ZXHN H108N
Home Gateway
Maintenance Management Manual

Version: V2.5

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

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2013–08–28	First release.

Serial No. SJ-20130716160034-002

Publishing Date: 2013–08–28(R1.0)

About This Manual

Purpose

This manual describes how to configure and maintain the ZXHN H108N device.

Intended Audience

This document is intended for:

- Network planning engineers
- Installation debugging engineers
- On-site maintenance engineers
- System maintenance engineers
- Data configuration engineers

What Is in This Manual

This manual contains the following chapters:

Chapter	Summary
1, Safety Precautions	Describes the safety precautions for the device operation.
2, Overview	Describes the product features and technical specifications.
3, Configuration Preparation	Describes the TCP/IP configuration and login procedure.
4, Status	Describes how to view the device status.
5, Quick Setup	Describes how to quick setup the device.
6, Network	Describes the WAN configuration, VLAN configuration, LAN configuration, IPv4 routing configuration, and IPv6 routing configuration.
7, Security	Describes the configuration of the firewall, IP filter, MAC filter, URL filter, service control, and ALG.

Chapter	Summary
8, Application	Describes the configuration of DDNS, DMZ, UPnP, port forwarding, DNS, QoS, SNTP, IGMP, MLD, USB storage, FTP application, port trigger, and application list.
9, Administration	Describes the configuration of TR-069, user management, login timeout, system management, log management, mobile network management, system diagnosis, WAN type, and IPv6 switch.

Conventions

This manual uses the following typographical conventions:

Typeface	Meaning
	Caution: indicates a potentially hazardous situation. Failure to comply can result in moderate injury, equipment damage, or interruption of minor services.
	Note: provides additional information about a certain topic.

Declaration of RoHS Compliance

To minimize environmental impacts and take more responsibilities to the earth we live on, this document shall serve as a formal declaration that the ZXHN H108N 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 (PBBs)
- PolyBrominated Diphenyl Ethers (PBDEs)

The ZXHN H108N 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.

1 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.

2 Overview

2.1 Product Introduction

The ZXHN H108N is an ADSL subscriber access device. The ZXHN H108N provides the broadband Internet service and enterprise network access service through the high-speed ADSL or 3G wireless access mode. The ZXHN H108N provides four 10/100Base-T Ethernet user interfaces and the wireless access function that complies with the IEEE 802.11b/g/n standard.

2.2 Product Features

The ZXHN H108N has the following features:

- Four 10 Mbps/100 Mbps Ethernet interfaces
- Network configuration through friendly GUI and TR-069.
- DHCP server functions
- Compatible with all the Internet standard applications
- Standard and compatible DSL interface
- Virtual server, IP address filter, and DMZ function
- System configuration in web mode
- Software upgrade
- Three upstream modes: ADSL, Ethernet, and 3G
- PPPoE, IPoE, and Static IP sessions, supporting up to eight sessions totally
- NAT protocol
- Wireless LAN IEEE 802.11b, 802.11g, and 802.11n protocols

2.3 Technical Specifications

Table 1 lists the ZXHN H108N technical specifications.

Table 1 Technical Specifications

Item	**Specification**
Dimensions	105 mm (height) ×108 mm (width) × 52 mm (depth)
Rated current	▯ Home Gateway with USB port: 1 A ▯ Home Gateway without USB port: 500 mA
Rated voltage	12 V DC
Working temperature	0 ℃ ~ 40 ℃ (32 °F~104 °F)
Working humidity	20% ~ 90%
Storage temperature	20 ℃ ~ 70 ℃
Storage humidity	5% ~ 95%

3 Configuration Preparation

3.1 Configuring TCP/IP

This procedure introduces how to configure TCP/IP for the ZXHN H108N device configuration.

Context

To ensure that the ZXHN H108N device accesses the ZXHN H108N successfully, configure the computer address in the same network segment as the ZXHN H108N address.

The default network settings for the ZXHN H108N are as follows:

- IP address: 192.168.1.254
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.254

Steps

1. Configure TCP/IP.
   i. In **Local Area Connection Properties** dialog box, 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**. For example, set the IP address to 192.168.1.7, the subnet mask to 255.255.255.0, and the default gateway to 192.168.1.1.
   iv. Click **OK**.

   NOTE ***Note:***

   The settings may 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 ZXHN H108N device.

   If pinging the device fails, verify the following:

   - The Ethernet cable between the ZXHN H108N device and the computer is not correctly connected.
   - The ZXHN H108N device is not powered on.

- The network adapter driver is not correctly installed on the computer.
- The TCP/IP settings on the computer are not correctly configured.

3.2 Logging In to the ZXHN H108N Device

This procedure introduces how to log in to the ZXHN H108N device by using the web browser.

Prerequisite

Before logging in to the ZXHN H108N device, make sure that:

- The computer is correctly connected to the ZXHN H108N device.
- The TCP/IP settings of the computer are configured correctly.

Context

The ZXHN H108N 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 2.

Table 2 User Rights

Role	User Name and Password	Rights
Administrator	User name: admin Password: admin	The administrator has the privileges to configure all the parameters in the Web configuration pages.
User	User name: user Password: user	The common user can only perform the following operation: - View the device or network information - Software upgrade - Modify the user name and password

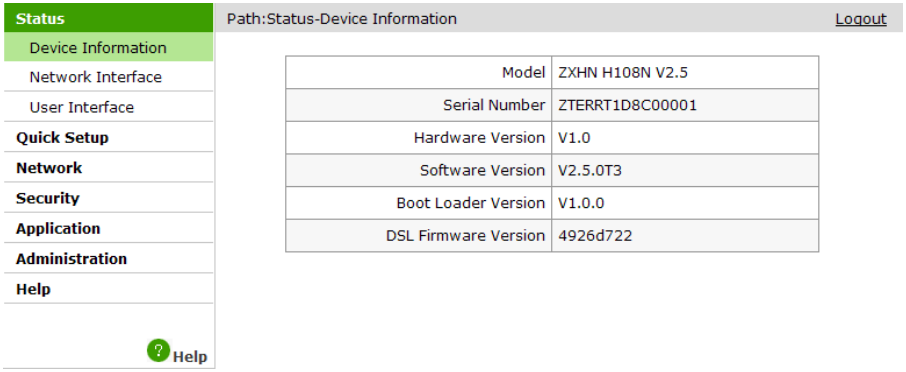
Steps

1. Open the Internet Explorer.
2. Type `http://192.168.1.254` in the address bar and press the **Enter** key. The login page is displayed, see Figure 1.

Figure 1 Login

3. In the **Username** and **Password** text boxes, type the user name and password (by default, both are `admin`). Click **Login**. The default home window is displayed, see Figure 2. On the left navigation tree, click to perform the corresponding configurations.

Figure 2 Home Page



Note:

The Web configuration pages may vary with the software versions. The configuration pages for the administrator and user accounts are different. The administrator account is used as an example in this manual.

4 Status

The relevant information of ZXHN H108N status shown as below.

- On the main page of the ZXHN H108N, select [**Status→Device Information**] to view the Device Information.
- On the main page of the ZXHN H108N, select [**Status→Network Interface**] to view the Network Interface Information, including **WAN Connection**, **3G Connection**, **4in6 Tunnel Connection**, **6in4 Tunnel Connection**, **Mobile Network** and **ADSL**.
- On the main page of the ZXHN H108N, select [**Status→User Interface**] to view the User Interface Information, including **WLAN**, **Etherent**, and **USB**.

5 Quick Setup

Steps

1. On the navigation tree, click **Quick Setup** to open the **Quick Setup** page as show in Figure 3.

Figure 3 Quick Setup

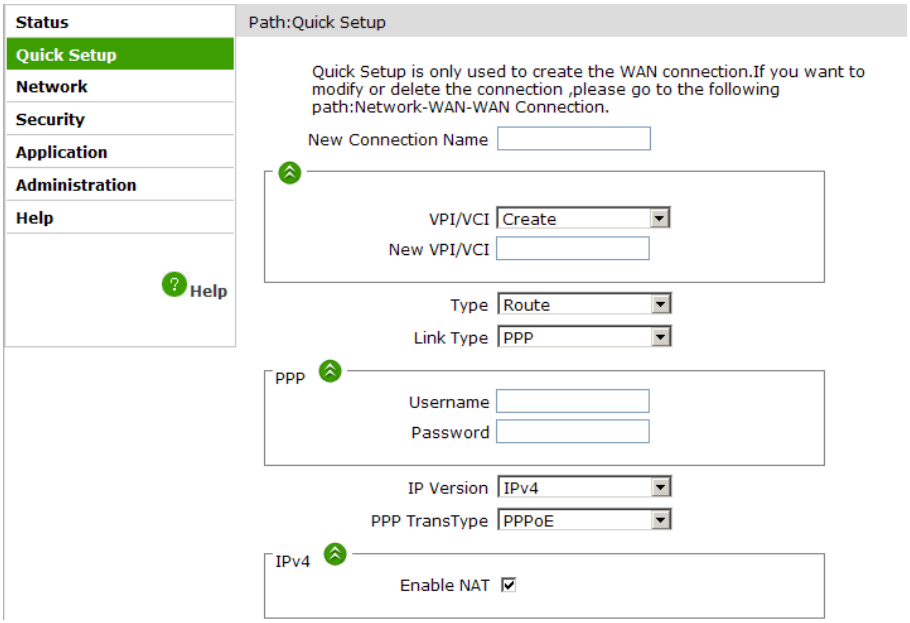


Table 3 describes the parameters for quick setup.

Table 3 The parameters for quick setup

Parameter	Description
New Connection Name	Specify the name of the new WAN connection.
VPI/VCI	Channel number of the ATM cell. Each ADSL port has eight PVCs, which can be configured with different VPIs and VCIs. This should be consistent with the port configuration on the NE.
New VPI/VCI	Create a VPI/VCI.

Parameter	Description
Type	There are two connection type: ▯ Route ▯ Bridge Connection
Link Type	There are two link types: ▯ PPP ▯ IP
Username/Password	PPP username/password provided by the ISP.
IP Version	The IP version includes: ▯ IPv4 ▯ IPv6 ▯ IPv4/v6
IP Type	There are three IP types: ▯ Static ▯ DHCP ▯ IPoA
PPP TransType	PPPoE or PPPoA.
Enable NAT	When multiple computers in a LAN share one IP address to access the Internet, NAT is used to transfer the private network address to the public network address of the WAN port.
IP Address	The IP address provided by the ISP.
Subnet Mask	The subnet mask provided by the ISP.
Gateway	The gateway address provided by the ISP.
DNS Server1 IP Address~DNS Server3 IP Address	The DNS address provided by the ISP.
IPv6 Info Get Mode	The IPv6 Info Get Mode includes: ▯ Auto Mode ▯ Manual Mode

Parameter	Description
GUA From	The GUA From includes: ▯ DHCPv6 ▯ Static ▯ SLAAC
GateWay From	The GateWay From includes: ▯ SLAAC ▯ Static
DNSv6 From	The DNSv6 From includes: ▯ DHCPv6 ▯ Static ▯ SLAAC
Prefix Delegation	Enable the Prefix Delegation.
Prefix Delegation for Allocation Address	Enable the Prefix Delegation for Allocation Address.

2. Specify the WAN connection parameters as required.

▯ To setup a bridge WAN connection, perform the following steps.

a) Select **Bridge Connection** from the **Type** drop-down list

b) Specify other parameters as required, and then click **Next**.

▯ To setup a PPPoE connection, perform the following steps.

a) Select **Route** from the **Type** drop-down list.

b) Select **PPP** from the **Link Type** drop-down list.

c) Type the user name and password in the **PPP** area

d) Select **PPPoE** from the **PPP TransType** drop-down list.

e) Specify other parameters as required, and then click **Next**.

▯ To setup a PPPoA connection, perform the following steps.

a) Select **Route** from the **Type** drop-down list.

b) Select **PPP** from the **Link Type** drop-down list.

c) Type the user name and password in the **PPP** area

d) Select **PPPoA** from the **PPP TransType** drop-down list.

e) Specify other parameters as required, and then click **Next**.

- To setup a static connection, perform the following steps.

  IPv4 static connection is used as an example.

  a) Select **Route** from the **Type** drop-down list.

  b) Select **IP** from the **Link Type** drop-down list.

  c) Select **Static** from the **IP Type** drop-down list.

  d) Specify the IP address, subnet mask, gateway, and DNS server in the **IPv4** area.

  e) Specify other parameters as required, and then click **Next**.

3. Click **Next** to open the page, as show in Figure 4.

Figure 4 WiFi Configuration

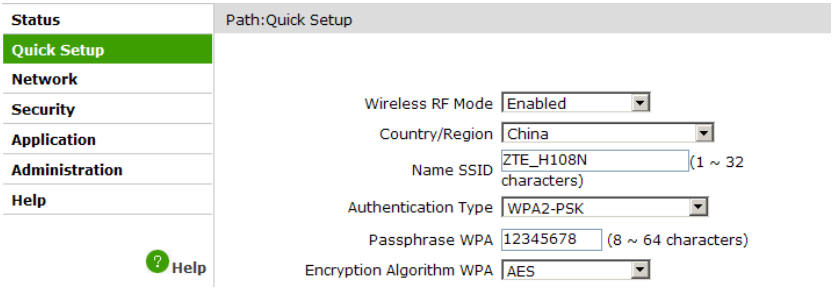


Table 4 describes the parameters for WiFi configuration.

Table 4 WiFi Configuration

Parameter	Description
Wireless RF Mode	Select **Enabled** to enable the wireless RF function.
Country/Region	Select the country or region.
Name SSID	Specify the SSID name.
Authentication Type	Select the authentication type. The provides the following access authentication modes: Open System: Authentication is not needed. Any client with a wireless network card can connect to the wireless access point. 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 it is securer. The data is encrypted before transmission. WPA2-PSK: It is the second version of WPA-PSK.

Parameter	Description
	▯ WPA/WPA2-PSK: It is a hybrid authentication mode.
Passphrase WPA	Range: 8 ~ 64 characters
Encryption Algorithm WPA	There are three options: ▯ TKIP:Temporal Key Integrity Protocol ▯ AES: Advanced Encryption Standard ▯ TKIP+AES: Adaptive encryption algorithm
WEP Encryption	**Enable**/**Disable** WEP Encryption.
WEP Encryption Level	The value can be **64bit** or **128bit**.
WEP Key Index	The WEP authentication provides four keys.
WEP Key	Use 5 ASCII characters or 10 hexadecimal digits to specify the WEP value for the 64 bit WEP encryption. Use 13 ASCII characters or 26 hexadecimal digits to specify the WEP value for the 128 bit WEP encryption.

4. Click **Next** to open the **User Configuration** page, as show in Figure 5.

Figure 5 User Configuration

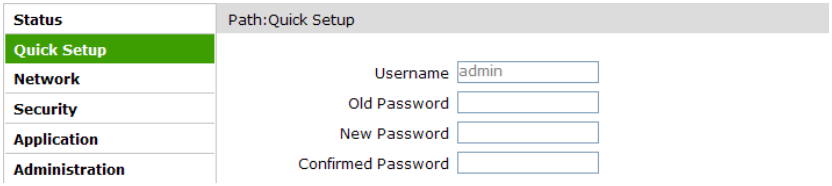


Table 5 describes the parameters for User configuration.

Table 5 User Configuration

Parameter	Description
Old Password	Input the old password of **admin**.
New Password	Specify the new password.
Confirmed Password	Confirm the new password.

5. Click **Next**, then click **Finish** to finish quick setup.

6 Network

6.1 WAN

This section includes the following:

- Configuring WAN Connection
- Configuring 3G Connection
- Configuring 4in6 Tunnel Connection
- Configuring 6in4 Tunnel Connection
- Configuring Port Binding
- Configuring ADSL Modulation

6.1.1 Configuring WAN Connection

This procedure introduces how to configure the WAN connection.

Context

The ZXHN H108N supports the following ADSL connection types:

- PPPoE
- PPPoA
- Static
- DHCP
- IPoA
- Bridge

The ZXHN H108N supports eight WAN connections.

Steps

1. On the navigation tree, click [**Network→ WAN→ WAN Connection**]. The WAN connection configuration page is displayed, see Figure 6.

Figure 6 WAN Connection

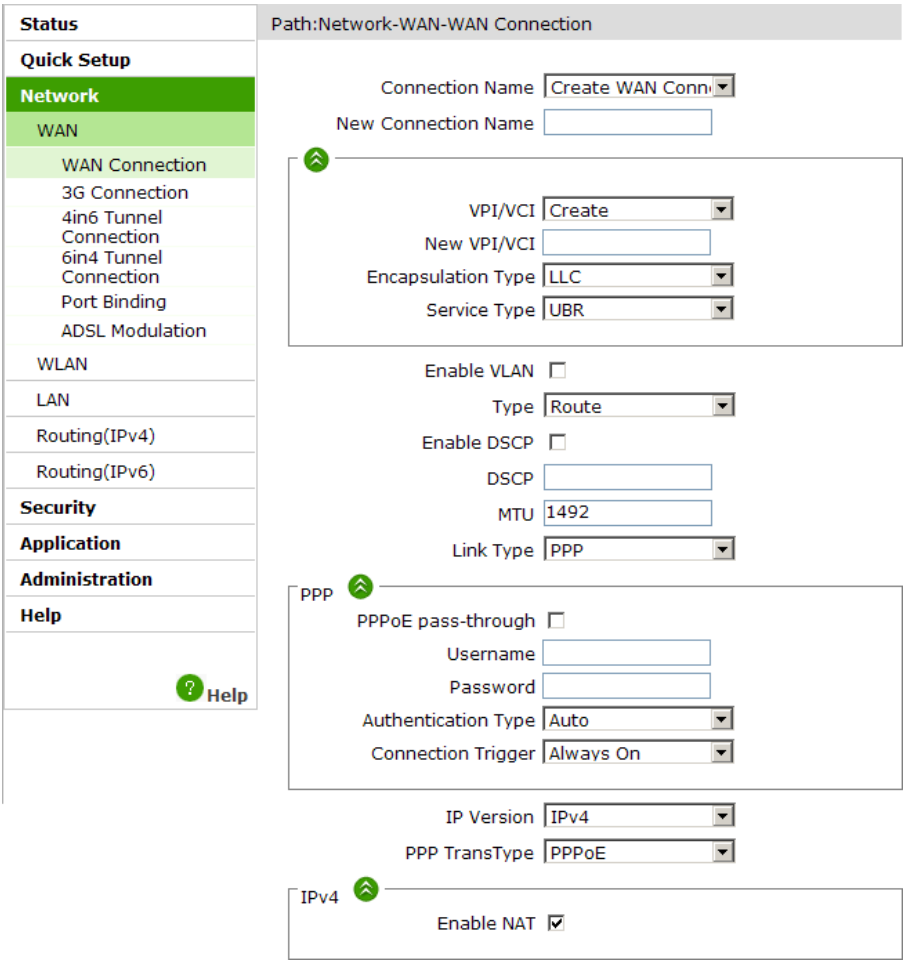


Table 6 describes the parameters for creating a new WAN connection.

Table 6 Parameters for Creating a New WAN Connection

Parameter	Description
Connection Name	The default is **Create WAN Connection**. Before creating a new connection, make sure the **Create WAN Connection** option is selected.
New Connection Name	Specify the name of the new WAN connection.

Parameter	Description
VPI/VCI	Channel number of the ATM cell Each ADSL port has eight PVCs, which can be configured with different VPIs and VCIs. This should be consistent with the port configuration on the NE.
New VPI/VCI	Create a VPI/VCI.
Encapsulation Type	Encapsulation type of the IP packets By default, it is LLC.
Service Type	Define the bit rate.
Enable VLAN	Enable the VLAN function.
VLAN ID	VLAN ID
802.1p	Specify the 802.1p value to modify the service priority. Range: 0~7
Type	Connection type ▯ Route ▯ Bridge Connection
Enable DSCP	This function is used together with the QoS function.
DSCP	Range: 0~63
MTU	Define the maximum transfer unit.
Link Type	There are two link types: ▯ PPP ▯ IP
Username	PPP user name provided by the ISP
Password	PPP password 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: The device will automatically dial up after the device is powered ON or the WAN connection is disconnected. ▯ On Demand: The device will dial up if there are data transmission requests and the WAN connection will be automatically disconnected after the WAN connection is idle for some time. ▯ Manual: The user manually dials up

Parameter	Description
IP Version	The IP version includes: ▯ IPv4 ▯ IPv6 ▯ IPv4/v6
PPP TransType	PPPoE or PPPoA
Enable NAT	When multiple computers in a LAN share one IP address to access the Internet, NAT is used to transfer the private network address to the public network address of the WAN port.
IP Address	The IP address provided by the ISP
Subnet Mask	The subnet mask provided by the ISP
Gateway	The gateway address provided by the ISP
DNS Server1 IP Address~DNS Server4 IP Address	The DNS address provided by the ISP
IPv6 Info Get Mode	The IPv6 Info Get Mode includes: ▯ Auto Mode ▯ Manual Mode
GUA From	The GUA From includes: ▯ SLAAC ▯ DHCPv6 ▯ Static
GateWay From	The GateWay From includes: ▯ SLAAC ▯ Static
DNSv6 From	The DNSv6 From includes: ▯ SLAAC ▯ DHCPv6 ▯ Static
Prefix Delegation	Enable the Prefix Delegation.
Prefix Delegation for Allocation Address	Enable the Prefix Delegation for Allocation Address.

2. Specify the WAN connection parameters as required.

- To setup a bridge WAN connection, perform the following steps.
  a) Select **Bridge Connection** from the **Type** drop-down list
  b) Specify other parameters as required, and then click **Next**.
- To setup a PPPoE connection, perform the following steps.
  a) Select **Route** from the **Type** drop-down list.
  b) Select **PPP** from the **Link Type** drop-down list.
  c) Type the user name and password in the **PPP** area
  d) Select **PPPoE** from the **PPP TransType** drop-down list.
  e) Specify other parameters as required, and then click **Next**.
- To setup a PPPoA connection, perform the following steps.
  a) Select **Route** from the **Type** drop-down list.
  b) Select **PPP** from the **Link Type** drop-down list.
  c) Type the user name and password in the **PPP** area
  d) Select **PPPoA** from the **PPP TransType** drop-down list.
  e) Specify other parameters as required, and then click **Next**.
- To setup a static connection, perform the following steps.

  IPv4 static connection is used as an example.
  a) Select **Route** from the **Type** drop-down list.
  b) Select **IP** from the **Link Type** drop-down list.
  c) Select **Static** from the **IP Type** drop-down list.
  d) Specify the IP address, subnet mask, gateway, and DNS server in the **IPv4** area.
  e) Specify other parameters as required, and then click **Next**.
- To setup an IPoA connection, perform the following steps.
  a) Select **Route** from the **Type** drop-down list.
  b) Select **IP** from the **Link Type** drop-down list.
  c) Select **DHCP** from the **IP Type** drop-down list.
  d) Specify other parameters as required, and then click **Next**.

A WAN connection is created.

The newly-created ADSL WAN connection is displayed in the **Connection Name** drop-down list.

6.1.2 Configuring 3G WAN Connection

The ZXHN H108N device supports 3G WAN connection by using the 3G USB network card. This procedure introduces how to configure the 3G WAN connection

Context

The ZXHN H108N device supports 3G WAN connection by using the 3G USB network card.

The ZXHN H108N supports eight WAN connections at most.

Steps

1. On the navigation tree, click [**Network→ WAN→ 3G Connection**]. The 3G WAN connection configuration page is displayed, as shown in Figure 7.

Figure 7 3G WAN Connection

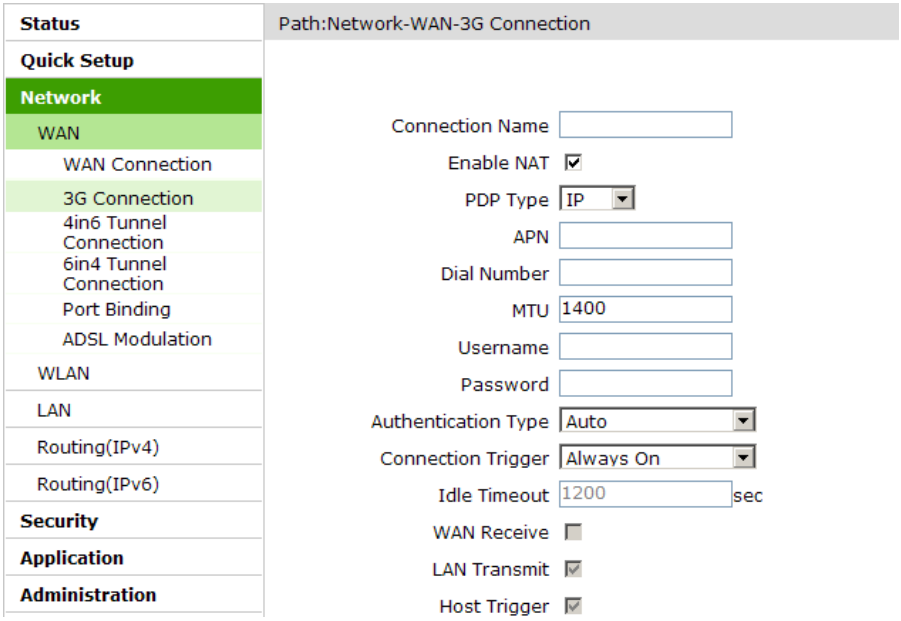


Table 7 describes the parameters for creating a new 3G WAN connection.

Table 7 3G WAN Connection Parameters

Parameter	Description
Connection Name	3G WAN connection name
Enable NAT	When multiple computers in a LAN share one IP address to access the Internet, NAT is used to transfer the private network address to the public network address of the WAN port.

Parameter	Description
PDP Type	There are two options: **IP** and **PPP**.
APN	Access point name, provided by the ISP
Dial Number	Dial number, provided by the ISP
MTU	Define the maximum transfer unit.
Username	User name provided by the ISP
Password	Password provided by the ISP
Authentication Type	There are three options: Auto, PAP and CHAP. By default, it is **Auto**. The authentication type should be the same as the authentication type for the upper-layer device.
Connection Trigger	There are three connection trigger modes: **Always On**: The device will automatically dial up after the device is powered ON or the WAN connection is disconnected. **On Demand**: The device will dial up if there are data transmission requests and the WAN connection will be automatically disconnected after the WAN connection is idle for some time. **Manual**: The user manually dials up
Idle Timeout	Idle time before the dial-up auto disconnection, available only in **On Demand** mode
WAN Receive	Launch the 3G connection if there is inbound traffic on the WAN side.
LAN Transmit	Launch the 3G connection if there is outbound traffic on the LAN side.
Host Trigger	The host triggers the 3G connection.

2. Specify the 3G connection name, and configure the other parameters.
3. After the configuration, click **Create**.

6.1.3 Configuring 4in6 Tunnel Connection

ZXHN H108N supports supports Dual–stack lite technology. DS lite technology allows the device to encapsulate the IPv4 packets inside IPv6 packets and send the IPv6 packets to the ISP's Carrier Grade NAT through its IPv6 WAN connection. The Carrier Grade NAT decapsulates the IPv6 packets, and then restores the original IPv4 packet. And then NAT is performed upon the IPv4 packet and is routed to the public IPv4 Internet.

This procedure introduces how to configure the 4in6 tunnel connection of DS lite type.

Prerequisite

The IPv6 WAN connection has been created.

Steps

1. On the navigation tree, [**Network→ WAN→4in6 Tunnel Connection**]. The 4in6 tunnel connection page is displayed, see Figure 8.

   Figure 8 4in6 Tunnel Connection

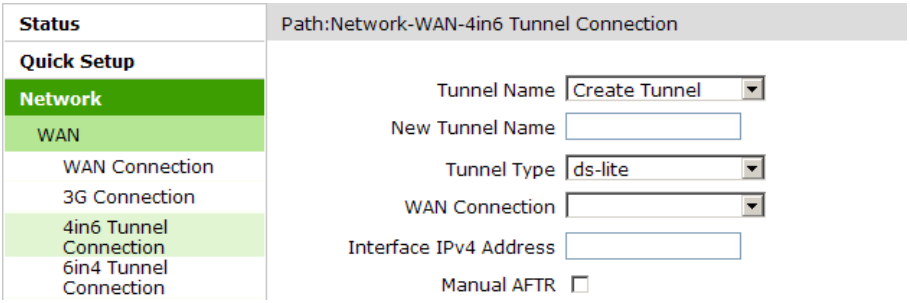


   Table 8 lists the 4in6 tunnel connection parameters.

   Table 8 4in6 Tunnel Connection Parameter

Parameter	Description
Tunnel Name	The default is **Create Tunnel**. Before creating a new tunnel name, make sure the **Create Tunnel** option is selected.
New Tunnel Name	Specify the new tunnel name.
Tunnel Type	At present, only **ds-lite** is supported.
WAN Connection	Select the IPv6 WAN connection that have been created.
Interface IPv4 Address	Range: `192.0.0.2` ~`192.0.0.6`
Manual AFTR	Select this option to manually specify the IPv6 address of the Carrier Grade NAT.

2. Specify the parameters according to the request, and then click **Create**.

6.1.4 Configuring 6in4 Tunnel Connection

This procedure introduces how to configure 6in4 tunnel connection.

Prerequisite

The IPv4 WAN connection has been created.

Steps

1. On the navigation tree, click [**Network→ WAN→6in4 Tunnel Connection**]. The 6in4 tunnel connection is displayed, see Figure 9.

Figure 9 6in4 Tunnel Connection

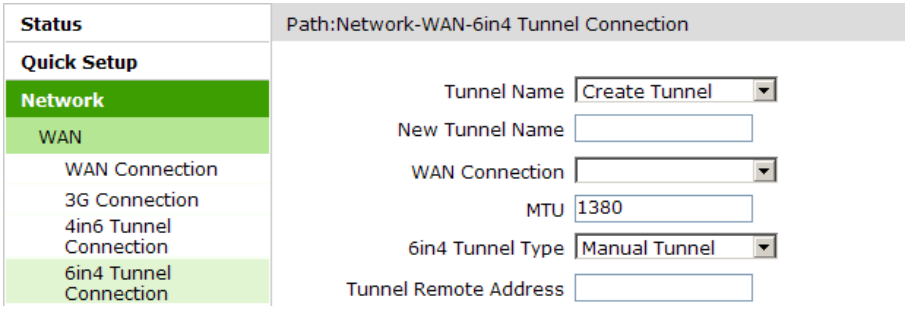


Table 9 lists the parameters for 6in4 tunnel connection.

Table 9 6in4 Tunnel Connection Parameter

Parameter	Description
Tunnel Name	The default is **Create Tunnel**. Before creating a new tunnel name, make sure the **Create Tunnel** option is selected.
New Tunnel Name	Specify the new tunnel name.
WAN Connection	Select the IPv4 WAN connection.
MTU	MTU size of the tunnel
6in4 Tunnel Type	There are two 6in4 tunnel types: ▯ Manual Tunnel ▯ 6rd
Tunnel Remote Address	Specify the tunnel remote address when the **Manual Tunnel** option is selected for the **6in4 Tunnel Type**.
6in4 Tunnel Configuration	The 6in4 Tunnel Configuration includes: ▯ Static ▯ Auto

Parameter	Description
6rd Prefix	Specify the 6rd Prefix.
IPv4 Masklen	Specify the IPv4 Masklen.
BR Address	Specify the BR Address.

2. Specify the parameters according to the request, and click **Create**.

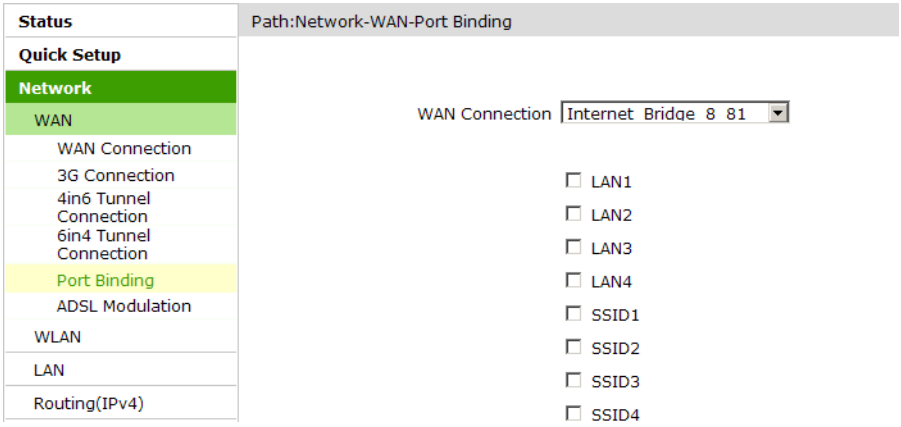
6.1.5 Configuring Port Binding

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

Steps

1. On the navigation tree, click [**Network→ WAN→ Port Binding**]. The port binding configuration page is displayed, see Figure 10.

   Figure 10 Port Binding



2. Select a WAN connection type from the **WAN Connection** drop-down list, and select the LAN port or SSID that you want to bind.
3. After the configuration, click **Submit**.

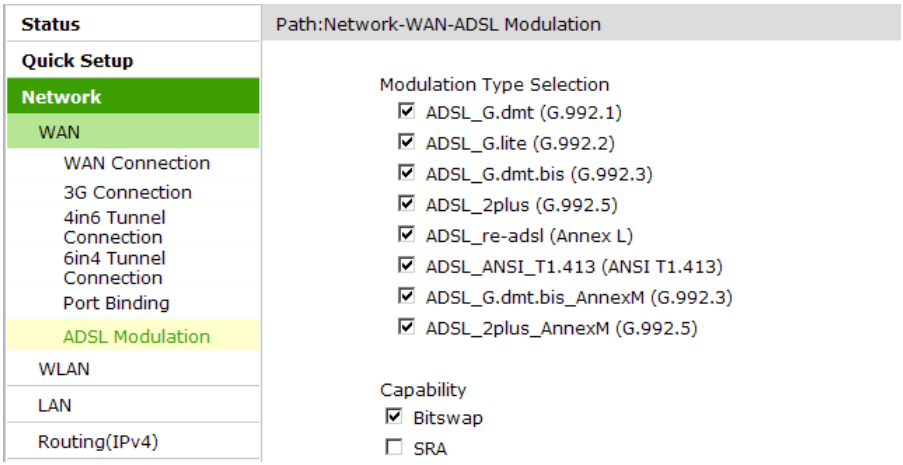
6.1.6 Configuring ADSL Modulation

This procedure introduces how to configure the ADSL modulation type.

Steps

1. On the navigation tree, click [**Network→ WAN→ ADSL Modulation**]. The ADSL modulation configuration page is displayed, see Figure 11.

Figure 11 ADSL Modulation



2. Select the ADSL modulation types and click **Submit**.

6.2 WLAN

This section includes the following:

- Configuring Basic WLAN Parameters
- Configuring SSID Settings
- Configuring Security
- Configuring Access Control List
- Displaying Associated Devices
- Configuring WiFi Restrictions
- Configuring WPS

6.2.1 Configuring Basic WLAN Parameters

This procedure introduces how to configure the basic WLAN parameters.

Context

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)

Steps

1. On the navigation tree, click [**Network→ WLAN→ Basic**]. The basic WLAN parameter configuration page is displayed, see Figure 12.

Figure 12 Basic WLAN Parameter Configuration

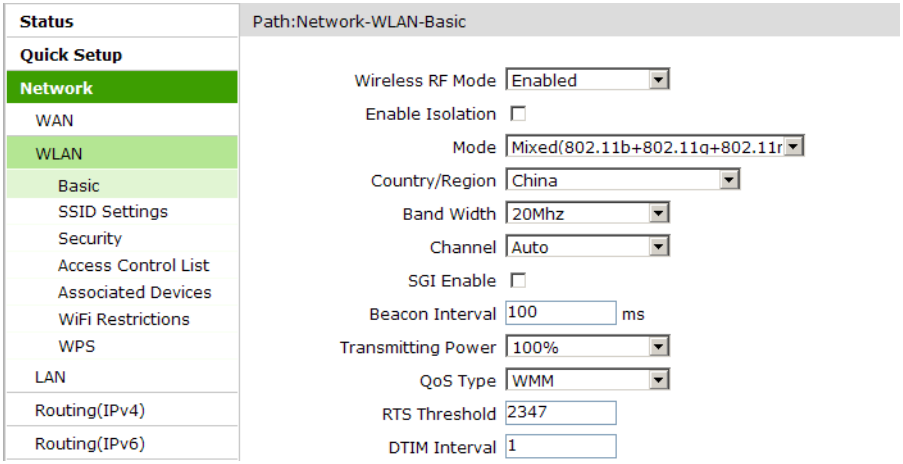


Table 10 lists the basic WLAN parameters.

Table 10 Basic WLAN Parameter

Parameter	Description
Wireless RF Mode	Select **Enabled** to enable the wireless RF function.
Enable Isolation	Select this option, and the wireless clients with the different SSIDs will can not access each other.
Mode	Select the wireless RF transmission mode.
Country/Region	Select the country or region.
Band Width	You can select 20Mhz or 40Mhz.
Channel	The default is **Auto**.
SGI Enable	Enable this option to increase the traffic flow.
Beacon Interval	Time interval for the wireless device to broadcast the SSID information. Keep the default value.

Parameter	Description
Transmitting Power	Select the transmitting power as required.
QoS Type	There are three QoS types: ▯ Disable ▯ WMM ▯ SSID The default QoS type is **WMM**.
RTS Threshold	Specify the request to send threshold for a packet. When a packet exceeds this value, the device sends the RTS value tothe destination point for negotiation. The default is 2347.
DTIM Interval	Range: 1 ~ 5 Default: 1

2. Select **Enabled** from the **Wireless RF Mode** drop-down list to enable the wireless transmission function, and then select the transmission mode. For example, select **IEEE 802.11n Only** from the **Mode** drop-down list, and specify the other parameters according the request.
3. After the configuration, click **Submit**.

6.2.2 Configuring SSID Settings

The ZXHN H108N device supports four SSIDs and each SSID supports up to 32 subscribers.

This procedure introduces how to configure the SSID settings.

Steps

1. On the navigation tree, click [**Network→ WLAN→ SSID Settings**]. The SSID setting page is displayed, see Figure 13.

Figure 13 SSID Settings

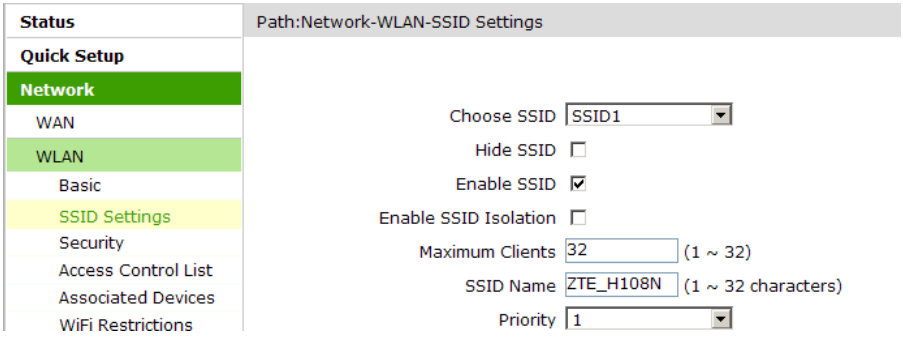


Table 11 lists the SSID parameters.

Table 11 SSID Parameters

Parameter	Description
Choose SSID	Select the SSID to be configured.
Hide SSID	Hide the SSID information to prevent illegal users.
Enable SSID	Enable the SSID broadcast.
Enable SSID Isolation	Enable SSID isolation. The wireless clients with the same SSID can not access each other.
Maximum Clients	Range: 1 ~ 32
SSID Name	Specify the SSID name.
Priority	Range: 0 ~ 7

2. Select an SSID from the **Choose SSID** drop-down list, and specify other parameters.
3. Click **Submit**.

6.2.3 Configuring Security

The ZXHN H108N device provides five WLAN authentication type, including open system, shared key, WPA PSK, WPA2-PSK, and WPA/WPA2-PSK.

This procedure introduces how to configure WLAN security settings.

Context

The ZXHN H108N provides the following access authentication modes:

- Open System

  Authentication is not needed. Any client with a wireless network card can connect to the wireless access point.

- 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 it is securer. 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.

Steps

1. On the navigation tree, click [**Network→ WLAN→Security**]. The security page is displayed, see Figure 14.

Figure 14 SSID Security Configuration

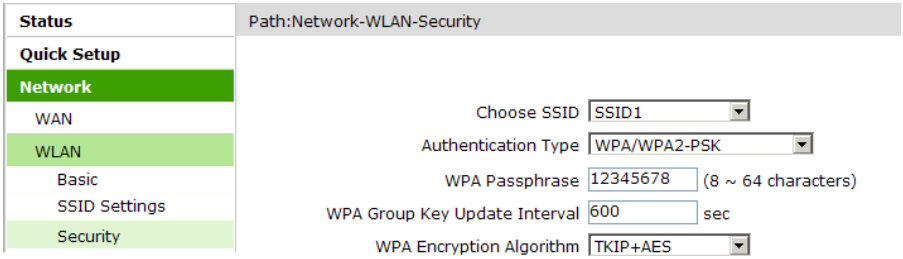


Table 12 lists the SSID security parameters.

Table 12 SSID Security Parameters

Parameter	Description
Choose SSID	Select the SSID to be configured.
Authentication Type	Select the authentication type.
WEP Encryption	**Enable**/**Disable** WEP Encryption.
WEP Encryption Level	The value can be **64bit** or **128bit**.
WEP Key Index	The WEP authentication provides four keys.
WEP Key1~WEP Key4	Use 5 ASCII characters or 10 hexadecimal digits to specify the WEP value for the 64 bit WEP encryption. Use 13 ASCII characters or 26 hexadecimal digits to specify the WEP value for the 128 bit WEP encryption.
WPA Passphrase	Range: 8 ~ 63 characters
WPA Group Key Update Interval	Default: 600 s
WPA Encryption Algorithm	There are three options: ▯ TKIP:Temporal Key Integrity Protocol ▯ AES: Advanced Encryption Standard ▯ TKIP+AES: Adaptive encryption algorithm

2. Select one SSID from the **Choose SSID** drop-down list and then select the authentication type from the **Authentication Type** drop-down list.
3. Specify other parameters.
4. Click **Submit**.

6.2.4 Configuring Access Control List

The ZXHN H108N device supports ACL function, which is used to permit or block the packets from the specified MAC address. This procedure introduces how to configure the ACL.

By default, the ACL function for the ZXHN H108N is enabled.

Steps

1. On the navigation tree, click [**Network→ WLAN→ Access Control List**]. The access control list configuration page is displayed, see Figure 15.

Figure 15 Access Control List

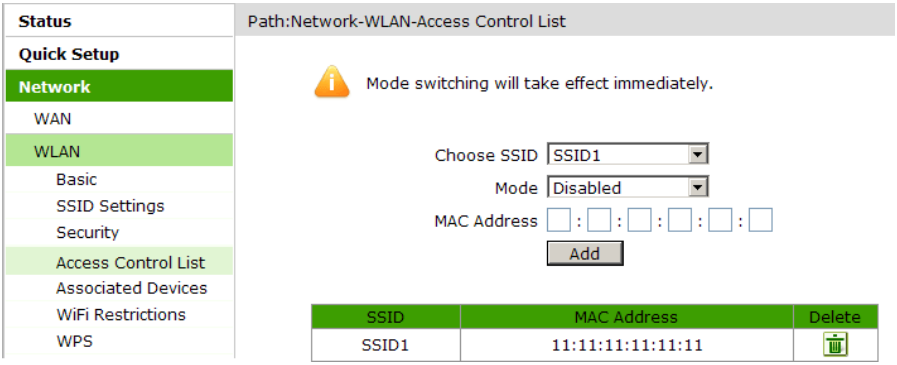


Table 13 lists the ACL parameters.

Table 13 ACL Parameter

Parameter	Description
Choose SSID	Choose the SSID to configure the ACL.
Mode	There are three options: ▯ Disabled: Disable the ACL function. ▯ Block: The wireless device whose MAC address is specified is not allowed to access the ZXHN H108N device. ▯ Permit: The wireless device whose MAC address is specified is allowed to access the ZXHN H108N device.
MAC Address	The MAC address of the wireless device

2. Select an SSID from the **Choose SSID** drop-down list, and then specify other parameters.
3. Click **Add** to add the MAC address to the access control list.

The ACL is configured.

The MAC address of the wireless device is added to the access control list.

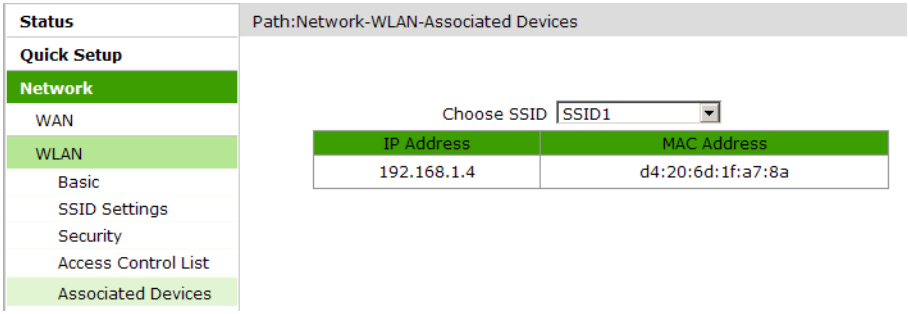
6.2.5 Displaying Associated Devices

This procedure introduces how to display the wireless devices that are connected to the ZXHN H108N device.

Steps

1. On the navigation tree, click [**Network→ WLAN→ Associated Devices**]. The associated device page is displayed.
2. Select an SSID (for example, **SSID1**) from the **Choose SSID** drop-down list. The system displays the MAC addresses of all the wireless devices that are using the specified SSID to connect the ZXHN H108N device, see Figure 16.

Figure 16 Associated Devices



6.2.6 Configuring WiFi Restrictions

This procedure introduces how to turn on or turn off the WiFi function on schedule.

Prerequisite

Before the operation, make sure that:

- The **Wireless RF Mode** is set to **Scheduled**.
- The network time synchronization has succeeded.

Steps

1. On the navigation tree, click [**Network→ WLAN→WiFi Restrictions**]. The WiFi restriction page is displayed, see Figure 17.

Figure 17 WiFi Restrictions

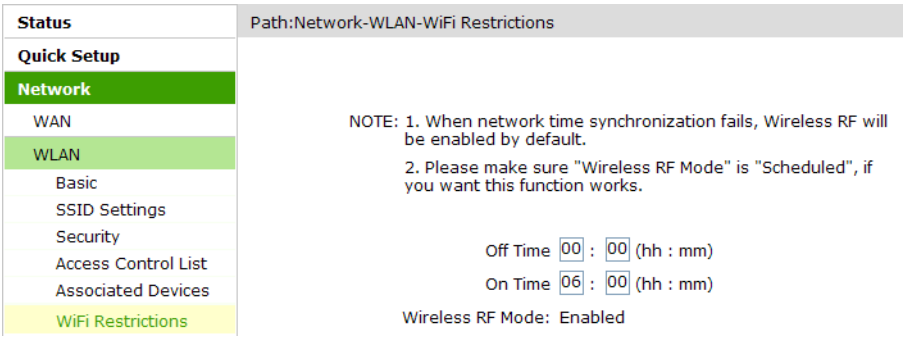


Table 14 lists the parameters for WiFi restriction.

Table 14 Parameter Description for WiFi Restriction

Parameter	Description
Off Time	Specify the time to disable the WiFi function.
On Time	Specify the time to enable the WiFi function.

2. Specify the time to enable or disable the WiFi function.
3. Click **Submit**.

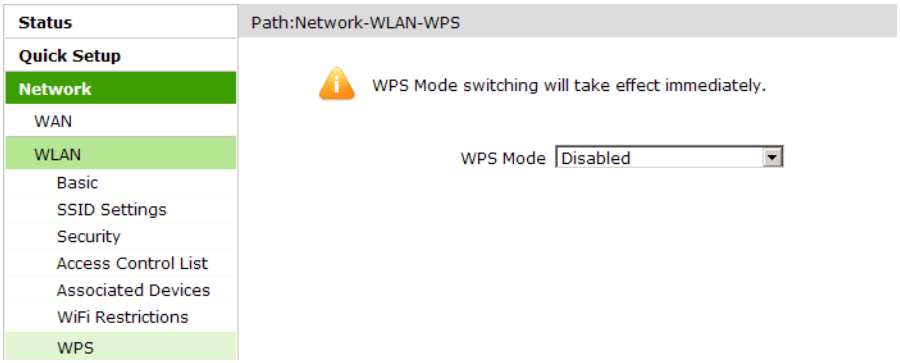
6.2.7 Configuring WPS

Configuring WPS to switiching WPS mode.

Steps

1. On the navigation tree, click [**Network→WLAN→WPS**]. The **WPS** page is displayed, see Figure 18.

Figure 18 WPS



2. Select **Disabled** or **PBC** from WPS Mode.

6.3 LAN

This section includes the following:

- Configuring DHCP Server
- Configuring IPv6 DHCP Server
- Configuring DHCP Binding
- Configuring DHCP Port Service
- Configuring IPv6 Static Prefix
- Configuring IPv6 Prefix Delegation
- Configuring IPv6 Port Service
- Configuring RA Service

6.3.1 Configuring DHCP Server

ZXHN H108N supports the dynamic IP address allocation to the user-side computers or the wireless devices connected to the ZXHN H108N device.

This procedure describes how to configure the DHCP server.

Steps

1. On the navigation tree, click [**Network→ LAN→ DHCP Server**]. The DHCP server configuration page is displayed, see Figure 19.

Figure 19 DHCP Server

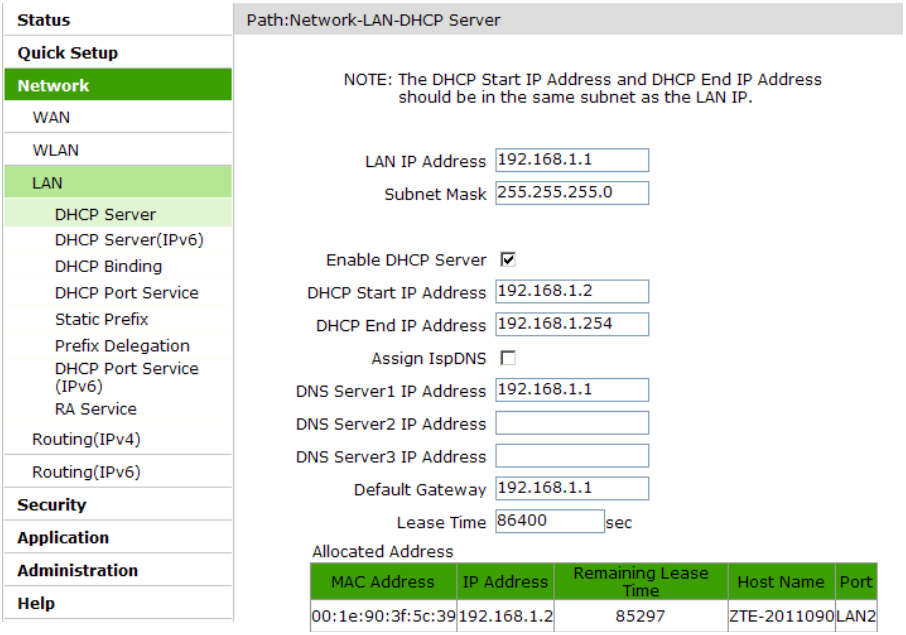


Table 15 lists the DHCP server parameters.

Table 15 DHCP Server Parameters

Parameter	Description
LAN IP Address	IP address of the ZXHN H108N device The device IP address should be in the same network segment as the DHCP address pool.
Subnet Mask	Subnet mask of the device
Enable DHCP Server	Select the **Enable DHCP Server** check box to let the device work as a DHCP server and assign IP addresses to the client PCs or wireless devices.
DHCP Start IP Address	The start IP address of the DHCP address pool
DHCP End IP Address	The end IP address of the DHCP address pool
Assign IspDNS	Select this option to let the DNS provided by the ISP to assign IP addresses to the client PCs or wireless devices.
DNS Server1 IP Address~DNS Server3 IP Address	IP addresses of the DNS server, provided by the ISP

Parameter	Description
Default Gateway	It is usually the IP address of the ZXHN H108N device by default.
Lease Time	The time during which the client PCs use the IP addresses assigned by the DHCP server After the lease time expires, the private IP address will be available for assigning to other network devices. Default: 86400 seconds

2. Specify the DHCP server parameters, and then click **Submit**.

The DHCP server is configured.

IP addresses are automatically assigned to the user-side PCs and wireless devices that are connected to the ZXHN H108N.

6.3.2 Configuring IPv6 DHCP Server

This procedure describes how to configure the IPv6 DHCP server to dynamically allocate IPv6 addresses to the user-side computers or wireless devices that are connected to the ZXHN H108N device.

Steps

1. On the navigation tree, click [**Network→ LAN→ DHCP Server(IPv6)**]. The IPv6 DHCP server configuration page is displayed, see Figure 20.

Figure 20 IPv6 DHCP Server

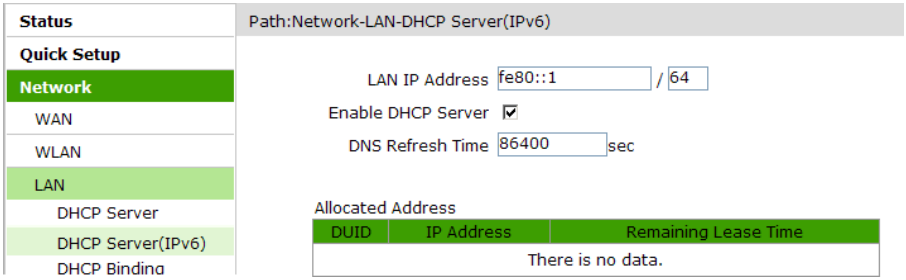


Table 16 lists the IPv6 DHCP server parameters.

Table 16 IPv6 DHCP Server Parameters

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

2. Specify the DHCP server parameters.
3. Click **Submit**.

6.3.3 Configuring DHCP Binding

This procedure describes how to bind the IP address with the specified MAC address.

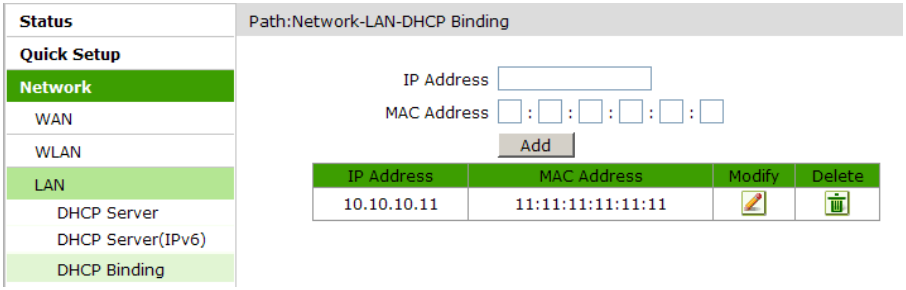
Prerequisite

The DHCP service is enabled.

Steps

1. On the navigation tree, click [**Network→ LAN→ DHCP Binding**] to open the DHCP binding configuration page.
2. Specify the **IP Address** and **MAC Address** to bind. The following **IP Address** and **MAC Address** are bound, see Figure 21.

Figure 21 DHCP Binding



3. Click **Add**.

The DHCP binding table is configured. When the device whose MAC address is in the DHCP binding table is connected to ZXHN H108N, it will be automatically assigned the corresponding IP address.

6.3.4 Configuring DHCP Port Service

This procedure introduces how to disable the DHCP service for the specified interface or SSID when the global DHCP function is enabled.

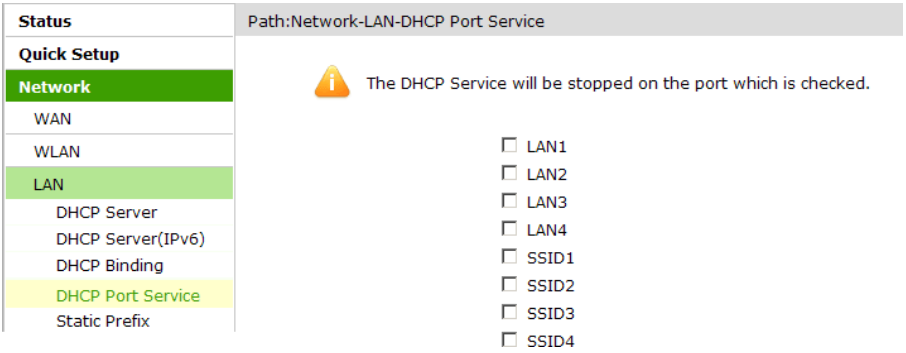
Prerequisite

Before configuring DHCP port service, make sure that the global DHCP service is enabled.

Steps

1. On the navigation tree, click [**Network→ LAN→ DHCP Port Service**]. The DHCP port service configuration page is displayed, see Figure 22.

   Figure 22 DHCP Port Service



2. Select the LAN interface or SSID whose DHCP function you want to disable.
3. Click **Submit**.

The DHCP function is disabled on the specified interface or SSID.

The devices that are connected to the specified LAN interface or use the SSID will not be assigned the IP addresses.

6.3.5 Configuring IPv6 Static Prefix

This procedure introduces how to configure the IPv6 static prefix.

Context

The prefix is distributed by the RA or DHCPv6 server. Only the GUA prefix with the length between 48 and 64 is supported. The valid life time should be longer than the preferred life time.

Steps

1. On the navigation tree, click [**Network→ LAN→ Static Prefix**], see Figure 23.

Figure 23 Static Prefix

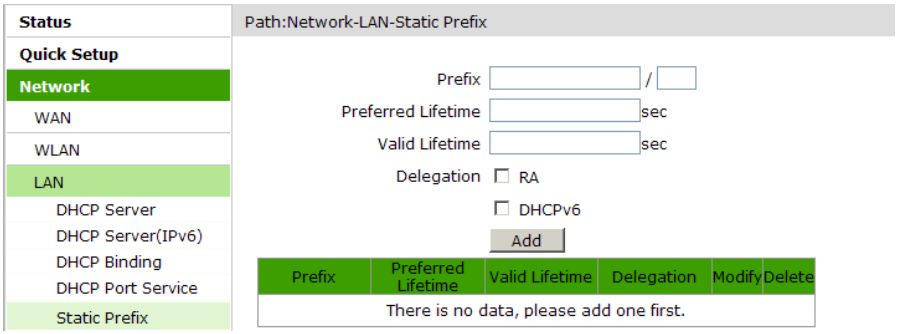


Table 17 describers the parameters for IPv6 static prefix.

Table 17 IPv6 Static Prefix Parameters

Parameter	Description
Prefix	IPv6 address prefix
Prefer LifeTime	Preferred life time of the prefix The device on the LAN side refreshes the IPv6 address in the preferred life time. Preferred life time should be no longer than Valid life time Unit: second
Valid LifeTime	Valid time of the prefix
Delegation	Prefix delegation mode: ▯ RA ▯ DHCPV6

2. Configure the parameters, and then click **Add**.

6.3.6 Configuring IPv6 Prefix Delegation

This procedure introduces how to configure the IPv6 prefix delegation mode for a specified WAN connection.

Prerequisite

Before configuring the prefix delegation, make sure that the prefix delegation is enabled for the specified IPv6 WAN connection.

Steps

1. On the navigation tree, choose [**Network→ LAN→Prefix Delegation**]. The IPv6 prefix delegation configuration page is displayed, see Figure 24.

Figure 24 IPv6 Prefix Delegation

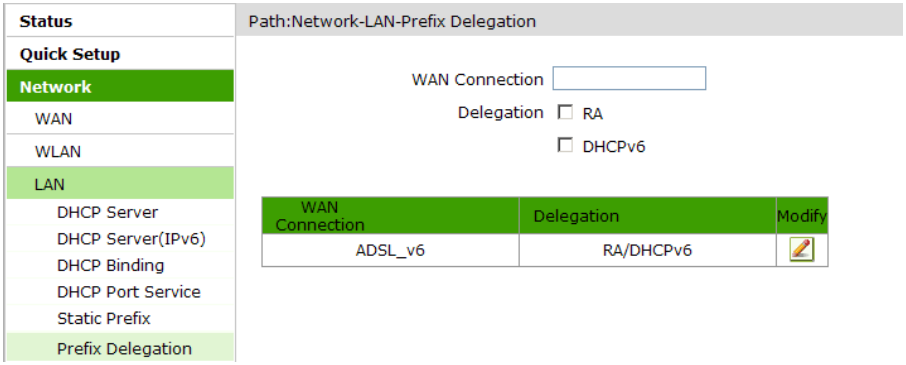


Table 18 describers the parameters for IPv6 prefix delegation.

Table 18 IPv6 Prefix Delegation Parameters

Parameter	Description
WAN Connection	The configured WAN connection
Delegation	Prefix delegation mode: ▯ RA ▯ DHCPV6

2. In the WAN list, click  and configure the prefix delegation mode.
3. After the configuration, click **Modify** to update.

6.3.7 Configuring IPv6 Port Service

This procedure introduces how to disable the IPv6 DHCP service for the specified interface or SSID when the global IPv6 DHCP function is enabled.

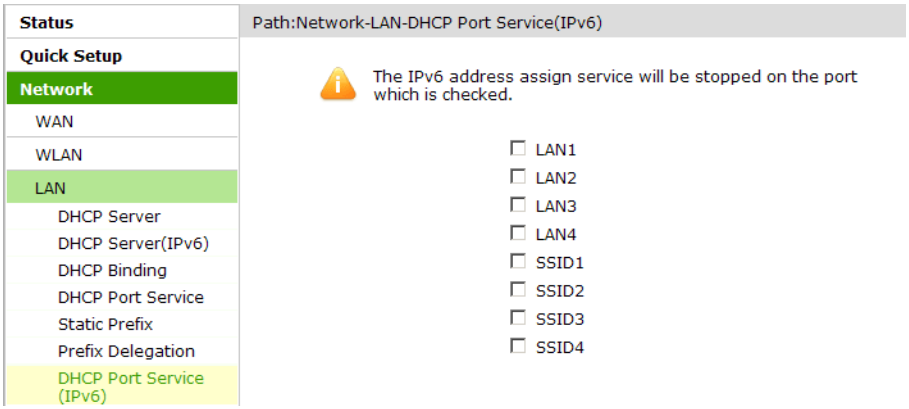
Prerequisite

Before configuring IPv6 port service, make sure that the global IPv6 DHCP service is enabled.

Steps

1. On the navigation tree, click [**Network→ LAN→ DHCP Port Service (IPv6)**]. The IPv6 port service configuration page is displayed, see Figure 25.

Figure 25 IPv6 Port Service



2. Select the LAN interface or SSID whose DHCP function you want to disable.
3. Click **Submit**.

The IPv6 DHCP function is disabled on the specified interface or SSID.

The devices that are connected to the specified LAN interface or use the SSID will not be assigned the IPv6 addresses.

6.3.8 Configuring RA Service

This procedure introduces how to configure the RA service.

Steps

1. On the navigation tree, click [**Network**→ **LAN**→ **RA Service**]. The RA service configuration page is displayed, see Figure 26.

Figure 26 RA Service

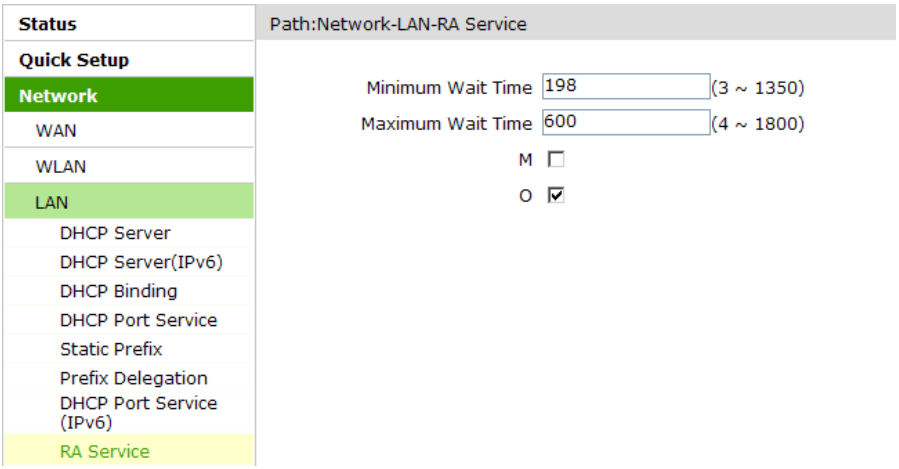


Table 19 describes the parameters for the RA service.

Table 19 Parameters for the RA Service

Parameter	Description
Minimum Wait Time	Minimum delegation interval
Maximum Wait Time	Maximum delegation interval
M	Managed flag Select this check box to enable the connected devices to obtain the IPv6 address through DHCPV6.
O	Other configure flag Select this check box to enable the connected devices to obtain DNS address through DHCPV6.

2. Configure the parameters, and then click **Submit**.

6.4 Routing (IPv4)

This section includes the following:

- Configuring IPv4 Default Gateway
- Configuring IPv4 Static Routing
- Configuring IPv4 Policy Routing
- Configuring IPv4 Routing Table

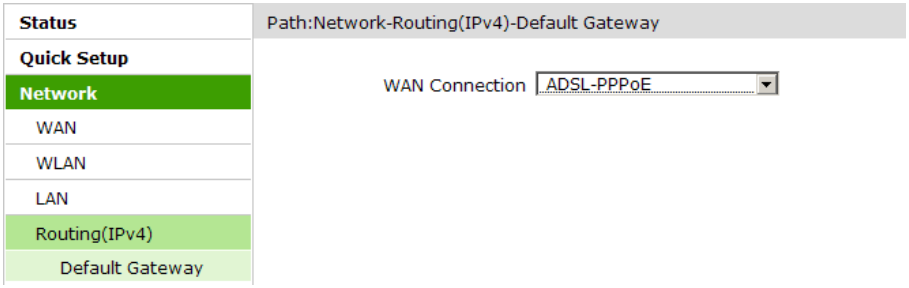
6.4.1 Configuring IPv4 Default Gateway

This procedure introduces how to configure one WAN connection as the IPv4 default gateway. All the user-side devices will access the Internet by using this WAN connection by default.

Steps

1. On the navigation tree, click [**Network→Routing(IPv4)→Default Gateway**]. The default gateway page is displayed, see Figure 27.

   Figure 27 Default Gateway



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

6.4.2 Configuring IPv4 Static Routing

This procedure introduces how to configure the static routing for the specified WAN connection.

Prerequisite

Before configuring static routing, make sure that the WAN connection is created.

Context

The gateway needs to be configured for the Static mode interface or IPoA mode interface during static routing configuration.

The gateway does not need to be configured for the PPPoA mode interface or PPPoE mode interface during static routing configuration.

Steps

1. On the navigation tree, click [**Network→Routing(IPv4)→ Static Routing**]. The static routing configuration page is displayed, see Figure 28.

Figure 28 Static Routing

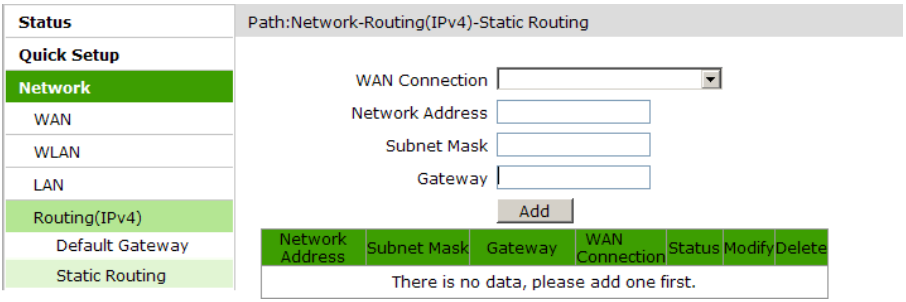


Table 20 lists the parameters for the static routing configuration.

Table 20 Parameters for Static Routing Configuration

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

2. Select one WAN connection from the **WAN Connection** drop-down list, and then specify other parameters.
3. After the configuration, click **Add**.

6.4.3 Configuring IPv4 Policy Routing

This procedure introduces how to configure the policy routing for the specified WAN connection.

Prerequisite

Before configuring policy routing, make sure that the WAN connection settings are complete.

Context

Policy routing is a routing rule. When it is configured, the packets are forwarded based on the routing policy. The ZXHN H108N supports packet forwarding based on the DSCP, source or destination IP address, protocol, source port number, or source MAC address.

Steps

1. On the navigation tree, click [**Network→Routing(IPv4)→ Policy Routing**]. The policy routing configuration page is displayed, see Figure 29.

Figure 29 Policy Routing

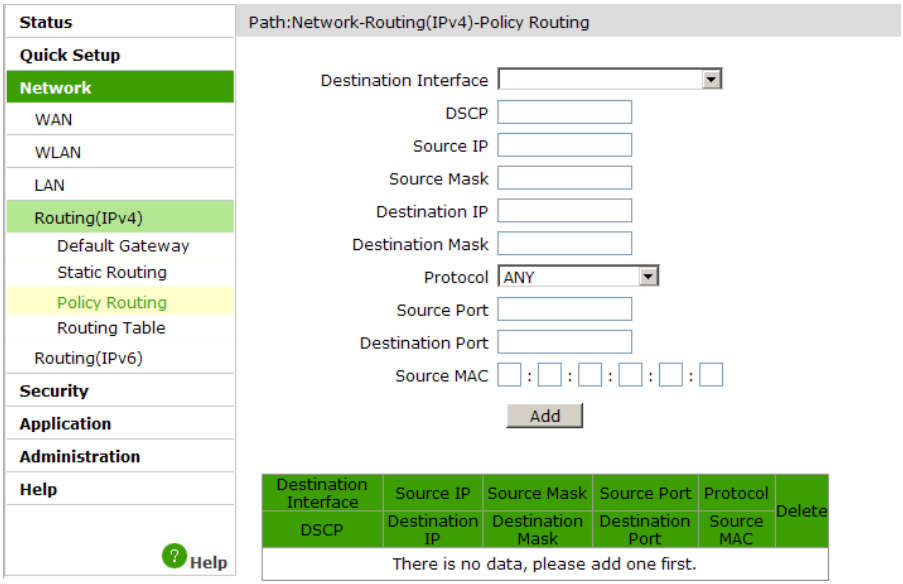


Table 21 lists the parameters for the policy routing configuration.

Table 21 Parameters for Policy Routing Configuration

Parameter	Description
Destination Interface	Determined by the carrier
DSCP	DSCP value
Source IP	Source IP address
Source Mask	Source mask of the network segment
Destination IP	Destination IP address
Destination Mask	Destination mask of the network segment
Protocol	The protocol includes the following: ▯ **TCP** ▯ **UDP** ▯ **ICMP** ▯ **ANY**
Source Port	Source port number
Destination Port	Destination port number
Source MAC	Source MAC address

2. Select an interface from the **Destination Interface** drop-down list, and specify the routing policy as required.
3. Click **Add**.

The policy routing rule is configured. The packets will be forwarded based on the policy routing.

6.4.4 Displaying IPv4 Routing Table

This procedure introduces how to display the routing table.

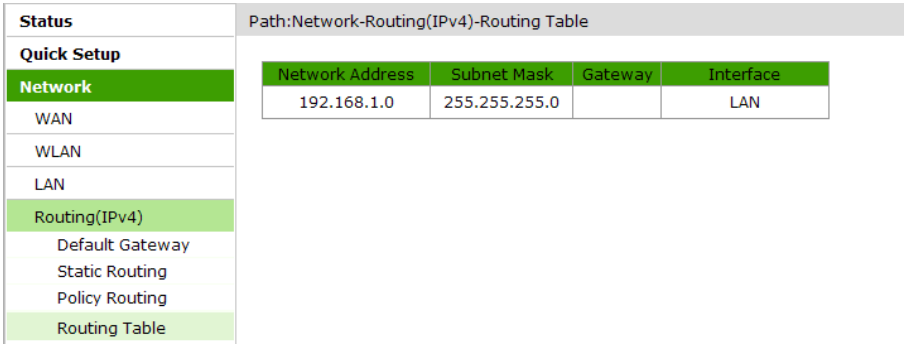
Prerequisite

The routing tables have been created.

Steps

1. On the navigation tree, click [**Network→Routing(IPv4)→ Routing Table**] to display the routing table, which displays the routing information, see Figure 30.

Figure 30 Routing Table



6.5 Routing (IPv6)

This section includes the following:

- Configuring IPv6 Default Gateway
- Configuring IPv6 Static Routing
- Configuring IPv6 Policy Routing
- Displaying IPv6 Routing Table

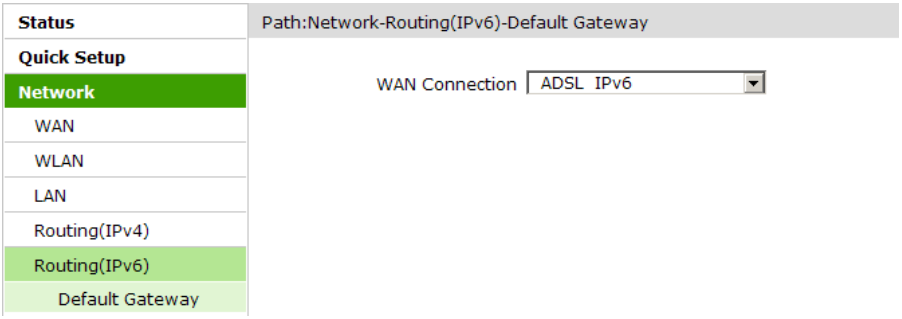
6.5.1 Configuring IPv6 Default Gateway

This procedure introduces how to configure one WAN connection as the IPv6 default gateway. All the user-side devices will access the Internet by using this WAN connection by default.

Steps

1. On the navigation tree, click [**Network→Routing(IPv6)→Default Gateway**]. The default gateway page is displayed, see Figure 31.

Figure 31 Default Gateway



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

6.5.2 Configuring IPv6 Static Routing

This procedure introduces how to configure IPv6 static routing.

Prerequisite

Before configuring static routing, make sure that the IPv6 WAN connection is created.

Steps

1. On the navigation tree, click [**Network→Routing(IPv6)→ Static Routing**]. The IPv6 static routing configuration page is displayed, see Figure 32.

Figure 32 IPv6 Static Routing

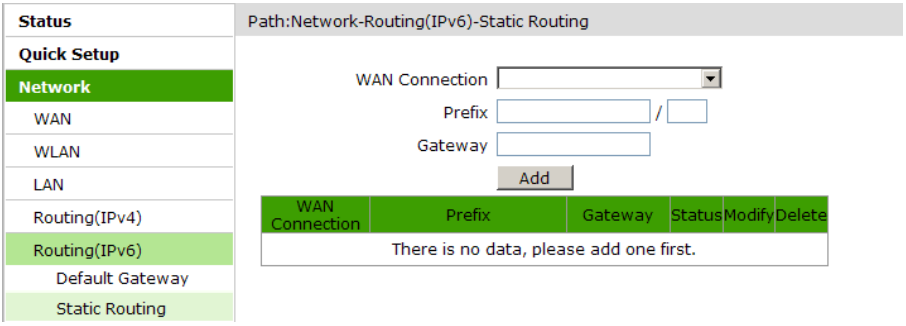


Table 22 describes the parameters for the static routing.

Table 22 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.

2. Configure the parameters, and then click **Add**.

6.5.3 ConfiguringIPv6 Policy Routing

This procedure introduces how to configure the IPv6 policy routing for the specified WAN connection.

Prerequisite

Before configuring IPv6 policy routing, make sure that the IPv6 WAN connection settings are complete.

Context

Policy routing is a routing rule. When it is configured, the packets are forwarded based on the routing policy. The ZXHN H108N supports packet forwarding based on the DSCP, source or destination IP address, protocol, source port number, or source MAC address.

Steps

1. On the navigation tree, click [**Network→Routing(IPv6)→ Policy Routing**]. The IPv6 policy routing configuration page is displayed, see Figure 33.

Figure 33 IPv6 Policy Routing

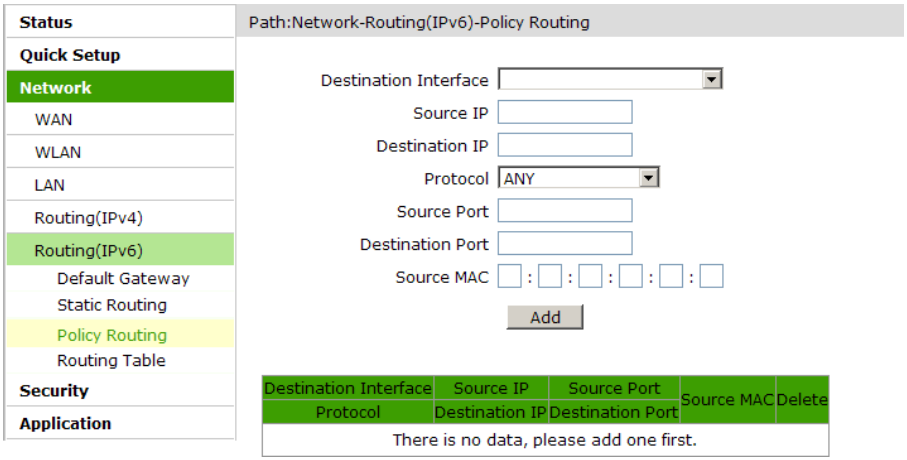


Table 23 lists the parameters for IPv6 policy routing configuration.

Table 23 Parameters for Policy Routing Configuration

Parameter	Description
Destination Interface	Determined by the carrier
Source IP	Source IPv6 IP address
Destination IP	Destination IPv6 IP address
Protocol	The protocol includes the following: ▯ **TCP** ▯ **UDP** ▯ **ANY**
Source Port	Source port number
Destination Port	Destination port number
Source MAC	Source MAC address

2. Select an interface from the **Destination Interface** drop-down list, and specify the routing policy as required.
3. Click **Add**.

The IPv6 policy routing rule is configured. The packets will be forwarded based on the policy routing.

6.5.4 Displaying IPv6 Routing Table

This procedure introduces how to display the IPv6 routing table.

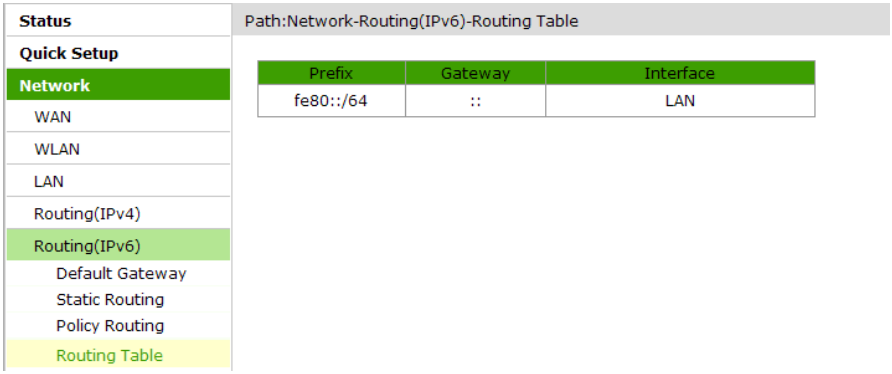
Prerequisite

The IPv6 routing tables have been created.

Steps

1. On the navigation tree, click [**Network→ Routing(IPv6)→ Routing Table**] to display the IPv6 routing table, which displays the IPv6 routing information, see Figure 34.

Figure 34 IPv6 Routing Table



7 Security

7.1 Configuring Firewall

This procedure introduces how to configure the firewall to prevent malicious attack from the external network and enhance device security.

Steps

1. On the navigation tree, click [**Security→ Firewall**]. The firewall configuration page is displayed, see Figure 35.

Figure 35 Firewall

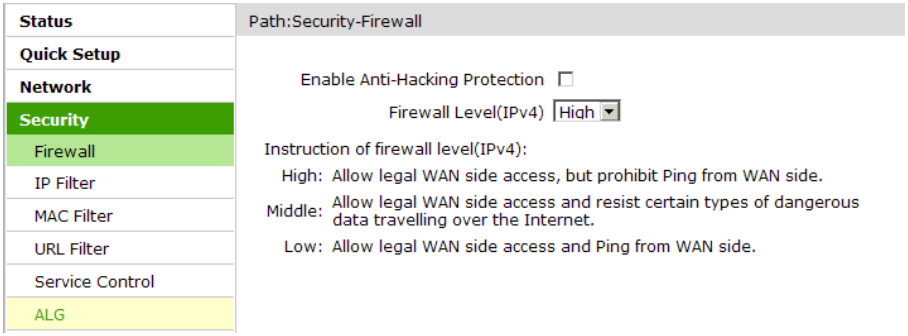


Table 24 lists the firewall parameters.

Table 24 Firewall Parameters

Parameter	Description
Enable Anti-Hacking Protection	Select the check box to enable the firewall settings and prevent the device from being attacked by the Internet data stream. These attacks include ping flood, ping to death and syn flood.
Firewall Leve(IPv4)	▯ High: It allows the legal WAN to access the device but forbids a device from the Internet to send ping packets to the WAN interface of the ZXHN H108N. ▯ Middle: It allows the legal WAN to access the device and a device from the Internet to send ping packets to the WAN interface of the ZXHN H108N. ▯ Low: Allow legal WAN side access and Ping from WAN side.

2. Specify the firewall parameters, and then click **Submit**.

The firewall is configured. The ZXHN H108N device will automatically block the external access based on the firewall security configuration.

7.2 Configuring IP Filter

The ZXHN H108N device supports filtering the packets based on the IP range, port range, and protocol. This procedure introduces how to permit or deny the specified packets to go through the device.

Steps

1. On the navigation tree, click [**Security→ IP Filter**]. The IP filter configuration page is displayed, see Figure 36. On this page, you can specify to discard or permit the data packages by configuring the IP address and protocol.

Figure 36 IP Filter

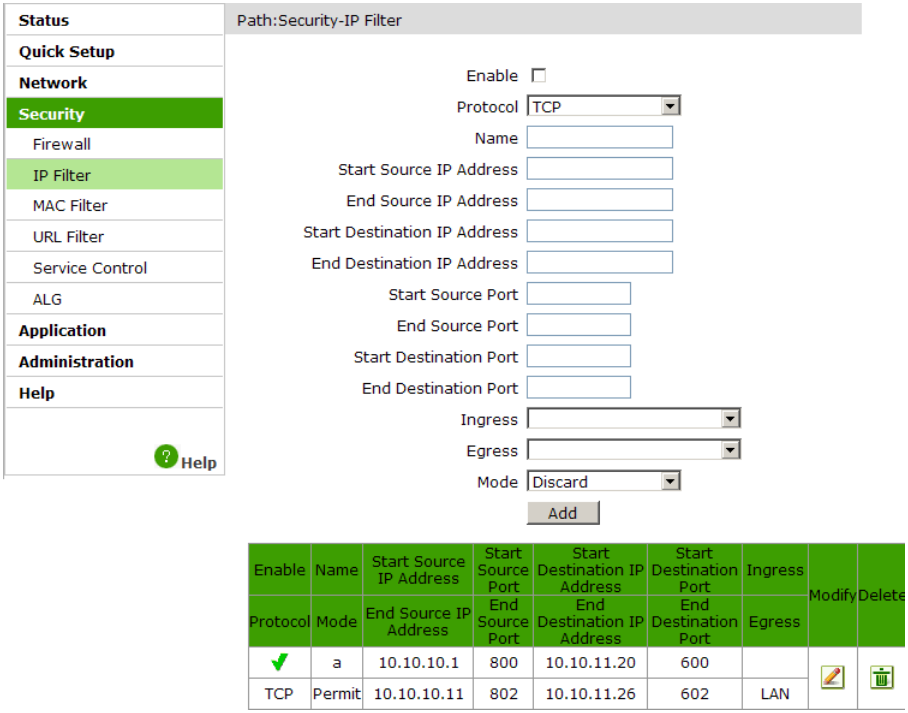


Table 25 lists the IP filter parameters.

Table 25 IP Filter Parameters

Parameter	Description
Enable	Enable the IP filter function.
Protocal	Select the protocol that needs to filter packets. By default, it is **TCP**.
Name	Name of the IP filter rules
Start/End Source IP Address	Range of source IP address
Start/End Destination IP Address	Range of destination IP address
Start/End Source Port	Range of source port
Start/End Destination Port	Range of destination port
Ingress/Engress	Data flow direction The ingress and egress cannot be the same ▯ If the ingress is LAN and egress is ADSL, the data flow is upstream. ▯ If the ingress is ADSL and egress is LAN, the data flow is downstream.
Mode	The mode can be **Discard** or **Permit**.

2. After the configuration, click **Add**.

7.3 Configuring MAC Filter

This procedure introduces how to configure MAC filter settings to permit or deny the packets with the specific MAC addresses to access the Internet.

Context

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

Steps

1. On the navigation tree, click [**Security→ MAC Filter**]. The MAC filter configuration page is displayed, see Figure 37. On this page, you can specify to discard or permit the data packages by configuring the MAC address, protocol, and the connection type.

Figure 37 MAC Filter

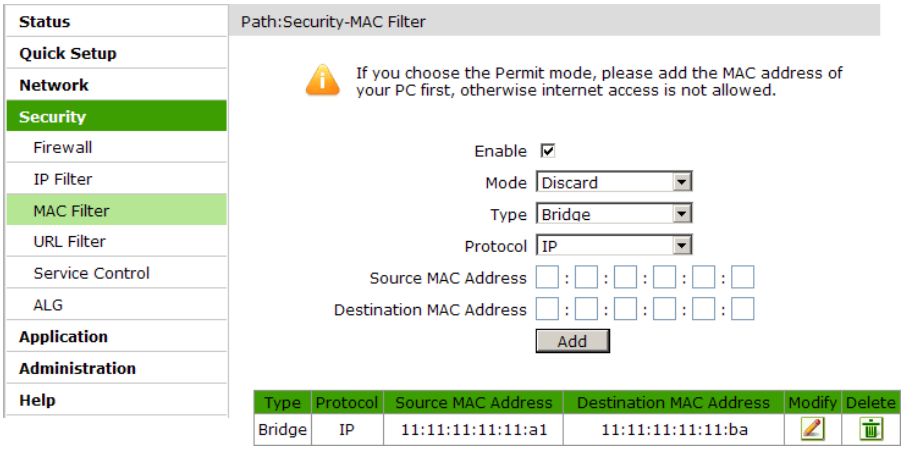


Table 26 lists the MAC filter parameters.

Table 26 MAC Filter Parameters

Parameter	Description
Enable	Enable the MAC filter function.
Mode	The mode can be **Discard** or **Permit**.
Type	The type can be **Bridge**, **Route**, or **Bridge+Route**.
Protocol	The protocol that the MAC filter rule will be applied to.
Source MAC Address/Destination MAC Address	MAC address that needs to be filtered. Both options cannot be null at the same time.

Note:

*If you select **Permit** from the **Mode** drop-down list, please add the MAC address of your PC first, otherwise you cannot access the Web configuration page by using the PC that is connected to the ZXHN H108N device.*

2. Configure the MAC filter parameters, and then click **Add**.

The MAC filter is configured.

The packets with the specified MAC address are denied or allowed to pass through.

7.4 Configuring URL Filter

This procedure introduces how to configure URL filter rules, so that users are permitted or denied to access the specific URL addresses.

Steps

1. On the navigation tree, click [**Security→ URL Filter**]. The URL filter configuration page is displayed, see Figure 38. On this page, you can specify the URL rules to permit or deny the users to access the specified URL addresses.

Figure 38 URL Filter

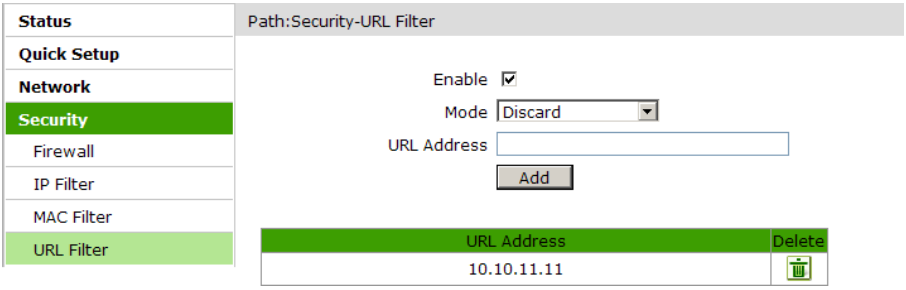


Table 27 lists the parameters for URL filter configuration.

Table 27 URL Filter Parameter

Parameter	Description
Enable	Enable the URL filter function
Mode	There are two modes: **Discard** and **Permit**. ▯ Discard: Deny the users to access the specified URL addresses. ▯ Permit: Permit the users to access the specified URL addresses.
URL Address	The URL address that is allowed to be accessed or denied

2. Specify the URL and other parameters, and then click **Add**.

The URL filter is configured.

Users are permitted or denied to access the specified URL addresses.

7.5 Configuring Service Control

This procedure introduces how to permit or discard the specified inbound access services by configuring the source IP address range and service type.

Context

By default, you cannot access the device through the WAN interface by FTP or web site.

Steps

1. On the navigation tree, click [**Security→ Service Control**]. The service control configuration page is displayed, see Figure 39. On this page, you can permit or discard the specified inbound access services by configuring the source IP address range and service types

Figure 39 Service Control

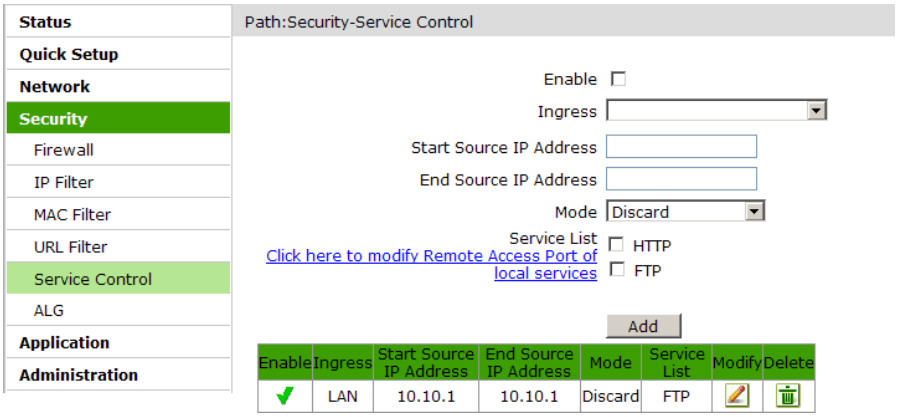


Table 28 lists the service control parameters.

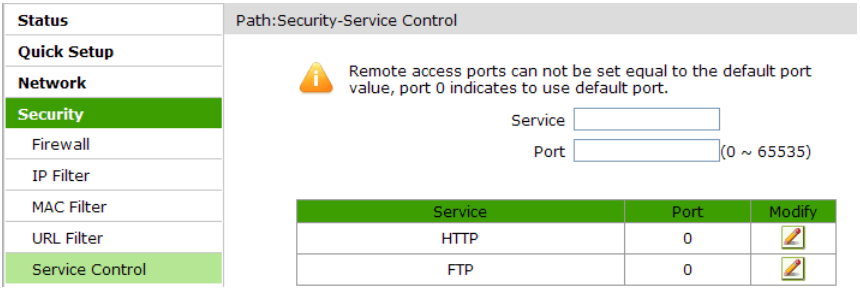
Table 28 Service Control Parameters

Parameter	Description
Enable	Select the **Enable** check box to enable the service control settings.
Ingress	Specify the data stream inbound direction, and this parameter must be specified. If the Ingress is **LAN**, the data flow is upstream. If the Ingress is a WAN or 3G_PPPoE connection, the data flow is downstream.
Start Source IP Address/End Source IP Address	The IP address segment that needs to be filtered When the IP segment is null, it refers to all the IP addresses.
Mode	The mode includes the following: ▯ **Discard** ▯ **Permit**
Service List	Specify the service that is permitted or denied to access.

2. Configure the service control parameters, and then click **Add**.
3. (Optional) Modify the remote access port of the specified service.

i. Click **Click here to modify Remote Access Port of local services** to open the remote access port modification page, see Figure 40.

Figure 40 Modify Remote Access port



ii. Click  of the service type and modify the port in the **Port** text box.

iii. Click **Modify**.

The service control settings are configured.

The users with the specified IP addresses are permitted or denied to access the services that the ZXHN H108N device provides.

7.6 Configuring ALG

The ZXHN H108N device supports the ALG function, which allows the system to convert the private addresses to the public addresses in the packets for the security purpose.

This procedure introduces how to configure the ALG settings.

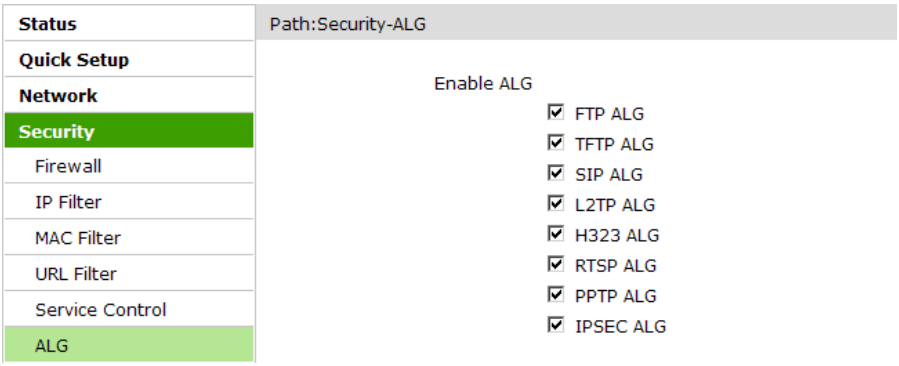
Context

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

Steps

1. On the navigation tree, click [**Security→ ALG**]. The ALG configuration page is displayed, see Figure 41.

Figure 41 ALG



2. Select the ALG services by selecting the corresponding options, and then click **Submit**.

8 Application

8.1 Configuring DDNS

ZXHN H108N supports the DDNS function. This procedure introduces how to configure DDNS to enable the host that has a dynamic IP address to provide the domain name service.

Prerequisite

Before configuring DDNS, make sure that:

- The inbound connection is enabled.
- The domain name has been registered.

Context

DNS is the way in which a URL or domain is converted to an IP address. In many home networking environments, the DSL IP address is provided by DHCP and therefore changes from time to time. Dynamic DNS (DDNS) allows you to have a website such as www.my-site.com in which the IP address is dynamically assigned.

After DDNS is applied, the device that has the dynamic IP address can also provide the domain name service. For example, when the device obtains an IP address through xDSL dial-up or DHCP server dynamic allocation, the device provides the domain name service. If the device IP address changes, it does not affect the subscriber's access to the host by using the domain name.

Steps

1. On the navigation tree, click [**Application**→ **DDNS**]. The DDNS configuration page is displayed, see Figure 42.

Figure 42 DDNS

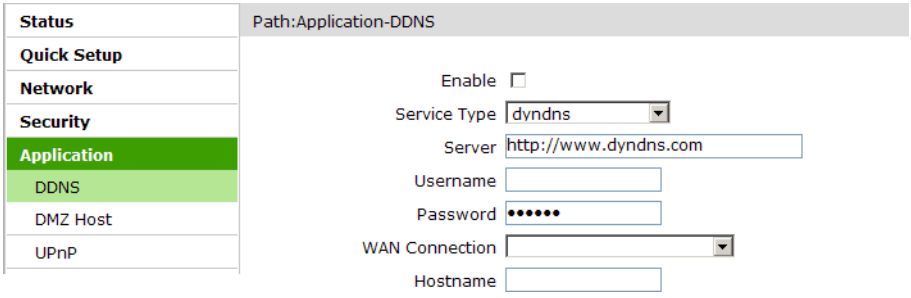


Table 29 lists the DDNS parameters.

Table 29 DDNS Parameters

Parameter	Description
Enable	Select to enable the DDNS function.
Service Type	DDNS service types
Server	Server address If the GNUDIP HTTP is used, the server address is a URL. By default, it is http://www.dyndns.com.
Username	DDNS server user name
Password	DDNS server password
WAN Connection	WAN connection type
Hostname	Host name corresponding to the user It takes effect only when the GNUDIP protocol is used.

2. Configure the DDNS parameters, and then click **Submit**.

8.2 Configuring DMZ Host

This procedure introduces how to configure the DMZ host for the specified WAN connection, so that the computers at the LAN side can provide services to the devices at the Internet side.

Context

By default, all the ports are opened.

Steps

1. On the navigation tree, click [**Application**→ **DMZ Host**]. The DMZ host configuration page is displayed, see Figure 43.

Figure 43 DMZ Host

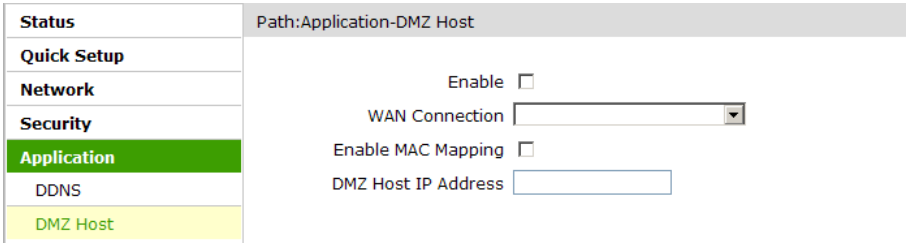


Table 30 lists the DMZ host parameters.

Table 30 DMZ Host Parameters

Parameter	Description
Enable	Enable the DMZ host function.
WAN Connection	The WAN connection that the computer at the LAN side uses to provide services to the devices at the Internet side.
Enable MAC Mapping	Enable the MAC mapping function. Enabled the MAC Mapping to configure **DMZ Host MAC Address**.
DMZ Host IP Address	IP address of the LAN-side host.
DMZ Host MAC Address	MAC address of the LAN-side host. When enabled **Enable MAC Mapping** to configure this parameter.

Note:

If the DMZ function is enabled, all the ports of the DMZ host machine are opened to the outside world, and DMZ host machine will provide services to the outside world through DNAT.

2. Configure the DMZ host parameters, and then click **Submit**.

8.3 Configuring UPnP

This procedure introduces how to configure UPnP function, which allows the device to dynamically join a network to obtain an IP address, announce its functions, and know the functions of other devices.

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

Steps

1. On the navigation tree, click [**Application**→ **UPnP**]. The UPnP configuration page is displayed, see Figure 44.

Figure 44 UPnP

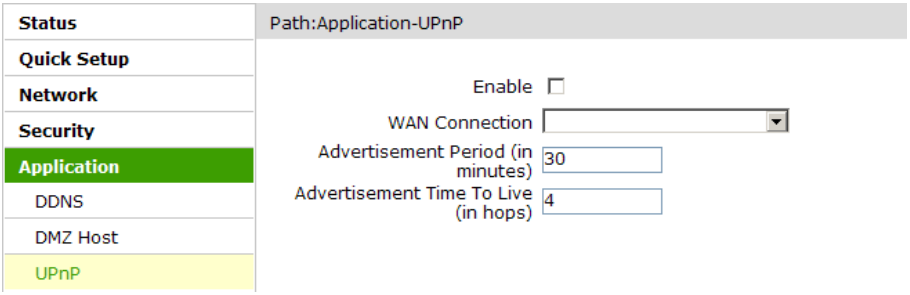


Table 31 lists the UPnP parameters.

Table 31 UPnP Parameters

Parameter	Description
Enable	Select this option 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 packets during this period, it indicates that the device is invalid. By default, the period is 30 minutes.
Advertisement Time To Live (in hops)	The TTL (Time to live) for the advertisement. The advertisement will be abandoned after it has been transferred for the specified times by the routers. The default value is 4.

2. Configure the UPnP parameters, and then cick **Submit**.

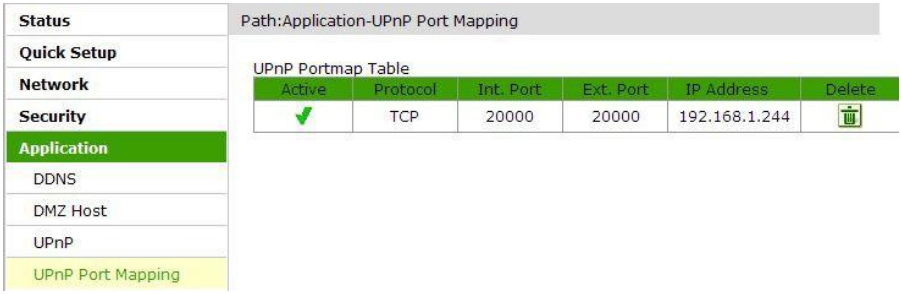
8.4 Displaying UPnP Port Mapping

This procedure introduces how to display the UPnP port mapping information, including the protocol, port, and IP address.

Steps

1. On the navigation tree, click [**Application→ UPnP Port Mapping**]. The UPnP port mapping page is displayed, see Figure 45.

Figure 45 UPnP Port Mapping



Note:

Protocol, ***Int.Port***, ***Ext.Port*** *and* ***IP Address*** *are configured by external tool.*

2. (Optional) Click **Refresh** to display the latest information.

8.5 Configuring Port Forwarding

This procedure introduces how to configure port forwarding so that a computer from the external network can access the LAN-side server through the CPE WAN connection.

Context

If you have local servers for different services and you want to make them publicly accessible, you need to specify the port forwarding policy. With NAT applied, it translates the internal IP addresses of these servers to a single IP address that is unique on the Internet.

To the Internet users, all virtual servers on your LAN have the same IP Address. This IP Address is allocated by your ISP. This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use Dynamic DNS feature to allow users to connect to your virtual servers by using a URL, instead of an IP address.

Steps

1. On the navigation tree, click [**Application→ Port Forwarding**]. The port forwarding configuration page is displayed, see Figure 46.

Figure 46 Port Forwarding

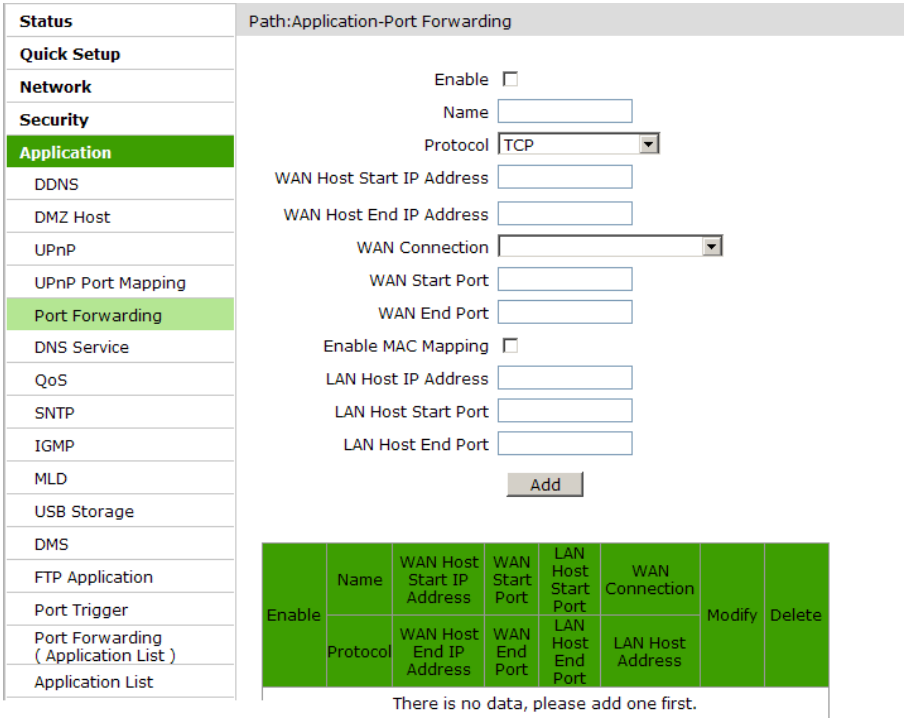


Table 32 lists the port forwarding parameters.

Table 32 Port Forwarding Parameters

Parameter	Description
Enable	Enable port forwarding function.
Name	Name of the port forwarding rules
Protocal	Protocol name, including TCP, UDP, as well as TCP AND UDP protocols. The default protocol is TCP.
WAN Host Start/End IP Address	Start/End IP address of the WAN-side computer
WAN Connection	WAN connection that is used to access the virtual host
WAN Start/End Port	Start/End port number of the WAN-side computer
Enable MAC Mapping	Enable MAC Mapping.
LAN Host IP Address	IP address of the LAN-side host
LAN Host MAC Address	MAC address of the LAN-side host
LAN Host Start/End Port	Start/End port number of the LAN-side host

2. Click **Submit**.

8.6 DNS Service

This section includes the following:

- Configuring Domain Name
- Configuring Hosts
- Configuring DNS

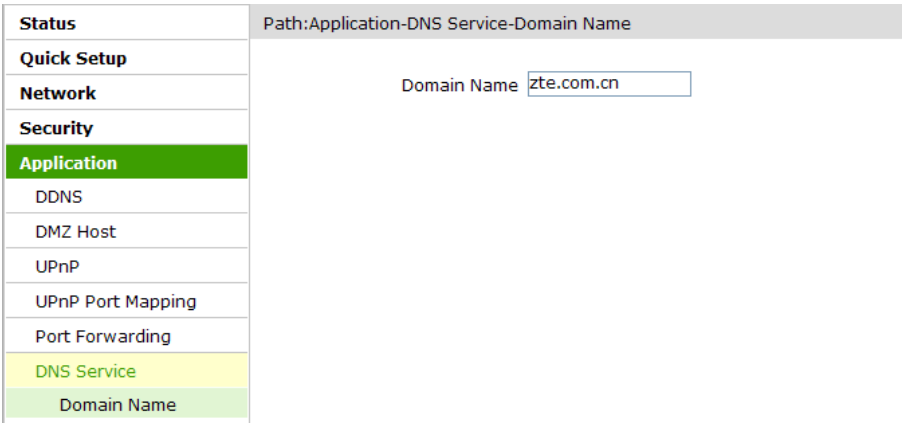
8.6.1 Configuring Domain Name

This procedure introduces how to configure the domain name to add the device to the corresponding network domain.

Steps

1. On the navigation tree, click [**Application→ DNS Service→ Domain Name**]. The domain name configuration page is displayed, see Figure 47.

Figure 47 Domain Name



2. Type the domain name in the **Domain Name** text box.
3. Click **Submit**.

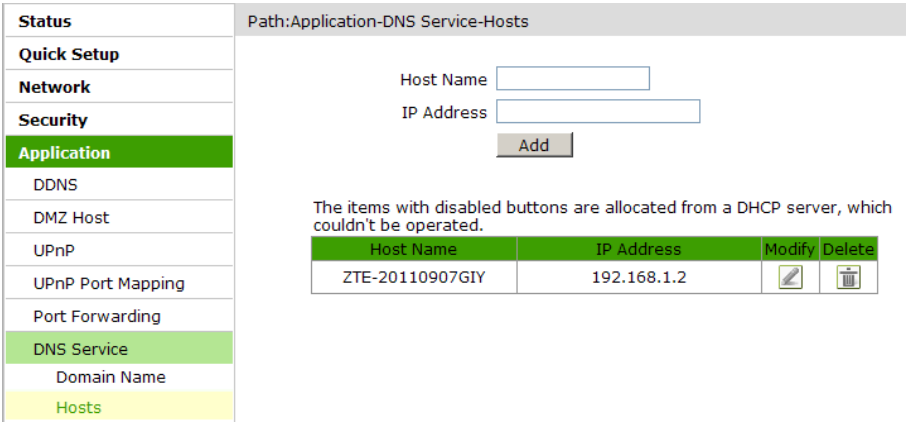
8.6.2 Configuring Hosts

This procedure introduces how to configure the mapping relationship between the user-side host name and IP address.

Steps

1. On the navigation tree, click [**Application**→ **DNS Service**→ **Hosts**]. The host configuration page is displayed, see Figure 48.

Figure 48 Hosts



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

3. Click **Add**.

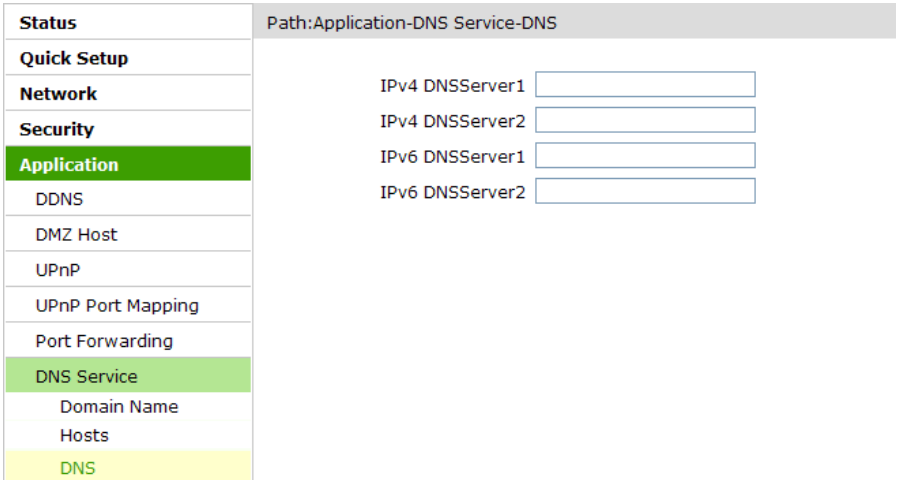
8.6.3 Configuring DNS

This procedure introduces how to configure the DNS server IP address.

Steps

1. On the navigation tree, click [**Application**→ **DNS Service**→ **DNS**]. The DNS configuration page is displayed, see Figure 49.

   Figure 49 DNS



2. Type the IP address of the DNS server assigned by the ISP.
3. Click **Submit**.

8.7 QoS

This section includes the following:

- Configuring Basic QoS Parameters
- Configuring QoS Classification
- Conducting Queue Management
- Configuring Committed Access Rate

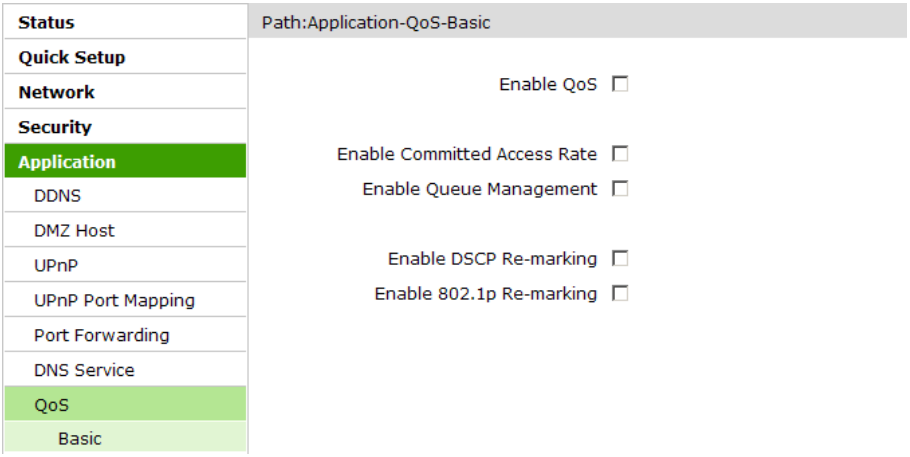
8.7.1 Configuring Basic QoS Parameters

This procedure introduces how to configure the basic QoS parameters.

Steps

1. On the navigation tree, click [**Application**→ **QoS**→ **Basic**]. The basic QoS parameter configuration page is displayed, see Figure 50.

   Figure 50 Basic QoS Parameters



2. Select **Enable QoS** to enable the QoS function, and then specify other parameters.
3. Click **Submit**.

8.7.2 Configuring QoS Classification

This procedure introduces how to configure the QoS classification rules, including layer-2 protocol, IP address range, and MAC address range.

Prerequisite

Before configuring QoS classification, make sure that the basic QoS configuration is completed.

Context

QoS is a network security mechanism that handles network transmission delay and congestion.

Steps

1. On the navigation tree, click [**Application**→ **QoS**→ **Classification**]. The QoS classification configuration page is displayed, see Figure 51.

Figure 51 QoS Classification

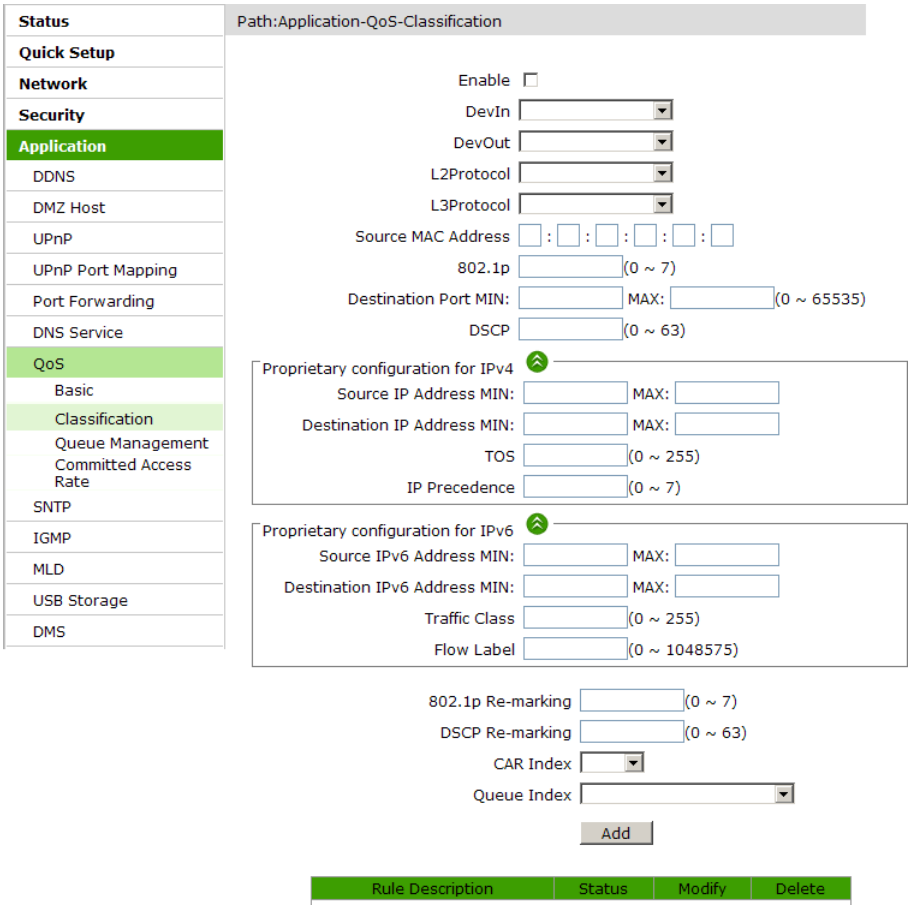


Table 33 lists the QoS classification parameters.

Table 33 QoS Classification Parameters

Parameter	Description
Enable	Enable the QoS classification
DevIn	Data flow ingress
DevOut	Data flow egress
L2Protocol	The layer 2 protocol includes IPv4, IPv6, ARP, and PPPoE.
L3Protocol	The layer 3 protocol includes TCP, UDP, and ICMP.
Source MAC Address	Source host MAC address

Parameter	Description
802.1p	Range: 0~7
Destination Port MIN/MAX	Destination port range
DSCP	Range: 0~63
Source IP address MIN/MAX	Source IP address range
Destination IP address MIN/MAX	Destination IP address range
TOS	Range: 0~255
IP Precedence	Range: 0~7
Source IPv6 Address MIN/MAX	Source IPv6 address range
Destination IPv6 Address MIN/MAX	Destination IPv6 address range
Traffic Class	Range: 0~255
Flow Label	Range: 0~1048575
802.1p Re-marking	802.1P identifier value Range: 0~7
DSCP Re-marking	DSCP identifier Range: 0~63
CAR Index	CAR index
Queue Index	QoS rule number Range: 1~8

2. Configure the QoS classification parameters, and then click **Add**.

8.7.3 Conducting Queue Mangement

This procedure introduces how to configure the QoS queue management parameters, including the priority, algorithm, and weight.

Prerequisite

Before managing queue index, make sure that:

- The basic QoS configuration is completed.
- The queue management function is enabled.

Steps

1. On the navigation tree, click [**Application→ QoS→ Queue Management**]. The queue management page is displayed, see Figure 52.

Figure 52 Queue Management

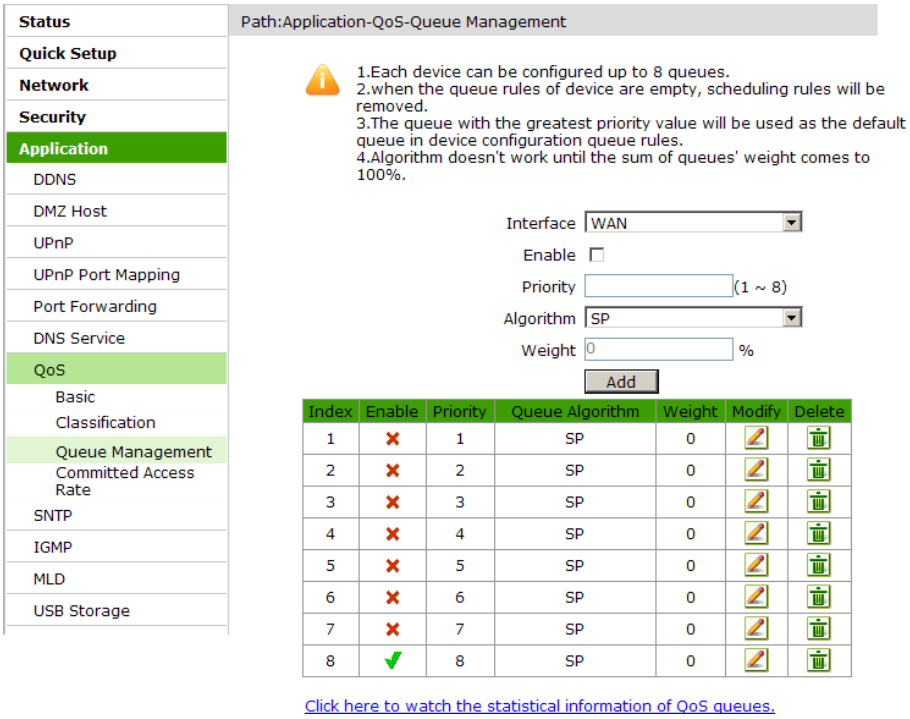


Table 34 lists the QoS Management parameters.

Table 34 Queue Management Parameters

Parameter	Description
Interface	This option includes **WAN** or **LAN**.
Enable	Enable the queue management function.
Priority	Queue priority. Range: 1 ~ 8
Algorithm	Queue algorithm. ▯ SP ▯ DWRR
Weight	The weight for the DWRR algorithm.

2. Click  of one index, and select the **Enable** check box.
3. Specify the parameters, and then click **Modify** to enable the specified queue index.

8.7.4 Configuring Committed Access Rate

This procedure introduces how to configure the committed access rate for the specified LAN interface or SSID.

Prerequisite

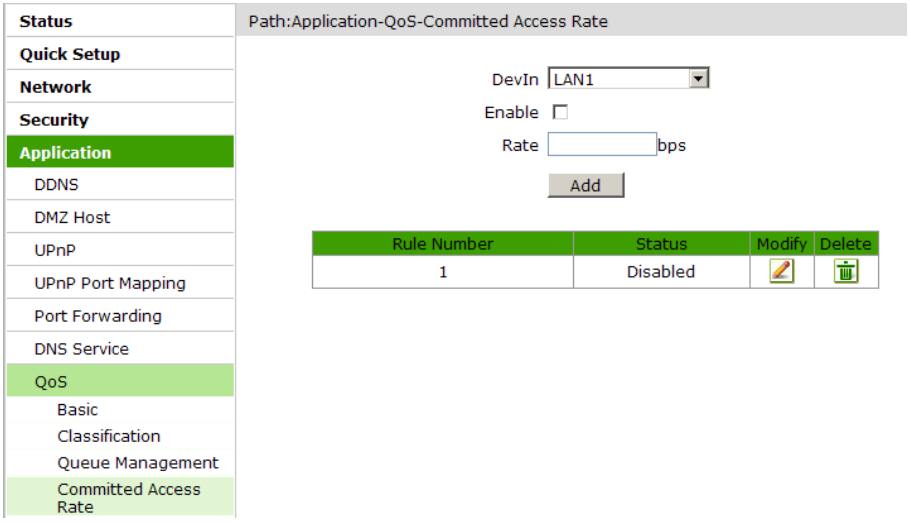
Before configuring committed access rate, make sure that:

- The basic QoS configuration is completed.
- The global committed access rate function is enabled.

Steps

1. On the navigation tree, click [**Application→ QoS→ Committed Access Rate**]. The committed access rate configuration page is displayed, see Figure 53.

   Figure 53 Committed Access Rate



2. Select the WAN interface, LAN interface or SSID from the **DevIn** drop-down list, enable the committed access rate function, and then configure the rate.
3. Click **Add**.

The committed access rate for the specified LAN interface or SSID is configured.

8.8 Configuring SNTP

This procedure introduces how to configure SNTP to synchronize the device time with the server time.

Steps

1. On the navigation tree, click [**Application**→ **SNTP**]. The SNTP configuration page is displayed, see Figure 54.

Figure 54 SNTP

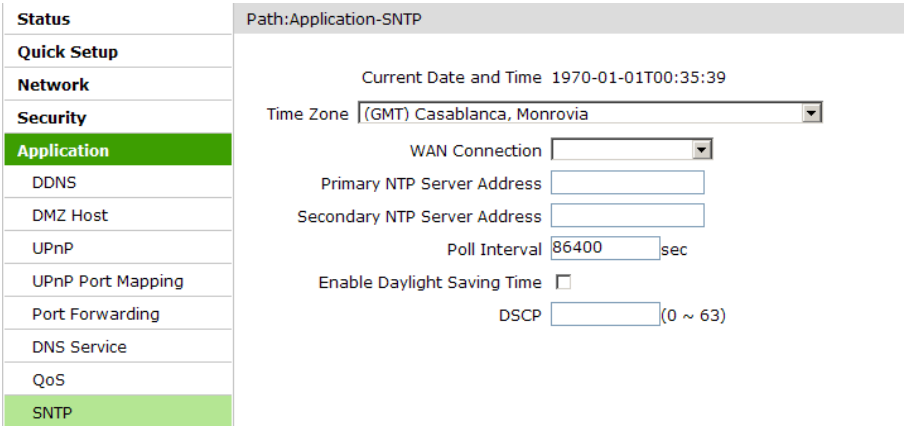


Table 35 lists the SNTP parameters.

Table 35 SNTP Parameters

Parameter	Description
Time Zone	Time zone
WAN Connection	Select the WAN connection
Primary NTP Server Address	IP address/realm name of the primary NTP server
Secondary NTP Server Address	IP address/realm name of the secondary NTP server
Poll Interval	Interval of time synchronization Unit: second
Enable Daylight Saving Time	Enable the Daylight Saving Time.
DSCP	Range: 0~63

2. Configure the SNTP parameters, and then click **Submit**.

8.9 IGMP

This section includes the following:

- Configuring WAN connection

- Configuring IGMP Basic Parameters

8.9.1 Configuring WAN Connection

This procedure introduces how to configure the WAN connection for IGMP function.

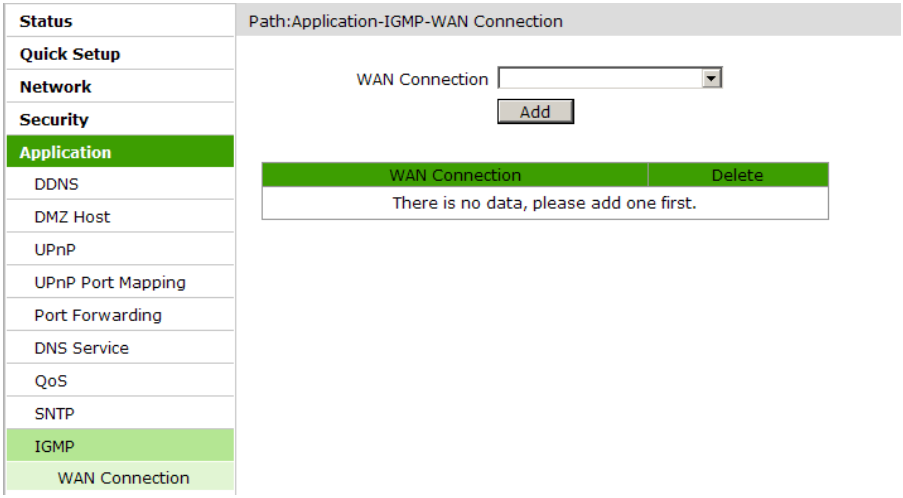
Prerequisite

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

Steps

1. On the navigation tree, click [**Application→ IGMP→ WAN Connection**]. The WAN connection configuration page is displayed, see Figure 55.

   Figure 55 IGMP WAN Connection



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

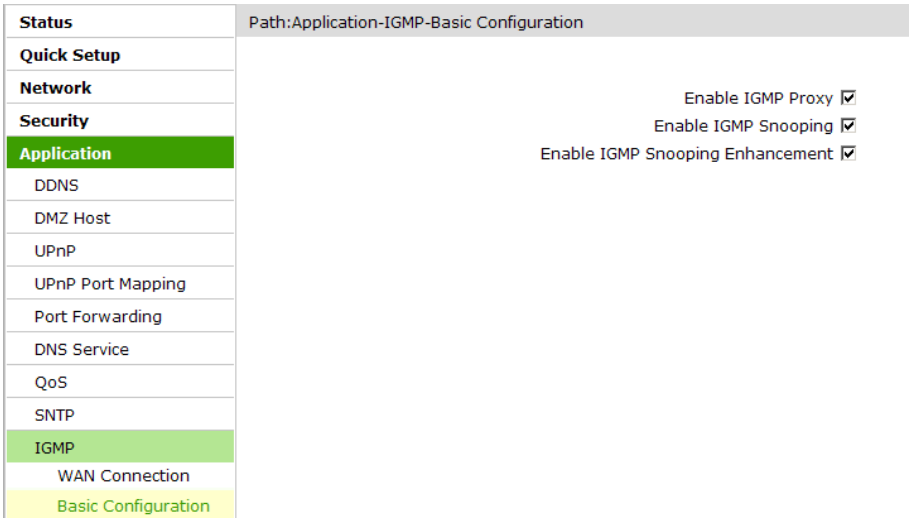
8.9.2 Configuring IGMP Basic Parameters

This procedure introduces how to enable the basic IGMP function.

Steps

1. On the navigation tree, click [**Application→ IGMP→ Basic Configuration**]. The IGMP basic configuration page is displayed, see Figure 56.

Figure 56 IGMP Basic Configuration



2. Enable the IGMP functions, and then click **Submit**.

8.10 MLD

This section includes the following:

- Configuring MLD Snooping
- Configuring MLD Proxy

8.10.1 Configuring MLD Snooping

This procedure introduces how to enable the MLD snooping function.

Prerequisite

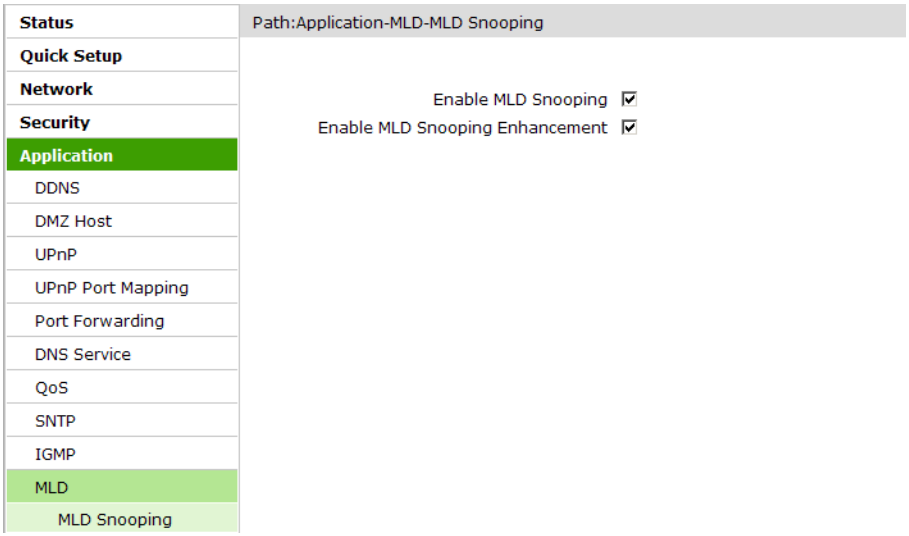
Before configuring MLD snooping, make sure that:

- IPv6 service is available.
- IPv6 WAN connection is created.

Steps

1. On the navigation tree, click [**Application→ MLD→ MLD Snooping**]. The MLD snooping configuration page is displayed, see Figure 57.

Figure 57 MLD Snooping



2. Enable the MLD snooping functions, and then click **Submit**.

8.10.2 Configuring MLD Proxy

This procedure introduces how to enable the MLD proxy function for the specified IPv6 WAN connection.

Prerequisite

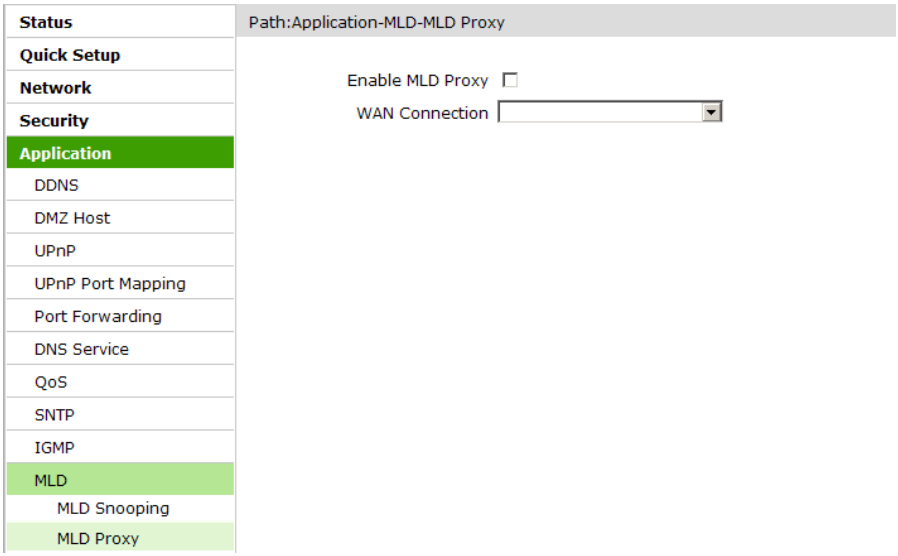
Before configuring MLD proxy, make sure that:

- IPv6 service is available.
- IPv6 WAN connection is created.

Steps

1. On the navigation tree, click [**Application**→ **MLD**→ **MLD Proxy**]. The MLD proxy configuration page is displayed, see Figure 58.

Figure 58 MLD Proxy



2. Select a WAN connection from the **WAN Connection** drop-down list, and select the **Enable MLD Proxy** check box to enable the MLD proxy function.
3. Click **Submit**.

8.11 Displaying USB Storage Information

This procedure introduces how to check the USB storage device information.

Prerequisite

Before displaying USB storage information, make sure that the USB storage device is connected to the ZXHN H108N device.

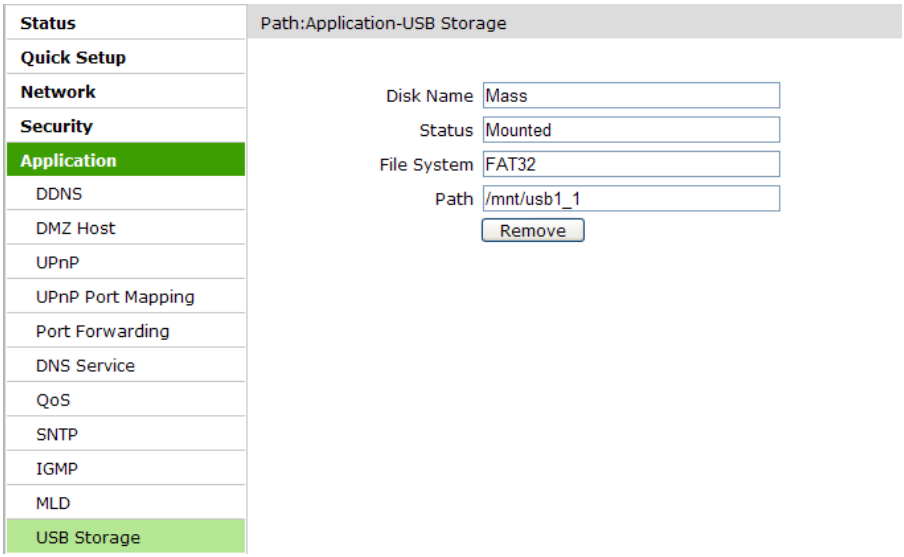
Context

The FTP protocol is used to manage the USB storage device.

Steps

1. On the navigation tree, click [**Application**→ **USB Storage**]. The USB storage information is displayed, see Figure 59.

Figure 59 USB Storage



2. (Optional) Click **Refresh** to display the latest information.

The USB storage device information is displayed.

8.12 Configuring DMS

This procedure introduces how to configure the DMS settings.

Prerequisite

Before configuring DMS, make sure that:

- The UPnP function is enabled.
- The USB device is connected to the ZXHN H108N device.

Context

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

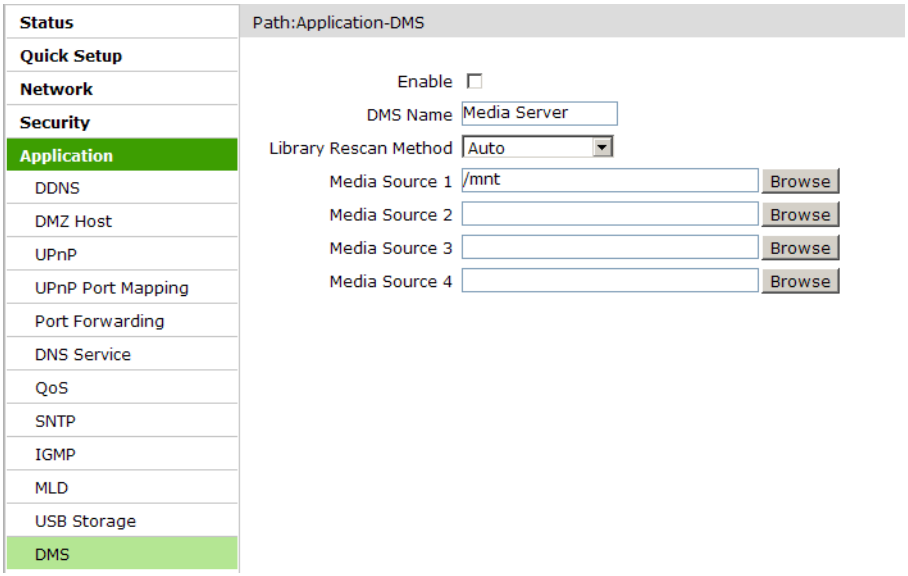
If the DMS function in enabled on the ZXHN H108N device, any client that supports UPnP function can use the specified DMP (for example, windows media player) to watch the media files or photos stored in the USB storage device.

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

Steps

1. On the navigation tree, click [**Application→ DMS**]. The DMS configuration page is displayed, see Figure 60.

   Figure 60 DMS



2. Enable the DMS function, and specify the place to store the media files.

   Note:

   By default, the media source is /mnt, that is the root directory of the USB device.

   You can change the root directory to other directory of the USB storage device.

3. After the configuration, click **Submit**.

8.13 Configuring FTP Application

This procedure introduces how to configure the FTP application.

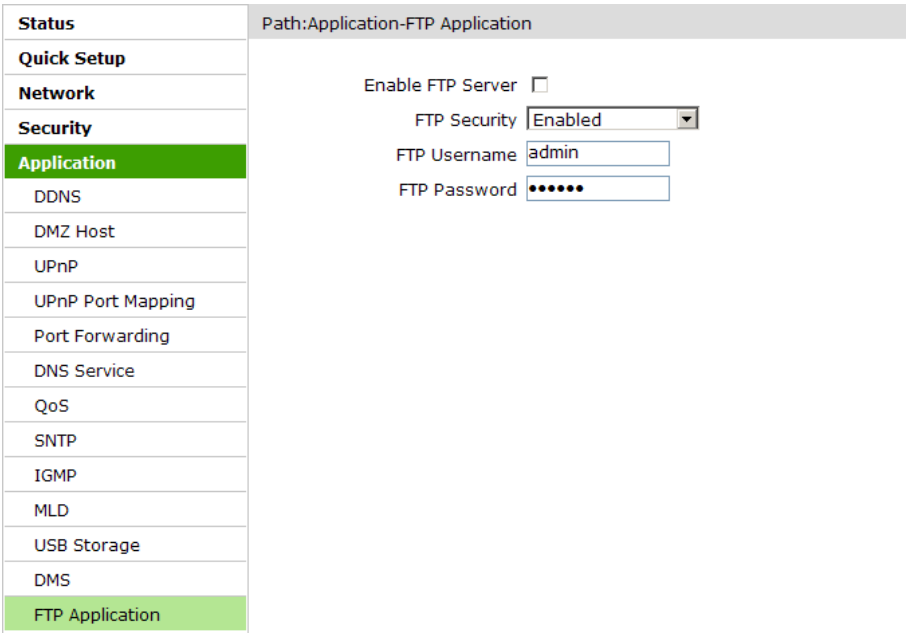
Prerequisite

Before configuring FTP application, make sure a USB storage device is connected to the ZXHN H108N device.

Steps

1. On the navigation tree, click [**Application→ FTP Application**]. The FTP application configuration page is displayed, see Figure 61.

Figure 61 FTP Application



2. Select the **Enable FTP Server** check box, and specify other parameters, and then click **Submit**.

The FTP application is configured.

You can upload or download the files to the specified FTP address of the ZXHN H108N device.

8.14 Configuring Port Trigger

This procedure introduces how to configure the port triggering function.

When one port is configured to be the triggering port, if one application uses that triggering port to setup a connection to the outside, the ZXHN H108N device will forward the outside connection to the internal forwarding port.

Context

The port triggering function is used to protect the ports. The system will not open these ports unless these ports are triggered.

Steps

1. On the navigation tree, click [**Application→Port Trigger**]. The port trigger page is displayed, see Figure 62.

Figure 62 Port Trigger

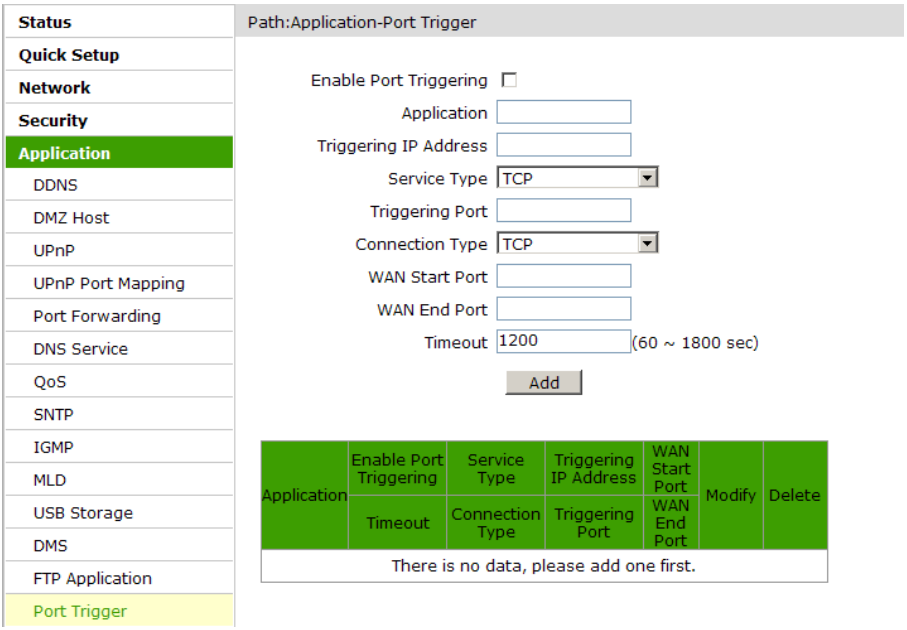


Table 36 lists the port trigger parameters.

Table 36 Port Trigger Parameter

Parameter	Description
Enable Port Triggering	Enable the port triggering function.
Application	Name of the port triggering item
Triggering IP Address	IP address of the computer in the LAN side
Service Type	The service type of the application including **TCP**, **UDP**, and **TCP AND UDP**
Triggering Port	The port that the application uses
Connection Type	The connection type that is used to connect the outside, including **TCP**, **UDP**, and **TCP AND UDP**

Parameter	Description
WAN Start/End Port	Specify the port range of the device protocol that the triggering port maps, that is, the layer-4 port number of the packets. Once the device accesses the triggering port, the service between the start port and end port will be enabled. The Start Port and End Port must be specified and meet the following conditions. ▯ The end port number is larger than the start port number. ▯ The difference between the end port number and the start port number is less than nine.
Timeout	The time when no traffic occurs

2. Configure the port trigger parameters according to the request.
3. Click **Add**.

8.15 Configuring Port Forwarding (Application List)

This procedure introduces how to configure the port forwarding function.

Prerequisite

The application name has been created.

Steps

1. On the navigation tree, click [**Application→Port Forwarding (Application List)**]. The Port Forwarding (Application List) is displayed, see Figure 63.

Figure 63 Port Forwarding (Application List)

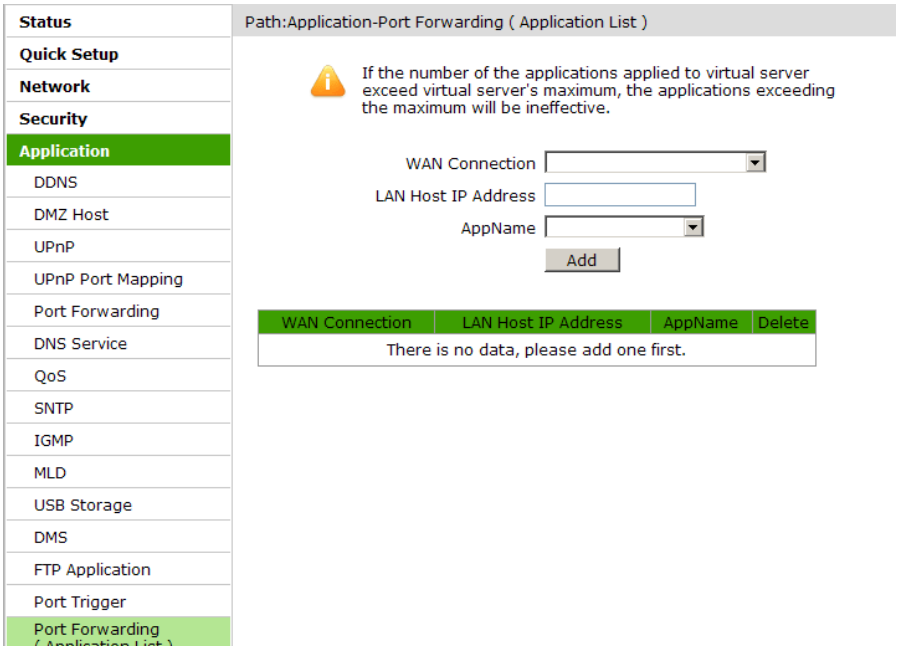


Table 37 lists the port trigger parameters.

Table 37 Port Forwarding (Application List) Parameter

Parameter	Description
WAN Connection	WAN connection that is used to access the virtual host
LAN Host IP Address	IP address of the LAN-side host
AppName	Application name

2. After the configuration, click **Add**.

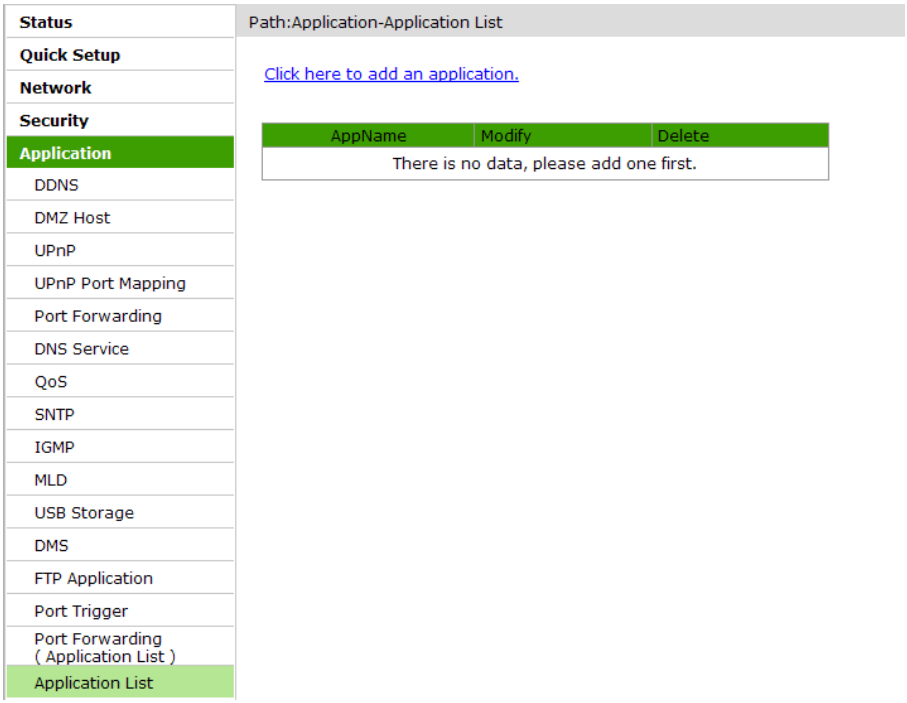
8.16 Configuring Application List

This procedure introduces how to configure the application list function.

Steps

1. On the navigation tree, click [**Application→Application List**]. The application list page is displayed, see Figure 64.

Figure 64 Application List



2. Click **Click here to add an application**. The application configuration page is displayed, see Figure 65.

Figure 65 Application List

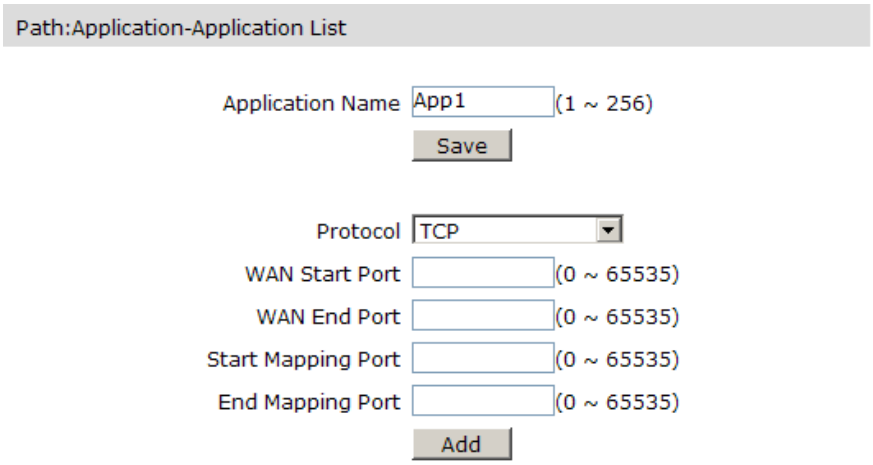


Table 38 lists the application list parameters.

Table 38 Application List Parameter

Parameter	Description
Application Name	Application name
Protocal	Protocol of the permitted packet including **TCP**, **UDP**, and **TCP AND UDP**
WAN Start/End Port	Port number range of the WAN-side hosts
Start/End Mapping Port	Port number range of the mapping-side hosts

3. Configure the application list parameters according to the request.
4. Click **Add**.

9 Administration

9.1 TR-069

This section includes the following:

- Configuring TR-069 Basic Parameters
- Importing TR-069 Certificates

9.1.1 Configuring TR-069 Basic Parameters

ZXHN H108N supports TR-069 protocol. This procedure introduces how to configure the TR-069 basic parameters.

Prerequisite

Before configuring TR-069 basic parameters, make sure that:

- The WAN connection is configured.
- The TR-069 certificate is imported.

Context

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

Steps

1. On the navigation tree, click [**Administration**→ **TR-069**→ **Basic**]. The TR-069 basic parameter configuration page is displayed, see Figure 66.

Figure 66 TR-069 Basic Parameter

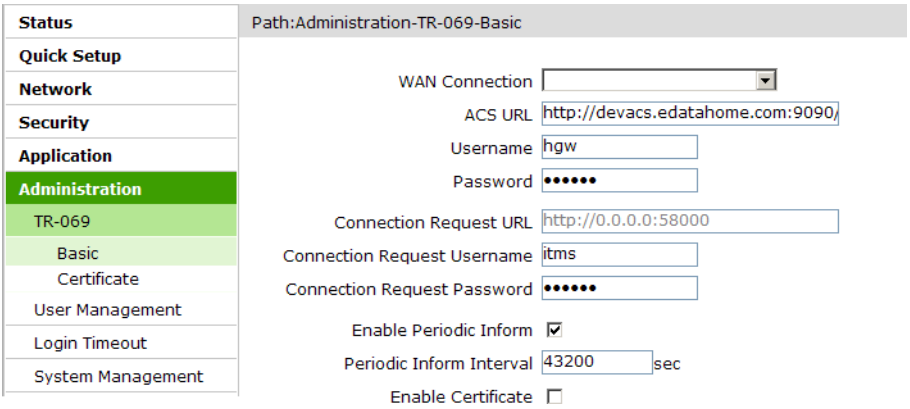


Table 39 lists the TR-069 basic parameters.

Table 39 TR-069 Basic Parameter

Parameter	Description
WAN Connection	WAN connection for the TR-069 service
ACS URL	The URL of the automatic configuration server that manages the device
Username/Password	User name and password for the ZXHN H108N device to log in to the automatic configuration server
Connection Request URL	Connection request URL, which is automatically generated by the system
Connection Request Username/Connection Request Password	User name and password for the TR-069 connection authentication that the automatic configuration server provides when it logs in to the ZXHN H108N device
Enable Periodic Inform	Enable the periodic inform function.
Periodic Inform Interval	Periodic inform interval of the device (unit: second)
Enable Certificate	Enable the TR-069 certificate. Before using the certificate, click [**Administration**→ **TR-069**→ **Certificate**] to open the certificate page, where you can import the certificate.

2. Configure the basic TR-069 parameters, and then click **Submit**.

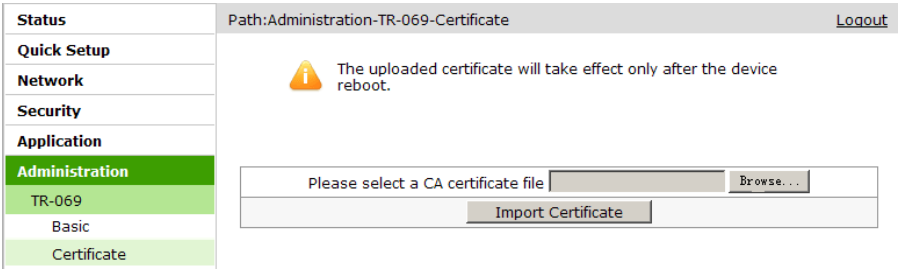
9.1.2 Importing TR-069 Certificates

This procedure introduces how to import the CA certificates.

Steps

1. On the navigation tree, click [**Administration→ TR-069→ Certificate**]. The certificate page is displayed, see Figure 67.

   Figure 67 Certificate



2. 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.

3. Click **Import Certificate**.

9.2 Managing Users

This procedure introduces how to manage the user accounts and rights.

Context

Table 40 lists the user rights.

Table 40 User Rights

Role	User Name and Password	Rights
Administrator	User name: admin Password: admin	The administrator has the privileges to configure all the parameters in the Web configuration pages.
User	User name: user Password: user	The common user can only perform the following operation: ▯ View the device or network information ▯ Software upgrade ▯ Modify the user name and password

Steps

1. On the navigation tree, click [**Administration→ User Management**]. The user management page is displayed, see Figure 68.

   Figure 68 User Management

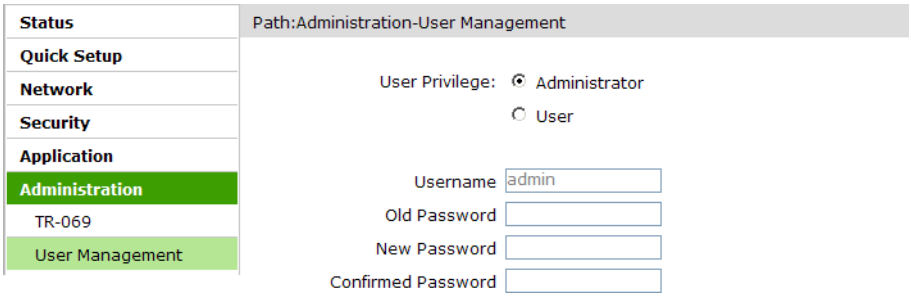


   Table 41 lists the user management parameters.

   Table 41 User Management Parameters

Parameter	Description
User Privilege	You can select **Administrator** or **User** to configure the accounts.
Username	The user name for the administrator or user privilege. The default user name of the administrator privilege is **admin**, which cannot be modified.
Old Password	The default passwords are as follows: ▯ Administrator: admin ▯ User: user
New Password	Specify the new password.
Confirmed Password	Confirm the new password.

2. Configure the user management parameters, and then click **Submit**.

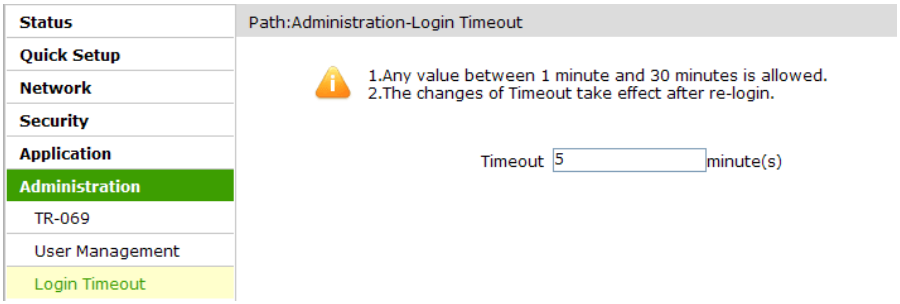
9.3 Configuring Login Timeout

This procedure introduces how to manage the login timeout. After the user logs in to the ZXHN H108N device, if no operations are conducted during the specified time, the user will log off.

Steps

1. On the navigation tree, click [**Administrator→ Login Timeout**]. The login timeout configuration page is displayed, see Figure 69.

   Figure 69 Login Timeout



2. Specify the time in the **Timeout** text box, and then click **Submit**.

The login timeout is configured. If no action is taken during the specified time, the configuration page will be closed, and the user will be in logout status.

9.4 System Management

This section includes the following:

- Managing the System
- Updating Software
- Managing User Configuration
- Managing Default Configuration

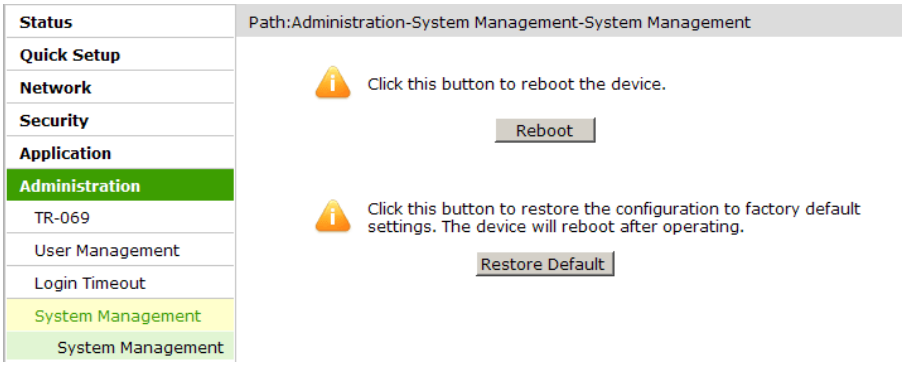
9.4.1 Managing the System

This procedure introduces how to reboot the device or restore the factory default settings.

Steps

1. On the navigation tree, click [**Administration→ System Management→ System Management**]. The system management page is displayed, see Figure 70.

Figure 70 System Management



2. On this page, you can perform the following operations:
   - Click **Reboot** to reboot the ZXHN H108N device.
   - Click **Restore Default** to restore the factory default settings.

9.4.2 Upgrading Software

This procedure introduces how to upgrade the software.

Prerequisite

Before upgrading software, make sure that the upgrade file is ready.

Context

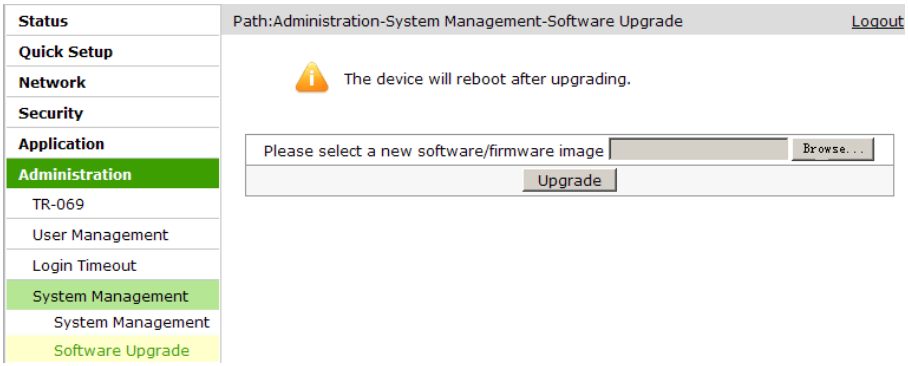
Caution!

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

Steps

1. On the navigation tree, click [**Administration→ System Management→ Software Upgrade**]. The software upgrade page is displayed, see Figure 71.

Figure 71 Software Upgrade



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

   Caution!

   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 page.

9.4.3 Managing User Configuration

This procedure introduces how to import or export the user configuration file.

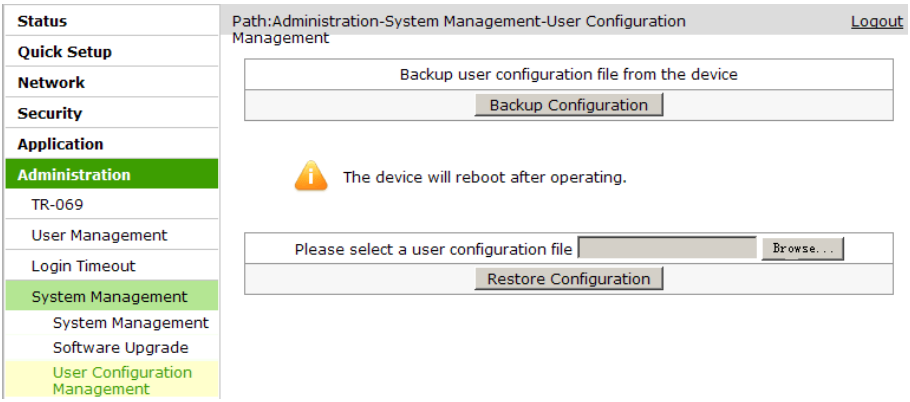
Context

User configuration refers to the customized configuration based on the factory defaults. The user can configure the device settings based on his own requirements, and the configuration can be backed up.

Steps

1. On the navigation tree, click [**Administration→ System Management→ User Configuration Management**]. The user configuration management page is displayed, see Figure 72.

Figure 72 User Configuration Management



2. On this page, you can perform the following operations:

   - Click **Backup Configuration** to export the user configuration file.
   - Click **Browse** to select the user configuration file, and then click **Restore Configuration** to restore the device to the user configuration.

   Note:

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

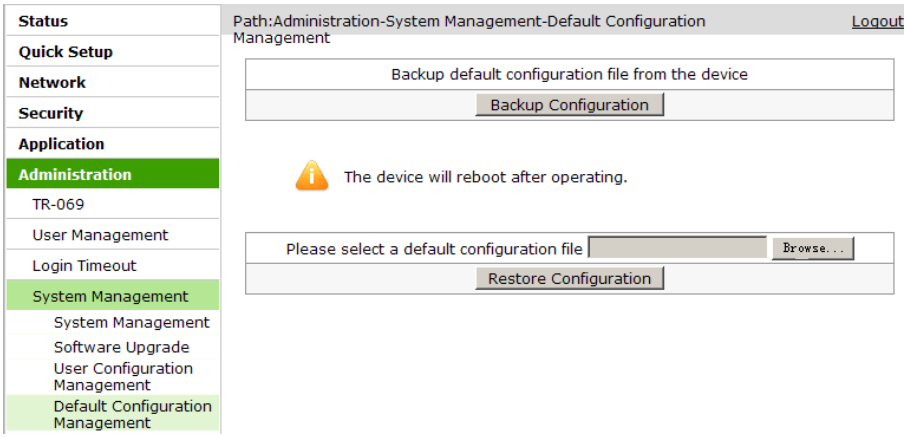
9.4.4 Managing Default Configuration

This procedure introduces how to import or export the default configuration file.

Steps

1. On the navigation tree, click [**Administration→ System Management→ Default Configuration Management**]. The default configuration management page is displayed, see Figure 73.

Figure 73 Default Configuration Management



2. On this page, you can perform the following operations:

   - Click **Backup Configuration** to export the default configuration file.
   - Click **Browse** to select the default configuration file, and then click **Restore Configuration** to restore the ZXHN H108N device to the default configuration.

   Note:

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

9.5 Managing Logs

This procedure introduces how to manage logs.

Steps

1. On the navigation tree, click [**Administration→ Log Management**]. The log management page is displayed, see Figure 74.

Figure 74 Log Management

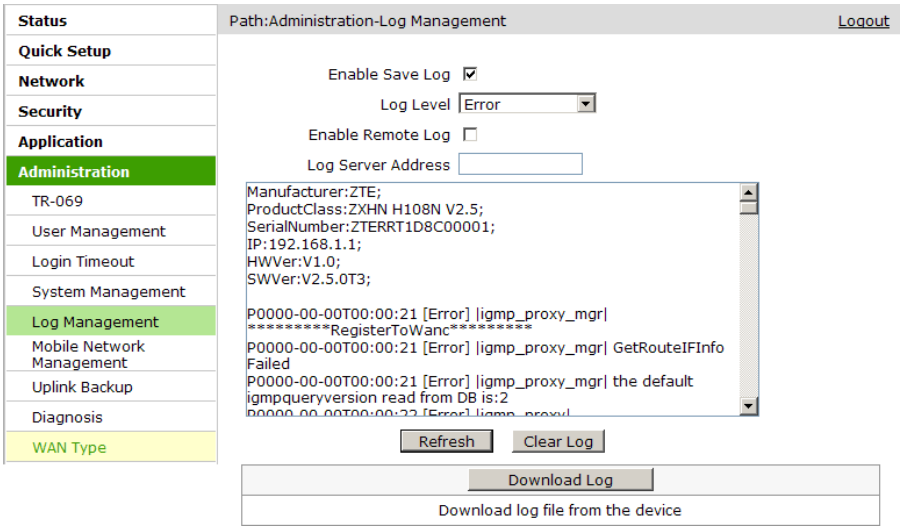


Table 42 lists the log management parameters and buttons.

Table 42 Log Management Parameters and Buttons

Item	Description
Enable Save Log	Select this option to save logs.
Log Level	There are eight levels, and they are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, and **Debug**. The options are listed in a descending order, and the **Emergency** is the highest level. When the log level is configured, only the logs of the configured log level and higher are saved.
Enable Remote Log	Select this option, and the device regularly sends the log to the log server.
Log Server Address	IP address of the log server
Refresh	Display the latest 20 logs in the text box.
Clear Log	Clear the current logs from the text box.
Download Log	Download the logs to the local disk.

2. Configure the log management parameters.
3. Click **Submit**.

The logs of the specified level are displayed in the text box.

```
Manufacturer:ZTE;
ProductClass:ZXHN H108N V2.5;
SerialNumber:;
IP:192.168.1.1;
HWVer:V1.0;
SWVer:V2.5.0T2;
```

9.6 Mobile Network Management

This section includes the following:

- Performing PIN Management
- Configuring Network Mode

9.6.1 Performing PIN Management

This procedure introduces how to perform the PIN management.

Prerequisite

Before performing PIN management, make sure that:

- 3G network card is ready.
- 3G WAN connection is created.

Steps

1. On the navigation tree, click [**Administration→ Mobile Network Management→ PIN Management**]. The PIN management page is displayed, see Figure 75.

Figure 75 PIN Management

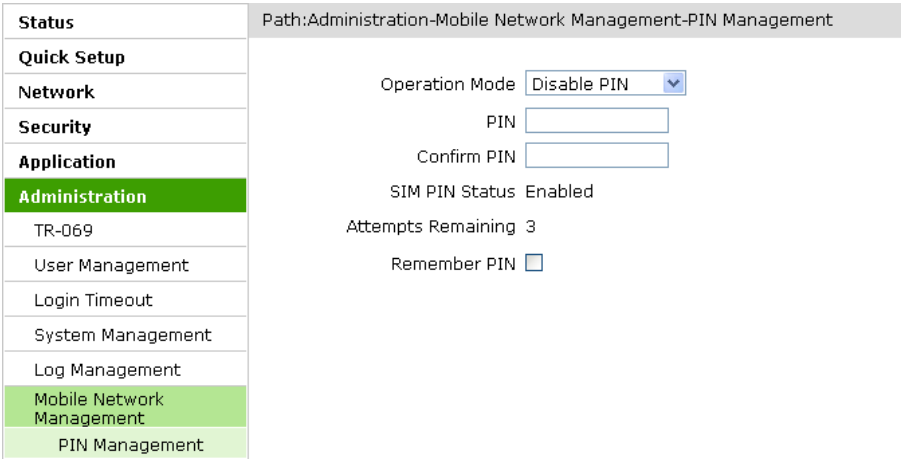


Table 43 lists the PIN configuration parameters.

Table 43 PIN configuration parameters

Parameter	Description
Operation Mode	Selecte the Operation Mode .
PIN	Type the PIN number.
Confirm PIN	Confirm the PIN number.
Remember PIN	Enable the remember PIN number function.

2. Configure the PIN management parameters, and then click **Submit**.

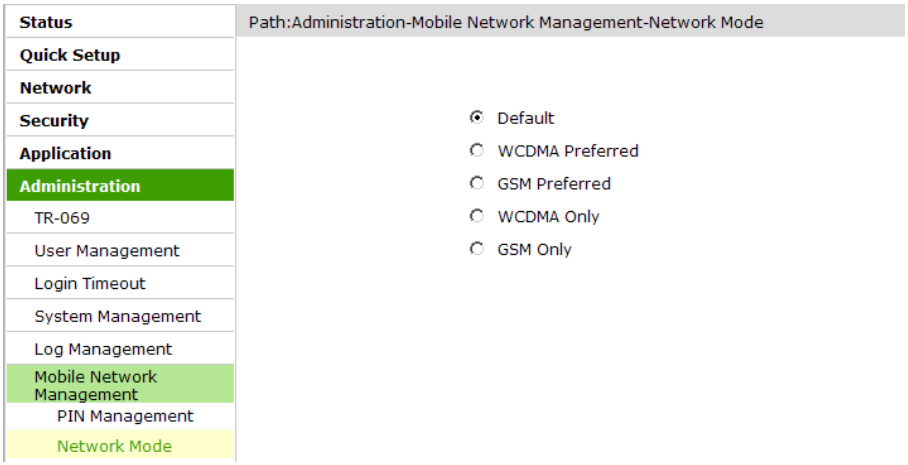
9.6.2 Configuring Network Mode

This procedure introduces how to select the 3G network mode.

Steps

1. On the navigation tree, click [**Administration→ Mobile Network Management→ Network Mode**]. The network mode page is displayed, see Figure 76.

Figure 76 Network Mode



2. Select one network mode, and click **Submit**.

Note:

The ZXHN H108N device only supports WCDMA 3G card for the moment. If the network mode is changed, it is necessary to unplug the card and plug it again to make the change come into effect.

9.7 Configuring Uplink Backup

ZXHN H108N supports DSL connection and 3G connection. When both DSL line and 3G card are available, DSL connection works as the primary uplink connection, and 3G connection works as the secondary uplink connections. If the DSL line fails to work, the 3G card works. When the DSL line resumes working, the 3G card automatically stops working.

This procedure introduces how to configure the switchover time between the primary connection and secondary connection.

Steps

1. On the navigation tree, click [**Administration→Uplink Backup**]. The uplink backup page is displayed, see Figure 77.

Figure 77 Uplink Backup

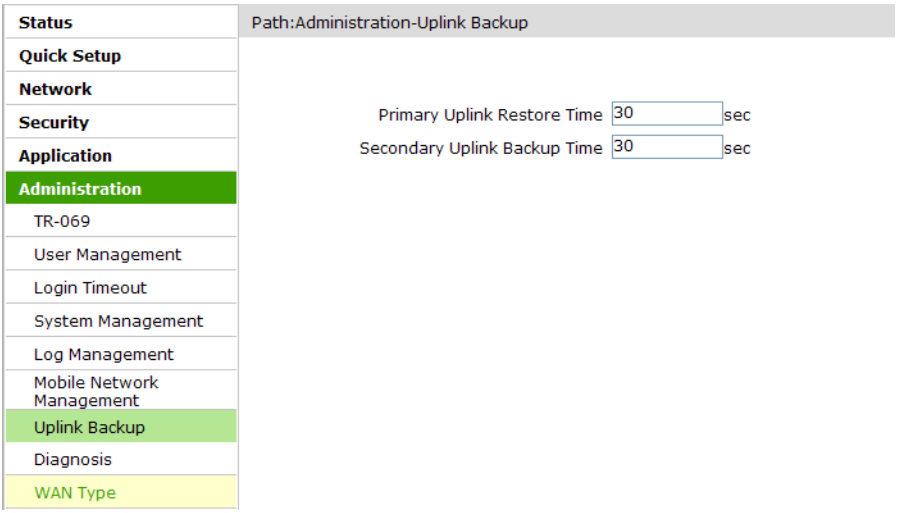


Table 44 lists the uplink backup parameters.

Table 44 Uplink Backup Parameter

Parameter	Description
Primary Uplink Restore Time	Specify the waiting time before switching to the primary connection and stop 3G connection after the primary connection works.
Secondary Uplink Backup Time	Specify the waiting time before dialing 3G connection after the primary connections stops working.

2. Configure the parameters, and then click **Submit**.

9.8 Diagnosis

This section includes the following:

- Diagnosing Network Connectivity
- Diagnosing Trace Route
- Diagnosing Simulation
- Performing AT Diagnosis
- Performing Mirror Configuration
- Diagnosing Line

- Diagnosing Ethernet Port
- Diagnosing PPPoE
- Diagnosing DNS
- Diagnosing IP
- Displaying MAC Table
- Displaying ARP Table

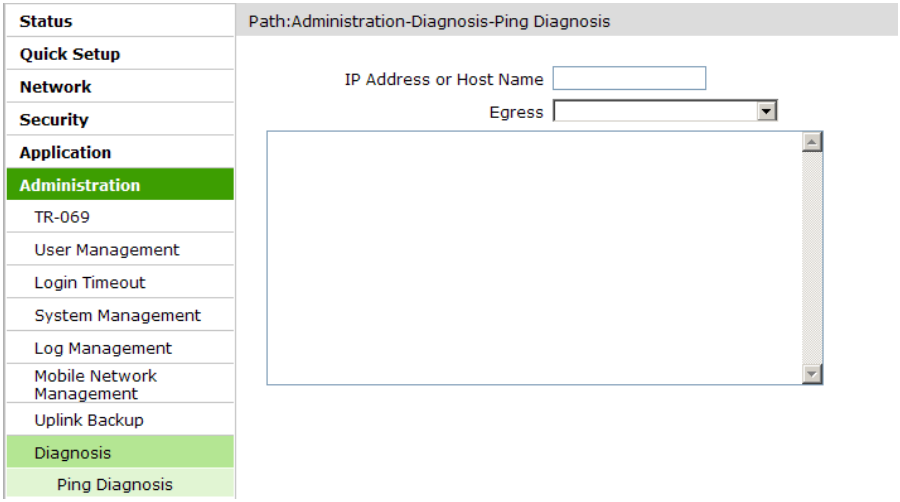
9.8.1 Diagnosing Network Connectivity

This procedure introduces how to diagnose the network connectivity.

Steps

1. On the menu bar, click [**Administration→ Diagnosis→ Ping Diagnosis**]. The ping diagnosis page is displayed, see Figure 78. On this page, you can select a WAN connection and test the connectivity with the specified address.

   Figure 78 Ping Diagnosis



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

```
PING 192.168.1.2 (192.168.1.2): 64 data bytes
Reply from 192.168.1.2: bytes=64 ttl=128 time=1.9ms seq=0
Reply from 192.168.1.2: bytes=64 ttl=128 time=0.6ms seq=1
Reply from 192.168.1.2: bytes=64 ttl=128 time=1.7ms seq=2
```

```
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.4/1.9 ms
```

The network connectivity between the ZXHN H108N device and specified IP address is diagnosed.

9.8.2 Diagnosing Trace Route

This procedure introduces how to display the information of the routes between the ZXHN H108N device and the specified address.

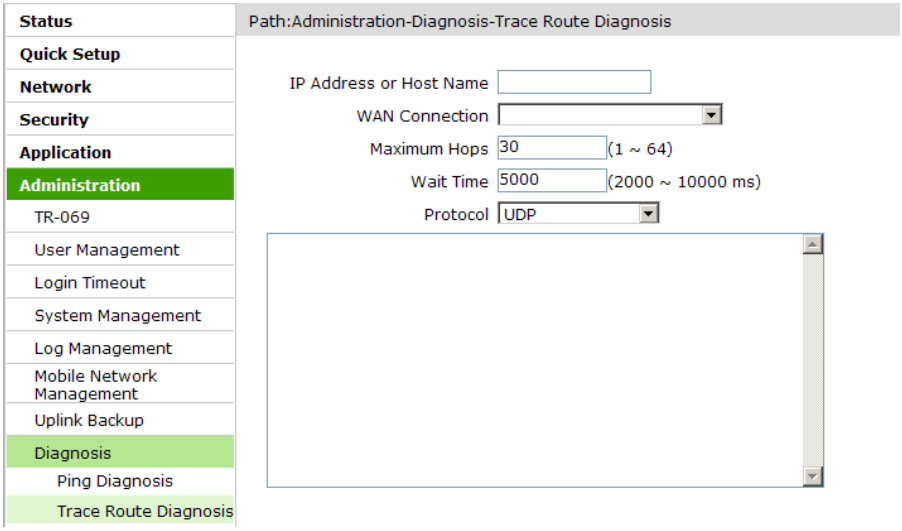
Prerequisite

Before the operation, make sure that the WAN connection is created.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ Trace Route Diagnosis**]. The trace route diagnosis page is displayed, see Figure 79.

   Figure 79 Trace Route Diagnosis



2. Type the IP address or host name in the **IP Address or Host Name** text box, select one WAN connection, specify the maximum hops, wait time, and protocol.
3. After the configuration, click **Submit**.

The information of the routers between the specified IP address and the ZXHN H108N device is displayed.

```
traceroute to 90.1.1.9 (90.1.1.9) ,40 byte packets
 1  * * * Request timed out.
 2  90.1.1.9 (90.1.1.9)  5 ms  4 ms  4 ms
Traceroute complete.
```

9.8.3 Diagnosing Simulation

Steps

1. On the navigation tree, click [**Administration→Diagnosis→Simulation**]. The **Simulation** page is displayed, see Figure 80.

   Figure 80 Diagnosing Simulation

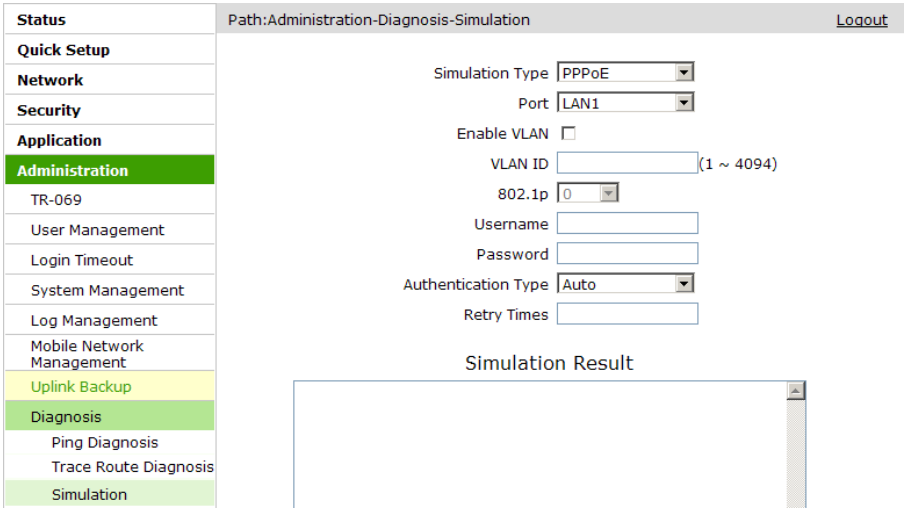


Table 45 lists the Diagnosing Simulation configuration parameters.

Table 45 Diagnosing Simulation parameters

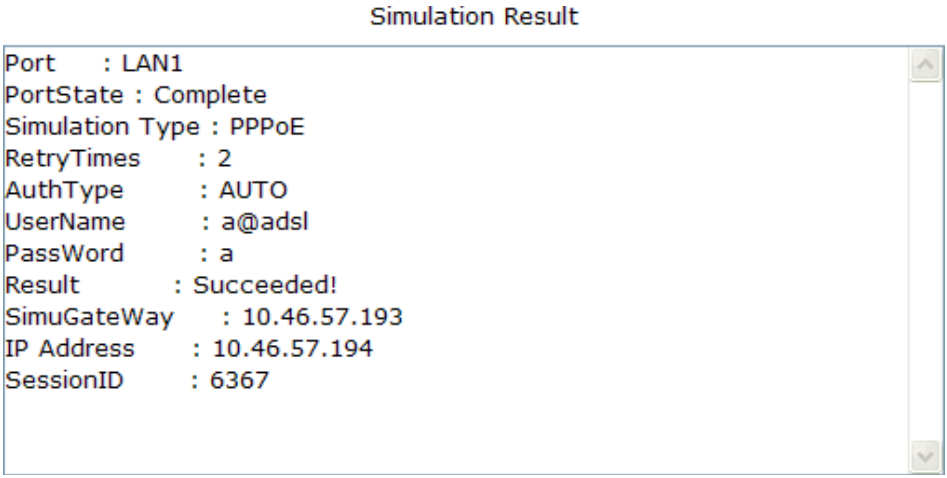
Parameter	Description
Simulation Type	Select the Simulation Type. The type includes **PPPoE** and **IPoE**.
Port	Select the port.
Enable VLAN	Enable the VLAN function.
VLAN ID	VLAN ID.
802.1p	Specify the 802.1p value to modify the service priority.

Parameter	Description
Username/Password	Username/Password provided by the ISP.
Authentication Type	The type includes **Auto**, **PAP**, and **CHAP**. By default, it is **Auto**.
Retry Times	Specify the retry times.

2. Configure the Diagnosing Simulation parameters, then click **Start**.

The information is displayed, as show in Figure 81.

Figure 81 Simulation Result



9.8.4 Performing AT Diagnosis

This procedure introduces how to diagnose the SIM card.

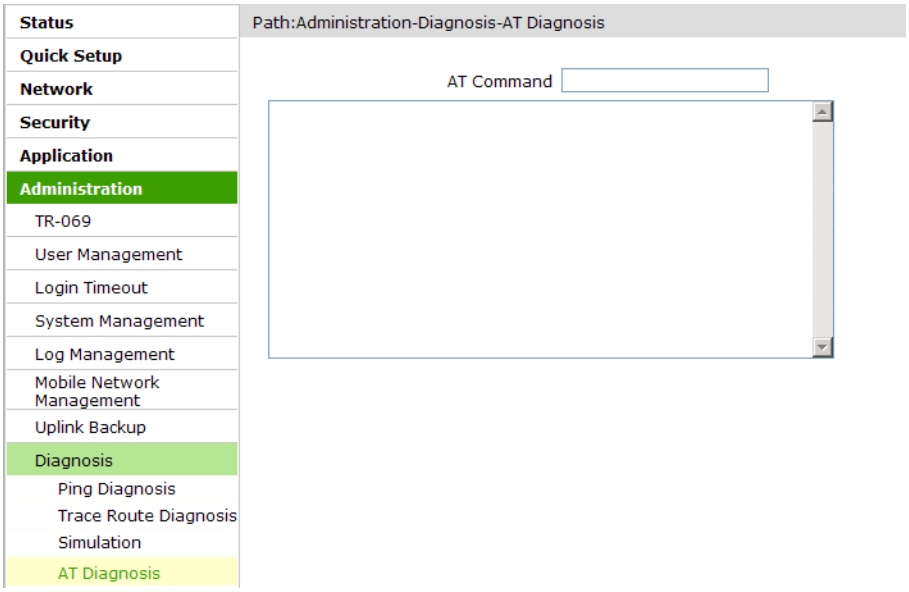
Prerequisite

Before performing AT diagnosis, make sure that the 3G USB wireless card is inserted to the ZXHN H108N device.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ AT Diagnosis**]. The AT Diagnosis page is displayed, see Figure 82.

Figure 82 AT Diagnosis



2. Type `AT` in the **At Command** text box, and then click **Submit**.
3. The system starts to test whether the 3G USB card works normally. If the message `OK` appears, it indicates the 3G card works normally.

9.8.5 Performing Mirror Configuration

This procedure introduces how to perform the mirror configuration.

Context

If the mirror configuration is performed, the packets at the WAN side will be copied to the specified LAN interface, and it can be used for the network analysis and troubleshooting.

Steps

1. On the navigation tree, click [**Administration**→ **Diagnosis**→ **Mirror Configuration**]. The mirror configuration page is displayed, see Figure 83.

Figure 83 Mirror Configuration

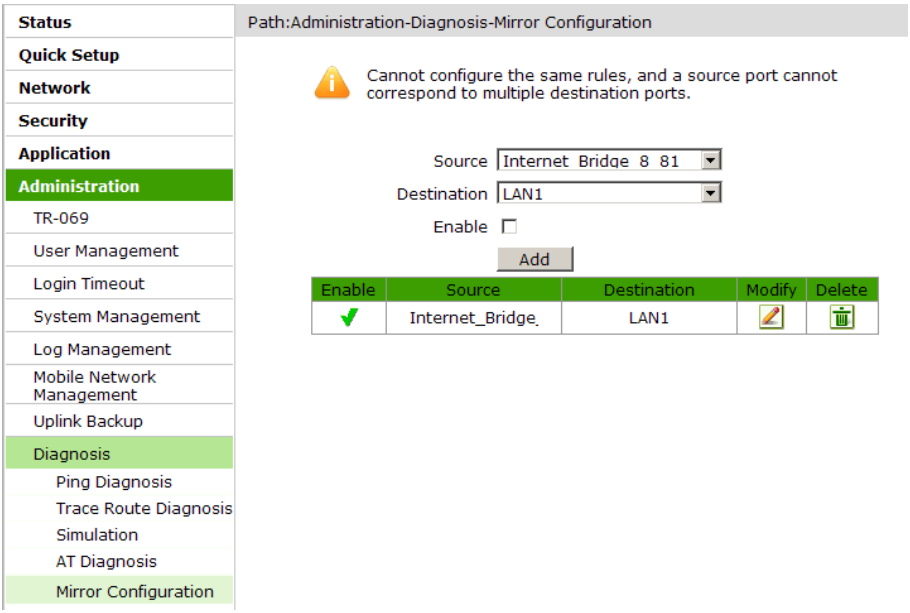


Table 46 lists the mirror configuration parameters.

Table 46 Mirror Configuration Parameters

Parameter	Description
Source	Network-side WAN interface
Destination	User-side LAN interface
Enable	Enable the port mirror function.

2. Configure the mirror parameters, and then click **Add**.

9.8.6 Diagnosing Line

This procedure introduces how to verify that the Modem of ADSL WAN connection is properly connected to the network.

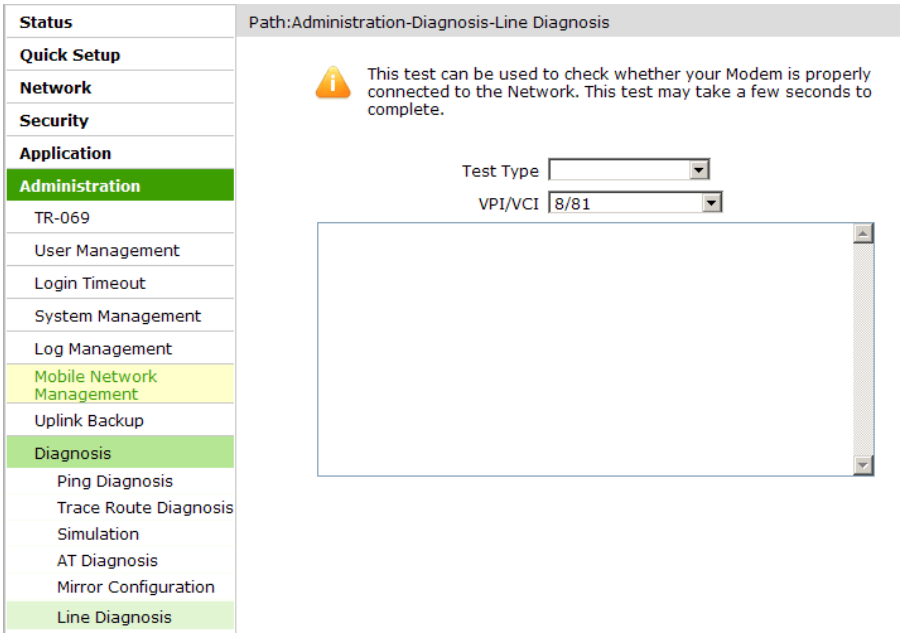
Prerequisite

The ADSL WAN connection is created.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ Line Diagnosis**]. The line diagnosis page is displayed, see Figure 84.

Figure 84 Line Diagnosis



2. Select the test type and VPI/VCI.
3. Click **Submit** to diagnose the connection.

The network connectivity between the ZXHN H108N device and network is diagnosed.

The diagnosis result is as follows:

```
Number of repetitions is 1
Success count is 1 Failure
count is 0
Average response time is 1.4 ms
Minimum response time is 0.6 ms
Maximum response time is 1.9 ms
```

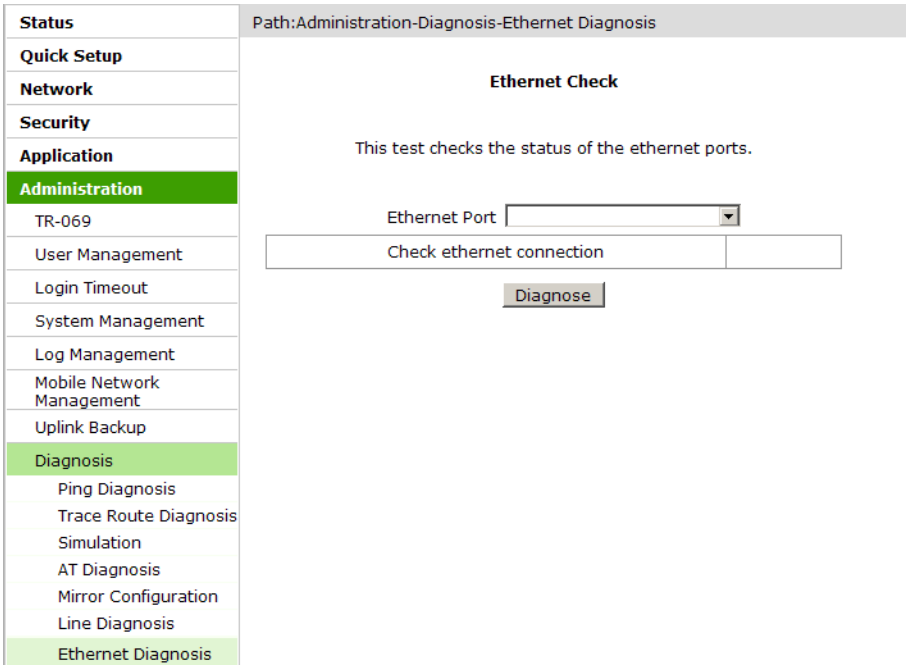
9.8.7 Diagnosing Ethernet Port

This procedure introduces how to diagnose the status of the Ethernet port.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ Ethernet Diagnosis**]. The Ethernet diagnosis page is displayed, see Figure 85.

Figure 85 Ethernet Diagnosis



2. Select one Ethernet port and click **Diagnose** to check the Ethernet connectivity.

The status of the specified Ethernet port is checked.

The **Check Ethernet connection** shows the diagnosis result is “pass”, which means the specified LAN interface is connected.

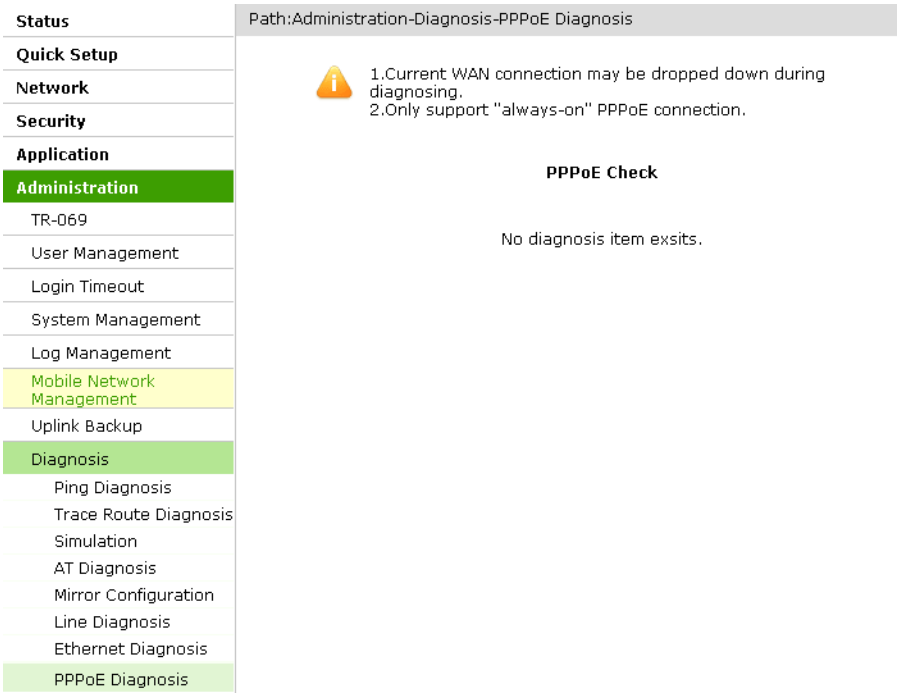
9.8.8 Diagnosing PPPoE

This procedure introduces how to diagnose the PPPoE link.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ PPPoE Diagnosis**]. The PPPoE diagnosis page is displayed, see Figure 86.

Figure 86 PPPoE Diagnosis



2. Select one PPPoE connection and click **Diagnose** to check the PPPoE link.

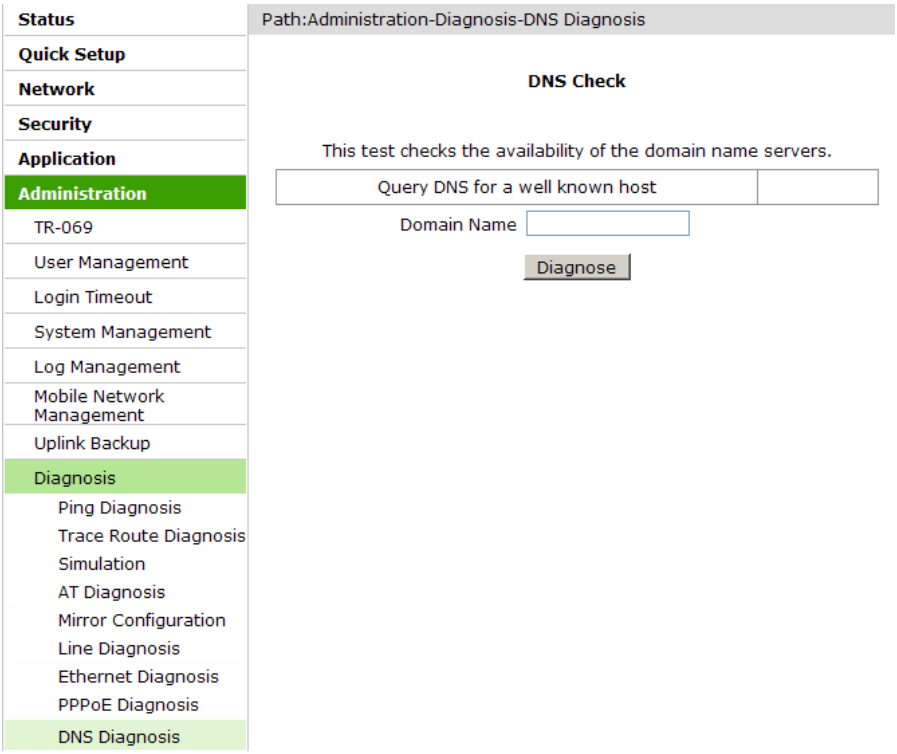
9.8.9 Diagnosing DNS

This procedure introduces how to verify that the existing DNS can translate the specified domain name.

Steps

1. On the navigation tree, click [**Administration→ Diagnosis→ DNS Diagnosis**]. The DNS diagnosis page is displayed, see Figure 87.

Figure 87 DNS Diagnosis



2. Type the domain name in the **Domain Name** text box and click **Diagnose** to perform the diagnosis.

9.8.10 Diagnosing IP

This procedure introduces how to diagnose the connectivity status for IPoE WANconnection.

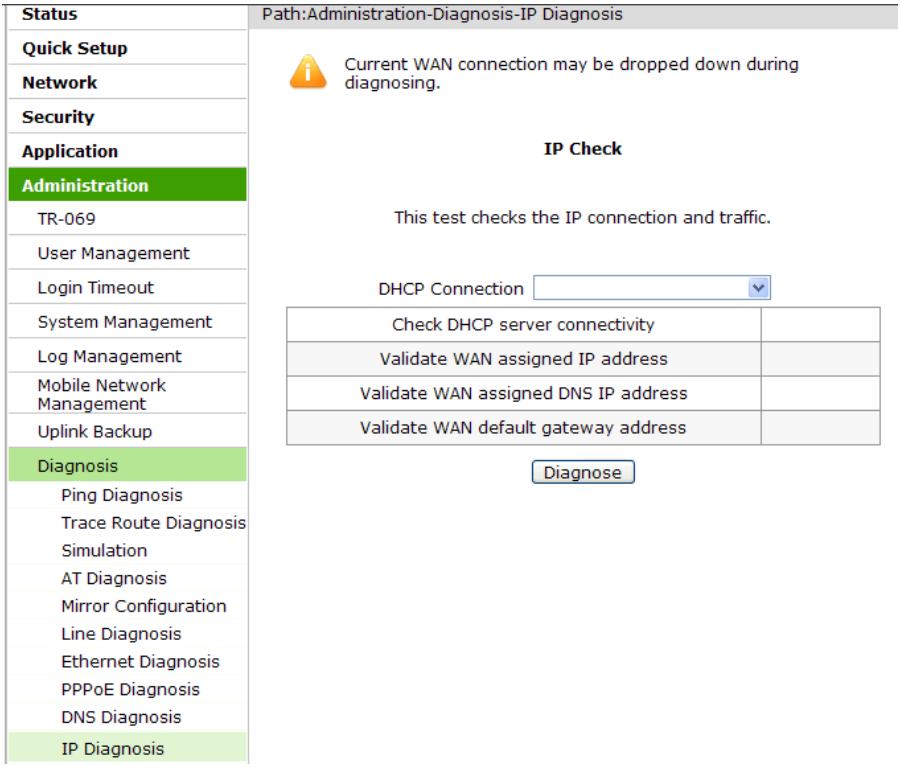
Prerequisite

The IPoE WAN connections are created.

Steps

1. On the navigation tree, click [**Administrator→ Diagnosis→ IP Diagnosis**]. The IP diagnosis page is displayed, see Figure 88.

Figure 88 IP Diagnosis



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

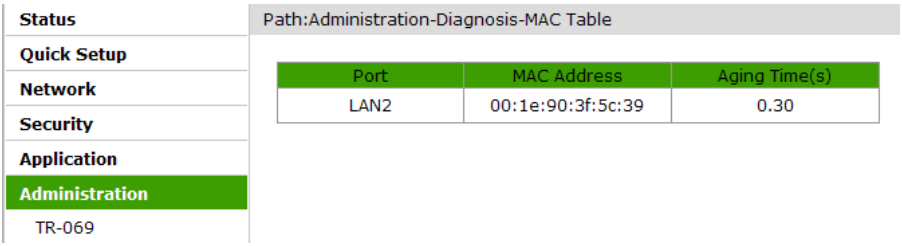
9.8.11 Displaying MAC Table

This procedure introduces how to display the MAC table information of the ZXHN H108N device.

Steps

1. On the navigation tree, click [**Administration→Diagnosis→MAC Table**]. The MAC table page displays the MAC information, see Figure 89.

Figure 89 MAC Table



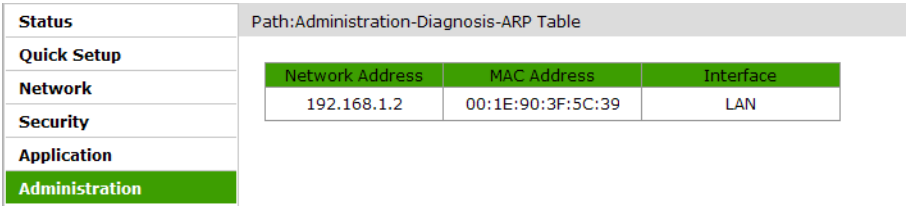
9.8.12 Displaying ARP Table

This procedure introduces how to display the ARP table information.

Steps

1. On the navigation tree, click [**Administration→Diagnosis→ARP Table**]. The ARP table page displays the ARP table information, including network address, MAC address, and interface, see Figure 90.

Figure 90 ARP Table



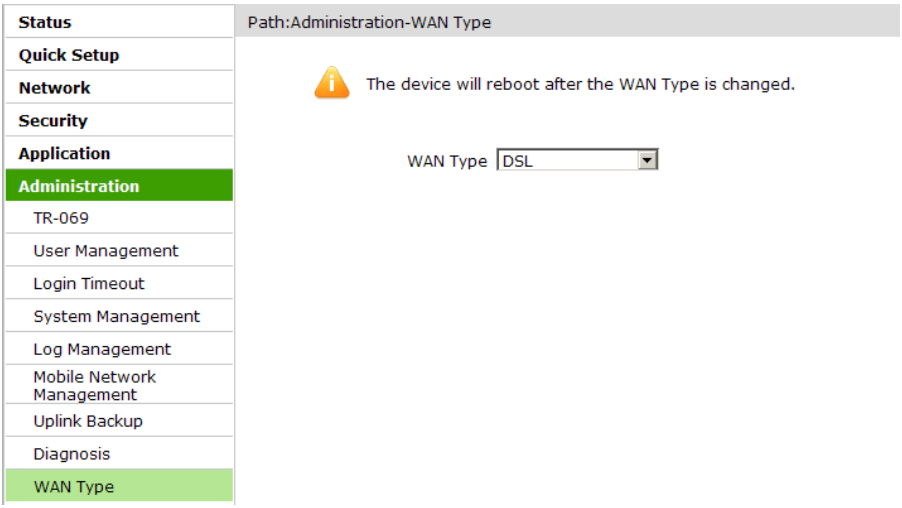
9.9 Configuring WAN Type

This procedure introduces how to specify the WAN type to be used.

Steps

1. On the navigation tree, click [**Administration→ WAN Type**]. The WAN type page is displayed, see Figure 91.

Figure 91 WAN Type



2. Select a WAN type from the **WAN Type** drop-down list.
3. After the configuration, click **Submit**.

Note:

If the WAN type is changed, the ZXHN H108N device will automatically recover to the corresponding WAN type factory configuration.

9.10 Configuring IPv6 Switch

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

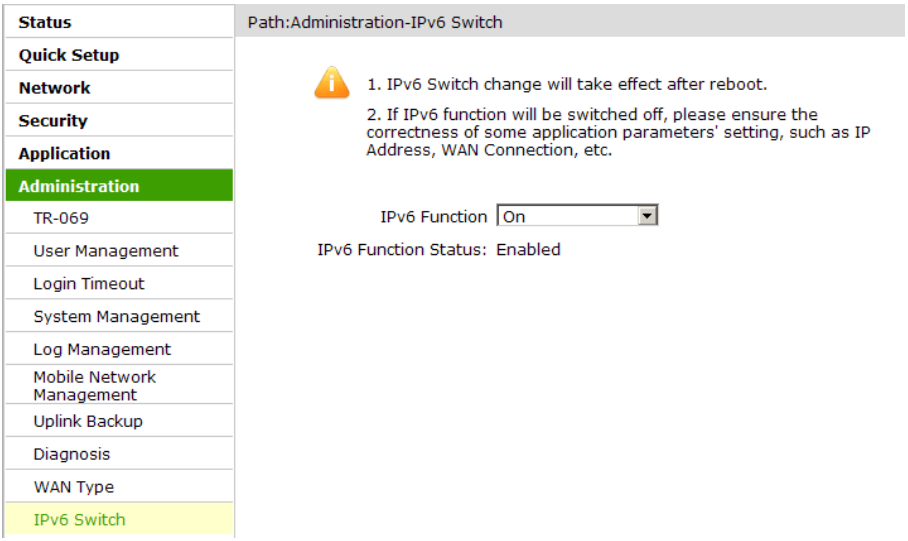
Context

The IPv6 function of the ZXHN H108N device is enabled by default.

Steps

1. On the navigation tree, click [**Administration→ IPv6 Switch**]. The IPv6 switch page is displayed, see Figure 92.

Figure 92 IPv6 Switch



2. Select **On** or **Off** from the **IPv6 Function** drop-down list to enable or disable the IPv6 function.
3. Click **Submit**.

Glossary

ACL - Access Control List

ADSL - Asymmetric Digital Subscriber Line

ARP - Address Resolution Protocol

ATM - Asynchronous Transfer Mode

CHAP - Challenge Handshake Authentication Protocol

CPE - Customer Premises Equipment

DC - Direct Current

DDNS - Dynamic Domain Name Server

DHCP - Dynamic Host Configuration Protocol

DMP - Dedicated signaling MP

DMS - Digital Media Server

DMZ - Demilitarized Zone

DNAT - Destination Network Address Translation

DNS - Domain Name System

DNS - Domain Name Server

DSCP - Differentiated Services Code Point

DSL - Digital Subscriber Line

FTP - File Transfer Protocol

GUI - Graphical User Interface

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IGMP - Internet Group Management Protocol

IP - Internet Protocol

IPoA - IP over ATM

IPoE - Internet Protocol over Ethernet

ISP - Internet Service Provider

LAN - Local Area Network

LLC - Logic Link Control

MAC - Media Access Control

MTU - Maximum Transfer Unit

NAT - Network Address Translation

NE - Network Element

NMS - Network Management System

NTP - Network Time Protocol

OS - Operating System

PAP - Password Authentication Protocol

PPP - Point-to-Point Protocol

PPPoA - Point to Point Protocol over ATM

PPPoE - Point to Point Protocol over Ethernet

PSK - Preshared Key

PVC - Permanent Virtual Channel

QoS - Quality of Service

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

UPnP - Universal Plug and Play

URL - Uniform Resource Locator

USB - Universal Serial Bus

VCI - Virtual Channel Identifier

VLAN - Virtual Local Area Network

VOD - Video On Demand

VPI - Virtual Path Identifier

WAN - Wide Area Network

WAN - Wide Access Network

WEP - Wired Equivalent Privacy

WLAN - Wireless Local Area Network

WPA - Wi-Fi Protected Access