

OrangeOS-AC User Manual

Product Name: OrangeOS-AC

Hardware Version: R124M_VER 2.0

Software Version: V2.3.0

Table of Contents

1 Log In

2 State

3 Network

3.1 Interface Designate

3.2 Internet Settings

3.3 Local Network Settings

3.4 DNS Settings

3.5 Balance

3.6 VLAN Settings

3.7 DNS Settings

3.8 Static Route

3.9 Directed Route

3.10 Timing Redial

4 AC Control

4.1 Group

4.2 Members

4.3 Batch Upgrade

4.4 Details

5 Authentication

5.1 Local Auth

5.1.1 OneKey Authentication

5.1.2 WeChat Authentication

5.1.3 Traffic Authentication

5.1.4 User Authentication

5.1.5 Password Authentication

5.2 Wifidog Auth

6 Bandwidth Control

6.1 QoS

6.2 IP Limit

6.3 Localnet Monitor

7 Firewall

7.1 IP Filter

7.2 MAC Filter

7.3 URL Filter

7.4 Port Filter

7.5 Port Mapping

7.6 DMZ settings

7.7 ARP Binding

7.8 Attack Protection

8 Service

8.1 DDNS Settings

8.2 Remote Management

8.3 VPN Client

8.3.1 PPTP Client

8.3.1 L2TP Client

8.4 VPN Server

8.4.1 PPTP Server

8.4.1 PPTP User

8.5 UPNP Settings

9 Log and Statistics

9.1 Log

9.2 Status Chart

10 System Tools

10.1 System Upgarde

10.2 Manage Config

10.3 Reboot

10.3.1 Reboot Now

10.3.2 Timed Restart

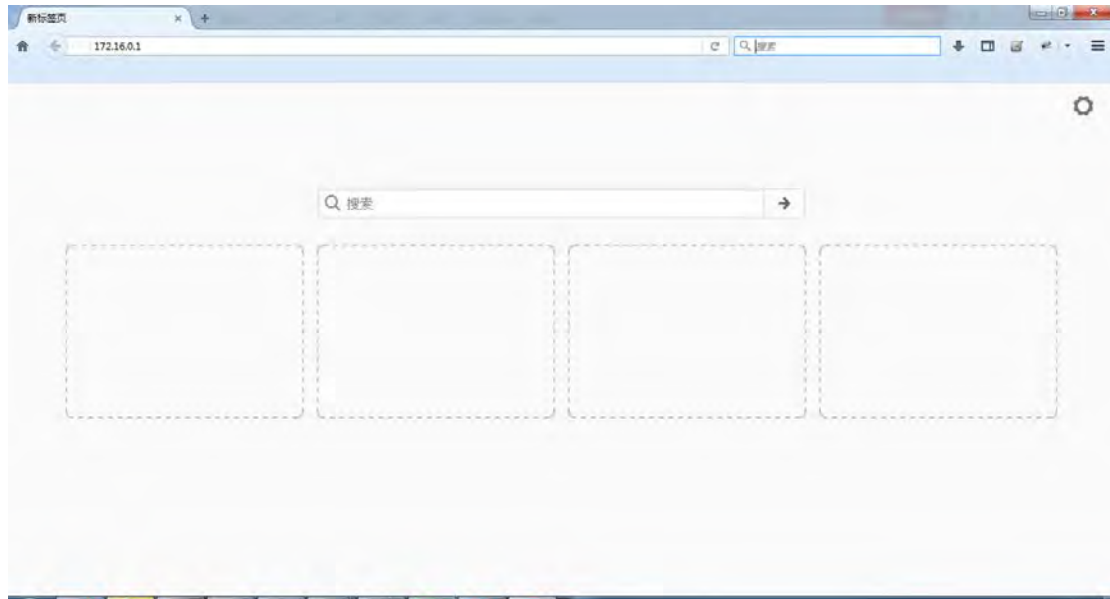
10.4 Password Setting

10.5 Time Setting

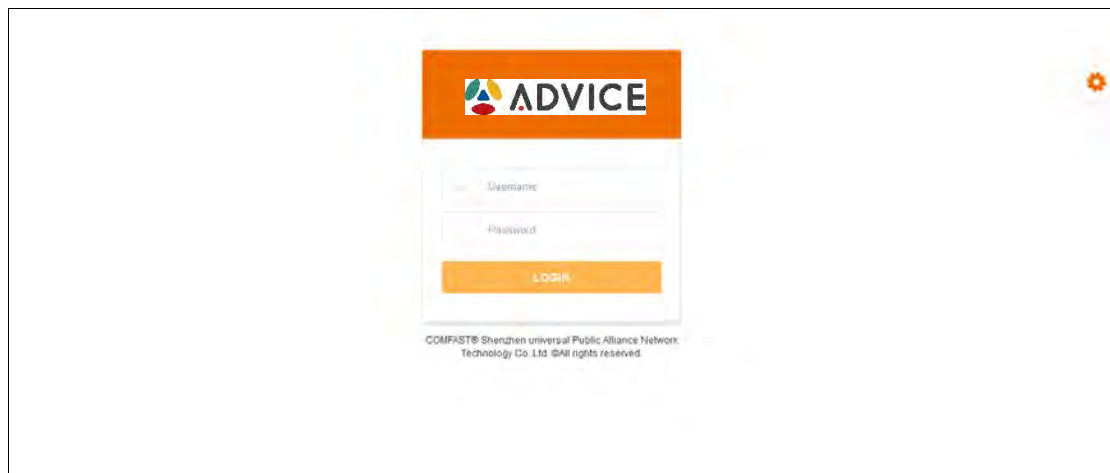
10.6 PING

1 Log In

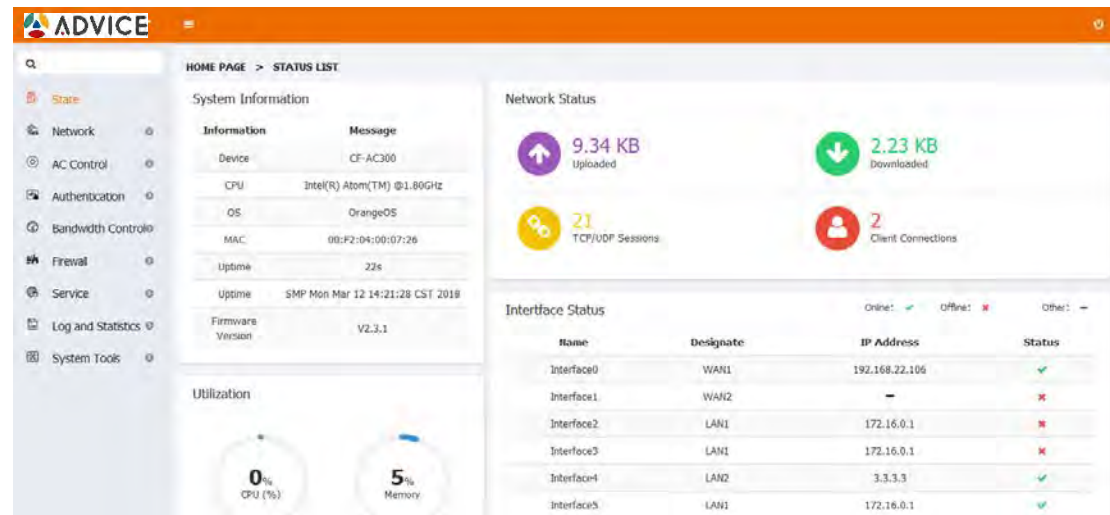
1.OrangeOS is based on the browser's configuration interface. Open your browser, and input IP address:172.16.0.1.



2. After finished the IP address and click Enter. Then it will get into OrangeOS' LOGIN interface as below:

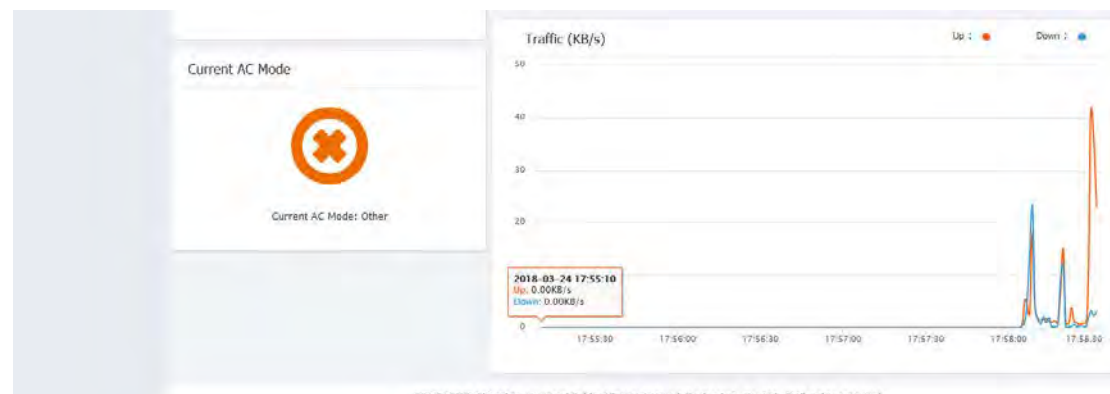
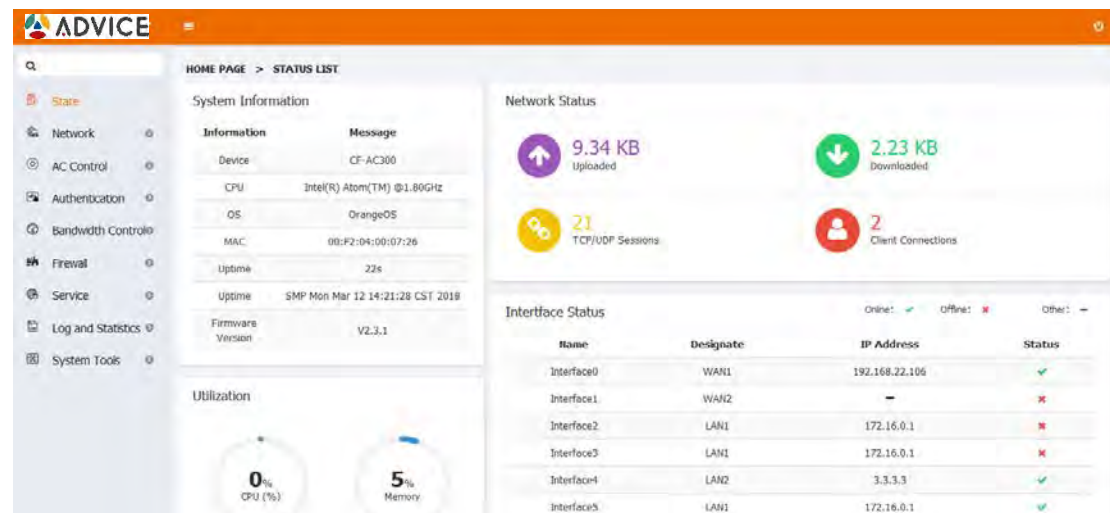


3. Input user name "admin", Password "admin". Then click LOGIN to get into the home page as below:



2 State

After login, it will get into the state information page directly. It will show you basic hardware information, CPU and memory utilization, rate data and Ethernet status.

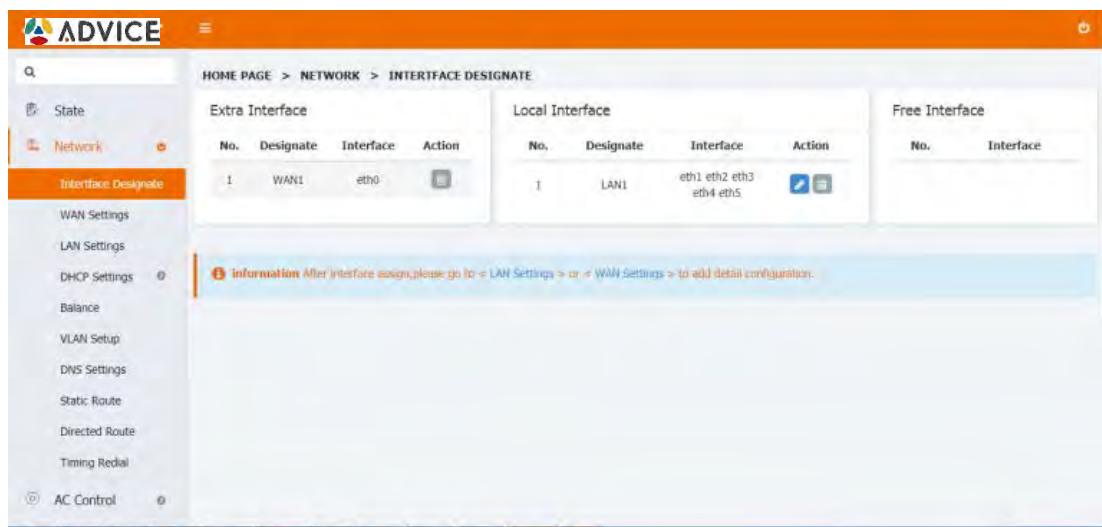


3 Network

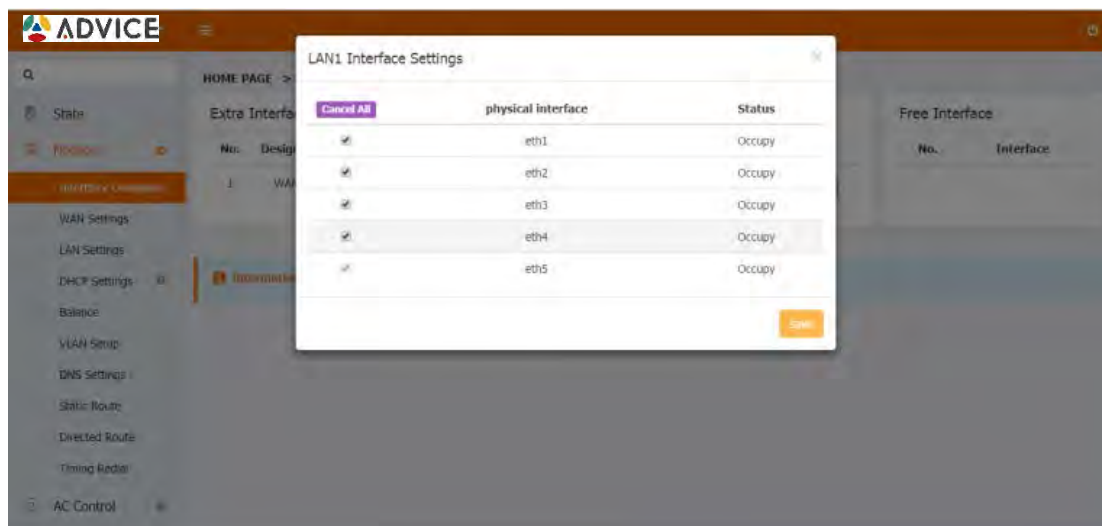
3.1 Interface Designate

The “eth0” is defaulted to be WAN port. “eth5” is defaulted to be LAN port and it can not edit. The rest “eth1-eth4” is customized to be WAN port or LAN port. After designated the WAN port or LAN port, pls set up the inner net and outer net by “Local Network” and “Internet Settings”.

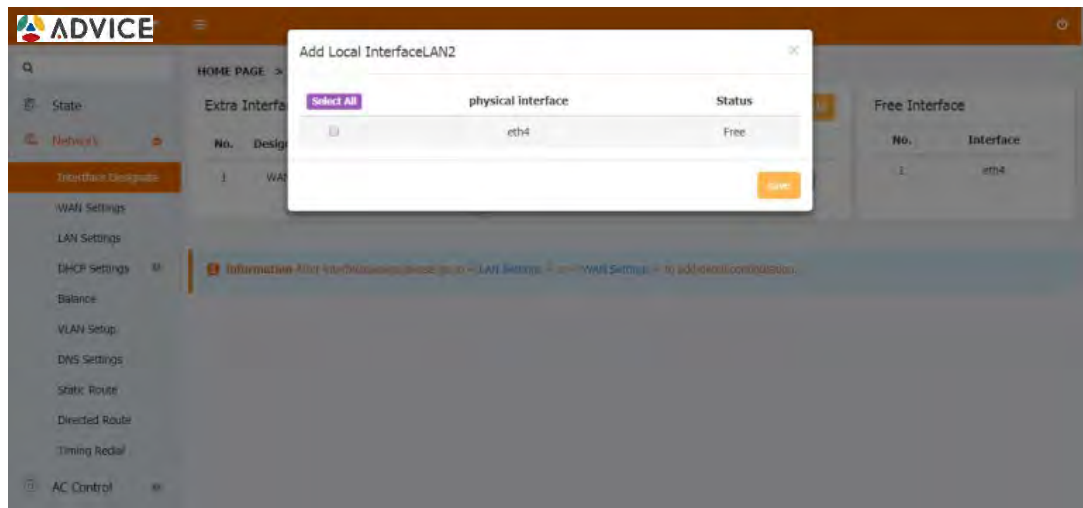
1. Click “Interface Designate” and get into the its setting page as below:



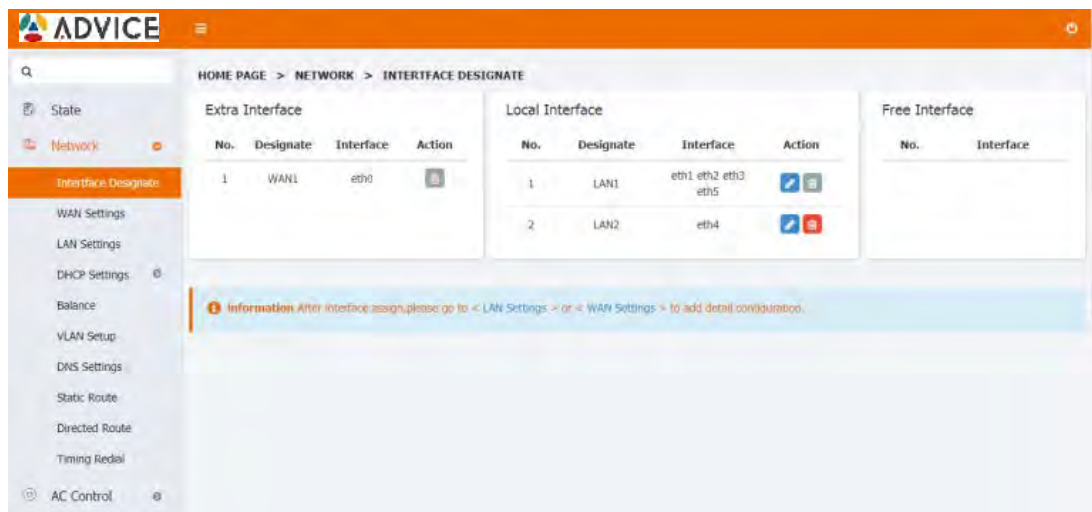
2. Click the “Edit” button to go into the “LAN1 Interface Settings” page, freely release 2 ethernet ports



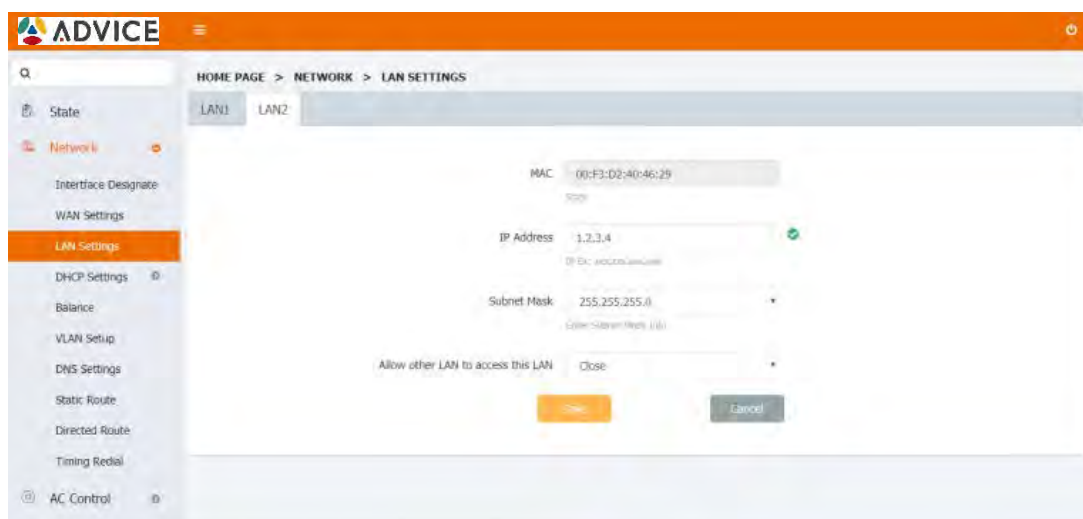
3. Click the “Add” button to get into the “Extra Interface”, Then go into the newly increased Local Interface page, tick to choose the INTERFACE which you want to add, as below:



4. Click "Save" and the INTERFACE list which you add will appear in the local Interface.



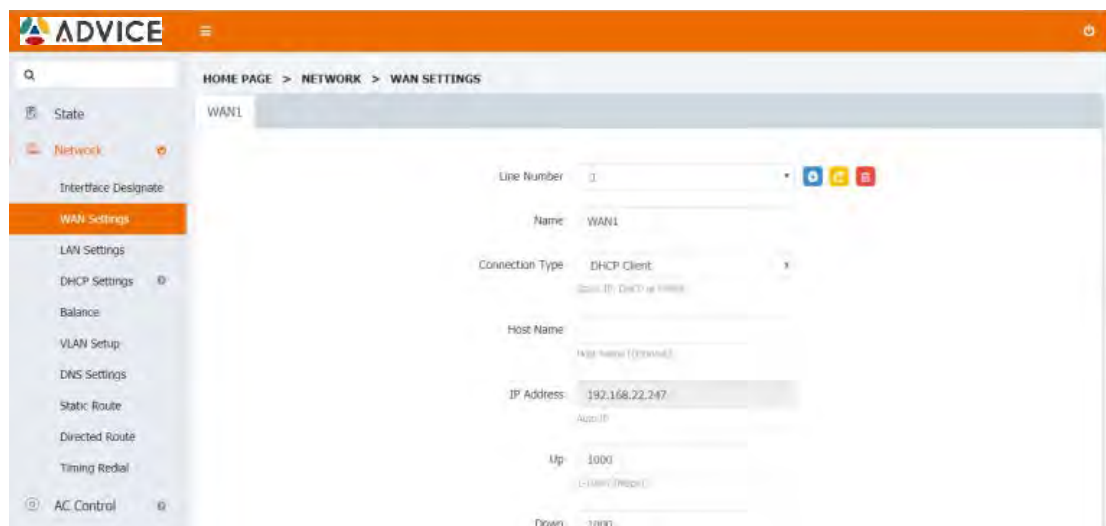
5. Click "Local Network", Setting the LAN2's IP Address and Subnet Mask parameter.



3.3 Internet Settings

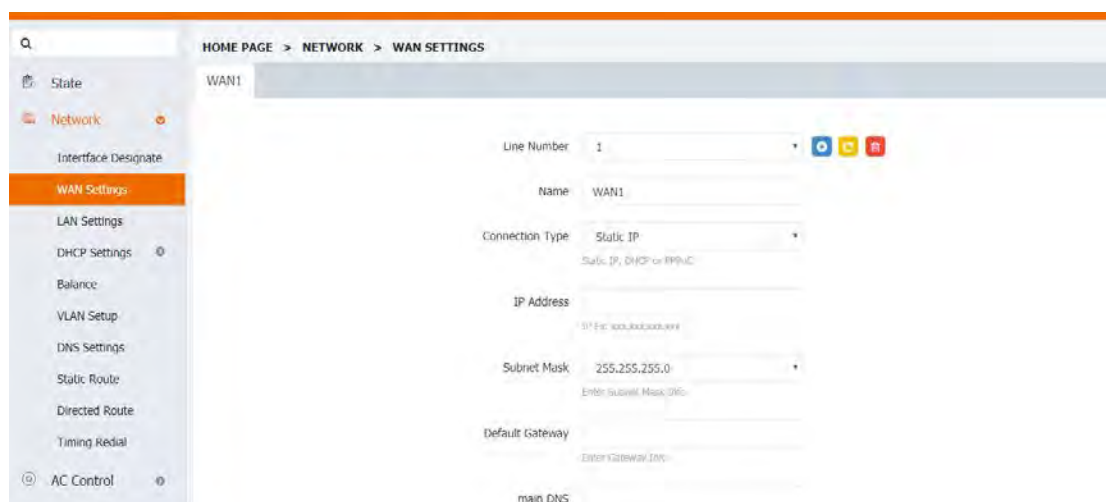
In “Internet Setting”,you can set up DHCP Client,Static IP,PPPoE this three connection types,it support Clone MAC address.

1.DHCP:if the internet achieve the IP automatically by the DHCP,you can use this connection type.

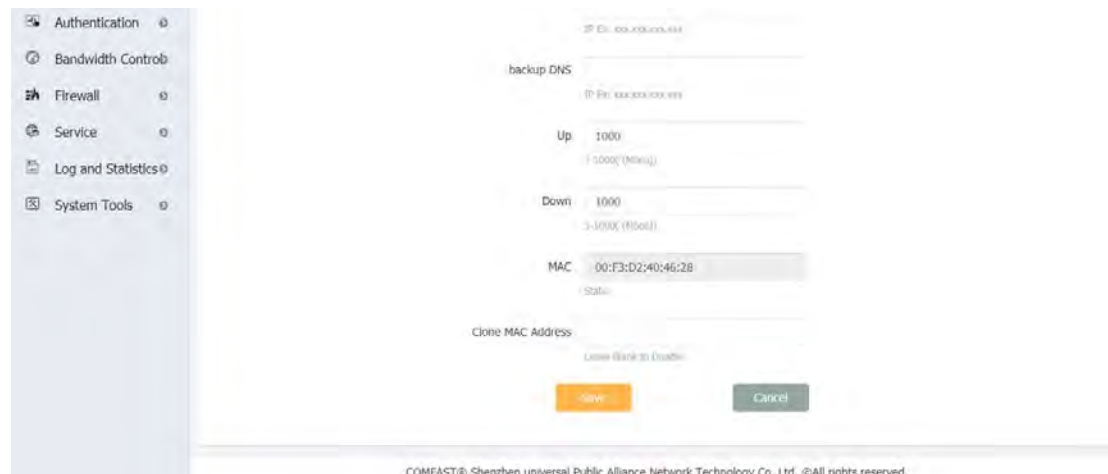


The screenshot shows the ADVICE web interface for configuring WAN settings. The left sidebar contains a menu with options: State, Network, Interface Designate, WAN Settings (highlighted), LAN Settings, DHCP Settings, Balance, VLAN Setup, DNS Settings, Static Route, Directed Route, Timing Redial, and AC Control. The main content area is titled 'HOME PAGE > NETWORK > WAN SETTINGS' and shows the 'WAN1' configuration. The 'Line Number' is set to 1. The 'Name' is 'WAN1'. The 'Connection Type' is 'DHCP Client'. The 'IP Address' is '192.168.22.247'. The 'Up' time is '1000' and the 'Down' time is '1000'.

2.Static IP:configure the fixed IP,Subnet Mask,Default Gateway and DNS to surf the internet.The fixed IP fiber optic always choose this connection type.

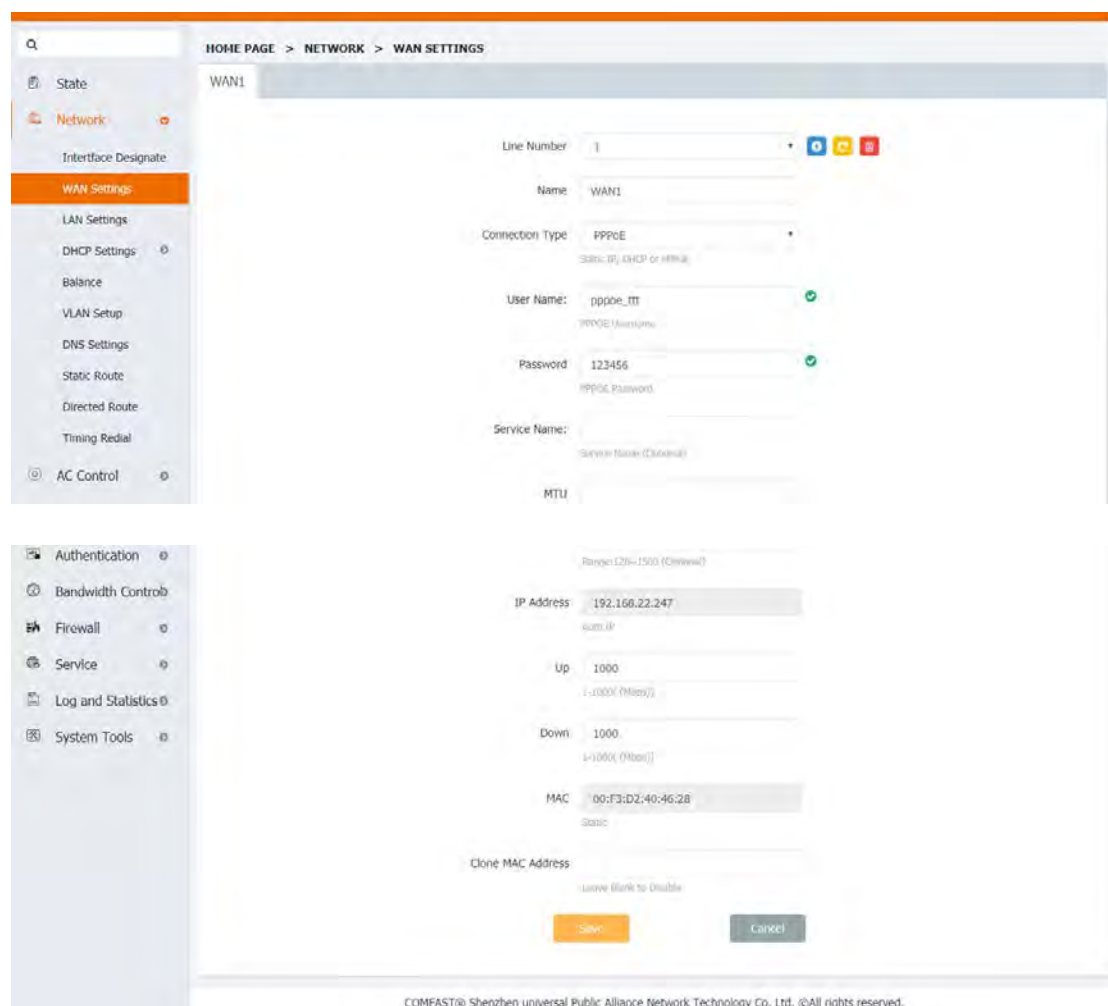


The screenshot shows the ADVICE web interface for configuring WAN settings. The left sidebar contains a menu with options: State, Network, Interface Designate, WAN Settings (highlighted), LAN Settings, DHCP Settings, Balance, VLAN Setup, DNS Settings, Static Route, Directed Route, Timing Redial, and AC Control. The main content area is titled 'HOME PAGE > NETWORK > WAN SETTINGS' and shows the 'WAN1' configuration. The 'Line Number' is set to 1. The 'Name' is 'WAN1'. The 'Connection Type' is 'Static IP'. The 'IP Address' is '192.168.22.247'. The 'Subnet Mask' is '255.255.255.0'. The 'Default Gateway' is '192.168.22.1'. The 'main DNS' is '192.168.22.1'.



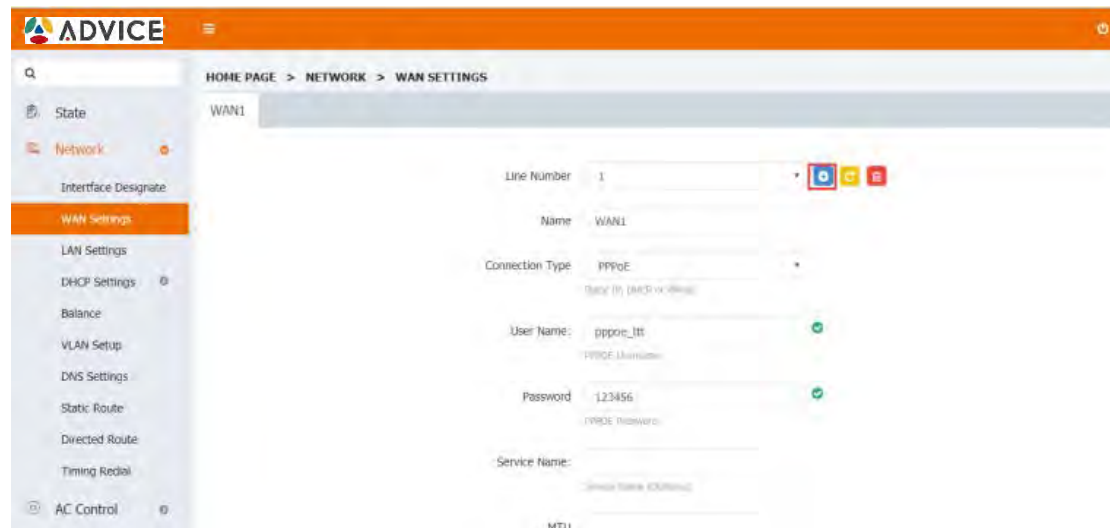
COMFAST® Shenzhen universal Public Alliance Network Technology Co., Ltd. ©All rights reserved.

3.ADSL/PPPoE:after choose this connection type,fill in the related User Name and Password,the state will show connected after success to dial.



COMFAST® Shenzhen universal Public Alliance Network Technology Co., Ltd. ©All rights reserved.

4.Clik“+”,to add multiple network connections on the same interface.



ADVICE

HOME PAGE > NETWORK > WAN SETTINGS

WAN1

Line Number: 1

Name: WAN1

Connection Type: PPPoE

User Name: pppoe_ltt

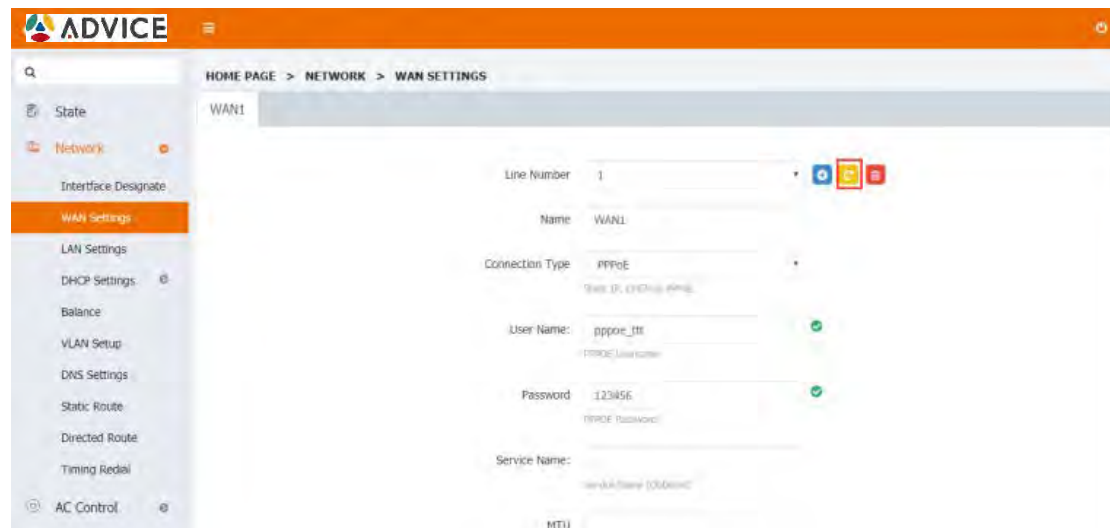
Password: 123456

Service Name:

MTU:

Redial

5. Click "Redial" button to redial the network line



ADVICE

HOME PAGE > NETWORK > WAN SETTINGS

WAN1

Line Number: 1

Name: WAN1

Connection Type: PPPoE

User Name: pppoe_ltt

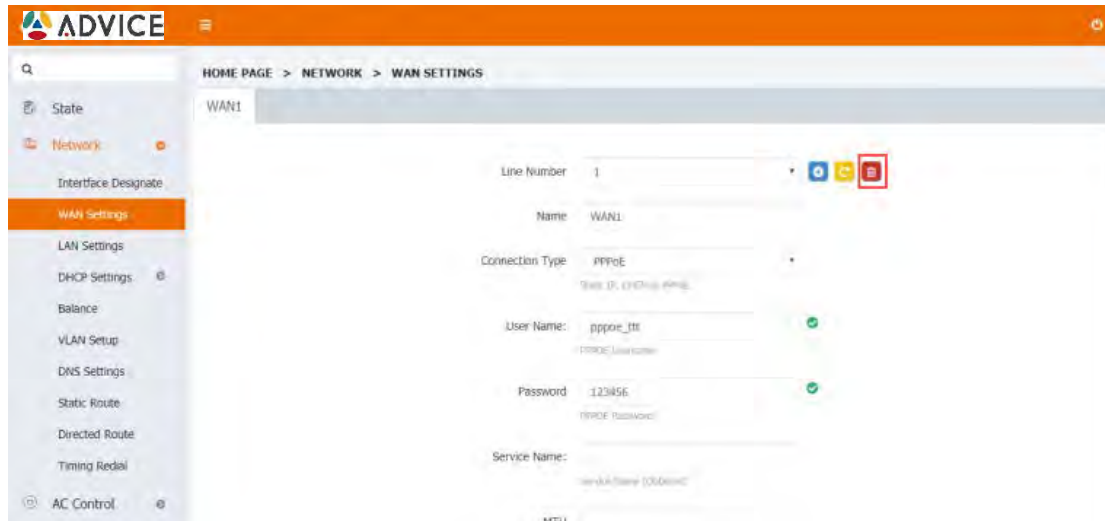
Password: 123456

Service Name:

MTU:

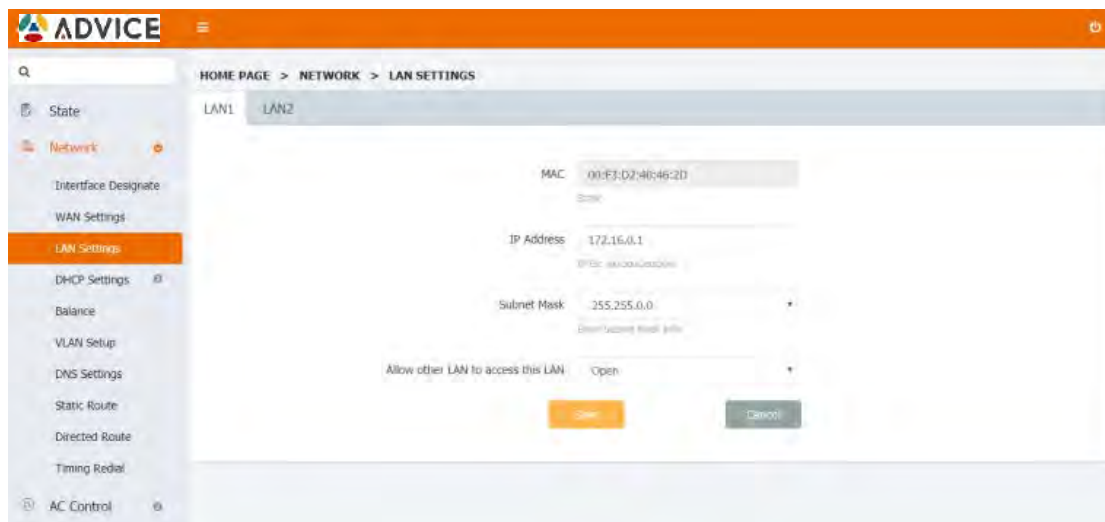
Redial

6. Click the delete button to delete unnecessary Internet lines. The first one cannot be deleted



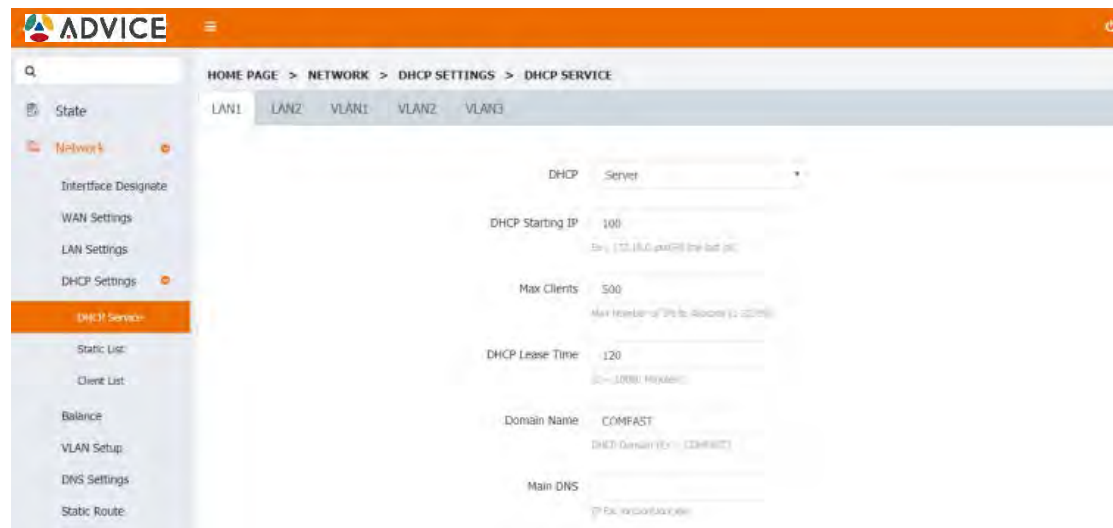
3.2 Local Network Settings

Can manual setting each Local Interface's IP Address and Subnet Mask , the default IP address is 172.16.0.1



3.5 DHCP Settings

DHCP Settings: Here you can set up DHCP start IP, Address number, DHCP Lease Time, Domain Name, main DNS and backup DNS, you can also disabled DHCP function. (Attention: At the situation of disabled DHCP function, the device will not offer IP to client, and client need to manual setting the IP address and the device manage IP in the same segment)



HOME PAGE > NETWORK > DHCP SETTINGS > DHCP SERVICE

LAN1 LAN2 VLAN1 VLAN2 VLAN3

DHCP Server

DHCP Starting IP 100
By: 192.168.1.1 (192.168.1.1)

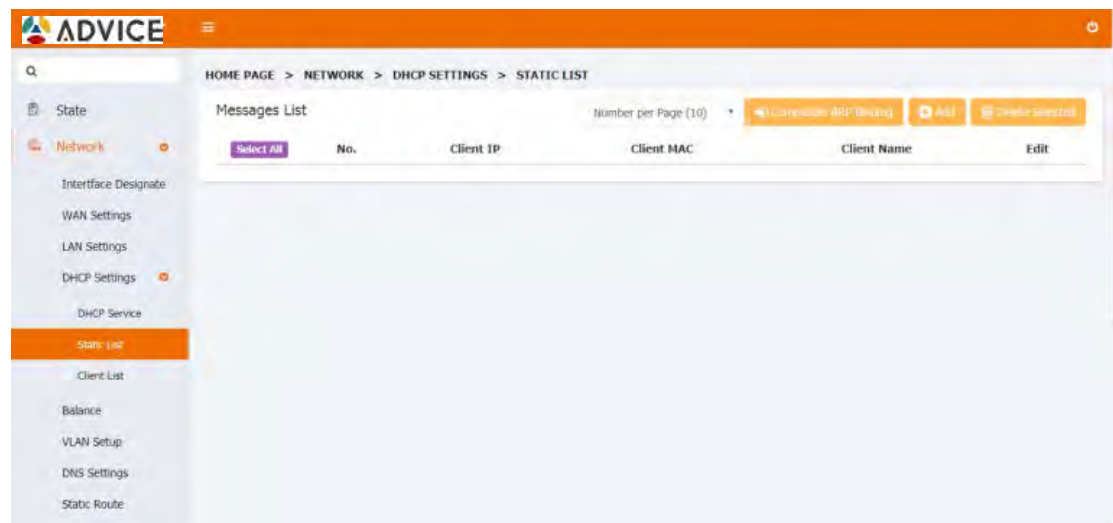
Max Clients 500
Max Number of IP to Assign (1-255)

DHCP Lease Time 120
0-1000 Minutes

Domain Name COMFAST
DHCP Domain Name (COMFAST)

Main DNS 192.168.1.1
IP Address (192.168.1.1)

Static List: Local network client get the IP address to the designated IP address by the DHCP, you can add it in this place. Here you can install the compatible ARP binding information, and also can install the PC or mobile device IP address to static allocation, then those device will get the fixed IP.



HOME PAGE > NETWORK > DHCP SETTINGS > STATIC LIST

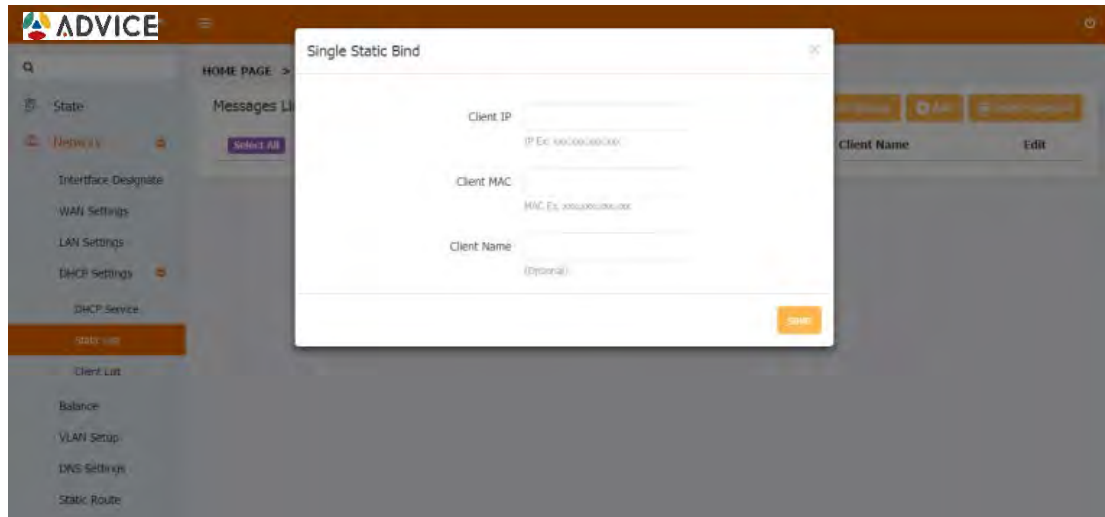
Messages List

Number per Page (10)

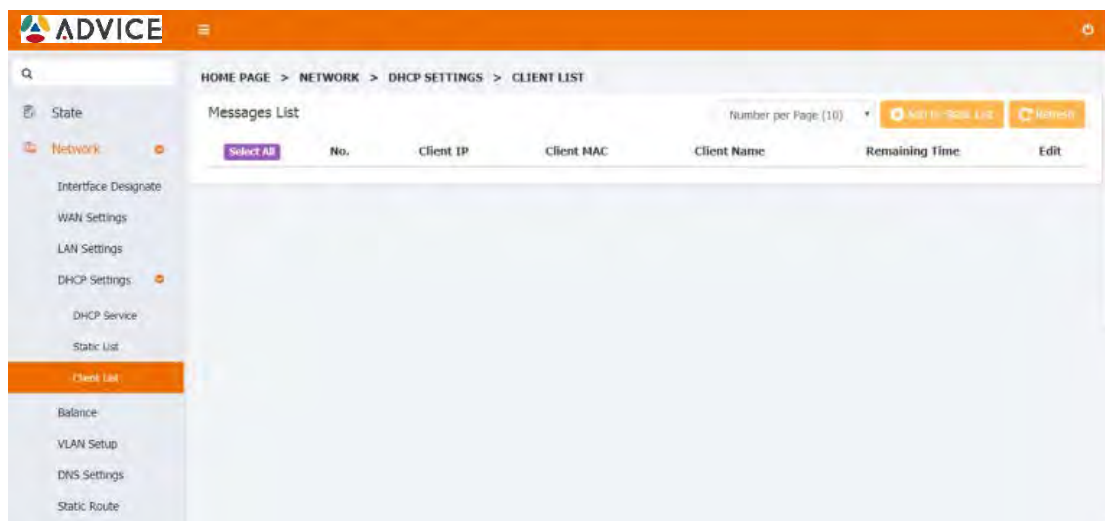
[Select All](#) [Add](#) [Delete Selected](#)

No.	Client IP	Client MAC	Client Name	Edit

Add single static bind, click “Add” button in the static list and got to set up.



Client List: Here will display the DHCP allocated CLIENT IP, CLIENT MAC, CLIENT NAME when you connect with the device. You can install which client IP to the static list by your actual needs.



3.5 Balance

Balance: when the multiple ISP line insert, choose balance strategy, install corresponding rate. the same or different ISP line will allocate the bandwidth by balance strategy.

HOME PAGE > NETWORK > BALANCE

Balance

Wan line	Balance	Weight:
WAN1	☐	1 ▼

Save Cancel

Multiline Route: Install purpose:play Netcom game through Netcom,play Telecom game through Telecom.

Multiline Route

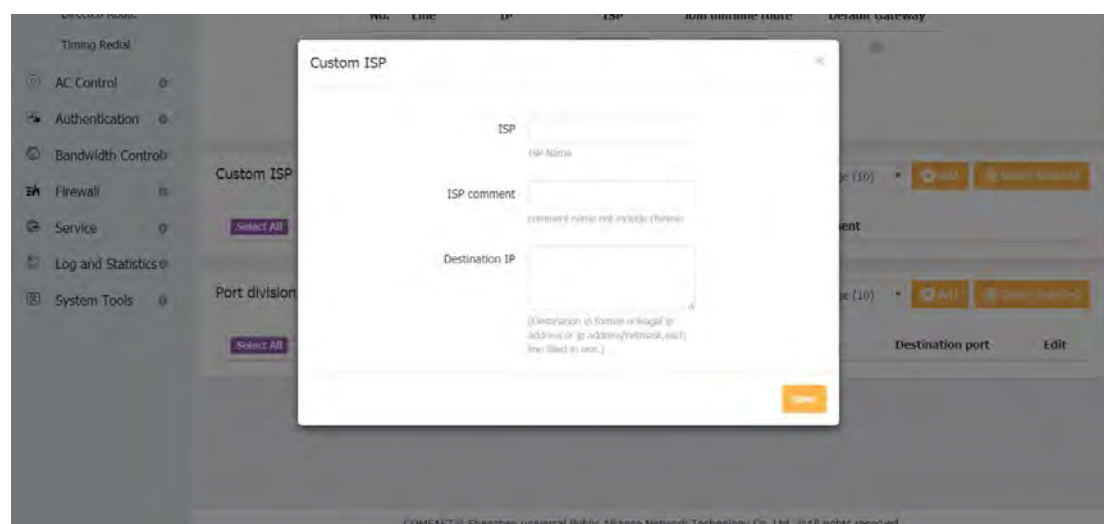
Multiline route switch (Multiple different ISP lines,please enable multiline route,and load balance is diabled.)

Enabled ▼

No.	Line	IP	ISP	Join multiline route	Default Gateway
1	WAN1	192.168.22.247	choose isp ▼	join ▼	☐

Save Cancel

Custom ISP:If the list haven't corresponding broadband ISP,you can custom add ISP.Collect the full ISP IP,add it according to the format,then install mutilive route.

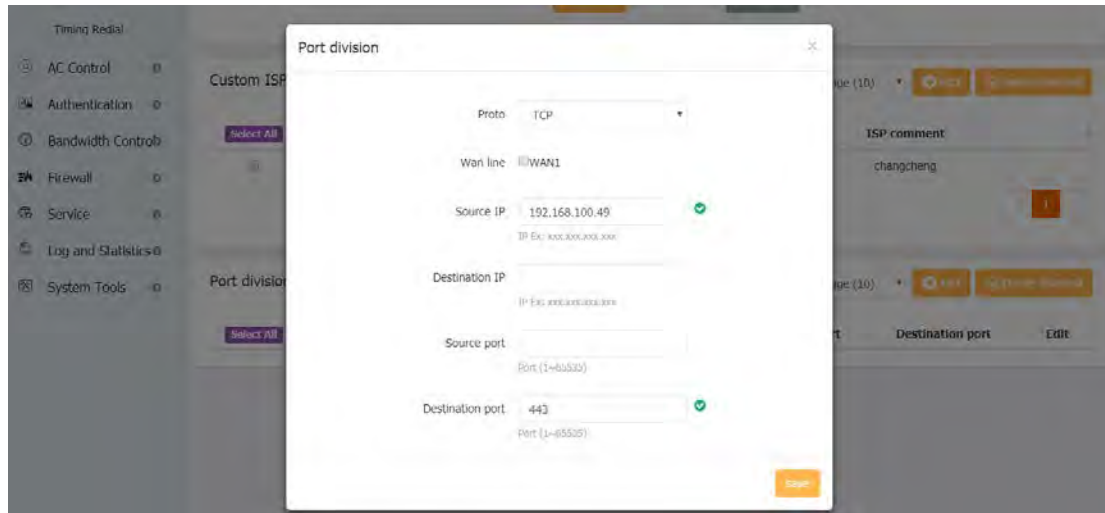


COMFAST © Shenzhen Universal Public Alliance Network Technology Co., Ltd. ©All rights reserved.

1. It will go through the specific exit when the local network appointed IP to visit some internet ports.

Attention:At the normal situation,you can not enter the DESTINATION IP and SOURCE PORT.When your local internet IP is specific,you will need to enter the DESTINATION IP.

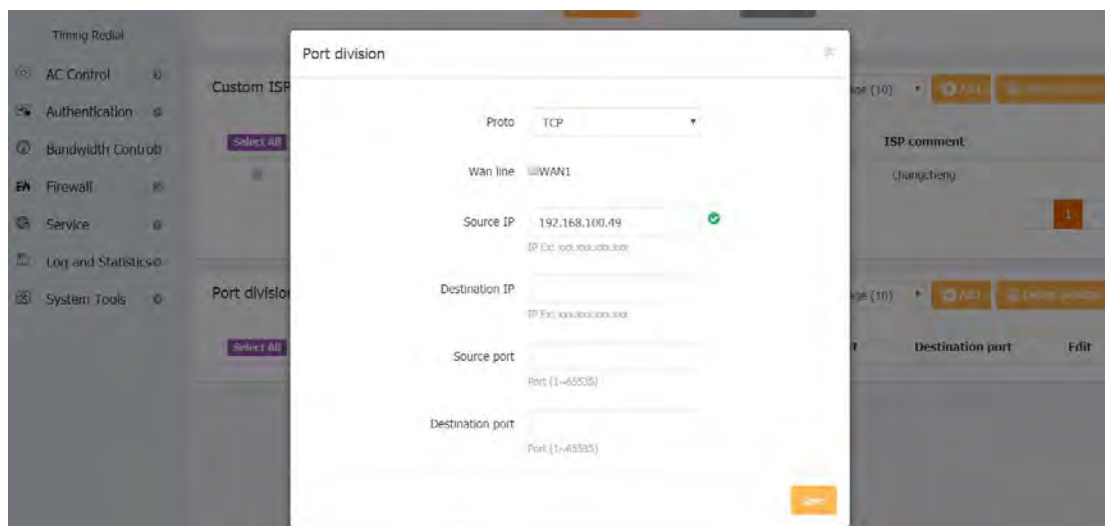
Port division		Number per Page (10)		Add		Delete Selected		
Select All	No.	Proto	Wan line	Source IP	Destination IP	Source port	Destination port	Edit



2.You can install local internet appointed IP in specific wan line

Step:Proto choose at random,Wan line choose appointed one you need,Source choose the appointed IP you need,Destination IP not need to write.

Example:192.168.100.49 enter in WAN2.



3.7 VLAN Settings

VLAN is a LAN device can be logically divided into a network segment, in order to achieve the virtual workgroup's emerging data exchange technology. This emerging technology is mainly used in switches and routers, but the mainstream application is still in the switch, but not all

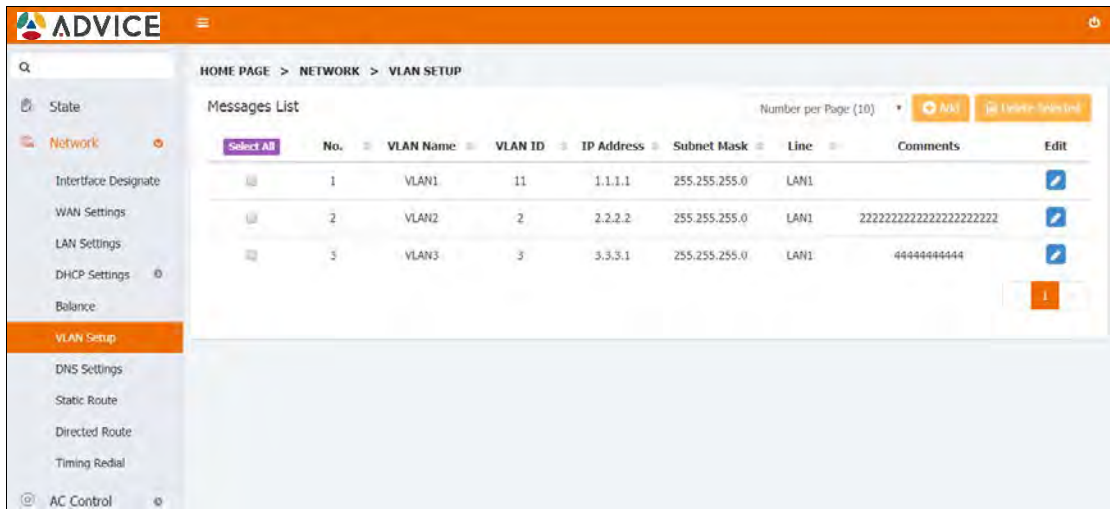
switches have this feature, only the VLAN protocol on the second floor of the switch with this feature, which can be through the corresponding switch Of the manual can be learned.

VLAN SETUP;

Visit the VLAN SETUP page, click “add” on the upper right corner. Create a VLAN and set a virtual IP address.

VLAN ID: Virtual LAN ID number, used to distinguish between different VLANs

IP: This IP address is the address of this VLAN.

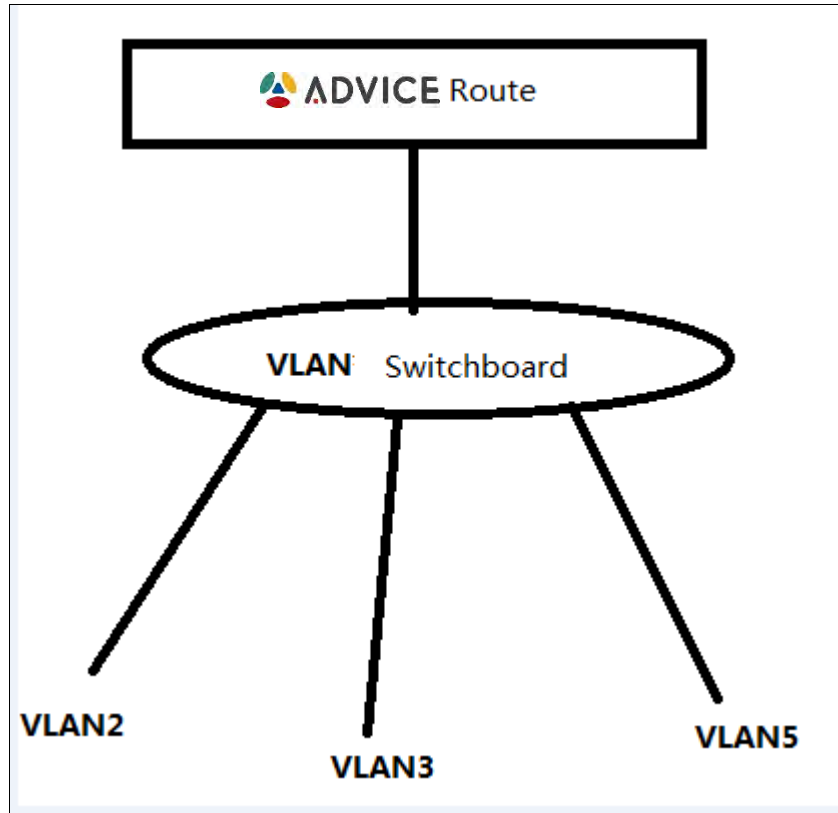


The screenshot shows the ADVICE web interface for VLAN SETUP. The breadcrumb navigation is HOME PAGE > NETWORK > VLAN SETUP. The main content area displays a 'Messages List' table with the following data:

No.	VLAN Name	VLAN ID	IP Address	Subnet Mask	Line	Comments	Edit
1	VLAN1	11	1.1.1.1	255.255.255.0	LAN1		
2	VLAN2	2	2.2.2.2	255.255.255.0	LAN1	22222222222222222222222222222222	
3	VLAN3	3	3.3.3.1	255.255.255.0	LAN1	444444444444	

The interface also includes a sidebar with navigation options: State, Network (selected), Interface Designate, WAN Settings, LAN Settings, DHCP Settings, Balance, VLAN Setup (highlighted), DNS Settings, Static Route, Directed Route, Timing Redial, and AC Control. The top right corner features a search bar and a 'Number per Page (10)' dropdown. The bottom right corner has a '1' button.

Basic VLAN topology:



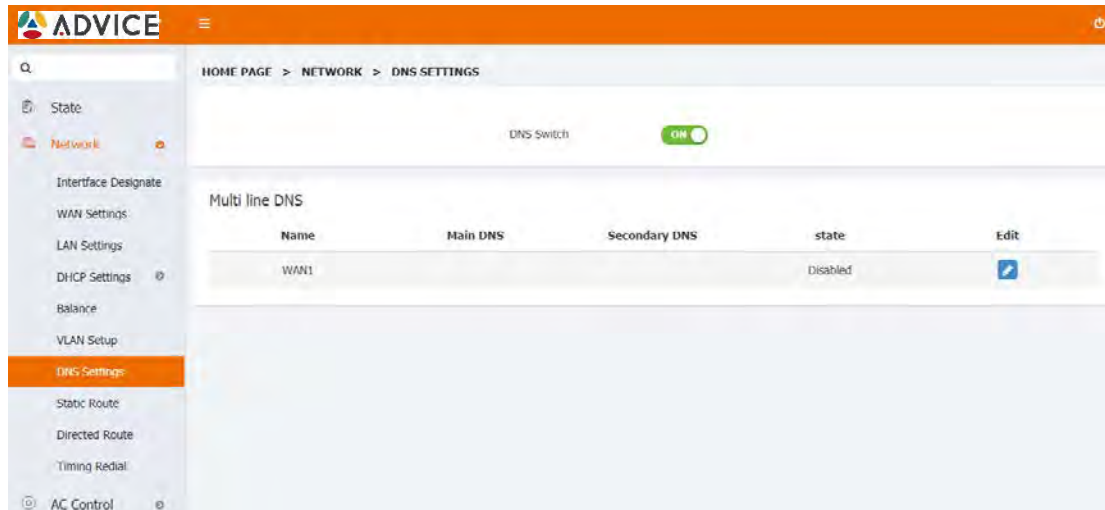
Note: The VLAN ID must correspond to the VLAN ID in the switch. The LAN port of the router directly connect to the trunk of VLAN switch.

3.7 DNS Settings

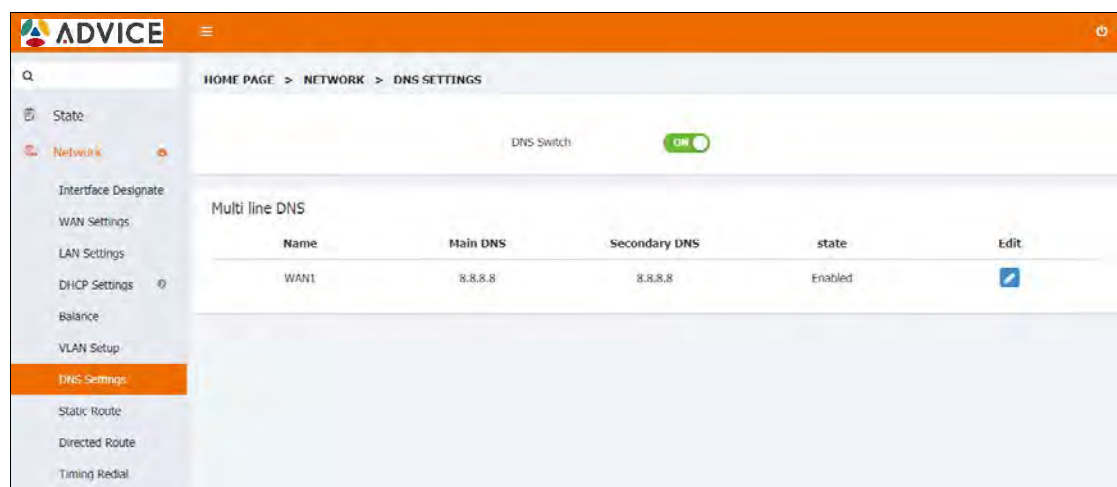
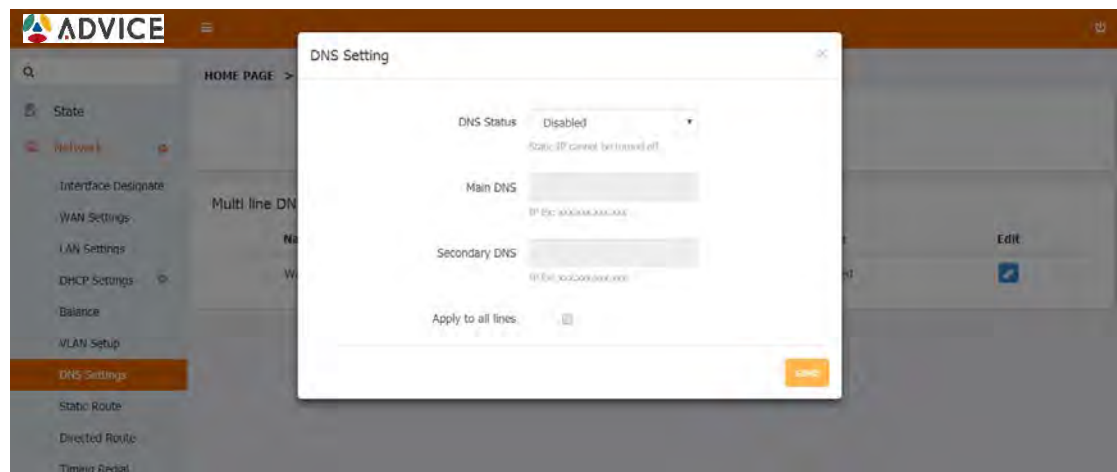
DNS Settings: DNS(Domain Name System), in the Internet, it is used as one distributed database by mutual mapping between the domain name and IP address. The process of finally getting this hostname-related IP through the hostname is called DNS (or Hostname Resolution). At the Static IP Mode, need to manually set up Main DNS and Secondary DNS. If you don't know your local DNS address, you can contact with your broadband network operator.

1、首页点击“网络设置-DNS 设置”，进入 DNS 设置界面，打开 DNS 开关

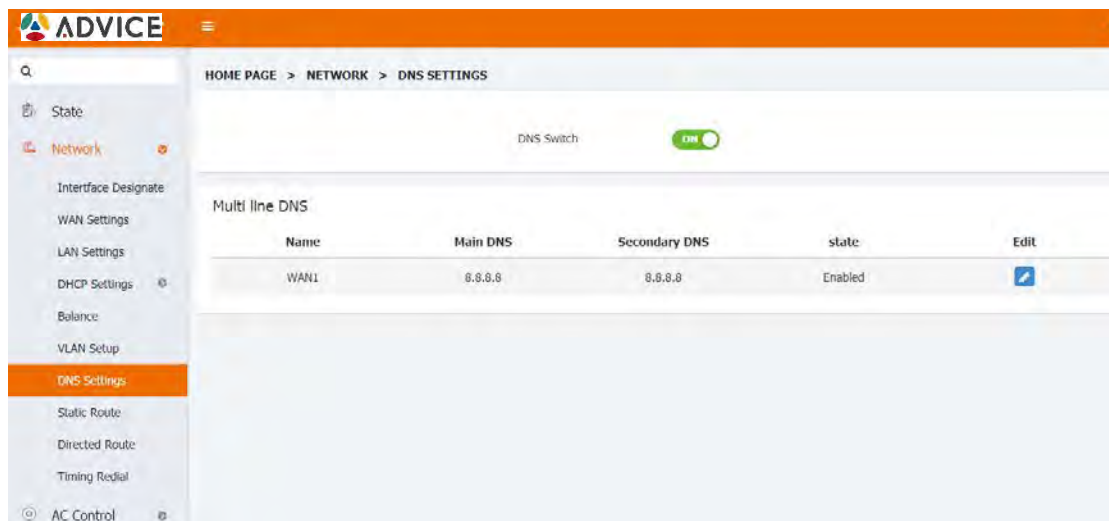
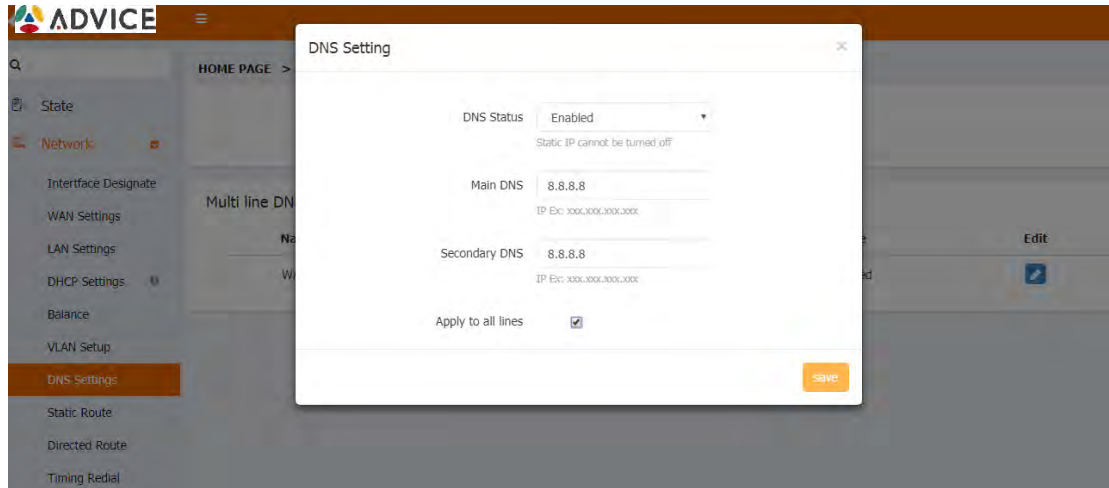
1. Homepage Click "Network - DNS Settings" to enter the DNS setting interface, open the DNS switch



2. Select the need to set the DNS line, click the operation button, pop-up action box, DNS state is selected as enabled, enter the main DNS or secondary DNS, click save

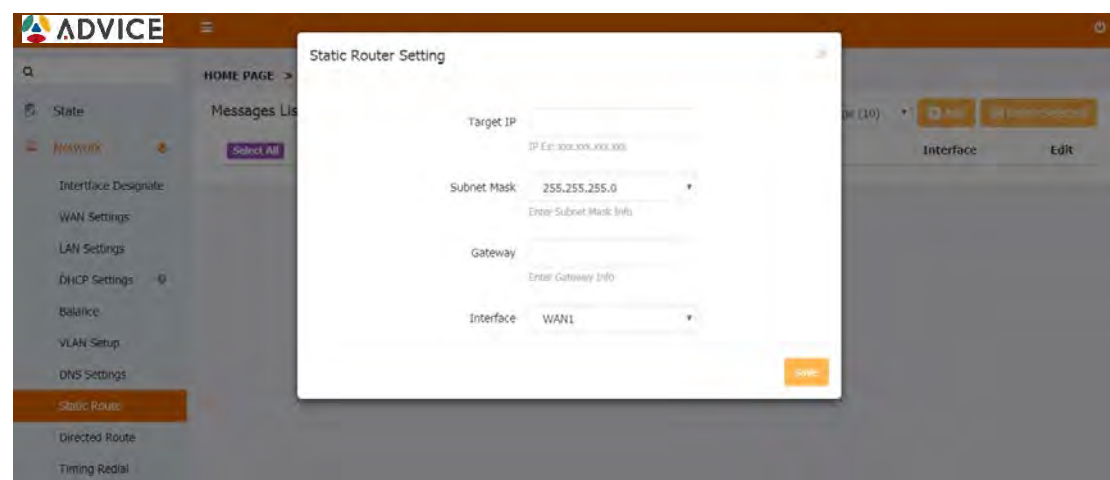
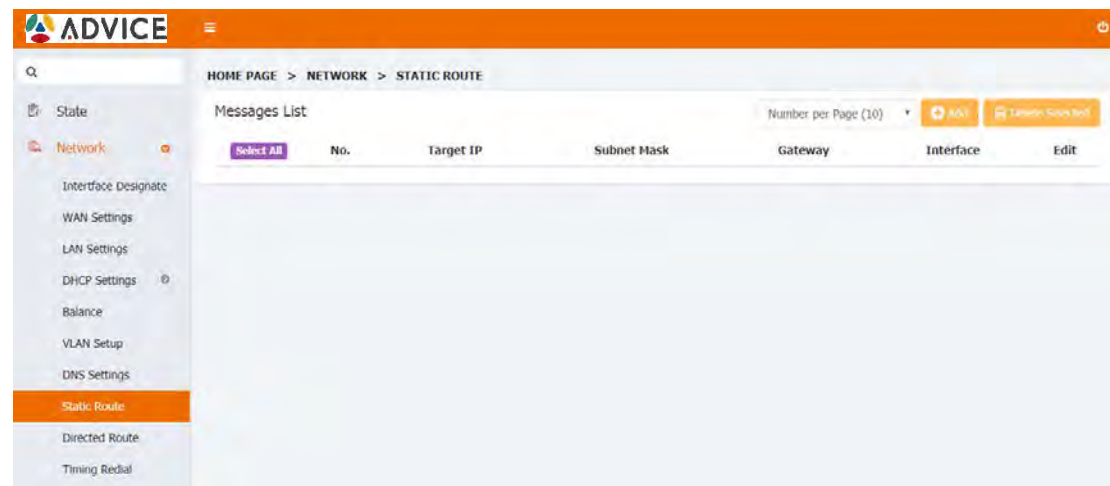


3. Click "Apply to all lines" in the action box and click save to apply the current settings to all lines



3.8 Static Route

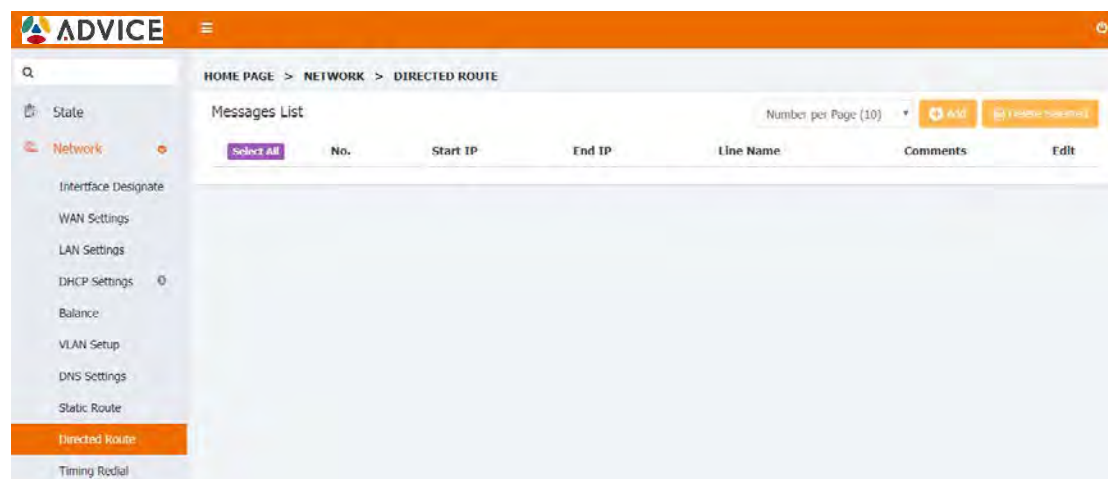
The route static allocation function,once the computer add the static allocation,the IP is appointed by the static allocation when you starting up next time.



3.9 Directed Route

Directed route means setting a fixed network flow direction and pointing data from one port to another fixed port instead of wide area and no purpose.

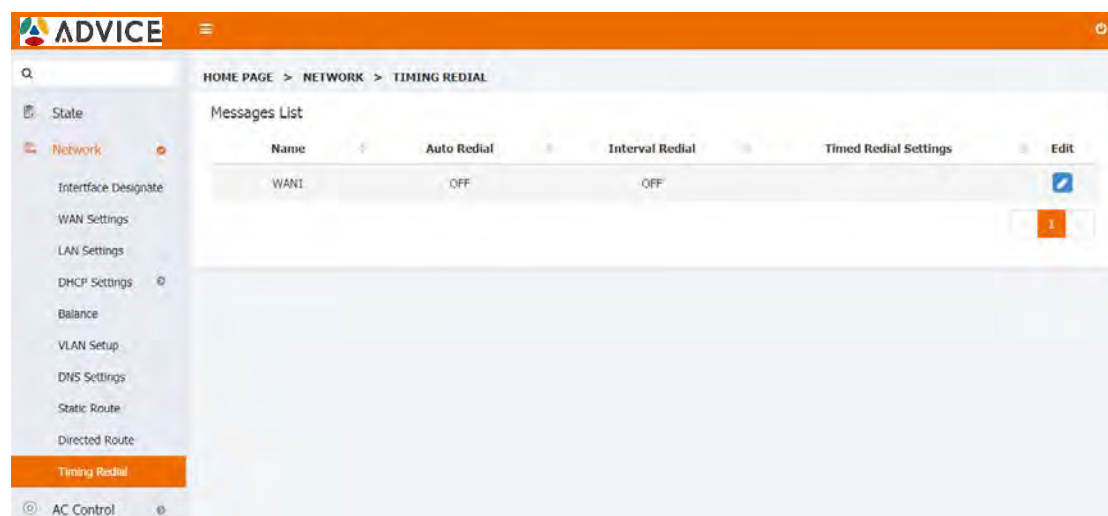
1. Click on "Network- Directed Route" to enter the Directional Routing Settings page, click the "+Add" button, enter the starting IP, end IP and destination line name, click Save, set the start IP to end all IP IP data The flow direction is specified to wan1 and does not pass through other wan ports.



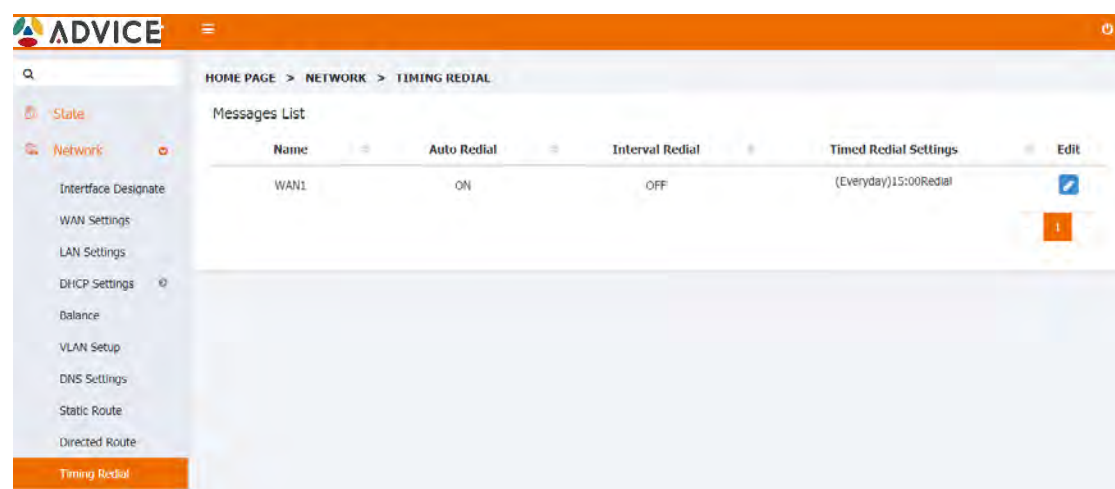
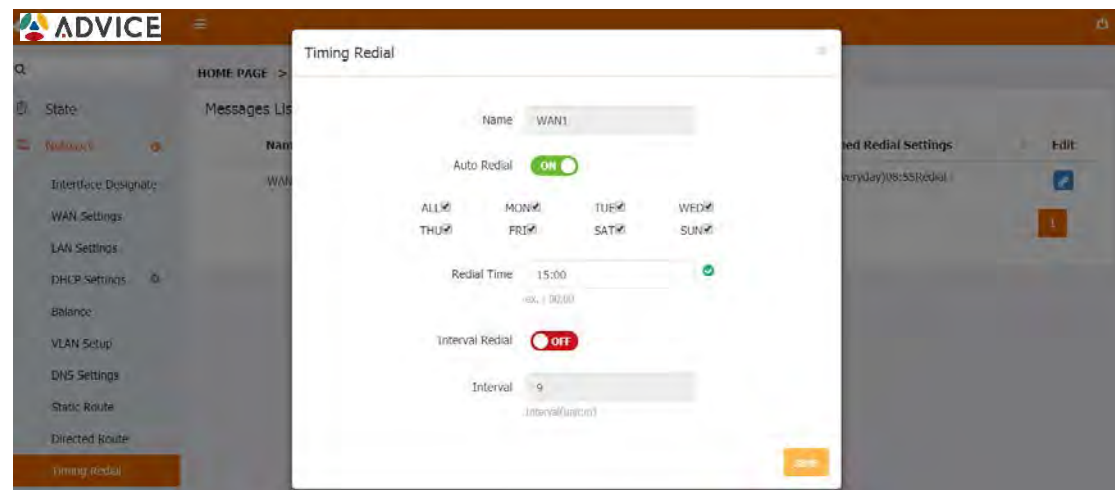
3.9 Auto Redial

Auto redial: set a specific time or a specific interval to allow automatic redialing of a specific line

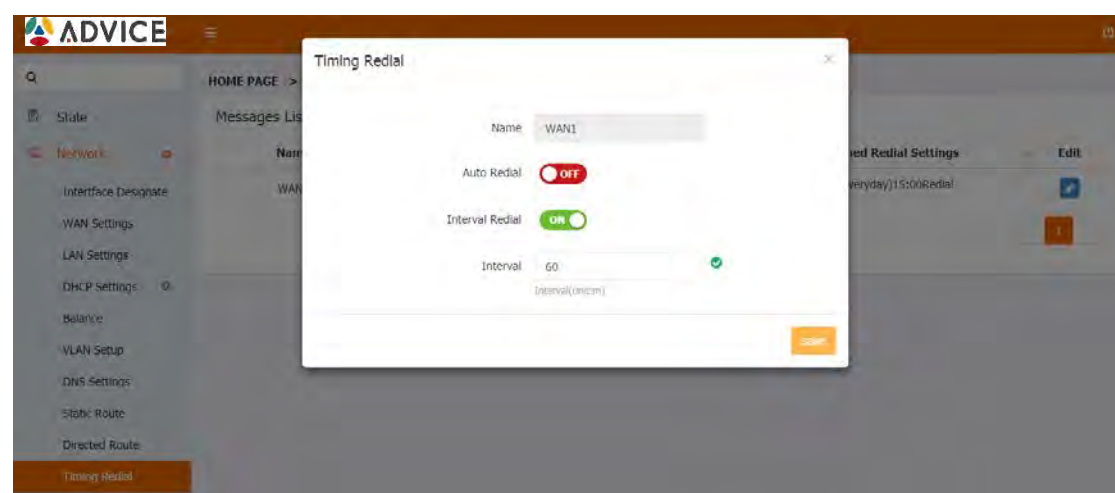
1. Click "Network - Auto Redial" to enter the auto redial page

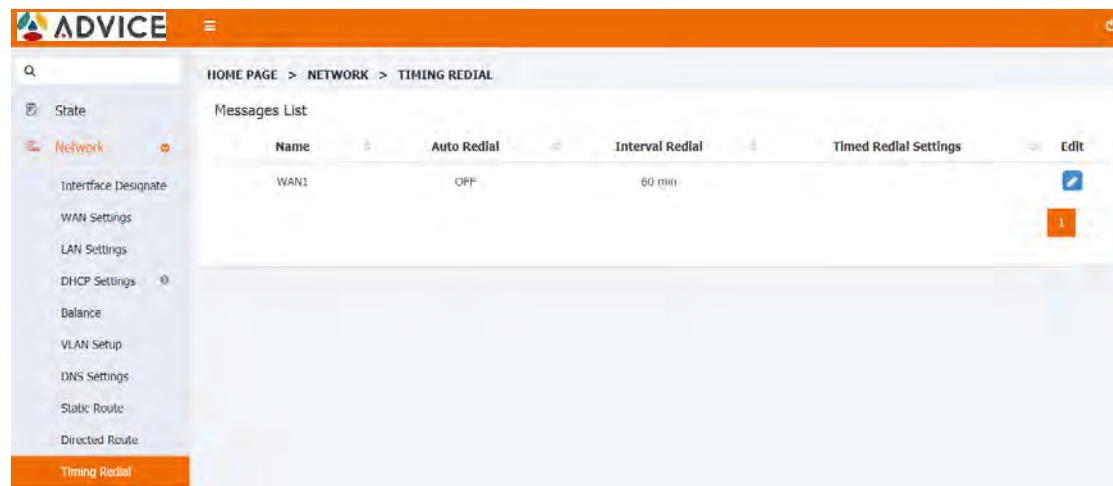


2. Click on the operation button of one of the lines to pop up the operation box, enable the auto redial status, check the date, and click save after completing the time. As shown in the photo below, the WAN1 line automatically redials at 15:00 every day.



3. The operation box to open the interval redial, enter the interval restart time, click save, as shown below, after successful preservation WAN1 line re-dial every 60 minutes





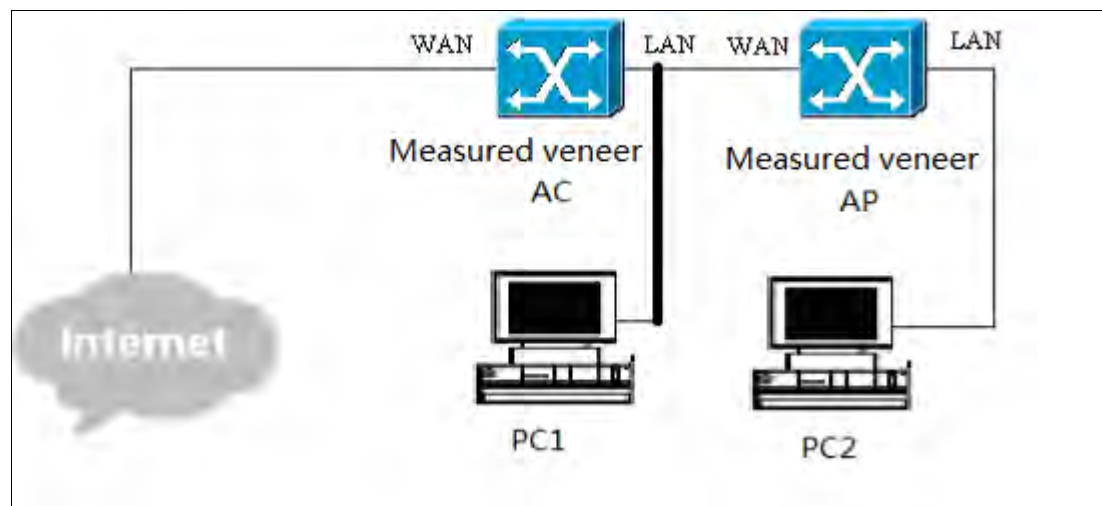
4 AC Control

Uplink AC and By-pass AC is the network develop type.

Uplink AC is the AP in AC's next level, the AP connects with the AC's internal network, and the connection way is AC's LAN port connects with AP's WAN port, detail as chart 1.

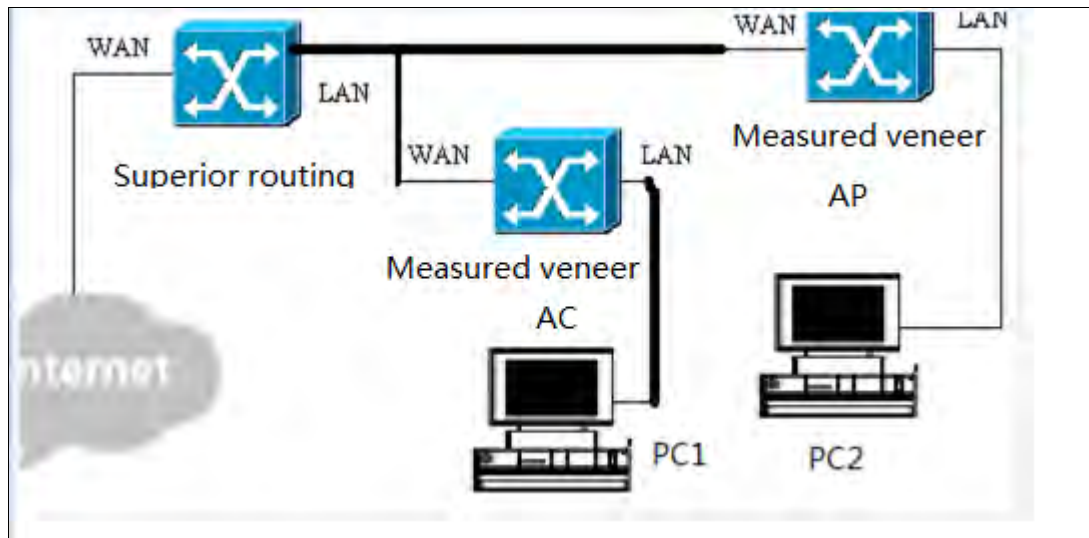
By-pass AC is AP and AC connect with the same network, the connection way is the up one level gateway connects with the WAN port of AC and AP, after the AC and AP connect successfully, you can visit AC management page through AC's WAN port IP, detail as chart 2.

Uplink AC Management



<Chart 1>

By-pass AC Management

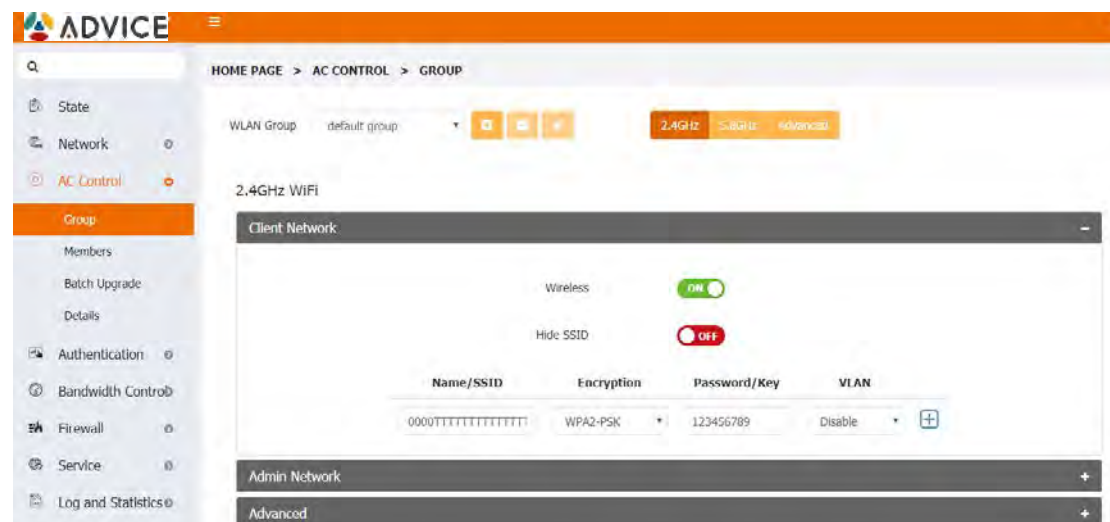


<Chart 2>

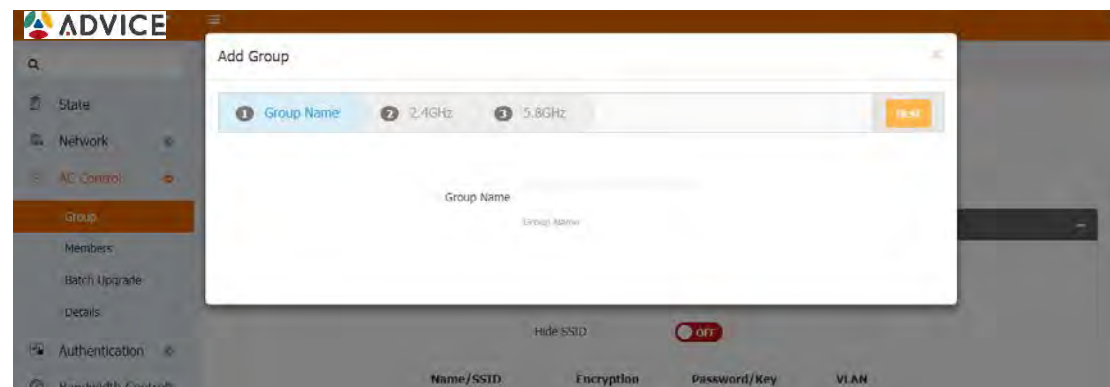
4.1 Group

Here you can install a new group, can install 2.4G and 5.8G SSID, wireless advanced install those parameters.

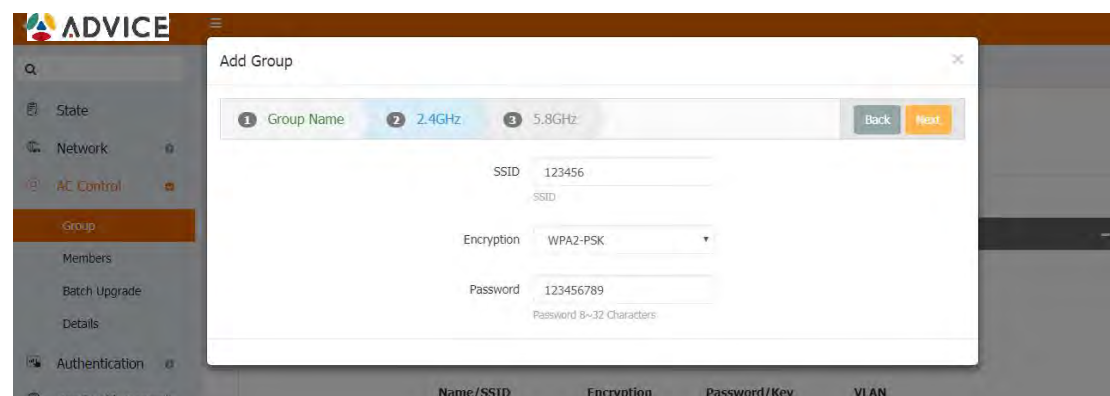
1. Open the WEB home page, go into AC Control's "Group" page, as below:



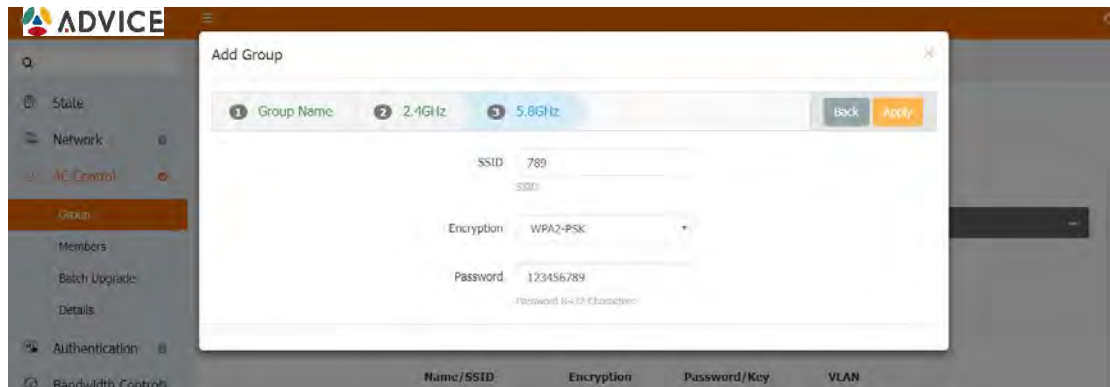
2. Click above picture's "+" button and go into the add group page, as below:



3. Setup 2.4GHz relative parameter (SSID/Encryption/Password), click Next:



4. Setup 5.8GHz relative parameter (SSID/Encryption/Password), click Next:



5. Click “Apply” and it will go to “GROUP” page, then it is success to add group. Choose the group name: comfast and you can detail setup this group.

Chart 1: Employee network, you can setup the NAME/SSID and PASSWORD/KEY.

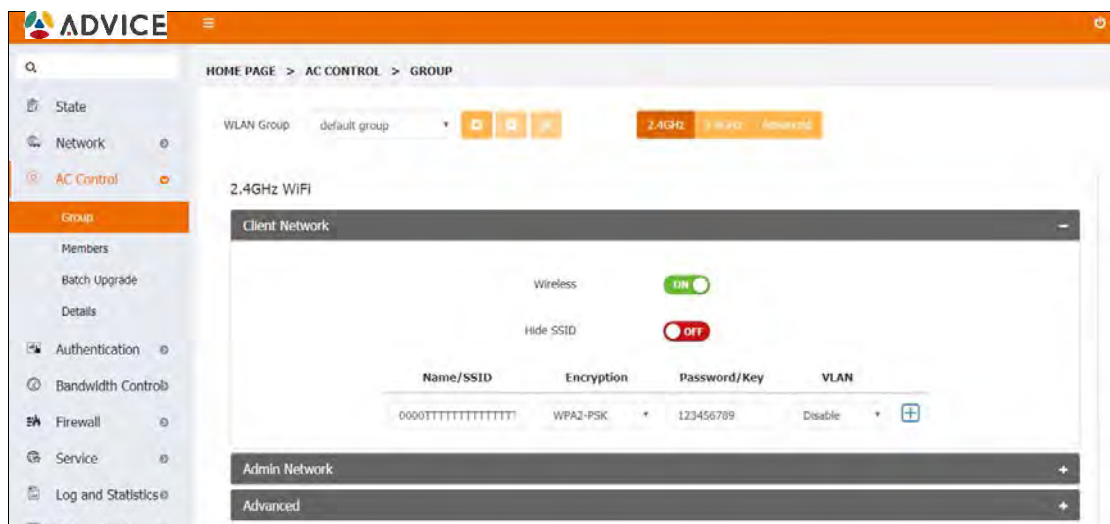


Chart 2: Management network, you can setup the NAME/SSID and PASSWORD/KEY.

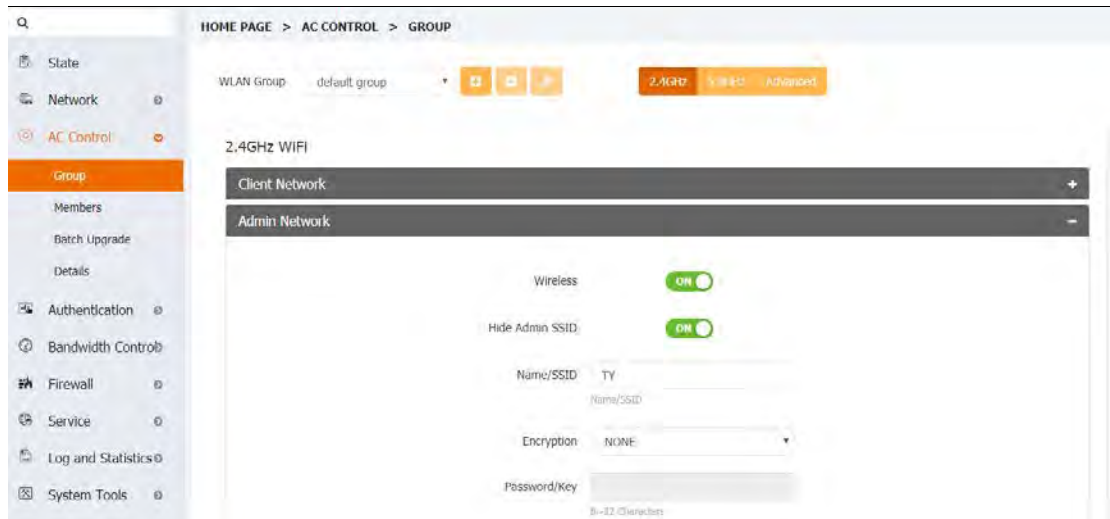
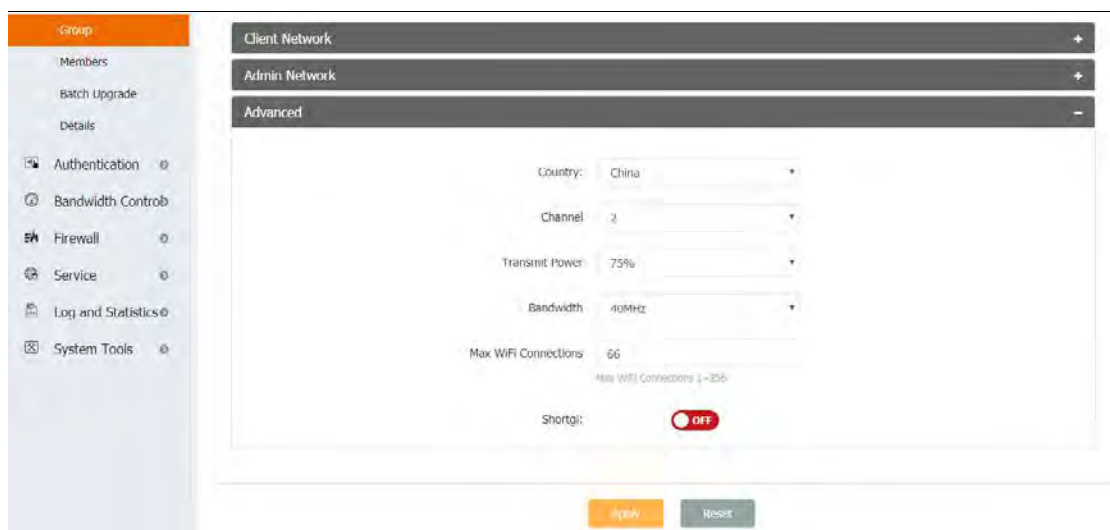
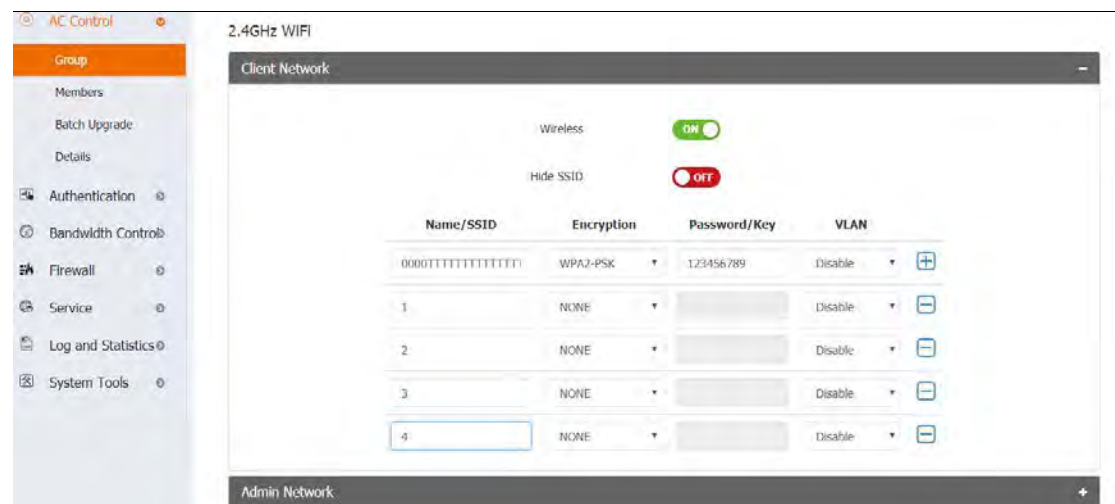


Chart3:Advanced,here you can setup Country,Channel and Txpower etc.relative parameters.

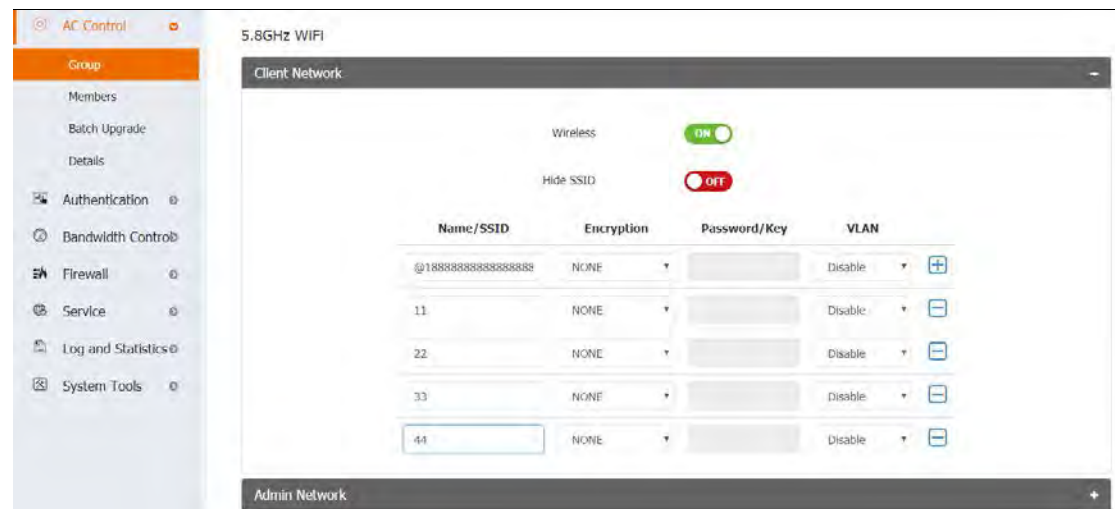


6. Click “Employee” bottom right “blue+” in above chart 1,you can setup multi SSID function,the most you can add 8 SSID(2.4G and 5.8G can add 4 SSID separately),as below:

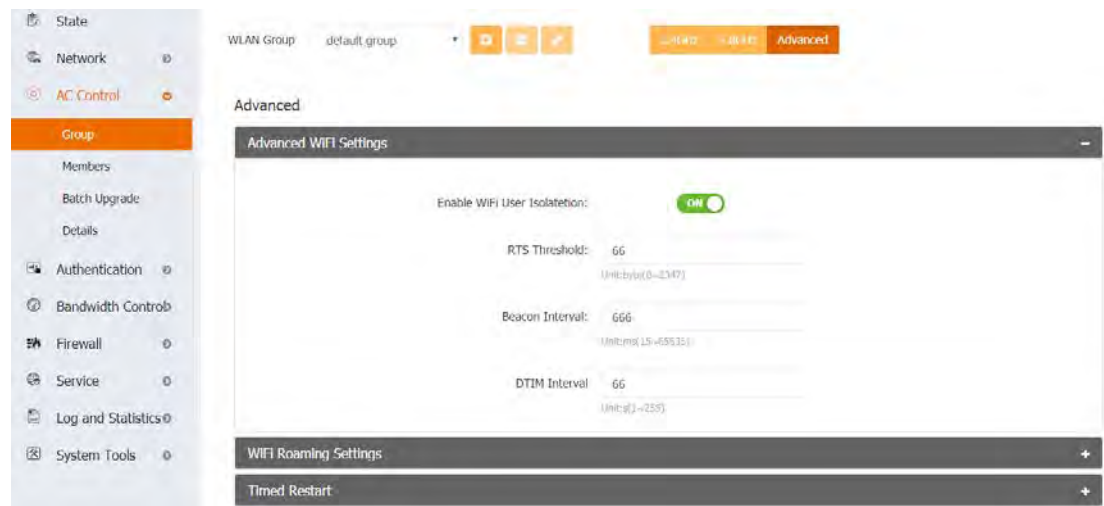
2.4G Multi -SSID:



5.8G Multi -SSID:



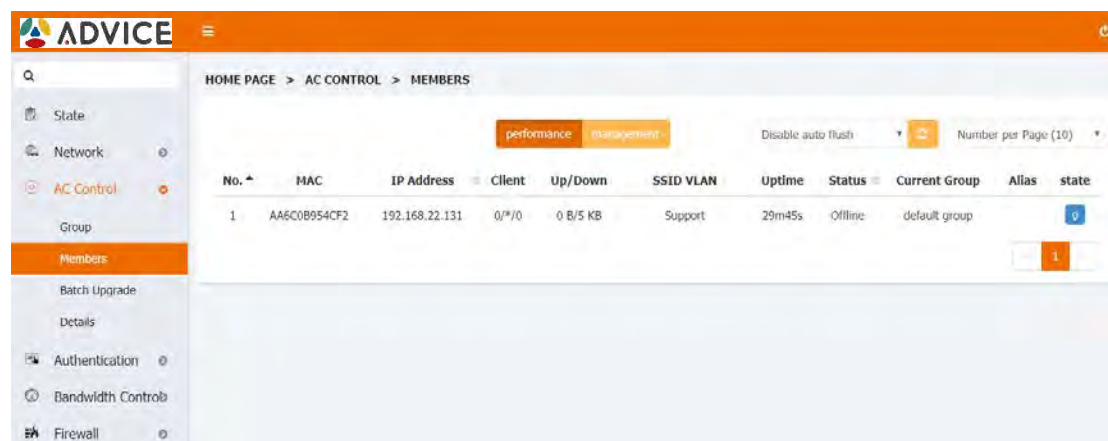
8. Click Advanced Settings to open Wireless User Isolation to isolate wireless users



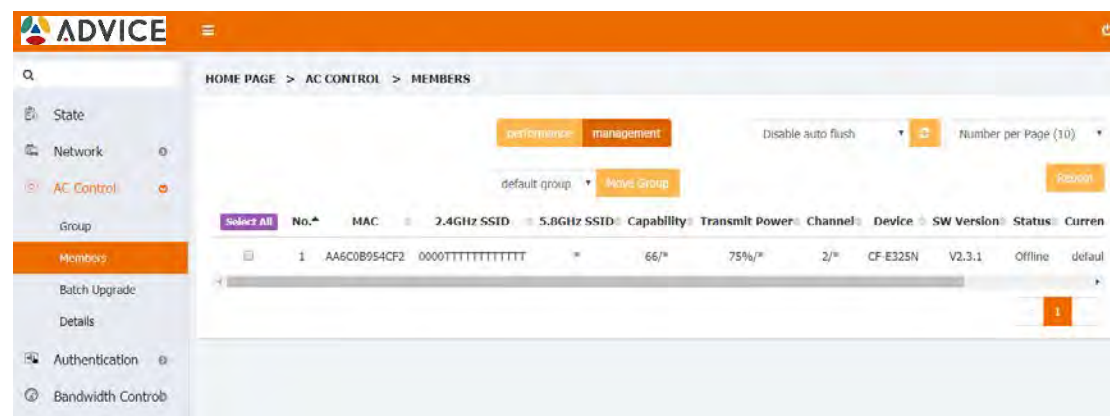
4.2 Members

If there have other devices connect with x86 network, the managed device information will be show on the performance page. Click management, and here you can modify the corresponding device's wireless SSID, country, channel, transmitted power, wireless bandwidth, max-awating amount and alias.

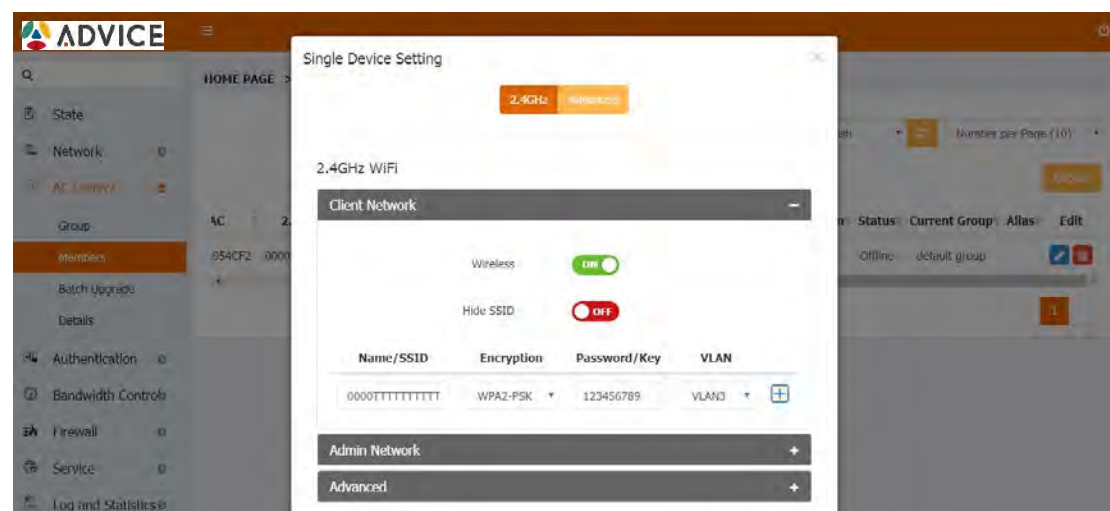
1. Open WEB home page and go into AC Control's "Members" page, as below:



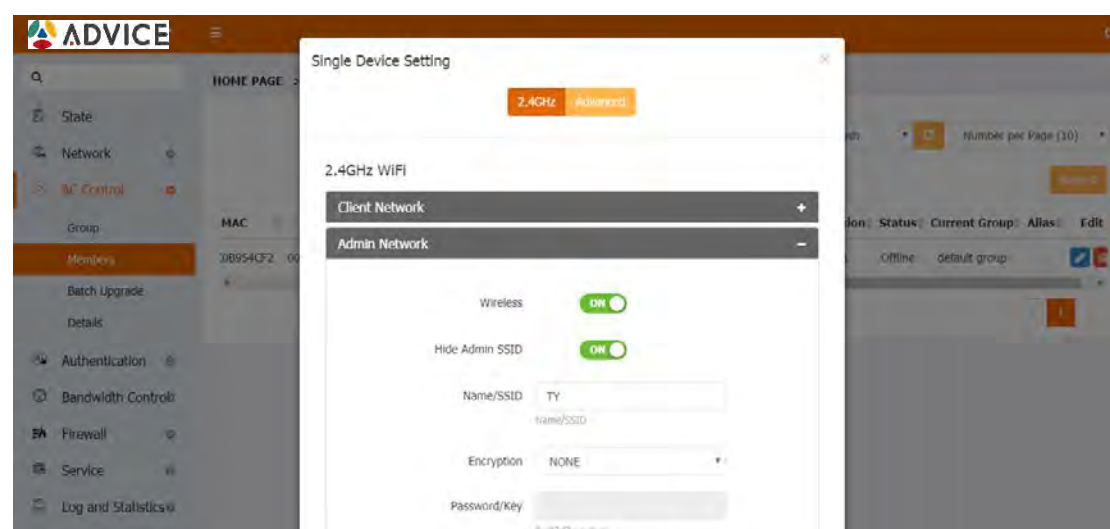
2. Click above picture's middle position "management" button, and go into the managing page, as below:



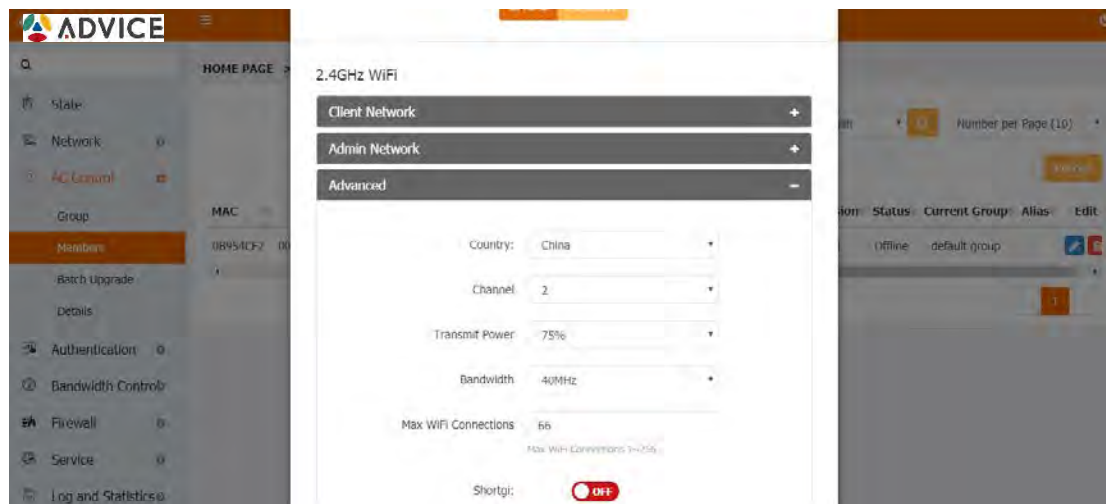
3. Click above picture's "blue" button then you can renew the device's SSID, Country, Channel and Txpower etc. detail managing information, as below:



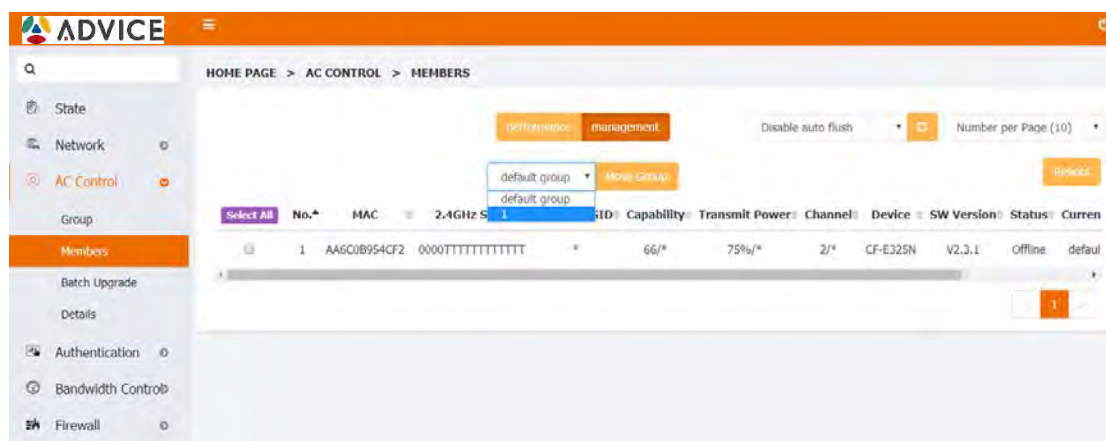
4. Click Management network



5. Click Advanced:

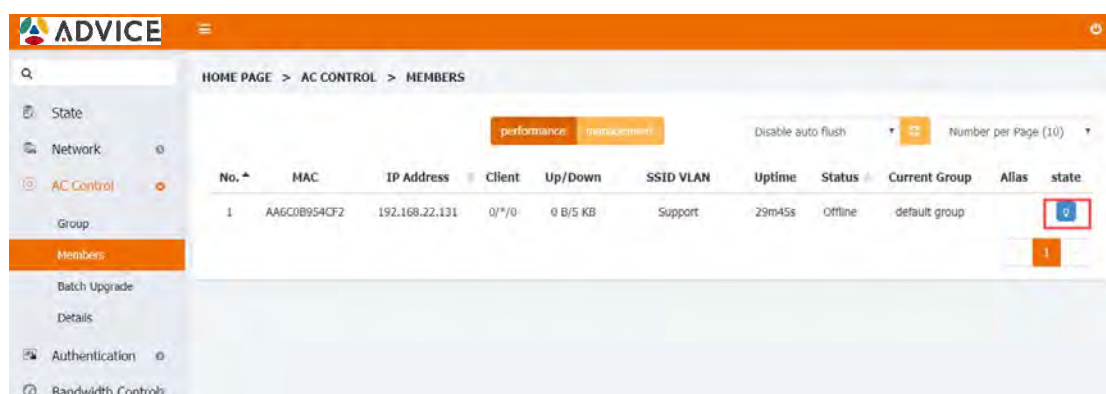


6. Change the group name: click the middle trilateral drop-down button -> choose the group name (comfast) -> select the devices -> click "move group" button.



6. Click "Performance" button to enter the performance display interface. Click the LED light control button to turn off the LED light of the management device.

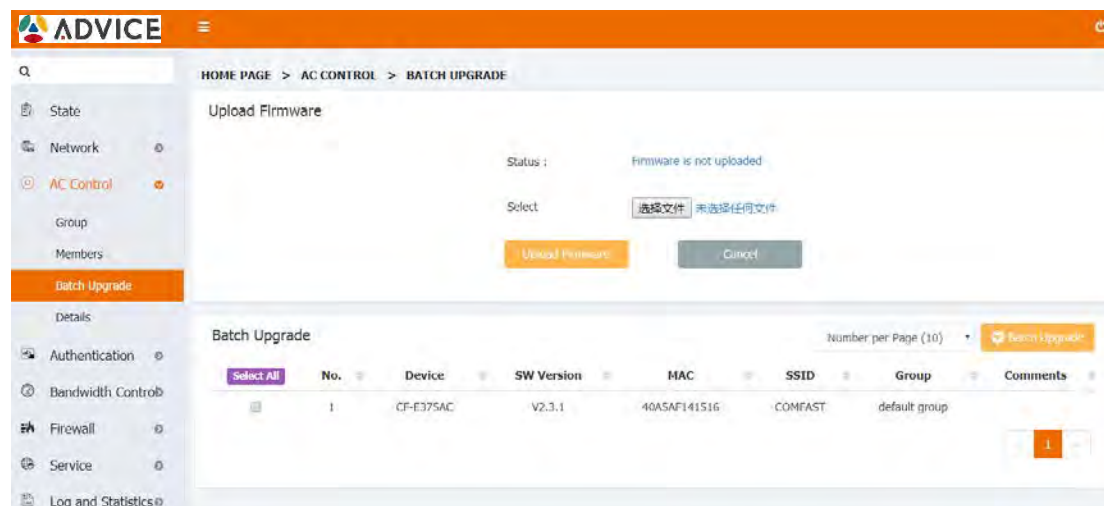
Click again to open the LED light of the management device.



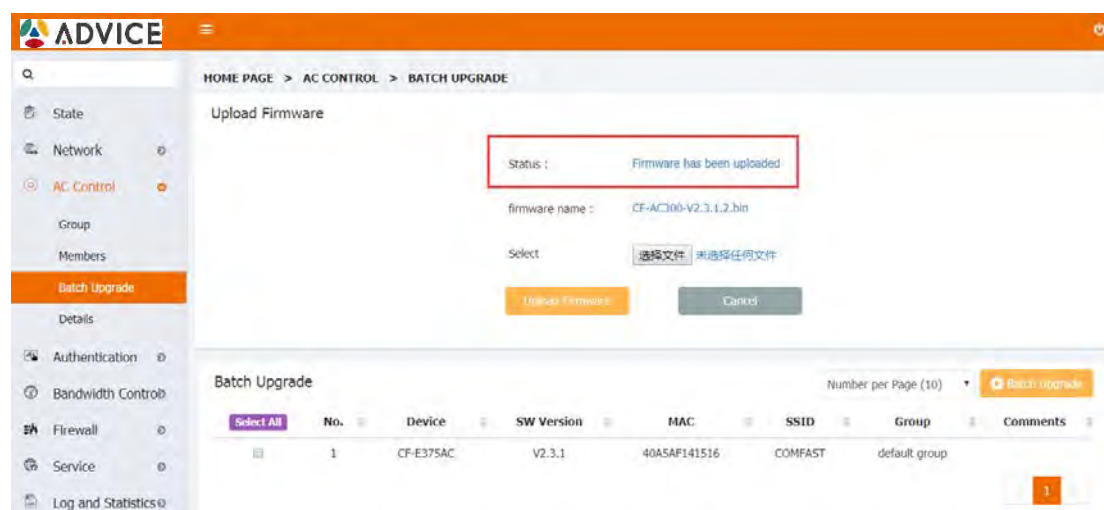
4.3 Batch Upgrade

When all devices in one group are batch upgrading, connect with the upgrading computer will appear "Network connection is broken, pls reconnection", You can check the firmware version and other information in the relogin upgrade device, and you will find that the firmware version was changed, but the wireless configuration information will keep the old configuration.

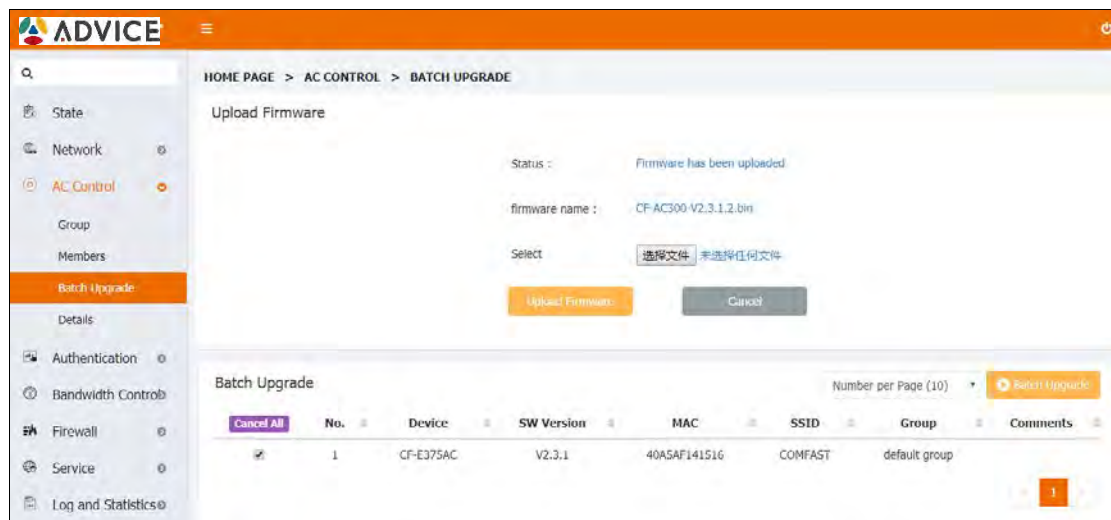
1. Open WEB home page, go into AC Control's Batch Upgrade page, as below:



2. Click above picture's "Browse" button, choose the newest firmware which you want to upgrade in the local computer, click "Upload Firmware" button, it will be success to upload after 5 seconds, and the status will show "Firmware is uploaded", as below:



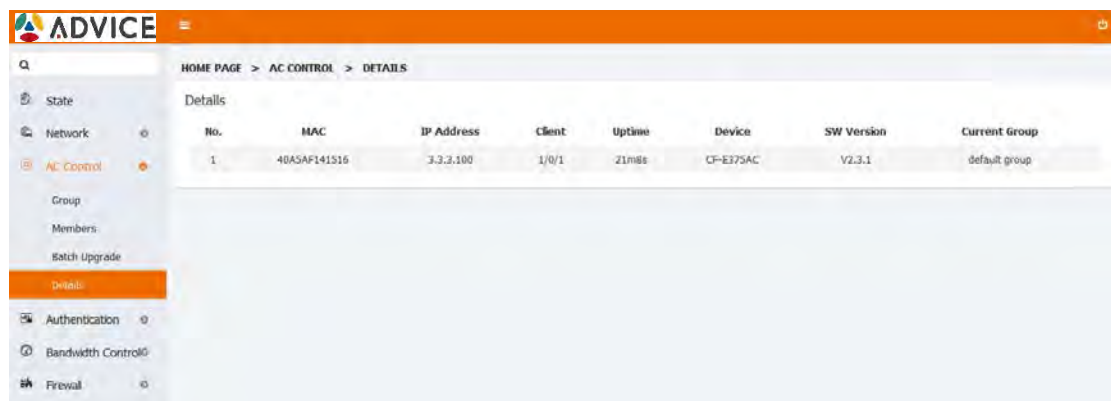
3. Choose the AP devices which you can to upgrade, click the "Batch Upgrade" button on the right, then the devices are on upgrading.



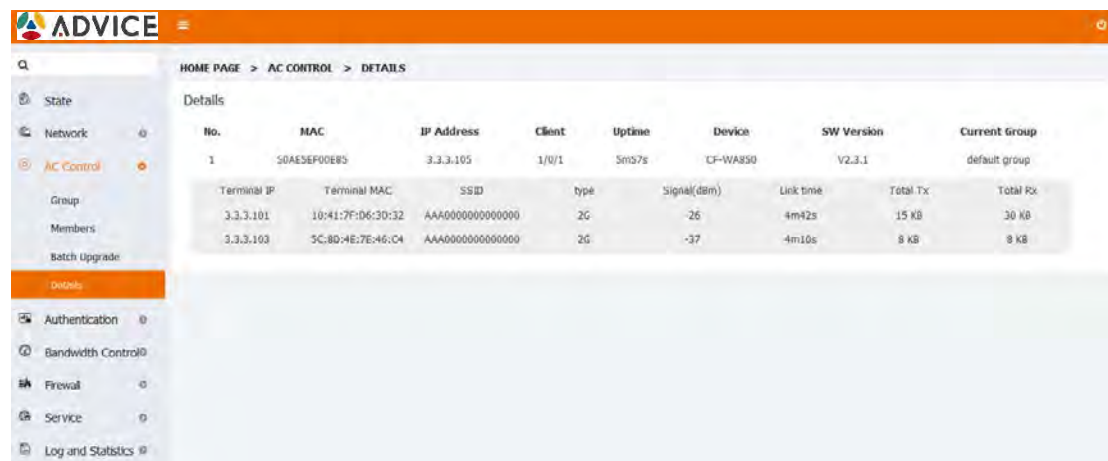
4.3 Details

This function displays all terminal entries under AC, including APs and wireless terminals connected to APs.

1. Login, enter the menu, AC Control-> Details.



2. Click on the AP entry, the details of the wireless terminal connected to the AP is displayed below



HOME PAGE > AC CONTROL > DETAILS

Details

No.	MAC	IP Address	Client	Uptime	Device	SW Version	Current Group
1	50AE5EF00E85	3.3.3.105	1/0/1	5m57s	CF-WA850	V2.3.1	default group

Terminal IP	Terminal MAC	SSID	type	Signal(dbm)	Link time	Total Tx	Total Rx
3.3.3.101	10:41:7F:D6:30:32	AAA0000000000000	2G	-26	4m42s	15 KB	30 KB
3.3.3.103	5C:80:4E:7E:46:C4	AAA0000000000000	2G	-37	4m10s	8 KB	8 KB

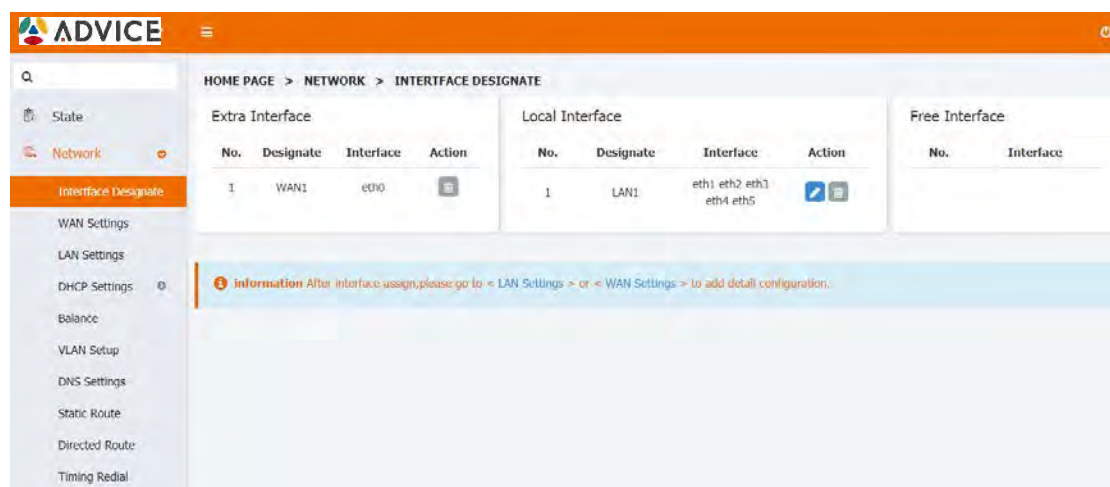
5 Authentication

5.1 Local Auth

5.1.1 OneKey Authentication

Onekey authentication to authenticate online by clicking on the authentication button on the page

1.Login OrangeOS and go into the home page,"Network "-->"Interface Designate".



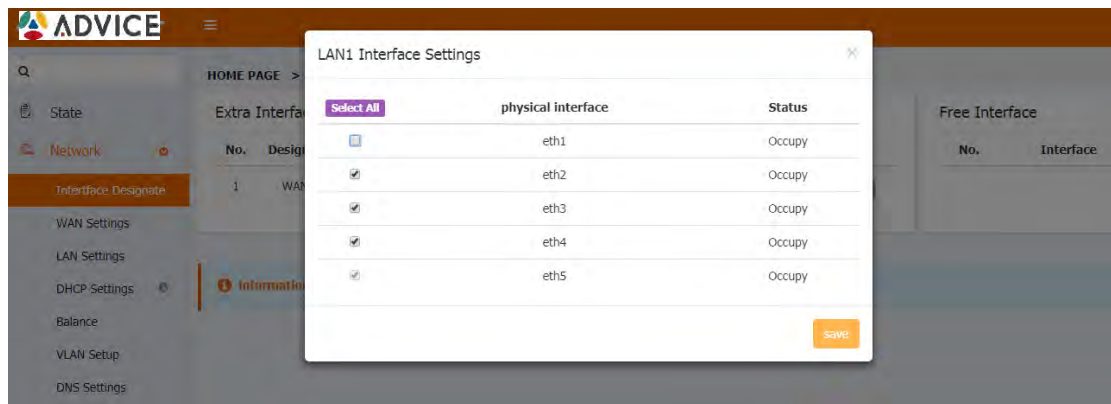
HOME PAGE > NETWORK > INTERFACE DESIGNATE

Extra Interface				Local Interface				Free Interface	
No.	Designate	Interface	Action	No.	Designate	Interface	Action	No.	Interface
1	WAN1	eth0		1	LAN1	eth1 eth2 eth3 eth4 eth5	 		

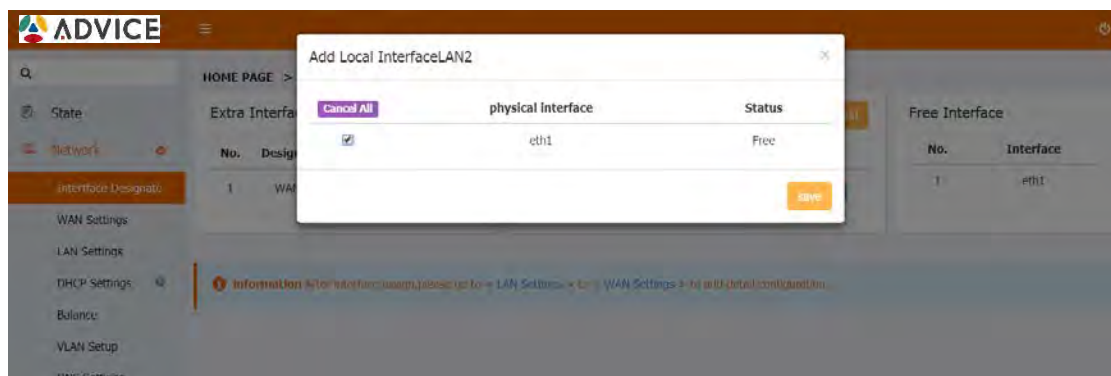
Information After interface assign, please go to < LAN Settings > or < WAN Settings > to add detail configuration.

2.In the Local Interface,click above picture's "blue" Edit button which under the local interface,click edit cancel the eth1 select in the LAN1 port setting page,then the eth1 prot will

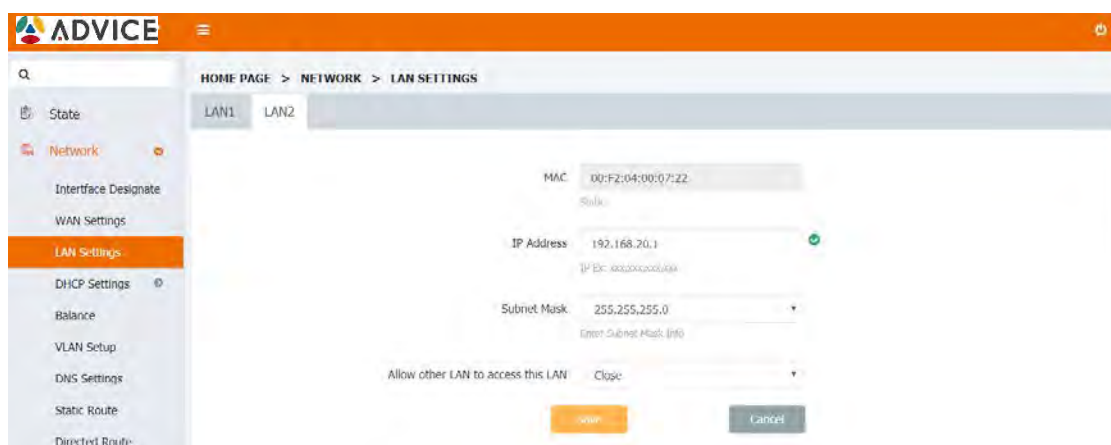
be freed, later click "save".



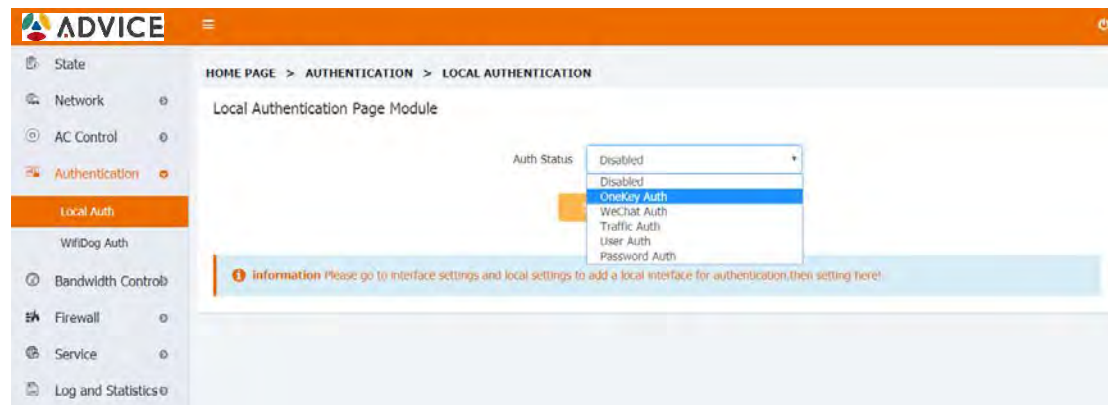
3. Add a Local Interface, Click add in the local interface, and select the port you need to allocate then click save.



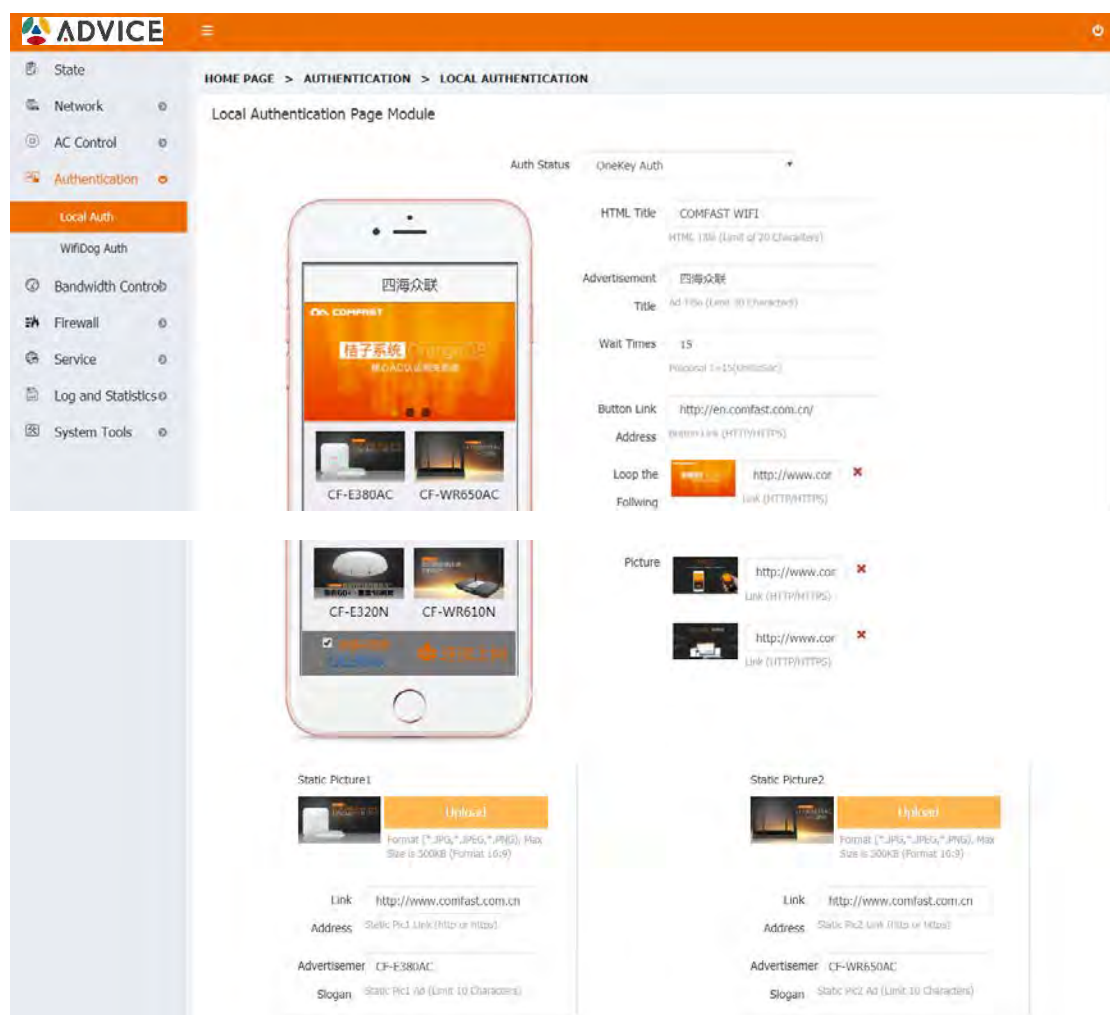
4. Go into Network--Local Network to setup LAN2's local address.



5. Click "Authentication Settings - Local Authentication" and select "Onekey Auth" for the authentication status.



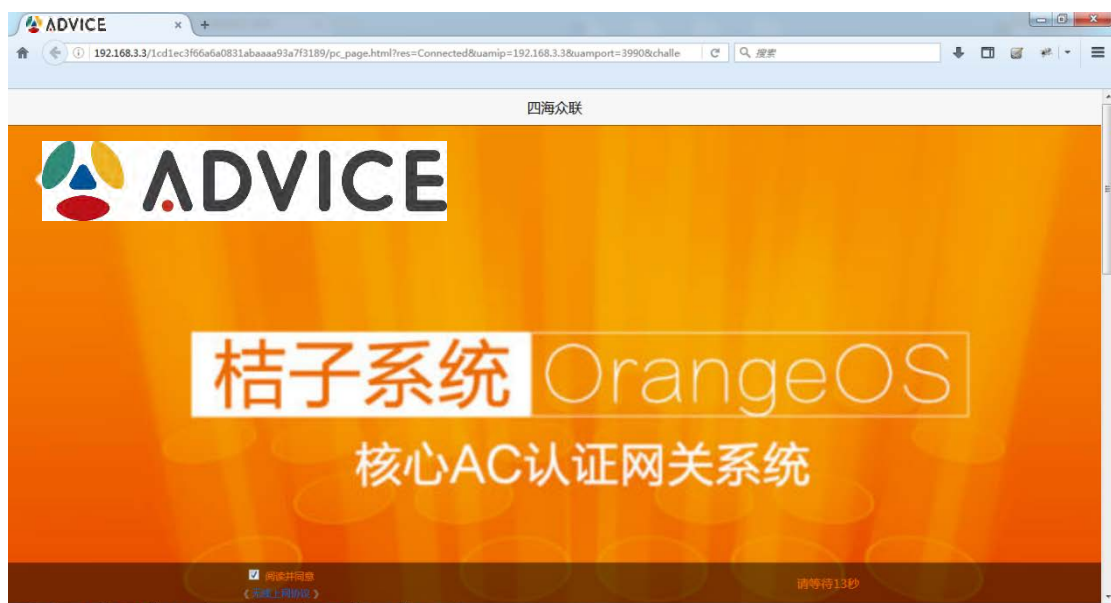
6. Back to the Local Authentication page module and choose the Authentication type as local portal, click Upload to choose the ad image and fill in the link address (the link address need to fill in the full network address, such as <http://www.comfast.com.cn>), click save button, as below:



7. Bind the local interface below the interface and select the newly created LAN2.



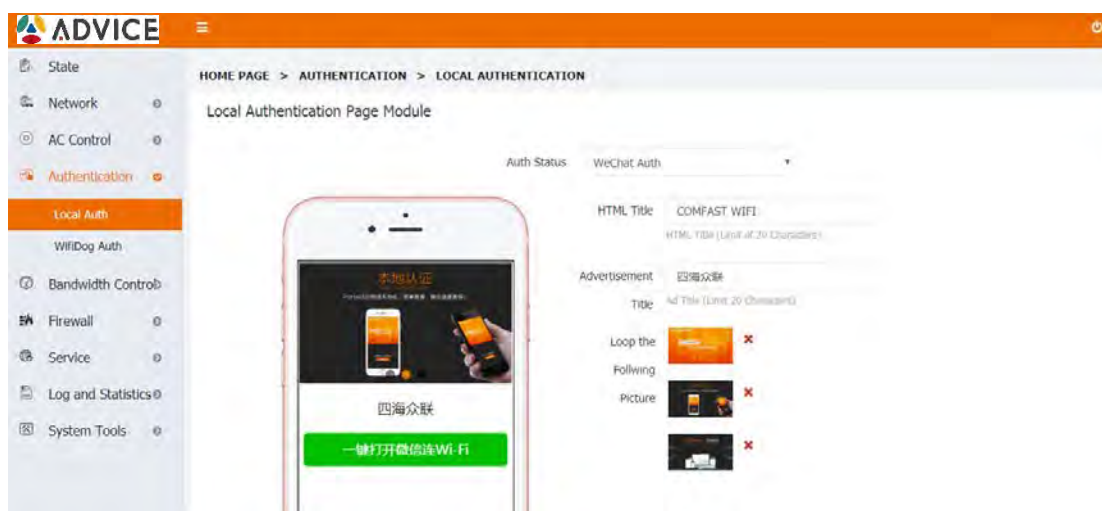
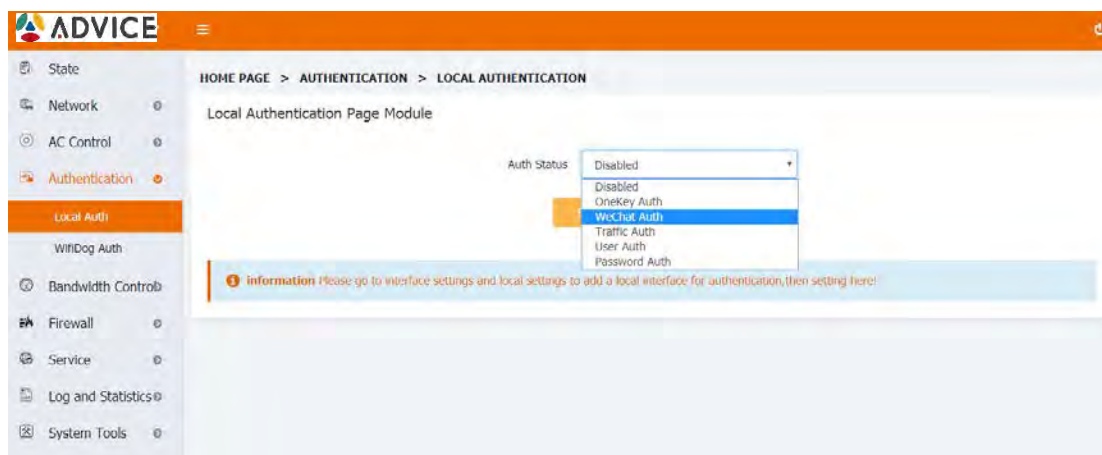
8. Finished setup,use laptop connect AC's LAN2,setup obtain an IP address Automatically,once connected pls open the browser and click the local portal page which popping from any website,wait for 10 seconds,and click below's "connect to surf the Internet"(All devices which connect through LAN2(such this example's configuration is the physical port eth1)all need to authenticate then can surf the Internet).



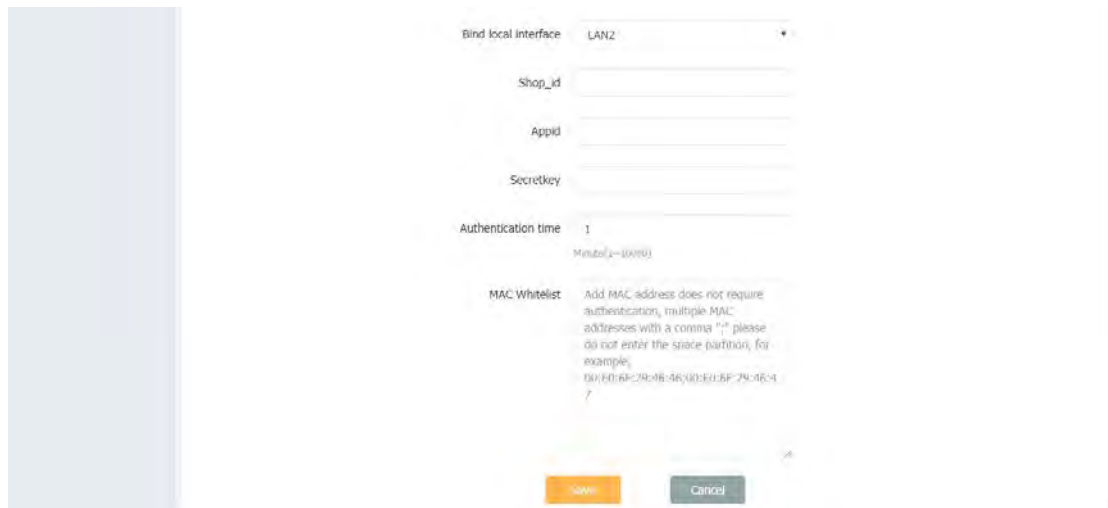
5.1.2 WeChat Authentication

Wechat Authentication is authenticating through Wechat function.

1. Please refer to 5.1.1 1-4 steps to complete the follow-up operation, choose Wechat Authentication and go to wechat authentication page, setup HTML title, ad title and static pic, then click save button.



2. Setup relative parameters, choose LAN2(It has already been set at local portal), then click save button,as below:



Bind local interface: LAN2

Shop_id:

Appid:

Secretkey:

Authentication time: 1

MAC Whitelist: Add MAC address does not require authentication, multiple MAC addresses with a comma "," please do not enter the space partition, for example: 00:ED:68:29:06:5E;00:ED:6F:29:06:04

Buttons: Save, Cancel

3. Once the setting is complete, use router's WAN port to connect with LAN2 of AC, setup obtain an IP address automatically, connect the router's wifi by cellphone, after connection, open the browser and click any website then it will popping the Wechat Authentication page,as below:



4. Click “A key to open the Wechat connect with Wi-Fi” on above picture, then it will go into Wechat connecting Wi-Fi page, as below:



5. Click above picture's “ connect immediately” button, then it will show connecting Wi-Fi successfully and Wechat Authentication is finished, and the cellphone can surf the Internet normally. All devices which connect through LAN2 (such as the example's configuration is the physical port eth1) need to authenticate then can surf the Internet.



5.1.3 Traffic Authentication

Traffic Authentication: Restrict user re-authentication by restricting traffic

1. Please refer to 5.1.1 1-4 steps to complete the follow-up operation, choose Traffic Authentication and go to traffic authentication page, setup HTML title, ad title and static pic, then click save button.

ADVICE HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION

Local Authentication Page Module

Auth Status: Traffic Auth

HTML Title: COMFAST WIFI
HTML Title (Limit 32 Characters)

Advertisement: COMFAST
Ad Title (Limit 32 Characters)

Title:
HTML Title (Limit 32 Characters)

Wait Times: 15
Wait Times (Limit 32 Characters)

Button Link: <http://en.comfast.com.cn/>
Button Link (HTTP/HTTPS)

Address:
Button Link (HTTP/HTTPS)

Loop the Following Picture:
Link (HTTP/HTTPS)

Static Picture1:
Format (*.JPG, *.JPEG, *.PNG), Max Size is 500KB (Format 10/0)

Link: <http://www.comfast.com.cn>
Static Pic Link (http or https)

Address:
Static Pic Link (http or https)

Advertisement: CF-E380AC
Static Pic1 Ad (Limit 10 Characters)

Slogan:
Static Pic1 Ad (Limit 10 Characters)

Static Picture2:
Format (*.JPG, *.JPEG, *.PNG), Max Size is 500KB (Format 10/0)

Link: <http://www.comfast.com.cn>
Static Pic2 Link (http or https)

Address:
Static Pic2 Link (http or https)

Advertisement: CF-WR650AC
Static Pic2 Ad (Limit 10 Characters)

Slogan:
Static Pic2 Ad (Limit 10 Characters)

Static Picture3:
Format (*.JPG, *.JPEG, *.PNG), Max Size is 500KB (Format 10/0)

Link:
Static Pic3 Link (http or https)

Address:
Static Pic3 Link (http or https)

Advertisement:
Static Pic3 Ad (Limit 10 Characters)

Slogan:
Static Pic3 Ad (Limit 10 Characters)

Static Picture4:
Format (*.JPG, *.JPEG, *.PNG), Max Size is 500KB (Format 10/0)

Link:
Static Pic4 Link (http or https)

Address:
Static Pic4 Link (http or https)

Advertisement:
Static Pic4 Ad (Limit 10 Characters)

Slogan:
Static Pic4 Ad (Limit 10 Characters)

2. Setup relative parameters, choose LAN2(It has already been set at local portal), fill in the restricted traffic (eg: 1024), then click save button,as below:

Bind local interface: LAN2

Limitation of delivery: 1024
Unit:KB

Authentication time: 2
Minute(1~10000)

MAC Whitelist:
Add MAC address does not require authentication, multiple MAC addresses with a comma "," please do not enter the space portion, for example, 00:E0:6F:29:46:45:09:E0:6F:29:46:47

[Save](#) [Cancel](#)

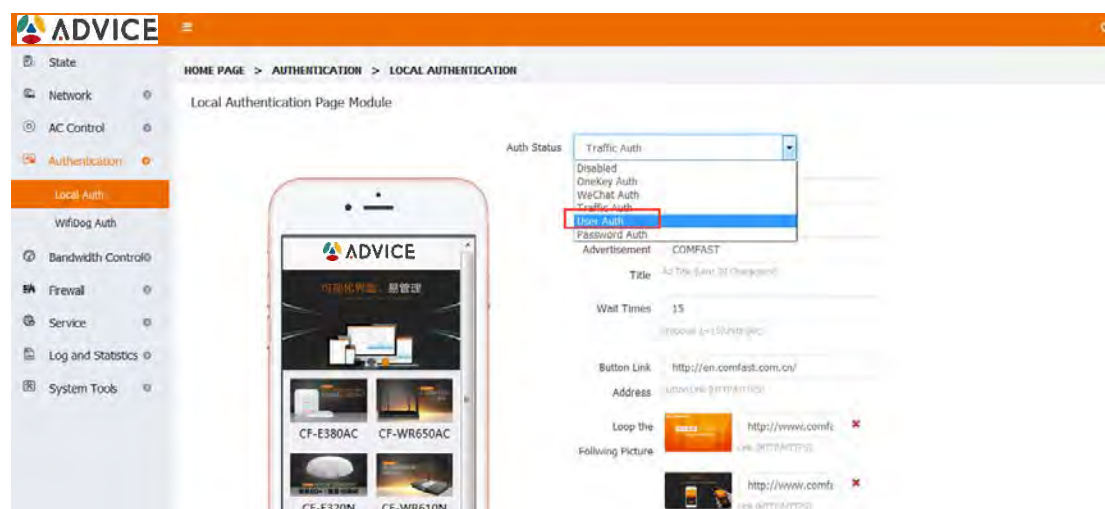
Information Please go to interface settings and local settings to add a local interface for authentication, then setting here!

3. Once the setting is complete, use router's WAN port to connect with LAN2 of AC, setup obtain an IP address automatically, connect the router's wifi by cellphone, after connection, open the browser and click any website then it will popping the traffic authentication page, after the authentication can be normally accessed. When the user uses more than 1024M of traffic, it will re-jump to the authentication page to re-authenticate

5.1.4 User Authentication

User authentication: authenticated by account and password

1. Please refer to 5.1.1 1-4 steps to complete the follow-up operation, choose User Authentication and go to user authentication page, setup HTML title, ad title and static pic, then click save button.



2. Bind local interface Select LAN2 port (It has already been set at local portal), set the authentication duration, and then click the save button, as below;

Bind local interface

LAN2

Authentication time

2

Minute(1~10080)

MAC Whitelist

Add MAC address does not require authentication, multiple MAC addresses with a comma ","; please do not enter the space partition, for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47

Save

Cancel

Information Please go to interface settings and local settings to add a local interface for authentication, then setting here!

3. Add authentication user information at the bottom of the page, click the "+Add" button, enter the account number and password in the pop-up input box (eg: KEN/123), click "Save"

Add authentication info

Username

KEN

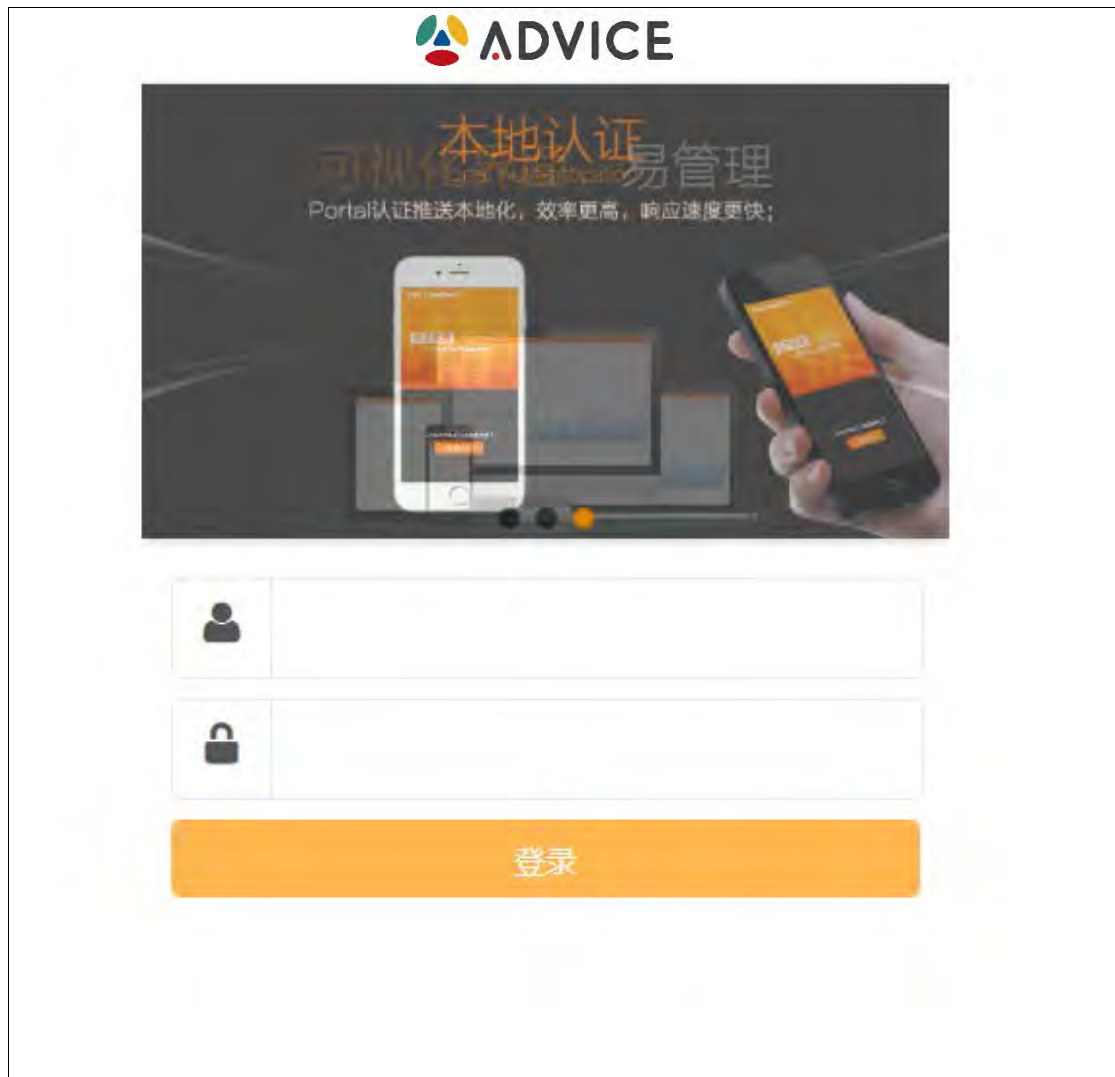
Password

123

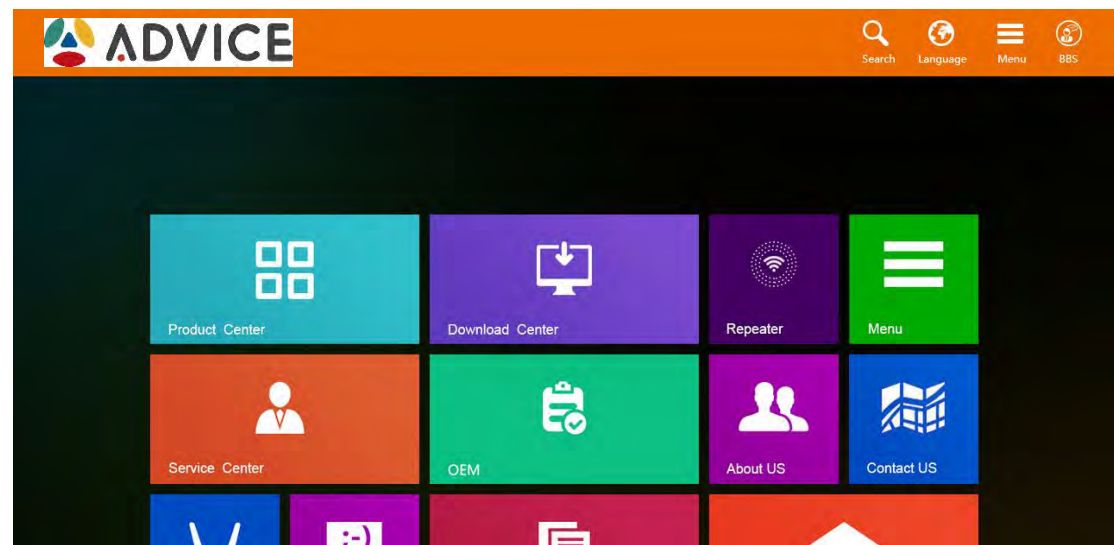
Save

Messages List					Number per Page (10)	Add	Delete Selected	Import	Export
Select All	No.	Username	Password	Edit					
☐	1	KEN	123	 					
					< 1 >				

4. Once the setting is complete, use router's WAN port to connect with LAN2 of AC, setup obtain an IP address automatically, connect the router's wifi by cellphone, after connection, open the browser and click any website then it will popping the Wechat Authentication page, as below:



5. Enter the correct authentication password (such as: KEN/123), click on the login, automatically jump to the page after successful login, this time the certification is completed, you can normally access the Internet

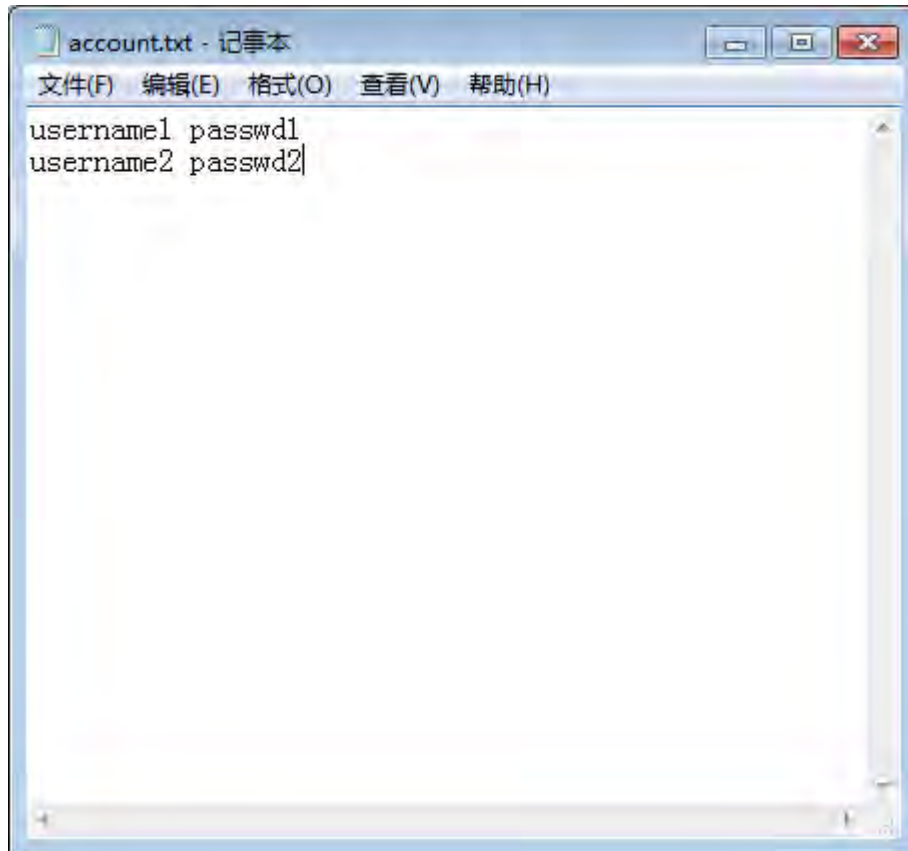


6. You can import account information in batches by importing files. The file content format is:

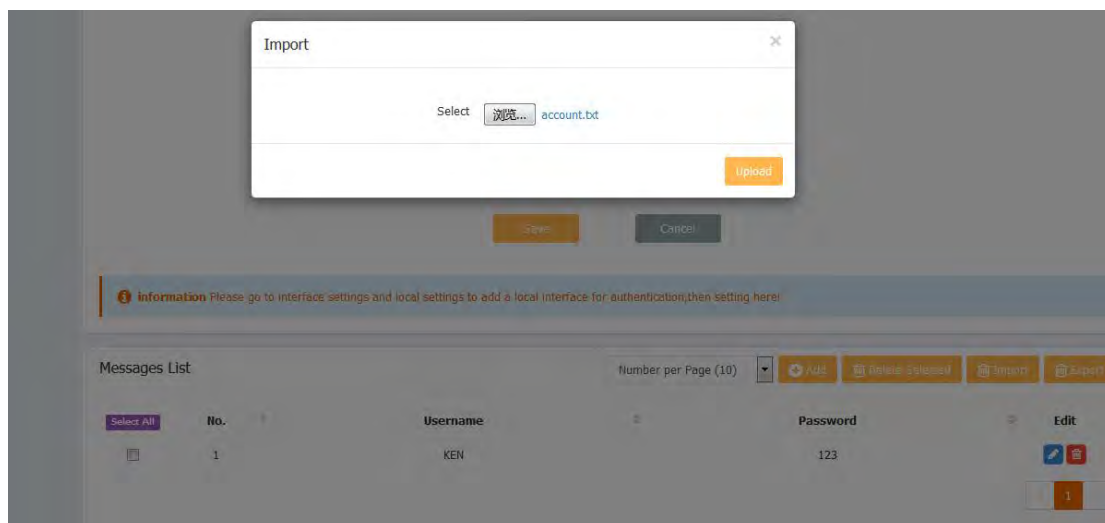
username1 passwd1

username2 passwd2

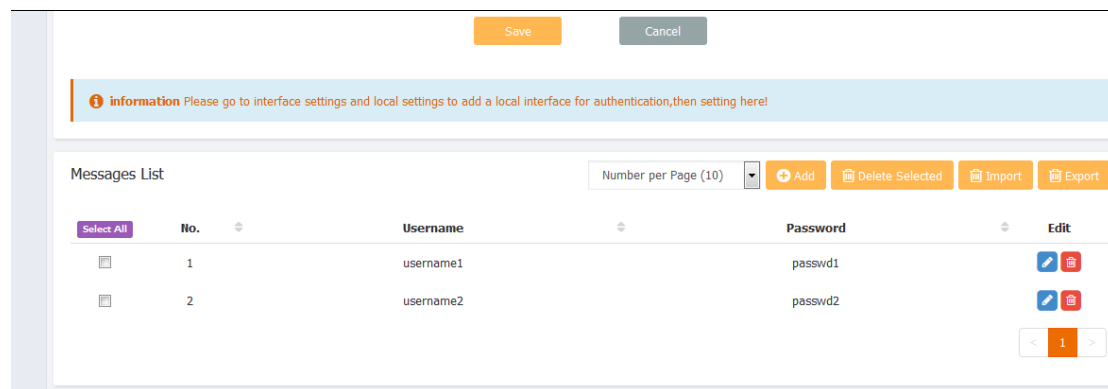
The file is encoded as ANSI or UTF-8 and does not support the unicode format. Save as txt suffix file. As shown below:



Click the Import File button and select the file account.txt.



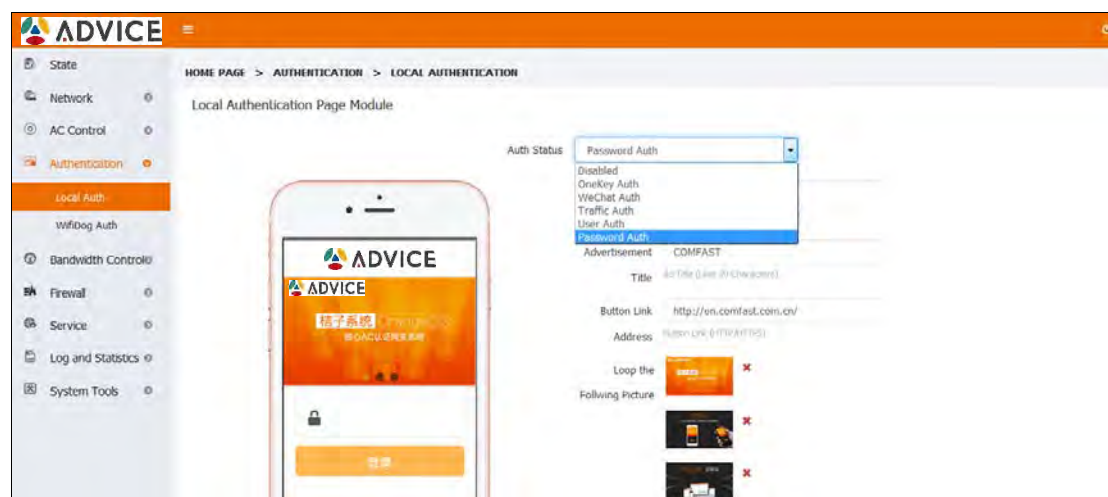
You can see that the user name and password were imported successfully, and the previously added account configuration will be overwritten, so before you import, you can export the previous useful account in advance.



Click Export File to export the current account information to the account.txt file.

5.1.4 Password Authentication

1. Please refer to 5.1.1 1-4 steps to complete the follow-up operation, choose Password Authentication and go to password authentication page, setup HTML title, ad title and static pic, then click save button.



2. Bind local interface Select LAN2 port (It has already been set at local portal), set the authentication duration, and then click the save button, as below;

Bind local interface

LAN2

Authentication time

2

Minute(1~10080)

MAC Whitelist

Add MAC address does not require authentication, multiple MAC addresses with a comma "," please do not enter the space partition, for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47

Save

Cancel

Information Please go to interface settings and local settings to add a local interface for authentication, then setting here!

3. Add the authentication password at the bottom of the page, click the "+Add" button, enter the authentication password in the pop-up input box (eg: 123), click "Save"

Add authentication info

Password

123

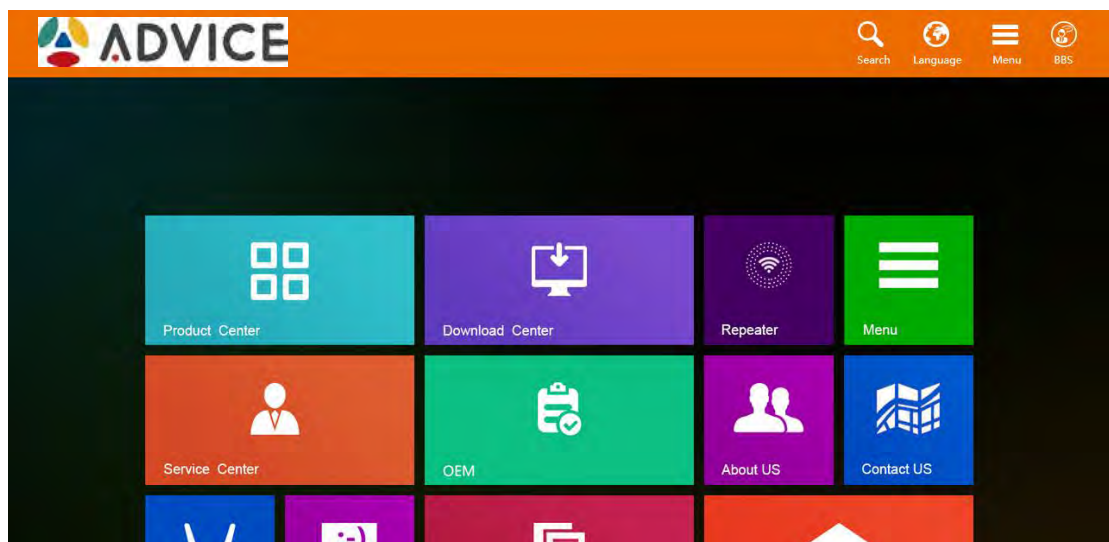
Save

Messages List			
		Number per Page (10)	+ Add Delete Selected Import Export
Select All	No.	Password	Edit
☐	1	123	
		< 1 >	

4. Once the setting is complete, use router's WAN port to connect with LAN2 of AC, setup obtain an IP address automatically, connect the router's wifi by cellphone, after connection, open the browser and click any website then it will popping the Password Authentication page, as below:



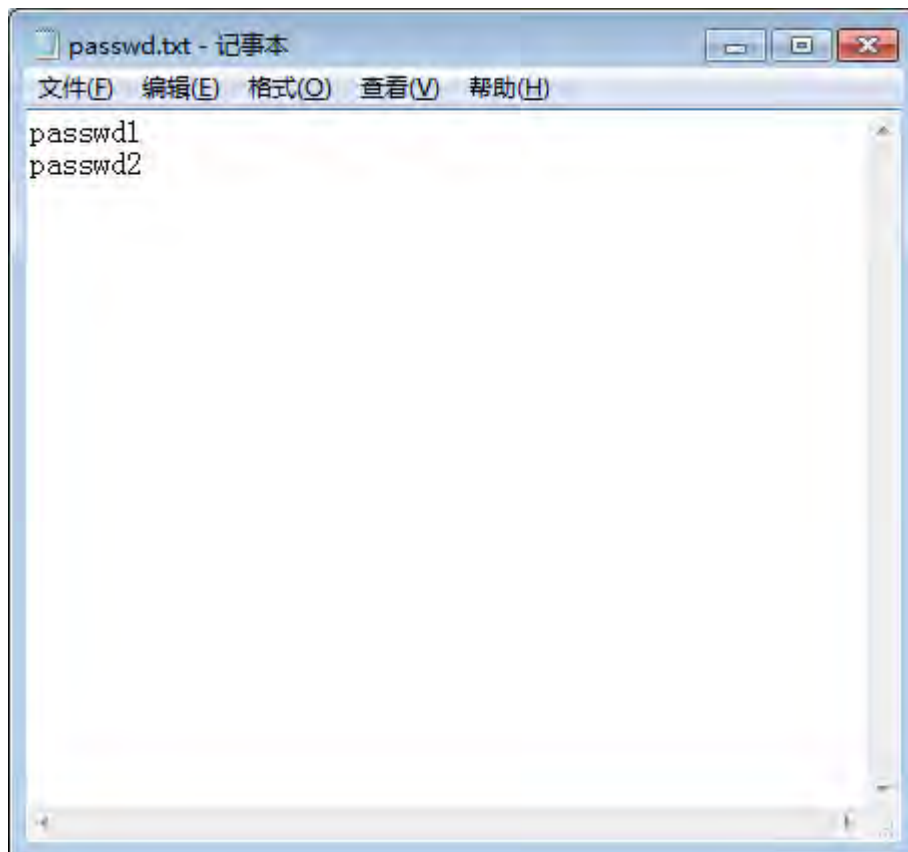
5. Enter the correct authentication password (such as: 123), click on the login, automatically jump to the page after successful login, this time the certification is completed, you can normally access the Internet



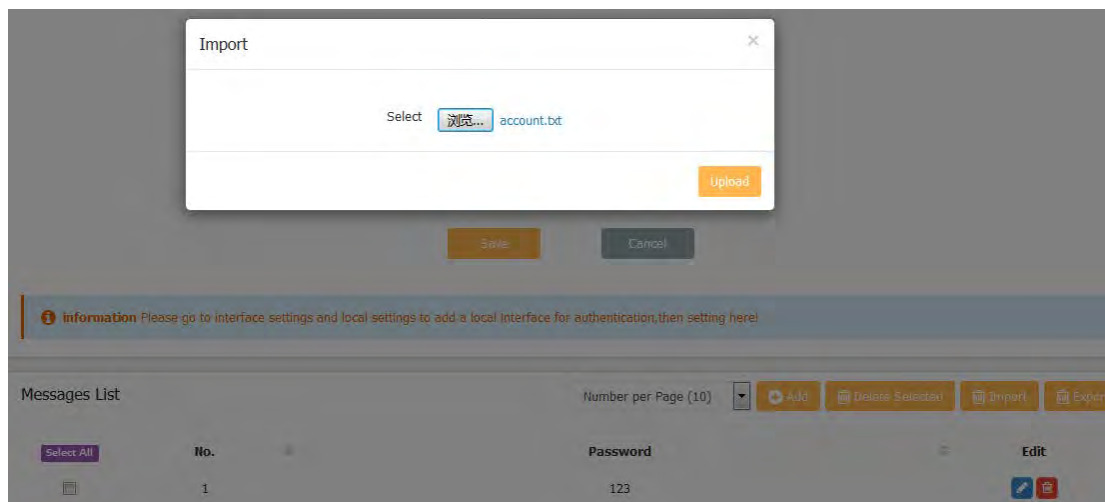
7. You can import account information in batches by importing files. The file content format is: passwd1

passwd2

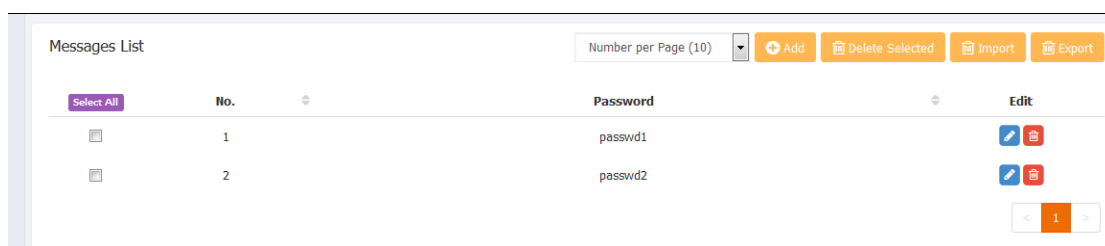
The file is encoded as ANSI or UTF-8 and does not support the unicode format. Save as txt suffix file. As shown below:



Click the Import File button and select the file passwd.txt.



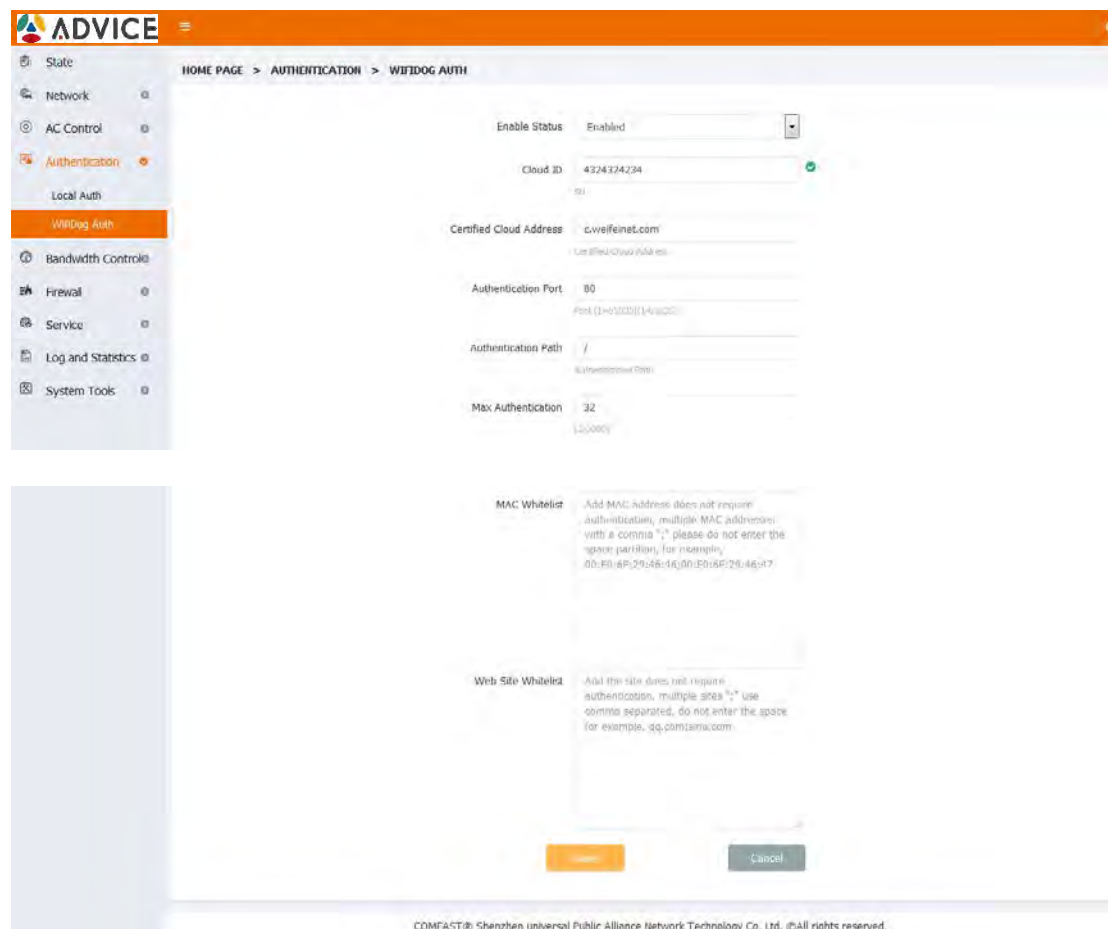
You can see that the user name and password were imported successfully, and the previously added account configuration will be overwritten, so before you import, you can export the previous useful account in advance.



Click Export File to export the current account information to the passwd.txt file.

5.2 Wifidog Auth

1.Go into WEB home page,"Authentication"---"wifidog auth",then choose the Enable status as Enable,setup relative parameters,click save button,as below:



2. Open the browser in the local computer, open the other website which haven't in the website white list, then it will popping the authentication page, as below:



3. Use device's PC which use MAC white list (two MAC all is the laptop's MAC) to open the browser, and here will not popping the authentication page in any websites, as below:

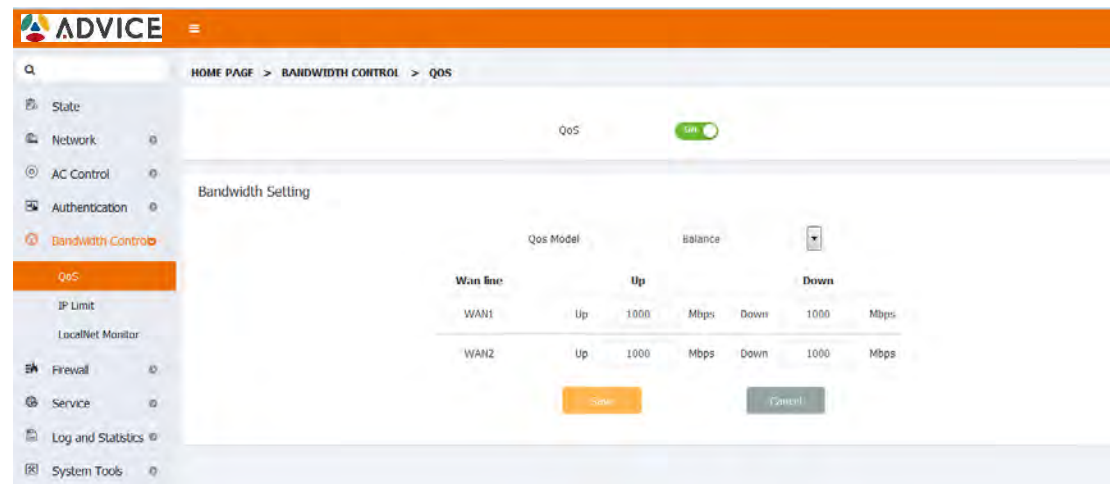


6 Traffic Control

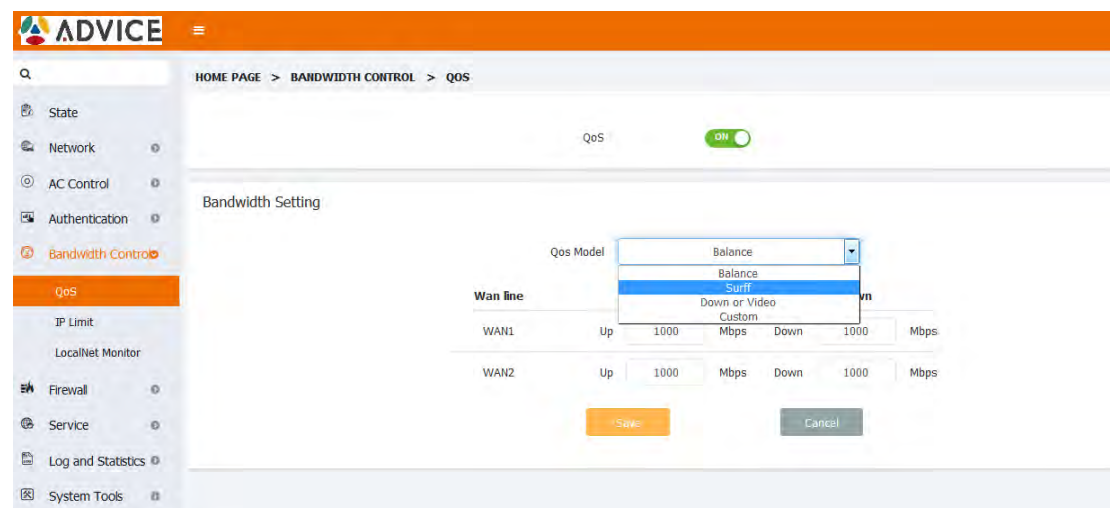
6.1 Qos

When here are many ISP lines connect to the device,open the traffic switch,setup every ISP line's upstream and downstream bandwidth by the real network situation.

1. Go to Oos page,setup the relative parameters, fill in the actual downlink bandwidth according to the bandwidth of each external network, and click save button,as below:



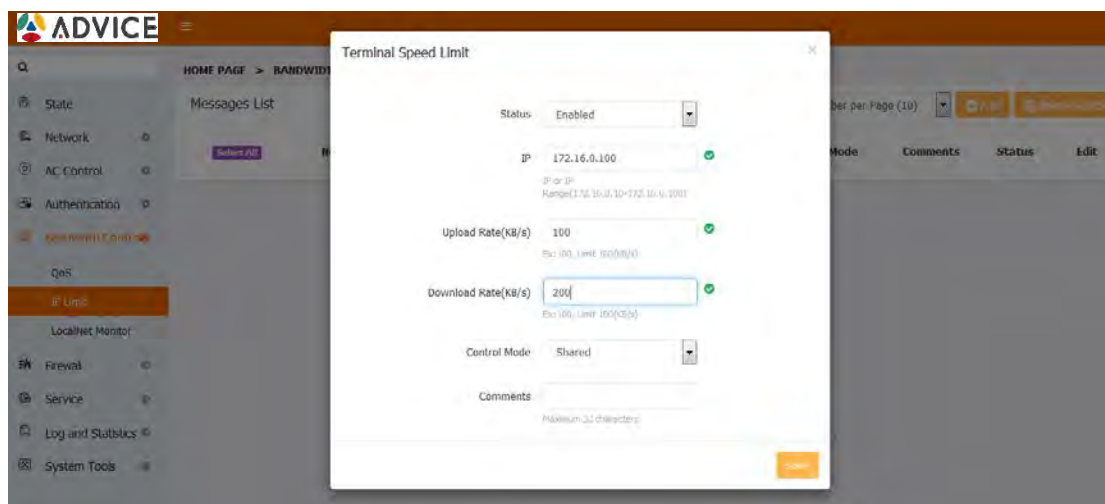
2. The line flow control mode can be adjusted according to the actual use of the user



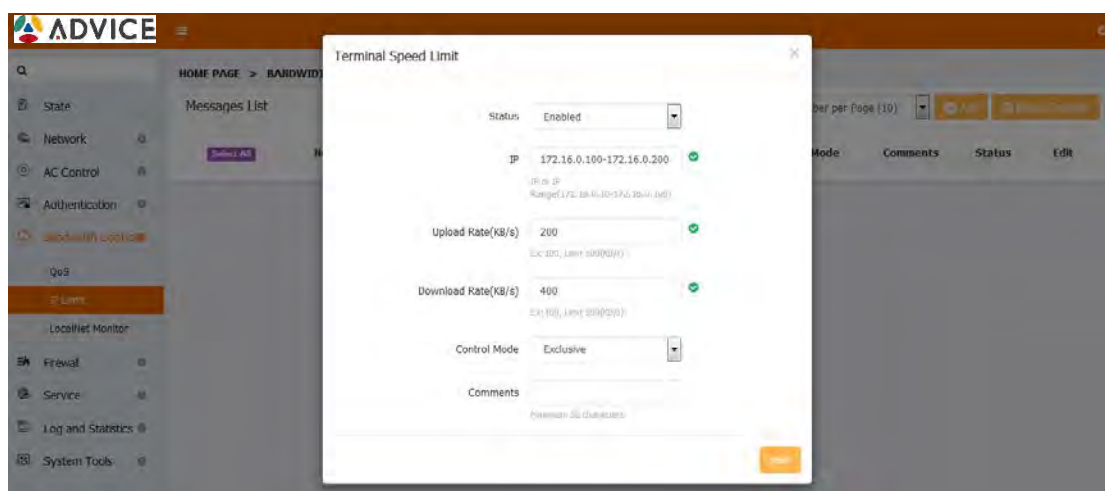
6.2 IP Limit

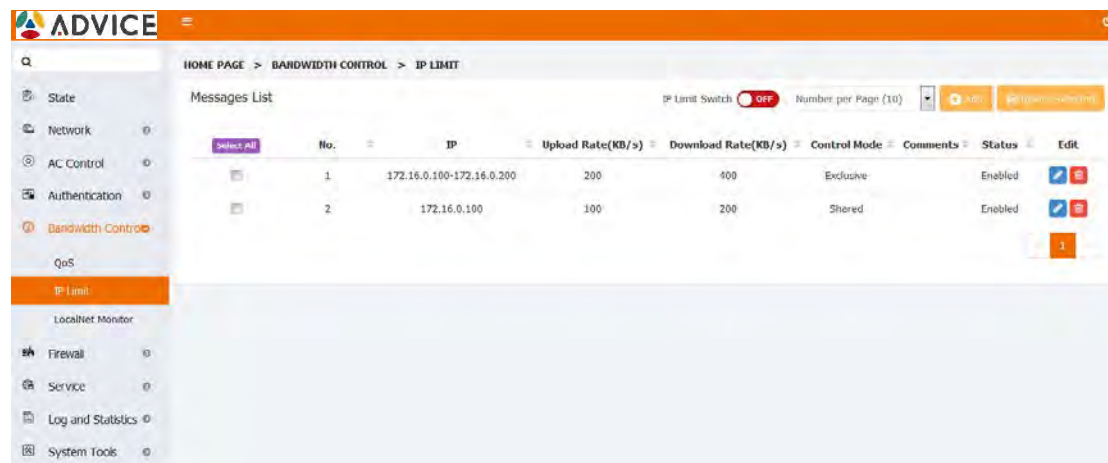
According to the IP address can control the uplink and downlink traffic of signal user.

1. Go into the IP LIMIT page, add a single IP speed limit information, IP: 172.16.0.100, up and down are 10 and 10, then the user's uplink and downlink speed and speed limit values should be same.



2. Go to the IP Limit page and add the IP limit information, ip: 172.16.0.100-172.16.0.200, with 200 and 400 upstream and downstream respectively. The exclusive bandwidth is the independent speed limit setting for all users in the network segment. The bandwidth and the shared bandwidth are the bandwidths shared by all users in the network segment. In this case, the user's uplink and downlink rates are consistent with the speed limit values.



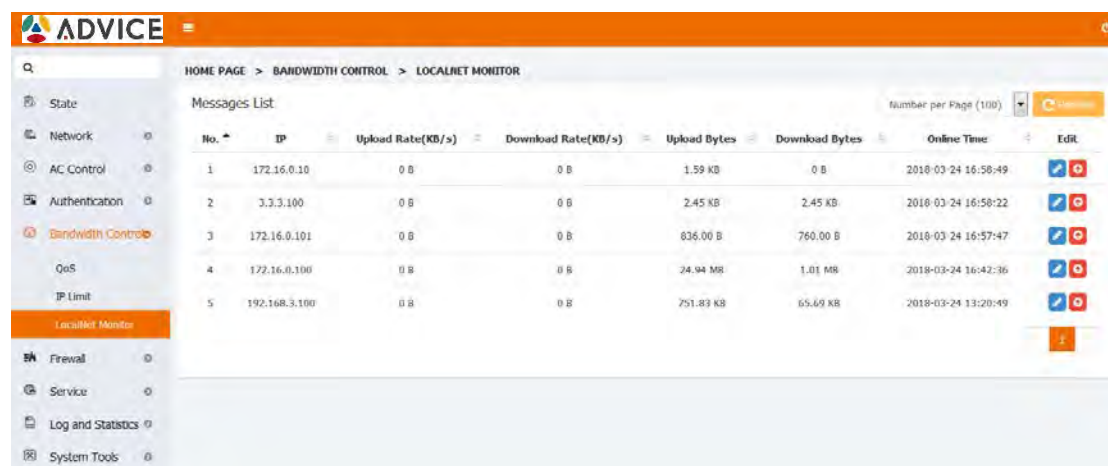


No.	IP	Upload Rate(KB/s)	Download Rate(KB/s)	Control Mode	Comments	Status	Edit
1	172.16.0.100-172.16.0.200	200	400	Exclusive		Enabled	 
2	172.16.0.100	100	200	Shared		Enabled	 

6.3 Localnet Monitor

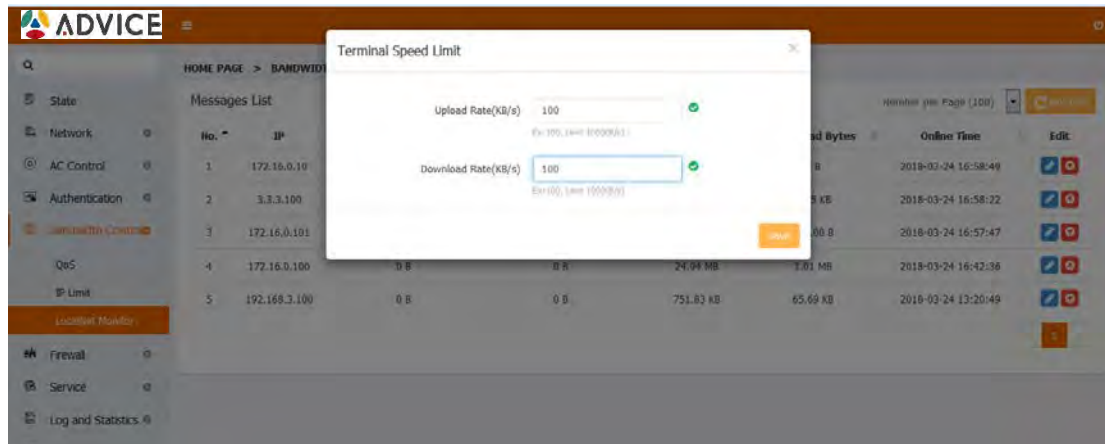
Real-time monitoring of each user's uplink and downlink rates and uplink and downlink total traffic, and will automatically update real-time, you can manually add each user to a single IP speed limit list to control a single user speed.

1.Go into localnet monitor page, each user corresponding to the uplink and downlink rate and the total flow is of the same line with the actual value

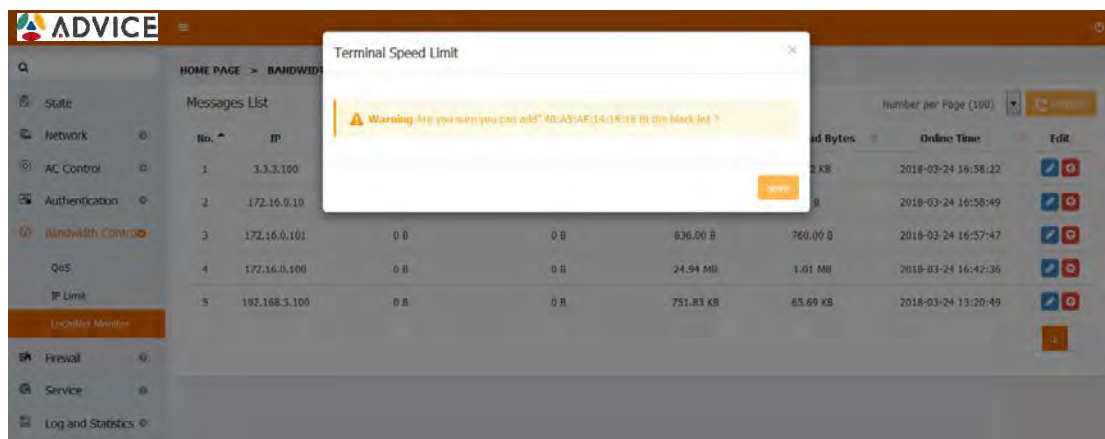


No.	IP	Upload Rate(KB/s)	Download Rate(KB/s)	Upload Bytes	Download Bytes	Online Time	Edit
1	172.16.0.10	0 B	0 B	1.59 KB	0 B	2018-03-24 16:58:49	 
2	3.3.3.100	0 B	0 B	2.45 KB	2.45 KB	2018-03-24 16:58:22	 
3	172.16.0.101	0 B	0 B	836.00 B	760.00 B	2018-03-24 16:57:47	 
4	172.16.0.100	0 B	0 B	24.94 MB	1.01 MB	2018-03-24 16:42:36	 
5	192.168.3.100	0 B	0 B	751.83 KB	65.69 KB	2018-03-24 13:20:49	 

2. Click on the 'Edit' icon of one user, to realize single IP speed limit of the user



3. An abnormal traffic user can be added to the black list to prevent the user from accessing the Internet.

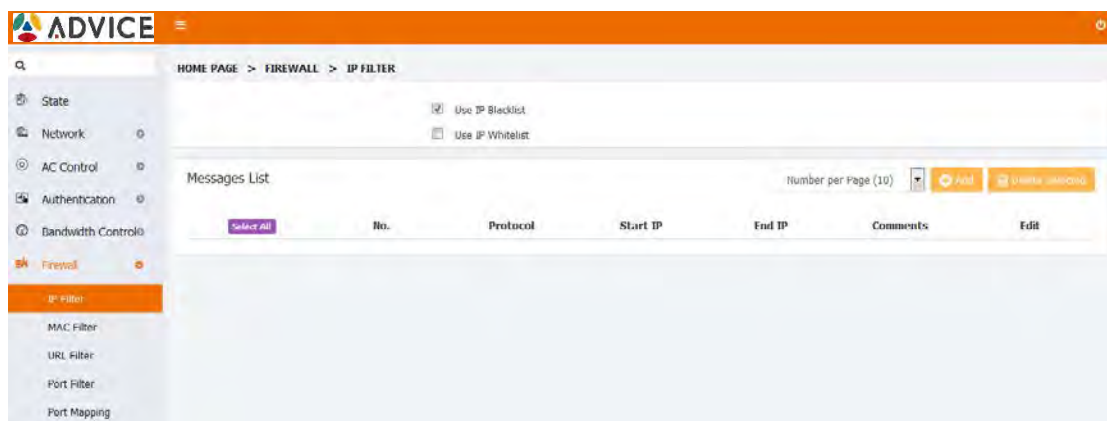


7 Firewall

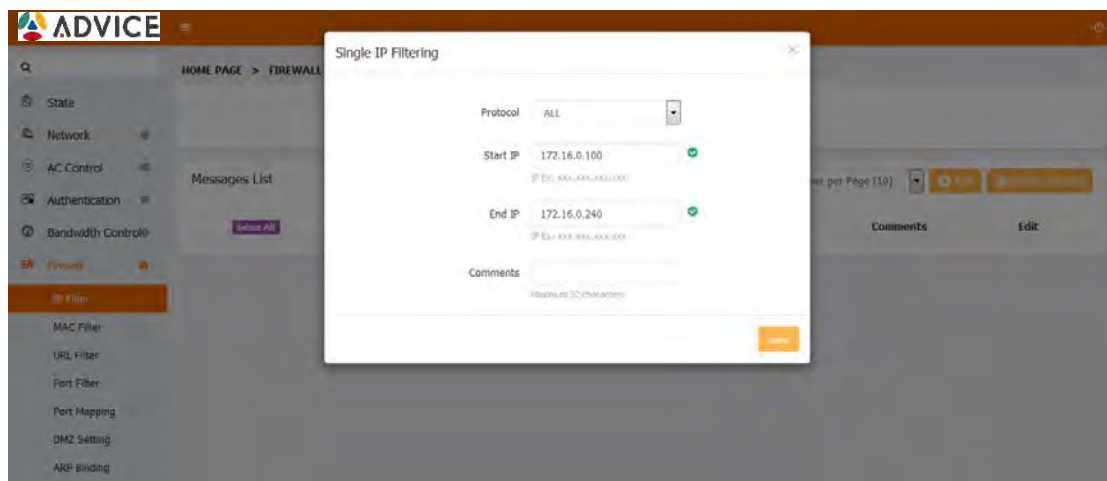
7.1 IP Filter

Here you must know the IP which the computer achieved and the device allocated, and confirm that which computer achieved IP or IP segment need to filter forbid visit network base on the practical situation.

1. Click the home page "Firewall" and go into the IP Filter page, as below:



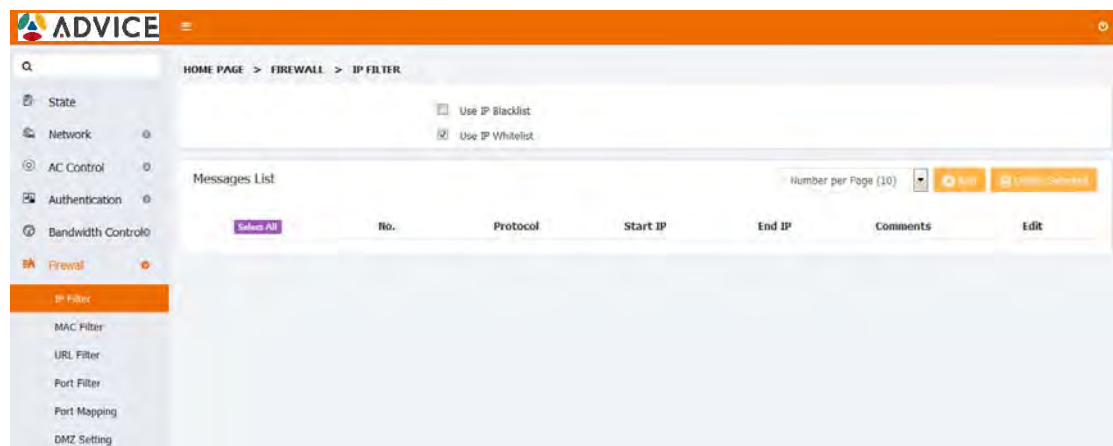
2.Click “Add” and go into IP Filter’s detail setup page,setting the filterable IP segment range which you need,then click “save” as below:



3.Open the native’s browser,and it can not open the website normally,because the native IP:192.168.10.101 is in the filterable segment range,as below:



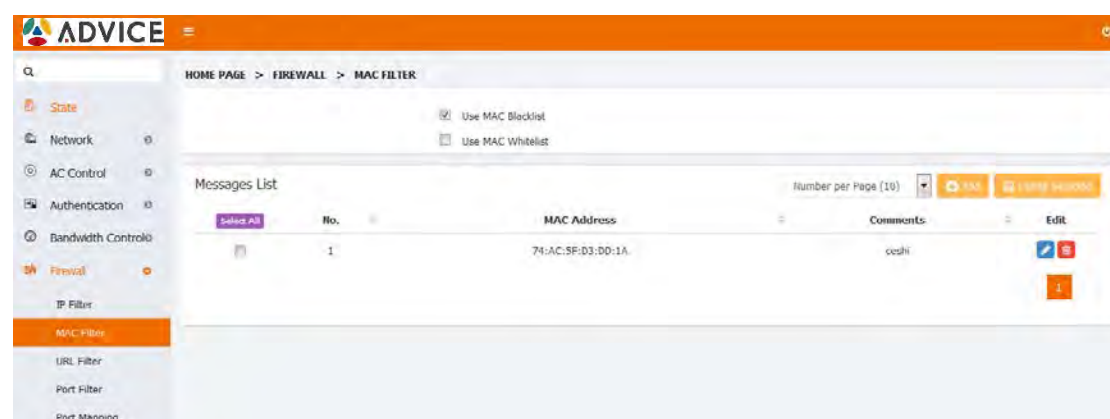
4. Switch to the white list. Only users in the white list can access the Internet. Other users cannot access the Internet.



7.2 MAC Filter

Here you must know the computer native lan card's MAC address, then enter the corresponding computer MAC address forbid visit network in the device MAC Filter.

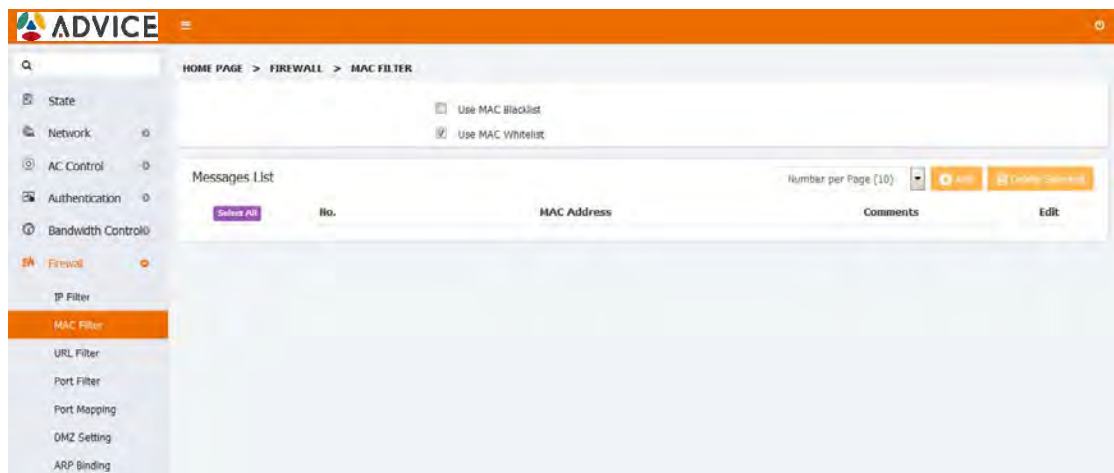
1. Login the router's WEB page, go into the "MAC Filter" page in Firewall, setup PC1 MAC address and save the setting.



2. Open the local browser. The filtered device cannot access the Internet normally.



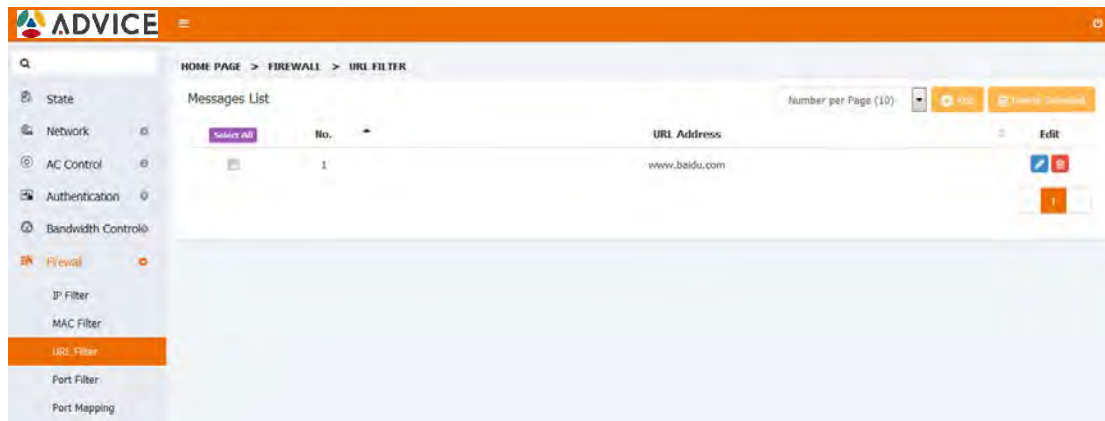
3. Modify the MAC address whitelist mode. Only devices in the whitelist can access the Internet. Other devices cannot access the Internet.



7.3 URL Filtering

Here you can setup the website address to filter which you need, and the setup address can not open.

1. Login the router's WEB page, click function setting and enter "www.baidu.com" in the website filter.



2. Open browser, visit www.baidu.com in the Internet, and this moment, the PC can not success to visit the website, but can visit the others.

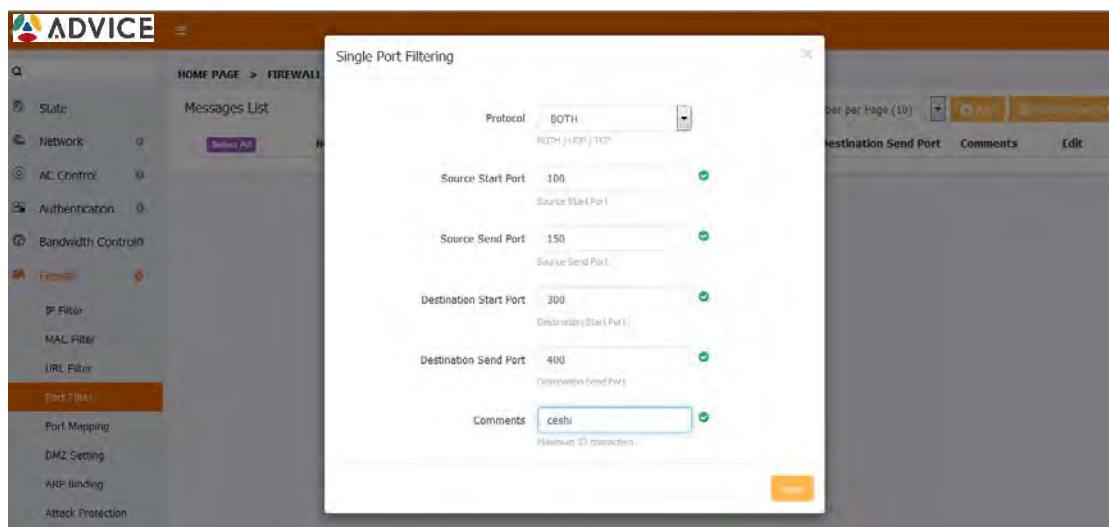
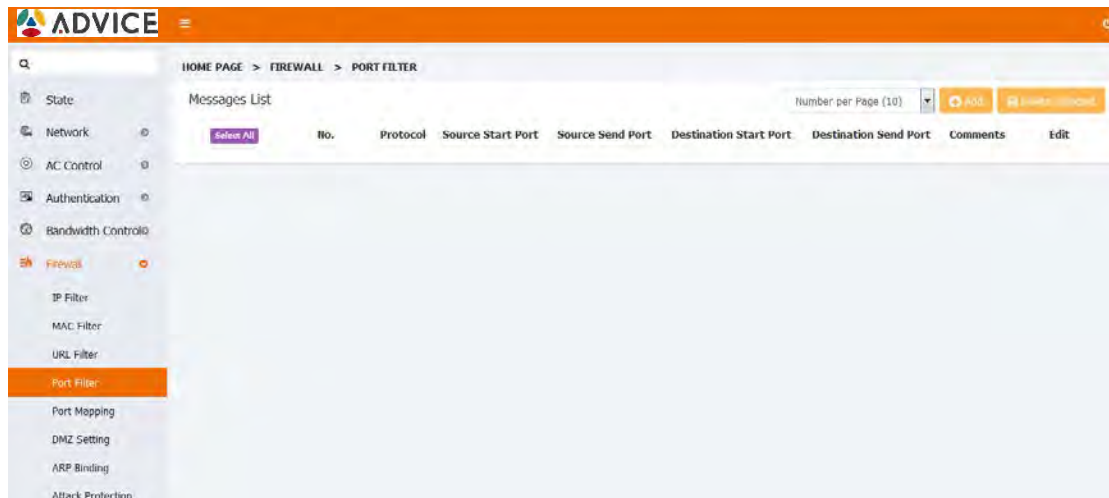


7.4 Port Filter

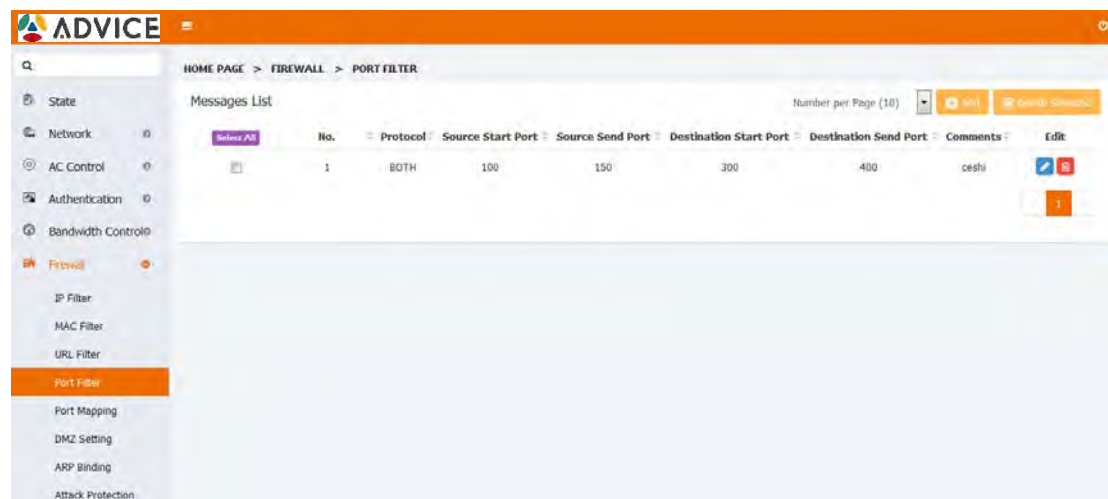
When in actual use, certain ports need to be filtered, the port filtering module allows some

internal services to be used or prohibited by internal users by opening or closing some ports.

1. Home page click on "Firewall-Port Filter" to enter the port filter page, click on the "+ Add" button to pop up the port filter settings box



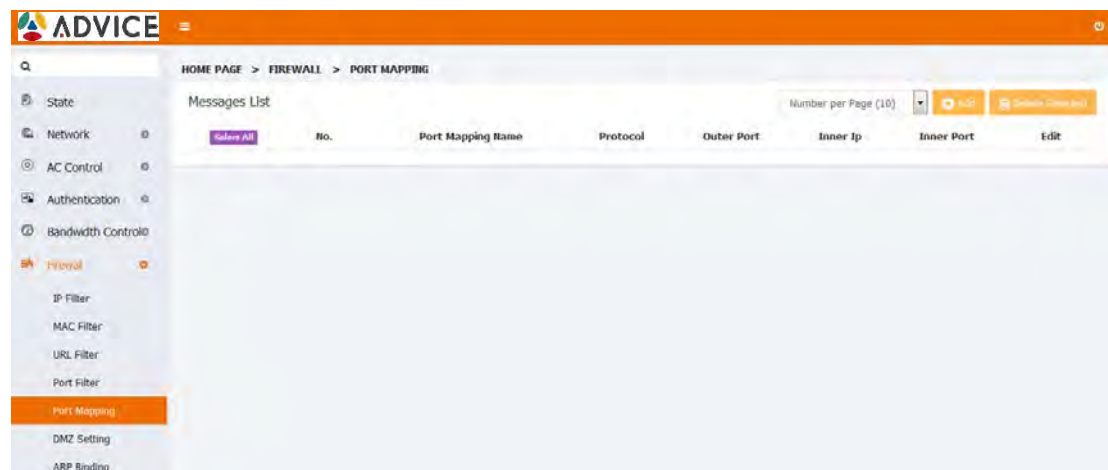
2. Fill in the source port and the destination port (set according to the actual situation). The source port refers to the local port and the destination port is the remote port. Then click Save. After the setting is successful, filter the local port 100-150, remote port 300-400



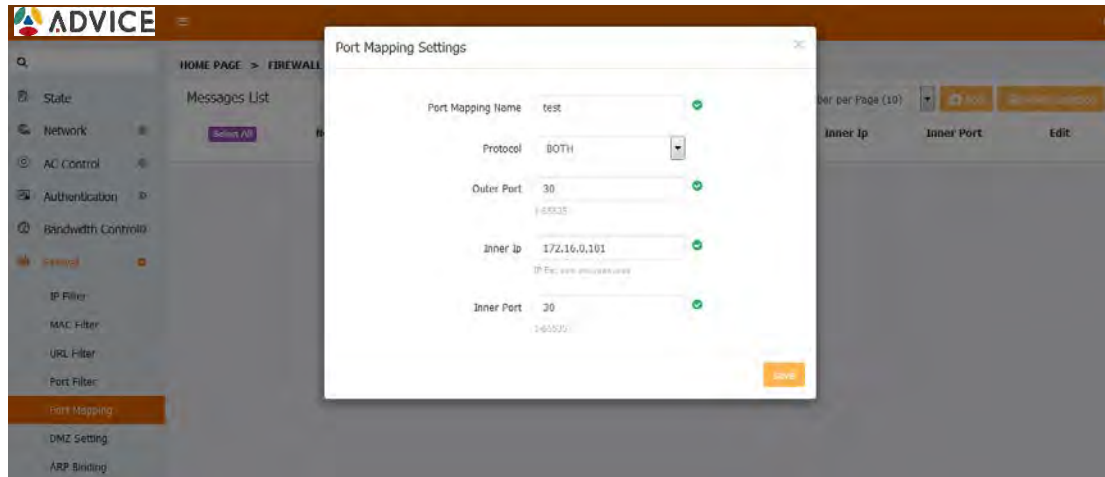
7.5 Port Mapping

Sometime called channel, it is one way for the save shell (SSH) use for the network safety communication. Port Forwarding is the behavior of forward one network port from one network node to the others, it is one port to let the external user reach one private inner IP (internal Internet) through one activated NAT router.

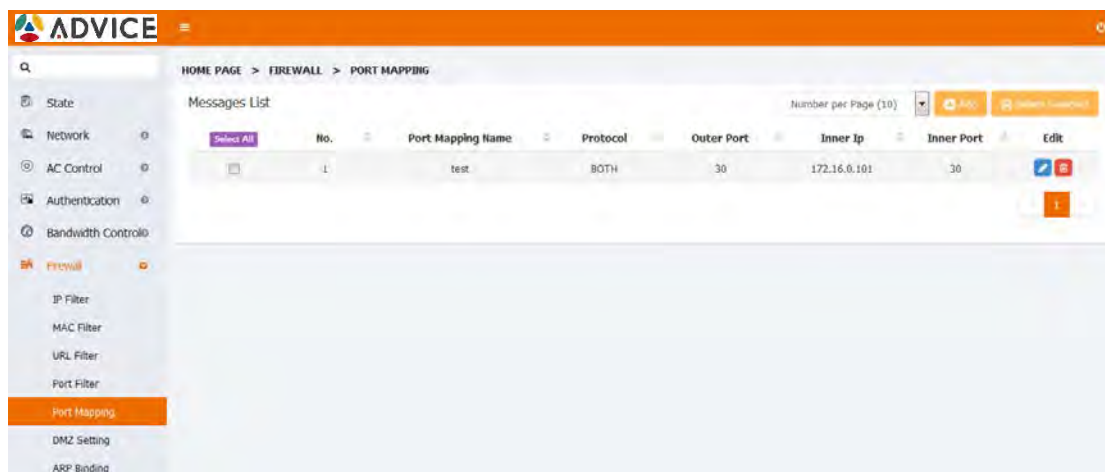
1. Login the router's Web page, finish setup in the firewall page.



2. Click above picture's "+add" button,go into the Single Port Filtering page,setup the relative parameters.



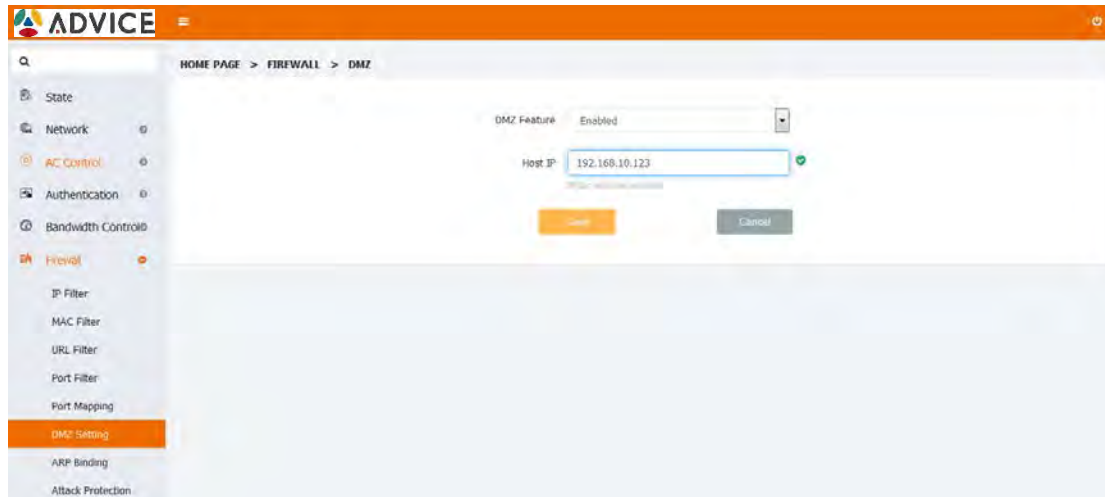
3. Click save and go into the Messages List page, and now the port forwarding function is successful configuration (the port is mapped to the external network port 30 to the internal network port 40).



7.6 DMZ settings

DMZ settings: DMZ is Demilitarized Zone. For solving the problem of external network accessing user can not visit the internal web server after install the firewall, so that set up this buffer

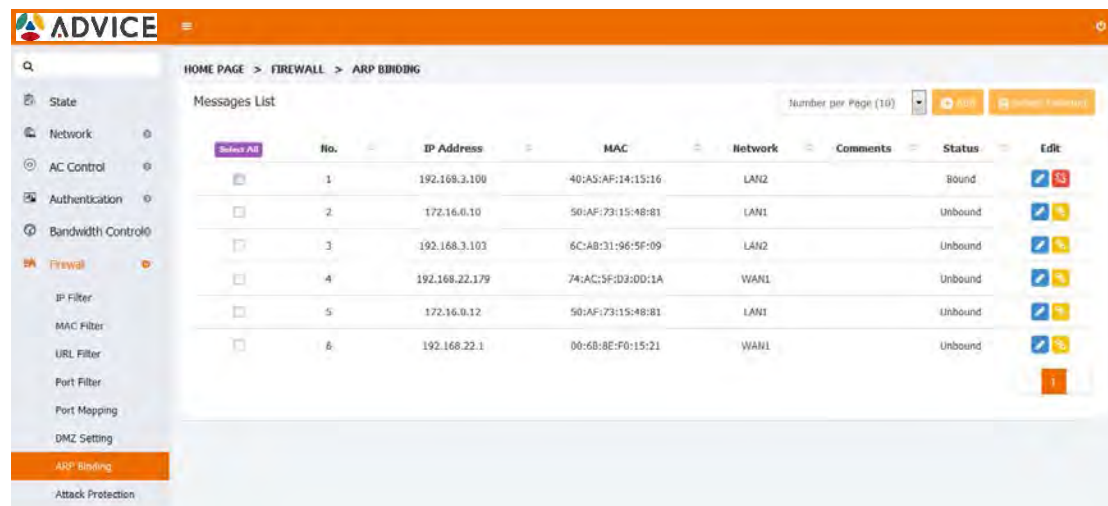
between nonsafety system and safety system. That buffer is located in a small web area between enterprise internal network and external network. You can place some server facilities which need to public in this small web area, such as enterprise Web server, FTP server and forum, etc. On the other hand, through this DMZ area, it is more effectively to protect the internal network. (Attn: when you use DMZ area, you need to eliminate your router's visit port in your DMZ.)



7.7 ARP Binding

ARP Binding: Address Resolution Protocol, it is a TCP/IP protocol which receives the physical address by IP.

Attention: ARP Binding isn't behave of your machine can receive the static IP, only receive it when you tick to choose compatible ARP binding list in DHCP static allocation.



HOME PAGE > FIREWALL > ARP BINDING

Messages List

Number per Page (10) [10] [20] [50] [100] [All]

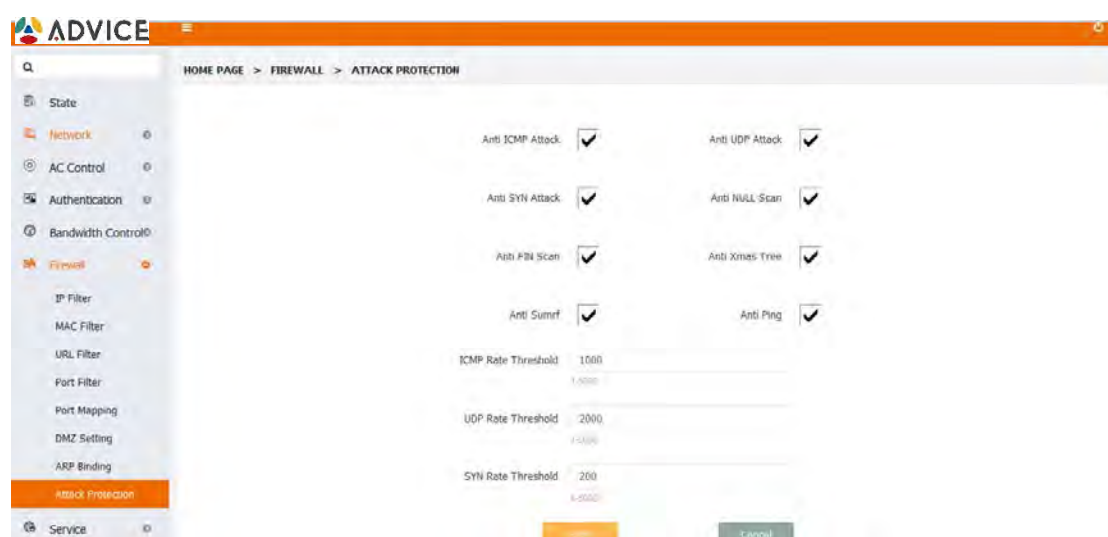
Select All	No.	IP Address	MAC	Network	Comments	Status	Edit
☐	1	192.168.3.100	40:AS:AF:14:15:16	LAN2		Bound	Edit Delete
☐	2	172.16.0.10	50:AF:73:15:48:81	LAN1		Unbound	Edit Delete
☐	3	192.168.3.103	6C:AB:31:96:5F:09	LAN2		Unbound	Edit Delete
☐	4	192.168.22.179	74:AC:5F:D3:00:1A	WAN1		Unbound	Edit Delete
☐	5	172.16.0.12	50:AF:73:15:48:81	LAN1		Unbound	Edit Delete
☐	6	192.168.22.1	00:68:8E:F0:15:21	WAN1		Unbound	Edit Delete

1

7.8 Attack Protection

Distributed Denial of Service (DDoS) attack is currently a common network attack method, and its English name is called Distributed Denial of Service. DDoS attacks are very harmful and difficult to prevent, and can directly cause website downtime and server crashes, causing authority. Damage, brand shame, loss of property, and other huge losses, open DDOS can effectively protect the network from attacks and protect the network security.

1. Go to the home page, click on "Firewall - Attack Protection" to enter the attack protection page, check the protection items, and click on save



HOME PAGE > FIREWALL > ATTACK PROTECTION

Anti ICMP Attack	☒	Anti UDP Attack	☒
Anti SYN Attack	☒	Anti NULL Scan	☒
Anti FIN Scan	☒	Anti Xmas Tree	☒
Anti Smurf	☒	Anti Ping	☒
ICMP Rate Threshold	1000 1-10000		
UDP Rate Threshold	2000 1-10000		
SYN Rate Threshold	200 1-10000		

[Save](#) [Cancel](#)

8 Service

8.1 DDNS Settings

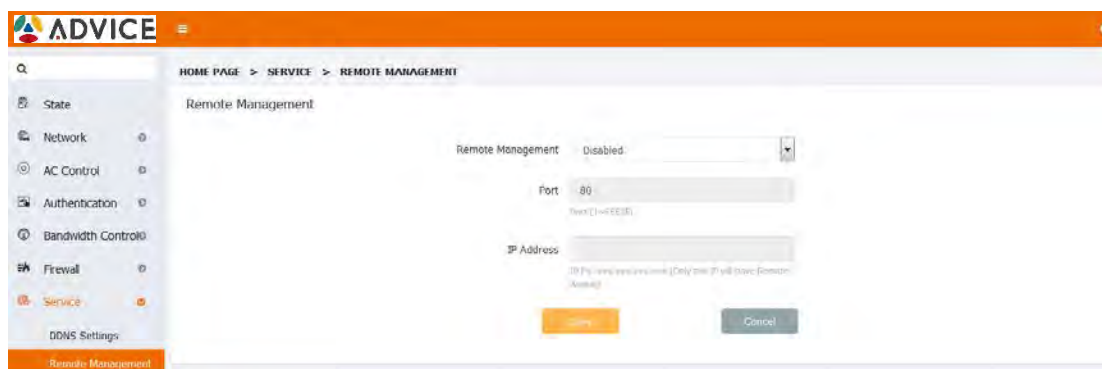
Add your domain name, domain name and password here. This supports dyndns, 3322, Oray three ways of domain name resolution. (Note: If the device is used as the primary route for PPPoE dialup, the source of the IP address is selected to resolve the network adapter. If you are doing the secondary or lower route, the source of the IP address here is to select the network)



8.2 Distance Setting

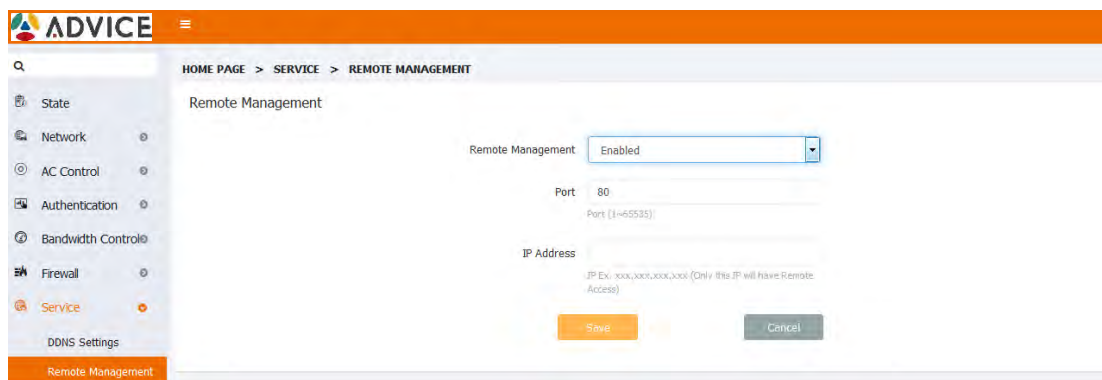
Enterprise network administrators want to manage routers anywhere on the network, allowing them to be managed and configured in real time and securely. Remote WEB management function can realize remote management of routers in the place of access to the Internet

1. Click "Service - Remote Management" on the main interface of the product to enter the remote setup page, as shown below



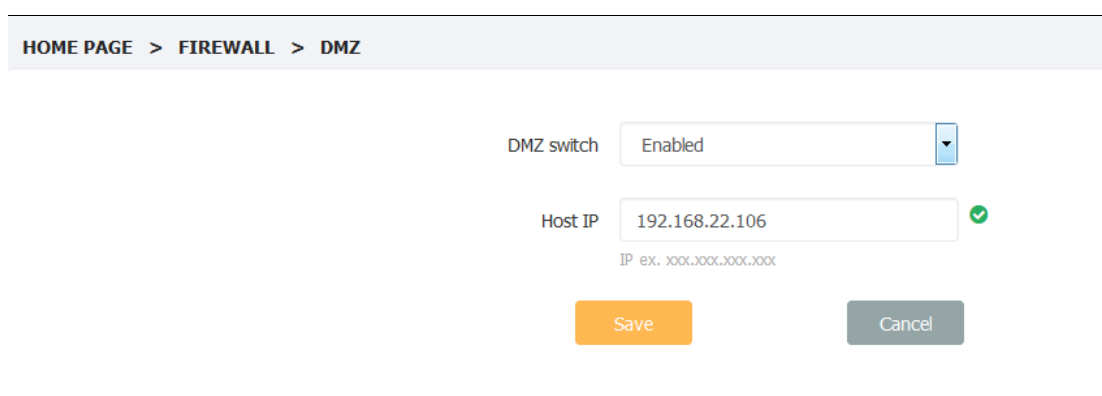
2. Switch is selected to start, the port enters 1~65535 any one port, ip address default to

remain empty, enter the specific ip only allow other network ip remote access, do not enter any external network IP remote access, and then click Save



3. Enter the gateway of the upper-level route to set up the virtual server, ip is the WAN port ip of the AC300, and the port number of the external network port and internal network port is the same as the port number set on the remote management page.

Name	Designate	IP Address	Status
Interface0	WAN1	192.168.22.106	✓
Interface1	LAN2	192.168.3.3	✓
Interface2	LAN1	172.16.0.1	✗
Interface3	LAN1	172.16.0.1	✗
Interface4	LAN1	172.16.0.1	✗



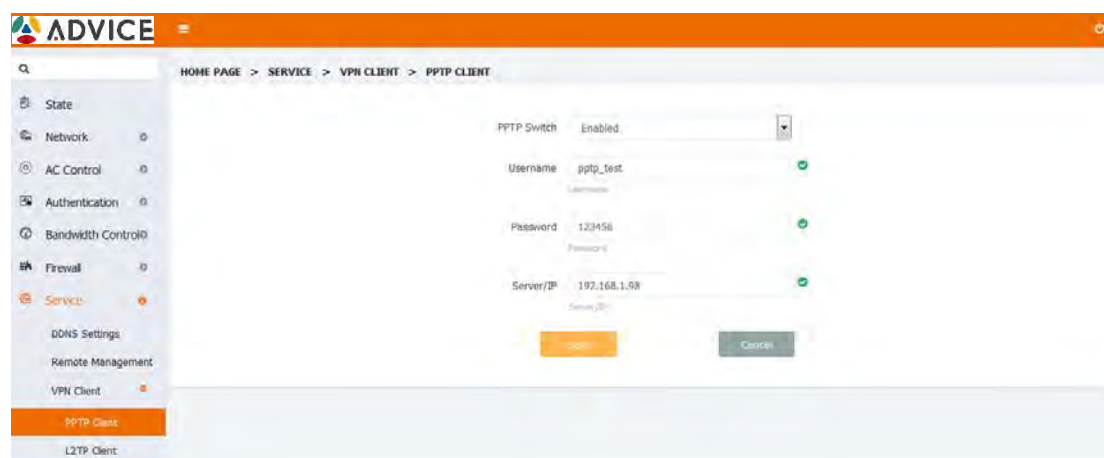
4. After added, connect to the upper-level route, enter the WAN port address of the device in the browser: port number (such as "192.168.22.106:80"), press Enter, you can access the gateway of the device remotely.

8.3 VPN Client

8.3.1 PPTP Client

PPTP Client:PPTP is Point to Point Tunneling Protocol.This protocol is a new enhanced security protocol which base on the PPP protocol,it support VPN,PAP and EAP,etc.enhanced security.It can also let the remote clients safety visit the enterprise network through dial-in ISP, directly connect the Internet or other network.

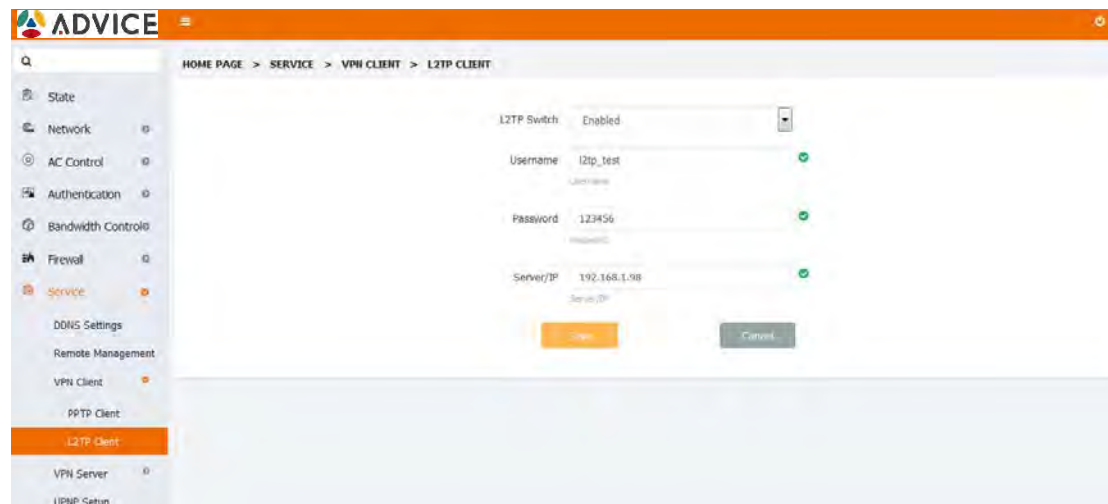
Use the PPTP client function,enabled the PPTP switch,enter the Username,Password and Server/IP,click “save”and finish the setting.



8.3.2 L2TP Client

L2TP Client:L2TP is an industrial standard Internet tunneling protocol,the function is the same as PPTP protocol,such as it can also encryption for the network traffic.But it also have the different,such as PPTP require the network as the IP network,L2TP require point to point connection for the data packet.PPTP use the single tunnel,L2TP use multi-tunnels.L2TP provide header compression and tunnel verify,but PPTP not support it.

Use L2TP Client,enabled L2TP Switch,enter the username,password and server/IP,click save then finish the L2TP client function setting.

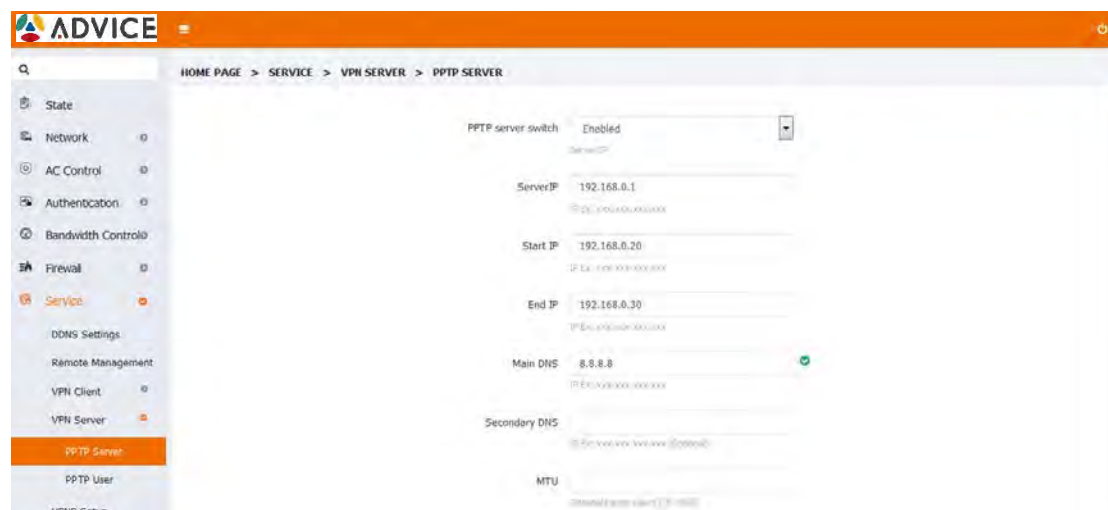


8.4 VPN Server

VPN is Virtual Private Network, it built up a temporary, safety and simulated point to point connection through a public network (such as Internet). This is an information tunnel which pass through the public network, the data can safety transmitting in the public network through this tunnel. So the user can vividly call it "Network of Network".

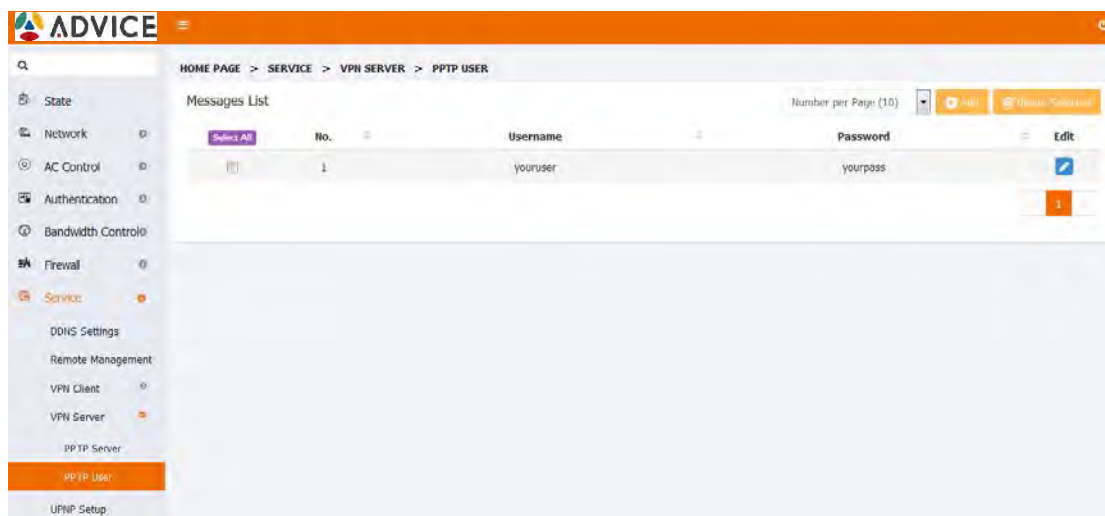
8.4.1 PPTP Server

1. Go into PPTP Server setting page, enter VPN account and password, as below:





2.Go into PPTP USER page, set up the user



3. Open another laptop, connect to the external network, ip address must follow the map VPN server is not in the same network segment, and set up a destination host ip 192.168.100.157 VPN connection, as below



3. Open the VPN quick connection to the laptop network connection, enter the user name and password added by PPTP, test the connection is successful, and assign the specified IP address, as below:



8.5 UPNP Settings

UPnP is a variety of intelligent devices, wireless devices and PC to realize peer to peer network connection (P2P) structure throughout the world. UPnP is a distributed and open network

structure.



ADVICE

首页 > 网络服务 > UPNP设置

信息列表

每页显示条数:10 UPNP开关 **ON**

编号	协议	内网地址	外网端口	内网端口	描述
1	TCP	192.168.100.45	44143	8000	DVR_NVR
2	TCP	192.168.100.45	41095	9010	DVR_NVR
3	TCP	192.168.100.45	50959	9020	DVR_NVR
4	TCP	192.168.0.102	46497	30005	PHICOMM
5	TCP	192.168.100.43	8000	8000	IPC_Control
6	TCP	192.168.100.41	47172	8000	IPC_Control
7	TCP	192.168.100.42	40981	8000	IPC_Control
8	TCP	192.168.1.150	13569	13569	Thunder5
9	UDP	192.168.1.150	13569	8927	Thunder5
10	TCP	192.168.1.191	17476	8896	Thunder5

< 1 2 3 4 5 ... 16 >

9 Log and Statistics

9.1 Log

User log: Here recorded the system's working status situation when the device is working.

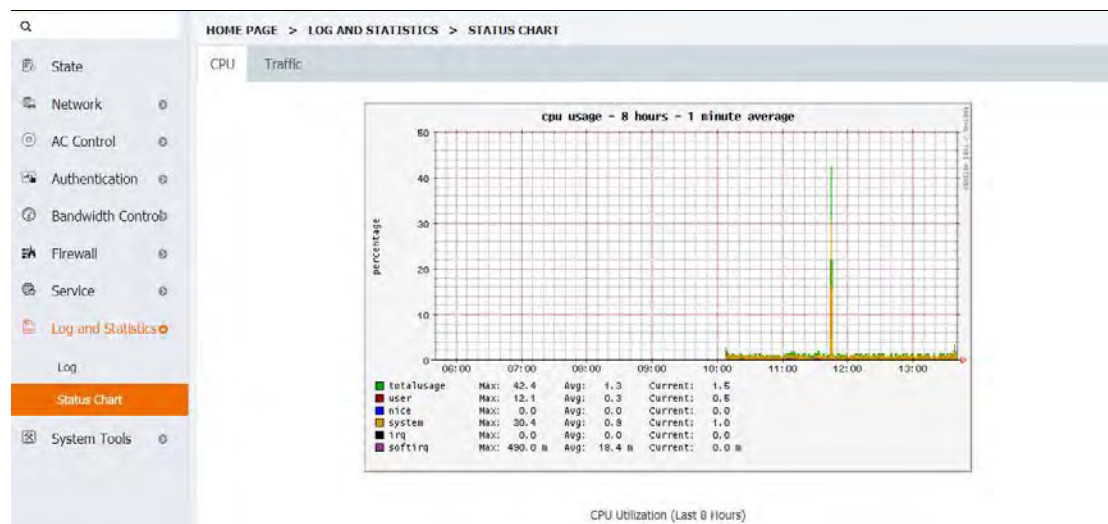
1. Go to WEB and open Log's User log page,click "GET LOG"button,then the bottom of the page will refresh the log details every moments,as below:

ADVICE			
HOME PAGE > LOG AND STATISTICS > LOG			
GET LOGS			
Date	Level	Log	
2018/3/24 13:43:00	Info	USER root pid 11229 cmd /etc/rd/loadrtd start	
2018/3/24 13:42:00	Info	USER root pid 11084 cmd /etc/rd/loadrtd start	
2018/3/24 13:41:00	Info	USER root pid 10948 cmd /etc/rd/loadrtd start	
2018/3/24 13:40:24	Info	DHCPACK on 192.168.3.100 to 40:a5:af:14:15:16 via br-lan1	
2018/3/24 13:40:24	Info	DHCPREQUEST for 192.168.3.100 from 40:a5:af:14:15:16 via br-lan1	
2018/3/24 13:40:24	Info	Wrote 5 leases to leases file.	
2018/3/24 13:40:00	Info	USER root pid 10768 cmd /etc/rd/loadrtd start	
2018/3/24 13:39:00	Info	USER root pid 10628 cmd /etc/rd/loadrtd start	
2018/3/24 13:38:01	Info	User admin/admin authorized OK	
2018/3/24 13:38:00	Info	USER root pid 10435 cmd /etc/rd/loadrtd start	
2018/3/24 13:37:00	Info	USER root pid 10299 cmd /etc/rd/loadrtd start	

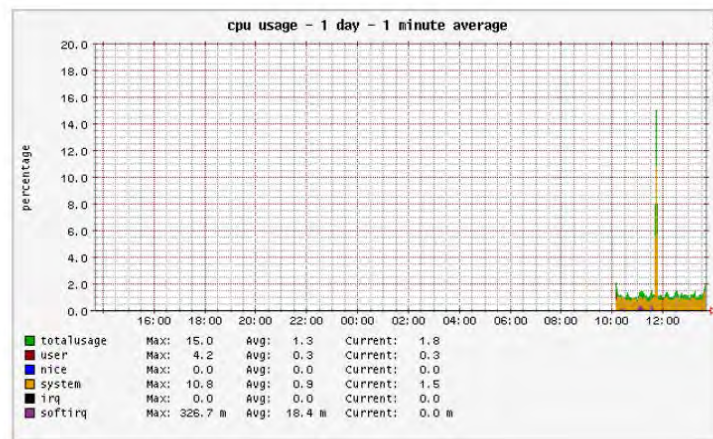
9.2 Status chart

Historical Statistics

1.CPU:here record the CPU usage information when the devise working 8 hours,one day and one week.

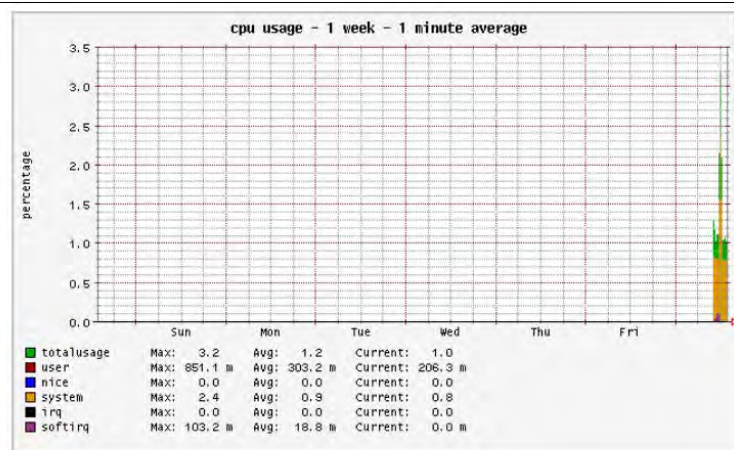


<8 Hours>



CPU Utilization (Last 1 Day)

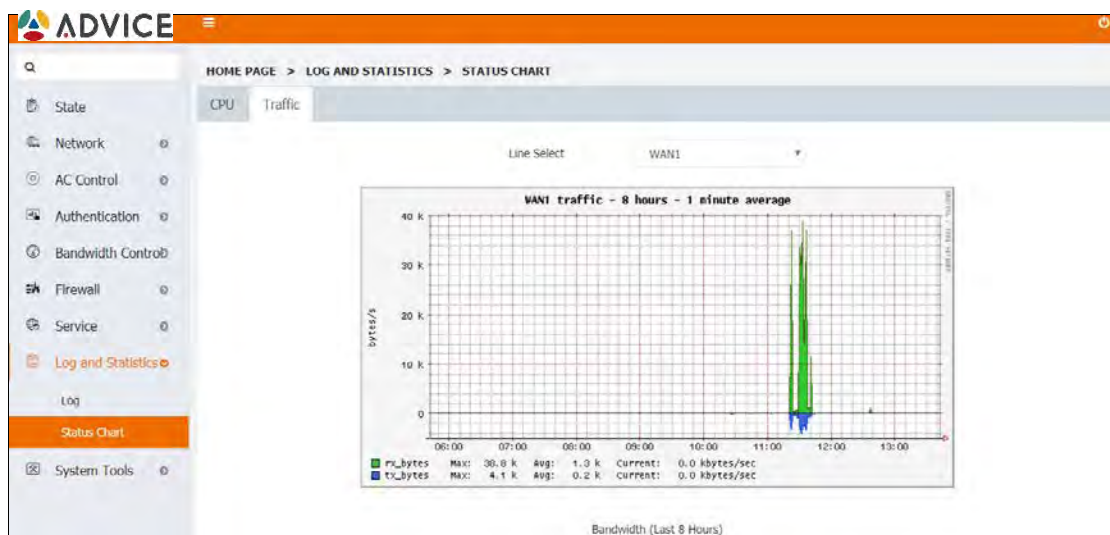
<One Day>



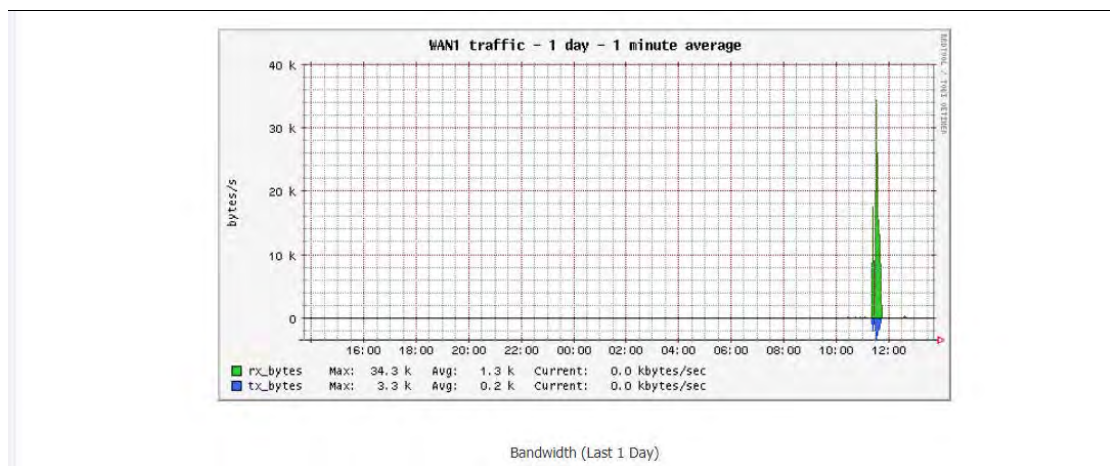
CPU Utilization (Last 1 Week)

<One Week>

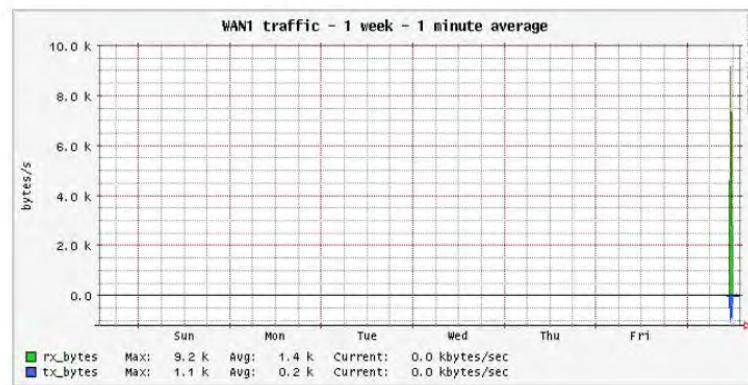
2.Traffic:here record the traffic status information when the devise working 8 hours,one day and one week.



<8 Hours>



<One Day>



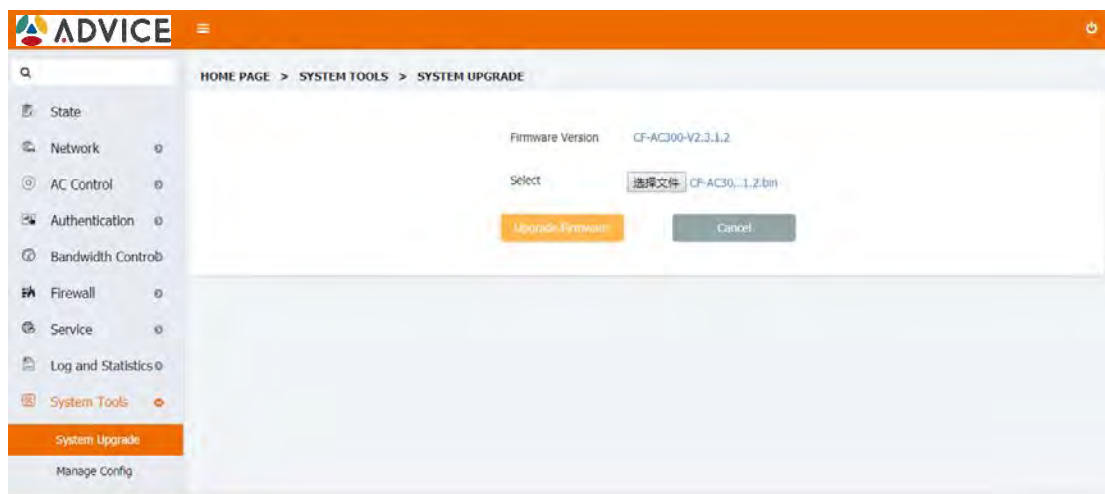
Bandwidth (Last 1 Week)

<One Week>

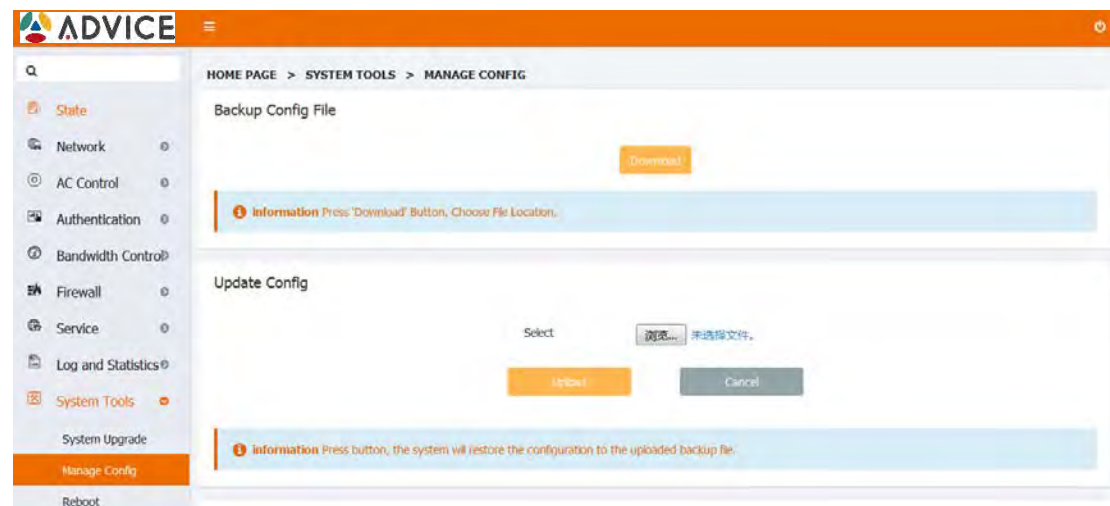
10 System Tools

10.1 System upgrade

1. Download the newest X86 OrangeOS firmware in the website www.comfast.com.cn, download and keep it on the computer. Go into the system upgrade page, click to choose the firmware you had downloaded in this page. Then click "Upgrade Firmware" button to upgrade.

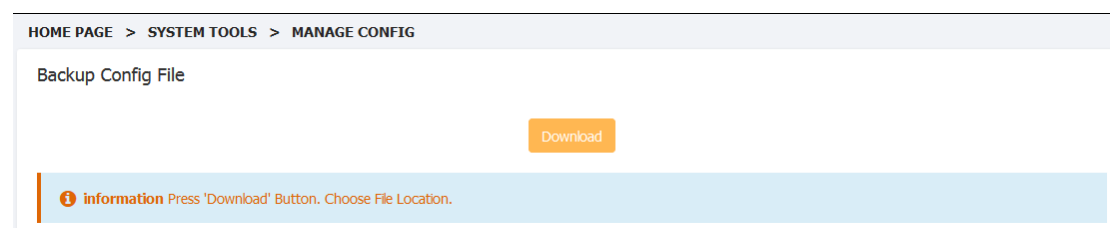


10.2 Configure Backup

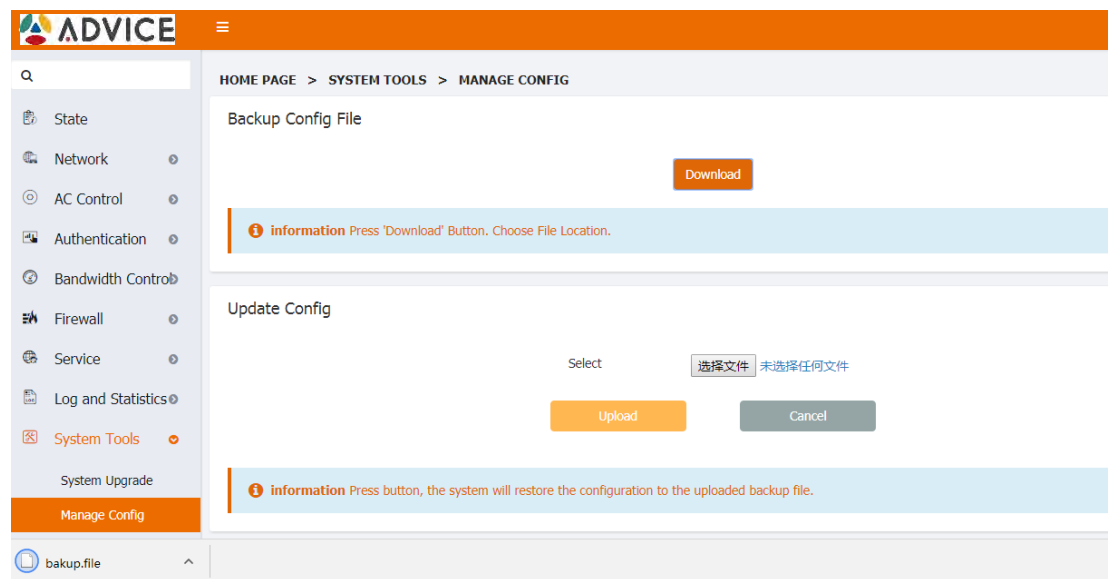


Configuration backup:after you configure the device's parameters,you can click "download"button to save the configure parameters.

1. Go into the configure backup page,click the configuration backup's "download"button.

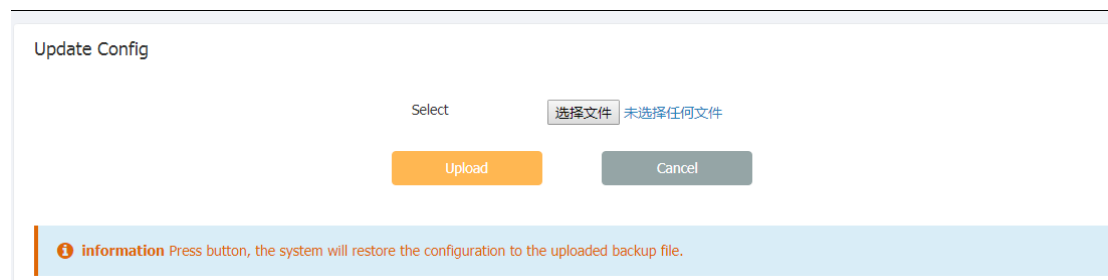


2. Select the path to save the configuration, and then click OK, the current configuration has been saved on the local computer desktop;

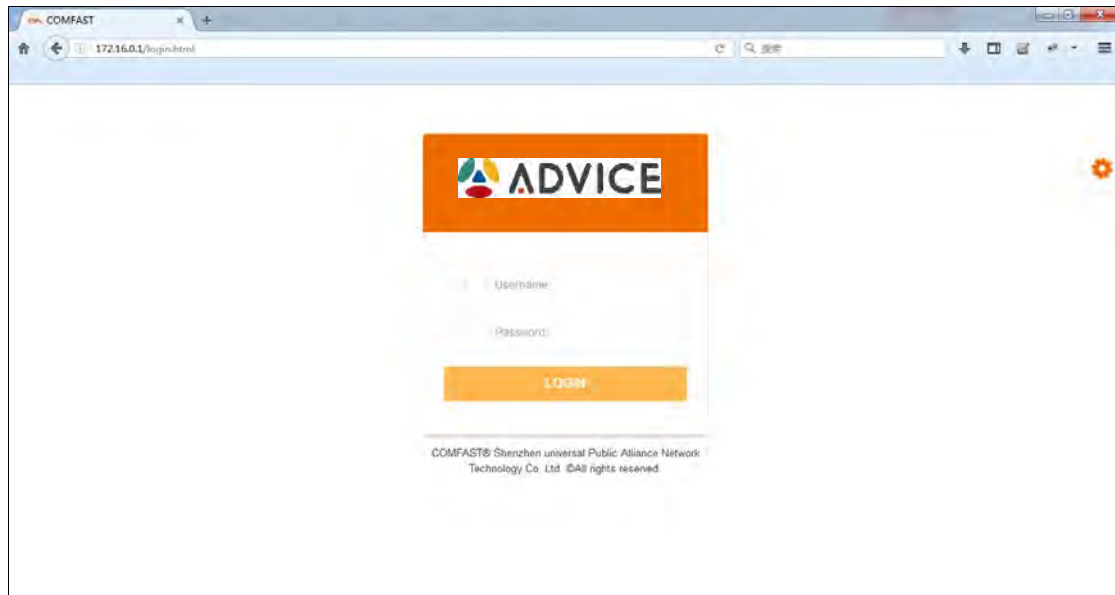


Configure Update: If you need to change the configure temporary or the device was restored the default settings carelessly, you can select to choose the configure file that you save before. click “upload” button to restore.

1. Go into the configure backup page, click configure update’s scan, choose the bakup.file you save before.

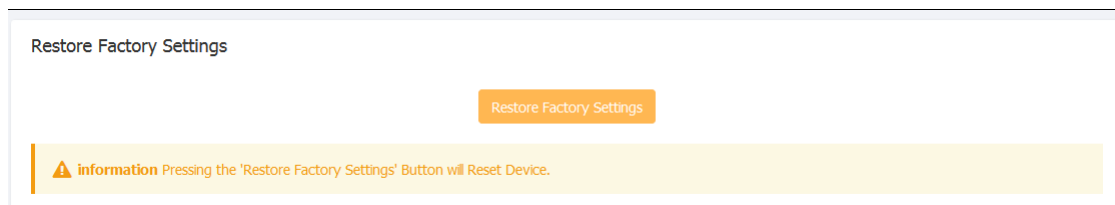


2. Click “Upload” and some times later here will popping the interface to login again.

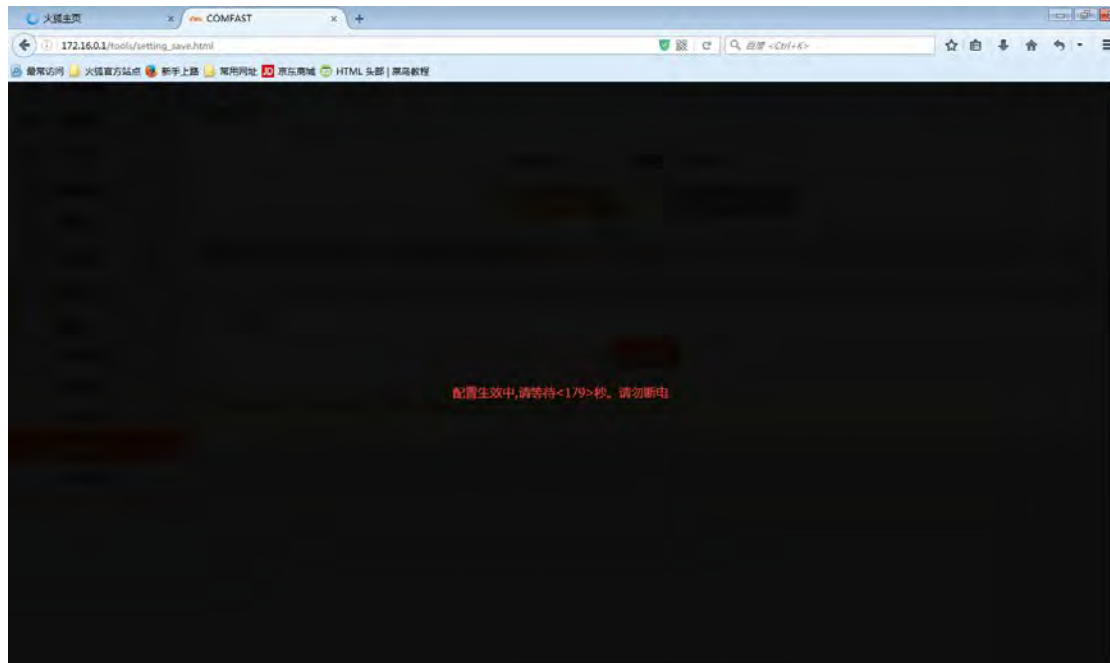


Restore factory settings:when you have setting lots of parameters or the device network throughput is unusually,you can click “restore factory settings”button to restore the factory status.

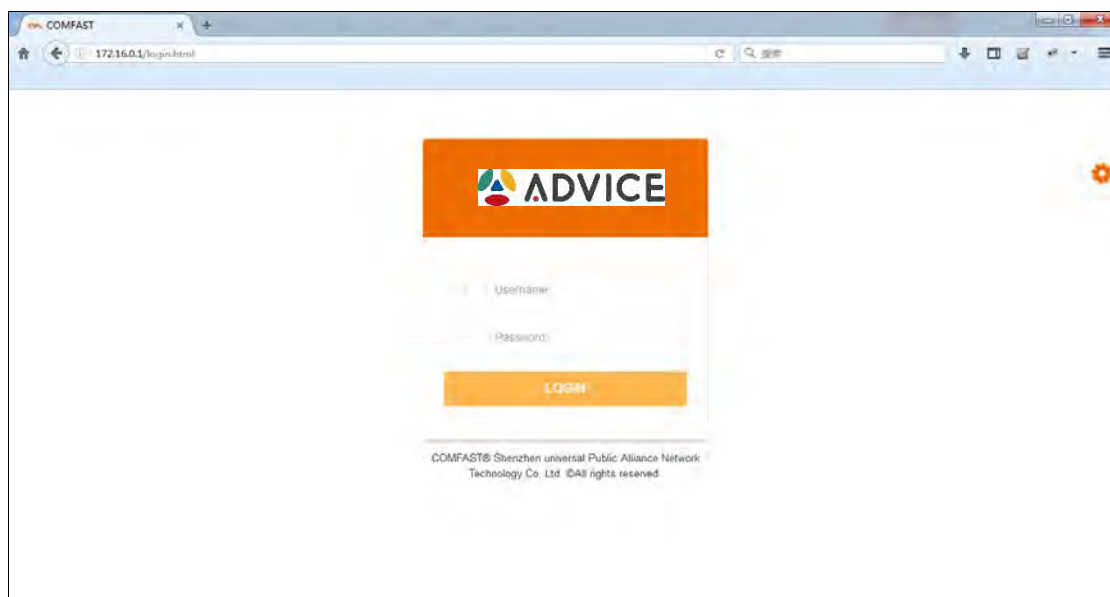
1.the configure backup page,click “restore factory settings”button



2.Here will popping the notice information:the configuration is effecting,pls wait for <180> seconds,Pls do not outage.



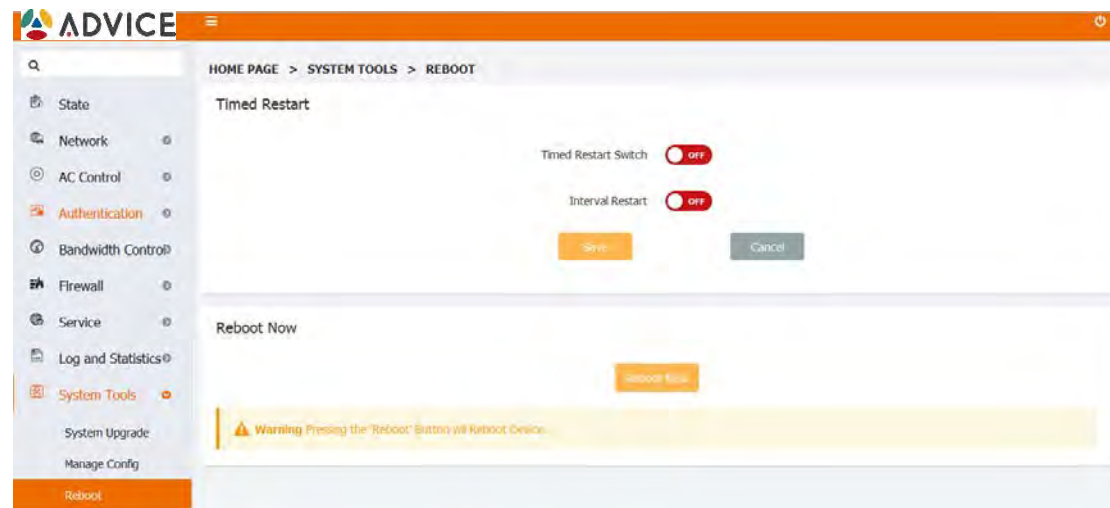
3. 3 minutes later here will automatic popping a interface to login again,it is success to restore factory settings.



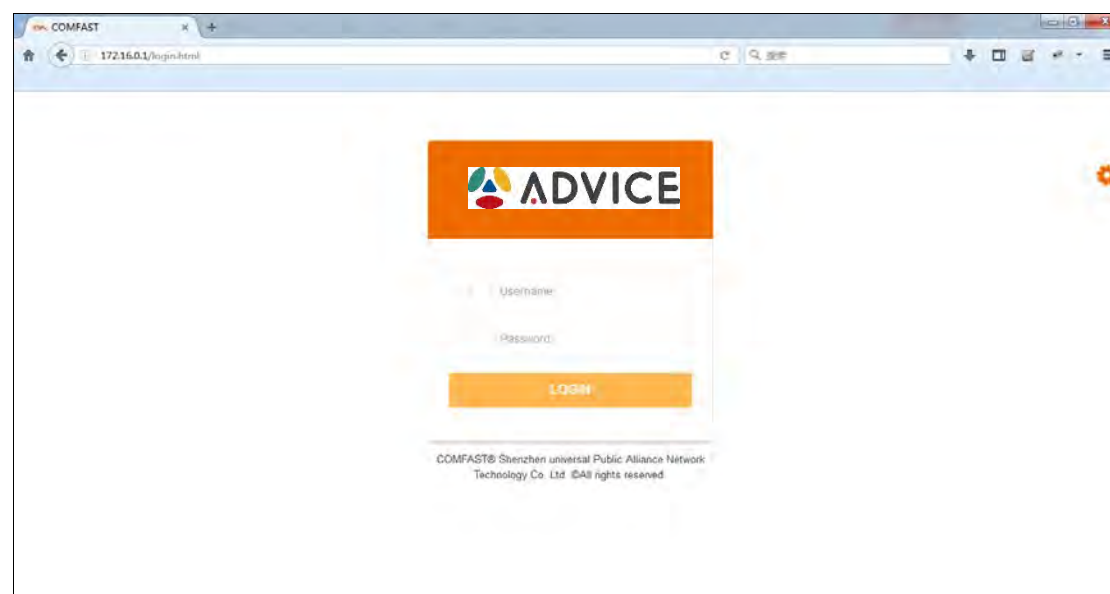
10.3 System Reboot

10.3.1 Reboot Now

1. Go into the system reboot page,click "Reboot Now" button.

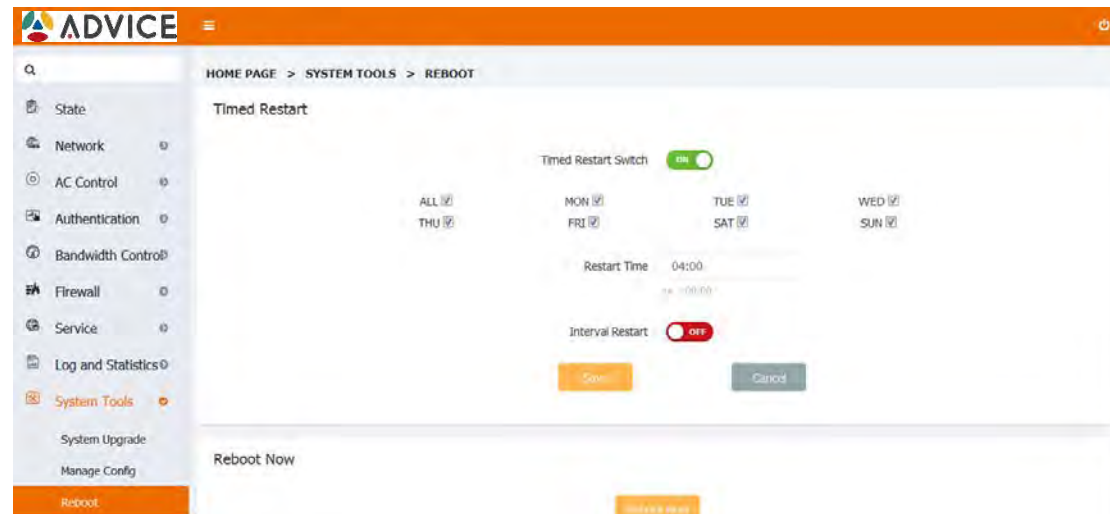


2. Wait for 1 minute, it will restart and come out login interface.

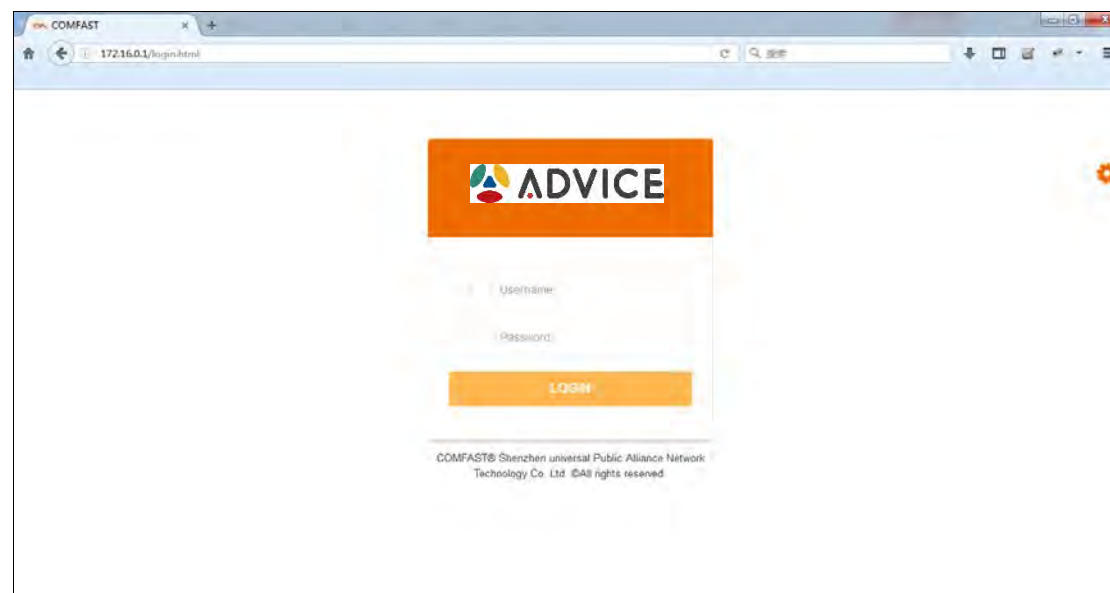


10.3.2 Timed Restart

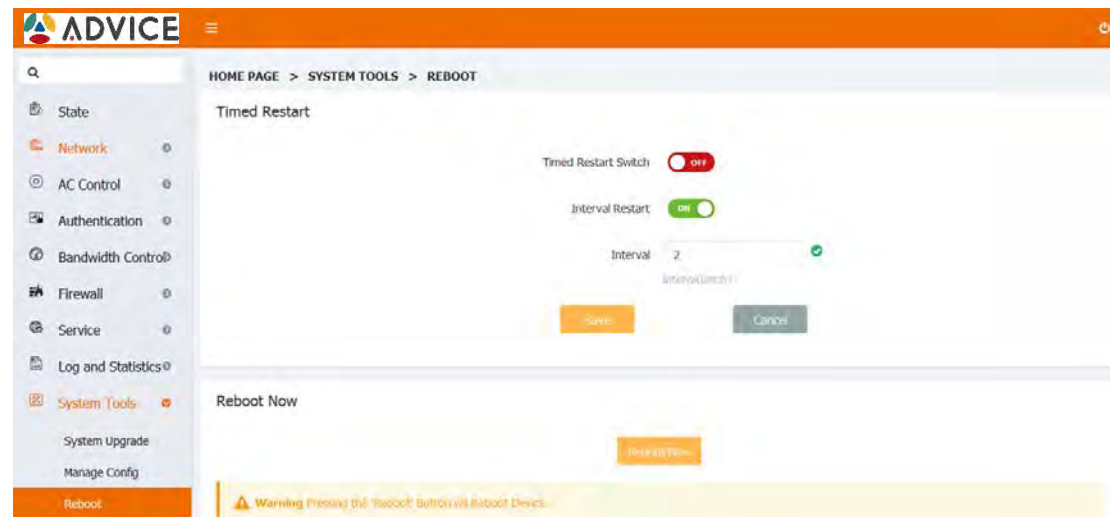
1. Go into the system restart page, you can open a scheduled reboot, check the restart date, fill in the restart time, click Settings



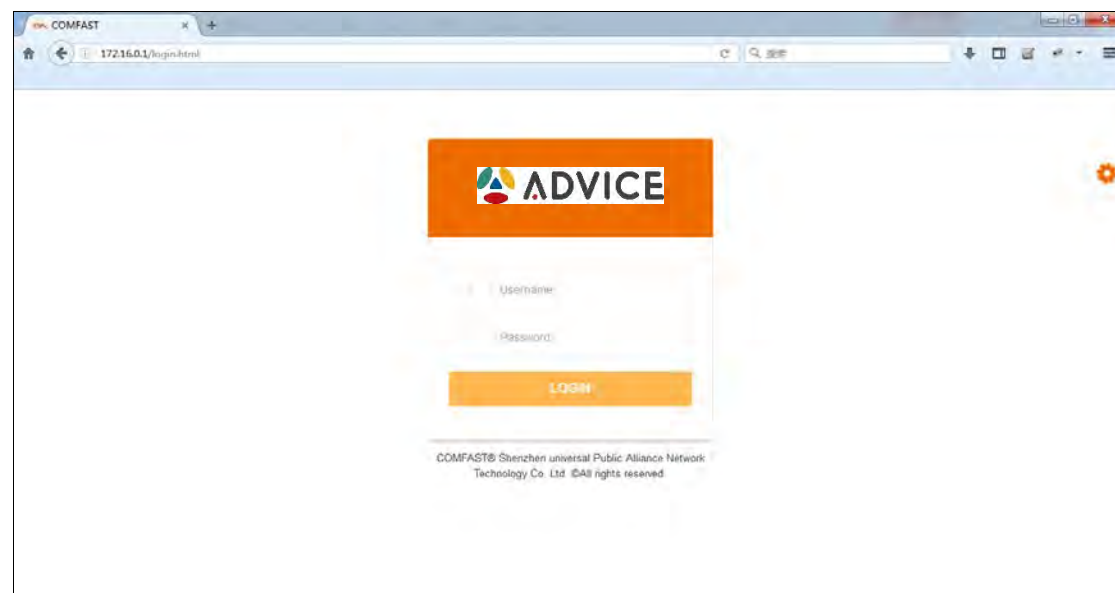
2. After successful saving, the device will restart automatically every time you fill in, automatically pop-up to re-enter the system interface



3. Go into the system restart page, you can restart the function interval, fill in the interval restart time, click Settings



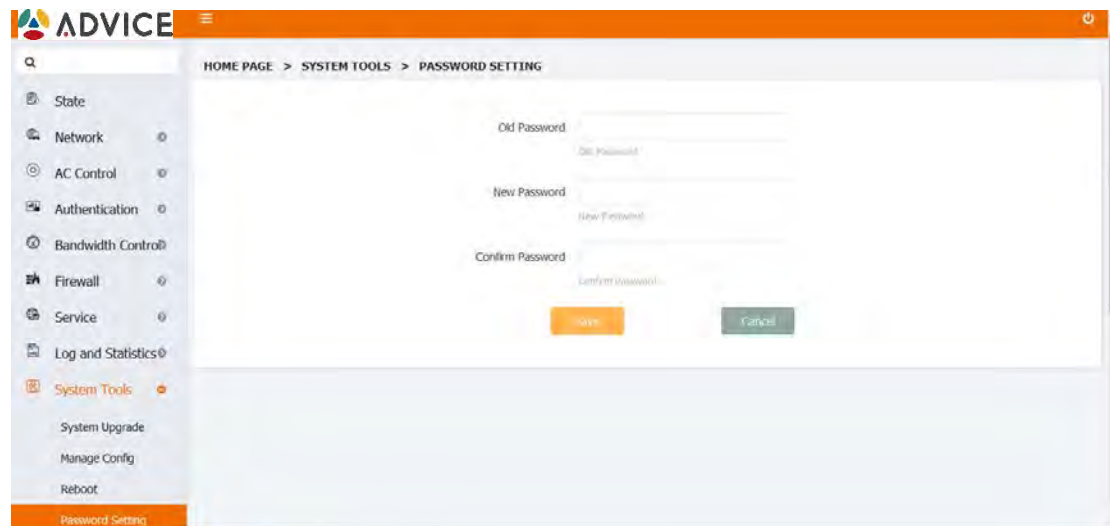
4. As shown above, the device restarts every two hours. After the restart is successful, the system will automatically re-enter the login interface.



10.4 User setting

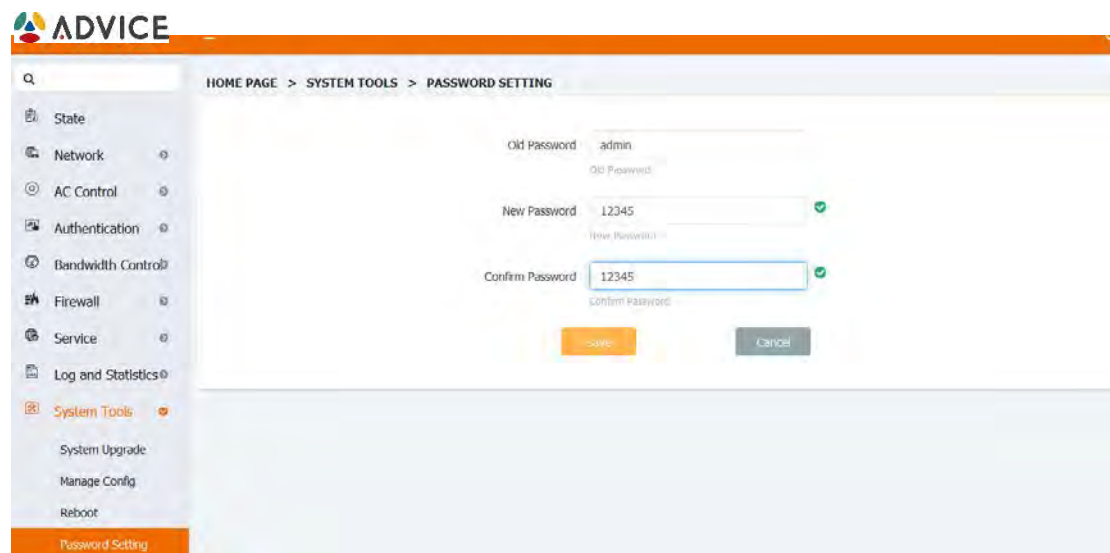
Here you can renew the Username and Password, after setting you need to use the new username and new password to login. (ATTN: the username support Chinese)

1. Go into WEB home page and open system tool "User setting" page, as below:



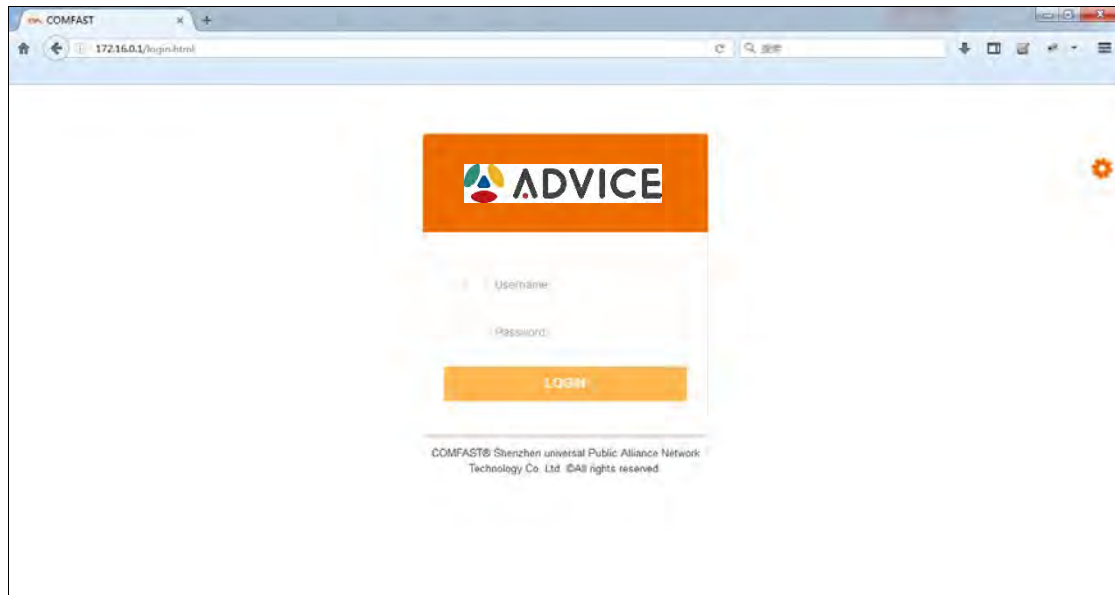
The screenshot shows the ADVICE web interface with the 'PASSWORD SETTING' page. The left sidebar contains a menu with options: State, Network, AC Control, Authentication, Bandwidth Control, Firewall, Service, Log and Statistics, System Tools (highlighted), System Upgrade, Manage Config, and Reboot. The main content area has a breadcrumb trail: HOME PAGE > SYSTEM TOOLS > PASSWORD SETTING. The form includes three input fields: 'Old Password', 'New Password', and 'Confirm Password'. Below these fields are 'Save' and 'Cancel' buttons. The 'Old Password' field contains the text 'admin'.

2. Enter the new password, click save:



This screenshot shows the same ADVICE web interface, but now the 'New Password' and 'Confirm Password' fields contain the text '12345'. Green checkmarks are visible to the right of these fields, indicating they are valid. The 'Old Password' field still contains 'admin'. The 'Save' and 'Cancel' buttons remain at the bottom of the form.

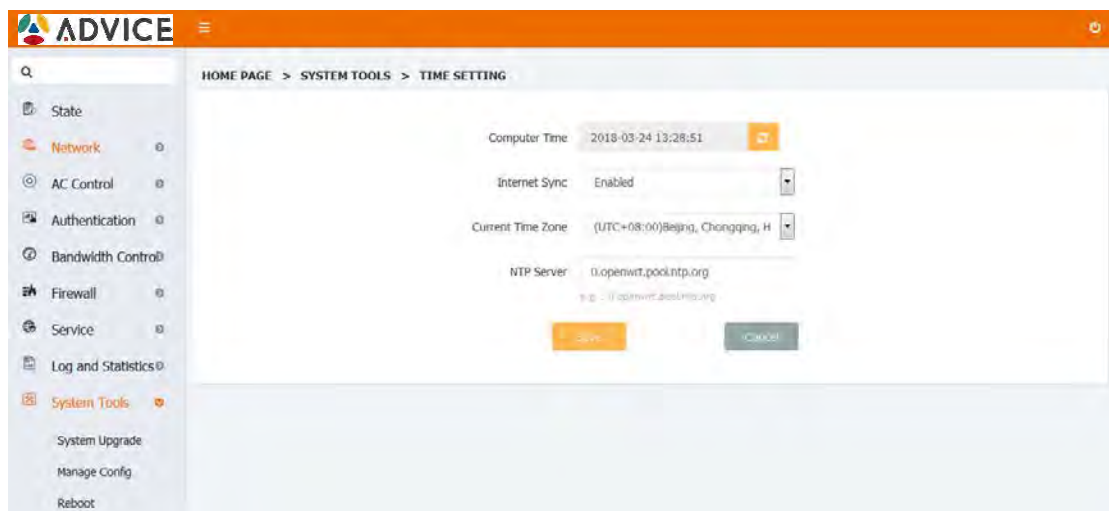
3. Wait for some seconds and here will popping anew login interface, and you need to enter the new password to login.



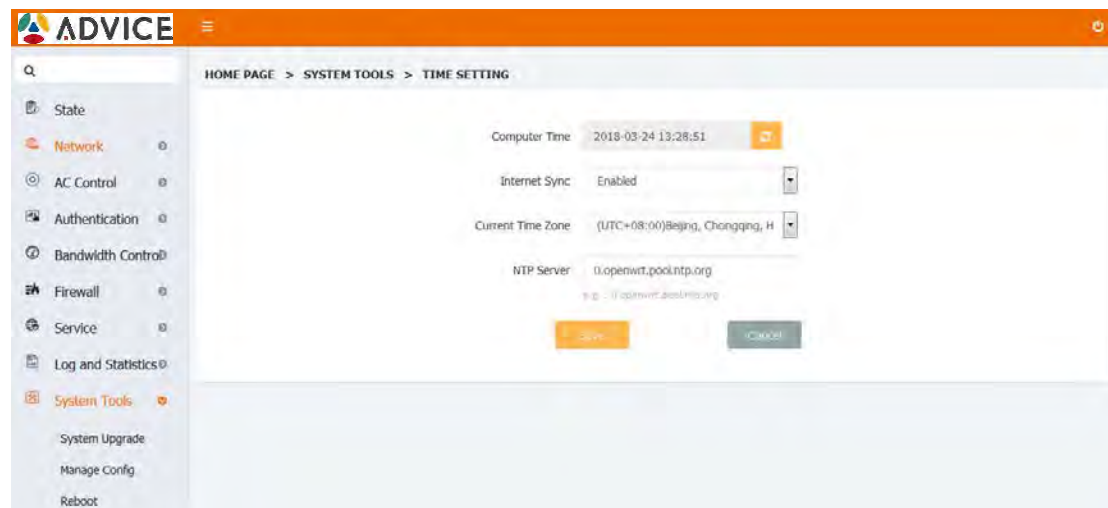
10.5 Time Setting

Here you can setting the sync Computer time,open Internet sync time,the device will be automatic sync server time at the situation of networking.

1.Go into WEB home page and open the system tool “PING”page,as below:

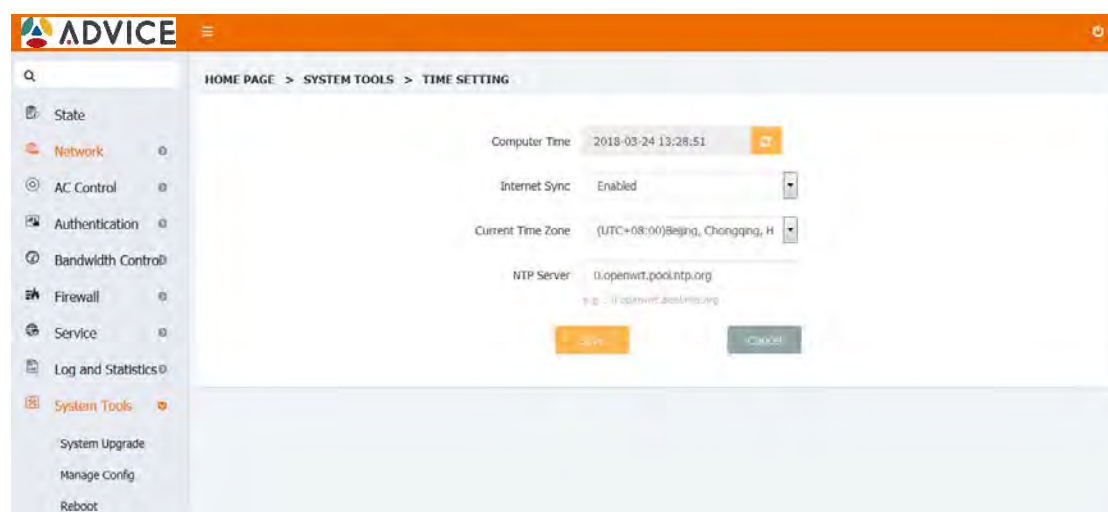


2. Click Internet sync switch's black button,choose “Enabled”,then click save.



3. Wait for 5 seconds, the computer time will be consistent with the network time, and will automatically synchronize;

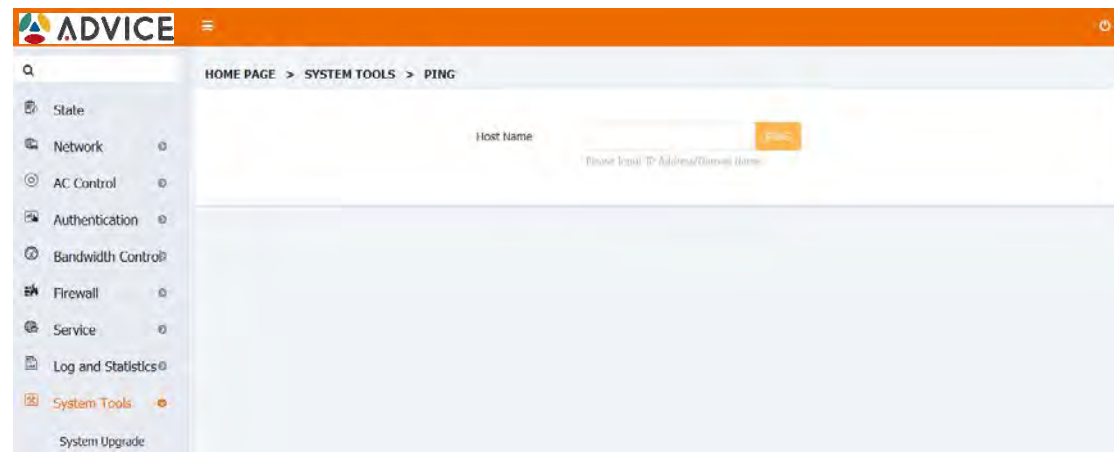
4. Disable the computer time, use the time set by the machine, you can turn off the Internet time synchronization, manually set the device time.



10.6 PING Tools

Here fill in the IP/Domain name, the system will show the situation that if it is connected, transmitted or received and delay.

1. Go into WEB home page and open the system tool “PING tools” page, as below:



2. Enter IP: 172.16.0.1, click "PING" button, wait some seconds later, it will show the result, as below:

