XonTel

XT-1000AC

Wireless Access Point Controller & Multi-WAN Gateway

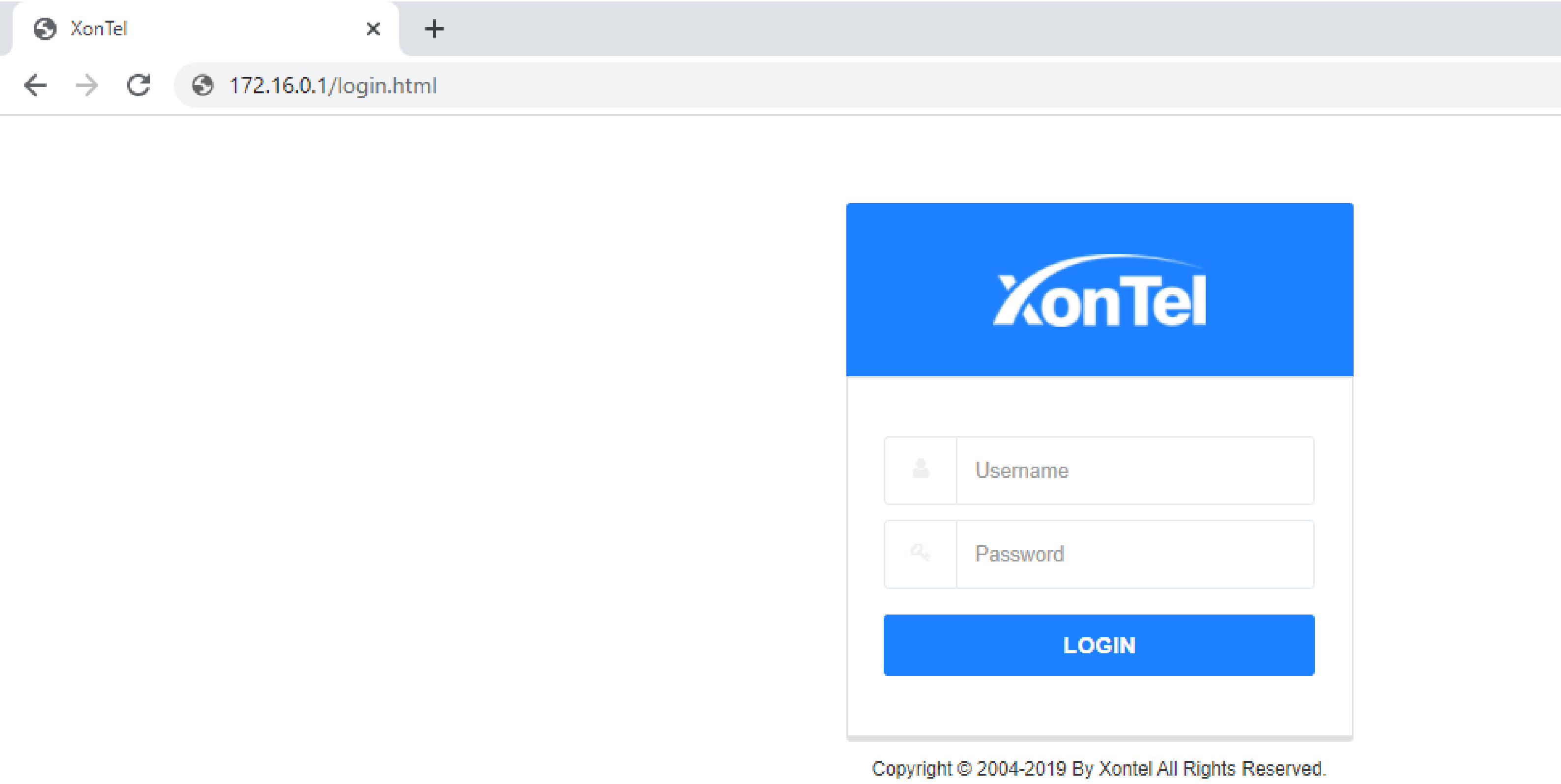
User Manual

Table of Contents

1 Log In

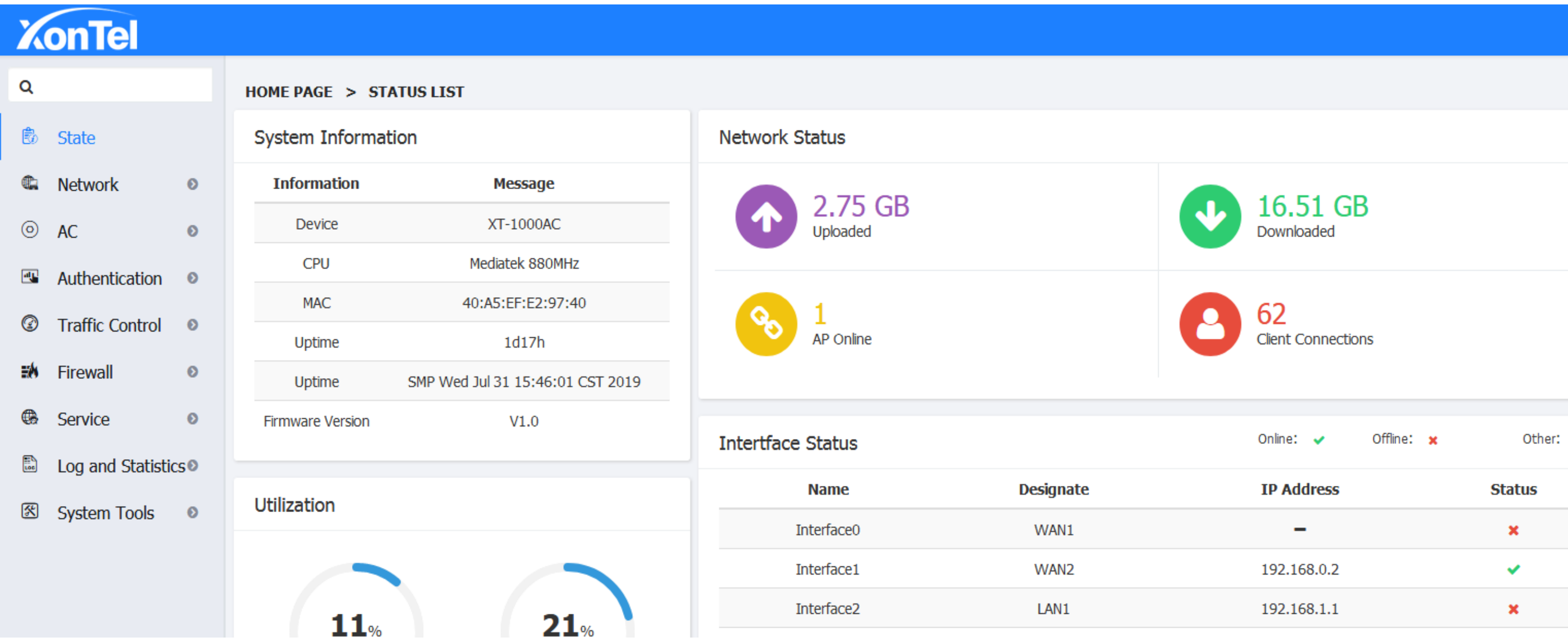
1. **XT-1000AC is based on the browser's configuration interface. Connect your PC to XT-100AC LAN (Eth5) port, open your browser and input IP address as 172.16.0.1**

2. Input user name " admin ", Password " xontel ". 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, Ethernet status and Traffic rate data



XonTel

HOME PAGE > STATUS LIST

- State
- Network
- AC
- Authentication
- Traffic Control
- Firewall
- Service
- Log and Statistics
- System Tools

System Information

Information	Message
Device	XT-1000AC
CPU	Mediatek 880MHz
MAC	40:A5:EF:E2:97:40
Uptime	1d17h
Uptime	SMP Wed Jul 31 15:46:01 CST 2019
Firmware Version	V1.0

Network Status

2.75 GB Uploaded

16.51 GB Downloaded

1 AP Online

62 Client Connections

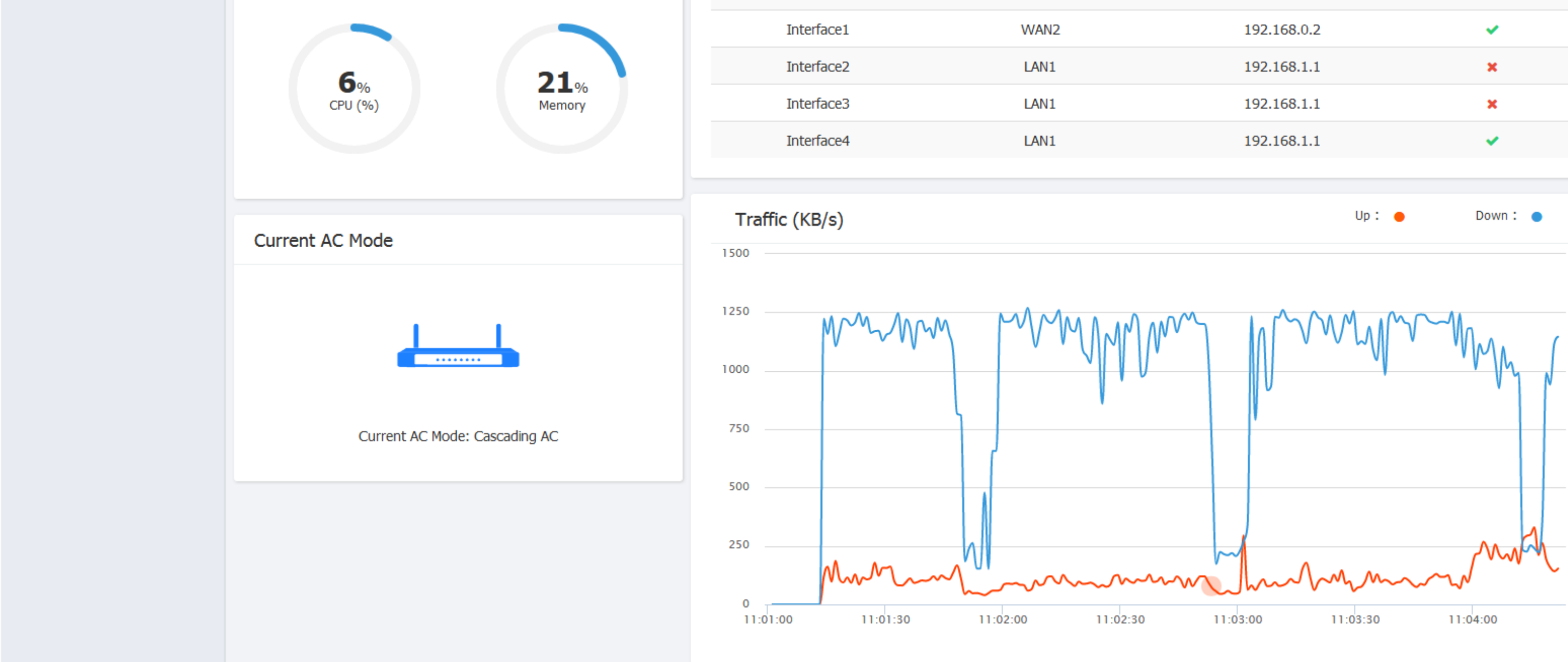
Intertface Status

Online: ✓ Offline: ✗ Other:

Name	Designate	IP Address	Status
Interface0	WAN1	–	✗
Interface1	WAN2	192.168.0.2	✓
Interface2	LAN1	192.168.1.1	✗

Utilization

11% 21%



Name	Designate	IP Address	Status
Interface1	WAN2	192.168.0.2	✓
Interface2	LAN1	192.168.1.1	✗
Interface3	LAN1	192.168.1.1	✗
Interface4	LAN1	192.168.1.1	✓

6% CPU (%)

21% Memory

Current AC Mode

Current AC Mode: Cascading AC

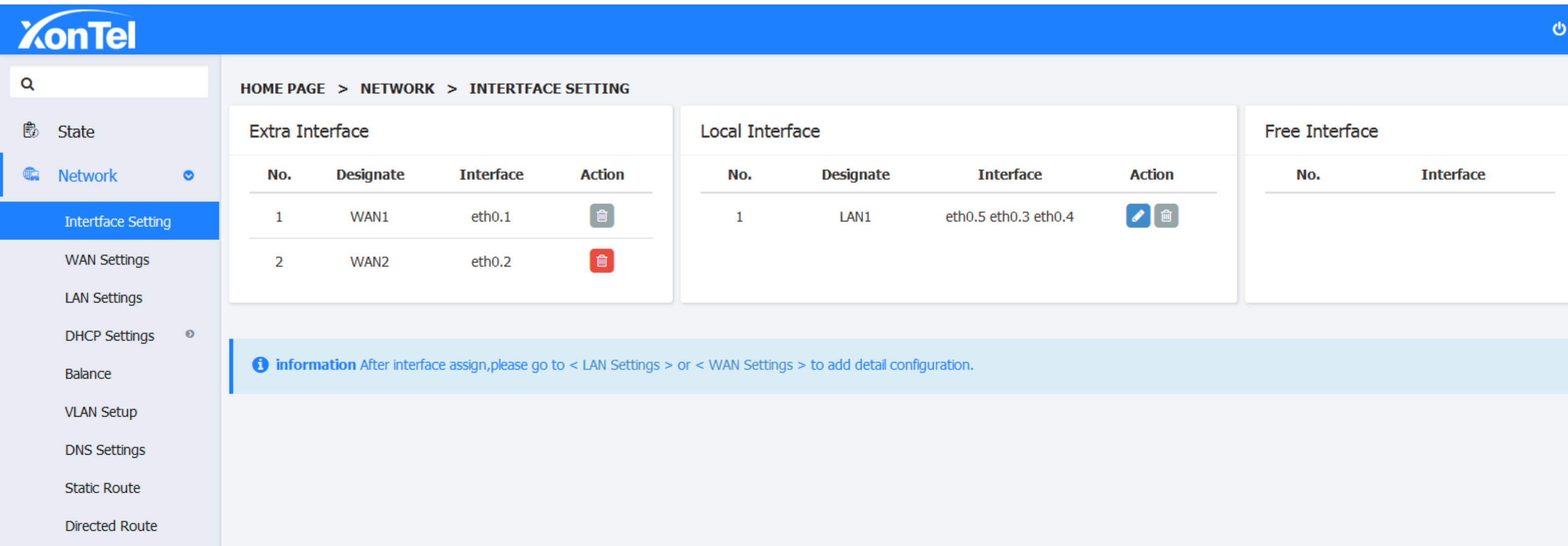
Traffic (KB/s)

3 Network

3.1 Interface Setting

The “eth0” is defaulted to be WAN port. “eth5” is defaulted to be LAN port and it cannot edit. The rest “eth1-eth4” is customized to be WAN port or LAN port. After designated the WAN port or LAN port, set up the internal network and outer network by “Local Network” and “WAN Settings”.

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



HOME PAGE > NETWORK > INTERTFACE SETTING

Extra Interface

No.	Designate	Interface	Action
1	WAN1	eth0.1	🗑
2	WAN2	eth0.2	🗑

Local Interface

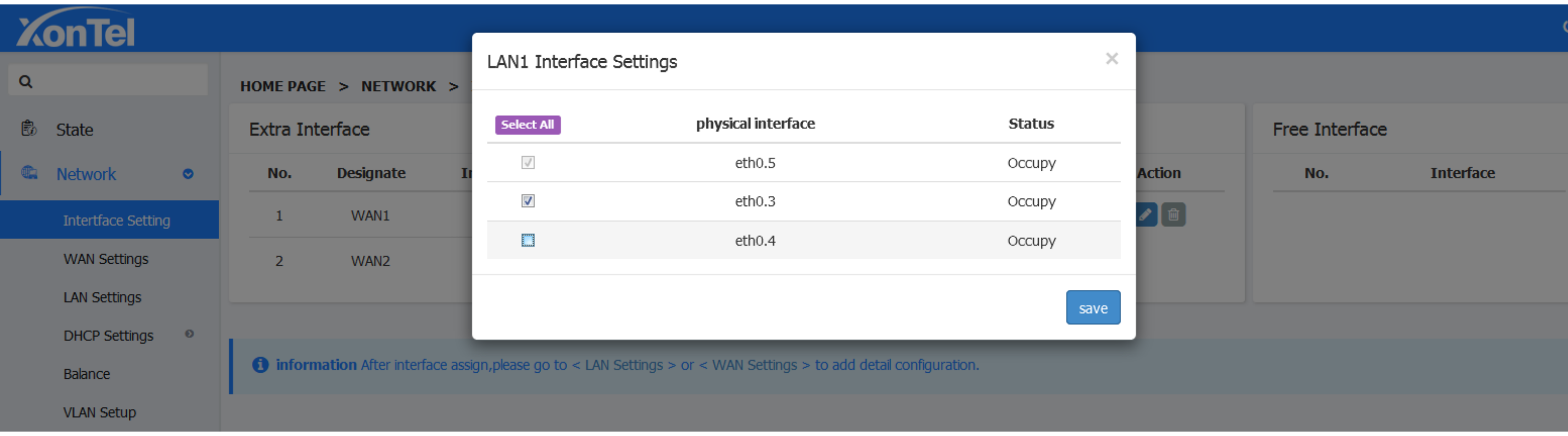
No.	Designate	Interface	Action
1	LAN1	eth0.5 eth0.3 eth0.4	✎ 🗑

Free Interface

No.	Interface

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

2. Click the “Edit” button to go into the “LAN1 Interface Settings” page, you can release free Ethernet ports. e.g eth0.4 is unchecked in below picture:

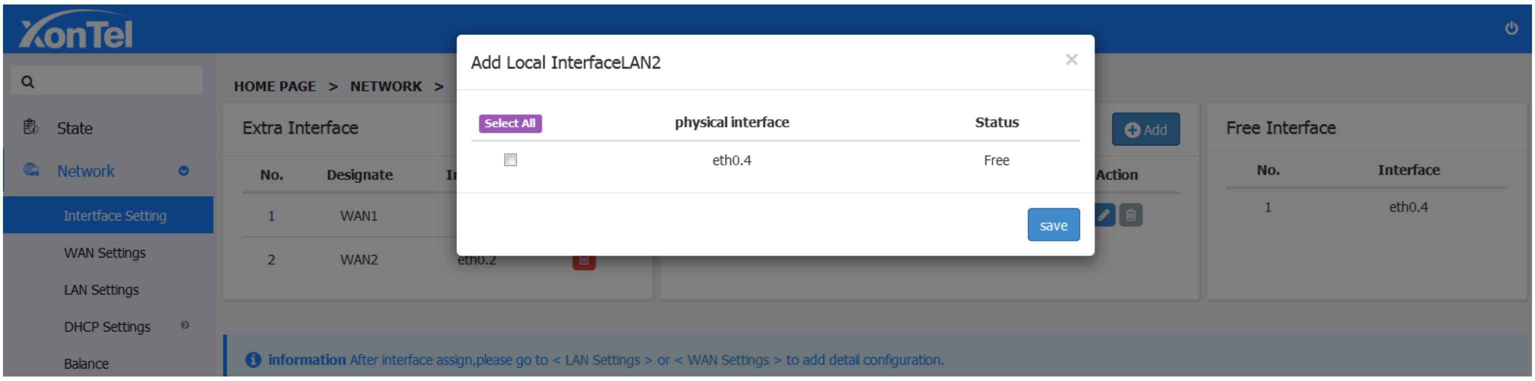


LAN1 Interface Settings

Select All	physical interface	Status
☑	eth0.5	Occupy
☑	eth0.3	Occupy
□	eth0.4	Occupy

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

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:



Add Local InterfaceLAN2

Select All	physical interface	Status
☐	eth0.4	Free

Extra Interface

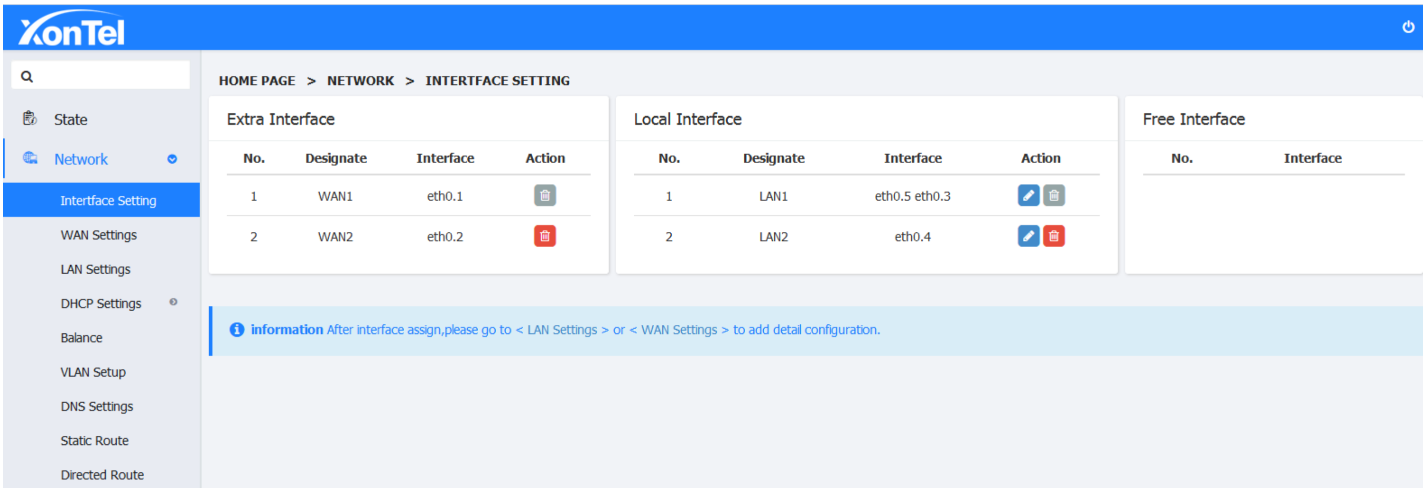
No.	Designate	I…
1	WAN1	
2	WAN2	eth0.2

Free Interface

No.	Interface
1	eth0.4

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

4. **Click “Save” and the Interface list which you add will appear in the local Interface as new Interface.**



Extra Interface

No.	Designate	Interface	Action
1	WAN1	eth0.1	🗑
2	WAN2	eth0.2	🗑

Local Interface

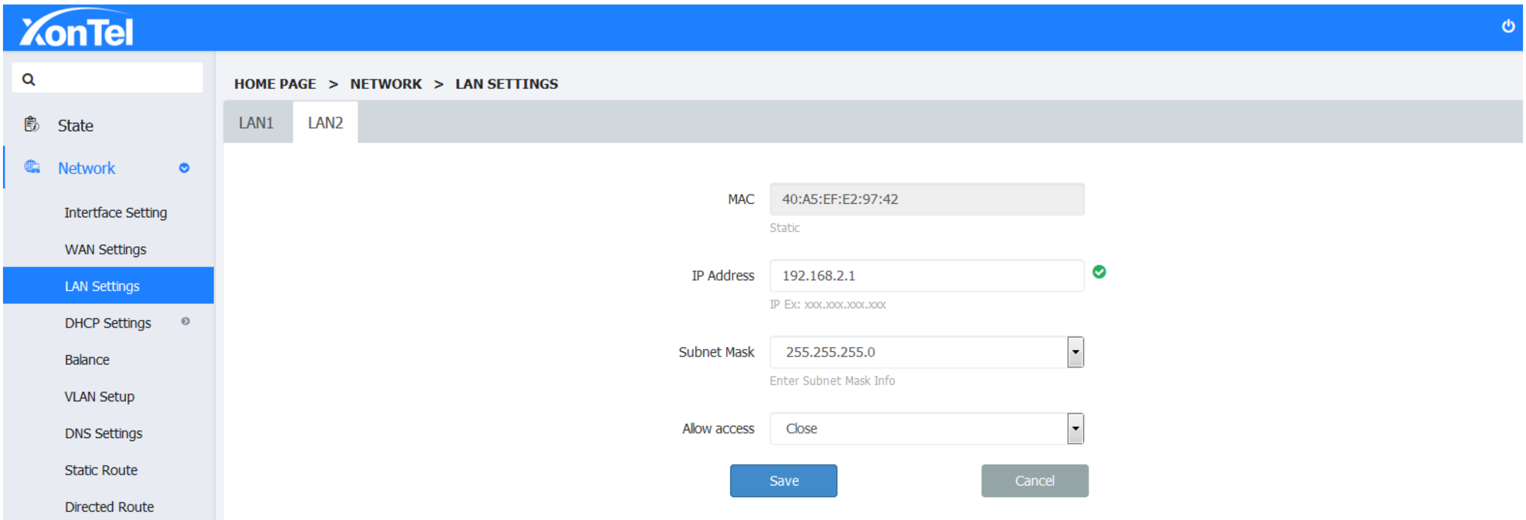
No.	Designate	Interface	Action
1	LAN1	eth0.5 eth0.3	✎ 🗑
2	LAN2	eth0.4	✎ 🗑

Free Interface

No.	Interface

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

5. **Click “LAN Settings” to set up the LAN2’s IP Address and Subnet Mask parameter.**



MAC 40:A5:EF:E2:97:42
Static

IP Address 192.168.2.1 ✓
IP Ex: xxx.xxx.xxx.xxx

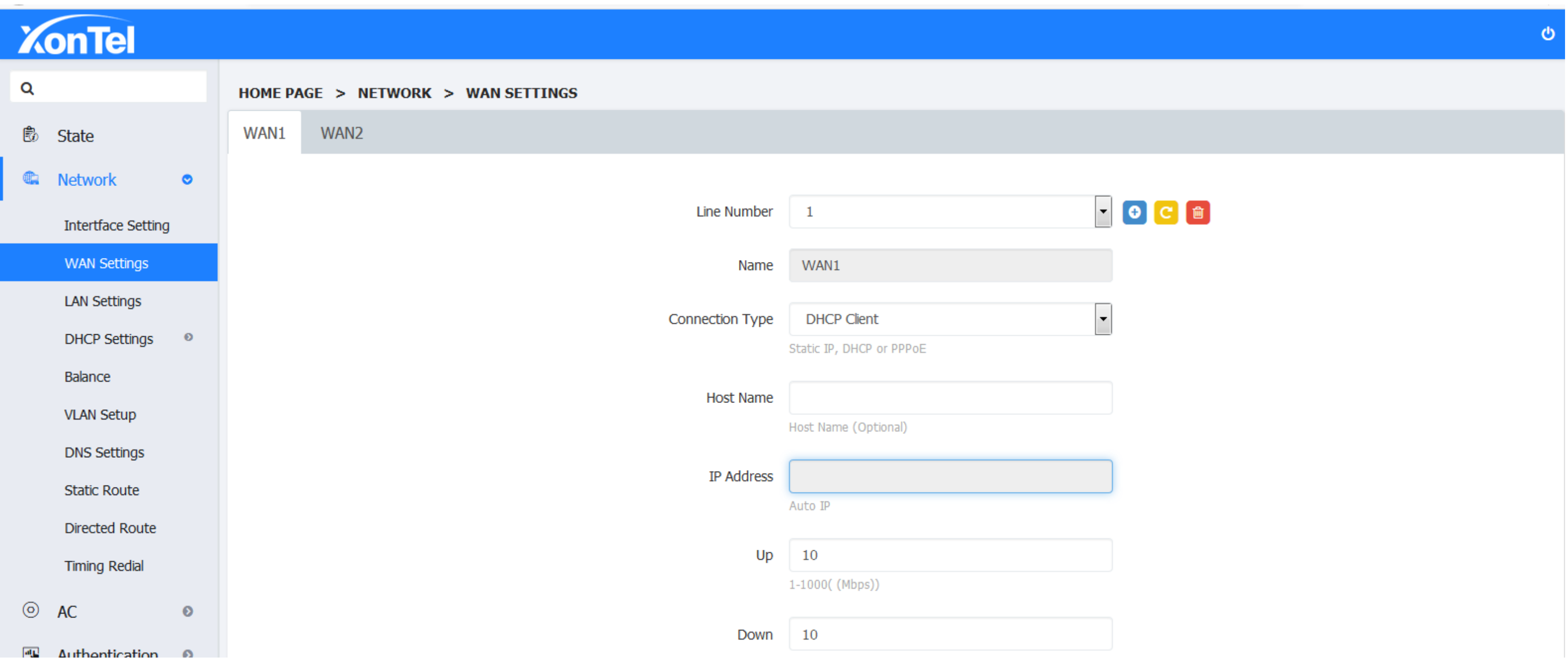
Subnet Mask 255.255.255.0
Enter Subnet Mask Info

Allow access Close

3.2 WAN Settings

In "WAN Settings" you can set up WAN Interface as DHCP Client, Static IP, PPPoE in connection types, it supports Clone MAC address.

1. **DHCP: If the WAN Port achieve the IP automatically by the DHCP, you can use this connection type.**



Line Number: 1

Name: WAN1

Connection Type: DHCP Client
Static IP, DHCP or PPPoE

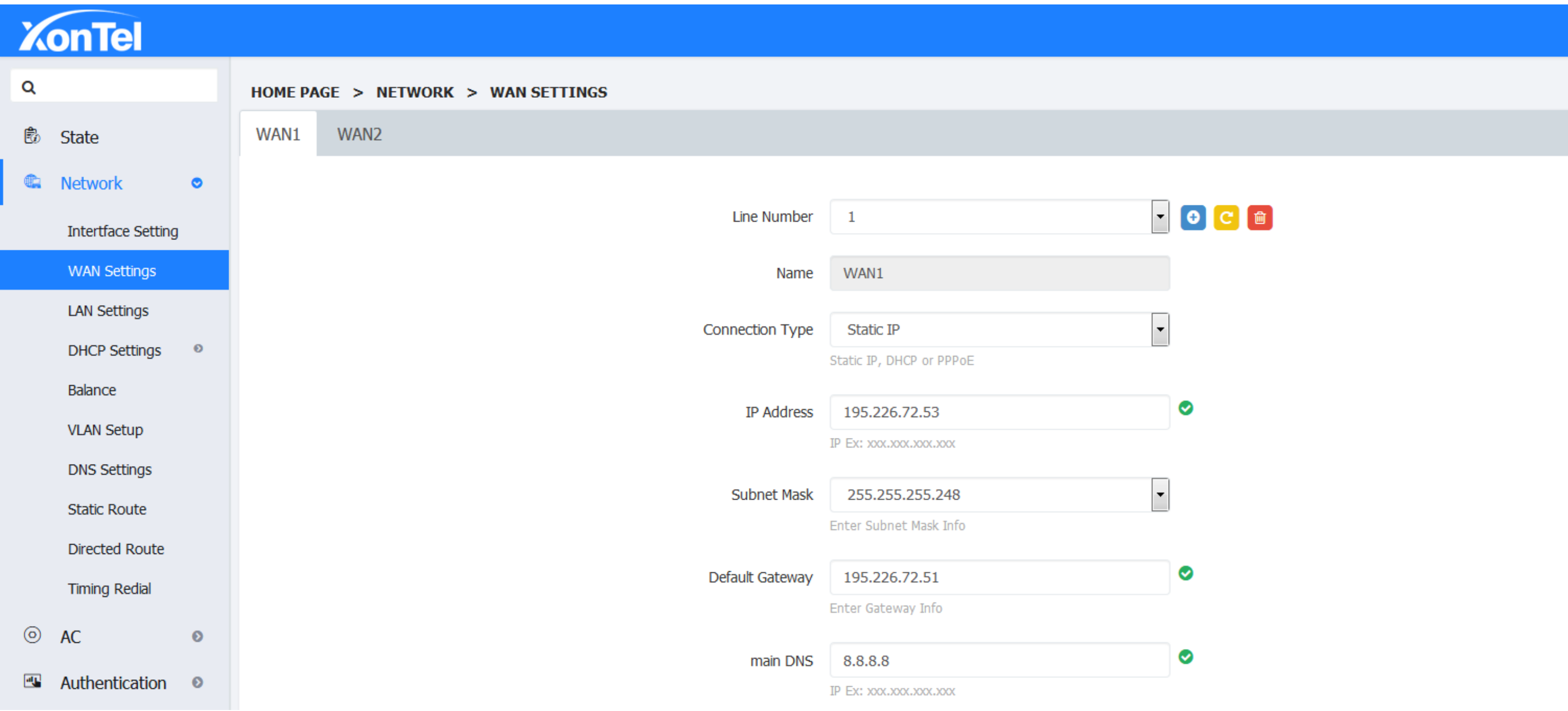
Host Name:
Host Name (Optional)

IP Address:
Auto IP

Up: 10
1-1000((Mbps))

Down: 10

2. **Static IP: Configure the Fixed IP, Subnet Mask, Default Gateway and DNS of the service.**



Line Number: 1

Name: WAN1

Connection Type: Static IP
Static IP, DHCP or PPPoE

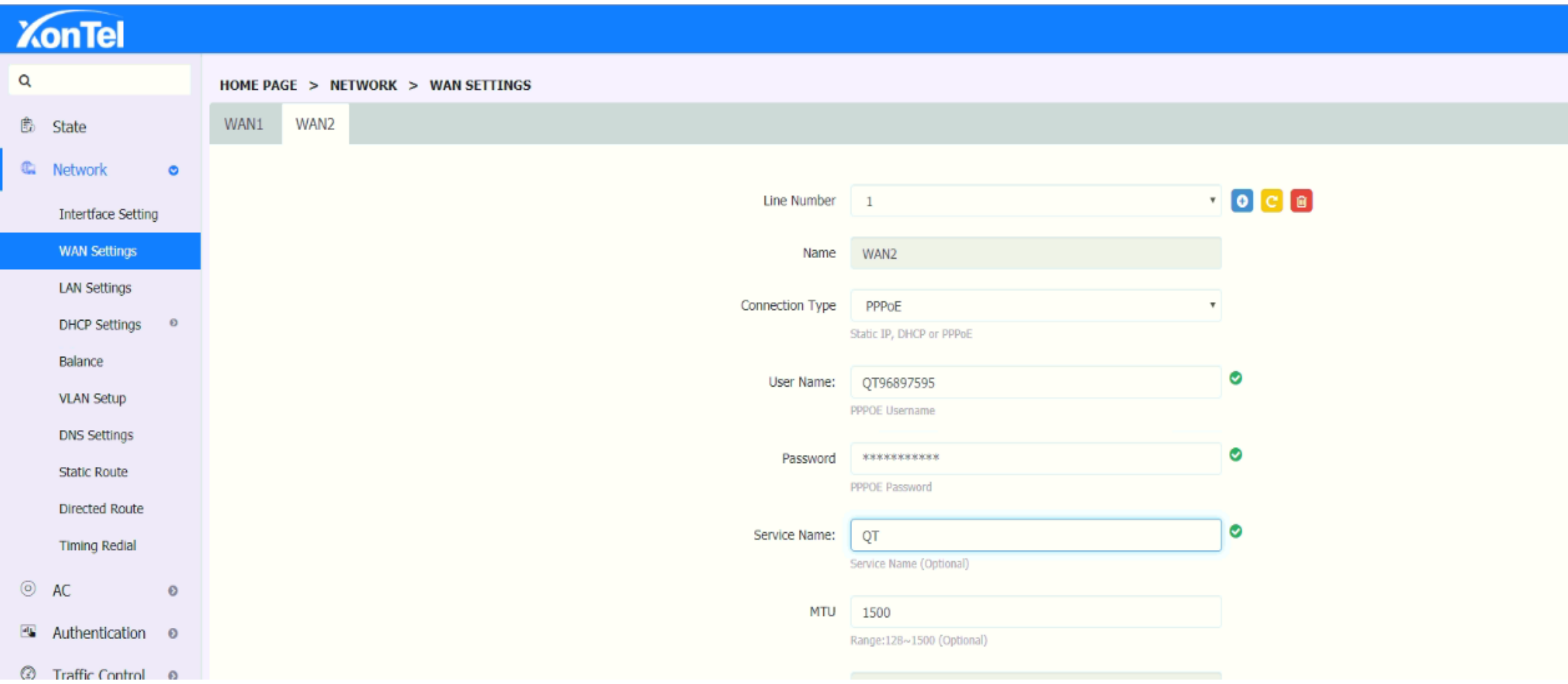
IP Address: 195.226.72.53 ✓
IP Ex: xxx.xxx.xxx.xxx

Subnet Mask: 255.255.255.248
Enter Subnet Mask Info

Default Gateway: 195.226.72.51 ✓
Enter Gateway Info

main DNS: 8.8.8.8 ✓
IP Ex: xxx.xxx.xxx.xxx

3. **PPPoE: If choose this connection type, fill in the related User Name and Password of the service, the state will show connected after success authentication.**



HOME PAGE > NETWORK > WAN SETTINGS

Line Number: 1

Name: WAN2

Connection Type: PPPoE (Static IP, DHCP or PPPoE)

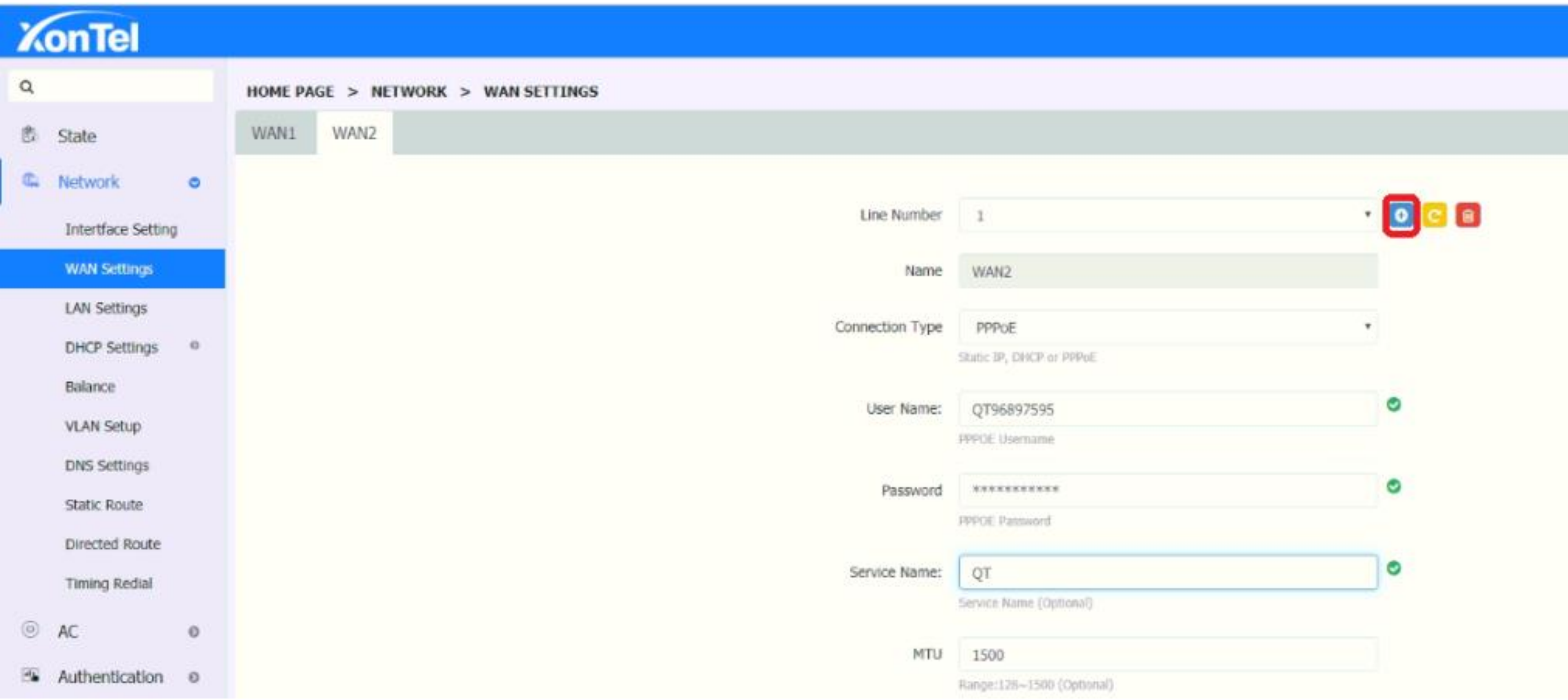
User Name: QT96897595 (PPPOE Username)

Password: *********** (PPPOE Password)

Service Name: QT (Service Name (Optional))

MTU: 1500 (Range:128~1500 (Optional))

4. Click "+" to add multiple network connections on the same interface.



HOME PAGE > NETWORK > WAN SETTINGS

Line Number: 1

Name: WAN2

Connection Type: PPPoE (Static IP, DHCP or PPPoE)

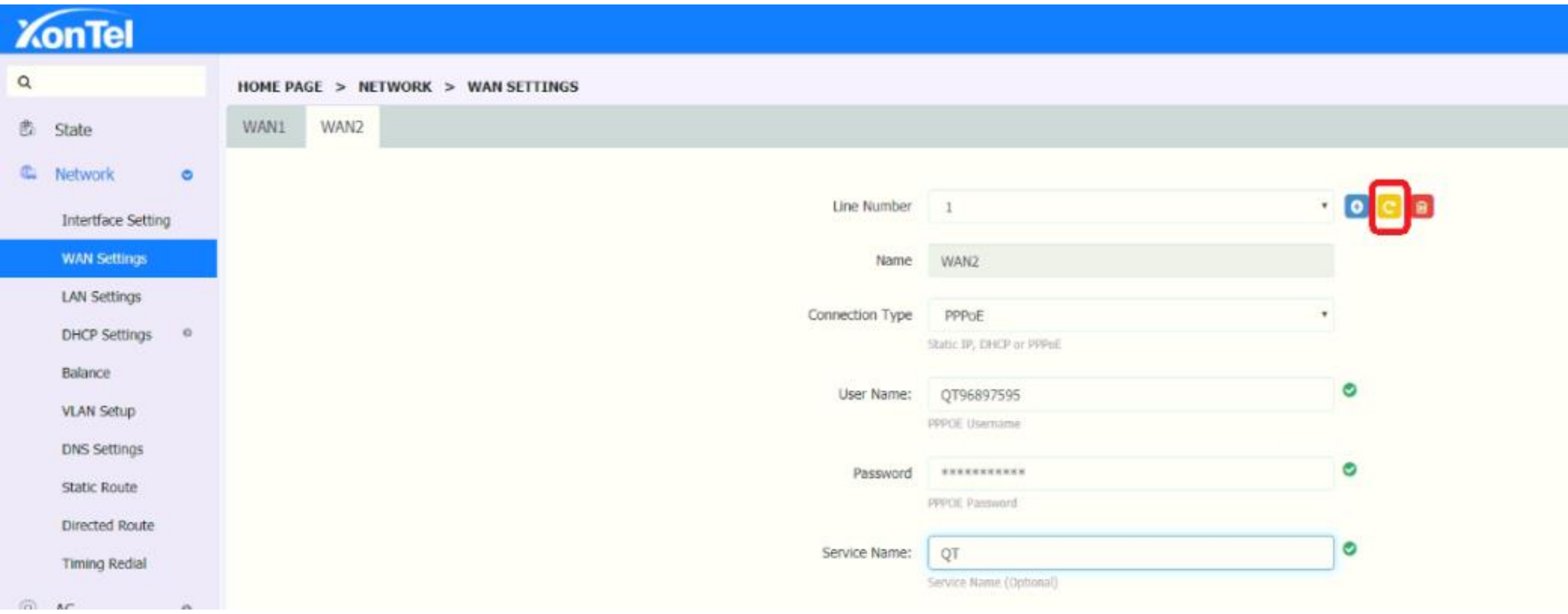
User Name: QT96897595 (PPPOE Username)

Password: *********** (PPPOE Password)

Service Name: QT (Service Name (Optional))

MTU: 1500 (Range:128~1500 (Optional))

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



HOME PAGE > NETWORK > WAN SETTINGS

WAN1 WAN2

Line Number: 1

Name: WAN2

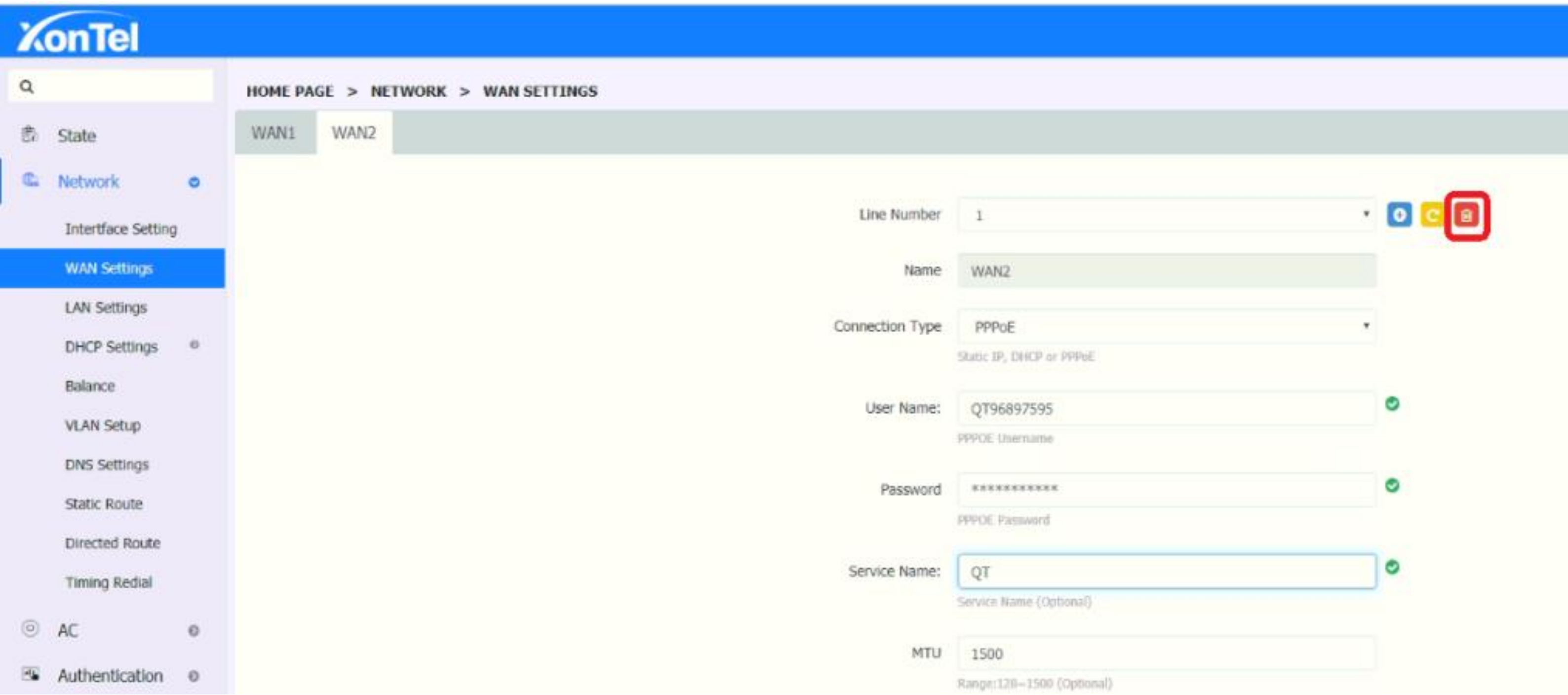
Connection Type: PPPoE
Static IP, DHCP or PPPoE

User Name: QT96897595
PPPOE Username

Password: ***********
PPPOE Password

Service Name: QT
Service Name (Optional)

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



HOME PAGE > NETWORK > WAN SETTINGS

WAN1 WAN2

Line Number: 1

Name: WAN2

Connection Type: PPPoE
Static IP, DHCP or PPPoE

User Name: QT96897595
PPPOE Username

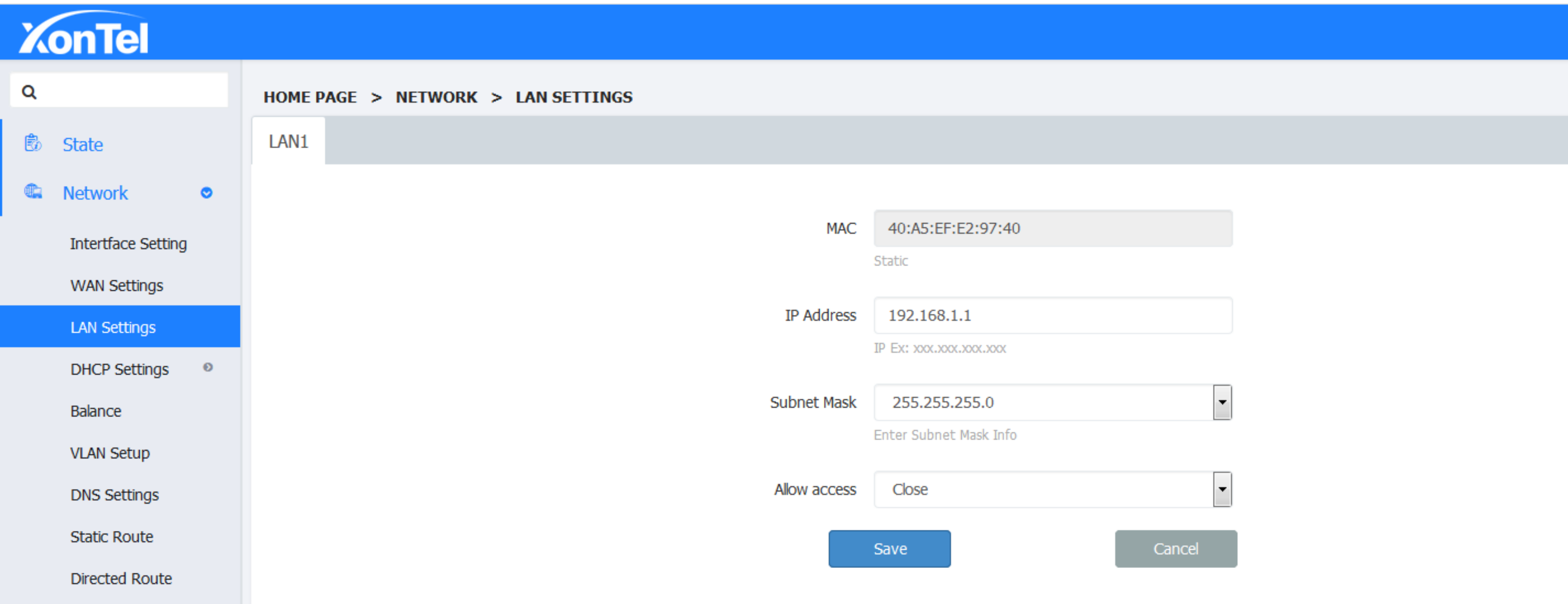
Password: ***********
PPPOE Password

Service Name: QT
Service Name (Optional)

MTU: 1500
Range:128~1500 (Optional)

3.3 Local Network Settings

You can manually set each LAN Interface's IP Address and Subnet mask. The default IP address is 192.168.1.1



HOME PAGE > NETWORK > LAN SETTINGS

MAC: 40:A5:EF:E2:97:40
Static

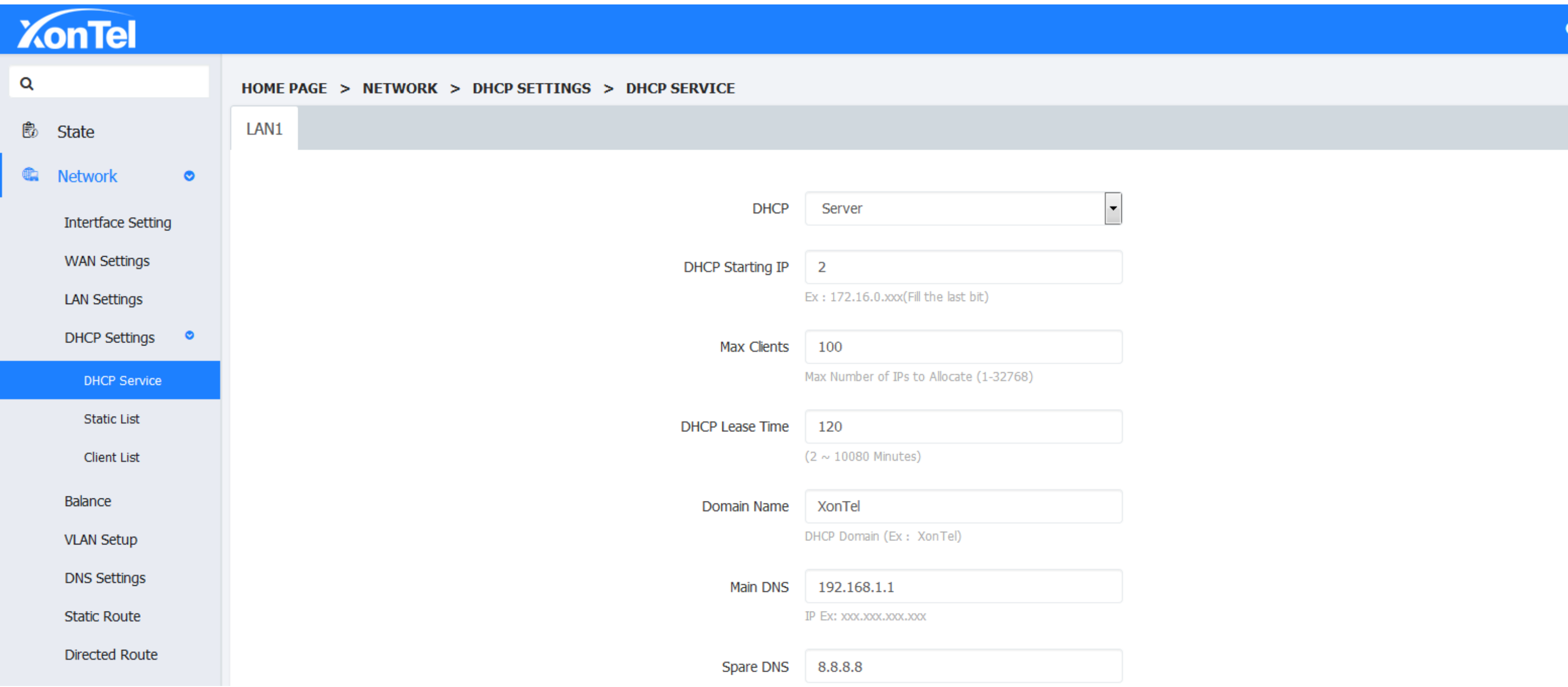
IP Address: 192.168.1.1
IP Ex: xxx.xxx.xxx.xxx

Subnet Mask: 255.255.255.0
Enter Subnet Mask Info

Allow access: Close

3.4 DHCP Settings

DHCP Service: Here you can set up DHCP as Server, start IP Address number, DHCP Lease Time, Domain Name, Main DNS and Backup DNS. You can also disable 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)



HOME PAGE > NETWORK > DHCP SETTINGS > DHCP SERVICE

DHCP: Server

DHCP Starting IP: 2
Ex : 172.16.0.xxx(Fill the last bit)

Max Clients: 100
Max Number of IPs to Allocate (1-32768)

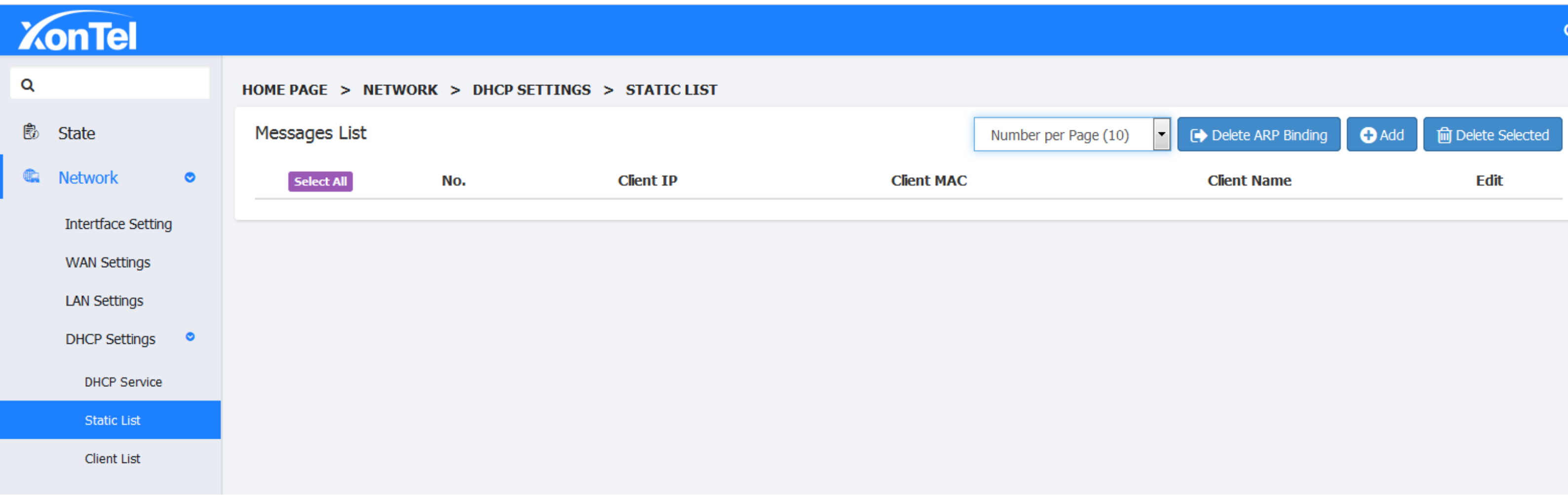
DHCP Lease Time: 120
(2 ~ 10080 Minutes)

Domain Name: XonTel
DHCP Domain (Ex : XonTel)

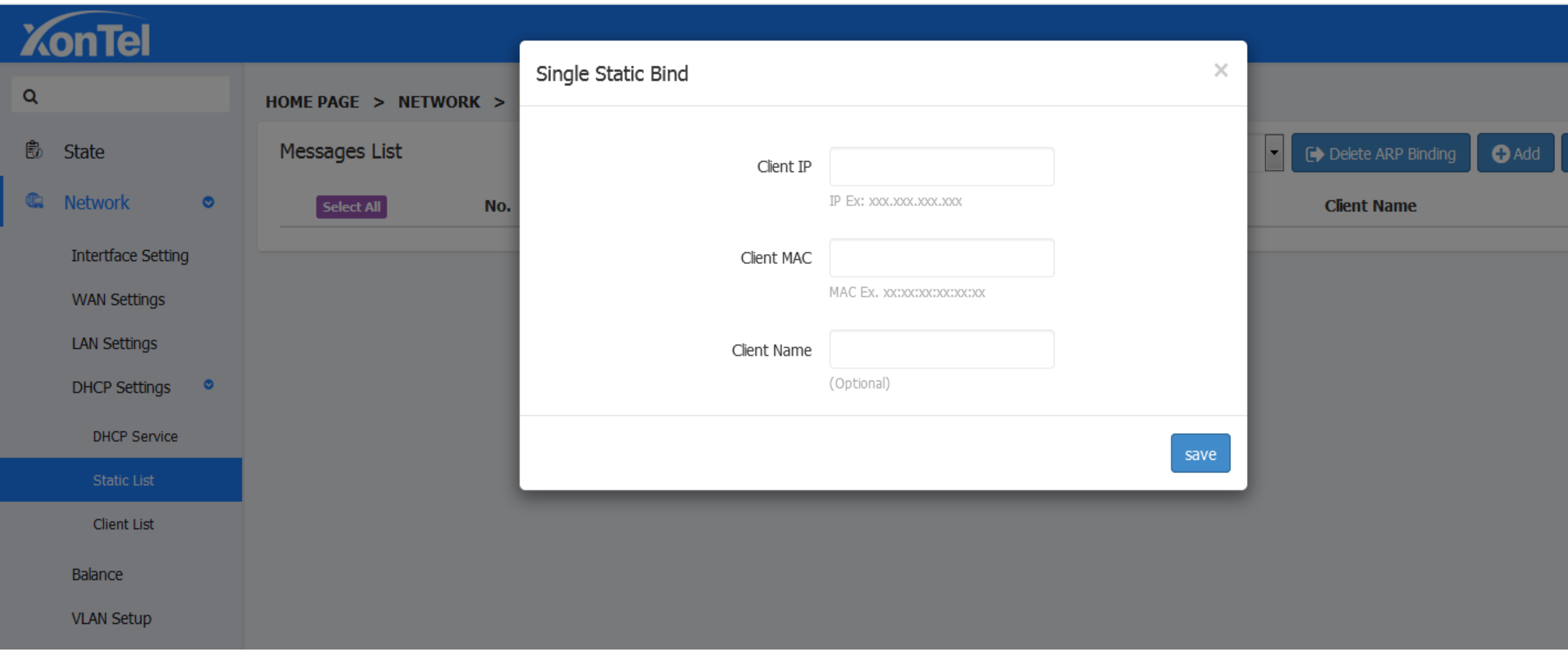
Main DNS: 192.168.1.1
IP Ex: xxx.xxx.xxx.xxx

Spare DNS: 8.8.8.8

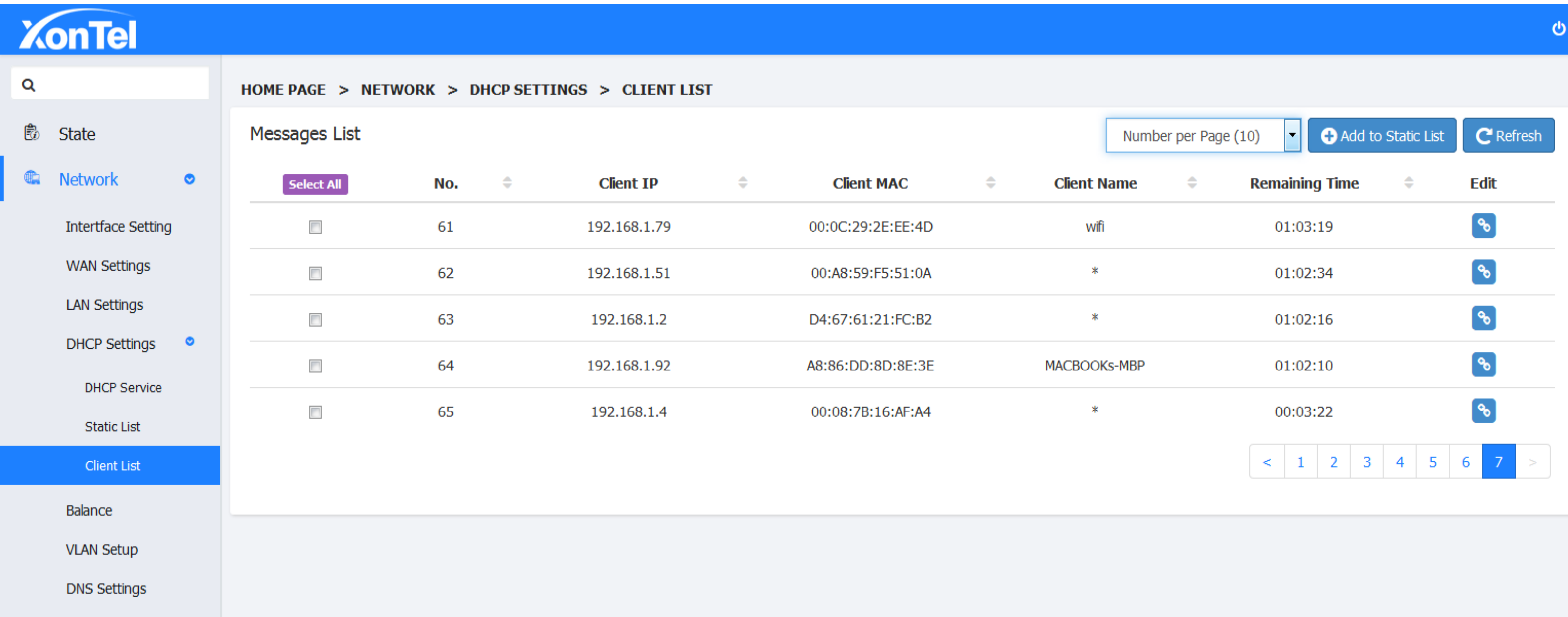
Static List: The DHCP service can always assign the same IP address to a specific computer on your LAN. To be more specific, the DHCP service assigns this static IP to a unique MAC address assigned to each NIC on your LAN. You can add it in this place. Here you can install the compatible ARP binding information and also can add the PC or mobile device IP address to static allocation, then those devices will get the fixed IP.



To add single static bind, click "Add" button in the static list and set up the Client IP and MAC.



Client List: Here System will display the DHCP allocated CLIENT IP, CLIENT MAC, CLIENT NAME which are connected with the device. You can add any particular client IP to the static list by clicking "Add to Static List" button.



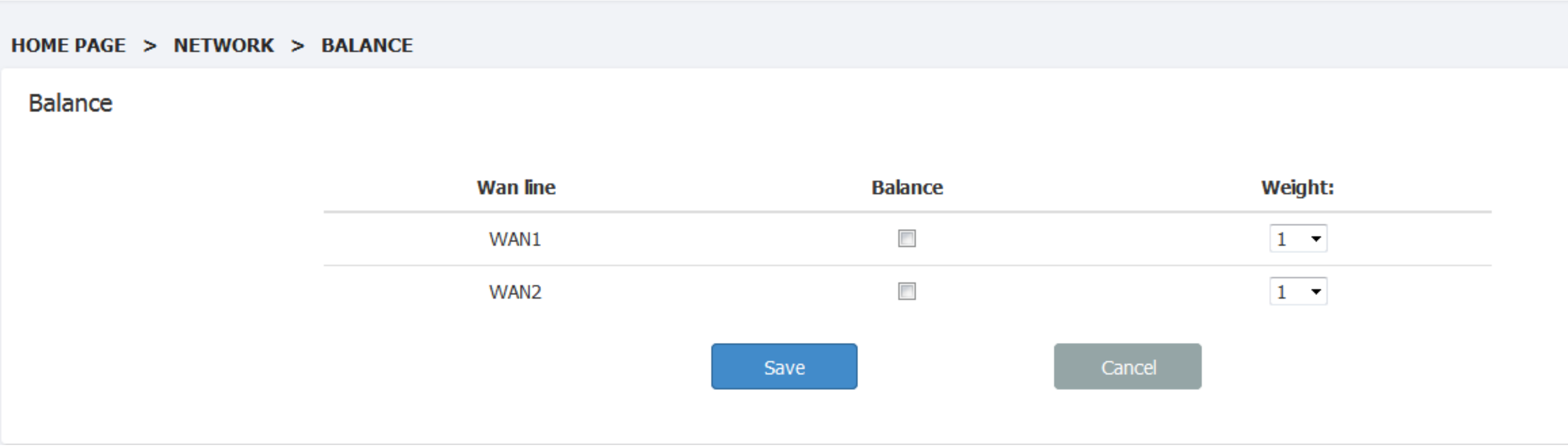
HOME PAGE > NETWORK > DHCP SETTINGS > CLIENT LIST

Messages List

Select All	No.	Client IP	Client MAC	Client Name	Remaining Time	Edit
□	61	192.168.1.79	00:0C:29:2E:EE:4D	wifi	01:03:19	
□	62	192.168.1.51	00:A8:59:F5:51:0A	*	01:02:34	
□	63	192.168.1.2	D4:67:61:21:FC:B2	*	01:02:16	
□	64	192.168.1.92	A8:86:DD:8D:8E:3E	MACBOOKs-MBP	01:02:10	
□	65	192.168.1.4	00:08:7B:16:AF:A4	*	00:03:22	

3.5 Balance

Balance: When the multiple ISP lines connected, choose balance strategy, choose corresponding rate as per their speed. The same or different ISP line will allocate the bandwidth by balance strategy.

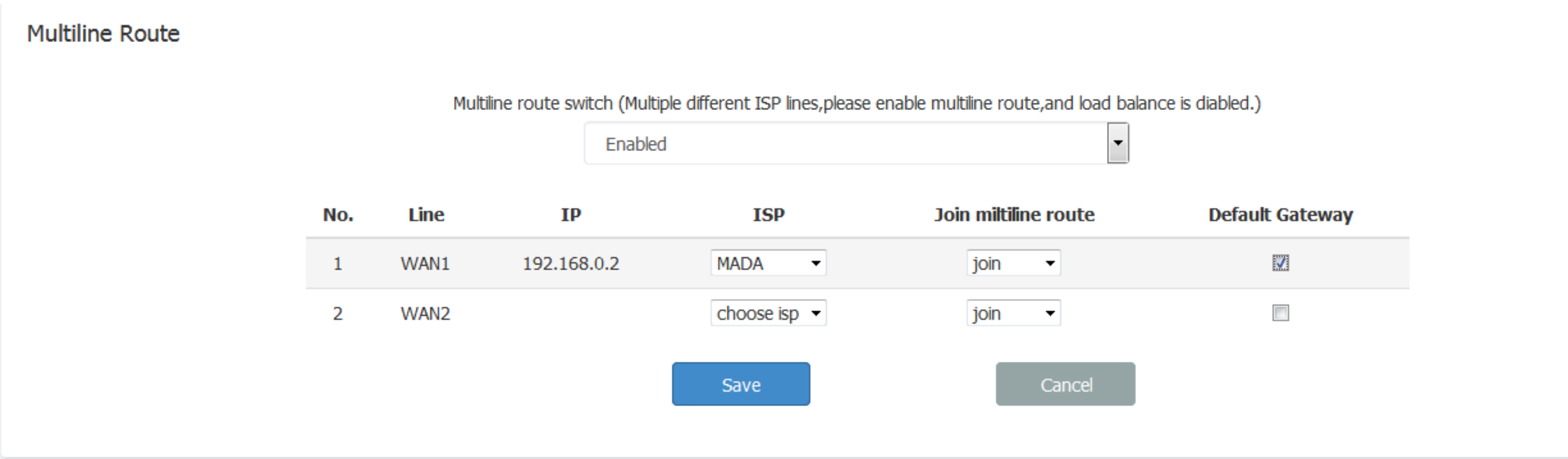


HOME PAGE > NETWORK > BALANCE

Balance

Wan line	Balance	Weight:
WAN1	□	1
WAN2	□	1

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



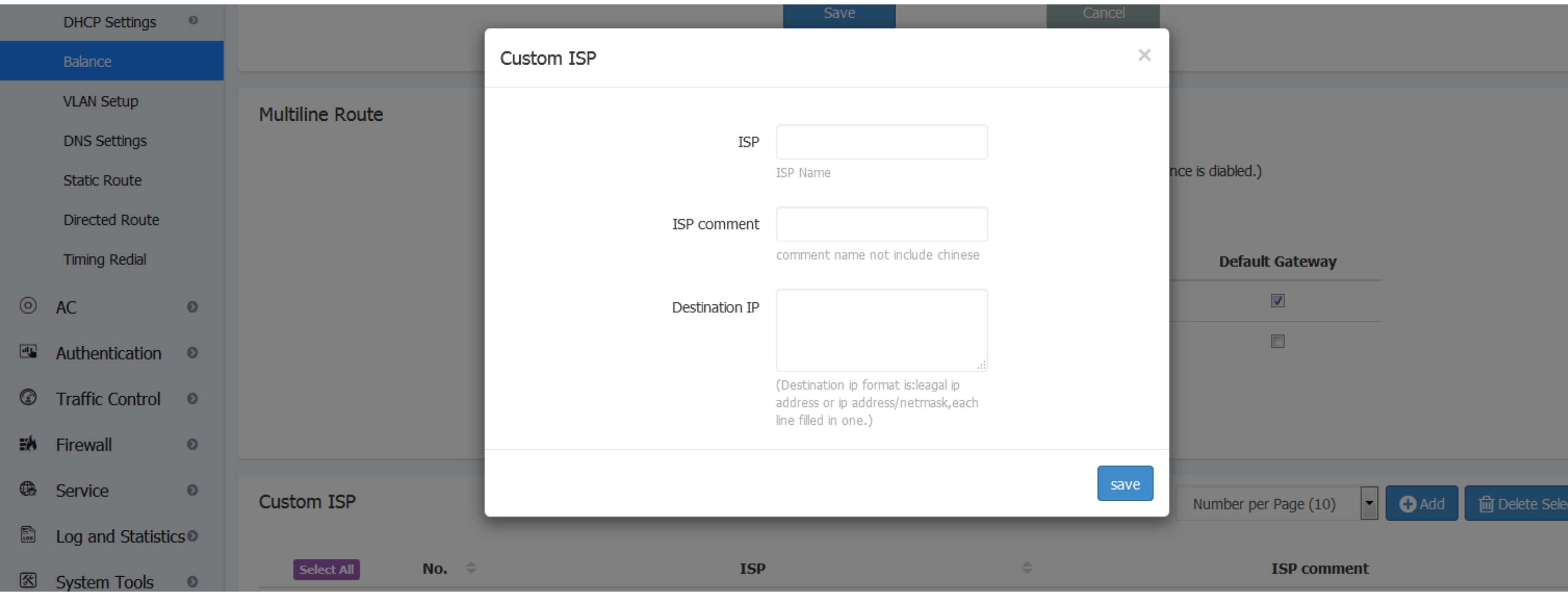
Multiline Route

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

Enabled

No.	Line	IP	ISP	Join miltiline route	Default Gateway
1	WAN1	192.168.0.2	MADA	join	☑
2	WAN2		choose isp	join	□

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

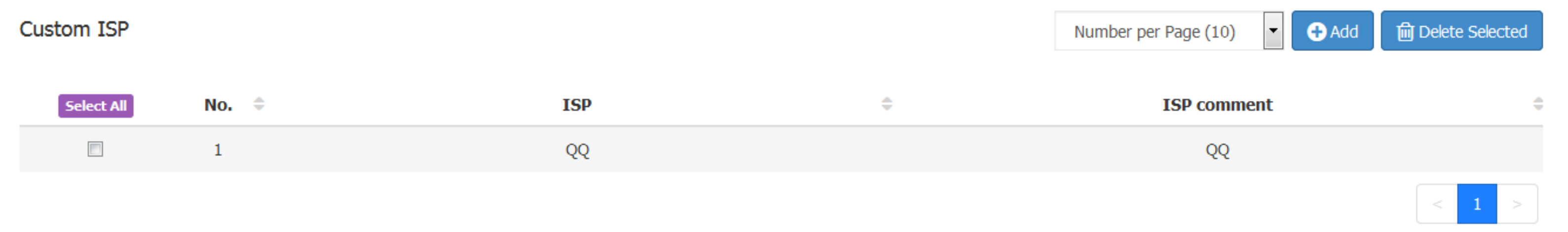


Custom ISP

ISP: ISP Name

ISP comment: comment name not include chinese

Destination IP: (Destination ip format is:leagal ip address or ip address/netmask,each line filled in one.)



Custom ISP

Select All	No.	ISP	ISP comment
□	1	QQ	QQ

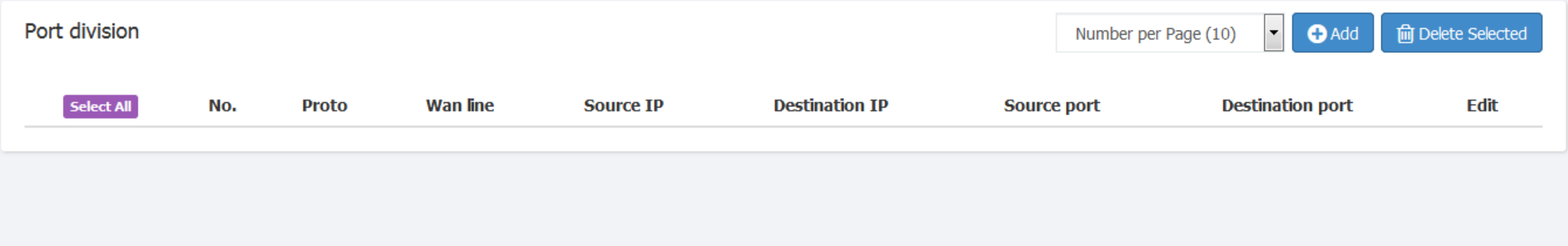
Port division:

1. **Traffic will go through the specific exit when the local network appointed IP wants to access some internet ports.**

Choose the appointed wan line you need, and enter the appointed IP in SOURCE IP. Enter your DESTINATION PORT.

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

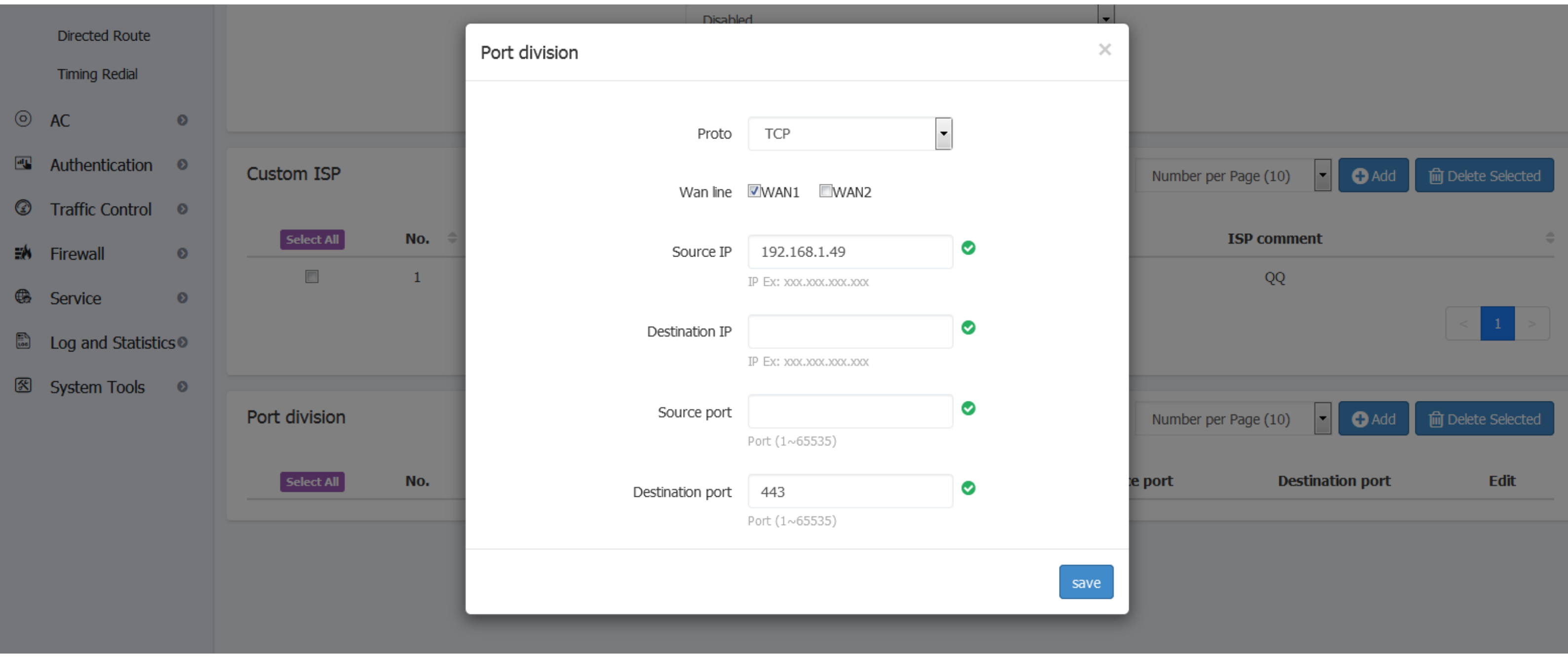
Example: Let 443 shutting into WAN1.



Port division

Number per Page (10) | Add | Delete Selected

Select All	No.	Proto	Wan line	Source IP	Destination IP	Source port	Destination port	Edit



Port division

Proto: TCP

Wan line: ☑WAN1 □WAN2

Source IP: 192.168.1.49
IP Ex: xxx.xxx.xxx.xxx

Destination IP:
IP Ex: xxx.xxx.xxx.xxx

Source port:
Port (1~65535)

Destination port: 443
Port (1~65535)

save

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

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

3.6 VLAN Settings

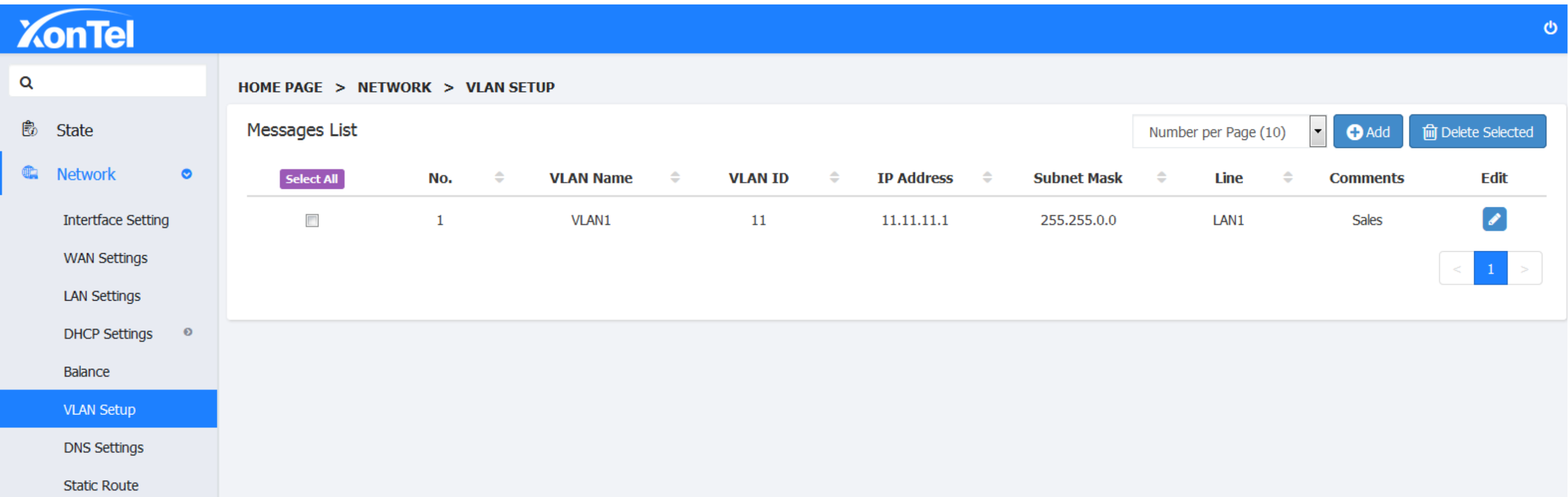
A VLAN is a group of devices on one or more LAN that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

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.



HOME PAGE > NETWORK > VLAN SETUP

Messages List

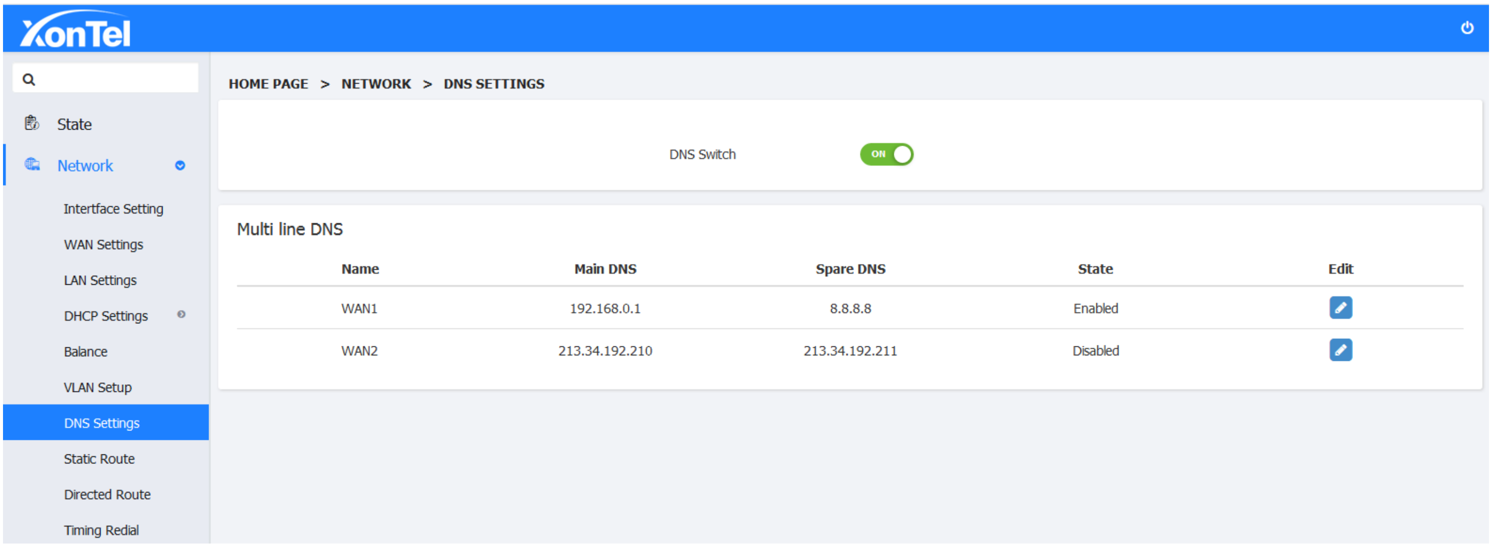
Select All	No.	VLAN Name	VLAN ID	IP Address	Subnet Mask	Line	Comments	Edit
□	1	VLAN1	11	11.11.11.1	255.255.0.0	LAN1	Sales	

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, or Domain Name System, is the mechanism by which a network device resolves a name like www.example.com to an IP address such as 198.51.100.25, or vice versa. Clients must have functional DNS if they are to reach other devices such as servers using their hostnames or fully qualified domain names. At the Static IP Mode, need to manual set up Main DNS and Secondary DNS. If you don’t know your local DNS address, you can contact with your Internet Service Provider.

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



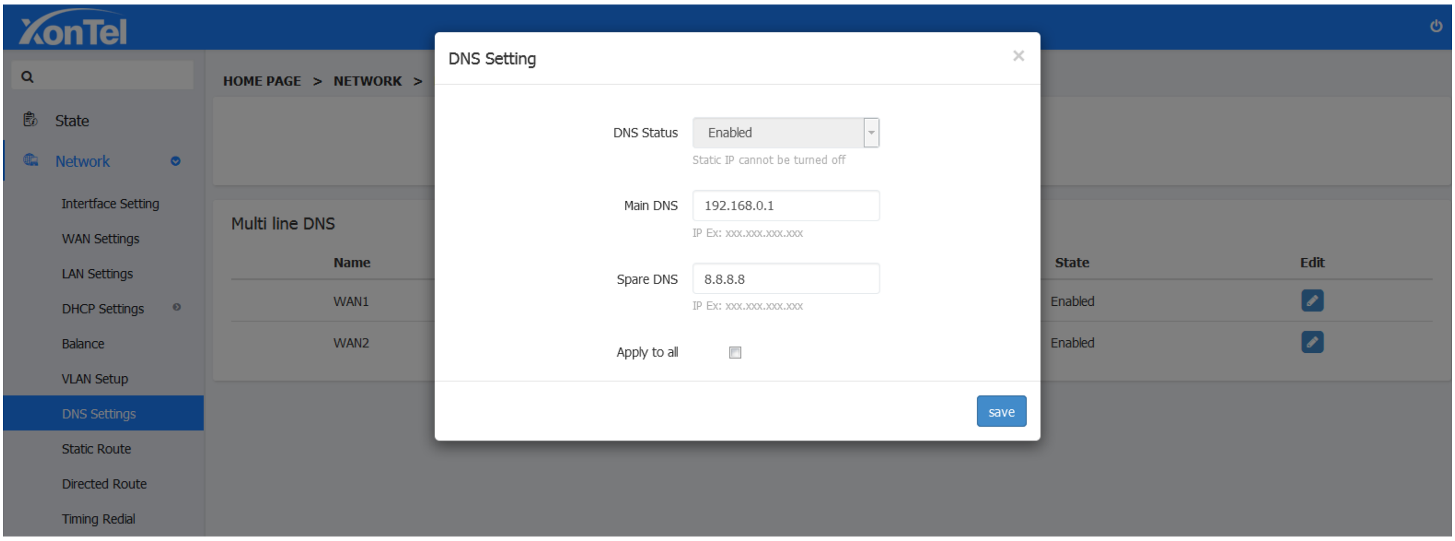
HOME PAGE > NETWORK > DNS SETTINGS

DNS Switch: ON

Multi line DNS

Name	Main DNS	Spare DNS	State	Edit
WAN1	192.168.0.1	8.8.8.8	Enabled	✎
WAN2	213.34.192.210	213.34.192.211	Disabled	✎

2. Select the need to set the DNS line, click the Edit button, you can select DNS Switch as On or Off, enter the main DNS or secondary DNS, click Save.



HOME PAGE > NETWORK >

DNS Setting

DNS Status: Enabled
Static IP cannot be turned off

Main DNS: 192.168.0.1
IP Ex: xxx.xxx.xxx.xxx

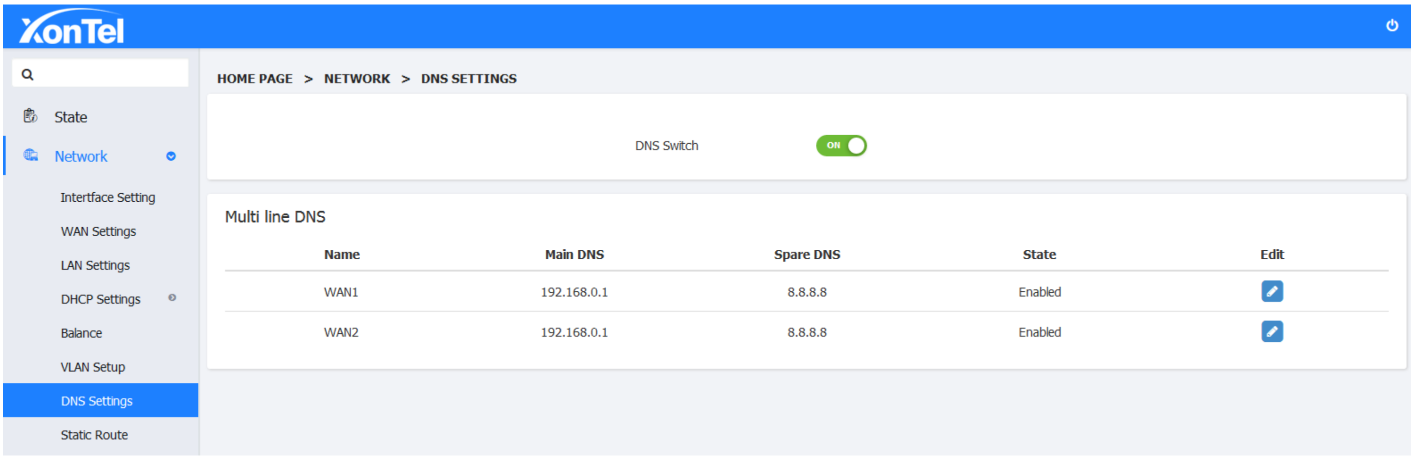
Spare DNS: 8.8.8.8
IP Ex: xxx.xxx.xxx.xxx

Apply to all ☐

Multi line DNS

Name	State	Edit
WAN1	Enabled	✎
WAN2	Enabled	✎

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



HOME PAGE > NETWORK > DNS SETTINGS

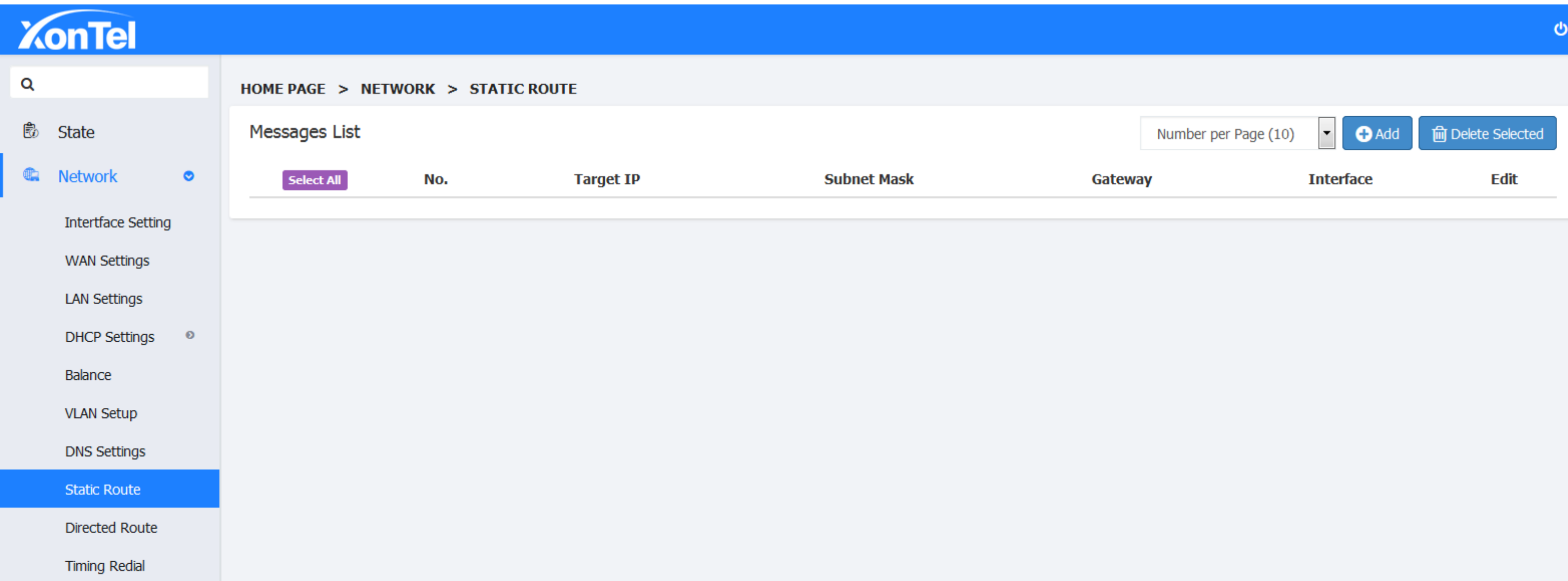
DNS Switch: ON

Multi line DNS

Name	Main DNS	Spare DNS	State	Edit
WAN1	192.168.0.1	8.8.8.8	Enabled	✎
WAN2	192.168.0.1	8.8.8.8	Enabled	✎

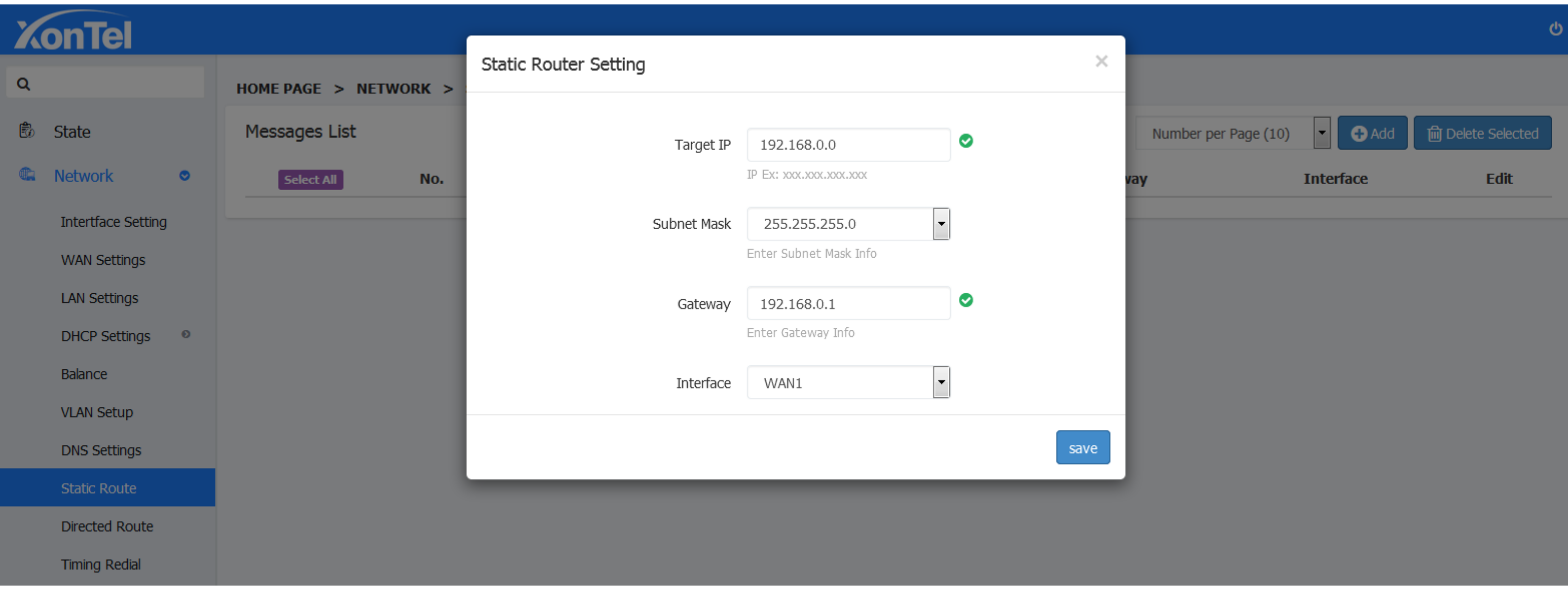
3.8 Static Route

Static Route is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.



Messages List

Select All	No.	Target IP	Subnet Mask	Gateway	Interface	Edit



Static Router Setting

Target IP: 192.168.0.0
IP Ex: xxx.xxx.xxx.xxx

Subnet Mask: 255.255.255.0
Enter Subnet Mask Info

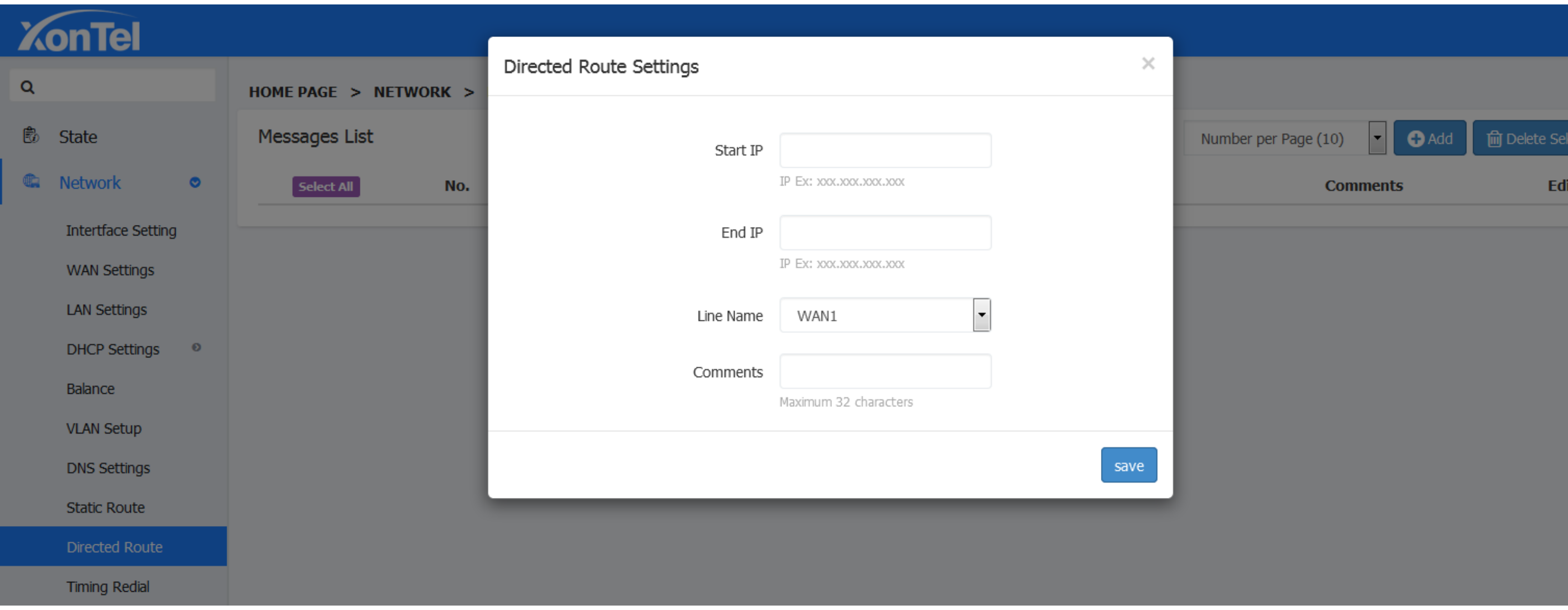
Gateway: 192.168.0.1
Enter Gateway Info

Interface: WAN1

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.

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



Directed Route Settings

Start IP
IP Ex: xxx.xxx.xxx.xxx

End IP
IP Ex: xxx.xxx.xxx.xxx

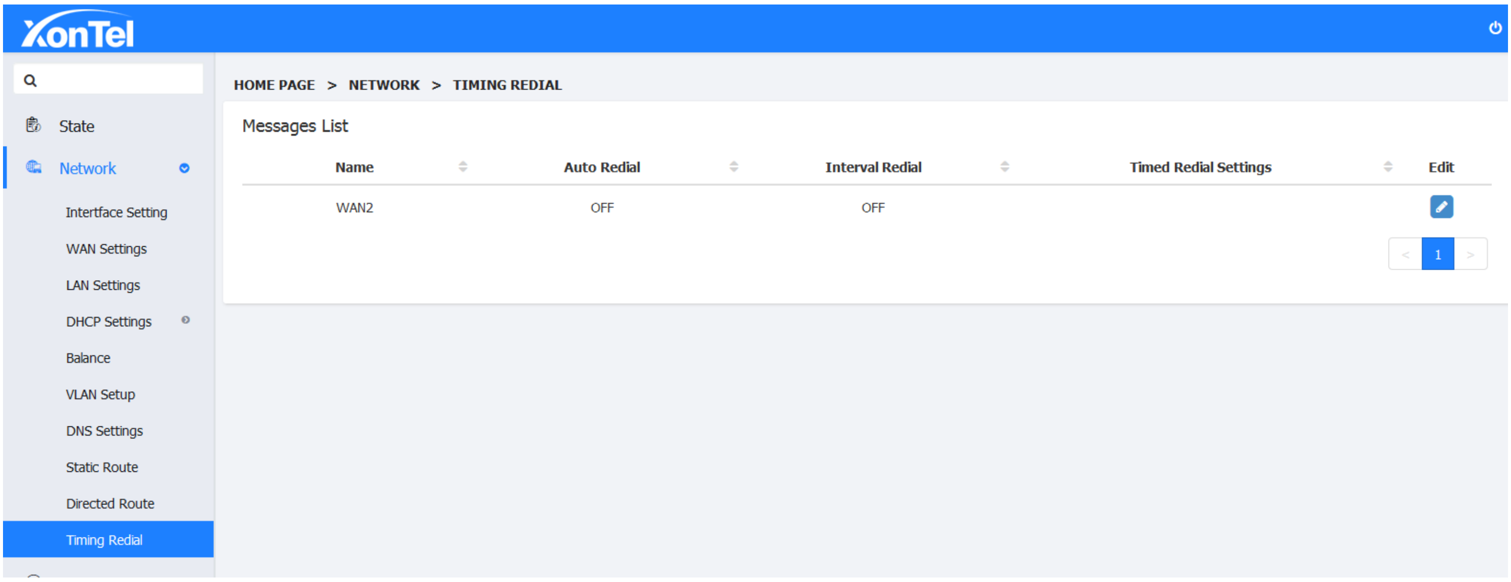
Line Name: WAN1

Comments
Maximum 32 characters

3.10 Timing Redial

Auto Redial: Set a specific time or a specific interval to allow automatic redialing of a WAN line which is DHCP Client or PPPoE.

1. **Click "Network - Timing Redial" to enter the Timing Redial page**

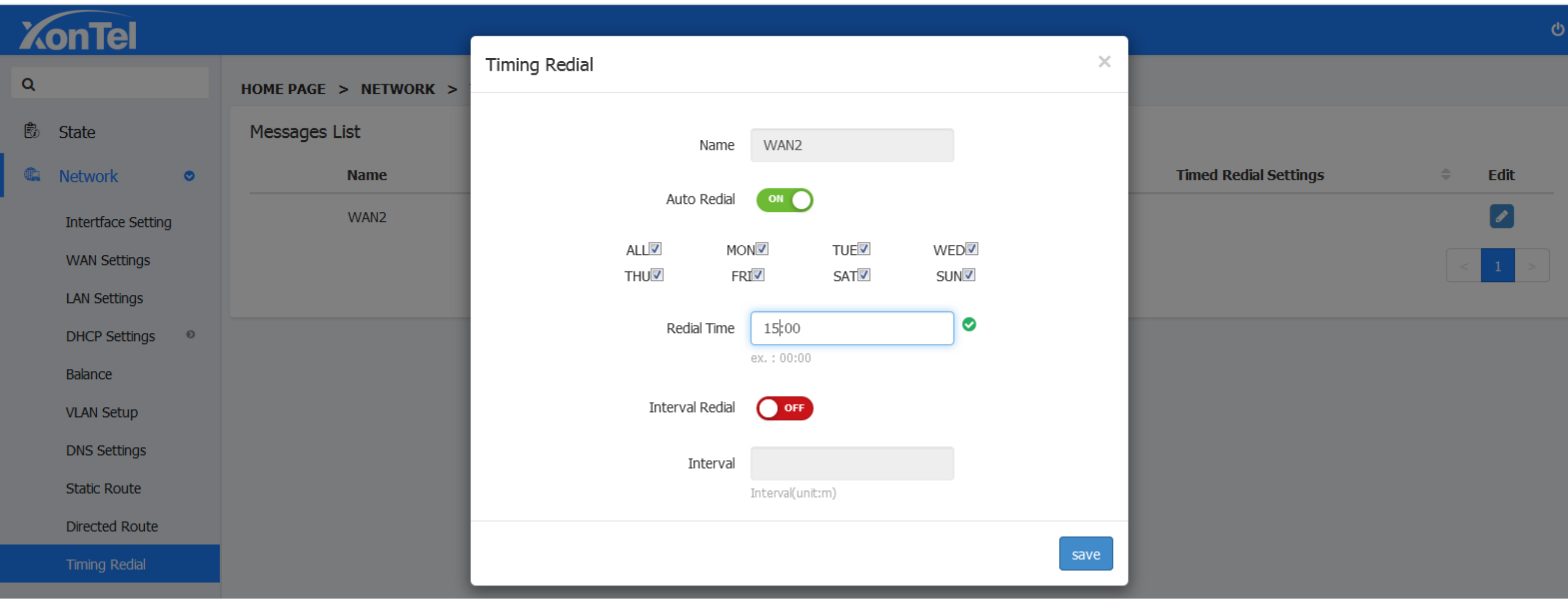


HOME PAGE > NETWORK > TIMING REDIAL

Messages List

Name	Auto Redial	Interval Redial	Timed Redial Settings	Edit
WAN2	OFF	OFF		

2. Click on the Edit 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 WAN2 line automatically redials at 15:00hours every day.



Timing Redial

Name: WAN2

Auto Redial: ON

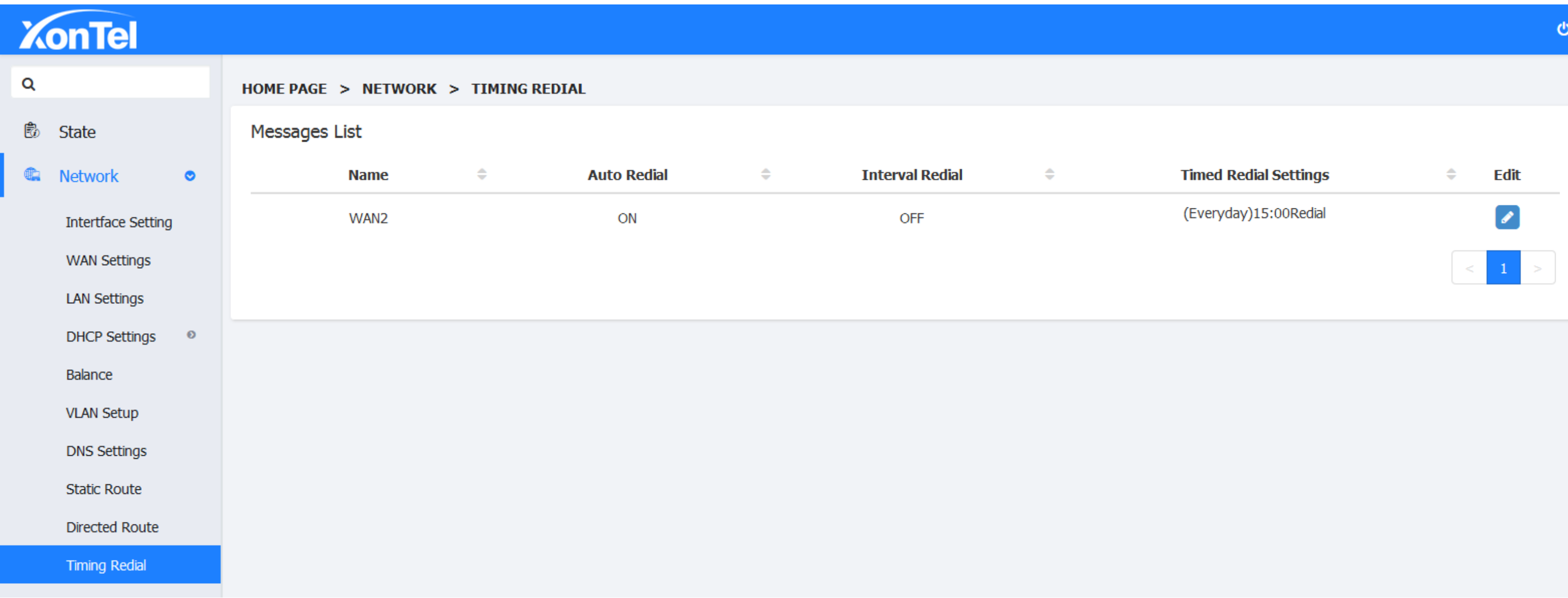
ALL☑ MON☑ TUE☑ WED☑
THU☑ FRI☑ SAT☑ SUN☑

Redial Time: 15:00 ✓
ex. : 00:00

Interval Redial: OFF

Interval:
Interval(unit:m)

save

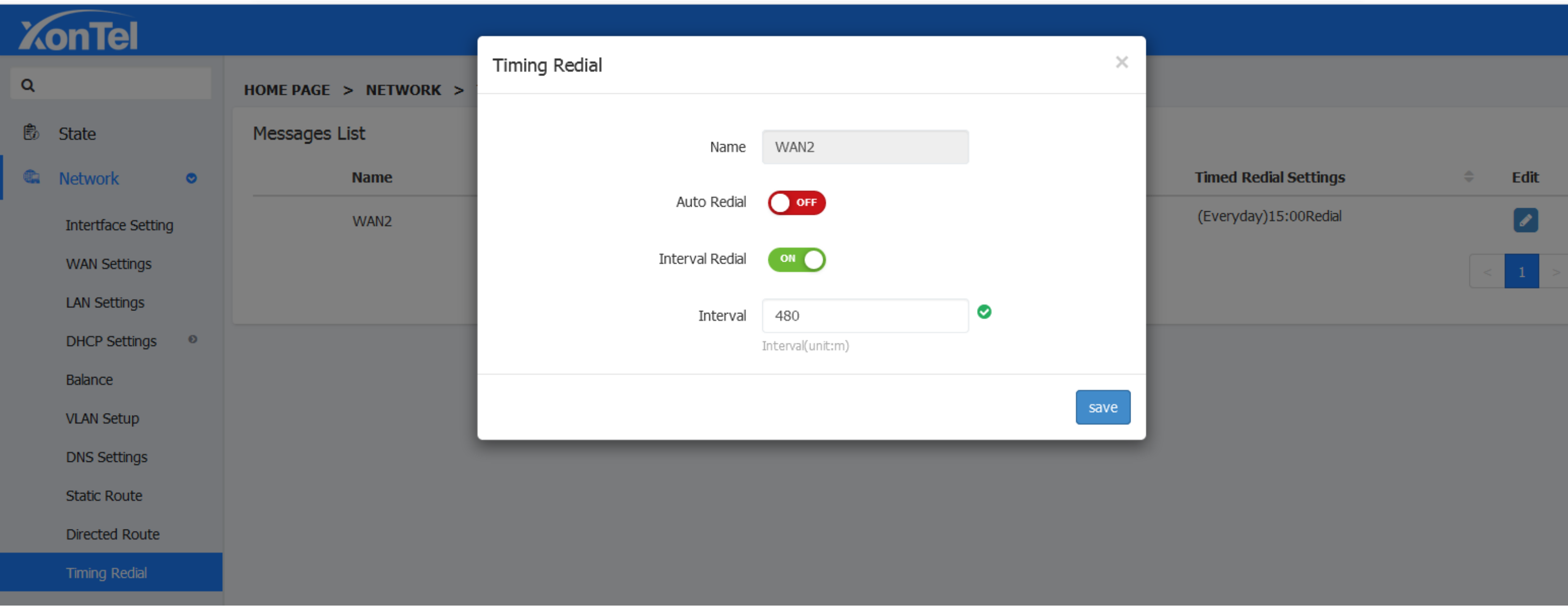


HOME PAGE > NETWORK > TIMING REDIAL

Messages List

Name	Auto Redial	Interval Redial	Timed Redial Settings	Edit
WAN2	ON	OFF	(Everyday)15:00Redial	

3. To perform Interval Redial, Click on Edit button and Turn on Interval Redial, enter the interval restart time, click Save as shown below. After this setting WAN2 line will re-dial every 480 minutes (Every 8 Hours).



Timing Redial

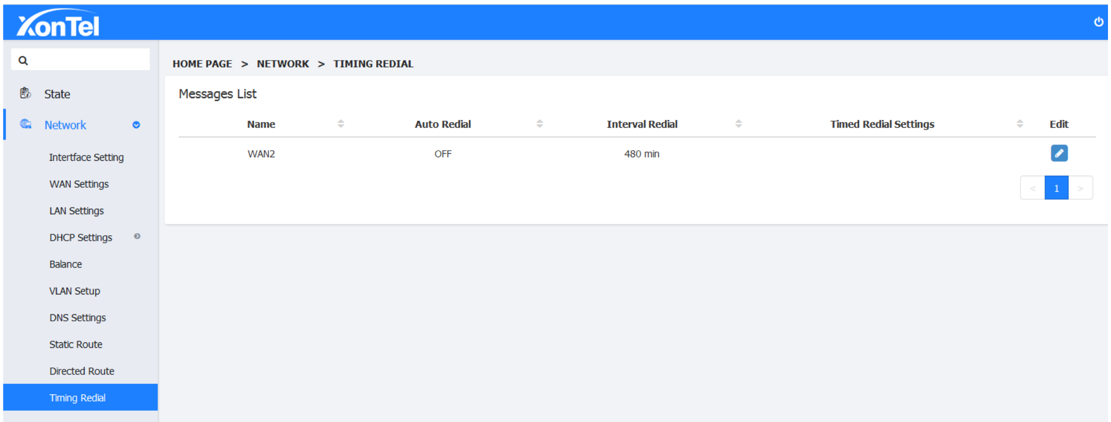
Name: WAN2

Auto Redial: OFF

Interval Redial: ON

Interval: 480

Interval(unit:m)



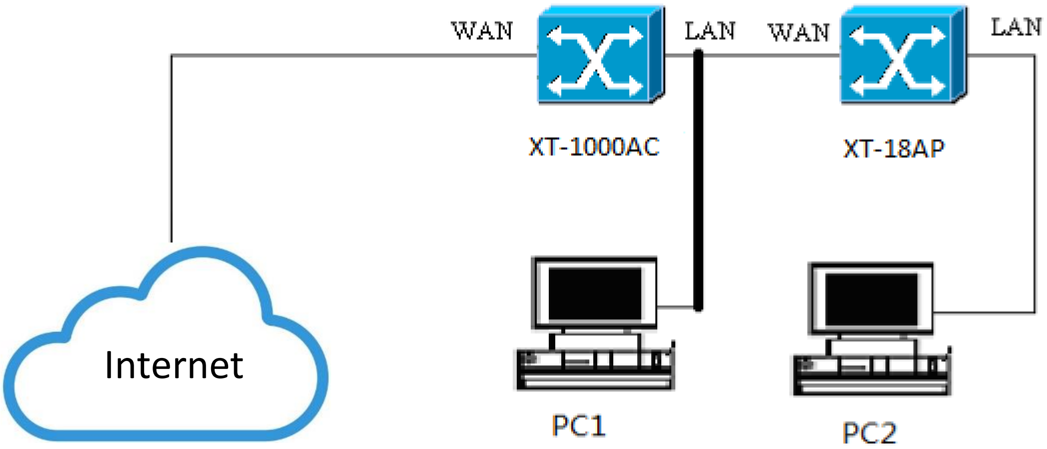
Messages List

Name	Auto Redial	Interval Redial	Timed Redial Settings	Edit
WAN2	OFF	480 min		

4 AC Control

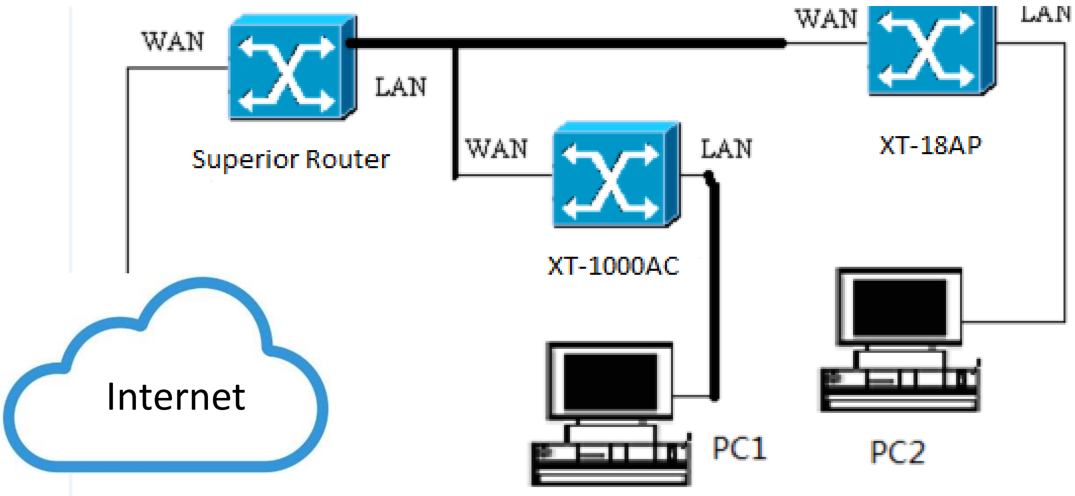
Cascading AC Mode

In Cascading AC mode, the Access Points (XT-18AP) connect with the XT-1000's internal network, and the connection way is XT-1000's LAN port connect with Access Point's WAN port as shown below:



By-Pass AC Mode

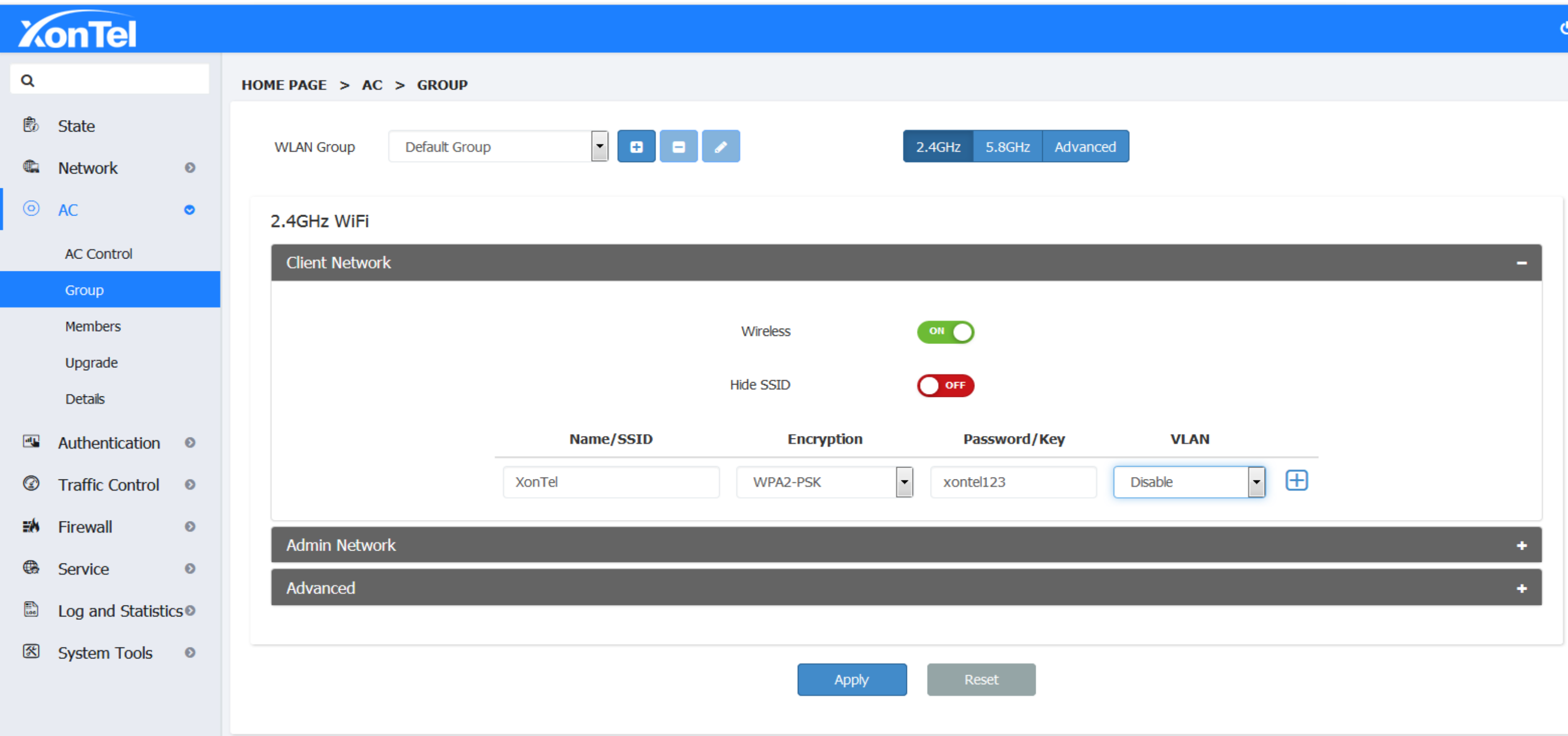
In By-Pass AC Mode Access Points (XT-18AP) and XT-1000AC connects with the same network. The connection way is the Superior Router's LAN port connects with the WAN port of XT-1000AC and XT-18AP. After the XT-1000AC and Xt-18AP consult successfully, you can visit XT-1000AC management page through XT-1000AC's WAN port IP.



4.1 Group

Here you can use the default group (For Mass APs Config) or create a new group, can setup 2.4GHz and 5.8GHz SSID, wireless advanced parameters.

1. Open the XT-1000AC's home page, go into AC Control's "Group" page as below:



WLAN Group: Default Group

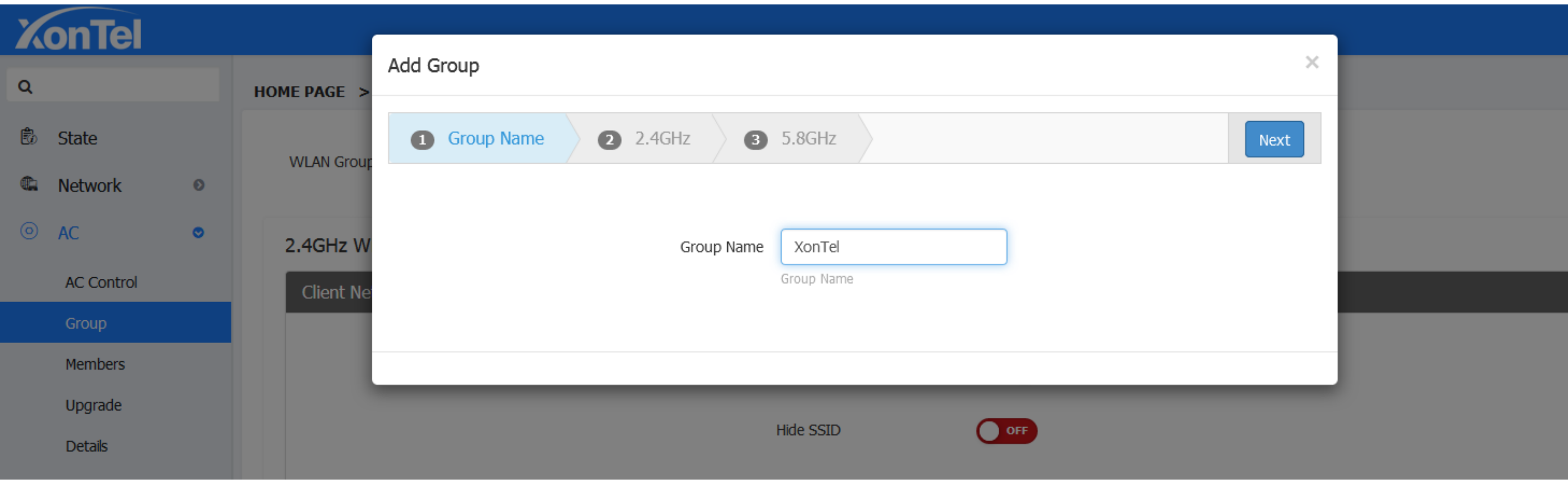
2.4GHz WiFi

Wireless: ON

Hide SSID: OFF

Name/SSID	Encryption	Password/Key	VLAN
XonTel	WPA2-PSK	xontel123	Disable

2. Click "+" button near WLAN Group and go into the add group wizard, Type Group Name as you like and click Next

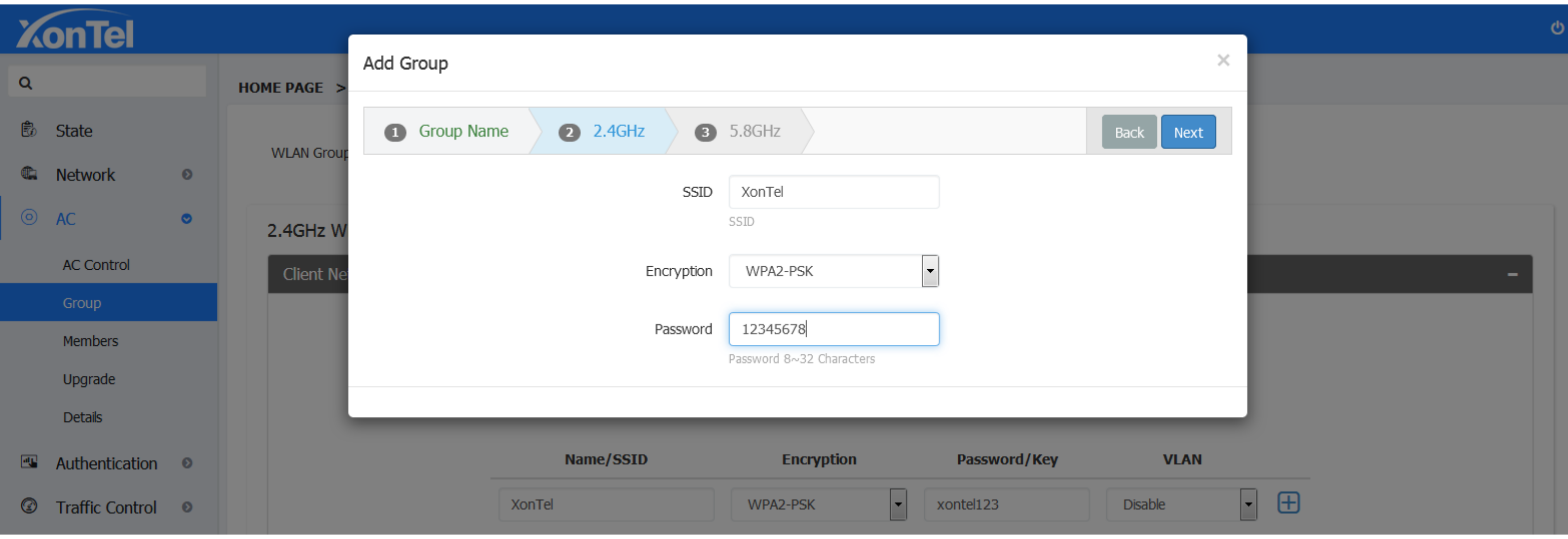


Add Group

Group Name: XonTel

Group Name

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



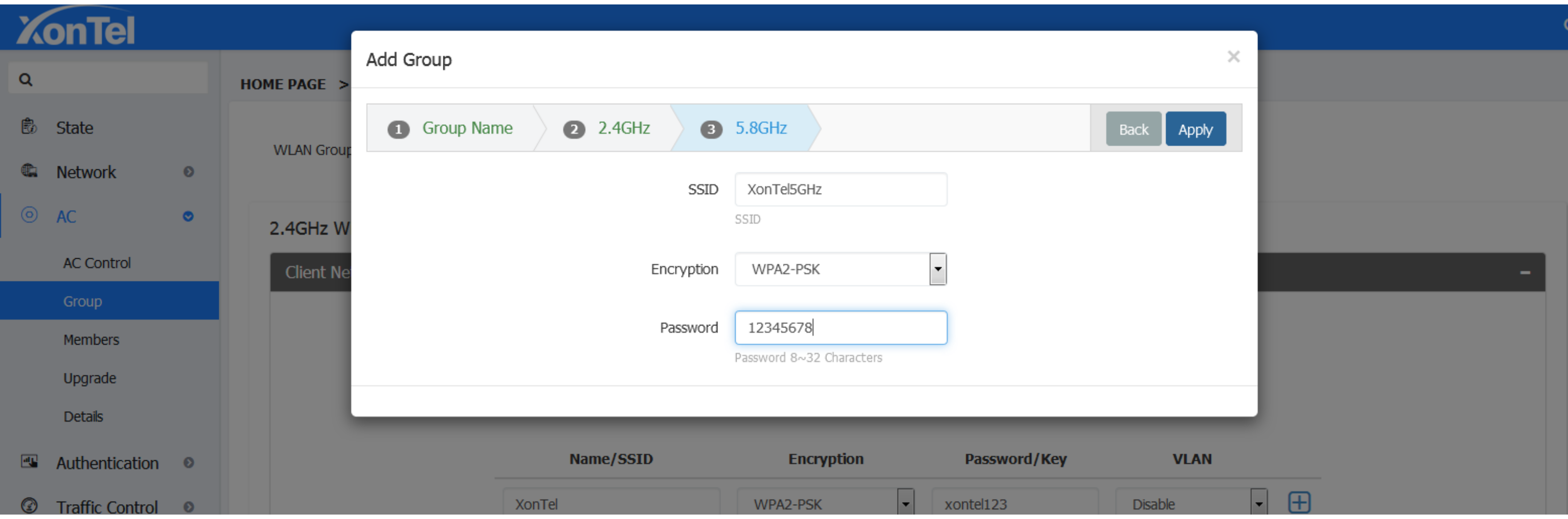
SSID: XonTel

Encryption: WPA2-PSK

Password: 12345678 (Password 8~32 Characters)

Name/SSID	Encryption	Password/Key	VLAN
XonTel	WPA2-PSK	xontel123	Disable

4. Setup 5.8GHz relative parameter (SSID/Encryption Type/Password)



SSID: XonTel5GHz

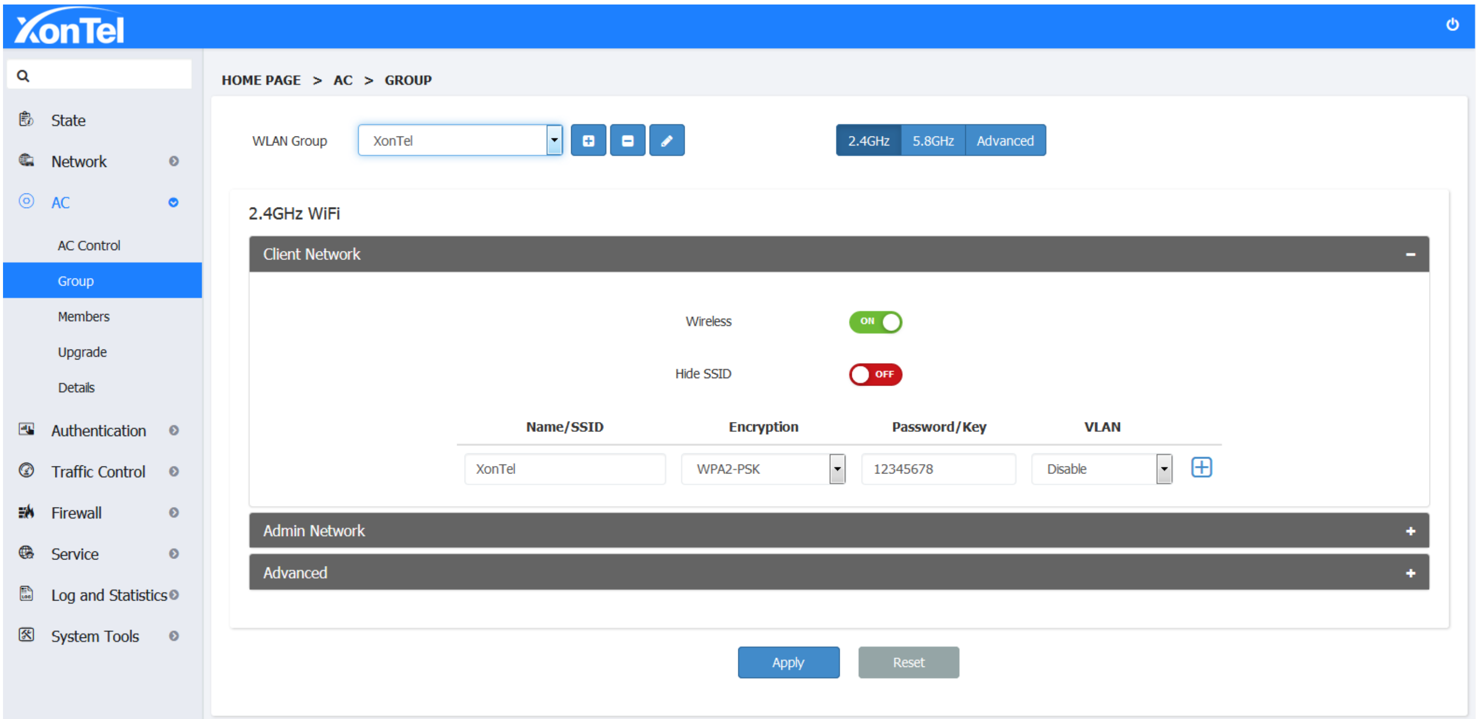
Encryption: WPA2-PSK

Password: 12345678 (Password 8~32 Characters)

Name/SSID	Encryption	Password/Key	VLAN
XonTel	WPA2-PSK	xontel123	Disable

5. Click "Apply" and it will go to "GROUP" page. Choose the group name which you set in wizard and you can view detail setup of that group.

1: Client Network: You can setup the NAME/SSID and PASSWORD/KEY for End Users.



HOME PAGE > AC > GROUP

WLAN Group: XonTel

2.4GHz WiFi

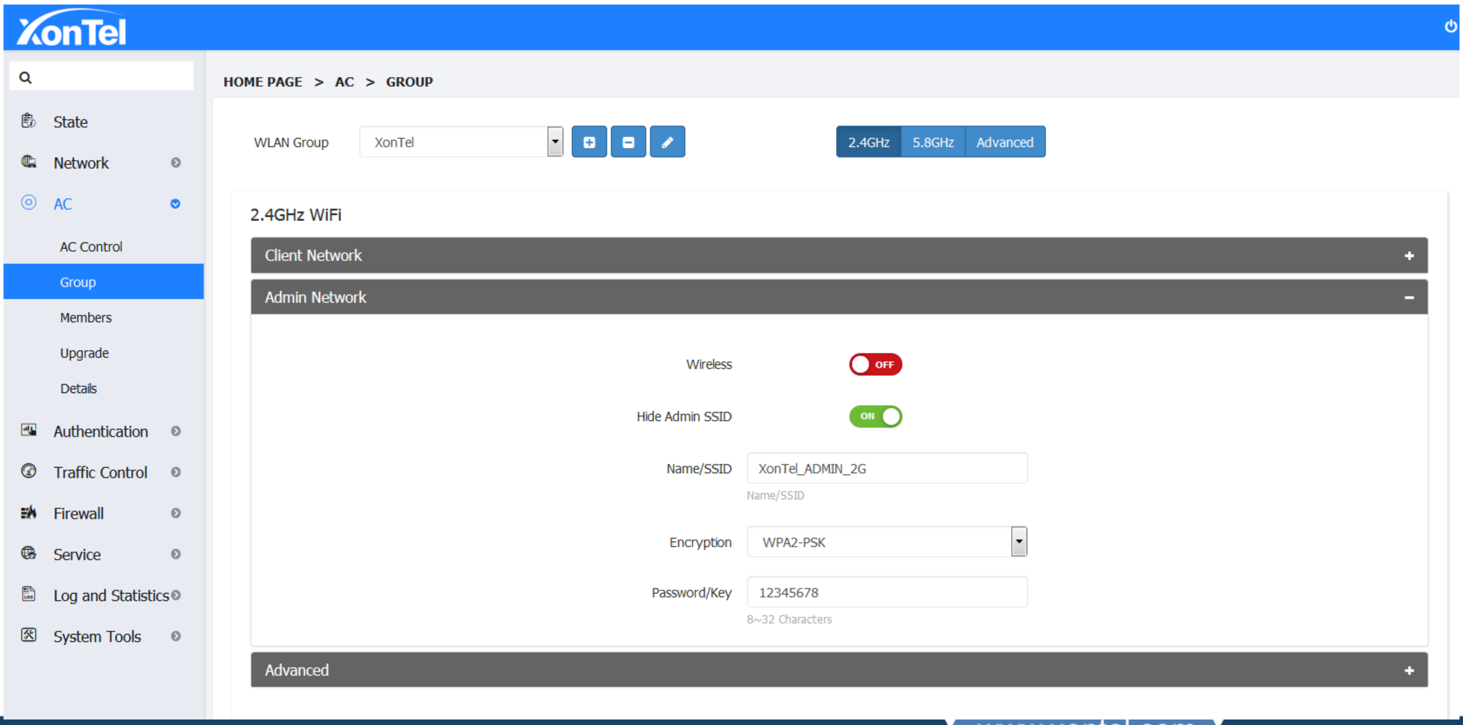
Client Network

Wireless: ON

Hide SSID: OFF

Name/SSID	Encryption	Password/Key	VLAN
XonTel	WPA2-PSK	12345678	Disable

2: Admin Network: You can setup the NAME/SSID and PASSWORD/KEY for Admin Network.



HOME PAGE > AC > GROUP

WLAN Group: XonTel

2.4GHz WiFi

Admin Network

Wireless: OFF

Hide Admin SSID: ON

Name/SSID: XonTel_ADMIN_2G

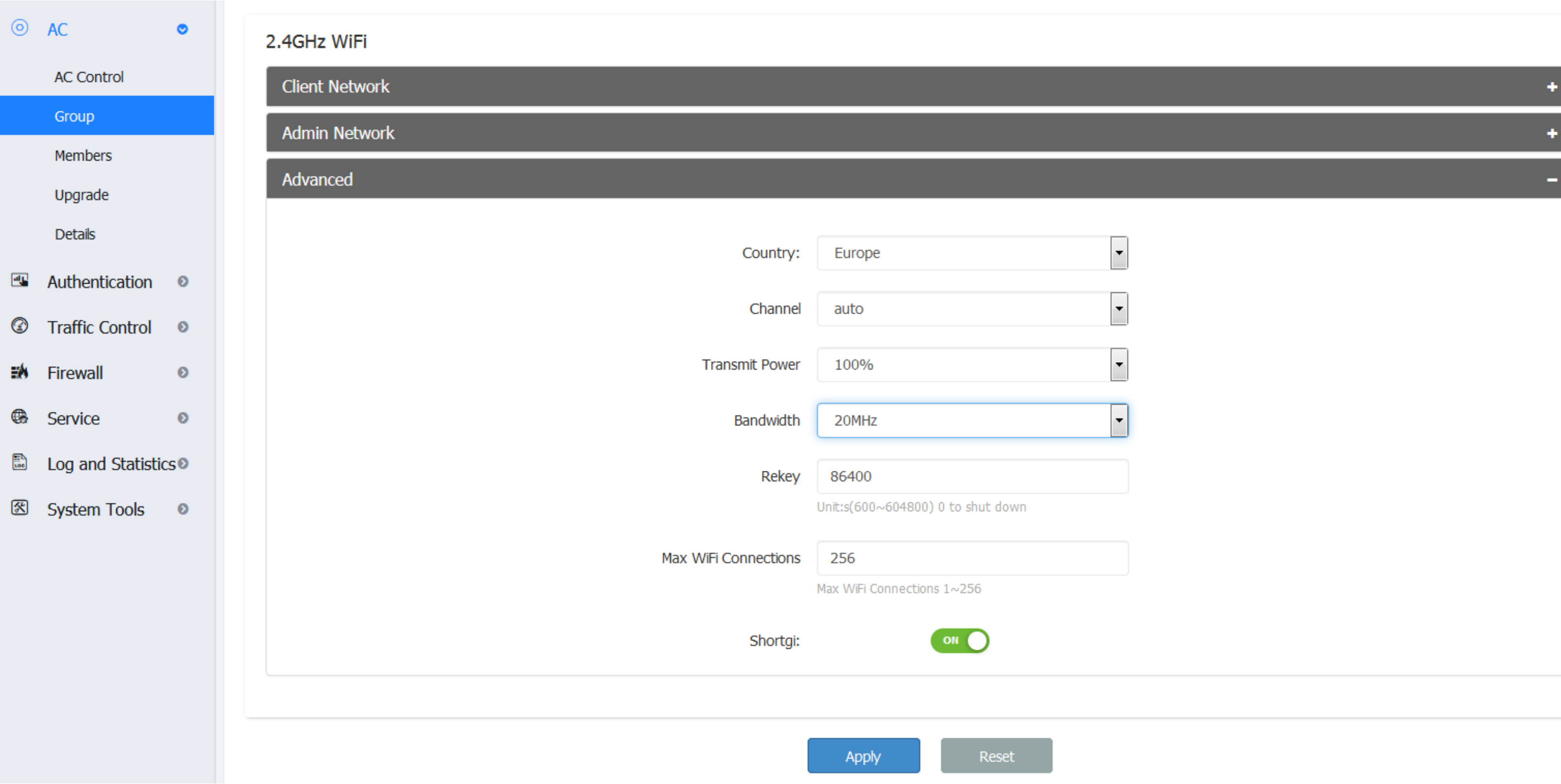
Name/SSID

Encryption: WPA2-PSK

Password/Key: 12345678

8~32 Characters

3: Advanced-Here you can setup Country, Channel, Transmit Power etc. relative parameters.



2.4GHz WiFi

Client Network +

Admin Network +

Advanced −

Country: Europe

Channel auto

Transmit Power 100%

Bandwidth 20MHz

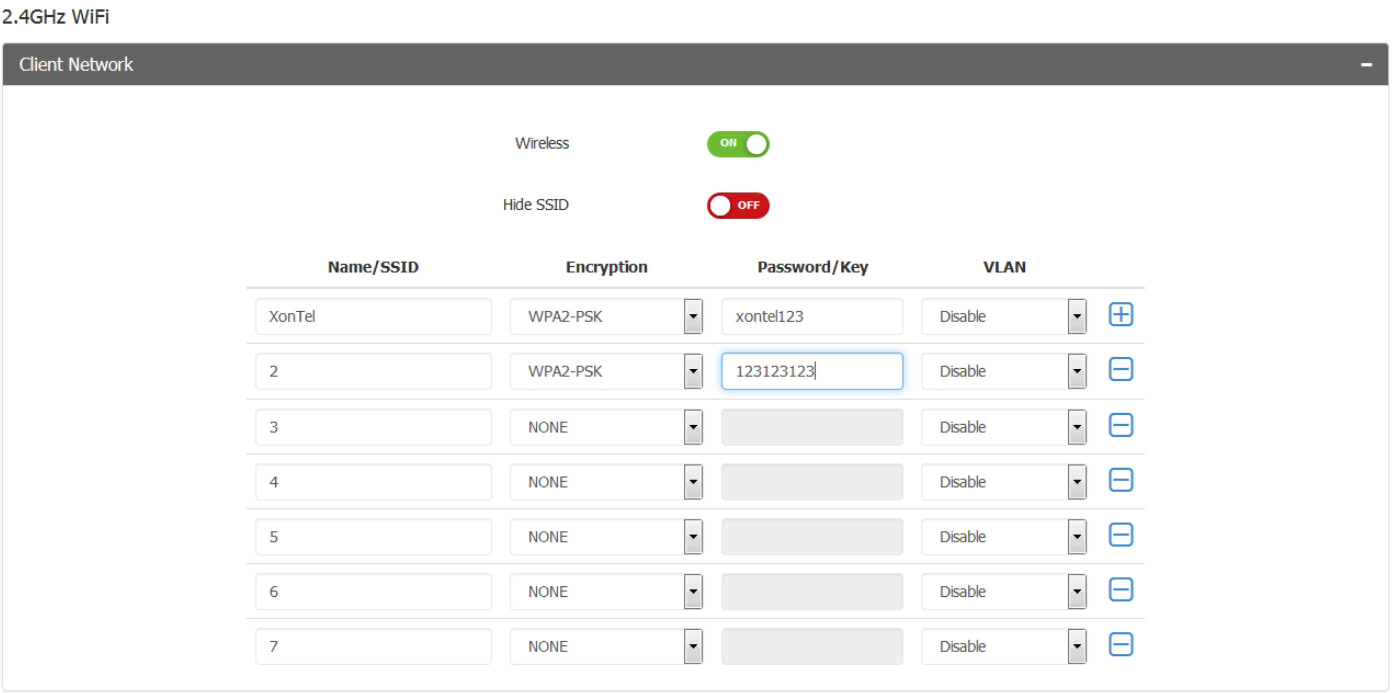
Rekey 86400
Unit:s(600~604800) 0 to shut down

Max WiFi Connections 256
Max WiFi Connections 1~256

Shortgi: ON

6. Inside Client Network click "+" sign to add multiple SSID. You can add extra 7 SSID both in 2.4GHz and 5.8GHz.

2.4G Multiple -SSID:



2.4GHz WiFi

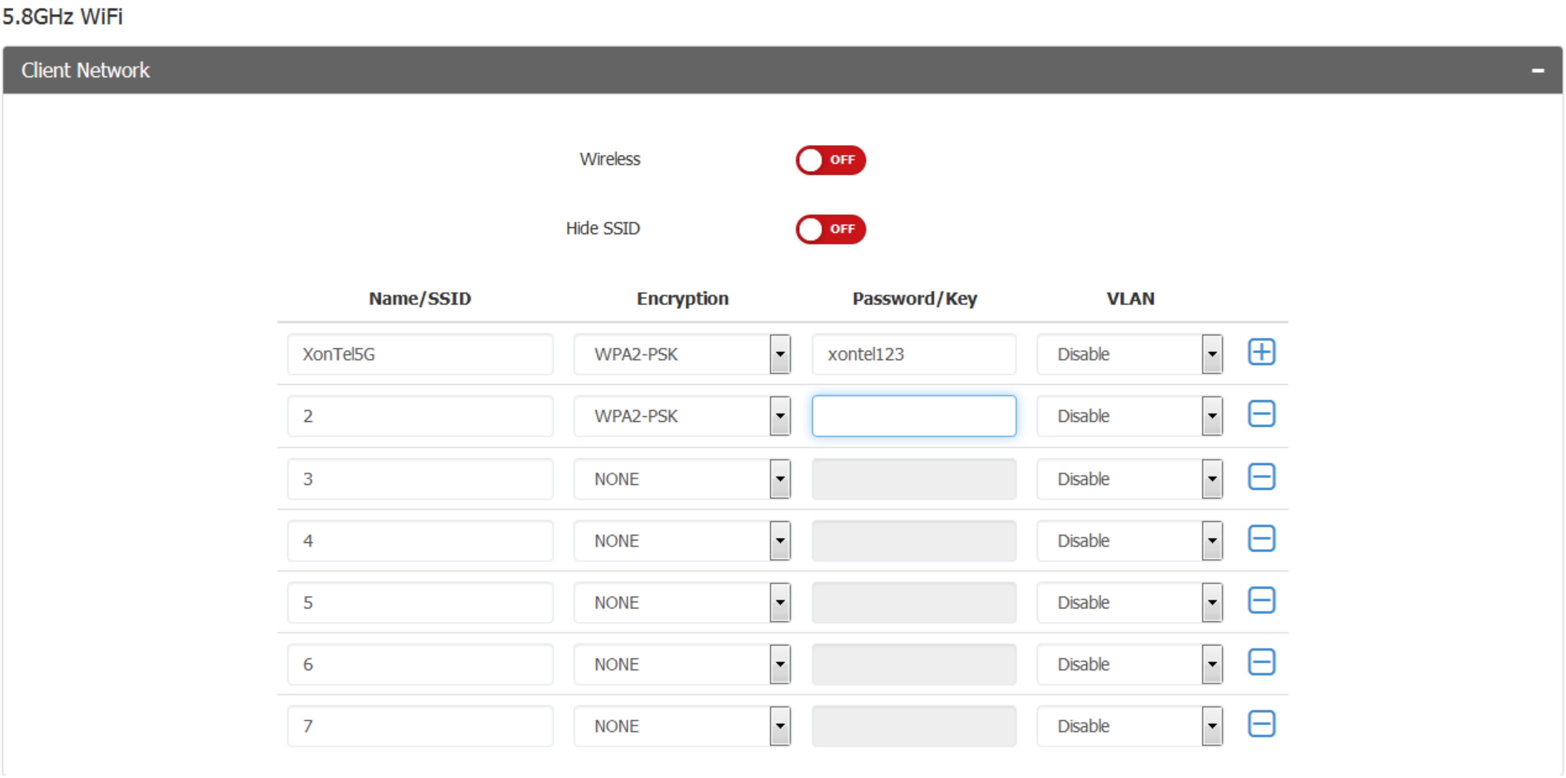
Client Network −

Wireless ON

Hide SSID OFF

Name/SSID	Encryption	Password/Key	VLAN	
XonTel	WPA2-PSK	xontel123	Disable	⊞
2	WPA2-PSK	123123123	Disable	⊟
3	NONE		Disable	⊟
4	NONE		Disable	⊟
5	NONE		Disable	⊟
6	NONE		Disable	⊟
7	NONE		Disable	⊟

5.8GHz Multiple -SSID:



5.8GHz WiFi

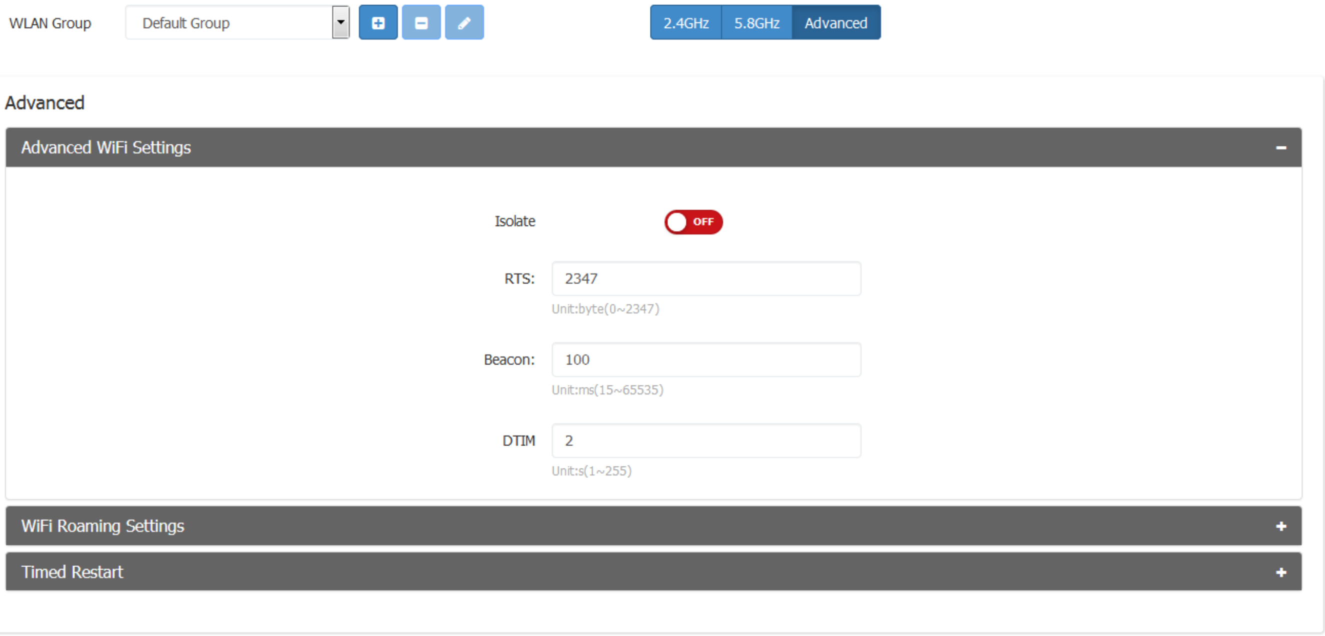
Client Network

Wireless OFF

Hide SSID OFF

Name/SSID	Encryption	Password/Key	VLAN
XonTel5G	WPA2-PSK	xontel123	Disable
2	WPA2-PSK		Disable
3	NONE		Disable
4	NONE		Disable
5	NONE		Disable
6	NONE		Disable
7	NONE		Disable

7. Click Advanced on top of the page, Advance WIFI Settings will open. Here you can Enable/Disable Wireless User Isolation to isolate wireless users. Also can setup Timed Restart or Interval Restart of the Access Points in that group.



WLAN Group: Default Group

Advanced

Advanced WiFi Settings

Isolate OFF

RTS: 2347
Unit:byte(0~2347)

Beacon: 100
Unit:ms(15~65535)

DTIM 2
Unit:s(1~255)

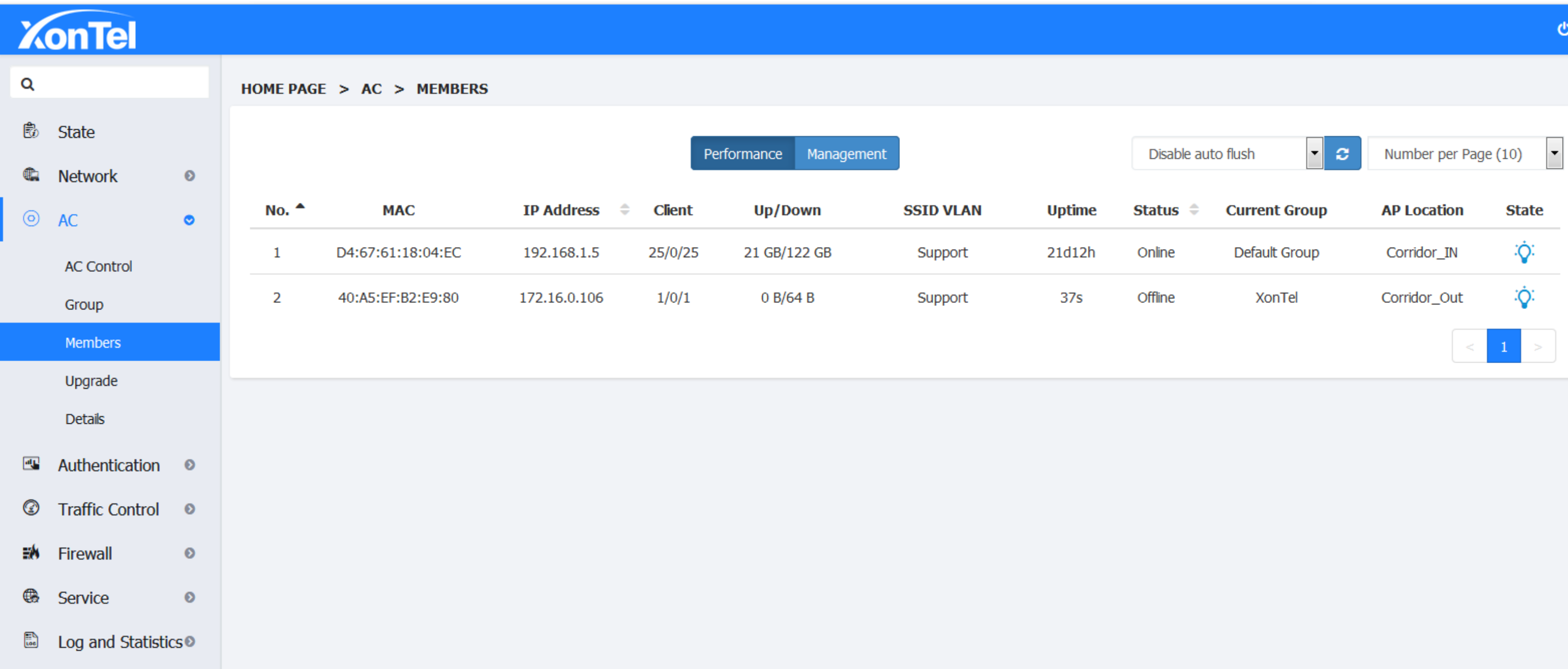
WiFi Roaming Settings

Timed Restart

4.2 Members

If there is multiple Access Points connect with XT-1000AC network, the managed device information will be shown on the Performance page. Click Management and here you can modify the corresponding device's wireless SSID, country, channel, transmitted power, wireless bandwidth, max-awaiting amount and alias.

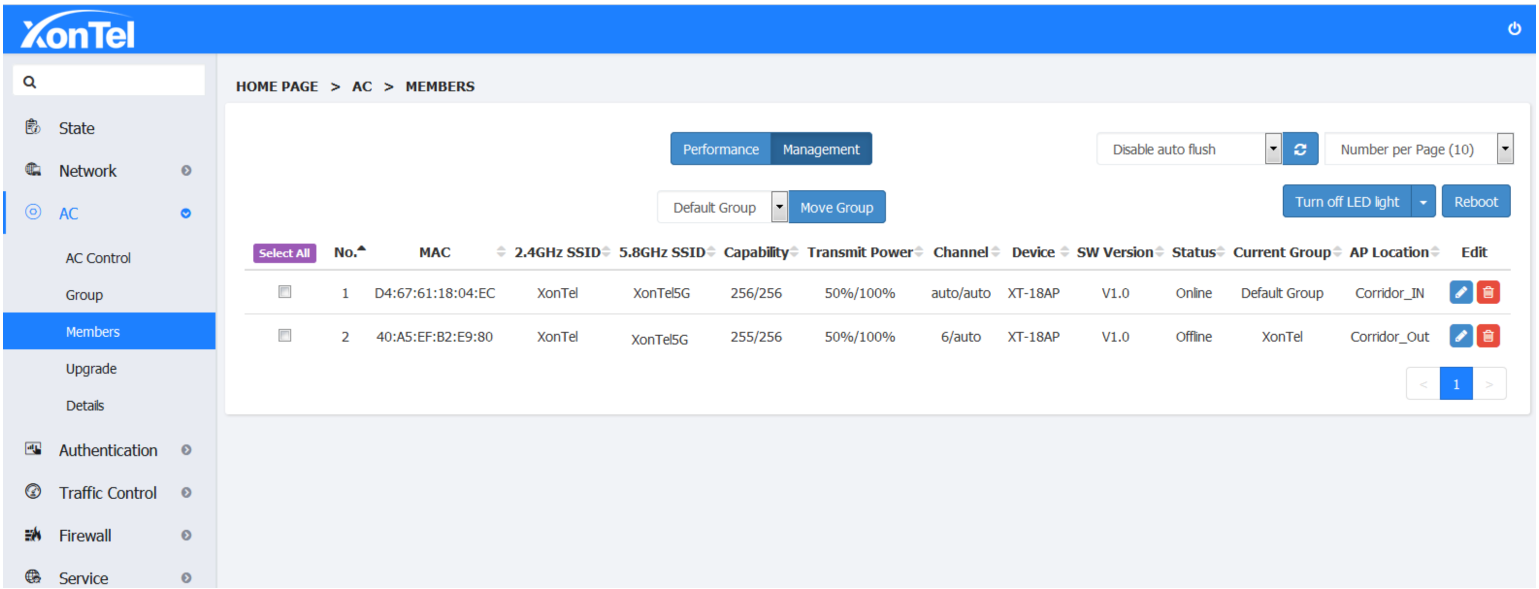
1. Open WEB home page and go into AC Control's "Members" page, as below:



HOME PAGE > AC > MEMBERS

No.	MAC	IP Address	Client	Up/Down	SSID VLAN	Uptime	Status	Current Group	AP Location	State
1	D4:67:61:18:04:EC	192.168.1.5	25/0/25	21 GB/122 GB	Support	21d12h	Online	Default Group	Corridor_IN	💡
2	40:A5:EF:B2:E9:80	172.16.0.106	1/0/1	0 B/64 B	Support	37s	Offline	XonTel	Corridor_Out	💡

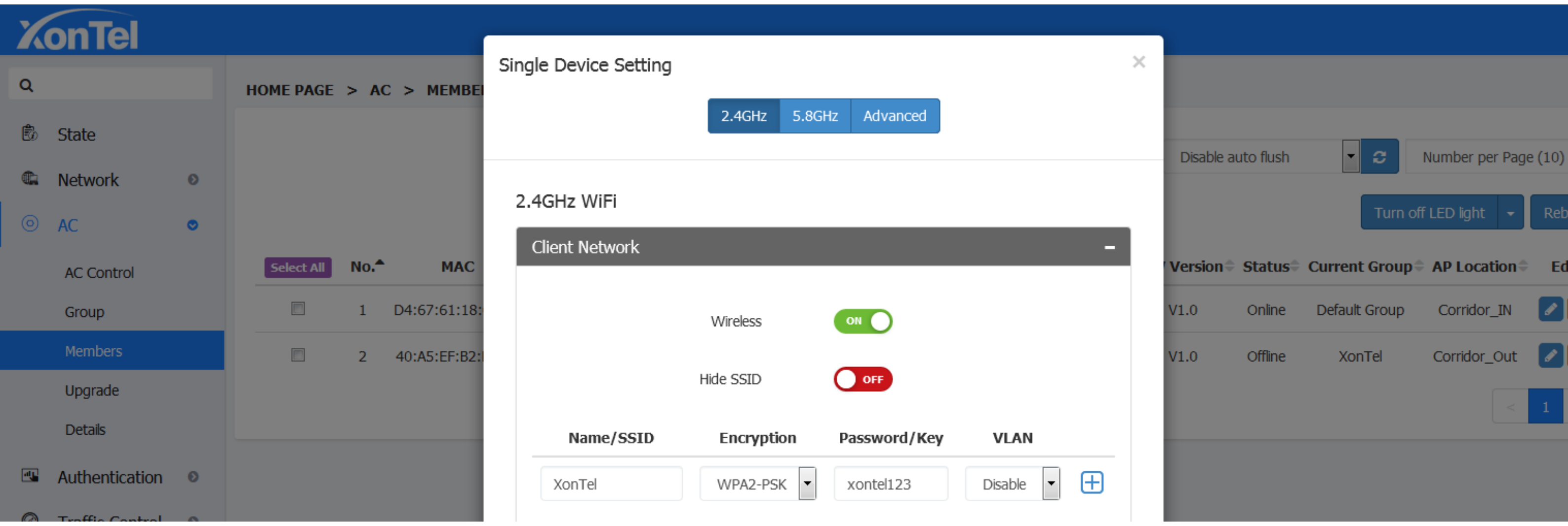
2. Click on above picture's "Management" button and go into the managing page, as below:



HOME PAGE > AC > MEMBERS

	No.	MAC	2.4GHz SSID	5.8GHz SSID	Capability	Transmit Power	Channel	Device	SW Version	Status	Current Group	AP Location	Edit
□	1	D4:67:61:18:04:EC	XonTel	XonTel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	✎ 🗑
□	2	40:A5:EF:B2:E9:80	XonTel	XonTel5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	✎ 🗑

3. Click below picture’s “Edit” button so you can reconfigure the device’s SSID, Country, Channel and TX Power etc. details as below:



Single Device Setting

2.4GHz | 5.8GHz | Advanced

2.4GHz WiFi

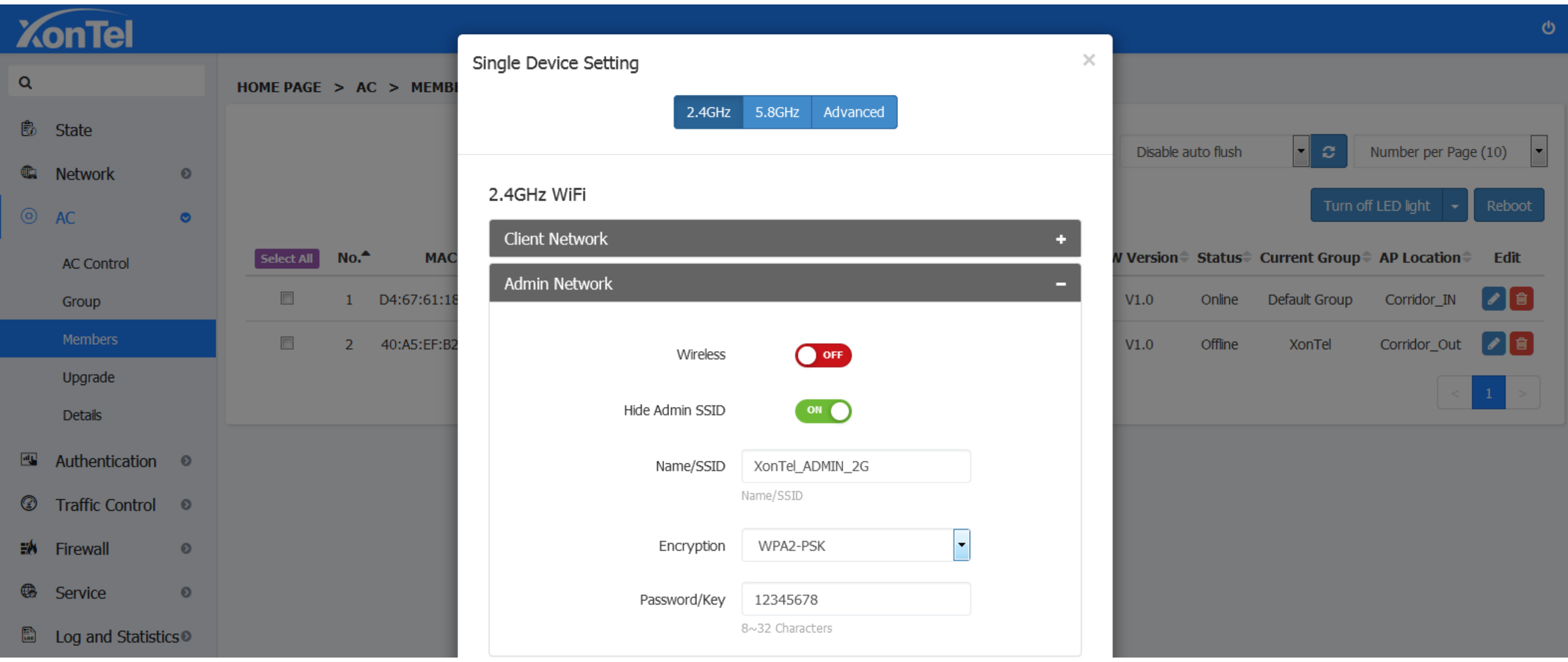
Client Network

Wireless: ON

Hide SSID: OFF

Name/SSID	Encryption	Password/Key	VLAN
XonTel	WPA2-PSK	xontel123	Disable

4. Click Admin Network



Single Device Setting

2.4GHz | 5.8GHz | Advanced

2.4GHz WiFi

Client Network +

Admin Network −

Wireless: OFF

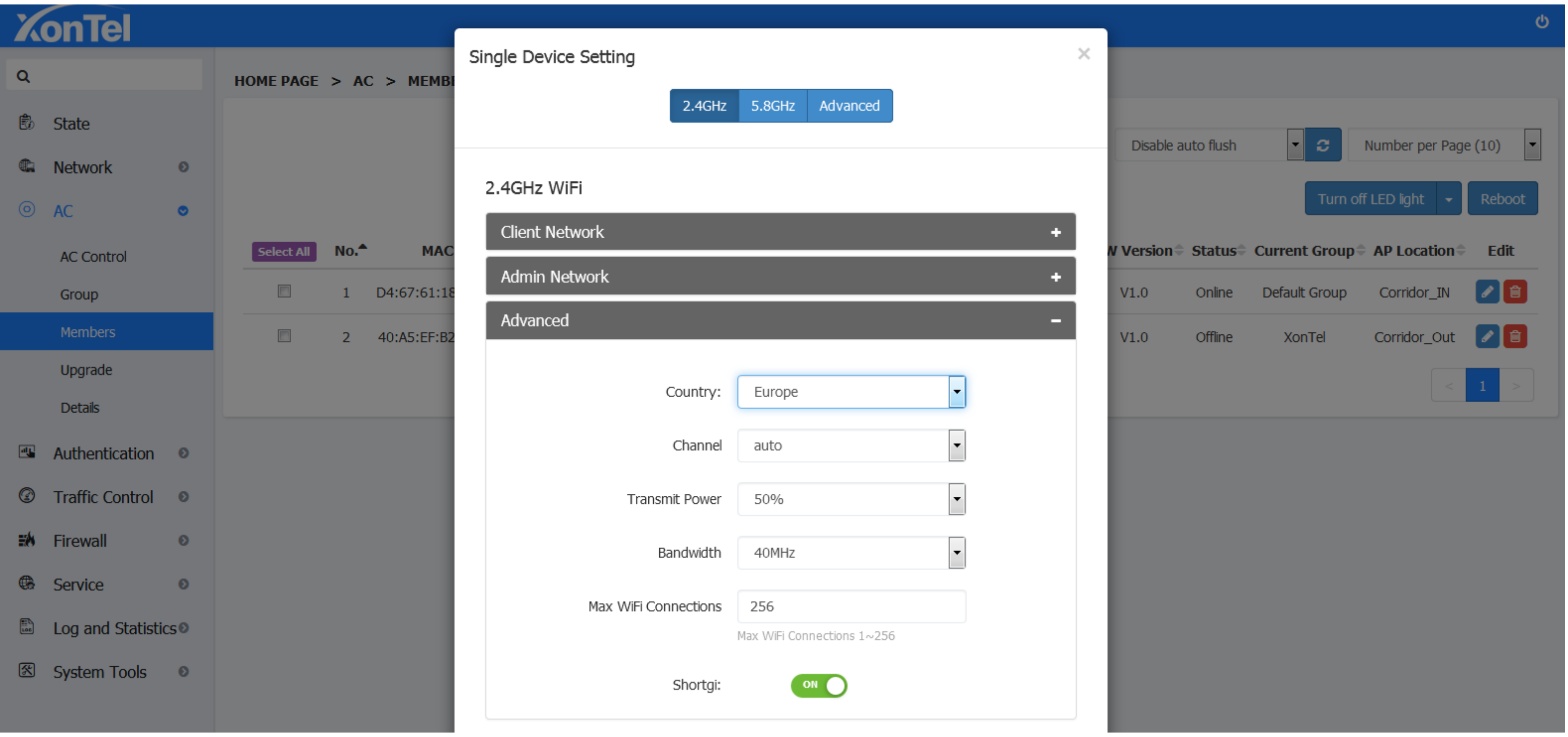
Hide Admin SSID: ON

Name/SSID: XonTel_ADMIN_2G
Name/SSID

Encryption: WPA2-PSK

Password/Key: 12345678
8~32 Characters

5.Click Advanced:



Single Device Setting

2.4GHz | 5.8GHz | Advanced

2.4GHz WiFi

- Client Network +
- Admin Network +
- Advanced −

Country: Europe

Channel: auto

Transmit Power: 50%

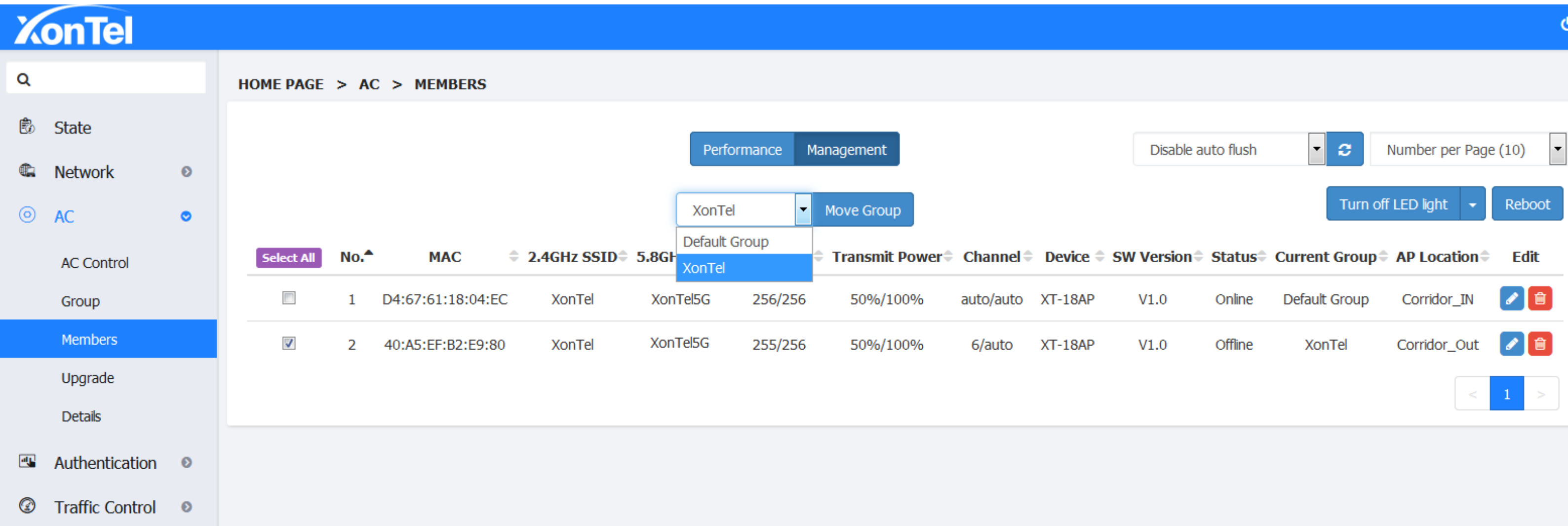
Bandwidth: 40MHz

Max WiFi Connections: 256

Max WiFi Connections 1~256

Shortgi: ON

6. **Move a device to different group: Select the devices you want to move to different group and choose the group name (XonTel) from the drop-down menu near “Move Group” button and then click on Move Group.**



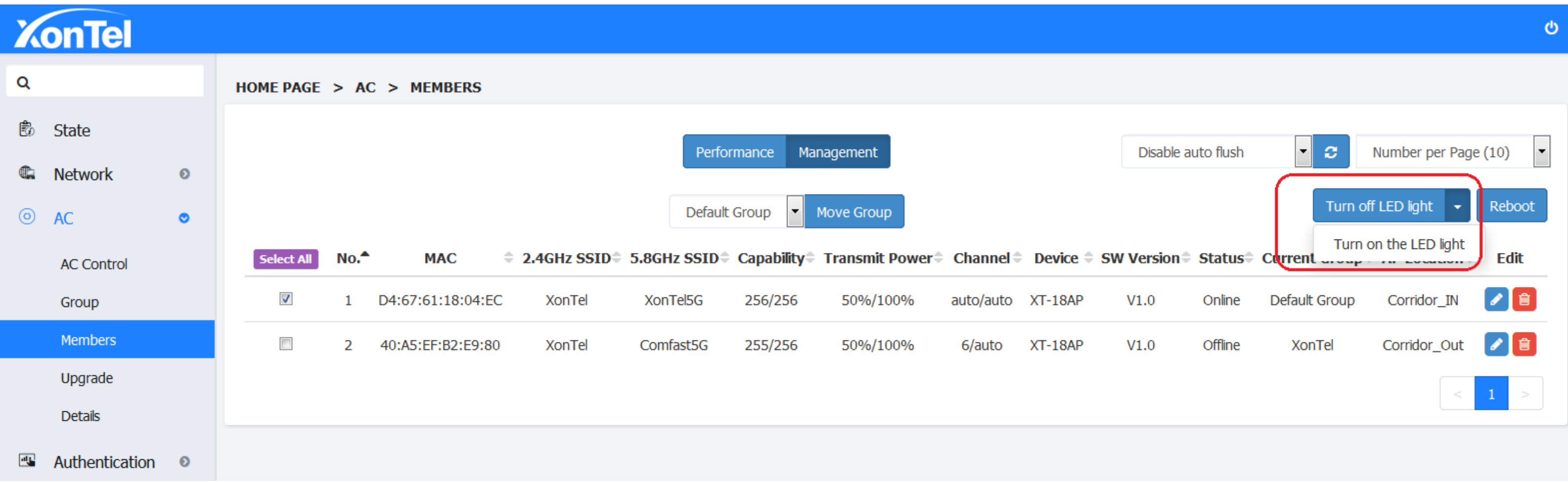
HOME PAGE > AC > MEMBERS

XonTel ▾ Move Group

Default Group
XonTel

	No.	MAC	2.4GHz SSID	5.8GH		Transmit Power	Channel	Device	SW Version	Status	Current Group	AP Location	Edit
□	1	D4:67:61:18:04:EC	XonTel	XonTel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	
☑	2	40:A5:EF:B2:E9:80	XonTel	XonTel5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	

7. Click the LED light control button to turn off the LED light of the Access Points. Click again to open the LED light of the Access Points.



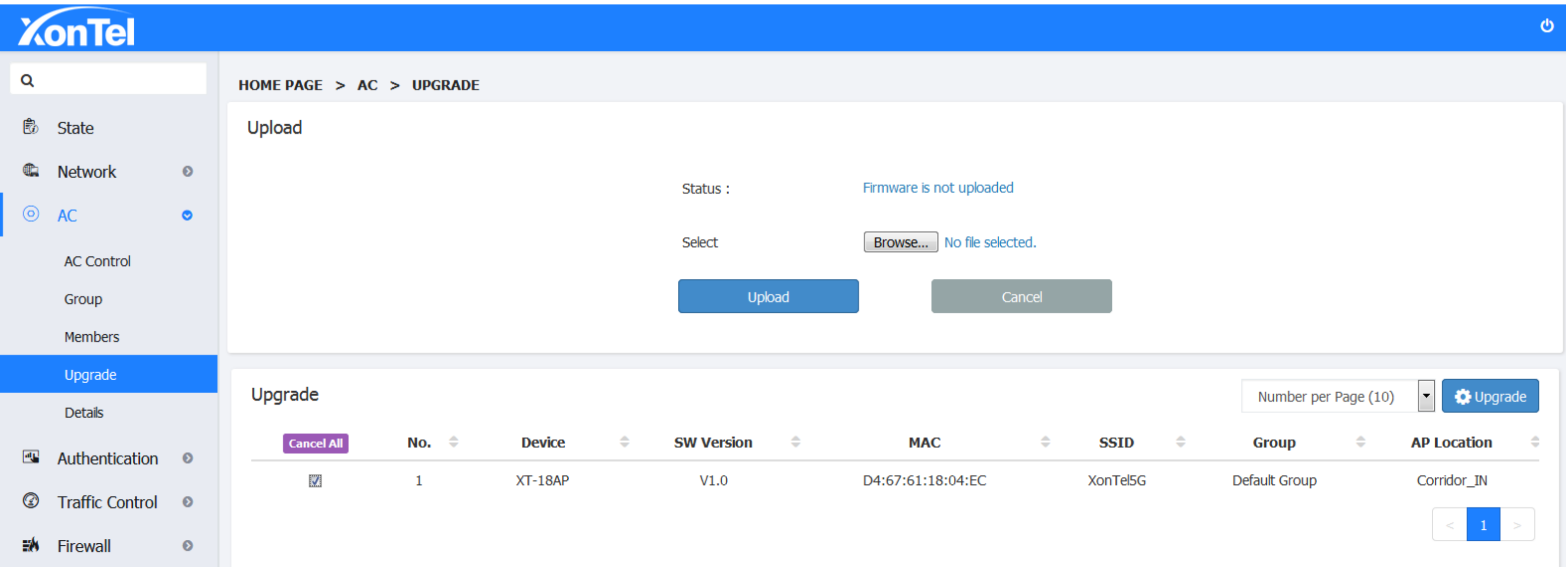
HOME PAGE > AC > MEMBERS

Select All	No.	MAC	2.4GHz SSID	5.8GHz SSID	Capability	Transmit Power	Channel	Device	SW Version	Status	Current		Edit
☑	1	D4:67:61:18:04:EC	XonTel	XonTel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	
☐	2	40:A5:EF:B2:E9:80	XonTel	Comfast5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	

4.3 Upgrade

Upgrade option can upgrade all Access Points at same time. You have to upload a firmware file and select the devices you upgrade.

1. Open XT-1000AC Upgrade page, as below:



HOME PAGE > AC > UPGRADE

Upload

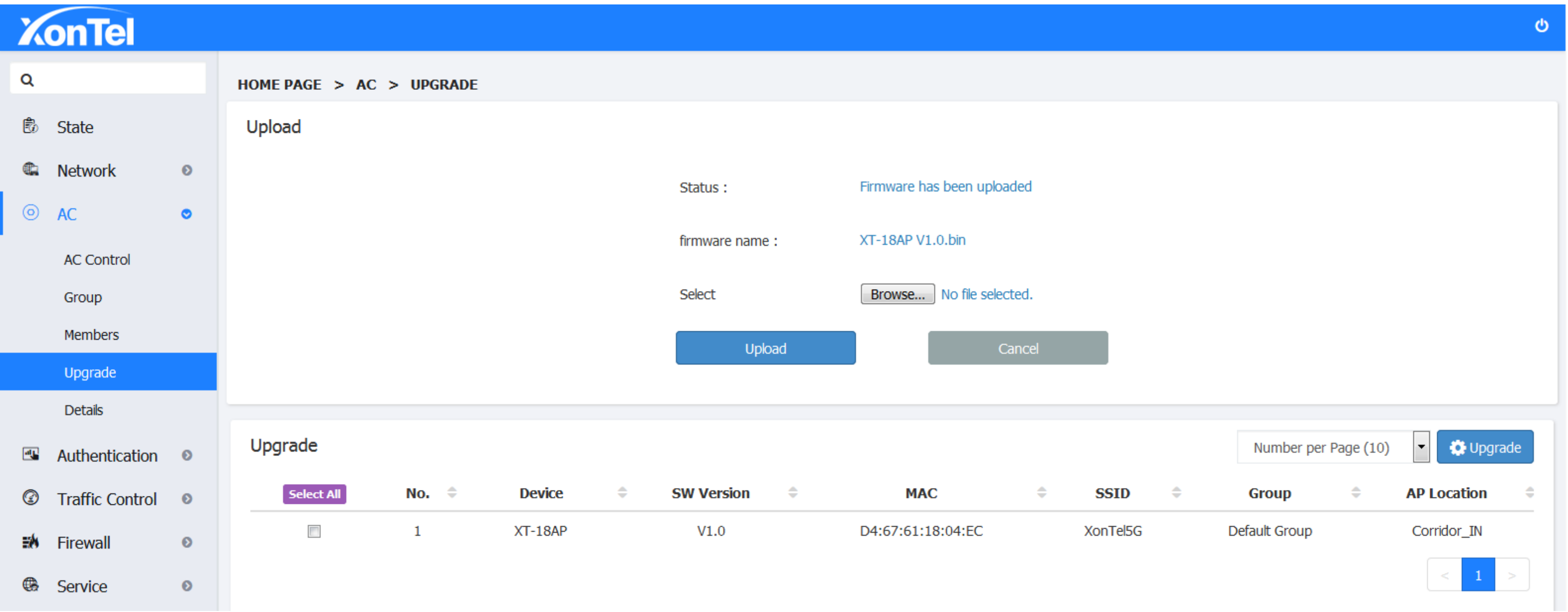
Status : Firmware is not uploaded

Select No file selected.

Upgrade

Cancel All	No.	Device	SW Version	MAC	SSID	Group	AP Location
☑	1	XT-18AP	V1.0	D4:67:61:18:04:EC	XonTel5G	Default Group	Corridor_IN

2. Click above picture's "Browse" button, choose the newest firmware which you want to upgrade for the Access Points, click "Upload" button "Firmware has been uploaded", as below:



HOME PAGE > AC > UPGRADE

Upload

Status : Firmware has been uploaded

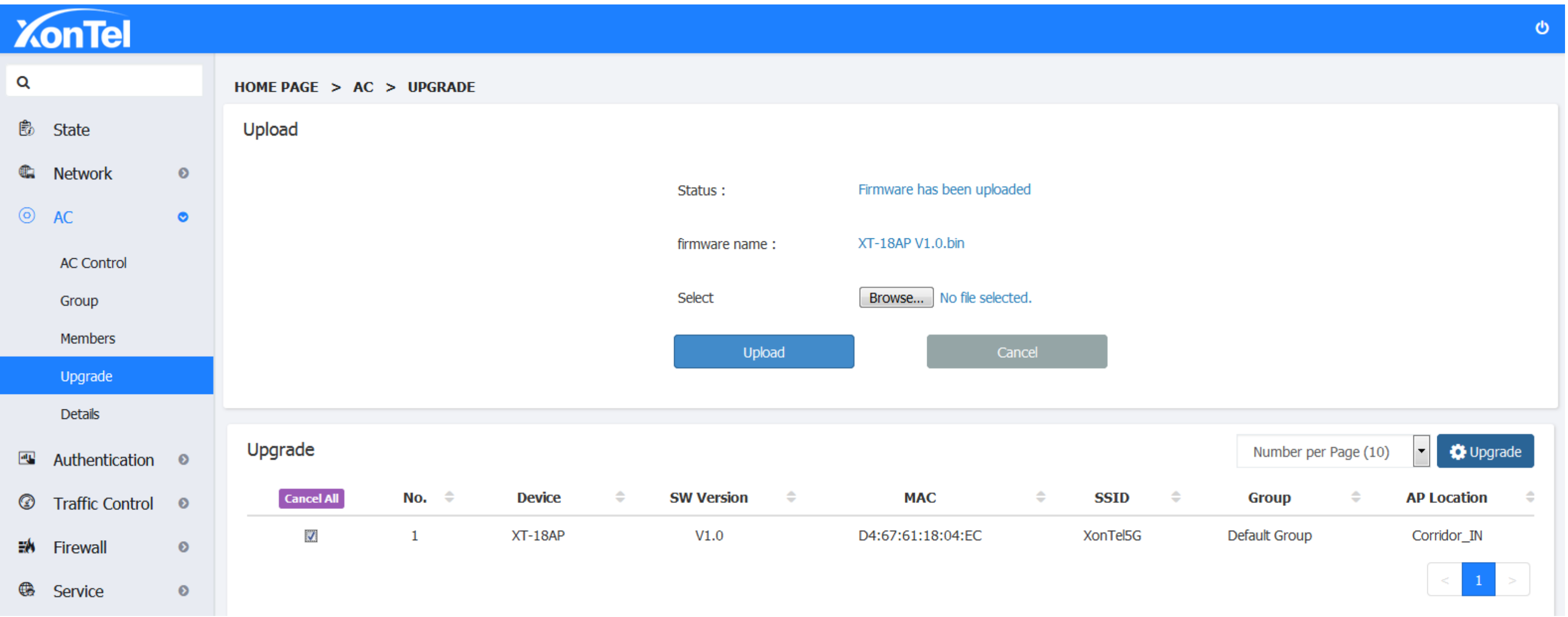
firmware name : XT-18AP V1.0.bin

Select No file selected.

Upgrade

Select All	No.	Device	SW Version	MAC	SSID	Group	AP Location
□	1	XT-18AP	V1.0	D4:67:61:18:04:EC	XonTel5G	Default Group	Corridor_IN

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



HOME PAGE > AC > UPGRADE

Upload

Status : Firmware has been uploaded

firmware name : XT-18AP V1.0.bin

Select No file selected.

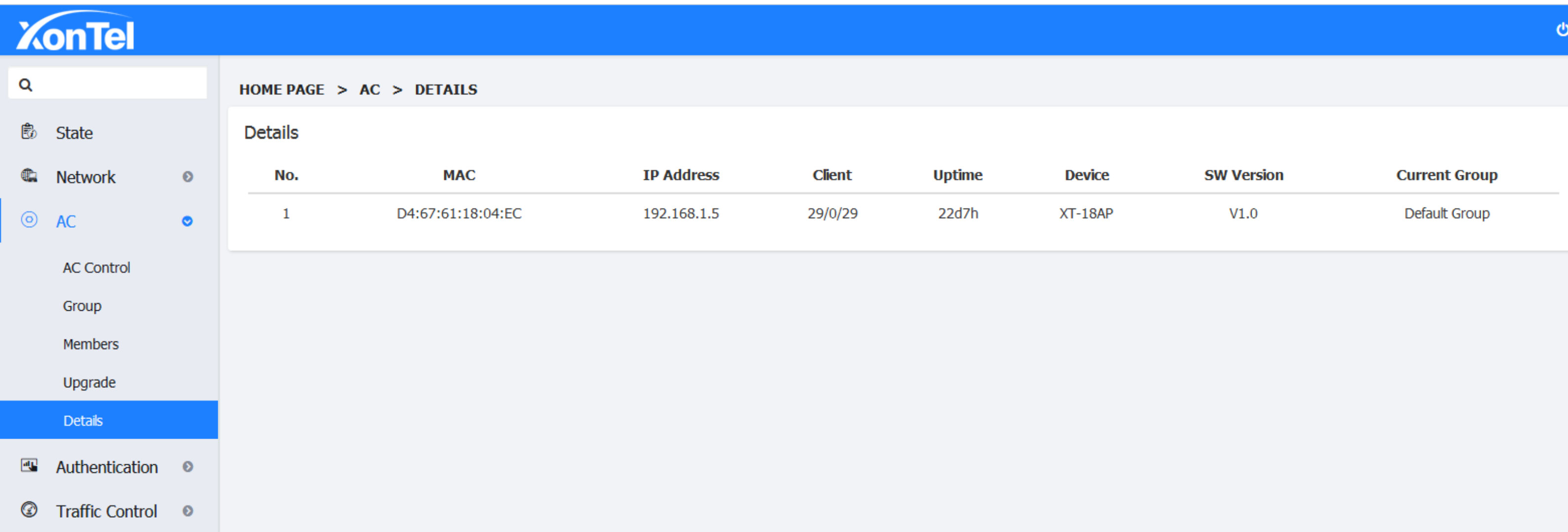
Upgrade

Cancel All	No.	Device	SW Version	MAC	SSID	Group	AP Location
☑	1	XT-18AP	V1.0	D4:67:61:18:04:EC	XonTel5G	Default Group	Corridor_IN

4.4 Details

This function displays all terminal entries under XT-1000AC, including Access Points and wireless terminals connected to Access Points.

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

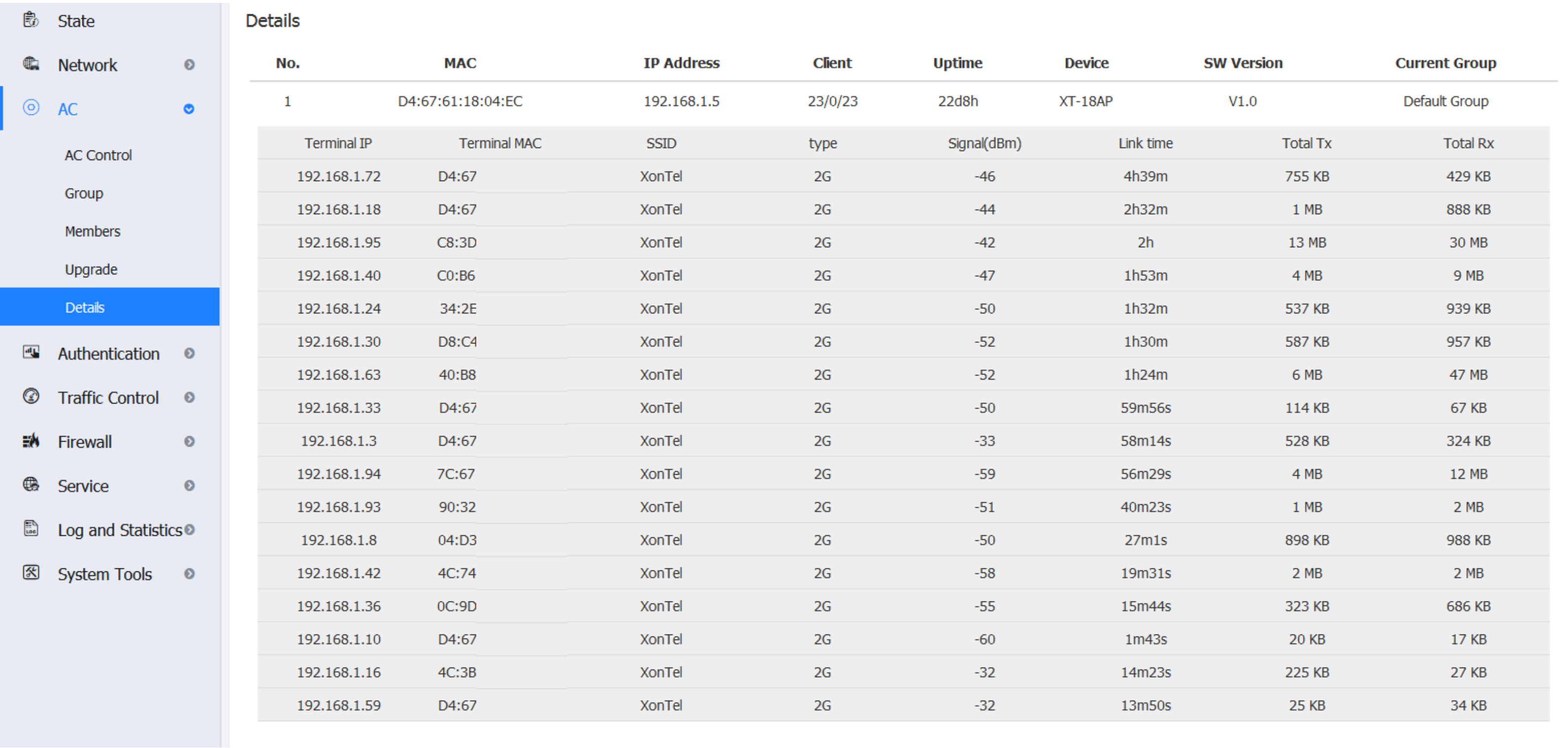


HOME PAGE > AC > DETAILS

Details

No.	MAC	IP Address	Client	Uptime	Device	SW Version	Current Group
1	D4:67:61:18:04:EC	192.168.1.5	29/0/29	22d7h	XT-18AP	V1.0	Default Group

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



Details

No.	MAC	IP Address	Client	Uptime	Device	SW Version	Current Group
1	D4:67:61:18:04:EC	192.168.1.5	23/0/23	22d8h	XT-18AP	V1.0	Default Group

Terminal IP	Terminal MAC	SSID	type	Signal(dBm)	Link time	Total Tx	Total Rx
192.168.1.72	D4:67	XonTel	2G	-46	4h39m	755 KB	429 KB
192.168.1.18	D4:67	XonTel	2G	-44	2h32m	1 MB	888 KB
192.168.1.95	C8:3D	XonTel	2G	-42	2h	13 MB	30 MB
192.168.1.40	C0:B6	XonTel	2G	-47	1h53m	4 MB	9 MB
192.168.1.24	34:2E	XonTel	2G	-50	1h32m	537 KB	939 KB
192.168.1.30	D8:C4	XonTel	2G	-52	1h30m	587 KB	957 KB
192.168.1.63	40:B8	XonTel	2G	-52	1h24m	6 MB	47 MB
192.168.1.33	D4:67	XonTel	2G	-50	59m56s	114 KB	67 KB
192.168.1.3	D4:67	XonTel	2G	-33	58m14s	528 KB	324 KB
192.168.1.94	7C:67	XonTel	2G	-59	56m29s	4 MB	12 MB
192.168.1.93	90:32	XonTel	2G	-51	40m23s	1 MB	2 MB
192.168.1.8	04:D3	XonTel	2G	-50	27m1s	898 KB	988 KB
192.168.1.42	4C:74	XonTel	2G	-58	19m31s	2 MB	2 MB
192.168.1.36	0C:9D	XonTel	2G	-55	15m44s	323 KB	686 KB
192.168.1.10	D4:67	XonTel	2G	-60	1m43s	20 KB	17 KB
192.168.1.16	4C:3B	XonTel	2G	-32	14m23s	225 KB	27 KB
192.168.1.59	D4:67	XonTel	2G	-32	13m50s	25 KB	34 KB

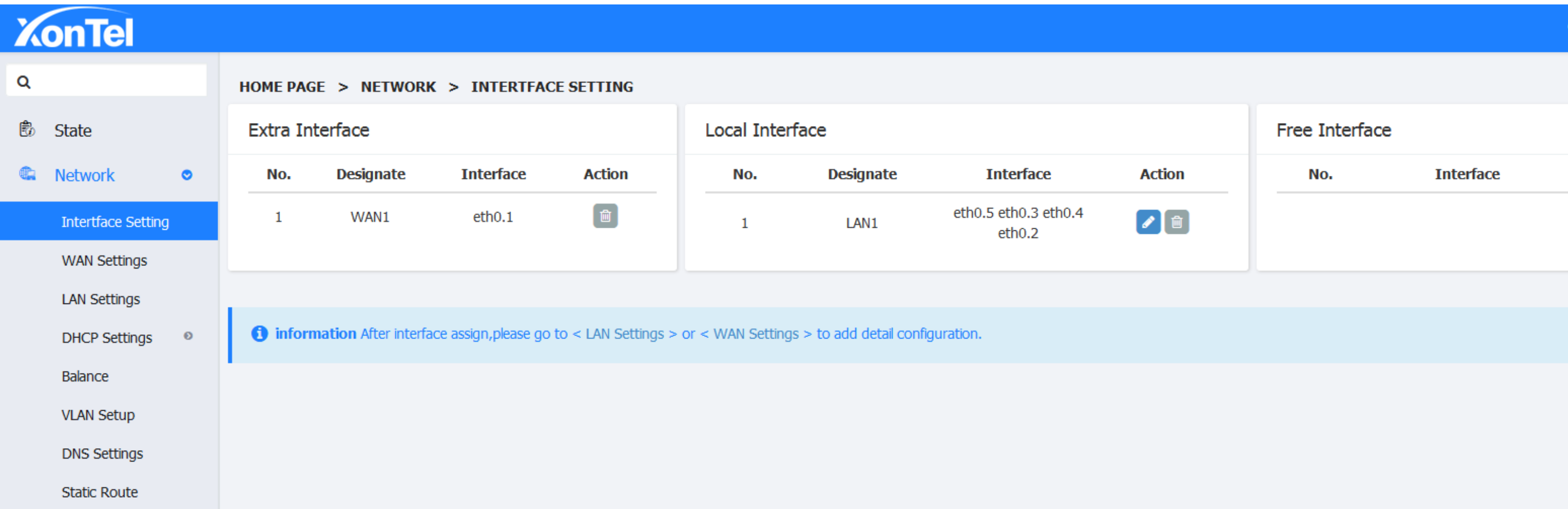
5 Authentication

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 XT-1000AC and go into the home page,” Network “-->” Interface Setting”.



HOME PAGE > NETWORK > INTERTFACE SETTING

Extra Interface

No.	Designate	Interface	Action
1	WAN1	eth0.1	

Local Interface

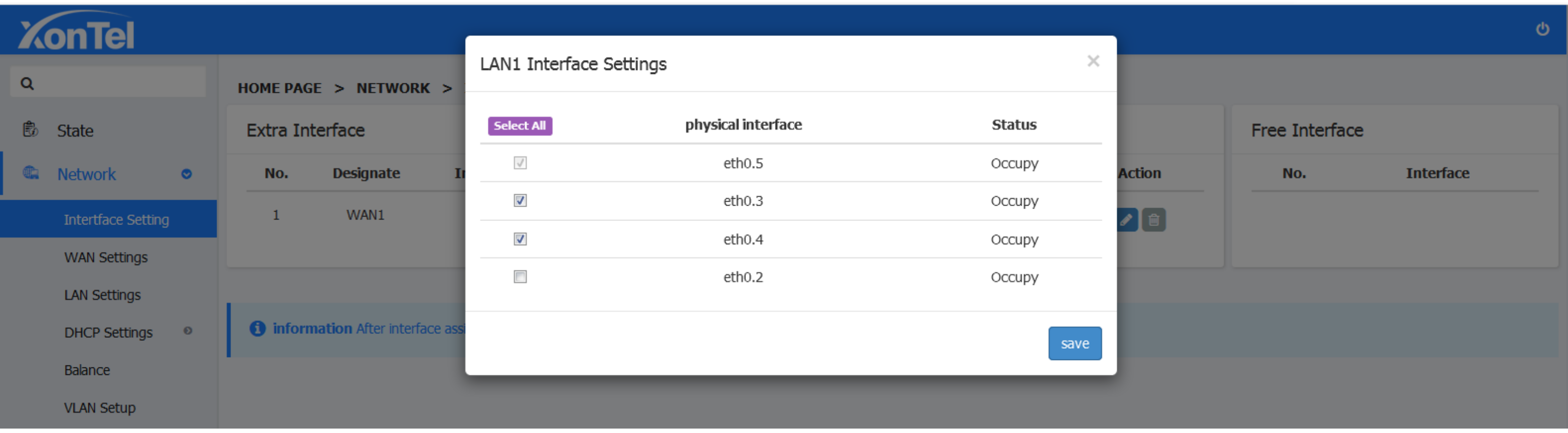
No.	Designate	Interface	Action
1	LAN1	eth0.5 eth0.3 eth0.4 eth0.2	

Free Interface

No.	Interface

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

2. In the Local Interface, click “Edit” button, uncheck the eth0.2from the LAN1 Interface Settings page, then the eth0.2 port will be freed, later click “Save”.

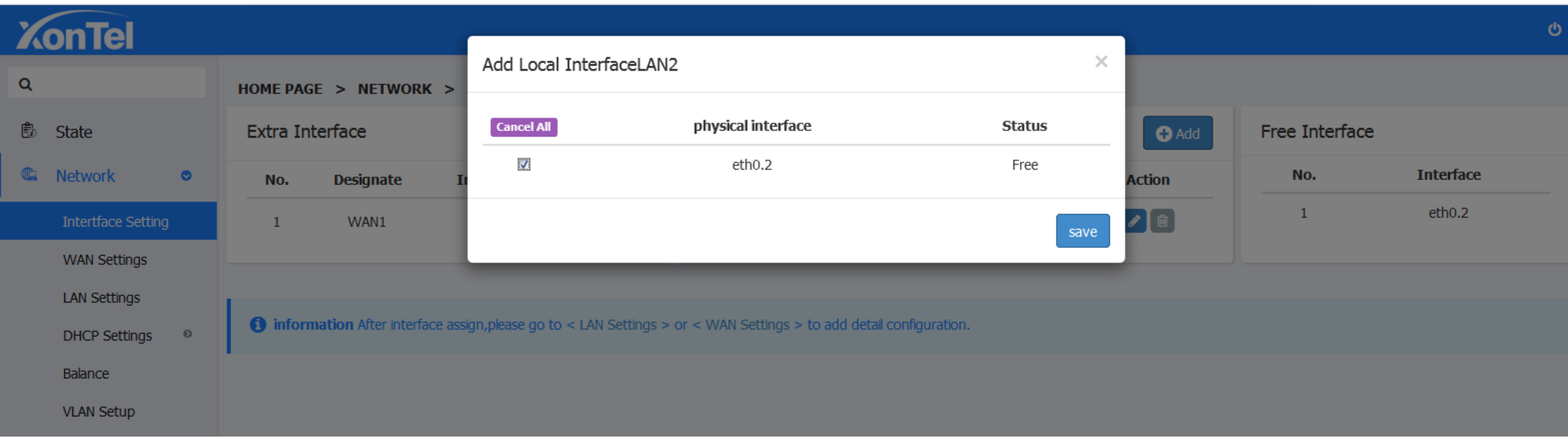


LAN1 Interface Settings

Select All	physical interface	Status
☑	eth0.5	Occupy
☑	eth0.3	Occupy
☑	eth0.4	Occupy
☐	eth0.2	Occupy

save

3.Add a New Local Interface: Click “Add” in the local interface, and select the port you need to allocate to Interface LAN2 then click save.



Add Local InterfaceLAN2

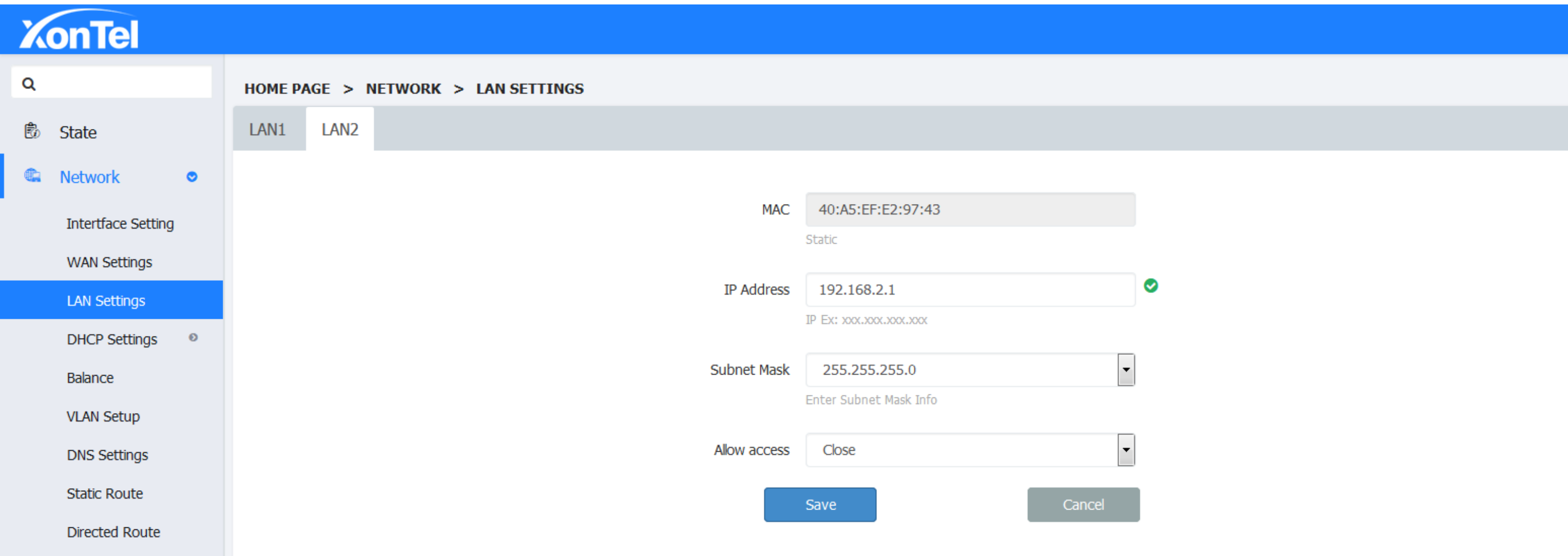
	physical interface	Status
☑	eth0.2	Free

No.	Designate	Action
1	WAN1	

No.	Interface
1	eth0.2

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

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



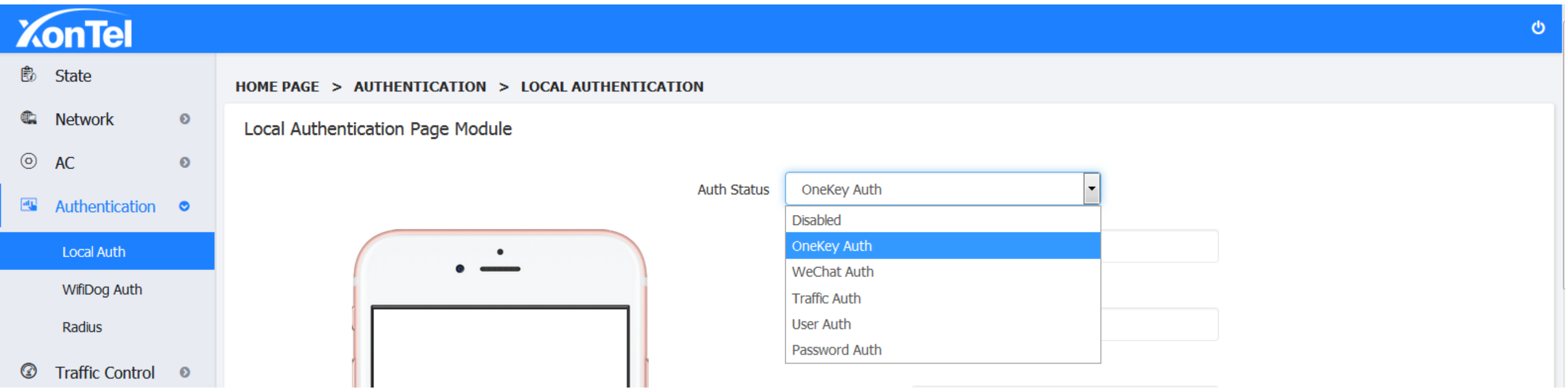
MAC: 40:A5:EF:E2:97:43
Static

IP Address: 192.168.2.1
IP Ex: xxx.xxx.xxx.xxx

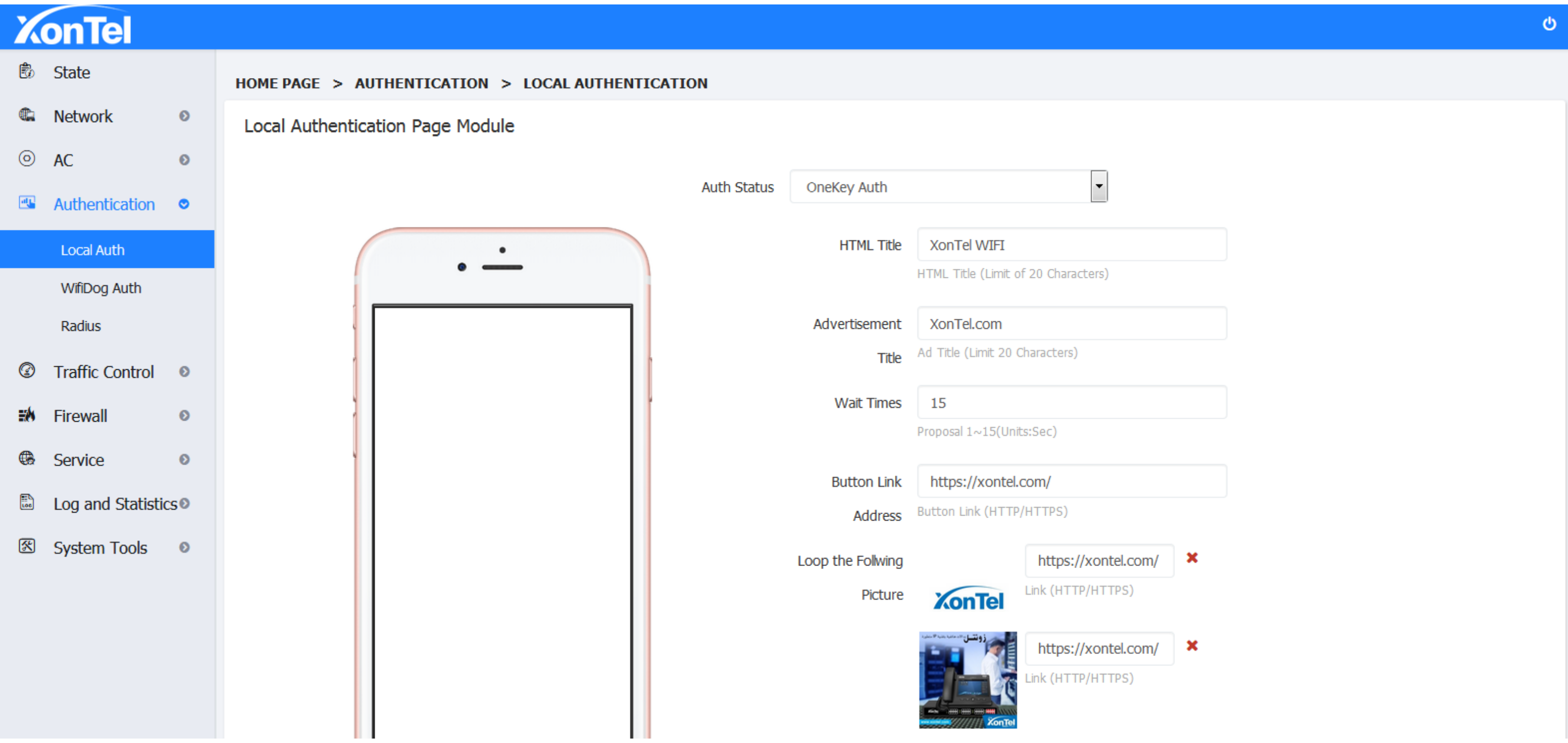
Subnet Mask: 255.255.255.0
Enter Subnet Mask Info

Allow access: Close

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



6. After you choose the Authentication type as One Key Auth, you can upload the ad image and fill in the link address(the link address need to fill in the full network address, such as https://xontel.com/).



Auth Status: OneKey Auth

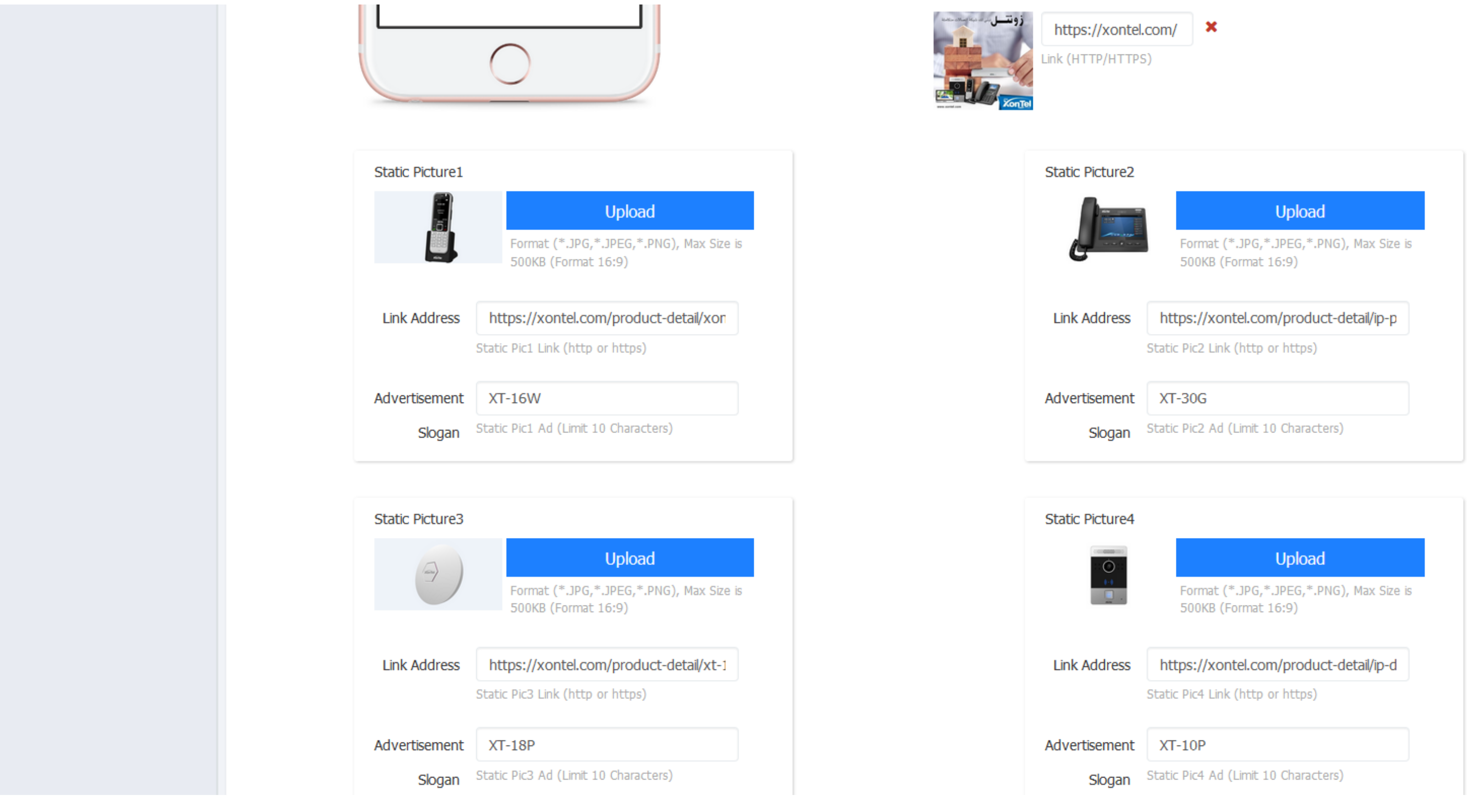
HTML Title: XonTel WIFI
HTML Title (Limit of 20 Characters)

Advertisement Title: XonTel.com
Ad Title (Limit 20 Characters)

Wait Times: 15
Proposal 1~15(Units:Sec)

Button Link Address: https://xontel.com/
Button Link (HTTP/HTTPS)

Loop the Follwing Picture: https://xontel.com/
Link (HTTP/HTTPS)
https://xontel.com/
Link (HTTP/HTTPS)



https://xontel.com/ ✖
Link (HTTP/HTTPS)

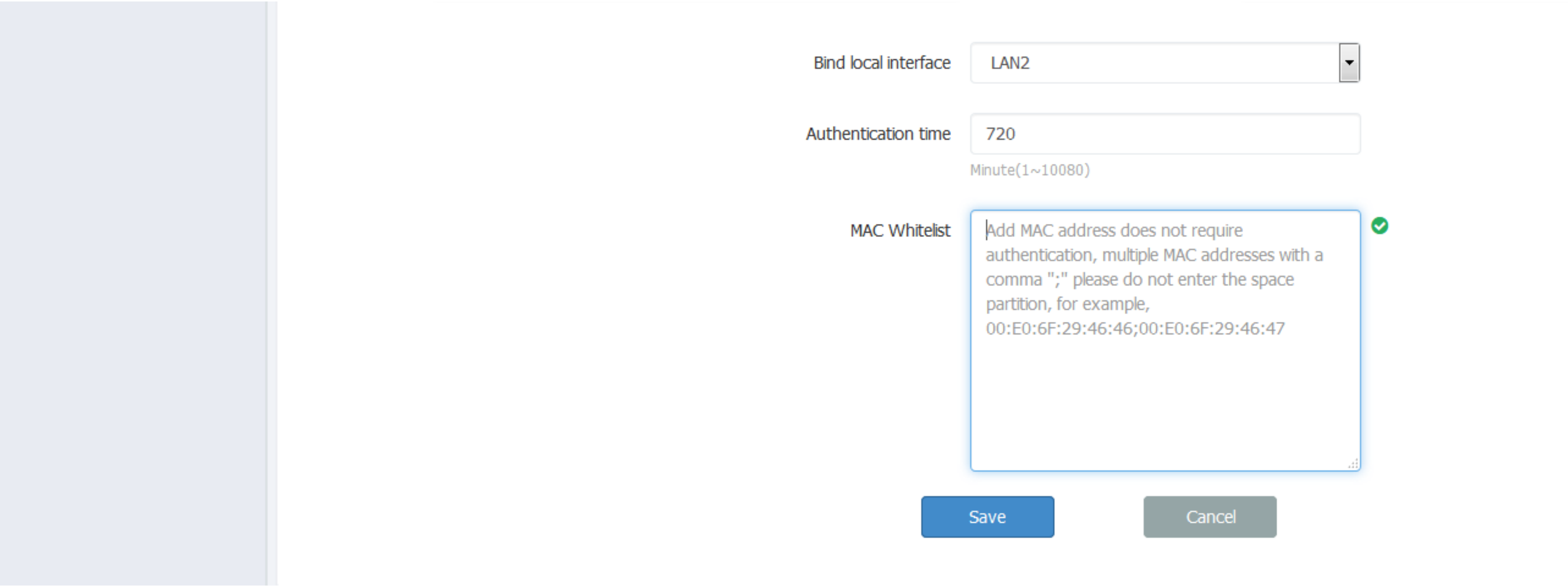
Static Picture1
Upload
Format (*.JPG,*.JPEG,*.PNG), Max Size is 500KB (Format 16:9)
Link Address: https://xontel.com/product-detail/xor
Static Pic1 Link (http or https)
Advertisement Slogan: XT-16W
Static Pic1 Ad (Limit 10 Characters)

Static Picture2
Upload
Format (*.JPG,*.JPEG,*.PNG), Max Size is 500KB (Format 16:9)
Link Address: https://xontel.com/product-detail/ip-p
Static Pic2 Link (http or https)
Advertisement Slogan: XT-30G
Static Pic2 Ad (Limit 10 Characters)

Static Picture3
Upload
Format (*.JPG,*.JPEG,*.PNG), Max Size is 500KB (Format 16:9)
Link Address: https://xontel.com/product-detail/xt-1
Static Pic3 Link (http or https)
Advertisement Slogan: XT-18P
Static Pic3 Ad (Limit 10 Characters)

Static Picture4
Upload
Format (*.JPG,*.JPEG,*.PNG), Max Size is 500KB (Format 16:9)
Link Address: https://xontel.com/product-detail/ip-d
Static Pic4 Link (http or https)
Advertisement Slogan: XT-10P
Static Pic4 Ad (Limit 10 Characters)

7. Go to “Bind local interface” below the and select the newly created LAN2 to bind with Authentication and then Save.

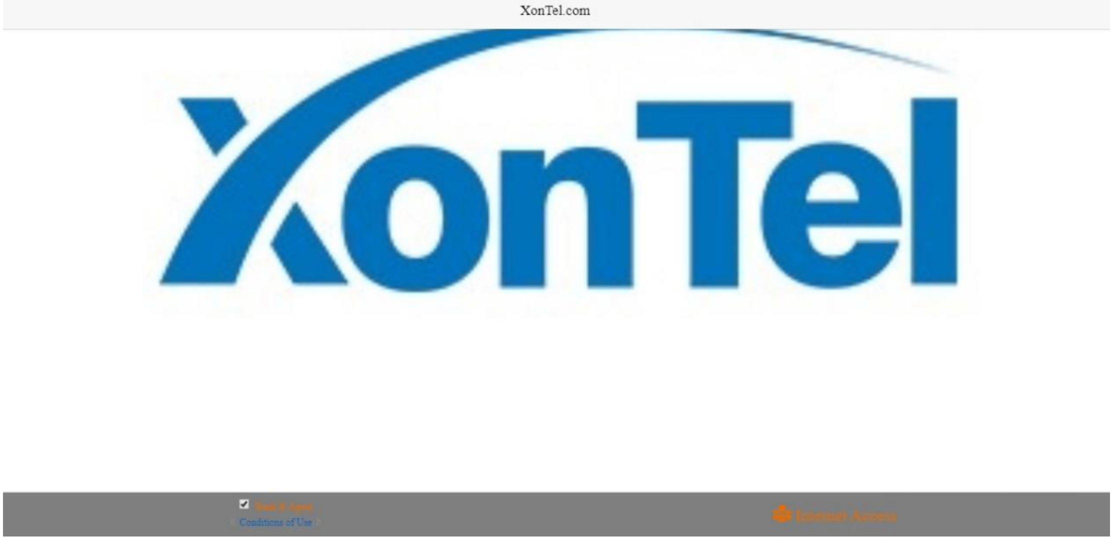


Bind local interface: LAN2

Authentication time: 720
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

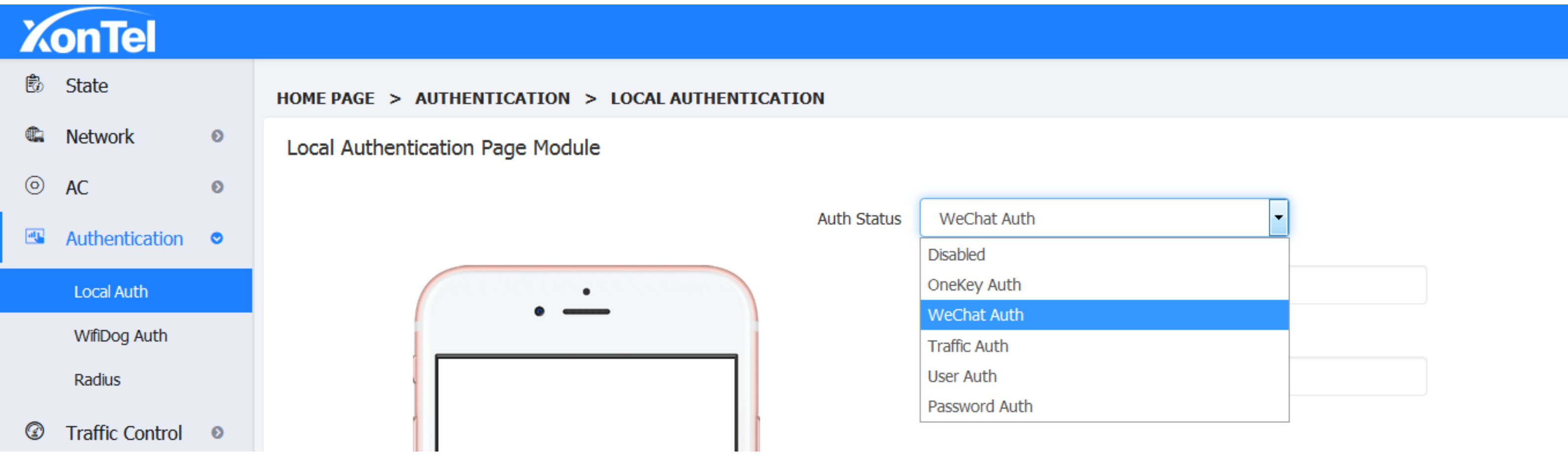
8. After finishing setup, clients connected with LAN2 Port (Direct with LAN2 or through Access Point connected on LAN2)when open any website in browser local portal page will appear and click for “Internet Access” button ,wait for 10 seconds and system will allow access for internet.



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.



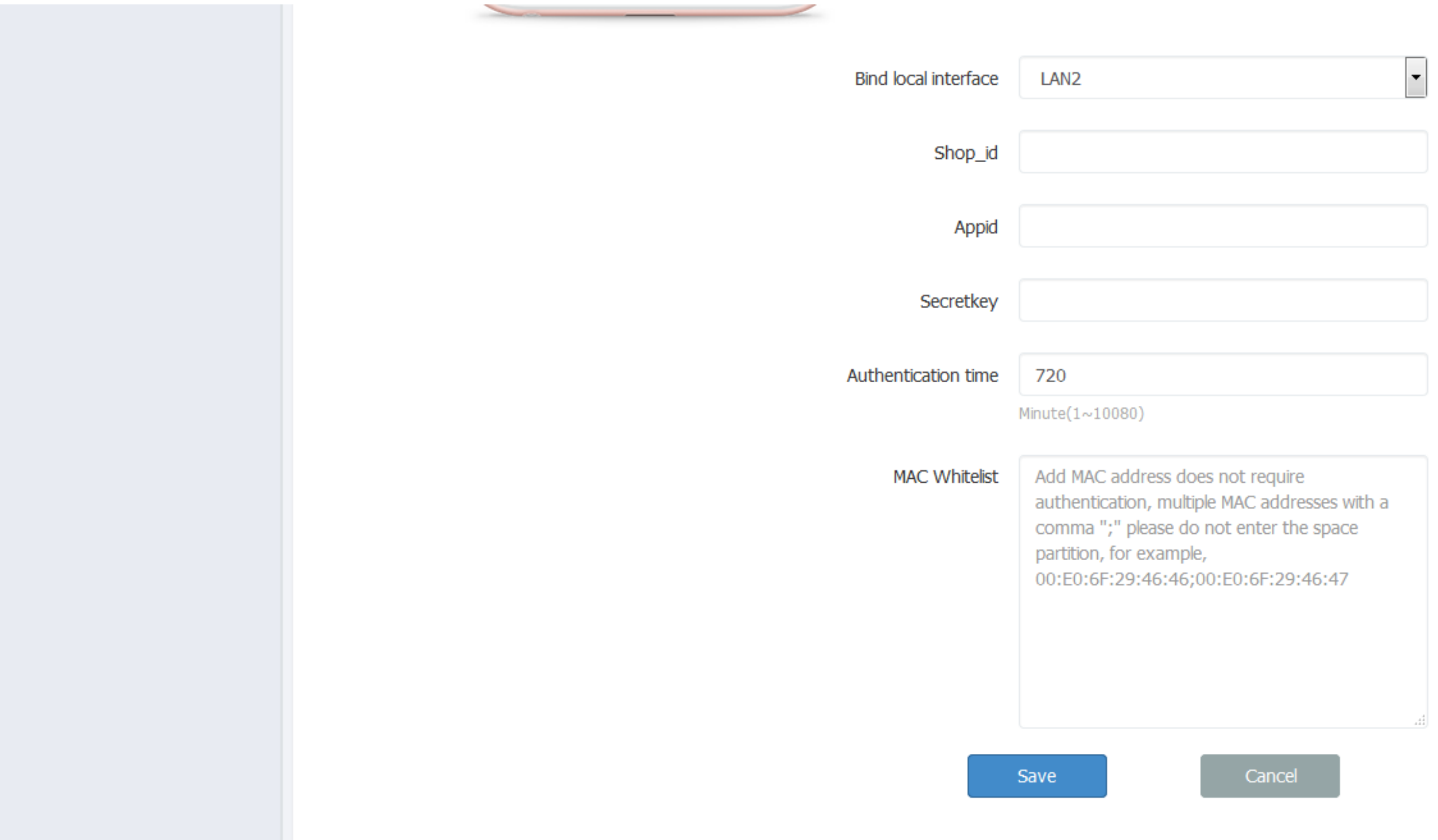
HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION

Local Authentication Page Module

Auth Status: WeChat Auth

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

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 be popping the WeChat Authentication page as below:



Bind local interface: LAN2

Shop_id:

Appid:

Secretkey:

Authentication time: 720

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

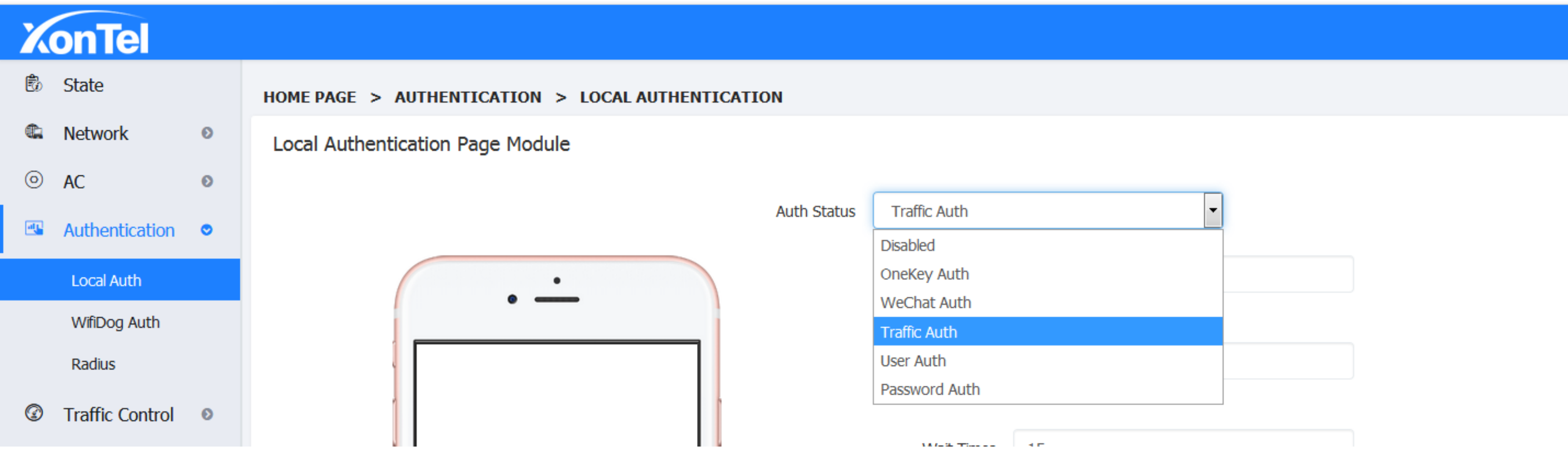
4.Click "A Key to open the WeChat connect with Wi-Fi" on the screen, then it will go into WeChat connecting Wi-Fi page.

5.Click on "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 eth0.2) need to authenticate then only access 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.

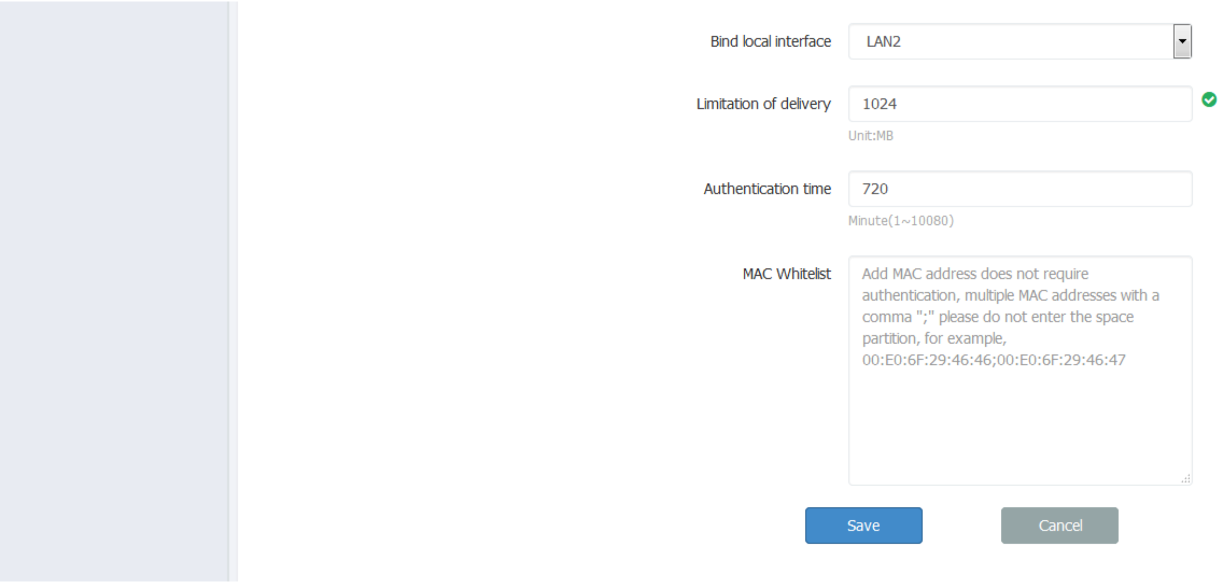


HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION

Local Authentication Page Module

Auth Status: Traffic Auth

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



Bind local interface: LAN2

Limitation of delivery: 1024
Unit:MB

Authentication time: 720
Minute(1~10080)

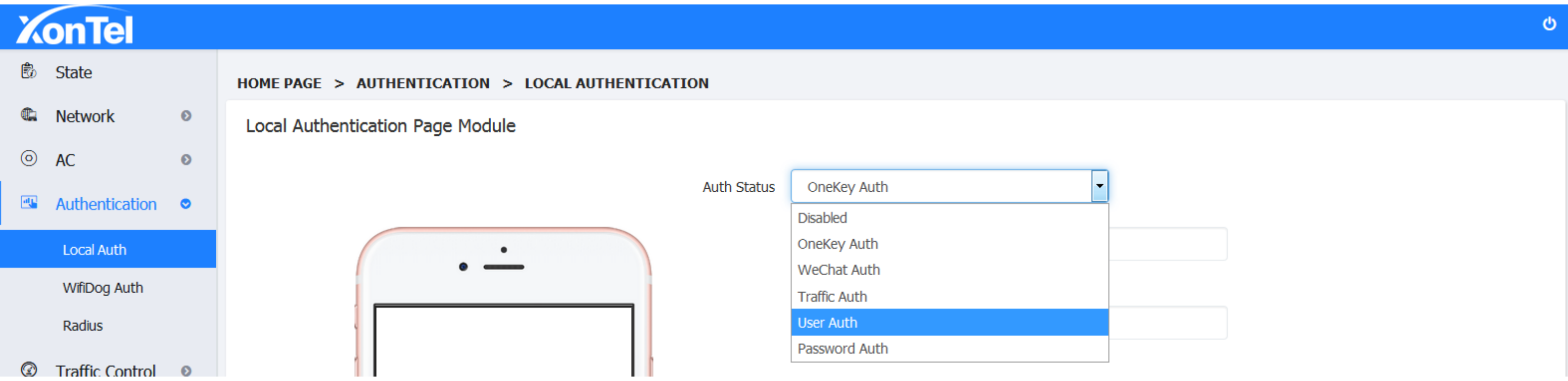
MAC Whitelist: Add MAC address does not require authentication, multiple MAC addresses with a comma ";" please do not enter the space partition, for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47

3. Once the setting is complete, after connection thought Interface LAN2, open the browser and click any website then it will pop up the traffic authentication page, after the authentication Internet can be 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: Authentication 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.

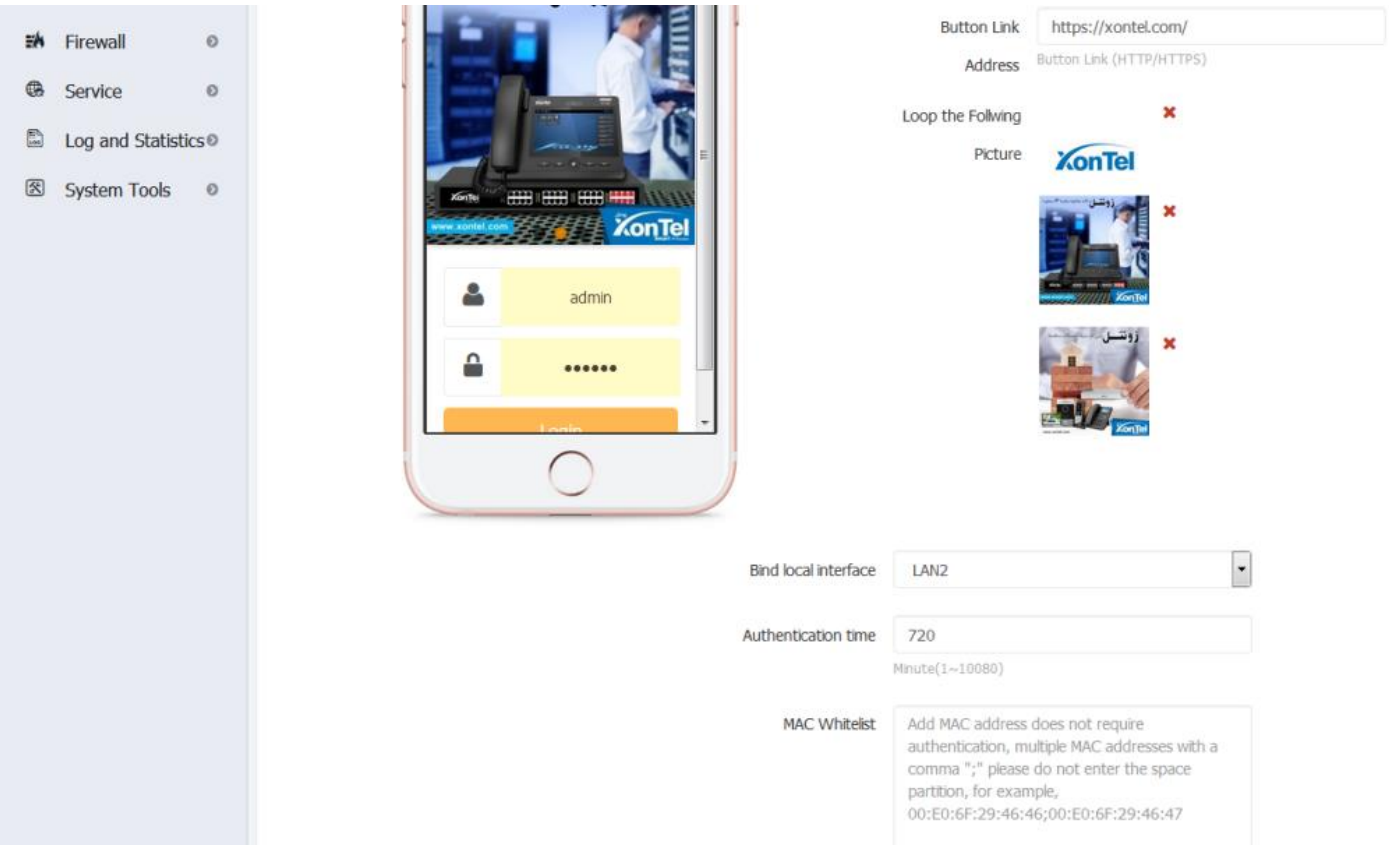


HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION

Local Authentication Page Module

Auth Status: OneKey Auth

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



Button Link Address: https://xontel.com/
Button Link (HTTP/HTTPS)

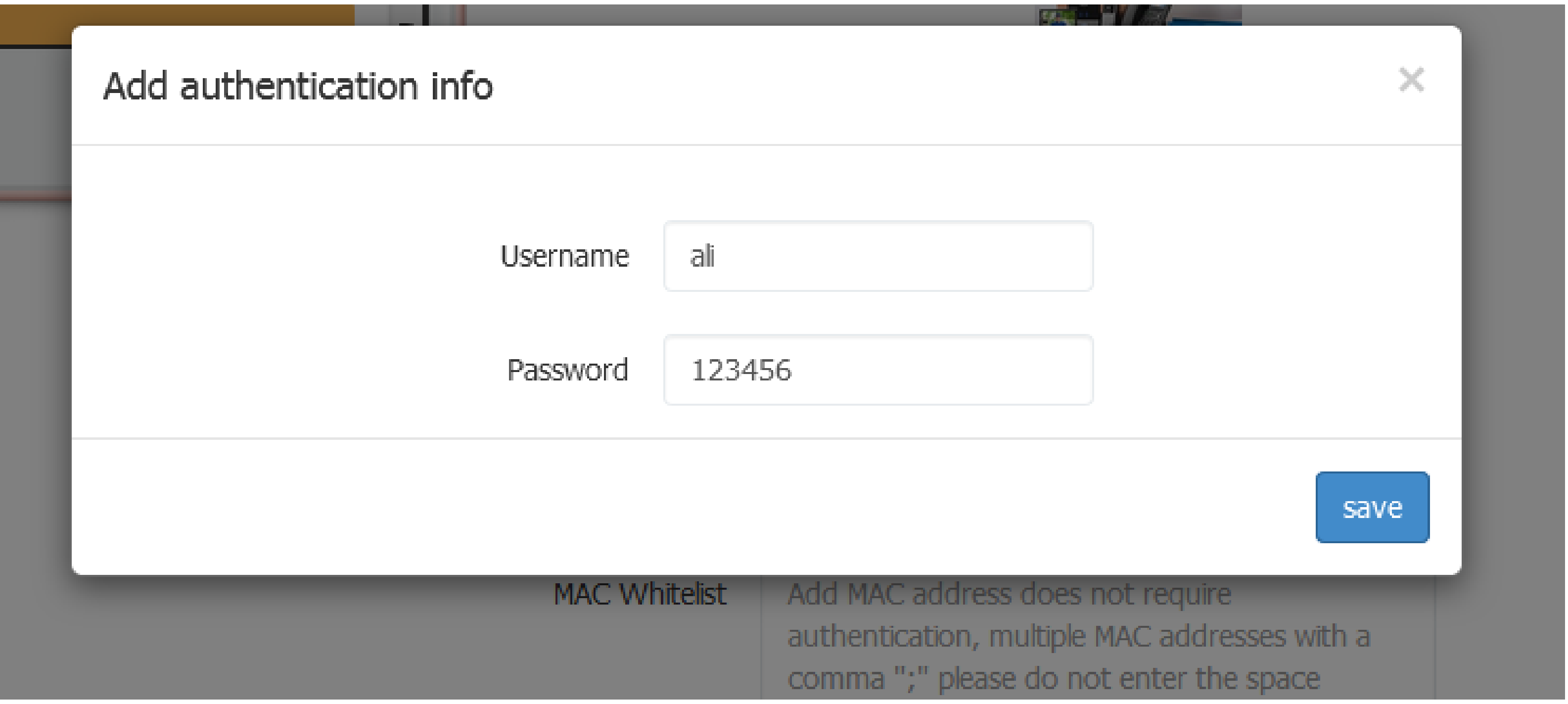
Loop the Follwing Picture

Bind local interface: LAN2

Authentication time: 720
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

3. **Add authentication user information at the bottom of the page, click the "+Add" button, enter the account username and password in the pop-up input box (e.g: ali/123456), click "Save"**

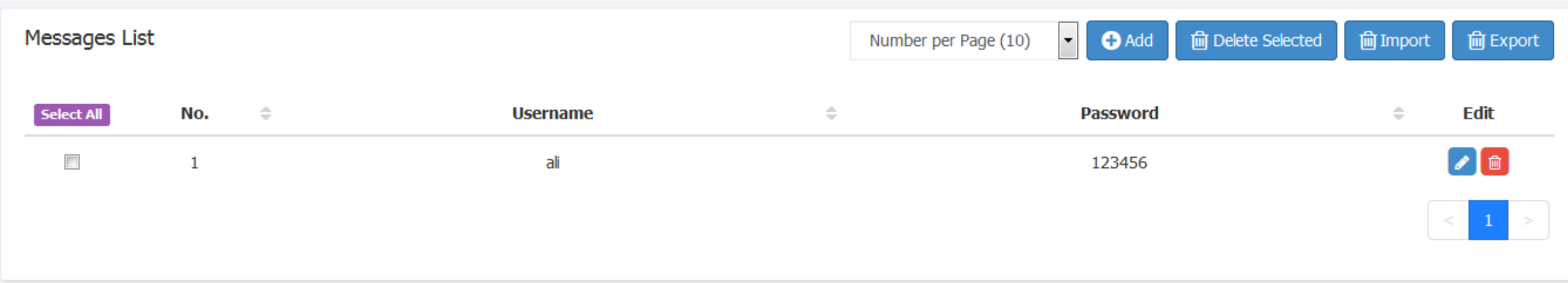


Add authentication info

Username: ali

Password: 123456

MAC Whitelist: Add MAC address does not require authentication, multiple MAC addresses with a comma ";" please do not enter the space

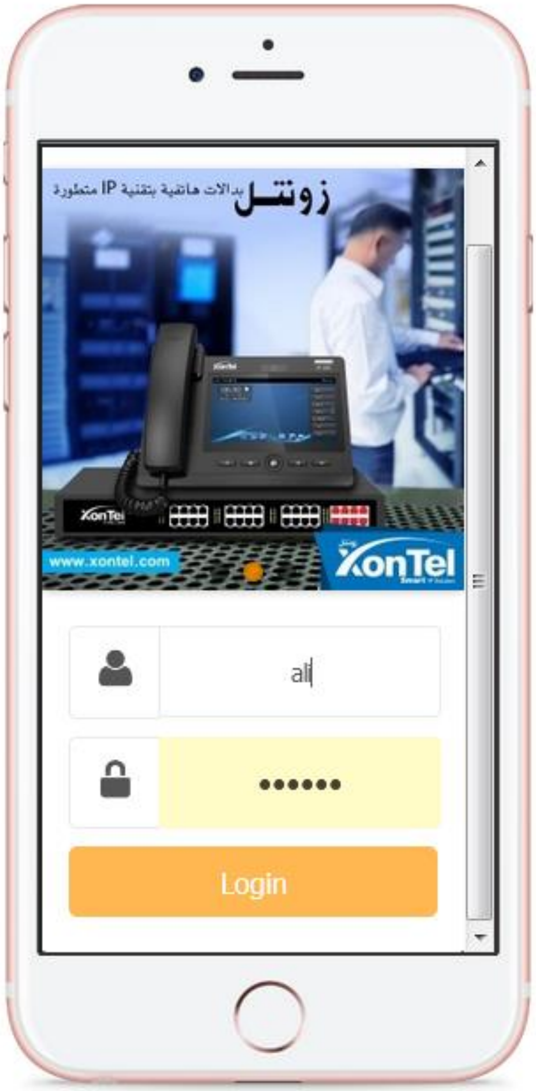


Messages List

Number per Page (10)

Select All	No.	Username	Password	Edit
☐	1	ali	123456	

4.Once the setting is complete, after connection through LAN2, open the browser and click any website then it will pop up the Authentication page as below:



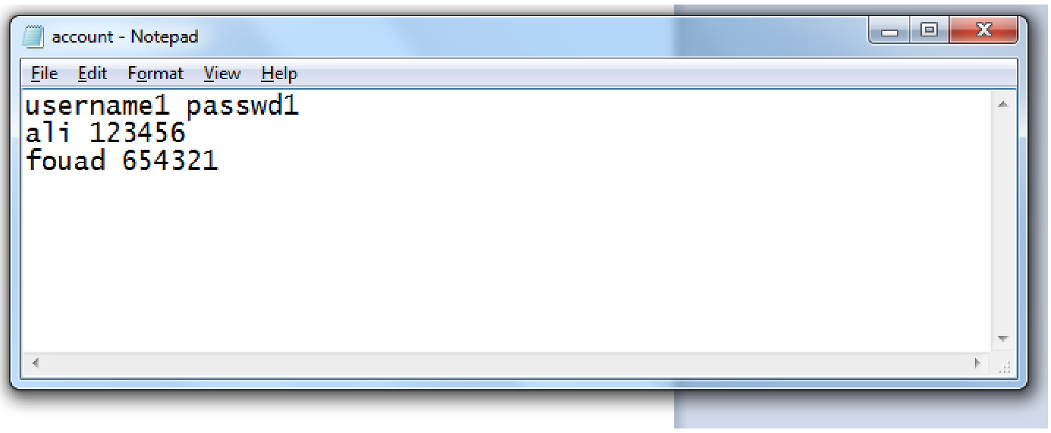
5. Enter the correct authentication password (such as: ali/123456), click on the login, automatically jump to the page after successful login, this time the certification is completed, you can normally access the Internet

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

username1 passwd1

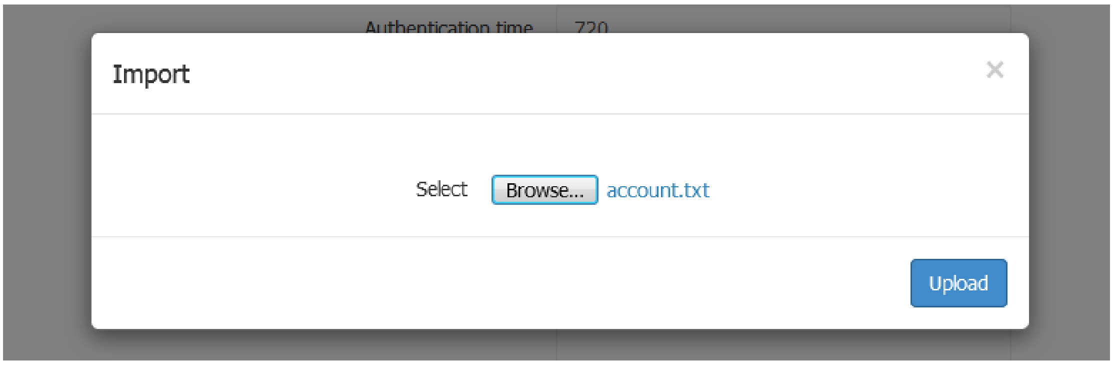
username2 passwd2

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

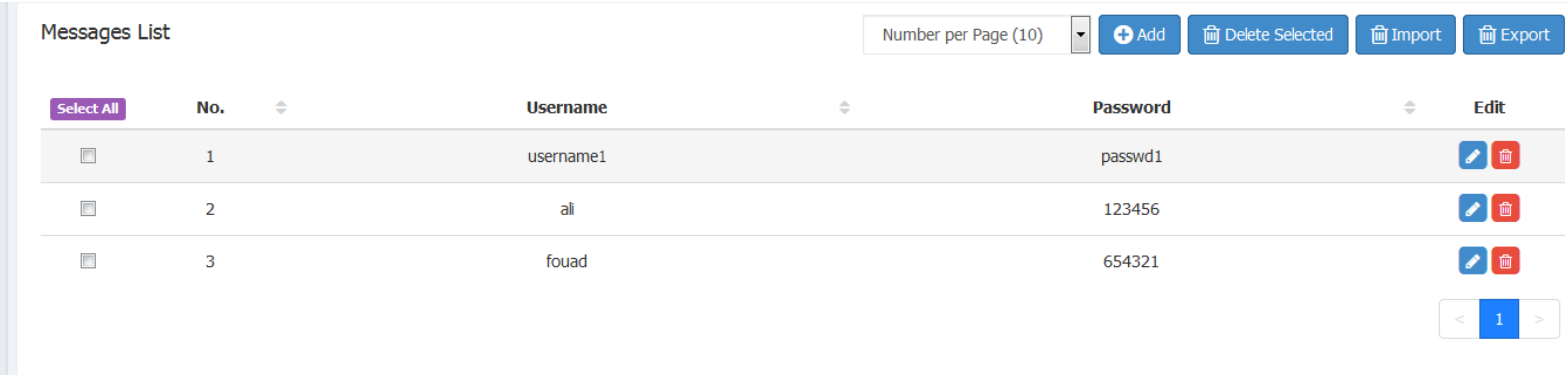


```
username1 passwd1
ali 123456
fouad 654321
```

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 previously added accounts in advance.

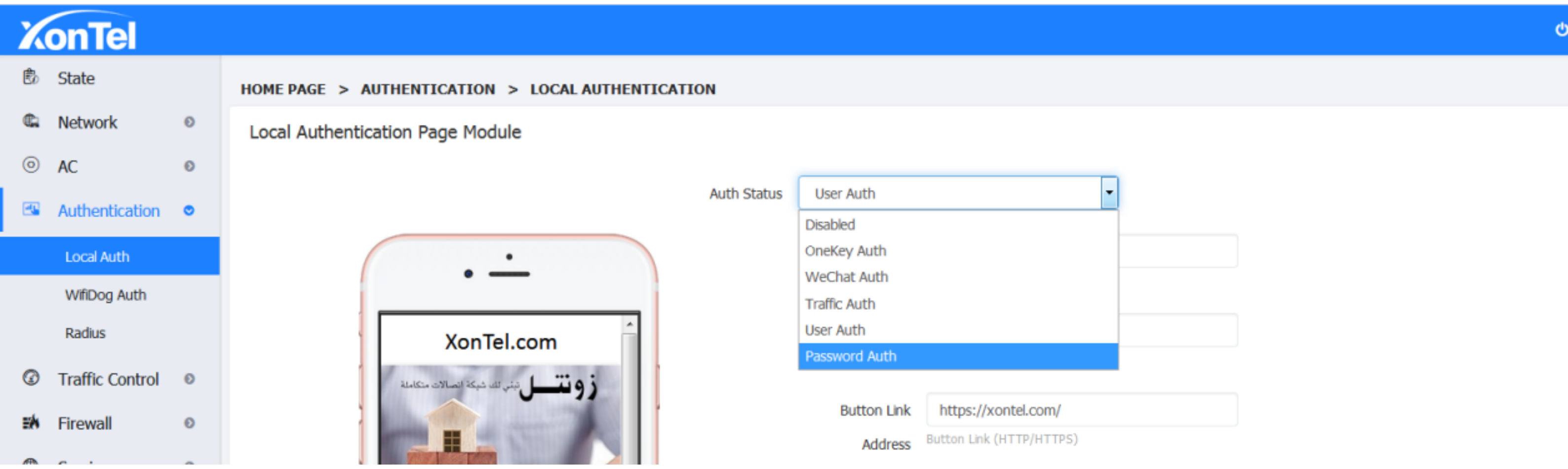


Select All	No.	Username	Password	Edit
□	1	username1	passwd1	
□	2	ali	123456	
□	3	fouad	654321	

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

5.1.5 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.



HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION

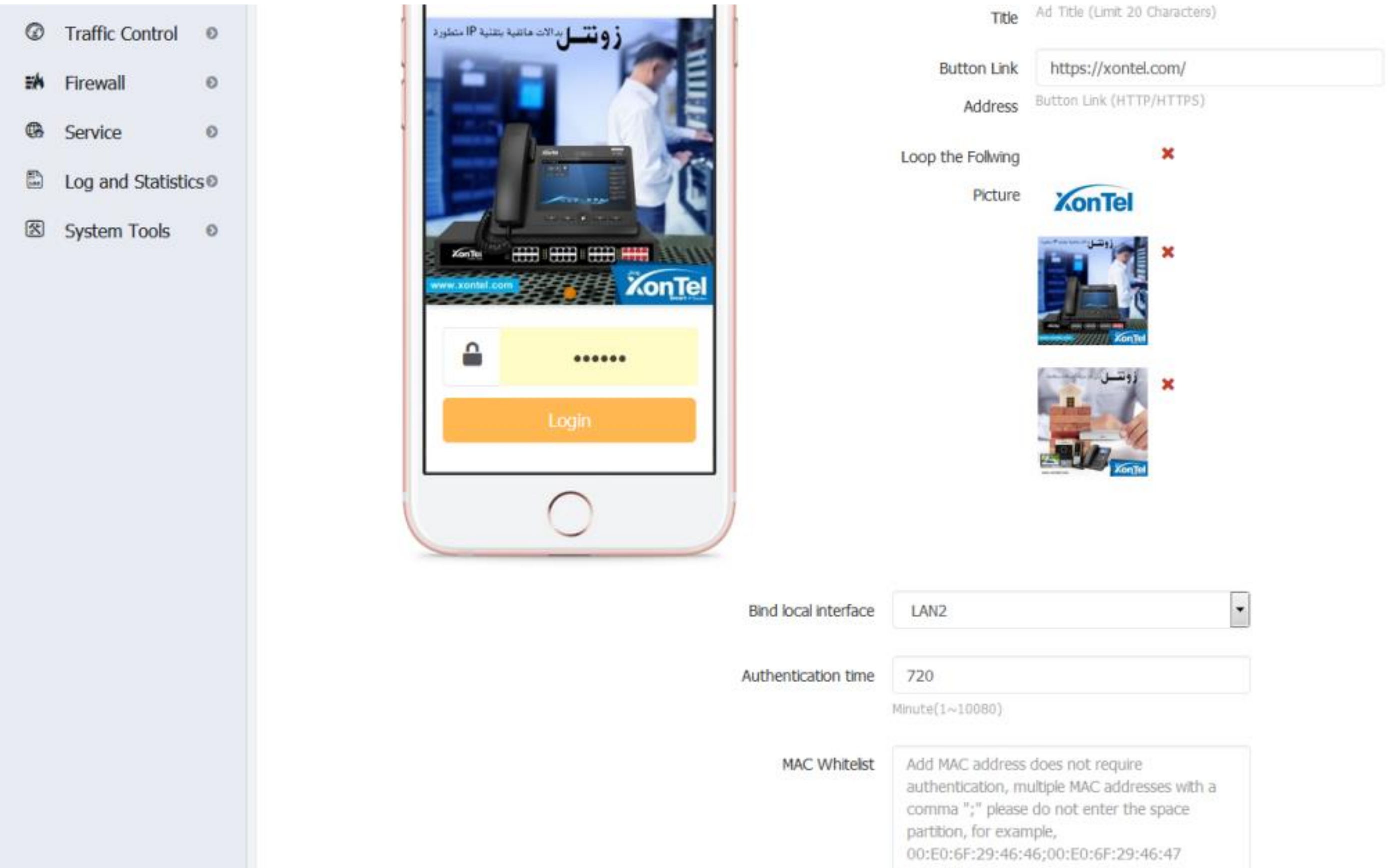
Local Authentication Page Module

Auth Status: User Auth

- Disabled
- OneKey Auth
- WeChat Auth
- Traffic Auth
- User Auth
- Password Auth

Button Link Address: https://xontel.com/
Button Link (HTTP/HTTPS)

2. Bind local interface- Select LAN2 port, set the authentication duration.



Title: Ad Title (Limit 20 Characters)

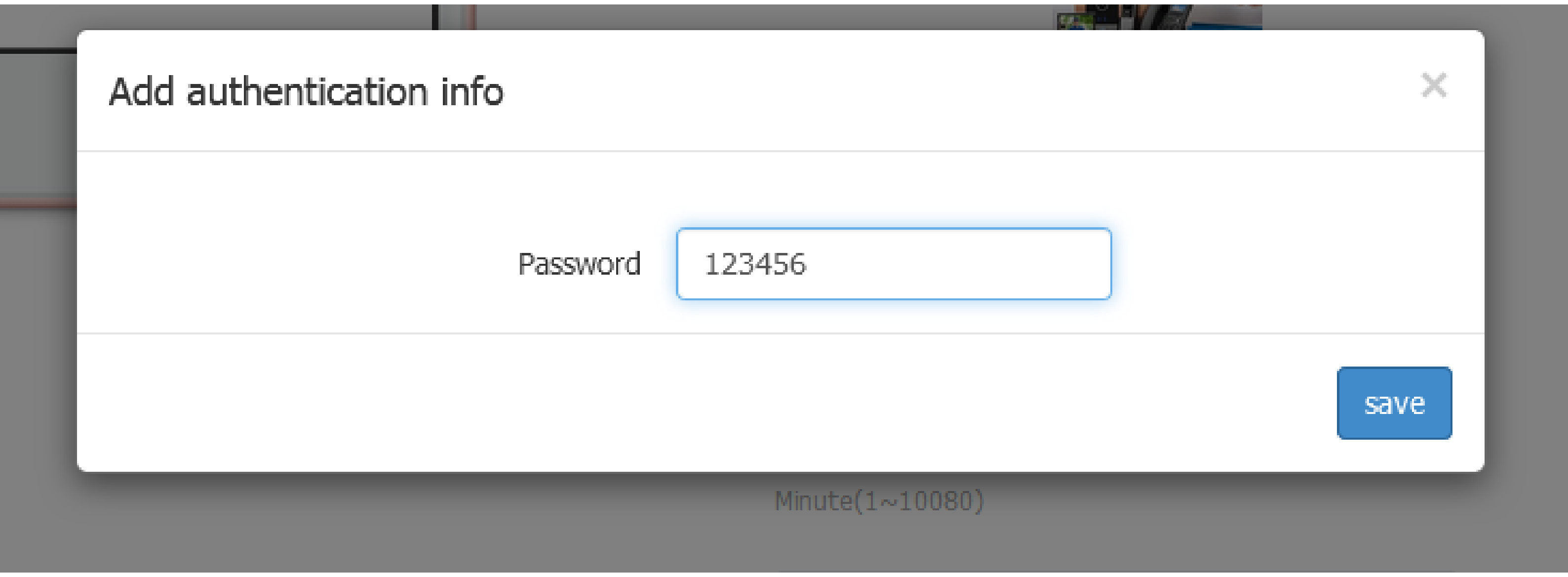
Button Link Address: https://xontel.com/
Button Link (HTTP/HTTPS)

Bind local interface: LAN2

Authentication time: 720
Minute(1~10080)

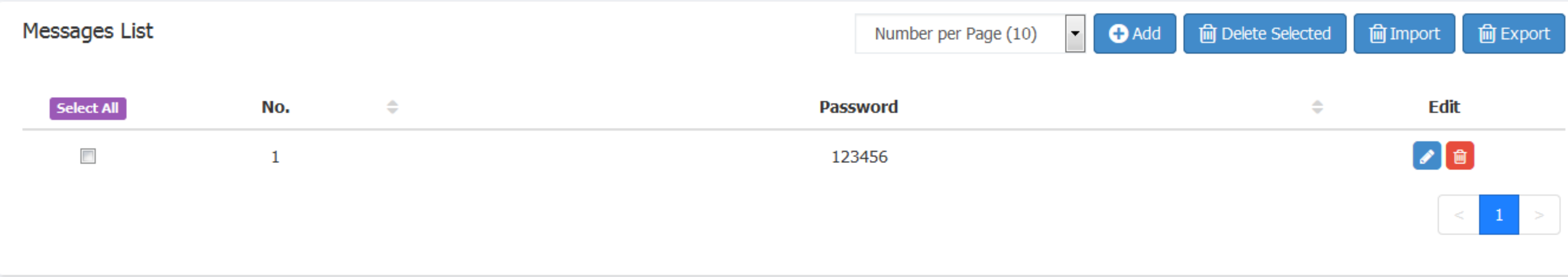
MAC Whitelist: Add MAC address does not require authentication, multiple MAC addresses with a comma ";" please do not enter the space partition, for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47

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 (e.g: 123456), click "Save"



Add authentication info

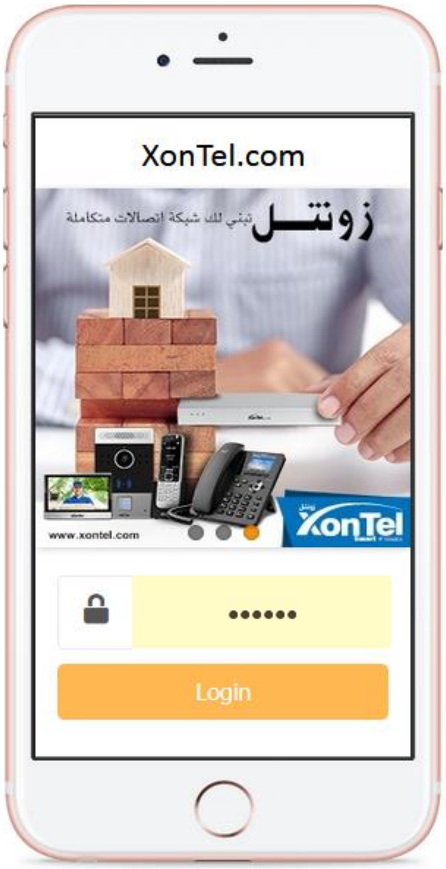
Password: 123456



Messages List

Select All	No.	Password	Edit
□	1	123456	✎ 🗑

4.Once the setting is complete, after connection through LAN2, open the browser and click any website then it will pop up the Authentication page as below:



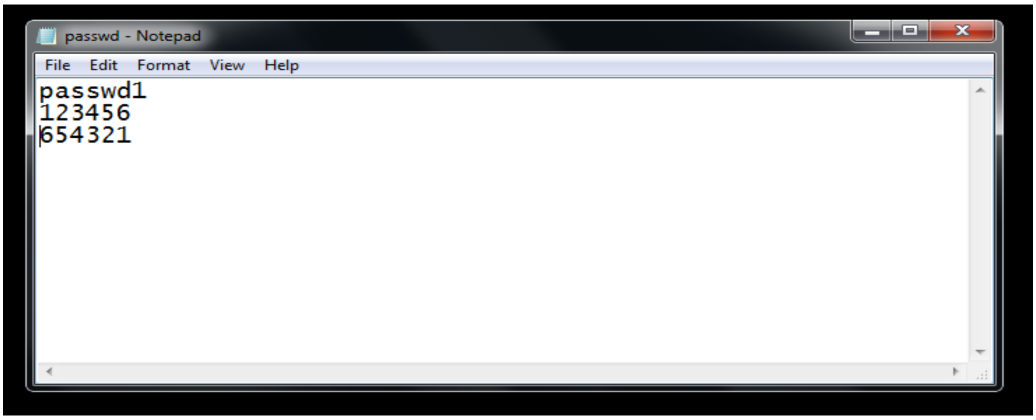
4. Enter the correct password (such as: 123456), click on the login, automatically jump to the page after successful login, this time the authentication is completed, you can normally access the Internet.

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

passwd1

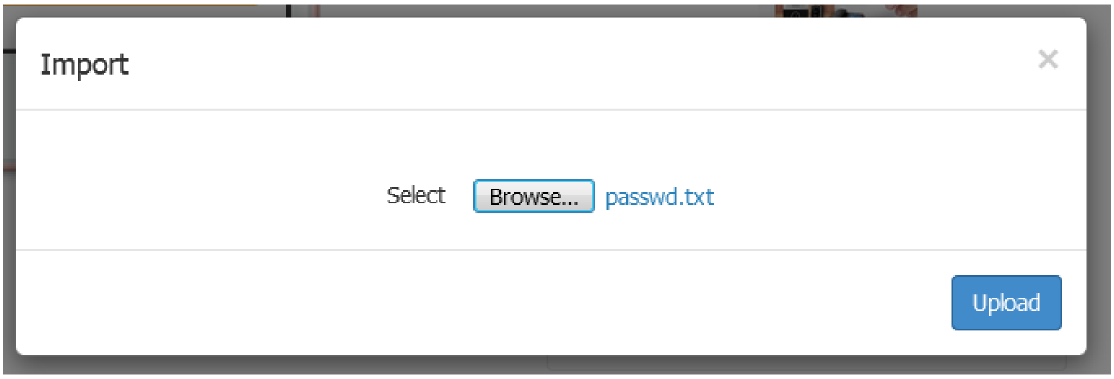
passwd2

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



```
passwd1
123456
654321
```

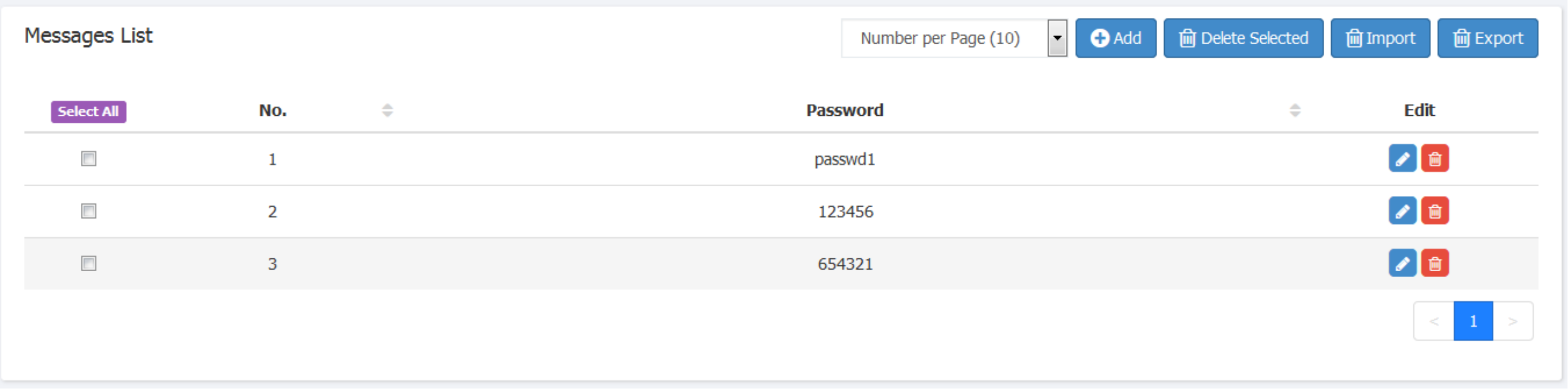
Click the Import File button and select the file passwd.txt:



Import

Select Browse... passwd.txt

You can see that the passwords 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.



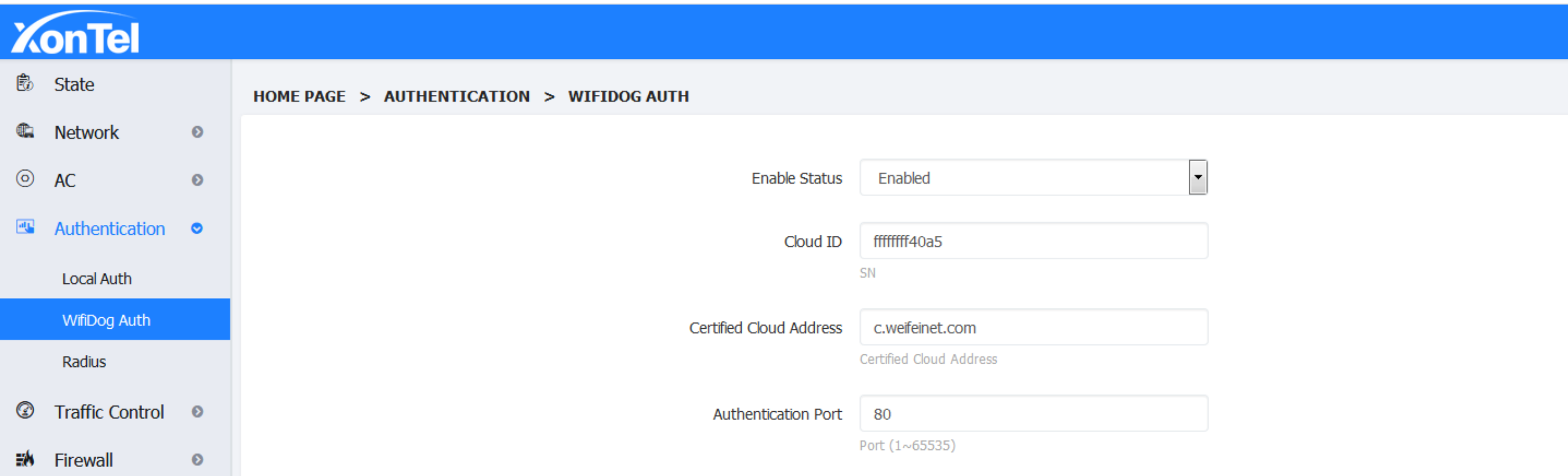
Messages List

Select All	No.	Password	Edit
□	1	passwd1	
□	2	123456	
□	3	654321	

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

5.2 WifiDog Auth

1. Go to" Authentication" ---" WifiDog Auth", then choose the status as Enable setup relative parameters click save button.



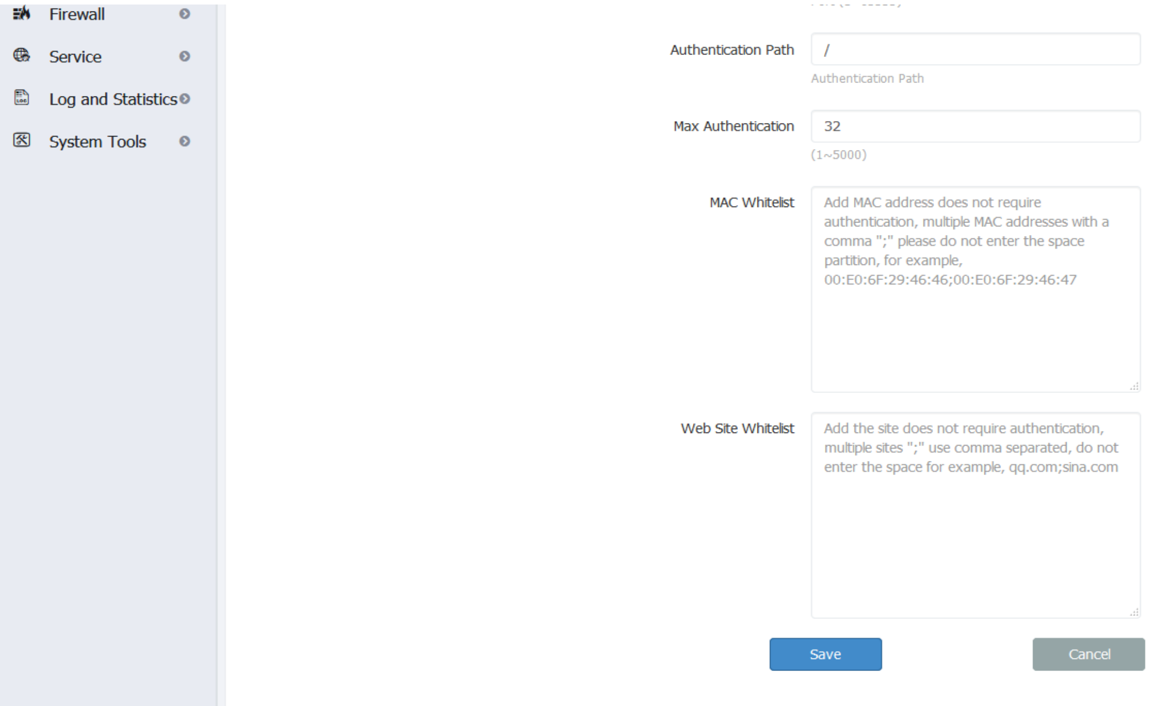
HOME PAGE > AUTHENTICATION > WIFIDOG AUTH

Enable Status: Enabled

Cloud ID: ffffffff40a5
SN

Certified Cloud Address: c.weifeinet.com
Certified Cloud Address

Authentication Port: 80
Port (1~65535)



Authentication Path: /
Authentication Path

Max Authentication: 32
(1~5000)

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

Web Site Whitelist: Add the site does not require authentication, multiple sites ";" use comma separated, do not enter the space for example, qq.com;sina.com

2.Open the browser in the local computer open the other website which are not in the "Website White list" system will pop up the authentication page.

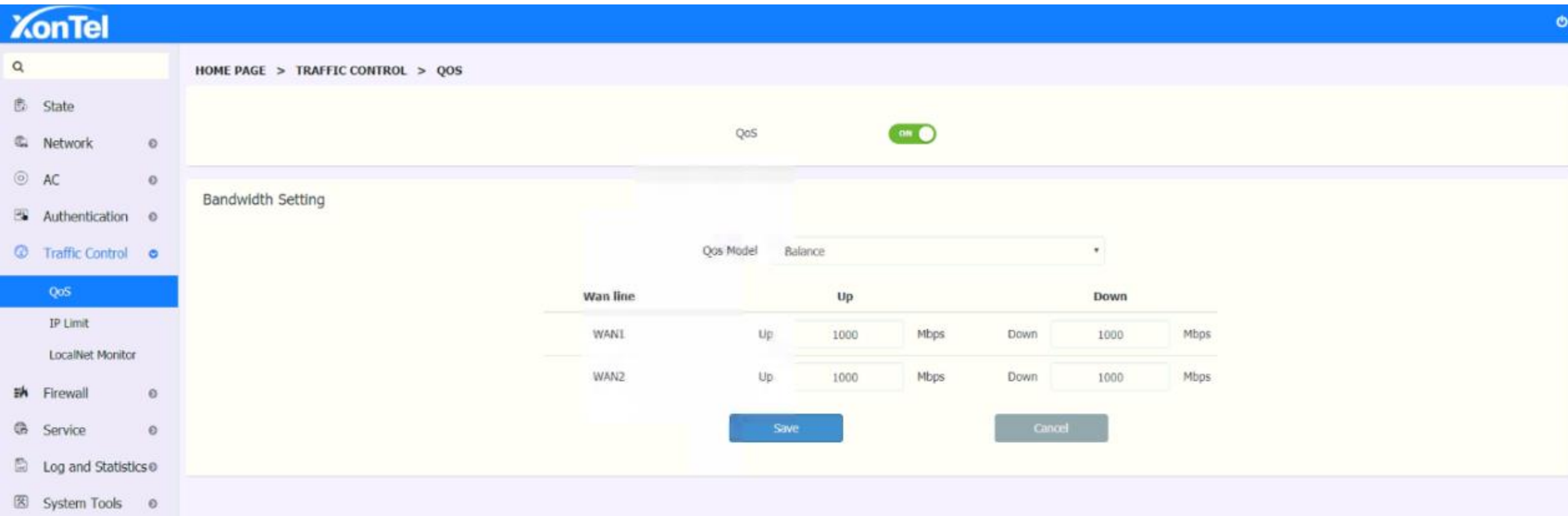
3.Use device's MAC address to add to white list to open the browser and system will not pop up the authentication page in any websites.

6 Traffic Control

6.1 QoS

When there 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 QoS page setup the relative parameters, fill in the actual UP/Down bandwidth according to the bandwidth of each external network, and click save button as below:



HOME PAGE > TRAFFIC CONTROL > QOS

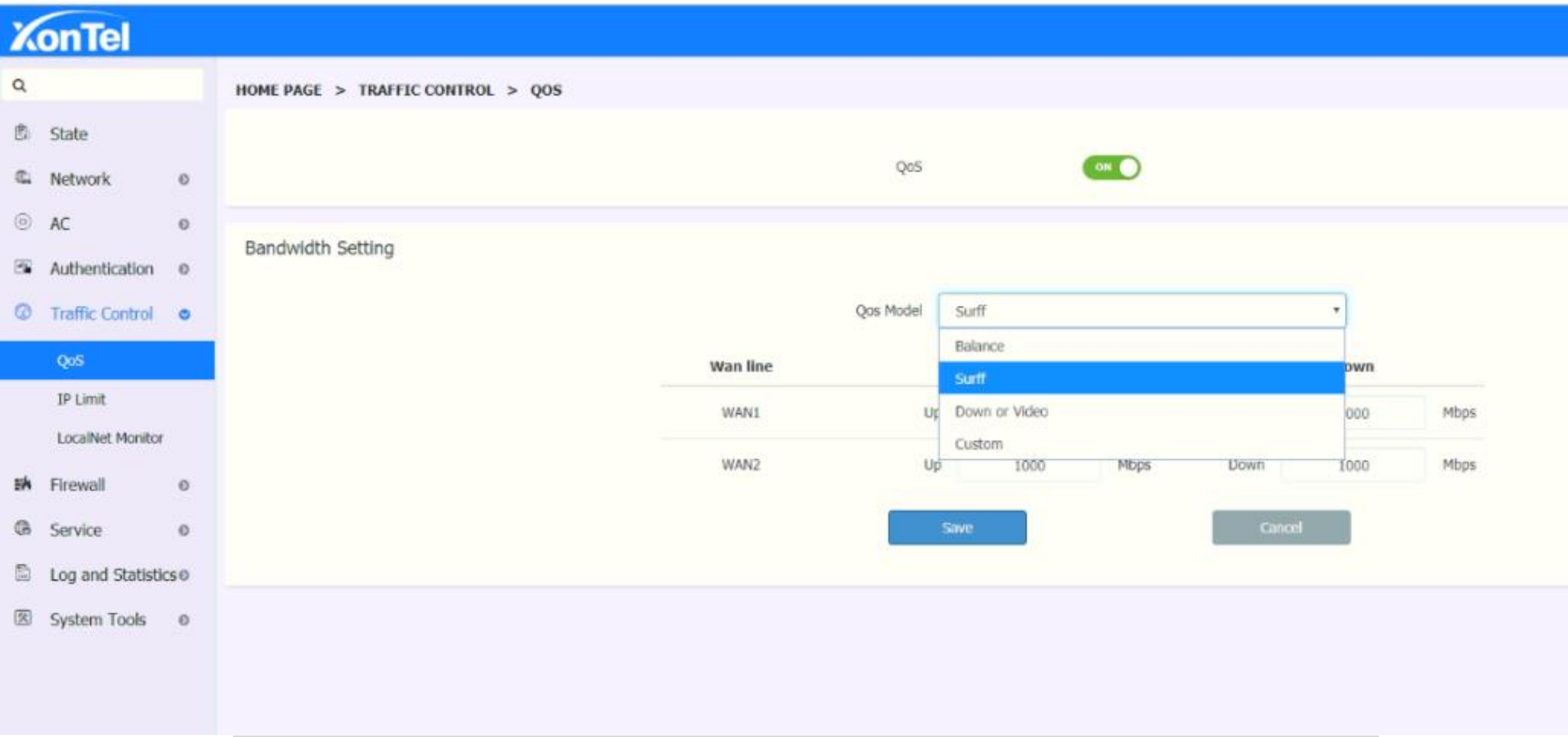
QoS: ON

Bandwidth Setting

Qos Model: Balance

Wan line		Up			Down	
WAN1	Up	1000	Mbps	Down	1000	Mbps
WAN2	Up	1000	Mbps	Down	1000	Mbps

2. The line flow control mode can be adjusted according to the actual usage of the clients:



HOME PAGE > TRAFFIC CONTROL > QOS

QoS: ON

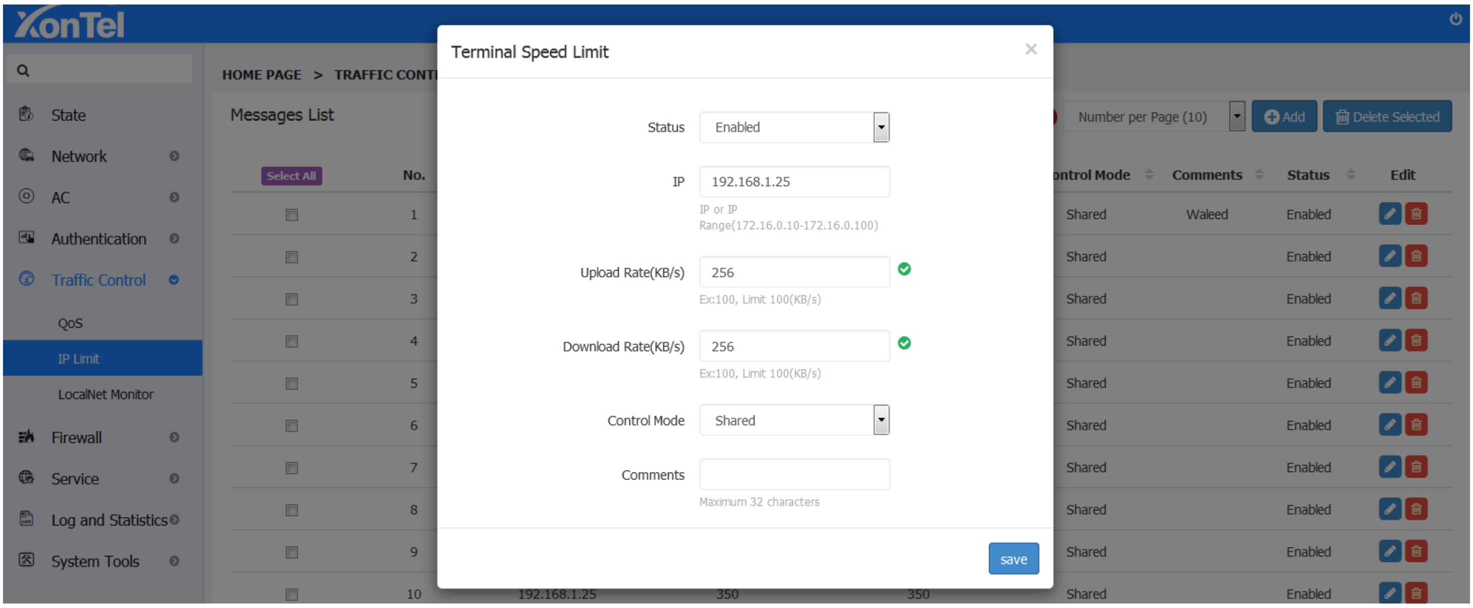
Bandwidth Setting

Qos Model: Surf

6.2 IP Limit

System can control the uplink and downlink traffic of single user according to the IP address.

1. Go into the IP LIMIT page, add a single IP speed limit information, e.g. IP: 192.168.1.30, up and down rate are 256 and 256, then the user's uplink and downlink speed values should be same.



Terminal Speed Limit

Status: Enabled

IP: 192.168.1.25
IP or IP Range(172.16.0.10-172.16.0.100)

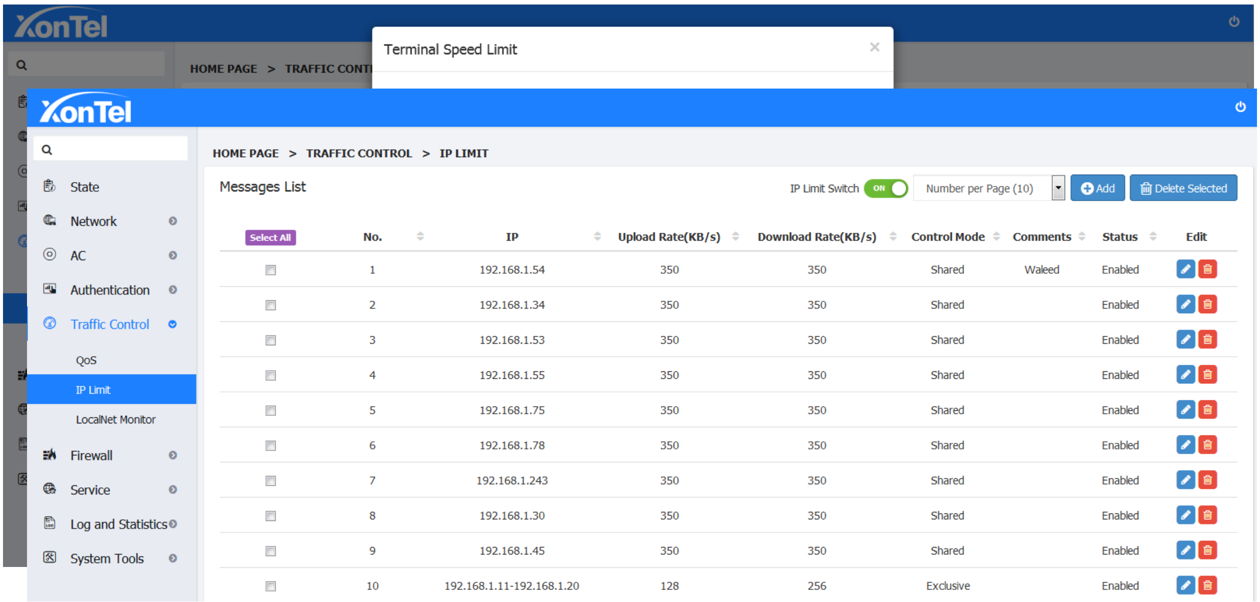
Upload Rate(KB/s): 256
Ex:100, Limit 100(KB/s)

Download Rate(KB/s): 256
Ex:100, Limit 100(KB/s)

Control Mode: Shared

Comments:
Maximum 32 characters

2. Speed Limit for Range of IPs: Go to the IP Limit page and add the IP range limit information, e.g. IP: 192.168.1.11-192.168.1.20, with 128 and 256 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.

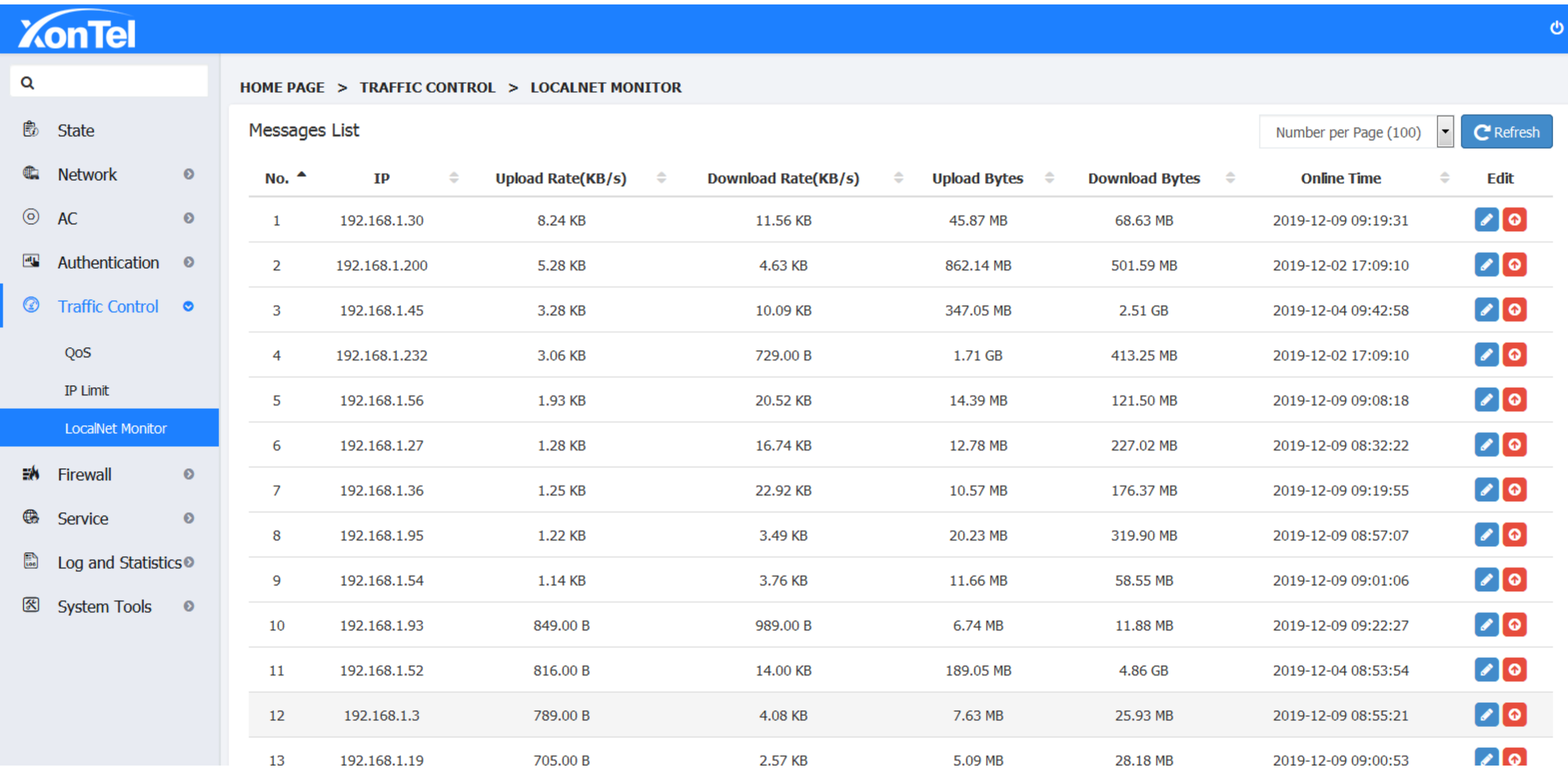


Select All	No.	IP	Upload Rate(KB/s)	Download Rate(KB/s)	Control Mode	Comments	Status	Edit
□	1	192.168.1.54	350	350	Shared	Waleed	Enabled	
□	2	192.168.1.34	350	350	Shared		Enabled	
□	3	192.168.1.53	350	350	Shared		Enabled	
□	4	192.168.1.55	350	350	Shared		Enabled	
□	5	192.168.1.75	350	350	Shared		Enabled	
□	6	192.168.1.78	350	350	Shared		Enabled	
□	7	192.168.1.243	350	350	Shared		Enabled	
□	8	192.168.1.30	350	350	Shared		Enabled	
□	9	192.168.1.45	350	350	Shared		Enabled	
□	10	192.168.1.11-192.168.1.20	128	256	Exclusive		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.

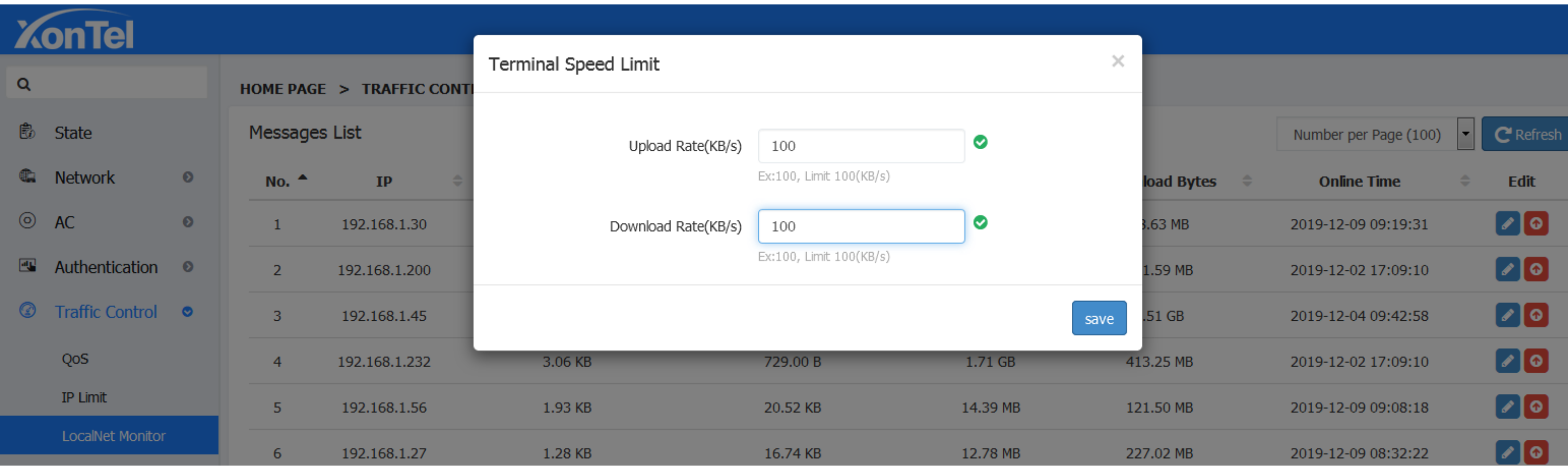


HOME PAGE > TRAFFIC CONTROL > LOCALNET MONITOR

Messages List

No.	IP	Upload Rate(KB/s)	Download Rate(KB/s)	Upload Bytes	Download Bytes	Online Time	Edit
1	192.168.1.30	8.24 KB	11.56 KB	45.87 MB	68.63 MB	2019-12-09 09:19:31	
2	192.168.1.200	5.28 KB	4.63 KB	862.14 MB	501.59 MB	2019-12-02 17:09:10	
3	192.168.1.45	3.28 KB	10.09 KB	347.05 MB	2.51 GB	2019-12-04 09:42:58	
4	192.168.1.232	3.06 KB	729.00 B	1.71 GB	413.25 MB	2019-12-02 17:09:10	
5	192.168.1.56	1.93 KB	20.52 KB	14.39 MB	121.50 MB	2019-12-09 09:08:18	
6	192.168.1.27	1.28 KB	16.74 KB	12.78 MB	227.02 MB	2019-12-09 08:32:22	
7	192.168.1.36	1.25 KB	22.92 KB	10.57 MB	176.37 MB	2019-12-09 09:19:55	
8	192.168.1.95	1.22 KB	3.49 KB	20.23 MB	319.90 MB	2019-12-09 08:57:07	
9	192.168.1.54	1.14 KB	3.76 KB	11.66 MB	58.55 MB	2019-12-09 09:01:06	
10	192.168.1.93	849.00 B	989.00 B	6.74 MB	11.88 MB	2019-12-09 09:22:27	
11	192.168.1.52	816.00 B	14.00 KB	189.05 MB	4.86 GB	2019-12-04 08:53:54	
12	192.168.1.3	789.00 B	4.08 KB	7.63 MB	25.93 MB	2019-12-09 08:55:21	
13	192.168.1.19	705.00 B	2.57 KB	5.09 MB	28.18 MB	2019-12-09 09:00:53	

2. Click on the 'Edit' icon of any user, to setup single IP speed limit of that user:

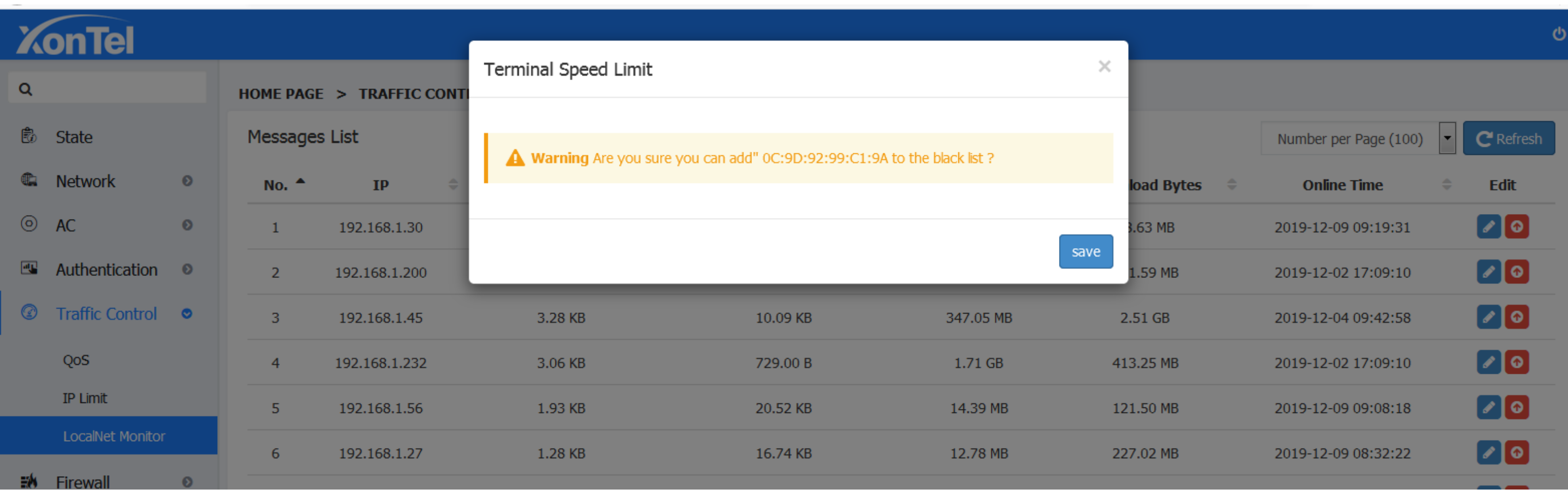


Terminal Speed Limit

Upload Rate(KB/s): 100
Ex:100, Limit 100(KB/s)

Download Rate(KB/s): 100
Ex:100, Limit 100(KB/s)

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



Terminal Speed Limit

⚠ **Warning** Are you sure you can add" 0C:9D:92:99:C1:9A to the black list ?

save

Messages List

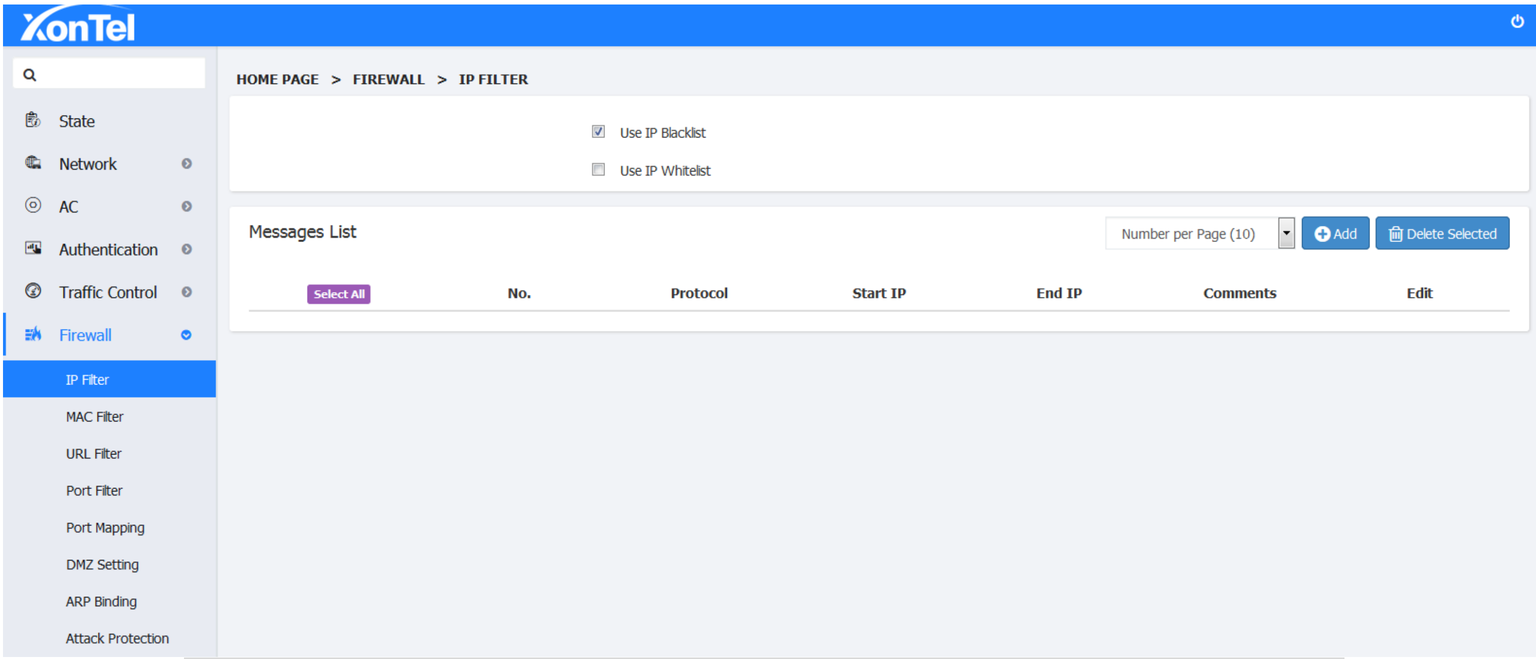
No.	IP				load Bytes	Online Time	Edit
1	192.168.1.30				.63 MB	2019-12-09 09:19:31	
2	192.168.1.200				1.59 MB	2019-12-02 17:09:10	
3	192.168.1.45	3.28 KB	10.09 KB	347.05 MB	2.51 GB	2019-12-04 09:42:58	
4	192.168.1.232	3.06 KB	729.00 B	1.71 GB	413.25 MB	2019-12-02 17:09:10	
5	192.168.1.56	1.93 KB	20.52 KB	14.39 MB	121.50 MB	2019-12-09 09:08:18	
6	192.168.1.27	1.28 KB	16.74 KB	12.78 MB	227.02 MB	2019-12-09 08:32:22	

7 Firewall

7.1 IP Filter

Here you must know the IP of 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:



HOME PAGE > FIREWALL > IP FILTER

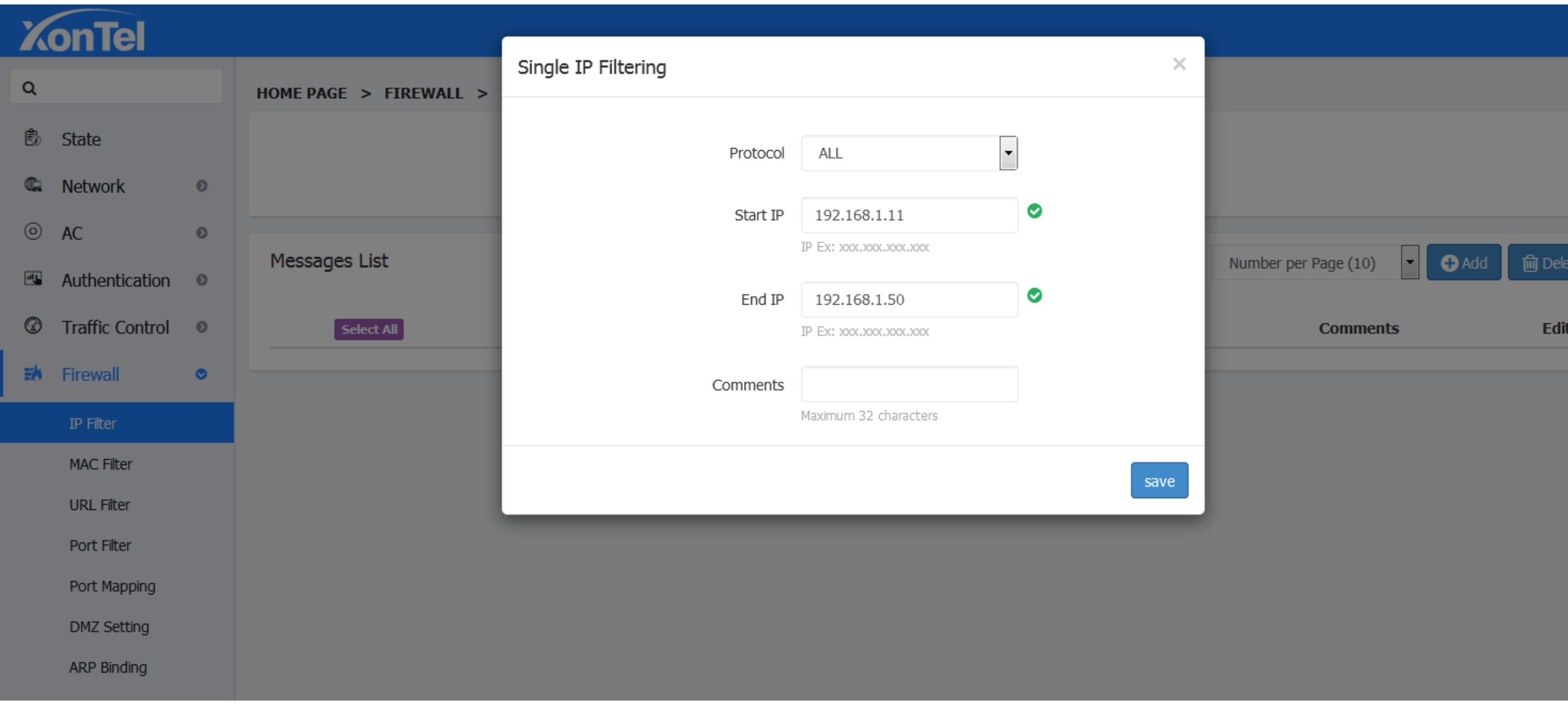
☑ Use IP Blacklist

□ Use IP Whitelist

Messages List

Select All	No.	Protocol	Start IP	End IP	Comments	Edit

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



Single IP Filtering

Protocol: ALL

Start IP: 192.168.1.11

IP Ex: xxx.xxx.xxx.xxx

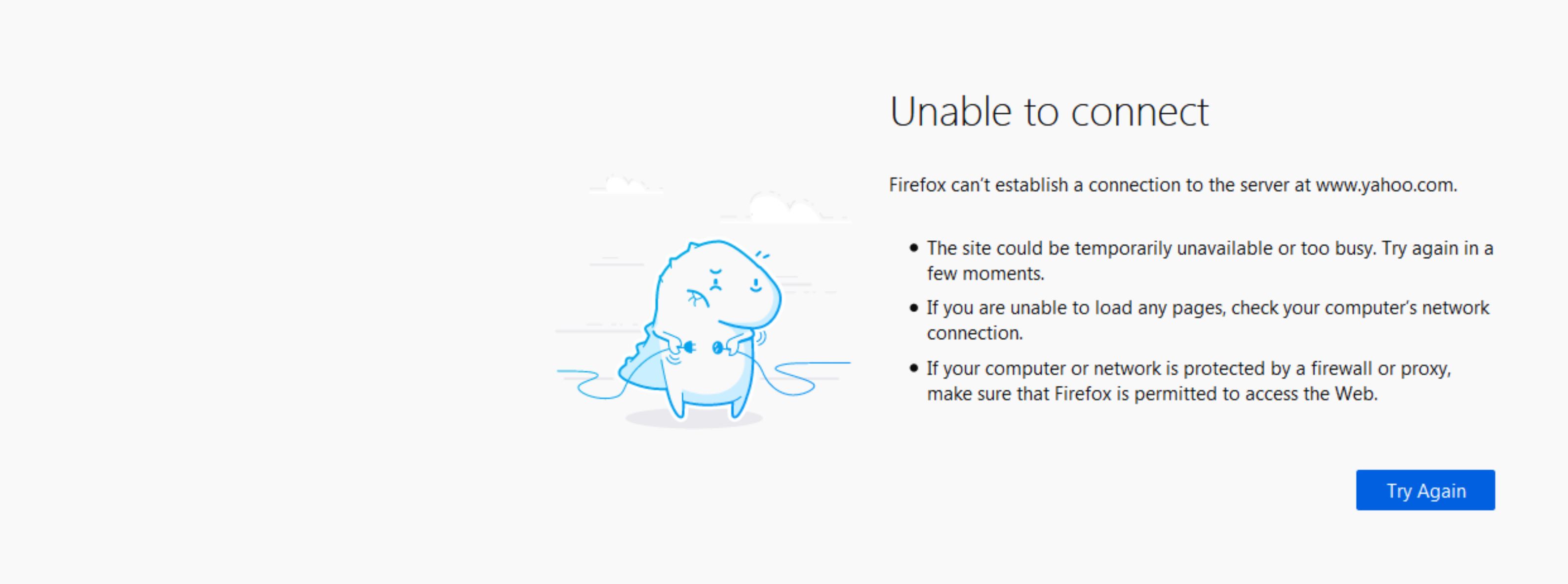
End IP: 192.168.1.50

IP Ex: xxx.xxx.xxx.xxx

Comments:

Maximum 32 characters

3.Open the native’s browser and it cannot open the website normally because the native IP:192.168.1.11 is in the IP Black List range:

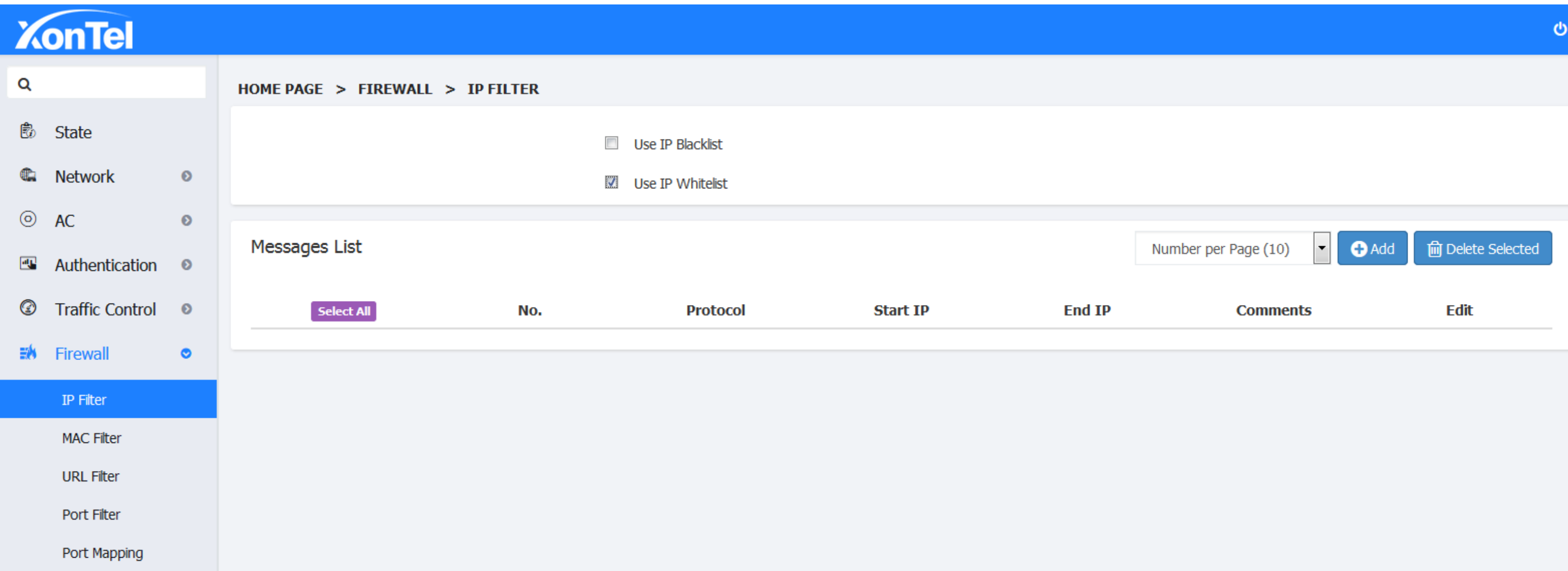


Unable to connect

Firefox can’t establish a connection to the server at www.yahoo.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

4. Switch to the White list. Only users in the White list can access the Internet. Other users cannot access the Internet. (Use this option with caution)



HOME PAGE > FIREWALL > IP FILTER

☐ Use IP Blacklist

☑ Use IP Whitelist

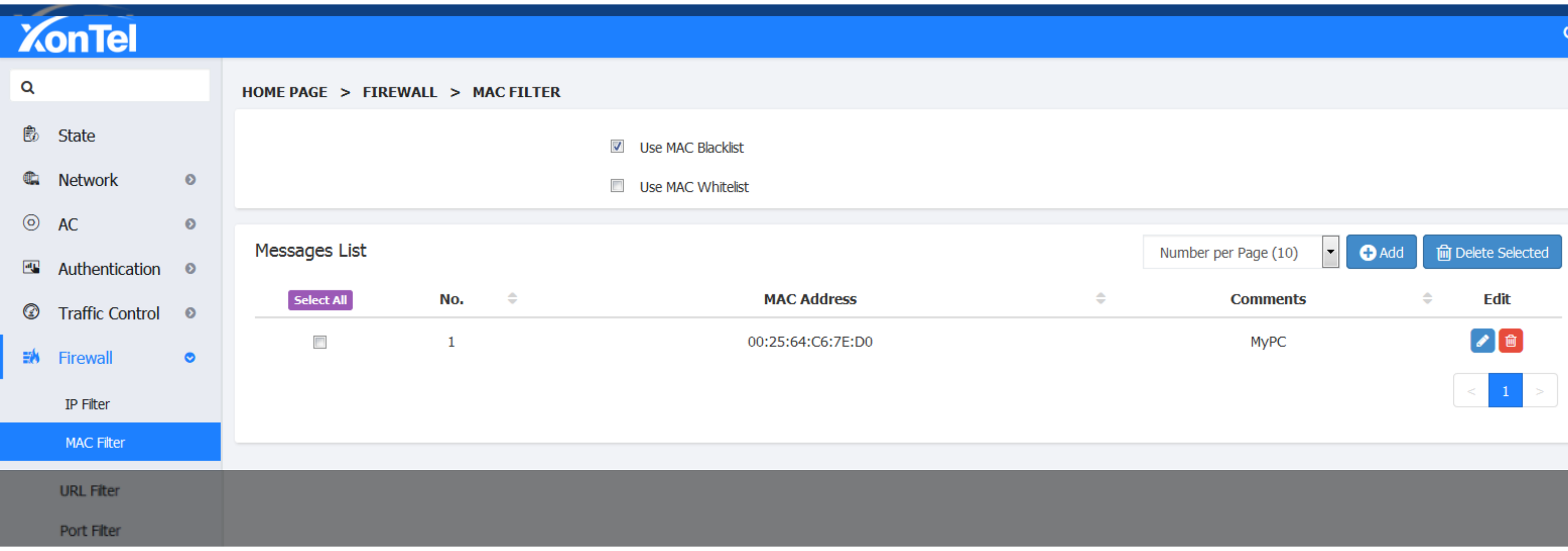
Messages List

Select All	No.	Protocol	Start IP	End IP	Comments	Edit

7.2 MAC Filter

Here you must know the computer LAN card’s MAC addres then enter the corresponding computer MAC address to block Internet in MAC Filter.

1. Login the router’s WEB page go into the “MAC Filter” page in Firewall setup PC's MAC address which you want block and save the setting.



HOME PAGE > FIREWALL > MAC FILTER

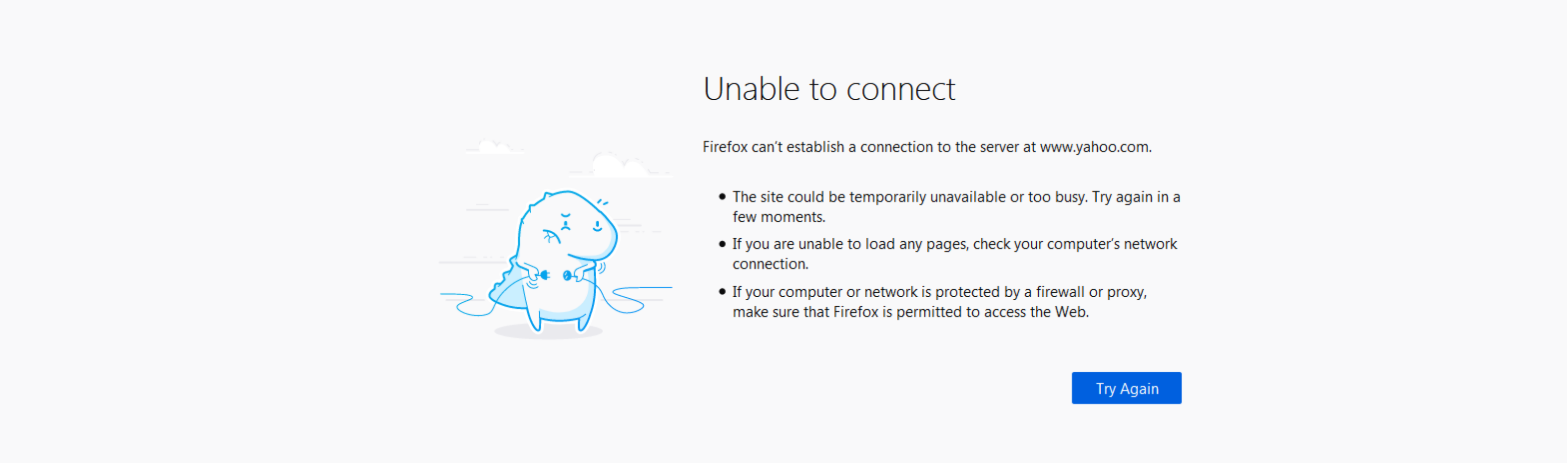
☑ Use MAC Blacklist

☐ Use MAC Whitelist

Messages List

Select All	No.	MAC Address	Comments	Edit
☐	1	00:25:64:C6:7E:D0	MyPC	

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

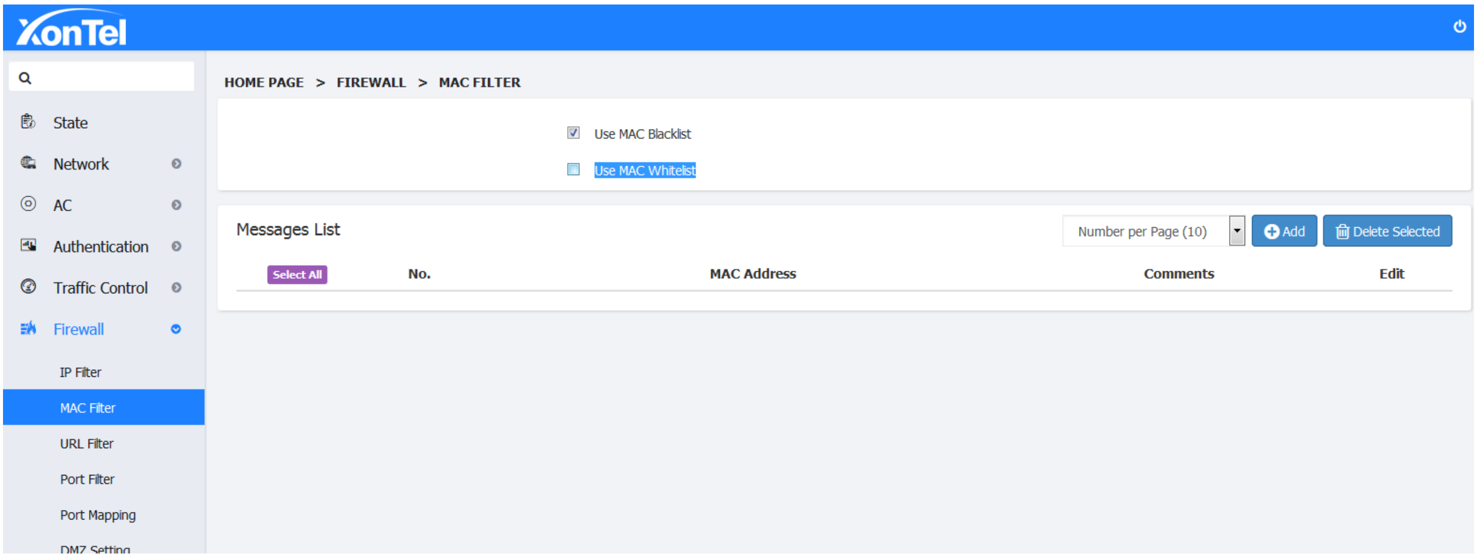


Unable to connect

Firefox can't establish a connection to the server at www.yahoo.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

3. Modify the MAC address whitelist mode. Only devices in the whitelist can access the Internet. Other devices cannot access the Internet. (Use this option with caution)



HOME PAGE > FIREWALL > MAC FILTER

☑ Use MAC Blacklist

□ Use MAC Whitelist

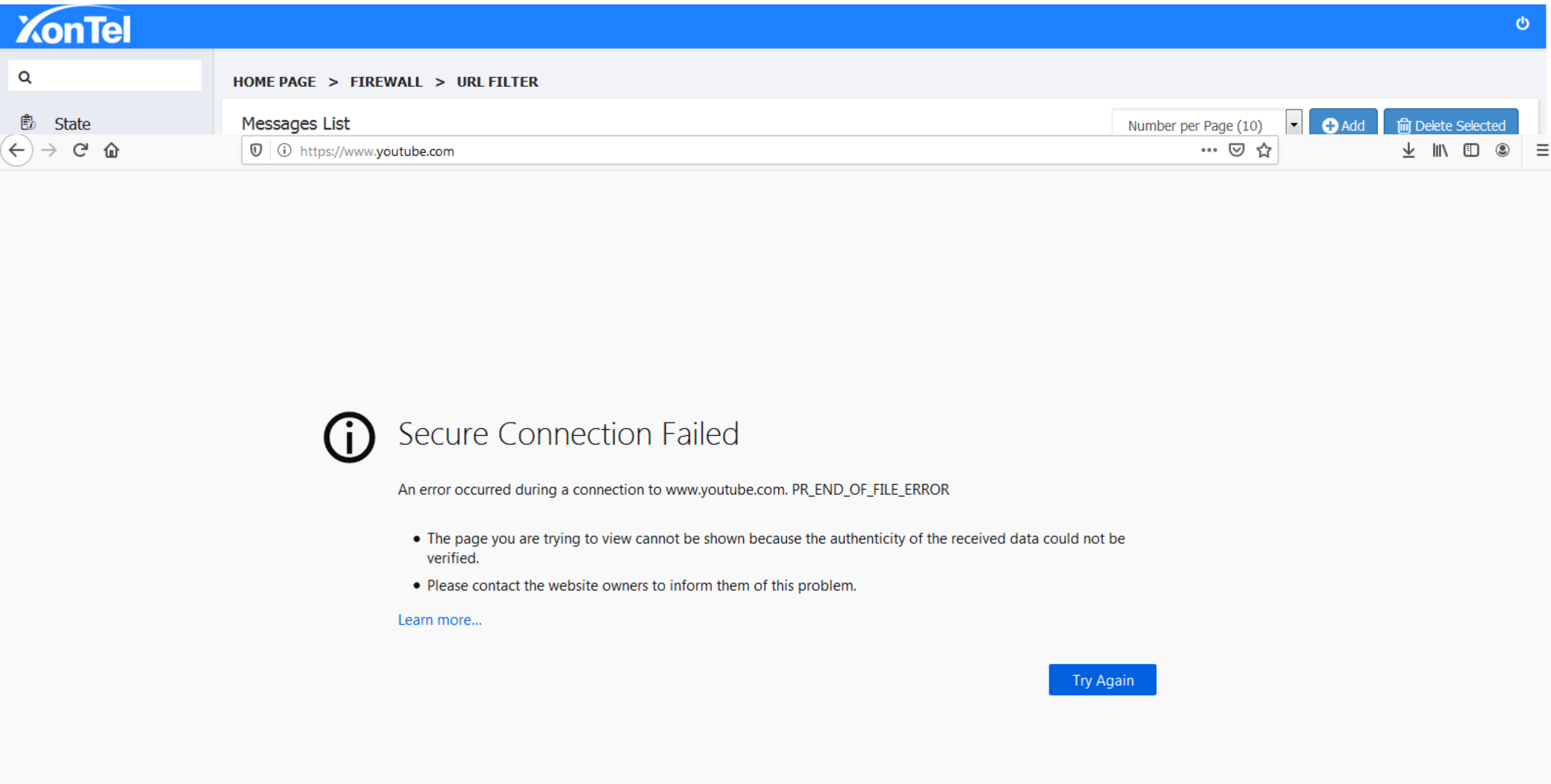
Messages List

Select All	No.	MAC Address	Comments	Edit

7.3 URL Filtering

Here you can setup the website address to filter which you need and the saved address (URLs) cannot be accessed.

1. Login the router's WEB page click URL Filter in Firewall and enter "www.youtube.com” in the website filter.



Secure Connection Failed

An error occurred during a connection to www.youtube.com. PR_END_OF_FILE_ERROR

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

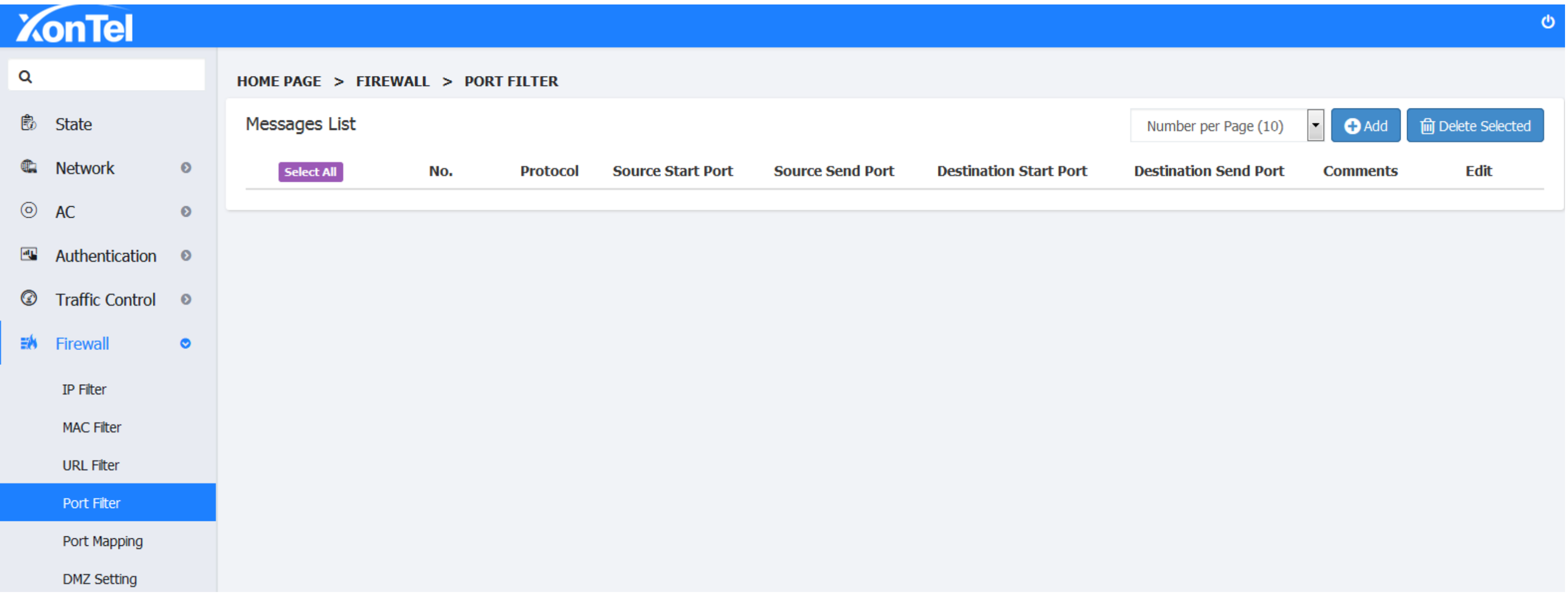
Try Again

2.Open browser and try to visit www.youtube.com, the PC cannot access the website but can visit other websites.

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.

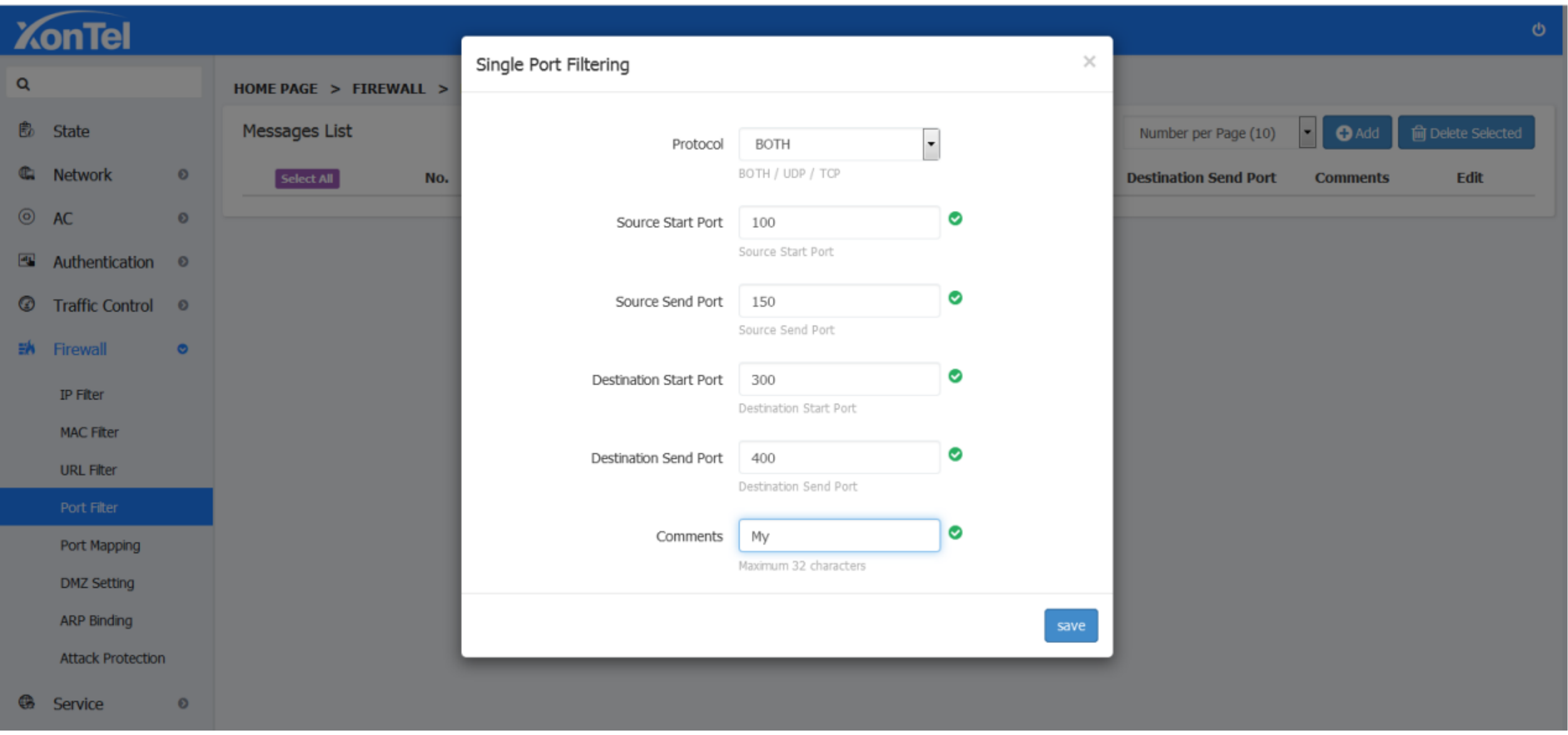
1. On home page click on "Firewall-Port Filter" to enter the port filter page, click on the "+ Add" button to pop up into the port filter settings box:



HOME PAGE > FIREWALL > PORT FILTER

Messages List

Select All	No.	Protocol	Source Start Port	Source Send Port	Destination Start Port	Destination Send Port	Comments	Edit



Single Port Filtering

Protocol: BOTH (BOTH / UDP / TCP)

Source Start Port: 100 (Source Start Port)

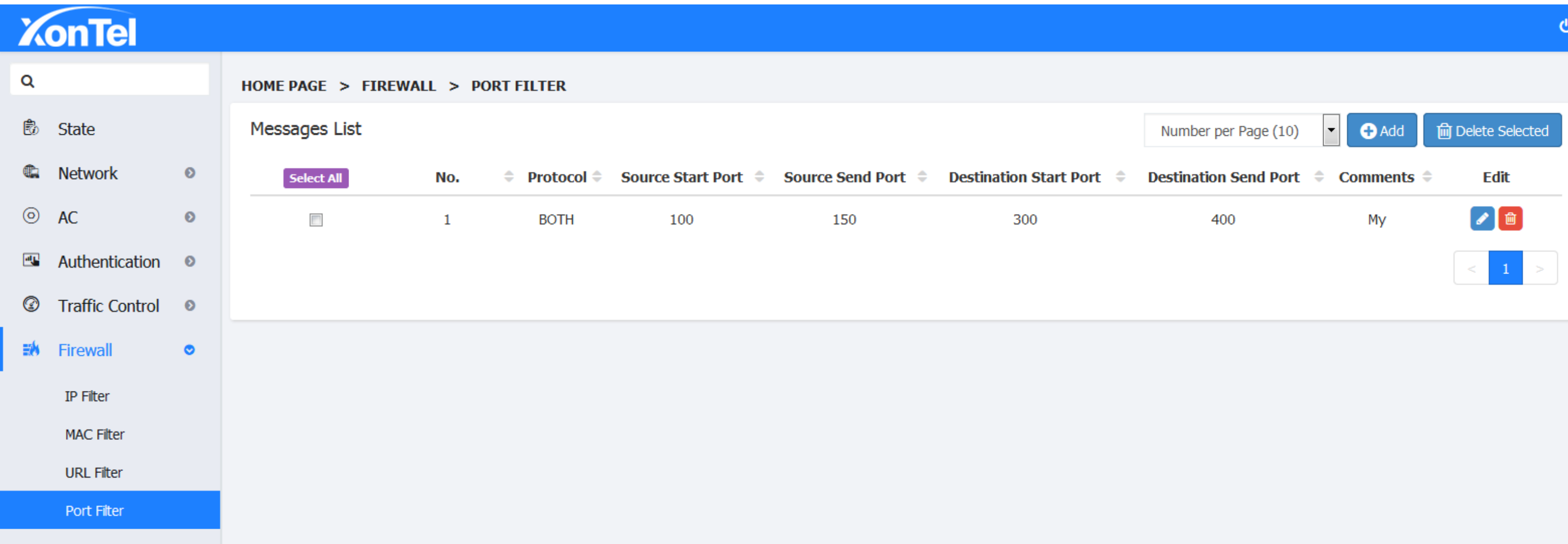
Source Send Port: 150 (Source Send Port)

Destination Start Port: 300 (Destination Start Port)

Destination Send Port: 400 (Destination Send Port)

Comments: My (Maximum 32 characters)

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



HOME PAGE > FIREWALL > PORT FILTER

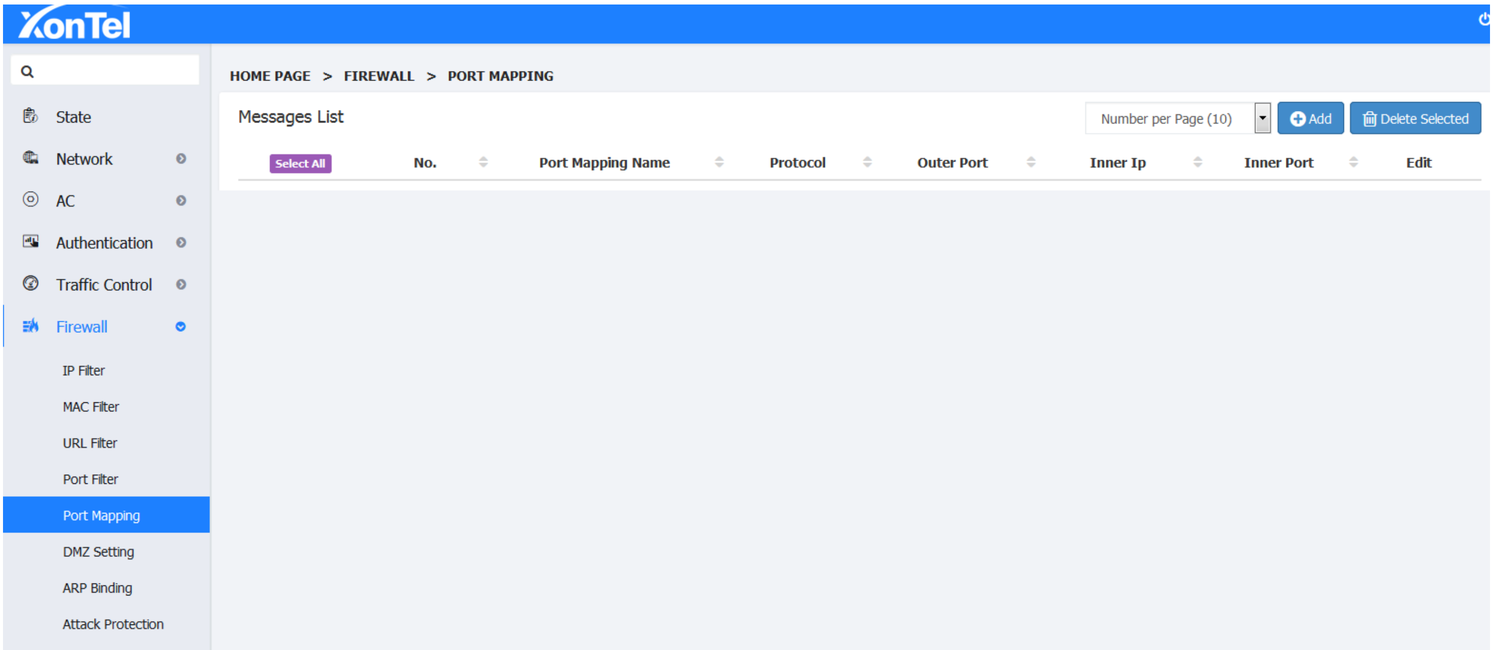
Messages List

Select All	No.	Protocol	Source Start Port	Source Send Port	Destination Start Port	Destination Send Port	Comments	Edit
□	1	BOTH	100	150	300	400	My	

7.5 Port Mapping

Port Mapping or **Port Forwarding** is an application of network address translation (NAT) that redirects a communication request from one address and **port** number combination to another while the packets are traversing a network gateway, such as XonTel XT-1000AC**.**

1. Login the XT-1000AC's Web page finish setup in the Firewall page.

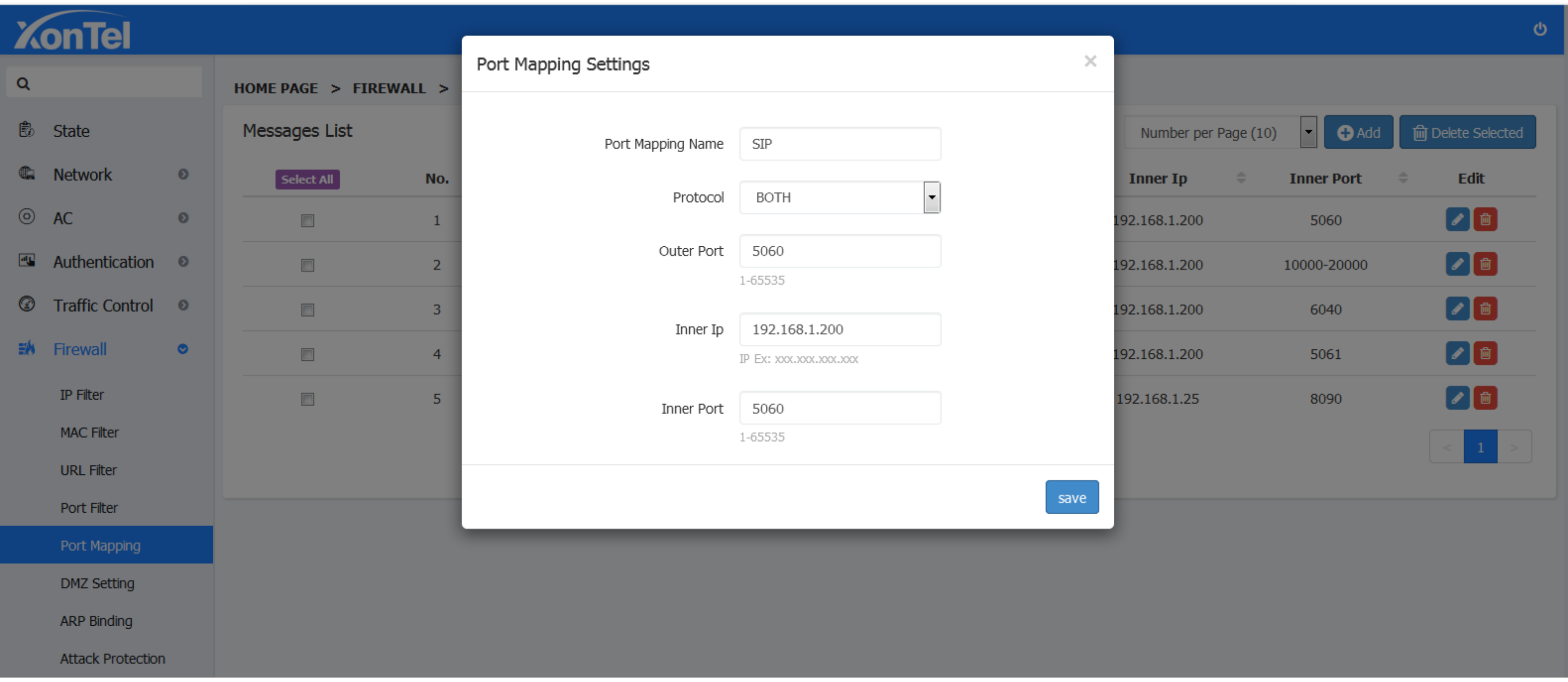


HOME PAGE > FIREWALL > PORT MAPPING

Messages List

Select All	No.	Port Mapping Name	Protocol	Outer Port	Inner Ip	Inner Port	Edit

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



Port Mapping Settings

Port Mapping Name: SIP

Protocol: BOTH

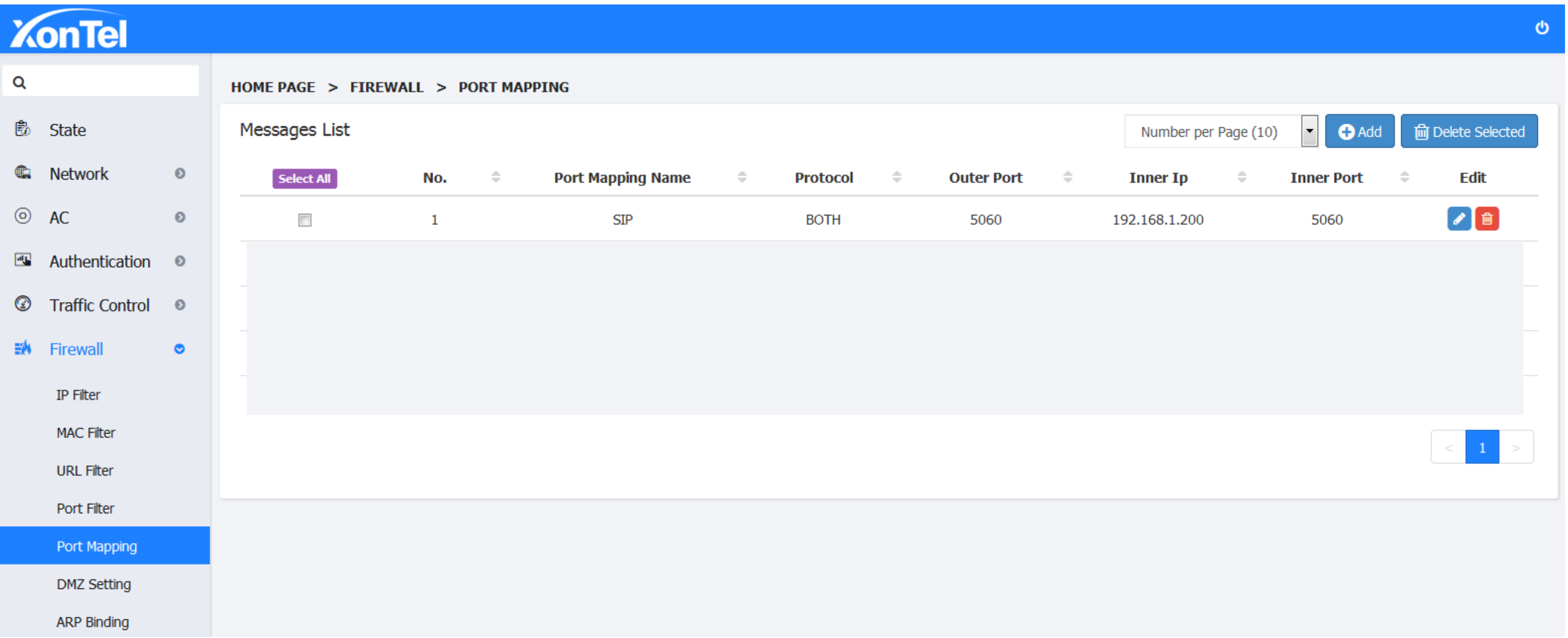
Outer Port: 5060
1-65535

Inner Ip: 192.168.1.200
IP Ex: xxx.xxx.xxx.xxx

Inner Port: 5060
1-65535

No.	Inner Ip	Inner Port
1	192.168.1.200	5060
2	192.168.1.200	10000-20000
3	192.168.1.200	6040
4	192.168.1.200	5061
5	192.168.1.25	8090

3. Click save and go into the Massages List page and the port forwarding function is successfully configured (the port is mapped to the external network port 5060 to the internal network port 5060 on IP Address 192.168.1.200).



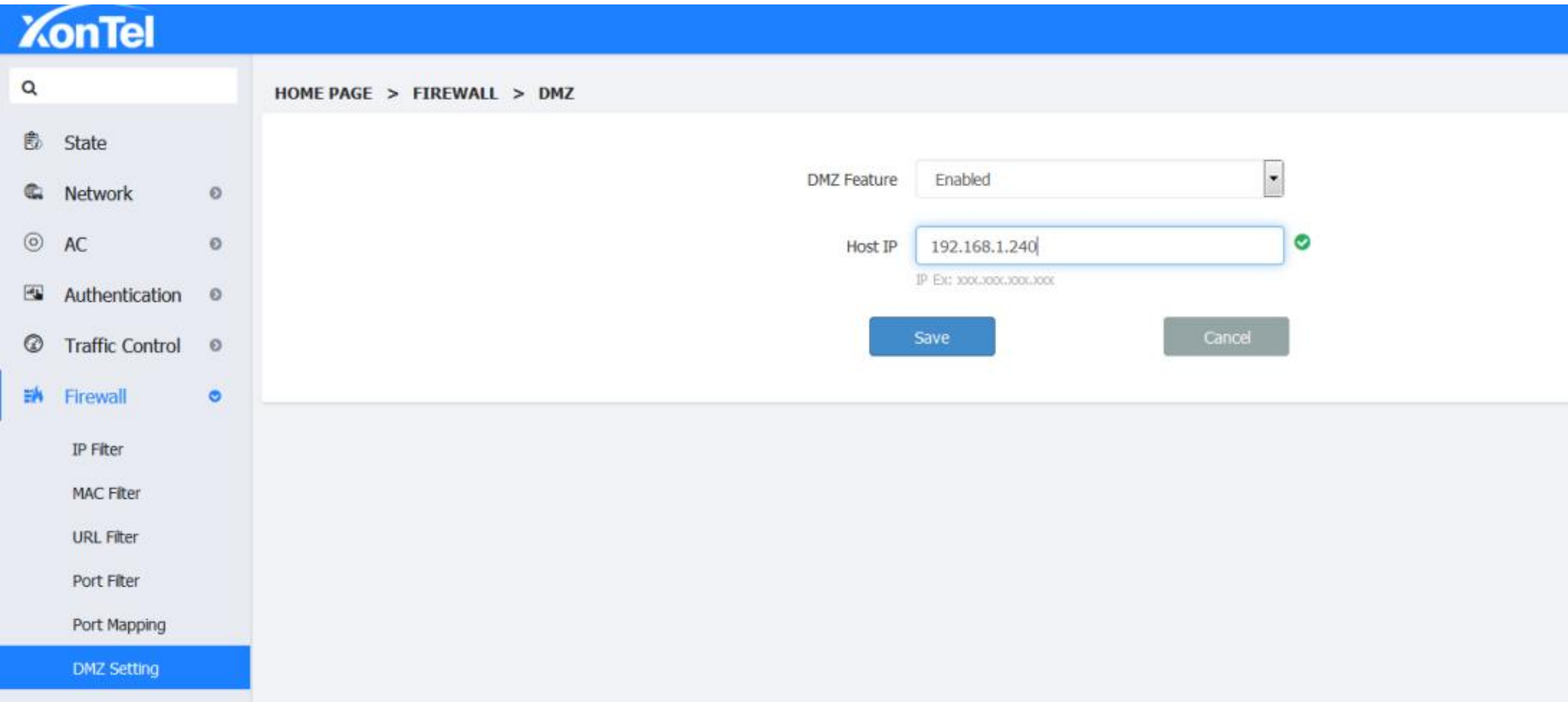
HOME PAGE > FIREWALL > PORT MAPPING

Messages List

No.	Port Mapping Name	Protocol	Outer Port	Inner Ip	Inner Port	Edit
1	SIP	BOTH	5060	192.168.1.200	5060	

7.6 DMZ settings

A DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened Subnet) is a physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. You can place some server facilities which needs to be 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.



HOME PAGE > FIREWALL > DMZ

DMZ Feature: Enabled

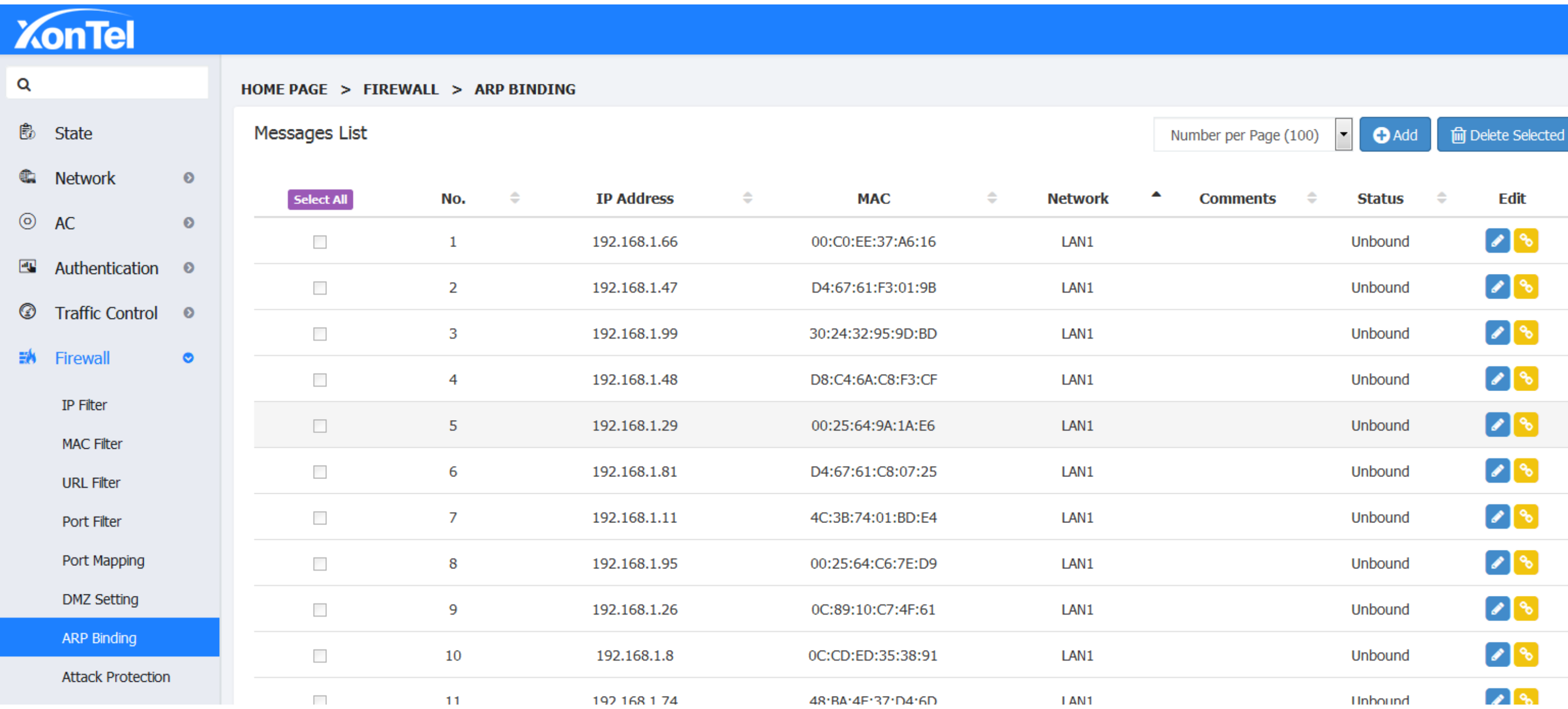
Host IP: 192.168.1.240

IP Ex: xxx.xxx.xxx.xxx

7.7 ARP Binding

The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

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



HOME PAGE > FIREWALL > ARP BINDING

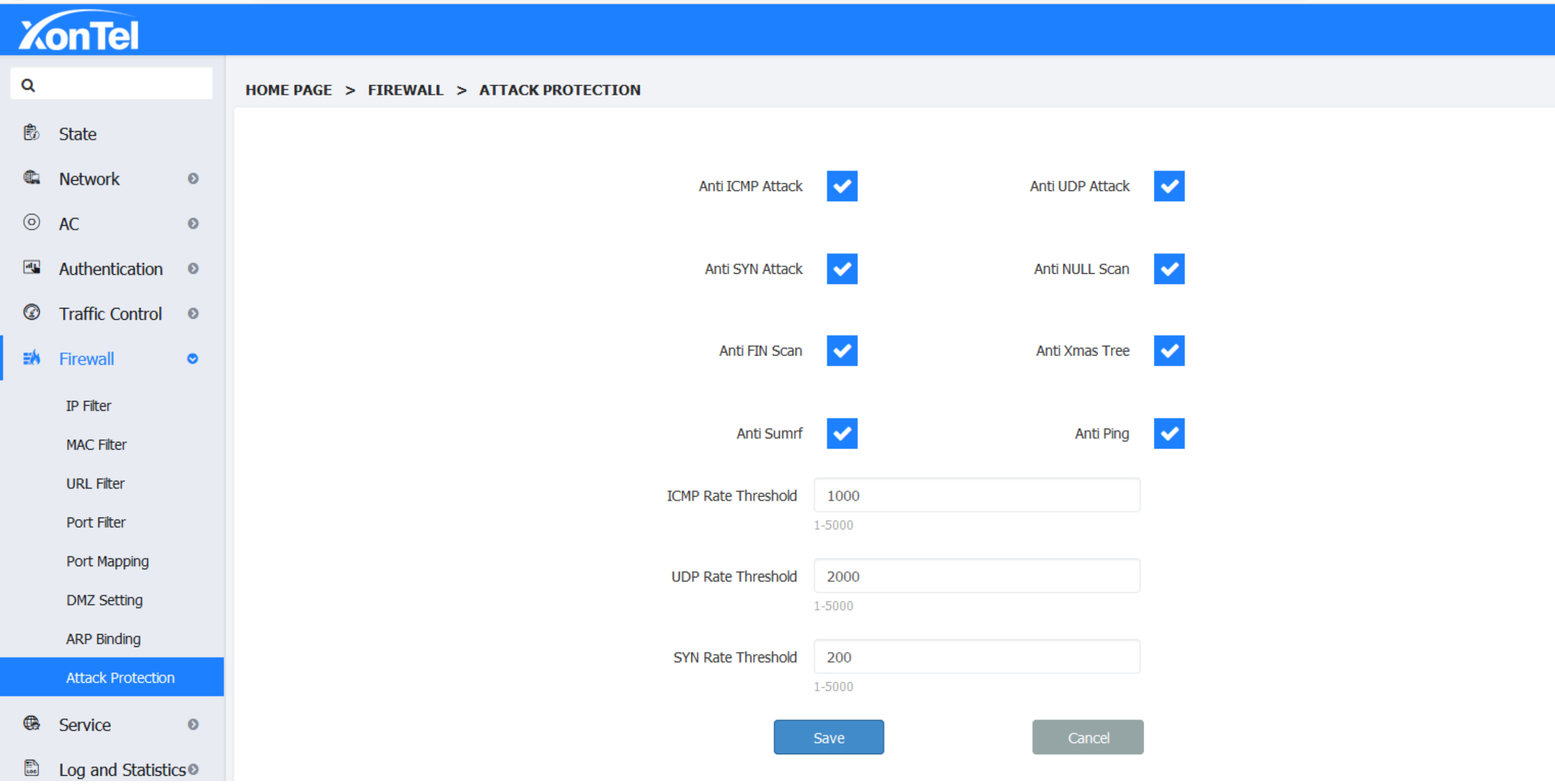
Messages List

Select All	No.	IP Address	MAC	Network	Comments	Status	Edit
□	1	192.168.1.66	00:C0:EE:37:A6:16	LAN1		Unbound	
□	2	192.168.1.47	D4:67:61:F3:01:9B	LAN1		Unbound	
□	3	192.168.1.99	30:24:32:95:9D:BD	LAN1		Unbound	
□	4	192.168.1.48	D8:C4:6A:C8:F3:CF	LAN1		Unbound	
□	5	192.168.1.29	00:25:64:9A:1A:E6	LAN1		Unbound	
□	6	192.168.1.81	D4:67:61:C8:07:25	LAN1		Unbound	
□	7	192.168.1.11	4C:3B:74:01:BD:E4	LAN1		Unbound	
□	8	192.168.1.95	00:25:64:C6:7E:D9	LAN1		Unbound	
□	9	192.168.1.26	0C:89:10:C7:4F:61	LAN1		Unbound	
□	10	192.168.1.8	0C:CD:ED:35:38:91	LAN1		Unbound	
□	11	192.168.1.74	48:BA:4F:37:D4:6D	LAN1		Unbound	

7.8 Attack Protection

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Attack Protection 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 types, and click on Save:



Anti ICMP Attack ☑ Anti UDP Attack ☑

Anti SYN Attack ☑ Anti NULL Scan ☑

Anti FIN Scan ☑ Anti Xmas Tree ☑

Anti Sumrf ☑ Anti Ping ☑

ICMP Rate Threshold: 1000 (1-5000)

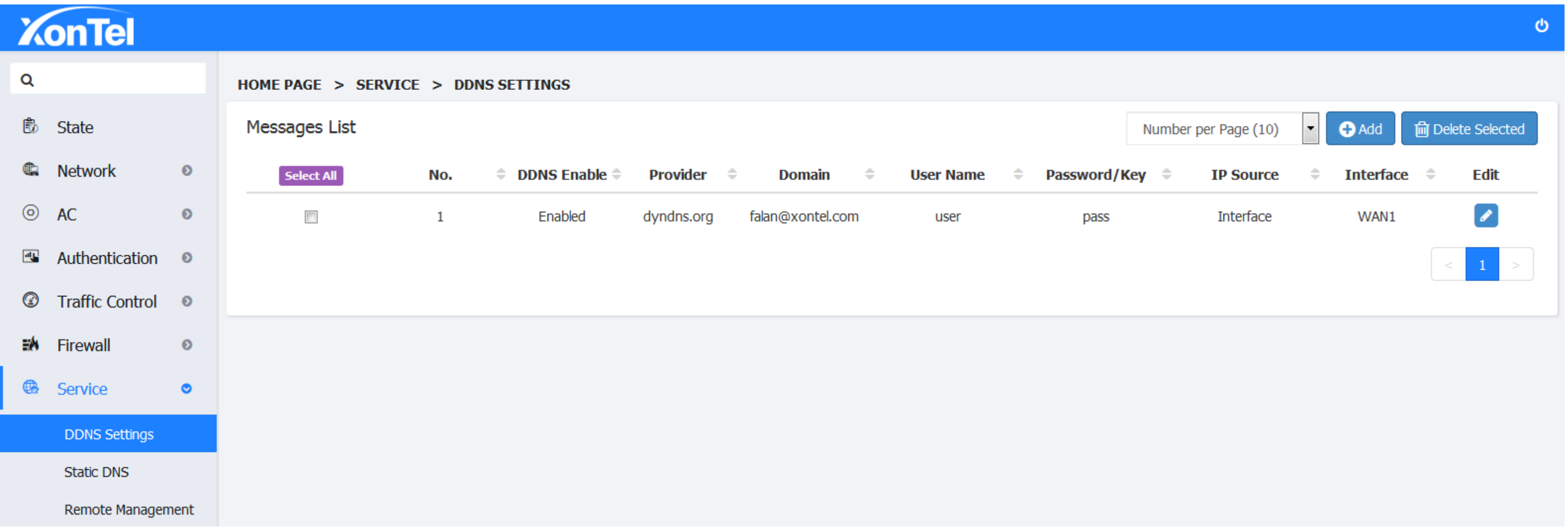
UDP Rate Threshold: 2000 (1-5000)

SYN Rate Threshold: 200 (1-5000)

8 Service

8.1 DDNS Settings

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



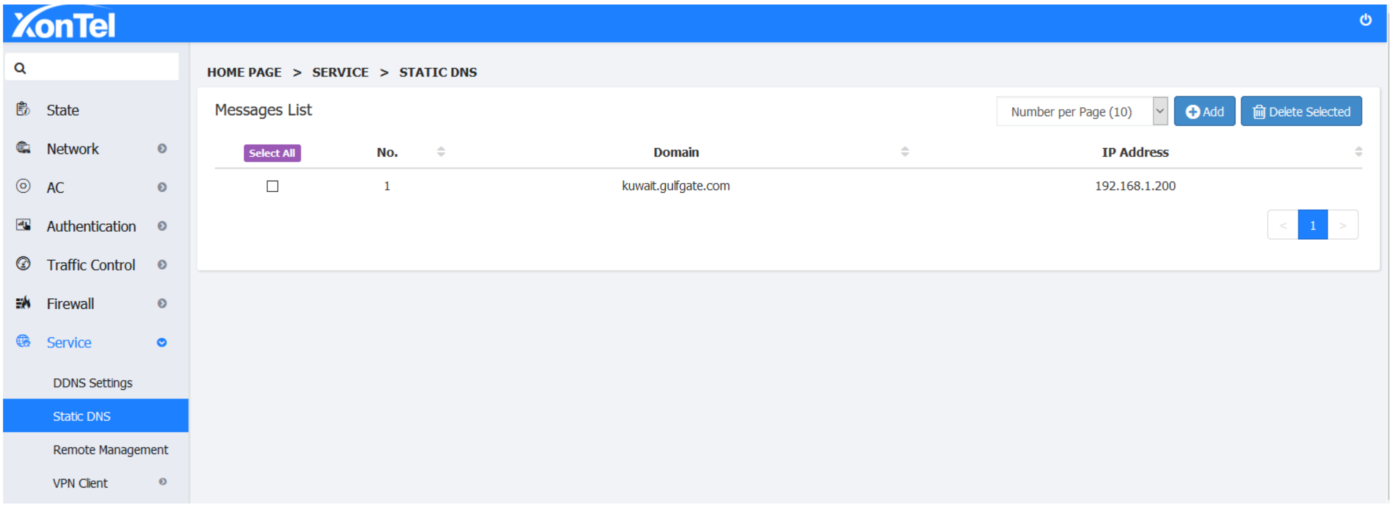
HOME PAGE > SERVICE > DDNS SETTINGS

Messages List

	No.	DDNS Enable	Provider	Domain	User Name	Password/Key	IP Source	Interface	Edit
□	1	Enabled	dyndns.org	falan@xontel.com	user	pass	Interface	WAN1	

8.2 Static DNS

Sometimes it required to use some service from your home/office device through Mobile App, locally and remote. Static DNS useful in that case. Static DNS can map a local IP address of the device with a Domain name. So the mobile app can work with that domain name either in private WiFi network or on public network (4G/5G, Public WiFi)



HOME PAGE > SERVICE > STATIC DNS

Messages List

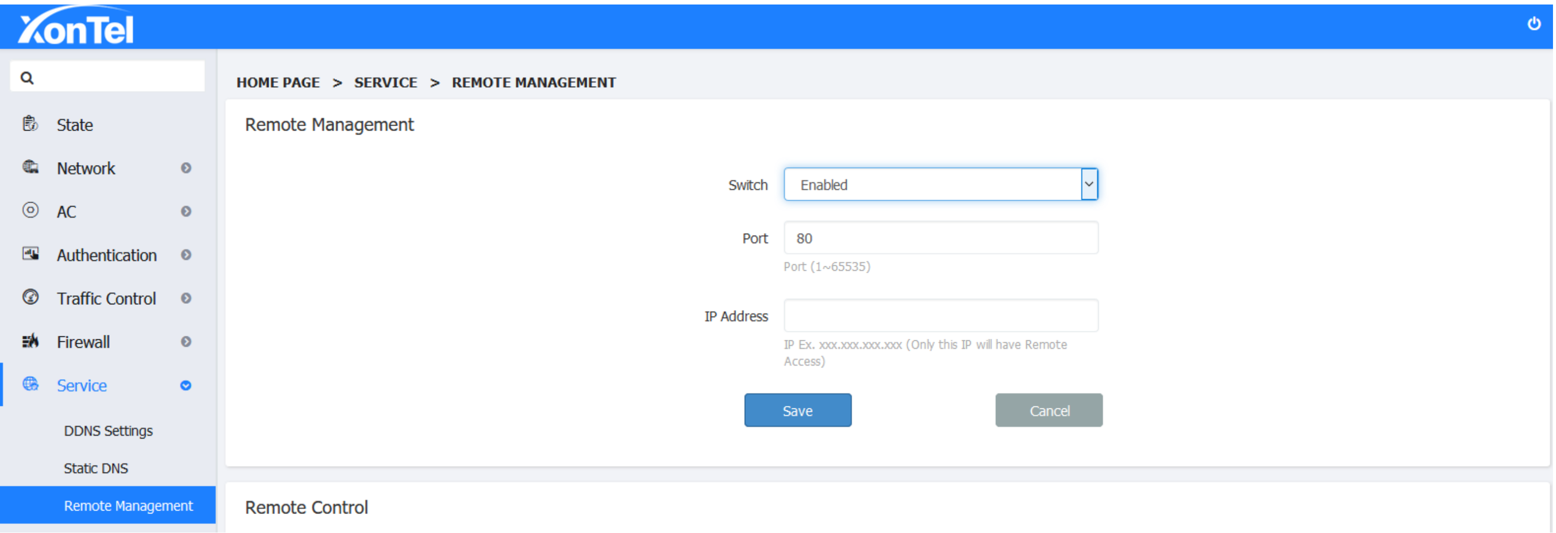
	No.	Domain	IP Address
□	1	kuwait.gulfgate.com	192.168.1.200

8.3 Remote Management Setting

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

1. Click "Service - Remote Management" on the main interface of the XT-1000AC to enter the remote setup page, as shown below:

2. Enable the service, the port enters 1-65535 any one port, IP address default to remain empty, enter the specific IP only allow that particular IP remote access, do not enter any external network IP remote access, and then click Save.



HOME PAGE > SERVICE > REMOTE MANAGEMENT

Remote Management

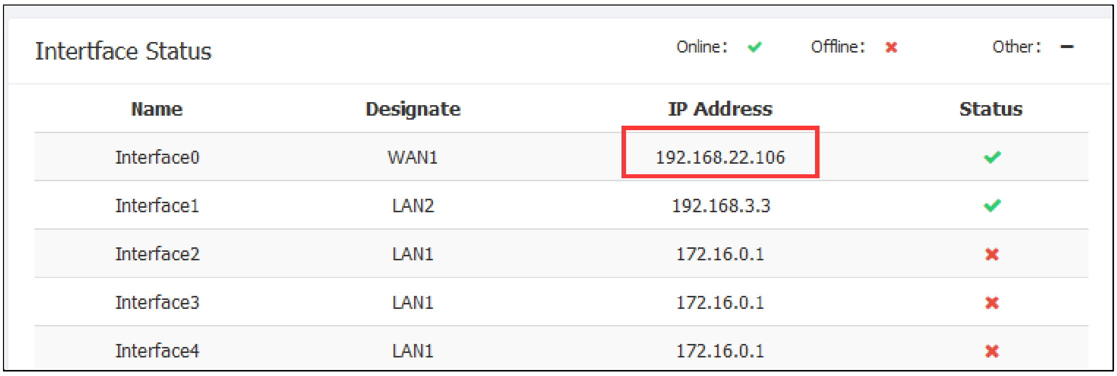
Switch: Enabled

Port: 80
Port (1~65535)

IP Address:
IP Ex. xxx.xxx.xxx.xxx (Only this IP will have Remote Access)

Remote Control

3. Enter the gateway of the upper-level route to set up the virtual server, IP is the WAN port IP of the XT-1000AC, 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.



Intertface Status — Online: ✓ Offline: ✖ Other: —

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	✖

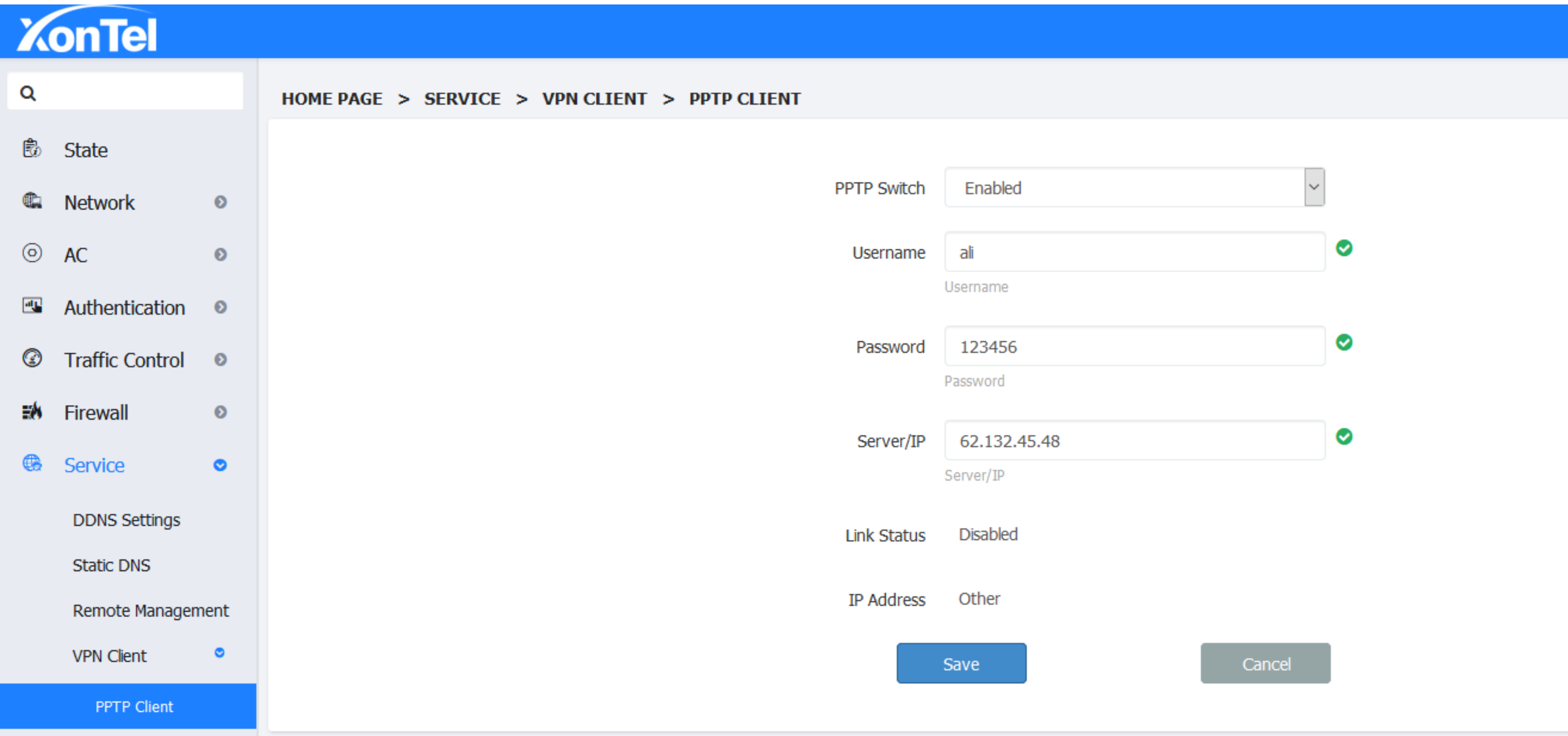
4.After added, connect to the upper-level route, enter the WAN port address of the device in the browser: port number (such as "192.168.22.106:80"), press Enter, you can access the gateway of the device remotely.

8.4 VPN Client

8.4.1 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.



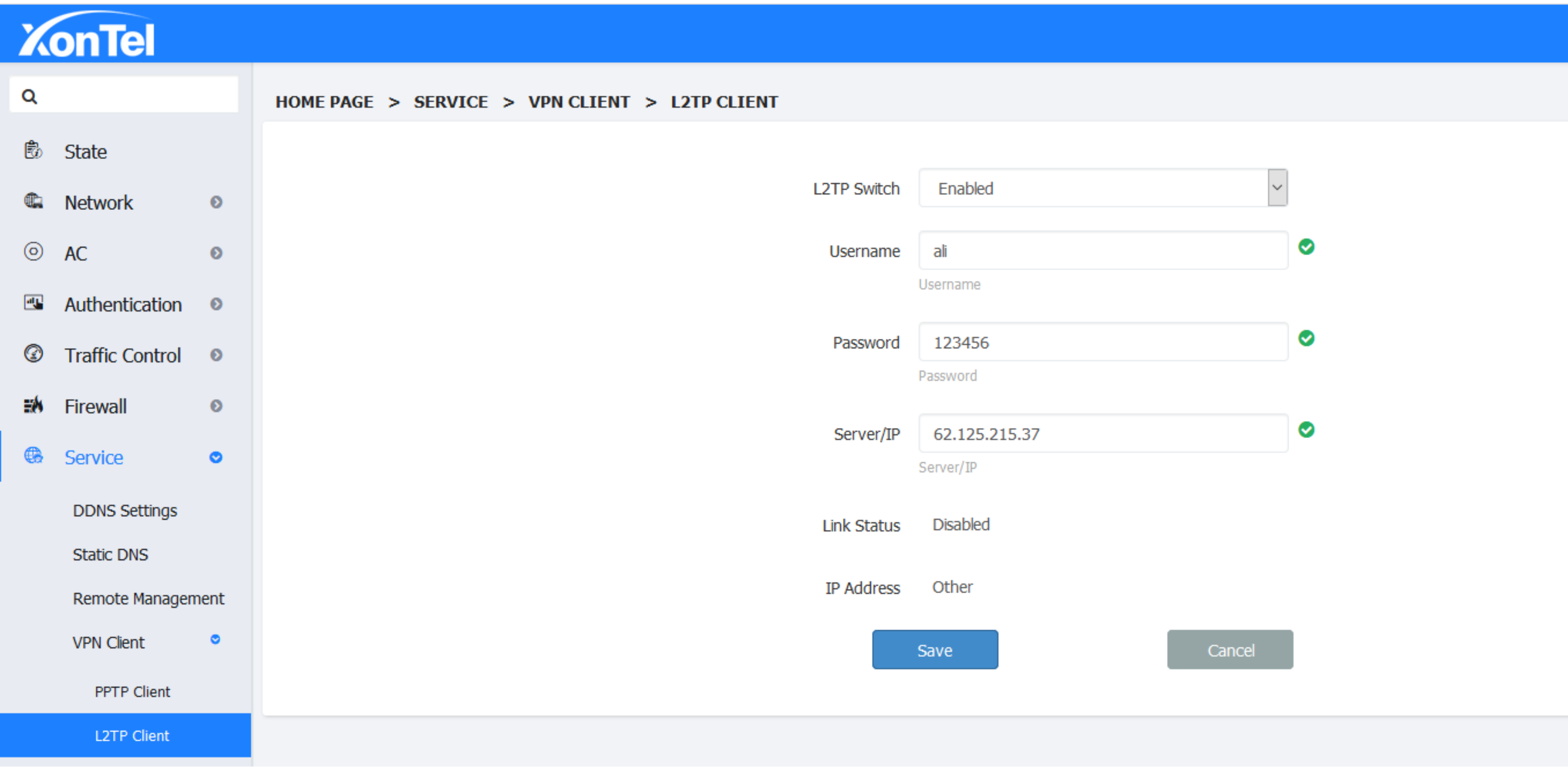
HOME PAGE > SERVICE > VPN CLIENT > PPTP CLIENT

PPTP Switch	Enabled
Username	ali
Password	123456
Server/IP	62.132.45.48
Link Status	Disabled
IP Address	Other

8.4.2 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.



HOME PAGE > SERVICE > VPN CLIENT > L2TP CLIENT

L2TP Switch: Enabled

Username: ali

Password: 123456

Server/IP: 62.125.215.37

Link Status: Disabled

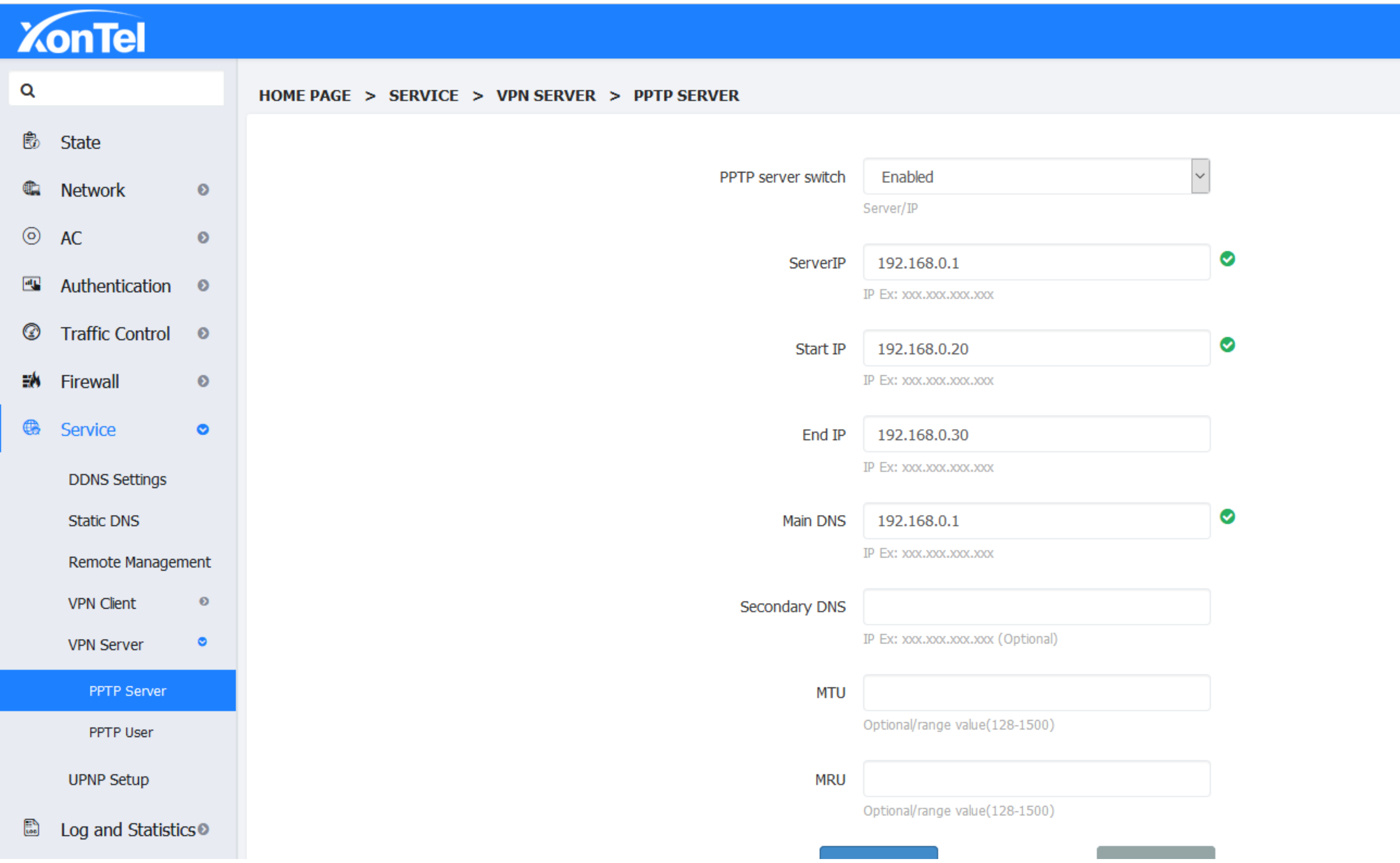
IP Address: Other

8.5 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".

8.5.1 PPTP Server

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

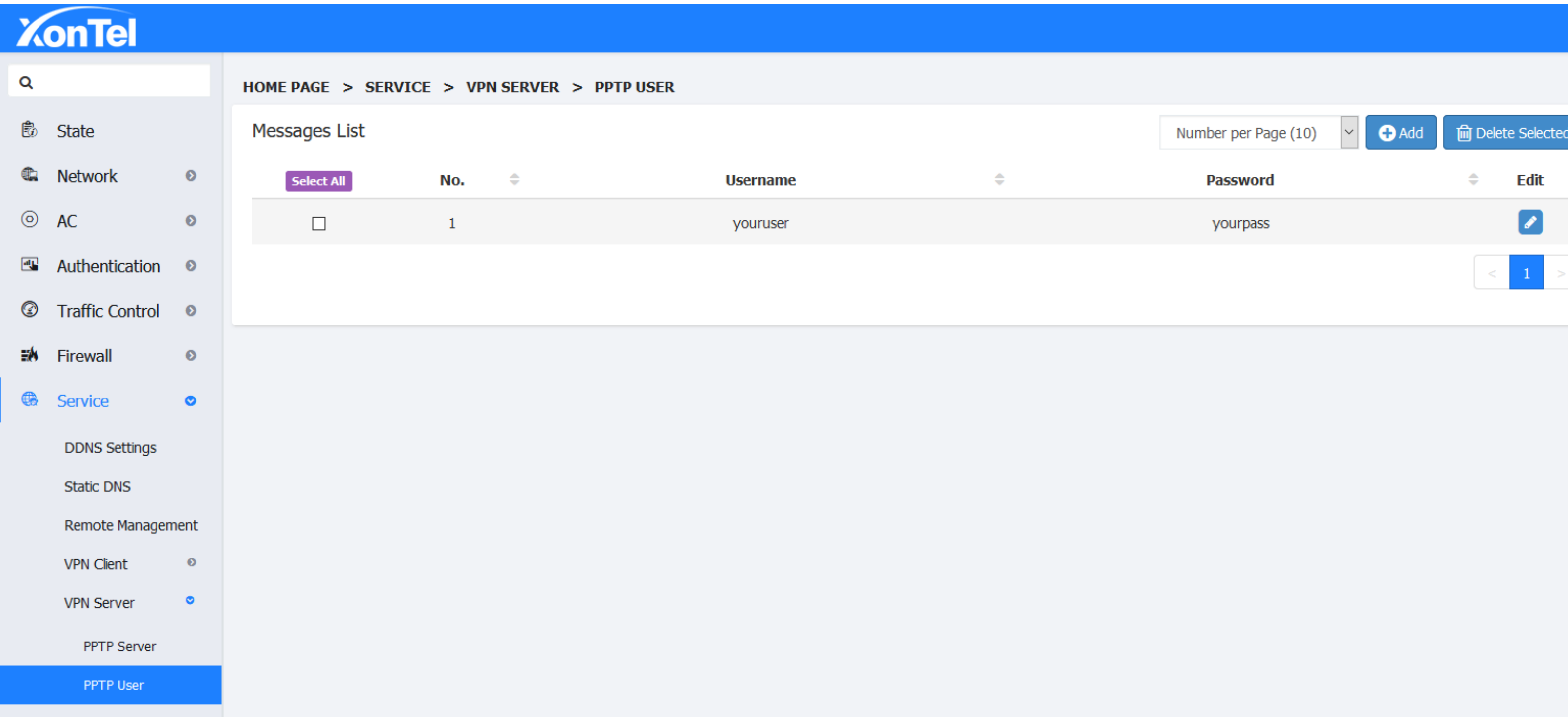


HOME PAGE > SERVICE > VPN SERVER > PPTP SERVER

PPTP server switch	Enabled Server/IP
ServerIP	192.168.0.1 ✓ IP Ex: xxx.xxx.xxx.xxx
Start IP	192.168.0.20 ✓ IP Ex: xxx.xxx.xxx.xxx
End IP	192.168.0.30 IP Ex: xxx.xxx.xxx.xxx
Main DNS	192.168.0.1 ✓ IP Ex: xxx.xxx.xxx.xxx
Secondary DNS	 IP Ex: xxx.xxx.xxx.xxx (Optional)
MTU	 Optional/range value(128-1500)
MRU	 Optional/range value(128-1500)

8.5.2 PPTP Server

Go into PPTP USER page, set up the user



HOME PAGE > SERVICE > VPN SERVER > PPTP USER

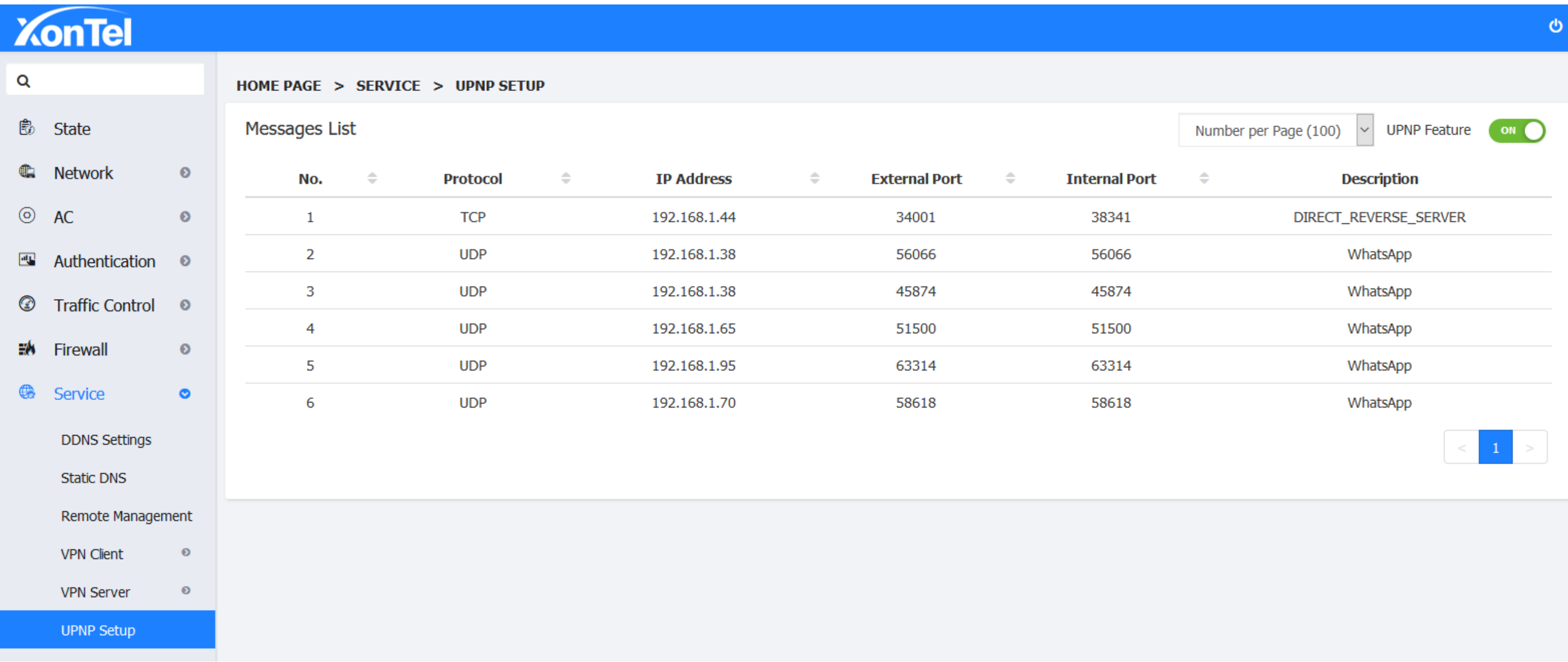
Messages List

Select All	No.	Username	Password	Edit
□	1	youruser	yourpass	

3. Setup a VPN connection in laptop which is on different network, enter the user name and password added by PPTP, test the connection, and get the specified IP address.

8.6 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.



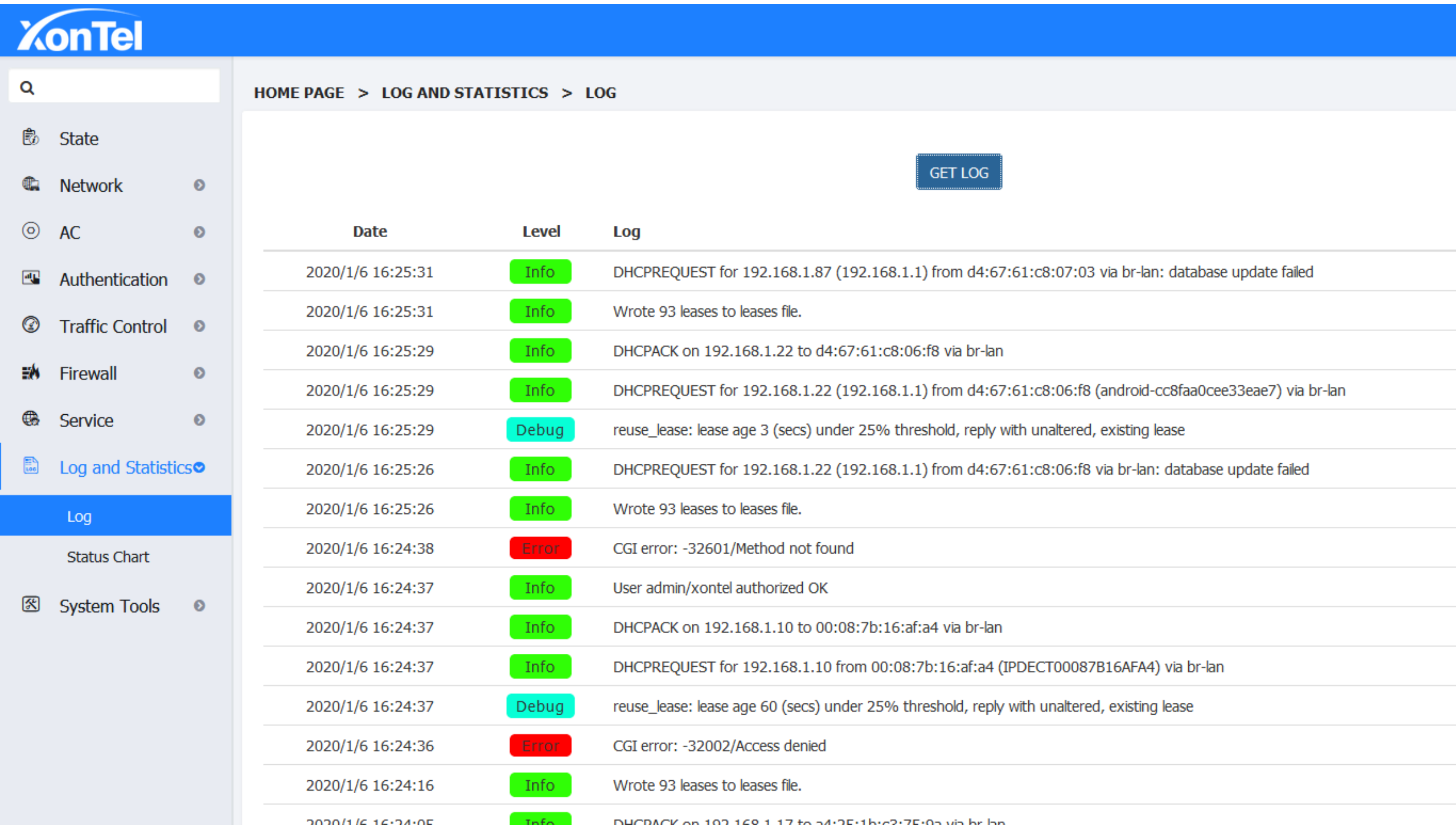
No.	Protocol	IP Address	External Port	Internal Port	Description
1	TCP	192.168.1.44	34001	38341	DIRECT_REVERSE_SERVER
2	UDP	192.168.1.38	56066	56066	WhatsApp
3	UDP	192.168.1.38	45874	45874	WhatsApp
4	UDP	192.168.1.65	51500	51500	WhatsApp
5	UDP	192.168.1.95	63314	63314	WhatsApp
6	UDP	192.168.1.70	58618	58618	WhatsApp

9 Log and Statistics

9.1 Log

Here you can view the system's working status when the device is working.

1.Go to WEB Interface and go to Log and Statistics-Log page, click "GET LOG" button, then the page will refresh the log details every moments, as below:

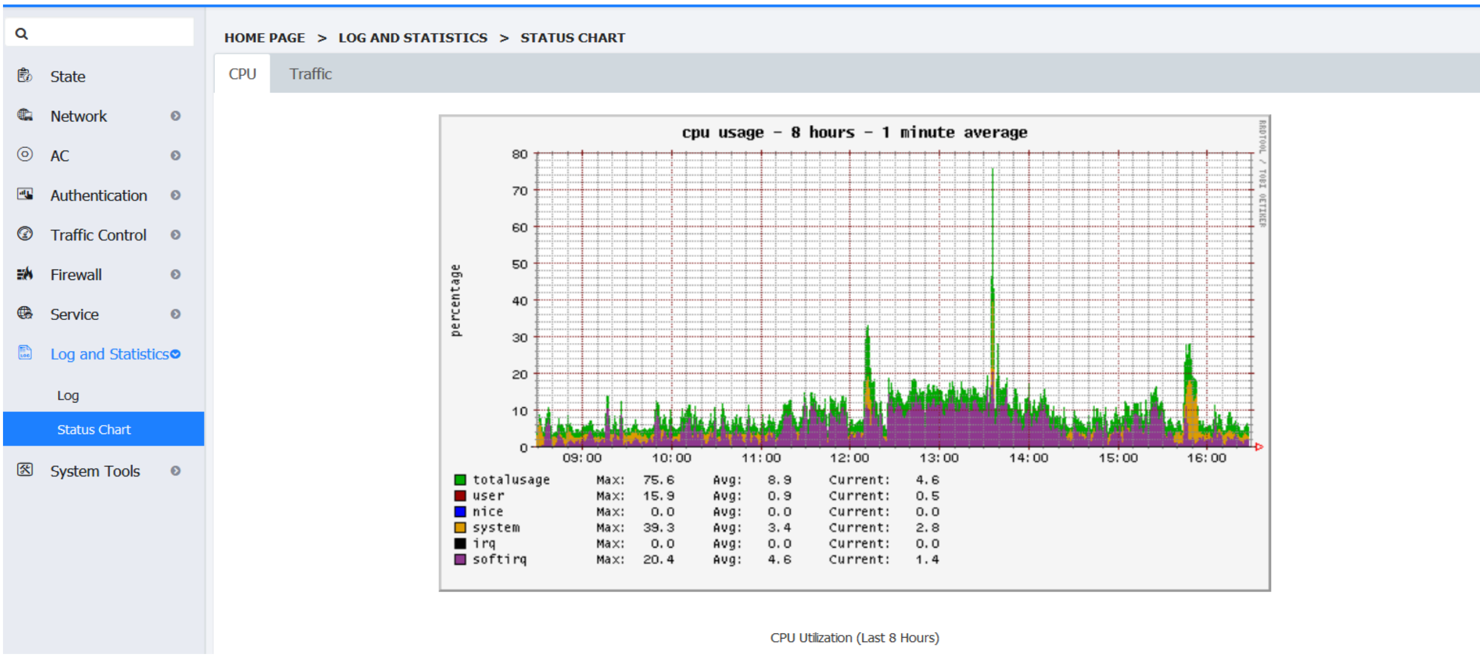


Date	Level	Log
2020/1/6 16:25:31	Info	DHCPREQUEST for 192.168.1.87 (192.168.1.1) from d4:67:61:c8:07:03 via br-lan: database update failed
2020/1/6 16:25:31	Info	Wrote 93 leases to leases file.
2020/1/6 16:25:29	Info	DHCPACK on 192.168.1.22 to d4:67:61:c8:06:f8 via br-lan
2020/1/6 16:25:29	Info	DHCPREQUEST for 192.168.1.22 (192.168.1.1) from d4:67:61:c8:06:f8 (android-cc8faa0cee33eae7) via br-lan
2020/1/6 16:25:29	Debug	reuse_lease: lease age 3 (secs) under 25% threshold, reply with unaltered, existing lease
2020/1/6 16:25:26	Info	DHCPREQUEST for 192.168.1.22 (192.168.1.1) from d4:67:61:c8:06:f8 via br-lan: database update failed
2020/1/6 16:25:26	Info	Wrote 93 leases to leases file.
2020/1/6 16:24:38	Error	CGI error: -32601/Method not found
2020/1/6 16:24:37	Info	User admin/xontel authorized OK
2020/1/6 16:24:37	Info	DHCPACK on 192.168.1.10 to 00:08:7b:16:af:a4 via br-lan
2020/1/6 16:24:37	Info	DHCPREQUEST for 192.168.1.10 from 00:08:7b:16:af:a4 (IPDECT00087B16AFA4) via br-lan
2020/1/6 16:24:37	Debug	reuse_lease: lease age 60 (secs) under 25% threshold, reply with unaltered, existing lease
2020/1/6 16:24:36	Error	CGI error: -32002/Access denied
2020/1/6 16:24:16	Info	Wrote 93 leases to leases file.
2020/1/6 16:24:05	Info	DHCPACK on 192.168.1.17 to a4:35:1b:c3:75:9a via br-lan

9.2 Status Chart

Historical Statistics

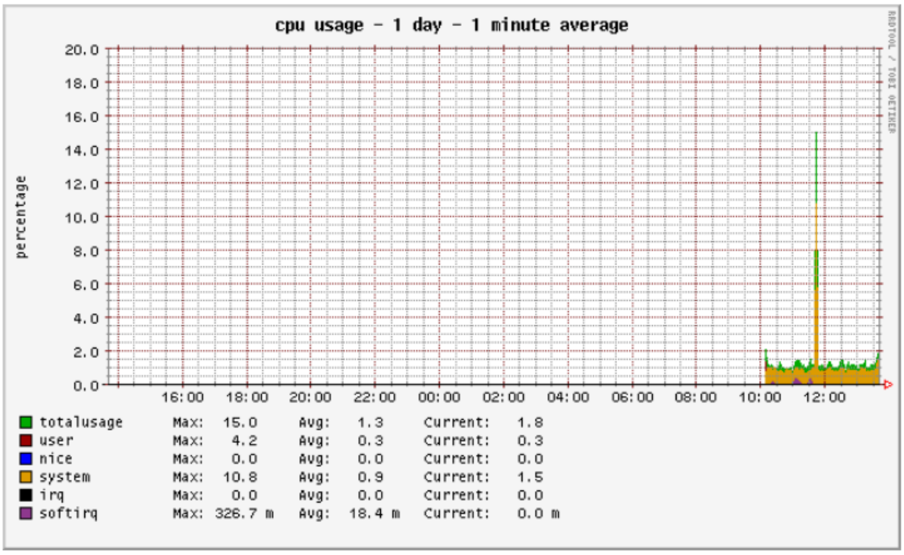
1.CPU: here record the CPU usage information when the devise working 8 hours, one day and one week.



```
🟩 totalusage     Max:  75.6    Avg:   8.9    Current:   4.6
🟥 user           Max:  15.9    Avg:   0.9    Current:   0.5
🟦 nice           Max:   0.0    Avg:   0.0    Current:   0.0
🟧 system         Max:  39.3    Avg:   3.4    Current:   2.8
⬛ irq            Max:   0.0    Avg:   0.0    Current:   0.0
🟪 softirq        Max:  20.4    Avg:   4.6    Current:   1.4
```

CPU Utilization (Last 8 Hours)

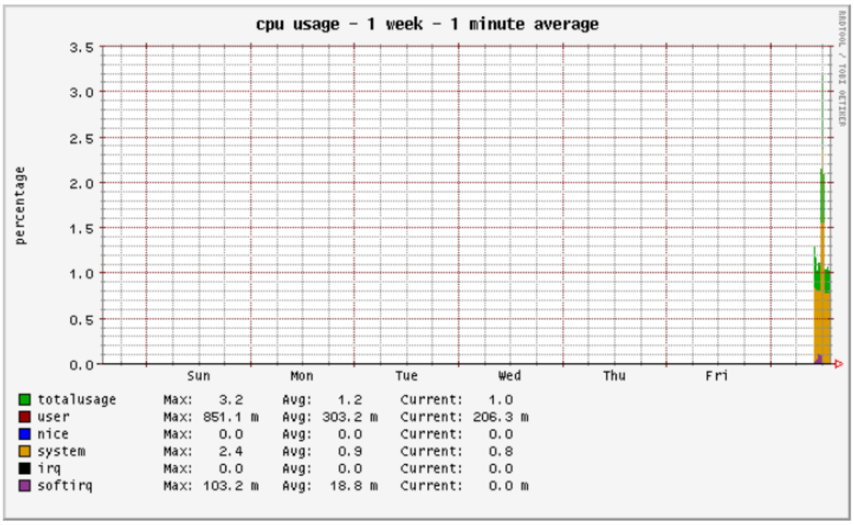
<8 Hours>



```
🟩 totalusage     Max:  15.0      Avg:   1.3      Current:   1.8
🟥 user           Max:   4.2      Avg:   0.3      Current:   0.3
🟦 nice           Max:   0.0      Avg:   0.0      Current:   0.0
🟧 system         Max:  10.8      Avg:   0.9      Current:   1.5
⬛ irq            Max:   0.0      Avg:   0.0      Current:   0.0
🟪 softirq        Max: 326.7 m    Avg:  18.4 m    Current:   0.0 m
```

CPU Utilization (Last 1 Day)

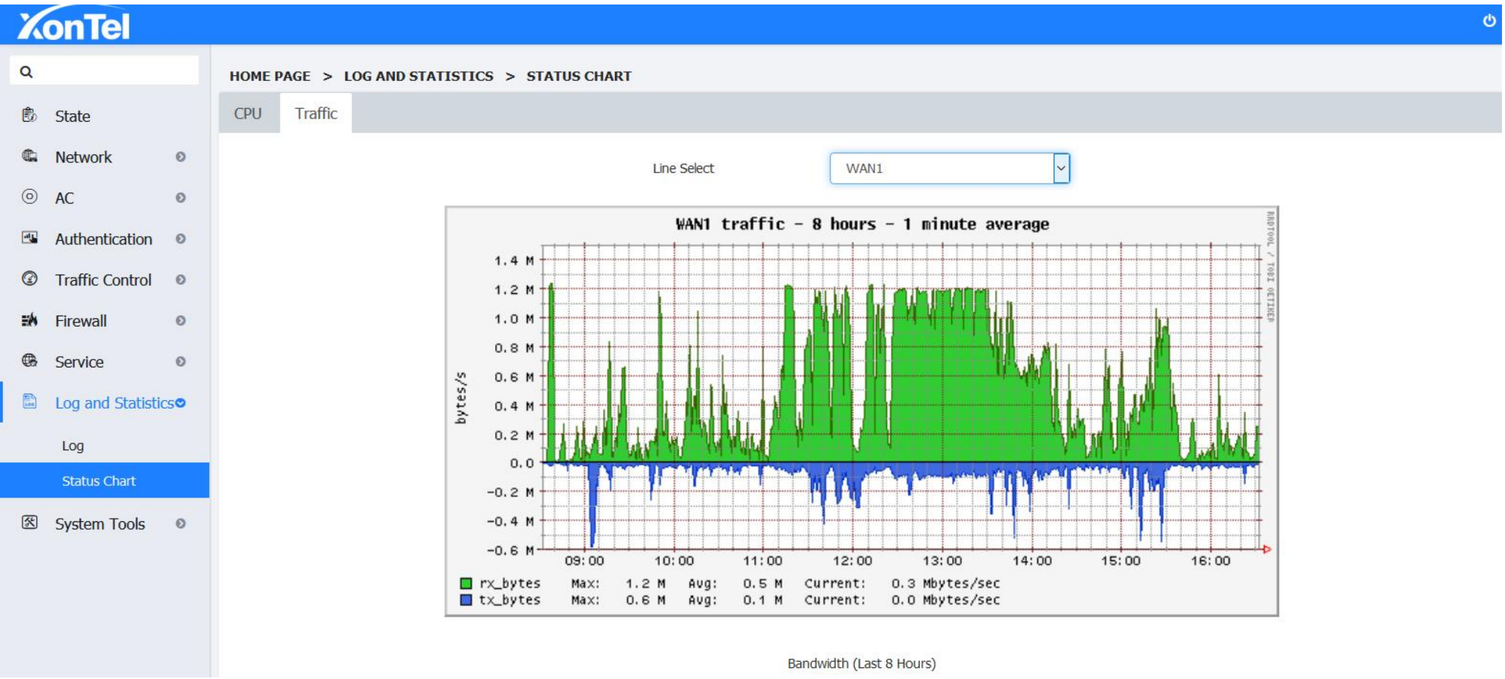
<One Day>



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.

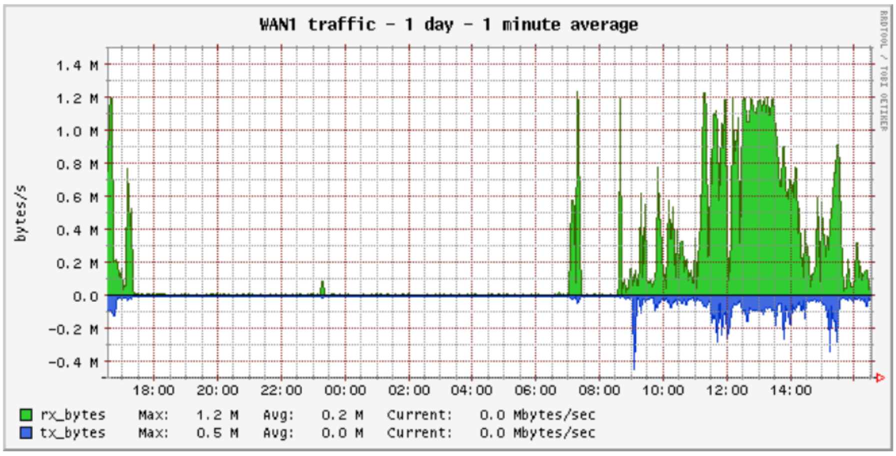


Line Select WAN1

WAN1 traffic - 8 hours - 1 minute average
bytes/s
1.4 M
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0.0
-0.2 M
-0.4 M
-0.6 M
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
RRDTOOL / TOBI OETIKER
🟩 rx_bytes Max: 1.2 M Avg: 0.5 M Current: 0.3 Mbytes/sec
🟦 tx_bytes Max: 0.6 M Avg: 0.1 M Current: 0.0 Mbytes/sec

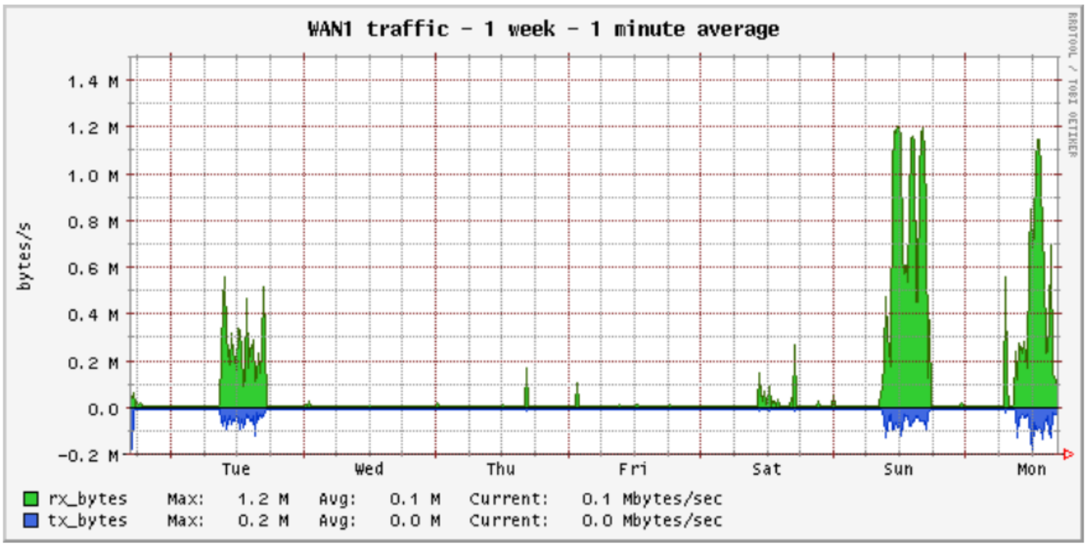
Bandwidth (Last 8 Hours)

<8 Hours>



Bandwidth (Last 1 Day)

<One Day>



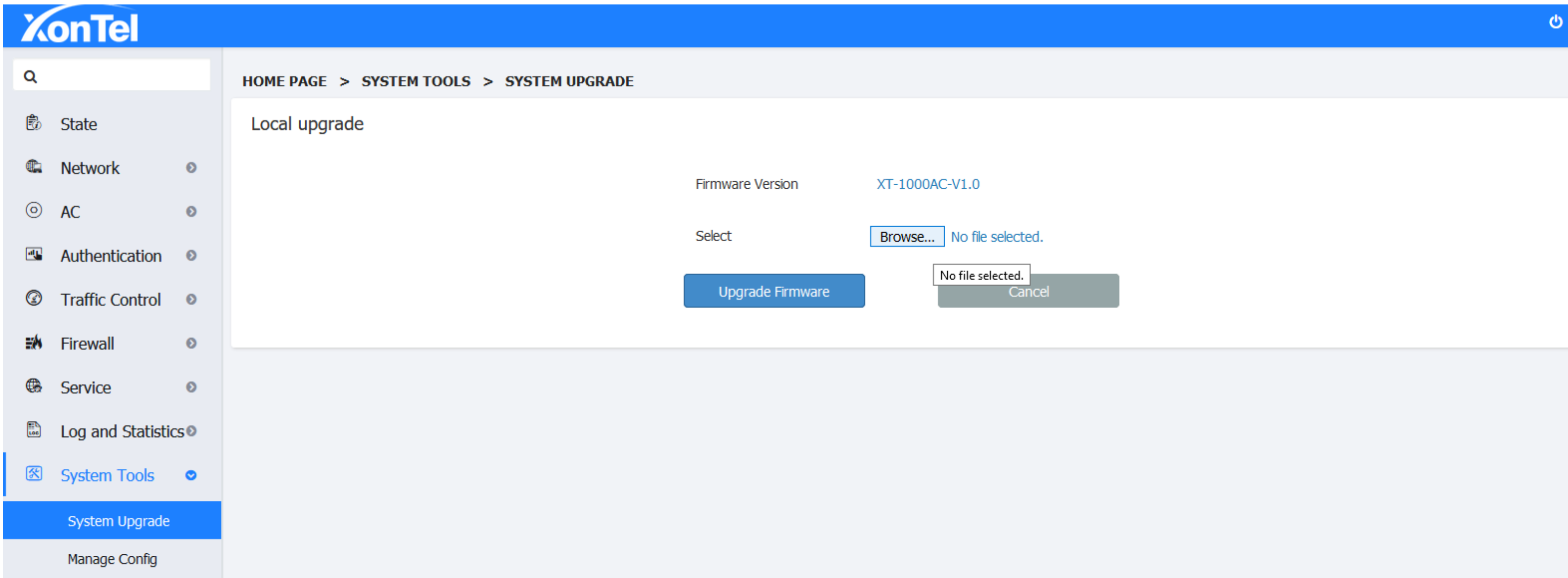
Bandwidth (Last 1 Week)

<One Week>

10 System Tools

10.1 System upgrade

Download the latest XT-1000AC firmware from the website https://xontel.com, download and save it on the computer. Go into the system upgrade page, click Browse to choose the firmware file you had downloaded in this page. Then click "Upgrade Firmware " button to upgrade.



HOME PAGE > SYSTEM TOOLS > SYSTEM UPGRADE

Local upgrade

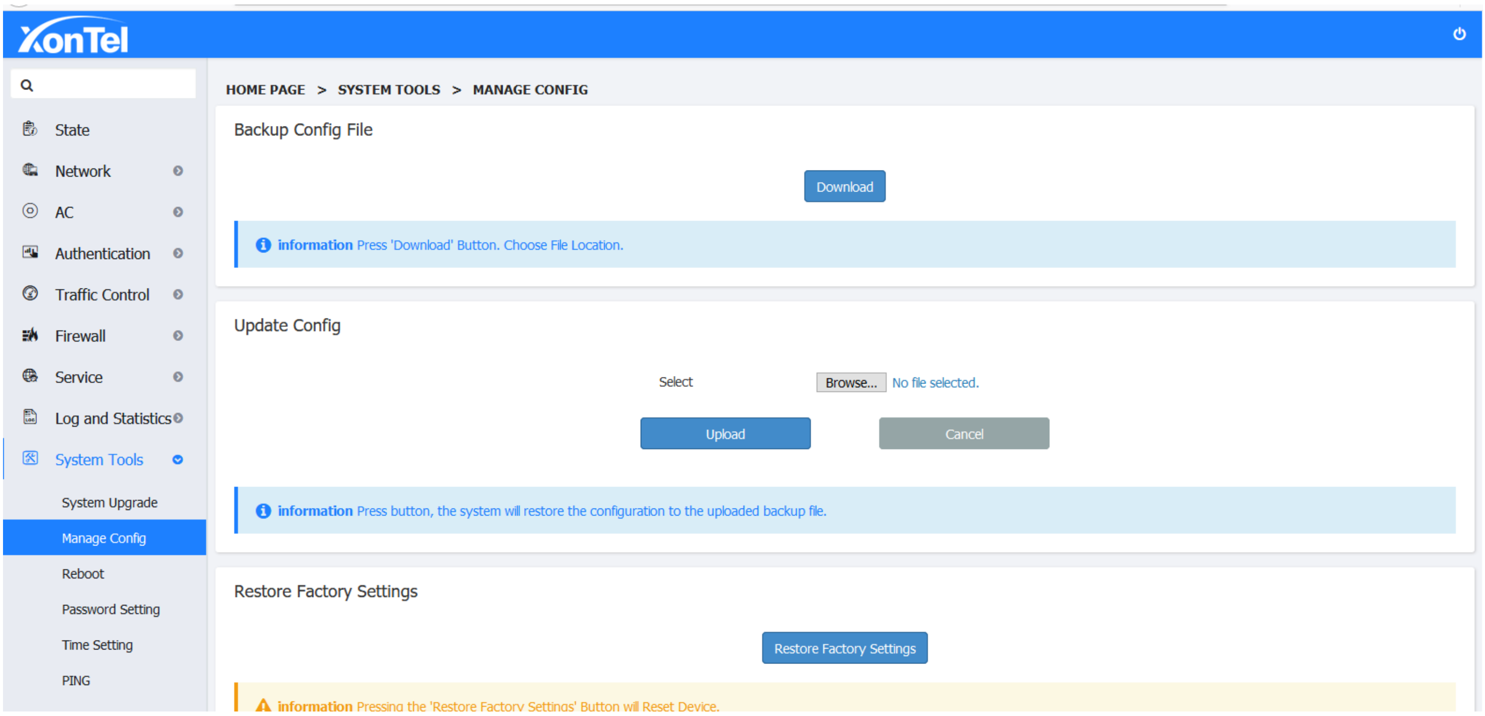
Firmware Version XT-1000AC-V1.0

Select Browse... No file selected.

No file selected.

10.2 Manage Config

Backup Config: After you configure the device's parameters, you can click "download" button to save the configure parameters in file to be used later.



HOME PAGE > SYSTEM TOOLS > MANAGE CONFIG

Backup Config File

information Press 'Download' Button. Choose File Location.

Update Config

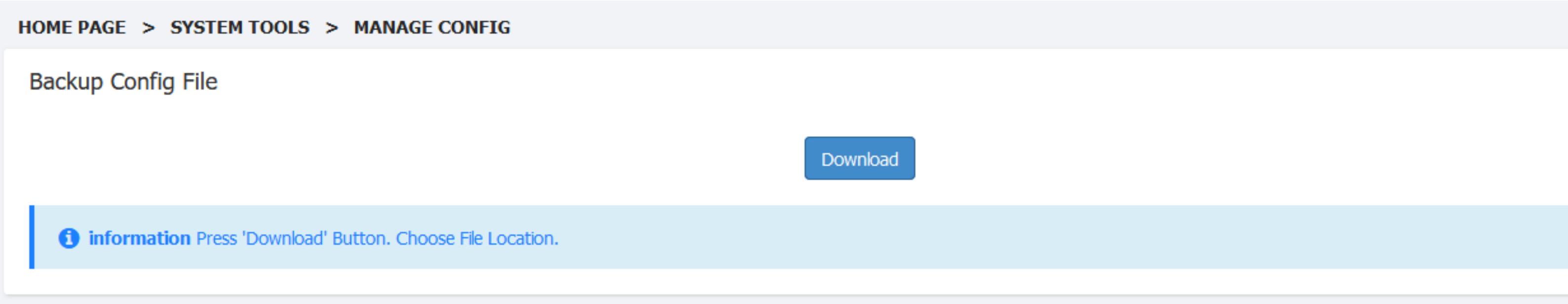
Select Browse... No file selected.

information Press button, the system will restore the configuration to the uploaded backup file.

Restore Factory Settings

information Pressing the 'Restore Factory Settings' Button will Reset Device.

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



HOME PAGE > SYSTEM TOOLS > MANAGE CONFIG

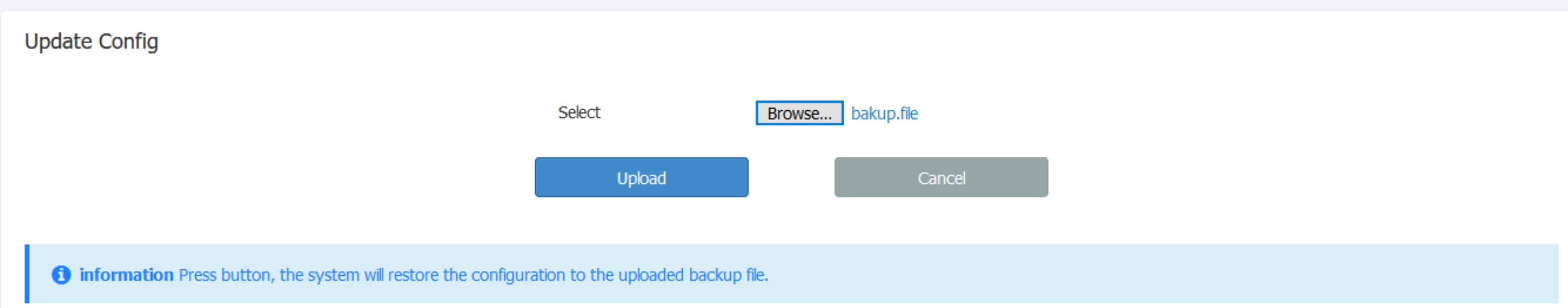
Backup Config File

information Press 'Download' Button. Choose File Location.

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

Update Config: If you need to change the configure temporary or the device was restored the default settings, you can select to choose the configure file that you save before.

1. Choose the configure file that you save before, Click "Upload" button to restore.

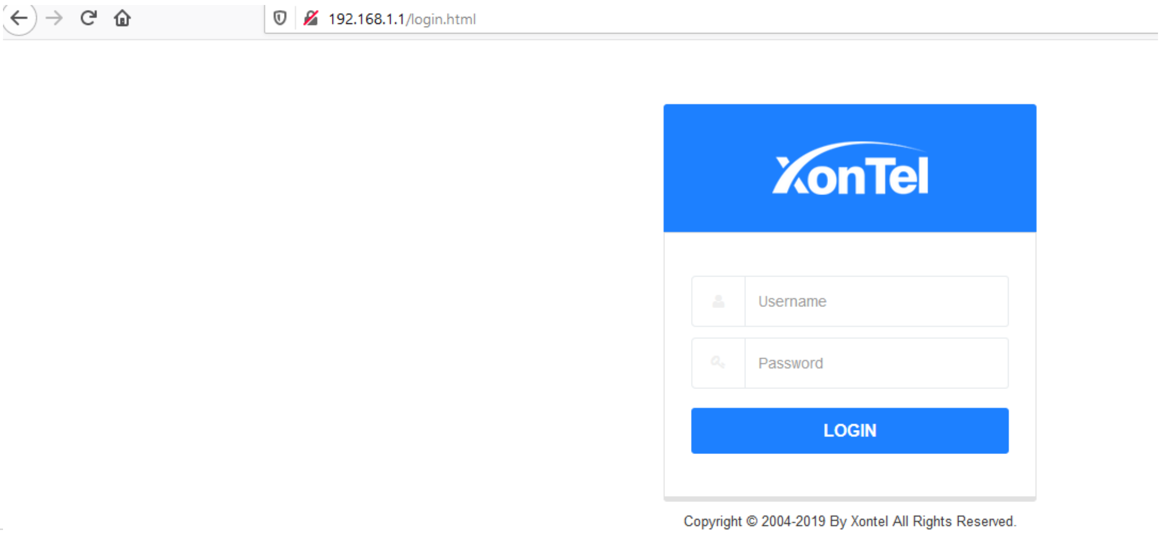


Update Config

Select Browse... bakup.file

information Press button, the system will restore the configuration to the uploaded backup file.

2. Click "Upload" and after a while system will popping the interface to login again.

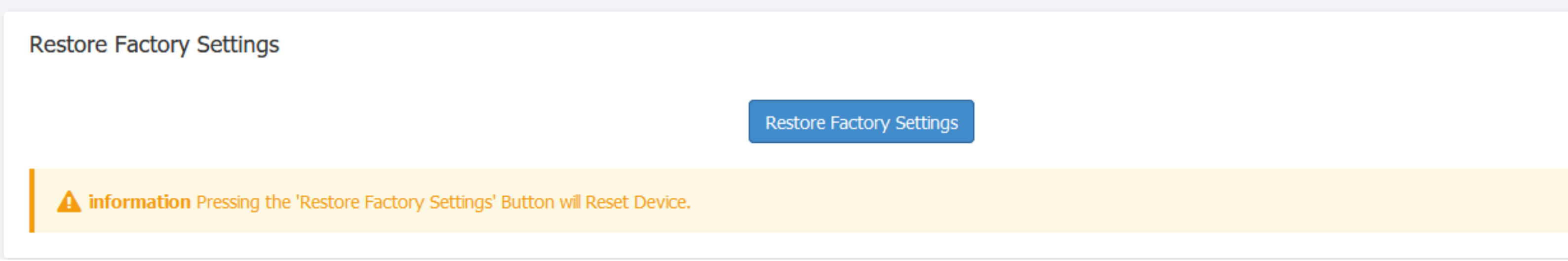


192.168.1.1/login.html

Copyright © 2004-2019 By Xontel All Rights Reserved.

Restore Factory Settings: If you want to reset the device to its factory default, you can click "Restore Factory Settings" button at the bottom of the Manage Config page.

1. **Go to the Manage Config page, click "Restore Factory Settings"**

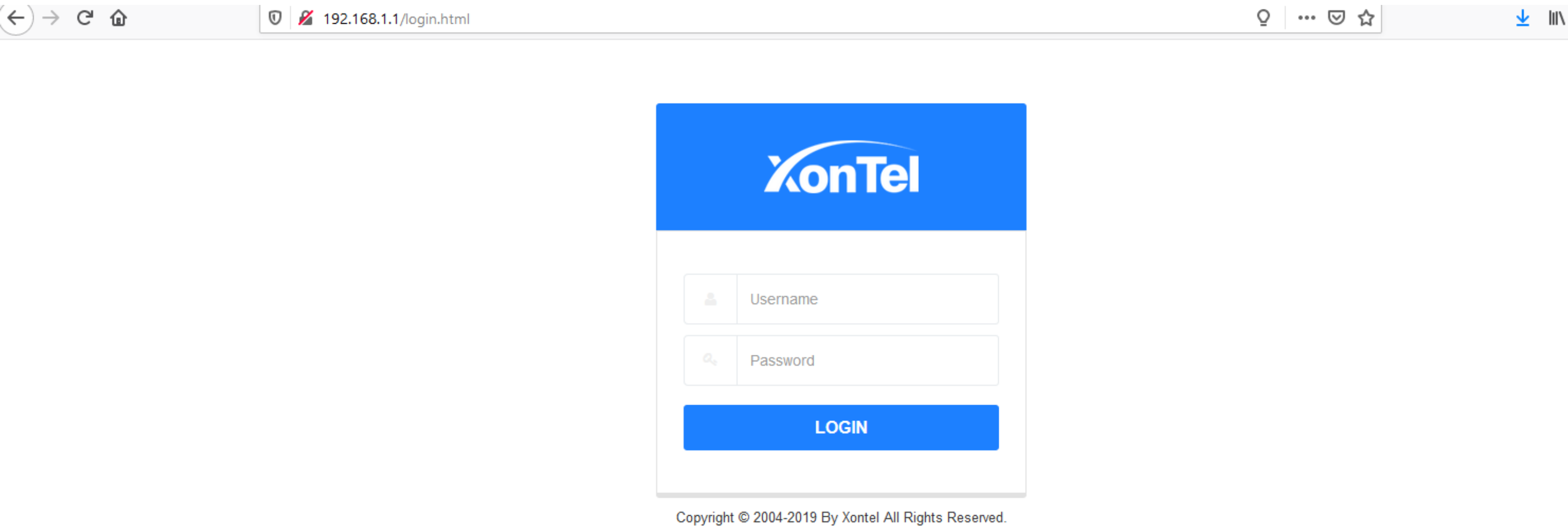


Restore Factory Settings

⚠ information Pressing the 'Restore Factory Settings' Button will Reset Device.

2. **System will pop the notice information, configuration will set to factory defaults, please wait for <180> seconds and Do Not disconnect the power.**

3. **3 minutes later system will automatic interface to login again, it is success to restore factory settings.**

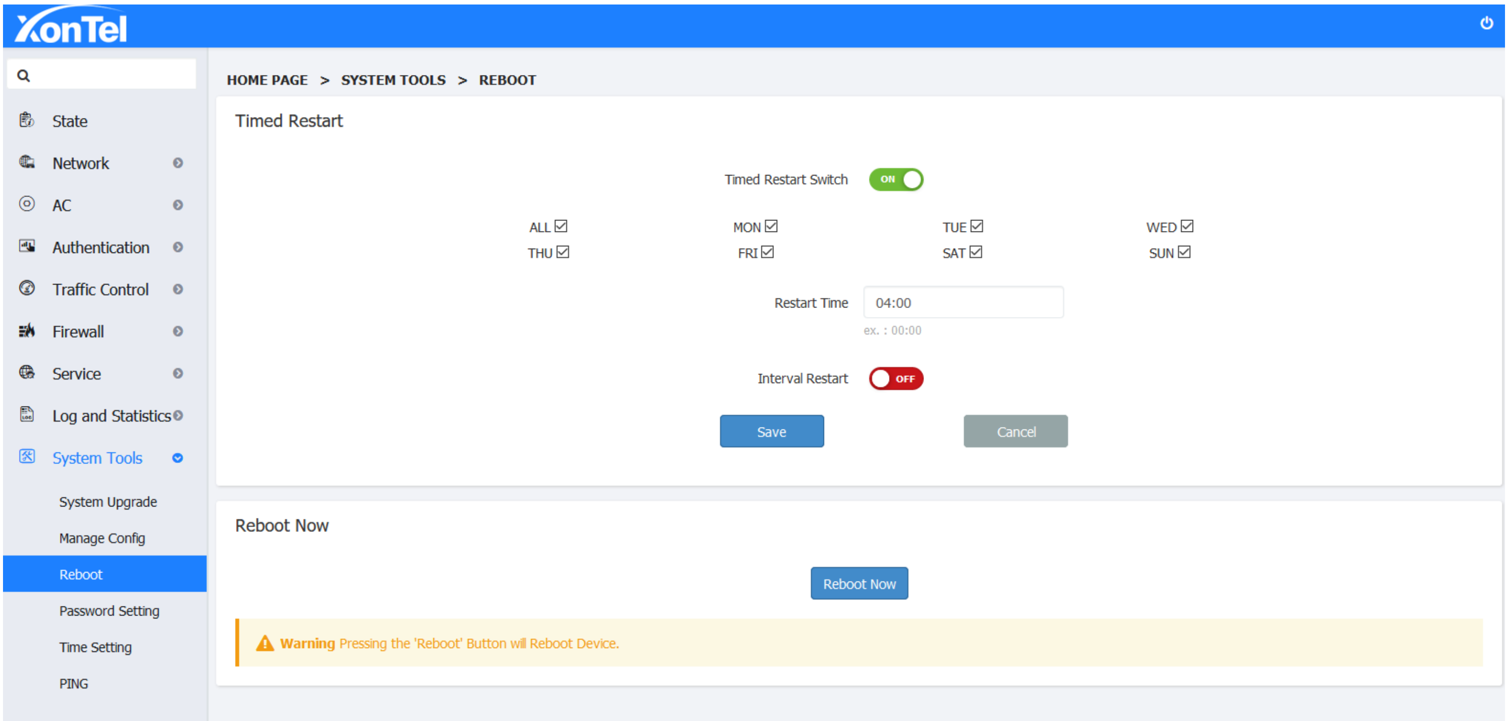


Copyright © 2004-2019 By Xontel All Rights Reserved.

10.3 System Reboot

10.3.1 Timed Restart

1. Go into the System Tools- Reboot page, you can On or Off scheduled reboot, select or remove the restart days of week, input the restart time click Save.



Timed Restart

Timed Restart Switch: ON

ALL ☑ MON ☑ TUE ☑ WED ☑
THU ☑ FRI ☑ SAT ☑ SUN ☑

Restart Time: 04:00
ex. : 00:00

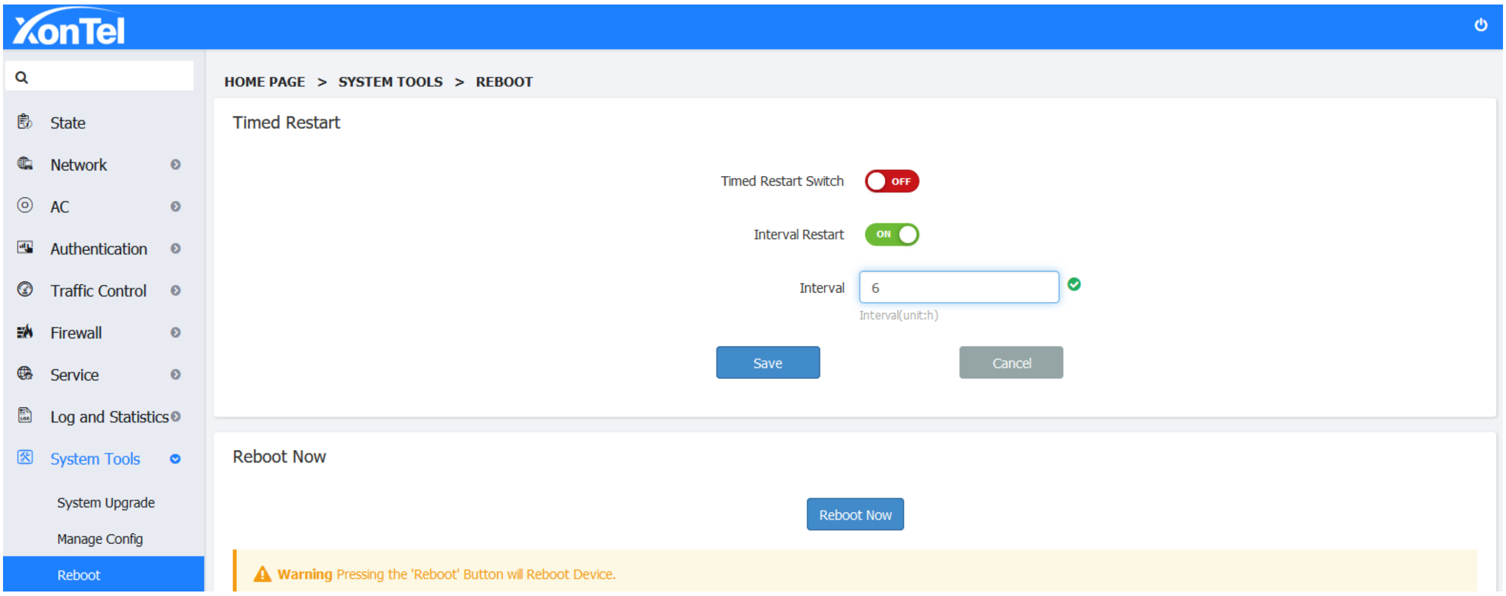
Interval Restart: OFF

Reboot Now

Warning Pressing the 'Reboot' Button will Reboot Device.

2. After this setup the device will restart automatically on the days and time your setup above.

Interval Restart: Go into the System Tools-reboot page, you can set up an interval Restart. Turn On the Interval Restart, input the interval restart time, click Save. As shown below the device restarts every 6 hours.



Timed Restart

Timed Restart Switch: OFF

Interval Restart: ON

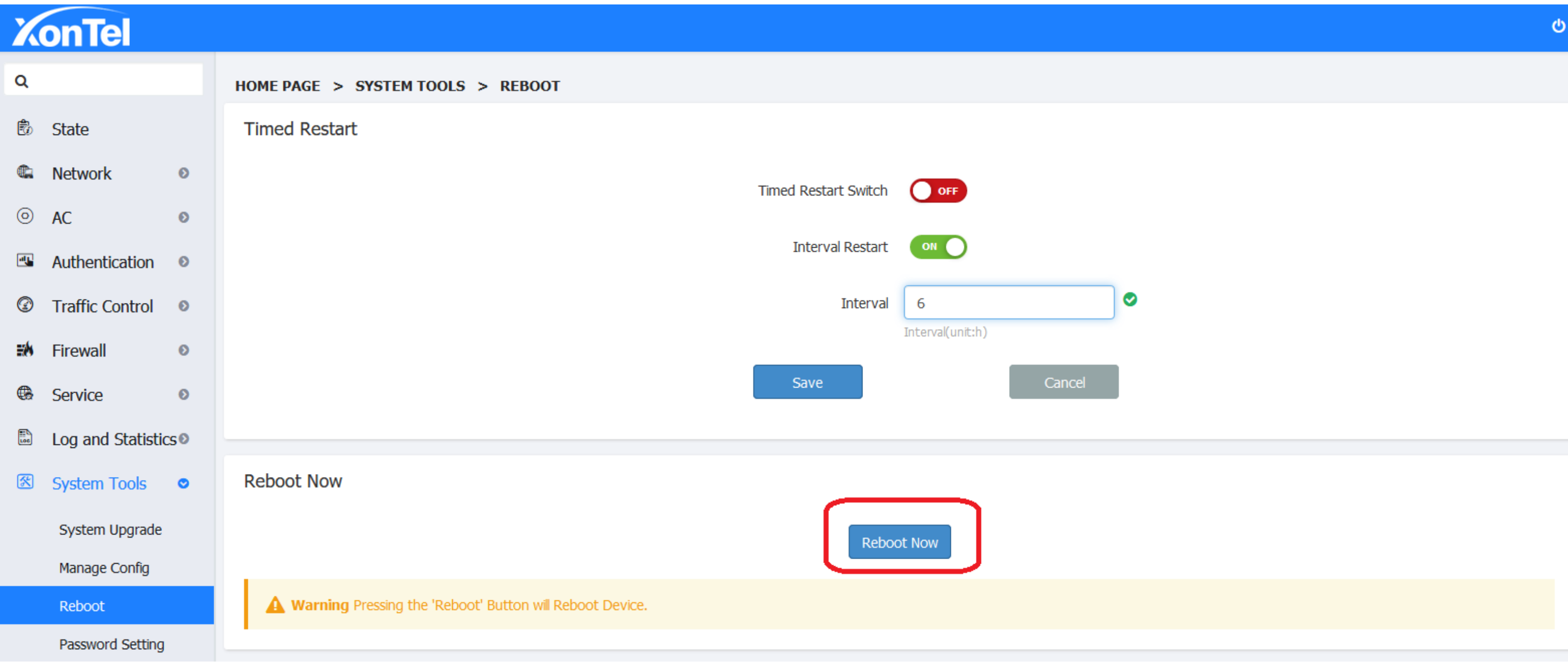
Interval: 6
Interval(unit:h)

Reboot Now

Warning Pressing the 'Reboot' Button will Reboot Device.

10.3.2 Reboot Now

1. If system required immediate restart go into the System Tools-Reboot page, click “Reboot Now” button.



Timed Restart Switch: OFF

Interval Restart: ON

Interval: 6

Interval(unit:h)

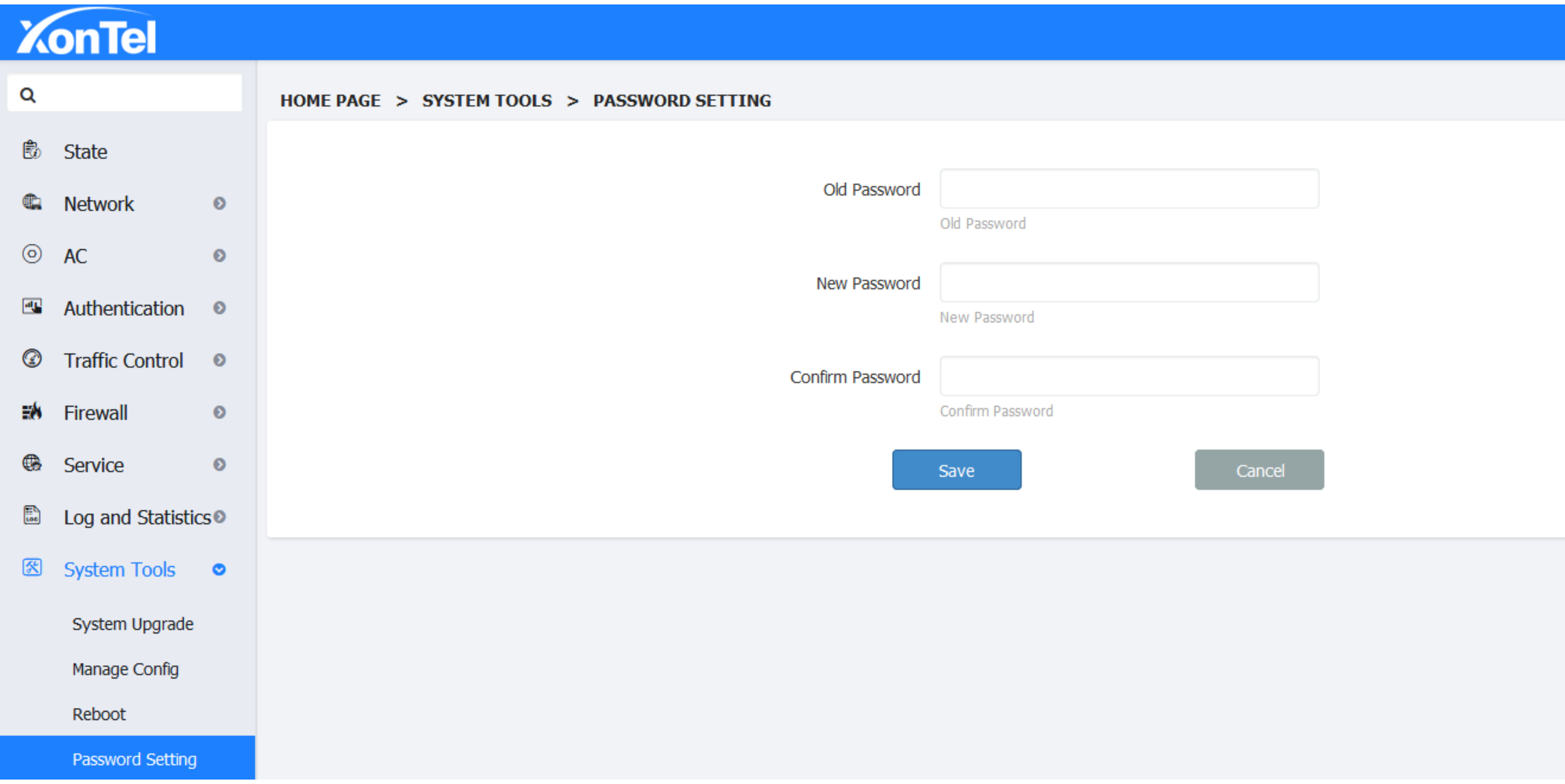
Warning Pressing the 'Reboot' Button will Reboot Device.

2. Wait for 1 minute for the system to come up again.

10.4 Password Setting

Here you can change the Admin Password. After setting you need to use the new password to login.

1. **Go into System home page and go to System Tools "Password Setting" page as below:**



Old Password
Old Password
New Password
New Password
Confirm Password
Confirm Password

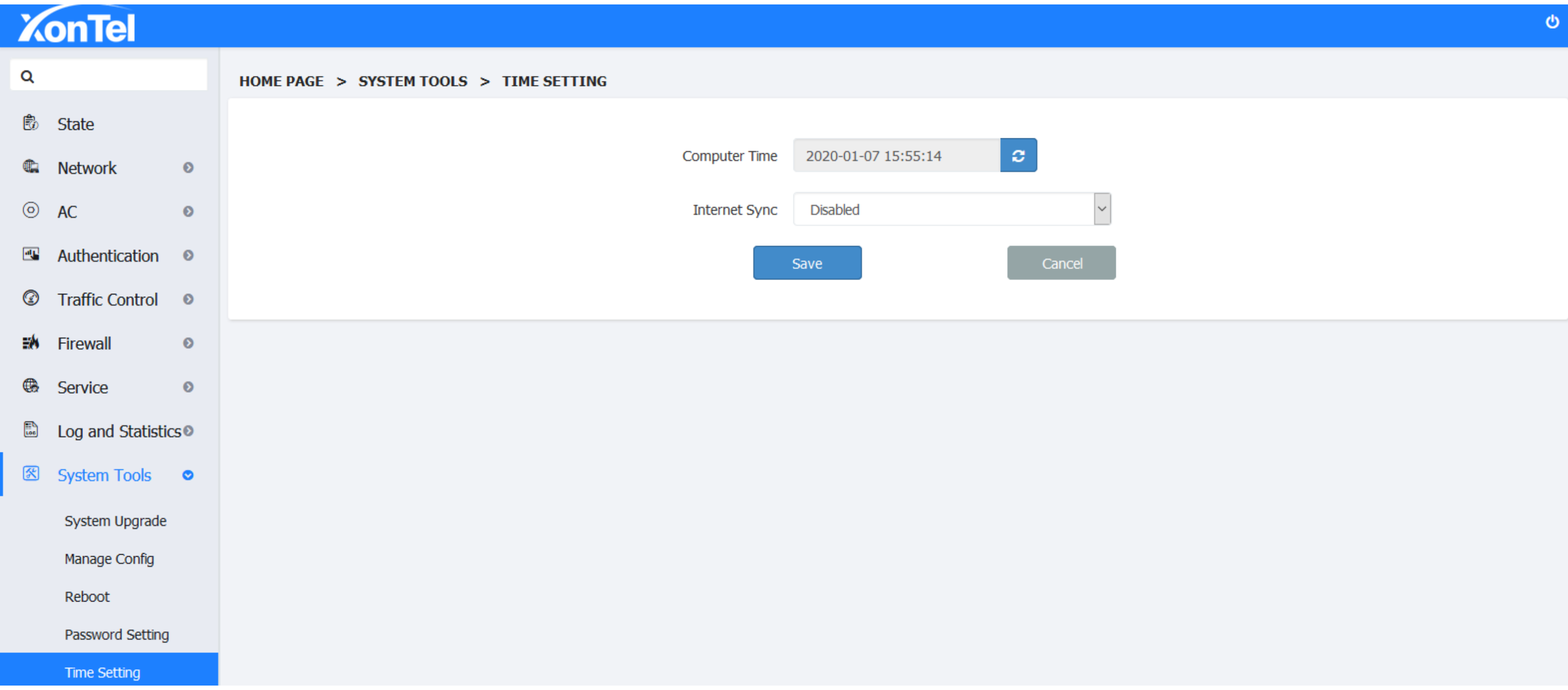
2. **Enter the new password two times and click Save:**

3. **After setting you need to use the new password to login again.**

10.5 Time Setting

Here you can the sync the system time with Computer time from where you logged in, Enable/Disable Internet Sync time. The device will be automatic sync system time with NTP server configured.

1.Go into System home page and go to System Tools -“Time Setting” page as below:

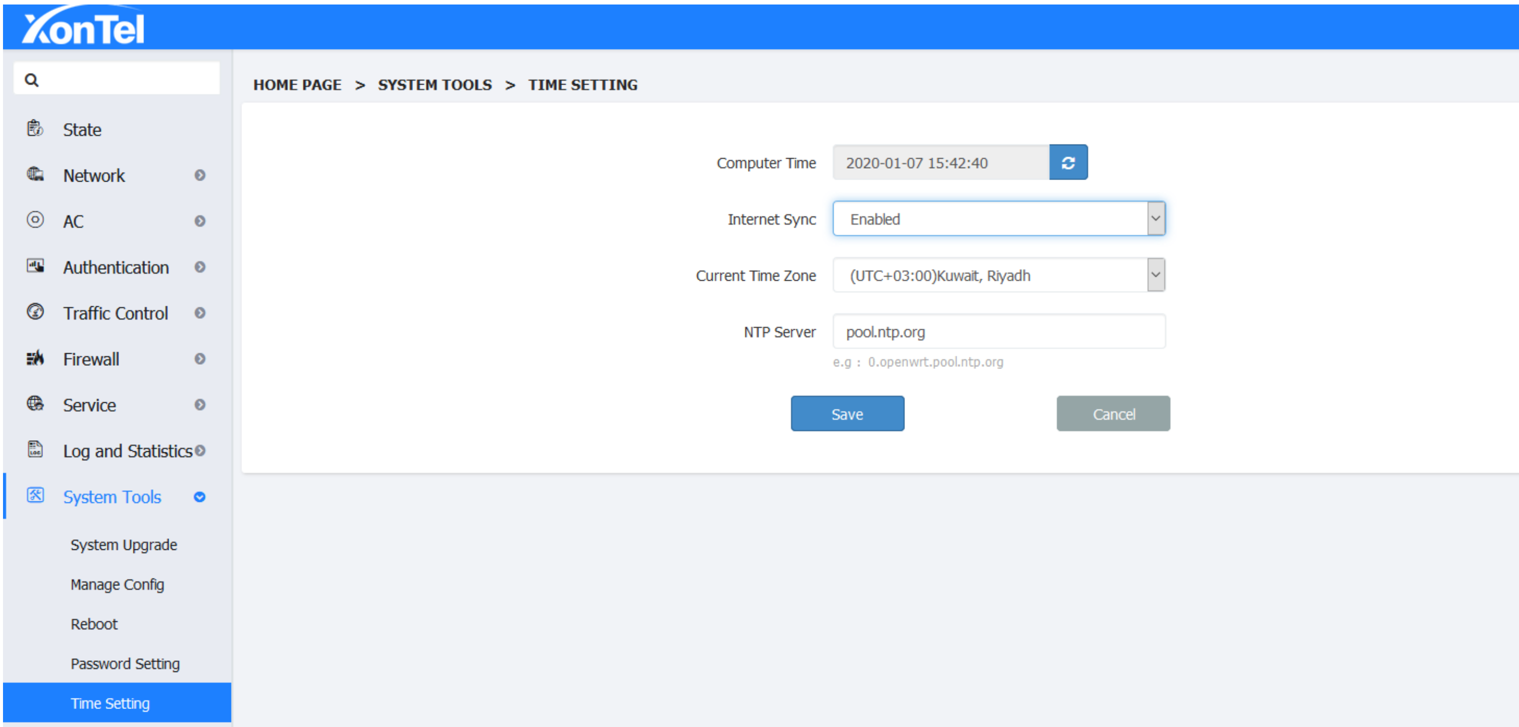


HOME PAGE > SYSTEM TOOLS > TIME SETTING

Computer Time: 2020-01-07 15:55:14

Internet Sync: Disabled

2. Click Internet Sync switch’s button, choose “Enabled” then click Save.



HOME PAGE > SYSTEM TOOLS > TIME SETTING

Computer Time: 2020-01-07 15:42:40

Internet Sync: Enabled

Current Time Zone: (UTC+03:00)Kuwait, Riyadh

NTP Server: pool.ntp.org

e.g： 0.openwrt.pool.ntp.org

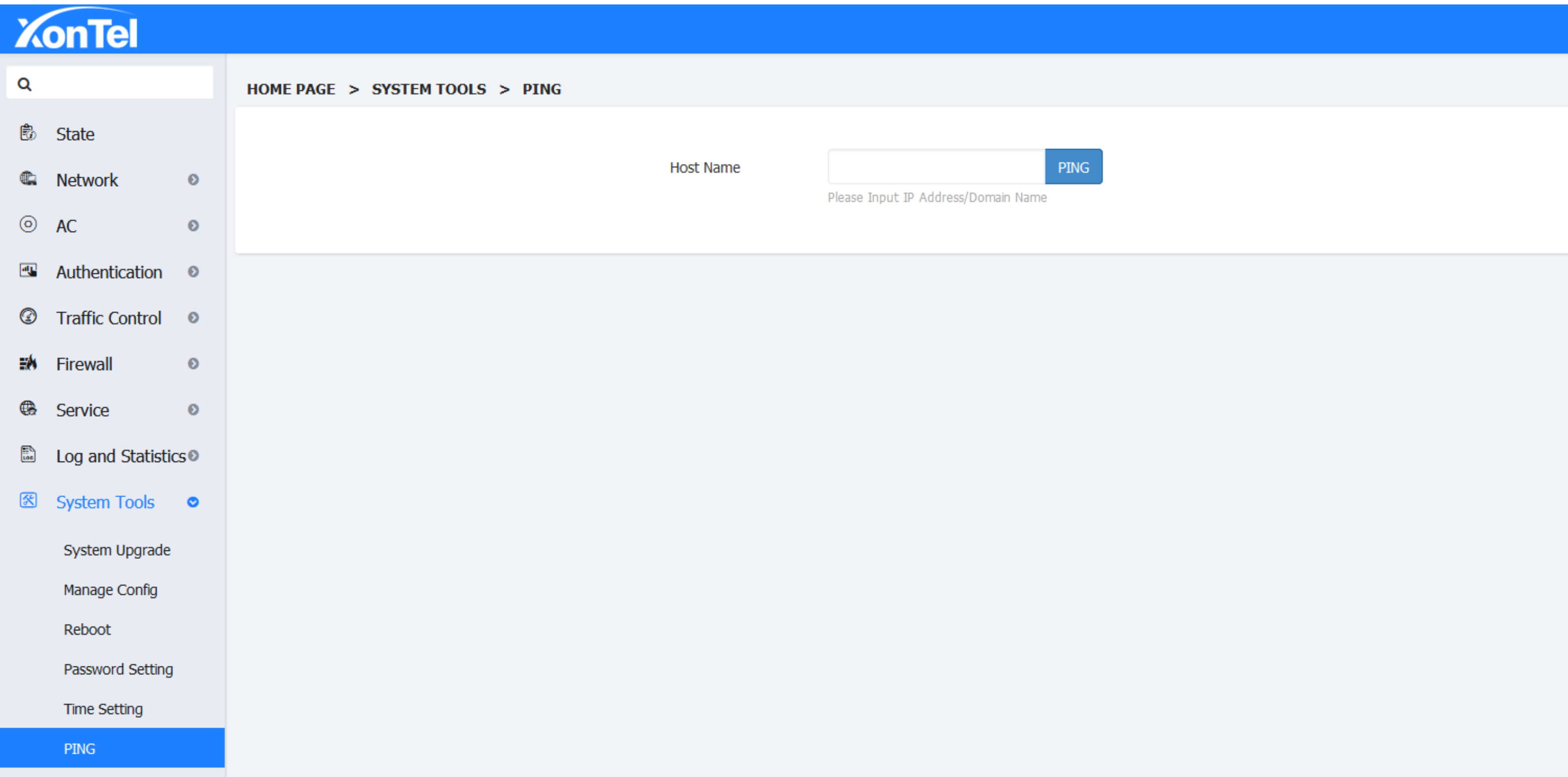
3. Wait for 5 seconds, the system time will be synchronized with the network time.

4. Disable the Internet Sync, use the option to sync time from the computer from which you logged in. This will be a onetime sync.

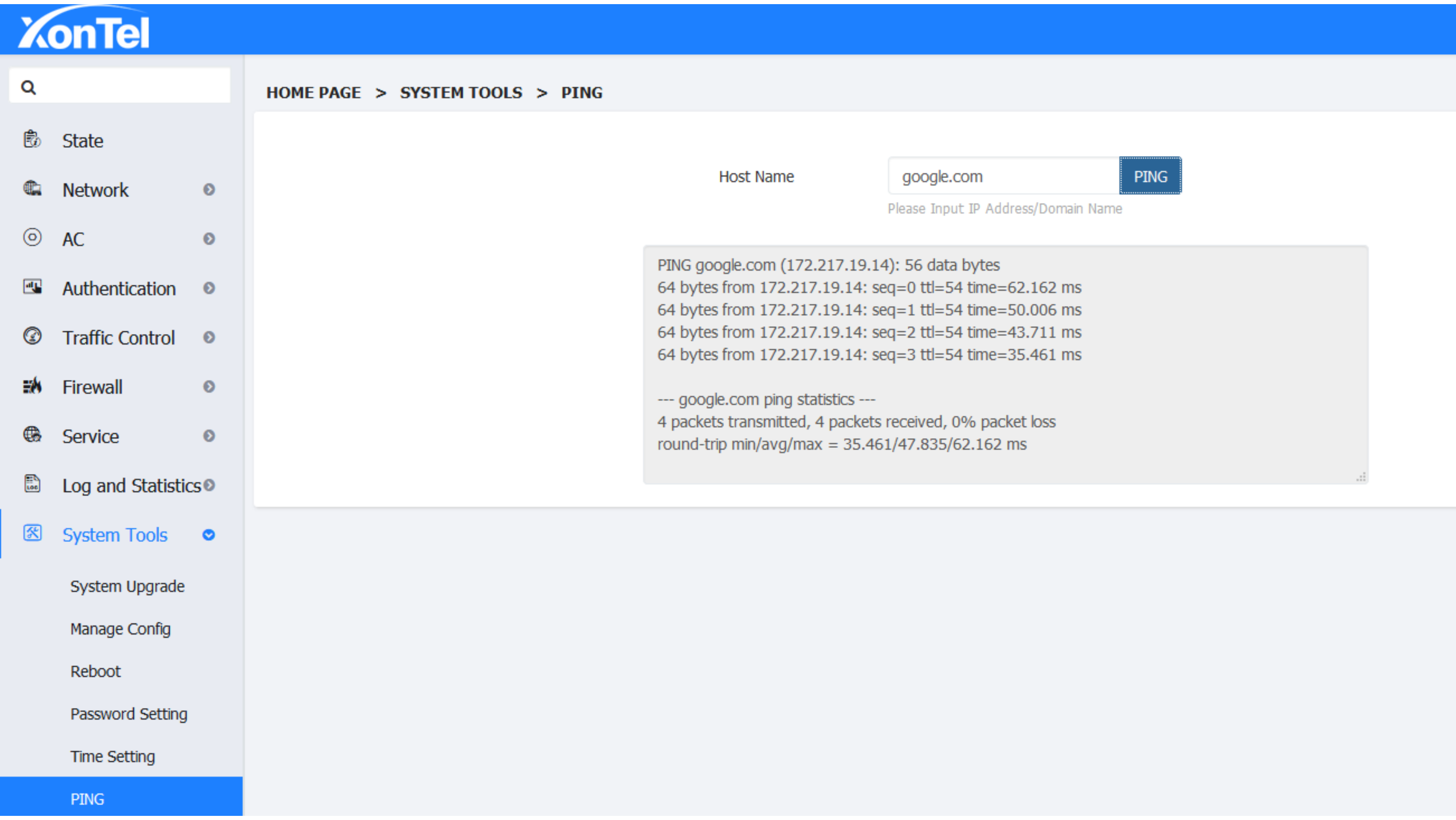
10.6 PING (Diagnostic Tool)

Here you can PING any IP address or Domain name to confirm the connectivity of the system to Internet.

1. Go into system home page and go to the System Tools "PING" page as below:



3. Enter IP address of google.com as 8.8.8.8 or the domain google.com itself, click "PING" button, wait some seconds, it will show the result as below:



Host Name: google.com

```
PING google.com (172.217.19.14): 56 data bytes
64 bytes from 172.217.19.14: seq=0 ttl=54 time=62.162 ms
64 bytes from 172.217.19.14: seq=1 ttl=54 time=50.006 ms
64 bytes from 172.217.19.14: seq=2 ttl=54 time=43.711 ms
64 bytes from 172.217.19.14: seq=3 ttl=54 time=35.461 ms

--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 35.461/47.835/62.162 ms
```