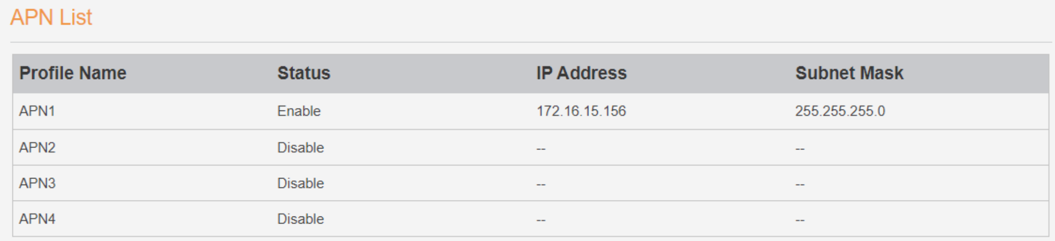
3.3 Viewing APN List

To view the APN list, perform the following steps:

1. Choose **Statistics**;
2. In the **APN List**, view the information about APN information. As shown in Figure 3-3.



APN List

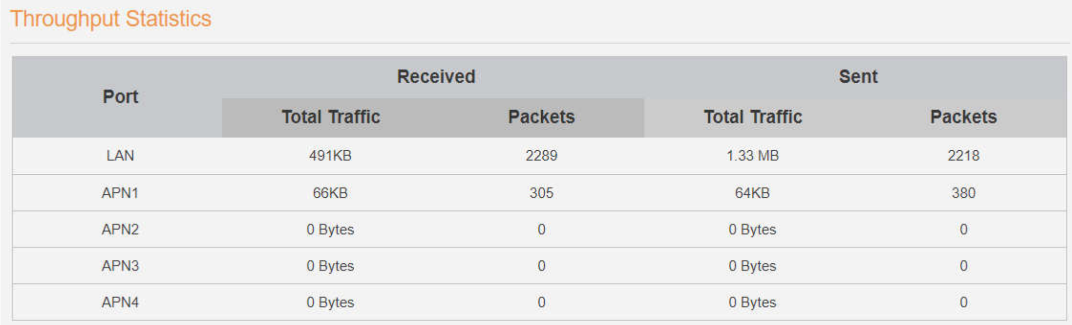
Profile Name	Status	IP Address	Subnet Mask
APN1	Enable	172.16.15.156	255.255.255.0
APN2	Disable	--	--
APN3	Disable	--	--
APN4	Disable	--	--

Figure 3-3

3.4 Viewing Throughput Statistics

To view the Throughput Statistics, perform the following steps:

1. Choose **Statistics**;
2. In the **Throughput Statistics** area, view the throughput statistics, such as APN throughput and LAN throughput.
3. In this area, also you can choose and click the button **Reset** to empty the throughput statistics. As shown in Figure 3-4.



Throughput Statistics

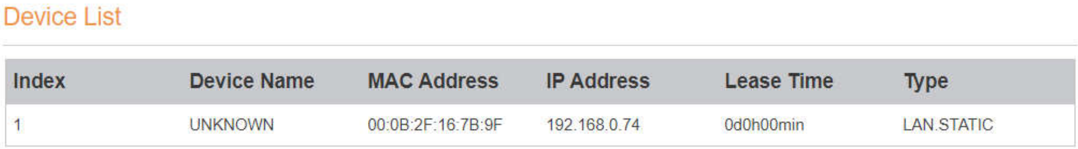
Port	Received		Sent	
	Total Traffic	Packets	Total Traffic	Packets
LAN	491KB	2289	1.33 MB	2218
APN1	66KB	305	64KB	380
APN2	0 Bytes	0	0 Bytes	0
APN3	0 Bytes	0	0 Bytes	0
APN4	0 Bytes	0	0 Bytes	0

Figure 3-4

3.5 Viewing Device List

To view the device list, perform the following steps:

1. Choose **Statistics**;
2. In the **Device List** area, view the device information which connect to the CPE, such as Device name, Mac address, IP address and Lease time. As shown in Figure 3-5.



Device List

Index	Device Name	MAC Address	IP Address	Lease Time	Type
1	UNKNOWN	00:0B:2F:16:7B:9F	192.168.0.74	0d0h00min	LAN.STATIC

Figure 3-5

4 Update

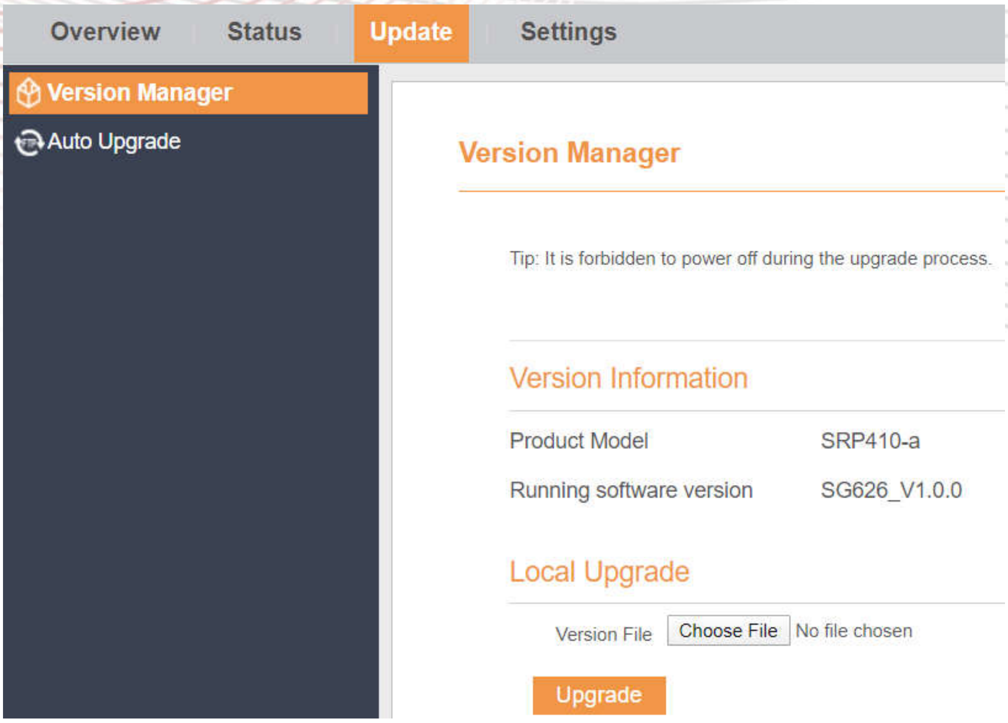
4.1 Version Manager

This function enables you to upgrade the software version of the CPE to a new version.

Viewing Version Info

To view the version info, perform the following steps:

1. Choose **Update**>**Version Manager**.
2. In the **Version Info** area, you can view the product name and software version. As shown in Figure 4-1.



Version Manager

Tip: It is forbidden to power off during the upgrade process.

Version Information

Product Model	SRP410-a
Running software version	SG626_V1.0.0

Local Upgrade

Version File: No file chosen

Figure 4-1

Version Upgrade

To perform an upgrade successfully, connect the CPE to your computer through a network cable, save the upgrade file on the computer, and make sure the CPE is not connected to anything other than a power adapter and the computer.

To perform an upgrade, perform the following steps:

1. Choose **Update**>**Version Manager**.
2. In the **Version Upgrade** area, click **Browser**. In the displayed dialog box, select the target software version file.
3. Click **Open**. The dialog box choses. The save path and name of the target software version

file are displayed in the Update file field.

4. Click **Submit**.
5. The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version. As shown in Figure 4-2.

⚠ During an upgrade, do not power off the CPE or disconnect it from the computer.

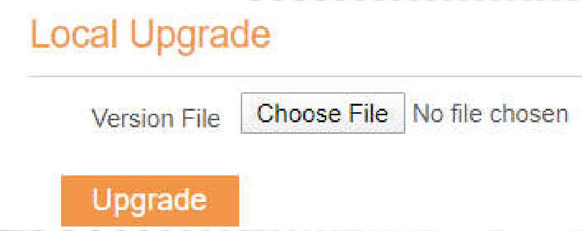


Figure 4-2

4.2 Auto upgrade

To perform a ftp auto upgrade successfully, make sure the CPE is connected to the Internet.

To perform a ftp auto upgrade, perform the following steps:

1. Choose **Update**>**Auto upgrade**.

2. Enable **auto upgrade**.

3. If you want to check new firmware after connect to Internet, you need to enable the item of **Check new firmware after connect to Internet**.

4. Set the ftp server address to the **Upgrade folder** box.

5. Set **Version file**. //This contain the new FW name

6. Set **User name** and **Password**.

7. Set the **Interval** of checking new firmware. //Check upgrade periodic

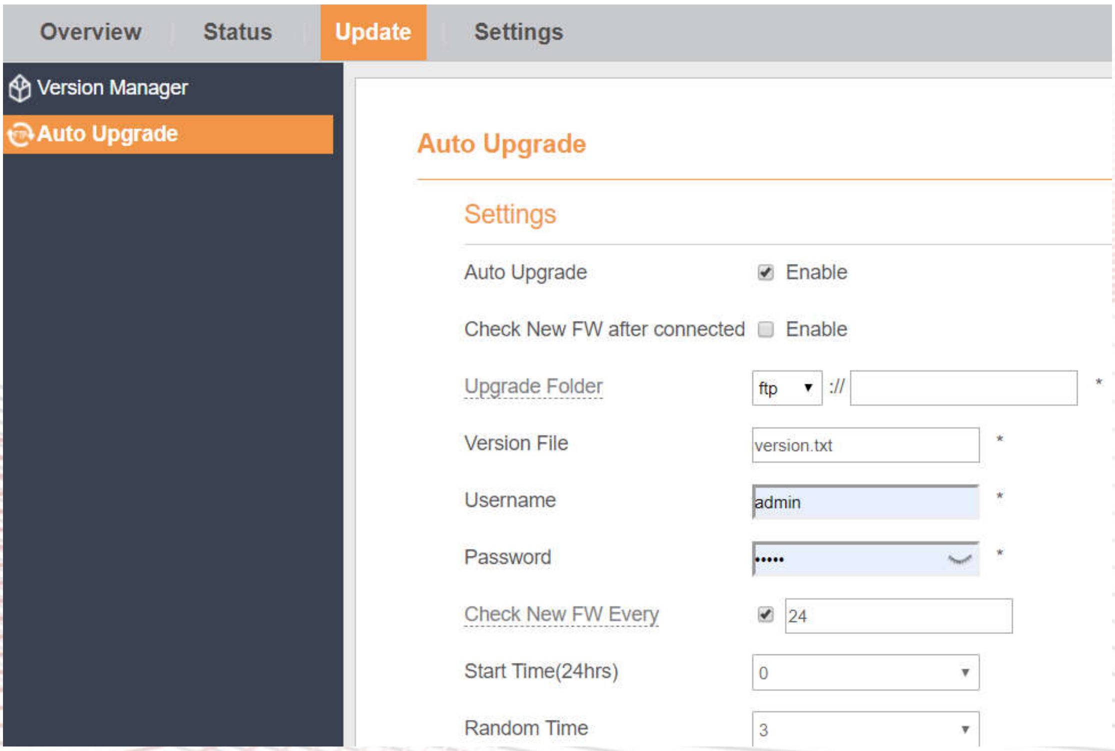
8. Set **Start time**.   // The time of upgrade begin

9. Set **Random time**. // Out of this time, UE will not upgrade.

10. Click **Submit**. As shown in Figure 4-3.

⚠ 1, The CPE will automatically upgrade according to the setting. During an upgrade, do not disconnect the power supply or operate the CPE.

2, If set interval of checking new FW, the start time and random time will shouldn’t be set.



Auto Upgrade

Settings

Auto Upgrade ☑ Enable

Check New FW after connected □ Enable

Upgrade Folder ftp ▾ :// *

Version File version.txt *

Username admin *

Password ••••• *

Check New FW Every ☑ 24

Start Time(24hrs) 0 ▾

Random Time 3 ▾

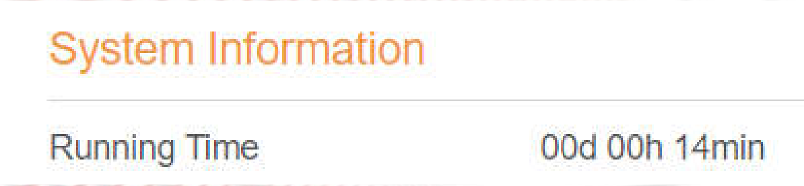
Figure 4-3

5 Settings

5.1 Viewing the Device Information

To view the System Information, perform the following steps:

1. Choose **Settings**;
2. In the **System Information** area, view the system status, such as Running time. As shown in Figure 5-1.



System Information

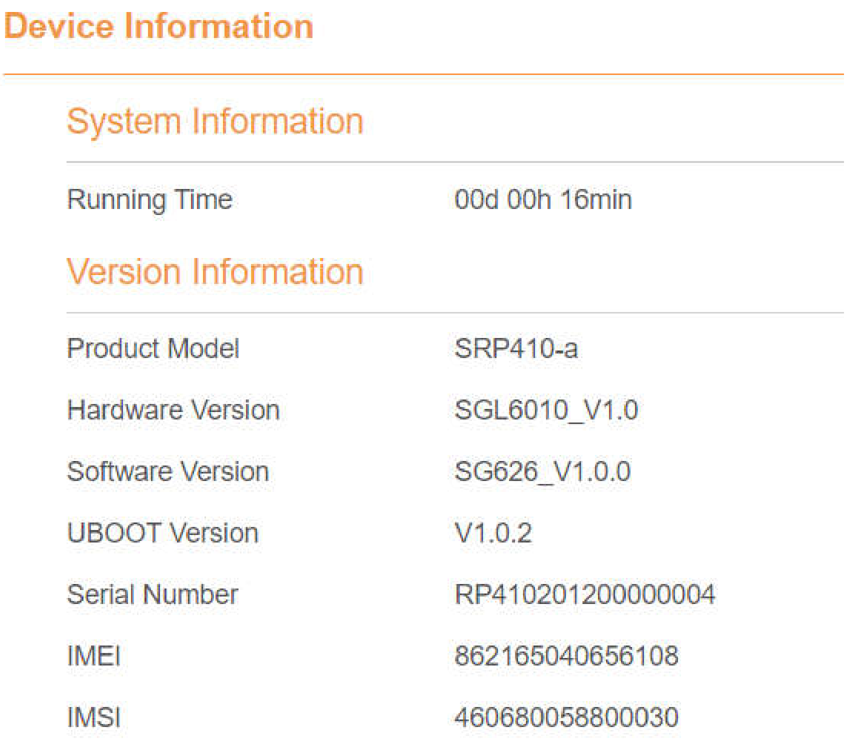
Running Time	00d 00h 14min

Figure 5-4

Viewing the Version Information

To view the Version Information, perform the following steps:

1. Choose **Settings**;
2. In the **Device Information** area, view the device information, such as Product name, Product Model, Hardware Version, Software version, UBoot version and CPE SN . As shown in Figure 5-2.



Device Information

System Information

Running Time	00d 00h 16min

Version Information

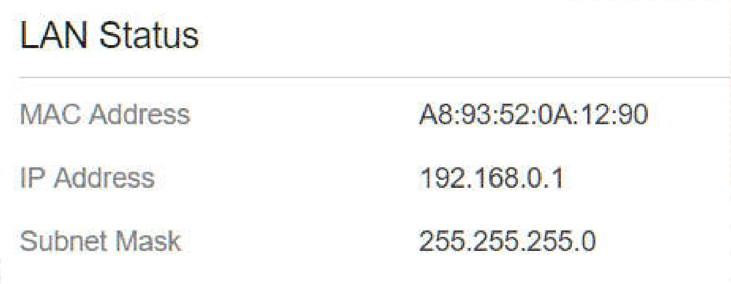
Product Model	SRP410-a
Hardware Version	SGL6010_V1.0
Software Version	SG626_V1.0.0
UBOOT Version	V1.0.2
Serial Number	RP410201200000004
IMEI	862165040656108
IMSI	460680058800030

Figure 5-5

Viewing LAN Status

To view the LAN status, perform the following steps:

1. Choose **Settings**;
2. In the **LAN Status** area, view the LAN status, such as Mac address, IP address and Subnet mask. As shown in Figure 5-4.



LAN Status

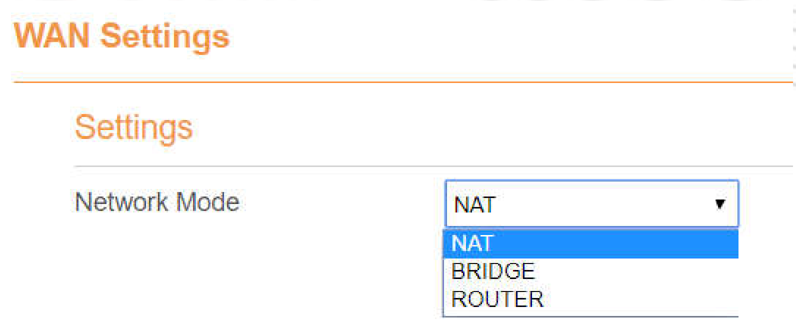
MAC Address	A8:93:52:0A:12:90
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

Figure 5-3

5.2 Viewing Network

5.2.1 Network Mode

1. To set the network mode, perform the following steps:
2. Choose **Network** >**WAN Settings**;
3. In the **Network Mode** area, select a mode between **NAT** and **ROUTER** and **Bridge**
4. Click **Submit**. As shown in Figure 5-5.



WAN Settings

Settings

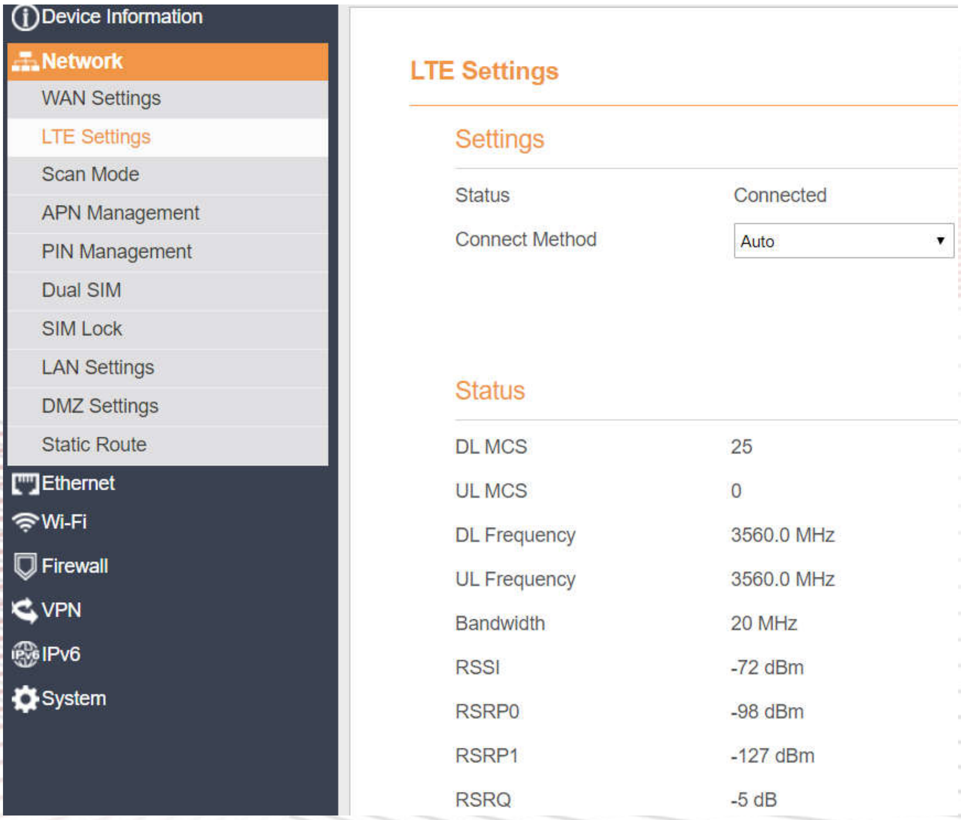
Network Mode: NAT

Figure 5-4

5.2.2 LTE Settings

To set the LTE network, perform the following steps:

1. Choose **Network** >**LTE Settings**;
2. In the **Settings** area, you can set the configuration of LTE network;
3. In the **Status** area, you can view the LTE network connect status, such as Frequency, RSSI, RSRP, RSRQ, CINR, SINR, Cell ID and so on. As shown in Figure 5-5.



LTE Settings

Settings

Status	Connected
Connect Method	Auto

Status

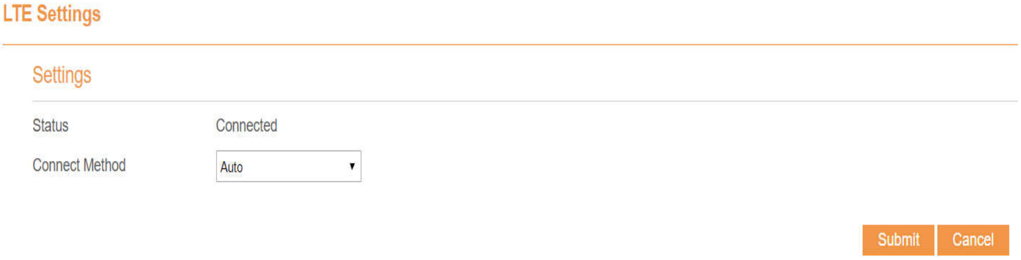
DL MCS	25
UL MCS	0
DL Frequency	3560.0 MHz
UL Frequency	3560.0 MHz
Bandwidth	20 MHz
RSSI	-72 dBm
RSRP0	-98 dBm
RSRP1	-127 dBm
RSRQ	-5 dB

Figure 5-5

Connect Method Setting

To set the connect method, perform the following steps:

1. Choose **Network > LTE Settings**;
2. In the **Setting** area, select a connect method between **Auto** and **Manual**. As shown in Figure 5-6.



LTE Settings

Settings

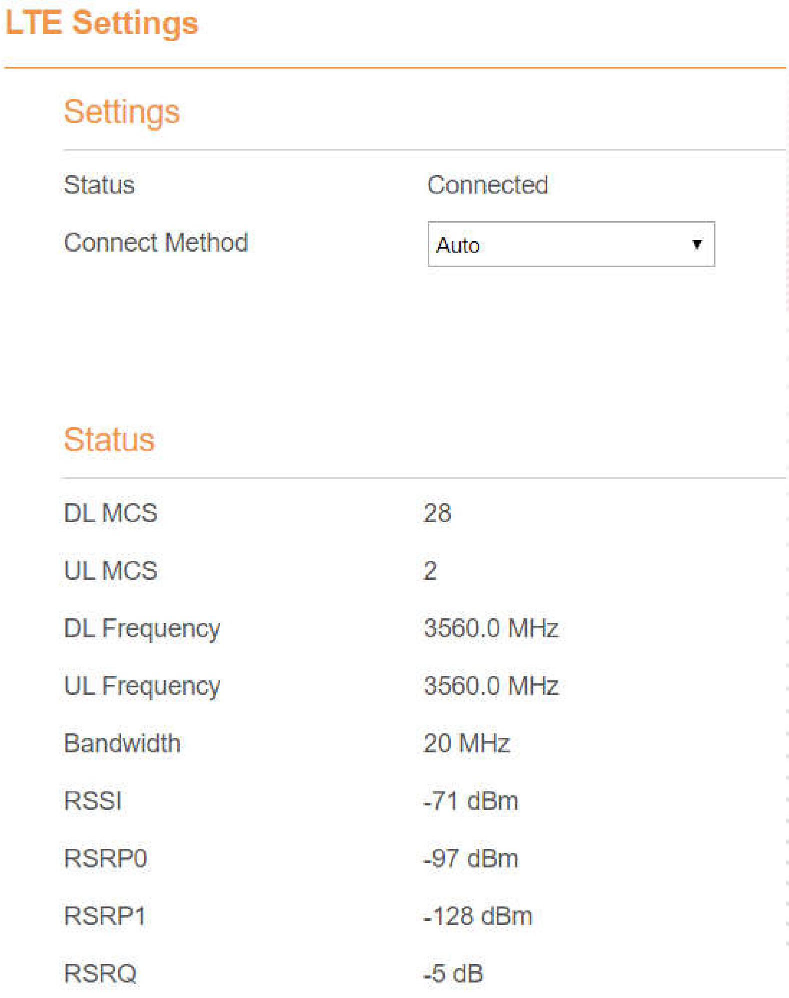
Status	Connected
Connect Method	Auto

Figure 5-6

Auto Connect LTE Network

To set the CPE automatically connect to the internet, perform the following steps:

1. Choose **Network > LTE Settings**;
2. In the **Setting** area, set the connect method as **Auto**. When the LTE network is ready, the CPE will be connected automaticity. As shown in Figure 5-7.



LTE Settings

Settings

Status	Connected
Connect Method	Auto ▼

Status

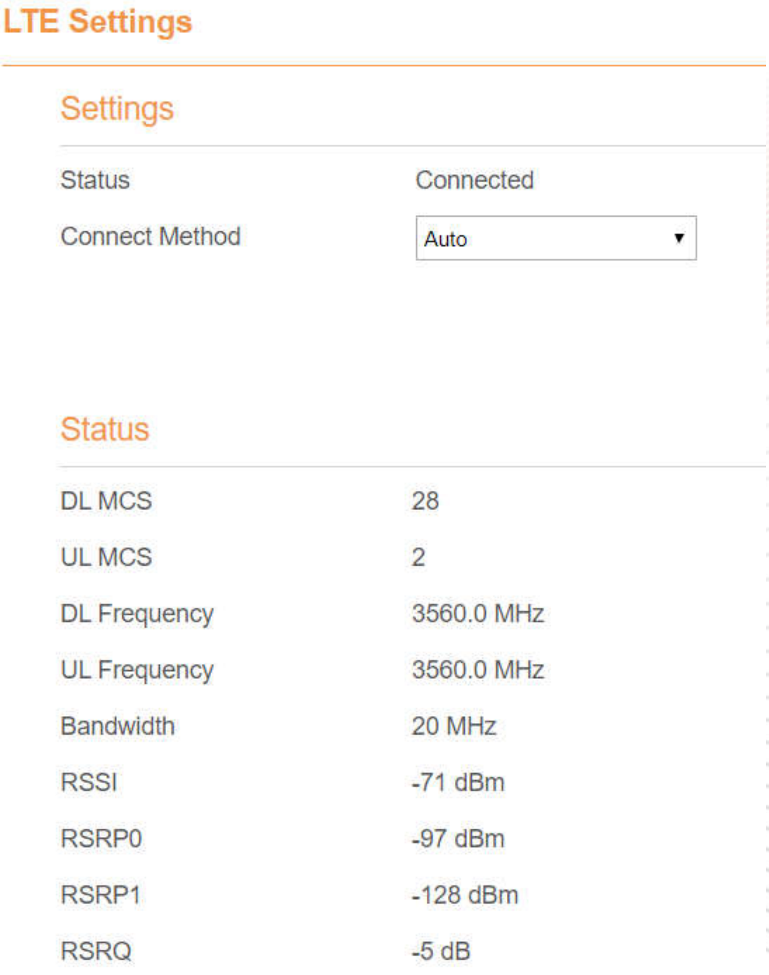
DL MCS	28
UL MCS	2
DL Frequency	3560.0 MHz
UL Frequency	3560.0 MHz
Bandwidth	20 MHz
RSSI	-71 dBm
RSRP0	-97 dBm
RSRP1	-128 dBm
RSRQ	-5 dB

Figure 5-7

Manual Connect Mobile Network

To set the mobile network manual connect to the internet, perform the following steps:

1. Choose **Network > LTE Settings**;
2. In the **Setting** area, set the connect method as **Manual**, when the LTE network is ready, you can set the CPE connect to the LTE network or disconnect from the LTE network. As shown in Figure 5-8.



LTE Settings

Settings

Status	Connected
Connect Method	Auto

Status

DL MCS	28
UL MCS	2
DL Frequency	3560.0 MHz
UL Frequency	3560.0 MHz
Bandwidth	20 MHz
RSSI	-71 dBm
RSRP0	-97 dBm
RSRP1	-128 dBm
RSRQ	-5 dB

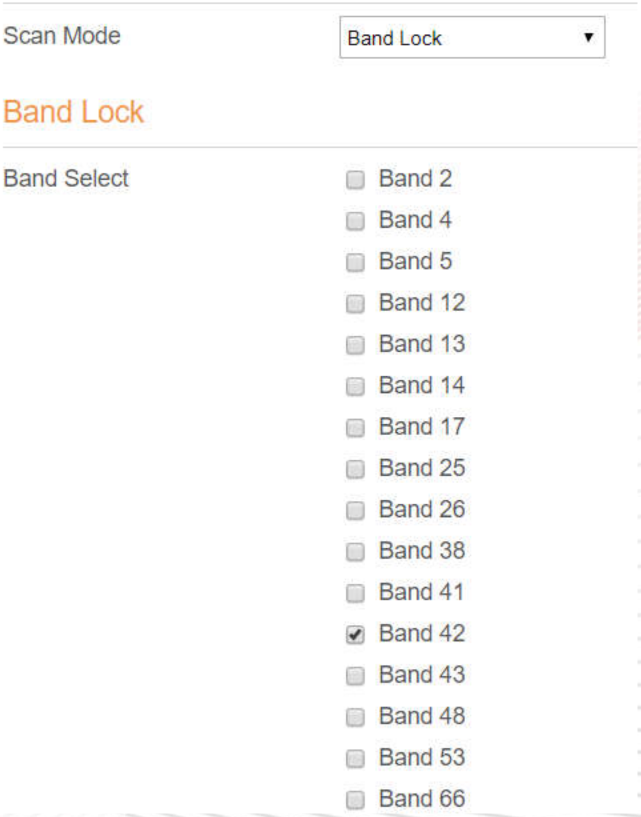
Figure 5-8

5.2.3 Scan Mode

This function is used to config UE mode of scan network. The default scan mode is fullband.

To set the LTE network scan mode, perform the following steps:

1. choose **Network>Scan mode**;
2. If select **Bandlock**, UE will only connect to the checked bands. Others will not be scanned.
3. Click **Submit**.



Scan Mode: Band Lock ▾

Band Lock

Band Select

☐ Band 2
☐ Band 4
☐ Band 5
☐ Band 12
☐ Band 13
☐ Band 14
☐ Band 17
☐ Band 25
☐ Band 26
☐ Band 38
☐ Band 41
☑ Band 42
☐ Band 43
☐ Band 48
☐ Band 53
☐ Band 66

Figure 5-9

Setting Frequency (Earfcn)

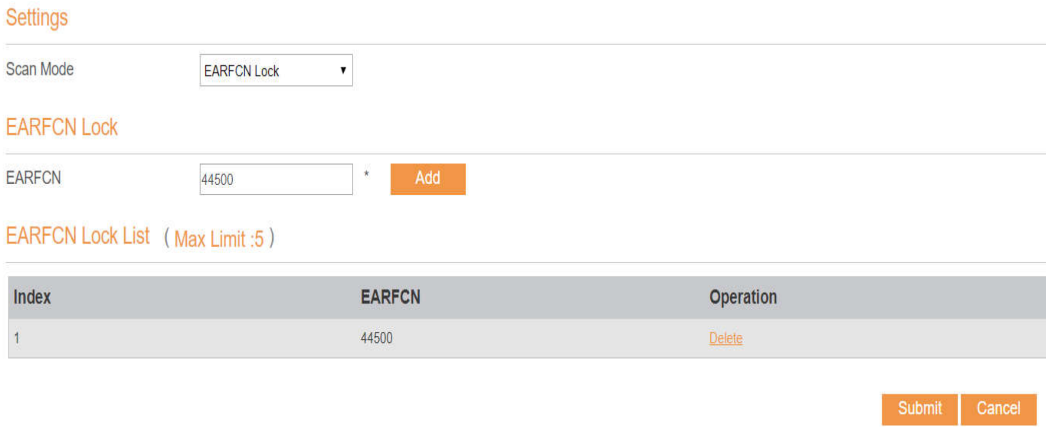
To set the frequency, perform the following steps:

1 Choose **Network**>**Scan Mode**.

2 In the **Scan Mode** area, choose **EARFCN Lock**.

3 In the **EARFCN Lock** area, you can set an **EARFCN**, then click **Add** to add it to the EARFCN lock list.

4 Click **Submit**. As shown in Figure 5-10.



Settings

Scan Mode: EARFCN Lock ▾

EARFCN Lock

EARFCN: 44500 *

EARFCN Lock List （Max Limit :5）

Index	EARFCN	Operation
1	44500	Delete

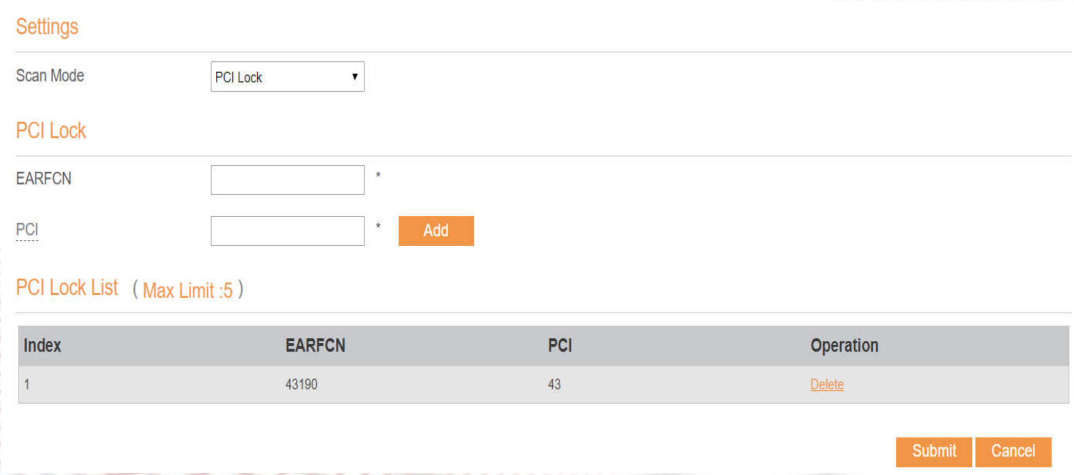
Figure 5-10

Setting PCI LOCK

To set the pci lock perform the following steps:

1. Choose **Network**>**Scan Mode**.
2. In the **Scan Mode** area, choose **PCI Lock**.

3. In the **PCI Lock** area, you can set **EARFCN** and **PCI** of the cell, then click **Add** to add it to the PCI lock list.
4. Click **Submit**. As shown in Figure 5-11.



Settings

Scan Mode: PCI Lock ▾

PCI Lock

EARFCN: *

PCI: * Add

PCI Lock List (Max Limit :5)

Index	EARFCN	PCI	Operation
1	43190	43	Delete

Submit Cancel

Figure 5-11

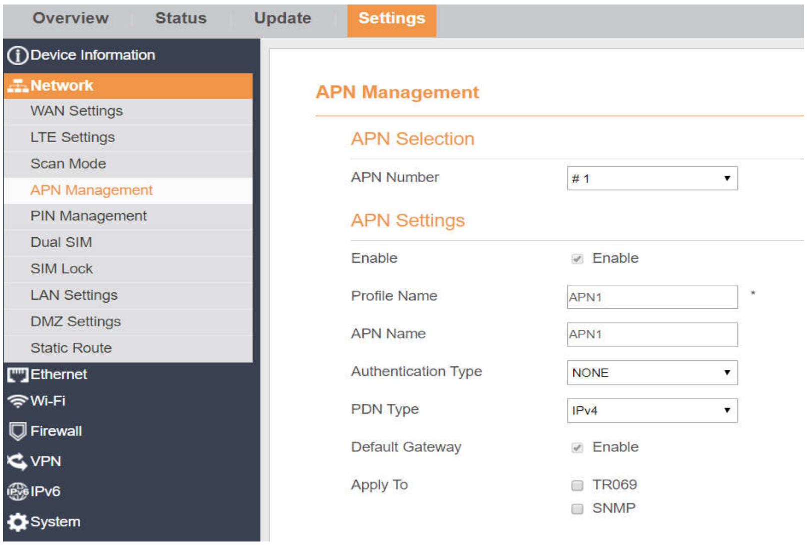
5.2.4 APN Management

To set and manage APN, perform the following steps:

1. Choose **Network**>**APN Management**.
2. In the **APN Management** area, you can set the APN.
3. Choose an **APN number** which you want to set, there are 4 APNs selected.
4. In the **APN Setting** area you can set the APN parameters, such as enable or disable the APN, APN name, profile name.
5. Set the authentication type (chap or pap or none) and the username, password of it.
6. Set the PDN type: IPv4 or IPv6 or IPv4/v6 dual stack.
7. Click **Submit.** As shown in Figure 5-12.

   If you want set an APN as **default gateway**, you should check that is enabled.

   And we can also set the APN apply to SNMP or TR069.



APN Management

APN Selection

APN Number: # 1 ▾

APN Settings

Enable: ☑ Enable

Profile Name: APN1 *

APN Name: APN1

Authentication Type: NONE ▾

PDN Type: IPv4 ▾

Default Gateway: ☑ Enable

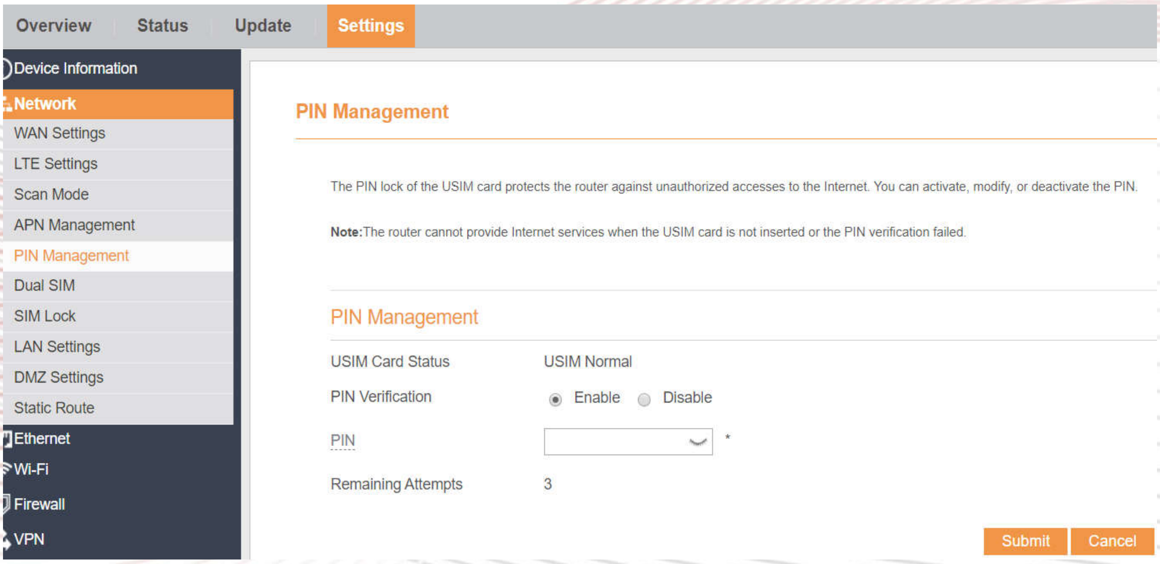
Apply To: ☐ TR069 ☐ SNMP

Figure 5-12

5.2.5 PIN Management

To manage the PIN, you can perform the following operations on the PIN Management page:

- Enable or disable the PIN verification.
- Verify the PIN.
- Change the PIN.
- Set automatic verification of the PIN. As shown in Figure 5-13



PIN Management

The PIN lock of the USIM card protects the router against unauthorized accesses to the Internet. You can activate, modify, or deactivate the PIN.

Note: The router cannot provide Internet services when the USIM card is not inserted or the PIN verification failed.

PIN Management

USIM Card Status USIM Normal

PIN Verification ● Enable ○ Disable

PIN *

Remaining Attempts 3

Figure 5-13

Viewing the Status of the USIM Card

To view the status of the USIM card, perform the following steps:

1. Choose **Network** >**PIN Management**.
2. View the status of the USIM card in the **USIM card status** field.

Enabling PIN Verification

To enable PIN verification, perform the following steps:

1. Choose **Network** >**PIN Management**.
2. Set **PIN verification** to **Enable**.
3. Enter the PIN (4 to 8 digits) in the **Enter PIN** box.
4. Click **Submit**.

Disabling PIN Verification

To disable PIN verification, perform the following steps:

1. Choose **Network** >**PIN Management**.
2. Set **PIN verification** to **Disable**.
3. Enter the PIN (4 to 8 digits) in the **Enter PIN** box.
4. Click **Submit**.

Verifying the PIN

If PIN verification is enabled but the PIN is not verified, the verification is required. To verify the PIN, perform the following steps:

1. Choose **Network** >**PIN Management**.

2 Enter the PIN (4 to 8 digits) in the **PIN** box.
3 Click **Submit**.

Changing the PIN

The PIN can be changed only when PIN verification is enabled and the PIN is verified.

To change the PIN, perform the following steps:

1 Choose **Network**>**PIN Management**.
2 Set PIN verification to **Enable**.
3 Set **Change PIN** to **Enable**.
4 Enter the current PIN (4 to 8 digits) in the **PIN** box.
5 Enter a new PIN (4 to 8 digits) in the **New PIN** box.
6 Repeat the new PIN in the **Confirm PIN** box.
7 Click **Submit**.

Setting Automatic Verification of the PIN

You can enable or disable automatic verification of the PIN. If automatic verification is enabled, the CPE automatically verifies the PIN after restarting. This function can be enabled only when PIN verification is enabled and the PIN is verified.

1 To enable automatic verification of the PIN, perform the following steps:
2 Choose **Network** > **PIN Management**.
3 Set Pin verification to Enable.
4 Set **Remember my PIN** to Enable.
5 Click Submit.

Verifying the PUK

If PIN verification is enabled and the PIN fails to be verified for three consecutive times, the PIN will be locked. In this case, you need to verify the PUK and change the PIN to unlock it.

To verify the PUK, perform the following steps:

1. Choose **Network**> **PIN Management**.

2. Enter the PUK in the **PUK** box.

3. Enter a new PIN in the New **PIN** box.

4. Repeat the new PIN in the **Confirm PIN** box.

Click **Submit**.

5.2.6 Dual SIM

If you have insert two SIM card in device, and want to exchange them. Please click here to switch them. As shown in Figure 5-14

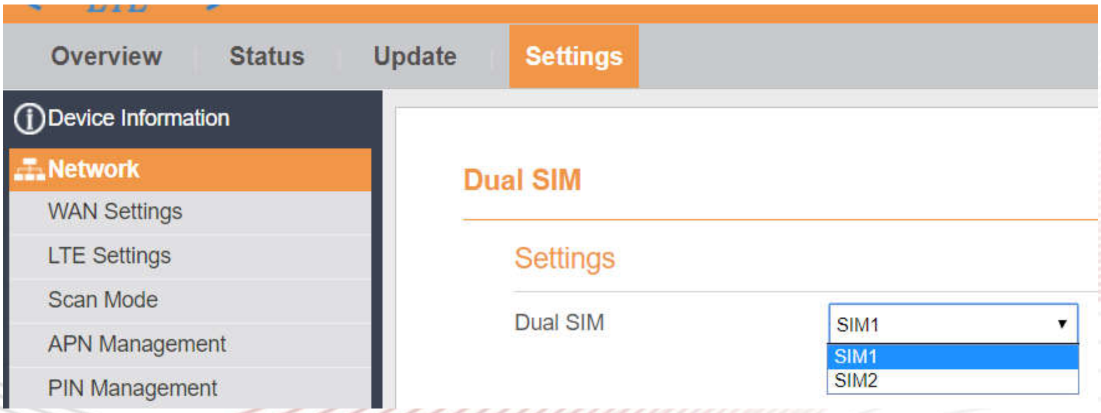


Figure 5-14

5.2.7 SIM Lock

If you want to connect a specify network, and the CPE can't connect other network, you can set a SIM lock.

To set the SIM lock, perform the following steps:

1. Choose **Network>SIM Lock.**
2. Input the PLMN you want to lock in the **PLMN** box.
3. Click **add** to add the PLMN in the lock list.
4. Click **Submit**. As shown in Figure 5-15.

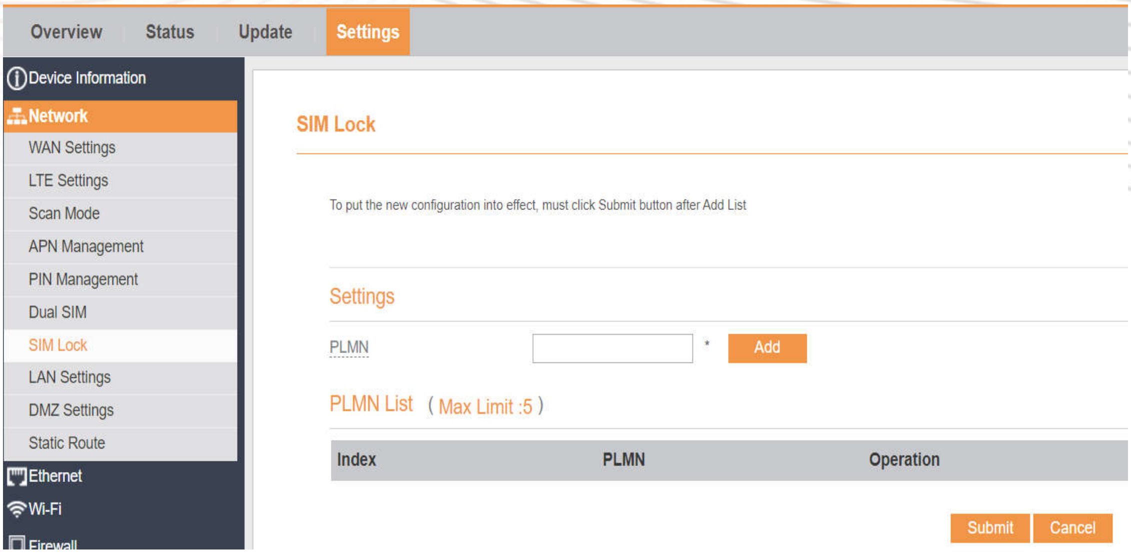


Figure 5-15

5.2.8 LAN Setting

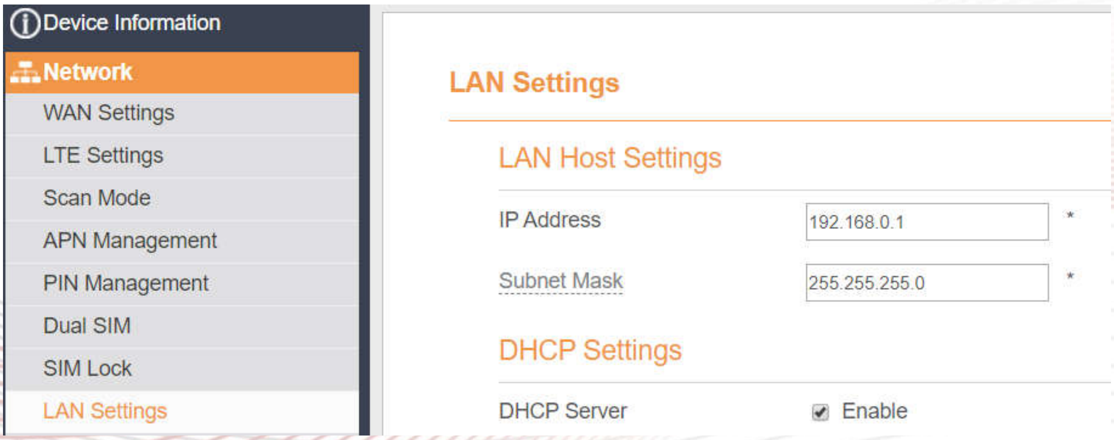
Setting LAN Host Parameters

By default, the IP address is 192.168.0.1 with a subnet mask of 255.255.255.0. You can change the host IP address to another individual IP address that is easy to remember. Make sure that IP address is unique on your network. If you change the IP address of the CPE, you need to access the web management page with the new IP address.

To change the IP address of the CPE, perform the following steps:

1. Choose **Network>LAN Settings**.
2. In the **LAN Host Settings** area, set IP address and subnet mask.

3. In the **DHCP Setting** area, set the DHCP server to **Enable**.
4. Click **Submit**. As shown in Figure 5-16.



LAN Settings

LAN Host Settings

IP Address: 192.168.0.1 *

Subnet Mask: 255.255.255.0 *

DHCP Settings

DHCP Server: ☑ Enable

Figure 5-16

Configuration the DHCP Server

DHCP enables individual clients to automatically obtain TCP/IP configuration when the server powers on. You can configure the CPE as a DHCP server or disable it. When configured as a DHCP server, the CPE automatically provides the TCP/IP configuration for the LAN clients that support DHCP client capabilities. If DHCP server services are disabled, you must have another DHCP server on your LAN, or each client must be manually configured.

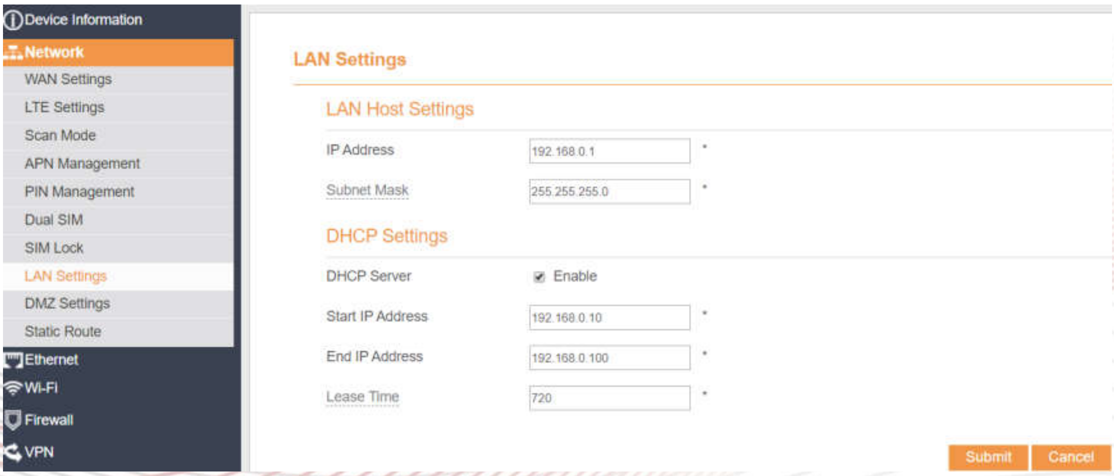
To configure DHCP settings, perform the following steps:

1. Choose **Network Setting** > **LAN Settings**.
2. Set the DHCP server to **Enable**.
3. Set **Start IP** address.

   This IP address must be different from the IP address set on the **LAN Host Settings** area, but they must be on the same network segment.
4. Set **End IP** address.

   This IP address must be different from the IP address set on the **LAN Host Settings** area, but they must be on the same network segment.
5. Set **Lease time**.

   Lease time can be set to 1 to 10,080 minutes. It is recommended to retain the default value.
6. Click **Submit**. As shown in Figure 5-17.



LAN Settings

LAN Host Settings

IP Address 192.168.0.1 *

Subnet Mask 255.255.255.0 *

DHCP Settings

DHCP Server ☑ Enable

Start IP Address 192.168.0.10 *

End IP Address 192.168.0.100 *

Lease Time 720 *

Figure 5-17

5.2.9 DMZ Settings

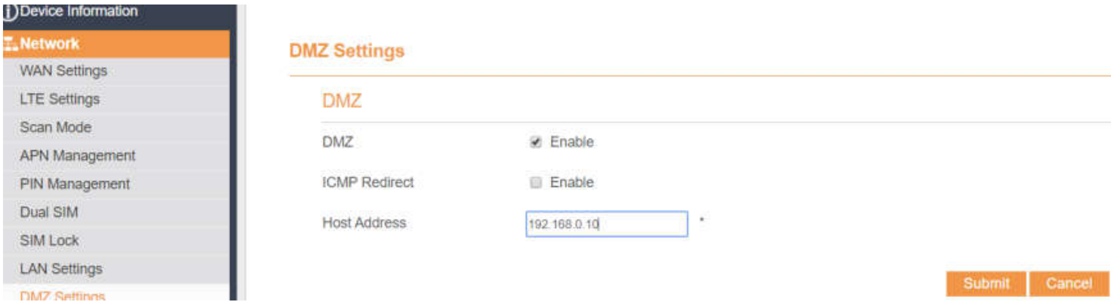
If the demilitarized zone (DMZ) is enabled, the packets sent from the WAN are directly sent to a specified IP address on the LAN before being discarded by the firewall.

To set DMZ, perform the following steps:

1. Choose **Network > DMZ Settings.**
2. Set DMZ to **Enable**.
3. (Optional) Set **ICMP Redirect** to **Enable**.
4. Set **Host address**.

   This IP address must be different from the IP address set on the **LAN Host Settings** page, but they must be on the same network segment.

5. Click **Submit**. As shown in Figure 5-18.



DMZ Settings

DMZ

DMZ ☑ Enable

ICMP Redirect □ Enable

Host Address 192.168.0.10 *

Figure 5-18

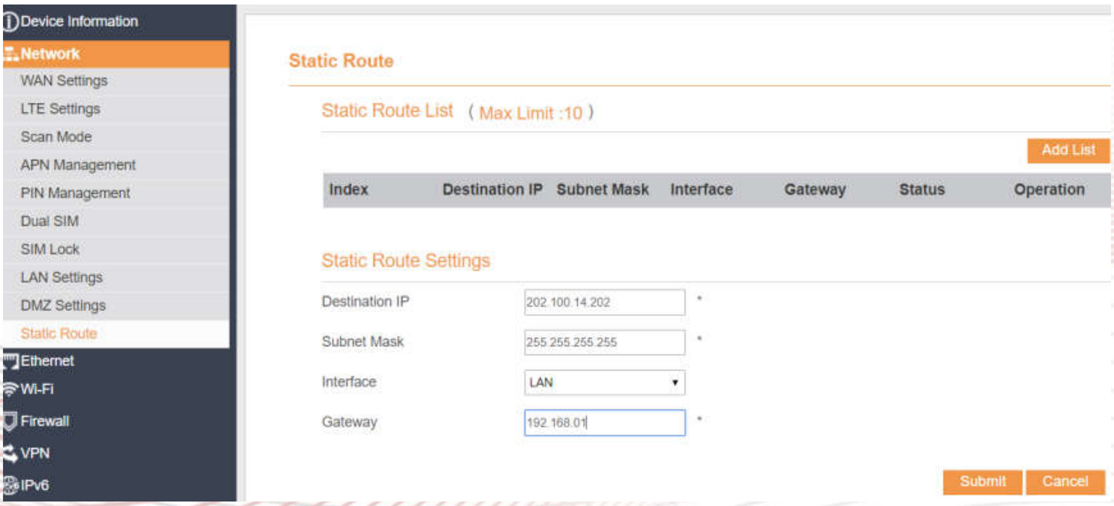
5.2.10 Static Route

Add Static Route

To add a static route, perform the following steps:

1. Choose **Network Setting>Static Route**.
2. Click **Add list**.
3. Set the **Dest IP address** and **Subnet mask**.
4. Select an **Interface** from the drop-down list.
5. If you select **LAN** as the interface, you need set a Gateway.

6. Click **Submit.** As shown in Figure 5-19.



Static Route

Static Route List （Max Limit :10）

Index	Destination IP	Subnet Mask	Interface	Gateway	Status	Operation

Static Route Settings

Destination IP: 202.100.14.202 *

Subnet Mask: 255.255.255.255 *

Interface: LAN

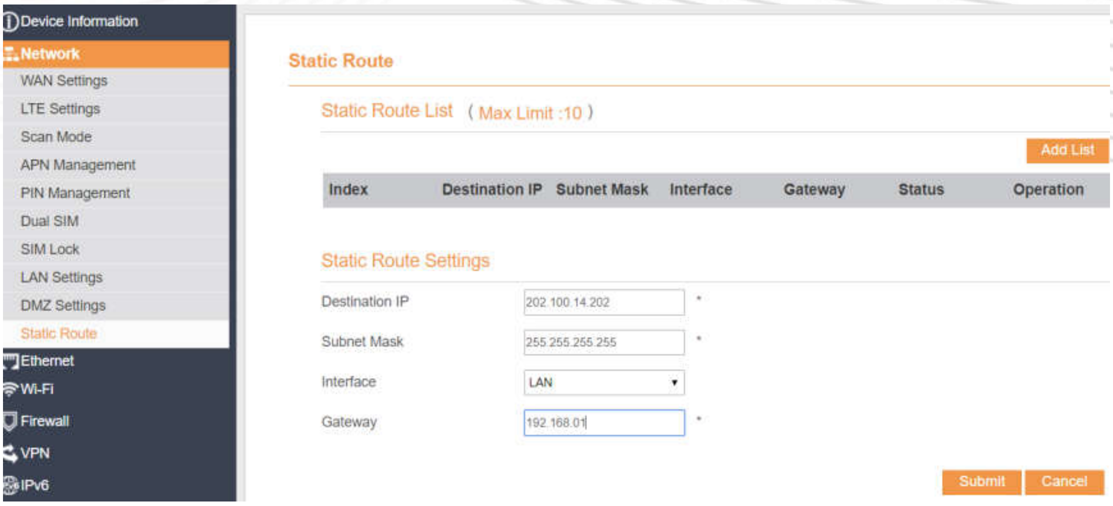
Gateway: 192.168.01 *

Figure 5-19

Modify Static Route

To modify an access restriction rule, perform the following steps:

1. Choose **Firewall**>**Static Route**.
2. Choose the item to be modified, and click **Edit**.
3. Repeat steps 3 through 5 in the previous procedure.
4. Click **Submit**. As shown in Figure 5-20.



Static Route

Static Route List （Max Limit :10）

Index	Destination IP	Subnet Mask	Interface	Gateway	Status	Operation

Static Route Settings

Destination IP: 202.100.14.202 *

Subnet Mask: 255.255.255.255 *

Interface: LAN

Gateway: 192.168.01 *

Figure 5-20

Delete Static Route

To delete a static route, perform the following steps:

1. Choose **Firewall**>**Static Route**.
2. Choose the item to be deleted, and click **Delete**.

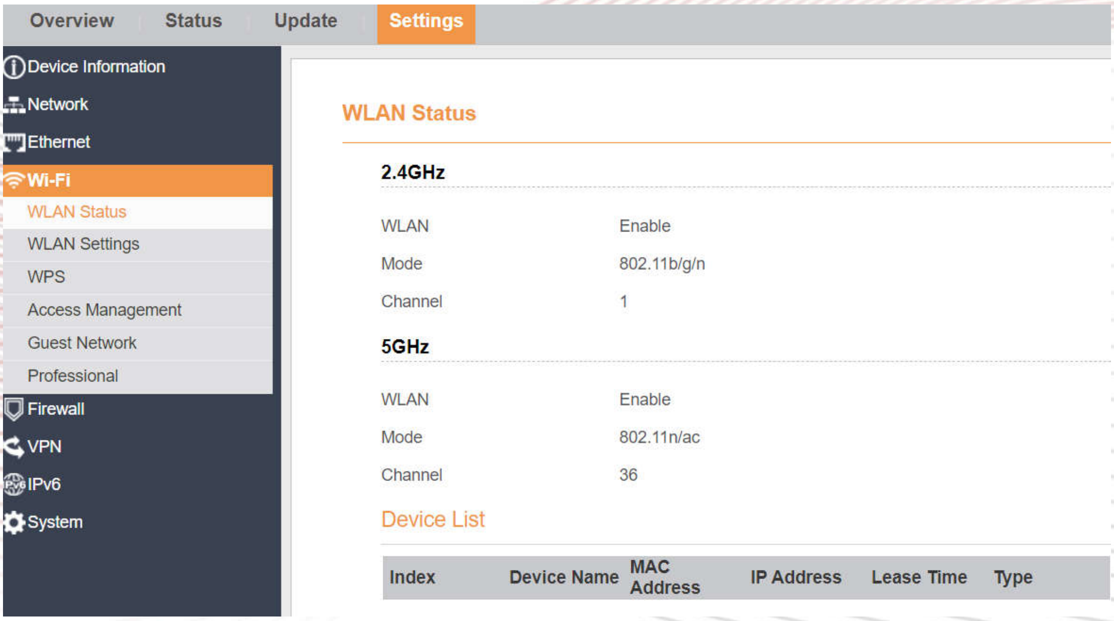
5.3 Wi-Fi

For SRP serial, SRP210 don’t support WIFI. SRP410-a and SRP410-b support 2.4G&5G dual band WIFI.

5.3.1 WLAN Status

To view the WLAN status, perform the following steps:

1. Choose **Wi-Fi**;
2. In the **WLAN Status** area, view the information about Wi-Fi status, 2.4G, 5G and Device list. As shown in Figure 5-22.



WLAN Status

2.4GHz

WLAN	Enable
Mode	802.11b/g/n
Channel	1

5GHz

WLAN	Enable
Mode	802.11n/ac
Channel	36

Device List

Index	Device Name	MAC Address	IP Address	Lease Time	Type

Figure 5-22

5.3.2 WLAN Settings

This function enables you to configure the Wi-Fi parameters.

Setting General Parameters

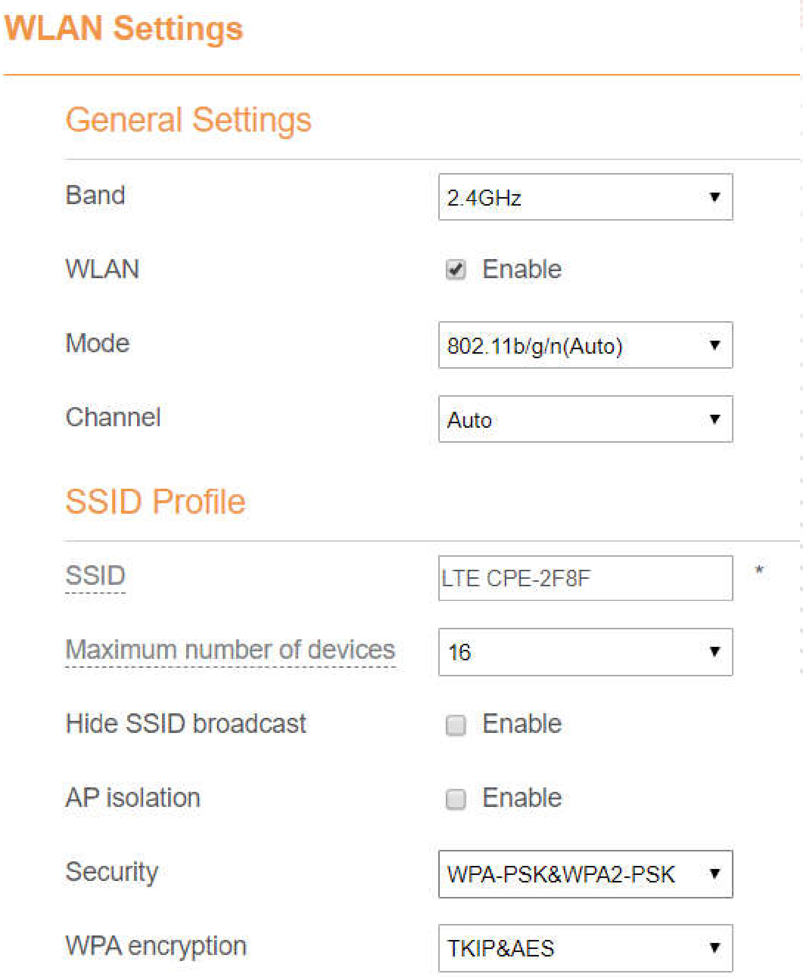
To configure the general Wi-Fi settings, perform the following steps:

1. Choose **Wi-Fi > Wi-Fi Settings**.
2. In the **General Settings** area, set WLAN to **Enable**.
3. Set **Mode** to one of the values described in the following table:

Parameter Value	Description
802.11 a/n/ac	The Wi-Fi client can connect to the CPE in 802.11a, 802.11n, or 802.11ac mode in 5G ISM frequency. If your device supports 802.11ac Protocol, we suggest to use 802.11ac protocol for better experience.
802.11b/g/n	The Wi-Fi client can connect to the CPE in 802.11b, 802.11g, or 802.11n mode. If the client connects to the CPE in 802.11n mode, the Advanced Encryption Standard (AES) encryption mode is required.
802.11b/g	The Wi-Fi client can connect to the CPE in

	802.11b or 802.11g mode.
802.11b	The Wi-Fi client can connect to the CPE in 802.11b mode.
802.11g	The Wi-Fi client can connect to the CPE in 802.11g mode.

4. Set the **Channel No.** 2.4G from 1 to 11, 5G from 40 to 165.
5. Click **Submit**. As shown in Figure 5-23.



WLAN Settings

General Settings

Band: 2.4GHz

WLAN: ☑ Enable

Mode: 802.11b/g/n(Auto)

Channel: Auto

SSID Profile

SSID: LTE CPE-2F8F *

Maximum number of devices: 16

Hide SSID broadcast: □ Enable

AP isolation: □ Enable

Security: WPA-PSK&WPA2-PSK

WPA encryption: TKIP&AES

Figure 5-23

Setting SSID Profile

After you configure the CPE on the **SSID Profile** page, the Wi-Fi client connects to the CPE based on preset rules, improving access Firewall.

To configure the CPE on the **SSID Profile** page, perform the following steps:

1. Choose **Wi-Fi** > **Wi-Fi Settings**.
2. Set **SSID**.

   The SSID can contain 1 to 32 ASCII characters. It cannot be empty and the last character cannot be a blank character. In addition, the SSID cannot contain the following special characters: / ' = " \ &

   The Wi-Fi client connects to the CPE using the found SSID.
3. Set **Maximum number of devices**.

   This parameter indicates the maximum number of Wi-Fi clients that connect to the CPE.

A maximum of 32 clients can connect to the CPE.

4. Set **Hide SSID broadcast** to **Enable**.

   If the SSID is hidden, the client cannot detect the CPE's Wi-Fi information.

5. Set **AP isolation** to **Enable**.

   The clients can connect to the CPE but cannot communicate with each other.

6. Set **Security**.

   If **Security** is set to **NONE (not recommended)**, Wi-Fi clients directly connect to the CPE. This Firewall level is low.

   If **Security** is set to **WEP**, Wi-Fi clients connect to the CPE in web-based encryption mode.

   If **Security** is set to **WPA-PSK**, Wi-Fi clients connect to the CPE in WPA-PSK encryption mode.

   If **Security** is set to **WPA2-PSK**, Wi-Fi clients connect to the CPE in WPA2-PSK encryption mode. This mode is recommended because it has a high Firewall level.

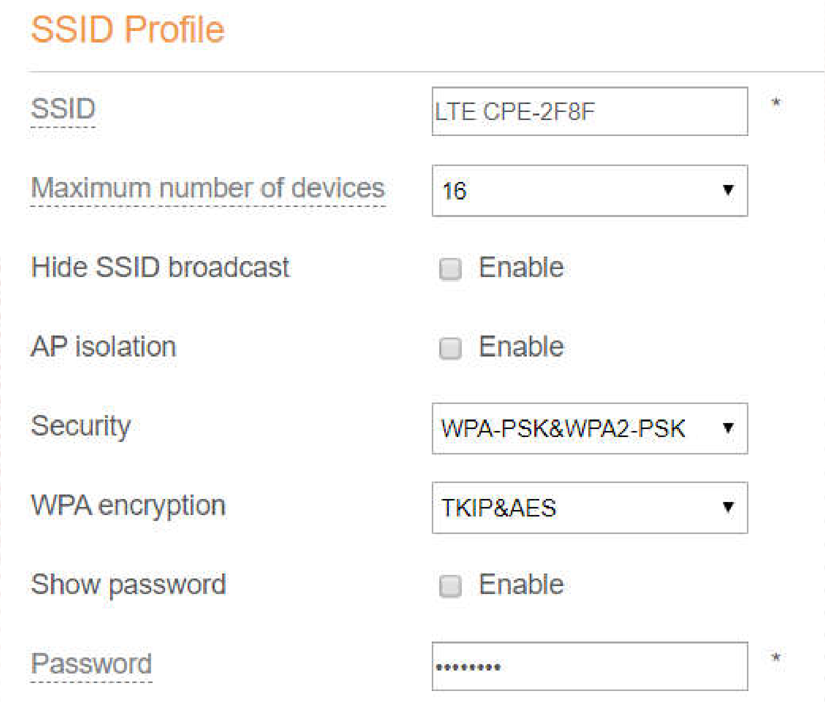
   If **Security** is set to **WPA-PSK & WPA2-PSK**, Wi-Fi clients connect to the CPE in WPA-PSK&WPA2-PSK encryption mode.

7. Set the encryption mode.

If…	Sets to	Description
WEP	Authentication mode	● **Shared authentication**: The client connects to the CPE in shared authentication mode. ● **Open authentication**: The client connects to the CPE in open authentication mode. ● **Both**: The client connects to the CPE in shared or open authentication mode.
	Encryption password length	● **128bit**: Only 13 ASCII characters or 26 hex characters can be entered in the **Key 1** to **Key 4** boxes. ● **64bit**: Only 5 ASCII characters or 10 hex characters can be entered in the **Key 1** to **Key 4** boxes.
	Current password index	This value can be set to **1**, **2**, **3**, or **4**. After a key index is selected, the corresponding key takes effect.
WPA-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.
WPA2-PSK(recommended)	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.
WPA-PSK & WPA2-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.

	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.

8. Click **Submit**. As shown in Figure 5-24.



SSID Profile

SSID	LTE CPE-2F8F *
Maximum number of devices	16
Hide SSID broadcast	□ Enable
AP isolation	□ Enable
Security	WPA-PSK&WPA2-PSK
WPA encryption	TKIP&AES
Show password	□ Enable
Password	•••••••• *

Figure 5-24

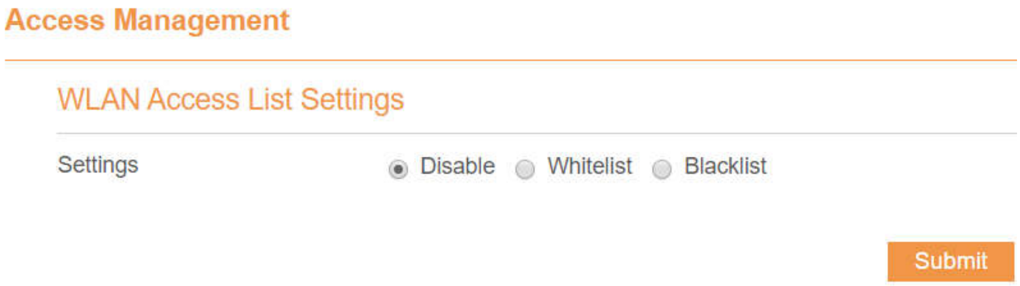
5.3.3 Access Management

Setting the Access Policy

This function enables you to set access restriction policies for each SSID to manage access to the CPE.

To configure Wi-Fi MAC control settings, perform the following steps:

1. Choose **Wi-Fi** > **Access Management**.
2. In the **WLAN Access List Settings** area, set Access Policy.
3. The access policy can be set to **Disable**, **Blacklist** or **Whitelist**.
   - If SSID's MAC Access is set to **Disable**, access restrictions do not take effect.
   - If SSID's MAC Access is set to **Blacklist**, only the devices that are not in the blacklist can connect to the CPE.
   - If SSID's MAC Access is set to **Whitelist**, only the devices in the whitelist can connect to the CPE.
4. Click **Submit**. As shown in Figure 5-25.



Access Management

WLAN Access List Settings

Settings ● Disable ○ Whitelist ○ Blacklist

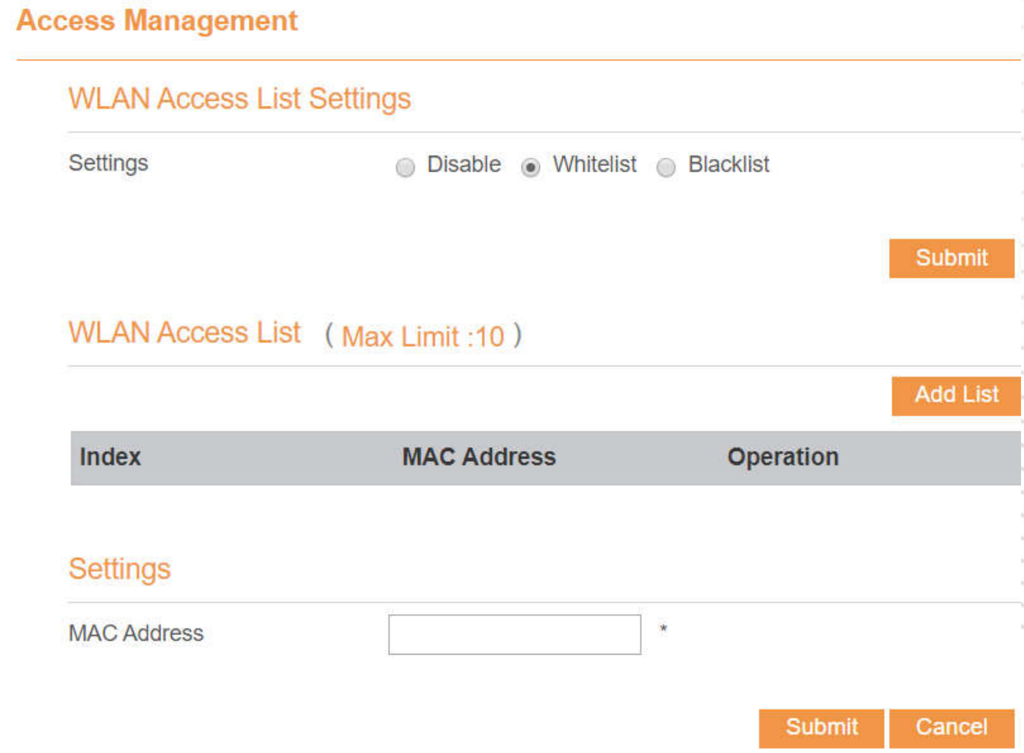
Figure 5-25

Managing the Wi-Fi Access List

This function enables you to set the SSID access policies based on MAC addresses.

To add an item to the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi** > **Access Management**.
2. Click **Add**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-26.



Access Management

WLAN Access List Settings

Settings ○ Disable ● Whitelist ○ Blacklist

WLAN Access List （Max Limit :10）

Index	MAC Address	Operation

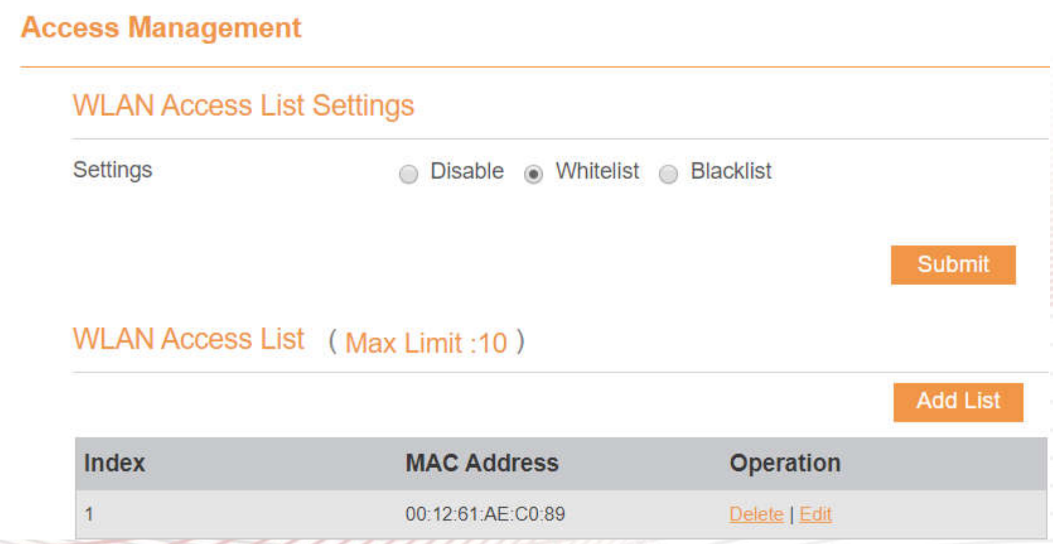
Settings

MAC Address ____ *

Figure 5-26

To modify an item in the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi** > **Access Management**.
2. Click **Edit MAC List**.
3. Choose the item to be modified, and click **Edit**.
4. Set MAC address.
5. Set one of the SSID to **Enable** to make the MAC address take effect for the SSID**.**
6. Click **Submit**. As shown in Figure 5-27.



Access Management

WLAN Access List Settings

Settings ○ Disable ● Whitelist ○ Blacklist

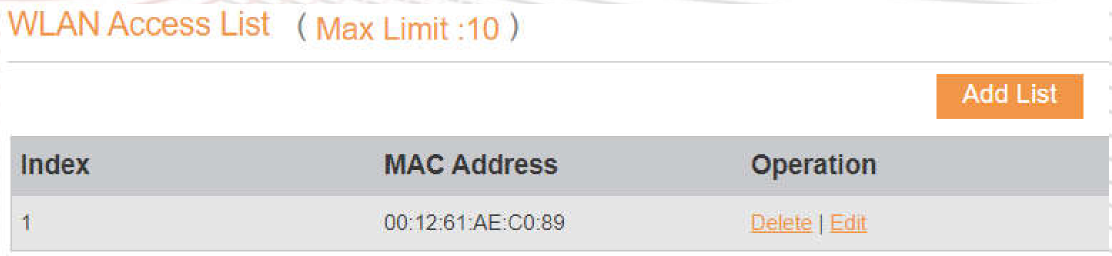
WLAN Access List （Max Limit :10）

Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete | Edit

Figure 5-27

To delete an item from the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi** > **Access Management**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-28.



WLAN Access List （Max Limit :10）

Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete | Edit

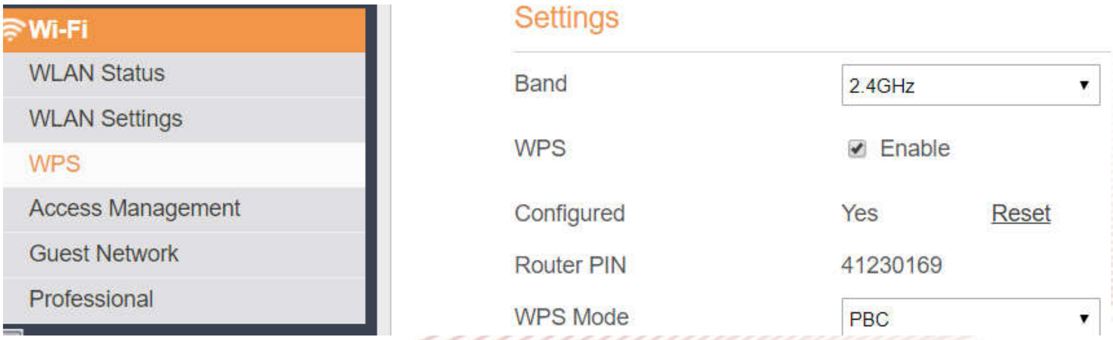
Figure 5-28

5.3.4 WPS Settings

Wi-Fi Protected Setup (WPS) enables you to simply add a wireless client to the network without needing to specifically configure the wireless settings, such as the SSID, Firewall mode and passphrase. You can use either the WPS button or PIN to add the wireless client.

To configure Wi-Fi WPS settings, perform the following steps:

1. Choose **Wi-Fi** > **WPS Settings**.
2. Set **WPS** to **Enable**.
3. Select WPS mode to PBC or router PIN as you want.
4. Click **Submit**. As shown in Figure 5-29.



Settings

Band: 2.4GHz ▼

WPS: ☑ Enable

Configured: Yes Reset

Router PIN: 41230169

WPS Mode: PBC ▼

Figure 5-69

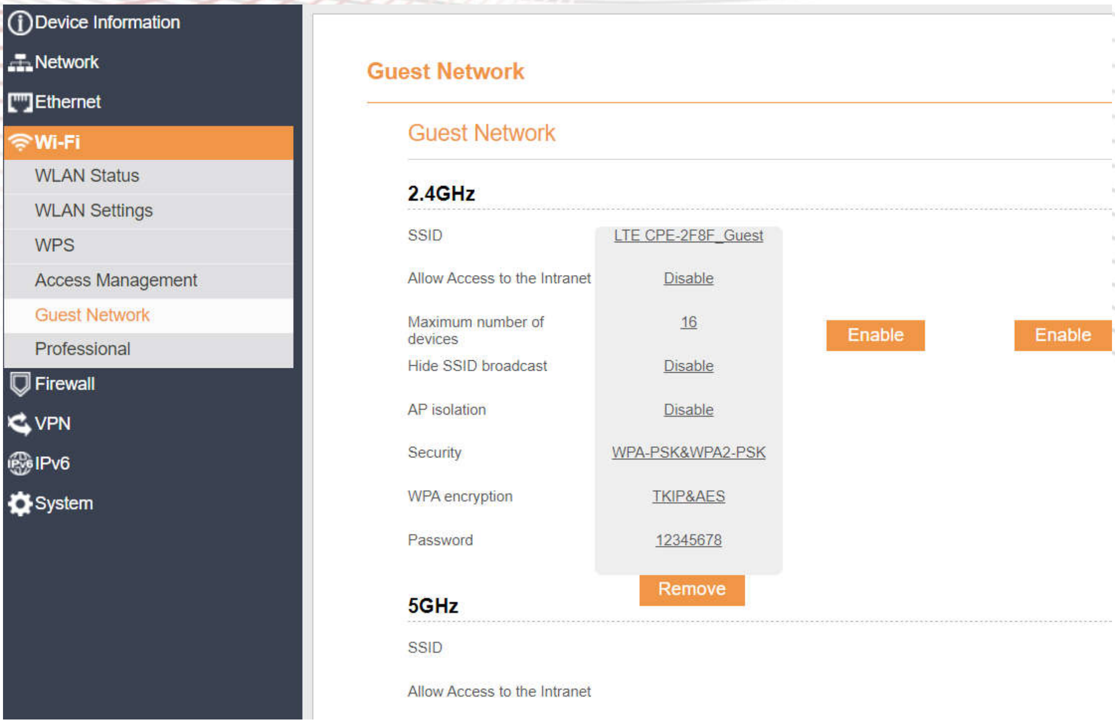
5.3.5 Guest Network

The function is to provide a wifi network for guests.

To configure the Guest Network, perform the following steps:

1.Choose **Wi-Fi > Guest Network**.

2.In the **Guest Network** area, set Guest network to **Enable**. As shown in Figure 5-30.



Guest Network

Guest Network

2.4GHz

SSID: LTE CPE-2F8F_Guest

Allow Access to the Intranet: Disable

Maximum number of devices: 16

Hide SSID broadcast: Disable

AP isolation: Disable

Security: WPA-PSK&WPA2-PSK

WPA encryption: TKIP&AES

Password: 12345678

5GHz

SSID

Allow Access to the Intranet

Figure 5-30

5.4 Firewall

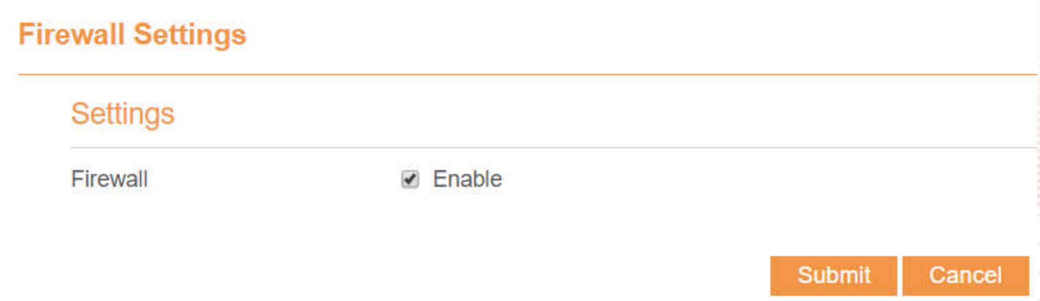
5.4.1 Setting Firewall

This page describes how to set the firewall. If you enable or disable the firewall, you can modify the configuration.

To set the firewall, perform the following steps:

1. Choose **Firewall**>**Firewall Setting**.

2. Choose **Enable** or **Disable** to modify the configuration.
3. Click **Submit**. As shown in Figure 5-31.



Firewall Settings

Settings

Firewall ☑ Enable

Figure 5-31

If you choose enable the firewall, you can modify the configuration about firewall, such as Mac filter, IP filter, URL filter and so on. If you choose disable, you can't modify any configurations about the firewall.

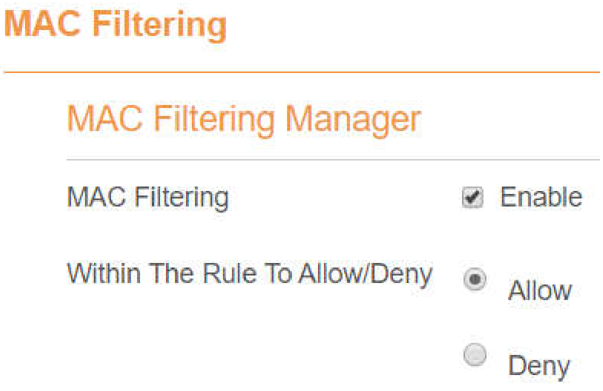
5.4.2 MAC Filtering

This page enables you to configure the MAC address filtering rules.

Enabling MAC Filter

To enable MAC address filter, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**
2. Set MAC filtering to **Enable**.
3. Click **Submit**. As shown in Figure 5-32.



MAC Filtering

MAC Filtering Manager

MAC Filtering ☑ Enable

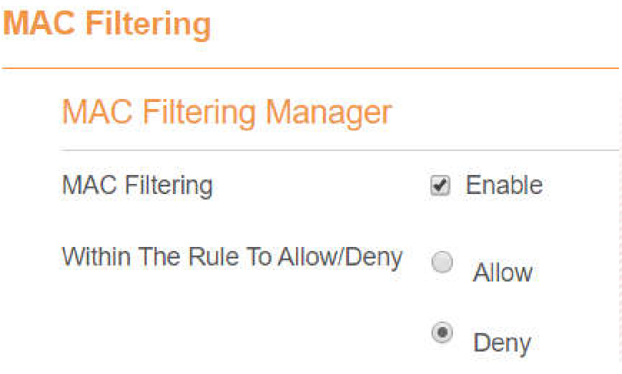
Within The Rule To Allow/Deny ● Allow ○ Deny

Figure 0-32

Disabling MAC Filter

To disable MAC address filter, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**
2. Set MAC filtering to **Disable**.
3. Click **Submit**. As shown in Figure 5-33.



MAC Filtering

MAC Filtering Manager

MAC Filtering ☑ Enable

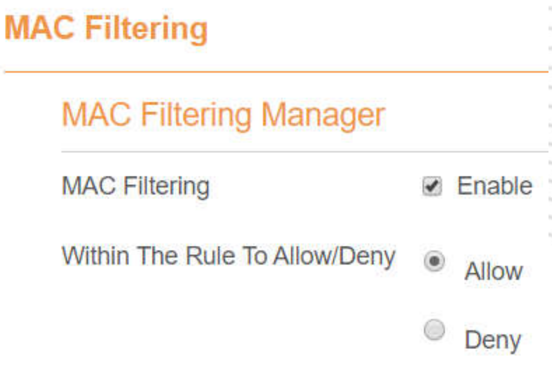
Within The Rule To Allow/Deny ○ Allow ● Deny

Figure 0-33

Setting Allow access network within the rules

To set allow access network within the rules, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**.
2. Set **Allow access network** within the rules.
3. Click **Submit**. As shown in Figure 5-34.



MAC Filtering

MAC Filtering Manager

MAC Filtering ☑ Enable

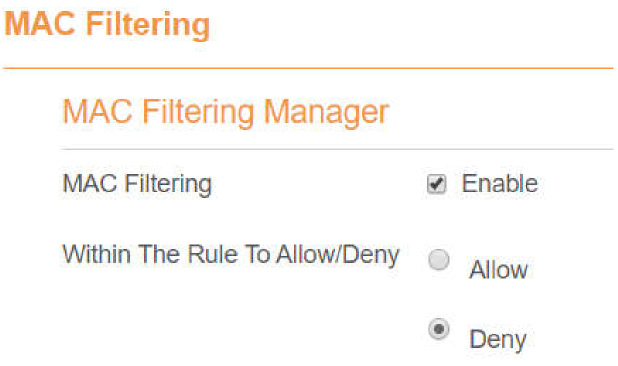
Within The Rule To Allow/Deny ● Allow ○ Deny

Figure 0-74

Setting Deny access network within the rules

To set deny access network within the rules, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**.
2. Set **Deny access network** within the rules.
3. Click **Submit**. As shown in Figure 5-35.



MAC Filtering

MAC Filtering Manager

MAC Filtering ☑ Enable

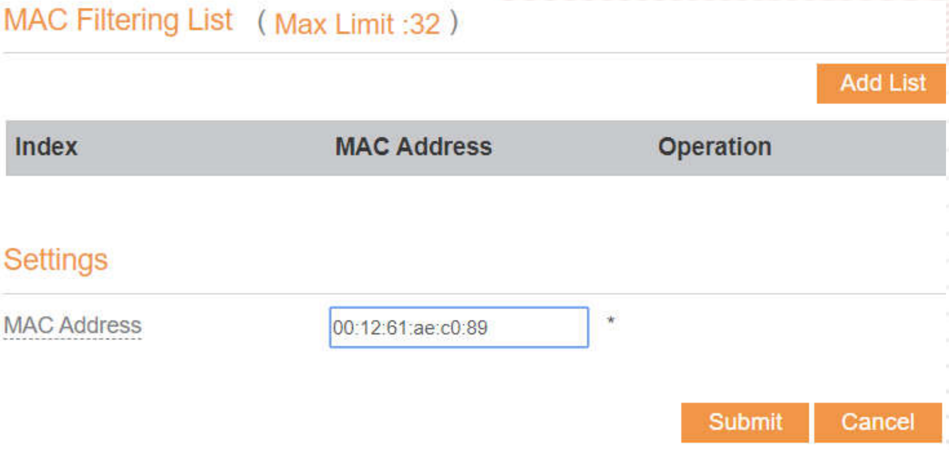
Within The Rule To Allow/Deny ○ Allow ● Deny

Figure 0-35

Adding MAC Filtering rule

To add a MAC filtering rule, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**.
2. Click **Add list**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-36.



MAC Filtering List （Max Limit :32）

Index	MAC Address	Operation

Settings

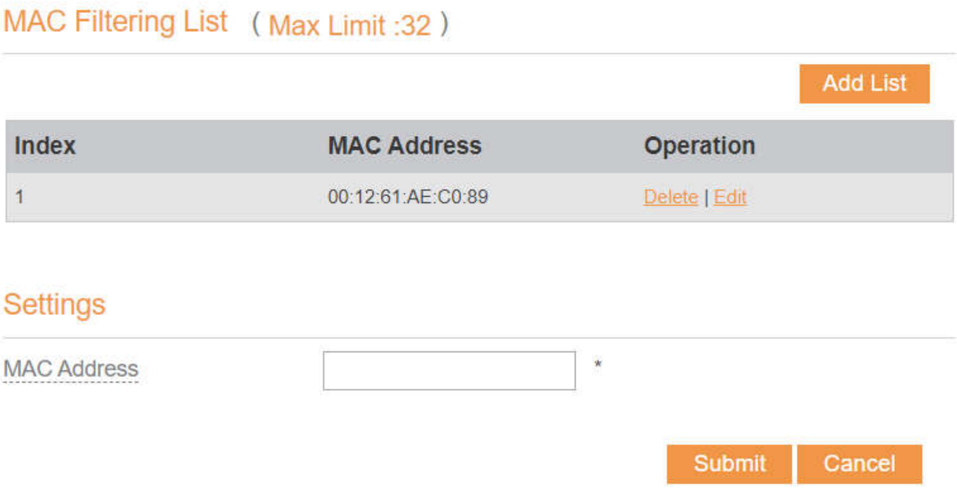
MAC Address: 00:12:61:ae:c0:89 *

Figure 0-36

Modifying MAC Filtering rule

To modify a MAC address rule, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-37.



MAC Filtering List （Max Limit :32）

Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete | Edit

Settings

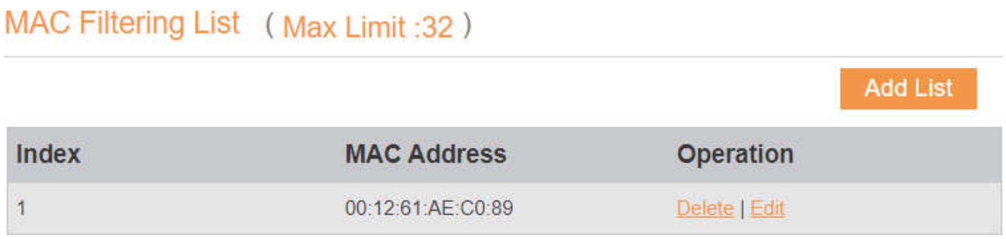
MAC Address: *

Figure 0-37

Deleting MAC Filtering rule

To delete a MAC address filter rule, perform the following steps:

1. Choose **Firewall**>**MAC Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-38.



MAC Filtering List （Max Limit :32）

Add List

Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete | Edit

Figure 0-38

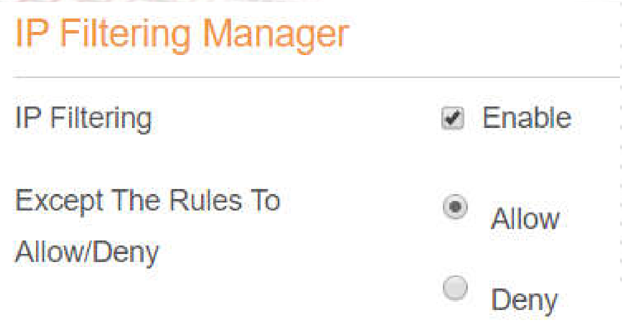
5.4.3 IP Filtering

Data is filtered by IP address. This page enables you to configure the IP address filtering rules.

Enabling IP Filtering

To enable IP Filtering, perform the following steps:

1. Choose **Firewall**>**IP Filtering**.
2. Set IP Filtering **Enable**.
3. Click **Submit**. As shown in Figure 5-39.



IP Filtering Manager

IP Filtering ☑ Enable

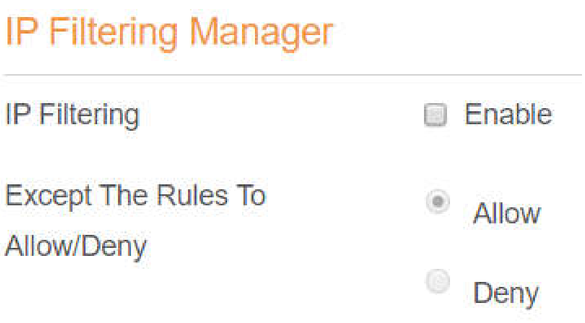
Except The Rules To Allow/Deny ● Allow ○ Deny

Figure 0-39

Disabling IP Filtering

To disable IP Filtering, perform the following steps:

1. Choose **Firewall**>**IP Filtering**.
2. Set IP Filtering **Disable**.
3. Click **Submit**. As shown in Figure 5-40.



IP Filtering Manager

IP Filtering □ Enable

Except The Rules To Allow/Deny ● Allow ○ Deny

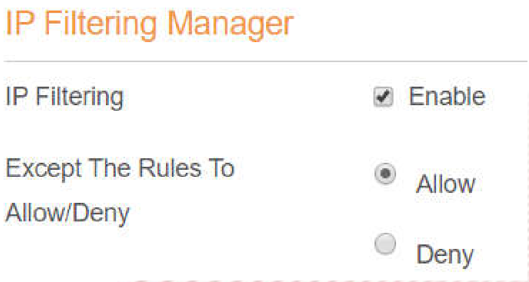
Figure 0-340

Setting Allow access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Firewall**>**IP Filtering**.
2. Set **Allow access network** outside the rules.

3. Click **Submit**. As shown in Figure 5-41.



IP Filtering Manager

IP Filtering ☑ Enable

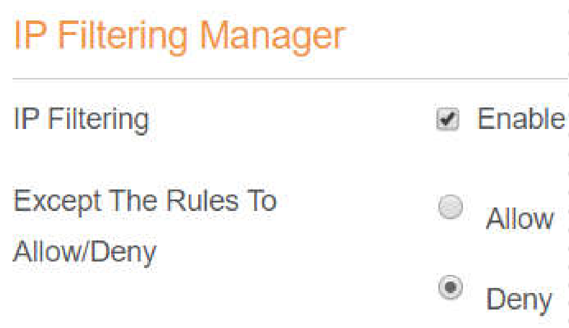
Except The Rules To Allow/Deny ● Allow ○ Deny

Figure 0-41

Setting Deny access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Firewall**>**IP Filtering**.
2. Set **Deny access network** outside the rules.
3. Click **Submit**. As shown in Figure 5-42.



IP Filtering Manager

IP Filtering ☑ Enable

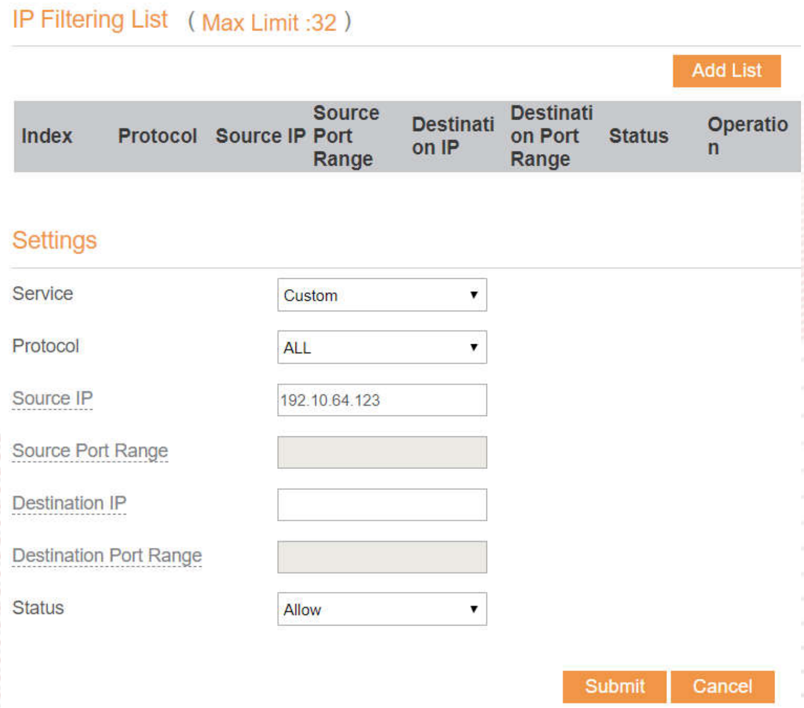
Except The Rules To Allow/Deny ○ Allow ● Deny

Figure 0-42

Adding IP Filtering rule

Add an IP address filtering rule, perform the following steps:

1. Choose **Firewall**>**IP Filtering**.
2. Click **Add list**.
3. Set **Service**.
4. Set **Protocol**.
5. In the **Source IP Address Range** box, enter the source IP address or IP address segment to be filtered.
6. In the **Source port range** box, enter the source port or port segment to be filtered.
7. In the **Destination IP Address Range** box, enter the destination IP address or IP address segment to be filtered.
8. In the **Destination port Range** box, enter the destination port or port segment to be filtered.
9. In the **Status** box, choose a status the rule will be executed.
10. Click **Submit**. As shown in Figure 5-43.



IP Filtering List (Max Limit :32)

Index	Protocol	Source IP	Source Port Range	Destination IP	Destination Port Range	Status	Operation

Settings

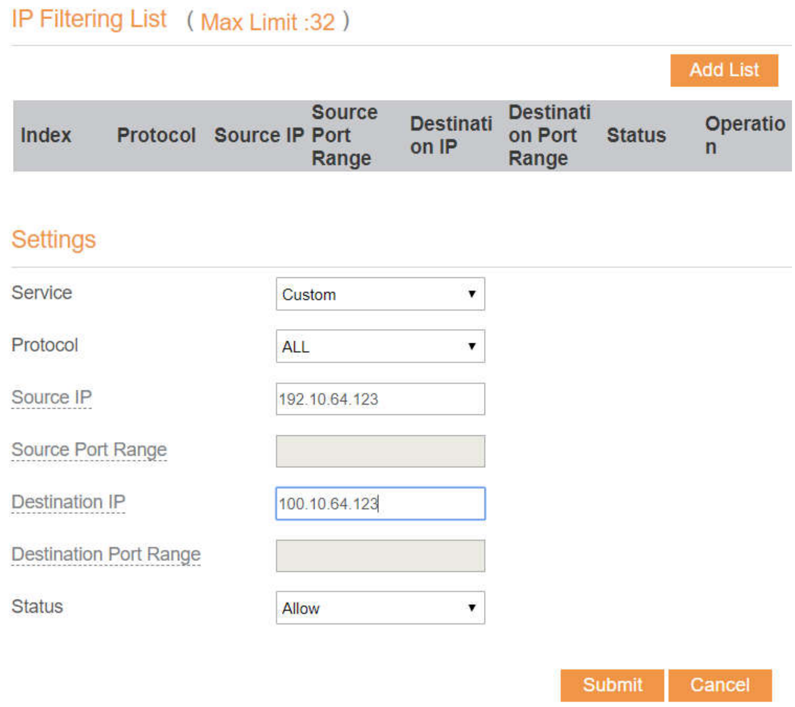
Service	Custom
Protocol	ALL
Source IP	192.10.64.123
Source Port Range	
Destination IP	
Destination Port Range	
Status	Allow

Figure 0-43

Modifying IP Filtering rule

To modify an IP filtering rule, perform the following steps:

1. Choose **Firewall > IP Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Repeat steps 3 through 9 in the previous procedure.
4. Click **Submit**. As shown in Figure 5-44.



IP Filtering List (Max Limit :32)

Index	Protocol	Source IP	Source Port Range	Destination IP	Destination Port Range	Status	Operation

Settings

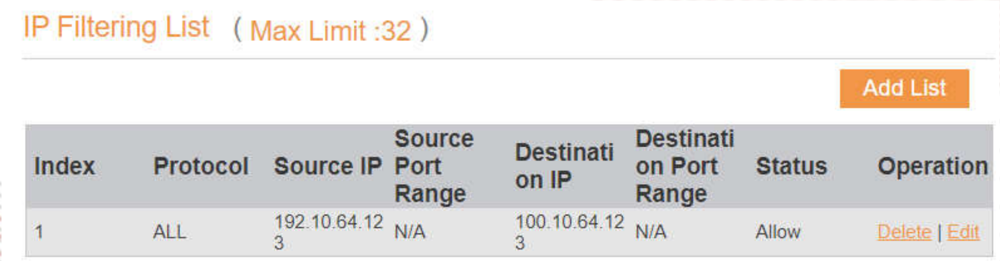
Service	Custom
Protocol	ALL
Source IP	192.10.64.123
Source Port Range	
Destination IP	100.10.64.123
Destination Port Range	
Status	Allow

Figure 0-44

Deleting IP Filtering rule

To delete an IP address filtering rule, perform the following steps:

1. Choose **Firewall > IP Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-45.



Index	Protocol	Source IP	Source Port Range	Destination IP	Destination Port Range	Status	Operation
1	ALL	192.10.64.123	N/A	100.10.64.123	N/A	Allow	Delete | Edit

Figure 0-45

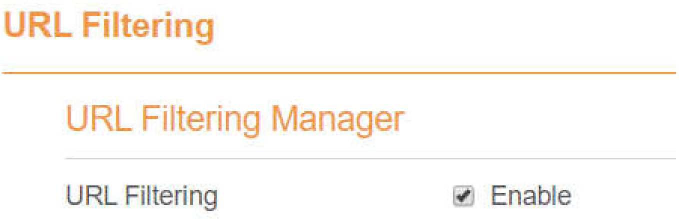
5.4.4 URL Filtering

Data is filtered by uniform resource locator (URL). This page enables you to configure URL filtering rules.

Enabling URL Filtering

To enable URL Filtering, perform the following steps:

1. Choose **Firewall**>**URL Filtering**.
2. Set **URL Filtering** to **Enable**.
3. Click **Submit**. As shown in Figure 5-46.



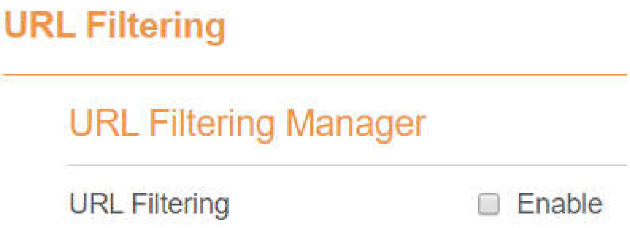
URL Filtering ☑ Enable

Figure 0-46

Disabling URL Filtering

To disable URL Filtering, perform the following steps:

1. Choose **Firewall**>**URL Filtering**.
2. Set **URL Filtering** to **Disable**.
3. Click **Submit**. As shown in Figure 5-47.



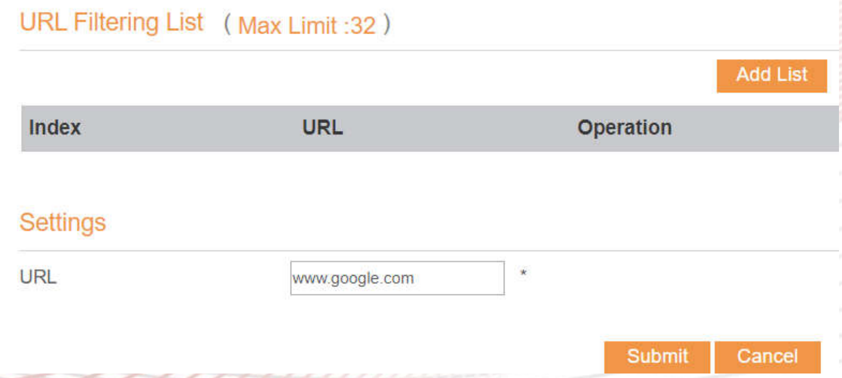
URL Filtering □ Enable

Figure 0-47

Adding URL Filtering list

To add an URL filtering list, perform the following steps:

1. Choose **Firewall**>**URL Filtering**.
2. Click **Add list**.
3. Set **URL**.
4. Click **Submit**. As shown in Figure 5-48.



Index	URL	Operation

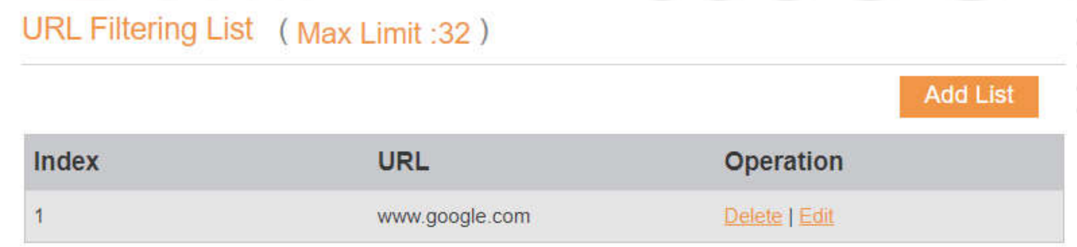
URL: www.google.com *

Figure 0-48

Modify URL Filtering list

To modify an URL filtering rule, perform the following steps:

1. Choose **Firewall**>**URL Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **URL** address.
4. Click **Submit**. As shown in Figure 5-49.



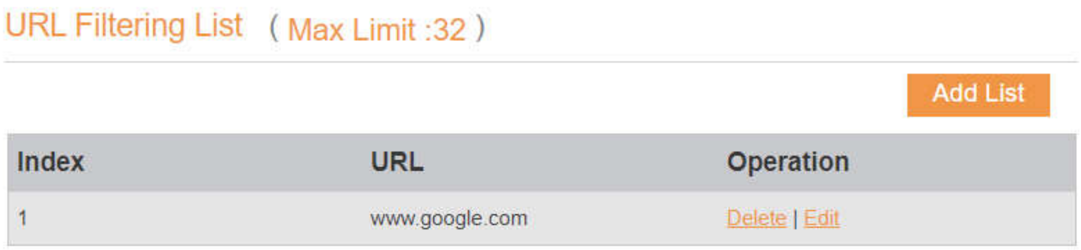
Index	URL	Operation
1	www.google.com	Delete | Edit

Figure 0-49

Deleting URL Filtering list

To delete an URL list, perform the following steps:

1. Choose **Firewall**>**URL Filtering**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-50.



Index	URL	Operation
1	www.google.com	Delete | Edit

Figure 0-50

5.4.5 Port Forwarding

When network address translation (NAT) is enabled on the CPE, only the IP address on the WAN side is open to the Internet. If a computer on the LAN is enabled to provide services for the Internet (for example, work as an FTP server), port forwarding is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN.

Adding Port Forwarding rule

To add a port forwarding rule, perform the following steps:

1. Choose **Firewall** > **Port Forwarding**.
2. Click **Add list**.
3. Set **Service**.
4. Set **Protocol**.
5. Set **Remote port range**.

   The port number ranges from 1 to 65535.

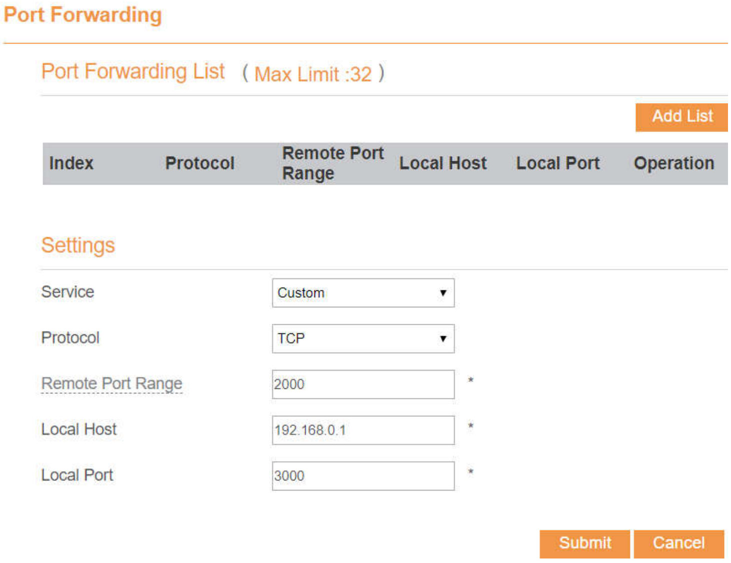
6. Set **Local host**.

   This IP address must be different from the IP address that is set on the **LAN Host Settings** page, but they must be on the same network segment.

7. Set **Local port**.

   The port number ranges from 1 to 65535.

8. Click **Submit**. As shown in Figure 5-50.



Port Forwarding

Port Forwarding List （Max Limit :32）

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation

Settings

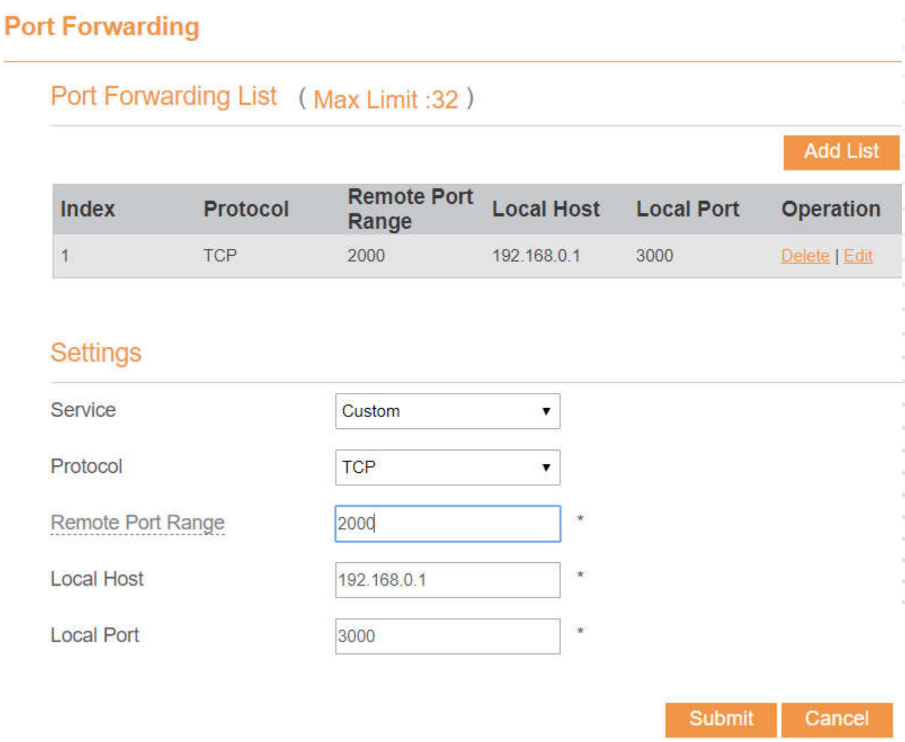
Service	Custom
Protocol	TCP
Remote Port Range	2000 *
Local Host	192.168.0.1 *
Local Port	3000 *

Figure 0-51

Modifying Port Forwarding rule

To modify a port forwarding rule, perform the following steps:

1. Choose **Firewall > Port Forwarding.**
2. Choose the item to be modified, and click **Edit**.
3. Re-config the service, protocol, and ports.
4. Click **Submit**. As shown in Figure 5-52.



Port Forwarding

Port Forwarding List (Max Limit :32)

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.0.1	3000	Delete | Edit

Settings

Service: Custom

Protocol: TCP

Remote Port Range: 2000 *

Local Host: 192.168.0.1 *

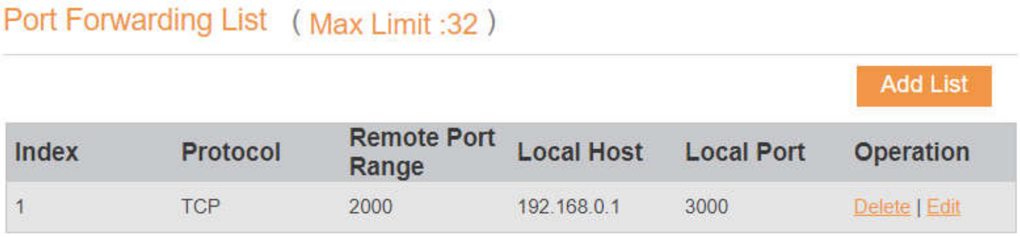
Local Port: 3000 *

Figure 0-52

Deleting Port Forwarding rule

To delete a port forwarding rule, perform the following steps:

1. Choose **Firewall > Port Forwarding.**
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-53.

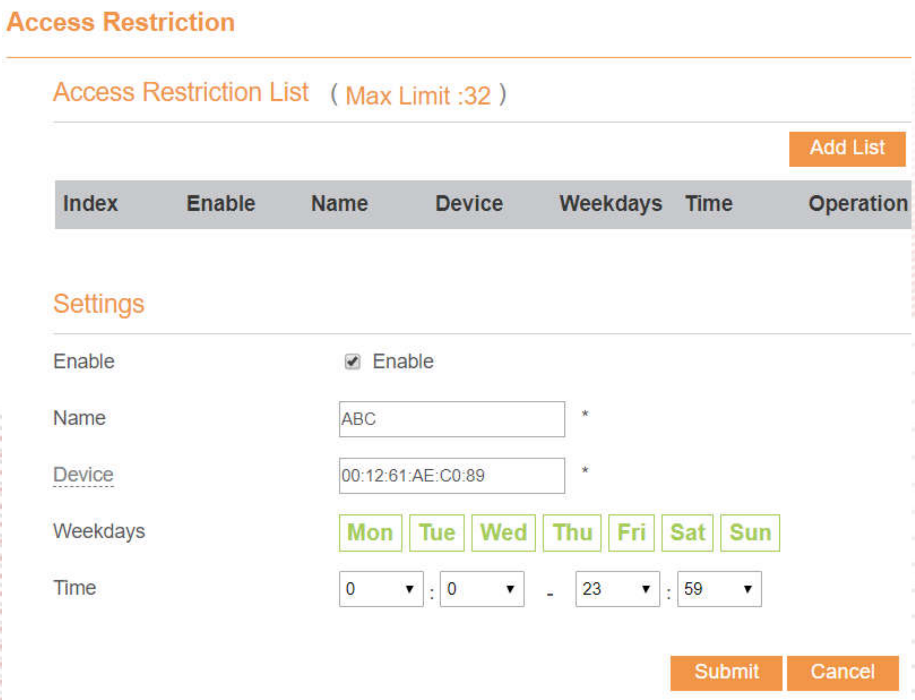


Port Forwarding List (Max Limit :32)

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.0.1	3000	Delete | Edit

Figure 0-53

5.4.6 Access Restriction



Access Restriction

Access Restriction List (Max Limit :32)

Add List

Index	Enable	Name	Device	Weekdays	Time	Operation

Settings

Enable	☑ Enable	
Name	ABC	*
Device	00:12:61:AE:C0:89	*
Weekdays	Mon Tue Wed Thu Fri Sat Sun	
Time	0 : 0 - 23 : 59	

Submit Cancel

Figure 5-54

Add Access Restriction

To add an access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.
2. Click **Add list**.
3. Set **Access Restriction** to **Enable**.
4. Set **Access Restriction Name**.
5. Set Device **MAC address** or **IP address**.
6. Set **Weekdays** and **time**.
7. Click **Submit**.

Modify Access Restriction

To modify an access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.
2. Choose the item to be modified, and click **Edit**.
3. Repeat steps 4 through 6 in the previous procedure.
4. Click **Submit**.

Delete Access Restriction

To delete a access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.

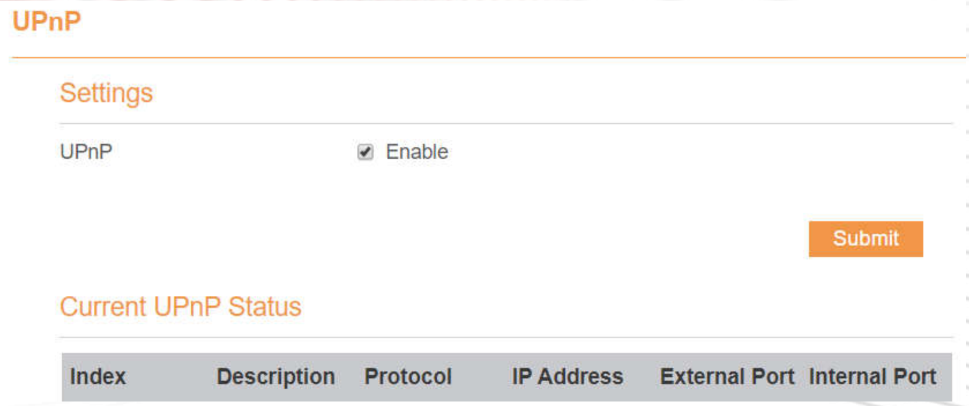
2. Choose the item to be deleted, and click **Delete**.

5.4.7 UPnP

On this page, you can enable or disable the Universal Plug and Play (UPnP) function.

To enable UPnP, perform the following steps:

1. Choose **Firewall > UPnP**.
2. Set **UPnP** to **Enable**.
3. Click **Submit**. As shown in Figure 5-55.



UPnP

Settings

UPnP ☑ Enable

Current UPnP Status

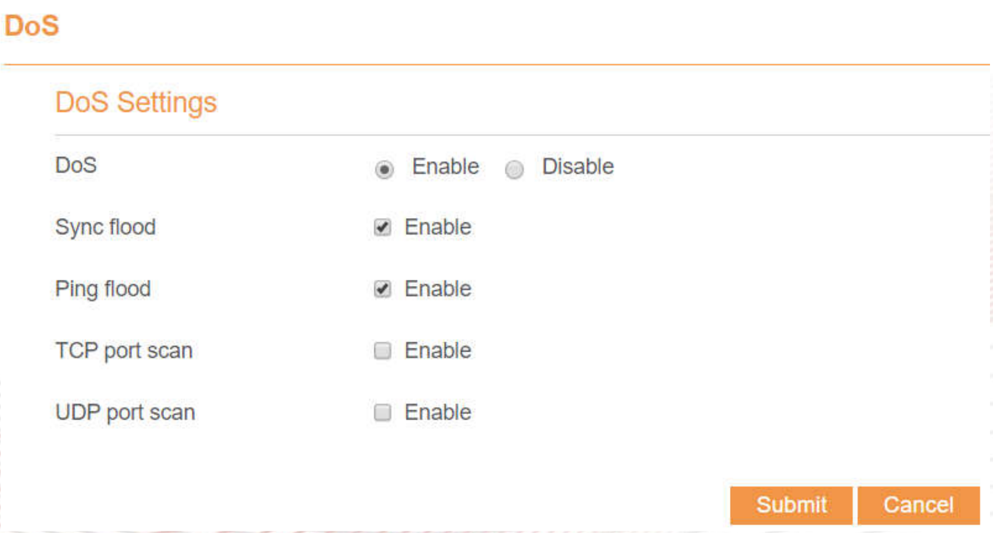
Index	Description	Protocol	IP Address	External Port	Internal Port

Figure 0-55

5.4.8 DoS

On this page, you can enable or disable the Denial of service (DoS) function.

1. Choose **Firewall > DoS**.
2. Set **UPnP** to **Enable**.
3. Click **Submit**. As shown in Figure 5-56.



DoS

DoS Settings

DoS ● Enable ○ Disable

Sync flood ☑ Enable

Ping flood ☑ Enable

TCP port scan □ Enable

UDP port scan □ Enable

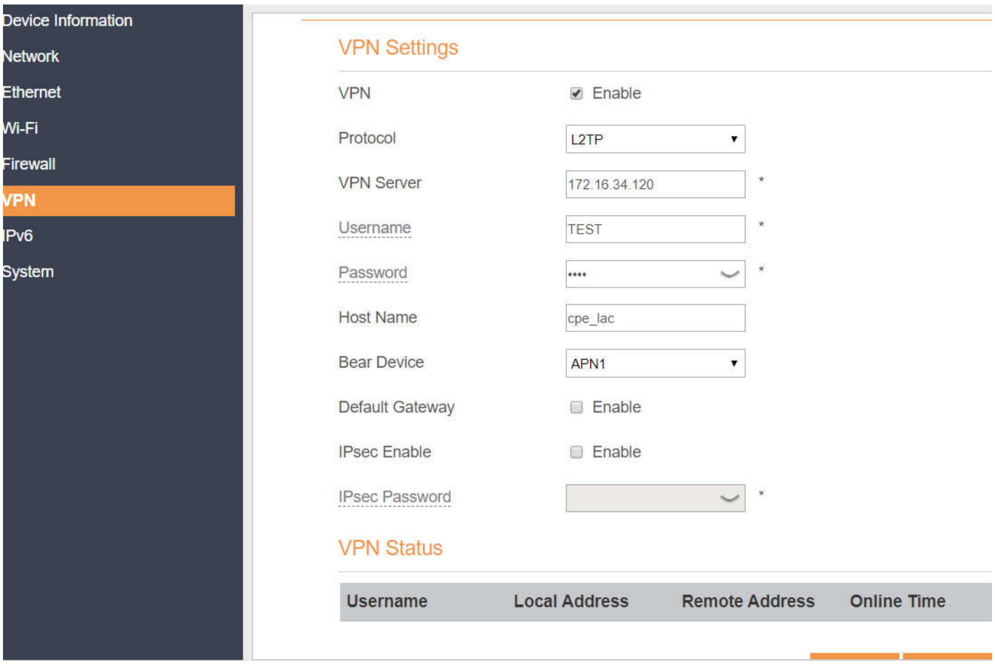
Figure 0-86

5.5 VPN

This function enables you to connect the virtual private network (VPN).

To connect the VPN, perform the following steps:

1. Choose **VPN.**
2. In the **VPN Settings** area, enable VPN.
3. Select a protocol from **Protocol** drop-down list.
4. Enter **Username** and **Password**.
5. Click **Submit**.
6. You can view the status in **VPN Status** area. As shown in Figure 5-57.



VPN Settings

VPN ☑ Enable

Protocol L2TP

VPN Server 172.16.34.120 *

Username TEST *

Password •••• *

Host Name cpe_lac

Bear Device APN1

Default Gateway □ Enable

IPsec Enable □ Enable

IPsec Password *

VPN Status

Username	Local Address	Remote Address	Online Time

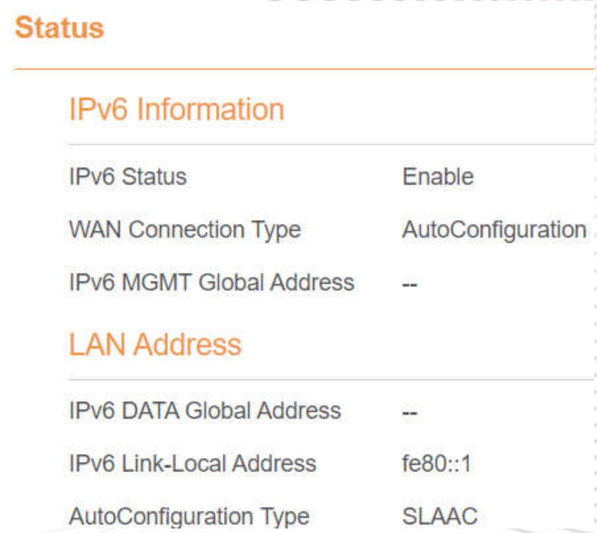
Figure 5-57

5.6 IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). Every device on the Internet is assigned an unique IP address for identification and location definition.

5.6.1 Status

The status page shows IPv6 information. As shown in Figure 5-58.



Status

IPv6 Information

IPv6 Status	Enable
WAN Connection Type	AutoConfiguration
IPv6 MGMT Global Address	--

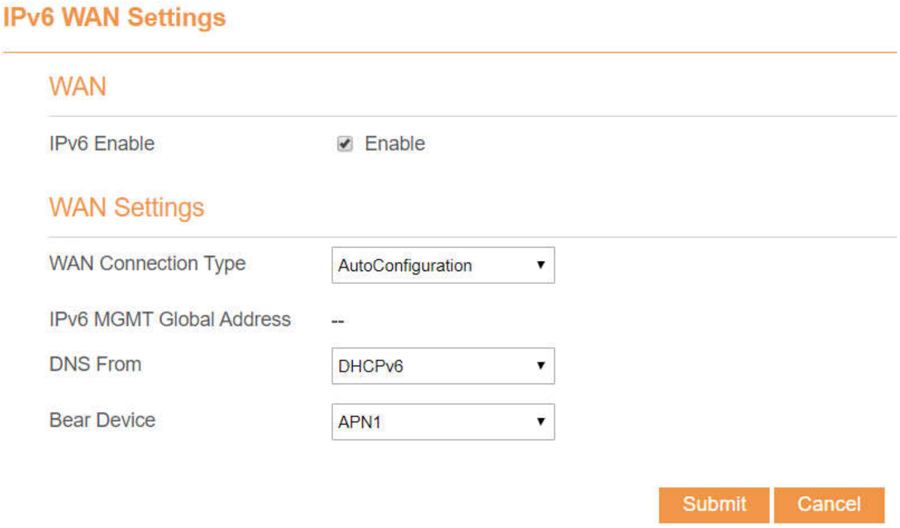
LAN Address

IPv6 DATA Global Address	--
IPv6 Link-Local Address	fe80::1
AutoConfiguration Type	SLAAC

Figure 5-58

5.6.2 IPv6 WAN Settings

In this page, user can enable or disable IPv6 function. Meanwhile, user can set WAN Connection Type and the type of DNS.As shown in Figure 5-59



IPv6 WAN Settings

WAN

IPv6 Enable	☑ Enable

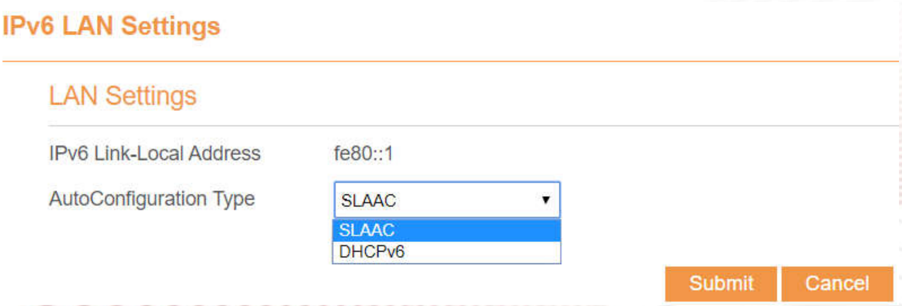
WAN Settings

WAN Connection Type	AutoConfiguration ▾
IPv6 MGMT Global Address	--
DNS From	DHCPv6 ▾
Bear Device	APN1 ▾

Figure 5-59

5.6.3 IPv6 LAN Settings

In this page, user can choose the Auto Configuration Type. As shown in Figure 5-60.



IPv6 LAN Settings

LAN Settings

IPv6 Link-Local Address fe80::1

AutoConfiguration Type SLAAC

Figure 5-60

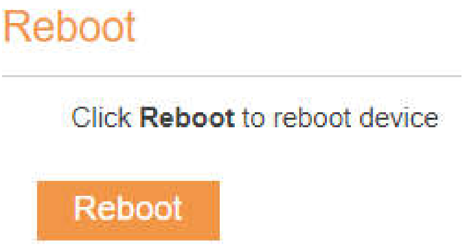
5.7 System

5.7.1 Maintenance

Reboot

This function enables you to restart the CPE. Settings take effect only after the CPE restarts. To restart the CPE, perform the following steps:

1. Choose **System**>**Maintenance**.
2. Click **Reboot**. As shown in Figure 5-61.
   The CPE then restarts.



Reboot

Click **Reboot** to reboot device

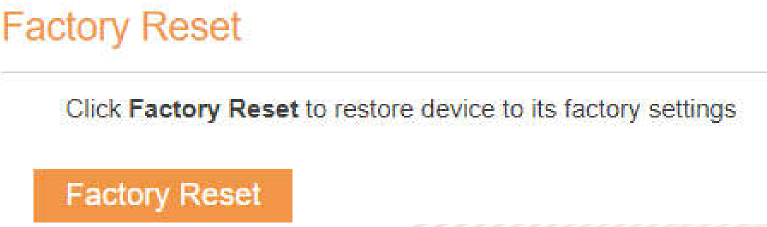
Figure 5-61

Reset

This function enables you to restore the CPE to its default settings.

To restore the CPE, perform the following steps:

1. Choose **System**>**Maintenance**.
2. Click **Factory Reset.** As shown in Figure 5-62.
   The CPE is then restored to its default settings.


Factory Reset

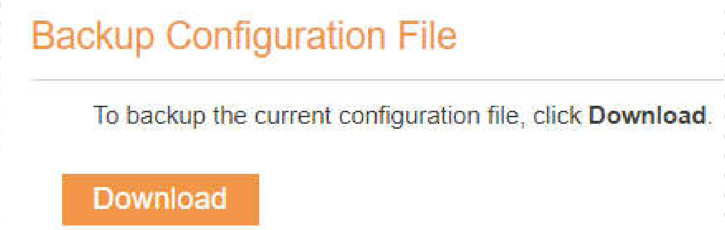
Click **Factory Reset** to restore device to its factory settings

Figure 5-62

Backup Configuration File

You can download the existing configuration file to back it up. To do so:

1. Choose **System**>**Maintenance**.
2. Click **Download** on the **Maintenance** page.
3. In the displayed dialog box, select the save path and name of the configuration file to be backed up.
4. Click **Save**. As shown in Figure 5-63.
   The procedure for file downloading may vary with the browser you are using.


Backup Configuration File

To backup the current configuration file, click **Download**.

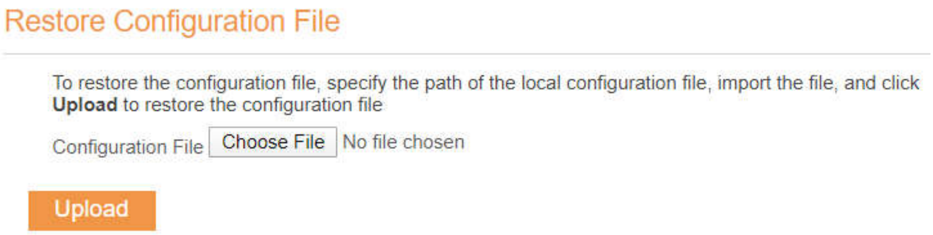
Figure 5-63

Upload Configuration File

You can upload a backed-up configuration file to restore the CPE. To do so:

1. Choose **System**>**Maintenance**.
2. Click **Browse** on the **Maintenance** page.
3. In the displayed dialog box, select the backed-up configuration file.
4. Click **Open**.
5. The dialog box chooses. In the box to be right of Configuration file, the save path and name of the backed-up configuration file are displayed.
6. Click **Upload**. As shown in Figure 5-64.

The CPE uploads the backed-up configuration file. The CPE then automatically restarts.


Restore Configuration File

To restore the configuration file, specify the path of the local configuration file, import the file, and click **Upload** to restore the configuration file

Configuration File Choose File No file chosen

Figure 5-64

5.7.2 TR069

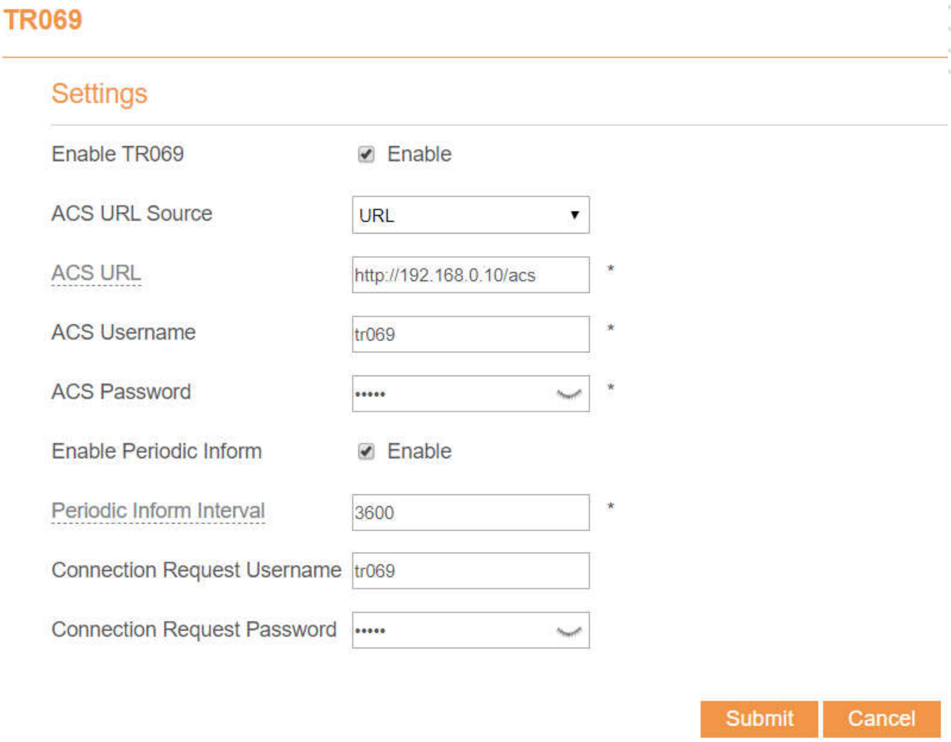
TR-069 is a standard for communication between CPEs and the auto-configuration server (ACS). If your service provider uses the TR069 automatic service provision function, the ACS automatically provides the CPE parameters. If you set the ACS parameters on both the CPE and ACS, the network parameters on the CPE are automatically set using the TR-069 function, and you do not need to set other parameters on the CPE.

To configure the CPE to implement the TR-069 function, perform the following steps:

1. Choose **System**>**TR069**.
2. Set **acs URL source**. There are two methods, such as **URL** and **DHCP**.
3. In the **ACS URL** box, enter the **ACS URL** address.
4. Enter ACS **user name** and **password** for the CPE authentication.

> To use the CPE to access the ACS, you must provide a user name and password for authentication. The user name and the password must be the same as those defined on the ACS.

5. If you set **Periodic inform** to **Enable**, set **Periodic inform interval**.
6. Set **connection request user name** and **password**.
7. Click **Submit**. As shown in Figure 5-65.



TR069

Settings

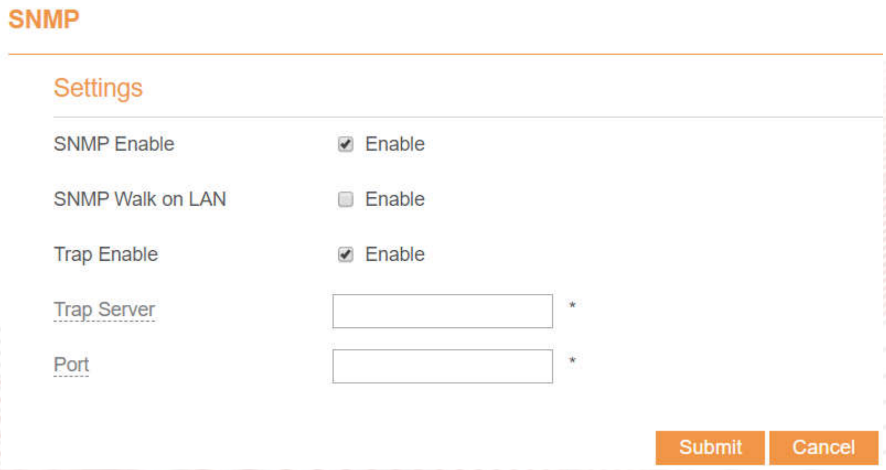
Enable TR069	☑ Enable
ACS URL Source	URL ▾
ACS URL	http://192.168.0.10/acs *
ACS Username	tr069 *
ACS Password	••••• *
Enable Periodic Inform	☑ Enable
Periodic Inform Interval	3600 *
Connection Request Username	tr069
Connection Request Password	•••••

Figure 5-65

5.7.3 SNMP

You can enable SNMP and set config SNMP trap.

The UE will actively report changes of some certain values to the SNMP server.



SNMP

Settings

SNMP Enable ☑ Enable

SNMP Walk on LAN □ Enable

Trap Enable ☑ Enable

Trap Server ____ *

Port ____ *

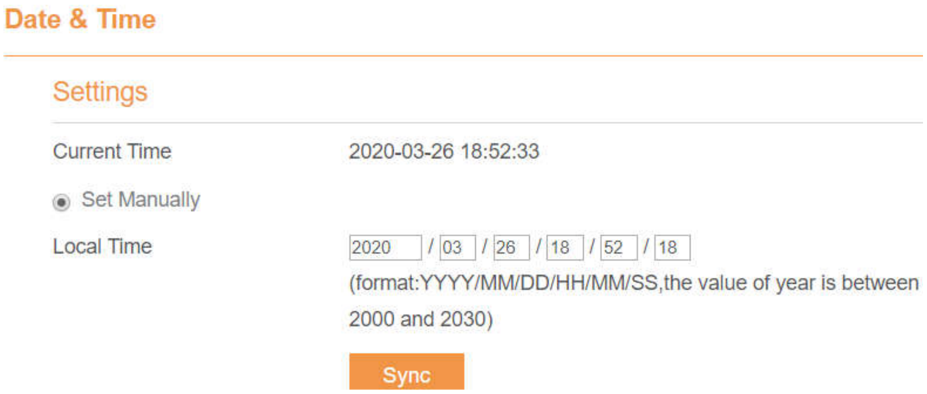
Figure 5-66

5.7.4 Date & Time

You can set the system time manually or synchronize it with the network. If you select **Sync from network**, the CPE regularly synchronizes the time with the specified Network Time Protocol (NTP) server. If you enable daylight saving time (DST), the CPE also adjusts the system time for DST.

To set the date and time, perform the following steps:

1. Choose System > Date & Time.
2. Select Set **manually**.
3. Set **Local time** or click Sync to automatically fill in the current local system time.
4. Click **Submit**. As shown in Figure 5-67.



Date & Time

Settings

Current Time 2020-03-26 18:52:33

● Set Manually

Local Time 2020 / 03 / 26 / 18 / 52 / 18

(format:YYYY/MM/DD/HH/MM/SS,the value of year is between 2000 and 2030)

Figure 5-67

To synchronize the time with the network, perform the following steps:

1. Choose **System > Date & Time**.
2. Select **Sync from network**.
3. From the **Primary NTP server** drop-down list, select a server as the primary server for time

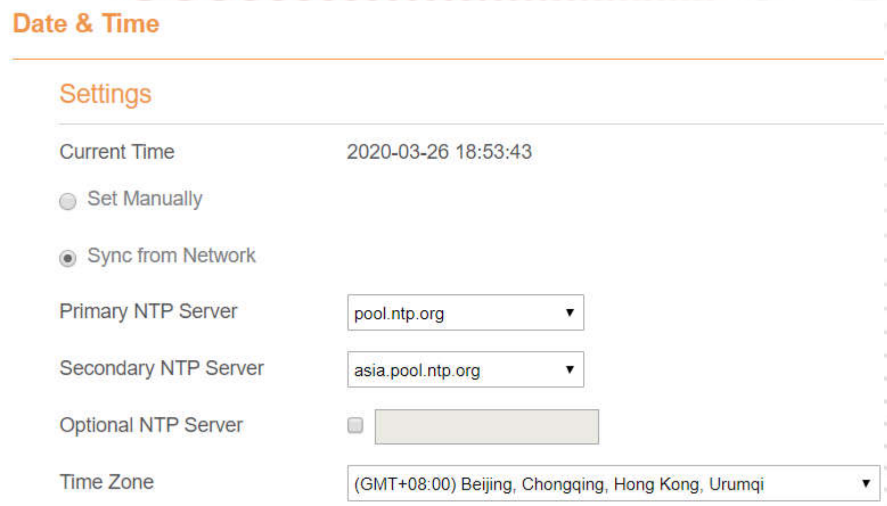
synchronization.

4. From the **Secondary NTP server** drop-down list, select a server as the IP address of the secondary server for time synchronization.

5. If you don’t want to use other NTP server, you need to enable **Optional ntp server**, and set a server IP address.

6. Set **Time zone**.

7. Click **Submit**. As shown in Figure 5-68.



Date & Time

Settings

Current Time 2020-03-26 18:53:43

○ Set Manually

● Sync from Network

Primary NTP Server: pool.ntp.org ▼

Secondary NTP Server: asia.pool.ntp.org ▼

Optional NTP Server: □

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi ▼

Figure 5-68

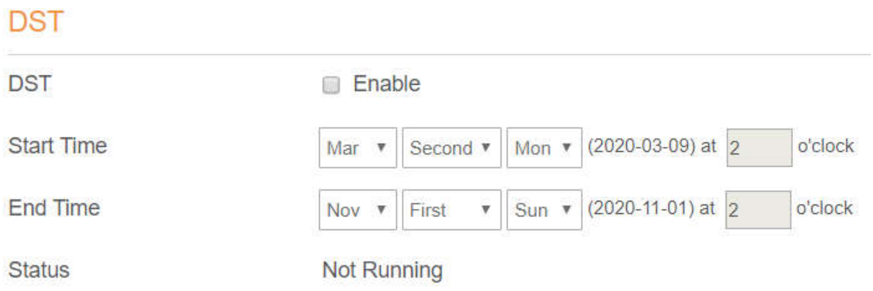
To set DST, perform the following steps:

1. Choose **System**>**Date&Time**.

2. Set **DST** enable.

3. Set **Start Time** and **End Time**.

4. Click **Submit**. As shown in Figure 5-69.



DST

DST: □ Enable

Start Time: Mar ▼ Second ▼ Mon ▼ (2020-03-09) at 2 o'clock

End Time: Nov ▼ First ▼ Sun ▼ (2020-11-01) at 2 o'clock

Status: Not Running

Figure 5-69

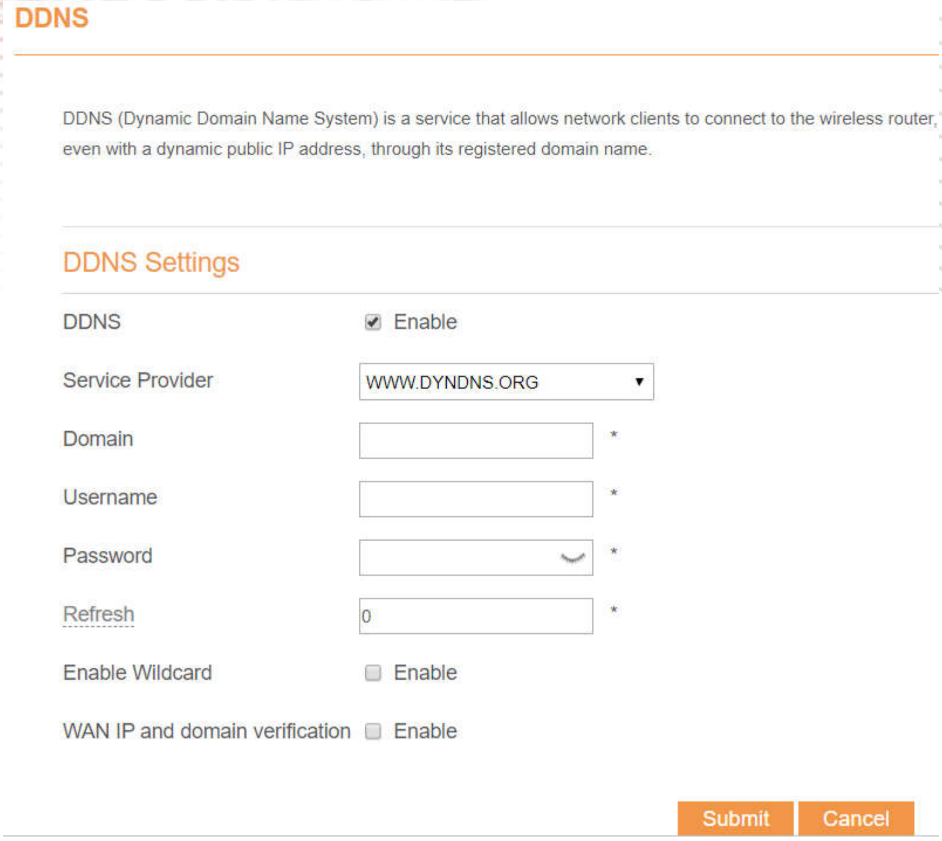
The CPE will automatically provide the DST time based on the time zone.

5.7.5 DDNS

Dynamic Domain Name Server (DDNS) service is used to map the user's dynamic IP address to a fixed DNS service.

To configure DDNS settings, perform the following steps:

1. Choose **System > DDNS**.
2. Set DDNS to **Enable**.
3. In **Service provider,** choose DynDNS.org or oray.com.
4. Enter **Domain name** and **Host name**. For example, if the domain name provided by your service provider is test.customtest.dyndns.org, enter customtest.dyndns.org as Domain name, and test as Host name.
5. Enter **User name** and **Password.**
6. Click **Submit**. As shown in Figure 5-70.



DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name.

DDNS Settings

DDNS ☑ Enable

Service Provider: WWW.DYNDNS.ORG

Domain *

Username *

Password *

Refresh: 0 *

Enable Wildcard ☐ Enable

WAN IP and domain verification ☐ Enable

Figure 5-70

5.7.6 Diagnosis

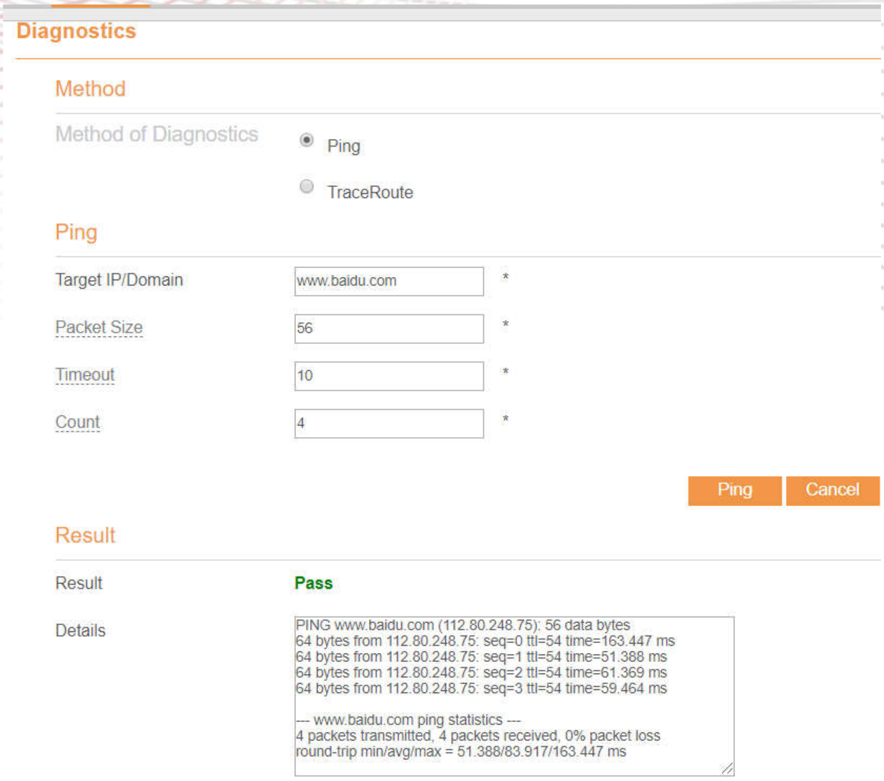
If the CPE is not functioning correctly, you can use the diagnosis tools on the **Diagnosis** page to preliminarily identify the problem so that actions can be taken to solve it.

Ping

If the CPE fails to access the Internet, run the ping command to preliminarily identify the problem. To do so:

1. Choose **System**>**Diagnosis**.
2. In the Method area, select **Ping**.
3. Enter the domain name in the **Target IP or domain** field, for example, www.google.com.
4. Set **Packet size** and **Timeout**.
5. Set **Count**.
6. Click **Ping**. As shown in Figure 5-71.

Wait until the ping command is executed. The execution results are displayed in the Results box.



Method of Diagnostics: ● Ping ○ TraceRoute

Target IP/Domain: www.baidu.com *

Packet Size: 56 *

Timeout: 10 *

Count: 4 *

Result: Pass

Details:

```
PING www.baidu.com (112.80.248.75): 56 data bytes
64 bytes from 112.80.248.75: seq=0 ttl=54 time=163.447 ms
64 bytes from 112.80.248.75: seq=1 ttl=54 time=51.388 ms
64 bytes from 112.80.248.75: seq=2 ttl=54 time=61.369 ms
64 bytes from 112.80.248.75: seq=3 ttl=54 time=59.464 ms

--- www.baidu.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 51.388/83.917/163.447 ms
```

Figure 5-71

Traceroute

If the CPE fails to access the Internet, run the Traceroute command to preliminarily identify the problem. To do so:

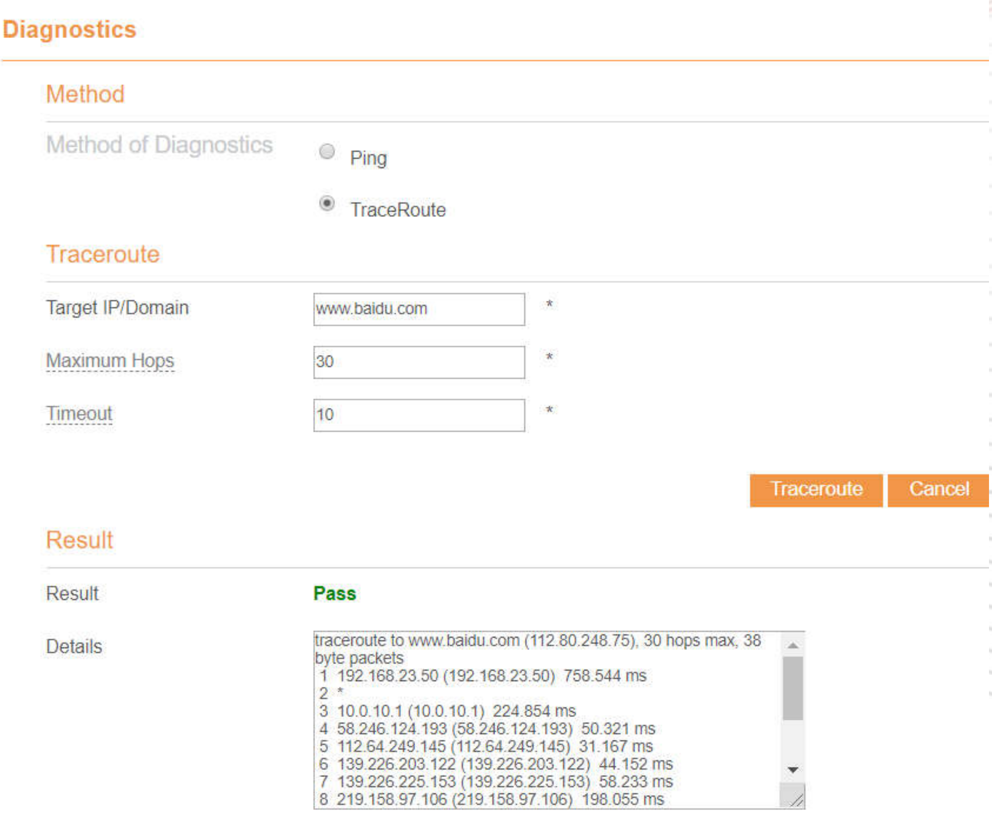
1. Choose **System**>**Diagnosis**.
2. In the Method area, select **Traceroute**.

3. Enter the domain name in the **Target IP or domain** field. For example, www.google.com.

4. Set **Maximum hops** ad **Timeout**.

5. Click **Traceroute**. As shown in Figure 5-72

Wait until the traceroute command is executed. The execution results are displayed in the Results box.



Diagnostics

Method

Method of Diagnostics ○ Ping ● TraceRoute

Traceroute

Target IP/Domain: www.baidu.com *

Maximum Hops: 30 *

Timeout: 10 *

Result

Result: Pass

Details:

```
traceroute to www.baidu.com (112.80.248.75), 30 hops max, 38
byte packets
 1  192.168.23.50 (192.168.23.50)  758.544 ms
 2  *
 3  10.0.10.1 (10.0.10.1)  224.854 ms
 4  58.246.124.193 (58.246.124.193)  50.321 ms
 5  112.64.249.145 (112.64.249.145)  31.167 ms
 6  139.226.203.122 (139.226.203.122)  44.152 ms
 7  139.226.225.153 (139.226.225.153)  58.233 ms
 8  219.158.97.106 (219.158.97.106)  198.055 ms
```

Figure 5-72

5.7.7 Port Mirror

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port. To do so:

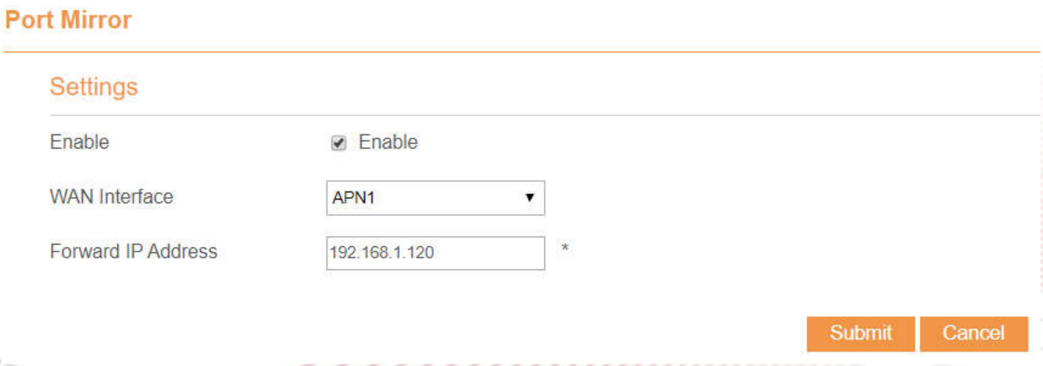
1. Choose **System**>**Port Mirror**.

2. Enable Port Mirror.

3. Select the **WAN Interface** which you want a copy.

4. Type the **Monitor IP**, where the copy will send to.

5. Click **Submit**. As shown in Figure 5-73.



Port Mirror

Settings

Enable ☑ Enable

WAN Interface APN1 ▼

Forward IP Address 192.168.1.120 *

Figure 5-73

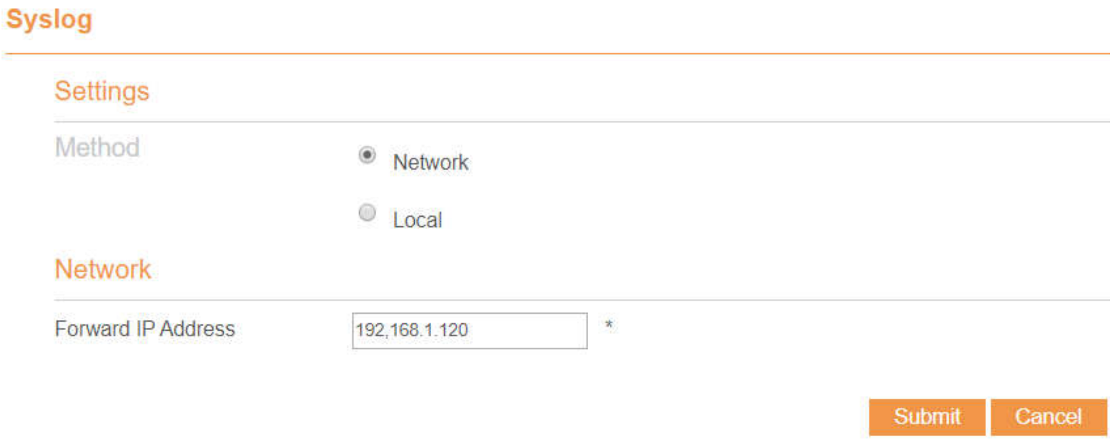
5.7.8 Syslog

The syslog record user operations and key running events.

Local

To set the syslog to local, perform the following steps:

1. Choose **System**>**Syslog**.
2. In the **Setting** area, set the method to **Local**.
3. In the **Level** drop-down list, select a log level.
4. Click **Submit**. As shown in Figure 5-74.



Syslog

Settings

Method ● Network ○ Local

Network

Forward IP Address 192,168.1.120 *

Figure 5-74

Viewing local syslog

To view the local syslog, perform the following steps:

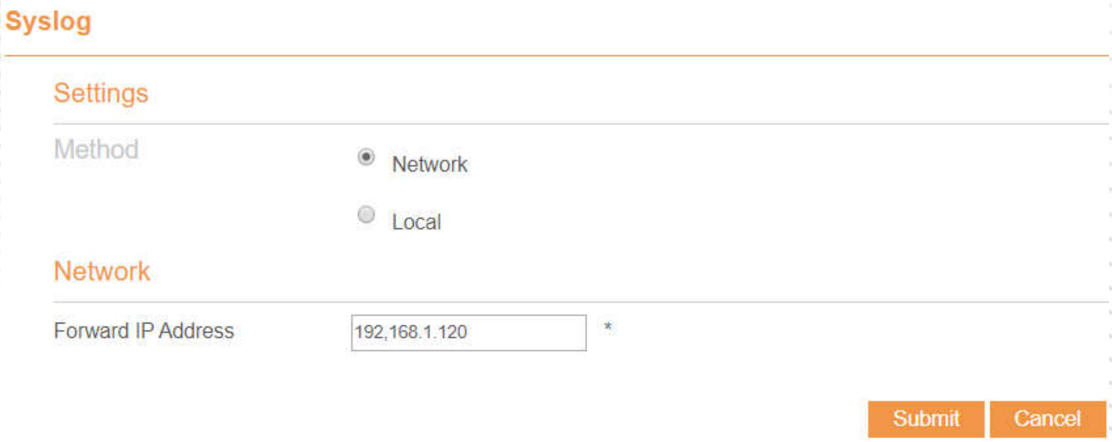
1. In the **Keyword** box, set a keyword.
2. Click **Pull**, the result box will display.

Network

To set the syslog to network, perform the following steps:

1. Choose **System**>**Syslog**.
2. In the **Setting** area, set the method to **Network**.
3. In the **Level** drop-down list, select a log level.
4. In the **Forward IP address** box, set an IP address.
5. Click **Submit**. As shown in Figure 5-75.

The syslog will transmit to some client to display through network.



Syslog

Settings

Method ● Network ○ Local

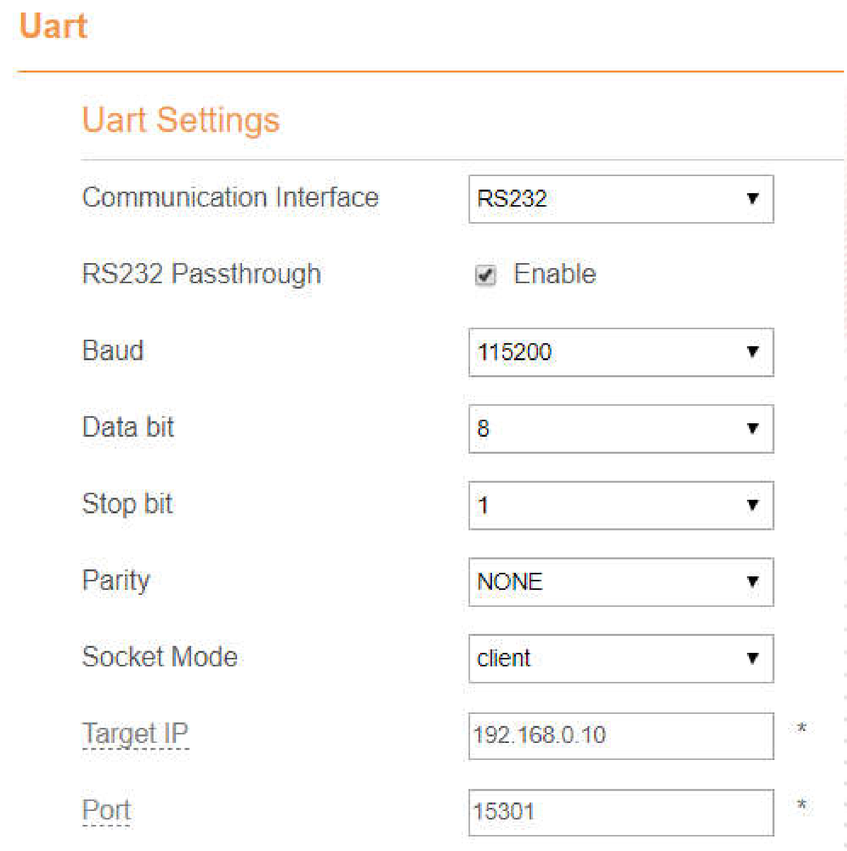
Network

Forward IP Address: 192,168.1.120 *

Figure 5-75

5.7.9 Uart

To use the RS232 or RS485 communicate, we should setting the value here.



Uart

Uart Settings

Communication Interface: RS232

RS232 Passthrough: ☑ Enable

Baud: 115200

Data bit: 8

Stop bit: 1

Parity: NONE

Socket Mode: client

Target IP: 192.168.0.10 *

Port: 15301 *

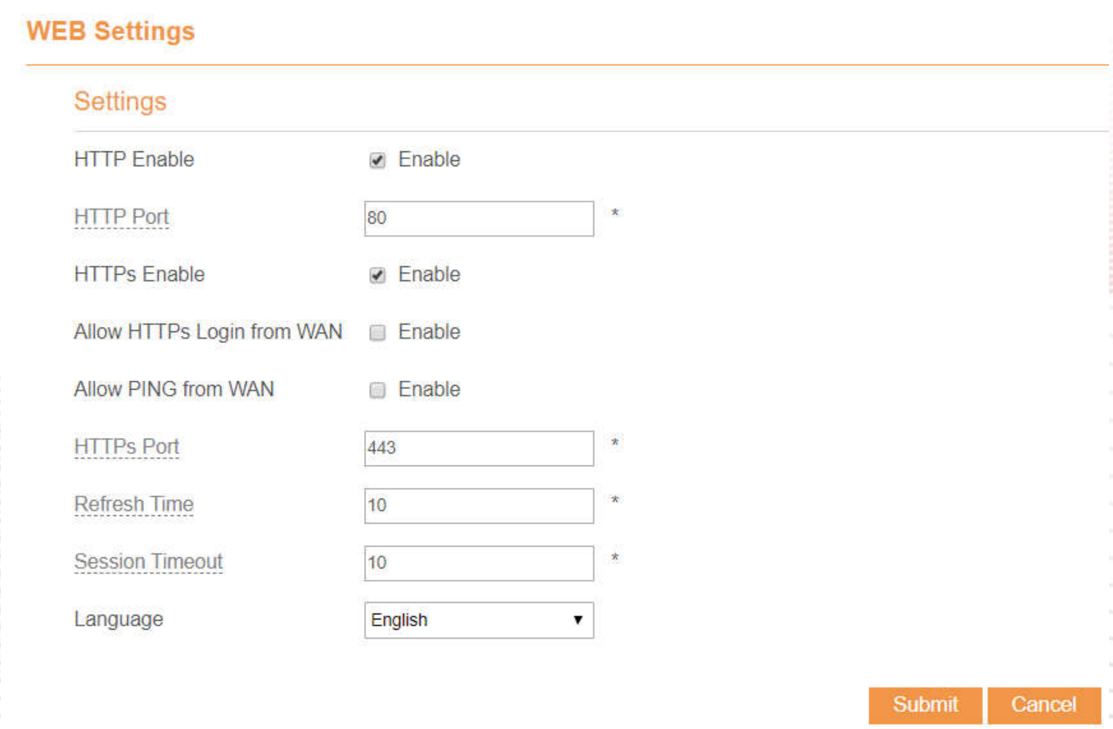
Figure 5-76

The target IP is terminal’s IP. The port should be set the same as terminal.

5.7.10 WEB Setting

To configure the parameters of WEB, perform the following steps:

1. Choose **System**> **WEB Setting**.
2. Set **HTTP** enable. If you set HTTP disable, you will can’t login the web management page with the HTTP protocol from WAN side.
3. Set **HTTP port**. If you want to change the login port, you can set a new port in the box, the default HTTP port is 80.
4. Set **HTTPS** enable. If you want to login the web management page with the HTTPS protocol from WAN side, you need to enable the HTTPS.
5. If you want to login the web management page form the **WAN**, you need to Enable **Allowing login from WAN**.
6. Set the **HTTPS port**.
7. Click **Submit**. As shown in Figure 5-77.



WEB Settings

Settings

HTTP Enable	☑ Enable
HTTP Port	80 *
HTTPs Enable	☑ Enable
Allow HTTPs Login from WAN	□ Enable
Allow PING from WAN	□ Enable
HTTPs Port	443 *
Refresh Time	10 *
Session Timeout	10 *
Language	English ▼

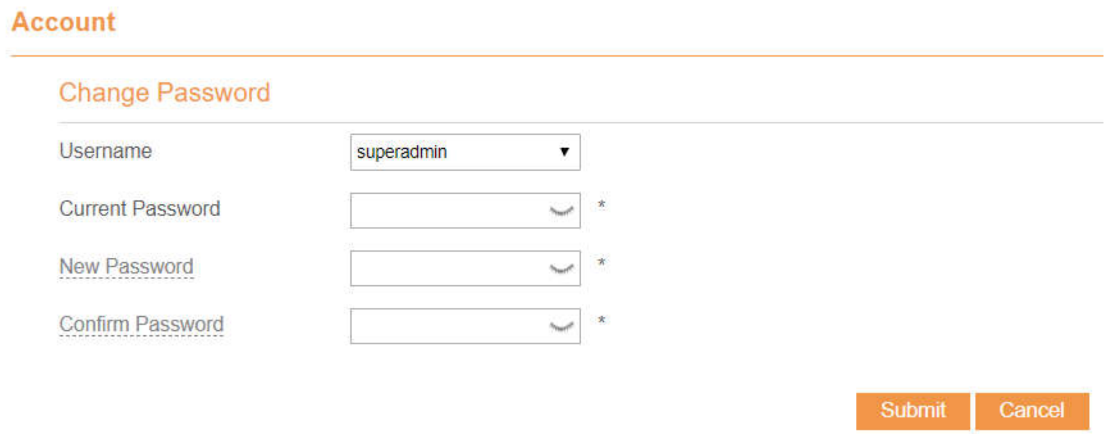
Figure 5-77

5.7.11 Account

This function enables you to change the login password of the user. After the password changes, enter the new password the next time you login.

To change the password, perform the following steps:

1. Choose **System**>**Account**.
2. Select the **user name**, if you want to change the password of normal user, you need to set **Enable User** enable.
3. Enter the **current password**, set a **new password**, and **confirm the new password**.
4. **New password** and **Confirm password** must contain 5 to 15 characters.
5. Click **Submit**. As shown in Figure 5-78.



Account

Change Password

Username	superadmin ▼
Current Password	*
New Password	*
Confirm Password	*

Figure 5-78

5.7.12 Logout

To logout the web management page, perform the following steps:

1. Choose **System** and click **Logout**

It will return to the login page.

FAQs

The POWER indicator does not turn on.

- Make sure that the power cable is connected properly and the CPE is powered on.
- Make sure that the power adapter is compatible with the CPE.

Fails to Log in to the web management page.

- Make sure that the CPE is started.
- Verify that the CPE is correctly connected to the computer through a network cable. If the problem persists, contact authorized local service suppliers.

The CPE fails to search for the wireless network.

- Check that the power adapter is connected properly.
- Check that the CPE is placed in an open area that is far away from obstructions, such as concrete or wooden walls.
- Check that the CPE is placed far away from household electrical appliances that generate strong electromagnetic field, such as microwave ovens, refrigerators, and satellite dishes.

If the problem persists, contact authorized local service suppliers.

The power adapter of the CPE is overheated.

- The CPE will be overheated after being used for a long time. Therefore, power off the CPE when you are not using it.
- Check that the CPE is properly ventilated and shielded from direct sunlight.

The parameters are restored to default values.

- If the CPE powers off unexpectedly while being configured, the parameters may be restored to the default settings.
- After configuring the parameters, download the configuration file to quickly restore the CPE to the desired settings.

FCC Regulations:

§ 15.19 (a)(3)

This mobile phone 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

§ 15.21

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

§ 15.105 (b)

This mobile phone 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 radiated 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.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF Exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 25cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmit.