Wireless Dual-Mode IoT Controller

R206A
User Manual

For IPK Version 0.0.0.98 and above

Table of Content

1. Introduction

R206A is a highly reliable wireless integrated control box. R206A can communicate with the devices of LoRa protocol and Zigbee. It acts as a gateway between the devices of LoRa protocol and Zigbee. It can automatically join the network and execute the configuration. It is the core control of Netvox M2 Internet of Things network. R206A is equipped with Wi-Fi technology; therefore, mobile devices (such as mobile phone) can easily control local IoT devices.

R206A connects to the Internet and combines with the Netvox cloud service platform to achieve remote monitoring. When going out, the user can connect to the cloud to access R206A through the Internet that is achieving remote control of IoT devices

The user can also remotely browse the surveillance camera, master all changes on the other side, and easily realize the Internet of Things remote control.

LoRa wireless technology:

LoRa is a wireless communication technology dedicated to long-distance low-power consumption. Its spread-spectrum modulation method greatly increases the communication distance compared with other communication methods, and can be widely used in long-distance low-rate IoT wireless communication fields in various occasions. Such as automatic meter reading, building automation equipment, wireless security systems, industrial monitoring and control. It has the characteristics of small size, low power consumption, long transmission distance and strong anti-interference ability.

ZigBee wireless technology:

ZigBee is a short range wireless transmission technology based on IEEE802.15.4 standard and supports multiple network topologies such as point-to-point, point-to-multipoint, and mesh networks. It is defined for a general-purpose, cost-effective, low-power-consumption, low-data-rate, and easy-to-install wireless solution for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation and home automation, etc.

Netvox Private LoRa Protocol:

A private wireless communication protocol based on LoRa long distance, low power consumption, CSMA/CA mechanism, and AES128 encryption mode.

Netvox Private LoRa Protocol band is as follows:

500.1 MHz_China Region

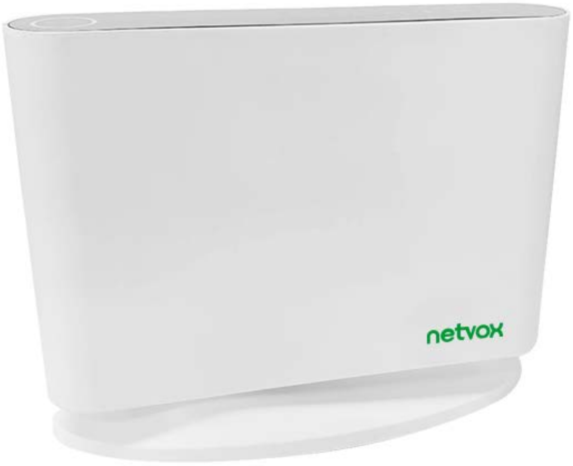
920.1 MHz_ Asia Region (includes Japan, Singapore, Southeast Asia and other regions)

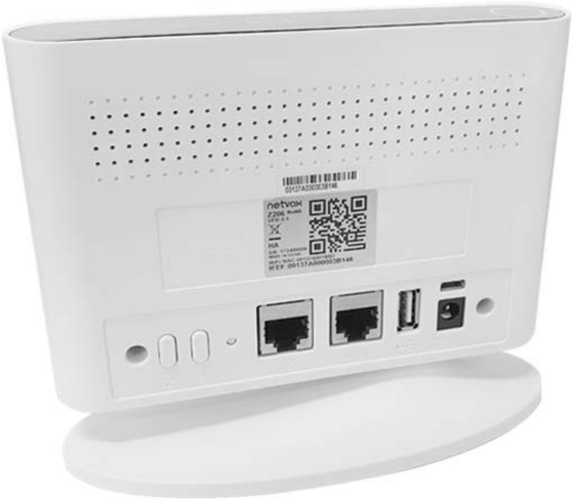
865.2 MHz_ India Region

868.0 MHz_ EU Region

915.1 MHz_ AU/US Region

2. Product Appearance



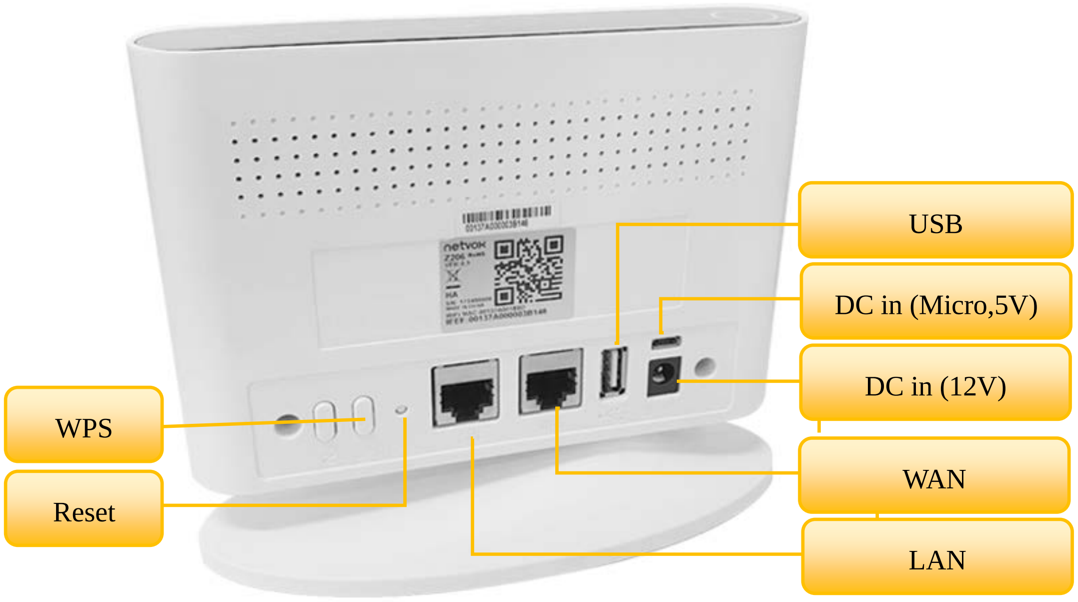


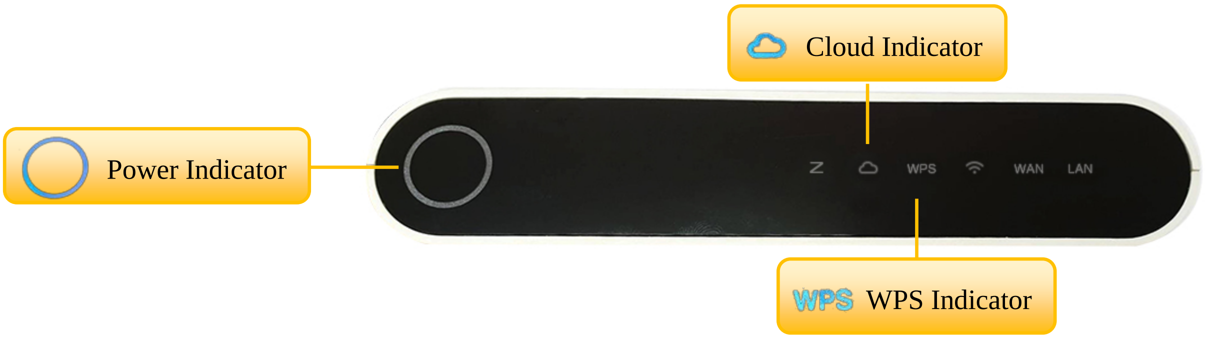
3. Main Characteristics

- Support Wi-Fi 1～14 channels (according to the regulation of each country)
- Two RJ-45(WAN/LAN)
- RTC (Real-time clock)
- Support LoRa and Zigbee
- Support 3.5G/4G USB dongle
- Support gateway / bridge / wi-fi AP mode
- Provide a web interface which can be set through a browser and is easy to operate
- As a Proprietary LoRa gateway, it can limit the devices that be joined to the network

4. Installation and Preparation

4.1 R206A Port/Indicator Instruction





4.2 Hardware Connection

A. Hardware Connection

(1) When use R206A alone

Connect the external network cable to the WAN of R206A.

(2) When connect with an IP camera

Connect one end of the network cable to the LAN of R206A, and connect the other end to the network port of the IP Camera to form an internal network. Then, connect the WAN port of R206A to the external network cable. (It doesn’t matter if do not connect the external network.)

(3) When connect with several IP cameras

It can connect the LAN of R206A to network expansion equipment (such as Router, Switch, or Hub) to increase the number of LANs. The network port of each IP Camera is connected to the network expansion device to form an internal network and connect the WAN port of R206A to the external network cable. (It doesn’t matter if do not connect the external network.)

(4) When connect IP Camera wirelessly

Connect the Wi-fi of the IP Camera to the R206A Wi-fi to form an internal network, and connect the WAN port of R206A to the external network cable. (It doesn’t matter if do not connect the external network.)

B. Power On

Plug in the DC 12V transformer, and then turn it on after the power indicator lights up, or use a 5V Micro USB transformer for power supply.

C. Reset Key Function

(1) Press the reset button in the power-on state, and the device will restart.

(2) Press and hold the Reset button for more than 5 seconds in the power-on state, and the device will restore to the factory setting.

D. WPS Button Function

(1) In the power-on state, press the WPS button to turn on the WPS function. Press the WPS of the device which the user wants to connect to Wi-fi within three minutes (such as mobile phone, tablet), and the device can connect to Wi-fi.

(2) If press the WPS button again within three minutes, the WPS function will be cancelled.

E. Indicator

Power Indicator	After power on, it stays on.
	After power off, the light turns off.
Cloud Indicator	When connected to the cloud, it stays on.
	When not connected to the cloud, the light is off.
WPS Indicator	After pressing the WPS button, the indicator light starts flashing to indicate that the WPS function is activated. If it successfully connects to the network, the light will stay on.
	If it doesn’t connect to the network within three minutes, the light will flash for 5 seconds and then turns off, indicating that the WPS function is off.
Wi-Fi Indicator	When the Wi-Fi function is turned on, the light keeps on.
	When the Wi-Fi function is turned off, the light turns off.
WAN/LAN Indicator	When the WAN/LAN is connected and operating normally, the light stays on.
	When the WAN/LAN is removed, the light turns off.

F. Backup Power

R206A provides micro 5v backup power which can be externally connected to mobile power, UPS power supply, etc.

Example:

Power Bank Capacity: 4400mAh/ Input: 100V-240V AC/ Output: 12V 1A

The power bank can make R206A work continuously for more than 6 hours.

(For reference only, please refer to the capacity of each brand.)

5. Network Management Interface Description

5.1 Connect to the device

Please connect the R206A LAN port to your computer with a network cable, power on the R206A, and turn on the power switch.

5.2 Check Computer Network Setting

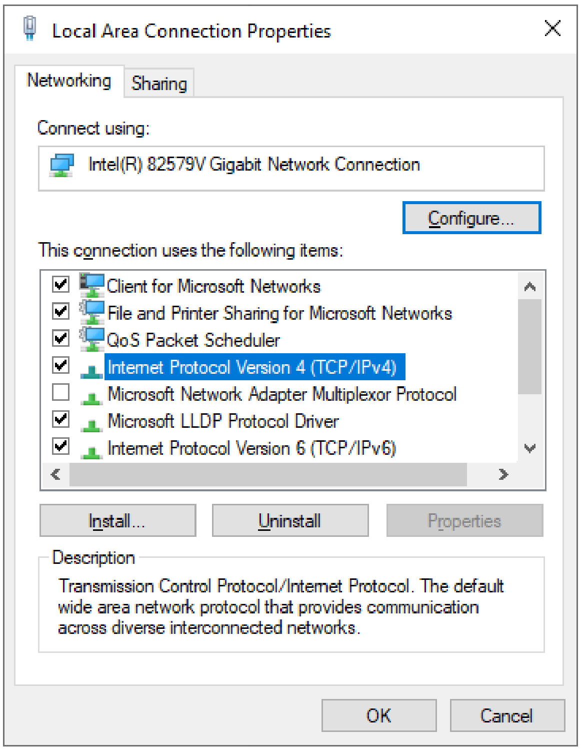
When setting up the network, please make sure that the computer obtains an IP automatically.

(1) Please connect the LAN of R206A to the computer and open the network setting.

(Take Win 10 operating system as an example.)

(2) Click the network icon in the lower right corner of the screen to enter the network setting. 🖳

(Or enter “Control Panel” > “Network and Internet” > “Network Connections” > Right click to open “Local Area Connection Properties” > “TCP/IPv4” > Obtain an IP address automatically)



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) 82579V Gigabit Network Connection

Configure...

This connection uses the following items:

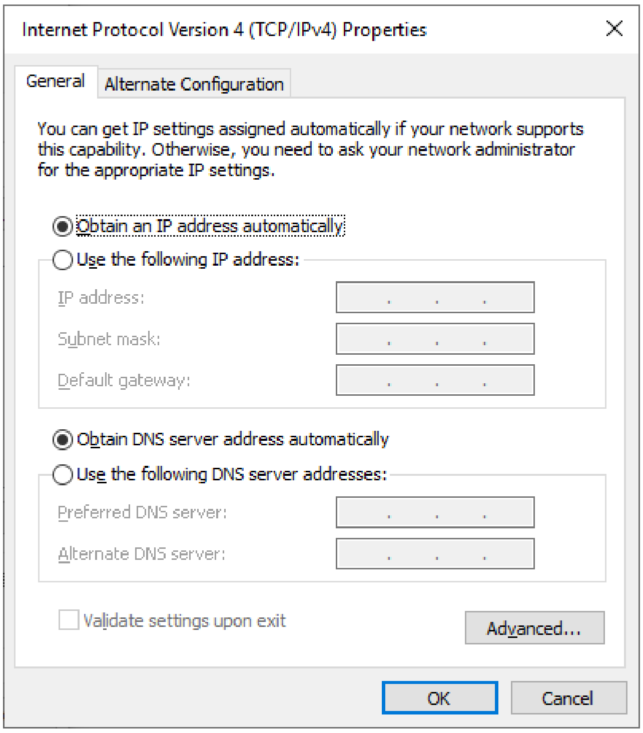
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK | Cancel

5.3 Log in to the management interface of R206A

Open the browser and log in to the setting screen of R206A

Default IP:

192.168.15.1

Default account / password

● Administrator:

operator / operator (The applicable gateway version is the shipment before 0.0.0.163)

operator / the last six codes of DevEUI (The applicable gateway version is the shipment after 0.0.0.163)

● Client:

admin / admin (The applicable gateway version is the shipment before 0.0.0.163)

admin / the last six codes of DevEUI (The applicable gateway version is the shipment after 0.0.0.163)

Note:

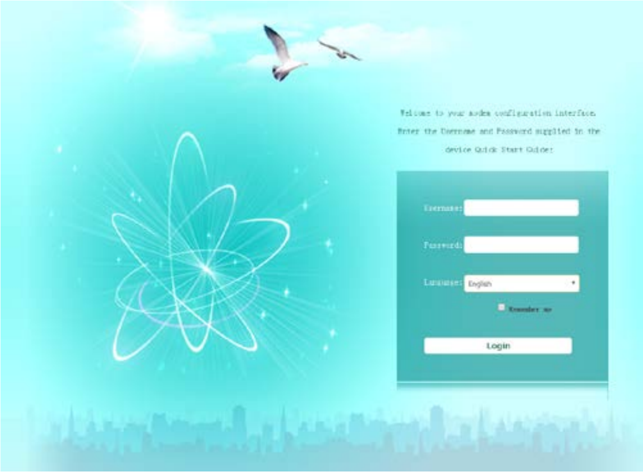
*It is recommended to change the password immediately when using it for the first time.

*Password Restriction: 1. It cannot be 123456.

2. The length must be greater than or equal to 6 digits.

3. It cannot be the same as the account.

*If the user uses mobile phone or tablet to connect to the Wi-Fi of R206A to log in to the setting screen of R206A, the Wi-Fi will be disconnected after setting. Therefore, the user needs to reconnect to the R206A Wi-Fi and then refresh the page.



Welcome to your modem configuration interface.
Enter the Username and Password supplied in the device Quick Start Guide:

Username:

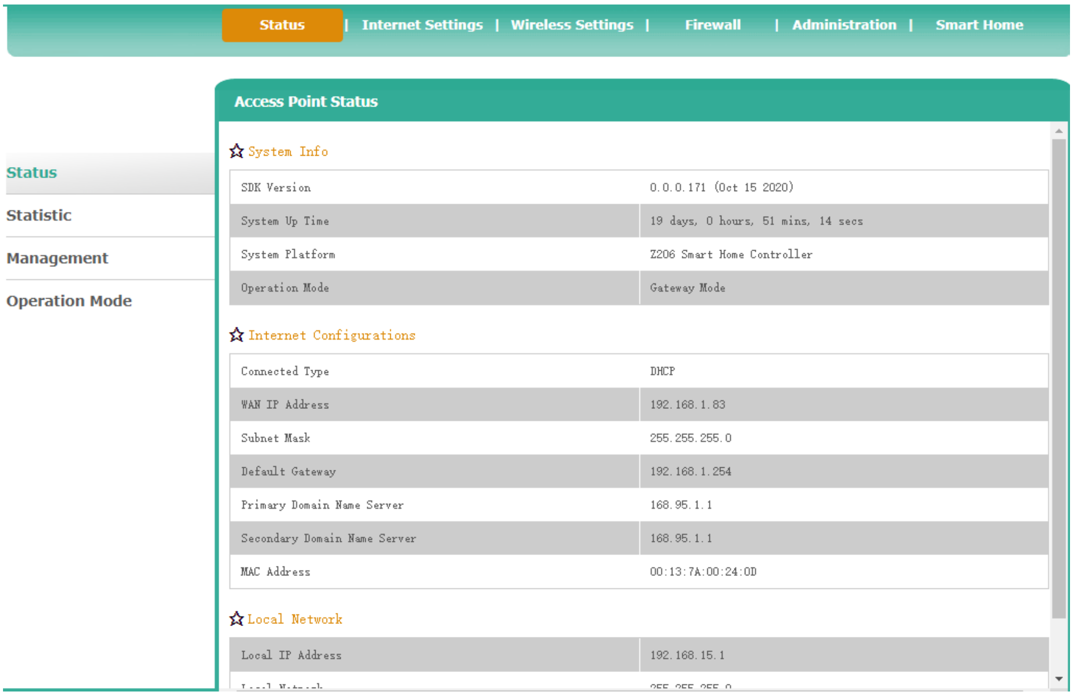
Password:

Language: English

□ Remember me

5.3.1 Status

Check the current system information and network status of the gateway



Access Point Status

☆ System Info

SDK Version	0.0.0.171 (Oct 15 2020)
System Up Time	19 days, 0 hours, 51 mins, 14 secs
System Platform	Z206 Smart Home Controller
Operation Mode	Gateway Mode

☆ Internet Configurations

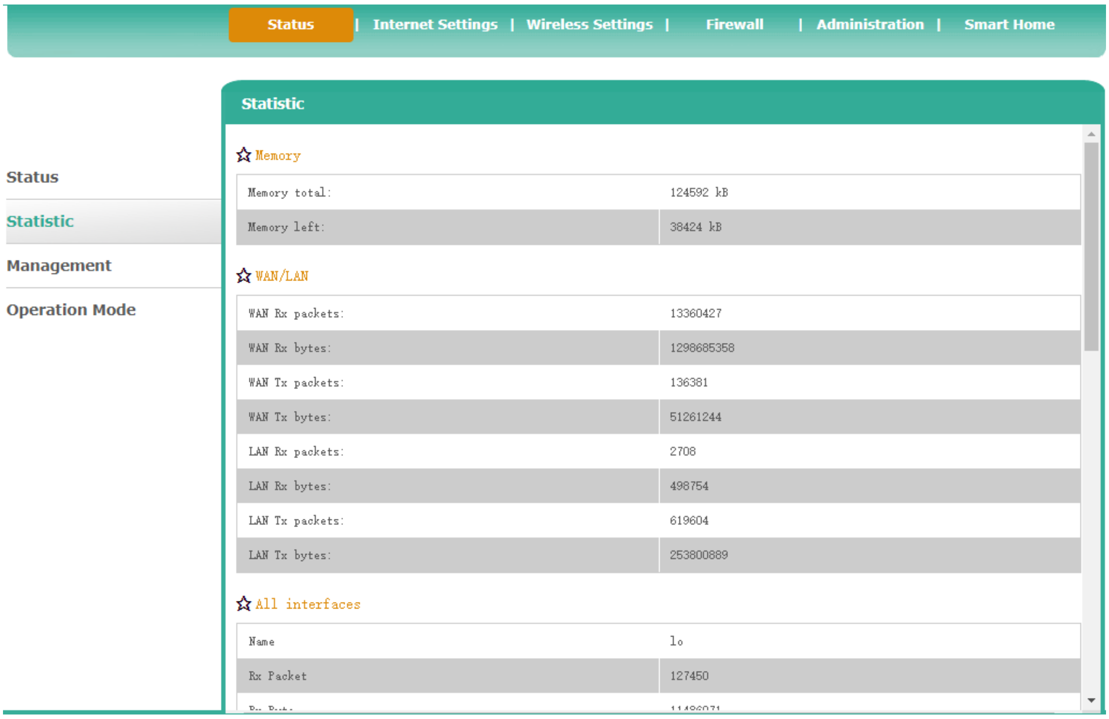
Connected Type	DHCP
WAN IP Address	192.168.1.83
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1
MAC Address	00:13:7A:00:24:0D

☆ Local Network

Local IP Address	192.168.15.1
Local Netmask	255.255.255.0

5.3.2 Statistic

Check the statistics of the gateway, including device memory capacity, WAN data packets, and LAN data packets.



Statistic

☆ Memory

Memory total:	124592 kB
Memory left:	38424 kB

☆ WAN/LAN

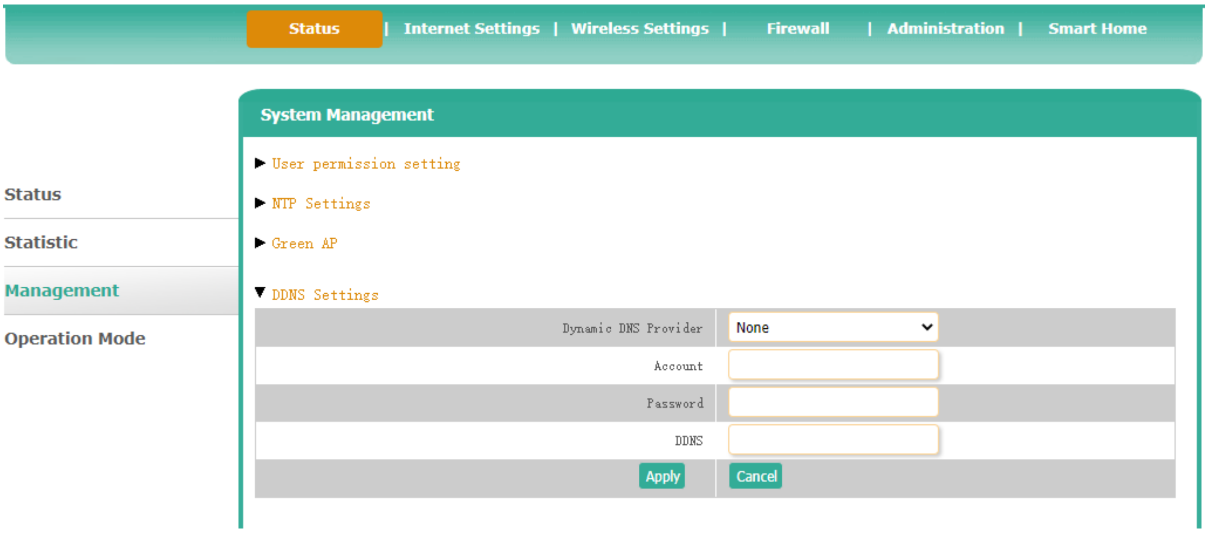
WAN Rx packets:	13360427
WAN Rx bytes:	1298685358
WAN Tx packets:	136381
WAN Tx bytes:	51261244
LAN Rx packets:	2708
LAN Rx bytes:	498754
LAN Tx packets:	619604
LAN Tx bytes:	253800889

☆ All interfaces

Name	lo
Rx Packet	127450
Rx Byte:	11486071

5.3.3 Management

Set User permission, NTP, Green AP, and DDNS.



System Management

▶ User permission setting

▶ NTP Settings

▶ Green AP

▼ DDNS Settings

Dynamic DNS Provider	None
Account	
Password	
DDNS	
Apply	Cancel

5.3.4 Operation Mode

Change the Operation Mode, such as Bridge mode, Gateway mode, AP Client mode, and decide whether to enable NAT.

A. Bridge mode

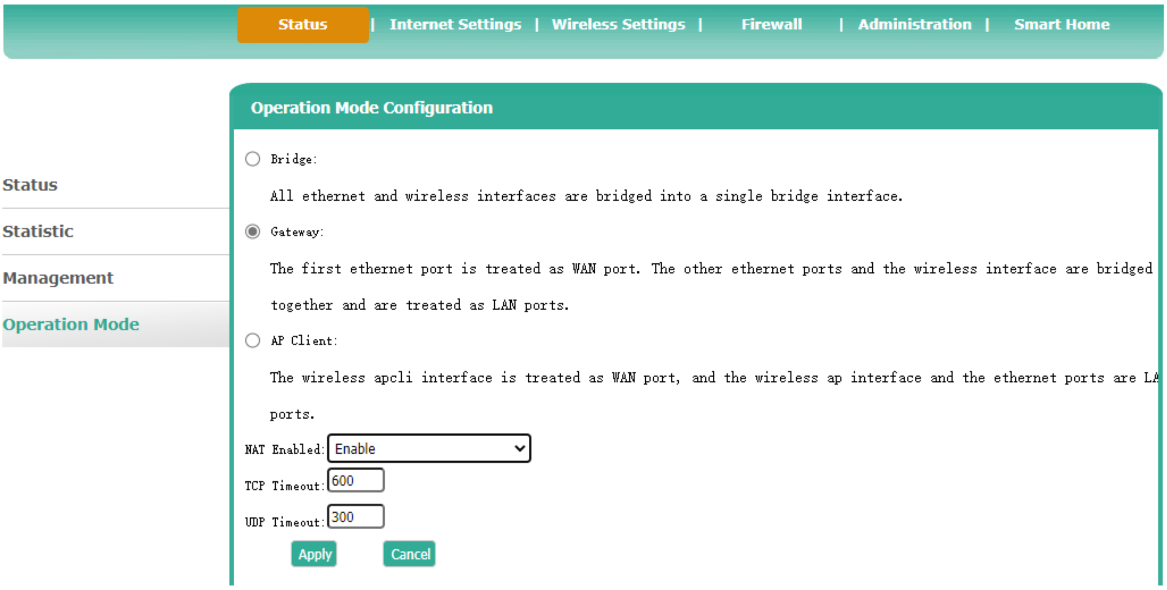
All ethernet and wireless interfaces are bridged into a single bridge interface.

B. Gateway mode

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

C. AP Client

The wireless AP Client interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LAN ports.



Operation Mode Configuration

○ Bridge:

All ethernet and wireless interfaces are bridged into a single bridge interface.

● Gateway:

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

○ AP Client:

The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports are LA ports.

NAT Enabled: Enable

TCP Timeout: 600

UDP Timeout: 300

Apply Cancel

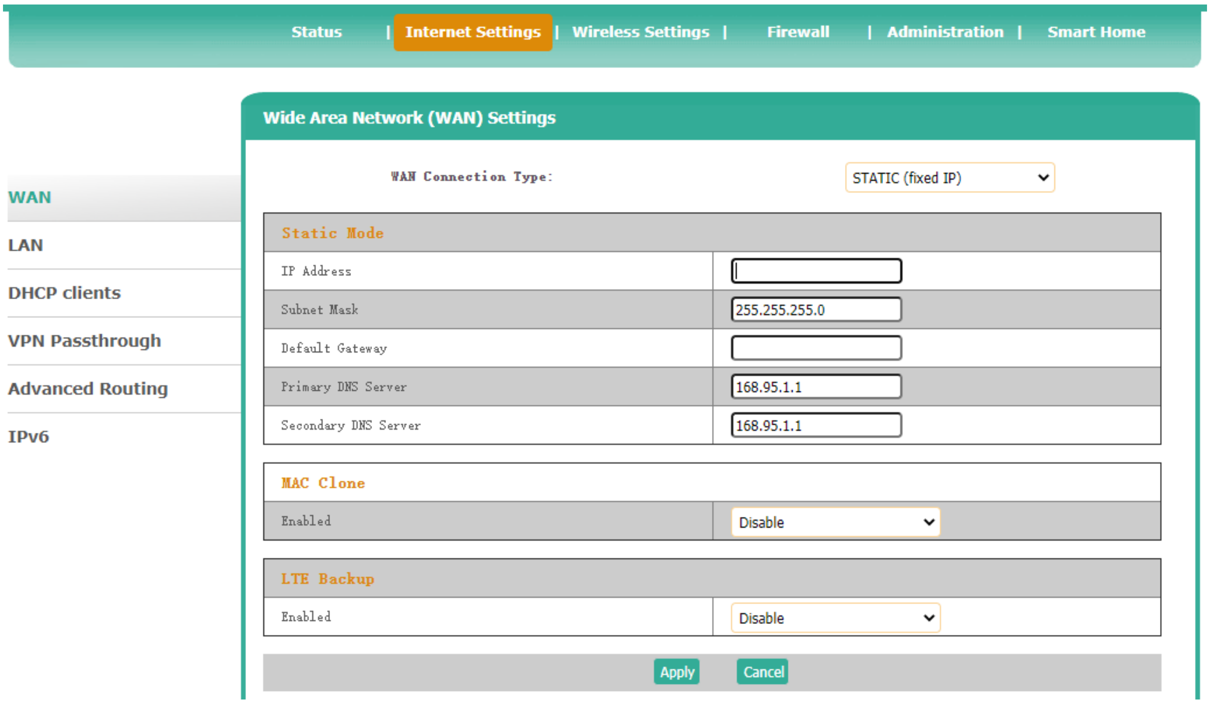
5.4 Internet Setting

5.4.1 WAN

Please select the connection type of WAN according to the environment.

A. Static IP

It needs to enter IP Address, Subnet Mask, Default Gateway, and DNS Server.



Wide Area Network (WAN) Settings

WAN Connection Type: STATIC (fixed IP)

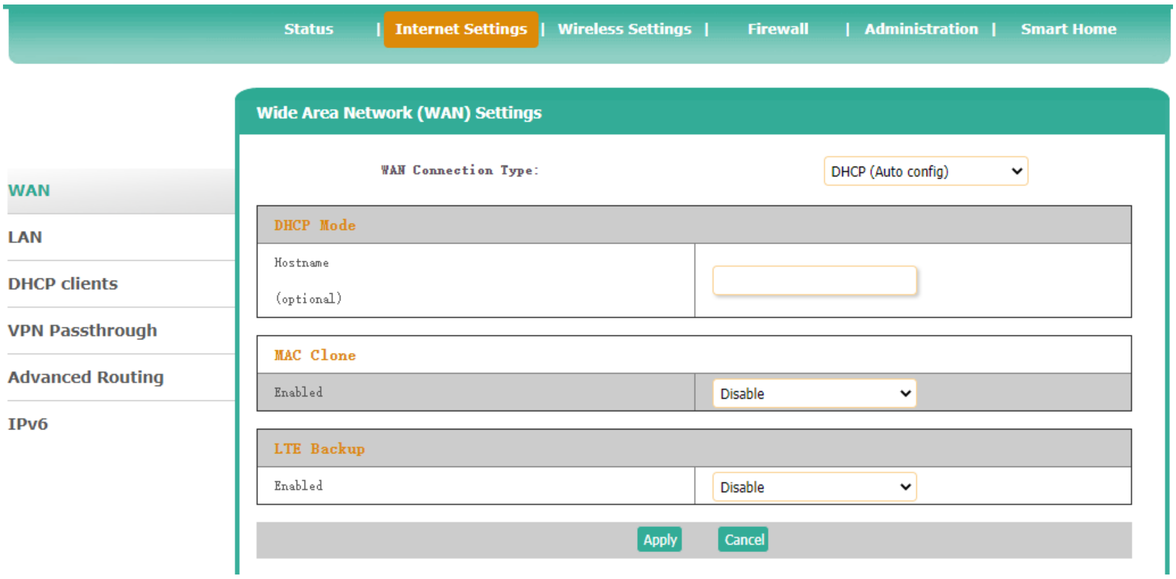
Static Mode	
IP Address	
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.1.1

MAC Clone	
Enabled	Disable

LTE Backup	
Enabled	Disable

B. DHCP

The network will automatically obtain an IP



Wide Area Network (WAN) Settings

WAN Connection Type: DHCP (Auto config)

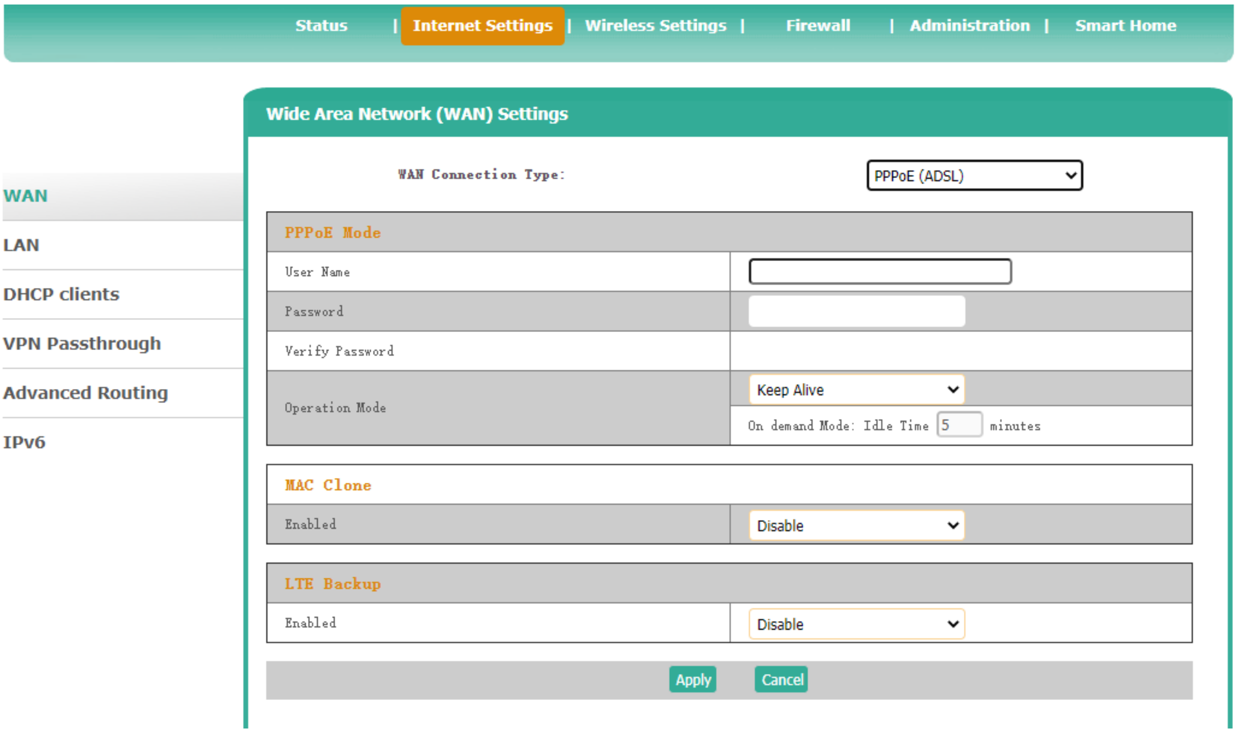
DHCP Mode	
Hostname (optional)	

MAC Clone	
Enabled	Disable

LTE Backup	
Enabled	Disable

C. PPPoE

It need to enter User Name and Password provided by the ISP



WAN Connection Type: PPPoE (ADSL)

User Name	
Password	
Verify Password	
Operation Mode	Keep Alive On demand Mode: Idle Time 5 minutes

MAC Clone — Enabled: Disable

LTE Backup — Enabled: Disable

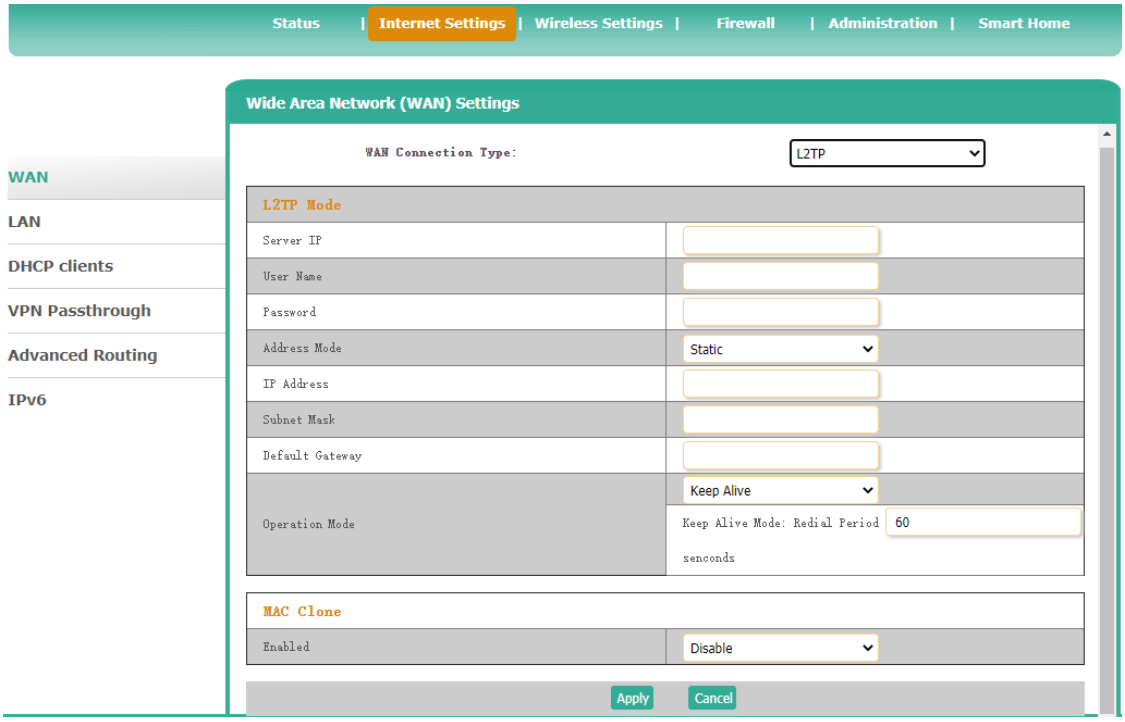
If the setting is the above three network modes-- static IP, dynamic IP, and PPPoE, and enables LTE support, it can automatically switch to 4G dongle to continue connecting to the network when the original mode cannot connect to the network . At present, it will check whether the 4G dongle is plugged in and the switch function is turned on every five minutes. If both are done, it will check the current network for about 10 minutes. During the process, if it connects to the network via the current mode successfully, the switch will be stopped. if it fails to connect to the network, the mode will be switched.

After switching, the gateway will not automatically switch to the original network mode, and the user needs to set the mode by self.

D. L2TP

When the IP Address Mode is Static, the user needs to manually enter the IP Address information.

When the IP Address Mode is Dynamic, the IP Address information can be obtained automatically.



Wide Area Network (WAN) Settings

WAN Connection Type: L2TP

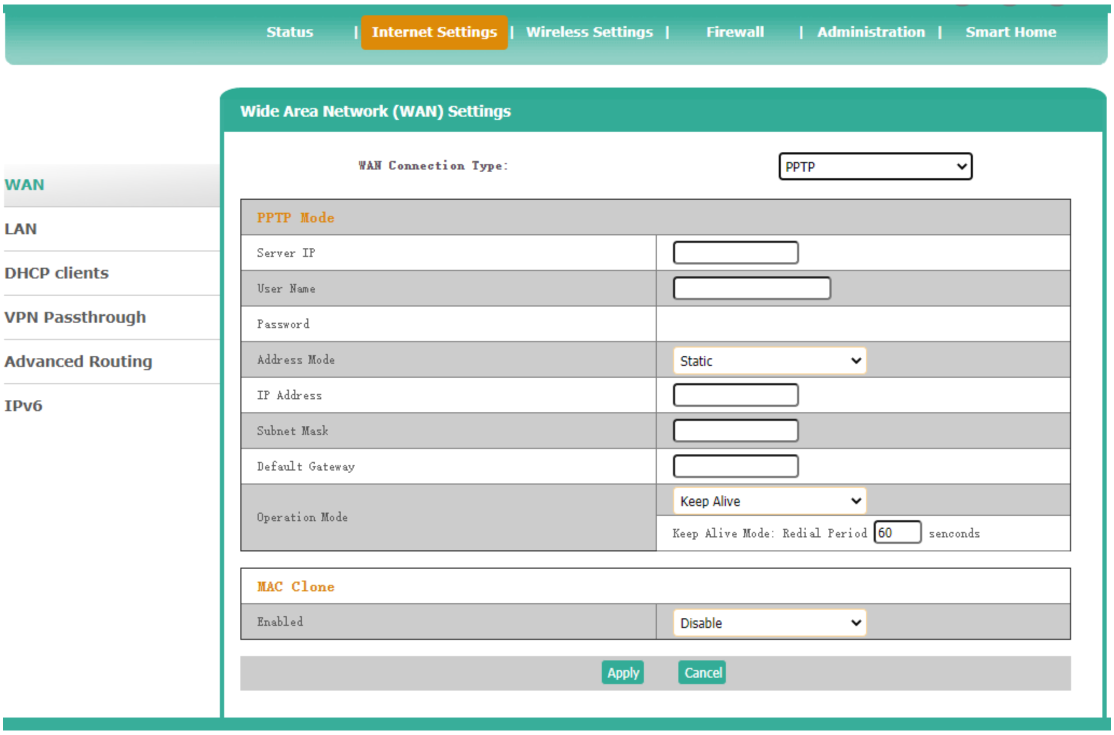
L2TP Mode	
Server IP	
User Name	
Password	
Address Mode	Static
IP Address	
Subnet Mask	
Default Gateway	
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds

MAC Clone	
Enabled	Disable

E. PPTP

When the IP Address Mode is Static, the user needs to manually enter the IP Address information.

When the IP Address Mode is Dynamic, the IP Address information can be obtained automatically.



Wide Area Network (WAN) Settings

WAN Connection Type: PPTP

PPTP Mode	
Server IP	
User Name	
Password	
Address Mode	Static
IP Address	
Subnet Mask	
Default Gateway	
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds

MAC Clone	
Enabled	Disable

F. 3G

It need to match a supported 3G USB Dongle and plug in the USB port of the gateway.

Default APN: internet

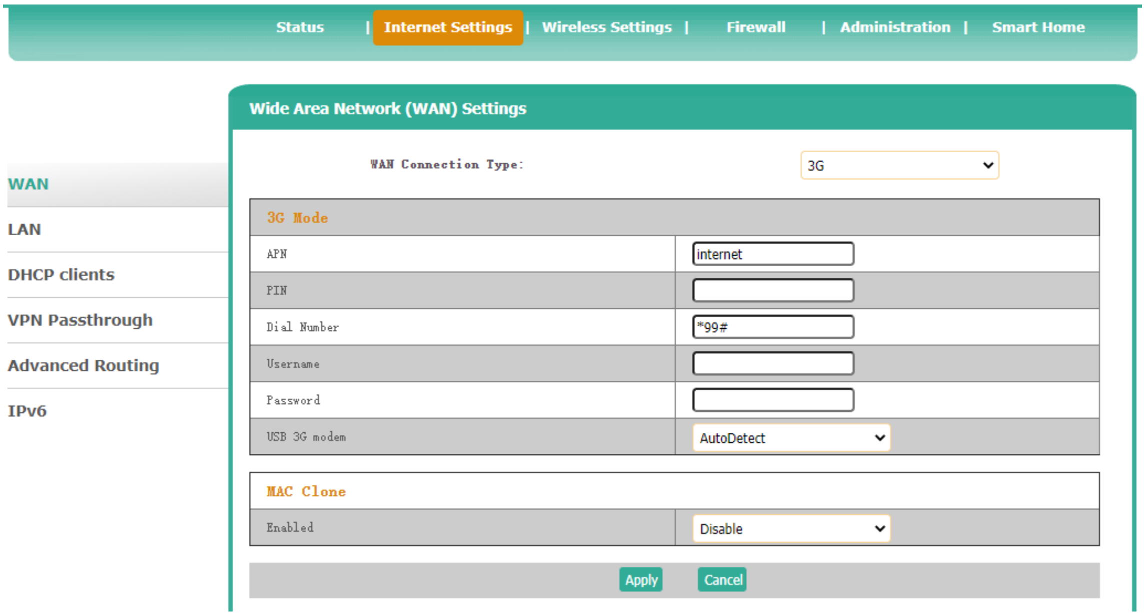
Default Dial Number:*99# (The rest of the setting items can be defaulted.)

Supported 3G USB Dongle: HUAWEI 169/E169u/E1750(StarHub)/E270/E166/EC1260/EC226/ EC122/EC189/E181/170/E172/E180/E219/E220/E230/E180/E1552/ E160E/Emobile D01HW/Emobile D02HW/E122(2010), Vodafone K4605/K3770/K3772, etc.

Note:

*Please fill in the APN and other information according to the information provided by the telecom.

*3G network card must be genuine. The parallel import and pirated version will be different and will not be used.



Wide Area Network (WAN) Settings

WAN Connection Type: 3G

3G Mode	
APN	internet
PIN	
Dial Number	*99#
Username	
Password	
USB 3G modem	AutoDetect

MAC Clone	
Enabled	Disable

G. LTE

It needs to match a supported LTE (4G) USB Dongle and plug in the USB port of the gateway.

Default APN: internet

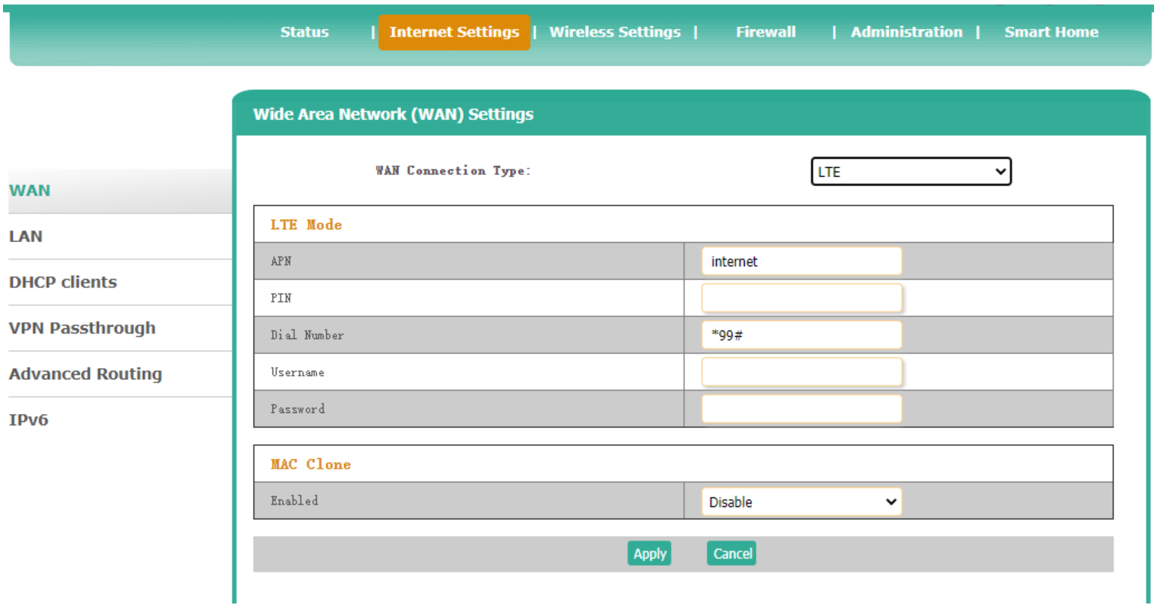
Default Dial Number:*99# (The rest of the setting items can be defaulted.)

Supported 4G USB Dongle: Huawei EC3372h-607, Huawei E3372h-607, Huawei EC3372-871,
Huawei E3372h-607, Alcatel Link Key 4G LTE IK 40

Note:

*Please fill in the APN and other information according to the information provided by the telecom.

*4G network card must be genuine. The parallel import and pirated version will be different and will not be used.



Wide Area Network (WAN) Settings

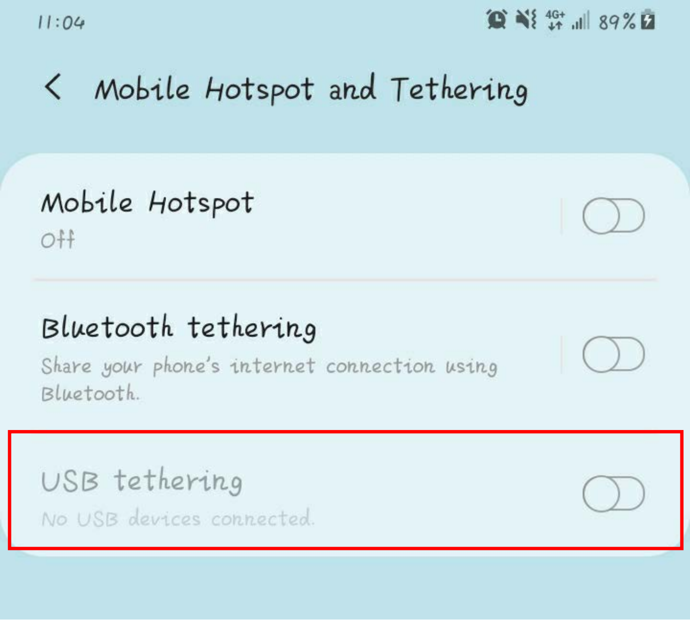
WAN Connection Type: LTE

LTE Mode	
APN	internet
PIN	
Dial Number	*99#
Username	
Password	

MAC Clone	
Enabled	Disable

In addition to using the 3G/4G USB Dongle to surf the Internet, the user can also connect to the USB port of the gateway through an Android phone to surf the Internet.

After plugging it in, the user must first turn on "USB Tethering" on the phone. When the phone is used as an LTE dongle, it can also provide the gateway with the Internet.



Mobile Hotspot
Off

Bluetooth tethering
Share your phone's internet connection using Bluetooth.

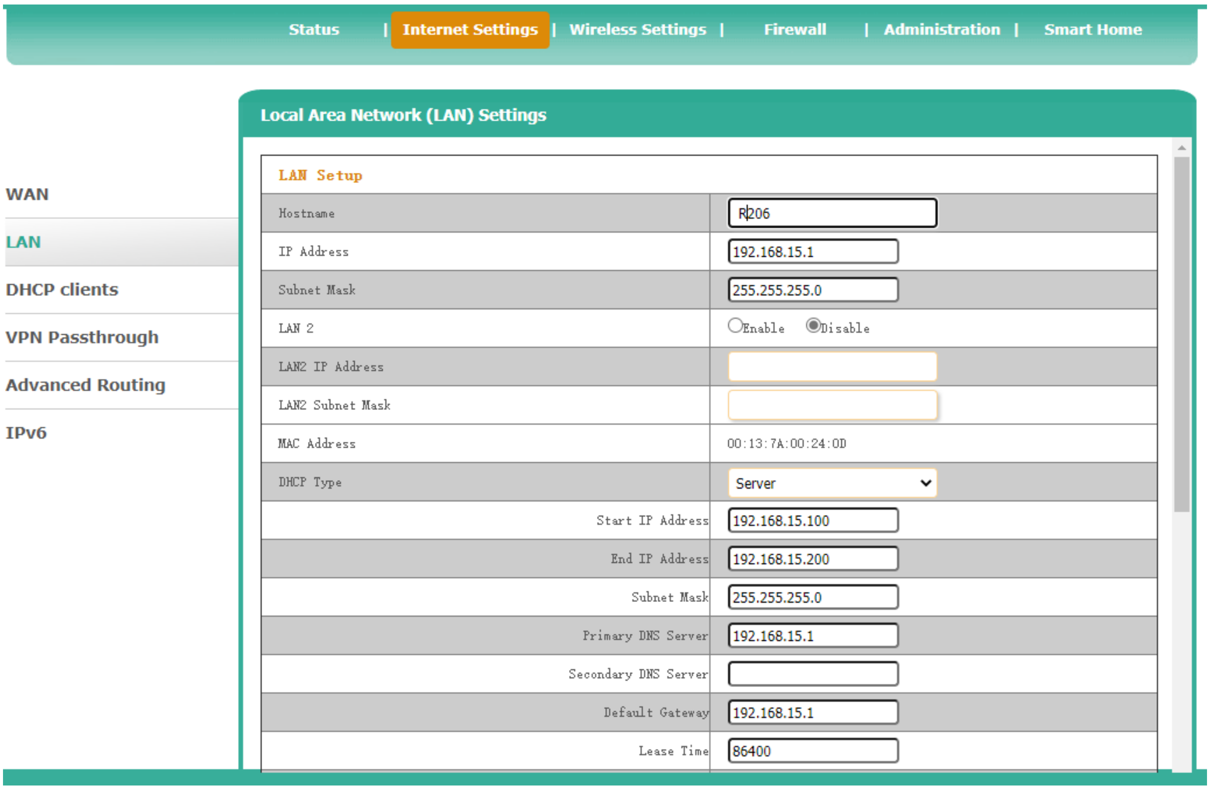
USB tethering
No USB devices connected.

Note:

*Some Android phones may not support.

5.4.2 LAN

The information of LAN can be set, such as changing IP and IP range, enabling/disabling UPNP, etc.



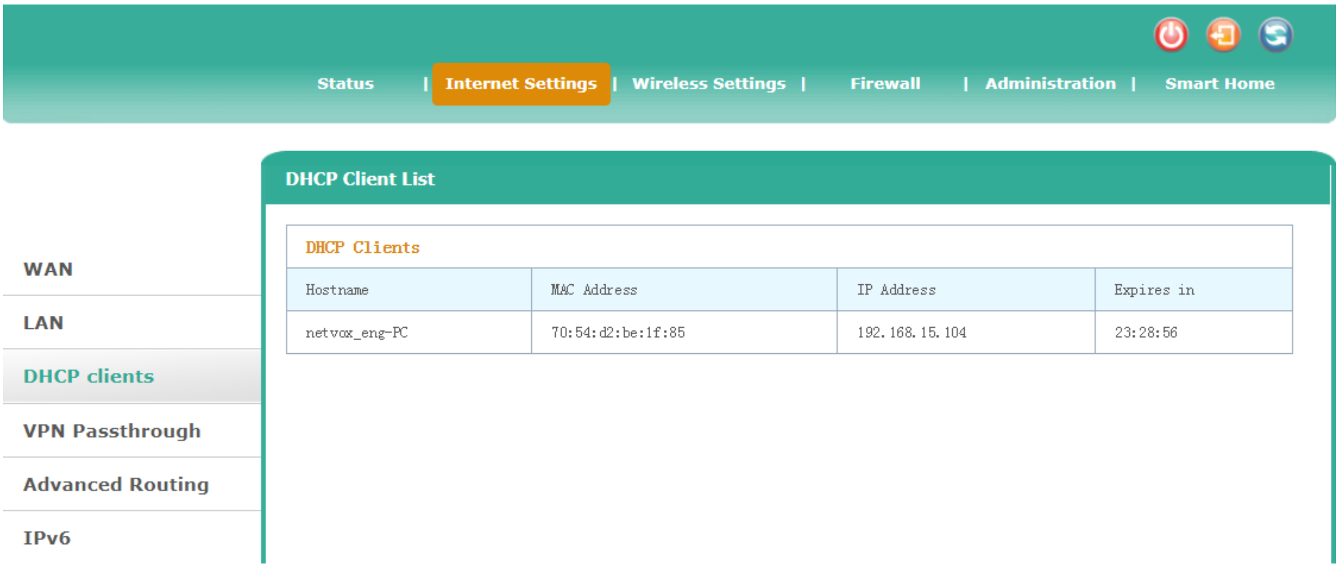
Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
WAN
LAN
DHCP clients
VPN Passthrough
Advanced Routing
IPv6

Local Area Network (LAN) Settings

LAN Setup	
Hostname	R206
IP Address	192.168.15.1
Subnet Mask	255.255.255.0
LAN 2	○Enable ●Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:13:7A:00:24:0D
DHCP Type	Server
Start IP Address	192.168.15.100
End IP Address	192.168.15.200
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.15.1
Secondary DNS Server	
Default Gateway	192.168.15.1
Lease Time	86400

5.4.3 DHCP Clients

Check the information of the devices connected with the gateway. Users can get the assigned IP address based on the network name or MAC address.



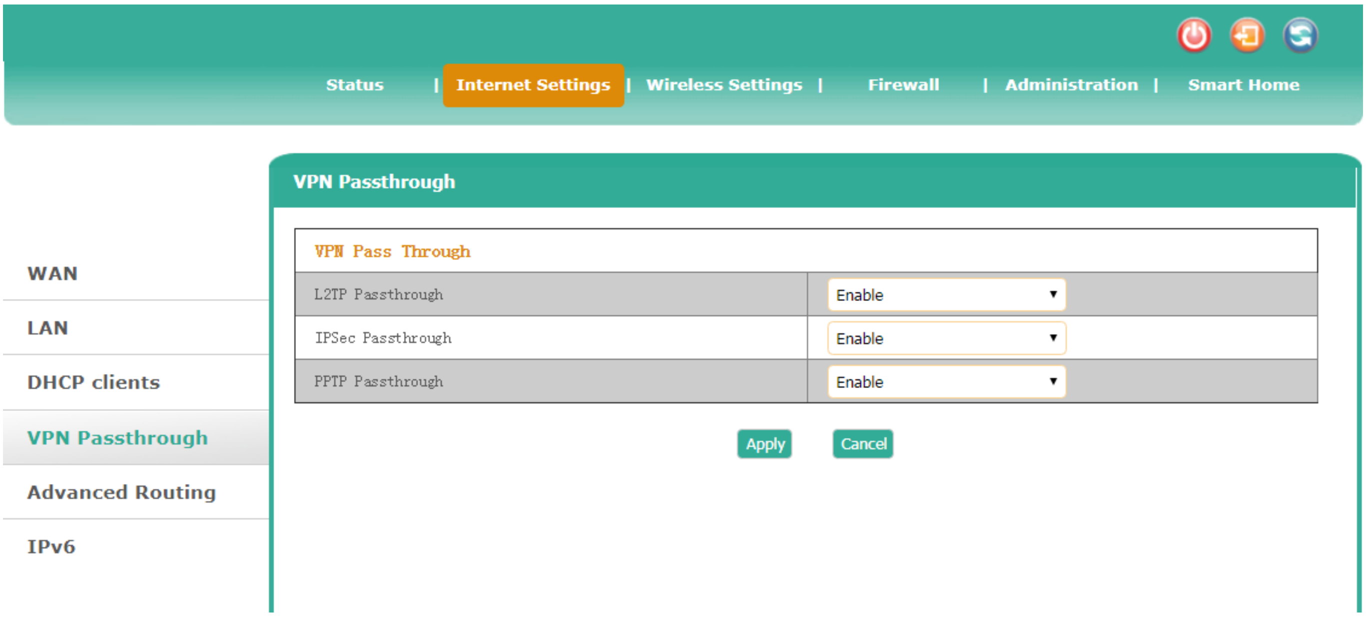
DHCP Client List

DHCP Clients

Hostname	MAC Address	IP Address	Expires in
netvox_eng-PC	70:54:d2:be:1f:85	192.168.15.104	23:28:56

5.4.4 VPN Passthrough

Users can enable/disable the VPN passthrough here, including: L2TP, IPSec, and PPTP passthrough.



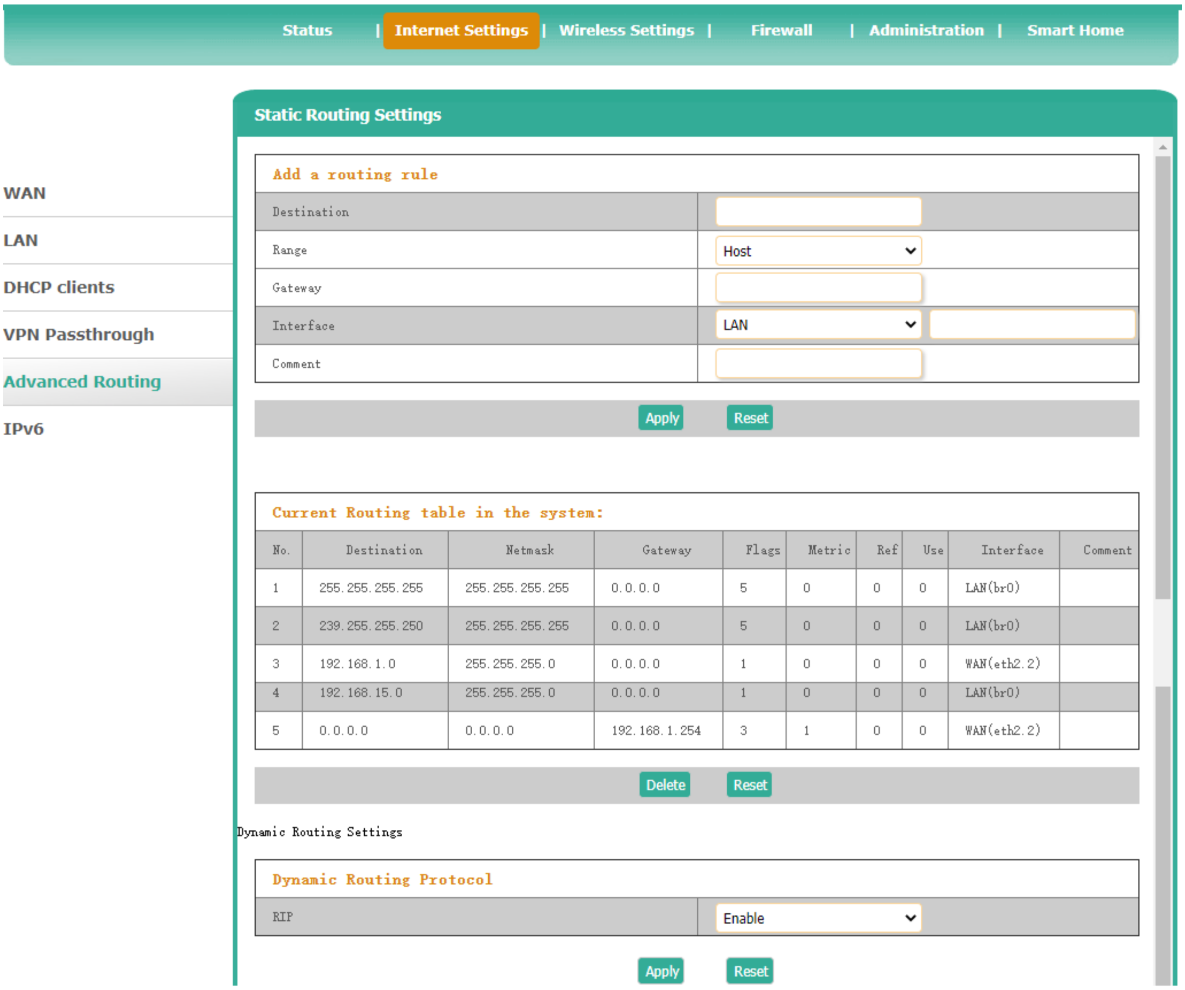
VPN Passthrough

VPN Pass Through

L2TP Passthrough	Enable
IPSec Passthrough	Enable
PPTP Passthrough	Enable

5.4.5 Advanced Routing

Users can add/remove static routing rules or enable/disable dynamic routing rules.



Static Routing Settings

Add a routing rule

Destination	
Range	Host
Gateway	
Interface	LAN
Comment	

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
3	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN(eth2.2)	
4	192.168.15.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
5	0.0.0.0	0.0.0.0	192.168.1.254	3	1	0	0	WAN(eth2.2)	

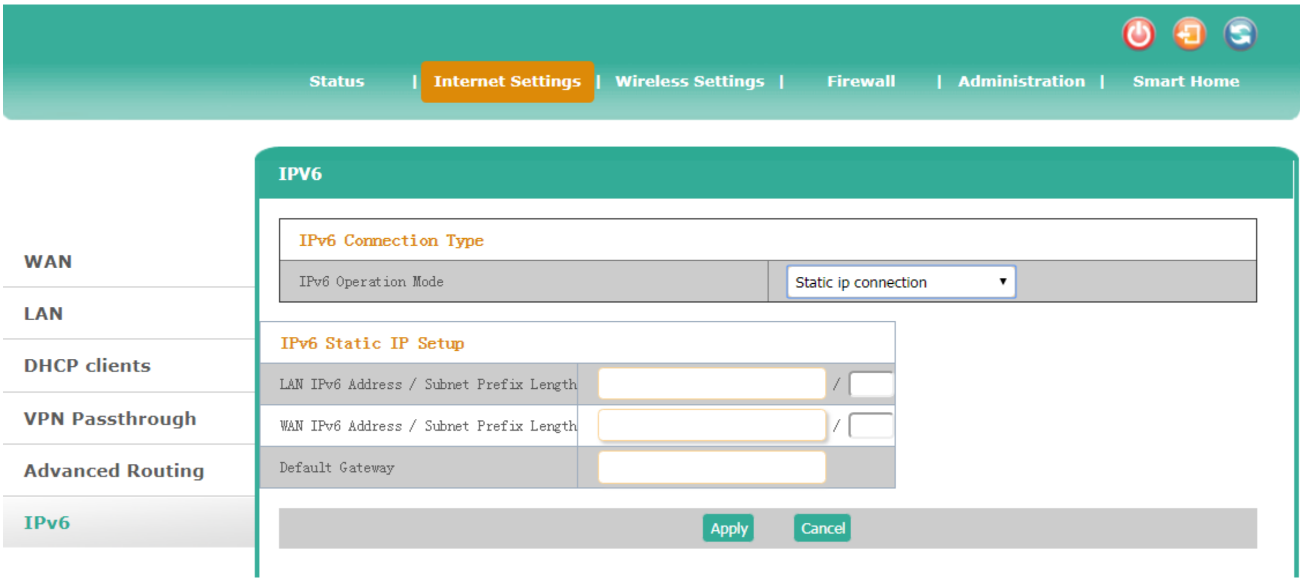
Dynamic Routing Settings

Dynamic Routing Protocol

RIP	Enable

5.4.6 IPv6

Enable IPv6 setting



IPV6

IPv6 Connection Type

IPv6 Operation Mode	Static ip connection

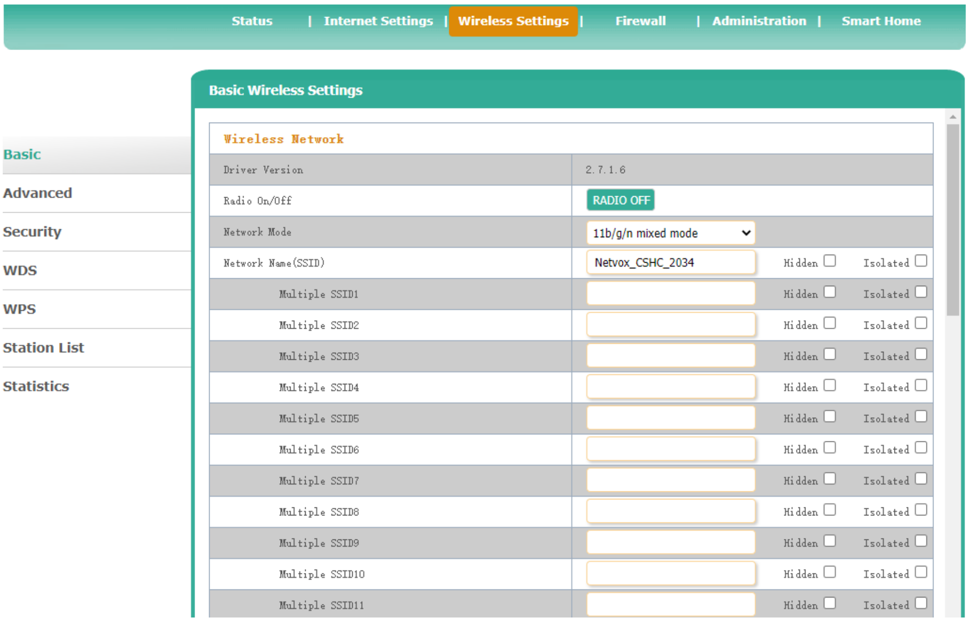
IPv6 Static IP Setup

LAN IPv6 Address / Subnet Prefix Length	/
WAN IPv6 Address / Subnet Prefix Length	/
Default Gateway	

5.5 Wireless Setting

5.5.1 Basic

Basic wireless network setting, such as changing wireless SSID, adding wireless SSID, and enabling/disabling Wi-Fi signal (Radio On/Off).



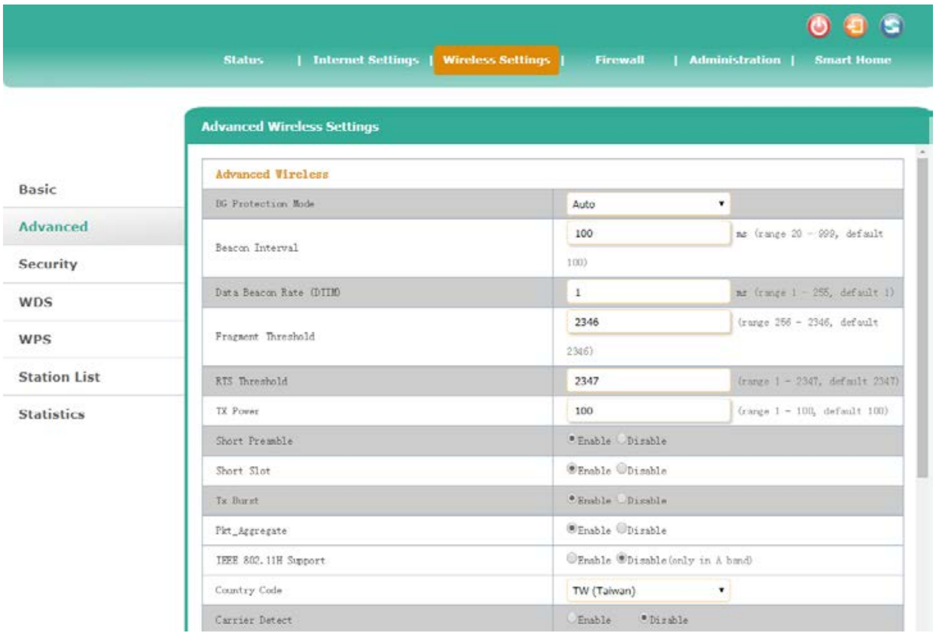
Wireless Network			
Driver Version	2.7.1.6		
Radio On/Off	RADIO OFF		
Network Mode	11b/g/n mixed mode		
Network Name(SSID)	Netvox_CSHC_2034	Hidden □	Isolated □
Multiple SSID1		Hidden □	Isolated □
Multiple SSID2		Hidden □	Isolated □
Multiple SSID3		Hidden □	Isolated □
Multiple SSID4		Hidden □	Isolated □
Multiple SSID5		Hidden □	Isolated □
Multiple SSID6		Hidden □	Isolated □
Multiple SSID7		Hidden □	Isolated □
Multiple SSID8		Hidden □	Isolated □
Multiple SSID9		Hidden □	Isolated □
Multiple SSID10		Hidden □	Isolated □
Multiple SSID11		Hidden □	Isolated □

Note:

*The Wi-Fi function of the gateway is turned off. The user needs to use the wired connection to enter the setting page of the gateway and reopen it before connecting to Wi-Fi.

5.5.2 Advanced

Users can set Beacon Interval, control transmission rate and basic data transmission rate, etc.



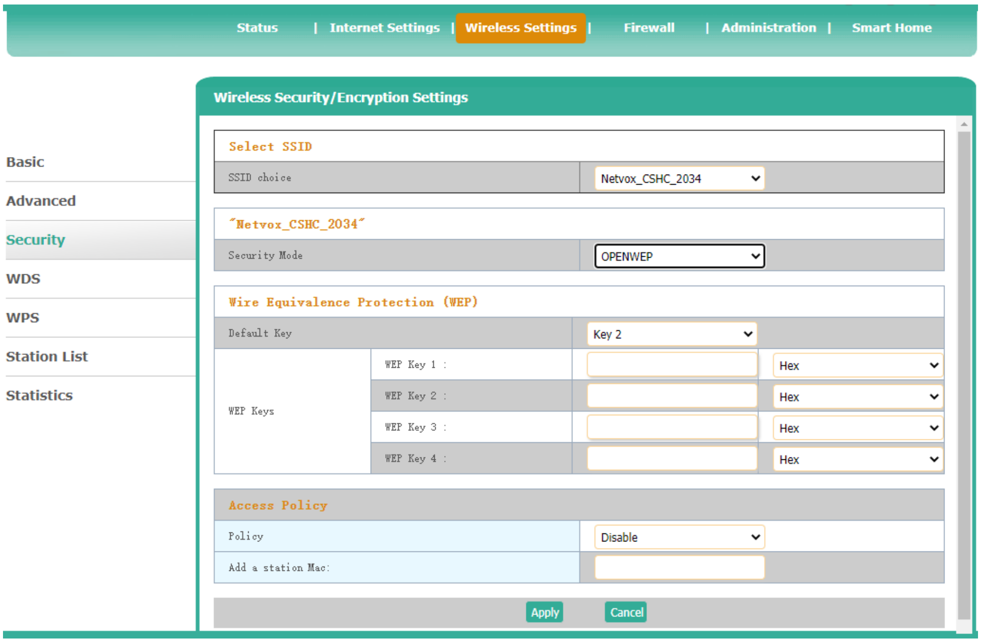
Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable (only in A band)
Country Code	TW (Taiwan)
Carrier Detect	○ Enable ● Disable

5.5.3 Security

Set the wireless SSID encryption method

A. Security Mode: OPENWEP

Network Mode does not support 11n


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Basic
Advanced
Security
WDS
WPS
Station List
Statistics
Apply
Cancel

Wireless Security/Encryption Settings

Select SSID

SSID choice: Netvox_CSHC_2034

"Netvox_CSHC_2034"

Security Mode: OPENWEP

Wire Equivalence Protection (WEP)

Default Key: Key 2

WEP Keys

WEP Key 1 : Hex

WEP Key 2 : Hex

WEP Key 3 : Hex

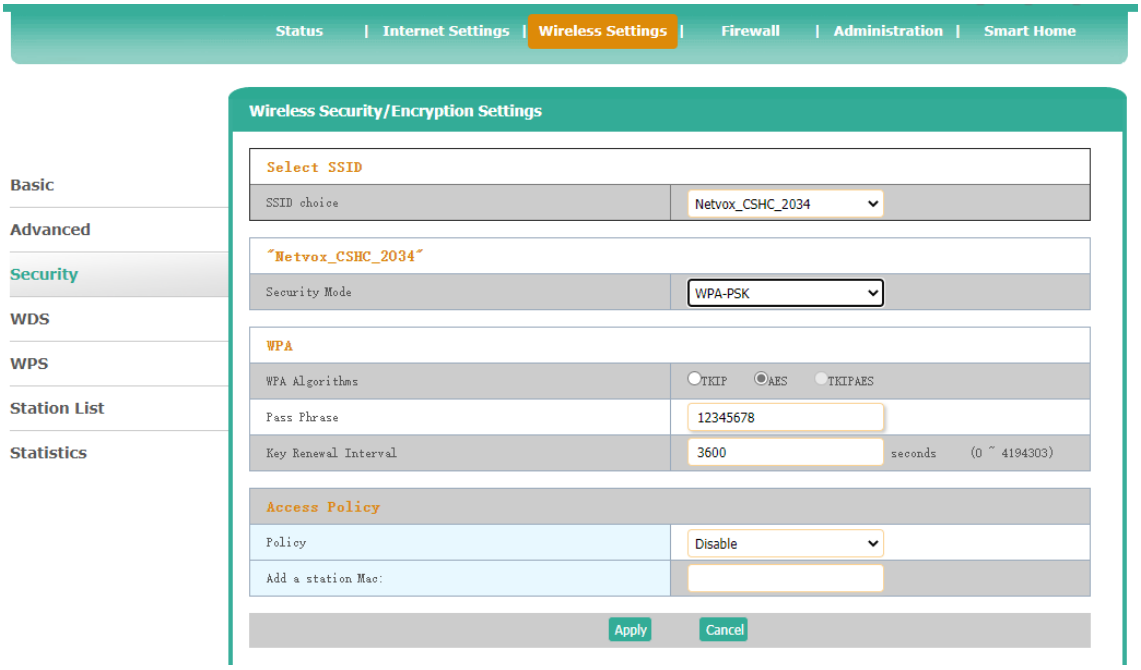
WEP Key 4 : Hex

Access Policy

Policy: Disable

Add a station Mac:

B. Security Mode: WPA-PSK


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Basic
Advanced
Security
WDS
WPS
Station List
Statistics
Apply
Cancel

Wireless Security/Encryption Settings

Select SSID

SSID choice: Netvox_CSHC_2034

"Netvox_CSHC_2034"

Security Mode: WPA-PSK

WPA

WPA Algorithms: ○TKIP ●AES ○TKIPAES

Pass Phrase: 12345678

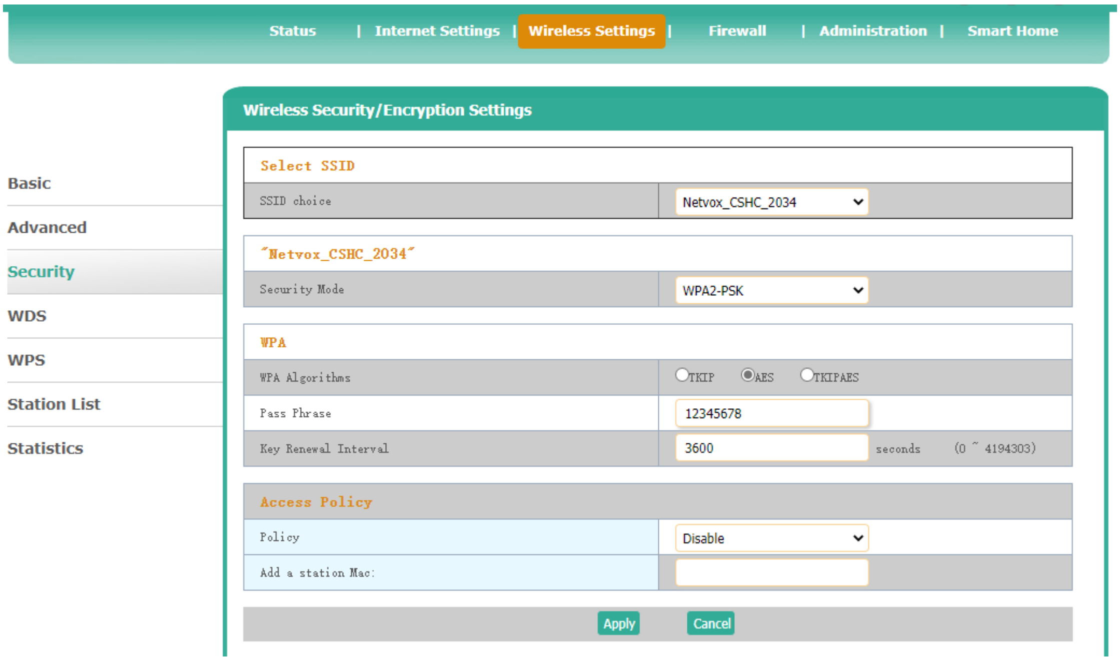
Key Renewal Interval: 3600 seconds (0 ~ 4194303)

Access Policy

Policy: Disable

Add a station Mac:

C. Security Mode: WPA2-PSK (Recommend)



Wireless Security/Encryption Settings

Select SSID

SSID choice	Netvox_CSHC_2034

"Netvox_CSHC_2034"

Security Mode	WPA2-PSK

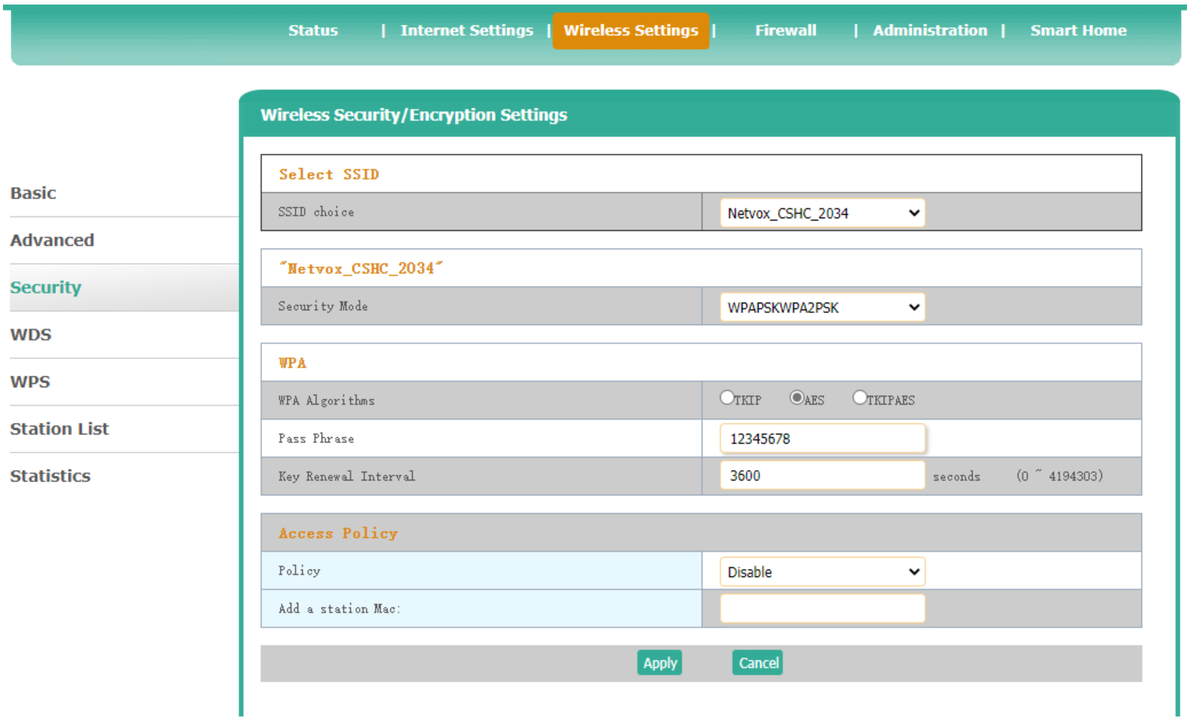
WPA

WPA Algorithms	○TKIP ●AES ○TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)

Access Policy

Policy	Disable
Add a station Mac:	

D. Security Mode: WPAPSKWPA2PSK



Wireless Security/Encryption Settings

Select SSID

SSID choice	Netvox_CSHC_2034

"Netvox_CSHC_2034"

Security Mode	WPAPSKWPA2PSK

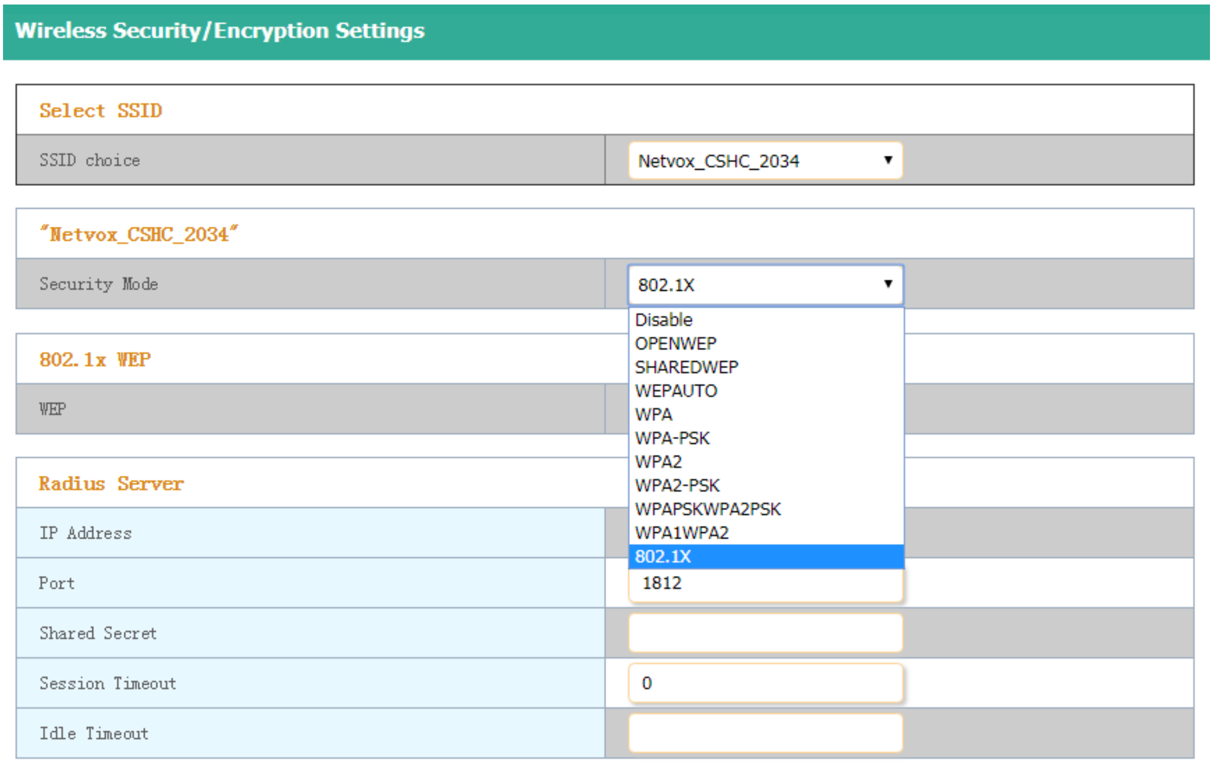
WPA

WPA Algorithms	○TKIP ●AES ○TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)

Access Policy

Policy	Disable
Add a station Mac:	

If WPS is disabled, the security mode will add the option about Radius Server: WPA, WPA2, WPA1, WPA2, and 802.1X



Wireless Security/Encryption Settings

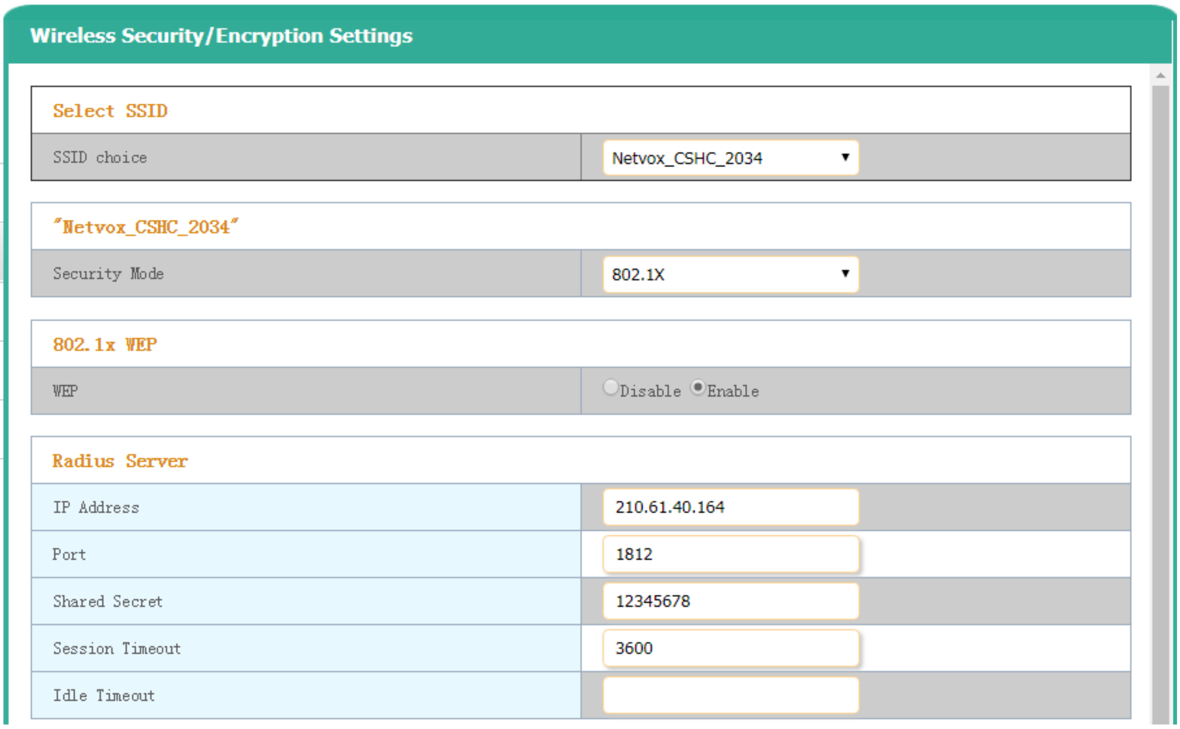
Select SSID	
SSID choice	Netvox_CSHC_2034 ▾

"Netvox_CSHC_2034"	
Security Mode	802.1X ▾

802.1x WEP	
WEP	

Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The method of setting Radius Server is as follows



Wireless Security/Encryption Settings

Select SSID	
SSID choice	Netvox_CSHC_2034 ▾

"Netvox_CSHC_2034"	
Security Mode	802.1X ▾

802.1x WEP	
WEP	○Disable ●Enable

Radius Server	
IP Address	210.61.40.164
Port	1812
Shared Secret	12345678
Session Timeout	3600
Idle Timeout	

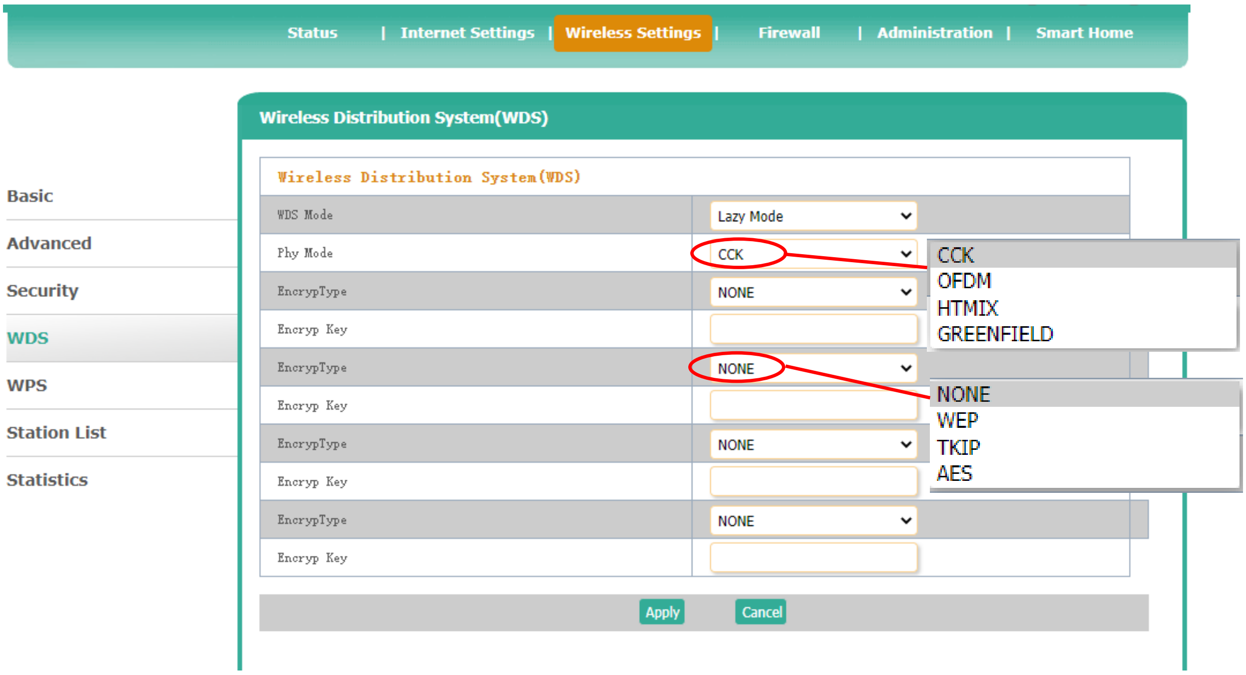
5.5.4 WDS

Enable/Disable WDS

A. Lazy Mode

Physical Mode support: CCK、OFDM、HTMIX、GREENFIELD

Encryption Key support: WEP、TKIP、AES



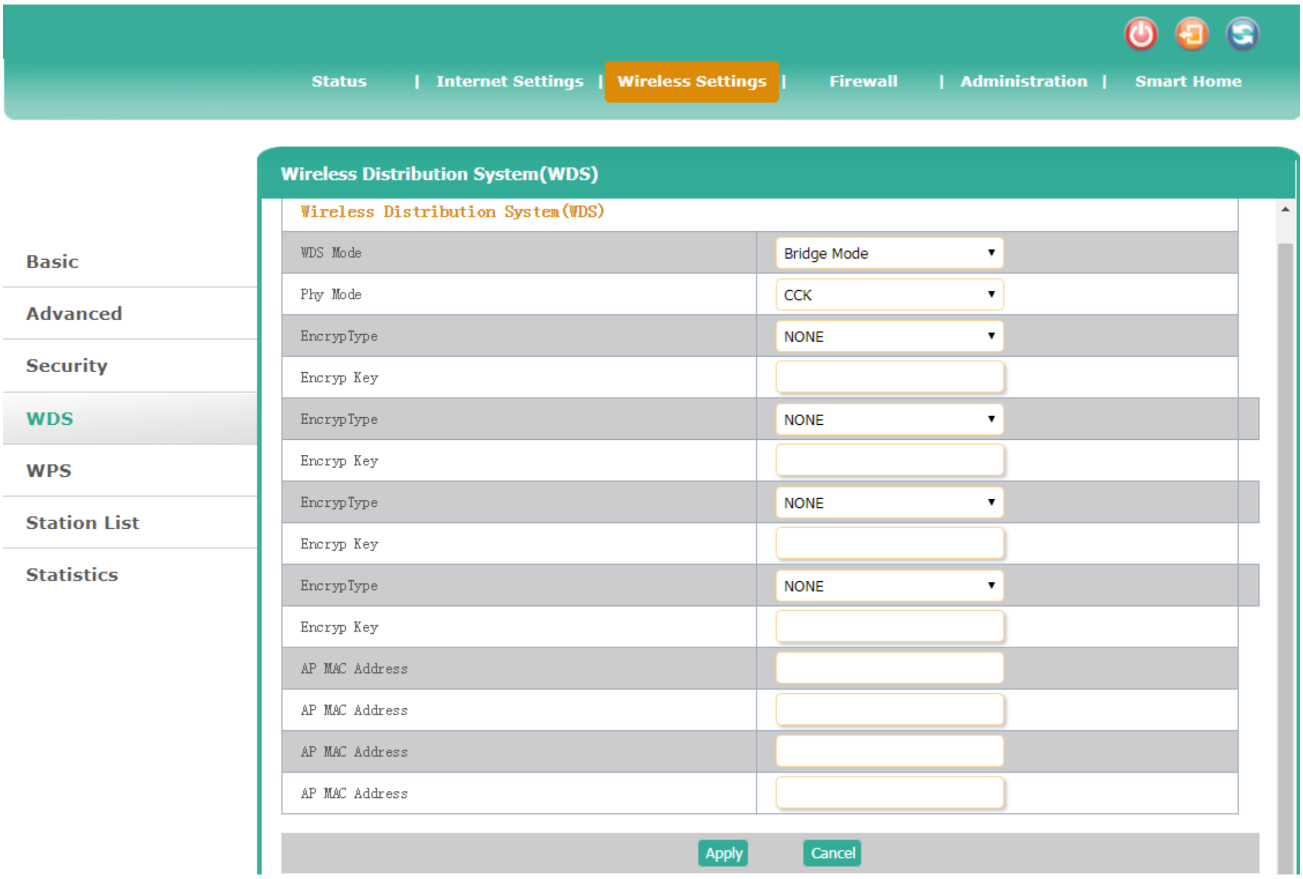
Wireless Distribution System(WDS)

Wireless Distribution System(WDS)

WDS Mode	Lazy Mode
Phy Mode	CCK
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	

B. Bridge Mode

Users need to manually enter AP MAC Address.



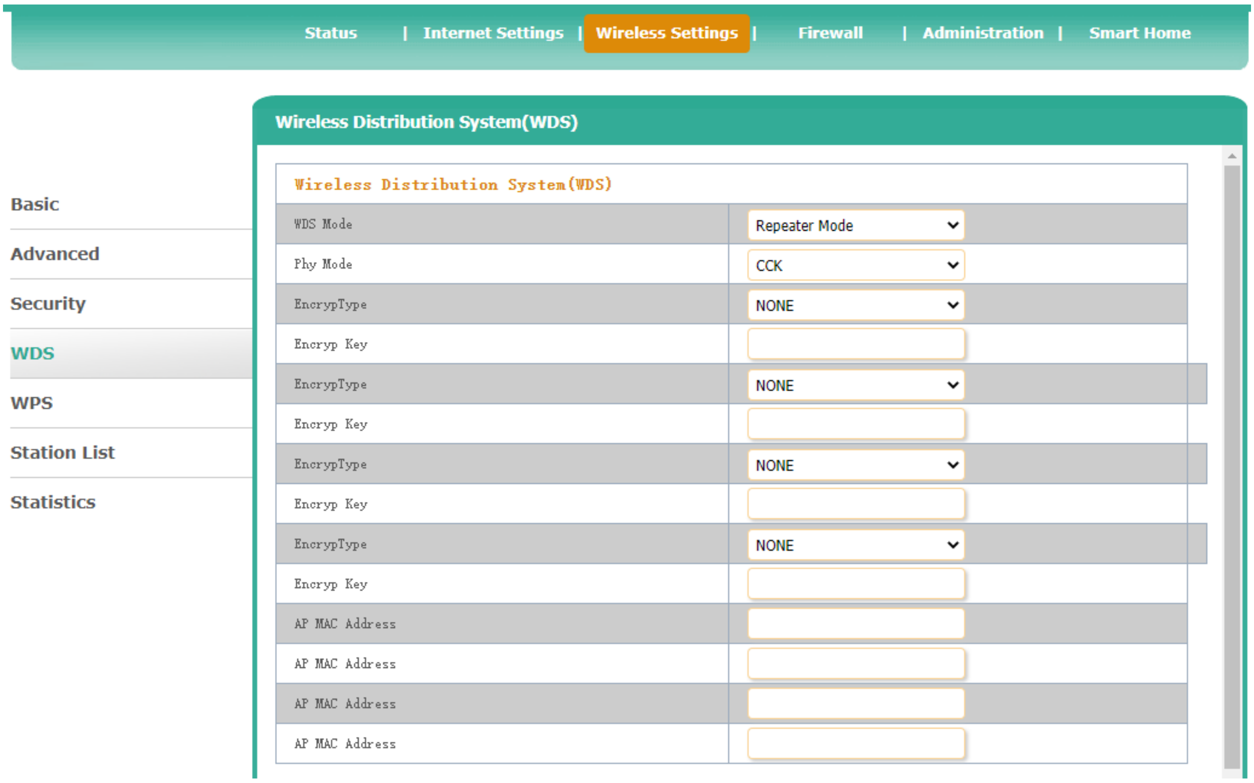
Wireless Distribution System(WDS)

Wireless Distribution System(WDS)

WDS Mode	Bridge Mode
Phy Mode	CCK
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
AP MAC Address	
AP MAC Address	
AP MAC Address	
AP MAC Address	

C. Repeater Mode

Users need to manually enter AP MAC Address.



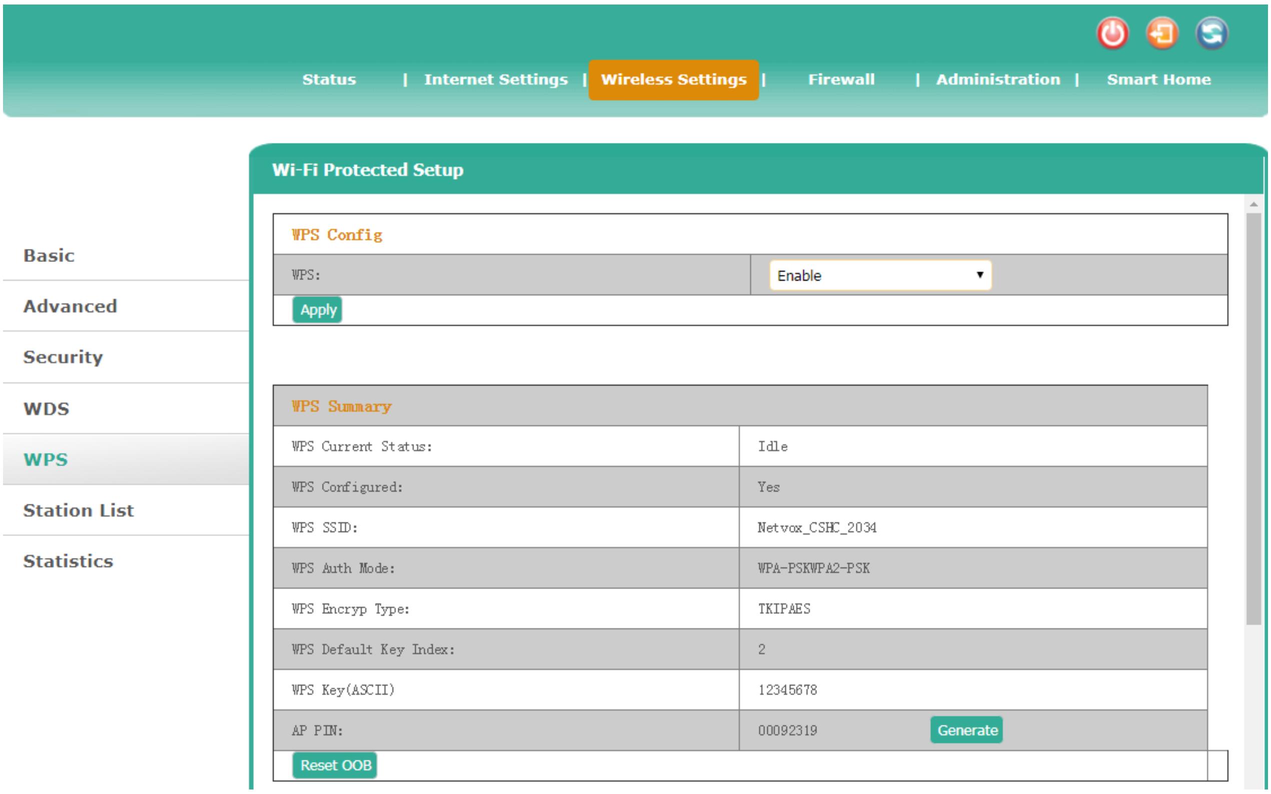
Wireless Distribution System(WDS)

Wireless Distribution System(WDS)

WDS Mode	Repeater Mode
Phy Mode	CCK
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
AP MAC Address	
AP MAC Address	
AP MAC Address	
AP MAC Address	

5.5.5 WPS

Users could setup security easily by choosing PIN method to do Wi-Fi Protected Setup.



Wi-Fi Protected Setup

WPS Config

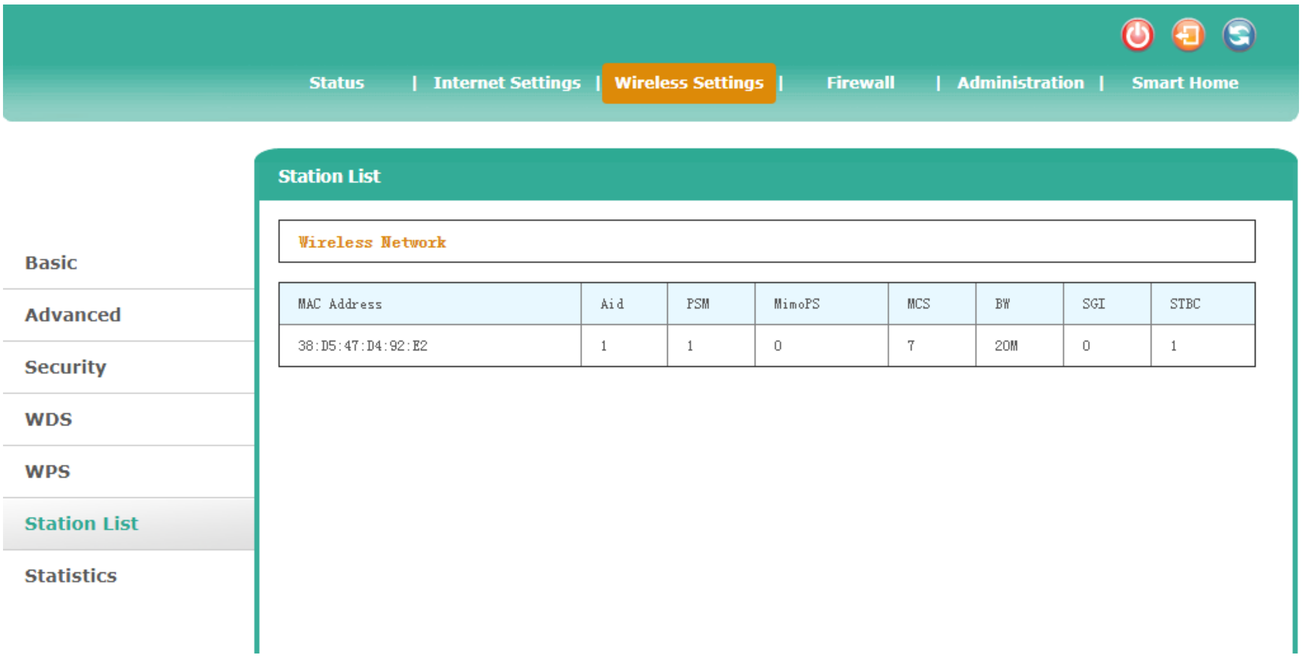
WPS:	Enable

WPS Summary

WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	Netvox_CSHC_2034
WPS Auth Mode:	WPA-PSKWPA2-PSK
WPS Encryp Type:	TKIPAES
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	00092319

5.5.6 Station List

Users could monitor stations which associated to this AP here.



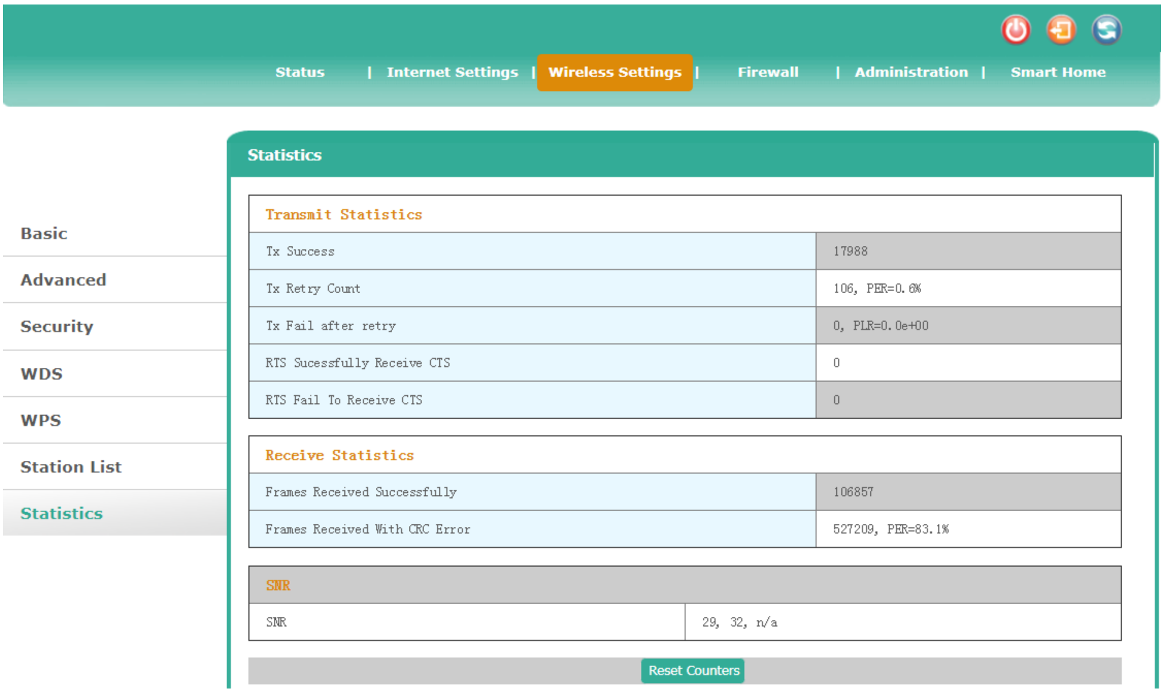
Station List

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
38:D5:47:D4:92:E2	1	1	0	7	20M	0	1

5.5.7 Statistics

Statistics and Information Collection (Transmit Statistics & Receive Statistics)



Statistics

Transmit Statistics	
Tx Success	17988
Tx Retry Count	106, PER=0.6%
Tx Fail after retry	0, PLR=0.0e+00
RTS Sucessfully Receive CTS	0
RTS Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	106857
Frames Received With CRC Error	527209, PER=83.1%

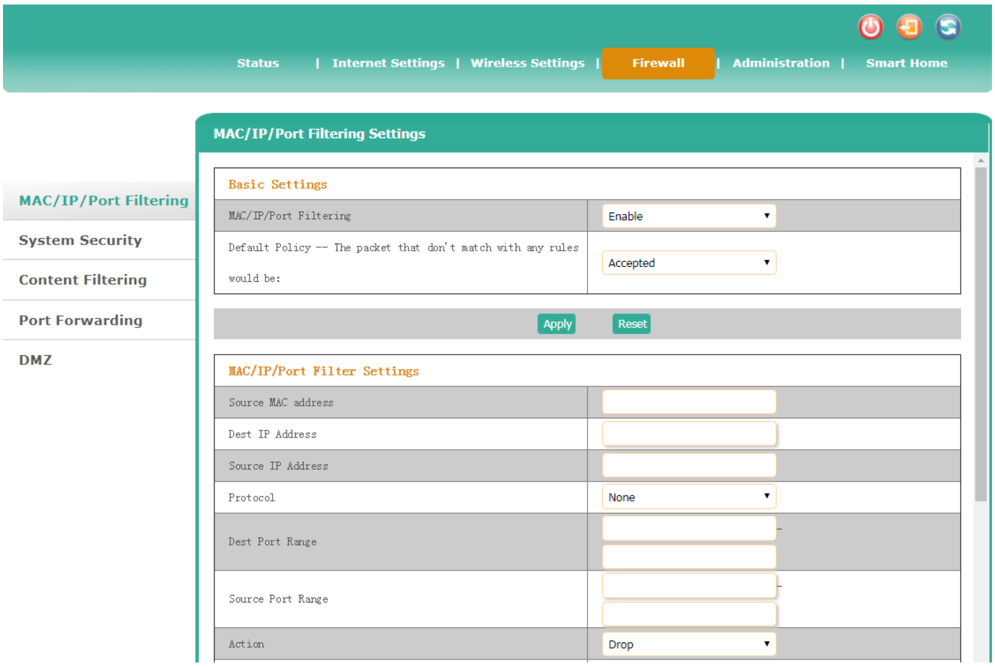
SNR	
SNR	29, 32, n/a

5.6 Firewall

Users can set up a firewall to protect against malicious attacks from the Internet.

5.6.1 MAC/IP/Port Filtering

MAC/IP/Port Filtering is disabled by default. If users need to access the external IP, it need to enable the function of MAC/IP/Port Filtering.



MAC/IP/Port Filtering Settings

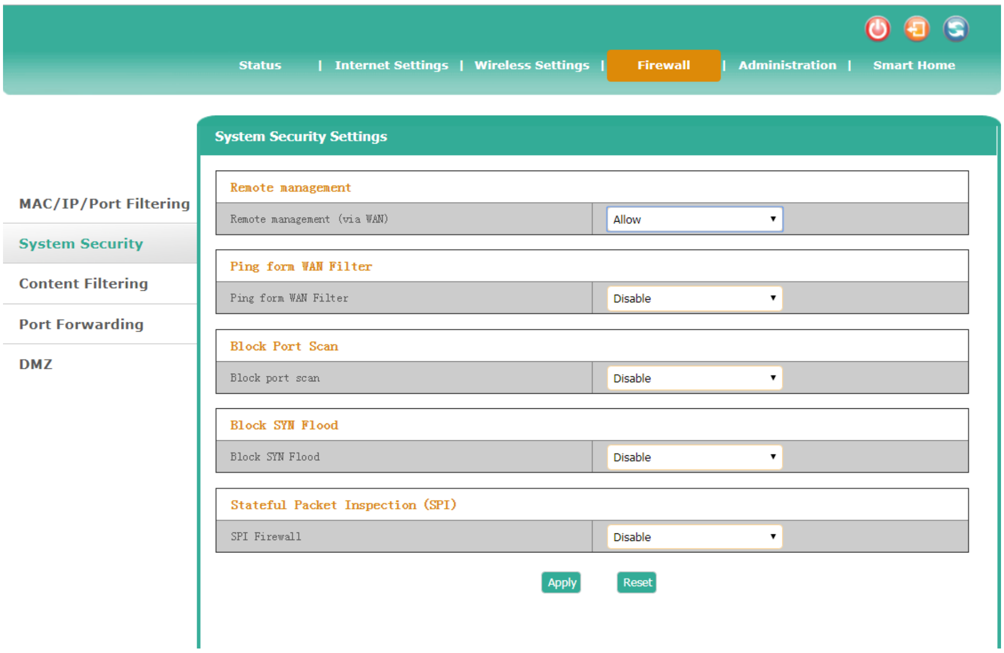
Basic Settings	
MAC/IP/Port Filtering	Enable
Default Policy -- The packet that don't match with any rules would be:	Accepted

MAC/IP/Port Filter Settings	
Source MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Drop

5.6.2 System Security

The router or wireless access point can be protected by setting the system firewall.

If users want to support the login operation of WAN, users need to set Remote management to the "Allow" state to support remote login. Other items are set according to users' different needs.



System Security Settings

Remote management	
Remote management (via WAN)	Allow

Ping form WAN Filter	
Ping form WAN Filter	Disable

Block Port Scan	
Block port scan	Disable

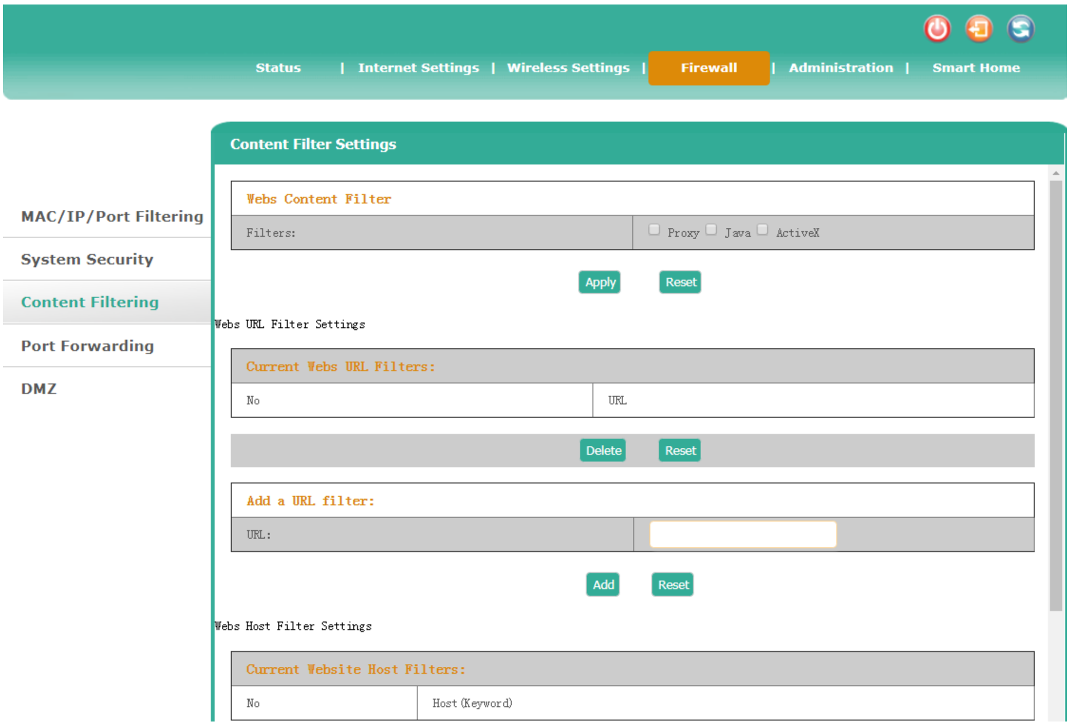
Block SYN Flood	
Block SYN Flood	Disable

Stateful Packet Inspection (SPI)	
SPI Firewall	Disable

5.6.3 Content Filtering

Users can set Content Filter to limit inappropriate web pages.

Enter the URL to be filtered and click Add to add a new rule of URL filtering.



Content Filter Settings

Webs Content Filter	
Filters:	□ Proxy □ Java □ ActiveX

Webs URL Filter Settings

Current Webs URL Filters:	
No	URL

Add a URL filter:	
URL:	

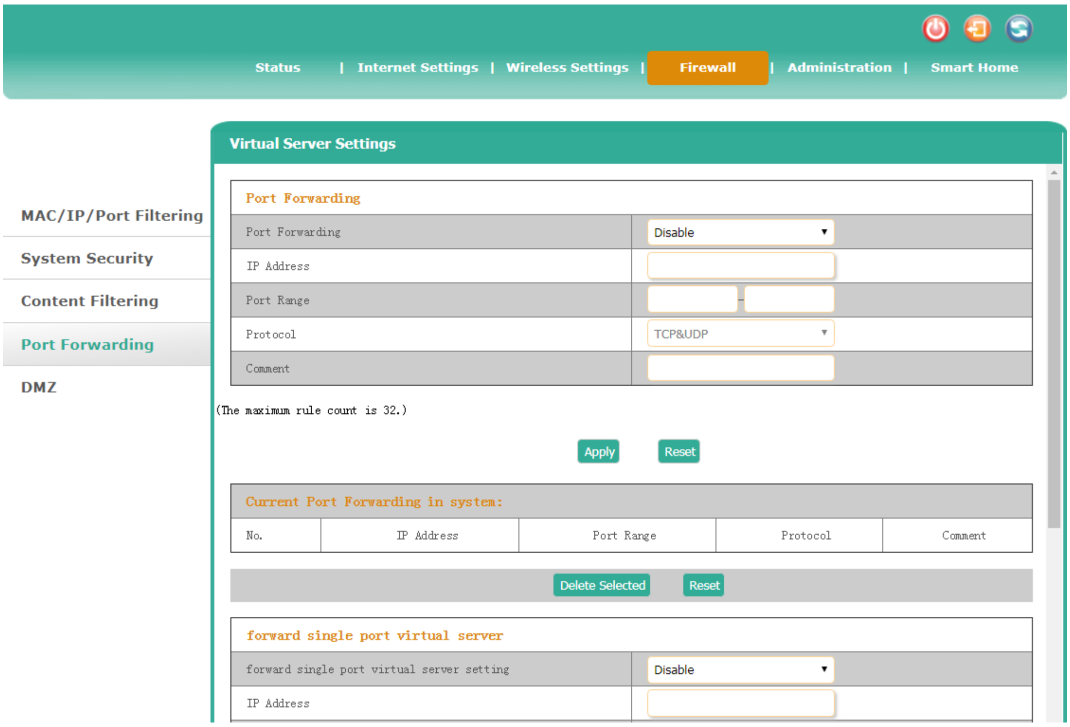
Webs Host Filter Settings

Current Website Host Filters:	
No	Host (Keyword)

5.6.4 Port Forwarding

Choose whether to enable Virtual Server Settings

When users enable the virtual server, users should enter the IP Address, Port Range, and Comment to create a virtual server to provide network services



Virtual Server Settings

Port Forwarding	
Port Forwarding	Disable
IP Address	
Port Range	-
Protocol	TCP&UDP
Comment	

(The maximum rule count is 32.)

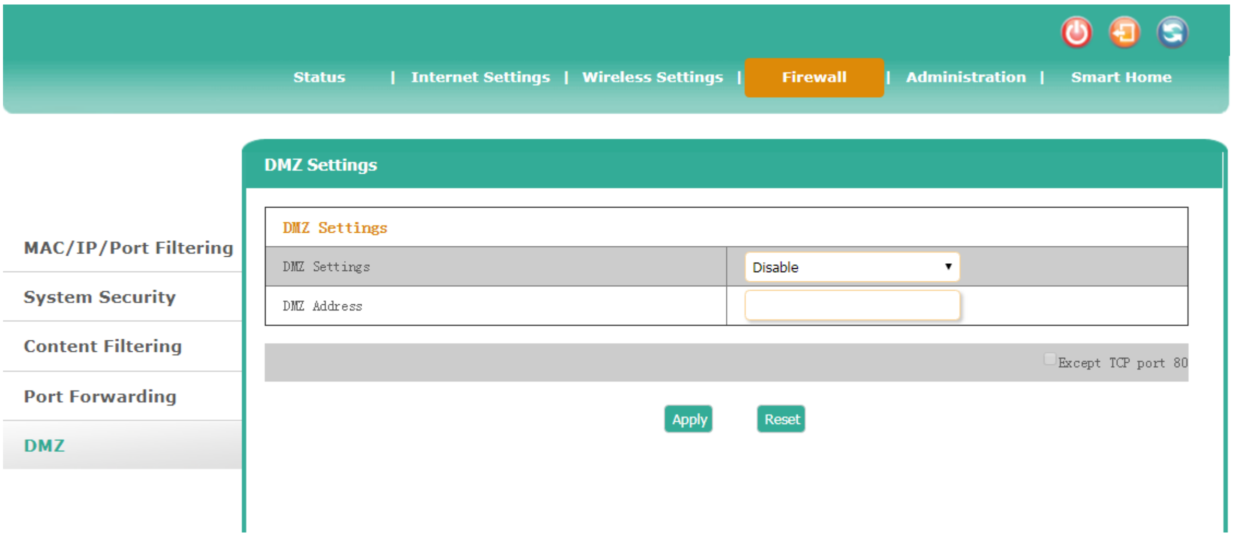
Current Port Forwarding in system:				
No.	IP Address	Port Range	Protocol	Comment

forward single port virtual server	
forward single port virtual server setting	Disable
IP Address	

5.6.5 DMZ

Whether to enable DMZ Settings

Establish a DMZ to distinguish the internal network from the Internet. Users need to set the DMZ IP address when enabling it.



DMZ Settings

DMZ Settings	
DMZ Settings	Disable ▾
DMZ Address	

☐ Except TCP port 80

5.7 Administration

5.7.1 Management

Modify gateway login Account and Password, NTP, Green AP, DDNS

In NTP Settings, users can check the current time and time zone of the gateway, network server, etc. When the current time of the gateway is different from the local time, users can click [Sync with host] to synchronize the time of the computer.

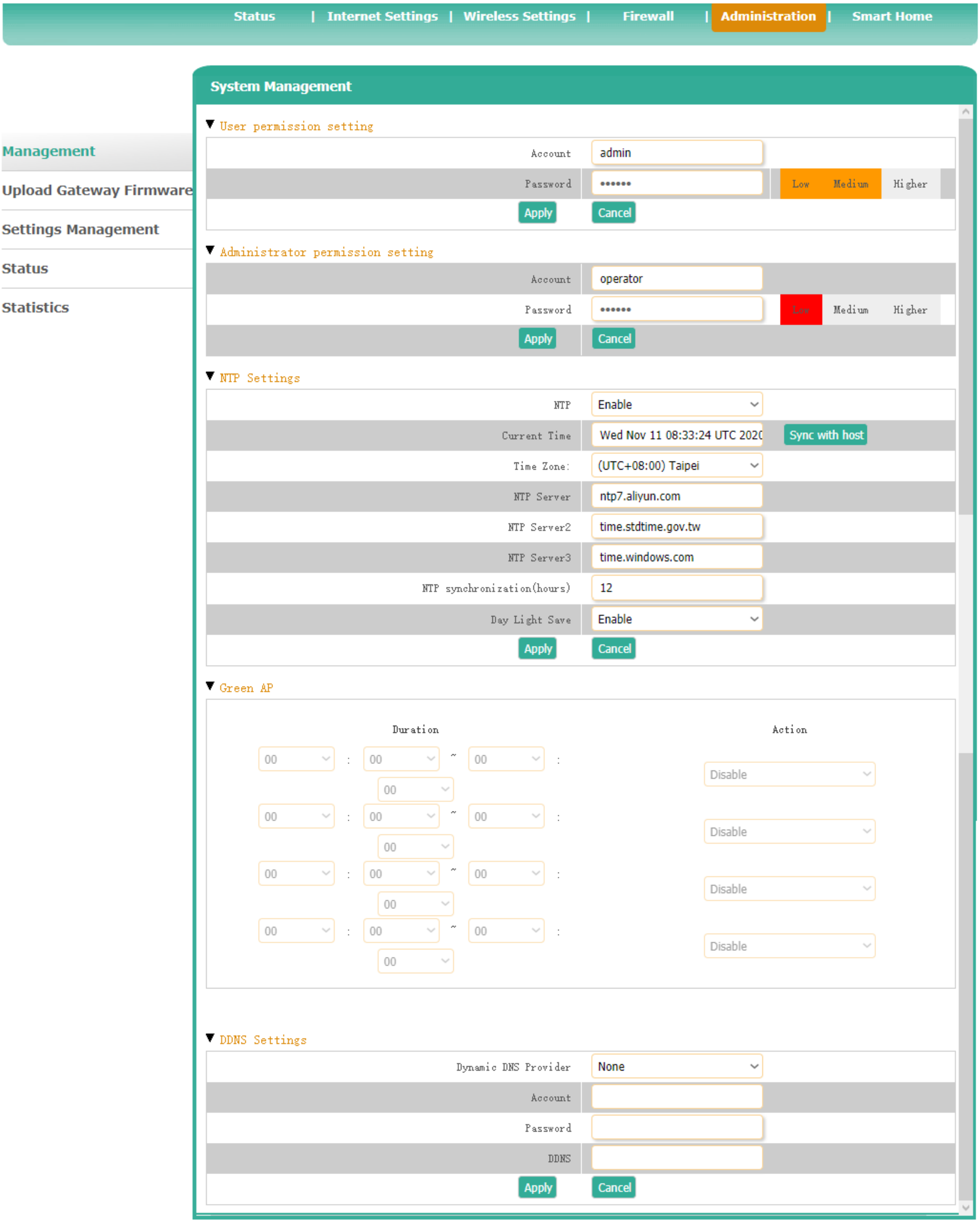
The NTP server is activated by default to ensure that the gateway synchronizes the time of the Internet every 12 hours. <u>The time zone must be consistent with the local time.</u>

There are three default network time servers:

NTP Server1：ntp7.aliyun.com

NTP Server2：time.stdtime.gov.tw

NTP Server3：time.windows.com



System Management

▼ User permission setting

Account: admin

Password: •••••• (Low / Medium / Higher)

▼ Administrator permission setting

Account: operator

Password: •••••• (Low / Medium / Higher)

▼ NTP Settings

NTP: Enable

Current Time: Wed Nov 11 08:33:24 UTC 2020

Time Zone: (UTC+08:00) Taipei

NTP Server: ntp7.aliyun.com

NTP Server2: time.stdtime.gov.tw

NTP Server3: time.windows.com

NTP synchronization(hours): 12

Day Light Save: Enable

▼ Green AP

Duration	Action
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable
00 : 00 ~ 00 : 00	Disable

▼ DDNS Settings

Dynamic DNS Provider: None

Account:

Password:

DDNS:

Note:

*Administrator permission setting will only be displayed after logging in to the operator account

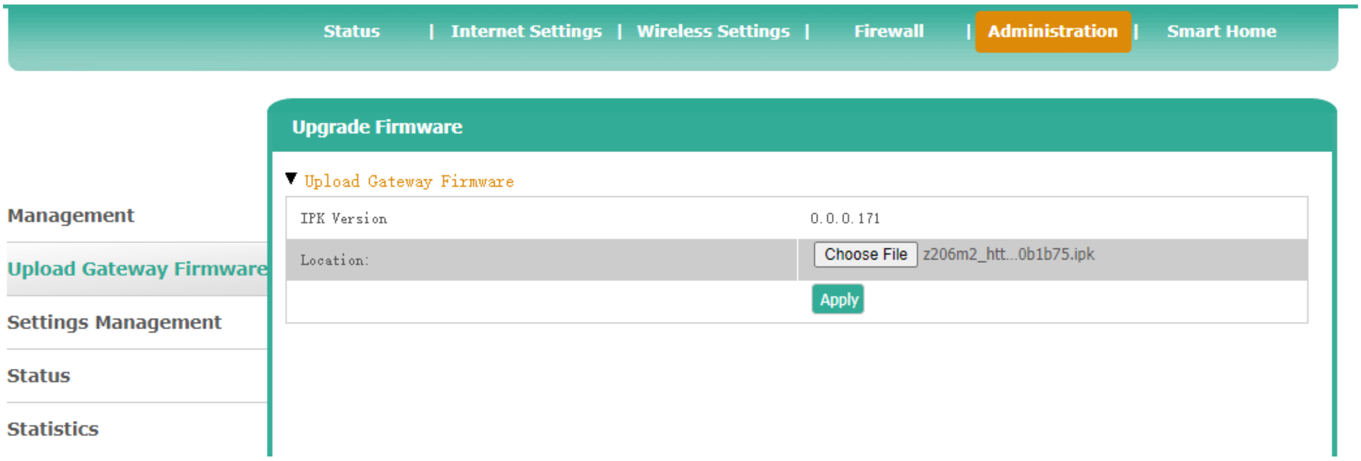
*Password Restriction: 1. It cannot be 123456.

2. The length must be greater than or equal to 6 digits.

3. It cannot be the same as the account. (after the version 0.0.0.163)

5.7.2 Upgrade Gateway Firmware

Upgrade the firmware of gateway



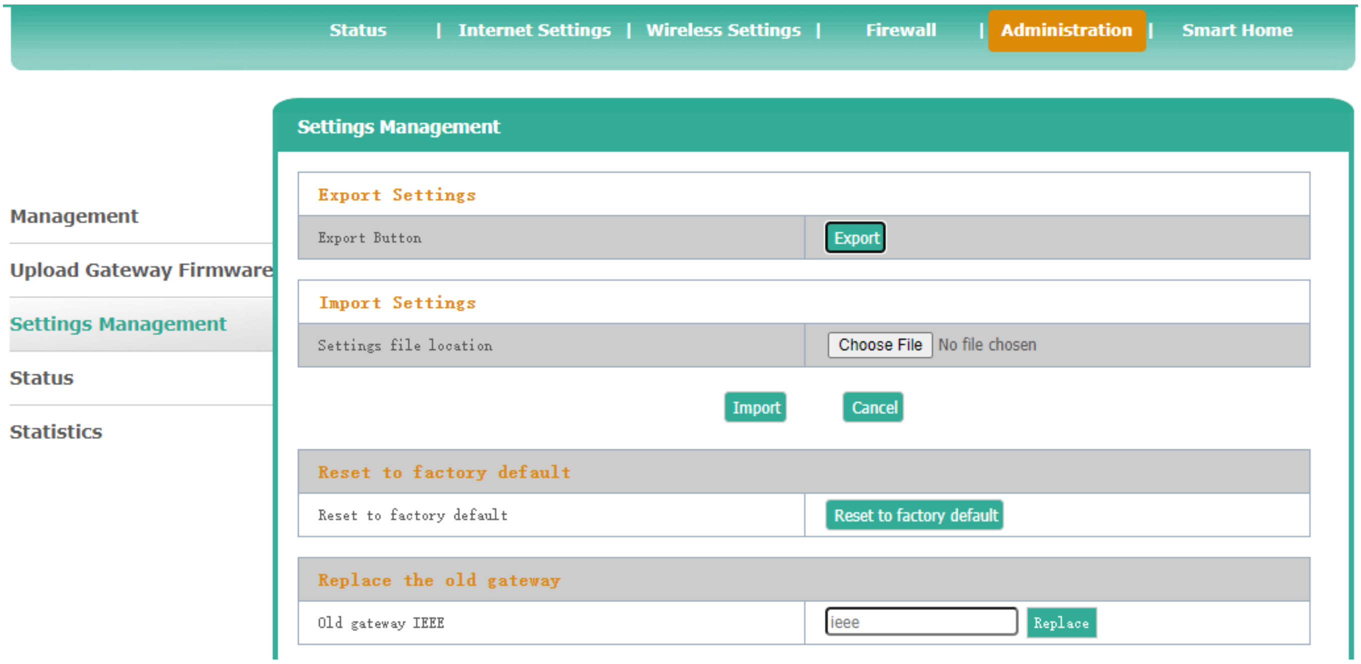
Upgrade Firmware

▼ Upload Gateway Firmware

IPK Version	0.0.0.171
Location:	z206m2_htt...0b1b75.ipk

5.7.3 Settings Management

A. Export/import gateway system configuration file (.dat) / Restore to factory default



Settings Management

Export Settings

Export Button

Import Settings

Settings file location: No file chosen

Reset to factory default

Reset to factory default

Replace the old gateway

Old gateway IEEE: ieee

B. Replace the Gateway

When the LoRa gateway is damaged or fails to operate normally, users can purchase a new LoRa gateway to replace the old one and change the new IEEE to the old IEEE.

(1) Only support IEEE address replacement of LoRa gateway

(2) The IPK version must be 0.0.0.143 and above.

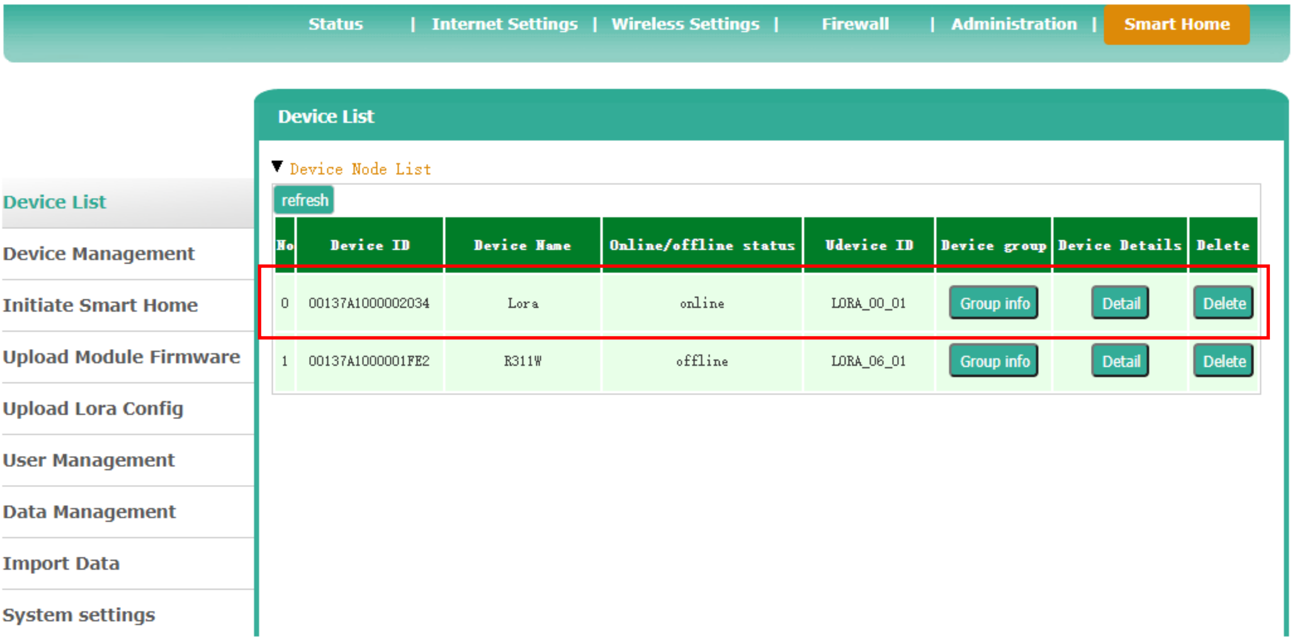
(3) After the replacement is successfully completed, the gateway is connected to the cloud and the backup data can be restored from the cloud. LoRa device needs to be powered on again to restore it.

1. Open the setting page of the new gateway, as the figure below

   The IEEE of new gateway: 00137A1000002034

   The IEEE of old gateway: 00137A1000001F1D

   Replace the IEEE of new gateway with the IEEE of old gateway.

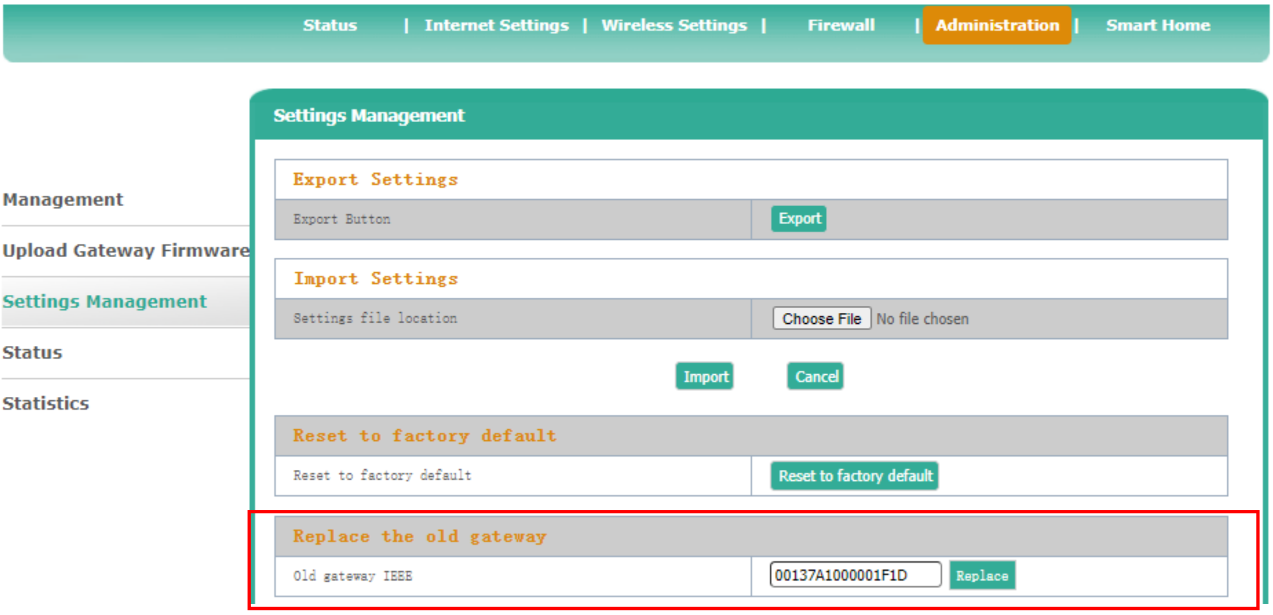


Device List

▼ Device Node List

No	Device ID	Device Name	Online/offline status	Udevice ID	Device group	Device Details	Delete
0	00137A1000002034	Lora	online	LORA_00_01	Group info	Detail	Delete
1	00137A1000001FE2	R311W	offline	LORA_06_01	Group info	Detail	Delete

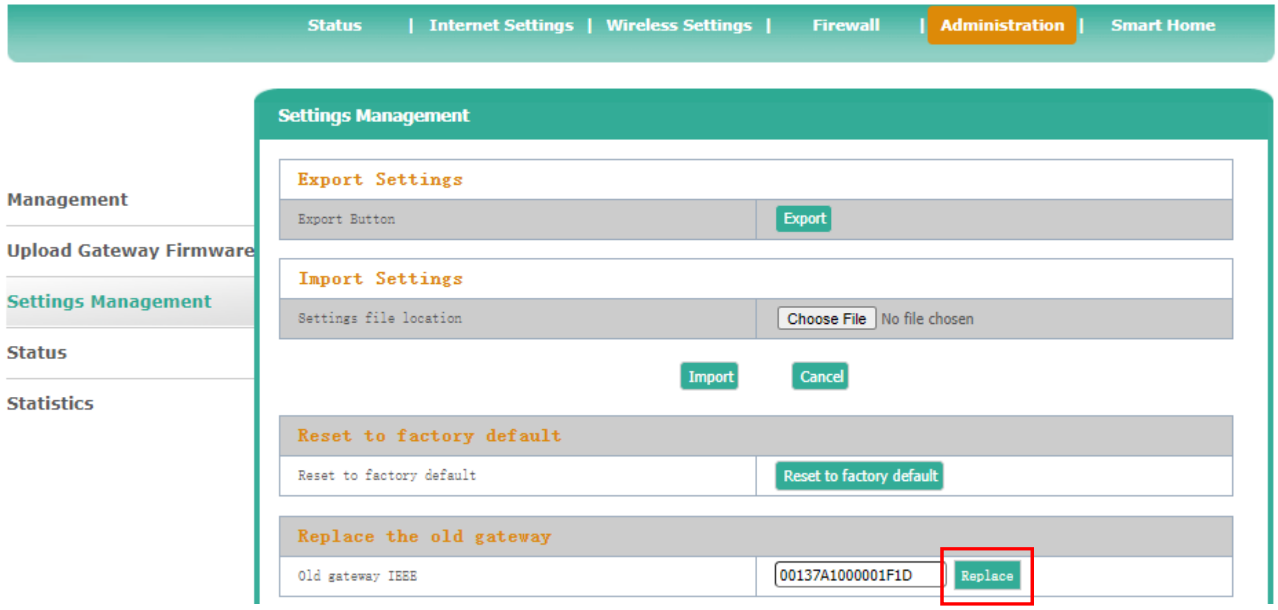
2. Click [Administration] > [Settings Management], and fill in the IEEE address of the old gateway in the input box, “Replace the old gateway”.



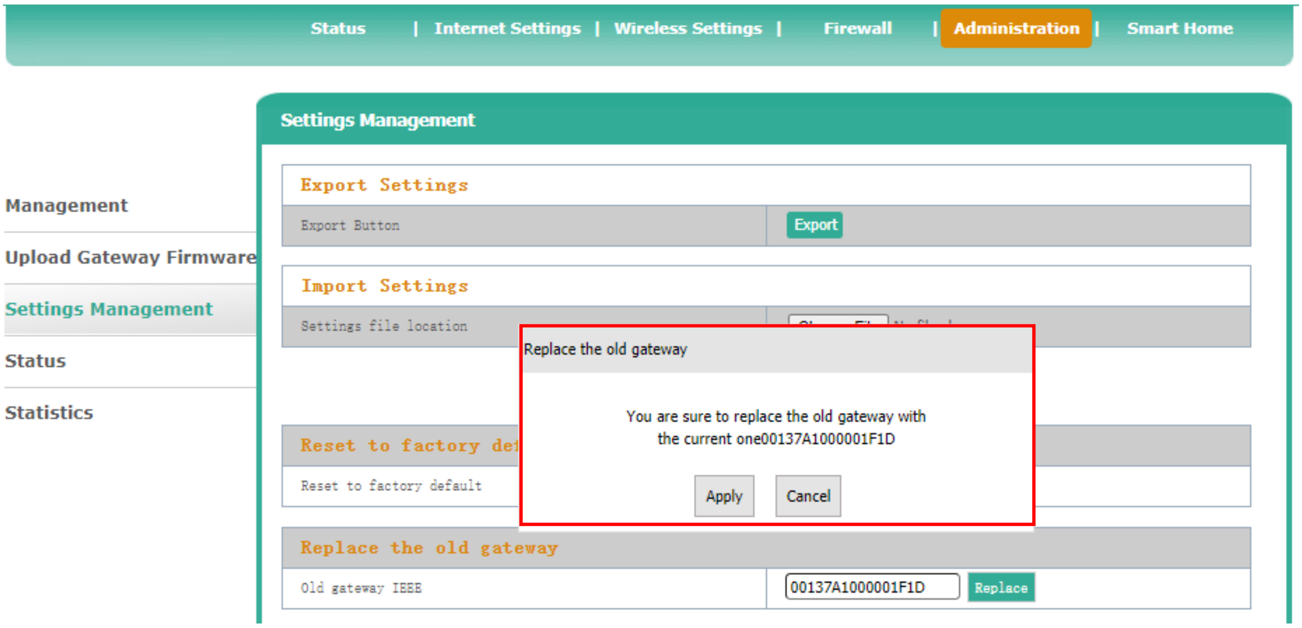
Settings Management

Export Settings	
Export Button	Export
Import Settings	
Settings file location	Choose File No file chosen
Reset to factory default	
Reset to factory default	Reset to factory default
Replace the old gateway	
Old gateway IEEE	00137A1000001F1D Replace

3. Click "Replace" and then click "Apply", and it can replace the IEEE address successfully



Old gateway IEEE: 00137A1000001F1D

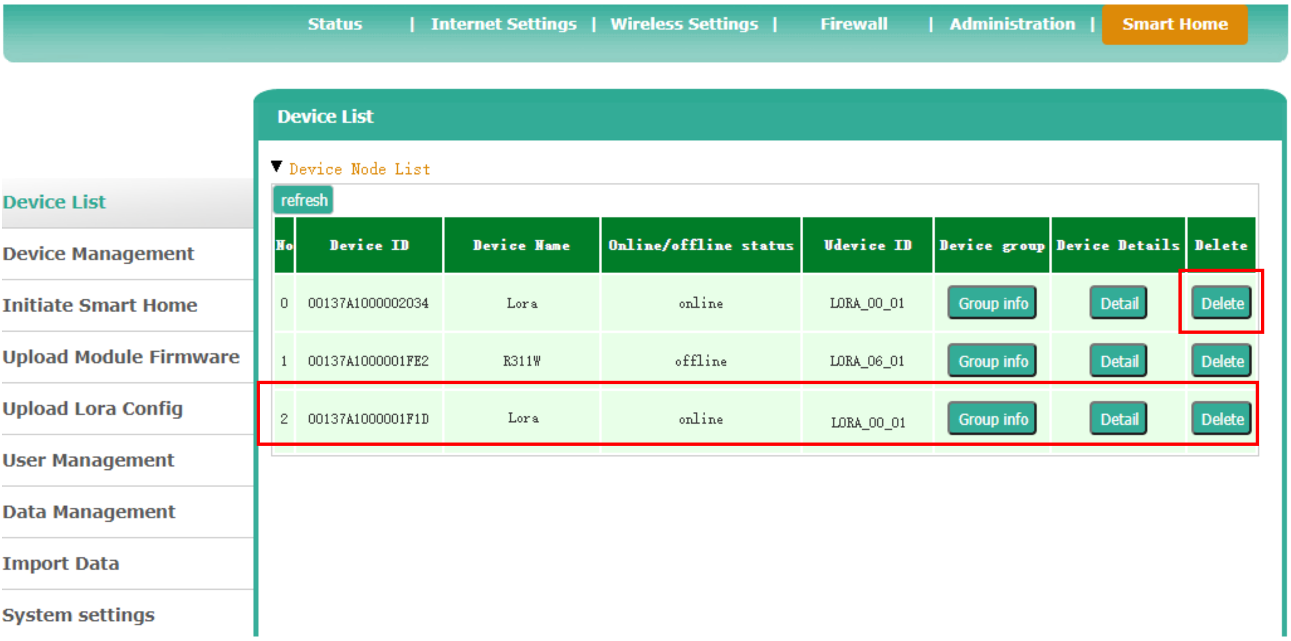


You are sure to replace the old gateway with the current one00137A1000001F1D

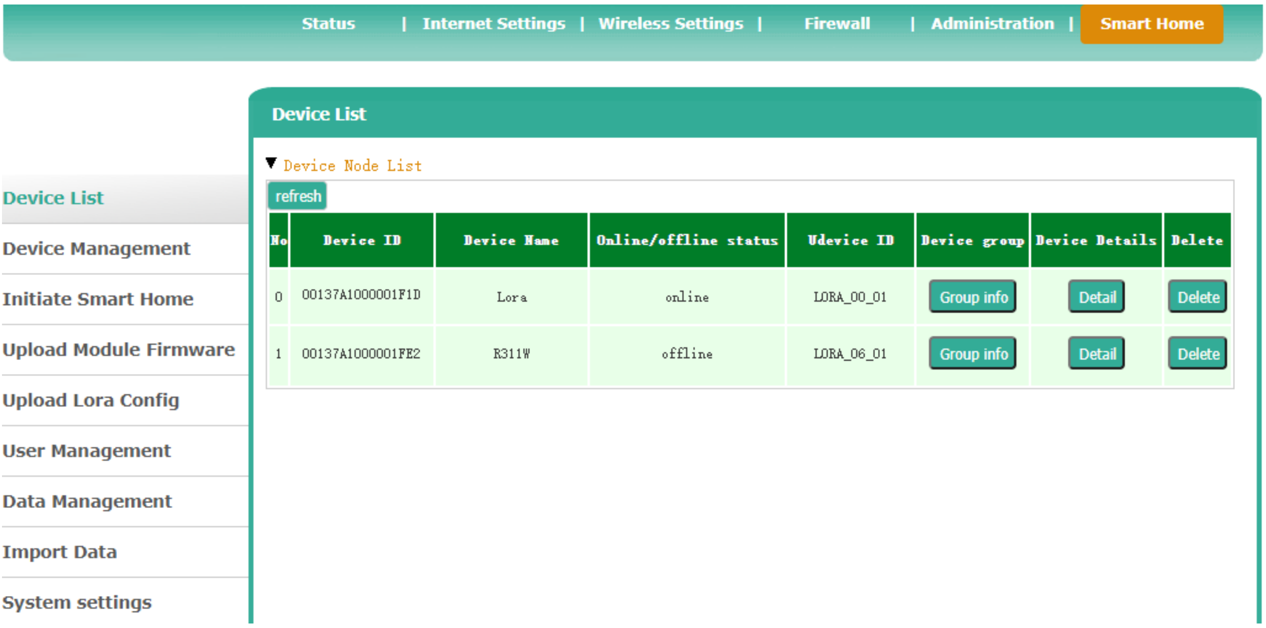
Old gateway IEEE: 00137A1000001F1D

4. After the replacement is successful, click [Smart Home] > [Device List], and the IEEE of old gateway (00137A1000001F1D) will be displayed.

   Then, you can delete the IEEE of the new gateway (00137A1000002034).

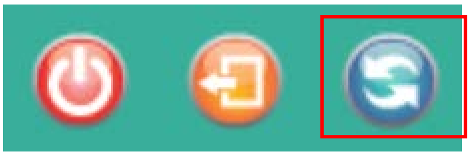


No	Device ID	Device Name	Online/offline status	Udevice ID	Device group	Device Details	Delete
0	00137A1000002034	Lora	online	LORA_00_01	Group info	Detail	Delete
1	00137A1000001FE2	R311W	offline	LORA_06_01	Group info	Detail	Delete
2	00137A1000001F1D	Lora	online	LORA_00_01	Group info	Detail	Delete



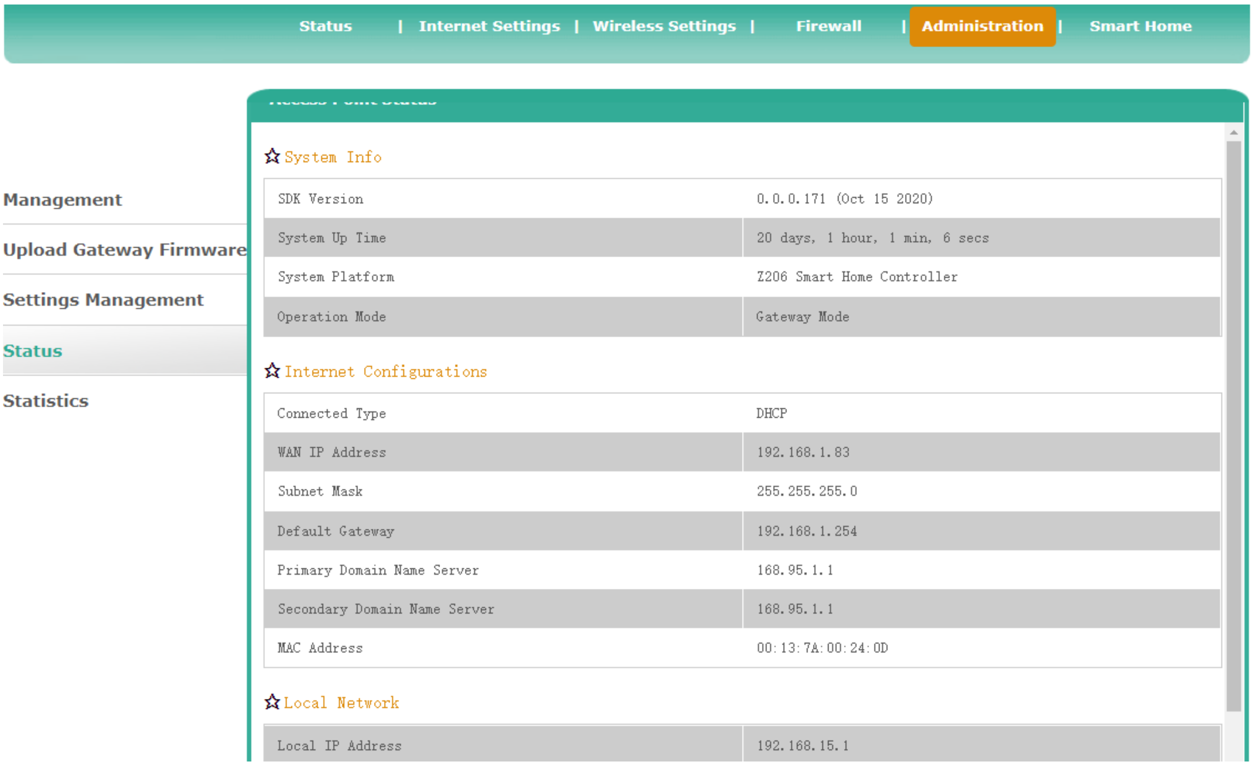
No	Device ID	Device Name	Online/offline status	Udevice ID	Device group	Device Details	Delete
0	00137A1000001F1D	Lora	online	LORA_00_01	Group info	Detail	Delete
1	00137A1000001FE2	R311W	offline	LORA_06_01	Group info	Detail	Delete

5. After the deletion is successful, click the restart button in the upper right corner to restart the gateway once and the replacement can be successful.



5.7.4 Status

Check the current system information and the network status of the gateway



☆System Info

SDK Version	0.0.0.171 (Oct 15 2020)
System Up Time	20 days, 1 hour, 1 min, 6 secs
System Platform	Z206 Smart Home Controller
Operation Mode	Gateway Mode

☆Internet Configurations

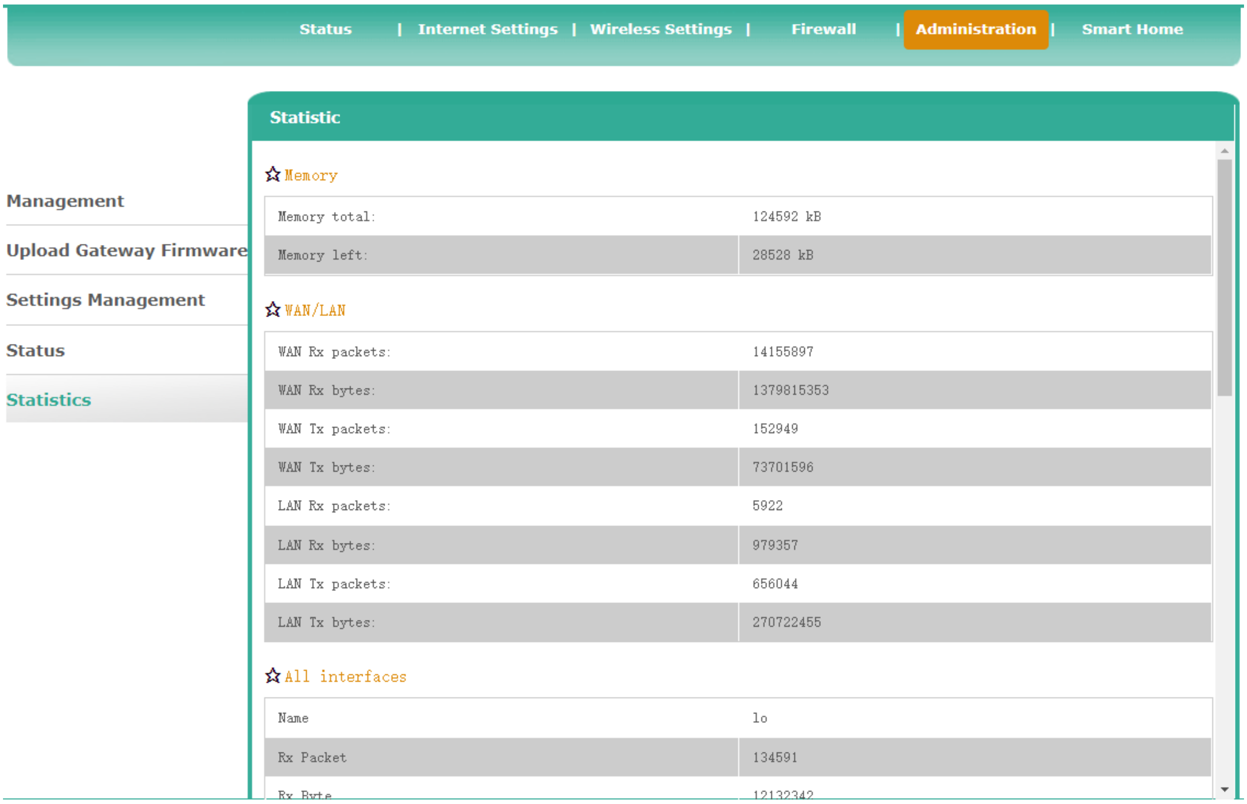
Connected Type	DHCP
WAN IP Address	192.168.1.83
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1
MAC Address	00:13:7A:00:24:0D

☆Local Network

Local IP Address	192.168.15.1

5.7.5 Statistic

Check the statistics of the gateway, including device memory capacity, WAN data packets, and LAN data packets



Statistic

☆Memory

Memory total:	124592 kB
Memory left:	28528 kB

☆WAN/LAN

WAN Rx packets:	14155897
WAN Rx bytes:	1379815353
WAN Tx packets:	152949
WAN Tx bytes:	73701596
LAN Rx packets:	5922
LAN Rx bytes:	979357
LAN Tx packets:	656044
LAN Tx bytes:	270722455

☆All interfaces

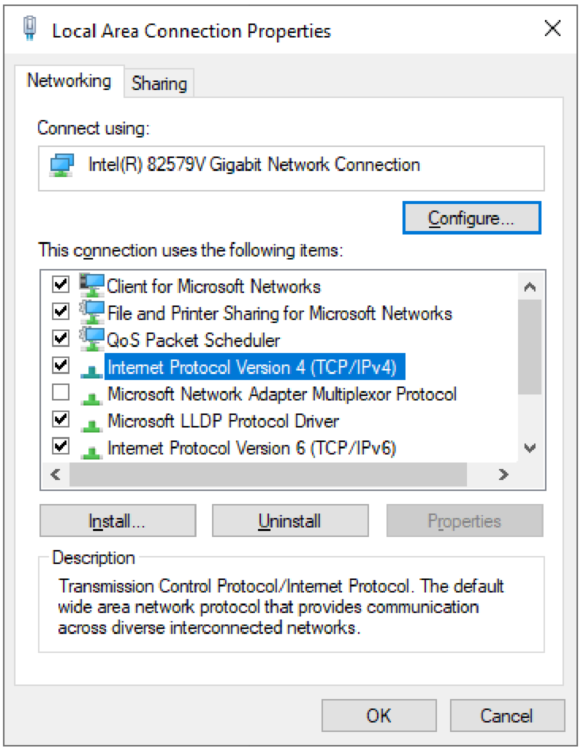
Name	lo
Rx Packet	134591
Rx Byte	12132342

5.8 Bridging Settings

Please use a network cable to connect the LAN port of R206 to the network port of your computer, and use the matching switch transformer to power up R206.

Set the computer IP to be acquired automatically:

1.Click the network icon on the computer taskbar ((Or enter “Control Panel” > “Network and Internet” > “Network Connections” > Right click to open“Local Area Connection Properties” > “TCP/IPv4” > Obtain an IP address automatically)



Local Area Connection Properties

Networking | Sharing

Connect using:

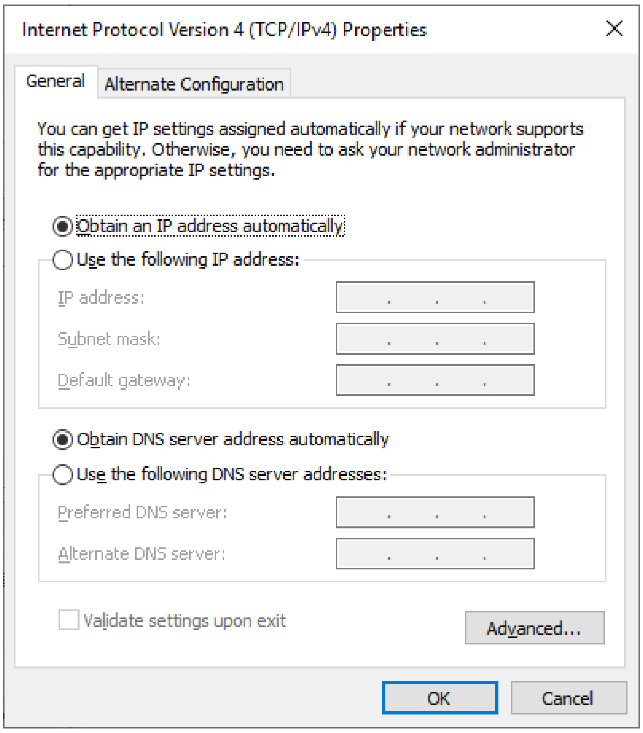
Intel(R) 82579V Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

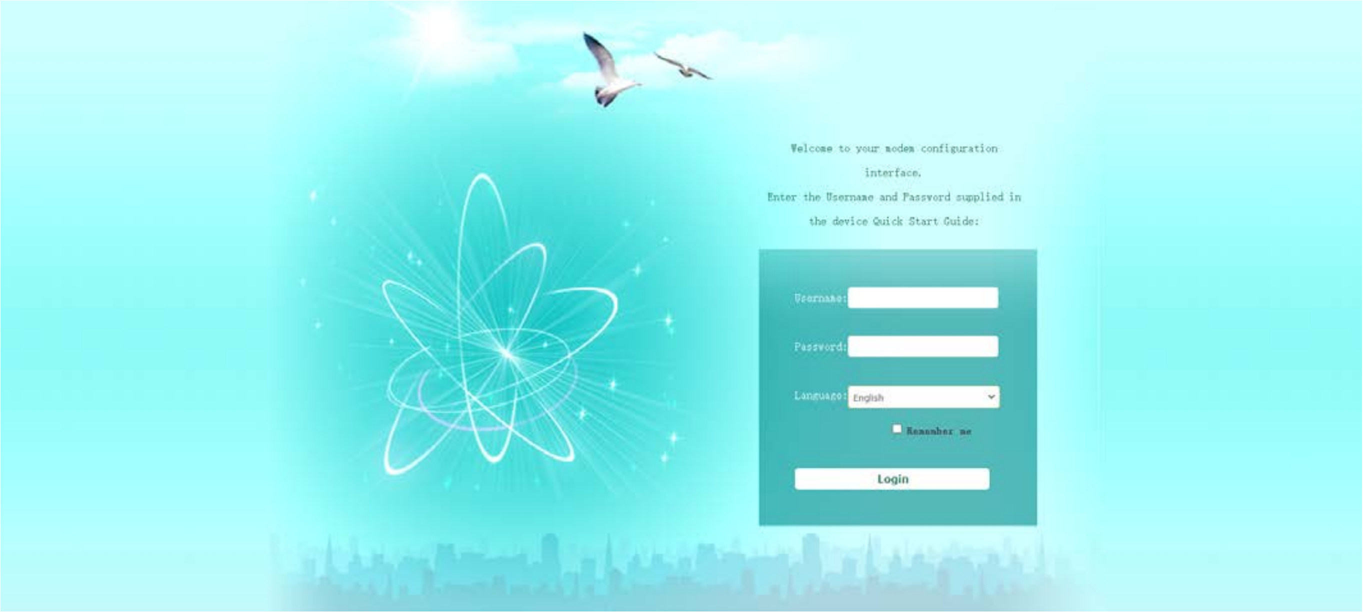
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

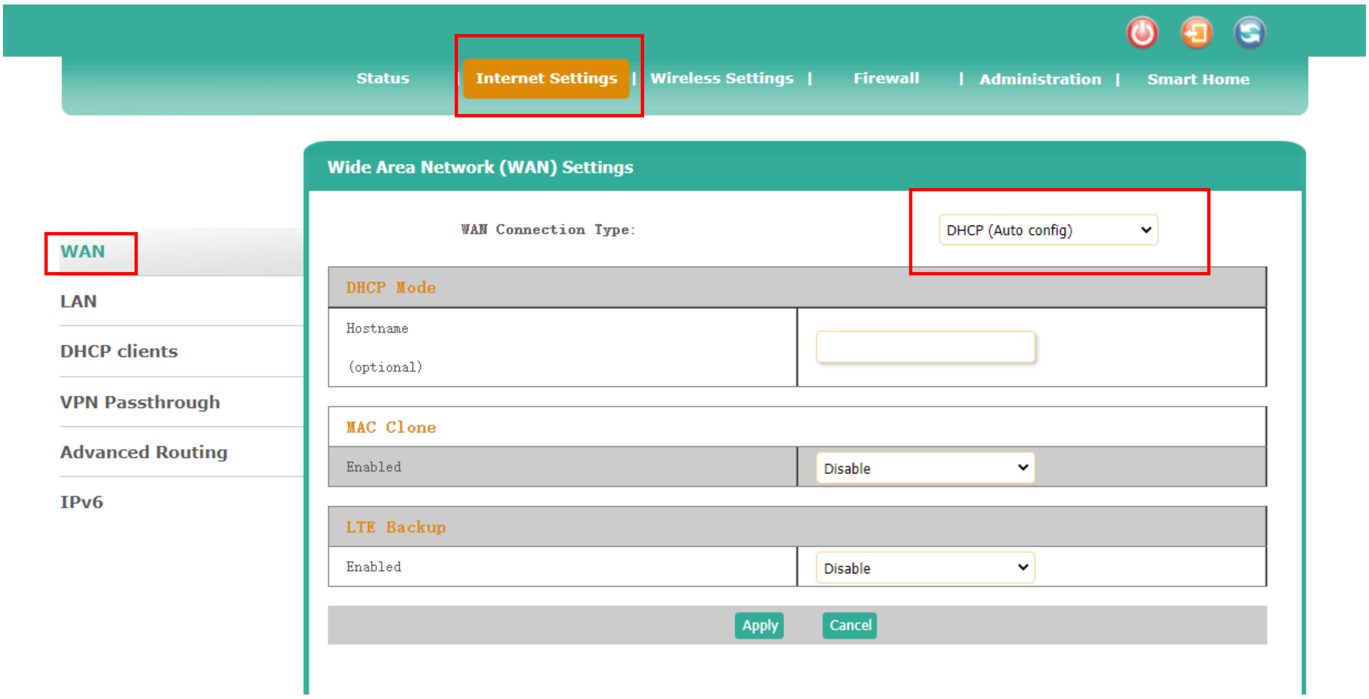
2. Wait for R206 startup to complete (WiFi light is on), open the browser to enter 192.168.15.1, and log in to R206 homepage.



Welcome to your modem configuration interface.
Enter the Username and Password supplied in the device Quick Start Guide:

Username:
Password:
Language: English
□ Remember me

3. After logging in, click [Internet Settings], set the [WAN Connection Type] as DHCP (Auto config), and click "OK".



Wide Area Network (WAN) Settings

WAN Connection Type: DHCP (Auto config)

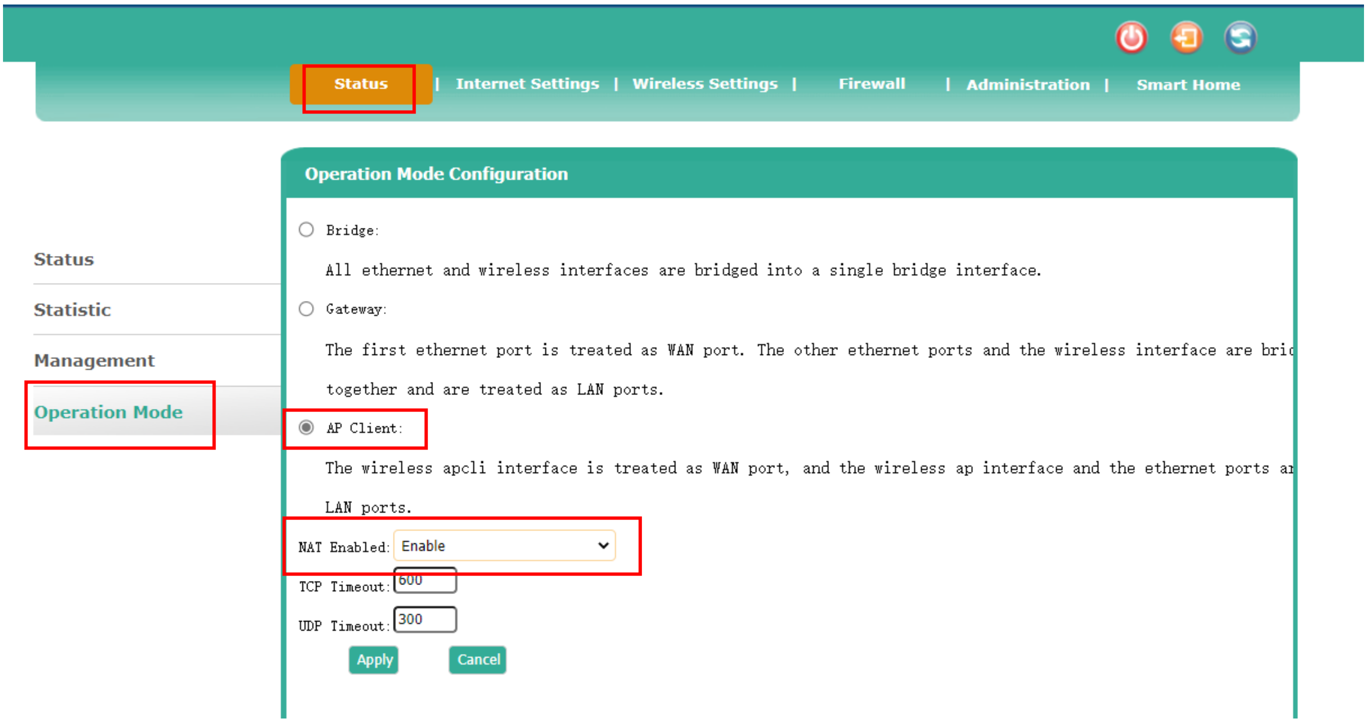
DHCP Mode	
Hostname (optional)	

MAC Clone	
Enabled	Disable

LTE Backup	
Enabled	Disable

4. Click [Status] → [Operation Mode], select [AP Client], set [NAT Enabled] as enable, and click [Apply].

(Note: If it cannot be modified to AP client after confirmation, it is recommended to change Google, Firefox and IE browsers and try again. After setting, the web page will be disconnected. Please wait for reconnection.)


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Status
Statistic
Management
Operation Mode

Operation Mode Configuration

○ Bridge:

All ethernet and wireless interfaces are bridged into a single bridge interface.

○ Gateway:

The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bric

together and are treated as LAN ports.

● AP Client:

The wireless apcli interface is treated as WAN port, and the wireless ap interface and the ethernet ports ar

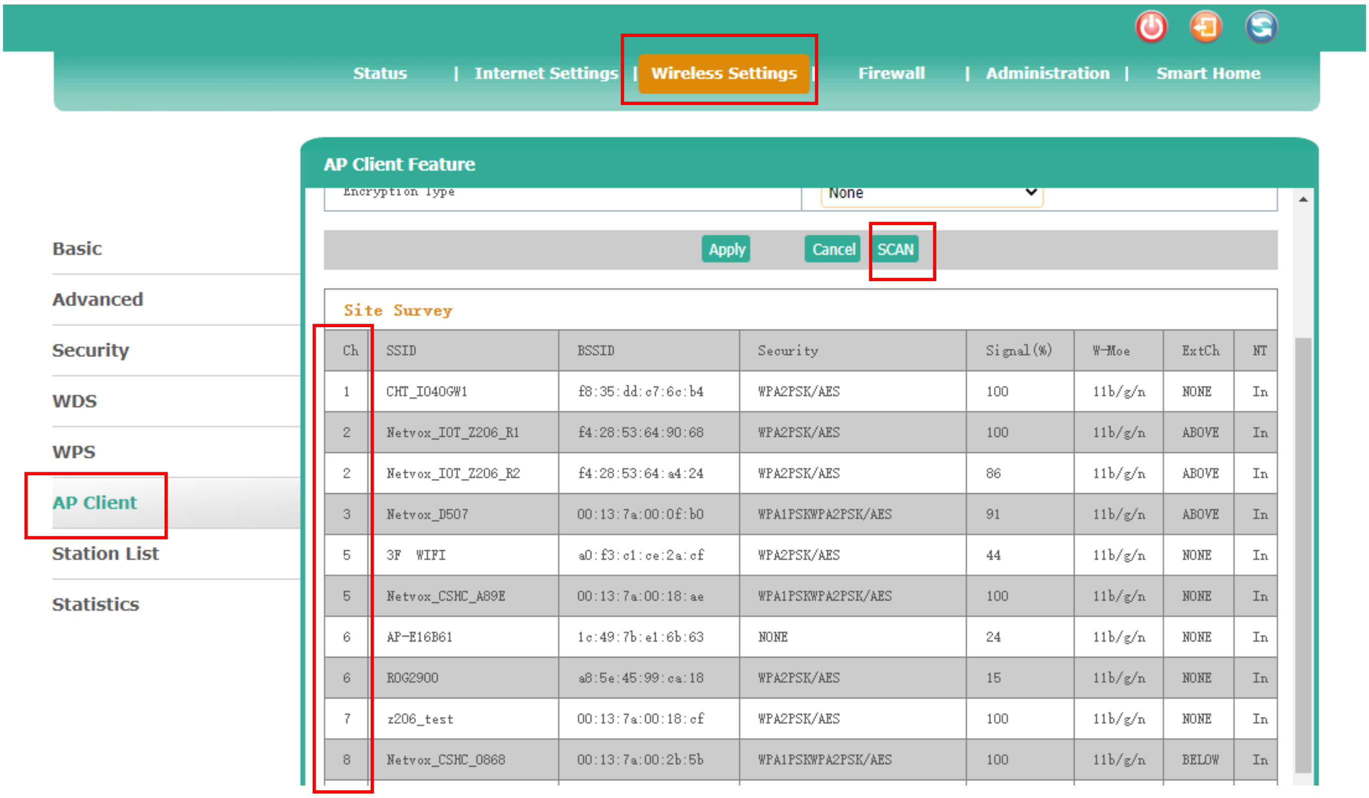
LAN ports.

NAT Enabled: Enable

TCP Timeout: 600

UDP Timeout: 300

5. After the webpage is reconnected, click [Wireless Settings] → [AP Client] to view the WiFi channel of the router to be bridged in the WiFi list.


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Basic
Advanced
Security
WDS
WPS
AP Client
Station List
Statistics

AP Client Feature

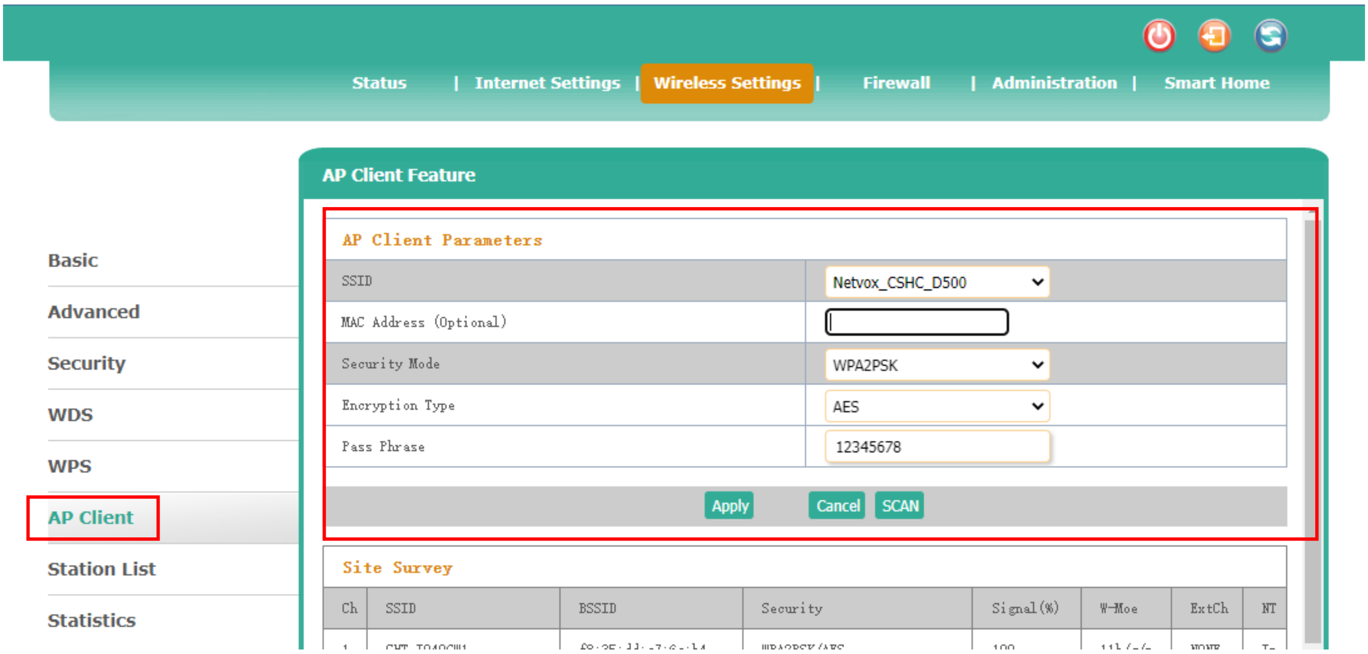
Encryption Type: None

Site Survey

Ch	SSID	BSSID	Security	Signal(%)	W-Moe	ExtCh	NT
1	CHT_I040GW1	f8:35:dd:c7:6c:b4	WPA2PSK/AES	100	11b/g/n	NONE	In
2	Netvox_IOT_Z206_R1	f4:28:53:64:90:68	WPA2PSK/AES	100	11b/g/n	ABOVE	In
2	Netvox_IOT_Z206_R2	f4:28:53:64:a4:24	WPA2PSK/AES	86	11b/g/n	ABOVE	In
3	Netvox_D507	00:13:7a:00:0f:b0	WPA1PSKWPA2PSK/AES	91	11b/g/n	ABOVE	In
5	3F WIFI	a0:f3:c1:ce:2a:cf	WPA2PSK/AES	44	11b/g/n	NONE	In
5	Netvox_CSHC_A89E	00:13:7a:00:18:ae	WPA1PSKWPA2PSK/AES	100	11b/g/n	NONE	In
6	AP-E16B61	1c:49:7b:e1:6b:63	NONE	24	11b/g/n	NONE	In
6	ROG2900	a8:5e:45:99:ca:18	WPA2PSK/AES	15	11b/g/n	NONE	In
7	z206_test	00:13:7a:00:18:cf	WPA2PSK/AES	100	11b/g/n	NONE	In
8	Netvox_CSHC_0868	00:13:7a:00:2b:5b	WPA1PSKWPA2PSK/AES	100	11b/g/n	BELOW	In

6. Enter the WiFi information of the router to be bridged (including WiFi name, Mac address, security mode, encryption method, WiFi password, etc.) in the [AP Client Feature] item, and then click [Apply]

(Note: the web page will be disconnected after setting, please wait for reconnection). After the web page is reconnected, the bridging setting is completed.


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Basic
Advanced
Security
WDS
WPS
AP Client
Station List
Statistics
Apply
Cancel
SCAN

AP Client Feature

AP Client Parameters

SSID	Netvox_CSHC_D500
MAC Address (Optional)	
Security Mode	WPA2PSK
Encryption Type	AES
Pass Phrase	12345678

Site Survey

Ch	SSID	BSSID	Security	Signal(%)	W-Moe	ExtCh	NT
1	[illegible]	[illegible]	WPA2PSK/AES	100	[illegible]	NONE	[illegible]

Note:

1. If the WiFi security mode of the router to be bridged is "WPAPSK/WPA2PSK", select "WPA2PSK" as the Security mode in "AP Client Feature".

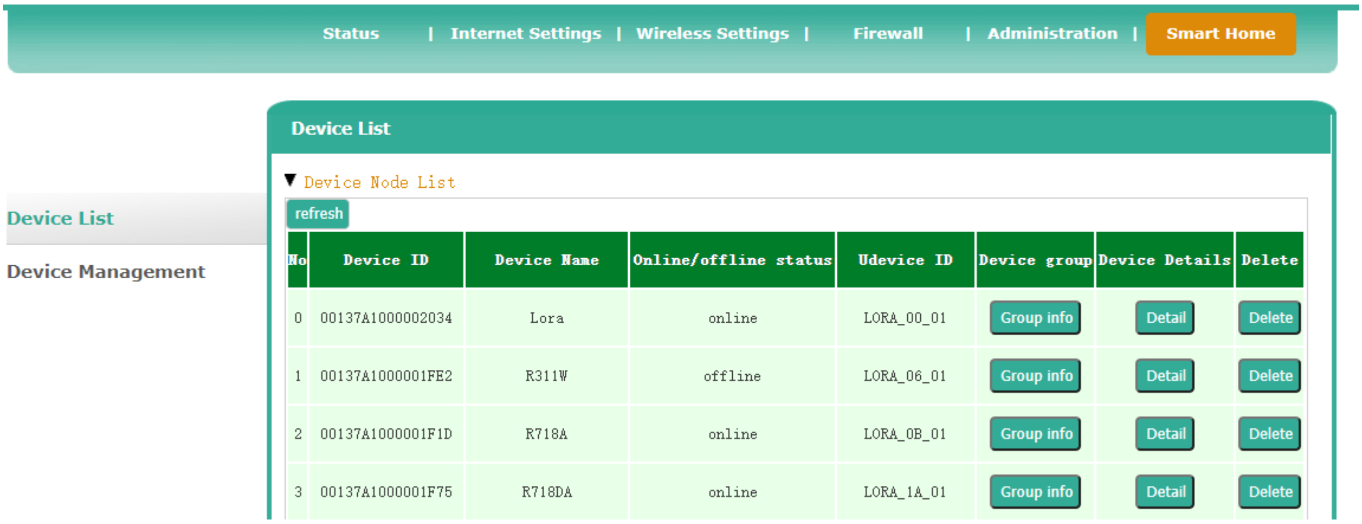
2. If you log in to the R206 homepage with a mobile phone or tablet connected to the R206 WiFi, the WiFi will be disconnected after making some settings. Please reconnect to the R206 WiFi before refreshing the page.

5.9 Smart Home

LoRa and Zigbee devices management

5.9.1 Device List

It can check the current device information, including Device ID, Device Name, Online/offline status, Device Details, etc.


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Device List
Device Management
refresh

Device List

▼ Device Node List

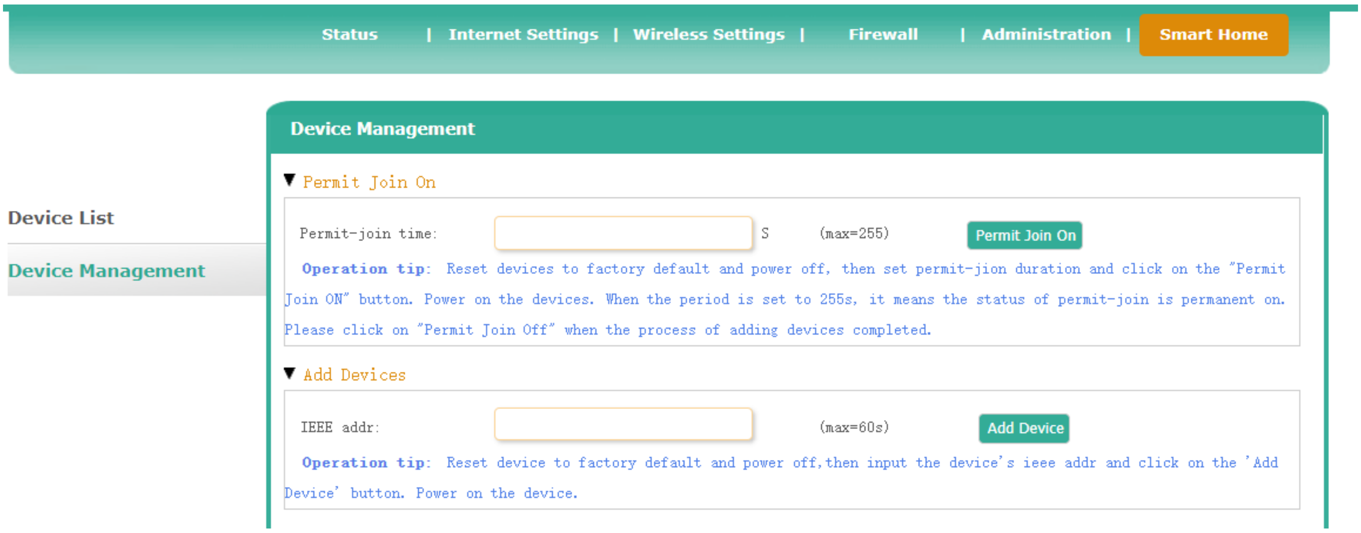
No	Device ID	Device Name	Online/offline status	Udevice ID	Device group	Device Details	Delete
0	00137A1000002034	Lora	online	LORA_00_01	Group info	Detail	Delete
1	00137A1000001FE2	R311W	offline	LORA_06_01	Group info	Detail	Delete
2	00137A1000001F1D	R718A	online	LORA_0B_01	Group info	Detail	Delete
3	00137A1000001F75	R718DA	online	LORA_1A_01	Group info	Detail	Delete

Note:

*LoRa doesn’t support Group info.

5.9.2 Device Management

When Lora devices join to the network, users need to enter IEEE (DevEUI) to enter the network. After joining, users can refresh the device list to check whether the device has been successfully joined.


Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Device List
Device Management
Permit Join On
Add Device

Device Management

▼ Permit Join On

Permit-join time: S (max=255)

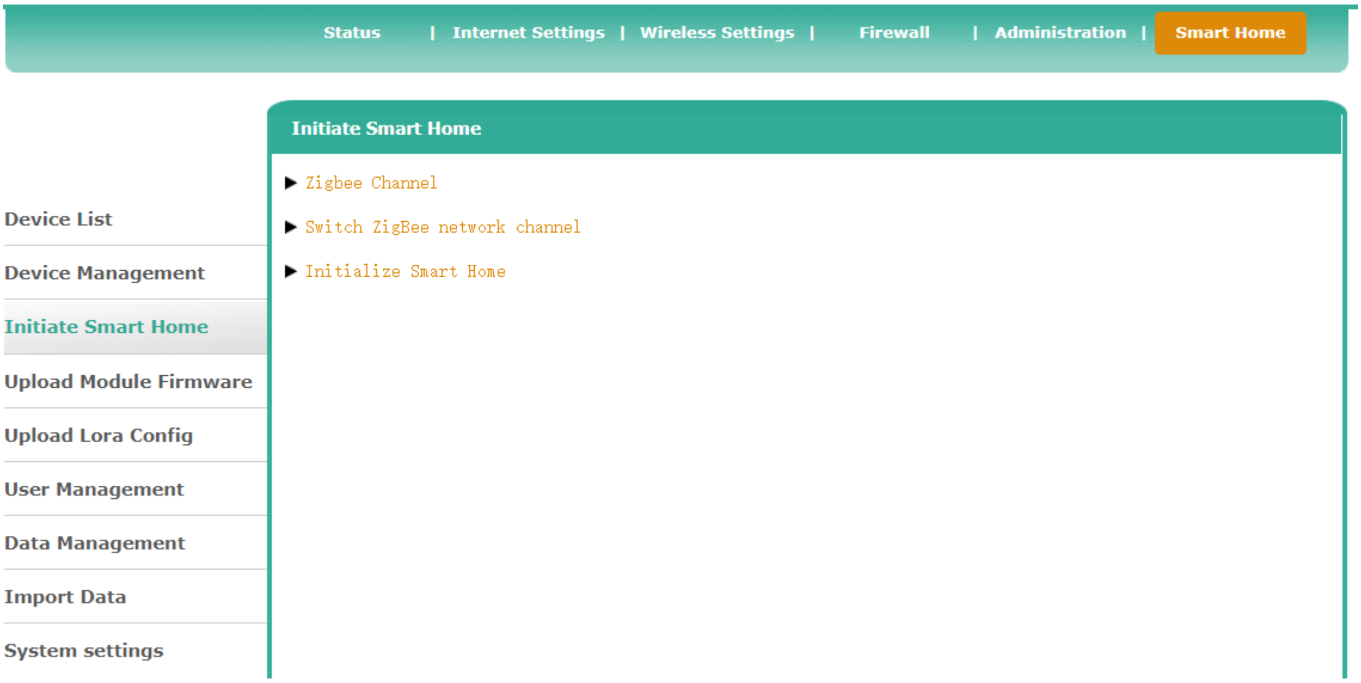
Operation tip: Reset devices to factory default and power off, then set permit-jion duration and click on the "Permit Join ON" button. Power on the devices. When the period is set to 255s, it means the status of permit-join is permanent on. Please click on "Permit Join Off" when the process of adding devices completed.

▼ Add Devices

IEEE addr: (max=60s)

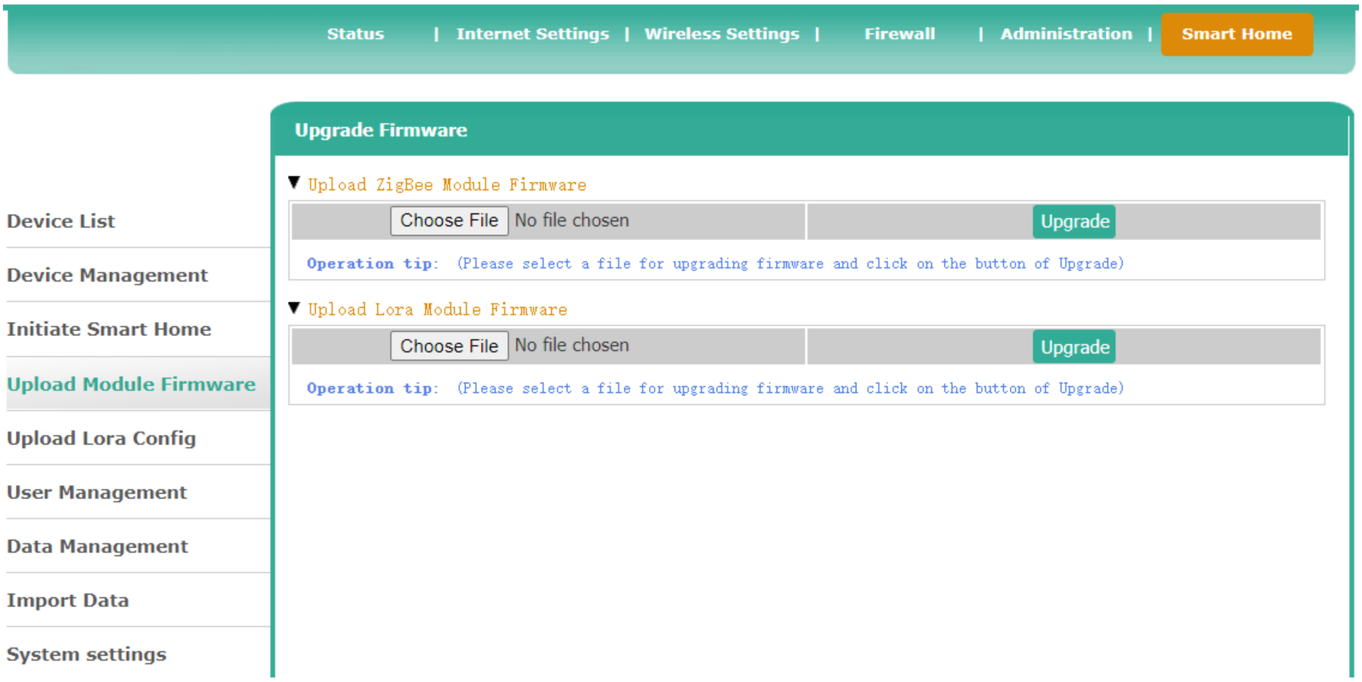
Operation tip: Reset device to factory default and power off,then input the device's ieee addr and click on the 'Add Device' button. Power on the device.

5.9.3 Initiate Smart Home (This item will only be displayed for operator accounts.)



5.9.4 Upload Module Firmware (This item will only be displayed for operator accounts.)

Upgrade LoRa module firmware (Zigbee module firmware upgrade is not supported.)

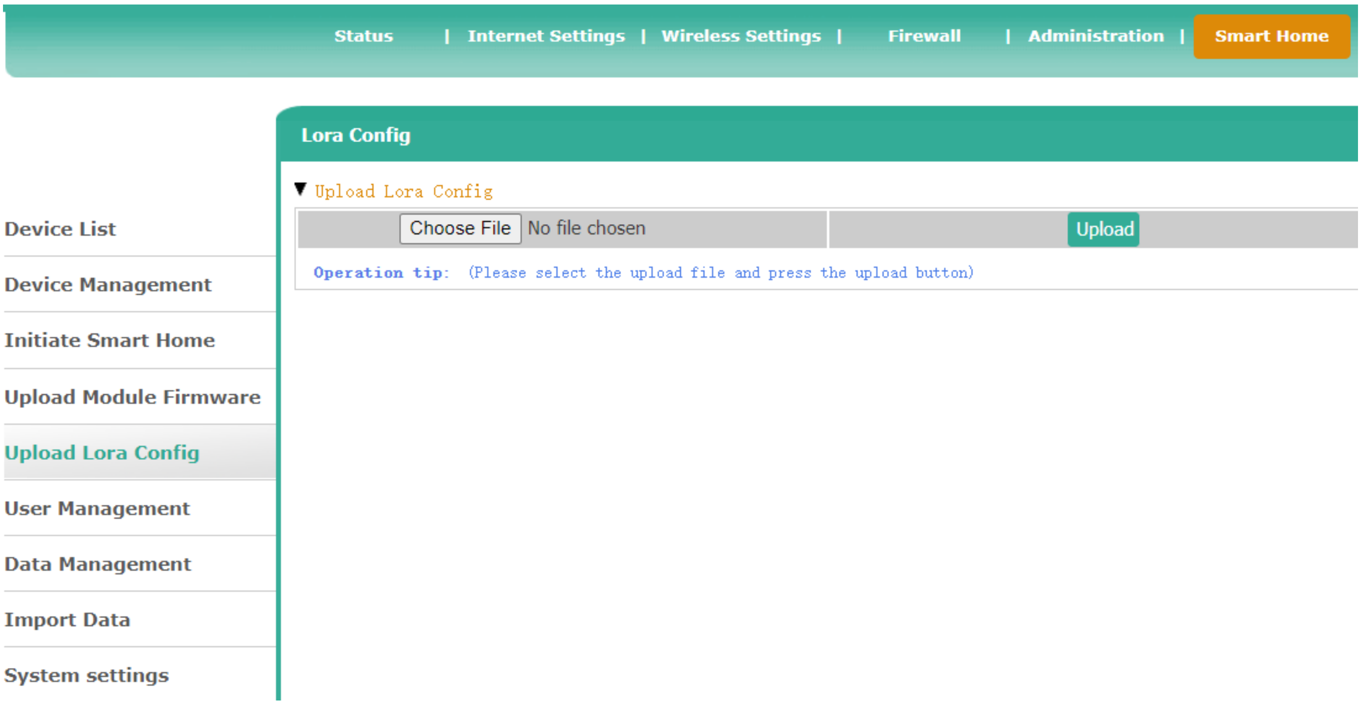

Status | Internet Settings | Wireless Settings | Firewall | Administration | Smart Home
Upgrade Firmware
▼ Upload ZigBee Module Firmware
Choose File No file chosen
Upgrade
▼ Upload Lora Module Firmware
Choose File No file chosen
Upgrade
Device List
Device Management
Initiate Smart Home
Upload Module Firmware
Upload Lora Config
User Management
Data Management
Import Data
System settings

Operation tip: (Please select a file for upgrading firmware and click on the button of Upgrade)

Operation tip: (Please select a file for upgrading firmware and click on the button of Upgrade)

5.9.5 Upload Lora Config (This item will only be displayed for operator accounts.)

Upload the LoRa configuration file. When the new device cannot get the cloud information, users can upload the LoRa configuration file (LoraAttr.xml) to update by self.



Lora Config

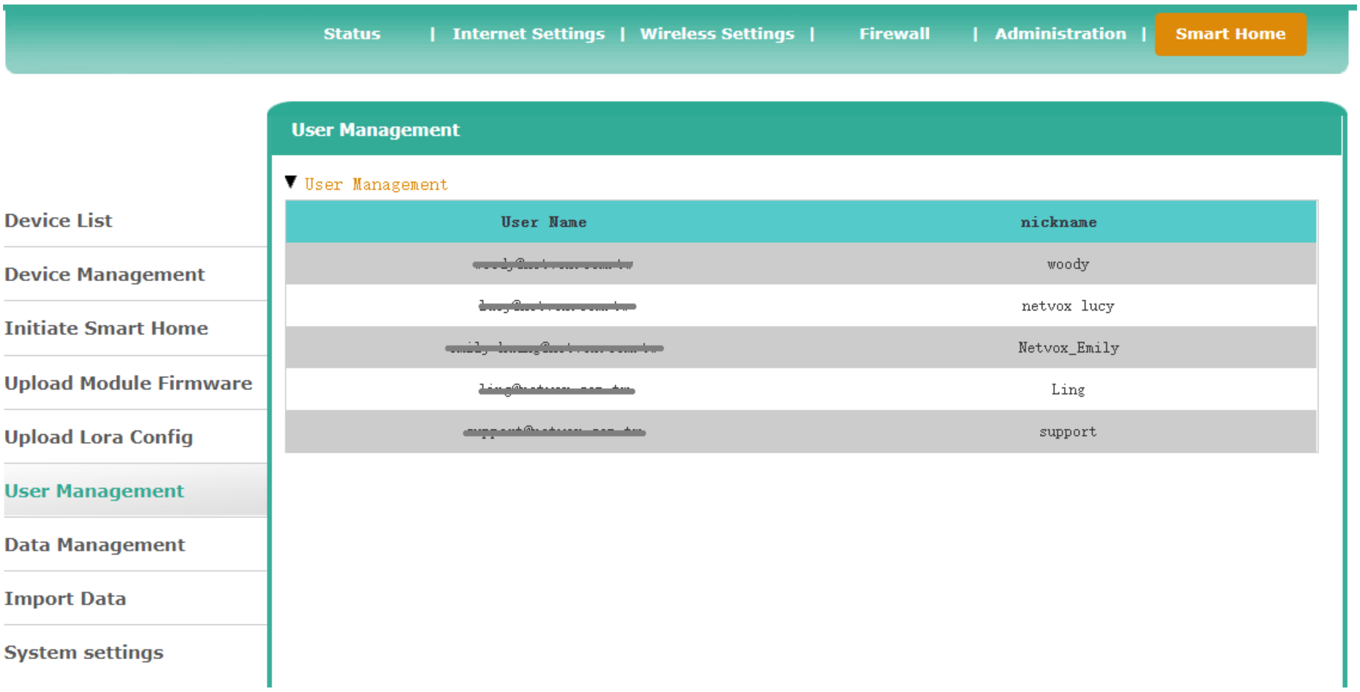
▼ Upload Lora Config

No file chosen

Operation tip: (Please select the upload file and press the upload button)

5.9.6 User Management (This item will only be displayed for operator accounts.)

Check the registered account of the gateway



User Management

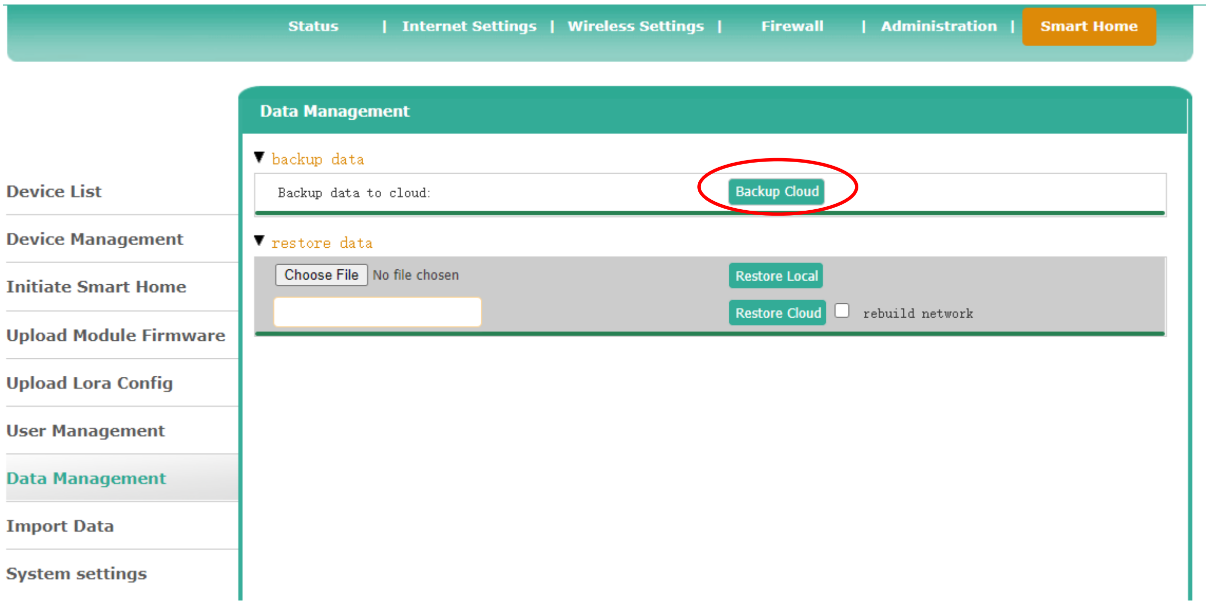
▼ User Management

User Name	nickname
[redacted]	woody
[redacted]	netvox lucy
[redacted]	Netvox_Emily
[redacted]	Ling
[redacted]	support

5.9.7 Data Management (This item will only be displayed for operator accounts.)

When the gateway is connected to the cloud, users can choose to manually back up the data to the cloud. Later, if the device is abnormally powered off and the file is lost, users can choose to restore the data backed up from the cloud.

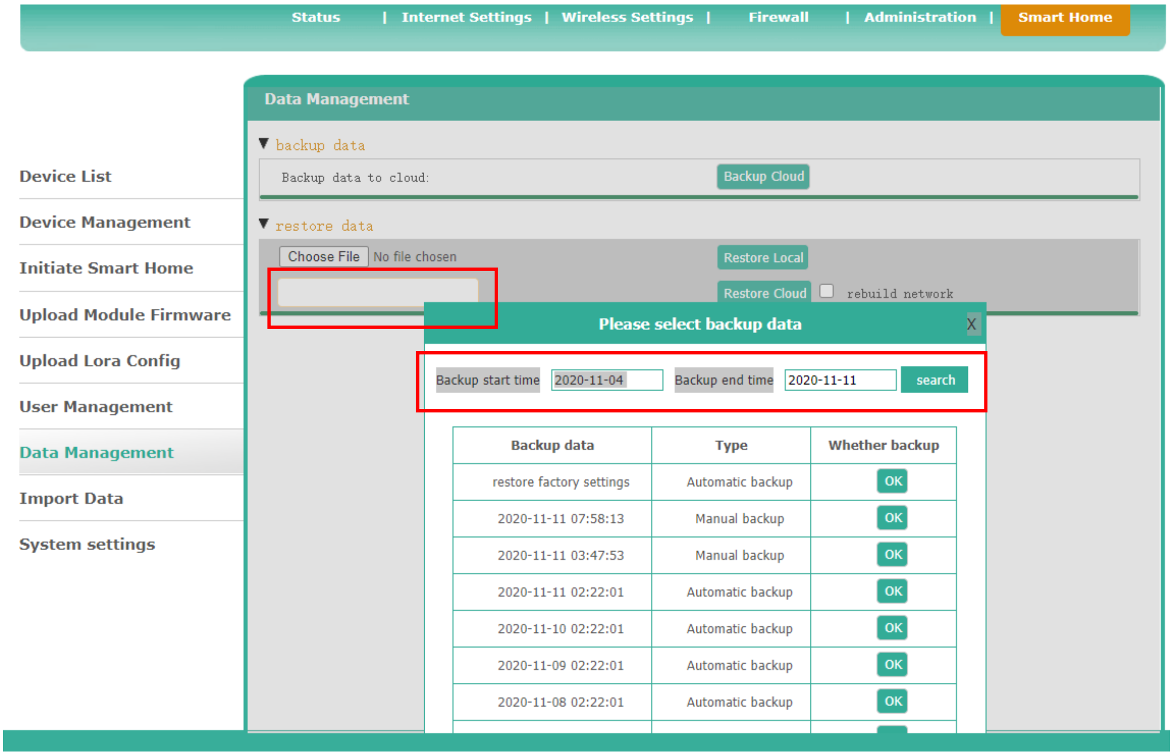
A. Backup the data of LoRa device to the cloud



B. Import cloud backup data

Select “Backup start time” and “Backup end time” in the restore data column, and click “search” to select the backup data of the corresponding date to restore.

After selecting the date, it will be displayed in the list, click the [OK] to restore the backed up data.



Backup start time 2020-11-04 Backup end time 2020-11-11

Backup data	Type	Whether backup
restore factory settings	Automatic backup	OK
2020-11-11 07:58:13	Manual backup	OK
2020-11-11 03:47:53	Manual backup	OK
2020-11-11 02:22:01	Automatic backup	OK
2020-11-10 02:22:01	Automatic backup	OK
2020-11-09 02:22:01	Automatic backup	OK
2020-11-08 02:22:01	Automatic backup	OK

Note:

*When the gateway is damaged and needs to replace with a new gateway, users can choose to restore cloud backup.

* Rebuild network: LoRa gateway does not support rebuild network.

5.9.8 Import Data (This item will only be displayed for operator accounts.)

R206A doesn’t support this function.

5.9.9 System Settings

Enable https and timestamp, set cloud proxy server or MQTT

A. https

Enable/ Disable https

B. Timestamp authentication

The factory setting defaults that “Timestamp authentication” is selected. If the gateway time is incorrectly deviated by 10 minutes from the local time, the timestamp authentication will be timeout.

The factory setting defaults that timestamp authentication is 10 minutes. Namely, only if the time lag between the gateway time and the local time is within plus and minus 10 minutes, can the communication be normal.

C. Callback Authorization

The factory setting defaults that “Callback Authorization” is selected. Therefore, users do not need to modify it.

D. Cloud Connection

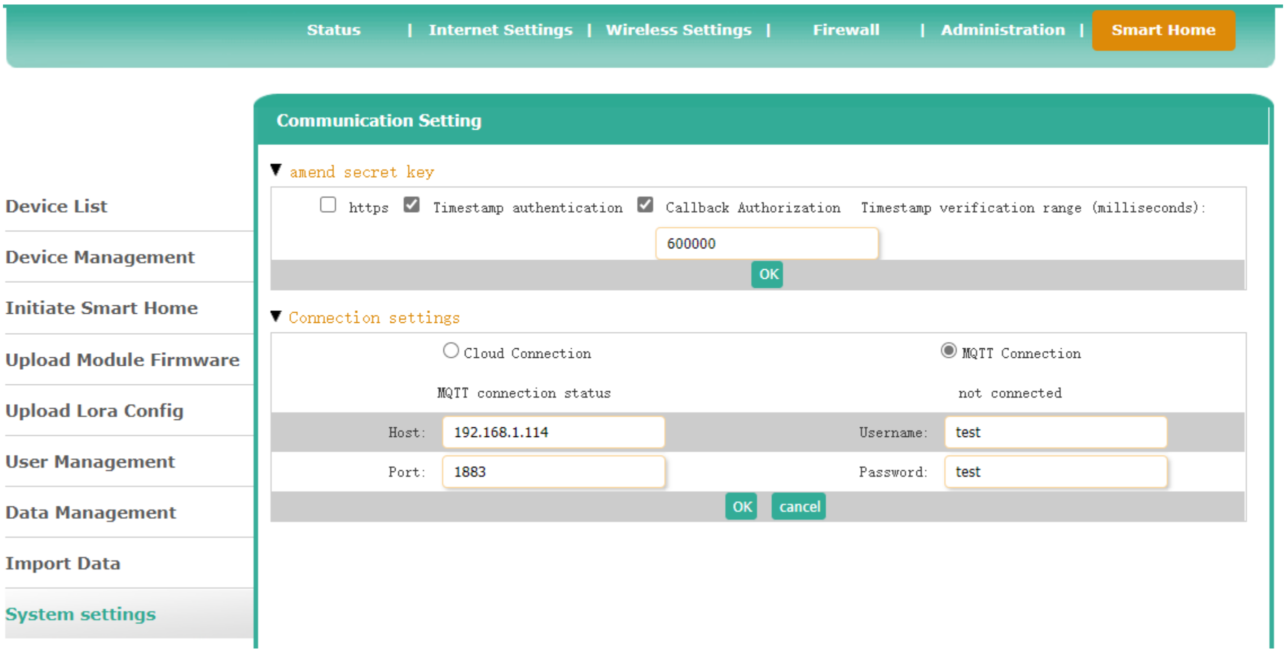
Default Cloud Address: mngm2.netvoxcloud.com:80

* Modifying to other URLs may cause the gateway to fail to connect to the cloud.

E. MQTT Connection

Please enter MQTT Host IP, Port, Username, and Password.

Note: MQTT messages are encrypted. The user needs to be authorized the GW REST API before using. For the related matters, please contact the sales executive.



Communication Setting

▼ amend secret key

☐ https ☑ Timestamp authentication ☑ Callback Authorization Timestamp verification range (milliseconds):

600000

OK

▼ Connection settings

○ Cloud Connection ● MQTT Connection

MQTT connection status not connected

Host: 192.168.1.114 Username: test

Port: 1883 Password: test

OK cancel

6. Related Product

R103 USB Dongle - Netvox Config Tool

7. Important Maintenance Instructions

Your device is a product of superior design and craftsmanship and should be used with care. The following suggestions will help you use the warranty service effectively.

- Keep the equipment dry. Rain, moisture, and various liquids or moisture may contain minerals that can corrode electronic circuits. In case the device is wet, please dry it completely.
- Do not use or store in dusty or dirty areas. This can damage its detachable parts and electronic components, destroy batteries, and deform or melt some plastic parts.
- Do not store in an excessive cold place. Otherwise, when the temperature rises to normal temperature, moisture will form inside, which will destroy the board.
- Do not throw, knock or shake the device. Rough handling of equipment can destroy internal circuit boards and delicate structures.
- Do not wash with strong chemicals, detergents or strong detergents.
- Do not apply with paint. Smudges can block debris in detachable parts and affect normal operation.
- Do not throw the battery into afire to prevent the battery from exploding. Damaged batteries may also explode.

All of the above suggestions apply equally to your device, battery and accessories. If any device is not working properly.

Please take it to the nearest authorized service facility for repair.