XT-2500AC

Access Controller User Manual

XonTel XT-2500AC
High Performance Gigabit AP Controller
CONSOLE
USB
LAN
100/1000/2500Mbps LAN/WAN
10G SFP LAN/WAN

Menu

1. Product Overview

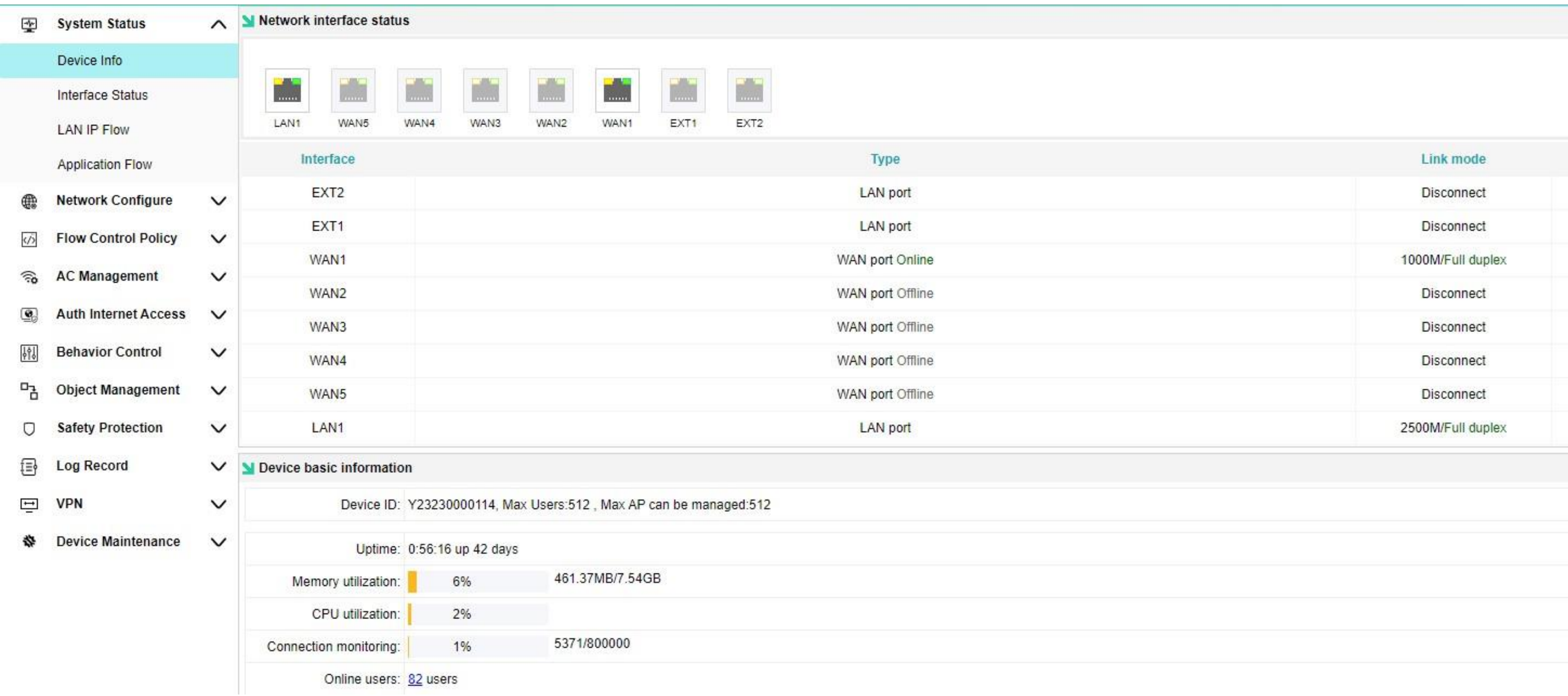
XonTel XT-2500AC is a multi-functional flow control gateway wireless control AC, which has the function of multi-line shunting and multi-line overlapping load balancing. It provides wireless data control services with large capacity, high performance, high reliability, easy installation and maintenance, and has the advantages of flexible networking, green energy conservation, etc.

2. WEB Login

2. 1. Power on gateway, when “Run” led blink regularly, connect computer to LAN port by ethernet cable.

2. 2. Visit default LAN IP **172.16.0.1:2011** in browser, default username & password are both: **admin**

Main page after login successfully:



Network interface status

Interface	Type	Link mode
EXT2	LAN port	Disconnect
EXT1	LAN port	Disconnect
WAN1	WAN port Online	1000M/Full duplex
WAN2	WAN port Offline	Disconnect
WAN3	WAN port Offline	Disconnect
WAN4	WAN port Offline	Disconnect
WAN5	WAN port Offline	Disconnect
LAN1	LAN port	2500M/Full duplex

Device basic information

Device ID: Y23230000114, Max Users:512 , Max AP can be managed:512

Uptime: 0:56:16 up 42 days

Memory utilization: 6% 461.37MB/7.54GB

CPU utilization: 2%

Connection monitoring: 1% 5371/800000

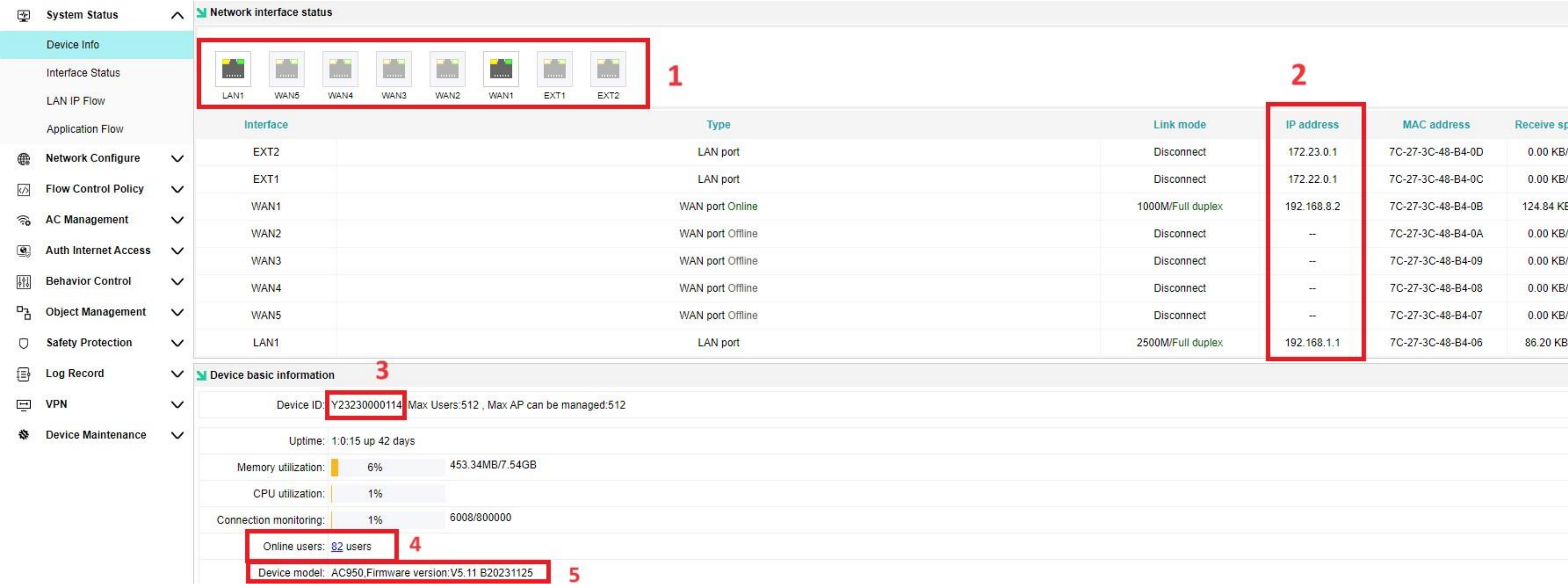
Online users: 82 users

3. Product Features

3. 1. System Status

Display a comprehensive information of the gateway, including the status of each interface, information of intranet clients, uplink and downlink, real-time uplink and downlink speed and total traffic of each application.

Device Info



Network interface status

Interface	Type	Link mode	IP address	MAC address	Receive sp
EXT2	LAN port	Disconnect	172.23.0.1	7C-27-3C-48-B4-0D	0.00 KB/
EXT1	LAN port	Disconnect	172.22.0.1	7C-27-3C-48-B4-0C	0.00 KB/
WAN1	WAN port Online	1000M/Full duplex	192.168.8.2	7C-27-3C-48-B4-0B	124.84 KB
WAN2	WAN port Offline	Disconnect	--	7C-27-3C-48-B4-0A	0.00 KB/
WAN3	WAN port Offline	Disconnect	--	7C-27-3C-48-B4-09	0.00 KB/
WAN4	WAN port Offline	Disconnect	--	7C-27-3C-48-B4-08	0.00 KB/
WAN5	WAN port Offline	Disconnect	--	7C-27-3C-48-B4-07	0.00 KB/
LAN1	LAN port	2500M/Full duplex	192.168.1.1	7C-27-3C-48-B4-06	86.20 KB

Device basic information

Device ID: Y23230000114 Max Users:512 , Max AP can be managed:512

Uptime: 1:0:15 up 42 days

Memory utilization: 6% 453.34MB/7.54GB

CPU utilization: 1%

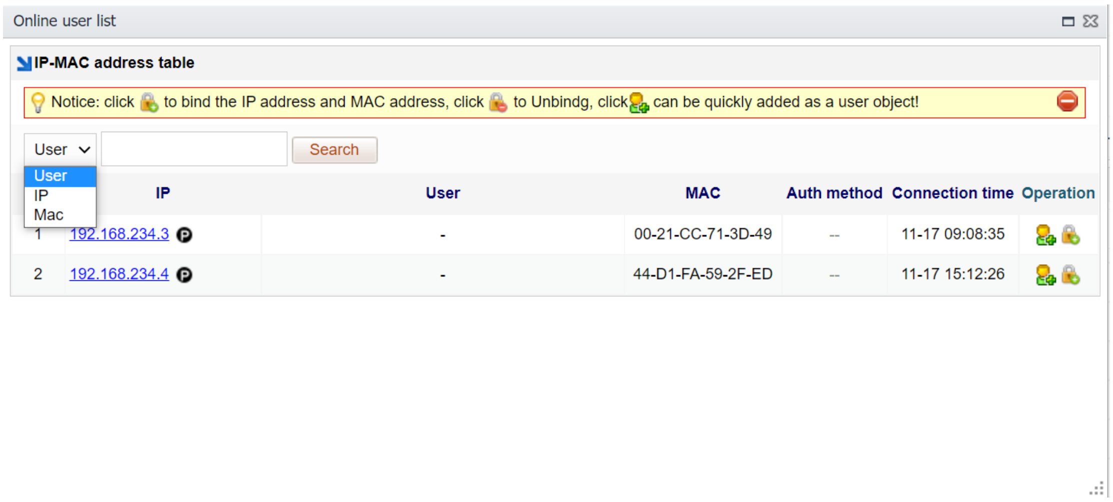
Connection monitoring: 1% 6008/800000

Online users: 82 users

Device model: AC950,Firmware version:V5.11 B20231125

SN 1: Display the physical connection of the interface, and the color icon represents connected
SN 2: Display interface IP address
SN 3: Device unique ID, used for remote access
SN 4: User quantity (AP quantity is excluded)
SN 5: Device model name

Click online users to filter AP and terminals according to three types of users, IP and MAC addresses, and view the corresponding relationship between IP and MAC.


Online user list

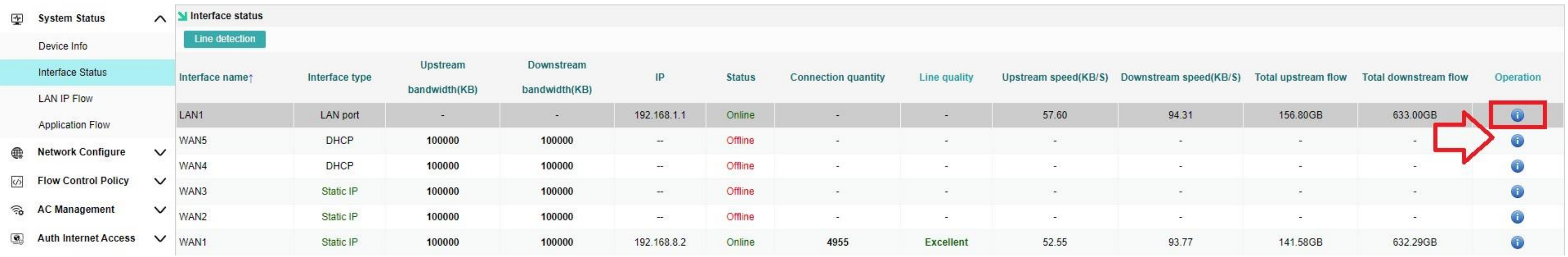
IP-MAC address table

Notice: click 🔒 to bind the IP address and MAC address, click 🔒 to Unbindg, click 👤 can be quickly added as a user object!

	IP	User	MAC	Auth method	Connection time	Operation
1	192.168.234.3	-	00-21-CC-71-3D-49	--	11-17 09:08:35	
2	192.168.234.4	-	44-D1-FA-59-2F-ED	--	11-17 15:12:26	

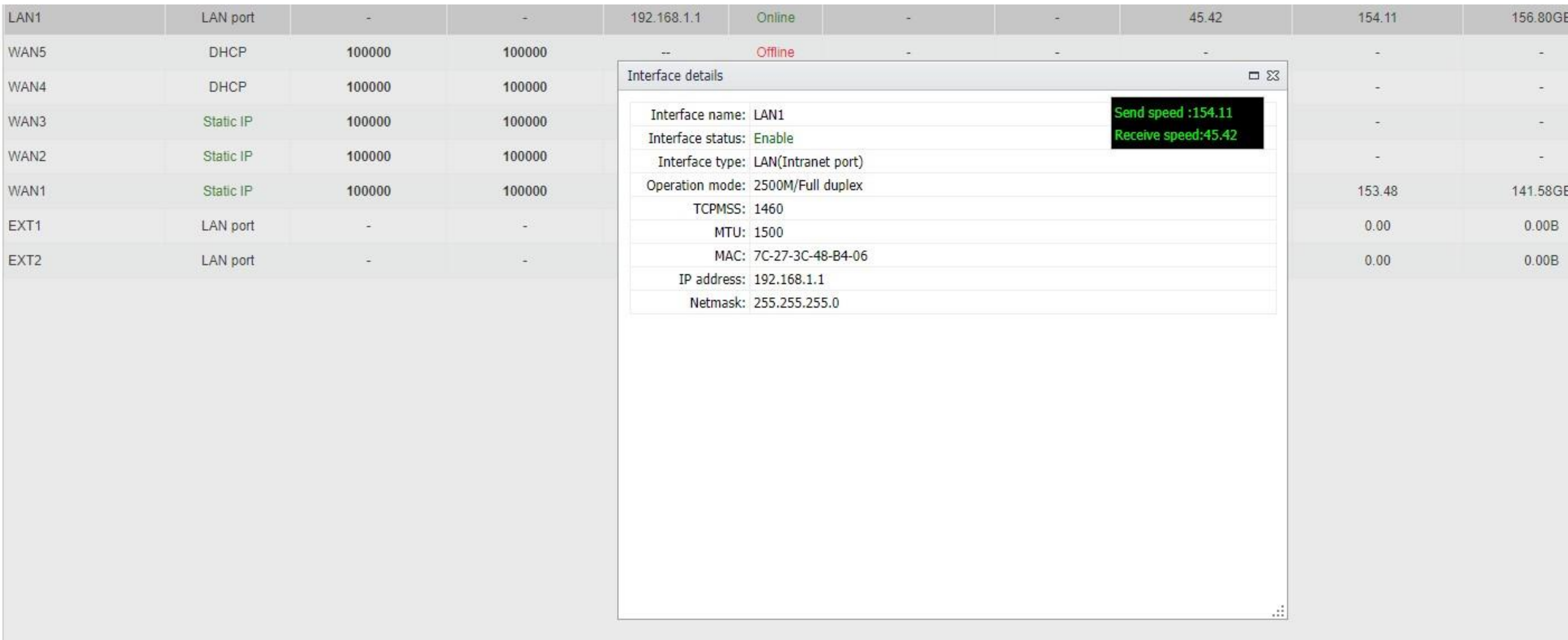
Interface Status

Check the comprehensive information of current interfaces.
SN 1: View interface details and WAN port speed.



Interface status

Interface name↑	Interface type	Upstream bandwidth(KB)	Downstream bandwidth(KB)	IP	Status	Connection quantity	Line quality	Upstream speed(KB/S)	Downstream speed(KB/S)	Total upstream flow	Total downstream flow	Operation
LAN1	LAN port	-	-	192.168.1.1	Online	-	-	57.60	94.31	156.80GB	633.00GB	ⓘ
WAN5	DHCP	100000	100000	--	Offline	-	-	-	-	-	-	ⓘ
WAN4	DHCP	100000	100000	--	Offline	-	-	-	-	-	-	ⓘ
WAN3	Static IP	100000	100000	--	Offline	-	-	-	-	-	-	ⓘ
WAN2	Static IP	100000	100000	--	Offline	-	-	-	-	-	-	ⓘ
WAN1	Static IP	100000	100000	192.168.8.2	Online	4955	Excellent	52.55	93.77	141.58GB	632.29GB	ⓘ


LAN1	LAN port	-	-	192.168.1.1	Online	-	-	45.42	154.11	156.80G
WAN5	DHCP	100000	100000	--	Offline	-	-	-	-	-
WAN4	DHCP	100000	100000						-	-
WAN3	Static IP	100000	100000						-	-
WAN2	Static IP	100000	100000						-	-
WAN1	Static IP	100000	100000						153.48	141.58G
EXT1	LAN port	-	-						0.00	0.00B
EXT2	LAN port	-	-						0.00	0.00B

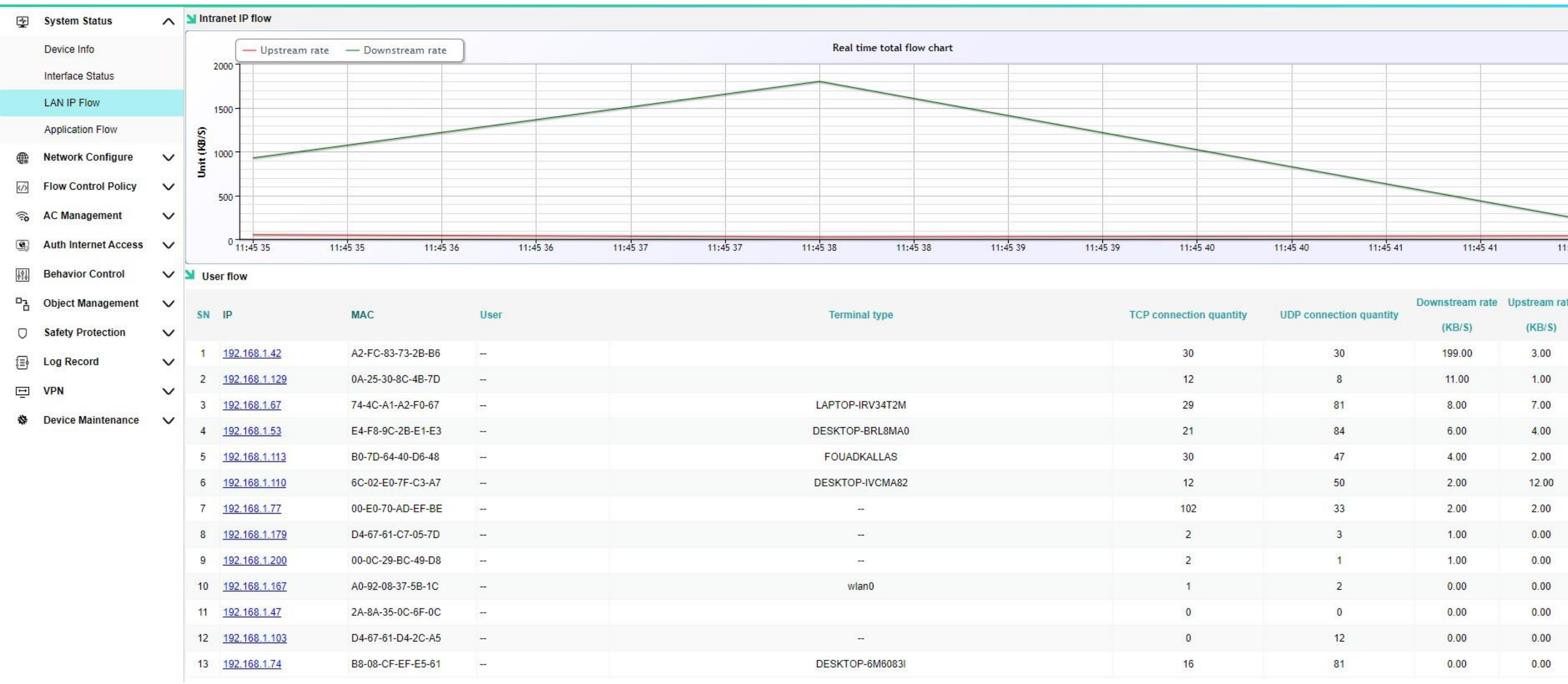
Interface details

Interface name: LAN1
Interface status: Enable
Interface type: LAN(Intranet port)
Operation mode: 2500M/Full duplex
TCPMSS: 1460
MTU: 1500
MAC: 7C-27-3C-48-B4-06
IP address: 192.168.1.1
Netmask: 255.255.255.0

Send speed :154.11
Receive speed:45.42

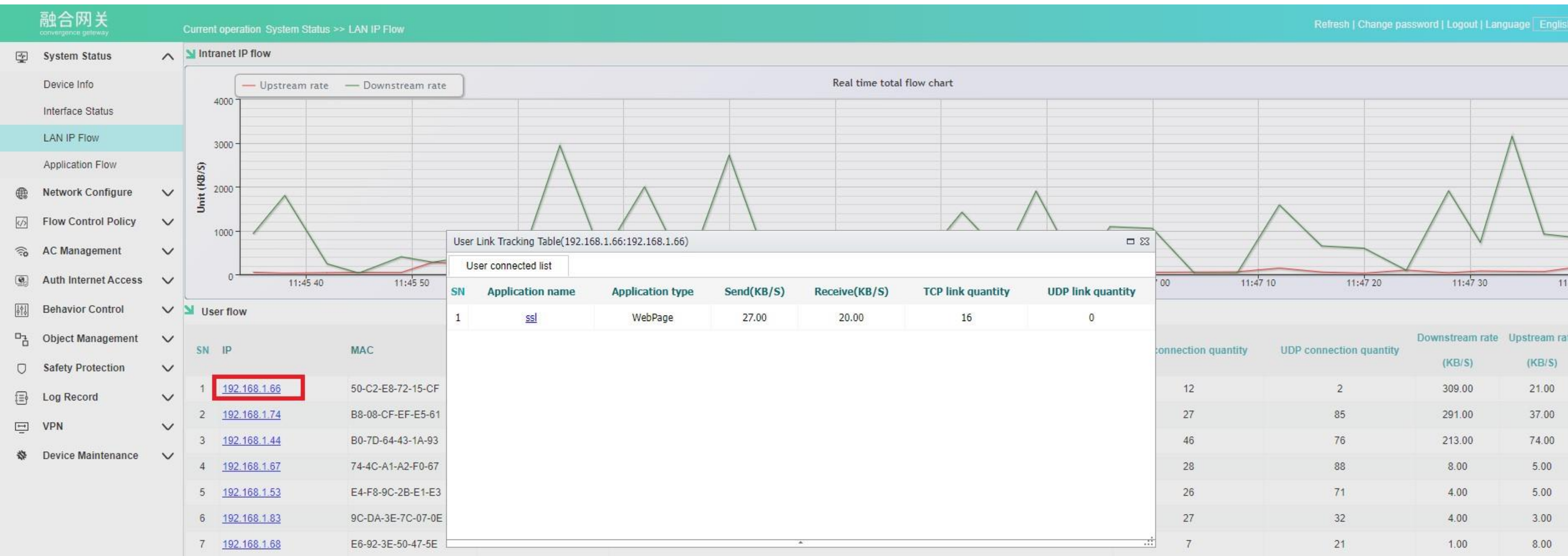
LAN IP Flow

View the traffic information independently used by each terminal of the intranet, as well as the link tracking table.



SN	IP	MAC	User	Terminal type	TCP connection quantity	UDP connection quantity	Downstream rate (KB/S)	Upstream rat (KB/S)
1	192.168.1.42	A2-FC-83-73-2B-B6	--		30	30	199.00	3.00
2	192.168.1.129	0A-25-30-8C-4B-7D	--		12	8	11.00	1.00
3	192.168.1.67	74-4C-A1-A2-F0-67	--	LAPTOP-IRV34T2M	29	81	8.00	7.00
4	192.168.1.53	E4-F8-9C-2B-E1-E3	--	DESKTOP-BRL8MA0	21	84	6.00	4.00
5	192.168.1.113	B0-7D-64-40-D6-48	--	FOUADKALLAS	30	47	4.00	2.00
6	192.168.1.110	6C-02-E0-7F-C3-A7	--	DESKTOP-IVCMA82	12	50	2.00	12.00
7	192.168.1.77	00-E0-70-AD-EF-BE	--	--	102	33	2.00	2.00
8	192.168.1.179	D4-67-61-C7-05-7D	--	--	2	3	1.00	0.00
9	192.168.1.200	00-0C-29-BC-49-D8	--	--	2	1	1.00	0.00
10	192.168.1.167	A0-92-08-37-5B-1C	--	wlan0	1	2	0.00	0.00
11	192.168.1.47	2A-8A-35-0C-6F-0C	--		0	0	0.00	0.00
12	192.168.1.103	D4-67-61-D4-2C-A5	--	--	0	12	0.00	0.00
13	192.168.1.74	B8-08-CF-EF-E5-61	--	DESKTOP-6M6083I	16	81	0.00	0.00

View the traffic type, speed, and number of protocol connections of selected user.



User Link Tracking Table(192.168.1.66:192.168.1.66)

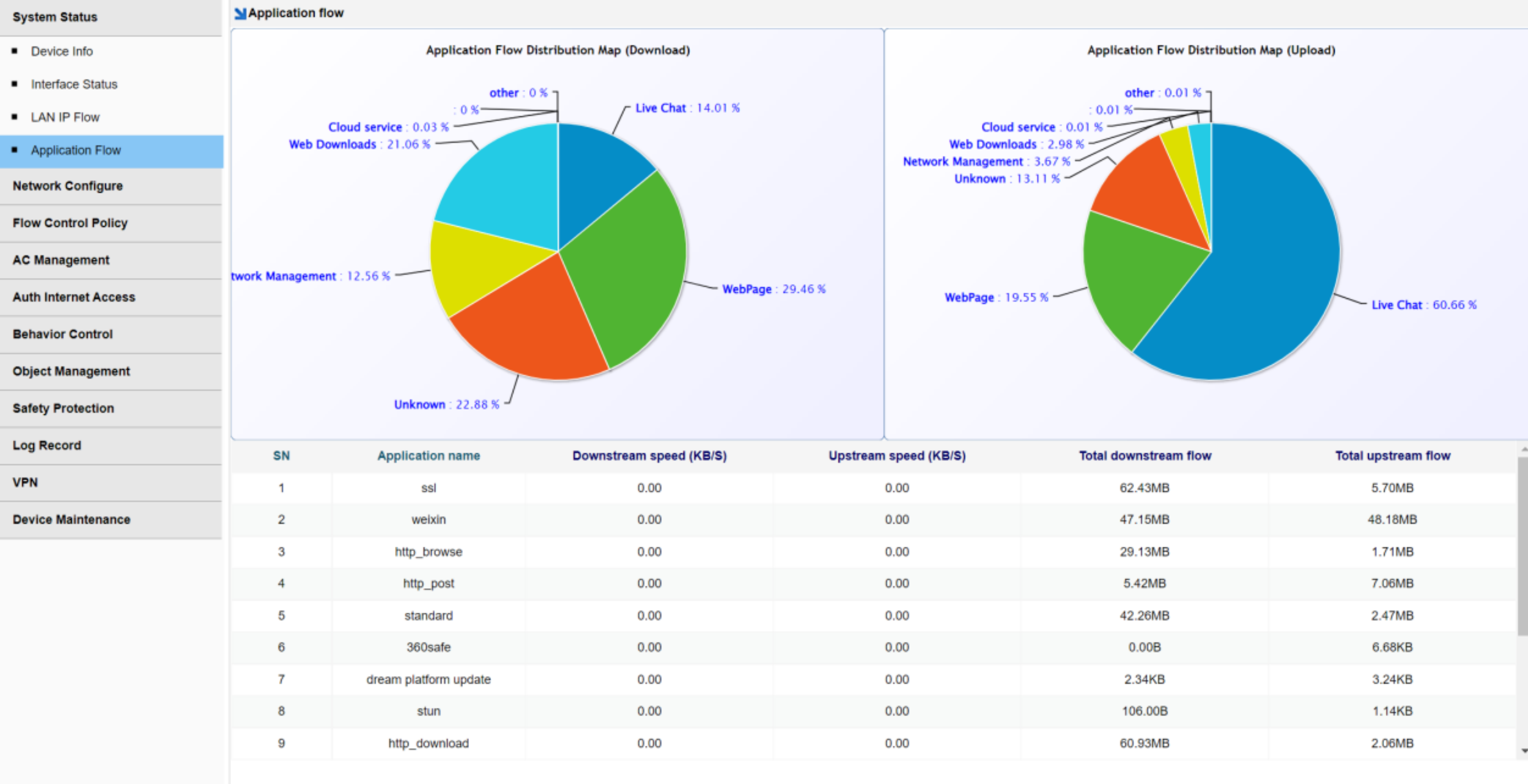
User connected list

SN	Application name	Application type	Send(KB/S)	Receive(KB/S)	TCP link quantity	UDP link quantity
1	ssl	WebPage	27.00	20.00	16	0

SN	IP	MAC	onnection quantity	UDP connection quantity	Downstream rate (KB/S)	Upstream ra (KB/S)
1	192.168.1.66	50-C2-E8-72-15-CF	12	2	309.00	21.00
2	192.168.1.74	B8-08-CF-EF-E5-61	27	85	291.00	37.00
3	192.168.1.44	B0-7D-64-43-1A-93	46	76	213.00	74.00
4	192.168.1.67	74-4C-A1-A2-F0-67	28	88	8.00	5.00
5	192.168.1.53	E4-F8-9C-2B-E1-E3	26	71	4.00	5.00
6	192.168.1.83	9C-DA-3E-7C-07-0E	27	32	4.00	3.00
7	192.168.1.68	E6-92-3E-50-47-5E	7	21	1.00	8.00

Application Flow

View the proportion of download and upload traffic.

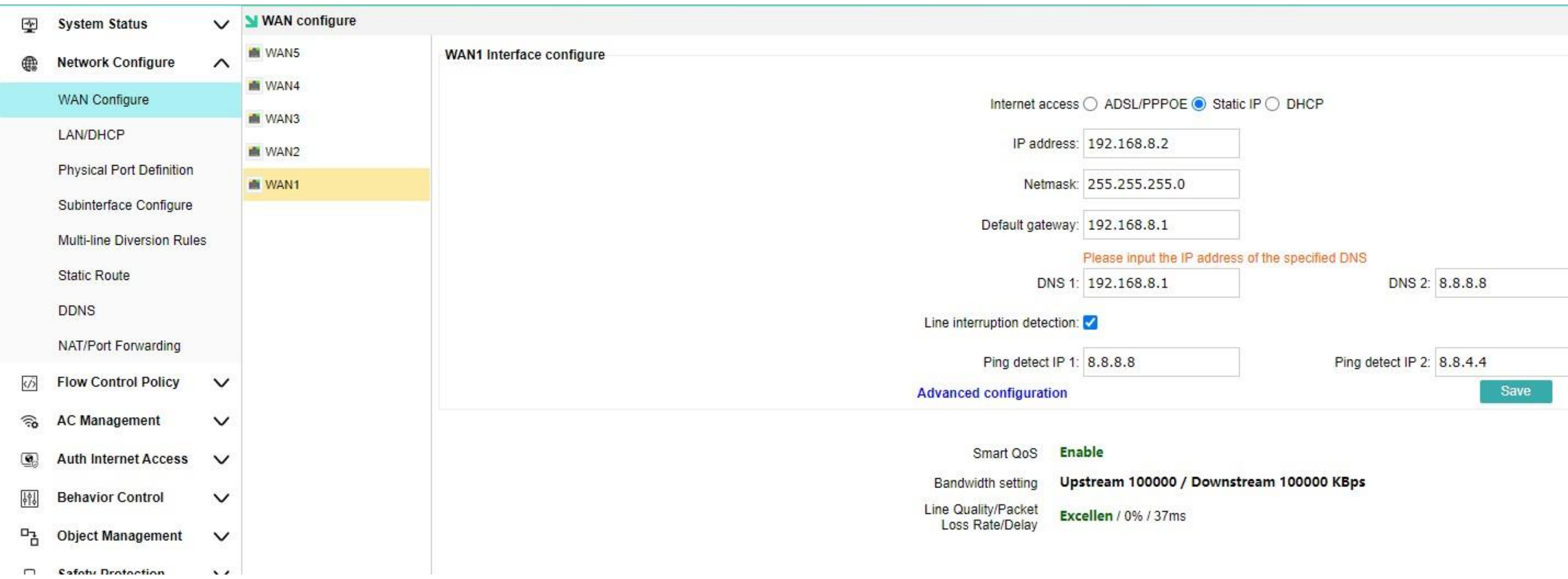


SN	Application name	Downstream speed (KB/S)	Upstream speed (KB/S)	Total downstream flow	Total upstream flow
1	ssl	0.00	0.00	62.43MB	5.70MB
2	weixin	0.00	0.00	47.15MB	48.18MB
3	http_browse	0.00	0.00	29.13MB	1.71MB
4	http_post	0.00	0.00	5.42MB	7.06MB
5	standard	0.00	0.00	42.26MB	2.47MB
6	360safe	0.00	0.00	0.00B	6.68KB
7	dream platform update	0.00	0.00	2.34KB	3.24KB
8	stun	0.00	0.00	106.00B	1.14KB
9	http_download	0.00	0.00	60.93MB	2.06MB

3. 2. Network Configure

Used to set the configuration information of the external network and the internal network, and the routing of the internal network.

WAN Configure



WAN1 Interface configure

Internet access ○ ADSL/PPPOE ● Static IP ○ DHCP

IP address: 192.168.8.2

Netmask: 255.255.255.0

Default gateway: 192.168.8.1

Please input the IP address of the specified DNS

DNS 1: 192.168.8.1 DNS 2: 8.8.8.8

Line interruption detection: ☑

Ping detect IP 1: 8.8.8.8 Ping detect IP 2: 8.8.4.4

Smart QoS Enable

Bandwidth setting Upstream 100000 / Downstream 100000 KBps

Line Quality/Packet Loss Rate/Delay Excellen / 0% / 37ms

Internet access-Select the Internet access mode according to the actual situation

- **ADSL/PPPOE**: Fill account and password supplied by operator
- **Static IP**: Fill IP, Netmask, Gateway, DNS supplied by operator
- **DHCP**: Directly insert the line provided by the operator to obtain the IP address.

Line interruption detection - Ping detection (Google, Facebook...). If the continuous ping fails, the delay is high, and there is no data interworking, it will be considered as a line exception. When the quality is poor, dial-up attempts to redial, DHCP attempts to retrieve, and fixed IP addresses are processed offline. Offline lines do not participate in the load. Multi line environment, it is recommended to enable line interruption detection, and automatic switching can only be performed when individual lines are offline.

Marks: If the operator prohibits ping, line detection cannot be enabled.
PING detection IP: 0.0.0.0 by default, which means the built-in IP (114DNS, Tencent official website, Alibaba DNS, Baidu DNS) is used for detection. If the local DNS can be pinged, or other public IP with lower latency can be pinged, it can be filled in as the detection basis.

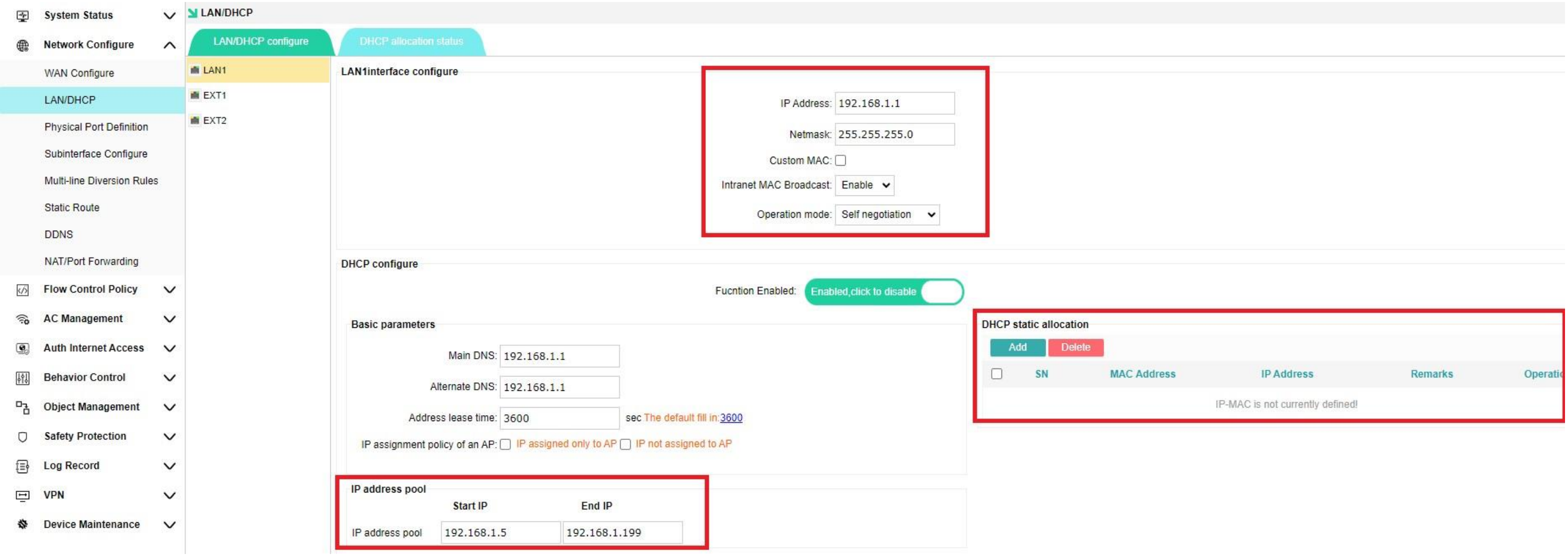
Tips: It is suggested that professional technicians should fill in the test IP after evaluation.

LAN/DHCP

SN 1: LAN1 IP address.

SN 2: IP address pool: IP address for users & APs managed by gateway. Can’t be same IP segment as obtained WAN IP address.

SN 3: DHCP, can manage banded IP and MAC.



LAN1interface configure

IP Address: 192.168.1.1
Netmask: 255.255.255.0
Custom MAC: □
Intranet MAC Broadcast: Enable
Operation mode: Self negotiation

DHCP configure

Fucntion Enabled: Enabled,click to disable

Basic parameters

Main DNS: 192.168.1.1
Alternate DNS: 192.168.1.1
Address lease time: 3600 sec The default fill in:3600
IP assignment policy of an AP: □ IP assigned only to AP □ IP not assigned to AP

IP address pool

	Start IP	End IP
IP address pool	192.168.1.5	192.168.1.199

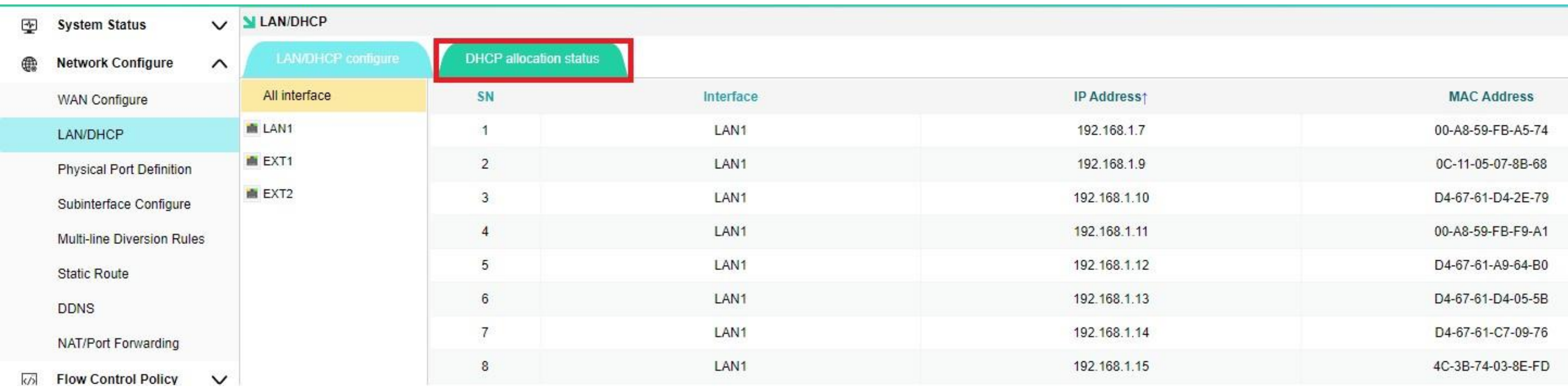
DHCP static allocation

Add Delete

□	SN	MAC Address	IP Address	Remarks	Operati

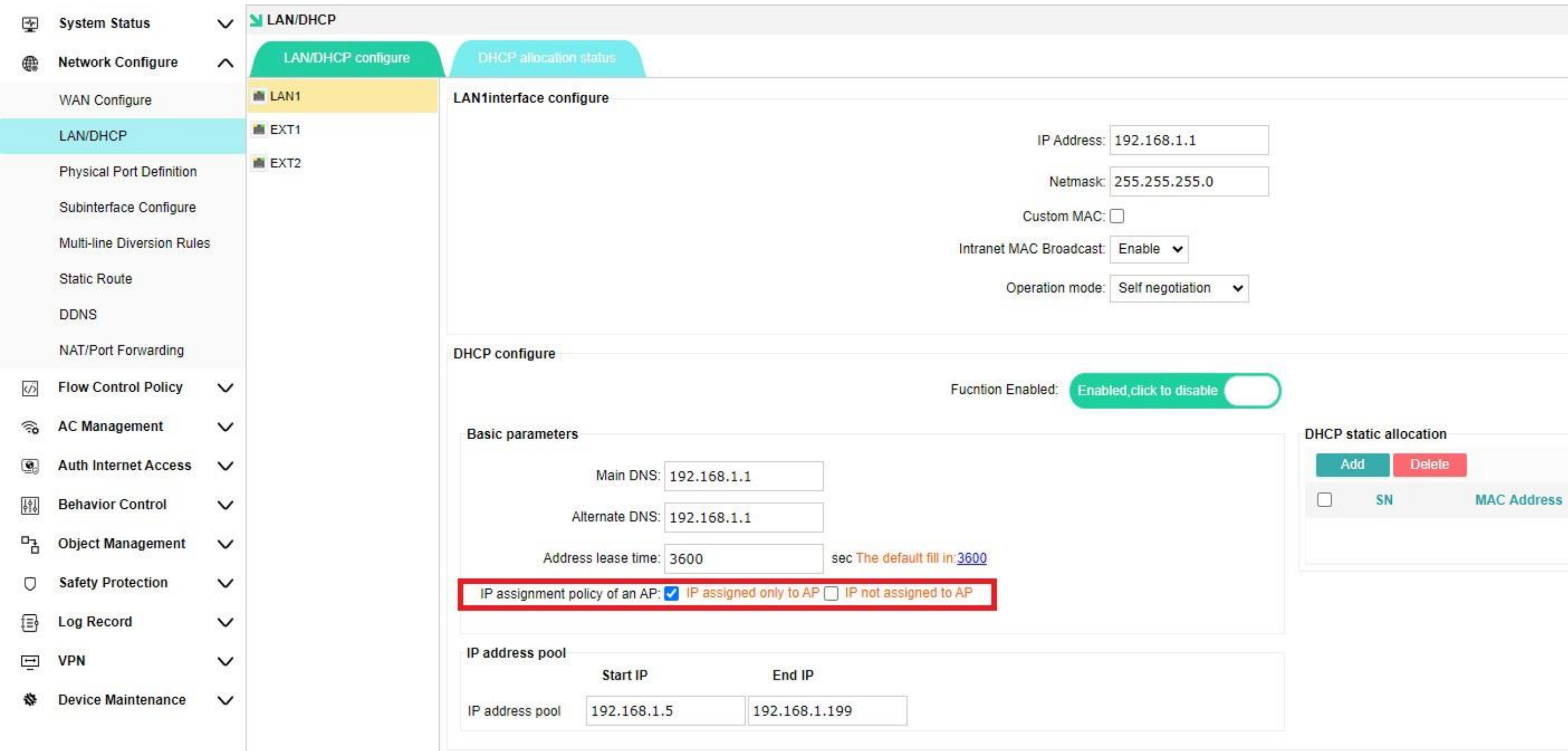
IP-MAC is not currently defined!

View DHCP allocation status



SN	Interface	IP Address↑	MAC Address
1	LAN1	192.168.1.7	00-A8-59-FB-A5-74
2	LAN1	192.168.1.9	0C-11-05-07-8B-68
3	LAN1	192.168.1.10	D4-67-61-D4-2E-79
4	LAN1	192.168.1.11	00-A8-59-FB-F9-A1
5	LAN1	192.168.1.12	D4-67-61-A9-64-B0
6	LAN1	192.168.1.13	D4-67-61-D4-05-5B
7	LAN1	192.168.1.14	D4-67-61-C7-09-76
8	LAN1	192.168.1.15	4C-3B-74-03-8E-FD

Markes: If gateway works as by pass mode, need to select “IP assigned only to AP”.



LAN1interface configure

IP Address: 192.168.1.1
Netmask: 255.255.255.0
Custom MAC: □
Intranet MAC Broadcast: Enable
Operation mode: Self negotiation

DHCP configure

Fucntion Enabled: Enabled,click to disable

Basic parameters

Main DNS: 192.168.1.1
Alternate DNS: 192.168.1.1
Address lease time: 3600 sec The default fill in:3600
IP assignment policy of an AP: ☑ IP assigned only to AP □ IP not assigned to AP

IP address pool

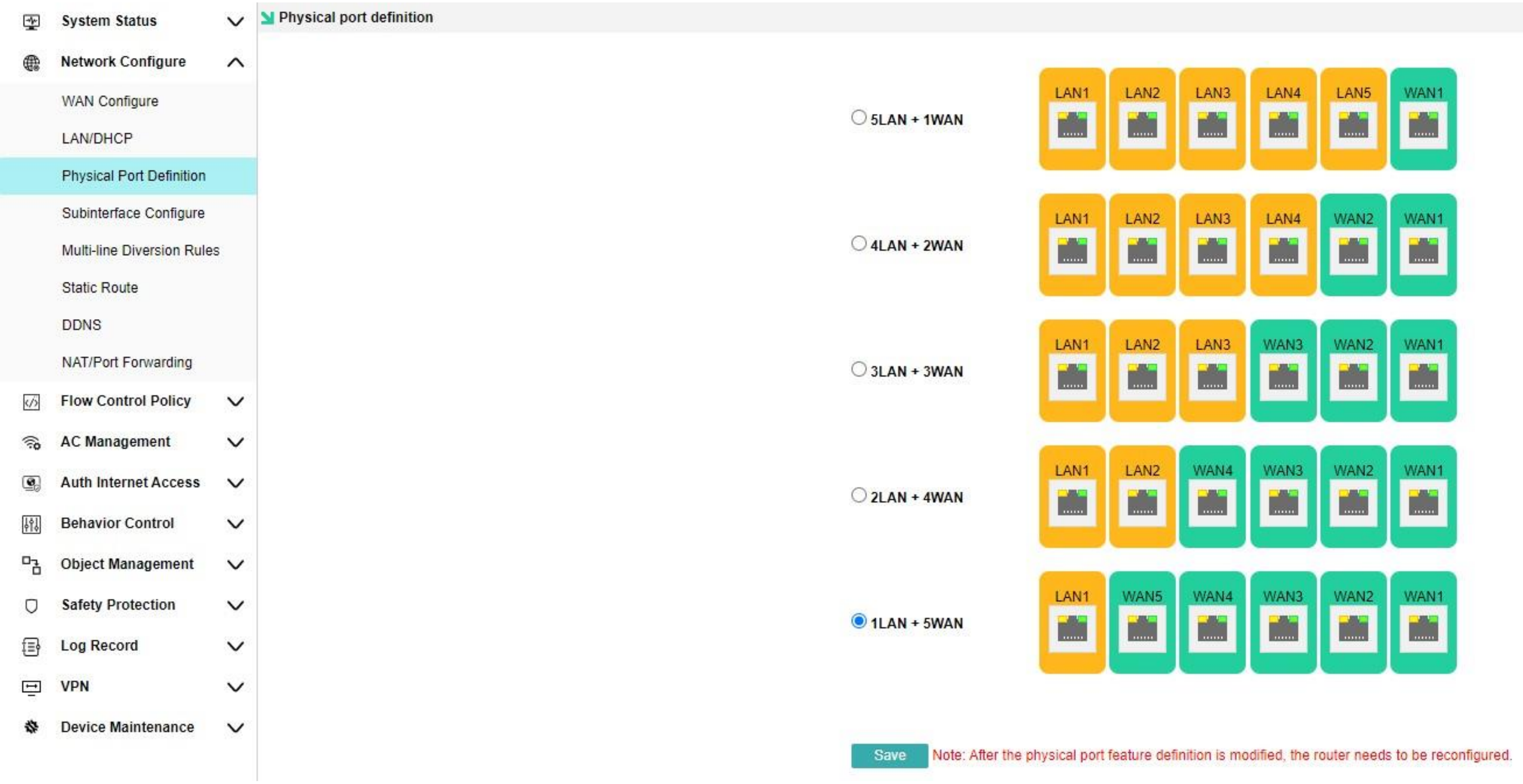
	Start IP	End IP
IP address pool	192.168.1.5	192.168.1.199

DHCP static allocation

□	SN	MAC Address

Physical Port Definition

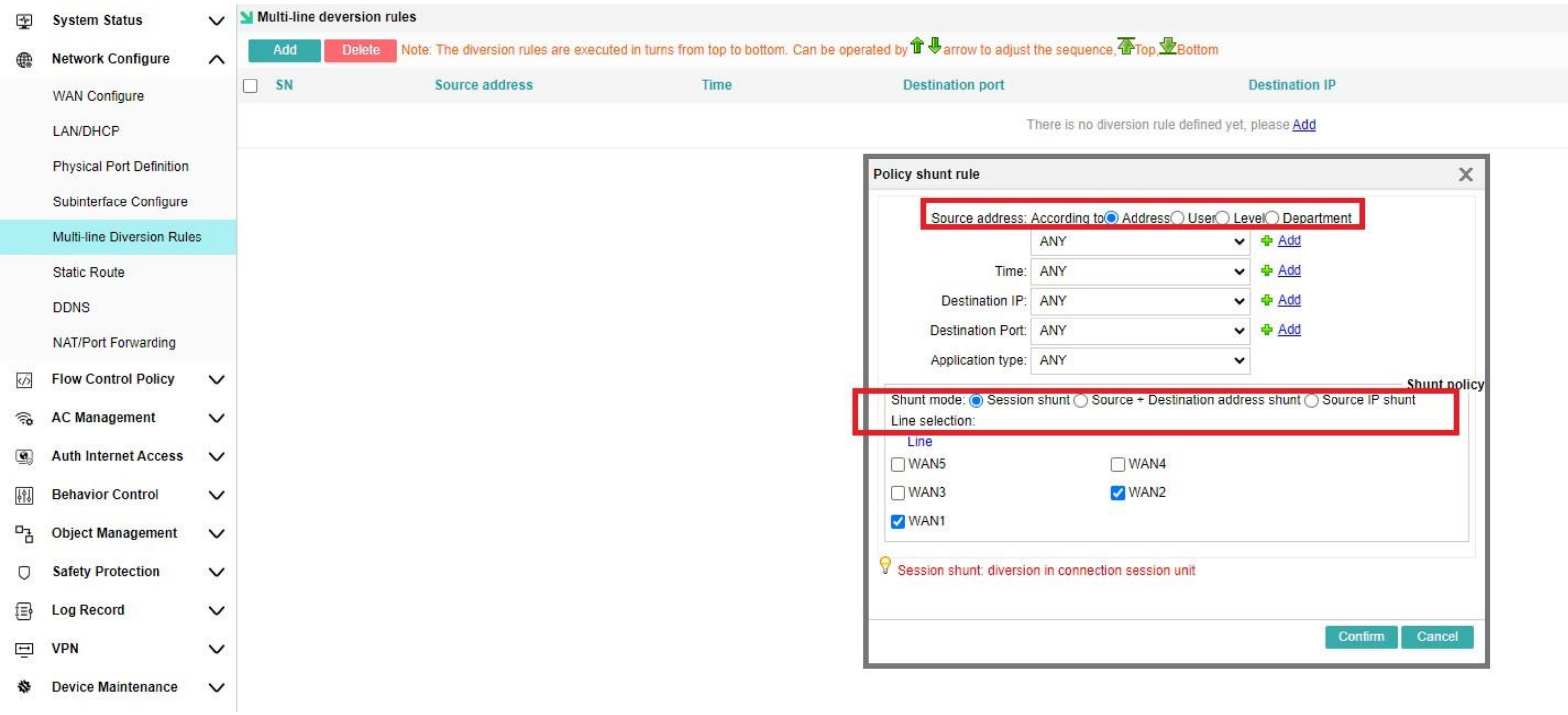
Divide multiple WAN ports and LAN ports according to requirements.



○ 5LAN + 1WAN	LAN1	LAN2	LAN3	LAN4	LAN5	WAN1
○ 4LAN + 2WAN	LAN1	LAN2	LAN3	LAN4	WAN2	WAN1
○ 3LAN + 3WAN	LAN1	LAN2	LAN3	WAN3	WAN2	WAN1
○ 2LAN + 4WAN	LAN1	LAN2	WAN4	WAN3	WAN2	WAN1
● 1LAN + 5WAN	LAN1	WAN5	WAN4	WAN3	WAN2	WAN1

Note: After the physical port feature definition is modified, the router needs to be reconfigured.

Multi-line Diversion Rules



Multi-line deversion rules

Note: The diversion rules are executed in turns from top to bottom. Can be operated by ⇧⇩ arrow to adjust the sequence, Top, Bottom

□ SN	Source address	Time	Destination port	Destination IP

There is no diversion rule defined yet, please Add

Policy shunt rule

Source address: According to ● Address ○ User ○ Level ○ Department
ANY Add
Time: ANY Add
Destination IP: ANY Add
Destination Port: ANY Add
Application type: ANY

Shunt policy
Shunt mode: ● Session shunt ○ Source + Destination address shunt ○ Source IP shunt
Line selection:
Line
□ WAN5 □ WAN4
□ WAN3 ☑ WAN2
☑ WAN1

Session shunt: diversion in connection session unit

Single line cannot be configured with shunting rules; When two or more WAN ports are connected to the external network, different source addresses and diversion modes can be selected for setting. There are three modes:

- Session shunt: Distribute all Internet connections to each line. For example, Jason started IDM downloading. Many concurrent links of IDM were distributed to three lines, and each line was connected to generate traffic, which was summarized to IDM, achieving the effect of bandwidth superposition。
- Source+Destination address shunt: On the basis of session shunting, determine that the source address and destination address are loaded onto each line. For example, Zhang San opened three websites at the same time, namely ICBC, Jingdong Mall and Taobao (for the purpose of explanation, it is considered that the IP addresses of these three websites are only A, B and C). Use source+destination address diffluence to divert all users to three external networks. The final effect is: Zhang San's ICBC fixed line 1; Jingdong Mall fixed line 2, Taobao fixed line 3.

- Source IP shunt: It is always shunted on one line according to the source address. Taking the environment of 3 extranets and 9 people online as an example, IP shunts all people to 3 extranets. The result is: Zhang San fixed line 1; Li Si fixed route 2; Wang Wu fixed route 3; Zhao Liu fixed the first route, apportioning the 9 people on 3 lines in turn. Since everyone is fixed on a line, the speed of Internet access is limited by the bandwidth of the line.

Weight: weight can be understood as "proportion", which is only effective for IP shunting. Taking the environment where 12 people access the Internet in 3 extranets as an example, IP shunting owners are shunted to 3 extranets, with line 1 weighting 3, line 2 weighting 2, and line 3 weighting 1. As a result, 6 people will be awarded for line 1, 4 for line 2, and 2 for line 1.

(The weight is the proportion. For example, the weight of the three lines is 4, 2, 1, and the effect is 4:2:1)

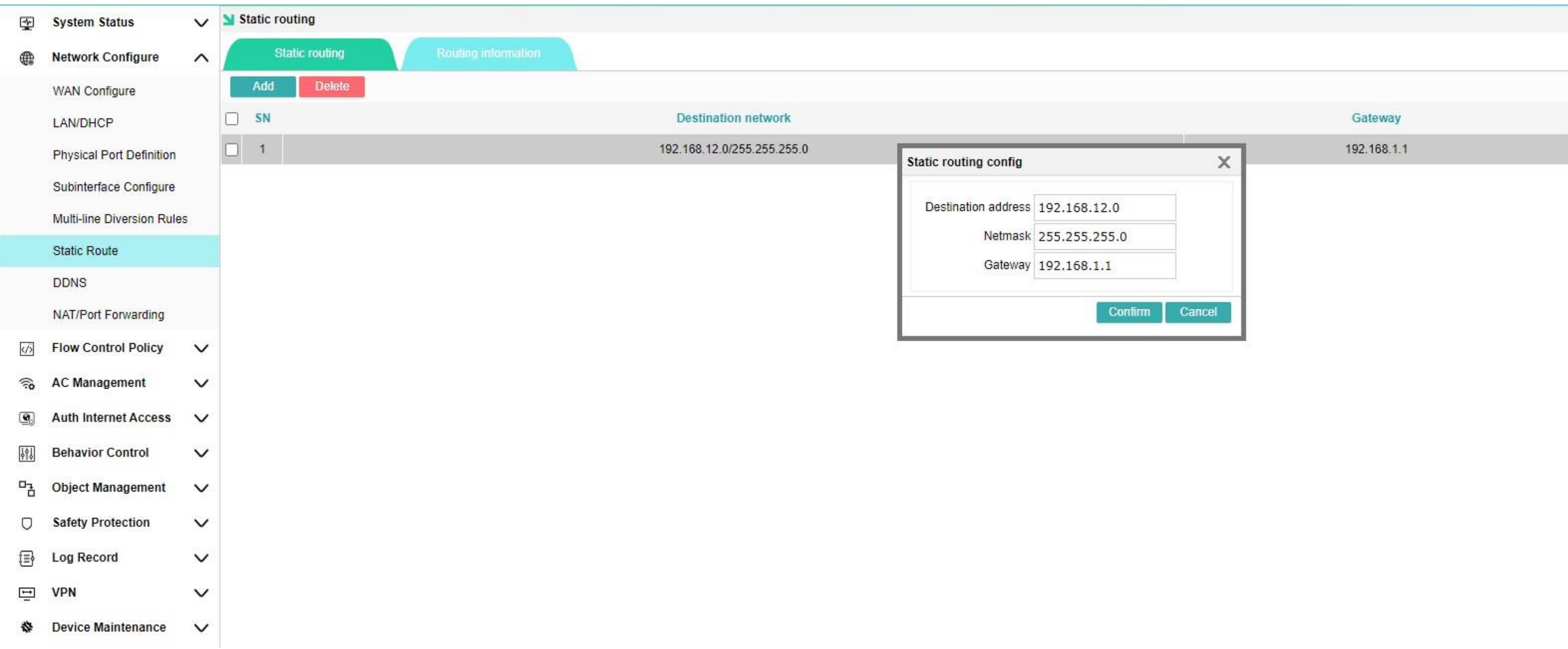
Conclusion: IP shunting is applicable to the condition that there are a lot of lines, so as to reduce the IP of WAN ports being consumed by multiple people at the same time and improve the utilization of IP. It is mainly used to do Taobao in the community broadband, and Amazon e-commerce users are also used in some game studios (because too many people access from a WAN port, e-commerce may regard it as a swipe and hang up).

Session shunt is applicable to streaming multi-threaded download services that require extreme streaming, such as streaming P2P downloads and game update servers.

Source+Destination address shunt, is recommended by default to achieve better compatibility on the basis of session splitting.

Static Route

Generally, when using the private network, it is required to set the terminal to access the corresponding IP segment and forward it to the corresponding gateway.

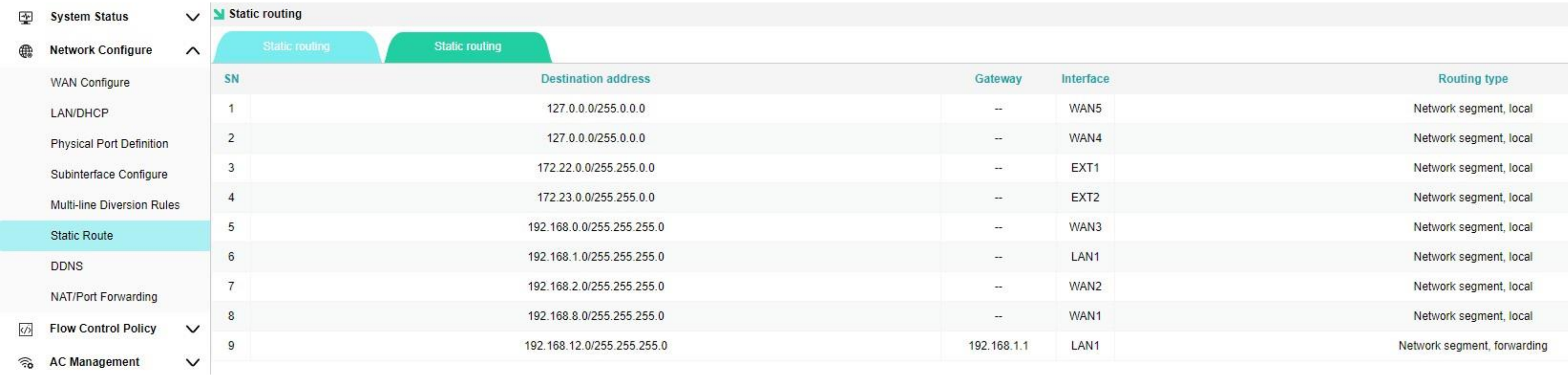


□	SN	Destination network	Gateway
□	1	192.168.12.0/255.255.255.0	192.168.1.1

Static routing config

Destination address 192.168.12.0
Netmask 255.255.255.0
Gateway 192.168.1.1

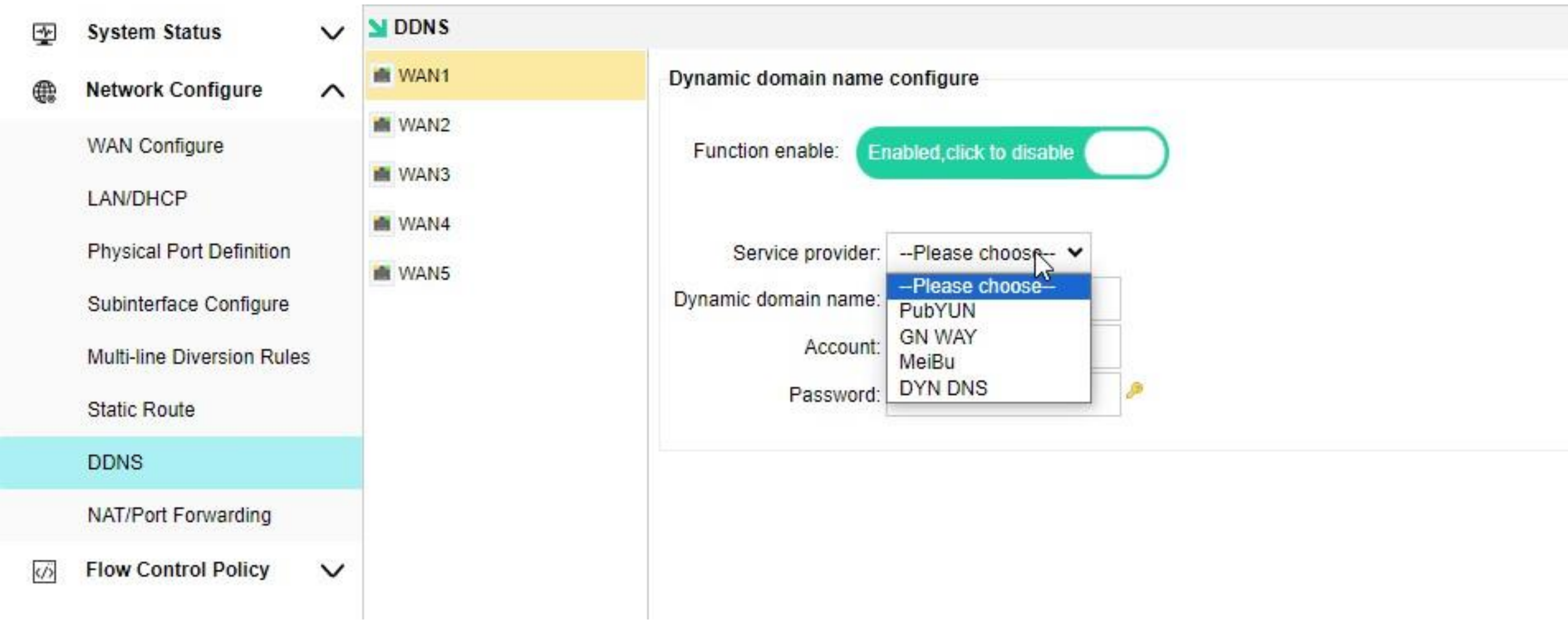
Check static routing form



SN	Destination address	Gateway	Interface	Routing type
1	127.0.0.0/255.0.0.0	--	WAN5	Network segment, local
2	127.0.0.0/255.0.0.0	--	WAN4	Network segment, local
3	172.22.0.0/255.255.0.0	--	EXT1	Network segment, local
4	172.23.0.0/255.255.0.0	--	EXT2	Network segment, local
5	192.168.0.0/255.255.255.0	--	WAN3	Network segment, local
6	192.168.1.0/255.255.255.0	--	LAN1	Network segment, local
7	192.168.2.0/255.255.255.0	--	WAN2	Network segment, local
8	192.168.8.0/255.255.255.0	--	WAN1	Network segment, local
9	192.168.12.0/255.255.255.0	192.168.1.1	LAN1	Network segment, forwarding

DDNS

The route is managed from the external network, that is, the dynamic domain name is accessed through the dynamic domain name, which is mainly provided by the dynamic domain name service provider.



Dynamic domain name configure

Function enable: Enabled,click to disable

Service provider: --Please choose--

Dynamic domain name:

Account:

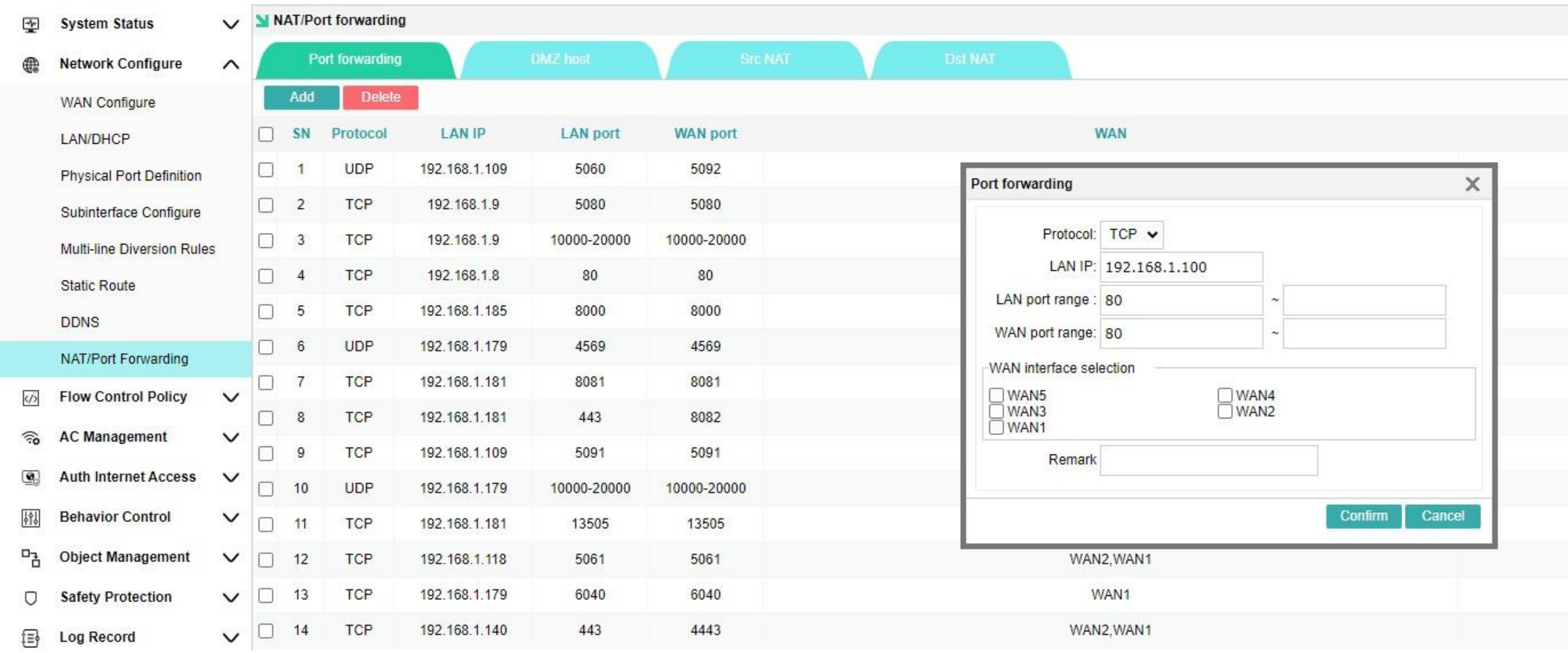
Password:

Marks:

1, Routing is only for IP reporting. The correctness and speed of the resolution depend on the 3322 service provider.
2, Some operators allocate the Internet access IP as a LAN IP, such as 10.10.99.99, which is a LAN IP and cannot be accessed by the external network. If it is a LAN IP, it is useless to configure a dynamic domain name.

NAT/Port Forwarding

Used to map LAN ports to the public network



□	SN	Protocol	LAN IP	LAN port	WAN port	WAN
□	1	UDP	192.168.1.109	5060	5092	
□	2	TCP	192.168.1.9	5080	5080	
□	3	TCP	192.168.1.9	10000-20000	10000-20000	
□	4	TCP	192.168.1.8	80	80	
□	5	TCP	192.168.1.185	8000	8000	
□	6	UDP	192.168.1.179	4569	4569	
□	7	TCP	192.168.1.181	8081	8081	
□	8	TCP	192.168.1.181	443	8082	
□	9	TCP	192.168.1.109	5091	5091	
□	10	UDP	192.168.1.179	10000-20000	10000-20000	
□	11	TCP	192.168.1.181	13505	13505	
□	12	TCP	192.168.1.118	5061	5061	WAN2,WAN1
□	13	TCP	192.168.1.179	6040	6040	WAN1
□	14	TCP	192.168.1.140	443	4443	WAN2,WAN1

Port forwarding ✕

Protocol: TCP

LAN IP: 192.168.1.100

LAN port range : 80 ~

WAN port range: 80 ~

WAN interface selection

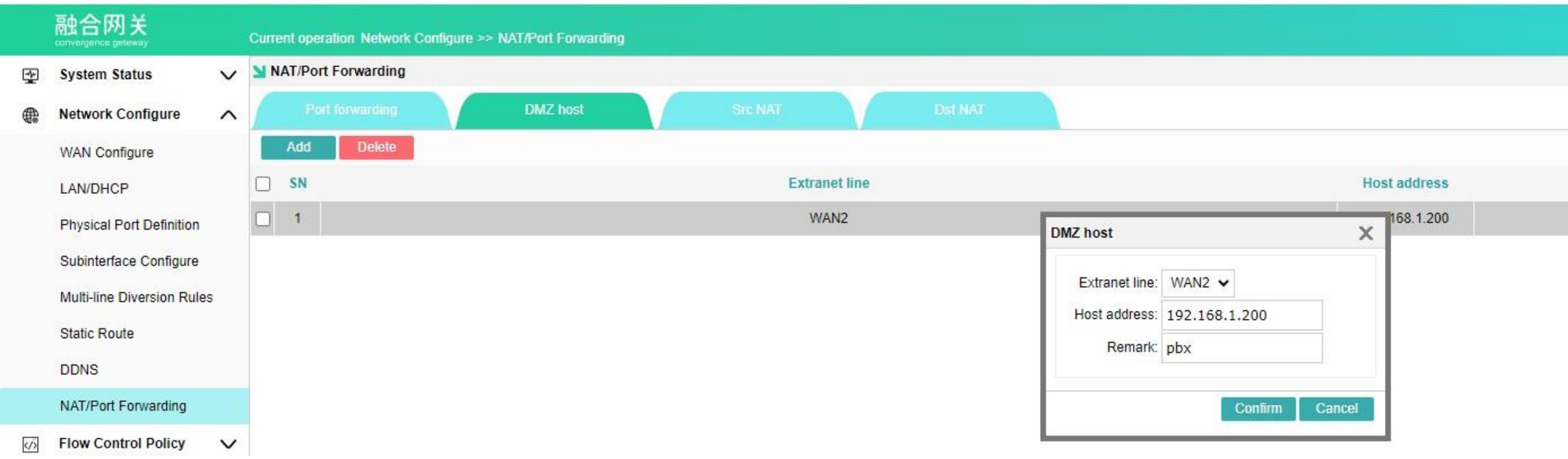
□ WAN5 □ WAN4
□ WAN3 □ WAN2
□ WAN1

Remark

Confirm Cancel

DMZ Host

To solve the problem that the external network cannot access the internal network server after the firewall is installed, click to open the DMZ host, and manually fill in the address and external network port to confirm that this function takes effect.



□	SN	Extranet line	Host address
□	1	WAN2	168.1.200

DMZ host ✕

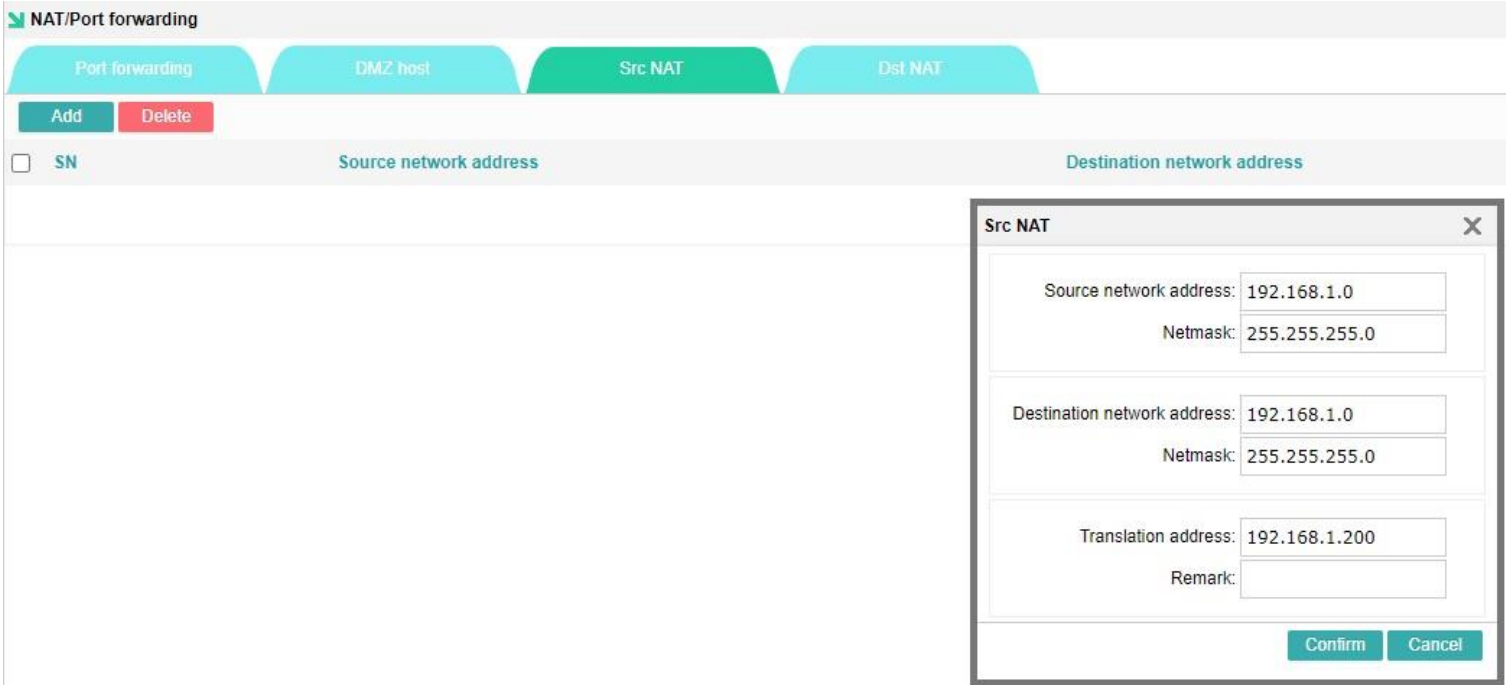
Extranet line: WAN2

Host address: 192.168.1.200

Remark: pbx

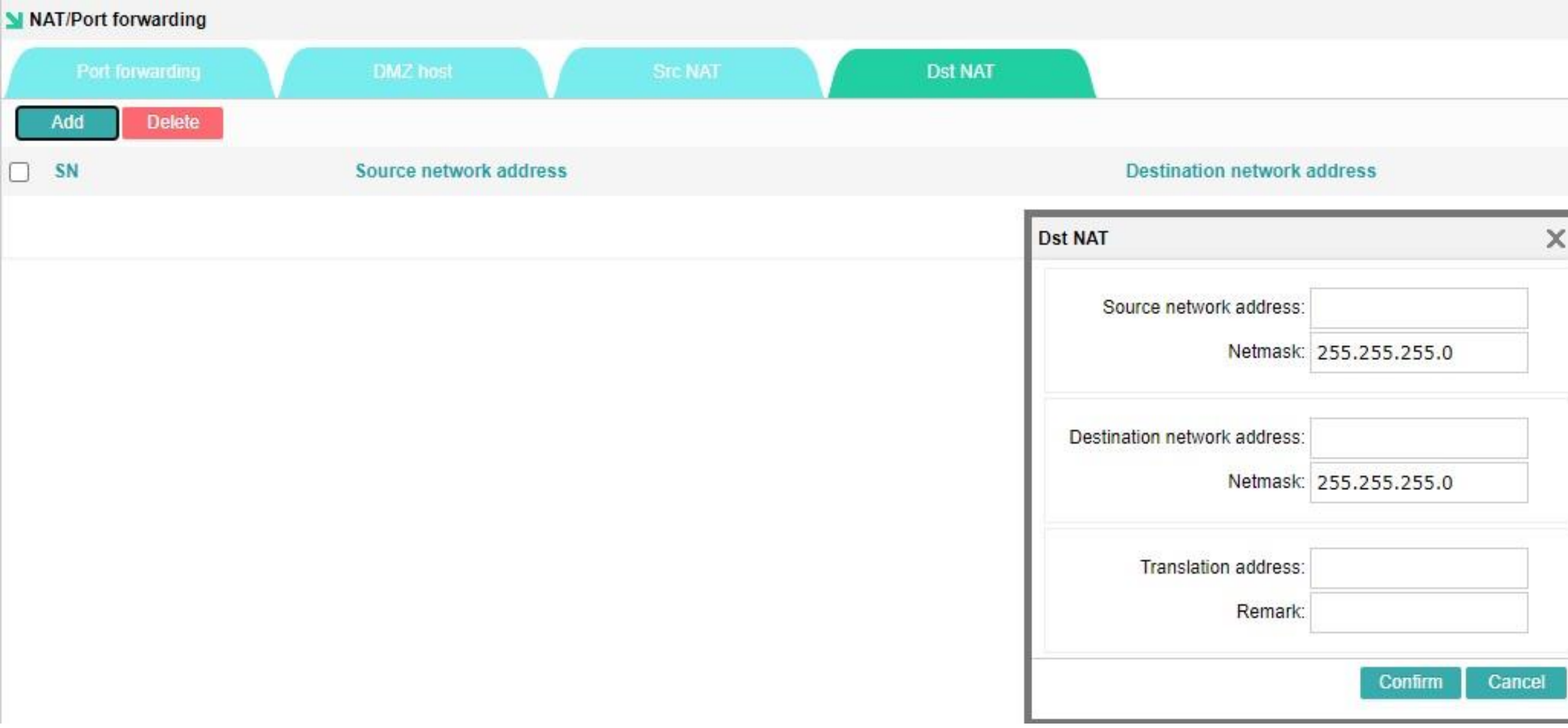
Confirm Cancel

Src NAT



Source network address: 192.168.1.0
Netmask: 255.255.255.0
Destination network address: 192.168.1.0
Netmask: 255.255.255.0
Translation address: 192.168.1.200
Remark:

Dst NAT

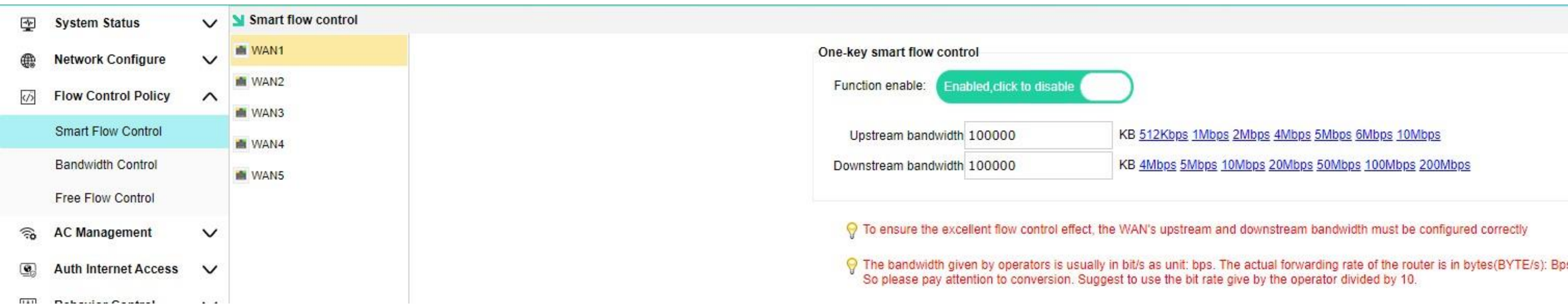


Source network address:
Netmask: 255.255.255.0
Destination network address:
Netmask: 255.255.255.0
Translation address:
Remark:

3. 3. Flow Control Policy

Manage the network speed of the terminal, and implement average bandwidth allocation or limit the bandwidth of the terminal.

Smart Flow Control



One-key smart flow control

Function enable: Enabled,click to disable

Upstream bandwidth 100000 KB 512Kbps 1Mbps 2Mbps 4Mbps 5Mbps 6Mbps 10Mbps

Downstream bandwidth 100000 KB 4Mbps 5Mbps 10Mbps 20Mbps 50Mbps 100Mbps 200Mbps

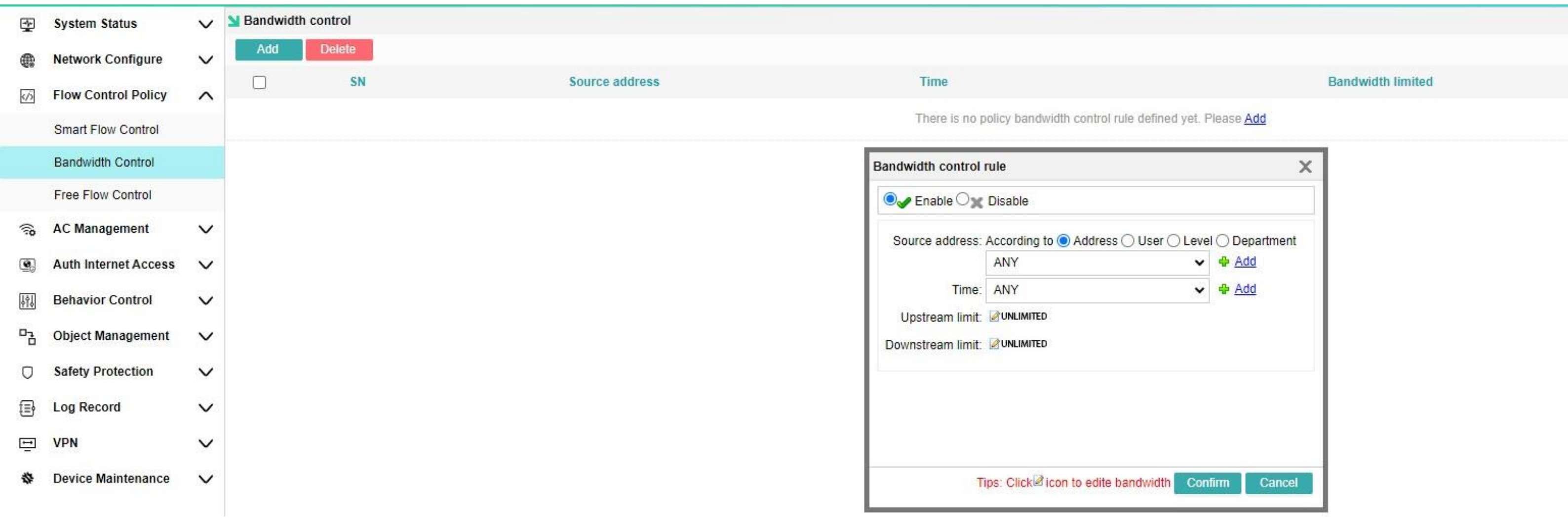
To ensure the excellent flow control effect, the WAN's upstream and downstream bandwidth must be configured correctly

The bandwidth given by operators is usually in bit/s as unit: bps. The actual forwarding rate of the router is in bytes(BYTE/s): Bps
So please pay attention to conversion. Suggest to use the bit rate give by the operator divided by 10.

For example, the uplink 20M and downlink 100M dial-up optical fiber can be configured with an uplink capacity of 2000KB and a downlink capacity of 10000KB. It is very important to configure the line bandwidth. The intelligent flow control automatically limits the speed according to the configured bandwidth. (You need to check the "Enable intelligent flow control" option to configure the bandwidth value.)

Bandwidth Control

Speed limit according to different source address rules



□	SN	Source address	Time	Bandwidth limited

There is no policy bandwidth control rule defined yet. Please Add

Bandwidth control rule

● Enable ○ Disable

Source address: According to ● Address ○ User ○ Level ○ Department

ANY Add

Time: ANY Add

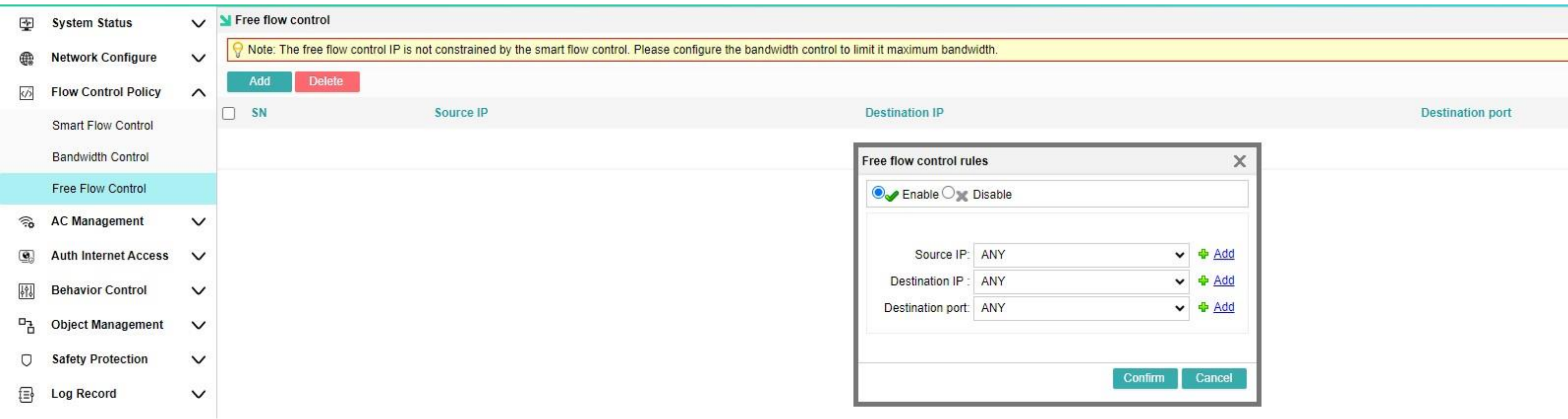
Upstream limit: UNLIMITED

Downstream limit: UNLIMITED

Tips: Click icon to edite bandwidth

Free Flow Control

The setting is not restricted by the overall network speed control of intelligent flow control, and its maximum bandwidth needs to be separately limited in the policy speed limit.



Free flow control

Note: The free flow control IP is not constrained by the smart flow control. Please configure the bandwidth control to limit it maximum bandwidth.

□	SN	Source IP	Destination IP	Destination port

Free flow control rules

● Enable ○ Disable

Source IP: ANY Add

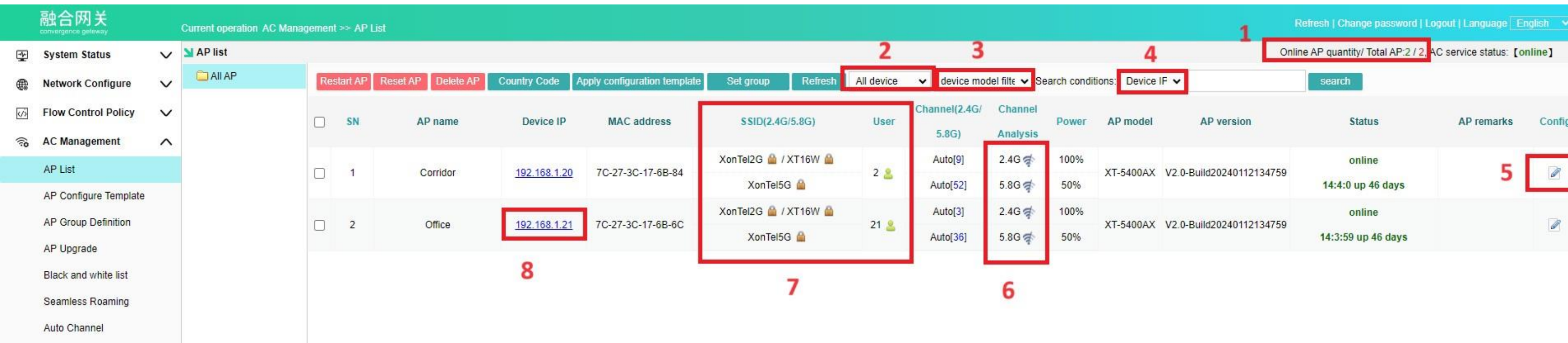
Destination IP : ANY Add

Destination port: ANY Add

3. 4. AC Management

AP List

Display all APs managed by AC, easy check and management.



Online AP quantity/ Total AP:2 / 2, AC service status: 【online】

□	SN	AP name	Device IP	MAC address	SSID(2.4G/5.8G)	User	Channel(2.4G/ 5.8G)	Channel Analysis	Power	AP model	AP version	Status	AP remarks	Config
□	1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	XonTel2G / XT16W XonTel5G	2	Auto[9] Auto[52]	2.4G 5.8G	100% 50%	XT-5400AX	V2.0-Build20240112134759	online 14:4:0 up 46 days		
□	2	Office	192.168.1.21	7C-27-3C-17-6B-6C	XonTel2G / XT16W XonTel5G	21	Auto[3] Auto[36]	2.4G 5.8G	100% 50%	XT-5400AX	V2.0-Build20240112134759	online 14:3:59 up 46 days		

SN 1: View the number of online APs. Green represents the number of online APs, and red represents the total number of connected APs.

SN 2: Filter displays only online or offline APs.

SN 3: Filter displays by single model APs.+

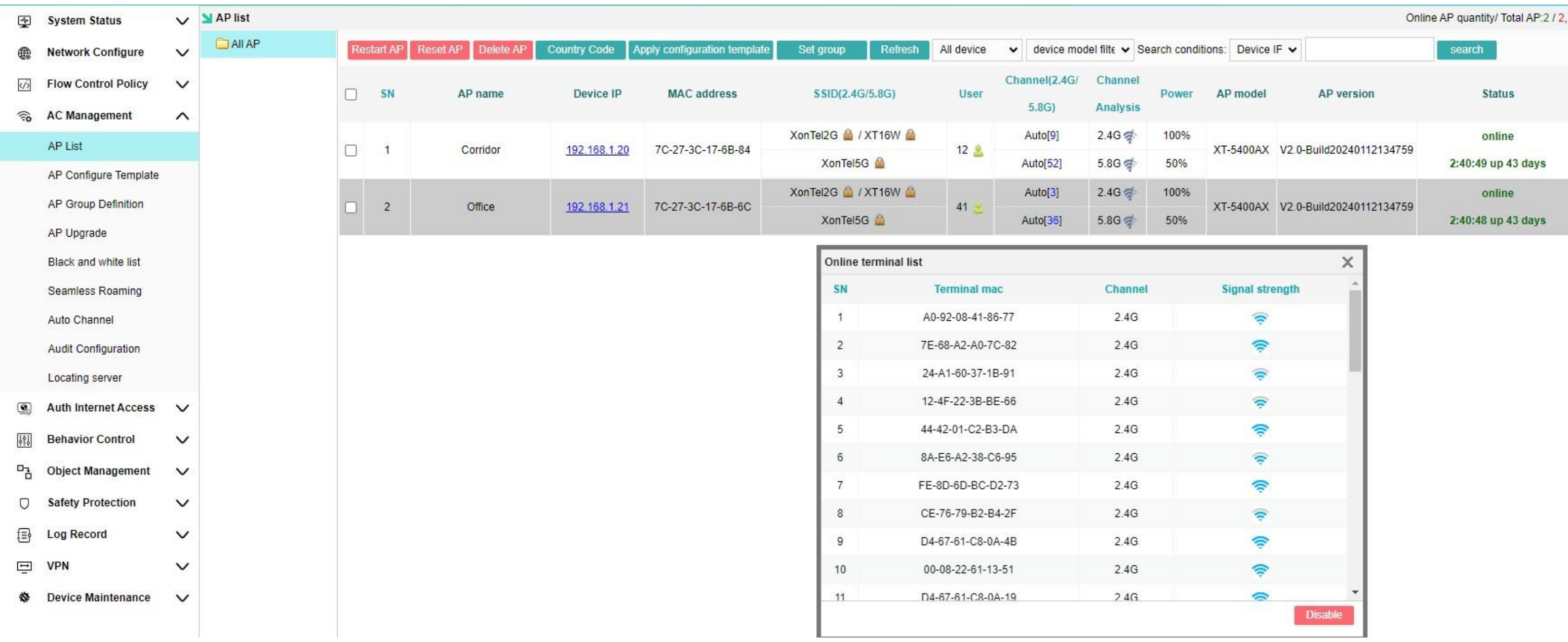
SN 4: Select to search according to the IP/MAC/name/model/version number of the AP device.

SN 5: Edit the parameters and configuration of a single AP.

SN 6: WIFI analyzer, used to scan WIFI of all channels in 2.4G or 5.8G frequency band of the AP.

SN 7: The SSID (wireless WIFI name) and channel of 2.4G, 5.8G and 5.8G2 of the AP are displayed. Click the green villain to display the terminal connected to the AP.

SN 8: AP server login address.



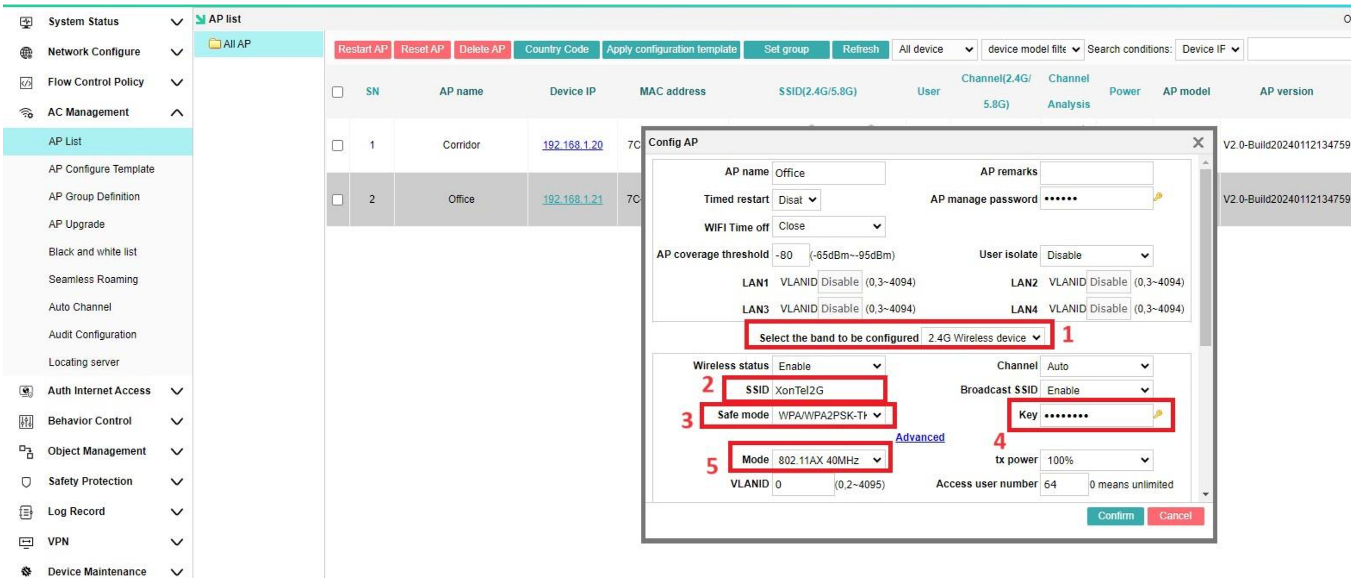
Online AP quantity/ Total AP:2 / 2,

□	SN	AP name	Device IP	MAC address	SSID(2.4G/5.8G)	User	Channel(2.4G/5.8G)	Channel Analysis	Power	AP model	AP version	Status
□	1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	XonTel2G / XT16W XonTel5G	12	Auto[9] Auto[52]	2.4G 5.8G	100% 50%	XT-5400AX	V2.0-Build20240112134759	online 2:40:49 up 43 days
□	2	Office	192.168.1.21	7C-27-3C-17-6B-6C	XonTel2G / XT16W XonTel5G	41	Auto[3] Auto[36]	2.4G 5.8G	100% 50%	XT-5400AX	V2.0-Build20240112134759	online 2:40:48 up 43 days

Online terminal list

SN	Terminal mac	Channel	Signal strength
1	A0-92-08-41-86-77	2.4G	
2	7E-68-A2-A0-7C-82	2.4G	
3	24-A1-60-37-1B-91	2.4G	
4	12-4F-22-3B-BE-66	2.4G	
5	44-42-01-C2-B3-DA	2.4G	
6	8A-E6-A2-38-C6-95	2.4G	
7	FE-8D-6D-BC-D2-73	2.4G	
8	CE-76-79-B2-B4-2F	2.4G	
9	D4-67-61-C8-0A-4B	2.4G	
10	00-08-22-61-13-51	2.4G	
11	D4-67-61-C8-0A-19	2.4G	

Click to edit AP configs



□	SN	AP name	Device IP	MAC address	SSID(2.4G/5.8G)	User	Channel(2.4G/5.8G)	Channel Analysis	Power	AP model	AP version
□	1	Corridor	192.168.1.20	7C							V2.0-Build20240112134759
□	2	Office	192.168.1.21	7C-							V2.0-Build20240112134759

Config AP

AP name: Office
AP remarks:
Timed restart: Disat
AP manage password: ••••••
WIFI Time off: Close
AP coverage threshold: -80 (-65dBm~-95dBm)
User isolate: Disable
LAN1 VLANID Disable (0,3~4094)
LAN2 VLANID Disable (0,3~4094)
LAN3 VLANID Disable (0,3~4094)
LAN4 VLANID Disable (0,3~4094)
Select the band to be configured: 2.4G Wireless device
Wireless status: Enable
Channel: Auto
SSID: XonTel2G
Broadcast SSID: Enable
Safe mode: WPA/WPA2PSK-TI
Key: ••••••••
Mode: 802.11AX 40MHz
tx power: 100%
VLANID: 0 (0,2~4095)
Access user number: 64 0 means unlimited

Main editorial columns:

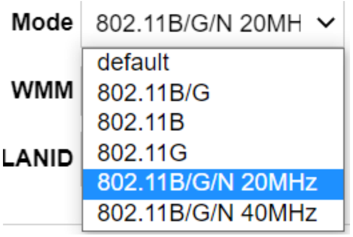
SN 1: Select band need to edit (2.4G/5.8G).

SN 2: Edit SSID name.

SN 3: Encryption, WPA2PSK is recommended.

SN 4: Edit wireless password. Click to view password.

SN 5: Select protocol mode.



Mode 802.11B/G/N 20MH

WMM

LANID

Secondary columns:

AP name, AP remarks: It is used to distinguish all positions of the AP. Generally, it can be marked as installation position or coverage position.

Time restart: Set AP to auto-restart by hours/ days.

AP manage password: AP web login password.

Wireless status: Enable/ disable selected band (2.4G/5.8G).

Channel: Automatic channel can be selected. AP will automatically search for the optimal channel, or manually select the specified channel.

Broadcast SSID: Enable/ disable SSID broadcast.

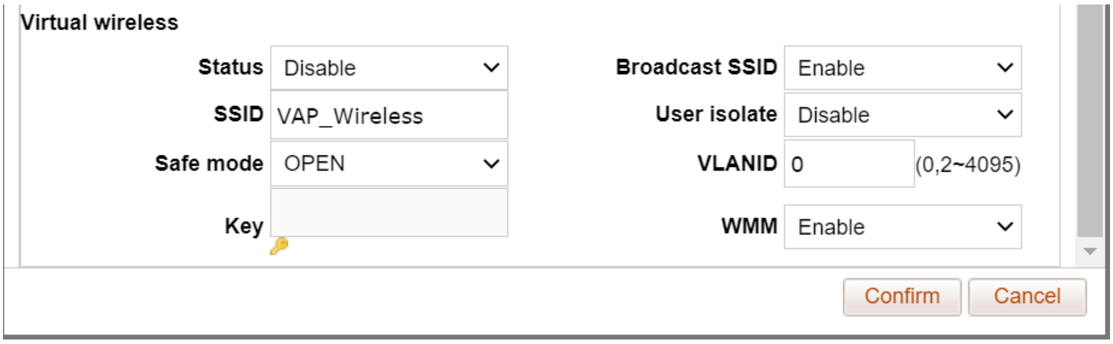
User isolate: Enable/ disable the terminals under the AP to access each other.

Tx power: default100%, optional: 75%/50%/25%/12%.

AP coverage threshold: If the connection strength of the detection terminal is weaker than the threshold value, the AP chooses to eliminate the terminal.

Access user number: Allowed accessed users quantity.

Virtual wireless: Up to 3 virtual WIFIs can be created in each frequency band, and different SSIDs and passwords can be set。

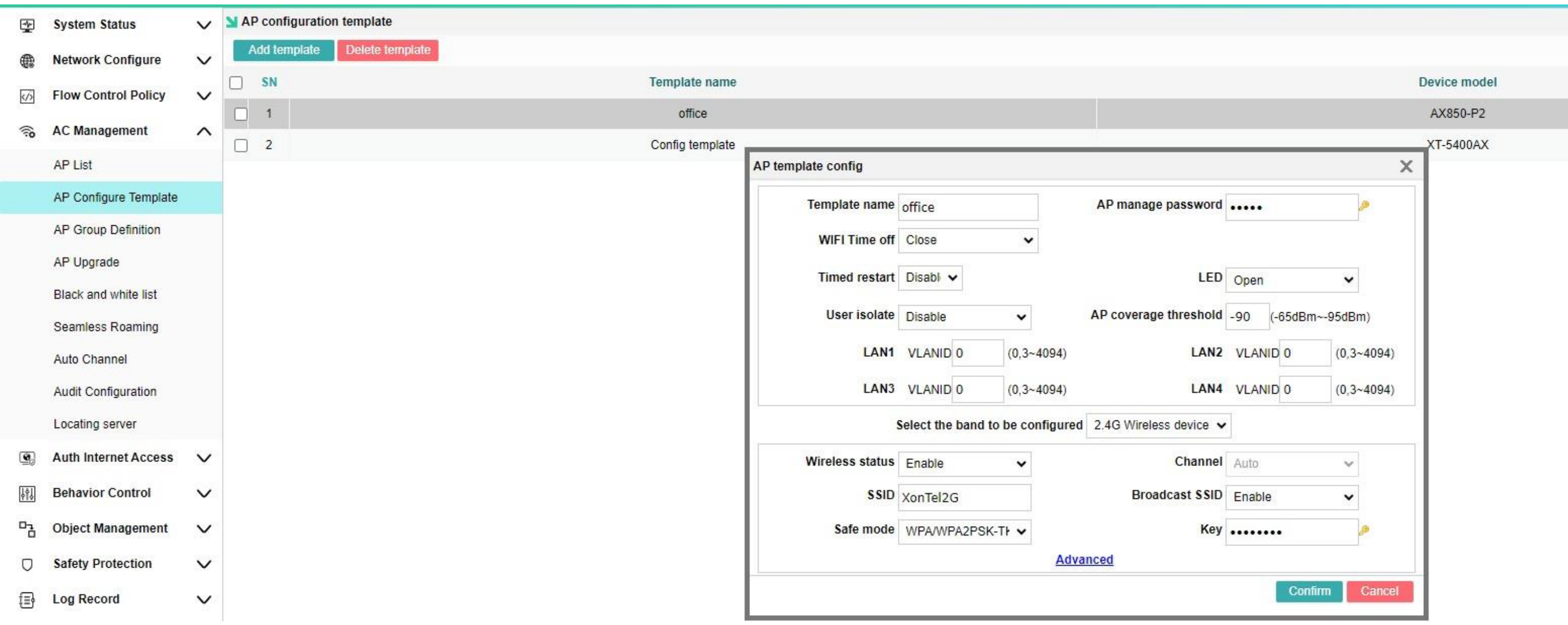


Virtual wireless

Status	Disable	Broadcast SSID	Enable
SSID	VAP_Wireless	User isolate	Disable
Safe mode	OPEN	VLANID	0 (0,2~4095)
Key		WMM	Enable

AP Configure Template

Select a model to add a template, configure the SSID and password, and then select all APs of the same model in the AP to select the corresponding template for application configuration.



AP configuration template

□	SN	Template name	Device model
□	1	office	AX850-P2
□	2	Config template	XT-5400AX

AP template config

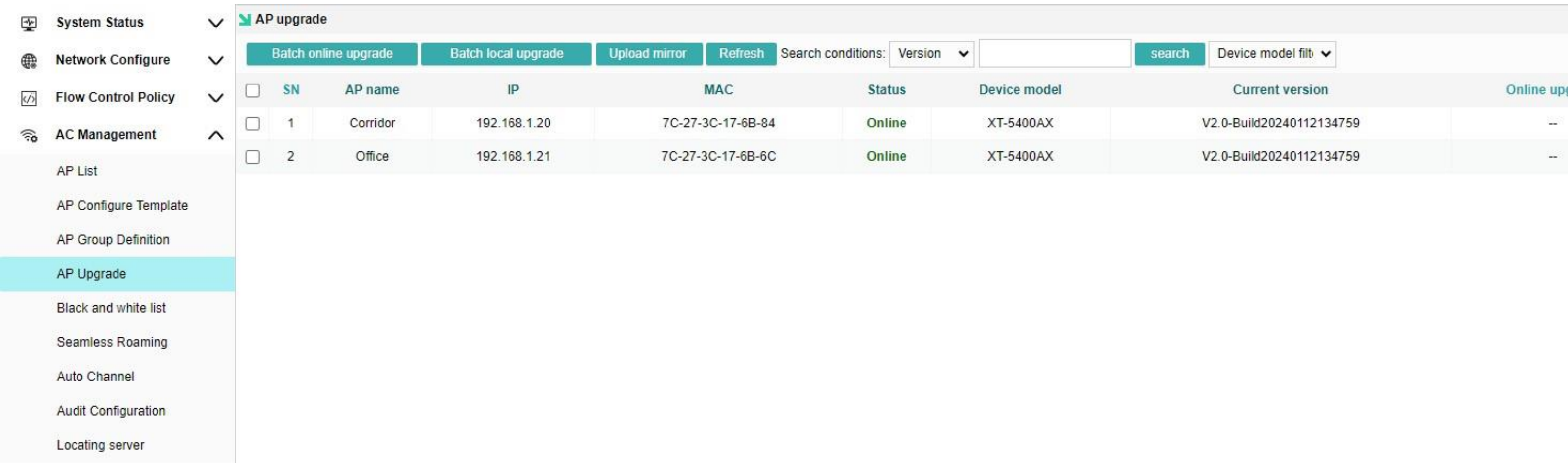
Template name: office
AP manage password: •••••
WIFI Time off: Close
Timed restart: Disabl
LED: Open
User isolate: Disable
AP coverage threshold: -90 (-65dBm~-95dBm)
LAN1 VLANID 0 (0,3~4094)
LAN2 VLANID 0 (0,3~4094)
LAN3 VLANID 0 (0,3~4094)
LAN4 VLANID 0 (0,3~4094)

Select the band to be configured: 2.4G Wireless device

Wireless status: Enable
Channel: Auto
SSID: XonTel2G
Broadcast SSID: Enable
Safe mode: WPA/WPA2PSK-TI
Key: ••••••••

AP Upgrade

Upgrade online or upload firmware for local upgrade.



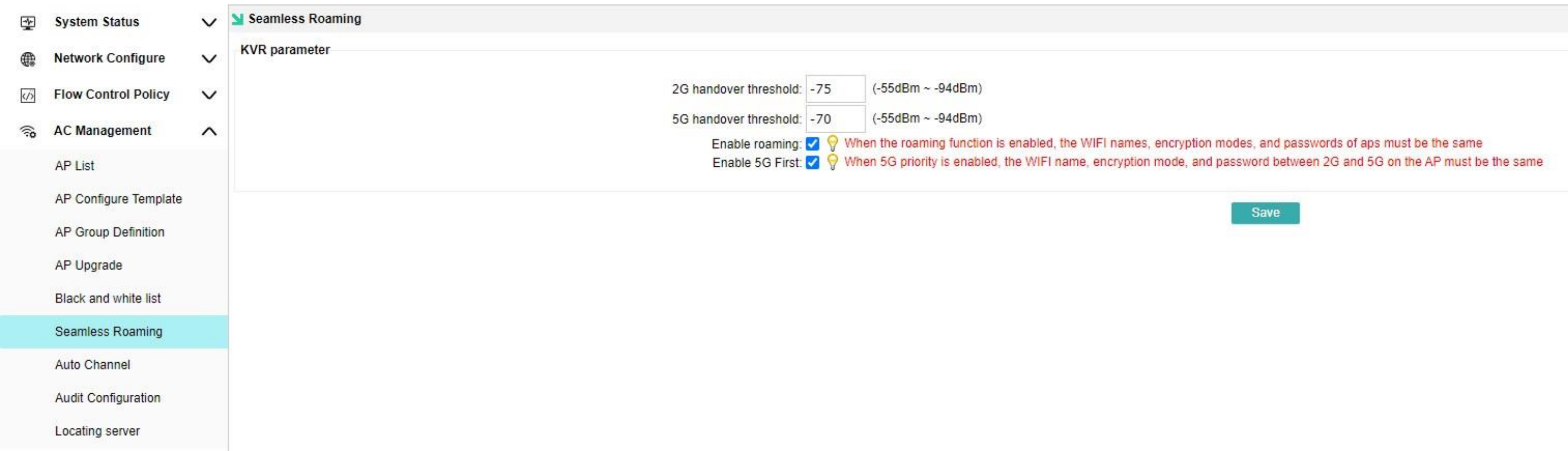
AP upgrade

Search conditions: Version
Device model filt

□	SN	AP name	IP	MAC	Status	Device model	Current version	Online up
□	1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	Online	XT-5400AX	V2.0-Build20240112134759	--
□	2	Office	192.168.1.21	7C-27-3C-17-6B-6C	Online	XT-5400AX	V2.0-Build20240112134759	--

Seamless Roaming

Automatic roaming is enabled by default.



Seamless Roaming

KVR parameter

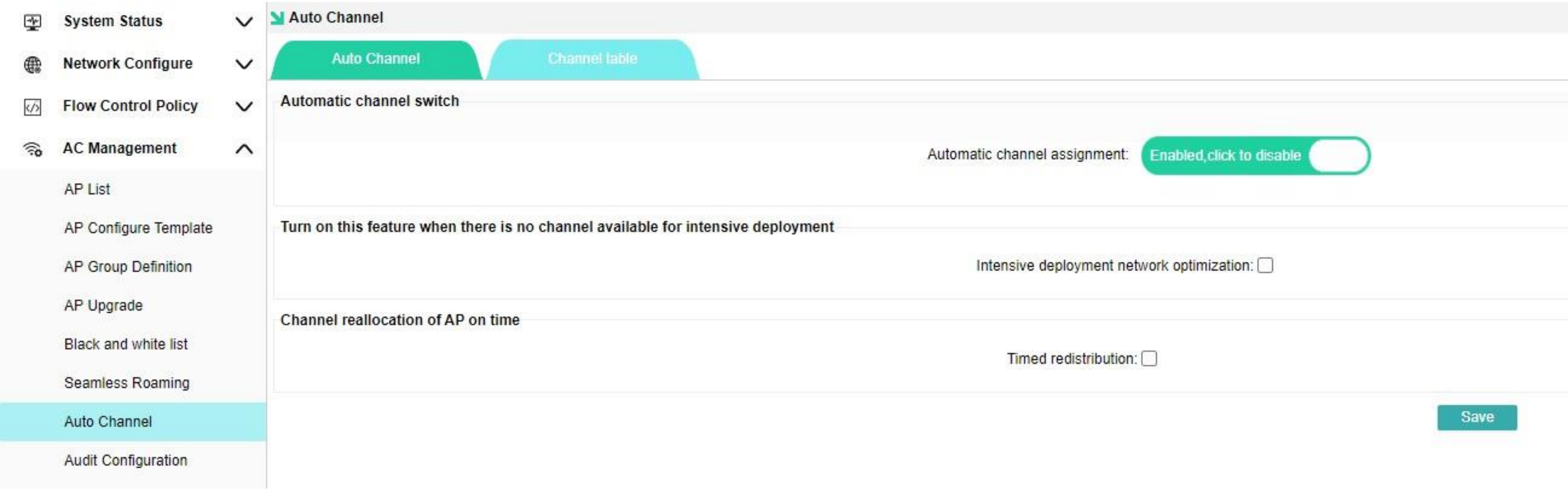
2G handover threshold: -75 (-55dBm ~ -94dBm)

5G handover threshold: -70 (-55dBm ~ -94dBm)

Enable roaming: ☑ When the roaming function is enabled, the WIFI names, encryption modes, and passwords of aps must be the same

Enable 5G First: ☑ When 5G priority is enabled, the WIFI name, encryption mode, and password between 2G and 5G on the AP must be the same

Auto Channel Select



Auto Channel

Automatic channel switch

Automatic channel assignment: Enabled,click to disable

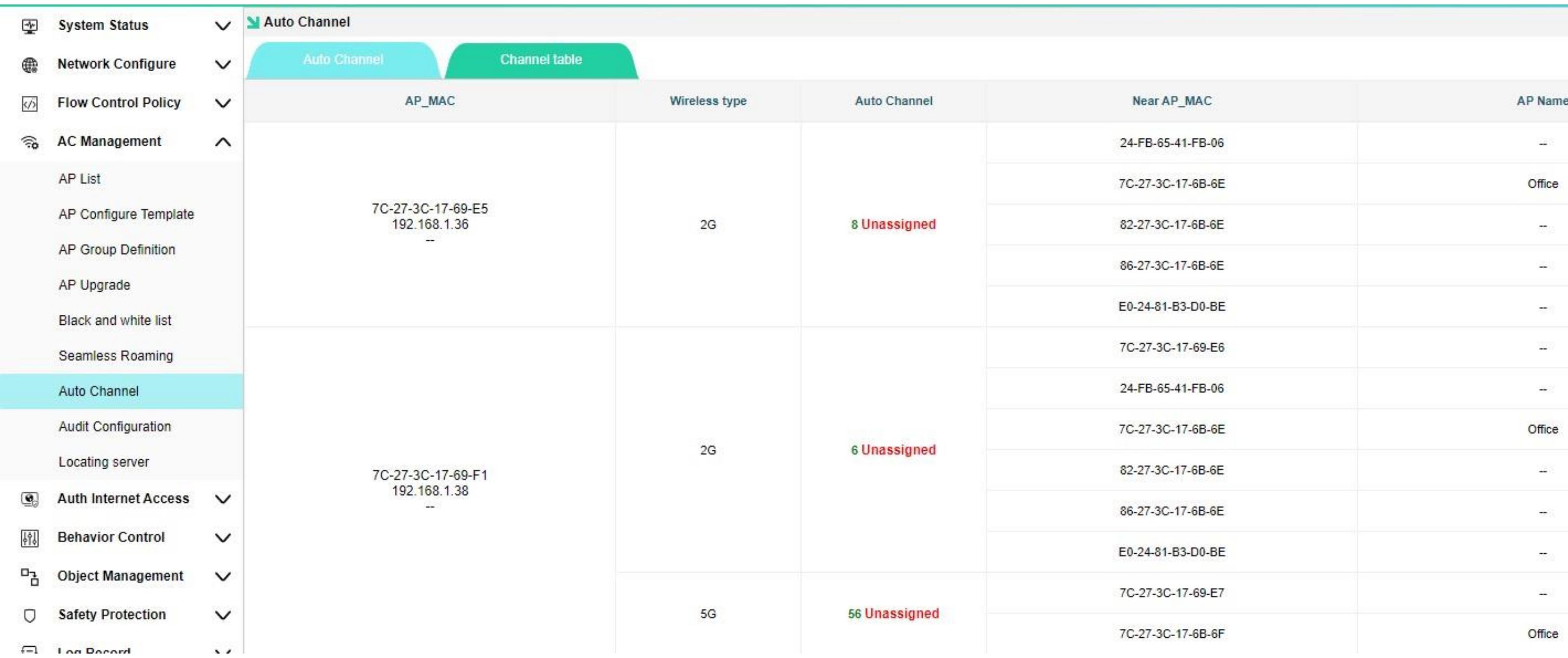
Turn on this feature when there is no channel available for intensive deployment

Intensive deployment network optimization: □

Channel reallocation of AP on time

Timed redistribution: □

Channel table: View all APs SSID, channel, RSSI.



AP_MAC	Wireless type	Auto Channel	Near AP_MAC	AP Name
7C-27-3C-17-69-E5 192.168.1.36 --	2G	8 Unassigned	24-FB-65-41-FB-06	--
			7C-27-3C-17-6B-6E	Office
			82-27-3C-17-6B-6E	--
			86-27-3C-17-6B-6E	--
			E0-24-81-B3-D0-BE	--
7C-27-3C-17-69-F1 192.168.1.38 --	2G	6 Unassigned	7C-27-3C-17-69-E6	--
			24-FB-65-41-FB-06	--
			7C-27-3C-17-6B-6E	Office
			82-27-3C-17-6B-6E	--
			86-27-3C-17-6B-6E	--
			E0-24-81-B3-D0-BE	--
	5G	56 Unassigned	7C-27-3C-17-69-E7	--
			7C-27-3C-17-6B-6F	Office

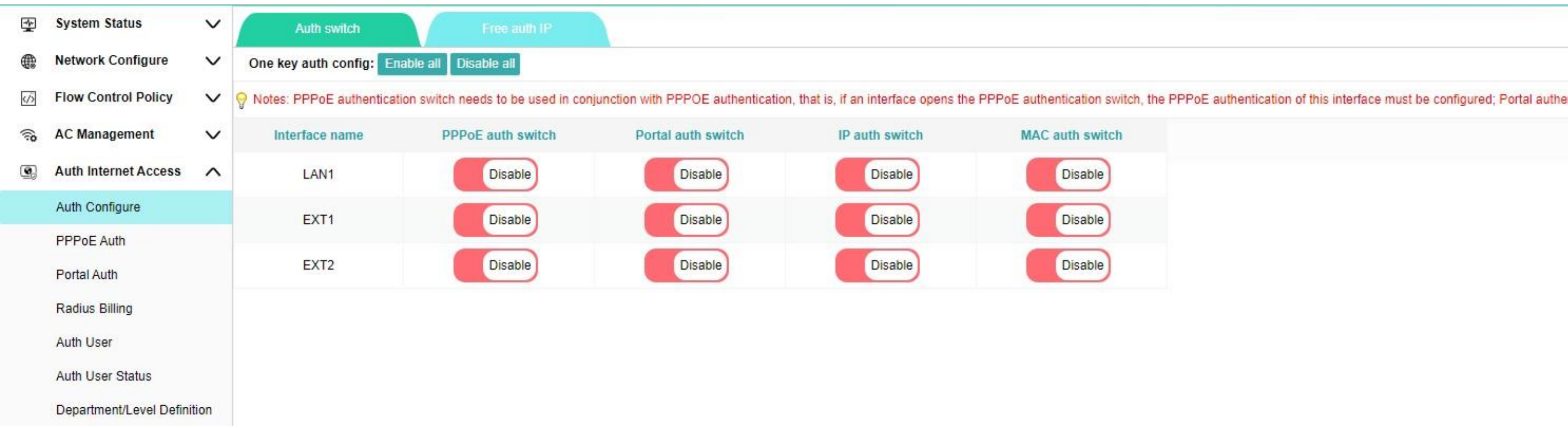
3. 5. Auth Internet Access

Generally, Internet users can access the Internet directly by configuring the IP address of the network card or by routing DHCP to assign the address to obtain the IP address.

Authenticated Internet access means that you need to be a "user" before you can access the Internet.

Auth Configure

Control the authentication switch of the corresponding LNA port.
Marks: As long as any one of the switches is turned on, it means that the LAN1 port is intercepted. Only authenticated users are allowed to access the Internet



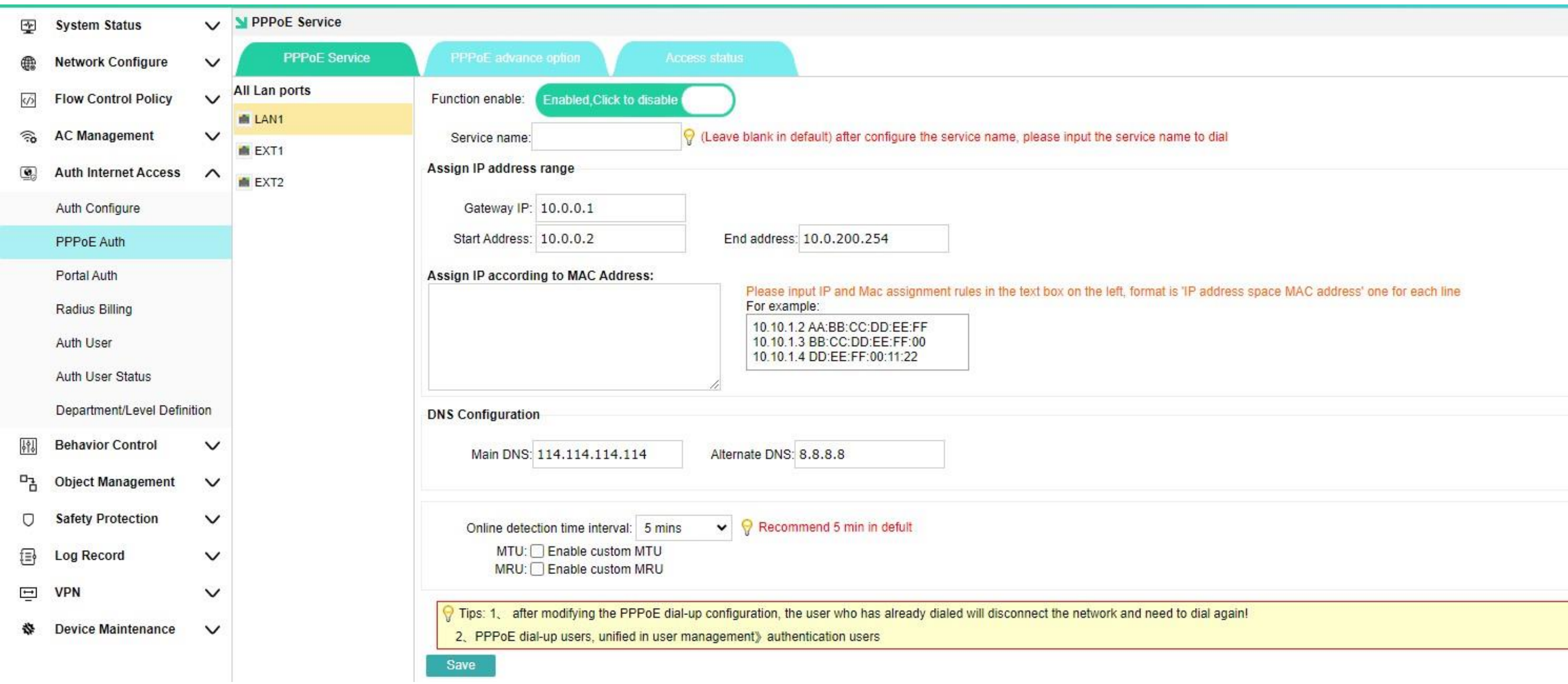
One key auth config: Enable all Disable all

Notes: PPPoE authentication switch needs to be used in conjunction with PPPOE authentication, that is, if an interface opens the PPPoE authentication switch, the PPPoE authentication of this interface must be configured; Portal authe

Interface name	PPPoE auth switch	Portal auth switch	IP auth switch	MAC auth switch
LAN1	Disable	Disable	Disable	Disable
EXT1	Disable	Disable	Disable	Disable
EXT2	Disable	Disable	Disable	Disable

PPPoE Auth

PPPoE authentication --- used for cell broadband. Intranet users can access the Internet through PPPoE dial-up. The dial-up account password is created on the route (for the connection with radius billing, it needs to be created on the radius billing system).
It is recommended to use the LAN address for the allocation of the address pool. The IP address of the LAN port must not be the same as the network segment. For example, the IP address of the LAN port is 192.168.1.1. The address pool here cannot be 192.168.1.xxx
DNS suggests to assign DNS of local operators.



Function enable: Enabled,Click to disable

Service name: (Leave blank in default) after configure the service name, please input the service name to dial

Assign IP address range

Gateway IP: 10.0.0.1

Start Address: 10.0.0.2 End address: 10.0.200.254

Assign IP according to MAC Address:

Please input IP and Mac assignment rules in the text box on the left, format is 'IP address space MAC address' one for each line
For example:
10.10.1.2 AA:BB:CC:DD:EE:FF
10.10.1.3 BB:CC:DD:EE:FF:00
10.10.1.4 DD:EE:FF:00:11:22

DNS Configuration

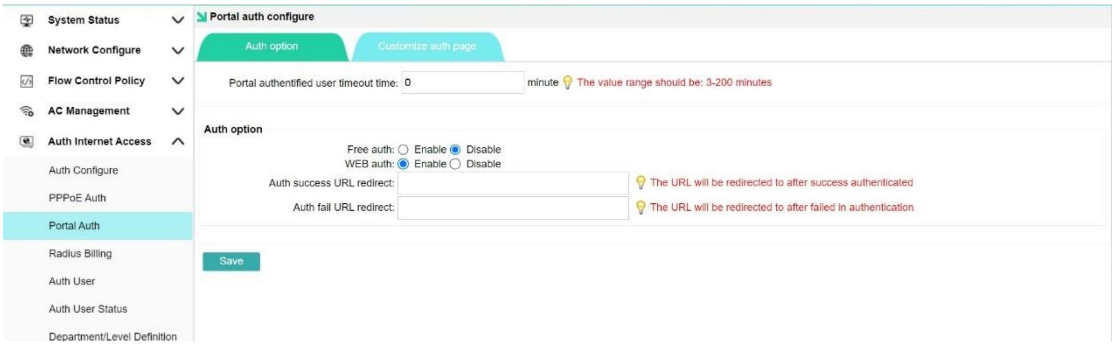
Main DNS: 114.114.114.114 Alternate DNS: 8.8.8.8

Online detection time interval: 5 mins Recommend 5 min in defult

MTU: □ Enable custom MTU
MRU: □ Enable custom MRU

Tips: 1、 after modifying the PPPoE dial-up configuration, the user who has already dialed will disconnect the network and need to dial again!
2、PPPoE dial-up users, unified in user management》authentication users

Portal Auth



Portal authentified user timeout time: 0 minute The value range should be: 3-200 minutes

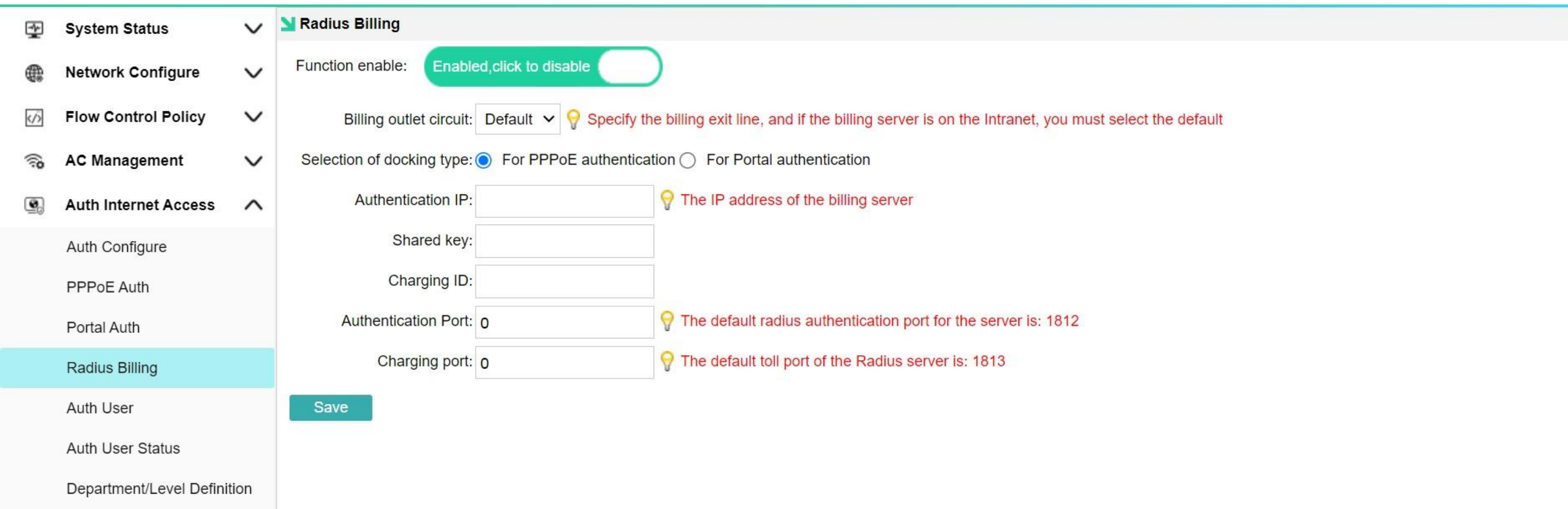
Auth option

Free auth: ○ Enable ● Disable
WEB auth: ● Enable ○ Disable
Auth success URL redirect: The URL will be redirected to after success authenticated
Auth fail URL redirect: The URL will be redirected to after failed in authentication

Free auth: It is used in hotels to prevent pinhole cameras from linking to WIFI network. One more manual click step is required. Equivalent to self-service click to release.

WEB auth: Users connected to the AP (such as mobile phones) can enter their username and password in the pop-up authentication window to access the Internet. The account password of the WEB password is created on the route (for the connection with radius billing, it needs to be created on the radius billing system)

Radius Billing



Radius Billing

Function enable: Enabled,click to disable

Billing outlet circuit: Default — Specify the billing exit line, and if the billing server is on the Intranet, you must select the default

Selection of docking type: ● For PPPoE authentication ○ For Portal authentication

Authentication IP: — The IP address of the billing server

Shared key:

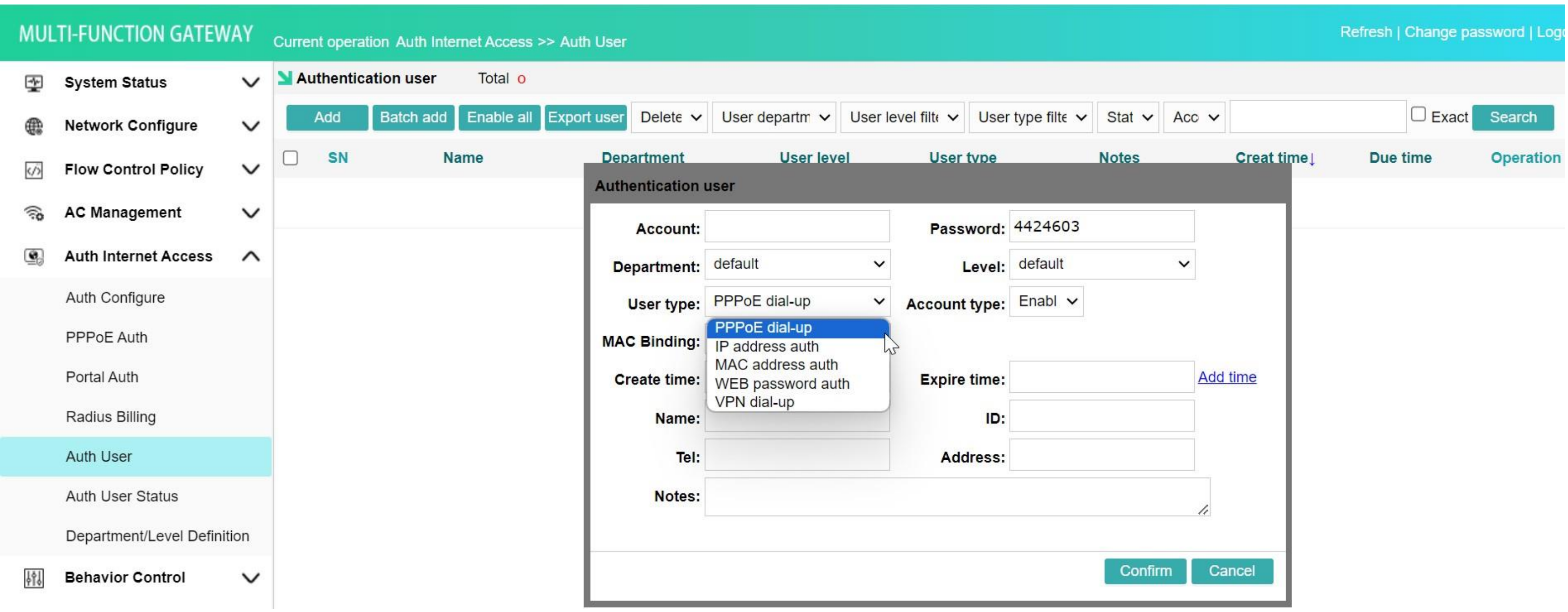
Charging ID:

Authentication Port: 0 — The default radius authentication port for the server is: 1812

Charging port: 0 — The default toll port of the Radius server is: 1813

Auth User

The following figure shows five types of users.



MULTI-FUNCTION GATEWAY

Current operation Auth Internet Access >> Auth User

Authentication user Total 0

☐	SN	Name	Department	User level	User type	Notes	Creat time↓	Due time	Operation

Authentication user

Account:

Password: 4424603

Department: default

Level: default

User type: PPPoE dial-up

Account type: Enabl

MAC Binding:

Create time:

Expire time:

Name:

ID:

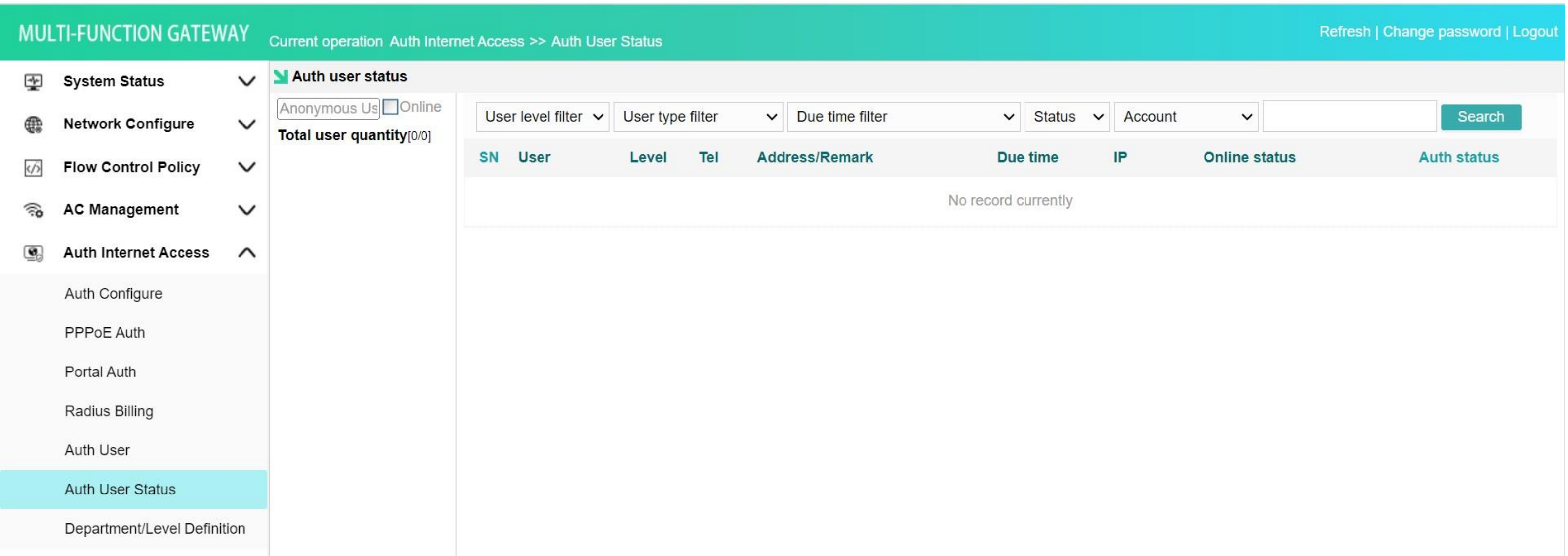
Tel:

Address:

Notes:

Auth User Status

Users can be seen online, and the green icon represents the online users, allowing online access.

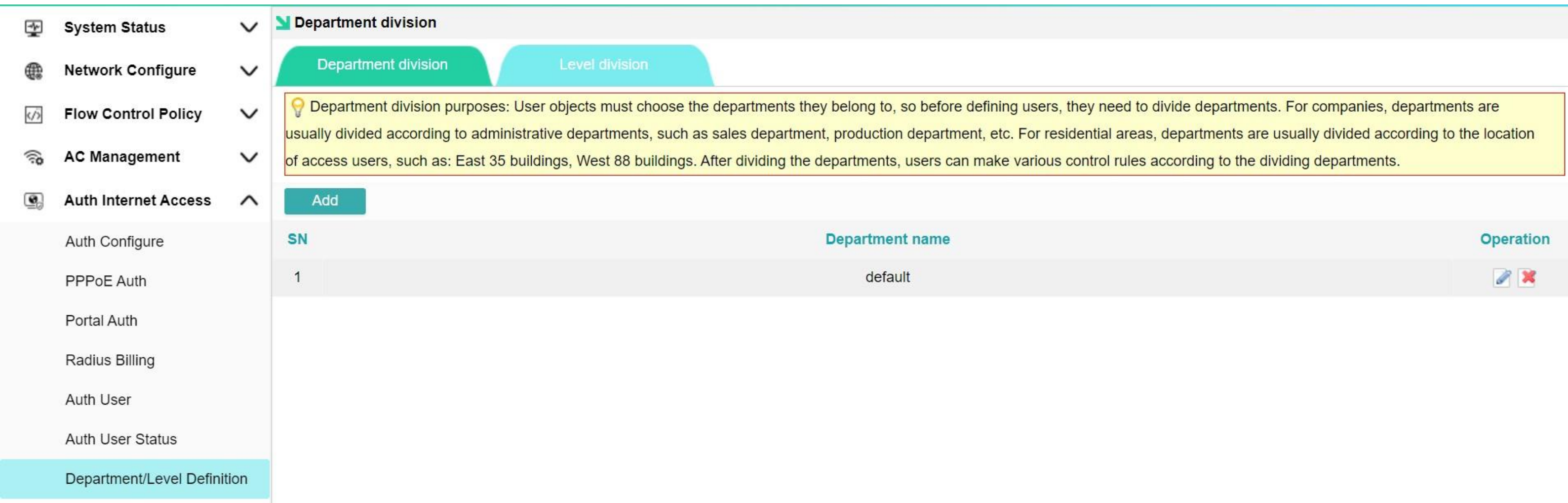


Total user quantity[0/0]

SN	User	Level	Tel	Address/Remark	Due time	IP	Online status	Auth status
No record currently								

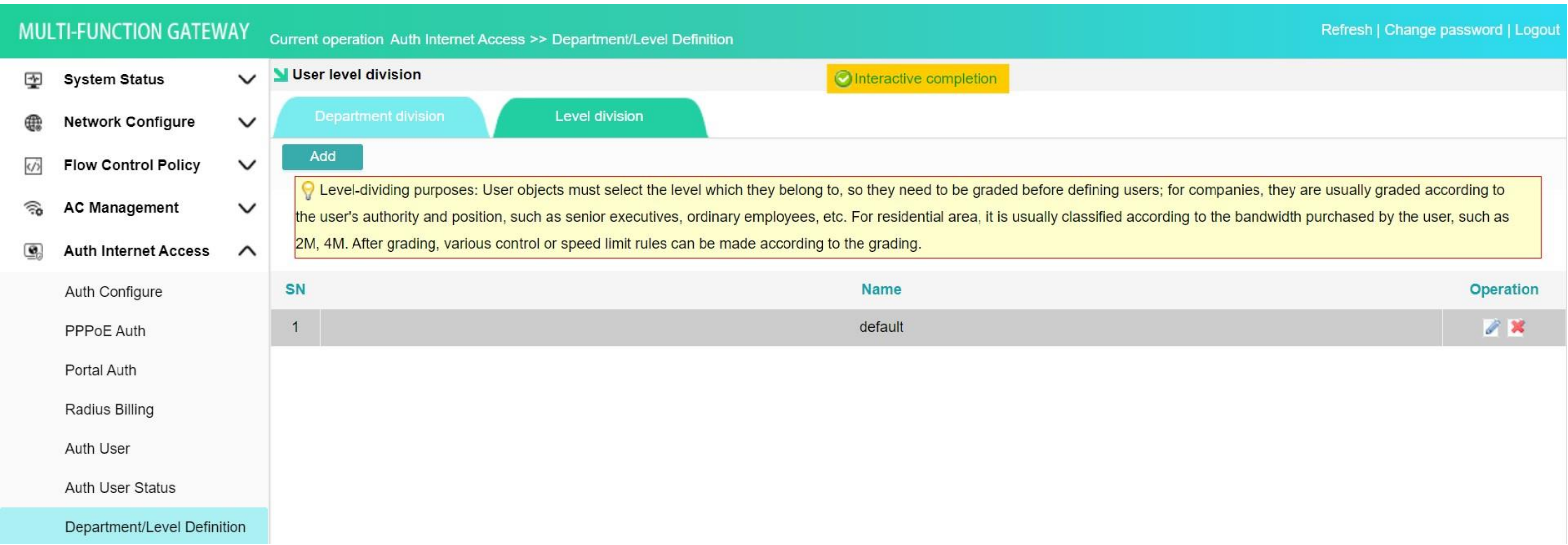
Department/Level Definition

Management department and level, used to bind the Internet users



Department division purposes: User objects must choose the departments they belong to, so before defining users, they need to divide departments. For companies, departments are usually divided according to administrative departments, such as sales department, production department, etc. For residential areas, departments are usually divided according to the location of access users, such as: East 35 buildings, West 88 buildings. After dividing the departments, users can make various control rules according to the dividing departments.

SN	Department name	Operation
1	default	✎ ✖



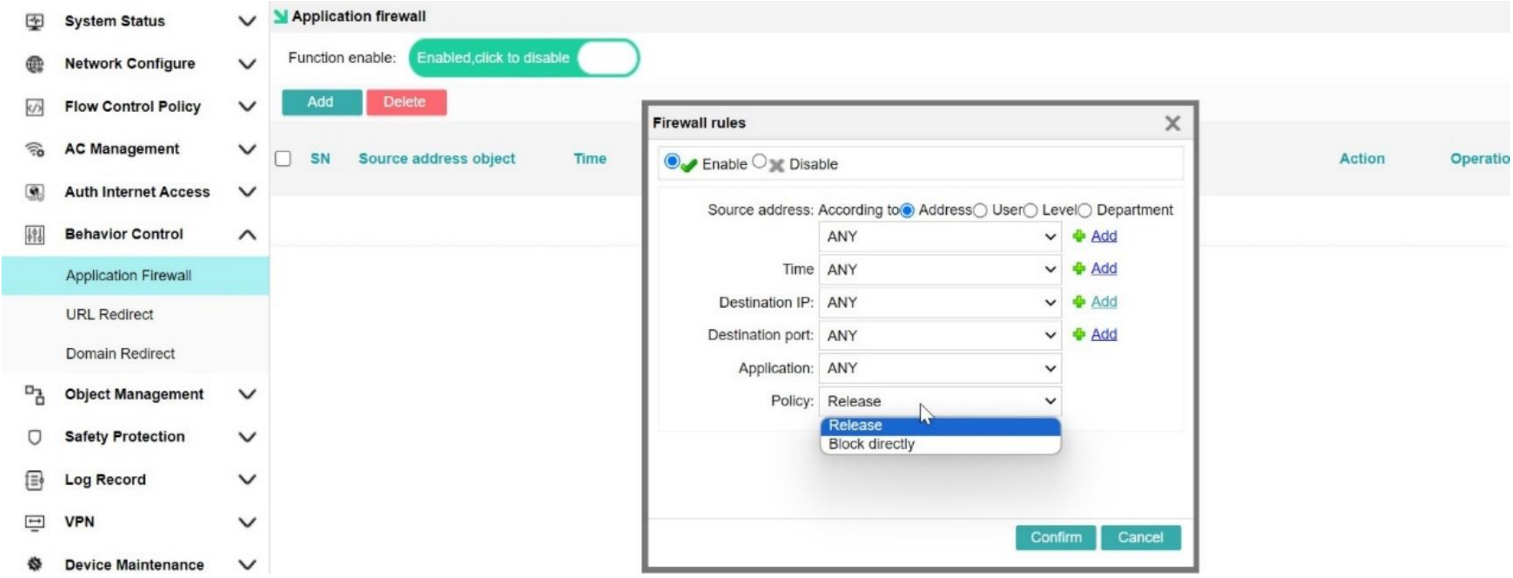
Level-dividing purposes: User objects must select the level which they belong to, so they need to be graded before defining users; for companies, they are usually graded according to the user's authority and position, such as senior executives, ordinary employees, etc. For residential area, it is usually classified according to the bandwidth purchased by the user, such as 2M, 4M. After grading, various control or speed limit rules can be made according to the grading.

SN	Name	Operation
1	default	

3. 6. Behavior Control

Application Firewall

Configure the required release and direct blocking destination IP, port and application according to the source and time.



Function enable: Enabled,click to disable

● Enable ○ Disable

Source address: According to ● Address ○ User ○ Level ○ Department

ANY Add

Time: ANY Add

Destination IP: ANY Add

Destination port: ANY Add

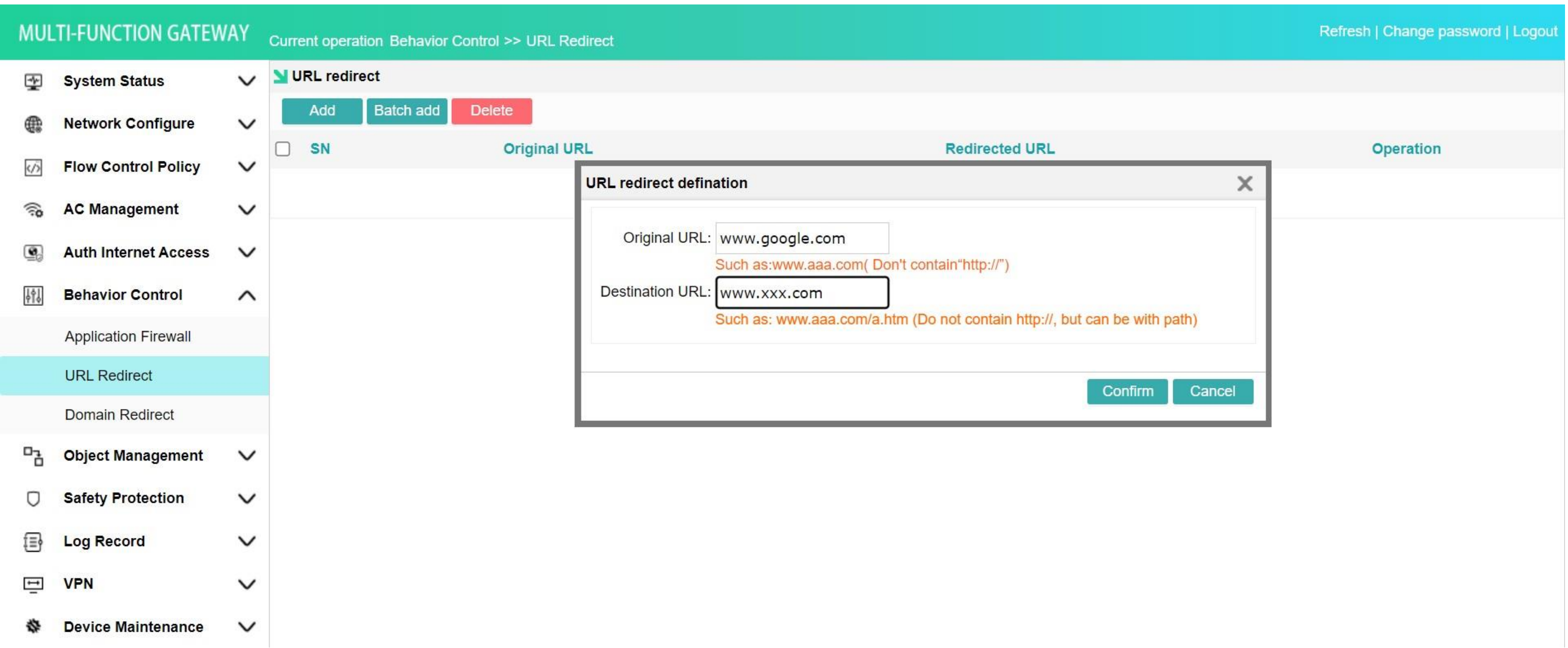
Application: ANY

Policy: Release

Release
Block directly

URL Redirect

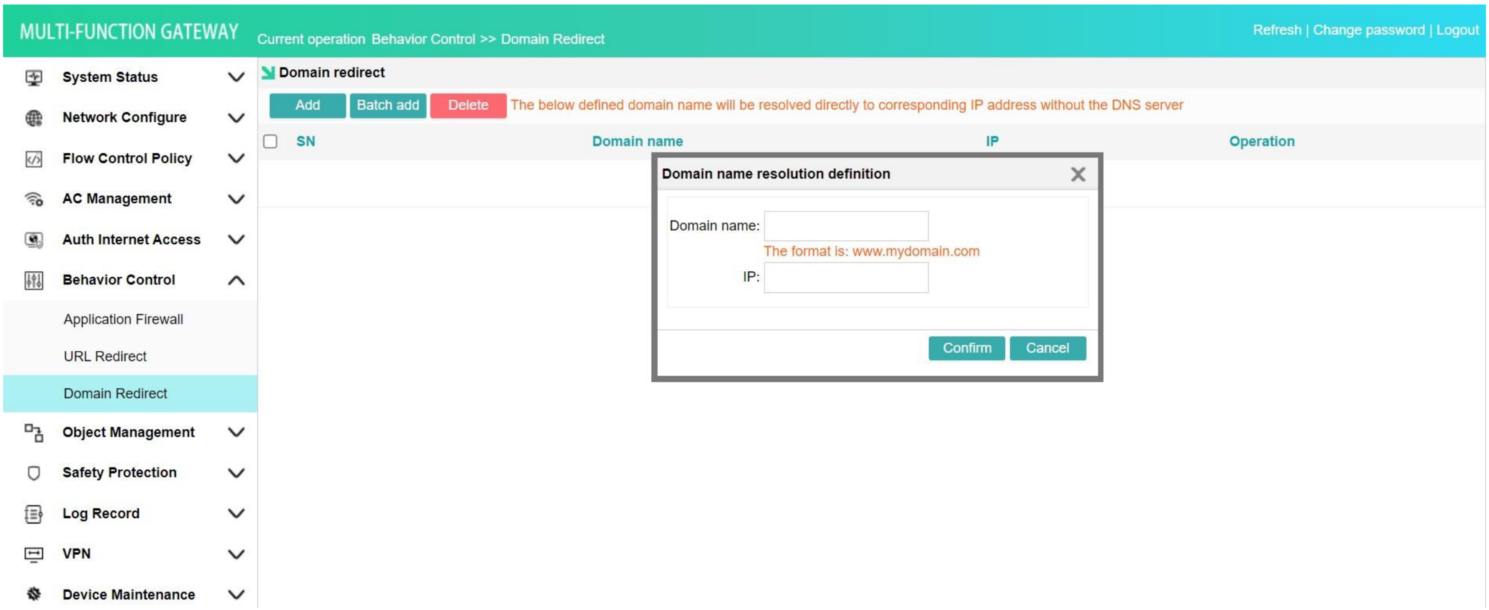
When the terminal accesses the original website, it will automatically jump to the destination website. (Takes effect after clearing the browser cache)



Original URL: www.google.com
Such as:www.aaa.com(Don't contain"http://")
Destination URL: www.xxx.com
Such as: www.aaa.com/a.htm (Do not contain http://, but can be with path)

Domain Redirect

Set that when the terminal accesses the domain name, it automatically resolves to the specified IP (takes effect after clearing the browser cache)

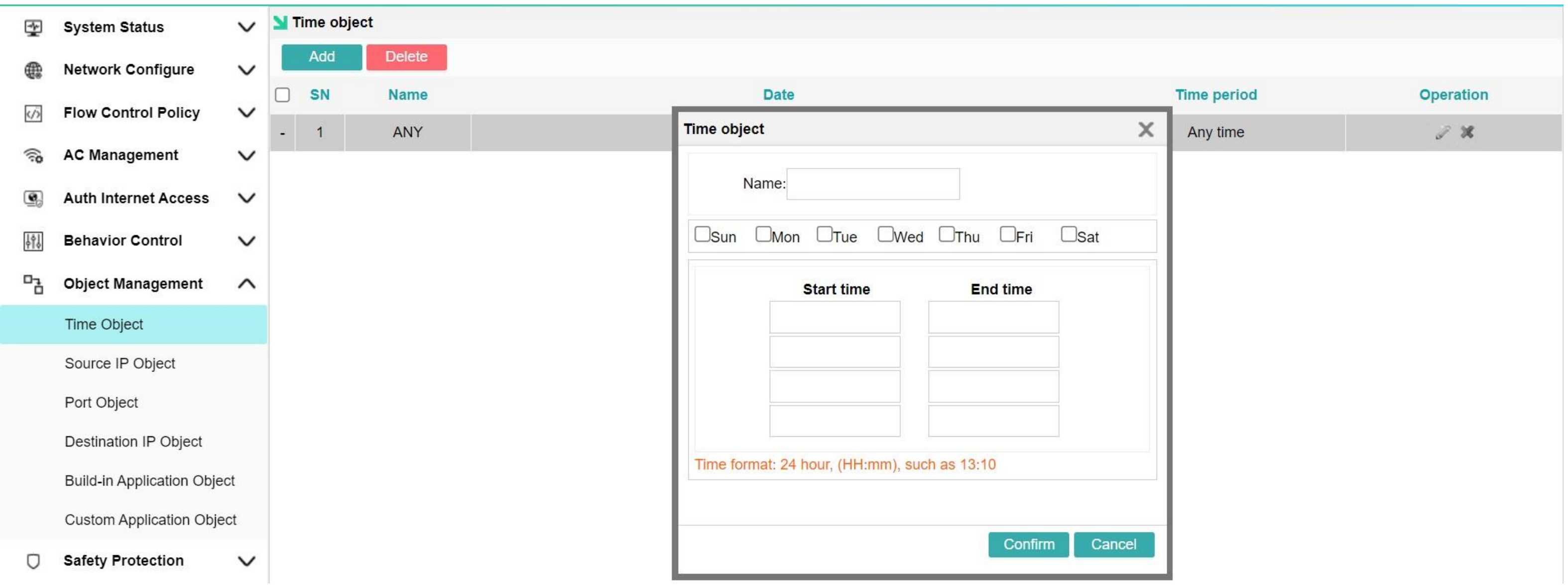


The below defined domain name will be resolved directly to corresponding IP address without the DNS server

Domain name:
The format is: www.mydomain.com
IP:

3. 7. Object Management

Time Object



	SN	Name	Date	Time period	Operation
-	1	ANY		Any time	

Time object

Name:

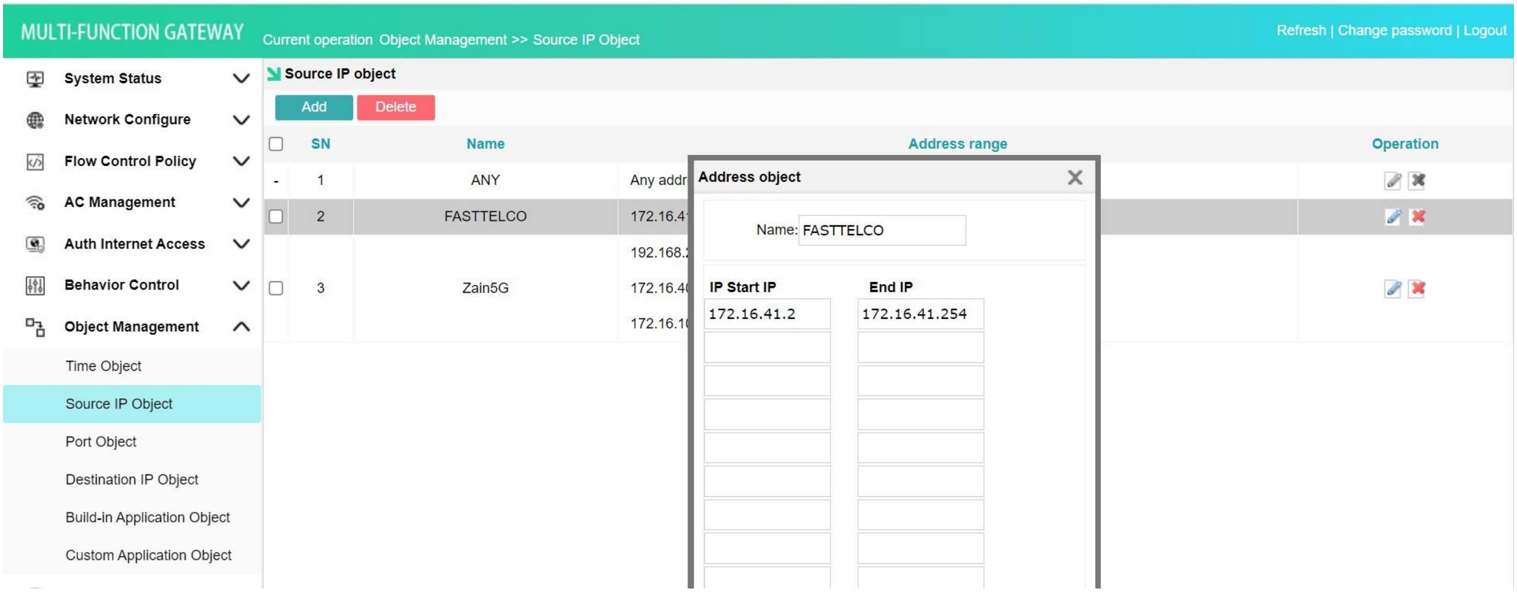
□Sun □Mon □Tue □Wed □Thu □Fri □Sat

Start time | End time

Time format: 24 hour, (HH:mm), such as 13:10

Source IP Object

Here you can define the range of IP addresses which you can use for example for multi diversion rules



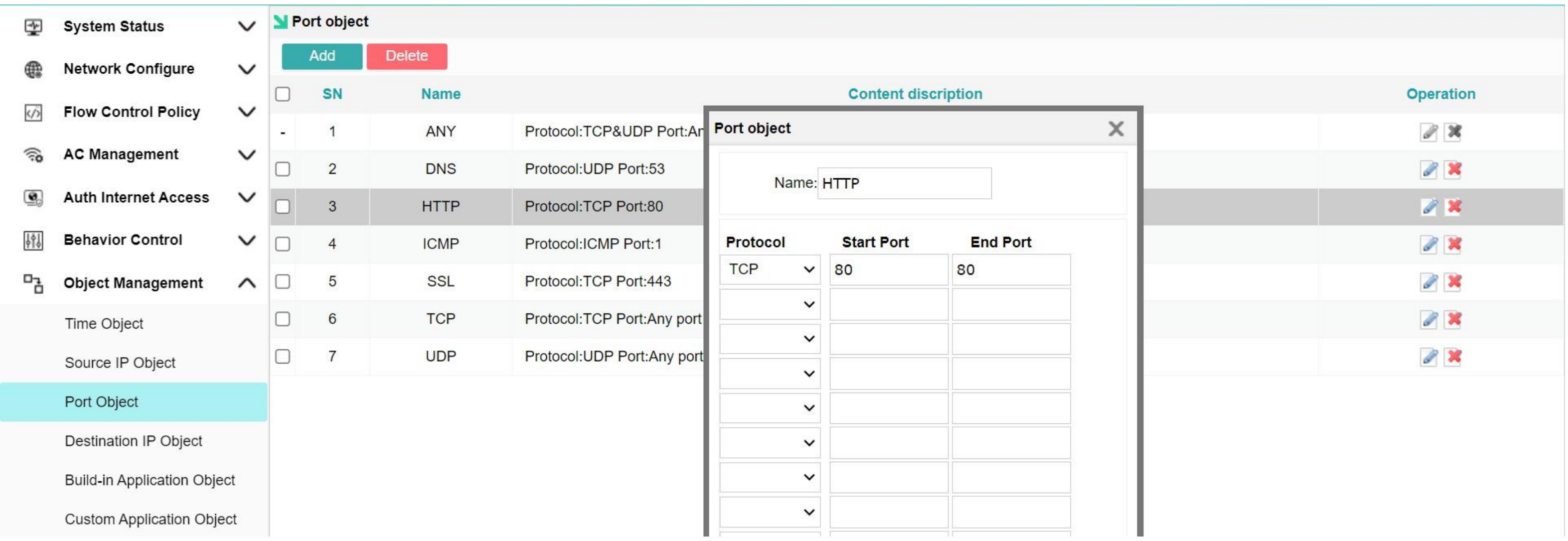
	SN	Name	Address range	Operation
-	1	ANY	Any addr	
□	2	FASTTELCO	172.16.4 192.168.	
□	3	Zain5G	172.16.4 172.16.1	

Address object

Name: FASTTELCO

IP Start IP	End IP
172.16.41.2	172.16.41.254

Port Object



Port object

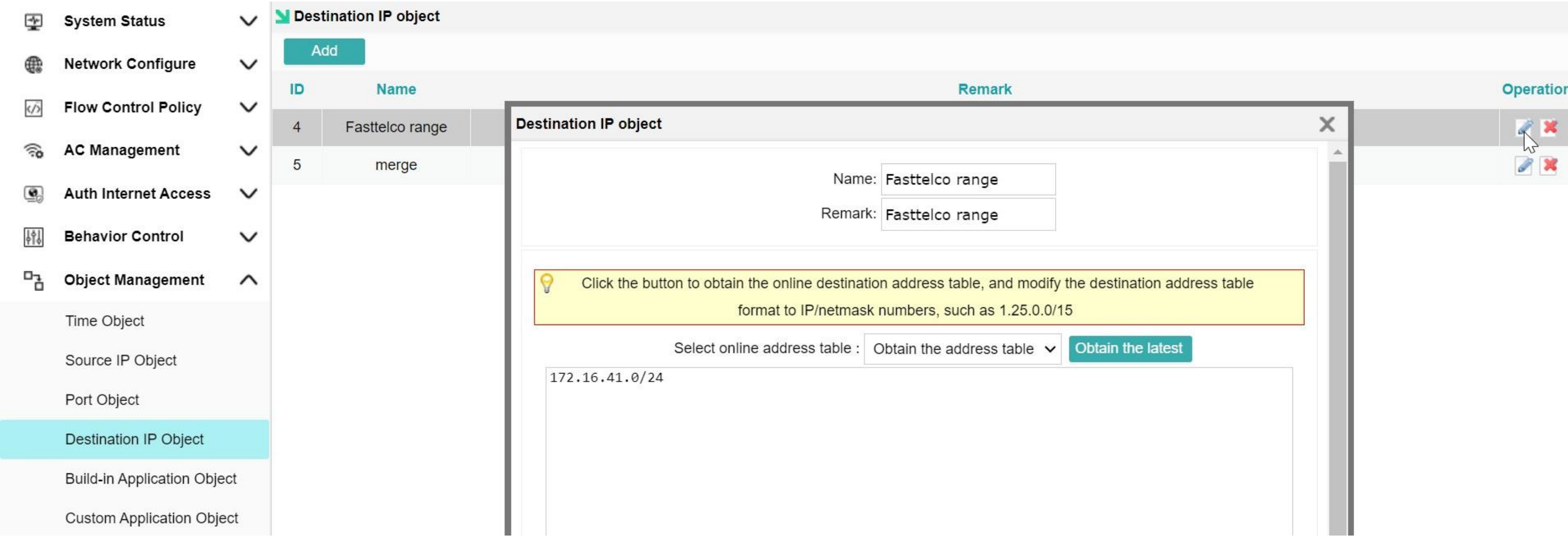
	SN	Name	Content discription	Operation
-	1	ANY	Protocol:TCP&UDP Port:An	
□	2	DNS	Protocol:UDP Port:53	
□	3	HTTP	Protocol:TCP Port:80	
□	4	ICMP	Protocol:ICMP Port:1	
□	5	SSL	Protocol:TCP Port:443	
□	6	TCP	Protocol:TCP Port:Any port	
□	7	UDP	Protocol:UDP Port:Any port	

Port object

Name: HTTP

Protocol	Start Port	End Port
TCP	80	80

Destination IP Object



Destination IP object

ID	Name	Remark	Operatior
4	Fasttelco range		
5	merge		

Destination IP object

Name: Fasttelco range

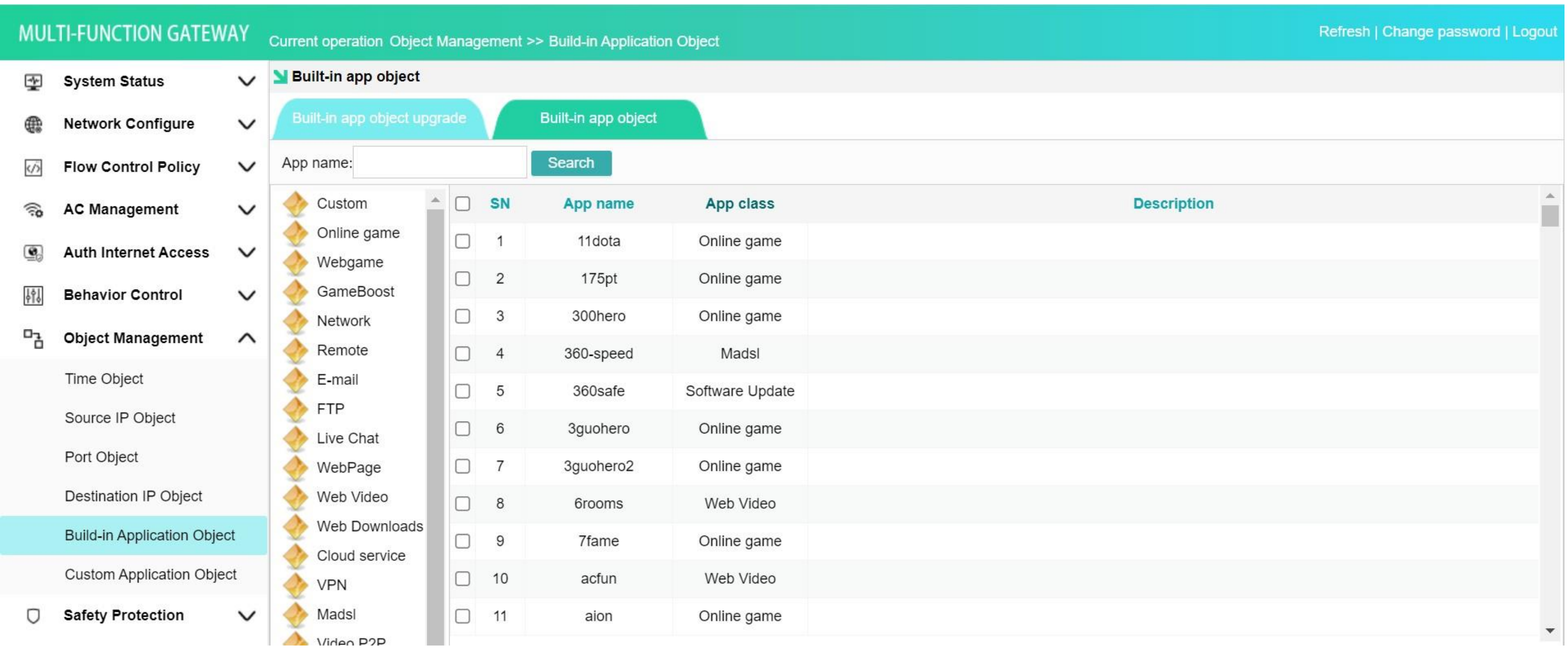
Remark: Fasttelco range

Click the button to obtain the online destination address table, and modify the destination address table format to IP/netmask numbers, such as 1.25.0.0/15

Select online address table : Obtain the address table

```
172.16.41.0/24
```

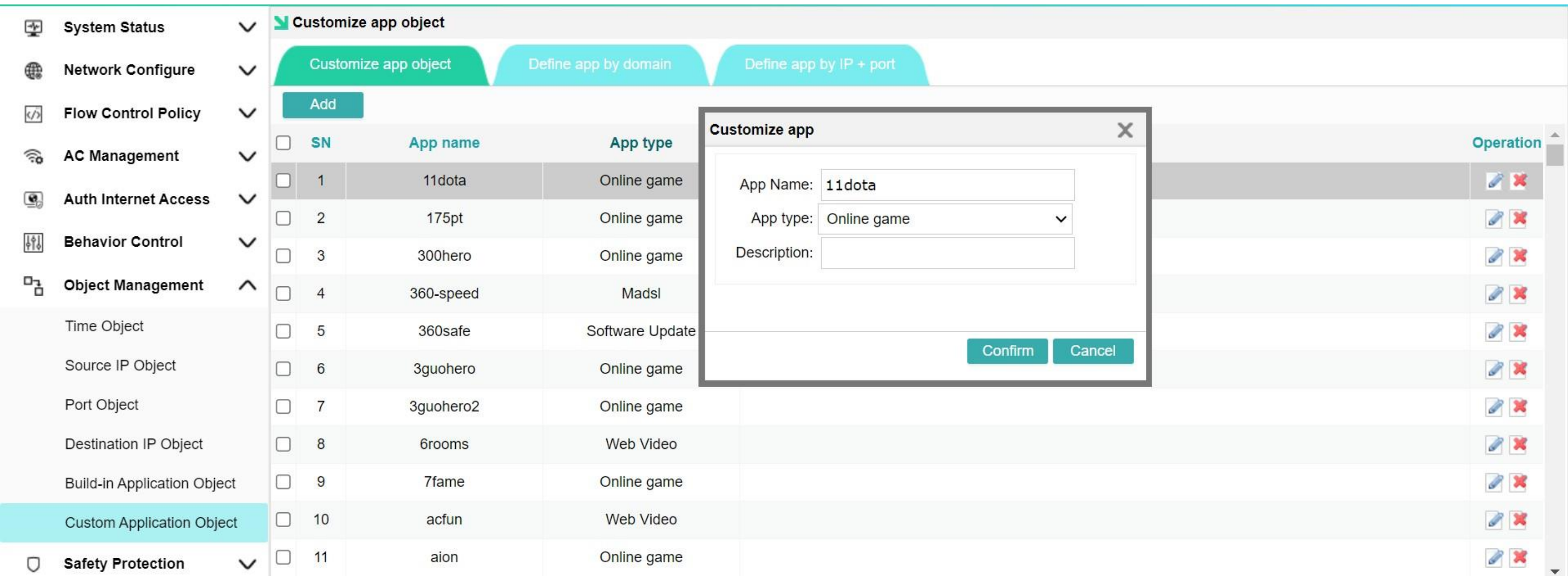
Built-in Application Object



App name:

□	SN	App name	App class	Description
□	1	11dota	Online game	
□	2	175pt	Online game	
□	3	300hero	Online game	
□	4	360-speed	Madsl	
□	5	360safe	Software Update	
□	6	3guohero	Online game	
□	7	3guohero2	Online game	
□	8	6rooms	Web Video	
□	9	7fame	Online game	
□	10	acfun	Web Video	
□	11	aion	Online game	

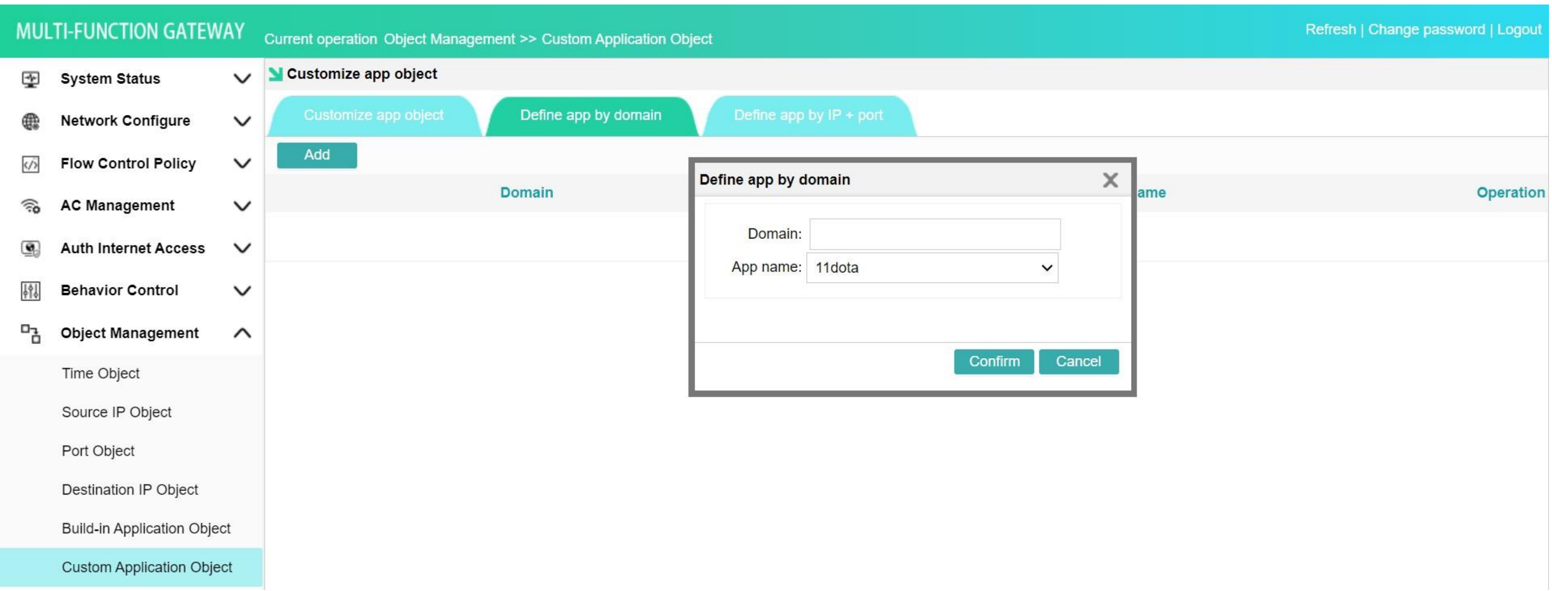
Custom Application Object



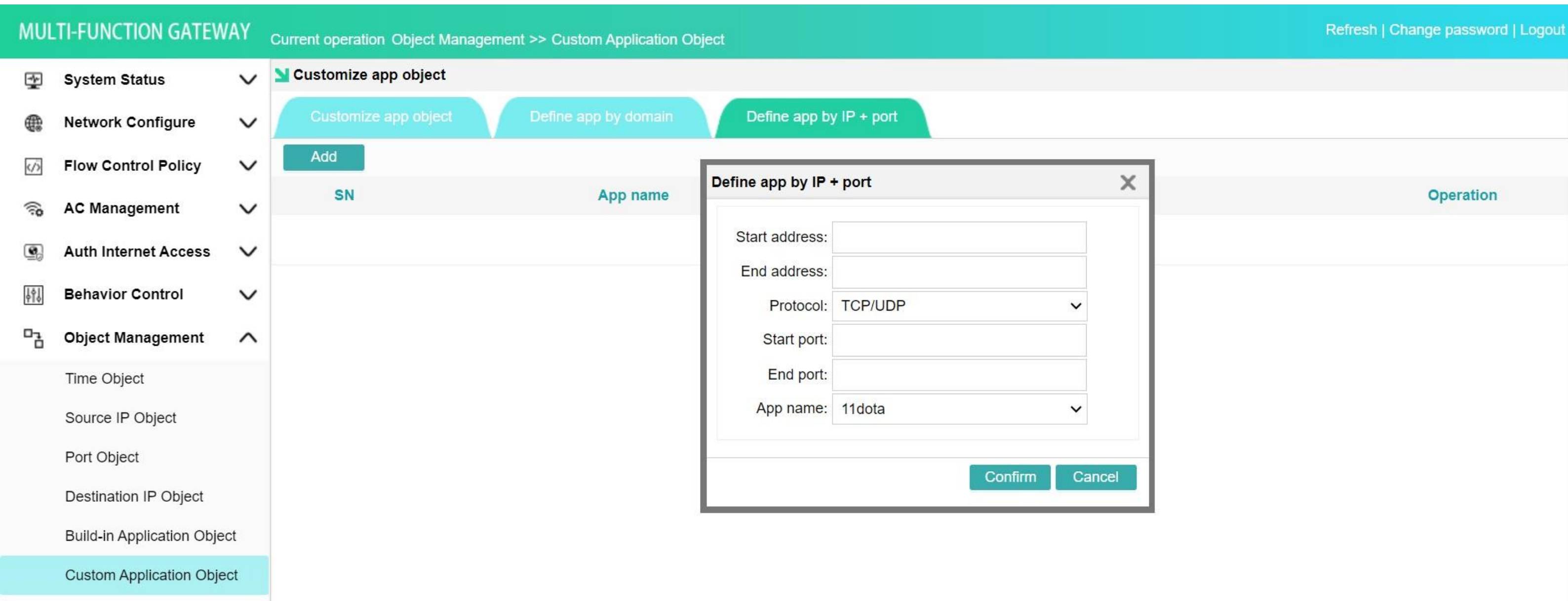
□	SN	App name	App type	Operation
□	1	11dota	Online game	
□	2	175pt	Online game	
□	3	300hero	Online game	
□	4	360-speed	Madsl	
□	5	360safe	Software Update	
□	6	3guohero	Online game	
□	7	3guohero2	Online game	
□	8	6rooms	Web Video	
□	9	7fame	Online game	
□	10	acfun	Web Video	
□	11	aion	Online game	

App Name: 11dota
App type: Online game
Description:

Define applications according to domain name or destination IP+port as shown in the figures below



Domain:
App name: 11dota

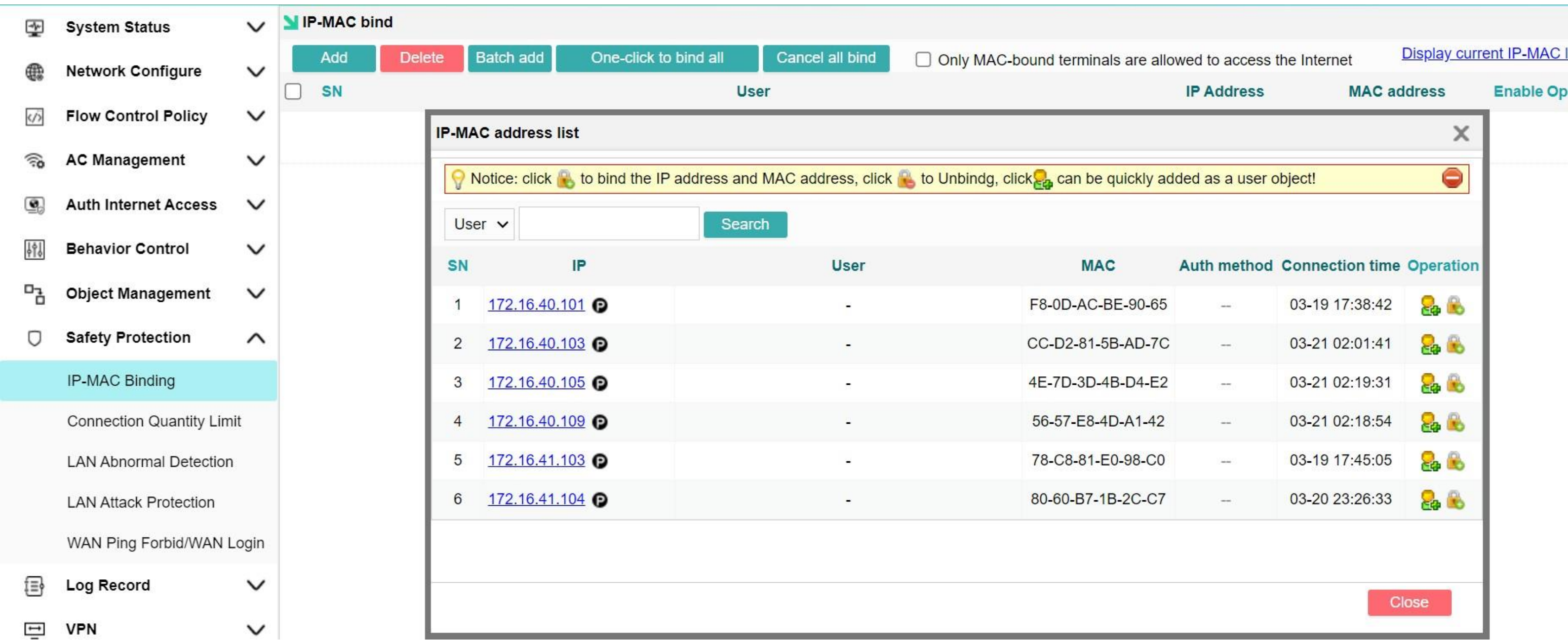


Start address:
End address:
Protocol: TCP/UDP
Start port:
End port:
App name: 11dota

3. 8. Safety Protection

IP-MAC Banding

After the IP-MAC is bound, the IP address cannot be modified at will, so it can avoid IP conflicts that affect other users' normal Internet access.



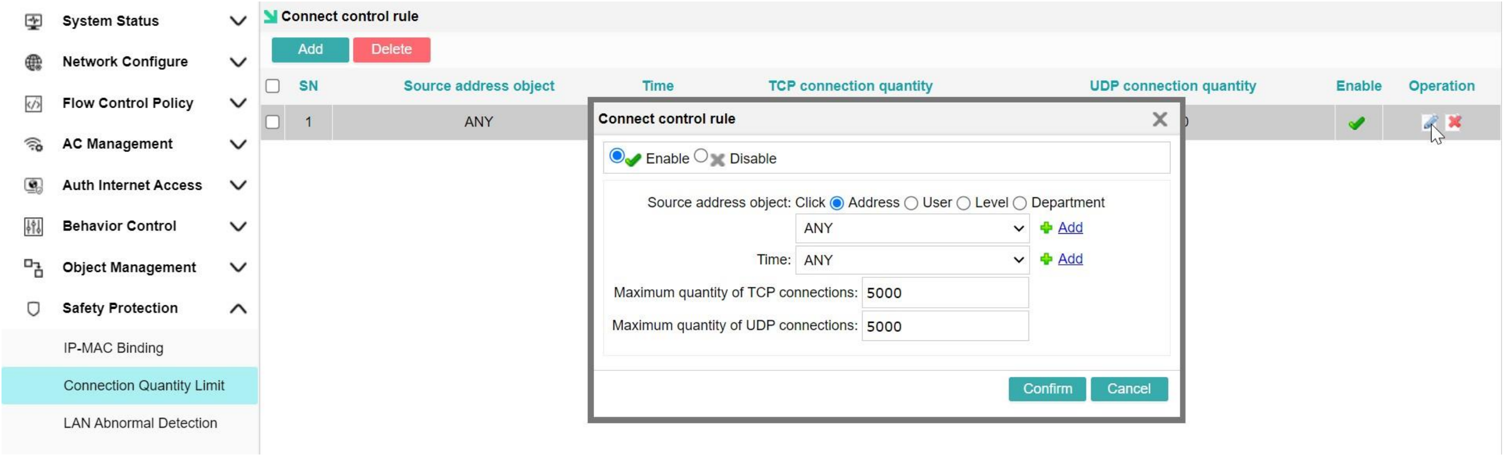
□ Only MAC-bound terminals are allowed to access the Internet

Notice: click to bind the IP address and MAC address, click to Unbindg, click can be quickly added as a user object!

SN	IP	User	MAC	Auth method	Connection time	Operation
1	172.16.40.101	-	F8-0D-AC-BE-90-65	--	03-19 17:38:42	
2	172.16.40.103	-	CC-D2-81-5B-AD-7C	--	03-21 02:01:41	
3	172.16.40.105	-	4E-7D-3D-4B-D4-E2	--	03-21 02:19:31	
4	172.16.40.109	-	56-57-E8-4D-A1-42	--	03-21 02:18:54	
5	172.16.41.103	-	78-C8-81-E0-98-C0	--	03-19 17:45:05	
6	172.16.41.104	-	80-60-B7-1B-2C-C7	--	03-20 23:26:33	

Connection Quantity Limit

Limit the maximum number of TCP and UDP connections of the source object.



SN	Source address object	Time	TCP connection quantity	UDP connection quantity	Enable	Operation
1	ANY				✓	

● Enable ○ Disable

Source address object: Click ● Address ○ User ○ Level ○ Department
ANY

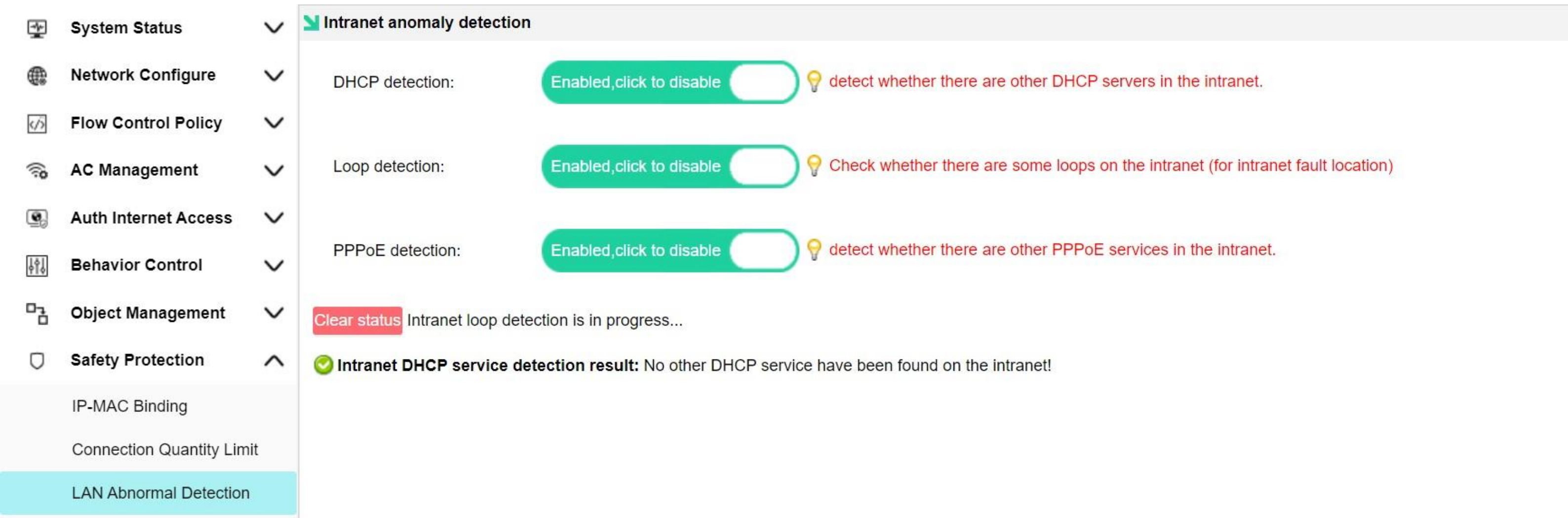
Time: ANY

Maximum quantity of TCP connections: 5000

Maximum quantity of UDP connections: 5000

LAN Abnormal Detection

Enable DHCP detection to search whether there are other DHCP servers in the LAN that cause IP address assignment conflicts.
It is normal for the AC gateway to find the main route when it is used as by pass mode.
Turn on loop detection to determine whether there is link loopback in the LAN switch, which causes a network broadcast storm and slow and unstable Internet access quality.



DHCP detection: Enabled,click to disable — detect whether there are other DHCP servers in the intranet.

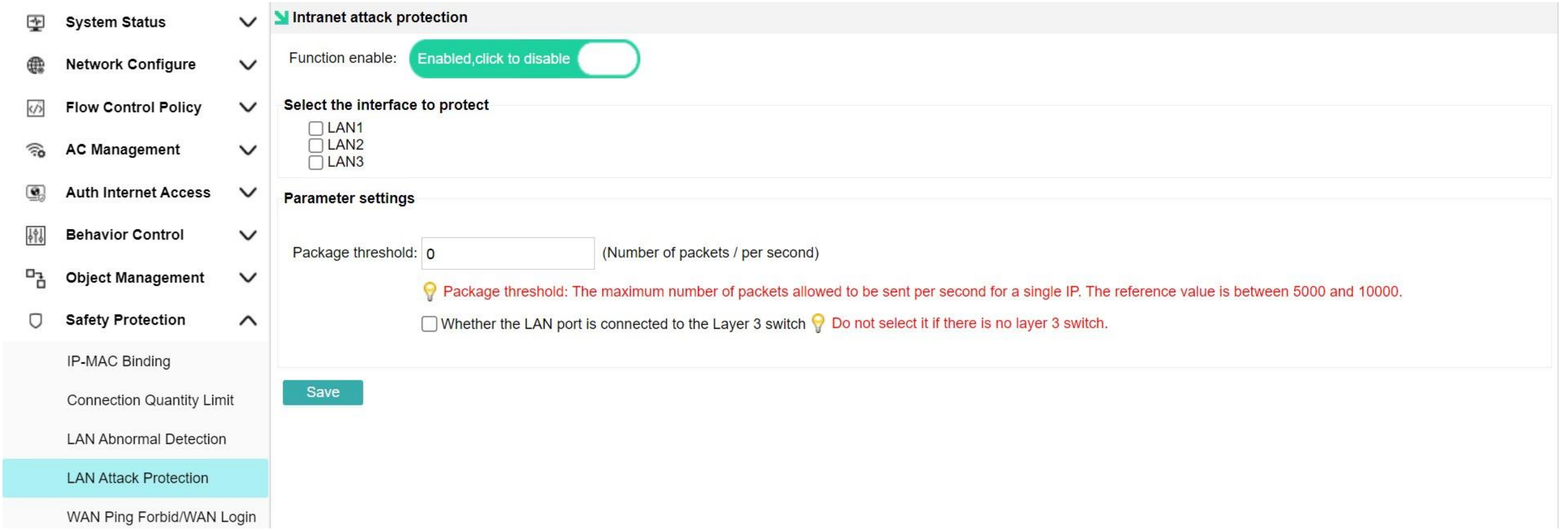
Loop detection: Enabled,click to disable — Check whether there are some loops on the intranet (for intranet fault location)

PPPoE detection: Enabled,click to disable — detect whether there are other PPPoE services in the intranet.

Clear status Intranet loop detection is in progress...

✓ **Intranet DHCP service detection result:** No other DHCP service have been found on the intranet!

LAN Attack Protection



Function enable: Enabled,click to disable

Select the interface to protect

□ LAN1
□ LAN2
□ LAN3

Parameter settings

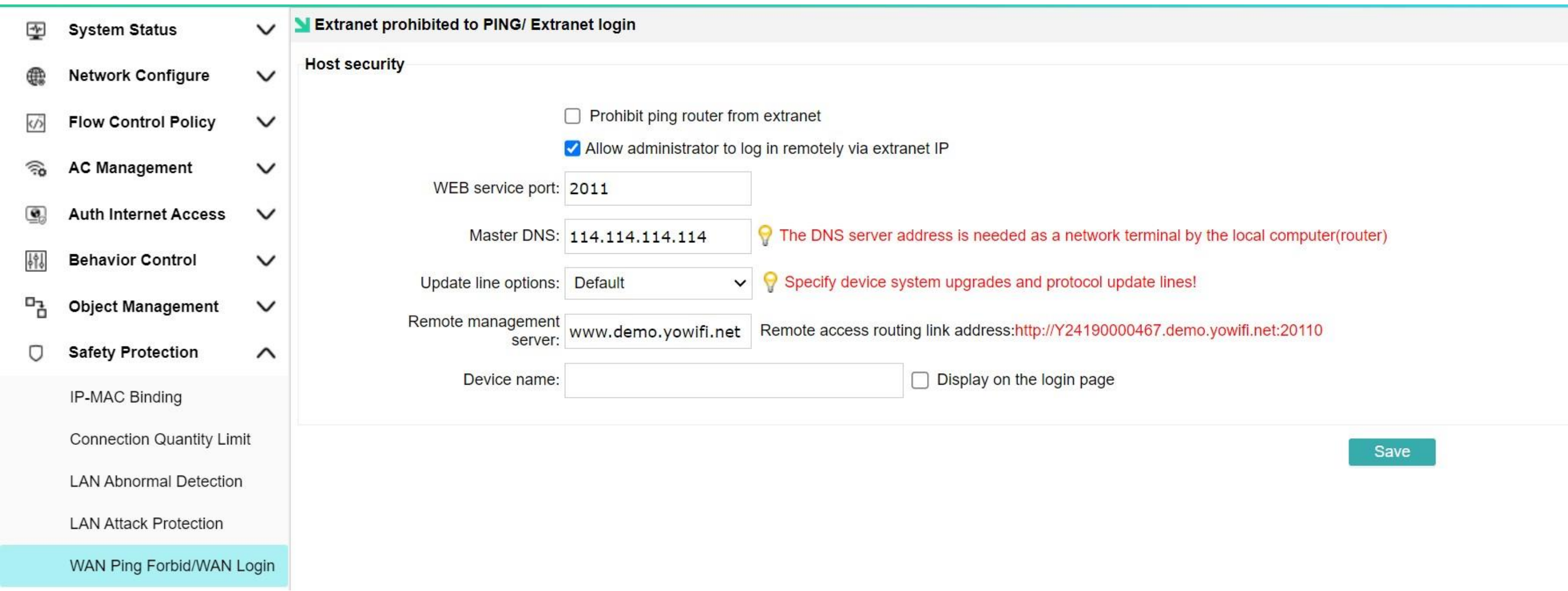
Package threshold: 0 (Number of packets / per second)

Package threshold: The maximum number of packets allowed to be sent per second for a single IP. The reference value is between 5000 and 10000.

□ Whether the LAN port is connected to the Layer 3 switch — Do not select it if there is no layer 3 switch.

WAN Ping Forbid/WAN Login

View remote login parameters and configurations.



Extranet prohibited to PING/ Extranet login

Host security

□ Prohibit ping router from extranet

☑ Allow administrator to log in remotely via extranet IP

WEB service port: 2011

Master DNS: 114.114.114.114 The DNS server address is needed as a network terminal by the local computer(router)

Update line options: Default Specify device system upgrades and protocol update lines!

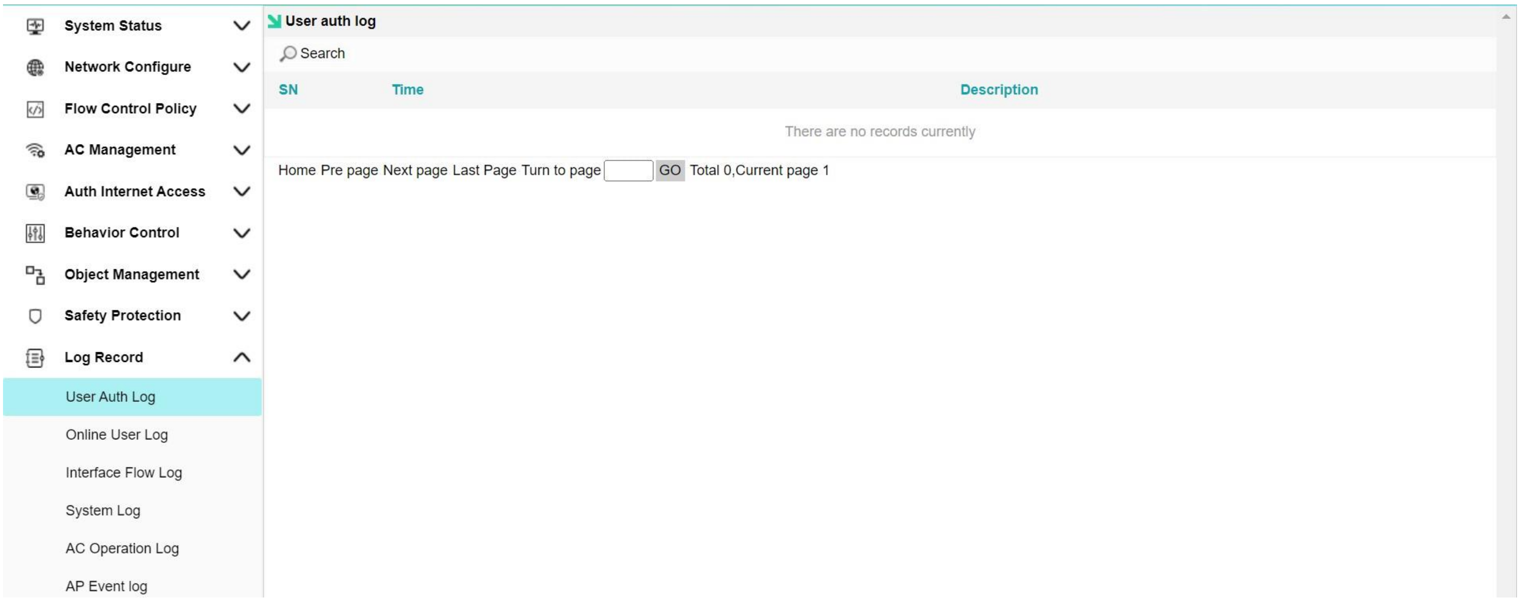
Remote management server: www.demo.yowifi.net Remote access routing link address:http://Y24190000467.demo.yowifi.net:20110

Device name: □ Display on the login page

3. 9. Log Record

User Auth Log

View users online/ offline records.

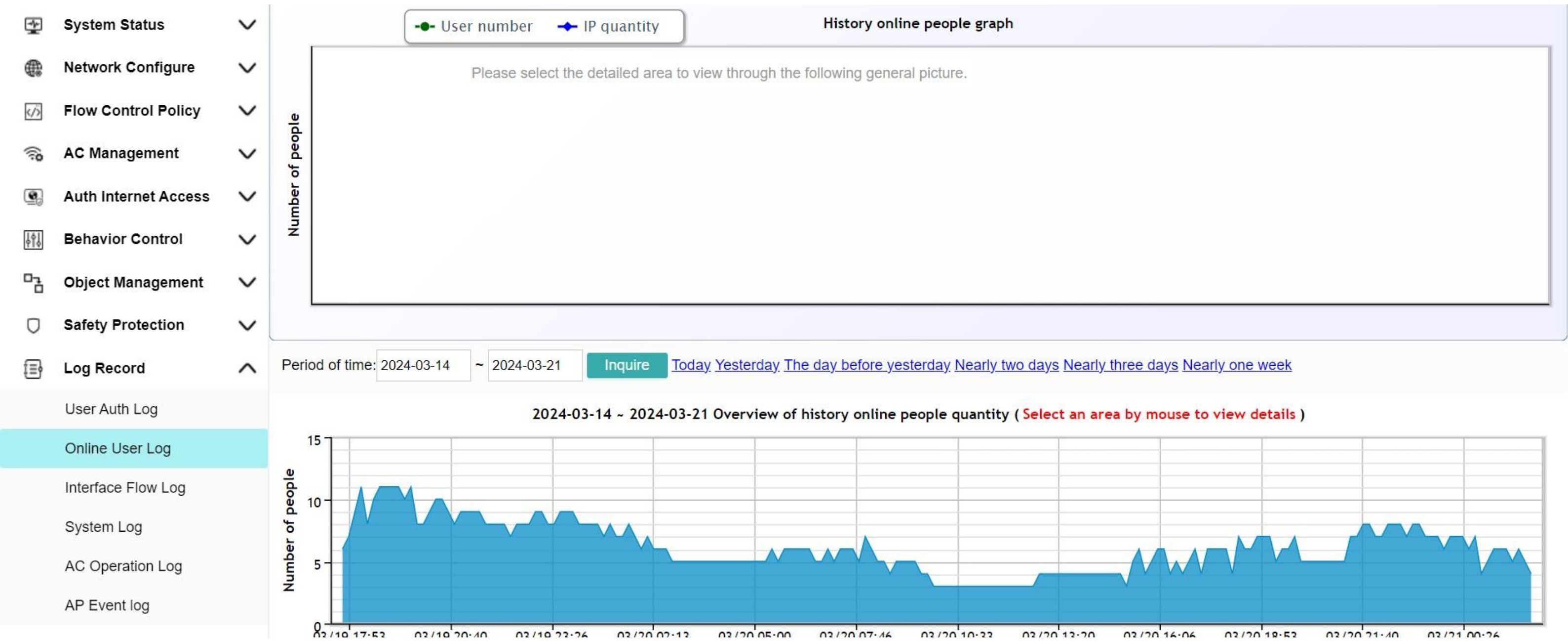


User auth log

SN	Time	Description
There are no records currently		

Total 0,Current page 1

Online User Log

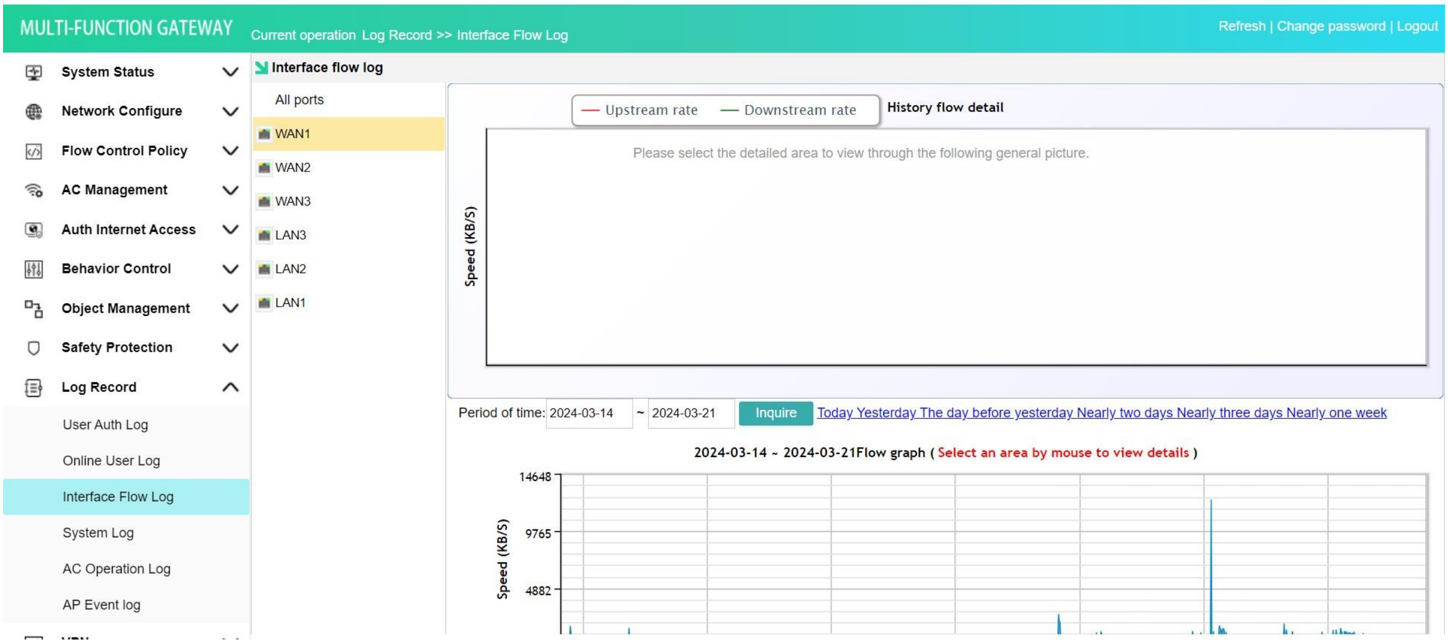


Please select the detailed area to view through the following general picture.

Period of time: 2024-03-14 ~ 2024-03-21

2024-03-14 ~ 2024-03-21 Overview of history online people quantity (Select an area by mouse to view details)

Interface Flow Log



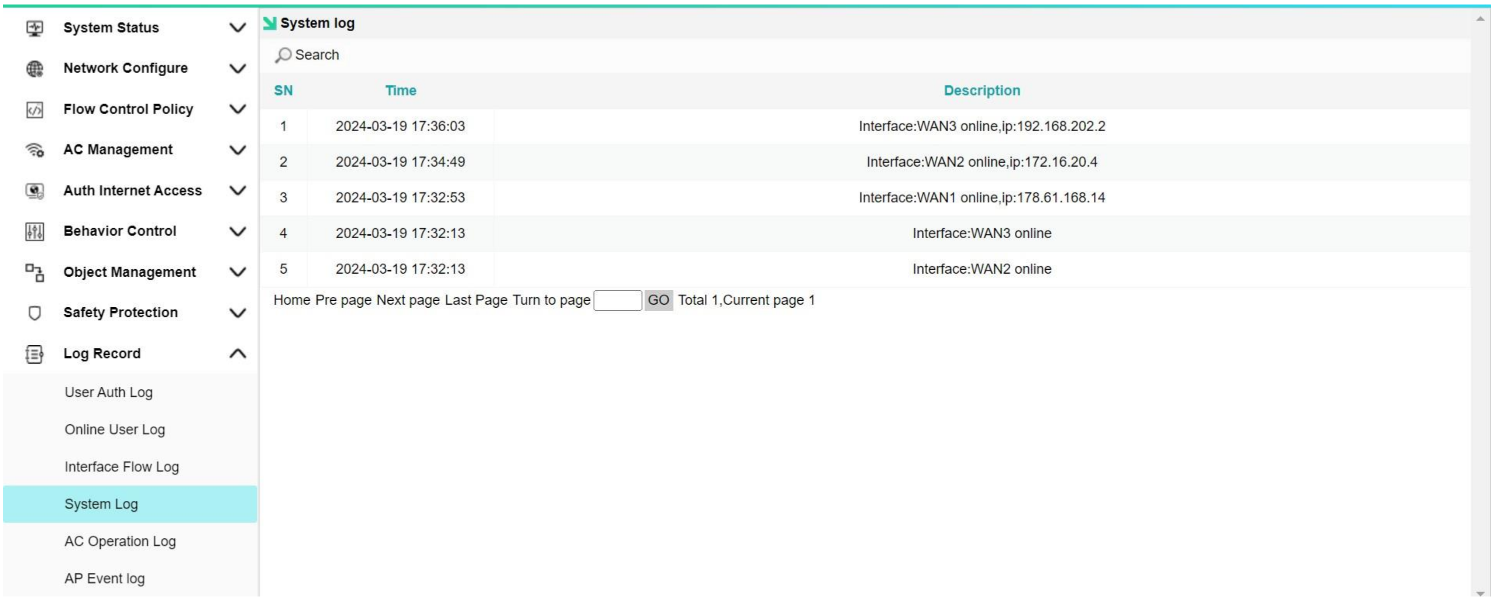
Current operation Log Record >> Interface Flow Log

Please select the detailed area to view through the following general picture.

Period of time: 2024-03-14 ~ 2024-03-21

2024-03-14 ~ 2024-03-21Flow graph (Select an area by mouse to view details)

System Log



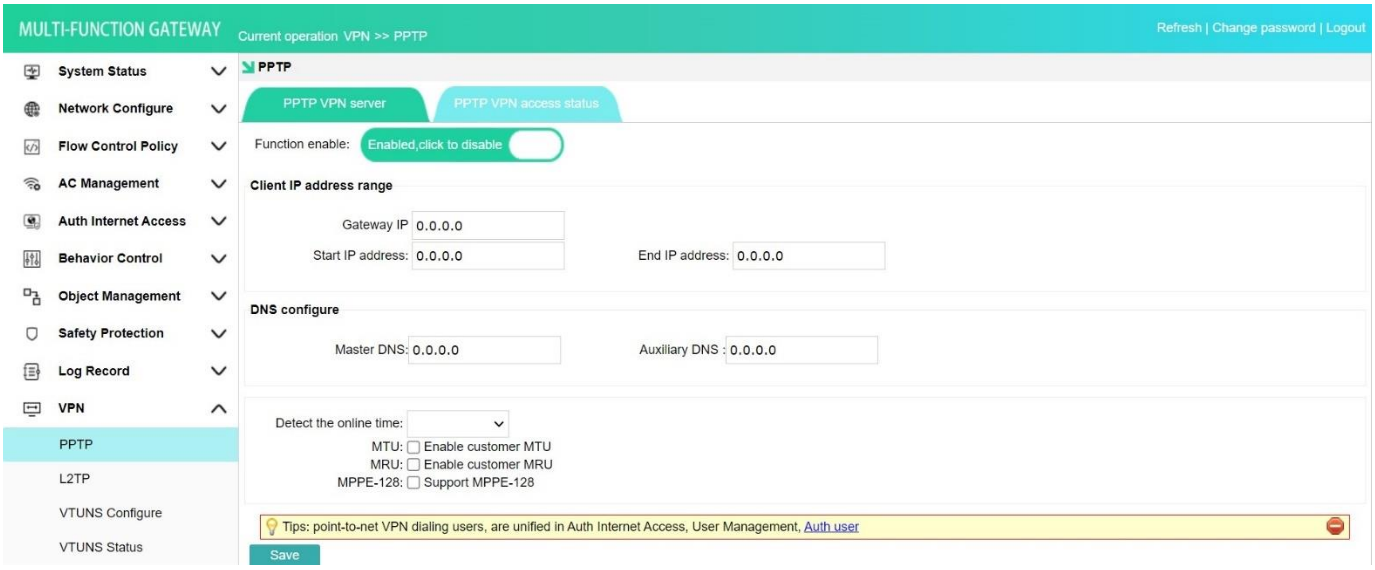
SN	Time	Description
1	2024-03-19 17:36:03	Interface:WAN3 online,ip:192.168.202.2
2	2024-03-19 17:34:49	Interface:WAN2 online,ip:172.16.20.4
3	2024-03-19 17:32:53	Interface:WAN1 online,ip:178.61.168.14
4	2024-03-19 17:32:13	Interface:WAN3 online
5	2024-03-19 17:32:13	Interface:WAN2 online

Home Pre page Next page Last Page Turn to page GO Total 1,Current page 1

3. 10. VPN

PPTP

To use this function, AC is required as the primary route, and the WAN interface is connected to the public IP provided by the external network for the operator.
Gateway IP and address pool are set according to the actual needs of DNS.



Current operation VPN >> PPTP

Function enable: Enabled,click to disable

Client IP address range

Gateway IP 0.0.0.0

Start IP address: 0.0.0.0 End IP address: 0.0.0.0

DNS configure

Master DNS: 0.0.0.0 Auxiliary DNS : 0.0.0.0

Detect the online time:

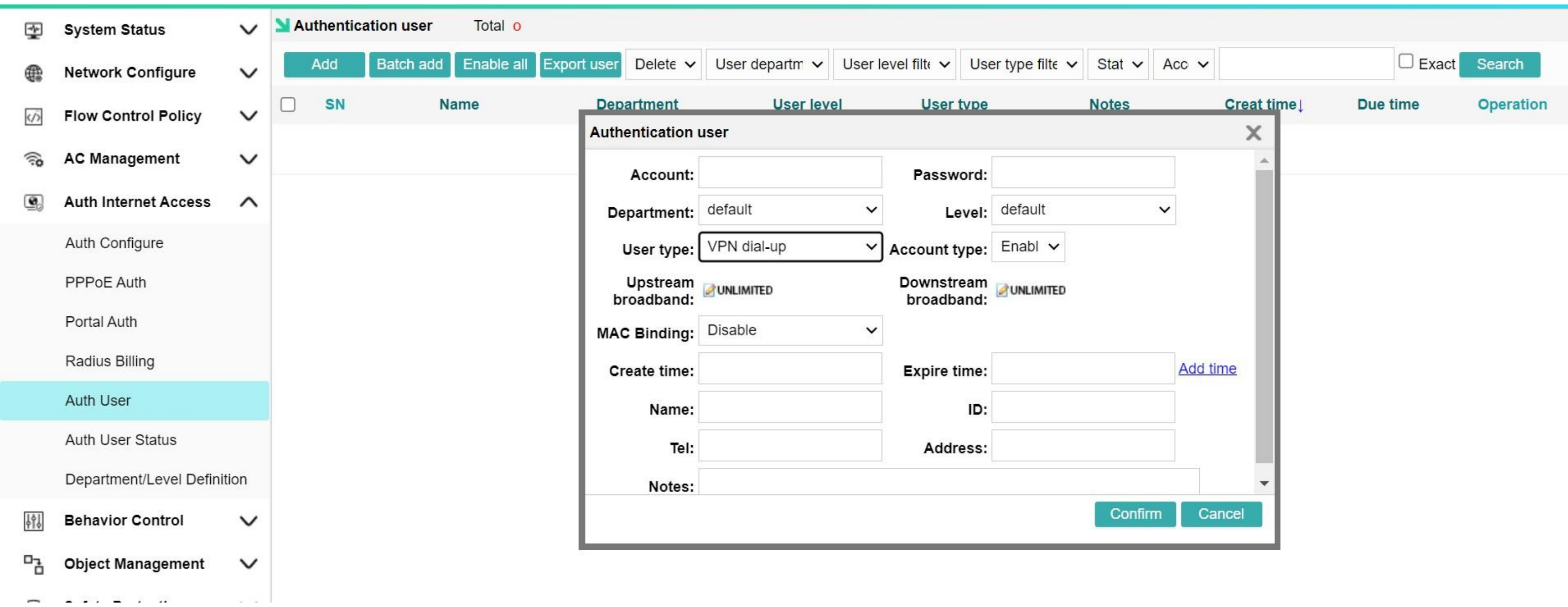
MTU: □ Enable customer MTU

MRU: □ Enable customer MRU

MPPE-128: □ Support MPPE-128

Tips: point-to-net VPN dialing users, are unified in Auth Internet Access, User Management, Auth user

Click Authentication User to jump to Create VPN Authentication User

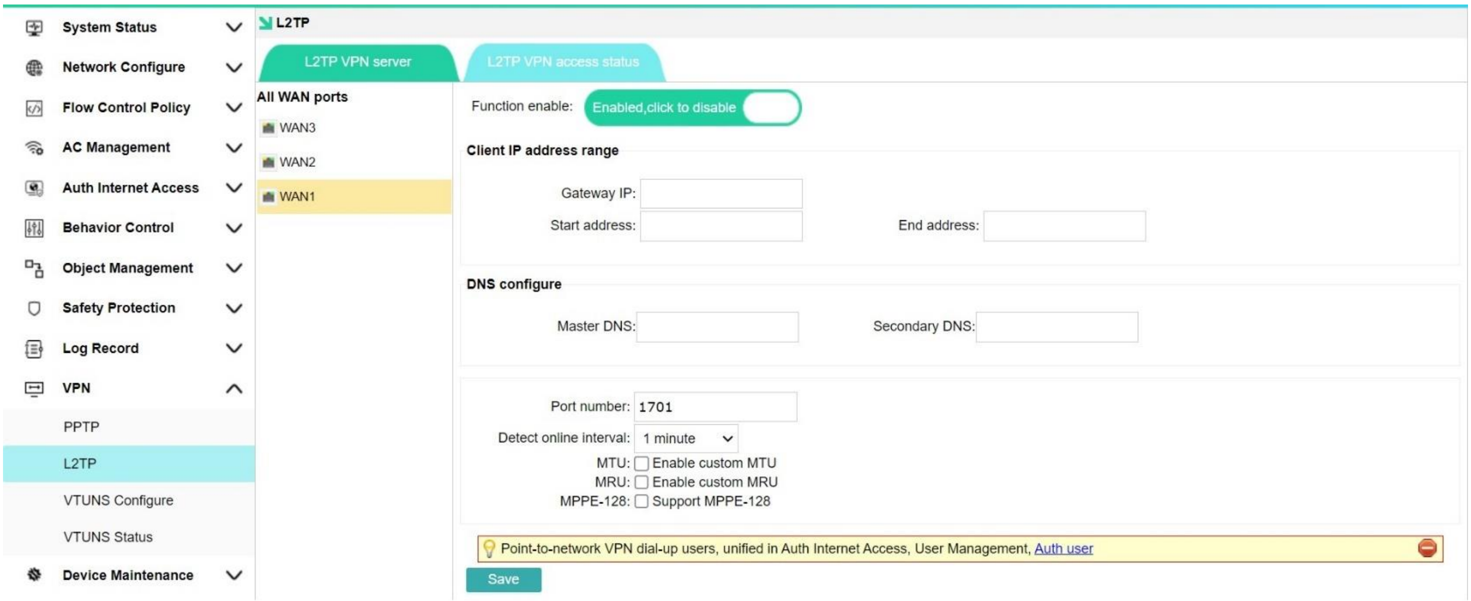


Authentication user

Account:
Password:
Department: default
Level: default
User type: VPN dial-up
Account type: Enabl
Upstream broadband: UNLIMITED
Downstream broadband: UNLIMITED
MAC Binding: Disable
Create time:
Expire time: Add time
Name:
ID:
Tel:
Address:
Notes:

L2TP

To use this function, AC is required as the primary route, and the WAN interface is connected to the public IP provided by the external network for the operator.
Gateway IP and address pool are set according to the actual needs of DNS.



Function enable: Enabled,click to disable

Client IP address range

Gateway IP:
Start address:
End address:

DNS configure

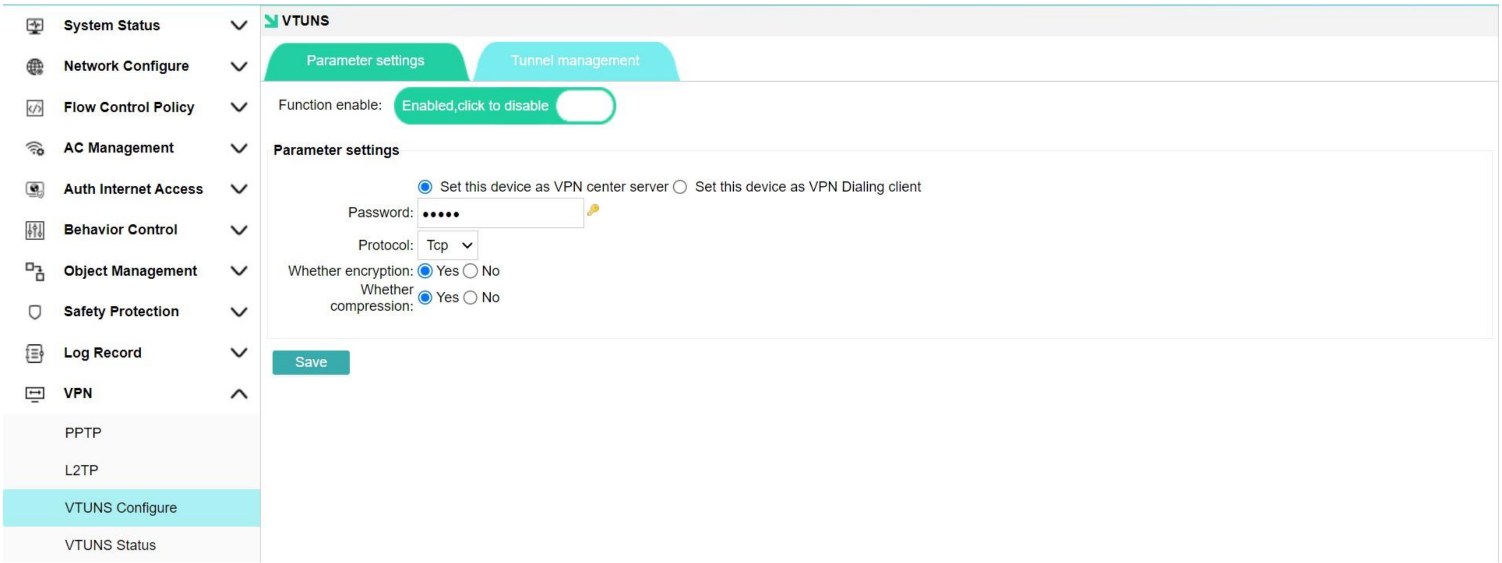
Master DNS:
Secondary DNS:

Port number: 1701
Detect online interval: 1 minute
MTU: □ Enable custom MTU
MRU: □ Enable custom MRU
MPPE-128: □ Support MPPE-128

Point-to-network VPN dial-up users, unified in Auth Internet Access, User Management, Auth user

VTUNS

The network to network virtual channel over TCP/IP is established for the combination of two LANs. The one with good performance is set as the server. The LAN segments on both sides cannot be the same. The server needs to have a public IP address.



Function enable: Enabled,click to disable

Parameter settings

● Set this device as VPN center server ○ Set this device as VPN Dialing client

Password: •••••

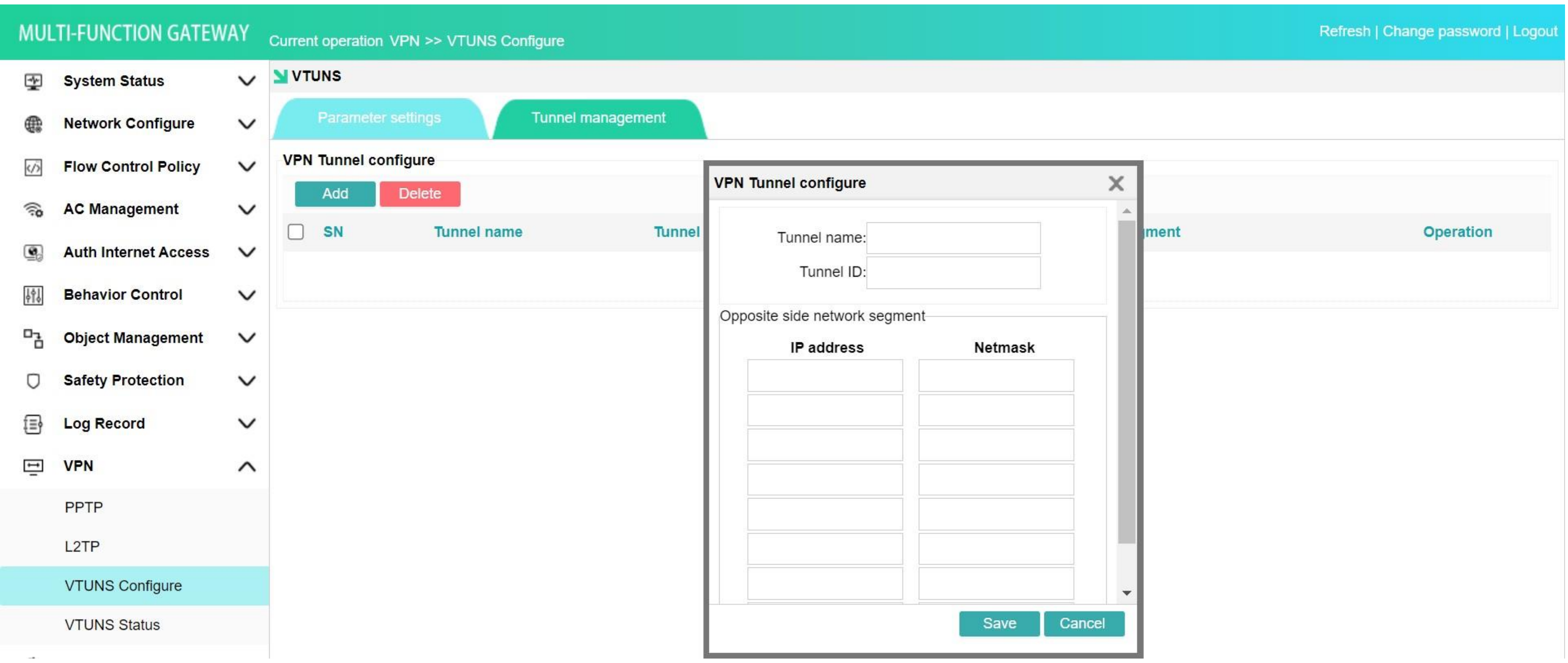
Protocol: Tcp

Whether encryption: ● Yes ○ No

Whether compression: ● Yes ○ No

Save

Tunnel management: Add the custom tunnel name and tunnel ID, and fill in the intranet segment of the VPN client, such as 192.168.1.0 and 255.255.255.0. Note that the tunnel name and tunnel ID must be consistent between the server and the client



VPN Tunnel configure

□	SN	Tunnel name	Tunnel	ment	Operation

VPN Tunnel configure

Tunnel name:

Tunnel ID:

Opposite side network segment

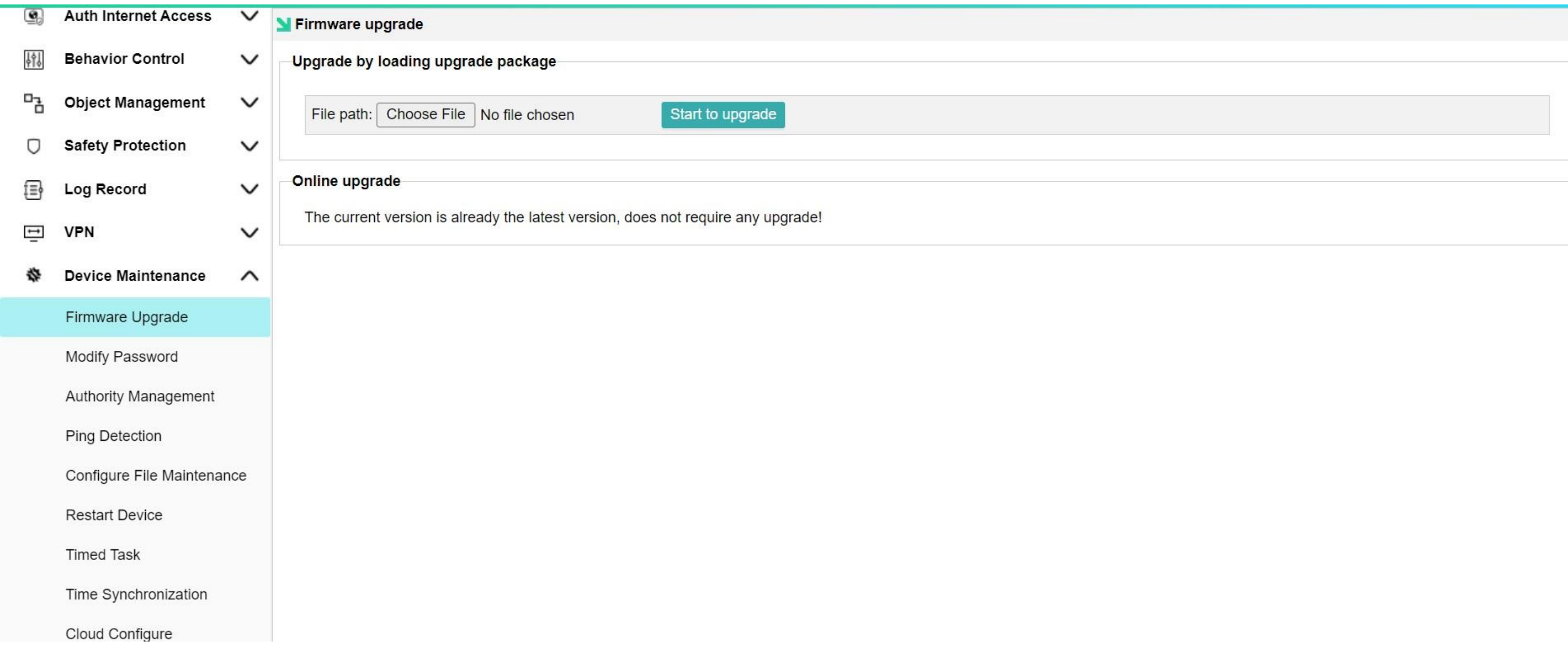
IP address	Netmask

Save Cancel

3. 11. Device Maintenance

Firmware Upgrade

Online upgrade, or select a specific local firmware upgrade

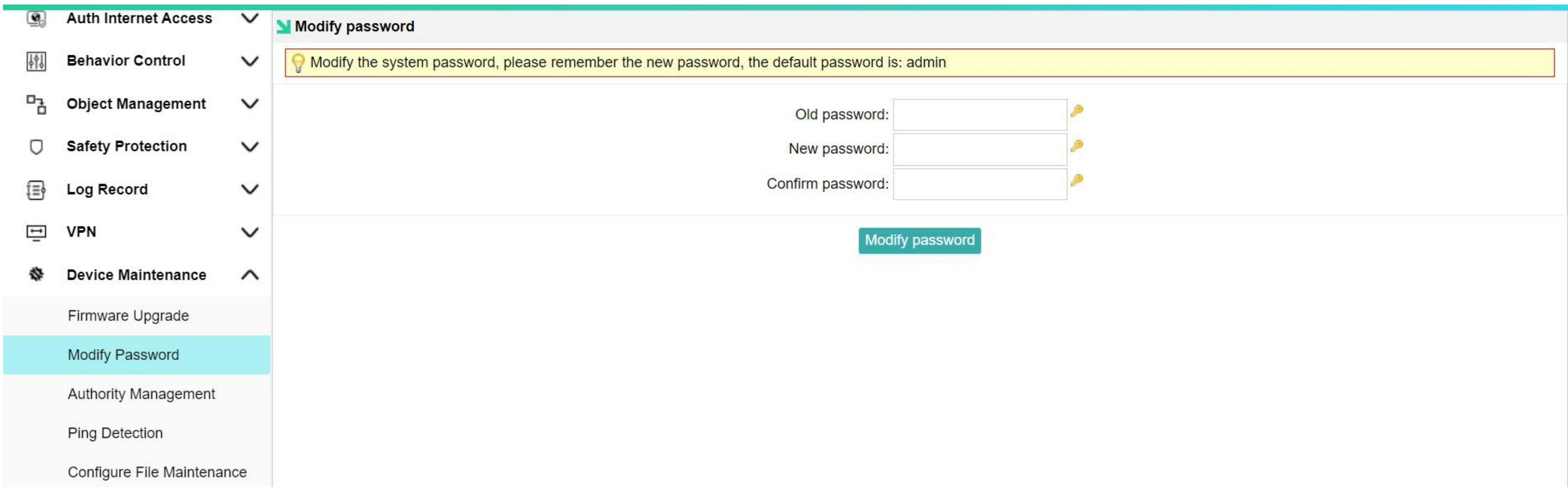


File path: No file chosen

The current version is already the latest version, does not require any upgrade!

Modify Password

Here you modify administrator user login password



Modify the system password, please remember the new password, the default password is: admin

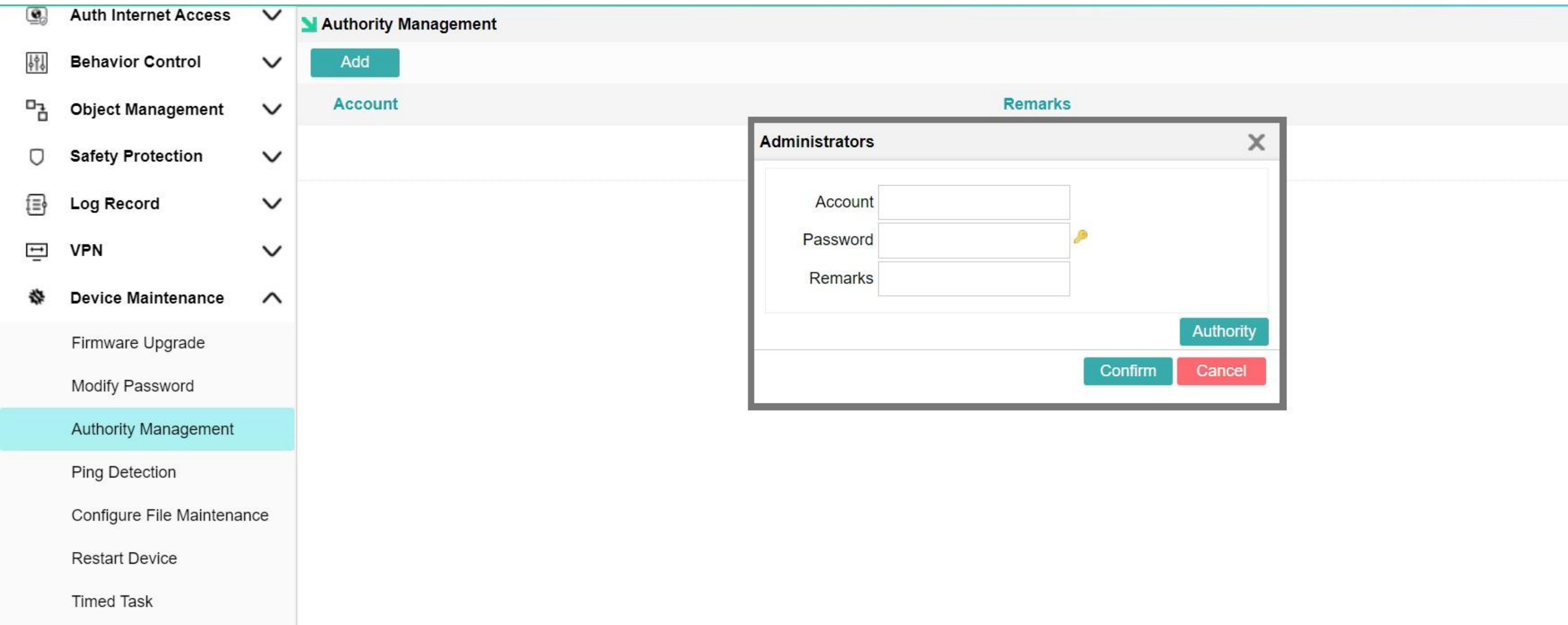
Old password:

New password:

Confirm password:

Authority Management

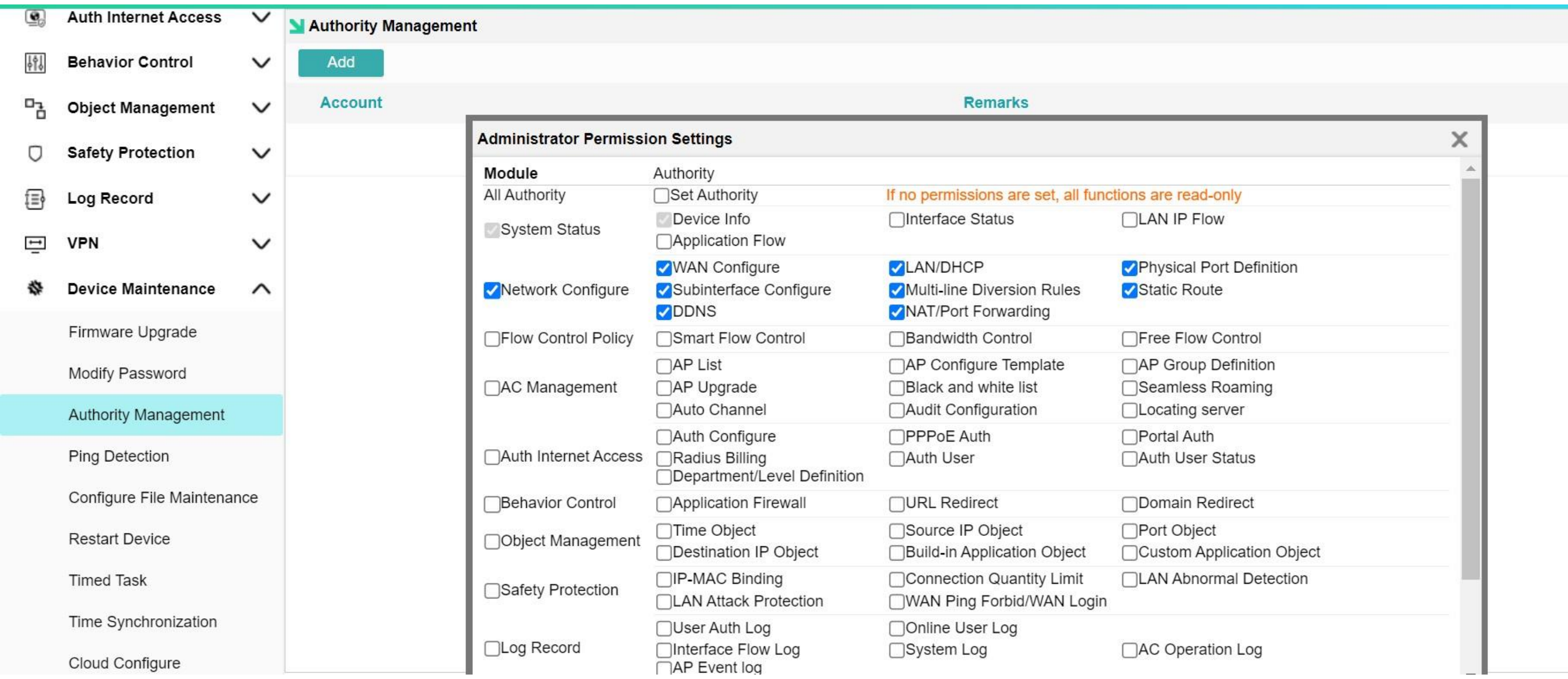
Here you can create multiple users with custom permissions as shown below



Account

Password

Remarks

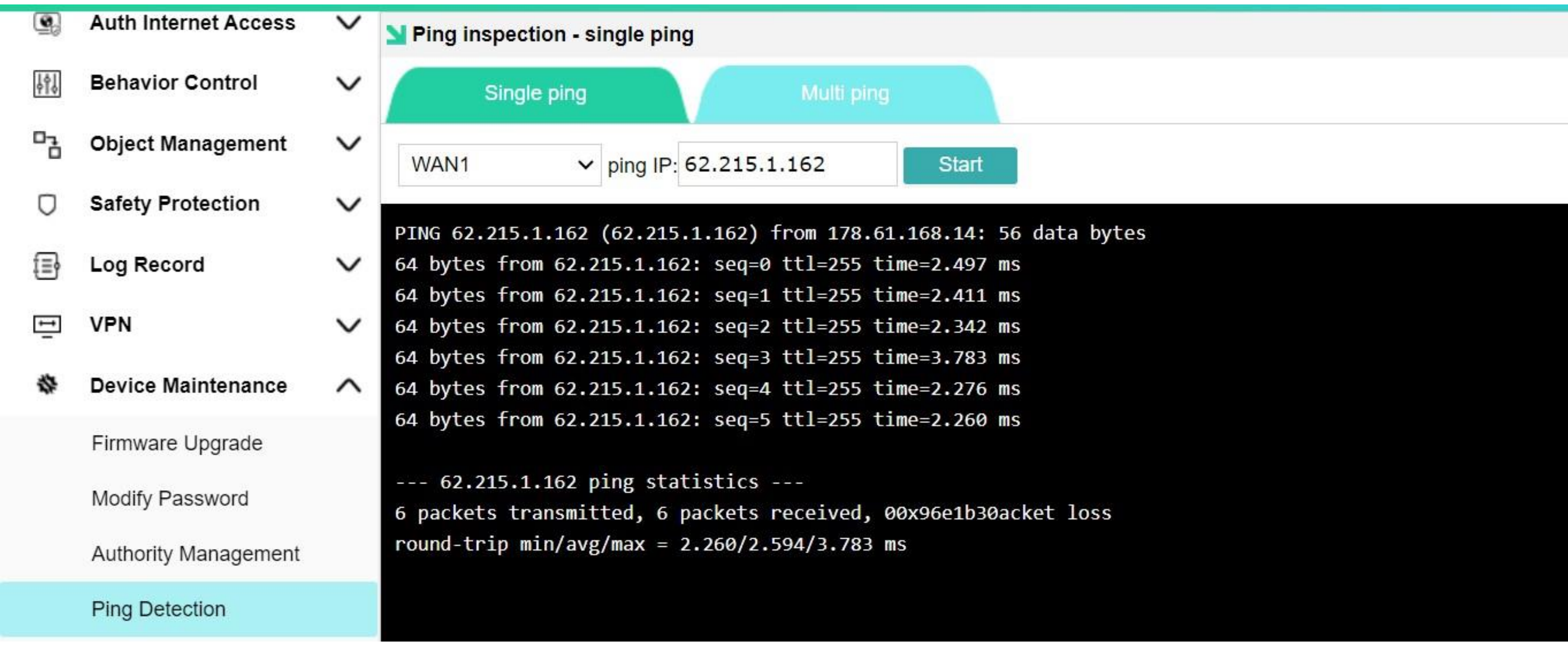


Administrator Permission Settings

Module	Authority		
All Authority	□Set Authority	If no permissions are set, all functions are read-only	
☑System Status	☑Device Info □Application Flow	□Interface Status	□LAN IP Flow
☑Network Configure	☑WAN Configure ☑Subinterface Configure ☑DDNS	☑LAN/DHCP ☑Multi-line Diversion Rules ☑NAT/Port Forwarding	☑Physical Port Definition ☑Static Route
□Flow Control Policy	□Smart Flow Control	□Bandwidth Control	□Free Flow Control
□AC Management	□AP List □AP Upgrade □Auto Channel	□AP Configure Template □Black and white list □Audit Configuration	□AP Group Definition □Seamless Roaming □Locating server
□Auth Internet Access	□Auth Configure □Radius Billing □Department/Level Definition	□PPPoE Auth □Auth User	□Portal Auth □Auth User Status
□Behavior Control	□Application Firewall	□URL Redirect	□Domain Redirect
□Object Management	□Time Object □Destination IP Object	□Source IP Object □Build-in Application Object	□Port Object □Custom Application Object
□Safety Protection	□IP-MAC Binding □LAN Attack Protection	□Connection Quantity Limit □WAN Ping Forbid/WAN Login	□LAN Abnormal Detection
□Log Record	□User Auth Log □Interface Flow Log □AP Event log	□Online User Log □System Log	□AC Operation Log

Ping Detection

Use to check whether there is a path between AC and the specified IP.

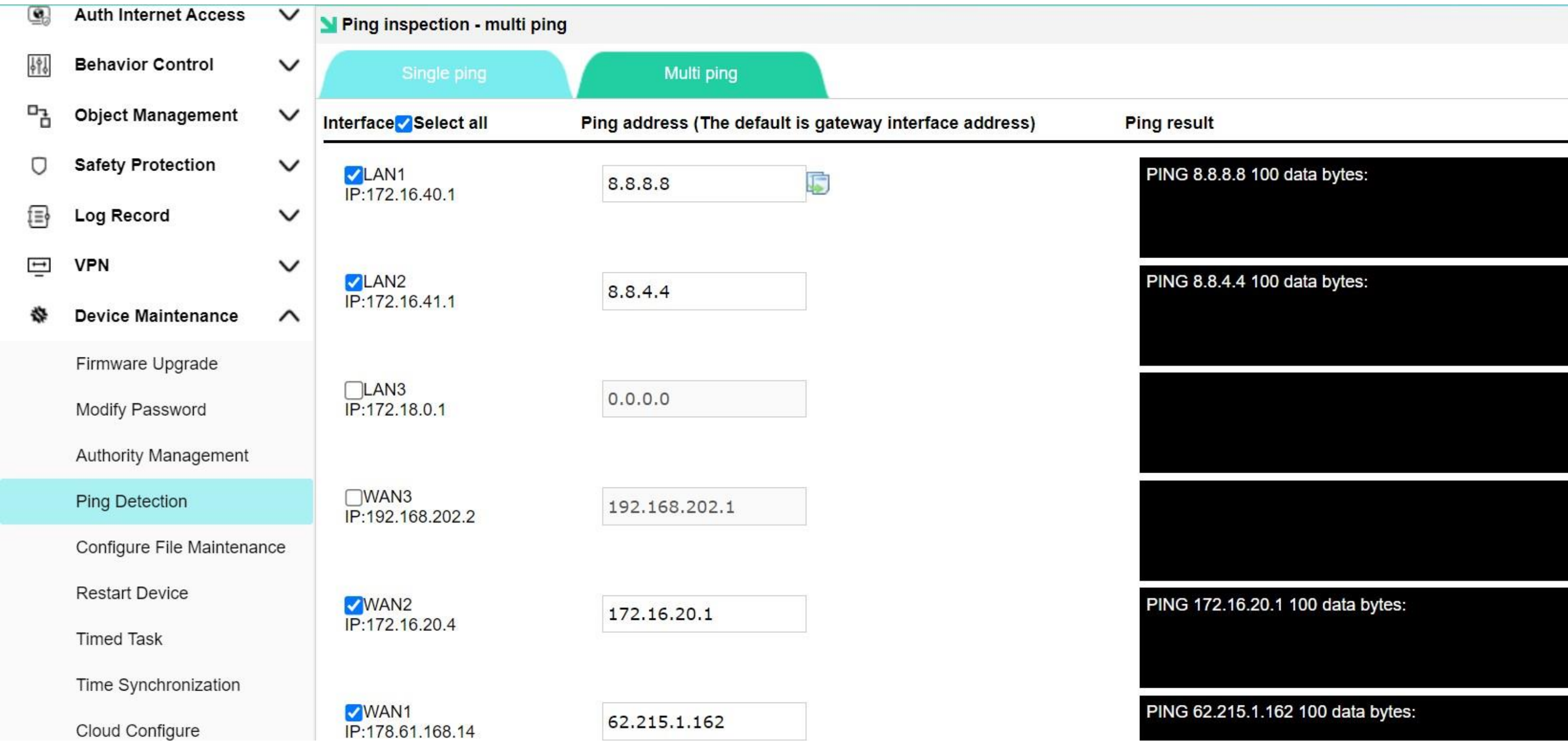


WAN1 ping IP: 62.215.1.162

```
PING 62.215.1.162 (62.215.1.162) from 178.61.168.14: 56 data bytes
64 bytes from 62.215.1.162: seq=0 ttl=255 time=2.497 ms
64 bytes from 62.215.1.162: seq=1 ttl=255 time=2.411 ms
64 bytes from 62.215.1.162: seq=2 ttl=255 time=2.342 ms
64 bytes from 62.215.1.162: seq=3 ttl=255 time=3.783 ms
64 bytes from 62.215.1.162: seq=4 ttl=255 time=2.276 ms
64 bytes from 62.215.1.162: seq=5 ttl=255 time=2.260 ms

--- 62.215.1.162 ping statistics ---
6 packets transmitted, 6 packets received, 00x96e1b30acket loss
round-trip min/avg/max = 2.260/2.594/3.783 ms
```

Multi Ping

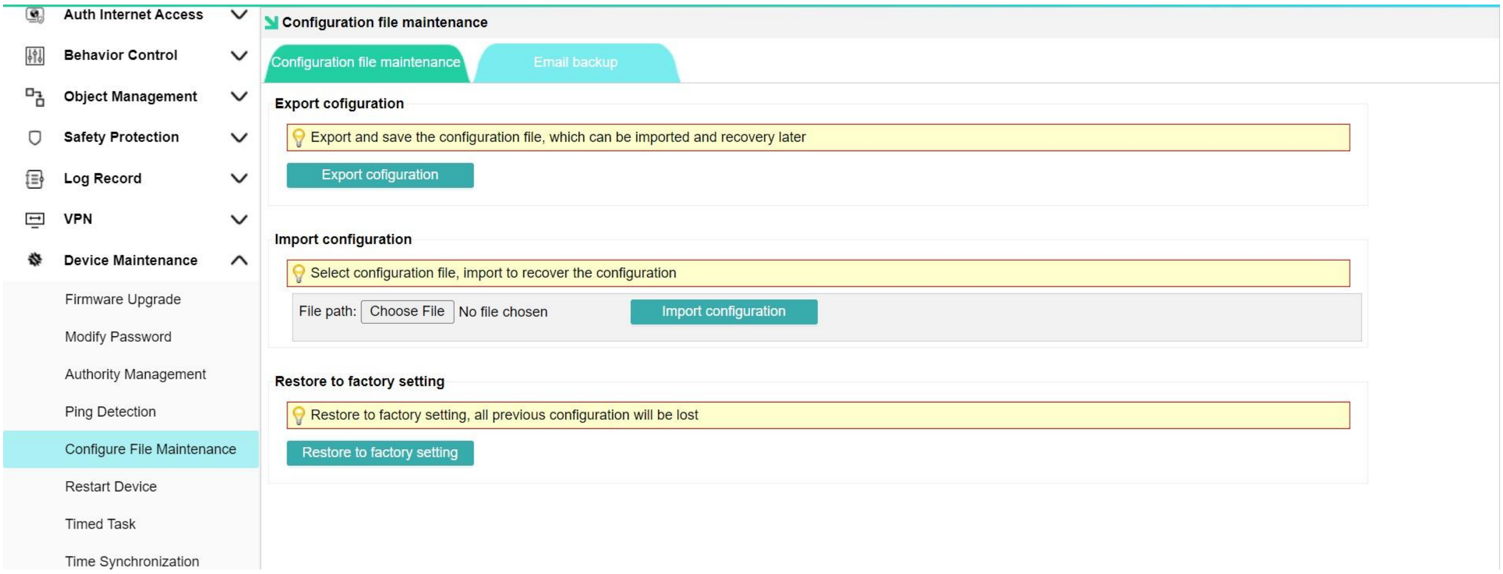


Ping inspection - multi ping

Interface ☑Select all	Ping address (The default is gateway interface address)	Ping result
☑LAN1 IP:172.16.40.1	8.8.8.8	PING 8.8.8.8 100 data bytes:
☑LAN2 IP:172.16.41.1	8.8.4.4	PING 8.8.4.4 100 data bytes:
□LAN3 IP:172.18.0.1	0.0.0.0	
□WAN3 IP:192.168.202.2	192.168.202.1	
☑WAN2 IP:172.16.20.4	172.16.20.1	PING 172.16.20.1 100 data bytes:
☑WAN1 IP:178.61.168.14	62.215.1.162	PING 62.215.1.162 100 data bytes:

Configure File Maintenance

Export and import the configuration information of the gateway and restore it to the factory.



Configuration file maintenance

Export cofiguration

Export and save the configuration file, which can be imported and recovery later

Import configuration

Select configuration file, import to recover the configuration

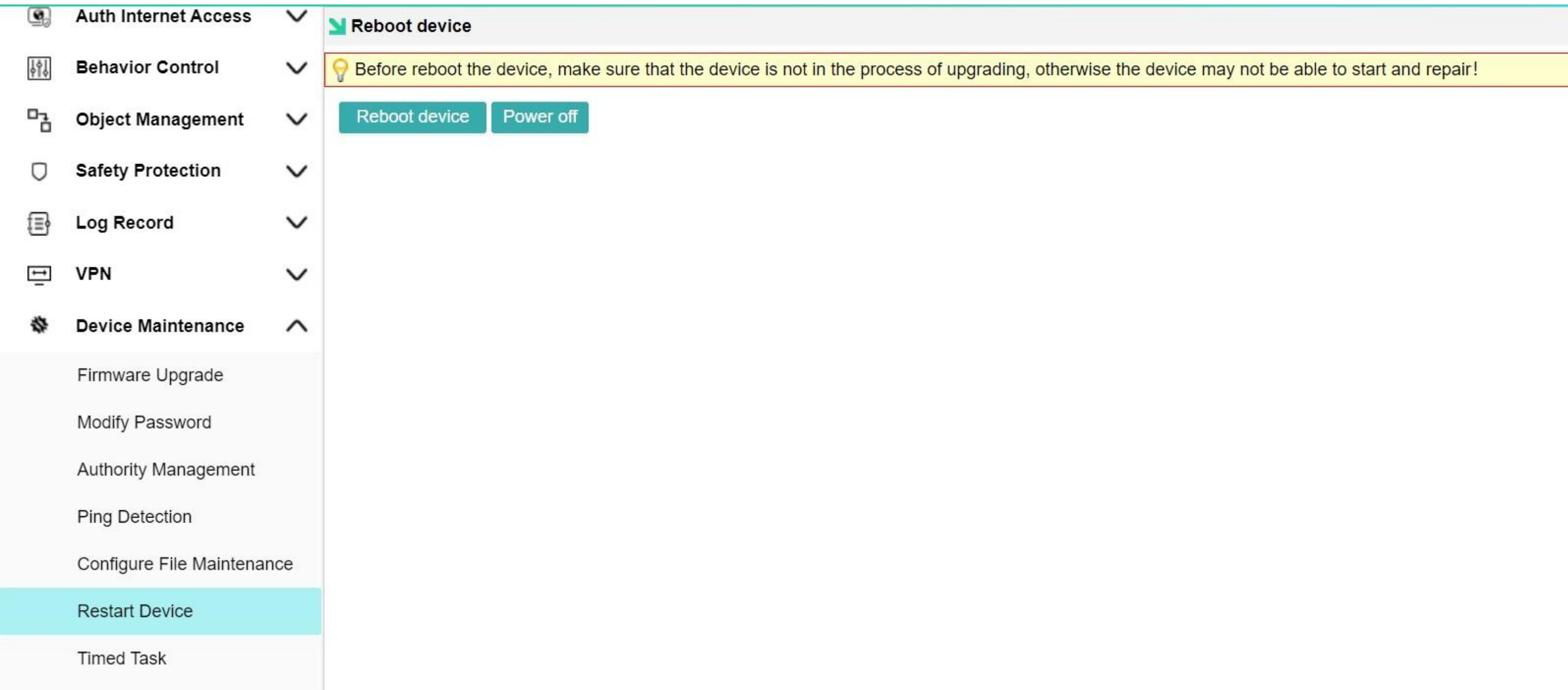
File path: Choose File No file chosen

Restore to factory setting

Restore to factory setting, all previous configuration will be lost

Restart Device

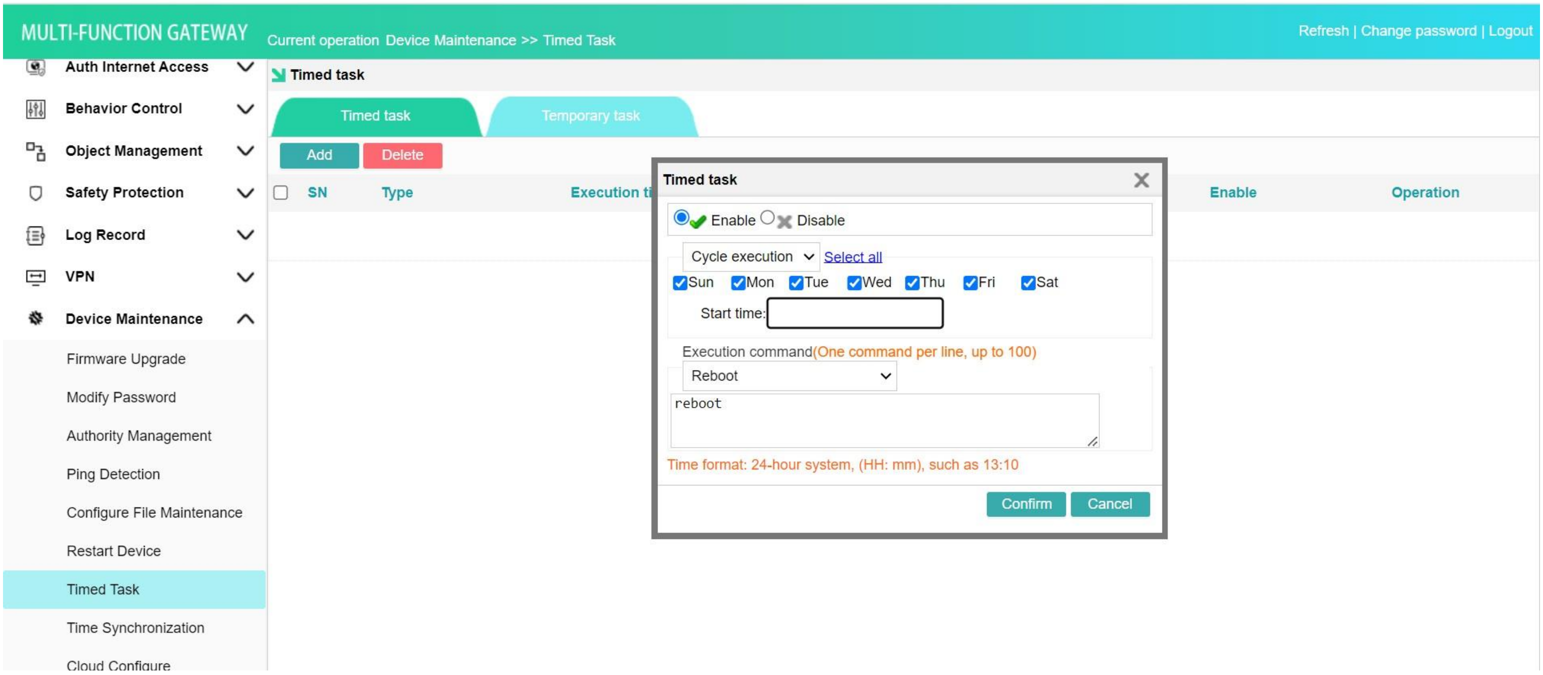
From here you can restart XT-2500AC or shutdown the device



Before reboot the device, make sure that the device is not in the process of upgrading, otherwise the device may not be able to start and repair!

Time Task

Set the timing operation of the gateway



● Enable ○ Disable

Cycle execution Select all

☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

Start time:

Execution command(One command per line, up to 100)

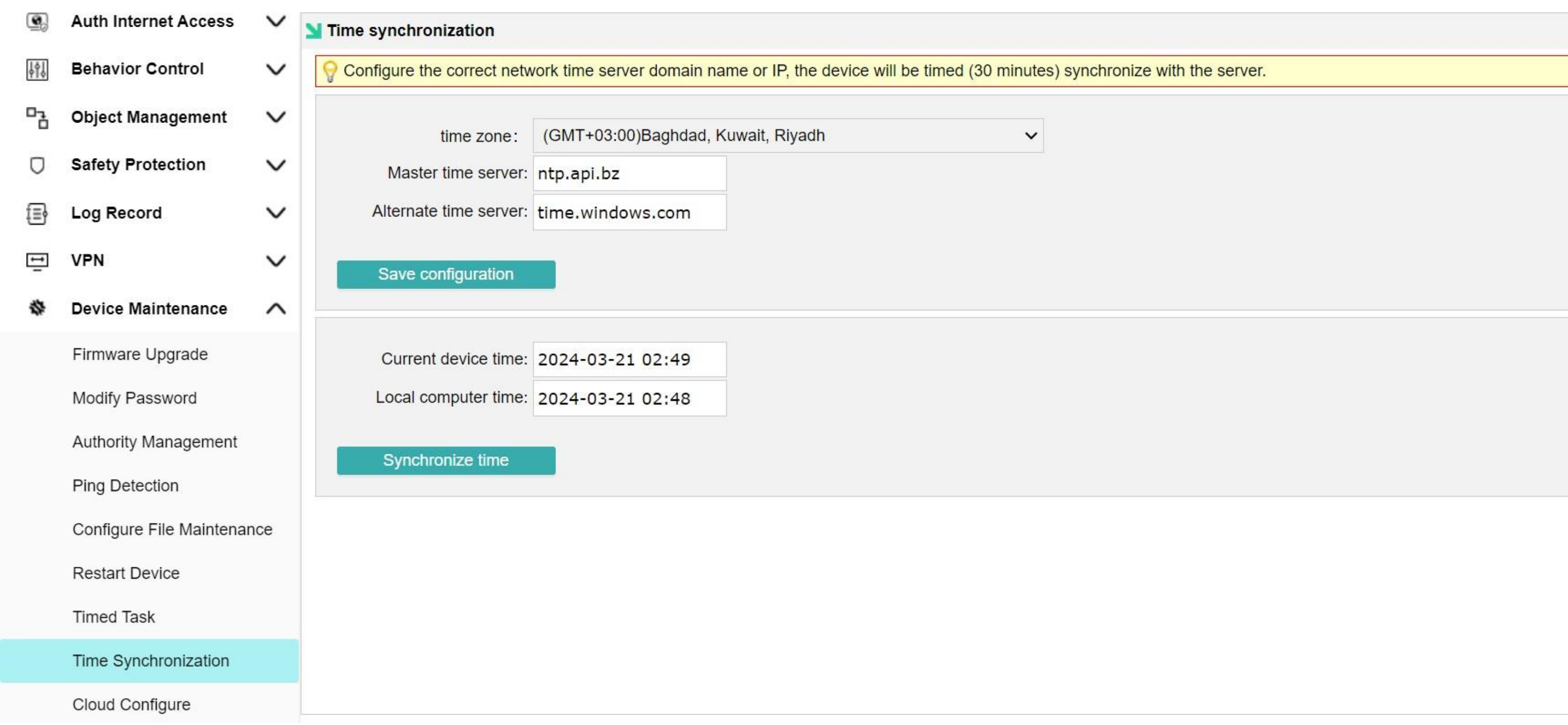
Reboot

```
reboot
```

Time format: 24-hour system, (HH: mm), such as 13:10

Time Synchronization

Different time zones and main time servers can be selected



Time synchronization

Configure the correct network time server domain name or IP, the device will be timed (30 minutes) synchronize with the server.

time zone: (GMT+03:00)Baghdad, Kuwait, Riyadh

Master time server: ntp.api.bz

Alternate time server: time.windows.com

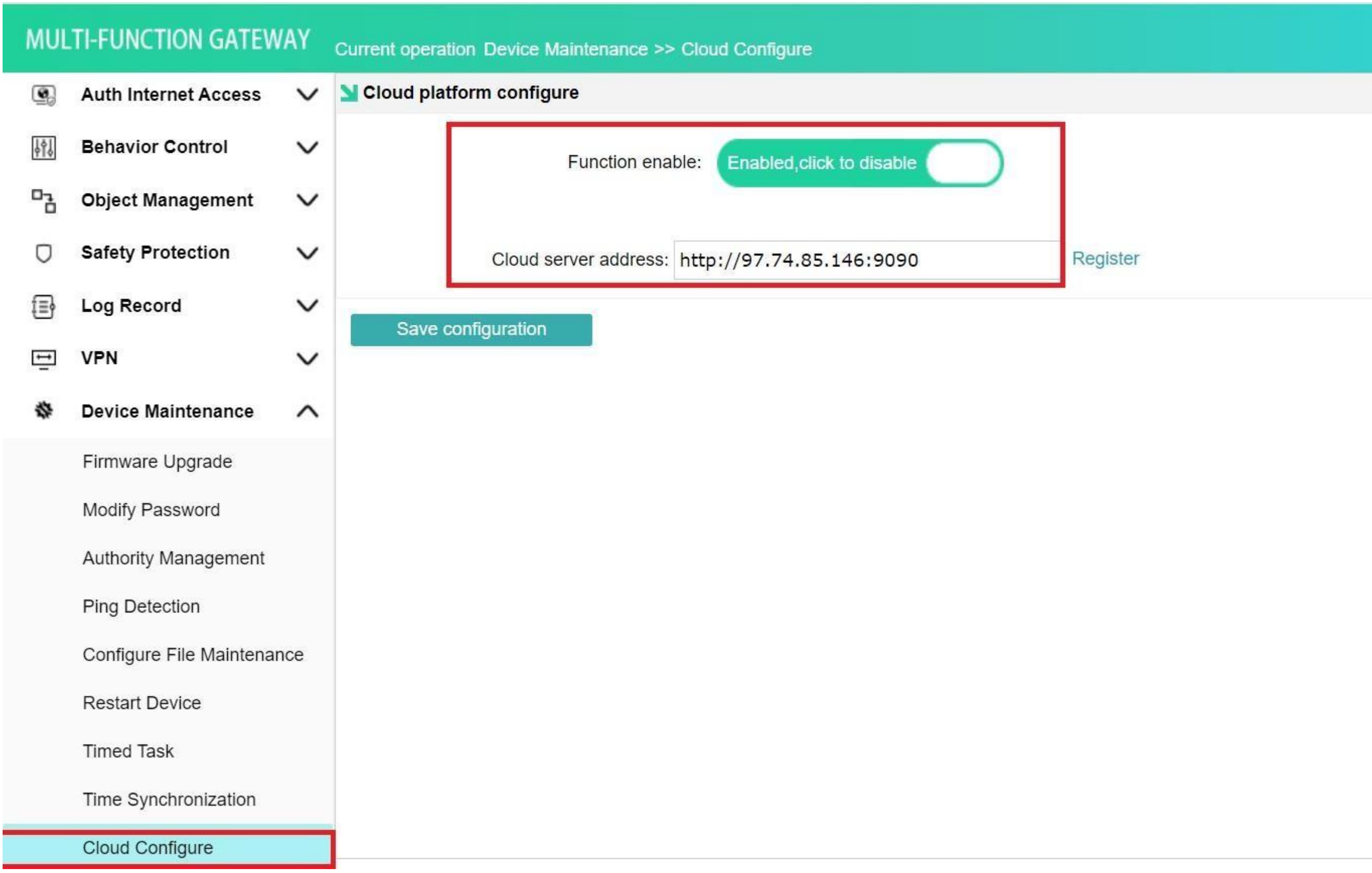
Current device time: 2024-03-21 02:49

Local computer time: 2024-03-21 02:48

Cloud Configure

Cloud configuration will allow you to manage your XT-2500AC remotely.

Create account in the cloud management (http://97.74.85.146:9090/) and Configure cloud management in controller.

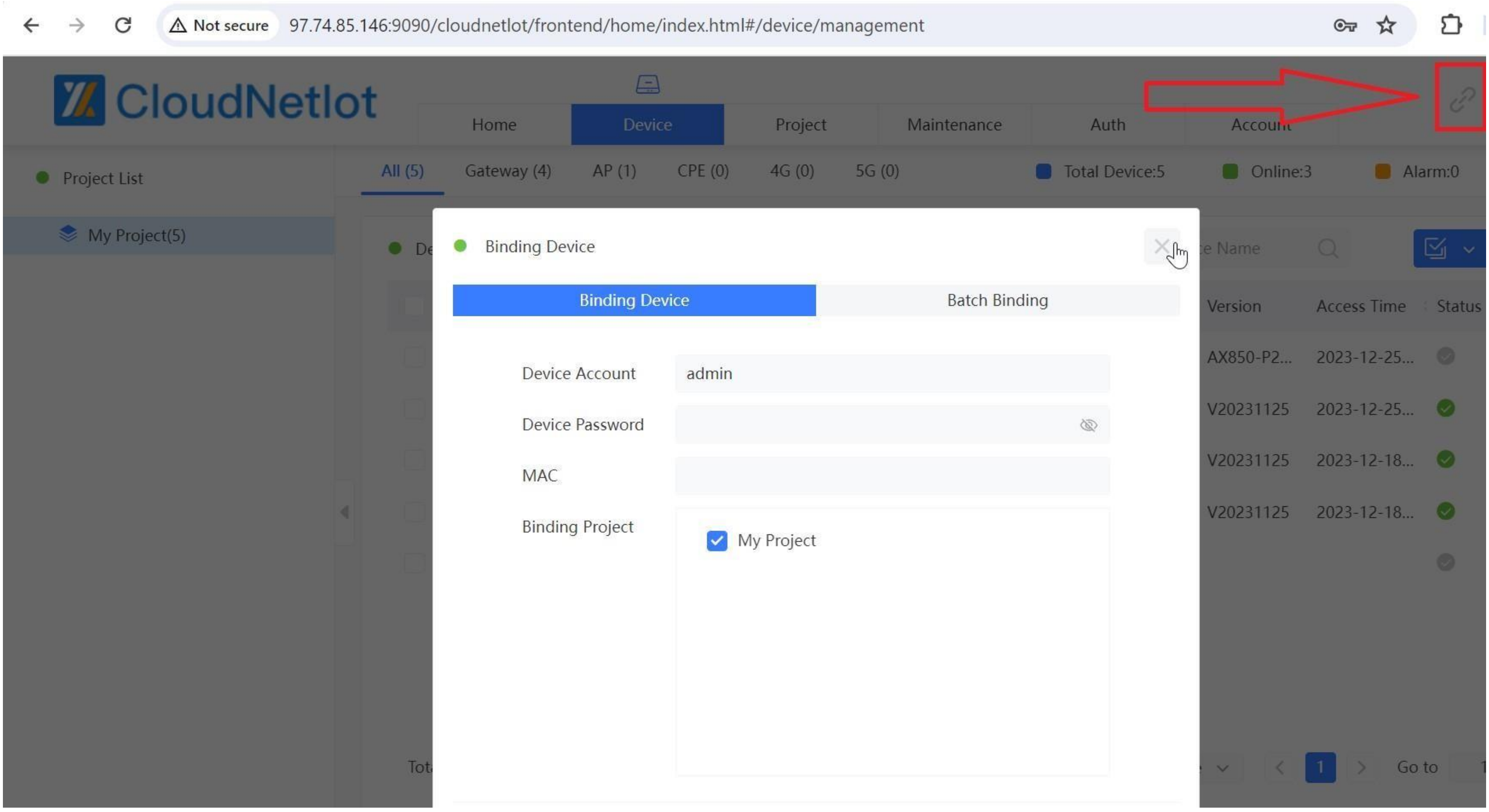


Cloud platform configure

Function enable: Enabled,click to disable

Cloud server address: http://97.74.85.146:9090

After logging successfully to your cloud management account successfully click on binding device as shown below.



Binding Device

Binding Device | Batch Binding

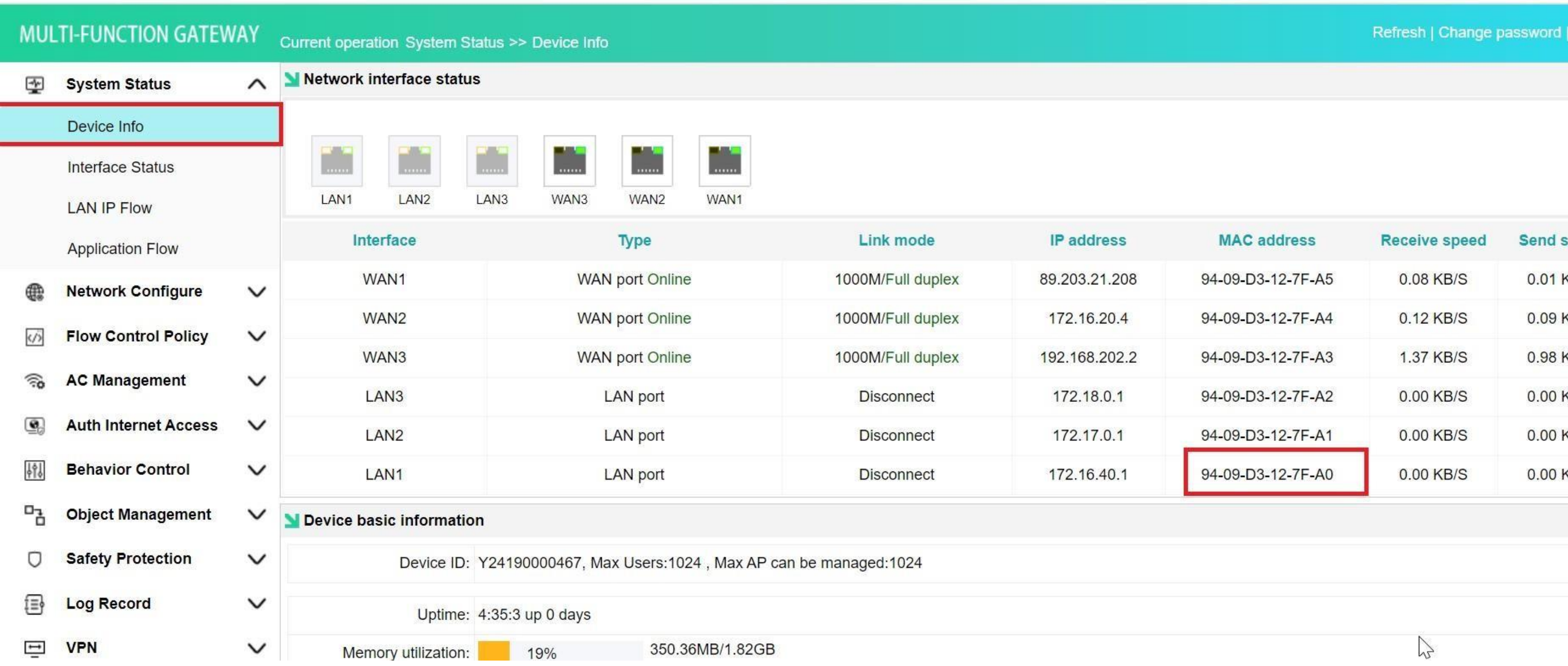
Device Account: admin

Device Password:

MAC:

Binding Project: ☑ My Project

Copy the active LAN MAC address from controller to setup in cloud management as shown in the figures below.



Network interface status

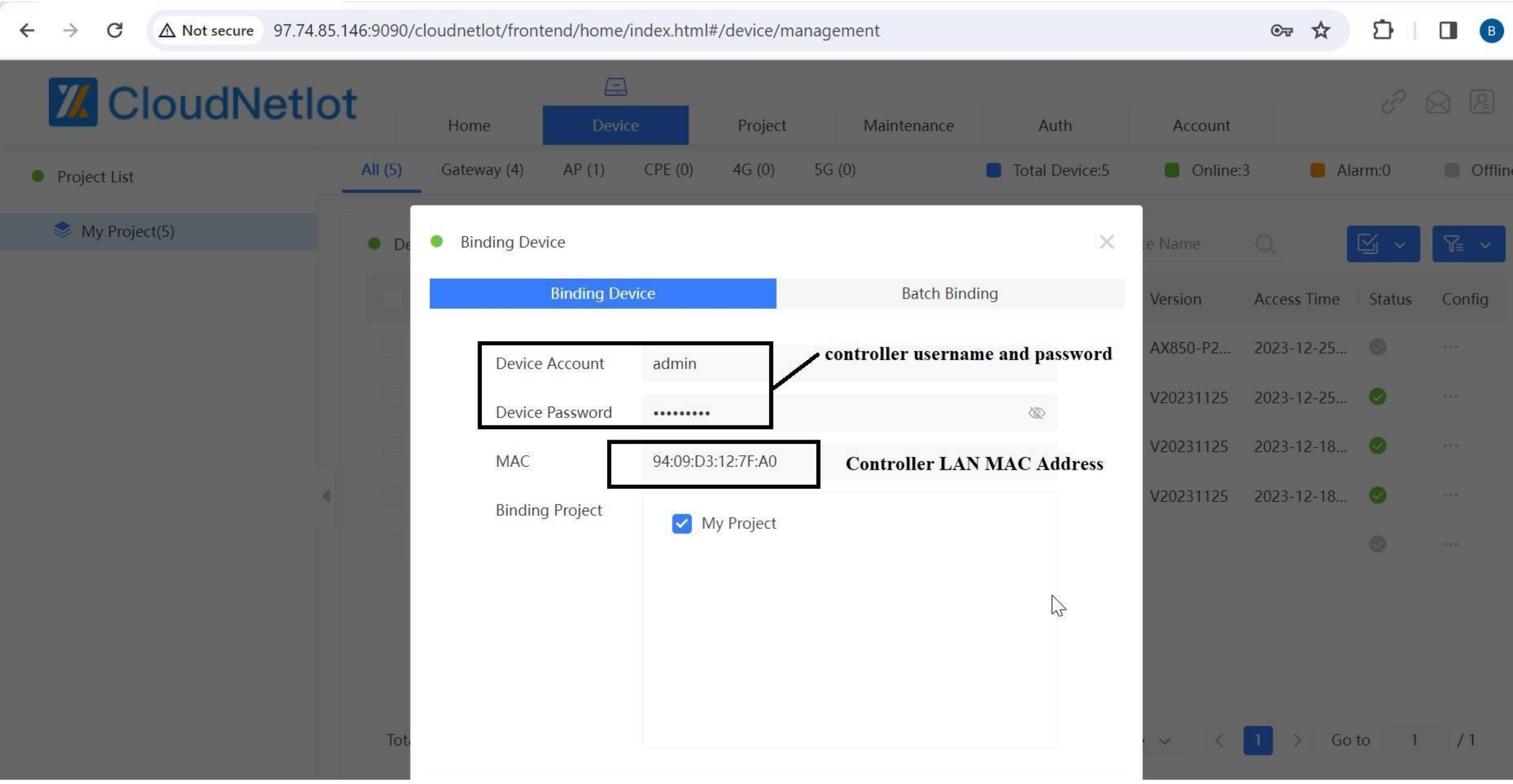
Interface	Type	Link mode	IP address	MAC address	Receive speed	Send s
WAN1	WAN port Online	1000M/Full duplex	89.203.21.208	94-09-D3-12-7F-A5	0.08 KB/S	0.01 K
WAN2	WAN port Online	1000M/Full duplex	172.16.20.4	94-09-D3-12-7F-A4	0.12 KB/S	0.09 K
WAN3	WAN port Online	1000M/Full duplex	192.168.202.2	94-09-D3-12-7F-A3	1.37 KB/S	0.98 K
LAN3	LAN port	Disconnect	172.18.0.1	94-09-D3-12-7F-A2	0.00 KB/S	0.00 K
LAN2	LAN port	Disconnect	172.17.0.1	94-09-D3-12-7F-A1	0.00 KB/S	0.00 K
LAN1	LAN port	Disconnect	172.16.40.1	94-09-D3-12-7F-A0	0.00 KB/S	0.00 K

Device basic information

Device ID: Y24190000467, Max Users:1024 , Max AP can be managed:1024

Uptime: 4:35:3 up 0 days

Memory utilization: 19% 350.36MB/1.82GB



Binding Device

Binding Device | Batch Binding

Device Account: admin

Device Password: •••••••••

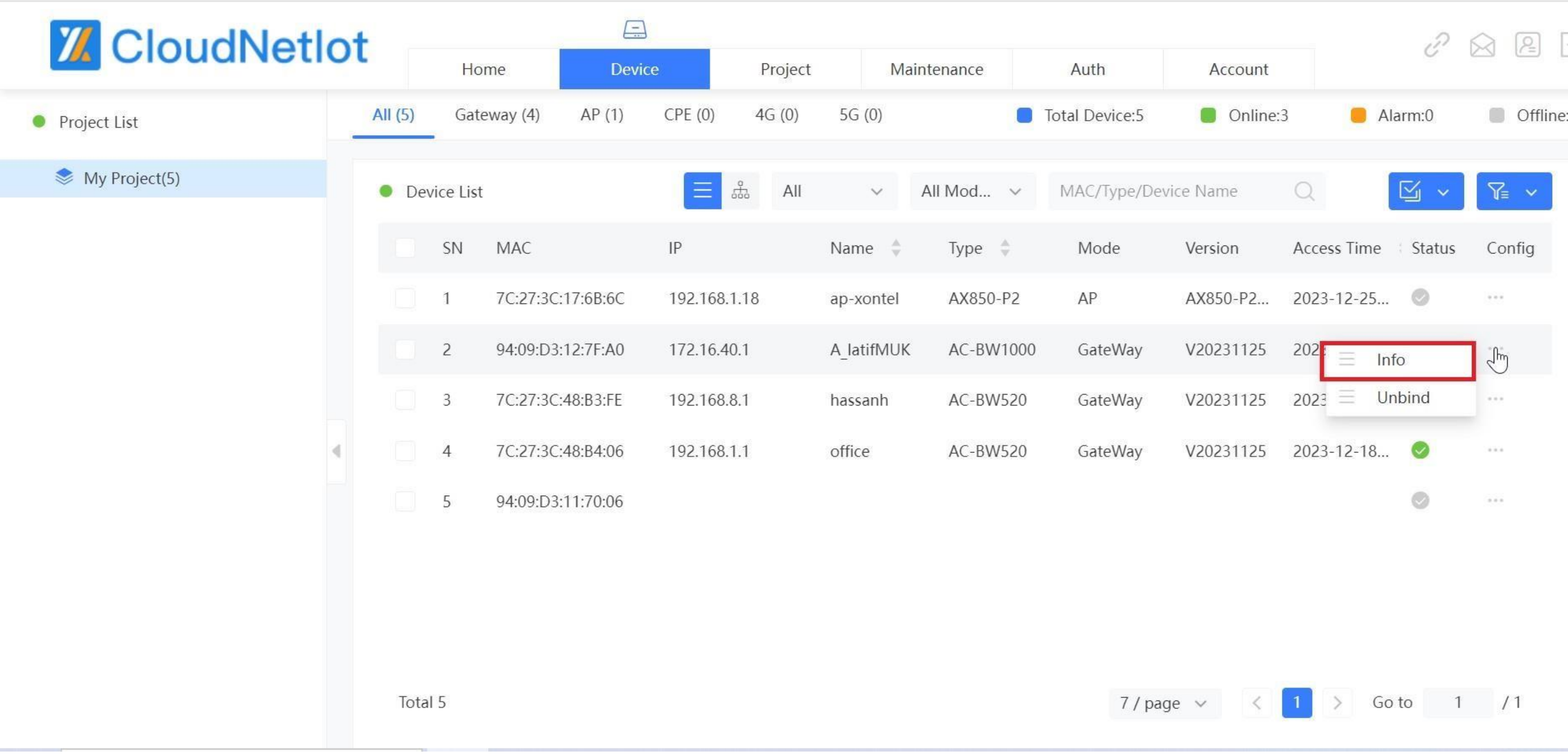
MAC: 94:09:D3:12:7F:A0

Binding Project: ☑ My Project

controller username and password

Controller LAN MAC Address

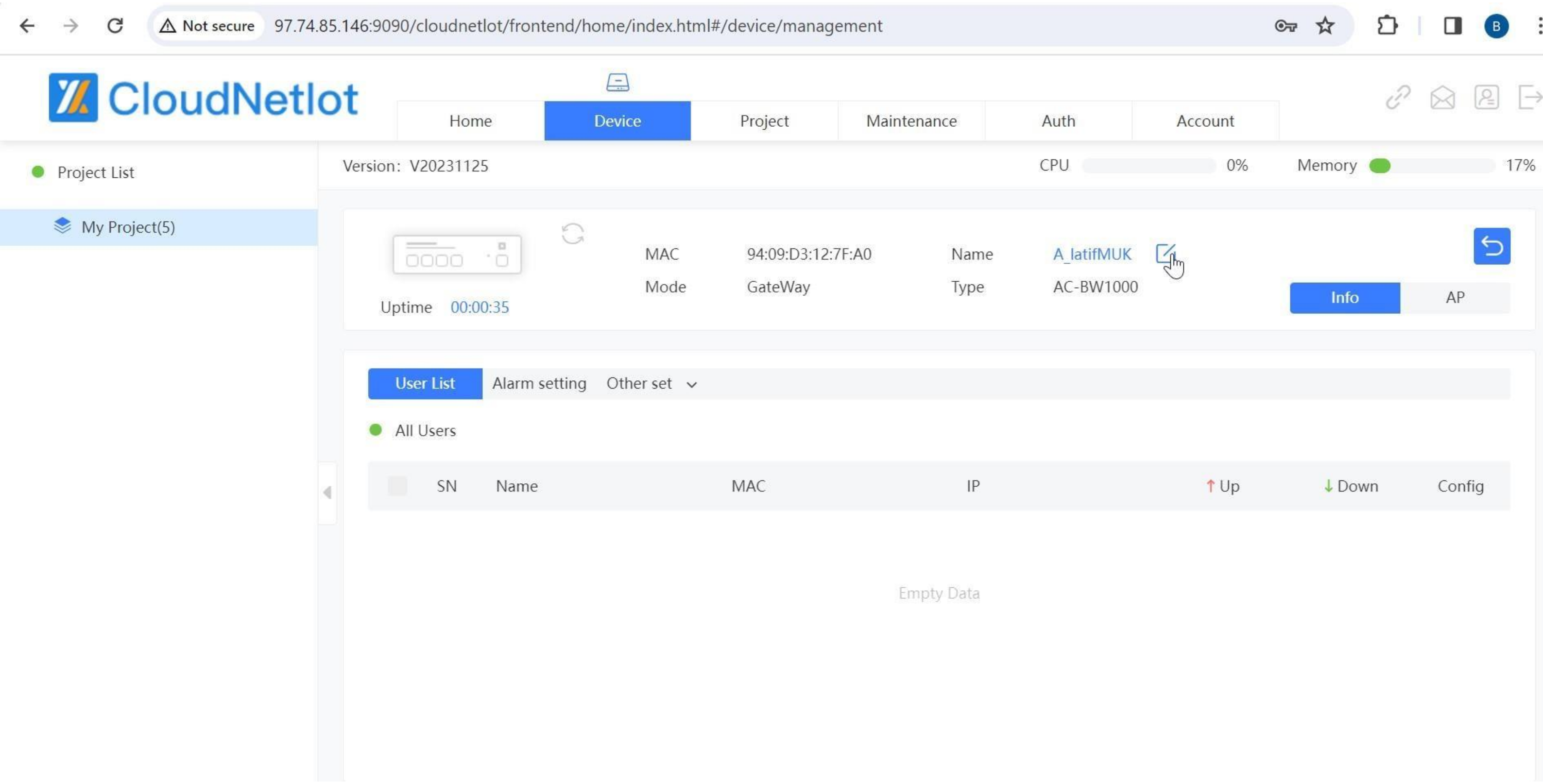
After binding controller successfully, you can manage the settings remotely as shown below



SN	MAC	IP	Name	Type	Mode	Version	Access Time	Status	Config
1	7C:27:3C:17:6B:6C	192.168.1.18	ap-xontel	AX850-P2	AP	AX850-P2...	2023-12-25...	●	···
2	94:09:D3:12:7F:A0	172.16.40.1	A_latifMUK	AC-BW1000	GateWay	V20231125	202		
3	7C:27:3C:48:B3:FE	192.168.8.1	hassanh	AC-BW520	GateWay	V20231125	2023		···
4	7C:27:3C:48:B4:06	192.168.1.1	office	AC-BW520	GateWay	V20231125	2023-12-18...	✓	···
5	94:09:D3:11:70:06							●	···

Total 5

7 / page 1 Go to 1 / 1



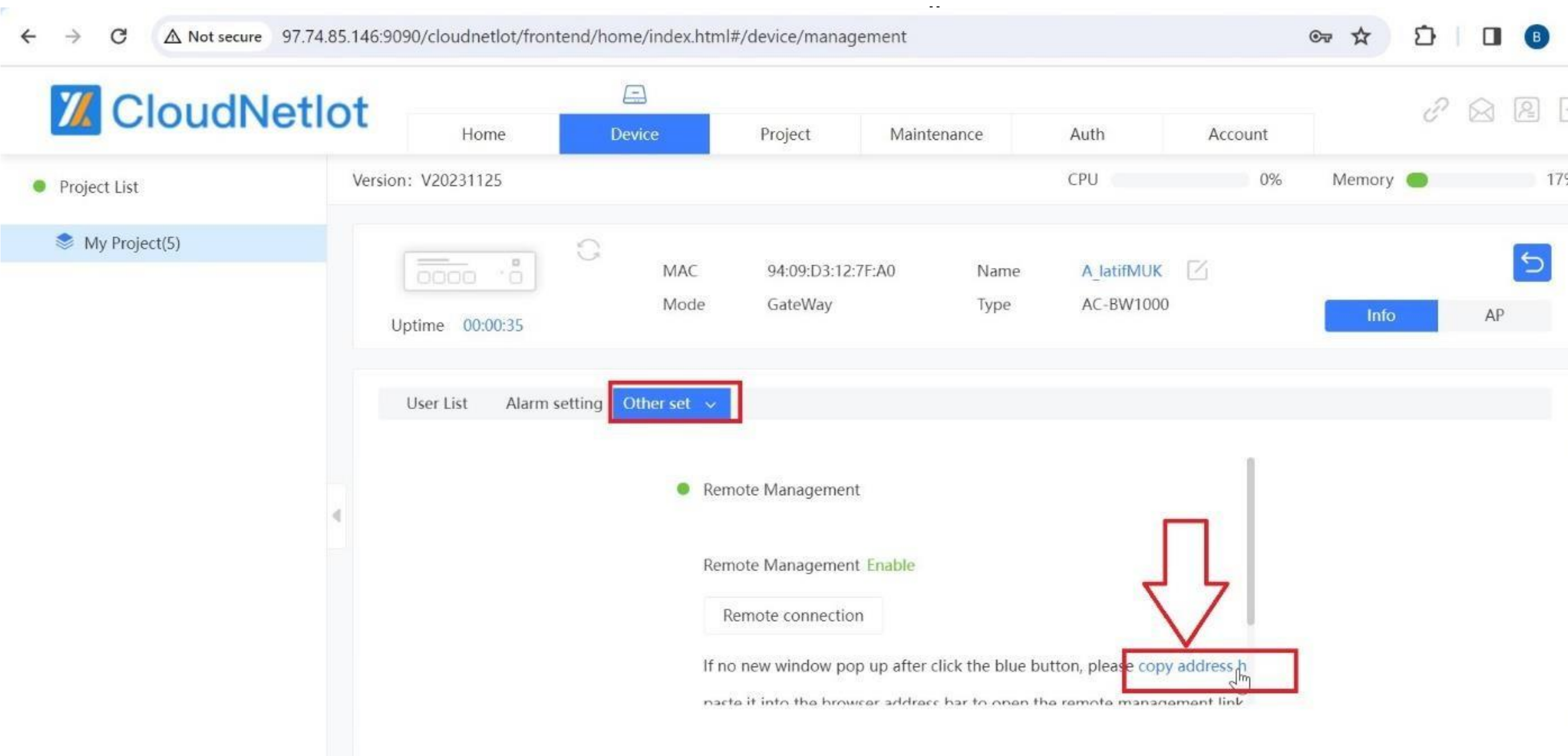
97.74.85.146:9090/cloudnetlot/frontend/home/index.html#/device/management

Version: V20231125 CPU 0% Memory 17%

MAC	94:09:D3:12:7F:A0	Name	A_latifMUK
Mode	GateWay	Type	AC-BW1000

Uptime 00:00:35

SN	Name	MAC	IP	↑ Up	↓ Down	Config



Version: V20231125 CPU 0% Memory 17

MAC 94:09:D3:12:7F:A0 Name A_latifMUK

Mode GateWay Type AC-BW1000

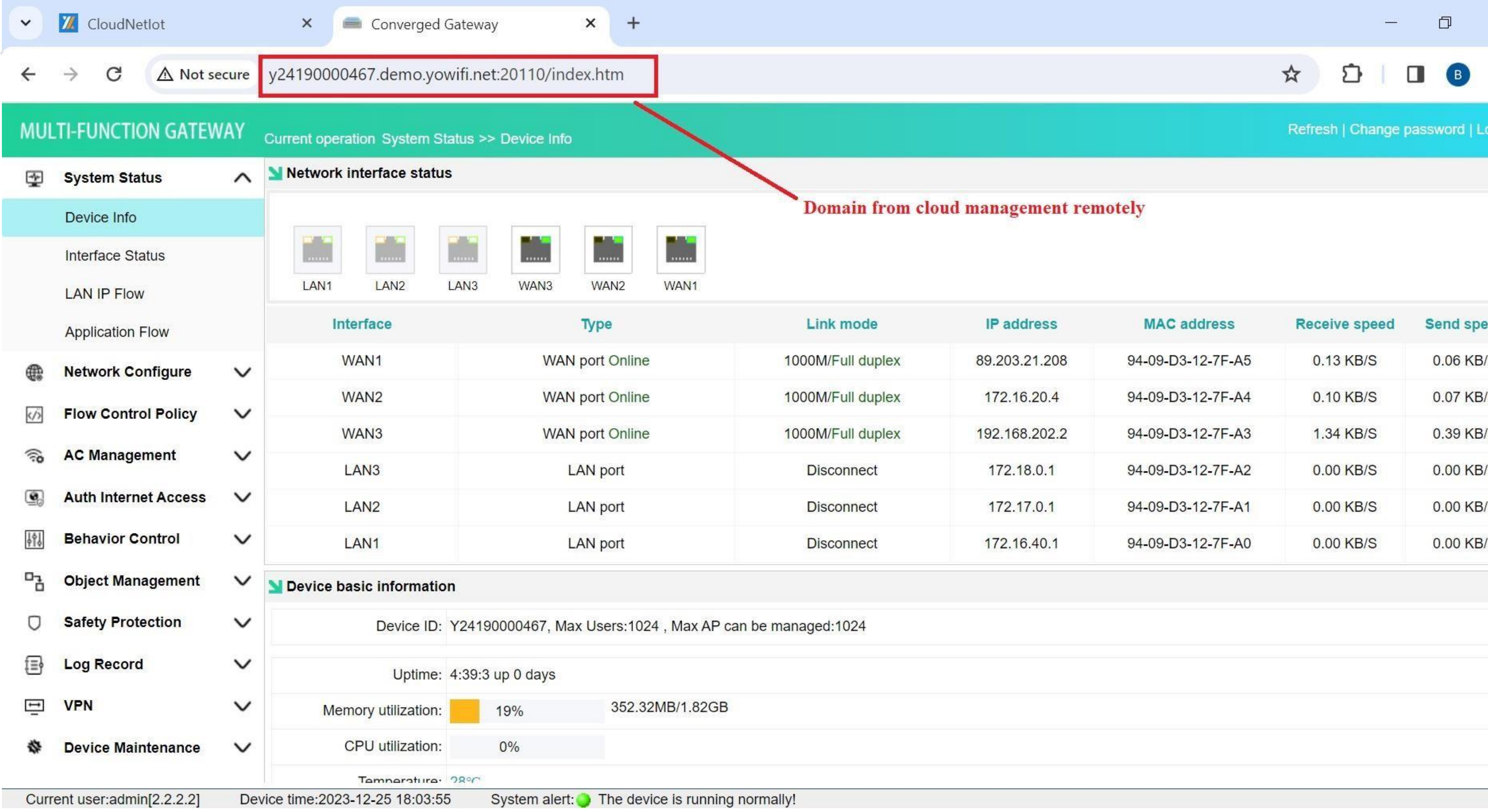
Uptime 00:00:35

Remote Management

Remote Management Enable

If no new window pop up after click the blue button, please copy address h

paste it into the browser address bar to open the remote management link



Current operation System Status >> Device Info

Network interface status

Domain from cloud management remotely

Interface	Type	Link mode	IP address	MAC address	Receive speed	Send spe
WAN1	WAN port Online	1000M/Full duplex	89.203.21.208	94-09-D3-12-7F-A5	0.13 KB/S	0.06 KB/
WAN2	WAN port Online	1000M/Full duplex	172.16.20.4	94-09-D3-12-7F-A4	0.10 KB/S	0.07 KB/
WAN3	WAN port Online	1000M/Full duplex	192.168.202.2	94-09-D3-12-7F-A3	1.34 KB/S	0.39 KB/
LAN3	LAN port	Disconnect	172.18.0.1	94-09-D3-12-7F-A2	0.00 KB/S	0.00 KB/
LAN2	LAN port	Disconnect	172.17.0.1	94-09-D3-12-7F-A1	0.00 KB/S	0.00 KB/
LAN1	LAN port	Disconnect	172.16.40.1	94-09-D3-12-7F-A0	0.00 KB/S	0.00 KB/

Device basic information

Device ID: Y24190000467, Max Users:1024 , Max AP can be managed:1024

Uptime: 4:39:3 up 0 days

Memory utilization: 19% 352.32MB/1.82GB

CPU utilization: 0%

Temperature: 28°C

Current user:admin[2.2.2.2] Device time:2023-12-25 18:03:55 System alert: The device is running normally!