MGL6201A

User Manual

Index

1 Getting Started..... 4
1.1 Welcome to the Module..... 4
1.2 Computer Configuration Requirements..... 4
1.3 Logging In to the Web Management Page..... 6
2 Overview..... 8
2.1 Viewing Current Connection..... 8
2.2 Viewing LTE Status..... 8
2.3 Viewing WAN Status..... 8
3 Statistics..... 9
3.1 Viewing CPU Usage..... 9
3.2 Viewing Memory Usage..... 10
3.3 Viewing APN List..... 10
3.4 Viewing Throughput Statistics..... 11
3.5 Viewing Device List..... 11
4 Update..... 12
4.1 Version Manager..... 12
Viewing Version Info..... 12
Version Upgrade..... 12
4.2 Auto upgrade..... 13
5 Settings..... 14
5.1 Viewing the Device Information..... 14
Viewing the Version Information..... 15
Viewing LAN Status..... 15
5.2 Viewing Network..... 16
LTE Settings..... 16
Scan Mode..... 18
APN Management..... 19
PIN Management..... 20
SIM Lock..... 22
LAN Setting..... 22
DMZ Settings..... 24
Static Route..... 25
5.3 Parental Controls..... 26
Parental Controls Manager..... 26
Parental Controls List..... 26
5.4 Firewall..... 27
Setting Firewall..... 27
MAC Filtering..... 28
IP Filtering..... 31

URL Filtering....34
Port Forwarding....36
UPnP....39
DoS....39
5.6 VPN....40
5.7 IPv6....40
Status....40
IPv6 WAN Settings....41
IPv6 LAN Settings....41
5.8 System....42
5.8.1 Maintenance....42
Reboot....42
Reset....42
Backup Configuration File....43
Upload Configuration File....43
5.8.2 TR069....44
5.8.3 Date & Time....45
5.8.4 DDNS....47
5.8.5 Diagnosis....48
Ping....48
Traceroute....49
5.8.6 Port Mirror....50
5.8.7 Syslog....51
Local....51
Network....51
5.8.8 WEB Setting....52
5.8.9 Account....53
5.8.10 Logout....54
6 FAQs....54

1 Getting Started

1.1Welcome to the Module

This Module needs to be installed on a specific backplane, 12V power supply, and an external antenna.The Module support B2/4/5/8/12/13/14/25/26/66/38/41/42/43/48/53.

And its tx power is 23±2.

Carefully read the following safety symbols to help you use your Module safely and correctly:

	Additional information
	Optional methods or shortcuts for an action
	Potential problems or conventions that need to be specified

Note: 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.

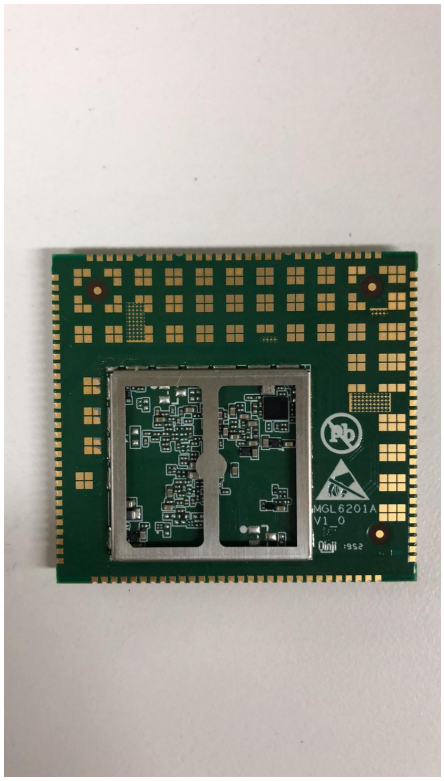
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

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.

The customer does not have permission to modify the parameters of the device.

The device usage scenario is 20cm away from the human body.



No professional installation of equipment is required.

MGL6201A has built-in rich network protocols, integrates multiple industry standard interfaces, and supports multiple drivers and software functions (for USB drivers under Windows 7/8 / 8.1 / 10, Linux, Android and other operating systems), greatly expanding The application scope of MGL6201A, such as CPE, router, data card, tablet PC, automotive, security and industrial PDA, etc.

1.2Computer Configuration Requirements

For optimum performance, make sure your computer meets the following requirements.

Item	Requirement
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard disk	50 MB available space
Operating system	• Microsoft: Windows XP, Windows Vista, or Windows 7 • Mac: Mac OS X 10.5 or higher
Display resolution	1024 x 768 pixels or higher

Browser	• Internet Explorer 7.0 or later • Firefox 3.6 or later • Opera 10 or later • Safari 5 or later • Chrome 9 or later

1.3Logging In to the Web Management Page

Use a browser to log in to the web management page to configure and manage the Module.

The following procedure describes how to use a computer running Windows XP and Internet Explorer 7.0 to log in to the web management page of the Module.

1. Connect the Module properly.
2. Launch Internet Explorer, enter http://192.168.1.1 in the address bar, and press Enter. As shown in Figure 1-1.

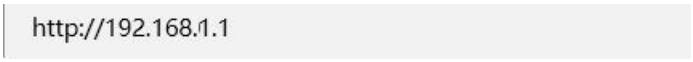


Figure 1- 1

3. Enter the user name and password, and click Log In.
4. You can log in to the web management page after the password is verified. As shown in Figure 1-2.

Figure 1- 2

The default user name and password are both **admin**. If you want to view or configure the CPE more, you should use the super account to log in to the web management page. The default super user name is **superadmin**, and the password is **admin**.

To protect your CPE from unauthorized access, change the password after your first

login.

The CPE supports diagnostic function. If you encounter problems, please contact customer service for the specific using method.

To ensure your data safety, it is recommended that you turn on the firewall, and conserve your login and FTP password carefully.

2 Overview

2.1Viewing Current Connection

To view the current connection, perform the following steps:

Choose **Overview**;

In the **Current Connection** area, view the connection status, such as DL/UL Data Rate and Online time. As shown in Figure 2-1.

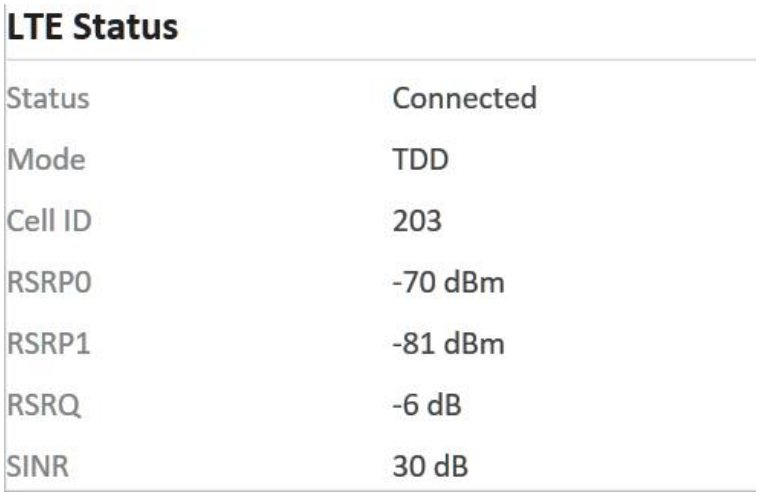
Current Connection	
DL Data Rate	Current: 63 KB/s | Max.: 63 KB/s | Min.: 0 Bytes/s
UL Data Rate	Current: 51 KB/s | Max.: 91 KB/s | Min.: 0 Bytes/s
Online Time	00d 00h 33min

Figure 2- 1

2.2Viewing LTE Status

To view the LTE network status, perform the following steps:

1. Choose **Overview**;
2. In the **LTE Status** area, view the information about Connect status, Mode, Cell ID, Signal quality and so on. As shown in Figure 2-3.



LTE Status	
Status	Connected
Mode	TDD
Cell ID	203
RSRP0	-70 dBm
RSRP1	-81 dBm
RSRQ	-6 dB
SINR	30 dB

Figure 2- 3

2.3Viewing WAN Status

To view the WAN status, perform the following steps:

1. Choose **Overview**;
2. In the **WAN Status** area, view the information about Connect Mode, IP, Subnet Mask, DNS Server and so on. As shown in Figure 2-4.

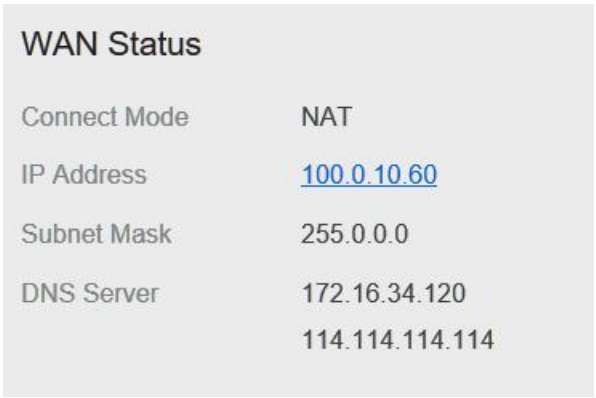


Figure 2-4

3 Statistics

3.1Viewing CPU Usage

To view the CPU usage, perform the following steps:

1. Choose **Statistics**;
2. In the **CPU Usage** area, view the CPU usage information, such as Current CPU usage, Max CPU usage, Min CPU usage. As shown in Figure 3-1.

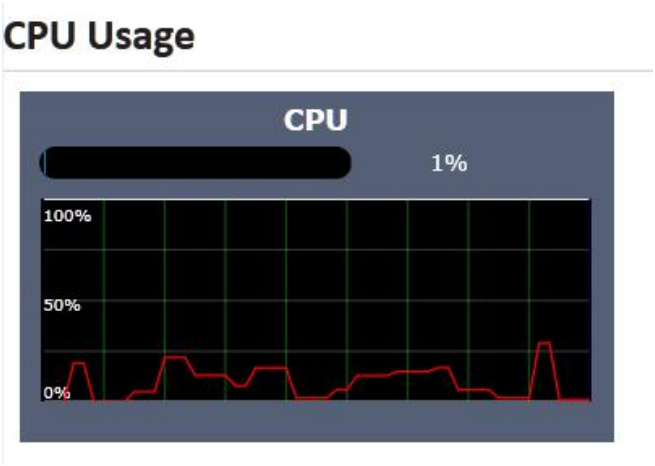


Figure 3- 1

3.2Viewing Memory Usage

To view the memory usage, perform the following steps:

1. Choose **Statistics**;
2. In the **Memory Usage** area, view the memory usage information, such as Total memory, Current memory usage, Max memory usage and Min memory usage. As shown in Figure 3-2.

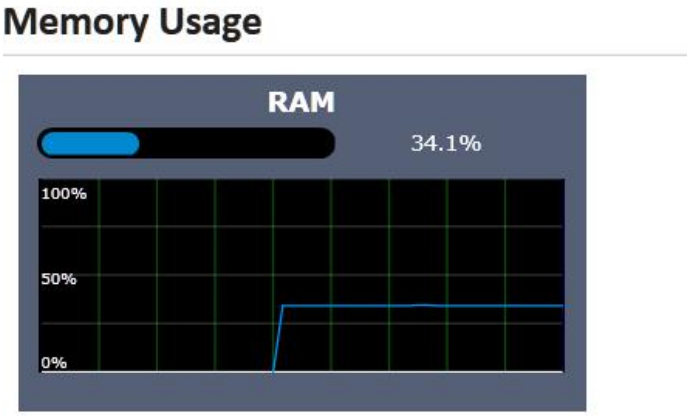


Figure 3- 2

3.3Viewing 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

APN Name	Status	IP Address	Subnet Mask
apn1	Enable	100.16.14.121	255.0.0.0
apn2	Disable	--	--
apn3	Disable	--	--
apn4	Disable	--	--

Figure 3- 3

3.4Viewing 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	Errors	Dropped	Total Traffic	Packets	Errors	Dropped
LAN	2.97 MB	18066	0	0	17.44 MB	24735	0	0
apn1	12.96 MB	16883	0	0	1.65 MB	12366	0	0
apn2	0 Bytes	0	0	0	0 Bytes	0	0	0
apn3	0 Bytes	0	0	0	0 Bytes	0	0	0
apn4	0 Bytes	0	0	0	0 Bytes	0	0	0

Reset

Figure 3- 4

3.5Viewing Device List

To view the device list, perform the following steps:

Choose **Statistics**;

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	jingjin-PC	c0:f8:da:ab:38:64	192.168.1.173	0days 11:59:51	WIFI

Figure 3- 5

4 Update

4.1 Version Manager

This function enables you to upgrade the software version of the CPE to the latest version. It is recommended that you upgrade the software because the new version, certain bugs have been fixed and the system stability is usually improved.

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.

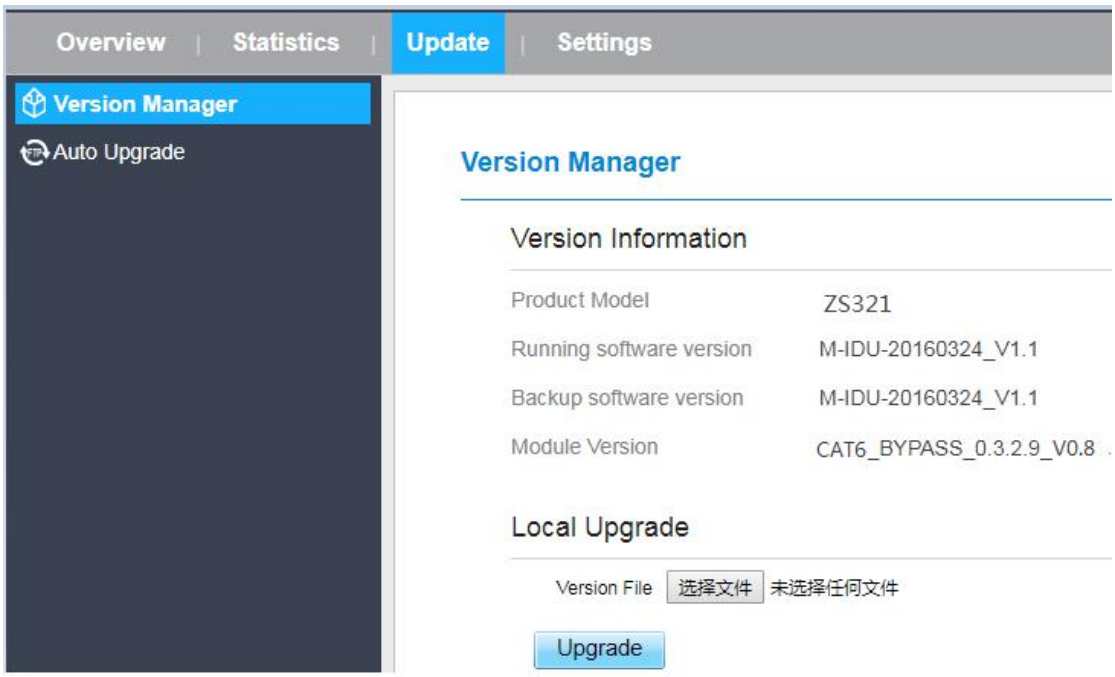


Figure 4- 1

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 **Browse**. 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

4.2Auto 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:

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

Enable **auto upgrade**.

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**.

Set a ftp address to the **Upgrade folder** box.

Set **Version file**.

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

Set the **Interval** of checking new firmware.

Set **Start time**.

Set **Random time**.

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

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

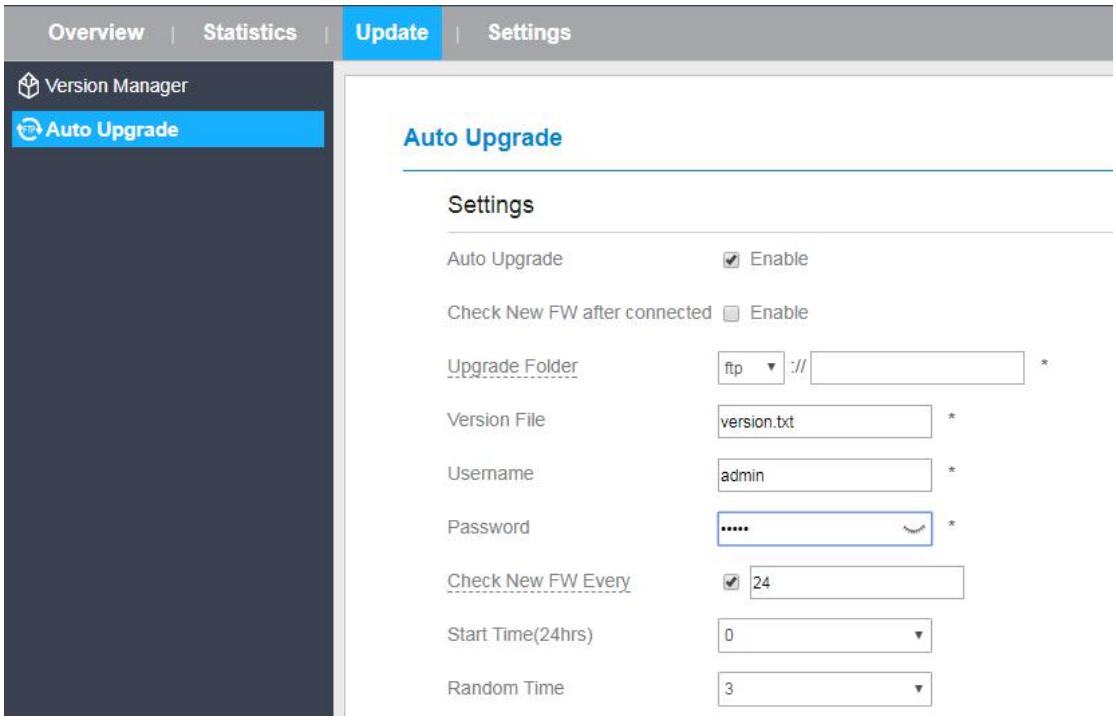


Figure 4- 3

5 Settings

5.1 Viewing the Device Information

To view the System Information, perform the following steps:

Choose **Settings**;

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

Figure 5- 1

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 Module, Hardware Version, Software version, UBoot version and CPE SN . As shown in Figure 5-2.

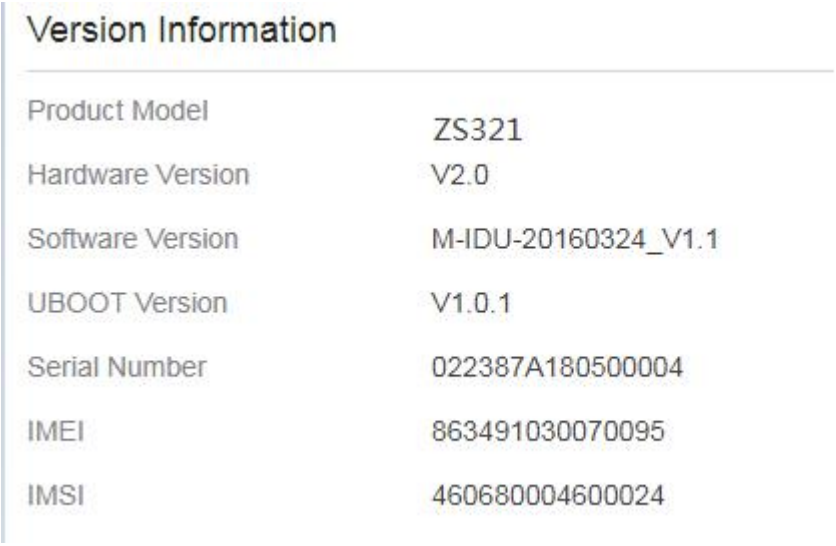


Figure 5- 2

Viewing LAN Status

To view the LAN status, perform the following steps:

Choose **Settings**;

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

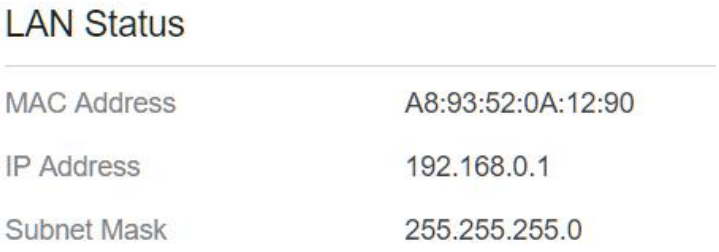


Figure 5- 4

5.2Viewing Network

Network Mode

To set the network mode, perform the following steps:

Choose **Network** >**WAN Settings**;

In the **Network Mode** area, select a mode between **NAT** and **ROUTER**;

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

Figure 5- 5

LTE Settings

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 5-7.

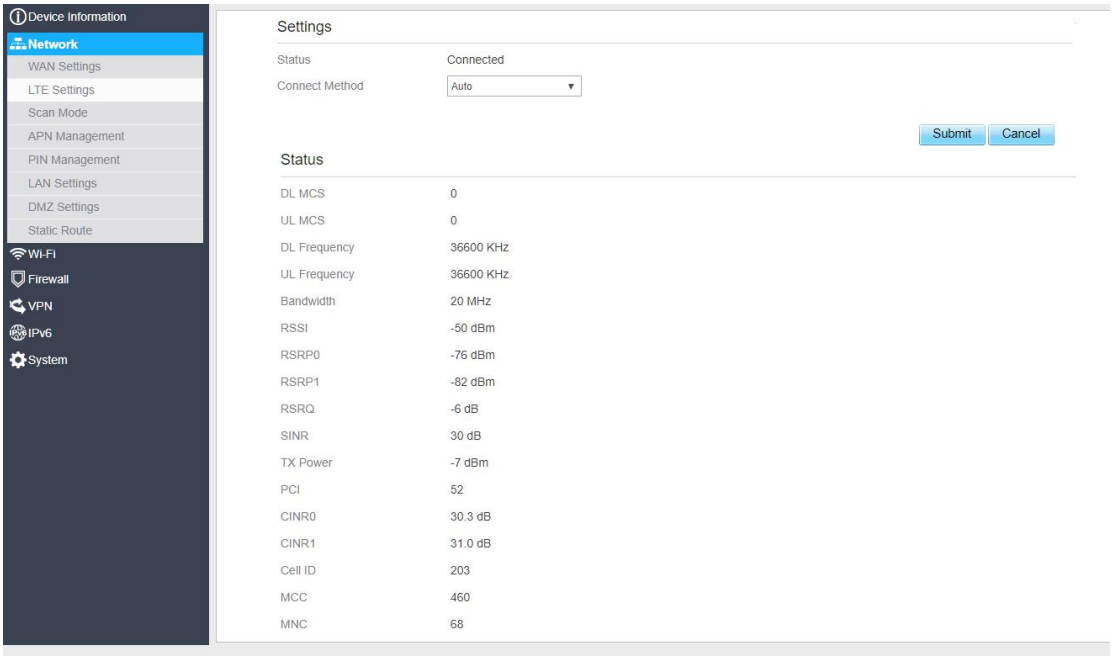


Figure 5-7

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 5-8.

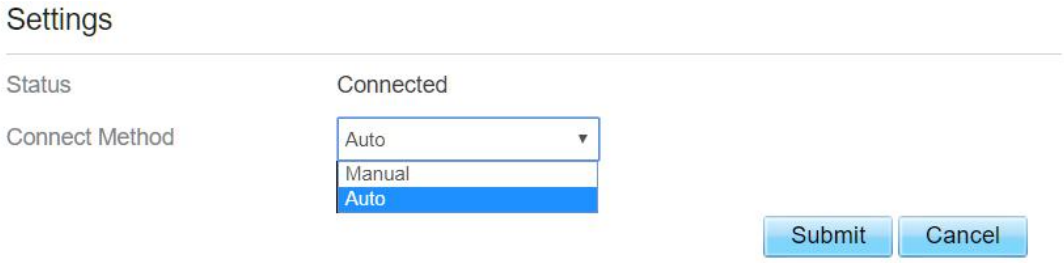


Figure 5-8

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 5-9.

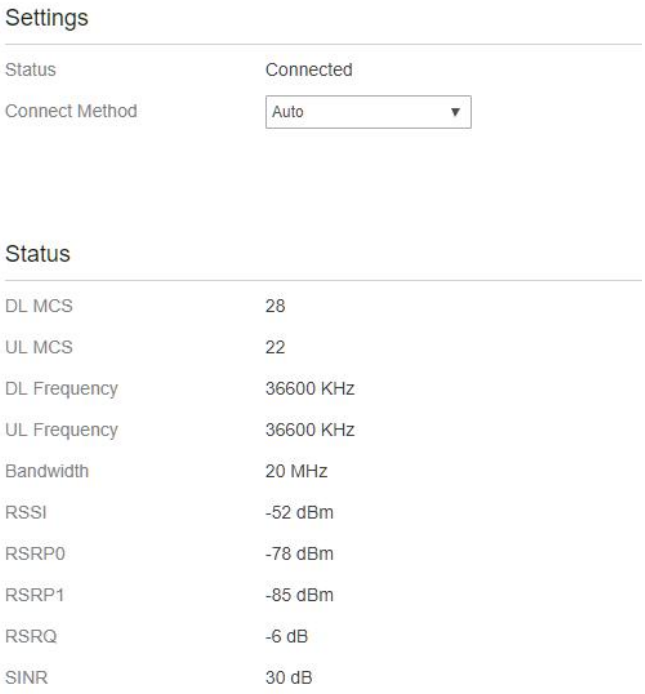


Figure 5-9

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 5-10.

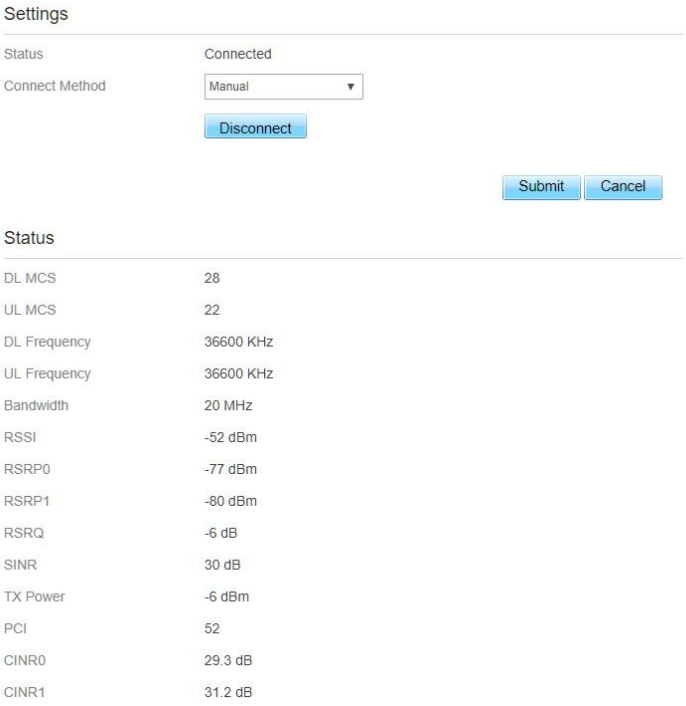


Figure 5- 10

Scan Mode

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

choose **Network>Scan mode**;

You can choose **full mode**, a band the CPE supported

Click **Submit**.

Setting Frequency (Earfcn)

To set the frequency, perform the following steps:

1 Choose **Network>Scan Mode**.

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

3 In the **Frequency Lock** area, you can choose a band, then click **Add list** to

choose a **Earfcn Number**.

4 Click **Submit**. As shown in Figure 5-11.

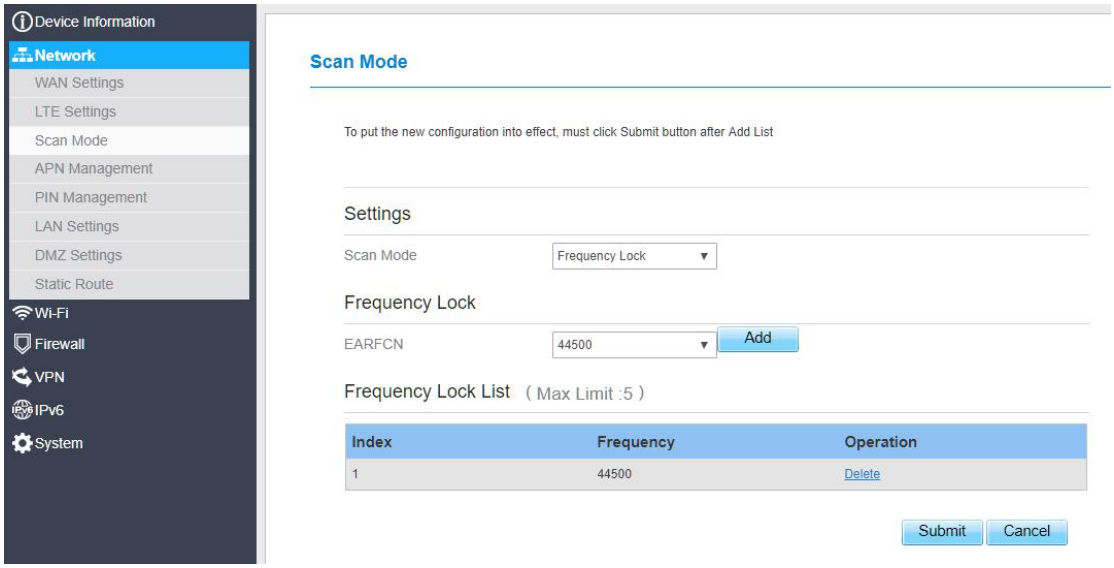


Figure 5- 11

APN Management

To set and manage APN, perform the following steps:

Choose **Network>APN Management**.

In the **APN Management** area, you can set the APN.

Choose a **APN number** which you want to set.

In the **APN Setting** area you can set the APN parameters, such as enable or disable the apn, apn name, username, password and so on.

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

Click **Submit.** As shown in Figure 5-12.

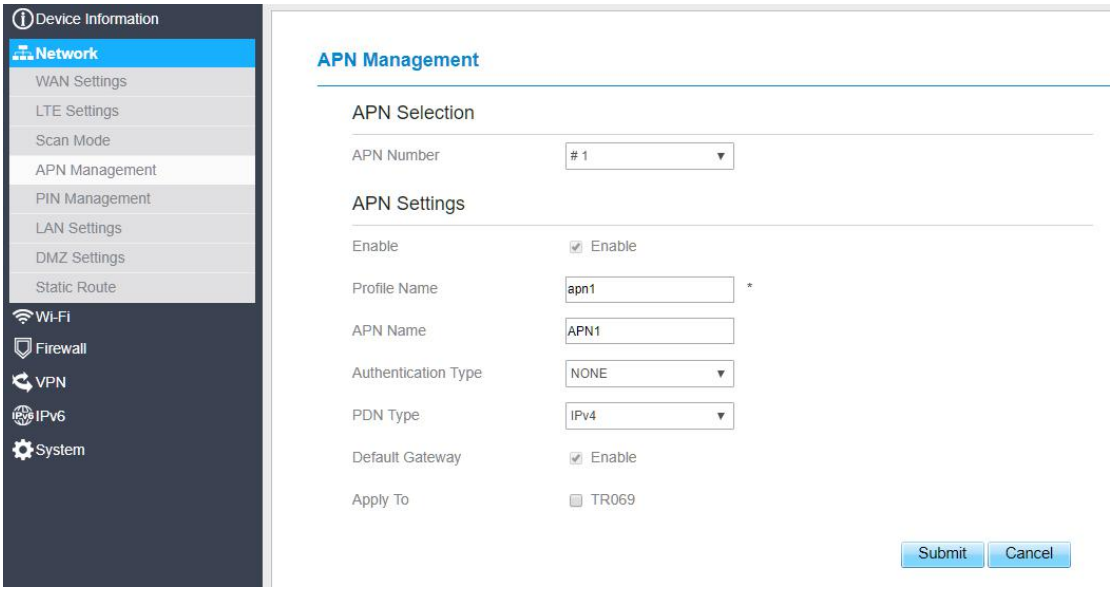


Figure 5- 12

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

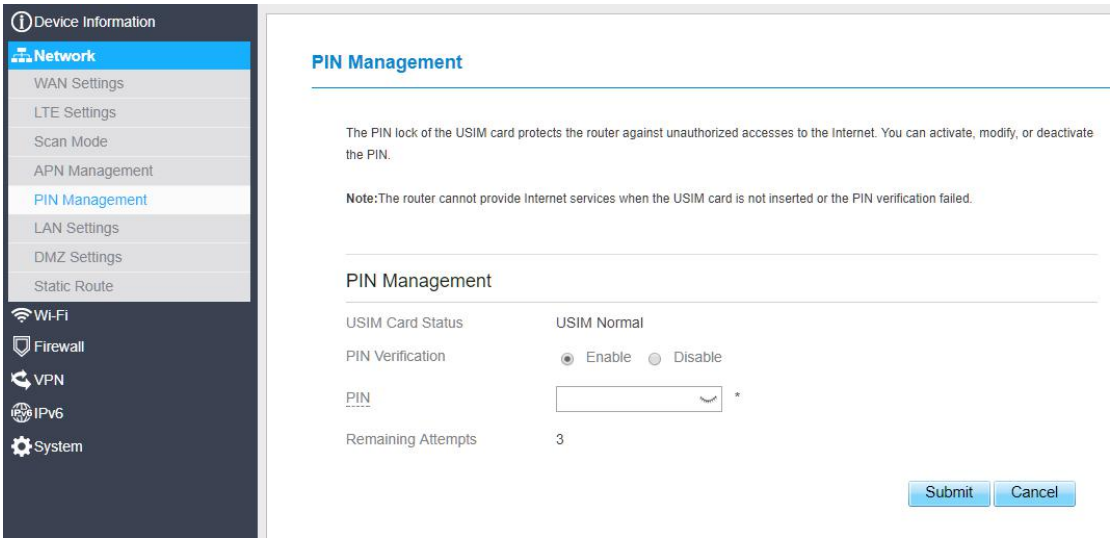


Figure 5- 13

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.

To enable automatic verification of the PIN, perform the following steps:

1. Choose **Network** > **PIN Management**.
2. Set **Pin verification** to **Enable**.
3. Set **Remember my PIN** to **Enable**.
4. 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:

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

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

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

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

Click **Submit**.

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. Enter the PLMN in the **PLMN** box.
3. Click **Submit**. As shown in Figure 3-9.

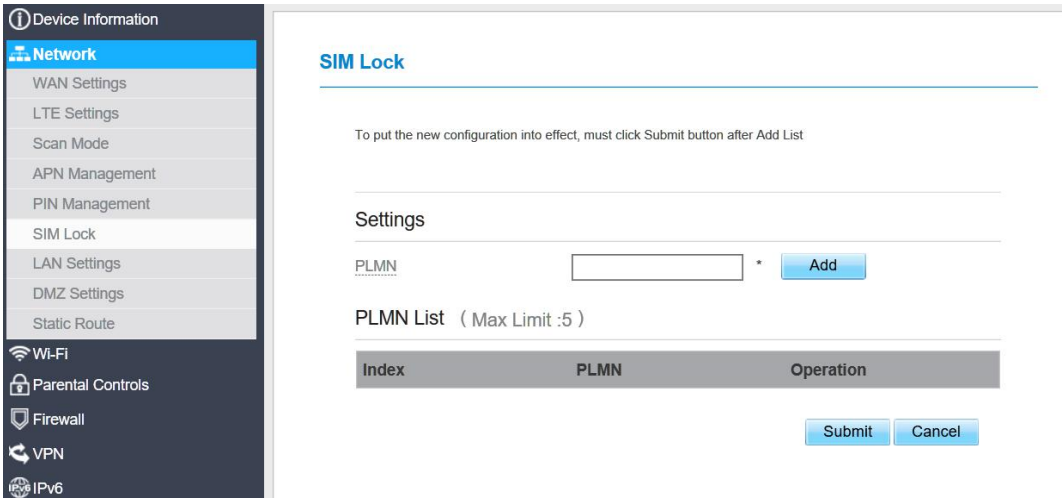


Figure 3- 9

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 5-14.

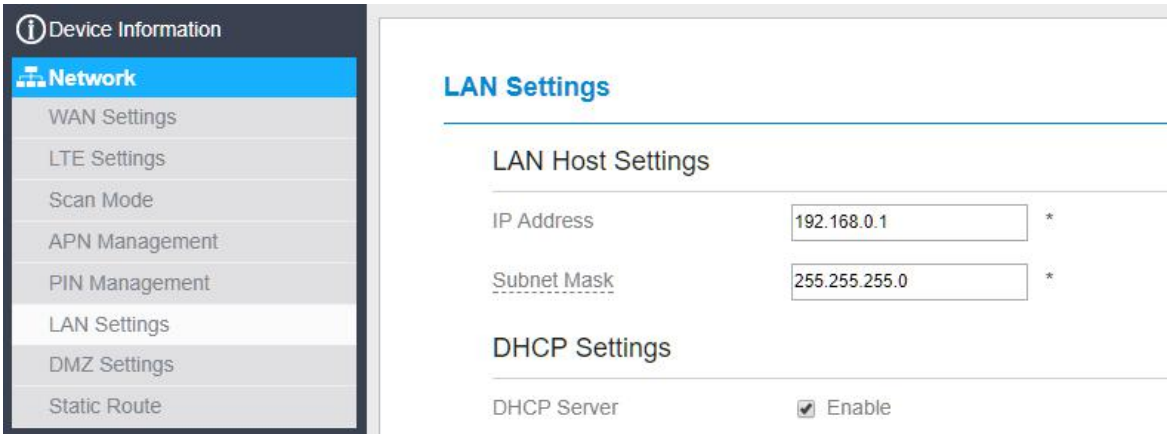


Figure 5- 14

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 5-15.

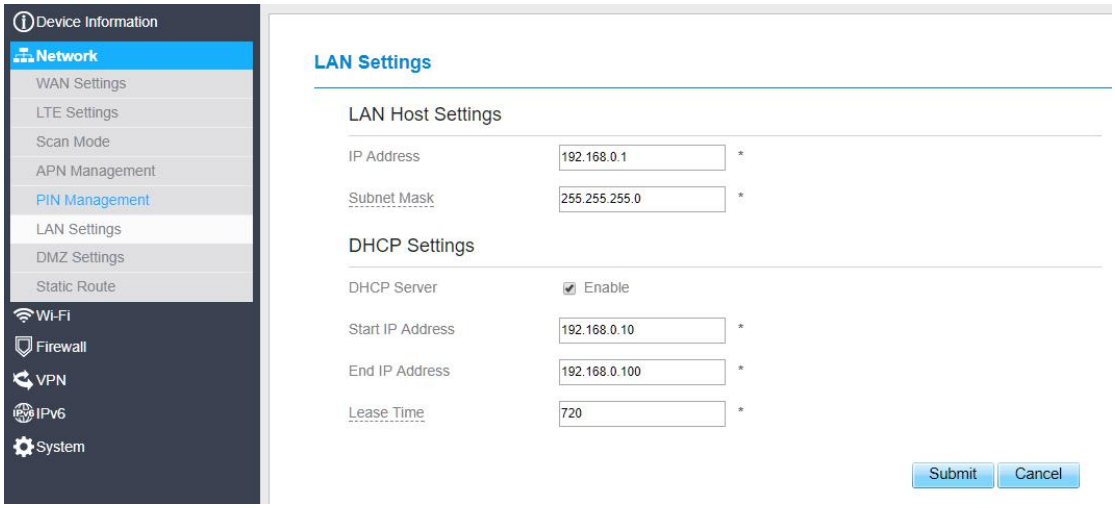


Figure 5- 15

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.

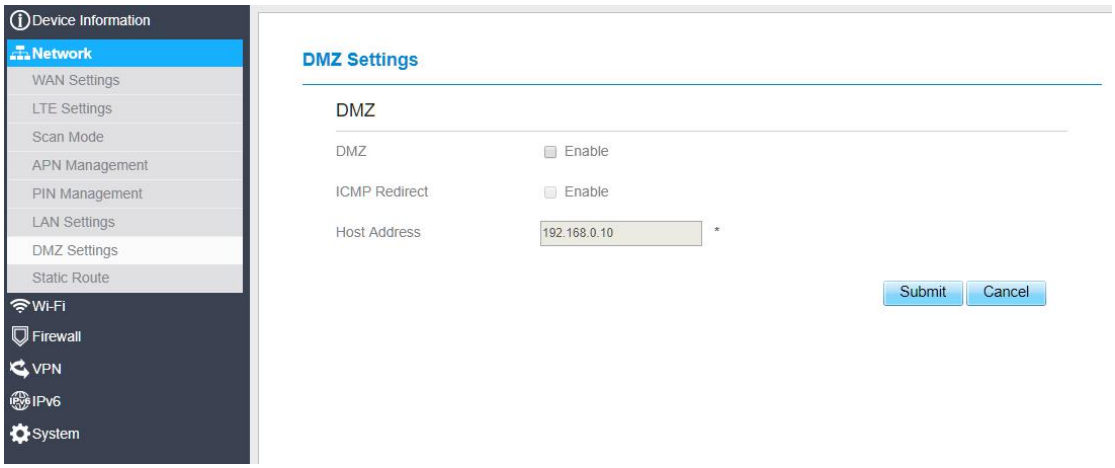


Figure 5- 18

Static Route

Add Static Route

To add a static route, perform the following steps:

Choose **Network Setting>Static Route**.

Click **Add list**.

Set the **Dest IP address** and **Subnet mask**.

Select an **Interface** from the drop-down list.

If you select **LAN** as the interface, you need set a Gateway.

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

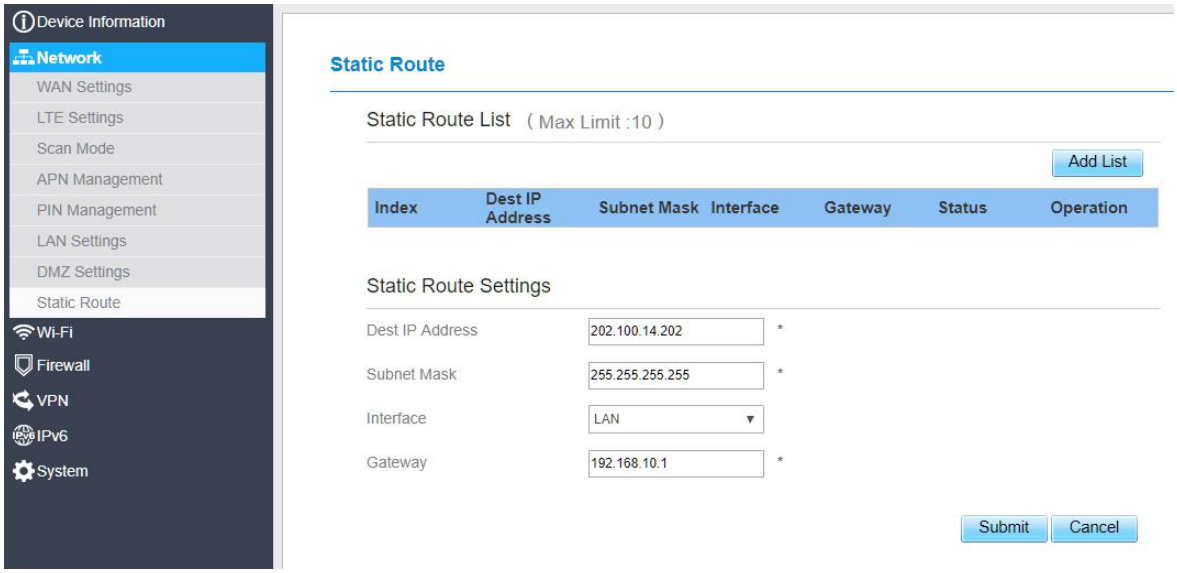


Figure 5- 19

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.

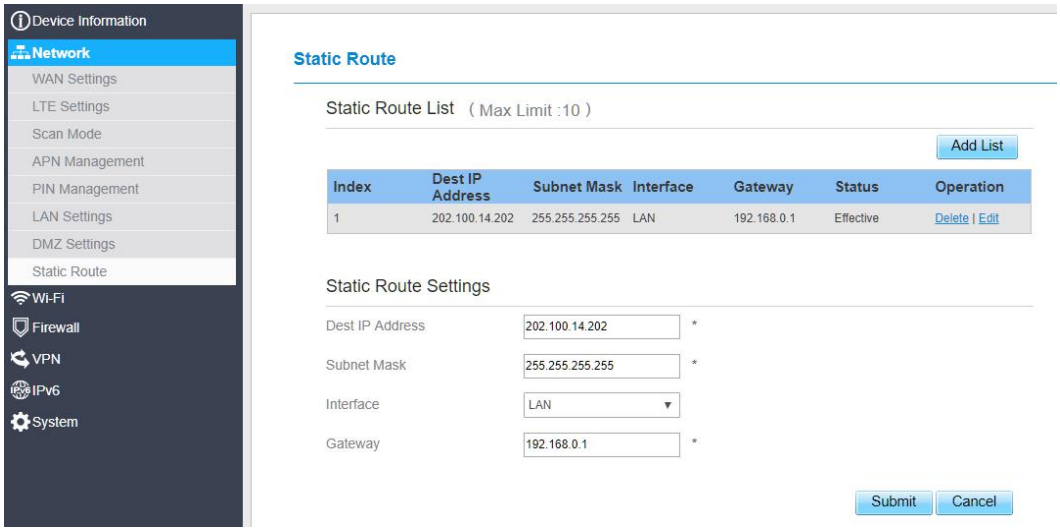


Figure 5- 20

Delete Static Route

To delete a static route, perform the following steps:

Choose **Firewall>Static Route**.

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

5.3 Parental Controls

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

Parental Controls Manager

Choose Parental Controls Manager, Choose **Enable ,and then click Submit Enabled the** Choose Parental function. As shown in Figure 5-4-1.

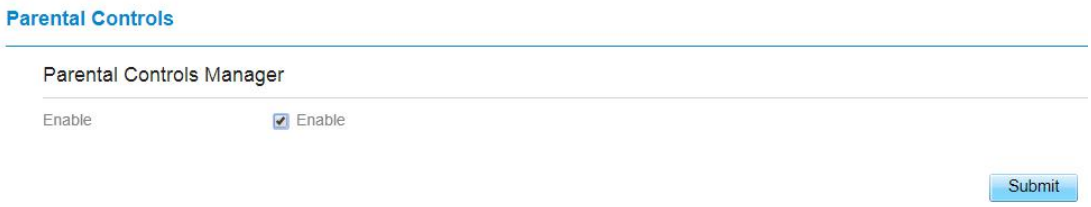


Figure 5-4-1.

Parental Controls List

This page is set the Parental Controls List. If this function is enabled, you can add some users. If someone in this List , he was forbidden from the Internet. If you want to allow him to access the

Internet, you can remove it from this Parental Controls List. As shown in Figure 5-4-2、5-4-3

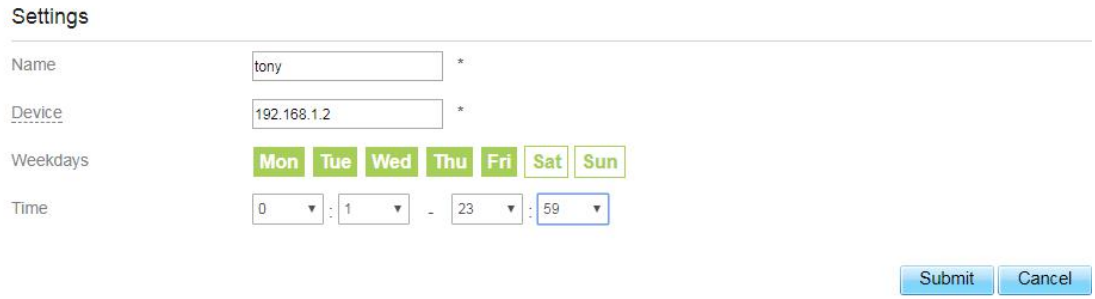


Figure 5-4-2

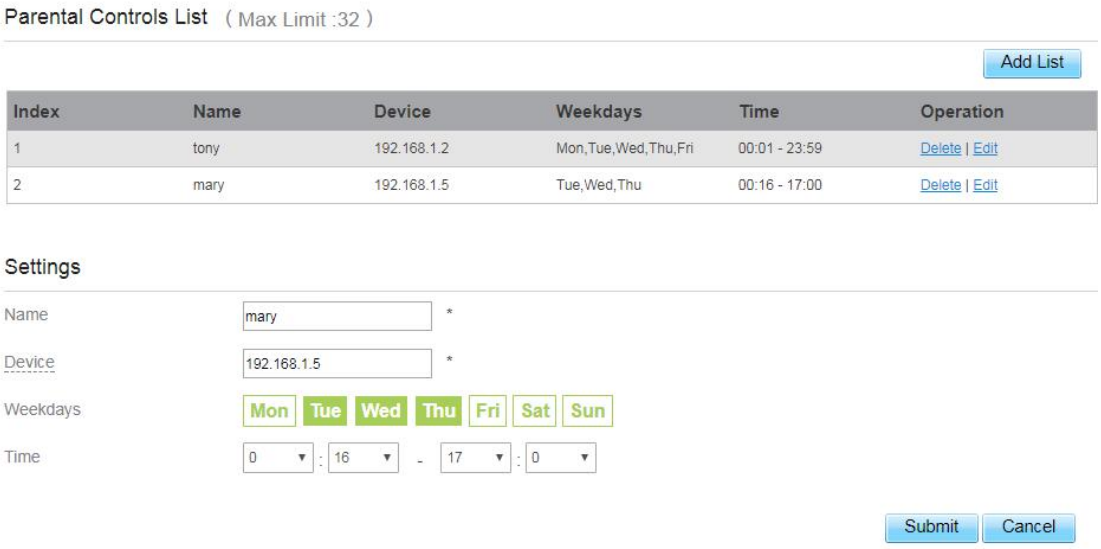


Figure 5-4-3

5.4 Firewall

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:

Choose **Firewall>Firewall Setting**.

Choose **Enable** or **Disable** to modify the configuration.

Click **Submit**. As shown in Figure 5-30.

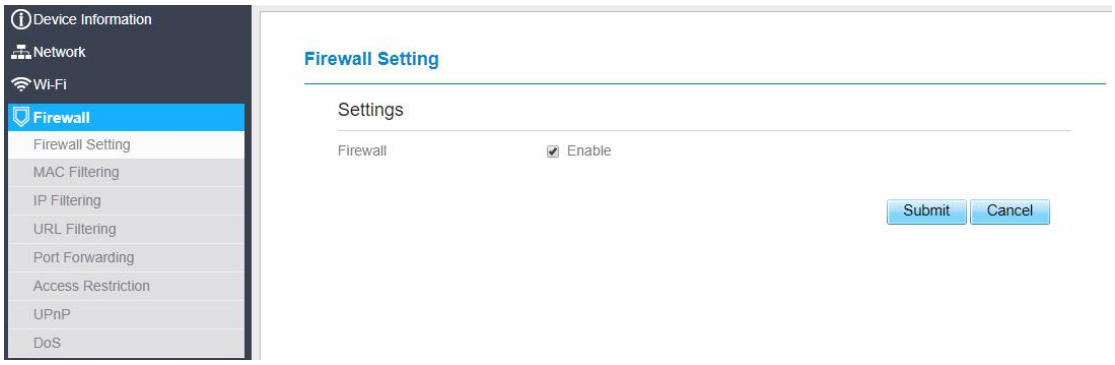


Figure 5-30

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.

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 5-31.

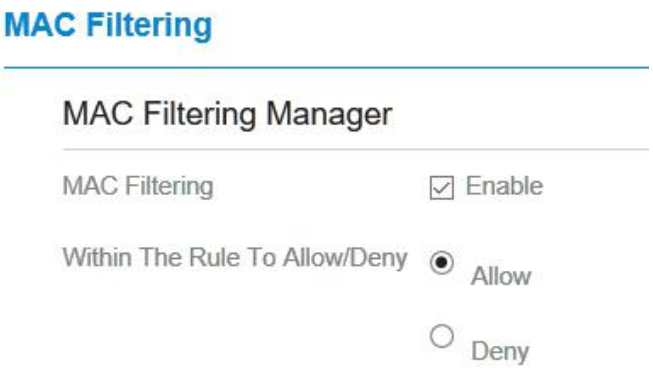


Figure 5-31

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 5-32.

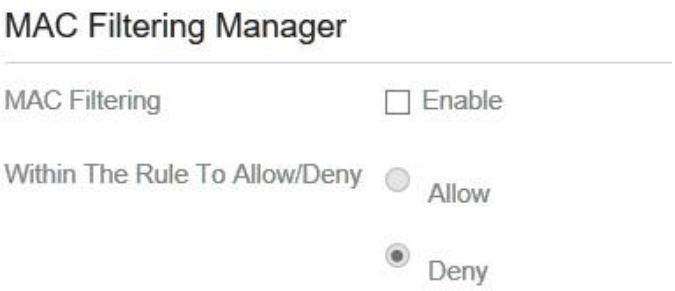


Figure 5- 32

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 5-33.

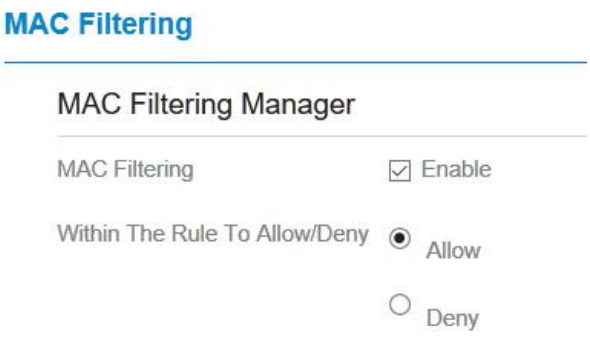


Figure 5- 33

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 5-34.

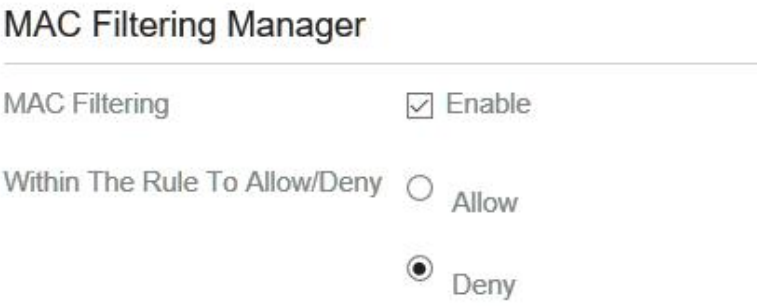


Figure 5- 34

Adding MAC Filtering rule

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

Choose **Firewall>MAC Filtering**.

Click **Add list**.

Set **MAC address**.

Click **Submit**. As shown in Figure 5-35.

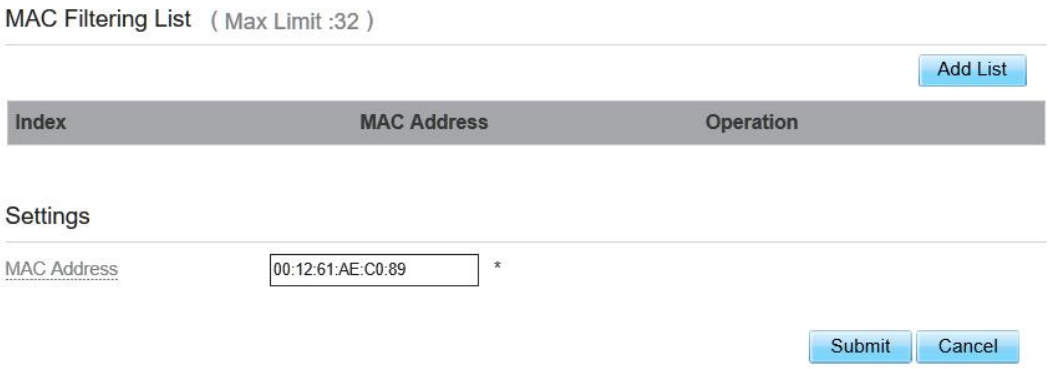


Figure 5-35

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 5-36.

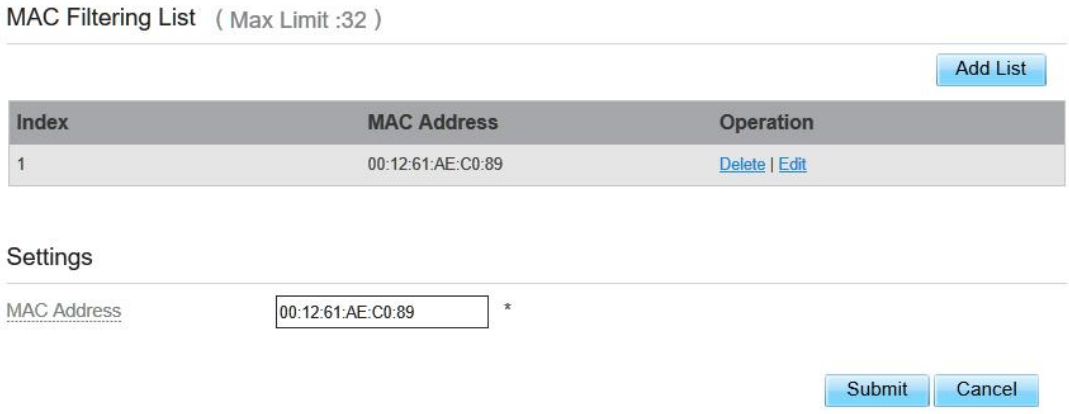


Figure 5-36

Deleting MAC Filtering rule

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

Choose **Firewall>MAC Filtering**.

Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-37.

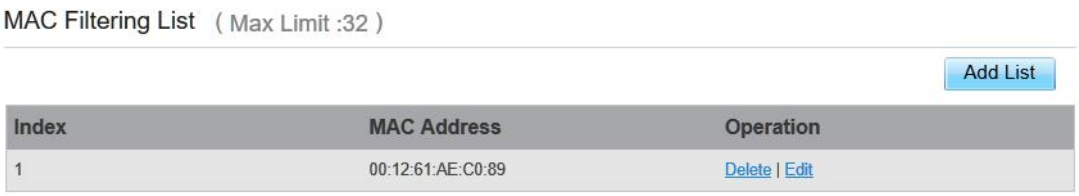


Figure 5-37

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 5-38.

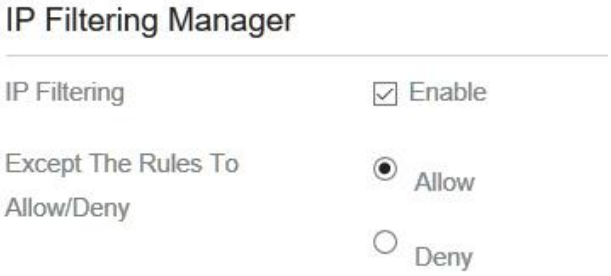


Figure 5-38

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 5-39.

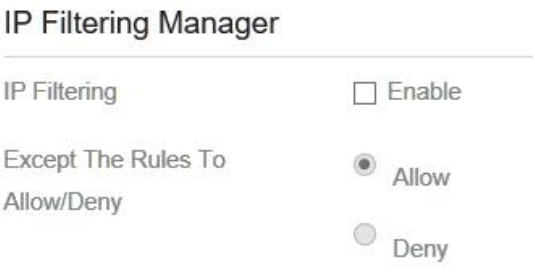


Figure 5-39

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 5-40.

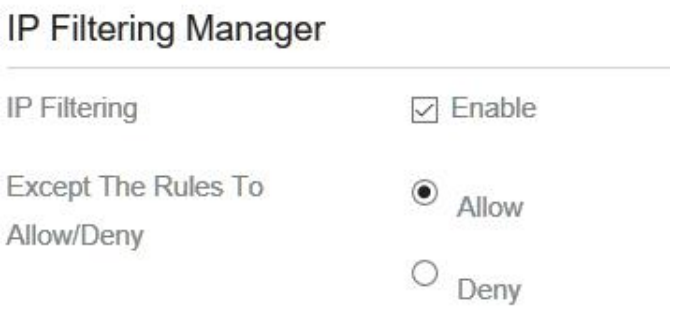


Figure 5- 40

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 5-41.

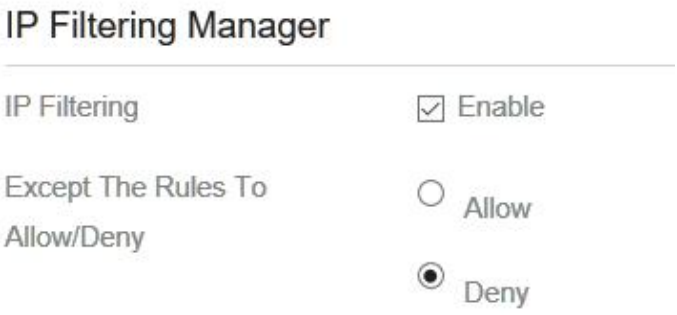


Figure 5- 41

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 5-42.

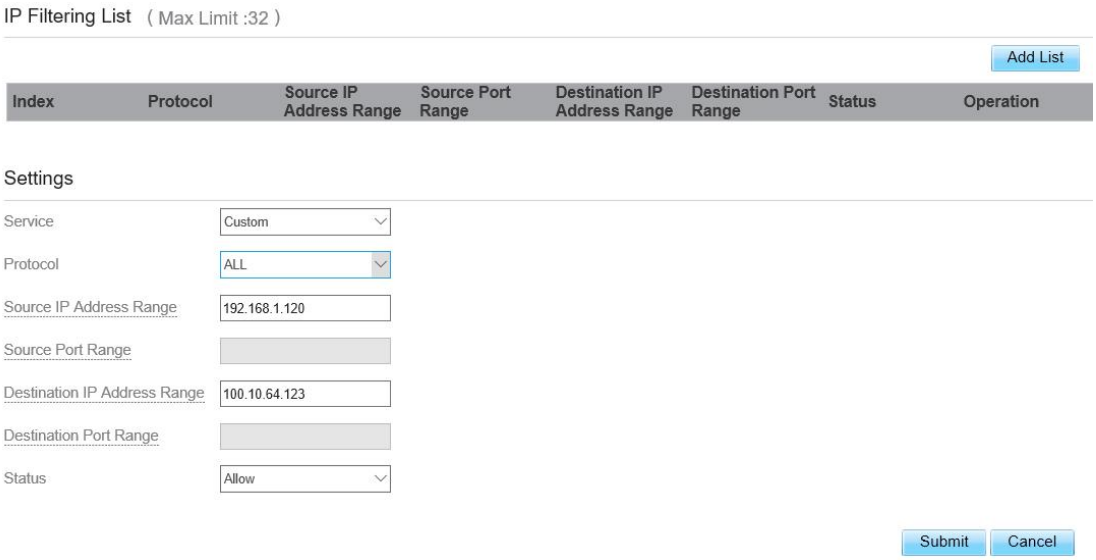


Figure 5- 42

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 5-43.

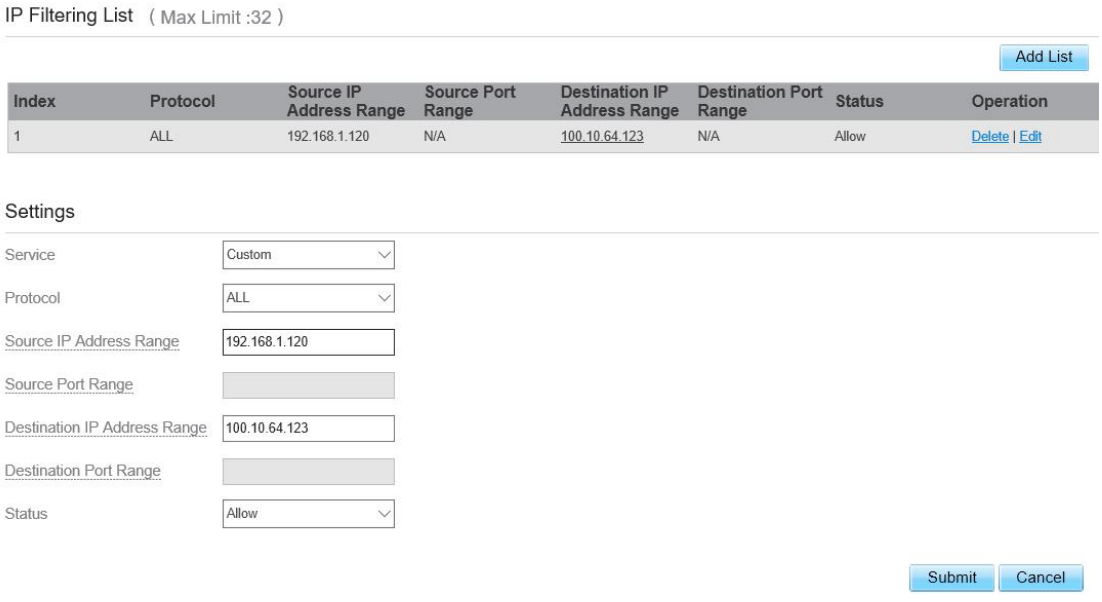


Figure 5- 43

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 5-44.

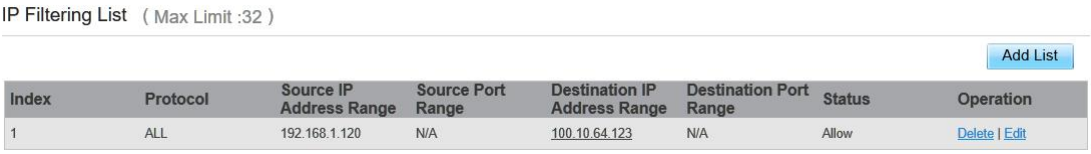


Figure 5- 44

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:

3. Choose **Firewall**>**URL Filtering**.
4. Set **URL Filtering** to **Enable**.
5. Click **Submit**. As shown in Figure 5-45.

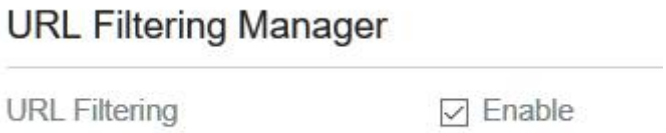


Figure 5- 45

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 5-46.

Figure 5- 46

Adding URL Filtering list

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

Choose **Firewall**>**URL Filtering**.

Click **Add list**.

Set **URL**.

Click **Submit**. As shown in Figure 5-47.

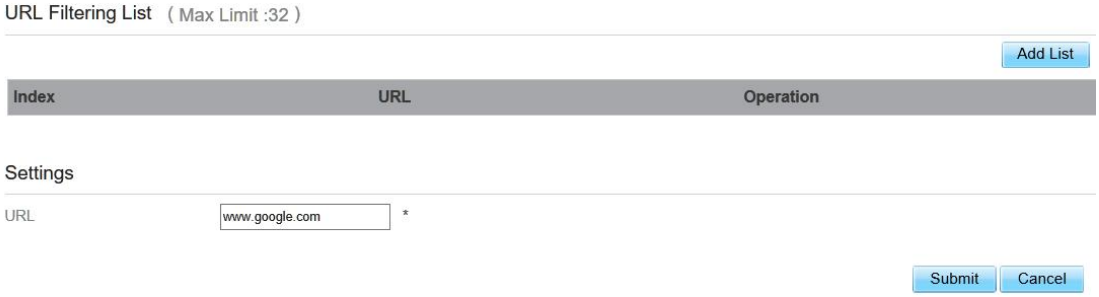


Figure 5- 47

Modify URL Filtering list

To modify a 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 5-48.

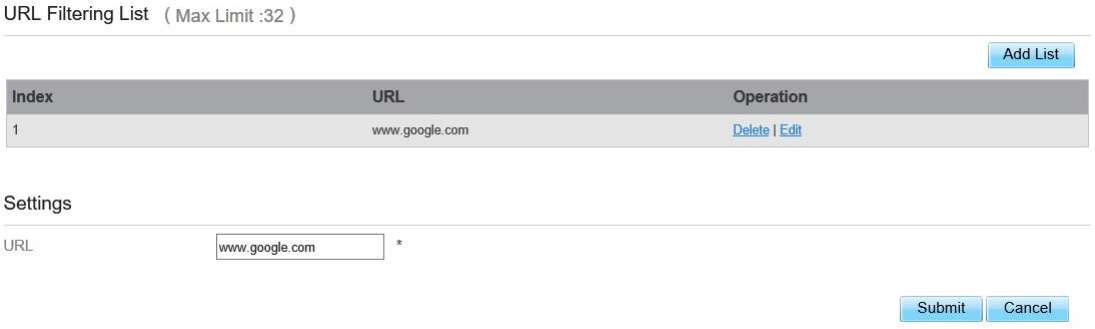


Figure 5- 48

Deleting URL Filtering list

To delete a 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 5-49.

Figure 5- 49

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:

Choose **Firewall** > **Port Forwarding**.

Click **Add list**.

Set **Service**.

Set **Protocol**.

Set **Remote port range**.

The port number ranges from 1 to 65535.

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.

Set **Local port**.

The port number ranges from 1 to 65535.

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

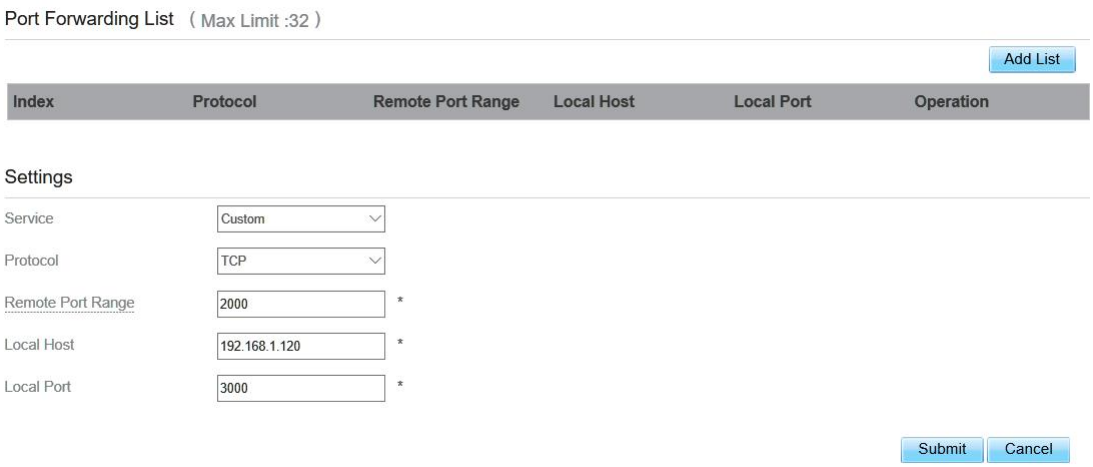


Figure 5- 50

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. Repeat steps 3 through7 in the previous procedure.
4. Click **Submit**. As shown in Figure 5-51.

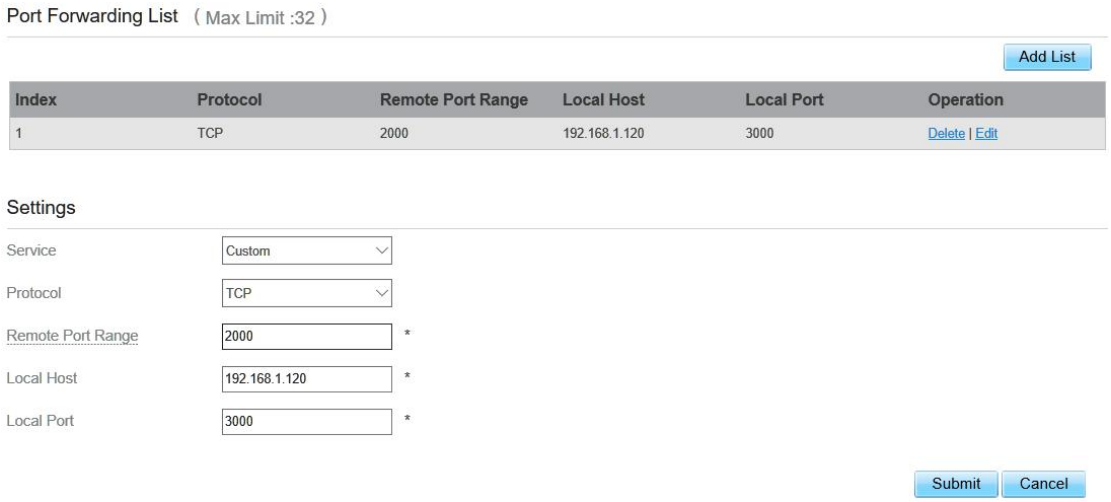


Figure 5- 51

Deleting Port Forwarding rule

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

Choose **Firewall > Port Forwarding.**

Choose the item to be deleted, and click **Delete**. As shown in Figure 5-52.

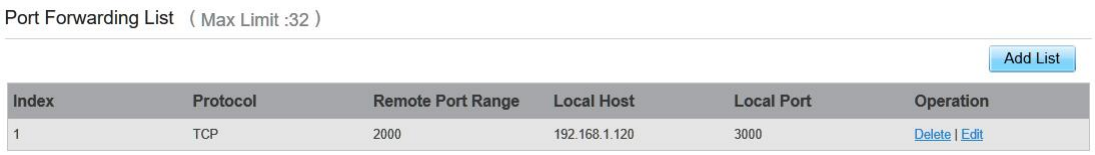


Figure 5- 52

Access Restriction

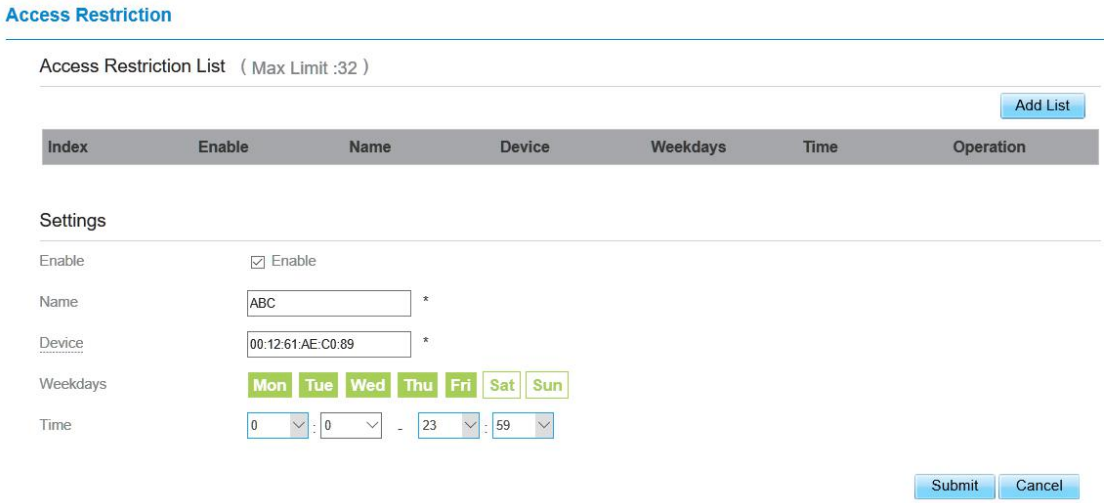


Figure 5-53

Add Access Restriction

To add a 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 a 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**.

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 5-54.

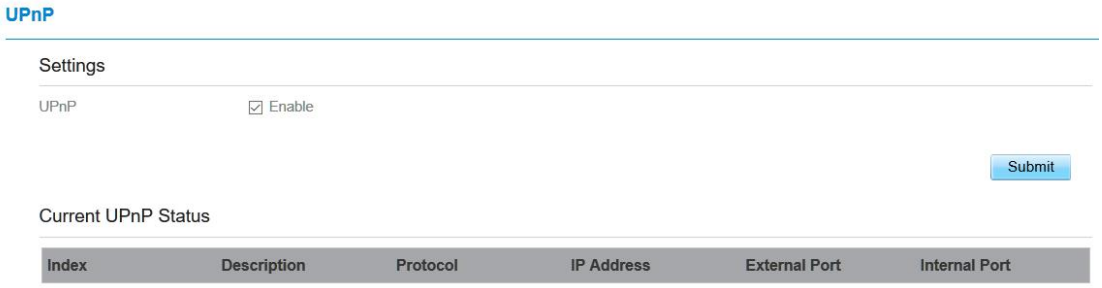


Figure 5- 54

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 5-55.

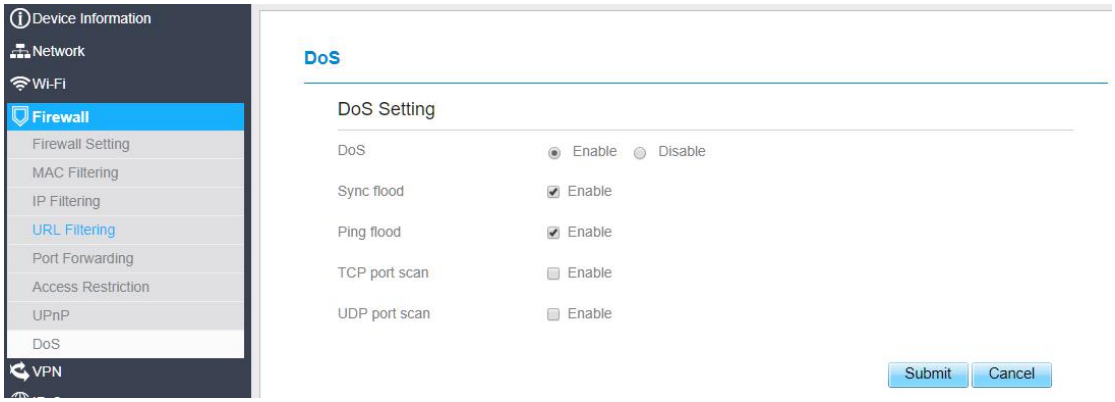


Figure 5- 55

5.6 VPN

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

To connect the VPN, perform the following steps:

Choose **VPN.**

In the **VPN Settings** area, enable VPN.

Select a protocol from **Protocol** drop-down list.

Enter **Username** and **Password**.

Click **Submit**.

You can view the status in **VPN Status** area. As shown in Figure 5-55.

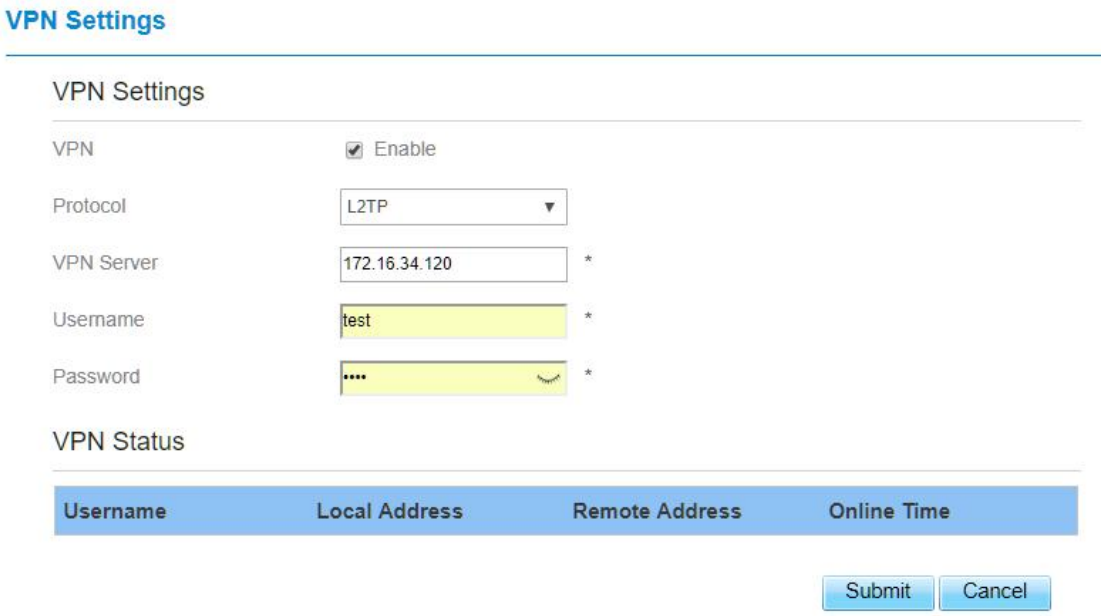


Figure 5- 55

5.7 IPv6

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

Status

The status page shows IPv6 information. As shown in Figure 5-56.

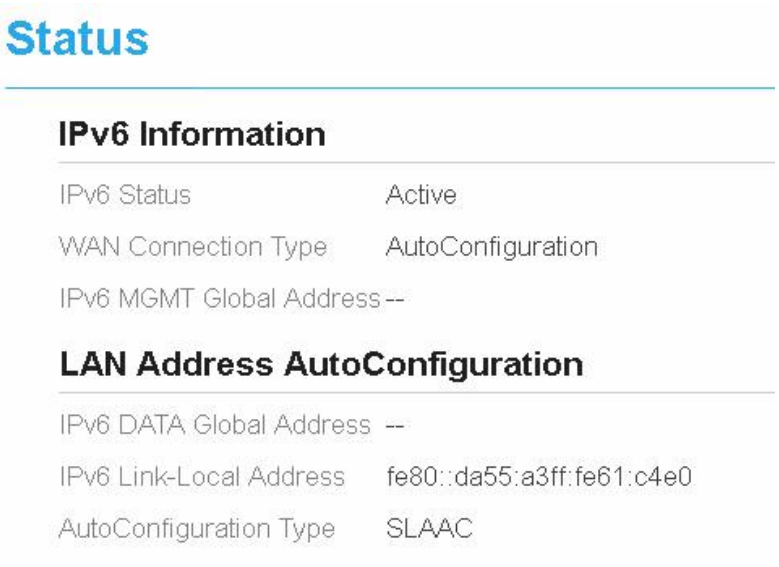


Figure 5-56

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 5-27

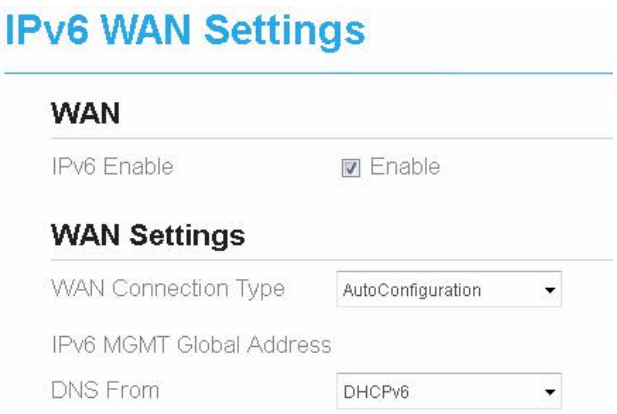


Figure 5-57

IPv6 LAN Settings

In this page, user can chose the AutoConfiguration Type. As shown in Figure 5-58.

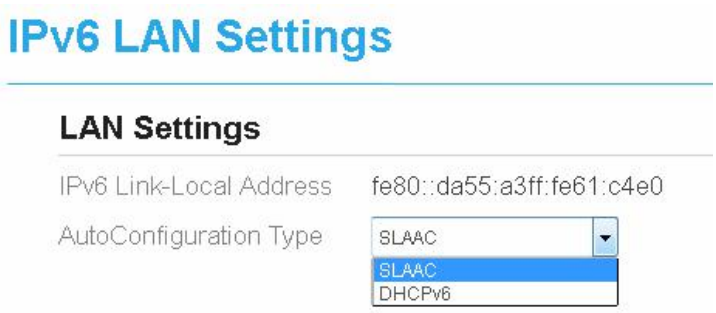


Figure 5-58

5.8 System

5.8.1 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 5-59.
   The CPE then restarts.

Figure 5- 59

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 5-60.
   The CPE is then restored to its default settings.

Figure 5- 60

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 5-61.
   The procedure for file downloading may vary with the browser you are using.

Figure 5- 61

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 choses. 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 5-62.

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

Figure 5- 62

5.8.2 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 7-5.

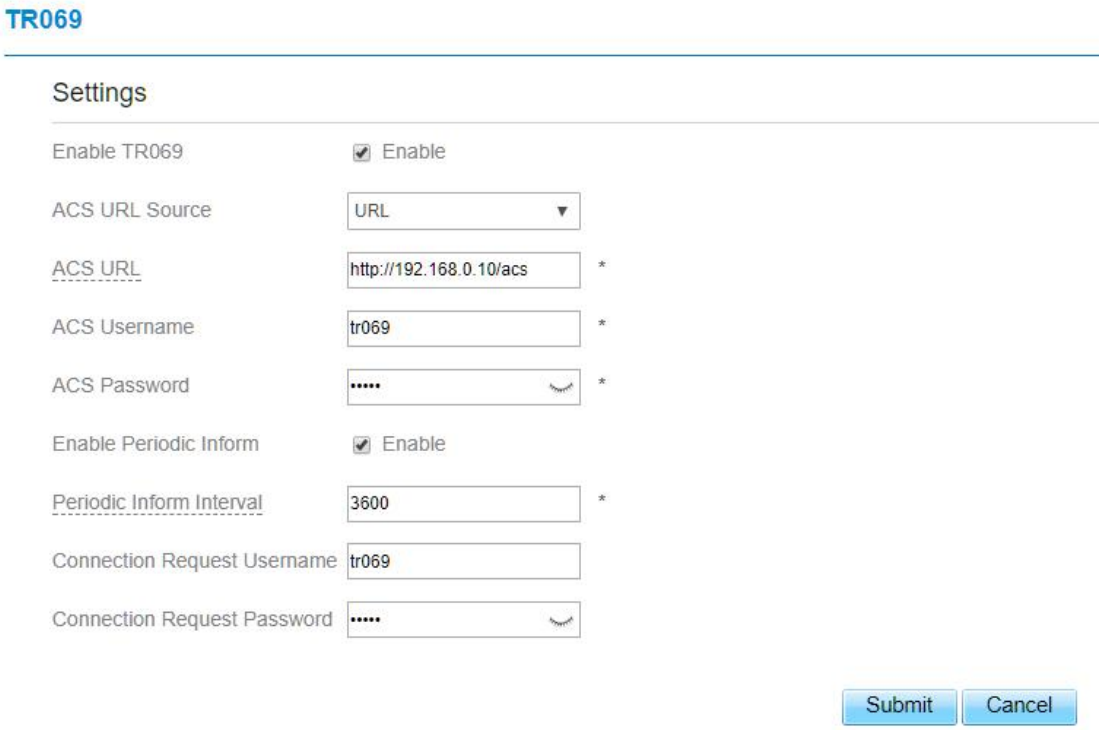


Figure 5- 63

5.8.3 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 5-64.

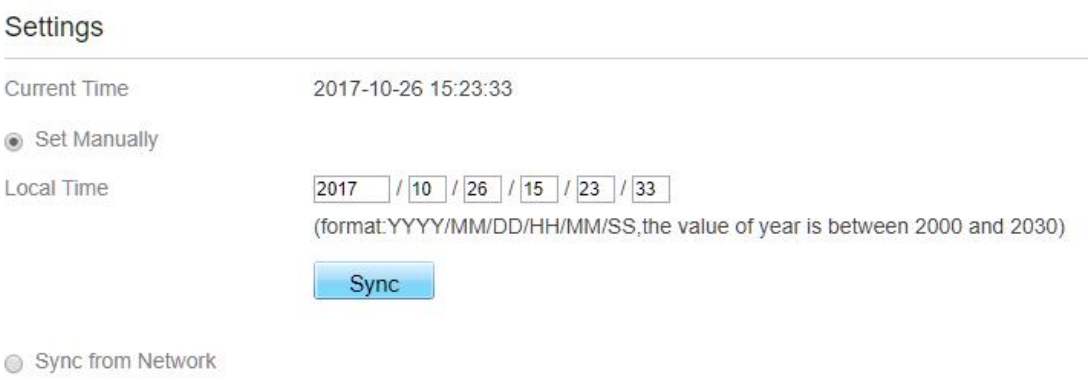


Figure 5-64

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 5-65.

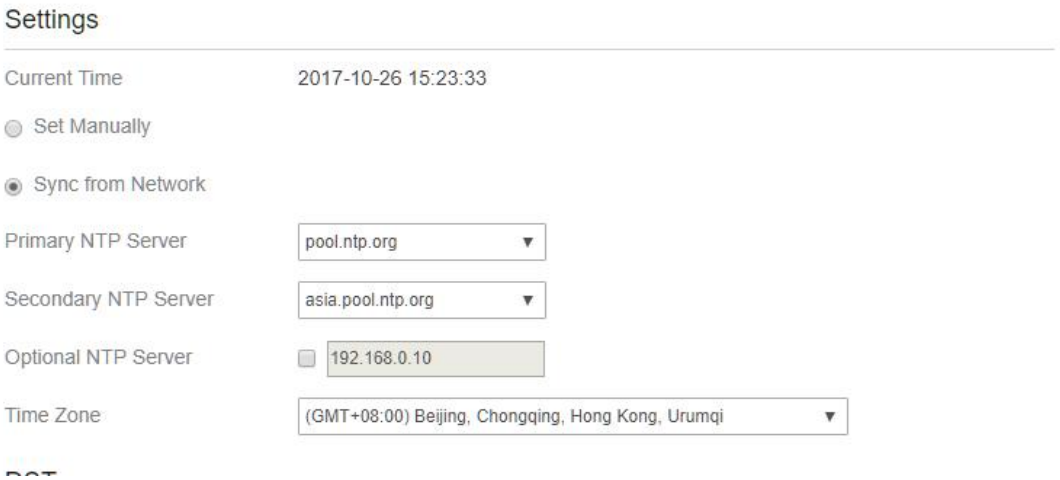


Figure 5- 65

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 5-66.

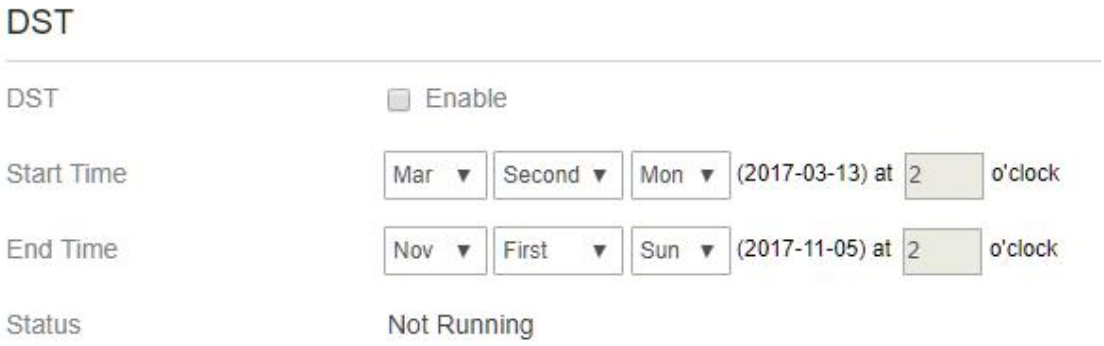


Figure 5-66

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

5.8.4 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 5-67.

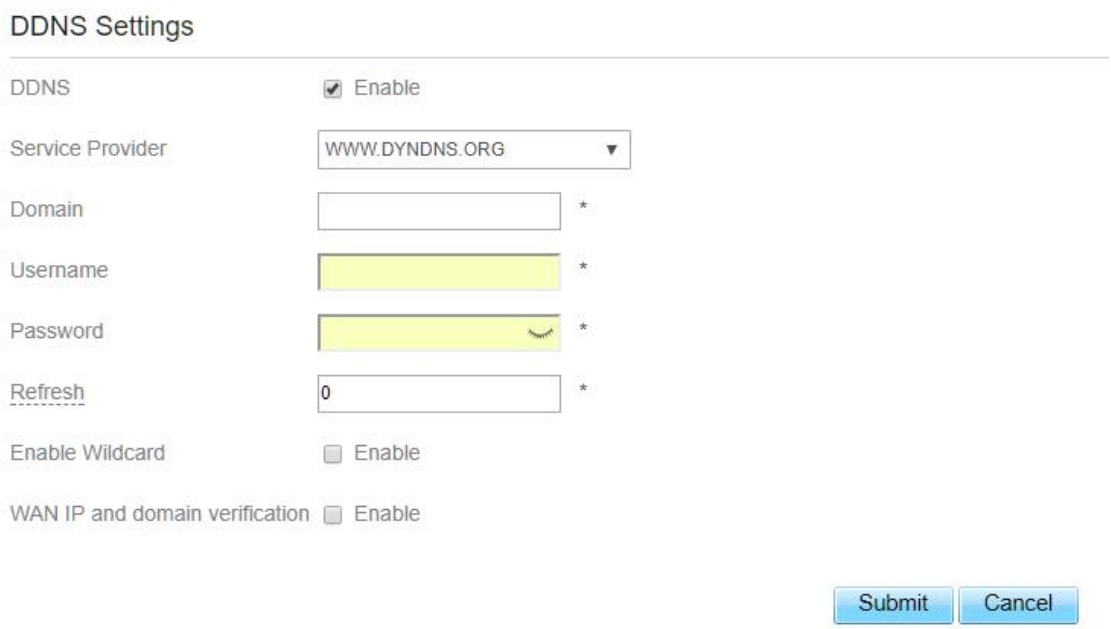


Figure 5-67

5.8.5 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:

Choose **System**>**Diagnosis**.

In the Method area, select **Ping**.

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

Set **Packet size** and **Timeout**.

Set **Count**.

Click **Ping**. As shown in Figure 5-68.

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

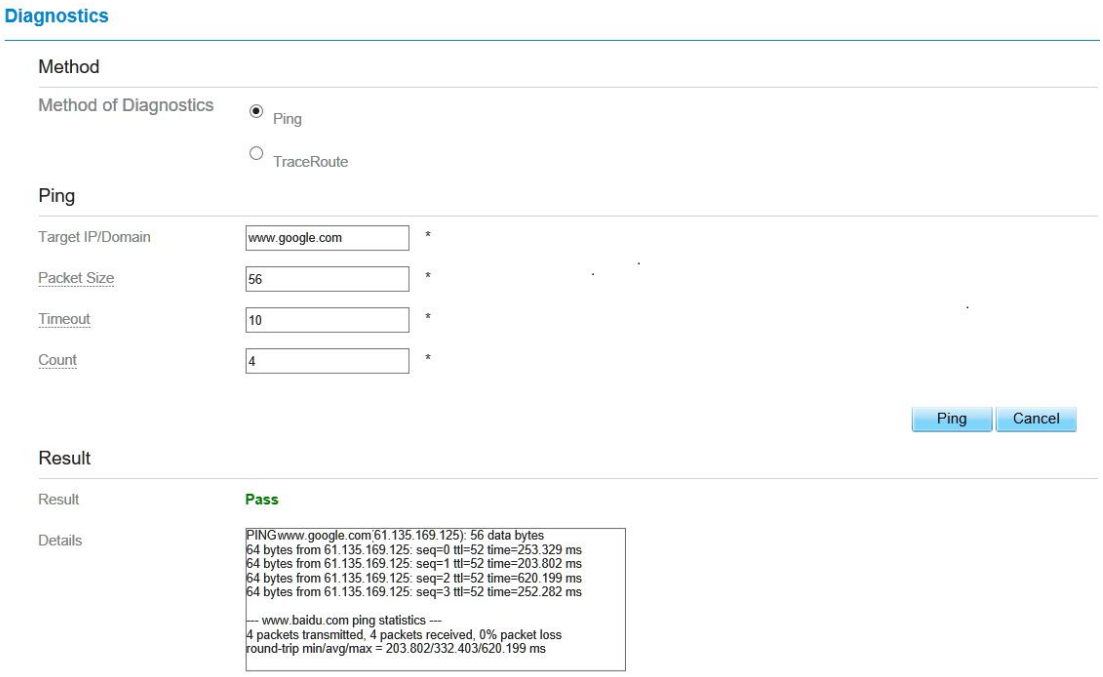


Figure 5-68

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 5-69

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

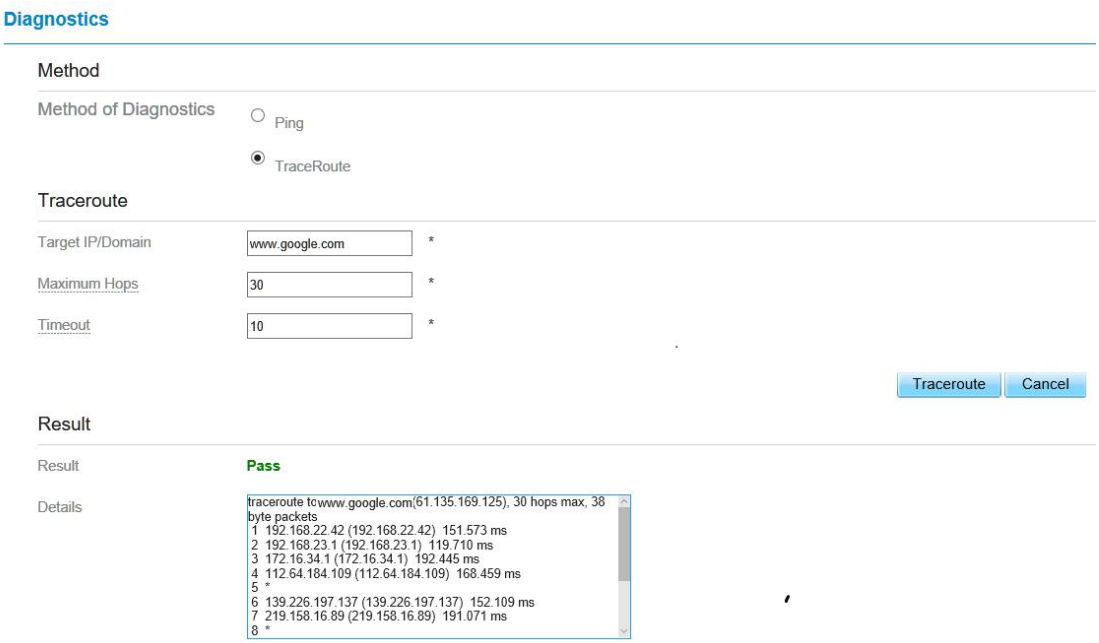


Figure 5-69

5.8.6 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 **Sbumit**. As shown in Figure 5-70.

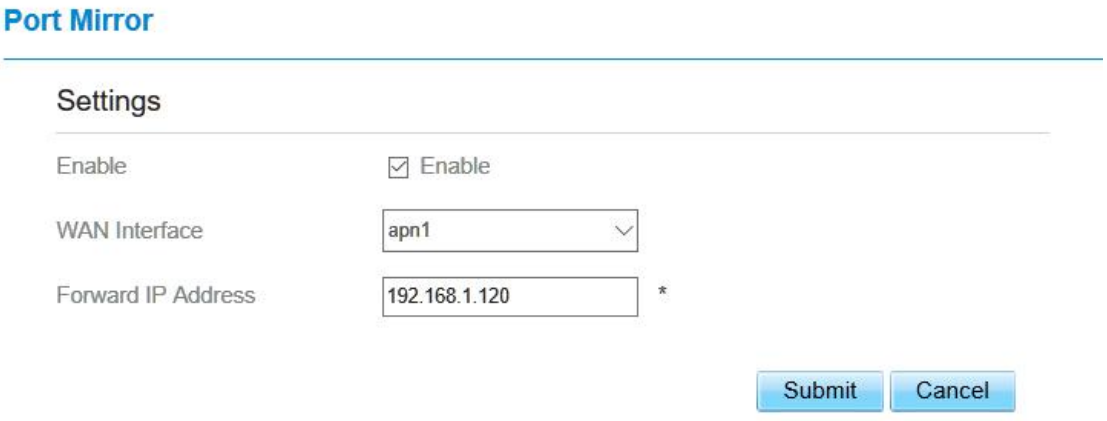


Figure 5-70

5.8.7 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 5-71.

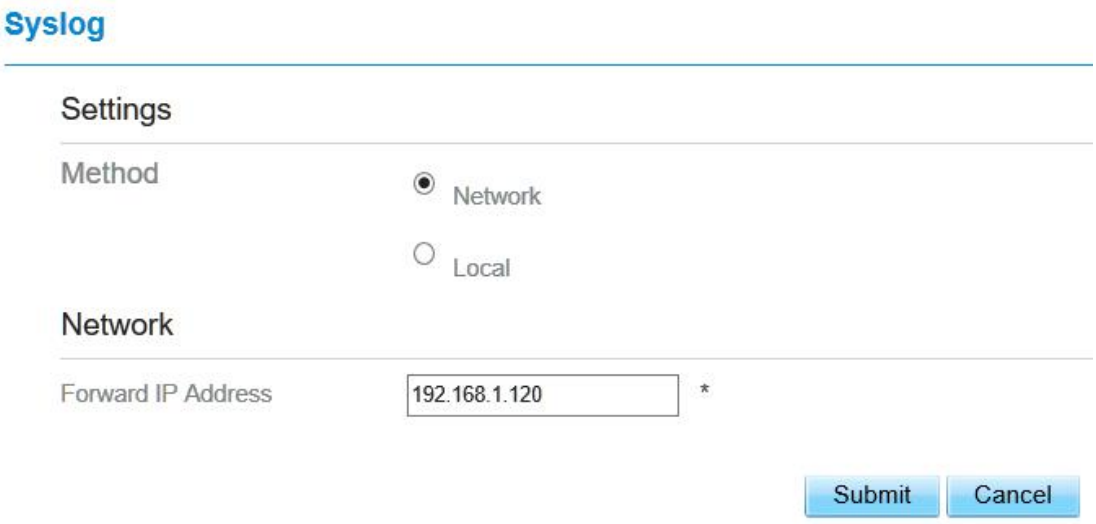


Figure 5-71

Viewing local syslog

To view the local syslog, perform the following steps:

In the **Keyword** box, set a keyword.

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 a IP address.
5. Click **Submit**. As shown in Figure 5-72.

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

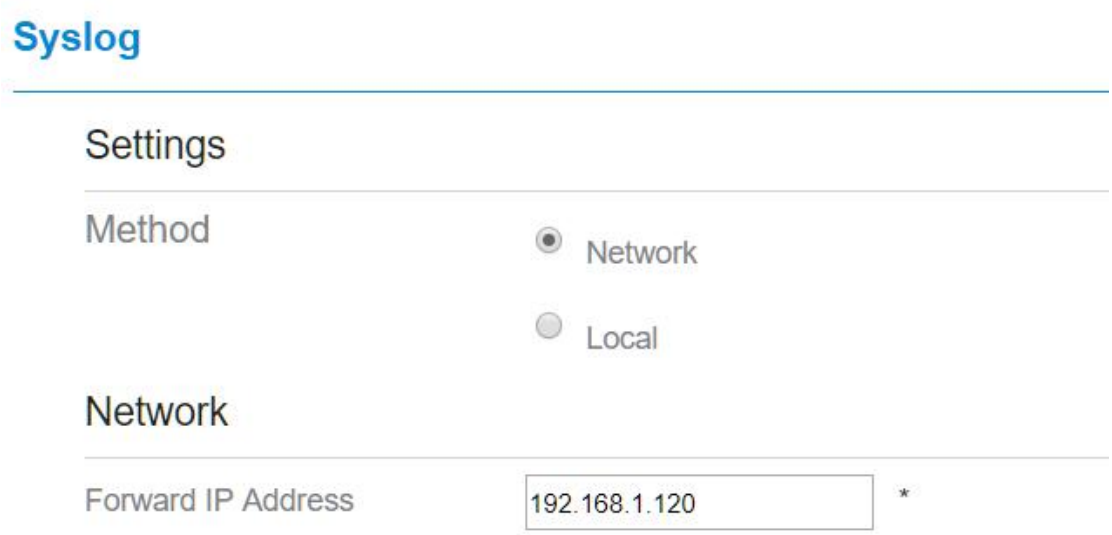


Figure 5-72

5.8.8 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 5-73.

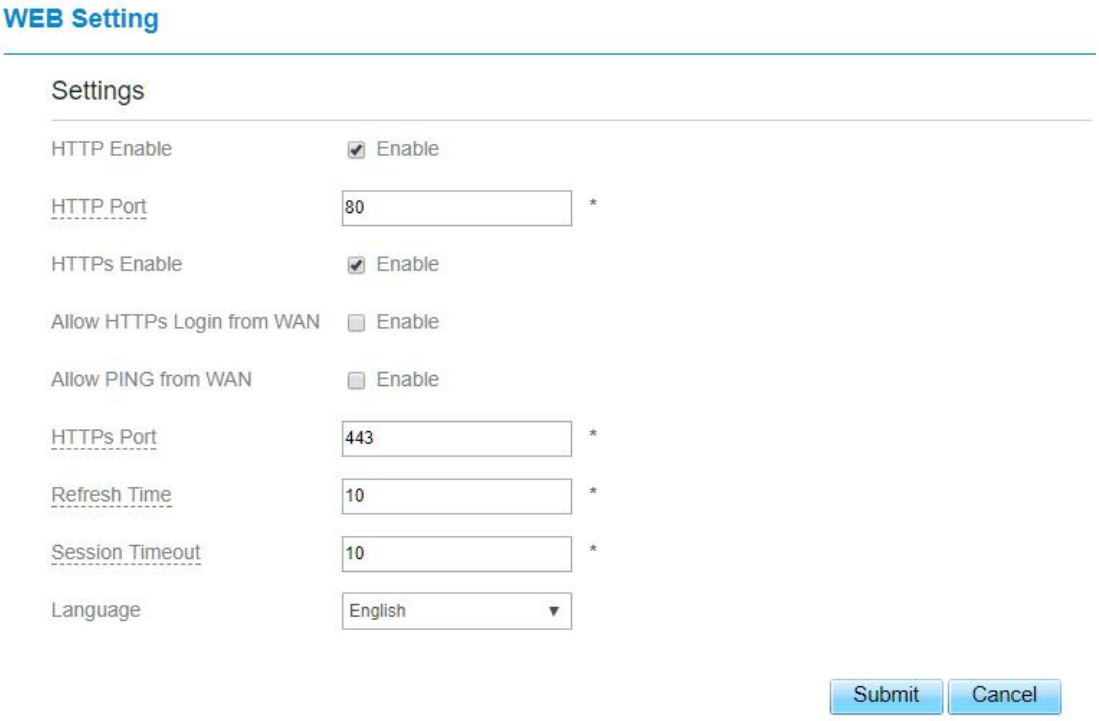


Figure 5-73

5.8.9 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 5-74.

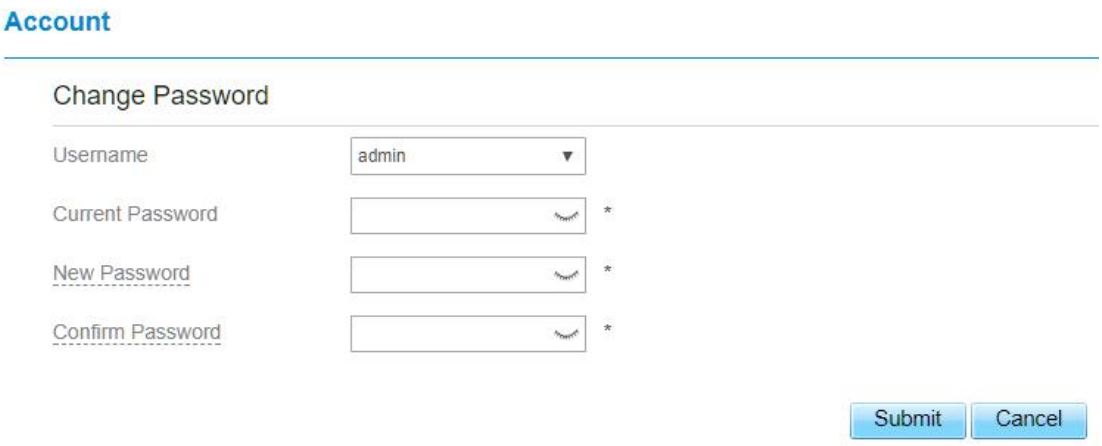


Figure 5-74

5.8.10 Logout

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

Choose **System** and click **Logout**

It will back to the login page.

6 FAQs

The POWER indicator does not turn on.

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

Fails to Log in to the web management page.

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

The Module fails to search for the wireless network.

- Check that the power adapter is connected properly.
- Check that the Module is placed in an open area that is far away from obstructions, such as concrete or wooden walls.
- Check that the Module 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 Module is overheated.

The Module will be overheated after being used for a long time. Therefore, power off the Module when you are not using it.

Check that the Module is properly ventilated and shielded from direct sunlight.

The parameters are restored to default values.

If the Module 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 Module to the desired settings.

FCC Certification Requirements.

According to the definition of mobile and fixed device is described in Part 2.1091(b), this device is a mobile device.

And the following conditions must be met:

1. This Modular Approval is limited to OEM installation for mobile and fixed applications only. The antenna installation and operating configurations of this transmitter, including any applicable source-based time- averaging duty factor, antenna gain and cable loss must satisfy MPE categorical Exclusion Requirements of 2.1091.

2. The EUT is a mobile device; maintain at least a 20 cm separation between the EUT and the user's body and must not transmit simultaneously with any other antenna or transmitter.

3. A label with the following statements must be attached to the host end product: This device contains FCC ID: 2AU8HMGL6201A.

4.To comply with FCC regulations limiting both maximum RF output power and human exposure to RF radiation, maximum antenna gain (including cable loss) must not exceed:

- ❒ <4.22dBi

5. This module must not transmit simultaneously with any other antenna or transmitter

6. The host end product must include a user manual that clearly defines operating requirements and conditions that must be observed to ensure compliance with current FCC RF exposure guidelines.

For portable devices, in addition to the conditions 3 through 6 described above, a separate approval is required to satisfy the SAR requirements of FCC Part 2.1093

If the device is used for other equipment that separate approval is required for all other operating configurations, including portable configurations with respect to 2.1093 and different antenna configurations.

For this device, OEM integrators must be provided with labeling instructions of finished products. Please refer to KDB784748 D01 v07, section 8. Page 6/7 last two paragraphs:

A certified modular has the option to use a permanently affixed label, or an electronic label.

For a permanently affixed label, the module must be labeled with an FCC ID - Section 2.926 (see 2.2 Certification (labeling requirements) above). The OEM manual must provide clear instructions explaining to the OEM the labeling requirements, options and OEM user manual instructions that are required (see next paragraph).

For a host using a certified modular with a standard fixed label, if (1) the module's FCC ID is not visible when installed in the host, or (2) if the host is marketed so that end users do not have straightforward commonly used methods for access to remove the module so that the FCC ID of the module is visible; then an additional permanent label referring to the enclosed module:"Contains Transmitter Module FCC ID: 2AU8HMGL6201A" or "Contains FCC ID: 2AU8HMGL6201A" must be used. The host OEM user manual must also contain clear instructions on how end users can find and/or access the module and the FCC ID.

The final host / module combination may also need to be evaluated against the FCC Part 15B criteria for unintentional radiators in order to be properly authorized for operation as a Part 15 digital device.

The user's 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.

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.

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

To ensure compliance with all non-transmitter functions the host manufacturer is responsible for ensuring compliance with the module(s) installed and fully operational. For example, if a host was previously authorized as an unintentional radiator under the Declaration of Conformity procedure without a transmitter certified module and a module is added, the host manufacturer is responsible for ensuring that the after the module is installed and operational the host continues to be compliant with the Part 15B unintentional radiator requirements.