ZXHN H298N
Home Gateway
Maintenance Manual

Version: V1.1

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26770800
Fax: +86-755-26770801
URL: http://ensupport.zte.com.cn
E-mail: 800@zte.com.cn

LEGAL INFORMATION

CE0197

Copyright © 2012 ZTE CORPORATION.

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

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

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

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

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

Users may visit ZTE technical support website http://ensupport.zte.com.cn to inquire related information.

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

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2012–10–08	First Edition

Serial No. SJ-20121008091953-002

Publishing Date: 2012-10-08 (R1.0)

Contents

About This Manual **7**
Declaration of RoHS Compliance **10**
Safety Precautions **11**
1 Overview **12**
1.1 Product Introduction 12
1.2 Packing List 12
1.3 Product Features 13
1.4 Interfaces and Buttons 14
1.5 Indicators 16
1.6 Technical Specifications 17
2 Configuration Preparation **19**
2.1 Hardware Connection 19
2.2 Configuring TCP/IP 22
2.3 Logging In to the Device 23
3 Status **25**
3.1 Device Information 25
3.2 Network Interface 25
3.2.1 WAN Connection 25
3.2.2 4in6 Tunnel Connection 26
3.2.3 6in4 Tunnel Connection 27
3.2.4 Ethernet 27
3.3 User Interface 28
3.3.1 WLAN 28
3.3.2 Ethernet 29
3.3.3 USB 30
3.4 VoIP Status 31
4 Network **32**
4.1 WAN 32
4.1.1 WAN Connection 32
4.1.2 4in6 Tunnel Connection 34
4.1.3 6in4 Tunnel Connection 36
4.1.4 Port Binding 37

4.2 WLAN 38
4.2.1 Basic WLAN Configuration 38
4.2.2 SSID Settings 41
4.2.3 Security 42
4.2.4 Access Control List 47
4.2.5 Associated Devices 48
4.2.6 WiFi Restrictions 49
4.3 LAN 50
4.3.1 DHCP Server 51
4.3.2 DHCP Server(IPv6) 52
4.3.3 DHCP Binding 53
4.3.4 DHCP Port Service 55
4.3.5 Static Prefix 55
4.3.6 Prefix Delegation 57
4.3.7 DHCP Port Service(IPv6) 58
4.3.8 RA Service 59
4.4 Routing(IPv4) 60
4.4.1 Default Gateway 60
4.4.2 Static Routing 61
4.4.3 Policy Routing 62
4.4.4 Routing Table 64
4.5 Routing(IPv6) 64
4.5.1 Default Gateway 65
4.5.2 Static Routing 65
4.5.3 Policy Routing 66
4.5.4 Routing Table 67
5 Security 69
5.1 Firewall 69
5.2 IP Filter 70
5.3 MAC Filter 71
5.4 URL Filter 73
5.5 Service Control 74
5.6 ALG 75
6 Application 77
6.1 VoIP 77

6.1.1 WAN Connection 77
6.1.2 Advanced 78
6.1.3 Fax 80
6.1.4 SIP 82
6.1.5 SIP Accounts 83
6.1.6 Media 85
6.1.7 VoIP Services 87
6.2 DDNS 88
6.3 DMZ Host 90
6.4 UPnP 91
6.5 UPnP Port Mapping 93
6.6 Port Forwarding 93
6.7 DNS Service 95
6.7.1 Domain Name 95
6.7.2 Hosts 96
6.7.3 DNS 98
6.8 QoS 99
6.8.1 Basic 99
6.8.2 Classification 101
6.8.3 Queue Management 103
6.8.4 Committed Access Rate 105
6.9 SNTP 107
6.10 IGMP 108
6.10.1 WAN Connection 108
6.10.2 Basic Configuration 109
6.11 MLD 110
6.11.1 MLD Snooping 110
6.11.2 MLD Proxy 111
6.12 USB Storage 112
6.13 FTP Application 113
6.14 Port Trigger 115
6.15 Port Forwarding (Application List) 116
6.16 Application List 117
7 Administration 120
7.1 TR-069 120

7.1.1 Basic 120
7.1.2 Certificate 121
7.2 User Management 122
7.3 System Management 124
7.3.1 System Management 124
7.3.2 Software Upgrade 125
7.3.3 User Configuration Management 125
7.3.4 Default Configuration Management 126
7.4 Diagnosis 127
7.4.1 Ping Diagnosis 127
7.4.2 Trace Route Diagnosis 128
7.5 IPv6 Switch 129
Glossary 131

About This Manual

Purpose

This manual provides procedures and guidelines that support the maintenance of the ZXHN H298N.

Intended Audience

This document is intended for:

- Network planning engineer
- Installation debugging engineer
- On-site maintenance engineer
- Network monitoring engineer
- System maintenance engineer
- Data configuration engineer

What Is in This Manual

This manual contains the following chapters:

Chapter	Summary
1, Overview	Describes the product packing list, product features, interfaces and indicators, and technical specifications.
2, Configuration Preparation	Describes the hardware connection, TCP/IP configuration, and login procedure.
3, Status	Describes how to view the device status.
4, Network	Describes the network configuration, including WAN configuration, configuration, WLAN configuration, LAN configuration, routing management, and IPv6 routing management.
5, Security	Describes the configuration of the firewall, IP filter, MAC filter, URL filter, service control, and ALG.

Chapter	Summary
6, Application	Describes the configuration of VoIP, DDNS, DMZ host, UPnP, UPnP port mapping, port forwarding, DNS service, QoS, SNTP, IGMP, MLD, USB storage, DMS, FTP, port triggering, port forwarding (Application List), and application list.
7, Administration	Describes the configuration of TR-069, user management, system management, log management, and system diagnosis.

Conventions

ZTE documents employ the following typographical conventions.

Typeface	Meaning
Italics	References to other Manuals and documents.
“Quotes”	Links on screens.
Bold	Menus, menu options, function names, input fields, radio button names, check boxes, drop-down lists, dialog box names, window names.
CAPS	Keys on the keyboard and buttons on screens and company name.
	Note: Provides additional information about a certain topic.
	Checkpoint: Indicates that a particular step needs to be checked before proceeding further.
	Tip: Indicates a suggestion or hint to make things easier or more productive for the reader.

Mouse operation conventions are listed as follows:

Typeface	Meaning
Click	Refers to clicking the primary mouse button (usually the left mouse button) once.
Double-click	Refers to quickly clicking the primary mouse button (usually the left mouse button) twice.
Right-click	Refers to clicking the secondary mouse button (usually the right mouse button) once.

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 the ZXHN H298N 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)

…

The ZXHN H298N manufactured by ZTE CORPORATION meets the requirements of EU 2002/95/EC; however, some assemblies are customized to client specifications. Addition of specialized, customer-specified materials or processes which do not meet the requirements of EU 2002/95/EC may negate RoHS compliance of the assembly. To guarantee compliance of the assembly, the need for compliant product must be communicated to ZTE CORPORATION in written form. 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.

Safety Precautions

Before using the device, read the following safety precautions. ZTE bears no liability to the consequences incurred by violation of the safety instructions.

- Read the user manuals before using the device.
- Pay attention to all the cautions in the user manuals and on the product.
- To avoid fire or product damage, do not use accessories that are not related to this product.
- Use the power adapter delivered with the device.
- Do not put anything on the device.
- Keep the device dry, clean, and well-ventilated.
- In thunder days, disconnect the device from the power supply to avoid thunder attack.
- Use soft and dry cloth to clean the device. Do not use liquid or spray to clean the device. Before cleaning the device, disconnect the power supply.
- Keep the air vent clean. Anything that dropping down into the device through the air vent may cause short circuit and lead to device damage or fire.
- Keep any liquid away from the device surface.
- Do not open the shell of the device, especially when the device is powered ON.

1 Overview

1.1 Product Introduction

The ZXHN H298N is an access device. The ZXHN H298N adopts computer network and broadband network access technologies to build a household network center, which interconnects network devices at your home to access the Internet. It provides users with diversified, personalized, convenient, comfortable, safe, and efficient services.

1.2 Packing List

After opening the ZXHN H298N packing box, make sure that it contains the following components, as listed in Table 1.

Table 1 Packing List

Component Name	Count	Image
ZXHN H298N host	1	
AC-DC power adapter	1	

Component Name	Count	Image
RJ-45 network cable	2	
RJ-11 telephone cable	1	

The *ZXHN H298N Home GateWay User Manual* is delivered with the product.

If any of the components is incorrect, lost, or damaged, contact the product agency. If you want to change the product, keep the packing box and components.

1.3 Product Features

The ZXHN H298N supports the following features:

- Providing one GE port with RJ-45 connector for Ethernet Uplink
- Providing four GE ports with RJ-45 connector for LAN
- Providing one USB 2.0 host
- Providing two FXS ports
- Supporting 802.11b/g/n
- Supporting Bridge and Router mode
- Supporting IGMPv2/v3 snooping in bridge mode and route mode
- Supporting TR069 remote management
- Supporting NAT/NPAT (Network Port Address Translation)
- Supporting ALGs (Application Level Gateways)
- Supporting Port mapping
- Supporting DMZ
- Supporting UPnP IGD (Internet Gateway Device) with NAT traversal capability
- Supporting Static Routing
- Supporting DNS Proxy
- Supporting DHCP Server/Client
- Supporting SNTP (Simple Network Time Protocol) to get current time from network time server

- Supporting IP QoS for prioritizing the transmission of different traffic classes
- Supporting Interface based marking with 802.1p bit and DSCP bit
- High reliability, simple operation and low power consumption

1.4 Interfaces and Buttons

Figure 1 and Figure 2 show the ZXHN H298N interfaces and buttons.

Figure 1 Interfaces and Buttons



Figure 2 USB Interface



Table 2 describes the ZXHN H298N interfaces and buttons.

Table 2 Interfaces and Buttons

Interface/Button	Description
ON/OFF	Power button
WPS	Establish WLAN Push-Button connection.
WLAN	WLAN button, used to switch on/off WLAN.
Reset	Reset button, used to restore the factory default settings when pressed for more than 5 seconds in power-ON state.
Power	Power jacket, 12 V DC.
LAN1–LAN4	RJ-45 LAN network ports, connected to the local network through the RJ-45 network cable.
Phone1 – Phone2	RJ-11 port, connected to the phone through the telephone line.
WAN	Uplink Ethernet interface.
USB1	USB HOST port, used for the USB storage device connection.

1.5 Indicators

Figure 3 shows the ZXHN H298N indicators.

Figure 3 Indicators



Table 3 describes the indicators on the front panel.

Table 3 Indicators on the Front Panel

Indicator	Color	Status	Description
Power	–	OFF	The device is powered OFF.
	Green	ON	The device is powered ON .
WAN	–	OFF	The link is not activated.
	Green	Flashing	There is data flow.
		ON	The link is activated.

Indicator	Color	Status	Description
Internet	–	OFF	The default route is not established.
	Green	Flashing	The default route is established .There is data flow through the route.
		ON	The default route is established.
LAN1–LAN4	–	OFF	There is Ethernet fault./ The network is disconnected.
	Green	Flashing	The network is in connection. There is data flow.
		ON	The network is in connection. There is no data flow.
WLAN	–	OFF	There is a fault./WLAN is disabled.
	Green	Flashing	There is data flow.
		ON	WLAN module is enabled. There is no data flow.
WPS	–	OFF	WPS button is not used./The indication of successful connection is over./There is a fault.
	Green	Flashing	WPS function is enabled. The device is implementing the relevant negotiations.
		ON	Wireless connection is successful. The indicator is OFF in five minutes.
Phone1 – Phone2	–	OFF	The device is not powered on/ The device fails to register to the soft switch.
	Green	Flashing	There is data flow.
		ON	The device has registered to the soft switch successfully. However, there is no data flow.
USB1	–	OFF	USB port is disabled or USB device is not connected.
	Green	Flashing	Date is transmitting through USB port.
		ON	USB device is connected and available.

1.6 Technical Specifications

Table 4 lists the ZXHN H298N technical specifications.

Table 4 Technical Specifications

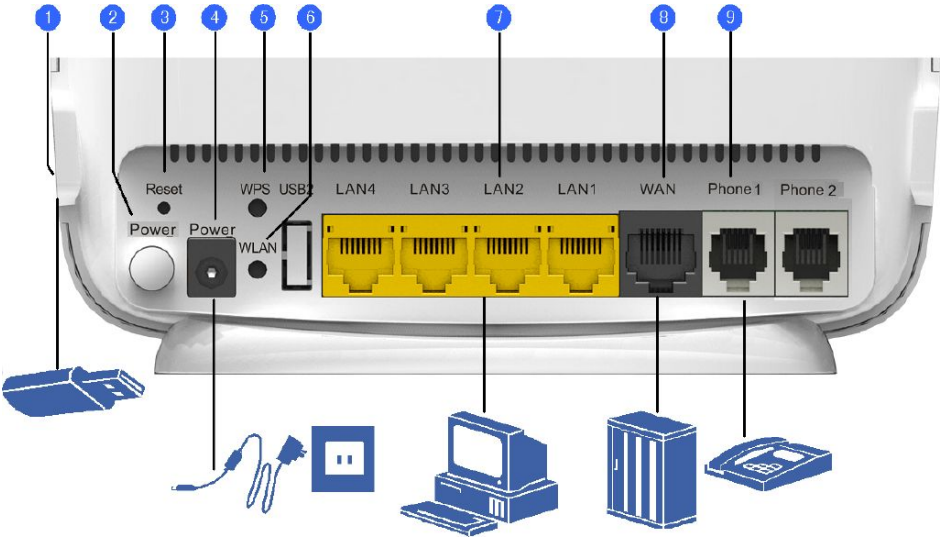
Item	Specification
Dimensions (Without the base)	170 mm × 56 mm × 140 mm (Length × Width × Height)
Rated current	1 A
Rated voltage	12 V DC
Working temperature	0℃ to 45℃
Working humidity	5% – 95%
Storage temperature	–40℃ to 70℃
Storage humidity	10% –100%

2 Configuration Preparation

2.1 Hardware Connection

Figure 4 shows the entire connections between the ZXHN H298N and other devices.

Figure 4 Entire Connection

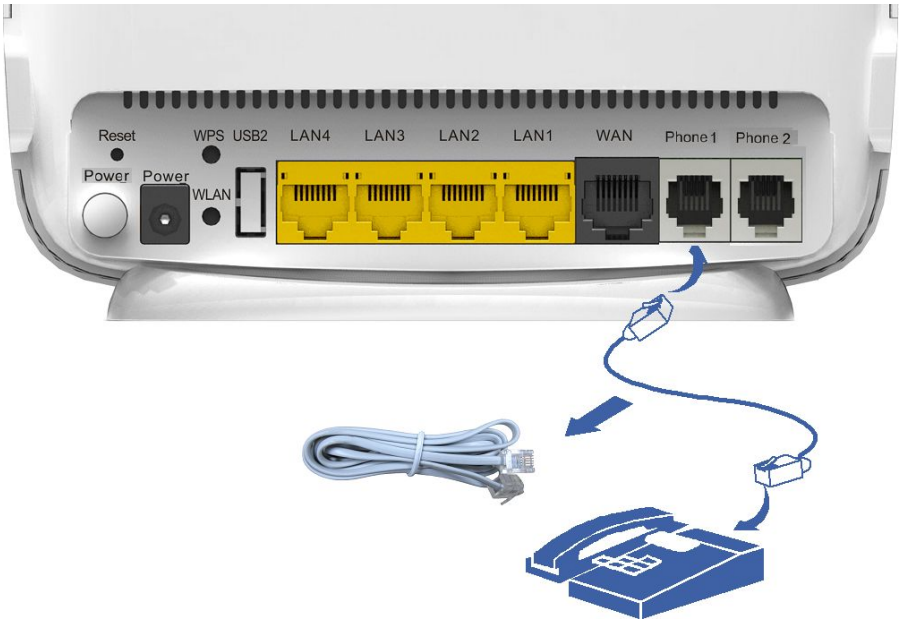


1. USB interface
2. Power button
3. Reset button
4. Power port
5. WPS button
6. WLAN button
7. LAN interface
8. WAN interface
9. Phone interface

The connections between the ZXHN H298N and other devices are as follows:

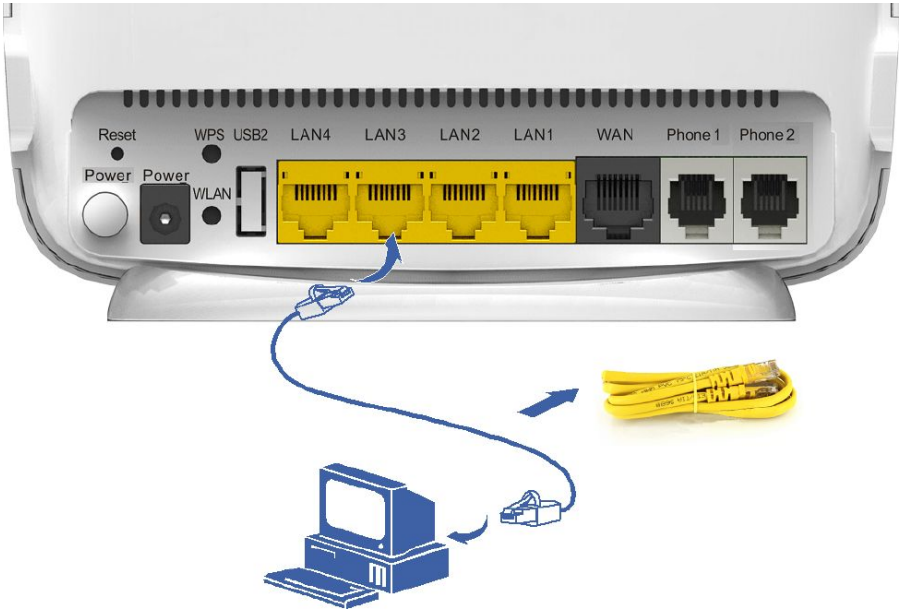
- Figure 5 shows the connection between the ZXHN H298N and the telephone.

Figure 5 Telephone Connection



- Figure 6 shows the connection between the ZXHN H298N and the computer.

Figure 6 LAN Interface Connection



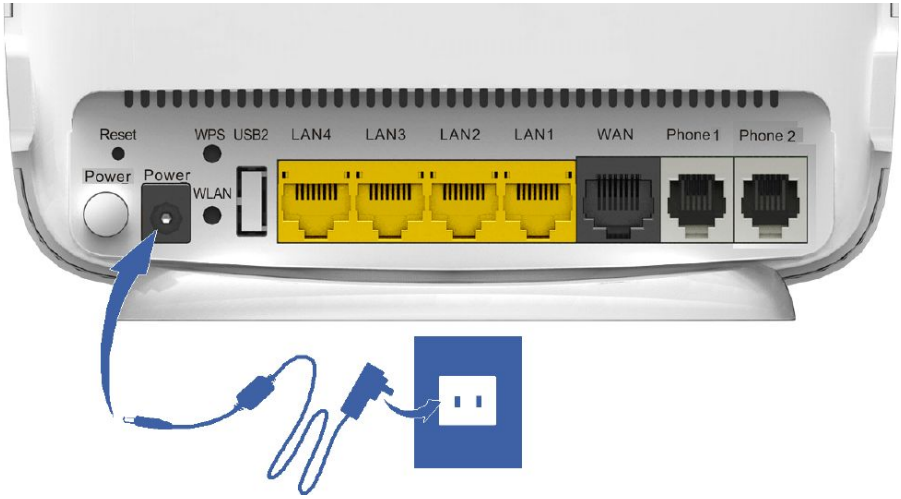
- Figure 7 shows the connection between the ZXHN H298N and the USB storage device.

Figure 7 USB Storage Device Connection



- Figure 8 shows the connection between the ZXHN H298N and the power supply.

Figure 8 Power Supply Connection



To supply power for the device, press the power button on the back of the device. When Internet indicator of the ZXHN H298N indicators is ON, you can access the Internet and use the phone.

2.2 Configuring TCP/IP

Perform this procedure to configure TCP/IP.

Context

To ensure that the device can access the Internet successfully, configure the computer address in the same network segment as the ZXHN H298N address.

The default network settings for the ZXHN H298N 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. Configure TCP/IP.
   i. In **Local Area Connection Properties**, select **Internet Protocol (TCP/IP)**.
   ii. Click **Properties** to open the **Internet Protocol (TCP/IP) Properties** dialog box.
   iii. In the **Internet Protocol (TCP/IP) Properties** dialog box, select **Use the following IP address**. Set **IP address**, **Subnet mask**, and **Default gateway**. Set the computer IP

address to be in the same network segment as the device address, that is, 192.168.1.7. The subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1.

iv. Click **OK**.

NOTE ***Note:***

The settings change with the network requirements. However, perform the steps above at the first time.

2. Check the TCP/IP settings.

   You can use the **Ping** command to check the connection between the computer and device.

   If the computer fails to ping the device, check the following items:

   - The Ethernet cable between the device and the computer is correctly connected.
   - The driver program of the network adapter on the computer is correctly installed.
   - The LAN indicator on the device and the network card indicator on the computer are ON.
   - The TCP/IP settings on the computer are correct.

TCP/IP is configured successfully.

2.3 Logging In to the Device

Perform this procedure to log in to the device.

Prerequisite

Before this operation, make sure that the device is properly connected and the computer is correctly configured.

Context

The ZXHN H298N provides the web-based configuration mode. You can configure and manage the device through the web browser. Different users have different configuration rights, as listed in Table 5.

Table 5 User Rights

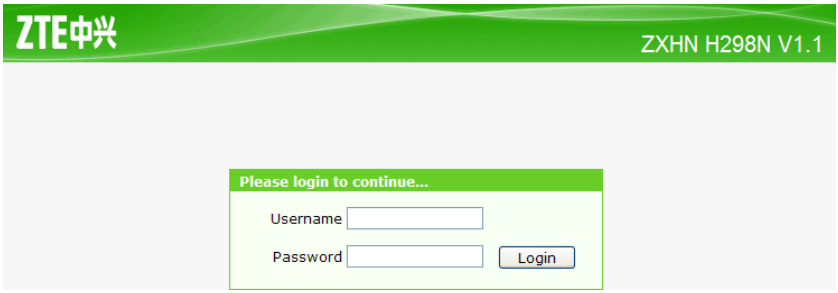
Role	User Name and Password	Right
Administrator	User name: admin Password: admin	The administrator has all the configuration rights.
Common user	User name: user Password: user	The common user has only some view rights.

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

Steps

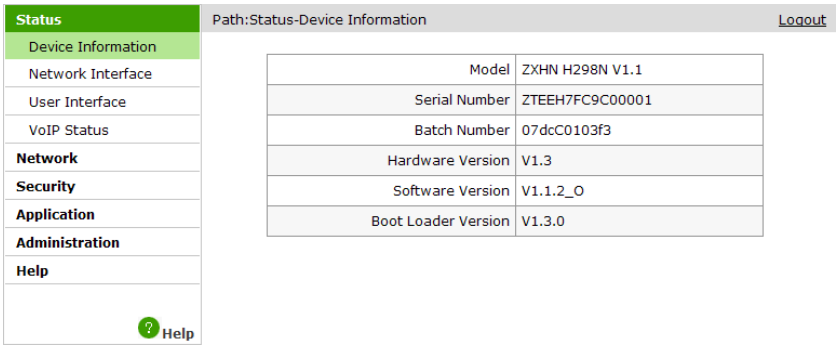
1. Open the Internet Explorer.
2. Type `http://192.168.1.1` on the address bar and press **Enter**. The login dialog box is displayed, as shown in Figure 9.

   Figure 9 Login



3. In **Username** and **Password**, type the user name and password (by default, the user name is `admin` and the password is `admin`). Click **Login** to open the homepage, as shown in Figure 10.

   Figure 10 Homepage



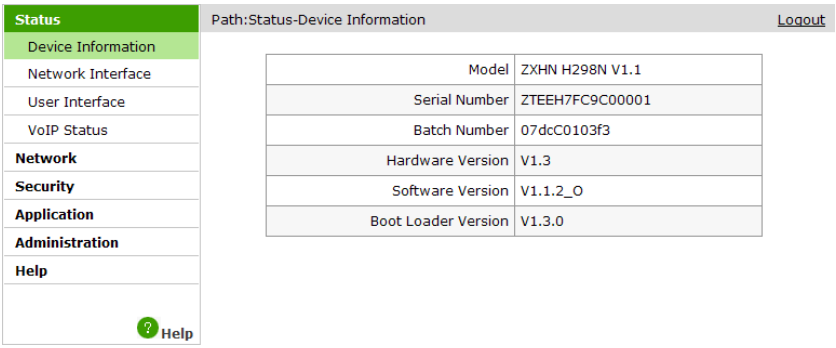
You have logged in to the device successfully.

3 Status

3.1 Device Information

Choose [**Status**→ **Device Information**]. The device information is displayed, as shown in Figure 11.

Figure 11 Device Information



Note:

The software version and boot loader version may be different from the delivery.

3.2 Network Interface

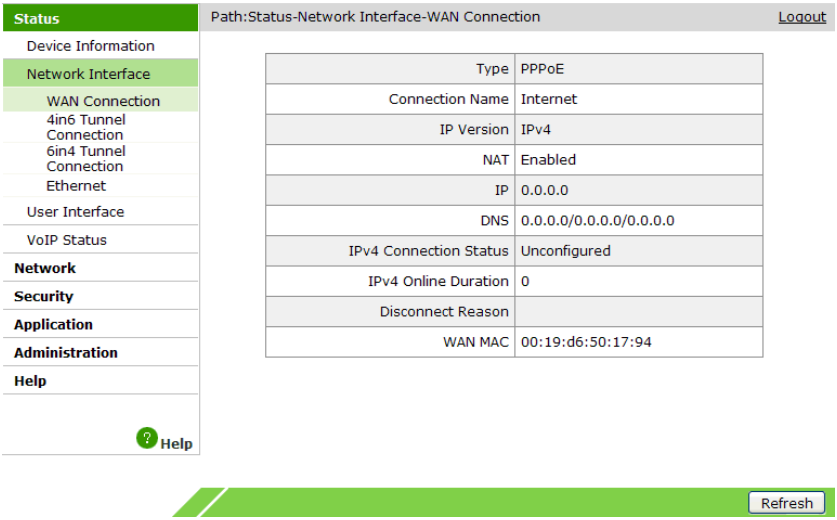
The network interface information includes the following:

- WAN Connection
- 4in6 Tunnel Connection
- 6in4 Tunnel Connection
- Ethernet

3.2.1 WAN Connection

Choose [**Status**→ **Network Interface**→ **WAN Connection**]. The WAN Connection information is displayed, as shown in Figure 12.

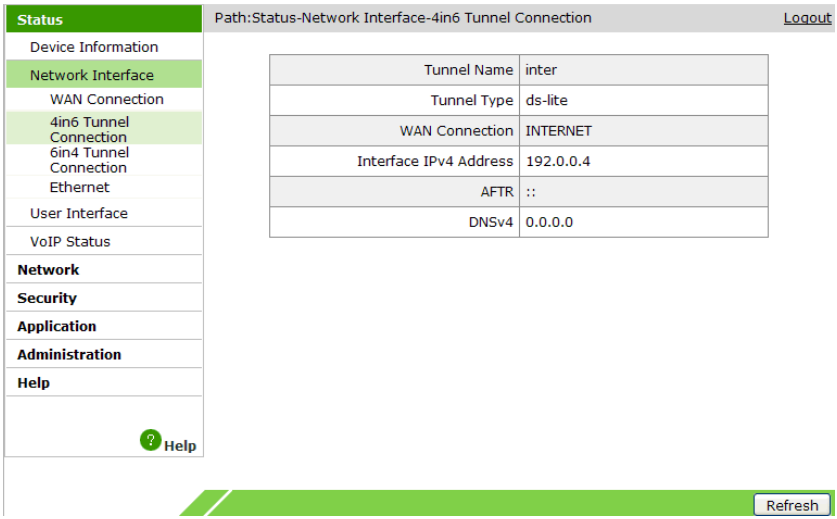
Figure 12 WAN Connection



3.2.2 4in6 Tunnel Connection

Choose [**Status→ Network Interface→ 4in6 Tunnel Connection**]. The 4in6 tunnel connection information is displayed, as shown in Figure 13.

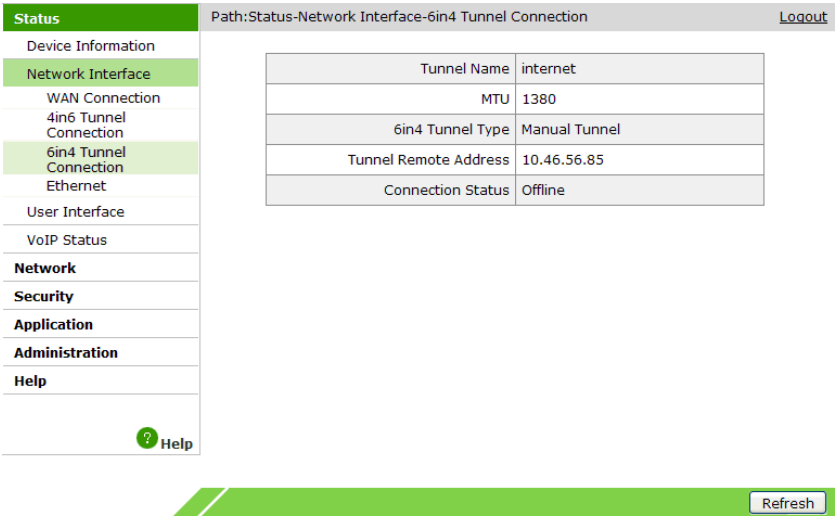
Figure 13 4in6 Tunnel Connection



3.2.3 6in4 Tunnel Connection

Choose [**Status→ Network Interface→ 6in4 Tunnel Connection**]. The 6in4 tunnel connection information is displayed, as shown in Figure 14.

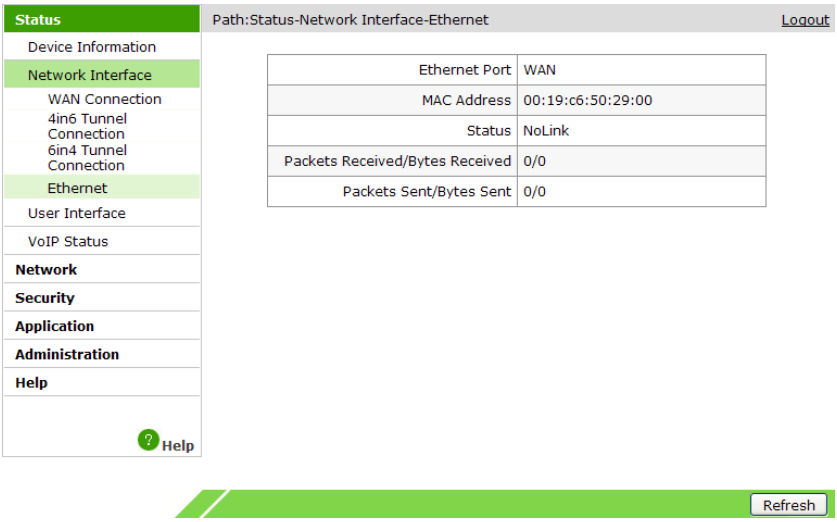
Figure 14 6in4 Tunnel Connection



3.2.4 Ethernet

Choose [**Status→ Network Interface→ Ethernet**]. The Ethernet information is displayed, as shown in Figure 15.

Figure 15 Ethernet



3.3 User Interface

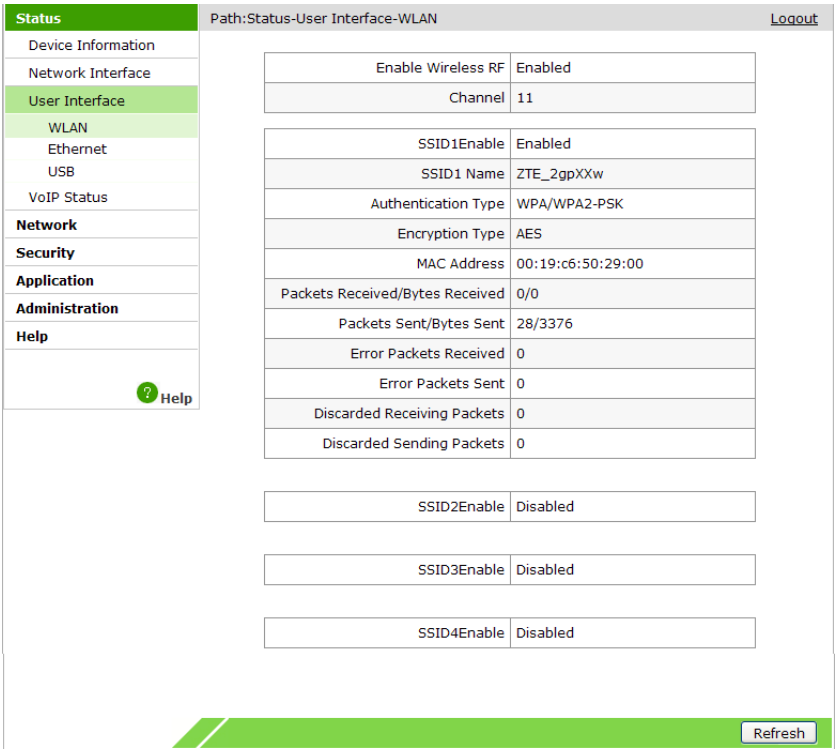
The user interface information includes the following:

- WLAN
- Ethernet
- USB

3.3.1 WLAN

Choose [**Status→ User Interface→ WLAN**]. The WLAN information is displayed, as shown in Figure 16.

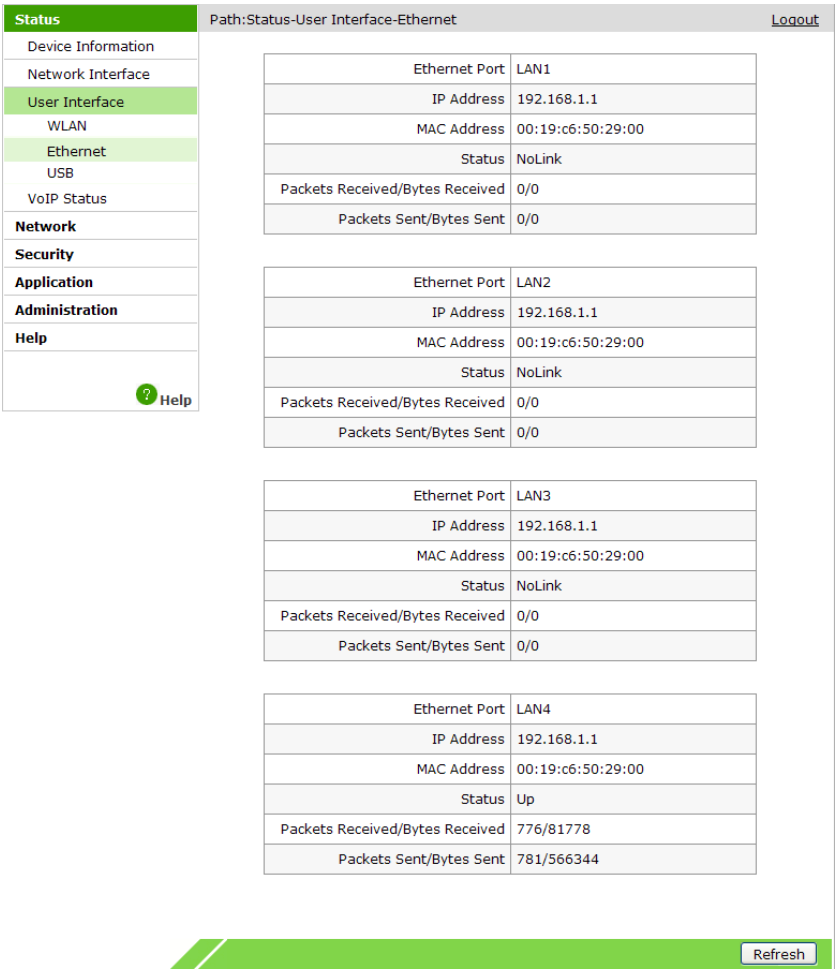
Figure 16 WLAN Status



3.3.2 Ethernet

Choose [**Status**→ **User Interface**→ **Ethernet**]. The Ethernet interface information is displayed, as shown in Figure 17.

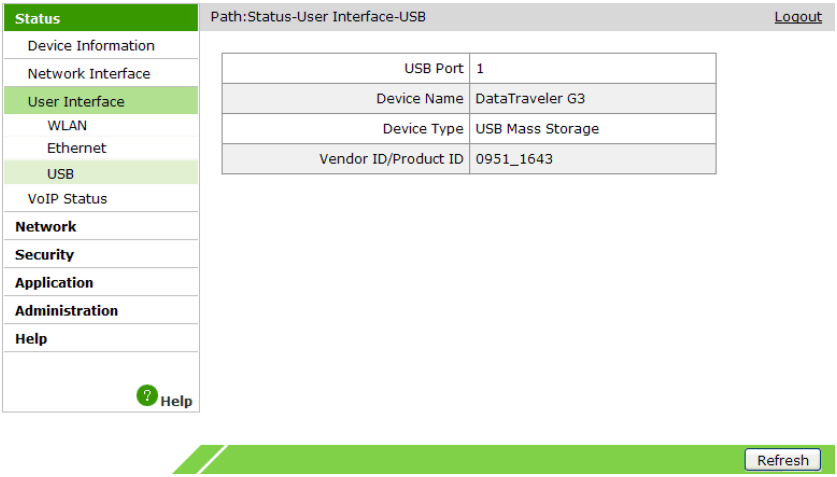
Figure 17 Ethernet Interface Status



3.3.3 USB

Choose [**Status→ User Interface→ USB**]. The USB interface information is displayed, as shown in Figure 18.

Figure 18 USB Interface Status



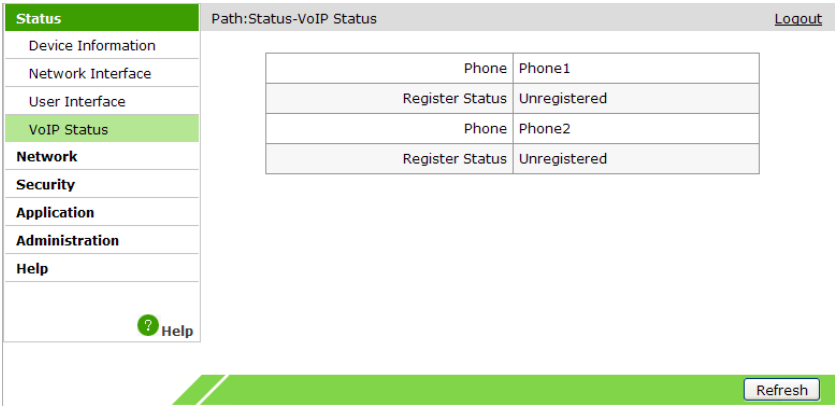
Note:

The FTP application must be configured before you access the USB device.

3.4 VoIP Status

Choose [**Status→ VoIP Status**]. The VoIP service information is displayed, as shown in Figure 19.

Figure 19 VoIP Status



4 Network

4.1 WAN

WAN configuration includes the following:

- WAN Connection
- 4in6 Tunnel Connection
- 6in4 Tunnel Connection
- Port Binding

4.1.1 WAN Connection

Perform this procedure to configure WAN connection.

Steps

1. Choose [**Network→ WAN→ WAN Connection**].
2. Select **Create WAN Connection** from the **Connection Name** drop-down list, and configure other parameters, as shown in Figure 20 .

Figure 20 WAN Connection

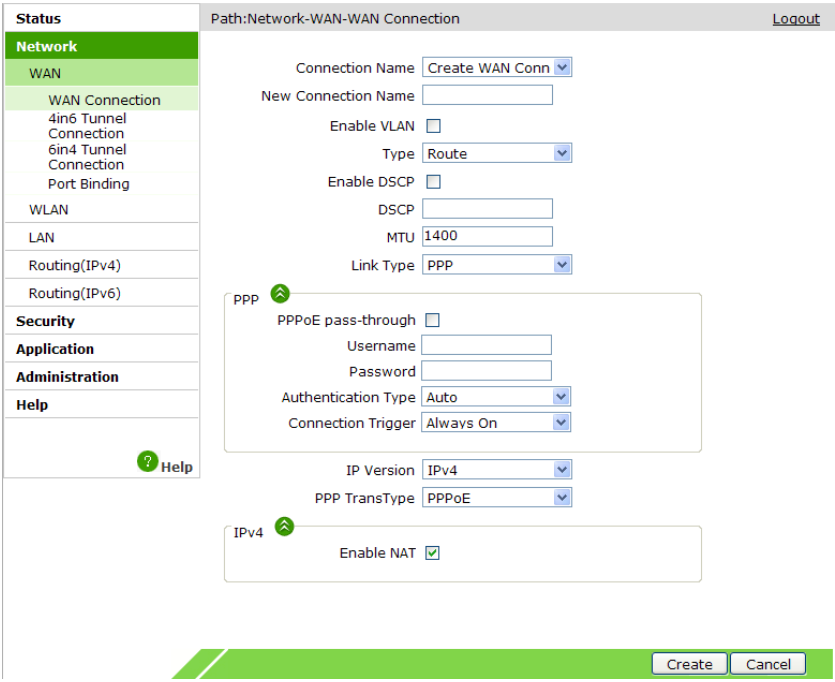


Table 6 describes the parameters for creating a new WAN connection.

Table 6 Parameters for Creating a New WAN Connection

Parameter	Description
Connection Name	The default is **Create WAN Connection**. The connection name is generated automatically.
New Connection Name	Name the connection.
Enable VLAN	Enable the VLAN function.
Type	Connection type
Enable DSCP	This function is used together with the QoS function. Enable it as required.
DSCP	The value ranges from 0 to 63.
MTU	Define the maximum transfer unit.
Link type	There are two link types: ▸ PPP ▸ IP

Parameter	Description
PPPoE pass-through	Enable the PPPoE pass-t;hrough function.
Username/Password	PPPoE username and password They are provided by the ISP.
Authentication Type	The type includes Auto, PAP, and CHAP. By default, it is Auto.
Connection Trigger	There are three connection trigger modes: ▸ Always On: When the device is started or gets offline, the system triggers PPPoE dialing automatically. ▸ On Demand: The system triggers PPPoE dialing on demand. ▸ Manual: The system triggers PPPoE dialing manually.
IP version	The IP version includes: ▸ IPv4 ▸ IPv6 ▸ IPv4/v6
PPP TransType	PPPoE
Enable NAT	When multiple computers in a LAN share one IP address to access the Internet. NAT is used to translate the private network address to the public network address of the WAN port.

3. Click **Create**.

4.1.2 4in6 Tunnel Connection

Perform this procedure to configure 4in6 tunnel connection.

Steps

1. Choose [**Network→ WAN→ 4in6 Tunnel Connection**].
2. Select **Create Tunnel** from the **Tunnel Name** drop-down list, and configure other parameters, as shown in Figure 21.

Figure 21 4in6 Tunnel Connection

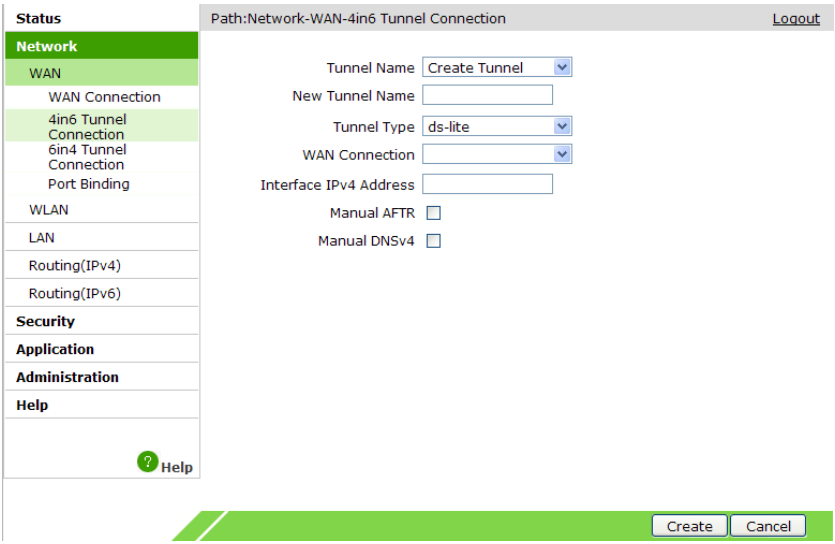


Table 7 describes the parameters for creating a new 4in6 tunnel connection.

Table 7 Parameters for Creating a New 4in6 Tunnel Connection

Parameter	Description
Tunnel Name	Tunnel name. The new DS-Lite tunnel (Create Tunnel) or the created DS-Lite tunnel is optional.
New Tunnel Name	When **Create Tunnel** is selected for **Tunnel Name**, enter the tunnel name in the **New Tunnel Name** text box.
Tunnel Type	At present, only DS-Lite is supported.
WAN Connection	WAN connection related to DS-Lite tunnel, which must be IPv6 WAN connection.
Interface IPv4 Address	IPv4 address of DS-Lite tunnel interface, which is reserved for the local device. The range of Interface IPv4 address is between 192.0.0.2 and 192.0.0.6.
Manual AFTR	When **Manual AFTR** is selected, the seventh parameter appears, indicating that the tunnel is a manual tunnel. If **Manual AFTR** is not selected, the seventh parameter does not appear, indicating that the tunnel is an automatic tunnel.
Manual DNSV4	When **Manual DNSV4** is selected, the ninth parameter appears, indicating that this parameter is entered manually. If **Manual DNSV4** is not selected, the ninth parameter does not appear, indicating that this parameter is obtained automatically.

3. Click **Create**.

4.1.3 6in4 Tunnel Connection

Perform this procedure to configure 6in4 tunnel connection.

Steps

1. Choose [**Network→ WAN→ 6in4 Tunnel Connection**].
2. Select **Create Tunnel** from the **Tunnel Name** drop-down list, and configure other parameters, as shown in Figure 22.

Figure 22 6in4 Tunnel Connection

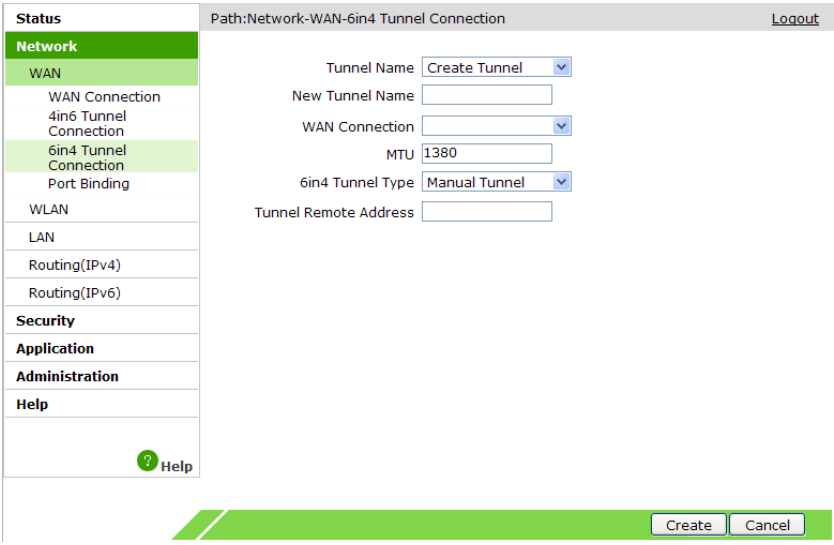


Table 8 describes the parameters for creating a new 6in4 tunnel connection.

Table 8 Parameters for Creating a New 6in4 Tunnel Connection

Parameter	Description
Tunnel Name	Tunnel name. The new tunnel (Create Tunnel) or the created tunnel is optional.
New Tunnel Name	When **Create Tunnel** is selected for **Tunnel Name**, enter the tunnel name in the **New Tunnel Name** text box.
WAN Connection	WAN connection related to the tunnel, which must be underlying WAN connection.
MTU	Define the maximum transfer unit.

Parameter	Description
6in4 Tunnel Type	There are two 6in4 tunnel types: ▸ Manual Tunnel ▸ 6rd
Tunnel Remote Address	When **Manual Tunnel** is selected for **6in4 Tunnel Type**, enter the parameter in the **Tunnel Remote Address** text box.

3. Click **Create**.

4.1.4 Port Binding

Perform this procedure to configure port binding.

Context

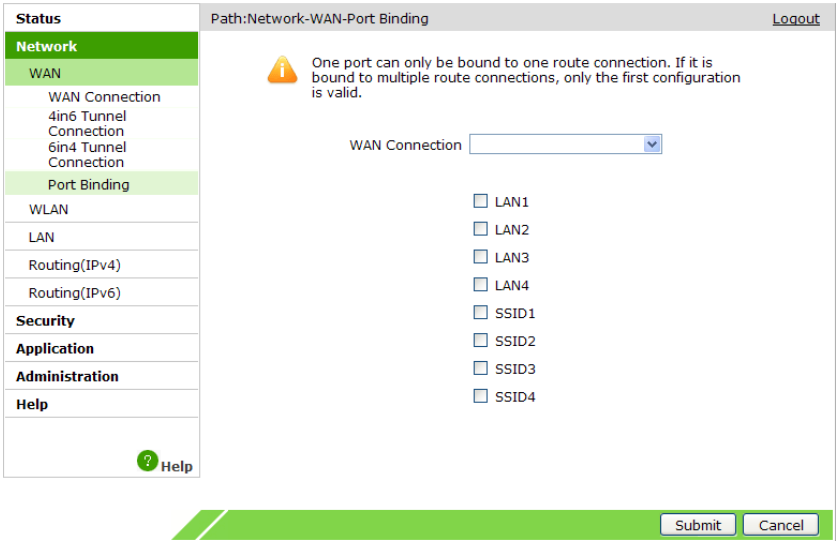
Port binding is to bind the LAN-side port with the WAN-side port.

To set port binding, perform the following steps:

Steps

1. Choose [**Network→ WAN→ Port Binding**].
2. Select a WAN connection type from the **WAN Connection** drop-down list, and select the LAN port that you need to bind, as shown in Figure 23.

Figure 23 Port Binding



3. Click **Submit**.

Port binding is configured.

4.2 WLAN

WLAN configuration includes the following:

- Basic 11n Configuration
- SSID Settings
- Security
- Access Control List
- Associated Devices
- WiFi Restrictions

4.2.1 Basic WLAN Configuration

Perform this procedure to configure the basic 11n parameters.

The WLAN basic configuration includes the following modes:

- IEEE 802.11b Only
- IEEE 802.11g Only
- IEEE 802.11n Only
- Mixed(802.11g+802.11n)
- Mixed(802.11b+802.11g)
- Mixed(802.11b+802.11g+802.11n)

IEEE 802.11b Only Configuration

To configure IEEE 802.11b Only, perform the following steps:

1. Choose [**Network**→ **WLAN**→ **Basic**].
2. Select **Enabled**, **Disabled** or **Scheduled** from the **Wireless RF Mode** drop-down list. Select **IEEE 802.11b Only** from the **Mode** drop-down list, as shown in Figure 24.

Figure 24 IEEE 802.11b Only Configuration

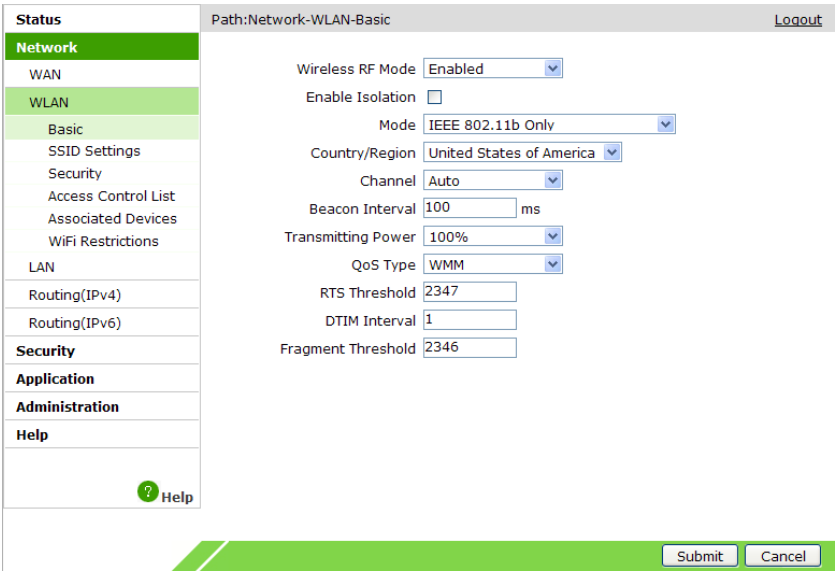


Table 9 lists the IEEE 802.11b Only parameters.

Table 9 IEEE 802.11b Only Parameters

Parameter	Description
Wireless RF Mode	Select **Enabled** to enable the wireless RF function.
Enable Isolation	When you select this check box, the subscribers with different SSIDs cannot visit each other.
Mode	Select the working mode according to the wireless network card configuration.
Country/Region	Select the country or region.
Channel	The default is Auto.
Beacon Interval	Time interval for the wireless device to broadcast the SSID Keep the default value.
Transmitting Power	Select the transmitting power as required.
QoS Type	Type of QoS
RTS Threshold	Specify the Request to Send threshold for a packet. When a packet exceeds this value, the device sends the RTS value to the destination point for negotiation. The default is 2347.

Parameter	Description
DTIM Interval	The value range is from 1 ms to 5 ms. The default is 1 ms.
Fragment Threshold	When a packet exceeds the fragment threshold, it is divided into multiple packets. Excessive packet fragments may affect the network performance, so the fragment threshold should not be set too big. It is recommended to set the threshold to an even value. An odd value is reduced by one to be an even value. The default is 2346.

3. Click **Submit**.

IEEE 802.11n Only Configuration

To configure IEEE 802.11n Only, perform the following steps:

1. Choose [**Network→ WLAN→ Basic**].
2. Select **Enabled**, **Disabled** or **Scheduled** from the **Wireless RF Mode** drop-down list. Select **IEEE 802.11n Only** from the **Mode** drop-down list, as shown in Figure 25.

Figure 25 IEEE 802.11n Only Configuration

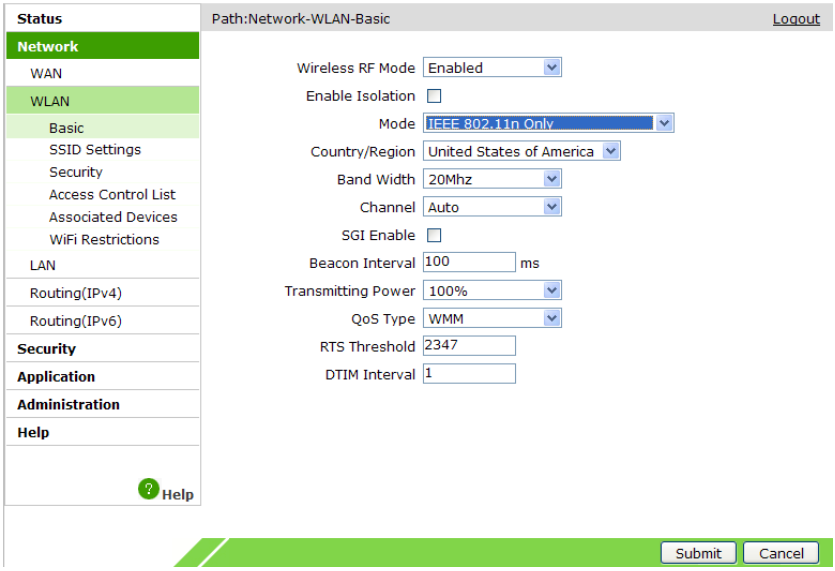


Table 10 lists the IEEE 802.11n Only parameters.

Table 10 IEEE 802.11n Only Parameters

Parameter	Description
Wireless RF Mode	Select **Enabled** to enable the wireless RF function.
Enable Isolation	When you select this check box, the subscribers with different SSIDs cannot visit each other.
Mode	Select the working mode according to the wireless network card configuration.
Country/Region	Select the country or region.
Band Width	You can select 20Mhz or 40Mhz.
Channel	The default is Auto.
SGI Enable	Select this check box to enable the short GI function.
Beacon Interval	Time interval for the wireless device to broadcast the SSID Keep the default value.
Transmitting Power	Select the transmitting power as required.
QoS Type	Type of QoS
RTS Threshold	Specify the Request to Send threshold for a packet. When a packet exceeds this value, the device sends the RTS value to the destination point for negotiation. The default is 2347.
DTIM Interval	The value range is from 1 ms to 5 ms. The default is 1 ms.

3. Click **Submit**.

4.2.2 SSID Settings

Perform this procedure to configure multiple SSIDs.

The ZXHN H298N can be specified with four SSIDs and each SSID supports up to 32 subscribers.

Steps

1. Choose [**Network→ WLAN→ SSID Settings**].
2. Select an SSID from the **Choose SSID** drop-down list, as shown in Figure 26.

Figure 26 SSID Settings

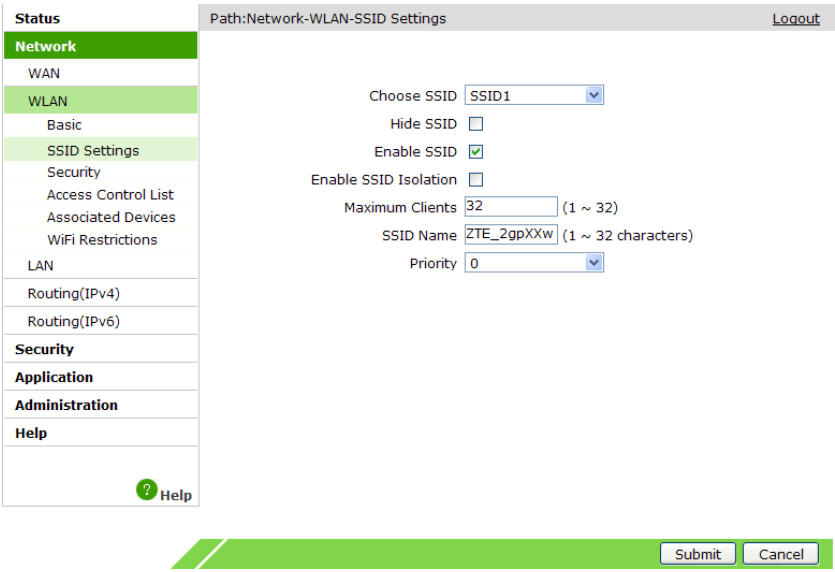


Table 11 lists the SSID setting parameters.

Table 11 Multi-SSID Parameters

Parameter	Description
Choose SSID	Select the SSID to be configured.
Hide SSID	You can hide the SSID to prevent illegal users.
Enable SSID	Enable the SSID broadcast.
Enable SSID Isolation	When you select this check box, the subscribers with different SSIDs cannot visit each other.
Maximum Clients	The value range is from 1 to 32.
SSID Name	Specify the SSID name.
Priority	SSID priority, ranging from 0 to 7

3. Click **Submit**.

SSIDs are configured.

4.2.3 Security

Perform this procedure to configure WLAN security.

Context

The ZXHN H298N provides the following access authentication modes:

- Open System

  Authentication is not needed. Any host with a wireless network card can be connected to the wireless access point. This mode provides WEP encryption.

- Shared Key

  This mode provides WEP encryption.

- WPA-PSK

  WPA-PSK is a version of WPA. It uses the pre-shared key. WPA-PSK is similar with WEP but is securer than WEP. The data is encrypted before transmission.

- WPA2-PSK

  It is the second version of WPA-PSK.

- WPA/WPA2-PSK

  It is a hybrid authentication mode.

Open System

To configure the Open System authentication mode, perform the following steps:

1. Choose [**Network**→ **WLAN**→ **Security**].

2. Select **Open System** from the **Authentication Type** drop-down list, as shown in Figure 27.

Figure 27 Open System

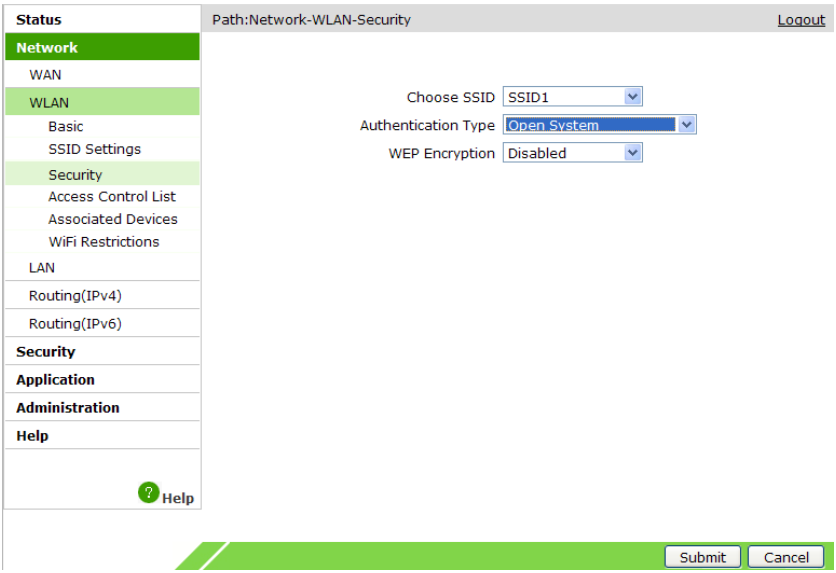


Table 12 lists the parameters for the Open System authentication mode.

Table 12 Parameters for the Open System Authentication Mode

Parameter	Description
Choose SSID	Select a SSID as required.
Authentication Type	Select **Open System**.
WEP Encryption	Select **Disabled** or **Enabled**.

3. Click **Submit**.

Shared Key

To configure the Shared Key authentication mode, perform the following steps:

1. Choose [**Network→ WLAN→ Security**].

2. Select **Shared Key** from the **Authentication Type** drop-down list, as shown in Figure 28.

Figure 28 Shared Key

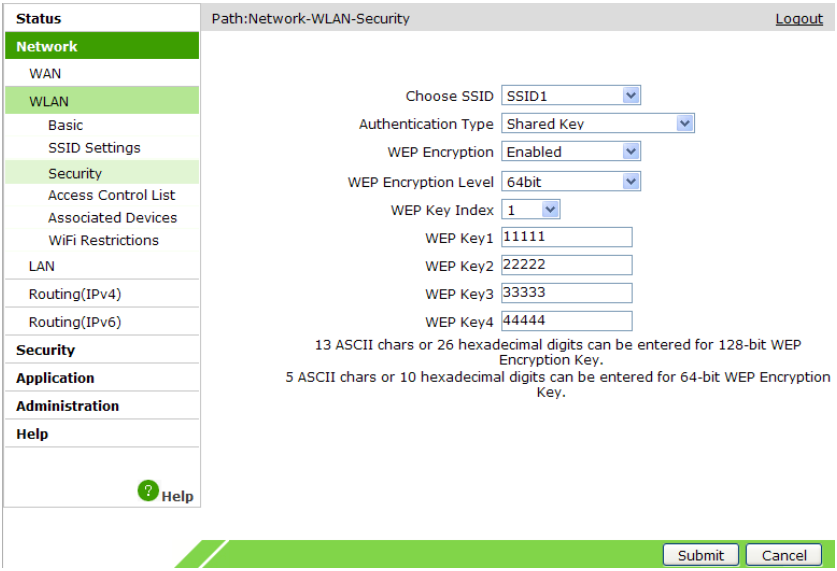


Table 13 lists the parameters for the Shared Key authentication mode.

Table 13 Parameters for the Shared Key Authentication Mode

Parameter	Description
Choose SSID	Select a SSID as required.
Authentication Type	Select **Shared Key**.
WEP Encryption	It is enabled by default.
WEP Encryption Level	The value can be 64bit or 128bit.
WEP Key Index	WEP provides four keys and they can be configured in **WEP Key1** to **WEP Key4**.

3. Click **Submit**.

WPA-PSK

To configure the WPA-PSK authentication mode, perform the following steps:

1. Choose [**Network→ WLAN→ Security**].

2. Select **WPA-PSK** from the **Authentication Type** drop-down list, as shown in Figure 29.

Figure 29 WPA-PSK

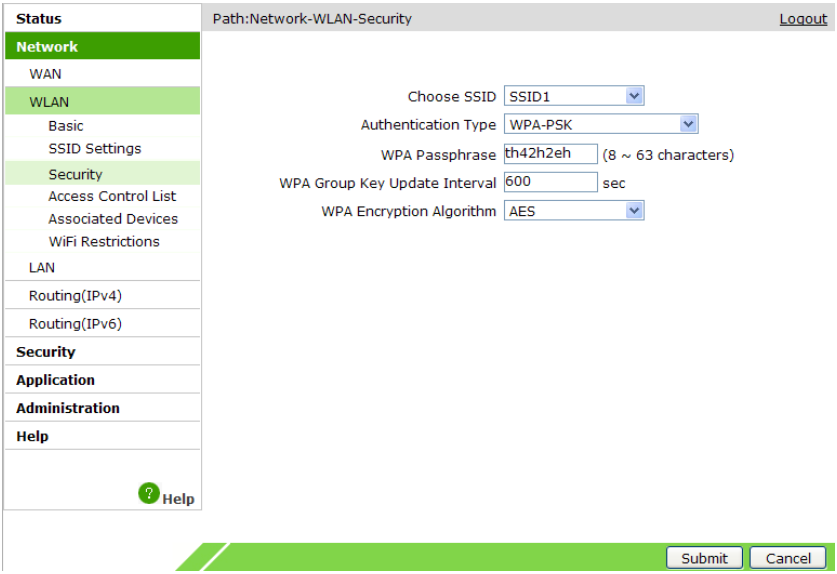


Table 14 lists the parameters for the WPA-PSK authentication mode.

Table 14 Parameters for the WPA-PSK Authentication Mode

Parameter	Description
Choose SSID	Select a SSID as required.
Authentication Type	Select **WPA-PSK**.
WPA Passphrase	Range: 8–63 characters
WPA Group Key Update Interval	Default: 600 seconds
WPA Encryption Algorithm	TKIP: Temporal Key Integrity Protocol AES: Advanced Encryption Standard TKIP+AES: Adaptive encryption algorithm

3. Click **Submit**.

WPA2-PSK and WPA/WPA2-PSK

The configuration methods for WPA2-PSK and WPA/WPA2-PSK are the same as that for WPA-PSK.

4.2.4 Access Control List

Context

By default, the ACL function for the ZXHN H298N is disabled.

To configure the ACL, perform the following steps:

Steps

1. Choose [**Network→ WLAN→ Access Control List**].
2. Select a SSID from the **Choose SSID** drop-down list. Select **Disabled**, **Block**, or **Permit**, as shown in Figure 30.

   Figure 30 Access Control List – I

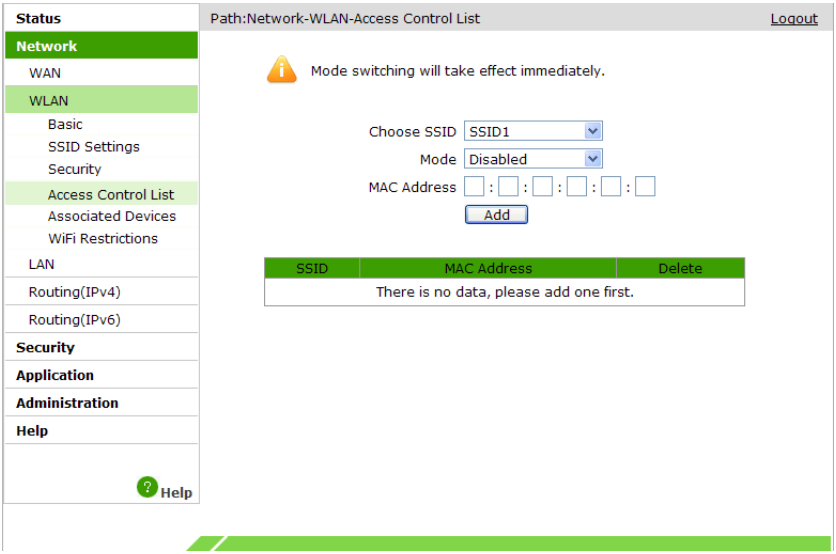


   Table 15 lists the ACL parameters.

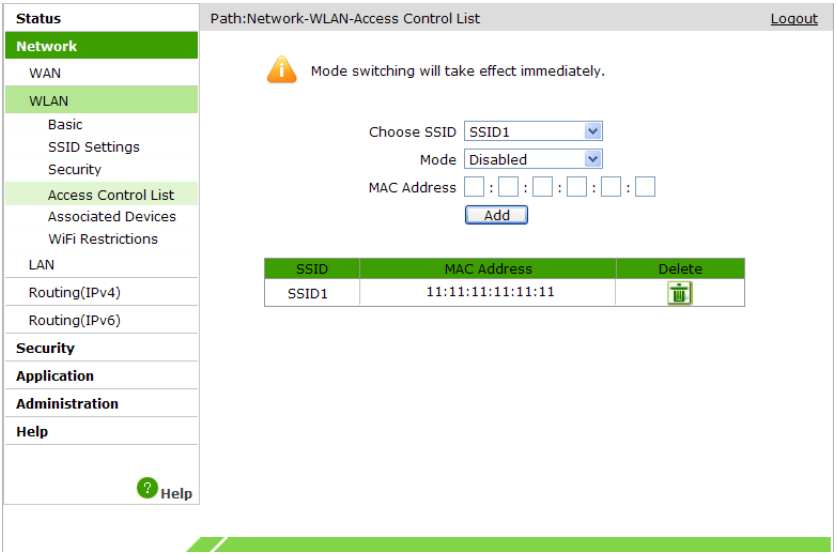
   Table 15 ACL Parameters

Parameter	Description
Disabled	Disable the ACL function.
Block	Permit all the MAC addresses except the typed MAC address.
Permit	Block all the MAC addresses except the typed MAC address.

3. In **MAC Address**, type the MAC address that you want to permit or block.
4. Click **Add**.

The MAC address that you want to permit or block is displayed on the page, as shown in Figure 31.

Figure 31 Access Control List – II



ACL is configured.

4.2.5 Associated Devices

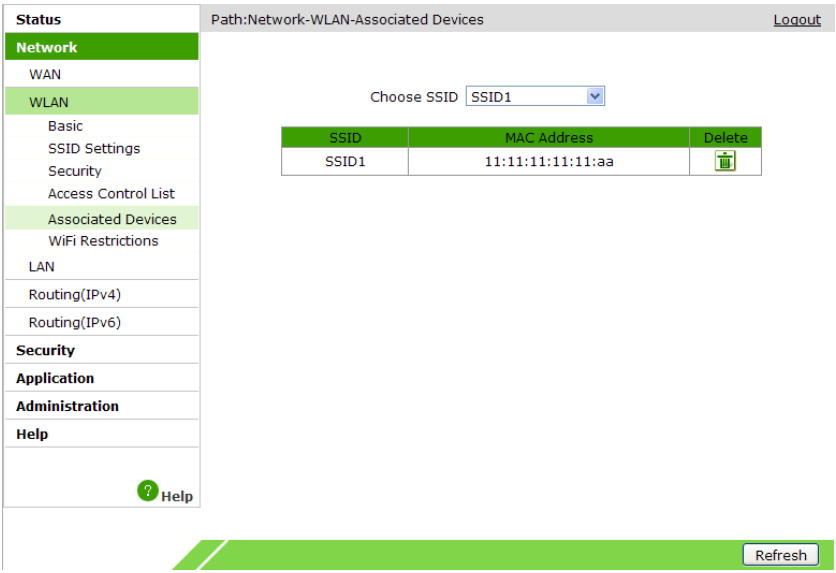
Context

To view the MAC address of the STA that is associated with an SSID, perform the following steps:

Steps

1. Choose [**Network→ WLAN→ Associated Devices**].
2. Select an SSID from the **Choose SSID** drop-down list. Then. The MAC address of the STA that is associated with the SSID is displayed, as shown in Figure 32.

Figure 32 Associated Devices



The associated devices are configured.

4.2.6 WiFi Restrictions

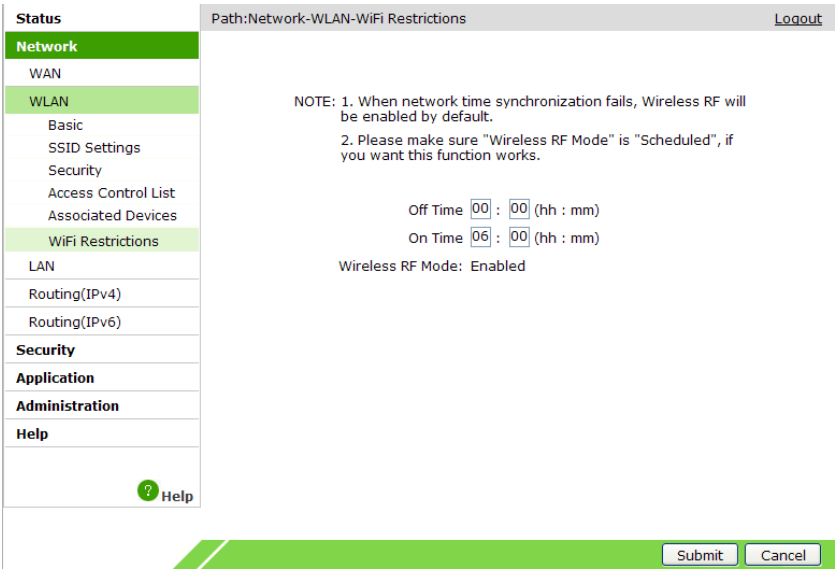
Context

To configure the WiFi restrictions, perform the following steps:

Steps

1. Choose [**Network→ WLAN→ WiFi Restrictions**], as shown in Figure 33.

Figure 33 WiFi Restrictions



2. Configure the WiFi off-time and on-time.
3. Click **Submit**.

The WiFi restrictions are configured.

4.3 LAN

LAN configuration includes the following:

- DHCP Server
- DHCP Server(IPv6)
- DHCP Binding
- DHCP Port Service
- Static Prefix
- Prefix Delegation
- DHCP Port Service(IPv6)
- RA Service

4.3.1 DHCP Server

Context

To configure the DHCP server, perform the following steps:

Steps

1. Choose [**Network→ LAN→ DHCP Server**].
2. Set the DHCP server parameters, as shown in Figure 34.

Figure 34 DHCP Server

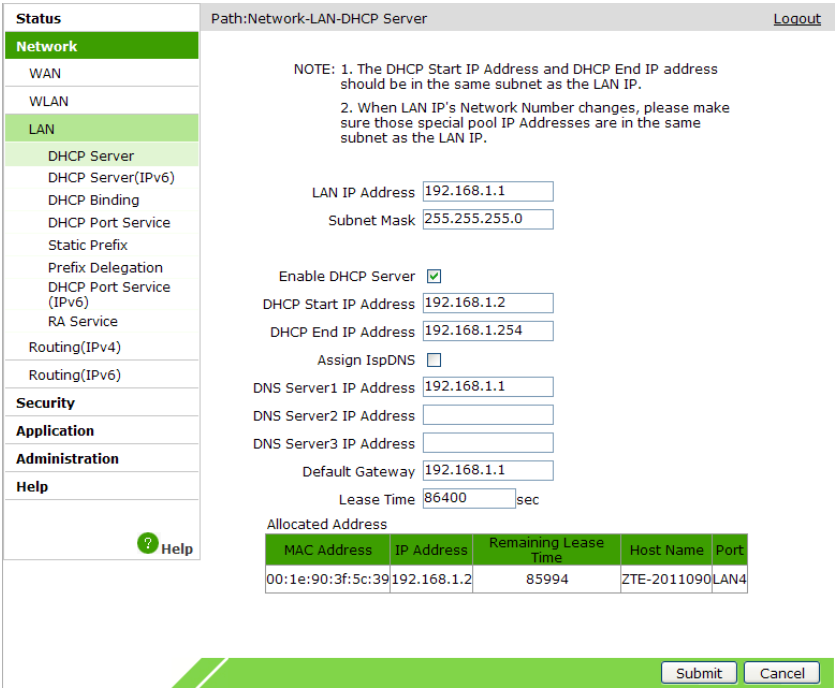


Table 16 lists the DHCP server parameters.

Table 16 DHCP Server Parameters

Parameter	Description
LAN IP Address/Subnet Mask	IP address and subnet mask of the device in the LAN The device IP address should be in the same network segment as the DHCP address pool.
Enable DHCP Server	Enable the DHCP server.

Parameter	Description
DHCP Start IP Address/DHCP End IP Address	DHCP address pool
Assign IspDNS	Assign the ISP DNS server.
DNS Server1 IP Address–DNS Server3 IP Address	IP addresses of the DNS server, provided by the ISP
Default Gateway	It is usually the LAN-side IP address of the device.
Lease Time	Lease time of the DHCP IP address. The default is 86400 seconds.

3. Click **Submit**.

The DHCP server is configured.

4.3.2 DHCP Server(IPv6)

Context

To configure the IPv6 DHCP server, perform the following steps:

Steps

1. Choose [**Network→ LAN→ DHCP Server(IPv6)**].
2. Set the DHCP server parameters, as shown in Figure 35.

Figure 35 IPv6 DHCP Server

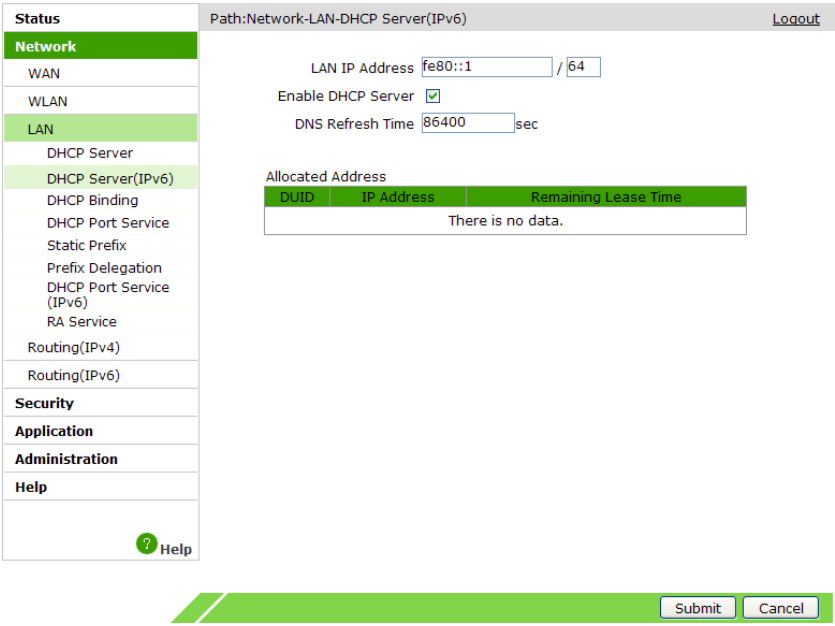


Table 17 lists the IPv6 DHCP server parameters.

Table 17 IPv6 DHCP Server Parameters

Parameter	Description
LAN IP Address	IPv6 address of the device in the LAN Default prefix length: 64 bits
Enable DHCP Server	Enable the DHCP server.
DNS Refresh Time	The time to refresh the DNS address on the LAN side to keep the address valid

3. Click **Submit**.

The IPv6 DHCP server is configured.

4.3.3 DHCP Binding

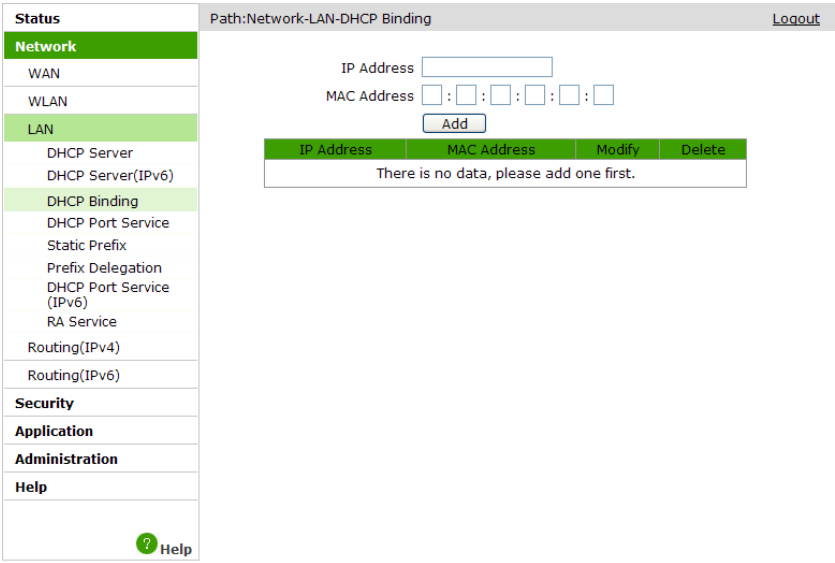
Context

To configure DHCP binding, perform the following steps:

Steps

1. Choose [**Network→ LAN→ DHCP Binding**].
2. Set the IP address and MAC address. The IP address is bound with the MAC address.
3. Click **Add**. The binding relationship is displayed, as shown in Figure 36.

Figure 36 DHCP Binding



DHCP binding is configured.

Postrequisite

You can also modify or delete the DHCP binding relationship, as listed in Table 18.

Table 18 DHCP Binding Operations

Button	Description
	To modify the binding relationship
	To delete the binding relationship

4.3.4 DHCP Port Service

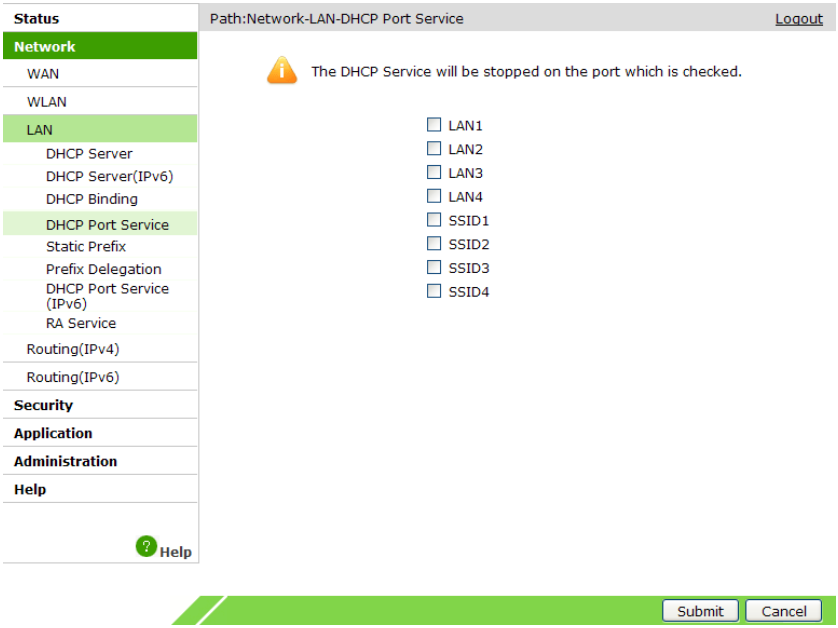
Prerequisite

Before this operation, make sure that the global DHCP service is enabled.

Steps

1. Choose [**Network→ LAN→ DHCP Port Service**], as shown in Figure 37.

   Figure 37 DHCP Port Service



2. Select the LAN interface for which you want to disable the DHCP function.
3. Click **Submit**.

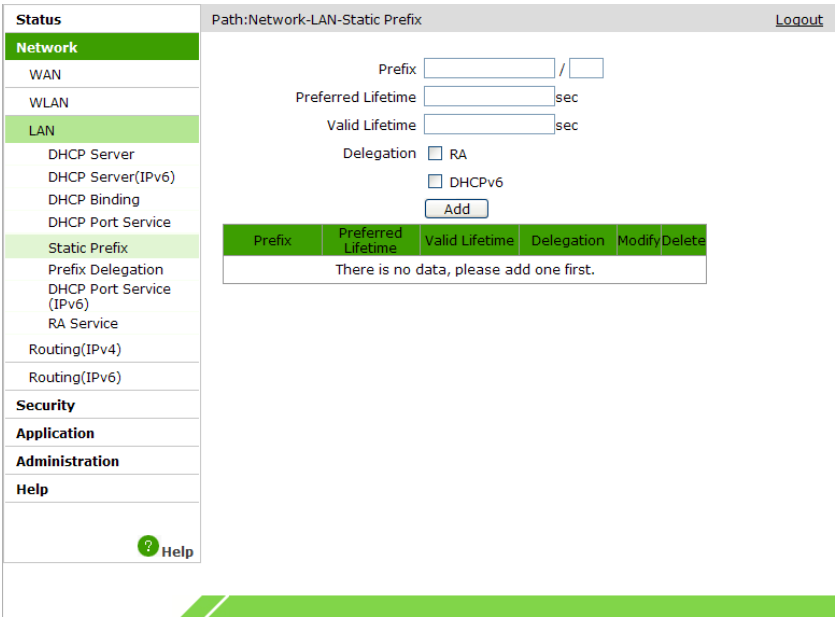
The DHCP port service is configured.

4.3.5 Static Prefix

Steps

1. Choose [**Network→ LAN→ Static Prefix**], as shown in Figure 38.

Figure 38 Static Prefix



2. Configure the parameters.

   Table 19 describes the parameters for static prefix.

Table 19 Static Prefix Parameters

Parameter	Description
Prefix	IPv6 address
Preferred Lifetime	Preferred life time of the prefix The length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated Preferred life time ≤ Valid life time Unit: second
Valid Lifetime	The length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.
Delegation	Prefix delegation mode: ▸ RA ▸ DHCPv6

3. Click **Add**.

The IPv6 static prefix is configured.

4.3.6 Prefix Delegation

Context

To configure the IPv6 prefix delegation mode, perform the following steps:

Steps

1. Choose [**Network→ LAN→Prefix Delegation**].
2. Click  to configure the parameters, as shown in Figure 39.

Figure 39 Prefix Delegation

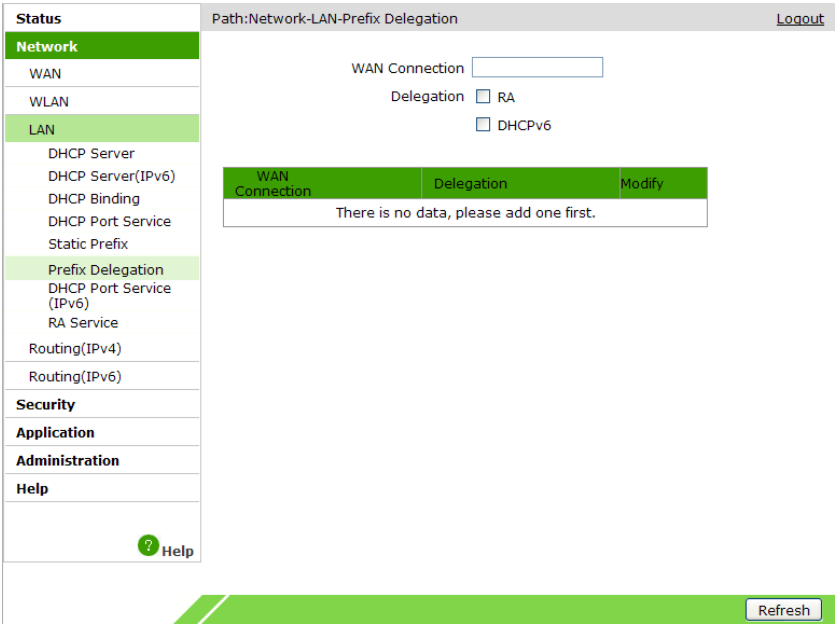


Table 20 describes the parameters for prefix delegation.

Table 20 Prefix Delegation Parameters

Parameter	Description
WAN Connection	WAN connection related to the tunnel.
Delegation	Prefix delegation mode: ▸ RA ▸ DHCPv6

3. Click **Modify**.

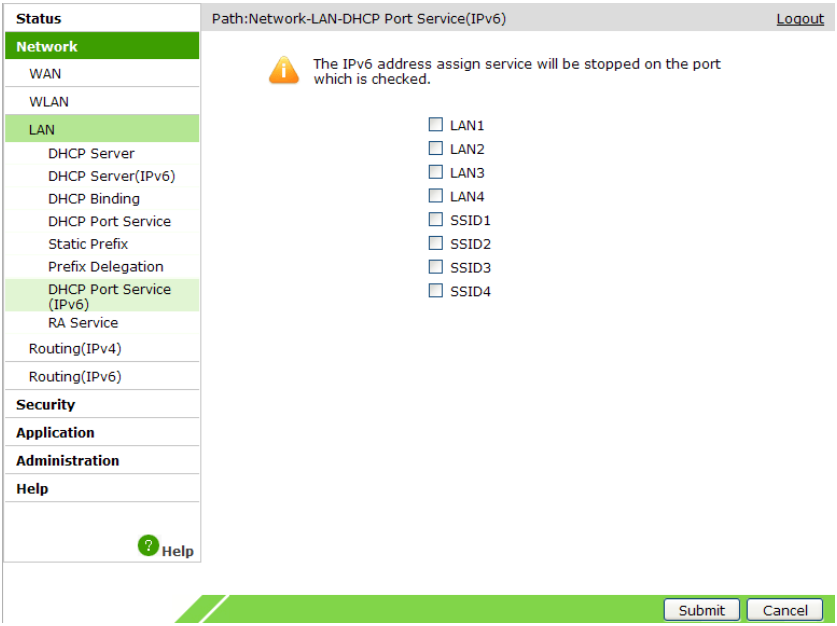
The prefix delegation mode for a specified WAN connection is configured.

4.3.7 DHCP Port Service(IPv6)

Steps

1. Choose [**Network→ LAN→ DHCP Port Service(IPv6)**].
2. Select the LAN ports on which you want to stop the IPv6 address assign service, as shown in Figure 40.

Figure 40 DHCP Port Service(IPv6)



3. Click **Submit**.

The IPv6 port service is configured.

4.3.8 RA Service

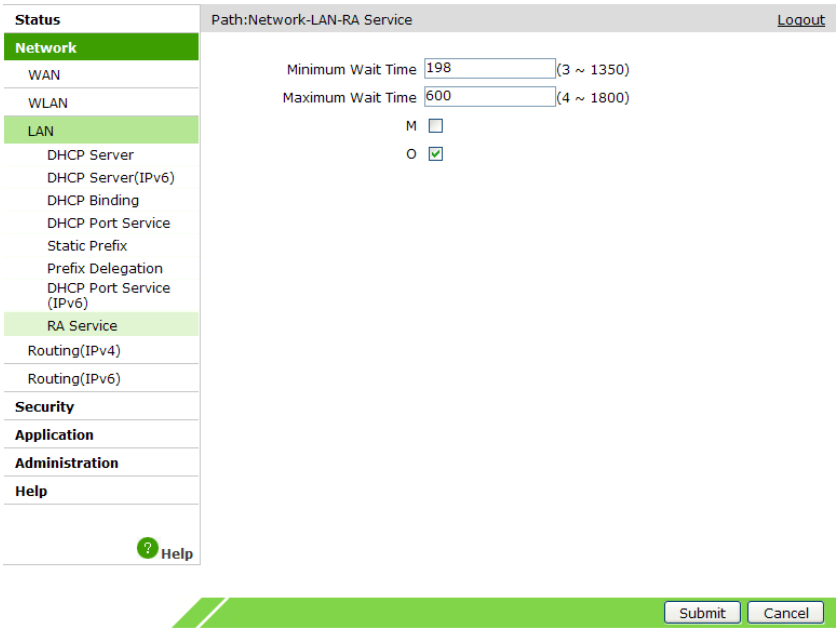
Context

To configure the wait time in active RA delegation mode, perform the following steps:

Steps

1. Choose [**Network→ LAN→ RA Service**], as shown in Figure 41.

   Figure 41 RA Service



2. Configure the parameters.

   Table 21 describes the parameters for the RA service.

   Table 21 Parameters for the RA Service

Parameter	Description
Minimum wait time	Minimum delegation interval
Maximum wait time	Maximum delegation interval

Parameter	Description
M	Managed flag The flag indicates whether or not addresses are to be configured using the stateful autoconfiguration mechanism.
O	OtherConfigFlag The flag indicates whether or not information other than addresses is to be obtained using the stateful autoconfiguration mechanism.

3. Click **Submit**.

The RA service is configured.

4.4 Routing(IPv4)

Routing configuration includes the following:

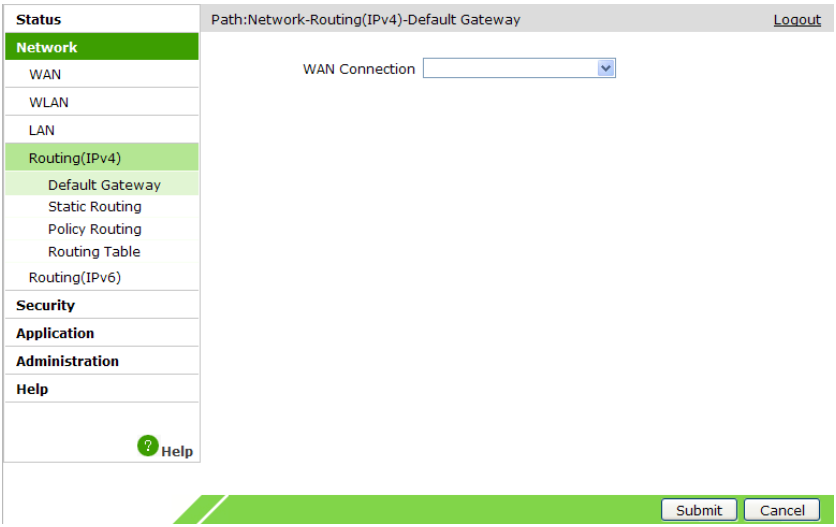
- Default Gateway
- Static Routing
- Policy Routing
- Routing Table

4.4.1 Default Gateway

Steps

1. Choose [**Network→ Routing(IPv4)→ Default Gateway**], as shown in Figure 42.

Figure 42 Default Gateway



2. From the **WAN Connection** drop-down list, select a WAN connection.

   Note:

   *The **WAN Connection** drop-down list is displayed by selecting [**Network→ WAN→ WAN Connection**].*

3. Click **Submit**.

4.4.2 Static Routing

Prerequisite

Before this operation, make sure that the WAN connection settings are complete.

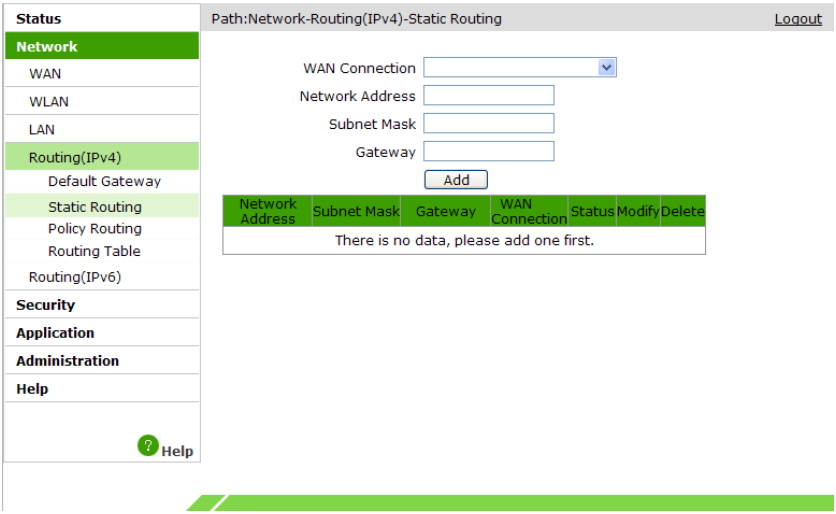
Context

To configure static routing, perform the following steps:

Steps

1. Choose [**Network→ Routing(IPv4)→ Static Routing**], as shown in Figure 43.

Figure 43 Static Routing



2. Configure the parameters.

   Table 22 describes the parameters for the static routing.

   Table 22 Parameters for the Static Routing

Parameter	Description
WAN Connection	WAN connection for static routing
Network Address	Destination network address
Subnet Mask	Subnet mask
Gateway	Gateway of the network segment which the network interface belongs to

3. Click **Add**.

Static routing is configured.

4.4.3 Policy Routing

Prerequisite

Before this operation, make sure that the WAN connection settings are complete.

Context

Policy routing is a routing rule. When it is configured, the packets are forwarded according to the routing policy. The ZXHN H298N supports packet forwarding according to the DSCP, source or destination IP address, protocol, source port number, or source MAC address.

To configure policy routing, perform the following steps:

Steps

1. Choose [**Network→ Routing(IPv4)→ Policy Routing**].
2. Select an interface from the **Destination Interface** drop-down list, as shown in Figure 44.

Figure 44 Policy Routing

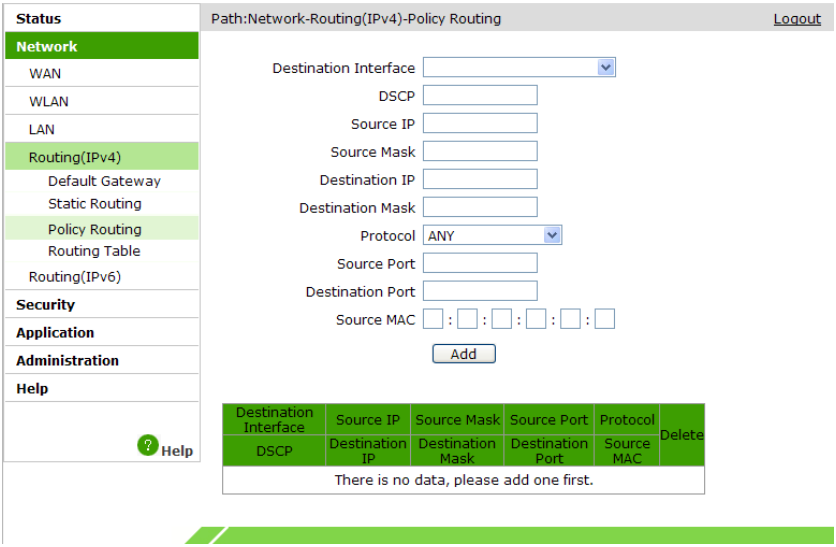


Table 23 lists the parameters for policy routing configuration.

Table 23 Parameters for Policy Routing Configuration

Parameter	Description
Destination Interface	Determined by the carrier
DSCP	Differential Services Code Point, whose value ranges from 0 to 63.
Source IP/Mask	Source IP address/mask.
Destination IP	Destination IP address
Destination Mask	Destination mask of the network segment
Protocol	Selected as required

Parameter	Description
Source Port	Source host Port
Destination Port	Destination host port
Source MAC	Source MAC address

3. Click **Add**.

Policy routing is configured.

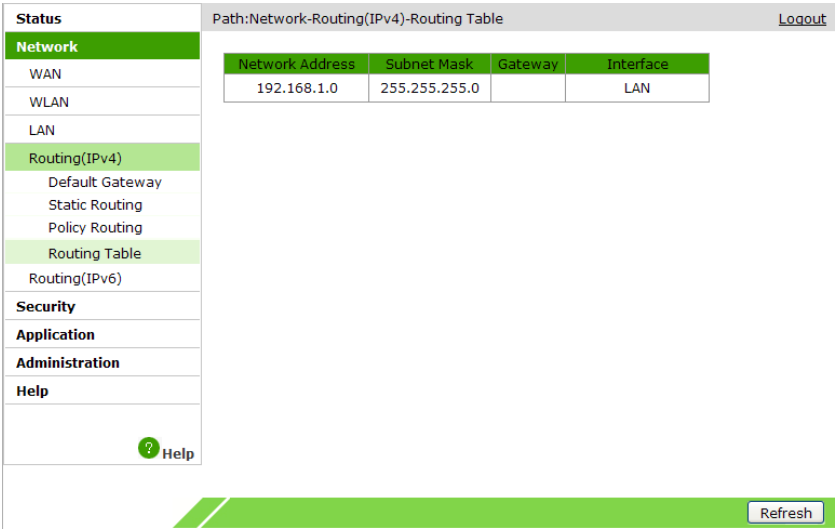
Postrequisite

You can also click  to delete the policy routing information.

4.4.4 Routing Table

Choose [**Network→ Routing(IPv4)→ Routing Table**], as shown in Figure 45.

Figure 45 Routing Table



4.5 Routing(IPv6)

IPv6 routing configuration includes the following:

- Default Gateway
- Static Routing
- Routing Table

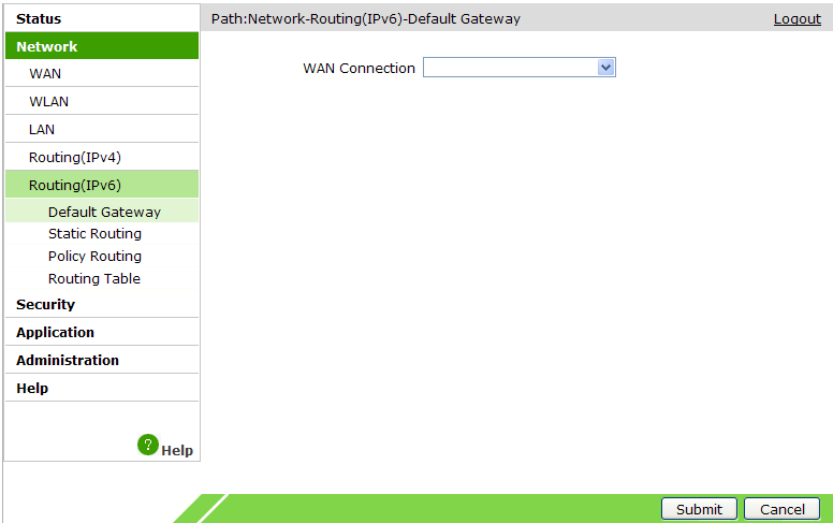
- Routing Table

4.5.1 Default Gateway

Steps

1. Choose [**Network→ Routing(IPv6)→ Default Gateway**], as shown in Figure 46.

   Figure 46 Default Gateway for IPv6 Routing Connection



2. Select the WAN connection from the **WAN Connection** drop-down list.
3. Click **Submit**.

4.5.2 Static Routing

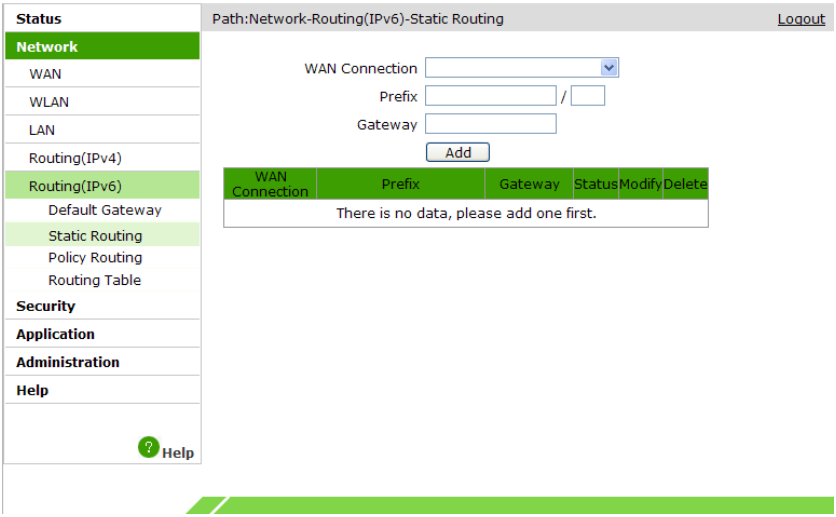
Context

To configure IPv6 static routing, perform the following steps:

Steps

1. Choose [**Network→ Routing(IPv6)→ Static Routing**], as shown in Figure 47.

Figure 47 IPv6 Static Routing



2. Configure the parameters.

   Table 24 describes the parameters for the static routing.

   Table 24 Parameters for the IPv6 Static Routing

Parameter	Description
WAN Connection	WAN connection for IPv6 static routing
Prefix	The prefix is consistent with the network segment of the IPv6 interface.
Gateway	The gateway is the next hop address when this routing interface transfers the packets of different network segment.

3. Click **Add**.

IPv6 static routing is configured.

4.5.3 Policy Routing

Steps

1. Choose [**Network→Routing(IPv6)→ Policy Routing**].
2. Select an interface from the **Destination Interface** drop-down list, as shown in Figure 48.

Figure 48 Policy Routing

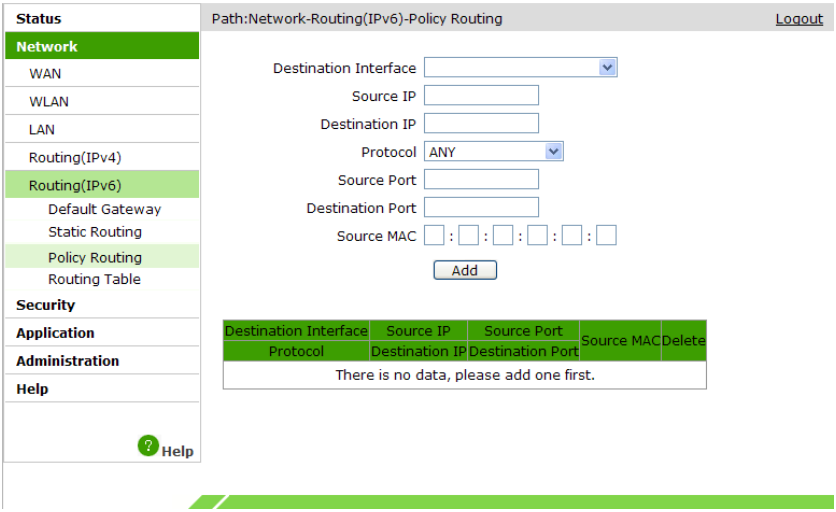


Table 25 lists the parameters for policy routing configuration.

Table 25 Parameters for Policy Routing Configuration

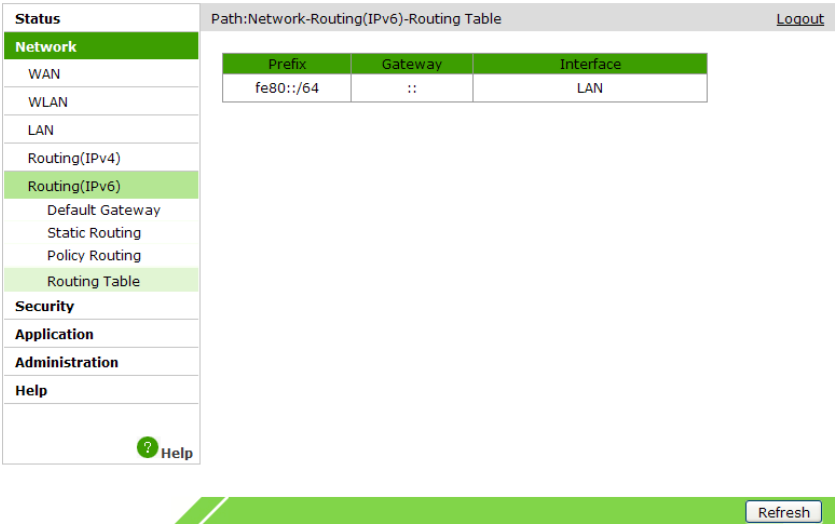
Parameter	Description
Destination Interface	Determined by the carrier
Source IP	Source IP address
Destination IP	Destination IP address
Protocol	Selected as required
Source Port	Source host Port
Destination Port	Destination host port
Source MAC	Source MAC address

3. Click **Add**.

4.5.4 Routing Table

Choose [**Network→ Routing(IPv6)→ Routing Table**], and the IPv6 routing table is displayed, as shown in Figure 49.

Figure 49 IPv6 Routing Table



5 Security

5.1 Firewall

Steps

1. Choose [**Security→ Firewall**].
2. Configure the firewall parameters, as shown in Figure 50.

Figure 50 Firewall

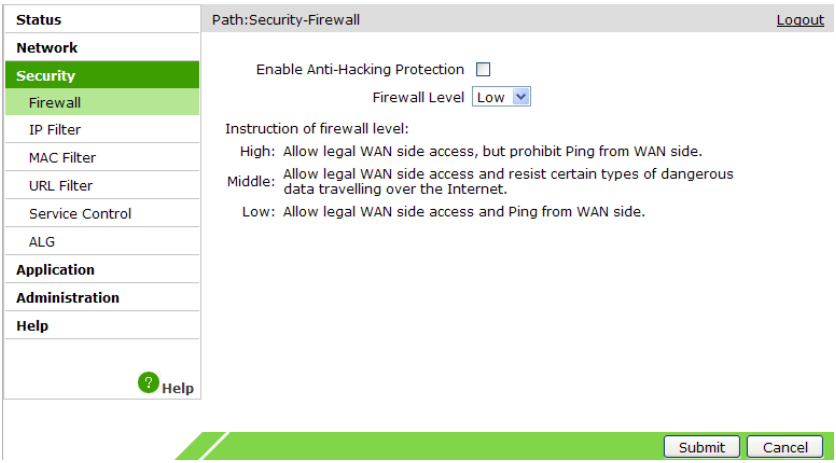


Table 26 lists the firewall parameters.

Table 26 Firewall Parameters

Parameter	Description
Enable Anti-Hacking Protection	Select the check box to enable anti-hacking protection. It prevents Ping flood, Ping to death, and Syn flood attack.
Firewall Level	Select the firewall level. The system supports the following firewall levels: ▸ Low ▸ Middle ▸ High

3. Click **Submit**.

The firewall is configured.

5.2 IP Filter

Context

To configure IP filter, perform the following steps:

Steps

1. Choose [**Security→ IP Filter**].
2. Configure the IP filter parameters, as shown in Figure 51.

Figure 51 IP Filter

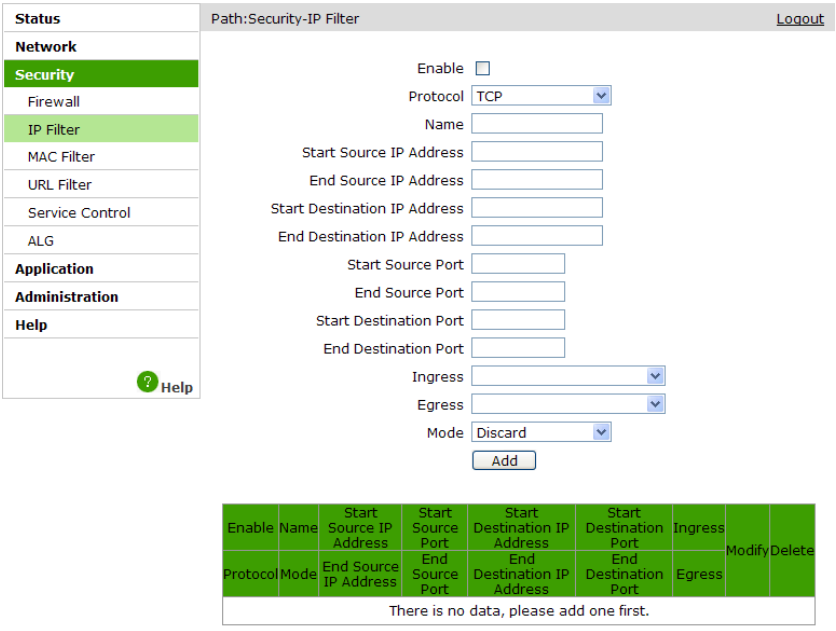


Table 27 lists the IP filter parameters.

Table 27 IP Filter Parameters

Parameter	Description
Enable	Select the check box to enable the IP filter item.
Protocol	Select the protocol that needs to filter packets. By default, it is TCP.
Name	Name of the IP filter item It cannot be null.
Start Source IP Address/End Source IP Address	Filter condition It can be null.
Start Destination IP Address/End Destination IP Address	Filter condition It can be null.
Start Source Port/End Source Port	Filter condition It can be null.
Start Destination Port/End Destination Port	Filter condition It can be null.
Ingress/Egress	Data flow direction The ingress and egress cannot be the same. ▸ If the ingress is LAN and egress is WAN, the data flow is upstream. ▸ If the ingress is WAN and egress is LAN, the data flow is downstream.
Mode	The mode can be **Discard** or **Permit**.

3. Click **Add**.

IP filter is configured.

5.3 MAC Filter

Context

MAC filter aims at the user-side LAN, that is, the upstream data flow.

To configure MAC filter, perform the following steps:

Steps

1. Choose [**Security→ MAC Filter**].
2. Configure the MAC filter parameters, as shown in Figure 52.

Figure 52 MAC Filter

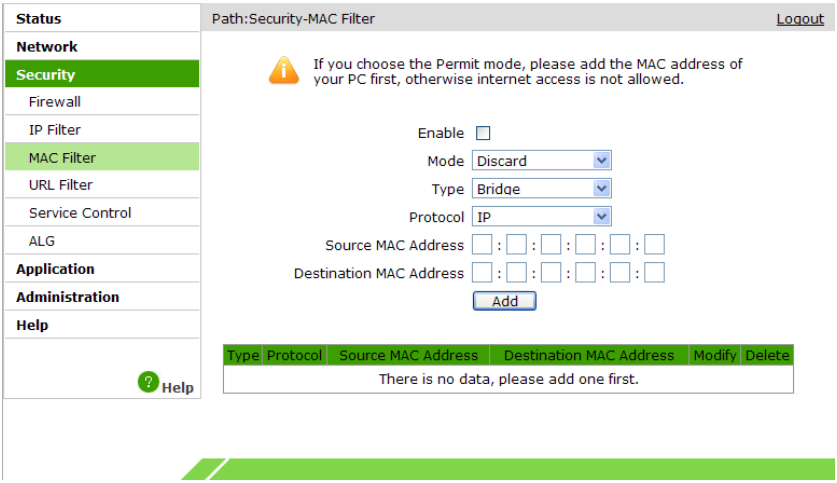


Table 28 lists the MAC filter parameters.

Table 28 MAC Filter Parameters

Parameter	Description
Enable	Select the check box to enable the MAC filter item.
Mode	The mode can be **Discard** or **Permit**.
Type	The type can be **Bridge**, **Route**, or **Bridge+Route**.
Protocol	Protocol type of the data flow
Source MAC Address/Destination MAC Address	MAC address that needs to be filtered It cannot be null.

3. Click **Add**.

MAC filter is configured.

Postrequisite

You can also modify or delete the MAC filter configuration, as listed in Table 29.

Table 29 MAC Filer Operations

Button	Description
	To modify the MAC filter configuration
	To delete the MAC filter configuration

5.4 URL Filter

Context

To configure URL filter, perform the following steps:

Steps

1. Choose [**Security→ URL Filter**].
2. Configure the URL filter parameters,as shown in Figure 53.

Figure 53 URL Filter

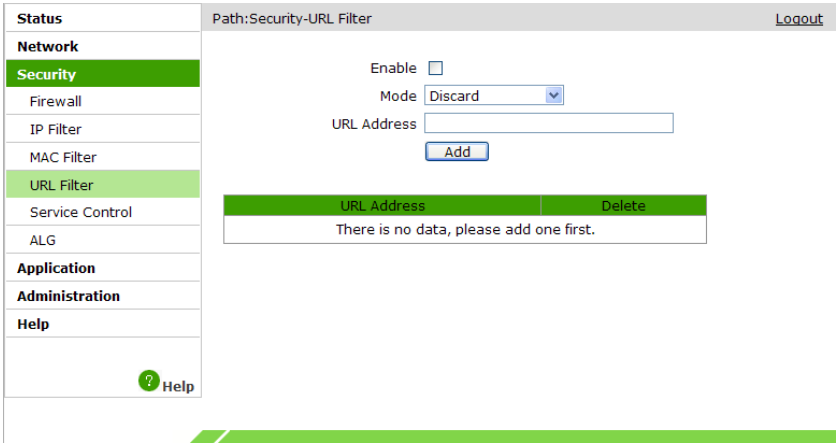


Table 30 lists the URL filter parameters.

Table 30 URL Filter Parameters

Parameter	Description
Enable	Select the check box to enable the URL filter item.
Mode	The mode can be **Discard** or **Permit**.
URL Address	URL address that needs to be filtered It cannot be null.

3. Click **Add**.

URL filter is configured.

Postrequisite

You can click to delete the URL filter item.

5.5 Service Control

Context

By default, you cannot visit the device through Telnet, FTP, or web site.

To configure service control, perform the following steps:

Steps

1. Choose [**Security→ Service Control**].
2. Configure the service control parameters,as shown in Figure 54.

Figure 54 Service Control

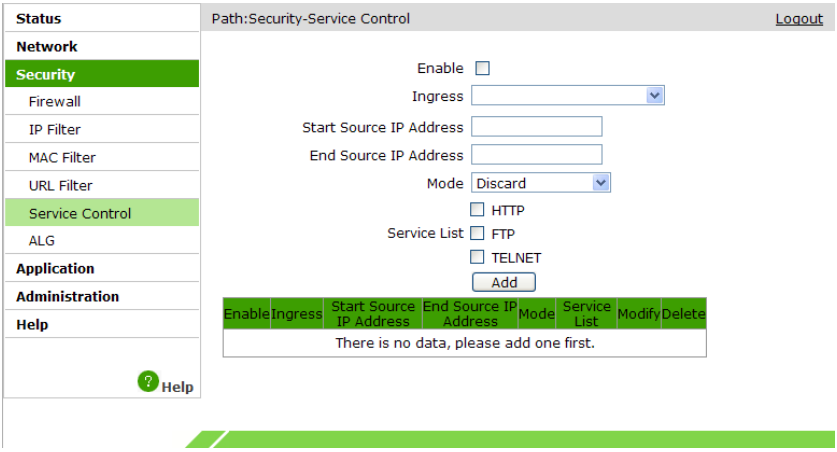


Table 31 lists the service control parameters.

Table 31 Service Control Parameters

Parameter	Description
Enable	Select the check box to enable the service control item.
Ingress	According to the data flow direction, the ingress can be as follows: ▸ WAN ▸ Broadcast connection ▸ LAN This parameter cannot be null.
Start Source IP Address/End Source IP Address	IP address segment that needs to be filtered When this parameter is null, it refers to all the IP addresses.

Parameter	Description
Mode	The mode can be **Discard** or **Permit**.
Service List	The service list includes **HTTP**, **FTP**, **TELNET** and **HTTPS**.

3. Click **Add**.

Service control is configured.

Postrequisite

You can also modify or delete the service control configuration, as listed in Table 32.

Table 32 Service Control Operations

Button	Description
	To modify the service control configuration
	To delete the service control configuration
Modify Remote Access Port	To modify the remote access port

5.6 ALG

Context

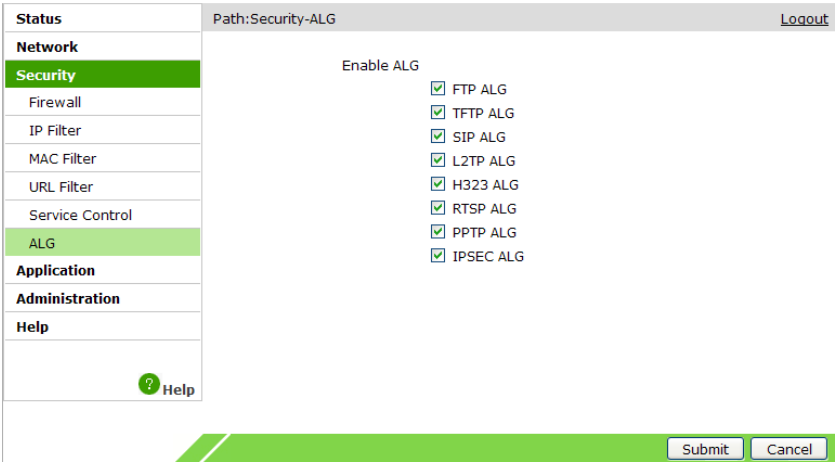
The ALG functions allows the system to convert the private addresses to the public addresses in the packets for the security purpose.

To configure the ALG setting, perform the following steps:

Steps

1. Choose [**Security→ ALG**].
2. Configure the service control parameters, as shown in Figure 55.

Figure 55 ALG



3. Click **Submit**.

The ALG setting is configured.

6 Application

6.1 VoIP

This section includes the following topics:

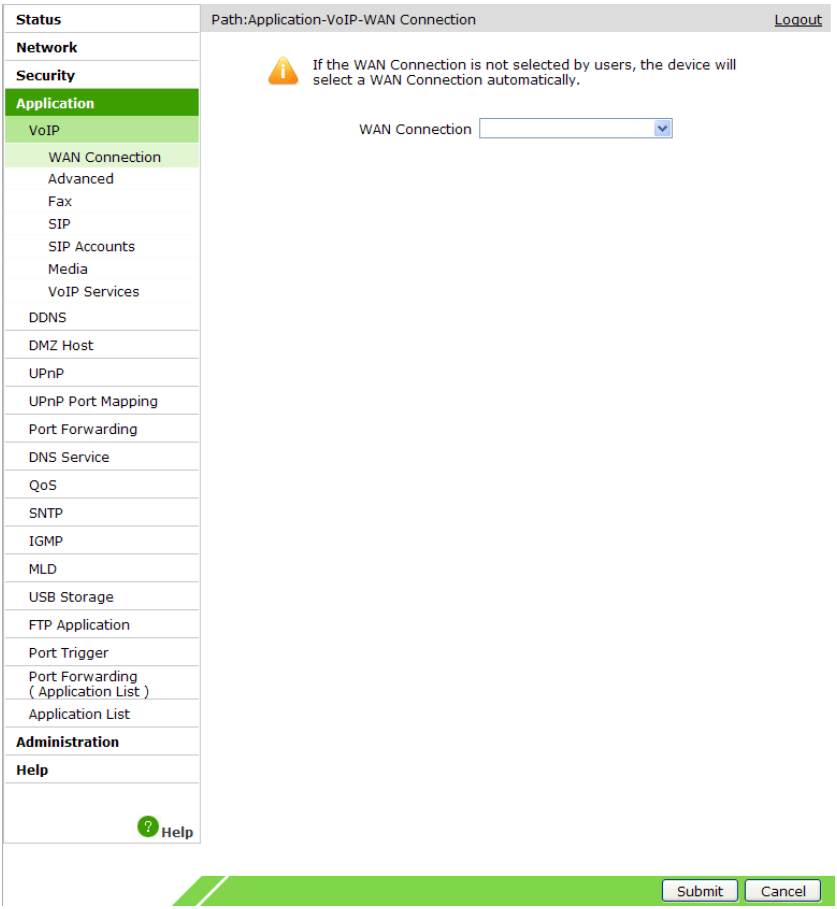
- WAN Connection
- Advanced
- Fax
- SIP
- SIP Accounts
- Media
- Dial Plan

6.1.1 WAN Connection

Steps

1. Choose [**Application→ VoIP→ WAN Connection**].
2. Select a WAN connection from the **WAN Connection** drop-down list, as shown in Figure 56.

Figure 56 VoIP WAN Connection



Note:

If the WAN connection is not selected by user, the device selects a WAN connection for the VoIP service automatically.

3. Click **Submit**.

6.1.2 Advanced

Context

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

Steps

1. Choose [**Application→ VoIP→ Advanced**].

2. Configure the VoIP advanced parameters, as shown in Figure 57.

Figure 57 VoIP Advanced Parameters

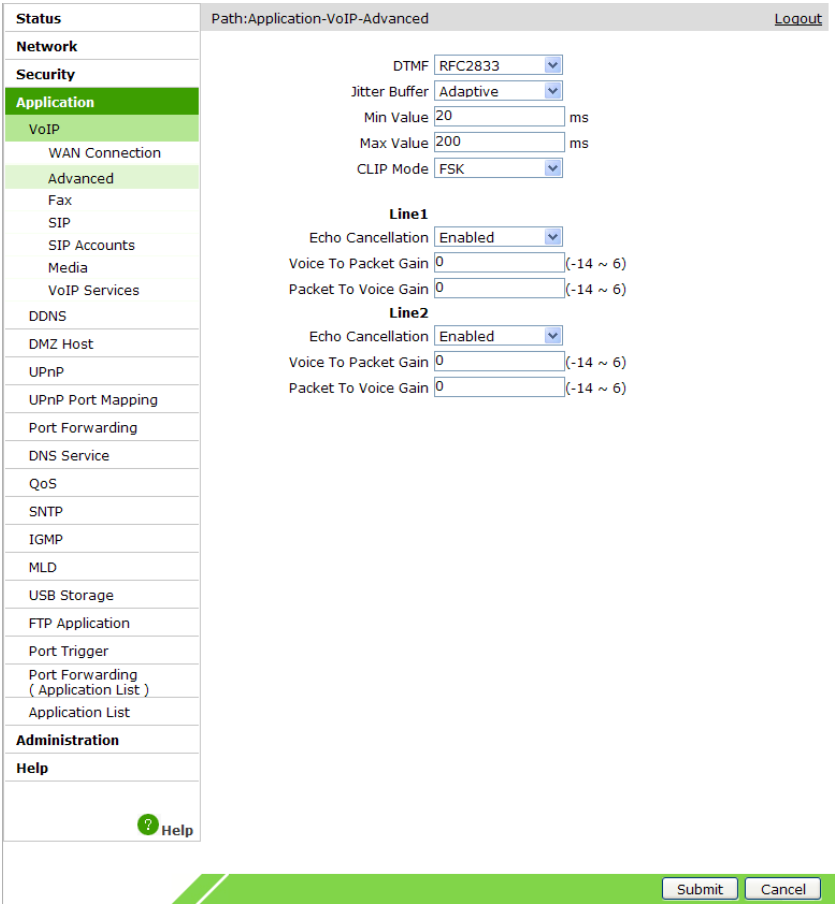


Table 33 describes the VoIP advanced parameters.

Table 33 VoIP Advanced Parameters

Parameter	Description
DTMF	DTMF mode There are two options: **RFC2833** and **DTMF in Voice**.
Jitter Buffer	There are two options: **Fixed** and **Adaptive**.
Min Value	Minimum jitter buffer value Default: 20 ms

Parameter	Description
Max Value	Maximum jitter buffer value Default: 20 ms
CLIP Mode	Calling line identification presentation mode
Echo Cancellation	Select this check box to enable the echo cancellation.
Voice To Packet Gain	Gain from the telepone to the network (tdm->net gain)
Packet To Voice Gain	Gain from the network to the telephone (net->tdm gain)

3. Click **Submit**.

The VoIP advanced parameters are configured.

6.1.3 Fax

Context

To configure the VoIP fax, perform the following steps:

Steps

1. Choose [**Application→ VoIP→ Fax**].
2. Configure the VoIP fax parameters, as shown in Figure 58.

Figure 58 VoIP Fax

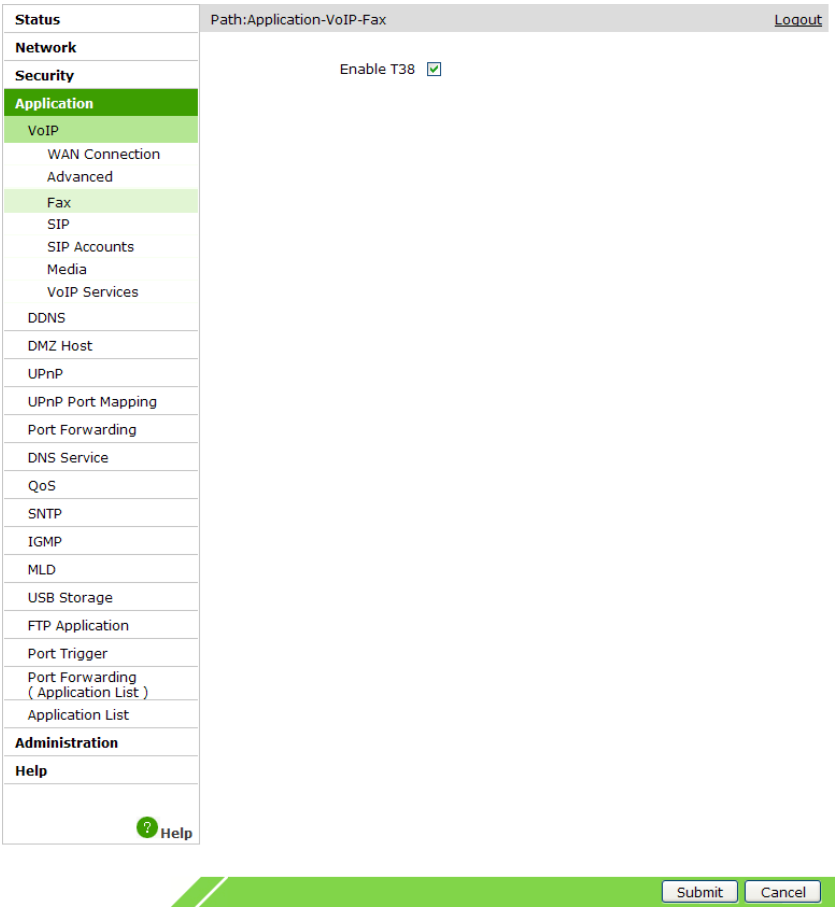


Table 34 describes the VoIP fax parameters.

Table 34 VoIP Fax Parameters

Parameter	Description
Enable T38	Select this check box to enable the T38 protocol function.

3. Click **Submit**.

The VoIP fax is configured.

6.1.4 SIP

Context

To configure the SIP parameters, perform the following steps:

Steps

1. Choose [**Application→ VoIP→ SIP**].
2. Configure the SIP parameters, as shown in Figure 59.

Figure 59 SIP

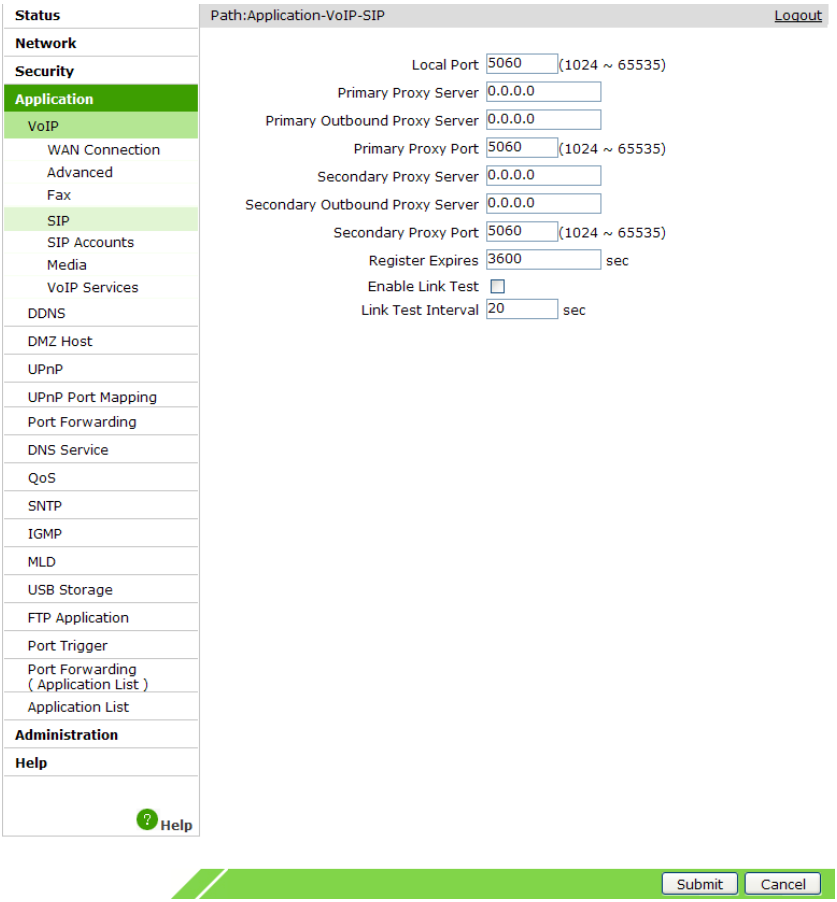


Table 35 describes the parameters for the SIP configuration.

Table 35 SIP Configuration Parameters

Parameter	Description
Local Port	Local port used by VoIP
Primary Proxy Server	Address of the primary proxy server
Primary Outbound Proxy Server	IP address of the primary outbound proxy server, provided by the ISP
Primary Proxy Port	Port number of the primary proxy server Range: 1024 – 65535 Default: 5060
Secondary Proxy Server	IP address of the secondary proxy server, provided by the ISP
Secondary Outbound Proxy Server	IP address of the secondary outbound proxy server, provided by the ISP
Secondary Proxy Port	Port number of the secondary proxy server Range: 1024 – 65535 Default: 5060
Register Expires	Registration valid period Default: 3600 seconds
Enable Link Test	To enable Link detection of the SIP signaling
Link Test Interval	Time interval to perform the link detection of the SIP signaling Default: 20 seconds

3. Click **Submit**.

The SIP parameters are configured.

6.1.5 SIP Accounts

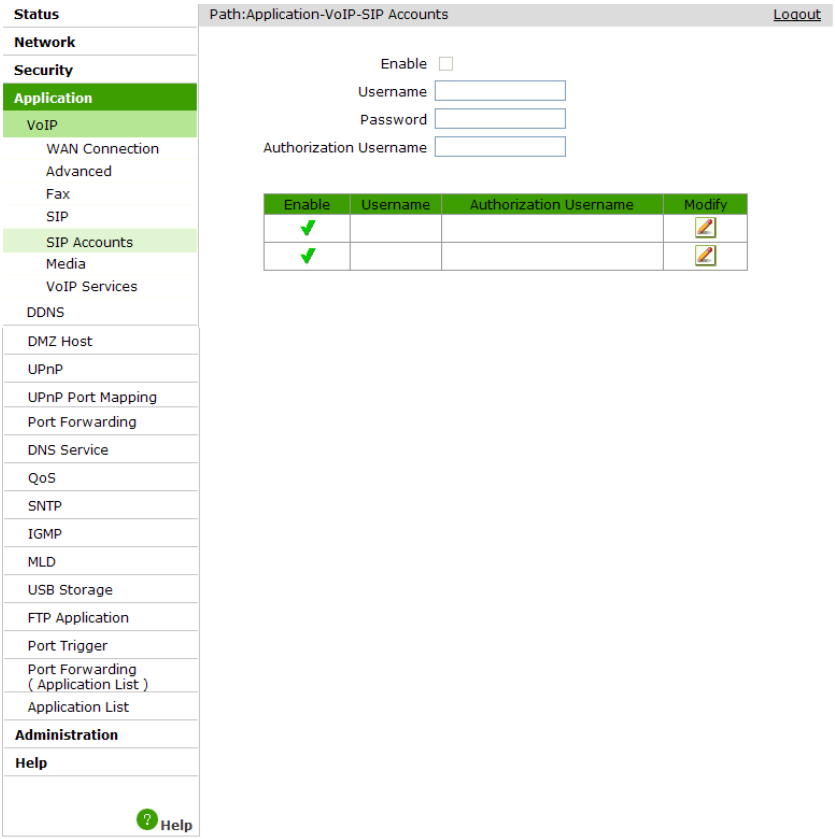
Context

To configure the SIP accounts, perform the following steps:

Steps

1. Choose [**Application→ VoIP→ SIP Accounts**] to display the SIP account information, as shown in Figure 60.

Figure 60 SIP Accounts



2. Click  to modify the SIP accounts, as shown in Figure 61.

Figure 61 SIP Account Modification

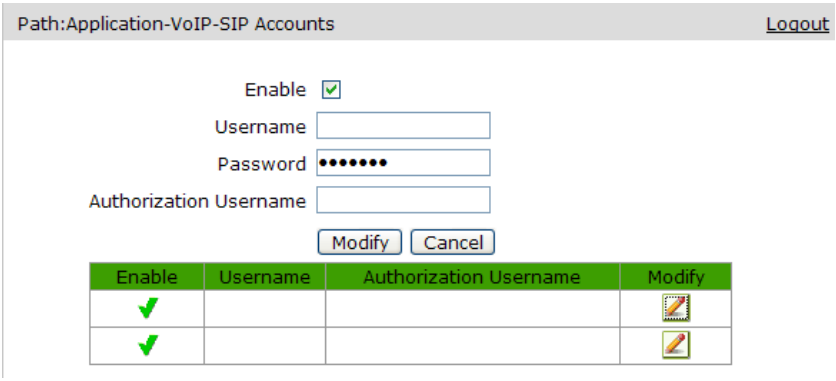


Table 36 describes the parameters for the SIP account configuration.

Table 36 Paramters for the SIP Account Configuration

Parameter	Description
Enable	To enable the SIP account authentication
Username	SIP registration user name, provided by ISP
Password	Registration password of SIP authentication user
Authorization Username	User name for the server to authenticate the sent message by the device

3. Click **Modify** to confirm the modification.

The SIP accounts are configured.

6.1.6 Media

Context

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

Steps

1. Choose [**Application→ VoIP→ Media**].
2. Configure the VoIP media parameters, as shown in Figure 62.

Figure 62 VoIP Media

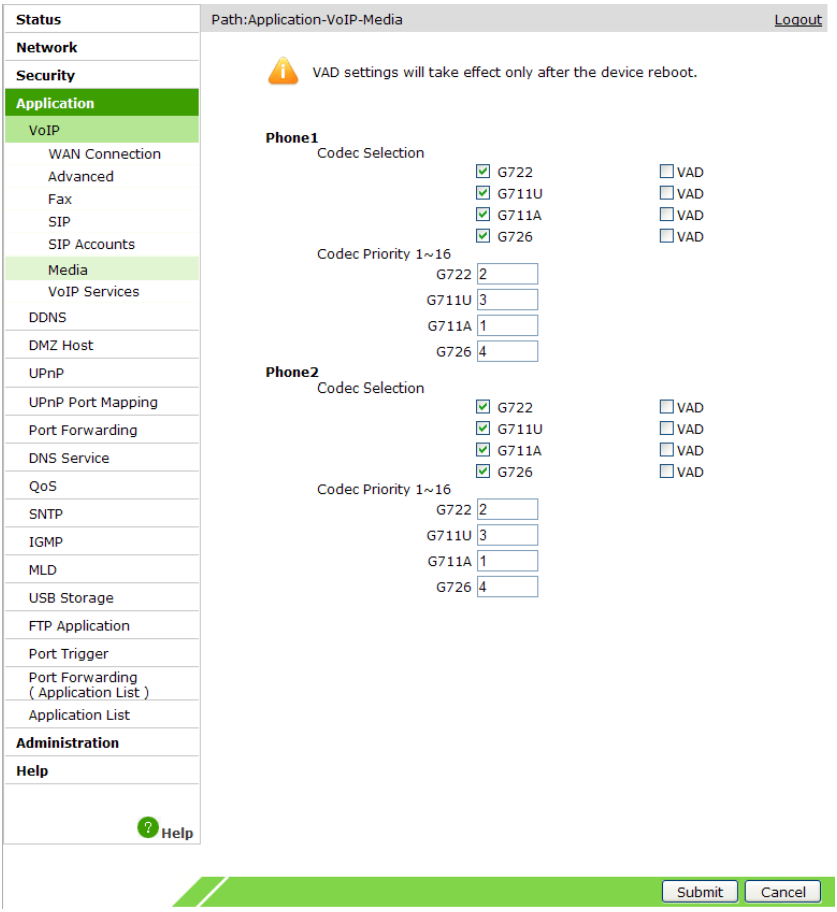


Table 37 describes the VoIP media parameters.

Table 37 VoIP Media Parameters

Parameter	Description
Codec Selection	Codec mode supported by the media
Codec Priority	Range: 1–16 1 means the highest priority and 16 means the lowest priority.

3. Click **Submit**.

The VoIP media parameters are configured.

6.1.7 VoIP Services

Steps

1. Choose [**Application→ VoIP→ VoIP Services**].
2. Configure the parameters, as shown in Figure 63.

Figure 63 VoIP Services

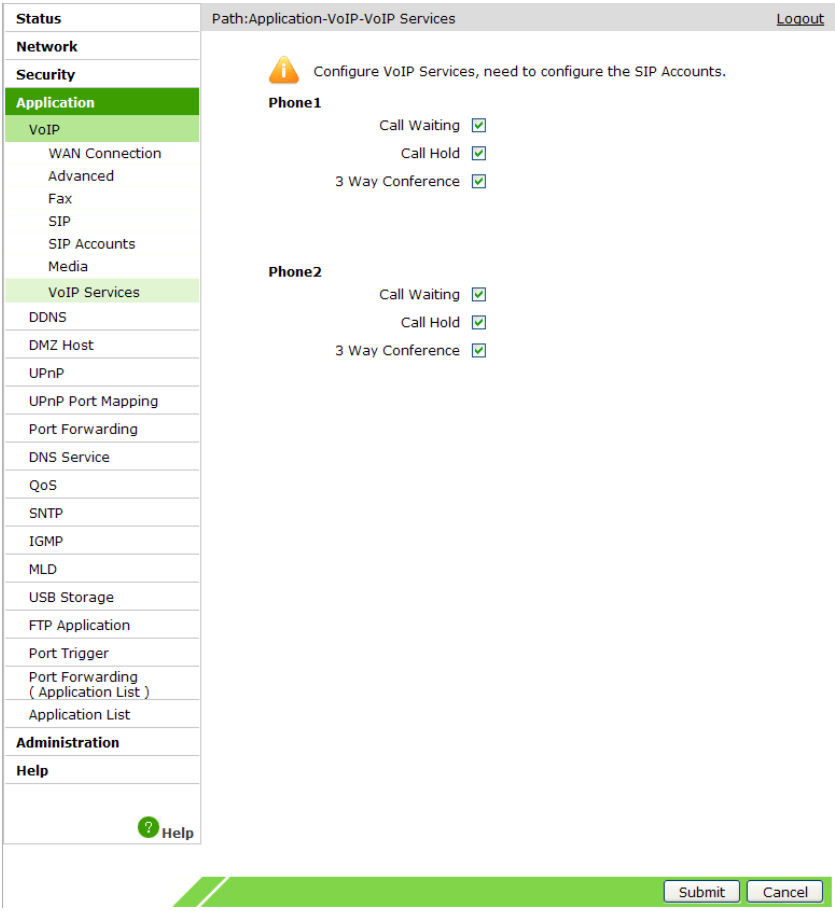


Table 38 describes the dial plan parameters.

Table 38 Dial Plan Parameters

Parameter	Description
Call Waiting	Select this check box to enable the call waiting function.
Call Hold	Select this check box to enable the call hold function.
3 Way Conference	Select this check box to enable the 3 Way Conference function.

3. Click **Add**.

The VoIP dial plan is configured.

6.2 DDNS

You can configure DDNS to enable the host that has a dynamic IP address to provide the domain name service.

DDNS is a method of updating, in real time, a Domain Name System to point to a changing IP address on the Internet. This is used to provide a persistent domain name for a resource that may change location on the network.

Steps

1. Choose [**Application→ DDNS**].
2. Configure the DDNS parameters, as shown in Figure 64.

Figure 64 DDNS

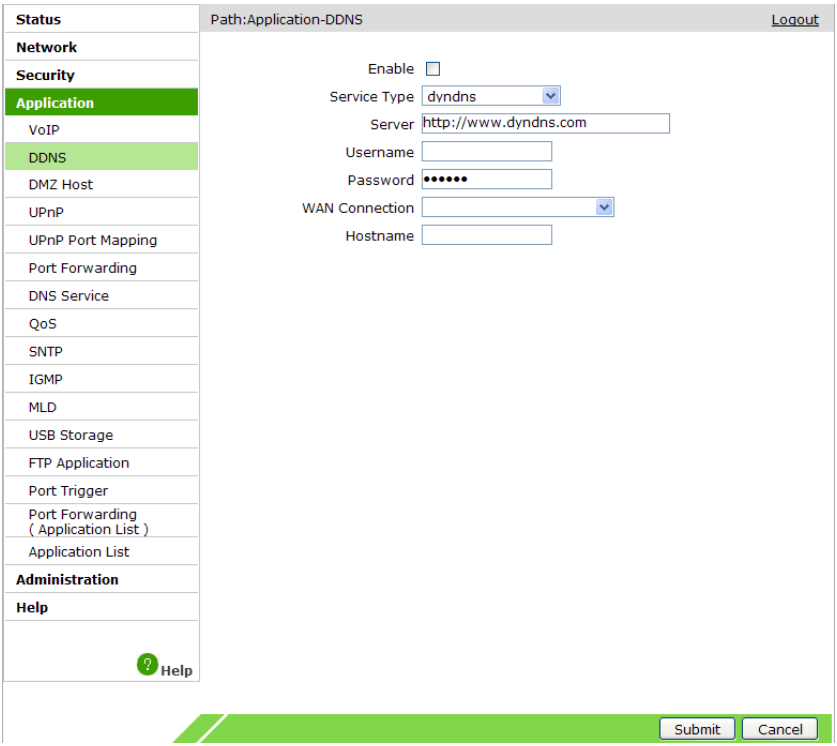


Table 39 lists the DDNS parameters.

Table 39 DDNS Parameters

Parameter	Description
Enable	Select the check box to enable the DDNS function.
Service Type	DDNS service type includes **dipc**, **dyndns**, and **DtDNS**.
Server	Server address If the GNUDIP HTTP is used, the server address is a URL. By default, it is http://ns.eagleeyes.com.cn/cgi-bin/gdipupdt.cgi.
Username	DDNS server user name
Password	DDNS server password
WAN Connection	WAN connection for routing.
Hostname	DDNS host name.

3. Click **Submit**.

DDNS is configured.

6.3 DMZ Host

You can configure DMZ to enable the DMZ all-port mapping function. The LAN-side host provides services through DNAT.

Context

To configure the DMZ host, perform the following steps:

Steps

1. Choose [**Application→ DMZ Host**].
2. Configure the DMZ host parameters, as shown in Figure 65.

Figure 65 DMZ Host

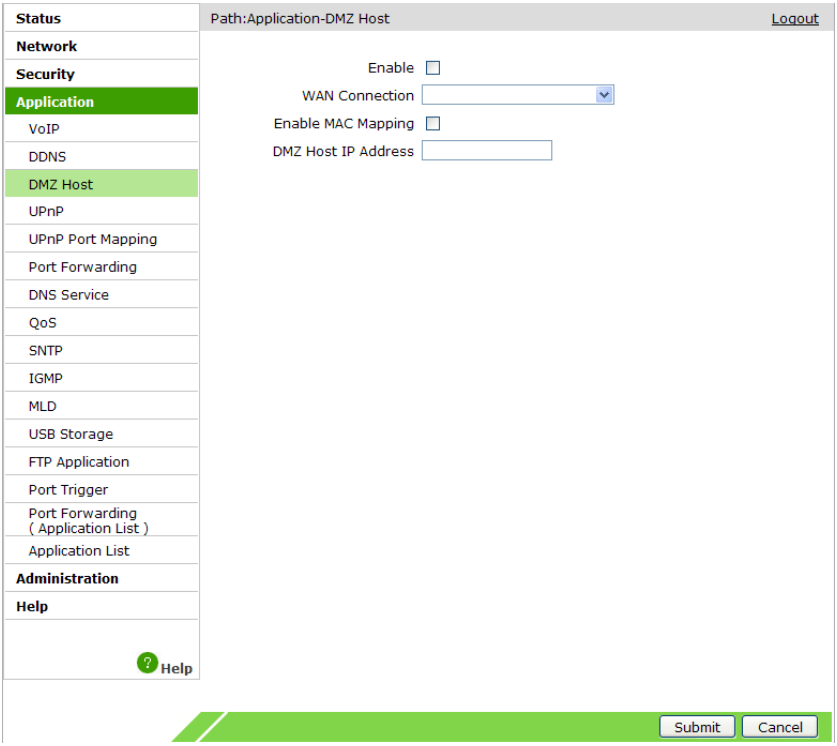


Table 40 lists the DMZ host parameters.

Table 40 DMZ Host Parameters

Parameter	Description
Enable	Select the check box to enable the DMZ host function.
WAN Connection	WAN connection used by the LAN-side host to provide services
Enable MAC Mapping	Select the check box to enable the MAC mapping function.
DMZ Host IP Address	IP address of the LAN-side host

3. Click **Submit**.

The DMZ host is configured.

6.4 UPnP

Context

The UPnP function supports zero configuration, invisible networking, and auto discovery on the device type.

To configure UPnP, perform the following steps:

Steps

1. Choose [**Application→ UPnP**].
2. Configure the UPnP parameters, as shown in Figure 66.

Figure 66 UPnP

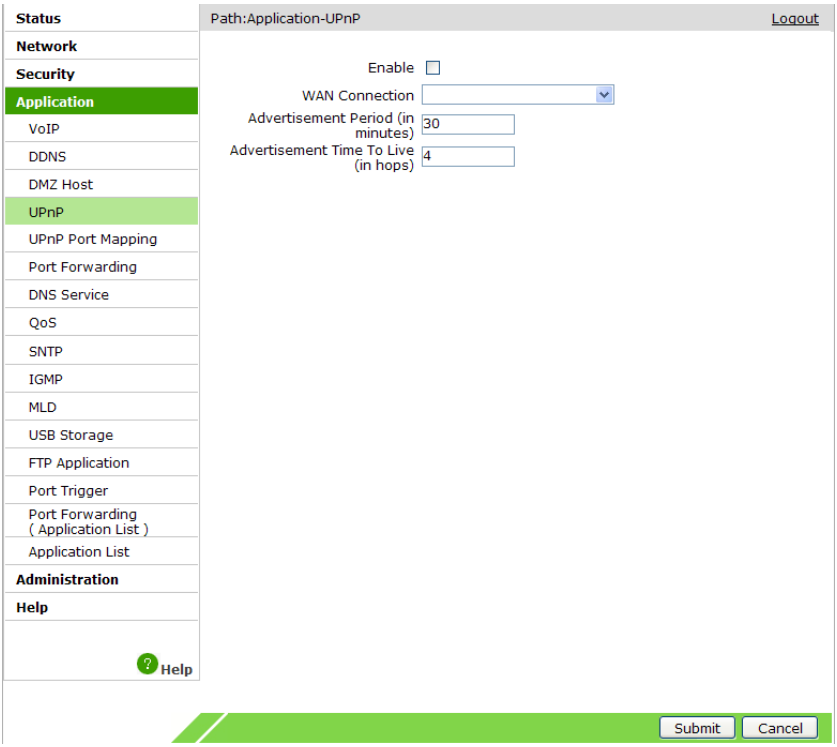


Table 41 lists the UPnP parameters.

Table 41 UPnP Parameters

Parameter	Description
Enable	Select the check box to enable the UPnP function.
WAN Connection	WAN connection
Advertisement Period (in minutes)	Time period that the UPnP device sends an announcement packet If the UPnP device does not send any announcement packet during this period, it indicates that the device is invalid. By default, the period is 30 minutes.
Advertisement Time To Live (in hops)	TTL value that the UPnP device sends the announcement packets, that is, the maximum routing times By default, it is 4.

3. Click **Submit**.

UPnP is configured.

6.5 UPnP Port Mapping

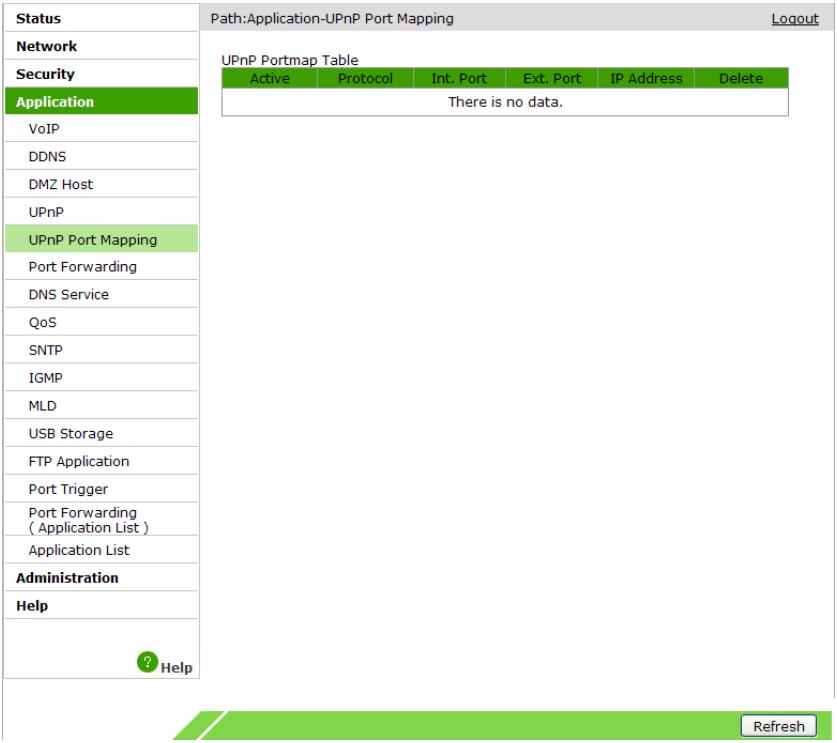
Prerequisite

The UPnP device is connected.

Steps

1. Choose [**Application→ UPnP Port Mapping**].
2. View the UPnP port mapping, as shown in Figure 67.

Figure 67 UPnP Port Mapping



6.6 Port Forwarding

Context

To configure port forwarding, perform the following steps:

Steps

1. Choose [**Application→ Port Forwarding**].
2. Configure the port forwarding parameters, as shown in Figure 68.

Figure 68 Port Forwarding

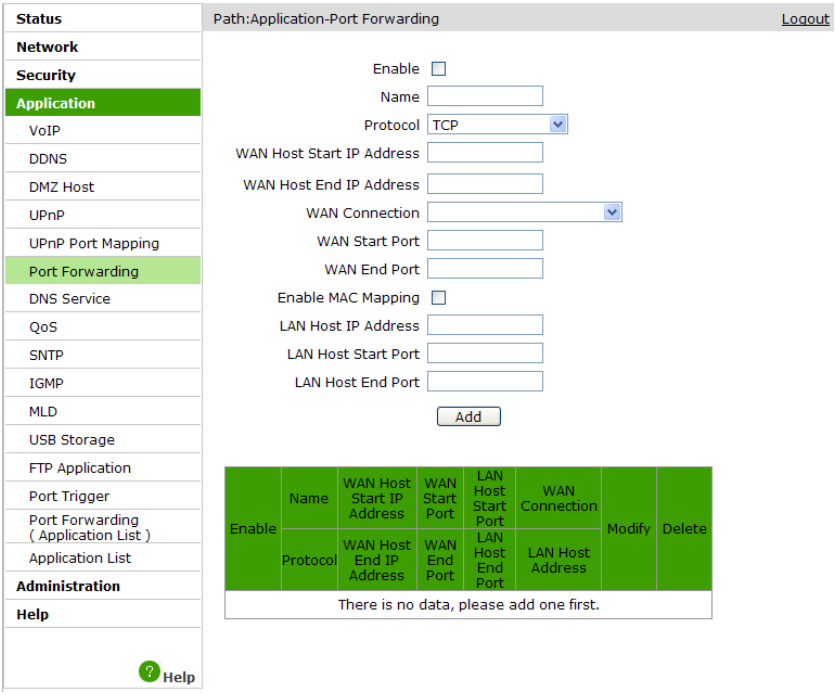


Table 42 lists the port forwarding parameters.

Table 42 Port Forwarding Parameters

Parameter	Description
Enable	Select the check box to enable port forwarding function.
Name	Virtual host name, which cannot be null
Protocol	Protocol of the permitted packet Default: TCP
WAN Host Start IP Address/WAN Host End IP Address	IP address segment of the WAN-side host
WAN Connection	WAN connection
WAN Start Port/WAN End Port	Port number range of the WAN-side host

Parameter	Description
Enable MAC Mapping	Select the check box to enable the MAC mapping function.
LAN Host IP Address	IP address of the LAN-side host
LAN Host Start Port/LAN Host End Port	Port number range of the LAN-side host

3. Click **Add**.

Postrequisite

You can also modify or delete the port forwarding configuration, as listed in Table 43.

Table 43 Port Forwarding Operations

Button	Description
	To modify the port forwarding configuration
	To delete the port forwarding configuration

6.7 DNS Service

DNS service configuration includes the following:

- Domain Name
- Hosts
- DNS

6.7.1 Domain Name

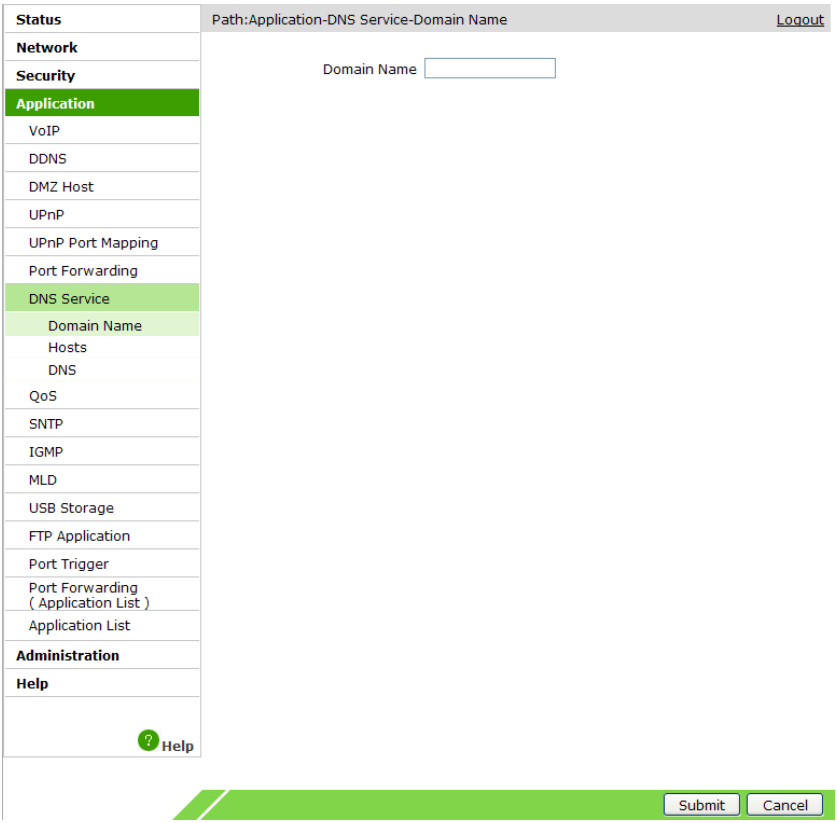
Context

To set the domain name, perform the following steps:

Steps

1. Choose [**Application**→ **DNS Service**→ **Domain Name**], as shown in Figure 69.

Figure 69 Domain Name



2. On the right pane, type the domain name in the **Domain Name** text box.
3. Click **Submit**.

The domain name is set.

6.7.2 Hosts

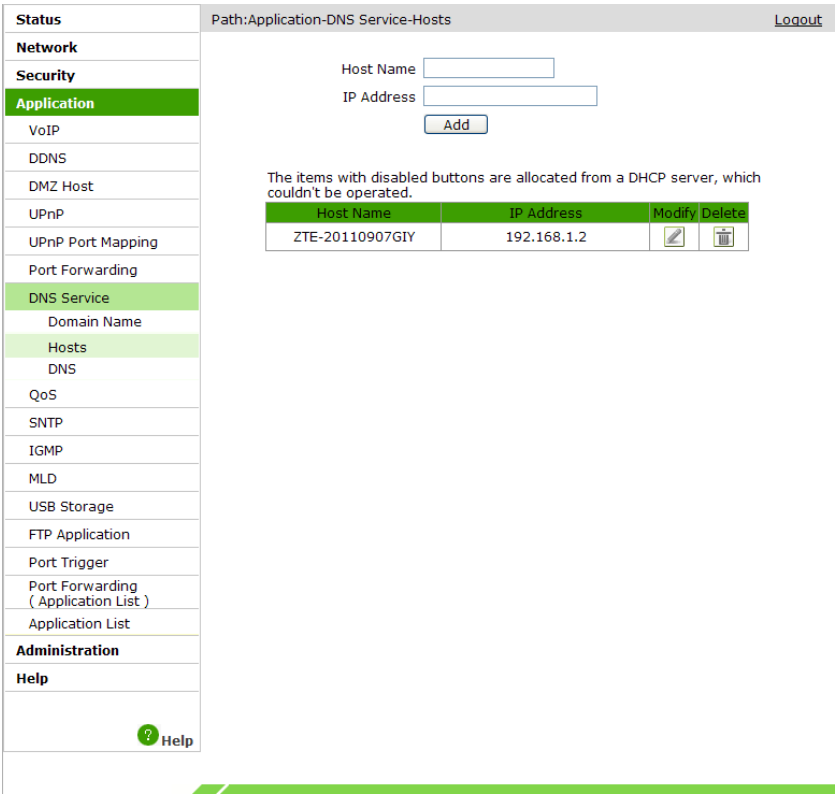
Context

To set the host name and IP address, perform the following steps:

Steps

1. Choose [**Application**→ **DNS Service**→ **Hosts**], as shown in Figure 70.

Figure 70 Hosts



2. Type the host name in the **Host Name** text box and IP address in the **IP Address** text box.
3. Click **Add**.

Postrequisite

You can also modify or delete the host name, as listed in Table 44.

Table 44 Host Name Operations

Button	Description
	To modify the host name or IP address
	To delete the host name or IP address

6.7.3 DNS

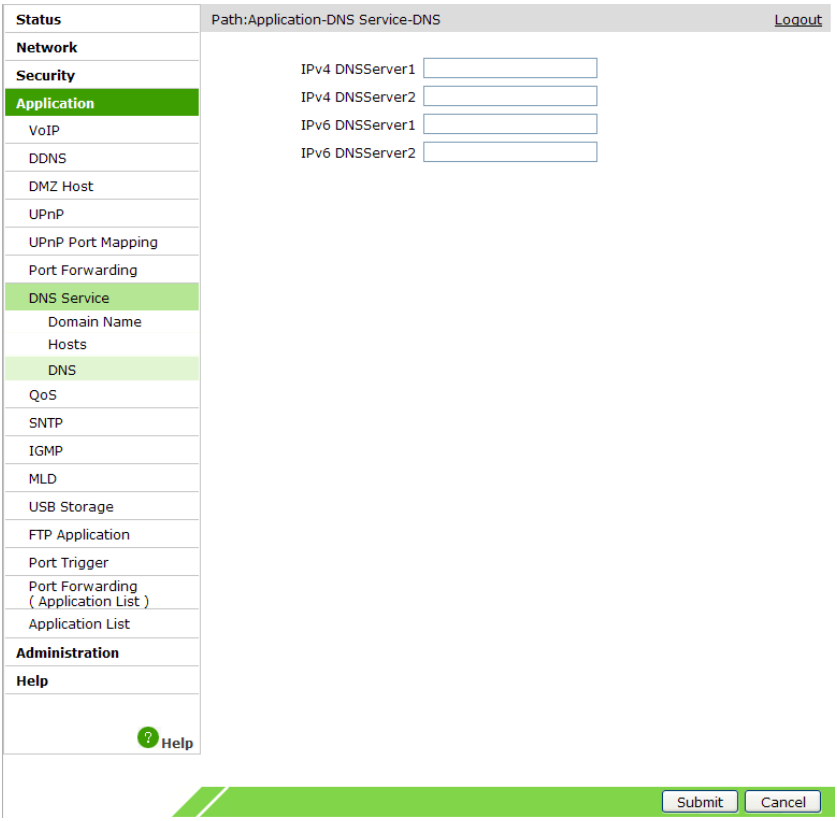
Perform this procedure to configure the global DNS parameters.

The global DNS parameters are configured. The DNS server assigns the IP address to the ZXHN H298N device.

Steps

1. Choose [**Application→ DNS Service→ DNS**], as shown in Figure 71.

Figure 71 DNS



2. On the right pane, type the DNS server names in the text boxes.
3. Click **Submit**.

The global DNS parameters are configured.

6.8 QoS

QoS configuration includes the following:

- Basic
- Classification
- Queue Management
- Committed Access Rate

6.8.1 Basic

Perform this procedure to enable or disable the QoS function.

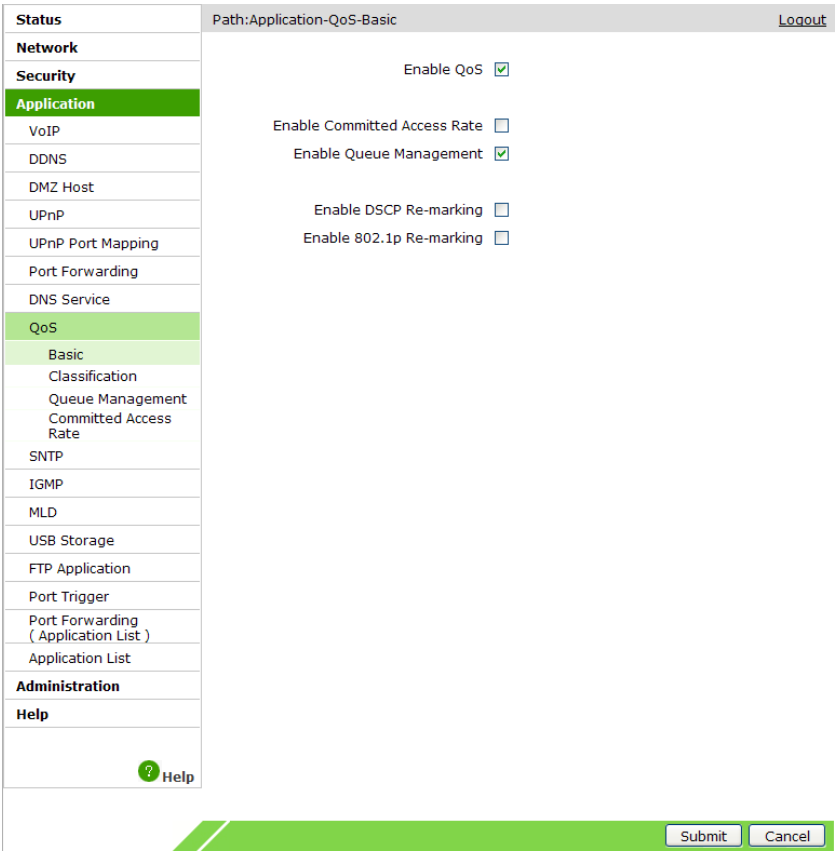
Context

To enable or disable the QoS function, perform the following steps:

Steps

1. Choose [**Application**→ **QoS**→ **Basic**], as shown in Figure 72.

Figure 72 Basic QoS Parameters



2. Configure the QoS basic parameters, as described in Table 45.

Table 45 QoS Basic Parameters

Parameter	Description
Enable QoS	To enable or disable the QoS function
Enable Committed Access Rate	To enable or disable Committed Access Rate (CAR) ▸ If CAR is enabled, the configurations on [**Application→ QoS→ Committed Access Rate**] are effective. ▸ If CAR is disabled, the configurations on [**Application→ QoS→Committed Access Rate**] are ineffective.

Parameter	Description
Enable Queue Management	To enable or disable upstream congestion management To configure the congestion management function, select [**Application→ QoS→ Queue Management**].
Enable DSCP Re-marking	To enable or disable DSCP Re-marking. To configure this function, select [**Application→ QoS→ Classification**].
Enable 802.1P Re-marking	To enable or disable 802.1p remarking To configure this function, select [**Application→ QoS→Classification**].

3. Click **Submit**.

The basic QoS parameters are configured.

6.8.2 Classification

Prerequisite

Before this operation, make sure that the basic QoS configuration is complete.

Steps

1. Choose [**Application→ QoS→ Classification**].
2. Configure the QoS classification parameters, as shown in Figure 73.

Figure 73 Classification

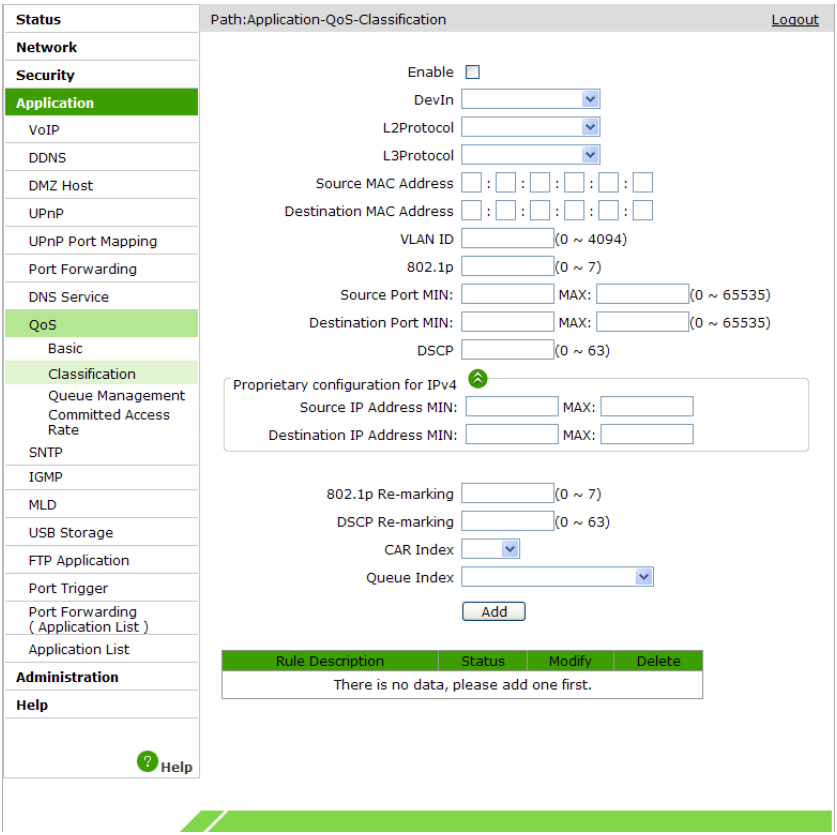


Table 46 lists the QoS classification parameters.

Table 46 QoS Classification Parameters

Parameter	Description
Enable	To enable the classification function
DevIn	Data flow ingress
L2Protocol	Range: IPv4, IPv6, ARP, PPPoE
L3Protocol	Range: TCP, UDP, ICMP
Source MAC Address	Source host MAC address
Destination MAC Address	Destination host MAC address
VLAN ID	Range: 0–4094
802.1p	Range: 0–7

Parameter	Description
Source Port MIN/MAX	Range: 0–65535
Destination Port MIN/MAX	Range: 0–65535
DSCP	Range: 0–63
Source IP Address MIN/MAX	Source IPv4 address range of the matched data flow
Destination IP Address MIN/MAX	Destination IPv4 address range of the matched data flow
802.1p Re-marking	To modify the 802.1p field value when the packet is sent from the WAN side. If the data flow that matches the classification rule is sent to the CPE, this parameter does not take effect. Range: 0–7
DSCP Re-marking	To modify the DSCP field value when the packet is sent from the WAN side. If the data flow that matches the classification rule is sent to the CPE, this parameter does not take effect. Range: 0–63
CAR Index	To limit the ingress rate for the data flow. Set the value range on **Rule Number** in **Committed Access Rate**.
Queue Index	To perform the queue rule processing when the packet is sent from the WAN. The content of the parameter is displayed as “queue rule ID&device name&queue priority”. For example, “Key1&eth0&Prio1” indicates to process the packet that match the classification rule in the first-priority queue on the eth0 device. If this packet is not sent from the eth0 device at last (this may occur on the ADSL uplink), this packet is processed in the default queue on the current device.

3. Click **Add**.

The QoS classification rules are configured.

6.8.3 Queue Management

Prerequisite

Before this operation, make sure that the basic QoS configuration is complete and the queue management is enabled.

Context

Each device can be configured up to 4 queues.

To configure the QoS queue management, perform the following steps:

Steps

1. Choose [**Application→ QoS→ Queue Management**].
2. Configure the queue settings of a queue, as shown in Figure 74.

Figure 74 Queue Management

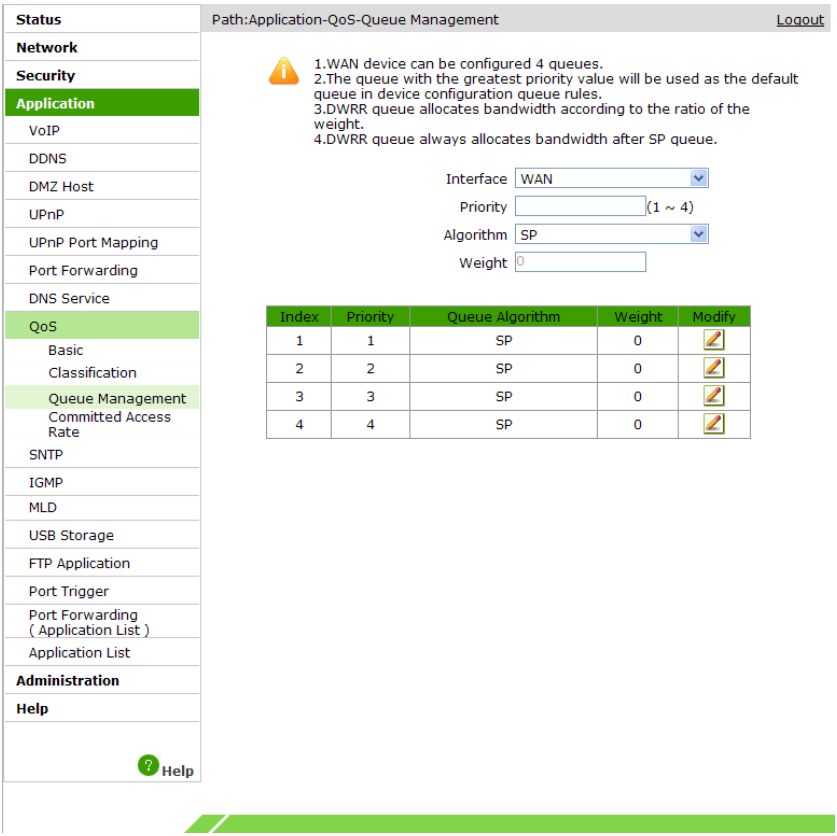


Table 47 lists the queue management parameters.

Table 47 Queue Management Parameters

Parameter	Description
Interface	Indicates the interface to which the queue management function applies: WAN, LAN1, LAN2, LAN3, or LAN4.
Priority	Indicates the processing priority in the range of 1-4. The queue with the greatest priority value will be used as the default queue in device configuration queue rules.
Algorithm	Indicates the queue algorithm, which is SP by default.
Weight	When **DWRR** is selected for **Algorithm**, enter the weight in the text box. Algorithm doesn't work until the sum of queues' weight comes to 100%.

3. Click **Add**.

QoS management is configured.

Postrequisite

You can also modify or delete the QoS rules, as listed in Table 48.

Table 48 Queue Management Operations

Button	Description
	To modify the rules of a queue
	To delete the rules of a queue

6.8.4 Committed Access Rate

Context

To configure the QoS committed access rate, perform the following steps:

Steps

1. Choose [**Application→ QoS→ Committed Access Rate**].
2. Configure the access rate parameters, as shown in Figure 75.

Figure 75 Committed Access Rate

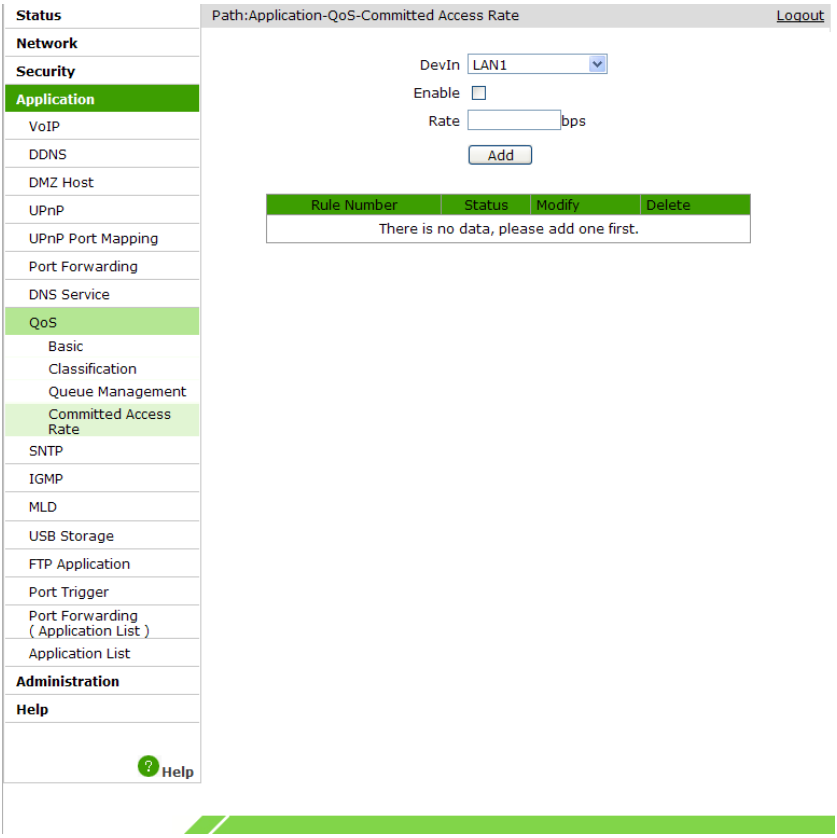


Table 49 describes the parameters for the committed access rate.

Table 49 Parameters for the Committed Access Rate

Parameter	Description
DevIn	The user interface to specify the committed access rate
Enable	To enable the committed access rate function
Rate	Committed access rate

3. Click **Add**.

The committed access rate is configured.

6.9 SNTP

Context

To configure SNTP, perform the following steps:

Steps

1. Choose [**Application→ SNTP**].
2. Configure the SNTP parameters, as shown in Figure 76.

Figure 76 SNTP

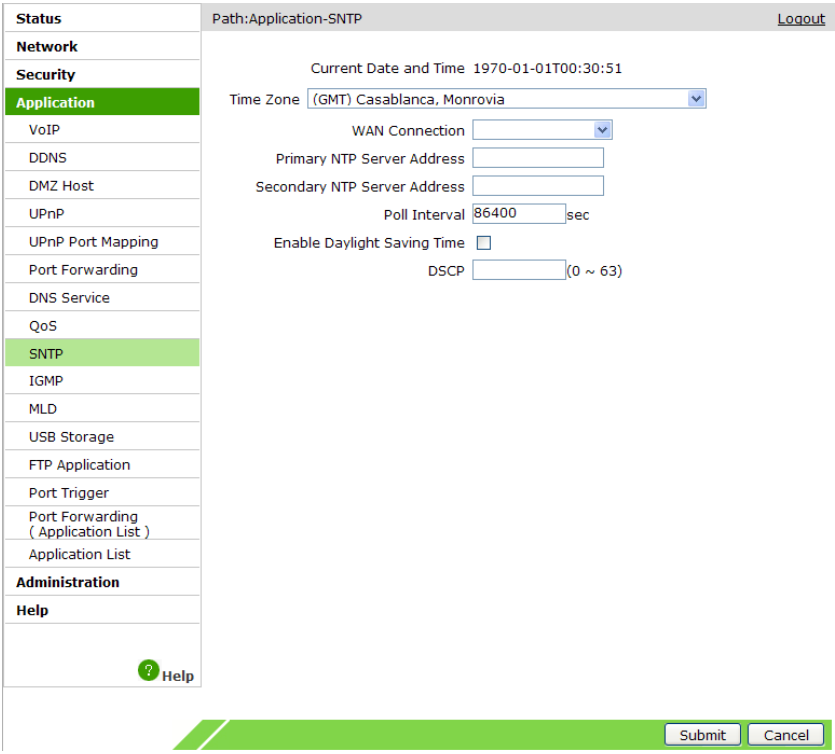


Table 50 lists the SNTP parameters.

Table 50 SNTP Parameters

Parameter	Description
WAN Connection	The configured WAN connection.
Time Zone	Time zone
Primary NTP Server Address	IP address of the primary NTP server

Parameter	Description
Secondary NTP Server Address	IP address of the secondary NTP server
Poll Interval	The time interval that the ZXHN H298N device sends synchronization packets to the NTP server. Unit: second
Enable Daylight Saving Time	Select this check box to enable the daylight saving time.
DSCP	Range: 0–63

3. Click **Submit**.

SNTP is configured.

6.10 IGMP

6.10.1 WAN Connection

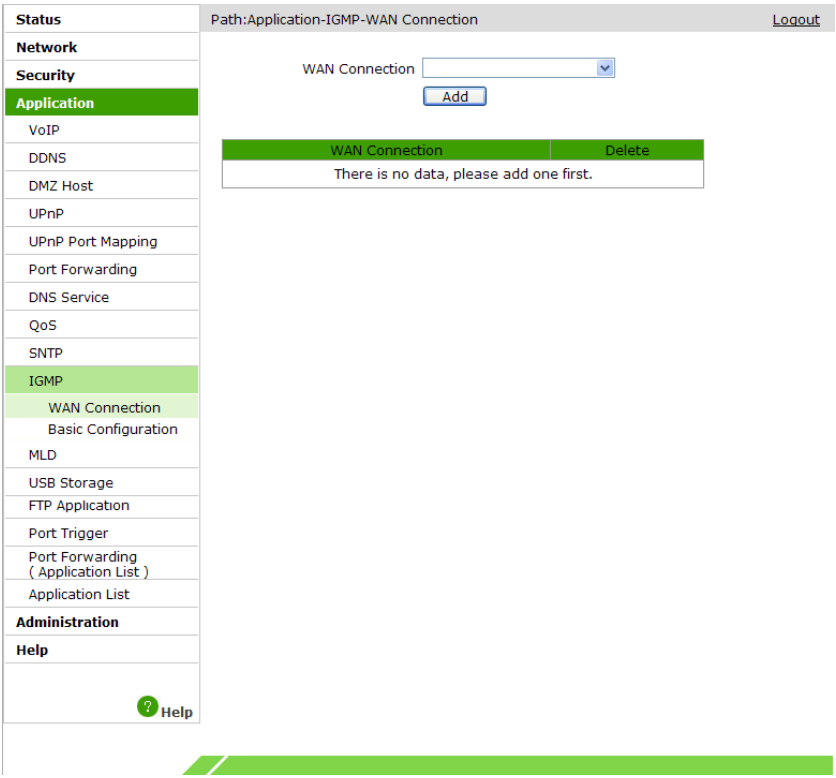
Prerequisite

Before this operation, make sure that the WAN connection configuration is complete.

Steps

1. Choose [**Application→IGMP→ WAN Connection**].
2. Select a WAN connection type in the **WAN Connection** drop-down list, as shown in Figure 77.

Figure 77 WAN Connection



3. Click **Add**.

The WAN connection for IGMP proxy is configured.

6.10.2 Basic Configuration

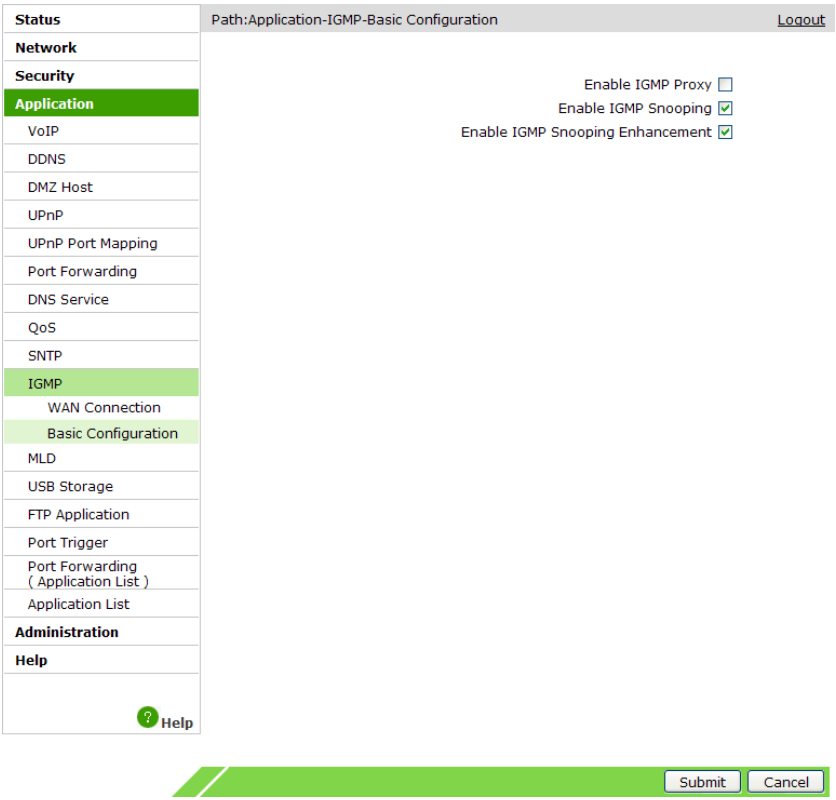
Context

To configure IGMP basic parameters, perform the following steps:

Steps

1. Choose [**Application→ IGMP→ Basic Configuration**].
2. Select **Enable IGMP Proxy**, **Enable IGMP Snooping**, or **Enable IGMP Snooping Enhancement**, as shown in Figure 78.

Figure 78 Basic Configuration



3. Click **Submit**.

IGMP basic parameters are configured.

6.11 MLD

MLD configuration includes the following:

- MLD Snooping
- MLD Proxy

6.11.1 MLD Snooping

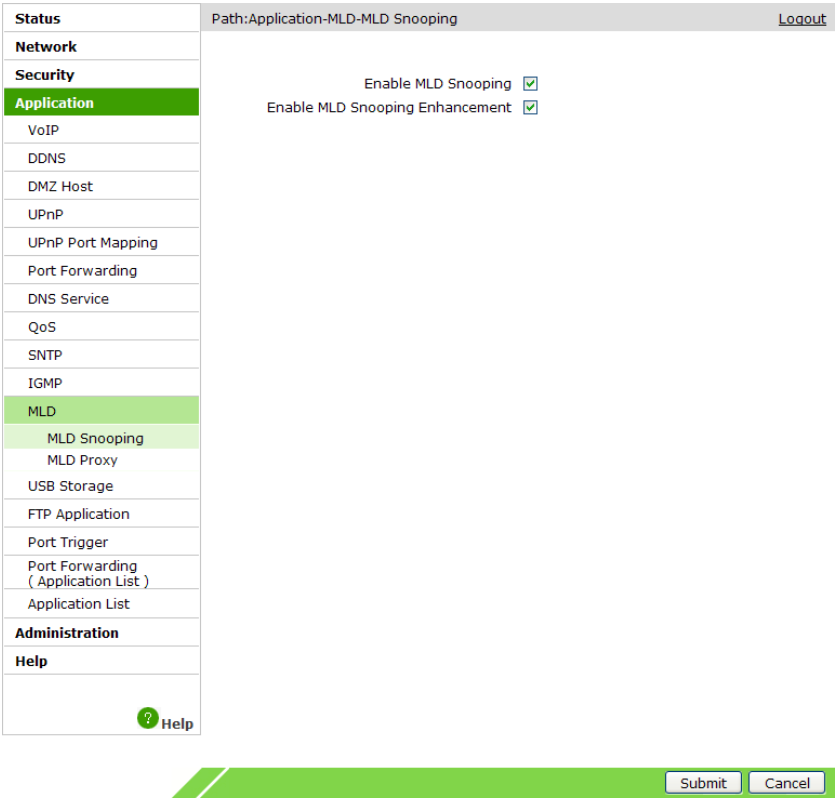
Context

To configure MLD snooping, perform the following steps:

Steps

1. Choose [**Application→MLD→ MLD Snooping**], as shown in Figure 79.

   Figure 79 MLD Snooping



2. Configure the parameters as required.
3. Click **Submit**.

MLD snooping is configured.

6.11.2 MLD Proxy

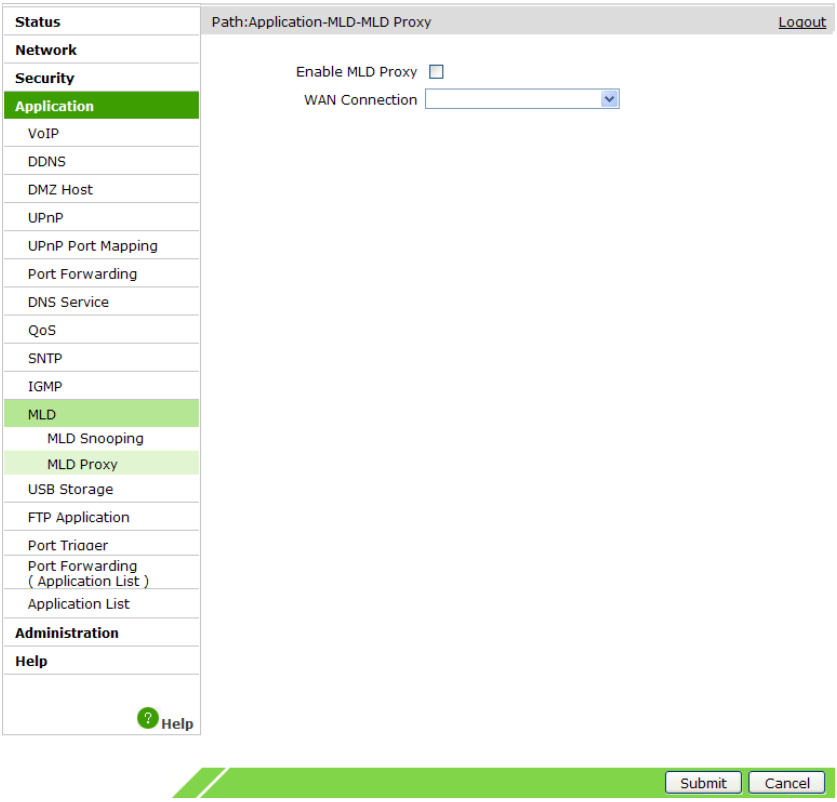
Context

To configure MLD proxy, perform the following steps:

Steps

1. Choose [**Application→ MLD→ MLD Proxy**], as shown in Figure 80.

Figure 80 MLD Proxy



2. Configure the parameters as required.

   The MLD proxy provides the similar functions as the IGMP proxy.

3. Click **Submit**.

MLD proxy is configured.

6.12 USB Storage

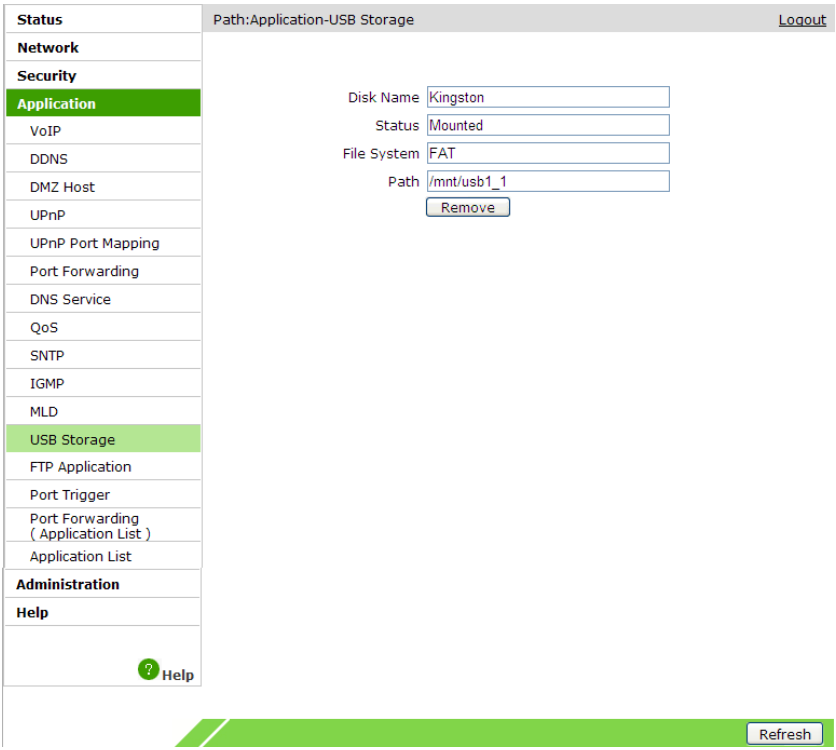
Context

To check the USB storage device information, perform the following steps:

Steps

1. Choose [**Application→ USB Storage**], the USB storage device information is displayed, as shown in Figure 81.

Figure 81 USB Storage



2. Click **Refresh** to refresh the information of the USB storage device.

The USB storage device information is displayed.

6.13 FTP Application

Context

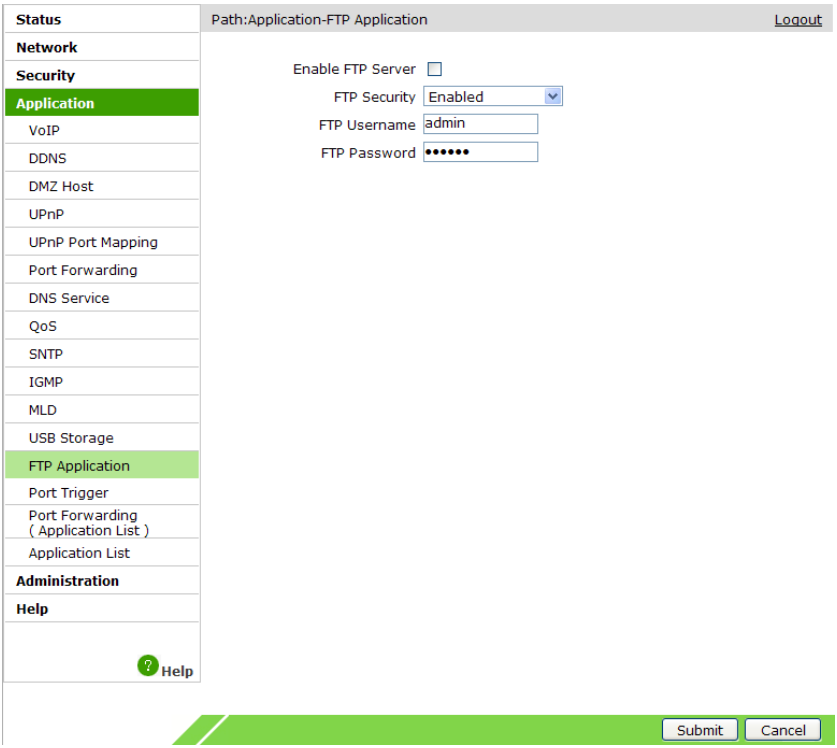
FTP file server requires that a USB storage device is already connected to the ZXHN H298N.

To configure the FTP application, perform the following steps:

Steps

1. Choose [**Application→ FTP Application**], as shown in Figure 82.

Figure 82 FTP Application



2. Configure the parameters as required.

   Table 51 lists the FTP application parameters.

   Table 51 FTP Application Parameters

Parameter	Description
Enable FTP Server	Enable FTP server function.
FTP Security	Enable FTP security.
FTP Username	Username of FTP file server
FTP Password	Password of FTP file server

3. Click **Submit**.

The FTP application is configured.

6.14 Port Trigger

Context

Port triggering is used on the protected ports. The system enables these ports only when port triggering is enabled.

To configure port triggering, perform the following steps:

Steps

1. Choose [**Application→ Port Trigger**].
2. Configure the port trigger parameters, as shown in Figure 83.

Figure 83 Port Trigger

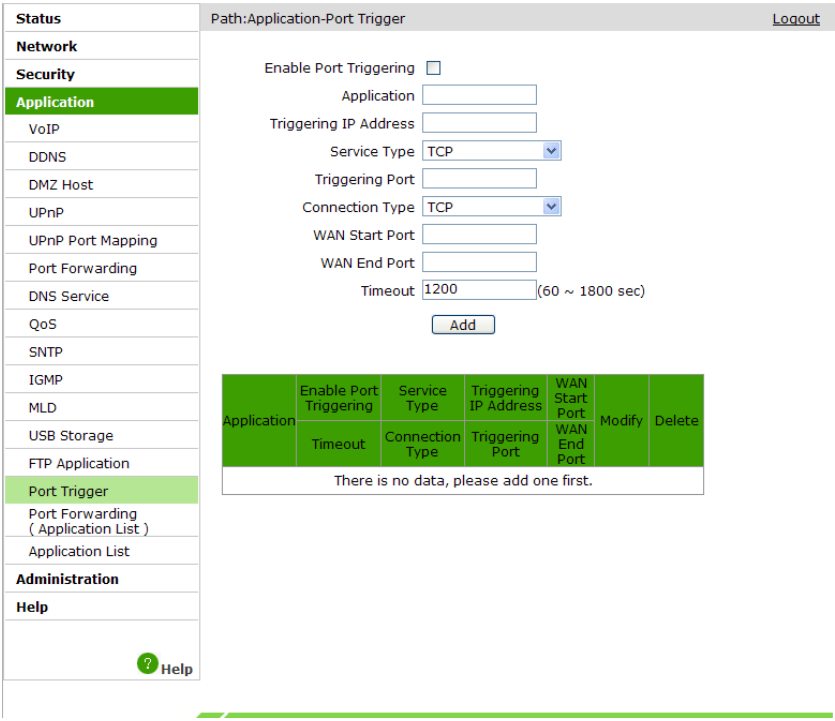


Table 52 lists the port trigger parameters.

Table 52 Port Trigger Parameters

Parameter	Description
Enable Port Triggering	To enable port triggering
Application	Name of the port triggering item
Triggering IP Address	IP address that the device accesses
Service Type	Service type Default: TCP
Triggering Port	Protocol port that the device accesses, which cannot be null
Connection Type	Connection type of the external router Default: TCP
WAN Start Port/End Port	Port range that triggers port mapping, that is, layer-4 port number of the packet Once port triggering is enable, the start port and end port services are enabled. This parameter cannot be null.
Timeout	Triggering timeout

3. Click **Add**.

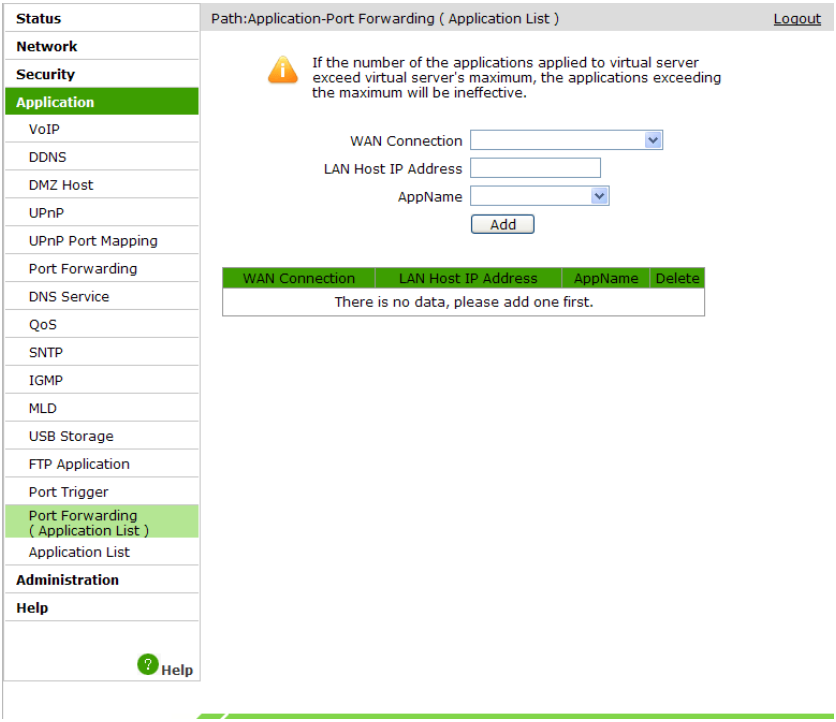
Port triggering is configured.

6.15 Port Forwarding (Application List)

Steps

1. Choose [**Application→ Port Forwarding (Application List)**], as shown in Figure 84.

Figure 84 Port Forwarding



2. Configure the parameters as required.

   Table 53 lists the port forwarding parameters.

   Table 53 Port Forwarding Parameters

Parameter	Description
WAN Connection	WAN connection type.
LAN Host IP Address	IP address of the LAN-side host.
AppName	Username of Application.

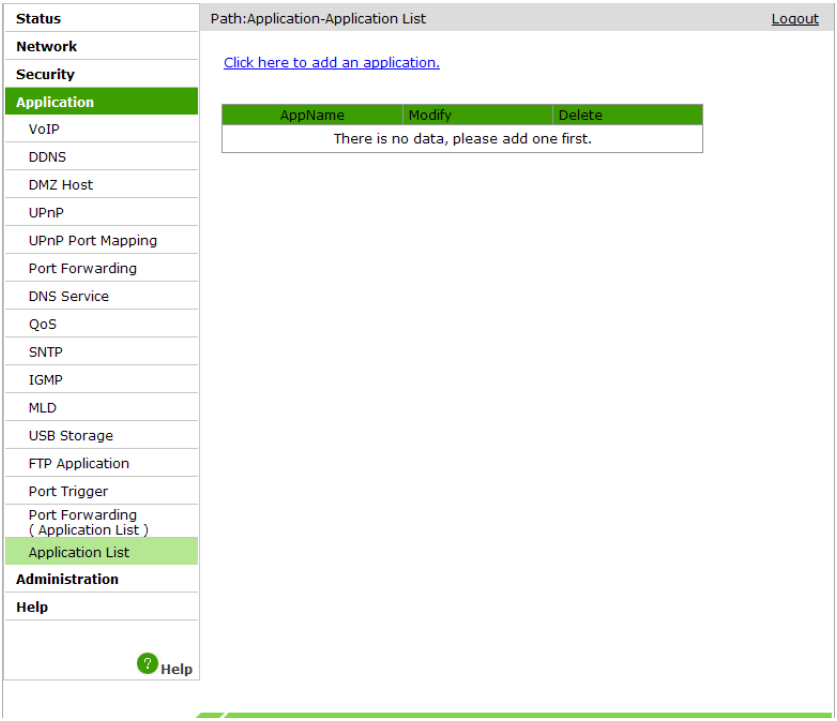
3. Click **Add**.

6.16 Application List

Steps

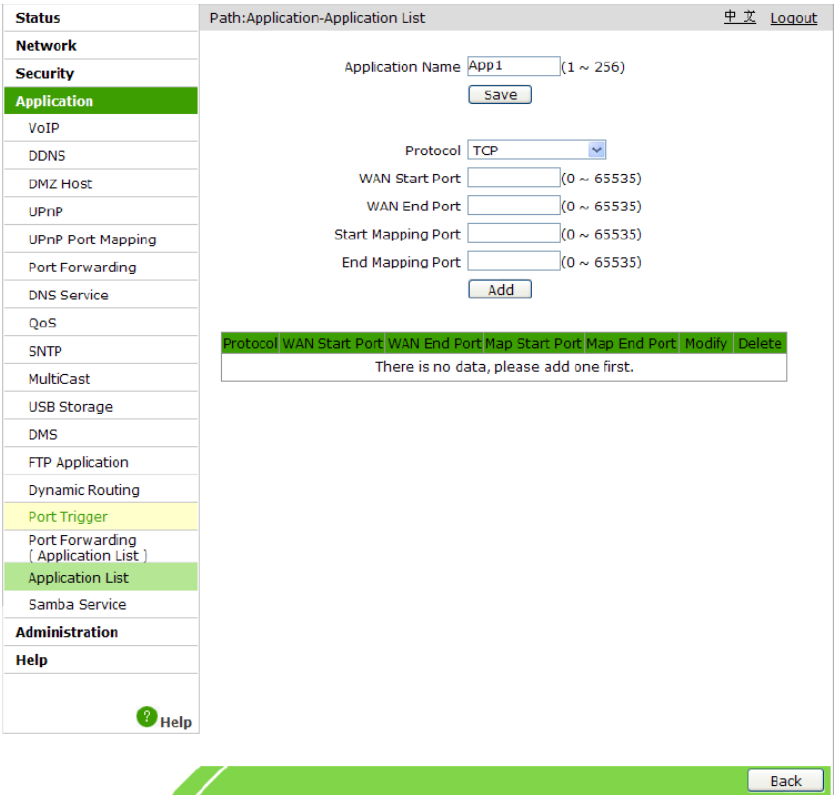
1. Choose [**Application→ Application List**], as shown in Figure 85.

Figure 85 Application List I



2. Click **Click here to add an application**, as shown in Figure 86.

Figure 86 Application List II



3. Configure the parameters as required.

   Table 54 lists the application list parameters.

   Table 54 Application List Parameters

Parameter	Description
Application Name	Username of Application List server.
Protocol	Protocol of the permitted packet. Default: TCP
WAN Start Port/WAN End Port	Port number range of the WAN-side host.
Start Mapping Port/End Mapping Port	Port number range of the Mapping-side host.

4. Click **Add**.

7 Administration

7.1 TR-069

TR-069 configuration includes the following:

- Basic
- Certificate

7.1.1 Basic

Context

TR-069, also known as CPE WAN management protocol, is a NMS protocol carried out by the DSL forum. It manages the terminal devices more effectively.

To configure the basic TR-069 parameters, perform the following steps:

Steps

1. Choose [**Administration→ TR-069→ Basic**].
2. Configure the basic TR-069 parameters, as shown in Figure 87.

Figure 87 Basic TR-069 Configuration

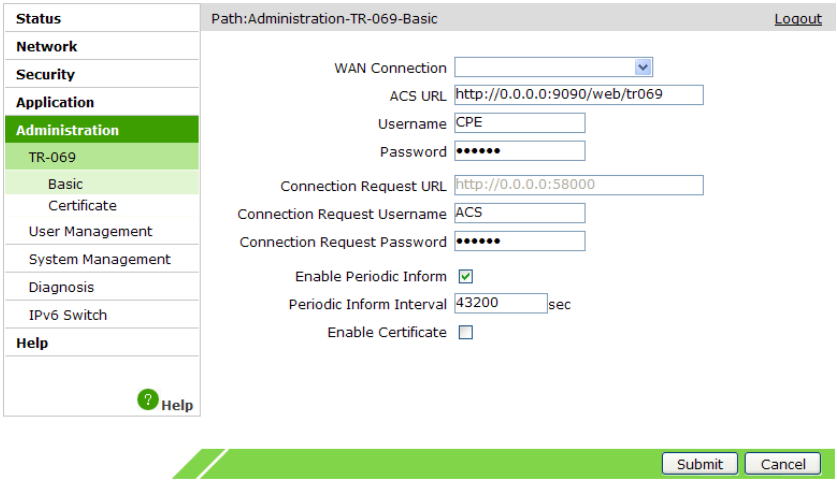


Table 55 lists the basic TR-069 parameters.

Table 55 Basic TR-069 Parameters

Parameter	Description
WAN Connection	The configured WAN connection.
ACS URL	NMS server URL Default: http://0.0.0.0:9090/web/tr069
Username/Password	User name and password for the device to access the NMS server
Connection Request URL	Generated automatically
Connection Request Username/Connection Request Password	User name and password for the NMS server to access the device
Enable Periodic Inform	To enable periodic inform
Periodic Inform Interval	Periodic inform interval of the device
Enable Certificate	To enable TR-069 certificate Configure the certificate through [**Administration**→ **TR-069**→ **Certificate**].

3. Click **Submit**.

The basic TR-069 parameters are configured.

7.1.2 Certificate

Context

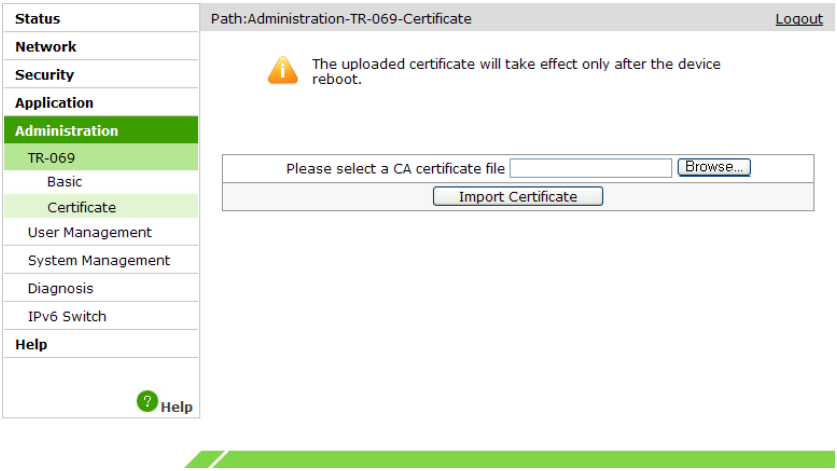
Enable the certificate in [**Administration**→ **TR-069**→ **Basic**].

To configure the CA certificate, perform the following steps:

Steps

1. Choose [**Administration**→ **TR-069**→ **Certificate**].
2. Configure the CA certificate, as shown in Figure 88.

Figure 88 Certificate



3. Click **Browse** to select the CA certificate file.

   Note:

   The CA certificate is provided by the ISP to the terminal user. It is imported from the local.

4. Click **Import Certificate**.

CA certificate is configured.

7.2 User Management

Context

Table 56 lists the user rights.

Table 56 User Rights

Role	User Name and Password	Right
Administrator	User name: admin Password: admin	The administrator has the configuration right on all the parameters.
User	User name: user Password: user	The common user has the following rights: ■ Information view ■ Software upgrade

To manage the user accounts and rights, perform the following steps:

Steps

1. Choose [**Administration→ User Management**].
2. Configure the user management parameters, as shown in Figure 89.

Figure 89 User Management

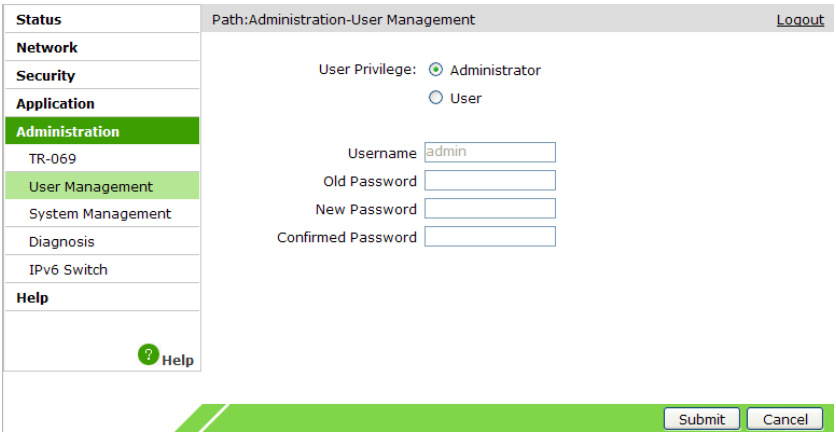


Table 57 lists the user management parameters.

Table 57 User Management Parameters

Parameter	Description
User Privilege	User right includes the right for: ▸ Administrator ▸ User
Username	The default is as follows: ▸ Administrator: admin ▸ User: user
Old Password	The default is as follows: ▸ Administrator: admin ▸ User: user
New Password	User self-defined password
Confirm Password	Consistent with the new password

3. Click **Submit**.

User accounts and rights are configured.

7.3 System Management

System management includes the following:

- System Management
- Software Upgrade
- User Configuration Management
- Default Configuration Management

7.3.1 System Management

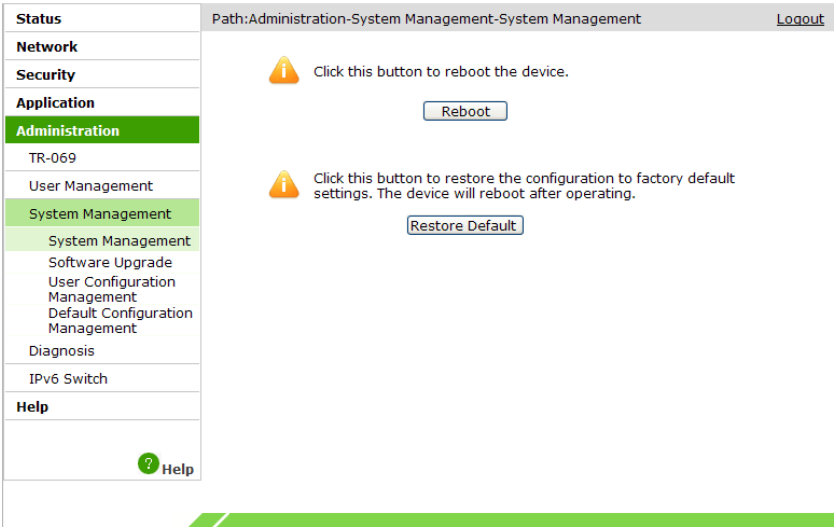
Context

To restart the device or restore the factory default settings, perform the following steps:

Steps

1. Choose [**Administration→ System Management→ System Management**], as shown in Figure 90.

   Figure 90 System Management



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

System management is complete.

7.3.2 Software Upgrade

Prerequisite

Before this operation, make sure that the upgrade file is ready.

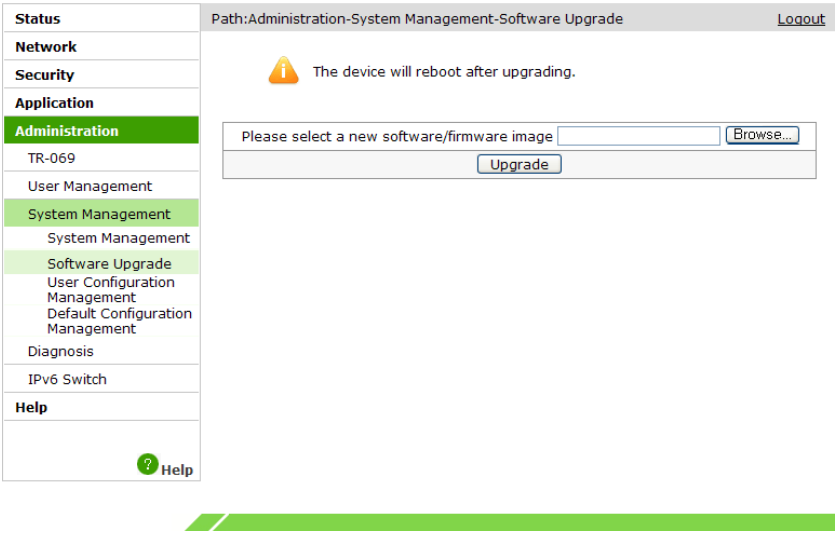
Context

To upgrade the software, perform the following steps:

Steps

1. Choose [**Administration→ System Management→ Software Upgrade**], as shown in Figure 91.

   Figure 91 Software Upgrade



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

   Note:

   The system prompts the upgrade progress. During the upgrade process, do not cut off the power supply. Otherwise, the device may be damaged.

After the software is upgraded, the system is automatically restarted and returns to the login dialog box.

7.3.3 User Configuration Management

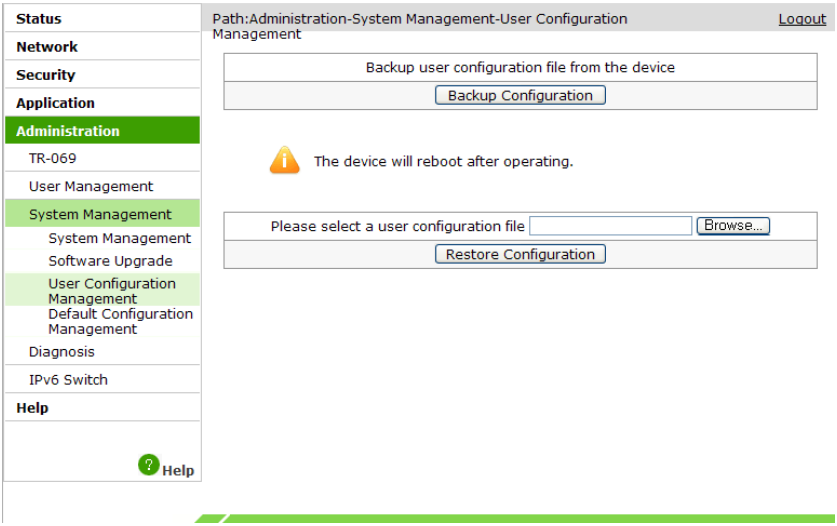
Perform this procedure to import and export the user configuration file.

Before restoring the configuration, it is necessary to back up the user configuration first. Otherwise this operation will not work.

Steps

1. Choose [**Administration→ System Management→ User Configuration Management**], as shown in Figure 92.

   Figure 92 User Configuration Management



2. Click **Backup Configuration** to export the user configuration file.
3. Click **Browse** to select the user configuration file.
4. Click **Restore Configuration** to import the user configuration file.

   NOTE ***Note:***

   After the user configuration file is imported, the system is restarted.

User configuration management is complete.

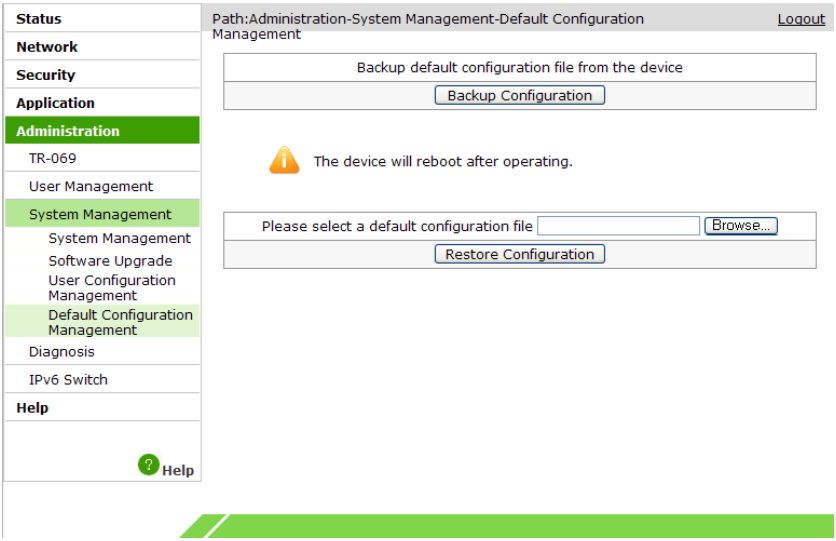
7.3.4 Default Configuration Management

Perform this procedure to import and export the default configuration file.

Steps

1. Choose [**Administration→ System Management→ Default Configuration Management**], as shown in Figure 93.

Figure 93 Default Configuration Management



2. Click **Backup Configuration** to export the default configuration file.
3. Click **Browse** to select the default configuration file.
4. Click **Restore Configuration** to import the default configuration file.

Note:

After the default configuration file is imported, the system is restarted.

7.4 Diagnosis

This section includes the following topics:

- Ping Diagnosis
- Trace Route Diagnosis

7.4.1 Ping Diagnosis

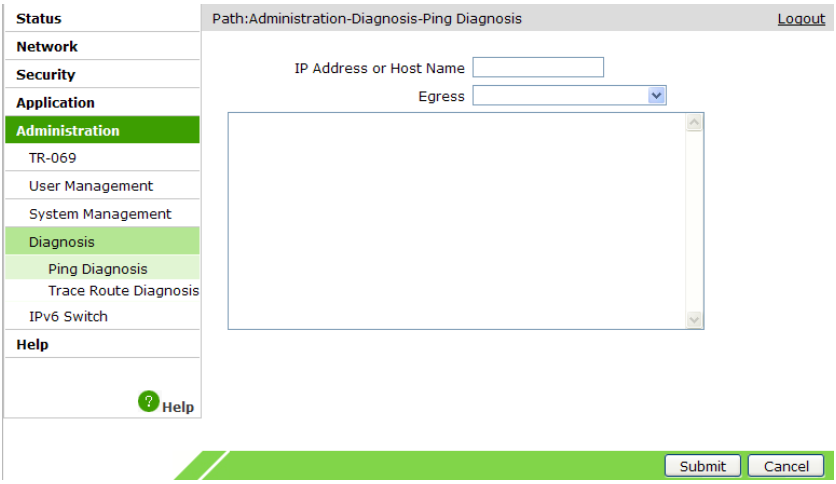
Context

To configure the Ping diagnosis, perform the following steps:

Steps

1. Choose [**Administration→ Diagnosis→ Ping Diagnosis**], as shown in Figure 94.

Figure 94 Ping Diagnosis



2. Type the host IP address or host name in the **IP Address or Host Name** text box, and select the egress from the **Egress** drop-down list.
3. Click **Submit** to diagnose the connection, and the system displays the diagnosis results.

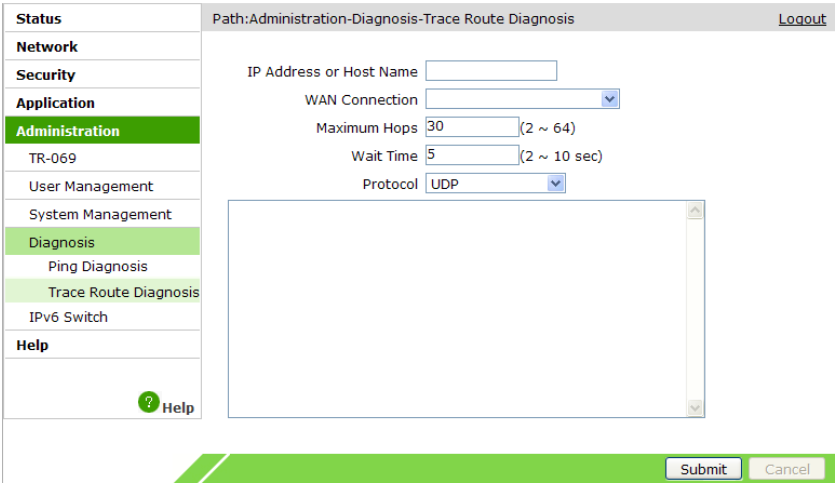
The Ping diagnosis is complete.

7.4.2 Trace Route Diagnosis

Steps

1. Choose [**Administration**→ **Diagnosis**→ **Trace Route Diagnosis**], as shown in Figure 95.

Figure 95 Trace Route Diagnosis



2. Type an IP address or a host name in the **IP Address or Host Name** text box, and select the configured WAN connection.
3. Click **Submit** and the system displays the results.

The trace route diagnosis is complete.

7.5 IPv6 Switch

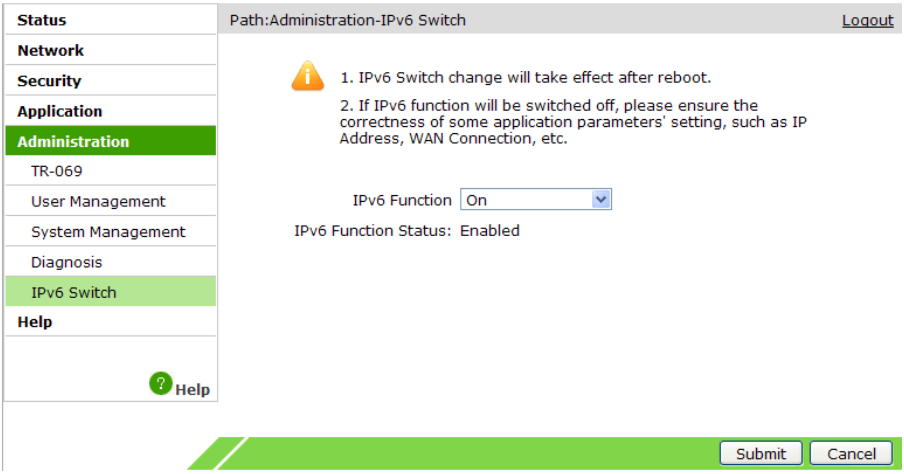
This procedure introduces how to switch on/off the IPv6 function.

The IPv6 function of the ZXHN H298N device is enabled by default.

Steps

1. On the navigation tree, click [**Administration→IPv6 Switch**]. The IPv6 switch page is displayed, as shown in Figure 96.

Figure 96 IPv6 Switch



2. Select On or Off from the **IPv6 Function** drop-down list to enable or disable the IPv6 function.
3. After the configuration, click **Submit** button to submit the change.

Glossary

AC - Alternating Current

ACL - Access Control List

ADSL - Asymmetric Digital Subscriber Line

ALG - Application Level Gateway

ARP - Address Resolution Protocol

CA - Certificate Authentication

CHAP - Challenge Handshake Authentication Protocol

CPE - Customer Premises Equipment

DC - Direct Current

DDNS - Dynamic Domain Name Server

DHCP - Dynamic Host Configuration Protocol

DMS - Digital Media Server

DMZ - Demilitarized Zone

DNS - Domain Name Server

DNS - Domain Name System

DSCP - Differentiated Services Code Point

DSL - Digital Subscriber Line

DTMF - Dual-Tone Multi-Frequency

FTP - File Transfer Protocol

GE - Gigabit Ethernet

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IGMP - Internet Group Management Protocol

IP - Internet Protocol

IPv4 - Internet Protocol version 4

IPv6 - Internet Protocol Version 6

ISP - Internet Service Provider

LAN - Local Area Network

MAC - Medium Access Control

MLD - Multicast Listener Discovery

MTU - Maximum Transfer Unit

NAT - Network Address Translation

NMS - Network Management System

NTP - Network Time Protocol

PAP - Password Authentication Protocol

PBB - Provider Backbone Bridge

PBDE - Polybrominated Biphenyl Ether

PPPoA - Point to Point Protocol over ATM

PPPoE - Point to Point Protocol over Ethernet

PSK - PreShared Key

QoS - Quality of Service

SIP - Session Initiation Protocol

SNTP - Simple Network Time Protocol

TCP - Transfer Control Protocol

TCP/IP - Transmission Control Protocol/Internet Protocol

TTL - Time To Live

UDP - User Datagram Protocol

UPnP - Universal Plug and Play

URL - Uniform Resource Locator

USB - Universal Serial Bus

VLAN - Virtual Local Area Network

VoIP - Voice over Internet Protocol

WAN - Wide Access Network

WAN - Wide Area Network

WEP - Wired Equivalent Privacy

WLAN - Wireless Local Area Network

WPA - Wi-Fi Protected Access