoS Parameters

Short Description

Perform this procedure to configure the basic QoS parameters.

Prerequisites

The user has logged in to the Web interface of the device.

Context

To configure the basic QoS parameters, perform the following steps:

Result

The host name is configured.
Steps

1. **On the Application tab, select QoS.** By default, **Basic** is selected, as shown in **Figure 6-17**.

   **Figure 6-17 Basic QoS Parameters**

   ![Figure 6-17 Basic QoS Parameters](image)

   **Note:**

   The template index is enabled immediately after changed.

2. **Configure the basic QoS parameters,** as shown in **Figure 6-18**.

   ![Figure 6-18 QoS Parameters](image)
Figure 6-18 Basic QoS Parameter Configuration

Table 6-7 lists the basic QoS parameters.

### Table 6-7 Basic QoS Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Index</td>
<td>Template index</td>
</tr>
<tr>
<td>Enable QoS</td>
<td>To enable or disable the QoS function</td>
</tr>
<tr>
<td>The Total Upstream Bandwidth</td>
<td>Upstream bandwidth through the WAN port</td>
</tr>
<tr>
<td></td>
<td>Range: 8000 – 104857600 bps</td>
</tr>
<tr>
<td>Queue Scheduling Algorithm</td>
<td>Queue scheduling algorithm</td>
</tr>
<tr>
<td></td>
<td>Range: SP and DWRR</td>
</tr>
<tr>
<td>DWRR bandwidth locked</td>
<td>To lock DWRR bandwidth (when the queue scheduling algorithm is DWRR)</td>
</tr>
<tr>
<td>Enable DSCP Re-marking</td>
<td>To enable or disable DSCP remarking</td>
</tr>
<tr>
<td>802.1P Re-mark Model</td>
<td>To enable or disable the 802.1p remarking mode</td>
</tr>
<tr>
<td></td>
<td>Range: disable, transparent transmission, and enable</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

---

**End of Steps**

**Result**

The basic QoS parameters are configured.
6.5.2 Configuring QoS Rule

Short Description

Perform this procedure to configure the QoS rule.

Prerequisites

The user has logged in to the Web interface of the device.

Context

To configure the QoS rule, perform the following steps:

Steps

1. On the Application tab, select QoS, and then select Rule, as shown in Figure 6-19.

Figure 6-19 QoS Rule

2. Configure the QoS rule parameters, as shown in Figure 6-20.
Table 6-8 lists the parameters for QoS rule configuration.

Table 6-8 Parameters for QoS Rule Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1p Re-marking</td>
<td>802.1P remarking</td>
</tr>
<tr>
<td>DSCP Re-marking</td>
<td>DSCP remarking</td>
</tr>
<tr>
<td>CAR(Committed Access Rate)</td>
<td>Ingress rate limit rule</td>
</tr>
<tr>
<td>Queue</td>
<td>Congestion management queue</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result

The QoS rule is configured.

6.5.3 Configuring QoS Rule Type

Short Description

Perform this procedure to configure the QoS rule type.

Prerequisites

The user has logged in to the Web interface of the device.
Context

To configure the QoS rule type, perform the following steps:

Steps

1. On the Application tab, select QoS, and then select Rule Type, as shown in Figure 6-21.

**Figure 6-21 Rule Type**

![Rule Type Configuration](image)

2. Configure the QoS rule type parameters, as shown in Table 6-9.

   **Table 6-9 Parameters for QoS Rule Type Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification Rules</td>
<td>Classification rules</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol</td>
</tr>
<tr>
<td>Type</td>
<td>Type</td>
</tr>
<tr>
<td>Minimum</td>
<td>Minimum value</td>
</tr>
<tr>
<td>Maximum</td>
<td>Maximum value</td>
</tr>
</tbody>
</table>

   | Range: TCP, UDP, ICMP, and RTP |

3. Click Add to finish the configuration, as shown in Figure 6-22.
4. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

   – End of Steps –

**Result**

The QoS rule type is configured.

### 6.5.4 Configuring QoS Local Application

**Short Description**

Perform this procedure to configure the QoS local application.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To configure the QoS local application, perform the following steps:

**Steps**

1. On the **Application** tab, select **QoS**, and then select **Local Application**, as shown in Figure 6-23.
2. In the **Queue** drop-down list, select a queue number.

**Note:**
At present, only the TR069 service mode is supported.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

**Result**
The QoS local application is configured.

### 6.5.5 Configuring QoS Queue Management

**Short Description**
Perform this procedure to configure QoS queue management.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
To configure QoS queue management, perform the following steps:
Steps

1. On the Application tab, select QoS, and then select Queue Management, as shown in Figure 6-24.

Figure 6-24 Queue Management

2. Click the Modify icons in the table to modify the queue management functions.
3. Select or clear Enable to enable or disable the queue management function.
4. Click Modify to finish the configuration.

Note:

1 indicates enabled and 0 indicates disabled.

When the congestion management algorithm is DWRR, the queue weight needs to be configured.

Weight refers to the ratio of the data flow passing through the queues to the total data flow.

– End of Steps –

Result

QoS queue management is configured.
6.5.6 Configuring QoS Ingress Rate Limit

Short Description
Perform this procedure to configure the QoS ingress rate limit.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the QoS ingress rate limit, perform the following steps:

Steps
1. On the Application tab, select QoS, and then select Ingress Rate Limit, as shown in Figure 6-25.

   **Figure 6-25 Ingress Rate Limit**

2. Configure the parameters for QoS ingress rate limit, as shown in Figure 6-26.
Table 6-10 lists the parameters for ingress rate limit configuration.

**Table 6-10 Parameters for Ingress Rate Limit Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visiting Interface</td>
<td>User interface for the rate limit rule</td>
</tr>
<tr>
<td>Enable</td>
<td>To enable the ingress rate limit function</td>
</tr>
<tr>
<td>Rate</td>
<td>Limit rate</td>
</tr>
<tr>
<td></td>
<td>8000 bps – 104857600 bps</td>
</tr>
</tbody>
</table>

3. Click **Add** to finish the configuration. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

– End of Steps –

**Result**

The QoS ingress rate limit is configured.

### 6.6 Configuring SNTP Client

**Short Description**

Perform this procedure to configure the SNTP client.

**Prerequisites**

The user has logged in to the Web interface of the device.
To configure the SNTP client, perform the following steps:

1. On the Application tab, select SNTP, as shown in Figure 6-27.

2. Configure the SNTP parameters, as shown in Figure 6-27.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Time zone where the subscriber is located</td>
</tr>
<tr>
<td>Primary NTP Server Address</td>
<td>IP address of the primary NTP server</td>
</tr>
</tbody>
</table>
### 6.7 IGMP Configuration

This topic includes the following:
- Configuring Basic IGMP Parameters
- Configuring Multicast VLAN
- Configuring Multicast MAC Limit
- Configuring MVLANTag Strip

#### 6.7.1 Configuring Basic IGMP Parameters

**Short Description**
Perform this procedure to configure the basic IGMP parameters.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
To configure the basic IGMP parameters, perform the following steps:

**Steps**
1. On the Application tab, select IGMP. By default, Basic is selected, as shown in Figure 6-29.
2. IGMP Mode includes IGMP Snooping, IGMP Proxy, and Disabled. Disabled indicates to disable the IGMP mode configuration.
   - Configure IGMP Snooping.
     From the IGMP Mode drop-down list, select IGMP Snooping, as shown in Figure 6-30.

![Figure 6-30 IGMP Snooping Configuration](image)

Table 6-12 lists the parameters for IGMP snooping configuration.

### Table 6-12 Parameters for IGMP Snooping Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Mode</td>
<td>IGMP mode</td>
</tr>
<tr>
<td>Multicast MAC Aging Time</td>
<td>Aging time of the multicast address</td>
</tr>
</tbody>
</table>
- Configure **IGMP Proxy**.

From the **IGMP Mode** drop-down list, select **IGMP Proxy**, as shown in **Figure 6-31**.

**Figure 6-31 IGMP Proxy Configuration**

Table 6-13 lists the parameters for IGMP proxy configuration.

**Table 6-13 Parameters for IGMP Proxy Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Mode</td>
<td>IGMP mode</td>
</tr>
<tr>
<td>Multicast MAC Aging Time</td>
<td>Aging time of the multicast address</td>
</tr>
<tr>
<td>Report Time</td>
<td>Periodical report time of multicast messages</td>
</tr>
</tbody>
</table>

**Note:**

ZXA10 F660 periodically reports the IGMP member report messages to the upper-layer multicast router according to the **Report Time**.

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

- **End of Steps** -
Result
The basic IGMP parameters are configured.

6.7.2 Configuring Multicast VLAN

Short Description
Perform this procedure to configure the multicast VLAN.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the multicast VLAN, perform the following steps:

Steps
1. On the Application tab, select IGMP, and then select Multicast VLAN, as shown in Figure 6-32.

   Figure 6-32 Multicast VLAN

2. Configure the multicast VLAN parameters, as shown in Figure 6-33.
Table 6-14 lists the parameters for the multicast VLAN configuration.

Table 6-14 Parameters for Multicast VLAN Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Mode</td>
<td>IGMP mode, configured on the Basic tab</td>
</tr>
<tr>
<td>Enable Multicast VLAN</td>
<td>To enable the multicast VLAN function</td>
</tr>
<tr>
<td>Enable Translation</td>
<td>To enable multicast VLAN translation</td>
</tr>
<tr>
<td>Multicast VLAN</td>
<td>To create a multicast VLAN</td>
</tr>
<tr>
<td>New VLAN</td>
<td>Multicast VLAN ID</td>
</tr>
<tr>
<td>Interface Name</td>
<td>LAN interface to be added to the multicast VLAN</td>
</tr>
</tbody>
</table>

3. Click Submit to finish the configuration. Click Cancel to cancel the configuration.

   – End of Steps –

Result

The multicast VLAN is configured.

6.7.3 Configuring Multicast MAC Limit

Short Description

Perform this procedure to configure multicast MAC limit.

Prerequisites

The user has logged in to the Web interface of the device.
Context

The multicast MAC limit function can be configured only when the IGMP mode is IGMP Snooping. IGMP Proxy does not support this function.

To configure multicast MAC limit, perform the following steps:

Steps

1. On the Application tab, select IGMP, and then select Multicast MAC Limit, as shown in Figure 6-34.

   Figure 6-34 Multicast MAC Limit

   ![Multicast MAC Limit](image)

   Table 6-15 lists the parameters for the multicast MAC limit configuration.

   Table 6-15

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Multicast MAC Address Limit</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN1</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>LAN2</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>LAN3</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>LAN4</td>
<td>256</td>
<td></td>
</tr>
</tbody>
</table>

2. Click the Modify icon to configure the multicast MAC limit, as shown in Figure 6-35.

   Figure 6-35 Multicast MAC Limit Configuration

   ![Multicast MAC Limit Configuration](image)
### Table 6-15 Parameters for Multicast MAC Limit Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast MAC Address Limit</td>
<td>Maximum multicast addresses for each LAN port</td>
</tr>
<tr>
<td></td>
<td>Range: 0 – 256</td>
</tr>
</tbody>
</table>

3. Click **Modify**.

    – End of Steps –

**Result**

Multicast MAC limit is configured.

### 6.7.4 Configuring MVLAN Tag Strip

**Short Description**

Perform this procedure to configure MVLAN tag strip.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

The MVLAN tag strip function can be configured only when the IGMP mode is **IGMP Snooping**. **IGMP Proxy** does not support this function.

To configure MVLAN tag strip, perform the following steps:

**Steps**

1. On the Application tab, select **IGMP**, and then select **Tag Stripe**, as shown in Figure 6-36.
2. Click the **Modify** icon to configure MVLAN tag strip, as shown in **Figure 6-37**.

![Figure 6-37 MVLAN Tag Strip Configuration](image)

**Table 6-16** lists the parameters for MVLAN tag strip configuration.

**Table 6-16 Parameters for MVLAN Tag Strip Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Tag Stripe</td>
<td>To enable the MVLAN tag strip function</td>
</tr>
</tbody>
</table>

3. Click **Modify**.

  – End of Steps –

**Result**

MVLAN tag strip is configured.
6.8 Configuring FTP Application

**Short Description**
Perform this procedure to configure FTP application.

**Prerequisites**
The user has logged in to the Web interface of the device.

**Context**
To configure FTP application, perform the following steps:

**Steps**
1. On the Application tab, select FTP Application, as shown in Figure 6-38.

   **Figure 6-38 FTP Server**

   ![FTP Server](image)

2. Configure the FTP server parameters, as shown in Figure 6-39.

   **Figure 6-39 FTP Server Configuration**

   ![FTP Server Configuration](image)
Table 6-17 lists the FTP server parameters.

**Table 6-17 FTP Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FTP Server</td>
<td>To enable the FTP server</td>
</tr>
<tr>
<td>FTP Username</td>
<td>FTP login user name</td>
</tr>
<tr>
<td>FTP Password</td>
<td>FTP login password</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

**Result**

FTP application is configured.
This page intentionally left blank.
Chapter 7
Device Management

Table of Contents
TR069 Configuration ................................................................................................................. 7-1
User Management ......................................................................................................................... 7-4
Device Management ..................................................................................................................... 7-5
Log Management .......................................................................................................................... 7-9
Ping Diagnosis .............................................................................................................................. 7-10

7.1 TR069 Configuration
This topic includes the following:

- Configuring Basic TR069 Parameters
- Importing TRO69 Certificate

7.1.1 Configuring Basic TR069 Parameters

Short Description
Perform this procedure to configure the basic TR069 parameters.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To configure the basic TR069 parameters, perform the following steps:

Steps
1. On the Administration tab, select TR-069. By default, Basic is selected, as shown in Figure 7-1.
2. Configure the basic TR069 parameters, as shown in Figure 7-2.

Figure 7-2 Basic TR069 Parameter Configuration

Table 7-1 lists the basic TR069 parameters.

Table 7-1 Basic TR069 Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Connection</td>
<td>WAN-side connection interface</td>
</tr>
<tr>
<td>ACS URL</td>
<td>Network server URL</td>
</tr>
<tr>
<td>Username</td>
<td>User name</td>
</tr>
<tr>
<td>Password</td>
<td>Password</td>
</tr>
<tr>
<td>Connection Request URL</td>
<td>Connection request URL</td>
</tr>
<tr>
<td>Connection Request User</td>
<td>Connection request user name</td>
</tr>
</tbody>
</table>
Chapter 7 Device Management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Request Password</td>
<td>Connection request password</td>
</tr>
<tr>
<td>Enable Periodic Inform</td>
<td>To enable periodic report</td>
</tr>
<tr>
<td>Periodic Inform Interval</td>
<td>Periodic report interval</td>
</tr>
<tr>
<td>Enable Certificate</td>
<td>To enable certificate</td>
</tr>
</tbody>
</table>

3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result
The basic TR069 parameters are configured.

7.1.2 Importing TRO69 Certificate

Short Description
Perform this procedure to import the TR069 certificate.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To import the TR069 certificate, perform the following steps:

Steps
1. On the **Administration** tab, select TR-069, and then select **Certificate**, as shown in Figure 7-3.

![Figure 7-3 TRO69 Certificate](Image)

2. Click **Browse** to select the certificate file.
3. Click **Import Certificate** to import the file.

   – End of Steps –

**Result**

The TR069 certificate is imported.

### 7.2 User Management

**Short Description**

Perform this procedure to manage users.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To manage users, perform the following steps:

**Steps**

1. On the **Administration** tab, select **User Management**, as shown in Figure 7-4.

**Figure 7-4 User Management**

![User Management Interface](image)

2. Configure the user management parameters.

   **Note:**

   **User Right** includes **Administrator** and **User**.
3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

**Result**

User management is complete.

7.3 Device Management

This topic includes the following:

- System Management
- Software Upgrade
- Configuration Management

7.3.1 System Management

**Short Description**

Perform this procedure to manage the system.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

To manage the system, perform the following steps:

**Steps**

1. On the **Administration** tab, select **System Management**, as shown in **Figure 7-5**.

**Figure 7-5 System Management**

2. Click **Reboot** to reboot the device.
3. Click **Restore Default** to restore the system to the factory default settings.

   – End of Steps –

**Result**

System management is complete.

### 7.3.2 Software Upgrade

**Short Description**

Perform this procedure to upgrade the software.

**Prerequisites**

The user has logged in to the Web interface of the device.

**Context**

⚠ **Caution!**

Generally, the software is upgraded by the ZTE CORPORATION engineers. If the user wants to upgrade the software, contact the local office of ZTE CORPORATION to obtain the latest software version.

To upgrade the software, perform the following steps:

**Steps**

1. On the **Administration** tab, select **System Management**, and then select **Software Upgrade**, as shown in **Figure 7-6**.

   **Figure 7-6 Software Upgrade**

2. Click **Browse** to select the software version.

3. Click **Upgrade** to upgrade the software, as shown in **Figure 7-7**.
Figure 7-7 Upgrading Software

Figure 7-8 shows the result of software upgrade.

**Figure 7-8 Software Upgrade Completed**

**Note:**

During the upgrade process, the device cannot be powered off; otherwise, it may be damaged.

During the upgrade process, the system prompts a message. After the upgrade is complete, the system returns to the login interface.

---

**Result**

The software is upgraded.
7.3.3 Configuration Management

Short Description
Perform this procedure to manage the device configuration.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To manage the device configuration, perform the following steps:

Steps
1. On the Administration tab, select System Management, and then select Configuration Management, as shown in Figure 7-9.

2. Click Backup Configuration to back up the existing configuration file.

3. Click Browse to select the backed up configuration file.

4. Click Restore Configuration to restore the backed up configuration file, as shown in Figure 7-10.
7.4 Log Management

Short Description
Perform this procedure to manage logs.

Prerequisites
The user has logged in to the Web interface of the device.

Context
To manage logs, perform the following steps:

Steps
1. On the Administration tab, select Log Management, as shown in Figure 7-11.
2. Configure the log management parameters, as listed in Table 7-2.

### Table 7-2 Log Management Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Enable</td>
<td>Whether to enable the log server</td>
</tr>
<tr>
<td>Log Level</td>
<td>Log level, including <strong>Debug</strong>, <strong>Informational</strong>, <strong>Notice</strong>, <strong>Warning</strong>, <strong>Error</strong>, <strong>Critical</strong>, <strong>Alert</strong>, and <strong>Emergency</strong> When Log Level is configured, only the logs above the specified level are saved.</td>
</tr>
</tbody>
</table>

3. Click **Refresh** to display the latest 20 logs.
4. Click **Clear Log** to clear the current log records.
5. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

   – End of Steps –

**Result**

Log management is complete.

### 7.5 Ping Diagnosis

**Short Description**

Perform this procedure to diagnose ping connection.

**Prerequisites**

The user has logged in to the Web interface of the device.
Context
To diagnose ping connection, perform the following steps:

Steps
1. On the Administration tab, select Diagnosis, as shown in Figure 7-12.

Figure 7-12 Ping Diagnosis

2. In Input IP Address or host name, enter the host IP address or host name.
3. Click Submit to diagnose the connection, as shown in Figure 7-13. Click Cancel to cancel the configuration.

Figure 7-13 Ping Diagnosis Result

– End of Steps –

Result
Ping diagnosis is complete.
This page intentionally left blank.
Chapter 8
FAQ

Table of Contents
FAQ ...........................................................................................................8-1

8.1 FAQ

How Can I set TCP/IP on the Computer Connected to the Device?
The default device IP address is 192.168.1.1. Therefore, set the computer IP address to 192.168.1.2 – 192.168.1.254 and the subnet mask to 255.255.255.0.

How Can I Ensure That My Computer Is Successfully Connected to the Device?
On the command line interface, carry out the ping 192.168.1.1 command. If the connection fails, the interface prompts connection timeout.

How Can I Set the Device Through the Web Interface?
Make sure that the computer is connected to the device. Then open the Internet Explorer and enter http://192.168.1.1 on the address bar to access the Web interface of the device. The default user name and password are admin.

How Can I Restore the Device to the Factory Default Settings?
Press the RST reset button for more than 10 seconds to reboot the device. Then the device is restored to the factory default settings.

Why Is the PON Link Indicator Always OFF?
If the PON link indicator is always OFF, it indicates that the PON link is not successfully set up. Make sure that the fiber is correctly connected with the PON port and the subscriber device. Make sure that the tail fiber is straight and is in good condition.

Why Does the Device Fail to Make a Call?
Check whether the telephone cable is correctly connected to the POTS1 or POTS2 port. Then access the Web interface of the device. Click the Application tab to check the VoIP configuration. If the VoIP configuration is correct and the telephone cable is correctly connected, but the call still cannot be made, contact the service provider.
This page intentionally left blank.
Glossary

CATV
- CAble Televsion

CNG
- Comfort Noise Generation

DC
- Direct Current

DDNS
- Dynamic Domain Name Server

DHCP
- Dynamic Host Configuration Protocol

DMZ
- Demilitarized Zone

DNAT
- Destination Network Address Translation

DNS
- Domain Name Server

DSCP
- Differentiated Services Code Point

DSL
- Digital Subscriber Line

DTMF
- Dual-ToneMulti-Frequency

DWRR
- Deficit Weighted Round Robin

FTP
- File Transfer Protocol

FTTH
- Fiber to the Home

GE
- Gigabit Ethernet

GPON
- Gigabit Passive Optical Network

HTTP
- Hypertext Transfer Protocol
ICMP
- Internet Control Message Protocol

IEEE
- Institute of Electrical and Electronics Engineers

IGMP
- Internet Group Management Protocol

IP
- Internet Protocol

IPTV
- Internet Protocol Television

ISP
- Internet Service Provider

ITU
- International Telecommunications Union

LAN
- Local Area Network

MAC
- Medium Access Control

NAT
- Network Address Translation

NTP
- Network Time Protocol

OLT
- Optical Line Terminal

OMCI
- ONT Management Control Interface

ONT
- Optical Network Terminal

ONU
- Optical Network Unit

PON
- Passive Optical Network

POTS
- Plain Old Telephone Service

PPPoE
- Point to Point Protocol over Ethernet

QoS
- Quality of Service
RF
- Radio Frequency

RTP
- Real-time Transport Protocol

SIP
- Session Initiation Protocol

SNTP
- Simple Network Time Protocol

SP
- Strict Priority

SS
- Soft Switch

TCP
- Transfer Control Protocol

TCP/IP
- Transfer Control Protocol/Internet Protocol

UDP
- User Datagram Protocol

URL
- Uniform Resource Locator

VAD
- Voice Activity Detectors

VLAN
- Virtual Local Area Network

VoIP
- Voice over Internet Protocol

WAN
- Wide Area Network

WEP
- Wired Equivalent Privacy

WLAN
- Wireless Local Area Network

WPA
- Wi-Fi Protected Access

Wi-Fi
- Wireless Fidelity