ZXA10 F460/F460B

Optical Network Unit

User Manual

Version 1.0

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

LEGAL INFORMATION

Revision History

Revision No.	Revision Date	Revision Reason
1.0	20/07/2009	First edition

Contents

About This Manual

Purpose

This manual provides procedures and guidelines that support the operation of the ZXA10 F460/F460B Optical Network Unit (the ZXA10 F460/F460B for short).

Intended Audience

This manual is intended for engineers and technicians who perform operation activities on the ZXA10 F460/F460B.

Prerequisite Skill and Knowledge

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

- ZXA10 system and its various components
- Local operating procedures

What Is in This Manual

This manual contains the following chapters:

Chapter	Summary
Chapter 1, Brief Introduction	Provides an overview of the product, including the component list, product features, appearance, and system requirements.
Chapter 2, System Connection	Describes the system application scenario, LAN interface connection, PON broadband port connection, telephone connection, and power adapter connection.
Chapter 3, Configuration Preparation	Describes the procedures for installing TCP/IP, configuration TCP/IP, checking TCP/IP configuration, and logging in to the device.
Chapter 4, Device Status	Describes the device information, network interface information, user interface information, and VoIP information.
Chapter 5, Network Configuration	Describes the configuration of WAN connection, WLAN, address management, route management, and PON broadband port.
Chapter 6, Security Configuration	Describes the procedures for configuring the firewall, IP filter, and URL filter.

Chapter	Summary
Chapter 7, Application Configurations	Describes the configuration of VoIP, DDNS, DMZ host, UPnP, port forwarding, DNS server, QoS, SNTP client, IGMP, and FTP application.
Chapter 8, Administration	Describes TRO69 configuration, user management, device management, log management, and diagnosis maintenance.
Chapter 9, Typical Applications	Describes the configuration of Internet access, VoIP application, WLAN access, and FTP server.

Conventions

ZTE documents employ the following typographical conventions.

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

Mouse operation conventions are listed as follows:

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

Information to User

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

NOTE 2: The Transmitter is using Internal antennas that operate at 20 cm or more from nearby persons. The power density at 20 cm is802.11b/g: 0.016mW/cm²

Declaration of RoHS Compliance

To minimize the environmental impact and take more responsibility to the earth we live, this document shall serve as formal declaration that F460/F460B manufactured by ZTE CORPORATION are in compliance with the Directive 2002/95/EC of the European Parliament - RoHS (Restriction of Hazardous Substances) with respect to the following substances:

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

…

The F460/F460B manufactured by ZTE CORPORATION meet 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 Brief Introduction

Product Introduction

Thank you for using the ZXA10 F460/F460B integrated gateway products.

ZXA10 F460/F460B is a modular access device at the user end. It adopts computer network and broadband optical network access technologies to build household network center, which interconnects network devices at your home to access the Internet. It provides users with colorful, diversified, personalized, convenient, comfortable, safe and efficient services.

Ports and functions of ZXA10 F460/F460B are introduced in Table 1.

Table 1 Functions of ZXA10 F460/F460B

Model	Port	Function
F460/F460B	4 GE ports, 2 POTS ports, 1 WIFI port, 2 USB ports	Support VoIP and WLAN

Appearance of ZXA10 F460/F460B is shown in Figure 1.

Figure 1 Appearance of ZXA10 F460/F460B

Warning:

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

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Package List

Please check that you have all the following items after you open the package of ZXA10 F460/F460B.

- One set of ZXA10 F460/F460B
- One AC-DC power adapter
- One piece of RJ-45 straight-through cable
- Two pieces of RJ-11 phone line
- ZXA10 F460/F460B Optical Network Terminal User Manual

If any of these items is misplaced, missing or broken, please contact your dealer. If you need to replace any item, please retain the package and all parts in it.

Product Characteristics

Port characteristics

- PON broadband port: conform to PON standard and SC/UPC
- Ethernet port: four 10 Mbps/100 Mbps/1000 Mbps adaptive RJ-45 GE ports, which abide by IEEE802.3 and IEEE802.3u
- VoIP port: two VoIP ports
- WLAN port: conform to IEEE 802.11b/g, built-in antenna
- USB port: two USB ports

Technical Features

The device undertakes data access and VoIP.

- It enables Layer-2 data switching and transfer for data access and realizes IP voice through collaboration with associated network devices on the basis of MGCP and SIP;
- It also provides device, user and service-based multi-level authentication as well as encryption of data channel for safety, QoS and network management concerns. It can satisfy QoS requirements for matching local devices, network, and multi-mode network management for various services.

Product Parameters

- Rated current: 1.3 A
- Rated voltage: DC 12 V
- Operating temperature: -10 ℃~55 ℃
- Operating humidity: 5% ~ 95%

- Dimensions: 290 mm (width) ×44 mm (height) ×180 mm (length)

Product Appearance

Front Panel

Front panel is shown in Figure 2.

Figure 2 Front Panel

The front panel has 10 indicator lamps, as described in Table 2.

Table 2 Meanings of lamps at front panel

Lamp	State	Description
PON state lamp (only for EPON access devices)	Green lamp remain lit	VoIP and OAM links of ONU/T have all been activated.
	Off	ONU/T has not detected or registered VOIP or OAM yet.
	Flash	ONU/T is trying to set up connection.
LOS	Red lamp remain lit	It indicates optical link connection failure.
	Flash	It indicates device failure or flash alternately with RUN lamp during version download.
WLAN indicator	Green lamp remain lit	Wireless ports have been enabled.
	Off	System has not been powered on or wireless ports have been disabled.
	Flash	Data transmission is going on.

Lamp	State	Description
VoIP	Green lamp remain lit	System has registered to soft-switch but no traffic stream is going on.
	Off	System has not been powered on or can't register to soft-switch.
	Flash	Traffic stream is being transmitted.
Power	Green lamp remain lit	System has been powered on.
	Off	System has not been powered on.
LAN1 LAN2 LAN3 LAN4	Green lamp remain lit	Network port has been connected and no data is being transmitted.
	Off	System has not been powered on or no network device has been connected to network port.
	Flash	Data transmission is going on.

Back panel

Back panel is shown in Figure 3.

Figure 3 Back Panel

The back panel provides RJ-45 LAN ports, RJ-11 phone ports, RST reset button, power socket, and USB port.

Ports and buttons on back panel are shown in Table 3.

Table 3 Ports and buttons at back panel

Port/button	Description
LAN1 LAN2 LAN3 LAN4	RJ-45LAN ports, connect to local net through RJ-45 cable
POTS1 POTS2	RJ-11 phone ports, connect to phone through RJ-11 phone line. ***Note:*** *PSTN service is not supported.*
USB	USB HOST port, connect to storage device or printer with USB port, can not connect to PC
UPS	This port is not used
POWER	Slot of power supply, connect to power adapter, DC 12V
WPS	WPS access switch
WLAN	WLAN button, switch on/off WLAN
RESET	Reset button, use a needle to press the button for over 10 seconds when the power is on and the default settings will be restored.

Side panel

There is an SC/UPC single-mode fiber socket at the side panel, through which users can access services from Internet Service Providers (ISP) by PON access (broadband access), as shown in Figure 4.

Figure 4 Side Panel

System Requirements

- You need to contact ISP so that you can access the services in PON mode (broadband access);

- A PC with 10 Mbps/100 Mbps/1000 Mbps Ethernet card;
- Build middle/small enterprise LAN with Ethernet HUB and Ethernet cables if necessary;
- If wireless access is needed, you ought to have an 802.11g/b WLAN card;
- Your computer should at least be able to run any of the following operation systems, Windows 98/ME/2000/NT/XP or Linux. You need to install the driver of the network adapter and the TCP/IP protocol properly and finish network settings correctly;
- Make sure that at least one PC in the LAN has WEB browser, such as Microsoft Internet Explorer 6.0 and Netscape Communicator 4.0 or their higher versions.

2 System Connections

System Application Environment

ZXA10 F460/F460B is an indoor model of the optical network terminal series. It works together with end equipment of PON to realize FTTH applications.

We can also achieve FTTO/B applications by combining multiplex user ports, HUB and Ethernet switch.

System application environment is shown in Figure 5.

Figure 5 System Application Environment

Connection to LAN Port

You can connect LAN ports of ZXA10 F460/F460B to PC or other network devices through cross-over/straight-through Ethernet cable or WLAN RF signal.

Connect to your LAN through Ethernet cable

The four LAN ports can work at the rate of 10 Mbps, 100 Mbps, 1000 Mbps, or the rate of auto-negotiation Ethernet.The transmission mode can be either half-duplex or duplex.

You can connect the LAN ports to PC or other network devices through cross-over or straight-through Ethernet cable.

Note:

Do not plug telephone line into any RJ-45 port as it can cause damage to the device. Be sure to use Ethernet cable with RJ-45 connector that conforms to CE standards.

Connect to your LAN through WLAN

If your PC has WLAN card, it can connect to your LAN through WLAN according to IEEE 802.11b/g. Place the device at the center of the WLAN to get better network coverage.

If you use WLAN to connect your LAN, make sure that the WLAN button at rear side of the device is switched on.

Connection to PON Broadband Port

Plug single-mode fiber with SC/UPC connector into PON broadband port of the device.

Connection to Telephone

Use telephone line with RJ-11 connector to connect telephone to VoIP port of the device.

Connection to Power Adapter

Connect to power supply through power adapter and make sure that the RUN lamp at the front panel is lit.

Adapter parameters

Input AC: 100 V~240 V/50 Hz~60 Hz

Output DC: 12 VDC/2.5 A

Note:

Please use the power adapter provided by ZTE, because unapproved adapters may damage the device.

3 Configuration Preparations

Overview of Configuration Preparations

In most cases, service providers have finished configuration of device and users only need to connect it to their systems before using it. However, in some cases, users may need to configure the device and, if so, please.

- Confirm that your PC has been connected to Ethernet port of the device directly through cross-over/straight-through Ethernet cable;
- Confirm that TCP/IP settings of your PC are correct;
- Prohibit running firewall and other security programs;
- Disable proxy settings of the browser;
- Make sure that you have all necessary information of relevant data. This can be obtained from your service provider.

Installation of TCP/IP

Prerequisite

The TCP/IP protocol has not been installed in your PC before.

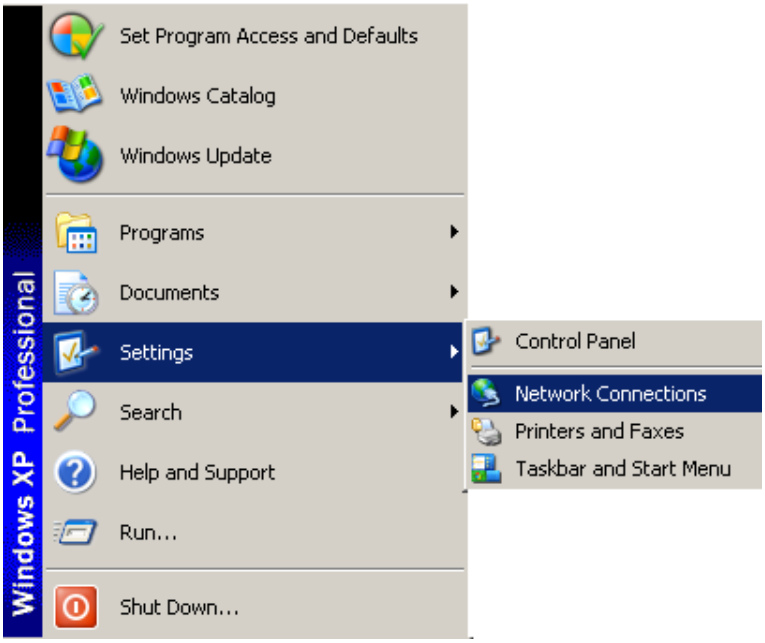
Context

Here we take Windows XP system for example to explain how the installation should be conducted.

Steps

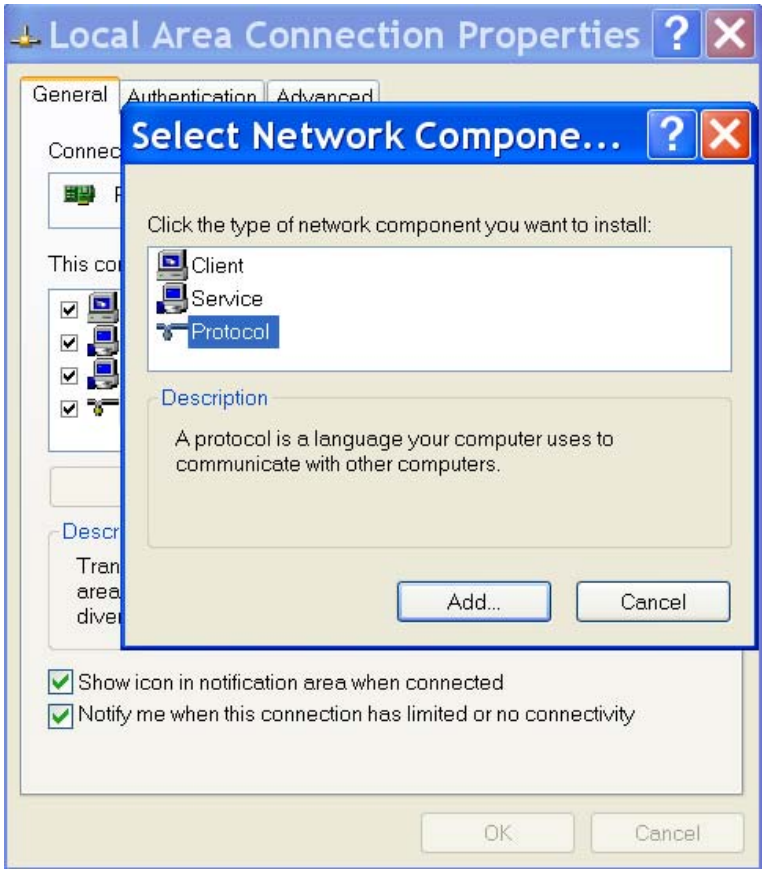
1. Click **Start > Settings > Network Connections**, as shown in Figure 6.

Figure 6 Local Connection 1



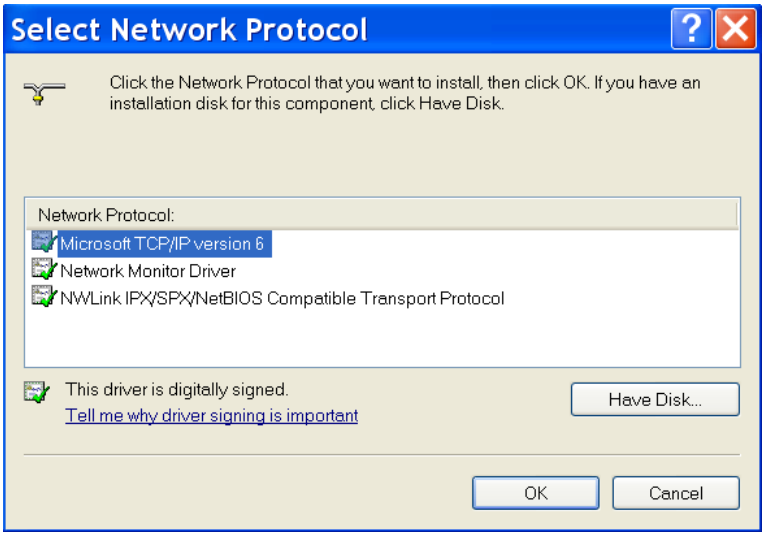
2. Click **Local Connection**. The state of local connection is displayed. Click **Properties**.
3. Select **Internet Protocol** in **Local Area Connection Properties** and click **Install**, as shown in Figure 7.

Figure 7 Local Connection 2



4. Select **Protocol** and click **Add**. Then, select **Microsoft TCP/IP version 6**, as shown in Figure 8.

Figure 8 Internet Protocol



Configuration of TCP/IP

Prerequisite

The TCP/IP protocol has not been installed in your PC before.

Context

Make sure that the device can access Internet properly and your PC and the device in the LAN are in one sub-net segment.

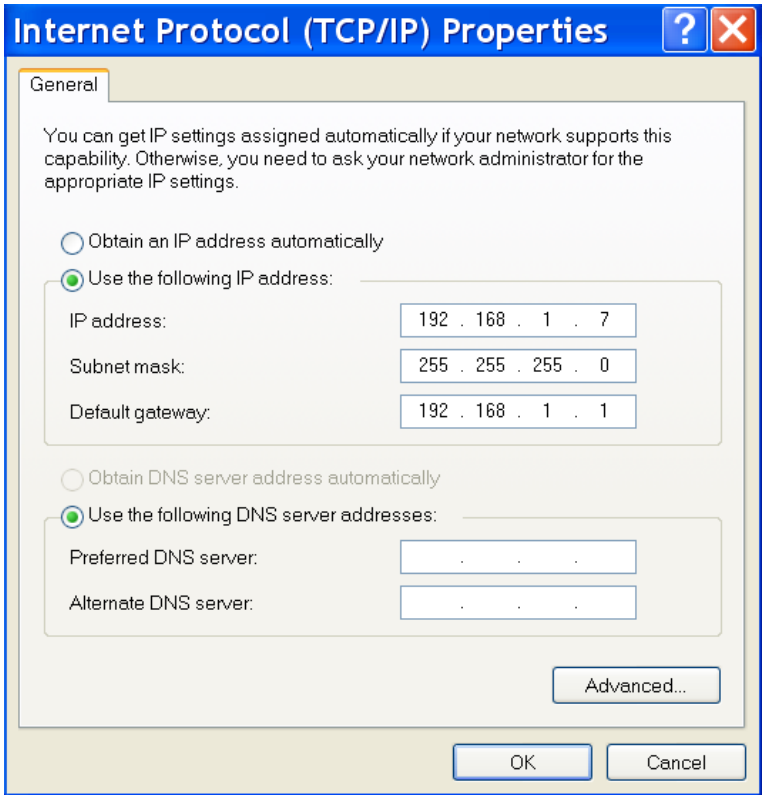
The default settings are:

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

Steps

1. Choose **Internet Protocol (TCP/IP)** in **Local Are Connection Properties**;
2. Click **Properties**. A box of **Internet Protocol (TCP/IP) Properties** pops up, as shown in Figure 9.

Figure 9 Internet Protocol (TCP/IP) Properties



3. Click **Use the following IP address in Internet Protocol (TCP/IP) Properties** and type in an IP address. The IP address shall be in one network segment with 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). For example, IP address 192.168.1.7, subnet mask 255.255.255.0 and default gateway 192.168.1.1.
4. Click **OK** to save your settings.

Note:

The settings can be changed according to your specific network conditions. However, do configure as you are told above if you are accessing the WEB page of the device for the first time.

Configuration Check

Prerequisite

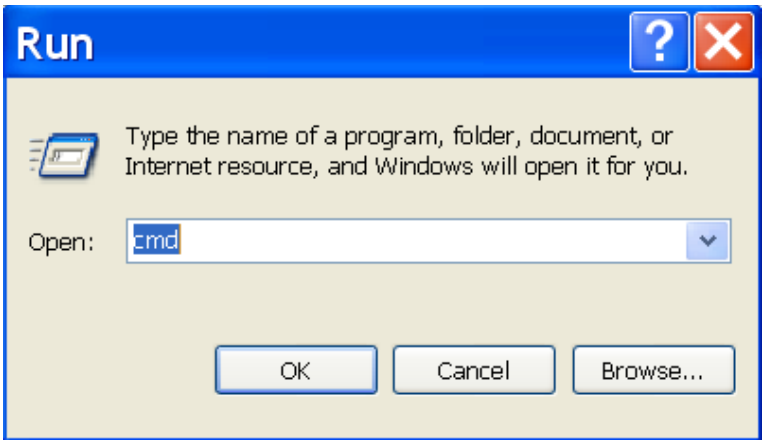
Switch on the power after all preparations are done. The device starts and checks all devices connected to it. Check if network ports have been connected to the device successfully by reading the indicator lamps.

You can check network connection with **Ping**. Here we take **Local Ethernet port check**in Windows XP for example.

Steps

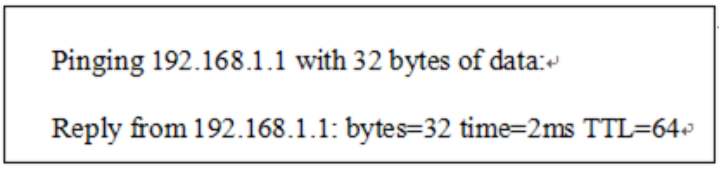
1. Click **Start** and choose **Run**.
2. Type in **cmd** after Open: and press Enter, as shown in Figure 10.

Figure 10 Run



3. Type in **ping 192.168.1.1** and you will see similar information shown in Figure 11.

Figure 11 Ping Information

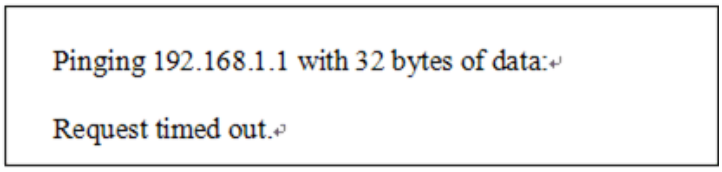


It indicates that the communication between your PC and the device is OK.

If you can Ping the device, you are ready to connect the Internet.

If you see similar information shown in Figure 12.

Figure 12 Ping Trouble Information



It suggests that something is wrong with your installation. Please check the following items:

a) Whether Ethernet cable between the device and your PC has been connected properly;

b) Whether driver of your network adapter has been installed properly;

c) Whether lamps of LAN ports at the device and network adapter of your PC are lit;

d) Whether TCP/IP has been configured correctly at your PC.

   If IP address of the device is 192.168.1.1, IP address of your PC shall fall into the range of 192.168.1.2~192.168.1.254, the subnet mask shall be 255.255.255.0 and the default gateway 192.168.1.1.

Login

Prerequisite

The device has been connected and your PC has been configured properly.

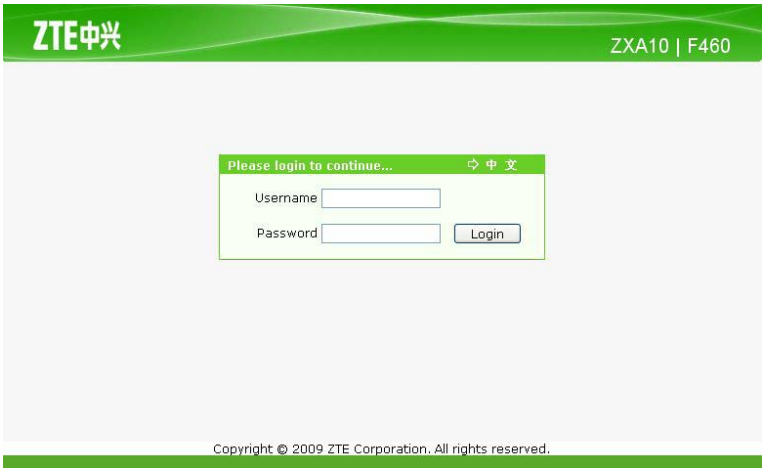
Context

ZXA10 F460/F460B provides WEB-based configuration tool, with which users can carry out configuration and management through WEB browser.

Steps

1. Open IE browser, type in the address of `http://192.168.1.1` (the default IP) and press Enter. The login page is shown in Figure 13.

Figure 13 Login Page



2. Type in username and password (Default username and password are “admin” and “admin”.) Click **Login** to enter the functionality configuration page, as shown in Figure 14.

Figure 14 Functionality Configuration

4 Device Status

Device Information

Click the **Status** tab in the WEB page and the tab shows carrier, model, serial number, hardware version, software version and BOOT loader version of the device, as shown in Figure 15.

Figure 15 Device Information

Network Interface

Network interface information of ZXA10 F460/F460B mainly consists of the following.

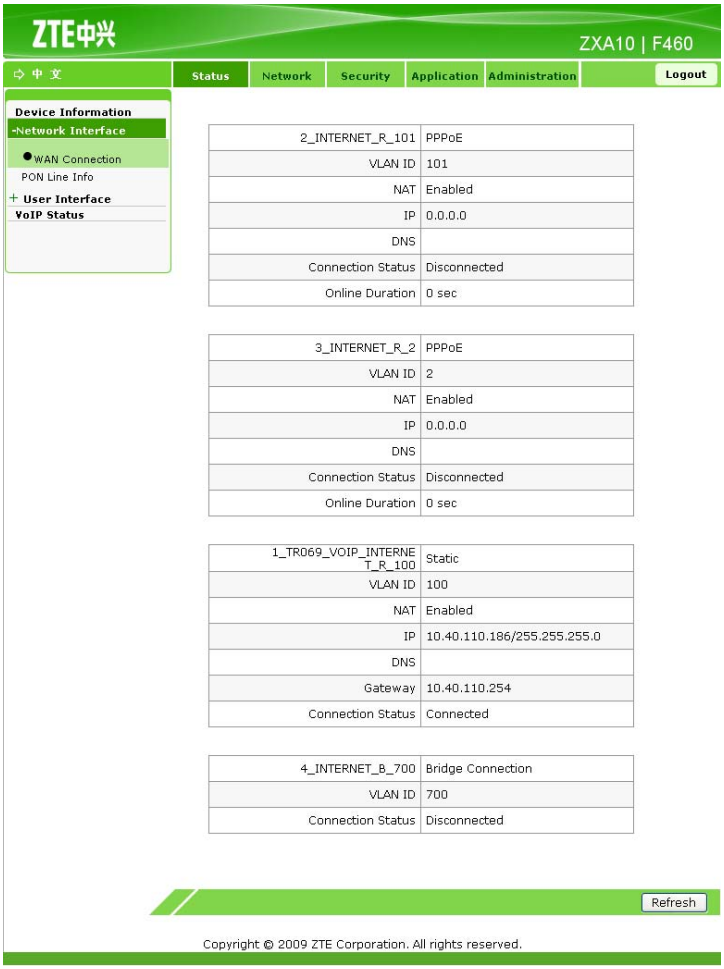
- WAN Connection
- PON Line Information

WAN Connection Information

Click **Status > Network Interface** at WEB page and **WAN connection information** will be shown by default, as you see in Figure 16.The page shows relevant information of WAN connection.

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

Figure 16 WAN Connection Information



PON Link Information

Click **Status > Network Interface > PON Line Information** at WEB page to open the **PON Line Information** page, as shown in Figure 17.The page shows relevant information of PON connection.

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

Figure 17 PON Line Information

User Interface Information

User port information of ZXA10 F460/F460B mainly consists of the following.

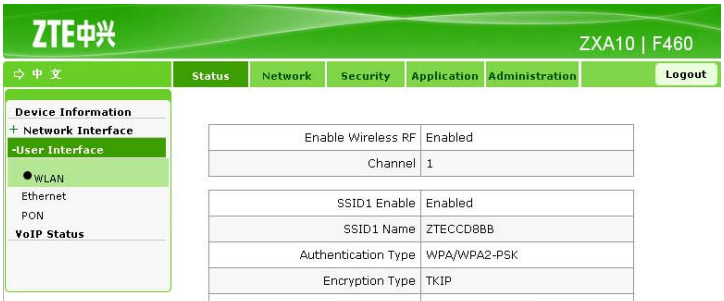
- WLAN Interface Information
- Ethernet Port Information
- PON Information

WLAN Interface Information

Click **Status > User Interface** at WEB page and the **WLAN interface information** page will be opened by default, as shown in Figure 18.The page shows information of wireless switch, packet sending/receiving and authentication.

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

Figure 18 WLAN Interface Information



Enable Wireless RF	Enabled
Channel	1

SSID1 Enable	Enabled
SSID1 Name	ZTECCD8BB
Authentication Type	WPA/WPA2-PSK
Encryption Type	TKIP
MAC Address	00:1e:73:cc:d8:bb
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	7638/320796
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	0

SSID2 Enable	Enabled
SSID2 Name	jhy-F460-2
Authentication Type	Shared Key
Encryption Type	WEP
MAC Address	06:1e:73:cc:d8:bb
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	7886/349137
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	0

SSID3 Enable	Enabled
SSID3 Name	jhy-F460-3
Authentication Type	WPA-PSK
Encryption Type	AES
MAC Address	0a:1e:73:cc:d8:bb
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	7886/349137
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	0

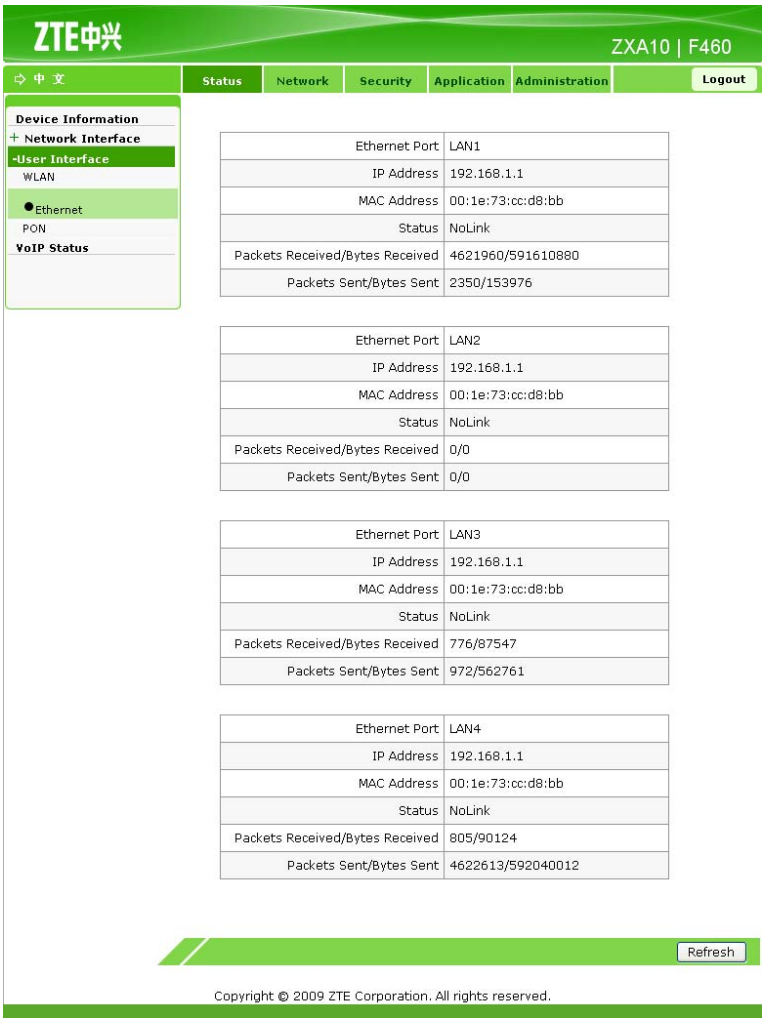
SSID4 Enable	Enabled
SSID4 Name	jhy-F460-4
Authentication Type	Open System
Encryption Type	None
MAC Address	0e:1e:73:cc:d8:bb
Packets Received/Bytes Received	0/0
Packets Sent/Bytes Sent	7887/349179
Error Packets Received	0
Error Packets Sent	0
Discarded Receiving Packets	0
Discarded Sending Packets	0

Ethernet Interface Information

Click **Status > User Interface > Ethernet** at WEB page to open the **Ethernet interface information** page, as shown in Figure 19.The page shows statistical data of packet sending/receiving at Ethernet interfaces.

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

Figure 19 Ethernet Interface Information



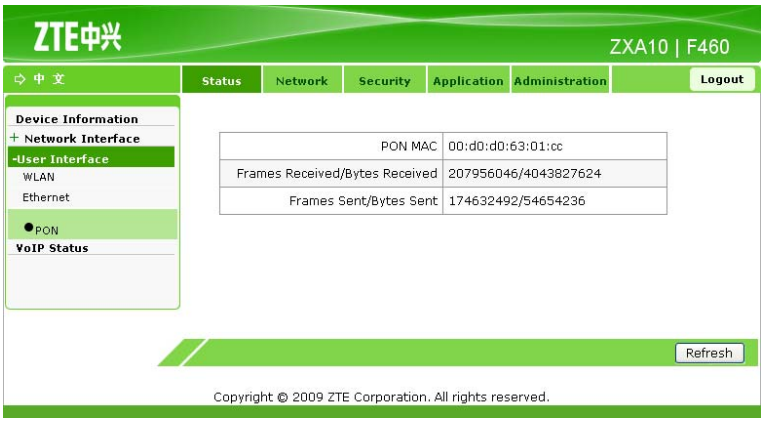
PON Information

Click **Status > User Interface > PON** at WEB page to open the **PON information** page, as shown in Figure 20.

The page shows statistical data of packet sending/receiving at PON broadband ports.

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

Figure 20 PON Information



VoIP Information

Click **Status > VoIP Status** at WEB page to open the **VoIP information** page, as shown inFigure 21.

The page shows registration information of VoIP services.

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

Figure 21 VoIP Information

5 Network Configuration

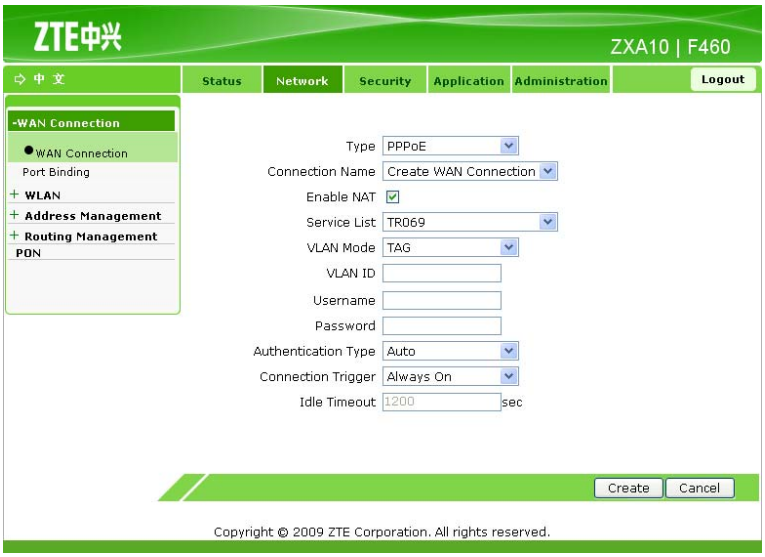
WAN Setting

WAN connection of ZXA10 F460/F460B mainly consists of

- WAN Connection Setting
- Port Binding Setting

Click the **Network** tab at the WEB page and the **WAN connection** page will be opened by default, as shown inFigure 22.

Figure 22 WAN Connection



WAN Connection Setting

Prerequisite

User has logged in WEB page of the device.

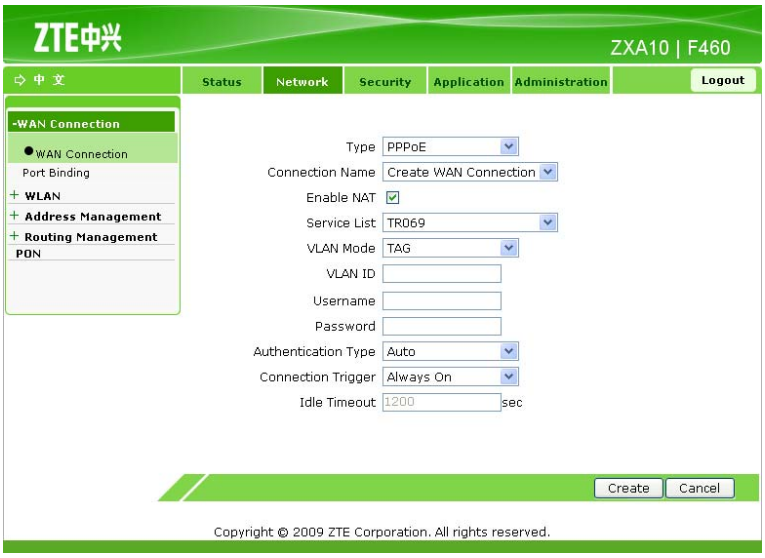
Context

Set WAN connection.

Steps

1. Click **WAN Connection** at the left side of the Network tab to open the **WAN Connection** page, as shown in Figure 23.

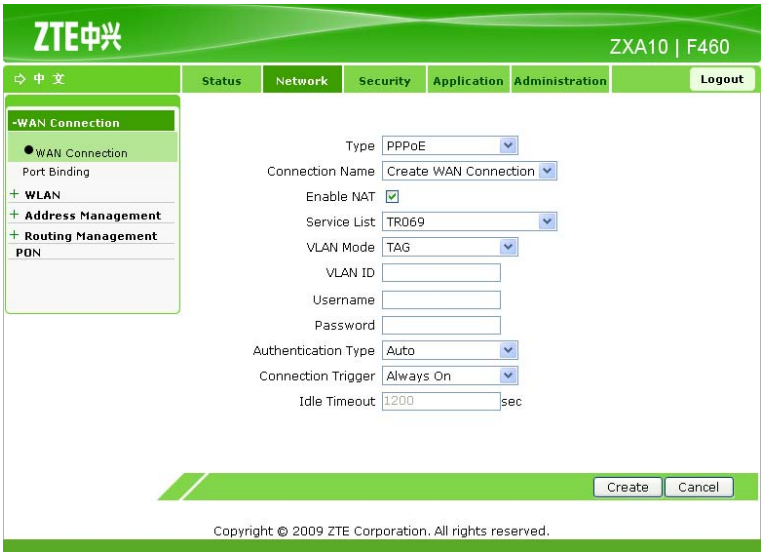
Figure 23 WAN Connection Setting



2. The device provides four link modes, PPPoE, Static, DHCP and bridge, for users to choose from in case of different connection types.
   i. Configuration of the PPPoE mode

      Click **WAN Connection** and choose the **PPPoE** mode, as shown in Figure 24.

Figure 24 Configuration of PPPoE Mode



Parameters of the PPPoE mode are described in Table 4.

Table 4 Parameters of PPPoE Mode

Parameter	Description
Name of connection	Name of new PPPoE connection, generated by system automatically
Enable NAT	Switch of Network Address Translation
Service list	Service modes supported by the device. You can configure various combinations of service modes. – TR069 service mode Remote maintenance and management service mode; – INTERNET service mode Broadband Internet surfing and IPTV service mode; – VOIP service mode Voice service mode
VLAN mode	TAGUNTAGTRANSPAREN
VLAN ID	VLAN ID
Username	Used for authentication upon interconnection with upper-layer devices
Password	Used for authentication upon interconnection with upper-layer devices

Parameter	Description
Authentication type	Same as authentication type of upper-layer devices
Connection trigger	Same dial-up mode as upper-layer devices
Idle timeout	Configure by system automatically

ii. Configuration of the Static mode

Click **WAN Connection** and choose the **Static** mode, as shown in Figure 25.

Figure 25 Configuration of Static Mode

Parameters of the Static mode are described inTable 5.

Table 5 Parameters of Static Mode

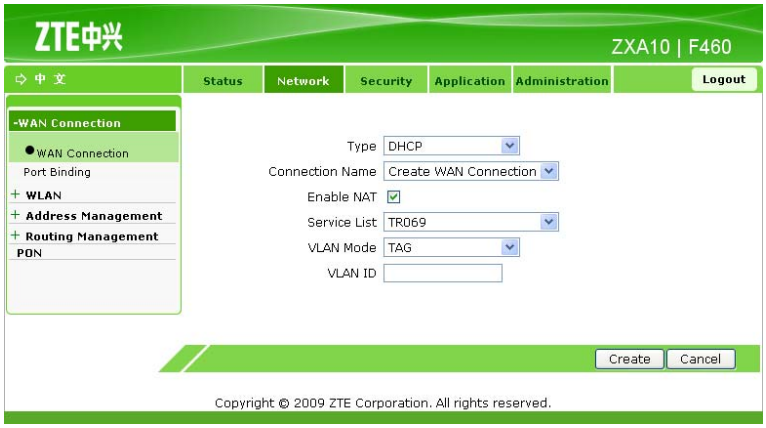
Parameter	Description
Name of connection	Name of new Static connection, generated by system automatically
Enable NAT	Switch of Network Address Translation

Parameter	Description
Service list	Service modes supported by the device. You can configure various combinations of service modes. - TR069 service mode Remote maintenance and management service mode; - INTERNET service mode Broadband Internet surfing and IPTV service mode; - VOIP service mode Voice service mode
VLAN mode	TAGUNTAGTRANSPAREN
VLAN ID	VLAN ID
IP address	IP address of ZXA10 F460/F460B in the network
Subnet mask	Mask of ZXA10 F460/F460B in the network
Gateway	Gateway of ZXA10 F460/F460B in the network
DNS Server1 IP address	DNS1 used by ZXA10 F460/F460B in the network
DNS Server2 IP address	DNS2 used by ZXA10 F460/F460B in the network
DNS Server3 IP address	DNS3 used by ZXA10 F460/F460B in the network

iii. Configuration of the DHCP mode

Click **WAN Connection** and choose the **DHCP** mode, as shown in Figure 26.

Figure 26 Configuration of DHCP Mode



Parameters of the DHCP mode are described in Table 6.

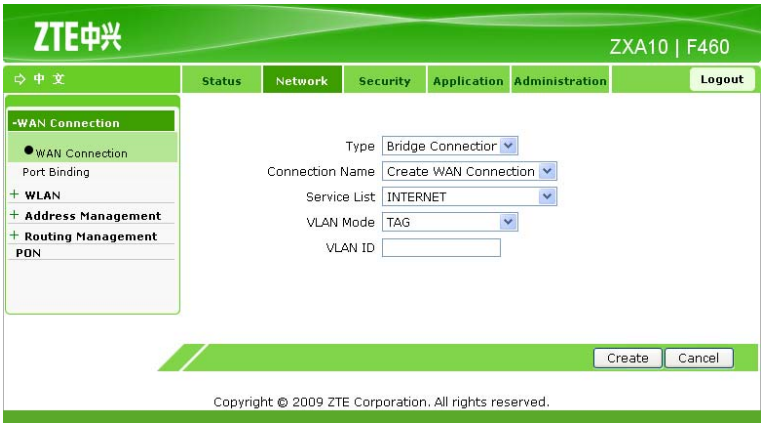
Table 6 Parameters of DHCP Mode

Parameter	Description
Name of connection	Name of new Static connection, generated by system automatically
Enable NAT	Switch of Network Address Translation
Service list	Service modes supported by the device. You can configure various combinations of service modes. - TR069 service mode Remote maintenance and management service mode; - INTERNET service mode Broadband Internet surfing and IPTV service mode; - VOIP service mode Voice service mode
VLAN mode	TAG, UNTAG, TRANSPAREN
VLAN ID	VLAN ID

iv. Configuration of the bridge mode

Open **WAN Connection** and choose the **bridge** mode, as shown in Figure 27.

Figure 27 Configuration of bridge Mode



Parameters of the bridge mode are described inTable 7.

Table 7 Parameters of bridge Mode

Parameter	Description
Connection name	Name of new Static connection, generated by system automatically
Service list	Service modes supported by the device. You can configure various combinations of service modes. - TR069 service mode Remote maintenance and management service mode; - INTERNET service mode Broadband Internet surfing and IPTV service mode; - VOIP service mode Voice service mode
VLAN mode	TAG, UNTAG, TRANSPAREN
VLAN ID	VLAN ID

3. Click **Create** to save the configurations or **Cancel** to undo them.

Port Binding

Prerequisite

User has logged in WEB page of the device.

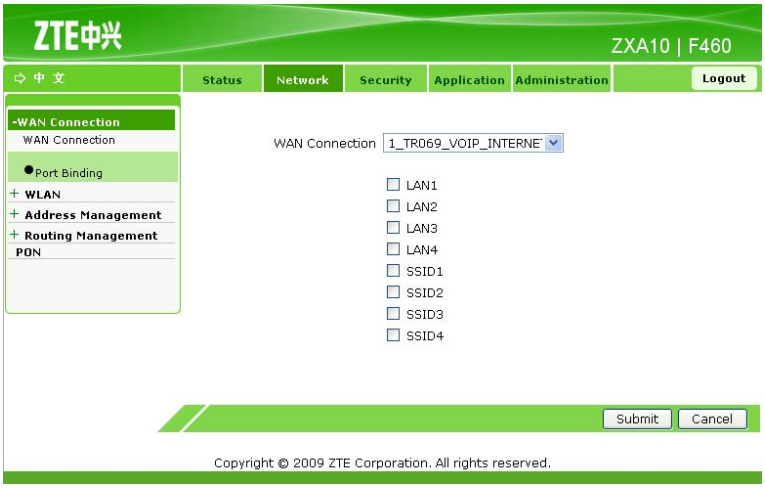
Context

Set WAN connection.

Steps

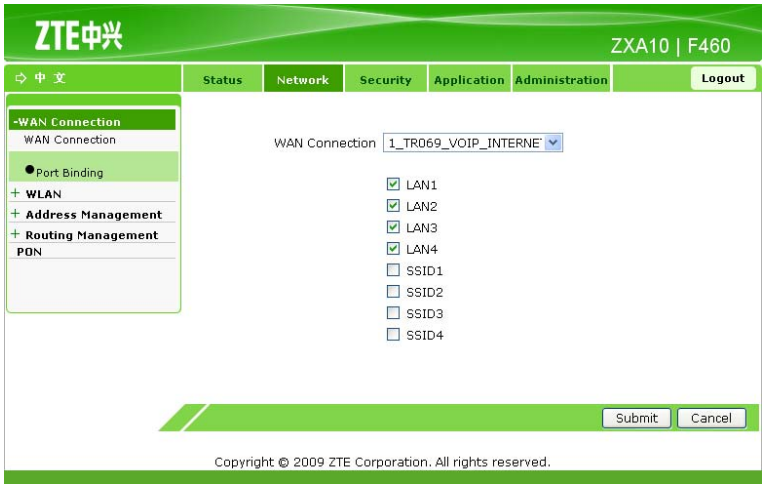
1. Click **WAN Connection > Port Binding** at the WEB page to open the **Port Binding** page, as shown in Figure 28.The page is used to configure port binding and specify the WAN channel through which port connects WAN.

   Figure 28 Port Binding



2. Choose the service type in the **WAN connection** list.
3. Choose the user port you need to bind in **Port Binding** page. LAN ports are user ports and SSID ports are WLAN ports, as shown inFigure 29. Please choose according to your specific conditions.

Figure 29 Port Binding Configuration



4. Click **Submit** to save the configurations or **Cancel** to undo them.

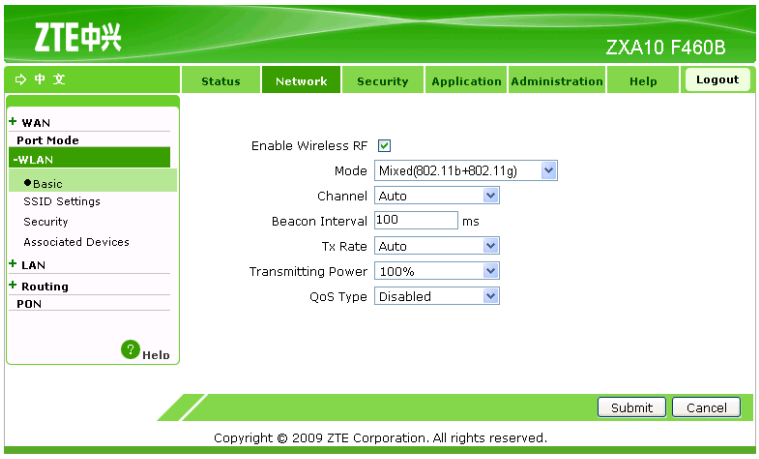
WLAN Setting

WLAN settings of ZXA10 F460/F460B mainly consist of

- Basic Settings
- SSID Settings
- Security Settings
- Associated Device

Click **Network > WLAN** in the WEB page to open the **WLAN** setting page, as shown inFigure 30.

Figure 30 WLAN Settings



Configuration of Basic WLAN Parameters

Prerequisite

User has logged in WEB page of the device.

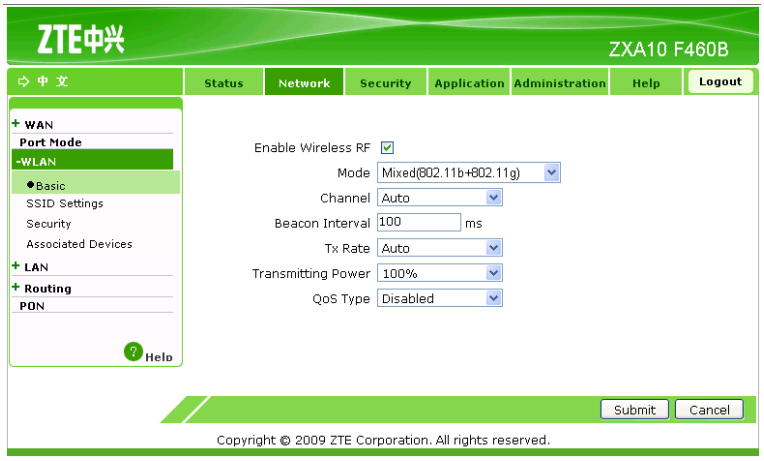
Context

Set basic parameters of WLAN.

Steps

1. Click **Network > WLAN** in the WEB page to open the **Basic Settings** page of WLAN, as shown in Figure 31.

Figure 31 Basic Settings of WLAN



2. Set basic parameters of WLAN as you need. Basic parameters of WLAN are described in Table 8.

Table 8 Basic Parameters of WLAN

Parameter	Description
Enable Wireless RF	Turn on/off RF of WLAN
Mode	Choose wireless communication mode from IEEE802.11b, IEEE802.11g or mix of the two.
Channel	Wireless channel ID. Choose appropriate channel according to country code.
Beacon Interval	Time interval between beacons (unit ms)
Tx Rate	Data transmission rate of the device. Lower rate generates bigger range of wireless communication.
Transmitting Power	Grade of transmitting power
QoS type	QoS PRI type

3. Click **Submit** to save the configurations or **Cancel** to undo them.

Multi-SSID Settings

Prerequisite

User has logged in WEB page of the device.

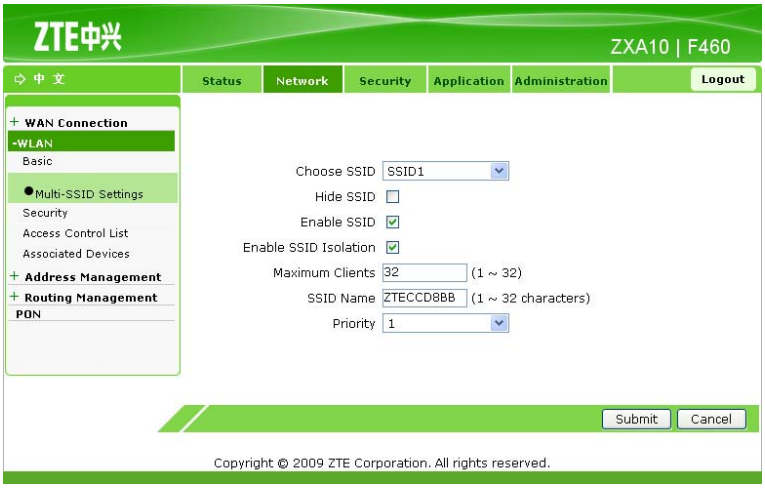
Context

Set SSID parameters of the device

Steps

1. Click **Network > WLA > Multi-SSID Settings** at the WEB page to open the **SSID setting** page, as shown in Figure 32.

Figure 32 SSID Settings



2. Set SSID-related configurations according to need. SSID parameters are described in Table 9.

Table 9 SSID configuration parameters

Parameter	Description
Choose SSID	Choose the SSID to be configured
Hide SSID	Enable or disable SSID broadcast
Enable SSID	Enable the SSID
Enable SSID isolation	Isolate users of the SSID from each other
Maximum clients	MAX number of clients allowed in the SSID

Parameter	Description
SSID name	Service area identifier of wireless network. The longest name can have 32 characters, uppercase/lowercase sensitive. It is used to control access to wireless network. Its value shall match SSIDs of all access points that communicate with it. Otherwise, access will be rejected. (Maximally four wireless network sub-ports can be enabled at one time.)
Priority	Choose priority level of SSID

3. Click **Submit** to save the configurations or **Cancel** to undo them.

WLAN Security Settings

Prerequisite

User has logged in WEB page of the device.

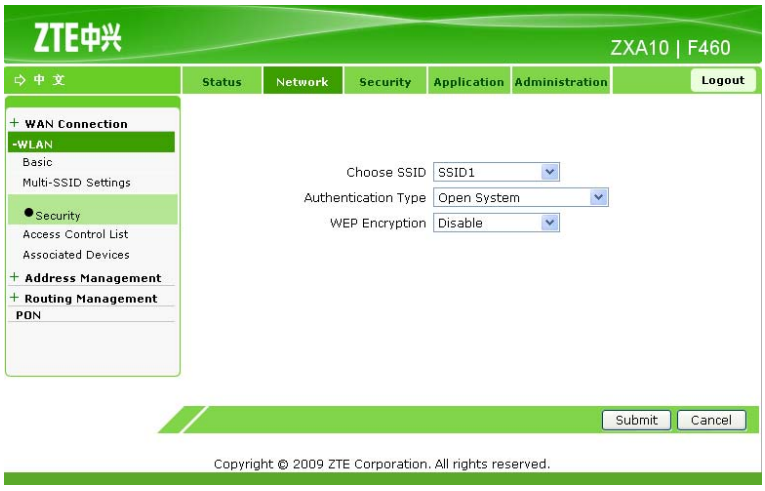
Context

Set WLAN security of the device

Steps

1. Click **Network > WLAN > Security** in the WEB page to open the security setting page, as shown in Figure 33.

Figure 33 Security Setting



SSID supports five authentication modes, namely Open System, SharedKey, WPA-PSK, WPA2-PSK and WPA-PSK/WPA2-PSK.

2. Open the **security setting** page and choose SSID you need to configure in the SSID list.
   i. To open the **Open System** page, as is shown in Figure 34, choose **Open System** in the Authentication Mode list and enable WEP encryption (WEP encryption is disabled by default).Parameters of Open System mode are described in Table 10.

Figure 34 Open System Configuration

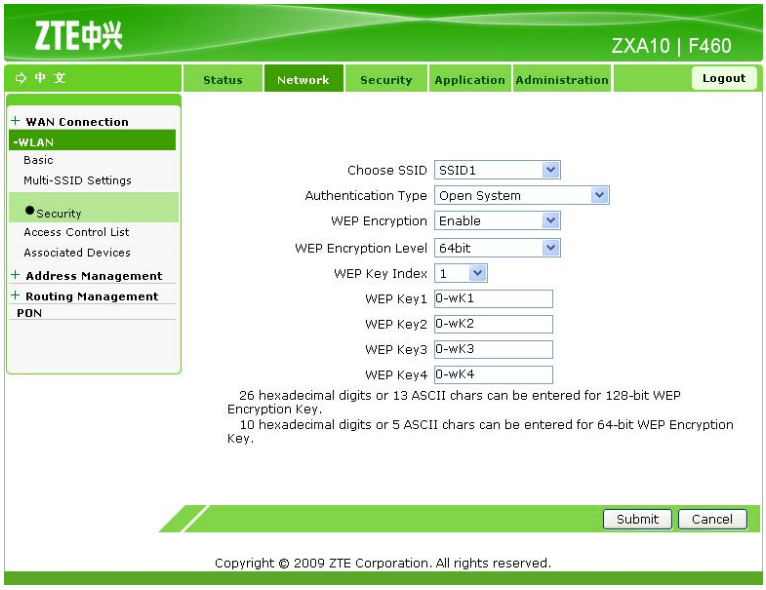


Table 10 Parameters of Open System Mode

Parameter	Description
Choose SSID	Current SSID
Authentication type	Authentication mode of current SSID
WEP encryption	Enable/disable WEP encryption
WEP encryption level	WEP key length, input 13-digit ASCII characters or 26-digit HEX number if it is a 128-bit key or input 5-digit ASCII characters or 10-digit HEX number if it is a 64-bit key. 64 bit or 128 bit. In most cases, 64-bit key can satisfy users' need. Choose 128-bit key if you need higher safety
WEP key index	Value of current key
WEP Key 1	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number.

Parameter	Description
WEP Key 2	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number
WEP Key 3	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number
WEP Key 4	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number

ii. Choose **Shared Key** mode (WEP encryption is enabled by default) in the authentication mode list to open the **SharedKey configuration** page, as shown in Figure 35.Parameters of Shared Key mode are described in Table 11.

Figure 35 Shared Key Configuration

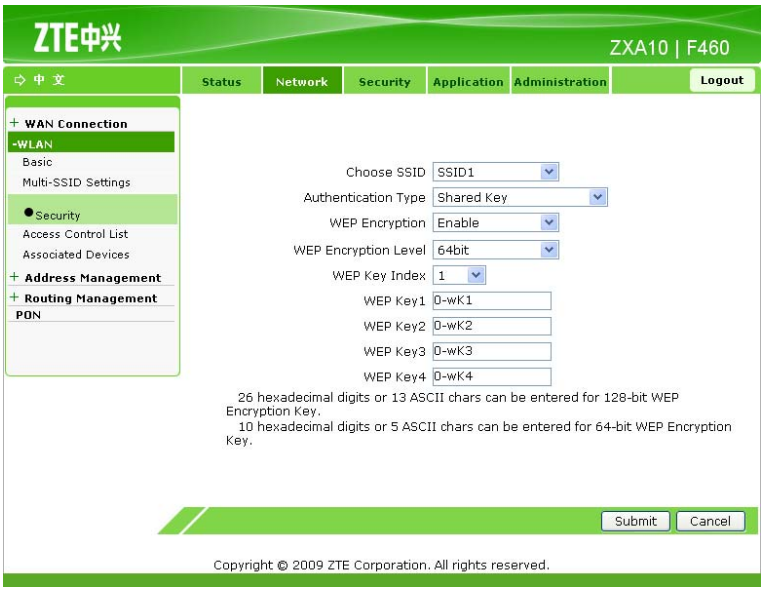


Table 11 Parameters of Shared Key Mode

Parameter	Description
Choose SSID	Current SSID
Authentication type	Authentication mode of current SSID
WEP encryption	Enable WEP encryption

Parameter	Description
WEP encryption level	WEP key length, input 13-digit ASCII characters or 26-digit HEX number if it is a 128-bit key or input 5-digit ASCII characters or 10-digit HEX number if it is a 64-bit key. 64 bit or 128 bit. In most cases, 64-bit key can satisfy users' need. Choose 128-bit key if you need higher safety
WEP key index	Value of current key
WEP Key 1	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number
WEP Key 2	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number
WEP Key 3	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number
WEP Key 4	Value of WEP encryption key. Value range: 5-digit ASCII character or 10-digit HEX number

iii. Choose **WPA-PSK** in the authentication mode list to open the **WPA-PSK** configuration page, as shown in Figure 36.Parameters of WPA-PSK mode are described in Table 12.

Figure 36 WPA-PSK Configuration

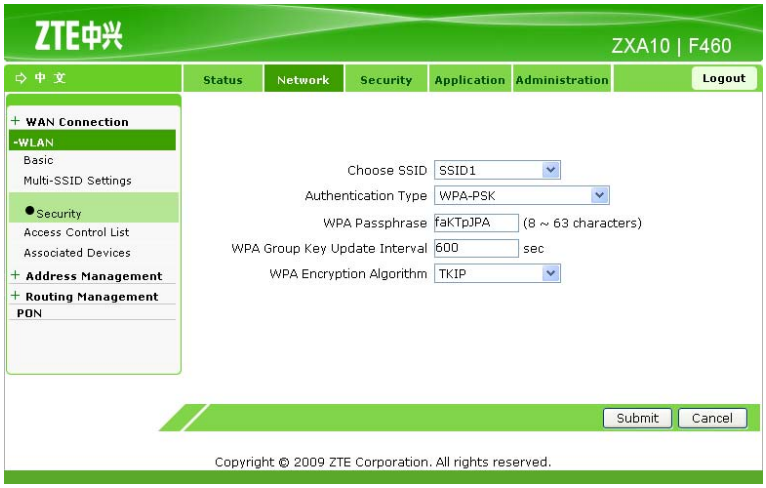


Table 12 Parameters of WPA-PSK Mode

Parameter	Description
Choose SSID	Current SSID
Authentication type	Authentication mode of current SSID
WPA Passphrase	Format of key. Value range: 8 ~ 63 characters
WPA group key update interval	WPA group key update period. Unit: s
WPA encryption algorithm	WPA encryption algorithm: TKIP, AES, TKIP+AES

Note:

Configuration of WPA2-PSK and WPA-PSK/WPA2-PSK is same as WPA-PSK.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

Check Associated Devices

Prerequisite

User has logged in WEB page of the device.

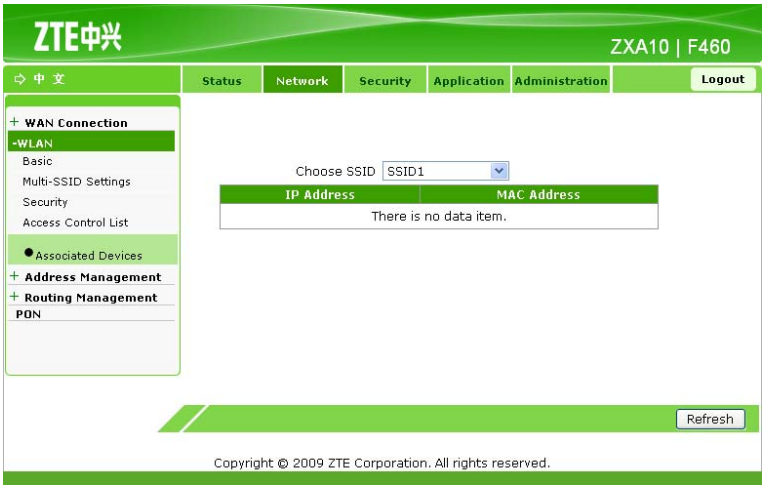
Context

Check information of associated WLAN devices.

Steps

1. Click **Network > WLAN > Associated Devices** in the WEB page to open the **associated device** page, as shown in Figure 37.

Figure 37 Associated Devices



2. Choose the SSID of the device you need to check in the SSID list, click **Refresh** and you will see a list of IP addresses and MAC addresses of the associated device.

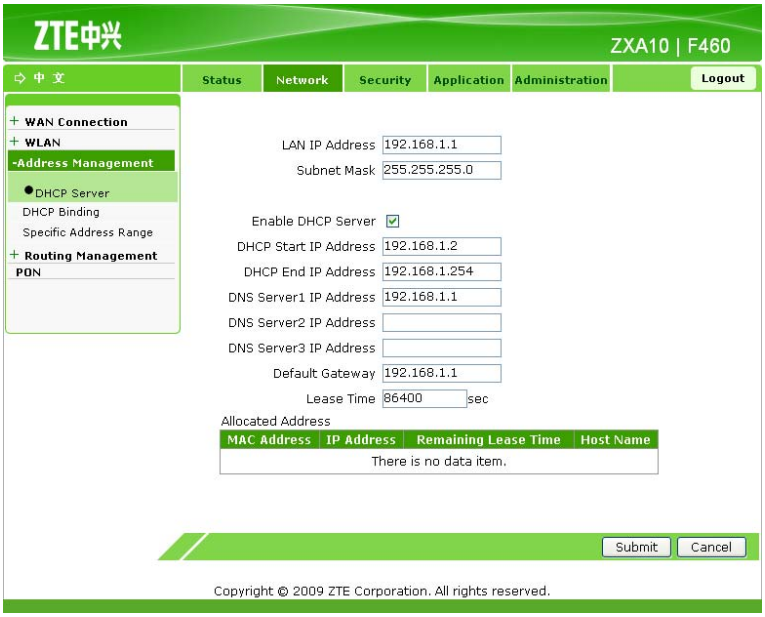
LAN Configuration

Address management configuration of ZXA10 F460/F460B mainly consists of:

- DHCP Server
- DHCP Binding
- Specific Address Range

Click **Network > Address Management** in the WEB page to open the **address management** page, as shown in Figure 38.

Figure 38 Address Management Configuration



DHCP Server

Prerequisite

User has logged in WEB page of the device.

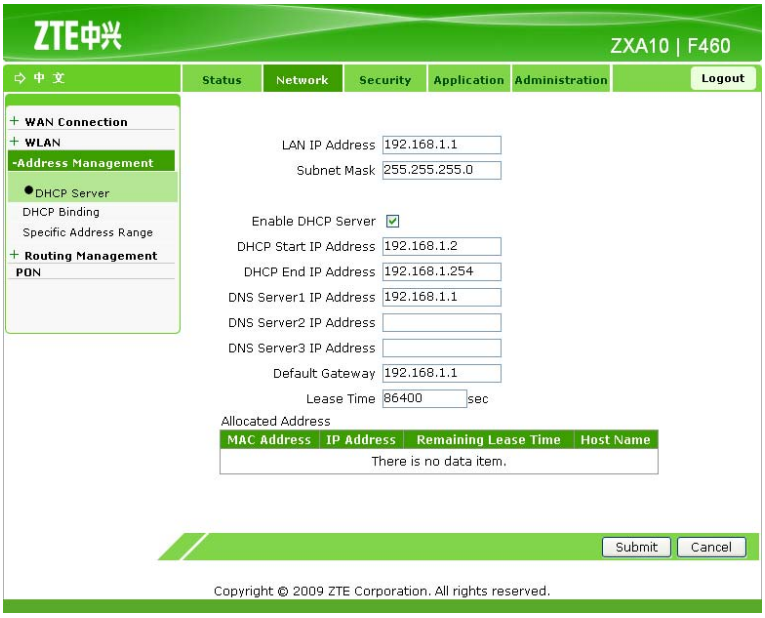
Context

Parameters of DHCP server of the device are configured in DHCP Server.

Steps

1. Click **Network > Address Management** in the WEB page and **DHCP Server** will be opened by default, as shown in Figure 39.

Figure 39 DHCP Server



2. Configure relevant parameters in **DHCP Server**. Users can configure them according to need. Parameters with default values can not be changed. Parameters in the page are described in Table 13.

Table 13 Parameters of Dynamic Address Management

Parameter	**Description**
LAN IP address	IP address of LAN group (port subnet)
Subnet mask	Subnet mask of LAN group
Start DHCP server	Start or shut down DHCP server
DHCP Start IP Address	Initial IP allocated to DHCP server
DHCP End IP Address	End IP allocated to DHCP server
DNS Server1 IP Address	IP address of DNS server
DNS Server2 IP Address	IP address of DNS server
DNS Server3 IP Address	IP address of DNS server
Default Gateway	IP address of default gateway
Lease Time	Time of DHCP server leasing IP address

3. Click **Submit** to save the configurations or **Cancel** to undo them.

DHCP Binding

Prerequisite

User has logged in WEB page of the device.

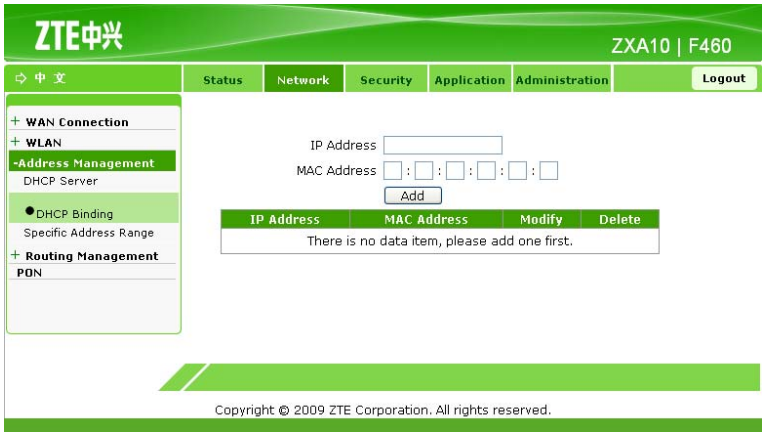
Context

Set bound parameters of DHCP.

Steps

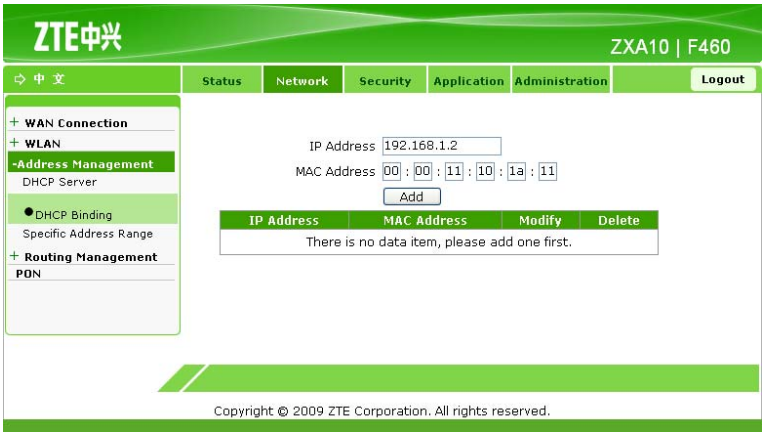
1. Click **Network > Address Management > DHCP Binding** in the WEB page to open the **DHCP Binding** page, as shown in Figure 40.

Figure 40 DHCP Binding



2. Configure MAC address as “00-00-11-10-1a-11” and IP address as “192.168.1.2”, as shown in Figure 41.

Figure 41 DHCP Binding Configuration



Note:

This step means that the IP address that DHCP server allocates to the host corresponding to the MAC address is 192.168.1.2.

Bind the MAC and the IP addresses and create a DHCP binding table that maps MAC and IP addresses of the client. DHCP Server allocates IP addresses according to the binding relation between MAC and IP addresses and the IP addresses shall never expire.

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

Routing Management

Routing management of ZXA10 F460/F460B mainly discusses:

- Default gateway
- Static routing

Click **Network > Routing Management** in the WEB page to open the **routing management** page, as shown in Figure 42.

Figure 42 Routing Management

Default Gateway Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set default gateway of the device.

Steps

1. Click **Network > Routing Management** in the WEB page and the Default Gateway page will be opened, as shown in Figure 43.

Figure 43 Default Gateway

2. Choose connection interface in **WAN Connection**.

   Note:

   The interface should not be used before it is configured in WAN Connection.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

Static Routing Settings

Prerequisite

User has logged in WEB page of the device.

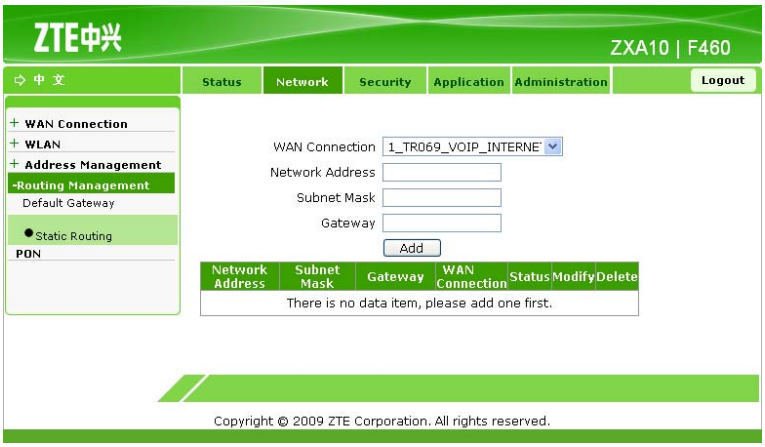
Context

Set static routing parameters of the device.

Steps

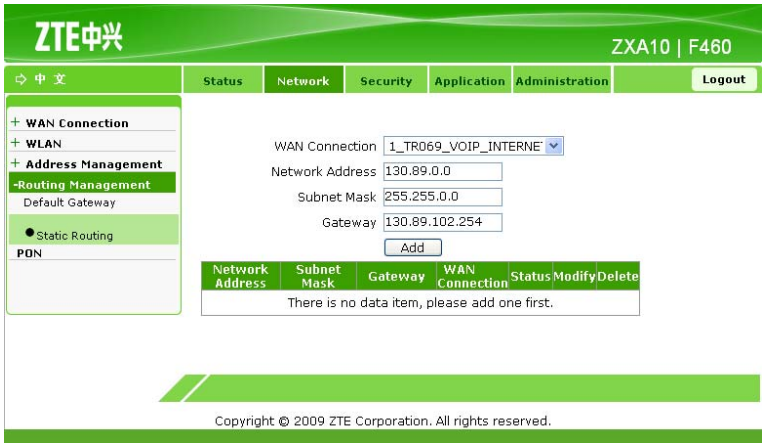
1. Click **Network > Routing Management > Static Routing** in the WEB page to open the **static routing** page, as shown in Figure 44.

   Figure 44 Static Routing Settings



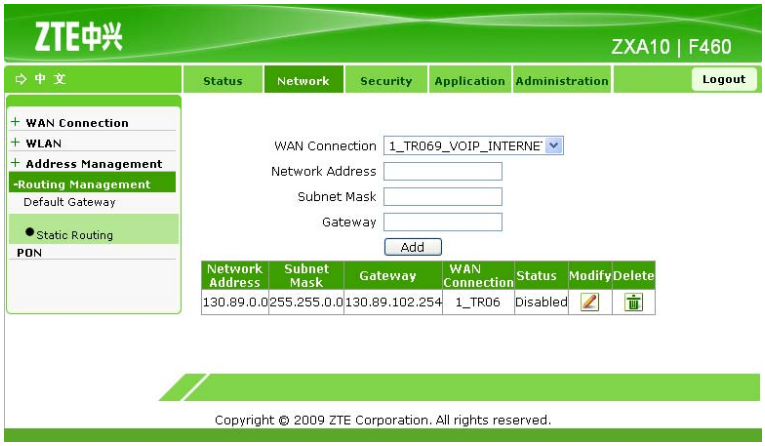
2. Choose the interface to be configured in WAN Connection.
3. Type in data in **Network Address**, **Subnet Mask** and **Gateway**, as shown in Figure 45.

Figure 45 Static Routing Settings



4. Click **Add** to finish the configuration, as shown in Figure 46.Click **Modify** to modify the configuration or **Delete** to delete the configuration.

Figure 46 Finishing Page of Static Routing Configuration



PON Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set PON broadband port parameters of the device.

Steps

1. Click **Network > PON** in the WEB page to open the page and start authentication of ONU (Optical Network Unit) ID, as shown in Figure 47.

   Figure 47 PON Settings

   Note:

   If OLT is chosen as ID authentication, you need to type in correct ONU ID at NM platform of OLT so that ONU can pass authentication and start service communication.

2. Type in data in **ONU ID** and **Password**.
   - ONU ID is “ztepon” by default;
   - Password is “ztepon” by default.
3. Click **Submit** to save the configurations or **Cancel** to undo them.

6 Security Configuration

Firewall Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set firewall parameters of the device.

Steps

1. Click **Security > Firewall** in the WEB page to open the **firewall** configuration page, as shown in Figure 48.

   Figure 48 Firewall Configuration

2. Enable anti-hacking protection.
3. Choose a firewall level.
4. Click **Submit** to save the configurations or **Cancel** to undo them.

IP Filter Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set IP filter parameters of the device.

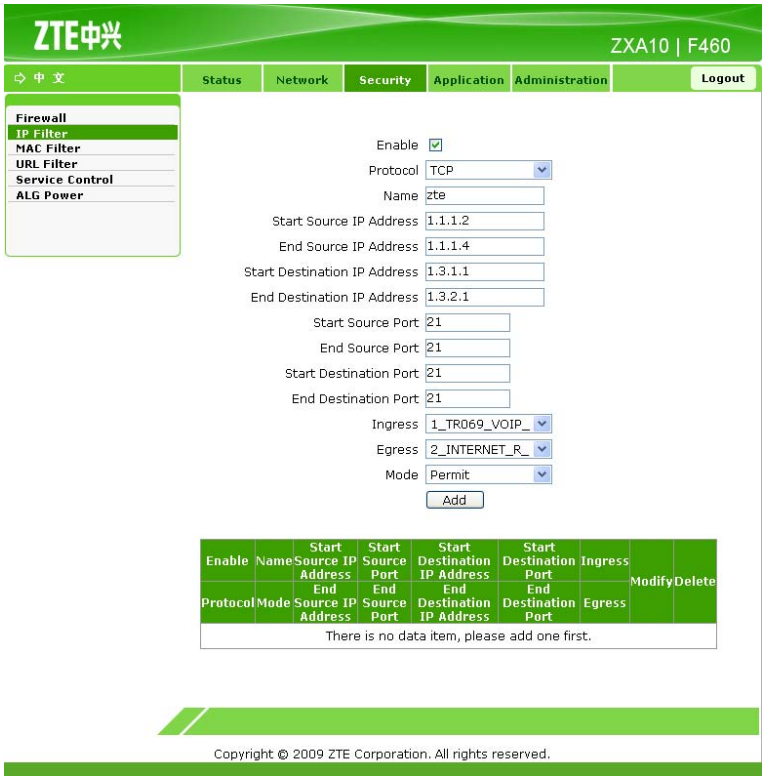
Steps

1. Click **Security > IP Filter** in the WEB page to open the **IP filter** configuration page, as shown in Figure 49.

Figure 49 IP Filter Configuration

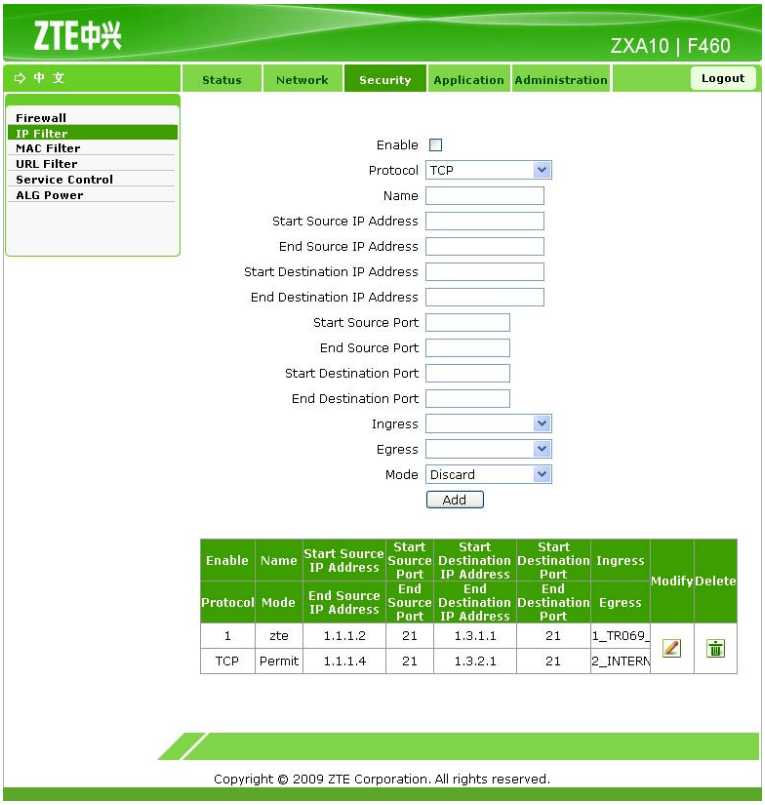
2. Configure filter parameters in the **IP Filter** page, as shown in Figure 50.

Figure 50 Filter Configuration



3. Click **Add** to finish the configurations, as shown in Figure 51.You can click **Modify** to modify a parameter or **Delete** to delete it.

Figure 51 Finishing Page of IP Filter Configuration



MAC Filter Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set MAC filter parameters of the device.

Steps

1. Click **Security > MAC Filter** in the WEB page to open the **MAC filter** configuration page, as shown in Figure 52.

Figure 52 MAC Filter Configuration

2. Configure **MAC filter** parameters in page as shown in Figure 53.

Figure 53 MAC Filter Configuration

3. Click **Add** to finish the configurations, as shown in Figure 54.You can click **Modify** to modify a parameter or **Delete** to delete it.

Figure 54 Finishing Page of MAC Filter Configuration

URL Filter Settings

Prerequisite

User has logged in WEB page of the device.

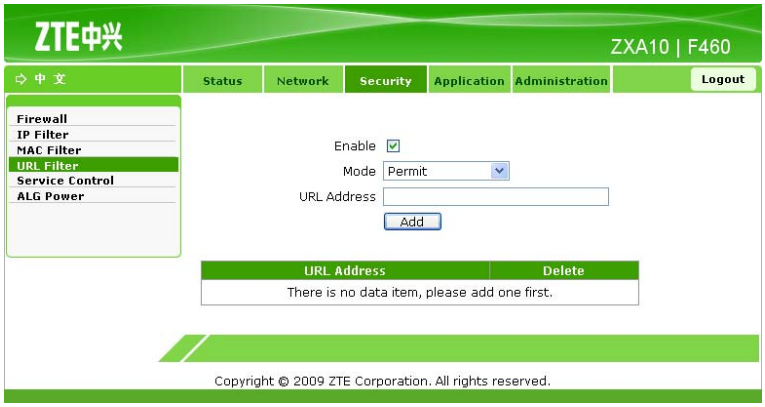
Context

Set URL filter parameters of the device.

Steps

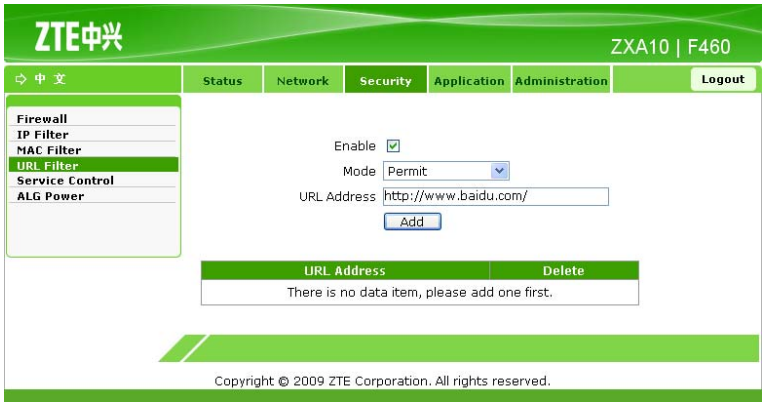
1. Click **Security > URL Filter** in the WEB page to open the **URL filter** configuration page, as shown in Figure 55.

Figure 55 URL Filter



2. Configure parameters in **URL filter** page as shown in Figure 56.

Figure 56 URL Filter Configuration



3. Click **Add** to finish the configurations, as shown in Figure 57.You can click **Delete** to delete a parameter.

Figure 57 Finishing Page of URL Filter Configuration

Access Control Settings

Prerequisite

User has logged in WEB page of the device.

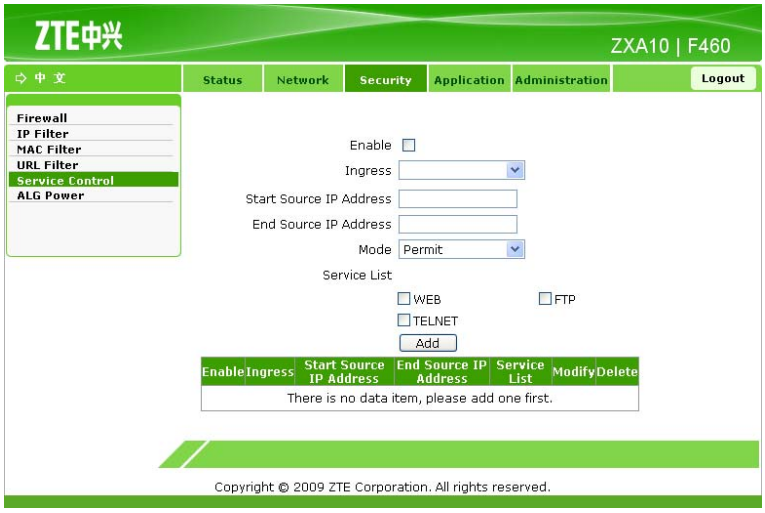
Context

Set access control parameters of the device.

Steps

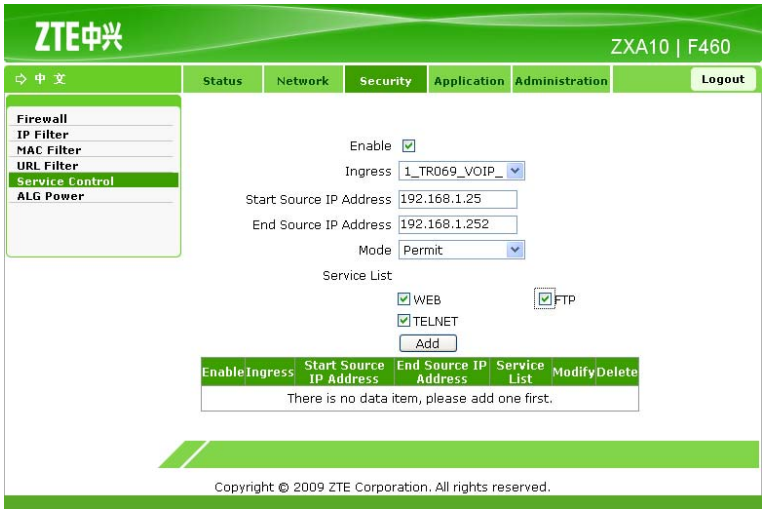
1. Click **Security > Service Control** in the WEB page to open the **service control** page, as shown in Figure 58.

Figure 58 Service Control



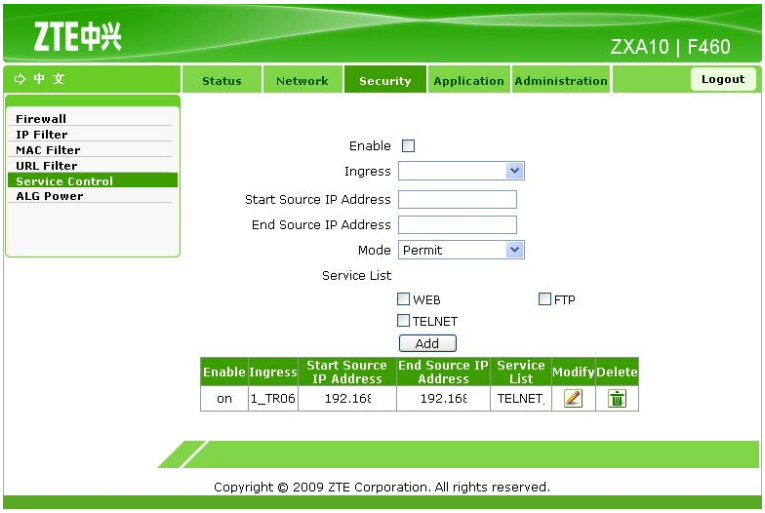
2. Configure filter parameters in **Service Control**, as shown in Figure 59.

Figure 59 Service Control Configuration



3. Click **Add** to finish the configuration, as shown in Figure 60.You can click **Modify** to modify a parameter or **Delete** to delete it.

Figure 60 Finishing Page of Service Control Configuration



ALG Switch Settings

Prerequisite

User has logged in WEB page of the device.

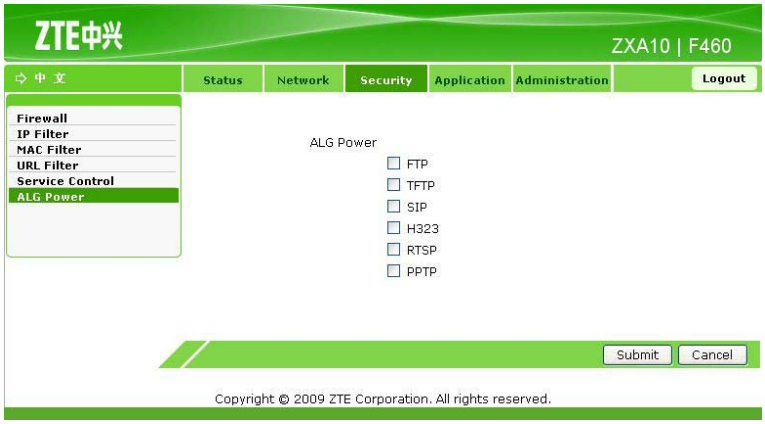
Context

Enable ALG switch of the device.

Steps

1. Click **Security > ALG Power** in the WEB page to open the **ALG switch** page, as shown in Figure 61.

Figure 61 ALG Switch



2. Choose service types for which ALG power needs to be enabled in the **ALG power** page, as shown in Figure 62.

Figure 62 ALG Switch Configuration

3. Click **Submit** to save the configurations or **Cancel** to undo them.

7 Application Configurations

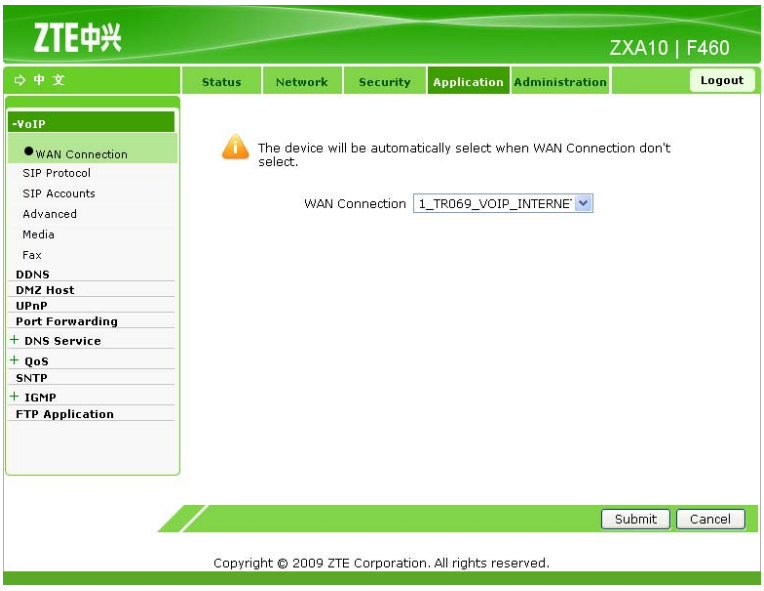
VoIP Settings

VoIP settings of ZXA10 F460/F460B mainly consist of the following:

- WAN Connection
- SIP Protocol
- SIP Accounts
- Advanced Configuration
- Media Settings
- FAX Settings

Click **Application > VoIP** in the WEB page to open the **VoIP setting** page, as shown in Figure 63.

Figure 63 VoIP Configuration



WAN Connection

Prerequisite

User has logged in WEB page of the device.

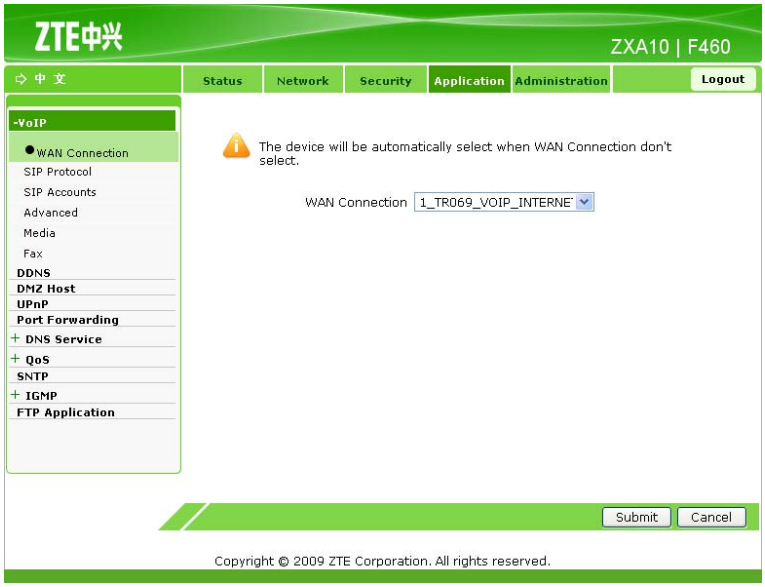
Context

Set WAN connection used for VoIP services.

Steps

1. Click **Application > VoIP** in the WEB page and the **WAN connection** page will be opened by default, as shown in Figure 64.

Figure 64 WAN Connection



2. Choose type of **WAN connection interface** in the WAN connection list.
3. Click **Submit** to save the configurations or **Cancel** to undo them.

SIP Protocol Configuration

Prerequisite

User has logged in WEB page of the device.

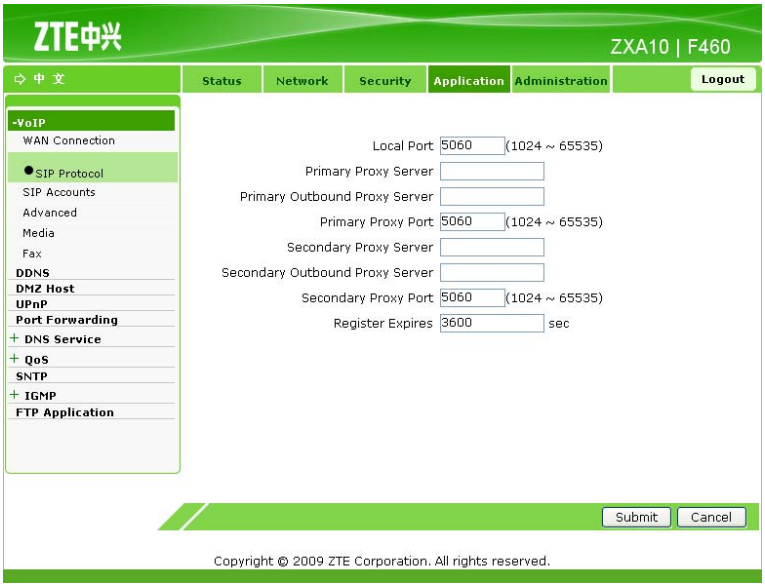
Context

Set SIP protocol parameters of the device.

Steps

1. Click **Application > VoIP > SIP Protocol** in the WEB page to open the **SIP configuration** page, as shown in Figure 65.

   Figure 65 SIP Protocol



2. Configure parameters of the SIP protocol in the page, as shown in Figure 66,Parameters of the SIP protocol are described in Table 14.

Figure 66 SIP Protocol Configuration

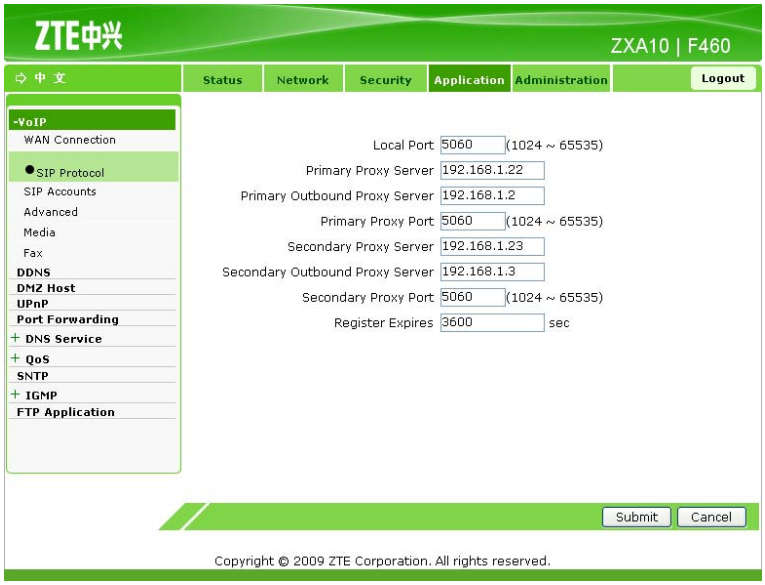


Table 14 SIP parameters

Parameter	Description
Local port	Local port used by VoIP
Primary proxy server	IP address of primary proxy server
Primary outbound proxy server	IP address of primary outbound proxy server
Primary proxy port	Port of primary proxy server
Secondary proxy server	IP address of secondary proxy server
Secondary outbound proxy server	IP address of secondary outbound proxy server
Secondary proxy port	Port of secondary proxy server
Register expires	Expiry term of register (unit: second)

3. Click **Submit** to save the configurations or **Cancel** to undo them.

SIP Account Information

Prerequisite

User has logged in WEB page of the device.

Context

Set SIP account parameters of the device.

Steps

1. Click **Application > VoIP > SIP Accounts** in the WEB page to open the **SIP account** page, as shown in Figure 67.

   Figure 67 SIP Account Information

2. Click **Modify** in the page to modify any parameters of SIP account, as shown in Figure 68. SIP account parameters are described in Table 15.

Figure 68 SIP Account Configuration

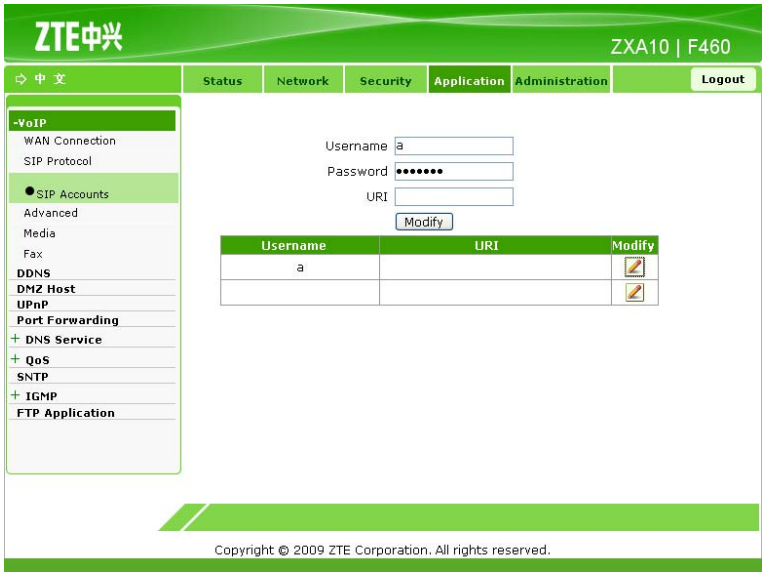


Table 15 Parameters of SIP Account

Parameter	Description
Username	Username for SIP authentication
Password	Registration password of SIP user
URI	URI can be seen as number of user's SIP call

3. Click **Modify** to finish the configuration.

Advanced Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set advanced parameters of the device.

Steps

1. Click **Application > VoIP > Advanced** in the WEB page to open the **advanced setting** page, as shown in Figure 69.

Figure 69 Advanced Settings

2. Configure advanced parameters in the page. Advanced parameters are described in Table 16.

Table 16 Advanced Parameters

Parameter	Description
Echo cancellation	Enable or disable echo suppression
DTMF	DTMF mode selection, support two modes, RFC2833 and transparent
Jitter buffer	Jitter buffer, support two modes, fixed and adaptive
MIN value	Minimum jitter amplitude, unit: ms
MAX value	Maximum jitter amplitude, unit: ms

3. Click **Submit** to save the configurations or **Cancel** to undo them.

Media Settings

Prerequisite

User has logged in WEB page of the device.

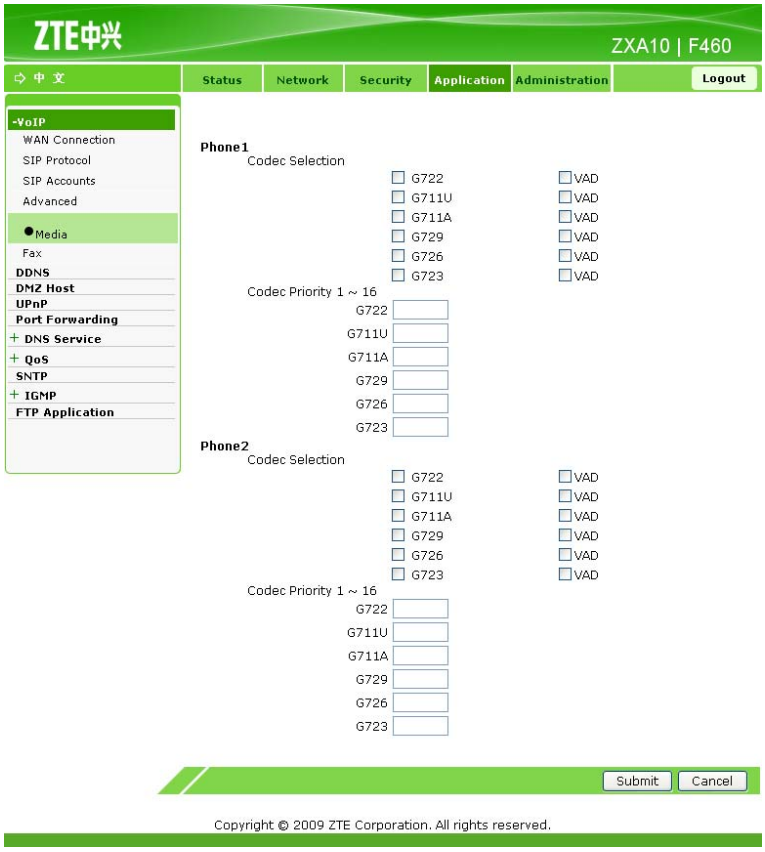
Context

Set media parameters of the device.

Steps

1. Click **Application > VoIP > Media** in the WEB page to open the **media** page, as shown in Figure 70.

Figure 70 Media Settings



2. Configure parameters in the **media** page, as shown in Figure 71. Parameters of media settings are described in Table 17.

Figure 71 Media Setting

Table 17 Media Setting Parameters

Parameter	Description
Codec selection	Codec mode supported by the media
Codec priority	Codec priority, the smaller number, the higher priority
VAD	Voice Activity Detect. It detects if the environment is mute (quiet) and enables CNG to create comforting sound if the environment is mute

3. Click **Submit** to save the configurations or **Cancel** to undo them.

FAX Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set FAX parameters of the device.

Steps

1. Click **Application > VoIP > FAX** in the WEB page to open the **FAX** page, as shown in Figure 72.

Figure 72 FAX Setting

2. Put a tick after Enable **T38** to enable the T.38 fax mode.

   Note:

   T30 mode will be enabled if you don't select Enable T38.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

DDNS Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set DDNS parameters of the device.

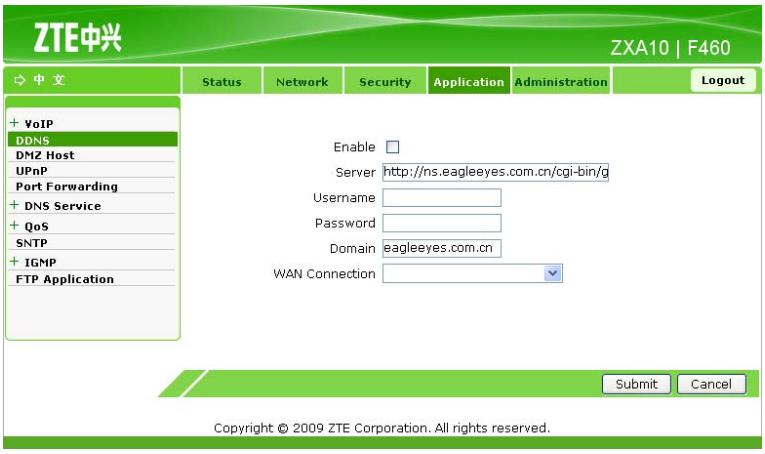
Note:

DDNS is the acronym of Dynamic Domain Name System. By using it, host with dynamic IP address can also provide domain name service. For example, assuming a host gets IP address through xDSL dial-up or DHCP server and provides domain name service to outside, users' access to the domain name will not be affected and users will not perceive change of address of the host if DDNS is enabled.

Steps

1. Click **Application > DDNS** in the WEB page to open the DDNS page, as shown in Figure 73.

Figure 73 DDNS Page



2. Configure DDNS parameters in the page shown in Figure 74.Parameters of DDNS are described in Table 18.

Figure 74 DDNS Configuration

Table 18 DDNS Parameters

Parameter	Description
Enable DDNS	Whether DDNS should be enabled or not
Server	Address of server. If HTTP of GNUDIP is used, the address is a URL,http://ns.eagleeyes.com.cn/cgi-bin/gdipupdt.cgi by default
Username	Username of DDNS server
Password	Password of DDNS server
Domain	Domain name of user, valid only when GNUDIP is used
WAN Connection	WAN connection interface

3. Click **Submit** to save the configurations or **Cancel** to undo them.

DMZ Settings

Prerequisite

User has logged in WEB page of the device.

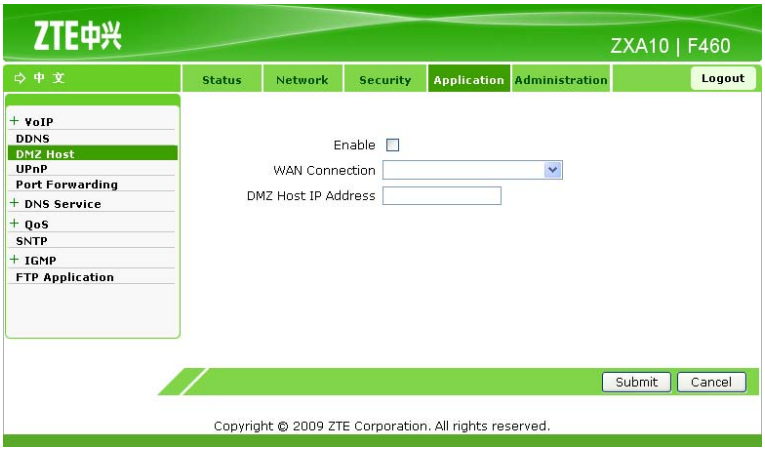
Context

Set DMZ parameters of the device.

Steps

1. Click **Application > DMZ Host** in the WEB page to open the **DMZ** page, as shown in Figure 75.

Figure 75 DMZ Page



2. Configure DMZ parameters in the page as shown in Figure 76.DMZ parameters are described in Table 19.

Figure 76 DMZ Configuration

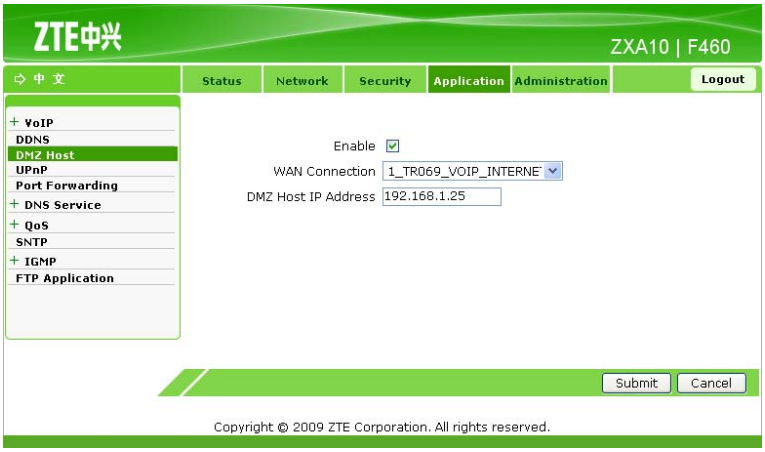


Table 19 DMZ Parameters

Parameter	Description
Enable	Enable DMZ host
WAN Connection	WAN connection interface
DMZ Host IP Address	IP address of DMZ host

Note:

After DMZ all-port mapping is enabled, all ports are opened by default and host at LAN side provides services to outside through DNAT.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

UPnP Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set UPnP parameters of the device.

UPnP enables auto-detection for zero-configuration, invisible network connection and type of vendor's devices. After the function is configured, the device can dynamically enter a network, get its IP address, report its functions and learn functions of other devices.

Steps

1. Click **Application > UPnP** in the WEB page to open the **UPnP** page, as shown in Figure 77.

Figure 77 UPnP Page

2. Configure UPnP parameters in the page as shown in Figure 78.UPnP parameters are described in Table 20.

Figure 78 UPnP Configuration

Table 20 UPnP Parameters

Parameter	Description
Enable UPnP	Enable UPnP
WAN Connection	WAN connection interface

3. Click **Submit** to save the configurations or **Cancel** to undo them.

Virtual Host Settings

Prerequisite

User has logged in WEB page of the device.

Context

Set port mapping parameters of the device.

Steps

1. Click **Application > Port Forwarding** in the WEB page to open the page, as shown in Figure 79.

Figure 79 Virtual Host

2. Configure virtual host parameters as shown in Figure 80.Parameters of virtual host are described in Table 21.

Figure 80 Virtual Host Configuration

Table 21 Parameters of Virtual Host

Parameter	Description
Enable	Enable virtual host
Name	Name of virtual host
Protocol	Choose protocol, including TCP, UDP and mix of the two
WAN host start IP address	Starting IP of WAN host
WAN host end IP address	Ending IP of WAN host
WAN connection	Established WAN connection
WAN start port	Destination start port at WAN
WAN end port	Destination end port at WAN
LAN host IP address	IP address of LAN host

Parameter	Description
LAN host start port	Start port of host at LAN
LAN host end port	End port of host at LAN

Note:

Configure a redirecting policy of port access that allows IP addresses at WAN to be the source and IP address at LAN to be the destination. It is applicable mainly when WAN, as the client, accesses the server at LAN.

3. Click **Add** to finish the configuration, as shown in Figure 81.You can click **Modify** to modify a virtual host parameter or click **Delete** to delete it.

Figure 81 Finishing Page of Virtual Host Configuration

Device Naming

DNS Service

Prerequisite

User has logged in WEB page of the device.

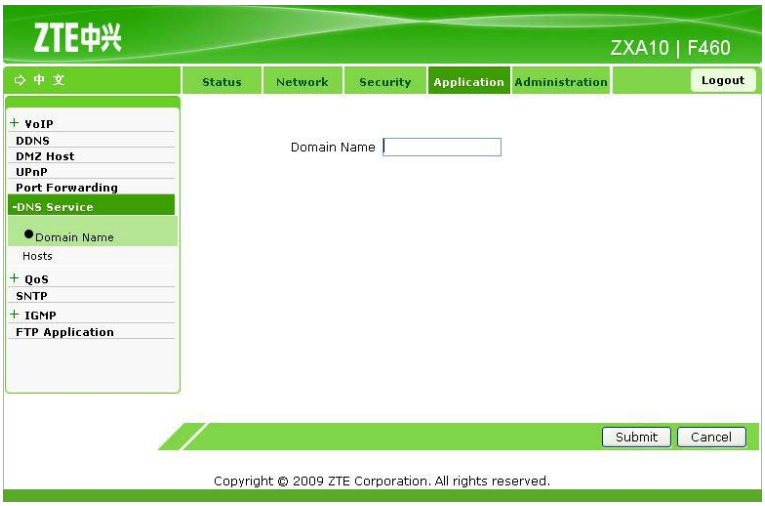
Context

Set domain name parameters of the device.

Steps

1. Click **Application > DNS Service** in the WEB page to open the page, as shown in Figure 82.

Figure 82 DNS Service



2. Type in domain name.
3. Click **Submit** to save the configurations or **Cancel** to undo them.

Host Name Setting

Prerequisite

User has logged in WEB page of the device.

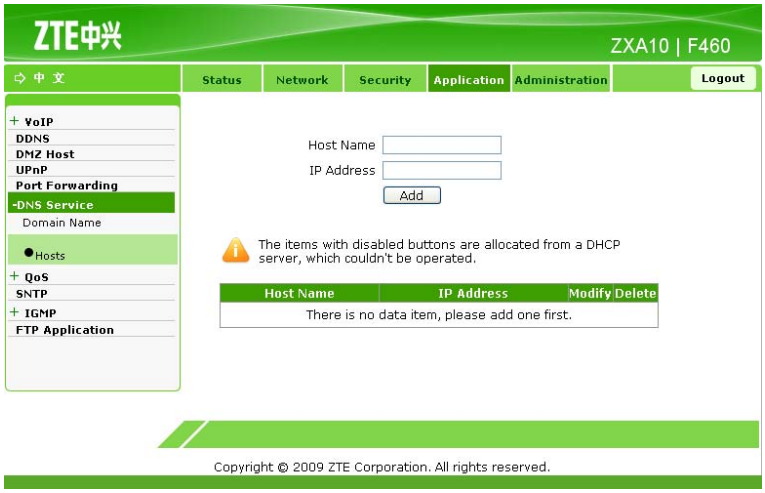
Context

Set host name parameters of the device.

Steps

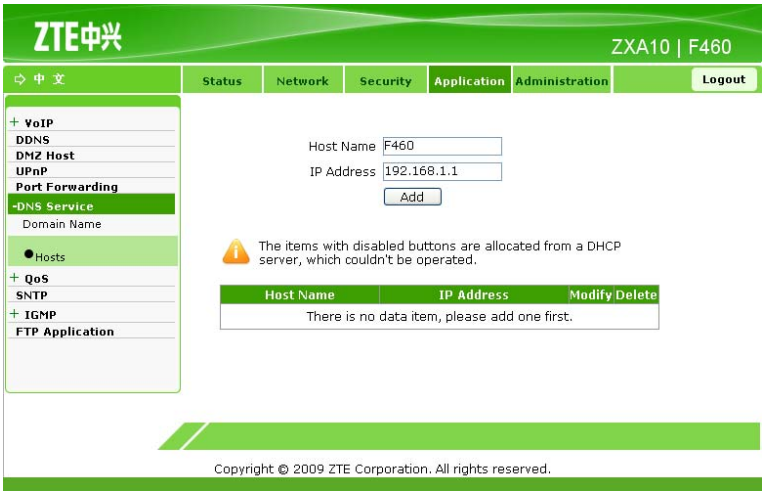
1. Click **Application > DNS Service > Hosts** in the WEB page to open the **host name** page, as shown in Figure 83.

Figure 83 Host Name



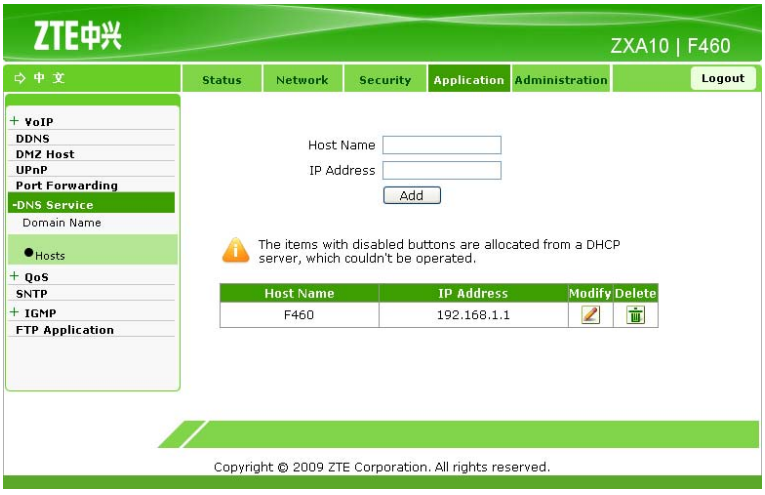
2. Type in **host name** and **IP address**, as shown in Figure 84.

Figure 84 Host Name Configuration



3. Click **Add** to finish the configuration, as shown in Figure 85.You can click **Modify** to modify a host name parameter or click **Delete** to delete it.

Figure 85 Finishing Page of Host Name Configuration



QoS Settings

Prerequisite

User has logged in WEB page of the device.

Context

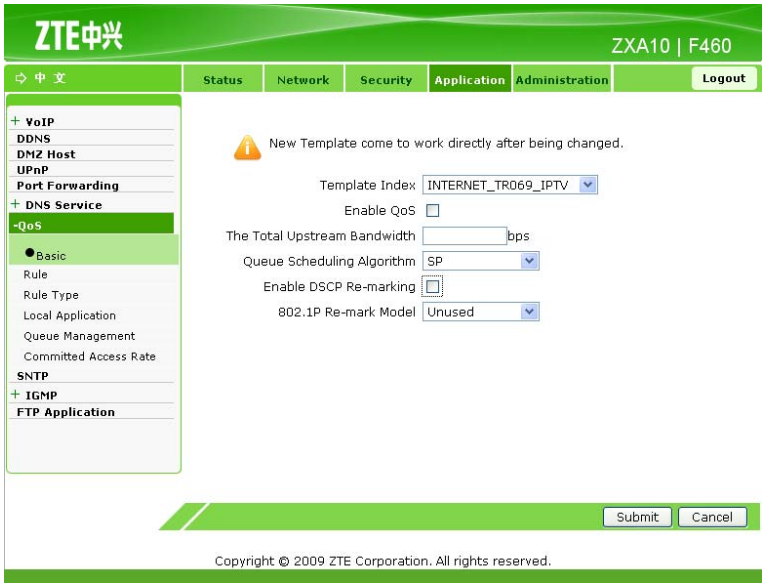
Configuration of ZXA10 F460/F460B QoS mainly include:

- Basic settings
- Rule settings
- Rule type
- Local application
- Queue management
- Committed access rate

Steps

1. Click **Application > QoS** in the WEB page to open the **QoS** configuration page, as shown Figure 86.

Figure 86 QoS Configuration



Basic QoS Parameters

Prerequisite

User has logged in WEB page of the device.

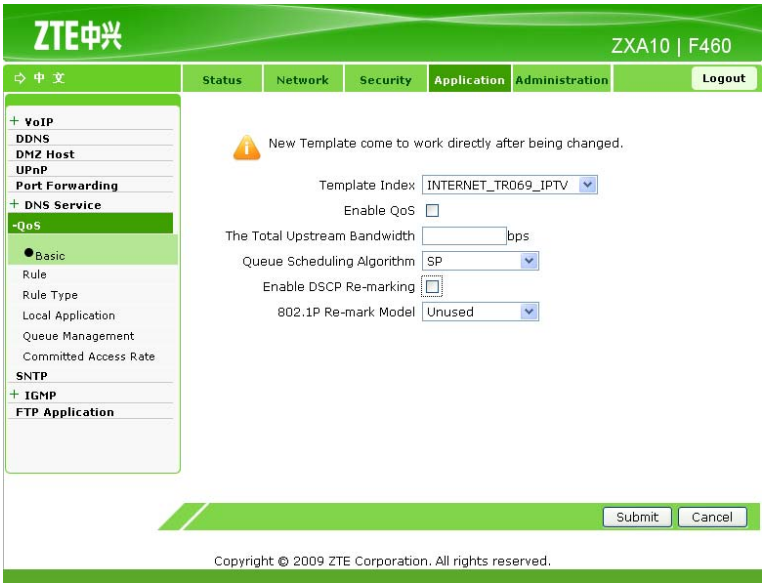
Context

Set basic QoS parameters of the device.

Steps

1. Click **Application > QoS** in the WEB page to open the **basic parameter** page, as shown in Figure 87.

Figure 87 Basic Settings



2. Configure basic QoS parameters, as shown in Figure 88.Basic QoS parameters are described in Table 22.

Figure 88 Basic QoS Parameters

Table 22 Basic QoS Parameters

Parameter	**Description**
Template index	Type of template index
Enable QoS	Enable QoS
Total upstream bandwidth	Uplink rate at WAN interface. Value range: 8000~104857600 bps
Queue scheduling algorithm	Choose queue scheduling algorithm. Support SP, DWRR and SP_DWRR
Enable DSCP re-marking	Enable DSCP re-marking
802.1P Re-mark Model	Enable 802.1p re-marking mode. Three modes are supported: unused, transparency and rewrite

Note:

SP (Strict Priority) is the simplest queuing mode. It serves the queue with the highest PRI first and will not turn to the queue with lower PRI until the first queue is empty. Advantage of this approach is that services with higher PRI will always be processed ahead of lower-PRI services. Nevertheless, lower-PRI services may be thoroughly blocked due to that.

The WRR (Weighted Round Robin) mode serves all queues and allocates precedence to queues of higher PRI. In most cases, WRR handles high-PRI services ahead of low-PRI services. However, it does not necessarily means that services of lower PRI will be thoroughly blocked, especially when number of high-PRI services is big.

If queue scheduling algorithm is configured as DWRR, you can enable the DWRR queue bandwidth lock.

DWRR Queue Bandwidth Lock: Remained bandwidth cannot be shared by other queues when this function is enabled. Remained bandwidth, if there is any, will be shared by other queues according to their weights if this function is not enabled.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

QoS Classification Rules

Prerequisite

User has logged in WEB page of the device.

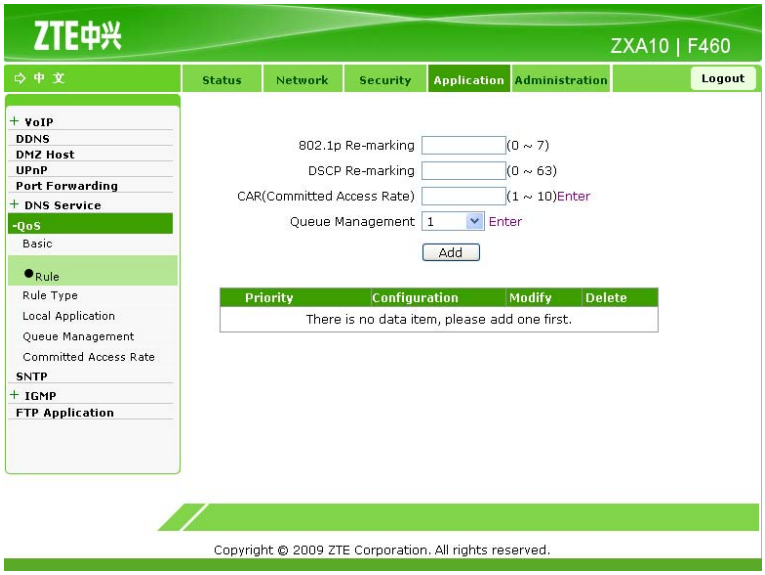
Context

Set parameters of QoS classification rules

Steps

1. Click **Application > QoS > Rule** in the WEB page to open the page as shown in Figure 89.

Figure 89 Rule Setting



2. Configure parameters of QoS rules, as shown in Figure 90.Parameters of QoS rules are configured in Table 23.

Figure 90 Rule Setting

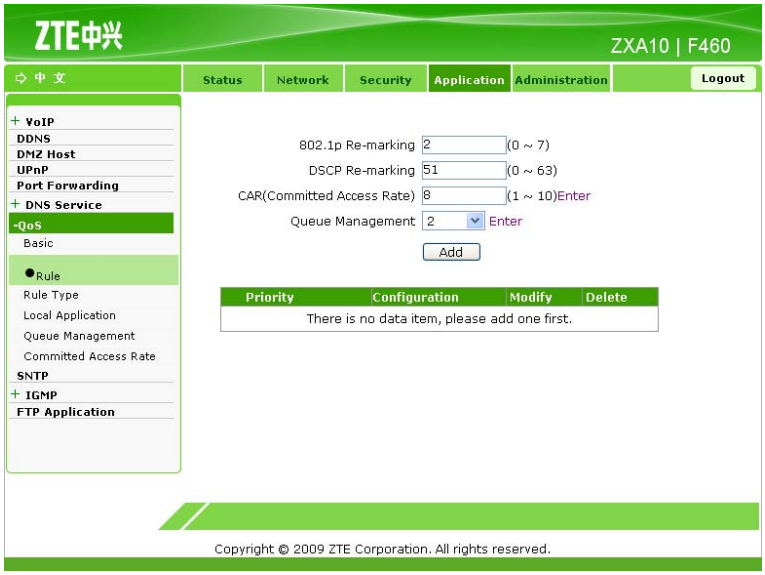


Table 23 Parameters of QoS Rules

Parameter	Description
802.1P re-marking	802.1p identifier value, range: 0-7
DSCP re-marking	DSCP identifier, range: 0-63
CAR (Committed Access Rate)	CAR rule, range: 0-10
Queue management	Queue ID, allocated by system upon configuration

3. Click **Submit** to save the configurations or **Cancel** to undo them.
4. Click **Enter** to start the configuration.

QoS Classification Rule Type

Prerequisite

User has logged in WEB page of the device.

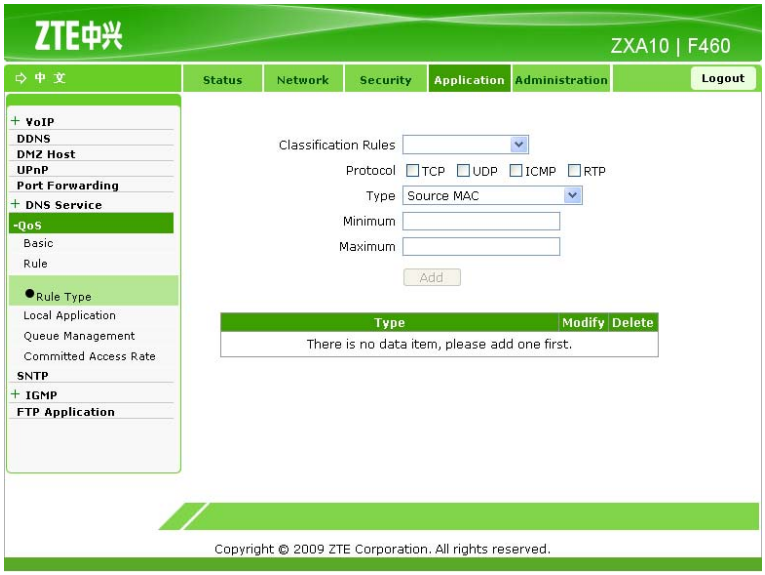
Context

Set parameters of QoS classification type.

Steps

1. Click **Application > QoS > Rule Type** in the WEB page to open the **rule type** page, as shown in Figure 91.

Figure 91 Classification Type Setting



2. Configure parameters of QoS rule type, as shown in .Parameters of QoS rule type are described in Table 24.

Table 24 Parameters of QoS Classification Type

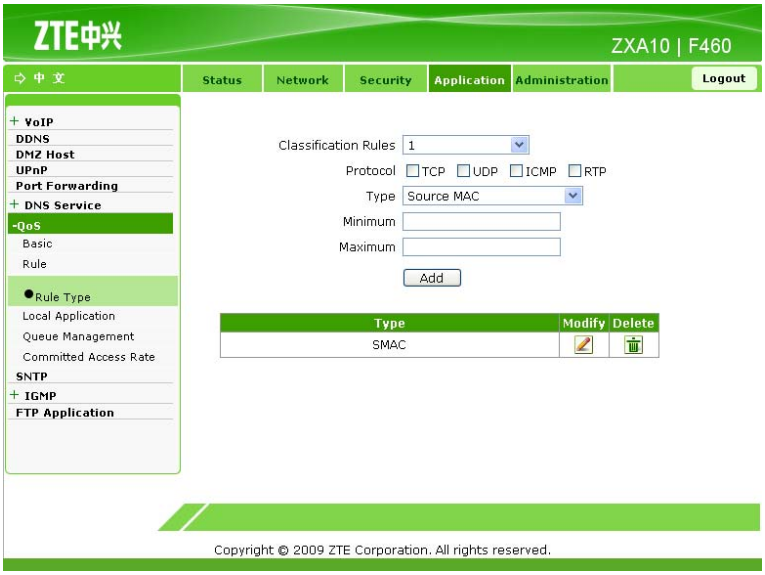
Parameter	Description
Classification Rules	Support 10 classification rules that correspond to CAR
Protocol	Configure an internal protocol, which can be one of TCP, UDP, ICMP and RTP
Type	Choose a type
Minimum	Configure the minimum value according to data type
Maximum	Configure the maximum value according to data type

Note:

Classification rules can be used only after CAR is configured.

3. Click **Add** to finish configuration of QoS classification rules, as shown in Figure 92.

Figure 92 Finishing Page of QoS Classification Type Configuration



4. You can click **Modify** to modify a parameter or **Delete** to delete it.

Local Applications of QoS

Prerequisite

User has logged in WEB page of the device.

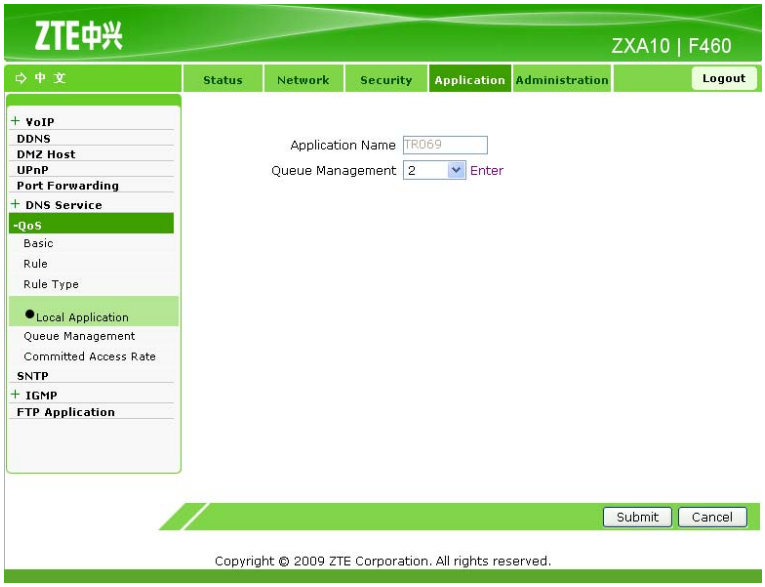
Context

Set parameters of QoS local application.

Steps

1. Click **Application > QoS > Local Application** in the WEB page to open **local application**, as shown in Figure 93.

Figure 93 Local Application



2. Choose queue ID in **Queue Management** and click **Enter** to start settings of **queue management**.

   Note:

   Only support TR069 mode at this moment.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

QoS Queue Management

Prerequisite

User has logged in WEB page of the device.

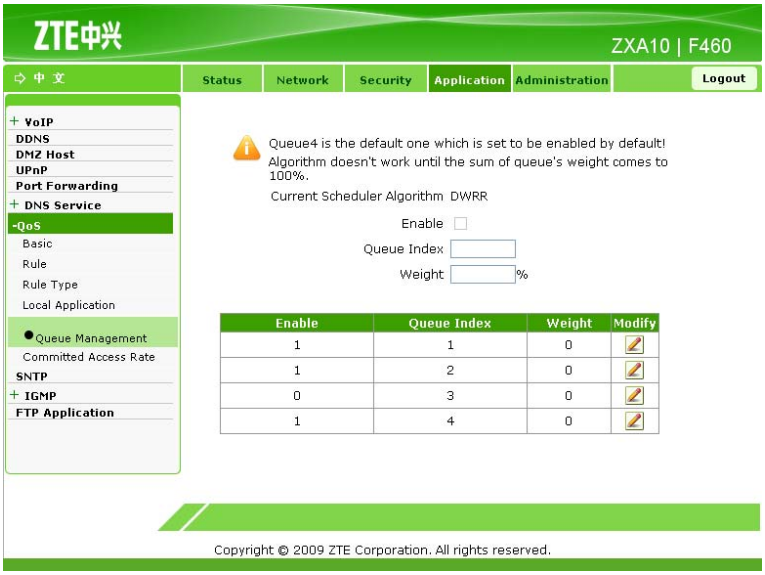
Context

Set parameters of QoS queue management.

Steps

1. Click **Application > QoS > Queue Management** in the WEB page to open the **queue management** page, as shown in Figure 94.

Figure 94 Queue Management Setting



2. Click **Modify** to modify queue management settings of a queue.
3. Choose if Queue Management should be enabled or not.
4. Click **Modify** to finish the configuration.

Note:

1 means enabled and 0 means disabled.

If the queue management algorithm is DWRR, you need to configure weight of queues.

Weight: Proportions of data stream that pass through each queue against the total volume.

Committed Access Rate of QoS

Prerequisite

User has logged in WEB page of the device.

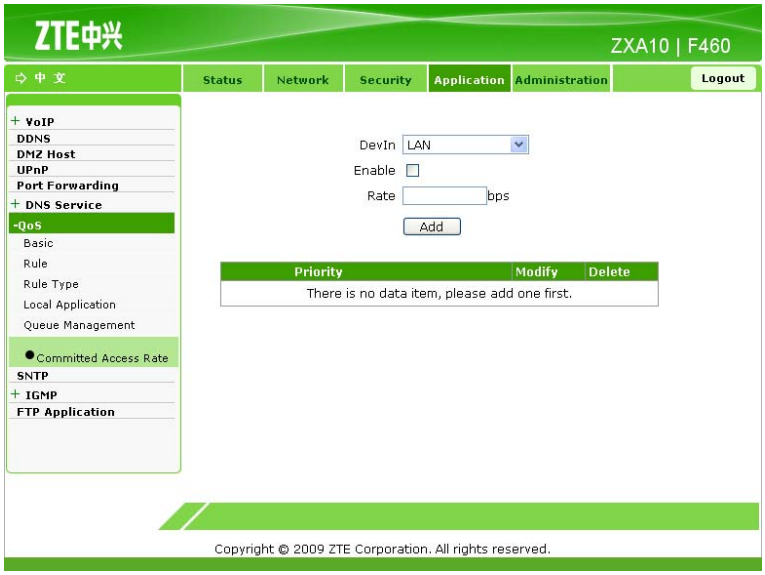
Context

Set parameters of QoS CAR.

Steps

1. Click **Application > QoS > Committed Access Rate** in the WEB page, as shown in Figure 95.

Figure 95 CAR Settings



2. Configure CAR parameters as shown in Figure 96.Parameters of CAR are described in Table 25.

Figure 96 CAR Settings

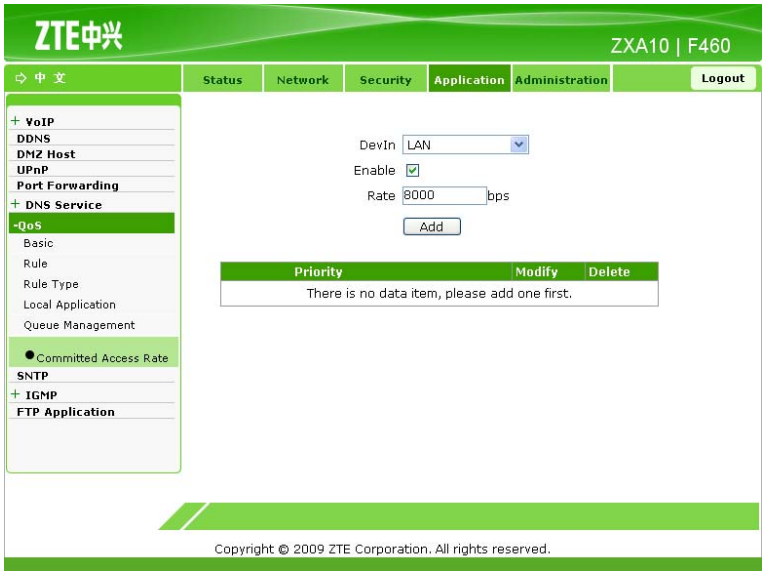


Table 25 CAR Parameters

Parameter	Description
DevIn	Choose CAR user interface
Enable	Enable CAR
Rate	Rate in the range of 8000~104857600 bps

3. Click **Add** to finish the configuration.
4. You can click **Modify** to modify a parameter or **Delete** to delete it.

Time Management

Prerequisite

User has logged in WEB page of the device.

Context

Set time management parameters of the device to realize time synchronization between the device and the NTP server.

Steps

1. Click **Application > SNTP** in the WEB page, as shown in Figure 97.

Figure 97 Time Management

2. Configure SNTP parameters in the page as shown in Figure 97. Parameters of SNTP are described in Table 26.

Figure 98 SNTP Configuration

Table 26 SNTP Parameters

Parameter	**Description**
Time zone	Set time zone of user
Primary NTP server address	Address of primary NTP server
Secondary NTP server address	Address of secondary NTP server
Poll interval	Poll interval (Unit: second), interval of time synchronization
Enable daylight saving time	Whether enable daylight saving time

3. Click **Submit** to save the configurations or **Cancel** to undo them.

8 Administration

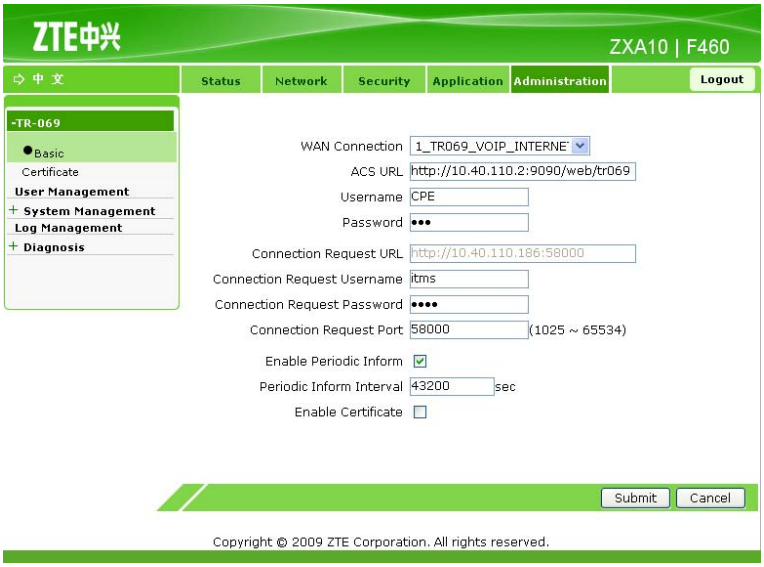
Remote Management

Remote management of ZXA10 F460/F460B mainly consists of:

- Basic Settings
- Certificate Settings

Click **Administration > TR-069** in the WEB page, as shown in Figure 99.

Figure 99 TR-069 management



Basic TR069 Parameters

Prerequisite

User has logged in WEB page of the device.

Context

Set basic TR069 parameters of the device.

Steps

1. Click **Administration > TR-069** in the WEB page to open the basic parameters of TR069, as shown in .

Basic Parameters of TR069

2. Configure basic parameters of TR069, as shown in Figure 100. Basic parameters of TR069 are described in Table 27.

Figure 100 Basic Parameters of TR069

Table 27 Basic Parameters of TR069

Parameter	Description
WAN connection	Connection interface at WAN side
ACS URL	ITMS server address
Username	Username for logging on ITMS server
Password	Password for logging on ITMS server
Connection request URL	Address of WAN connection interface
Connection request username	Connection request username
Connection request password	Connection request password
Connection request port	TR069 protocol port, i.e. communication port between F460/F460 and itms. Value range: 1025 ~65534
Enable periodic inform	Enable periodic inform
Periodic inform interval	Interval of periodic inform (unit:s)
Enable certificate	Enable certificate

3. Click **Submit** to save the configurations or **Cancel** to undo them.

TR069 Certificate Management

Prerequisite

User has logged in WEB page of the device.

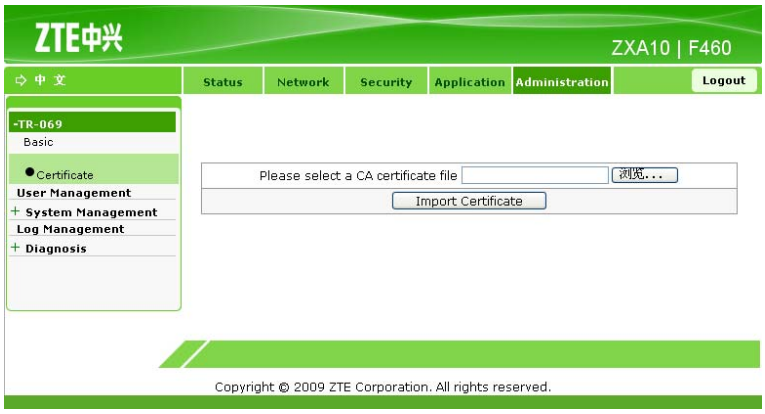
Context

Import TR069 certificate.

Steps

1. Click **Administration > Certificate** in the WEB page, as shown in Figure 101.

Figure 101 Certificate Setting



2. Click **Browse** and choose the CA file you need to import.
3. Click **Import Certificate** to import the certificate.

User Management

Prerequisite

User has logged in WEB page of the device.

Context

Set user management parameters of the device.

Steps

1. Click **Administration > User Management** in the WEB page, as shown in Figure 102.

Figure 102 User Management

2. Configure user management parameters.

   Note:

   There are two types of user right, administrator and user.

3. Click **Submit** to save the configurations or **Cancel** to undo them.

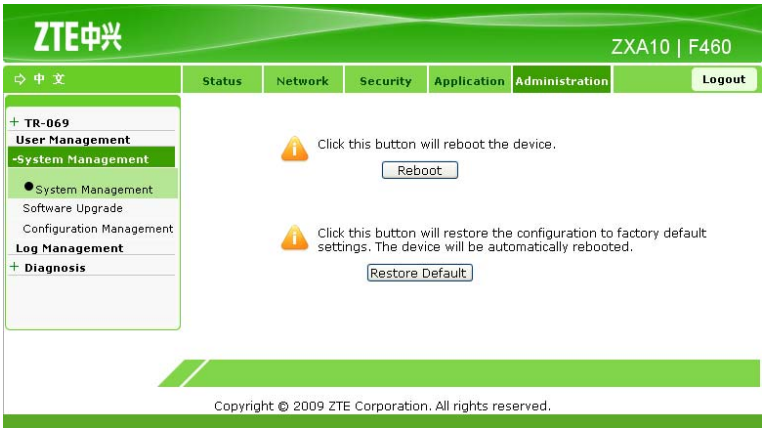
System Management

ZXA10 F460/F460B system management mainly consists of:

- System Management
- Software Upgrade
- Configuration Management

Click **Administration > System Management** in the WEB page to open the **system management** page, as shown in Figure 103.

Figure 103 System Management



System Management

Prerequisite

User has logged in WEB page of the device.

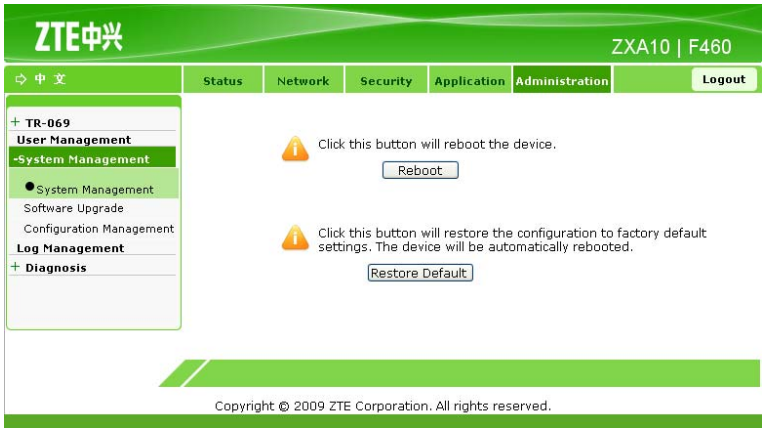
Context

Set system management parameters of the device.

Steps

1. Click **Administration > System Management** in the WEB page and the **system management** page will be opened by default, as shown in Figure 104.

Figure 104 System Management



2. Click **Reboot** and system reboots.
3. Click **Restore** Default and default settings are restored.

Software Upgrade

Prerequisite

User has logged in WEB page of the device.

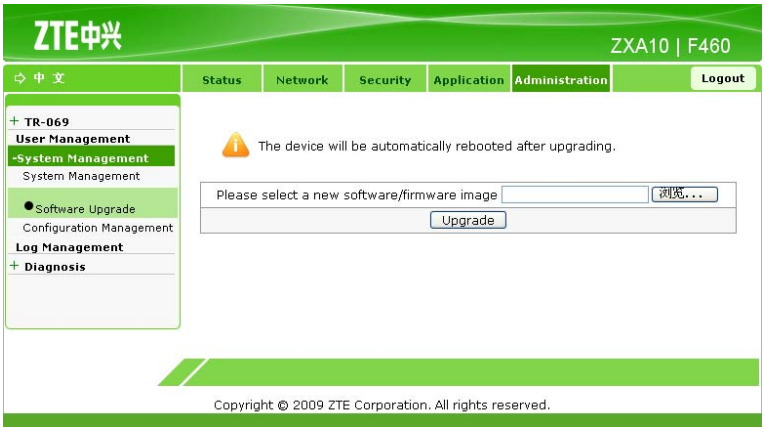
Context

Upgrade software of the device.

Steps

1. Click **Administration > System Management > Software Upgrade** in the WEB page to open the **software upgrade** page, as shown in Figure 105.

Figure 105 Software Upgrade



2. Click **Browse** to choose the software file you need to upgrade.
3. Click **Upgrade** to upgrade it.

Note:

Power-off during upgrade may damage the device.

Prompts are shown during upgrade. The system automatically returns to login page after upgrade succeeds.

Configuration Management

Prerequisite

User has logged in WEB page of the device.

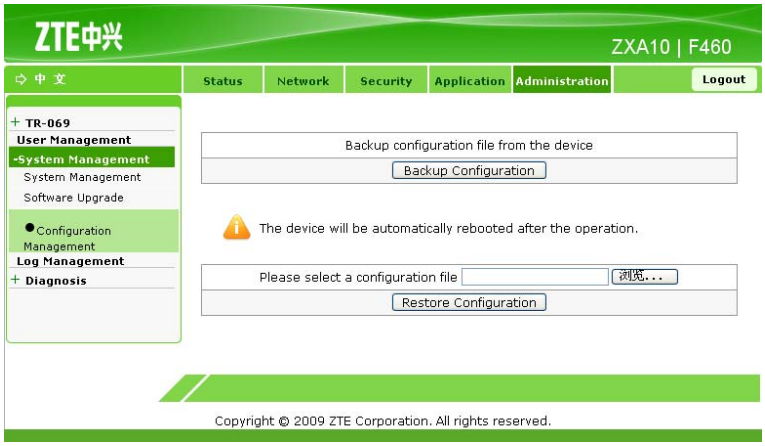
Context

Set configuration management parameters of the device.

Steps

1. Click **Administration > System Management > Configuration Management** in the WEB page as shown in Figure 106.

Figure 106 Configuration Management



2. Click **Backup Configuration** to export configuration file.
3. Click **Browse** to choose the configuration file you need to import.
4. Click **Restore Configuration** to import the file.

Log Management

Prerequisite

User has logged in WEB page of the device.

Context

Set log management parameters of the device.

Steps

1. Click **Administration > Log Management** in the WEB page to open the **log management** page, as shown in Figure 107.

Figure 107 Log Management

2. Configure log management parameters, which are described inTable 28.

Table 28 Log Management Parameters

Parameter	Description
Log enable	Whether enable log server
Log level	Logs are of the following levels, Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency in ascending order. After log level is configured, only logs of the very level and above will be recorded

3. Click **Refresh** and the latest 20 records will be displayed.
4. Click **Clear Log** to clear current log records.
5. Click **Download Log** to save log files to local.

Diagnosis Maintenance

Ping Diagnosis

Prerequisite

User has logged in WEB page of the device.

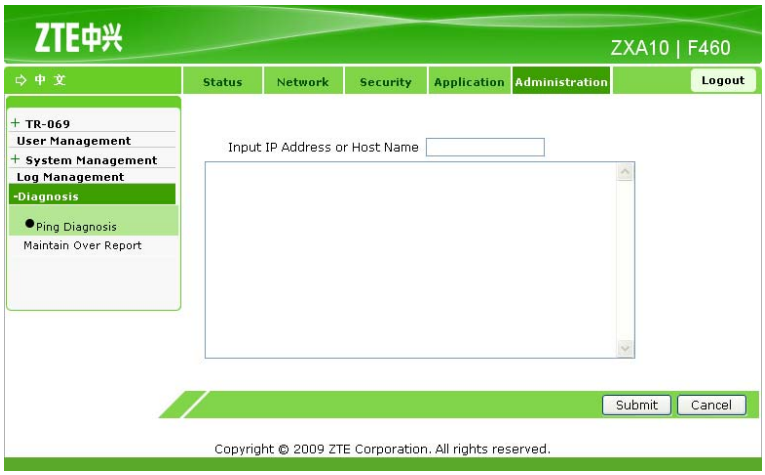
Context

Use PING diagnosis to test links.

Steps

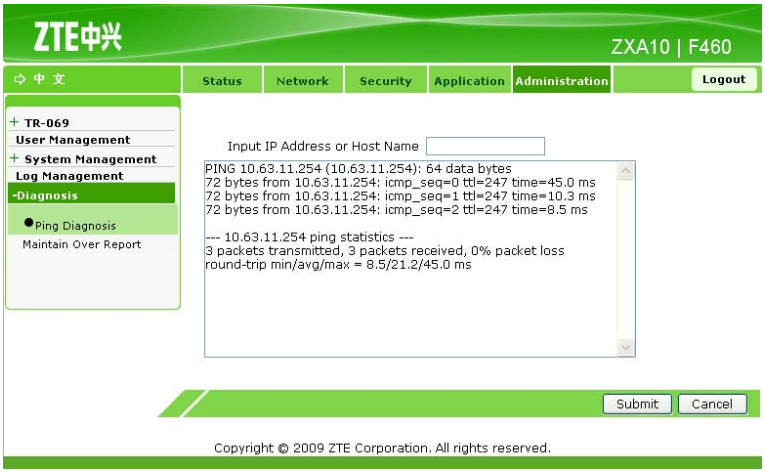
1. Click **Administration > Diagnosis** in the WEB page to open the **Diagnosis** page, as shown in Figure 108.

Figure 108 Diagnosis



2. Type in host IP or hostname in Input **IP Address** or **Host Name**.
3. Click **Submit** to start link test, as shown in Figure 109.

Figure 109 Result of Ping Diagnosis



Maintain Over Report

Prerequisite

User has logged in WEB page of the device.

Context

Generate maintenance report of the device.

Steps

1. Click **Administration > Diagnosis > Maintain Over Report** in the WEB page as shown in Figure 110.

Figure 110 Maintain Over Report

2. Click **Maintain Over** to generate maintain report.

9 Typical Applications

Internet Access

Click **Network** in the WEB page to open **WAN Connection** where broadband connection parameters can be configured. Refer to Section 5.1 for details.

VoIP Configuration

Click **Application** in the WEB page to open the **VoIP configuration** page where VoIP parameters can be configured. Refer to Section 7.1 for details.

Wireless Terminal Access

Click **Network > WLAN** in the WEB page to open **WLAN configuration** where access parameters of wireless terminals can be configured. Refer to Section 5.2 for details.

File Server Configuration

Using file server, you can access files in USB storage devices through FTP as if they are files in file server.

Click **Application > FTP Application** in the WEB page to open the **FTP configuration** page where parameters of FTP server can be configured. Refer to Section 7.10 for details.

Click **Start > Run** in Windows system and type in FTP access address of ZXA10 F460/F460B, for example FTP:// 192.168.1.1. Use the username and the password configured in **FTP Application** to open the file server of ZXA10 F460/F460B and access contents in USB devices.

A Frequently Asked Questions

- How to configure TCP/IP before my PC can get connected to the device?

  You need to configure IP address of your PC manually. Default IP of the device is `192.168.1.1` so IP address of your PC should be in the range of 192.168.1.2~192.168.1.254 and the subnet mask should be 255.255.255.0.

- How to find out if my PC has been connected to the device?

  You can execute **PING 192.168.1.1** to check the connection. It gets time-out if anything is wrong with the connection.

- How to set the device through WEB?

  Open IE after you are connected to the device and type in http://192.168.1.1 to access WEB configuration page of the device. Default username and password are both “admin”.

- Can I restore default settings of the device?

  Yes. To do that, please press the RST button for over 10 seconds and the device will restart and default settings will be restored.

- What should I do if the PON link lamp stays off?

  If the PON link lamp stays off, it indicates the PON link has not been established yet. Please check if fiber is firmly plugged in PON broadband port, if the other end of fiber is properly connected to lead-in port and if fiber tail at the device side is bent or folded.

- What should I do if the RUN lamp does not flash as it should when the device is running normally?

  If the RUN lamp is off, it indicates the power adapter is out of order. If the RUN lamp is off meanwhile the ALARM lamp is red and remains lit, it indicates that power-on self-test of the device has failed due to version or configuration problem and you need to change the version. Or, please press the RST button for over 10 seconds to redo the configurations if the problem is caused by wrong configuration.

- What should I do if I can’t make calls?

  Check if you can hear beep from the phone connected to PHONE1 or PHONE2 port of the device, by which you can judge if the phone has been connected properly. Then, open the WEB page of the device, click **Application** and examine VoIP configurations as you are told in Section 7.1. If you cannot make calls still while the configurations are correct and the phone has been connected properly, please contact your service provider.

B Glossary

10Base-T/100Base-TX

It is the adaptive version of the Ethernet protocol. 10Base-T uses a twisted pair with the MAX length 100m and the MAX rate 10Mbps. 100Base-TX is similar to 10Base-T except that is uses two high-quality twisted pairs and the MAX rate is 100Mbps.

Adapter

It is used to connect devices in a network segment, such as Ethernet, MODEM and adapter.

WEP

WEP is the acronym of Wired Equivalent Privacy. It is a data encryption method based on 64bit shared key. It is described in IEEE 8.0.11b.

Bandwidth

Data volume that can be transmitted within specific time

DDNS

DDNS is the network server that binds fixed domain name and dynamic-changing IP.

DHCP

DHCP is the acronym of Dynamic Host Configuration Protocol. It allocates dynamic IP addresses to network devices. Dynamic address means that a device can have different IP address every time it connects the network.

DNS

DNS means Domain Name Server. It translates name of network node into network address in Internet.

Domain Name

Domain name is used to mark name of one or more hosts. For example, the domain name www.yahoo.com represents a number of IP addresses. A part of URL, domain name is used to indicate address of specific Web page, for example, domain name is www.zte.com.cn in http://www.zte.com.cn/index.jsp.

Ethernet

Ethernet is one of the most common LAN protocols. It supports the bus technology and the transmission rate is 10 Mbps~1000 Mbps.

Explorer

Explorer is used to search and display Web pages, for example Netscape Navigator and Microsoft Internet Explorer.

Firewall

Firewall is the safety screen between internal and external networks. To be exact, firewall is a series of components configured between networks or security domains. It screens information, structure and running status of client's network by monitoring, restricting or changing data streams of different domains.

IEEE

IEEE is the acronym of Institute of Electrical and Electronics Engineers. It is the most prestigious organization that formulates standards for electrical and electronics fields.

Internet

Internet is a global network where millions of computers exchange data, news and views.

IP Address

IP address is a 32-bit address used to identify host in TCP/IP

IPSec

It is a VPN protocol widely accepted by the industry. Safety and reliability of data transmission can be strengthened by establishment of IPSec VPN.

ISP

Internet Service Provider provides access to personal and corporate users of Internet.

LAN

LAN is a network environment that connects communication devices (such as computer, terminal and printer) in limited areas like room and campus.

MAC Address

Medium Access Control address is the Layer 2 address of a network node. Every network device, such as network card, hub and switch, has its own MAC address. Layer 2 switch sends data to the correct destination node by judging destination MAC address of data packets.

NAT

NAT is the acronym of Network Address Translation. When more than one computers in a LAN share one IP address to access Internet, they need NAT to translate private network address into public network address of WAN port.

PPP

PPP is the Point-to-Point protocol. It offers a standard mode of message transmission at point-to-point links, for example telephone line.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is an extended protocol of PPP. It provides point-to-point connection in Ethernet to establish user-oriented session channel (user authentication needed).

PPTP

It is a VPN protocol that allows PPP packets to be safety transmitted at the IP layer.

Protocol

It means communication protocol here. Communication protocols set forth rules by which network devices send/receive data.

Router

Router is used to interconnect networks of different types through WAN. It interconnects with the router or other network device at the other side of WAN through ISP line so that data can be transmitted through long distance. The process of selecting path to destination according to address information in data packet is called “routing”.

SPI

SPI is the acronym of Stateful Packet Inspection. It inspects not only head of packets but also content of packets. It helps us to determine source and destination addresses of packets as well as other information. Stateful inspection firewall keeps ports closed until clear port request arrives.

TR069

It is one of terminal management protocols of WAN users (CPE WAN Management Technical Report 069). According to TR069, operator and family gateway perform safe interaction so that initial configuration and auto-upgrade of family gateway can be conducted. It lowers cost and risk.

VPN

Virtual Private Network provides a safe method for data transmission in Internet with access control and encryption. The effect can reach or be close to safety level of private network.

WAN

Though some WANs are also private, it is generally regarded as public access network.

Figures

Tables