

WF820+ Outdoor LTE CPE

With Wi-Fi Router

User Manual

WF820+ Router

FCC ID: SRQ-WF820R

LTE CPE

FCC ID: SRQ-WF820E

Index

Index	2
1 Getting Started	5
1.1 Welcome to the CPE	5
1.2 Computer Configuration Requirements	5
1.3 Logging In to the Web Management Page	5
2 Overview.....	6
2.1 Viewing the System Information	6
2.2 Viewing the Version Information	7
2.3 Viewing CPU Usage	7
2.4 Viewing Memory Usage	8
2.5 Viewing 4G Status	8
2.6 Viewing LAN Status	8
2.7 Viewing Wi-Fi Status.....	9
2.8 Viewing Throughput Statistics.....	9
2.9 Viewing Device List.....	10
3 Network.....	10
3.1 WAN Settings.....	10
3.1.1 Network Mode	10
3.2 LTE Settings.....	10
3.2.1 LTE Setting	10
3.2.2 Connect Method Setting.....	11
3.3 APN Management	13
3.3.1 APN Settings in NAT mode	13
3.3.2 APN Settings in BRIDGE mode	14
3.3.3 APN list.....	15
3.4 PIN Management	15
3.4.1 Viewing the Status of the USIM Card.....	16
3.4.2 Enabling PIN Verification	16
3.4.3 Disabling PIN Verification	16
3.4.4 Verifying the PIN	16
3.4.5 Changing the PIN.....	17
3.4.6 Setting Automatic Verification of the PIN	17
3.4.7 Verifying the PUK.....	17
3.5 LAN Setting.....	18
3.5.1 Setting LAN Host Parameters	18
3.5.2 Configuration the DHCP Server.....	18
3.5.3 Bundled Address List	19
3.6 DMZ Settings	20
3.7 Static Route	20
3.7.1 Add Static Route	20
3.7.2 Modify Static Route	21
3.7.3 Delete Static Route.....	22

4 Wi-Fi	22
4.1 WLAN Setting	22
4.1.1 Setting General Parameters	22
4.1.2 WPS Settings.....	23
4.2 Setting SSID Profile	23
4.3 Access Management.....	25
4.3.1 Setting the Access Policy	25
4.3.2 Managing the Wi-Fi Access List	26
4.4 WDS.....	27
5 Security	28
5.1 MAC Filtering.....	28
5.1.1 Enabling MAC Filter.....	28
5.1.2 Disabling MAC Filter	28
5.1.3 Setting Allow access network within the rules.....	29
5.1.4 Setting Deny access network within the rules.....	29
5.1.5 Adding MAC Filtering rule.....	29
5.1.6 Modifying MAC Filtering rule.....	30
5.1.7 Deleting MAC Filtering rule.....	30
5.2 IP Filtering	30
5.2.1 Enabling IP Filtering	31
5.2.2 Disabling IP Filtering.....	31
5.2.3 Setting Allow access network outside the rules	31
5.2.4 Setting Deny access network outside the rules	32
5.2.5 Adding IP Filtering rule	32
5.2.6 Modifying IP Filtering rule	33
5.2.7 Deleting IP Filtering rule.....	34
5.3 URL Filtering	34
5.3.1 Enabling URL Filtering.....	34
5.3.2 Disabling URL Filtering.....	34
5.3.3 Adding URL Filtering list	35
5.3.4 Modify URL Filtering list	35
5.3.5 Deleting URL Filtering list.....	36
5.4 Port Forwarding.....	36
5.4.1 Adding Port Forwarding rule	36
5.4.2 Modifying Port Forwarding rule	37
5.4.3 Deleting Port Forwarding rule.....	38
5.5 UPnP	38
5.6 DOS.....	38
6 VPN Setting	39
7 VOIP	40
7.1 View VOIP Information	40
7.2 Configuring SIP Server	40
7.3 Configuring SIP Account	41
7.4 Advanced SIP	42

8 IPv6.....	42
8.1 Status.....	42
8.2 IPv6 WAN Settings	43
8.3 IPv6 LAN Settings	43
9 System.....	44
9.1 Maintenance	44
9.1.1 Restart	44
9.1.2 Factory Reset.....	44
9.1.3 Backup Configuration File	45
9.1.4 Upload Configuration File	45
9.2 Version Manager	45
9.2.1 Viewing Version Info	46
9.2.2 Local Upgrade.....	46
9.2.3 Online Upgrade	47
9.3 Module Manager.....	47
9.3.1 Viewing Version Info	47
9.3.2 Module Upgrade.....	48
9.4 FTP auto upgrade	48
9.5 TR069	49
9.6 FOTA	50
9.7 Date & Time	51
9.8 DDNS	52
9.9 Iperf.....	53
9.10 Diagnosis	54
9.10.1 Ping	54
9.10.2 Traceroute.....	55
9.11 Port Mirror	56
9.12 Syslog.....	56
9.13 Account	56
9.14 WEB Setting.....	57
9.15 Logout	58
10 FAQs	58

1 Getting Started

1.1 Welcome to the CPE

In this document, the LTE (Long Term Evolution) CPE (customer premises equipment) will be replaced by the CPE. Carefully read the following safety symbols to help you use your CPE safely and correctly:



Additional information



Optional methods or shortcuts for an action



Potential problems or conventions that need to be specified

1.2 Computer 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

1.3 Logging In to the Web Management Page

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

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 CPE.

1. Connect the CPE 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.

You can log in to the web management page after the password is verified. As shown in Figure 1-2.

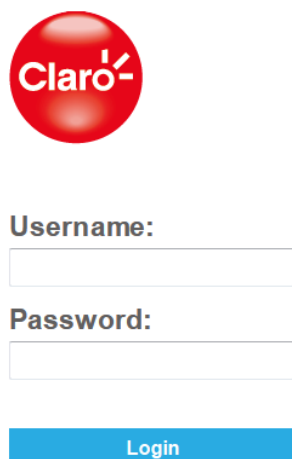


Figure 1-2

 The default user name is **1admin0**, and password is **ltecl4r0**. If you want to view or configure the CPE more, you should use the super account to log in to the web management page. Please contact customer service for the super account.

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

2.1 Viewing the System Information

To view the System Information, perform the following steps:

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

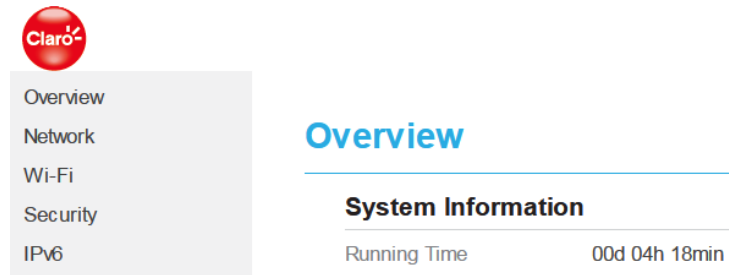


Figure 2-1

2.2 Viewing the Version Information

To view the Version Information, perform the following steps:

1. Choose **Overview**;
2. In the **Device Information** area, view the version information, such as Product name, Software version, UBoot version. As shown in Figure 2-2.

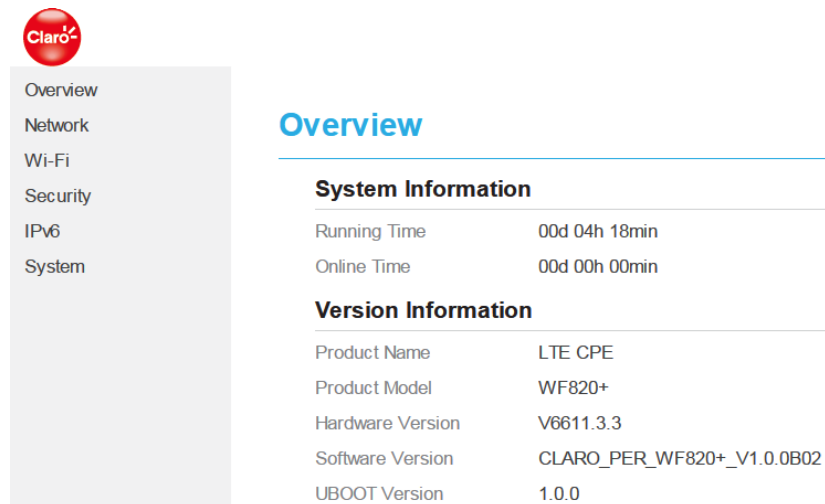


Figure 2-2

2.3 Viewing CPU Usage

To view the CPU usage, perform the following steps:

1. Choose **Overview**;
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 2-3.

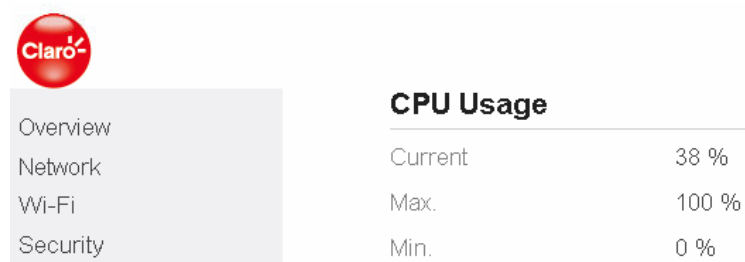


Figure 2-3

2.4 Viewing Memory Usage

To view the memory usage, perform the following steps:

1. Choose **Overview**;
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 2-4.



Memory Usage	
Total	61672 KB
Current	36 %
Max.	38 %
Min.	27 %

Figure 2-4

2.5 Viewing 4G Status

To view the 4G network status, perform the following steps:

1. Choose **Overview**;
2. In the **LTE Status** area, view the information about USIM card status, Connect status, Operator, Current Mobile Network, Signal quality and so on. As shown in Figure 2-5.



LTE Status	
USIM Card Status	USIM Normal
Status	Connected
Operator	China Unicom
RSSI	0 dBm
RSRP0	-115.15 dBm
RSRP1	-117.66 dBm
RSRQ	-12.87 dB
SINR	-0.79 dB
Cell ID	12642051

Figure 2-5

2.6 Viewing LAN Status

To view the LAN status, perform the following steps:

1. Choose **Overview**;
2. In the **LAN Status** area, view the LAN status, such as Mac address, IP address and Subnet mask.
As shown in Figure 2-6.



Overview	LAN Status
Network	MAC Address D8:55:A3:61:C4:E0
Wi-Fi	IP Address 192.168.1.1
Security	Subnet Mask 255.255.255.0
VoIP	

Figure 2-6

2.7 Viewing Wi-Fi Status

To view the Wi-Fi status, perform the following steps:

1. Choose **Overview**;
2. In the **Wi-Fi Status** area, view the information about Wi-Fi status, SSID, Chanel NO., MAC address and WDS status. As shown in Figure 2-7.



Overview	Wi-Fi Status
Network	WLAN Enable
Wi-Fi	SSID CLARO_C4E2
Security	Channel 6
VoIP	Mode 802.11b/g/n(Auto)
IPv6	MAC Address D8:55:A3:61:C4:E2
System	WDS Host Mode

Figure 2-7

2.8 Viewing Throughput Statistics

To view the throughput statistics, perform the following steps:

1. Choose **Overview**;
2. In the **Throughput Statistics** area, view the throughput statistics, such as WAN throughput and LAN throughput. As shown in Figure 2-8.

Throughput Statistics

Port	Received				Sent			
	Total Traffic	Packets	Errors	Dropped	Total Traffic	Packets	Errors	Dropped
CLARO DATOS TDD	97 KB	1119	0	0	171 KB	1663	0	0
CLARO VOZ TDD	930 Bytes	3	0	0	227 KB	604	0	0
APN3	--	--	--	--	--	--	--	--
APN4	--	--	--	--	--	--	--	--
LAN	1.98 MB	37448	0	0	3.69 MB	23653	0	0

Figure 2-8

2.9 Viewing Device List

To view the device list, perform the following steps:

1. Choose **Overview**;
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 2-9.

Device List

Index	Device Name	MAC Address	IP Address	Lease Time	Type
1	wangfei-PC	00:e0:4c:36:02:d3	192.168.1.122	00d 00h 35min	LAN,DHCP

Figure 2-9

3 Network

3.1 WAN Settings

3.1.1 Network Mode

To set the network mode, perform the following steps:

1. Choose **Network >WAN Settings**;
2. In the **Network Mode** area, select a mode between **BRIDGE** and **NAT**;
3. Click **Submit**. As shown in Figure 3-1.

The screenshot shows the 'WAN Settings' page. Under the 'Network Mode' section, there are two dropdown menus. The first is 'WAN Interface' with 'LTE over Ether' selected. The second is 'Network Mode' with a dropdown menu open showing three options: 'ROUTER', 'NAT' (which is highlighted in blue), and 'BRIDGE'.

Figure 3-1

3.2 LTE Settings

3.2.1 LTE Setting

To set the LTE network, perform the following steps:

1. Choose **Network >LTE Settings**;
2. In the **Setting** area, you can set the configuration of LTE network;

3. In the **LTE Settings** 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 3-2.

LTE Settings

Module Information

Module Model	MLH7872
Module Version	4.2.2.0-30436-BYPASS-1.1.1
IMEI	860524031509399
IMSI	460015630770541

Settings

Status	Connected
Connect Method	Auto
Scan Mode	FullBand
Frequency(EARFCN)	Click For Setting

Status

DL Frequency	2565000 KHz
UL Frequency	2565000 KHz
RSSI	-71 dBm
RSRP0	-115.64 dBm

Figure 3-2

3.2.2 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 3-3.

Settings

Status	Connected
Connect Method	Auto Manual Auto
Scan Mode	
Frequency(EARFCN)	Click For Setting

Figure 3-3

3.2.2.1 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 3-4.

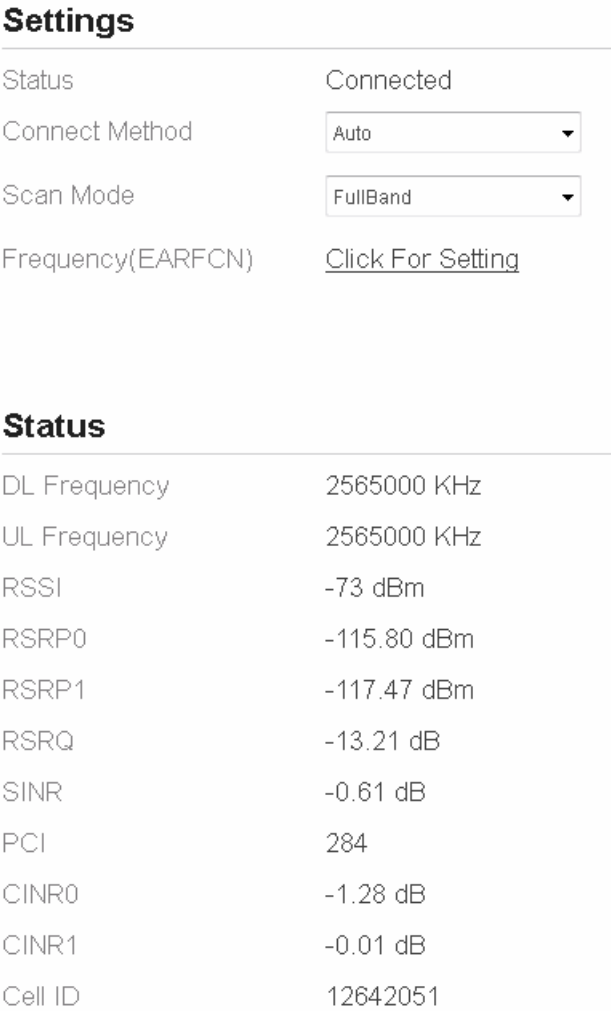


Figure 3-4

3.2.2.2 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 3-5.

Settings

Status

Disconnected

Connect Method

Manual

Connect

Scan Mode

FullBand

Frequency(EARFCN)

Click For Setting

Status

DL Frequency

2565000 KHz

UL Frequency

2565000 KHz

RSSI

-73 dBm

RSRP0

-115.75 dBm

RSRP1

-117.72 dBm

RSRQ

-14.02 dB

SINR

0.18 dB

PCI

284

CINR0

-1.24 dB

CINR1

-0.37 dB

Figure 3-5

3.3 APN Management

3.3.1 APN Settings in NAT mode

To set and manage APN in NAT mode, perform the following steps:

1. Choose **Network>APN Management**.
2. In the **APN Management** area, you can set the APN.
3. Choose a **APN number** which you want to set.
4. 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.
5. If you want set a APN as **default gateway**, you should check that is enabled.
6. Select a APN type from the drop-down list, such as VoIP, TR069 or VoIP+TR069.
7. Click **Submit**. As shown in Figure 3-6.

APN Management

APN Selection

APN Number # 1 ▼

APN Settings

Enable ☒ Enable

Name CLARO DATOS TDD *

APN Name datace.claro.pe

Authentication Type NONE ▼

PDN Type IPv4v6 ▼

MTU 1500 (576-1500)

Default Gateway ☒ Enable

Apply To No Specified ▼

Figure 3-6

3.3.2 APN Settings in BRIDGE mode

If you want to set the CPE work in bridge mode, please set and manage APN performing the following steps:

1. Choose **Network>WAN Settings**.
2. Set the network mode as **BRIDGE**.
3. Choose **Network> APN Management**.
4. In the **APN Management** area, you can set the APN.
5. Choose a **APN number** which you want to set.
6. In the **APN Settings** area, set the mode as **Bridge**.
7. Set the APN parameters, such as enable or disable the APN, APN name, username, password and so on.
8. In the **LAN Port Settings** list, select a LAN port you want to use as bridge mode.
9. Click **Submit**. As shown in Figure 3-7.

APN Management

APN Selection

APN Number

2

APN Settings

Enable

☒ Enable

Mode

BRIDGE

* (If the value is 'BRIDGE', the 'Apply To' option will be 'No Specified')

Name

CLARO VOZ TDD

*

APN Name

voip.claro.pe

Authentication Type

NONE

PDN Type

IPv4v6

MTU

1500

(576-1500)

Bundled LAN port

APN Name	LAN 1	LAN 2	LAN 3
CLARO VOZ TDD	☐	☒	☐

Submit

Cancel

Figure 3-7

3.3.3 APN list

To view the APN list, perform the following steps:

1. Choose **Network>APN Management**.
2. In the **APN list** area you can view the APN list. As shown in the figure 3-8.

APN List					
APN Name	Enable	Mode	Default Gateway	Apply To	LAN Port
CLARO DATOS TDD	Enable	NAT	Enable	--	--
CLARO VOZ TDD	Enable	NAT	--	VOIP	--
APN3	Disable	NAT	--	--	--
APN4	Disable	NAT	--	--	--

Figure 3-9

3.4 PIN Management

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

1. Enable or disable the PIN verification.
2. Verify the PIN.
3. Change the PIN.
4. Set automatic verification of the PIN. As shown in Figure 3-9.

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
Remember My PIN	☐ Enable
PIN	* 4-8 digit
Remaining Attempts	3

Submit

Cancel

Figure 3-9

3.4.1 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.

3.4.2 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**.

3.4.3 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**.

3.4.4 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**.

3.4.5 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**.

3.4.6 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**.

3.4.7 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.
5. Click **Submit**.

3.5 LAN Setting

3.5.1 Setting LAN Host Parameters

By default, the IP address is 192.168.1.1 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 Setting**>**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 3-10.

LAN Settings

LAN Host Settings

IP Address	192.168.1.1	*
Subnet Mask	255.255.255.0	* Format 255.255.255.*

DHCP Settings

DHCP Server	☒ Enable	
Start IP Address	192.168.1.2	*
End IP Address	192.168.1.250	*
Lease Time	60	* minutes (2~1440)

Figure 3-10

3.5.2 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 2 to 1440 minutes. It is recommended to retain the default value.

6. Click **Submit**. As shown in Figure 3-11.

DHCP Settings

DHCP Server	☒ Enable
Start IP Address	192.168.1.2 *
End IP Address	192.168.1.250 *
Lease Time	60 * minutes (2~1440)

Figure 3-11

3.5.3 Bundled Address List

You can bind an IP address to a device based on its MAC address. The device will receive the same IP address each time it accesses the DHCP server. For example, you can bind an IP address to an FTP server on the LAN.

To add an item to the setup list, perform the following steps:

1. Choose **Network Setting > LAN Settings**.
2. Click **Add list**.
3. Set the **MAC address** and **IP Address**.
4. Click **Submit**. As shown in Figure 3-12.

Bundled Address List			
			Add List
Index	IP Address	MAC Address	Operation
Settings			
IP Address	192.168.1.115 *		
MAC Address	00:e0:4c:36:02:d3 *	* Format xxxxxxxxxx	
			Submit Cancel

Figure 3-12

To modify an item in the setup list, perform the following steps:

1. Choose **Network Setting > LAN Settings**.
2. Choose the item to be modified, and click **Edit**.
3. Set the **MAC address** and **IP Address**.
4. Click **Submit**. As shown in Figure 3-13.

Bundled Address List

				Add List
Index	IP Address	MAC Address	Operation	
1	192.168.1.115	00:E0:4C:36:02:D1	Delete Edit	

Settings

IP Address *

MAC Address * Format xxxx:xx:xx:xx:xx:xx

Figure 3-13

To delete an item in the setup list, perform the following steps:

1. Choose **Network Setting > LAN Settings**.
2. Choose the item to be deleted, and click **Delete**.

3.6 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 Setting > 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 3-14.

DMZ Settings

DMZ

DMZ ☒ Enable

ICMP Redirect ☒ Enable

Host Address * Format : 192.168.1.x

Figure 3-14

3.7 Static Route

3.7.1 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 3-15.

Static Route

Static Route List

Add List

Index	Dest IP Address	Subnet Mask	Interface	Gateway	Status	Operation
-------	-----------------	-------------	-----------	---------	--------	-----------

Static Route Settings

Dest IP Address

8.8.8.0

*

Subnet Mask

255.255.255.0

*

Interface

LAN

Gateway

192.168.1.1

*

Submit

Cancel

Figure 3-15

3.7.2 Modify Static Route

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

1. Choose **Security>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 3-16.

Static Route

Static Route List

Add List

Index	Dest IP Address	Subnet Mask	Interface	Gateway	Status	Operation
1	8.8.8.0	255.255.255.0	LAN	192.168.1.1	Effective	Delete Edit

Static Route Settings

Dest IP Address

8.8.8.0

*

Subnet Mask

255.255.255.0

*

Interface

LAN

Gateway

192.168.1.1

*

Submit

Cancel

Figure 3-16

3.7.3 Delete Static Route

To delete a static route, perform the following steps:

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

4 Wi-Fi

4.1 WLAN Setting

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

4.1.1 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
802.11b/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.** from 1 to 11.
5. Set the Tx Power from 20% to 100%.
6. Click **Submit**. As shown in Figure 4-1.

WLAN Settings

General Settings

WLAN	☒ Enable
Mode	802.11 b/g/n(Auto) ▼
Channel	Auto ▼
Tx Power	100% ▼

Figure 4-1

4.1.2 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, security 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. Click **Submit**. As shown in Figure 4-2.

WPS Settings

WPS	☒ Enable
-----	--

Figure 4-2

4.2 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 security.

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 security 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 security 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 4-3.

SSID Profile

SSID

CLARO_C4E2

* (1–32 ASCII characters)

Maximum number of devices

10

Hide SSID broadcast

☒ Enable

AP isolation

☒ Enable

Security

WPA-PSK&WPA2-PSK

WPA encryption

TKIP&AES

Show password

☒ Enable

Password

.....

* (8-63 ASCII characters or 8-64 hexadecimal characters)

Figure 4-3

4.3 Access Management

4.3.1 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.

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.

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

Access Management

WLAN Access List Settings

Settings

☒ Disable
 ☐ Whitelist
 ☐ Blacklist

Submit

WLAN Access List

Add List

Index	MAC Address	Operation
-------	-------------	-----------

Figure 4-4

4.3.2 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 4-5.

The screenshot shows the 'WLAN Access List' configuration page. At the top right is an 'Add List' button. Below it is a table with three columns: 'Index', 'MAC Address', and 'Operation'. The 'Index' column is empty. The 'MAC Address' column contains the text '00:e0:4c:36:02:d1'. The 'Operation' column is empty. Below the table is a 'Settings' section with a 'MAC Address' label and a text input field containing '00:e0:4c:36:02:d1'. To the right of the input field is an asterisk '*'. At the bottom right are 'Submit' and 'Cancel' buttons.

Figure 4-5

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 4-6.

The screenshot shows the 'WLAN Access List' configuration page. At the top right is an 'Add List' button. Below it is a table with three columns: 'Index', 'MAC Address', and 'Operation'. The 'Index' column contains the number '1'. The 'MAC Address' column contains the text '00:E0:4C:36:02:D1'. The 'Operation' column contains the text 'Delete | Edit'. Below the table is a 'Settings' section with a 'MAC Address' label and a text input field containing '00:E0:4C:36:02:D1'. To the right of the input field is an asterisk '*'. At the bottom right are 'Submit' and 'Cancel' buttons.

Figure 4-6

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 4-7.

The screenshot shows the 'WLAN Access List' configuration page. At the top right is an 'Add List' button. Below it is a table with three columns: 'Index', 'MAC Address', and 'Operation'. The 'Index' column contains the number '1'. The 'MAC Address' column contains the text '00:E0:4C:36:02:D1'. The 'Operation' column contains the text 'Delete | Edit'. Below the table is a 'Settings' section with a 'MAC Address' label and a text input field containing '00:E0:4C:36:02:D1'. To the right of the input field is an asterisk '*'. At the bottom right are 'Submit' and 'Cancel' buttons.

Figure 4-7

4.4 WDS

The CPE supports the wireless distribution system (WDS). All Wi-Fi devices in a WDS must be configured to use the same radio channel, encryption mode, SSID, and encryption key. You can set the WDS encryption mode to NONE or WPA/WPA2. If you set the WDS encryption mode to NONE, the Wi-Fi clients can use NONE or WEP encryption mode. If you set the WDS encryption mode to WPA/WPA2-PSK, the Wi-Fi clients can use WPA/WPA2-PSK encryption mode. After WDS is enabled, disable DHCP on CPEs that are not directly connected to the WAN port.

If WDS is enabled, the WPS function will not take effect. If the channel is set to **Auto**, you need to set the channel.

To configure the WDS, perform the following steps:

- 1. Choose **Wi-Fi > WDS**.
- 2. Set **WDS** to **Enable**.
- 3. Set WDS Mode as **Repeater Mode**;
- 4. Click **Scan**.
From the search results, choose the SSID of the networking device.
- 5. Set **Security**.
WPA-PSK can contain 8 to 63 ASCII characters or 64 hex characters.
- 6. Click **Submit**. As shown in Figure 4-8.

WDS

The Wi-Fi module supports the wireless distribution system (WDS) in repeater mode. The Wi-Fi clients must be configured to use the same radio channel, encryption mode, and the encryption key. WDS can select NONE or WPA/WPA2 encryption. When using WPA/WPA2-PSK encryption, the Wi-Fi Client can use WPA/WPA2-PSK encryption. After WDS is enabled, disable the DHCP on CPEs that are not directly connected to the WAN port. Be sure that the CPEs are not using the same gateway IP address, and all their gateway IP addresses are in the same network segment.

Settings

Enable☒ Enable

Scan

Scan

Index	SSID	BSSID	Channel	Select
1	w7fTestF	24:05:0f:a1:7a:25	1	☐
2	DT360-wuzh01	00:1f:bc:9:3a:bf	1	☐
3	snake-2.4	8c:ab:8e:69:98:80	2	☐
4	Kevin_PocketAP	38:83:45:36:69:a0	1	☐
5	TP-LINK-007	00:27:19:4a:68:50	1	☐
6	Jifen-610-mi	28:6c:07:6b:a7:7a	4	☐
7	Kylin	8c:ab:8e:94:04:98	3	☐
8	qlansuo	00:0e:a9:26:02:c0	6	☐

Figure 4-8

5 Security

5.1 MAC Filtering

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

5.1.1 Enabling MAC Filter

To enable MAC address filter, perform the following steps:

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

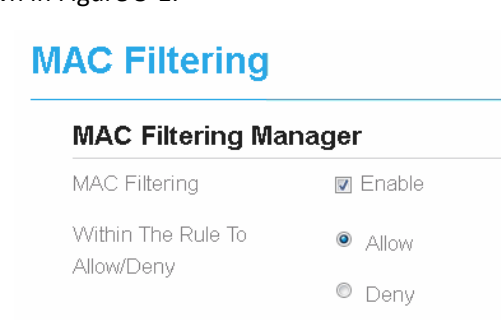


Figure 5-1

5.1.2 Disabling MAC Filter

To disable MAC address filter, perform the following steps:

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

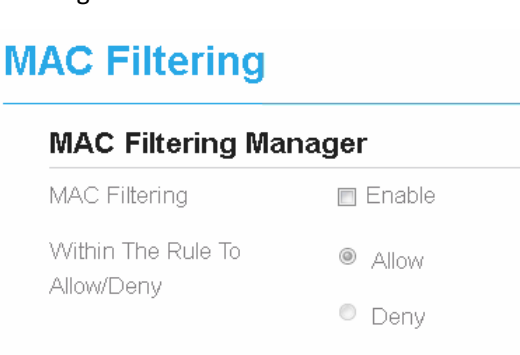


Figure 5-2

5.1.3 Setting Allow access network within the rules

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

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

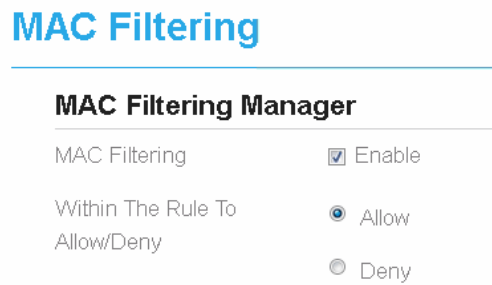


Figure 5-3

5.1.4 Setting Deny access network within the rules

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

1. Choose **Security>MAC Filtering**.
2. Set **Deny access network** within the rules.
3. Click **Submit**. As shown in Figure 5-4.

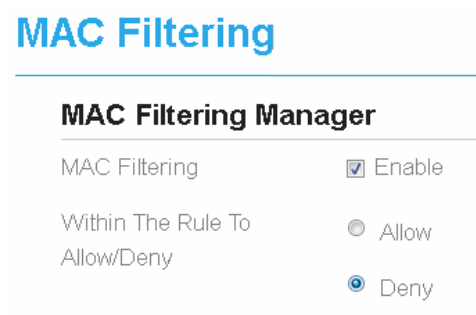


Figure 5-4

5.1.5 Adding MAC Filtering rule

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

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

MAC Filtering List

[Add List](#)

Index	MAC Address	Operation
-------	-------------	-----------

Settings

MAC Address * Format xxxxxx:xxxxxx:xxxxxx

[Submit](#) [Cancel](#)

Figure 5-5

5.1.6 Modifying MAC Filtering rule

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

1. Choose **Security>MAC Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-6.

MAC Filtering List

[Add List](#)

Index	MAC Address	Operation
1	00:E0:4C:36:02:D1	Delete Edit

Settings

MAC Address * Format xxxxxx:xxxxxx:xxxxxx

[Submit](#) [Cancel](#)

Figure 5-6

5.1.7 Deleting MAC Filtering rule

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

1. Choose **Security>MAC Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-7.

MAC Filtering List

[Add List](#)

Index	MAC Address	Operation
1	00:E0:4C:36:02:D1	Delete Edit

Figure 5-7

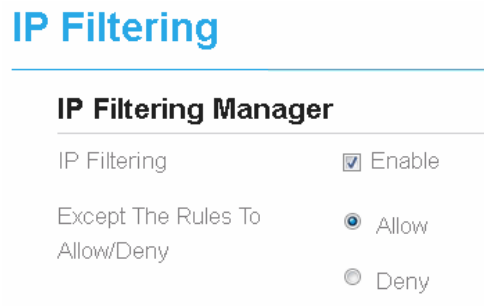
5.2 IP Filtering

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

5.2.1 Enabling IP Filtering

To enable IP Filtering, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set IP Filtering **Enable**.
3. Click **Submit**. As shown in Figure 5-8.



The screenshot shows the 'IP Filtering' configuration page. The title 'IP Filtering' is at the top in blue. Below it is the 'IP Filtering Manager' section. It contains two rows of settings: 'IP Filtering' with a checked checkbox and the label 'Enable', and 'Except The Rules To Allow/Deny' with two radio buttons, 'Allow' (selected) and 'Deny'.

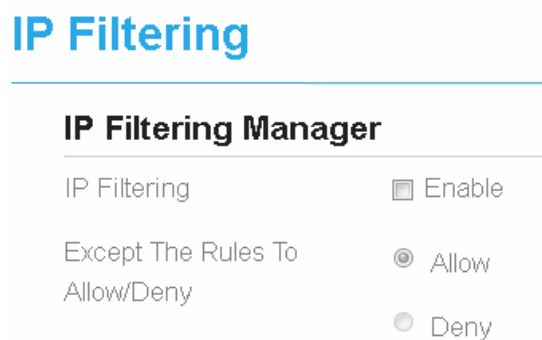
IP Filtering Manager	
IP Filtering	☒ Enable
Except The Rules To Allow/Deny	☒ Allow
	☐ Deny

Figure 5-8

5.2.2 Disabling IP Filtering

To disable IP Filtering, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set IP Filtering **Disable**.
3. Click **Submit**. As shown in Figure 5-9.



The screenshot shows the 'IP Filtering' configuration page. The title 'IP Filtering' is at the top in blue. Below it is the 'IP Filtering Manager' section. It contains two rows of settings: 'IP Filtering' with an unchecked checkbox and the label 'Enable', and 'Except The Rules To Allow/Deny' with two radio buttons, 'Allow' (selected) and 'Deny'.

IP Filtering Manager	
IP Filtering	☐ Enable
Except The Rules To Allow/Deny	☒ Allow
	☐ Deny

Figure 5-9

5.2.3 Setting Allow access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set **Allow access network** outside the rules.
3. Click **Submit**. As shown in Figure 5-10.

IP Filtering

IP Filtering Manager

IP Filtering	☒ Enable
Except The Rules To Allow/Deny	☒ Allow
	☐ Deny

Figure 5-10

5.2.4 Setting Deny access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set **Deny access network** outside the rules.
3. Click **Submit**. As shown in Figure 5-11.

IP Filtering

IP Filtering Manager

IP Filtering	☒ Enable
Except The Rules To Allow/Deny	☐ Allow
	☒ Deny

Figure 5-11

5.2.5 Adding IP Filtering rule

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

1. Choose **Security>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 5-12.

IP Filtering List

Add List

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

Settings

Service

Custom

Protocol

ALL

Source IP Address Range

192.168.1.22

(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]

Source Port Range

(Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Destination IP Address Range

8.8.8.8

(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]

Destination Port Range

(Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Status

Allow

Submit

Cancel

Figure 5-12

5.2.6 Modifying IP Filtering rule

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

- 1. Choose **Security > 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 5-13.

IP Filtering List

Add List

Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation
1	ALL	192.168.1.22		8.8.8.8		Allow	Delete Edit

Settings

Service

Custom

Protocol

ALL

Source IP Address Range

192.168.1.22

(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]

Source Port Range

(Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Destination IP Address Range

8.8.8.8

(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]

Destination Port Range

(Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Status

Allow

Submit

Cancel

Figure 5-13

5.2.7 Deleting IP Filtering rule

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

1. Choose **Security > IP Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-14.

IP Filtering List

Add List

Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation
1	ALL	192.168.1.22		8.8.8.8		Allow	Delete Edit

Figure 5-14

5.3 URL Filtering

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

5.3.1 Enabling URL Filtering

To enable URL Filtering, perform the following steps:

3. Choose **Security>URL Filtering**.
4. Set **URL Filtering** to **Enable**.
5. Click **Submit**. As shown in Figure 5-15.

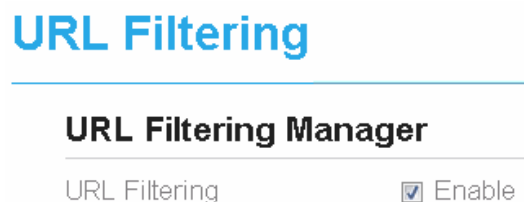


Figure 5-15

5.3.2 Disabling URL Filtering

To disable URL Filtering, perform the following steps:

1. Choose **Security>URL Filtering**.
2. Set **URL Filtering** to **Disable**.
3. Click **Submit**. As shown in Figure 5-16.

URL Filtering

URL Filtering Manager

URL Filtering

☐ Enable

Figure 5-16

5.3.3 Adding URL Filtering list

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

1. Choose **Security>URL Filtering**.
2. Click **Add list**.
3. Set **URL**.
4. Click **Submit**. As shown in Figure 5-17.

URL Filtering List

[Add List](#)

Index	URL	Operation
-------	-----	-----------

Settings

URL *

[Submit](#) [Cancel](#)

Figure 5-17

5.3.4 Modify URL Filtering list

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

1. Choose **Security>URL Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **URL** address.
4. Click **Submit**. As shown in Figure 5-18.

URL Filtering List

[Add List](#)

Index	URL	Operation
1	www.google.com	Delete Edit

Settings

URL *

[Submit](#) [Cancel](#)

Figure 5-18

5.3.5 Deleting URL Filtering list

To delete a URL list, perform the following steps:

1. Choose **Security>URL Filtering**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-19.

URL Filtering List

Add List		
Index	URL	Operation
1	www.google.com	Delete Edit

Figure 5-19

5.4 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.

5.4.1 Adding Port Forwarding rule

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

1. Choose **Security > 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 5-20.

Port Forwarding

Port Forwarding List

Add List

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
-------	----------	-------------------	------------	------------	-----------

Settings

Service

Custom

Protocol

TCP

Remote Port Range

3000

* (Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Local Host

192.168.1.125

*

Local Port

8080

*

Submit

Cancel

Figure 5-20

5.4.2 Modifying Port Forwarding rule

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

1. Choose **Security > 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 5-21.

Port Forwarding

Port Forwarding List

Add List

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	3000	192.168.1.125	8080	Delete Edit

Settings

Service

Custom

Protocol

TCP

Remote Port Range

3000

* (Format: 1000-1500 Or 1000 Or null; Port range: [1-65535])

Local Host

192.168.1.125

*

Local Port

8080

*

Submit

Cancel

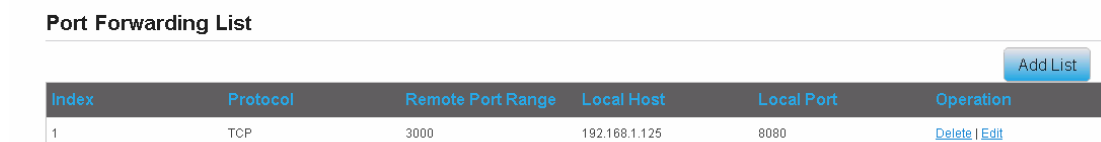
Figure 5-21

5.4.3 Deleting Port Forwarding rule

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

1. Choose **Security > Port Forwarding**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-22.

Port Forwarding



						Add List
Index	Protocol	Remote Port Range	Local Host	Local Port	Operation	
1	TCP	3000	192.168.1.125	8080	Delete Edit	

Figure 5-22

5.5 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 **Security > UPnP**.
2. Set **UPnP** to **Enable**.
3. Click **Submit**. As shown in Figure 5-23.

UPnP

Settings

UPnP

☒ Enable

Submit

Current UPnP Status

Index	Description	Protocol	IP Address	External Port	Internal port
-------	-------------	----------	------------	---------------	---------------

Figure 5-23

5.6 DOS

On this page, you can enable or disable the DOS function.

Enable DOS, perform the following steps:

1. Choose **Security > DOS**.

2. Set **DOS** to **Enable**.
3. Click **Submit**. As shown in Figure 5-24.

DoS

DoS Setting

DoS

☒ Enable ☐ Disable

Sync flood

☐ Enable

Ping of death

☐ Enable

Ping flood

☐ Enable

TCP port scan

☐ Enable

UDP port scan

☐ Enable

Submit

Cancel

Figure 5-24

6 VPN Setting

This function enables you to connect the virtual private network (VPN).
To connect the VPN, perform the following steps:

1. Choose **VPN Setting**.
2. In the **VPN Setting** 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 6-1.

VPN Settings

VPN Settings

VPN

☒ Enable

Protocol

PPTP

VPN Server

112.64.184.12

*

Username

test

*

Password

....

*

VPN Status

Username	Local Address	Remote Address	Online Time
----------	---------------	----------------	-------------

Submit

Cancel

Figure 6-1

7 VOIP

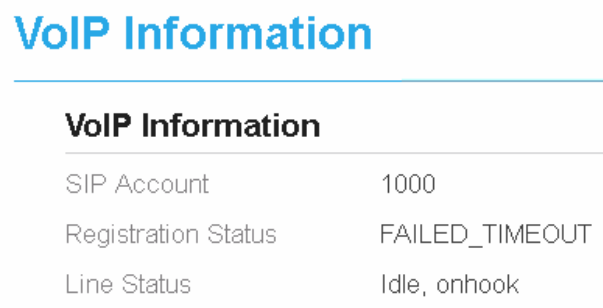
The CPE supports voice services based on the Session Initiation Protocol (SIP) and enables voice service interworking between the Internet and Public Switched Telephone Networks (PSTNs).

7.1 View VOIP Information

To view VOIP information, perform the following steps:

1. Choose **VOIP > VOIP Information**;
2. View the VOIP information, such as the SIP account and status of the SIP registration server.

As shown in Figure 7 - 1.



VoIP Information	
SIP Account	1000
Registration Status	FAILED_TIMEOUT
Line Status	Idle, onhook

Figure 7-1

7.2 Configuring SIP Server

To set the SIP server parameters, perform the following steps:

1. Choose **VOIP > SIP Server**;
2. In the **User Agent port** box, enter the port of the SIP account provided by your service provider.
3. In the **SIP server domain name** box, enter the domain name of the SIP server.
4. In the **Proxy server address** box, enter the address of the proxy server provided by your service provider, for example, 192.168.1.10.
5. In the **Proxy server port box**, enter the port of the proxy server provided by your service provider, for example, 5060. The value ranges from 1 to 65535.
6. In the **Registration server address** box, enter the address of the registration server provided by your service provider, for example, 192.168.1.11.
7. In the **Registration server port** box, enter the port of the registration server provided by your service provider, for example, 5060. The value ranges from 1 to 65535.
8. Click Submit. As shown in Figure 7 - 2.

SIP Server

Sip Local Port

User Agent port * (1~65535)

Registration Server

SIP server domain name * (IP address or domain name)

Proxy server address * (IP address or domain name)

Proxy server port * (1~65535)

Registration server address * (IP address or domain name)

Registration server port * (1~65535)

Registration Expiry Time * Seconds (90~86400)

Submit

Cancel

Figure 7 - 2.

7.3 Configuring SIP Account

Before configuring SIP accounts, make sure that the registration server has been properly configured.

To configure SIP account, perform the following steps:

1. Choose **VoIP > SIP Account**.
2. Set SIP Account Enable.
3. In the **User name and Password** boxes, enter the user name and password of the SIP account provided by your service provider.
4. In the **Phone Number** box, enter the SIP Phone number provided by your service provider.
5. In the **Display Name** box, enter the display name provided by your service provider.
6. In the **Codec Priority area**, set the codec priority.
7. Click Submit. As shown in Figure 7 - 3.

SIP Account

SIP Account

Enable ☒ Enable

Username * (a maximum of 64 characters)

Password * (a maximum of 64 characters)

Phone Number * (a maximum of 64 digits)

Display Name * (a maximum of 64 characters)

Codec Priority

Priority - 1

Priority - 2

Submit

Cancel

Figure 7 - 3

7.4 Advanced SIP

User can import Digit Map, ether can enable Three-way conversion.

To import digit map, perform the following steps:

- 1. Choose **VOIP>Advance SIP**.
- 2. Click Browse on the Advance SIP page.
- 3. Click Open.
- 4. The dialog box choses. In the box to be right of Configuration file, the save path and name of the digit map file are displayed.
- 5. Click Submit. As shown in Figure 7 - 4.

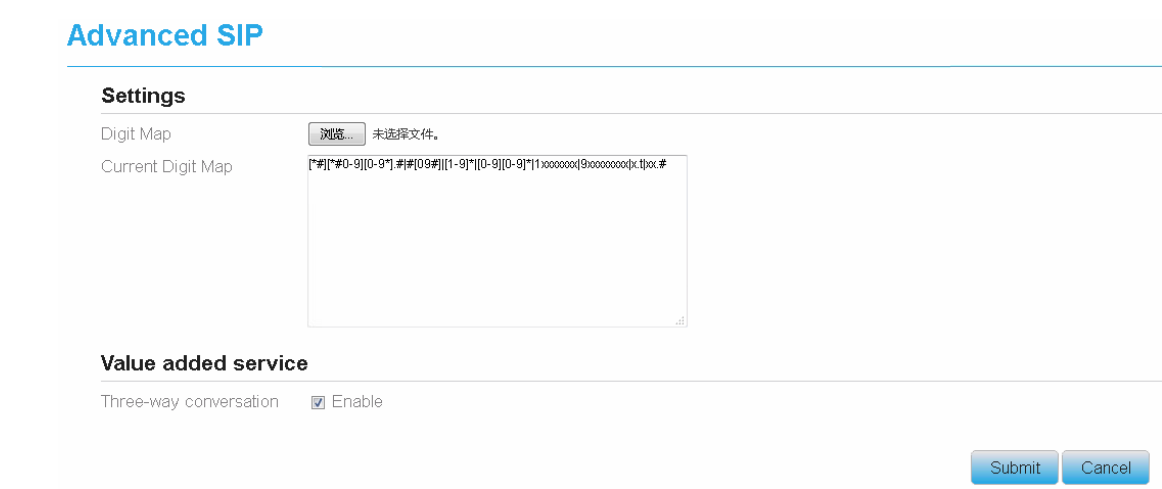


Figure 7 - 4

8 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.

8.1 Status

The status page shows IPv6 information. As shown in Figure 8-1.

Status

IPv6 Information

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

LAN Address AutoConfiguration

IPv6 DATA Global Address	--
IPv6 Link-Local Address	fe80::da55:a3ff:fe61:c4e0
AutoConfiguration Type	SLAAC

Figure 8-1

8.2 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 8-2

IPv6 WAN Settings

WAN

IPv6 Enable ☒ Enable

WAN Settings

WAN Connection Type AutoConfiguration ▼

IPv6 MGMT Global Address

DNS From DHCPv6 ▼

Figure 8-2

8.3 IPv6 LAN Settings

In this page, user can chose the AutoConfiguration Type. As shown in Figure 8-3.

IPv6 LAN Settings

LAN Settings

IPv6 Link-Local Address	fe80::da55:a3ff:fe61:c4e0
AutoConfiguration Type	SLAAC SLAAC DHCPv6

Figure 8-3

9 System

9.1 Maintenance

9.1.1 Restart

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 **Restart**. As shown in Figure 9-1.

The CPE then restarts.

Reboot

Click **Reboot** to reboot device

Reboot

Figure 9-1

9.1.2 Factory 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 9-2.

The CPE is then restored to its default settings.

Factory Reset

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

Factory Reset

Figure 9-2

9.1.3 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 9-3.

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 9-3

9.1.4 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 closes. In the box to the right of Configuration file, the save path and name of the backed up configuration file are displayed.
6. Click **Upload**. As shown in Figure 9-4.

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 未选择文件。



Figure 9-4

9.2 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.

9.2.1 Viewing Version Info

To view the version info, perform the following steps:

1. Choose **System>Version Manager**.
2. In the **Version Info** area, you can view the product name and software version. As shown in Figure 9-5.

Version Manager

Version Information	
Product Model	WF820+
Board SN	6453015520600233
Running software version	CLARO_PER_WF820+_V1.0.0B02-F
Backup software version	COMBA_FJ_001

Figure 9-5

9.2.2 Local 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:

6. Choose **System>Version Manager**.
7. In the **Version Upgrade** area, click **Browse**. In the displayed dialog box, select the target software version file.
8. Click **Open**. The dialog box closes. The save path and name of the target software version file are displayed in the Update file field.
9. Click **Submit**.
10. The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version. As shown in Figure 9-6.

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

Local Upgrade

Version File 未选择文件。

Figure 9-6

9.2.3 Online Upgrade

This function is designed for FOTA. If you have set the FOTA settings, you can click **check** to check whether there is a new version for the CPE.

To perform an upgrade, perform the following steps:

1. Choose **System>Version Manager**.
2. In the **Online Upgrade** area, click check.
3. The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version. As shown in Figure 9-7.



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

Online Upgrade

Click **Check** button to check new version online.



Figure 9-7

9.3 Module Manager

This function enables you to upgrade the ODU 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.

9.3.1 Viewing Version Info

To view the version info, perform the following steps:

3. Choose **System>Module Manager**
4. In the **Version Info** area, you can view the product name and software version. As shown in Figure 9-8.

Module Manager	
Module Information	
Module Model	MH841e
Module Version	4.1.1.1-25026-BYPASS-1.5.1

Figure 9-8

9.3.2 Module Upgrade

To perform an upgrade, perform the following steps:

1. Choose **System>Module Upgrade**.
2. In the **Module Upgrade** area, click **Browse**. In the displayed dialog box, select the target software version file.
3. Click **Open**. The dialog box closes. 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 9-9.



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

Module Upgrade

Version File 未选择文件。

Figure 9-9

9.4 FTP 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 **System>FTP auto upgrade**.
2. Enable **FTP 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 a ftp address to the **Upgrade folder** box.
5. Set **Version file**.
6. Set **User name** and **Password**.
7. Set the **Interval** of checking new firmware.
8. Set **Start time**.
9. Set **Random time**.
10. Click **Submit**. As shown in Figure 9-10.



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

FTP Auto Upgrade

Settings

FTP Auto Upgrade	☒ Enable
Check New FW after connected	☐ Enable
Upgrade Folder	ftp://192.168.1.172 ftp://xxx
Version File	version.txt *
Username	root *
Password	***** *
Check New FW Every	☒ 24 hrs(1~740)
Start Time(24hrs)	0

Figure 9-10

9.5 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>TR-069 Settings**.
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 9-11.

TR069

Settings

Enable TR069	☒ Enable
ACS URL Source	URL
ACS URL	192.168.22.38:8080 * http://xxx
ACS Username	cwmp69 *
ACS Password	***** *
Enable Periodic Inform	☒ Enable
Periodic Inform Interval	240 * Seconds (20~86400)
Connection Request Username	admin
Connection Request Password	*****

Submit Cancel

Figure 9-11

9.6 FOTA

Over-the-air programming (OTA) refers to various methods of distributing new software. One important feature of OTA is that one central location can send an update to all the users, who are unable to refuse, defeat, or alter that update, and that the update applies immediately to everyone on the channel.

To configure the FOTA to implement the FOTA function, perform the following steps:

1. Choose **System>FOTA**.
2. Set **FOTA URL source**. It is a http address of xml configuration.
3. Check the **Start Time(24hrs)** and **Random Time**. You can determine which time to check the FOTA server.
4. Click **Submit**. As shown in Figure 9-12.

FOTA

Settings

Enable	☒ Enable
FOTA on BOOT	☒ Enable
URL	http://claro.com.pe/OTA/ZTE_ * http://xxx
Start Time(24hrs)	0
Random Time	3
Status	Check firmware success

Submit Cancel

Figure 9-12

9.7 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 9-13.

Date & Time

Settings

Current Time 2017-07-21 10:00:22

☒ Set Manually

Local Time 2017 / 07 / 21 / 10 / 00 / 22
(format: YYYY/MM/DD/HH/MM/SS, the value of year is between 2000 and 2030)

☐ Sync from Network

Figure 9-13

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 9-14.

Date & Time

Settings

Current Time	2017-07-21 10:00:22
☐ Set Manually	
☒ Sync from Network	
Primary NTP Server	pool.ntp.org
Secondary NTP Server	asia.pool.ntp.org
Optional NTP Server	☒ 192.168.22.110
Time Zone	(GMT-05:00) Peru

Figure 9-14

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 9-15.

DST

DST	☒ Enable
Start Time	May 8 00 00 00 (MM DD HH:MM:SS)
End Time	Oct 8 00 00 00 (MM DD HH:MM:SS)
Status	Not Running

Figure 9-15

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

9.8 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 9-16.

DDNS

DDNS Settings

DDNS	☒ Enable
Service Provider	DynDNS.org ▼
Domain	mypersonaldomain.dyndns.c *
Username	myusername *
Password	 *

DDNS Status

Connect status	Disconnected
----------------	--------------

Figure 9-16

9.9 Iperf

Iperf is a widely-used tool for network performance measurement and tuning. Iperf has client and server functionality, and can create data streams to measure the throughput between the two ends in one or both directions.

To perform iperf, perform the following steps

1. Choose **System > IPERF**.
2. Set **Server Address** which iperf client running.
3. Click start to perform iperf. As shown in Figure 9-17.

Settings

Server Address	192.168.12.22	*
Server Port	5001	* (1024~65535)
Management Port	5001	* (1024~65535)
Measurement Time	30	* (10~86400)Seconds
Protocol Type	TCP	

Start

Figure 9-17

9.10 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.

9.10.1 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 9-18.

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

Diagnosis

Method

Method of Diagnosis

☒ Ping

☐ TraceRoute

Ping

Target IP/Domain

www.twitter.com

*

Packet Size

56

* bytes (1~9000)

Timeout

5

* seconds (1~5)

Count

4

* times (1~10)

Ping

Cancel

Figure 9-18

9.10.2 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** and **Timeout**.
5. Click **Traceroute**. As shown in Figure 9-19.

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

Diagnosis

Method

Method of Diagnosis

☐ Ping

☒ TraceRoute

Traceroute

Target IP/Domain

www.google.com

*

Maximum Hops

30

* (1~30)

Timeout

5

* seconds (1~5)

Traceroute

Cancel

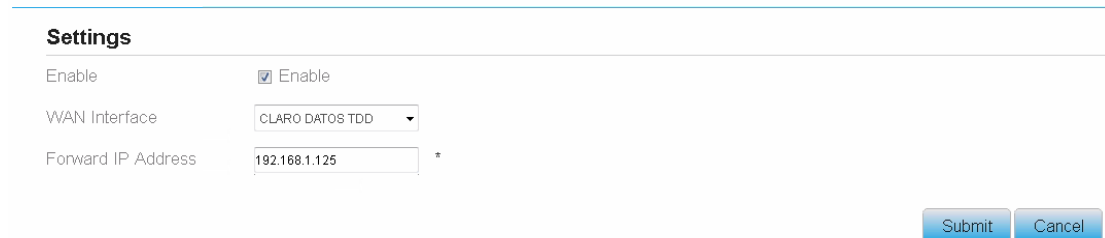
Figure 9-19

9.11 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 9-20.

Port Mirror



Settings

Enable ☒ Enable

WAN Interface

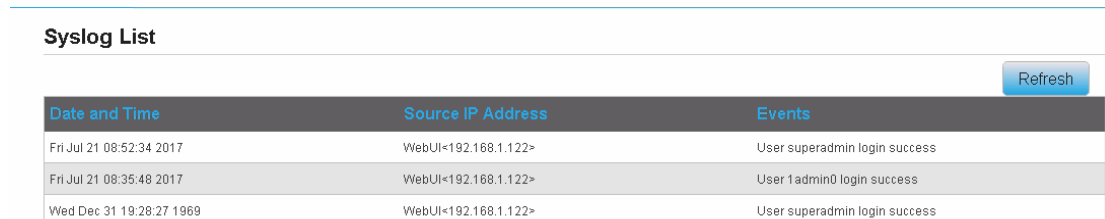
Forward IP Address *

Figure 9-20.

9.12 Syslog

The syslog record user operations and key running events. You can click Refresh to reload the logs. As shown in Figure 9-21.

Syslog



Syslog List

Date and Time	Source IP Address	Events
Fri Jul 21 08:52:34 2017	WebUI<192.168.1.122>	User superadmin login success
Fri Jul 21 08:35:48 2017	WebUI<192.168.1.122>	User 1admin0 login success
Wed Dec 31 19:28:27 1969	WebUI<192.168.1.122>	User superadmin login success

Figure 9-21

9.13 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 9-22.

Account

Change Password

Username

Current Password *

New Password * (5-15 ASCII characters)

Confirm Password * (5-15 ASCII characters)

Settings

Enable User ☒ Enable

Figure 9-22

9.14 WEB Setting

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

1. Choose **System> web settings**
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. Set the **Refresh Time**.
8. Set the **Session Timeout**.
9. Set the **language**.
10. Click **Submit**. As shown in Figure 9-23.

WEB Setting

Settings

HTTP Enable	☒ Enable	
HTTP Port	80	* (80~65535)
HTTPS Enable	☒ Enable	
Allow HTTPS Login from WAN	☒ Enable	
HTTPS Port	443	* (81~65535)
Refresh Time	10	* Seconds (5~60)
Session Timeout	10	* Minutes (5~1440)
Language	English	

Submit

Cancel

Figure 9-23

9.15 Logout

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

1. Choose **System** and click **Logout**
2. It will back to the login page.

10 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

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.

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.

Caution:

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

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body. The antennas must not be co-located with other transmitter antennas.

The device can only operate indoor, and can not operate in outdoor condition.