ZXA10 F660

Optical Network Terminal

Maintenance Management Manual

V1.0

Jamii Telecommunications Limited
http://jamii.co.ke
E-mail: jtlsupport@jtl.co.ke
Tel pilot: +254 203975100
Saf pilot: +254 711054110

LEGAL INFORMATION

Revision History

Revision No.	Revision Date	Revision Reason
1.0	2011–05–17	First Edition

Serial Number: SJ-20110517135211-002

Publishing Date: 2011-05-17 (R1.0)

Contents

Chapter 1
Overview

Table of Contents

1.1 Safety Precautions

Usage Cautions

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

Note

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

Environment Requirements

- Ensure the proper ventilation to the device. Place the device out of the direct sunlight.
- Keep the device ventilated and dry. Never spill any liquid on the device.
- Do not place any object on the device, in case it gets deformed and damaged.
- Do not place the device near any source of heat or water.
- Keep the device away from any household appliances with strong magnetic or electric fields, such as microwave oven and refrigerator.

Cleaning Requirements

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

Environment Protection

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

1.2 Packing List

After opening the ZXA10 F660 packing box, make sure that it contains the following components, as listed in Table 1.

Table 1 Packing List

Component Name	Count	Image
ZXA10 F660 host	1	
Power adapter	1	
Power cable	1	

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

One *ZXA10 F660 (V1.0) Optical Network Terminal User Manual* is delivered with the product.

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

1.3 Features and Specifications

System Features

The ZXA10 F660 has the following features:

- MAC cache: 4K
- Multicast services: 1024 multicast groups
- VLAN range: 1–4095
- GEM ports: 32
- T-CONTs: 8

Interface Features

The interface features are as follows:

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

Technical Features

The ZXA10 F660 implements the following functions:

- For data access, the ZXA10 F660 implements L2 data switching and forwarding.

  By working with relevant network devices through signaling protocols such as H.248 and SIP, the ZXA10 F660 implements the IP voice function.

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

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

Product Specifications

The ZXA10 F660 specifications are as follows:

- Rated current: 1.3 A
- Rated voltage: 12 V DC
- Operating temperature: –5℃ to 50℃
- Operating humidity: 5%–95%
- Dimensions: 260 mm × 50 mm × 185 mm (Width × Height × Depth)

1.4 Product Appearance

Front Panel

Figure 1 shows the front panel of the ZXA10 F660.

Figure 1 Front Panel

Table 2 lists LEDs on the front panel.

Table 2 Front Panel LEDs

LED	Status	Description
PON	Solid green	The ONT GPON is registered and the link is activated.
	OFF	The ONT is not discovered and registered.
	Flashing	The ONT is trying to be registered or set up the connection.
LOS	Solid red	The ONU receives the optical power abnormally.
	OFF	The ONU receives the optical power normally.
	Flashing	The WAN connection is abnormal. The ONU fails to acquire the IP address.

LED	Status	Description
WLAN	Solid green	The WLAN function is enabled.
	OFF	The device is not powered ON or the wireless interface is disabled.
	Flashing	Data is being transmitted.
USB	Solid green	The USB interface is connected but no data is going through.
	OFF	The USB interface is not connected to a storage device.
	Flashing	There is data going through the USB interface.
POTS1–POTS2	Solid green	The device is registered on the SS, but no data is being transmitted.
	OFF	The device is not powered ON or fails to be registered on the SS.
	Flashing	Data is being transmitted.
LAN1–LAN4	Solid green	The network interface is connected, but no data is being transmitted.
	OFF	The device is not powered ON or the network interface is not connected with a network device.
	Flashing	Data is being transmitted.
Power indicator	Solid blue	The device is powered ON normally.
	OFF	The device is not powered ON.

Back Panel

Figure 2 shows the back panel of the ZXA10 F660.

Figure 2 Back Panel

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

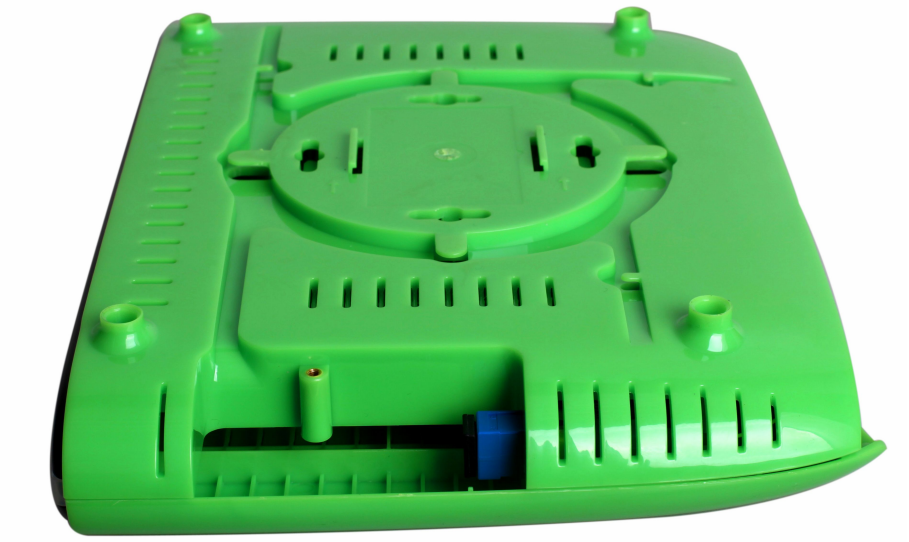
Table 3 Interfaces and Buttons on the Back Panel

Interface/Button	Description
LAN1–LAN4	RJ-45 LAN interface, connecting to the local network through the RJ-45 network cable
POTS1–POTS2	RJ-11 telephone interface, connecting to the telephone through the RJ-11 telephone cable
USB	USB interface, connecting to a storage device that has a USB interface
UPS	Secondary power monitoring interface
POWER	Power socket, connecting to the power adapter, 12 V DC
WLAN	WLAN button, to enable or disable WLAN
RESET	When the device is powered ON, press the button for more than five seconds to restore the factory default settings.

Side Panel

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

Figure 3 Side Panel



1.5 System Requirements

The ZXA10 F660 system requirements are as follows:

- An ISP is needed so that the device can access the services provided by the ISP in PON access mode.
- A computer that is installed with a 10 Mbps/100 Mbps/1000 Mbps Ethernet card is needed.

- If necessary, create a medium and small LAN by adding Ethernet hubs and cables.
- To use wireless access, an 802.11g/b wireless network card or a built-in 802.11g/b wireless network card is required.
- The computer that accesses the network should be installed with Windows 98/Me/2000/NT/XP/Vista/7 or Linux, network card driver program, and TCP/IP protocol, and its network settings should be correct.
- A computer in the LAN is installed with a Web browser, such as Microsoft Internet Explorer 6.0 or later version, Netscape Communicator 4.0 or later version.

1.6 System Application Environment

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

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

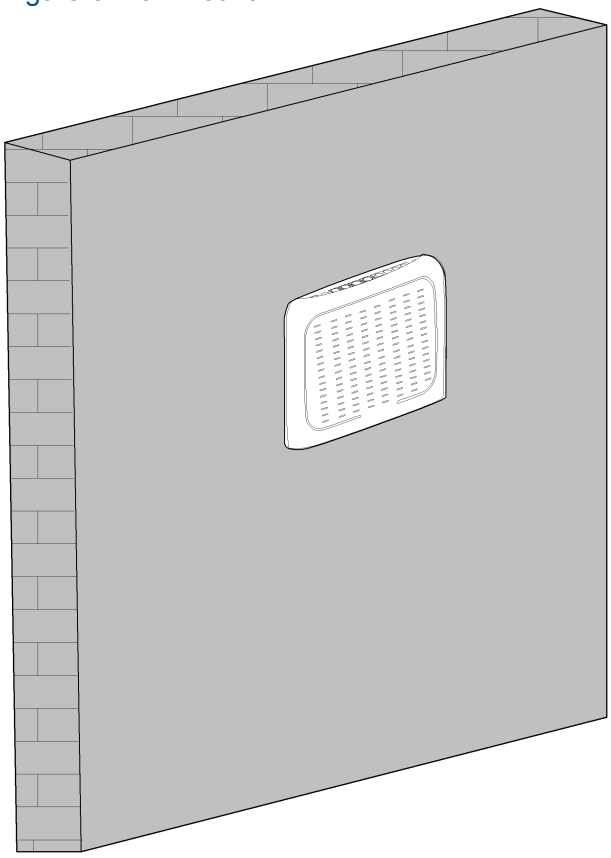
Figure 4 shows the ZXA10 F660 application environment.

Figure 4 System Application Environment

As an indoor device, the ZXA10 F660 can be put on the desk with the base or hung on the wall without the base.

Figure 5 shows the ZXA10 F660 on a wall.

Figure 5 Wall-Mount



Chapter 2
Configuration Preparation

Table of Contents

2.1 Preliminary Setup

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

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

2.2 Configuring TCP/IP

ShortDescription

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

Context

This instance takes Windows XP as an example.

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

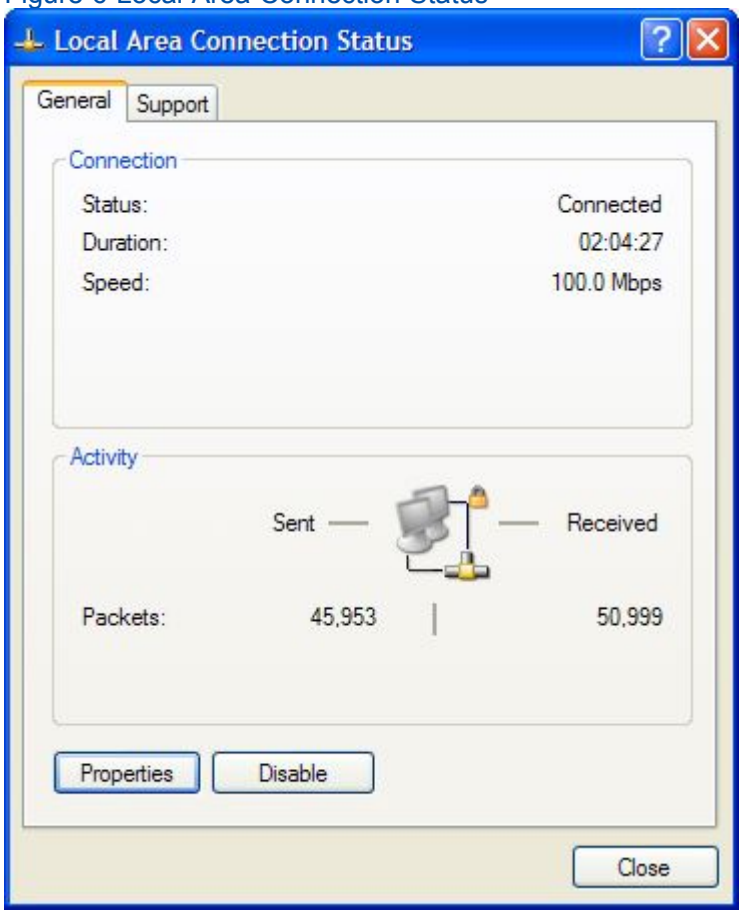
- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1

To configure TCP/IP, perform the following steps:

Steps

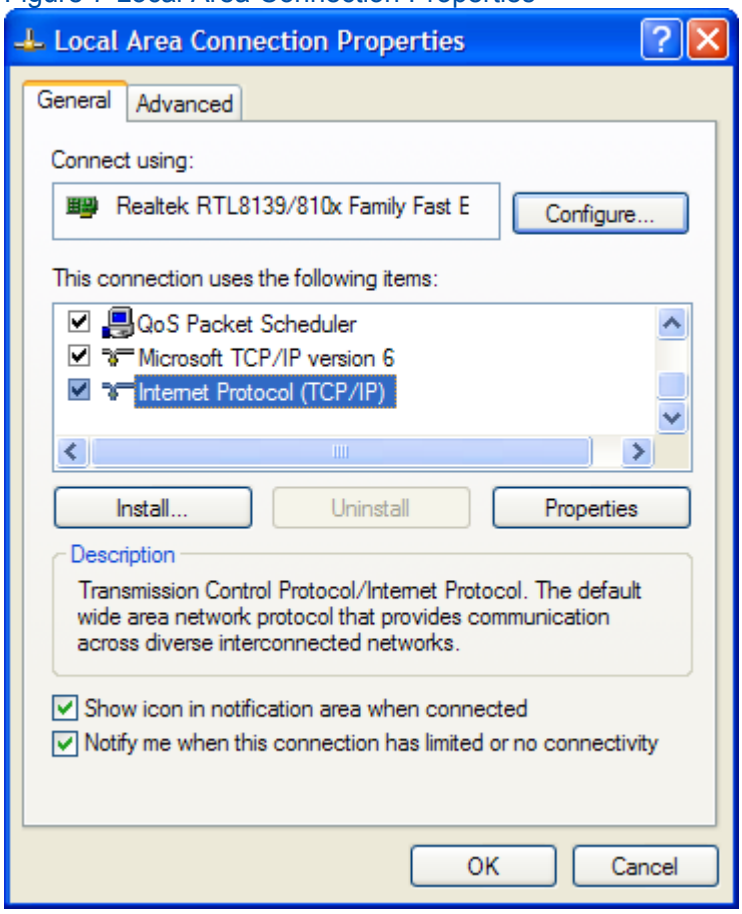
1. Choose **Start> Settings> Network Connections** to open the **Network Connections** window.
2. Double-click **Local Area Connection** to open the **Local Area Connection Status** dialog box, as shown in Figure 6.

Figure 6 Local Area Connection Status



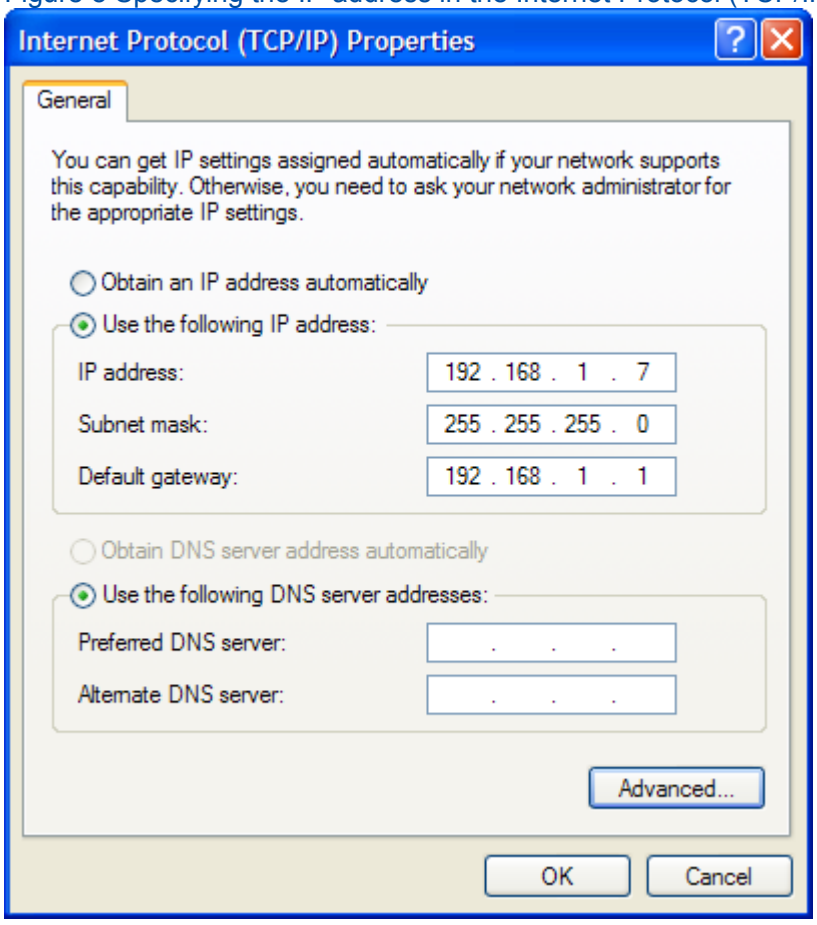
3. Click **Properties** in the **General** tab to open the **Local Area Connection Properties** dialog box.
4. Select **Internet Protocol (TCP/IP)**, as shown in Figure 7.

Figure 7 Local Area Connection Properties



5. Click **Properties** to open the **Internet Protocol (TCP/IP) Properties** dialog box. Select **Use the following IP address** and specify the **IP address**, **Subnet mask**, and **Default gateway**. For example, you can set the **IP address** to `192.168.1.7`, **Subnet mask** to `255.255.255.0`, and **Default gateway** to `192.168.1.1`, as shown in Figure 8.

Figure 8 Specifying the IP address in the Internet Protocol (TCP/IP) Properties



NOTE **Note**

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

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

NOTE **Note**

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

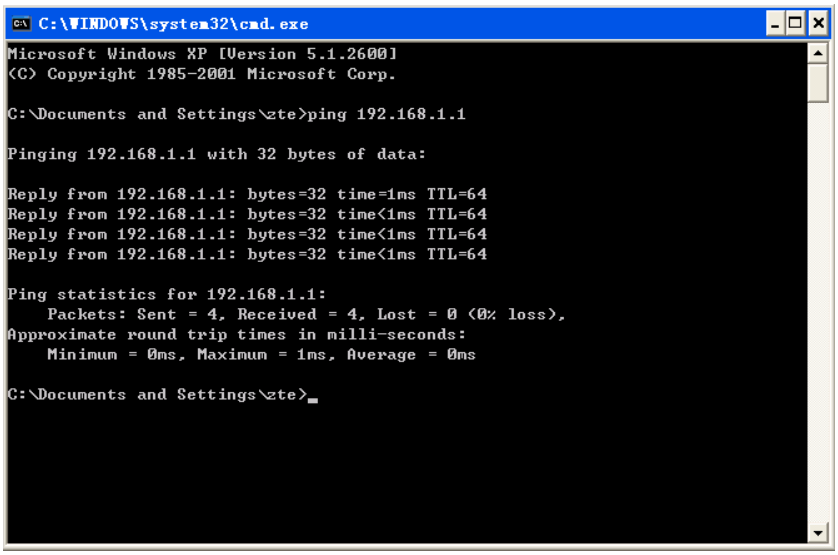
– End of Steps –

Follow-Up Action

1. Choose **Start> Run** to open the **Run** dialog box.

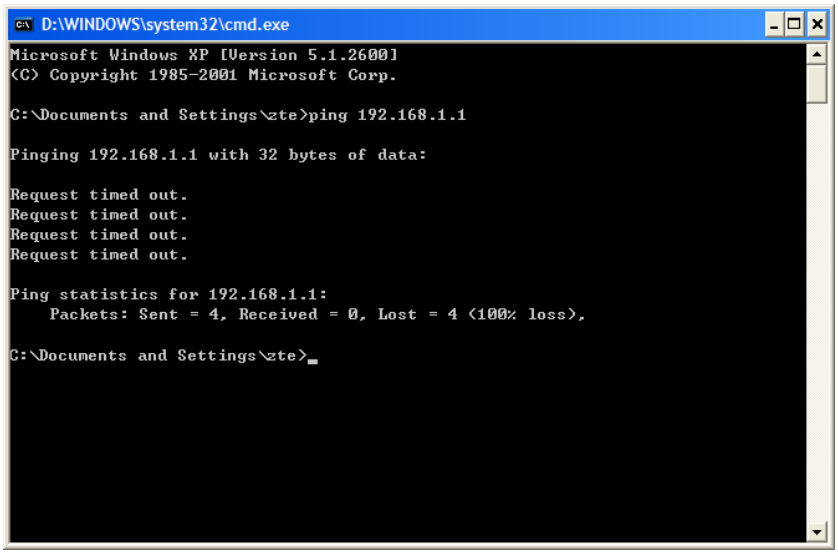
2. Type `CMD` in the **Open** text box, and click **OK**.
3. Type `ping 192.168.1.1` in the pop-up window and press **Enter** to carry out the ping command.
   - If the command window displays the messages, as shown in Figure 9, it indicates that the communication between your PC and the device is normal and you are able to access the Internet now.

Figure 9 Successful Ping Message



   - If the command window displays the messages, as shown in Figure 10, it indicates that the communication between your PC and the device fails.

Figure 10 Failed Ping Message



If the communication between your PC and the device fails, ensure the following items:

- The Ethernet cable between the device and your PC has been connected properly.
- The driver of your network adapter has been installed properly.

- The TCP/IP setting has been configured correctly on your PC.

  If the ZXA10 F660 IP address is 192.168.1.1, the IP address of the computer must be from 192.168.1.2 to 192.168.1.254. The subnet mask must be 255.255.255.0 and the default gateway must be 192.168.1.1.

2.3 Logging In to the Device

ShortDescription

Perform this procedure to log in to the device.

Pre-requisites

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

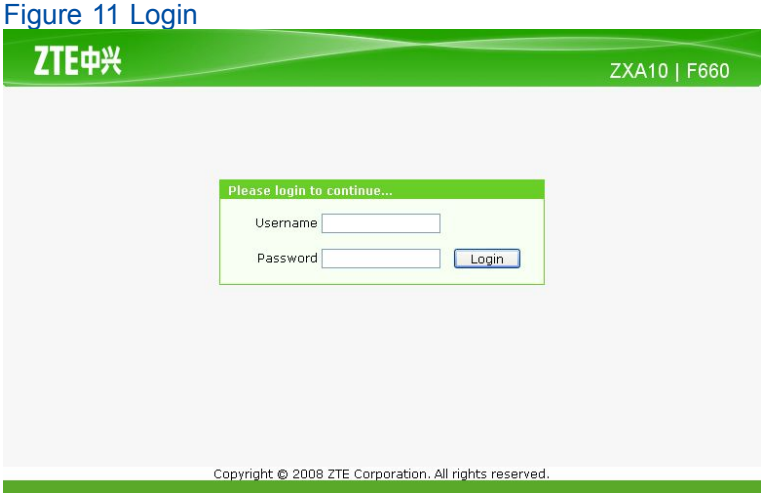
Context

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

Steps

1. Open the Internet Explorer. Enter `http://192.168.1.1` (default IP address of the device) on the address bar and press **Enter**. The login dialog box is displayed, as shown in Figure 11.

Figure 11 Login



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

– End of Steps –

Result

Logging in to the device is successful.

Chapter 3
Device Status

Table of Contents

3.1 Device Information

On the Web interface of the device, click the **Status** tab. By default, the **Device Information** is selected. The right pane displays the device type, serial number, and version information, and registration password, as shown in Figure 12.

Figure 12 Device Information

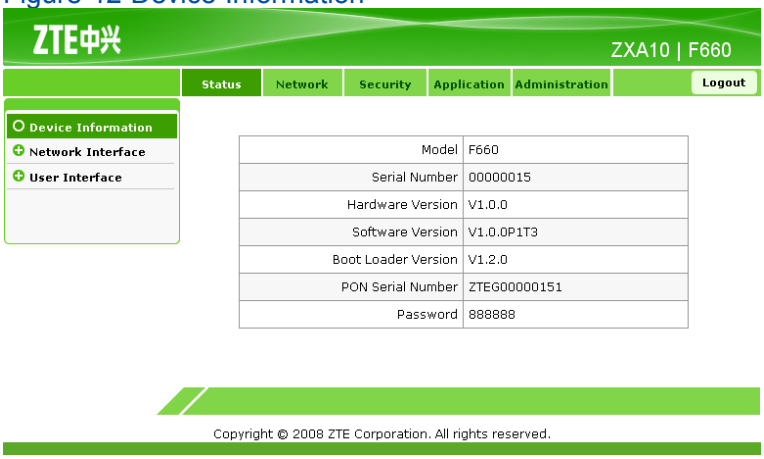


Table 4 lists the parameters for the device information.

Table 4 Device Information Parameters

Parameter	Description
Model	Device type
Serial Number	Device serial number
Hardware Version	Hardware version number
Software Version	Software version number

Parameter	Description
Boot Loader Version	Boot version number
PON Serial Number	PON serial number
Password	Password used by the ONU registration on the OLT

3.2 Network Connection Information

On the **Status** tab, select **Network Interface**. By default, the **WAN Connection** sub-node is selected. The right pane displays the WAN connection information, as shown in Figure 13.

Click **Refresh** to view the latest information.

Figure 13 WAN Connection

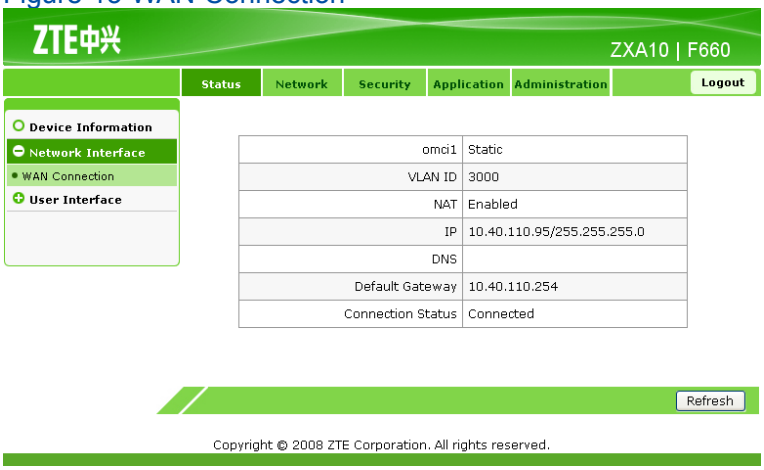


Table 5 lists the parameters for the network connection information.

Table 5 Parameters for the Network Connection Information

Parameter	Description
omci1	WAN connection type
VLAN ID	VLAN ID used by the WAN interface to send and receive data
NAT	Whether to enable the NAT function
IP	IP address used by ZXA10 F660
DNS	DNS used by ZXA10 F660
Default Gateway	Gateway used by ZXA10 F660
Connection Status	WAN connection status

Note

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

3.3 User Interface Information

This topic includes the following:

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

3.3.1 WLAN Interface Information

On the **Status** tab, select **User Interface**. By default, **WLAN** is selected. The right pane displays the WLAN switch information, packet receiving and sending information, and authentication information, as shown in Figure 14.

Click **Refresh** to view the latest information.

Figure 14 WLAN Interface Information

Table 6 lists the parameters for the WLAN interface information.

Table 6 Parameters for the WLAN Interface Information

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

3.3.2 Ethernet Interface Information

On the **Status** tab, select **User Interface**. Select **Ethernet**. The right pane displays the packet receiving and sending information on the Ethernet interface, as shown in Figure 15.

Click **Refresh** to view the latest information.

Figure 15 Ethernet Interface Information

Table 7 lists the parameters for the Ethernet interface information.

Table 7 Parameters for the Ethernet Interface Information

Parameter	Description
Ethernet Port	Port name
Packets Received/Bytes Received	Number of received packets or bytes
Packets Sent/Bytes Sent	Number of sent packets or bytes
Error Frames	Ethernet error frames

3.3.3 VoIP Status Information

On the **Status** tab, select **User Interface**. Select **VoIP Status**. The right pane displays the VoIP status information, as shown in Figure 16.

Click **Refresh** to view the latest information.

Figure 16 VoIP Status Information

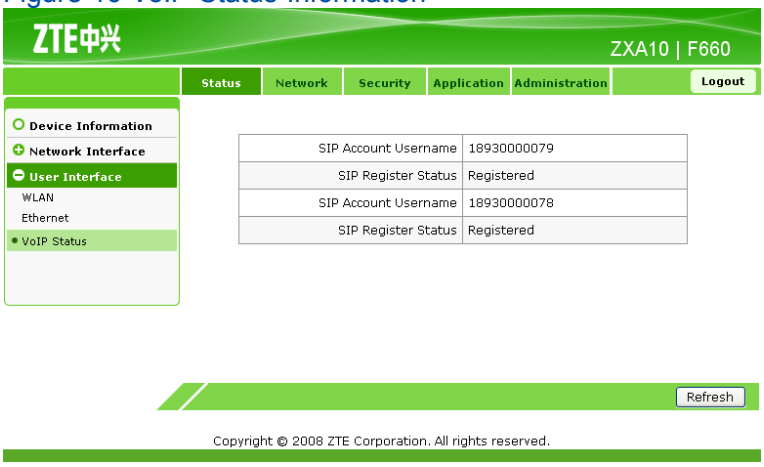


Table 8 lists the parameters for the VoIP status information.

Table 8 Parameters for the VoIP Status Information

Parameter	Description
SIP Account Username	Telephone number
SIP Register Status	Registration status of the voice service

Chapter 4
Network Configuration

Table of Contents

4.1 Configuring WAN Connection

ShortDescription

Perform this procedure to configure the WAN connection.

Pre-requisites

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

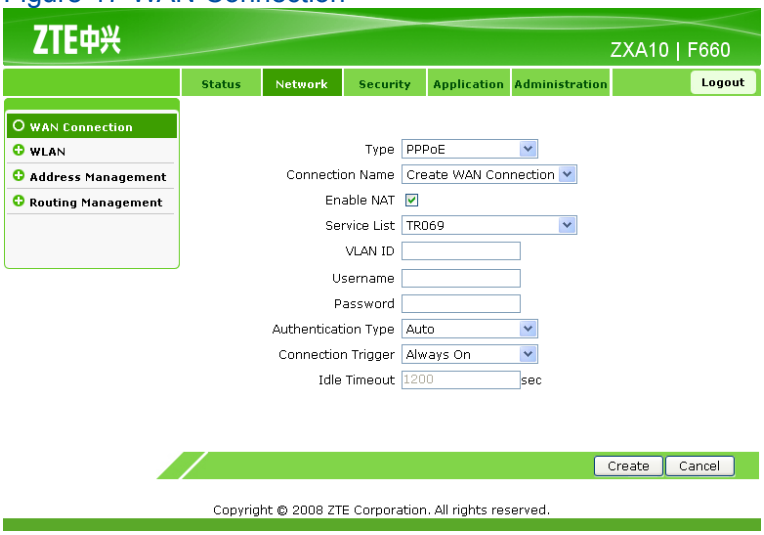
Context

To configure the WAN connection, perform the following steps:

Steps

1. On the Web interface of the device, click the **Network** tab. By default, **WAN Connection** is selected, as shown in Figure 17.

Figure 17 WAN Connection



2. The connection type can be **PPPoE**, **Static**, or **DHCP**.

   a. Configure the PPPoE mode.

   Select **PPPoE** for **Type**, as shown in Figure 18.

Figure 18 PPPoE Mode Configuration

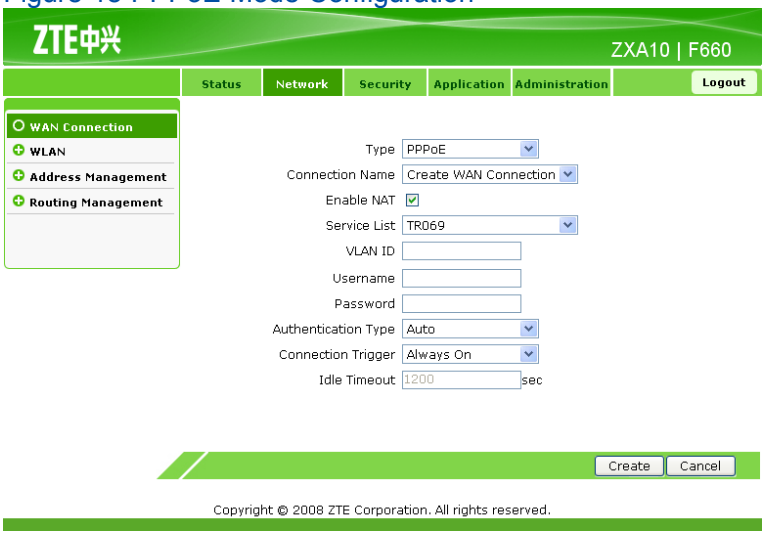


Table 9 lists the parameters for the PPPoE mode configuration.

Table 9 Parameters for PPPoE Mode Configuration

Parameter	Description
Type	Connection mode
Connection Name	PPPoE connection name, automatically generated by the system
Enable NAT	Whether to enable the NAT function

Parameter	Description
Service List	Service modes supported by the system: ● Tr-069 service mode Remote maintenance and management mode ● Internet service mode Broadband and IPTV service mode ● VoIP service mode Voice service mode
VLAN ID	VLAN ID
Username	User name, used by the device authentication on interworking
Password	Password, used by the device authentication on interworking
Authentication Type	Authentication type, the same as the authentication type for the uppper-layer device
Connection Trigger	Dial-up connection mode: ● Always On ● On Demand ● Manual
Idle Timeout	Idle time before the dial-up auto disconnection, available only in On Demand mode

b. Configure the static mode.

Select **Static** for **Type**, as shown in Figure 19.

Figure 19 Static Mode Configuration

Table 10 lists the parameters for the static mode configuration.

Table 10 Static Mode Configuration

Parameter	Description
Type	Connection mode
Connection Name	Static connection name, automatically generated by the system
Enable NAT	Whether to enable the NAT function
Service List	Service modes supported by the system: ● Tr-069 service mode Remote maintenance and management mode ● Internet service mode Broadband and IPTV service mode ● VoIP service mode Voice service mode
VLAN ID	VLAN ID
IP Address	IP address used by ZXA10 F660
Subnet Mask	Subnet mask used by ZXA10 F660
Default Gateway	Gateway used by ZXA10 F660
DNS Server1 IP Address	IP address of DNS1 used by ZXA10 F660
DNS Server2 IP Address	IP address of DNS2 used by ZXA10 F660
DNS Server3 IP Address	IP address of DNS3 used by ZXA10 F660

c. Configure the DHCP mode.

Select **DHCP** for **Type**, as shown in Figure 20.

Figure 20 DHCP Mode Configuration

Table 11 lists the parameters for the DHCP mode configuration.

Table 11 DHCP Mode Configuration

Parameter	Description
Type	Connection mode
Connection Name	DHCP connection name, automatically generated by the system
Enable NAT	Whether to enable the NAT function
Service List	Service modes supported by the system: ● Tr-069 service mode Remote maintenance and management mode ● Internet service mode Broadband and IPTV service mode ● VoIP service mode Voice service mode
VLAN ID	VLAN ID

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

– End of Steps –

Result

WAN connection configuration is complete.

4.2 WLAN Configuration

This topic includes the following:

- Configuring Basic WLAN Parameters
- Configuring Multi-SSID Parameters
- Configuring Security Properties
- Viewing Associated Devices

4.2.1 Configuring Basic WLAN Parameters

ShortDescription

Perform this procedure to configure the basic WLAN parameters.

Pre-requisites

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

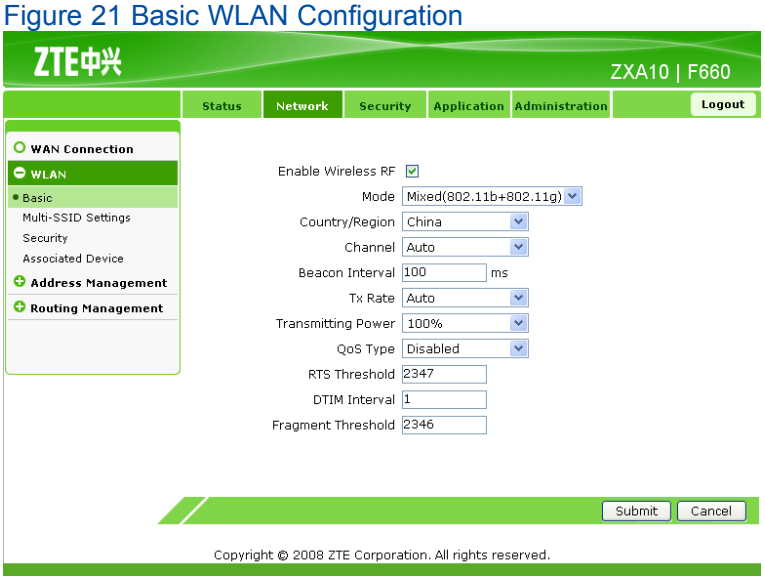
Context

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

Steps

1. On the **Network** tab, select **WLAN** on the left pane. By default, the **Basic** sub-node is selected, as shown in Figure 21.

Figure 21 Basic WLAN Configuration



2. Configure the basic WLAN parameters, as listed in Table 12.

Table 12 Basic WLAN Parameters

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

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

– End of Steps –

Result

The basic WLAN parameters are configured.

4.2.2 Configuring Multi-SSID Parameters

ShortDescription

Perform this procedure to configure multi-SSID parameters.

Pre-requisites

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

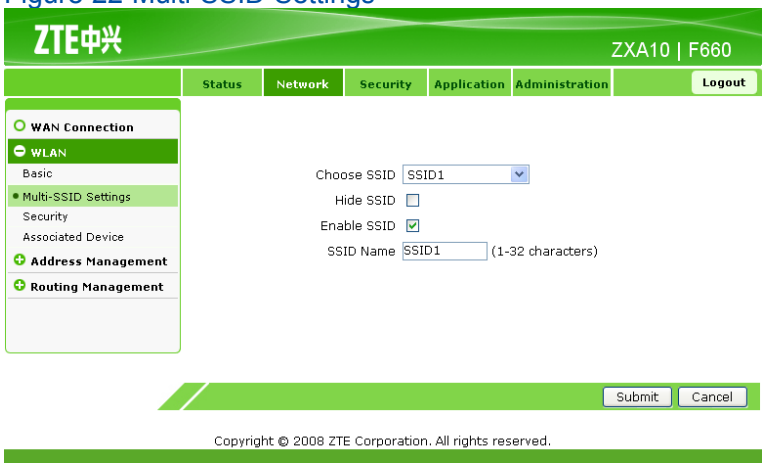
Context

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

Steps

1. On the **Network** tab, click **WLAN** on the left pane. Select **Multi-SSID Settings**, as shown in Figure 22.

Figure 22 Multi-SSID Settings



2. Configure the multi-SSID parameters as shown in Table 13.

Table 13 Multi-SSID Parameters

Parameter	Description
Choose SSID	Choose the SSID that needs to be configured.
Hide SSID	Disable or enable SSID broadcast.
Enable SSID	Enable the SSID.

Parameter	Description
SSID Name	SSID name. It cannot exceed 32 characters and is case sensitive. It is used to control the WLAN access. The SSID name must match all the SSIDs of the related access nodes; otherwise, the device cannot be accessed. Up to four WLAN sub-ports are supported.

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

– End of Steps –

Result

The multi-SSID parameters are configured.

4.2.3 Configuring Security Properties

ShortDescription

Perform this procedure to configure the security properties.

Pre-requisites

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

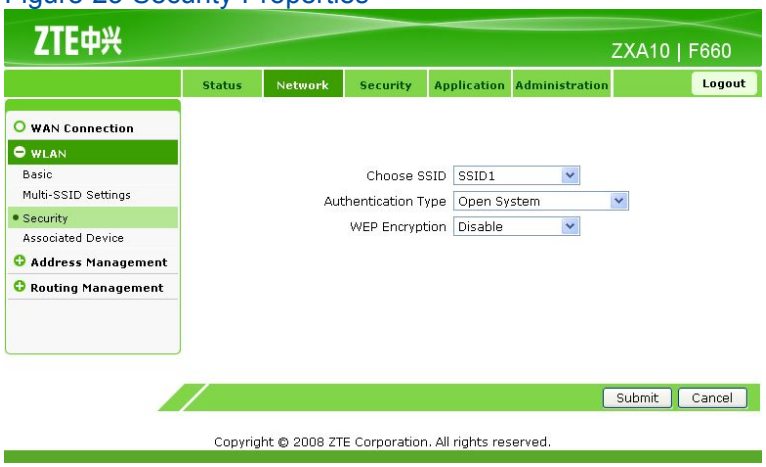
Context

To configure the security properties, perform the following steps:

Steps

1. On the **Network** tab, select **WLAN**, and then select **Security**, as shown in Figure 23.

Figure 23 Security Properties



SSID supports four authentication modes: **Open System**, **Shared Key**, **WPA-PSK**, and **WPA2-PSK**.

2. From the **Choose SSID** drop-down list, select an SSID.

a. In **Authentication Type**, select **Open System**, and then enable **WEP Encryption** (by default, it is disabled). The **Open System** configuration information is displayed, as shown in Figure 24.

Figure 24 Open System Configuration

Table 14 lists the parameters for the **Open System** authentication mode.

Table 14 Parameters for Open System Authentication Mode

Parameter	Description
Choose SSID	Current SSID
Authentication Type	Current SSID authentication mode
WEP Encryption	To enable or disable WEP encryption
WEP Encryption Level	WEP encryption length ● The 128–bit encryption can be a 13–bit ASCII codes or a 26–bit hexadecimal number. ● The 64–bit encryption can be a 5–bit ASCII code or a 10–bit hexadecimal number. Generally, the 64–bit encryption can meet the user requirements. To enhance security, use the 128–bit encryption.
WEP Key Index	Current encryption value
WEP Key1	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number
WEP Key2	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number
WEP Key3	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number

Parameter	Description
WEP Key4	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number

b. In **Authentication Type**, select **Shared Key**. By default, **WEP Encryption** is enabled. The **Shared Key** configuration information is displayed, as shown in Figure 25.

Figure 25 Shared Key Configuration

Table 15 lists the parameters for the **Shared Key** authentication mode.

Table 15 Parameters for Shared Key Authentication Mode

Parameter	Description
Choose SSID	Current SSID
Authentication Type	Current SSID authentication mode
WEP Encryption	To enable or disable WEP encryption
WEP Encryption Level	WEP encryption length ● The 128–bit encryption can be a 13–bit ASCII codes or a 26–bit hexadecimal number. ● The 64–bit encryption can be a 5–bit ASCII code or a 10–bit hexadecimal number. Generally, the 64–bit encryption can meet the user requirements. To enhance security, use the 128–bit encryption.
WEP Key Index	Current encryption value
WEP Key1	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number

Parameter	Description
WEP Key2	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number
WEP Key3	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number
WEP Key4	WEP encryption value Range: 5–bit ASCII code or 10–bit hexadecimal number

c. In **Authentication Type**, select **WPA-PSK**. The **WPA-PSK** configuration information is displayed, as shown in Figure 26.

Figure 26 WPA-PSK Configuration

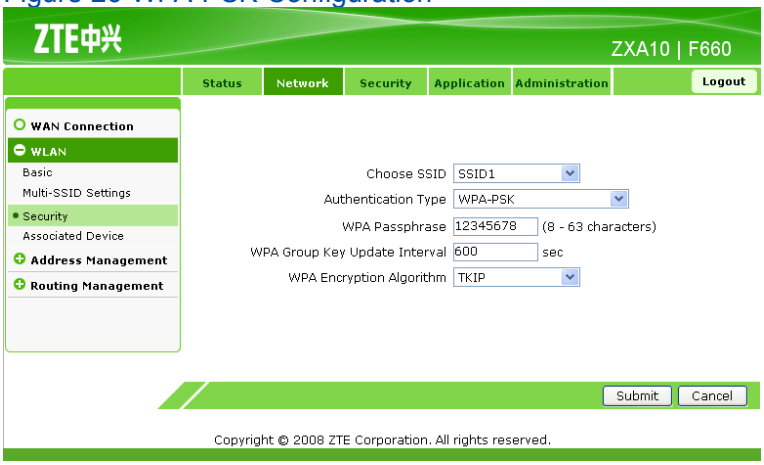


Table 16 lists the parameters for the **WPA-PSK** authentication mode.

Table 16 Parameters for WPA-PSK Authentication Mode

Parameter	Description
Choose SSID	Current SSID
Authentication Type	Current SSID authentication mode
WPA Passphrase	WPA pre-shared key Range: 8 – 63 characters
WPA Group Key Update Interval	Update interval of the WPA group key
WPA Encryption Algorithm	WPA encryption algorithm

NOTE **Note**

The configuration method for the **WPA2-PSK** authentication mode is the same as that for the **WPA-PSK** authentication mode.

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

– End of Steps –

Result

The security properties are configured.

4.2.4 Viewing Associated Devices

ShortDescription

Perform this procedure to view the associated devices.

Pre-requisites

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

Context

To view the associated devices, perform the following steps:

Steps

1. On the **Network** tab, select **WLAN**, and then select **Associated Device**, as shown in Figure 27.

Figure 27 Associated Device

2. Select **SSID**, and then click **Refresh** to view the MAC addresses of the associated devices.

– End of Steps –

Result

The associated devices are listed.

4.3 Address Management Configuration

This topic includes the following:

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

4.3.1 Configuring DHCP Server

ShortDescription

Perform this procedure to configure the DHCP server.

Pre-requisites

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

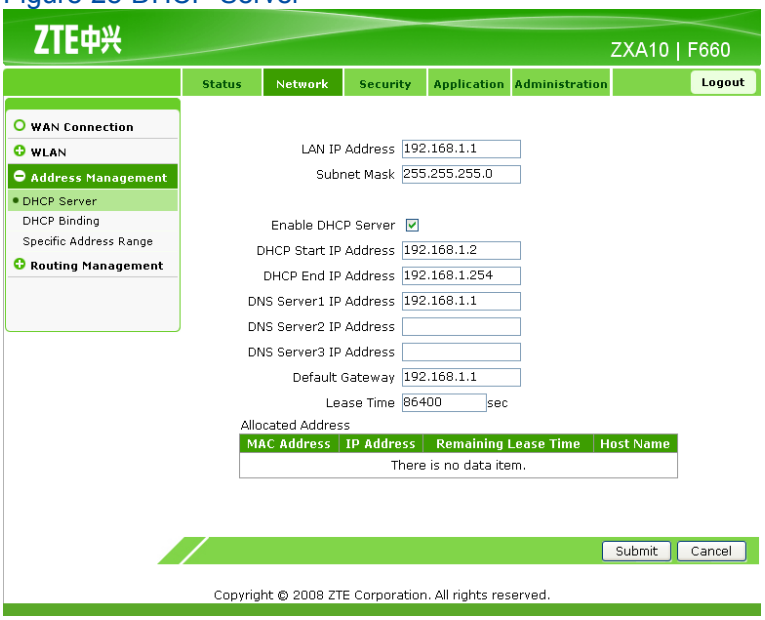
Context

To configure the DHCP server, perform the following steps:

Steps

1. On the **Network** tab, select **Address Management**. By default, **DHCP Server** is selected, as shown in Figure 28.

Figure 28 DHCP Server



2. On the **DHCP Server** tab, configure the parameters, as listed in Table 17.

Table 17 Parameters for DHCP Server Configuration

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

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

– End of Steps –

Result

The DHCP server is configured.

4.3.2 Configuring DHCP Binding

ShortDescription

Perform this procedure to configure the DHCP binding.

Pre-requisites

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

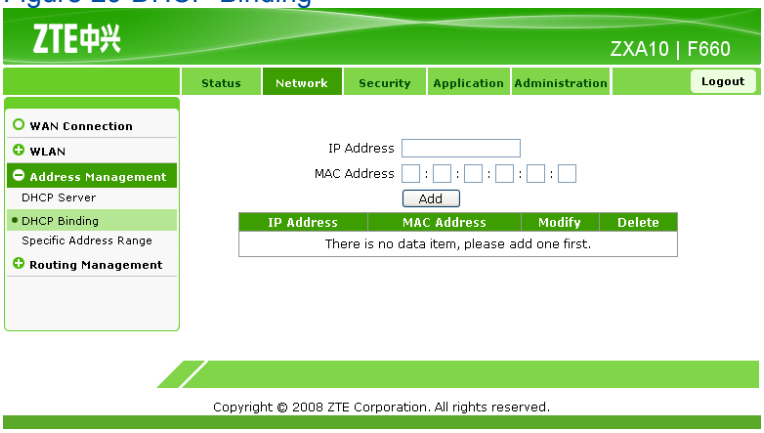
Context

To configure the DHCP binding, perform the following steps:

Steps

1. On the **Network** tab, select **Address Management**, and then select **DHCP Binding**, as shown in Figure 29.

Figure 29 DHCP Binding



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

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

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

NOTE **Note**

The IP address belongs to the address pool that is provided by the DHCP server in the LAN group.

---

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

   – End of Steps –

Result

DHCP binding is configured.

4.3.3 Configuring Specific Address Range

ShortDescription

Perform this procedure to configure the specific address range.

Pre-requisites

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

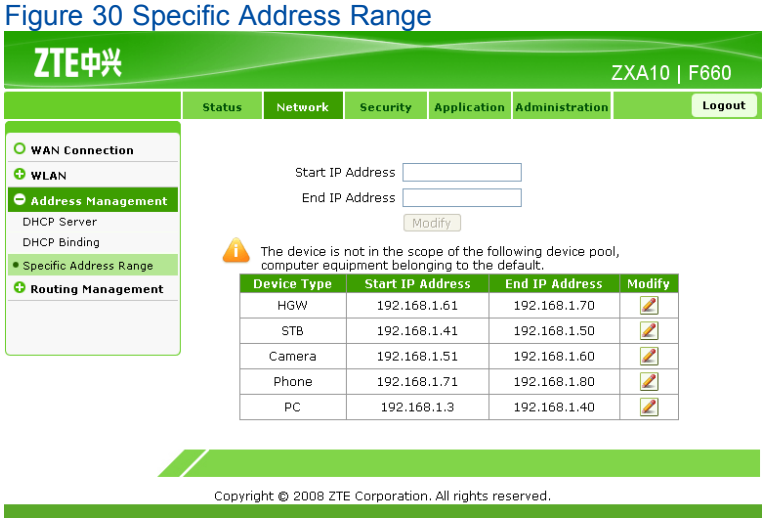
Context

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

Steps

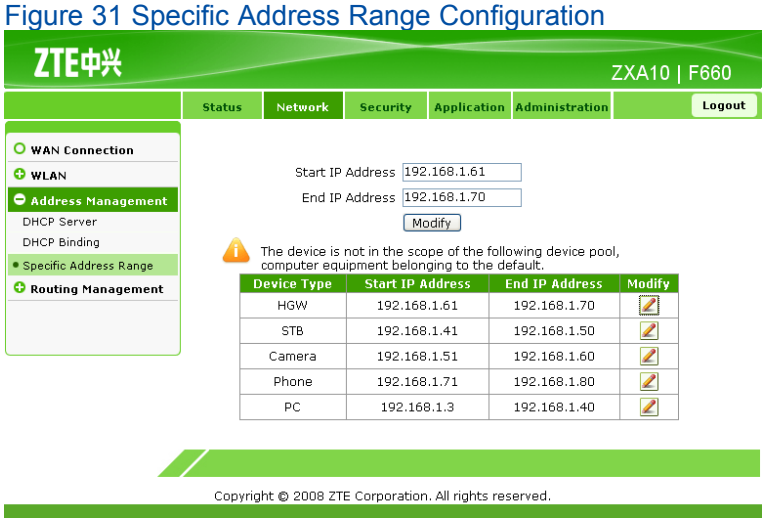
1. On the **Network** tab, select **Address Management**, and then select **Specific Address Range**, as shown in Figure 30.

Figure 30 Specific Address Range



2. Click **Modify** to modify the parameters, as shown in Figure 31.

Figure 31 Specific Address Range Configuration



3. In **Start IP Address** and **End IP Address**, enter the IP addresses, and then click **Modify**.

– End of Steps –

Result

The specific address range is configured.

4.4 Route Management Configuration

This topic includes the following:

- Configuring Default Gateway
- Configuring Static Routing

4.4.1 Configuring Default Gateway

ShortDescription

Perform this procedure to configure the default gateway.

Pre-requisites

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

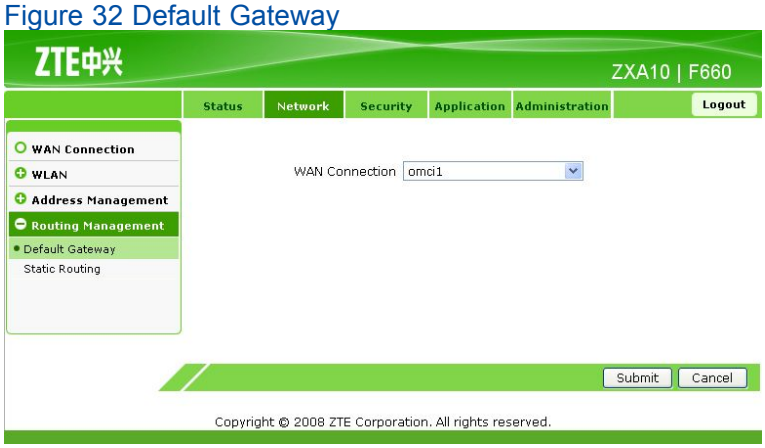
Context

To configure the default gateway, perform the following steps:

Steps

1. On the **Network** tab, select **Routing Management**. By default, **Default Gateway** is selected, as shown in Figure 32.

Figure 32 Default Gateway



2. From **WAN Connection**, select the connection interface at the WAN side.

NOTE **Note**

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

---

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

– End of Steps –

Result

The default gateway is configured.

4.4.2 Configuring Static Routing

ShortDescription

Perform this procedure to configure the static routing.

Pre-requisites

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

Context

To configure the static routing, perform the following steps:

Steps

1. On the **Network** tab, select **Routing Management**, and then select **Static Routing**, as shown in Figure 33.

Figure 33 Static Routing

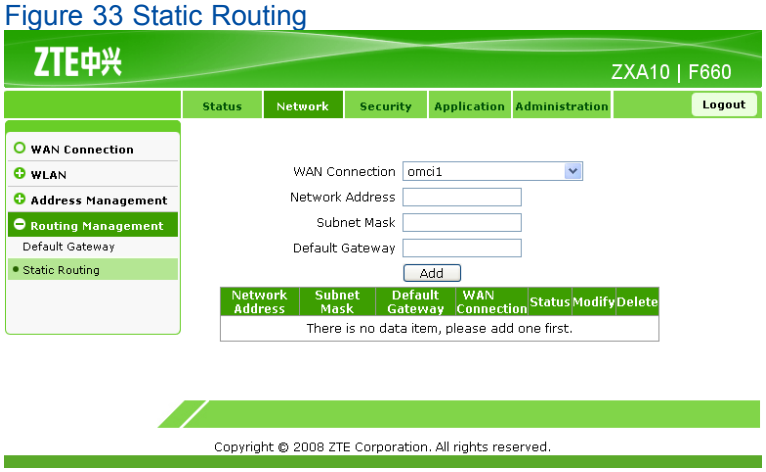


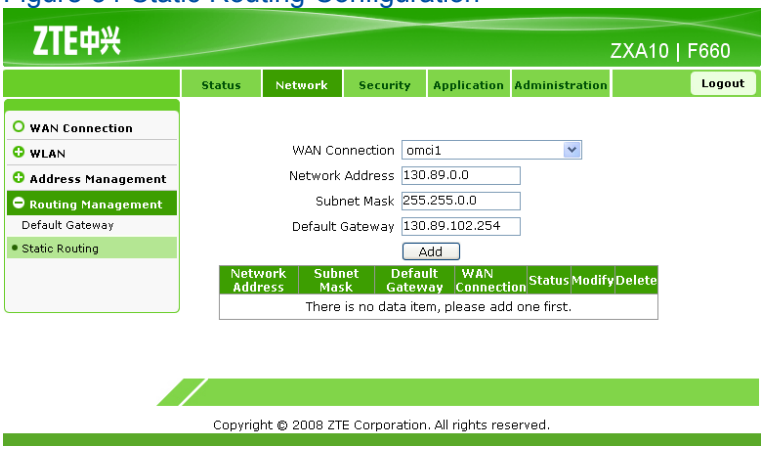
Table 18 lists the parameters for static routing configuration.

Table 18 Parameters for Static Routing Configuration

Parameter	Description
WAN Connection	Network-side interface type
Network Address	Network address
Subnet Mask	Subnet mask
Default Gateway	Gateway

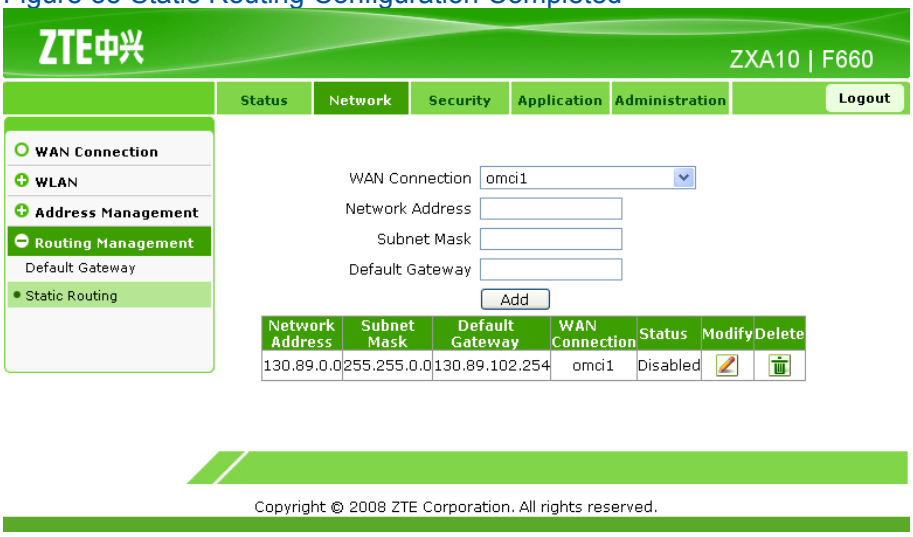
2. From the **WAN Connection** drop-down list, select the network-side interface.
3. Configure **Network Address**, **Subnet Mask**, and **Default Gateway**, as shown in Figure 34.

Figure 34 Static Routing Configuration



4. Click **Add** to finish the configuration, as shown in Figure 35. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

Figure 35 Static Routing Configuration Completed



– End of Steps –

Result

The static routing is configured.

Chapter 5
Security Configuration

Table of Contents

5.1 Configuring Firewall

ShortDescription

Perform this procedure to configure the firewall.

Pre-requisites

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

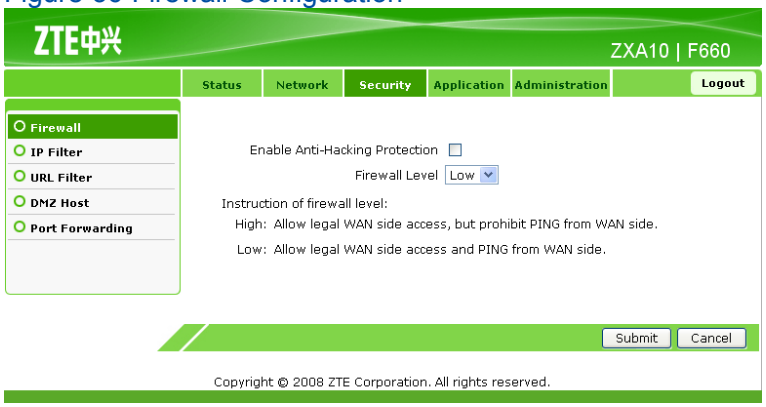
Context

To configure the firewall, perform the following steps:

Steps

1. On the Web interface, click the **Security** tab. By default, **Firewall** is selected, as shown in Figure 36.

Figure 36 Firewall Configuration



2. Set the firewall parameters, as listed in Table 19.

Table 19 Firewall Parameters

Parameter	Description
Enable Anti-Hacking Protection	To enable or disable anti-hacking protection
Firewall Level	Firewall level ● **High**: Allow legal WAN-side access but prohibit WAN-side ping. ● **Low**: Allow legal WAN-side access and WAN-side ping.

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

– End of Steps –

Result
The firewall is configured.

5.2 Configuring IP Filter

ShortDescription
Perform this procedure to configure IP filter.

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

Context
To configure IP filter, perform the following steps:

Steps
1. On the **Security** tab, select **IP Filter**, as shown in Figure 37.

Figure 37 IP Filter

Table 20 lists the parameters for IP filter configuration.

Table 20 Parameters for IP Filter Configuration

Parameter	Description
Enable	To enable the IP filter function
Protocol	Protocol
Name	Name
Start Source IP Address	Starting source IP address
End Source IP Address	Ending source IP address
Start Destination IP Address	Starting destination IP address
End Destination IP Address	Ending destination IP address
Start Source Port	Starting source port number
End Source Port	Ending source port number
Start Destination Port	Starting destination port number
End Destination Port	Ending destination port number
Ingress	Ingress interface
Egress	Egress interface
Mode Discard Permit	Mode, including discard and permit

2. On the **IP Filter** tab, set the filter parameters, as shown in Figure 38.

Figure 38 IP Filter Configuration

3. Click **Add** to finish the configuration, as shown in Figure 39. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

Figure 39 IP Filter Configuration Completed

– End of Steps –

Result

IP filter is configured.

5.3 Configuring URL Filter

ShortDescription

Perform this procedure to configure the URL filter.

Pre-requisites

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

Context

To configure the URL filter, perform the following steps:

Steps

1. On the **Security** tab, select **URL Filter**, as shown in Figure 40.

Figure 40 URL Filter

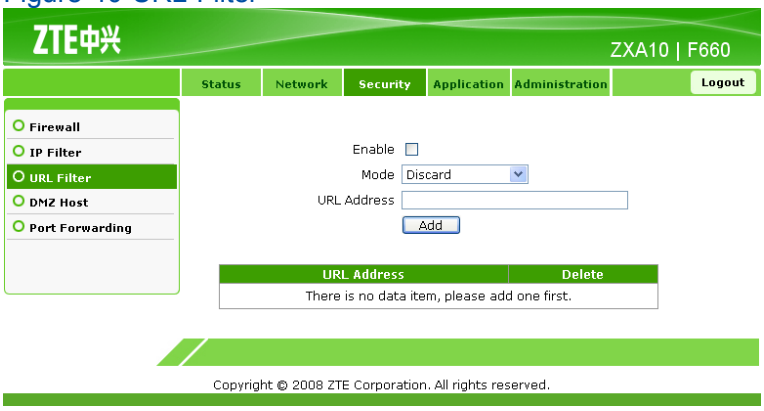


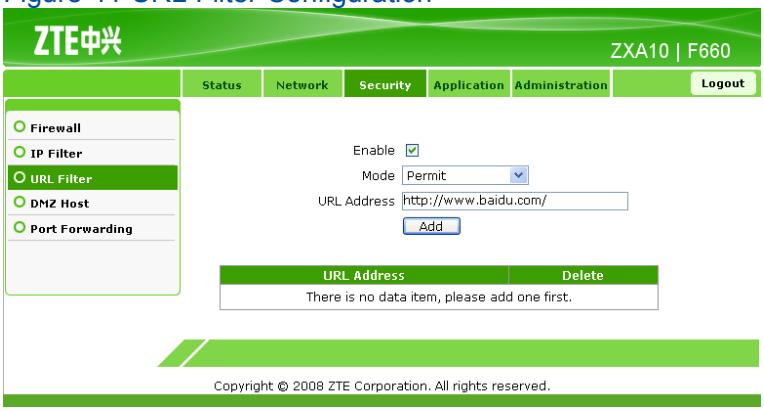
Table 21 lists the parameters for URL filter configuration.

Table 21 Parameters for URL Filter Configuration

Parameter	Description
Enable	To enable the URL filter function
Mode	Mode, including discard and permit
URL Address	URL address

2. On the **URL Filter** tab, set the filter parameters, as shown in Figure 41.

Figure 41 URL Filter Configuration



3. Click **Add** to finish the configuration, as shown in Figure 42. Click **Delete** to delete the configuration.

Figure 42 URL Filter Configuration Completed

– End of Steps –

Result

URL filter is configured.

5.4 Configuring DMZ Host

ShortDescription

Perform this procedure to configure the DMZ host.

Pre-requisites

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

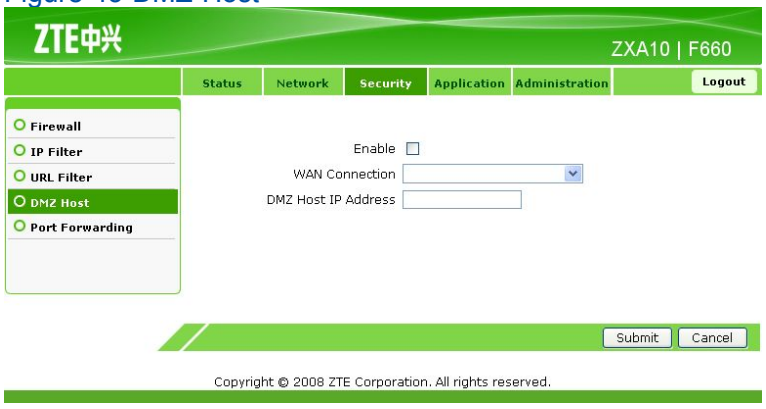
Context

To configure the DMZ host, perform the following steps:

Steps

1. On the **Security** tab, select **DMZ Host**, as shown in Figure 43.

Figure 43 DMZ Host



2. Configure the DMZ host parameters, as shown in Figure 44.

Figure 44 DMZ Host Configuration

Table 22 lists the parameters for DMZ host configuration.

Table 22 Parameters for DMZ Host Configuration

Parameter	Description
Enable	To enable the DMZ host
WAN Connection	WAN-side connection interface
DMZ Host IP Address	IP address of the DMZ host

Note

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

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

– End of Steps –

Result

The DMZ host is configured.

5.5 Configuring Port Forwarding

ShortDescription

Perform this procedure to configure port forwarding.

Pre-requisites

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

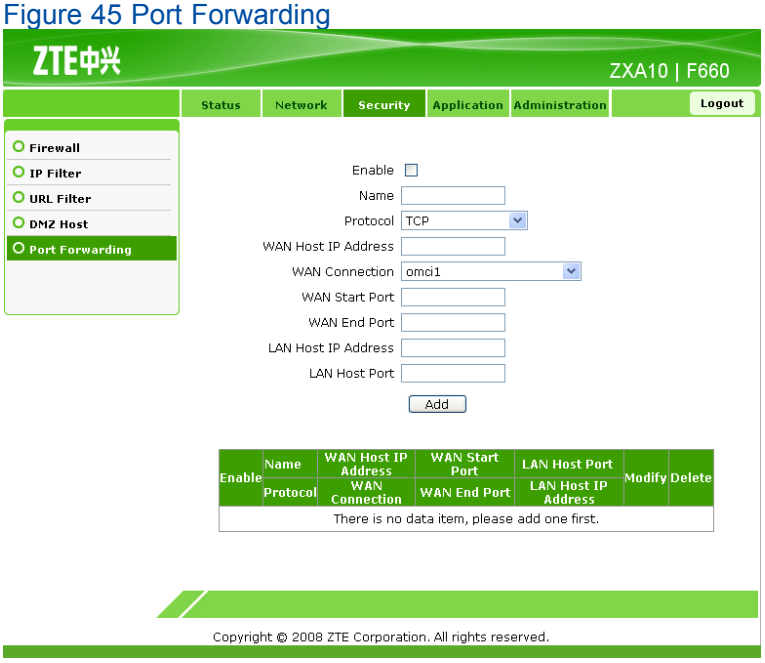
Context

To configure port forwarding, perform the following steps:

Steps

1. On the **Security** tab, select **Port Forwarding**, as shown in Figure 45.

Figure 45 Port Forwarding



2. Configure the port forwarding parameters, as shown in Figure 46.

Figure 46 Port Forwarding Configuration

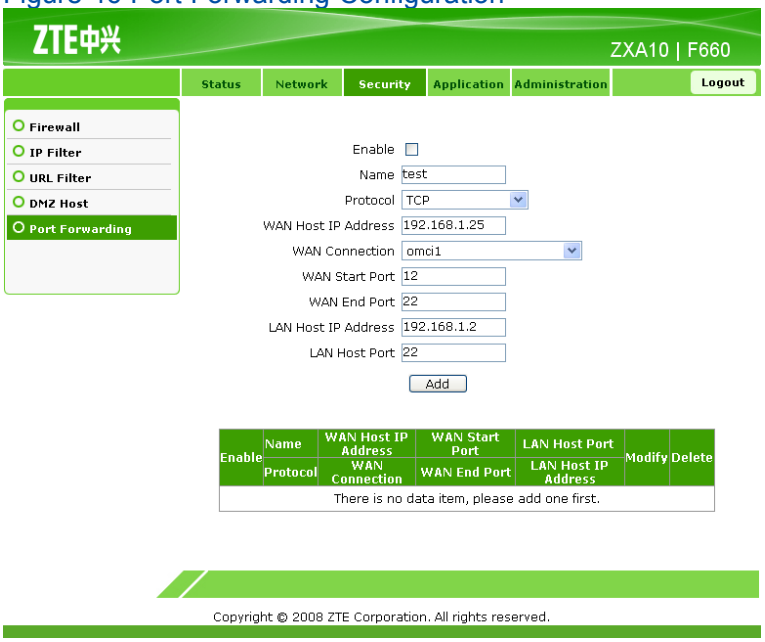


Table 23 lists the parameters for port forwarding configuration.

Table 23 Parameters for Port Forwarding Configuration

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

Note

If a redirection policy of port access with the source address of the WAN-side IP address and the destination address of the LAN-side IP address is configured, it is used in the scenario where the WAN-side client accesses the LAN-side server.

3. Click **Add** to finish the configuration, as shown in Figure 47. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

Figure 47 Port Forwarding Configuration Completed

– End of Steps –

Result

Port forwarding is configured.

Chapter 6
Service Configuration

Table of Contents

6.1 SIP VoIP Service Configuration

This topic includes the following:

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

6.1.1 Configuring VoIP WAN Connection

ShortDescription

Perform this procedure to configure the VoIP WAN connection.

Pre-requisites

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

Context

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

Steps

1. On the Web interface, click the **Application** tab. Select **VoIP**. By default, **WAN Connection** is selected, as shown in Figure 48.

Figure 48 WAN Connection

2. Select a connection interface from **WAN Connection**.
3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result

The VoIP WAN connection is configured.

6.1.2 Configuring SIP

ShortDescription

Perform this procedure to configure SIP.

Pre-requisites

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

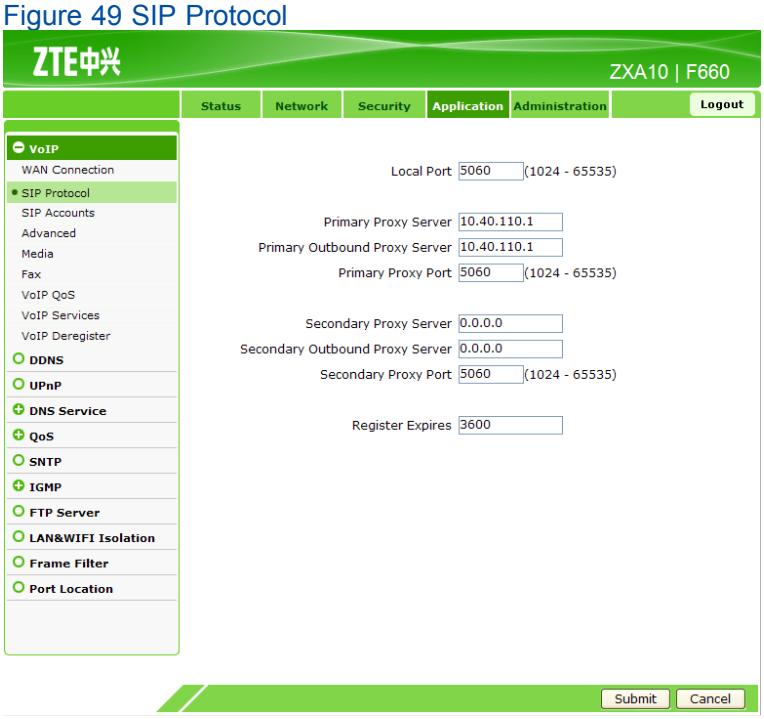
Context

To configure SIP, perform the following steps:

Steps

1. On the **Application** tab, select **VoIP**, and then select **SIP Protocol**, as shown in Figure 49.

Figure 49 SIP Protocol



2. Configure the SIP protocol parameters, as listed in Table 24.

Table 24 Parameters for SIP Protocol Configuration

Parameter	Description
Local Port	Local port number used by the VoIP protocol
Primary Proxy Server	IP address of the primary proxy server
Primary Outbound Proxy Server	IP address of the primary outbound proxy server
Primary Proxy Port	Port number of the primary proxy server
Secondary Proxy Server	IP address of the secondary proxy server
Secondary Outbound Proxy Server	IP address of the secondary outbound proxy server
Secondary Proxy Port	Port number of the secondary proxy server
Register Expires	Registration expiration time Unit: second

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

– End of Steps –

Result

SIP is configured.

6.1.3 Configuring SIP Accounts

ShortDescription

Perform this procedure to configure SIP accounts.

Pre-requisites

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

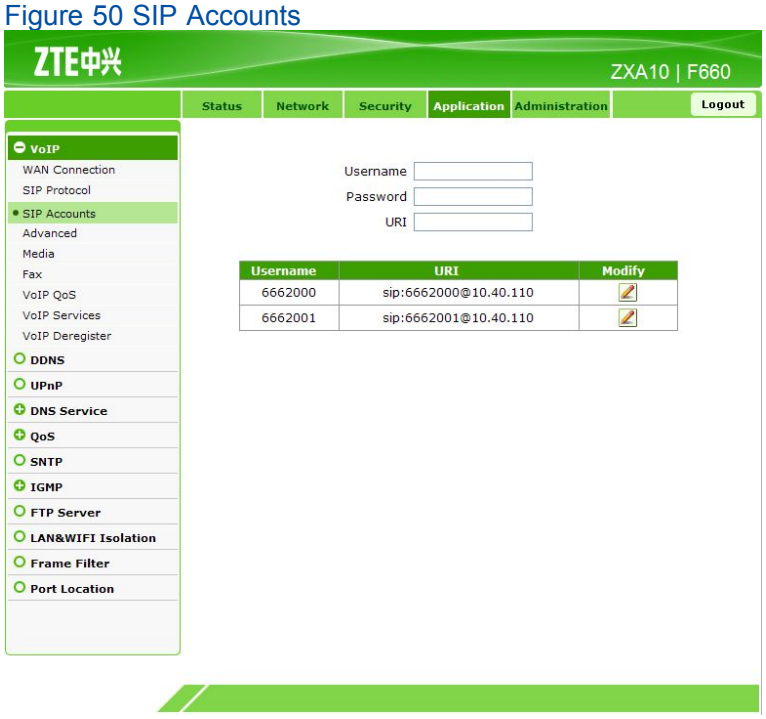
Context

To configure SIP accounts, perform the following steps:

Steps

1. On the **Application** tab, select **VoIP**, and then select **SIP Accounts**, as shown in Figure 50.

Figure 50 SIP Accounts



2. Click **Modify** to modify the account parameters, as shown in Figure 51.

Figure 51 SIP Account Configuration

Table 25 lists the parameters for SIP account configuration.

Table 25 Parameters for SIP Account Configuration

Parameter	Description
Username	Name of the SIP authentication user
Password	Password of the SIP authentication user
URI	User registration identification, that is, the user SIP call number

3. Click **Modify**.

– End of Steps –

Result

The SIP accounts are configured.

6.1.4 Configuring VoIP Advanced Parameters

ShortDescription

Perform this procedure to configure the VoIP advanced parameters.

Pre-requisites

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

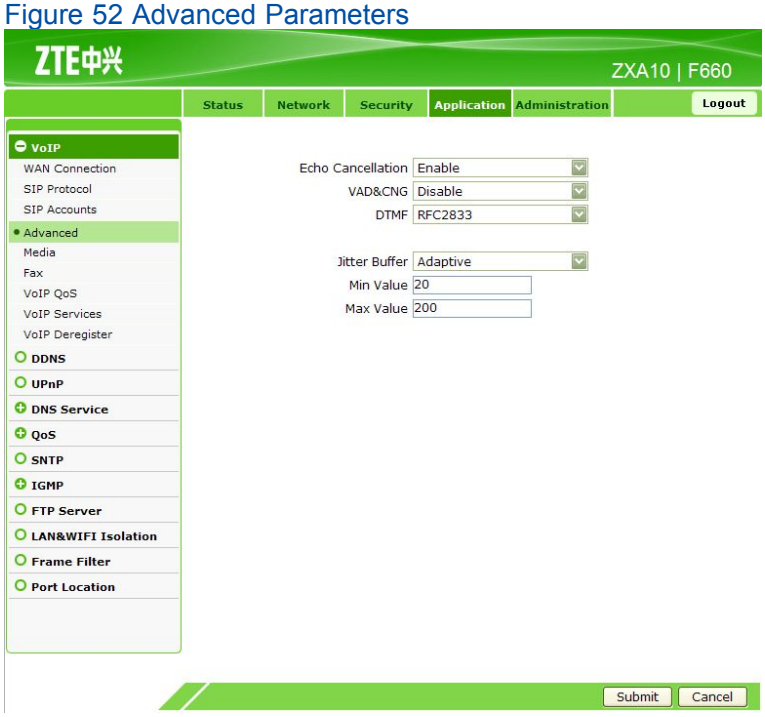
Context

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

Steps

1. On the **Application** tab, select **VoIP**, and then select **Advanced**, as shown in Figure 52.

Figure 52 Advanced Parameters



2. Configure the advanced parameters, as shown in Table 26.

Table 26 Advanced Parameters

Parameter	Description
Echo Cancellation	To enable or disable echo cancellation
VAD&CNG	To enable or disable VAD and CNG
DTMF	DTMF mode, including RFC2833, RFC2198, and DTMF in Voice
Jitter Buffer	Jitter buffer, including fixed and adaptive
Min Value	Minimum jitter buffer value Unit: ms
Max Value	Maximum jitter buffer value Unit: ms

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

– End of Steps –

Result

The VoIP advanced parameters are configured.

6.1.5 Configuring VoIP Media Parameters

ShortDescription

Perform this procedure to configure the VoIP media parameters.

Pre-requisites

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

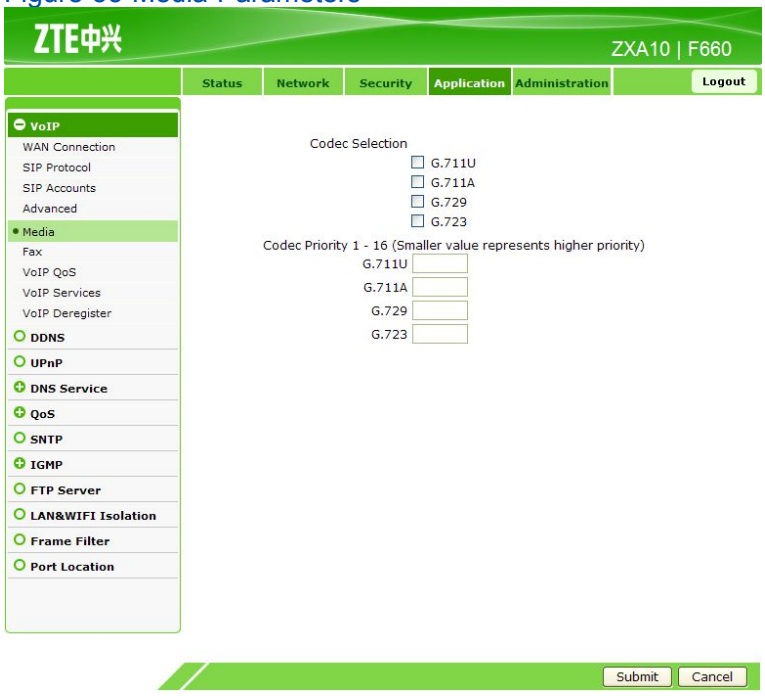
Context

To configure VoIP media parameters, perform the following steps:

Steps

1. On the **Application** tab, select **VoIP**, and then select **Media**, as shown in Figure 53.

Figure 53 Media Parameters



2. Configure the media parameters, as shown in Figure 54.

Figure 54 Media Parameter Configuration

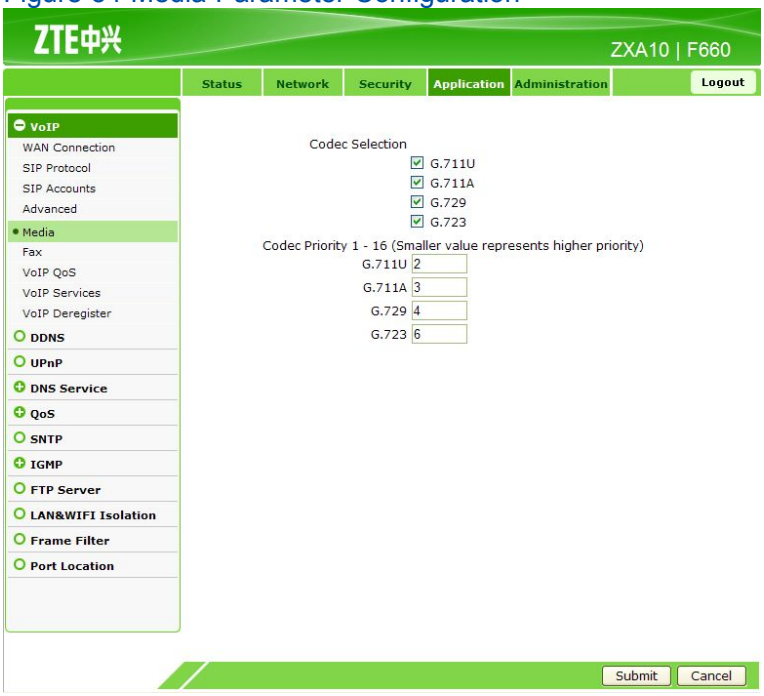


Table 27 lists the media parameters.

Table 27 Media Parameters

Parameter	Description
Codec Selection	Code type
Codec Priority	Code priority The smaller the value is, the higher the priority is.

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

– End of Steps –

Result

The VoIP media parameters are configured.

6.1.6 Configuring Fax

ShortDescription

Perform this procedure to configure fax.

Pre-requisites

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

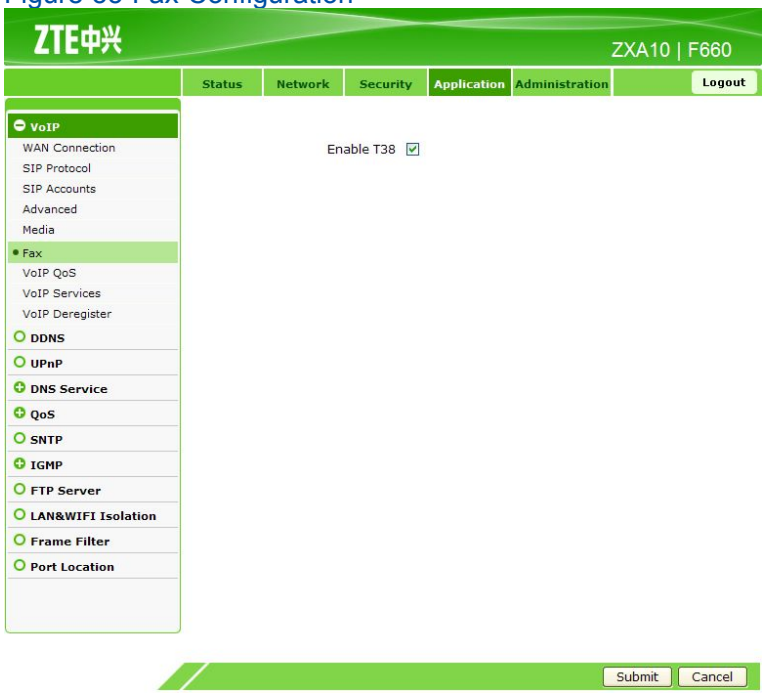
Context

To configure fax, perform the following steps:

Steps

1. On the **Application** tab, select **VoIP**, and then select **Fax**, as shown in Figure 55.

Figure 55 Fax Configuration



2. Select **Enable T38**.

NOTE **Note**

To disable T38 fax mode, clear the check box.

---

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

– End of Steps –

Result

Fax is configured.

6.2 Configuring DDNS

ShortDescription

Perform this procedure to configure DDNS.

Pre-requisites

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

Context

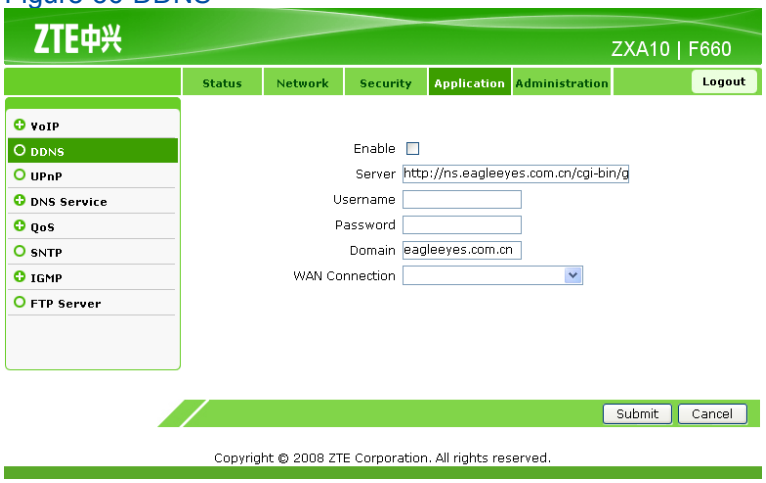
After DDNS is applied, the host that has the dynamic IP address can also provide the domain name service. For example, when the host obtains an IP address through xDSL dial-up or DHCP server dynamic allocation, and the host provides the domain name service, by using DDNS, the effect on the domain name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

To configure DDNS, perform the following steps:

Steps

1. On the **Application** tab, select **DDNS**, as shown in Figure 56.

Figure 56 DDNS



2. Configure the DDNS parameters, as shown in Figure 57.

Figure 57 DDNS Configuration

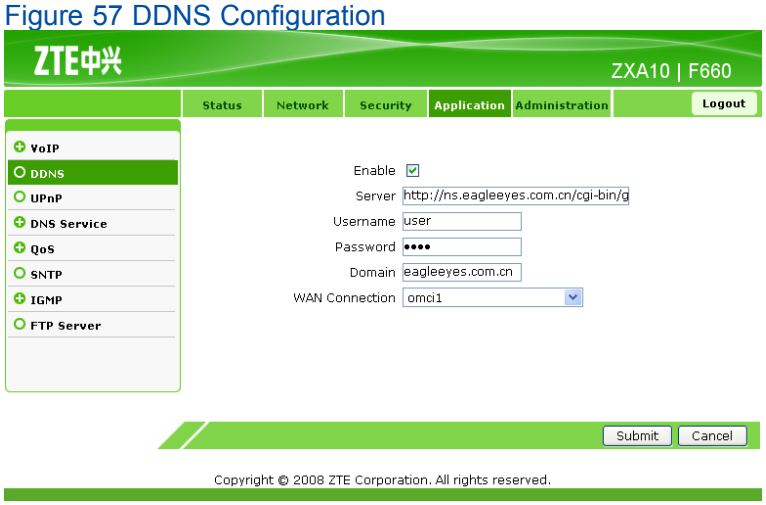


Table 28 lists the parameters for DDNS configuration.

Table 28 Parameters for DDNS Configuration

Parameter	Description
Enable	To enable the DDNS function
Server	Server address If the GNUDIP HTTP protocol is used, the sever address is a URL address. By default, it is http://ns.eagleeyes.com.cn/cgi-bin/gdipupdt.cgi.
Username	DDNS server user name
Password	DDNS server password
Domain	Domain name corresponding to the user, valid only when the GNUDIP protocol is used
WAN Connection	WAN-side connection interface

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

– End of Steps –

Result

DDNS is configured.

6.3 Configuring UPnP

ShortDescription

Perform this procedure to configure UPnP.

Pre-requisites

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

Context

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

To configure UPnP, perform the following steps:

Steps

1. On the **Application** tab, select **UPnP**, as shown in Figure 58.

Figure 58 UPnP

2. Configure the UPnP parameters, as shown in Figure 59.

Figure 59 UPnP Configuration

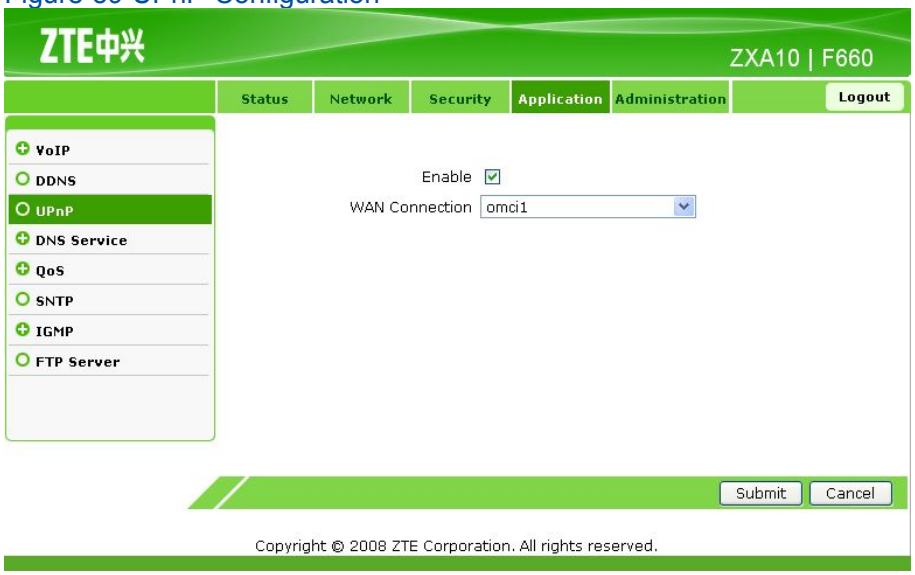


Table 29 lists the UPnP parameters.

Table 29 UPnP Parameters

Parameter	Description
Enable	To enable UPnP
WAN Connection omci1	WAN-side connection interface

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

– End of Steps –

Result

UPnP is configured.

6.4 DNS Configuration

This topic includes the following:

- Configuring Domain Name
- Configuring Host Name

6.4.1 Configuring Domain Name

ShortDescription

Perform this procedure to configure the domain name.

Pre-requisites

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

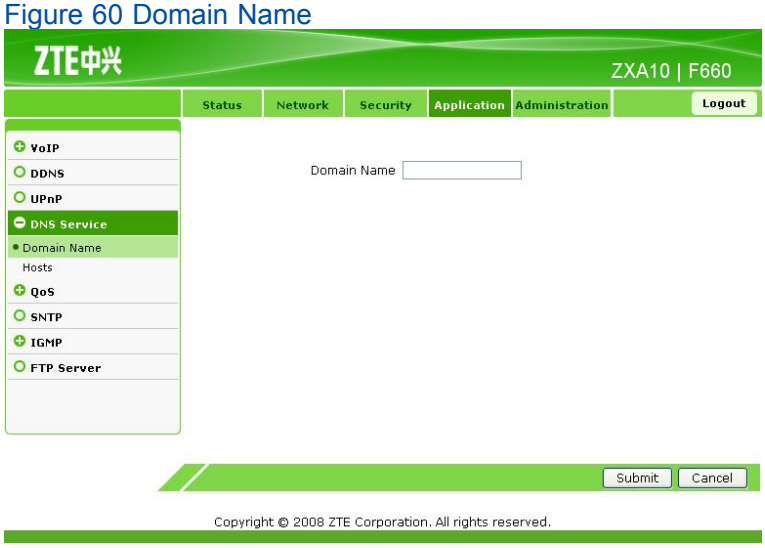
Context

To configure the domain name, perform the following steps:

Steps

1. On the **Application** tab, select **DNS Service**. By default, **Domain Name** is selected, as shown in Figure 60.

Figure 60 Domain Name



2. Set **Domain Name**.
3. Click **Submit** to finish the configuration. Click **Cancel** to cancel the configuration.

– End of Steps –

Result

The domain name is configured.

6.4.2 Configuring Host Name

ShortDescription

Perform this procedure to configure the host name.

Pre-requisites

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

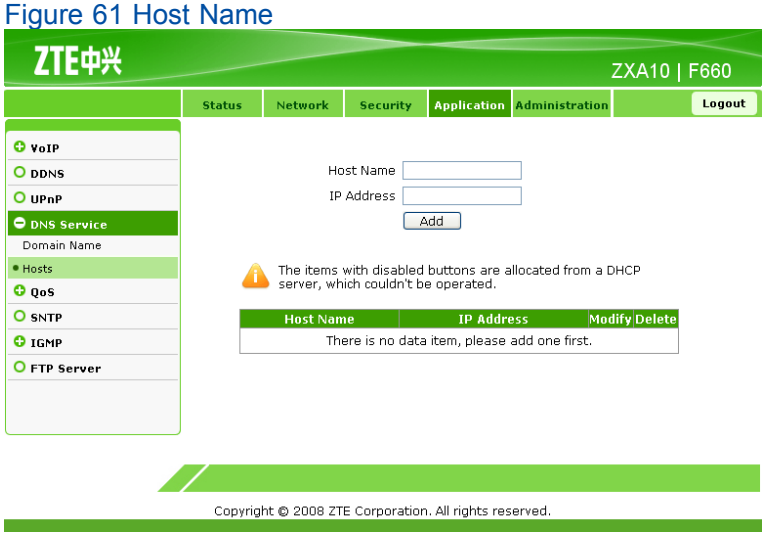
Context

To configure the host name, perform the following steps:

Steps

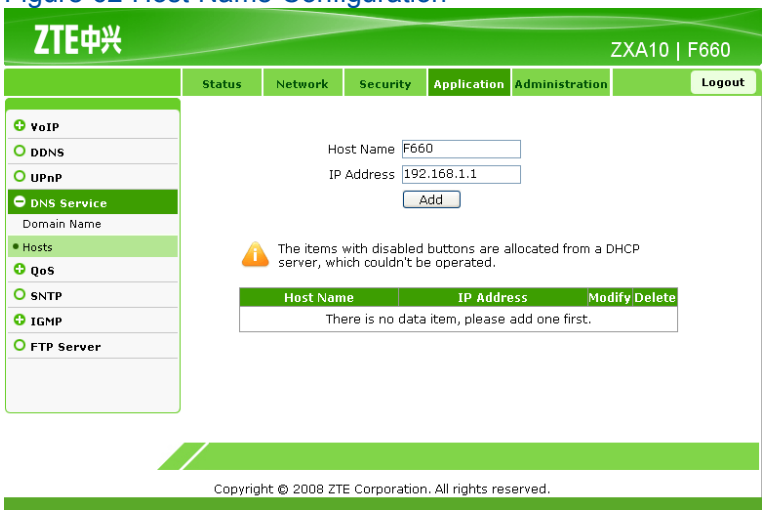
1. On the **Application** tab, select **DNS Service**, and then select **Hosts**, as shown in Figure 61.

Figure 61 Host Name



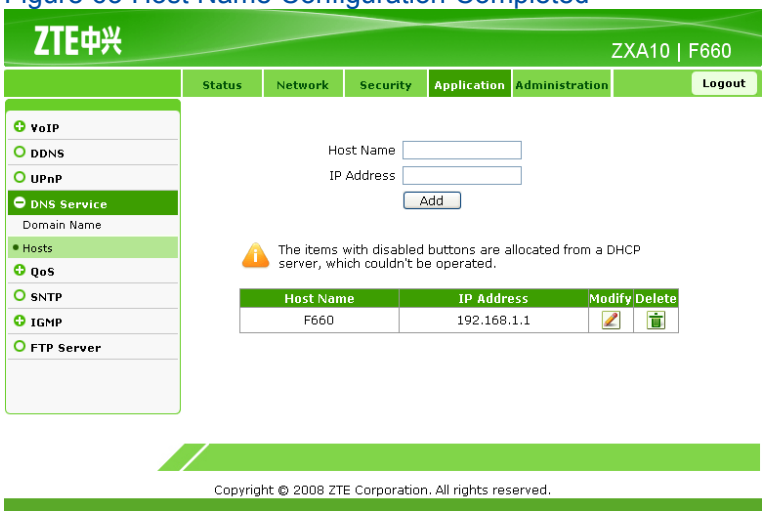
2. Set **Host Name** and **IP Address**, as shown in Figure 62.

Figure 62 Host Name Configuration



3. Click **Add** to finish the configuration, as shown in Figure 63. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

Figure 63 Host Name Configuration Completed



– End of Steps –

Result

The host name is configured.

6.5 QoS Configuration

This topic includes the following:

- Configuring Basic QoS Parameters
- Configuring QoS Rule
- Configuring QoS Rule Type
- Configuring QoS Local Application
- Configuring QoS Queue Management

- Configuring QoS Ingress Rate Limit

6.5.1 Configuring Basic QoS Parameters

ShortDescription

Perform this procedure to configure the basic QoS parameters.

Pre-requisites

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

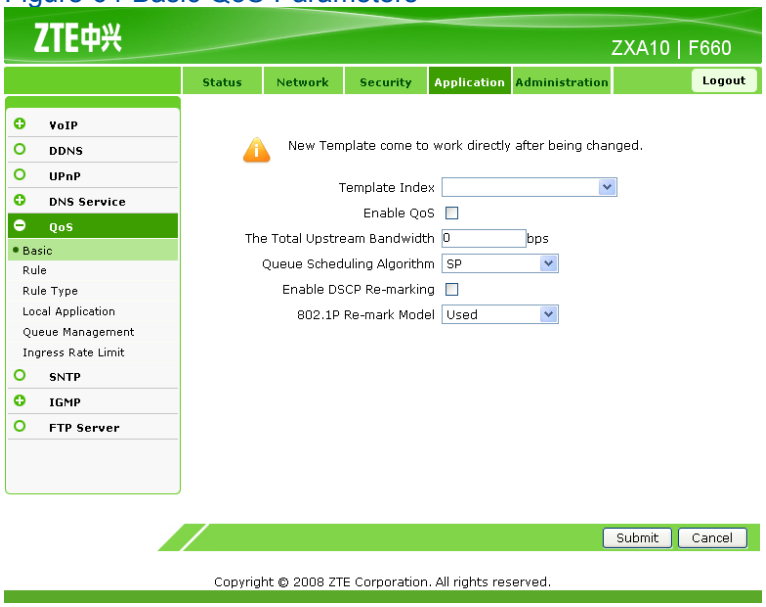
Context

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

Steps

1. On the **Application** tab, select **QoS**. By default, **Basic** is selected, as shown in Figure 64.

Figure 64 Basic QoS Parameters



NOTE **Note**

The template index is enabled immediately after changed.

2. Configure the basic QoS parameters, as shown in Figure 65.

Figure 65 Basic QoS Parameter Configuration

Table 30 lists the basic QoS parameters.

Table 30 Basic QoS Parameters

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

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

– End of Steps –

Result

The basic QoS parameters are configured.

6.5.2 Configuring QoS Rule

ShortDescription

Perform this procedure to configure the QoS rule.

Pre-requisites

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

Context

To configure the QoS rule, perform the following steps:

Steps

1. On the **Application** tab, select **QoS**, and then select **Rule**, as shown in Figure 66.

Figure 66 QoS Rule

2. Configure the QoS rule parameters, as shown in Figure 67.

Figure 67 QoS Rule Configuration

Table 31 lists the parameters for QoS rule configuration.

Table 31 Parameters for QoS Rule Configuration

Parameter	Description
802.1p Re-marking	802.1P remarking
DSCP Re-marking	DSCP remarking
CAR(Committed Access Rate)	Ingress rate limit rule
Queue	Congestion management queue

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

– End of Steps –

Result

The QoS rule is configured.

6.5.3 Configuring QoS Rule Type

ShortDescription

Perform this procedure to configure the QoS rule type.

Pre-requisites

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

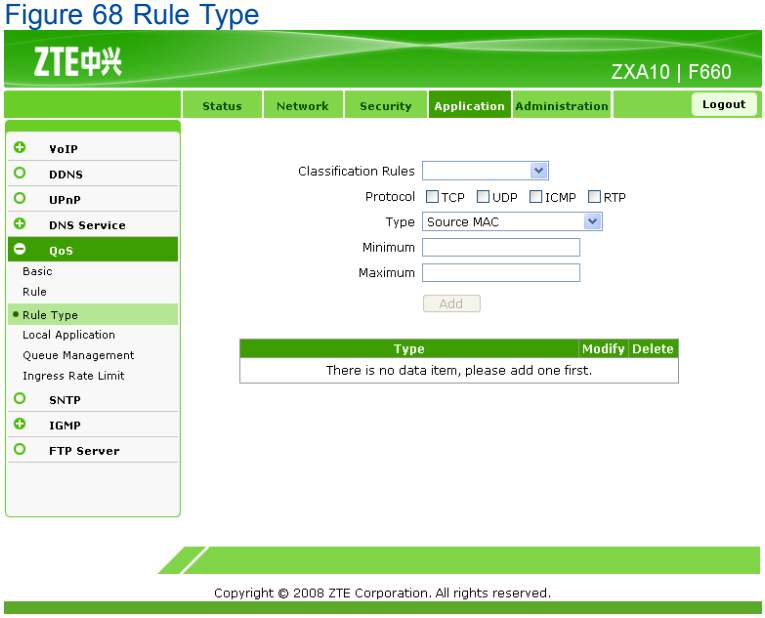
Context

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

Steps

1. On the **Application** tab, select **QoS**, and then select **Rule Type**, as shown in Figure 68.

Figure 68 Rule Type



2. Configure the QoS rule type parameters, as shown in Figure 69.

Figure 69 Rule Type Configuration

Table 32 lists the parameters for QoS rule type Configuration

Table 32 Parameters for QoS Rule Type Configuration

Parameter	Description
Classification Rules	Classification rules

Parameter	Description
Protocol	Protocol Range: TCP, UDP, ICMP, and RTP
Type	Type
Minimum	Minimum value
Maximum	Maximum value

3. Click **Add** to finish the configuration, as shown in Figure 70.

Figure 70 Rule Type Configuration Completed

4. Click **Modify** to modify the configuration. Click **Delete** to delete the configuration.

– End of Steps –

Result

The QoS rule type is configured.

6.5.4 Configuring QoS Local Application

ShortDescription

Perform this procedure to configure the QoS local application.

Pre-requisites

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

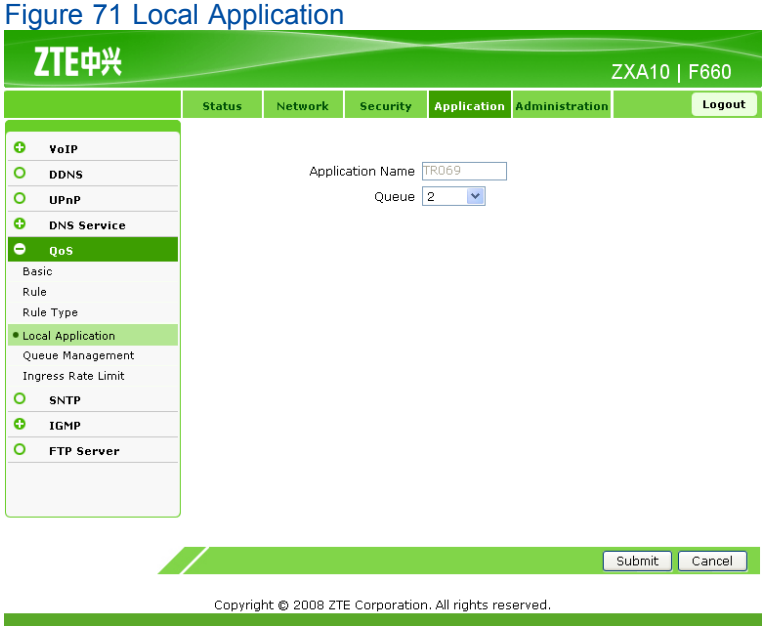
Context

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

Steps

1. On the **Application** tab, select **QoS**, and then select **Local Application**, as shown in Figure 71.

Figure 71 Local Application



2. In the **Queue** drop-down list, select a queue number.

NOTE **Note**

At present, only the Tr-069 service mode is supported.

---

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

– End of Steps –

Result

The QoS local application is configured.

6.5.5 Configuring QoS Queue Management

ShortDescription

Perform this procedure to configure QoS queue management.

Pre-requisites

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

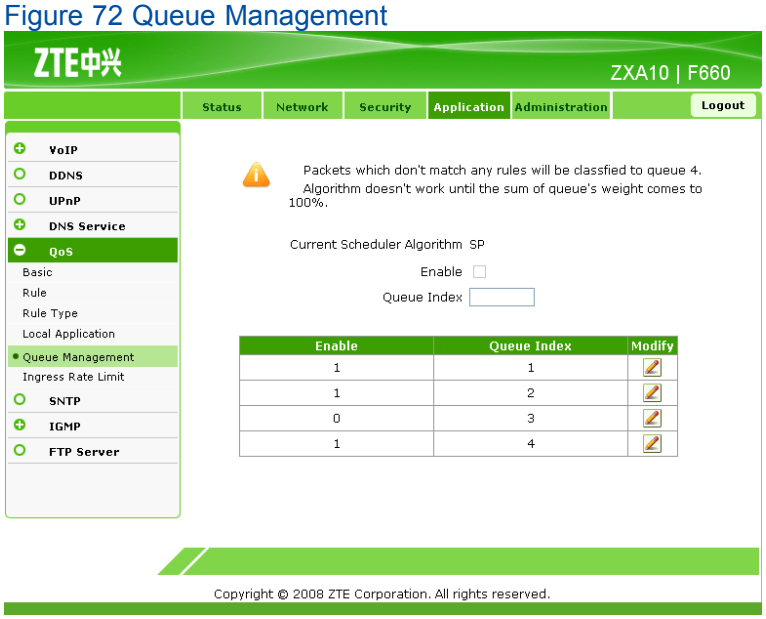
Context

To configure QoS queue management, perform the following steps:

Steps

1. On the **Application** tab, select **QoS**, and then select **Queue Management**, as shown in Figure 72.

Figure 72 Queue Management



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

NOTE **Note**

1 indicates enabled and **0** indicates disabled.

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

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

– End of Steps –

Result

QoS queue management is configured.

6.5.6 Configuring QoS Ingress Rate Limit

ShortDescription

Perform this procedure to configure the QoS ingress rate limit.

Pre-requisites

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

Context

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

Steps

1. On the **Application** tab, select **QoS**, and then select **Ingress Rate Limit**, as shown in Figure 73.

Figure 73 Ingress Rate Limit

2. Configure the parameters for QoS ingress rate limit, as shown in Figure 74.

Figure 74 Ingress Rate Limit Configuration

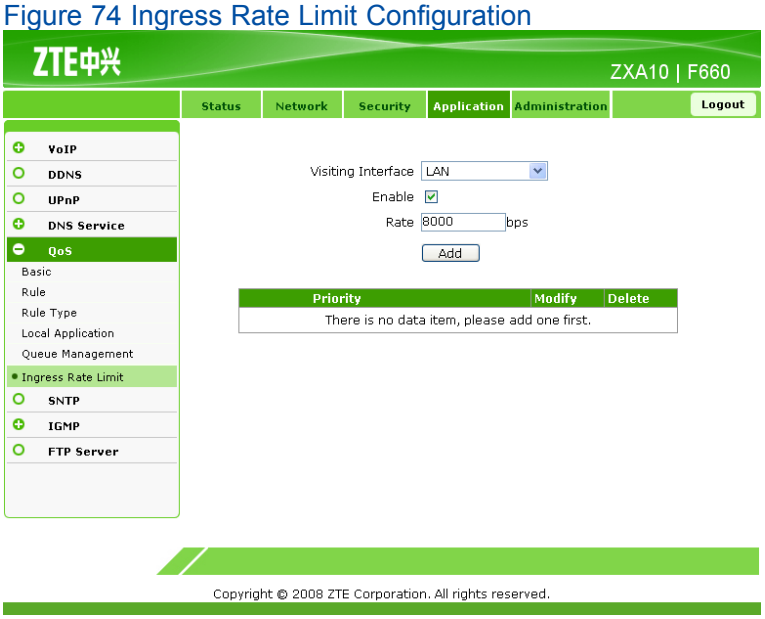


Table 33 lists the parameters for ingress rate limit configuration.

Table 33 Parameters for Ingress Rate Limit Configuration

Parameter	Description
Visiting Interface	User interface for the rate limit rule
Enable	To enable the ingress rate limit function
Rate	Limit rate 8000 bps – 104857600 bps

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

– End of Steps –

Result

The QoS ingress rate limit is configured.

6.6 Configuring SNTP Client

ShortDescription

Perform this procedure to configure the SNTP client.

Pre-requisites

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

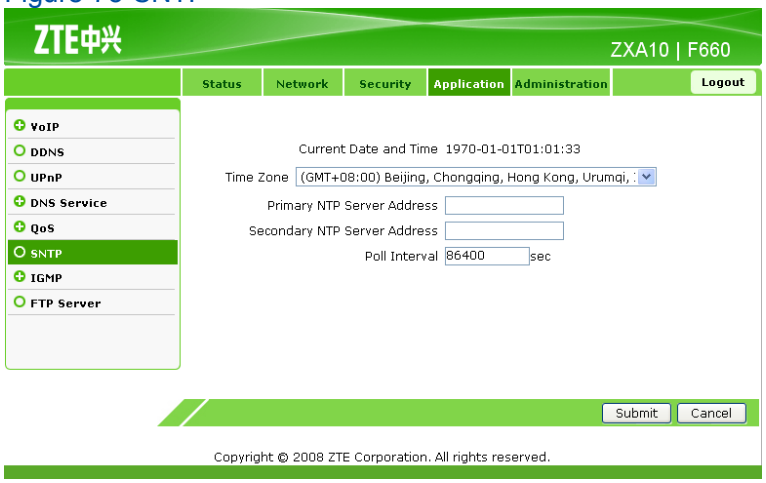
Context

To configure the SNTP client, perform the following steps:

Steps

1. On the **Application** tab, select **SNTP**, as shown in Figure 75.

Figure 75 SNTP



2. Configure the SNTP parameters, as shown in Figure 75.

Figure 76 SNTP Configuration

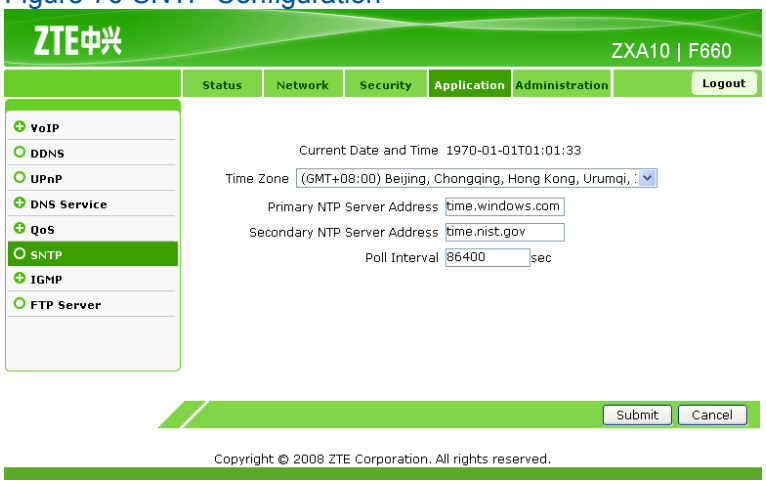


Table 34 lists the SNTP parameters.

Table 34 SNTP Parameters

Parameter	Description
Time Zone	Time zone where the subscriber is located
Primary NTP Server Address	IP address of the primary NTP server
Secondary NTP Server Address	IP address of the secondary NTP server
Poll Interval	Interval for server synchronization Unit: second

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

– End of Steps –

Result

The SNTP client is configured.

6.7 IGMP Configuration

This topic includes the following:

- Configuring Basic IGMP Parameters
- Configuring Multicast VLAN
- Configuring Multicast MAC Limit
- Configuring MVLAN Tag Strip

6.7.1 Configuring Basic IGMP Parameters

ShortDescription

Perform this procedure to configure the basic IGMP parameters.

Pre-requisites

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

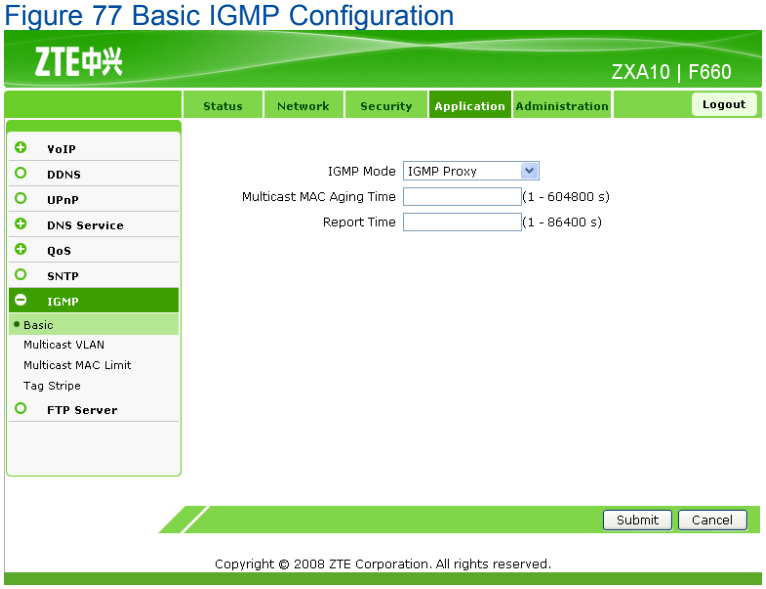
Context

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

Steps

1. On the **Application** tab, select **IGMP**. By default, **Basic** is selected, as shown in Figure 77.

Figure 77 Basic IGMP Configuration



2. **IGMP Mode** includes **IGMP Snooping**, **IGMP Proxy**, and **Disabled**. **Disabled** indicates to disable the IGMP mode configuration.

- Configure **IGMP Snooping**.

  From the **IGMP Mode** drop-down list, select **IGMP Snooping**, as shown in Figure 78.

Figure 78 IGMP Snooping Configuration

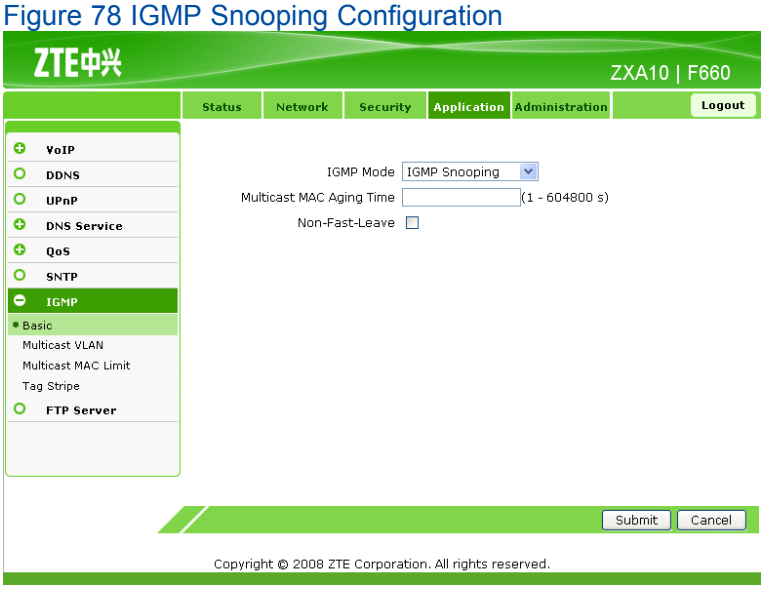


Table 35 lists the parameters for IGMP snooping configuration.

Table 35 Parameters for IGMP Snooping Configuration

Parameter	Description
IGMP Mode	IGMP mode
Multicast MAC Aging Time	Aging time of the multicast address
Non-Fast-Leave	To enable the Non-Fast-Leave mode

- Configure **IGMP Proxy**.

  From the **IGMP Mode** drop-down list, select **IGMP Proxy**, as shown in Figure 79.

Figure 79 IGMP Proxy Configuration

Table 36 lists the parameters for IGMP proxy configuration.

Table 36 Parameters for IGMP Proxy Configuration

Parameter	Description
IGMP Mode	IGMP mode
Multicast MAC Aging Time	Aging time of the multicast address
Report Time	Periodical report time of multicast messages

Note

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

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

– End of Steps –

Result

The basic IGMP parameters are configured.

6.7.2 Configuring Multicast VLAN

ShortDescription

Perform this procedure to configure the multicast VLAN.

Pre-requisites

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

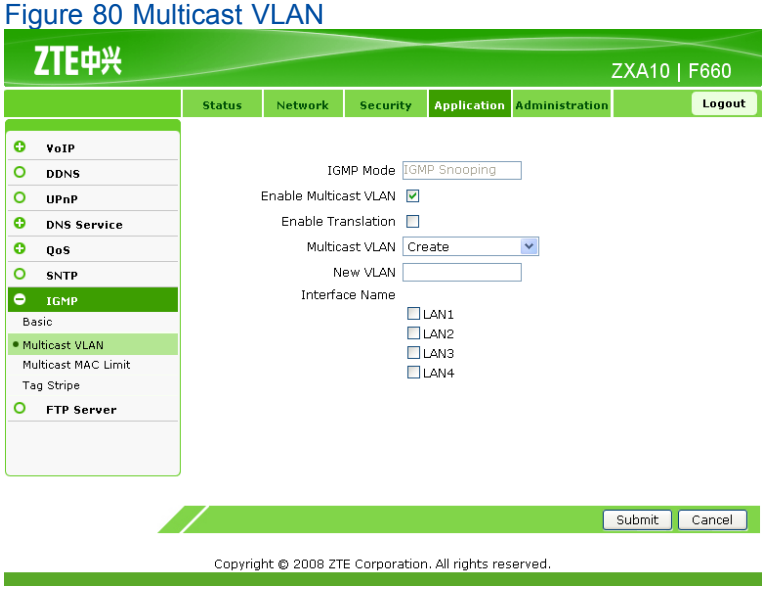
Context

To configure the multicast VLAN, perform the following steps:

Steps

1. On the **Application** tab, select **IGMP**, and then select **Multicast VLAN**, as shown in Figure 80.

Figure 80 Multicast VLAN



2. Configure the multicast VLAN parameters, as shown in Figure 81.

Figure 81 Multicast VLAN Configuration

Table 37 lists the parameters for the multicast VLAN configuration.

Table 37 Parameters for Multicast VLAN Configuration

Parameter	Description
IGMP Mode	IGMP mode, configured on the **Basic** tab
Enable Multicast VLAN	To enable the multicast VLAN function
Enable Translation	To enable multicast VLAN translation
Multicast VLAN	To create a multicast VLAN
New VLAN	Multicast VLAN ID
Interface Name	LAN interface to be added to the multicast VLAN

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

– End of Steps –

Result

The multicast VLAN is configured.

6.7.3 Configuring Multicast MAC Limit

ShortDescription

Perform this procedure to configure multicast MAC limit.

Pre-requisites

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

Context

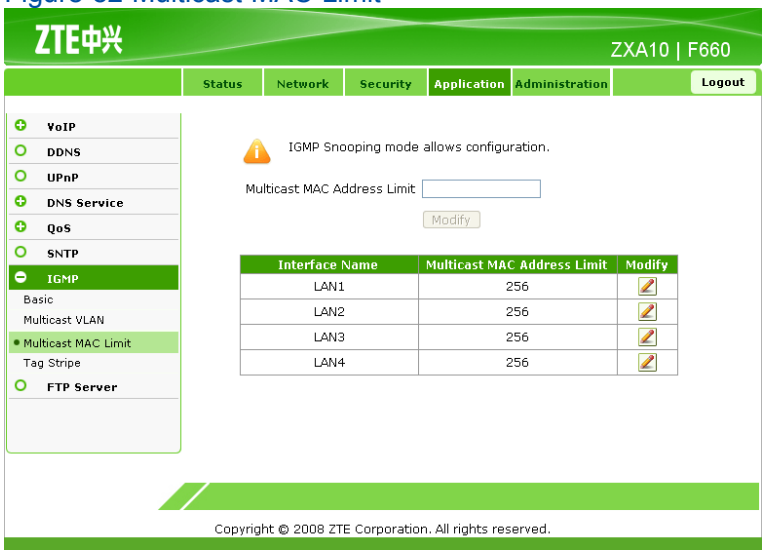
The multicast MAC limit function can be configured only when the IGMP mode is **IGMP Snooping**. **IGMP Proxy** does not support this function.

To configure multicast MAC limit, perform the following steps:

Steps

1. On the **Application** tab, select **IGMP**, and then select **Multicast MAC Limit**, as shown in Figure 82.

Figure 82 Multicast MAC Limit



2. Click the **Modify** icon to configure the multicast MAC limit, as shown in Figure 83.

Figure 83 Multicast MAC Limit Configuration

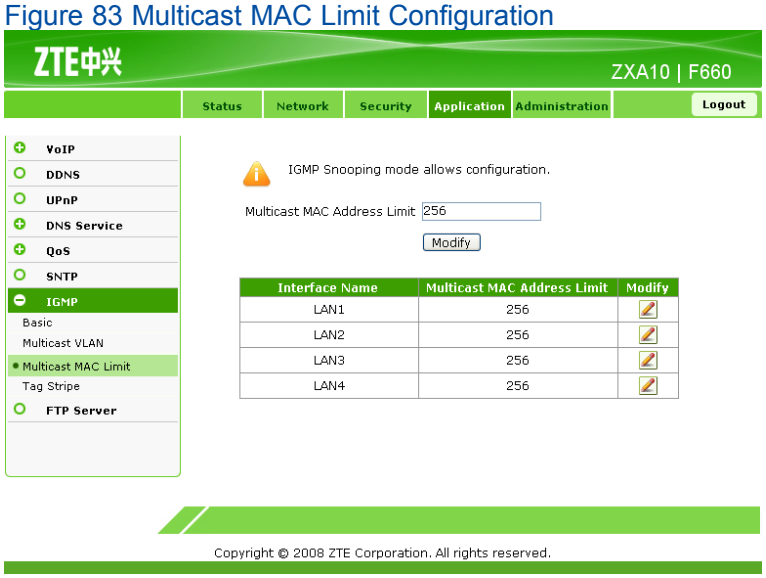


Table 38 lists the parameters for the multicast MAC limit configuration.

Table 38 Parameters for Multicast MAC Limit Configuration

Parameter	Description
Multicast MAC Address Limit	Maximum multicast addresses for each LAN port Range: 0 – 256

3. Click **Modify**.

– End of Steps –

Result

Multicast MAC limit is configured.

6.7.4 Configuring MVLAN Tag Strip

ShortDescription

Perform this procedure to configure MVLAN tag strip.

Pre-requisites

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

Context

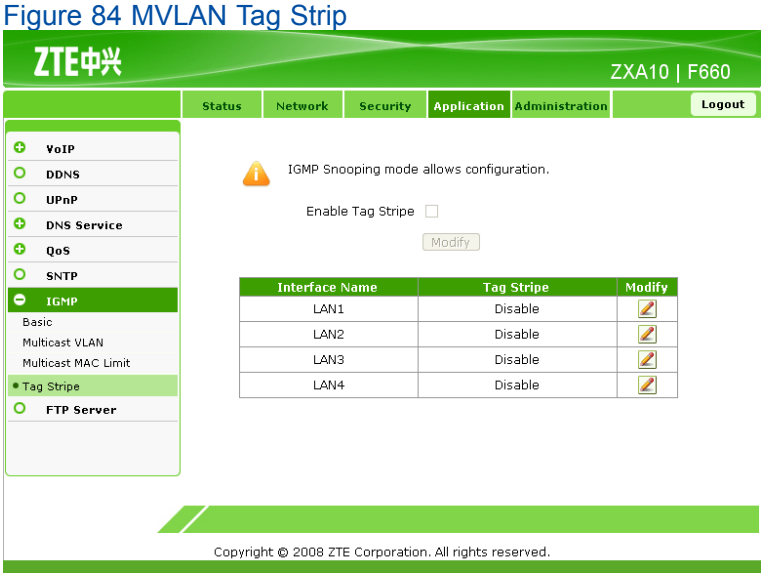
The MVLAN tag strip function can be configured only when the IGMP mode is **IGMP Snooping**. **IGMP Proxy** does not support this function.

To configure MVLAN tag strip, perform the following steps:

Steps

1. On the **Application** tab, select **IGMP**, and then select **Tag Stripe**, as shown in Figure 84.

Figure 84 MVLAN Tag Strip



2. Click the **Modify** icon to configure MVLAN tag strip, as shown in Figure 85.

Figure 85 MVLAN Tag Strip Configuration

Table 39 lists the parameters for MVLAN tag strip configuration.

Table 39 Parameters for MVLAN Tag Strip Configuration

Parameter	Description
Enable Tag Stripe	To enable the MVLAN tag strip function

3. Click **Modify**.

– End of Steps –

Result

MVLAN tag strip is configured.

6.8 Configuring FTP Application

ShortDescription

Perform this procedure to configure FTP application.

Pre-requisites

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

Context

To configure FTP application, perform the following steps:

Steps

1. On the **Application** tab, select **FTP Application**, as shown in Figure 86.

Figure 86 FTP Server

2. Configure the FTP server parameters, as shown in Figure 87.

Figure 87 FTP Server Configuration

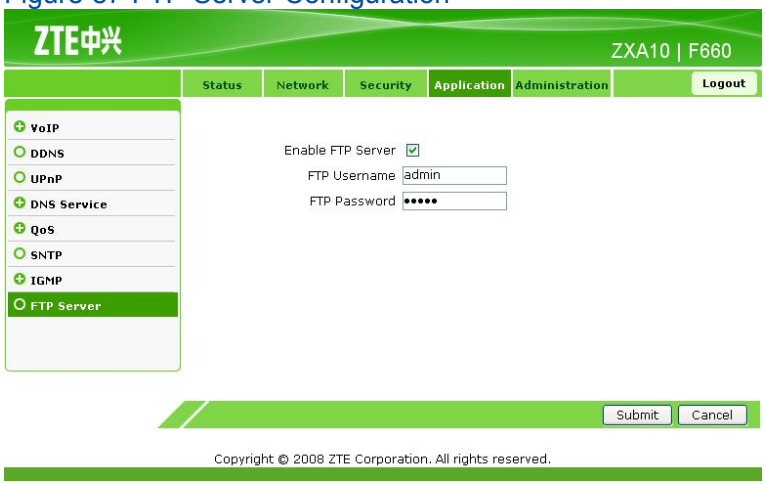


Table 40 lists the FTP server parameters.

Table 40 FTP Server Parameters

Parameter	Description
Enable FTP Server	To enable the FTP server
FTP Username	FTP login user name
FTP Password	FTP login password

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

– End of Steps –

Result

FTP application is configured.

Chapter 7
Device Management

Table of Contents

7.1 TR-069 Configuration

This topic includes the following:

- Configuring Basic TR-069 Parameters
- Importing TR-069 Certificate

7.1.1 Configuring Basic TR-069 Parameters

ShortDescription

Perform this procedure to configure the basic TR-069 parameters.

Pre-requisites

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

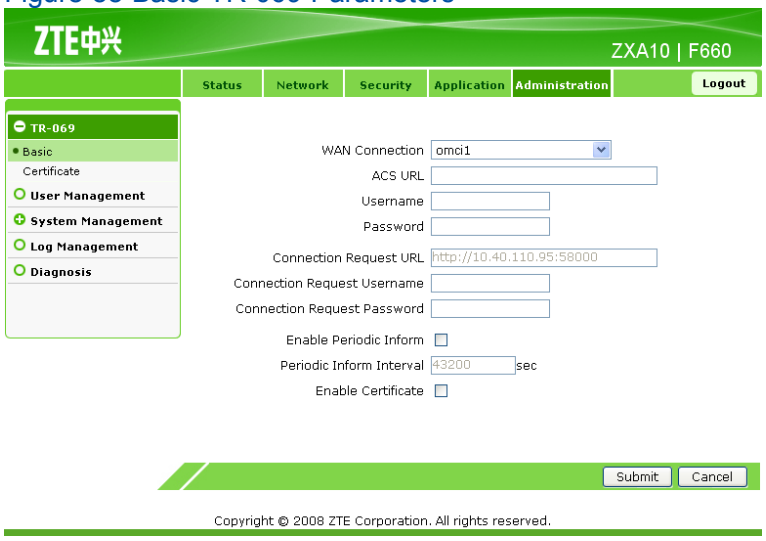
Context

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

Steps

1. On the **Administration** tab, select **TR-069**. By default, **Basic** is selected, as shown in Figure 88.

Figure 88 Basic TR-069 Parameters



2. Configure the basic TR-069 parameters, as shown in Figure 89.

Figure 89 Basic TR-069 Parameter Configuration

Table 41 lists the basic TR-069 parameters.

Table 41 Basic TR-069 Parameters

Parameter	Description
WAN Connection	WAN-side connection interface
ACS URL	Network server URL
Username	User name
Password	Password
Connection Request URL	Connection request URL
Connection Request Username	Connection request user name

Parameter	Description
Connection Request Password	Connection request password
Enable Periodic Inform	To enable periodic report
Periodic Inform Interval	Periodic report interval
Enable Certificate	To enable certificate

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

– End of Steps –

Result

The basic TR-069 parameters are configured.

7.1.2 Importing TR-069 Certificate

ShortDescription

Perform this procedure to import the TR-069 certificate.

Pre-requisites

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

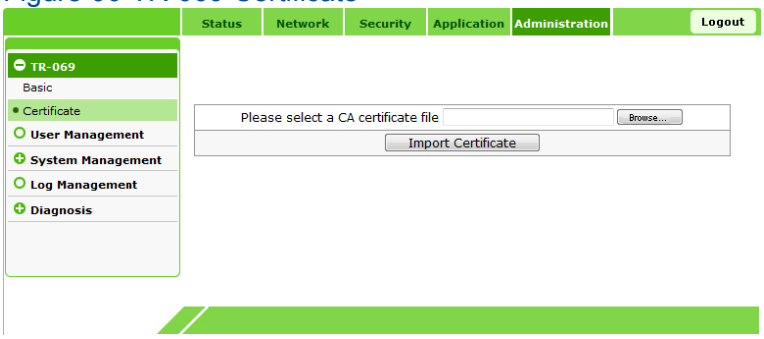
Context

To import the TR-069 certificate, perform the following steps:

Steps

1. On the **Administration** tab, select **TR-069**, and then select **Certificate**, as shown in Figure 90.

Figure 90 TR-069 Certificate



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

– End of Steps –

Result

The TR-069 certificate is imported.

7.2 User Management

ShortDescription

Perform this procedure to manage users.

Pre-requisites

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

Context

To manage users, perform the following steps:

Steps

1. On the **Administration** tab, select **User Management**, as shown in Figure 91.

Figure 91 User Management

2. Configure the user management parameters.

Note

User Right includes **Administrator** and **User**.

---

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

– End of Steps –

Result

User management is complete.

7.3 Device Management

This topic includes the following:

- System Management
- Software Upgrade
- Configuration Management

7.3.1 System Management

ShortDescription

Perform this procedure to manage the system.

Pre-requisites

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

Context

To manage the system, perform the following steps:

Steps

1. On the **Administration** tab, select **System Management**, as shown in Figure 92.

Figure 92 System Management

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

– End of Steps –

Result

System management is complete.

7.3.2 Software Upgrade

ShortDescription

Perform this procedure to upgrade the software.

Pre-requisites

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

Context

Caution

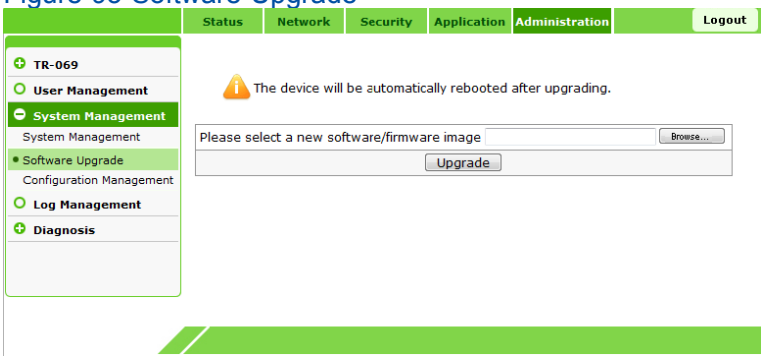
Generally, the software is upgraded by the ZTE CORPORATION engineers. If the user wants to upgrade the software, contact the local office of ZTE CORPORATION to obtain the latest software version.

To upgrade the software, perform the following steps:

Steps

1. On the **Administration** tab, select **System Management**, and then select **Software Upgrade**, as shown in Figure 93.

Figure 93 Software Upgrade



2. Click **Browse** to select the software version.
3. Click **Upgrade** to upgrade the software, as shown in Figure 94.

Figure 94 Upgrading Software

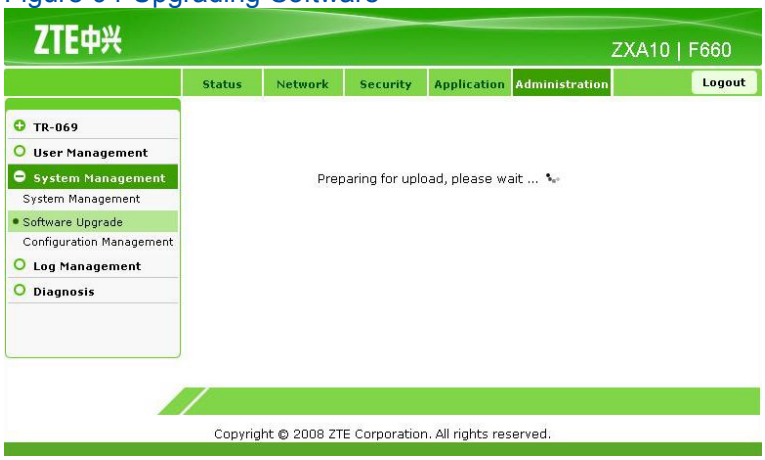


Figure 95 shows the result of software upgrade.

Figure 95 Software Upgrade Completed

Note

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

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

– End of Steps –

Result

The software is upgraded.

7.3.3 Configuration Management

ShortDescription

Perform this procedure to manage the device configuration.

Pre-requisites

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

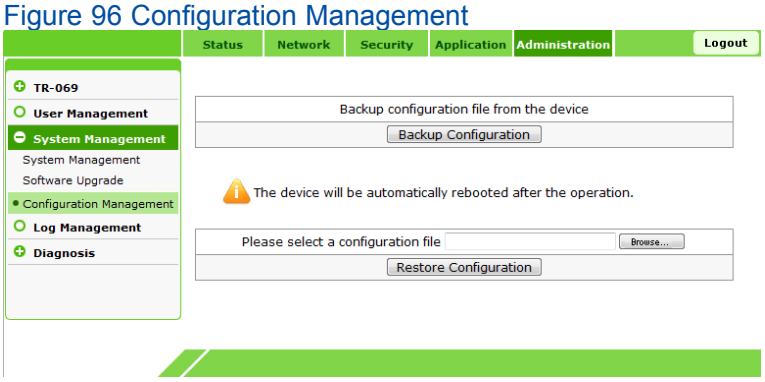
Context

To manage the device configuration, perform the following steps:

Steps

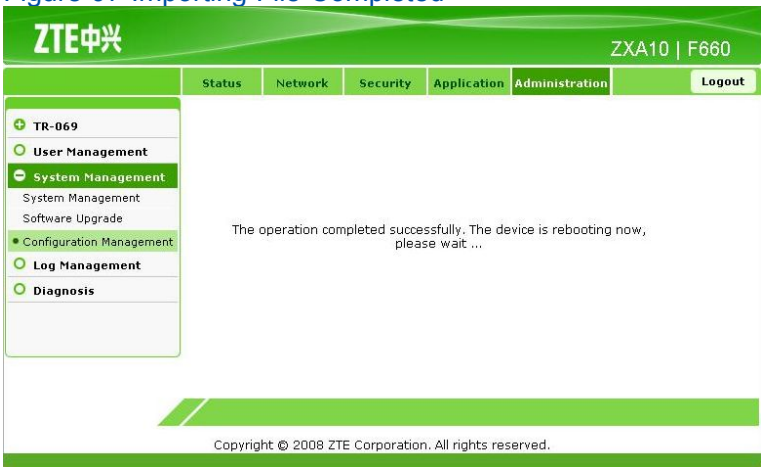
1. On the **Administration** tab, select **System Management**, and then select **Configuration Management**, as shown in Figure 96.

Figure 96 Configuration Management



2. Click **Backup Configuration** to back up the existing configuration file.
3. Click **Browse** to select the backed up configuration file.
4. Click **Restore Configuration** to restore the backed up configuration file, as shown in Figure 97.

Figure 97 Importing File Completed



– End of Steps –

Result

The configuration management is complete.

7.4 Log Management

ShortDescription

Perform this procedure to manage logs.

Pre-requisites

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

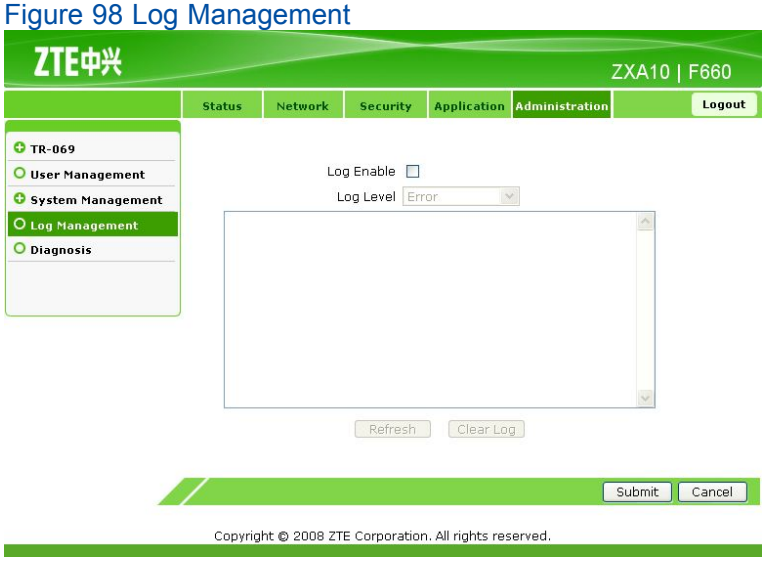
Context

To manage logs, perform the following steps:

Steps

1. On the **Administration** tab, select **Log Management**, as shown in Figure 98.

Figure 98 Log Management



2. Configure the log management parameters, as listed in Table 42.

Table 42 Log Management Parameters

Parameter	Description
Log Enable	Whether to enable the log server
Log Level	Log level, including **Debug**, **Informational**, **Notice**, **Warning**, **Error**, **Critical**, **Alert**, and **Emergency** When **Log Level** is configured, only the logs above the specified level are saved.

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

– End of Steps –

Result
Log management is complete.

7.5 Ping Diagnosis

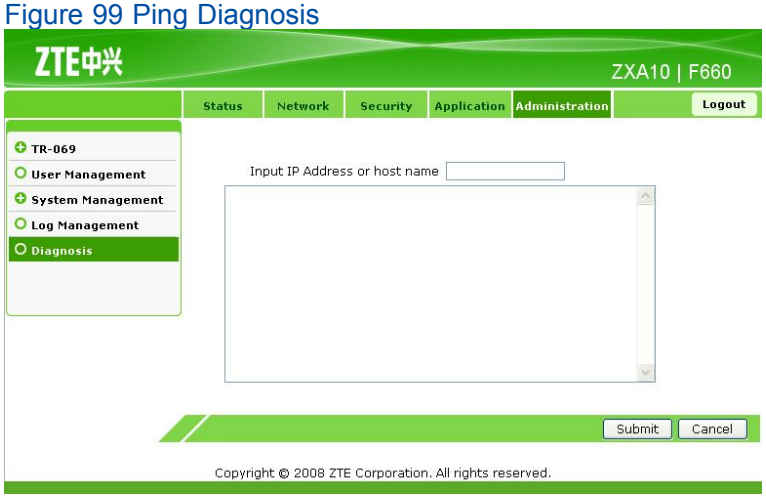
ShortDescription
Perform this procedure to diagnose ping connection.

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

Context
To diagnose ping connection, perform the following steps:

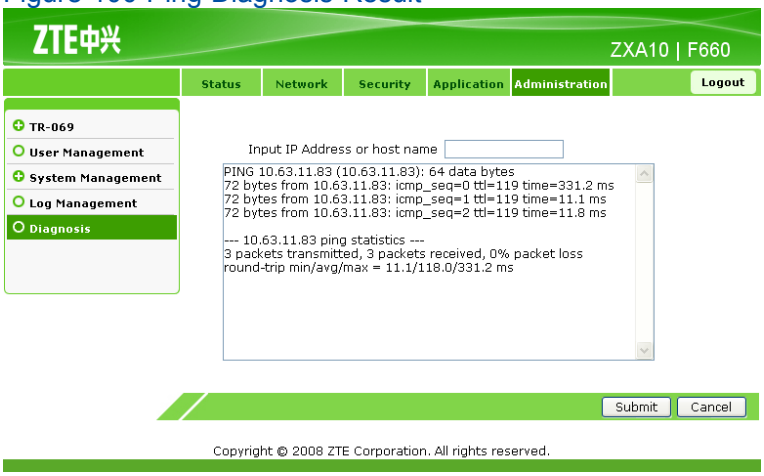
Steps
1. On the **Administration** tab, select **Diagnosis**, as shown in Figure 99.

Figure 99 Ping Diagnosis



2. In **Input IP Address or host name** , enter the host IP address or host name.
3. Click **Submit** to diagnose the connection, as shown in Figure 100. Click **Cancel** to cancel the configuration.

Figure 100 Ping Diagnosis Result



– End of Steps –

Result

Ping diagnosis is complete.

Appendix A
FAQ

Table of Contents:

A .1 FAQ

How Can I set TCP/IP on the Computer Connected to the Device?

The default device IP address is `192.168.1.1`. Therefore, set the computer IP address to 192.168.1.2 – 192.168.1.254 and the subnet mask to 255.255.255.0.

How Can I Ensure That My Computer Is Successfully Connected to the Device?

On the command line interface, carry out the **ping 192.168.1.1** command. If the connection fails, the interface prompts connection timeout.

How Can I Set the Device Through the Web Interface?

Make sure that the computer is connected to the device. Then open the Internet Explorer and enter `http://192.168.1.1` on the address bar to access the Web interface of the device. The default user name and password are `admin`.

How Can I Restore the Device to the Factory Default Settings?

Press the **RST** reset button for more than 10 seconds to reboot the device. Then the device is restored to the factory default settings.

Why Is the PON Link Indicator Always OFF?

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

Why Does the Device Fail to Make a Call?

Check whether the telephone cable is correctly connected to the POTS1 or POTS2 port. Then access the Web interface of the device. Click the **Application** tab to check the

VoIP configuration. If the VoIP configuration is correct and the telephone cable is correctly connected, but the call still cannot be made, contact the service provider.

Index

S

U

V

W

Glossary

CNG
- Comfort Noise Generation

DC
- Direct Current

DDNS
- Dynamic Domain Name Server

DHCP
- Dynamic Host Configuration Protocol

DMZ
- Demilitarized Zone

DNAT
- Destination Network Address Translation

DNS
- Domain Name Server

DSCP
- Differentiated Services Code Point

DSL
- Digital Subscriber Line

DTMF
- Dual-ToneMulti-Frequency

DWRR
- Deficit Weighted Round Robin

FTP
- File Transfer Protocol

FTTH
- Fiber to the Home

GE
- Gigabit Ethernet

GPON
- Gigabit Passive Optical Network

HTTP
- Hypertext Transfer Protocol

ICMP
- Internet Control Message Protocol

IEEE
- Institute of Electrical and Electronics Engineers

IGMP
- Internet Group Management Protocol

IP
- Internet Protocol

IPTV
- Internet Protocol Television

ISP
- Internet Service Provider

ITU
- International Telecommunications Union

LAN
- Local Area Network

MAC
- Medium Access Control

NAT
- Network Address Translation

NTP
- Network Time Protocol

OLT
- Optical Line Terminal

OMCI
- ONT Management Control Interface

ONT
- Optical Network Terminal

ONU
- Optical Network Unit

PON
- Passive Optical Network

POTS
- Plain Old Telephone Service

PPPoE
- Point to Point Protocol over Ethernet

QoS
- Quality of Service

RF
- Radio Frequency

RTP
- Real-time Transport Protocol

SIP
- Session Initiation Protocol

SNTP
- Simple Network Time Protocol

SP
- Strict Priority

SS
- Soft Switch

TCP
- Transfer Control Protocol

TCP/IP
- Transfer Control Protocol/Internet Protocol

UDP
- User Datagram Protocol

URL
- UniformResource Locator

VAD
- Voice Activity Detectors

VLAN
- Virtual Local Area Network

VoIP
- Voice over Internet Protocol

WAN
- Wide Area Network

WEP
- Wired Equivalent Privacy

WLAN
- Wireless Local Area Network

WPA
- Wi-Fi Protected Access