



COMMANDO MSG-1200 Multi-Service Cloud Gateway Web Configuration Guide



INTRODUCTION

COMMANDO MSG-1200 Multi-Service Cloud Gateway with 4x10/100/1000/2500 Mbps-RJ45 Ports and 2x10G SFP+ Slots with configurable and interchangeable LAN/WAN Ports, with functions like Gateway, Wireless Controller, Multi WAN Load Balancer, Firewall with Captive portal along with Standard Wireless Roaming Mechanism (802.11r), Authentication Server to Integrate and Simplify the Traditional Networking Mode, AC Management, Portal Authentication, Deep Packet Inspection (DPI) Seven-Layer flow Control, Supports Intelligent Networking (SD-WAN), 3200+ Application Protocol Identification.

It has excellent data processing capability and multiple powerful functions including MultiWAN Load Balancer, Access Control, Bandwidth Control, Session Limit, IM/P2P Blocking, VPN server, PPPoE Server, auto WAN failover recovery and captive portal to access infrastructure from anywhere via internet. It meets the needs of small, medium and large enterprise, Big commercial set up where no down time affordable due to network issue, hotels and communities with Up to 1200 users demanding a efficient and always UP network with high security. It is basically 6 in 1 Multi-Service device having feature like Multi-WAN load balancer with auto fail-over mechanism for recovery due fault in connected multiple WAN links, Firewall, VPN Server, WLAN Controller up to 1024 COMMANDO AirX Series AP/APO, Cloud-based 10 different kinds of authentication Configuration and monitoring along with SDWAN for Enterprise Wired Gateway with features like static, Default and Dynamic connected route.

COMMANDO MSG-1200 Multi-Service Cloud Gateway is multi-functional gateway with functions like Wireless Controller, Load Balancer with Multi-WAN auto failover, Firewall, VPN Server with Captive portal with following useful functions.

- Standard Wireless Roaming Mechanism (802.11r)
- WLAN controller can manage up to 1024 AP/APO and up to 1200 users, with Discovery, Configuration, and Monitoring Functions.
- DPI (Deep Packet Inspection) Seven Layer Flow Control
- Supports One Click Flow Control and Manual Flow Control

- 3200+ Application Protocol Identification, for more Accurate Flow Control, Improved Bandwidth Utilization
- Multi-WAN load balance with auto fail-over recovery for reliable and efficient access
- Access Point Management via Easy WEB GUI, Telnet and Cloud based Portal Authentication
- AC Intelligent Management Function, works together with COMMANDO AirX Series
- Wireless products with easy Access Point Management
- Supports COMMANDO Platform Management, Centralized Management and Maintenance via lifetime free Cloud base account
- VPN for Encrypted Communication, Ensure Remote Access Security
- Supports Multi-Vendor WAN Line simultaneous Access, WAN load sharing and
- balancing by different ISP, Rational use, Load Balancing with fail-over, Reduce Bandwidth Costs
- Wireless Marketing Function, various Authentication Methods to meet the needs of Different Users and Scenarios
- Tag based and port based VLANs to group control and relocate traffic pattern
- Fully protocol stack for both IPv4 and IPv6 and 100,00 concurrent sessions
- Supports IPsec, PPTP and L2TP VPN support up to 64 concurrent tunnels with max 2Gbps throughput (IPSec).
- QoS and Bandwidth Management for optimal bandwidth usage.
- High Availability for mission critical application with Multi-WAN load balance
- User certification by X.509 and authentication by Radius/AD/LDAP server for user and group management.
- Supports Multiple WANs, Failover/ Load Balance with configurable Ethernet
- Support DHCP based dynamic IP, Static IP, PPPoE, PPTP, L2TP
- IPv6 with Dual Stack, 6-in-4, 6-to-4, Dynamic, Static, PPPoE

- Supports VLAN Port Based, Tag- based
- NAT: ALG, Special AP, DMZ Host, Virtual Server/ Computer, PPTP/ L2TP/IPSec Pass-through, Up to 100,000 Sessions
- Supports Routing with Static, Default and Dynamically learn connected route
- Client & Server for DHCP, DDNS, IGMP
- Management Features with Web, Simple Telnet CLI, SNMP
- AP Auto Discovery, Monitoring & Alerting, Profile based Configuration, AP Load balance,
- AP Blacklisting and Whitelisting
- User Accounts, User Grouping, Bound Services
- Firewall, Access Control with Packet Filters, URL Blocking, Web Content Filters, Application Filters, MAC filter
- Support One Click Flow Control and Manual Flow Control
- Access Point Management with Cloud Portal Authentication, Connected LAN PC WEB GUI and Telnet.

MSG-1200 Functions can be broadly classified as follows:

Cloud Base Wired Router

It is 4x10/100/1000/2500 Mbps-RJ45 Ports and 2x10G SFP+ Slots with configurable and interchangeable LAN/WAN Ports which support up to 1200 Users with standard Wireless Roaming Mechanism (802.11r) with DPI (Deep Packet Inspection) Seven Layer Flow Control along with Portal based web access from anyone having credential via internet from any place. Support COMMANDO Cloud Platform Management, Centralized Management and Maintenance VPN for Encrypted Communication. Ensure Remote and cloud Access with security.

Multi-WAN load balancing with auto Fail over Mechanism

Support up to 5 WAN, Multi WAN Access, Simultaneous WAN access provided by different (ISP) Operators with all used at a time via load balancing and preventing network outage automatically via fail-over mechanism, Rational use, Reduce Bandwidth Costs.

Wireless Marketing Function

High Authentication Methods via cloud based, time based, ticket based to meet the needs of different Users and Scenarios, Multi-functional Fusion. The COMMANDO Integrates Functions Such as DPI Flow Control, Load Balancing, AC Controller, VPN, and Authentication Server to Integrate and Simplify the Traditional Networking Mode. Equivalent to Integrating Multiple Devices and a Unified Network Management Platform into one Device, greatly reducing Networking and Maintenance costs

Deep Packet Inspection

It supports Multi-line and each line is backed up with Each other. It has new Generation of DPI-based Traffic Identification Mechanism, and Fine Traffic Control with Link Balancing and Application Offloading to offload Core Applications.

Wireless Access Point Controller

It acts as Controller for COMMANDO AirX Series AP/APO, Support COMMANDO's AirX AP/APO Centralized Management, AP can be configured as Virtual Antenna available with this controller without any Configuration and connection to Controller. It automatically Read Wireless Configuration after accessing the Network, AP Zero-based Networking, Expansion at any time, Support Standard Wireless Roaming Mechanism (802.11r), to achieve Seamless Roaming between APs, Live streaming of Games, Video, Movies, voice, etc. is Uninterrupted.

Network Security

Built-efficient Behavior Management Routing and Firewall Modules, Support Flexible user Access Control Policies, Network Security, Network security to meet Different Customer needs. MAC Filtering function to block the access of illegal hosts. Supporting One-Click IPMAC Binding to avoid ARP spoofing.

VPN Virtual Private Network

Support IPsec, PPTP, L2TP and Open VPN, Allowing Offices in Different Regions of the Enterprise to Access ERP, CRM, Internal Server and other Production Systems of the company's Local Area Network at Any Time to Improve Work Efficiency. Out-of-office Employees can Access the Company's internal Network Resources through Secure Channels anytime and anywhere via COMMANDO Cloud access.

SD-WAN

SD-WAN enables to securely connect users, applications and data across multiple locations while providing improved performance, reliability and scalability. Virtual WAN architecture that allows enterprises to leverage any combination of transport services and provides centralized control and visibility over the entire network.

Online Behavior Management

Access Rules can permit or deny user for applications of FTP downloading, Email, Web browsing and so on. Supporting URL Filtering to prevent potential hazards from visiting the malicious Web sites. Bandwidth Control with flexible bandwidth management to automatically control the bandwidth of the host in bi-direction to avoid bandwidth over occupation, as well as optimize bandwidth usage. Session Limit to avoid few people to access resource.

Auto MDIX Capabilities

Auto sensing 10/100/100/2500 /10000 Mbps ports with auto MDIX capabilities which also removes speed and duplex mismatches automatically.

System security

- Application identification for service awareness technology to identify packets of dynamic protocols such as HTTP and RTP by checking Layer 4 to Layer 7 information in the packets, helping implement fine grained QoS management.
- URL filtering: URL filtering regulates online behavior by controlling which URLs users can access to secure the network and system data.
- Intrusion prevention: Intrusion prevention detects intrusions, such as buffer overflow attacks, Trojan horses, and worms, by analyzing network traffic and takes actions to

quickly terminate the intrusions. In this way, intrusion prevention protects the information system and network architecture of enterprises.

Built-in application identification server

Supports Layer 4 to Layer 7 application identification and can identify over 3200+ applications and application-based policy control technologies, including traffic blocking, traffic limit, and priority adjustment policies.

It has WAN1 which is by Default WAN port. WAN ports can be configured in ADSL/PPPoE, Static IP or DHCP mode as per settings provided by ISP. We can setup multiple WAN ports based on requirement. LAN1 & WAN1 are by default ports & rest all configurable into WAN/LAN ports as per customer requirement. LAN1 is default LAN Port. USB port for mainly to upgrade system. Power to power ON the device, Power LED indicator will be on. SYS indication Green and ON to show system working properly. NET is Green and ON to show Gateway connected to internet.

How to take access of COMMANDO MSG-1200?

Connect any port of LAN (1-6) to PC via RJ-45 cable. Open network and sharing center. Go to Change adapter settings.

Double click on Local Area Connection.

Go to Properties. Double click on Internet Protocol Version 4(TCP/IPv4) option and set Internet Protocol Version 4(TCP/IPv4) to auto shown below.

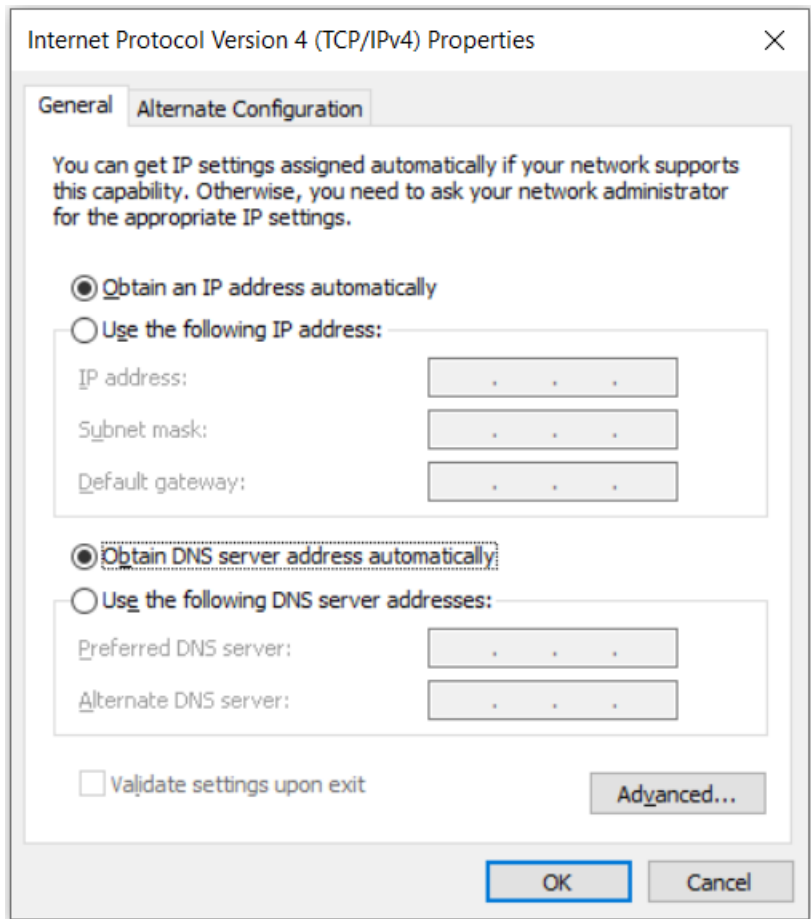


Fig 1. IP setting in PC connected to COMMANDO MSG-1200

Open any web browser like Chrome/Firefox/Internet Explorer/Opera etc. and enter default IPv4 Default Gateway address field.

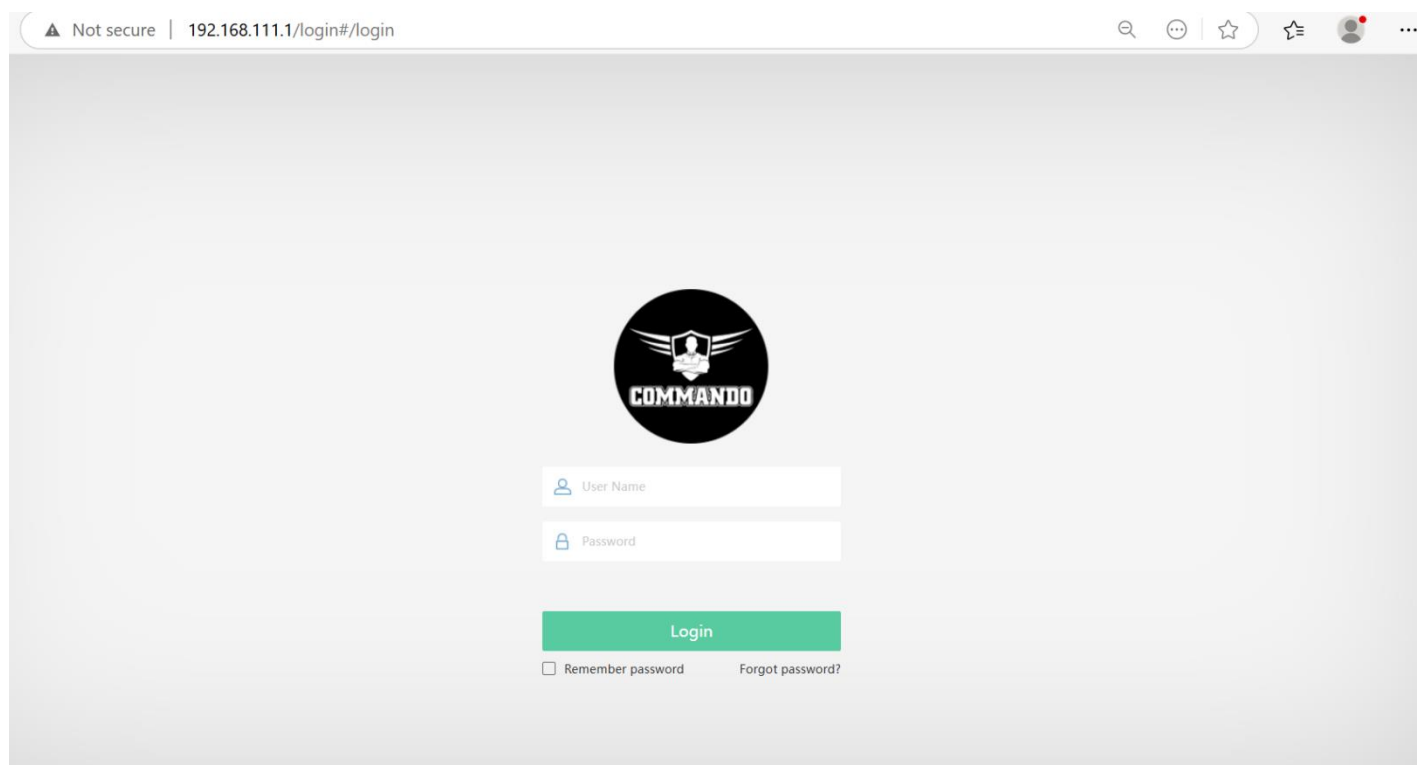
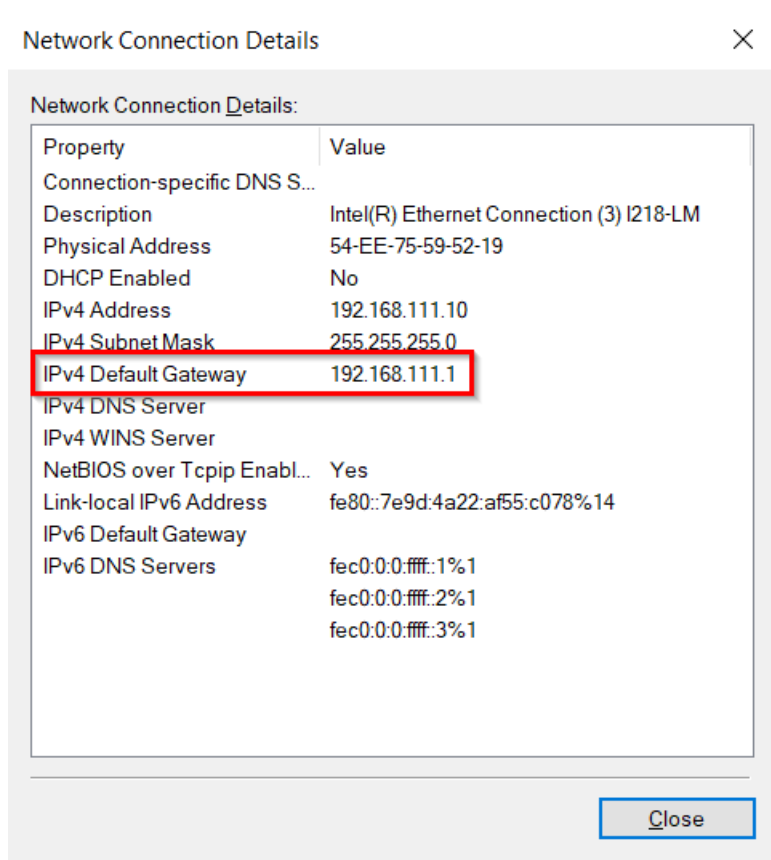


Fig 2. Login page for MSG-1200

Default Username: admin

Default Password: *****

(Default password is written on backside of device)

Note: Both Username and Password can be changed as per user choice.

After giving proper username and password. The System Overview page displays the basic system information like connection, interface, traffic analysis.

In system overview you can monitor network performance and many parameters on single page. You can check, Rate Status, Connection Status, Interface Status, AC Status and also monitor traffic analysis for different services.

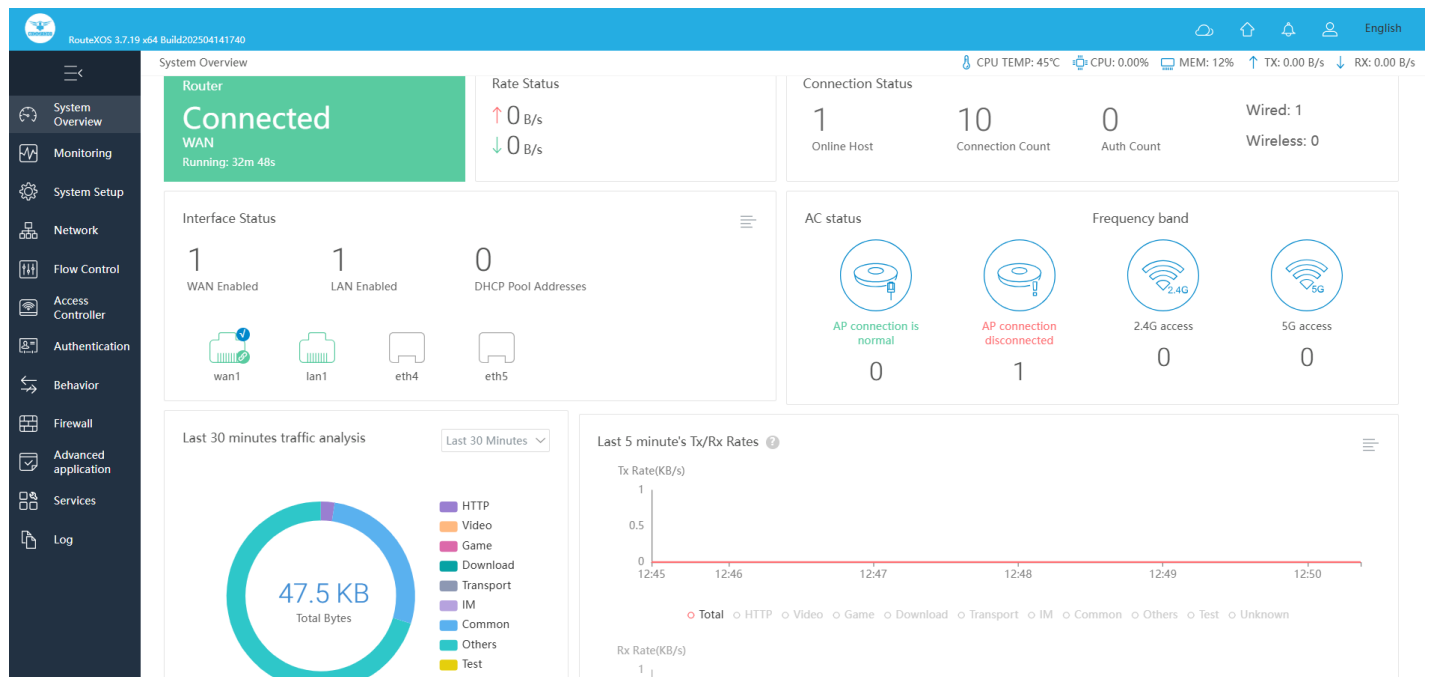


Fig 3. Default System Overview page

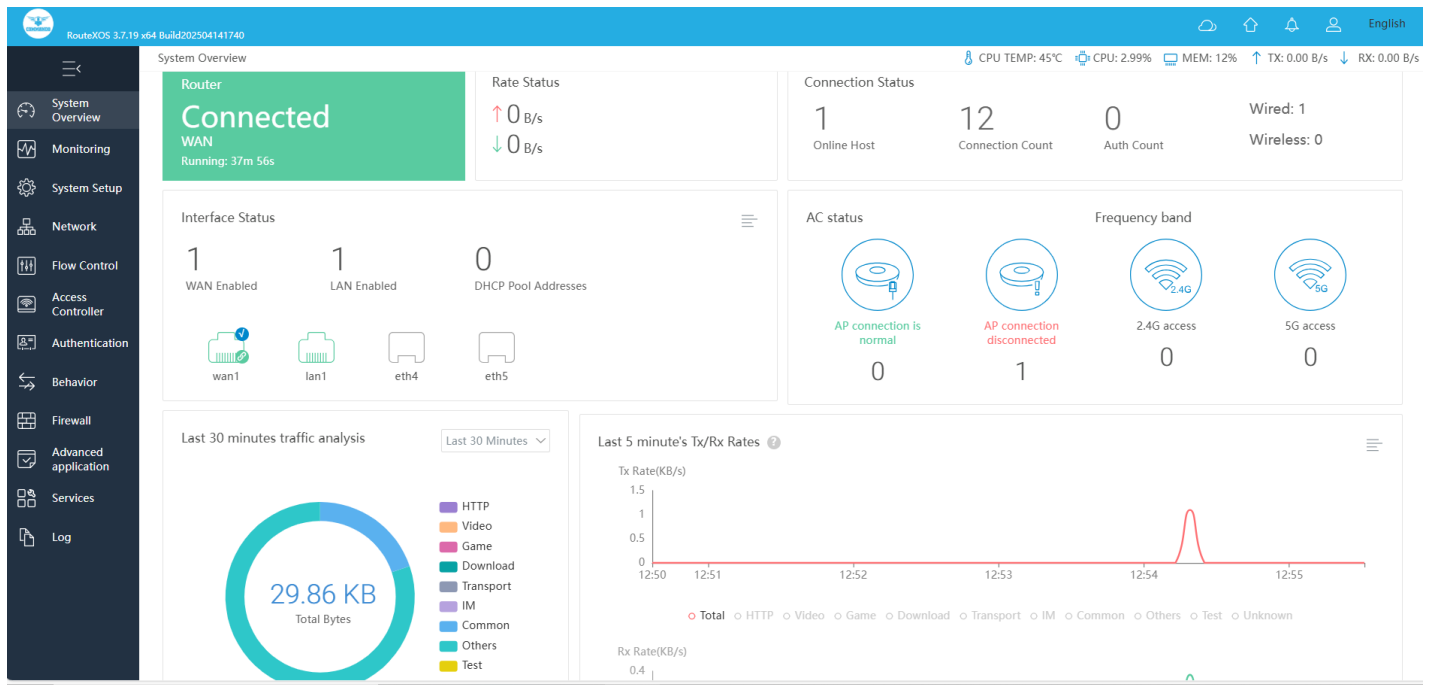


Fig 4. System Overview page after connecting LAN and WAN ports

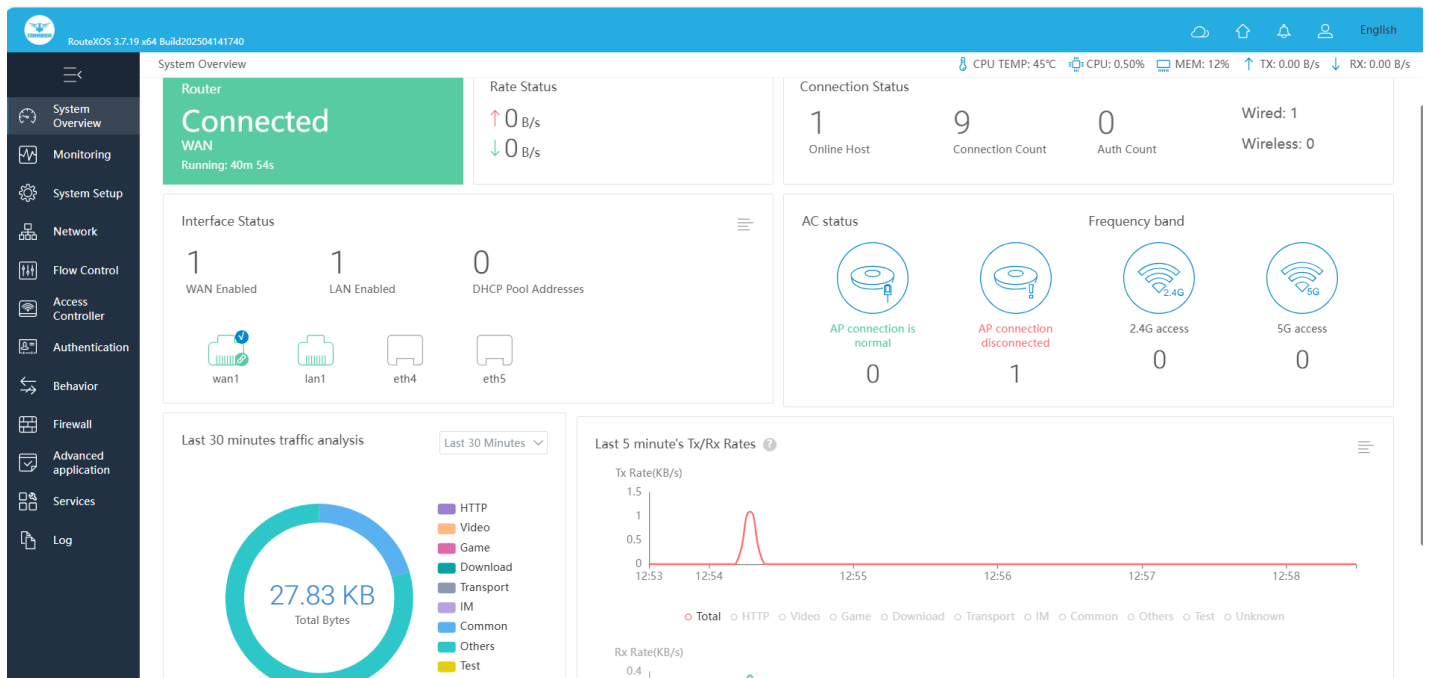


Fig 5. Connection status LAN and WAN ports.

Trouble in getting Internet Via DHCP WAN: If DHCP WAN link not able to provide proper DNS via connected WAN link DHCP server following measure will solve the issue.

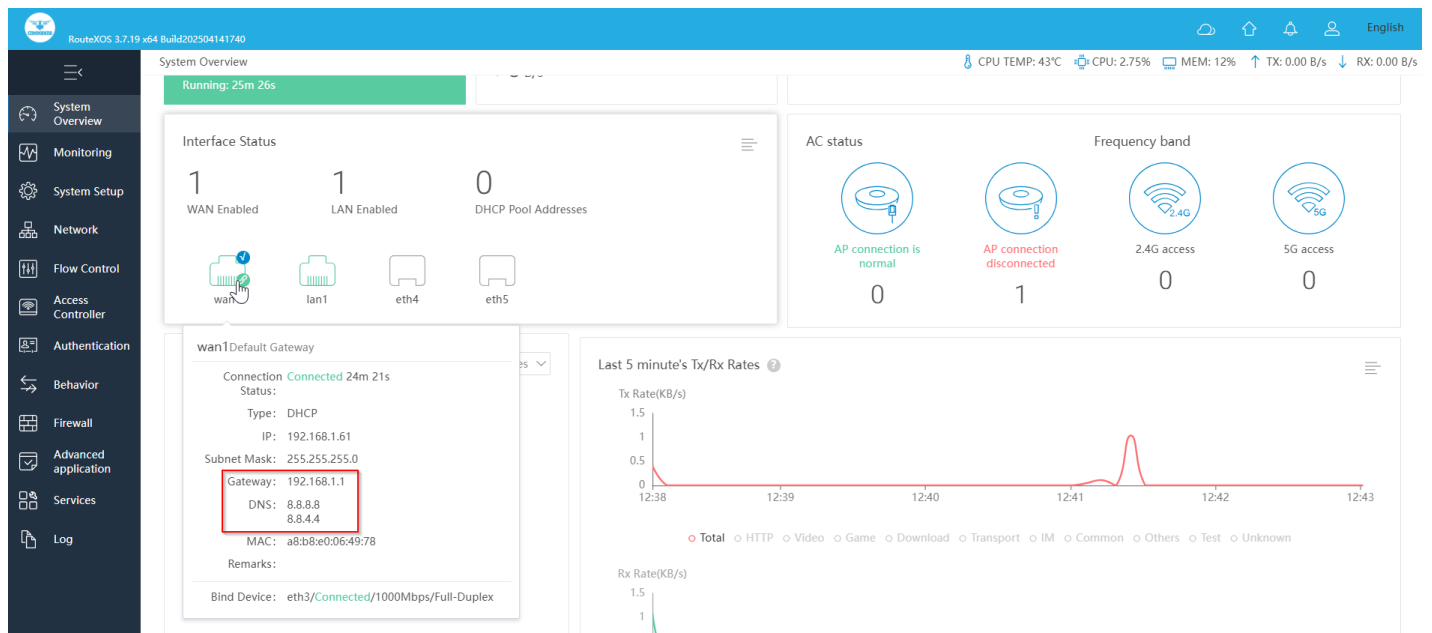


Fig 6. Non-Proper DNS via DHCP Server

Note: Changed LAN IP and taken access of MSG-1200 via new set LAN IP as DHCP server in WAN is set as 192.168.1.0/24 network.

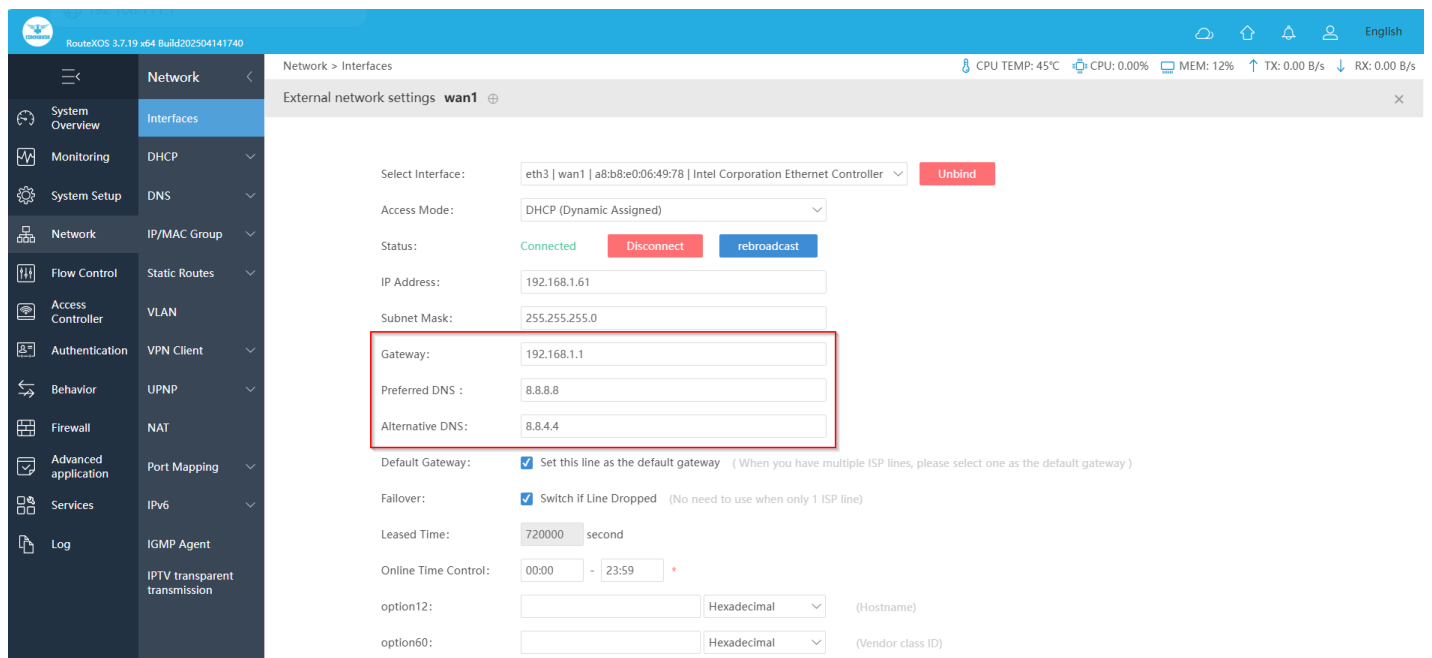


Fig 7. WAN-1 Getting 192.168.1.1 as preferred DNS server IP automatically

To solve this issue, Click on Network>DNS> Multiline DNS then Click add

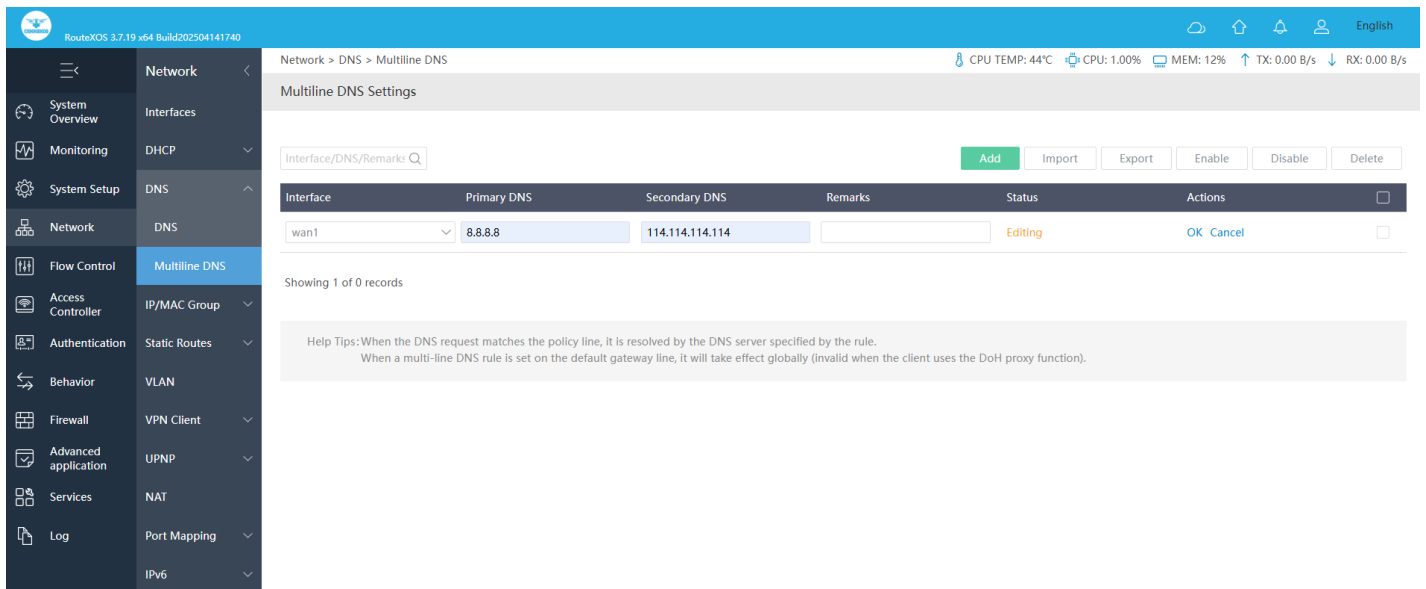


Fig 8. Multi DNS server Setting in MSG-1200.

Then add proper DNS server IP and see the system overview page.

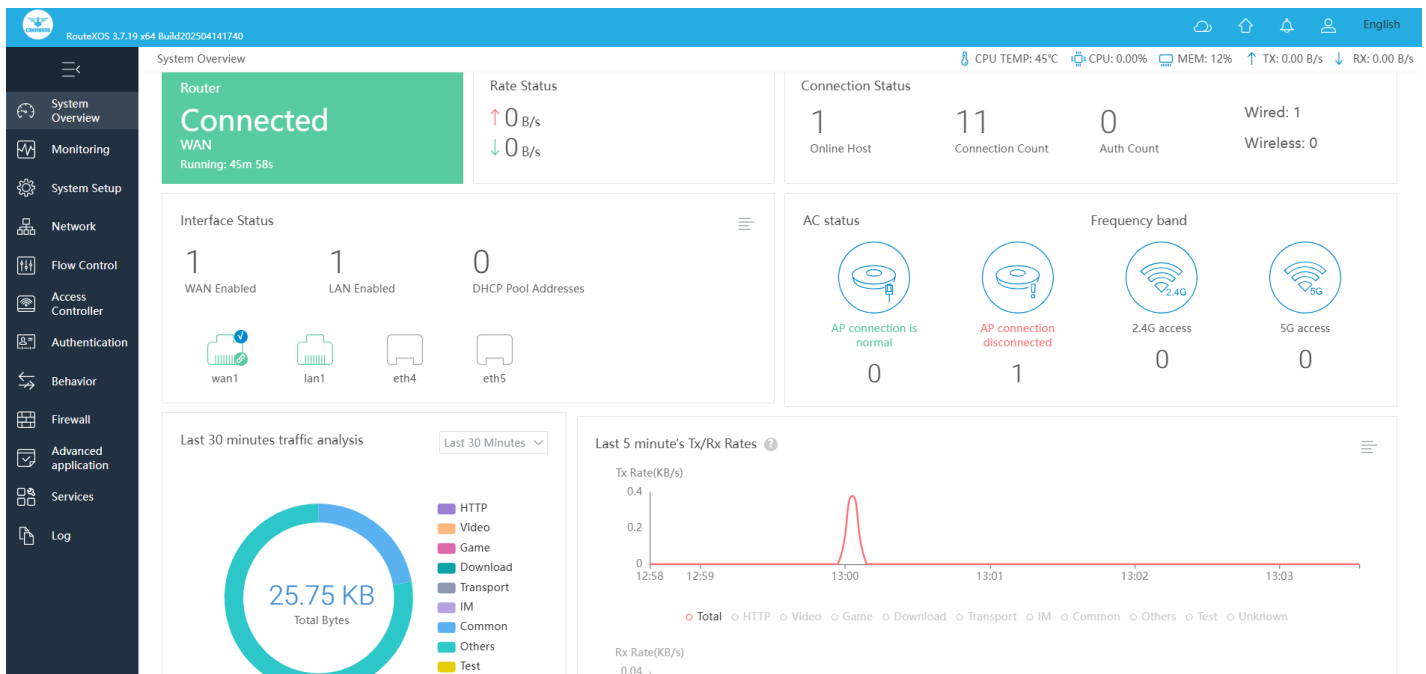


Fig 9. System overview page after proper setting LAN and WAN along with DNS server.

Traffic Analysis

It displays detailed information relating to the data traffic of all interfaces and IP addresses. You can monitor the traffic according to this information for last 30 minutes, 1hour or 1day.

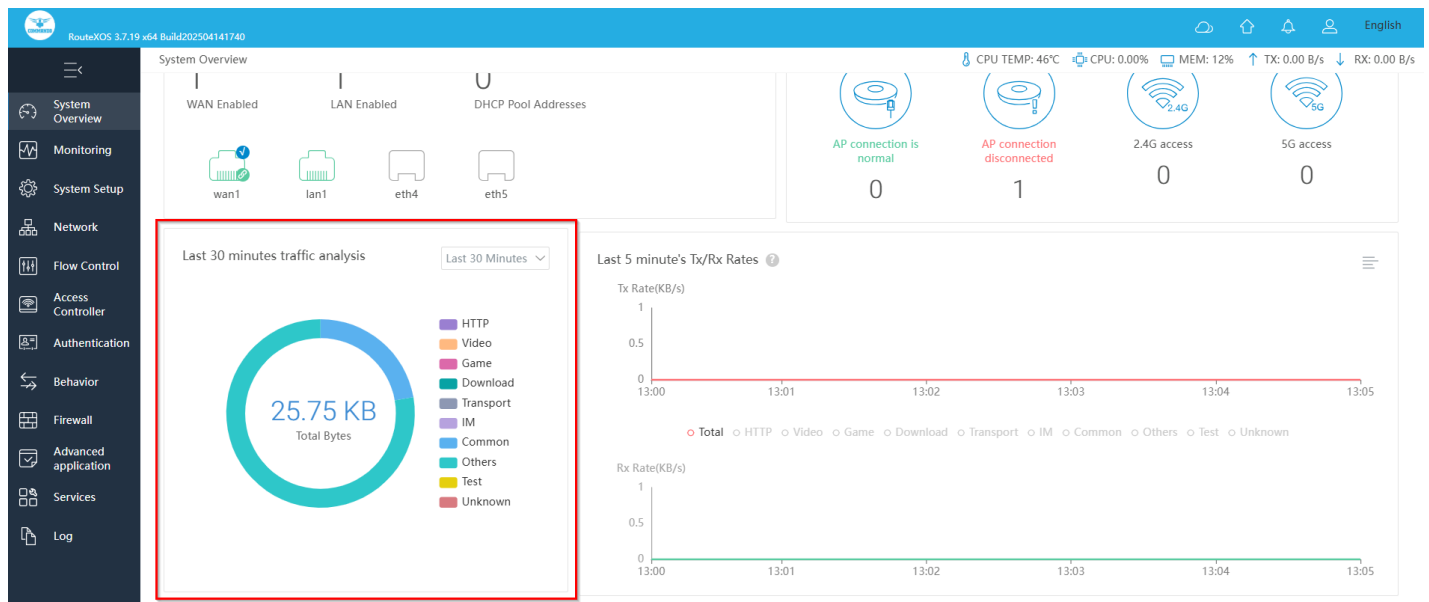


Fig 10. Traffic analysis for all application from last 30 minutes.

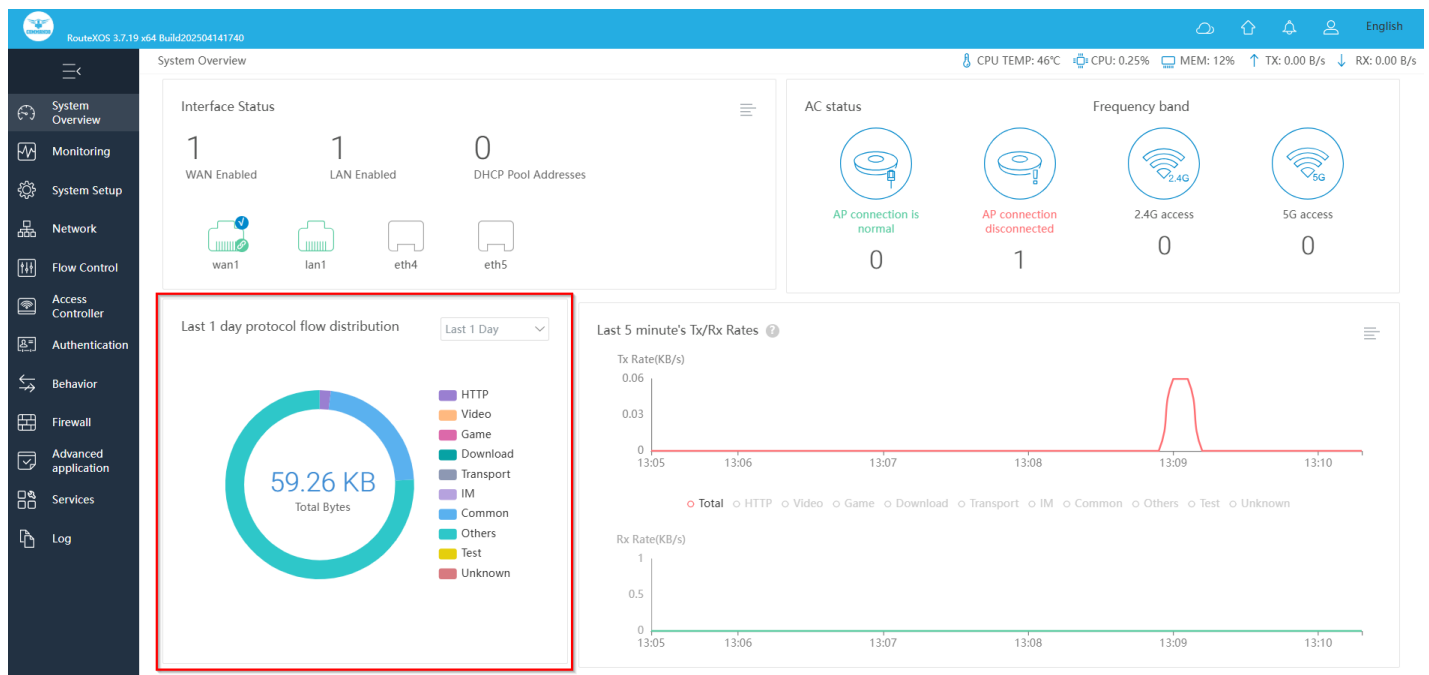


Fig 11. Traffic analysis for video application for 1 day

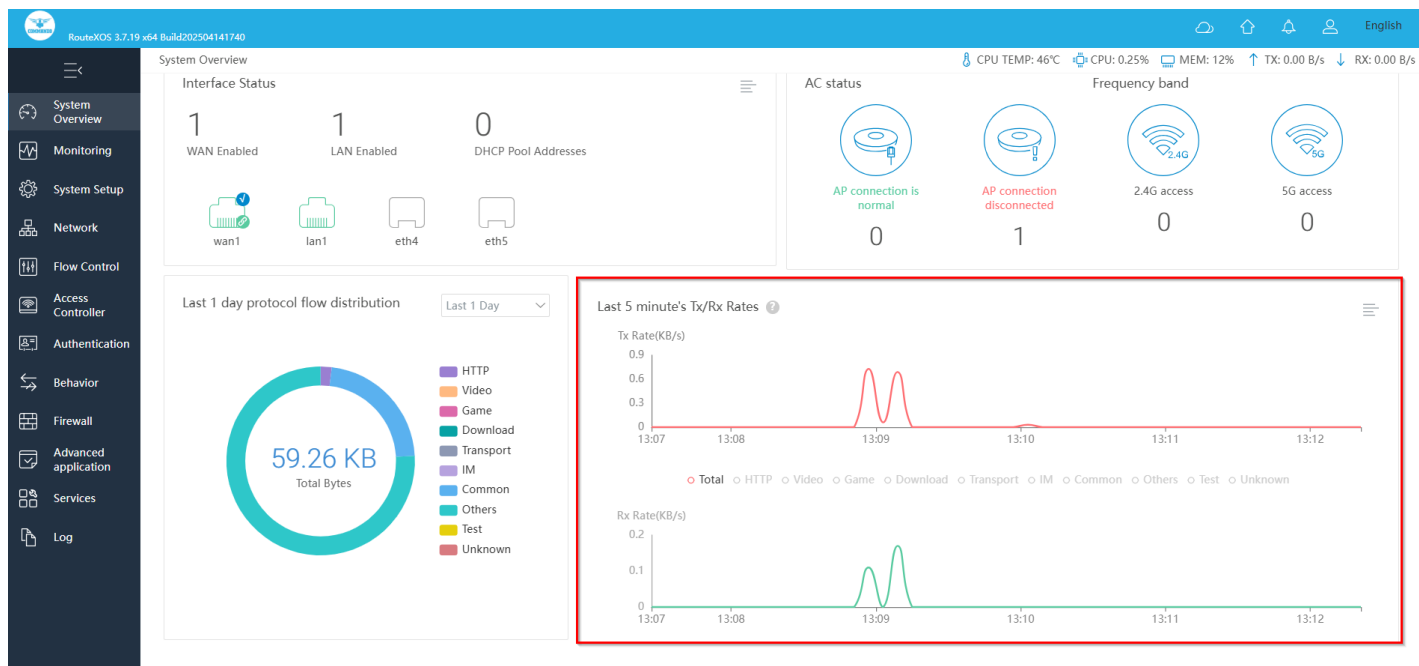


Fig 12. Transmission and Receiving Rate Graphs

II. Default page for shortcut Buttons for easy access to important web pages for users

Account Setting: On this page, you can view the detailed information of all accounts you have established.

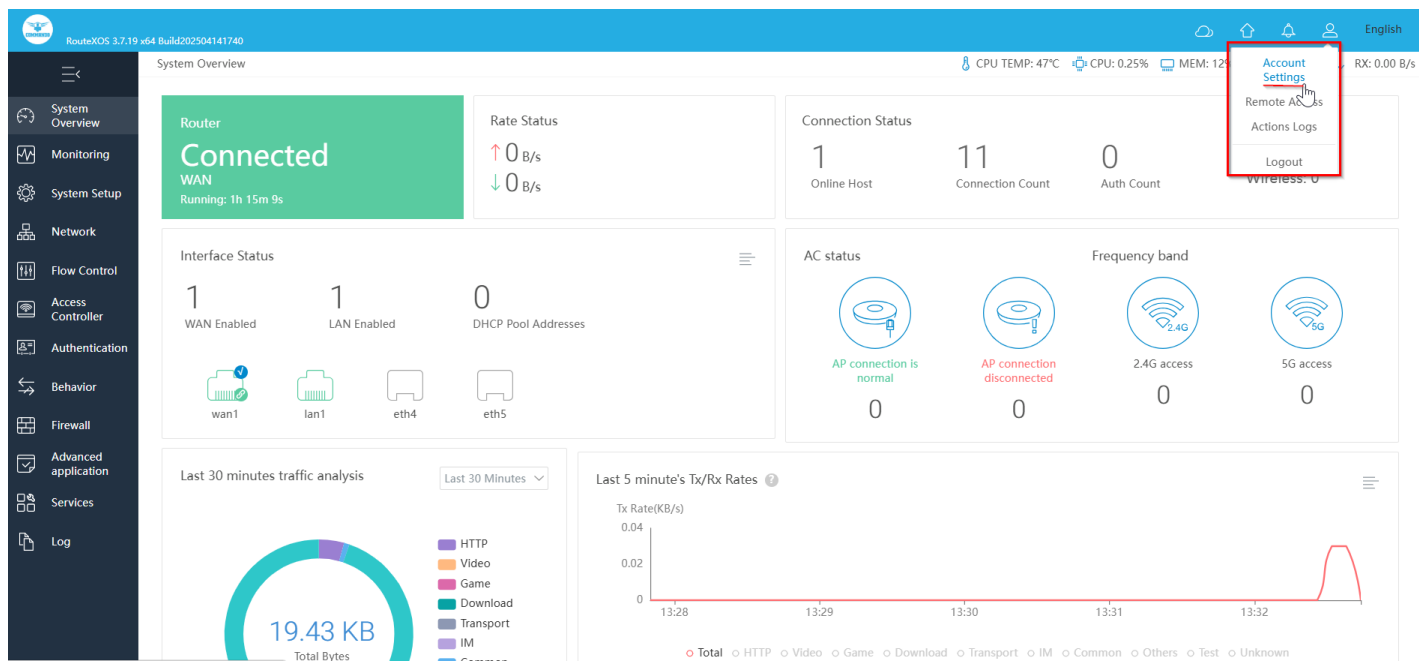


Fig 13. Account setting icon

After clicking on account setting icon user will be redirected to page System Setup > Administration > User Accounts

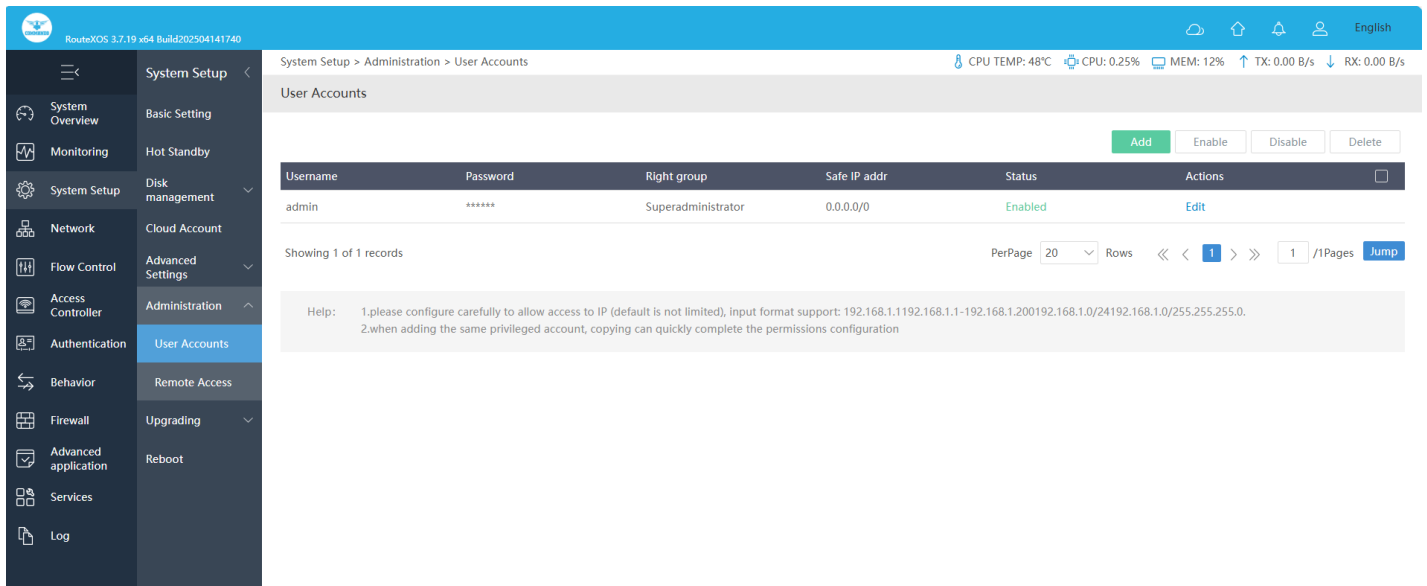


Fig 14. Default User Account setting

From Edit and Add account option you can create username and password as per your choice and even change the admin account for login to device.

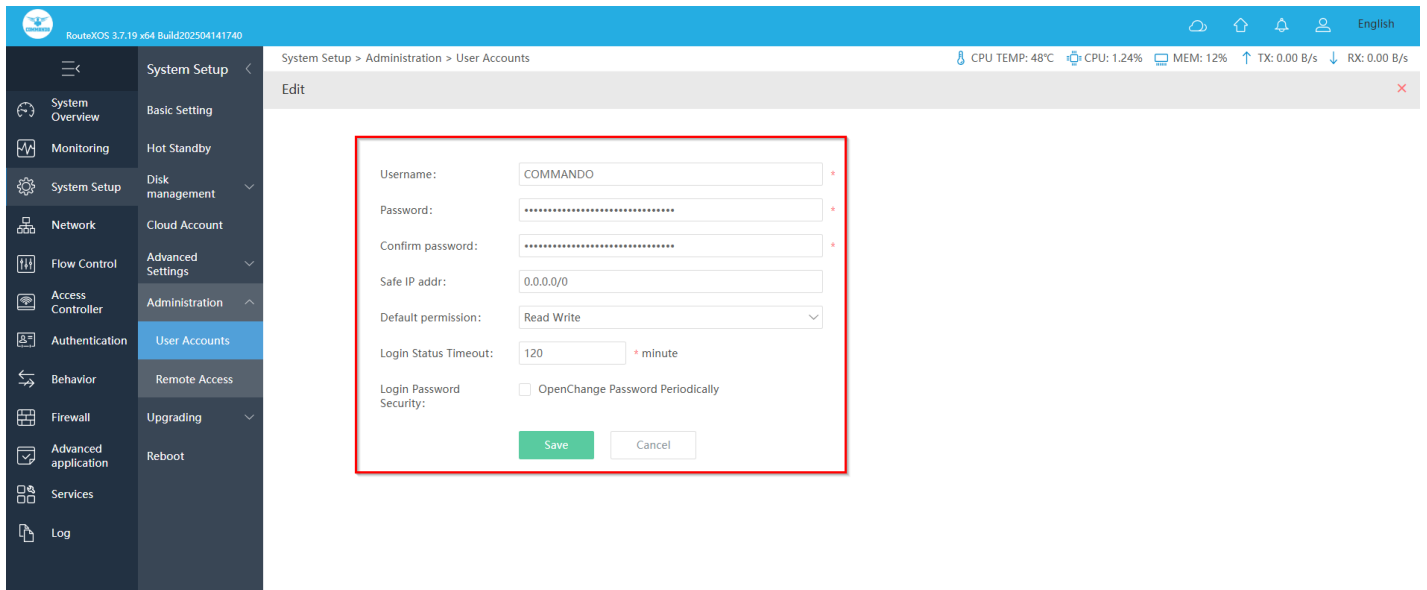


Fig 15. Editing User Account setting

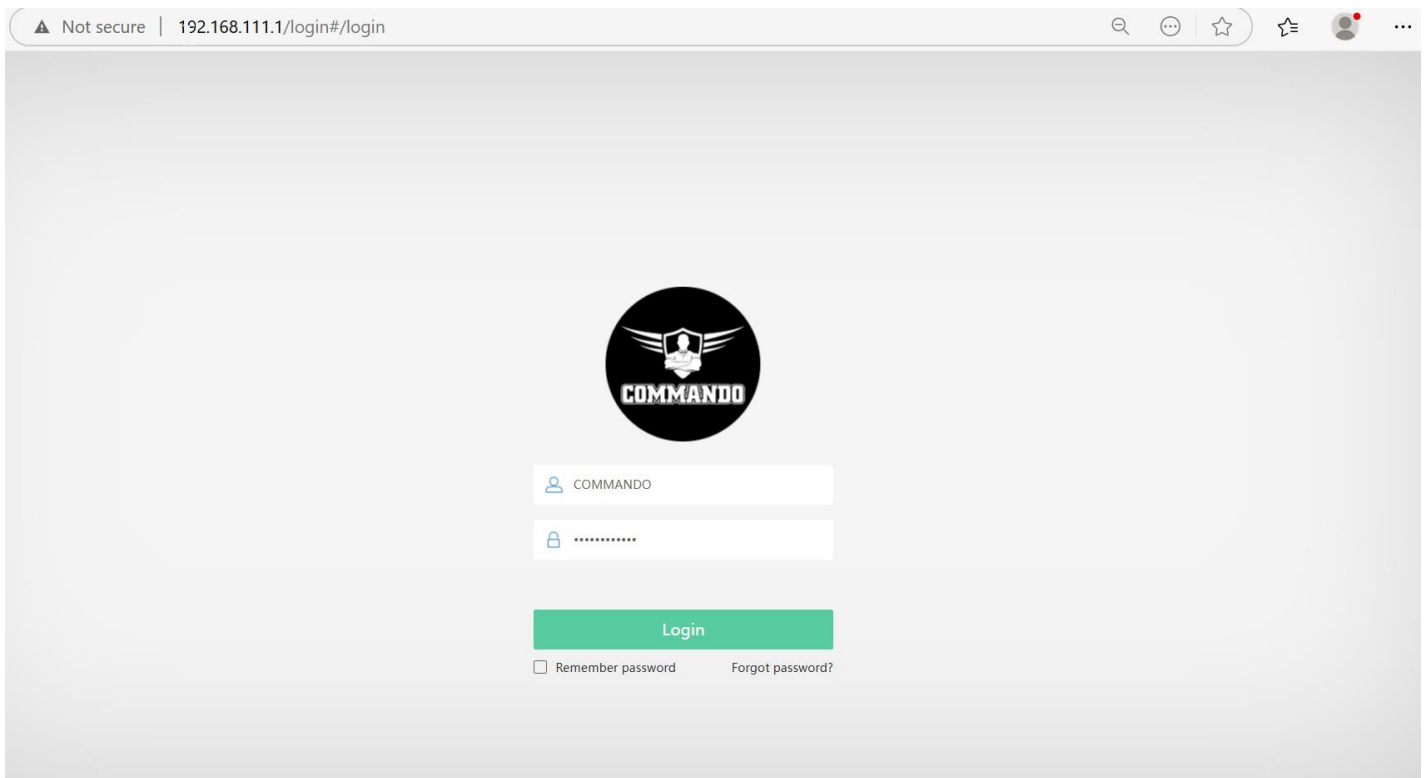


Fig 16. Logging with New account

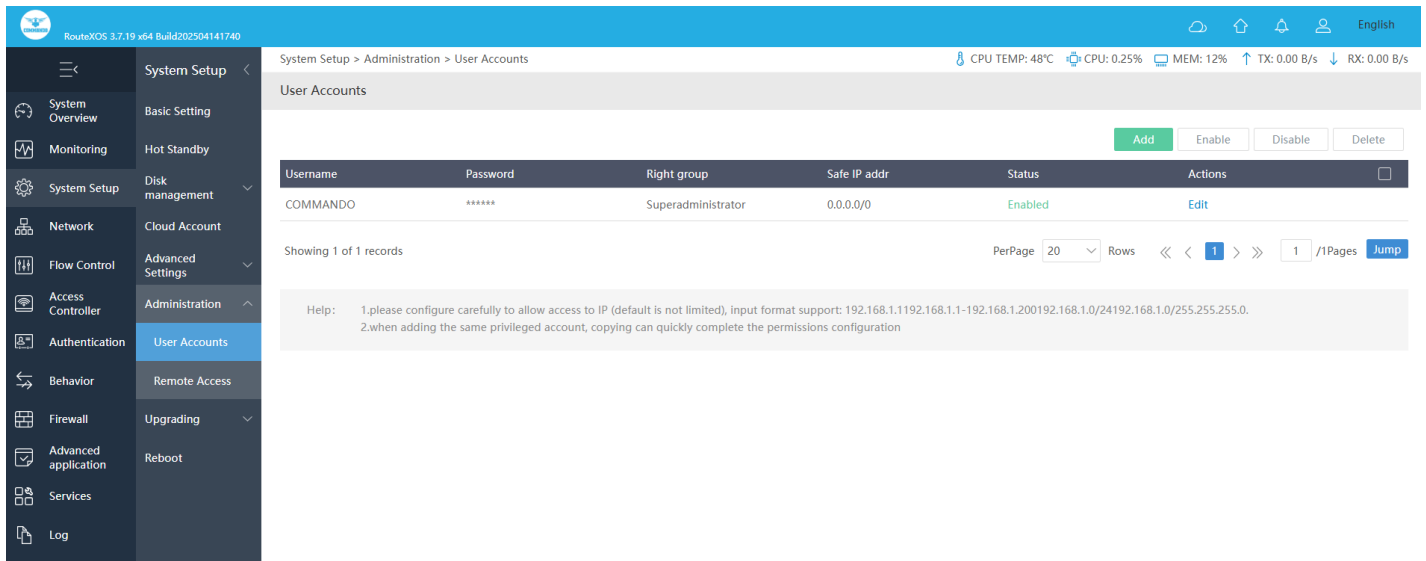


Fig 17. User Account setting after changing accounts

Remote Access: Supports Remote telnet and Web management via remote access. By default, all remote access is disabled.

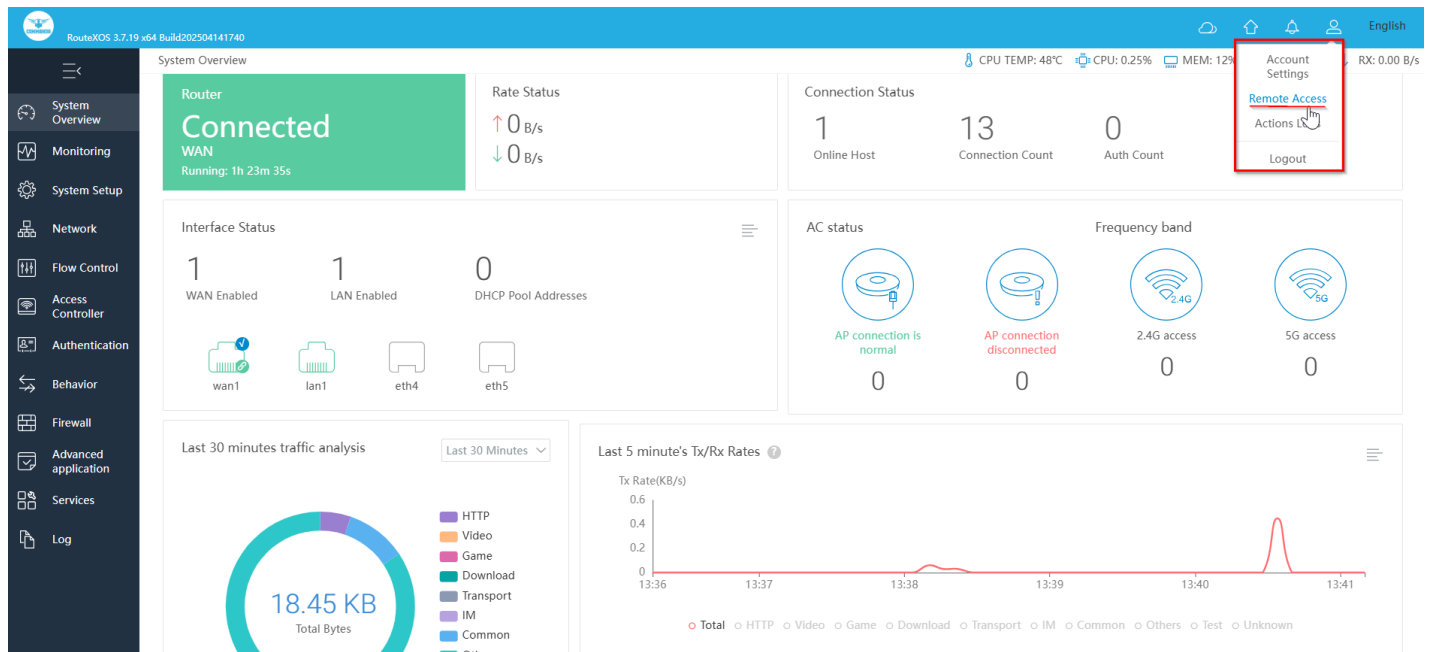


Fig 18. Remote access shortcut

After clicking remote access user will be directed to System Setup > Administration > Remote Access pages

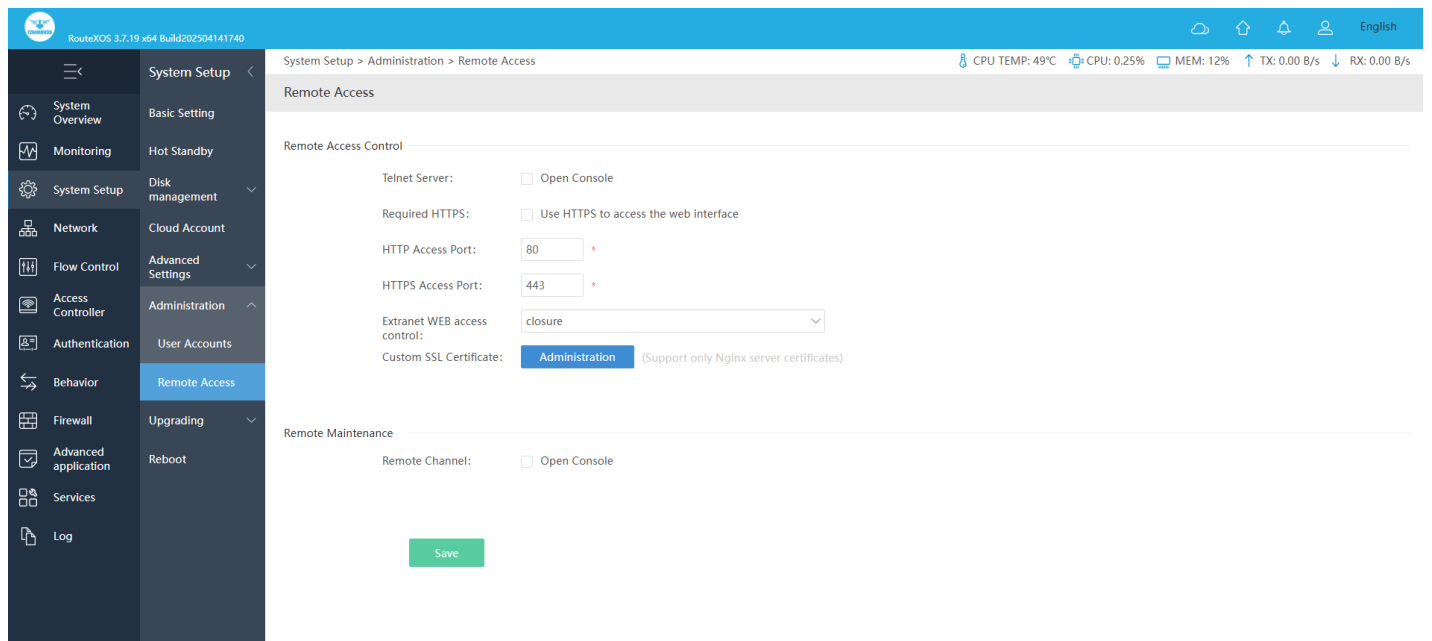


Fig 19. Default Remote access control.

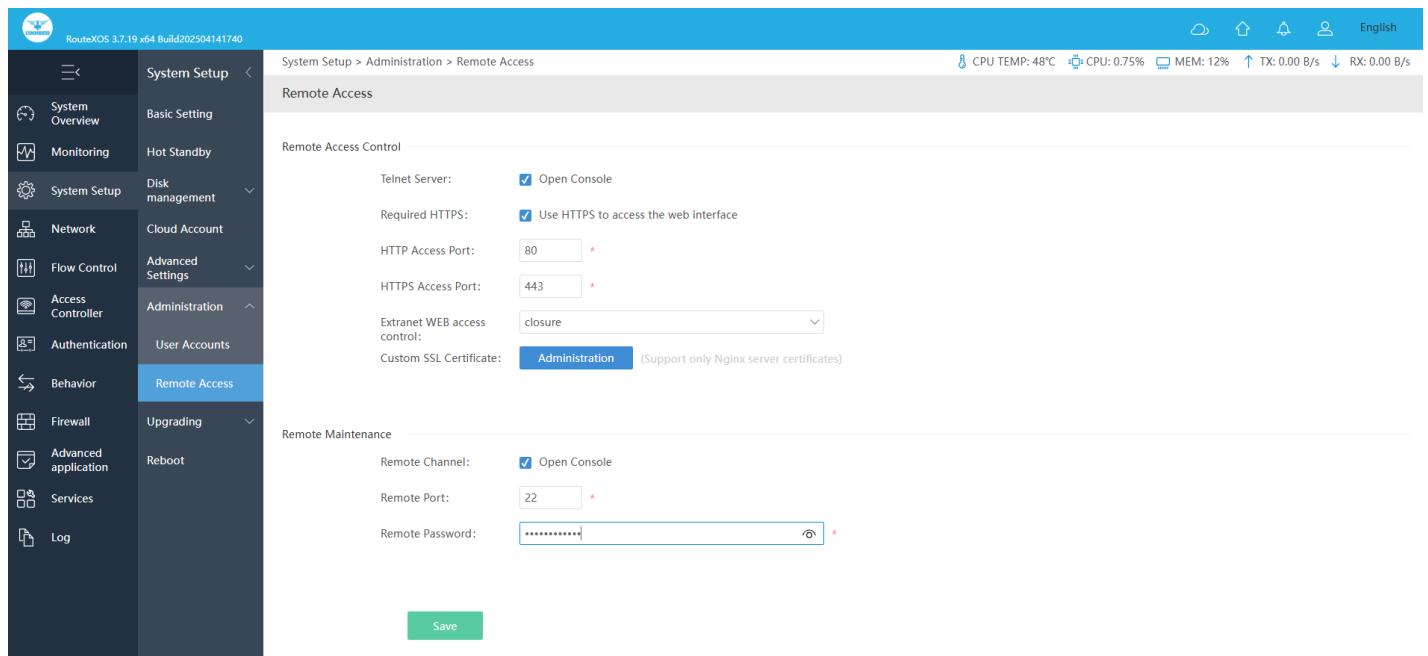


Fig 20. Changing Remote access control setting.

```

username: COMMANDO
passwd:
  console for English                                     Version:
  CMD-COS-v1.01

-----
0. System status | WEB Address -> http://192.168.0.1:80
0
1. Set ether band | lan1 (veth1 08:9b:4b:50:1c:bc)
bc) LinkUp
2. Set lan/wan address | lan1 (veth2 08:24:7c:e0:63:30)
30) LinkUp
3. Set WEB port | lan1 (veth3 08:24:7c:e0:63:31)
31) LinkUp
4. Ping Test | lan1 (veth4 08:24:7c:e0:63:32)
32) LinkDown
5. Clean acl rule | wan1 (veth5 08:24:7c:e0:63:33)
33) LinkUp
6. Restore default |
7. Restore WEB passwd |
8. Reboot/Shutdown |
9. Ethernet driver |
o. Other option |
q. Quit |

Please input:
  console for English                                     Version: CMD-COS-v1.01
-----
0. System status | WEB Address -> http://192.168.0.1:80
1. Set ether band | lan1 (veth1 08:9b:4b:50:1c:bc) LinkUp
2. Set lan/wan address | lan1 (veth2 08:24:7c:e0:63:30) LinkUp
3. Set WEB port | lan1 (veth3 08:24:7c:e0:63:31) LinkUp
4. Ping Test | lan1 (veth4 08:24:7c:e0:63:32) LinkDown
5. Clean acl rule | wan1 (veth5 08:24:7c:e0:63:33) LinkUp
6. Restore default |
7. Restore WEB passwd |
8. Reboot/Shutdown |
9. Ethernet driver |
o. Other option |
q. Quit |

```

Fig 21. Telnet access of MSG-1200

Action Logs: The Log system of Gateway can record, classify and manage the system information effectively.

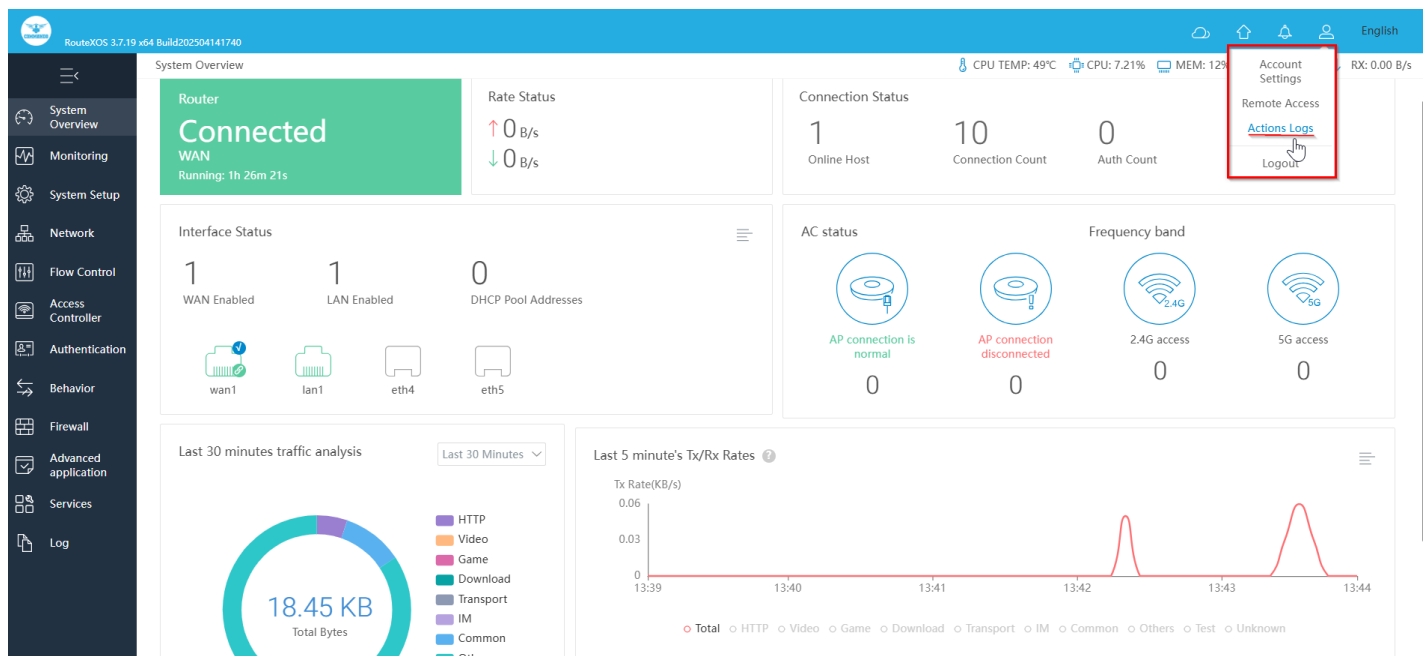


Fig 22. Action Logs shortcut

After clicking action log user will be directed to Log > System Logs > Action Logs

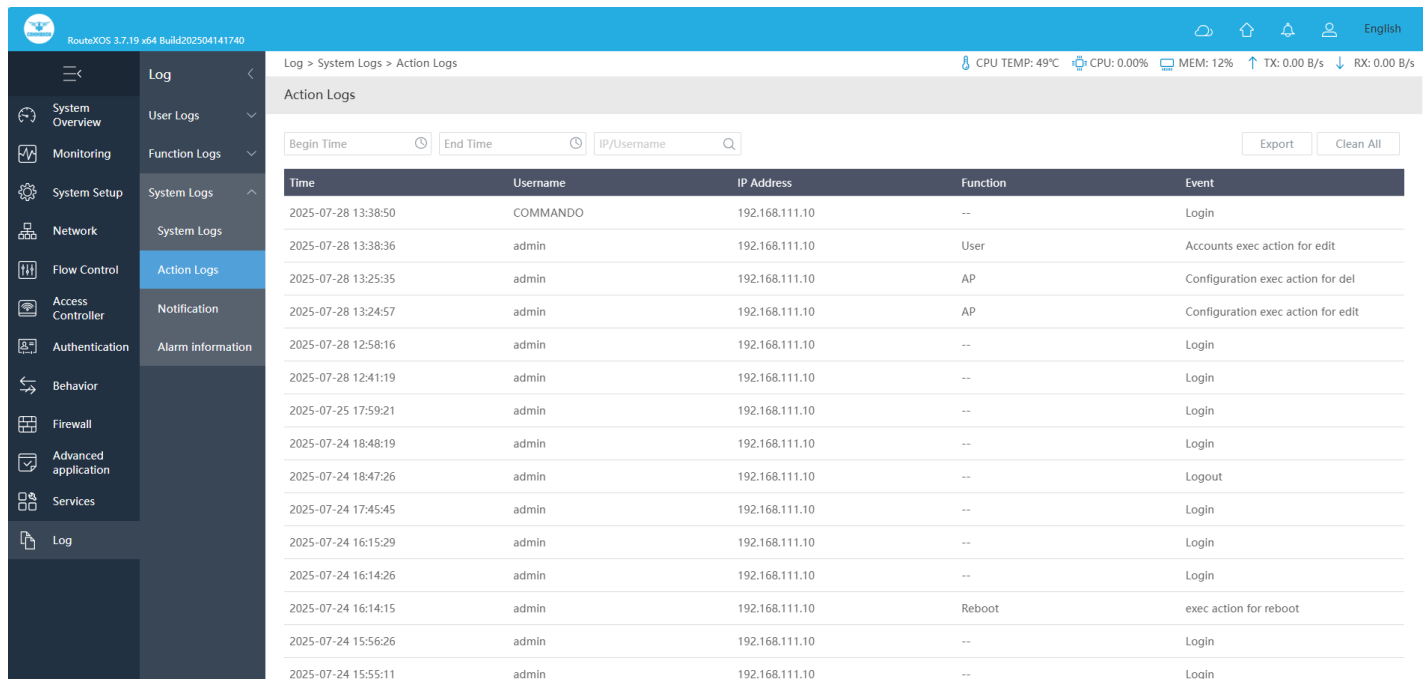


Fig 23. Action Logs in system logs to show the date, time, users, IP and interface to login in MSG-1200

Logout: Logging out means to end access of device. Logging out informs the device that the current user wishes to end the login session.

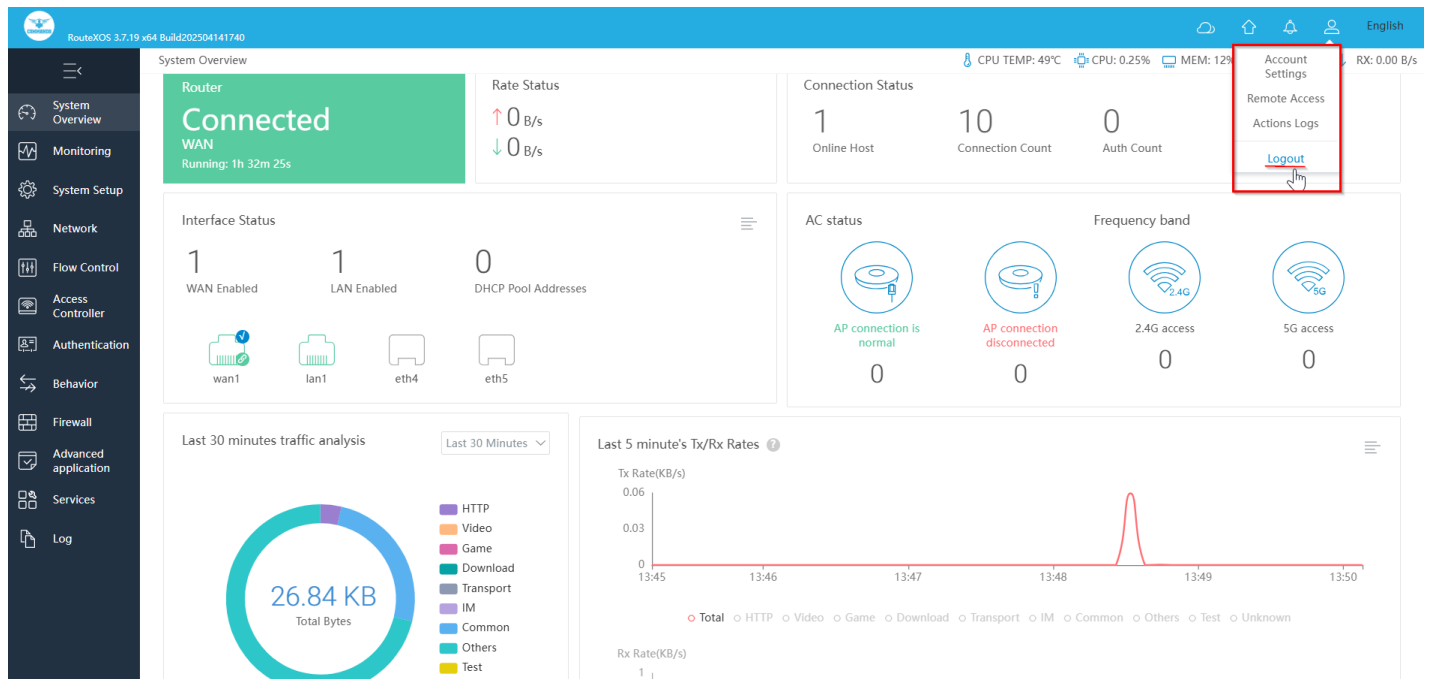


Fig 24. Logout shortcut

After Clicking Logout, it will be directed to Login page.

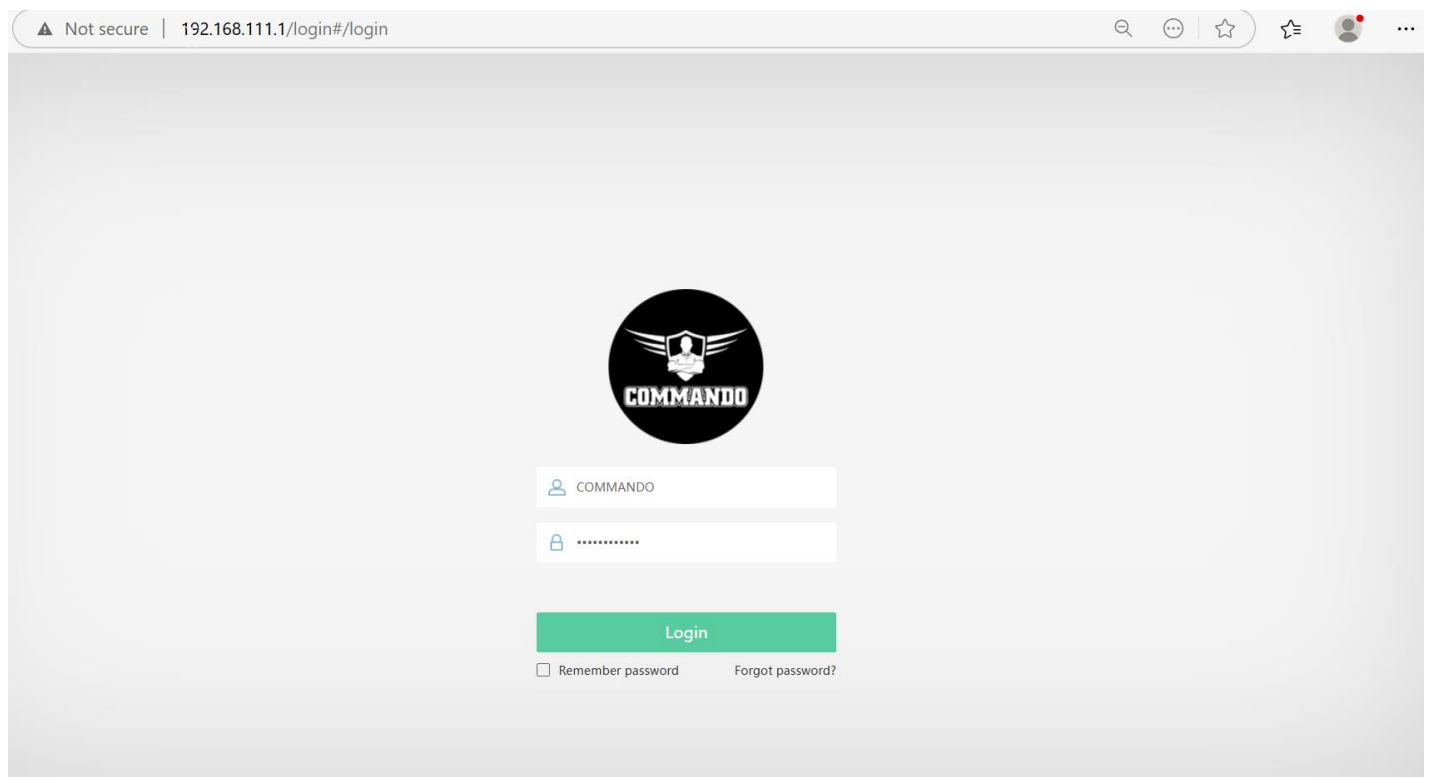


Fig 25. Login page after Logout

Message Notification: Message notifications shows level 5 having severity Normal but significant conditions for user action logs.

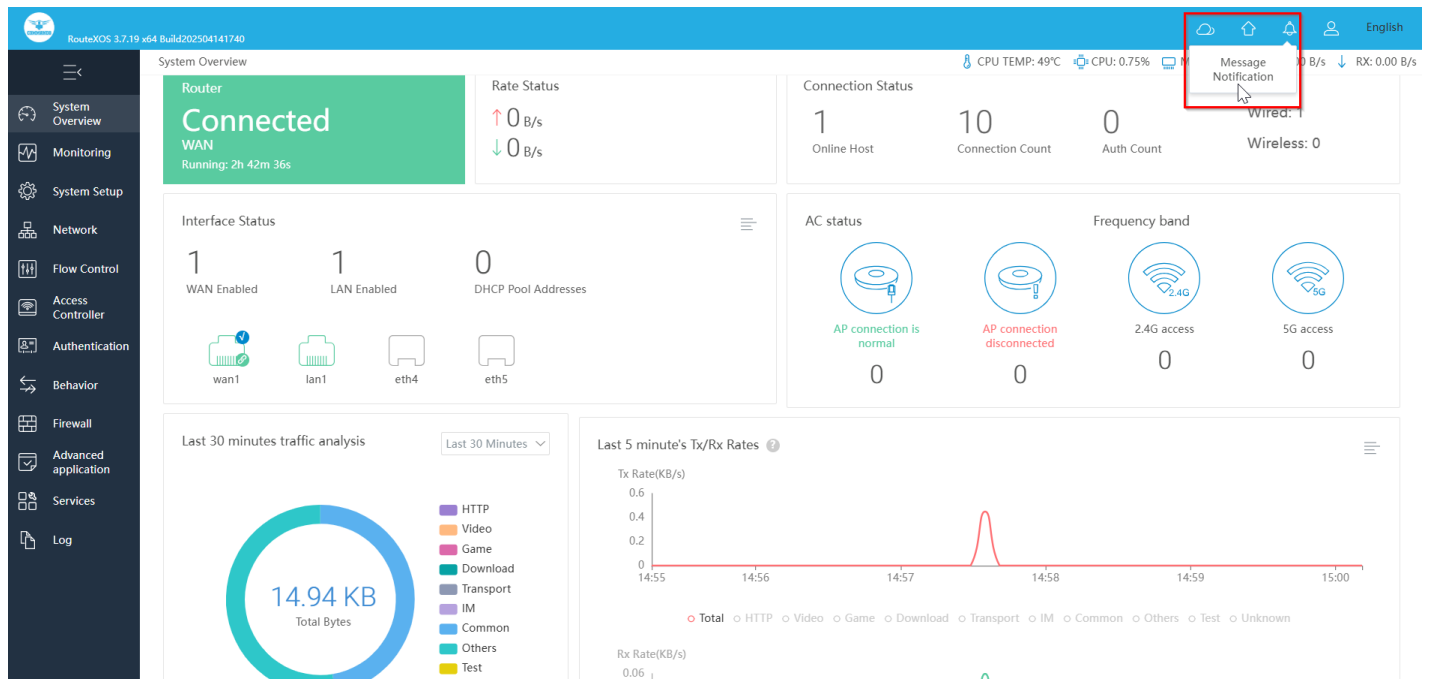


Fig 26. Message notifications Shortcut

After clicking Message Notification, Log > System Logs > Notification page will be opened.

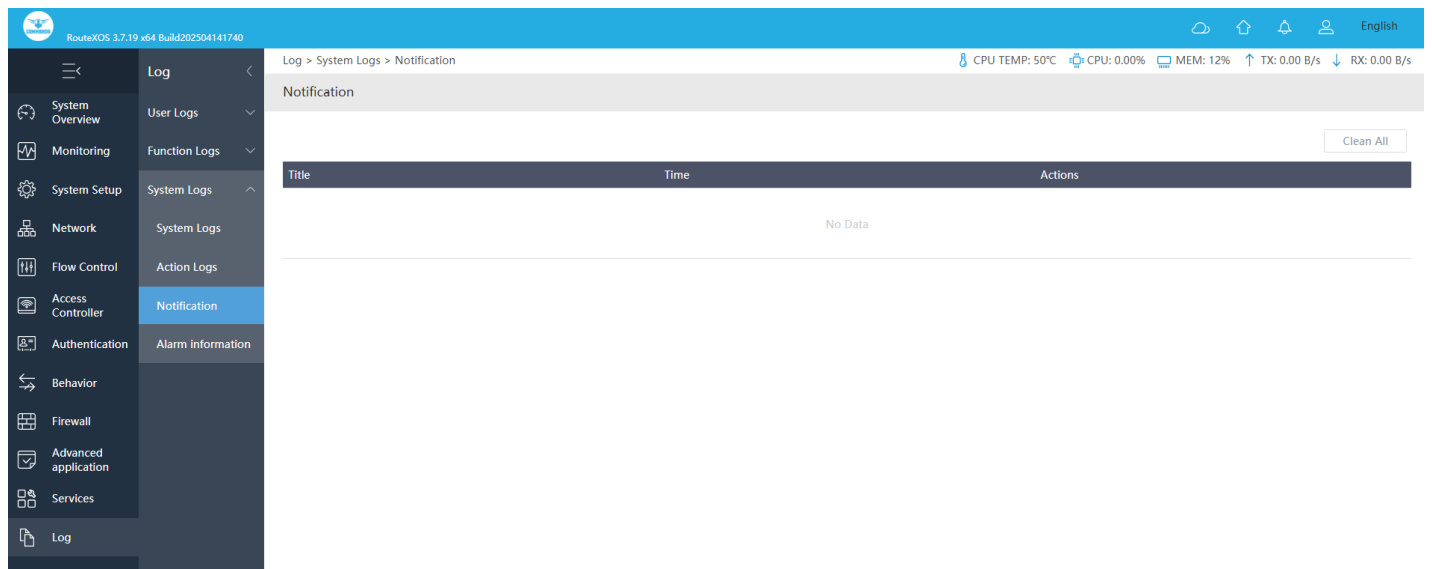


Fig 27. Default Message notifications page

Version Upgrade: Displays the current configuration version of the Gateway and allows Automatic or manual Updates.

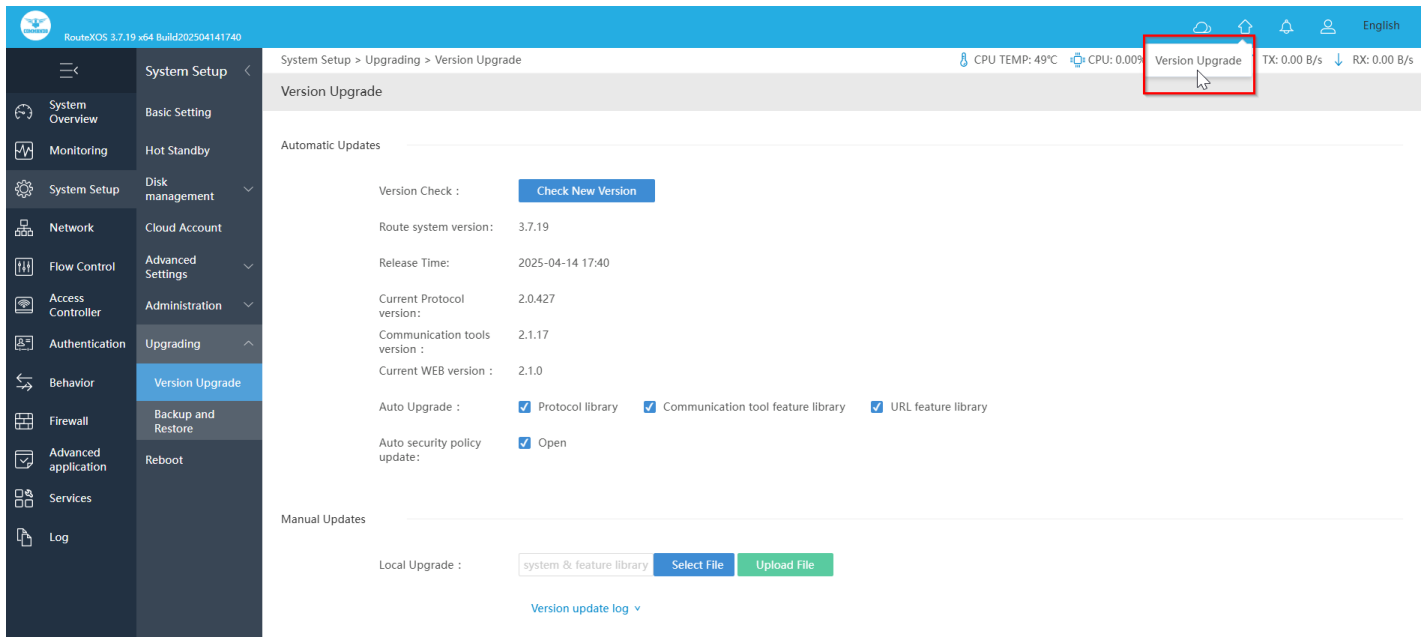


Fig 28. Version Upgrade page

After clicking Version, Upgrade System Setup > Upgrading > Version Upgrade page will be opened.

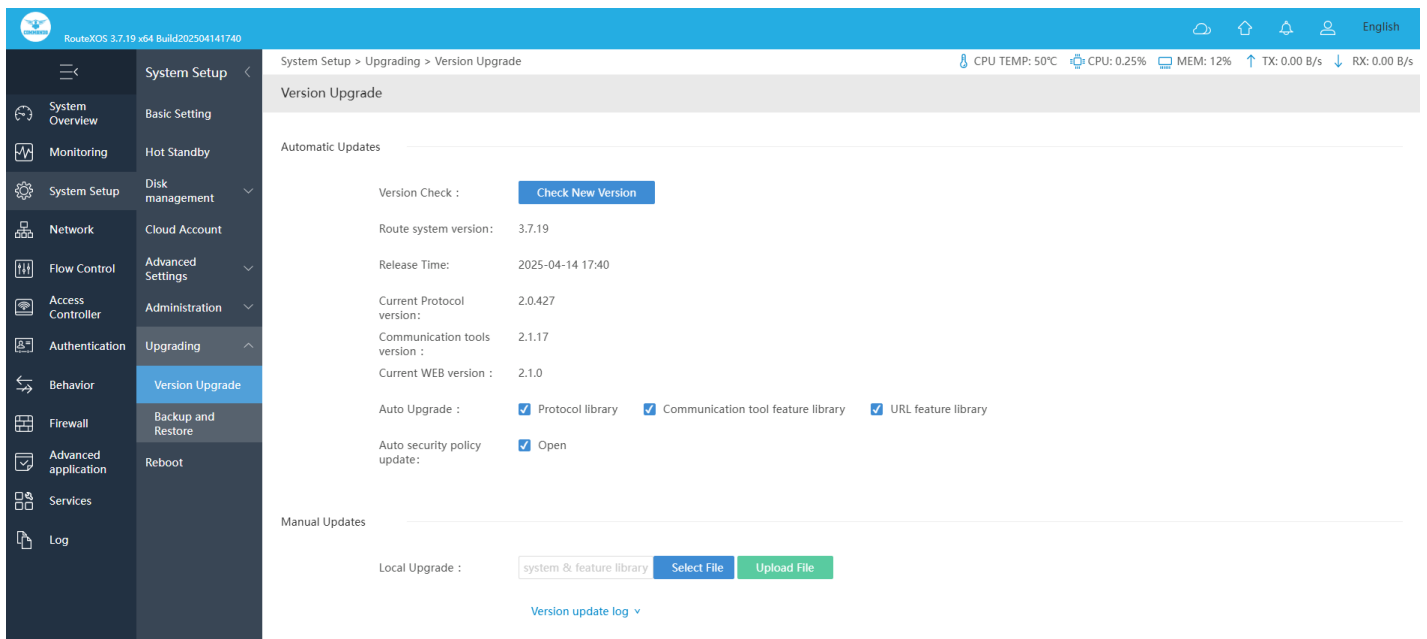


Fig 29. Default Version Upgrade page

Link to Cloud: Cloud service helps users to log ON online for managing the Gateway. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal.

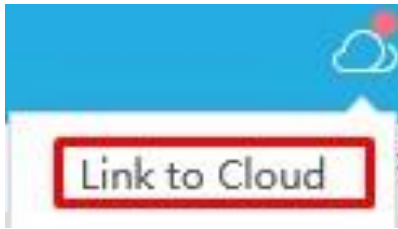


Fig 30. Link to Cloud shortcut

After clicking System Setup > Cloud Account, Cloud account page will be opened.

The screenshot shows the 'System Setup > Cloud Account' page. The left sidebar contains a menu with 'System Setup' highlighted. The main content area has a header with system status: CPU: 2.72%, MEM: 19%, TX: 4.37 KB/s, RX: 68.12 KB/s. Below the header is the 'Cloud Account' section with three input fields: 'Router ID' (pre-filled with '247ce0632ec88bde3e5053d6d00818e8'), 'Account Code' (empty), and 'Comment' (empty). Each field has a red asterisk indicating it is required. Below the fields is a green 'Save' button. At the bottom, there is a 'Help' section with three sub-sections: 'What is cloud service?', 'How to connect to cloud service?', and 'How to manage?'. The 'How to connect to cloud service?' section includes a link 'Into cloud platform'.

Fig 31. Link to Cloud account page

CPU, Memory, Trans and receive icons:

These help us to know running status of Gateway.

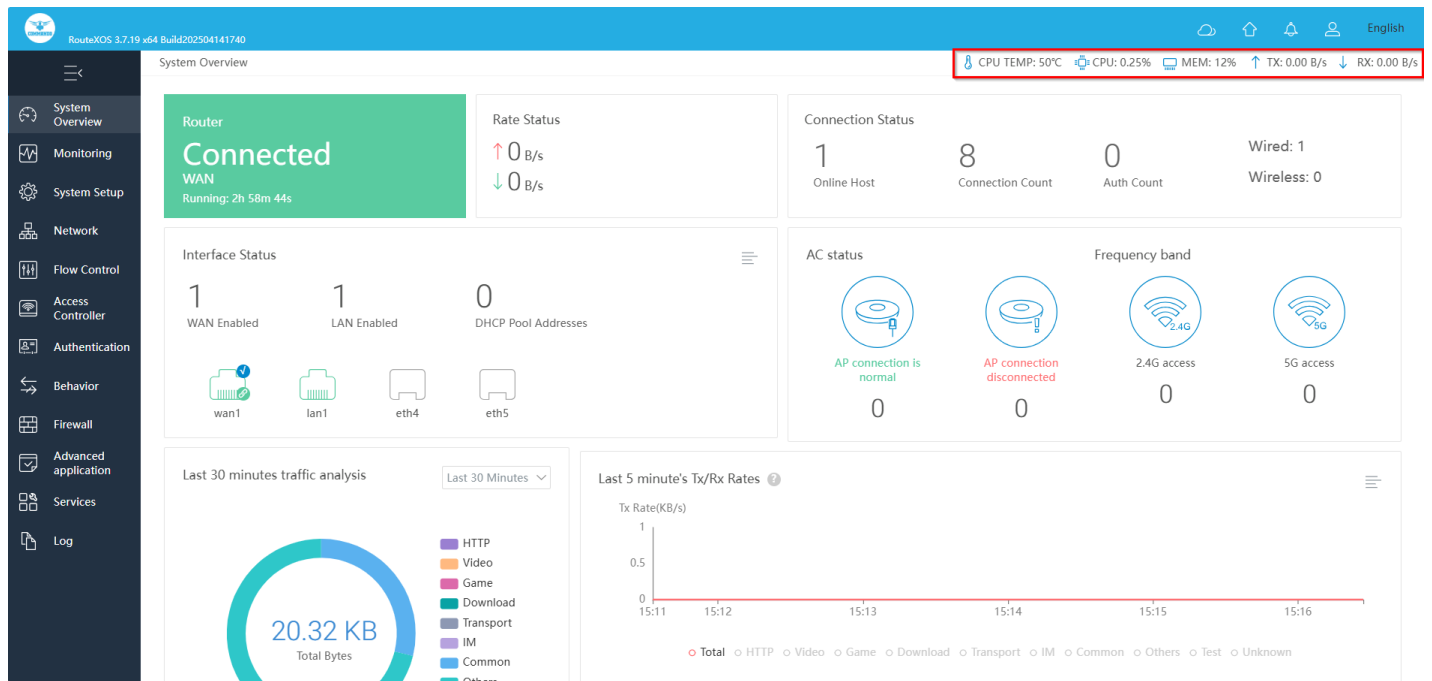


Fig 32. CPU, Memory, Trans and receive icon default display



Fig 33. CPU, Memory, Trans and receive icon display after data transfer enabled

Language Options: Helps to select language as per choice of user.

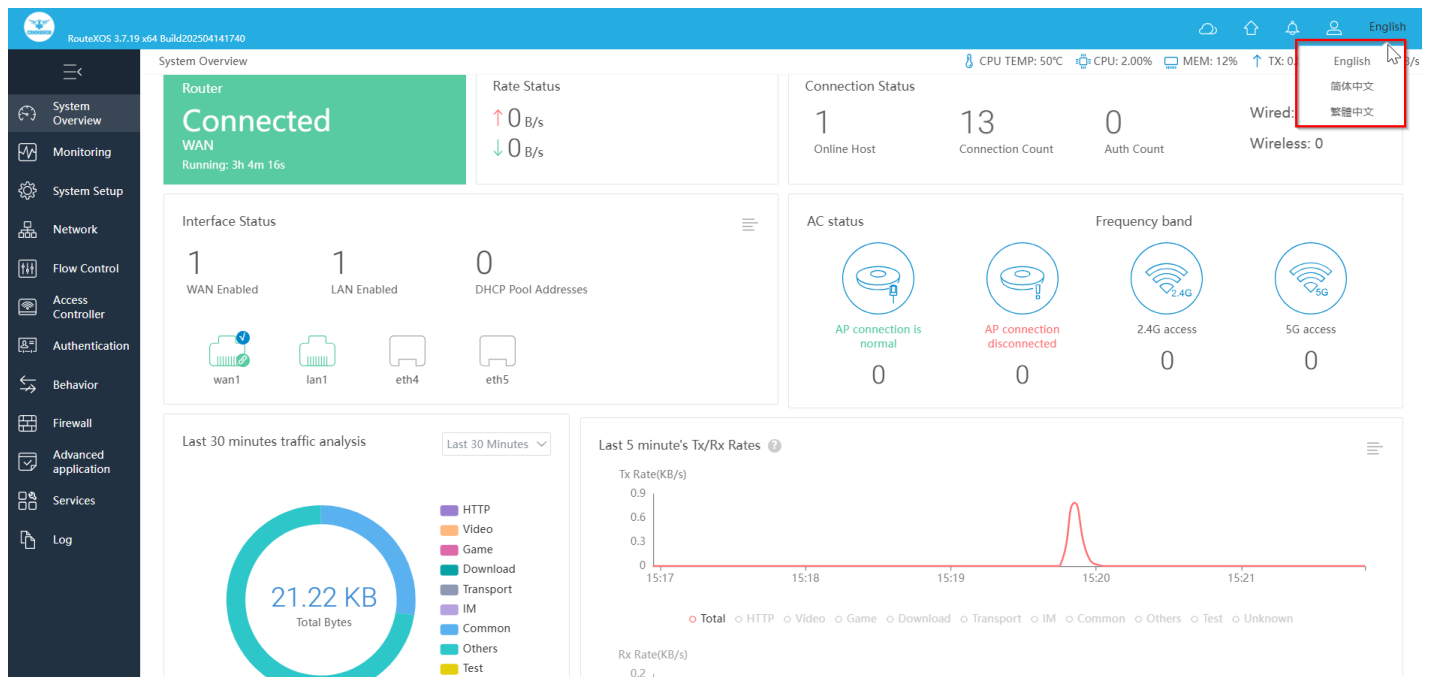


Fig 34. Language selection icon

MONITORING

Monitoring helps to monitor users, devices, ports and devices already configured in network setup.

Interface: Displays the current enabled WAN/LAN port(s). All Interface Status automatically refresh in 5 sec intervals.

Terminal: Terminal monitoring helps to see all IP/MAC binding with Trans, Receive Rates, Uptime of all users and devices with names in remark and also can change, limit and modify the users

Protocol: Protocol Monitoring refresh automatically every 5 seconds by default. It shows Flow/Connections distribution for protocols like HTTP, video, Game, Download, Transport, IM, Common, Test, Unknown, other with percentage and KB or MB downloads.

Policy: Strategy Monitoring for created policy for the entry of the packets allowed or prohibited.

System: System Monitoring shows performance load for 1hrs, 1day, 7 days or 30 days with avg and peak for CPU Usage, Memory Usage, Disk Usage, Online terminal with specific selection options.

Flow Control: Displays the number of flow control frames received or transmitted on the port.

1. Interface

Physical interfaces exist on interface cards and transmit service data. Physical interfaces are classified into the following types:

LAN-side interface used to exchange data with network devices on LANs like Ethernet/Fast Ethernet/ Gigabit Ethernet.

Management interface used to log in to Gateway for configuration and management purposes.

USB interface are data transmission interface.

By clicking on Monitoring > Interface we can view the Interface Monitoring

The screenshot displays the 'Interface Monitoring' page in the RouteXOS management interface. The left sidebar shows the navigation menu with 'Monitoring' selected. The main content area shows the 'Interface Status' section with icons for lan1, wan1, eth4, and eth5. Below this is the 'All Interface Status' table, which lists the IP addresses and connection details for each interface. The 'Outbound Interface Status' table is also visible at the bottom.

Interface	IP Address	Connection Number	Tx	Rx	Tx Bytes	Rx Bytes	Tx Packets/day	Rx Packets/day	Remarks	Actions
lan1	192.168.111.1	--	0 B/s	0 B/s	5.48 MB	34.3 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		
wan1	192.168.1.61	0	0 B/s	41 B/s	1.26 MB	15.12 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		Details

Interface	IP Address	Gateway	Access Mode	Link Time	Failover	Status
wan1	192.168.1.61	192.168.1.1	DHCP	2025-07-28 12:18:40	ON	detected

Fig 1.1.1 Default interface monitoring page

This screenshot shows the 'Interface Monitoring' page after the IP addresses for the LAN and WAN interfaces have been changed. The 'All Interface Status' table now reflects the new IP addresses: 192.168.0.1 for lan1 and 192.168.1.61 for wan1. The 'Outbound Interface Status' table remains the same, showing the wan1 interface with its current configuration.

Interface	IP Address	Connection Number	Tx	Rx	Tx Bytes	Rx Bytes	Tx Packets/day	Rx Packets/day	Remarks	Actions
lan1	192.168.0.1	--	1.06 KB/s	3.29 KB/s	6.15 MB	37.1 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		
wan1	192.168.1.61	1	61 B/s	440 B/s	1.52 MB	18.27 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		Details

Interface	IP Address	Gateway	Access Mode	Link Time	Failover	Status
wan1	192.168.1.61	192.168.1.1	DHCP	2025-07-28 12:18:40	ON	detected

Fig 1.1.2 Interface monitoring page after changing LAN and WAN IP

Following fig shows LAN cable is connected to LAN1, LAN2, LAN3 with 1000Mbps full duplex speed along with Ip address 192.168.0.1/24, MAC : 08:9b:4b:50:1c:bc and LAN4 not connected.

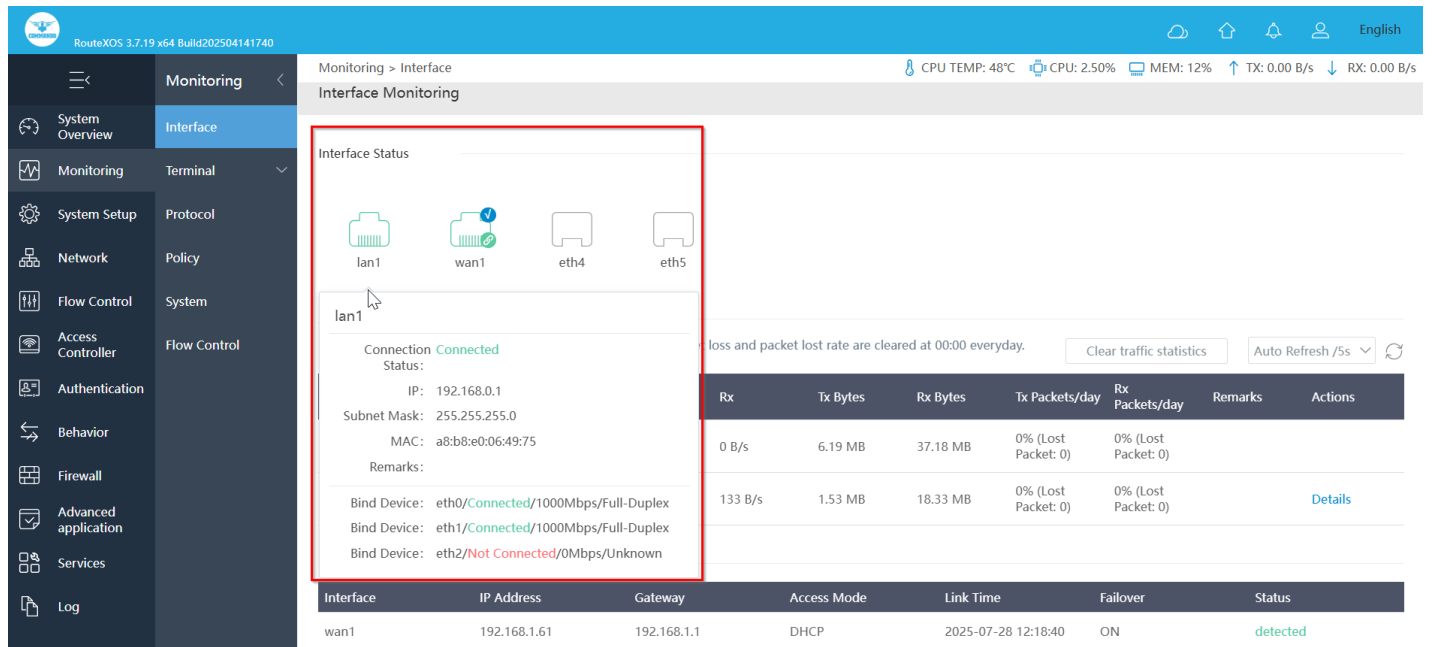


Fig 1.1.3 LAN Interface status

Following fig shows WAN cable is connected to WAN1 and is configured as a Default Gateway. It is up from duration mentioned in figure. It is connected and getting IP from External DHCP server having IP address 192.168.1.38/24 with gateway 192.168.1.1 and DNS : 192.168.1.1 having MAC id 08:24:7c:e0:63:33. Bind Device used is veth5 with speed of connection 100Mbps, Full-Duplex.

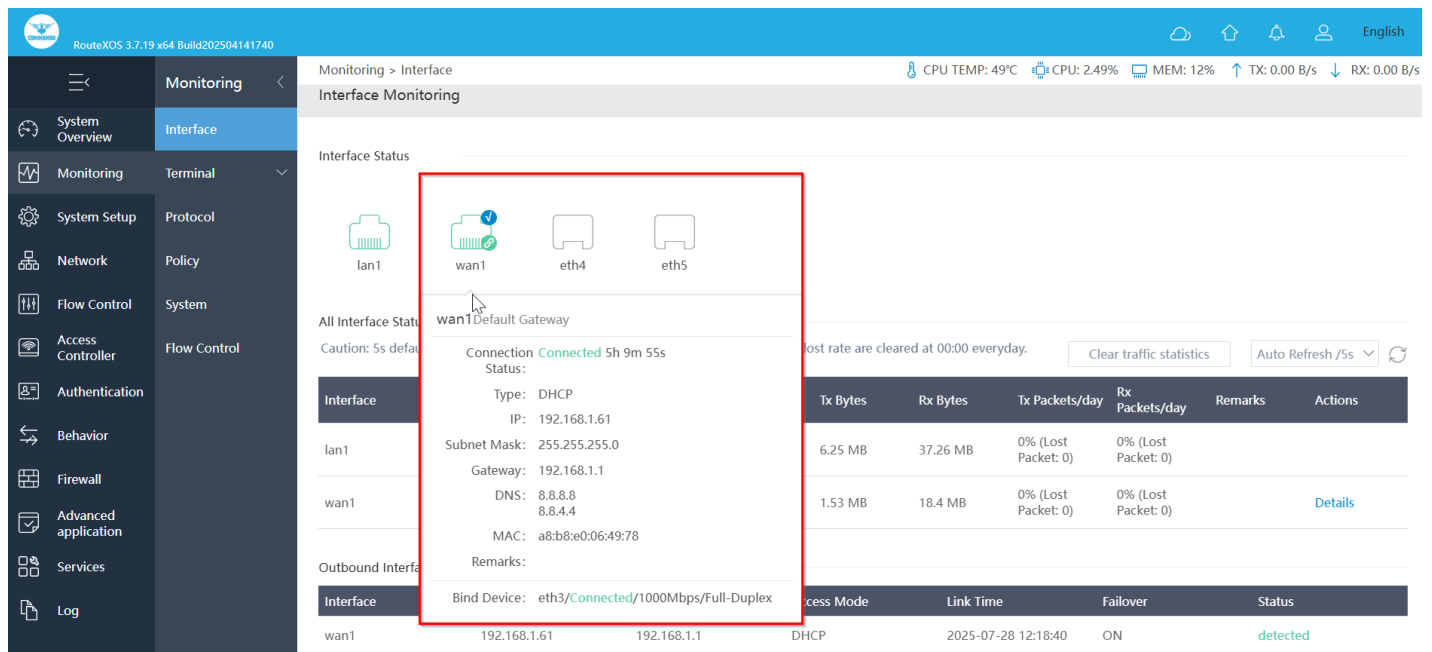


Fig 1.1.4 WAN Interface status

2. Terminal

Terminal monitoring helps to see all IP/MAC binding with Trans, Receive Rates, Uptime of all users and devices with names in remark and also can change, limit and modify the users.

For Configure and view Terminal Monitoring, Click on Monitoring > Terminal

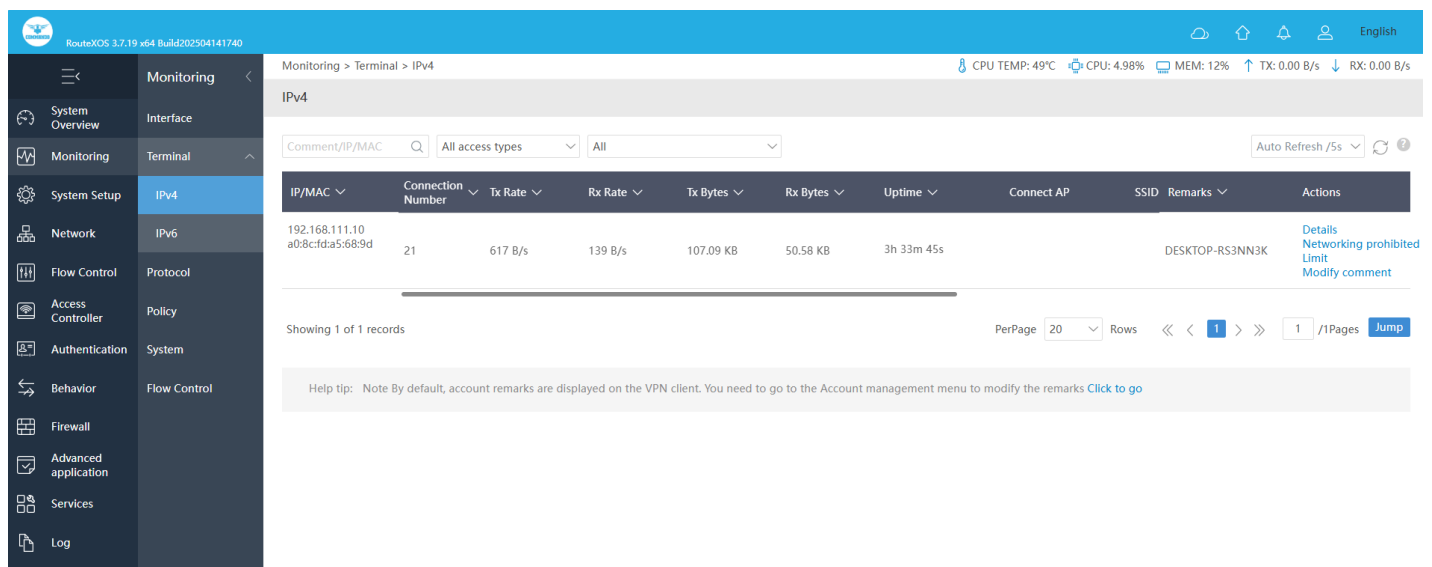


Fig 1.2.1 Default Terminal Monitoring page

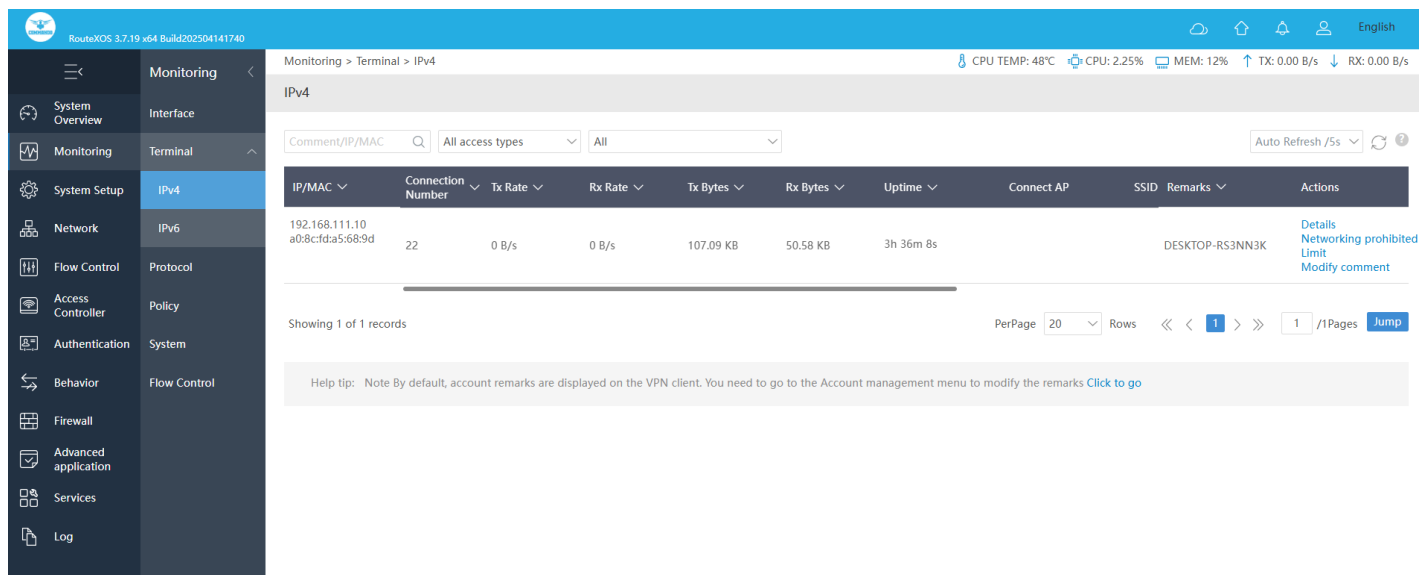


Fig 1.2.2 Terminal Monitoring after connecting devices page

We can take actions to connected IP/MAC devices as per action clicked.

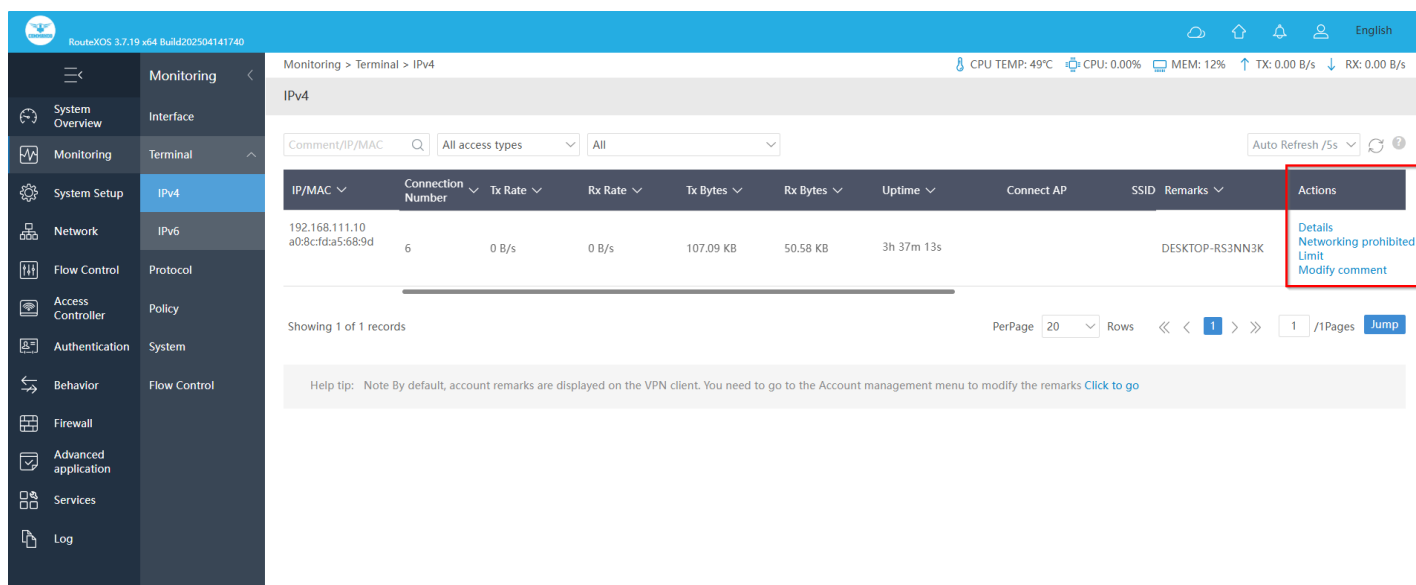


Fig 1.2.3 Terminal Monitoring action page

By clicking details for Monitoring > Terminal Details for connected DESKTOP (PC) having IP 192.168.0.14 following pages are displayed.

The screenshot displays the 'Terminal Monitoring' interface for a specific terminal (DESKTOP-RS3NN3K) with IP 192.168.111.10. The left sidebar shows the navigation menu with 'Monitoring' selected. The main content area is titled 'Terminal Details - DESKTOP-RS3NN3K (IP:192.168.111.10)' and features four tabs: 'Basic Information', 'Connection Details', 'Flow Details', and 'History Logs'. The 'Basic Information' tab is active, showing the following details:

- IP Address:** 192.168.111.10
- MAC Address:** a0:8c:fd:a5:68:9d
- Remarks:** DESKTOP-RS3NN3K
- Terminal type/device manufacturer:** Windows10 / HP
- Uptime:** 3h 38m 44s
- Access Information:**
 - Access mode:** Wired
 - Connect AP:**
 - Connect SSID:**
- Account Information:**
 - Auth Type:**
 - Username:**
 - Affiliation Package:** Custom
 - Bind to MAC Method:** Manual
 - Account Status:**
 - Password:**
 - Valid Date:** Permanent
 - Share:** 1

Fig 1.2.4 Terminal Monitoring details Basic information page

The screenshot displays the 'Terminal Monitoring' interface for the same terminal (DESKTOP-RS3NN3K) with IP 192.168.111.10. The 'Connection Details' tab is active, showing a table of current connections. The table has 11 columns: App Name, Protocol, Interface, WAN Address, Src.Port, Dst.Address, Dst.Port, Tx Bytes, Rx Bytes, and Link Status. There are 11 connections listed, all of which are 'WebAccess' applications using 'tcp' protocol on 'lan1' interface, connecting to '192.168.111.10' on port 80. The 'Link Status' column shows 'ESTABLISHED' for the first and last connections, and 'CLOSE' for the others.

App Name	Protocol	Interface	WAN Address	Src.Port	Dst.Address	Dst.Port	Tx Bytes	Rx Bytes	Link Status
WebAccess	tcp	lan1	192.168.111.10	54858	192.168.111.1	80	802 B	92 B	ESTABLISHED
WebAccess	tcp	lan1	192.168.111.10	54854	192.168.111.1	80	967 B	2 KB	CLOSE
WebAccess	tcp	lan1	192.168.111.10	54855	192.168.111.1	80	967 B	2 KB	CLOSE
WebAccess	tcp	lan1	192.168.111.10	54853	192.168.111.1	80	0.98 KB	1.47 KB	CLOSE
WebAccess	tcp	lan1	192.168.111.10	54857	192.168.111.1	80	873 B	1.13 KB	CLOSE
WebAccess	tcp	lan1	192.168.111.10	53885	192.168.111.1	80	9.05 KB	11.04 KB	ESTABLISHED
WebAccess	tcp	lan1	192.168.111.10	54856	192.168.111.1	80	925 B	1.19 KB	CLOSE
WebAccess	tcp	lan1	192.168.111.10	54859	192.168.111.1	80	847 B	92 B	ESTABLISHED

Fig 1.2.5 Terminal Monitoring connection details page

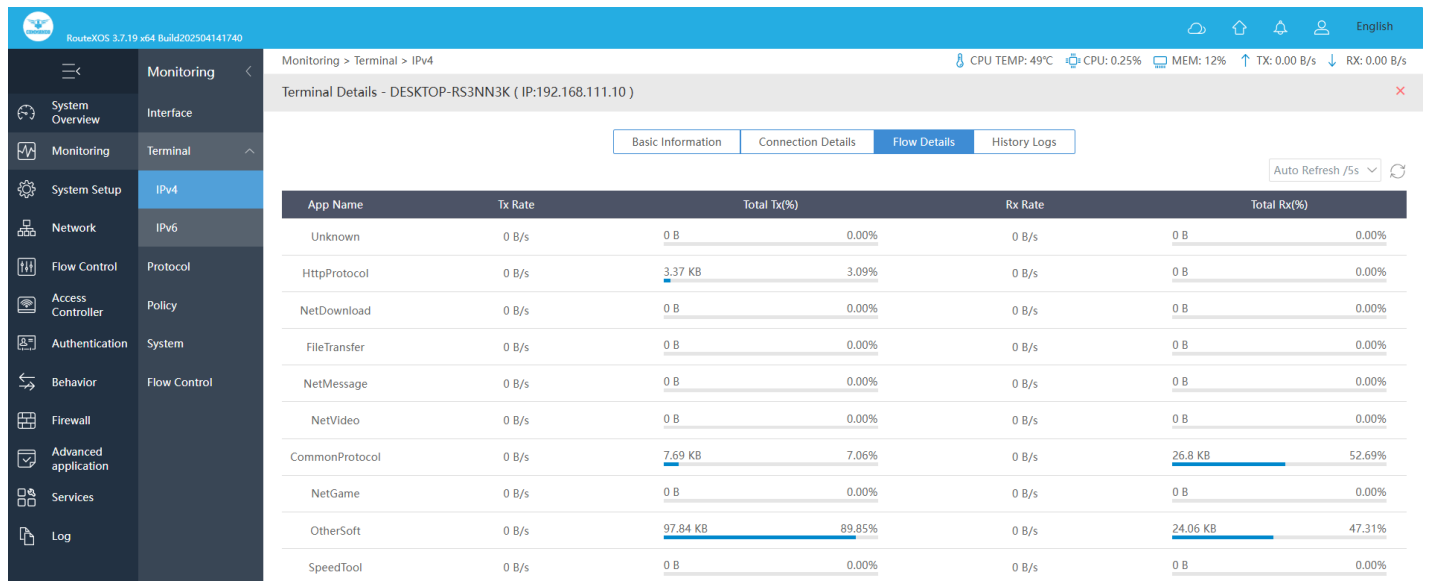


Fig 1.2.6 Terminal Monitoring flow details page

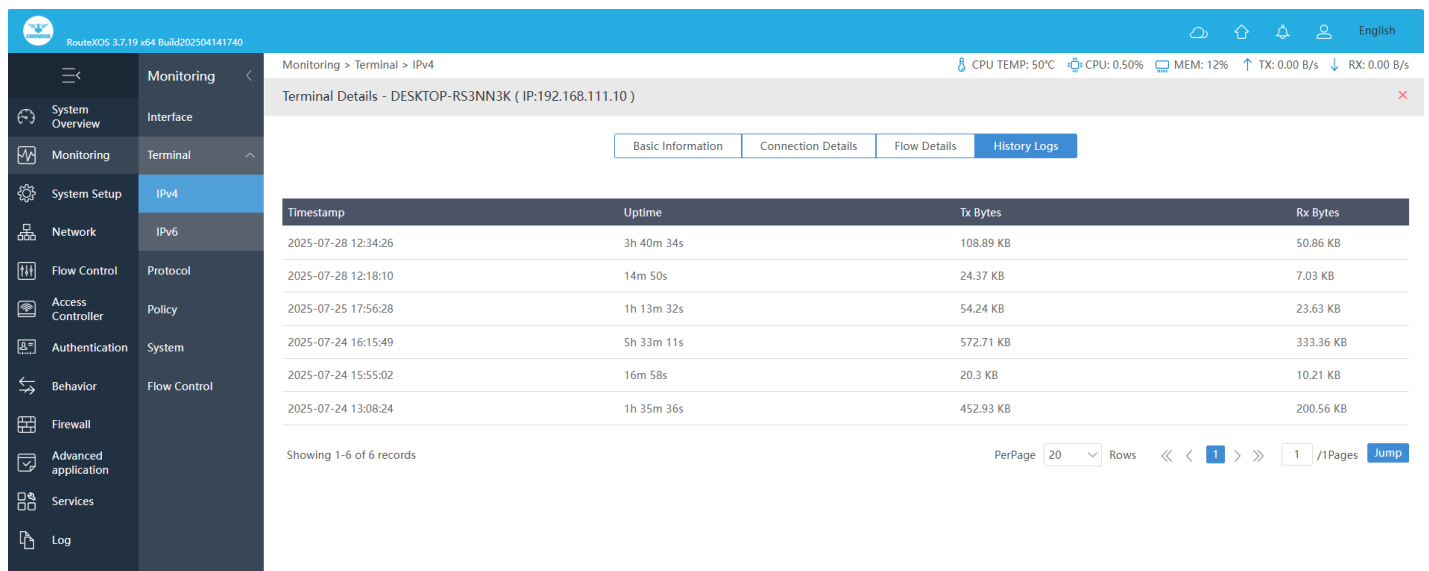


Fig 1.2.7 Default Terminal Monitoring History Logs page

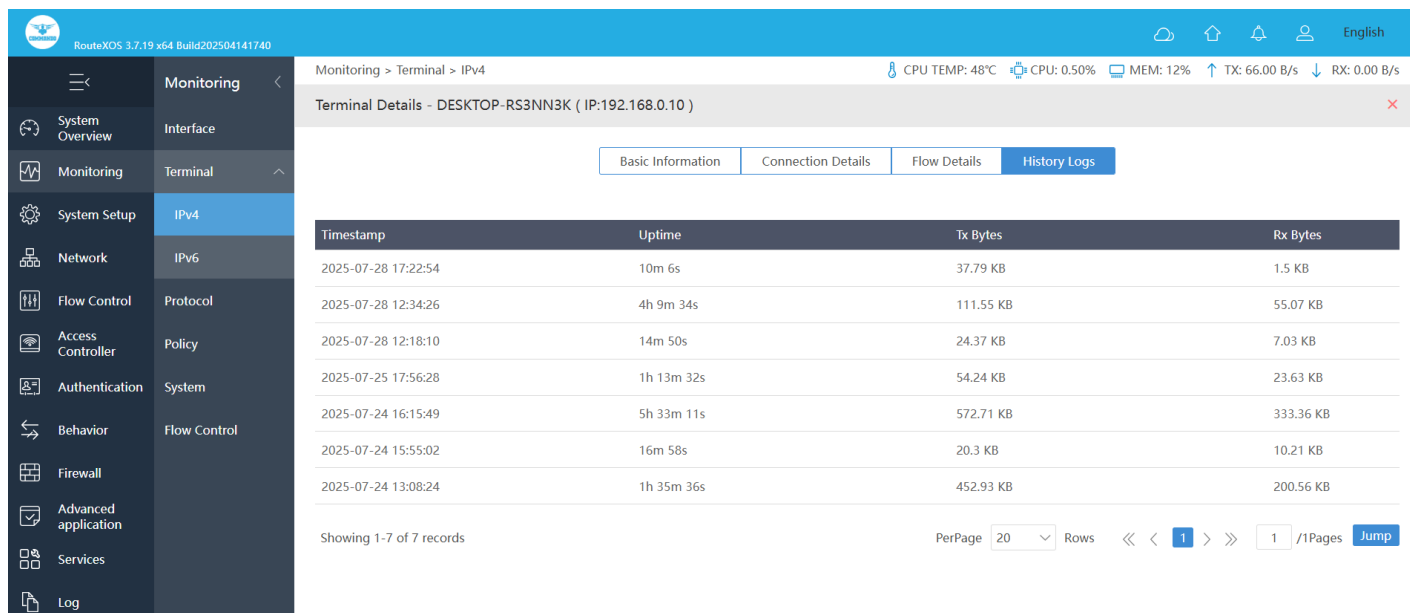


Fig 1.2.8 Terminal Monitoring History Logs page

3. Protocol

Protocol Monitoring shows Flow/Connections distribution for protocols like HTTP, video, Game, Download, Transport, IM, Common, Test, Unknown, other with percentage and KB or MB downloads.

For Protocol Monitoring, Click on Monitoring > Protocol

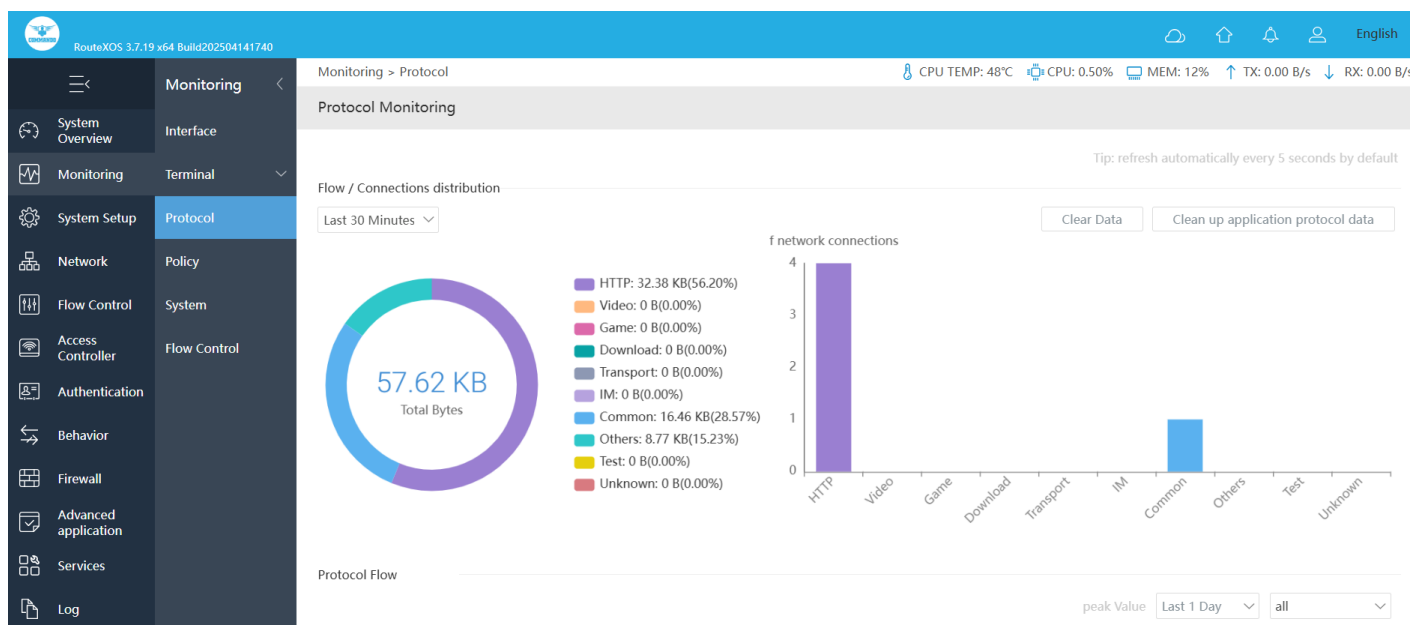


Fig 1.3.1 Protocol Monitoring flow/connections distribution default page

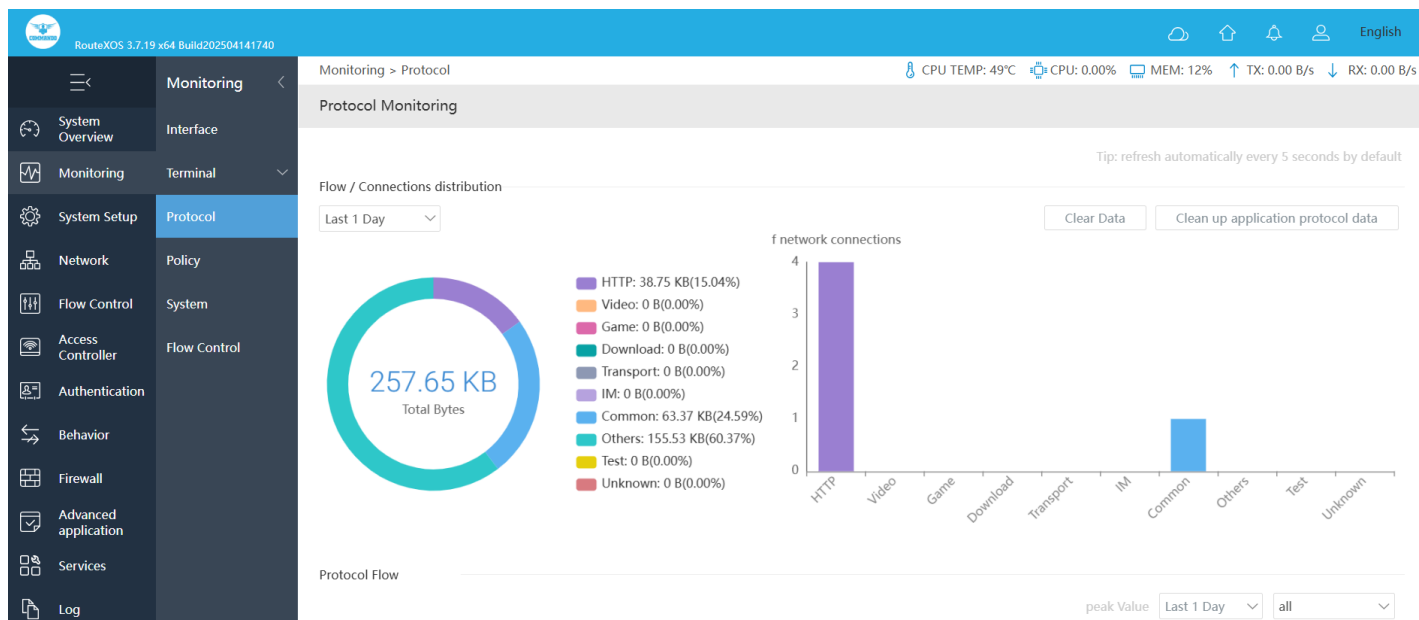


Fig 1.3.2 Protocol Monitoring flow/connections distribution for 1 day page

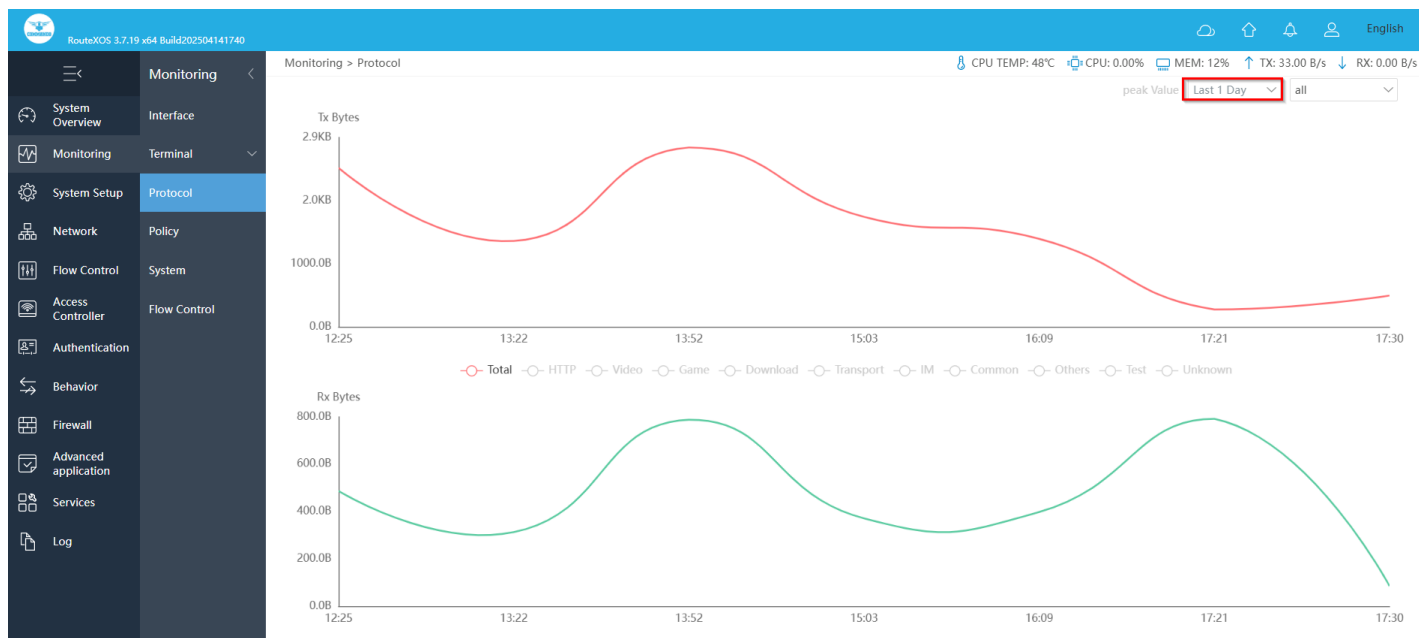


Fig 1.3.3 Default Protocol Monitoring Graphs default page



Fig 1.3.4 Protocol Monitoring Graphs for last 1 hour page

4. Policy

Network policy is a collection of rules that govern the behaviors of network devices. The primary purpose of a network security policy is to inform users and staff the requirements for protecting various assets. These assets take many forms, including passwords, documents, or even servers. Strategy Monitoring for created policy for the entry of the packets allowed or prohibited.

For Strategy Monitoring, Click on Monitoring > Policy

The screenshot displays the 'Monitoring > Policy' page in the RouteXOS interface. The left sidebar shows the navigation menu with 'Monitoring' selected. The main area contains a table titled 'Strategy Monitoring'. The table has columns: Strategy name, Prio, IP, Up speed (KB/s), Down rate (KB/s), Total Tx, and Total Rx. The table is currently empty, showing 'No Data'. The top status bar indicates system metrics: CPU TEMP: 48°C, CPU: 1.75%, MEM: 12%, TX: 33.00 B/s, and RX: 0.00 B/s. A 'Select' button and an 'Auto Refresh /5s' dropdown menu are visible. A tip at the bottom right states: 'Tip: refresh automatically every 5 seconds by default'.

Strategy name	Prio	IP	Up speed (KB/s)	Down rate (KB/s)	Total Tx	Total Rx
No Data						

Fig 1.4.1 Default Policy Monitoring page

5. System

System Monitoring shows performance load for 1hrs, 1day,7 days or 30 days with avg and peak for CPU Usage, Memory Usage, Disk Usage, Online terminal with specific selection options.

System Monitoring for Performance/Network Load, Click on Monitoring > System

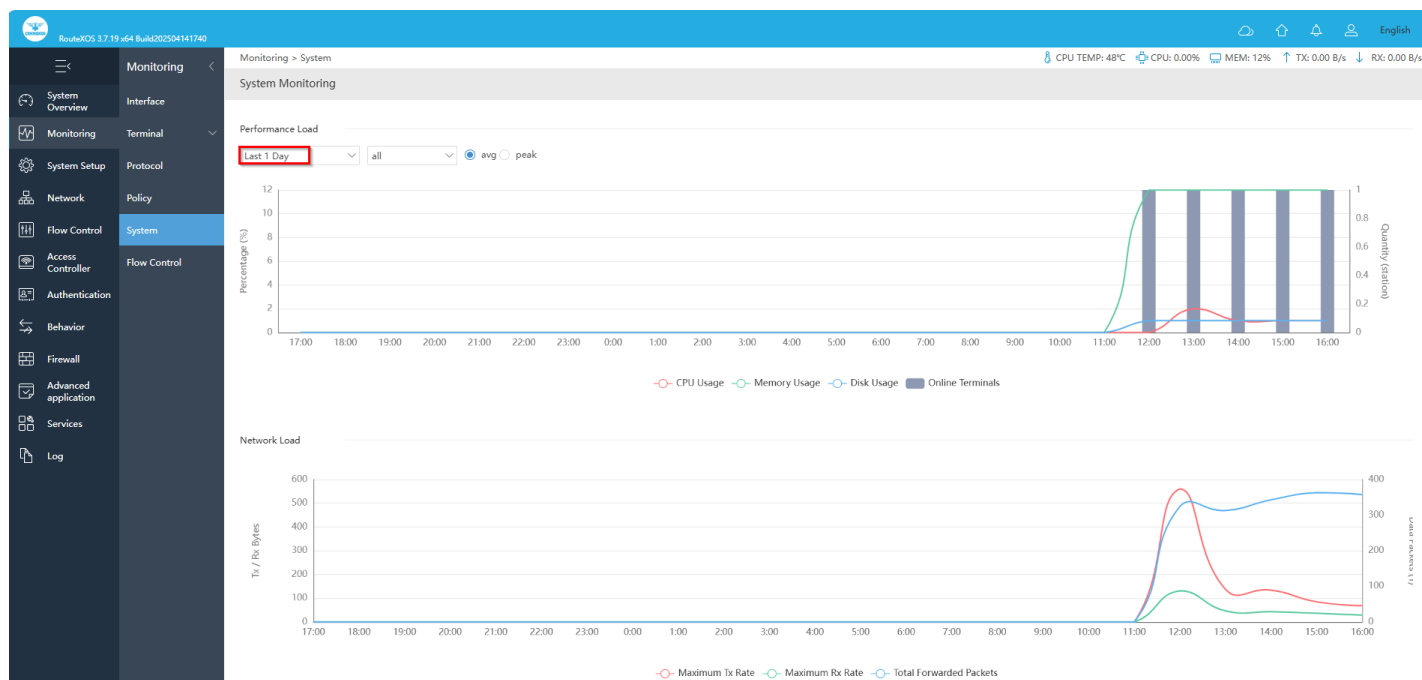


Fig 1.5.1 Default System Monitoring page

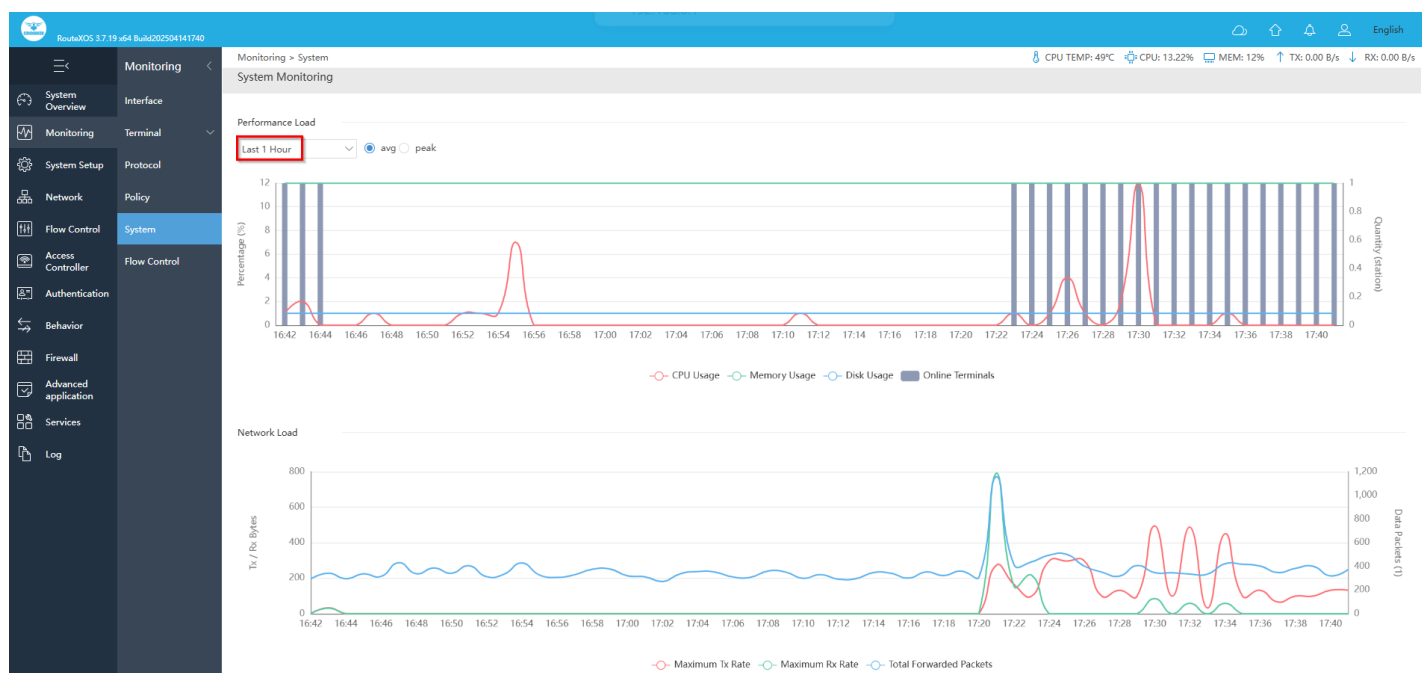


Fig 1.5.2 System Monitoring for 1hour page

6. Flow Control

Flow control determines how resources in a network are allocated to packets traversing the network. Displays the number of flow control frames received or transmitted on the port.

For Flow Control Monitoring, Click on Monitoring > Flow Control

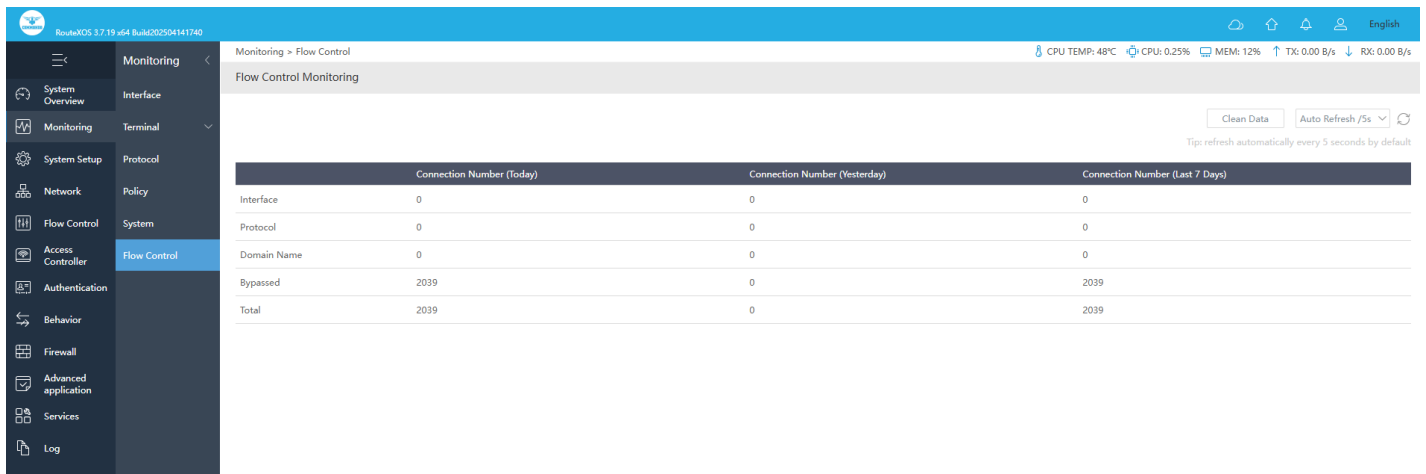


Fig 1.6.1 Default Flow Control page

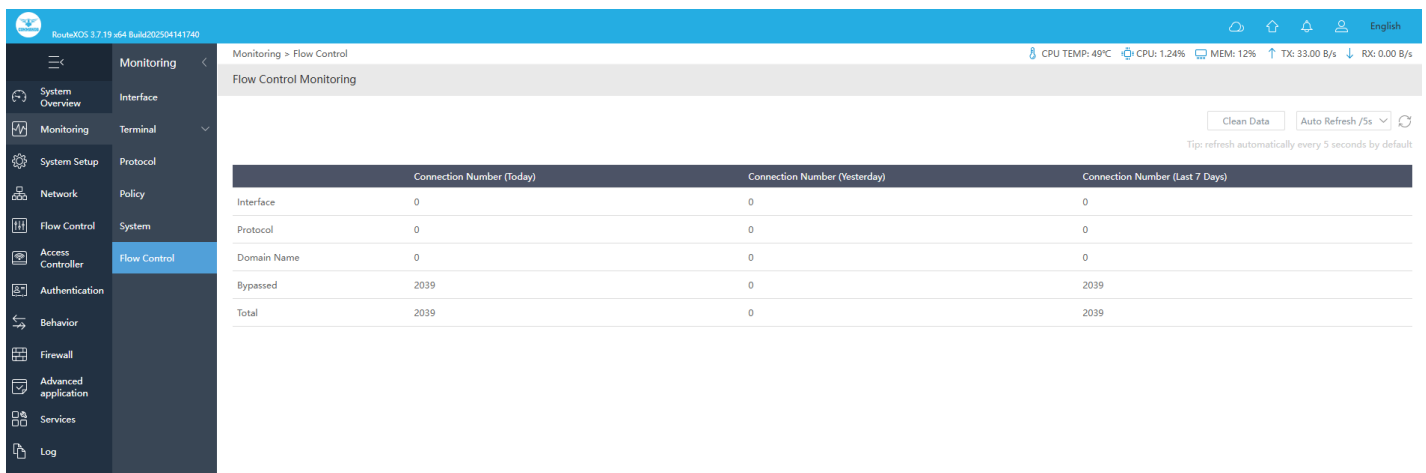


Fig 1.6.2 Flow Control page

7. Switch Monitoring

Switch monitoring provides real-time insights into the status and performance of network switches, displaying key metrics such as port activity, errors, and traffic statistics.

For Switch Monitoring, Click on Monitoring > Switch Monitoring

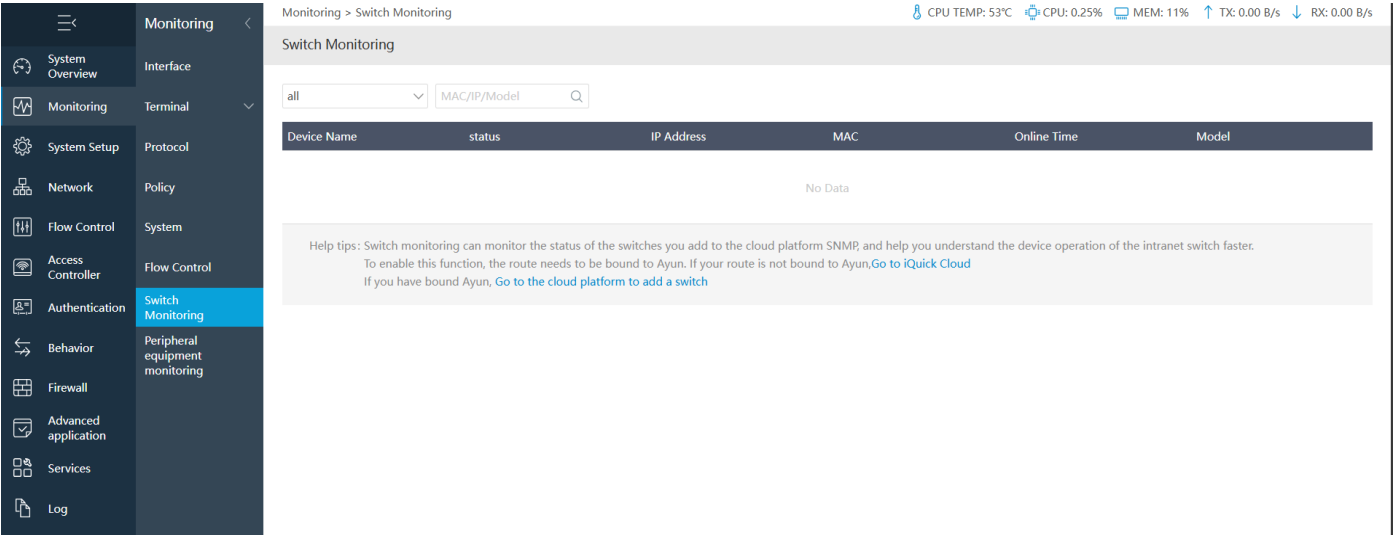


Fig 1.7.1 Default Switch Monitoring page

8. Peripheral equipment monitoring

Peripheral equipment monitoring tracks the status and performance of connected devices, displaying key metrics such as activity, errors, and operational statistics.

For Flow Control Monitoring, Click on Monitoring > Peripheral equipment monitoring

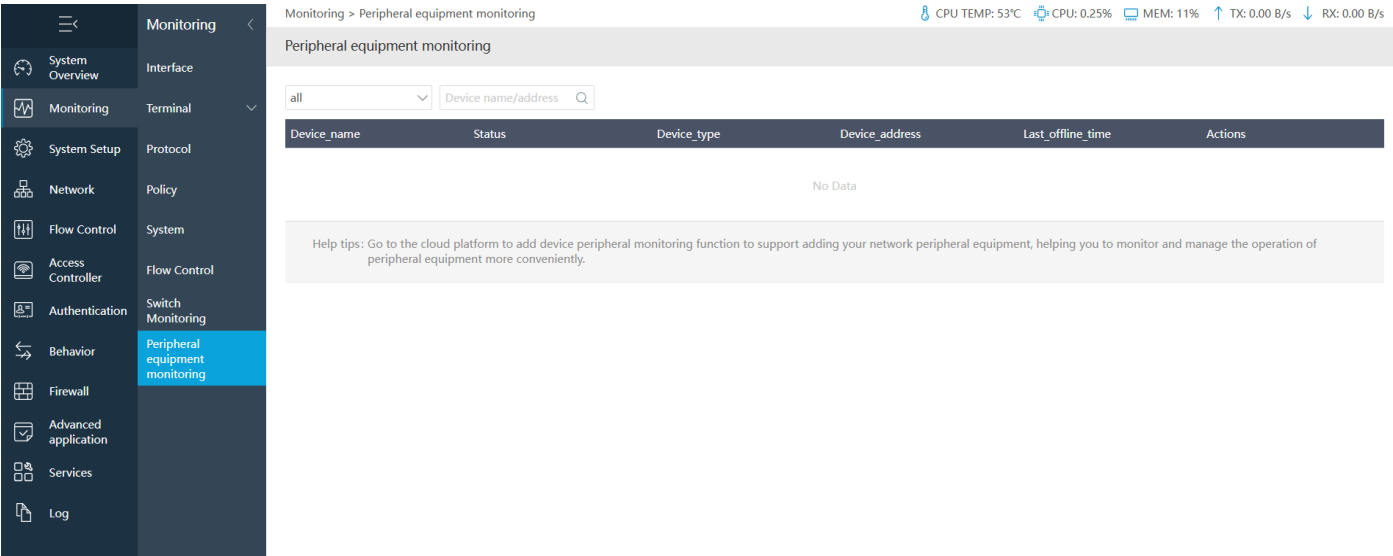


Fig 1.8.1 Default Flow Control page

SYSTEM SETUP

System Setup allows you to configure various services and system setting and consist of following options

Basic Setting: Basic Settings shows System Information like device name, Network mode, Time Settings for System Time along with Time Zone, Time Setting.

Disk management: Each hard disk can support up to 8 partitions, and the system disk can be divided into 4 additional partitions and External hard disks must be formatted or partitioned after binding services, otherwise related services will use system disk space by default. Disk partitions support bundled functional services including ordinary storage, behavior records, Cache Service (partition size 10G and above)

Cloud Account: Cloud service allows to manage the Gateway from anywhere. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal.

Advanced Settings: Allows or disallow FTP, TFTP, SIP, H323 ALG setting.

Administration: Can add, delete or modify user account and allow Remote Access Control for telnet and web access.

Upgrading: Displays the current configuration version of the Gateway and allows Automatic or manual Updates. Backup the current configuration, Upload the backup configuration and Restore default configuration. It can also make device to restore to Factory reset.

Reboot: Reboot at Schedule date and time with daily or user specified time.

1. Basic Setting

Basic Settings is for setting System Information like device name, Network mode, Time Settings for System Time along with Time Zone, Time Setting. Device name is name given to device to be displayed on system Overview page for easy identification of Gateway.

To configure and view basic setting click on System Setup > Basic Setting

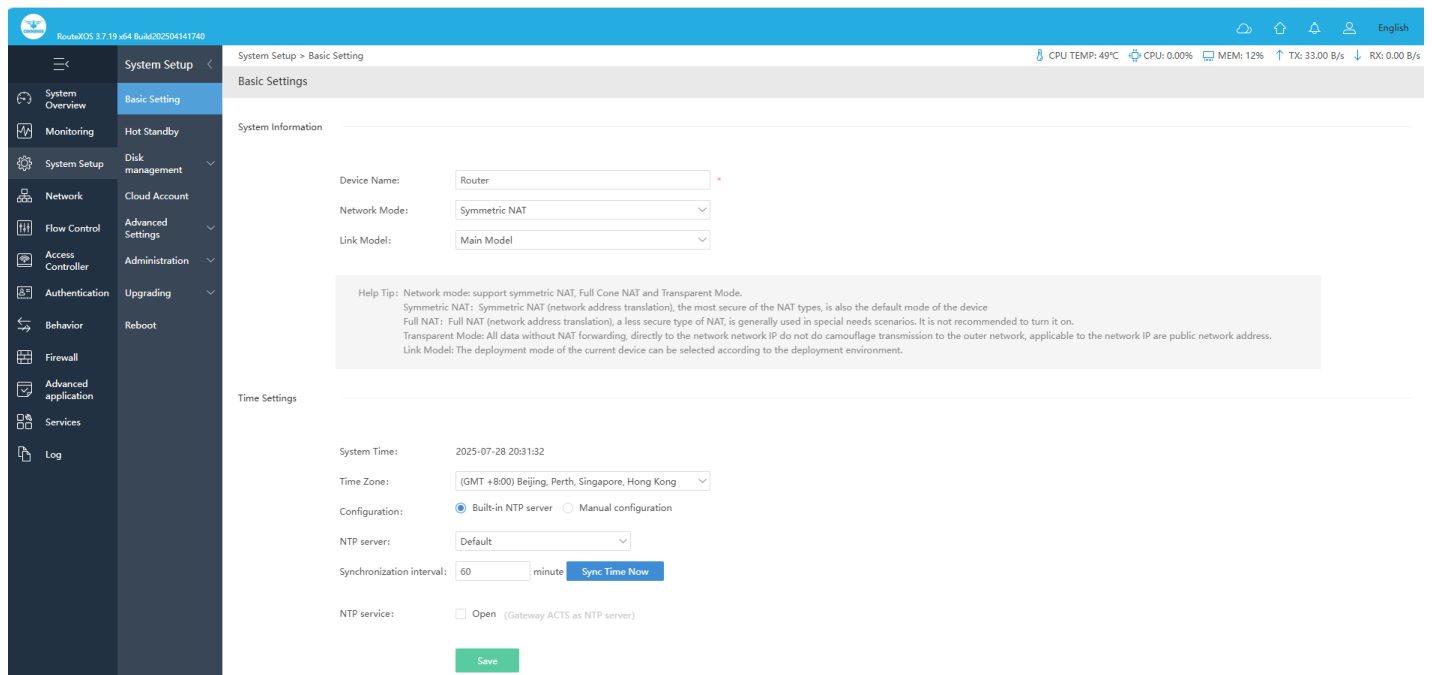


Fig 2.1.1 Default Basic setting page

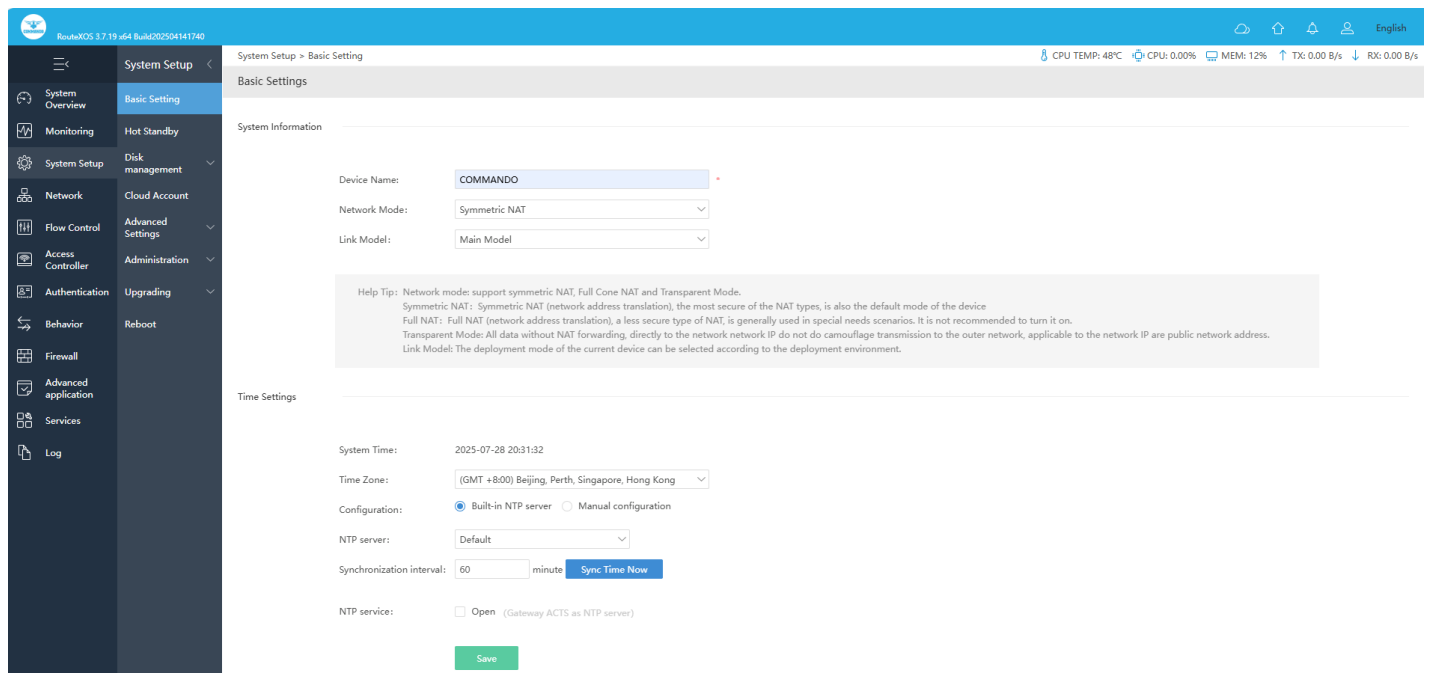


Fig 2.1.2 Basic setting for changing device name page

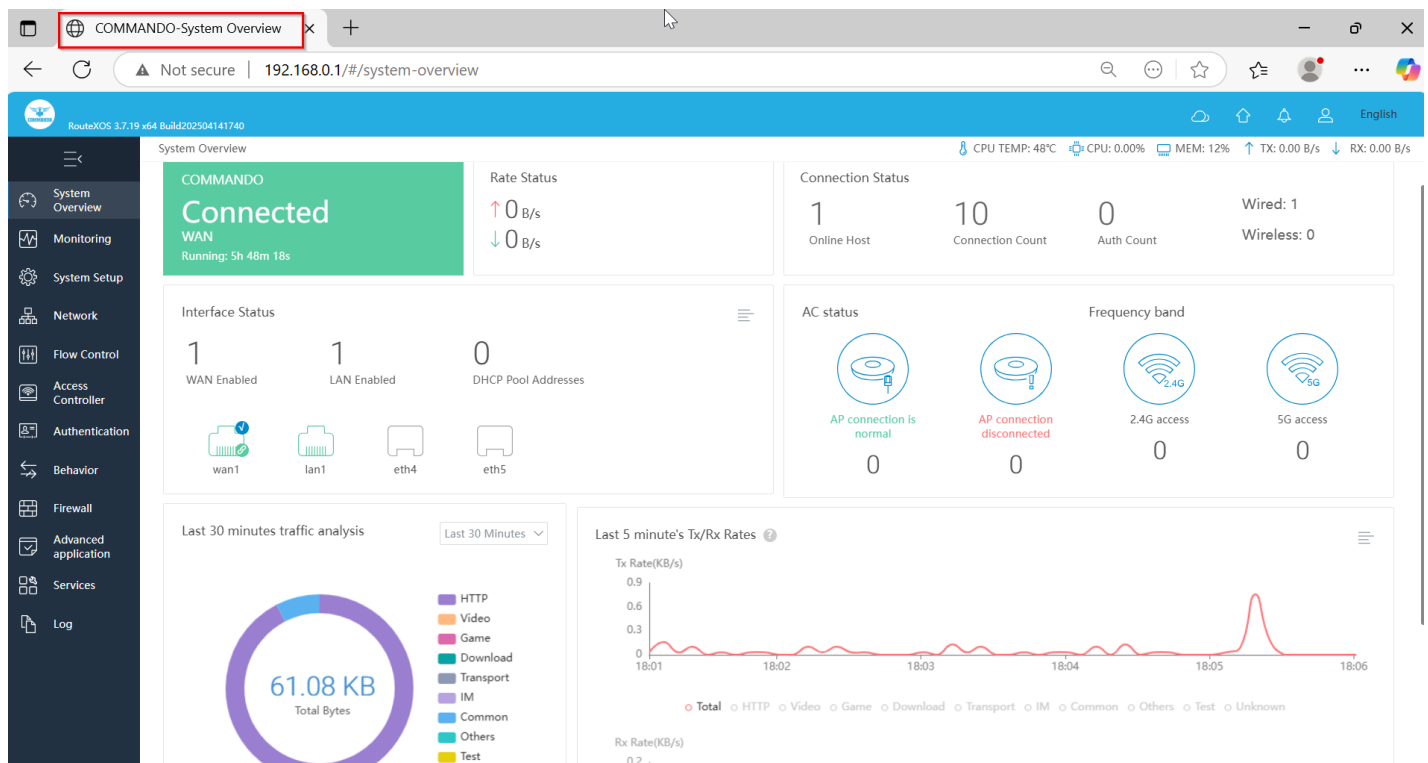


Fig 2.1.3 XYZ Device name page

Network Mode: Network mode is used to configure Network Address Translation (NAT). It is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT (Network Address Translation) is the translation between private IP and public IP, which allows private network users to visit the public network using private IP addresses. With the explosion of the Internet, the number of available IP addresses is not enough. NAT provides a way to allow multiple private hosts to access the public network with one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security of the network since the address of LAN host never appears on the Internet. In this Gateway support symmetric NAT, Full Cone NAT and Transparent Mode NAT. Symmetric NAT is the most secure of the NAT types, is also the default mode of the device. Full NAT, a less secure type of NAT, is generally used in special needs scenarios. It is not recommended to turn it on. In transparent Mode all data without NAT forwarding, directly to the network IP do not do camouflage transmission to the outer network, applicable to the network IP are public network address.

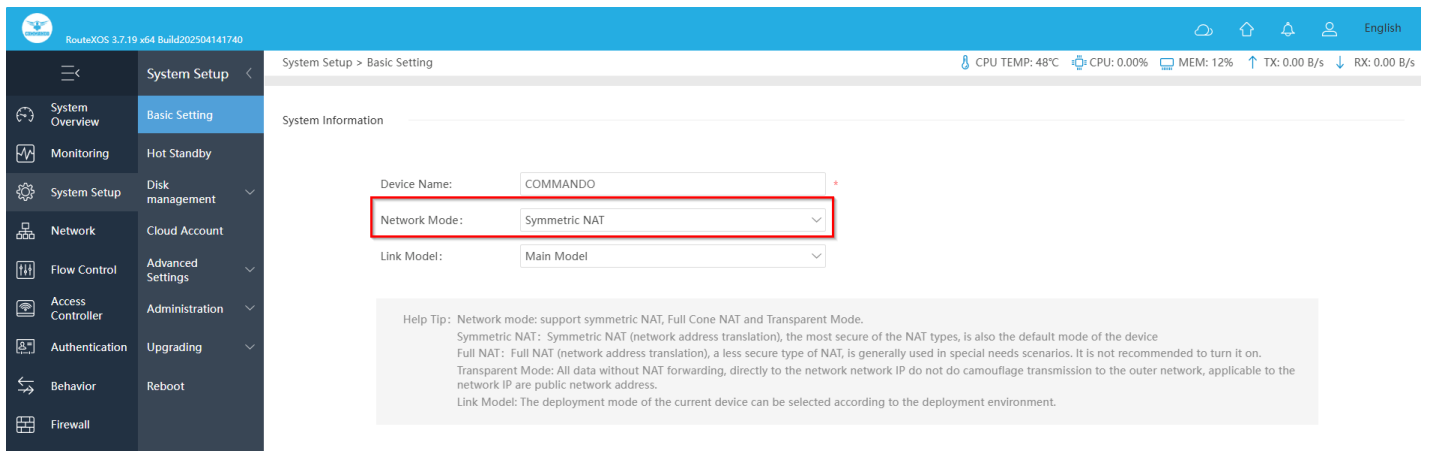


Fig 2.1.4 Default network mode Symmetric mode page

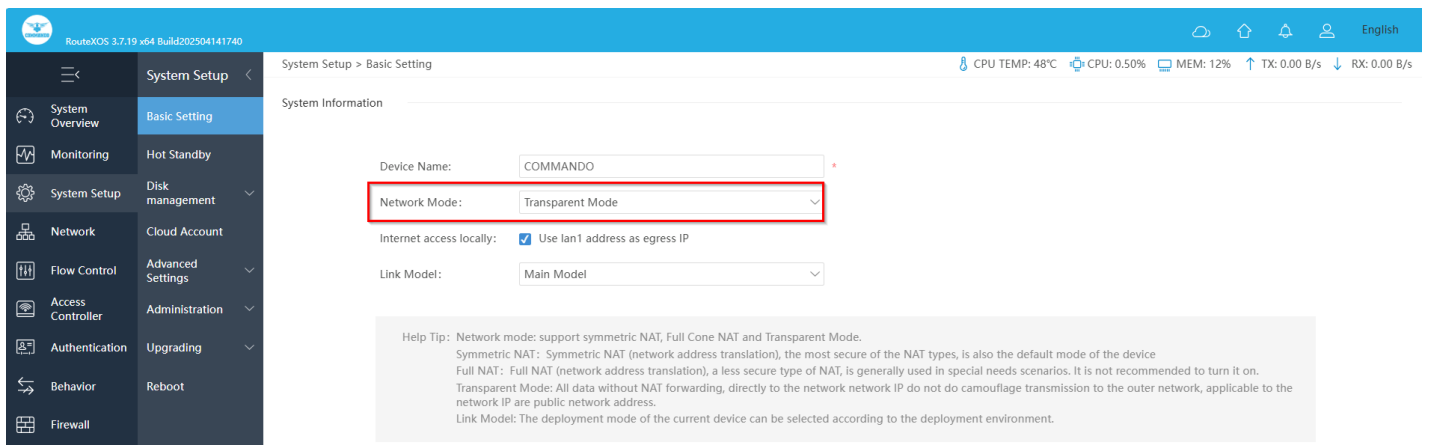


Fig 2.1.5 Changing network mode Symmetric mode to Transparent mode page

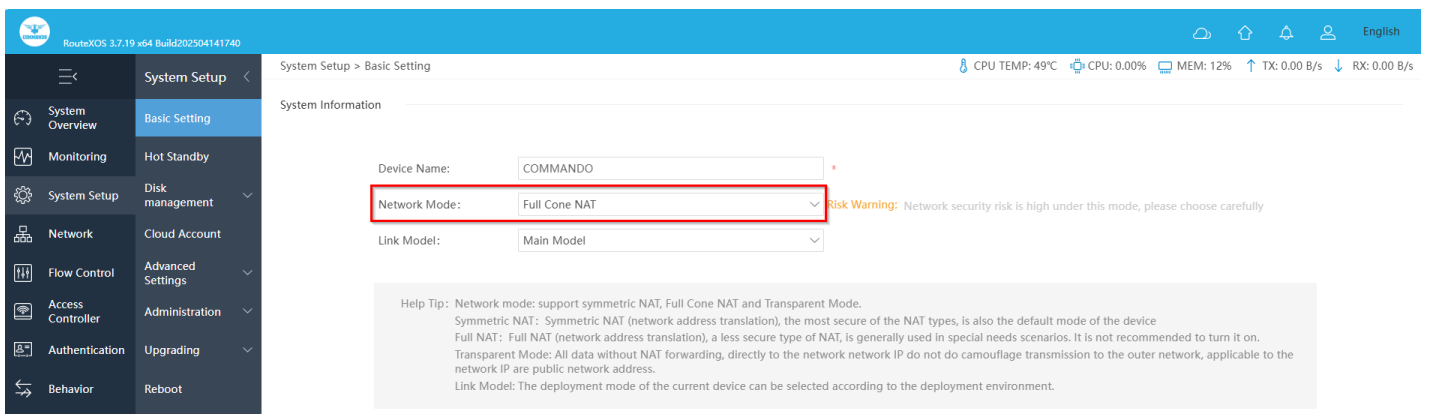


Fig 2.1.6 Changing network mode Symmetric mode to Full Clone NAT Page

Link Model: The deployment mode of the current device can be selected according to the deployment environment. The device supports Main Model, Side Model, and SD-WAN Bridge modes, each designed for different networking scenarios.

- Main Model serves as the primary link for network traffic, acting as the core connection point to the external network. It is typically used in standard deployments where the device handles all incoming and outgoing traffic.
- Side Model functions as a supplementary connection, often used for load balancing or backup purposes, ensuring network redundancy and stability.
- SD-WAN Bridge mode enables seamless integration into a software-defined WAN environment, allowing for optimized traffic routing, enhanced security, and improved network performance across multiple WAN links.

Selecting the appropriate link model ensures efficient network operation and aligns with the deployment requirements of the organization.

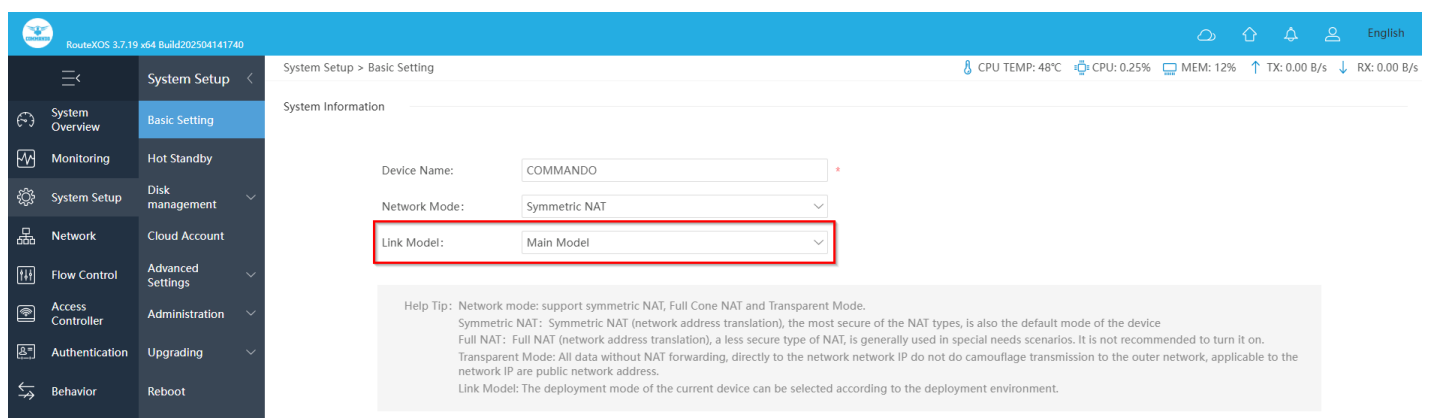


Fig 2.1.7 Default Link Model as Main Model page

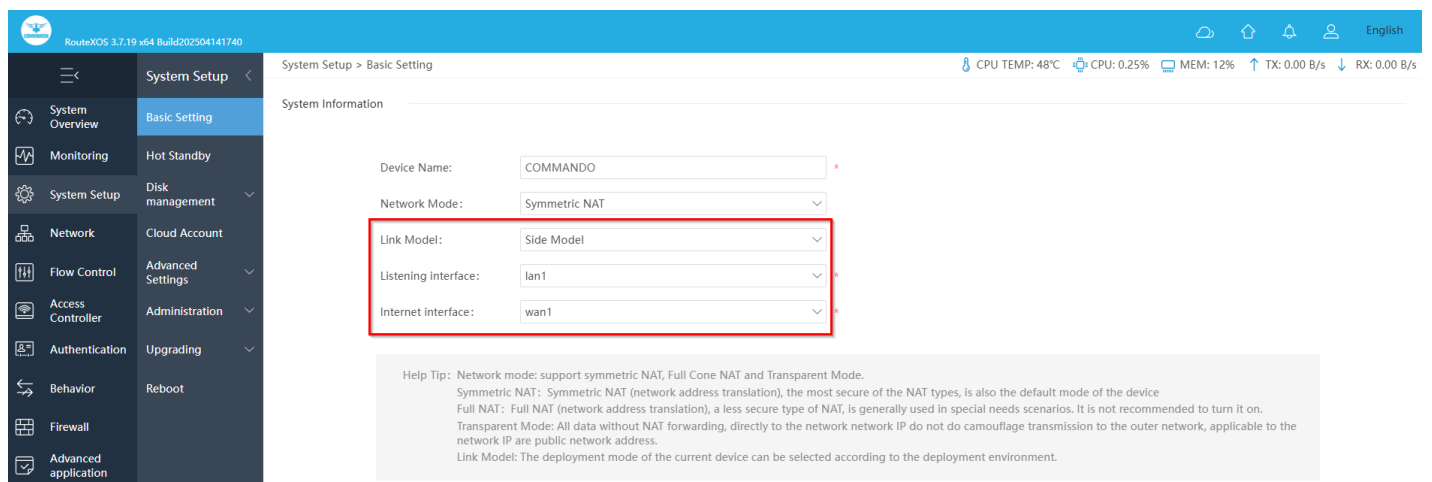


Fig 2.1.8 Changing Link Model as Side Model page

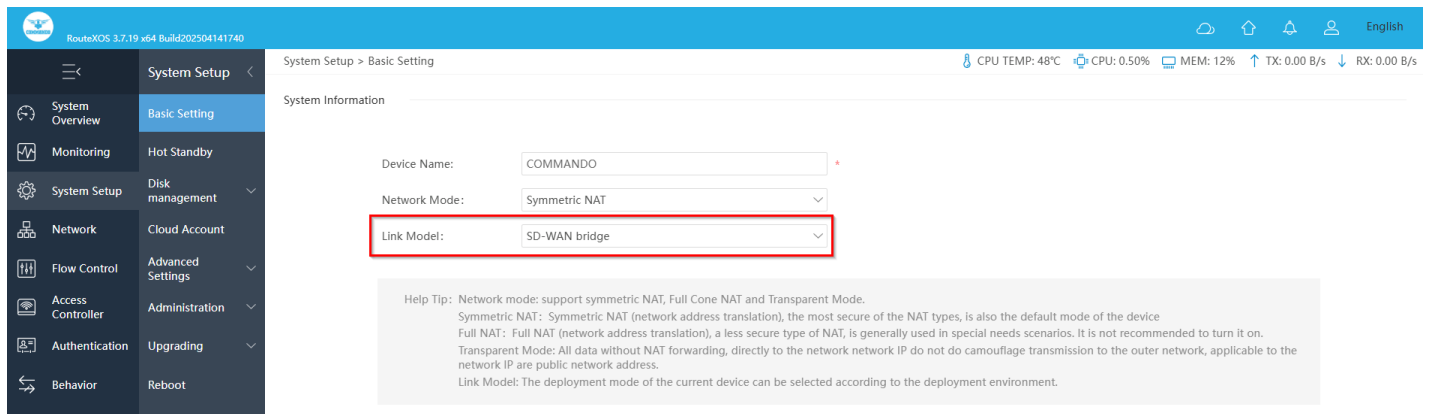


Fig 2.1.9 Changing Link Model as SD-WAN bridge page

Time setting: System Time is the time displayed while the Gateway is running. On this page you can configure the system time and the settings here will be used for other time-based functions like Access Rule, PPPoE and Logs.

In time setting you can set System Time, Time Zone, Set Time Automatically and with help of NTP service. System Time displays the current date and time of the Gateway. Time Zone displays the current time zone of the Gateway. You can configure the time zone and NTP Server. The Gateway will get GMT automatically if it has connected to a NTP Server. Manual time can also be set by feeding date and time manually.

Synchronize with PC'S Clock is best and recommended option for the administrator PC's clock is utilized for setting time.

To configure Time Settings, click on System Setup > Basic Setting go to Time Settings.

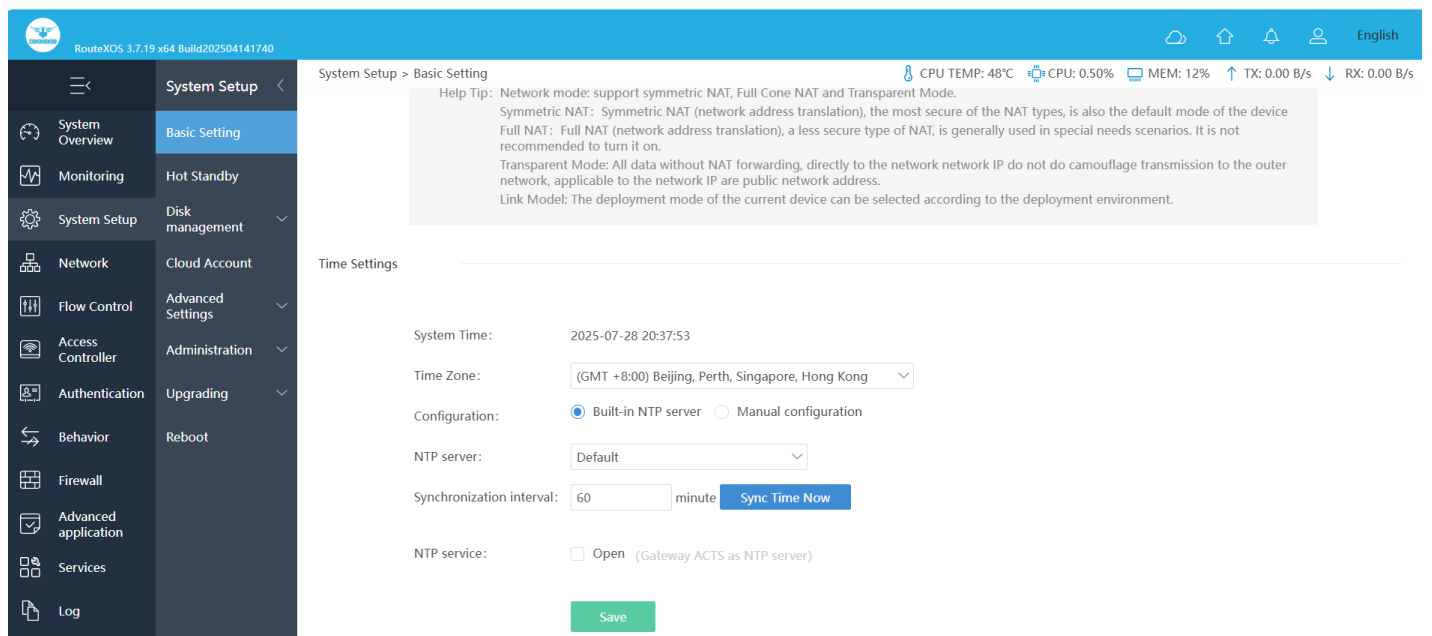


Fig 2.1.10 Time Settings with Sync time now option page

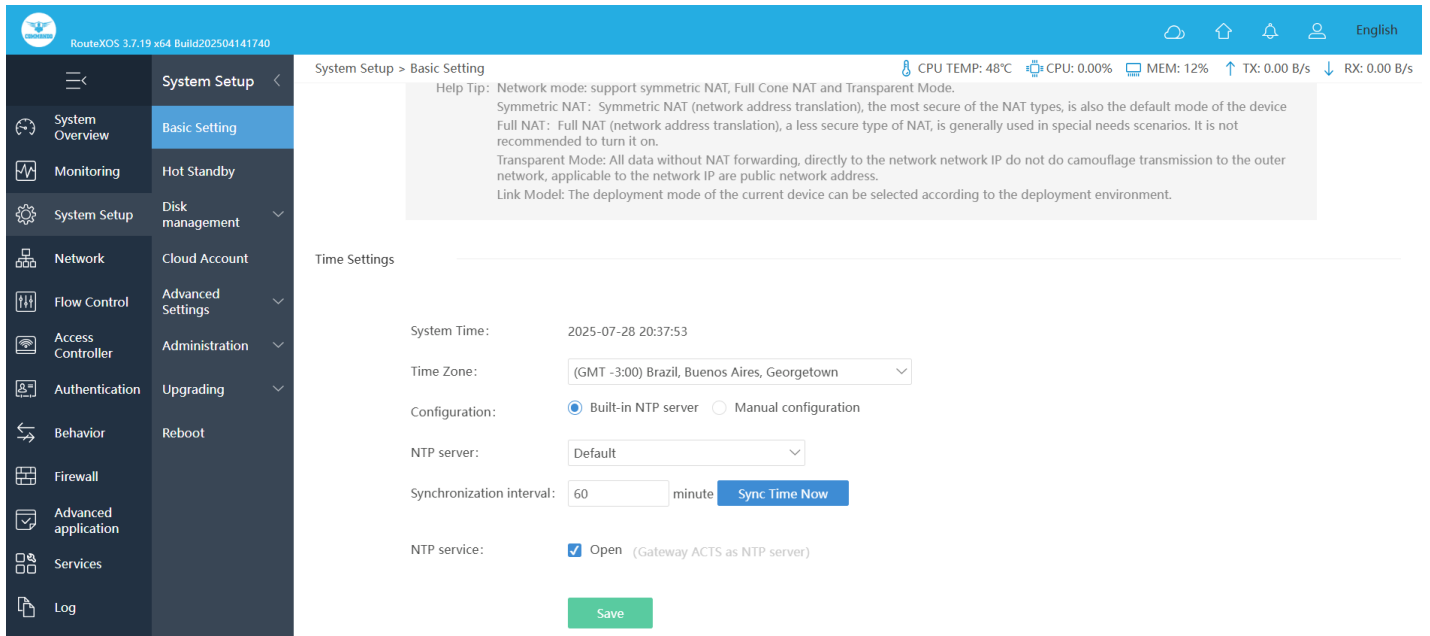


Fig 2.1.11 Time Settings with NTP service and changing Time zone page

2. Disk management

Gateway can operate as a file server for storage devices that are connected via USB or Hard disk. Your home network's LAN devices can share the storage device as a mapped network drive. The web-based management provides disk management utilities such as fdisk for partitioning the drive as a physical disk or logical disk, as well as format utilities for formatting the partitions.

The Gateway supports up to 8 zoning quantity. To access to this page click on System Setup > Disk management > Disk partition

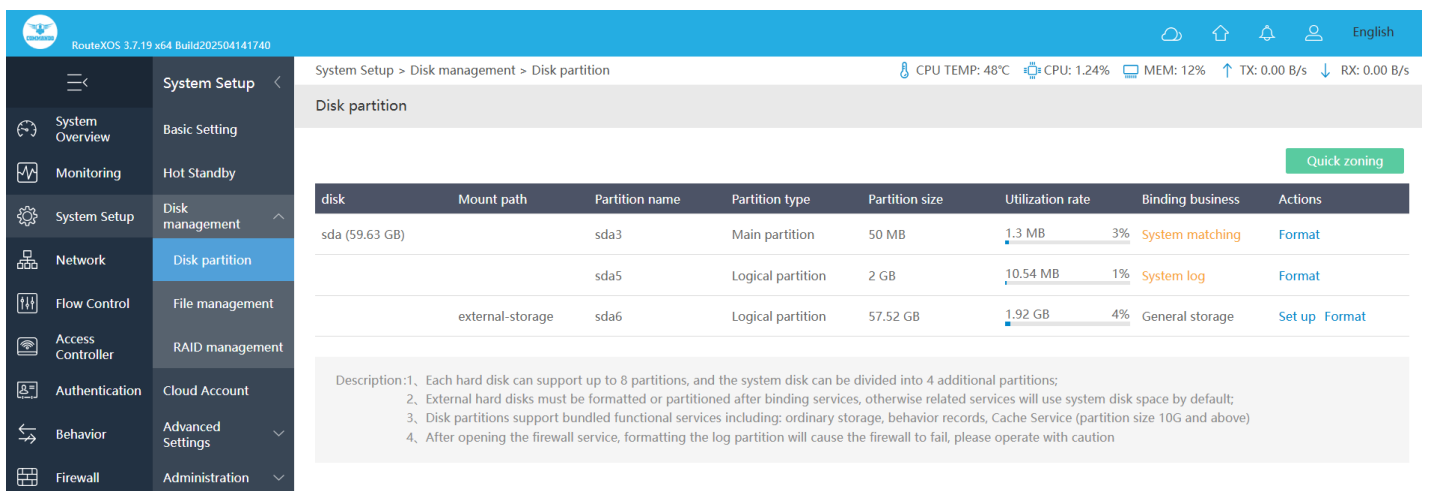


Fig 2.2.1 Disk partition page

The screenshot shows the 'Disk partition' page in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar contains navigation options: System Overview, Monitoring, System Setup (selected), Network, Flow Control, Access Controller, and Authentication. Under 'System Setup', the sub-menu 'Disk partition' is highlighted. The main content area shows the 'Quick zoning' section with the following settings: 'Select disk:' set to 'sda(59.63 GB)', 'Zoning quantity:' set to '1', and 'Disk partition size:' set to '59 GB (System log partition)'. There are 'Save' and 'Cancel' buttons at the bottom.

Fig 2.2.2 Disk partition quick zoning page

This screenshot shows the 'Disk partition quick zoning' page. The settings are: 'Select disk:' set to 'sda(59.63 GB)', 'Zoning quantity:' set to '2', and 'Disk partition size:' set to '1 GB (System log partition)'. A dropdown menu for 'Disk partition size' is open, showing options 1, 2, 3, and 4. 'Save' and 'Cancel' buttons are at the bottom.

Fig 2.2.3 Disk partition quick zoning quantity page

The Gateway supports file management. To access this page, click on System Setup > Disk management > File management

The screenshot shows the 'File management' page in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar shows 'File management' selected under 'System Setup'. The main content area displays a table of files. The table has columns: File name, Size, Type, and Modification time. There is a filter 'All disk' and a table with one row of data.

File name	Size	Type	Modification time
external-storage	56.32 GB	Disk	2025-07-28 12:18:40

Fig 2.2.4 Default file Management page

The Gateway supports RAID management for redundancy. To access this page, click on System Setup > Disk management > Raid Management

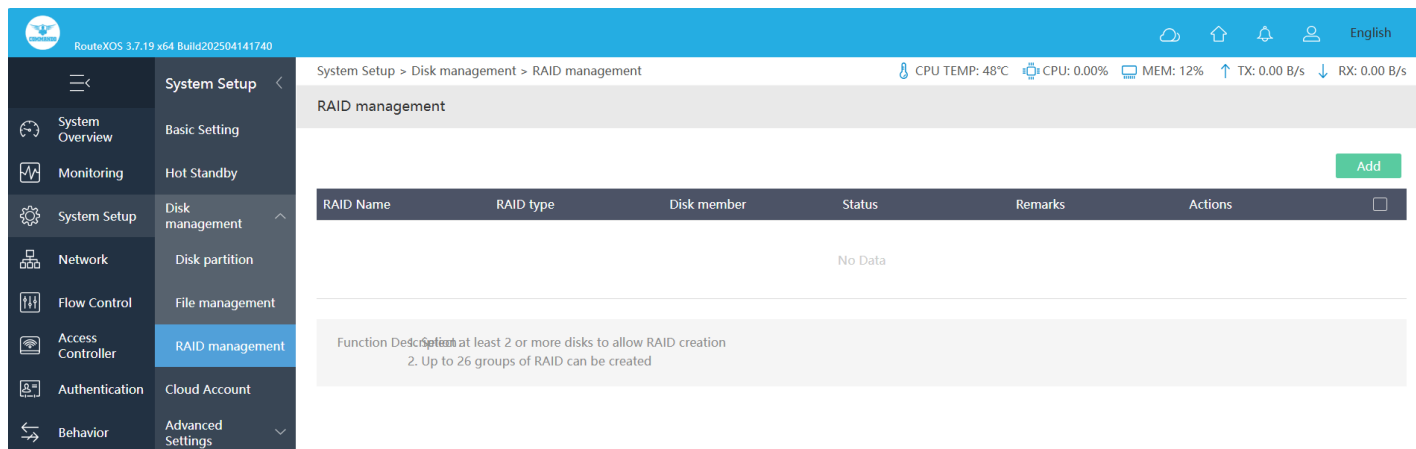


Fig 2.2.5 Default RAID Management page

3. Cloud Account

What is cloud service?

Cloud service focuses on managing the Gateway. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal. From captive portal you can access the device from anywhere in the world.

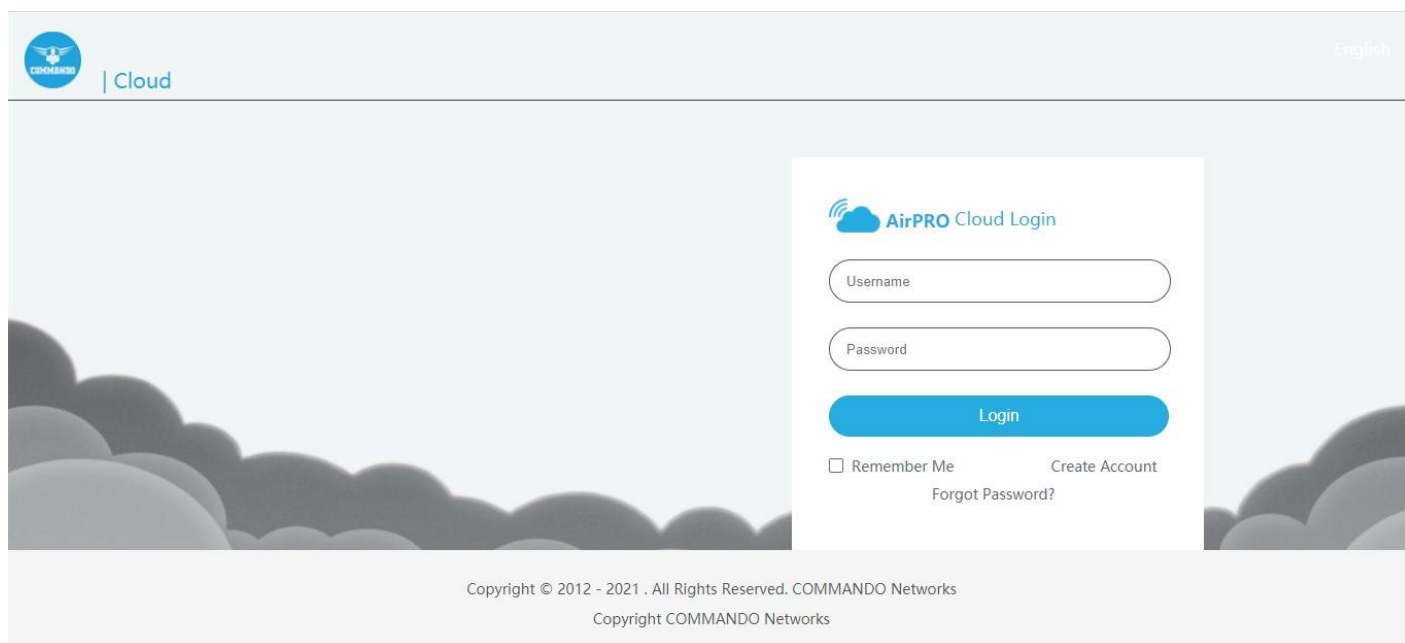


Fig 2.3.1 Cloud Login page

How to connect to cloud service?

Go to browser and type <http://commandonetworks.com.cn/#/login>

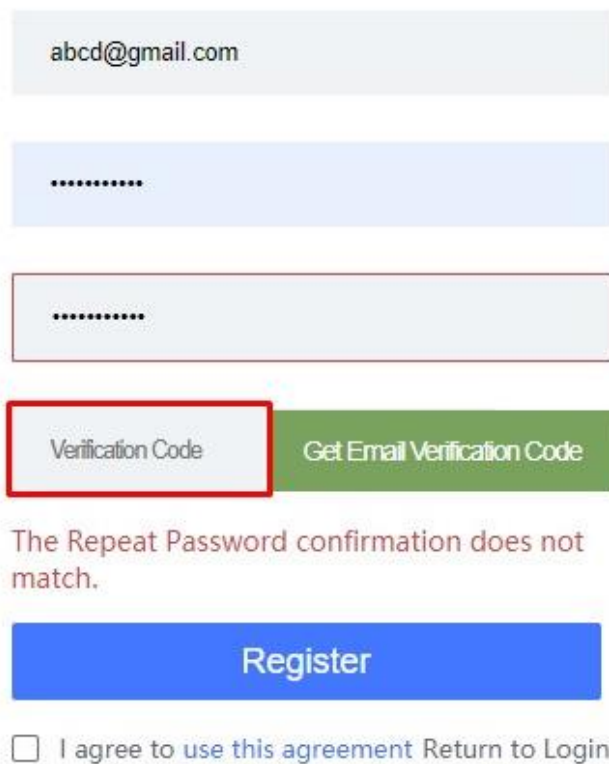
Click on the create account for first time access



The image shows the 'AirPRO Cloud Login' interface. At the top is the logo, which consists of a blue cloud with three white signal waves to its left, followed by the text 'AirPRO Cloud Login' in a blue sans-serif font. Below the logo are two rounded rectangular input fields: the first is labeled 'Username' and the second is labeled 'Password'. Under these fields is a solid blue button with the word 'Login' in white. Below the 'Login' button is a checkbox labeled 'Remember Me' and a link labeled 'Forgot Password?'. To the right of the 'Remember Me' checkbox is a red rectangular button with the text 'Create Account' in black.

Fig 2.3.2 Create Cloud Login account page

Register



The image shows the 'Register' form. At the top is the heading 'Register' in a grey font. Below it is a horizontal line. The form contains several input fields: a light grey field with the email 'abcd@gmail.com', a light blue field with seven dots, and a light grey field with seven dots. Below these is a red rectangular button labeled 'Verification Code' and a green rectangular button labeled 'Get Email Verification Code'. Below the buttons is a red error message: 'The Repeat Password confirmation does not match.' At the bottom is a solid blue button labeled 'Register'. Below the 'Register' button is a checkbox labeled 'I agree to use this agreement' followed by a link 'Return to Login'.

Fig 2.3.3 Register Cloud Login account page

Provide Email ID, password as per your choice and get the verification code either in inbox or spam folder of Email which you submitted.

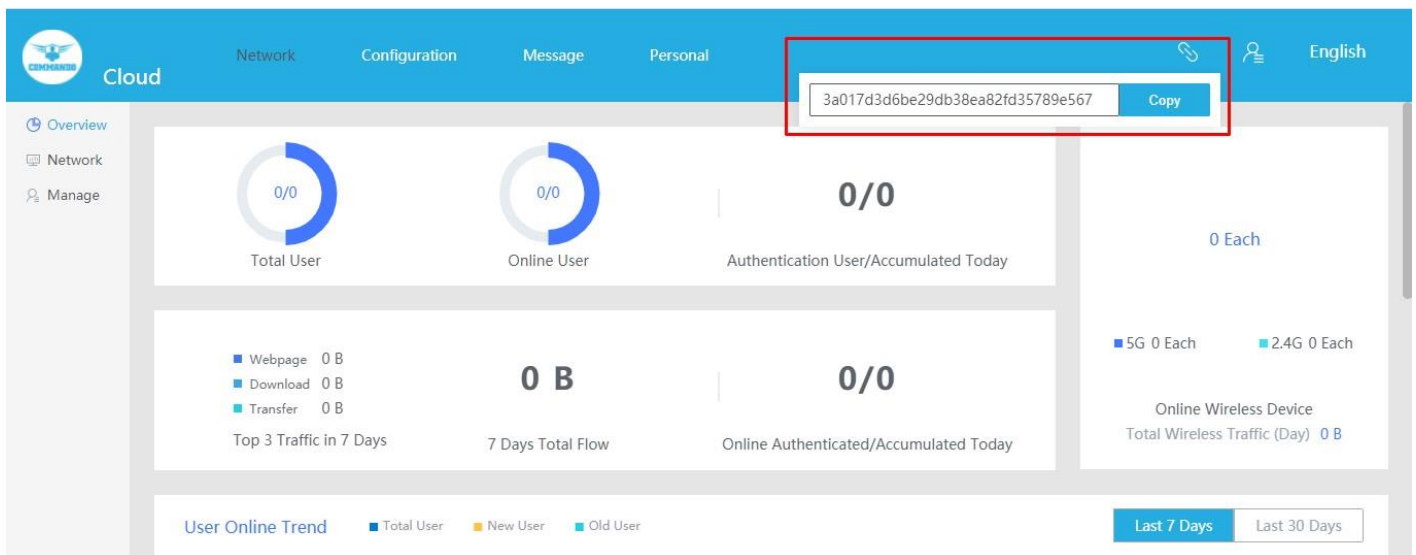


Fig 2.3.4 Binding code for Cloud Login account page

Get the binding code from cloud and then go to System Setup > Cloud Account and put this code in Account code

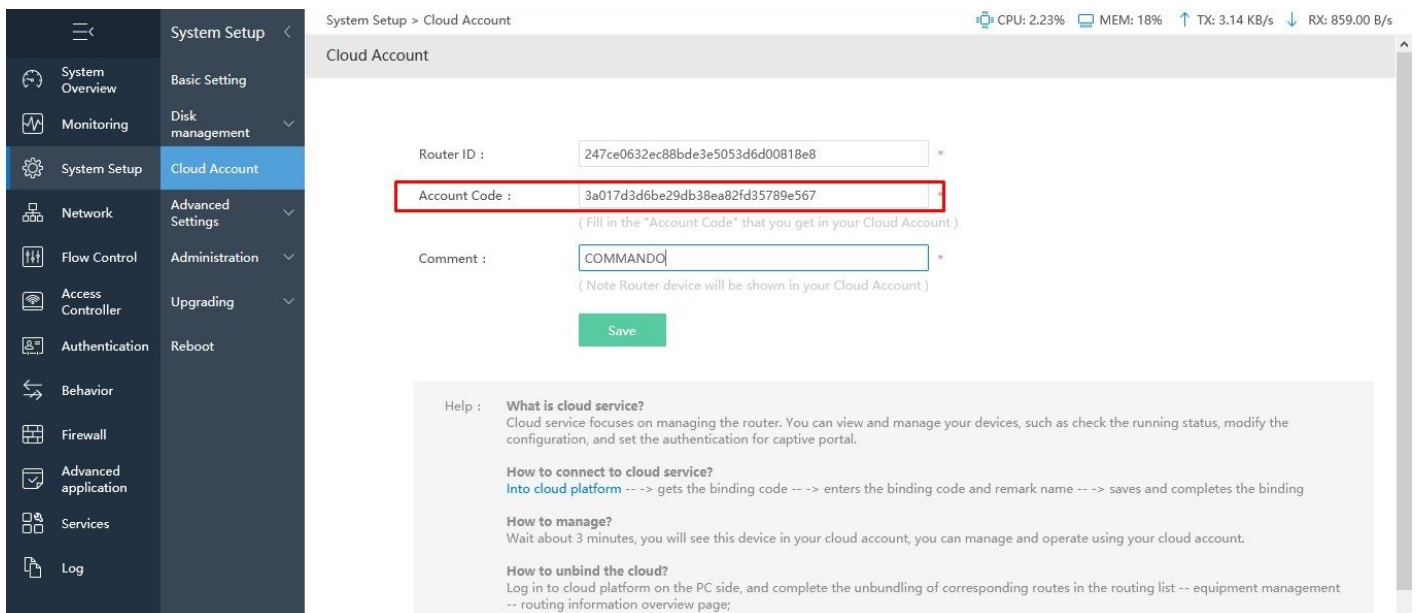


Fig 2.3.5 Binding code MSG-1200 Gateway with cloud portal page

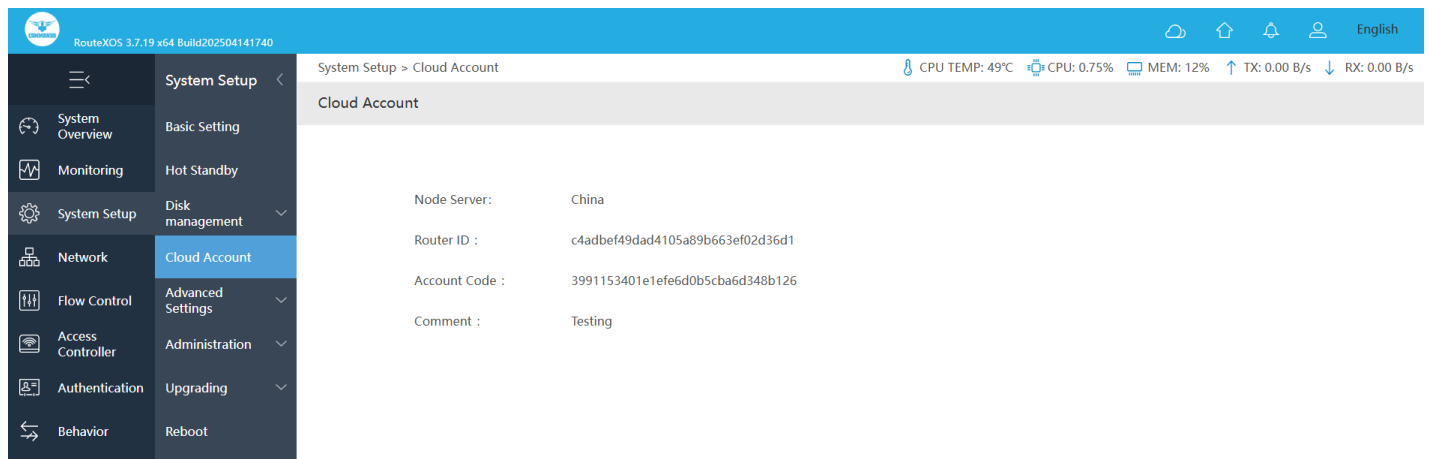


Fig 2.3.6 After Binding MSG-1200 Gateway with cloud page

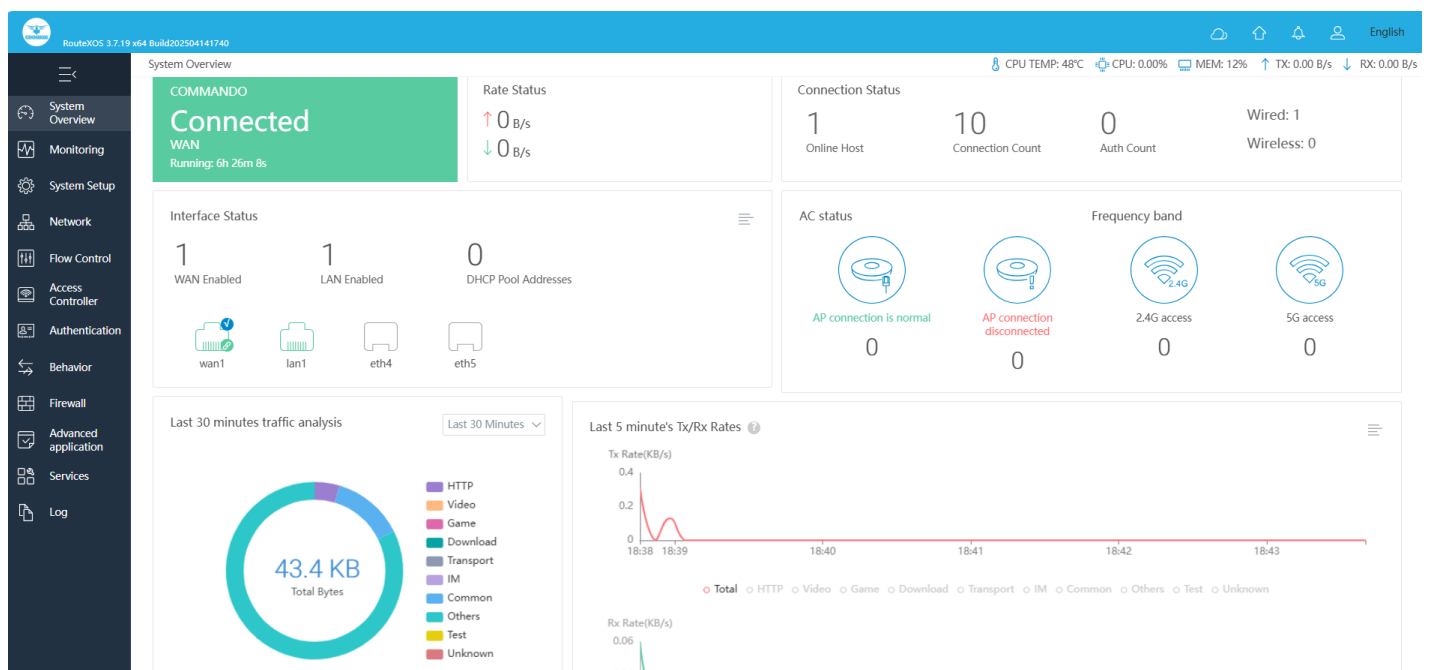


Fig 2.3.7 Normal MSG-1200 Gateway system overview page

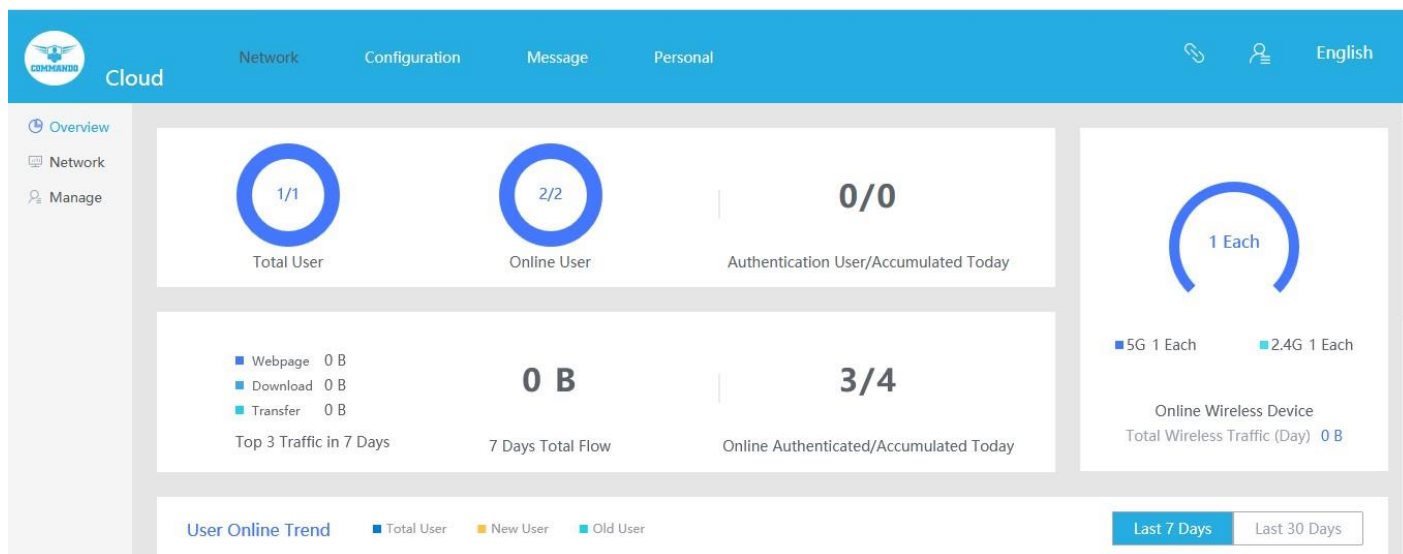


Fig 2.3.8 Cloud access of MSG-1200 Gateway with cloud page

The screenshot displays the 'AP List' page within the 'Cloud' interface. The top navigation bar and left sidebar are consistent with the previous figure. The main content area shows a table of Access Points (APs) with the following columns: Status, Remarks, Address, Version, Model, and Operation. The table contains two entries, both marked as 'Online'.

Status	Remarks	Address: [0]	Version	Model	Operation
Online		08:9b:4b:9e:f4:e3	1.5.7	AP	View
Online		08:9b:4b:99:a3:94	1.5.5	AP	View

Below the table, there is a pagination control showing 'Total 2', '10/page', and 'Go to 1'.

Fig 2.3.9 Cloud access of MSG-1200 Gateway with AP page

How to manage?

Wait about 3 minutes, you will see this device in your cloud account which is online t, you can manage and operate using your cloud account.

How to unbind the cloud?

Log in to cloud platform on the PC side and complete the unbinding of corresponding routes in the routing list -- equipment management -- routing information overview page.

4. Advanced Settings

- **ALG Set**

ALG or Application Layer Gateway is a software component that manages specific application protocols such as SIP (Session Initiation Protocol) and FTP (File Transfer Protocol). An ALG acts as an intermediary between the Internet and an application server that can understand the application protocol. Some special protocols such as FTP, H.323, SIP, IPsec and PPTP will work properly only when ALG (Application Layer Gateway) service is enabled.

To get access to ALG set click on System Setup > Advanced Settings > ALG Set

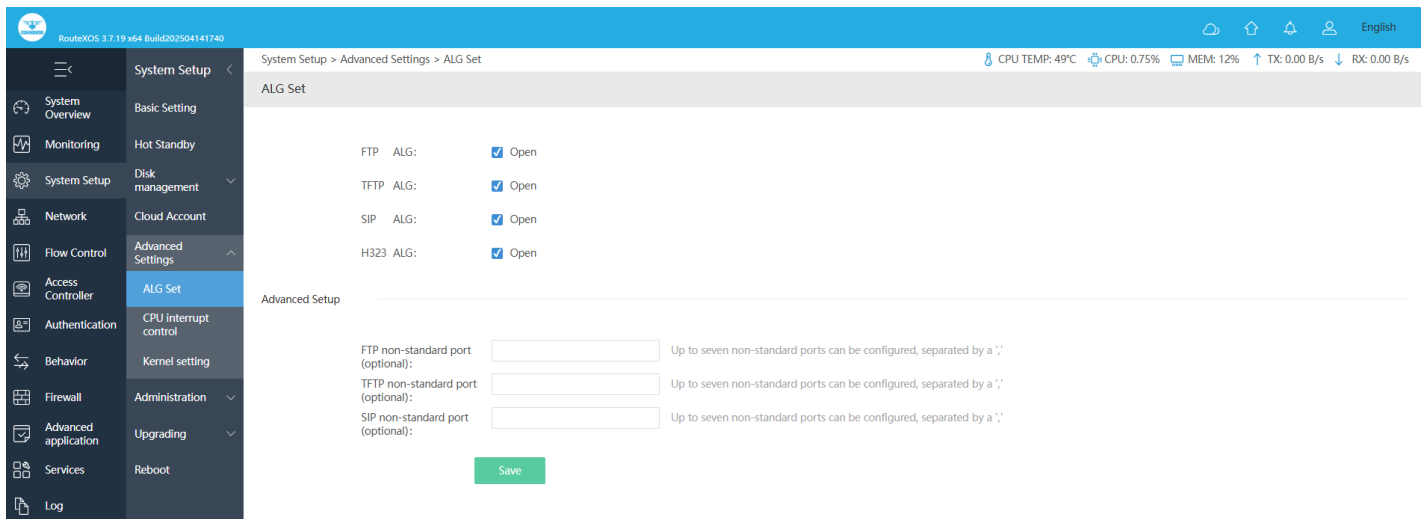


Fig 2.4.1 ALG set page

- **CPU interrupt control**

CPU interrupt control manages the handling of hardware and software interrupts to ensure efficient task prioritization and system responsiveness. It allows the processor to temporarily halt its current task to address high-priority events, such as input/output operations or critical system requests. By efficiently managing interrupt requests, the system minimizes processing delays and optimizes overall performance, preventing bottlenecks and ensuring smooth operation of network and computing devices.

To get access to ALG set click on System Setup > Advanced Settings > CPU interrupt control

RoutexOS 3.7.19 x64 Build202504141740

System Setup

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

System Setup

Basic Setting

Hot Standby

Disk management

Cloud Account

Advanced Settings

ALG Set

CPU interrupt control

Kernel setting

Administration

Upgrading

Reboot

System Setup > Advanced Settings > CPU interrupt control

CPU TEMP: 49°C

CPU: 1.50%

MEM: 12%

Tx: 0.00 B/s

Rx: 0.00 B/s

English

System Setup > Advanced Settings > CPU interrupt control

CPU interrupt control

CPU Remax: OFF

CPU freq mode: Performance

CPU Interrupt Set

CPU ID	CPU current frequency	CPU USE	CPU Physical ID	CPU Core ID	NIC Soft Interrupt	NIC Hard Interrupt	Actions
cpu0	703 MHz	0.00%	0	0	Open	Open	Close Soft Close Hard
cpu1	703 MHz	0.99%	0	1	Open	Open	Close Soft Close Hard
cpu2	711 MHz	0.00%	0	2	Open	Open	Close Soft Close Hard
cpu3	740 MHz	0.00%	0	3	Open	Open	Close Soft Close Hard

NIC Hard Interrupt Set

NIC Queue	Current Assignment CPU	Assign CPU Manually	Actions
eth0	cpu0	auto	Edit View Status
eth0-TxRx-0	cpu1	auto	Edit View Status
eth0-TxRx-1	cpu2	auto	Edit View Status
eth0-TxRx-2	cpu3	auto	Edit View Status
eth0-TxRx-3	cpu0	auto	Edit View Status
eth1	cpu1	auto	Edit View Status
eth1-TxRx-0	cpu2	auto	Edit View Status

Fig 2.4.2 CPU interrupt control page

- Kernel Settings

Kernel settings manage the core configurations of the operating system, controlling how it interacts with hardware and software components. These settings define system behavior, including memory management, process scheduling, network parameters, and security policies. By optimizing kernel configurations, performance, stability, and security can be enhanced, ensuring efficient resource allocation and seamless operation of network and computing devices.

To get access to ALG set click on System Setup > Advanced Settings > Kernel settings

© 2025 COMMANDO Networks Inc. All rights reserved.

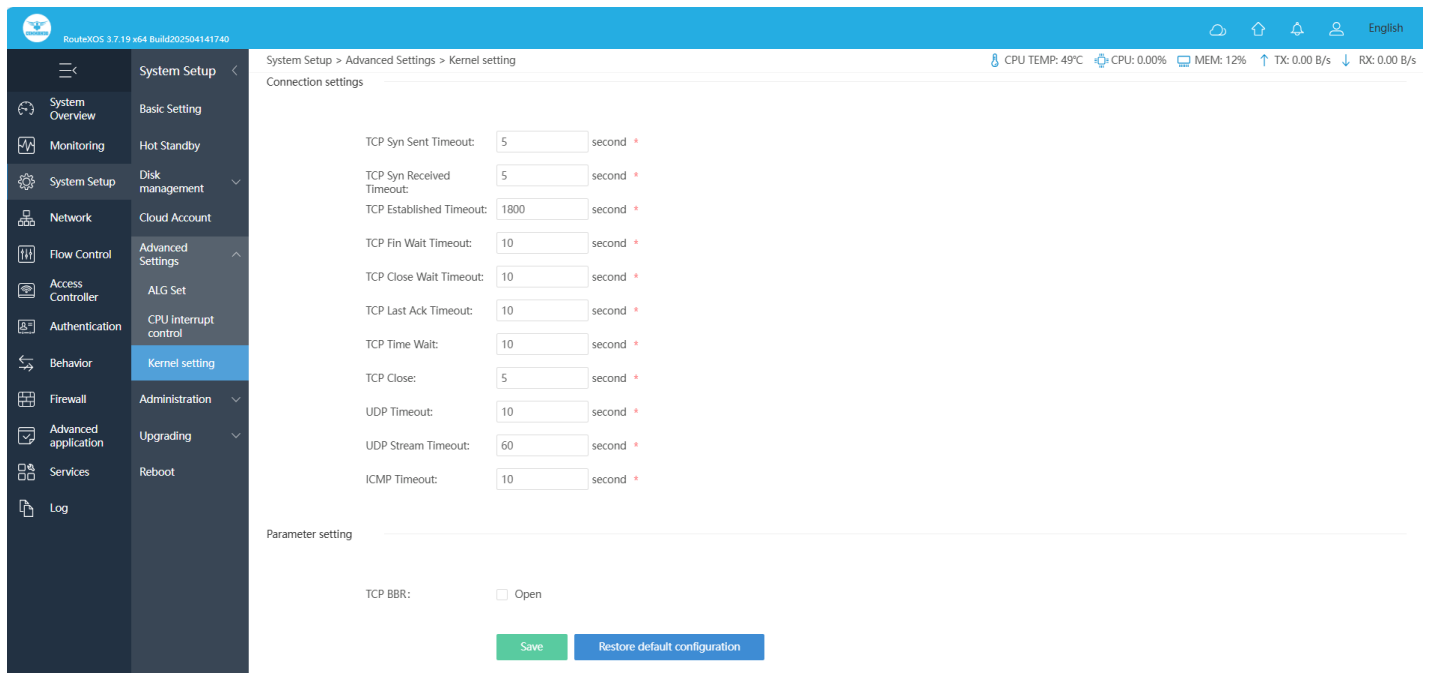


Fig 2.4.3 Kernel Setting page

5. Administration

On this page, you can modify the factory default username and password of the Gateway and create multiple new users and passwords with specific access profiles and rights to manage the device. You can also allow telnet or remote WEB access of device.

Note: The factory default username is admin and password is mentioned in backside of device.

You can modify default username and passwords and can create multiple logins. The Password length minimum 6 and maximum 64 characters, and can contain letters, numbers, special symbols as per user. All the fields are case-sensitive.

To access User Account, click on System Setup > Administration > User Accounts

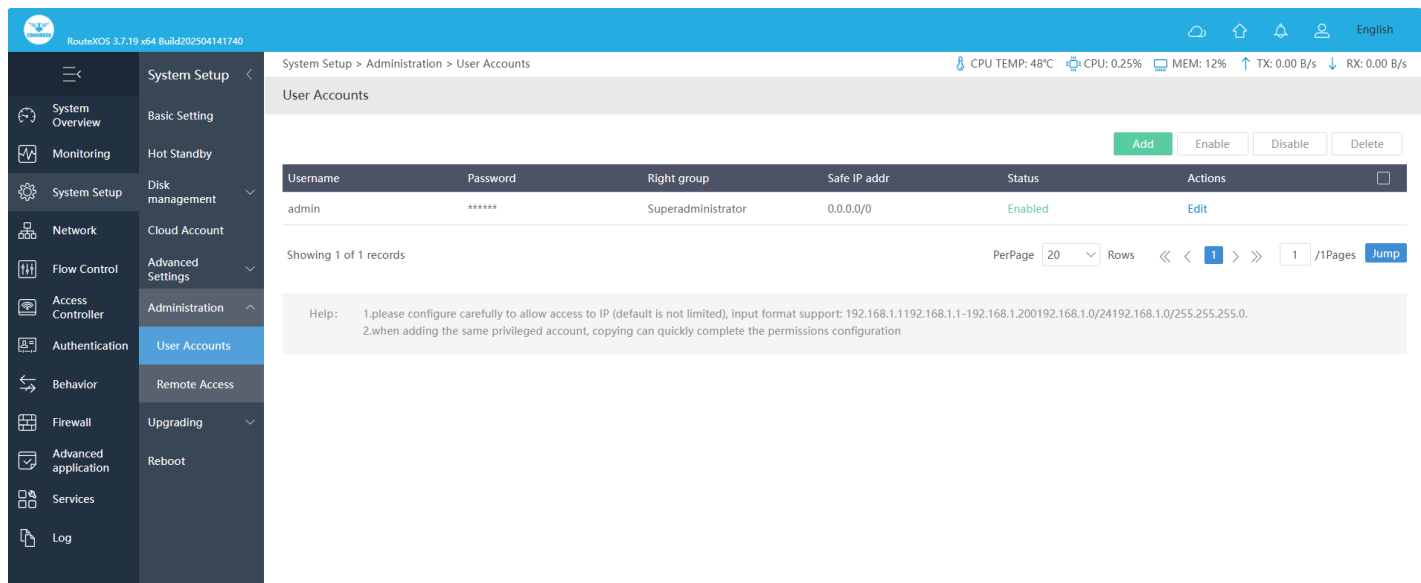


Fig 2.5.1 Default User Accounts page

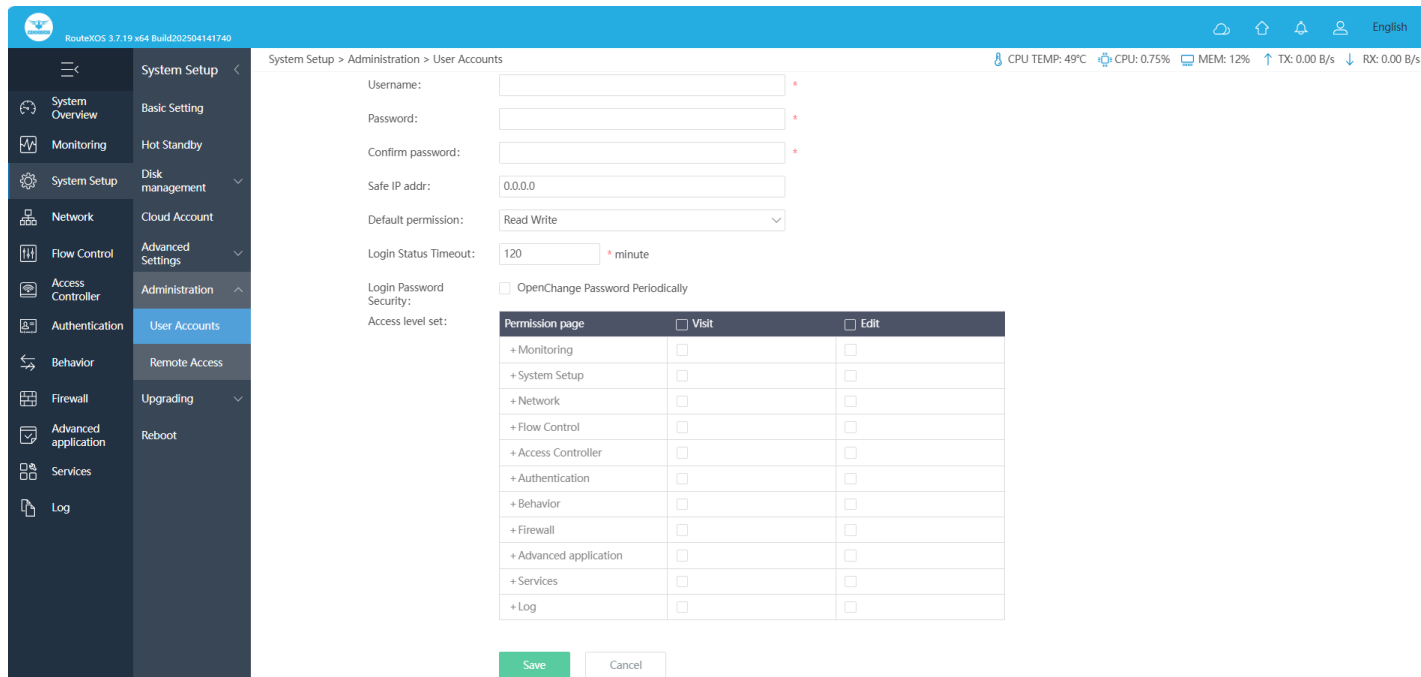


Fig 2.5.2 Add User Accounts page

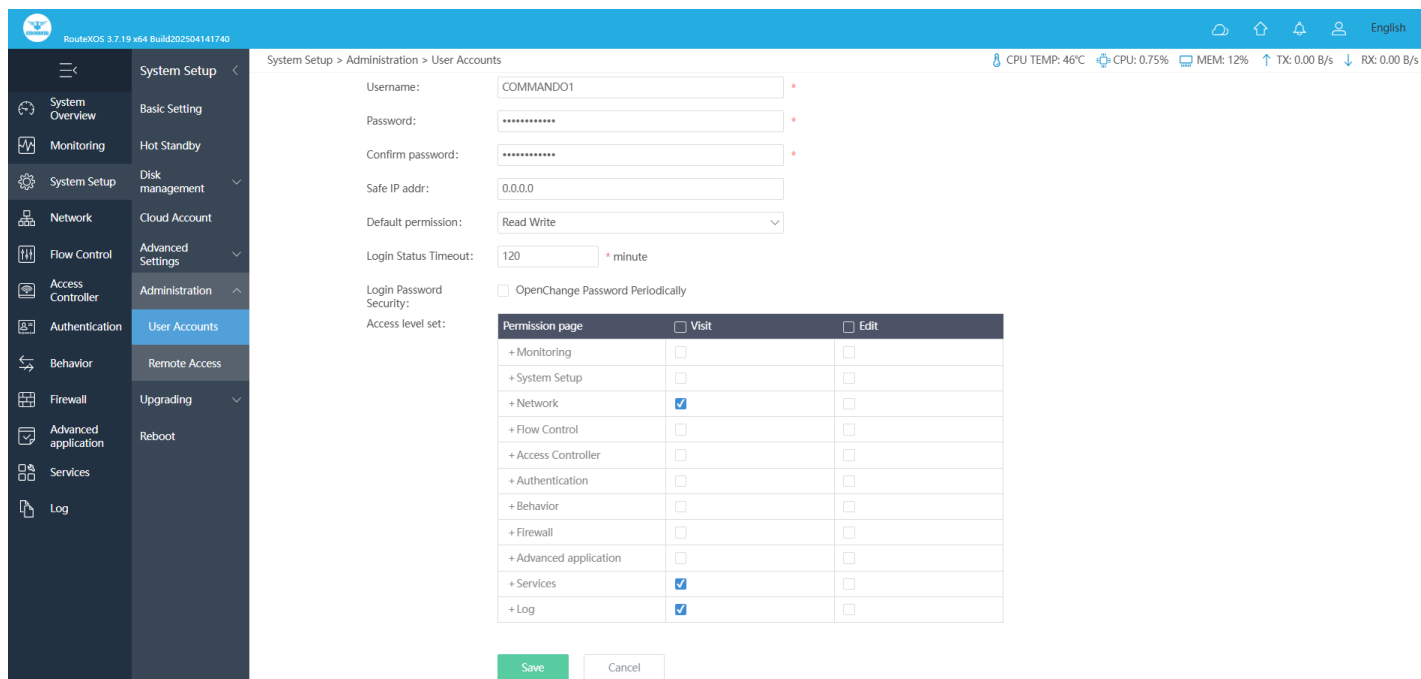


Fig 2.5.3 Add User Account with visit permission page

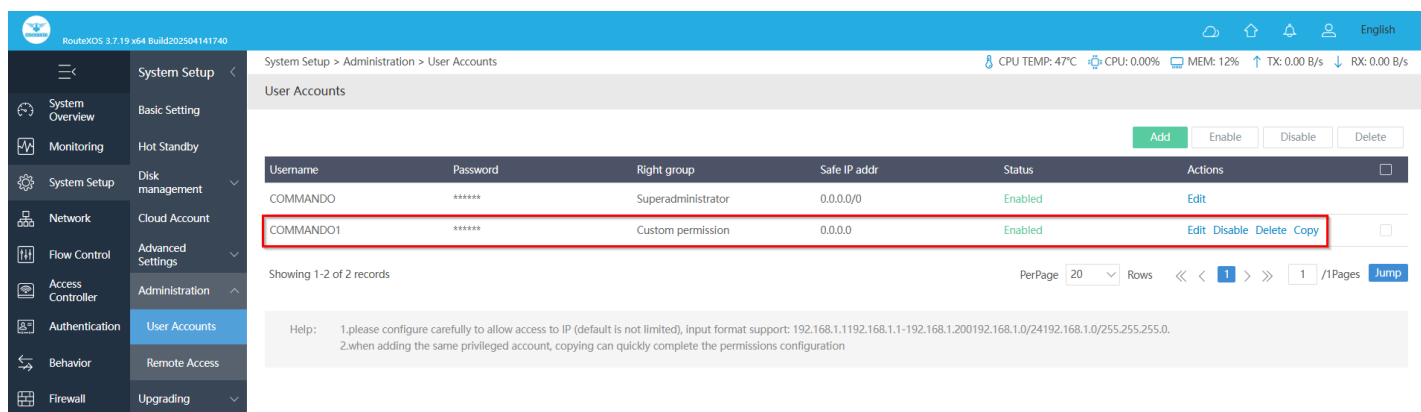


Fig 2.5.4 User Account COMMAND01 with visit permission page

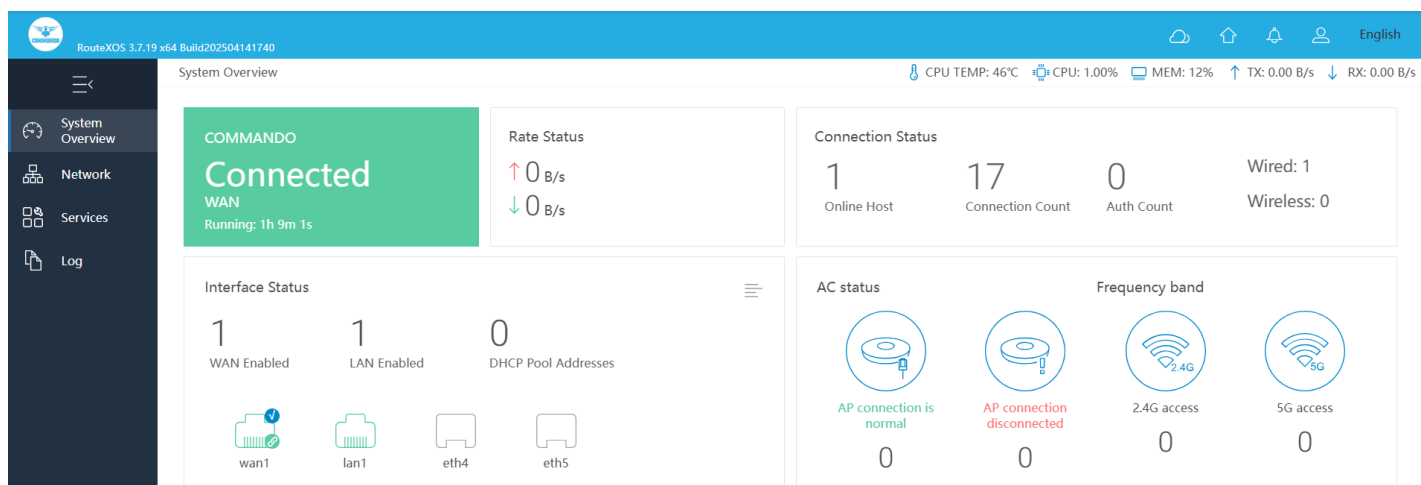


Fig 2.5.6 Customized access as per User Account COMMANDO1 with visit permission page

By default, remote access is disabled. To change, modify or allow, click on System Setup > Administration > User Accounts

Telnet (Telecommunication Network protocol): Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system.

Web Interface: Allow access to web interface from public network

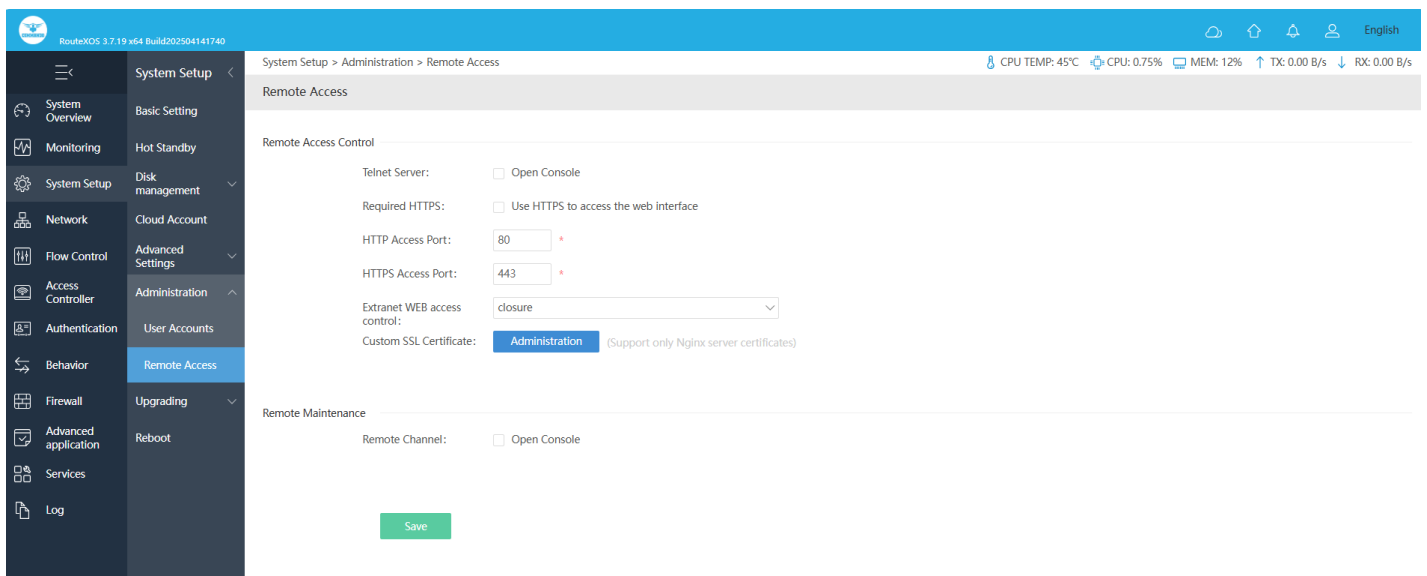


Fig 2.5.7 Remote Access control page

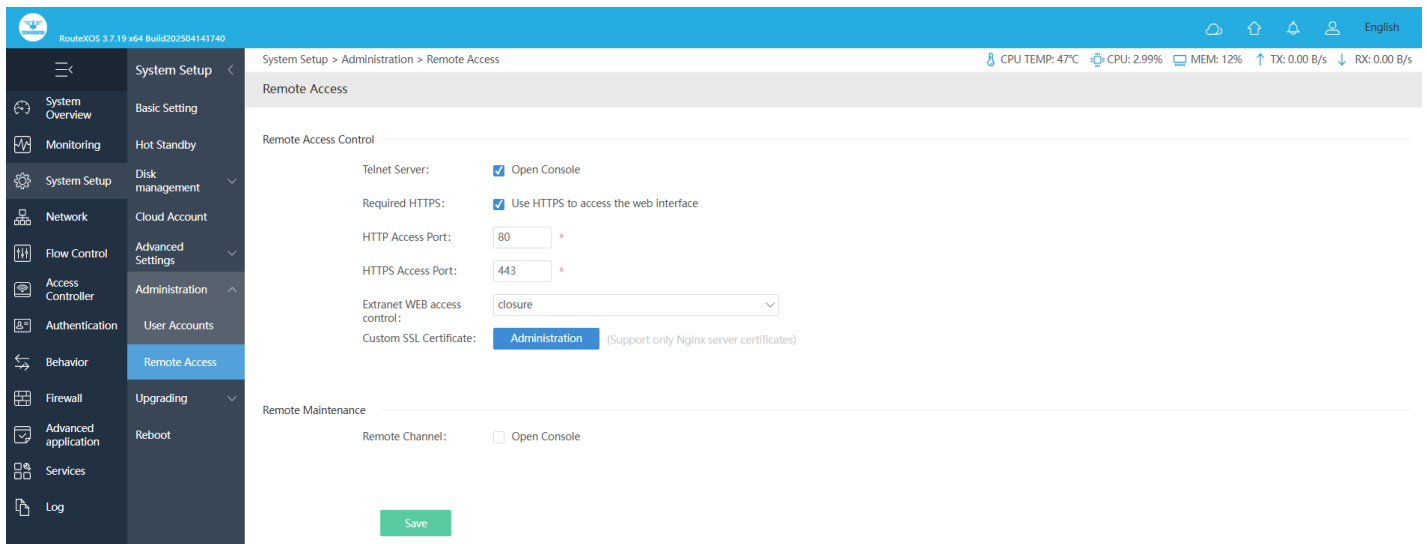


Fig 2.5.8 Enabling Remote Access control page

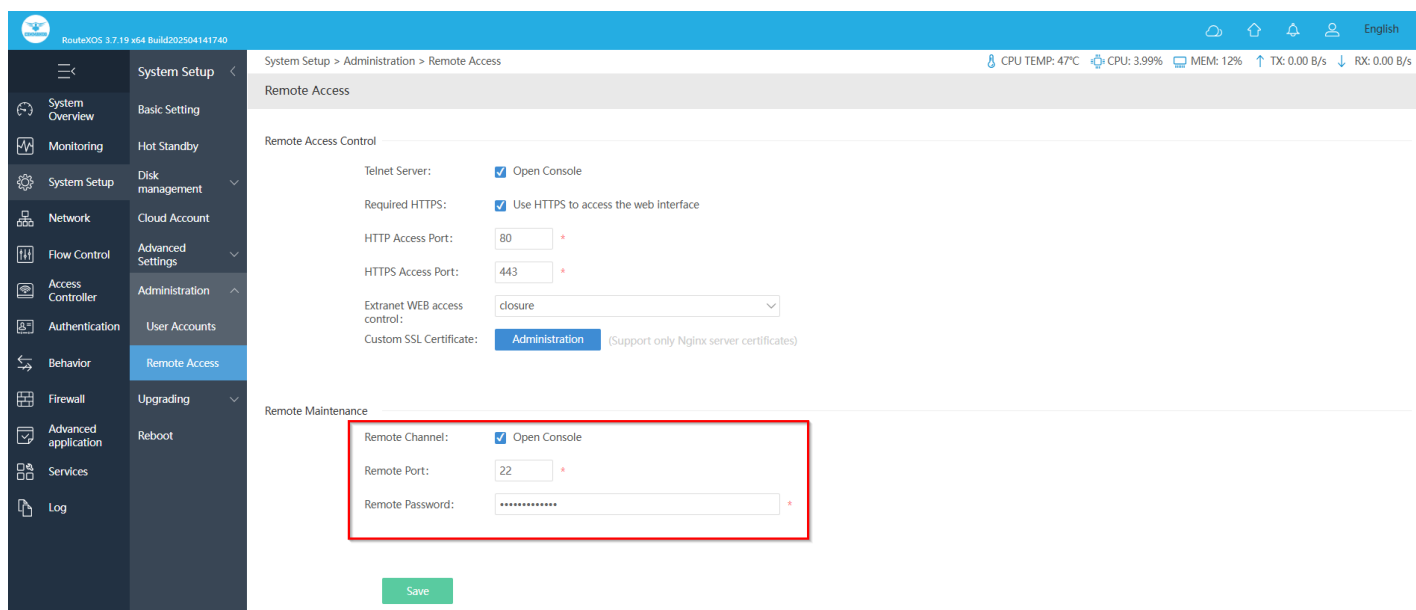


Fig 2.5.9 Setting password for Remote Access page

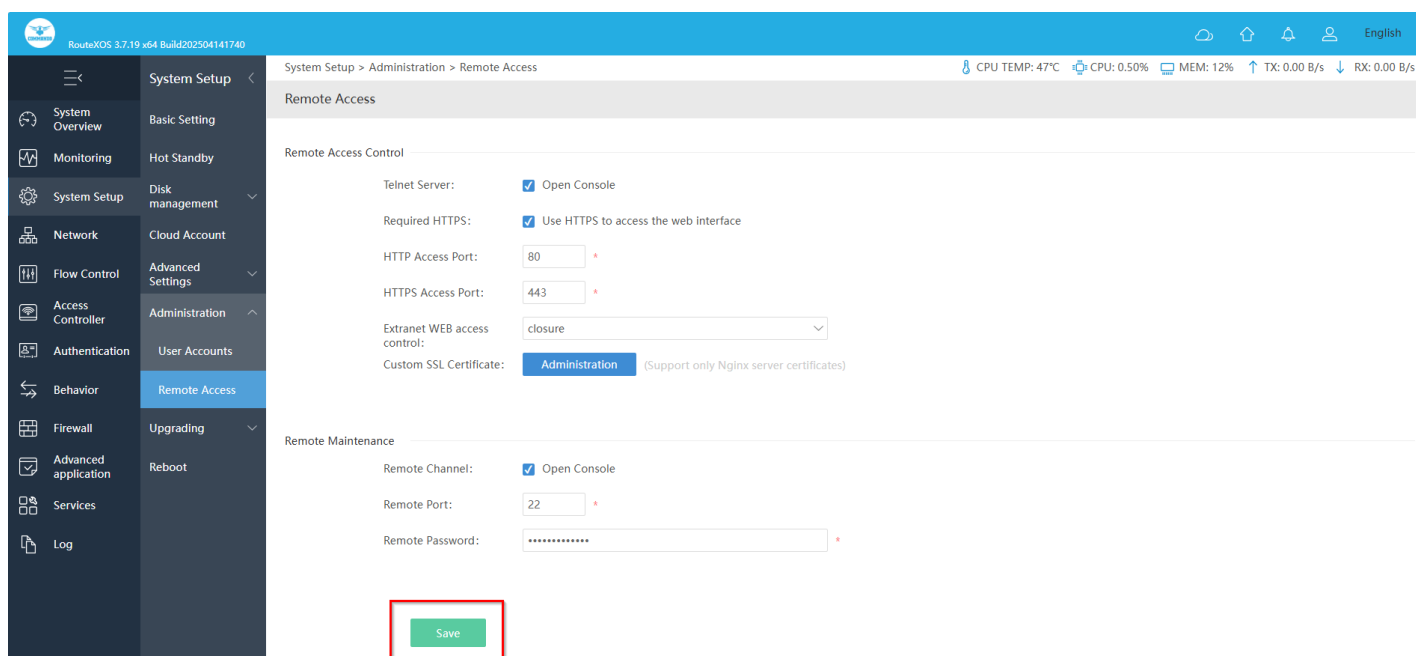


Fig 2.5.10 Enabling Remote Access with save button page

Administration (Custom SSL Certificate): SSL certificates are what enable websites to move from HTTP to HTTPS, which is more secure. An SSL certificate is a data file hosted in a website's origin server. SSL Certificates are small data files that digitally bind a cryptography key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. It can be Local authentication and Remote authentication.

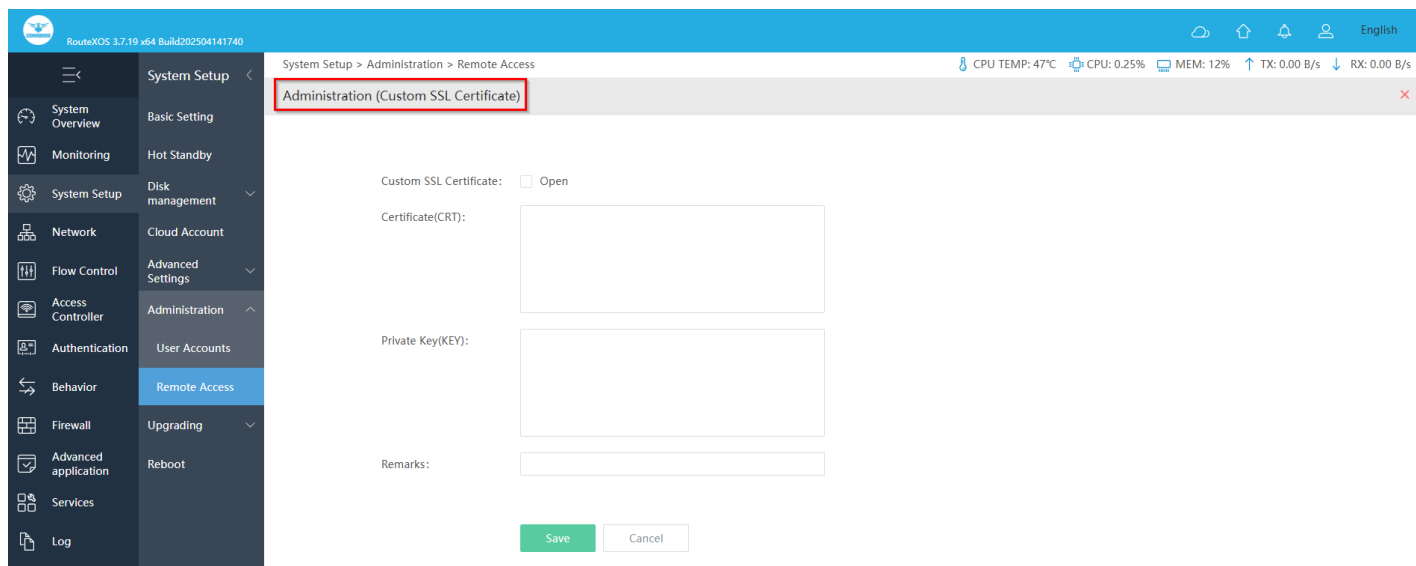


Fig 2.5.11 Administration (Custom SSL Certificate) page

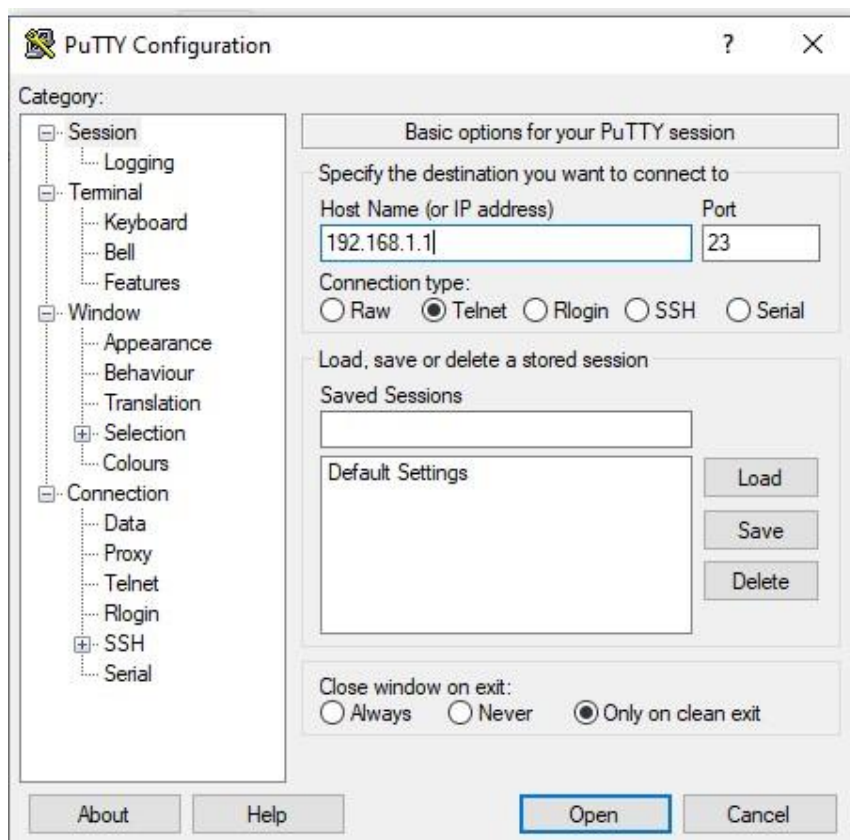


Fig 2.5.12 Putty for Telnet access of device page

```
192.168.1.1 - PuTTY
username: admin
passwd:
  console for English
  CMD-COS-v1.01
  Version:

-----
0. System status | WEB Address -> http://192.168.1.1:80
0
1. Set ether band | lan1 (veth1 08:9b:4b:50:1c:bc)
bc) LinkUp
2. Set lan/wan address | lan1 (veth2 08:24:7c:e0:63:30)
30) LinkDown
3. Set WEB port | lan1 (veth3 08:24:7c:e0:63:31)
31) LinkDown
4. Ping Test | lan1 (veth4 08:24:7c:e0:63:32)
32) LinkDown
5. Clean acl rule | wan1 (veth5 08:24:7c:e0:63:33)
33) LinkDown
6. Restore default |
7. Restore WEB passwd |
8. Reboot/Shutdown |
9. Ethernet driver |
o. Other option |
q. Quit |

Please input:
  console for English
  Version: CMD-COS-v1.01
  -----
0. System status | WEB Address -> http://192.168.1.1:80
1. Set ether band | lan1 (veth1 08:9b:4b:50:1c:bc) LinkUp
2. Set lan/wan address | lan1 (veth2 08:24:7c:e0:63:30) LinkDown
3. Set WEB port | lan1 (veth3 08:24:7c:e0:63:31) LinkDown
4. Ping Test | lan1 (veth4 08:24:7c:e0:63:32) LinkDown
5. Clean acl rule | wan1 (veth5 08:24:7c:e0:63:33) LinkDown
6. Restore default |
7. Restore WEB passwd |
8. Reboot/Shutdown |
9. Ethernet driver |
o. Other option |
q. Quit |

Please input: █
```

Fig 2.5.13 Telnet access of device page

6. Upgrading

Configuration Version: Displays the current Configuration version of the Gateway To upgrade the Gateway is to get more functions and better performance.

Note:

- After upgrading, the device will reboot automatically.
- To avoid damage to device, please don't turn off the device while upgrading.
- It is advised to backup the configuration before upgrading.

For Version upgrade click on System Setup > Upgrading > Version Upgrade You can check the New version available online or manual update from file.

For Automatic version update click on button check new Version.

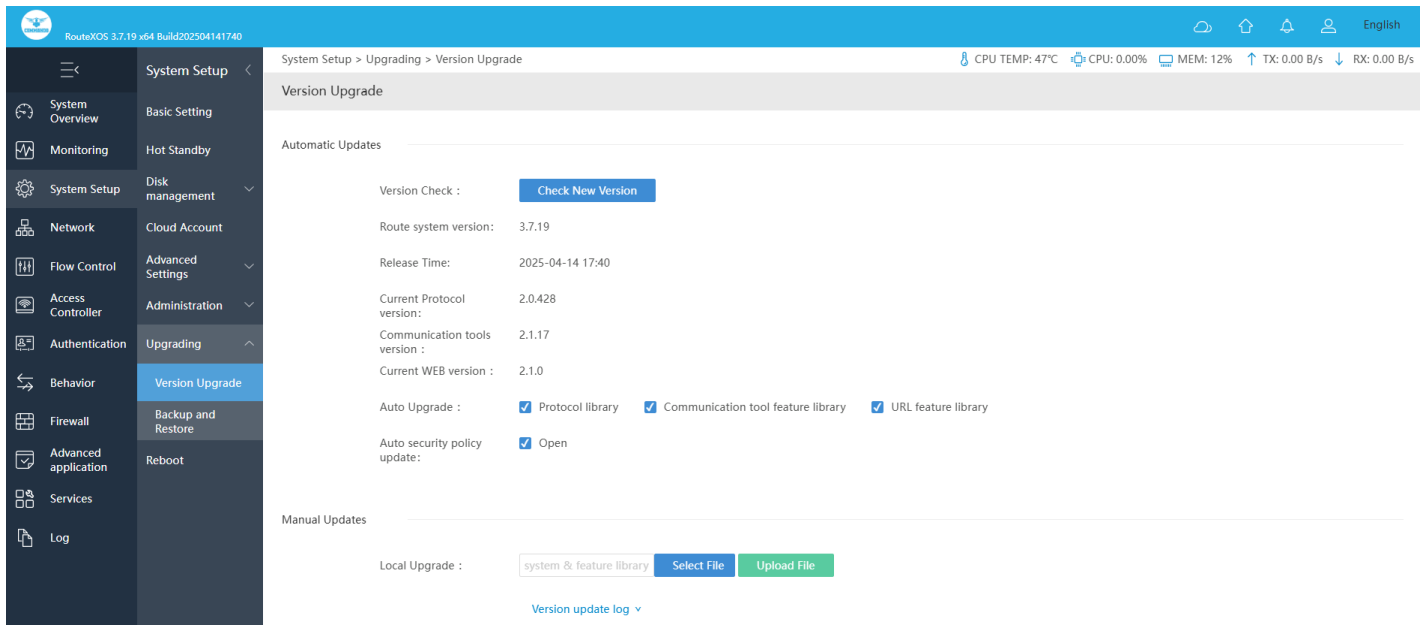


Fig 2.6.1 Version Upgrade page

Step 1: For Manual firmware update to version : 3.4.5 COMMANDO Series MSG-1200 by clicking System Setup >> Upgrading >> Version Upgrade or click Version update button on main page and go to local update, select the file mt7621v1-m1_sysupgrade_3.4.5_build202011161736 cma. bin

Step 2: Don't Power ON/OFF device. After that you must remove all browser history to login again with new firmware.

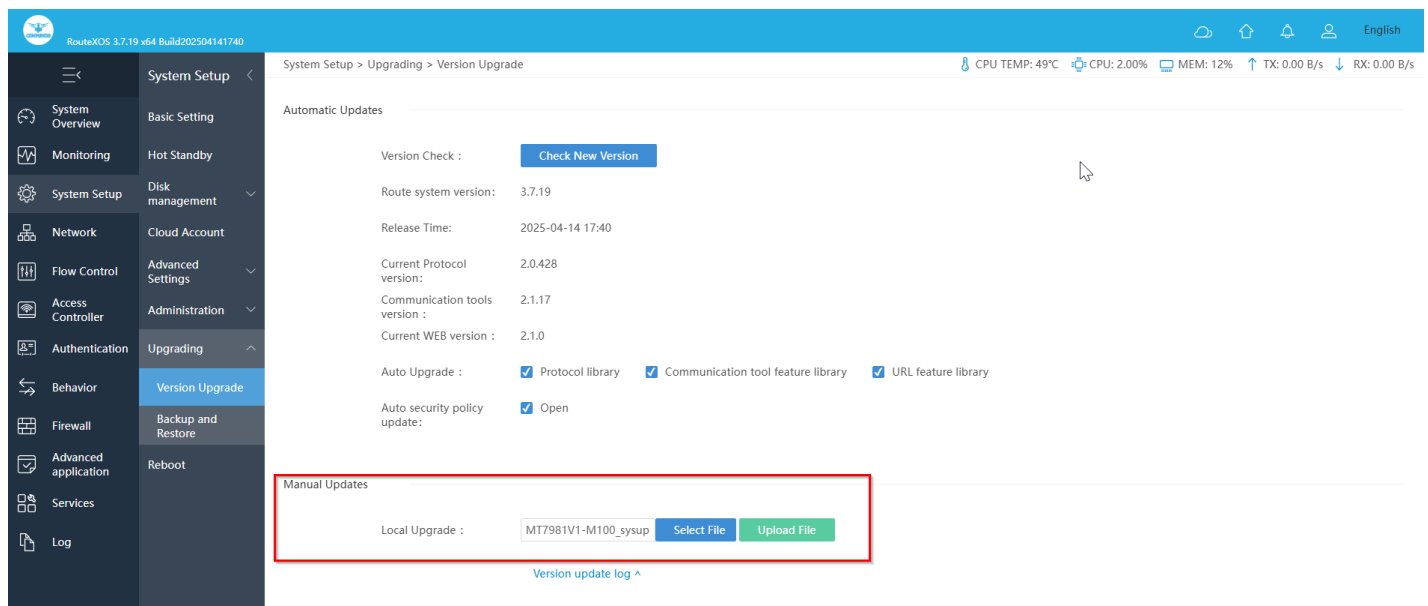


Fig 2.6.2 Manual Version Upgrade page

Backup and Restore: The Backup and Restore configuration feature allow end users to backup all configurations made to the Gateway. In cases when you need to reset the Gateway to factory default settings, you will be able to restore your previous configuration using the backup configuration file. This will save you time by not going through the process of reconfiguring the Gateway manually.

You can restore the Gateway to its factory default settings by the Reset button or by factory reset option in this page. It must be noted that once the Gateway is reset, all the current configuration settings will be lost. If you want old config files which is backup already then can use option upload backup. Use the page to restore the Gateway to the factory defaults or use the button to restore the Gateway to the factory defaults.

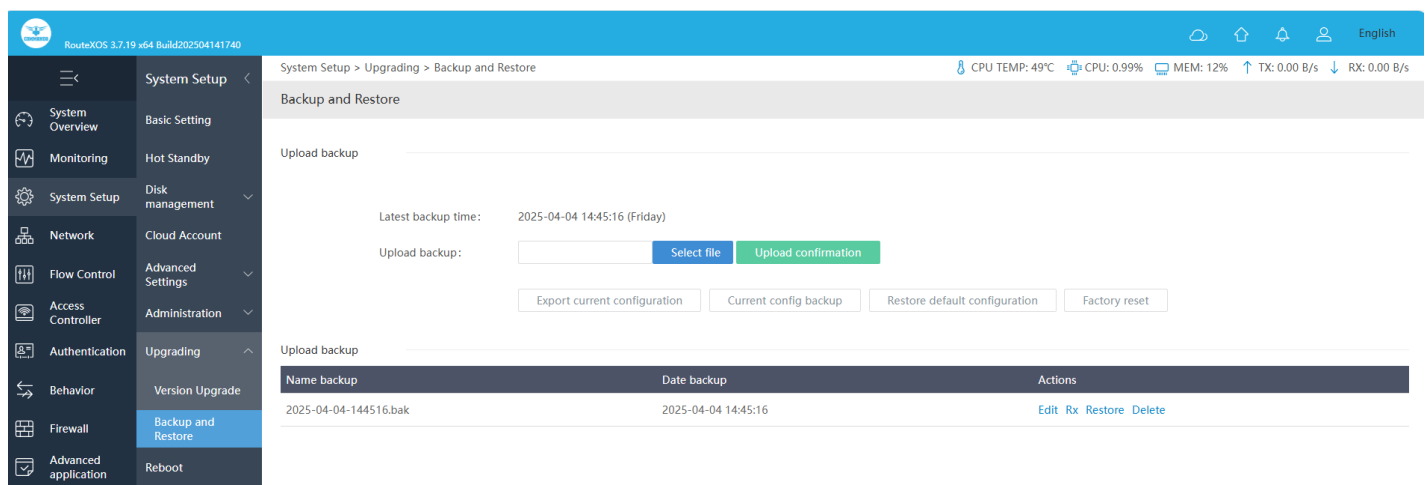


Fig 2.6.3 Default Backup and Restore page

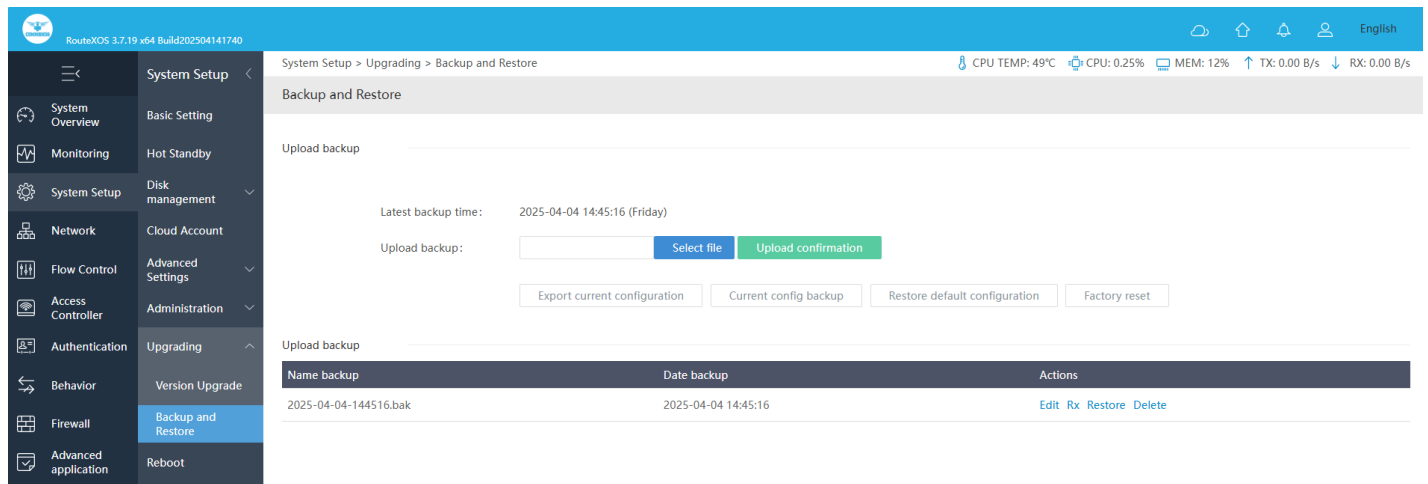


Fig 2.6.4 Options Backup and Restore page

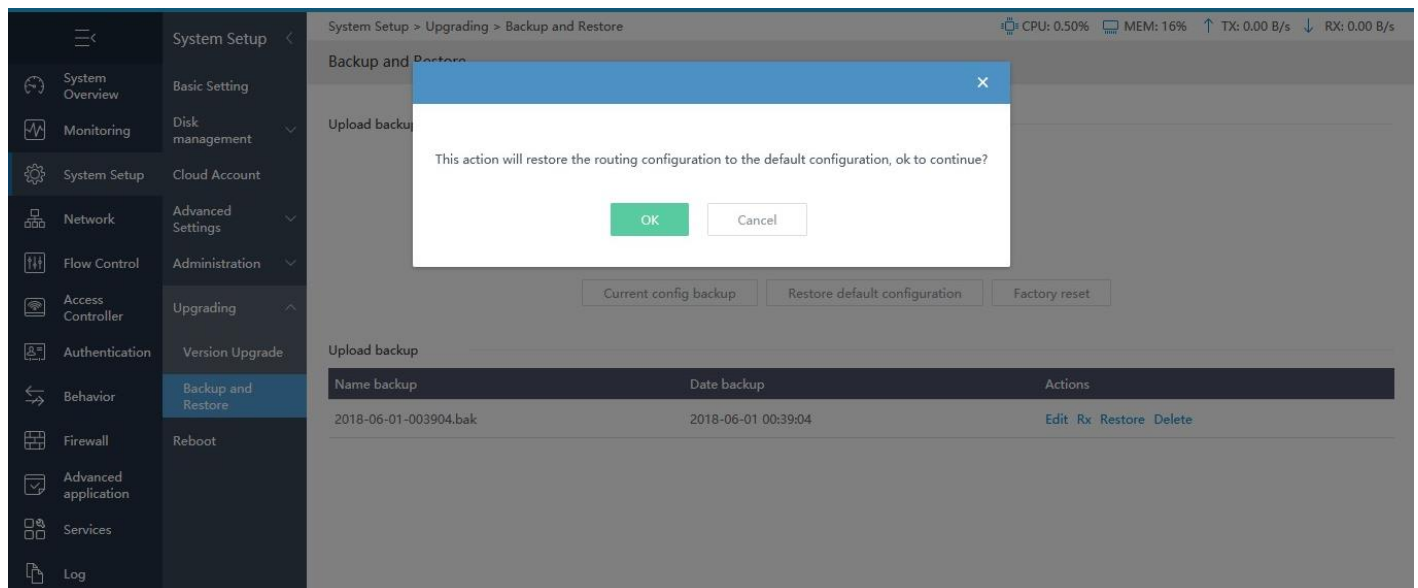


Fig 2.6.5 Backup the current configuration page

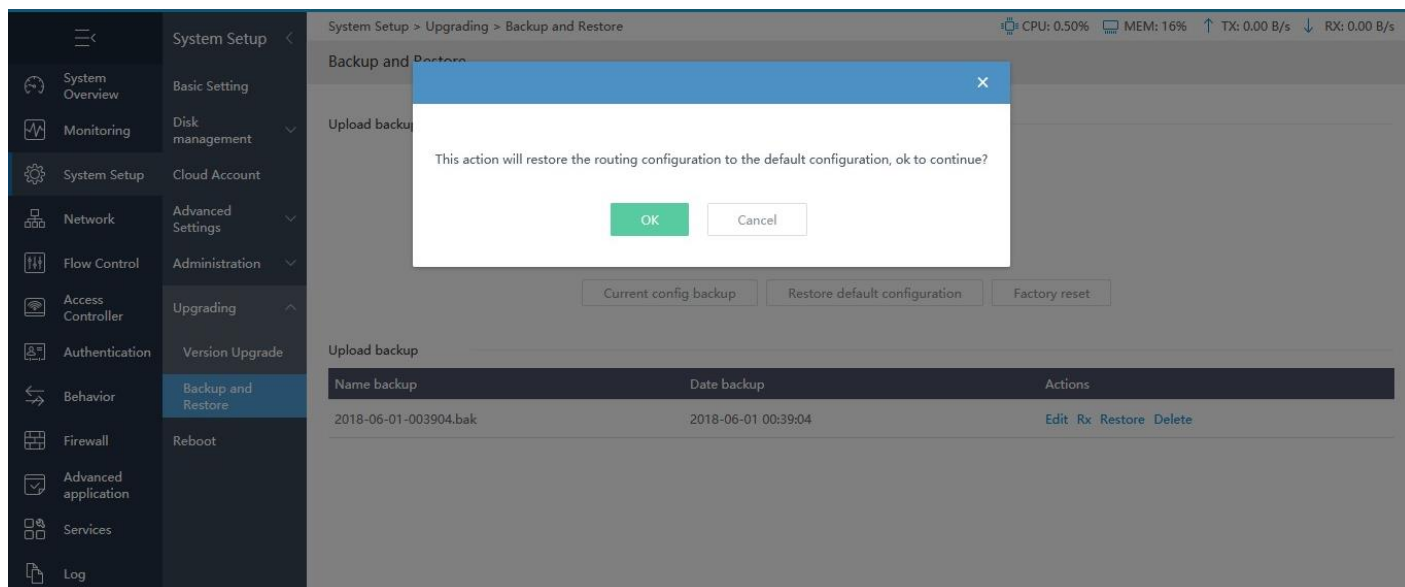


Fig 2.6.6 Restoring default configuration page

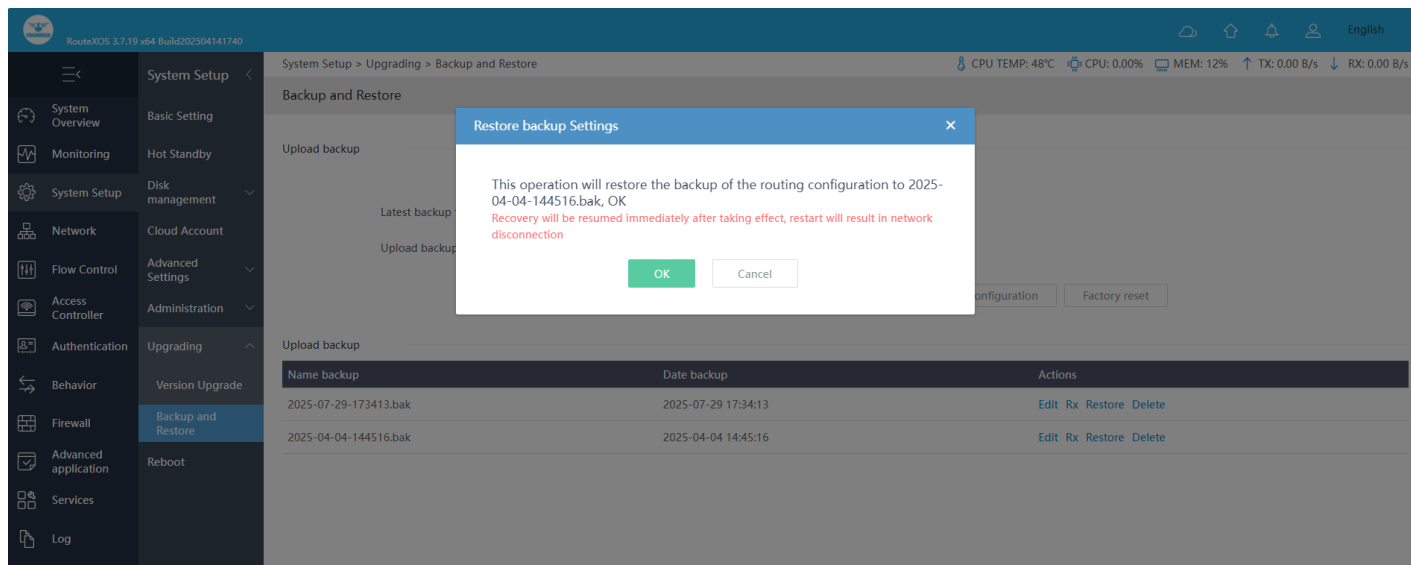


Fig 2.6.7 Restore Factory setting page

7. Reboot

The configuration will not be lost after rebooting. The Internet connection will be temporarily interrupted while rebooting.

For Reboot, Click on System Setup > Reboot

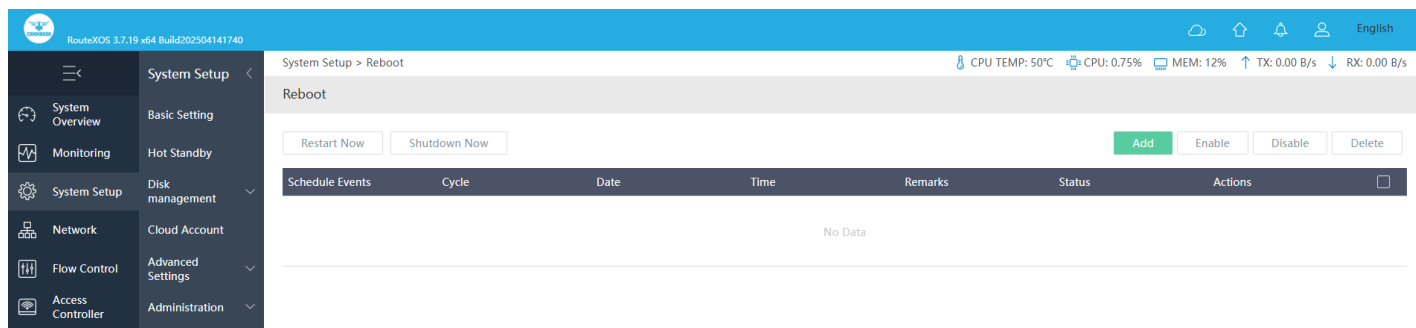


Fig 2.7.1 Default Reboot page

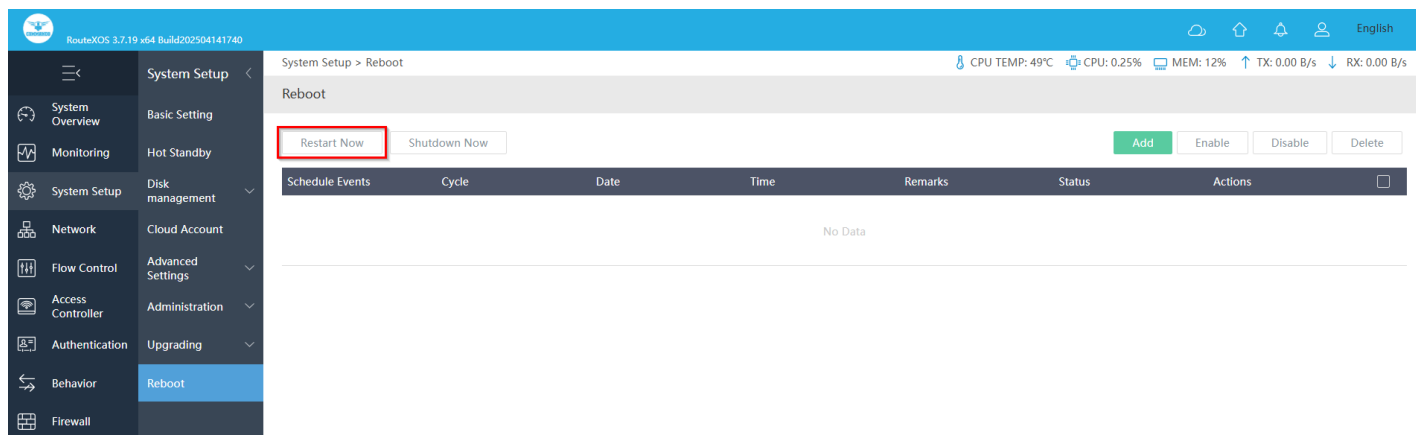


Fig 2.7.2 Restart Now page

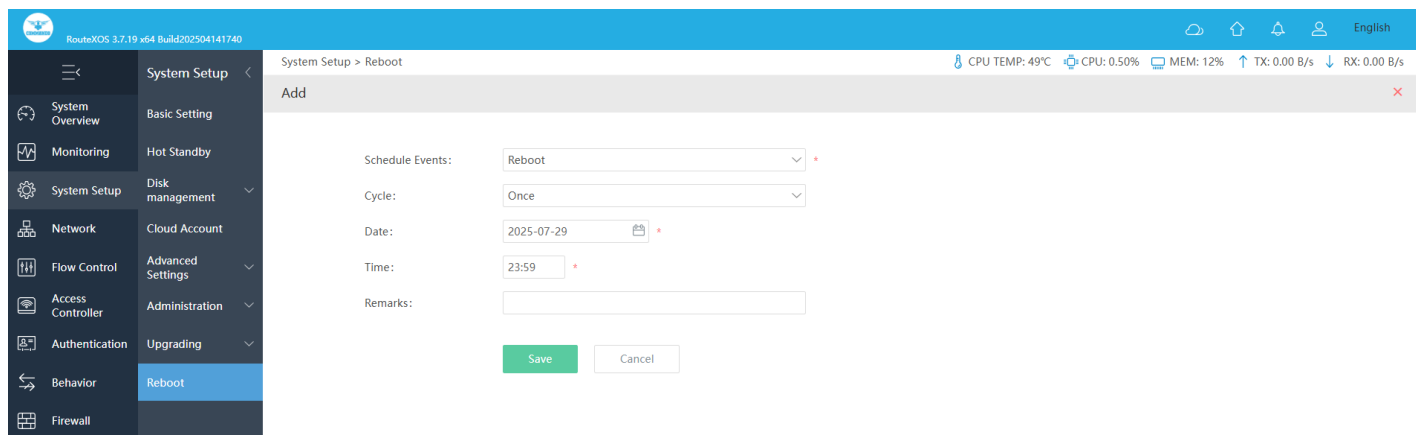


Fig 2.7.3 Default Schedule Restart page

RouteXOS 3.7.19 x64 Build202504141740

System Setup > Reboot

CPU TEMP: 49°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Schedule Events: Reboot

Cycle: Everyday

Time: 12:50

Remarks: Daily Reboot

Save Cancel

Fig 2.7.4 Add Schedule Restart page

RouteXOS 3.7.19 x64 Build202504141740

System Setup > Reboot

CPU TEMP: 50°C CPU: 6.02% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Reboot

Restart Now Shutdown Now Add Enable Disable Delete

Schedule Events	Cycle	Date	Time	Remarks	Status	Actions
Reboot	Everyday	--	12:50	Daily Reboot	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 2.7.5 Schedule Restart everyday page

NETWORK

Interfaces: Interface Settings can be change along with monitor Connection Count, WAN count, LAN Count and Device Connected and also check status of LAN and WAN connection.

DHCP: You can add address pool for a specific Interface. So that the client connected with that interface can dynamically (Automatically) be allocated IP addresses. Import and Export feature of DHCP Server setting helps you to save your time in reconfiguring same setting if server migrated to another place. Restart DHCP Service feature available. This is required after new configuration done to take effect. DHCP Server Settings, DHCP Static IP Mapping with Compatible ARP binding list is statically assigned, Viewing DHCP Leases, Black List or White List. In Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses) Whitelist Mode (All MACs except whitelist prohibit IP address assignment) Synchronize MAC access control (DHCP black and White List Settings are synchronized with behavior control-mac access control).

DNS: Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. It can add separate Primary and Secondary DNS for different WAN. In DNS Settings we can set preferred DNS, Alternative DNS, DNS Acceleration Service and mode.

IP/MAC Group: It configured here can be used as effective IP addresses for multiple functions like Bandwidth Control, Session Limit, Policy Routing and so on.

Static Routes: You can configure policy routing rules and static routing. Policy routing provides a more accurate way to control the routing based on the policy defined by the network administrator. Static routing is a form of routing that is configured manually by adding non-aging entries into a routing table. The manually configured routing information guides the Gateway in forwarding data packets to the specific destination.

VLAN: The VLAN function can prevent the broadcast storm in LANs and enhance the network security. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own.

UPNP: UPnP (Universal Plug and Play) protocol from different manufacturer can automatically discover and communicate with one another.

NAT: It is the translation between private IP and public IP vice a versa. NAT provides a way to allow multiple private hosts to access the public network using one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security since the address of LAN host never appears on the internet. The Gateway supports following NAT features like One-to-One NAT which creates a relationship between a private IP address and a public IP address. A device with a private IP address can be accessed through the corresponding valid public IP address. When users are set to be a DMZ (Demilitarized Zone) hosts in the local network are totally exposed to the internet attacks due to bidirectional communication between internal hosts and external attackers. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the user to be a DMZ host.

Port Mapping: Port Mapping / Port Forwarding Settings is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway. DMZ (Demilitarized Zone) feature, you are allowing the Gateway to forward all incoming traffic from the internet to the device specified, virtually disabling the Gateway "firewall protection". This may expose the device to a variety of security risks, so only use this option as a last resort.

IPv6: Configure the network for IPv6. Configure your primary name service (DNS, NIS, or LDAP) to recognize IPv6 addresses after the Gateway is configured for IPv6. DHCPv6 to allocate IPV6 address dynamically. You can also modify the addresses for the IPv6-enabled interfaces on hosts and servers.

IGMP Agent: The IGMP Agent is responsible for forwarding multicast messages only to VMs that are registered to that multicast group, while respecting the filtering fields that are defined in IGMPv3. VM registration is detected by processing IGMP Join packets that all subscribed VMs send.

IPTV transparent transmission: IPTV transparent transmission ensures the seamless delivery of IPTV traffic without altering packet structures or affecting data integrity. This option allows multicast and unicast IPTV streams to pass through the network without interference, preserving video quality and minimizing latency. By enabling transparent transmission, the system ensures smooth playback, reduces buffering, and maintains compatibility with various IPTV services and devices.

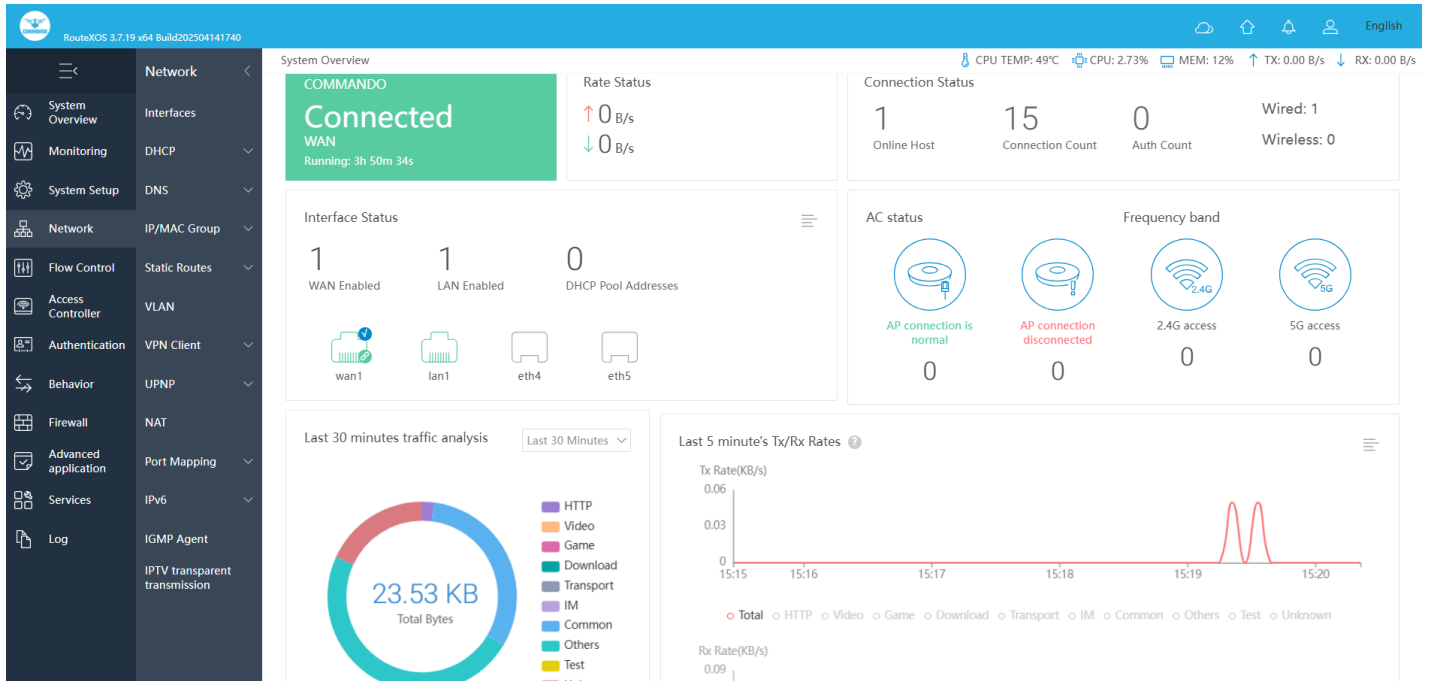


Fig 3.1 Network Tab options page

1. Interfaces

Select interface for creating multiple LAN and WAN ports. By default, WAN1 and LAN1 port is created. You can create maximum 4 separate LAN port and 4 WAN ports. The entry will take effect when the interface to which the data is flowing is selected.

You can create and access all ports parameter of interfaces by clicking Network > Interfaces

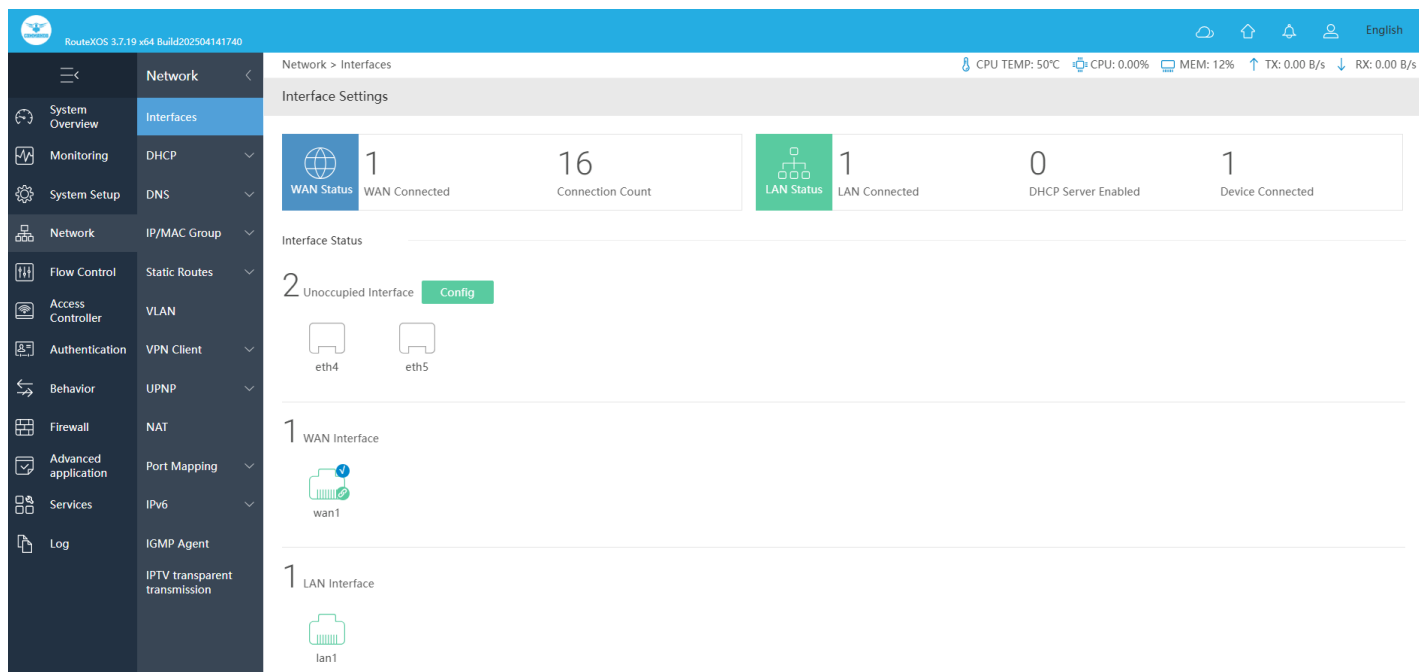


Fig 3.1.1 Default interface setting page

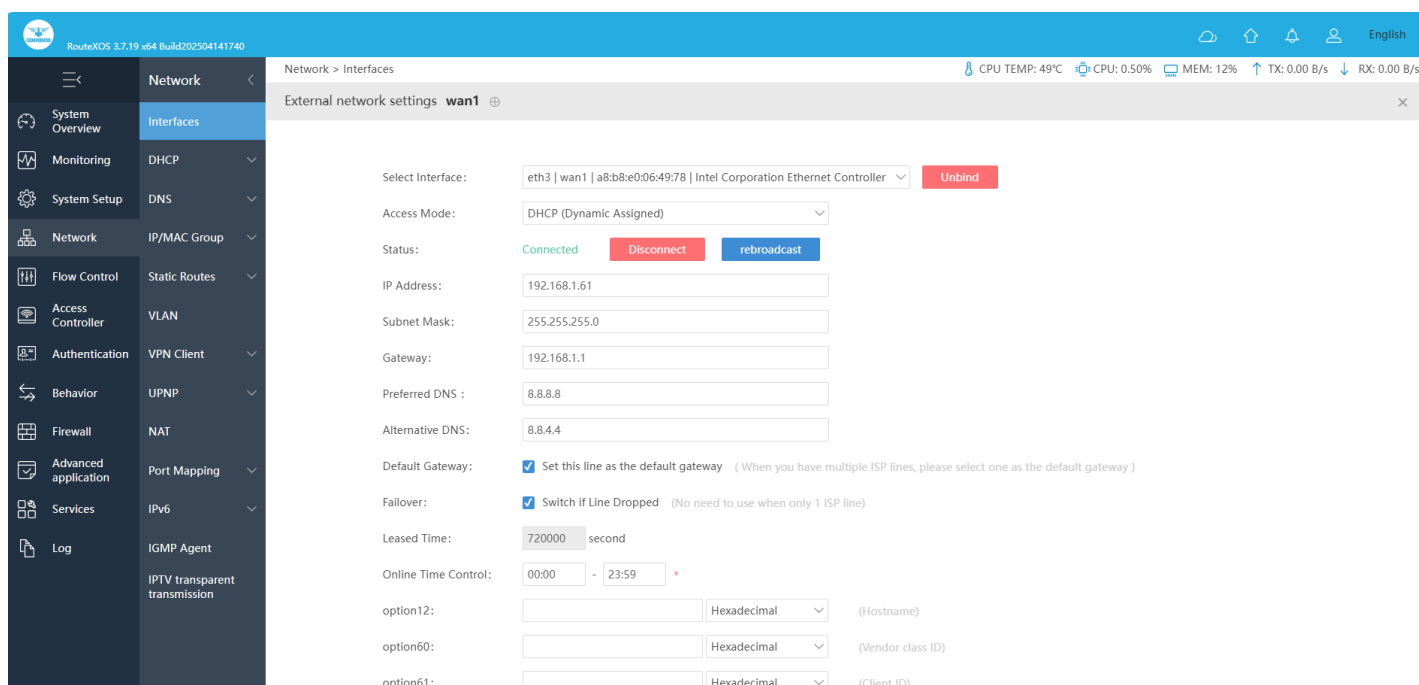


Fig 3.1.2 Default External Network setting options

RouteXOS 3.7.19 x64 Build202504141740

Network > Interfaces

CPU TEMP: 50°C CPU: 0.74% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

External network settings **wan1**

Select Interface: eth3 | wan1 | a8:b8:e0:06:49:78 | Intel Corporation Ethernet Controller Unbind

Access Mode: DHCP (Dynamic Assigned)

Status: Connected Disconnect rebroadcast

IP Address: 192.168.1.61

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Preferred DNS : 8.8.8.8

Alternative DNS: 8.8.4.4

Default Gateway: ☒ Set this line as the default gateway (When you have multiple ISP lines, please select one as the default gateway)

Fallover: ☒ Switch if Line Dropped (No need to use when only 1 ISP line)

Leased Time: 720000 second

Online Time Control: 00:00 - 23:59 *

option12: Hexadecimal (Hostname)

option60: Hexadecimal (Vendor class ID)

Fig 3.1.3 Setting External Network setting for WAN1 interface page

RouteXOS 3.7.19 x64 Build202504141740

Network > Interfaces

CPU TEMP: 50°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Intranet settings **lan1**

Select Interface: eth0 | lan1 | a8:b8:e0:06:49:75 | Intel Corporation Ethernet Controller I

IP Address: 192.168.0.1 *

Subnet Mask: 255.255.255.0(24)

Remarks:

Advanced Settings ▾

Save Cancel

Fig 3.1.5 Default intranet Network setting for LAN1 interface page

Note: By default all 4 LAN ports are mapped and activated namely veth 1,2,3,4 in LAN1.

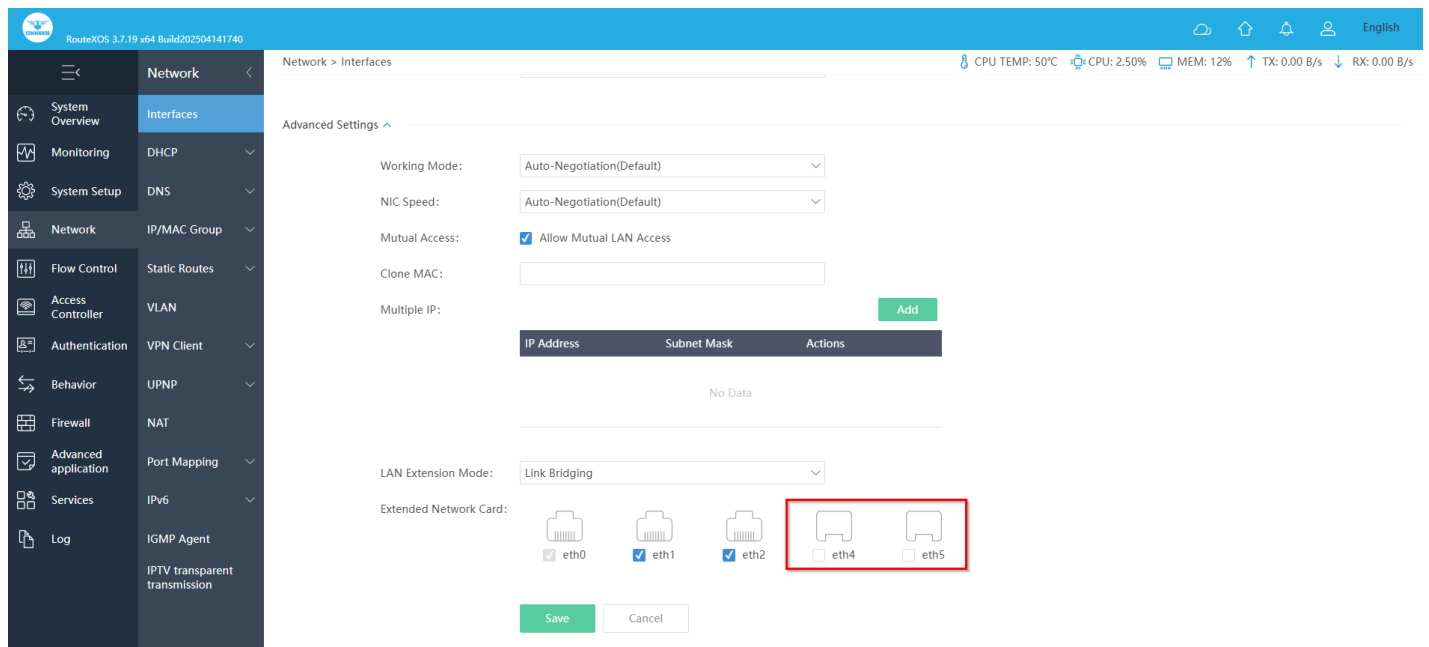


Fig 3.1.6 Intranet Network setting for releasing ports form LAN1 interface page

Note: To release and reuse other port from LAN1 interface unclick on highlighted button.

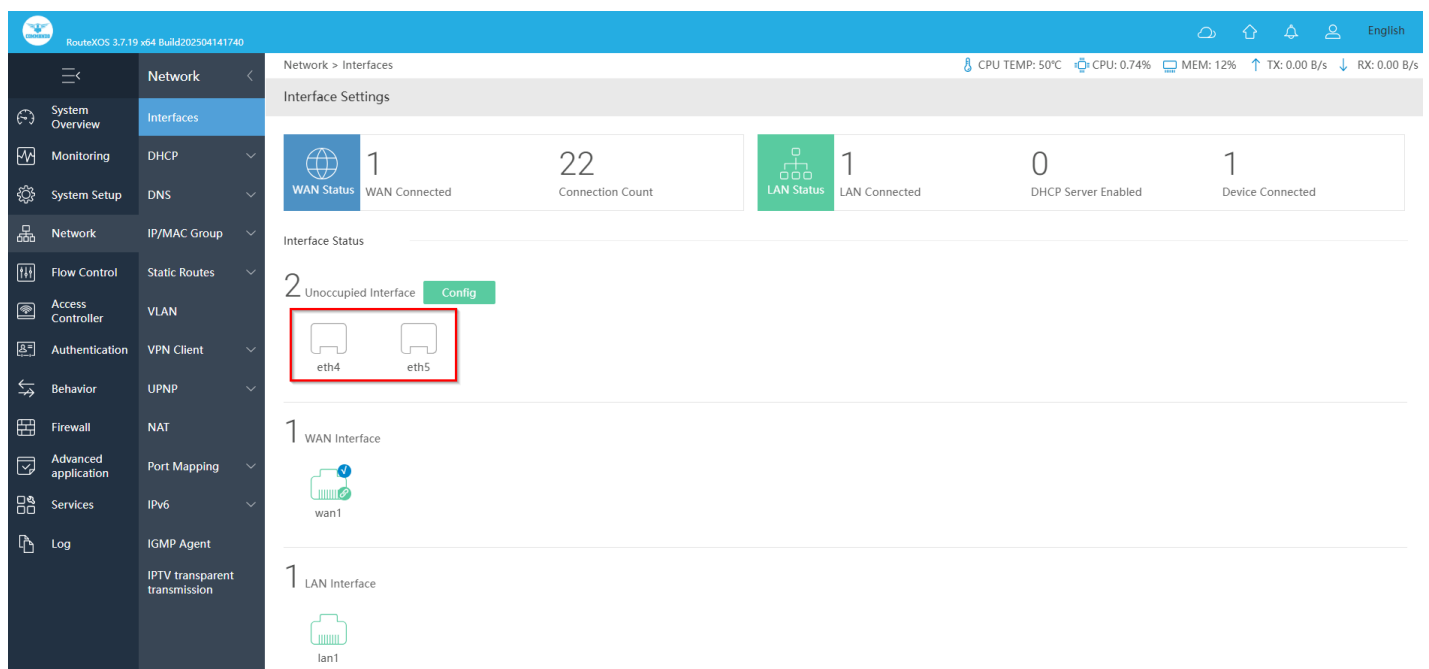


Fig 3.1.7 Interface setting after releasing ports form LAN1 interface page

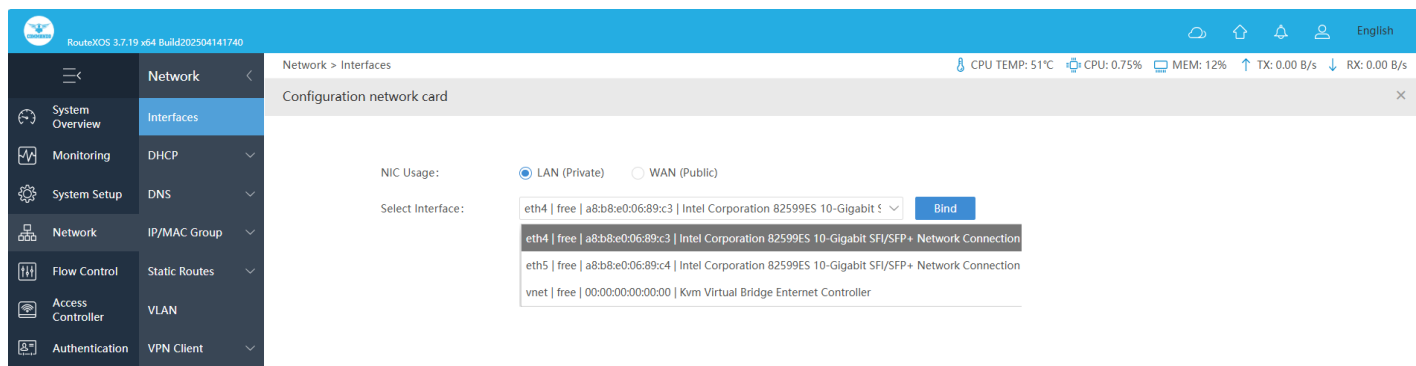


Fig 3.1.8 Select Interface setting for LAN and WAN interface page

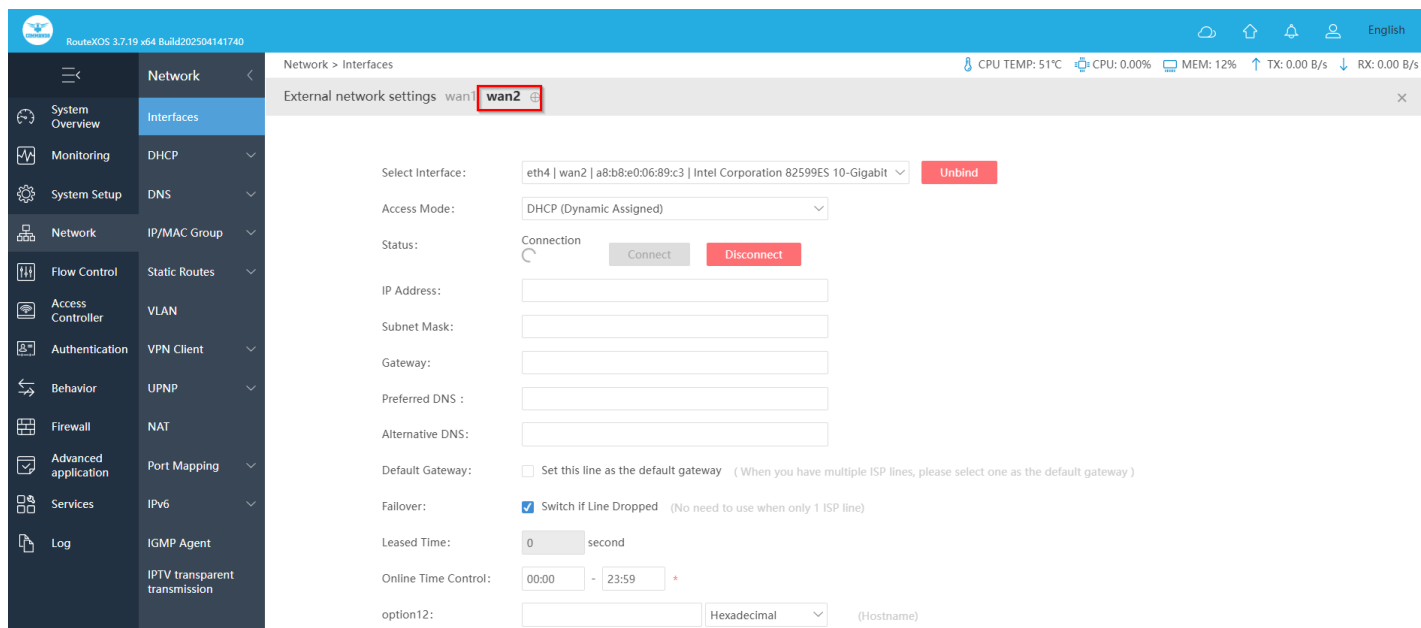


Fig 3.1.9 Creating WAN2 interface page

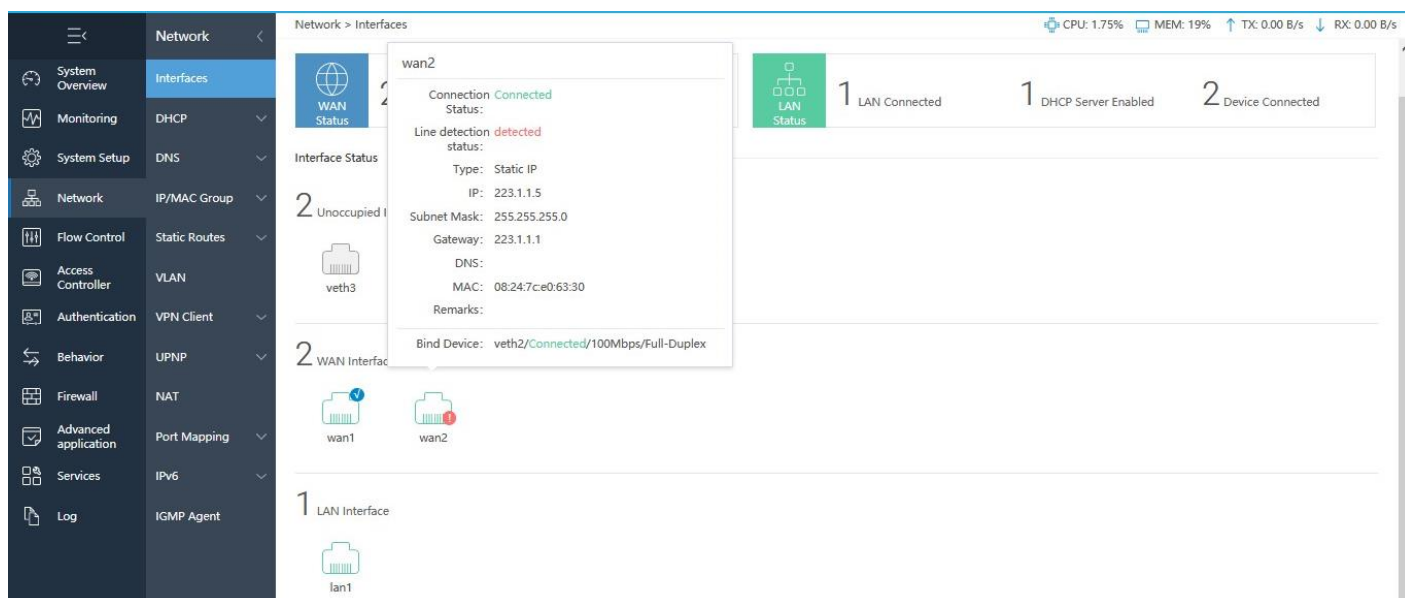


Fig 3.1.10 Network interface page after creating WAN2 interface page

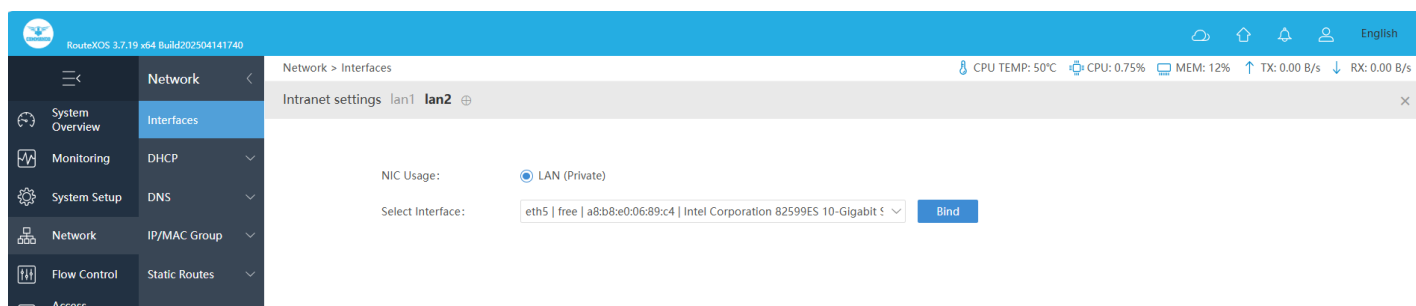


Fig 3.1.11 Creating LAN2 interface page

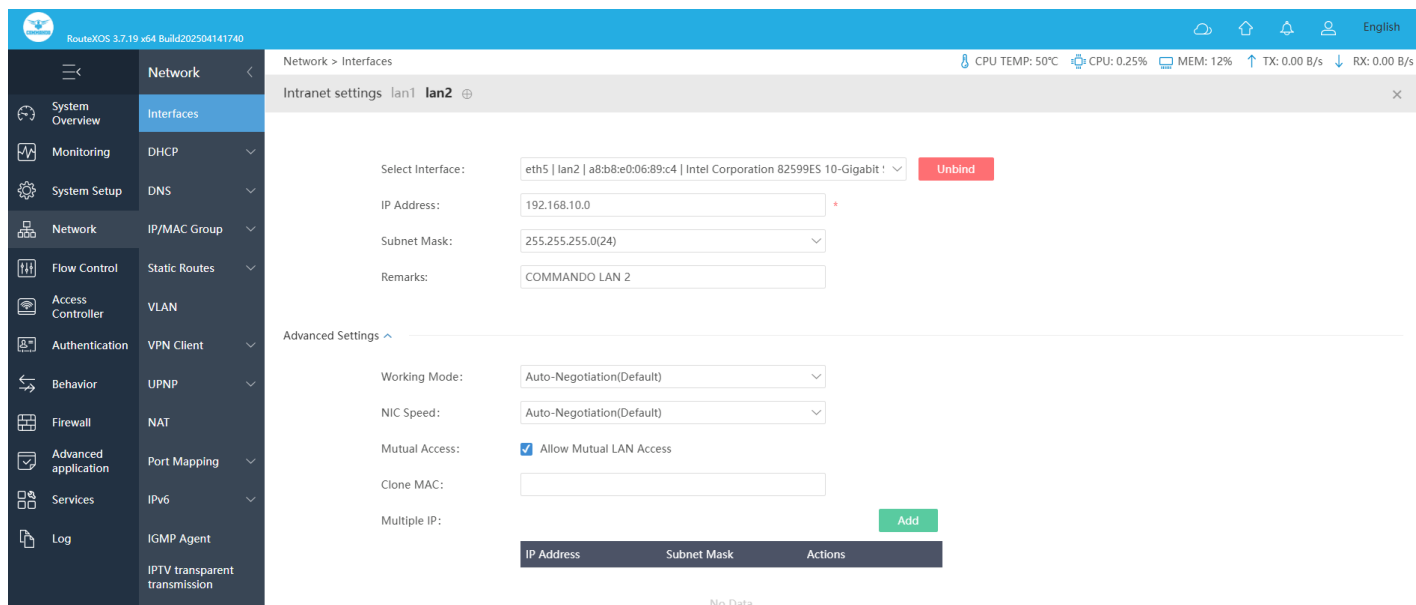


Fig 3.1.12 Setting LAN2 interface parameter page

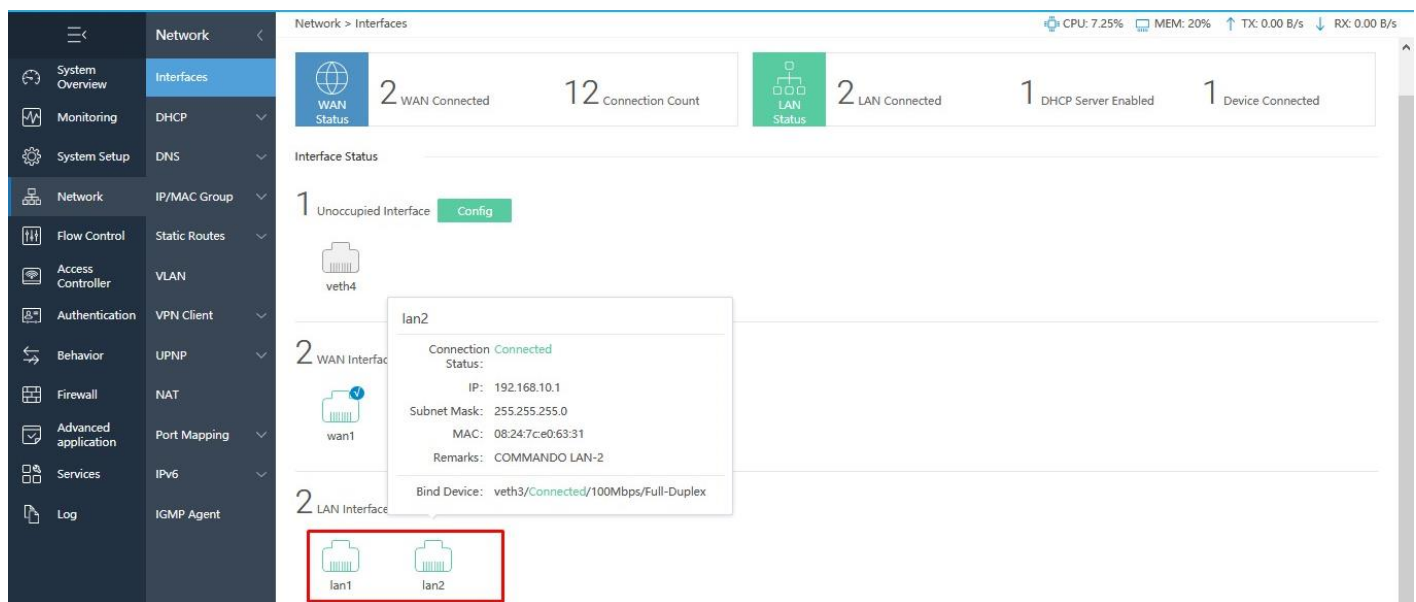


Fig 3.1.13 Network interface page after creating LAN2 interface page

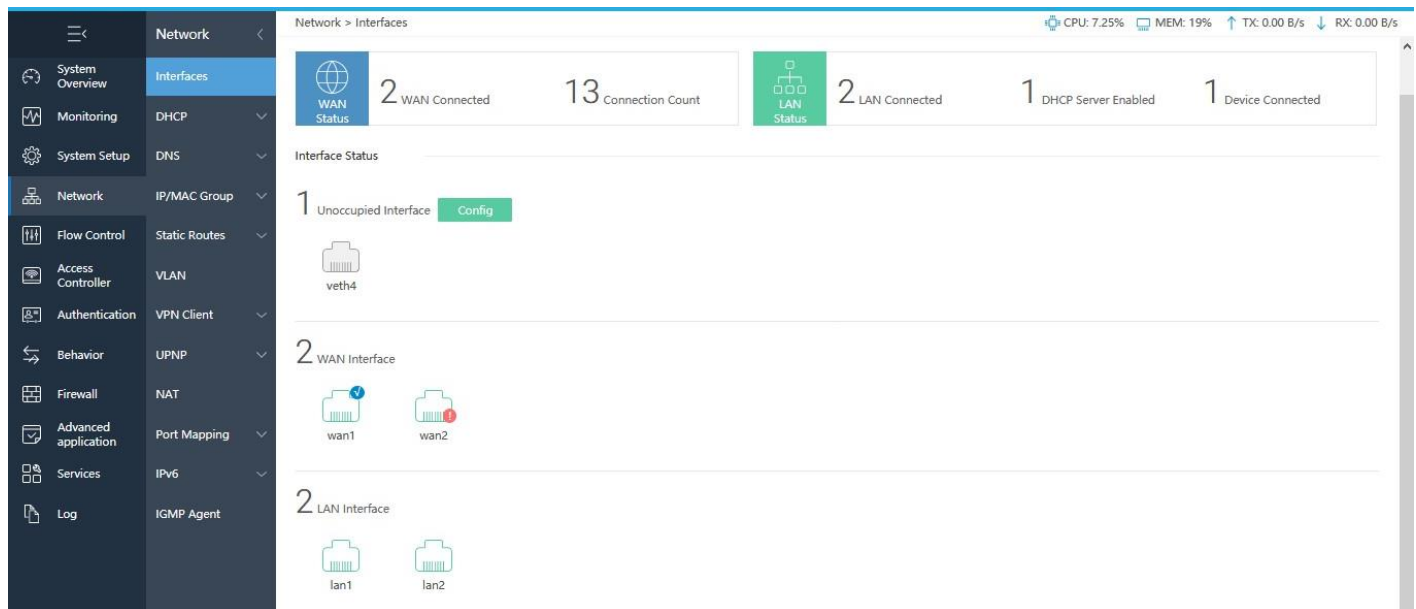


Fig 3.1.14 Network interface page after creating user defined interfaces page

How to delete unwanted interfaces?

Deleting an unwanted network interface or create a new one by sparing ports which already created is very necessary sometimes.

Example: If you want to delete LAN2 port

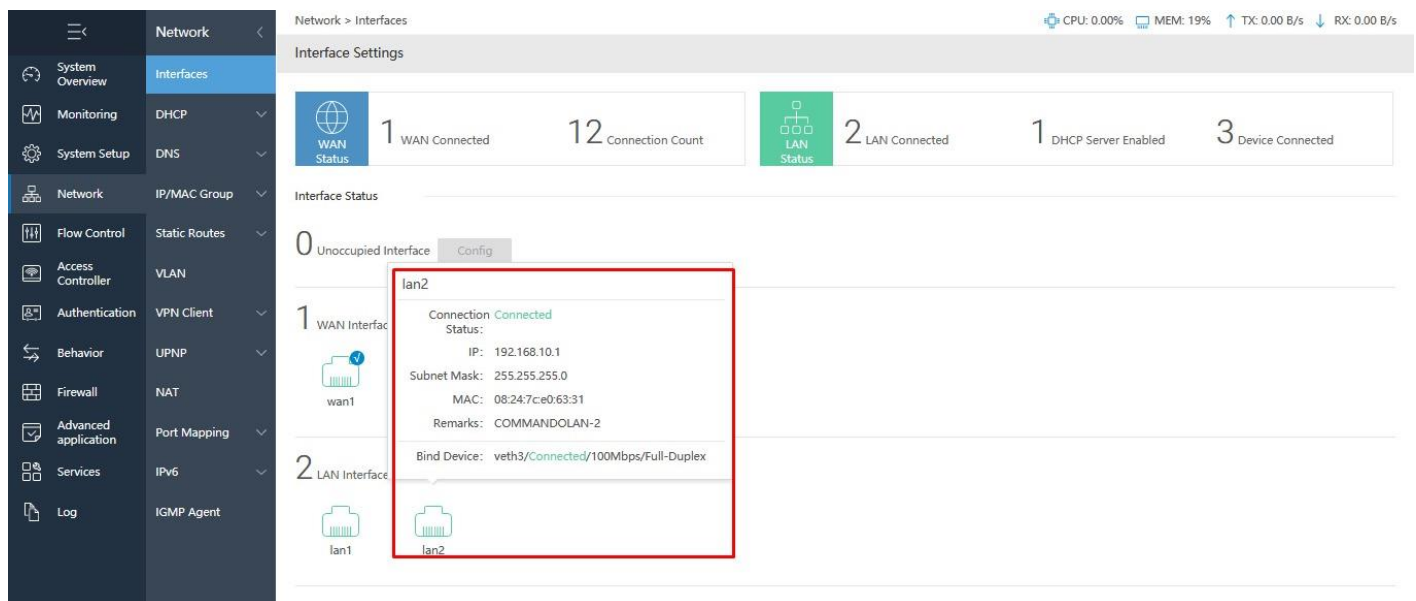


Fig 3.1.15 Deleting interface after creating user defined LAN2 interface page

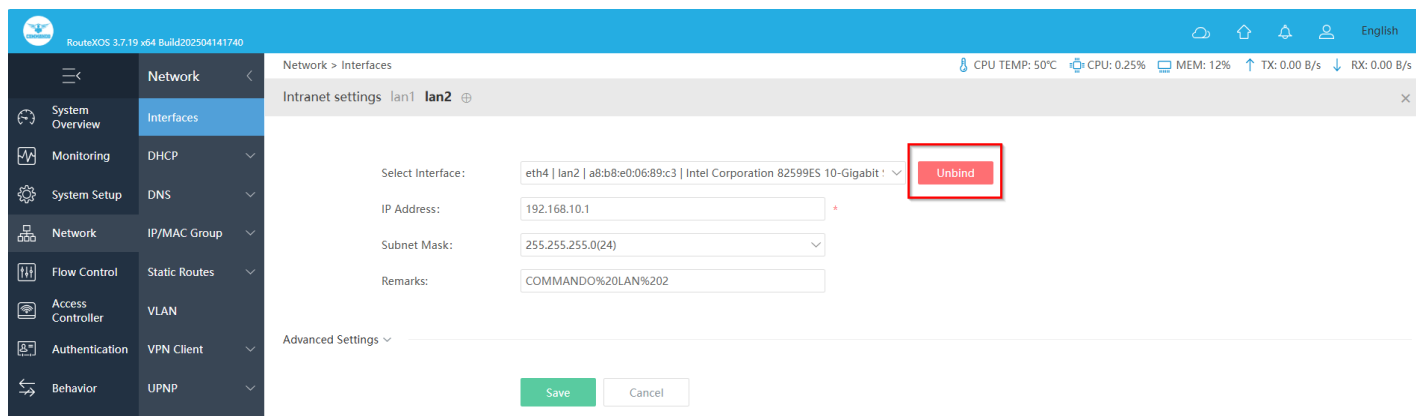


Fig 3.1.16 Unbinding port from LAN2 interface page

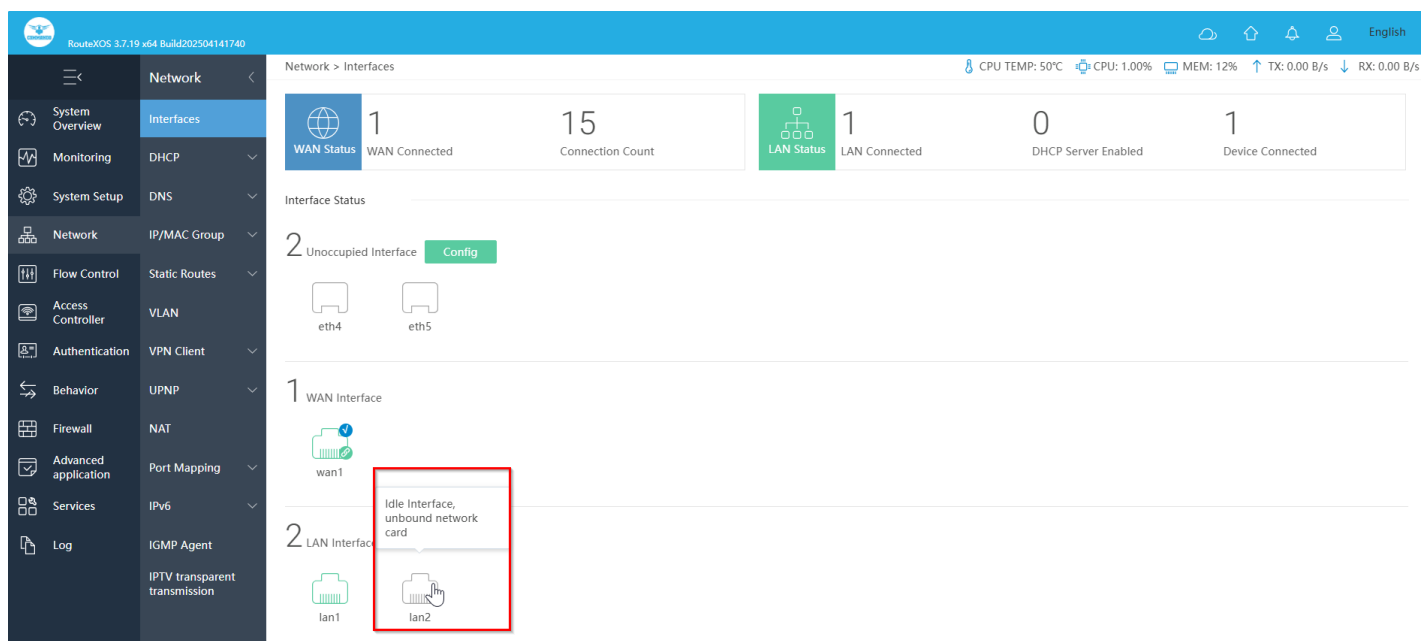


Fig 3.1.17 Network interface page after unbinding port from LAN2 interface page

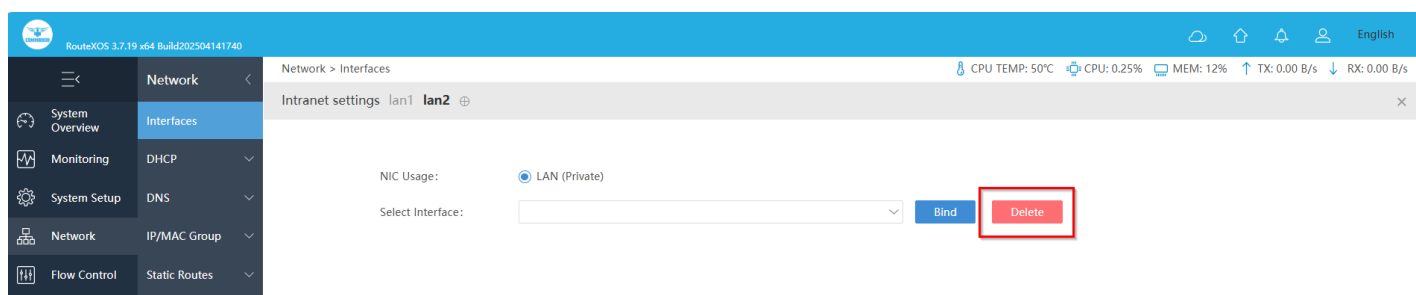


Fig 3.1.18 Deleting port from LAN2 interface page

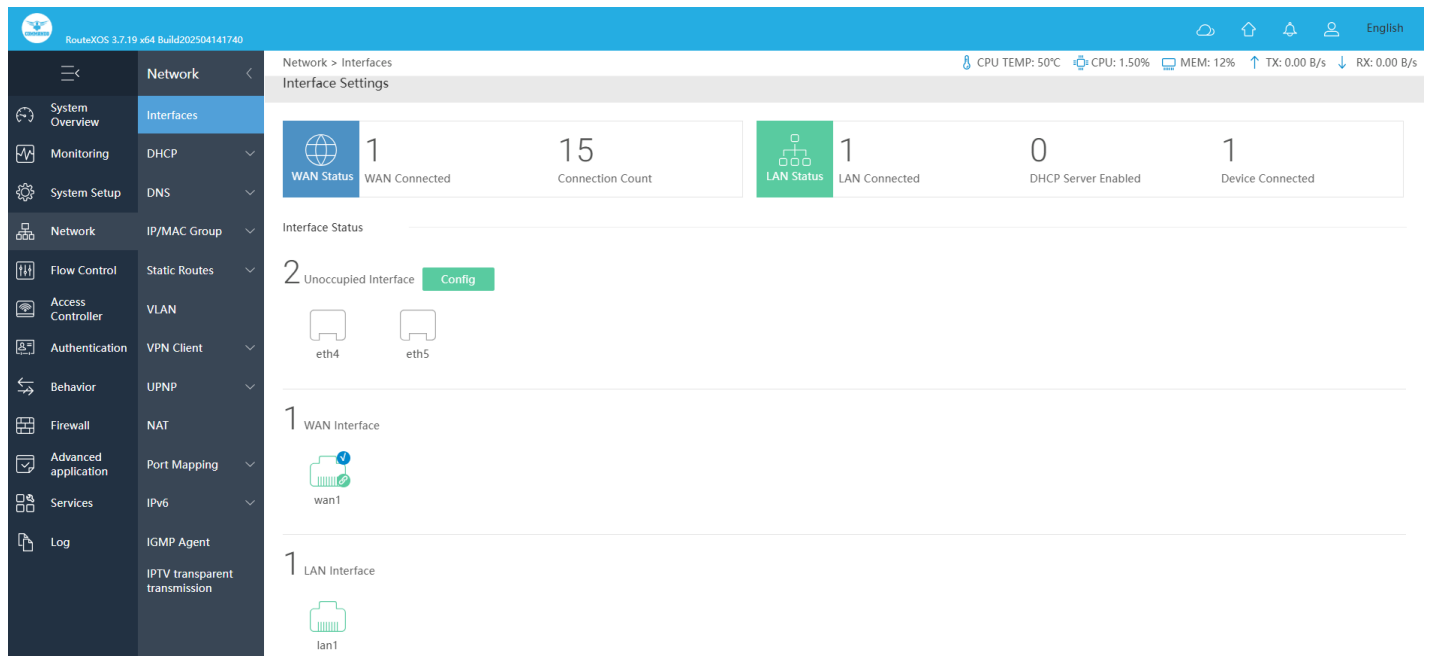


Fig 3.1.19 Network interface page after deleting LAN2 interface page

How to bind all 4 ports to LAN1 interface?

Click on Network > Interfaces LAN1 port, go to advance setting and click veth2,3,4 to bind ports to LAN1.

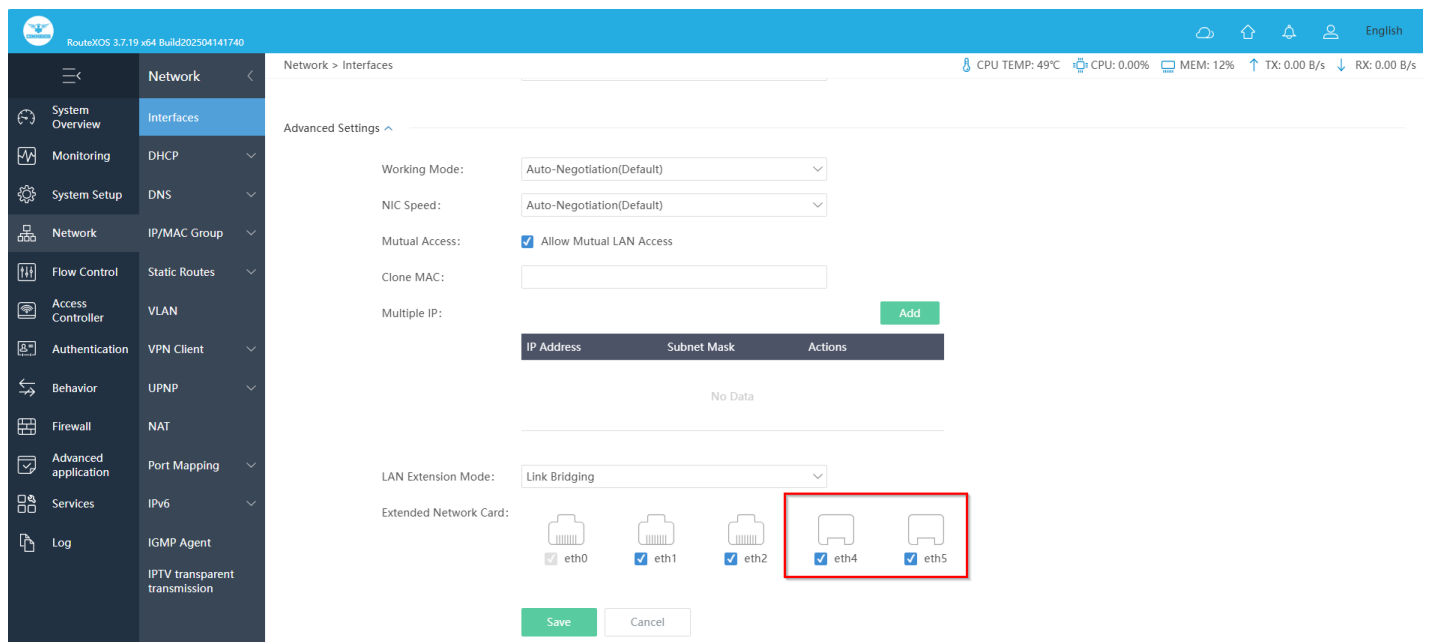


Fig 3.1.20 Binding ports 4,5 to LAN1 interface page

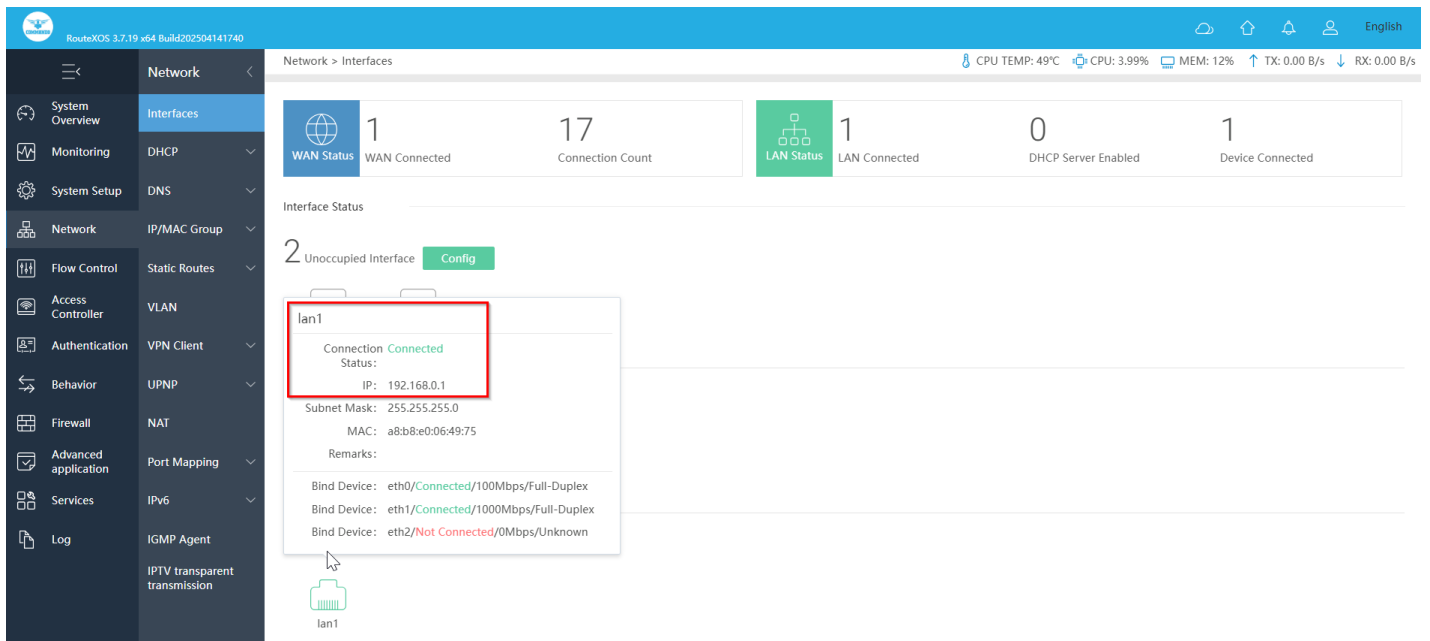


Fig 3.1.21 Interface setting of LAN1 interface page

2. DHCP

The Gateway with its DHCP (Dynamic Host Configuration Protocol) server enabled can automatically assign an IP address to the devices in the LAN. All Four LAN ports can be configured with 4 different DHCP servers as per requirement.

DHCP Server: A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

Interface: You can provide and create DHCP server on any LAN selected and also can define and set different DHCP pool for each LAN interface.

Address Pool: Address pool consist of start IP address first IP to be assign as dynamic IP addresses. This address should be in the same IP address subnet with the Gateway's LAN IP address. The default address is 192.168.1.100 and end IP address to define end Ip address to assign as dynamic IP addresses. This address should be in the same IP address subnet with the Gateway's LAN IP address. The default end address is 192.168.1.200 with DHCP server IP pool length 100. You can modify settings as per requirements.

Subnet Mask: A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network.

Gateway

Primary DNS: A primary DNS server is the first point of contact for a browser, application or device that needs to translate a human-readable hostname into an IP address.

Secondary DNS: The secondary DNS server is an authoritative server that obtains information about a zone from the primary server via zone transfer. DNS IP address of your ISP's is in Secondary DNS.

Lease(minute) This DHCP-assigned IP address is not permanent and by default expires in about 120 minutes. This is called DHCP lease time. Unless otherwise mentioned, the DHCP server assumes that all IP addresses are temporary and expire after some time.

Check interface IP validity: Check Ip is used by anyone in LAN before assign to avoid conflicts.

Applies only to DHCP relay: The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

Domain Name: Can set your domain name.

Main WINS server: WINS is an essential part of the Microsoft networking topology. In the older days, you were required to run a WINS server in order to avoid name resolution problems within a Windows network. In short, DNS maps TCP/IP host names to IP addresses and WINS maps NetBIOS host names to IP addresses.

To change or modify DHCP server setting, Click on Network > DHCP > DHCP Server

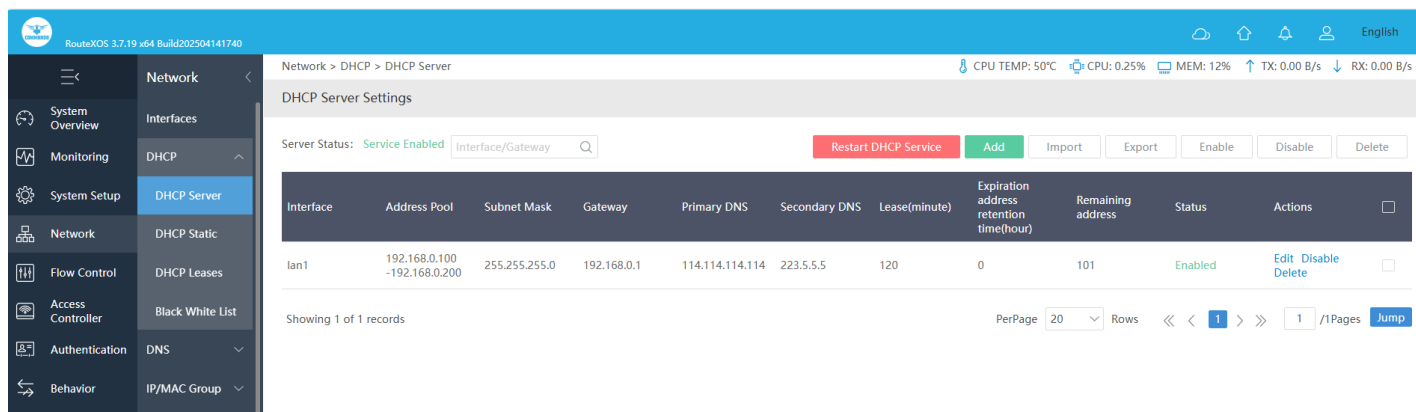


Fig 3.2.1 Default DHCP Server Settings of LAN1 interface page

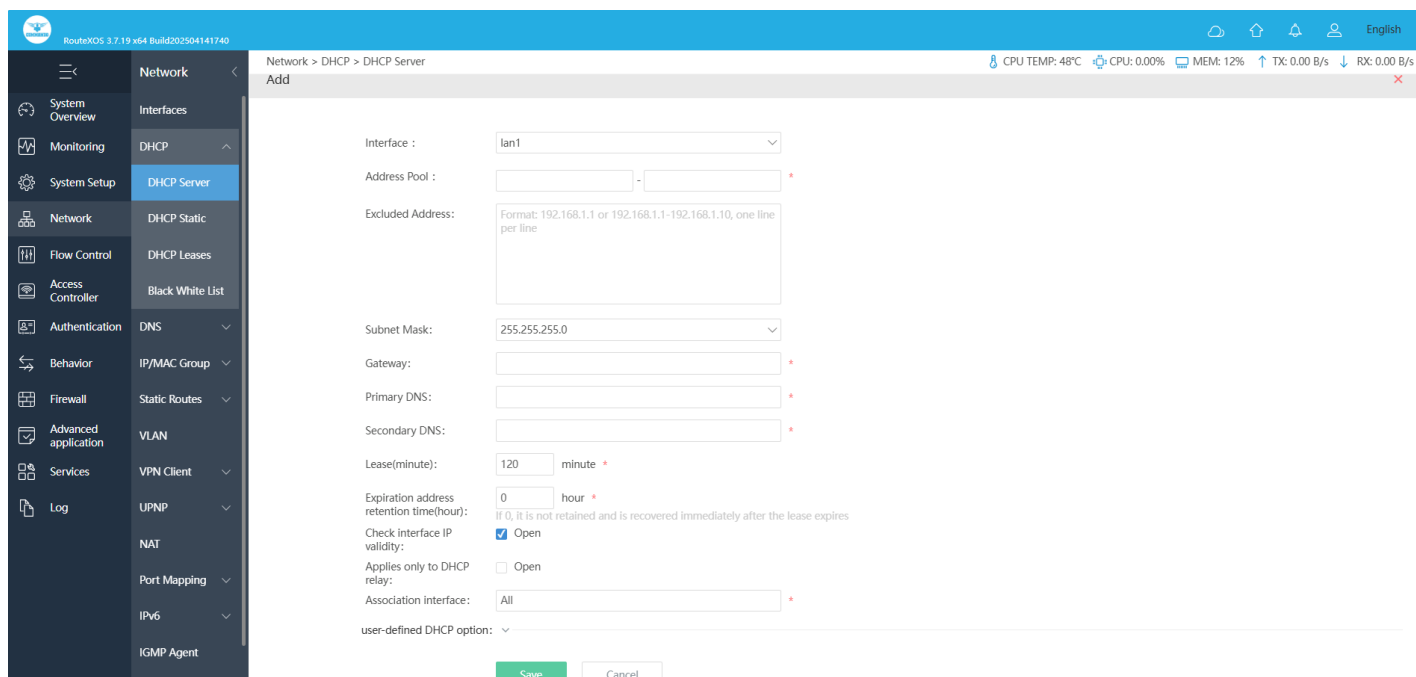


Fig 3.2.2 Add DHCP Server Settings of LAN1 interface page

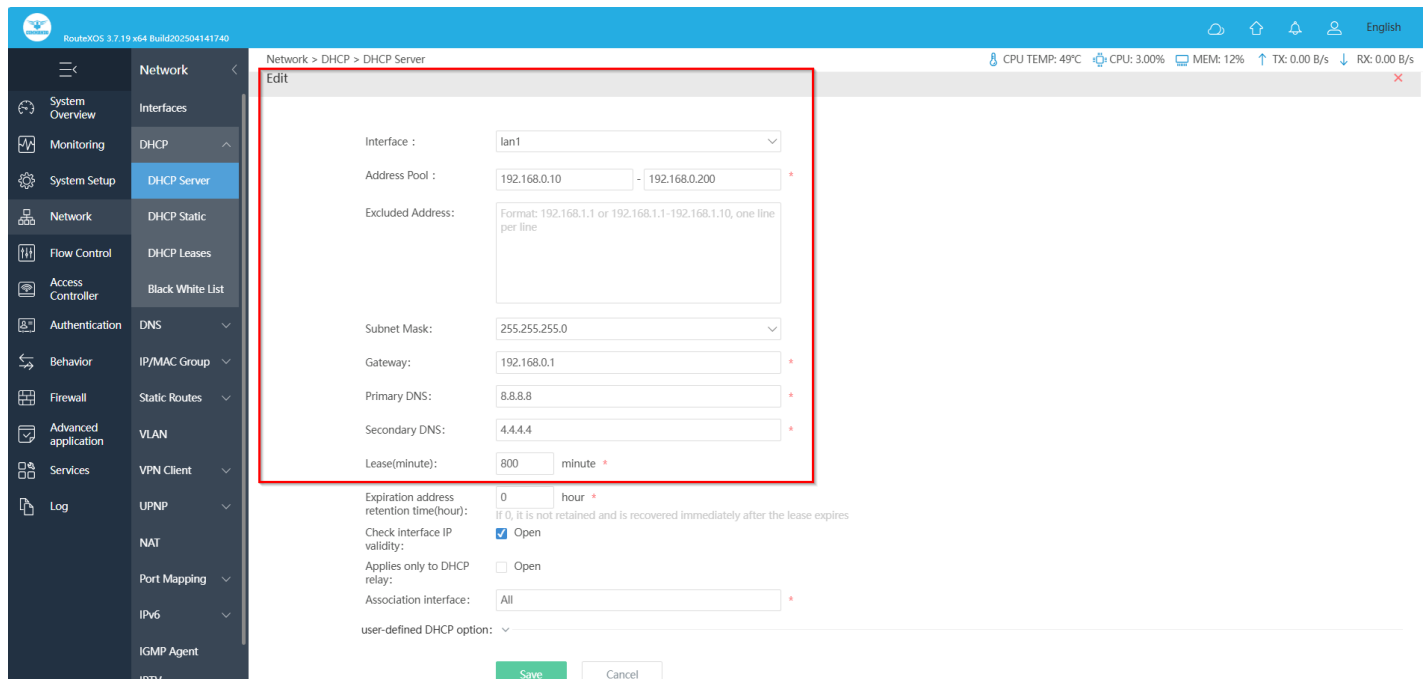


Fig 3.2.3 Editing DHCP Server Settings of LAN1 interface page

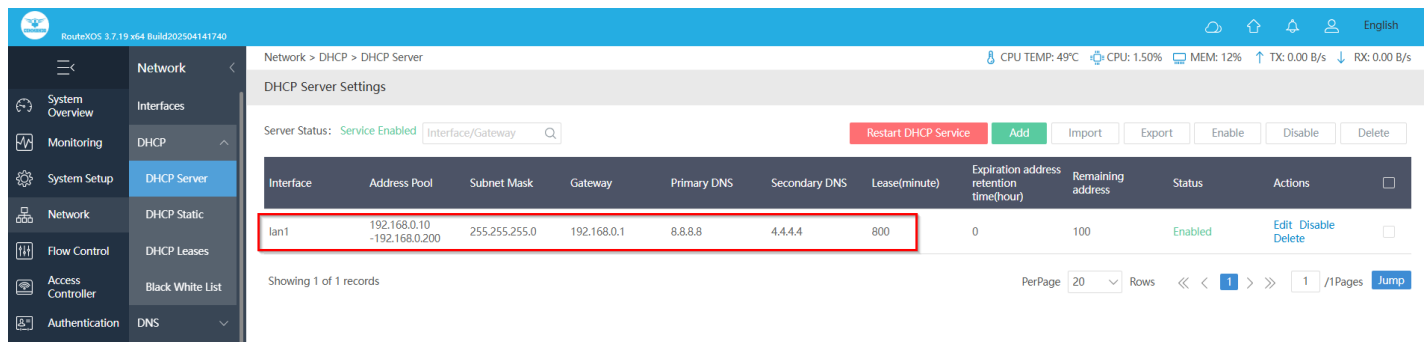


Fig 3.2.4 DHCP Server Settings of LAN1 interface page DHCP Static binding

A static IP address binding is ultimately set by an administrator and does not change. Although DHCP stands for dynamic host configuration protocol, you can still set up static IP addresses using DHCP. This allows the network server to always get the same IP even after it reboots, without dynamically assigning the IP. The DHCP Static IP Mapping feature enables assignment of static IP addresses with MAC address without taking IP addresses from DHCP pool with manual bindings. Compatible ARP binding list is statically assigned.

To configure DHCP Static IP Mapping, Click on Network > DHCP > DHCP Static.

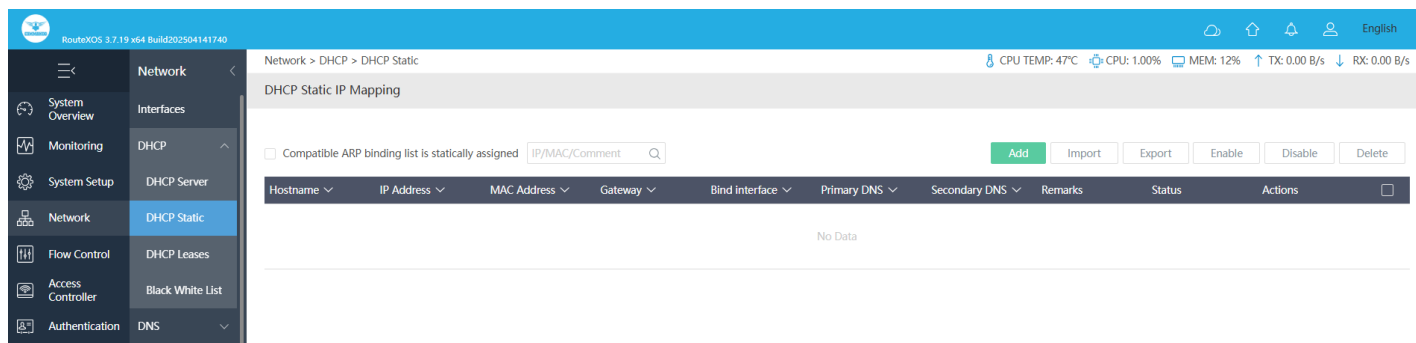


Fig 3.2.5 Default DHCP Static IP Mapping page

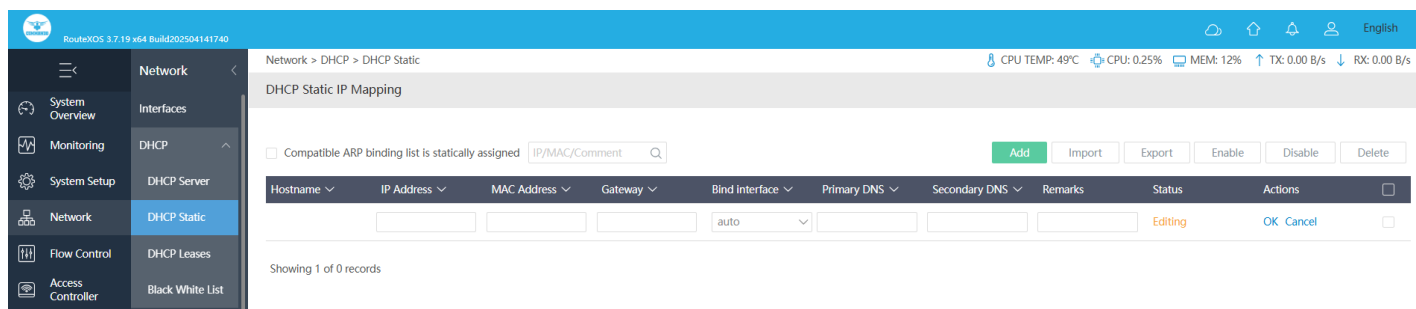


Fig 3.2.6 Default DHCP Static IP Mapping Add page

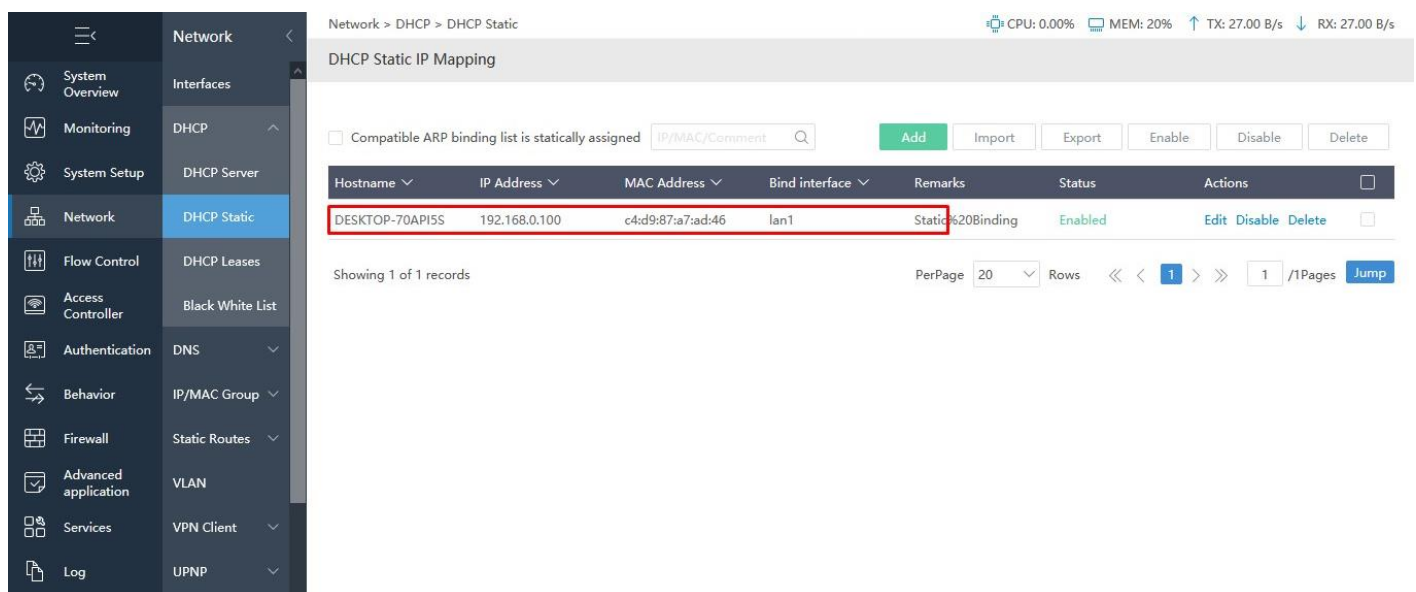


Fig 3.2.7 DHCP Static IP Mapping Add page Viewing

DHCP Leases: A DHCP lease is a temporary assignment of an IP address to a device on the network. When using DHCP to manage a pool of IP addresses, each client served on the network is only “renting” its IP address. Thus, IP addresses managed by a DHCP server are only assigned for a limited period of time. That can be viewed by administrator.

For Viewing DHCP Leases, Click on Network > DHCP > DHCP Leases

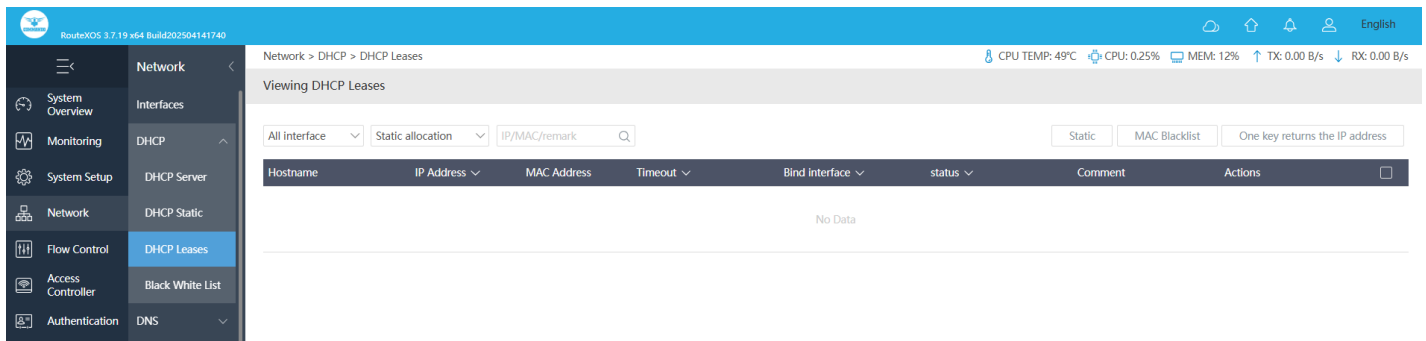


Fig 3.2.8 Default Viewing DHCP Leases page

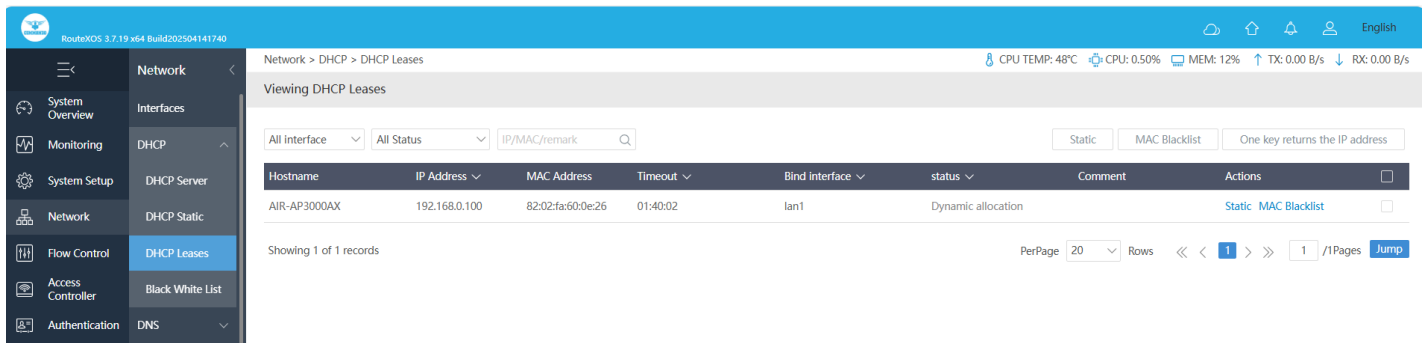


Fig 3.2.9 Viewing DHCP Leases page

Black White List: In Blacklist Mode, all MACs are forbidden to assign IP addresses. In Whitelist Mode all MACs except whitelist prohibit IP address assignment. Synchronize MAC access control (DHCP black and white list Settings are synchronized with behavior control-mac access control).

For Black White List users in network, Click on Network > DHCP > Black White List

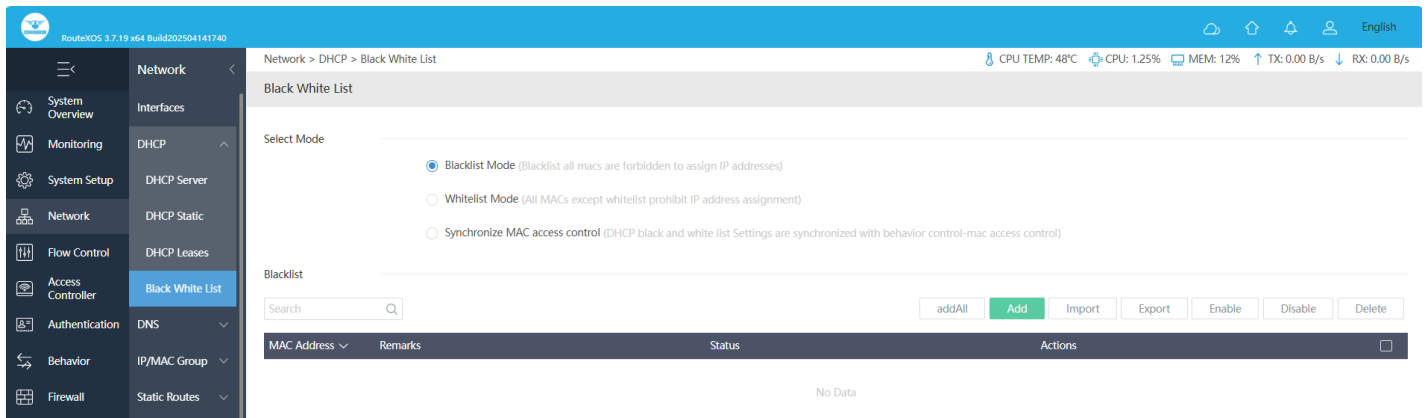


Fig 3.2.10 Default Blacklist Mode setting in device page

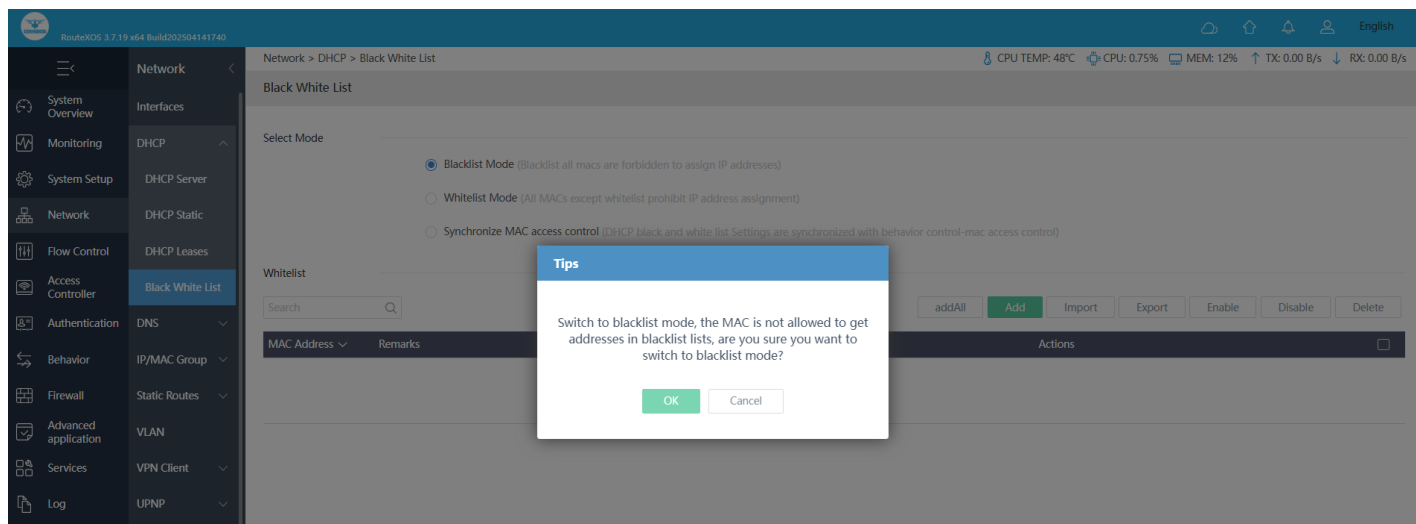


Fig 3.2.11 Blacklist Mode setting in device page

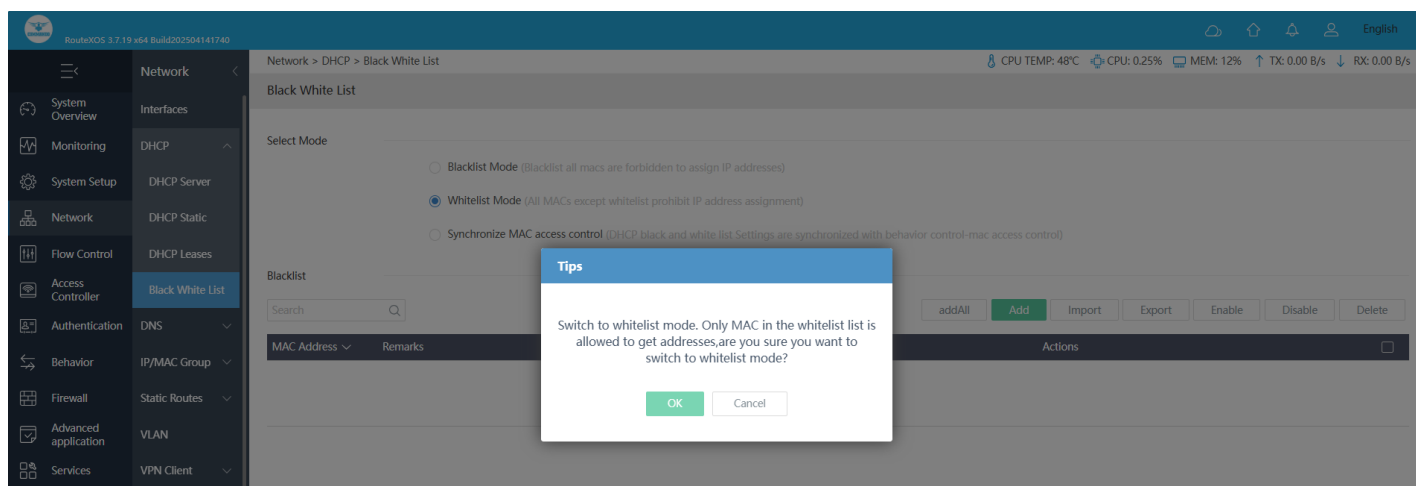


Fig 3.2.12 Changing mode to Whitelist Mode setting in device page

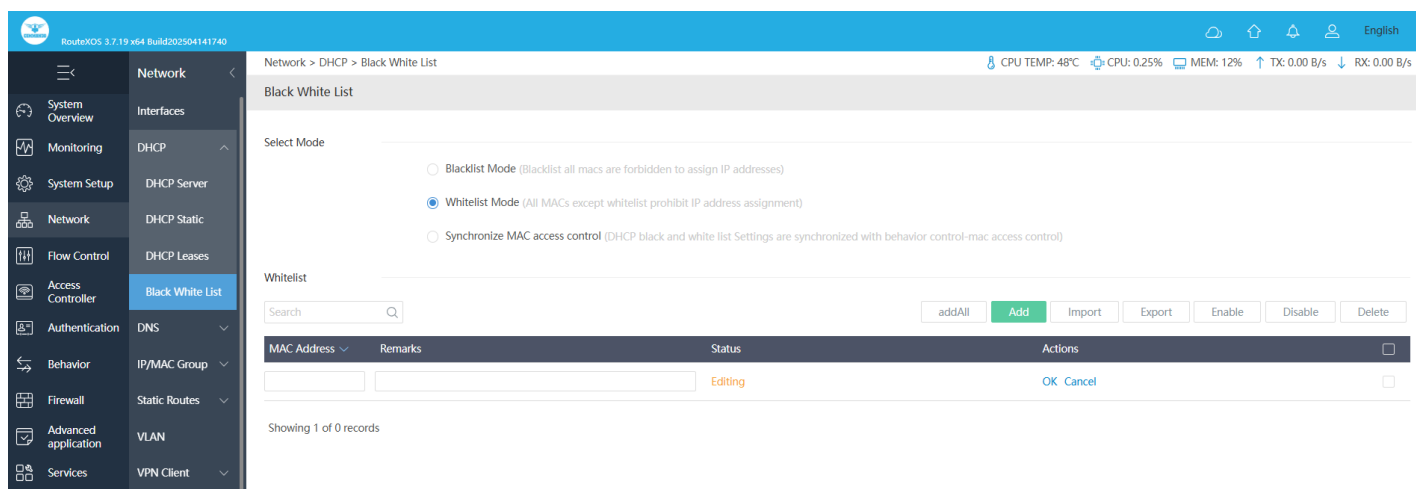


Fig 3.2.13 White list Mode setting in device page

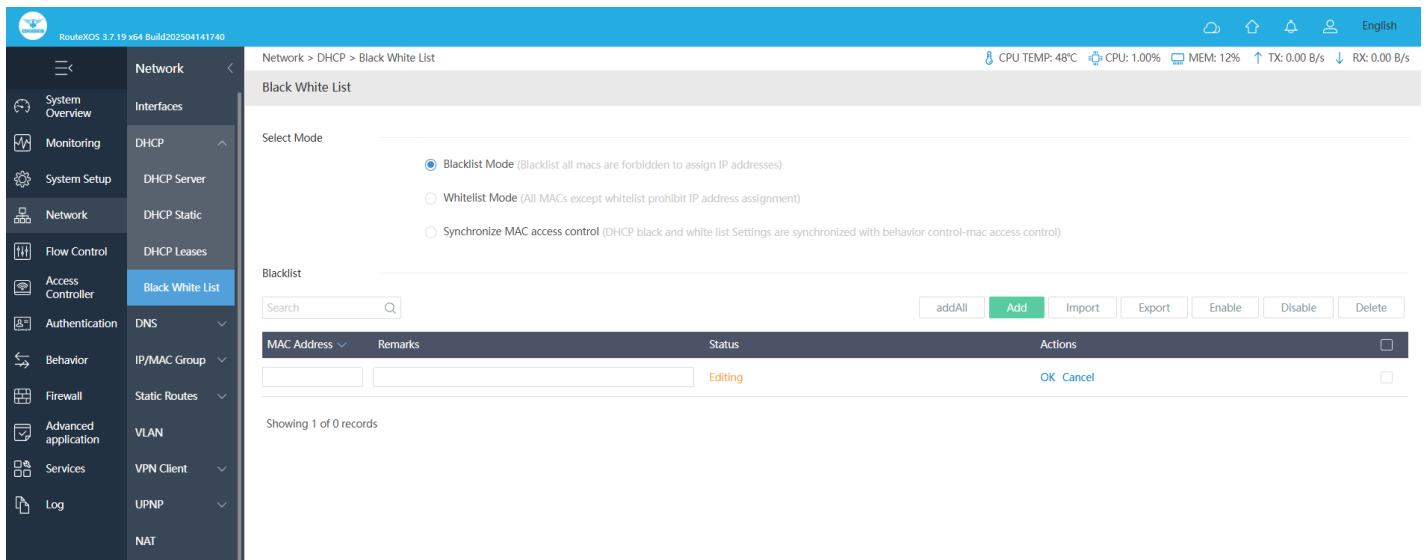


Fig 3.2.14 Blacklist mode add page

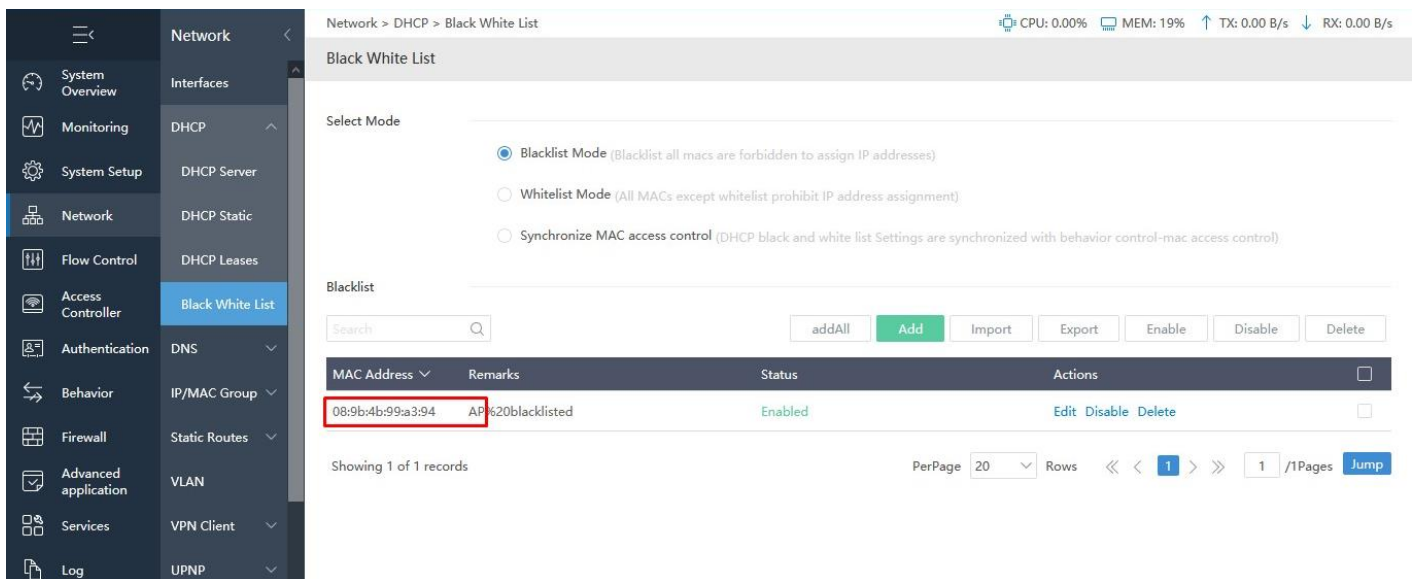


Fig 3.2.14 Blacklist mode MAC address page

So though AP connected in network, It will not get any network access after blacklisting.

3. DNS

The Domain Name System (DNS) converts domain names into IP addresses. This automatically makes any devices joining your network to use created DNS without having to go in and configure each device individually.

For DNS Settings page, Click on Network > DNS > DNS

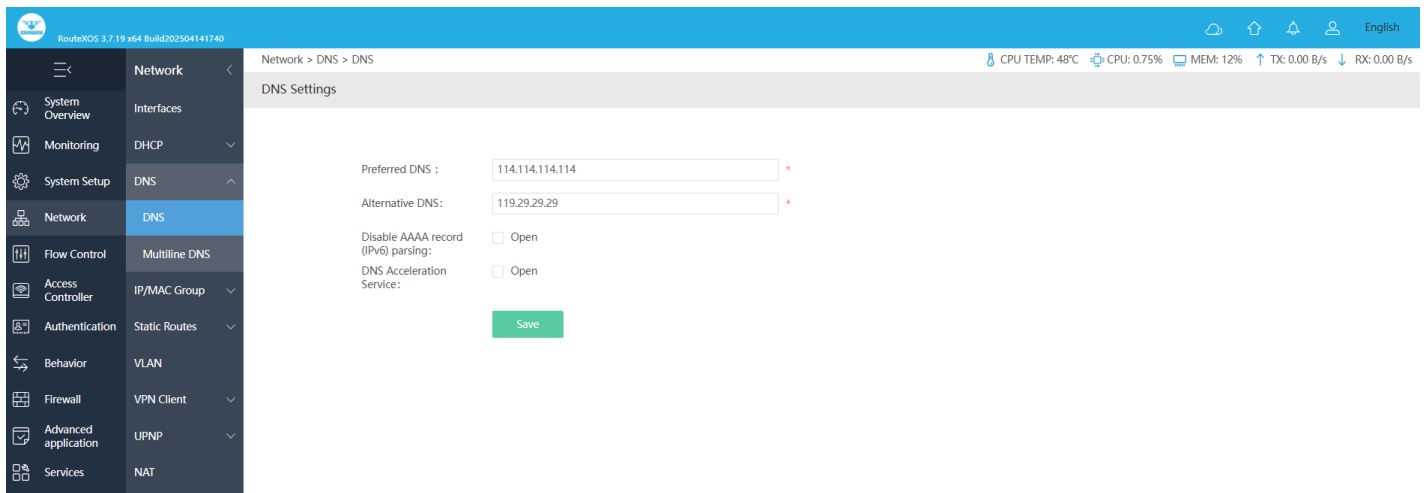


Fig 3.3.1 Default DNS Settings page

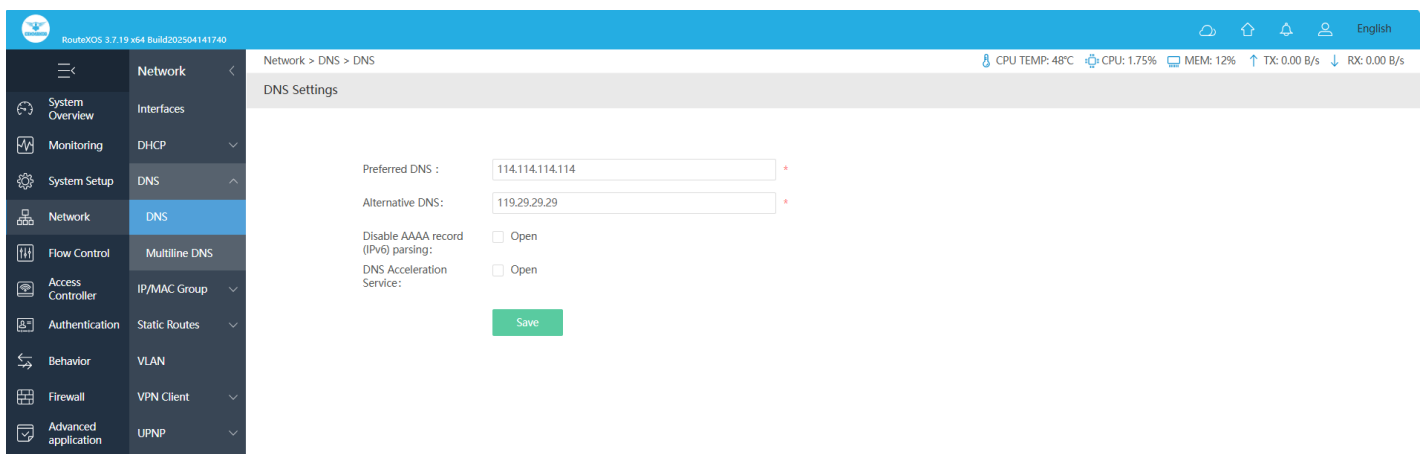


Fig 3.3.2 Default DNS Settings after opening page

When you enable DNS acceleration feature, it acts as a high-speed DNS caching name server. This feature provides DNS cache acceleration support for recursive UDP, DNS queries. DNS proxy mode is valid when the client DNS is the ramp address. DNS enforcement proxy does not verify the client DNS address, forcing the client to use the DNS proxy service. DNS cache mode is local DNS cache acceleration service.

How to change the DNS Acceleration Mode?

Click on Network > DNS > DNS then open DNS acceleration service and click on mode.

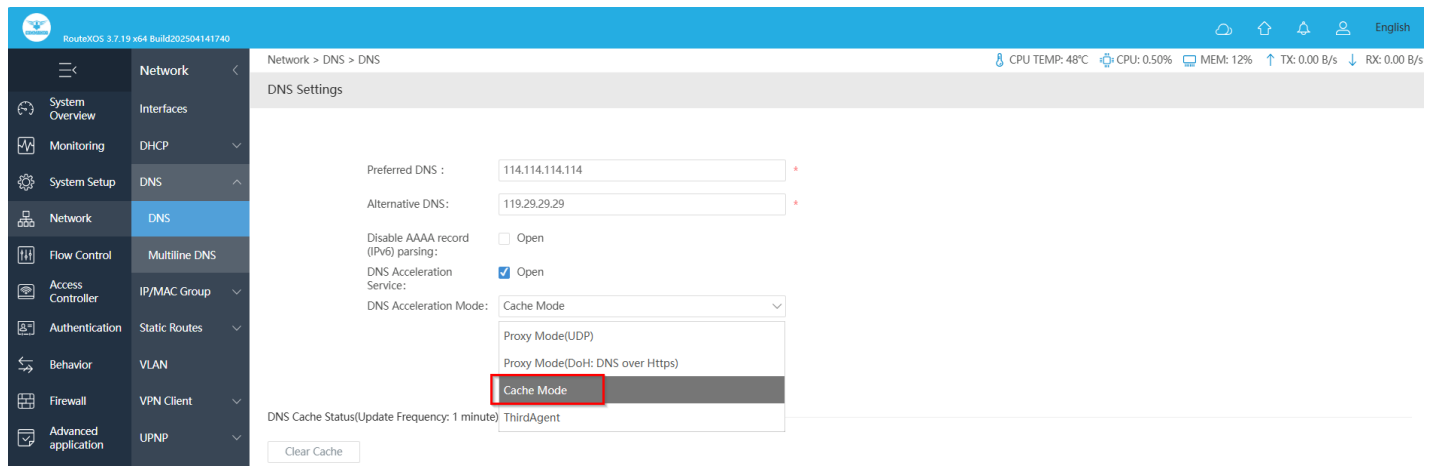


Fig 3.3.3 Changing DNS acceleration mode to cache page

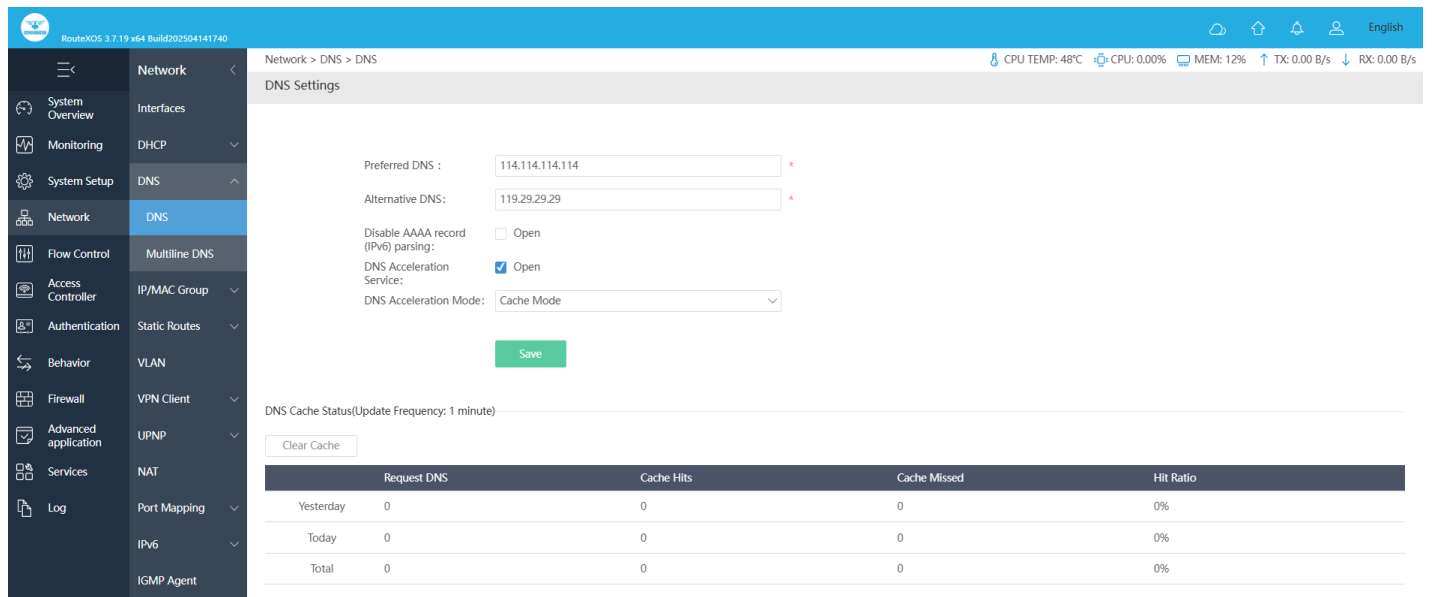


Fig 3.3.4 DNS cache status page

A DNS reverse proxy is a type of DNS proxy server that is available in private network and directs client requests to the appropriate backend DNS server. A reverse proxy provides an additional level of abstraction and control to ensure the smooth flow of network traffic between clients and DNS servers.

Network > DNS > DNS

CPU: 34.25% MEM: 18% TX: 0.00 B/s RX: 683.00 B/s

Save

DNS Cache Status

Clear Cache

	Request DNS	Cache Hits	Cache Missed	Hit Ratio	Time Saved
Yesterday	0	0	0	0%	0 ms
Today	38	1	37	2.63%	320 ms
Total	38	1	37	2.63%	320 ms

DNS Reverse Proxy

Find DNS: Add Import Export Enable Disable Delete

Domain Name	IP Address	Remarks	Status	Actions
commandonetworks.com	114.114.223.223	Reverse proxy	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1 Pages: 1 Jump

Caution: DNS proxy mode: valid when the client DNS is the ramp address;
DNS enforcement proxy: does not verify the client DNS address, forcing the client to use the DNS proxy service;
DNS cache mode: local DNS cache acceleration service

Fig 3.3.5 DNS Reverse Proxy page Multiline

DNS Settings: When multiple WAN connected to your Gateway with different DNS setting or access IP then for each WAN can create and add Multiline DNS. DNS Proxy Mode is effective when client set the gateway address as DNS. Forced DNS Proxy forces the client to use the DNS Proxy service. DNS Cache Mode is use as local DNS cache for acceleration.

For Multiline DNS Settings, Click on Network > DNS > Multiline

RouteXOS 3.7.19 x64 Build202504141740

Network > DNS > Multiline DNS

CPU TEMP: 48°C CPU: 2.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Multiline DNS Settings

Interface/DNS/Remarks: Add Import Export Enable Disable Delete

Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions
No Data					

Help Tips: When the DNS request matches the policy line, it is resolved by the DNS server specified by the rule.
When a multi-line DNS rule is set on the default gateway line, it will take effect globally (invalid when the client uses the DoH proxy function).

Fig 3.3.6 Default Multiline DNS Settings page

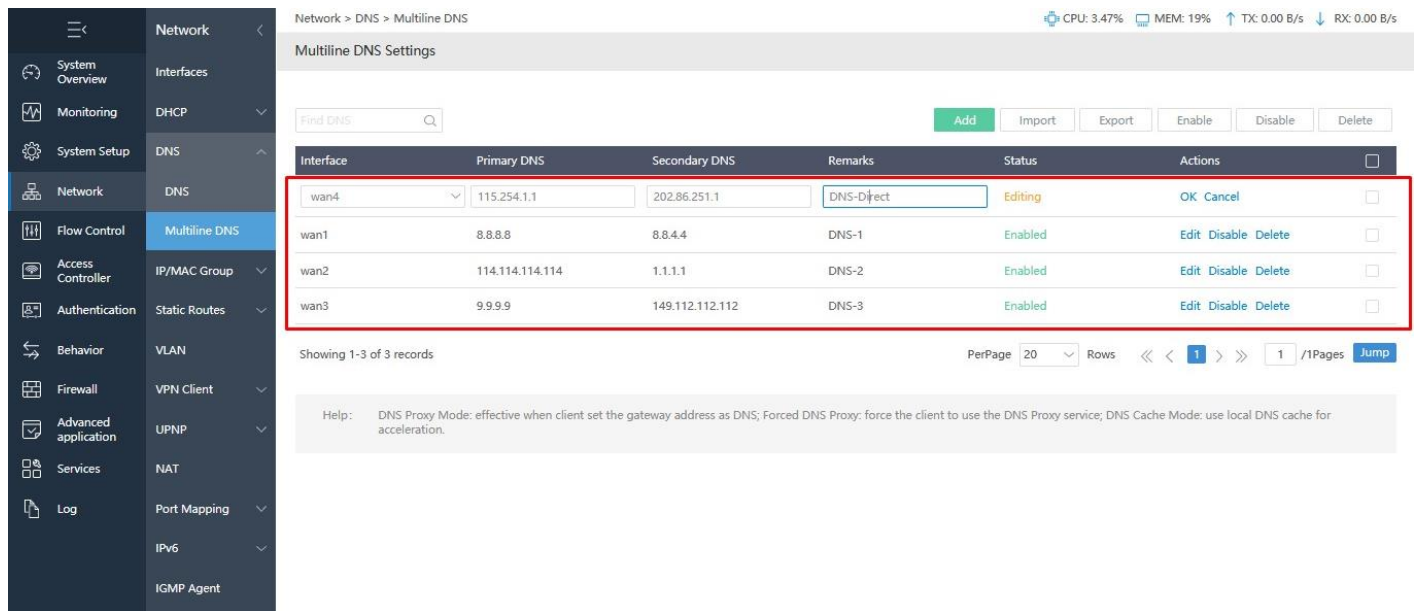


Fig 3.3.7 Multiline DNS Settings page

4. IP/MAC Group

A single IP address divides into two sections: Network ID and Host ID. The Network ID defines the logical group where devices belong. Similarly, we can define IP group which tells Gateway what groups the users are defined.

To Manage IP/MAC Address Group, Click on Network > IP/MAC Group > IP Group

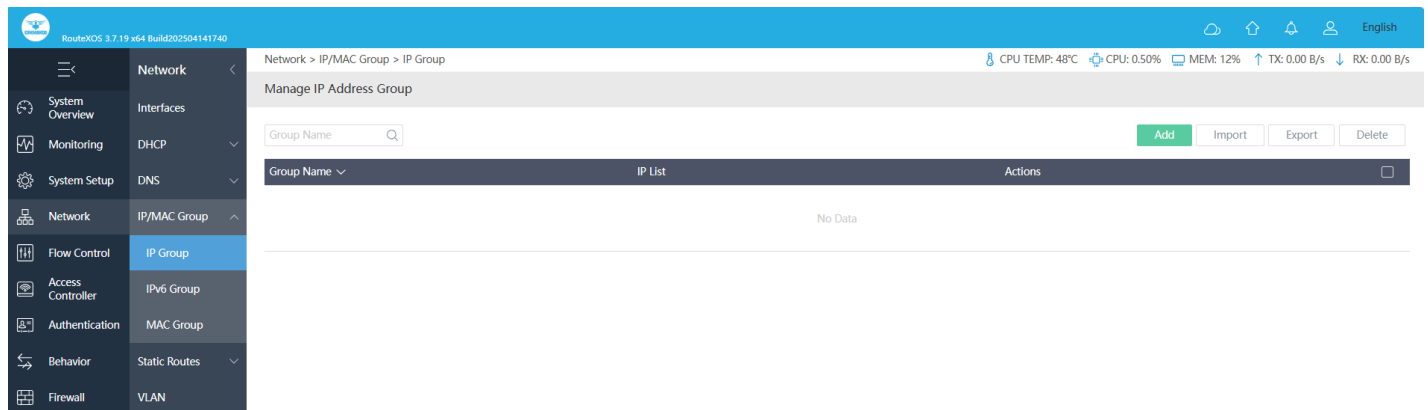


Fig 3.4.1 Manage IP Address Group page

You can add Group Name and IP List. It supports a single IP address or IP segment, and each data is switched to a different format as follows. 192.168.1.1, 192.168.1.1 Remarks1, 192.168.1.0/24 Remarks2, 192.168.1.1-192.168.1.111 Remarks3.

RouteXOS 3.7.19 x64 Build202504141740

Network > IP/MAC Group > IP Group

CPU TEMP: 48°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Group Name:

address pool: ☐ Enable (when checked, you can set the binding address pool in account management)

IP List:

Support a single IP address or IP segment, and each data is switched to a different format:
 192.168.1.1
 192.168.1.1 Remarks1
 192.168.1.0/24 Remarks2
 192.168.1.1-192.168.1.111 Remarks3

Save Cancel

Fig 3.4.2 Default Add IP Address Group page

RouteXOS 3.7.19 x64 Build202504141740

Network > IP/MAC Group > IP Group

CPU TEMP: 47°C CPU: 1.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Edit

Group Name:

address pool: ☐ Enable (when checked, you can set the binding address pool in account management)

IP List:

Support a single IP address or IP segment, and each data is switched to a different format:
 192.168.1.1
 192.168.1.1 Remarks1
 192.168.1.0/24 Remarks2
 192.168.1.1-192.168.1.111 Remarks3

Save Cancel

Fig 3.4.3 Edit IP Address Group page

RouteXOS 3.7.19 x64 Build202504141740

Network > IP/MAC Group > IP Group

CPU TEMP: 48°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Manage IP Address Group

Group Name Add Import Export Delete

Group Name	IP List	Actions
COMMANDO	192.168.0.0/24	Edit Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 >> >> 1 /1Pages Jump

Fig 3.4.4 Manage IP Address Group page

The IPv6 Group tab functions similarly to the IP Group tab used for IPv4, allowing users to define logical groups of devices based on their IPv6 addresses. Just like in the IP Group

tab, users can add a Group Name and an IP List, supporting single IPv6 addresses or address segments. This enables efficient management and organization of network resources by grouping users based on their assigned IPv6 addresses, helping Gateway determine network access rules.

The screenshot shows the 'Add' page for an IPv6 Group. The breadcrumb trail is 'Network > IP/MAC Group > IPv6 Group'. The page has a sidebar on the left with a menu where 'IPv6 Group' is selected under 'Access Controller'. The main content area has a title bar 'Add' with a close button. Below the title bar, there are two input fields: 'Group Name:' and 'IP List:'. The 'IP List' field has a red asterisk indicating it is required. Below the input fields, there is a text block explaining the format: 'Support a single IP address or IP segment, and each data is switched to a different format: 2e80:8252aa1c33ace8c9 2e80:8252aa1c33ace8c9 Remarks1 2e80:8252aa1c33ace8c9/64 Remarks2'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Fig 3.4.5 Manage IPv6 Address Group page

A single MAC address divides into two sections: Organizational unique Identifier and Network Interface Specific identifier. The MAC ID group defines the logical group where devices belong. Similarly, we can define MAC group which tells Gateway what groups the users are defined. The MAC format can be 58:FB:84:3B:74:BF (MAC ID), 58:FB:84:3B:74:BF Remarks (MAC ID Remarks).

To Manage IP/MAC Address Group, Click on Network > IP/MAC Group > MAC Group

The screenshot shows the 'Manage MAC Address Group' page. The breadcrumb trail is 'Network > IP/MAC Group > MAC Group'. The sidebar on the left has 'MAC Group' selected under 'Authentication'. The main content area has a title bar 'Manage MAC Address Group'. Below the title bar, there is a search bar for 'Group Name' and buttons for 'Add', 'Import', 'Export', and 'Delete'. Below these is a table with columns 'Group Name', 'Mac List', and 'Actions'. The table is currently empty, showing 'No Data'.

Fig 3.4.6 Default Manage MAC Address Group page

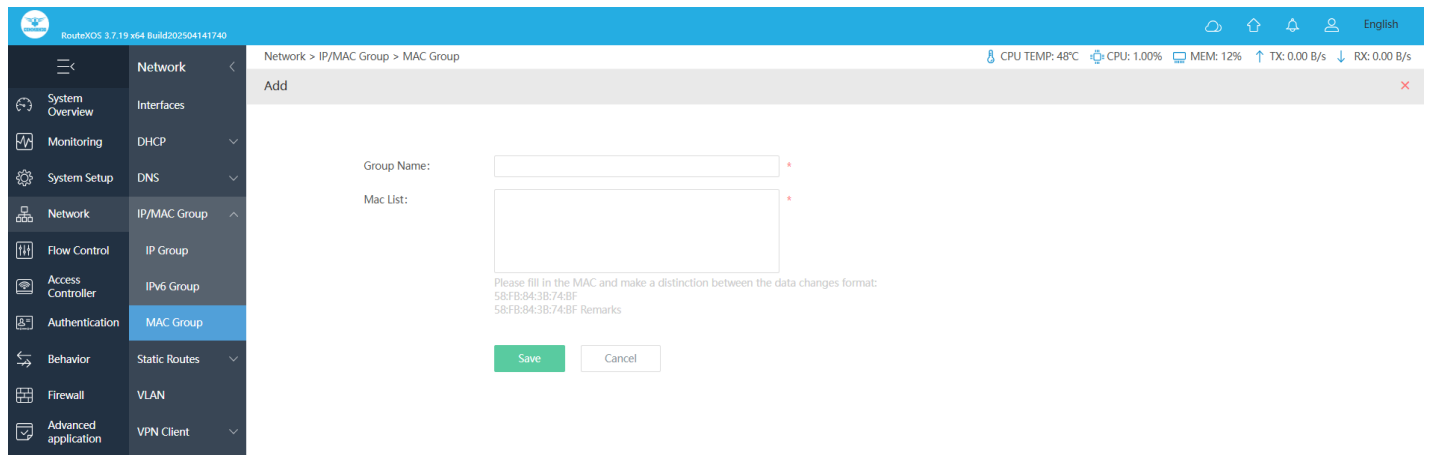


Fig 3.4.7 Add MAC Address Group page

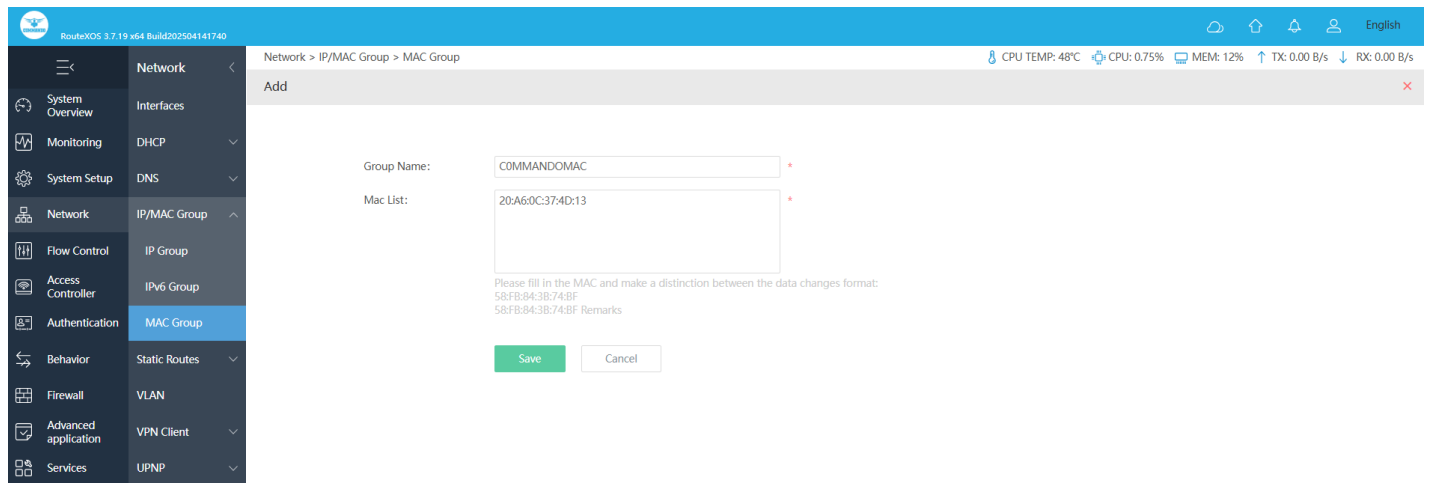


Fig 3.4.8 Adding specific MAC page

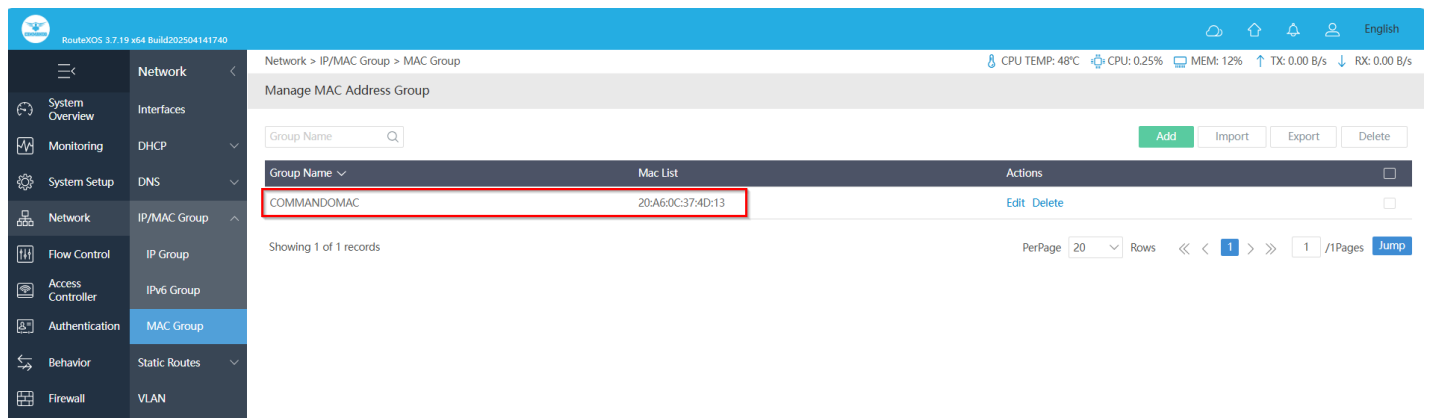


Fig 3.4.9 Manage MAC Address Group page

5. Static Routes

Routing is the process of selecting optimized paths in a network along which to send network traffic. Static Route is a kind of special routing configured by the administrator, which is simple, efficient, and reliable. Commonly used in small-sized network with fixed topology, Static Route does not change along with the network topology automatically.

The administrator should modify the static route information manually as long as the network topology or link status is changed. A static IPv4 route is a predetermine path that network information must follow to reach a specific host or network which is having the destination IPv4 address of the packets. It can be based on Next Hop IPv4 gateway address to which the packet should be sent next. User can Specify the administrative distance, which is the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1. We can also set default route which is a special type of static route, which specifies a path that the device should use if the destination address is not included in any other routes. Therefore, a default route can solve this problem: if no route to the destination is specified, the device will send the packets to a specific device, that is, the default gateway. Then the default gateway will forward the packets to the destination. A default route consists of three parts manly Destination, Subnet Mask and Next Hop (Gateway). The destination and subnet mask are both the fixed value 0.0.0.0, which means arbitrary destination IP addresses that are not matched by other route entries.

Routing table is used for a Layer 3 device to forward packets to the correct destination. When the Gateway receives packets of which the source IP address and destination IP address are in different subnets. It will check the routing table, find the correct outgoing interface then forward the packets. The routing table mainly contains two types of routing entries: Dynamic routing entries and Static routing entries.

Dynamic routing entries: Dynamic routing entries are automatically generated by the Gateway learned from connected interfaces. The Gateway uses dynamically learned route to automatically calculate the best route to forward packets.

Static routing entries: Static routing entries are manually added non-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

For adding and deleting static route, Click on Network > Static Routes > Static Routes.

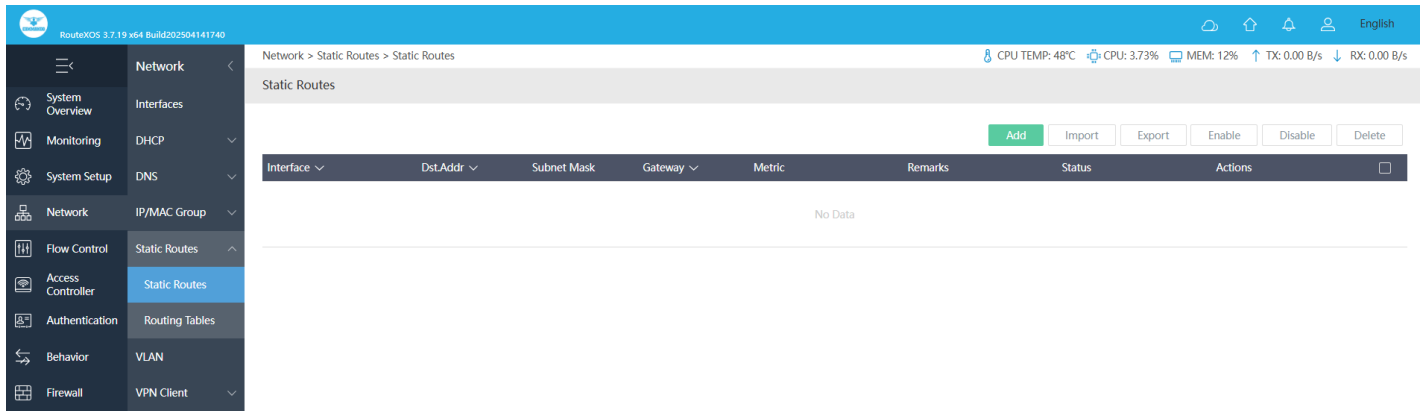


Fig 3.5.1 Default static route page

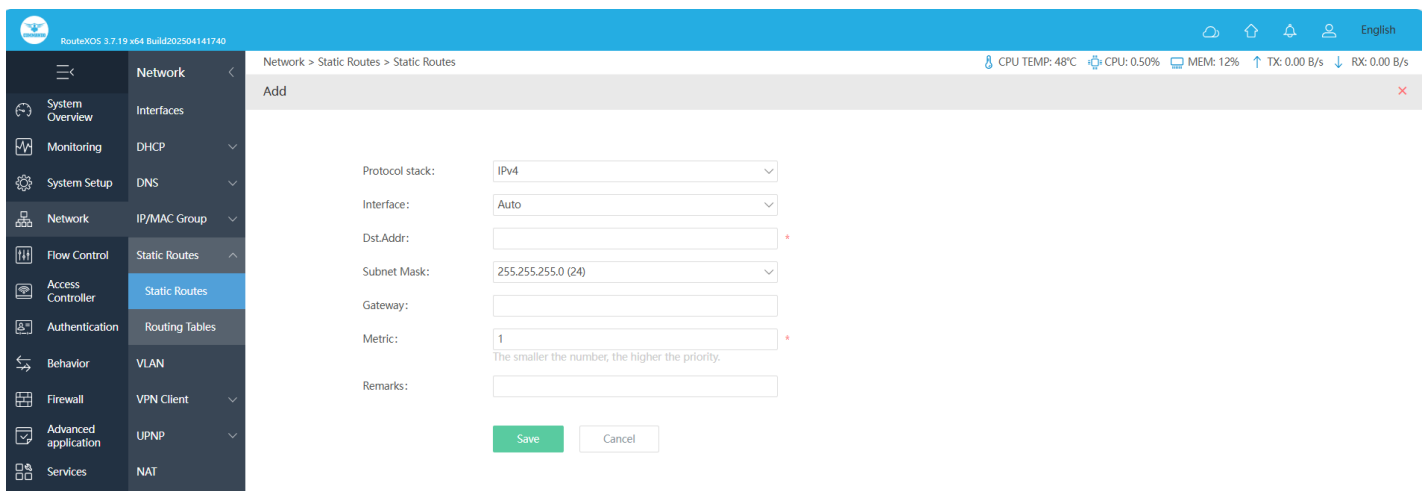


Fig 3.5.2 Default Add static route page

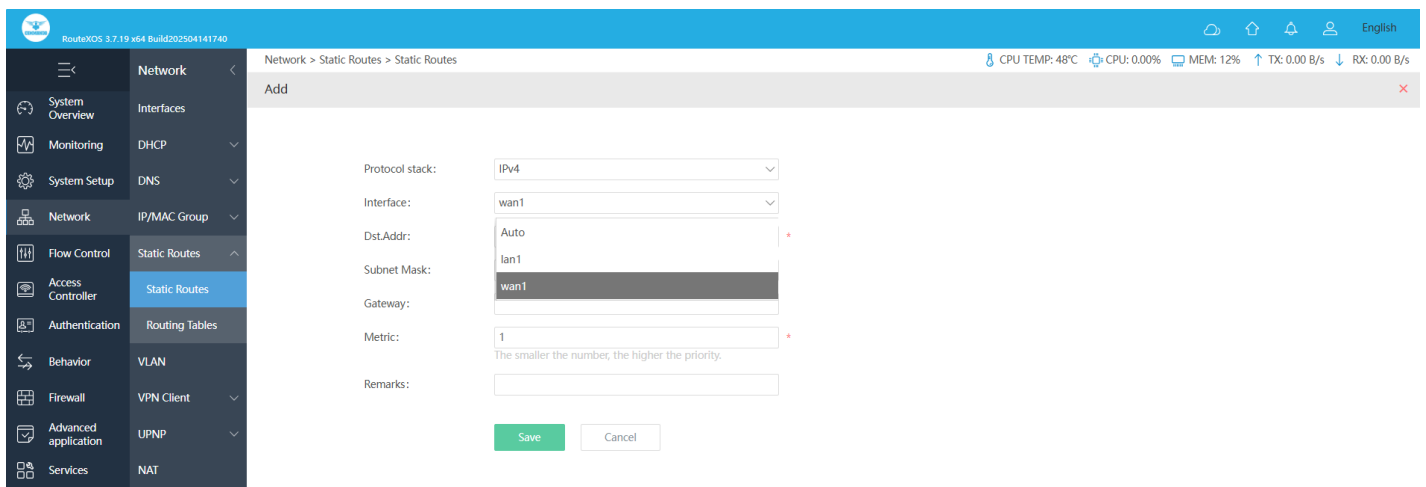


Fig 3.5.3 Selecting interface in static route page

RouterXOS 3.7.19 x64 Build202504141740

Network > Static Routes > Static Routes

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Protocol stack: IPv4

Interface: wan1

Dst.Addr: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 192.168.20.1

Metric: 2

Remarks: Airtel LAN

Save Cancel

Fig 3.5.4 Adding Default route (Gateway of last resort) page

Note: You can add multiple gateways of last resort by changing administrative distance.

RouterXOS 3.7.19 x64 Build202504141740

Network > Static Routes > Static Routes

CPU TEMP: 49°C CPU: 2.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Static Routes

Add Import Export Enable Disable Delete

Interface	Dst.Addr	Subnet Mask	Gateway	Metric	Remarks	Status	Actions
wan1	0.0.0.0	0.0.0.0	192.168.20.1	2	Airtel LAN	Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

PerPage 20 Rows 1 / 1 Pages Jump

Fig 3.5.5 Default route page

RouterXOS 3.7.19 x64 Build202504141740

Network > Static Routes > Static Routes

CPU TEMP: 49°C CPU: 0.50% MEM: 12% TX: 143.00 B/s RX: 31.00 B/s

Edit

Protocol stack: IPv4

Interface: Auto

Dst.Addr: 10.0.0.0

Subnet Mask: 255.0.0.0 (8)

Gateway: 172.10.1.1

Metric: 1

Remarks: COMMANDO Route

Save Cancel

Fig 3.5.6 Adding a Specific Static route page

Network > Static Routes > Static Routes

Static Routes

Buttons: Add, Import, Export, Enable, Disable, Delete

Interface	Dst.Addr	Subnet Mask	Gateway	Metric	Remarks	Status	Actions
wan1	0.0.0.0	0.0.0.0	192.168.20.1	2	Airtel LAN	Enabled	Edit Copy Disable Delete
Auto	10.0.0.0	255.0.0.0 (8)	172.10.1.1	1	COMMANDO Route	Enabled	Edit Copy Disable Delete

Showing 1-2 of 2 records

PerPage: 20 Rows: 1 / 1Pages: Jump

Fig 3.5.7 Specific Static route page Routing

Tables: The routing table contains network/next hop associations. These associations tell a Gateway that a particular destination can be optimally reached by sending the packet to a specific Gateway that represents the next hop on the way to the final destination.

To view routing table, Click on Network > Static Routes > Routing Tables

Network > Static Routes > Routing Tables

Viewing Routing Tables

Buttons: IPv4, IPv6

Interface	Dst.Addr	Subnet Mask	Gateway	Metric
wan1	0.0.0.0	0.0.0.0	192.168.1.1	0
wan1	0.0.0.0	0.0.0.0	192.168.1.1	1
lan1	192.168.0.0	255.255.255.0	0.0.0.0	0
wan1	192.168.1.0	255.255.255.0	0.0.0.0	0

Showing 1-4 of 4 records

PerPage: 20 Rows: 1 / 1Pages: Jump

Fig 3.5.8 Routing Tables page

6. VLAN

A VLAN (Virtual Local Area Network) allows you to divide the physical LAN into multiple logical LANs so as to control the communication among the ports. The VLAN function can prevent the broadcast storm in LANs and enhance the network security. By creating VLANs, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own.

Hosts in the same LAN communicate with one another as if they are in a LAN. However, hosts in different VLANs cannot communicate with one another directly. Therefore, broadcasting of packets are limited due to VLAN. A VLAN is simply an administratively

defined subset of ports that are in the same broadcast domain. You can create a VLANs with a unique VID (VLAN ID) with a value Integers in between 0~4090. VLAN configuration lets you assign IP/MAC on the Gateway. After you create a new VLAN ID, use interface option and Multiple IP option for setting ports for mode like Hybrid, Access, Trunk, Tunnel and also PVID in VLAN range 0-4090.

To access VLAN Settings page, Click on Network > VLAN

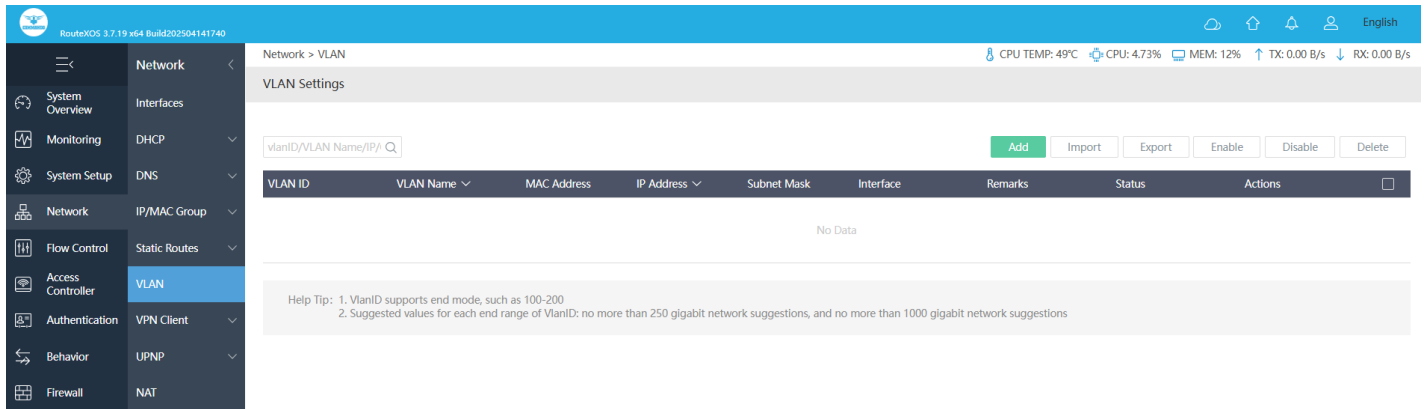


Fig 3.6.1 Default VLAN Setting page

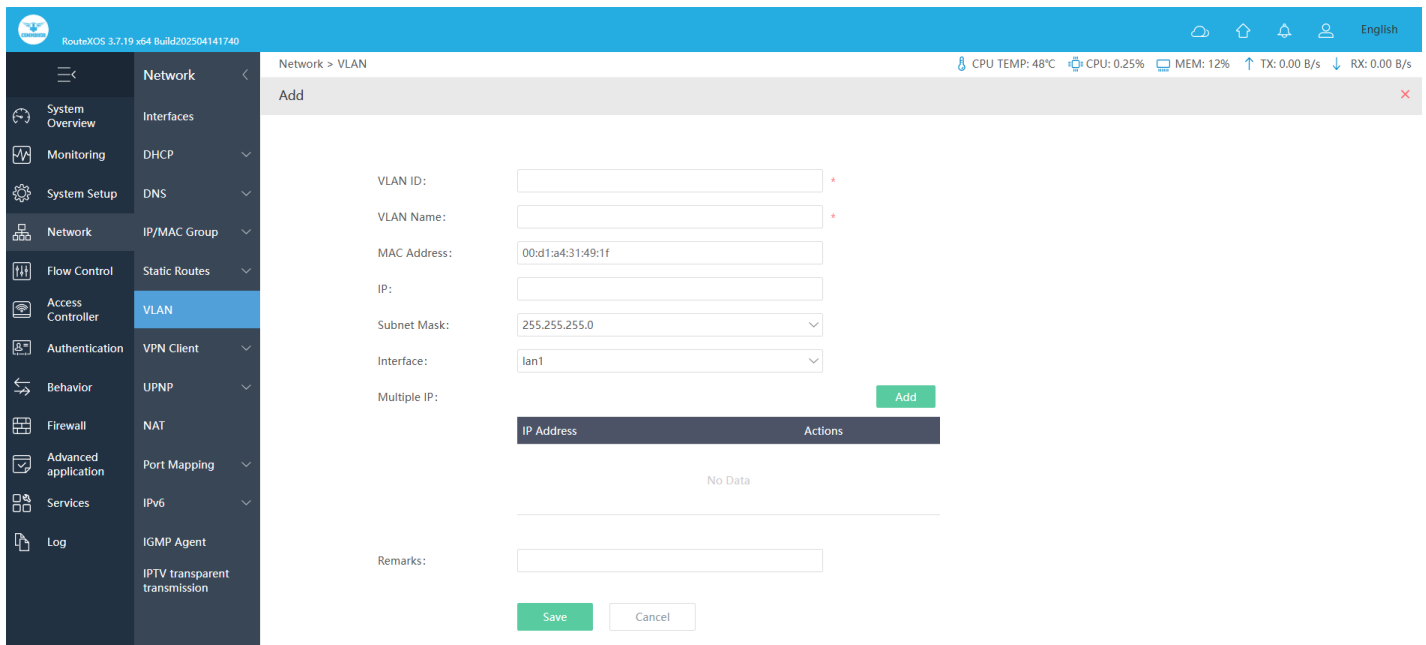


Fig 3.6.2 Add VLAN Setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VLAN

CPU TEMP: 42°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

VLAN ID: 2

VLAN Name: vlan0002

MAC Address: 00:f4:58:33:c3:a0

IP:

Subnet Mask: 255.255.255.0

Interface: lan1

Multiple IP: [Add](#)

IP Address	Actions
No Data	

Remarks:

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

Fig 3.6.3 Add VLAN2 Setting on lan1 interface page

RouteXOS 3.7.19 x64 Build202504141740

Network > VLAN

CPU TEMP: 42°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

VLAN Settings

[Add](#) [Import](#) [Export](#) [Enable](#) [Disable](#) [Delete](#)

VLAN ID	VLAN Name	MAC Address	IP Address	Subnet Mask	Interface	Remarks	Status	Actions
2	vlan0002	00:f4:58:33:c3:a0		255.255.255.0	lan1		Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage: 20 Rows: << < 1 > >>

1 / 1 Pages [Jump](#)

Help Tip: 1. VlanID supports end mode, such as 100-200
2. Suggested values for each end range of VlanID: no more than 250 gigabit network suggestions, and no more than 1000 gigabit network suggestions

Fig 3.6.4 VLAN2 Setting on lan1 interface page

Adding Multiple IP: It supports multiple IP addresses per VLAN and loopback interface. This allows the user to specify any number of secondary IP addresses. Secondary IP addresses can be used in a variety of situations like, If an insufficient number of host addresses are available on a particular network segment. Using secondary IP addresses on the Gateway or access devices allows you to have two logical subnets using one physical subnet. If the older network is built using Layer 2 bridges and has no subnetting. Secondary addresses can aid in the transition to a subnetted, Gateway-based network. Two subnets of a single

network might be otherwise separated by another network. You can create a single network from subnets that are physically separated by another network using a secondary address.

RouteXOS 3.7.19 x64 Build202504141740

Network > VLAN

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Edit

VLAN ID: 2

VLAN Name: vlan0002

MAC Address: 00:d1:a4:31:49:1f

IP:

Subnet Mask: 255.255.255.0

Interface: lan1

Multiple IP:

IP Address	Actions
192.168.10.0	255.255.255.0(24) Edit Delete

Remarks:

Save Cancel

Fig 3.6.5 Adding Multiple IP address page

7. VPN Client

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. VPNs can be divided into three main categories – remote access, intranet-based site-to-site, and extranet-based site-to-site. VPN client establishes a secure connection between the user and a VPN server.

Note:

The name must begin with the "VPN client" used and cannot exceed 15 digits

PPTP: PPTP stands for Point-to-Point Tunneling Protocol is a network protocol used to implement Virtual Private Network (VPN) tunnels between public networks. PPTP uses a control channel over Transmission Control Protocol (TCP) and a Generic Routing Encapsulation (GRE) tunnel operating to encapsulate Point-to-Point (PPP) packets. As a tunneling protocol, PPTP encapsulates network protocol datagrams within an IP envelope. PPTP was designed to allow users to connect to a VPN server from any point on the

Internet and still have the same authentication, encryption, and corporate LAN access they'd have from connecting directly into it.

To set PPTP Client Setting, click on Network>VPN Client>PPTP

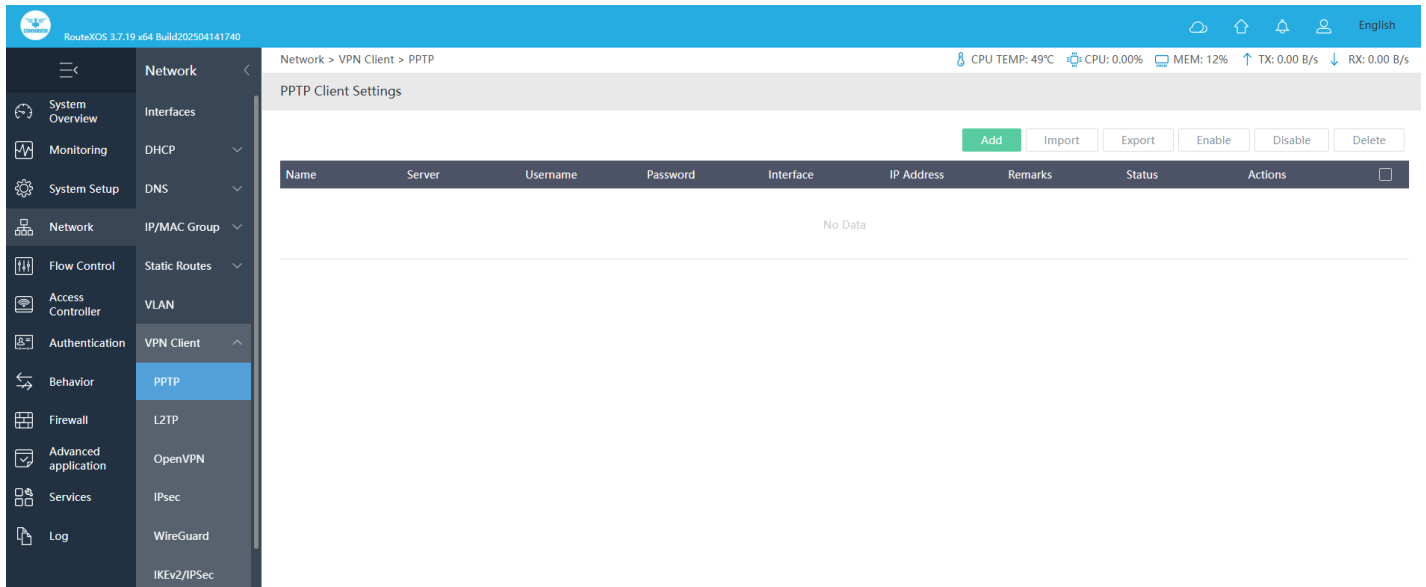


Fig 3.7.1 Default PPTP Setting page

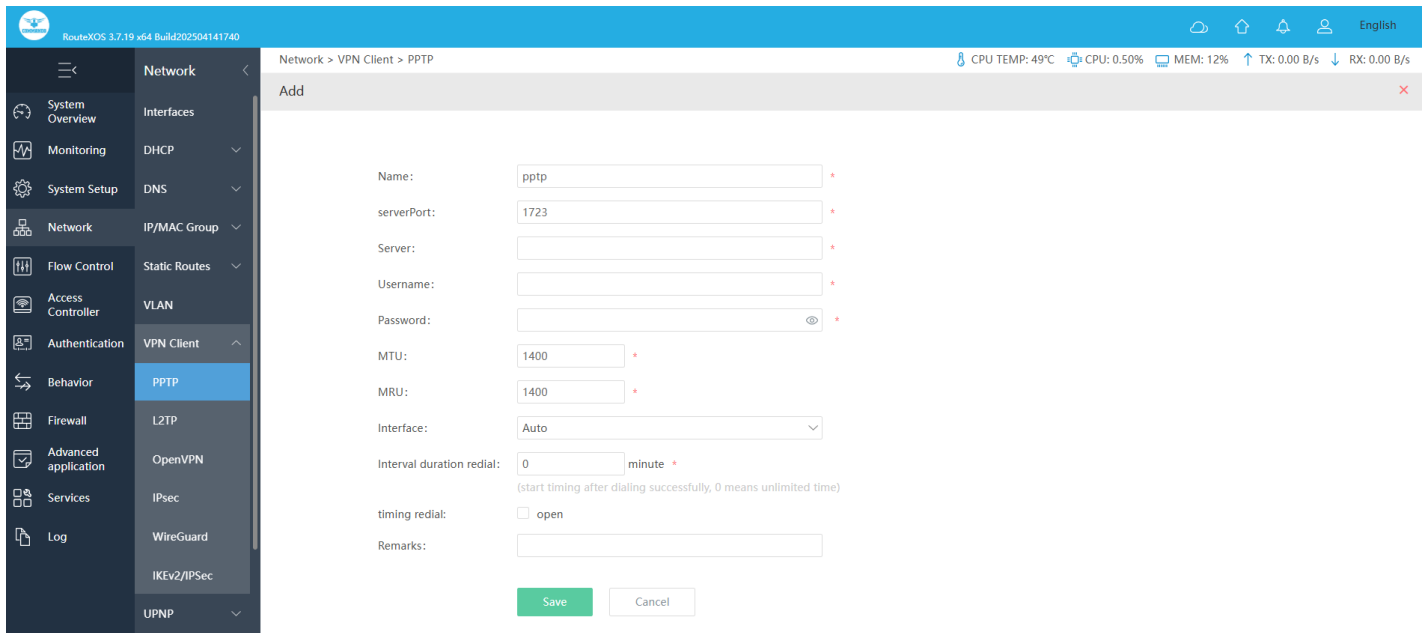


Fig 3.7.2 Add PPTP Setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > PPTP

CPU TEMP: 50°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Name: pptpCOMMANDO *

serverPort: 1723 *

Server: 10.10.10.1 *

Username: admin *

Password: ***** *

MTU: 1400 *

MRU: 1400 *

Interface: Auto

Interval duration redial: 0 minute *

(start timing after dialing successfully, 0 means unlimited time)

timing redial: ☐ open

Remarks:

Save Cancel

Fig 3.7.3 Add PPTP with username and password setting page

Note:

The name must begin with the PPTP and cannot exceed 15 digits

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > PPTP

CPU TEMP: 50°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

PPTP Client Settings

Add Import Export Enable Disable Delete

Name	Server	Username	Password	Interface	IP Address	Remarks	Status	Actions
pptpCOMMANDO	10.10.10.1	admin	*****	Auto			Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 / 1 Pages Jump

Fig 3.7.4 PPTP Client setting page L2TP

The Layer 2 Tunneling Protocol (L2TP) is a standard protocol for tunneling L2 traffic over an IP network. An L2TP-based VPN works well to allow individual clients to make single links with a remote LAN. Its ability to carry almost any L2 data format over IP or other L3 networks makes it particularly useful. PPTP (Point-to-Point Tunneling Protocol) is a lowerlevel encryption method compared to L2TP and OpenVPN.

L2TP (Layer Two Tunneling Protocol) is considered a bit more secure than PPTP as it uses 256bit keys giving a higher level of encryption. L2TP encapsulates data twice making it less efficient and slightly slower. An L2TP connection comprises two components: a tunnel and a session. The tunnel provides a reliable transport between two L2TP Control Connection Endpoints (LCCs) and carries only control packets. The session is logically contained within the tunnel and carries user data. A single tunnel may contain multiple sessions, with user data kept separate by session identifier numbers in the L2TP data encapsulation headers.

To configure L2TP Client Setting, Click on Network>VPN Client>L2TP

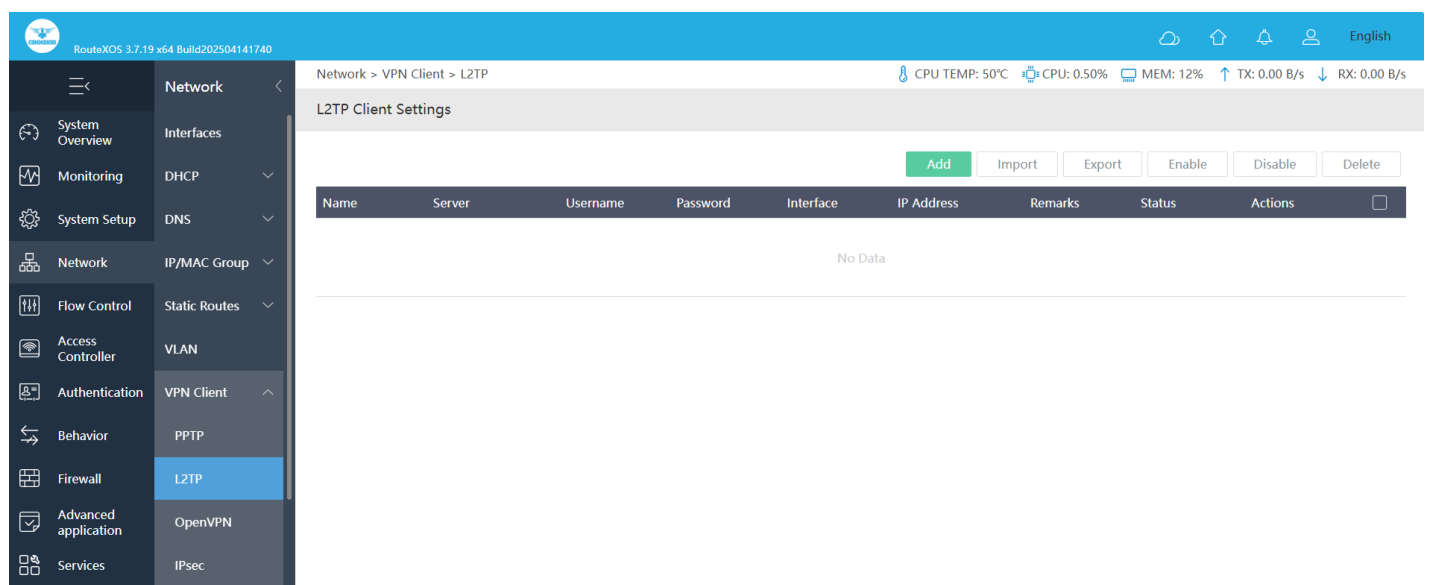


Fig 3.7.5 Default L2TP Client setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > L2TP

CPU TEMP: 50°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Name: l2tp *

serverPort: 1701 *

Server: *

Username: *

Password: *

MTU: 1400 *

MRU: 1400 *

Pre-Shared Key:

Local ID:

Peer ID:

Interface: Auto

Interval duration redial: 0 minute *

(start timing after dialing successfully, 0 means unlimited time)

timing redial: ☐ open

Remarks:

Save Cancel

Fig 3.7.6 Add L2TP Client setting page

Network > VPN Client > L2TP

CPU: 0.50% MEM: 18% TX: 194.00 B/s RX: 173.00 B/s

Add

Name: l2tpCOMMANDO *

serverPort: 1701 *

Server: 10.10.10.1 *

Username: admin123 *

Password: ***** *

MTU: 1400 *

MRU: 1400 *

Pre-Shared Key: abcdxyz

Interface:

Interval duration redial: 0 minute *

(start timing after dialing successfully, 0 means unlimited time)

timing redial: ☐ open

Save Cancel

Fig 3.7.7 L2TP Client setting with details page

Note:

The name must begin with the L2TP and cannot exceed 15 digits

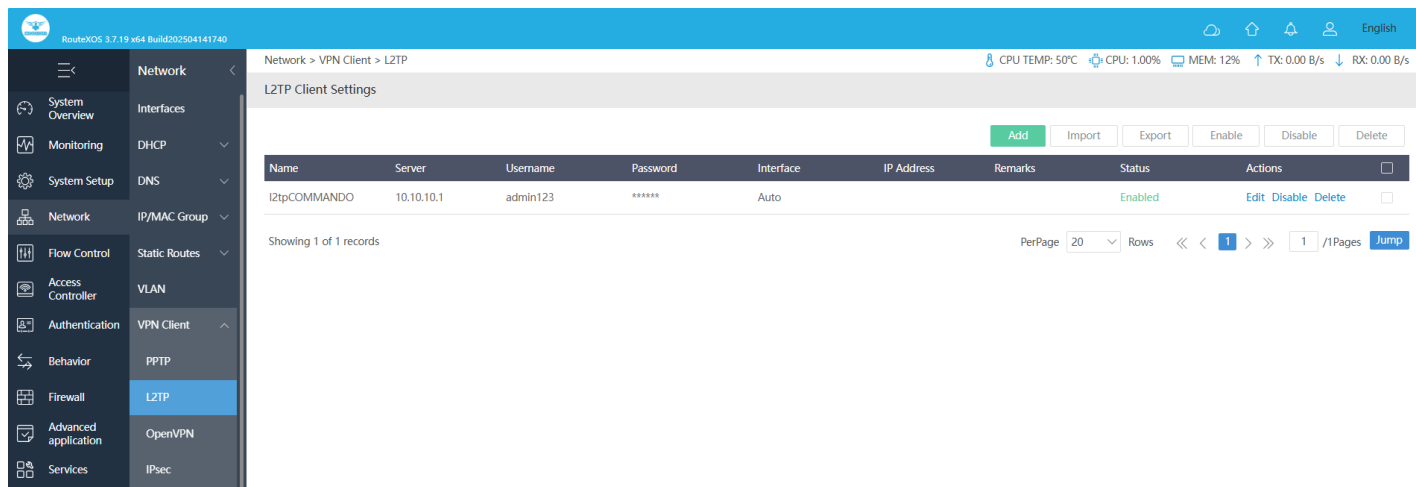


Fig 3.7.8 L2TP Client setting page

OpenVPN: OpenVPN is short for open-source VPN. A Gateway running OpenVPN in client mode, for example, facilitates users within that network to access their VPN without having to install OpenVPN on each computer on that network. A Gateway running OpenVPN in client mode, for example, allows any device on a network to access a VPN without needing the capability to install OpenVPN. OpenVPN is an open-source connection protocol used to facilitate a secure tunnel between two points in a network. OpenVPN is a trusted technology used by many virtual private networks, or VPNs, to make sure any data sent over the internet is encrypted and private.

To configure OpenVPN Client Setting, Click on Network>VPN Client>OpenVPN

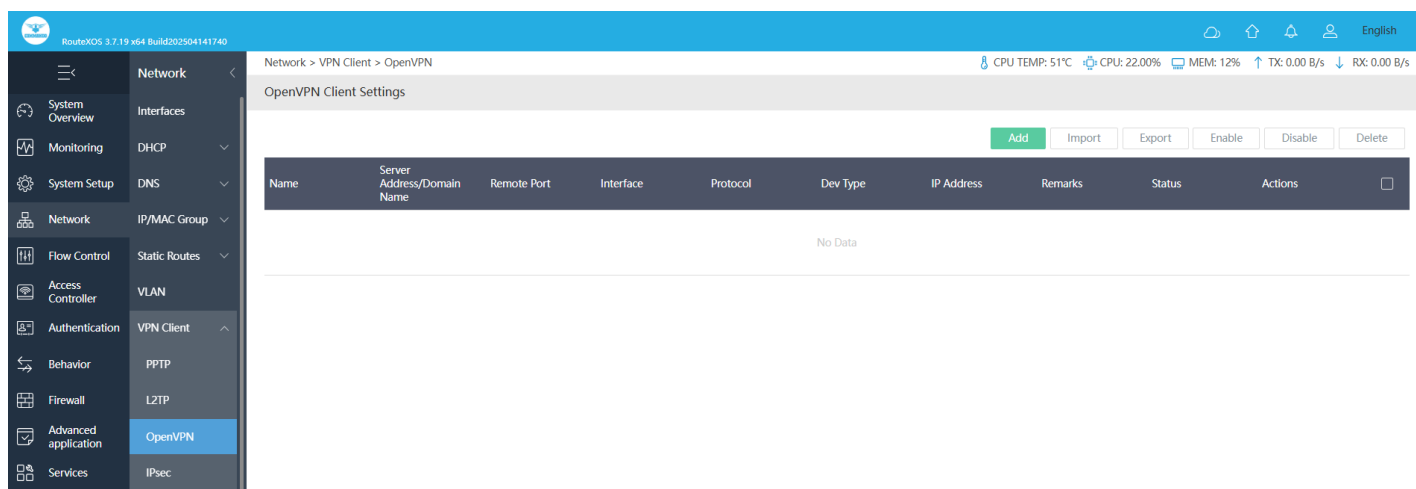


Fig 3.7.9 Default OpenVPN Client setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > OpenVPN

CPU TEMP: 50°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Name: ovpn

Server Address/Domain Name:

Remote Port: 1194

Verification Method: Account Verification

Username:

Password:

Interface: Auto

Protocol: UDP

Dev Type: TUN

Cipher: BF-CBC

Comp Lzo: ☒ Open

MTU: 1400

CA:

Fig 3.7.10 Add OpenVPN Client setting page

Note:

The name must begin with the ovpn and cannot exceed 15 digits

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > OpenVPN

CPU TEMP: 50°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Cert:

Key:

Extra Config: For example:
tcp-queue-limit 32
mtu-disc no

Accept Push Route: ☐ Open

Route: format:192.168.1.0/24

timing redial: ☐ open

Remarks:

Save Cancel

Fig 3.7.11 OpenVPN Client details setting page

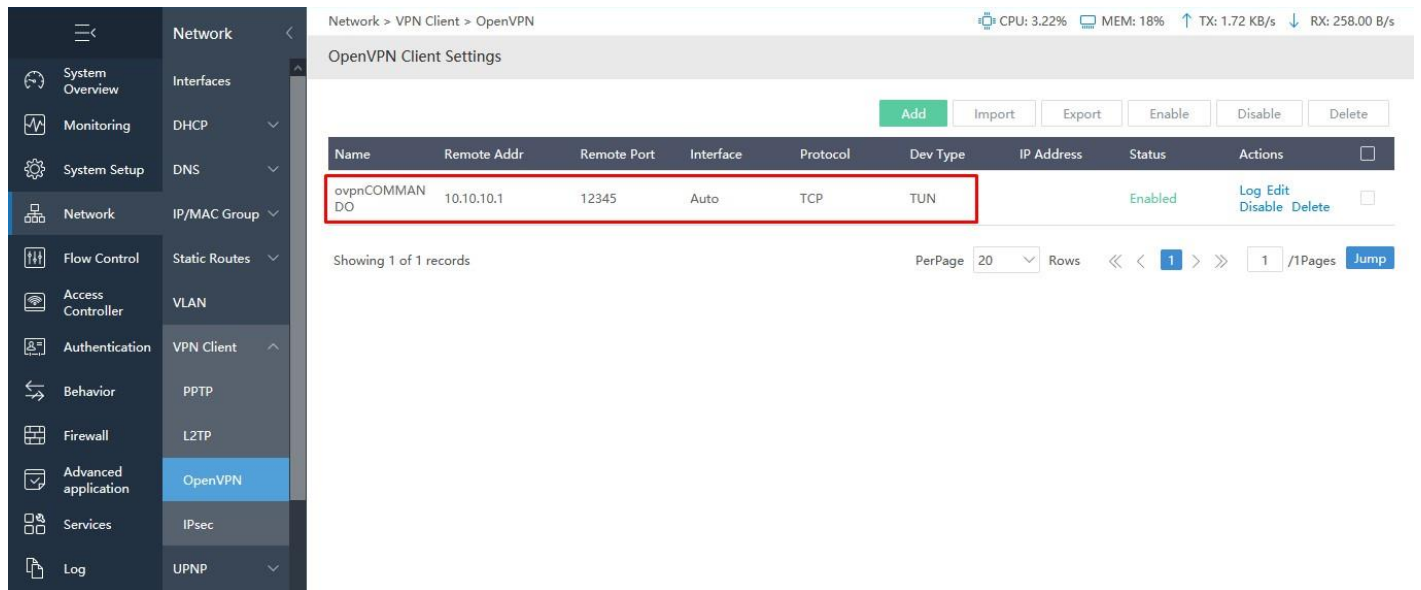


Fig 3.7.12 OpenVPN Client setting page

IPsec: Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. IPsec (IP security) is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network. IPSec VPN is one of two common VPN protocols or set of standards used to establish a VPN connection. IPsec is set at the IP layer, and it is often used to allow secure, remote access to an entire network (rather than just a single device). IPSec VPNs come in two types: tunnel mode and transport mode.

What is IPsec?

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from. Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure." The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using IP addresses. IPsec is secure because it adds encryption* and authentication to this process.

How do users connect to an IPsec VPN?

Users can access an IPsec VPN by logging into a VPN application, or "client." This typically requires the user to have installed the application on their device. VPN logins are usually password-based. While data sent over a VPN is encrypted, if user passwords are compromised, attackers can log into the VPN and steal this encrypted data. Using twofactor authentication can strengthen IPsec VPN security, since stealing a password alone will no longer give an attacker access.

What is the difference between IPsec tunnel mode and IPsec transport mode?

IPsec tunnel mode is used between two dedicated Gateways, with each Gateway acting as one end of a virtual "tunnel" through a public network. In IPsec tunnel mode, the original IP header containing the final destination of the packet is encrypted, in addition to the packet payload. To tell intermediary Gateways where to forward the packets, IPsec adds a new IP header. At each end of the tunnel, the Gateways decrypt the IP headers to deliver the packets to their destinations.

In transport mode, the payload of each packet is encrypted, but the original IP header is not. Intermediary Gateways are thus able to view the final destination of each packet — unless a separate tunneling protocol (such as GRE) is used.

To configure IPsec Setting, Click on Network>VPN Client>IPsec

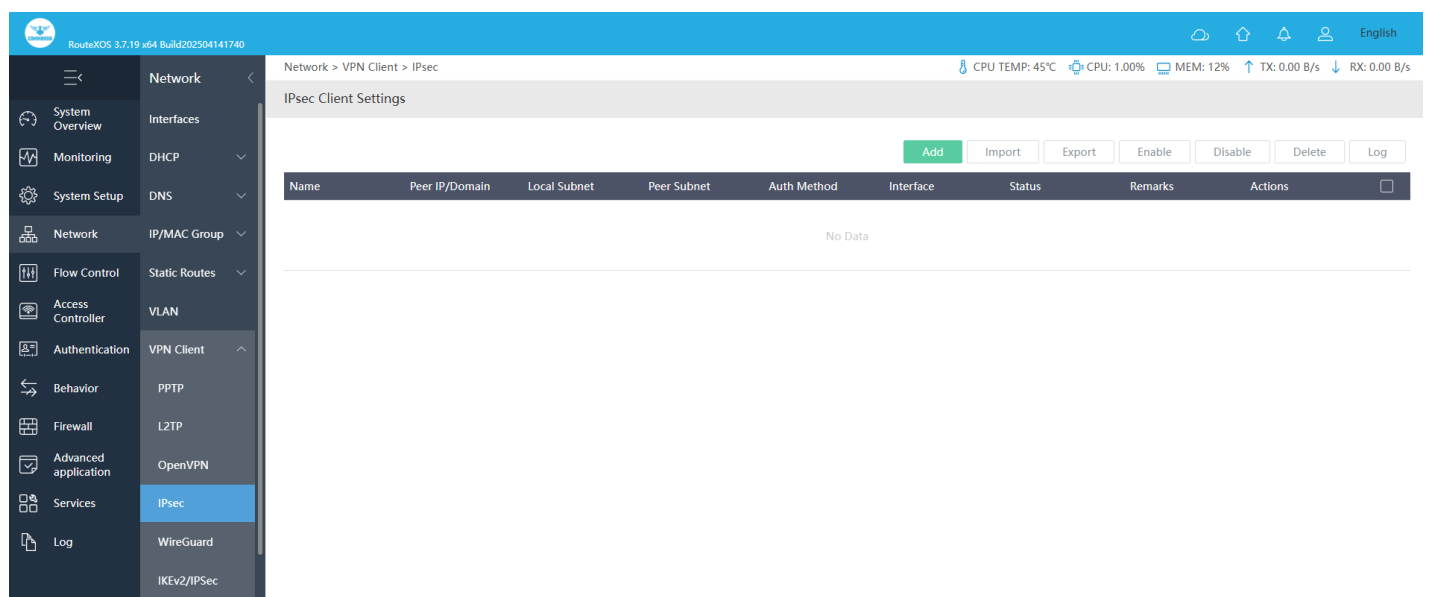


Fig 3.7.13 Default IPsec Client setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > IPsec

CPU TEMP: 45°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Name : ipsec *

Peer IP/Domain:

Local Subnet: 192.168.0.0/24 *

(Such as: 192.168.1.0/24 or 0.0.0.0/0)

Peer Subnet: 192.168.10.0/24 *

(Such as: 192.168.1.0/24)

Interface: Auto

IKE Version: IKEv2

IKE Lifetime: 3 *

(Unit: hour, range: 1~72)

IKE Proposal: Auto, Auto, Auto

Auth Method: Pre-Shared Key

Pre-Shared Key: abcxyz *

Local ID:

Peer ID:

ESP Time : 1 *

(Unit: hour, range: 1~72)

ESP Encryption : Auto

ESP Auth : Auto

Allow Compression: ☐ Allow

DPD detection: Close

Remarks:

Save Cancel

Fig 3.7.14 Add IPsec Client setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > IPsec

CPU TEMP: 46°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Name : ipsec *

Peer IP/Domain: 10.10.10.1

Local Subnet: 192.168.0.0/24 *

(Such as: 192.168.1.0/24 or 0.0.0.0/0)

Peer Subnet: 192.168.10.0/24 *

(Such as: 192.168.1.0/24)

Interface: Auto

IKE Version: IKEv2

IKE Lifetime: 3 *

(Unit: hour, range: 1~72)

IKE Proposal: Auto, Auto, Auto

Auth Method: Pre-Shared Key

Pre-Shared Key: abcxyz *

Local ID:

Peer ID:

ESP Time : 1 *

(Unit: hour, range: 1~72)

ESP Encryption : Auto

Fig 3.7.15 IPsec Client details setting page

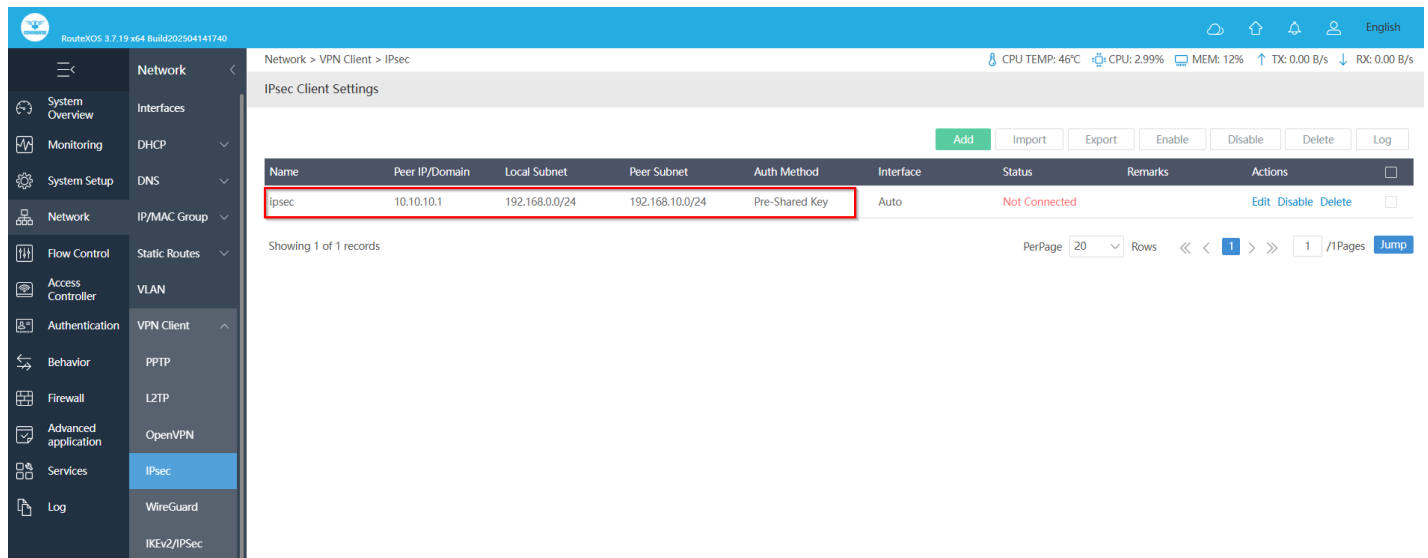


Fig 3.7.16 IPsec Client setting page

WireGuard: WireGuard is a modern, high-performance VPN protocol designed for simplicity, speed, and security. It establishes secure point-to-point connections by encrypting network traffic between devices over an Internet Protocol network. Unlike traditional VPN protocols, WireGuard is lightweight, easier to configure, and utilizes state-of-the-art cryptographic techniques to ensure data integrity, confidentiality, and authentication. It operates at the network layer and is often used for secure remote access, site-to-site connections, and privacy-focused networking.

What is WireGuard?

WireGuard is an advanced VPN protocol that provides fast, secure, and efficient encrypted communication between devices. It is designed to be simpler and more efficient than IPsec and OpenVPN, with a minimal codebase that enhances security and performance. WireGuard encrypts packets using modern cryptographic principles, ensuring secure data transmission over public and private networks. Unlike traditional VPN protocols, WireGuard establishes persistent, stateful connections between peers, making it an ideal solution for mobile devices and dynamic network environments.

How do users connect to a WireGuard VPN?

Users can connect to a WireGuard VPN by installing the WireGuard client on their device and configuring a secure connection using private and public key pairs. Instead of using complex authentication mechanisms like passwords, WireGuard relies on pre-shared

public keys for authentication. Once connected, the VPN client securely tunnels all traffic through the encrypted WireGuard connection, ensuring data privacy and protection against eavesdropping.

What is the difference between WireGuard and IPsec?

WireGuard differs from IPsec in several key ways. While IPsec uses a suite of cryptographic protocols and operates in either tunnel mode or transport mode, WireGuard simplifies encryption by using a single, modern cryptographic suite. WireGuard is designed for speed and efficiency, with lower overhead and improved performance on both high-bandwidth and low-power devices. Unlike IPsec, which requires complex configuration and key management, WireGuard provides a more streamlined setup, making it easier to deploy and maintain.

To configure WireGuard Settings, click on Network > VPN Client > WireGuard.

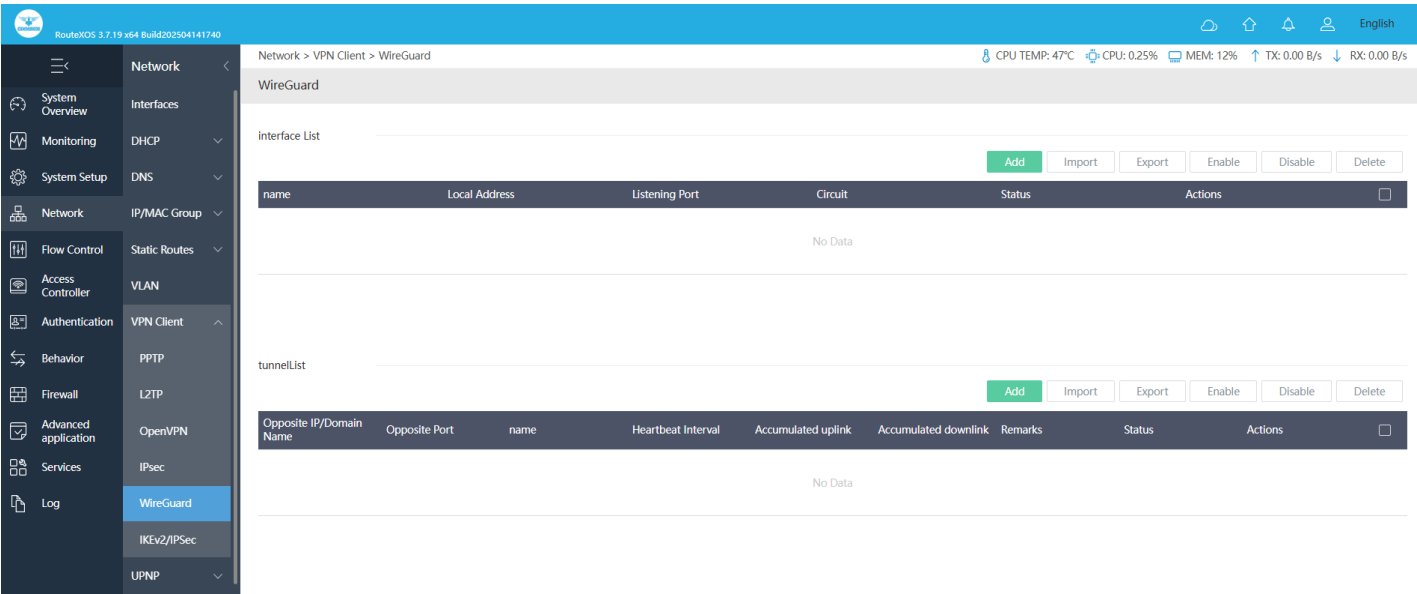


Fig 3.7.17 Default WireGuard Client setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > WireGuard

CPU TEMP: 46°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

name: wg

Local Address: 10.0.8.1/24 Format: 192.168.100.1/24

Local Private Key: X/ZT4nCU14X/H8OeO/Yl+TOW1XOeNWSR5UDMVMldUI Generate a Local Key

localprivateKey: aBZPNIE30lNeqmEd7/EuERKr+r/OgboKDj2KBroCJ1M=

Circuit: Auto

Listening Port: 50000

mtu: 1420

Save Cancel

Fig 3.7.18 Add interface List page

RouteXOS 3.7.19 x64 Build202504141740

Network > VPN Client > WireGuard

CPU TEMP: 47°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Opposite IP/Domain Name:

Opposite Port:

name: wg_1 Addname

Peer Public Key:

Pre-shared Key: Generate a Pre-shared Key

Heartbeat Interval: 10 second * 0 means off

Allow Target Network Segments: format:192.168.1.0/24

Remarks:

Save Cancel

Fig 3.7.19 Add Tunnel List page

IKEv2/IPsec: IKEv2 (Internet Key Exchange version 2) is a VPN protocol used to establish and manage secure key exchanges between devices, often in combination with IPsec for encryption and authentication. It provides a stable, secure, and efficient VPN connection, particularly suited for mobile devices due to its ability to seamlessly re-establish connections when network changes occur. IKEv2/IPsec is widely used for remote access and site-to-site VPNs, offering strong security, fast reconnection times, and support for modern cryptographic standards.

What is IKEv2/IPsec?

IKEv2 is a key management protocol that facilitates the secure exchange of cryptographic keys between VPN peers. It works alongside IPsec to create an encrypted communication channel that ensures data confidentiality, integrity, and authentication. IKEv2 is particularly known for its Mobility and Multihoming Protocol (MOBIKE) support, which allows VPN connections to persist even when switching between different networks, such as Wi-Fi and mobile data. This makes it an ideal choice for mobile users who require a stable and reliable VPN connection.

How do users connect to an IKEv2/IPsec VPN?

Users can connect to an IKEv2/IPsec VPN by installing a compatible VPN client and configuring it with the necessary connection parameters, including the VPN server address, authentication credentials, and security certificates. IKEv2 supports certificate-based authentication and pre-shared keys, ensuring a secure and efficient handshake process. Once established, the VPN tunnel encrypts all traffic between the client and server, protecting sensitive data from interception.

What is the difference between IKEv2/IPsec and other VPN protocols?

IKEv2/IPsec differs from other VPN protocols like OpenVPN and WireGuard in several ways. Compared to OpenVPN, IKEv2 is faster due to its lightweight design and built-in support in many modern operating systems. Unlike WireGuard, which uses a simpler cryptographic approach, IKEv2 provides robust key management features, making it more suitable for enterprise deployments. Additionally, IKEv2's ability to handle network changes without reconnecting gives it an edge over IPsec alone, making it the preferred choice for mobile VPN users.

To configure IKEv2/IPsec Settings, click on Network > VPN Client > IKEv2/IPsec.

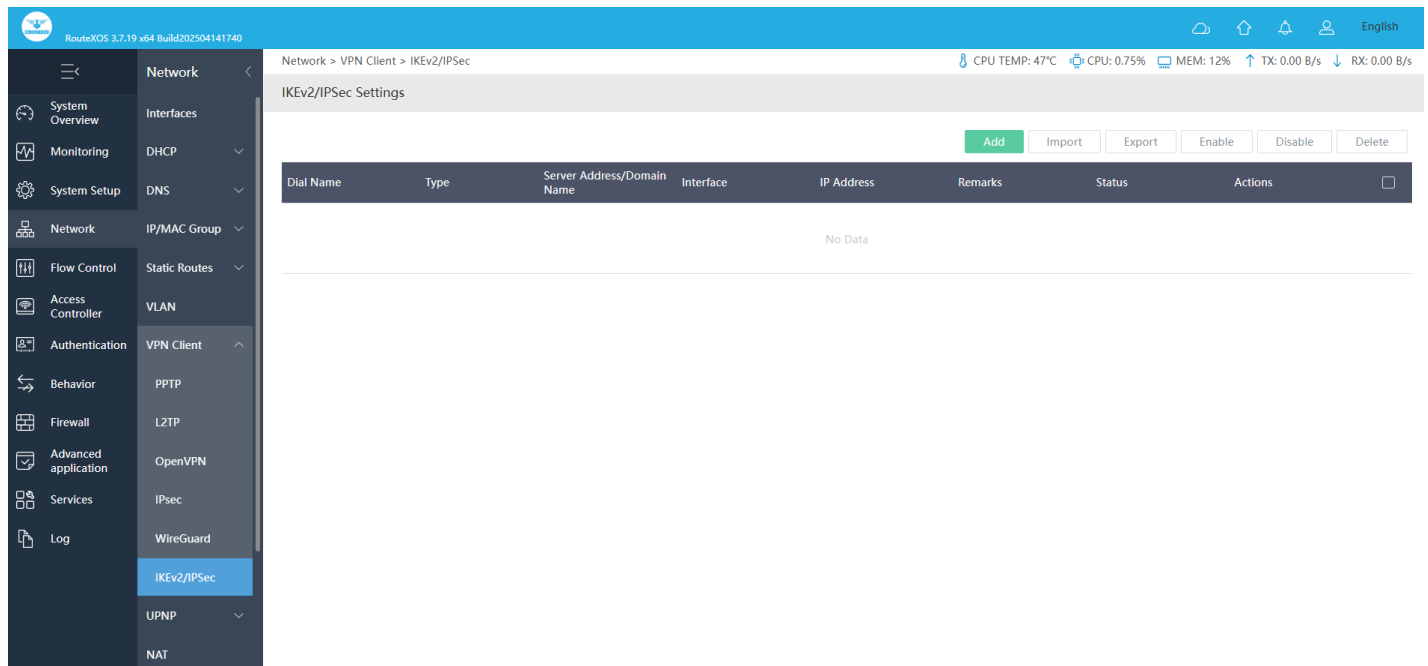


Fig 3.7.20 Default IKEv2/IPSec Settings page

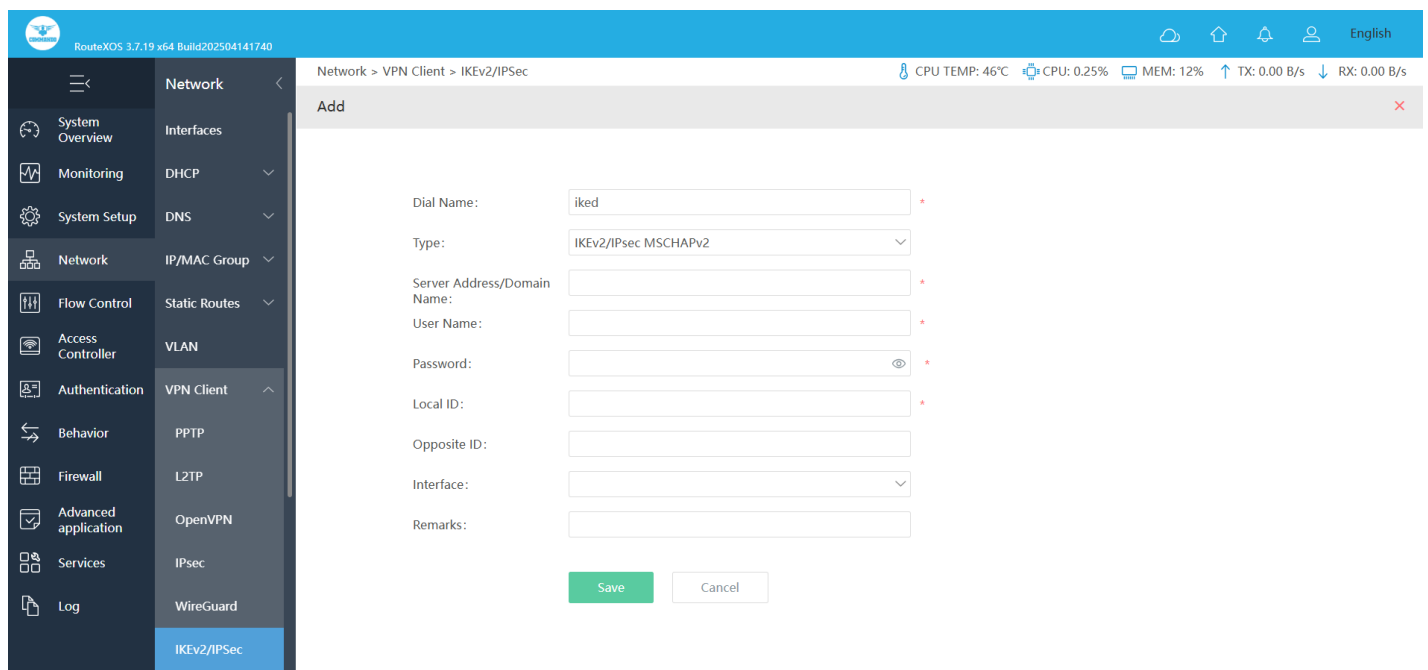


Fig 3.7.21 Add Dial settings page

3.8 UPNP

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices to seamlessly discover each other's presence on the network and establish functional network services. Devices based on UPnP (Universal Plug and Play) protocol from different manufacturer can automatically discover and communicate with one

another. Devices based on UPnP (Universal Plug and Play) protocol from different manufacturer can automatically discover and communicate with one another.

To configure UPNP Setting, Click on Network>UPNP>UPNP

RouteXOS 3.7.19 x64 Build202504141740

Network > UPNP > UPNP

CPU TEMP: 48°C CPU: 10.97% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

UPnP Settings

Upnp Server: ☐ Open

Exclude Port:
Please enter a port range, which can be separated by commas,such as: 80-100,21,200-300

Allow LAN IP Mapping:

Default Interface Settings:

Drop test: ☐ Open

Time to restart: ☐ Open Some upnp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch

[Save](#)

[Add](#) [Import](#) [Export](#) [Enable](#) [Disable](#) [Delete](#)

LAN IP	Interface	Comment	Status	Actions
No Data				

Fig 3.8.1 Default UPnP setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > UPNP > UPNP

CPU TEMP: 47°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

UPnP Settings

Upnp Server: ☒ Open

Exclude Port:
Please enter a port range, which can be separated by commas,such as: 80-100,21,200-300

Allow LAN IP Mapping:

Default Interface Settings:

Drop test: ☒ Open

Testing cycle: minute(range 1-59)

Time to restart: ☐ Open Some upnp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch

[Save](#)

[Add](#) [Import](#) [Export](#) [Enable](#) [Disable](#) [Delete](#)

LAN IP	Interface	Comment	Status	Actions
No Data				

Fig 3.8.2 Enabling UPnP setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > UPNP > UPNP

CPU TEMP: 48°C CPU: 2.49% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

LAN IP: Use *-.* for IP range 192.168.0.1

Join >> << Remove

No Group Add Group
Once configured, please Refresh

Interface: wan1

Remarks: UPNP_COMMANDO

Save Cancel

Fig 3.8.3 Add UPnP setting page

RouteXOS 3.7.19 x64 Build202504141740

Network > UPNP > UPNP

CPU TEMP: 47°C CPU: 2.74% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

UPnP Settings

Upnp Server: ☒ Open

Exclude Port: 1-1024
Please enter a port range, which can be separated by commas,such as: 80-100,21,200-300

Allow LAN IP Mapping: 0.0.0.0-255.255.255.255

Default Interface Settings: Any

Drop test: ☒ Open

Testing cycle: 5 minute(range 1-59)

Time to restart: ☐ Open Some upnp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch

Save

Add Import Export Enable Disable Delete

LAN IP	Interface	Comment	Status	Actions
192.168.0.1	wan1	UPNP_COMMANDO	Enabled	Edit Disable Delete

Fig 3.8.4 UPnP setting page UPNP

Status: Conceptually, UPnP extends plug and play—a technology for dynamically attaching devices directly to Gateway for zero-configuration networking. UPnP devices are "plug and play" in that, when connected to a network, they automatically establish working configurations with other devices. Once a device has established an IP address, the next step in UPnP networking is discovery. The UPnP discovery protocol is known as the Simple Service Discovery Protocol (SSDP). When a device is added to the network,

SSDP allows that device to advertise its services to control points on the network. This is achieved by sending SSDP alive messages. When a control point is added to the network, SSDP allows that control point to actively search for devices of interest on the network or listen passively to the SSDP alive messages of device. The fundamental exchange is a discovery message or status containing a few essential specifics about the device or one of its services, for example, its type, identifier, and a pointer (network location) to more detailed information.

To configure UPNP Setting, Click on Network>UPNP>UPNP Status

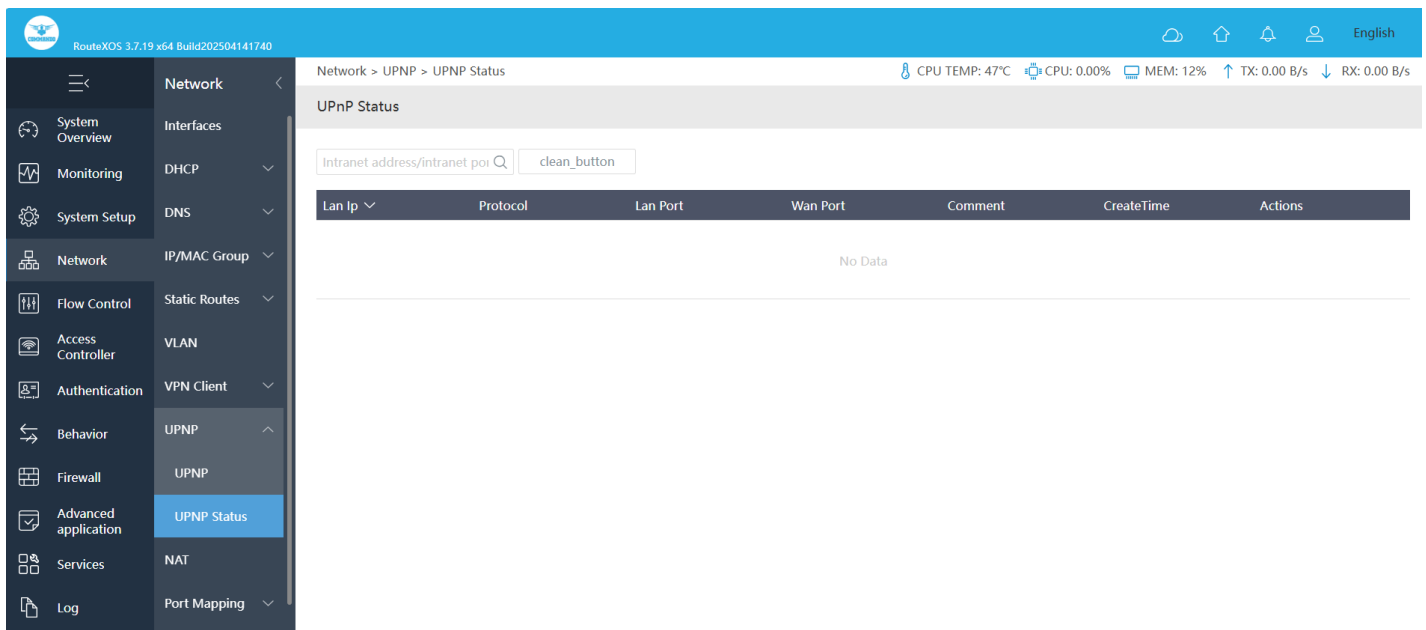


Fig 3.8.5 UPnP Status page

3.9 NAT

NAT (Network Address Translation) is the translation between private IP and public IP, which allows private network users to visit the public network using private IP addresses. With the explosion of the Internet, the number of available IP addresses is not enough. NAT provides a way to allow multiple private hosts to access the public network with one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security of the network since the address of LAN host never appears on the Internet.

It translates the IP address in an IP datagram header to another IP address, allowing users on private networks to access public networks. Basic NAT implements one-to-one translation between one private IP address and one public IP address, whereas Network

Address and Port Translation (NAPT) implements one-to-many translation between one public IP address and multiple private IP addresses. The Exhaustion of IPv4 addresses has become a bottleneck for the network development. IPv6 can solve the problem of IPv4 address shortage, but numerous network devices and applications are based on IPv4.

Major transitional technologies such as classless inter-domain routing (CIDR) and private network addresses are used before the wide use of IPv6 addresses. NAT enables users on private networks to access public networks. When a host on a private network accesses a public network, NAT translates the host's private IP address to a public IP address. Multiple hosts on a private network can share one public IP address. This implements network communication while saving public IP addresses. In addition to one-to-one address translation, NAPT allows multiple private IP addresses to be mapped to the same public IP address. It is also called many-to-one address translation or address reuse.

NAPT translates the IP address and port number of a packet so that multiple users on a private network can use the same public IP address to access the public network. Static NAT/NAPT

Static NAT indicates that a private IP address is statically bound to a public IP address when NAT is performed. Only this private IP address can be translated to this public IP address.

Static NAPT indicates that the combination of a private IP address, protocol number, and port number is statically bound to the combination of a public IP address, protocol number, and port number. Multiple private IP addresses can be translated to the same public IP address.

Static NAT/NAPT can also translate host IP addresses in the specified private address range to host IP addresses in the specified public address range. When an internal host accesses the external network, static NAT or NAPT translates the IP address of the internal host to a public address if the IP address of the internal host is in the specified address range. An external host can directly access an internal host if the private IP address translated from the IP address of the external host is in the specified internal address range.

NAT ALG

NAT and NATPT can translate only IP addresses in IP datagram headers and port numbers in TCP/UDP headers. For some special protocols such as FTP, IP addresses or port numbers may be contained in the Data field of the protocol packets. Therefore, NAT cannot translate the IP addresses or port numbers. A good way to solve the NAT issue for these special protocols is to use the Application Level Gateway (ALG) function.

As a special translation agent for application protocols, the ALG interacts with the NAT device to establish states. It uses NAT state information to change the specific data in the Data field of IP datagrams and complete other necessary work, so that application protocols can run across private and public networks. NAT allows hosts on private networks to access public networks, hosts in different virtual private networks (VPNs) on a private network to access a public network through the same outbound interface, and hosts with the same IP address in different VPNs to access a public network simultaneously. The NAT also supports NAT server associated with VPNs. It allows a host on a public network to access hosts in different VPNs on a private network, and a host on a public network to access hosts with the IP address in different VPNs on a private network. After NAT mapping is enabled on a public network, it seems that all flows from a private network come from the same IP address because hosts on the private network share the same public IP address. When a host on the private network initiates a session request to a host on the public network, the NAT device searches the NAT translation table for the related session record. If the NAT device finds the session record, it translates the private IP address and port number and forwards the request. If the NAT device does not find the session record, it translates the private IP address and port number and meanwhile adds a session record to the NAT translation table. NAT mapping includes the following modes:

Endpoint-independent mapping: The NAT uses the same IP address and port mapping for packets sent from the same private IP address and port to any public IP address and port.

Endpoint and port-dependent mapping: The NAT uses the same port mapping for packets sent from the same private IP address and port to the same public IP address and port if the mapping is still active.

To configure Network Address Translation, Click on Network > NAT

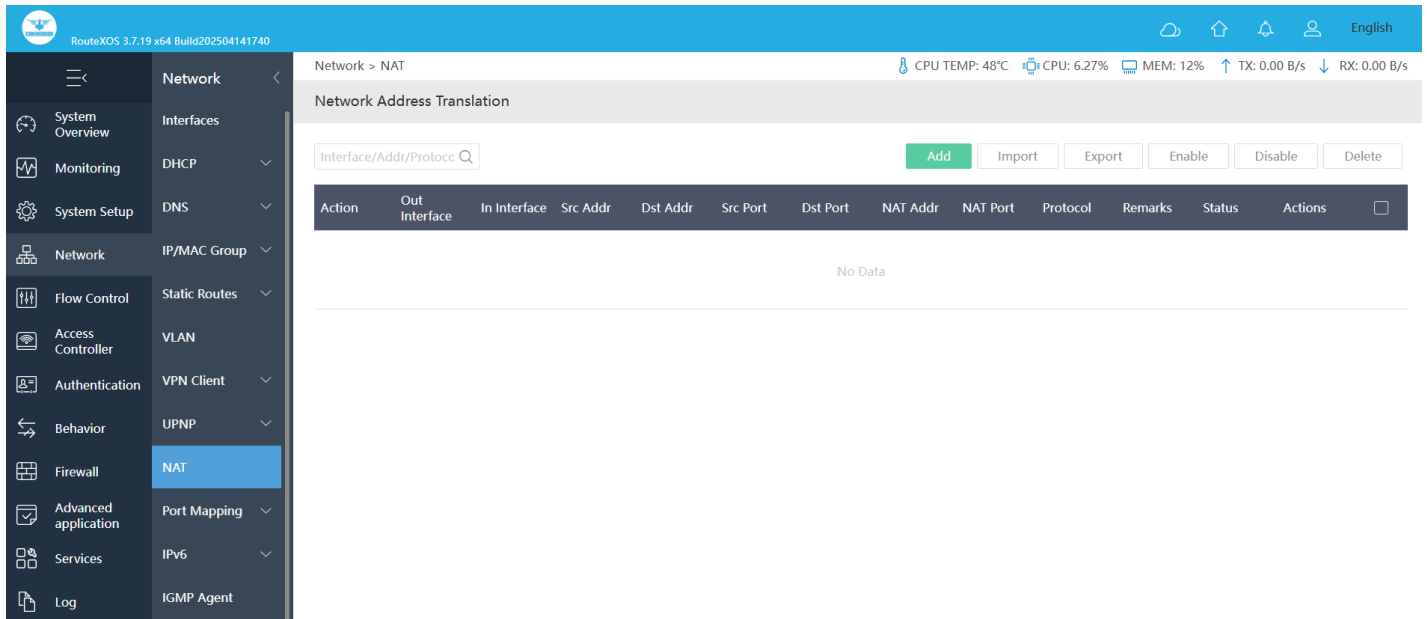


Fig 3.9.1 Default Network Address Translation page

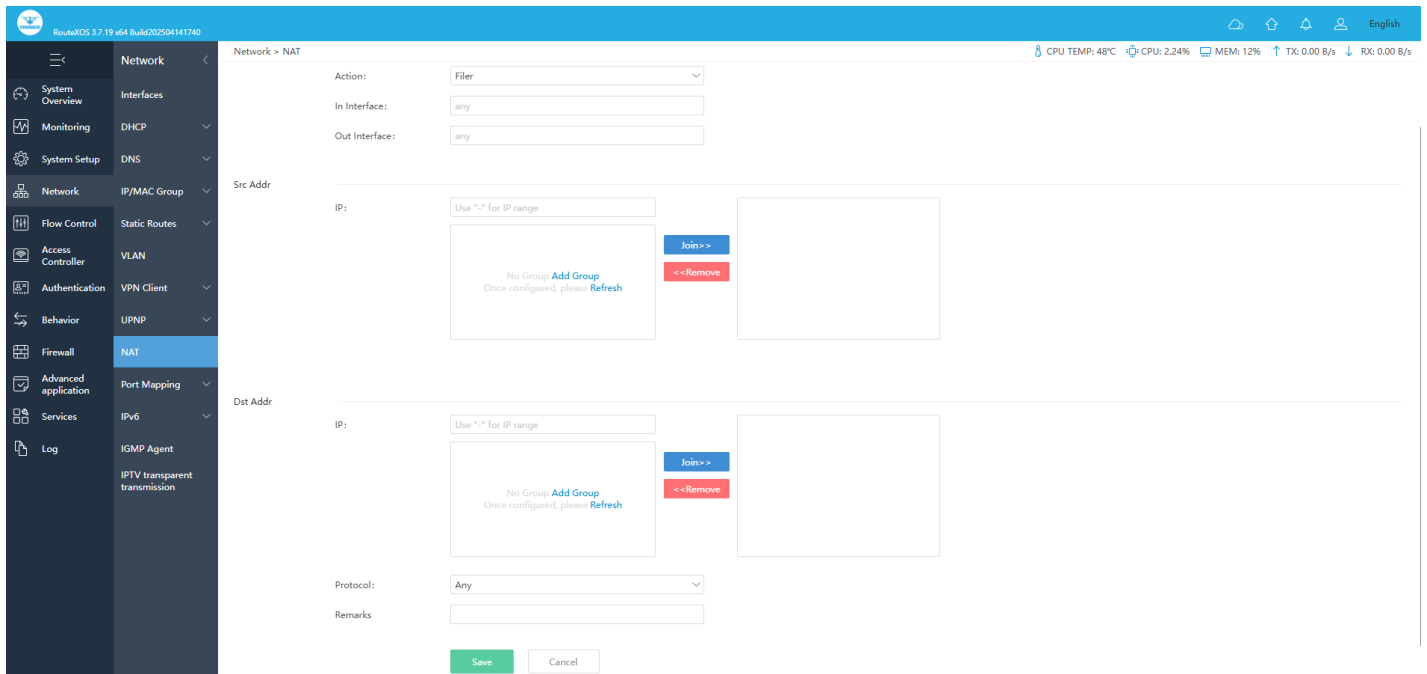


Fig 3.9.2 Default Add Network Address Translation page

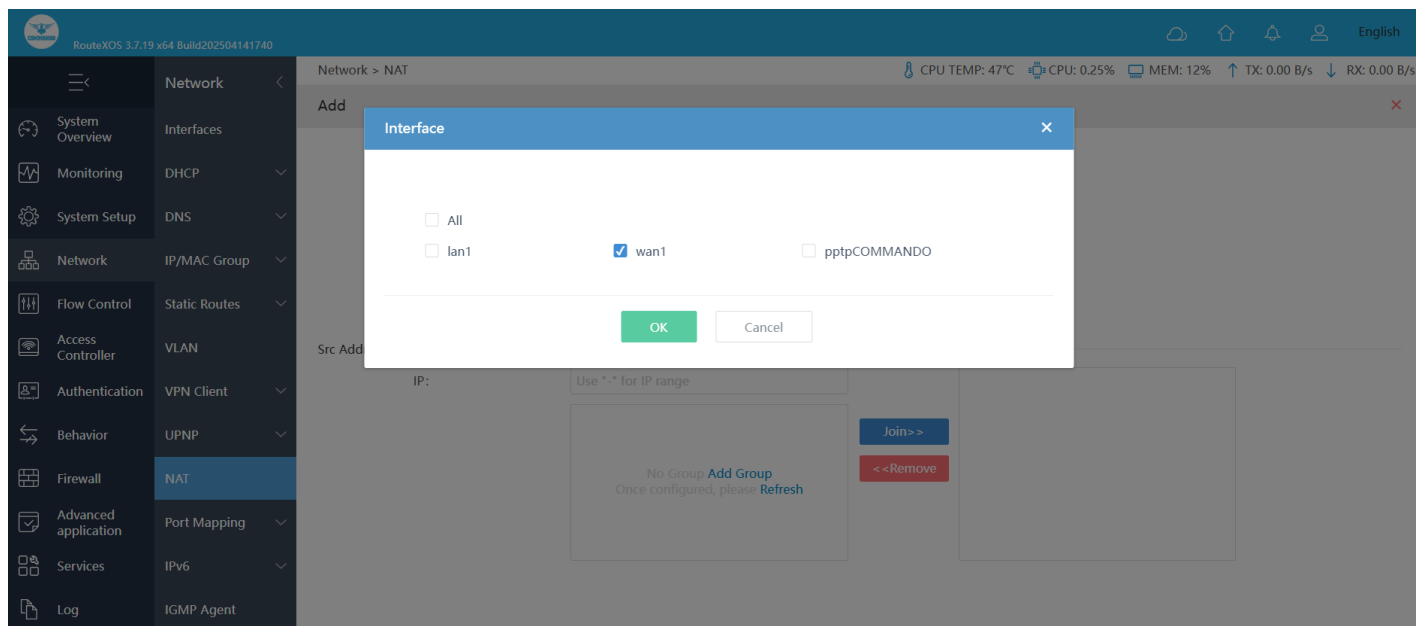


Fig 3.9.3 Add Network Address Translation for specific or all created interfaces page

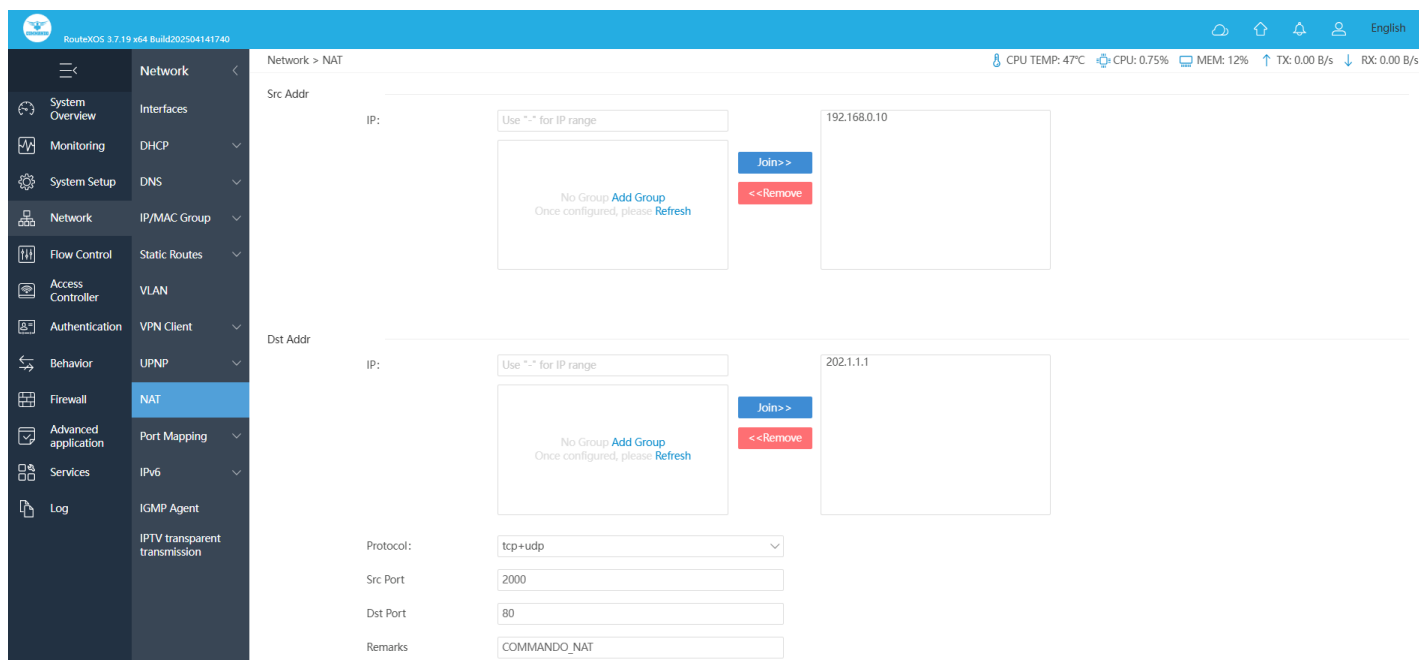


Fig 3.9.4 Network Address Translation details page

3.10 Port Mapping / Port Forwarding

Port mapping / Port Forwarding is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a Gateway. When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network,

located on a specific host or server. External hosts must know this port number and the address of the gateway to communicate with the network-internal service. Often, the port numbers of well-known Internet services, such as port number 80 for web services (HTTP), are used in port forwarding, so that common Internet services may be implemented on hosts within private networks.

Typical applications include running a public HTTP server within a private LAN, Permitting Secure Shell access to a host on the private LAN from the Internet, Permitting FTP access to a host on a private LAN from the Internet, Running a publicly available game server within a private LAN

Administrators configure port forwarding in this Gateway and achieve many advantages. Usually only one of the private hosts can use a specific forwarded port at one time, but configuration is sometimes possible to differentiate access by the originating host's source address.

Local port forwarding is the most common type of port forwarding. It is used to let a user connect from the local computer to another server, ie. forward data securely from another client application running on the same computer as a Secure Shell (SSH) client. Some uses of local port forwarding:

Remote port forwarding of port enables applications on the server side of a Secure Shell (SSH) connection to access services residing on the SSH's client side. Remote port forwarding lets users connect from the server side of a tunnel, SSH or another, to a remote network service located at the tunnel's client side.

Dynamic port forwarding (DPF) is an on-demand method of traversing a firewall or NAT through the use of firewall pinholes. The goal is to enable clients to connect securely to a trusted server that acts as an intermediary for the purpose of sending/receiving data to one or many destination servers. DPF can be implemented by setting up a local application, such as SSH, as a SOCKS proxy server, which can be used to process data transmissions through the network or over the Internet. Programs, such as web browsers, must be configured individually to direct traffic through the proxy, which acts as a secure tunnel to another server. Once the connection is established, DPF can be used to provide additional security for a user connected to an untrusted network. Since data must pass through the secure tunnel to another server before being forwarded to its original destination, the user is protected from packet sniffing that may occur on the LAN. DPF

can also be used to bypass firewalls that restrict access to outside websites, such as in corporate networks.

To configure Port Mapping / Port Forwarding Settings, Click on Network > Port Mapping > Port Mapping

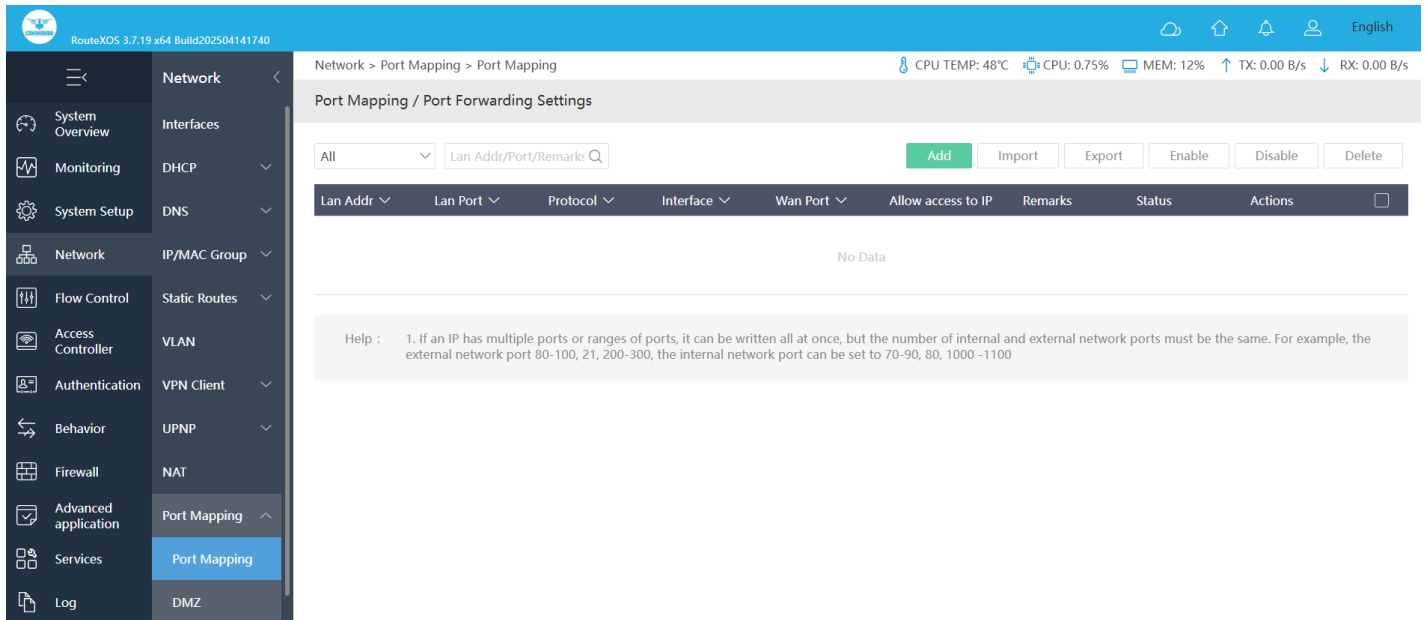


Fig 3.10.1 Default Port Mapping / Port Forwarding Settings page

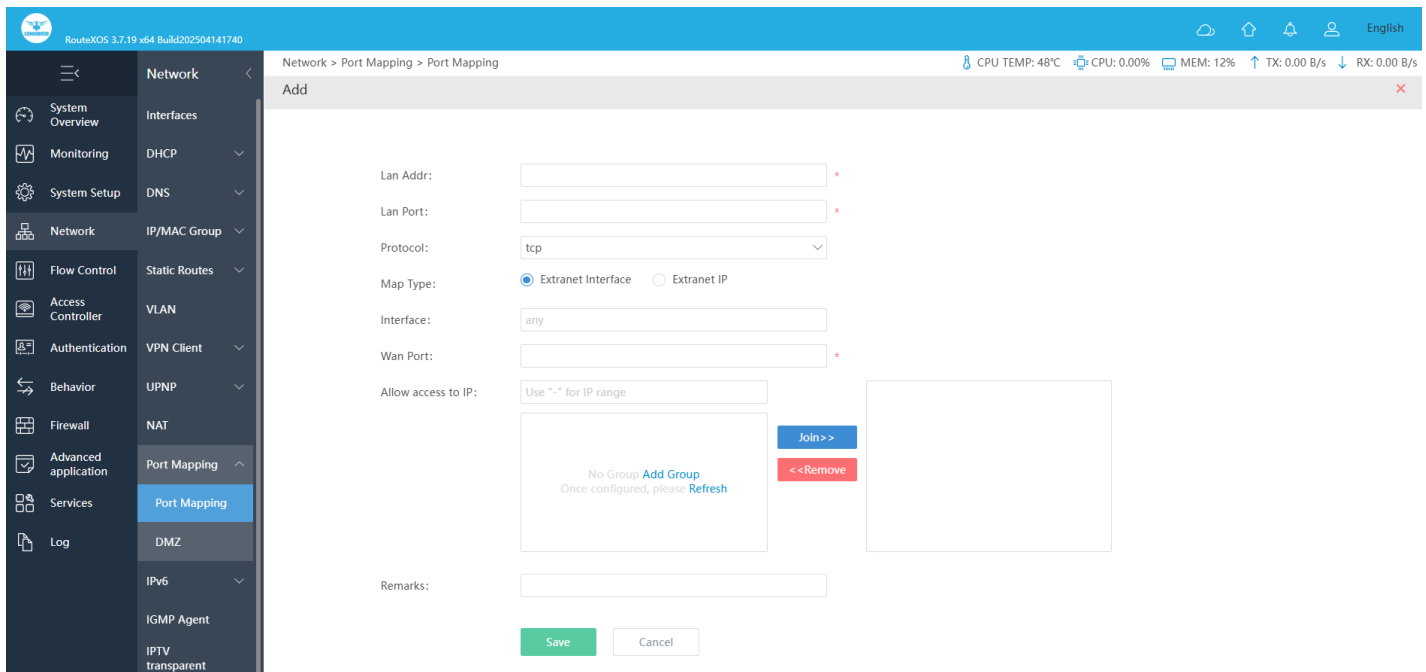


Fig 3.10.2 Add Port Mapping / Port Forwarding Settings page

RouteXOS 3.7.19 x64 Build202504141740

Network > Port Mapping > Port Mapping

CPU TEMP: 48°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Lan Addr: 192.168.1.10

Lan Port: 80

Protocol: tcp+udp

Map Type: ☐ Extranet Interface ☒ Extranet IP

Interface: 202.202.1.220

Wan Port: 64901

Allow access to IP: Use "*" for IP range

No Group [Add Group](#)
Once configured, please [Refresh](#)

[Join >>](#) [<< Remove](#)

Remarks: LAN Server Globally available via Public IP

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

Fig 3.10.3 Port Mapping / Port Forwarding Detail Settings page

RouteXOS 3.7.19 x64 Build202504141740

Network > Port Mapping > Port Mapping

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Port Mapping / Port Forwarding Settings

All [Add](#) [Import](#) [Export](#) [Enable](#) [Disable](#) [Delete](#)

Lan Addr	Lan Port	Protocol	Interface	Wan Port	Allow access to IP	Remarks	Status	Actions
192.168.1.10	80	tcp+udp	202.202.1.220	64901		LAN Server Globally available via Public IP	Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

PerPage: 20 Rows: << < 1 > >> 1 / 1 Pages [Jump](#)

Help : 1. If an IP has multiple ports or ranges of ports, it can be written all at once, but the number of internal and external network ports must be the same. For example, the external network port 80-100, 21, 200-300, the internal network port can be set to 70-90, 80, 1000 -1100

Fig 3.10.4 Port Mapping / Port Forwarding page

Now with public IP (created on WAN port generally) and port number in example 202.202.1.220:64901 you can access internal server 192.168.1.10:80.

DMZ: DMZ or demilitarized zone is a physical or logical subnetwork that contains portion of your network carved off and isolated from the rest of your network of an organization's external-facing services to an untrusted, usually larger, network such as the Internet.

The main benefit of a DMZ is to provide an internal network with an additional security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization's private network. The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe from attackers.

To set DMZ Settings, Click on Network > Port Mapping > DMZ

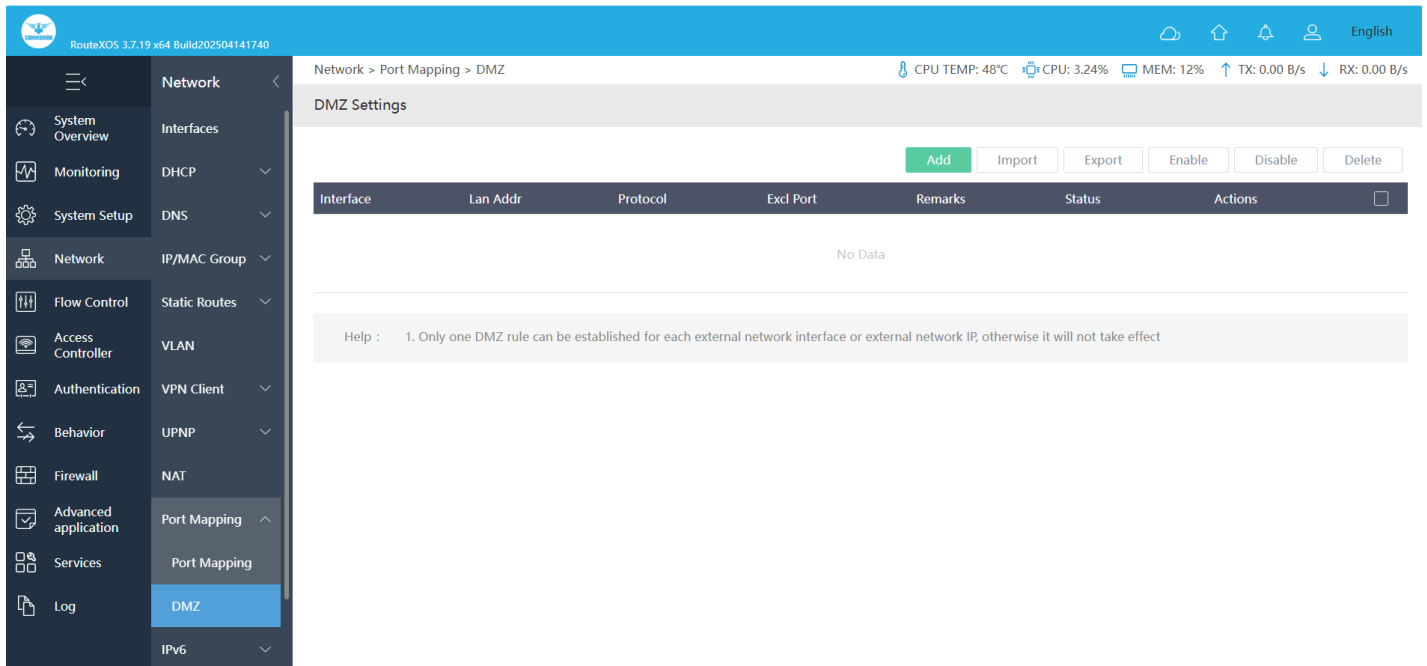


Fig 3.10.5 Default DMZ Settings page

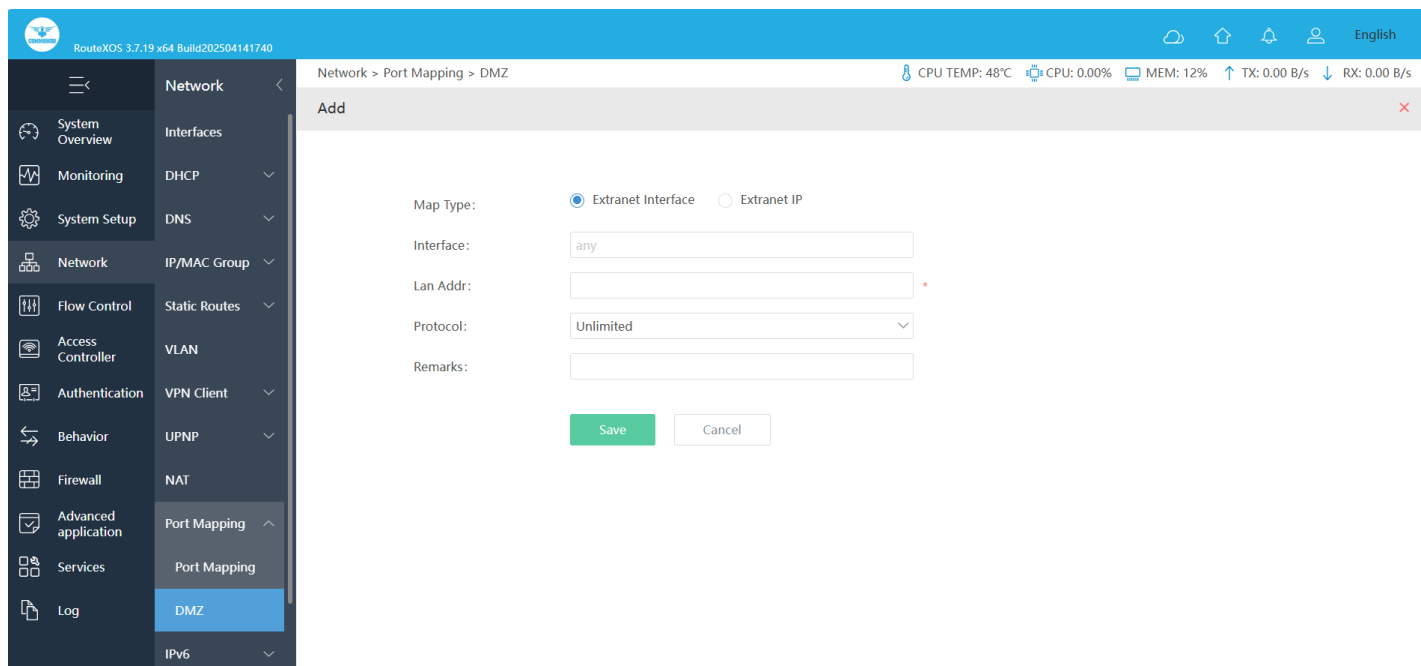


Fig 3.10.6 Add DMZ Settings page

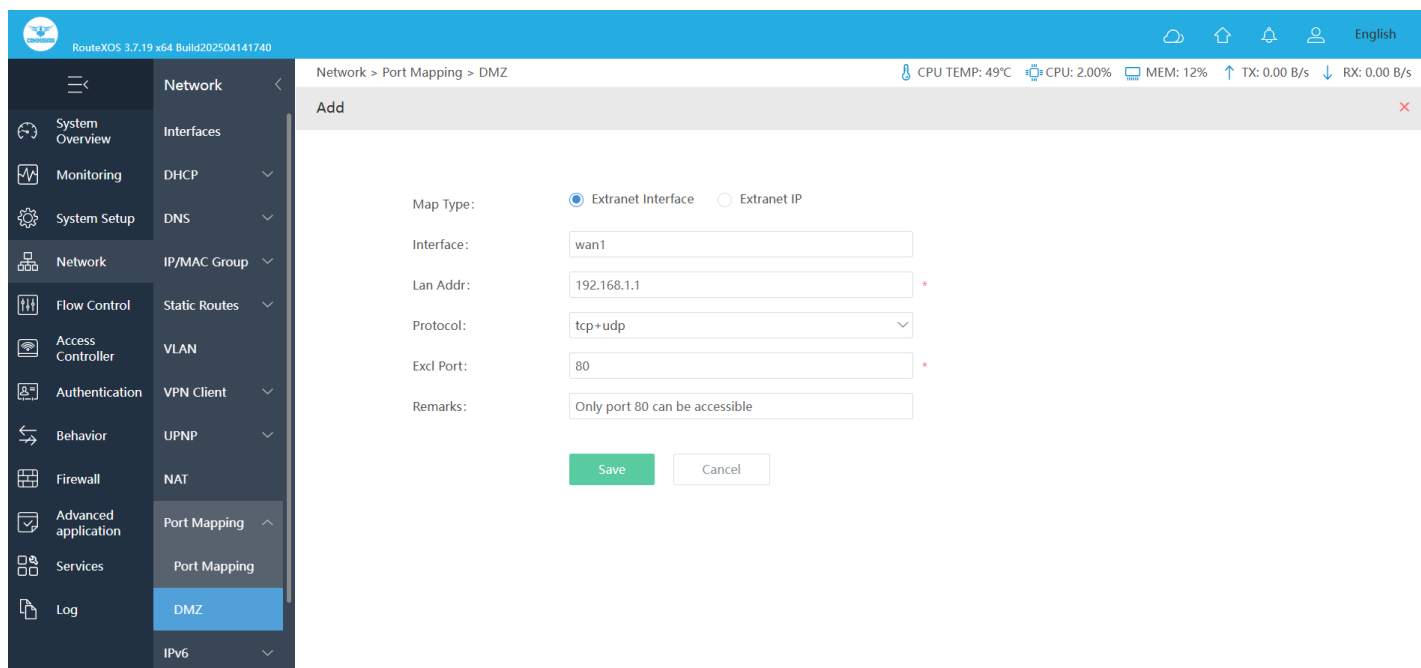


Fig 3.10.7 DMZ detail Settings page

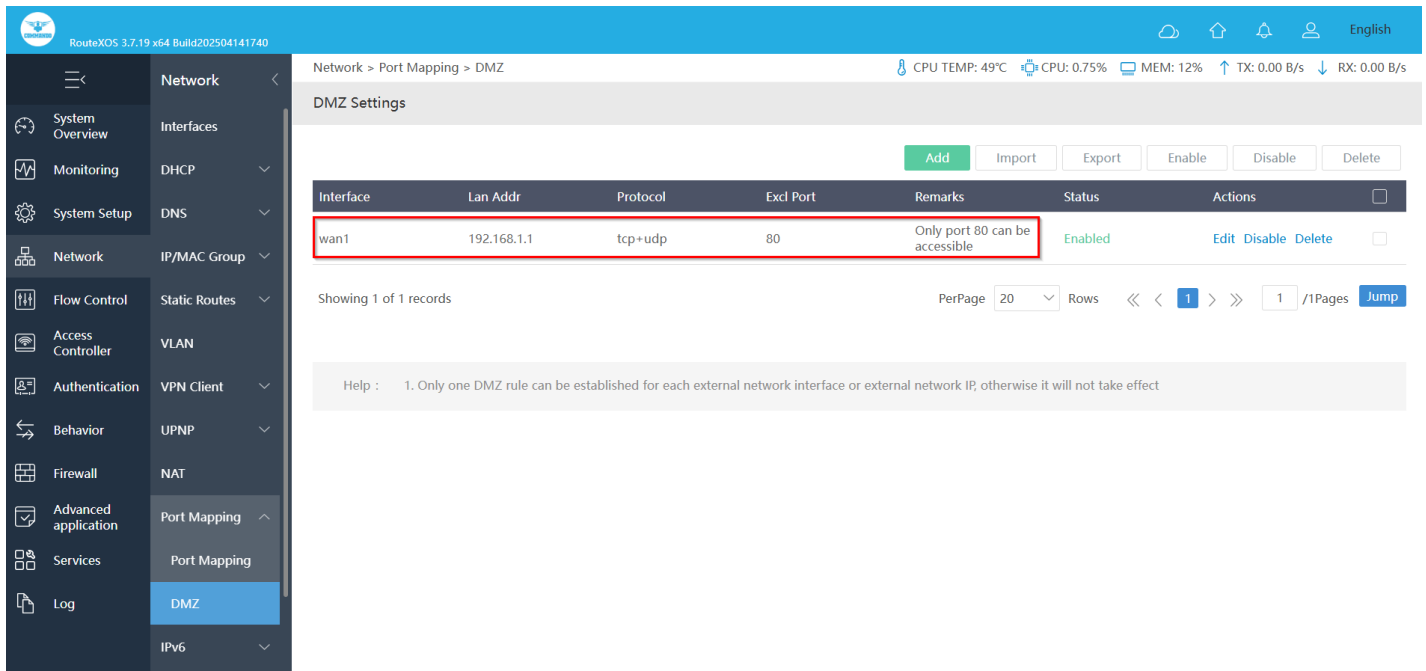


Fig 3.10.8 DMZ Settings page

3.11 IPv6

An IPv6 address is 128 bits in length and consists of eight groups of four hexadecimal digits (base 16 digits represented by the numbers 0-9 and the letters A-F) with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. IPv6 uses 128-bit addresses, allowing 340 trillion IP addresses. IPv6 eliminates the need for NAT by having more IP addresses than can possibly be used and assigning them sparsely. Since IP addresses are no longer a scarce commodity, giant blocks can be handed out for only a few devices without a risk of exhaustion. The IPv6 protocol can handle packets more efficiently, improve performance and increase security. It enables internet service providers to reduce the size of their routing tables by making them more hierarchical. IPv6 Address has two parts:

Network prefix: Same as Network ID of an IPv4 address.

Interface identifier (interface ID): Same as host ID of an IPv4 address. You can manually configure the interface ID or generate it in IEEE 64-bit Extended Unique Identifier (EUI-64) format. Generating an interface ID in EUI-64 format is the most common practice. IEEE EUI-64 standards convert an interface MAC address into an IPv6 interface ID.

IPv6 Address Types: IPv6 addresses can be classified as unicast, multicast, anycast. Unlike IPv4, there is no broadcast IPv6 address. Instead, a multicast address can be used as a broadcast address.

An IPv6 unicast address identifies each interface which belongs to a node, the IPv6 unicast address of any interface can identify the relevant node. Packets sent to an IPv6 unicast address are delivered to the interface identified by that address. IPv6 defines multiple types of unicast addresses, including the unspecified address, loopback address, global unicast address, link-local address, and unique local address.

The IPv6 unspecified address is 0:0:0:0:0:0:0:0/128 or ::/128, indicating that an interface or a node does not have an IP address. It can be used as the source IP address of some packets, such as Neighbor Solicitation (NS) messages, in duplicate address detection. Devices do not forward packets with an unspecified address as the source IP address.

The IPv6 loopback address is 0:0:0:0:0:0:0:1/128 or ::1/128. Similar to the IPv4 loopback address 127.0.0.1, the IPv6 loopback address is used when a node needs to send IPv6 packets to itself. This IPv6 loopback address is usually used as the IP address of a virtual interface, such as a loopback interface. The loopback address cannot be used as the source or destination IP address of packets needing to be forwarded.

An IPv6 global unicast address is an IPv6 address with a global unicast prefix, which is similar to an IPv4 public address. IPv6 global unicast addresses support route prefix summarization, helping limit the number of global routing entries. Global routing prefix is assigned by a service provider to an organization. A global routing prefix is comprised of at least 48 bits. Subnet ID is used by organizations to construct a local network segment.

Interface ID: identifies a device (host).

Link-local addresses are used only in communication between nodes on the same local link. A link-local address uses a link-local prefix of FE80::/10 as the first 10 bits (1111111010 in binary).

When IPv6 runs on a node, a link-local address that consists of a fixed prefix and an interface ID in EUI-64 format is automatically assigned to each interface of the node. This mechanism enables two IPv6 nodes on the same link to communicate without any configuration, making link-local addresses widely used in neighbor discovery and

stateless address configuration. Devices do not forward IPv6 packets with the link-local address as a source or destination address to devices on different links.

Unique local addresses are used only within a site. Site-local addresses have been replaced by unique local addresses. Unique local addresses are similar to IPv4 private addresses. Any organization that does not obtain a global unicast address from a service provider can use a unique local address. However, they are routable only within a local network, not the Internet as a whole. A node may belong to any number of multicast groups. Packets sent to an IPv6 multicast address are delivered to all the interfaces identified by the multicast address.

An IPv6 multicast address is composed of a prefix, a flag, a scope, and a group ID (global ID).

An Anycast address identifies a group of network interfaces, which usually belong to different nodes. Packets sent to an Anycast address are delivered to the nearest interface that is identified by the Anycast address, depending on the routing protocols. Anycast addresses implement redundancy backup and load balancing functions when multiple hosts or nodes are provided with the same services. Currently, a unicast address is assigned to more than one interface to make a unicast address become an anycast address. When sending data packets to anycast addresses, senders cannot determine which of the assigned devices will receive the packets. Which device receives the packets depends on the routing protocols running on the network. Anycast addresses are used in stateless applications, such as Domain Name Service (DNS). IPv6 anycast addresses are allocated from the unicast address space.

To configure IPv6, Click on Network > IPv6 > IPv6 Set

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 48°C CPU: 2.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

extranet Configuration

Buttons: Add, Import, Export, Enable, Disable, Delete

Interface	Access Method	IPv6 Addr	IPv6 Prefix	IPv6 address	IPv6 gateway	Status	Actions
	DHCPv6 client(dynamic acquisition)					Disabled	Edit Enable Delete

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1Pages: Jump

Intranet Configuration

Buttons: Add, Import, Export, Enable, Disable, Delete

Intranet Interface	Configuration Type	Bind external network lines	IPv6 Addr	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term
lan1	Automatic Acquisition		fe80::aab8:e0ff:fe06:4975/64		open	Stateless + stateful	120

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1Pages: Jump

Fig 3.11.1 Default IPv6 Page

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 49°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Intranet Interface: lan1

Configuration Type: Automatic Acquisition

Bind external network lines: *

Prefix Length: Automatic

DHCPv6: ☒ Open

DHCPv6 Mode: Stateless + stateful

RA Advertisement Binding: ☐ Open
(After the RA notification binding is enabled, the terminal must match the prefix static allocation rules in order to obtain the stateless v6 address or gateway address)

IPv6 DNS: ☐ Open

Lease Term: 120 minute (Tip: Changes in the IPv6 prefix of the wan port will affect the terminal IP lease period)

RA MTU: ☐ Open

Buttons: Save, Cancel

Fig 3.11.2 Add IPv6 Page

To enable DHCPv6 client (dynamic acquisition) and getting IPv6 address automatically to interface.

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 48°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

IPv6

Extranet Configuration

Buttons: Add, Import, Export, Enable, Disable, Delete

Interface	Access Method	IPv6 Addr	IPv6 Prefix	IPv6 address	IPv6 gateway	Status	Actions
wan1	DHCPv6 client(dynamic acquisition)	fe80::aab8:e0ff:fe06:4978				Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1 Pages: 1 Jump

Intranet Configuration

Buttons: Add, Import, Export, Enable, Disable, Delete

Intranet Interface	Configuration Type	Bind external network lines	IPv6 Addr	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term
lan1	Automatic Acquisition		fe80::aab8:e0ff:fe06:4975/64		open	Stateless + stateful	120

Fig 3.11.3 Enabling DHCPv6 Page

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Intranet Interface: lan1

Configuration Type: Automatic Acquisition

Bind external network lines: *

Prefix Length: Automatic

DHCPv6: ☒ Open

DHCPv6 Mode: Stateless + stateful

RA Advertisement Binding: ☐ Open
(After the RA notification binding is enabled, the terminal must match the prefix static allocation rules in order to obtain the stateless v6 address or gateway address)

IPv6 DNS: ☐ Open

Lease Term: 120 minute (Tip: Changes in the IPv6 prefix of the wan port will affect the terminal IP lease period)

RA MTU: ☐ Open

Buttons: Save, Cancel

Fig 3.11.4 Automatic Acquisition of IPv6 address for LAN1 interface Page

Network > IPv6 > IPv6 Set

CPU: 0.75% MEM: 18% TX: 33.00 B/s RX: 33.00 B/s

IPv6

Extranet Configuration

Interface	Access Method	IPv6 Prefix	IPv6 address	IPv6 gateway	Status	Actions
wan1	DHCPv6 client(dynamic acquisition)			fe80::1	Enabled	Edit Disable

Intranet Configuration

[Add](#) [Enable](#) [Disable](#) [Delete](#)

Intranet Interface	Link local address	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term	Preferred DNS	Alternative DNS	Status	Actions
lan1	fe80::a9b4bfff50:1cbc	fc00:ec88:bde3:1::1/64	open	Stateless + stateful	120	fe80::1		Enabled	Edit Disable Delete

Fig 3.11.5 Automatic IPv6 address for LAN1 interface Page

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Intranet Interface:

Configuration Type:

IPv6 address:

DHCPv6: ☒ Open

DHCPv6 Mode:

IPv6 DNS: ☒ Open

Preferred DNS:

Alternative DNS:

Lease Term: minute (Tip: Changes in the IPv6 prefix of the wan port will affect the terminal IP lease period)

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

Fig 3.11.6 Manual IPv6 address for vlan0002 interface Page

RouteXOS 3.7.19 x64 Build202504141740

Network > IPv6 > IPv6 Set

CPU TEMP: 48°C CPU: 1.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

IPv6

Extranet Configuration

Iface Wan	Access Method	IPv6 Addr	IPv6 Prefix	IPv6 address	IPv6 gateway	Status	Actions
wan1	DHCPv6 client(dynamic acquisition)	fe80::aab8:e0ff:fe06:4978				Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Intranet Configuration

Intranet Interface	Configuration Type	Bind external network lines	IPv6 Addr	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term	Status	Actions
vlan0002	Static Configuration		fe80::2f4:58ff:fe33:c3a0/64	2001:5bcd:1cc1::1/64	open	Stateful	120	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 3.11.7 Manual IPv6 address for vlan0002 interface Page

DHCPv6 Terminal: Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network. It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4. IPv6 hosts may automatically generate IP addresses internally using stateless address auto configuration (SLAAC), or they may be assigned configuration data with DHCPv6. IPv6 hosts (Here referred as Terminal) use stateless auto configuration may require information other than an IP address or route. DHCPv6 can be used to acquire this information, even though it is not being used to configure IP addresses. DHCPv6 is not necessary for configuring hosts with the addresses of Domain Name System (DNS) servers, because they can be configured using Neighbor Discovery Protocol, which is also the mechanism for stateless auto configuration.

To view DHCPv6 Terminal, Click on Network > IPv6 > DHCPv6 Terminal

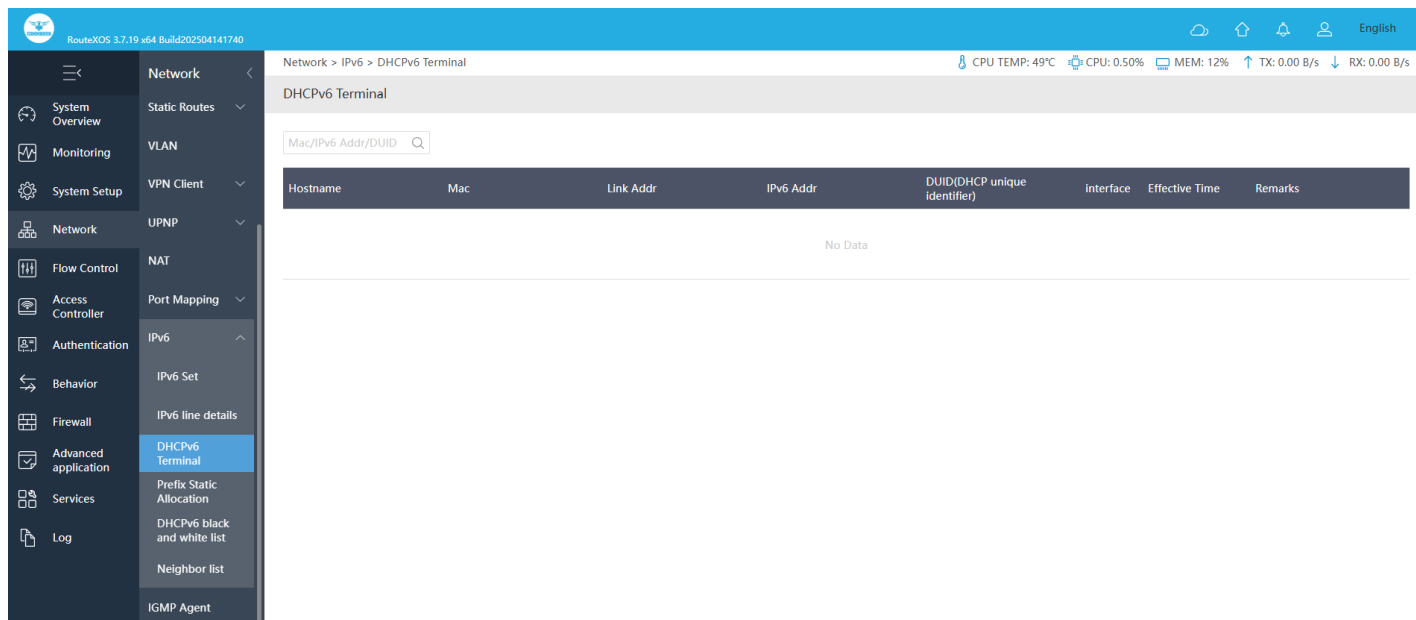


Fig 3.11.8 Default DHCPv6 Terminal Page

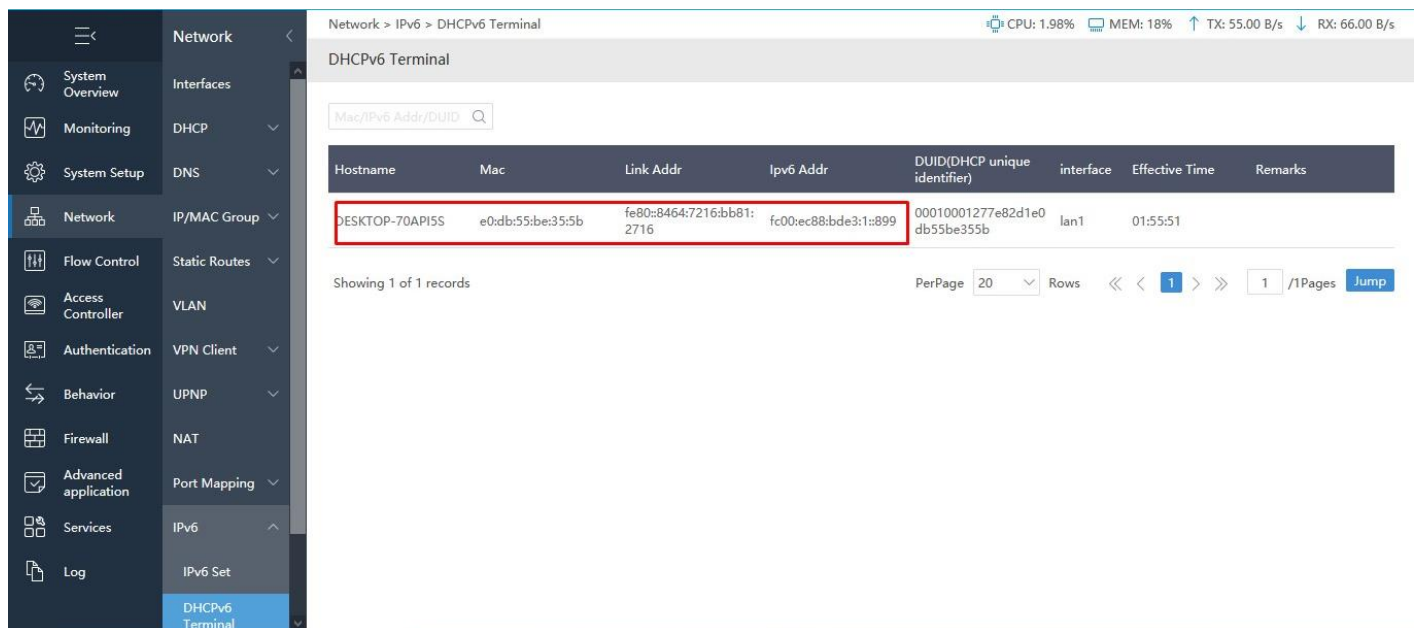


Fig 3.11.9 DHCPv6 Terminal Page Neighbor

List: For IPv6, ICMPv6 neighbor discovery replaces Address Resolution Protocol (ARP) for resolving network addresses to link-level addresses. Neighbor discovery also handles changes in link-layer addresses, inbound load balancing, anycast addresses, and proxy advertisements. You can display the IPv6 neighbor table, which contains an entry for each IPv6 neighbor with which the Gateway exchanges IPv6 packets.

To view DHCPv6 Terminal, Click on Network > IPv6 > Neighbor List

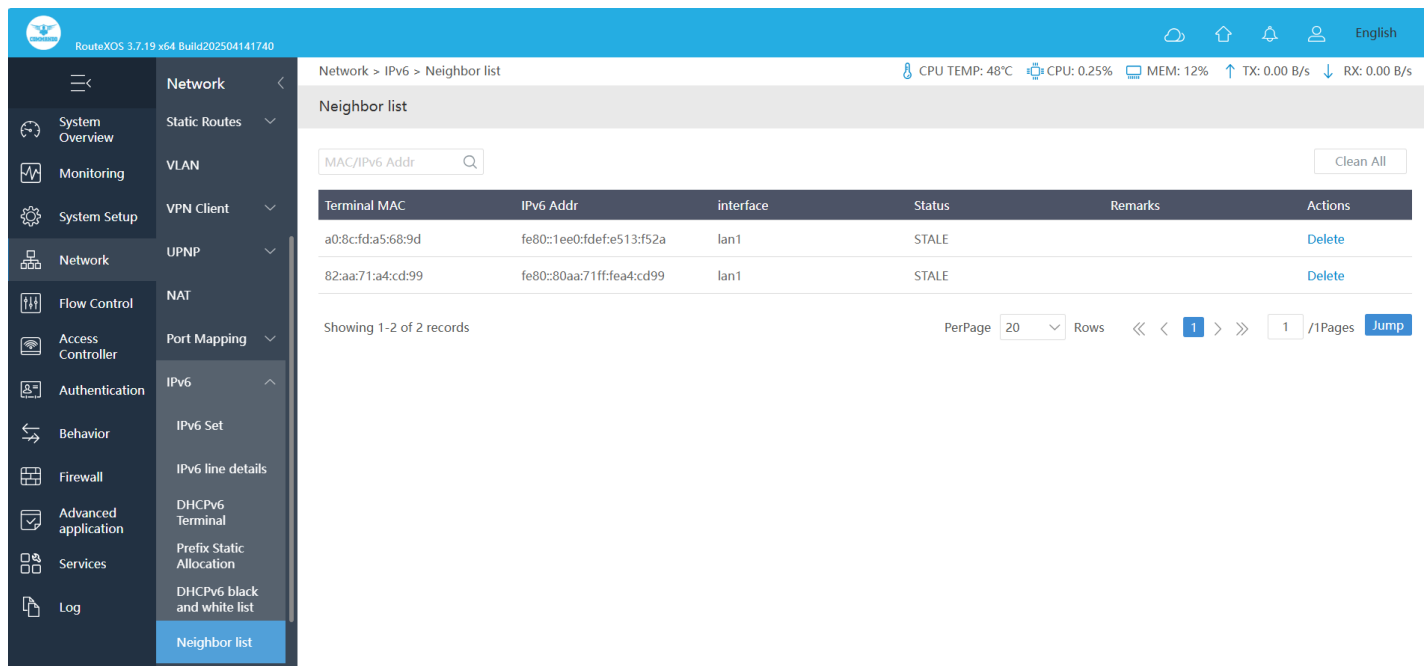


Fig 3.11.10 Default IPv6 Neighbor List Page

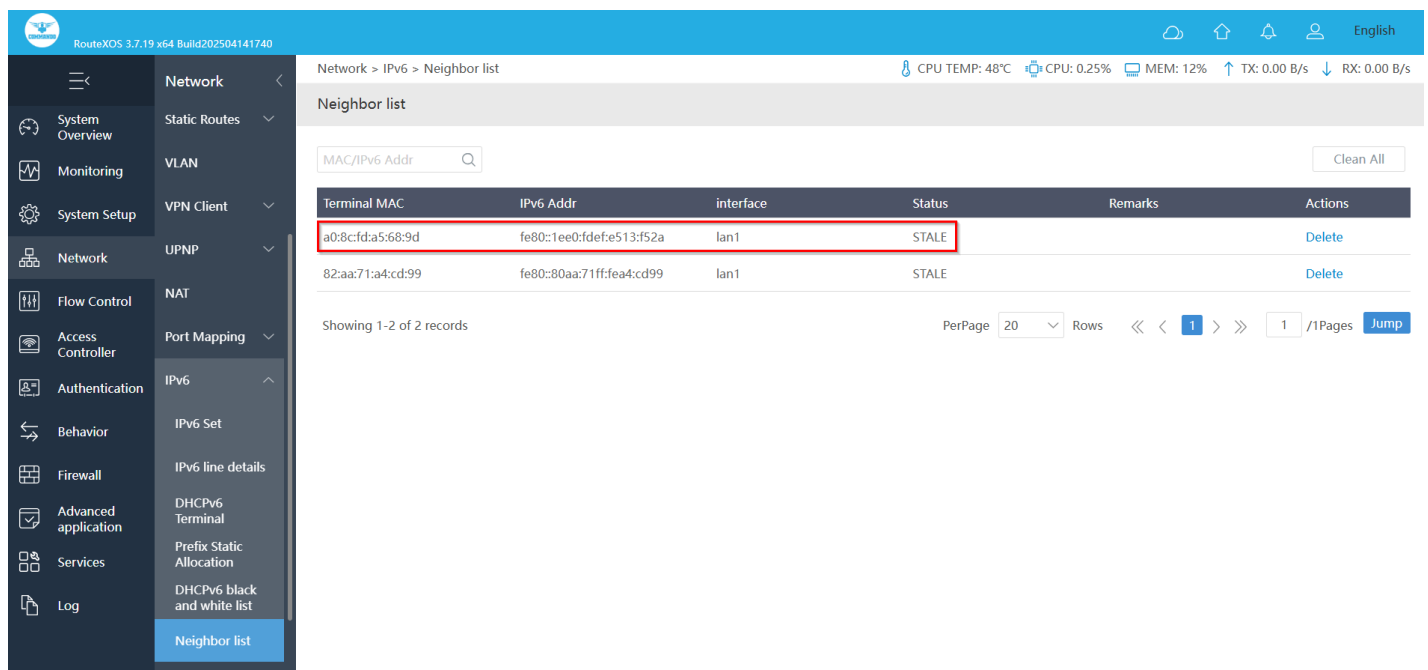


Fig 3.11.11 IPv6 Neighbor List Page

3.12 IGMP Agent

The Internet Group Management Protocol (IGMP) used by hosts and multicast Gateways to exchange their IP multicast group memberships with each other. It manages the membership of hosts and routing devices in multicast groups. IP hosts use IGMP to report

their multicast group memberships to any immediately neighboring multicast routing devices.

To configure and View IGMP Agent, Click on Network > IGMP Agent

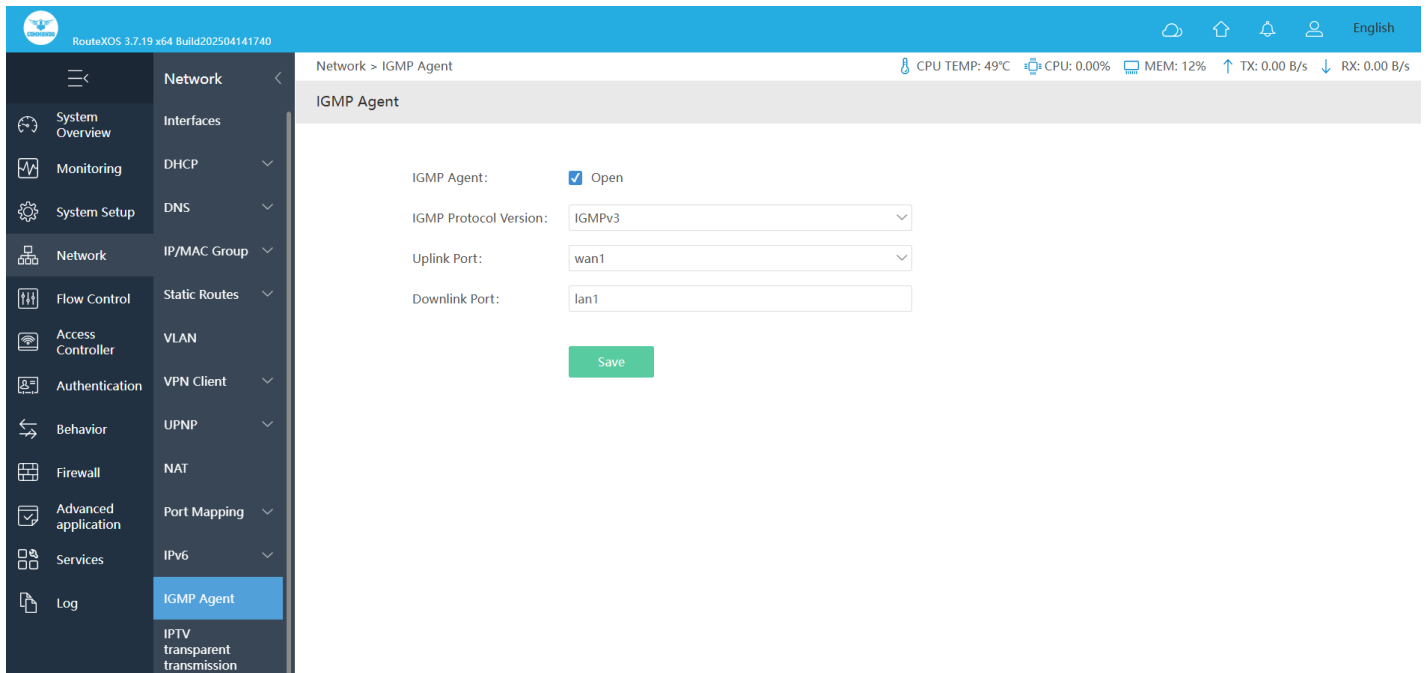


Fig 3.12.1 Default IGMP Agent Page

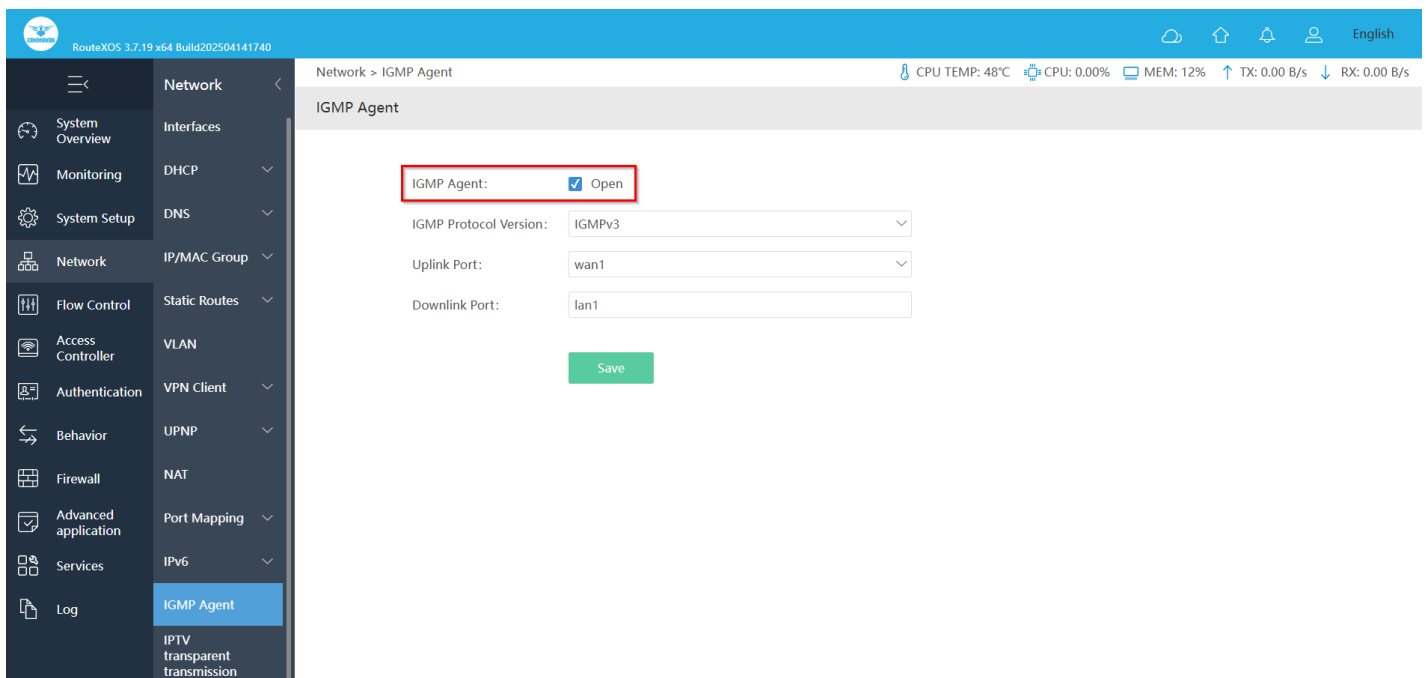


Fig 3.12.2 Enabling IGMP Agent Page

3.13 IPTV transparent transmission

IPTV Transparent Transmission ensures seamless multicast and unicast IPTV traffic delivery across the network without modifying packet structures or affecting data integrity. It allows IPTV streams to pass through the network without interference, preserving video quality and reducing latency. This feature helps optimize network performance for IPTV services by ensuring smooth playback, minimizing buffering, and maintaining compatibility with various IPTV devices.

To configure and view IPTV Transparent Transmission, click on Network > IPTV Transparent Transmission.

The screenshot displays the 'IPTV transparent transmission' configuration page within the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar shows a navigation menu with 'Network' selected, and 'IPTV transparent transmission' highlighted under the 'Network' section. The main content area is titled 'Network > IPTV transparent transmission' and includes system status indicators: CPU TEMP: 50°C, CPU: 1.99%, MEM: 12%, TX: 66.00 B/s, and RX: 0.00 B/s. The configuration options are as follows:

- IPTV transparent transmission:** ☐ Open
- Transparent mode:** Transparent transmission (dropdown menu) This mode applies to the internal network port directly connected to the set-top box
- Input network port:** eth0 (lan1) (dropdown menu)
- Business VLAN ID:** (empty text field with a red asterisk indicating a required field)
- Output network port:** (empty dropdown menu)

A green 'Save' button is located at the bottom of the configuration area.

Fig 3.13.1 Default IPTV transparent transmission Page

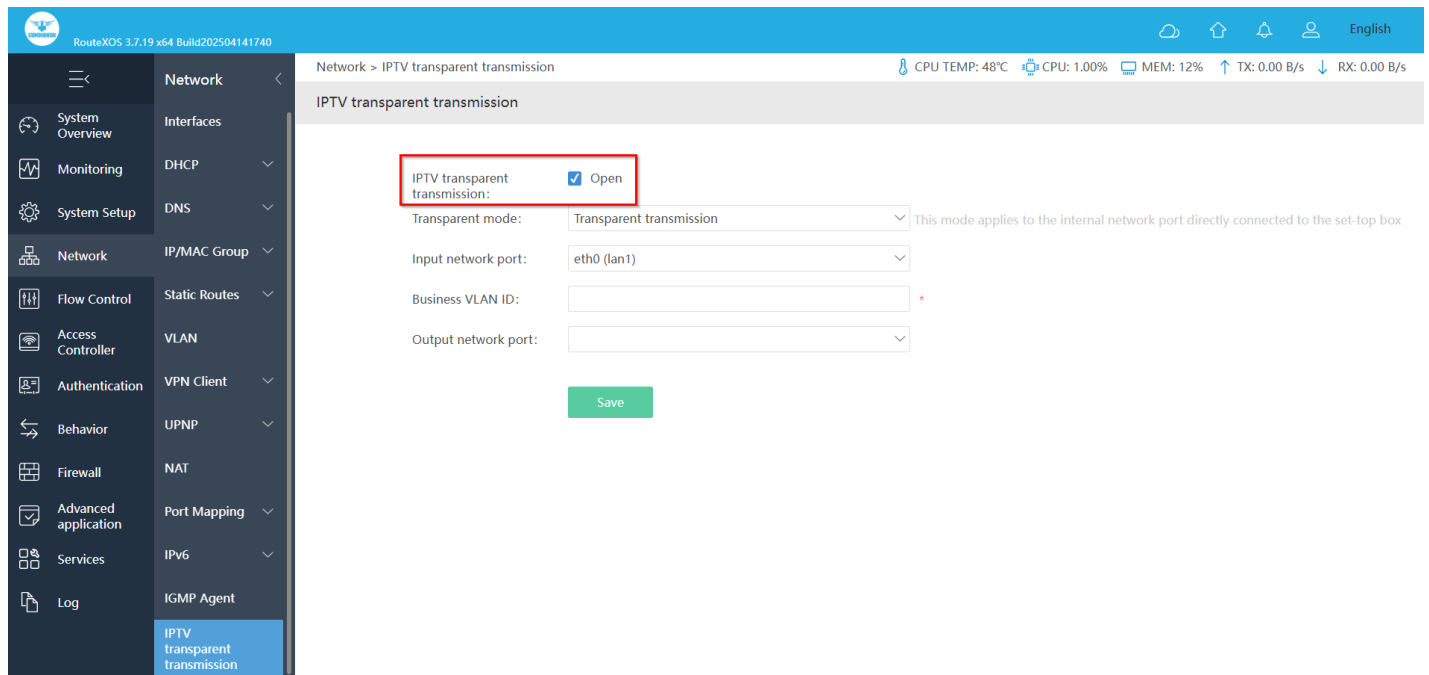


Fig 3.13.2 IPTV transparent transmission Page

FLOW CONTROL

Multi-WAN: Providing Four adjustable WAN/LAN ports for users to configure WAN ports based on need and connect multiple Internet lines for bandwidth expansion as well as load balance with auto fail-over recovery for reliable and efficient multiple Load Balance modes, including Bandwidth Based Balance Routing, Application Optimized Routing, and Policy Routing to optimize bandwidth usage. It has Multi-Vendor WAN Line simultaneous Access, WAN load sharing and balancing by different ISP, Rational use, Load Balancing with fail-over, Reduce Bandwidth Costs.

Smart Flow Control: Enabling flow control can optimize the bandwidth and improve the network experience of important applications, especially in the bandwidth environment.

IP/MAC Limiters: It supports bandwidth control for IP/MAC connected to it. If you need to set a IP/MAC limiter setting for Interface, IP, Source Port, Destination Port, Speed limit mode for upload and download. This IP/MAC Limit is used for setting a Speed Limit Values.

Protocol Library: Can set Custom Protocol, Advanced Custom Protocol for different class

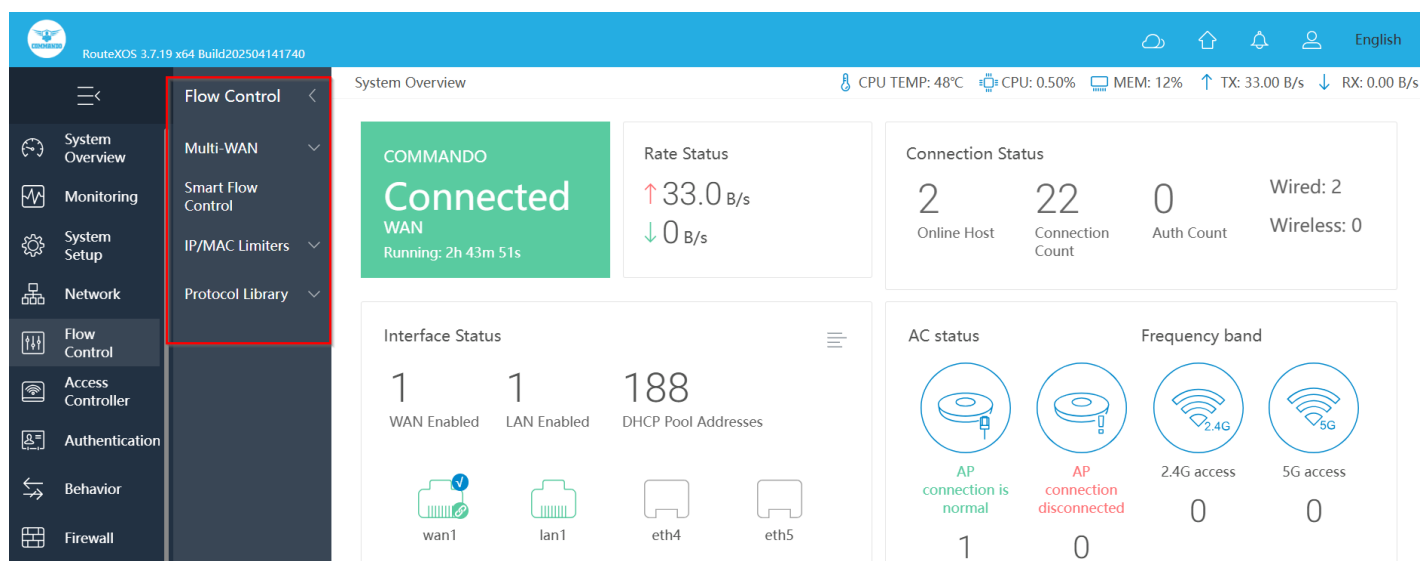


Fig 4.1 Flow control configuration page

Failover and backup

Multi-WAN Gateways are highly useful for those who need the Internet at all times and when even a few minutes of nonavailability can impact them in a big way. With multi-WAN Gateways, you don't have to rely on a single Internet ISP only and this is a big advantage when you live in an area with a patchy Internet connection. These Gateways allow you to have an Internet connection from one to four different ISPs, so even if one fails, you still have access to the other.

You can even configure the first connection as the primary and the others as a backup connection so that the backup will switch over when the main Internet connection fails.

Load balancing

Internet load balancing allows reliable Internet service at all times with all WAN connection used at a same time. When you use many applications such as web browsers, VPNs, streaming services, and emails, you tend to use high amounts of bandwidth and the entire load is passed to a single ISP in a traditional Gateway setup. But with multi-WAN Gateways, this load is spread across two or more ISPs, so the overall Internet speed tends to be faster. Such Multi WAN load balancing ensures that you have access to high-speed Internet at all times, regardless of the load and size of applications that use it.

1. Multi-WAN Load Balancing

Multi WAN Link load balancing with failover protection provides advanced failover and bandwidth and load management for full utilization of all available multiple WAN connections and ensure continuous operation in the event that one or more ISP links become unavailable or slow to respond. It has load balancing feature which intelligently analyzes ISP WAN links to allocate bandwidth, assign priority and enable seamless failover for business-critical applications. This Multi WAN link load balancers help guarantee uptime and service level agreements, reduce bandwidth costs and improve the end-user experience.

To configure Multi-WAN Load Balancing Settings, Click on Flow Control > Multi-WAN > Load Balancing

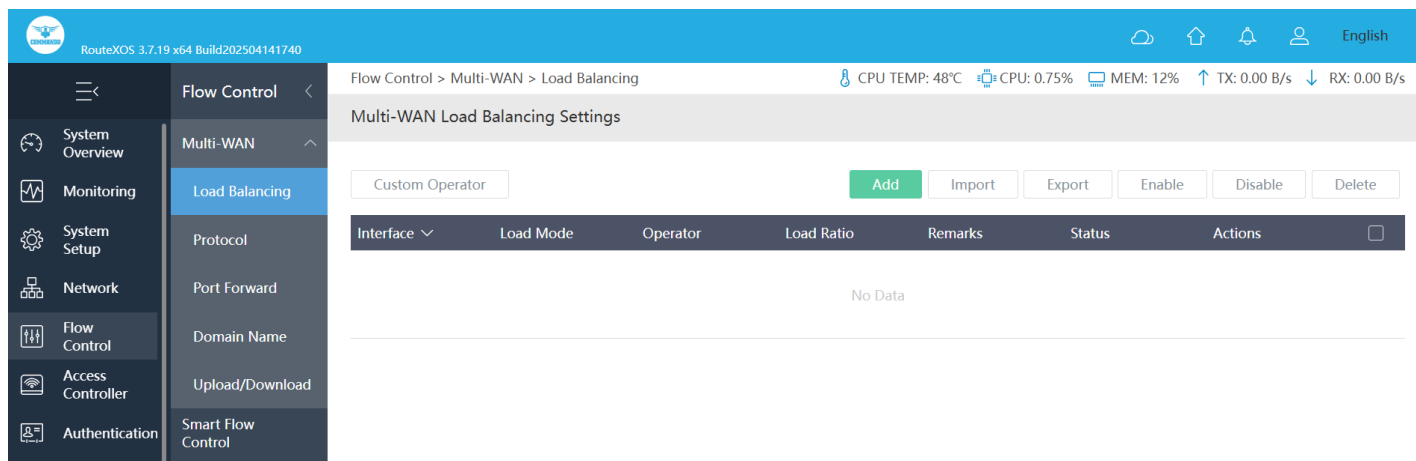


Fig 4.1.1 Default Multi-WAN Load Balancing Settings page

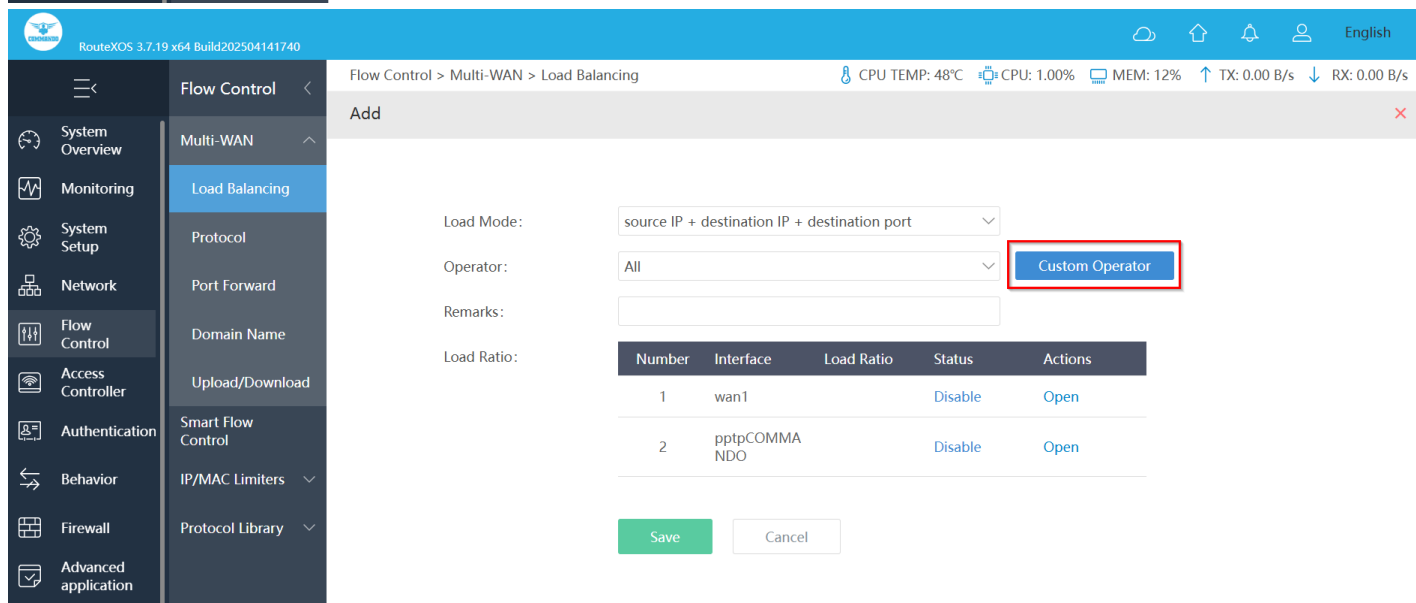
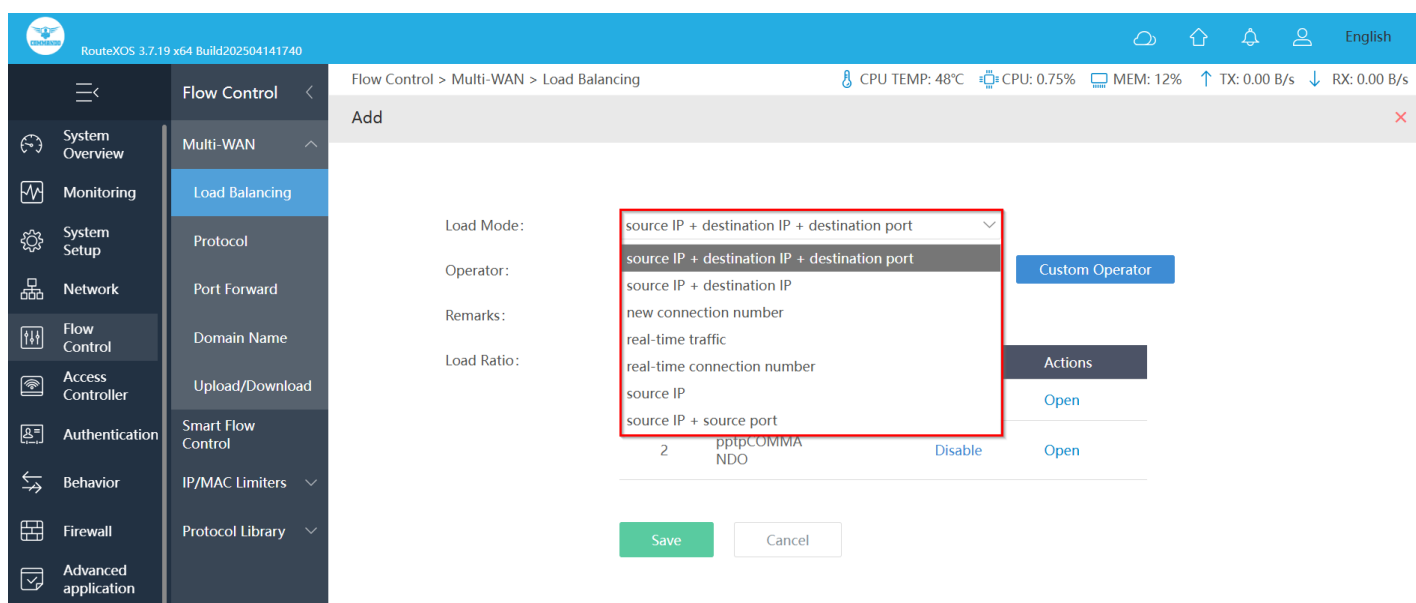


Fig 4.1.2 Add Multi-WAN Load Balancing Settings page

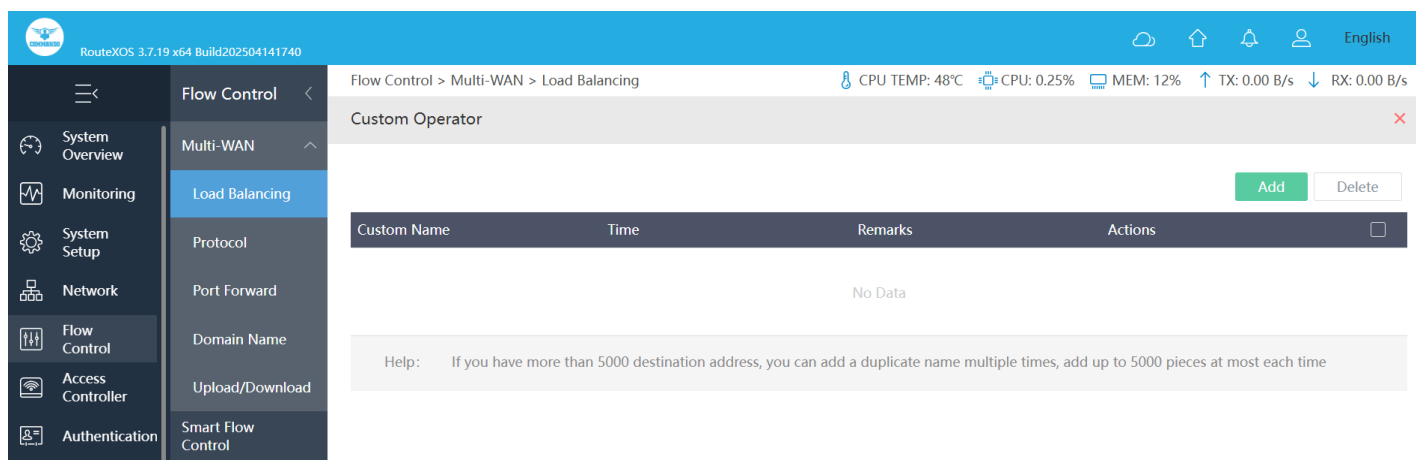


Fig 4.1.3 Default Custom operator page

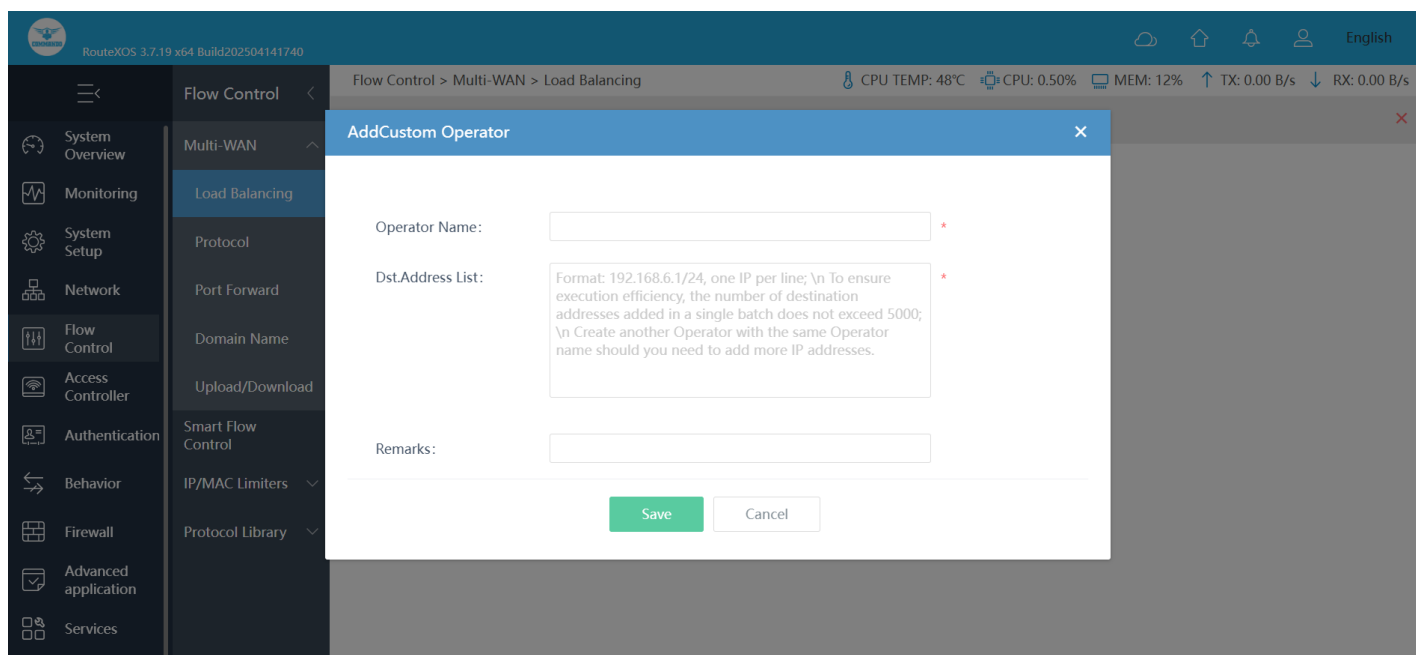


Fig 4.1.4 Add Custom operator page

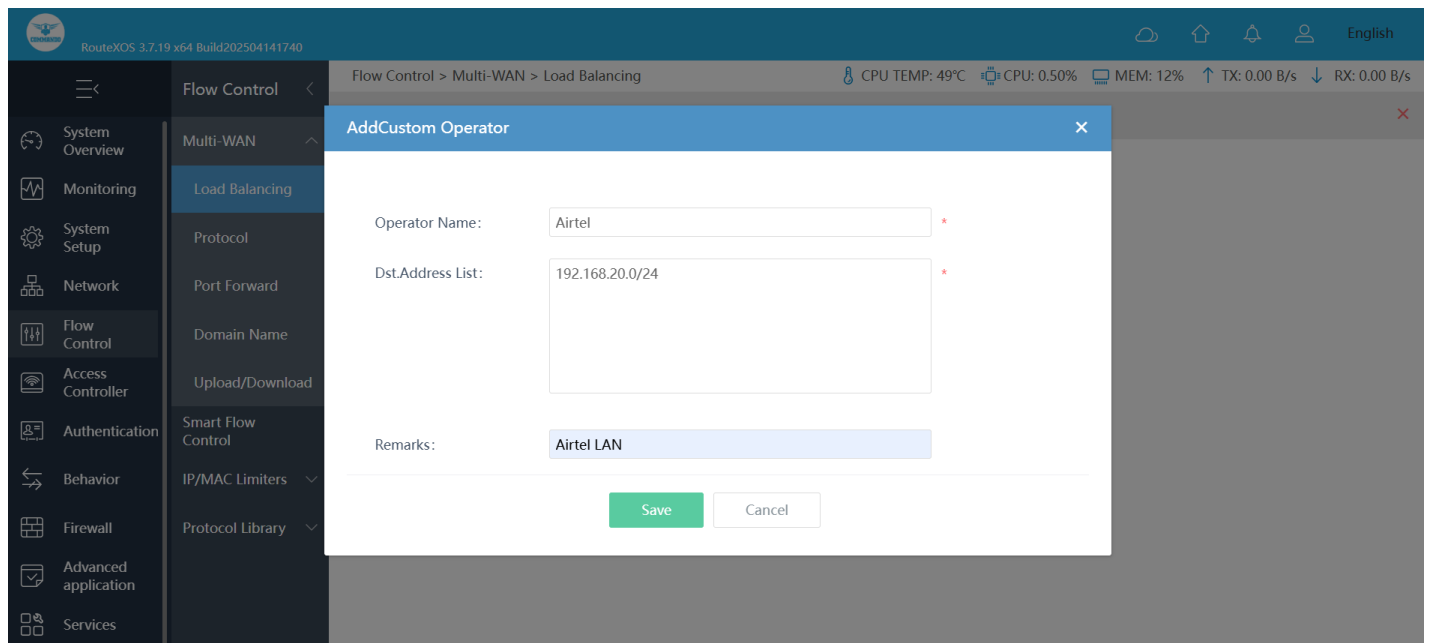


Fig 4.1.5 Setting Custom operator page

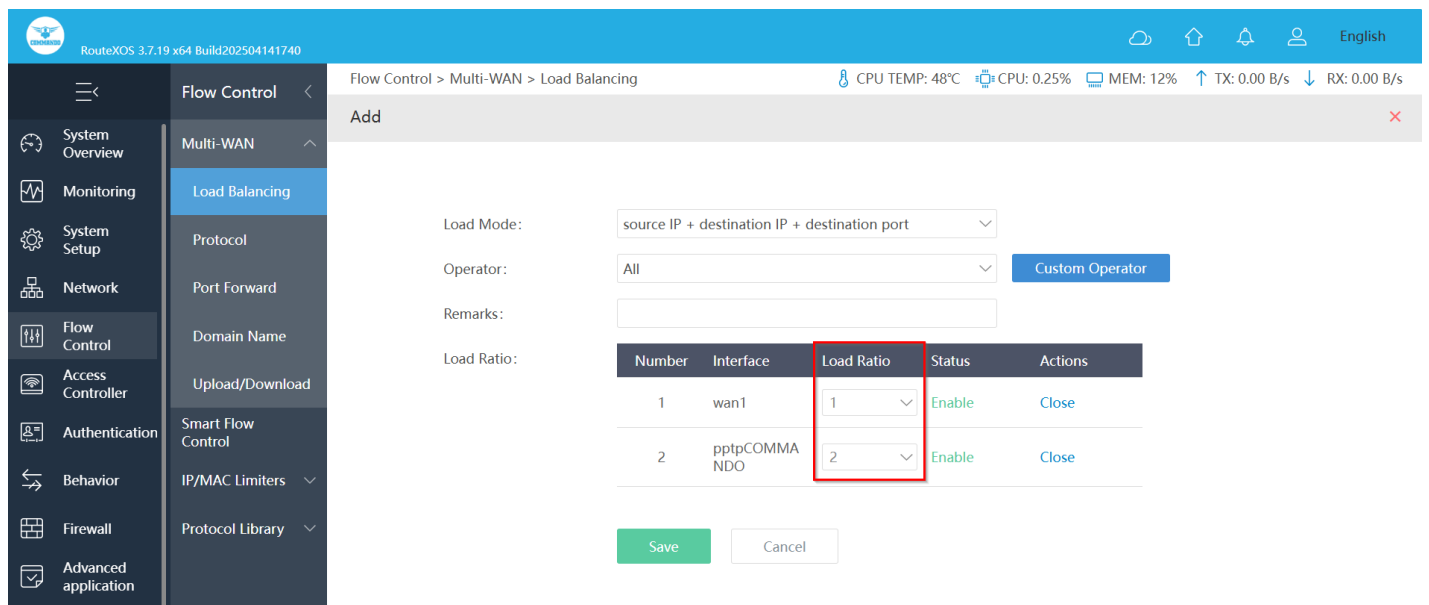


Fig 4.1.6 Setting Proper Load ratio for efficient use of WAN link page

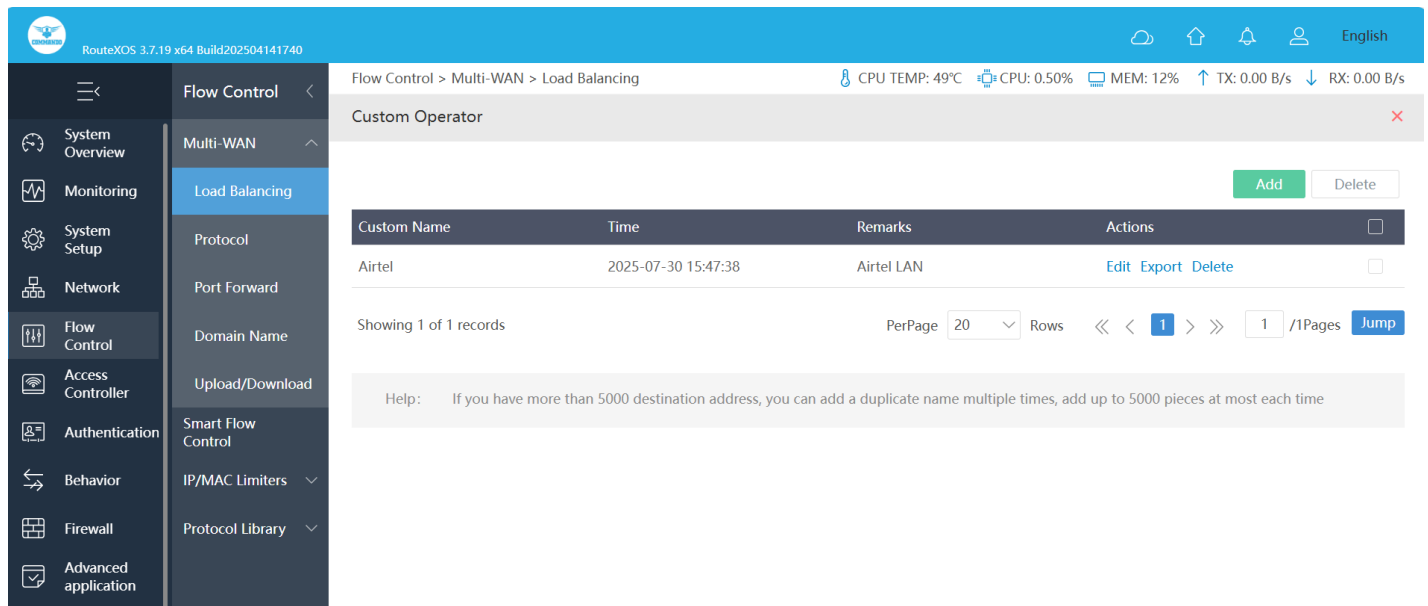


Fig 4.1.7 Custom operator page

Multi-WAN

Protocol Control Settings: Turn On Enhanced Flow Control (Only for multi-line environments), opening flow control can greatly improve the protocol flow control effect.

To configure Multi-WAN Protocol Control Settings, Click on Flow Control > Multi-WAN > Protocol

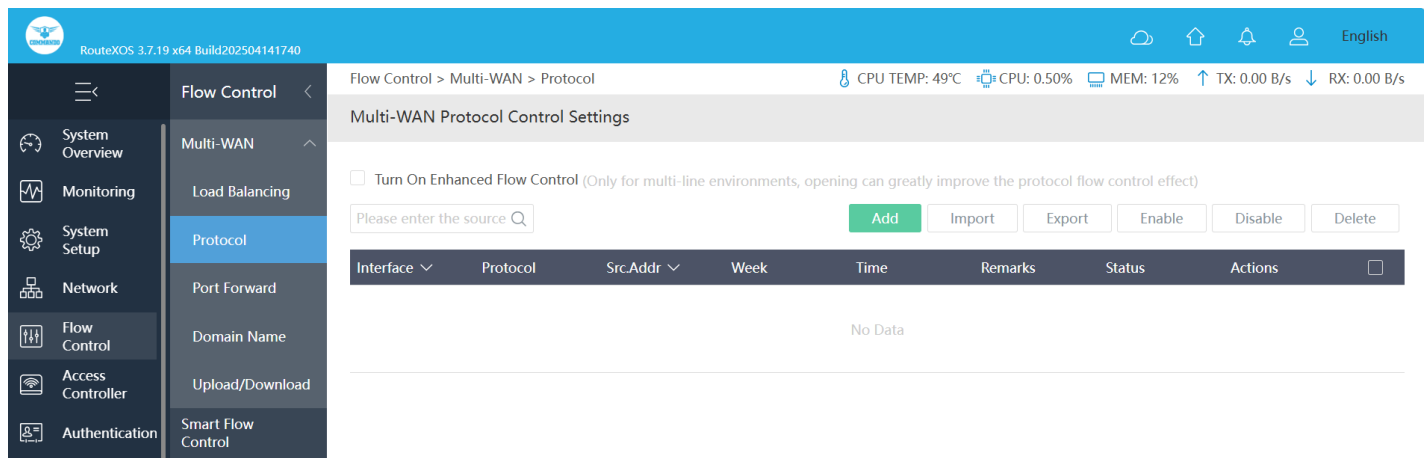


Fig 4.1.8 Default Multi-WAN Protocol Control Settings page

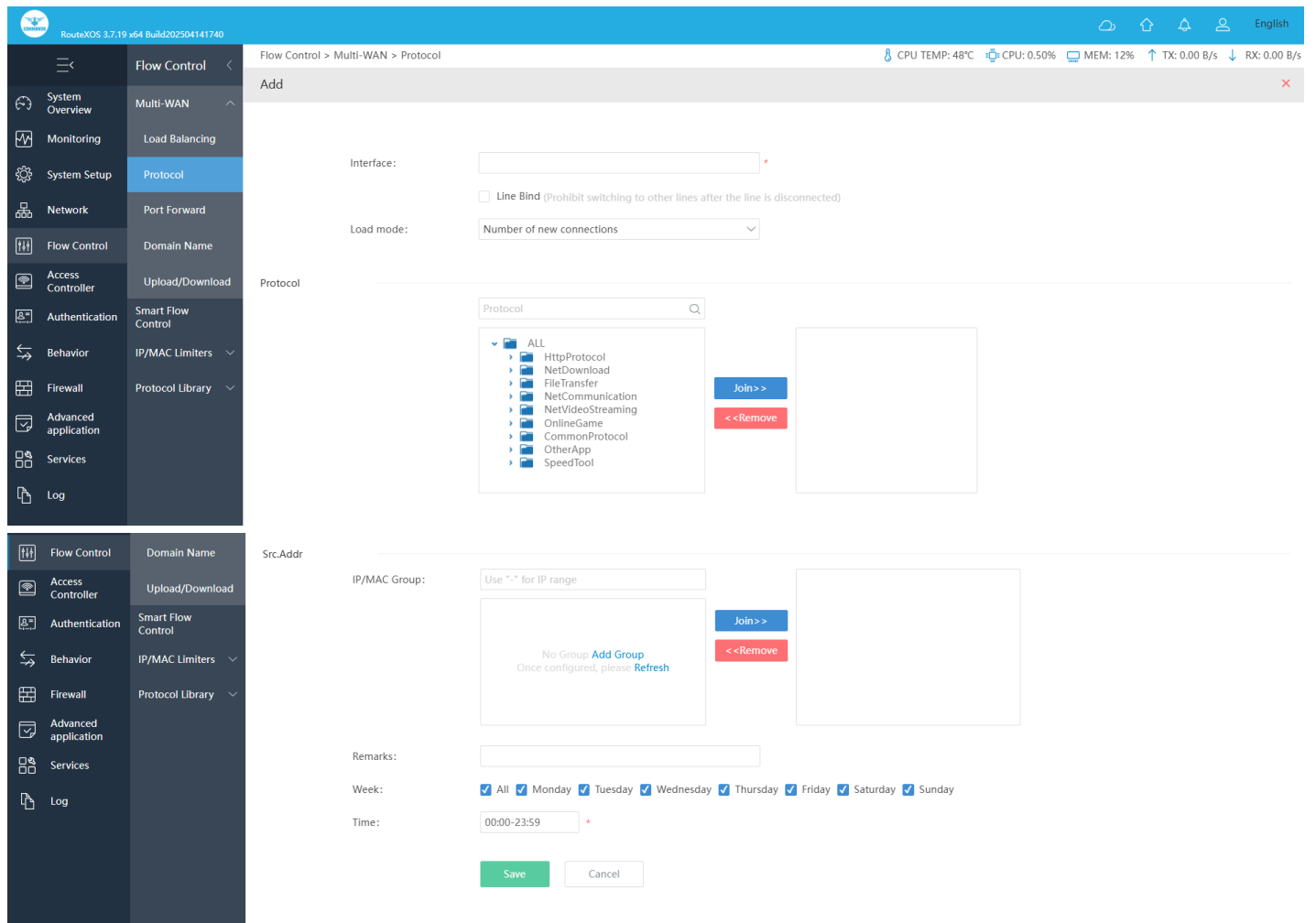


Fig 4.1.9 Add Multi-WAN Protocol Control Settings page

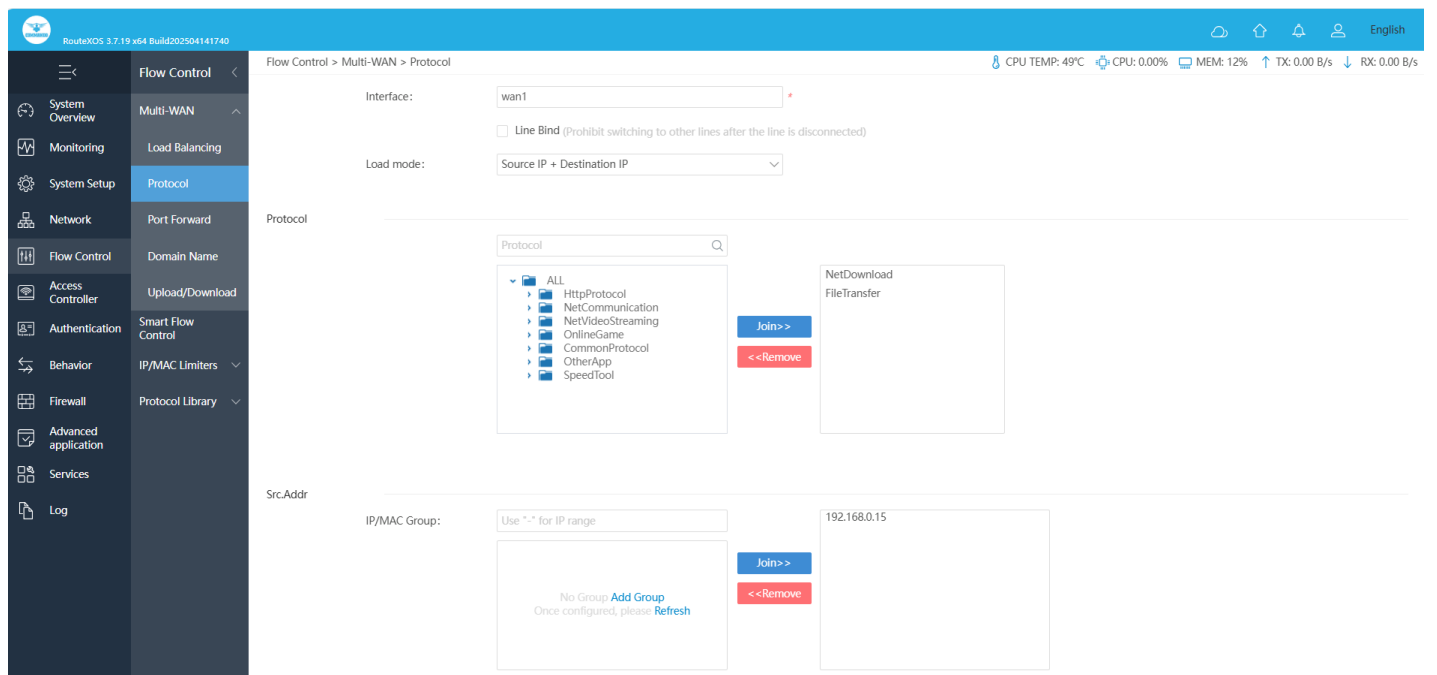


Fig 4.1.10 Add Details to Multi-WAN Protocol Control Settings page

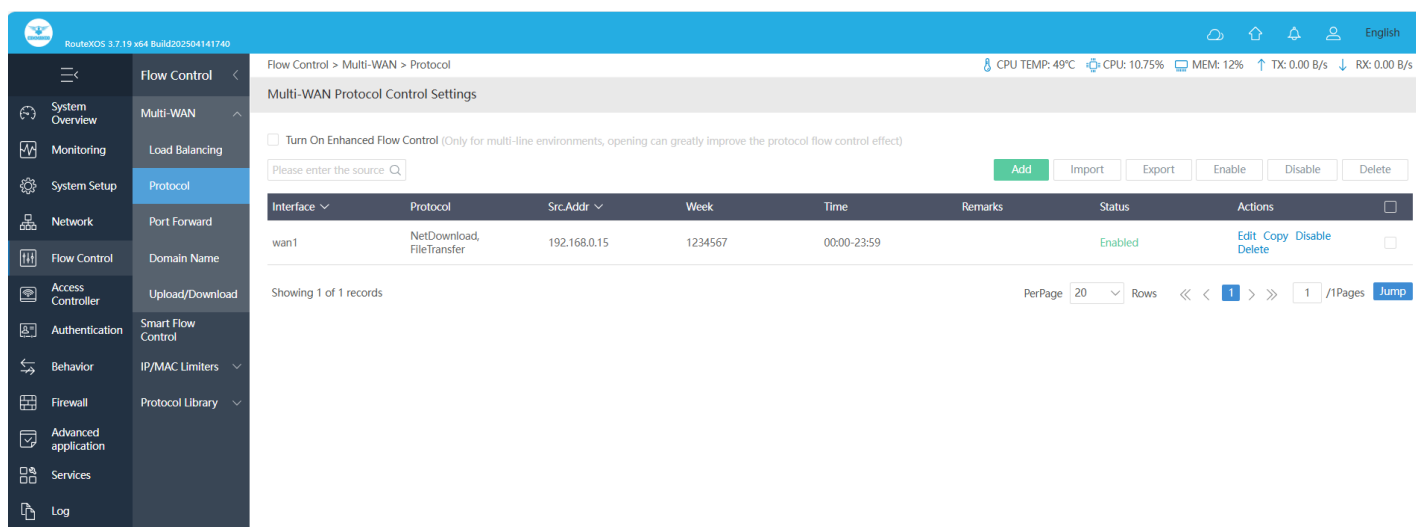


Fig 4.1.11 Multi-WAN Protocol Control Settings page

Multi-WAN Port Forwarding Settings: Each port forward applies to a single WAN interface. A given port can be opened on multiple WAN interfaces by using multiple port forward entries, one per WAN interface. 1:1 NAT entries are specific to a single WAN interface and, like outbound NAT, they only control what happens to the addresses on packets as they pass through an interface. Internal systems can be configured with a 1:1 NAT entry on each WAN interface, or a 1:1 entry on one or more WAN interfaces and use the default outbound NAT on others. Where 1:1 entries are configured, they always override any other Outbound NAT configuration for that specific interface.

If a local device must always use a 1:1 NAT entry on a specific WAN, then traffic from that device must be forced to use that specific WAN gateway

To configure Multi-WAN Port Forwarding Settings, click on Flow Control > Multi-WAN > Port Forward

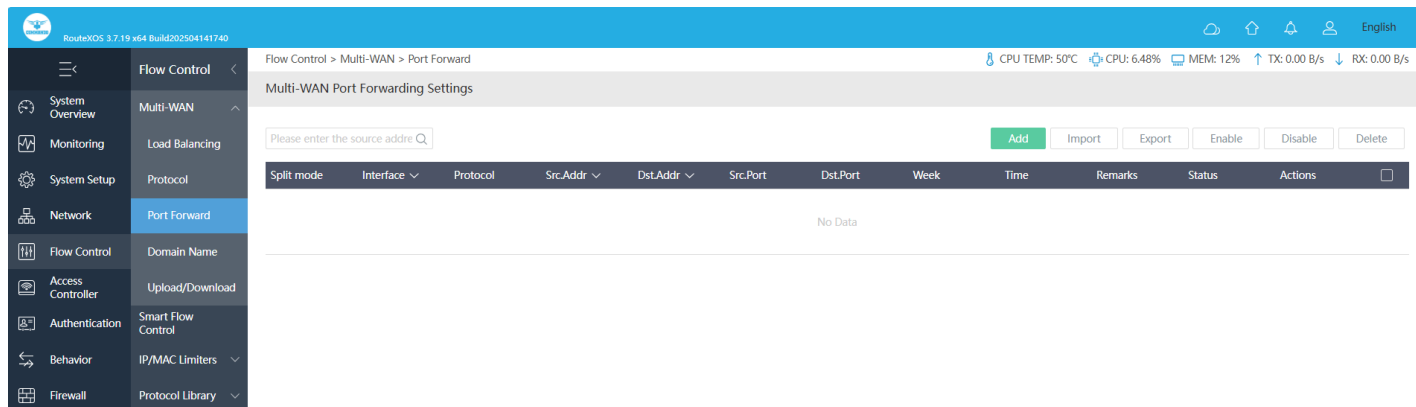


Fig 4.1.12 Default Multi-WAN Port Forwarding Settings page

RouteXOS 3.7.19 x64 Build202504141740

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

Multi-WAN

Load Balancing

Protocol

Port Forward

Domain Name

Upload/Download

Smart Flow Control

IP/MAC Limiters

Protocol Library

Flow Control > Multi-WAN > Port Forward

CPU TEMP: 49°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Split mode: External network line

Interface: *

☐ Line Bind (Prohibit switching to other lines after the line is disconnected)

Load mode: Number of new connections

Protocol: any

Src.Addr

IP/MAC Group: Use "*" for IP range

No Group Add Group Once configured, please Refresh

Join>>

<<Remove

Dst.Addr

IP/MAC Group: Use "*" for IP range

No Group Add Group Once configured, please Refresh

Join>>

<<Remove

Src.Port:

Dst.Port:

Remarks:

Week: ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Time: 00:00-23:59 *

Save Cancel

Fig 4.1.13 Add Multi-WAN Port Forwarding Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Port Forward

CPU TEMP: 50°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Split mode: External network line

Interface: wan1

☒ Line Bind (Prohibit switching to other lines after the line is disconnected)

Load mode: Source IP + Destination IP + Destination Port

Protocol: tcp+udp

Src.Addr

IP/MAC Group: Use "-" for IP range

COMMANDOMAC

COMMANDO

Join>>

<<Remove

Fig 4.1.14 Adding details to Multi-WAN Port Forwarding Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Port Forward

CPU TEMP: 50°C CPU: 0.74% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Multi-WAN Port Forwarding Settings

Please enter the source addr

Add Import Export Enable Disable Delete

Split mode	Interface	Protocol	Src.Addr	Dst.Addr	Src.Port	Dst.Port	Week	Time	Remarks	Status	Actions
External network line	wan1	tcp+udp	COMMANDO				1234567	00:00-23:59		Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 4.1.15 Multi-WAN Port Forwarding Settings page

Multi-WAN Domain Name Control Settings: Basically, our LAN is connected over the Internet through a multi-WAN Gateway, which will route local hosts over WAN1 to WAN4 depending on line overflow/fail and load setting you provided to Gateway. But local hosts will use a local DNS server, which might serve wrong or non-optimal resolution of IP addresses, giving unpredictable results and delays. If local Host-A might DNS query the local server (routed to WAN1), while the host requesting the name resolution is routed at the same time to WAN3. Multi-WAN Domain Name Control Settings is a way to keep settings, routing and DNS requests consistent. The DNS server can have knowledge where the requesting host will be routed for DNS resolution.

To configure Multi-WAN Domain Name Control Settings, Click on Flow Control > MultiWAN > Domain Name

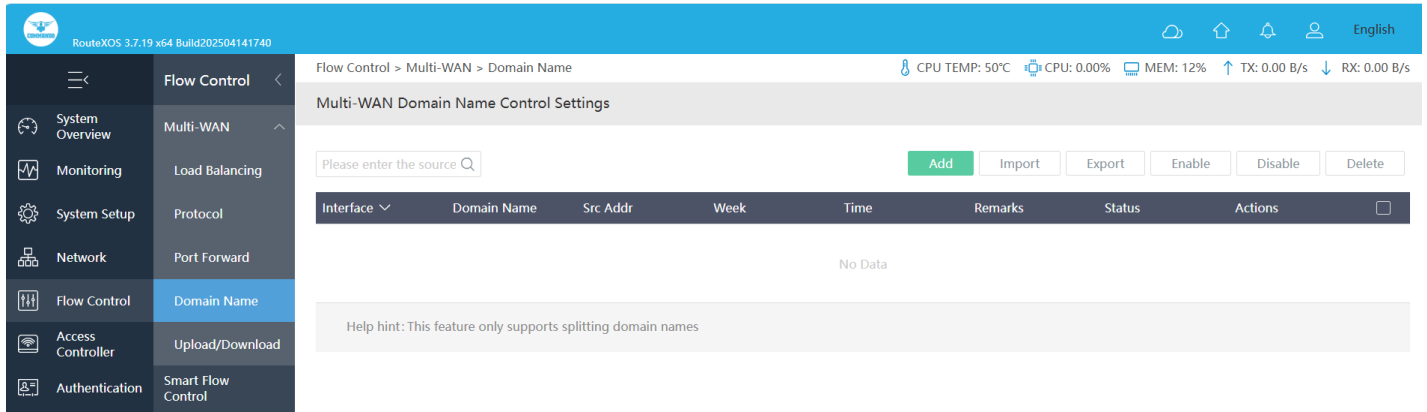


Fig 4.1.16 Default Multi-WAN Domain Name Control Settings page

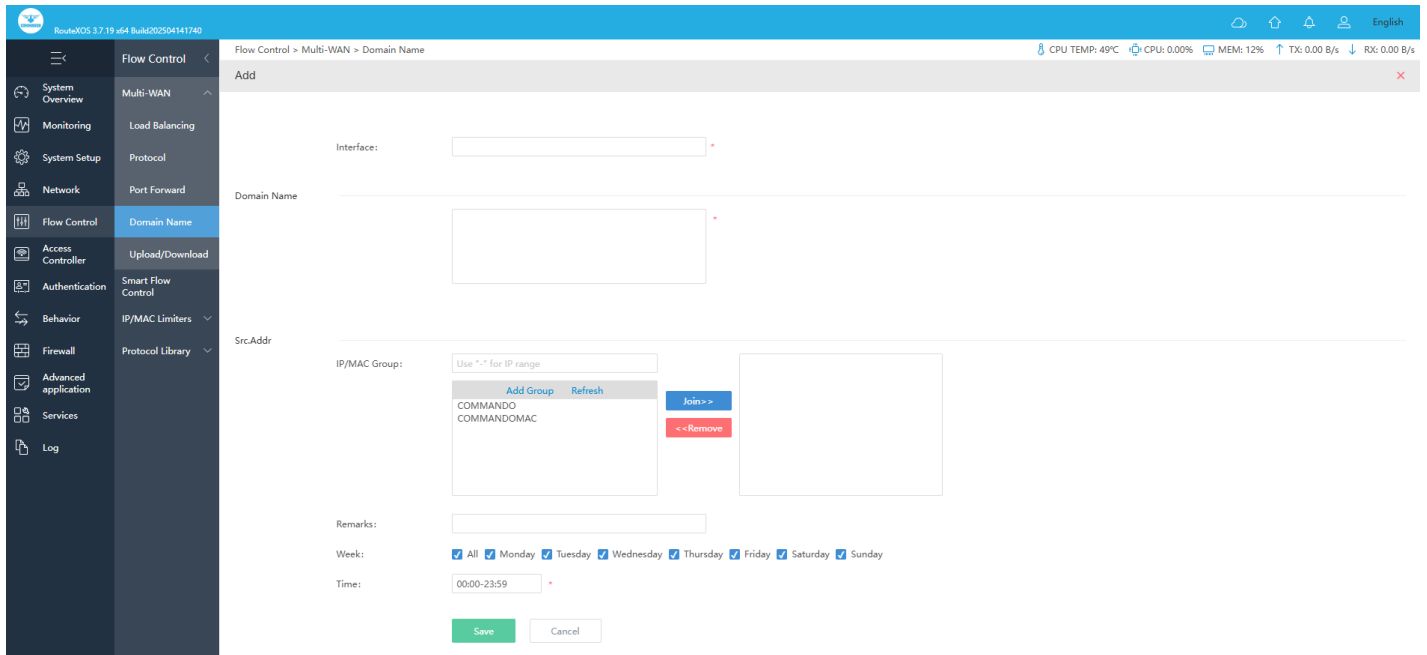


Fig 4.1.17 Add Multi-WAN Domain Name Control Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Domain Name

Interface:

Domain Name:

Src Addr:

IP/MAC Group:

Remarks:

Week: ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Time:

Fig 4.1.18 Details of Multi-WAN Domain Name Control Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Domain Name

Multi-WAN Domain Name Control Settings

Please enter the source

Interface	Domain Name	Src Addr	Week	Time	Remarks	Status	Actions
wan1.pptpCOMMANDO	www.commandonetworks.com	192.168.1.0/24 COMMANDO	1234567	00:00-23:59	COMMANDO Domain	Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

PerPage Rows / 1Pages

Help hint: This feature only supports splitting domain names

Fig 4.1.19 Multi-WAN Domain Name Control Settings page

strong> Multi-WAN

Upload and Download Control Settings: Implement upload traffic and download traffic on separated transmission, only after the upload traffic matches the policy rule, the downstream traffic of the upstream traffic request data will return according to the download line specified by the rule. (The ratio for the multiple lines is 1:1). For other line configurations (default gateway, multi-line load, and offload settings), there is actually no functional priority association. This function belongs to the “effective policy after

matching”. This function takes effect only after matching the upload data rule. And the priority is the highest according to the effect of use.

For configuration of Multi-WAN Upload and Download Control Settings, Click on flow Control > Multi-WAN > Upload/Download

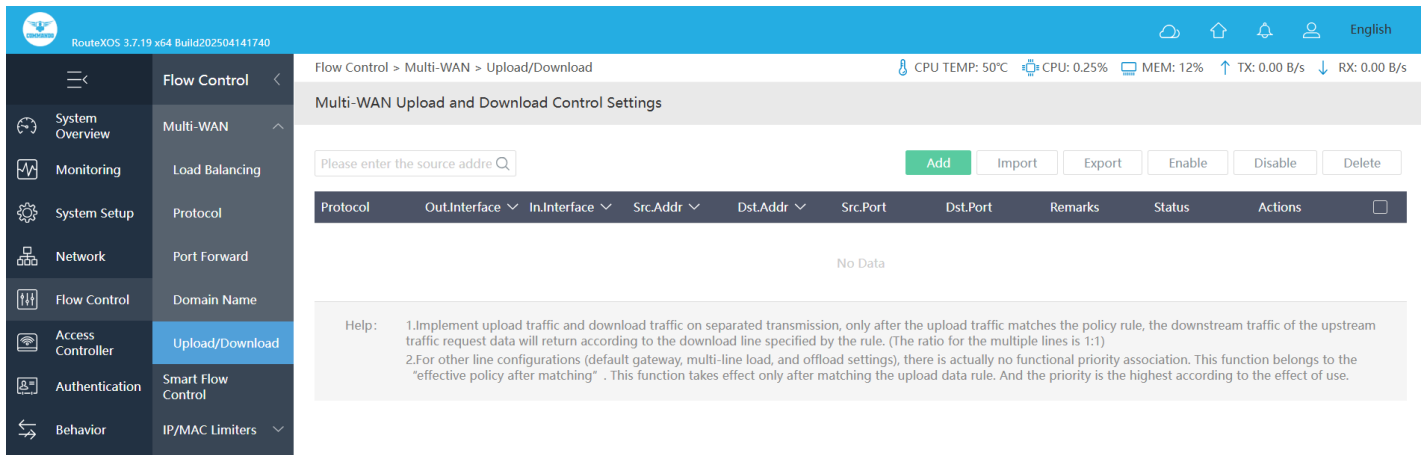


Fig 4.1.20 Multi-WAN Upload and Download Control Settings page

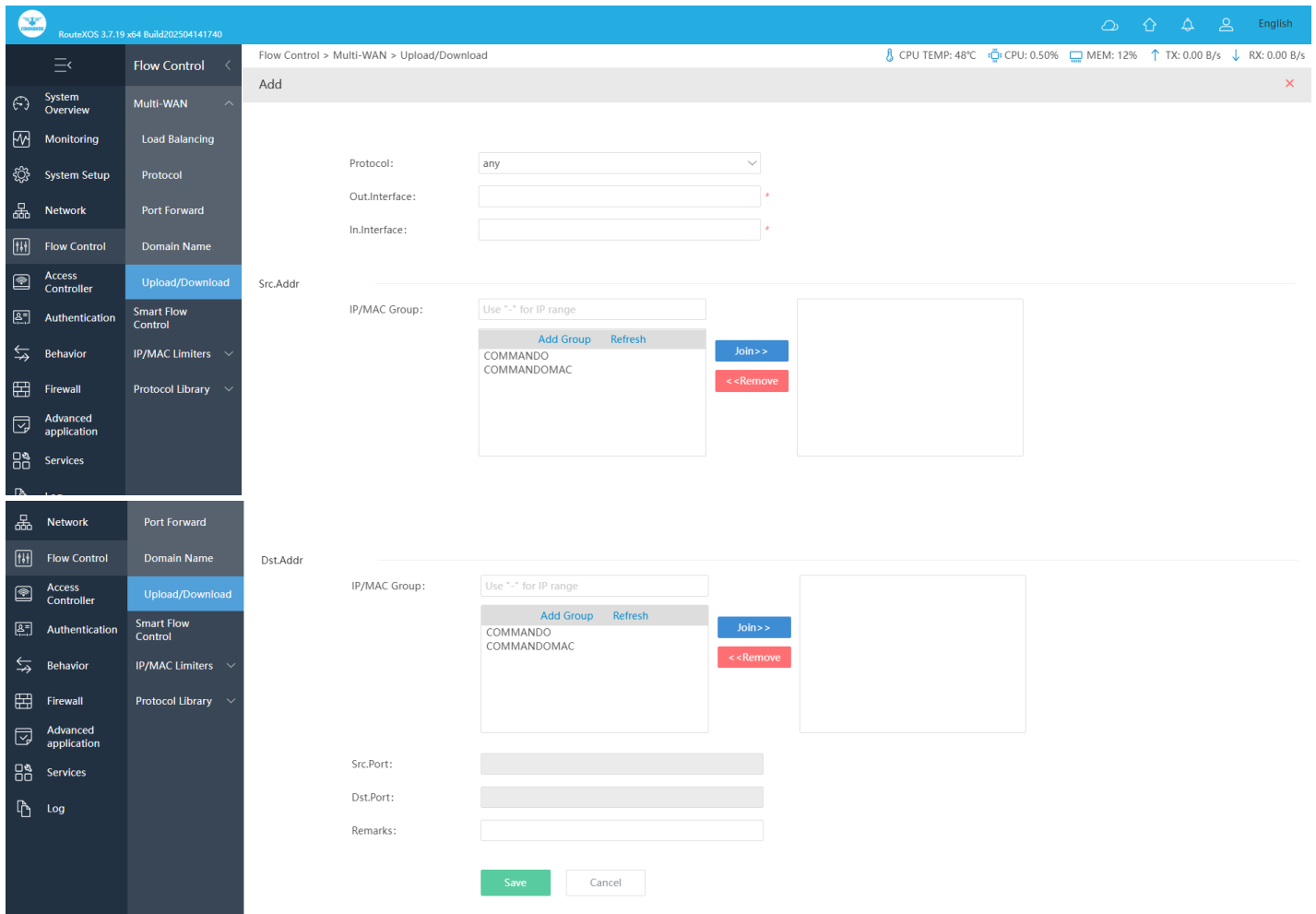


Fig 4.1.21 Add Multi-WAN Upload and Download Control Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Upload/Download

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Protocol: tcp+udp

Out.Interface: wan1

In.Interface: wan1

Src.Addr

IP/MAC Group: Use "*" for IP range

COMMANDO

Join >>

<< Remove

Dst.Addr

IP/MAC Group: Use "*" for IP range

COMMANDO

Join >>

<< Remove

Src.Port:

Dst.Port:

Remarks: COMMANDO Upload

Save Cancel

Fig 4.1.22 Details for Multi-WAN Upload and Download Control Settings page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Multi-WAN > Upload/Download

CPU TEMP: 50°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Multi-WAN Upload and Download Control Settings

Please enter the source address

Add Import Export Enable Disable Delete

Protocol	Out.Interface	In.Interface	Src.Addr	Dst.Addr	Src.Port	Dst.Port	Remarks	Status	Actions
tcp+udp	wan1	wan1	COMMANDO	COMMANDOMAC			COMMANDO Upload	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 / 1 Pages Jump

Help: 1.Implement upload traffic and download traffic on separated transmission, only after the upload traffic matches the policy rule, the downstream traffic of the upstream traffic request data will return according to the download line specified by the rule. (The ratio for the multiple lines is 1:1)
2.For other line configurations (default gateway, multi-line load, and offload settings), there is actually no functional priority association. This function belongs to the "effective policy after matching". This function takes effect only after matching the upload data rule. And the priority is the highest according to the effect of use.

Fig 4.1.23 Multi-WAN Upload and Download Control Settings page

4.2 Smart Flow Control

Smart Flow Control Settings is an appropriate flow control strategy can improve network performance by using the available resources efficiently and by alleviate congestion and to obtain an efficient network performance. Head-of-line (HOL) blocking problem can occur in

the FIFO queue and Round-Robin (RR)-based scheduling mechanism. In the HOL blocking, when the first packet in buffer queues is blocked, the other packets behind them cannot pass through the lines even if there are enough resources. Therefore, network performance is reduced severely in the presence of HOL blocking. Enabling flow control can optimize the bandwidth and improve the network experience of important applications, especially in the bandwidth environment

Intelligent mode: Simple and fast intelligent flow control mode, suitable for the vast majority of network environment, official comprehensive cloud big data optimization flow control configuration recommended.

Manual mode: Users with a deep understanding of the convective control function and their own network environment are relatively complex and support more customization options.

Note: Opening this feature will increase the performance of Gateway for specific applications.

To configure Smart Flow Control Settings, Click on Flow Control > Smart Flow Control

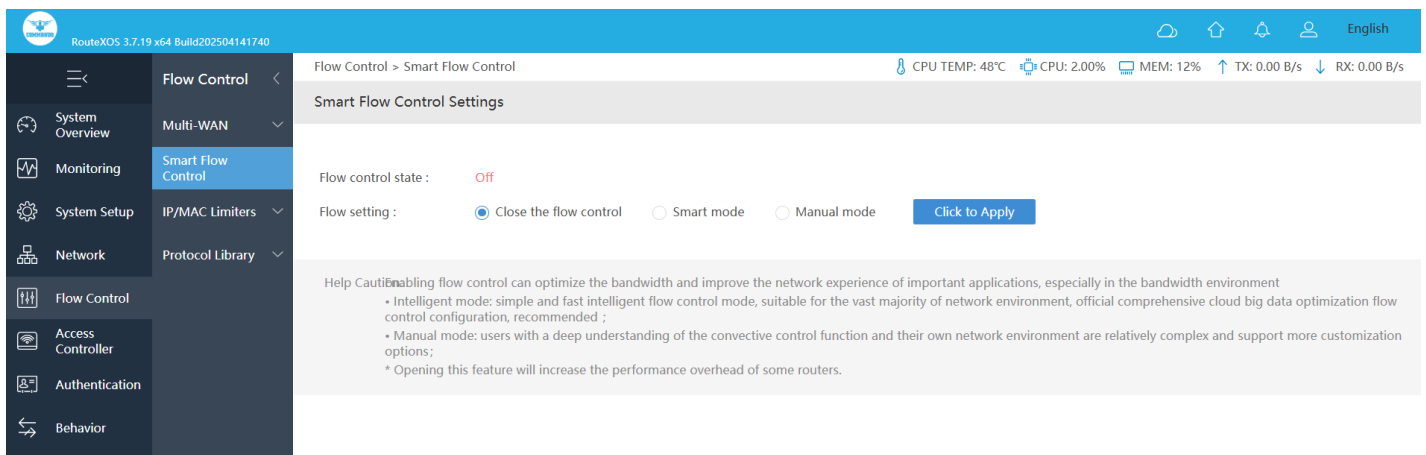


Fig 4.2.1 Default Flow Control Settings page

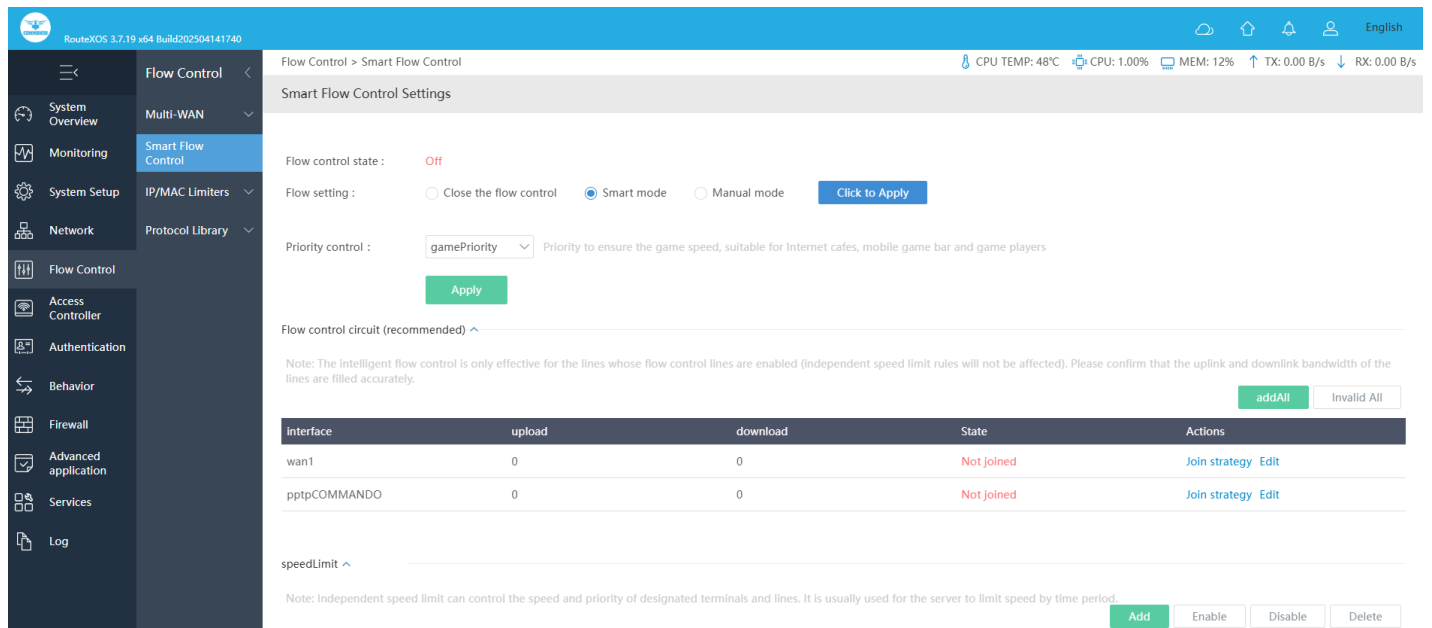


Fig 4.2.2 Smart Flow Control Settings page

Custom: Current protocol priority (Adjustment can be made according to need, after modification, it needs to be applied). Priority represents the status of different types of traffic in system forwarding, high priority forwarding, low priority.

Webpage Priority: Priority is given to ensuring the speed of web access. It is recommended to use the office network environment.

Game Priority: Priority to ensure the game speed, suitable for Internet cafes, mobile game bar and game players.

Video Priority: Priority should be given to ensuring video and live application speed, suitable for users with such entertainment needs.

Download Priority: It is preferred to use the bandwidth for all kinds of download software, please select carefully if there is no special requirement.

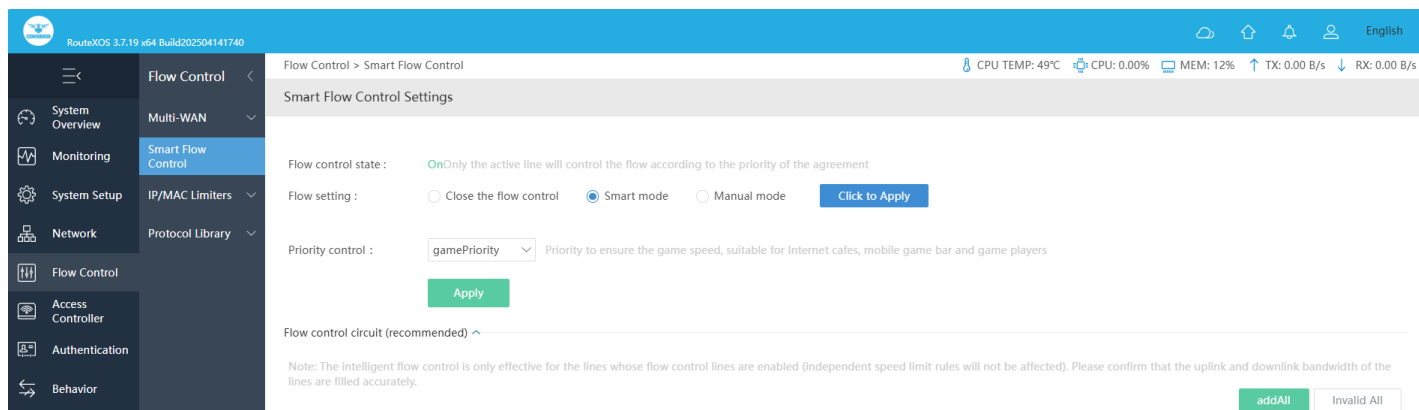


Fig 4.2.3 Default game Priority in Smart Flow Control Settings page

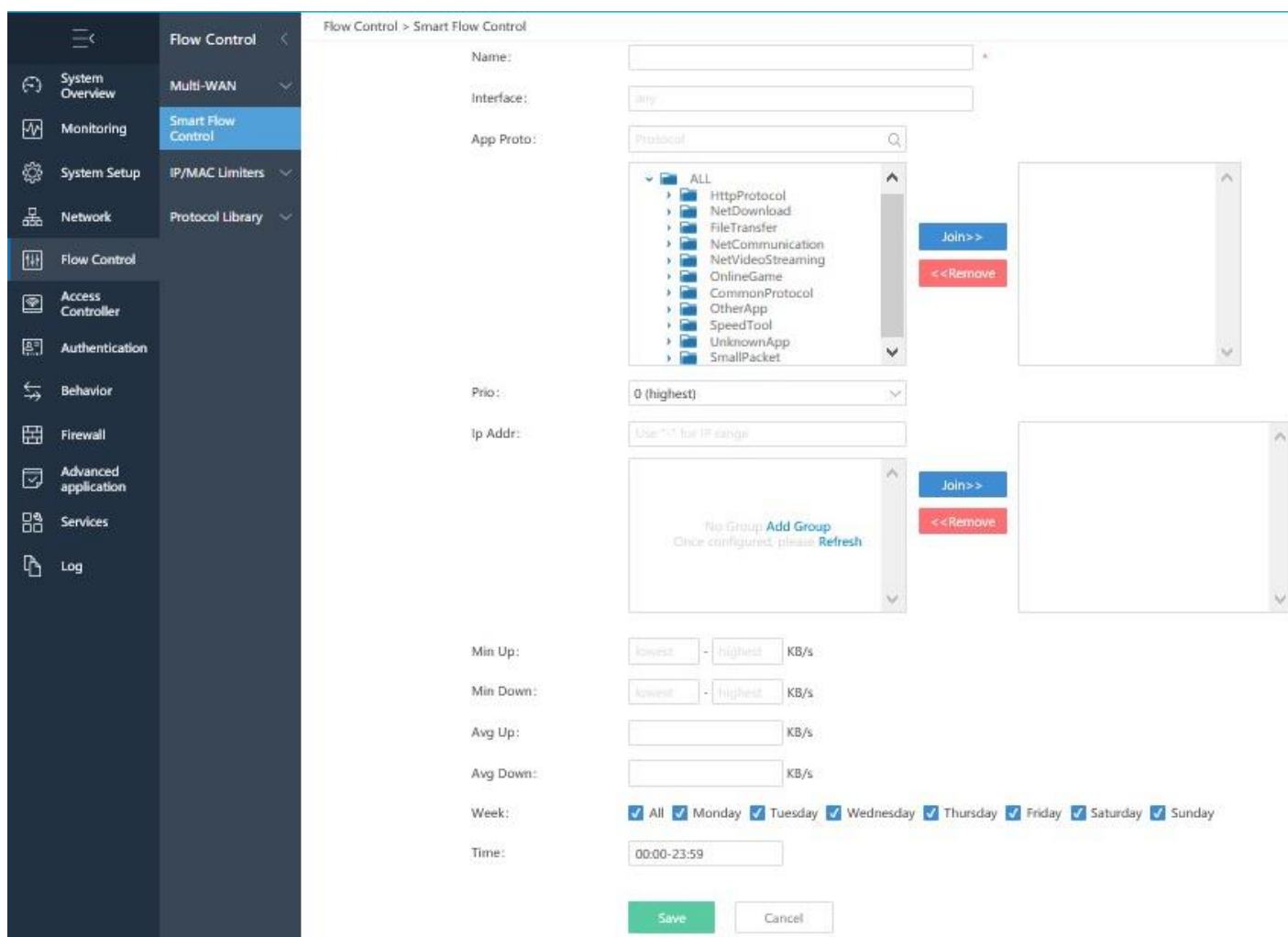


Fig 4.2.4 Add Smart Flow Control Settings page

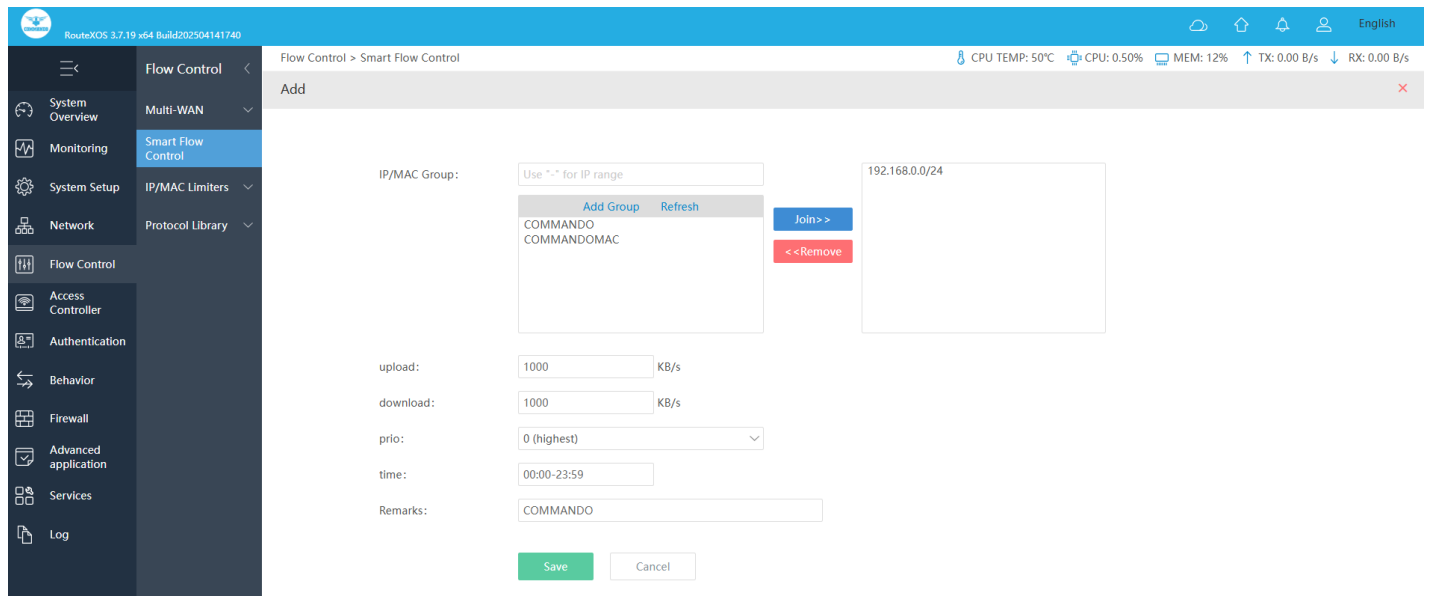


Fig 4.2.5 Changing Smart Flow Control Settings page

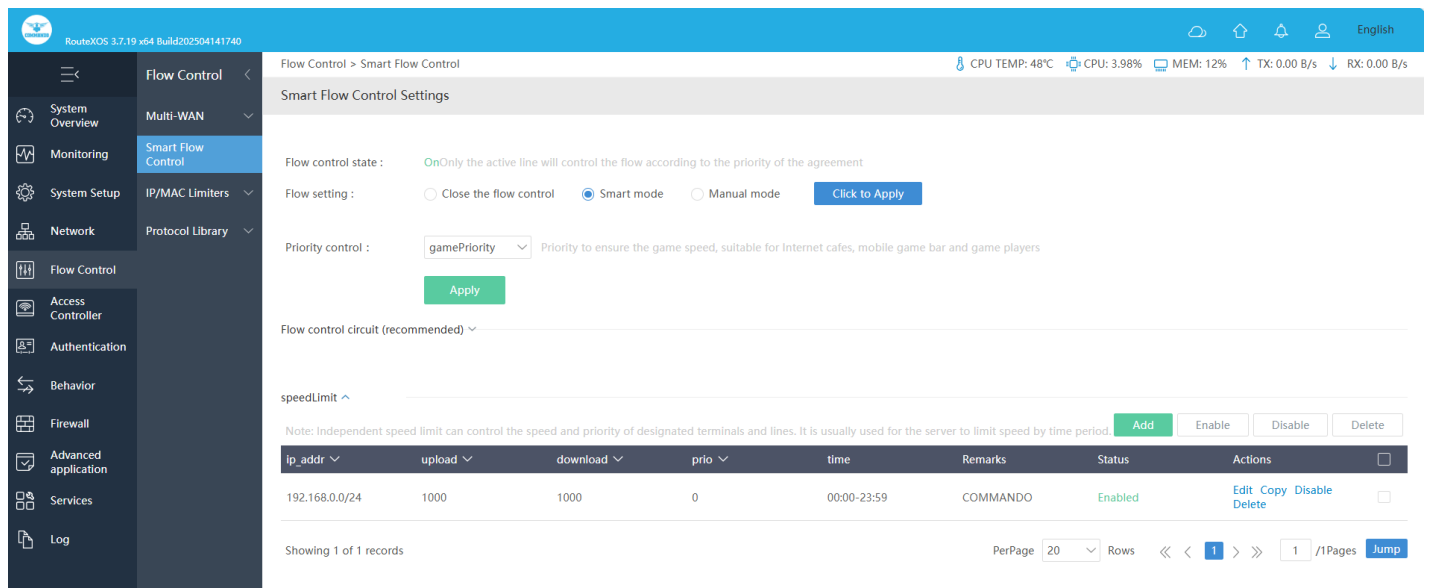


Fig 4.2.6 Smart Flow Control Settings page

4.3 IP/MAC Limiters

Traffic Control functions to control the bandwidth by configuring rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized. Speed limit enables the user to allow and control the amount of bandwidth they're allowed to use and let you control network traffic and set a maximum bandwidth transfer speed limit for IP or MAC address.

Speed Limiter Using IP Address: Limit bandwidth on your Gateway to control those devices of particular IP address. Each device will be allowed only maximum bandwidth set.

To configure Speed Limiter Using IP Address, Click on Flow Control > IP/MAC Limiters > IP Limiter

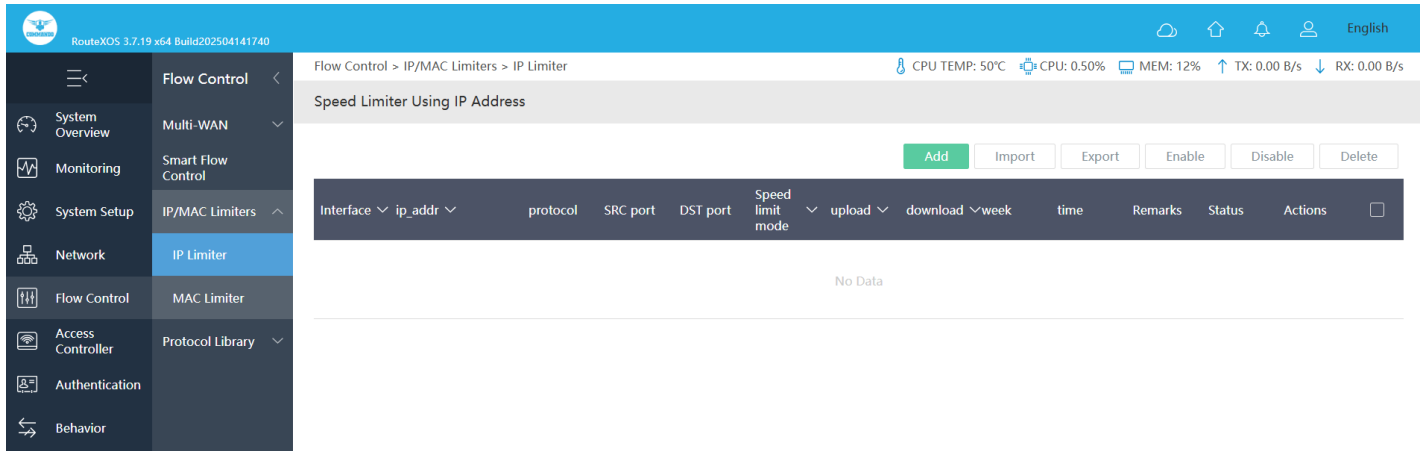


Fig 4.3.1 Default Speed Limiter Using IP Address page

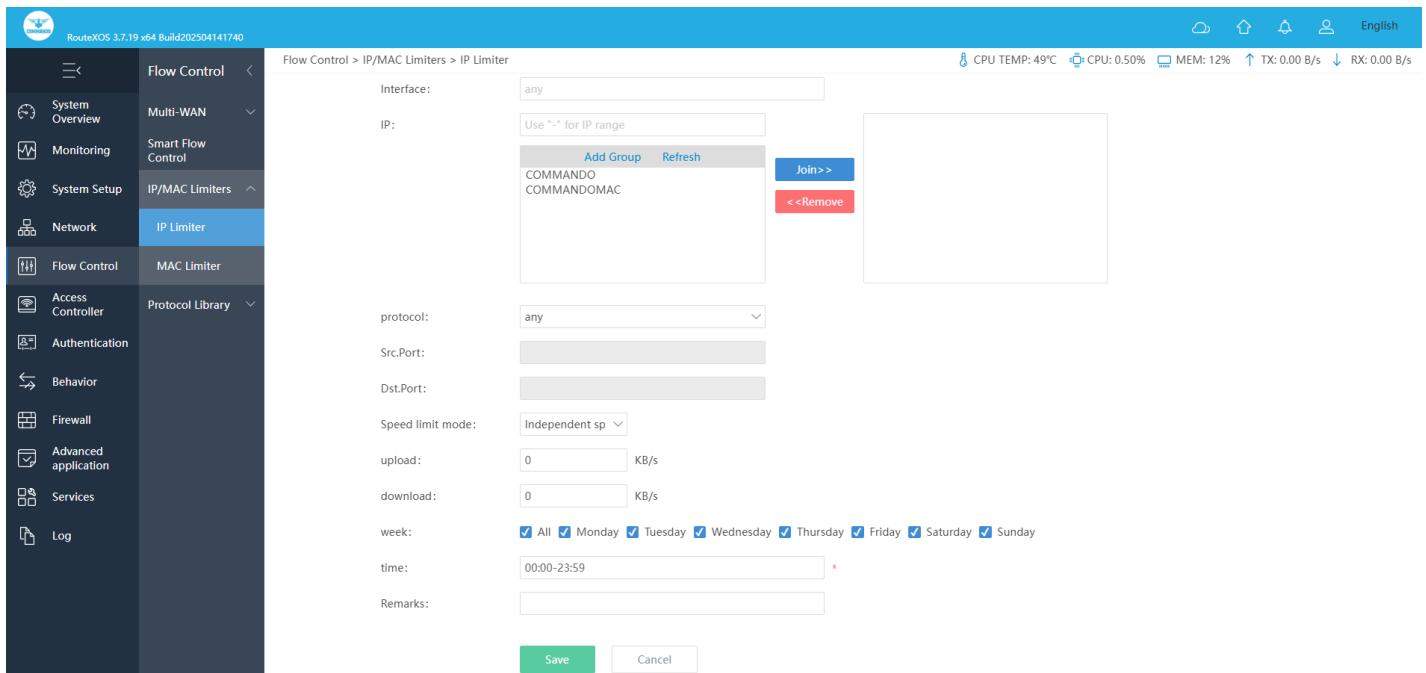


Fig 4.3.2 Add Speed Limiter Using IP Address page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > IP/MAC Limiters > IP Limiter

Interface: wan1

IP: 192.168.0.10

protocol: tcp+udp

Src.Port:

Dst.Port:

Speed limit mode: Independent sp

upload: 1000 KB/s

download: 100 KB/s

week: ☐ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday ☐ Sunday

time: 00:00-23:59

Remarks: Setting speed limit

Save Cancel

Fig 4.3.3 Speed Limiter for Particular IP Address Page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > IP/MAC Limiters > IP Limiter

Speed Limiter Using IP Address

Add Import Export Enable Disable Delete

Interface	ip_addr	protocol	SRC port	DST port	Speed limit mode	upload	download	week	time	Remarks	Status	Actions
wan1	192.168.0.10	tcp+udp			Independent speed limit	1000	100	12345	00:00-23:59	Setting speed limit	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 / 1 Pages Jump

Fig 4.3.4 Speed Limiter Using IP Address Page Speed

Limiter Using MAC Address: Limit bandwidth on your Gateway to control those devices of particular MAC address. Each device will be allowed only maximum bandwidth set.

To configure Speed Limiter Using IP Address, Click on Flow Control > IP/MAC Limiters > MAC Limiter

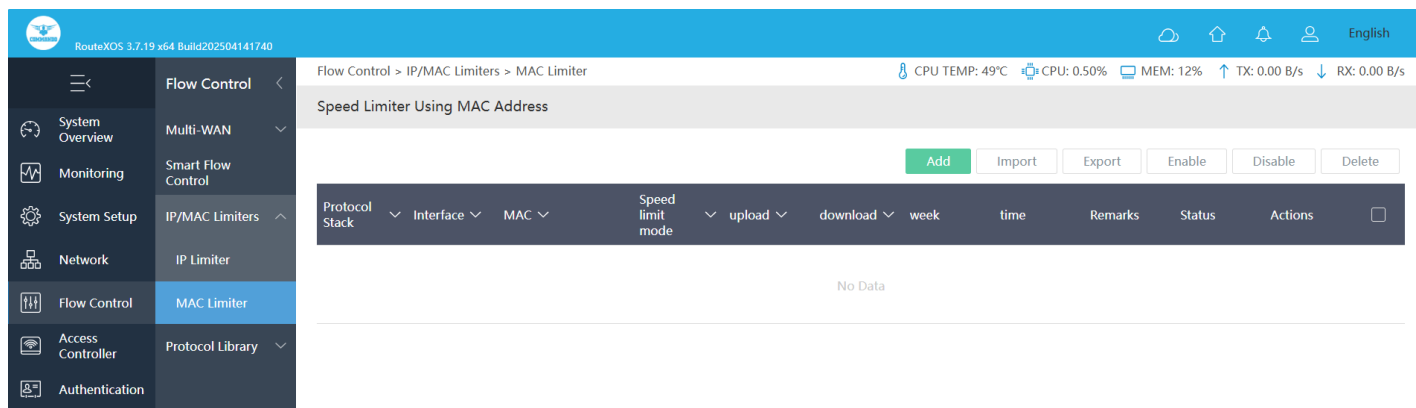


Fig 4.3.5 Default Speed Limiter Using MAC Address page

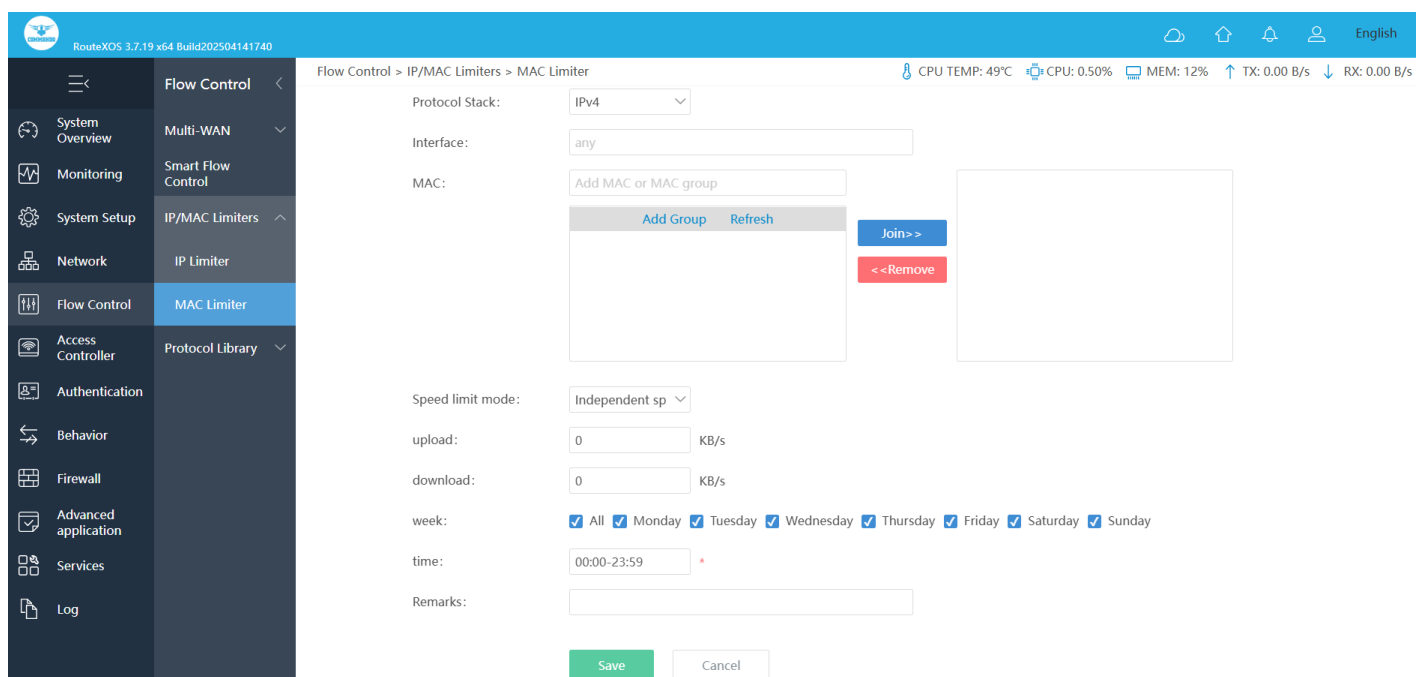


Fig 4.3.6 Add Speed Limiter Using MAC Address page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > IP/MAC Limiters > MAC Limiter

CPU TEMP: 50°C CPU: 2.49% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Interface: wan1

MAC: Add MAC or MAC group

COMMANDOMAC

No Group Add Group Once configured, please Refresh

Join> <<Remove

Speed limit mode: Independent sp

upload: 1000 KB/s

download: 10000 KB/s

week: All Monday Tuesday Wednesday Thursday Friday Saturday Sunday

time: 00:00-23:59

Remarks: COMMANDO MAC Address Speed Limit

Save Cancel

Fig 4.3.7 Speed Limiter For COMMANDOMAC Group MAC Address

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > IP/MAC Limiters > MAC Limiter

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Speed Limiter Using MAC Address

Add Import Export Enable Disable Delete

Protocol Stack	Interface	MAC	Speed limit mode	upload	download	week	time	Remarks	Status	Actions
IPv4	wan1	COMMANDOMAC	Independent speed limit	1000	10000	1234567	00:00-23:59	COMMANDO MAC Address...	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 4.3.8 Speed Limiter for COMMANDOMAC Group page

4.4 Protocol Library

Network Based Application Recognition recognizes and classifies network traffic on the basis of a set of protocols and application types. You can add to the set of protocols and application types that classifies network traffic by protocol or application. Creating custom protocols is an optional process. However, custom protocols extend the capability to classify and monitor additional static port applications and allow you to classify non supported static port traffic.

To set Customized Protocol, Click on Flow Control > Protocol Library > Custom Protocol

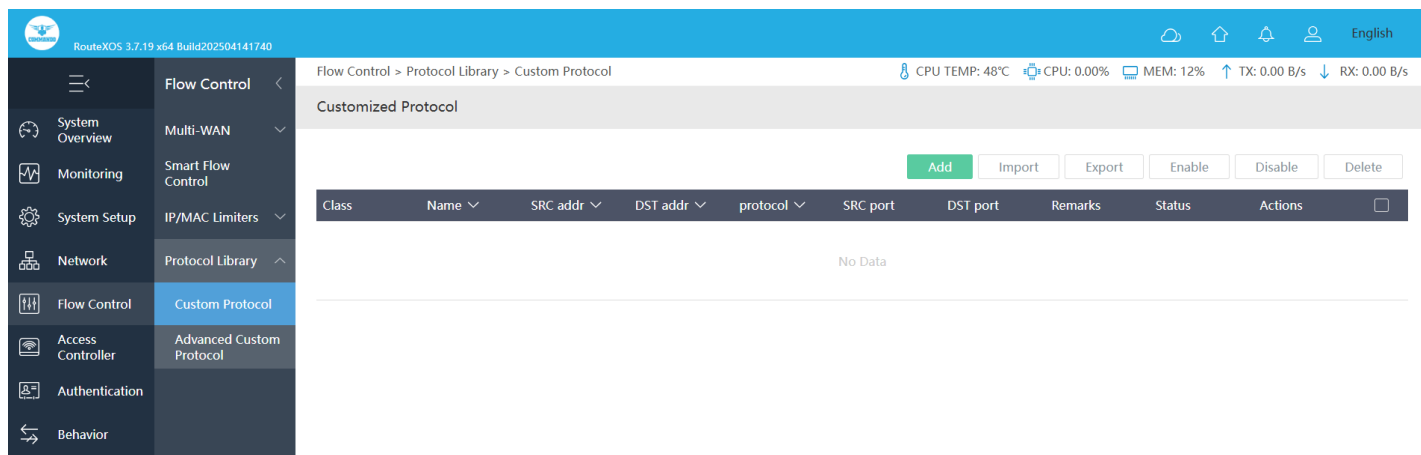


Fig 4.4.1 Default Customized Protocol page

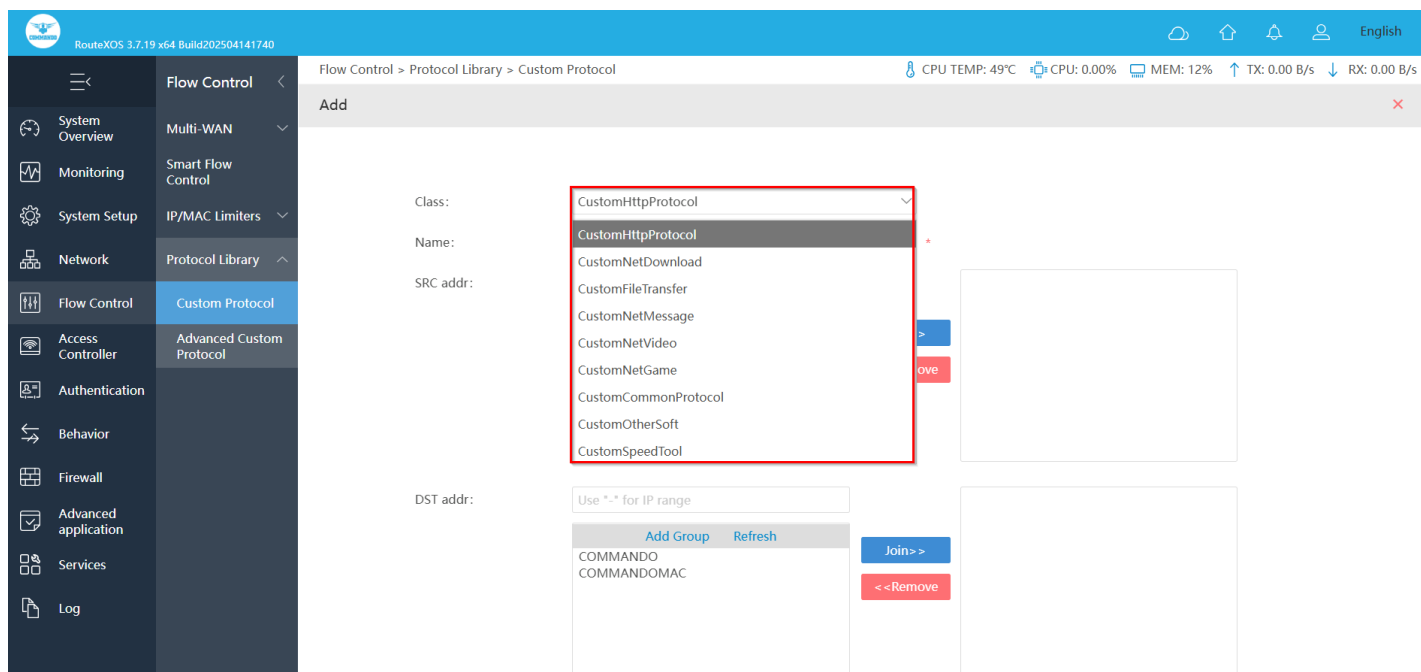


Fig 4.4.2 Add Customized Protocol page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Protocol Library > Custom Protocol

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Class: CustomFileTransfer

Name: FileCOMMANDO

SRC addr: Use *.* for IP range

192.168.0.0/24

COMMANDO
COMMANDOMAC

Join>> <<Remove

DST addr: Use *.* for IP range

192.168.1.0/24

COMMANDO
COMMANDOMAC

Join>> <<Remove

protocol: tcp+udp

Src.Port:

Dst.Port:

Remarks:

Save Cancel

Fig 4.4.3 Customized Protocol for particular source and destination address page

RouteXOS 3.7.19 x64 Build202504141740

Flow Control > Protocol Library > Custom Protocol

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Customized Protocol

Add Import Export Enable Disable Delete

Class	Name	SRC addr	DST addr	protocol	SRC port	DST port	Remarks	Status	Actions
CustomFileTransfer	FileCOMMANDO	192.168.0.0/24	192.168.1.0/24	tcp+udp				Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 / 1 Pages Jump

Fig 4.4.4 Customized Protocol page

Advanced Custom Protocol Settings: It supports the use of custom protocols to identify custom applications. Custom protocols support static port-based protocols. It can have custom applications can be assigned and each custom application can have up TCP and UDP ports each mapped to the individual custom protocol.

To configure Advanced Custom Protocol Settings, Click on Flow Control > Protocol Library > Advanced Custom Protocol

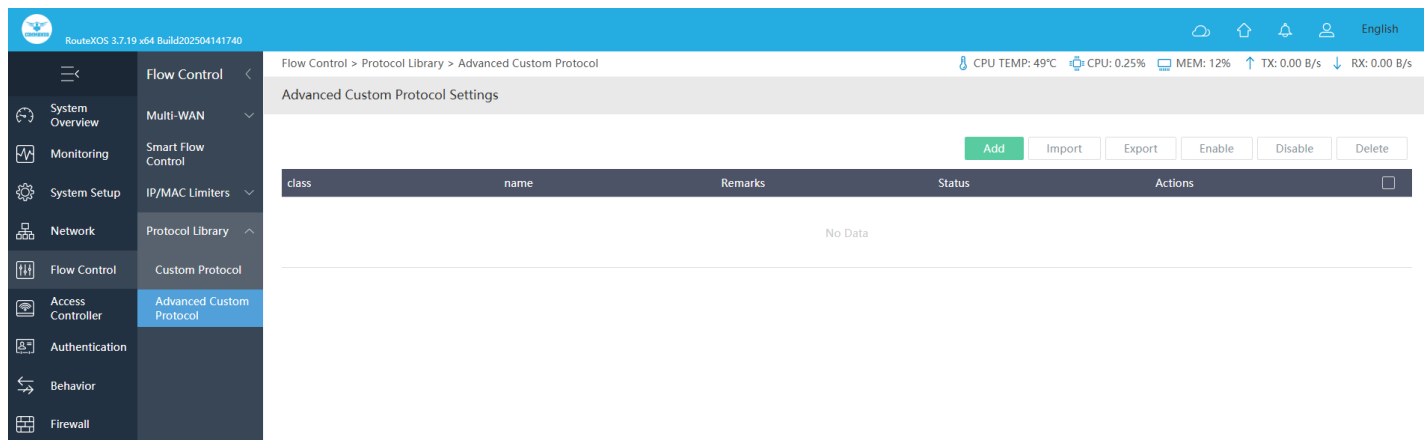


Fig 4.4.5 Default Advanced Custom Protocol page

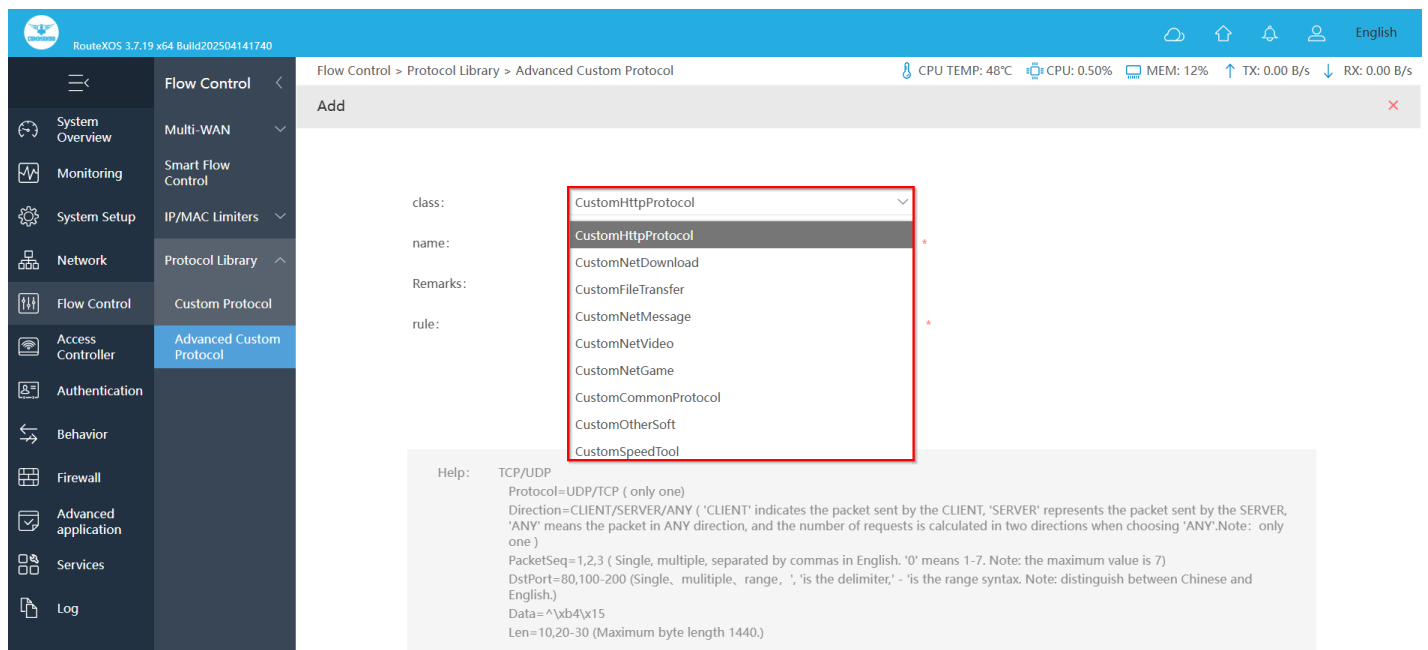


Fig 4.4.6 Add Advanced Custom Protocol page

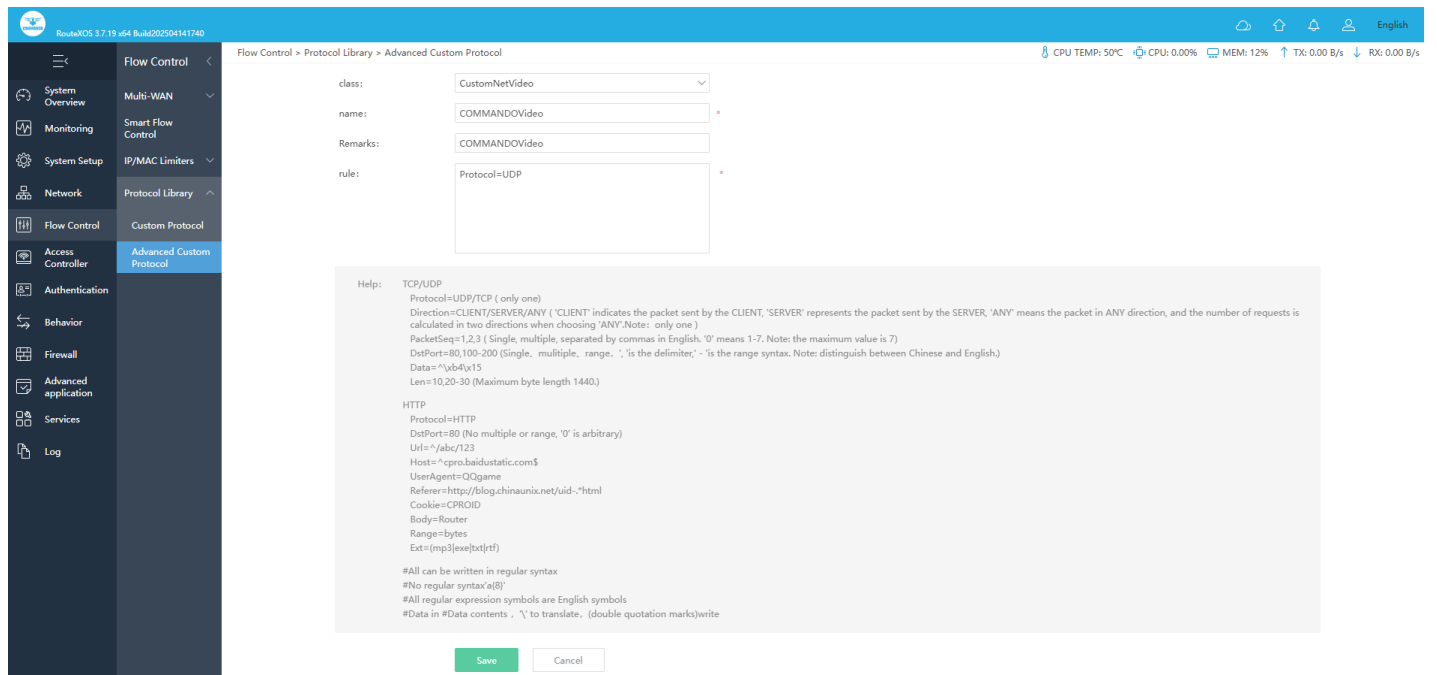


Fig 4.4.7 Advanced Custom Protocol setting for video page

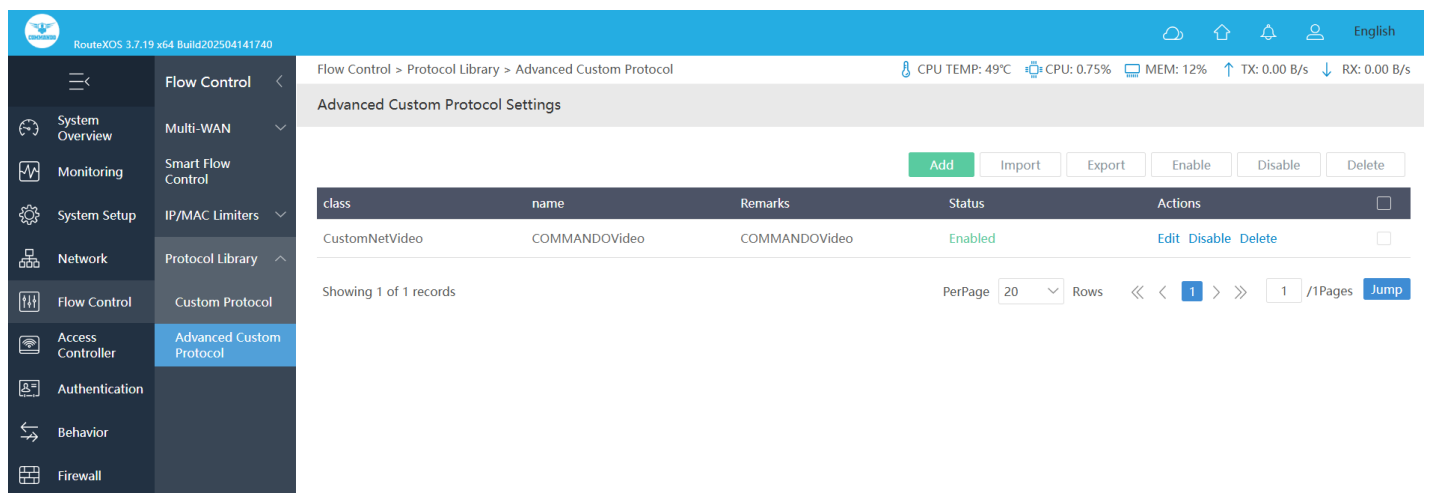


Fig 4.4.8 Advanced Custom Protocol page

ACCESS CONTROLLER

The wireless controller can discover peer wireless AP regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to different IP subnet. When the controller discovers and validates AP, the controller takes over the management of the AP.

Wireless overview: It shows running AP status, terminal statistics, wireless Network Rating, traffic statistics with average rate, terminal association details, network transmission quality.

AP Configuration: It shows all groupings, status, frequency of AP. You can do Interference Analysis and configure Terminal detail along with peripheral channel scanning.

AP group: Group name is required to group AP. AP that join the group use the group configuration uniformly.

AP Firmware Upgrades: You can view the current firmware version of connected AP's & latest if any under this option. Select the Batch online upgrade/ Batch local upgrade option to upgrade all AP's.

Wireless black and white list: You can Blacklist AP to Disable the MAC connection specified SSID or Whitelist AP along with all users associate with it.

User Information: You can view User Information like IP Address, MAC, AP Information, SSID, Signal, Connect Time, Transmission and Receive rate along with connected wireless device name and details.

Wireless Terminal VLAN: Allows segmentation of wireless clients into different VLANs for enhanced security, traffic management, and access control.

Wireless Network Optimization: Improves wireless performance by automatically adjusting channels, transmission power, and interference settings for a stable and efficient connection.

Common terms used in Access Controller are as follows.

Restart AP: Restart the selected AP from the list.

Reset AP: Restore selected AP to factory default.

Delete AP: Delete the chosen wireless AP from the list.

Refresh: Refresh the displayed AP List.

All Device: Show the complete list of wireless AP connected to this controller

Online Device: Show the list of wireless AP which are online

Offline Device: Show the list of wireless AP which are offline

Device IP: The wireless AP's IP address

MAC Address: MAC address of wireless AP

SSID: Shows the SSID of wireless AP

Users: Shows how many users are connected with wireless AP

Status: Displays if AP is Online/ Offline

Channel: Shows the wireless AP channel, including both the frequency bands.

AP Model: Model number of wireless AP

AP Version: Display AP firmware version

Uptime: Display running time of AP

Black White List: AP Mac address can be Black/white List to allow/ block access to respective AP's and all users associated with it.

Config: You can edit/ modify the configuration of respective AP under this option

5.1 Wireless overview

A WLAN controller manages wireless network access points that allow wireless devices to connect to the network. You can view running AP status, terminal statistics, wireless Network Rating, traffic statistics with average rate, terminal association details, network transmission quality.

To view Wireless overview, Click on **Access Controller > Wireless overview**

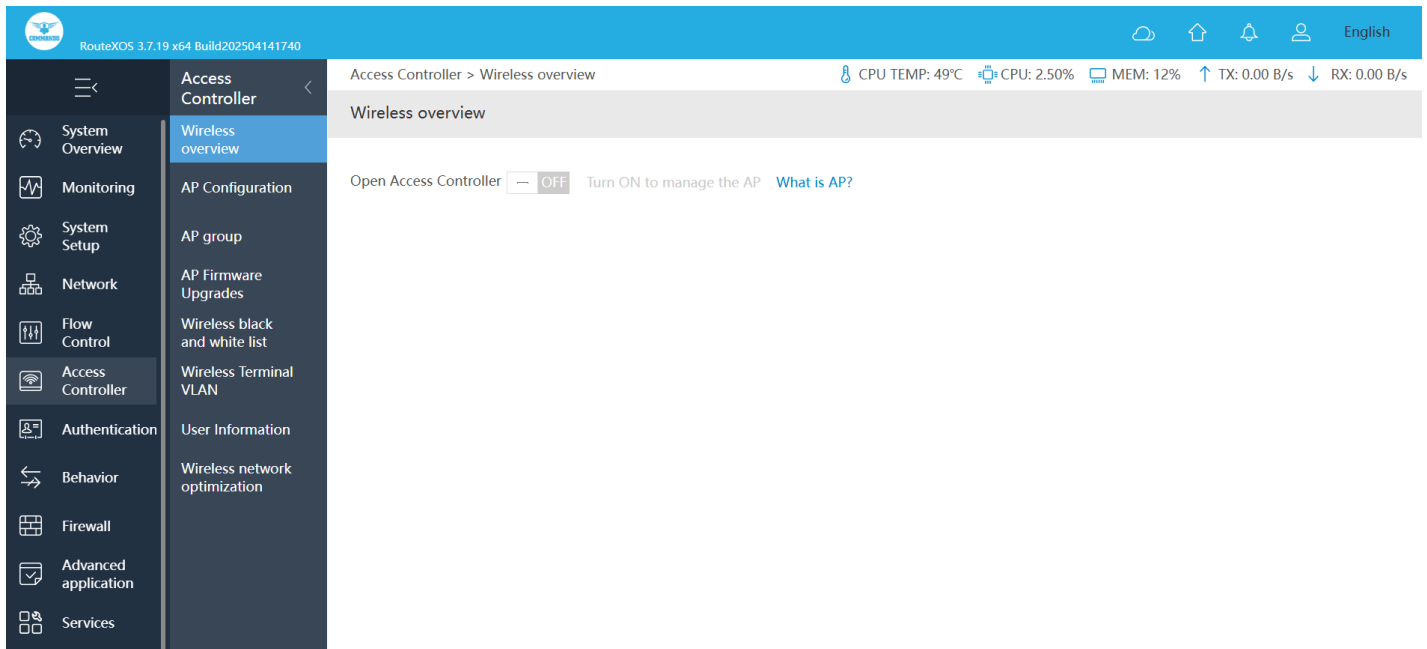


Fig 5.1.1 Default Wireless overview OFF page

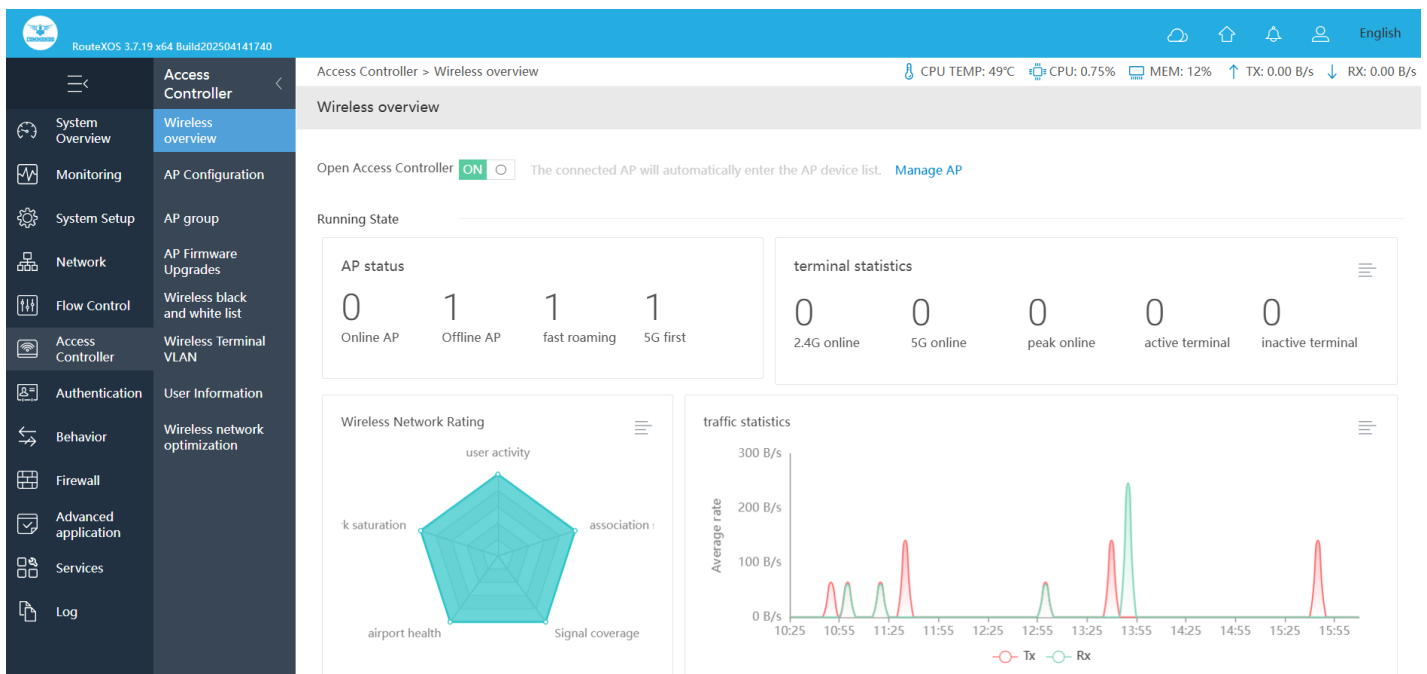


Fig 5.1.2 Default Wireless overview ON page

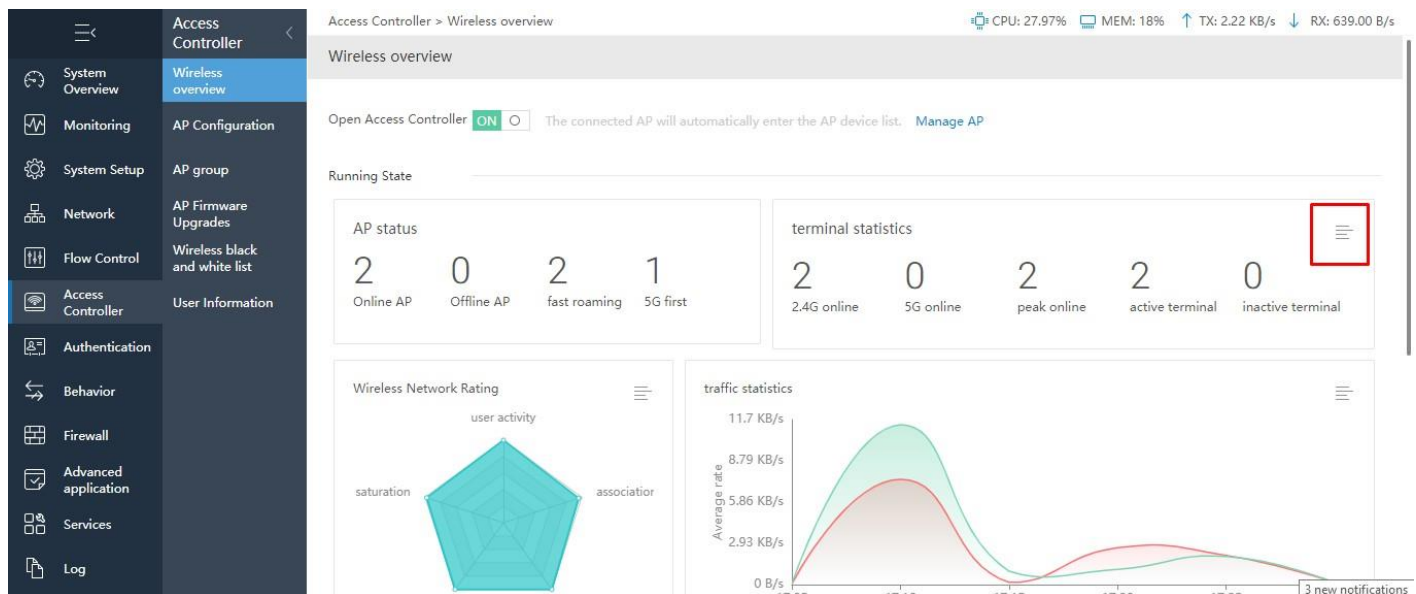


Fig 5.1.3 Wireless overview after connecting AP and users' page

After clicking above highlighted icon following page will be displayed

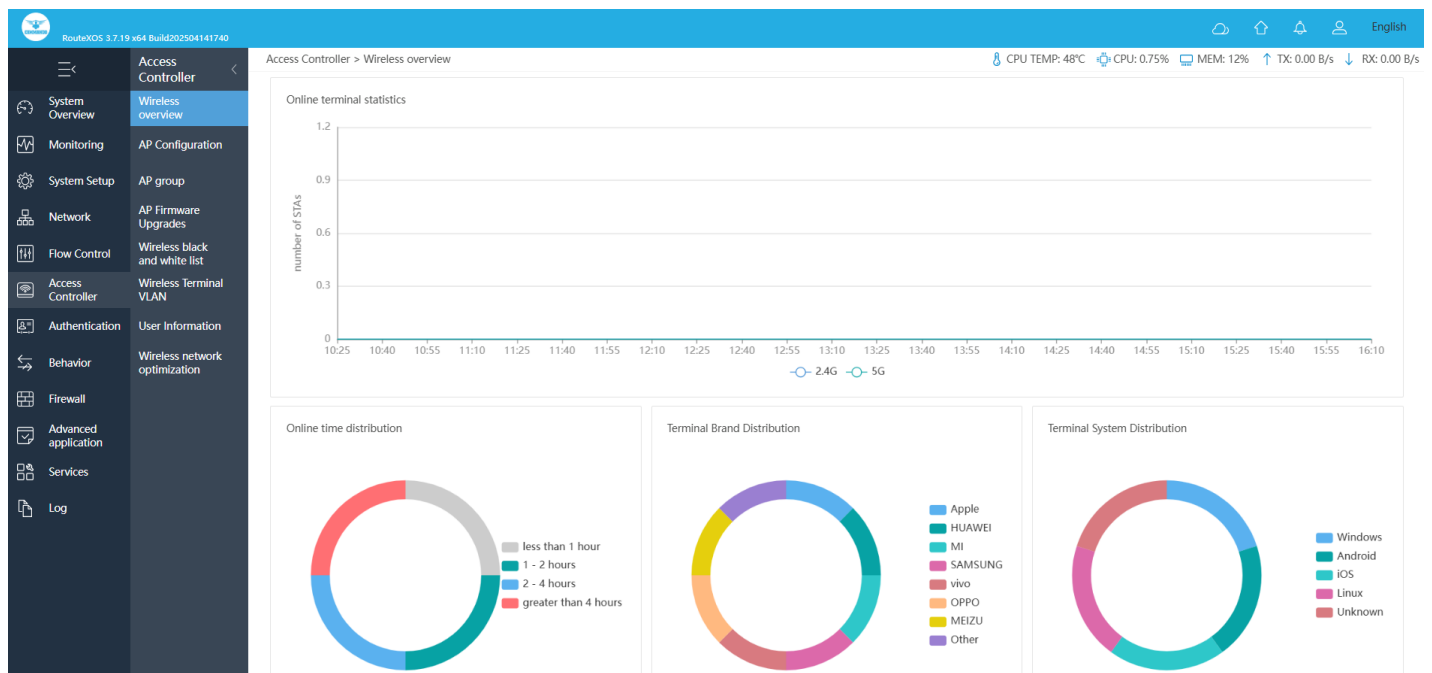


Fig 5.1.4 Online terminal statistics, distribution, System page

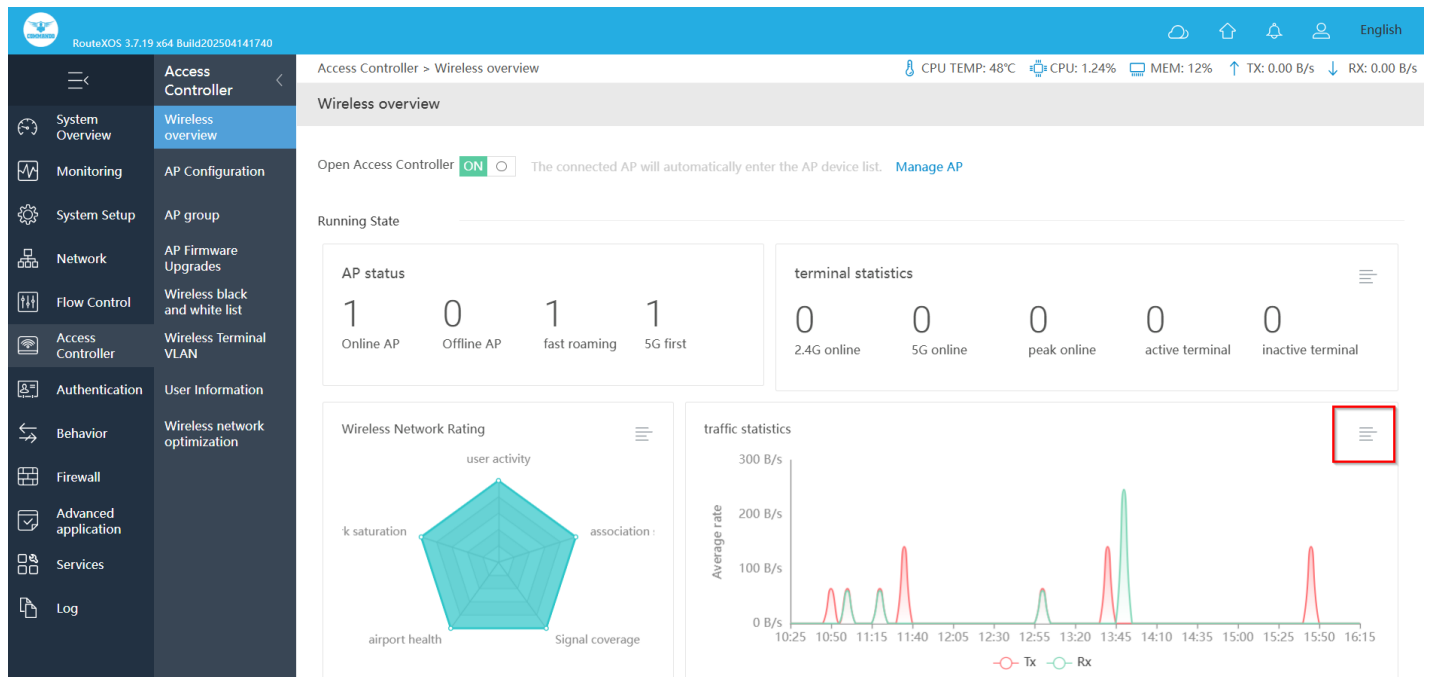


Fig 5.1.5 Traffic statistics page

After clicking above highlighted icon following page will be displayed

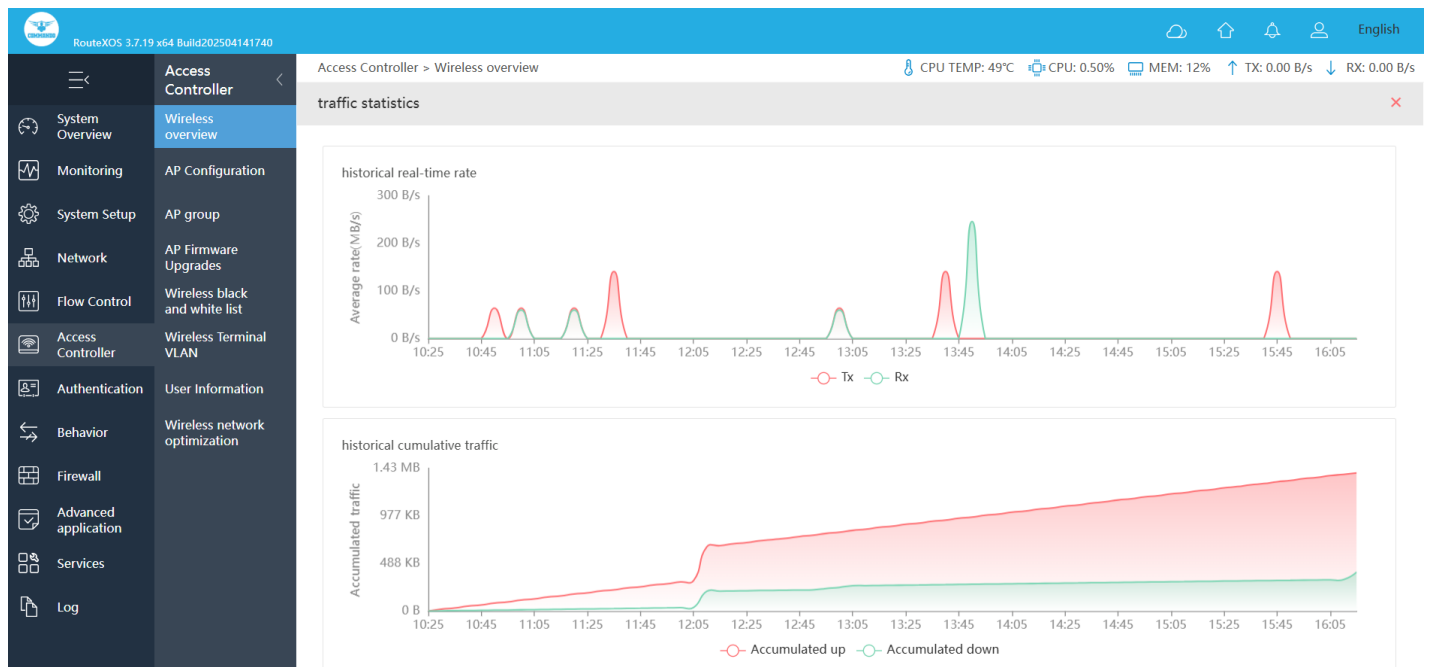


Fig 5.1.6 Traffic statistics with historical real-time rate, cumulative traffic page

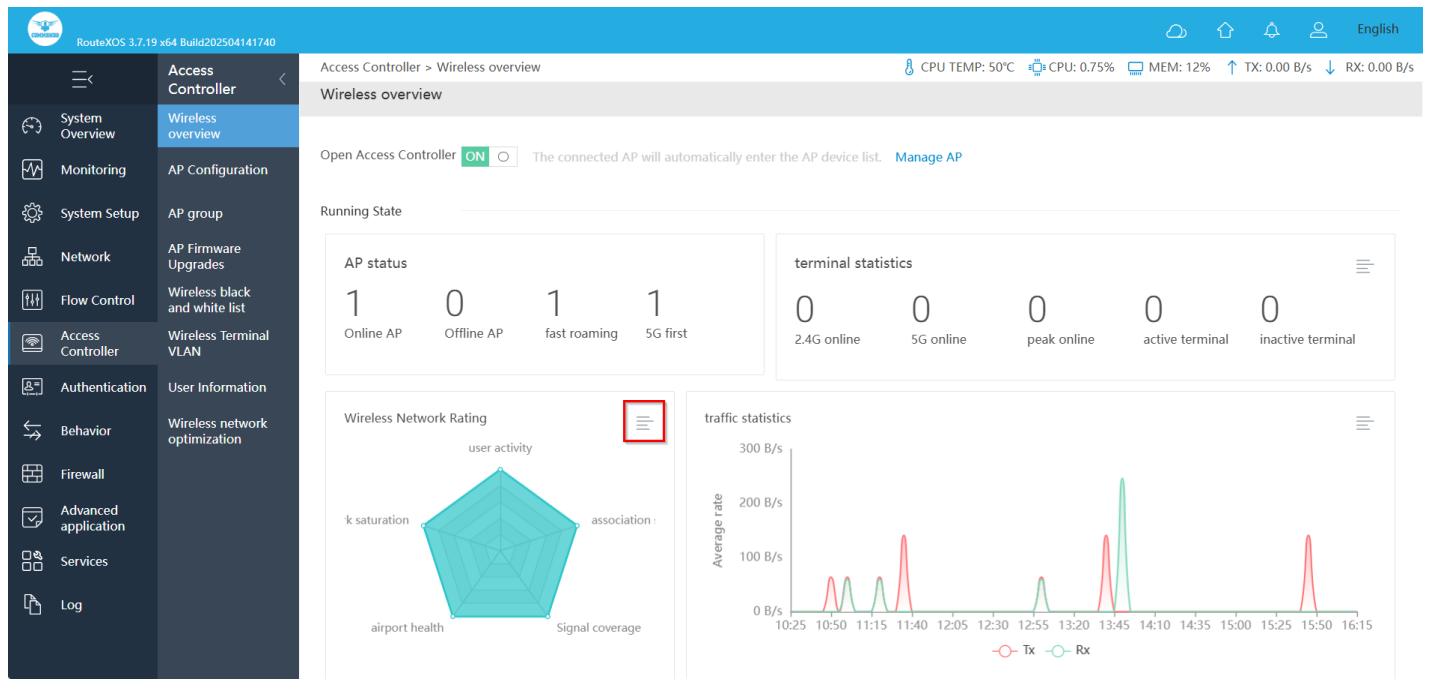


Fig 5.1.7 Wireless Network Rating page

After clicking above highlighted icon following page will be displayed



Fig 5.1.8 Wireless Network Rating channel and terminal environment page

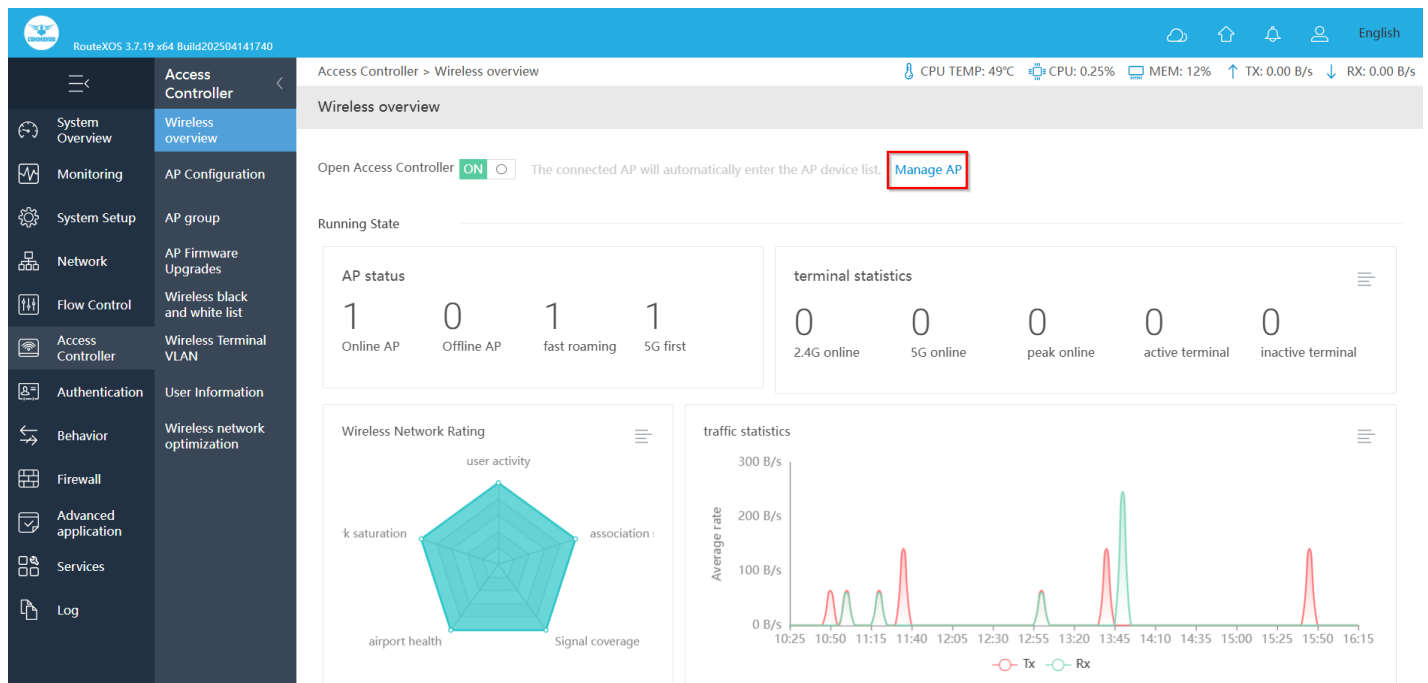


Fig 5.1.9 Open Access Controller Manage AP page

It will direct with Access Controller > AP Configuration page.

5.2 AP Configuration

Access

Point Configuration: You can view the AP configuration with Terminal details and to modify AP Details and editing. You can Join group and Peripheral channel scanning. The wireless controller can discover peer wireless AP regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to a different IP subnet. When the controller discovers and validates AP, the controller takes over the management of the AP automatically.

For Access Point Configuration, click on Access Controller > AP Configuration

Note: List automatically refreshes every 10 seconds and stops refreshing when the mouse moves to the list or check the checkbox. The APs that join the group support the separate configuration part option, and the individual configuration priority is higher than

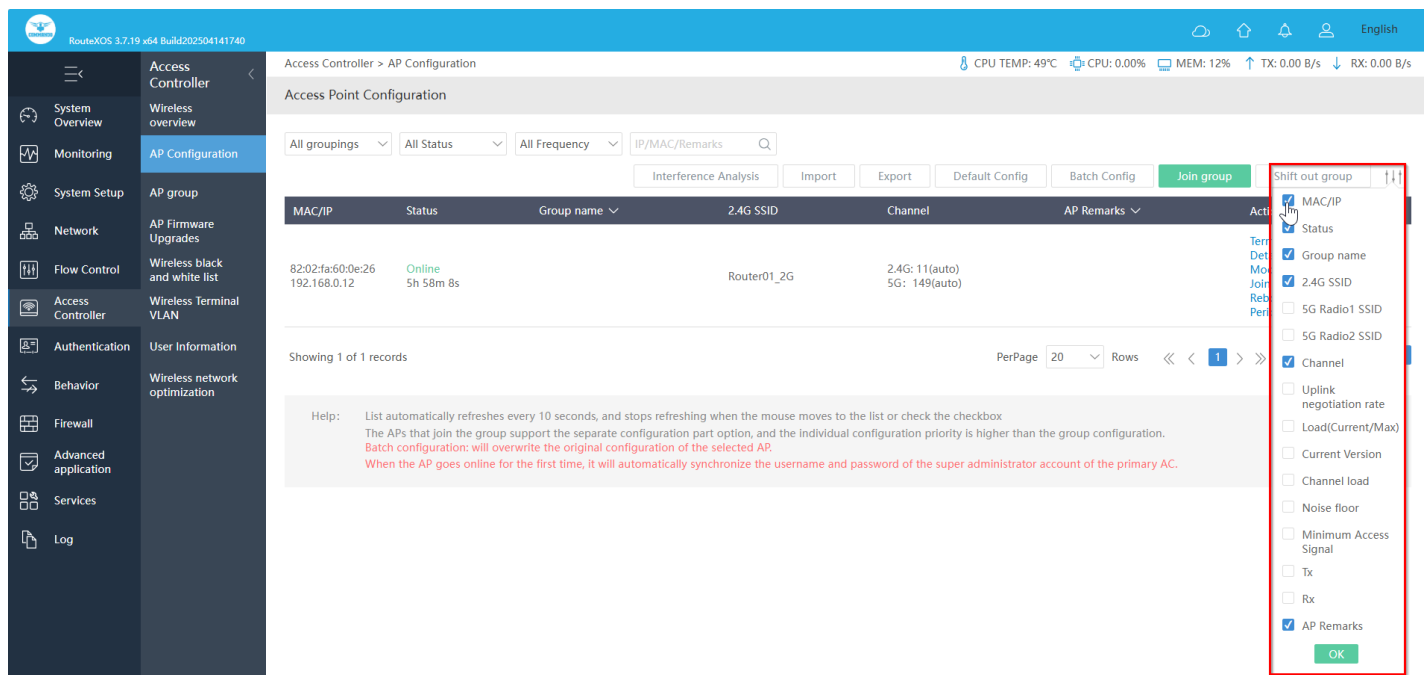
the group configuration. Batch configuration will overwrite the original configuration of the selected AP.

The screenshot shows the 'Access Point Configuration' page in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar contains navigation options: System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Access Controller' section is expanded, showing 'Wireless overview' and 'AP Configuration'. The main content area displays a table of Access Points with columns: MAC/IP, Status, Group name, 2.4G SSID, Channel, AP Remarks, and Actions. A single AP is listed with MAC/IP 82:02:fa:60:0e:26, Status Online, Group name Router01_2G, 2.4G SSID 192.168.0.12, and Channel 2.4G: 11(auto) 5G: 149(auto). The Actions column includes links for Terminal details, Details and editing, Modify comment, Join group, Locate, Reboot, and Peripheral channel scanning. Below the table, it shows 'Showing 1 of 1 records' and pagination controls. A help message at the bottom states: 'List automatically refreshes every 10 seconds, and stops refreshing when the mouse moves to the list or check the checkbox. The APs that join the group support the separate configuration part option, and the individual configuration priority is higher than the group configuration. Batch configuration: will overwrite the original configuration of the selected AP. When the AP goes online for the first time, it will automatically synchronize the username and password of the super administrator account of the primary AC.'

Fig 5.2.1 Default Access Point Configuration page

The screenshot shows the 'Access Point Configuration' page in the RouteXOS 3.7.19 x64 Build202504141740 interface, similar to Fig 5.2.1. The left sidebar and navigation options are the same. The main content area displays a table of Access Points with columns: MAC/IP, Status, Group name, 2.4G SSID, Channel, AP Remarks, and Actions. A single AP is listed with MAC/IP 82:02:fa:60:0e:26, Status Online, Group name Router01_2G, 2.4G SSID 192.168.0.12, and Channel 2.4G: 11(auto) 5G: 149(auto). The Actions column includes links for Terminal details, Details and editing, Join group, Locate, Reboot, and Peripheral channel scanning. Below the table, it shows 'Showing 1 of 1 records' and pagination controls. A help message at the bottom states: 'List automatically refreshes every 10 seconds, and stops refreshing when the mouse moves to the list or check the checkbox. The APs that join the group support the separate configuration part option, and the individual configuration priority is higher than the group configuration. Batch configuration: will overwrite the original configuration of the selected AP. When the AP goes online for the first time, it will automatically synchronize the username and password of the super administrator account of the primary AC.'

Fig 5.2.2 Access Point Configuration Online/Offline AP page



5.2.3 Access Point Configuration Default AP page

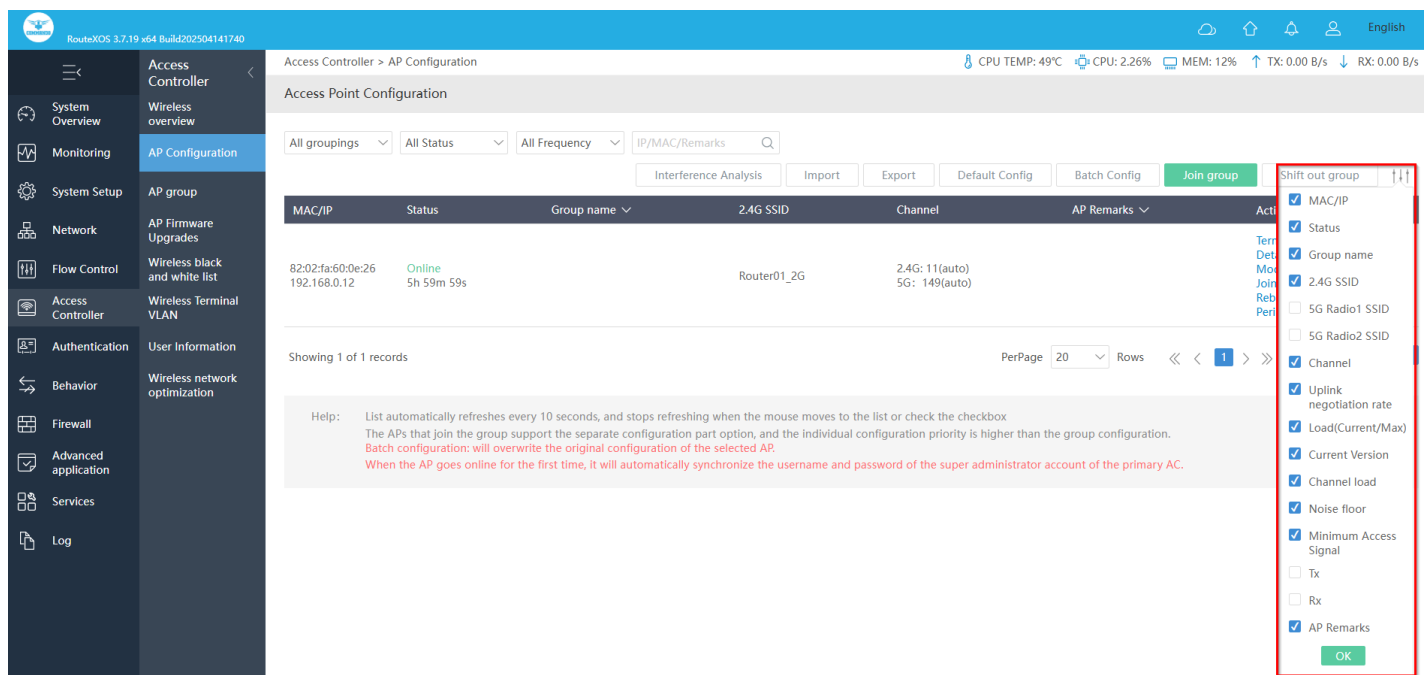


Fig 5.2.4 Access Point Configuration Customize display page

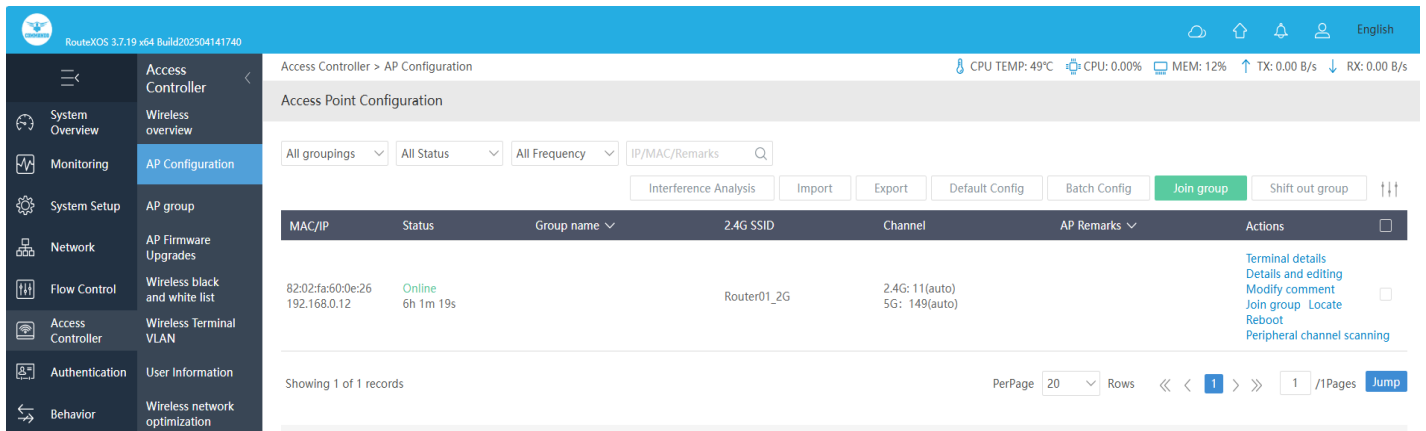


Fig 5.2.5 Access Point Configuration Customized AP page

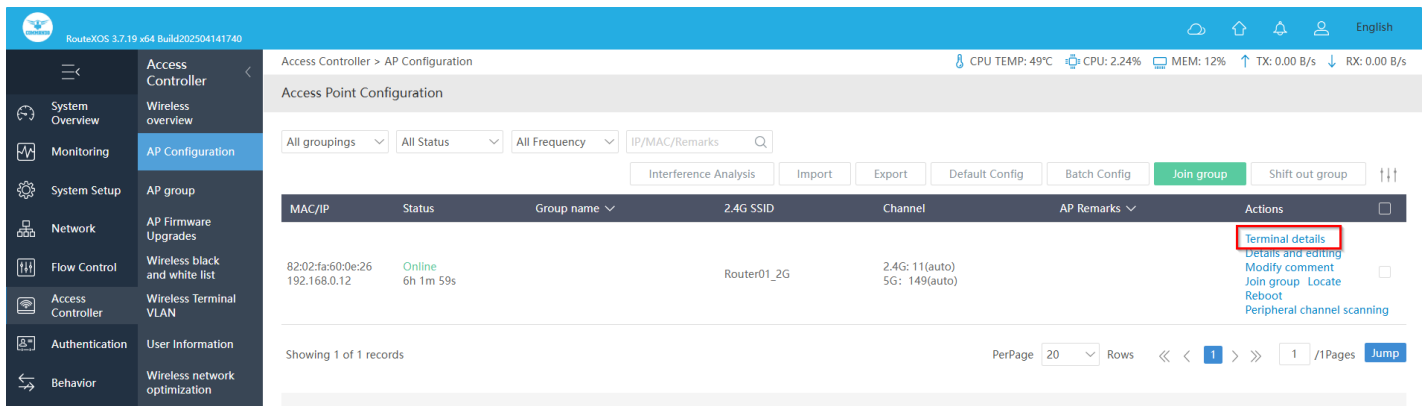


Fig 5.2.6 Access Point Configuration Terminal Details page

After clicking above highlighted icon you will be directed to User Information page as if you clicked Access Controller > User Information for particular AP page will be displayed.

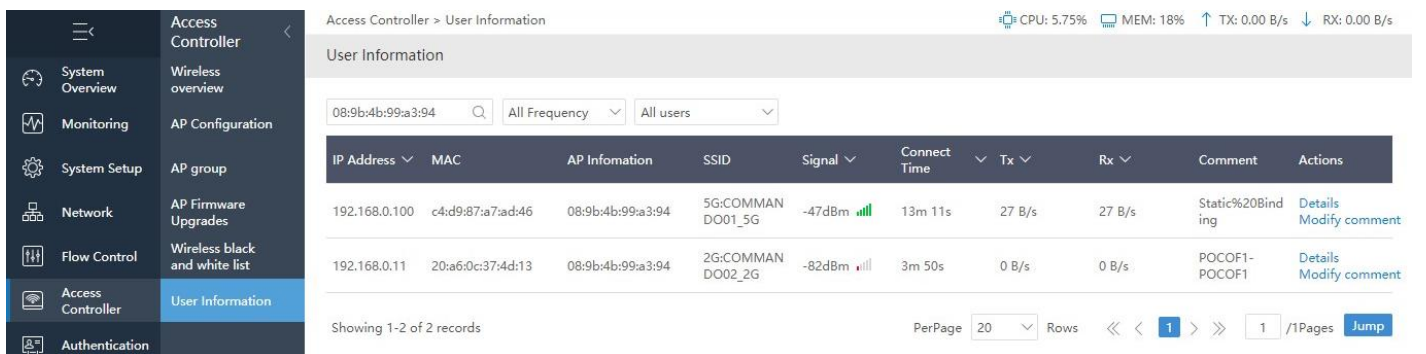


Fig 5.2.7 Access Point Configuration Terminal Details page

Access Controller > AP Configuration

Access Point Configuration

All groupings All Status All Frequency IP/MAC/Model/Remark

Interference Analysis Import Export Default Config Batch Config Join group Shift out group

MAC/IP	Status	Group name	2.4G SSID	Channel	Actions
08:9b:4b:9e:f4:e3 192.168.0.13	Online 9m 34s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto)	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning
08:9b:4b:99:a3:94 192.168.0.10	Online 9m 18s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto) 5G: 149(auto)	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

Showing 1-2 of 2 records

PerPage 20 Rows 1 /1Pages Jump

Help: List automatically refreshes every 10 seconds, and stops refreshing when the mouse moves to the list or check the checkbox.
The APs that join the group support the separate configuration part option, and the individual configuration priority is higher than the group configuration.
Batch configuration: will overwrite the original configuration of the selected AP.

Fig 5.2.8 Details and editing AP Configuration page

Access Controller > AP Configuration

Equipment Status 2.4G 5G Other Setting

SSID1 Name: COMMANDO01_2G SSID2 Name: COMMANDO02_2G

SSID1 Security: No Password SSID2 Security: No Password

SSID1 VLAN: Close SSID2 VLAN: Close

Hide SSID1 Name: Open Hide SSID2 Name: Open

SSID rate limit: Open SSID rate limit: Open

Guest Mode: Open (Isolate guest devices discovery and access to wired network) Guest Mode: Open (Isolate guest devices discovery and access to wired network)

SSID3 Name: SSID4 Name:

SSID3 Security: No Password SSID4 Security: No Password

SSID3 VLAN: Close SSID4 VLAN: Close

Hide SSID3 Name: Open Hide SSID4 Name: Open

SSID rate limit: Open SSID rate limit: Open

Guest Mode: Open (Isolate guest devices discovery and access to wired network) Guest Mode: Open (Isolate guest devices discovery and access to wired network)

Channel: Auto

RF access strategy: Close

Min signal(%): 0 Close

AP Signal: 100%

Channel width: 20 MHz

Airtime scheduling: Open

advanced settings: Open

Save Cancel

Fig 5.2.9 Default 2.4G AP Configuration page

How to change SSID (Wi-Fi Name)?

For changing SSID name, click on Access Controller > AP Configuration click 2.4G and Edit SSID Name.

RouteXOS 3.7.19 x64 Build202504141740

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Access Controller > AP Configuration

SSID1 Name: COMMAND001_2G
 SSID1 Security: WPA-PSK+WPA2-PSK
 SSID1 Password: *****
 SSID1 VLAN: Close
 Hide SSID1 Name: ☐ Open
 SSID rate limit: ☐ Open
 Guest Mode: ☐ Open (Isolate guest devices discovery and access to wired network)

SSID2 Name: Network 1
 SSID2 Security: WPA-PSK+WPA2-PSK
 SSID2 Password: *****
 SSID2 VLAN: Close
 Hide SSID2 Name: ☐ Open
 SSID rate limit: ☐ Open
 Guest Mode: ☐ Open (Isolate guest devices discovery and access to wired network)

SSID3 Name: Network 2
 SSID3 Security: WPA-PSK+WPA2-PSK
 SSID3 Password: *****
 SSID3 VLAN: Close
 Hide SSID3 Name: ☐ Open
 SSID rate limit: ☐ Open
 Guest Mode: ☐ Open (Isolate guest devices discovery and access to wired network)

SSID4 Name: Network 3
 SSID4 Security: WPA-PSK+WPA2-PSK
 SSID4 Password: *****
 SSID4 VLAN: Close
 Hide SSID4 Name: ☐ Open
 SSID rate limit: ☐ Open
 Guest Mode: ☐ Open (Isolate guest devices discovery and access to wired network)

Channel: Auto
 RF access strategy: Close
 Min signal(%)(%): 0 Close
 AP Signal: 100%
 Channel width: 20 MHz
 Airtime scheduling: ☐ Open
 advanced settings: ☐ Open

Save Cancel

Fig 5.2.10 Changing SSID Configuration page

RouteXOS 3.7.19 x64 Build202504141740

CPU TEMP: 50°C CPU: 2.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Access Controller > AP Configuration

Access Point Configuration

All groupings All Status All Frequency IP/MAC/Remarks

Interference Analysis Import Export Default Config Batch Config Join group Shift out group

MAC/IP	Status	Group name	2.4G SSID	Channel	AP Remarks	Actions
82:02:fa:50:0e:26 192.168.0.12	Online 6h 30m 55s		COMMAND001_2G Network 1 Network 2 Network 3	2.4G: 11(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

Showing 1 of 1 records

PerPage 20 Rows 1 / 1Pages Jump

Fig 5.2.11 AP configuration after Changing SSID Configuration page

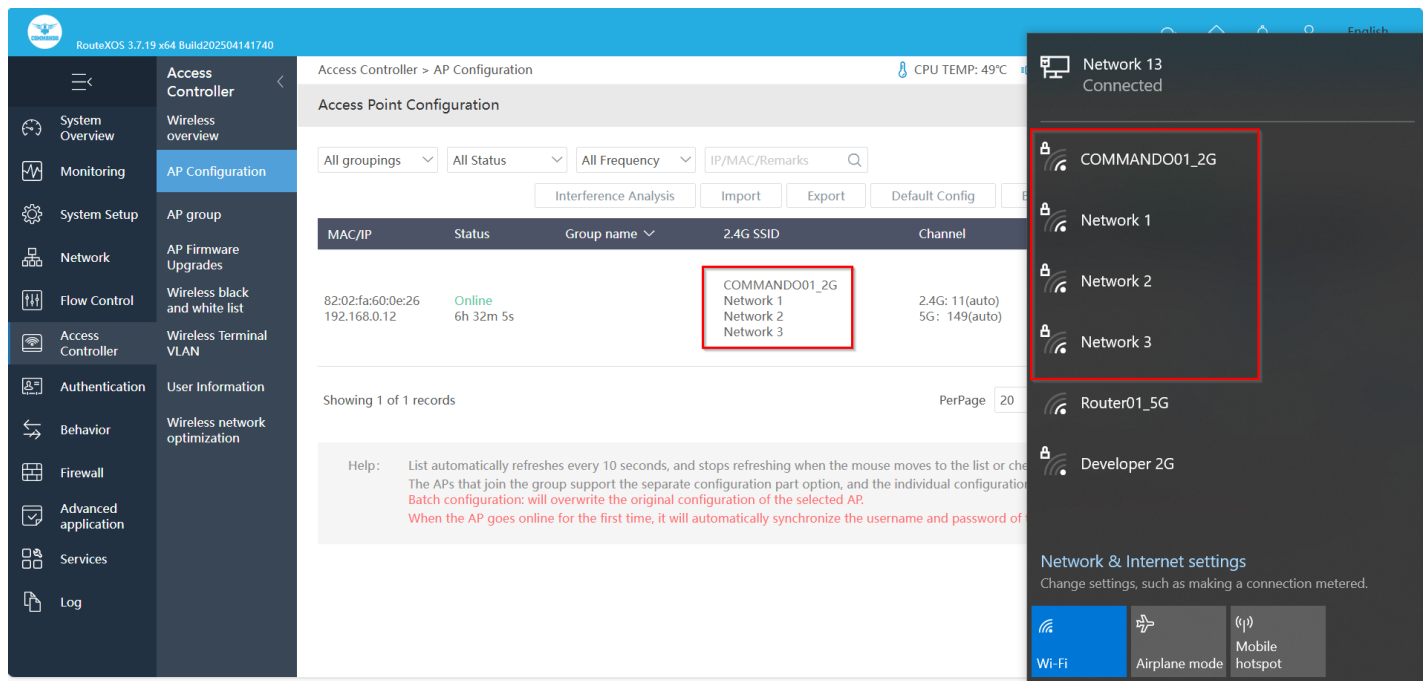


Fig 5.2.12 SSID available for users page

How to set up manually Selected channel?

Direct communication between an 802.11 client radio and an access point occurs over a common ISM Band channel frequency. You set the channel manually or auto in the access point, if you set radio card automatically tunes its transceiver to the frequency of the access point having the strongest signal.

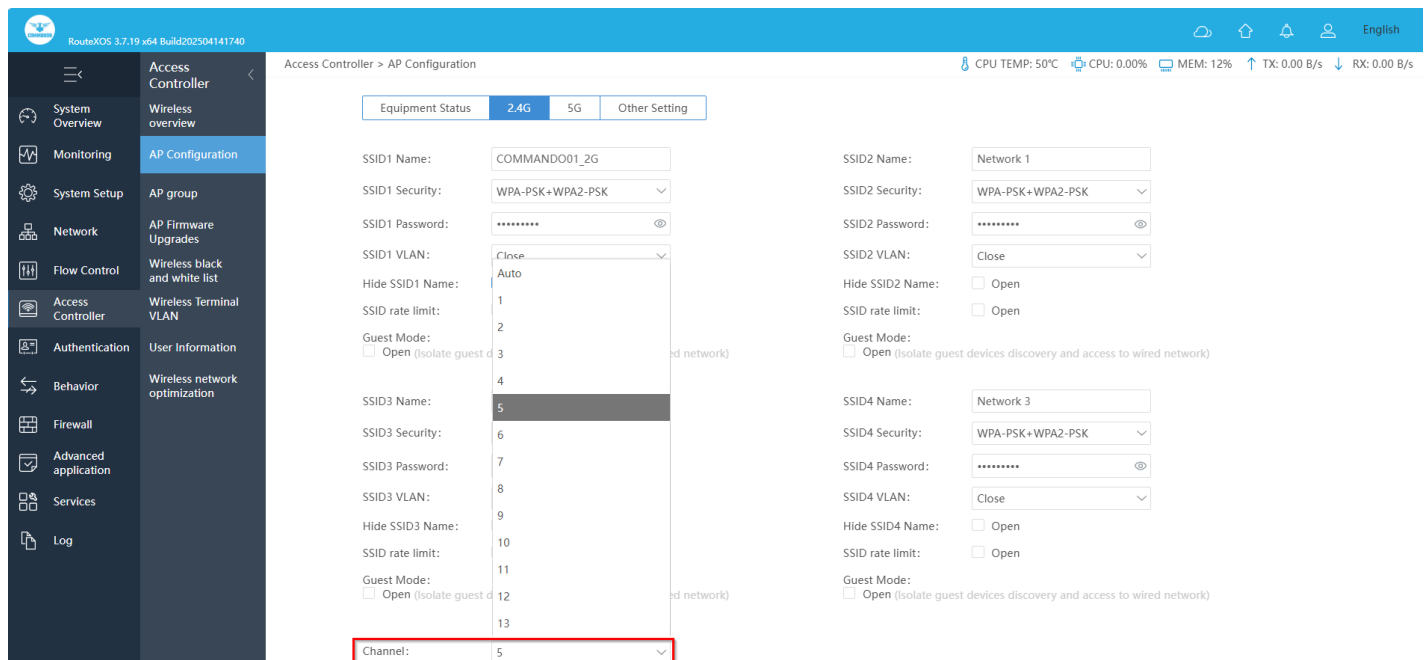


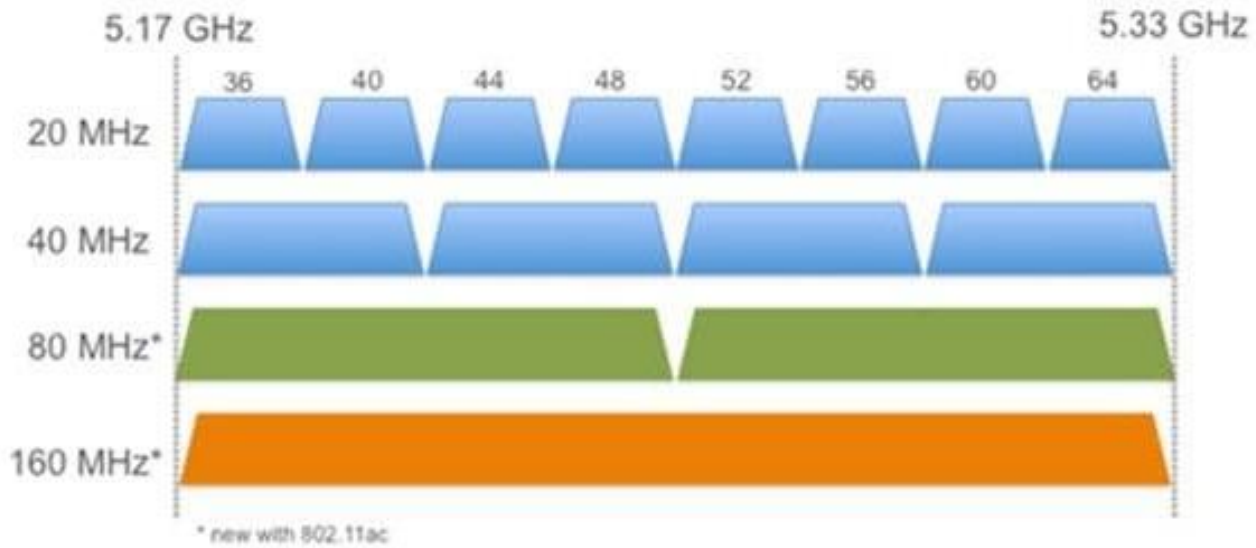
Fig 5.2.13 Changing Channel for SSID page

Fig 5.2.14 Manual Channel for AP configuration page

Setting Channel Bandwidth: By default, the 2.4 GHz frequency uses a 20 MHz channel width. In crowded areas with a lot of frequency noise and interference, a single 20MHz channel will be more stable. 40MHz channel width allows for greater speed and faster transfer rates but it doesn't perform as well in crowded areas.

Standard	Frequency	Bandwidth	Modulation	Max Data Rate
802.11	2.4 Ghz	20 MHz	DSSS, FHSS	2Mbps
802.11a	5 Ghz	20 MHz	DSSS	54 Mbps
802.11b	2.4 Ghz	20 MHz	OFDM	11 Mbps
802.11g	2.4 Ghz	20 MHz	OFDM	54 Mbps
802.11n	2.4 and 5 Ghz	20 MHz, 40 MHz	OFDM	600 Mbps
802.11ac	2.4 and 5 Ghz	20, 40, 80, 80+80, 160	OFDM	6.93 Gbps

5 GHz Channelization



	Channel Width			
# Spatial Streams	20 MHz	40 MHz	80 MHz	160 MHz
1	86 Mbps	200 Mbps	433 Mbps	866 Mbps
2	173 Mbps	400 Mbps	866 Mbps	1.73 Gbps
3	288.9 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps
4	346.7 Mbps	800 Mbps	1.73 Gbps	3.46 Gbps

Fig 5.2.14 Channel Width and Max. Data rate relation

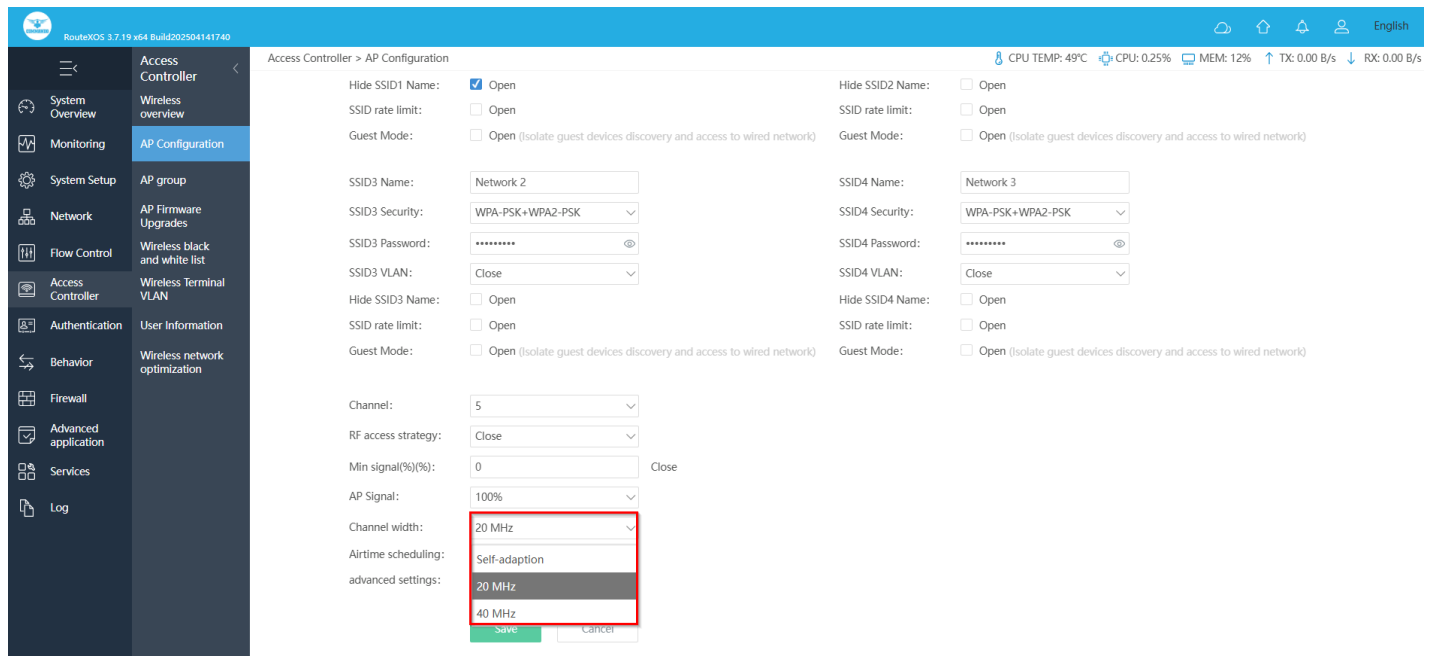
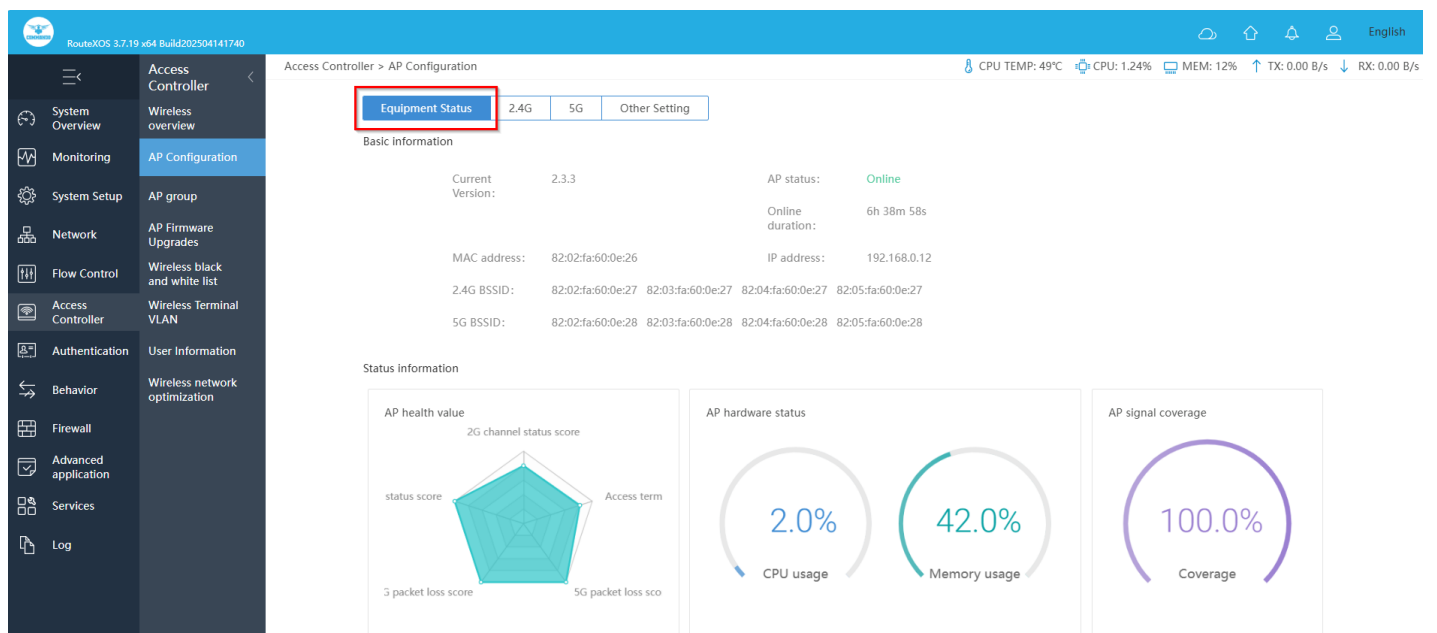


Fig 5.2.15 Changing Channel Width for AP configuration page



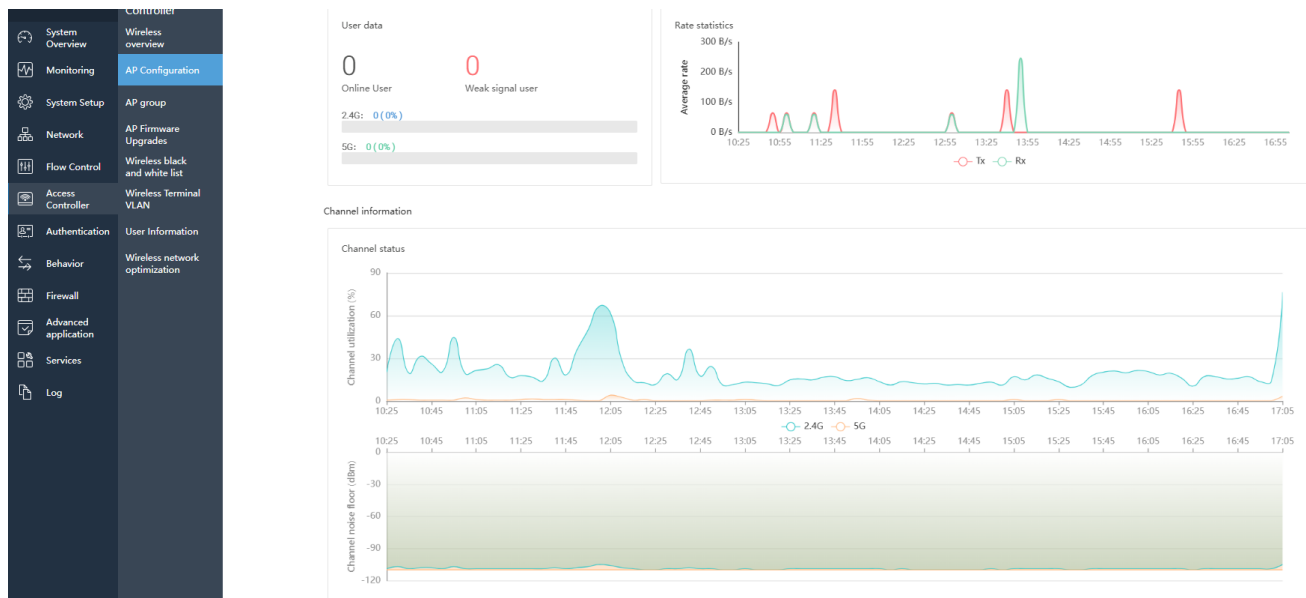


Fig 5.2.16 Equipment Status of AP page

How to schedule timing of AP usage as per user requirement?

For changing Schedule timing of AP from all time to restricted timing and secure Wi-Fi network from unauthorized access, click on Access Controller > AP Configuration click other setting and Edit Plan as per requirement.

The screenshot shows the 'Access Controller > AP Configuration' page. The top bar includes the 'RouteXOS 3.7.19 x64 Build202504141740' version and system status (CPU TEMP: 48°C, CPU: 2.48%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s). The left navigation menu is the same as in Fig 5.2.16. The main content area has tabs for 'Equipment Status', '2.4G', '5G', and 'Other Setting'. The 'Other Setting' tab is active, showing the following configuration options:

- Basic Information:**
 - AP remarks: (text input field)
 - Schedule: ☐ Plan 1, ☐ Plan 2, ☐ Plan 3
 - Restart: ☐ Open
 - Port 1 VLAN: (dropdown menu, currently set to 'Close')
 - Status light: ☒ Open
 - Gateway check: ☐ Open (When the AP cannot ping the default gateway, the RF signal will be automatically turned off)
- roaming settings:**
 - roaming sensitivity: (dropdown menu, currently set to 'lower') (Wireless terminals in the mobile state, actively link to the best sensitivity of wireless signals)

At the bottom are 'Save' and 'Cancel' buttons.

Fig 5.2.17 Default Other Setting of AP configuration page

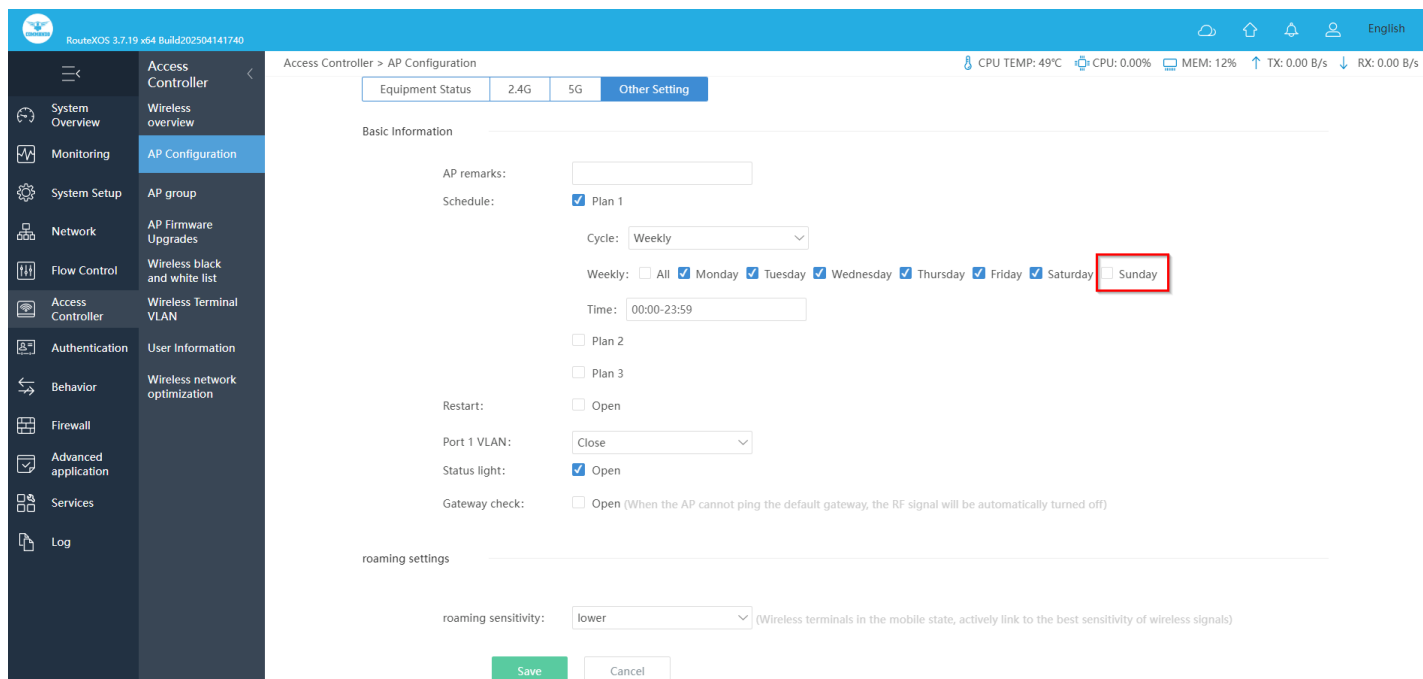


Fig 5.2.18 Other Setting of AP configuration to turn OFF Wi-Fi on Sunday page

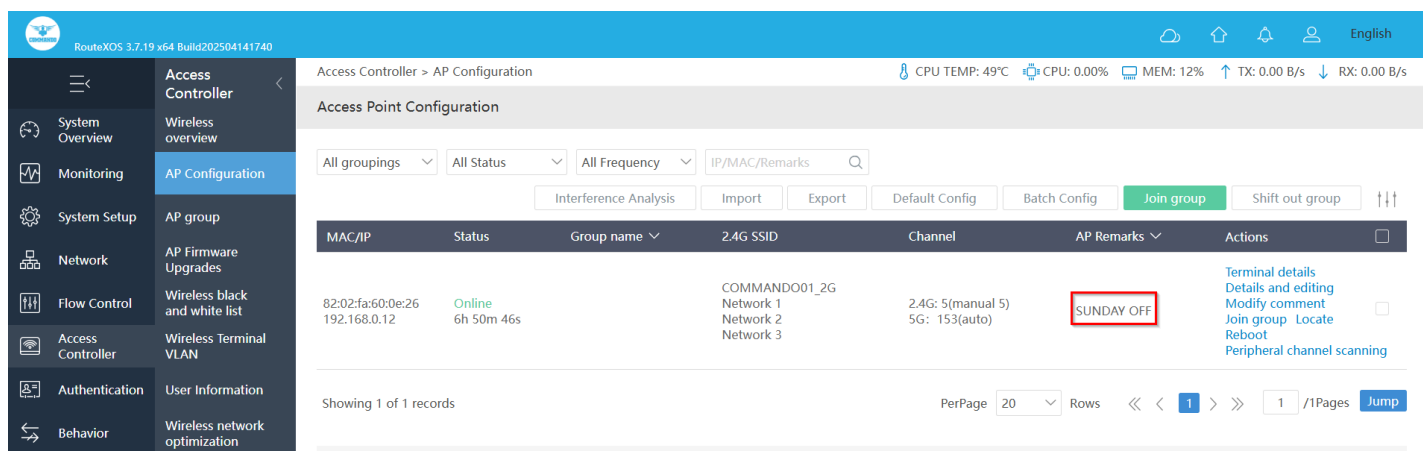


Fig 5.2.19 AP configuration to turn OFF Wi-Fi on Sunday page

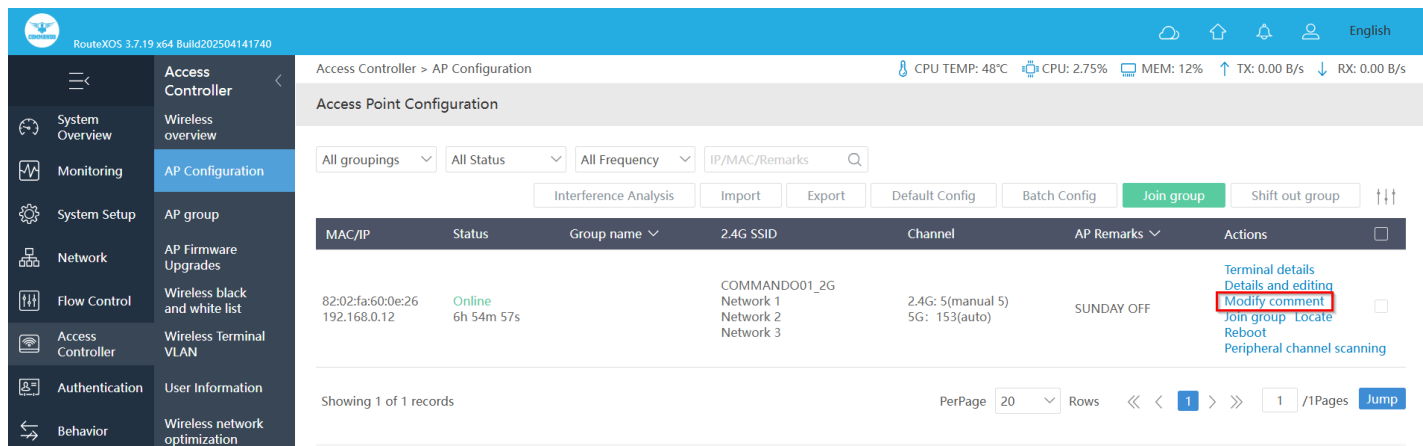


Fig 5.2.20 Modify Comment page

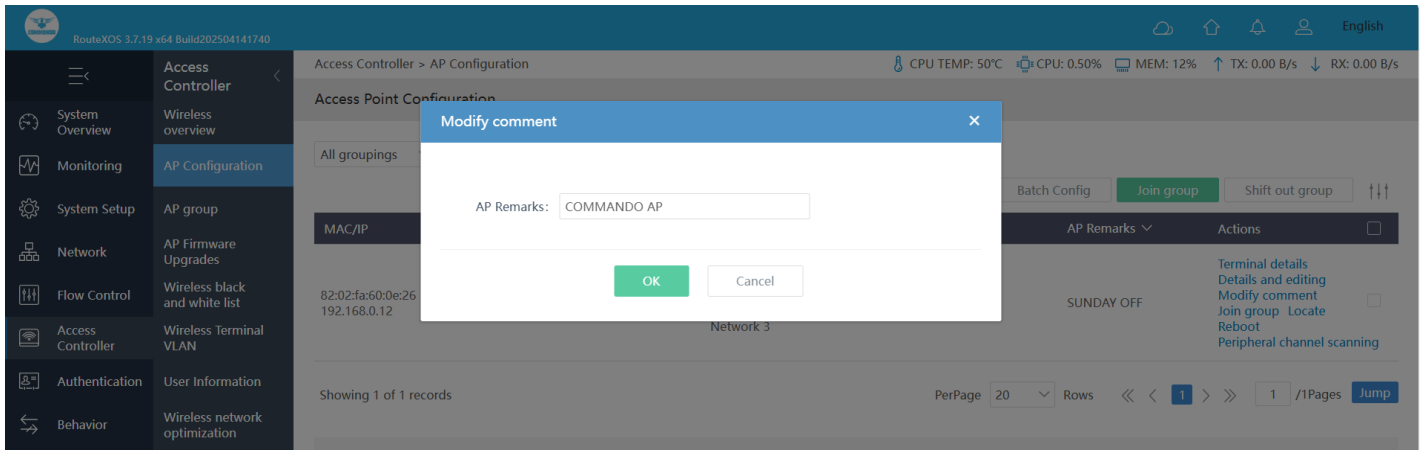


Fig 5.2.21 Changing Modify Comment page

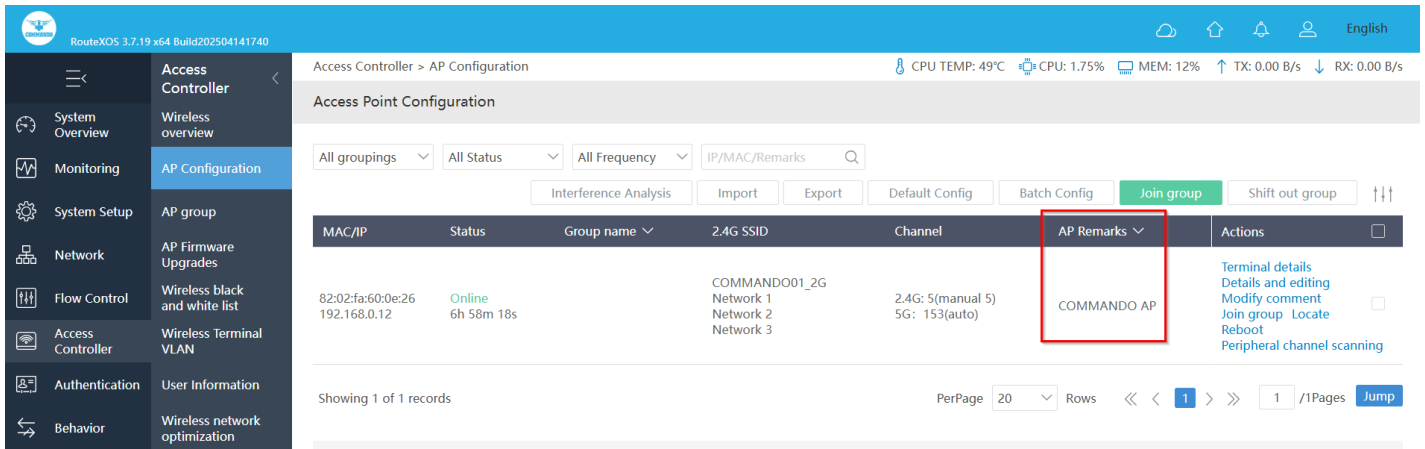


Fig 5.2.22 AP Remark after Modify Comment page

After joining the group, the group configuration will be used, and the AP original configuration will be restored after the group is removed.

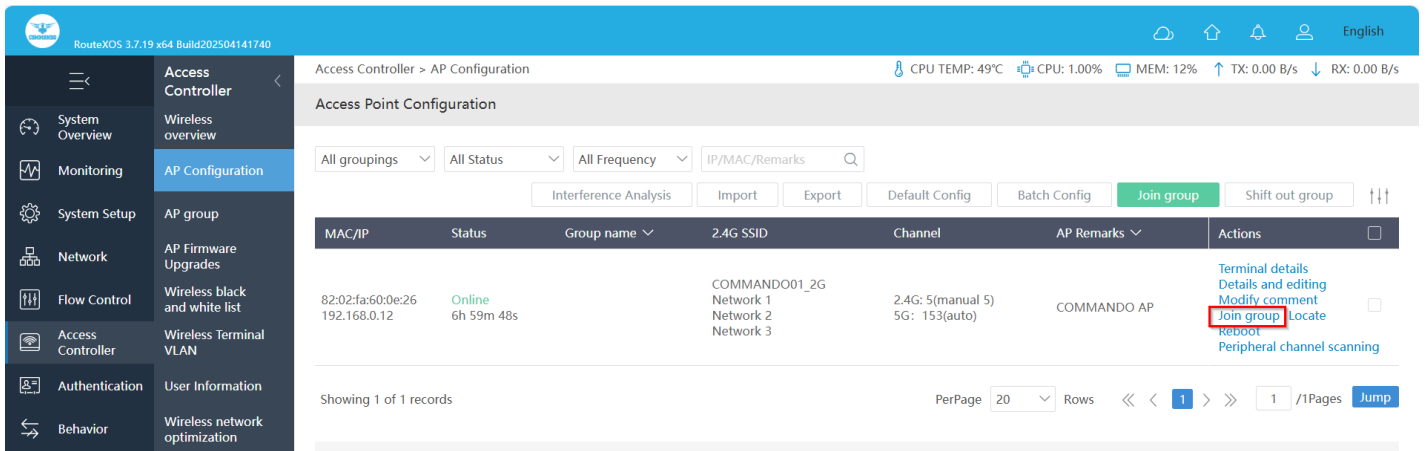


Fig 5.2.23 Default Join group page

Note: Above page will be Editable after creating AP Group only

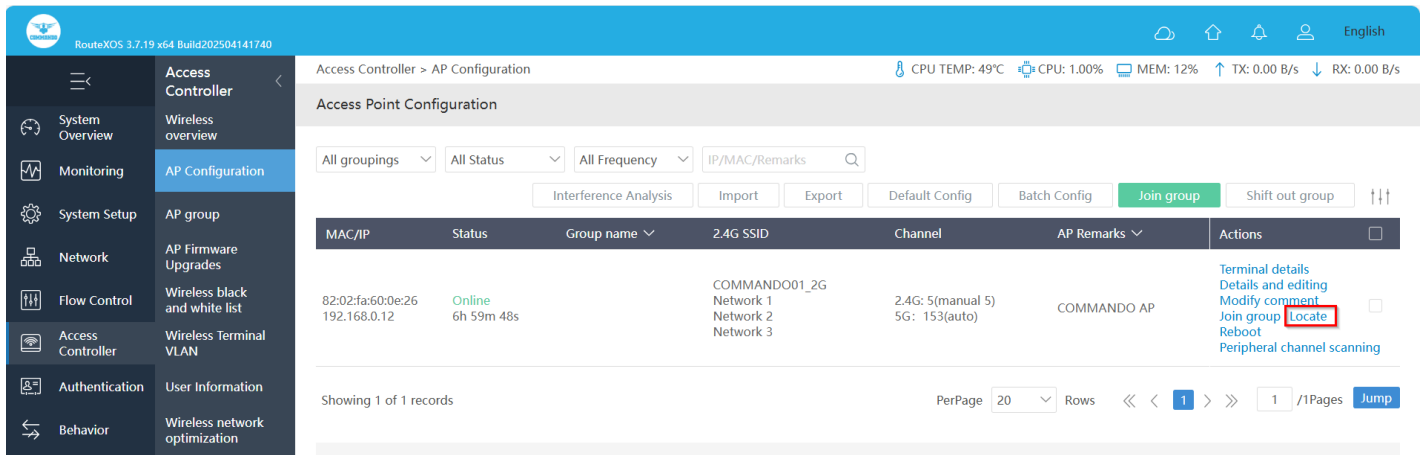


Fig 5.2.24 Default Locate AP page

Note: If you are having number of AP installed in premises and want to find the particular AP out of bunch of APs then this will be very handy tool. Please look for the AP that the light flicker and click "Stop Locate" after finding.

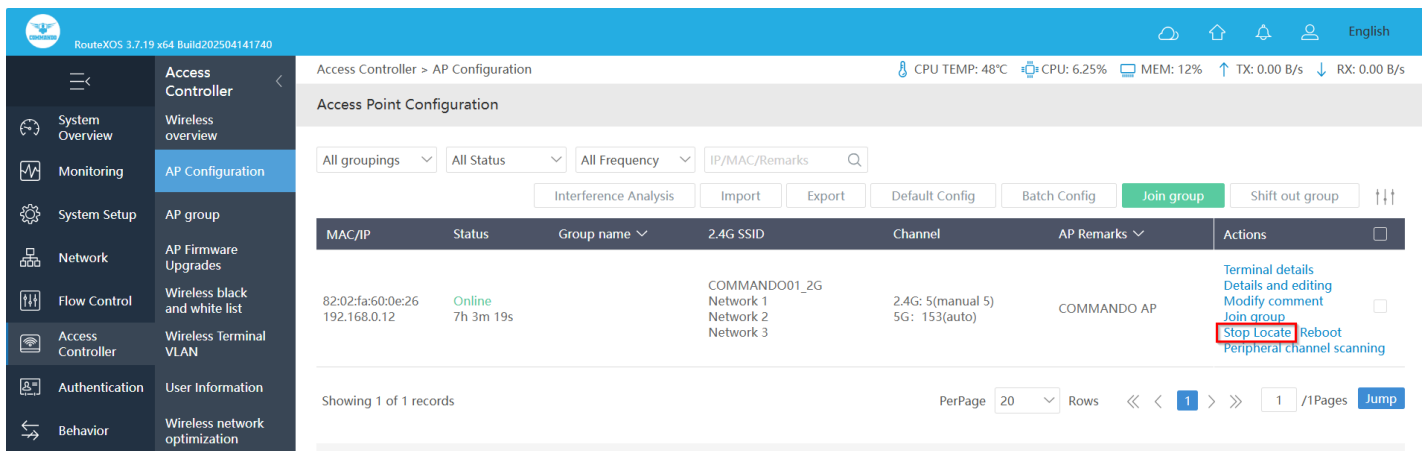


Fig 5.2.25 For Locate particular AP page

Rebooting an AP means restart an AP ie. "Cold" Restart AP Now. Reboot will cause the terminal to disconnect.

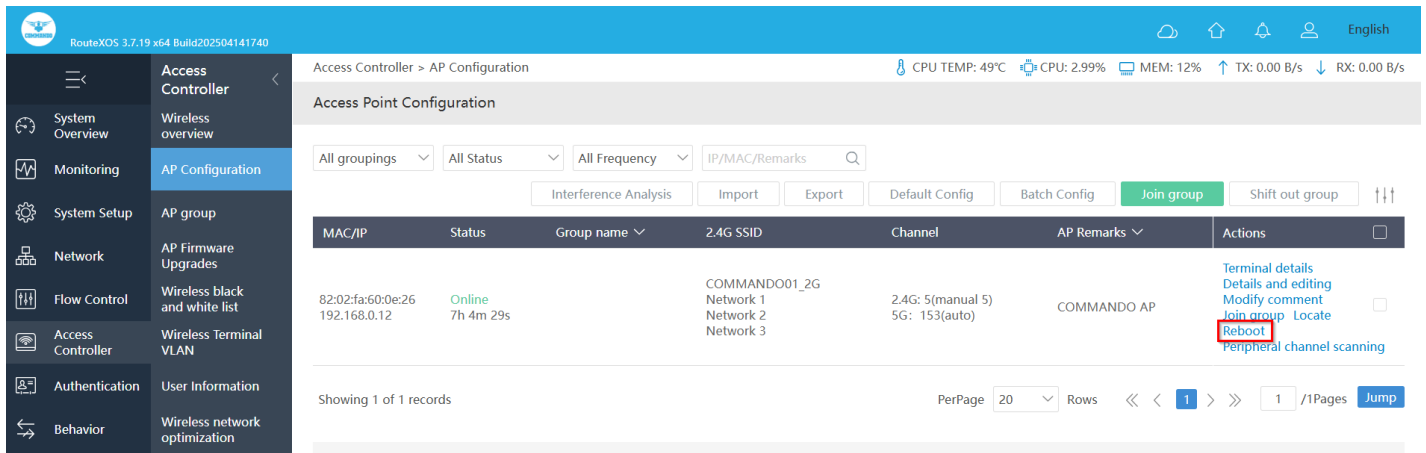


Fig 5.2.26 Reboot option in AP configuration page

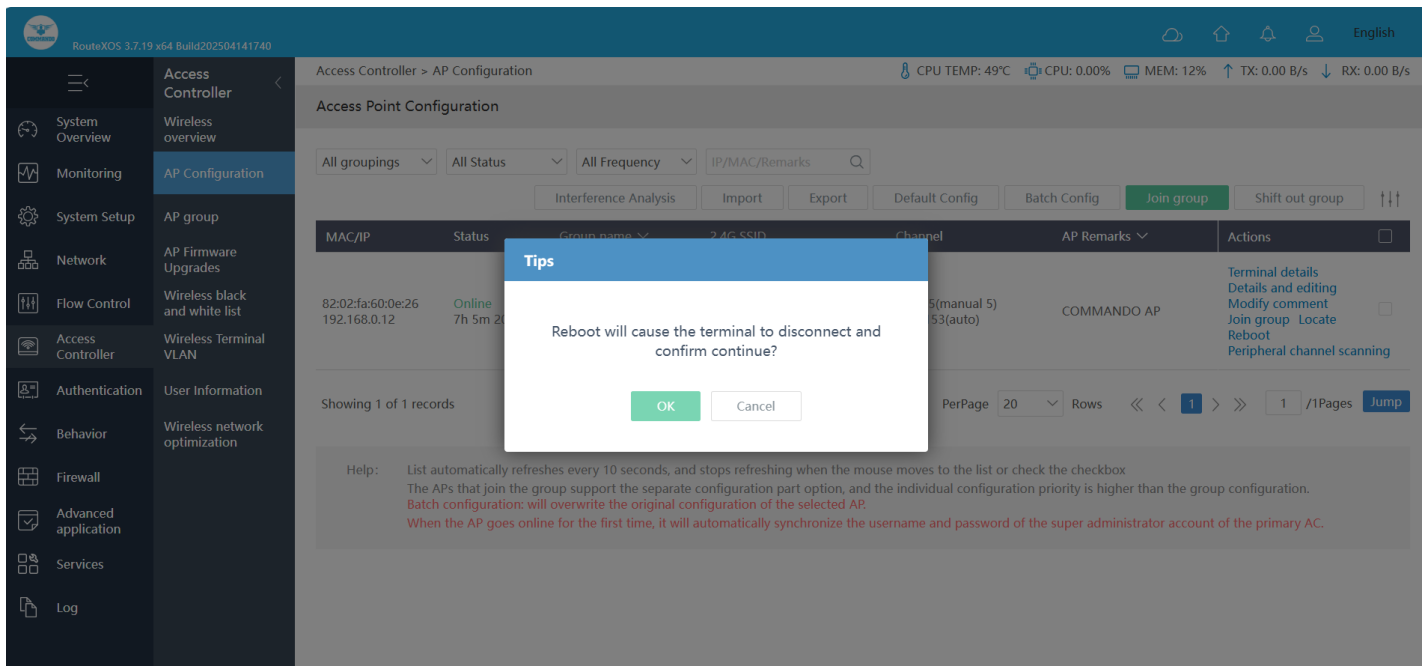


Fig 5.2.27 Reboot AP page

Peripheral

Channel Scanning: The scanning process consists in actively probing the radio channels to gather access points information.

Note:

1. Please select AP for signal scanning.
2. The signal strength is negative, the larger the value, the stronger the signal

- If the signal has a channel overlap, it will cause the same frequency interference, the signal quality will decrease, the network speed will be slower Peripheral channel scanning

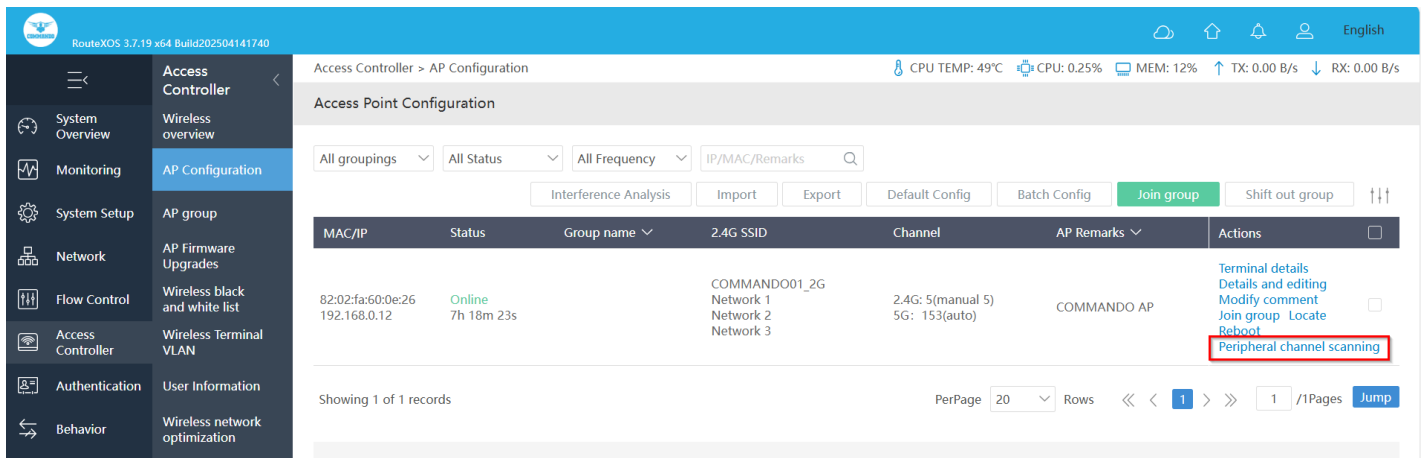


Fig 5.2.28 Default Peripheral channel scanning option page

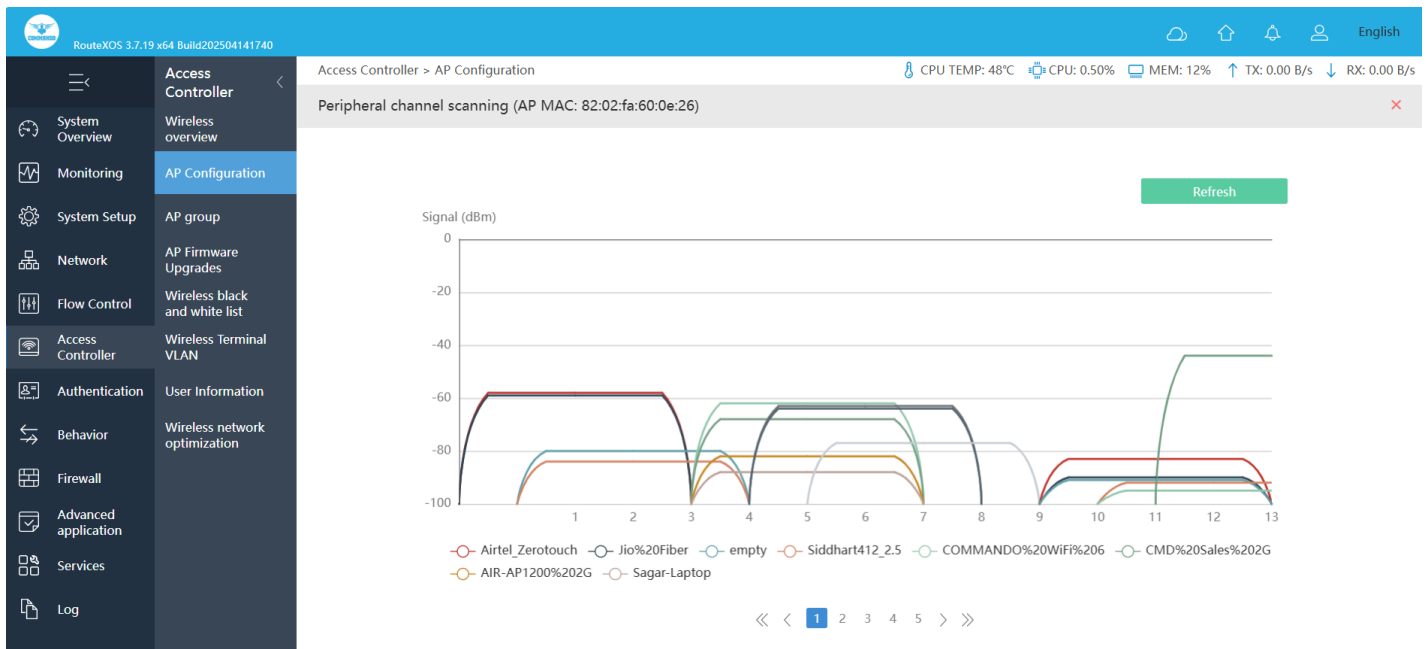


Fig 5.2.29 Peripheral channel scanning page

5.3 AP Group

An AP group is a set of APs to which the same configuration is applied. The APs that join the group use the group configuration uniformly. After the packets are removed, the original AP configuration is restored.

To configure AP Group Access, Click on Controller > AP group

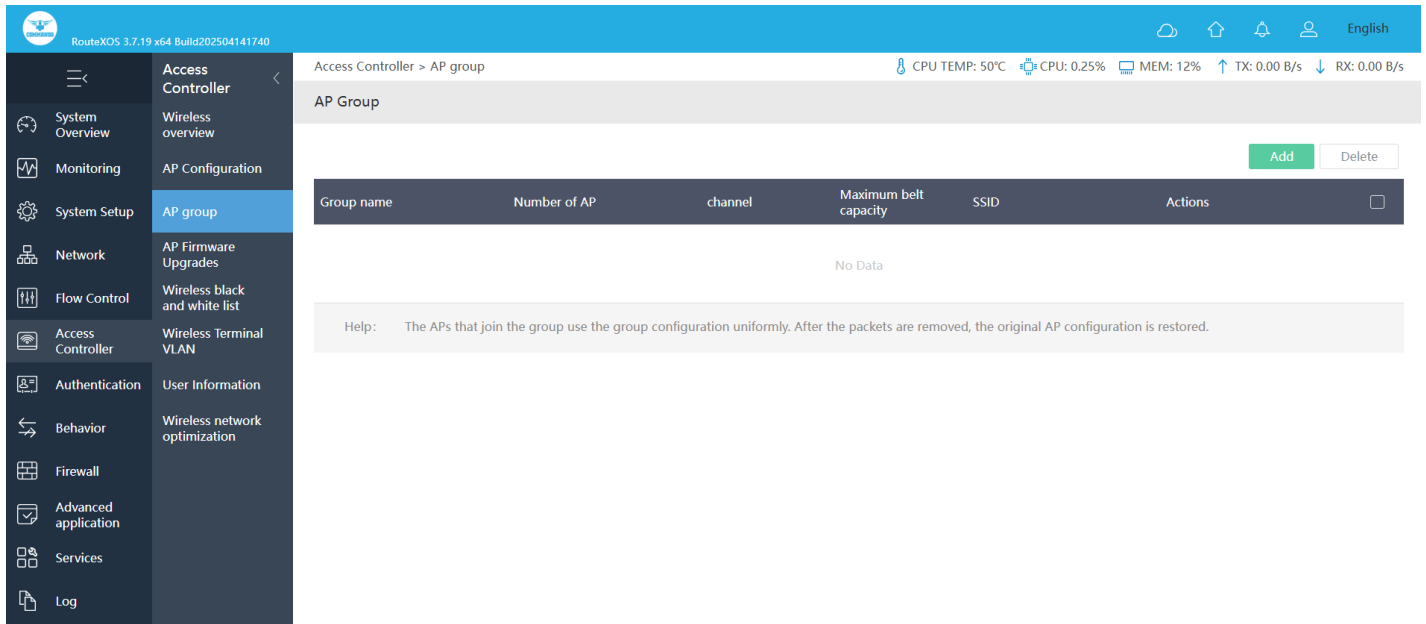


Fig 5.3.1 Default AP Group page

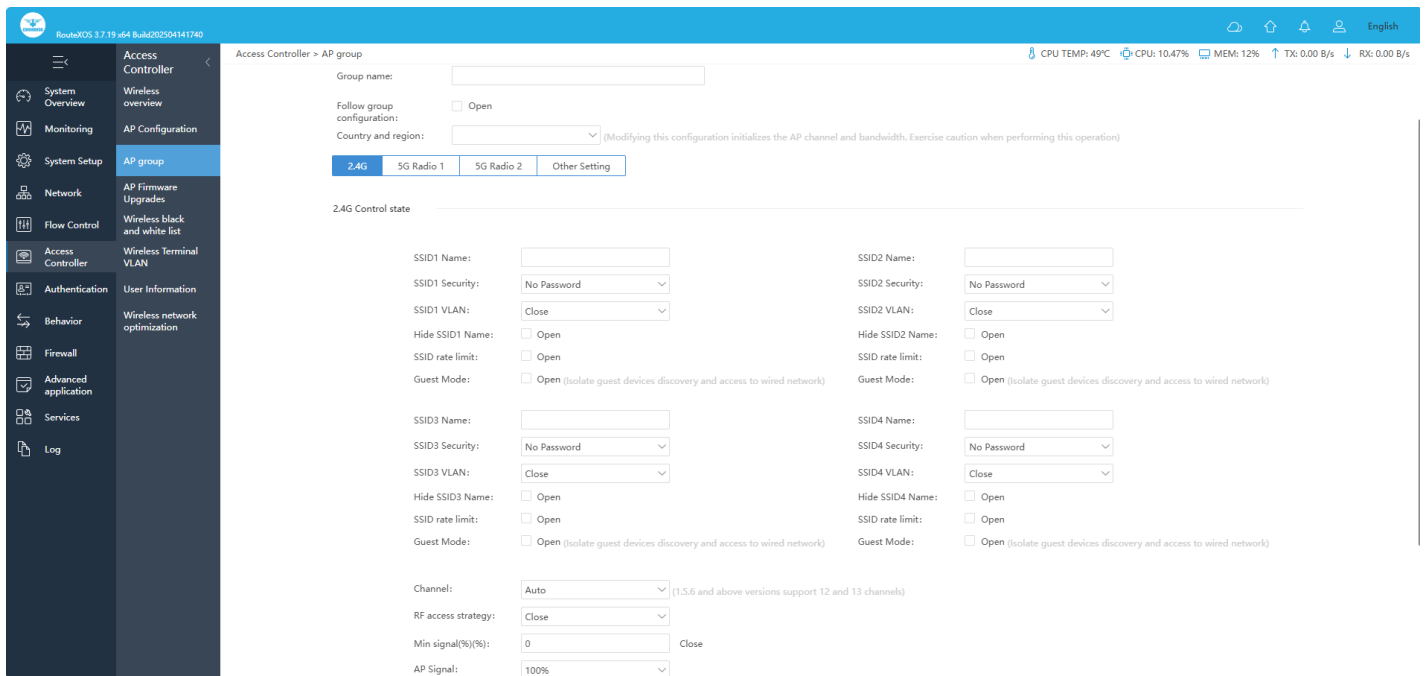


Fig 5.3.2 Default Edit AP Group page

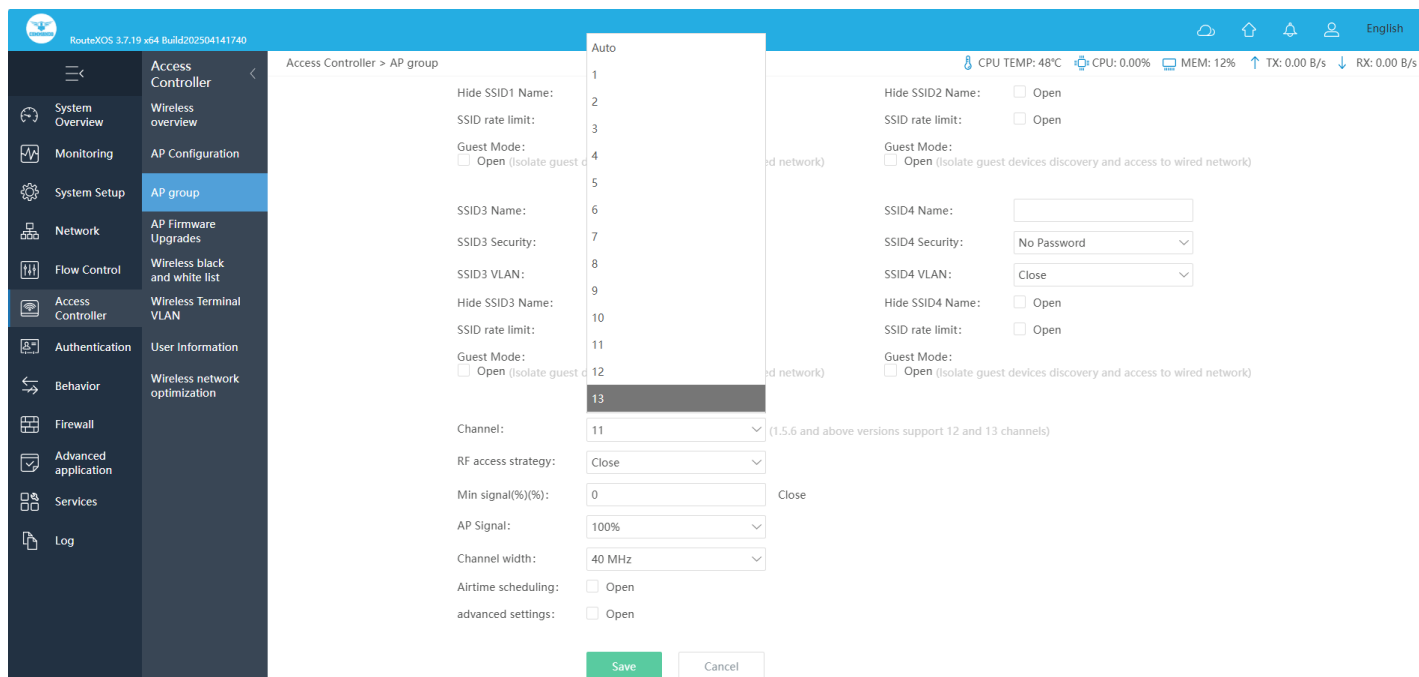


Fig 5.3.4 Group AP Channel selection in 2.4GHz page

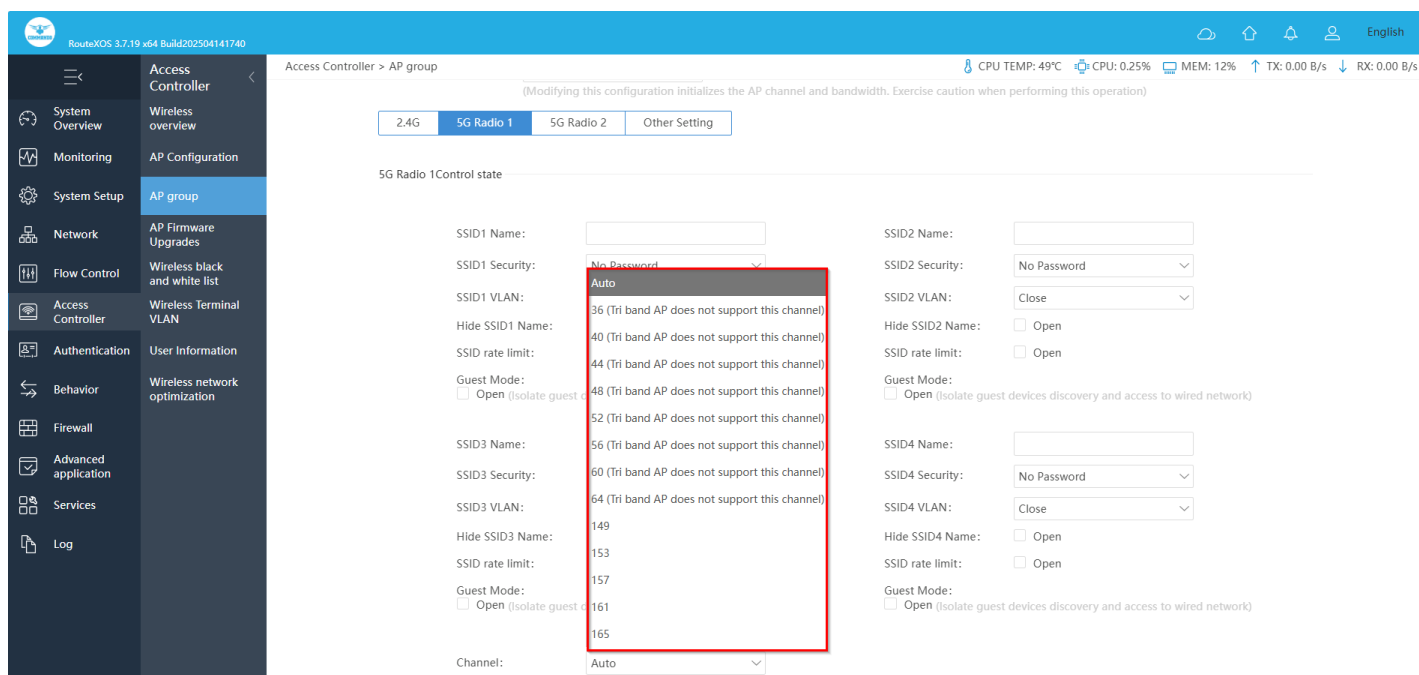


Fig 5.3.5 Group AP Channel selection in 5GHz Radio1 page

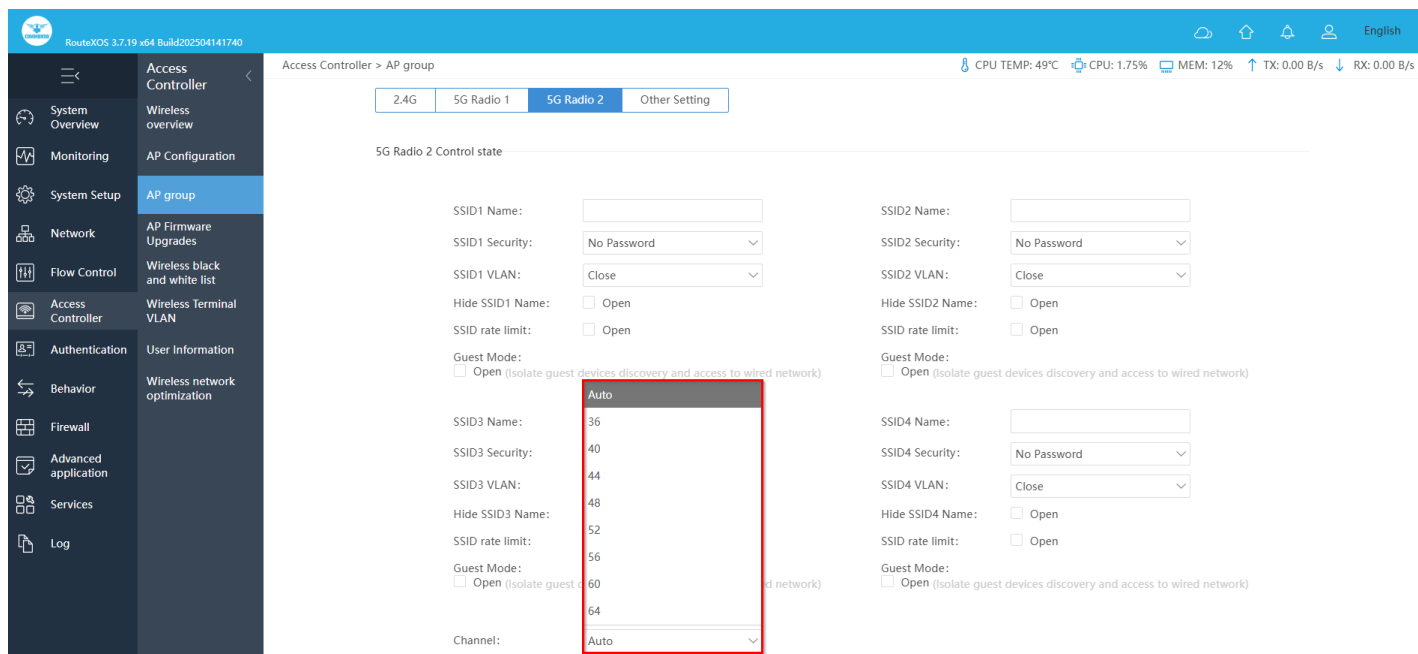


Fig 5.3.6 Group AP Channel selection in 5GHz Radio2 page

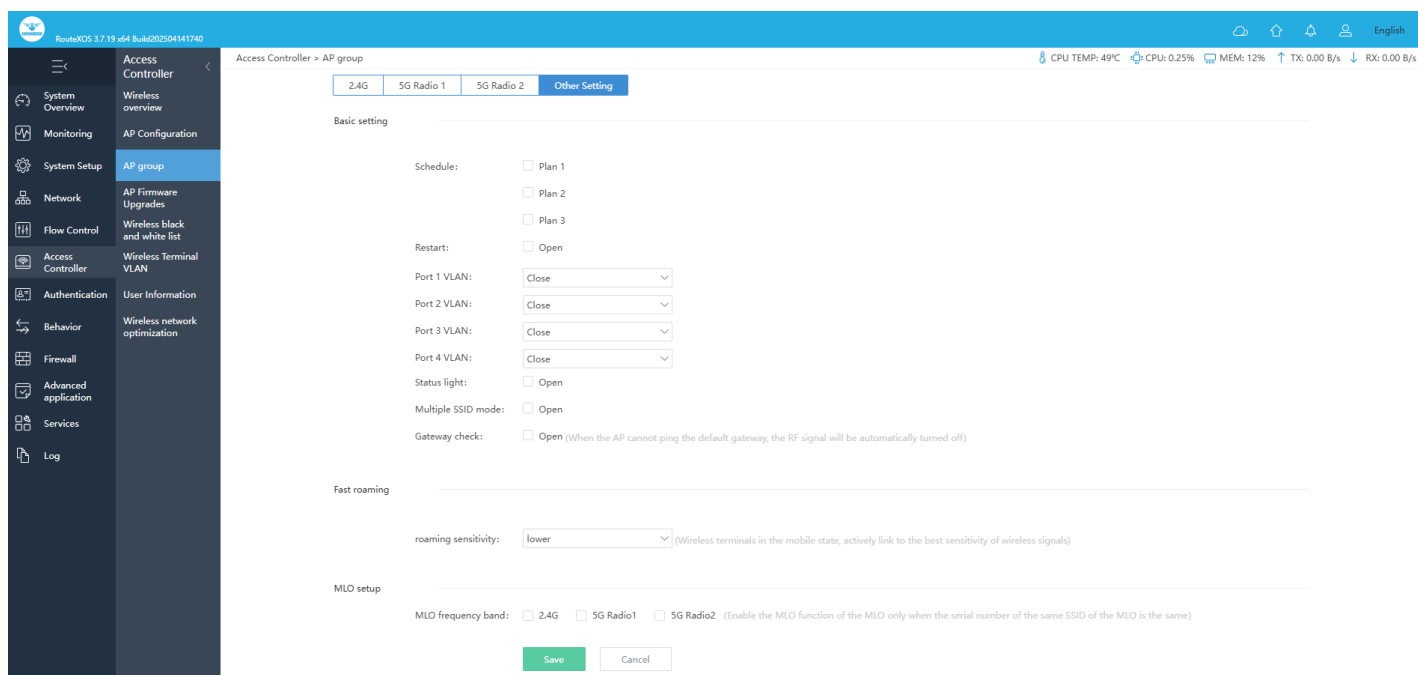


Fig 5.3.7 Group AP Default Other setting page

RouteXOS 3.7.19 x64 Build202504141740

Access Controller > AP group

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

AP Group

Add Delete

Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions
COMMANDO	0	2.4G: 11 5G Radio1: auto 5G Radio2: auto	2.4G: unlimited 5G Radio1: unlimited 5G Radio2: unlimited	2.4G: Net1 2.4G: Net2	Edit Management AP Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Help: The APs that join the group use the group configuration uniformly. After the packets are removed, the original AP configuration is restored.

Fig 5.3.8 AP Group page

How to add AP in created Group?

To add AP in created Group click on Management AP of Created AP Group page.

RouteXOS 3.7.19 x64 Build202504141740

Access Controller > AP group

CPU TEMP: 48°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

AP Group

Add Delete

Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions
COMMANDO	0	2.4G: 11 5G Radio1: auto 5G Radio2: auto	2.4G: unlimited 5G Radio1: unlimited 5G Radio2: unlimited	2.4G: Net1 2.4G: Net2	Edit Management AP Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Help: The APs that join the group use the group configuration uniformly. After the packets are removed, the original AP configuration is restored.

Fig 5.3.9 Management AP Group page

Click on Management AP to configure Access Controller > AP group >> Management AP "GROUP NAME"

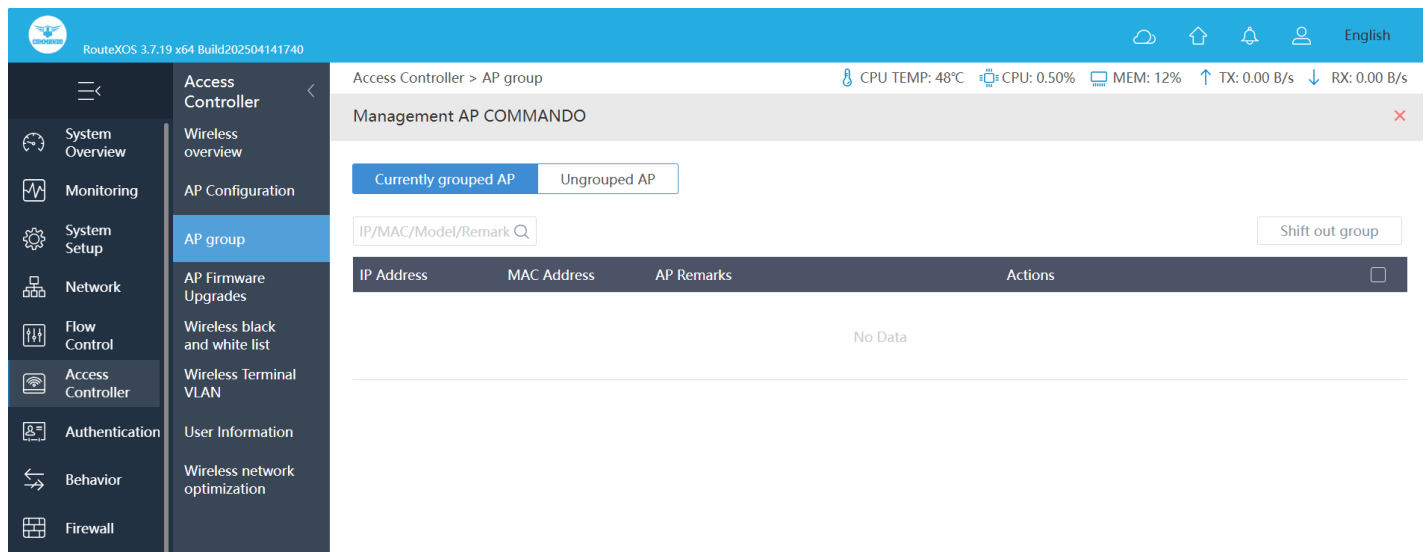


Fig 5.3.10 Default Management AP Group page

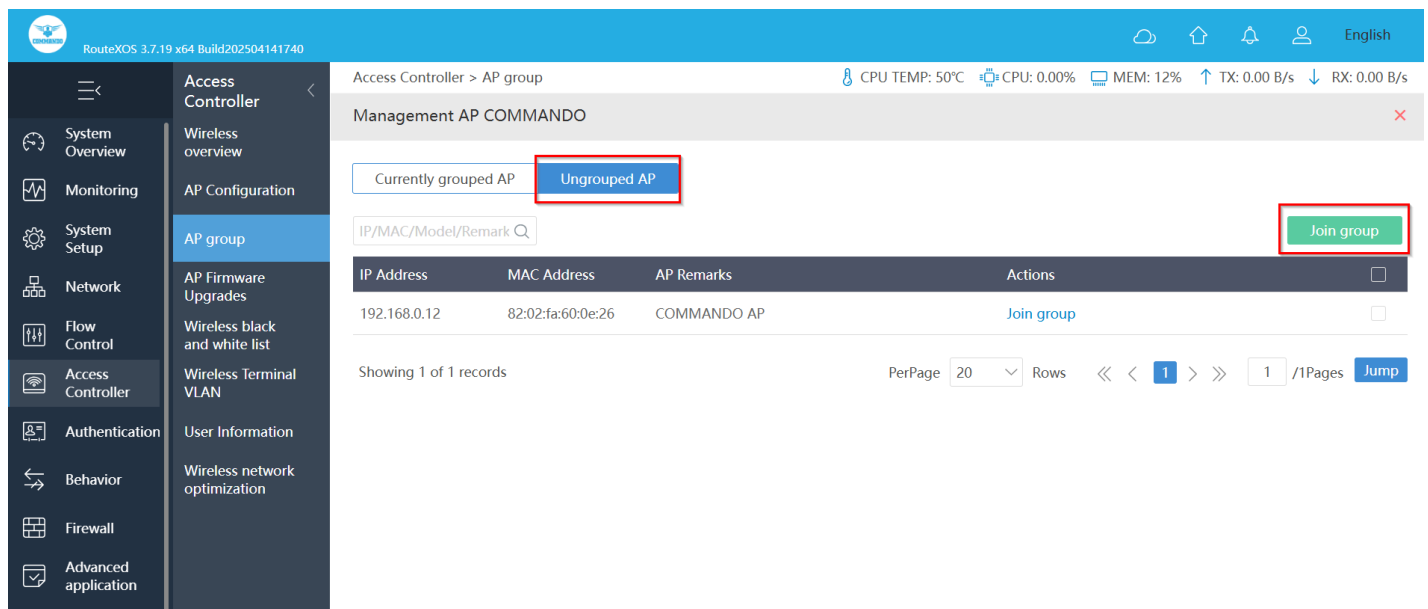


Fig 5.3.11 Join Management AP Group page

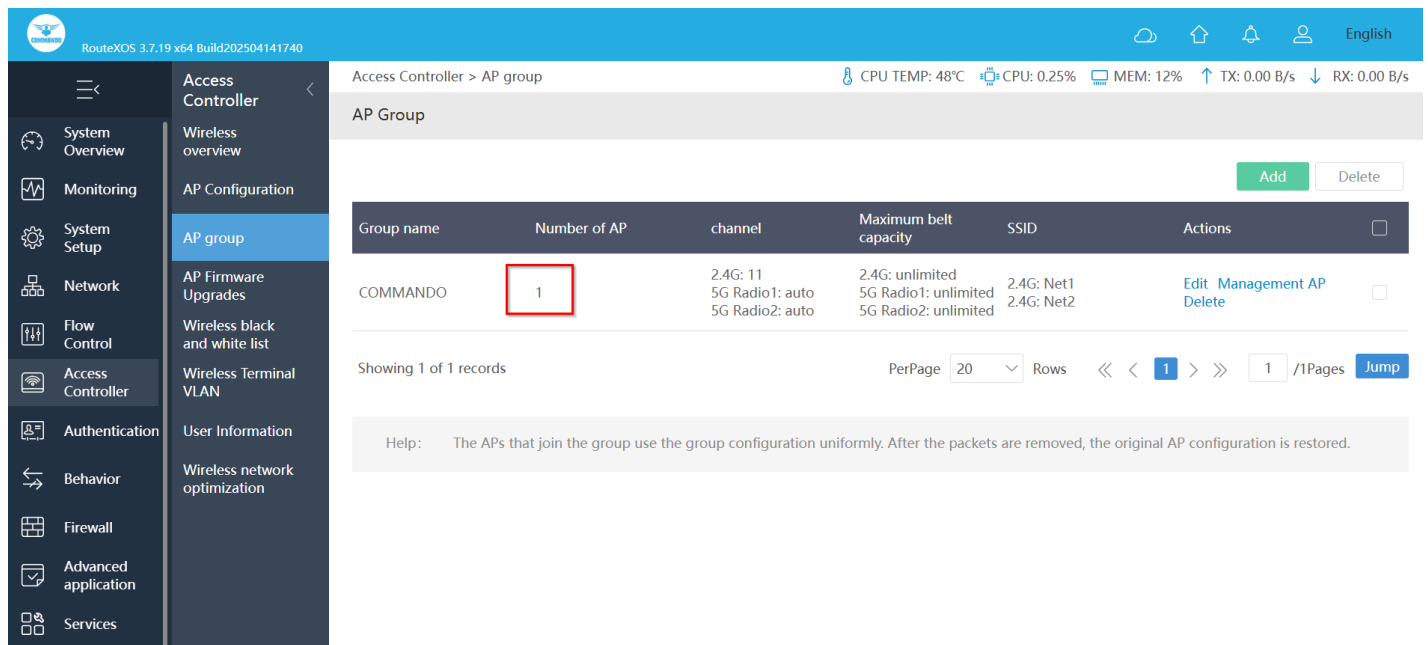


Fig 5.3.12 Join Management AP Group page

5.4 AP Firmware Upgrades

A firmware update will upgrade your AP with advanced operational instructions without needing any upgradation in the hardware. By updating the firmware, you will be able to explore new features that are added to the device and also have an enhanced user experience while interacting with the device. When the firmware is upgraded, device performance and functionality is improved through feature enhancements and bug fixes.

To upgrade firmware of Access Point, Click on Access Controller > AP Firmware Upgrades

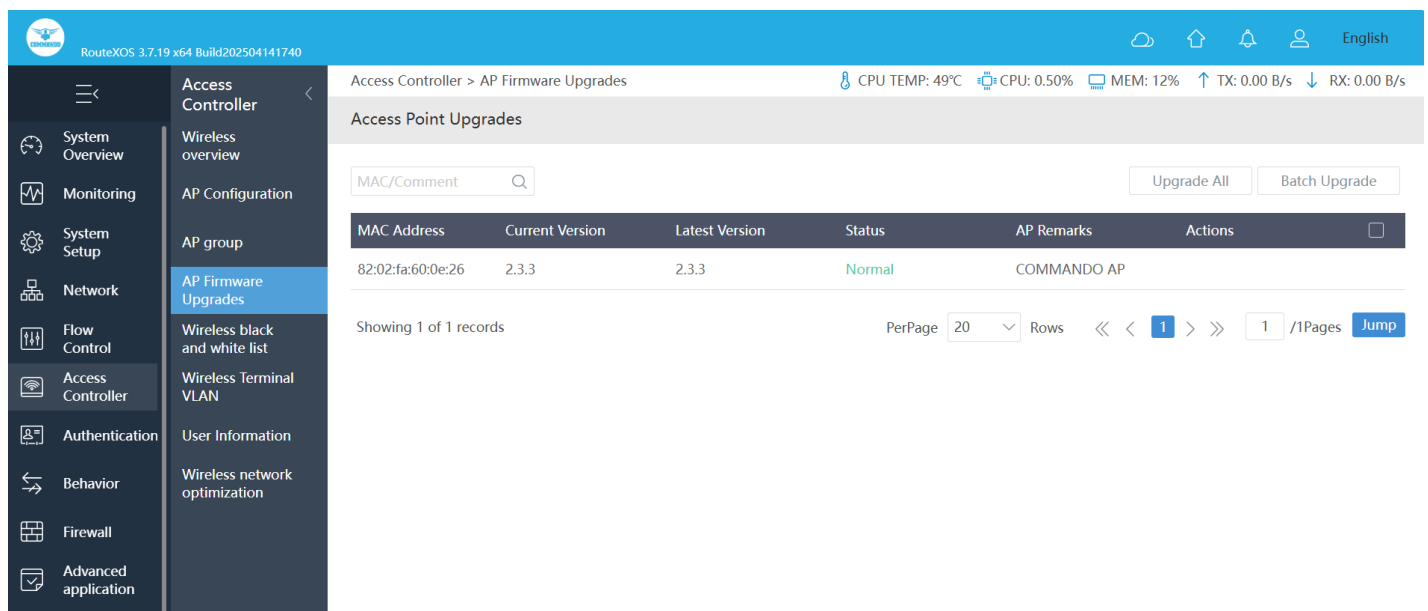


Fig 5.4.1 Default Upgrade firmware of Access Point page

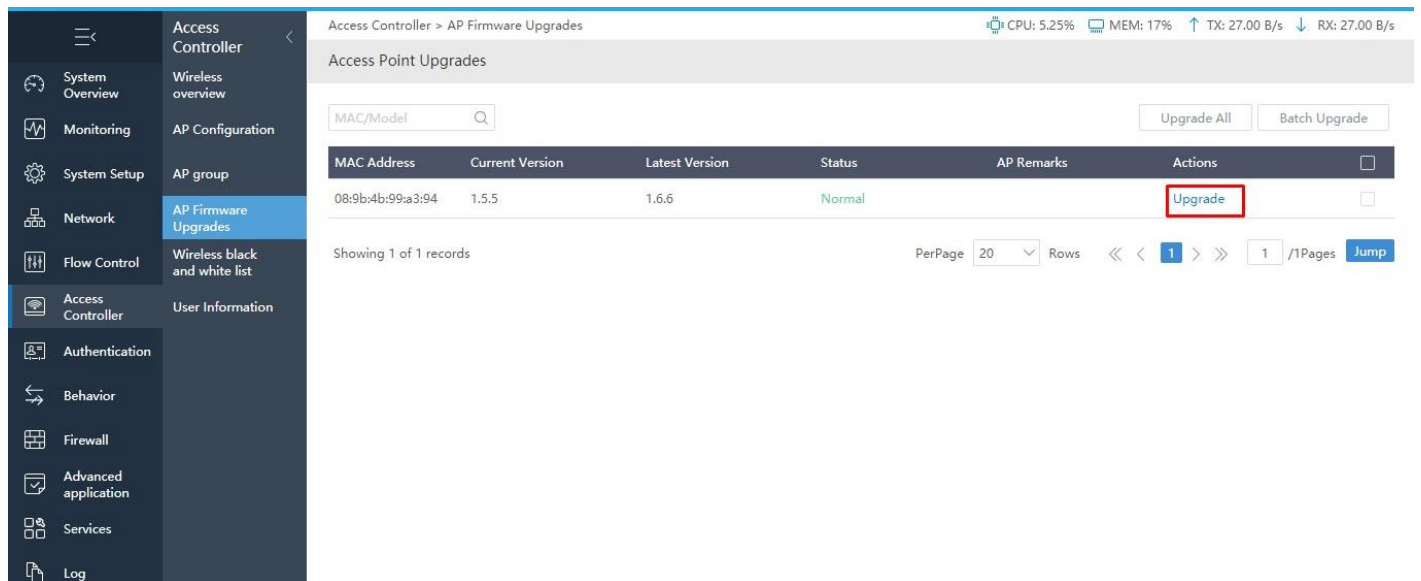


Fig 5.4.2 Upgrade firmware of Access Point page

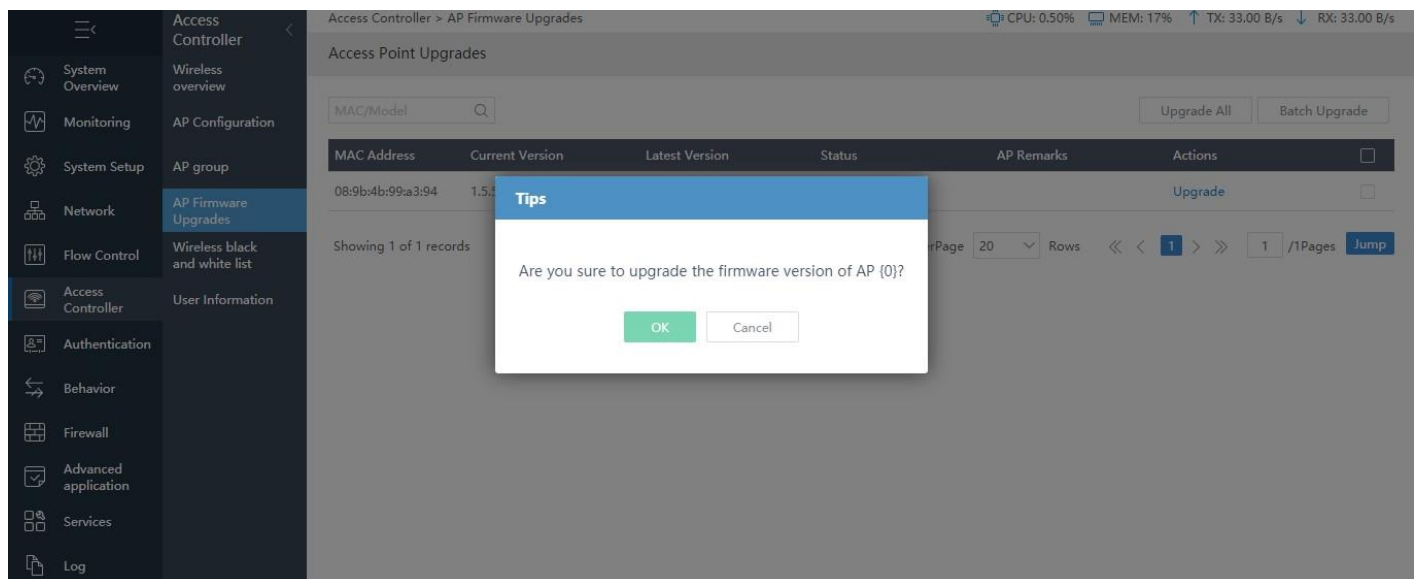


Fig 5.4.3 Upgrade firmware of selected Access Point page

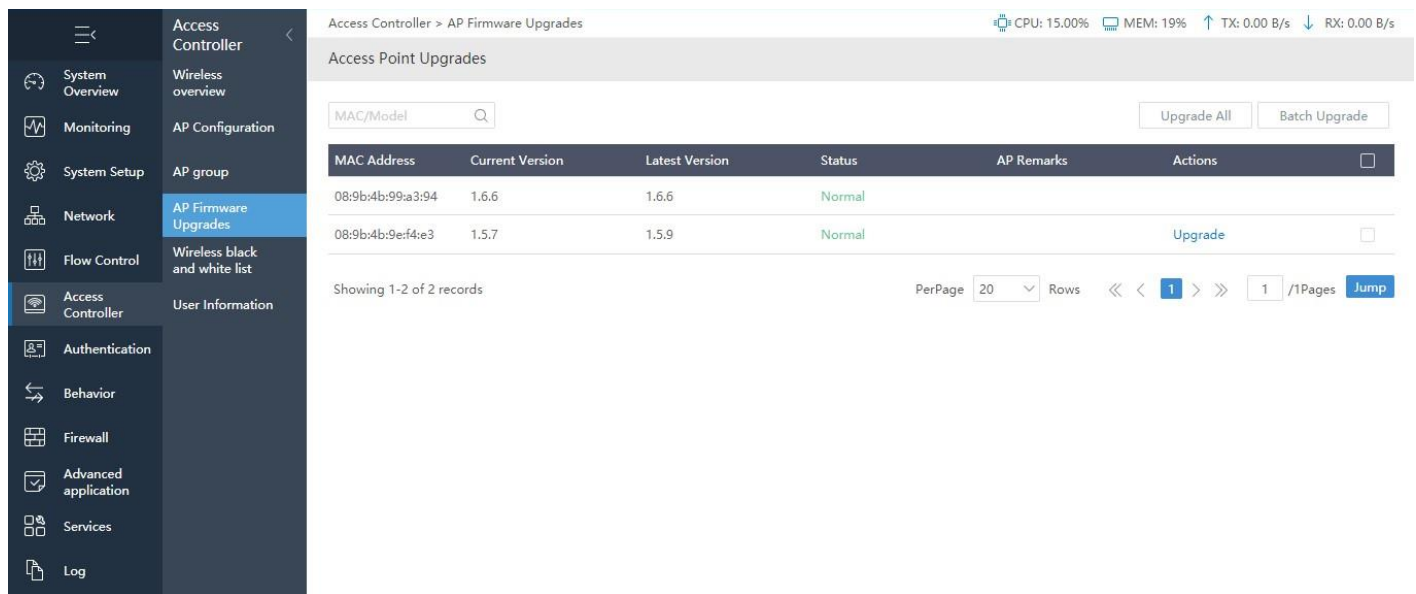


Fig 5.4.6 After Upgrading firmware Access Point Upgrade page

5.5 Wireless black and White List

In Blacklist Mode, administrator can Disable the MAC connection specified SSID in the rule. In

Whitelist Mode Only the MAC connection specified in the rule is allowed to have an SSID others all blocked.

To configure Wireless black and White List, Click on Access Controller > Wireless black and white list

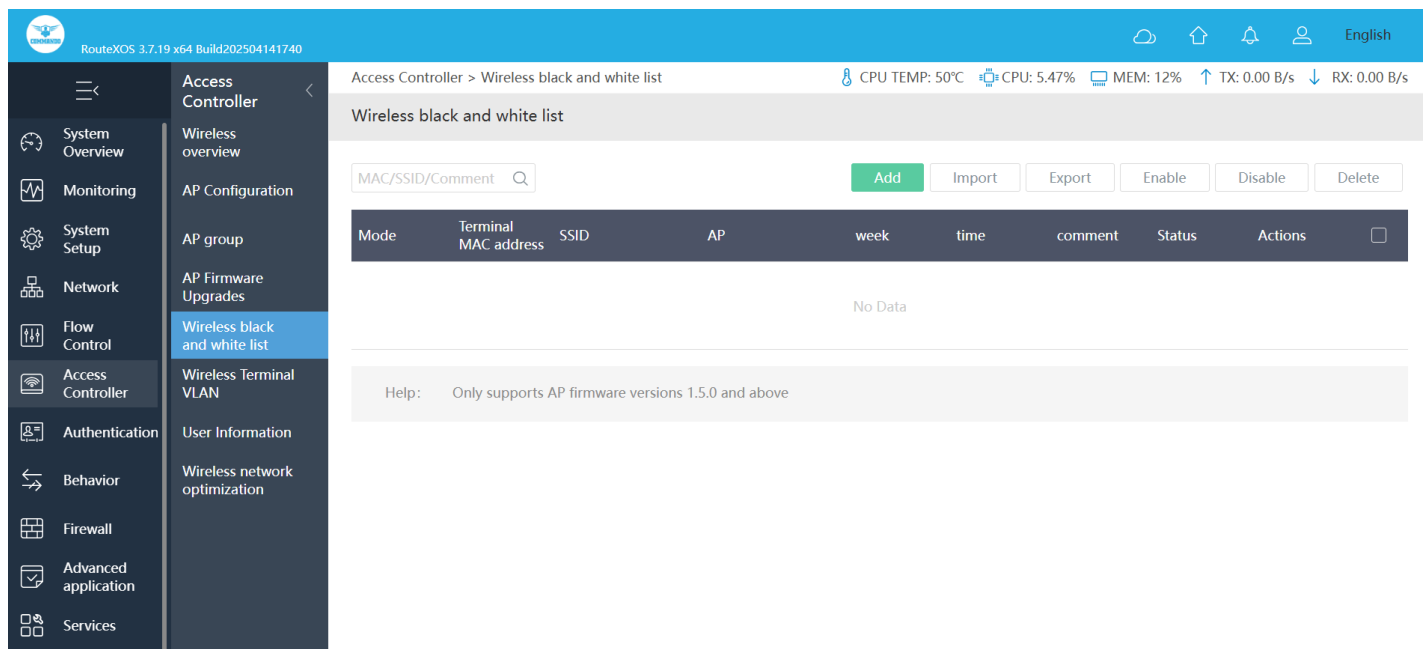


Fig 5.5.1 Default Wireless black and white list page

RouteXOS 3.7.19 x64 Build202504141740

English

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

Access Controller

Wireless overview

AP Configuration

AP group

AP Firmware Upgrades

Wireless black and white list

Wireless Terminal VLAN

User Information

Wireless network optimization

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

AP Firmware Upgrades

Wireless black and white list

Wireless Terminal VLAN

User Information

Wireless network optimization

Access Controller > Wireless black and white list

CPU TEMP: 49°C
CPU: 0.50%
MEM: 12%
TX: 0.00 B/s
RX: 0.00 B/s

Add

Mode:

☒ Blacklist Mode (Disable the MAC connection specified SSID in the rule)
☐ Whitelist Mode (Only the MAC connection specified in the rule is allowed to have an SSID)

Terminal MAC address:

Add MAC or MAC group

Add Group

Refresh

Join >>

<< Remove

SSID:

all
COMMANDO01_2G
Net1
Net2
Network 1
Network 2
Network 3
Router01_2G
Router01_5G

Join >>

<< Remove

AP:

all
82:02:fa:60:0e:26(COMMANDO AP)

Join >>

<< Remove

Week:

☒ All
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday
☒ Sunday

Time:

00:00-23:59

Remarks:

Save

Cancel

Fig 5.5.2 Add Wireless black and white list page

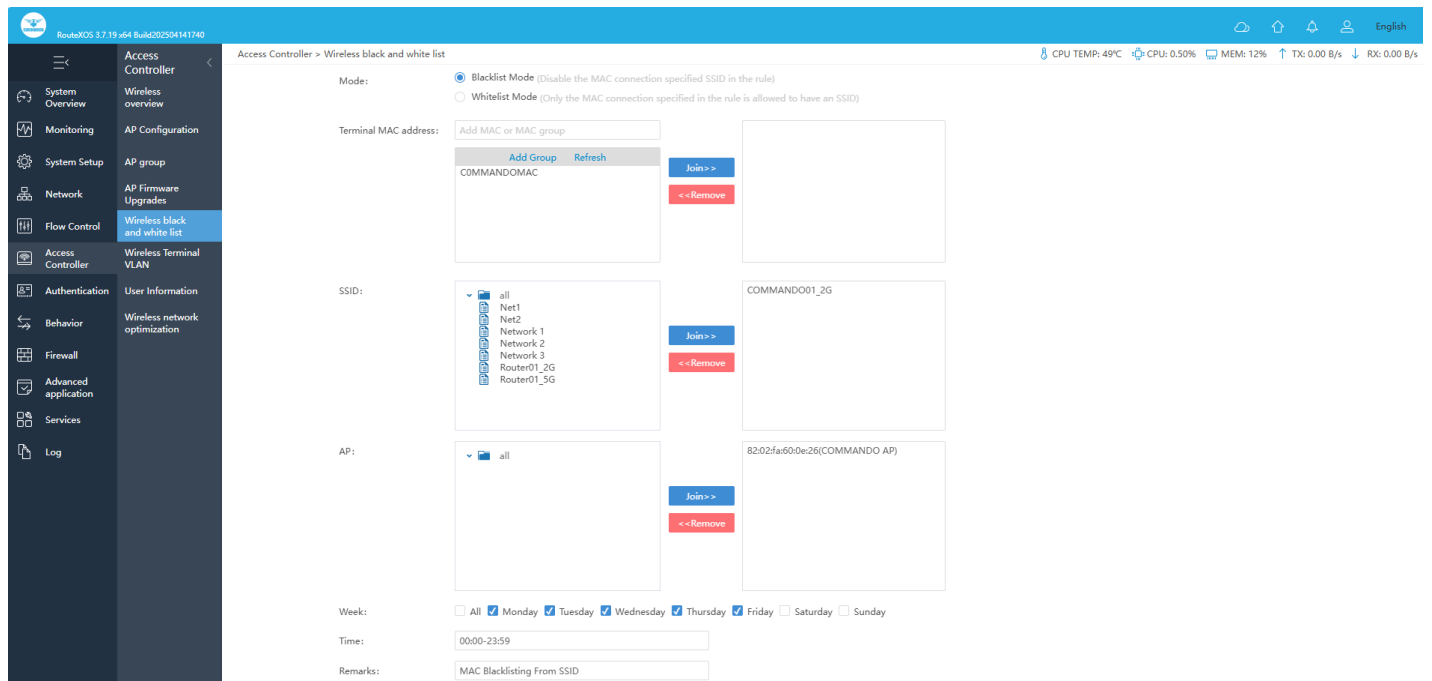


Fig 5.5.3 Wireless blacklisting for particular MAC page

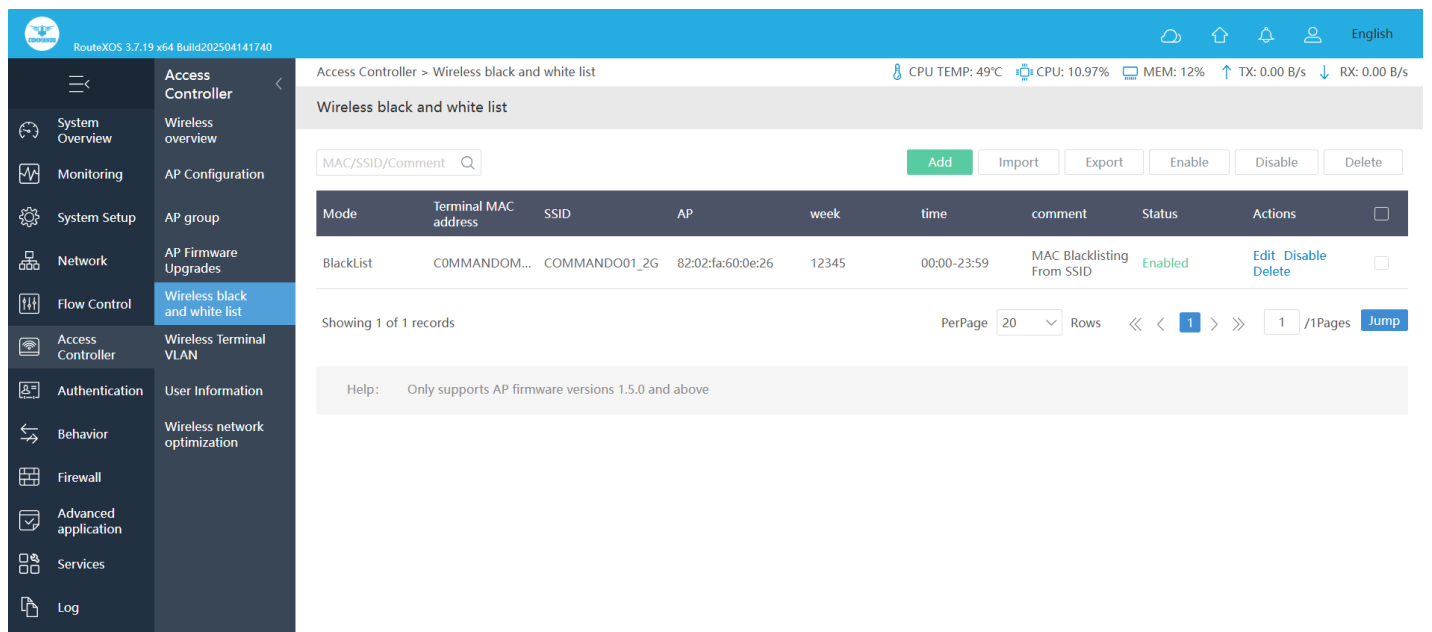


Fig 5.5.4 Wireless black and white list page

5.6 User Information

All connected users to all AP's and SSID are listed here for viewing.

To view User Information, Click on Access Controller > User Information

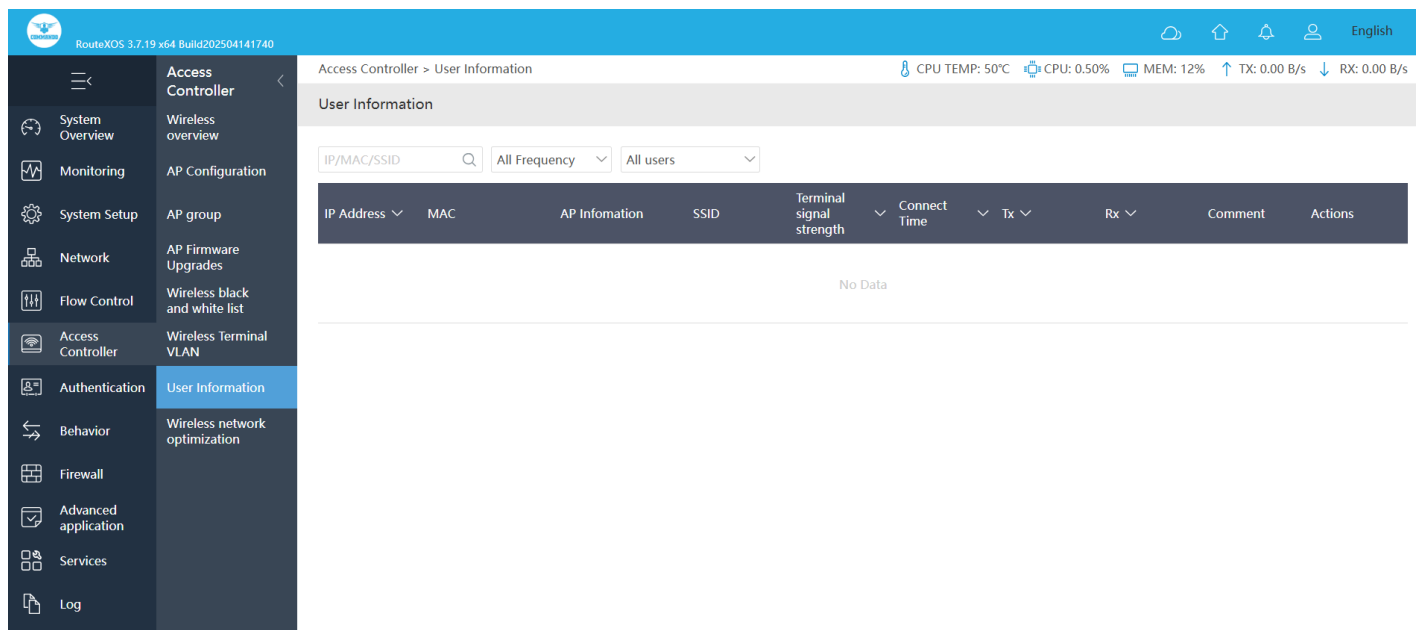


Fig 5.6.1 Default User Information page

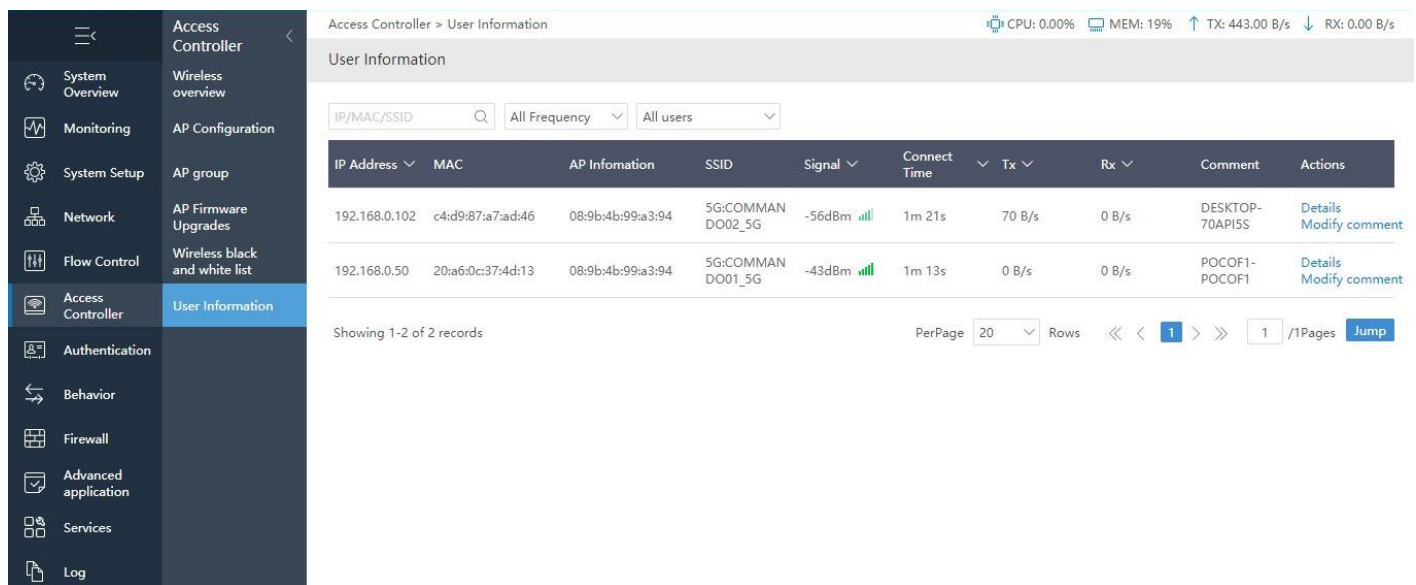


Fig 5.6.2 User Information after connecting users' page

5.7 Wireless Terminal VLAN

Wireless Terminal VLAN allows administrators to segment wireless clients into different VLANs based on predefined rules, enhancing network security and traffic management.

To configure Wireless Terminal VLAN, click on Access Controller > Wireless Terminal VLAN.

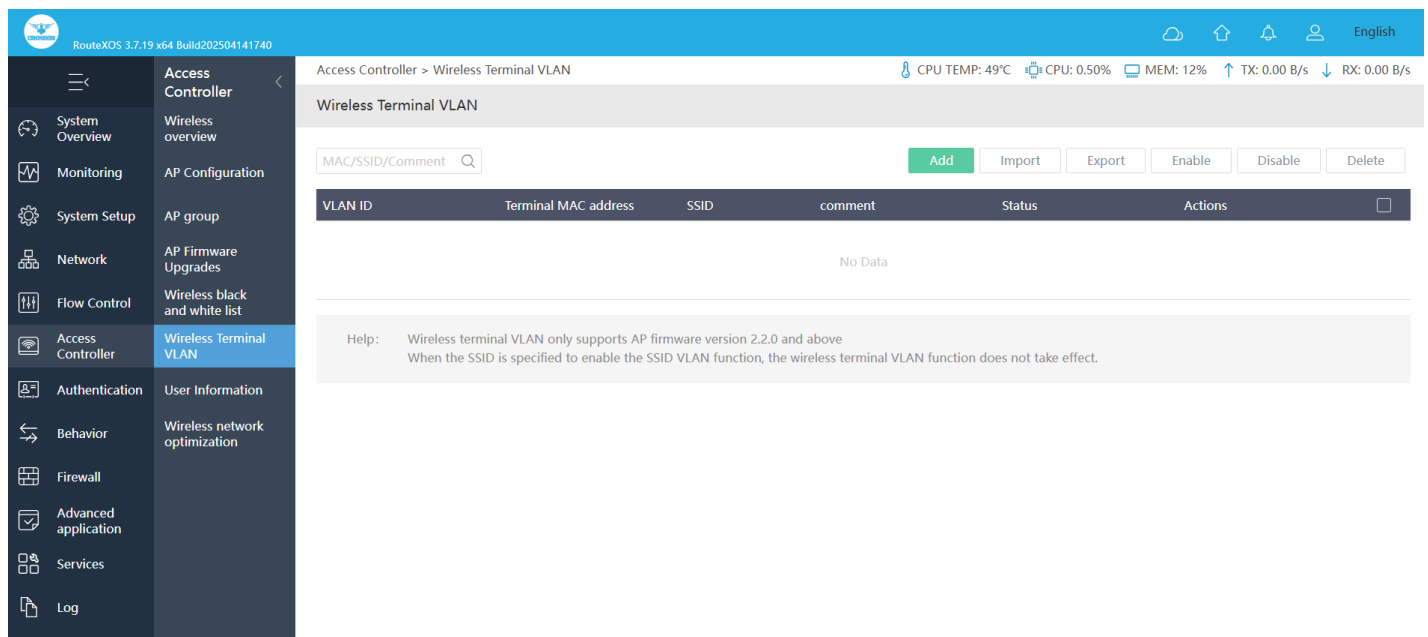


Fig 5.7.1 Default Wireless Terminal VLAN page

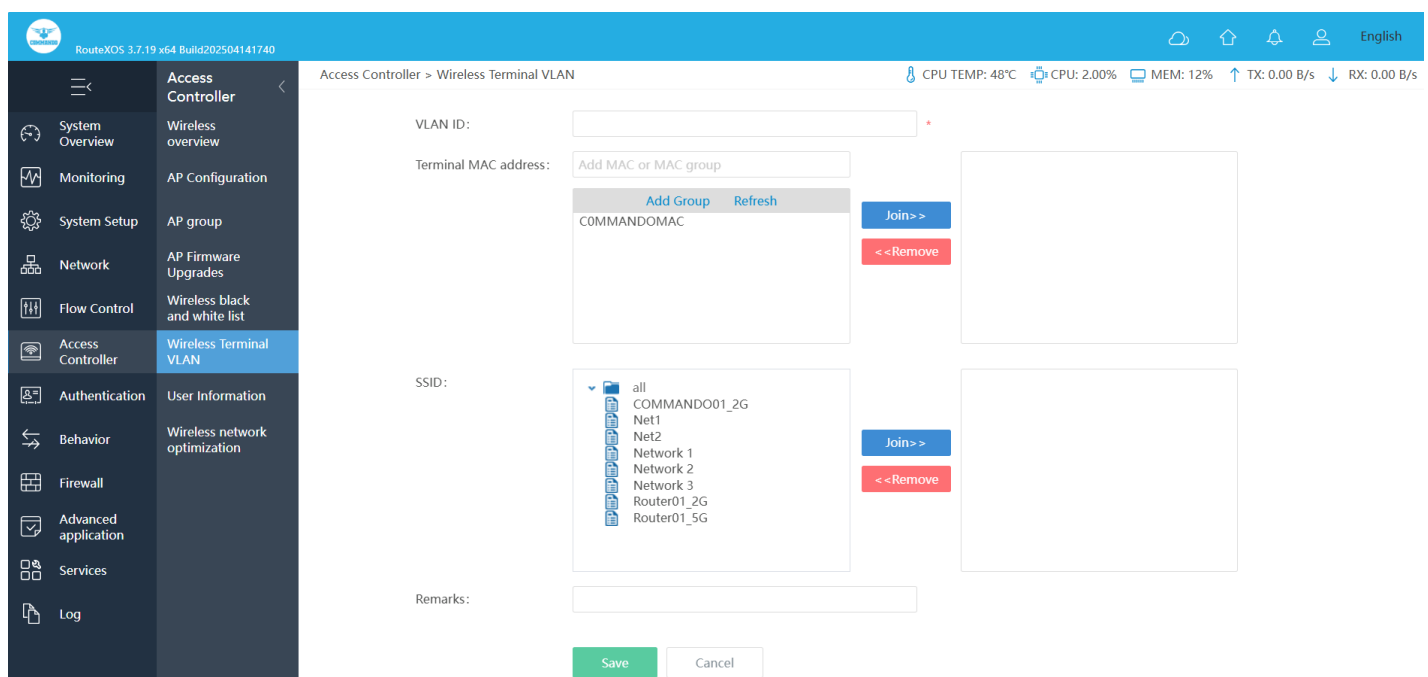


Fig 5.7.2 Add Wireless Terminal VLAN page

5.8 Wireless network optimization

Wireless Network Optimization enhances network performance by dynamically adjusting parameters like channel selection, transmission power, and interference control for a stable and efficient connection.

To configure Wireless Network Optimization, click on Access Controller > Wireless Network Optimization.

RouteXOS 3.7.19 x64 Build202504141740

Access Controller

Wireless overview

AP Configuration

AP group

AP Firmware Upgrades

Wireless black and white list

Wireless Terminal VLAN

User Information

Wireless network optimization

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application


Services

Log

Access Controller > Wireless network optimization

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Wireless network optimization



Radio frequency optimization BETA

Optimize channel only optimization2.4G+5G

Optimization record

Select optimized AP

IP/Remarks

IP Address	Remarks	Belonging to ...	Actions
192.168.0.12	COMMANDO AP	COMMANDO	Add

Optimization List

Delete all

IP Address	Remarks	Belonging to ...	Actions
------------	---------	------------------	---------

Help:

1. Select the optimized AP list to display only APS that support this function

2. The current version supports up to 50 APs per optimization

Fig 5.8.1 Default Wireless network optimization page

AUTHENTICATION

Online Auth Users: For Viewing Online Authentication Users.

Captive Portal: Portal authentication is a Network Admission Control (NAC) method. Portal authentication is also called web authentication. Generally, Portal authentication websites are referred to as Portal websites. Users must be authenticated by the Portal websites before they can use network services.

VPN Server: Can configure parameters for PPPoE, PPTP, L2TP, OpenVPN Server.

Auth Account: User accounts are created in the internal database on the controller. You can create a user role like package account, self-password management, general Ledger access code which will allow authenticate account using captive portal when user log into a captive portal login page to gain Internet access.

Push Notification: Real-time, Periodic, Expiration Reminder and Dial-up User Expiration can be notified to users connected.

Agent Service Management

Agent Service Management allows administrators to manage agent accounts and monitor active sessions in real time for secure and efficient access control.

6.1 Online Auth Users

Auth Service can quickly build secure and reliable users. The administrator can configure Auth Service and manage users.

For Viewing Online Authentication Users, Click on Push Notification Authentication > Online Auth Users

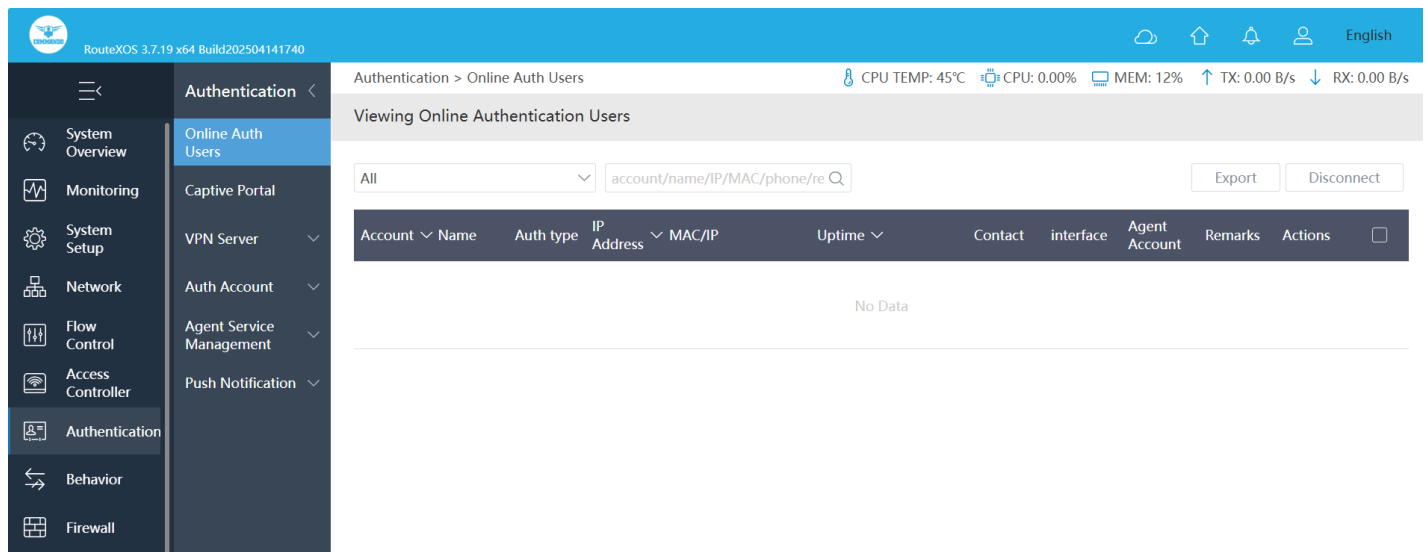


Fig 6.1.1 Default Online Authentication Users page

6.2 Captive Portal

A captive portal is a web page to which a client is redirected for authentication. The client can only gain access to the Internet after they successfully authenticated by external captive portal. Before enabling this function, you need to bind the device to the Cloud , enable authentication in the cloud, and complete the authentication configuration. Otherwise, the intranet host cannot access the external network.

Multiple devices in the same LAN, after configuring the same authentication group ID and key, can implement the user roaming-free authentication service under multiple gateway devices.

For enabling Captive Portal Settings, Click on Authentication > Captive Portal

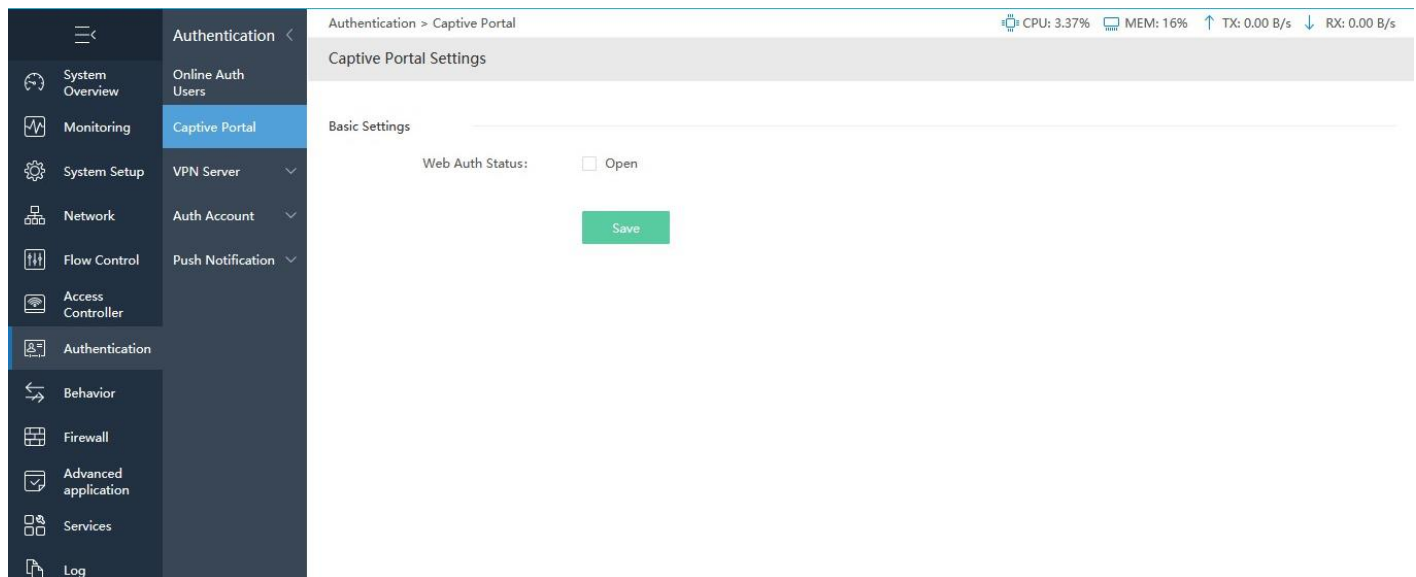


Fig 6.2.1 Default Captive Portal Settings page

How to enable Captive Portal Settings?

For enabling Captive Portal Settings, Click on Authentication > Captive Portal Click on open in Web Auth Status and Save button.

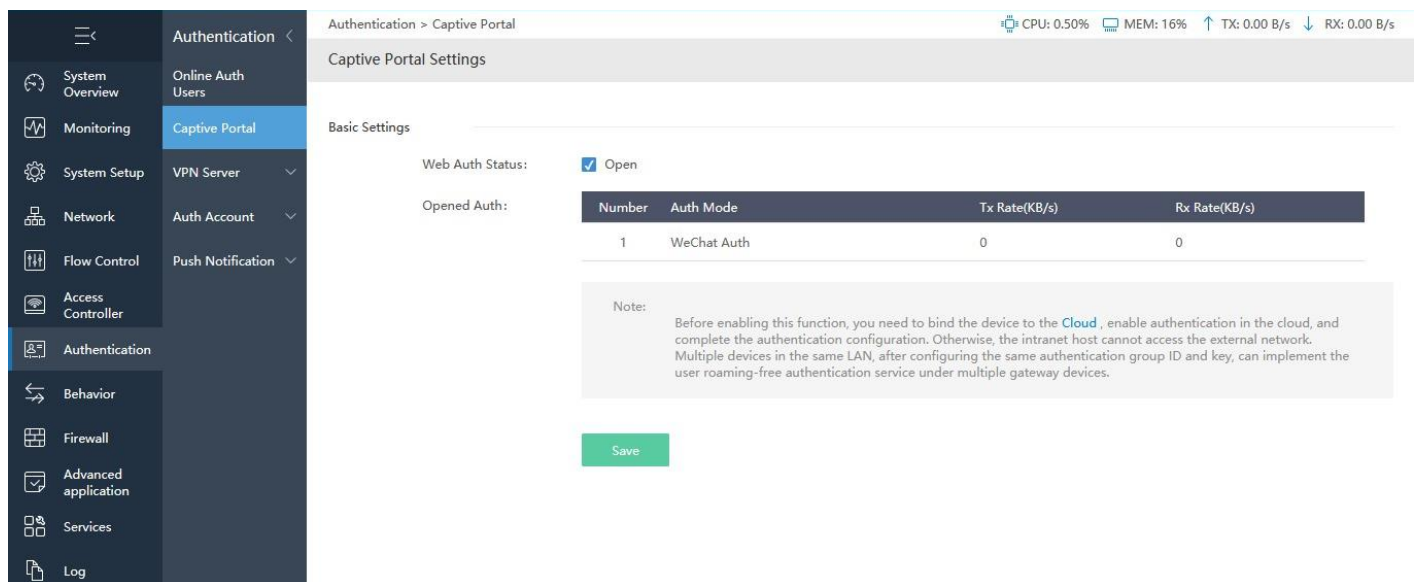


Fig 6.2.2. Enabling Captive Portal Settings page

6.3 VPN Server

Virtual Private Network (VPN) establishes a secure, encrypted communications between your local server and connected internet users. A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address, so your online actions are virtually untraceable. Enter your VPN account username and password used to provide

virtual (as opposed to physical) access to a private network. The VPN security model provides confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and deep packet inspection), an attacker would see only encrypted data sender authentication to prevent unauthorized users from accessing the VPN message integrity to detect any instances of tampering with transmitted messages. PPPoE is an acronym that stands for Point-to-Point Protocol over Ethernet. PPPoE was designed for managing how data is transmitted over Ethernet networks (cable networks), and it allows a single server connection to be divided between multiple clients, using Ethernet.

To configure PPPoE Server Settings, Click on Authentication > VPN Server > PPPoE Server

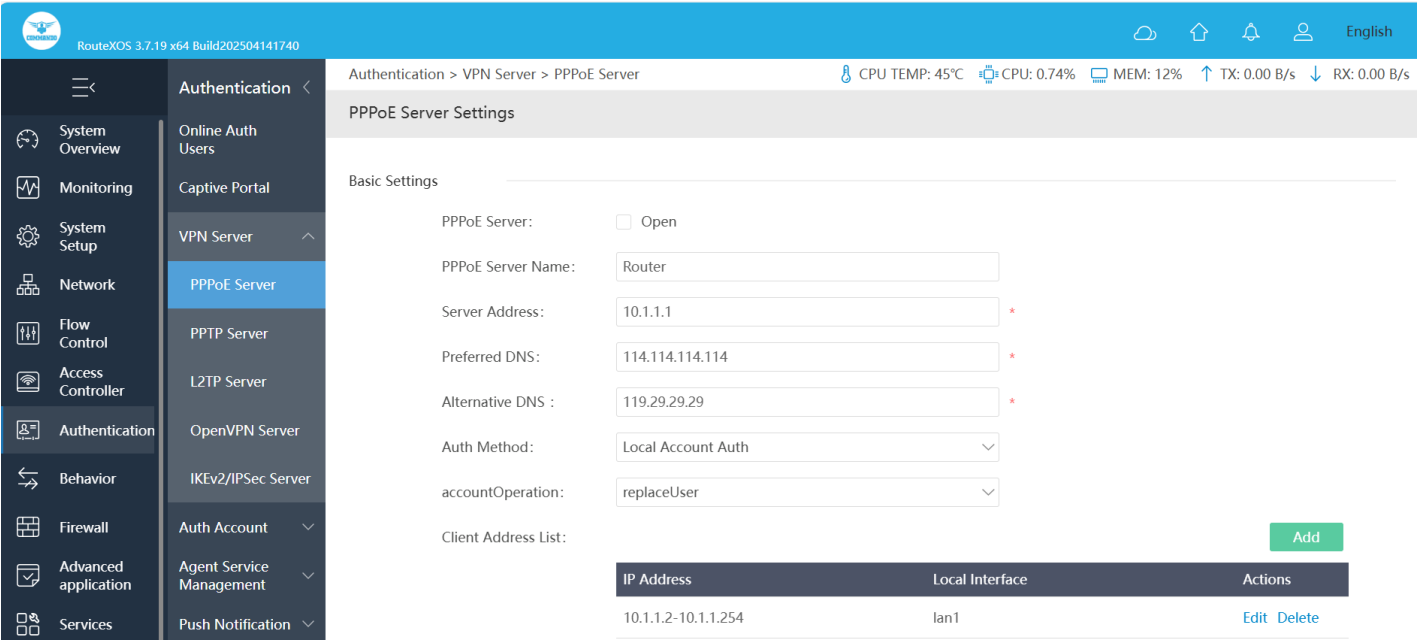


Fig 6.3.1 Default PPPoE Server Settings page

Fig 6.3.2 Setting PPPoE Server Settings page PPTP

Server: A PPTP Server (Point-To-Point Tunneling Protocol) allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office, etc. This way you can use the services provided in your office at the comfort of your home. It enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. To use the VPN feature, you should enable PPTP VPN Server on your Gateway.

Note:

- No encryption: If the client needs encryption, the server will be disconnected, the connection speed will be faster without encryption
- Optional encryption: can be connected without encryption, the connection speed will be faster without encryption
- Requires encryption: if the client refuses, server will be disconnected.

To configure PPTP Server Settings, Click on Authentication > VPN Server > PPTP Server

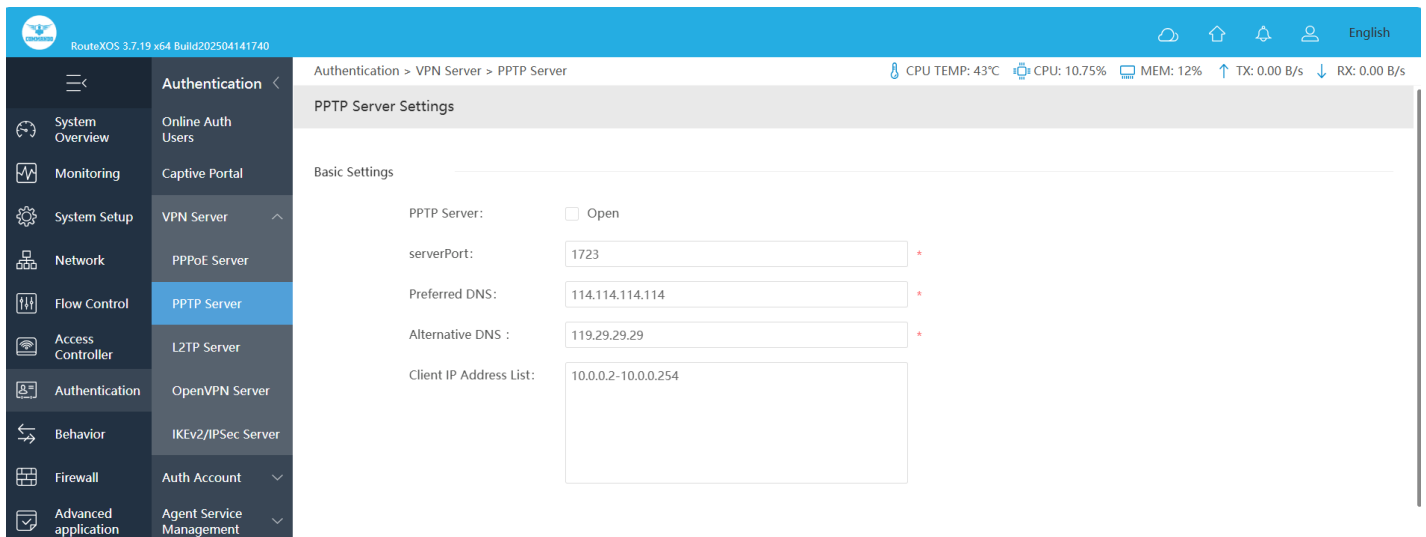


Fig 6.3.3 Default PPTP Server Settings page

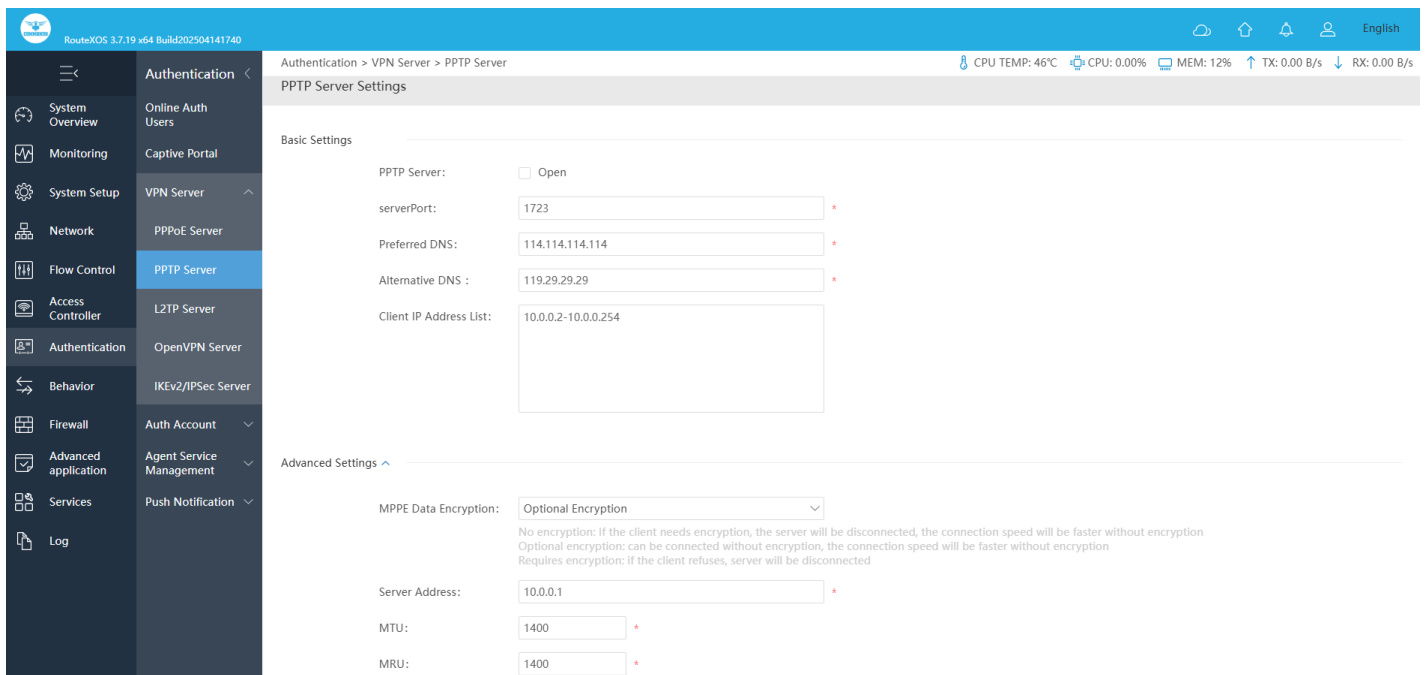


Fig 6.3.4 PPTP Server Settings after configuration page

L2TP Server Settings: Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP protocol is based on the client and server model. L2TP (Layer Two Tunneling Protocol) is considered a bit more secure than PPTP as it uses 256bit keys giving a higher level of encryption. L2TP encapsulates data twice making it less efficient and slightly slower.

To configure L2TP Server Settings, Click on Authentication > VPN Server > L2TP Server

RouteXOS 3.7.19 x64 Build202504141740

Authentication > VPN Server > L2TP Server

CPU TEMP: 46°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

L2TP Server Settings

L2TP Server: ☐ Open

serverPort:

Client IP Address List:

Server Address:

Preferred DNS:

Alternative DNS :

MTU:

MRU:

Pre-shared Key:

Local ID:

Peer ID:

Deny non-encrypted connections: ☐ Open

Fig 6.3.5 Default L2TP Server Settings page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > VPN Server > L2TP Server

CPU TEMP: 47°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

L2TP Server Settings

L2TP Server: ☒ Open

serverPort:

Client IP Address List:

Server Address:

Preferred DNS:

Alternative DNS :

MTU:

MRU:

Pre-shared Key:

Local ID:

Peer ID:

Deny non-encrypted connections: ☒ Open

Fig 6.3.6 Setting L2TP Server Settings page OpenVPN

Server Settings: OpenVPN Access Server is a set of installation and configuration tools that come in one package that simplifies the rapid deployment of a VPN remote access solution. Thus, OpenVPN Access Server streamlines the configuration and management of an OpenVPN based secure remote access deployment. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for

creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

To configure OpenVPN Server Settings, Click on Authentication > VPN Server > OpenVPN Server

The screenshot shows the 'OpenVPN Server Settings' page in the RouteXOS interface. The left sidebar contains a menu with 'Authentication' selected, and 'OpenVPN Server' highlighted under it. The main content area displays the following settings:

- OpenVPN Server:** ☐ Open
- Server Port:** 1194
- VPN Segment:** 10.7.7.0
- Subnet Mask:** 255.255.255.0
- Verification Method:** Account Verification
- Tunnel Protocol:** UDP
- Tunnel Type:** TUN
- Topology type:** SUBNET
- Encryption Algorithm:** BF-CBC
- LZO Compression:** ☒ Open
- MTU:** 1400

Buttons at the top of the settings area include 'Export windows client configuration', 'Show log', and 'Restore default'. The top status bar shows system metrics: CPU TEMP: 47°C, CPU: 0.74%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s.

Fig 6.3.7 Default OpenVPN Server Settings page

The screenshot shows the 'OpenVPN Server Settings' page after configuration. The settings are as follows:

- OpenVPN Server:** ☒ Open
- Server Port:** 1194
- VPN Segment:** 192.168.7.0
- Subnet Mask:** 255.255.255.0
- Verification Method:** Account Verification
- Tunnel Protocol:** TCP
- Tunnel Type:** TUN
- Topology type:** SUBNET
- Encryption Algorithm:** BF-CBC
- LZO Compression:** ☒ Open
- MTU:** 1500

The top status bar shows updated system metrics: CPU TEMP: 46°C, CPU: 0.00%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s.

Fig 6.3.8 Setting OpenVPN Server Settings page

IKEv2/IPSec Server Settings: IKEv2/IPSec Server provides a secure and efficient VPN solution for remote access and site-to-site connectivity. It simplifies the deployment and management of encrypted VPN tunnels, ensuring data confidentiality, integrity, and authentication. IKEv2 offers strong security, fast reconnection capabilities, and seamless mobility support, making it ideal for enterprise and mobile users.

To configure IKEv2/IPSec Server Settings, click on Authentication > VPN Server > IKEv2/IPSec Server

The screenshot shows the 'IKEv2/IPSec Server' configuration page within the 'Authentication > VPN Server' menu. The interface includes a top status bar with system metrics (CPU TEMP: 47°C, CPU: 0.50%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s) and a left sidebar with navigation options. The main configuration area contains the following fields:

- Ipssec IKEv2 Server Status:** A checkbox labeled 'Open'.
- Type:** A dropdown menu set to 'IKEv2/IPsec MSCHAPv2'.
- Client Address Pool:** A text input field containing '10.6.1.0/24'.
- Preferred DNS:** A text input field containing '114.114.114.114'.
- Alternate DNS:** A text input field containing '119.29.29.29'.
- Local ID:** An empty text input field with a red asterisk and a 'Generate PK and Certificates' button.
- Opposite ID:** An empty text input field with a note: 'Empty means that the client's local ID can be set to any'.
- Server Certificate:** A large empty text area with a note below it: 'The default certificate is a self-signed certificate, which is only applicable to Router client and server connections'.
- Private Key:** A large empty text area.

Fig 6.3.9 Default IKEv2/IPSec Server page

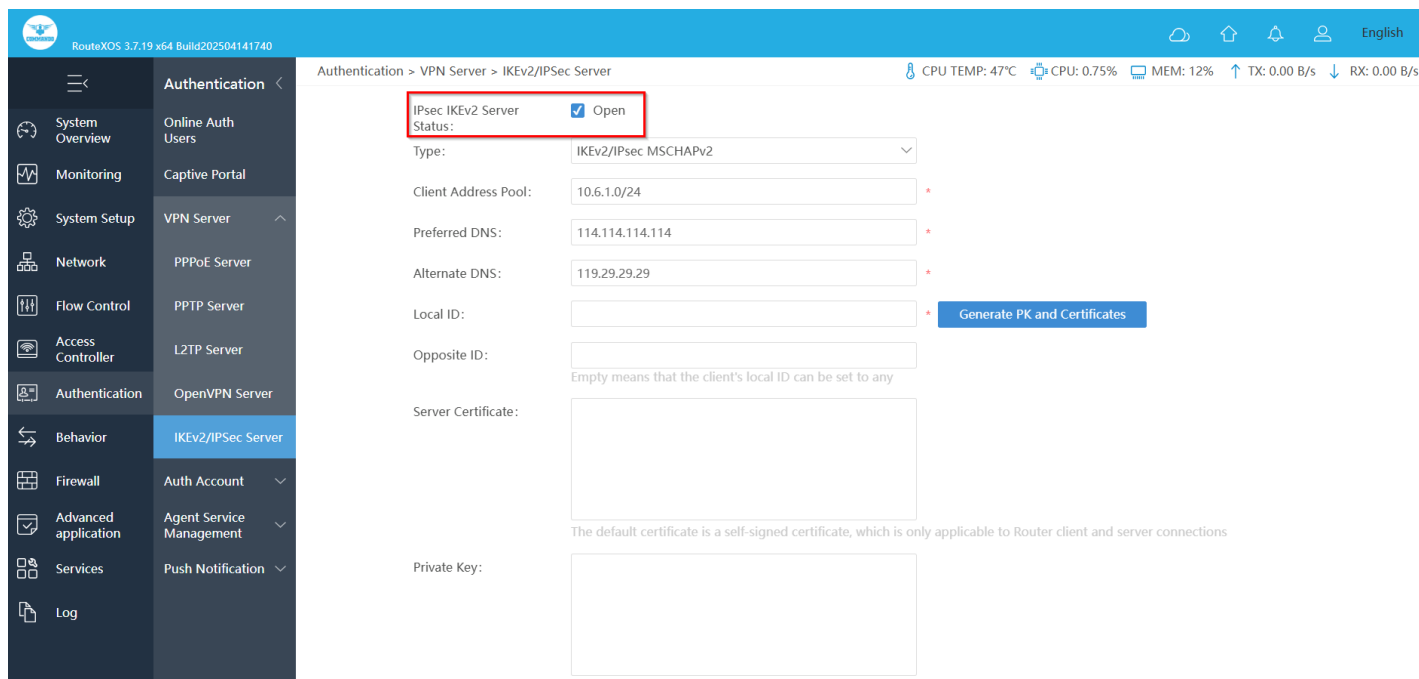


Fig 6.3.10 Setting up OpenVPN Server page

6.4 Authentication Account

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID.

To Manage Package, Click on Authentication > Auth Account > Package

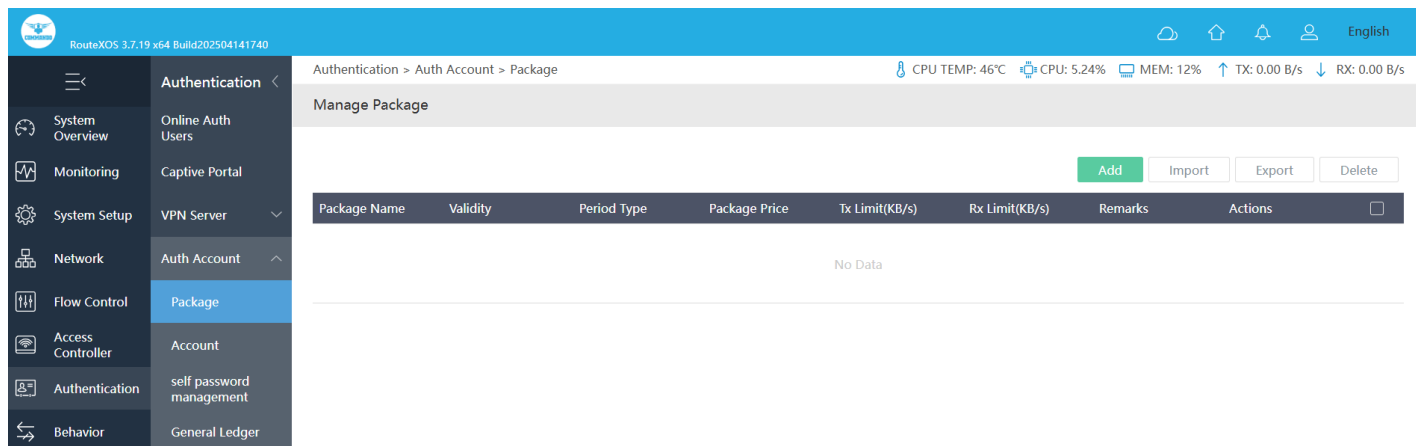


Fig 6.4.1 Default Manage Package Account page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 47°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Online account configuration

Account: *

Password: *

Auth type: Any

Package type: Custom *

Up speed: 0 KB/s *

Down rate: 0 KB/s *

Start time: 2025-08-01 13:04:02 *

Due time: Select Date *

Payment amount:

Share: 1 *

Bind VLAN: 0 *

The default value is 0, Only support PPPoE, support QinQ, 2008.100

☒ Auto VLAN

Fig 6.4.2 Add Online Account configuration page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Package

CPU TEMP: 47°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Package Name: COMMANDO *

Period Type: Hour

Validity: 20 *

Package Price: 200 *

Tx Limit(KB/s): 1000 *

Rx Limit(KB/s): 1000 *

Remarks: COMMANDO Package

Save Cancel

Fig 6.4.3 Add particular Online Account configuration page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Package

CPU TEMP: 47°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Manage Package

Add Import Export Delete

Package Name	Validity	Period Type	Package Price	Tx Limit(KB/s)	Rx Limit(KB/s)	Remarks	Actions
COMMANDO	20	Hour	200	1000	1000	COMMANDO Package	Edit Copy Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 6.4.4 Manage package page

Manage Account: For creating and managing account use the following tabs.

To Manage Account, Click on Authentication > Auth Account > Account

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 49°C CPU: 13.28% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Manage Account

Total condition All time All auth Please input account, name, Q

Add Import Export Enable Disable Delete

Account	Username	Auth type	Current type	Due time	Online/offline duration	Remarks	Status	Actions
No Data								

Fig 6.4.5 Default Mange Account page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 46°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Online account configuration

Account:

Password:

Auth type:

Package type:

Up speed: KB/s

Down rate: KB/s

Start time:

Due time:

Payment amount:

Share:

Fig 6.4.6 Add Manage Account page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 45°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Binding NIC:

Binding MAC:

MAC addr:

IP binding type:

Fixed IP:

Online customer information

Username:

ID number:

Telephone:

Addr:

Remarks:

Save Cancel

Fig 6.4.7 Add Online account configuration page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 48°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Online account configuration

Account: COMMANDOAC *

Password: ***** *

Auth type: Any

Package type: Custom *

Up speed: 100 KB/s *

Down rate: 50 KB/s *

Start time: 2025-08-01 13:09:00 *

Due time: 2025-08-22 13:13:38 *

Payment amount: 2000

Share: 1 *

Bind VLAN: 0 *

The default value is 0,Only support PPPoE,support QinQ,802.1Q

☒ Auto VLAN

Fig 6.4.8 Add particular Online account configuration page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Account

CPU TEMP: 48°C CPU: 12.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Manage Account

Total condition: All time All auth Please input account, name, Q

Add Import Export Enable Disable Delete

Account	Username	Auth type	Current type	Due time	Online/offline duration	Remarks	Status	Actions
COMMANDOAC		Any	Custom	2025-08-22 13:13:38			Yes	Detail Charge Edit Disable Delete

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1 Pages Jump

Fig 6.4.9 Manage Online account page

Self password management: A password, sometimes called a passcode, is secret data, typically a string of characters. For self correction issuance of replacements for lost passwords, a feature called self service password.

To configure and enable self password management, Click on Authentication > Auth Account > self password management

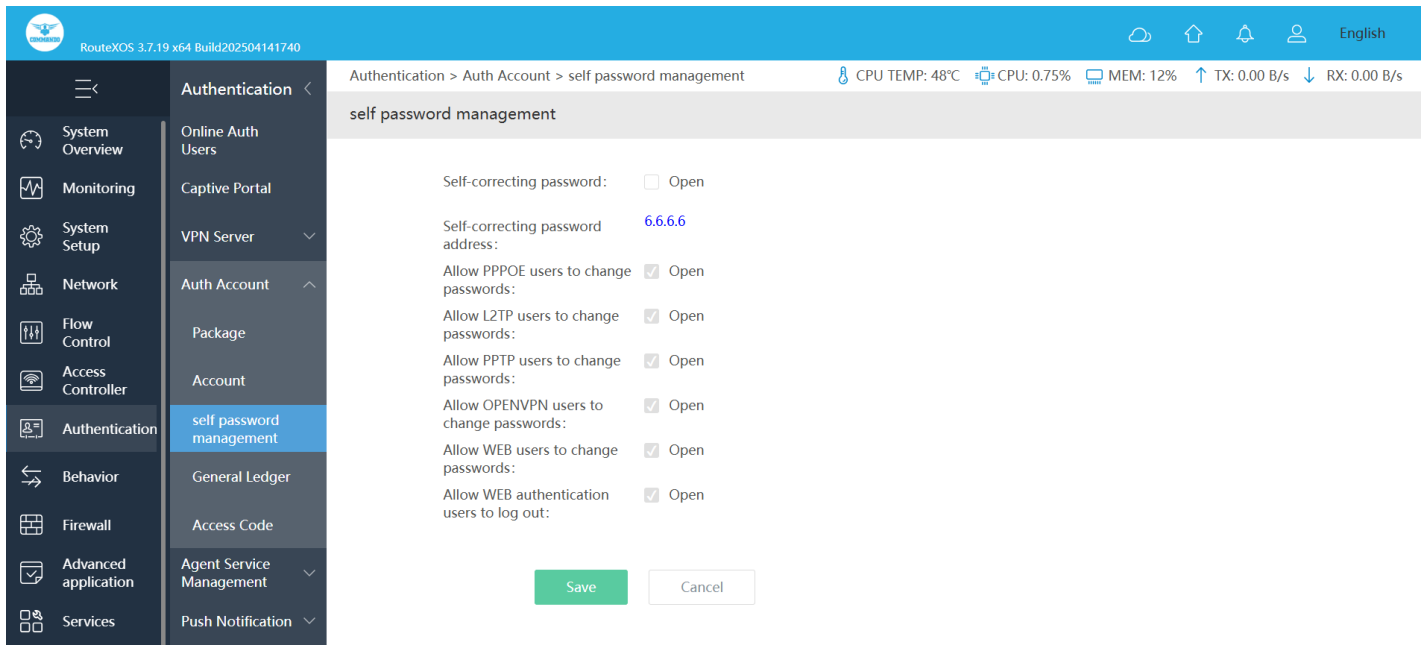


Fig 6.4.10 Default self password management page

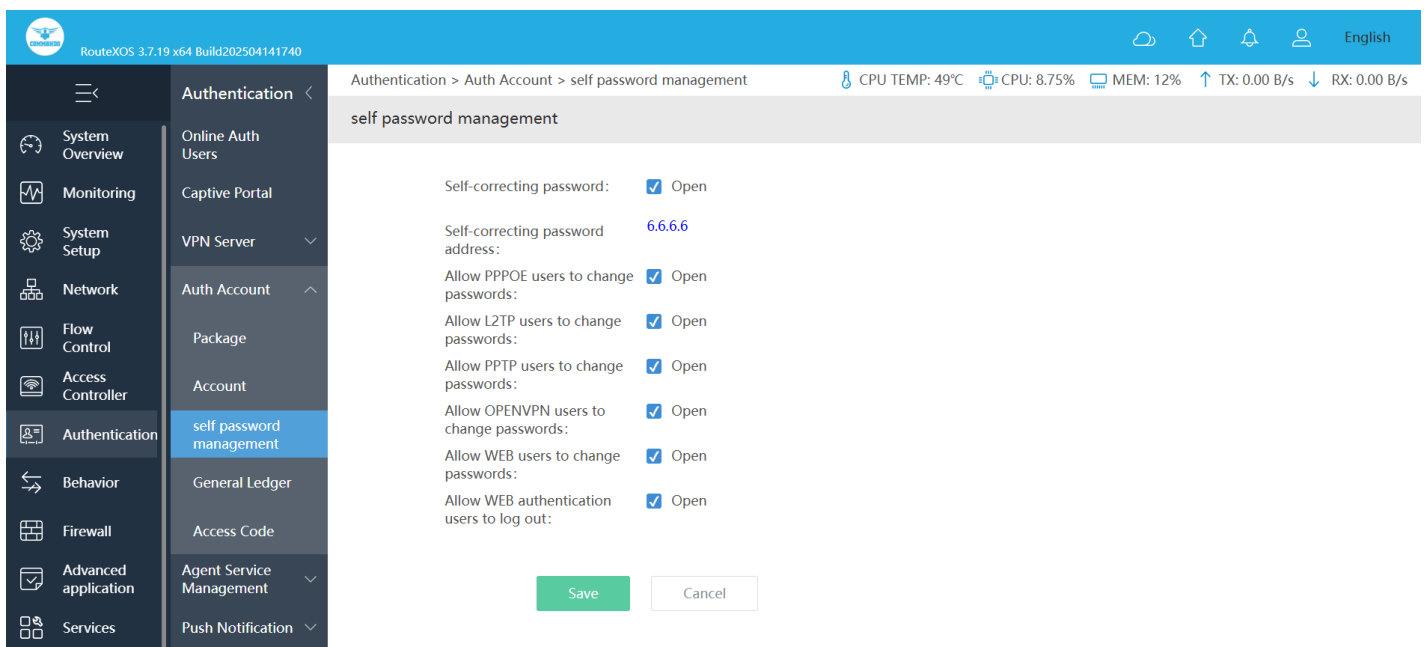


Fig 6.4.11 Enabling self password management page

General Ledger: A general ledger contains accounts record of all past transactions of a part of the entire network, making it less dependent on a single centralized node. A general ledger is for keeping record of a company's total financial accounts.

For Viewing General Ledger, Click on Authentication > Auth Account > General Ledger

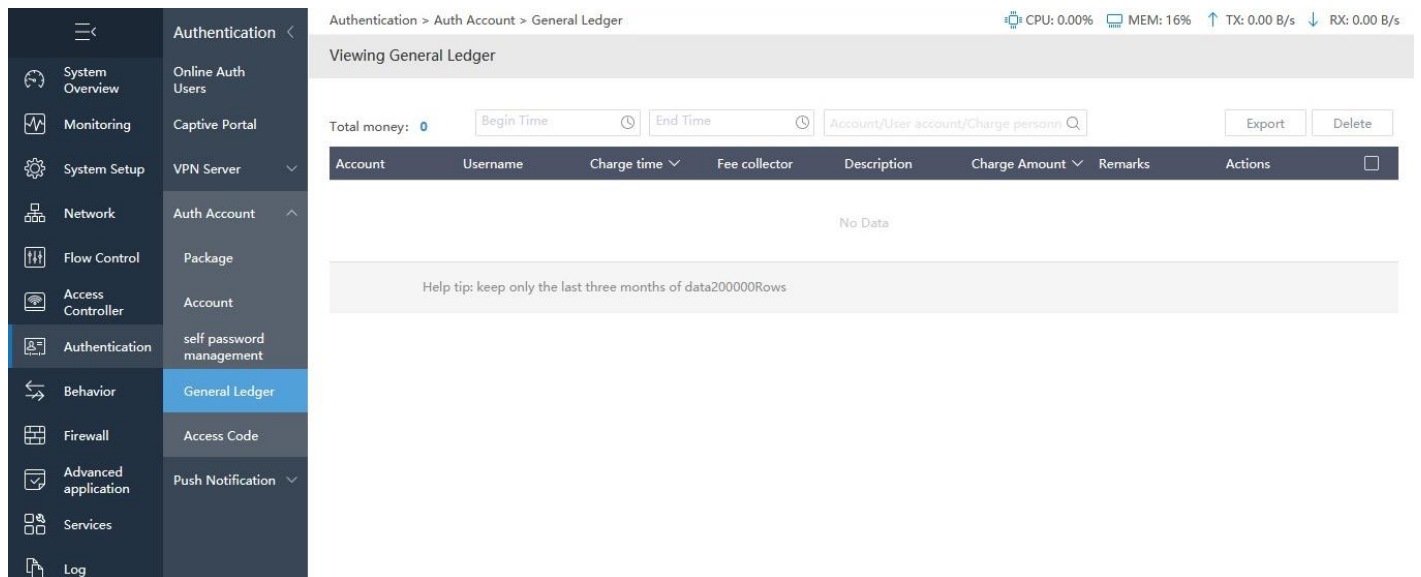


Fig 6.4.12 Default General Ledger page

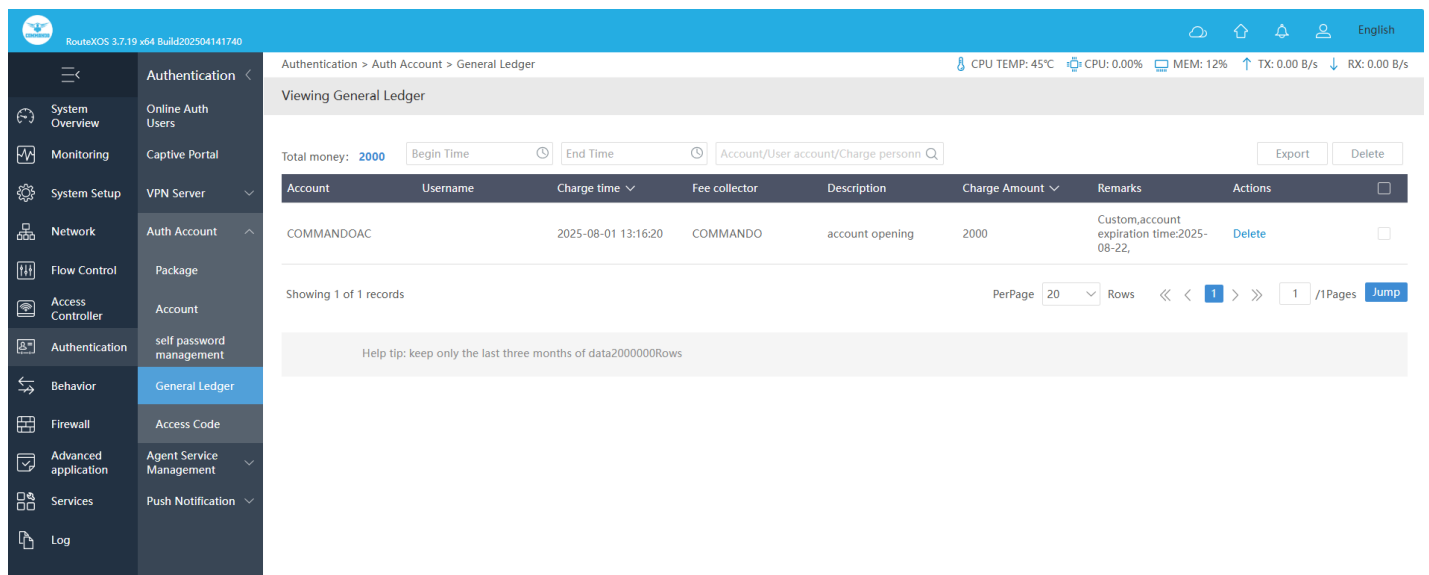


Fig 6.4.13 Viewing General Ledger page

Manage Access Code: It is a code or a password that a user enters to gain access to a private network, Internet or server. It is a form of authentication that either permits or blocks an access attempt from entering a corporate system. A remote access code is important for businesses that use remote access technology. An access code is a password you use to access internet or be online. The content you access depends on your set choice it can include internet, e-book, practice exam questions, interactive videos to help you understand course concepts, and course assignments.

For configure and Manage Access Code, Click on Authentication > Auth Account > Access Code

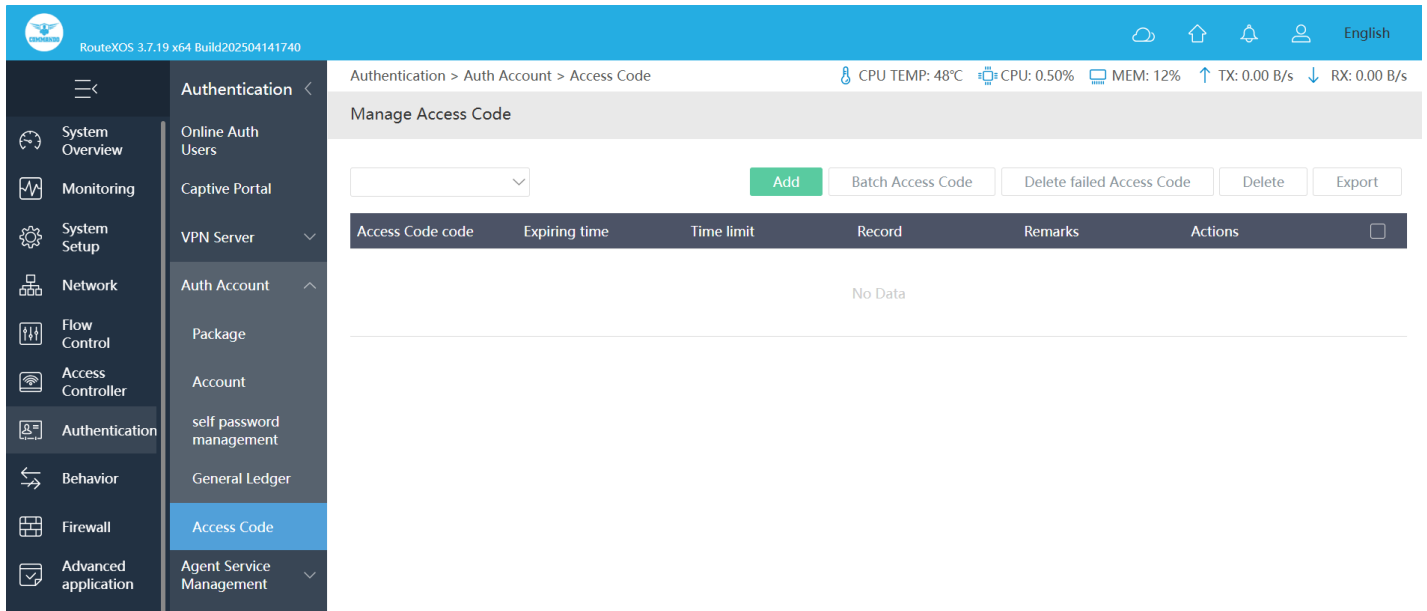


Fig 6.4.14 Default Manage Access Code page

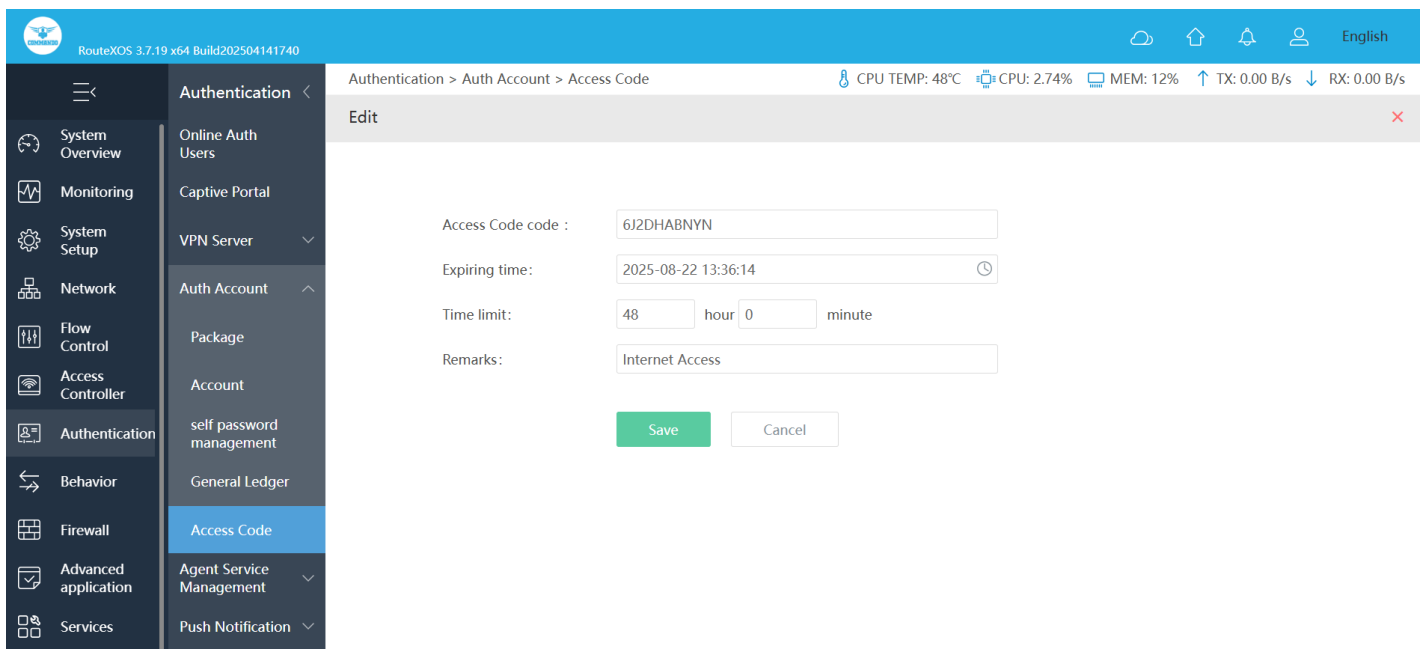


Fig 6.4.15 Add Manage Access Code page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Auth Account > Access Code

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Manage Access Code

Access Code code Expiring time Time limit Record Remarks Actions

6J2DHABNBN	2025-08-22 13:36:14	48Hour0Minute	Unused	Internet Access	Edit Delete
------------	---------------------	---------------	--------	-----------------	-------------

Showing 1 of 1 records

PerPage 20 Rows 1 / 1Pages Jump

Fig 6.4.16 Manage Access Code page

6.5 Push Notification

A push notification is a message that pops up on an end device like PC or mobile. R100 can send them at any time. Push notifications are short, meant as a marketing tool to get your users to engage with your application. Push notifications powered by COMMANDO Cloud. If a message is delivered through one of these push services, the notification from the other cloud service is suppressed. This ensures that the user will only receive the push notification once.

Note: Countdown 0s means no countdown is enabled or no countdown time is set, or a confirmation button on the notification page is manually clicked during the countdown time, otherwise port 80 will be used all the time. Please use the real-time notification function with caution.

To configure Real-time Notification Settings, Click on Authentication > Push Notification > Real-time

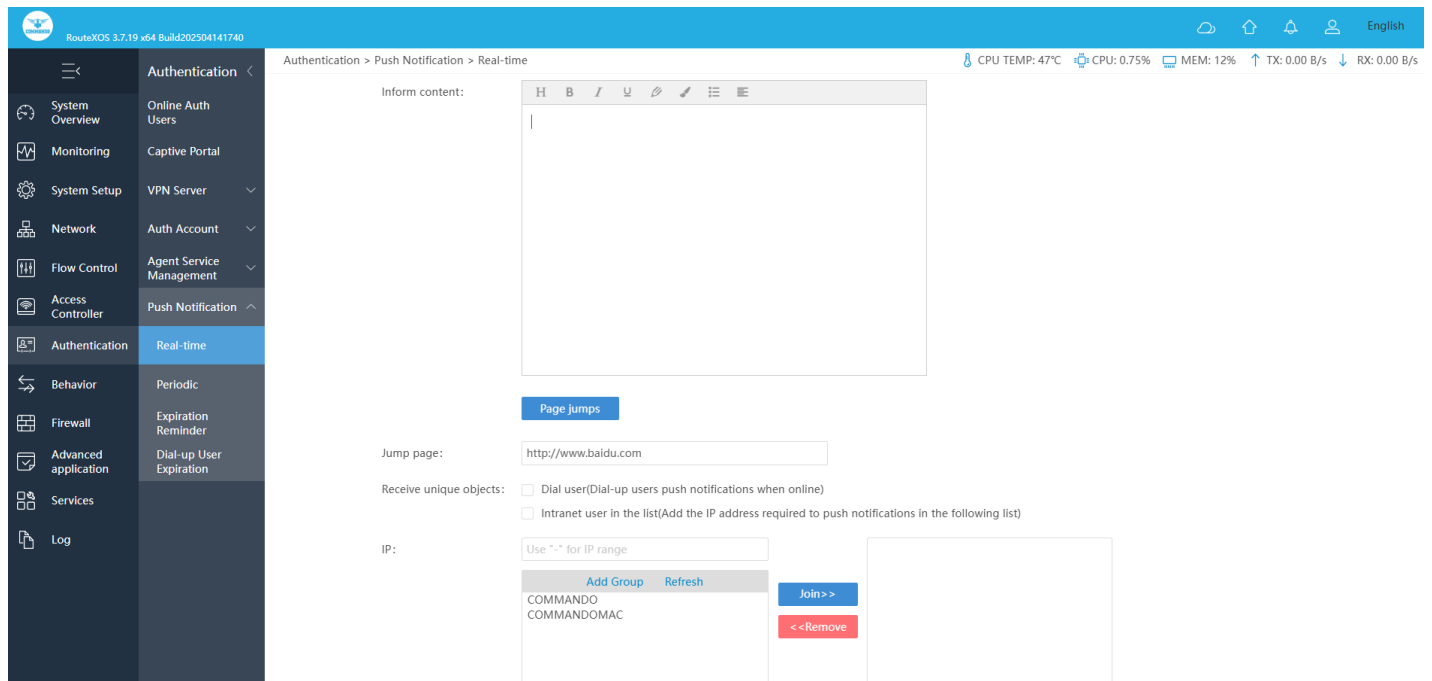


Fig 6.5.1 Default Real-time Notification Settings page

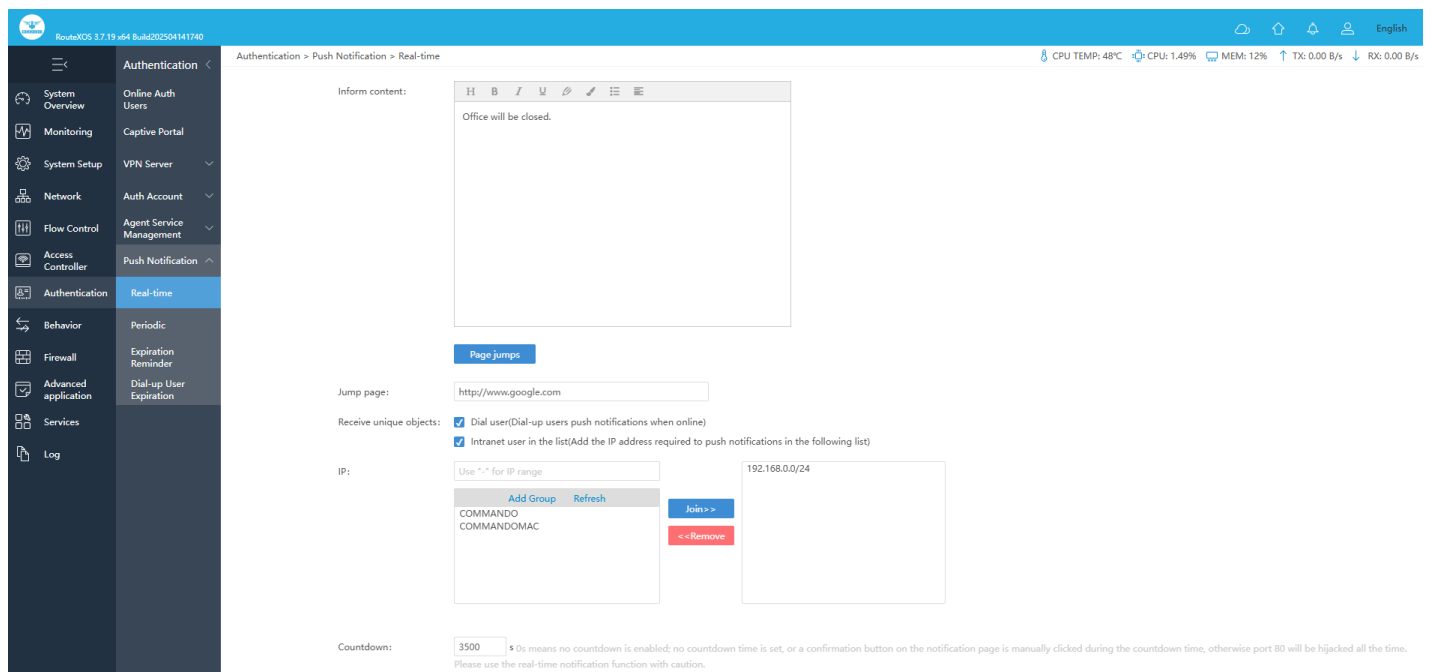


Fig 6.5.2 Real-time Notification Settings page

Periodic Notification Settings: It based on an interval queue by default. You can customize notification reminders so that you get notifications the way you want them Customize Notification Periodically.

To configure Periodic Notification Settings, Click on Authentication > Push Notification > Periodic

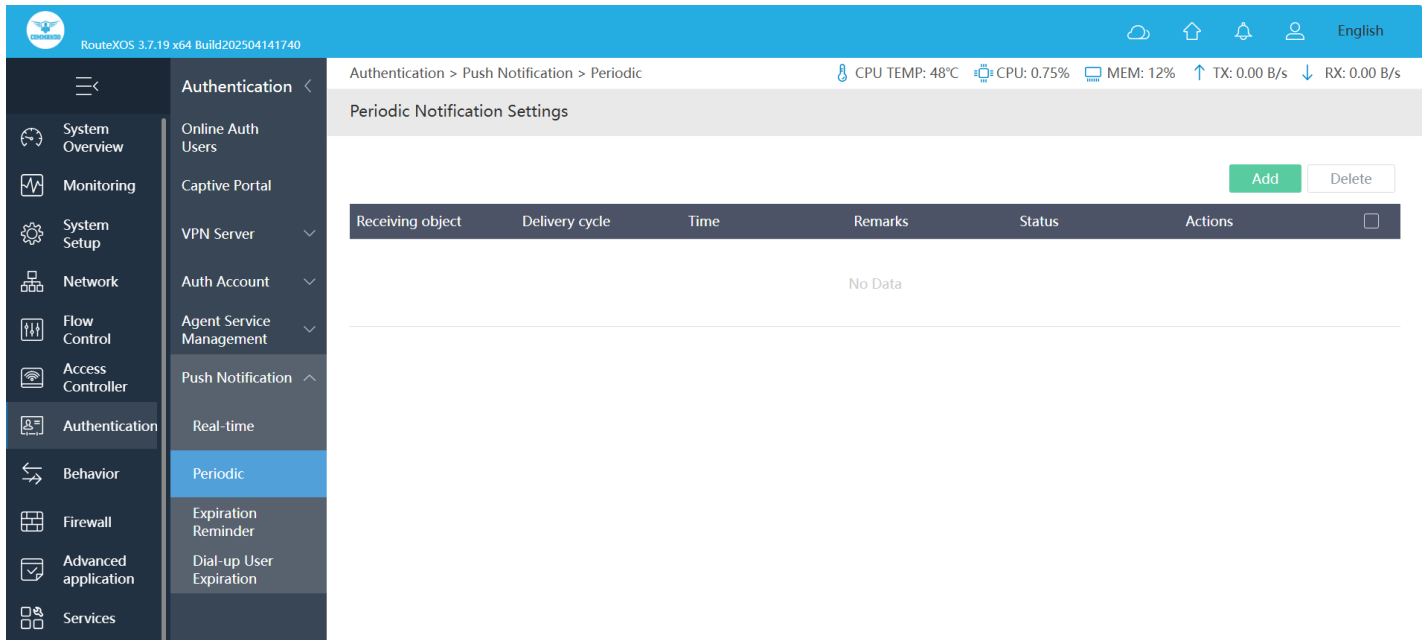


Fig 6.5.3 Default Periodic Notification Settings page

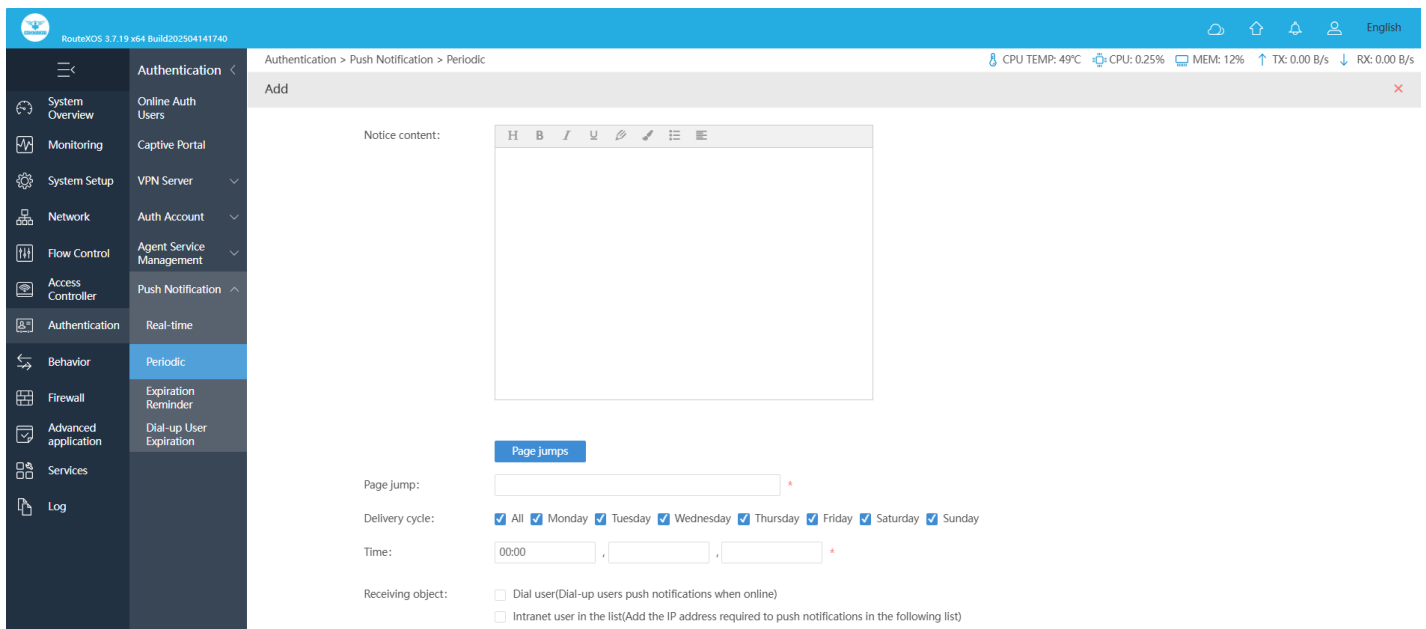


Fig 6.5.4 Add Periodic Notification Settings page

RouteXOS 3.7.19 x64 Build202504141740

English

System Overview
Monitoring
System Setup
Network
Flow Control
Access Controller
Authentication
Behavior
Firewall
Advanced application
Services
Log

Authentication <

Online Auth Users
Captive Portal
VPN Server
Auth Account
Agent Service Management
Push Notification
Real-time
Periodic
Expiration Reminder
Dial-up User Expiration

Authentication > Push Notification > Periodic

CPU TEMP: 49°C
CPU: 0.00%
MEM: 12%
TX: 0.00 B/s
RX: 0.00 B/s

Add

Notice content:

H
B
I
U

Hello User,

You are using COMMANDO Network.

Page jumps

Page jump:

http://www.google.com

Delivery cycle:

☒ All
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday
☒ Sunday

Time:

00:00

Receiving object:

☐ Dial user(Dial-up users push notifications when online)
☐ Intranet user in the list(Add the IP address required to push notifications in the following list)

IP:

Use "-" for IP range

192.168.0.0/24

Add Group
Refresh

COMMANDO
COMMANDOMAC

Join>>
<<Remove

Remarks:

COMMANDO Push Notification

Countdown:

3500

0s means no countdown is enabled; no countdown time is set, or a confirmation button on the notification page is manually clicked during the countdown time, otherwise port 80 will be hijacked all the time. Please use the real-time notification function with caution.

Save

Cancel

Fig 6.5.5 Periodic Notification Settings page

Expiration Reminder Settings: Expiration Reminder allows tracking of expiration dates and renewals for services, contracts, permits etc.

To configure Expiration Reminder Settings, Click on Authentication > Push Notification > Expiration Reminder

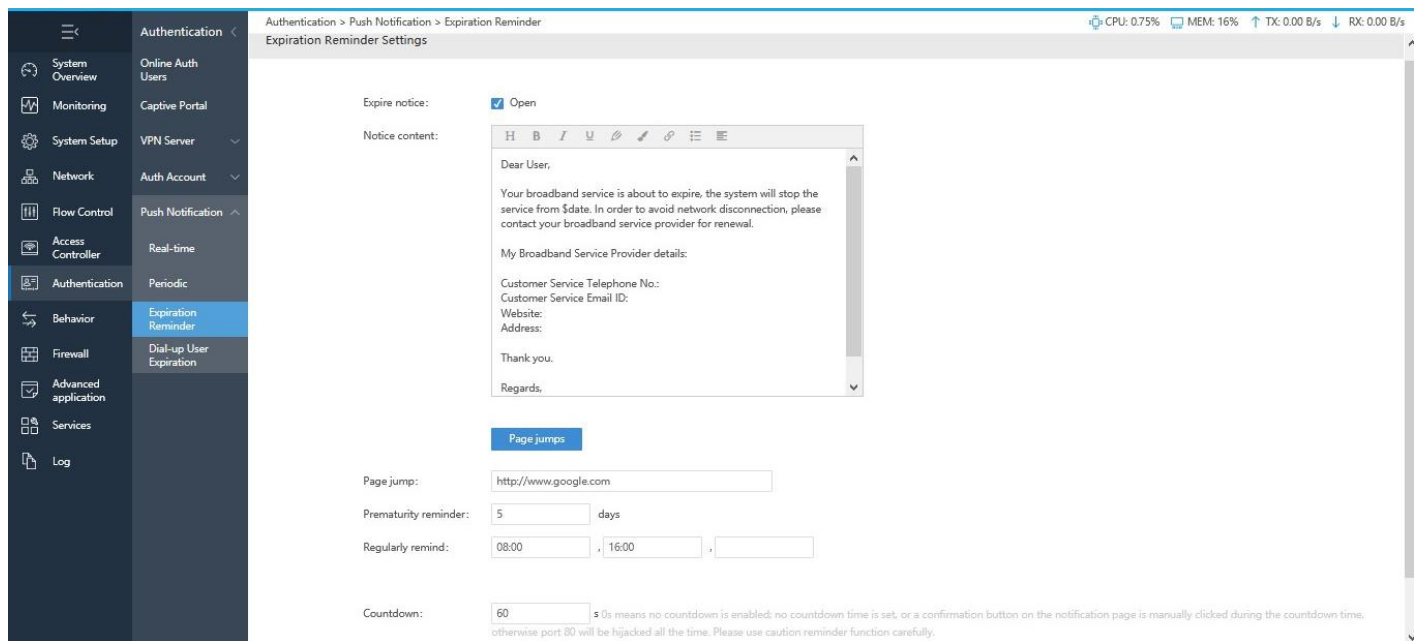


Fig 6.5.6 Default Expiration Reminder Settings page

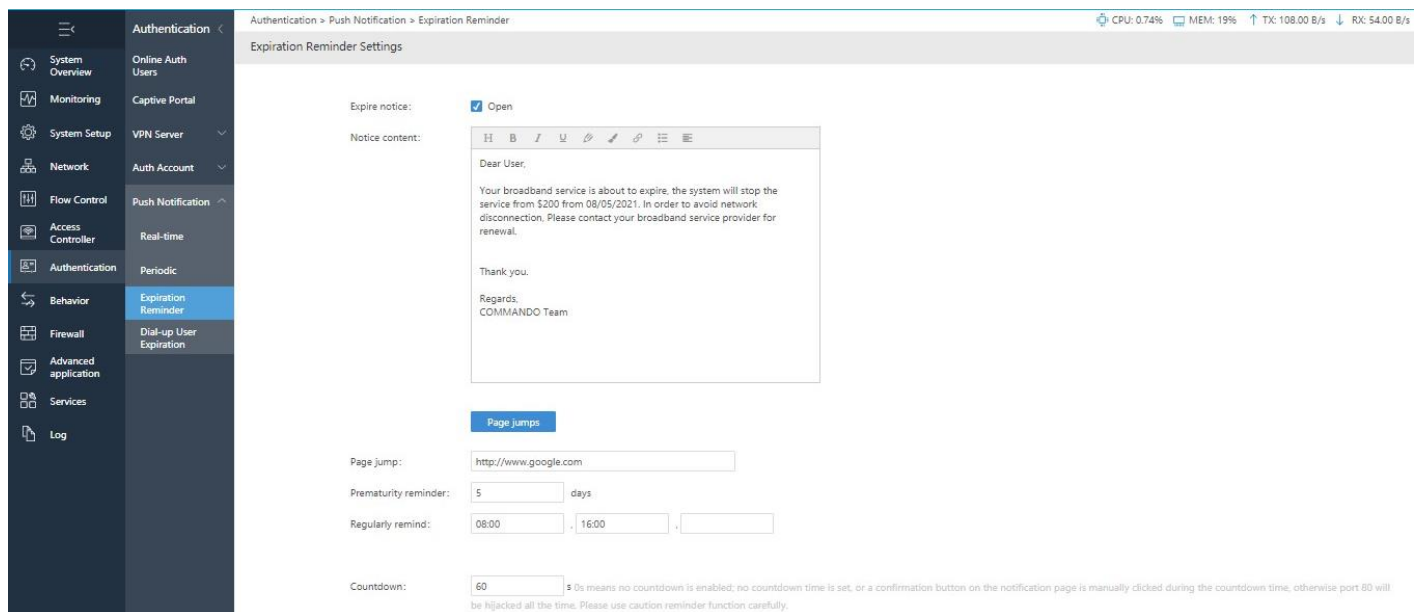


Fig 6.5.7 Expiration Reminder Settings page

Dial-up User Expiration Notification: Dial-up User Expiration Notification to notify expire in a specified number of days.

To configure Dial-up User Expiration Notification Settings, Click on Authentication > Push Notification > Dial-up User Expiration

6.6 Agent Service Management

Agent Service Management provides a centralized interface to manage agent accounts and monitor active online accounts. It enables administrators to create, modify, and delete agent accounts while tracking real-time session details, ensuring secure and efficient account management.

Agent Account Management: Agent Account Management allows administrators to add, edit, or remove agent accounts, assigning roles and access levels as needed for secure authentication and authorization.

To configure Agent Account Management, click on Authentication > Agent Service Management > Agent Account Management.

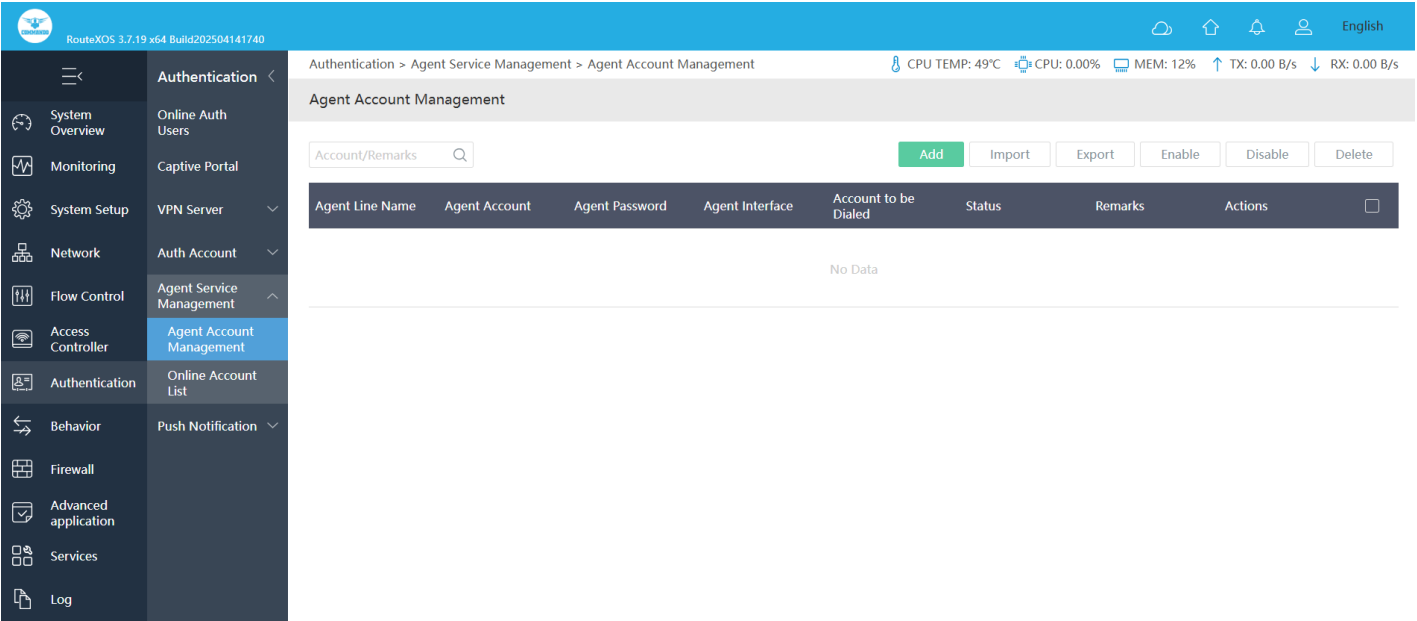


Fig 6.6.1 Default Agent Account Management Settings page

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Agent Service Management > Agent Account Management

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Agent Account:

Agent Password:

Agent Interface:

Account to be Dialed (Username):

Remarks:

Save Cancel

Fig 6.6.2 Add Agent Account Management Settings page

Online Account List: The Online Account List displays real-time information on active agent sessions, including login details, IP addresses, and session durations, allowing for monitoring and security oversight.

To view Online Account List, click on Authentication > Agent Service Management > Online Account List.

RouteXOS 3.7.19 x64 Build202504141740

Authentication > Agent Service Management > Online Account List

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Online Account List

Account/Remarks

Agent Account	IP Address	Netmask	Gateway	Account to be Dialed	Remarks
No Data					

Fig 6.6.3 Default Online Account List Settings page

BEHAVIOUR

Behaviour Audit: Can configure Activate Audit, Record-free setting, Web Browsing, IM, Terminal Online/Offline.

Mark MAC Address: Mark MAC Address to Readable Hostname.

MAC Control: Blacklist Mode to blacklist MAC and does not allow access. Whitelist Mode to whitelist MAC to allowed access.

Website Control: Website control to Blacklist Mode (By default all domain names can be accessed, and domain names in the list cannot be accessed) and Whitelist Mode (The default domain name is not accessible, and the domain name in the list can be accessed).

URL Control: For configuration of URL Jump, Keyword Replace, Parameter Replace.

Application Protocol Control: An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application protocol Control the processing of applications.

Secondary Routing: Using secondary IP addresses on the Gateways or access servers allows you to have two logical subnets using one physical subnet. To create a single network from subnets that are physically separated by another network by using a secondary address first network is extended or layered on top of the second network which can be routed separately. Note If any Gateway on a network segment uses a secondary address, all other Gateways on that same segment must also use a secondary address from the same network or subnet.

QQ Blacklist/Whitelist: Black mode (All QQ can be logged in by default. QQ is not allowed to login in the blacklist) and White mode (All QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed).

7.1 Behavior Audit with Mark MAC Address

A behavior audit is carefully designed to obtain insight into website browsing history, IM online record, Client's upper and lower-line records.

To enable Behavior Audit Settings, click on Behavior > Behavior Audit > Activate Audit

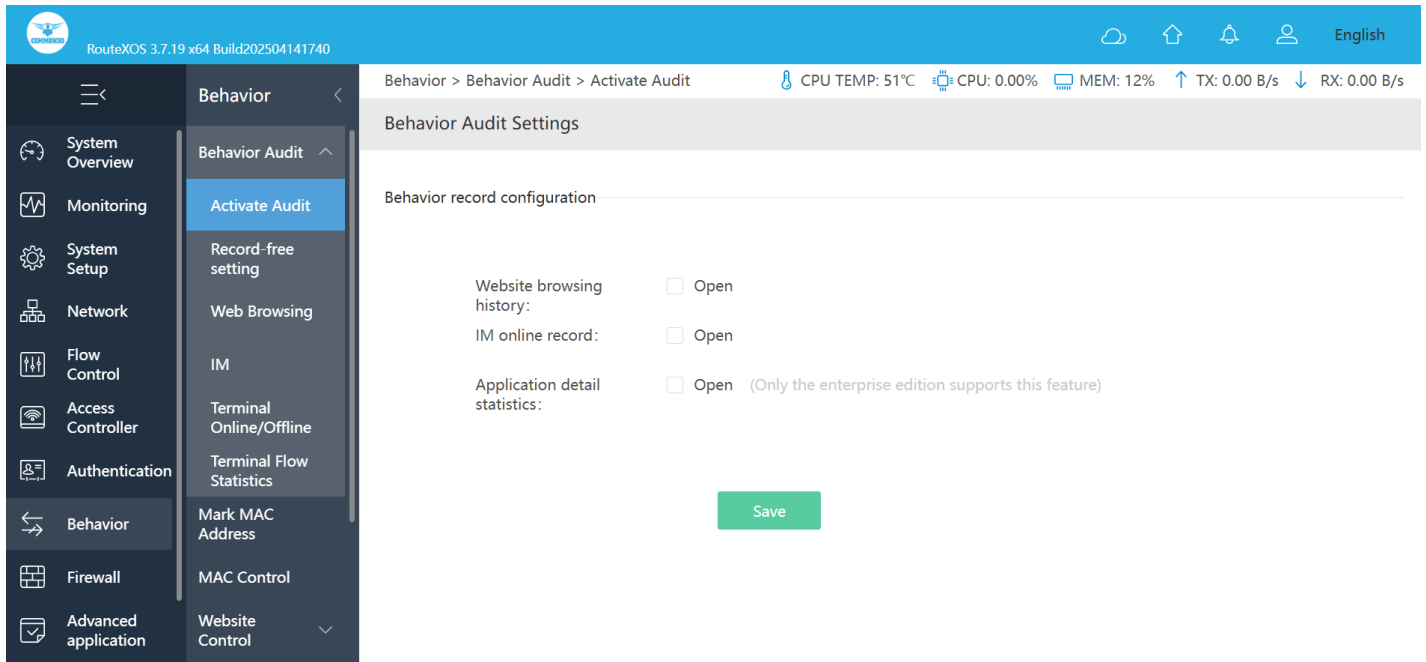


Fig 7.1.1 Default Behavior Audit Settings page

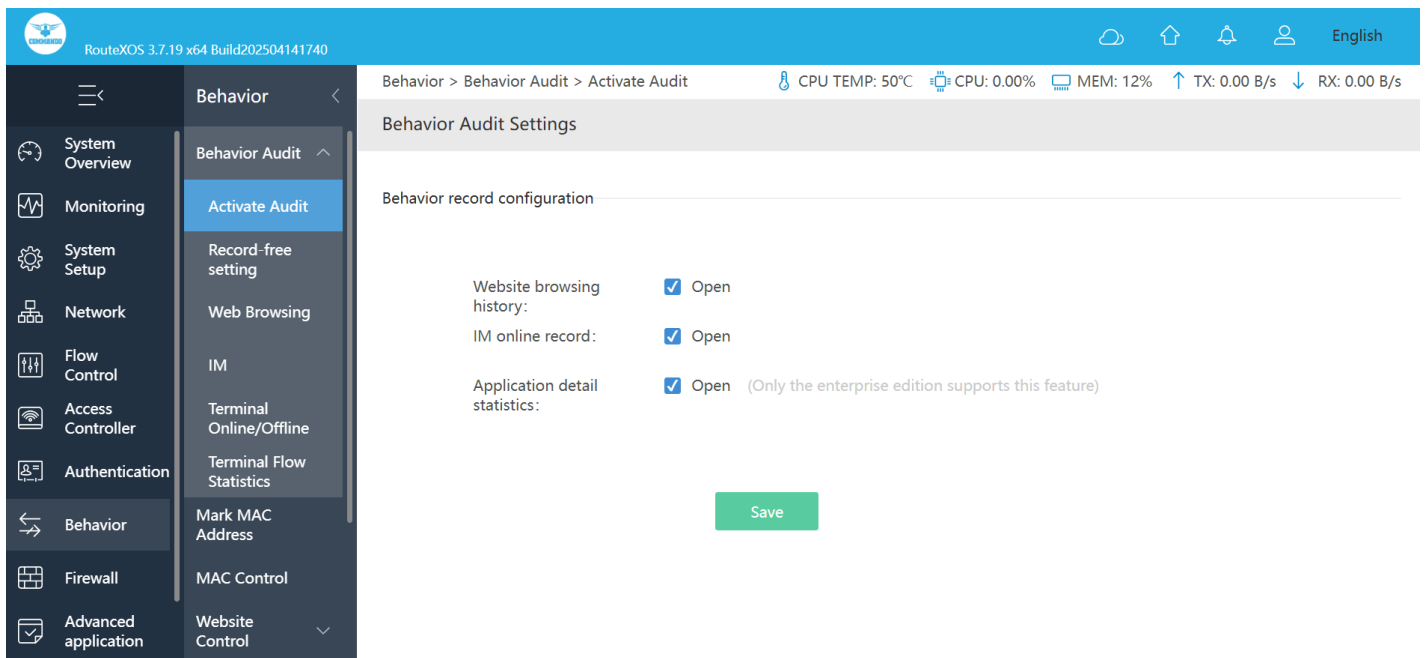


Fig 7.1.2 Enable Behavior Audit Settings page

Record-free setting: A whitelist is only giving administrator-approved programs, and IP and email addresses, system access whatever is not on the list is blocked. The Administrators tailor-make whitelists based on their unique wants and needs. The goal of whitelisting is to protect computers and networks from potentially harmful applications. In general, a whitelist is an index of approved entities. Whitelisting works best in audits with Record-free setting, where systems are subject to a consistent workload.

To enable Record-free setting, Click on Behavior > Behavior Audit > Record-free setting

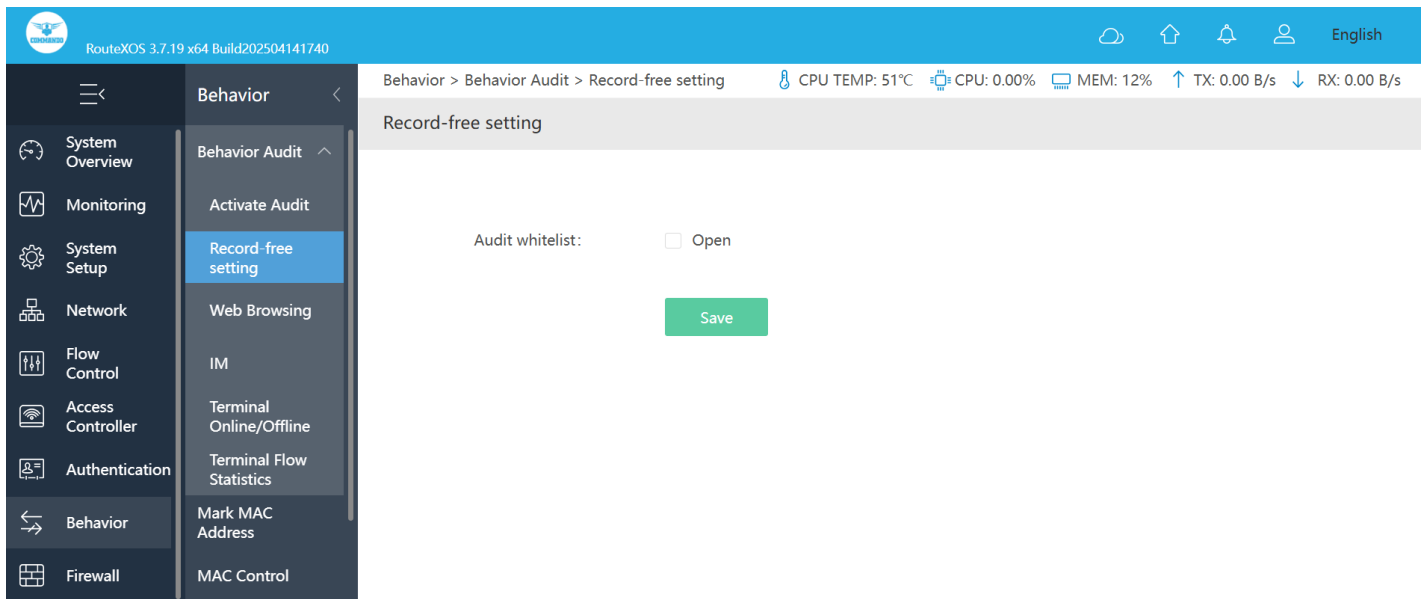


Fig 7.1.3 Default Record-free setting page

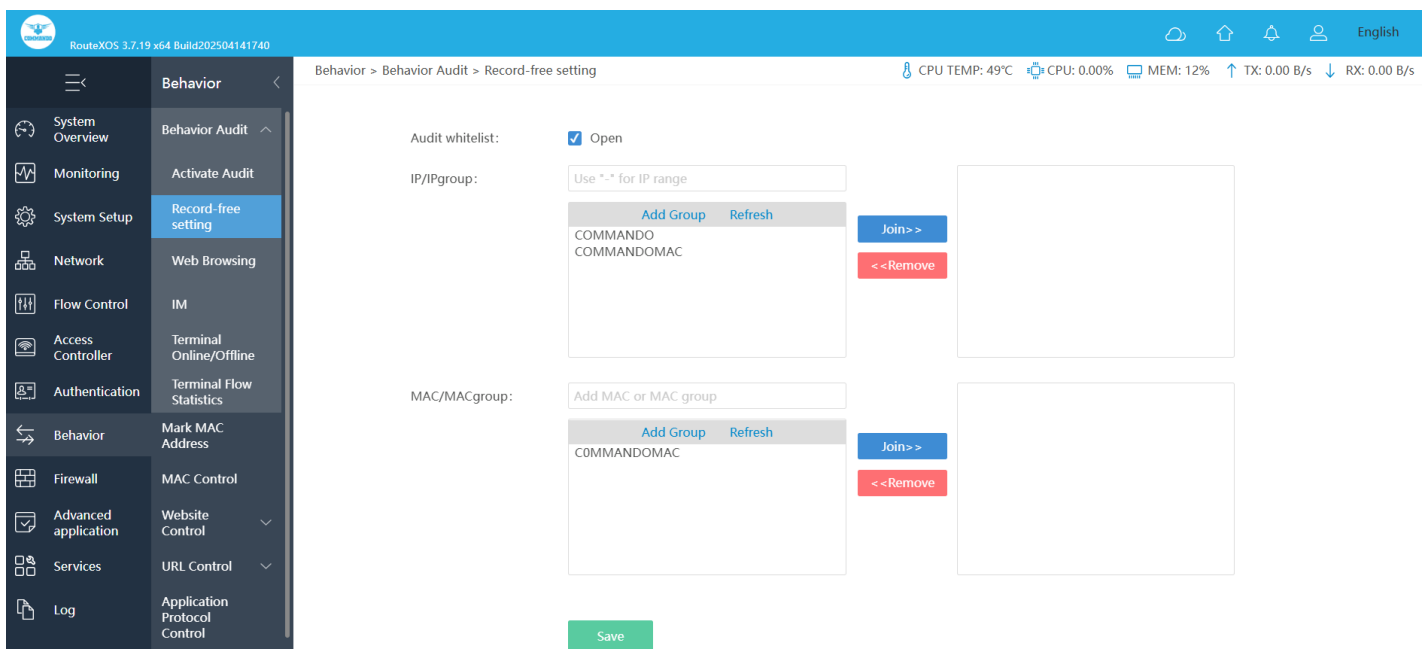


Fig 7.1.4 Enabling Record-free setting page

Viewing Web Browsing History: Web browsing history refers to the list of web pages all users have visited, as well as associated data such as page title and time of visit. It is usually stored locally by R100 in order to provide all users history to monitor all previously visited pages.

For Viewing Web Browsing History, Click on Behavior > Behavior Audit > Web Browsing

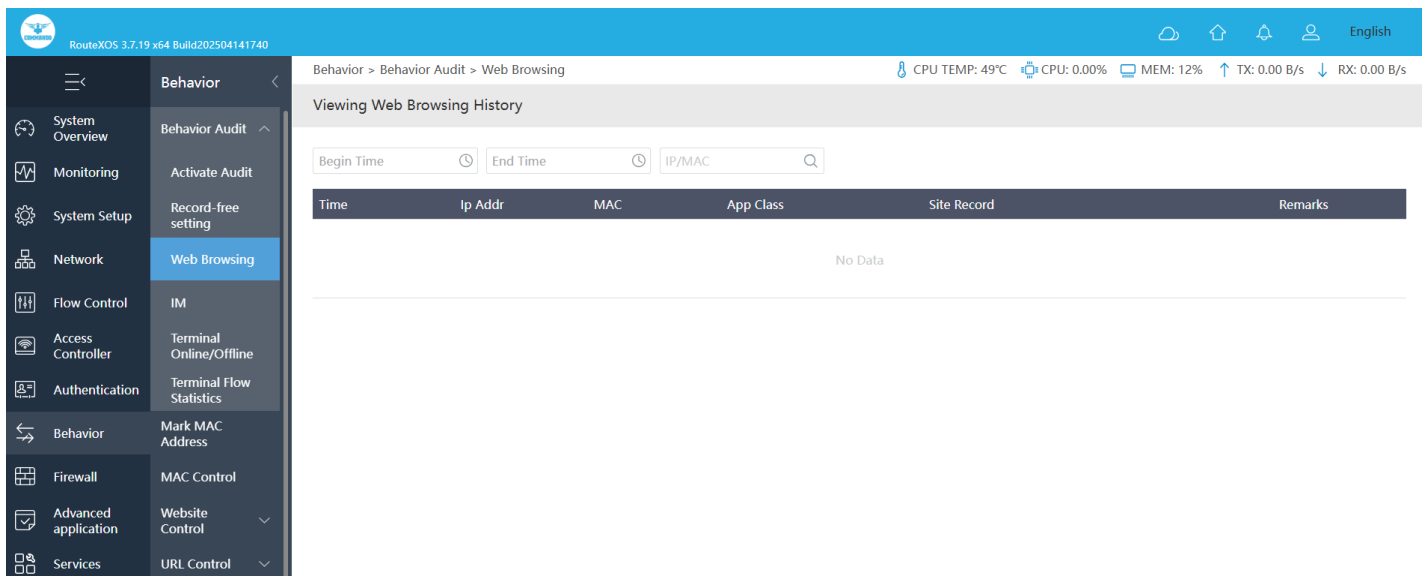


Fig 7.1.5 Default Viewing Web Browsing History page

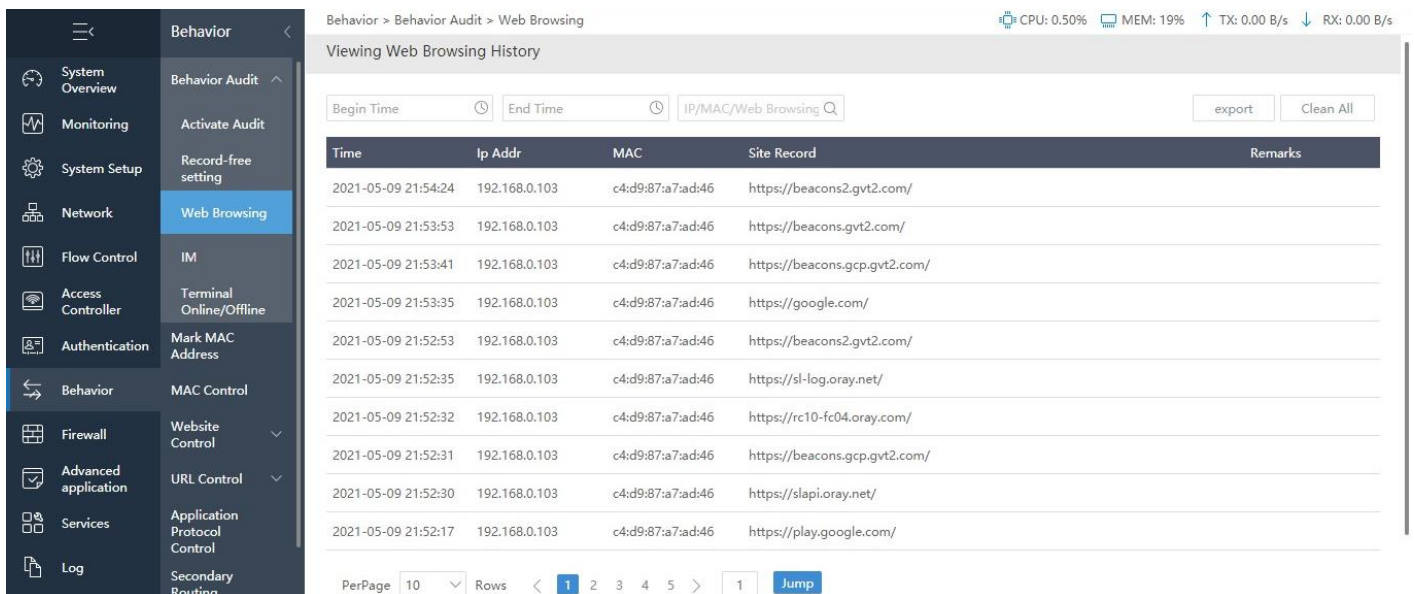


Fig 7.1.6 Viewing Web Browsing History page

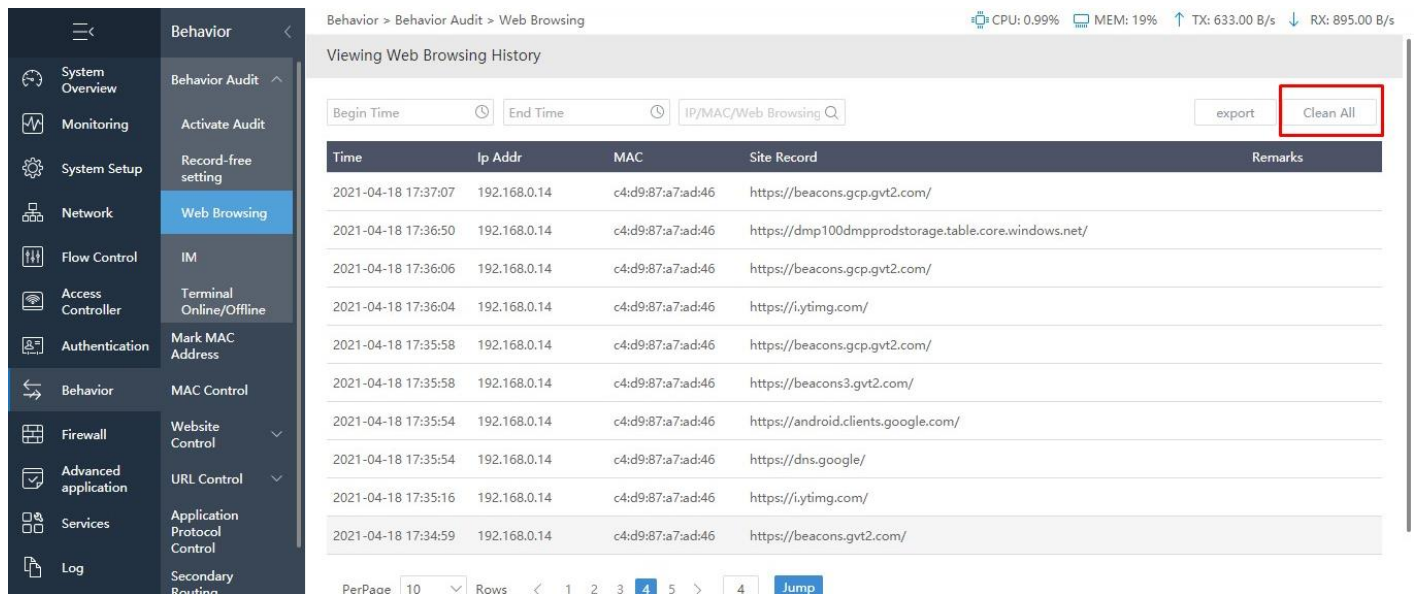


Fig 7.1.7 Cleaning all Web Browsing History page

Viewing IM History: Instant messaging (IM) technology is a type of online chat that offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted between two parties, when each user chooses to complete a thought and select "send". Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, or video chat.

For Viewing IM History, Click on Behavior > Behavior Audit > IM

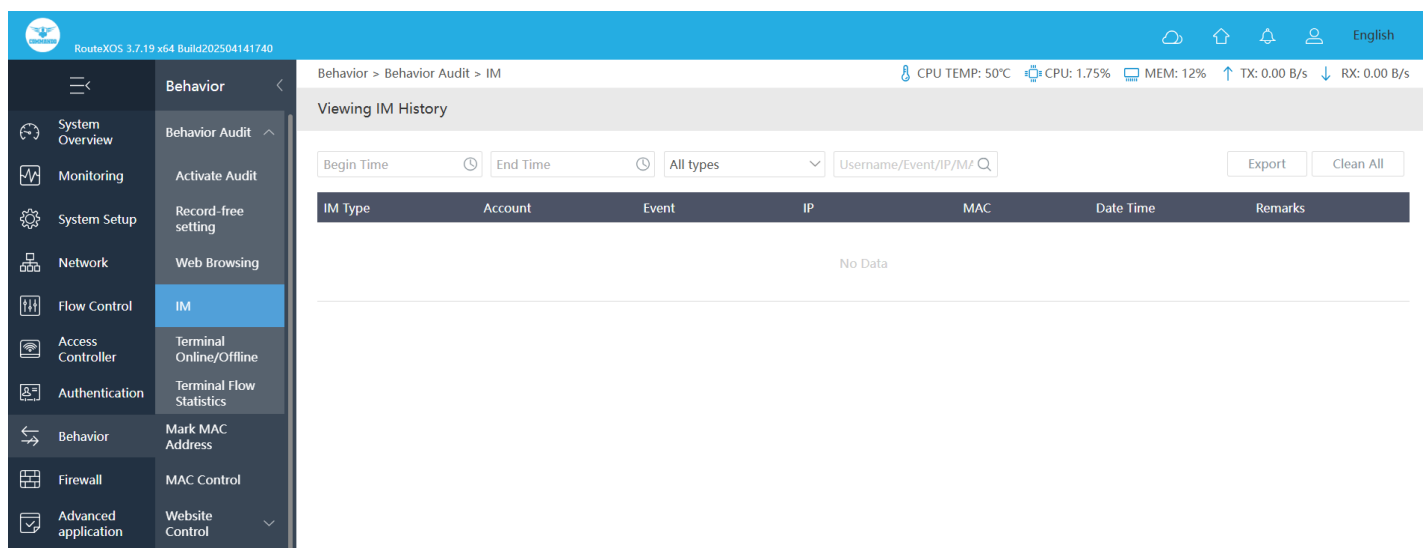


Fig 7.1.8 Viewing IM History page

Terminal Online/Offline History: For Viewing Terminal Online/Offline History, Click on Behavior > Behavior Audit > Terminal Online/Offline

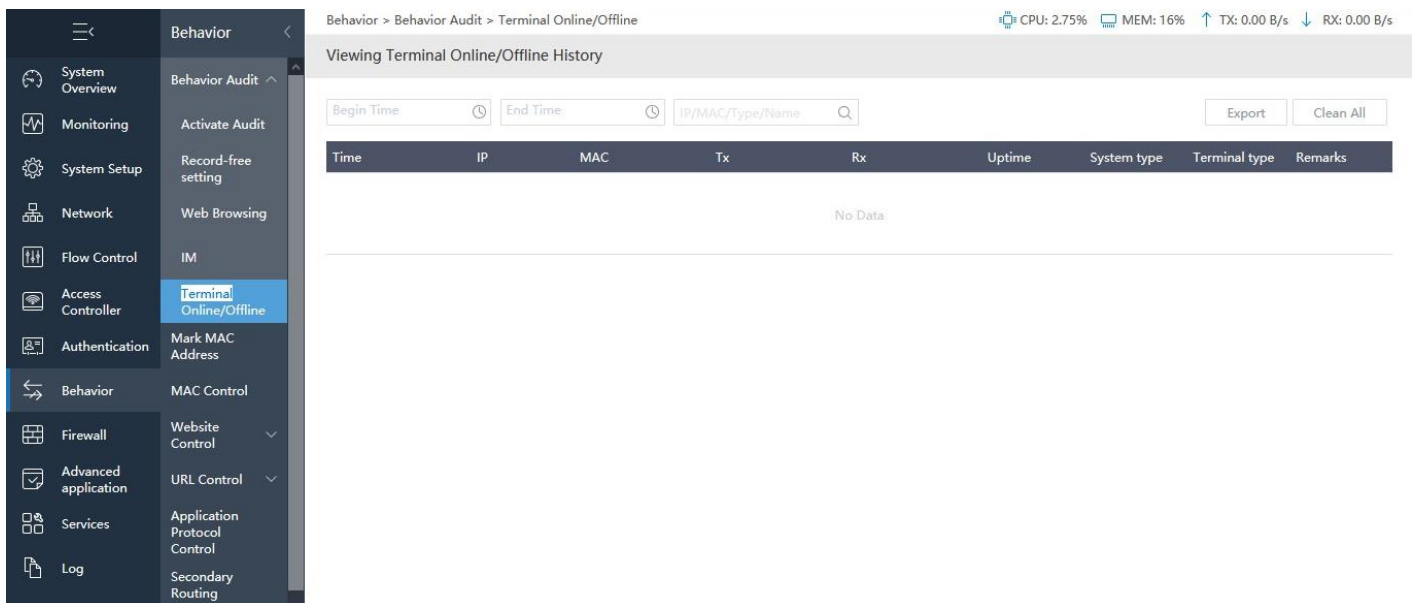


Fig 7.1.9 Default Viewing Terminal Online/Offline History page

RouteXOS 3.7.19 x64 Build202504141740

Behavior > Behavior Audit > Terminal Online/Offline

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Viewing Terminal Online/Offline History

Begin Time End Time IP/MAC/Terminal type/Rer Export Clean All

Time	IP	MAC	Tx	Rx	Uptime	System type	Terminal type	Remarks
2025-08-01 14:50:52	192.168.0.10	a0:8c:fd:a5:68:9d	88.77 KB	43.59 KB	2h 55m 8s	Windows10	HP	
2025-08-01 14:34:45	192.168.0.10	a0:8c:fd:a5:68:9d	35.66 KB	9.05 KB	14m 15s	Windows10	HP	
2025-07-30 12:54:57	192.168.0.12	82:02:fa:60:0e:26	288 B	588 B	8h 3s	Unknown	Unknown	
2025-07-30 12:53:55	192.168.0.10	a0:8c:fd:a5:68:9d	262.5 KB	99.25 KB	8h 1m 5s	Windows10	HP	
2025-07-29 14:42:58	192.168.0.10	a0:8c:fd:a5:68:9d	808.54 KB	119.62 KB	6h 43m 2s	Windows10	HP	
2025-07-29 14:31:54	192.168.0.10	a0:8c:fd:a5:68:9d	532.12 KB	45.75 KB	10m 6s	Windows10	HP	
2025-07-29 14:25:00	192.168.0.10	a0:8c:fd:a5:68:9d	43.76 KB	4.26 KB	3m	Windows10	HP	
2025-07-29 14:20:20	192.168.0.10	a0:8c:fd:a5:68:9d	10.74 KB	1.34 KB	2m 40s	Windows10	HP	
2025-07-29 14:00:50	192.168.0.10	a0:8c:fd:a5:68:9d	829.97 KB	74.5 KB	18m 10s	Windows10	HP	
2025-07-28 19:52:54	192.168.0.10	a0:8c:fd:a5:68:9d	148.06 KB	16.55 KB	1h 43m 6s	Windows10	HP	
2025-07-28 15:04:26	192.168.111.10	a0:8c:fd:a5:68:9d	111.55 KB	55.07 KB	4h 9m 34s	Windows10	HP	
2025-07-28 14:48:10	192.168.111.10	a0:8c:fd:a5:68:9d	24.37 KB	7.03 KB	14m 50s	Windows10	HP	

Fig 7.1.10 Viewing Terminal Online/Offline History page

Terminal Flow Statistics: Terminal Flow Statistics provides real-time and historical data on network traffic for connected terminals. It helps administrators monitor bandwidth usage, analyze traffic patterns, and identify potential network congestion or anomalies for better network management. The statistics can be viewed classified via MAC or via ACCOUNT.

For Viewing Terminal Online/Offline History, Click on Behavior > Behavior Audit > Terminal Flow Statistics

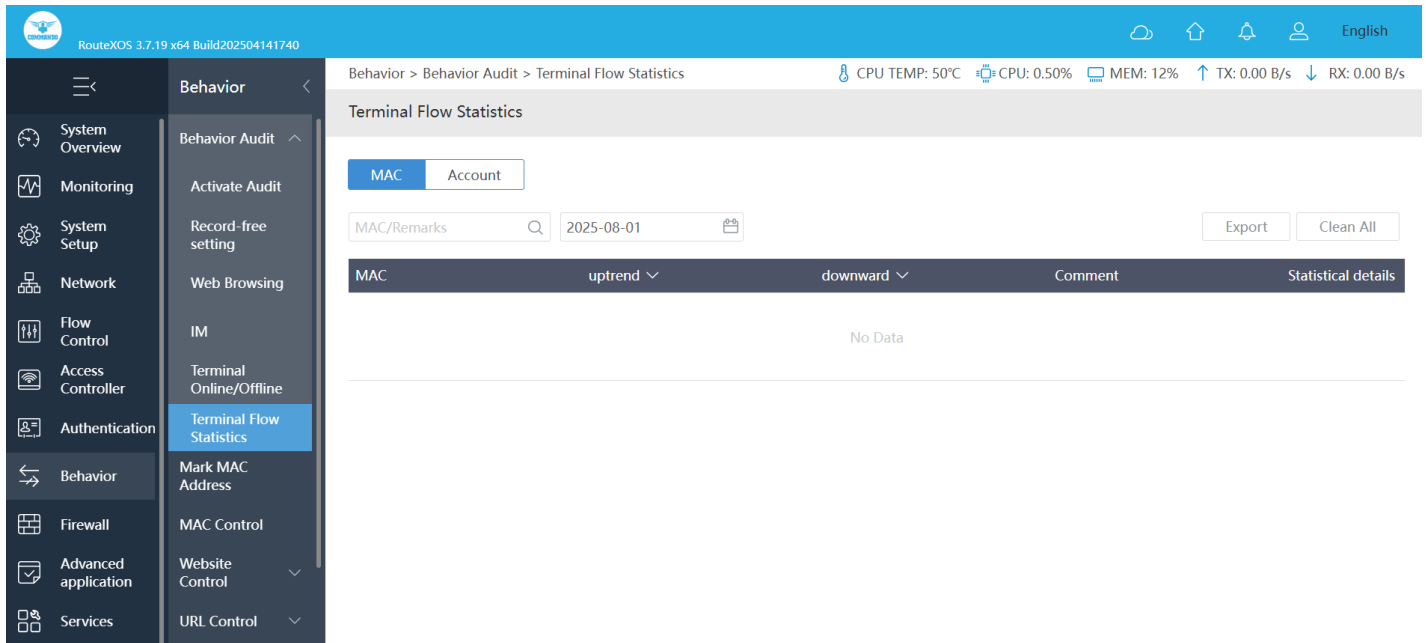


Fig 7.1.11 Viewing Terminal Flow Statistics page

7.2 Mark MAC Address

The MAC address is the physical address of a network interface can be marked to local hostname so to identify mac easily by human understandable names.

For assigning Mark MAC Address to Readable Hostname, Click on Behavior > Mark MAC Address

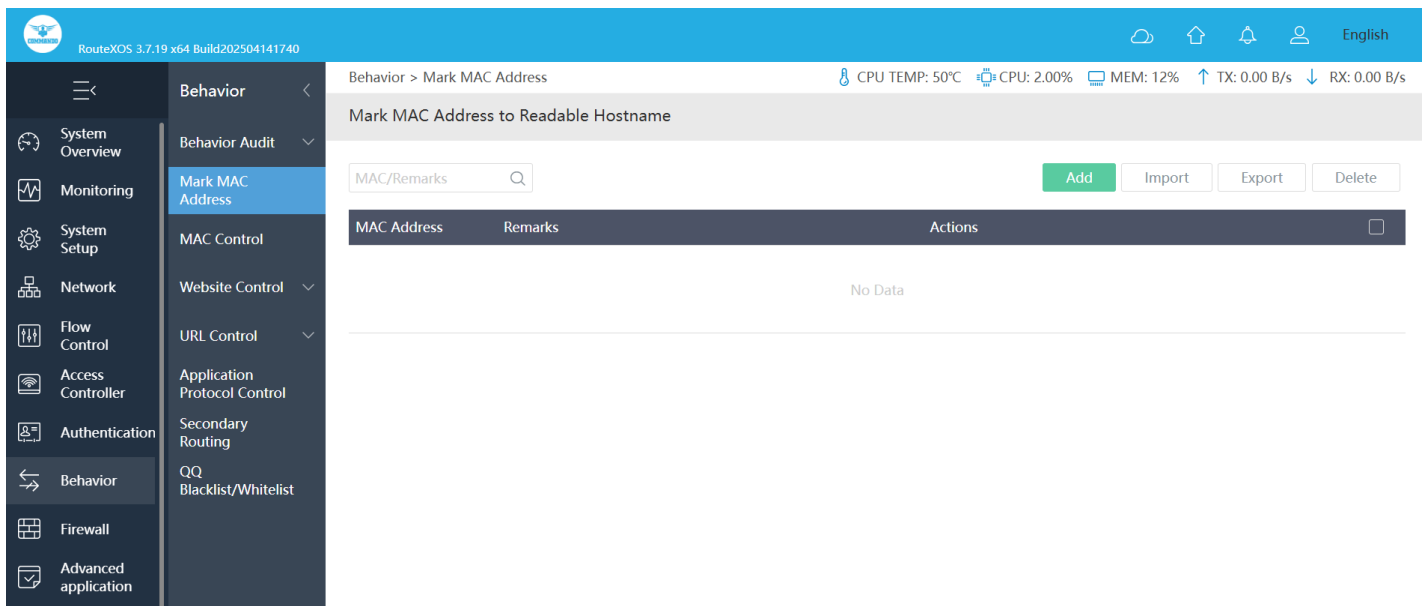


Fig 7.2.1 Default Mark MAC Address to Readable Hostname page

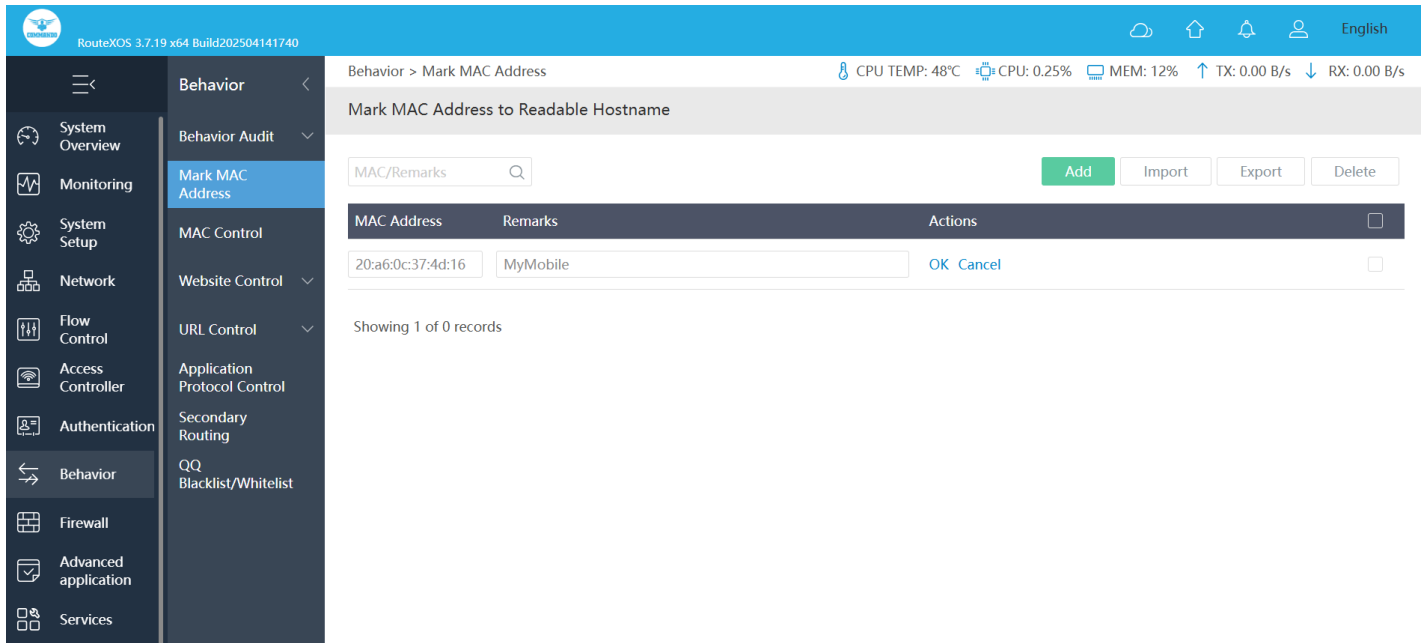


Fig 7.2.2 Adding Mark MAC Address to Readable Hostname page

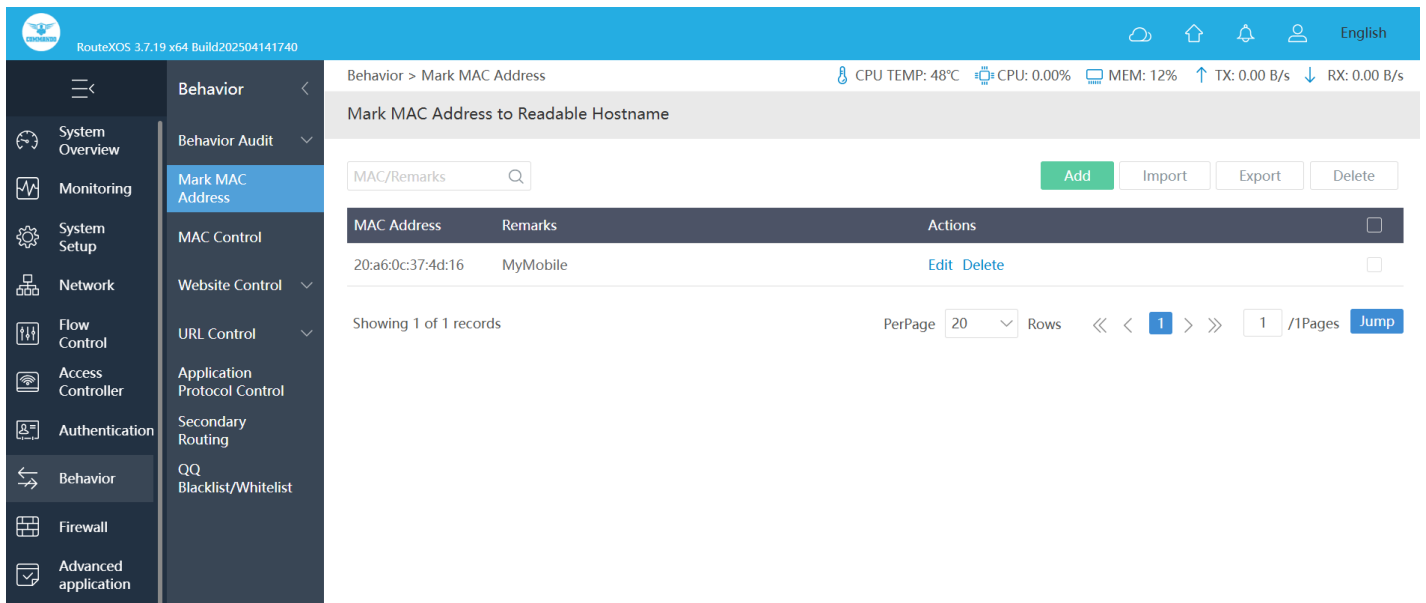


Fig 7.2.3 Mark MAC Address to Readable Hostname page

7.3 MAC Control

In Blacklist Mode, all MACs are allowed to access the network, and the MAC in the blacklist does not allow access. In Whitelist Mode all MACs are not allowed to access the network by default, only MACs in the whitelist are allowed to access the network.

To configure Blacklist or Whitelist MAC Address, Click on Behavior > MAC Control

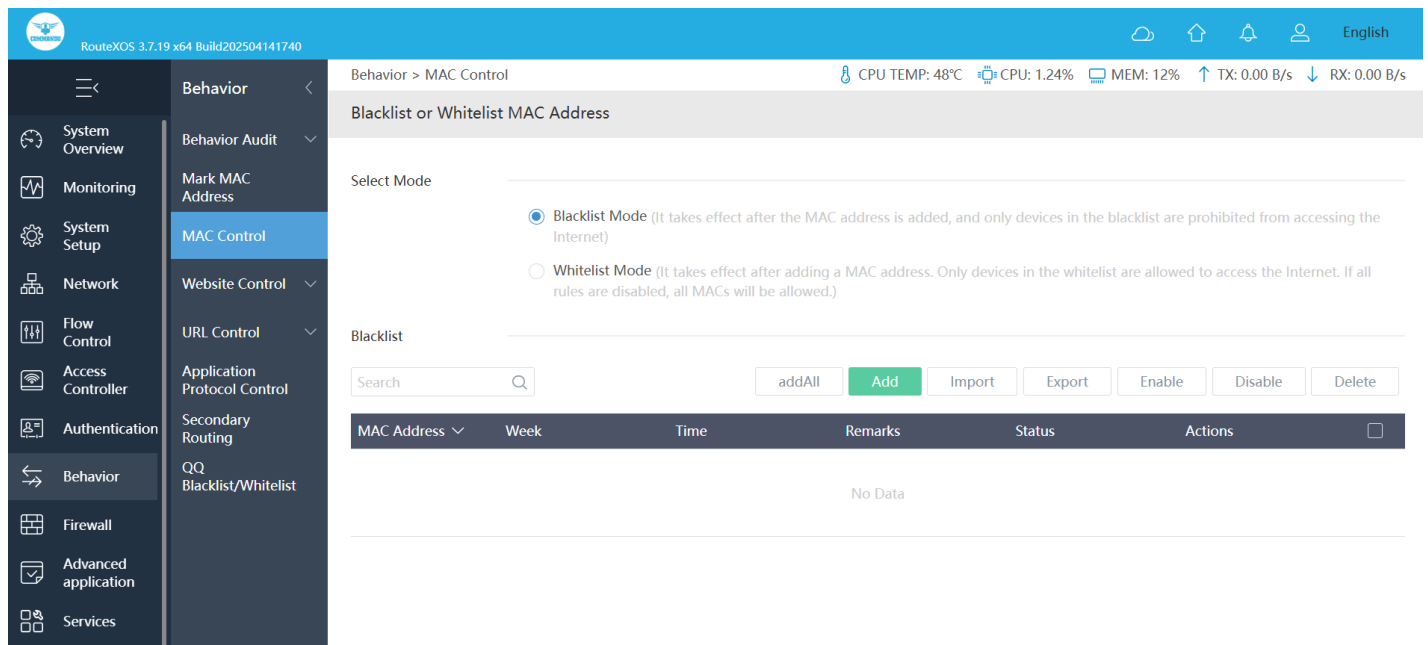


Fig 7.3.1 Default Blacklist or Whitelist MAC Address page

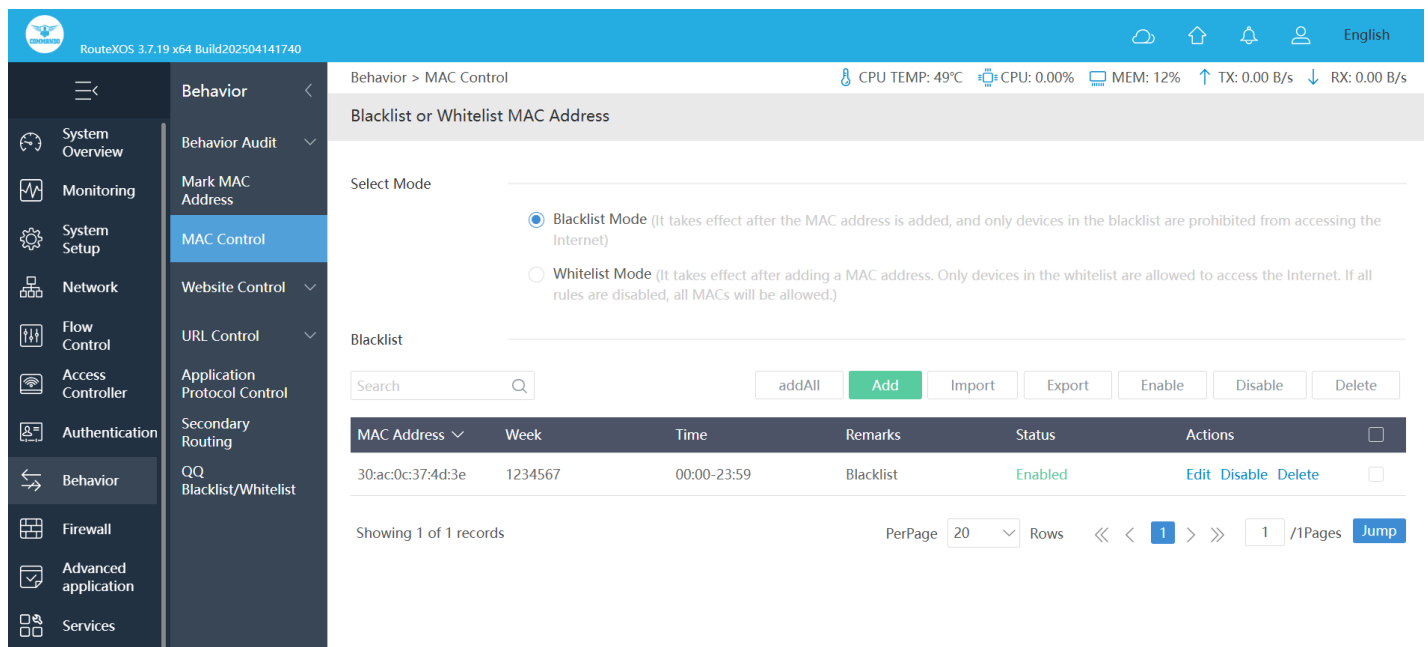


Fig 7.3.2 Blacklist MAC Address page

7.4 Website Control

You can block and allow URLs so that users can only visit certain websites. Restricting users' internet access can increase productivity and protect your organization from viruses and malicious content found on some websites. Allow access to all URLs except the ones you block. Use the blacklist to prevent users from visiting certain websites, while allowing them access to the rest of the web. Block access to all URLs except the

ones you allow ie. Whitelisting. Use the Whitelist to block access to all URLs. Then, use the allow list to allow access to a limited list of URLs.

To configure Blacklist/Whitelist Website, Click on Behavior > Website Control > Blacklist/Whitelist

This page can also allow or deny access to external links in the whitelist list (HTTP only)

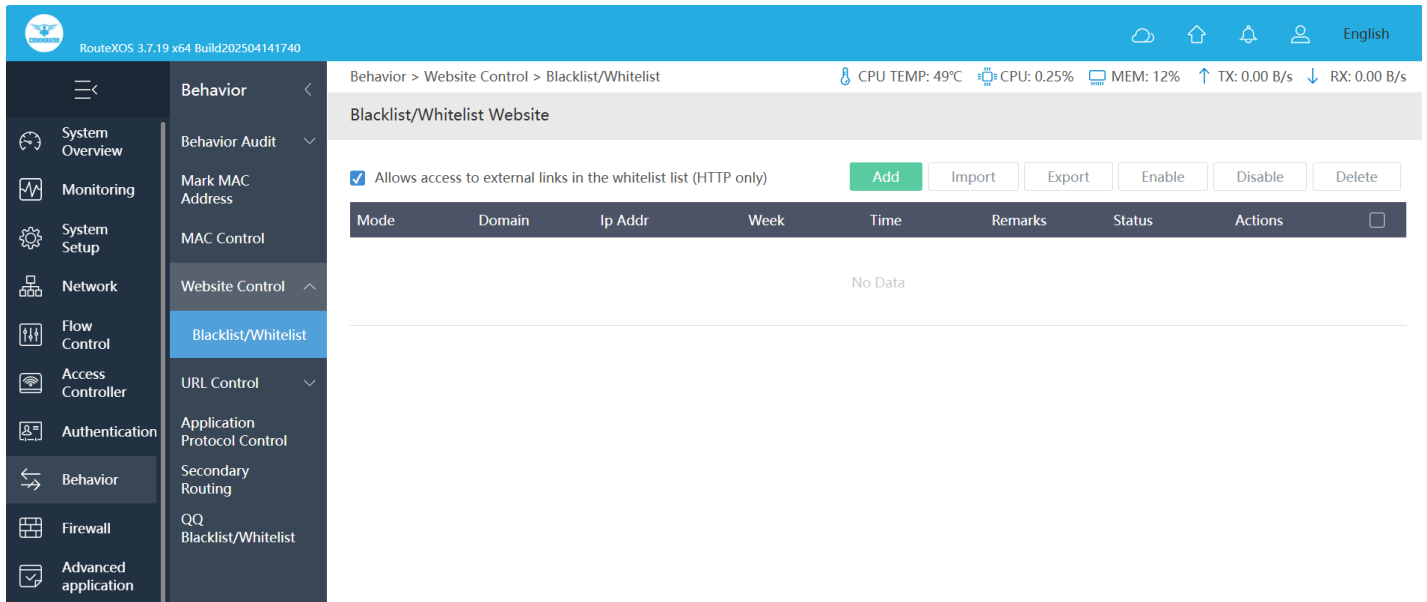


Fig 7.4.1 Default Blacklist/Whitelist Website page

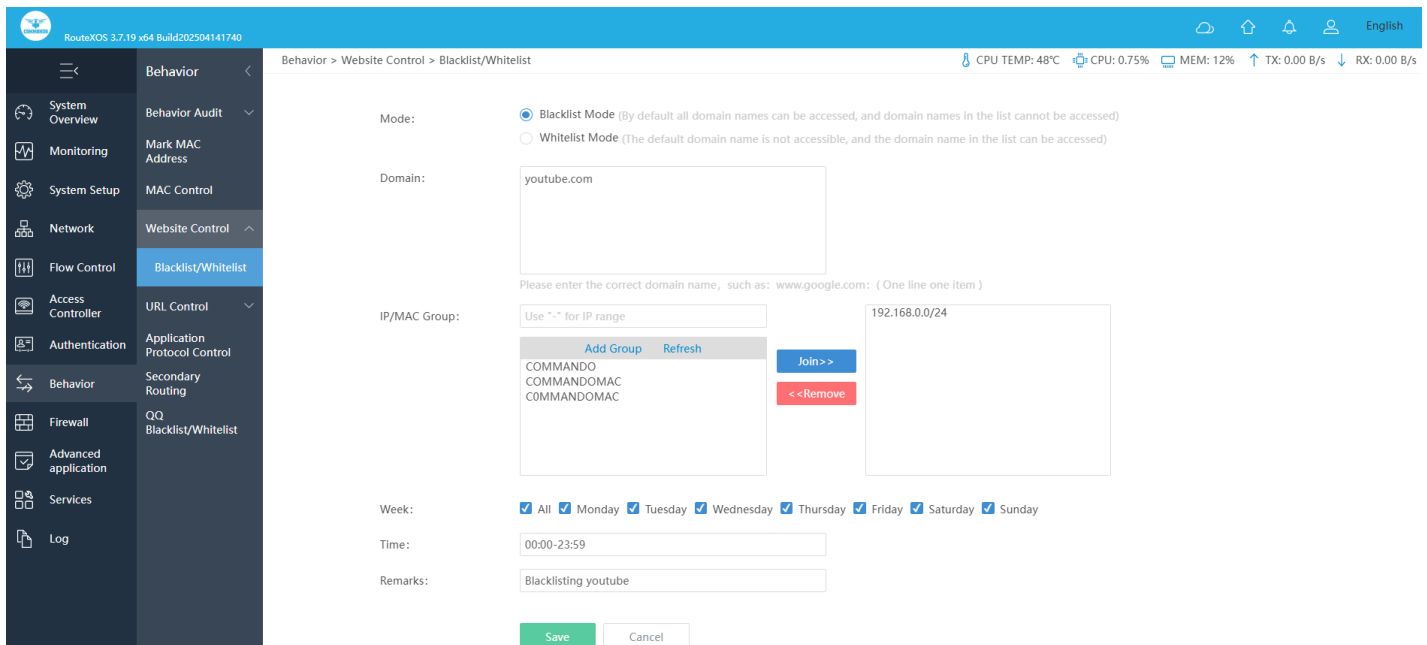


Fig 7.4.2 Blacklist particular Website page

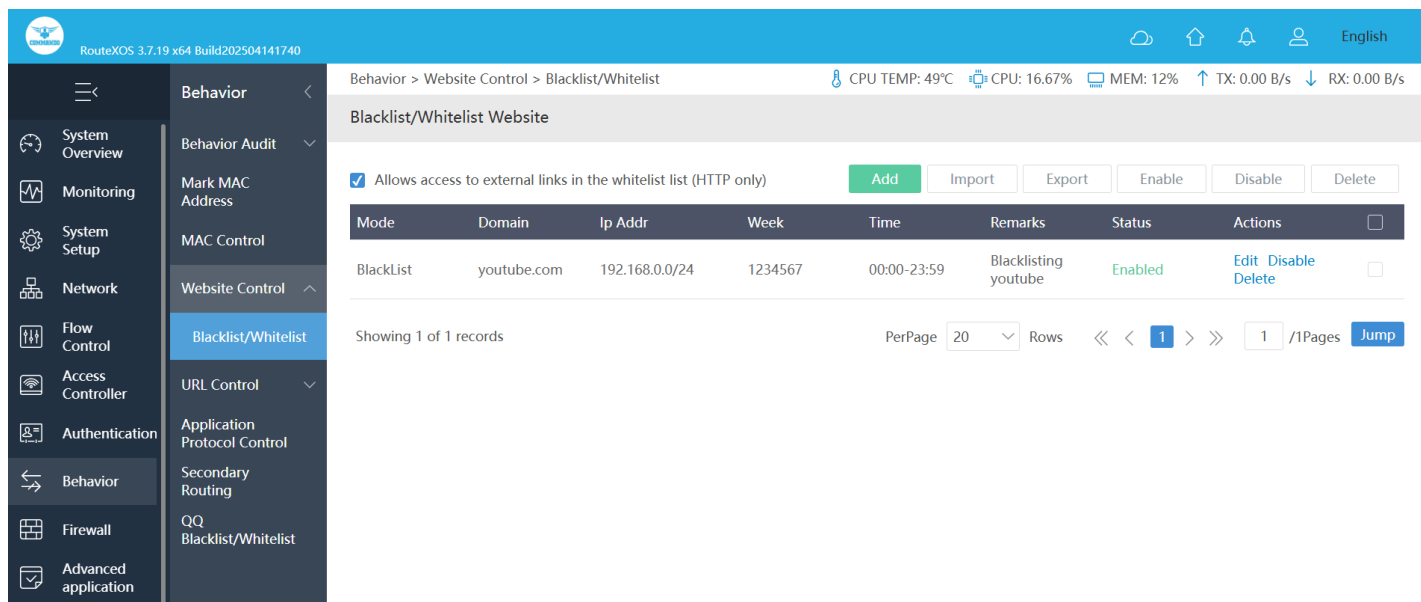


Fig 7.4.3 Blacklist Website page

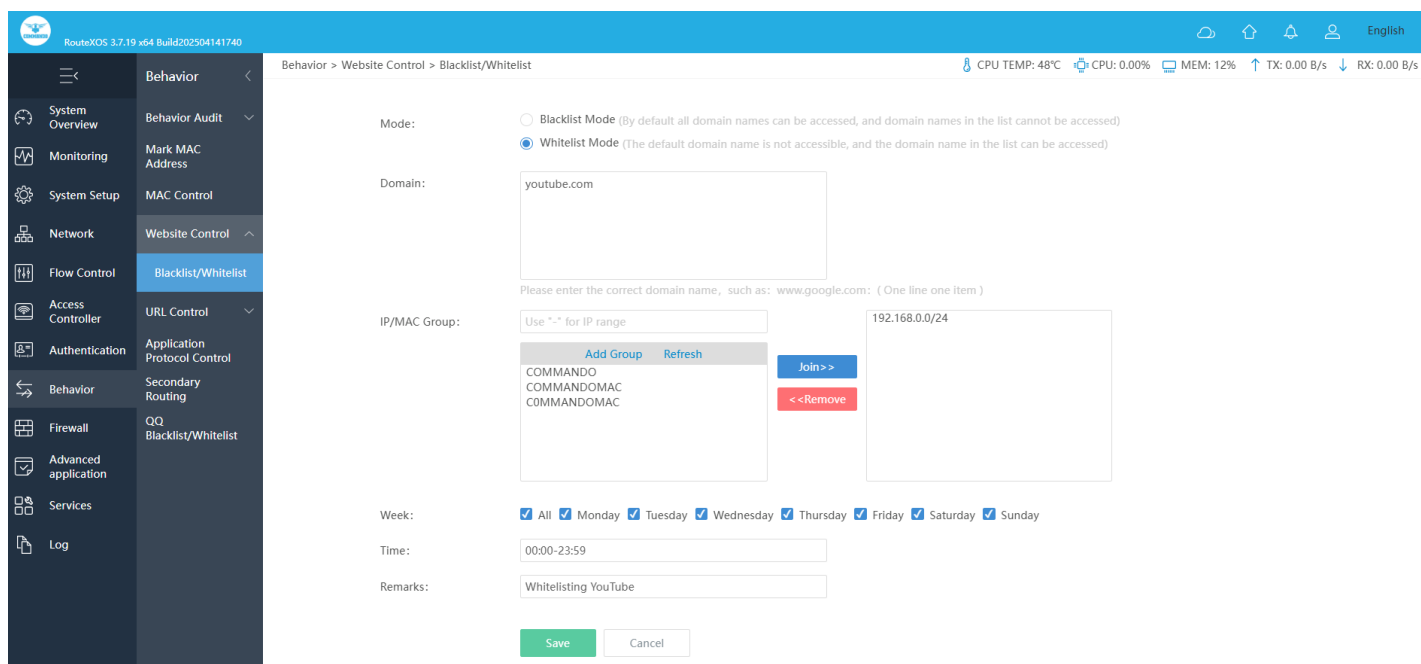


Fig 7.4.4 Whitelisting particular Website page

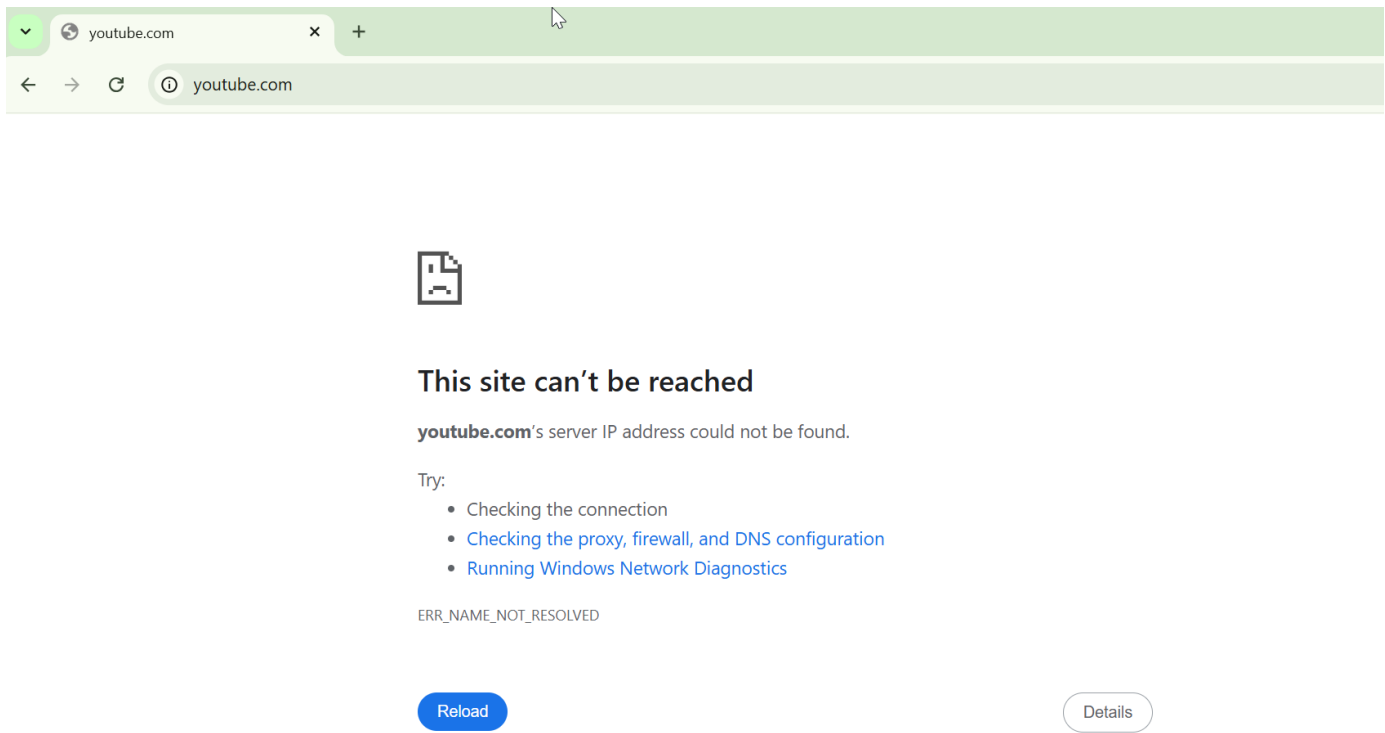


Fig 7.4.5 Result of Blacklisting particular Website page

7.5 URL Control

Organizations can create policies such as permanently allowing or blocking access to specific sites or groups of websites, such as social networking pages to either redirect, filter or blocked. URL filtering is a type of web filtering and is used to restrict web content in order to restrict what content their employees can access over company networks. URL blocking refers process of allowing or denying the access to a certain websites or certain URL addresses for the web users either temporarily or permanently. If a URL is blocked, then the user will not be able to view the URL address or its web content.

URL Redirect Settings:

URL redirection, also called URL forwarding is a technique which is used to redirect your domain's visitors to a different URL. You can forward your domain name to any website, webpage, etc. which is available online. Principle. In HTTP, redirection is triggered by a server sending a special redirect response to a request. Redirect responses have status codes and a Location header holding the URL to redirect to. When browsers receive a redirect, they immediately load the new URL provided in the Location header.

To configure URL Redirect Settings, Click on Behavior > URL Control > URL Jump

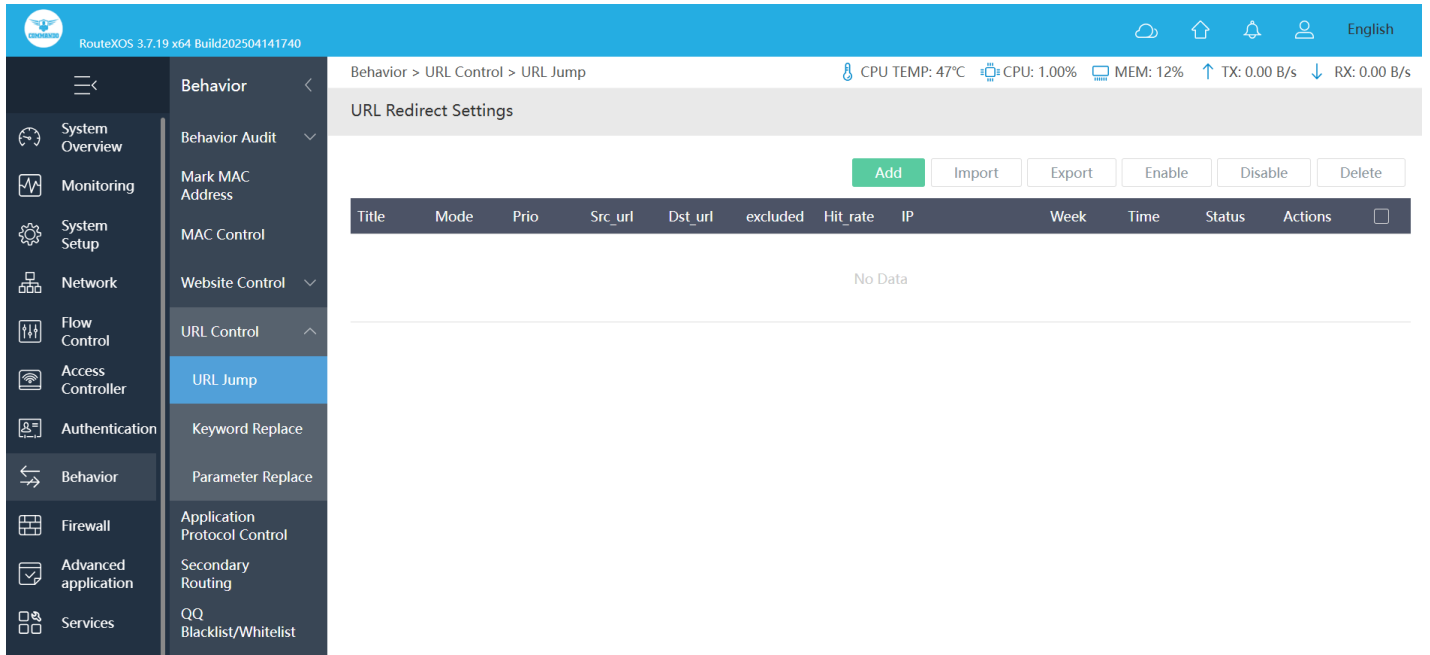


Fig 7.5.1 Default URL Redirect Settings page

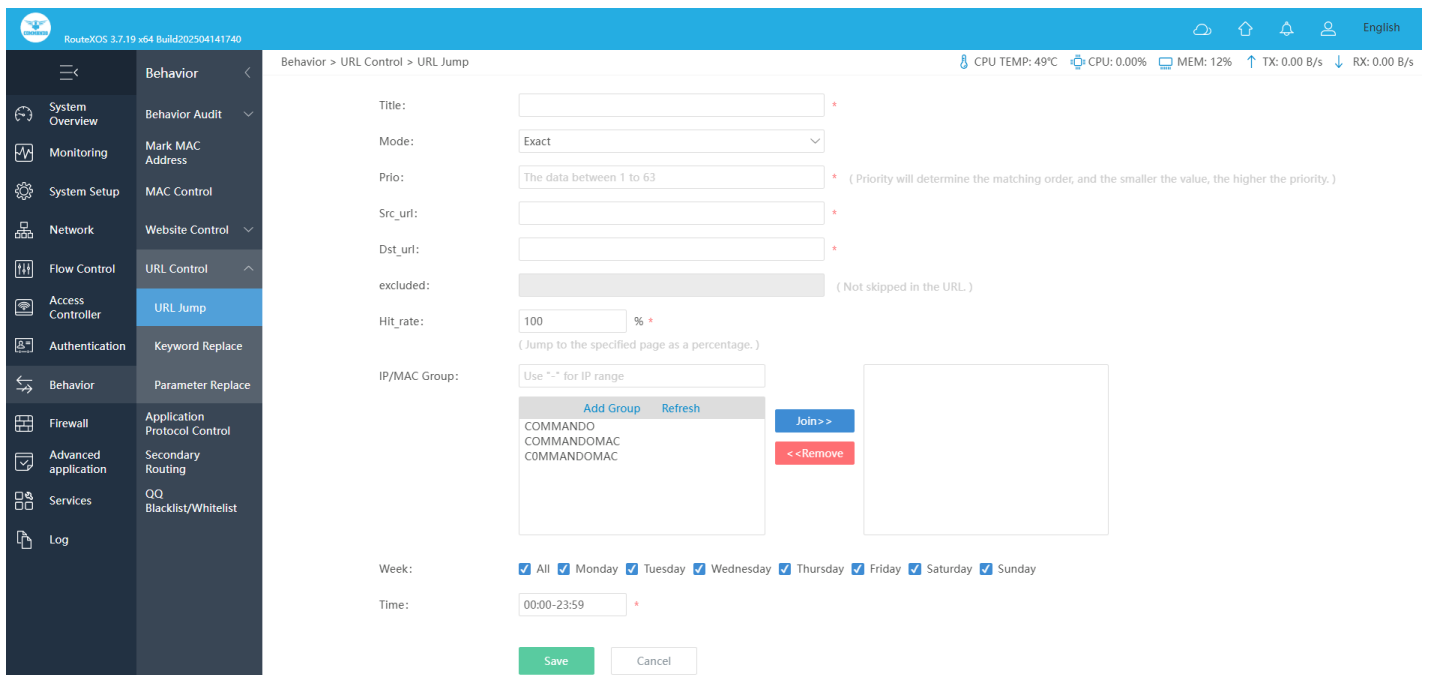


Fig 7.5.2 Add URL Redirect Settings page

RouteXOS 3.7.19 x64 Build202504141740

Behavior > URL Control > URL Jump

CPU TEMP: 49°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Title: COMMANDO *

Mode: Exact

Prio: 2 *

(Priority will determine the matching order, and the smaller the value, the higher the priority.)

Src_url: www.cmdnw.com *

Dst_url: www.commandonetworks.com *

excluded: (Not skipped in the URL.)

Hit_rate: 100 % *

(Jump to the specified page as a percentage.)

IP/MAC Group: Use "-" for IP range 192.168.0.0/24

Fig 7.5.3 Add particular URL Redirect Settings page

RouteXOS 3.7.19 x64 Build202504141740

Behavior > URL Control > URL Jump

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

URL Redirect Settings

Add Import Export Enable Disable Delete

Title	Mode	Prio	Src_url	Dst_url	excluded	Hit_rate	IP	Week	Time	Status	Actions	
COMMANDO	Exact	2	www.cmdnw.com	www.commandonetworks.com		100	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete	

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 7.5.4 URL Redirect Settings page

URL Keywords Replacement Settings: You can replace URL for a selected group of keywords with a single new URL or Search and replace all or part of the URLs for a group of keywords or Append to the end of the URL for a group of keywords.

To configure URL Keywords

Replacement Settings, Click on Behavior > URL Control > Keyword Replace

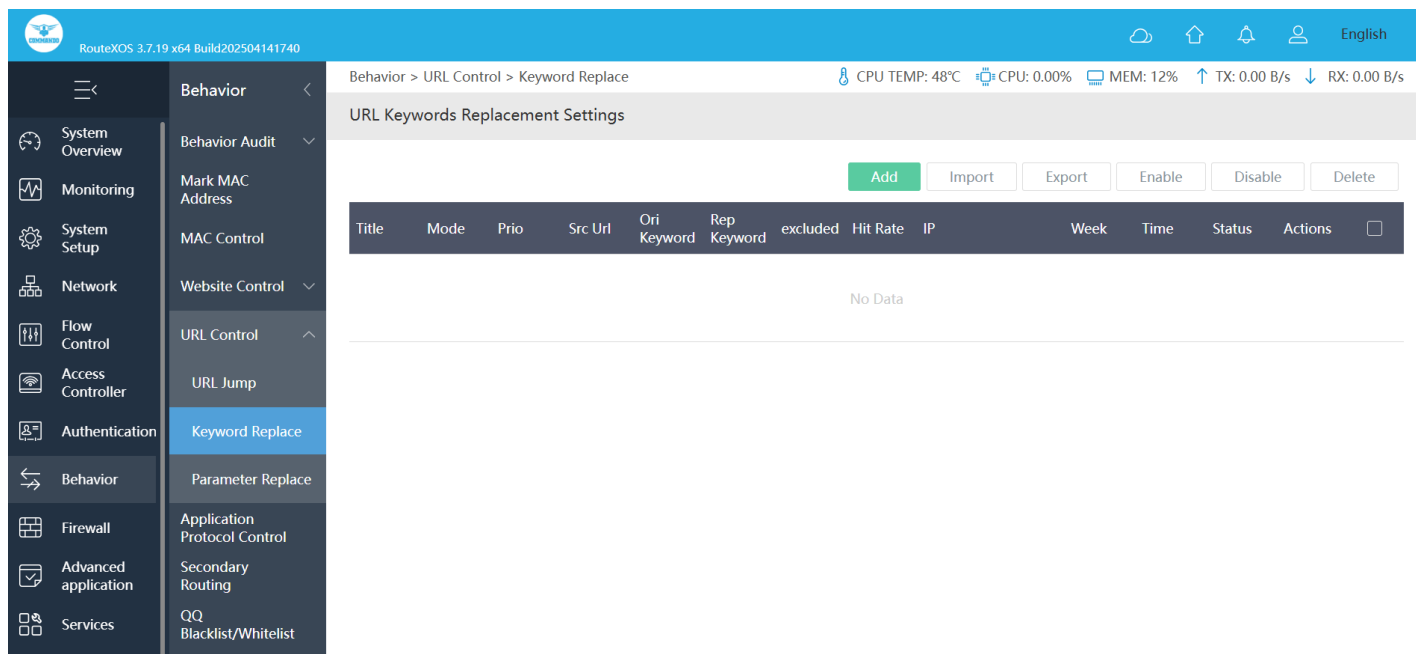


Fig 7.5.5 Default URL Keywords Replacement Settings page

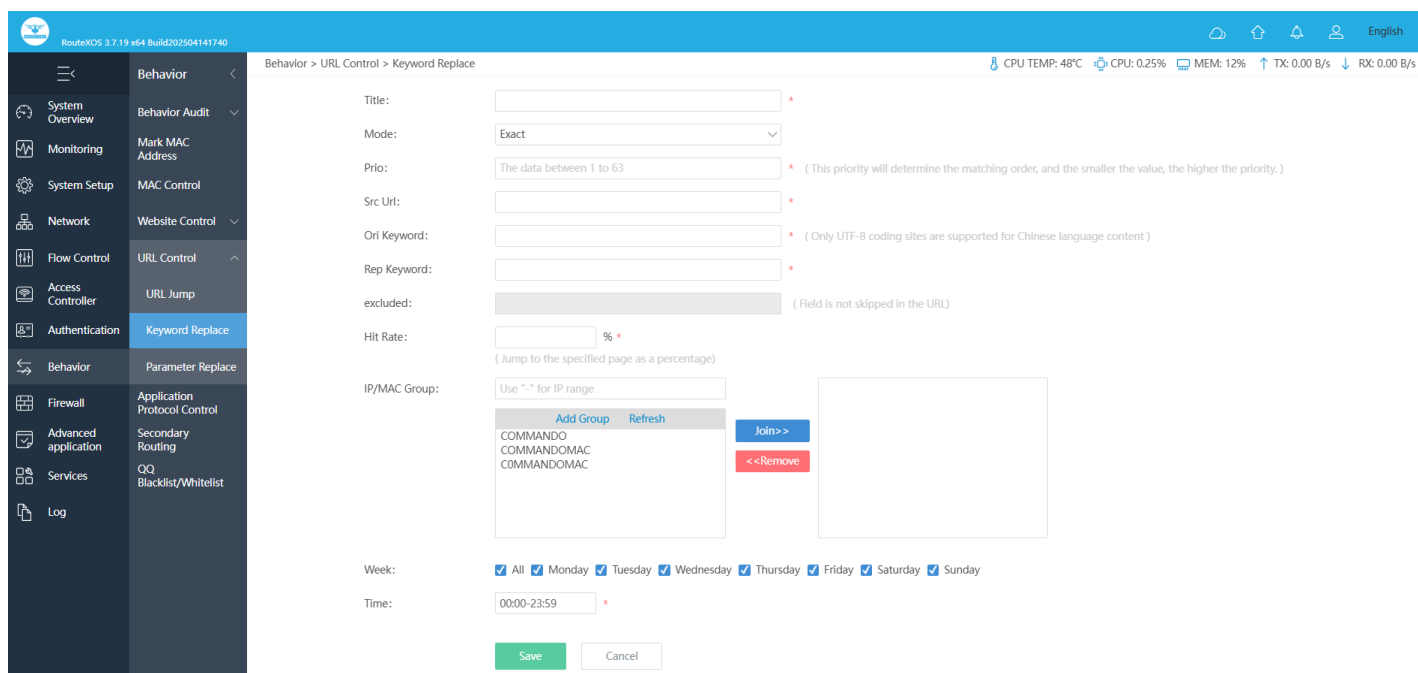


Fig 7.5.6 Add Keywords Replacement Settings page

RouteXOS 3.7.19 x64 Build202304141740

Behavior > URL Control > Keyword Replace

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Title:

Mode:

Prio: (This priority will determine the matching order, and the smaller the value, the higher the priority.)

Src Url:

Ori Keyword: (Only UTF-8 coding sites are supported for Chinese language content)

Rep Keyword:

excluded:

Hit Rate: % (Jump to the specified page as a percentage)

IP/MAC Group:

Week: ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Time:

Fig 7.5.7 Keywords Replacement Settings with keyword page

RouteXOS 3.7.19 x64 Build202304141740

Behavior > URL Control > Keyword Replace

CPU TEMP: 50°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

URL Keywords Replacement Settings

Title	Mode	Prio	Src Url	Ori Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions
COMMANDO1	Exact	1	www.cmdnw.com	cmdnw	commandonetworks		70	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage: Rows: / 1 Pages

Fig 7.5.8 URL Keywords Replacement Settings page

URL Parameter Replacement Settings: URL Parameter Replacement, also called URL rewriting, is the process of altering the parameters in a URL (Uniform Resource Locator). URL manipulation can be employed as a convenience by a Web server administrator, or for nefarious purposes by a hacker. To identify a URL parameter, refer to the portion of the URL that comes after a question mark (?). URL parameters are made of a key and a value, separated by an equal sign (=). Multiple parameters are each then separated by an ampersand (&).

To configure URL Parameter Replacement Settings, Click on Behavior > URL Control > Parameter Replace

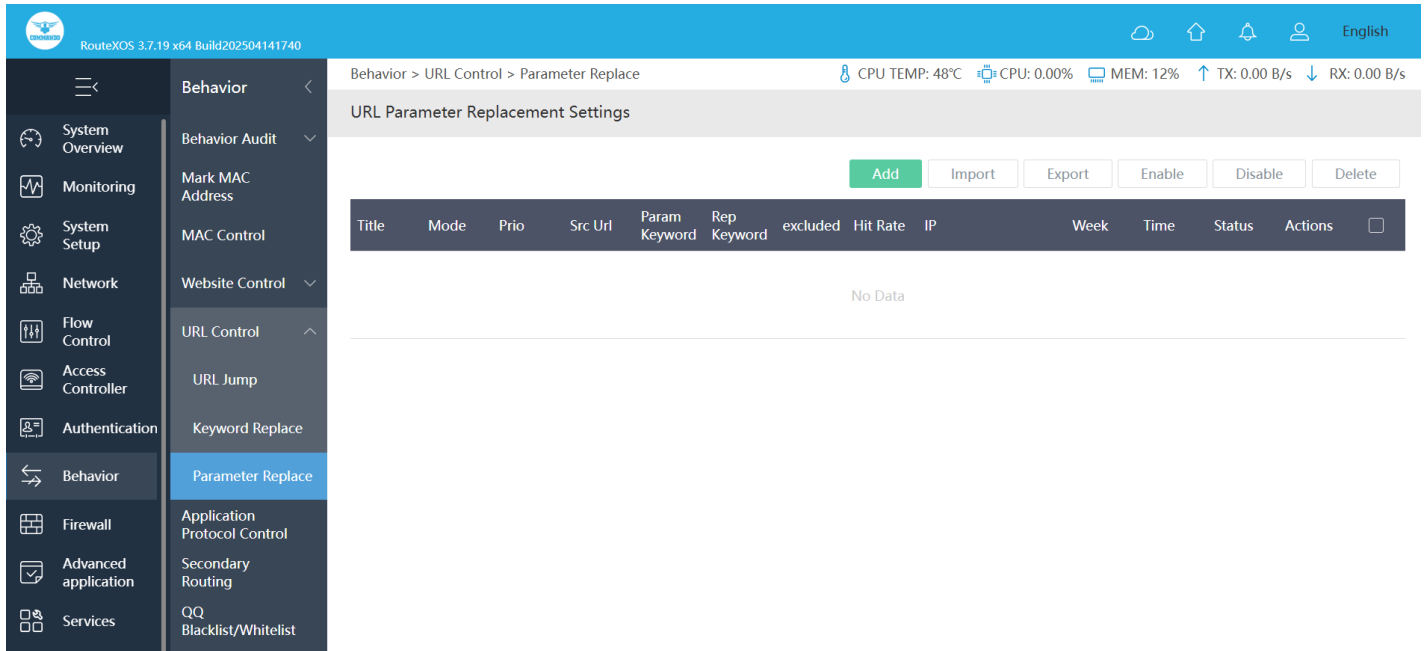


Fig 7.5.9 Default URL Parameter Replacement Settings page

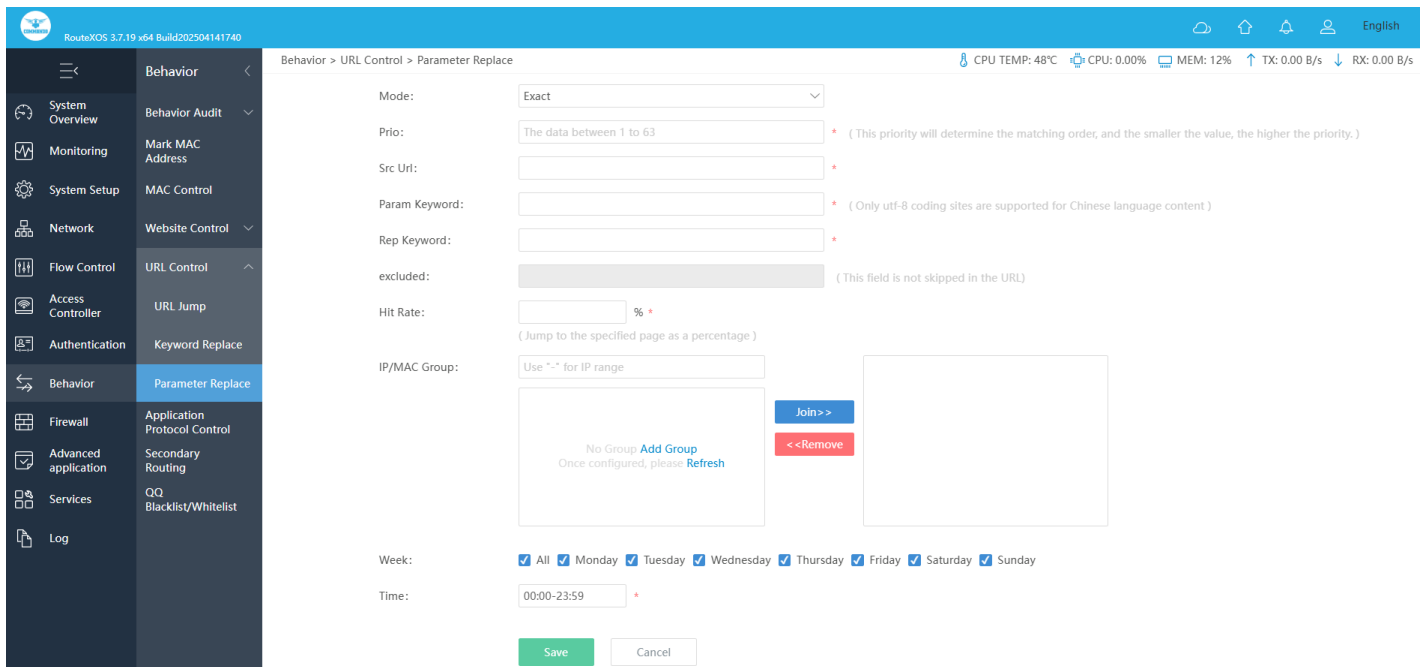


Fig 7.5.10 Add URL Parameter Replacement Settings page

Behavior > URL Control > Parameter Replace

Title: COMMANDOPParameter

Mode: Exact

Prio: 10

Src Url: www.commandonetworks.com

Param Keyword: -

Rep Keyword: -

excluded: (This field is not skipped in the URL)

Hit Rate: 70 %

(Jump to the specified page as a percentage)

IP/MAC Group: 192.168.0.0/24

Week: ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Time: 00:00-23:59

Save Cancel

Fig 7.5.11 URL Parameter Replacement Settings add particular keyword page

Behavior > URL Control > Parameter Replace

URL Parameter Replacement Settings

Add Import Export Enable Disable Delete

Title	Mode	Prio	Src Url	Param Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions
COMMAN DOParame ter	Exact	10	www.com mandonet works.com	-	-		70	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 / 1Pages Jump

Fig 7.5.12 URL Parameter Replacement Settings page

7.6 Application Protocol Control

An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer protocol has different types of messages, e.g., request messages and response messages. we can control application layer: authentication, password policies, access control and authorization, encryption, session management.

Note:

1. High-priority policies will be matched first, and it is recommended to choose a priority between 10 and 50.
2. The default priority for “allow” is 31, and the default for “block” is 32.
3. If the configuration has the same priority, the first configured policy is matched.

To configure Application protocol control, Click on Behavior > Application Protocol Control

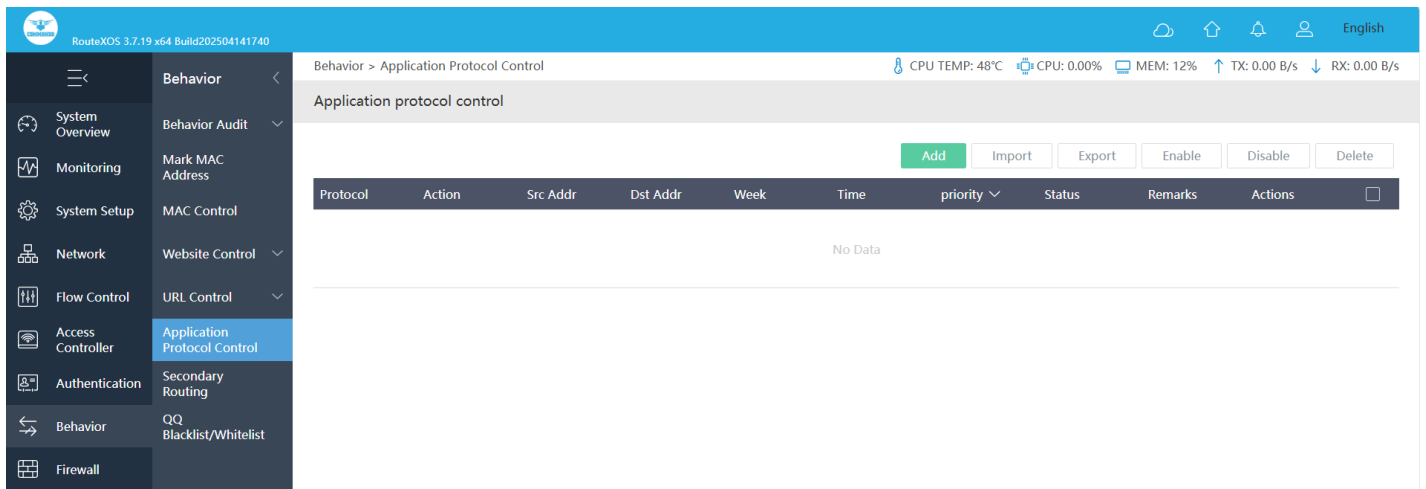


Fig 7.6.1 Default Application protocol control page

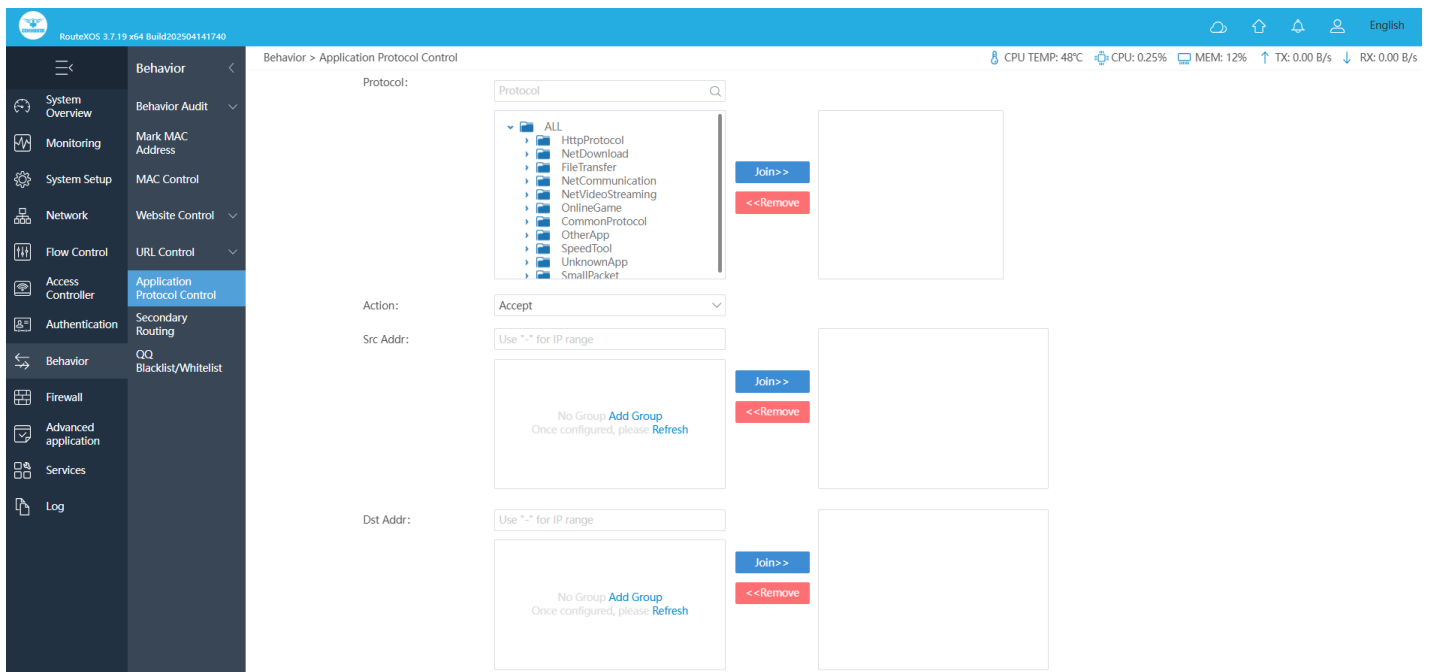


Fig 7.6.2 Add Application protocol control page

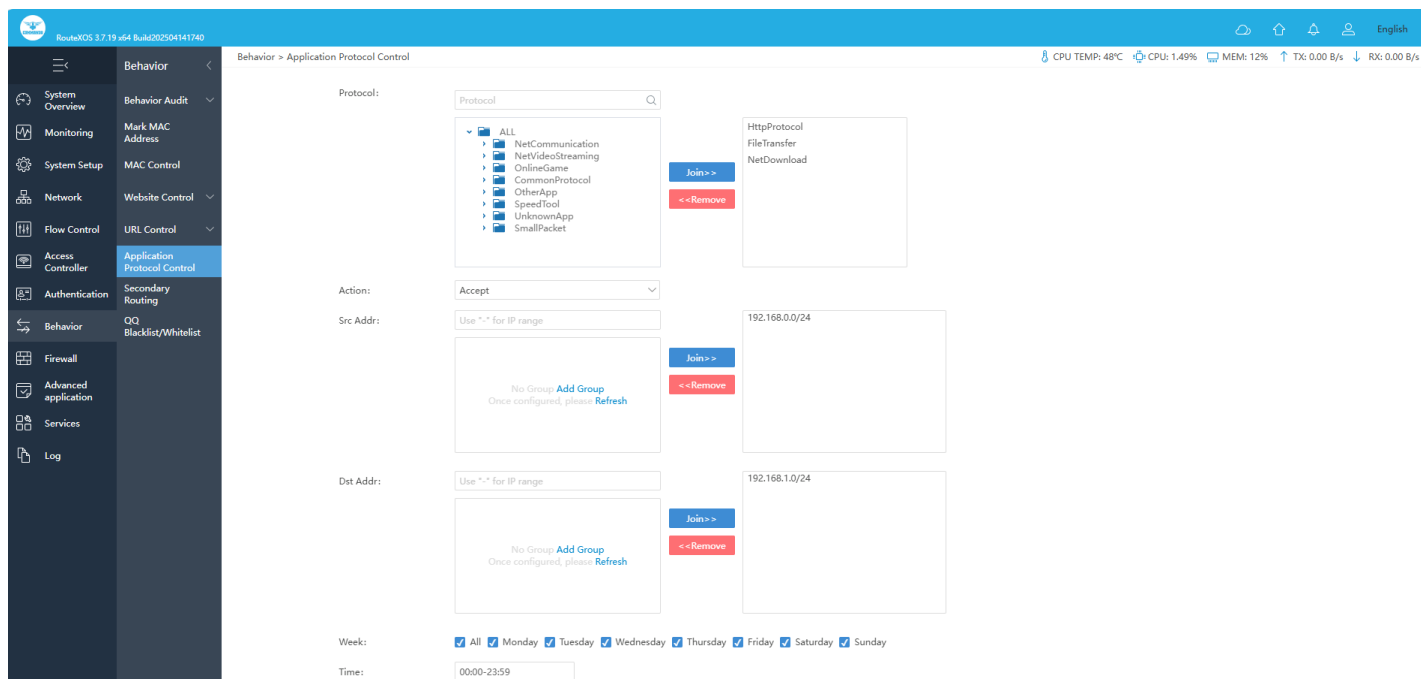


Fig 7.6.3 Application protocol control add particular action page

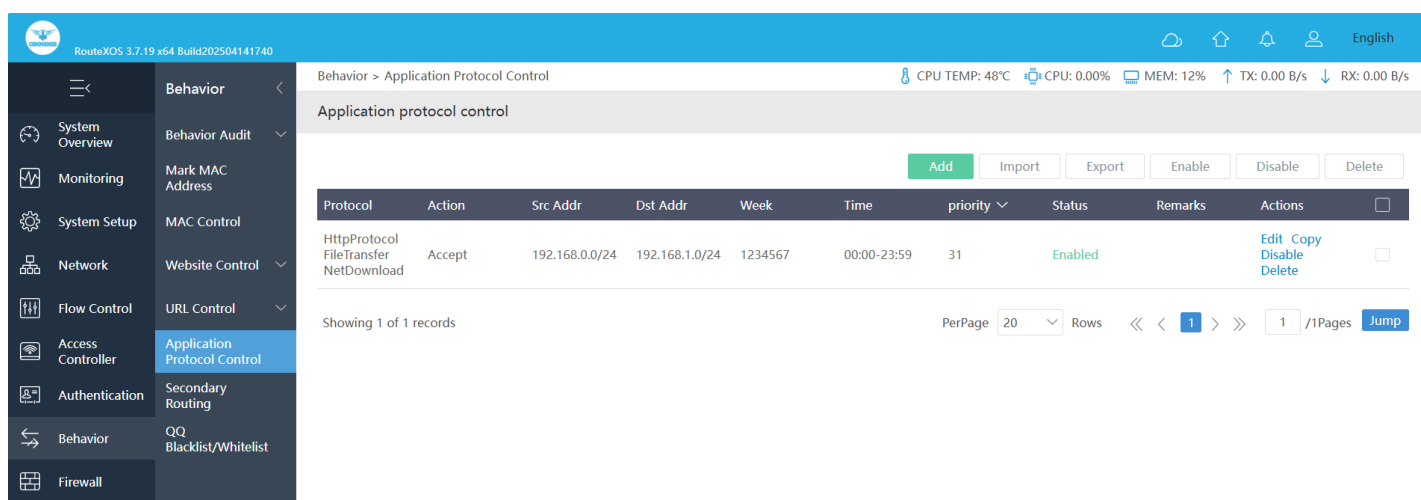


Fig 7.6.4 Application protocol control page

7.7 Secondary Routing

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as Gateways, gateways, firewalls, or switches. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

To configure Secondary Routing Settings, Click on Behavior > Secondary Routing

The screenshot shows the 'Behavior > Secondary Routing' settings page. The left sidebar contains a menu with options: System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior (selected), Firewall, Advanced application, Services, and Log. The 'Behavior' section is expanded, showing 'Secondary Routing' as the active option. The main content area is titled 'Secondary Routing Settings' and includes the following fields: 'No Secondary Routing' (checkbox, currently unchecked), 'Custom TTL' (input field with value '1'), 'Forbid Time' (input field with value '00:00-23:59'), and 'Exceptional address range' (input field with placeholder 'Use *.* for IP range'). Below these fields is a 'Save' button. On the right side, there is a 'Join >>' button and a '<< Remove' button. A message box states 'No Group Add Group Once configured, please Refresh'.

Fig 7.7.1 Default Secondary Routing Settings page

The screenshot shows the 'Behavior > Secondary Routing' settings page with 'No Secondary Routing' checked. The left sidebar is the same as in Fig 7.7.1. The main content area is titled 'Secondary Routing Settings' and includes the following fields: 'No Secondary Routing' (checkbox, currently checked), 'Custom TTL' (input field with value '1'), 'Forbid Time' (input field with value '00:00-23:59'), and 'Exceptional address range' (input field with placeholder 'Use *.* for IP range'). Below these fields is a 'Save' button. On the right side, there is a 'Join >>' button and a '<< Remove' button. A message box states 'No Group Add Group Once configured, please Refresh'. The 'Exceptional address range' field now contains the IP ranges '192.168.1.0/24' and '192.168.0.0/24'.

Fig 7.7.2 Secondary Routing Settings page

7.7 QQ Blacklist/Whitelist

Whitelisting is a much stricter approach to access control than blacklisting, as the default is to deny items and only let in those that are proven to be safe. This means that the risks of someone malicious gaining access of network are much lower when using the whitelisting approach. In Blacklisting mode all QQ can be logged in by default. QQ is not

allowed to login in the blacklist. In Whitelist mode all QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed.

To configure QQ Blacklist/Whitelist Settings, Click on Behavior > QQ Blacklist/Whitelist

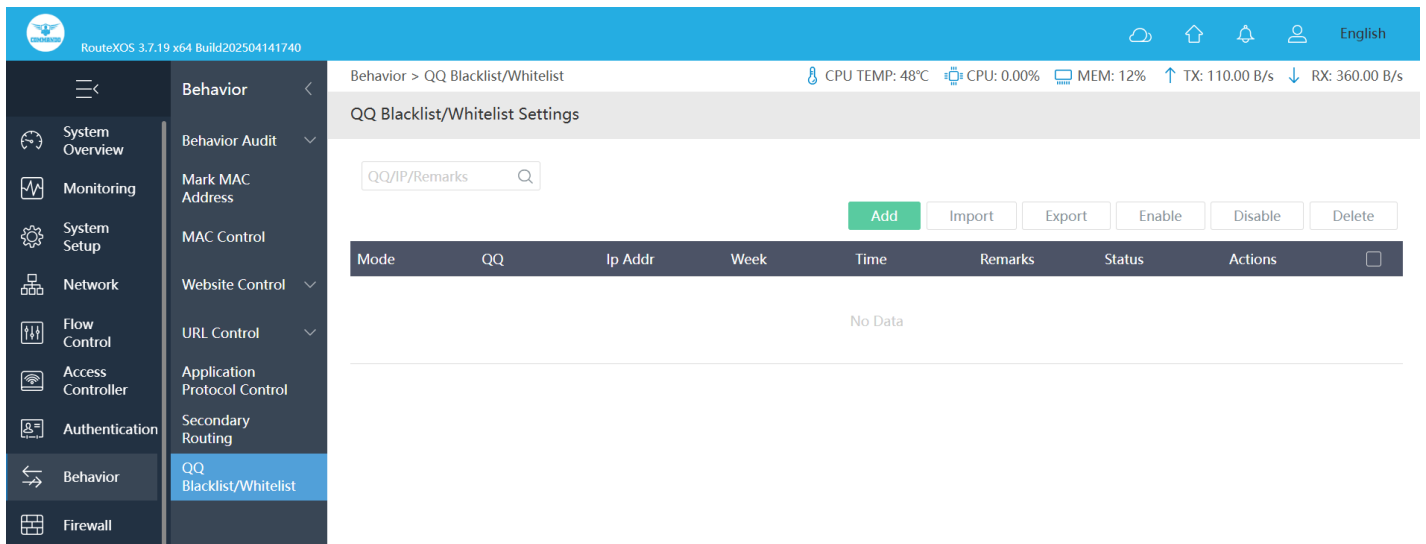


Fig 7.8.1 Default QQ Blacklist/Whitelist Settings page

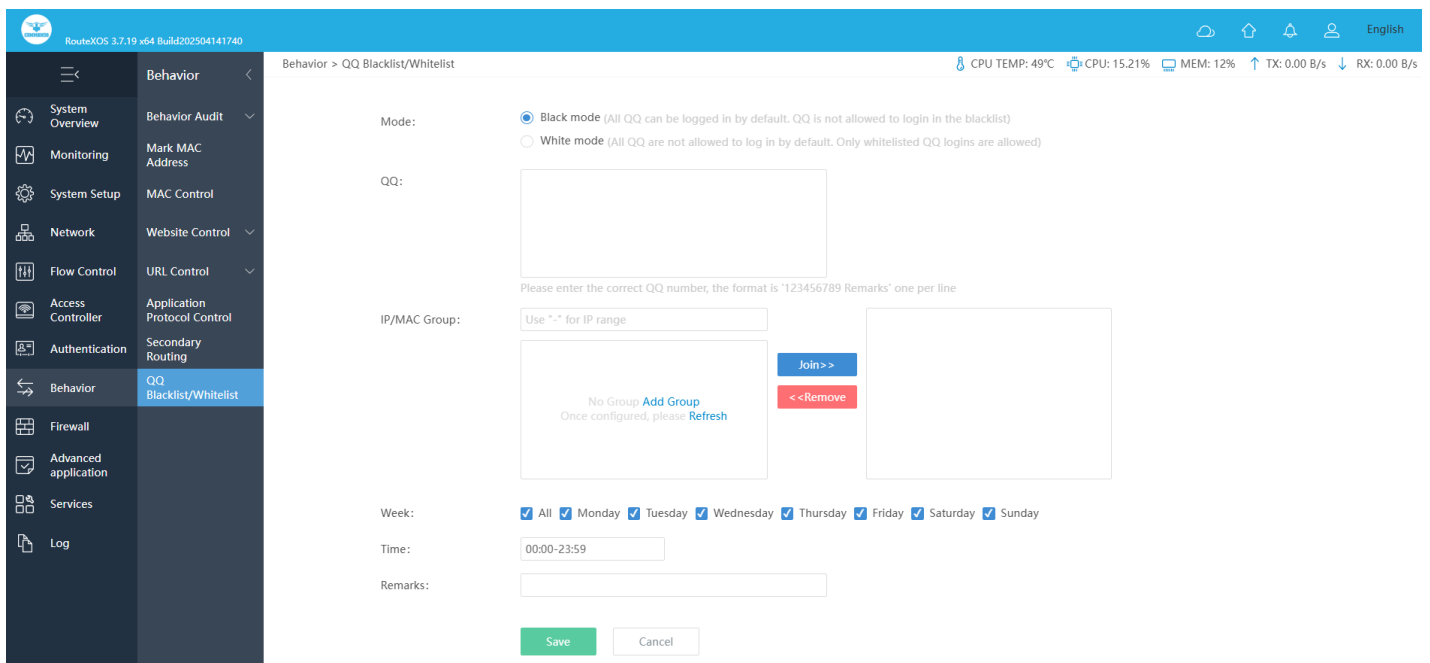


Fig 7.8.2 Add QQ Blacklist/Whitelist Settings page

RouteXOS 3.7.19 x64 Build202504141740

CPU TEMP: 49°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Behavior

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

Behavior

Behavior Audit

Mark MAC Address

MAC Control

Website Control

URL Control

Application Protocol Control

Secondary Routing

QQ Blacklist/Whitelist

Behavior > QQ Blacklist/Whitelist

Mode:

Black mode (All QQ can be logged in by default. QQ is not allowed to login in the blacklist)

White mode (All QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed)

QQ:

12345

Please enter the correct QQ number, the format is "123456789 Remarks" one per line

IP/MAC Group:

Use "-" for IP range

192.168.0.0/24

No Group Add Group

Once configured, please Refresh

Join >>

<< Remove

Week:

All

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Time:

00:00-23:59

Remarks:

Whitelist QQ

Save

Cancel

Fig 7.8.3 QQ Blacklist/Whitelist Settings for particular Network page

RouteXOS 3.7.19 x64 Build202504141740

CPU TEMP: 49°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Behavior

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

Behavior

Behavior Audit

Mark MAC Address

MAC Control

Website Control

URL Control

Application Protocol Control

Secondary Routing

QQ Blacklist/Whitelist

Behavior > QQ Blacklist/Whitelist

QQ Blacklist/Whitelist Settings

QQ/IP/Remarks

Add

Import

Export

Enable

Disable

Delete

Mode	QQ	Ip Addr	Week	Time	Remarks	Status	Actions
Whitelist	12345	192.168.0.0/24	1234567	00:00-23:59	Whitelist QQ	Enabled	<a>Edit <a>Disable <a>Delete

Showing 1 of 1 records

PerPage

20

Rows

<<

<

1

>

>>

1 / 1 Pages

Jump

Fig 7.8.4 QQ Blacklist/Whitelist Settings page

© 2025 COMMANDO Networks Inc. All rights reserved.

FIREWALL

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic. Firewall is barrier in between a private internal network and the public Internet. Firewall can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access. It monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules.

ACL Rules: Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack.

ARP binding: IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

Connection Limiter: Some programs use more bandwidth, limiting access for other users more important applications. A connection limiter helps control upload and download speeds on your network. A connection limiter will also show exactly what apps are more demanding in terms of network data.

Advanced Firewall: This advance firewall to Block PING from internal network, Block PING from public network, Disable tracert (Trace Route), Hijack all PING values, Discard invalid connection, Enable internal network DOS attack defense, Enable TCP maximum message length.

8.1 ACL Rules

An Access Control List (ACL) is a set of rules that is usually used to filter network traffic. Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. The ACL works according to rules and checks all

incoming and outgoing data to determine whether it complies with these rules. To configure Access Control List Rules Settings, Click on Firewall > ACL Rules

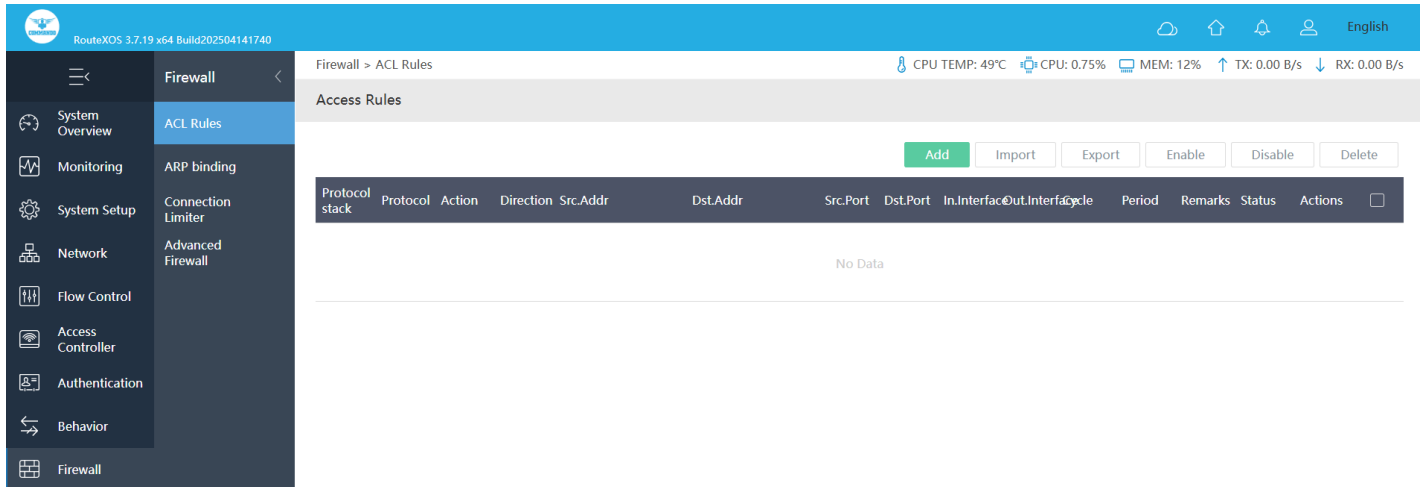
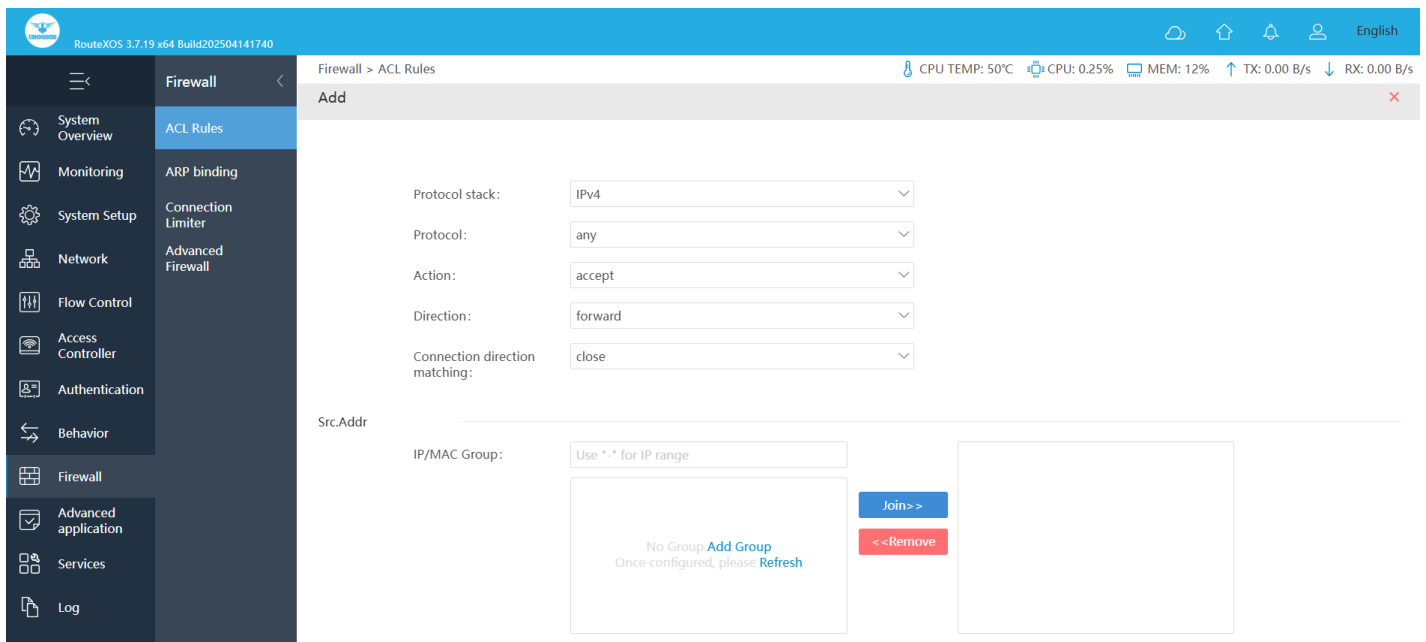


Fig 8.1.1 Default Access Control List Rules page



System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

ACL Rules

ARP binding

Connection Limiter

Advanced Firewall

Dst.Addr

IP/MAC Group: Use *.* for IP range

No Group Add Group

Once configured, please Refresh

Join>>

<<Remove

Src.Port:

Dst.Port:

In.Interface:

any

Out.Interface:

any

Cycle:

☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Period:

00:00-23:59

(please input as "00:00-09:00")

Remarks:

Save

Cancel

Fig 8.1.2 Add Access Control List Rules page

RouteXOS 3.7.19 x64 Build202504141740

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

ACL Rules

ARP binding

Connection Limiter

Advanced Firewall

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

ACL Rules

ARP binding

Connection Limiter

Advanced Firewall

Firewall > ACL Rules

CPU TEMP: 49°C

CPU: 0.00%

MEM: 12%

TX: 0.00 B/s

RX: 0.00 B/s

Add

Protocol stack:

IPv4

Protocol:

icmp

Action:

accept

Direction:

forward

Connection direction matching:

Original direction

Src.Addr

IP/MAC Group:

Use "-" for IP range

No Group

Add Group

Once configured, please Refresh

Join >>

<< Remove

192.168.0.0/24

Dst.Addr

IP/MAC Group:

Use "-" for IP range

No Group

Add Group

Once configured, please Refresh

Join >>

<< Remove

192.168.1.0/24

Src.Port:

Dst.Port:

In.Interface:

lan1,wan1

Out.Interface:

lan1,wan1

Cycle:

☒ All
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday
☒ Sunday

Period:

00:00-23:59

(please input as "00:00-09:00")

Remarks:

Blocking Ping

Save

Cancel

Fig 8.1.3 Add particular Access Control List Rules page

© 2025 COMMANDO Networks Inc. All rights reserved.

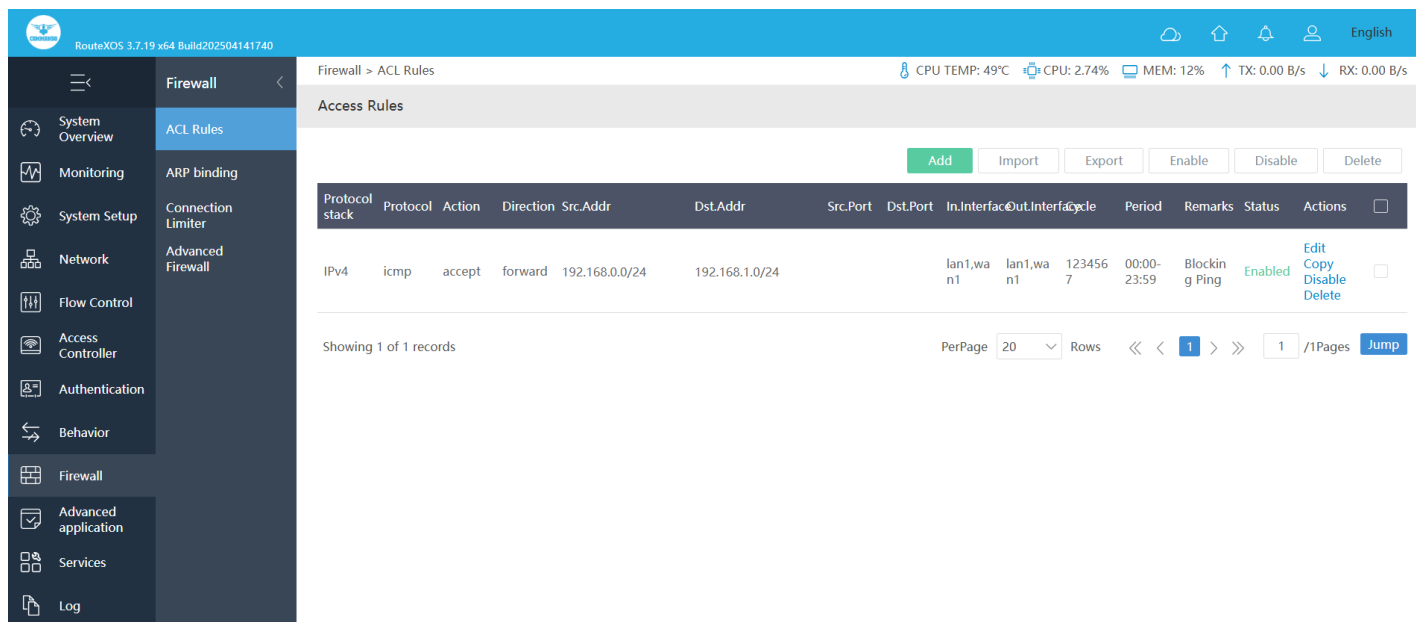


Fig 8.1.4 Access Control List Rules setting page

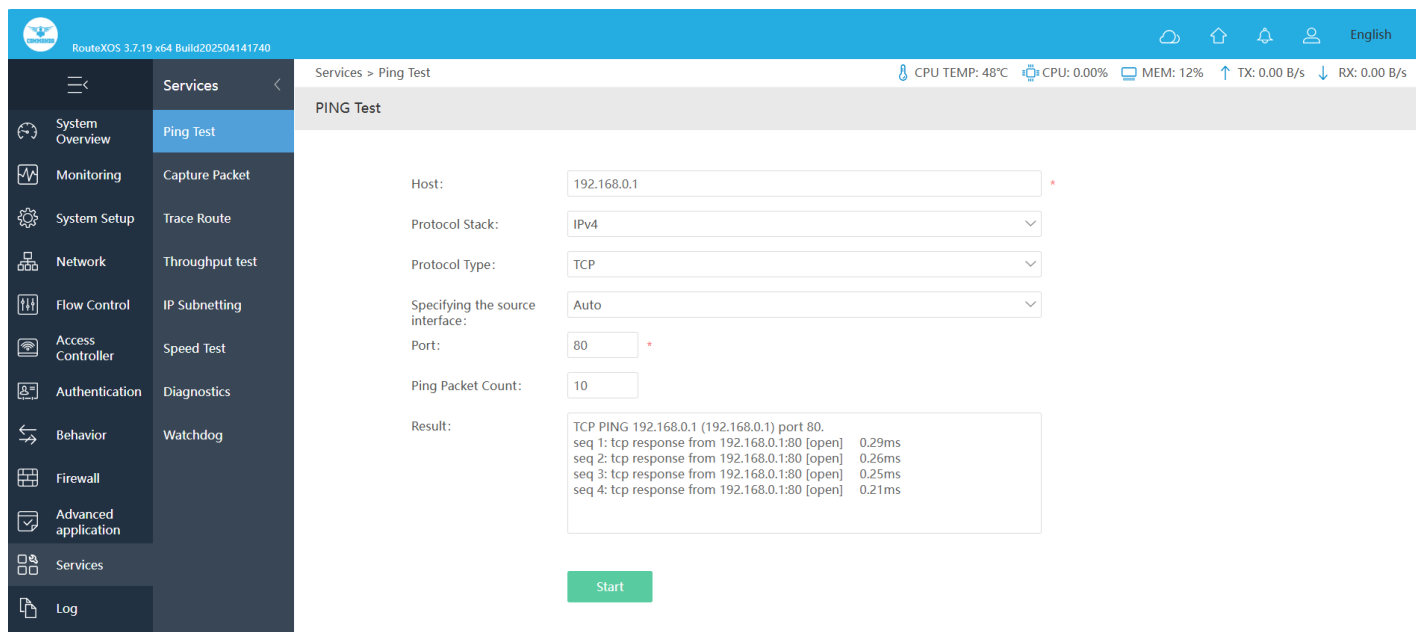


Fig 8.1.5 Impact of Access Control List Rules page

8.2 Arp Binding

Static ARP can implement the binding of IP addresses and MAC addresses to prevent ARP entries from being updated by forged ARP packets sent by attackers. Static ARP entries can be implemented when networks contain critical devices such as servers so that network attackers cannot update the ARP entries containing IP addresses of the critical devices on the switch using ARP attack packets, thereby ensuring communication between users and the critical devices. When network administrator wants to prevent an

IP address from accessing devices to bind the IP address to an unavailable MAC address. ARP binding fixes an IP address to a MAC address, so packets coming from any other IP/MAC combination won't be accepted. ARP binding essentially means binding together the MAC and IP addresses, so that all requests from that IP address are served only by the PC having that particular MAC address means that if the IP address or the MAC address changes, the device can no longer access the network.

Note: By default all IP and MAC are in Unbinding state. It is generally between IP and MAC (default). Only IP and MAC, if not correctly matched, can't access network resources. The only binding advice is to statically assign the checked and compatible ARP list to the DHCP client. Exports or imports the list of ARPs in the bound state

For ARP Binding, Click on Firewall > ARP binding

RouteXOS 3.7.19 x64 Build202504141740

Firewall > ARP binding

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

ARP Binding

Compatibility has been bound to DHCP static allocation: ☐ Open

Unbound MAC is not allowed to surf the Internet: ☐ Open

Save

ARP Binding List

IP/MAC/Remarks

Add Import Export Bind Clean Delete

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.10	a0:8c:fd:a5:68:9d	lan1	General		Unbinding	Bind Edit Delete
192.168.1.1	08:9b:4b:12:4d:53	wan1	General		Unbinding	Bind Edit Delete

Showing 1-2 of 2 records

PerPage 20 Rows 1 / 1Pages Jump

Fig 8.2.1 Default ARP Binding page

RouteXOS 3.7.19 x64 Build202504141740

Firewall > ARP binding

CPU TEMP: 48°C CPU: 2.76% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

ARP Binding

Compatibility has been bound to DHCP static allocation: ☐ Open

Unbound MAC is not allowed to surf the Internet: ☐ Open

Save

ARP Binding List

IP/MAC/Remarks

Add Import Export Bind Clean Delete

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.10	a0:8c:fd:a5:68:9d	lan1	General		Binding	Edit Delete
192.168.1.1	08:9b:4b:12:4d:53	wan1	General		Binding	Edit Delete

Showing 1-2 of 2 records

PerPage 20 Rows 1 / 1 Pages Jump

Fig 8.2.2 After Binding ARP page

RouteXOS 3.7.19 x64 Build202504141740

Firewall > ARP binding

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

IP: 192.168.10.1

MAC: 44:99:87:77:ad:46

NIC belongs: lan1

Bind type: General

Remarks: IP and MAC Static Binding

Save Cancel

Fig 8.2.3 Add ARP Binding page

RouteXOS 3.7.19 x64 Build202504141740

Firewall > ARP binding

CPU TEMP: 50°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Save

ARP Binding List

IP/MAC/Remarks

Add Import Export Bind Clean Delete

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.10	a0:8cfd:a5:68:9d	lan1	General		Binding	Edit Delete
192.168.1.1	08:9b:4b:12:4d:53	wan1	General		Binding	Edit Delete
192.168.10.1	44:99:87:77:ad:46	lan1	General	IP and MAC Static Binding	Binding	Edit Delete

Showing 1-3 of 3 records

PerPage 20 Rows 1 / 1 Pages Jump

Fig 8.2.4 Static ARP Binding page

8.3 Connection Limiter

Some IPs use more bandwidth, limiting access for other, more important applications. A connection limiter for network helps control upload and download speeds on your network.

To configure Connection Limiter Settings, Click on Firewall > Connection Limiter

RouteXOS 3.7.19 x64 Build202504141740

Firewall > Connection Limiter

CPU TEMP: 48°C CPU: 2.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Connection Limiter Settings

Add Import Export Enable Disable Delete

IP Address	Protocol	WAN Port	Limit	Cycle	Period	Remarks	Status	Actions
No Data								

Fig 8.3.1 Default Connection Limiter Settings page

RouteXOS 3.7.19 x64 Build202504141740

Firewall > Connection Limiter

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

IP Address: Use *.* for IP range 192.168.0.0/24

No Group Add Group Once configured, please Refresh

Join>> <<Remove

Protocol: icmp

WAN Port:

Limit: 3

Cycle: ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Period: 00:00-23:59 (please input as "00:00-09:00")

Remarks: ICMP Limit

Save Cancel

Fig 8.3.2 Add Connection Limiter Settings page

RouteXOS 3.7.19 x64 Build202504141740

Firewall > Connection Limiter

CPU TEMP: 48°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Connection Limiter Settings

Add Import Export Enable Disable Delete

IP Address	Protocol	WAN Port	Limit	Cycle	Period	Remarks	Status	Actions
192.168.0.0/24	icmp		3	1234567	00:00-23:59	ICMP Limit	Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 8.3.3 Connection Limiter Settings page

8.4 Advanced Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Generally, Firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall is a security device in network that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access. A firewall is an essential part of security system. Without it, your network is open to threats and attacks. A firewall keeps destructive and disruptive forces out and controls the incoming and outgoing

network traffic based on security parameters that you can control and define. Advance firewall to Block PING from internal network, Block PING from public network, Disable tracert (Trace Route), Hijack all PING values, Discard invalid connection and also enable internal network DOS attack defense and TCP maximum message length.

To configure Advanced Firewall Configuration, Click on Firewall > Advanced Firewall

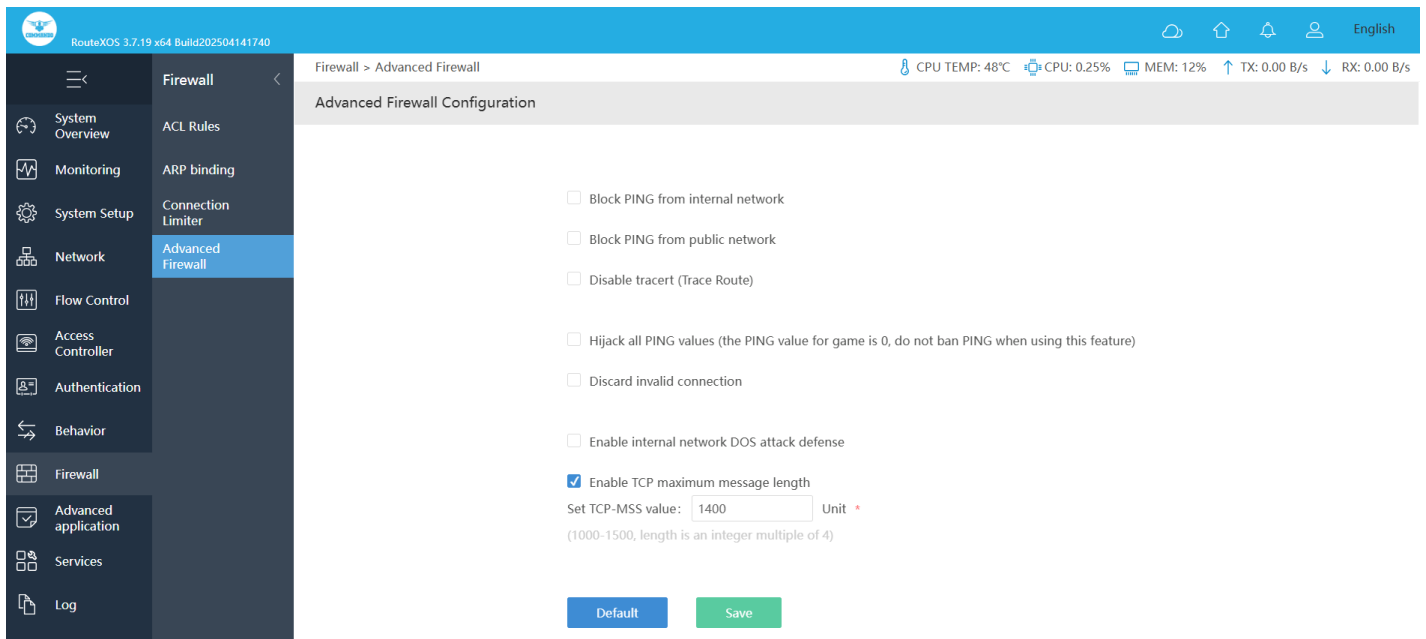


Fig 8.4.1 Default Advanced Firewall Configuration page

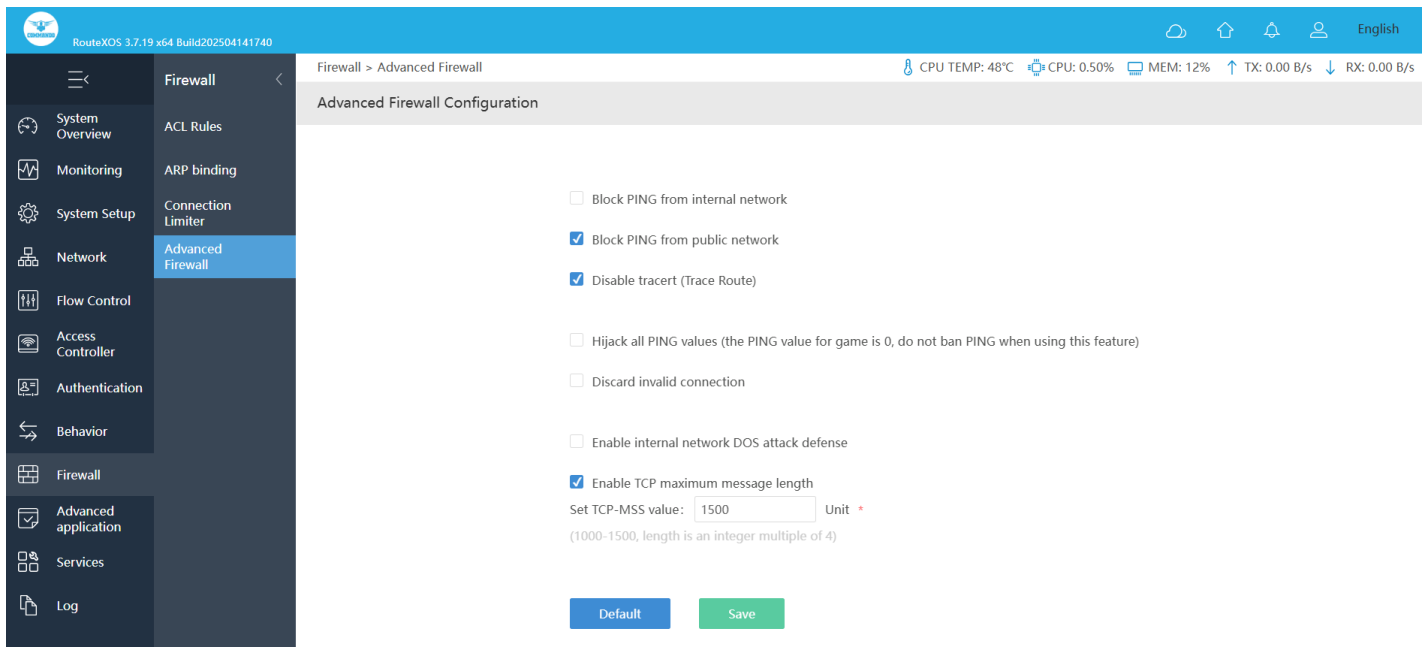


Fig 8.4.2 Advanced Firewall Configuration page

ADVANCED APPLICATION

Cache Service: Cache Service improves network performance by temporarily storing frequently accessed data to reduce latency and bandwidth usage. It enhances speed by serving cached content instead of fetching it from the original source repeatedly.

- **Cache Service Tab:** Enables configuration of caching policies and storage allocation for optimized performance.
- **Cache Status Tab:** Displays real-time cache usage, hit rate, and performance metrics.

Dynamic DNS: DDNS (Dynamic DNS) server provides a fixed domain name for DDNS client and maps its latest IP address to this domain name.

SNMP: SNMP stands for Simple Network Monitoring Protocol. It is a protocol for management information transfer in networks, for use in LANs especially.

Application across three layers: The protocol's client/server architecture has three components SNMP Manager, SNMP Agent and Management Information Base (MIB). The SNMP Manager acts as the client, the SNMP Agent acts as the server and the Management Information Base acts as the server's database. When the SNMP Manager asks the Agent a query, the Agent uses the MIB provide reply.

Port Mirroring: Port Mirroring allows network administrators to monitor and analyze network traffic by duplicating packets from one or more ports to a designated monitoring port. This feature is useful for network troubleshooting, security analysis, and performance diagnostics.

Virtual Machine: The Virtual Machine feature enables users to create and manage virtualized environments on the device, allowing multiple operating systems to run simultaneously. This enhances resource utilization, testing, and deployment of isolated applications.

Plugin Management: Plugin Management provides a centralized interface for installing, updating, and managing additional software modules or extensions, enabling enhanced functionality and customization of the system.

Wake on LAN: This utility allows you to easily turn on one or more computers remotely by sending Wake-on-LAN (WOL) packet to the remote computers. Wake-on-LAN (WOL) allows a computer to be powered on or awakened from standby, hibernate or shutdown from another device on a network.

FTP Server: FTP is a widely used network protocol for transferring files over a TCP/IP-based network, such as the Internet. FTP allows applications exchange and share data within their offices and across the Internet. FTP servers are the solutions used to facilitate file transfers across the internet. If you send files using FTP, files are either uploaded or downloaded to the FTP server.

Samba Server: Samba Server allows file and printer sharing across different operating systems within a network. It enables seamless interoperability between Windows and Unix/Linux-based systems by implementing the SMB/CIFS protocol.

HTTP Server: An HTTP server is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view web pages). An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device.

UDPXY Set: UDPXY is a UDP-to-HTTP multicast traffic relay daemon it forwards UDP traffic from a given multicast subscription to the requesting HTTP client. UDPXY listens (on a dedicated address/port) for HTTP requests issued by clients.

1. Cache Service

Cache Service enhances network efficiency by storing frequently accessed data, reducing latency, and optimizing bandwidth usage. It allows faster retrieval of cached content instead of repeatedly fetching it from the original source. This improves overall performance for users accessing the same data multiple times.

The Cache Service feature enables administrators to configure caching policies, define storage allocation, and manage cache refresh intervals for optimal performance. The Cache Status tab provides real-time insights into cache usage, hit rates, and overall system efficiency.

To configure Cache Service settings, Click on Advanced Application > Cache Service

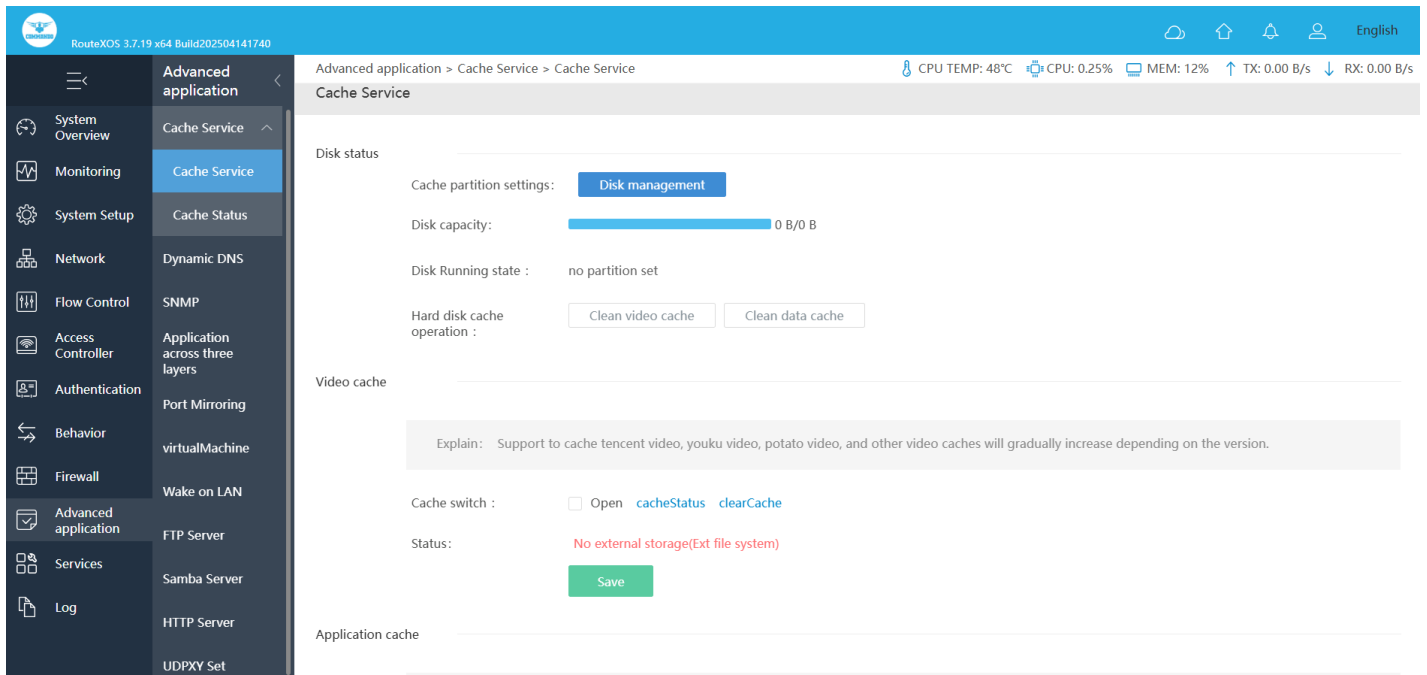


Fig 9.1.1 Default Cache Service Settings page

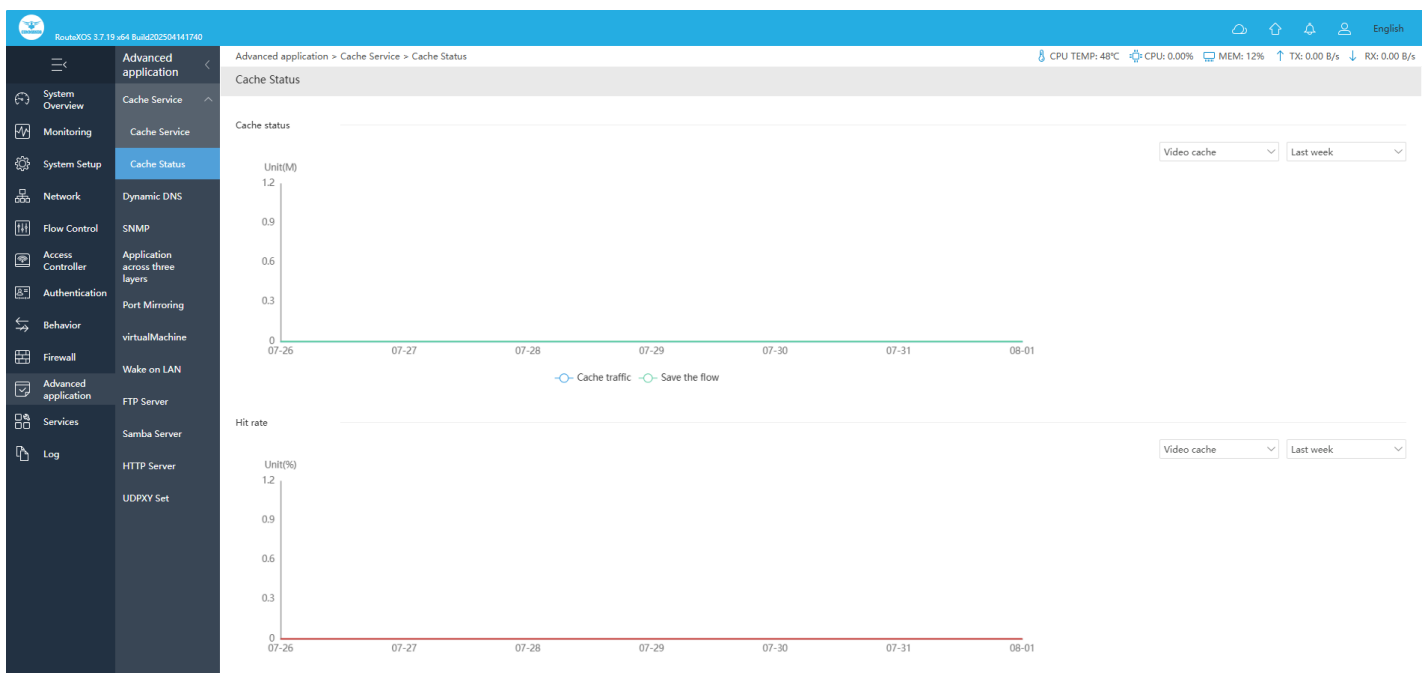


Fig 9.1.2 Default Cache Service Settings page

2. Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows controller with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider and set up an account with a DDNS service, the host & domain name, username, password detail will be provided by the account provider.

It allows address, which enables the Internet hosts to access the Gateway or the hosts in LAN using the domain names. As many ISPs use DHCP to assign public IP addresses in WAN, the public IP address assigned to the client is unfixed. In this way, it's very difficult for other clients to get the latest IP address of this client for access.

DDNS (Dynamic DNS) server provides a fixed domain name for DDNS client and maps its latest IP address to this domain name. When DDNS server works, DDNS client informs the DDNS server of the latest IP address, the server will update the mappings between the domain name and IP address in DNS database. Therefore, the users can use the same domain name to access the DDNS client even if the IP address of the DDNS client has changed. DDNS is usually used for the Internet users to access the private website and FTP server, both of which are established based on Web server.

To configure Dynamic DNS Settings, Click on Advanced application > Dynamic DNS

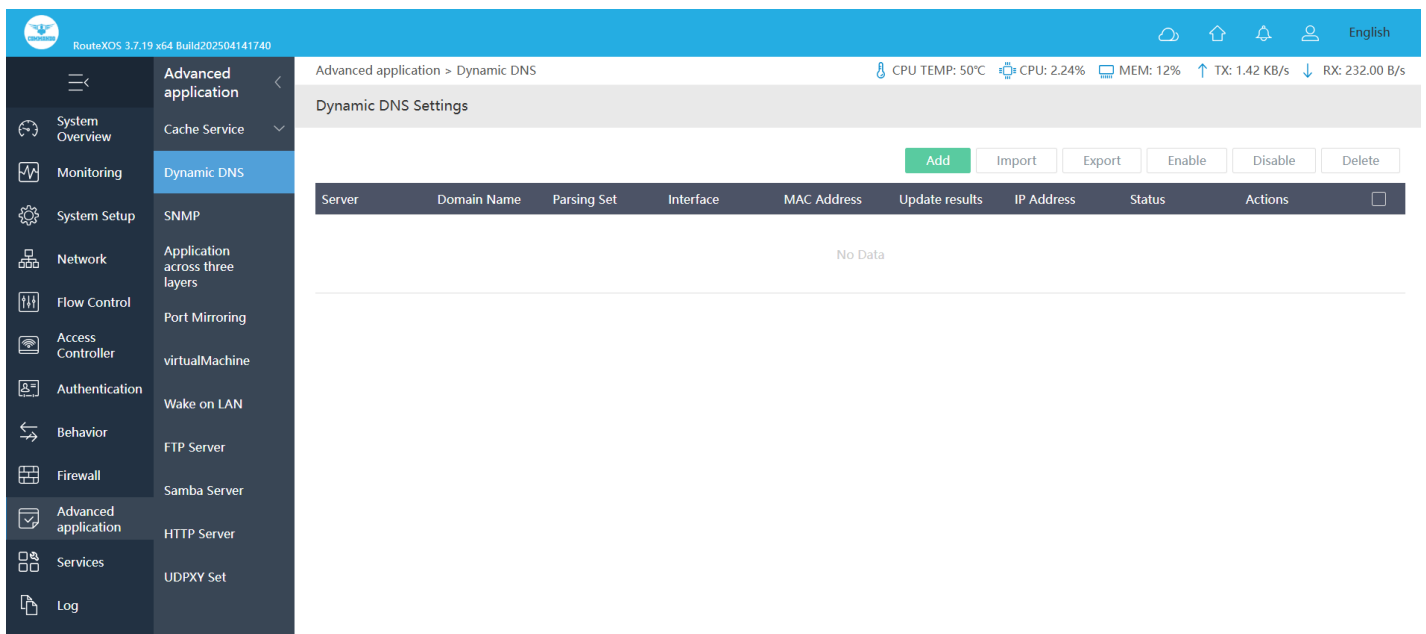


Fig 9.2.1 Default Dynamic DNS Settings page

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > Dynamic DNS

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Server: 3322.org

Domain Name: *

Username: *

Password: *

Interface: *

Parsing IP type: Interface IP *

Record Type: A Record(IPv4) *

Save Cancel

Fig 9.2.2 Add Dynamic DNS Settings page

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > Dynamic DNS

CPU TEMP: 48°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

Server: 3322.org

Domain Name: www.commandonetworks.com *

Username: admin *

Password: ***** *

Interface: auto *

Record Type: A Record(IPv4) *

Save Cancel

Fig 9.2.3 Add Particular Dynamic DNS Settings page

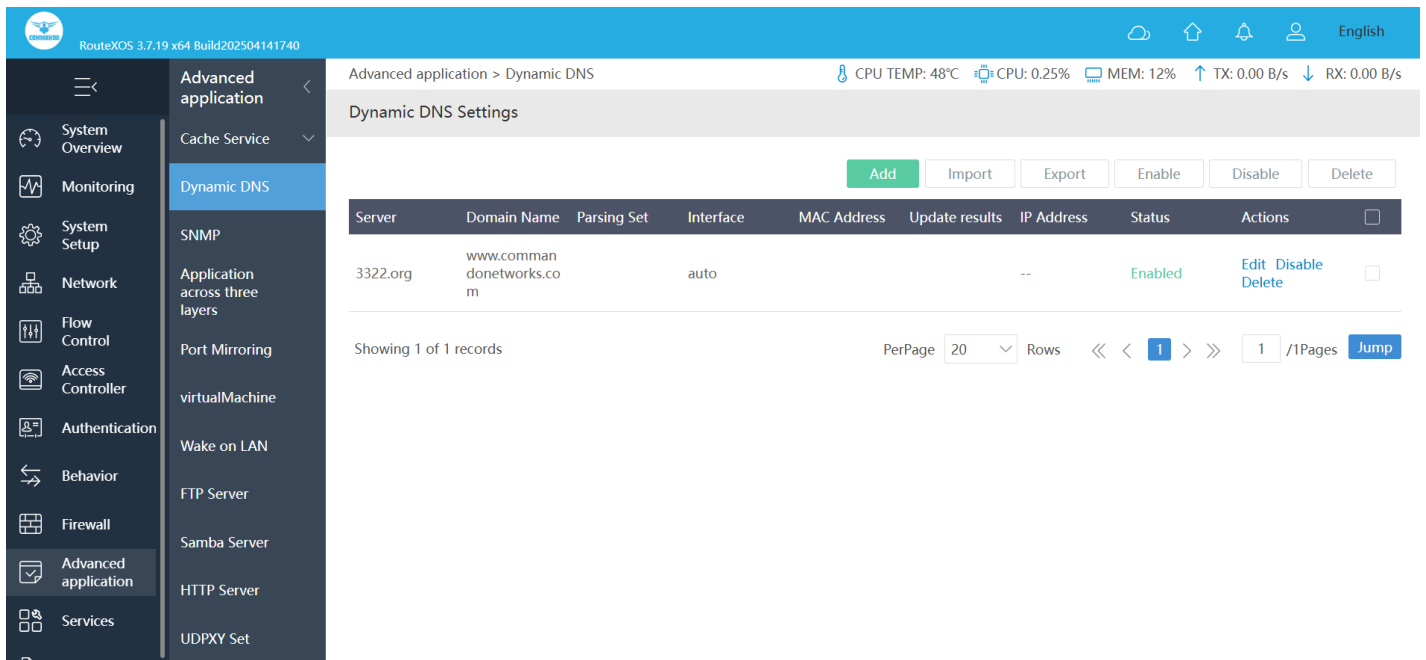


Fig 9.2.4 Dynamic DNS Settings page

3. SNMP

SNMP stands for Simple Network Monitoring Protocol. It is a protocol for management information transfer in networks, for use in LANs especially for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. SNMP has been defined with four major functional areas to support the core function of allowing managers to manage agents:

Data Definition: The syntax conventions for how to define the data to an agent or manager. These specifications are called the Structure of Management Information (SMI).

MIBs: Over 100 Internet standards define different MIBs, each for a different technology area, with countless vendor proprietary MIBs as well. The MIB definitions conform to the appropriate SMI version.

Protocols: The messages used by agents and managers to exchange management data.

Security and Administration: Definitions for how to secure the exchange of data between agents and managers

Understanding SNMP

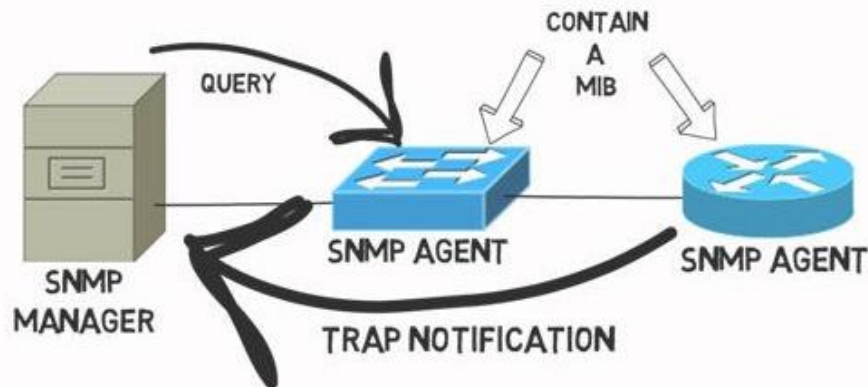


Fig 9.3.1 SNMP Community concept SNMP

Version

v1 - simple authentication with communities but used MIB-I originally.

v2 - Uses SMIv2, removed requirement for communities, added Get Bulk and Inform messages, but began with MIB-II originally. 2c Pseudo-release (RFC 1905) that allowed SNMPv1-style communities with SNMPv2; otherwise, equivalent to SNMPv2.

v3 - Mostly identical to SNMPv2, but adds significantly better security, although it supports communities for backward compatibility. Uses MIB-II.

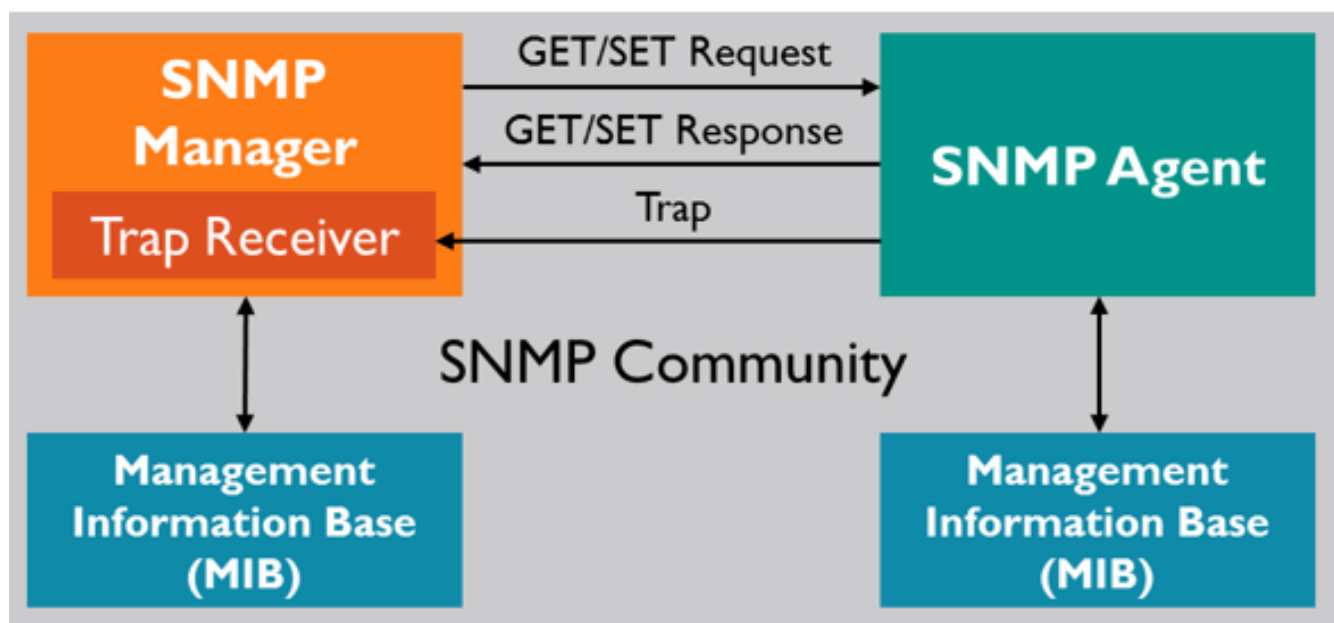


Fig 9.3.2 SNMP Community concept

How to enable Simple Network Monitoring Protocol?

To configure and enable Simple Network Monitoring Protocol Settings, Click on Advanced application > SNMP

The screenshot shows the 'Simple Network Monitoring Protocol Settings' page in the RouteXOS interface. The left sidebar contains a menu with 'Advanced application' selected. The main content area is titled 'Simple Network Monitoring Protocol Settings' and is divided into two sections: 'SNMP Configuration' and 'Advanced Configuration'. In the 'SNMP Configuration' section, the 'SNMP' checkbox is unchecked, and the 'Monitor Port' is set to 161. In the 'Advanced Configuration' section, the 'SNMP Configuration' dropdown is set to 'SNMP V2C', the 'Name' is 'public', the 'Permission' is 'Read only', and the 'IP Address' field is empty.

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > SNMP

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Simple Network Monitoring Protocol Settings

SNMP Configuration

SNMP: ☐ Open

Monitor Port:

Physical Location:

Contact:

System Information:

Advanced Configuration

SNMP Configuration:

Name:

Permission: ☒ Read only ☐ Read-write

IP Address :

Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)

Fig 9.3.3 Default Simple Network Monitoring Protocol Settings page

The screenshot shows the 'Simple Network Monitoring Protocol Settings' page in the RouteXOS interface, but with SNMP enabled and configured. In the 'SNMP Configuration' section, the 'SNMP' checkbox is checked, and the 'Monitor Port' is still 161. The 'Physical Location' is now 'COMMANDOHQ', the 'Contact' is 'ABC', and the 'System Information' is 'SNMPServer'. In the 'Advanced Configuration' section, the 'SNMP Configuration' dropdown is still 'SNMP V2C', the 'Name' is 'public', the 'Permission' is now 'Read-write', and the 'IP Address' is '192.168.0.10/24'.

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > SNMP

CPU TEMP: 49°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Simple Network Monitoring Protocol Settings

SNMP Configuration

SNMP: ☒ Open

Monitor Port:

Physical Location:

Contact:

System Information:

Advanced Configuration

SNMP Configuration:

Name:

Permission: ☐ Read only ☒ Read-write

IP Address :

Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)

Fig 9.3.4 Simple Network Monitoring Protocol Settings page

9.4 Application across three layers

The protocol's client/server architecture has three components SNMP Manager, SNMP Agent and Management Information Base (MIB). The SNMP Manager acts as the client, the SNMP Agent acts as the server and the Management Information Base acts as the server's database. When the SNMP Manager asks the Agent a query, the Agent uses the MIB provide reply.

To configure Application across three layers, Click on Advanced application > Application across three layers

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > Application across three layers

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Application across three layers

Access frequency: 0 s [Setting](#) 0 means real-time data acquisition

[Add](#) [Import](#) [Export](#) [Enable](#) [Disable](#) [Delete](#)

SNMP Server IP	IpSegment	SNMP service listening port	SNMP protocol version	Remarks	Status	Actions
No Data						

Fig 9.4.1 Default Application across three layers page

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > Application across three layers

CPU TEMP: 49°C CPU: 1.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Add

SNMP Server IP:

(Fill in the IP of the three-layer device in the internal network, and the device needs to open SNMP service)

IpSegment:

Use "-" for IP range

No Group [Add Group](#)
Once configured, please [Refresh](#)

Join > >
<< Remove

SNMP service listening port:

SNMP protocol version:

Remarks:

team Name:

Save Cancel

Fig 9.4.2 Add Application across three layers page

RouteXOS 3.7.19 x64 Build202504141740

Advanced application > Application across three layers

CPU TEMP: 49°C CPU: 0.75% MEM: 12% TX: 1.39 KB/s RX: 340.00 B/s

Add

SNMP Server IP:

(Fill in the IP of the three-layer device in the internal network, and the device needs to open SNMP service)

IpSegment:

Use "-" for IP range

192.168.0.0/24

No Group [Add Group](#)
Once configured, please [Refresh](#)

Join > >
<< Remove

SNMP service listening port:

SNMP protocol version:

Remarks:

team Name:

Save Cancel

Fig 9.4.3 Application across three layers for particular SNMP server page

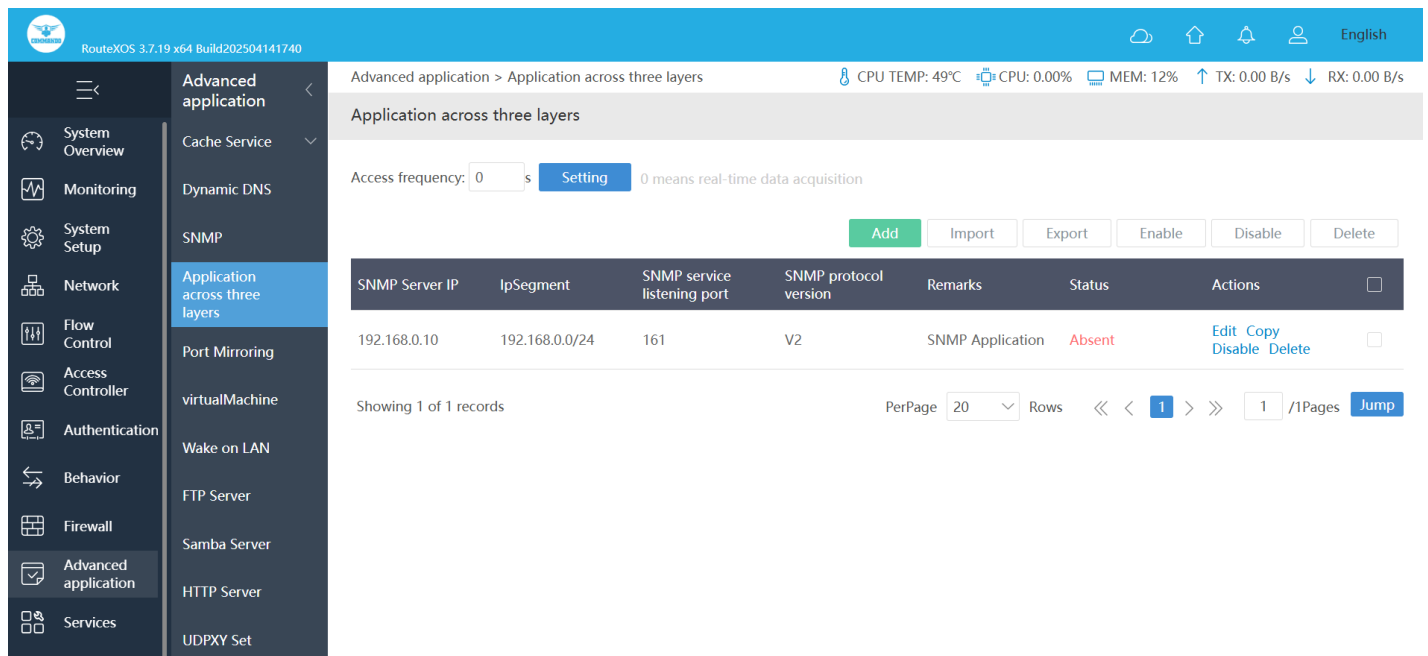


Fig 9.4.4 Application across three layers page

9.5 Port Mirroring

Port Mirroring is a network monitoring feature that allows administrators to duplicate network traffic from one or multiple ports to a designated monitoring port. This helps in analyzing network activity, troubleshooting issues, and enhancing security by capturing real-time data packets for inspection.

The Port Mirroring feature enables users to configure source and destination ports, select mirroring modes, and define traffic types to be mirrored. It ensures effective network diagnostics without disrupting live traffic flow.

To configure Port Mirroring settings, Click on Advanced Application > Port Mirroring

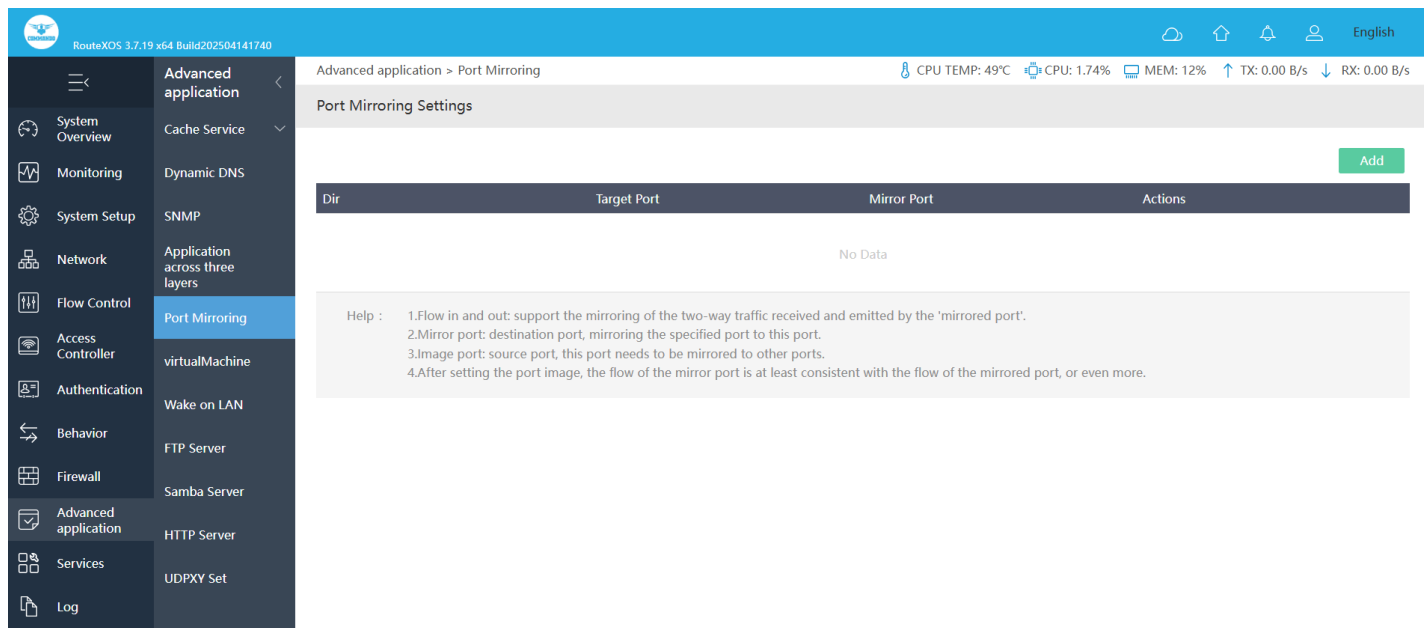


Fig 9.5.1 Default Port Mirroring Settings page

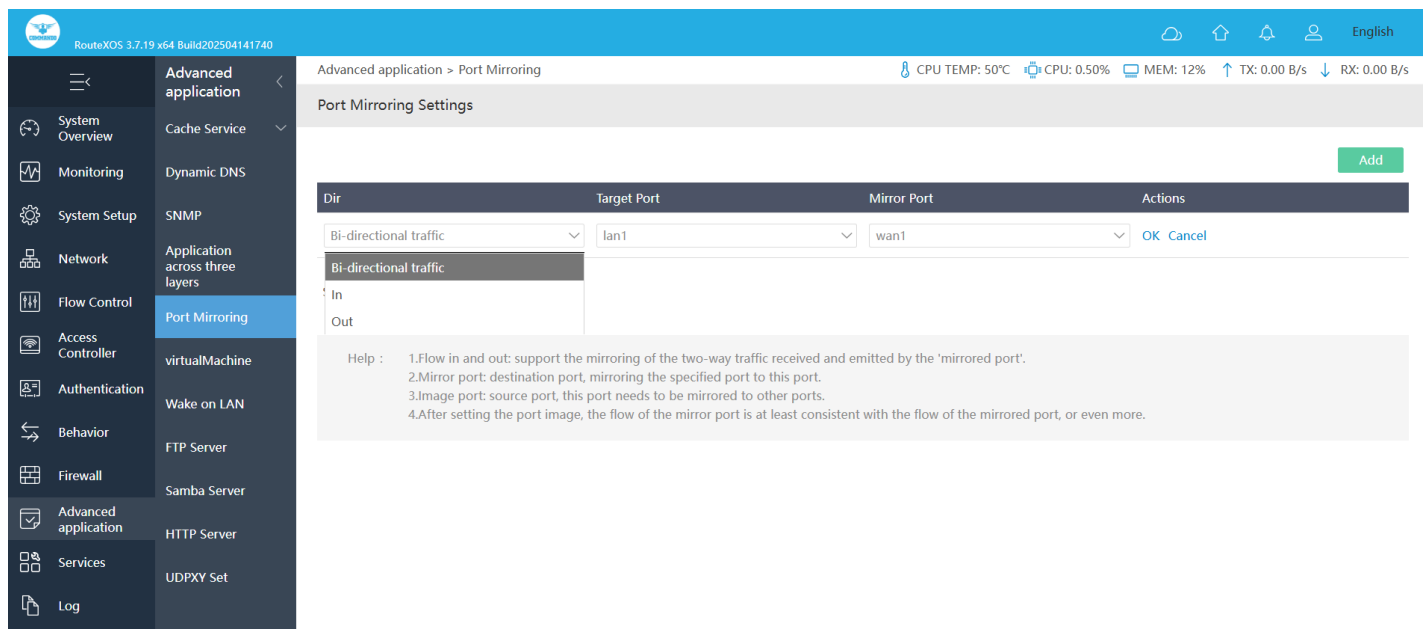


Fig 9.5.2 Add Port Mirroring Settings page

9.6 Virtual Machine

The Virtual Machine (VM) feature allows users to create and manage virtual instances within the controller, enabling efficient resource utilization and isolation of different workloads. Virtual machines help in running multiple operating systems on the same hardware, optimizing performance, and simplifying network management.

The Virtual Machine interface provides options to create, configure, and monitor VM instances. Users can allocate CPU, memory, and storage, manage snapshots, and configure networking settings for each virtual machine.

To configure Virtual Machine settings, Click on Advanced Application > Virtual Machine

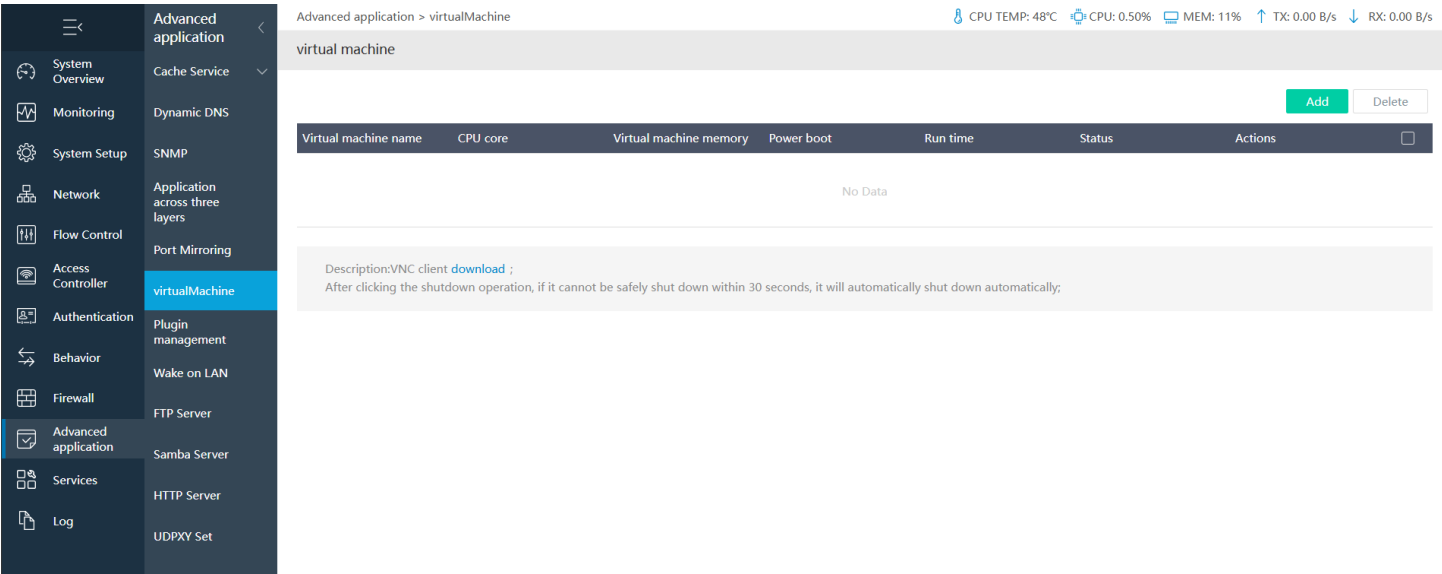


Fig 9.6.1 Default Virtual Machine Management page

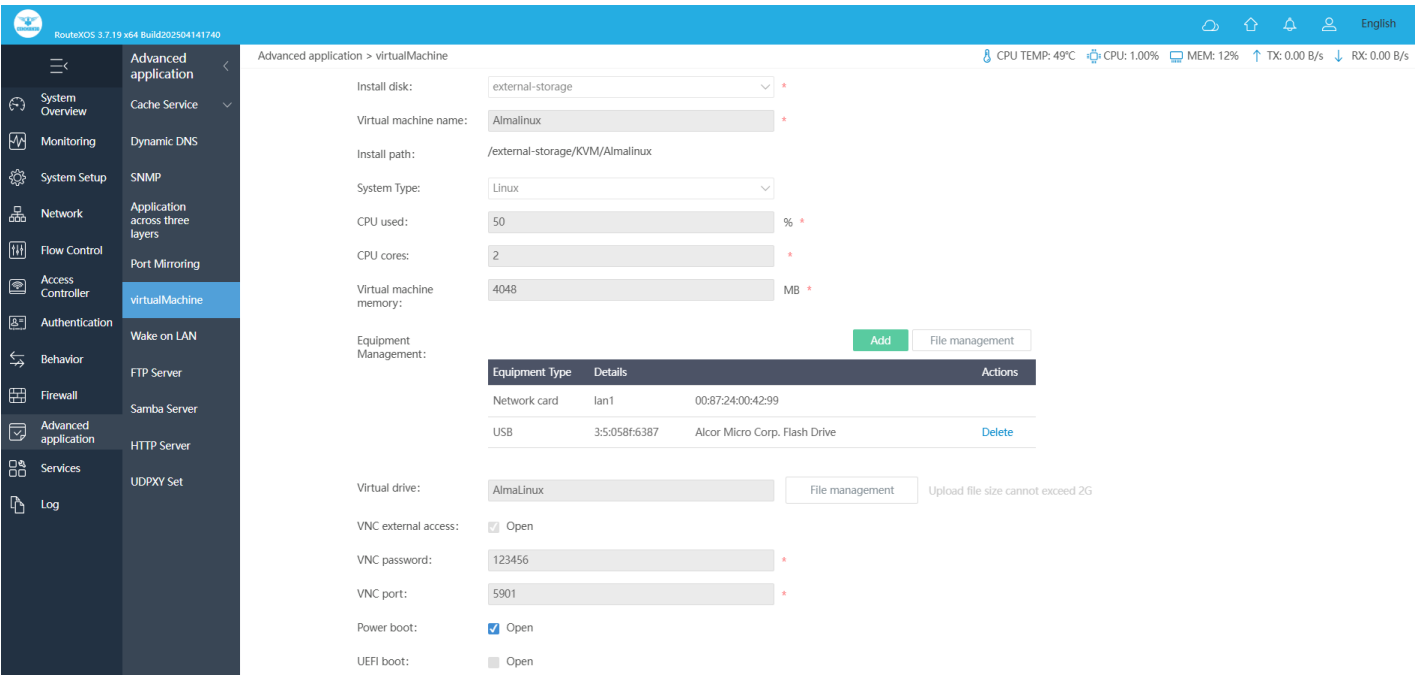


Fig 9.6.2 Add New Virtual Machine page

9.7 Plugin Management

The Plugin Management feature allows users to extend the functionality of the controller by installing, managing, and updating various plugins. Plugins provide additional capabilities such as enhanced security, monitoring, and automation, enabling users to customize the system based on their needs.

The Plugin Management interface offers options to browse available plugins, install or uninstall them, and manage updates. Users can also configure plugin settings to optimize performance and compatibility with the existing system.

To configure Plugin Management settings, Click on Advanced Application > Plugin Management

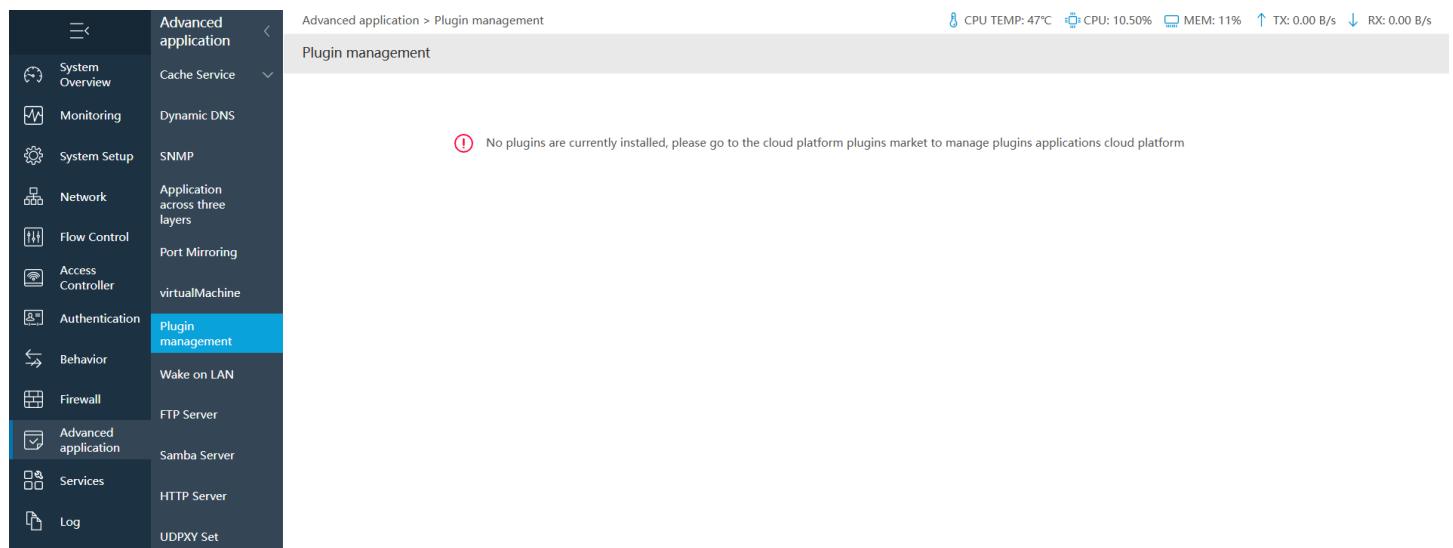


Fig 9.7.1 Default Plugin Management page

9.8 Wake on LAN

This utility allows you to easily turn on one or more computers remotely by sending Wakeon-LAN Settings (WOL) packet to the remote computers for waking computers up from a very low power mode remotely. The WOL feature allows the administrator to remotely power up all sleeping machines so that they can receive updates. WOL sends coded network packets, called magic packets, to systems equipped and enabled to respond to these packets. WOL is based on the principle that when the PC shuts down, the NIC still receives power, and keeps listening on the network for the magic packet to arrive. This magic packet can be sent over connectionless protocols (generally UDP).

To configure Wake-on-LAN Settings, Click on Advanced application > Wake on LAN

The screenshot shows the 'Wake-on-LAN Settings' page in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar contains a menu with 'Advanced application' selected, and 'Wake on LAN' highlighted under the 'Advanced application' section. The main content area is titled 'Wake-on-LAN Settings' and includes a status bar at the top showing system metrics: CPU TEMP: 49°C, CPU: 0.50%, MEM: 12%, TX: 0.00 B/s, and RX: 0.00 B/s. Below the status bar, there are two sections: 'Immediate Wake-up' and 'Regular Wake-up List'. The 'Immediate Wake-up' section has a 'MAC Address' input field and a 'Wakeup' button. The 'Regular Wake-up List' section has buttons for 'Add', 'Import', 'Export', 'Enable', 'Disable', 'Wakeup', and 'Delete'. Below these buttons is a table with columns: MAC Address, Terminal Status, Cycle, Date, Time, Remarks, Planned Task, and Actions. The table is currently empty, showing 'No Data'.

Fig 9.8.1 Default Wake-on-LAN Settings page

The screenshot shows the 'Add' page for configuring Wake-on-LAN settings in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar is the same as in Fig 9.8.1, with 'Wake on LAN' highlighted. The main content area is titled 'Add' and includes a status bar at the top showing system metrics: CPU TEMP: 48°C, CPU: 0.25%, MEM: 12%, TX: 0.00 B/s, and RX: 0.00 B/s. Below the status bar, there are four input fields: 'MAC' (with value 'c4:d9:87:a7:ad:46'), 'Cycle' (with value 'Everyday'), 'Time' (with value '10:00'), and 'Remarks' (with value 'WOL Packets'). There are 'Save' and 'Cancel' buttons at the bottom.

Fig 9.8.2 Add Wake-on-LAN Settings page

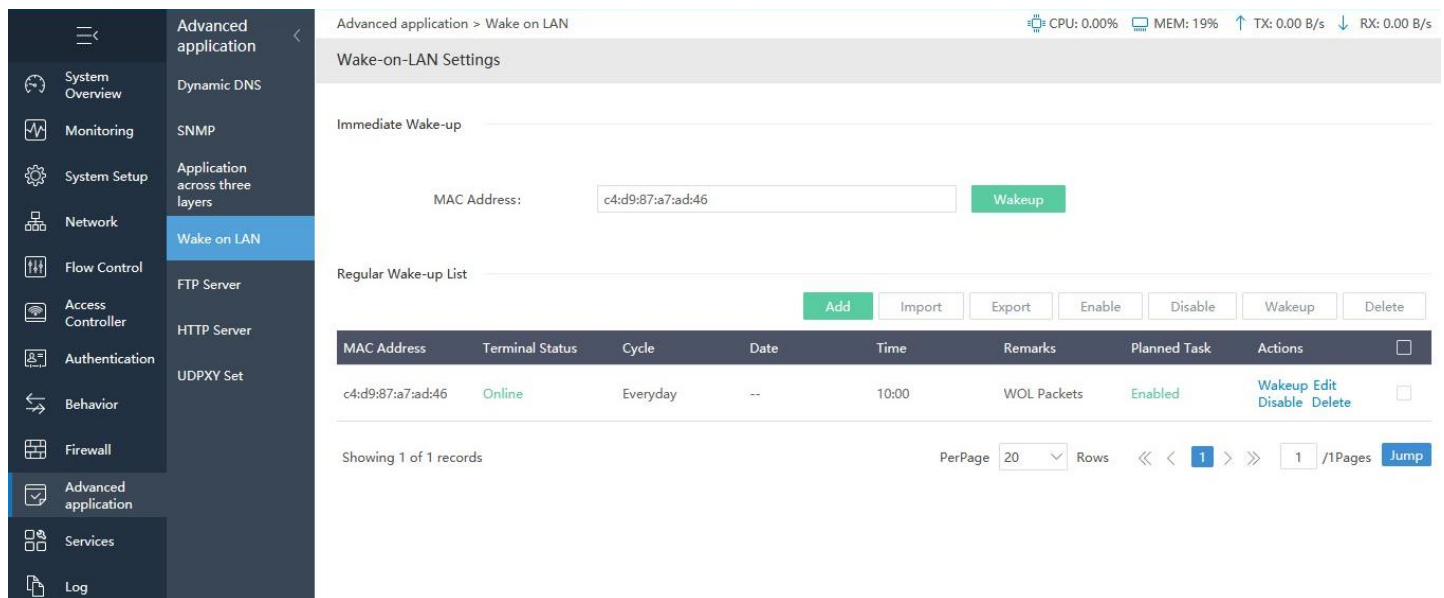


Fig 9.8.3 Wake-on-LAN Settings page

9.9 FTP Server

FTP is a widely used network protocol for transferring files over a TCP/IP-based network, such as the Internet. FTP allows applications exchange and share data within their offices and across the Internet and are useful especially if you are hosting files that will be accessed by remote users on the Internet. FTP servers are the solutions used to facilitate file transfers across the internet. If you send files using FTP, files are either uploaded or downloaded to the FTP server.

To configure FTP Server, Click on Advanced application > FTP Server

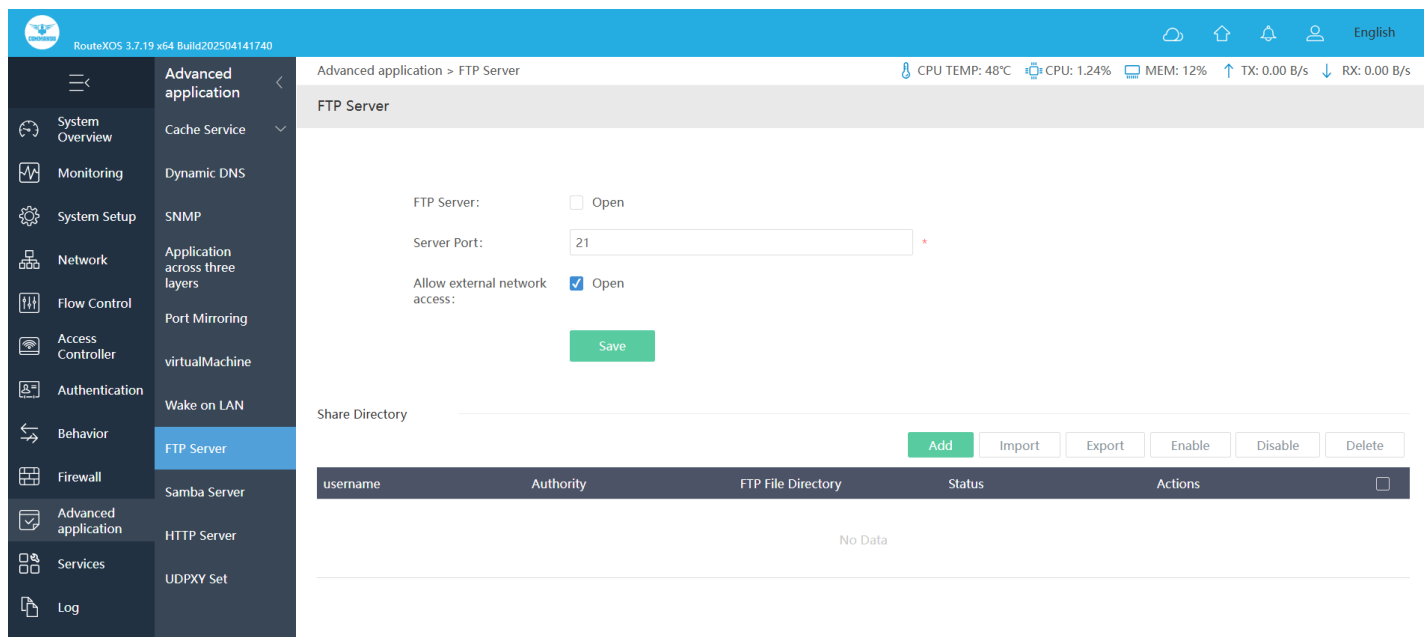


Fig 9.9.1 Default FTP Server page

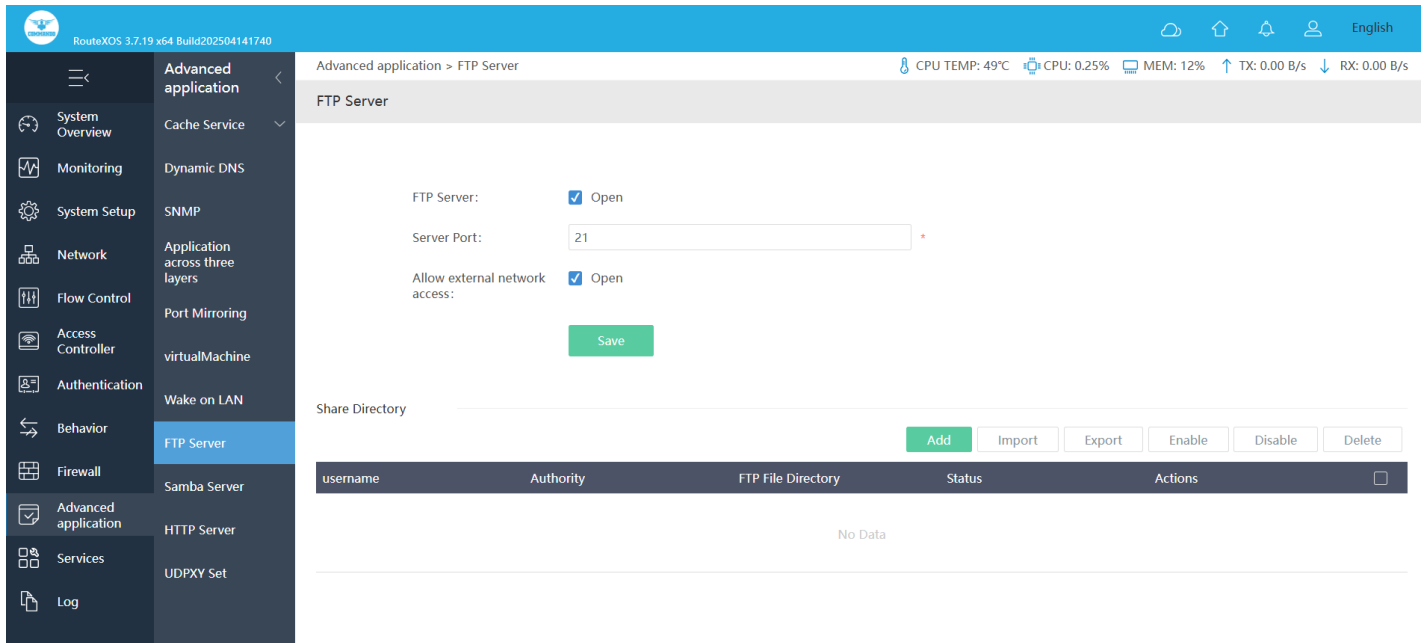


Fig 9.9.2 Enabling FTP Server page

9.10 Samba Server

The Samba Server enables file and printer sharing between different operating systems, allowing seamless integration of Windows, Linux, and macOS devices within the same network. It provides secure and efficient file access, supporting user authentication, shared directories, and access permissions.

The Samba Server interface allows administrators to configure shared folders, set user access controls, and monitor file-sharing activities. It supports multiple authentication methods and integrates with domain controllers for centralized management.

To configure Samba Server settings, Click on Advanced Application > Samba Server

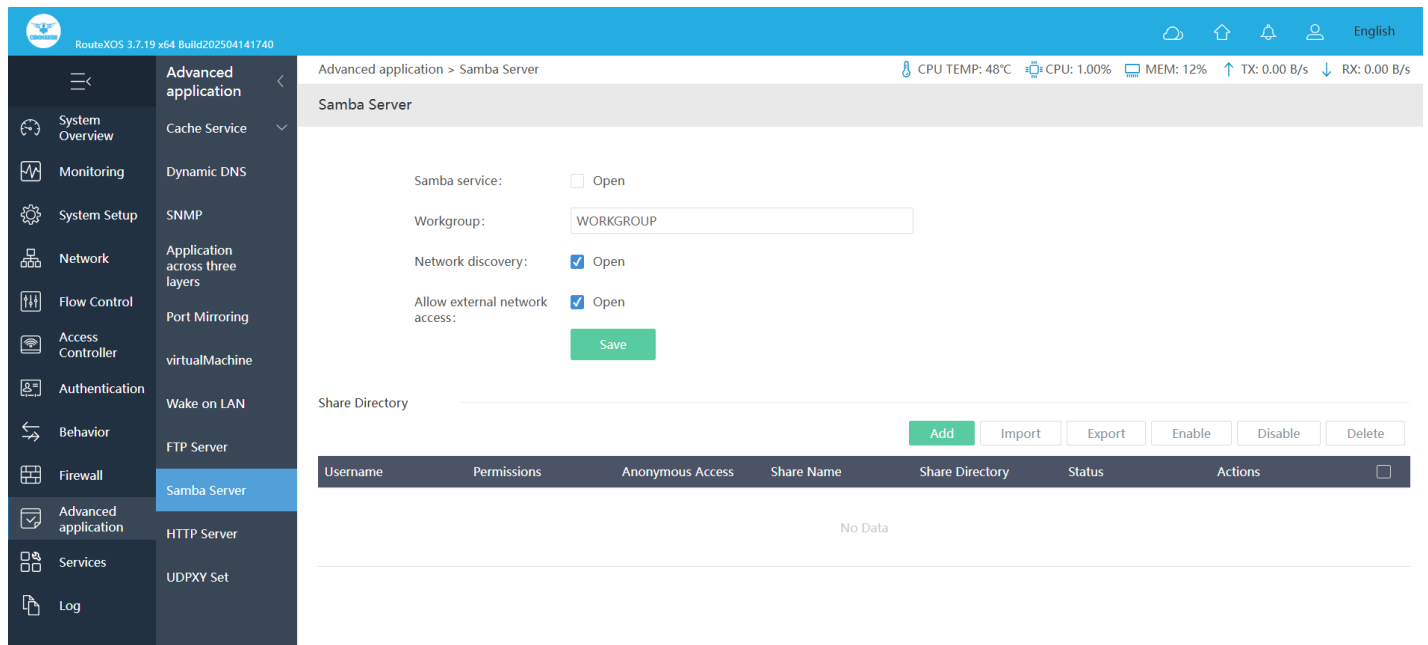


Fig 9.10.1 Default Samba Server page

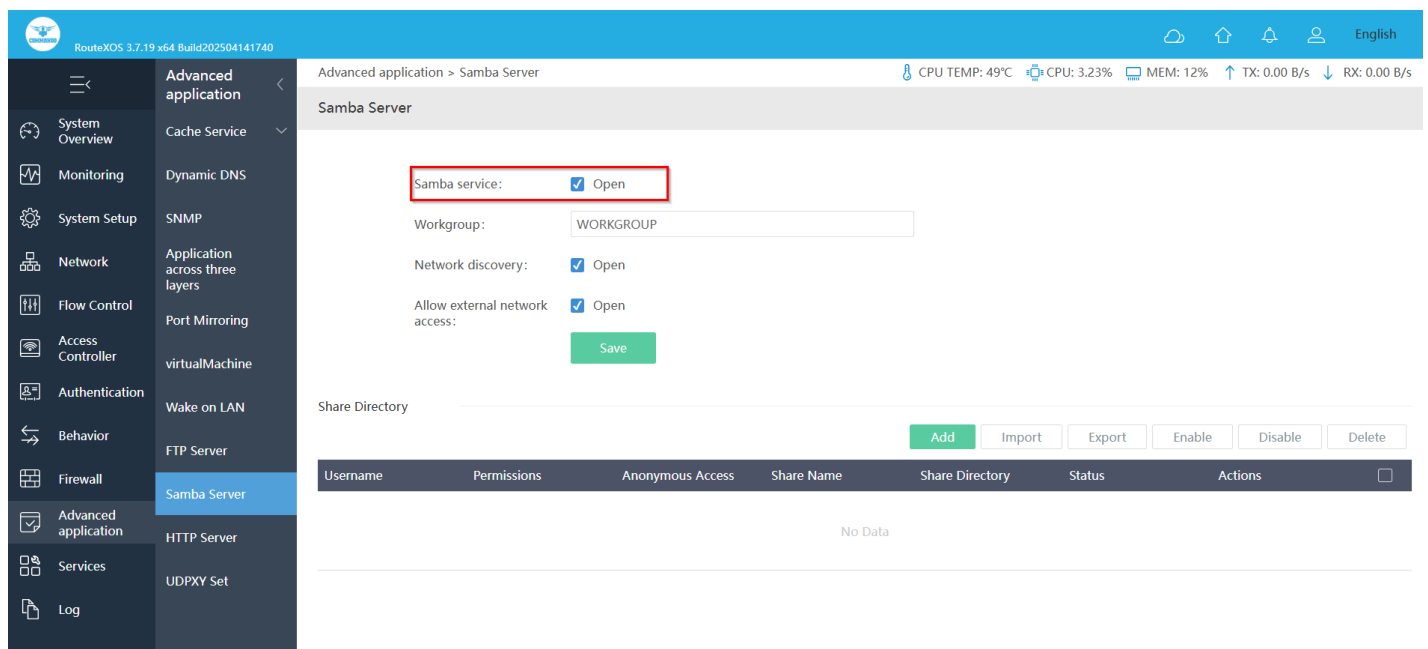


Fig 9.10.2 Enabling Samba Server page

9.11 HTTP Server

An HTTP server is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view web pages). An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device.

To configure HTTP Server, Click on Advanced application > HTTP Server

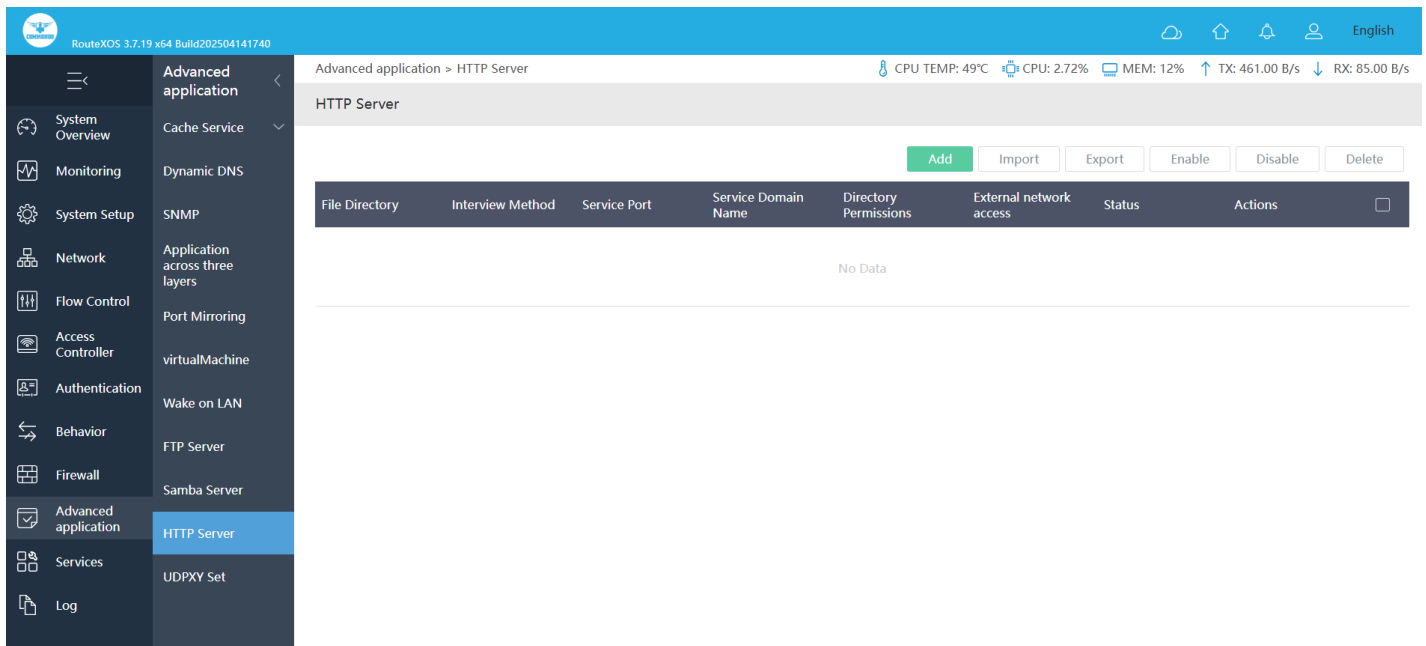


Fig 9.11.1 Default HTTP Server page

9.12 UDPXY Set

UDPXY is a data stream relay which reads data streams from a multicast groups and forwards the data to the requesting clients. UDPXY is designed to serve a small number of clients and is best suited for home usage.

To configure UDPXY Set, Click on Advanced application > UDPXY Set

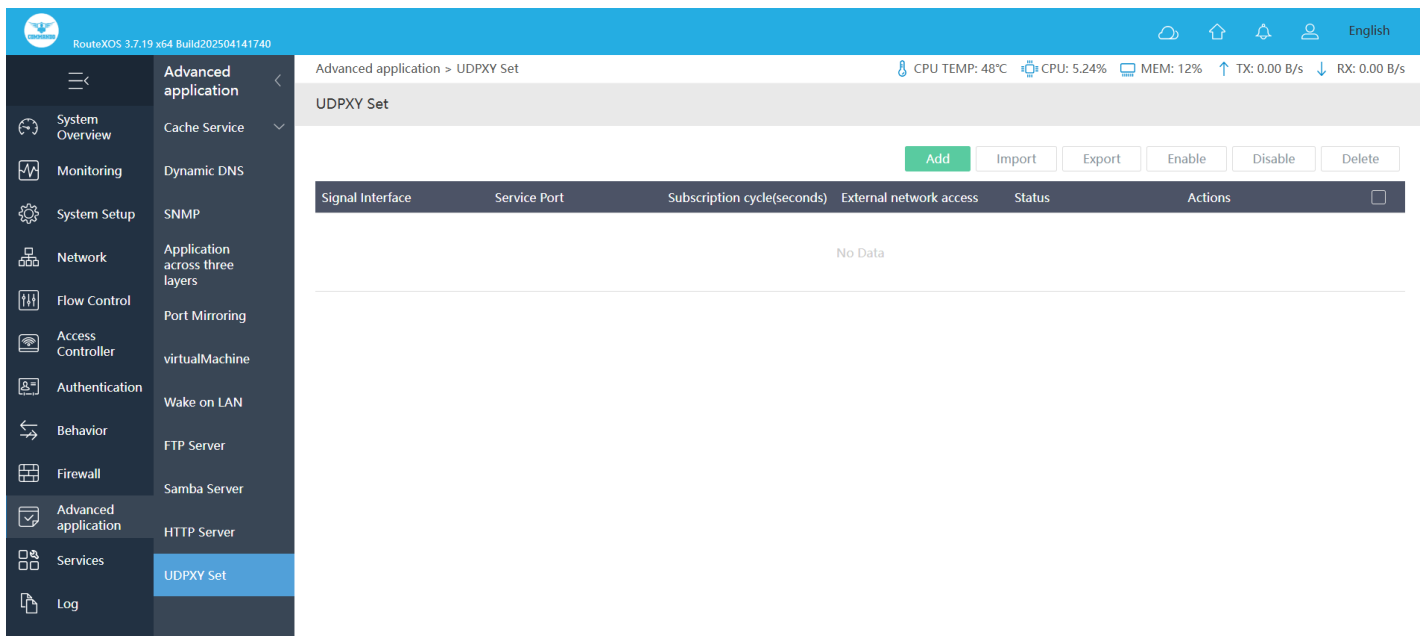


Fig 9.12.1 Default UDPXY Set page

RouteXOS 3.7.19 x64 Build202504141740

English

System Overview

Monitoring

System Setup

Network

Flow Control

Access Controller

Authentication

Behavior

Firewall

Advanced application

Services

Log

Advanced application

Cache Service

Dynamic DNS

SNMP

Application across three layers

Port Mirroring

virtualMachine

Wake on LAN

FTP Server

Samba Server

HTTP Server

UDPROXY Set

Advanced application > UDPROXY Set

CPU TEMP: 49°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

UDPROXY Set

Add

Import

Export

Enable

Disable

Delete

Signal Interface	Service Port	Subscription cycle(seconds)	External network access	Status	Actions	
wan1	215	0	Yes	Enabled	Edit Disable Delete	<input type="checkbox"/>

Showing 1 of 1 records

PerPage 20 Rows << < 1 > >> 1 /1Pages [Jump](#)

Fig 9.12.2 UDPROXY Set page

SERVICES

Ping Test: Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time. Can test Hostname, IP with particular interface with ping Packet Count.

Capture Packet: Capture packet for analysis purpose of particular Interface, IP, Port number and MAC address with packet Number. Agreement Type support TCP, UDP, ICMP, ARP and other protocol types.

Trace Route: Trace route discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the device. The Trace route page shows each hop between the device and a target host, and the round-trip time to each such hop. Trace Hostname or IP address with particular Source Interface, also can define max hops, timeout.

Throughput Test: The Throughput Test measures the data transfer rate between two network nodes by sending test packets and analyzing transmission speed. It can test bandwidth capacity, network efficiency, and potential bottlenecks for a specified interface.

IP Subnetting: IP Subnet Calculator is very handy tool for finding Network Address, Valid address range and total available addresses in each subnet.

Speed Test: Speed Test is to find minimum, average, maximum transmission and receiving rate on particular Interface.

Diagnostics: Diagnostics offer proactive diagnostics of Device all Interfaces, DHCP server, PPPoE, Gateway and cloud platform. You can observe the diagnostic information to easily locate and rectify fault occurred and can provide easy troubleshooting and support to network infrastructure.

Watchdog: Health Watchdog for physical hardware Active health detection.

10.1 Ping Test

PING the Packet Internet Groper is used to test whether a particular host is reachable across an IP network. and measures the time it takes for round-trip of the packet and any losses along the way. The ping operation monitors link connectivity and host reachability on a network. In a ping operation, the source sends an Internet Control Message Protocol (ICMP) Request message to the destination and the destination returns an ICMP Response message to the source.

For PING Test, Click on Services > Ping Test

The screenshot shows the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar contains a menu with options: System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Services' menu is expanded, showing 'Ping Test' as the selected option. The main panel is titled 'Services > Ping Test' and 'PING Test'. It contains the following fields: Host (www.google.com), Protocol Stack (IPv4), Protocol Type (ICMP), Specifying the source interface (Auto), Ping Packet Count (10), and a Result field. A green 'Start' button is located below the fields. The top status bar shows CPU TEMP: 49°C, CPU: 0.25%, MEM: 12%, TX: 0.00 B/s, and RX: 0.00 B/s.

Fig 10.1.1 Default PING Test page

The screenshot shows the RouteXOS 3.7.19 x64 Build202504141740 interface after a ping test. The left sidebar is the same as in the previous screenshot. The main panel is titled 'Services > Ping Test' and 'PING Test'. The fields are: Host (www.google.com), Protocol Stack (IPv4), Protocol Type (ICMP), Specifying the source interface (Auto), Ping Packet Count (3), and a Result field. The Result field contains the following text: PING www.google.com (172.217.174.68) 56(84) bytes of data. 32 bytes from 172.217.174.68: icmp_req=1 ttl=120 time=2.37 ms 32 bytes from 172.217.174.68: icmp_req=2 ttl=120 time=6.76 ms 32 bytes from 172.217.174.68: icmp_req=3 ttl=120 time=2.18 ms --- www.google.com ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2s. A green 'Start' button is located below the fields. The top status bar shows CPU TEMP: 49°C, CPU: 0.50%, MEM: 12%, TX: 39.00 B/s, and RX: 88.00 B/s.

Fig 10.1.2 PING to particular website page

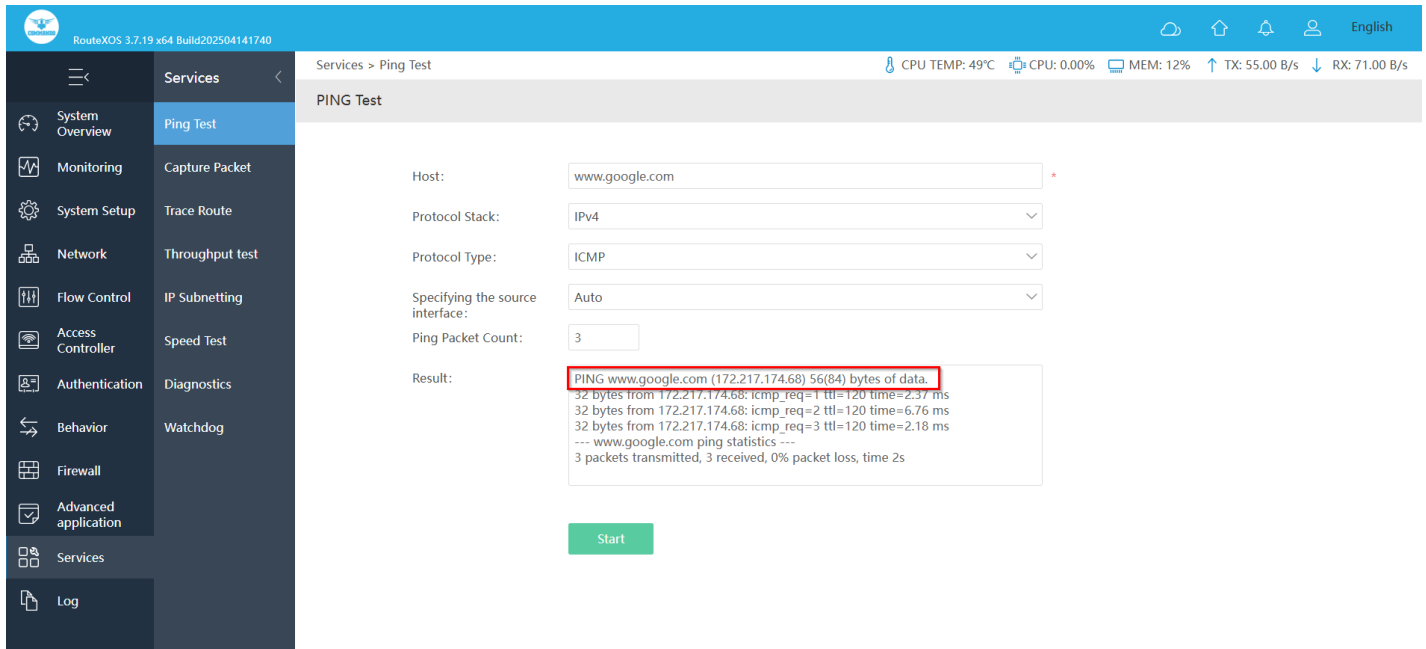


Fig 10.1.3 PING to particular IP address page

10.2 Capture Packet

Packet Capture is a networking term for intercepting a data packet that is crossing a specific point in a data network. Once a packet is captured in real-time, it is stored for a period of time so that it can be analyzed, and then either be downloaded, archived or discarded. The biggest advantage of packet capturing is that it grants visibility. You can use packet data to pinpoint the root cause of network problems. You can monitor traffic sources and identify the usage data of applications and devices. Packet capture technology captures packets from devices and provides a way to locate network problems

To Capture Packet, Click on Services > Capture Packet

RouteXOS 3.7.19 x64 Build202504141740

Services > Capture Packet

CPU TEMP: 45°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Capture Packet

Capture Interface:

IP:

Port:

MAC:

Agreement Type: Support tcp, udp, icmp, arp and other protocol types

Storage location:

packet Number: * Range: 1-80000

[Start Packet](#)

Fig 10.2.1 Default Capture Packet page

RouteXOS 3.7.19 x64 Build202504141740

Services > Capture Packet

CPU TEMP: 45°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Capture Interface:

IP:

Port:

MAC:

Agreement Type: Support tcp, udp, icmp, arp and other protocol types

Storage location:

packet Number: * Range: 1-80000

[Start Packet](#)

Capture Results

file Time: 2025-08-02 11:52:40

file Size: 24 B

Used Memory: 24 B

[Download Document](#) [Delete](#)

Fig 10.2.2 Capture Packet result page

10.3 Trace Route

Trace Route is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the Gateways it pinged in between. Trace Route also records the time taken for each hop the packet makes during its route to the destination. The trace route command can be used to identify the path used by a packet to reach its target. It identifies all the Gateways in the

path from the source host to destination host and it can be useful when troubleshooting network problems.

For Trace Route, Click on Services > Trace Route

RouteXOS 3.7.19 x64 Build202504141740

Services > Trace Route

CPU TEMP: 47°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Trace Route

Host:

Source Interface:

Max Hops:

Timeout:

Result:

Fig 10.3.1 Default Trace Route page

RouteXOS 3.7.19 x64 Build202504141740

Services > Trace Route

CPU TEMP: 47°C CPU: 0.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Trace Route

Host:

Source Interface:

Max Hops:

Timeout:

Result:

```
tracert to www.google.com (172.217.174.68), 5 hops max, 46 byte packets
1 192.168.1.1 (192.168.1.1) 0.539 ms 0.426 ms 0.402 ms
2 * * *
3 72.14.208.165 (72.14.208.165) 2.066 ms 2.406 ms 7.740 ms
4 192.178.111.151 (192.178.111.151) 3.085 ms 2.503 ms 2.135 ms
5 142.250.228.49 (142.250.228.49) 3.701 ms 3.200 ms 2.999 ms
```

Fig 10.3.2 Trace Route particular website page

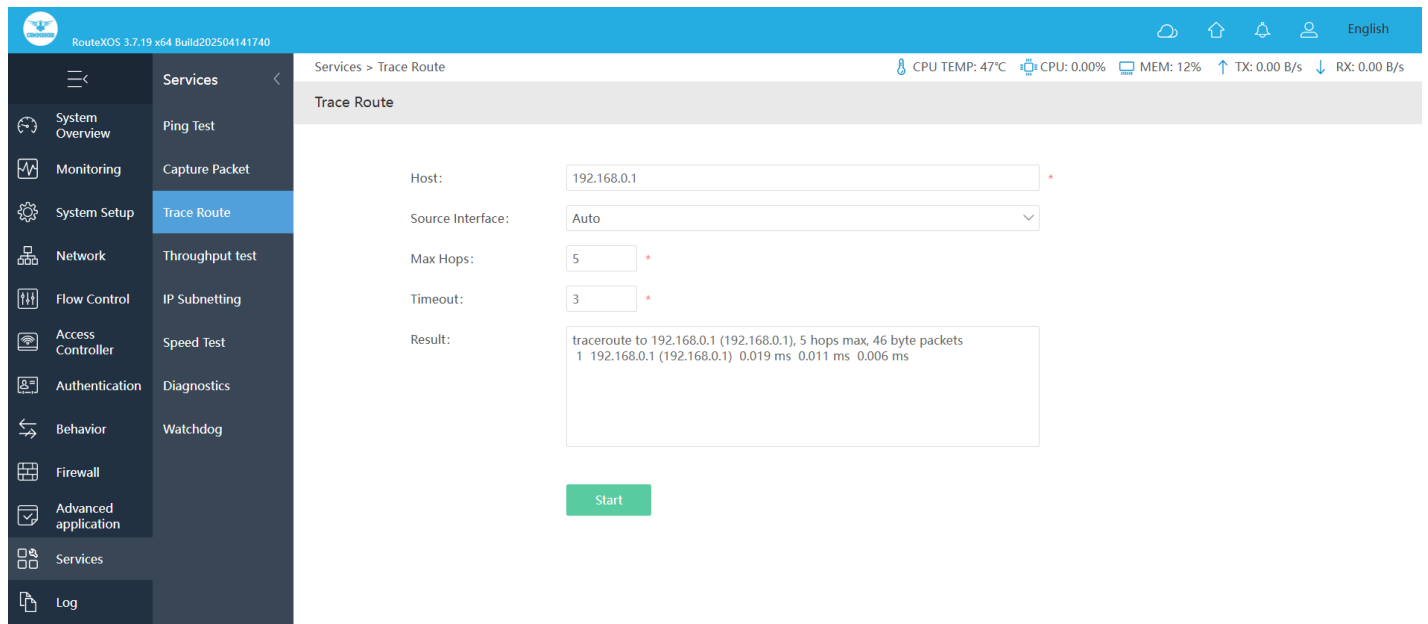


Fig 10.3.3 Trace Route particular IP address page

10.4 Throughput Test

The Throughput Test measures the data transfer rate between two network points, helping assess network performance and bandwidth capacity. It evaluates the maximum achievable speed by sending test data and analyzing transmission efficiency, latency, and potential bottlenecks.

For Throughput Test, click on Services > Throughput Test.

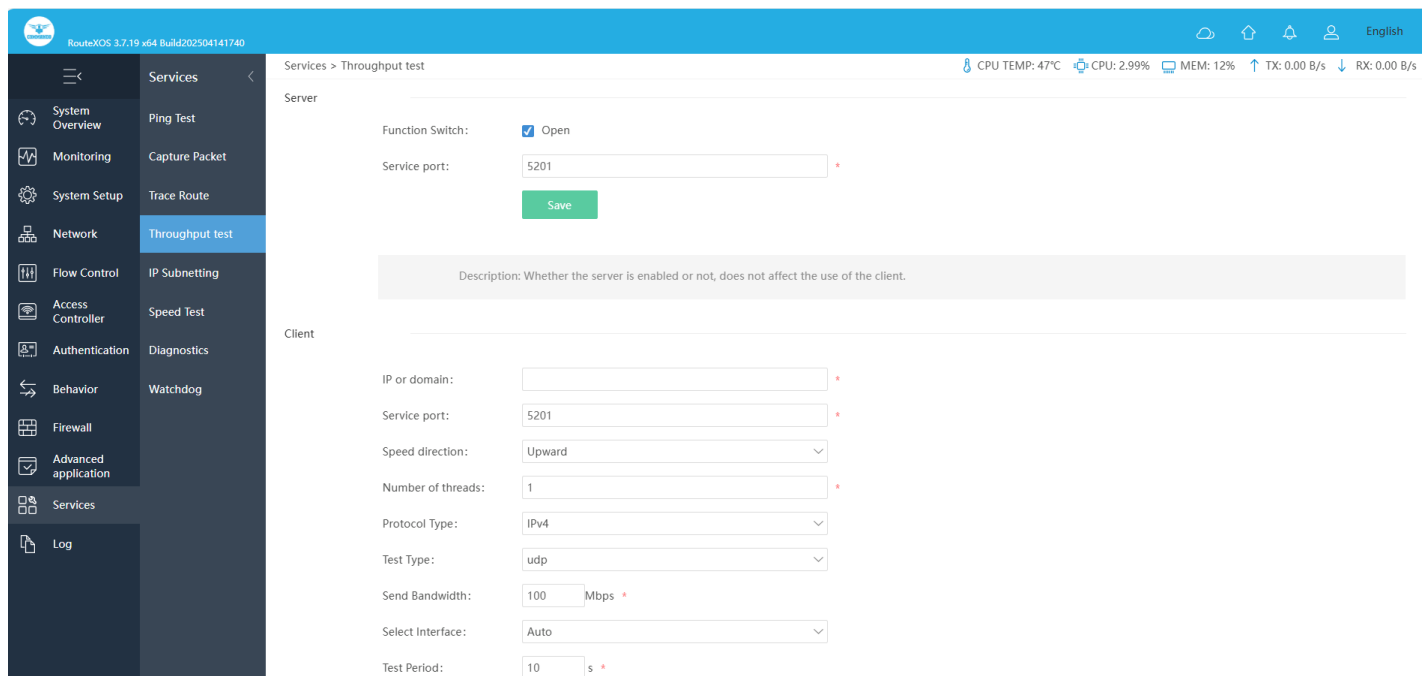


Fig 10.4.1 Default Throughput test page

The screenshot shows the 'Throughput test' configuration page. The left sidebar contains a menu with options: System Overview, Monitoring, System Setup, Network (selected), Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Services' section is expanded, showing 'Throughput test' as the active option. The main content area is titled 'Services > Throughput test'. At the top, system status is displayed: CPU TEMP: 48°C, CPU: 0.00%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s. The 'Server' section has a 'Function Switch' set to 'Open' (highlighted with a red box), a 'Service port' of 5201, and a 'Save' button. Below this is a description: 'Whether the server is enabled or not, does not affect the use of the client.' The 'Client' section contains fields for 'IP or domain', 'Service port' (5201), 'Speed direction' (Upward), 'Number of threads' (1), and 'Protocol Type' (IPv4).

Fig 10.4.2 Start Throughput test server settings page

The screenshot shows the 'Start Throughput test' configuration page. The left sidebar is identical to the previous figure. The main content area is titled 'Services > Throughput test'. System status at the top shows: CPU TEMP: 47°C, CPU: 3.23%, MEM: 12%, TX: 0.00 B/s, RX: 0.00 B/s. The 'Client' section is active, showing fields for 'IP or domain' (192.168.0.1), 'Service port' (5201), 'Speed direction' (Upward), 'Number of threads' (1), 'Protocol Type' (IPv4), 'Test Type' (udp), 'Send Bandwidth' (100 Mbps), 'Select Interface' (Auto), 'Test Period' (10 s), and 'Interval time' (1 s). A 'Test result' section displays a log of test data:

[ID]	Interval	Transfer	Bitrate	Total Datagrams
[6]	0.00-1.00 sec	11.9 MBytes	100 Mb/s	382
[6]	1.00-2.00 sec	11.9 MBytes	99.9 Mb/s	381
[6]	2.00-3.00 sec	11.9 MBytes	100 Mb/s	382
[6]	3.00-4.00 sec	11.9 MBytes	99.9 Mb/s	381
[6]	4.00-5.00 sec	11.9 MBytes	99.9 Mb/s	381
[6]	5.00-6.00 sec	11.9 MBytes	100 Mb/s	382
[6]	6.00-7.00 sec	11.9 MBytes	99.9 Mb/s	381
[6]	7.00-8.00 sec	11.9 MBytes	100 Mb/s	382

Fig 10.4.3 Start Throughput test client settings page

10.5 IP Subnetting

IP Subnetting is a logical subdivision of an IP network. Subnet calculator performs network calculations using IP address, mask bits, performs network calculations using IP address, mask bits and determines the resulting Network Address, Subnet Mask, Address Range and available addresses. Subnetting ensures that traffic destined for a device

within a subnet stays in that subnet, which reduces congestion. Through strategic placement of subnets, you can help reduce your network's load and more efficiently route traffic.

For Subnet Calculator, Click on Services > IP Subnetting

The screenshot shows the 'Subnet Calculator' page in the RouteXOS 3.7.19 x64 Build202504141740 interface. The left sidebar contains a menu with 'Services' selected. The main content area is titled 'Subnet Calculator' and features several input fields: 'IP Format' (set to 'IP Segment'), 'IP Segment' (with a red asterisk), 'Network Address', 'Subnet Mask', 'Address Range', 'Available Addresses', and 'Random Address'. A blue 'Calculate' button is positioned below the 'IP Segment' field. The top status bar displays system metrics: CPU TEMP: 47°C, CPU: 0.50%, MEM: 12%, TX: 0.00 B/s, and RX: 0.00 B/s.

Fig 10.5.1 Default Subnet Calculator page

This screenshot shows the 'Subnet Calculator' page after entering an IP segment. The 'IP Segment' field now contains '192.168.100.0 / 27'. The 'Calculate' button has been clicked, and the output fields are populated: 'Network Address' is '192.168.100.0', 'Subnet Mask' is '255.255.255.224', 'Address Range' is '192.168.100.1 - 192.168.100.30', 'Available Addresses' is '30', and 'Random Address' is '192.168.100.15'. The interface remains the same as in Fig 10.5.1, with the same sidebar and top status bar.

Fig 10.5.2 IP Segment Subnet Calculator page

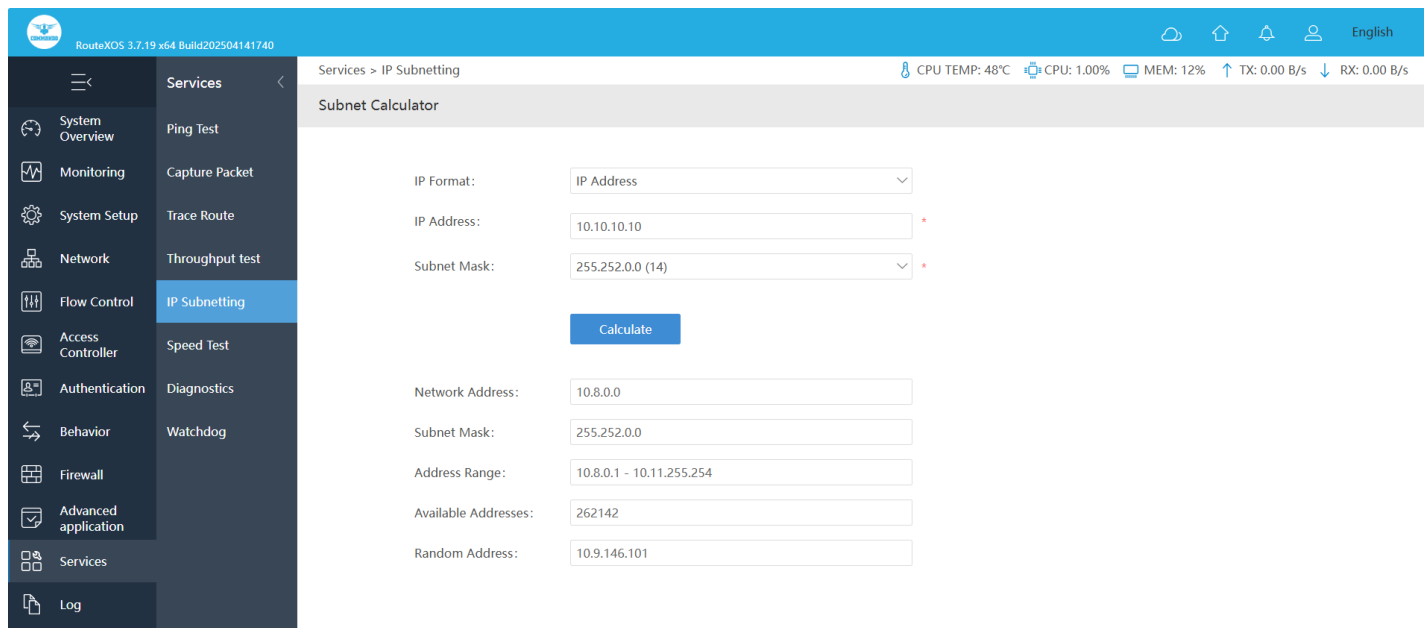


Fig 10.5.3 IP address Subnet Calculator page

10.6 Speed Test

Speed Test is to find minimum, average, maximum transmission and receiving rate on particular Interface. Speed Test provides advanced diagnostics of the performance of your internet connection through quick measurements.

For Speed Test, Click on Services > Speed Test

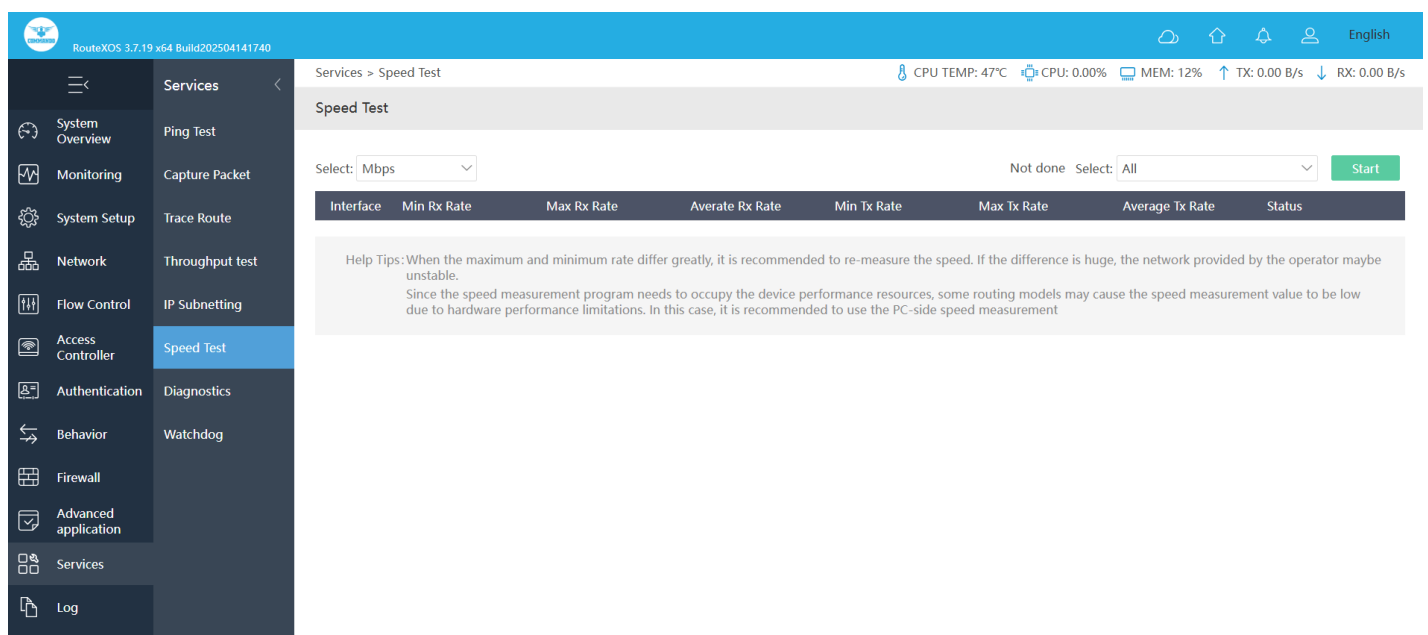


Fig 10.6.1 Default Speed Test page

RouteXOS 3.7.19 x64 Build202504141740

Services > Speed Test

CPU TEMP: 47°C CPU: 0.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Speed Test

Select: Mbps Last tested time is : 2025-08-02 12:32:42 Select: All Start

Interface	Min Rx Rate	Max Rx Rate	Average Rx Rate	Min Tx Rate	Max Tx Rate	Average Tx Rate	Status
wan1	22.15 Mbps	43.62 Mbps	32.66 Mbps	31.23 Mbps	45.36 Mbps	37.23 Mbps	speedtest

Help Tips: When the maximum and minimum rate differ greatly, it is recommended to re-measure the speed. If the difference is huge, the network provided by the operator may be unstable. Since the speed measurement program needs to occupy the device performance resources, some routing models may cause the speed measurement value to be low due to hardware performance limitations. In this case, it is recommended to use the PC-side speed measurement

Fig 10.6.2 Speed Test page

10.7 Diagnostics

Diagnostics offer proactive diagnostics of Device all Interfaces, DHCP server, PPPoE, Gateway and cloud platform. You can observe the diagnostic information to easily locate and rectify fault occurred and can provide easy troubleshooting and support to network infrastructure. It can quickly and conveniently detect the fault and allows to run diagnostic checks of network. Diagnostics offer proactive diagnostics and real-time alerts and provides higher network availability and increased operational efficiency.

For Device Diagnostic, Click on Services > Diagnostics

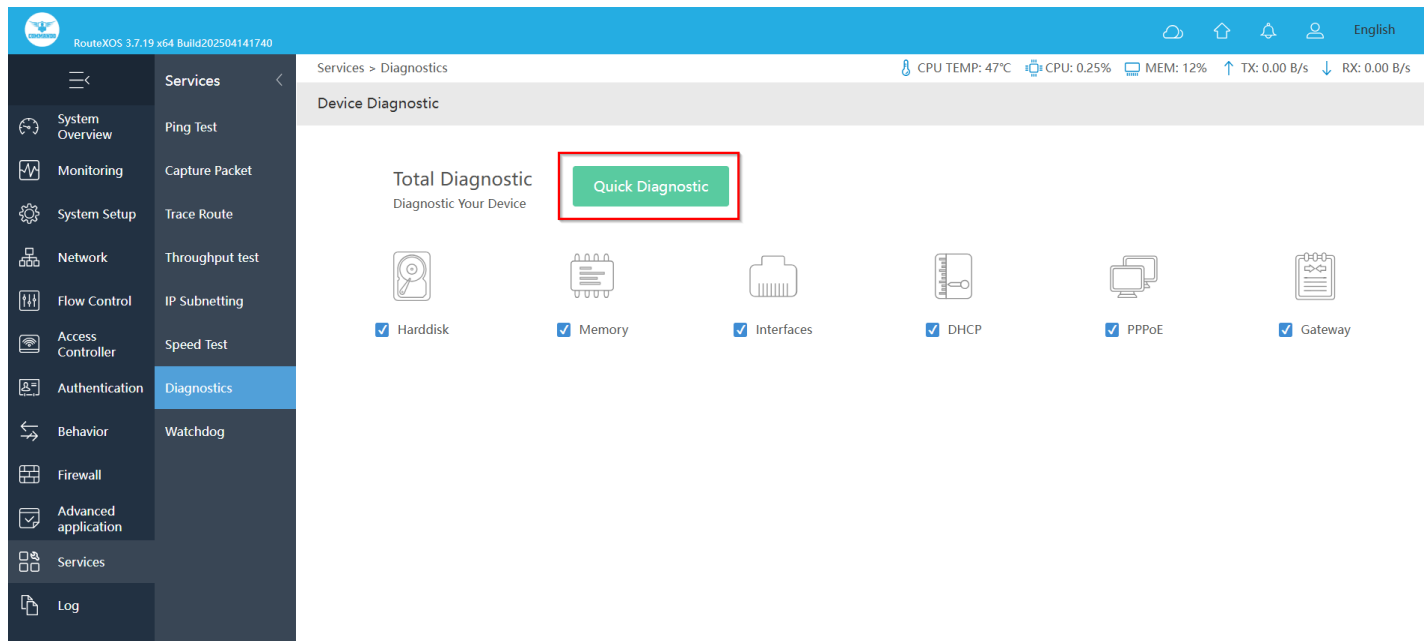


Fig 10.7.1 Default Device Diagnostic page

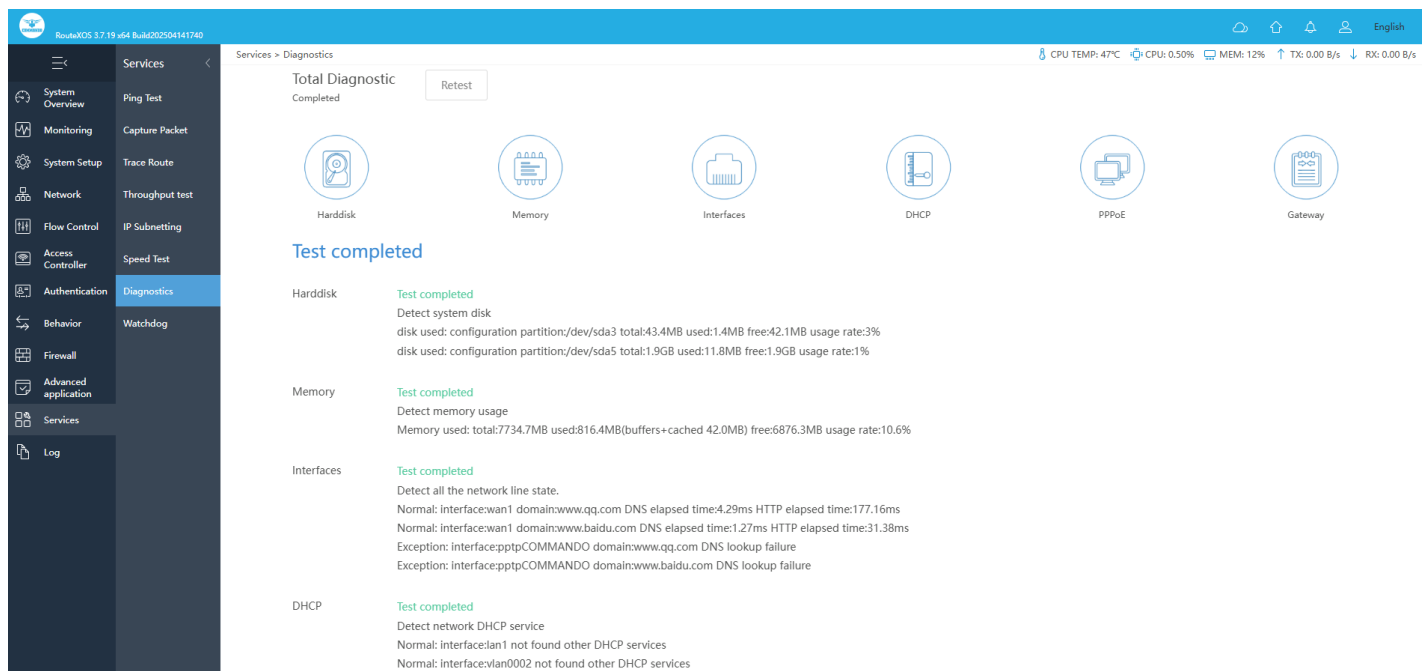


Fig 10.7.2 Device Diagnostic page

10.8 Watchdog

A watchdog timer is a simple countdown timer which is used to reset a microprocessor after a specific interval of time. COMMANDO processors have timers that guard against certain types of system hangs. The CPU periodically resets a watchdog timer. The watchdog timer basically controls the maximum time of each process. If a process is

longer than set timer then it should be reset. The watchdog timer is used to escape from hanged process.

For setting Health Watchdog, Click on Services > Watchdog

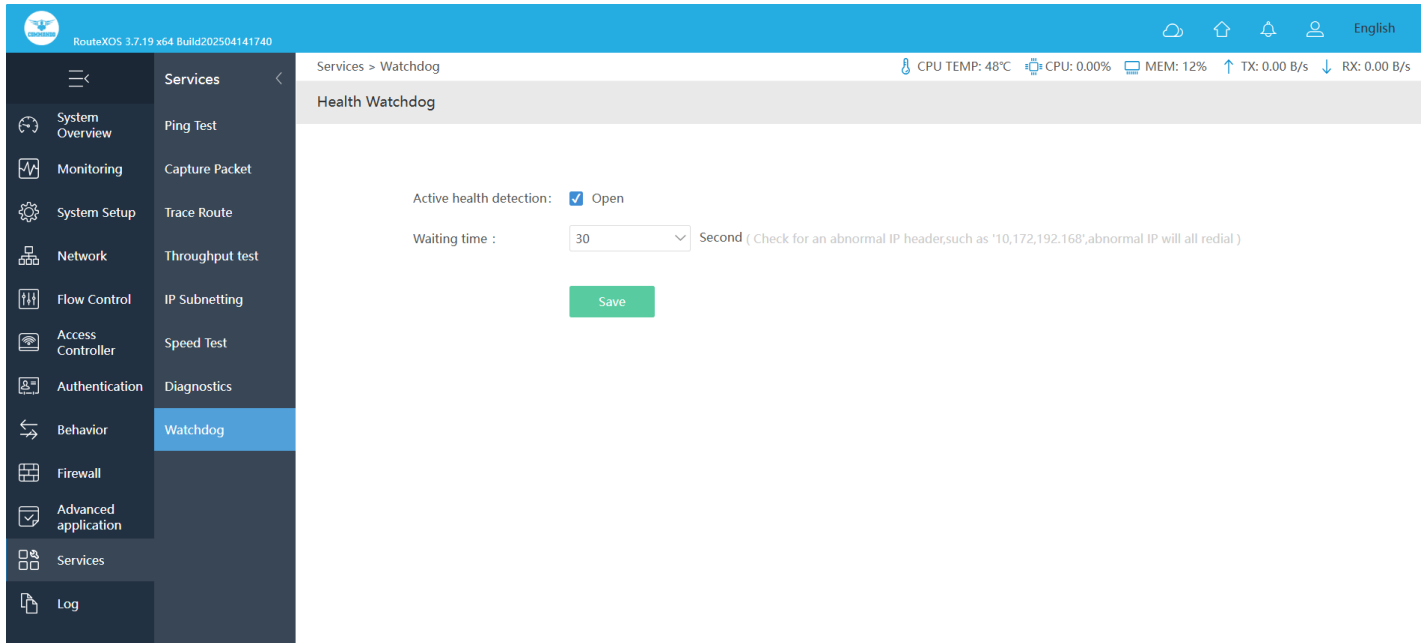


Fig 10.8.1 Default Health Watchdog page

LOG

The Logs can record system information effectively. The logs allow thorough tracking, alerting, and analysis when something does go wrong. It also determines the root cause of any issue.

Logs: This is for viewing Auth Logs, ARP Logs, Terminal Logs.

Function Logs: This is for viewing DHCP Logs, DDNS Logs, VPN Logs, Notification Logs.

System Logs: This is for viewing System Logs, Action Logs, Notification.

11.1 User Logs

User Logs feature allows to record and monitor the activities Authentication, ARP, and Terminal connection

Auth Logs: The Authorization Log tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords.

For Auth Logs, Click on Log > User Logs > Auth Logs

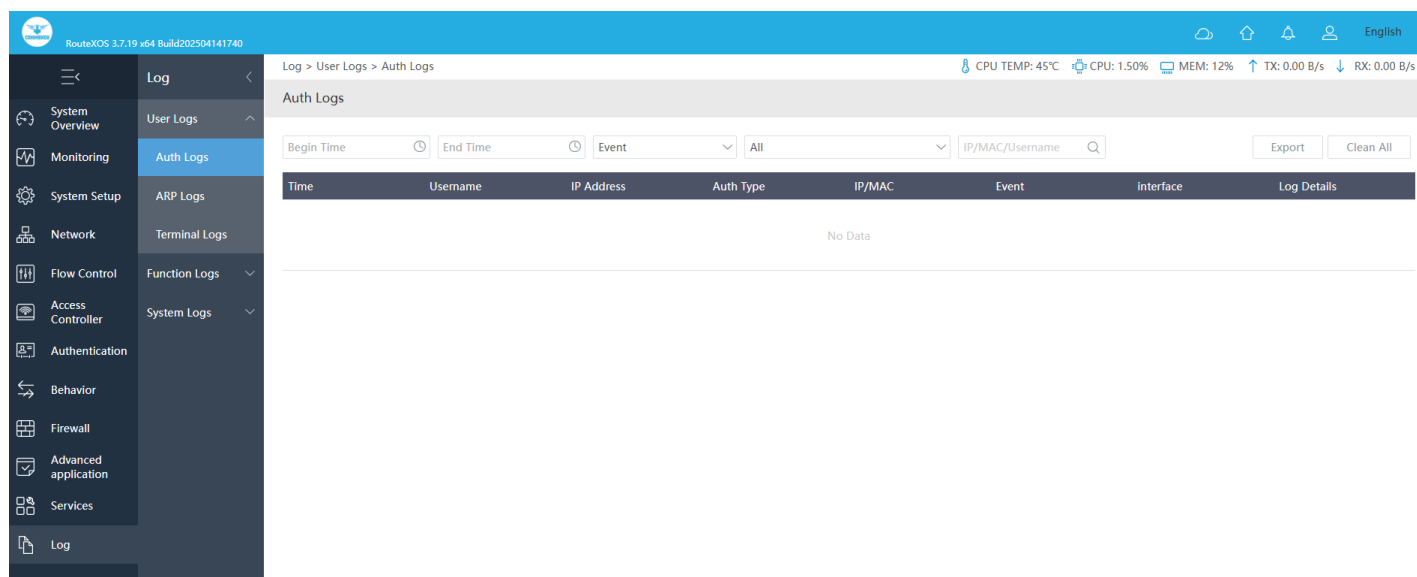


Fig 11.1.1 Default Auth Logs page

ARP Logs: Address Resolution Protocol (ARP) Logs are used to view map of layer-3 network addresses to data-link addresses.

For ARP Logs, Click on Log > User Logs > ARP Logs

RouteXOS 3.7.19 x64 Build202504141740

Log > User Logs > ARP Logs

CPU TEMP: 48°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

ARP Logs

Begin Time End Time Event

Export Clean All

Time	Event
2025-04-09 12:33:14	detection one arp deceive at interface(qtap1_lan1_1): 192.168.111.100 54:ee:75:59:52:19->00:87:24:00:42:99
2025-04-08 21:00:27	detection one arp deceive at interface(qtap1_lan1_1): 192.168.111.100 54:ee:75:59:52:19->00:87:24:00:42:99
2025-04-08 20:26:18	detection one arp deceive at interface(qtap1_lan1_1): 192.168.111.100 54:ee:75:59:52:19->00:87:24:00:42:99

Showing 1-3 of 3 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Fig 11.1.2 Default ARP Logs page Terminal

Logs: Terminal Logs you can monitor, MAC Address, AP, SSID, Signal Strength and Event type.

For Terminal Logs, Click on Log > User Logs > Terminal Logs

RouteXOS 3.7.19 x64 Build202504141740

Log > User Logs > Terminal Logs

CPU TEMP: 47°C CPU: 14.50% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Terminal Logs

Begin Time End Time All IP/MAC/remark

Export Clean All

Time	MAC Address	MAC notes	AP	AP notes	BSSID	SSID	Signal Strength	Event type	Action
2025-07-30 12:10:25	82:aa:71:a4:cd:99	--	82:02:fa:60:0e:26	--	82:02:fa:60:0e:27	2G:Router 01_2G	-49dBm	drop out	Success
2025-07-30 12:10:06	82:aa:71:a4:cd:99	--	82:02:fa:60:0e:26	--	82:02:fa:60:0e:27	2G:Router 01_2G	-48dBm	login successful	Success

Showing 1-2 of 2 records

PerPage 20 Rows << < 1 > >> 1 /1Pages Jump

Note: This feature supports only AP version 1.1.2 and above

Fig 11.1.3 Default Terminal Logs page

11.2 Function Logs

You Can monitor function Logs like DHCP Logs, DDNS Logs and VPN Logs.

DHCP Logs: DHCP logs contains MAC address, associated IP, message type and connected interface which can be crucial for identifying connected user. Monitoring and alerting to unknown and unrecognized users are also important for most of organizations.

To monitor DHCP Logs, Click on Log > Function Logs > DHCP Logs

RouteXOS 3.7.19 x64 Build202504141740

Log > Function Logs > DHCP Logs

CPU TEMP: 47°C CPU: 0.75% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

DHCP Logs

Begin Time End Time IP/MAC Export Clean All

Time	msgtype	interface	MAC/IPv6 Addr	IP	event
2025-08-02 12:24:34	DHCPACK	lan1	a0:8cfd:a5:68:9d	192.168.0.10	--
2025-08-02 12:24:34	DHCPINFORM	lan1	a0:8cfd:a5:68:9d	192.168.0.10	--
2025-08-02 11:03:39	DHCPACK	lan1	00:87:24:00:42:99	192.168.0.11	--
2025-08-02 11:03:39	DHCPREQUEST	lan1	00:87:24:00:42:99	192.168.0.11	--
2025-08-02 11:03:37	DHCPOFFER	lan1	00:87:24:00:42:99	192.168.0.11	--
2025-08-02 11:03:37	DHCPDISCOVER	lan1	00:87:24:00:42:99	--	--
2025-08-02 11:03:35	DHCPOFFER	lan1	00:87:24:00:42:99	192.168.0.11	--
2025-08-02 11:03:35	DHCPDISCOVER	lan1	00:87:24:00:42:99	--	--
2025-08-01 12:14:45	DHCPNAK	lan1	a0:8cfd:a5:68:9d	192.168.0.10	not found old address at leases
2025-08-01 12:14:45	DHCPINFORM	lan1	a0:8cfd:a5:68:9d	192.168.0.10	--
2025-08-01 12:05:21	DHCPACK	lan1	00:87:24:00:42:99	192.168.0.11	--
2025-08-01 12:05:21	DHCPREQUEST	lan1	00:87:24:00:42:99	192.168.0.11	--

Fig 11.2.1 Default DHCP Logs page

Time	Interface	Action	Status	Error
2025-08-02 12:15:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 12:10:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 12:05:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 12:00:02	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:55:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:50:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:45:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:40:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:35:02	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:30:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:25:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:20:02	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:15:01	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:10:02	--	www.commandonetworks.com	Auto	fail
2025-08-02 11:05:01	--	www.commandonetworks.com	Auto	fail

Fig 11.2.4 DDNS Logs page

VPN Logs: VPN logs are the data that providers keep regarding usage of their service. When it comes to what they could store, you have to remember that your provider has access to all of your internet activities. The logs that indicate all connection and authentication attempts are crucial for the security of a VPN setup, as the VPN endpoint is exposed to attackers.

For VPN Logs, Click on Log > Function Logs > VPN Logs

Time	Interface	Log Details
No Data		

Fig 11.2.5 Default VPN Logs page

Time	Interface	Log Details
2025-08-02 12:42:59	pptpCOMMANDO	Call manager exited with error 256
2025-08-02 12:42:59	pptpCOMMANDO	Exit.
2025-08-02 12:42:59	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2025-08-02 12:42:59	pptpCOMMANDO	connect: Connection timed out
2025-08-02 12:40:39	pptpCOMMANDO	Call manager exited with error 256
2025-08-02 12:40:39	pptpCOMMANDO	Exit.
2025-08-02 12:40:39	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2025-08-02 12:40:39	pptpCOMMANDO	connect: Connection timed out
2025-08-02 12:38:20	pptpCOMMANDO	Call manager exited with error 256
2025-08-02 12:38:20	pptpCOMMANDO	Exit.
2025-08-02 12:38:20	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2025-08-02 12:38:20	pptpCOMMANDO	connect: Connection timed out
2025-08-02 12:36:01	pptpCOMMANDO	Call manager exited with error 256
2025-08-02 12:36:01	pptpCOMMANDO	Exit.

Fig 11.2.6 VPN Logs page Notification

Logs: It shows Severity Normal but significant conditions.

For Notification Logs, Log > Function Logs > Notification Logs.

Time	IP Address	Event	Type
No Data			

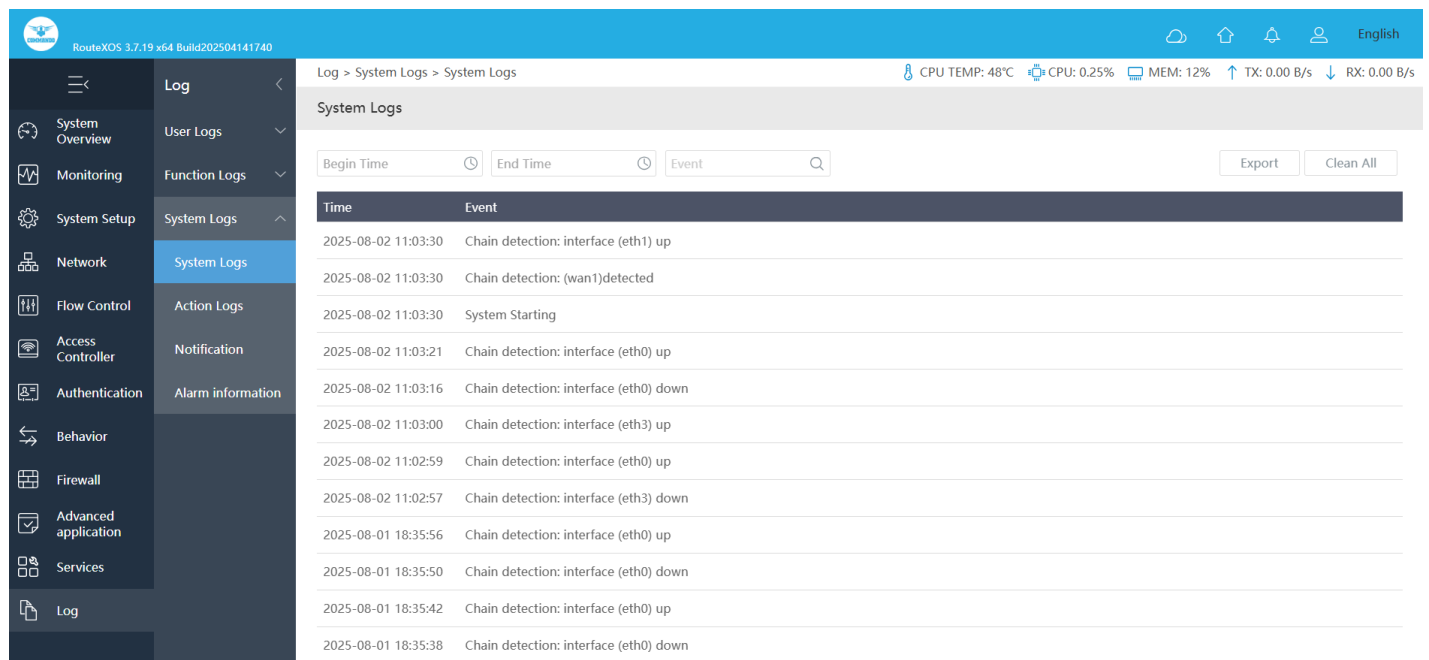
Fig 11.2.7 Default Notification Logs page

11.3 System Logs

The System Logs provides a variety of logs that you can use to troubleshoot and debug transactions and events that take place within the instance Action and Notification Logs.

System Logs: These logs are invaluable for monitoring and troubleshooting your system.

For configure System Logs, Click on Log > System Logs > System Logs.



RouteXOS 3.7.19 x64 Build202504141740

Log > System Logs > System Logs

CPU TEMP: 48°C CPU: 0.25% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

System Logs

Begin Time End Time Event

Export Clean All

Time	Event
2025-08-02 11:03:30	Chain detection: interface (eth1) up
2025-08-02 11:03:30	Chain detection: (wan1)detected
2025-08-02 11:03:30	System Starting
2025-08-02 11:03:21	Chain detection: interface (eth0) up
2025-08-02 11:03:16	Chain detection: interface (eth0) down
2025-08-02 11:03:00	Chain detection: interface (eth3) up
2025-08-02 11:02:59	Chain detection: interface (eth0) up
2025-08-02 11:02:57	Chain detection: interface (eth3) down
2025-08-01 18:35:56	Chain detection: interface (eth0) up
2025-08-01 18:35:50	Chain detection: interface (eth0) down
2025-08-01 18:35:42	Chain detection: interface (eth0) up
2025-08-01 18:35:38	Chain detection: interface (eth0) down

Fig 11.3.1 Default System Logs page Action

Logs: Action logs are a useful tool for logging the actions of a Time, Username, IP Address, Function and Events.

To configure Action Logs, Click on Log > System Logs > Action Logs.

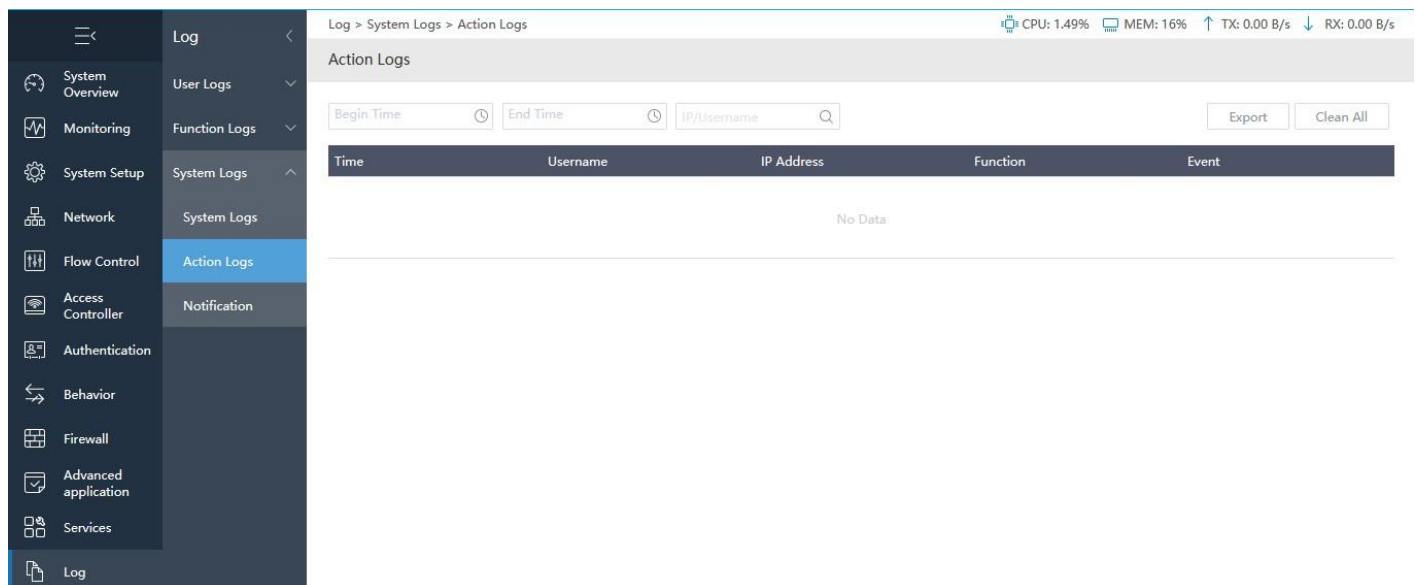


Fig 11.3.2 Default Action Logs page

RouteXOS 3.7.19 x64 Build202504141740

Log > System Logs > Action Logs

CPU TEMP: 48°C CPU: 1.00% MEM: 12% TX: 0.00 B/s RX: 0.00 B/s

Action Logs

Begin Time End Time IP/Username

Export Clean All

Time	Username	IP Address	Function	Event
2025-08-02 12:32:48	COMMANDO	192.168.0.10	Speed	Test exec action for clean
2025-08-02 12:32:47	COMMANDO	192.168.0.10	Speed	Test exec action for clean
2025-08-02 12:32:46	COMMANDO	192.168.0.10	Speed	Test exec action for clean
2025-08-02 12:29:35	COMMANDO	192.168.0.10	Speed	Test exec action for clean
2025-08-02 11:44:19	COMMANDO	192.168.0.10	--	Login
2025-08-01 18:34:51	COMMANDO	192.168.0.10	UDPXY	Set exec action for edit
2025-08-01 18:34:36	COMMANDO	192.168.0.10	UDPXY	Set add a rule
2025-08-01 18:29:06	COMMANDO	192.168.0.10	Wake	on LAN exec action for waking up
2025-08-01 18:29:04	COMMANDO	192.168.0.10	Wake	on LAN exec action for up
2025-08-01 18:28:47	COMMANDO	192.168.0.10	Wake	on LAN exec action for waking up
2025-08-01 18:28:30	COMMANDO	192.168.0.10	Wake	on LAN exec action for edit
2025-08-01 18:28:20	COMMANDO	192.168.0.10	Wake	on LAN exec action for waking up

Fig 11.3.3 Action Logs page

Notification: For viewing Username, Time and Actions.

For viewing Notification, Click on Log > System Logs > Notification.

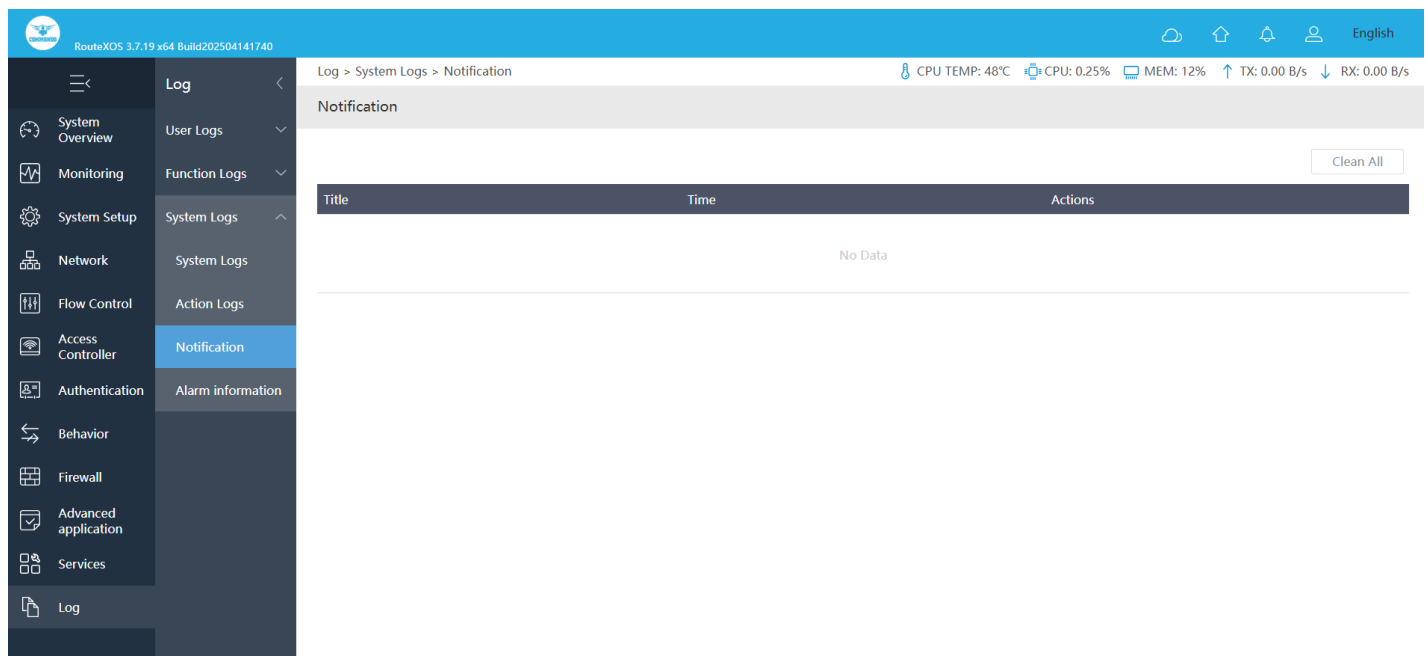


Fig 11.3.4 Notification page

Alarm Information: Alarm Information provides critical alerts related to system events, network issues, and hardware faults, helping administrators quickly identify and resolve potential problems.

To view Alarm Information, click on Log > System Logs > Alarm Information.

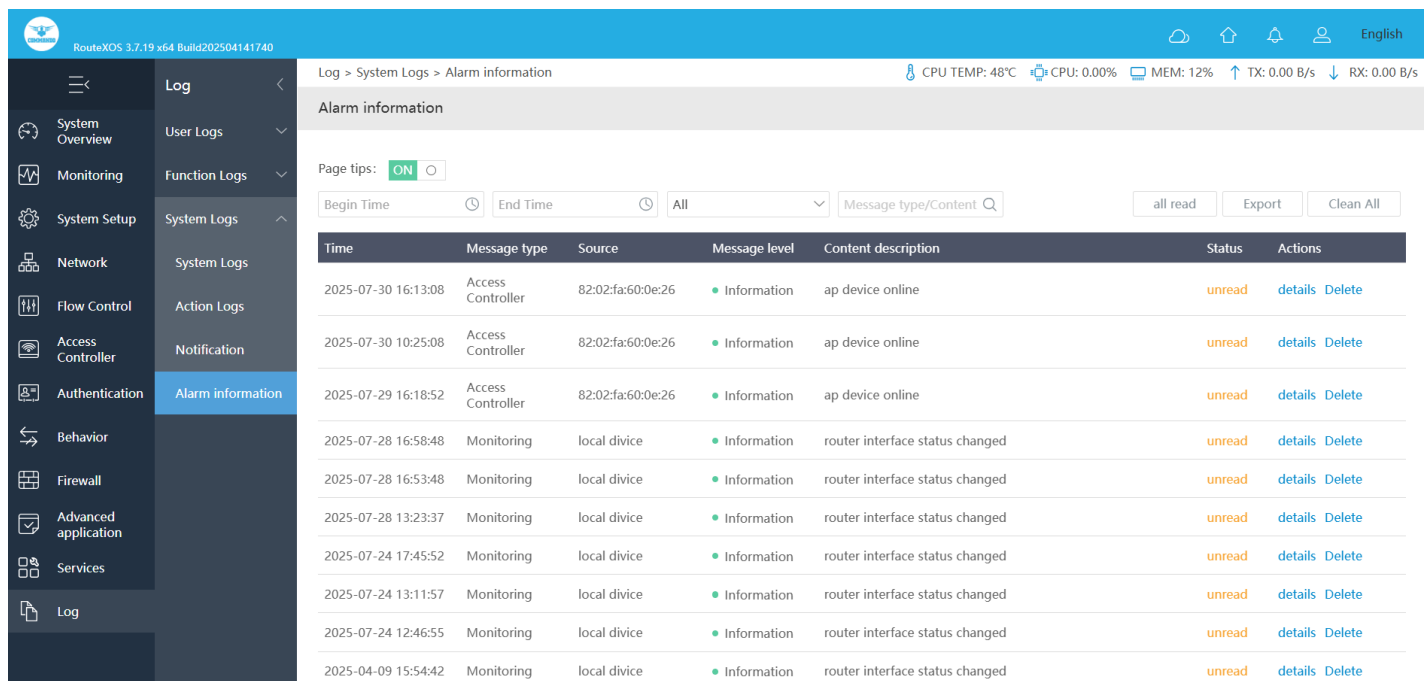


Fig 11.3.5 Alarm information

COMMANDO Cloud

In FIT mode this AP can connect with cloud, and you can configure cloud settings under this option.

What is cloud service?

Cloud service focuses on managing the router. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal.

How to connect to cloud service?

Into cloud platform <http://commandonetworks.com.cn/#/> ---> gets the binding code ---> enters the binding code in router and remark name ---> saves and completes the binding.

How to manage?

Wait about 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.

How to unbind the cloud?

Log in to cloud platform on the PC side and complete the unbundling of corresponding routes in the routing list -- equipment management -- routing information overview page.

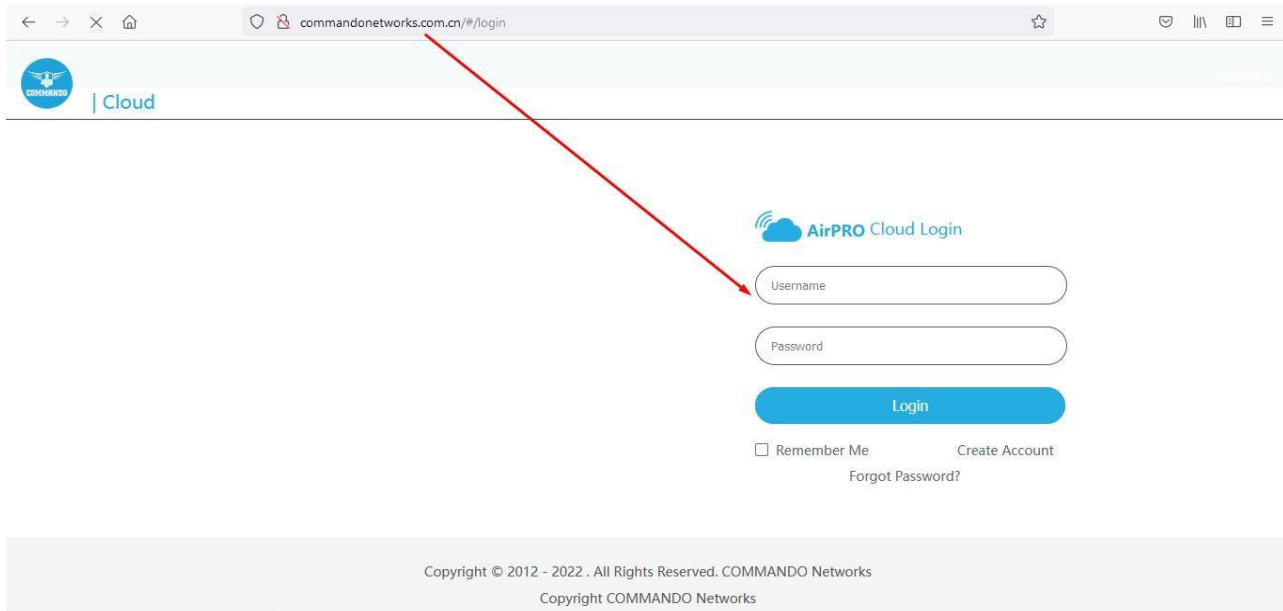


Fig 6.1 Cloud Login page

How to create the account in COMMANDO cloud for login?

Go to any browser and type <http://commandonetworks.com.cn/#/>. Then cloud login page as follows will appear.

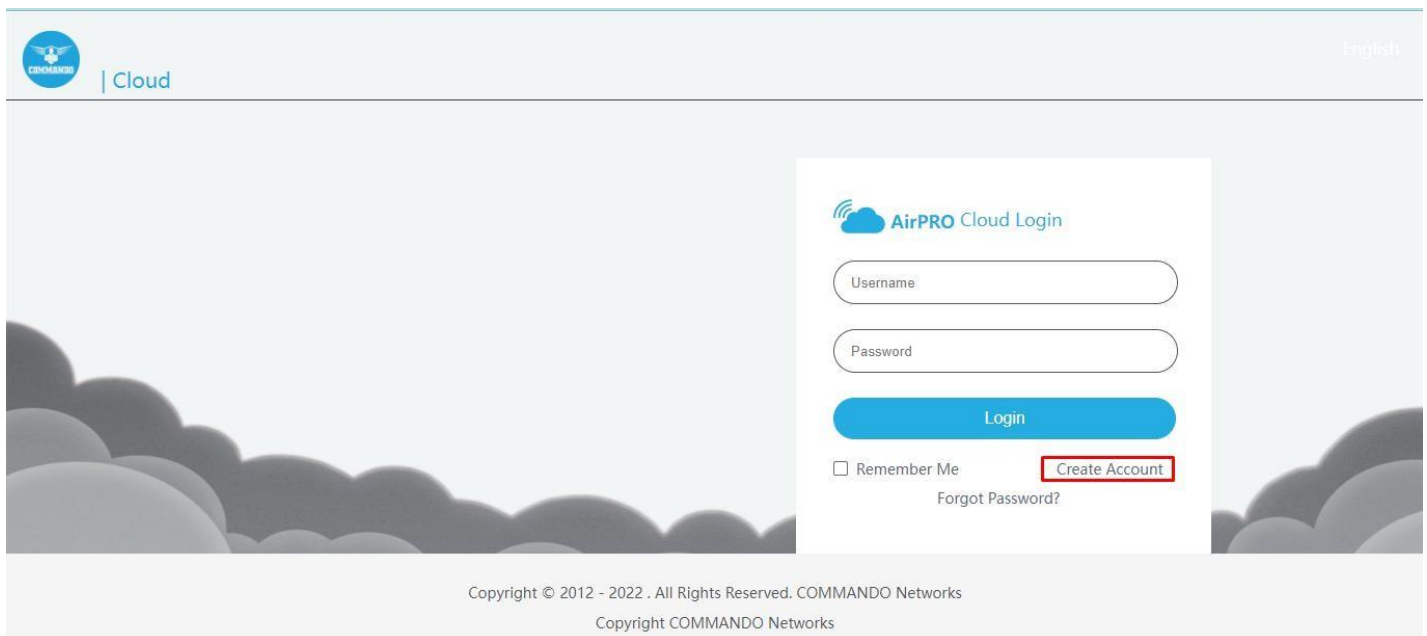


Fig 6.2 Create Cloud Login page

Click on the create account (This process is for creating new account).

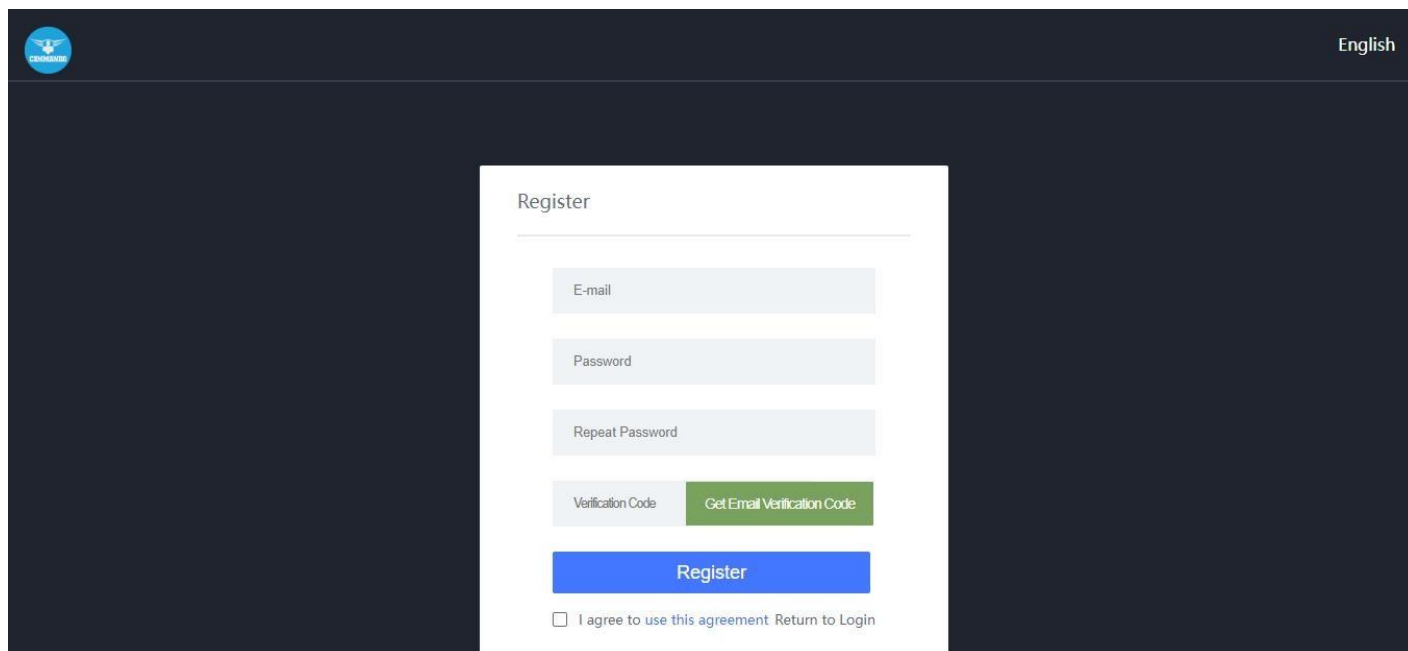


Fig 6.3 Register Cloud Login Email and password page

You can choose Register Cloud Login Email and password as per choice of administrator.
Note: Email ID should be a valid Email ID.

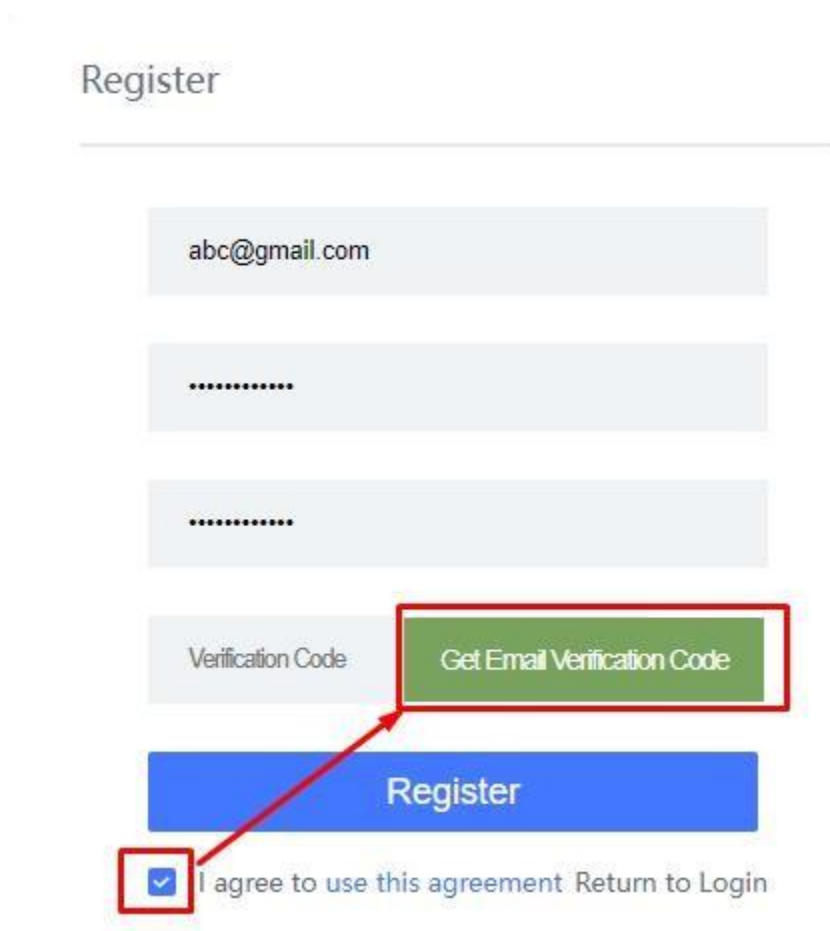


Fig 6.4 Email Verification code page

With the help of RouteX Controller, you can bind with Cloud and can configure AP from cloud itself. How to bind RouteX Controller with COMMANDO cloud login?



Login in the portal with created email credential and copy cloud binding code.

Fig 6.5 Cloud Binding page

Then take access of RouteX Controller connected to internet and go to System Setup > Cloud Account and bind that copied code to router ID.

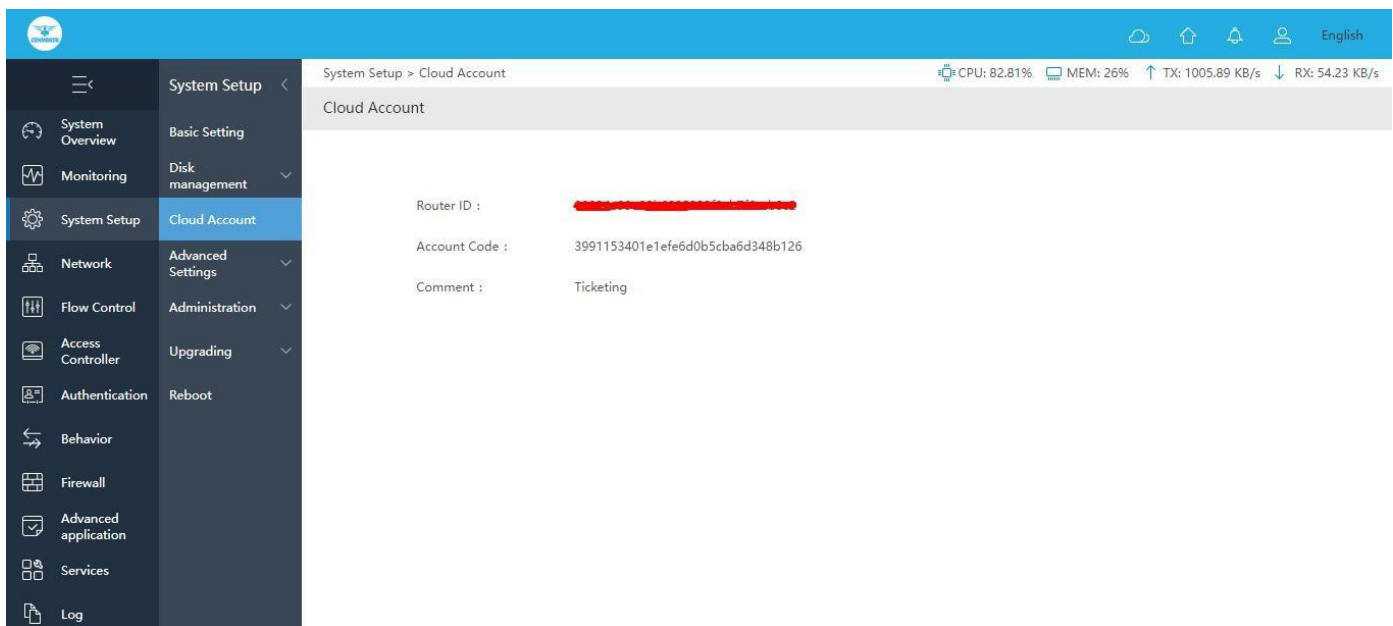


Fig 6.6 RouteX Controller Cloud Account Binding page

After binding code, the cloud portal can access and configure RouteX Controller from anywhere in the world if having correct login credential.

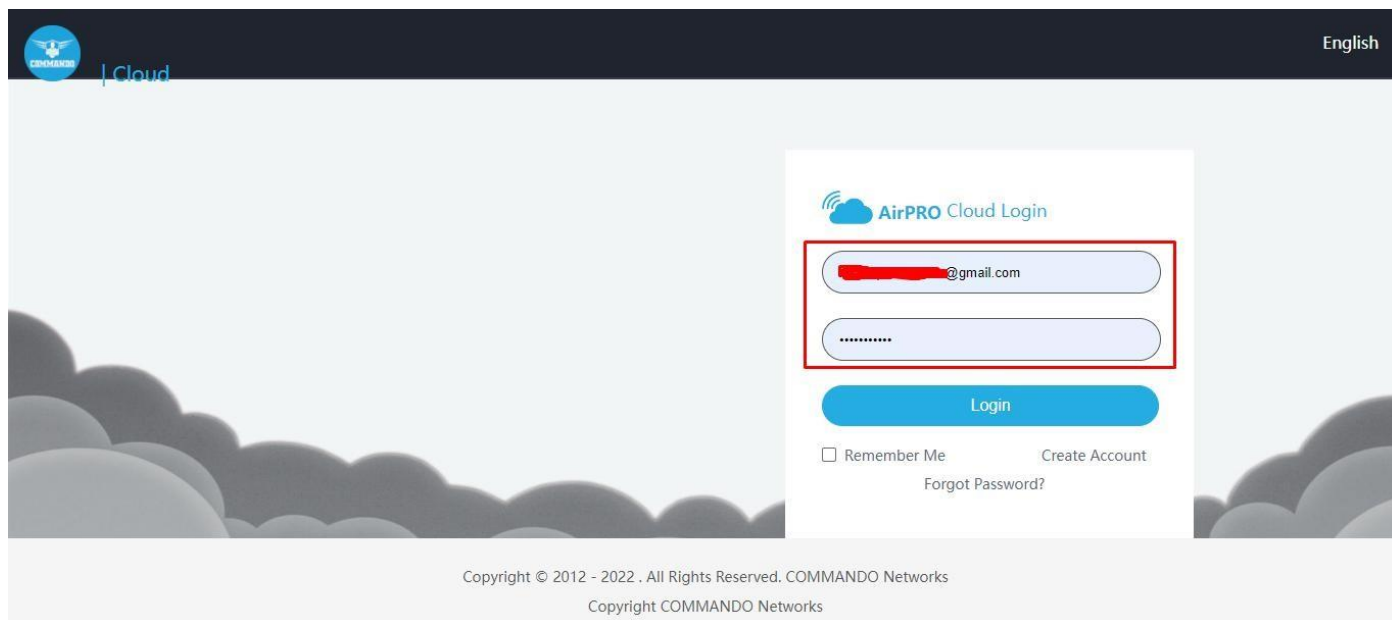


Fig 6.7 Cloud login after binding page

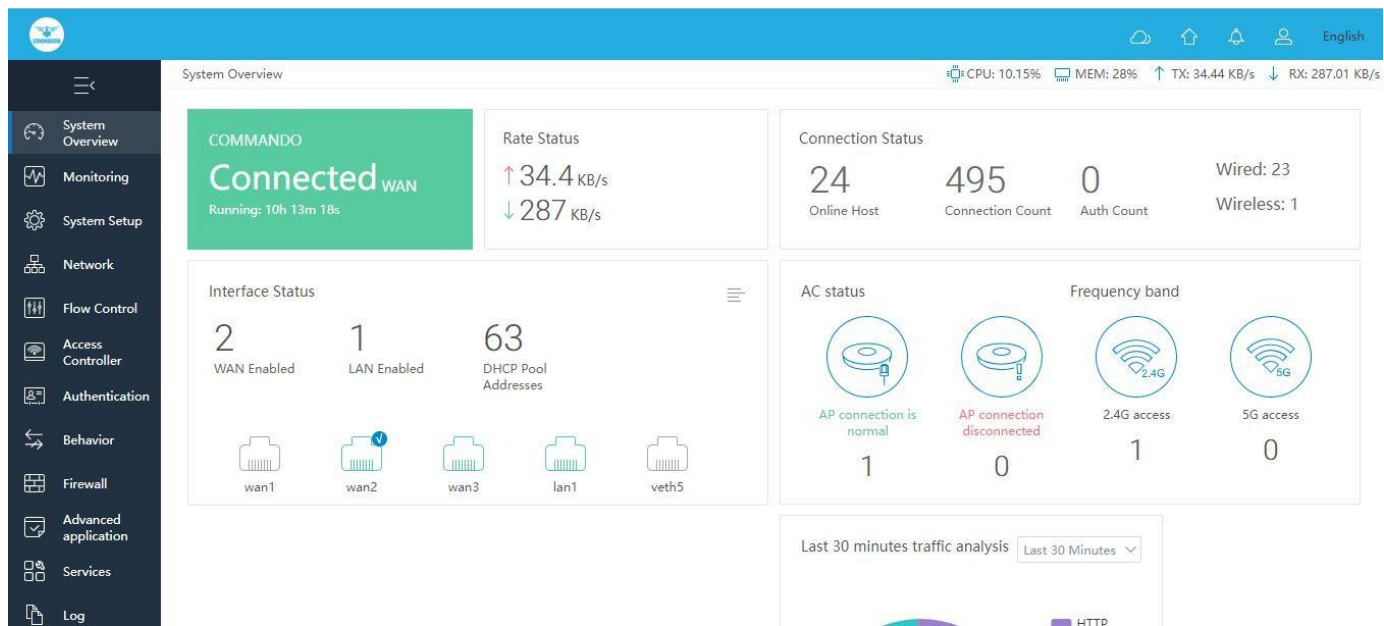


Fig 6.8 RouteX Controller device live access page

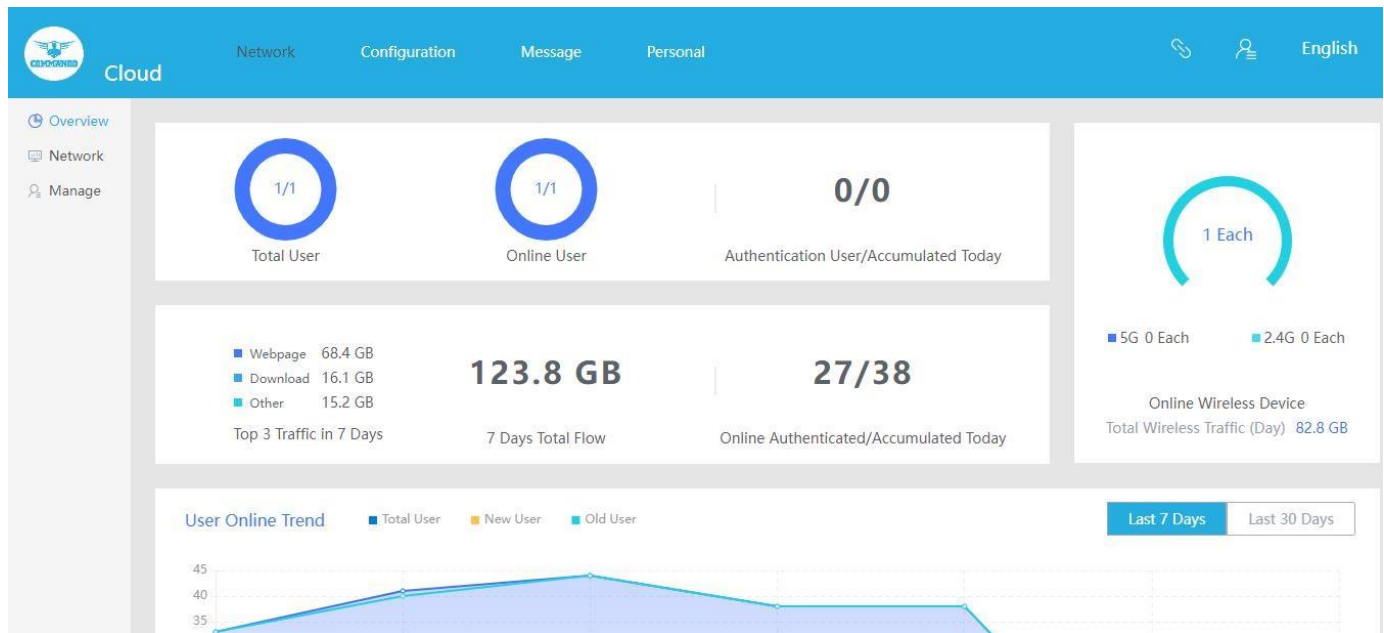


Fig 6.9 RouteX Controller cloud live access page

If password is forgotten, then following process to be followed.

How to recover from lost cloud portal password?

For recover from lost cloud portal password go to the cloud portal of COMMANDO and click Forgot Password.

The screenshot shows the AirPRO Cloud Login page. The page has a light blue header with the COMMANDO logo and the word 'Cloud'. The main content area features a login form with the following elements:

- Username:** A text input field.
- Password:** A text input field.
- Login:** A blue button.
- Remember Me:** A checkbox.
- Create Account:** A link.
- Forgot Password?:** A link highlighted with a red box.

Fig 6.10 F orgot password page

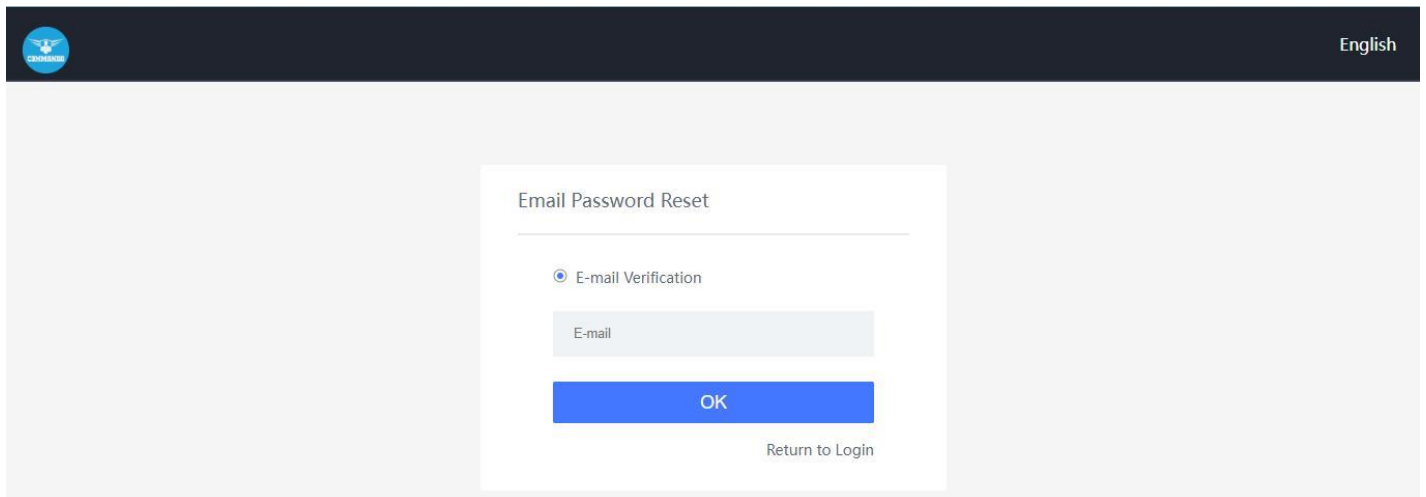


Fig 6.11 Email for password reset page



Fig 6.12 AirPRO Email received for password reset page

The reset email will send on email provided for request to recover or change the password for COMMANDO AirPRO account. Set a new password or change your password and said link will be valid for 2 hours only.

<http://commandonetworks.com.cn/password/reset>. If you do not wish to recover/change your password or didn't make this request, please ignore or delete

this information. You can also contact COMMANDO support for any query.

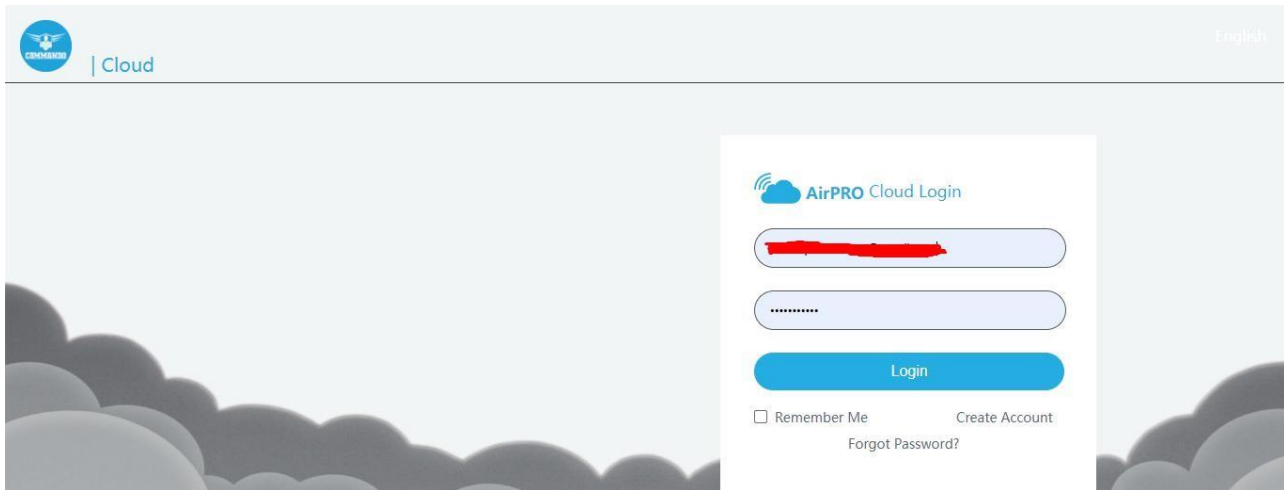


Fig 6.13 AirPRO cloud login after password reset page.

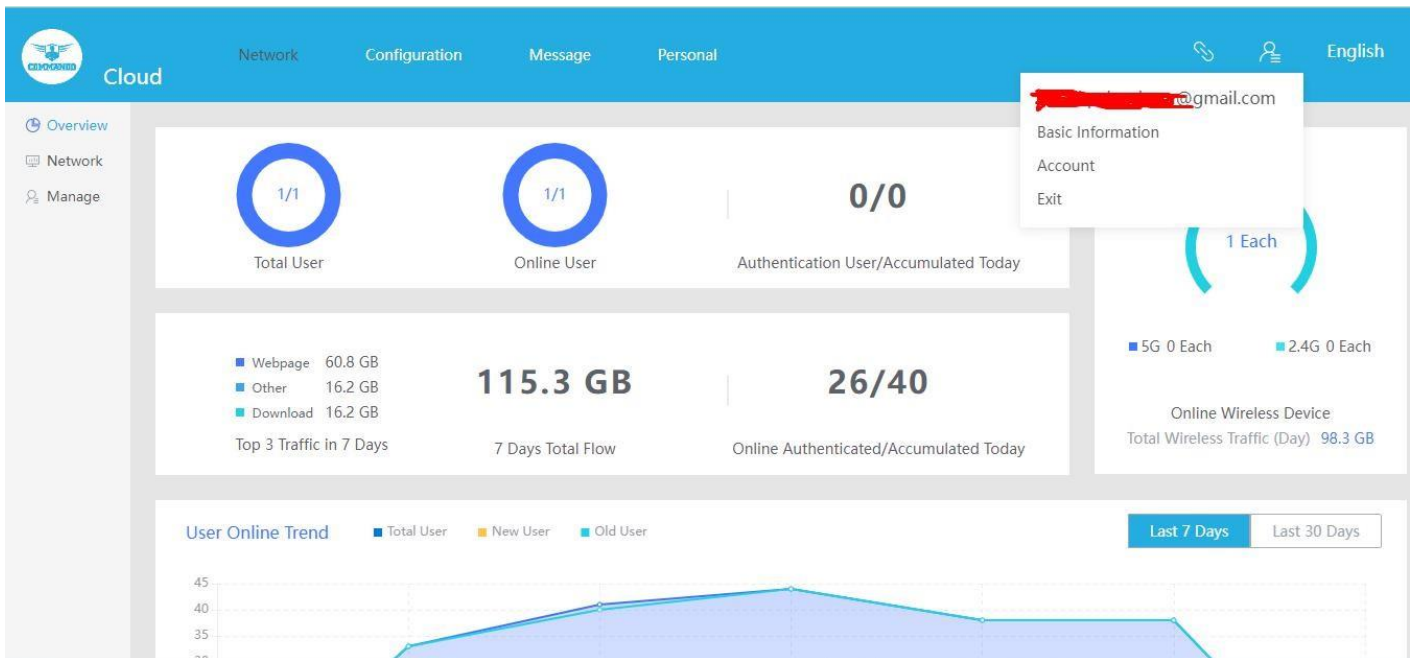


Fig 6.14 AirPRO cloud login page





Fig 6.15 Cloud User Language setting page

1.1.1 AirPRO Cloud Overview

A cloud-managed access point or networking solution allows business owners to manage Wi-Fi and network infrastructure over the cloud with zero maintenance charges, centralize control painlessly. This means businesses can connect to the cloud by subscribing to a pay-as-you-go, on-demand model.

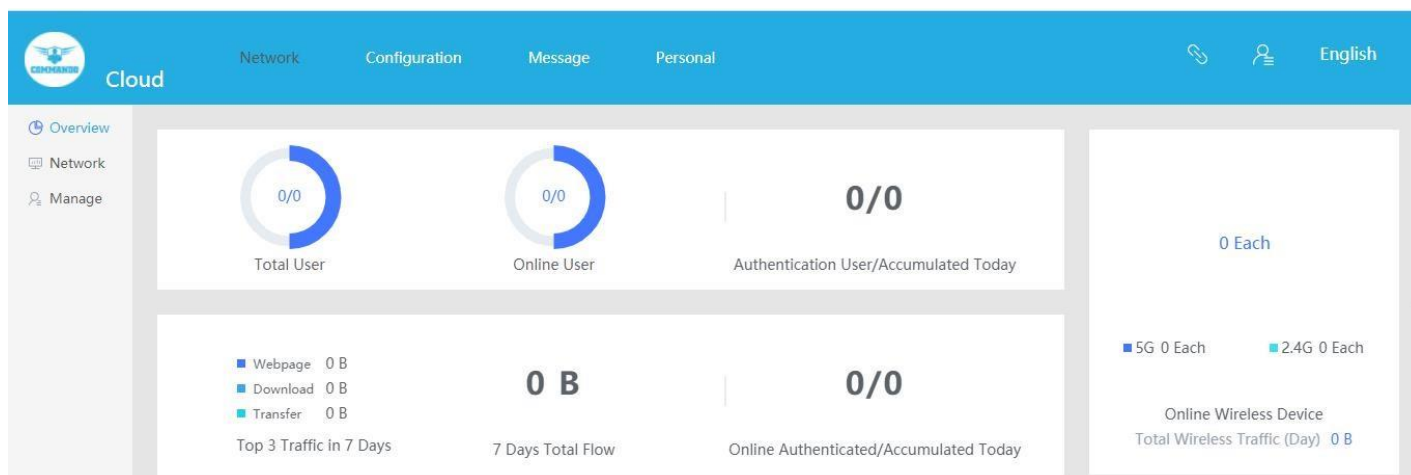


Fig 6.1.1 Default Cloud Overview page

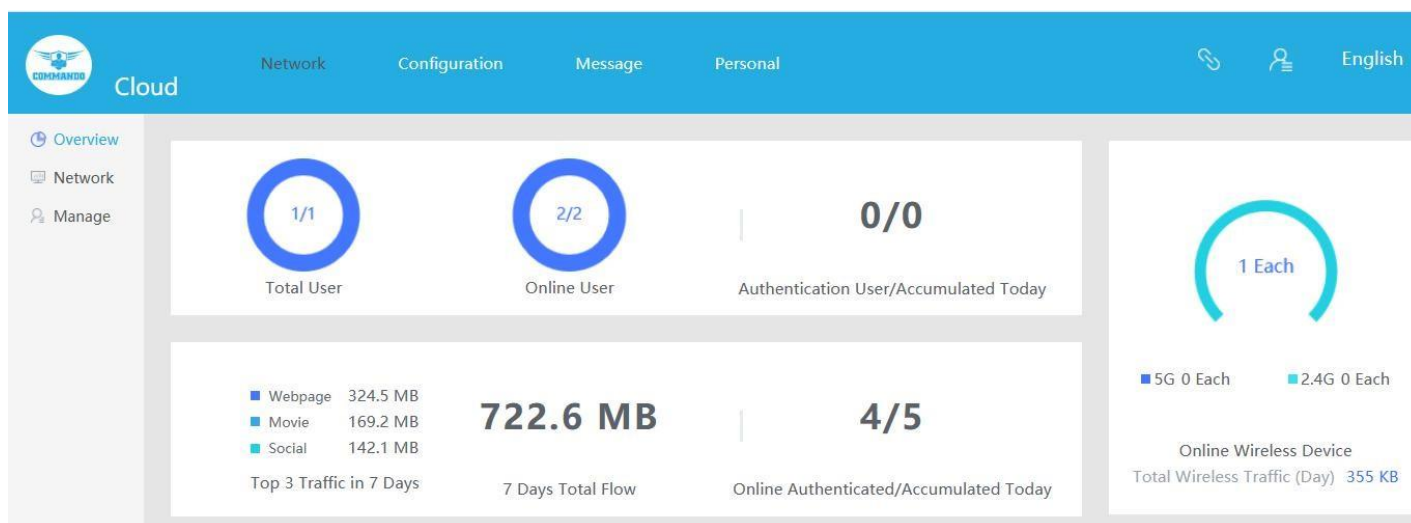


Fig 6.1.2 Cloud Overview page



Fig 6.1.3 Cloud User online trend page

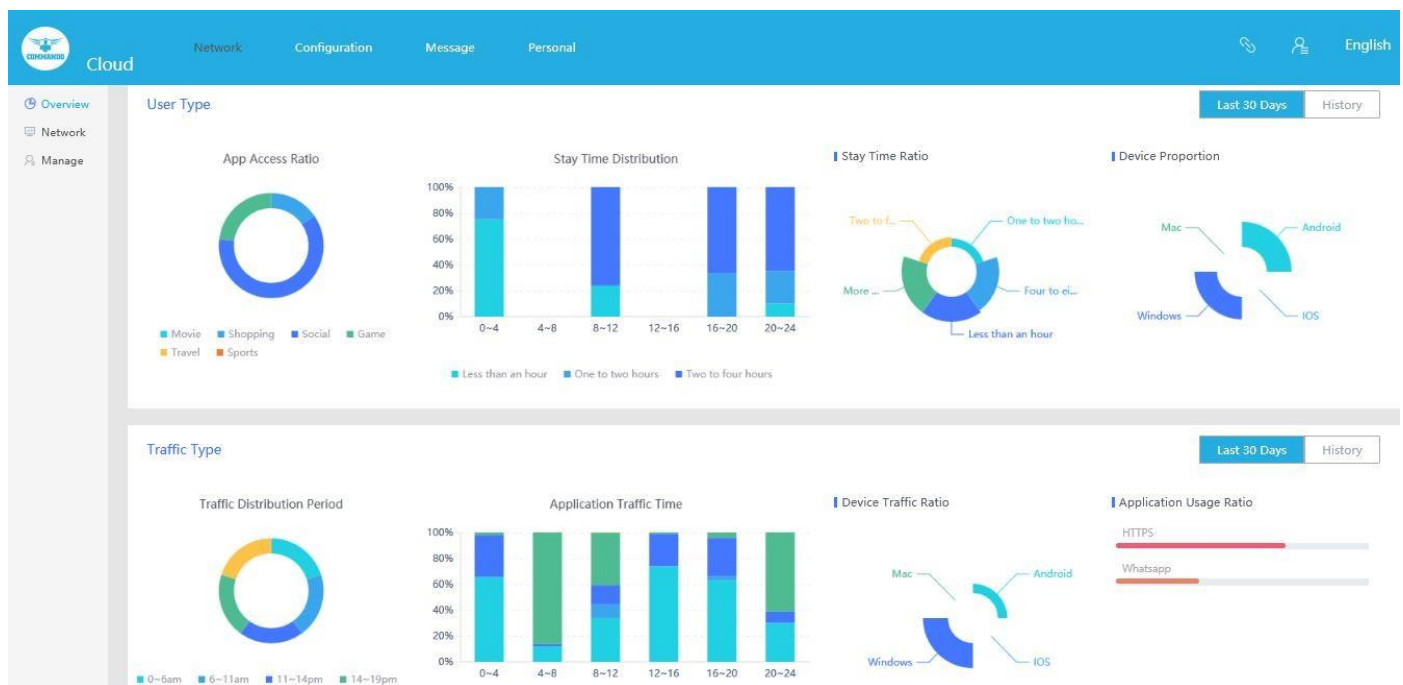


Fig 6.1.4 Cloud User Type page

1.2 Network

Cloud Networking Solutions are Designed to Enhance Your access and IT infrastructure in which some or all of an organization's network capabilities and resources are hosted cloud account.

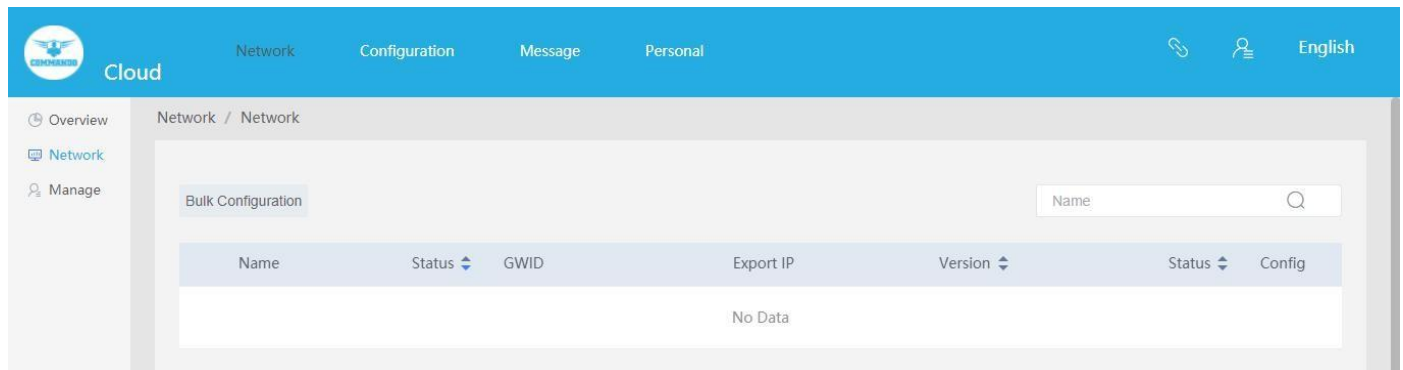


Fig 6.2.1 Default Bulk configuration page

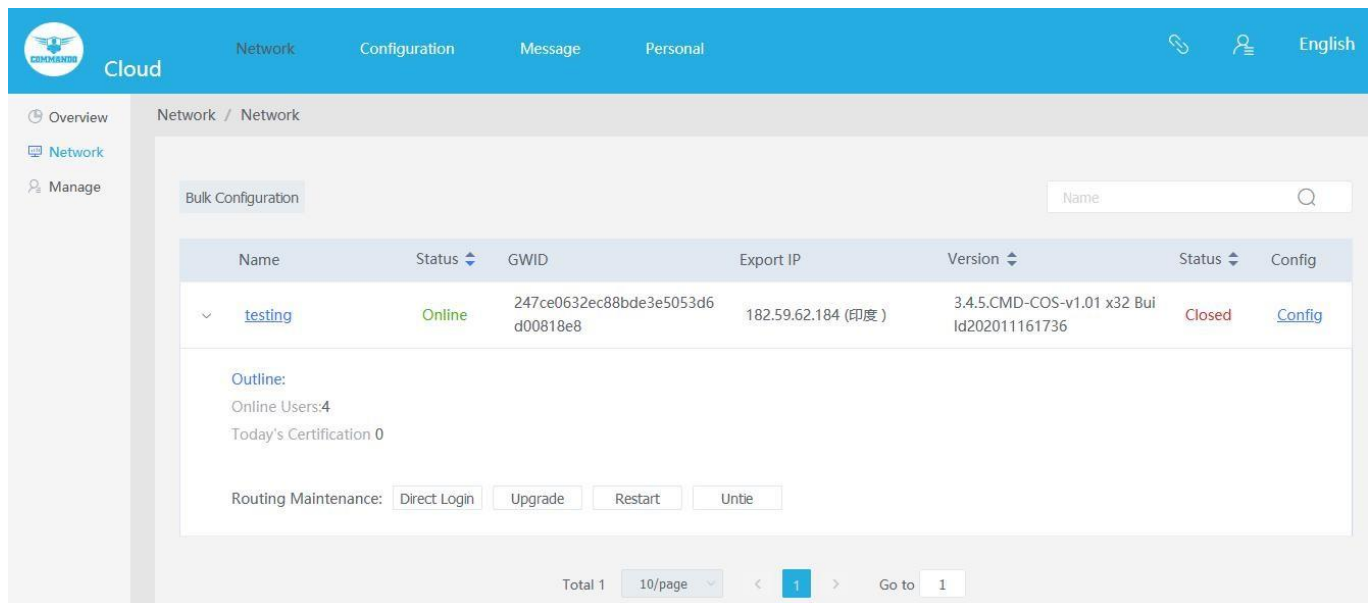


Fig 6.2.2 Bulk configuration page

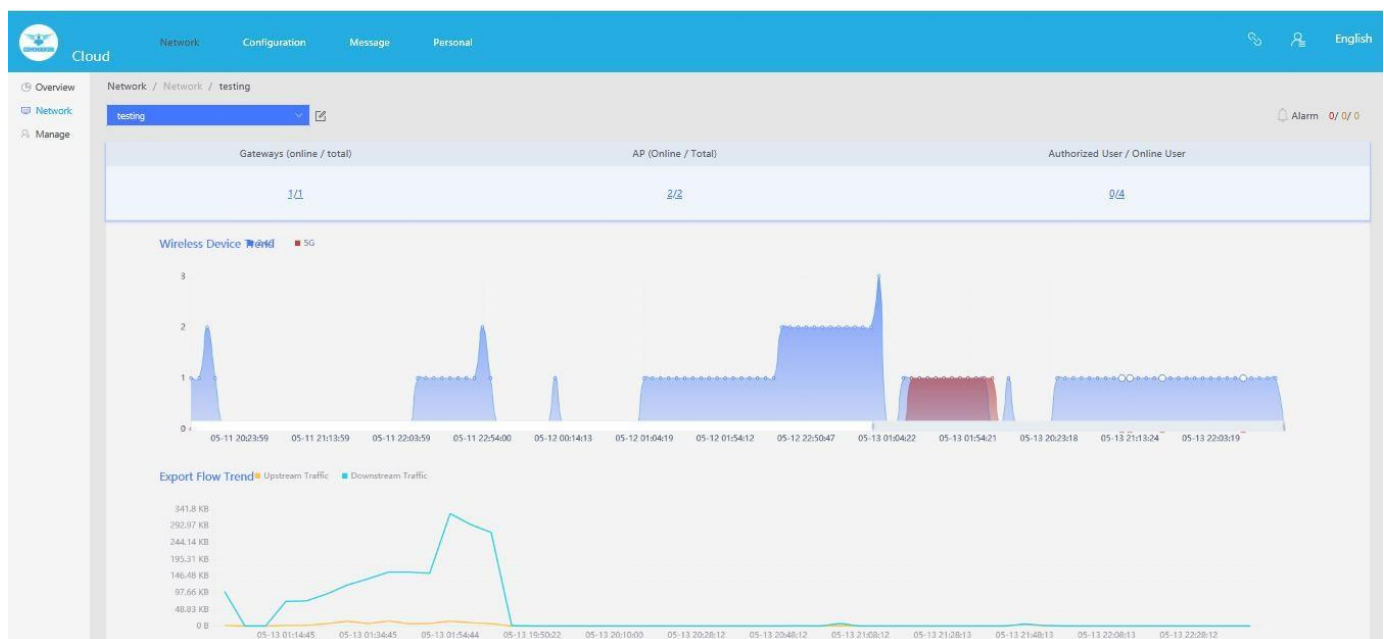


Fig 6.2.3 Network Devices listed in Cloud page

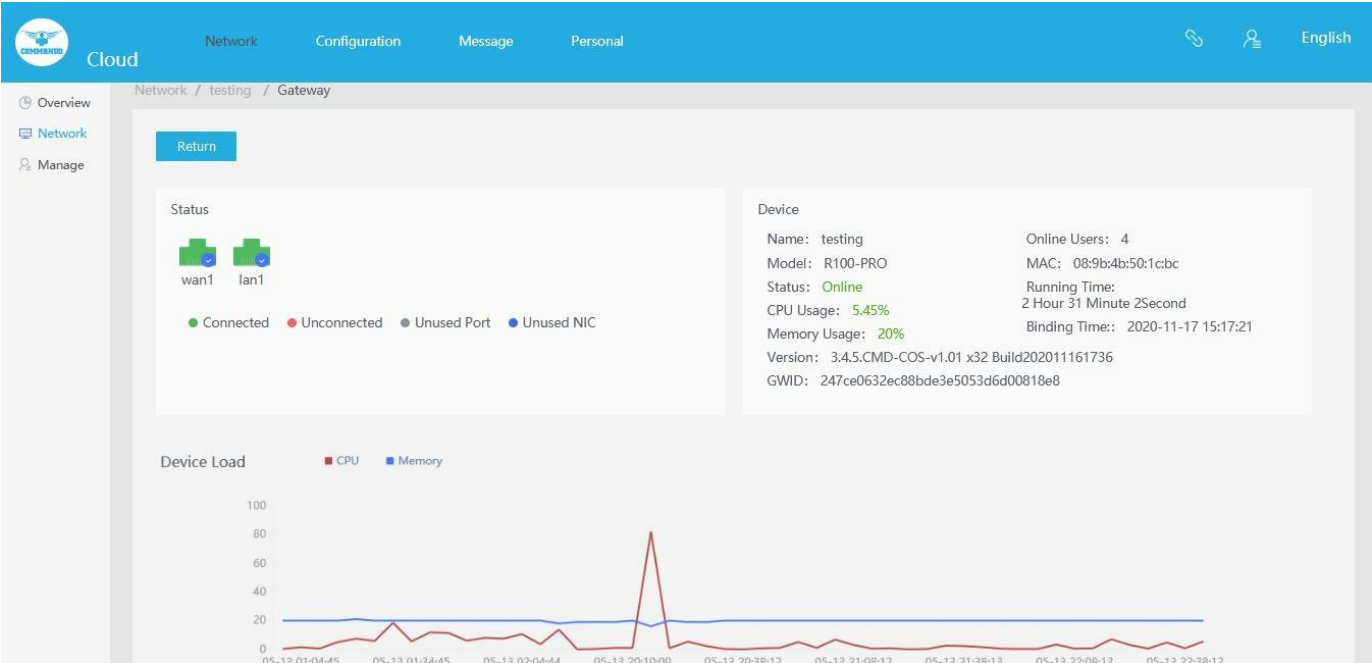


Fig 6.2.4 Gateway page

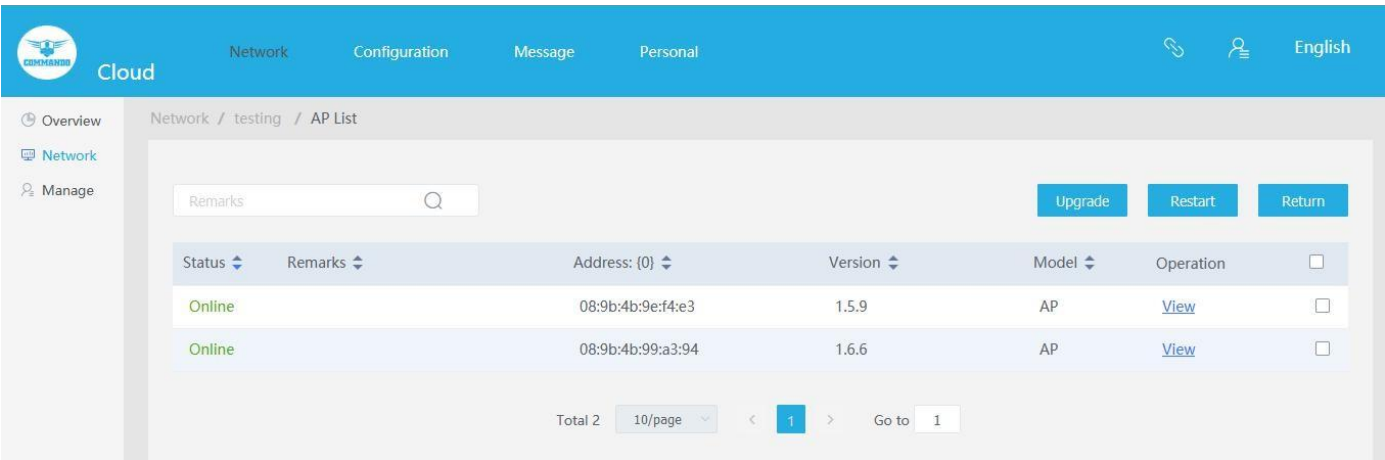


Fig 6.2.5 AP List page

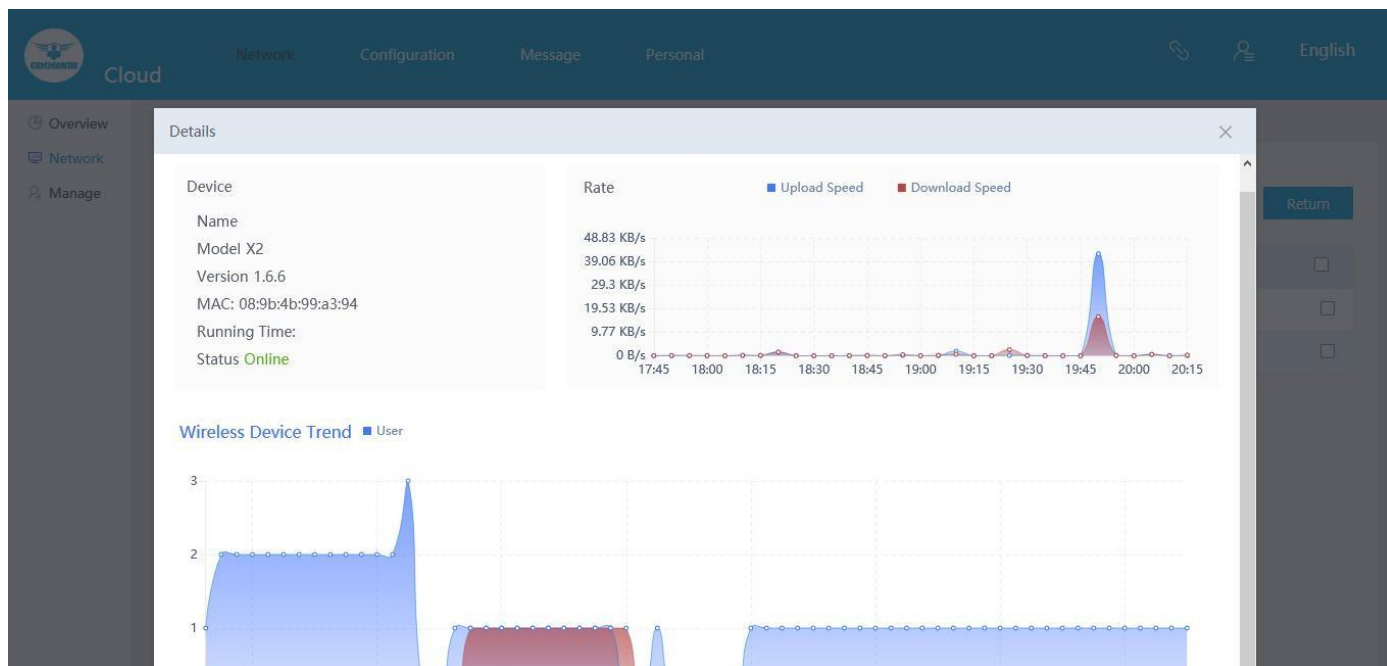


Fig 6.2.5 Bulk configuration for particular AP Device page

testing

Device:

Device	IP	MAC	AP_MAC	Total Tx	Total Rx	Total Time	Online time	Operation
DESKTOP-70API5S	192.168.0.101	c4:d9:87:a7:a d:46	c4:d9:87:a7:a d:46	6.14 MB	61.47 MB	2 Hour 19 Minute 11Second	2021-05-13 17:54	
	192.168.0.100	e0:db:55:be:35:5b	e0:db:55:be:35:5b	1.01 KB	11.43 KB	2 Hour 12 Minute 32Second	2021-05-13 18:01	
AP	192.168.0.102	08:9b:4b:9e:f4:e3	08:9b:4b:9e:f4:e3	680.00 Byte	708.00 Byte	2 Hour 30 Minute 20Second	2021-05-13 17:43	
AP	192.168.0.105	08:9b:4b:99:a3:94	08:9b:4b:99:a3:94	500.00 Byte	567.00 Byte	2 Hour 30 Minute 5Second	2021-05-13 17:43	

Total 4 10/page < 1 > Go to 1

Fig 6.2.6 Network Management for all users' page

1.3 Configuration

The Cloud authentication can be done with three server method namely Cloud Platform, Customize as per user requirement and Web-Radius. Cloud networking allows users to build networks using cloud-based services with help of certification process with Global Portal and WeChat Mini Program. A reliable cloud network provides centralized management, control and visibility, for example, managing devices in different physical locations using the internet. It can be used for connectivity, security, management and control.

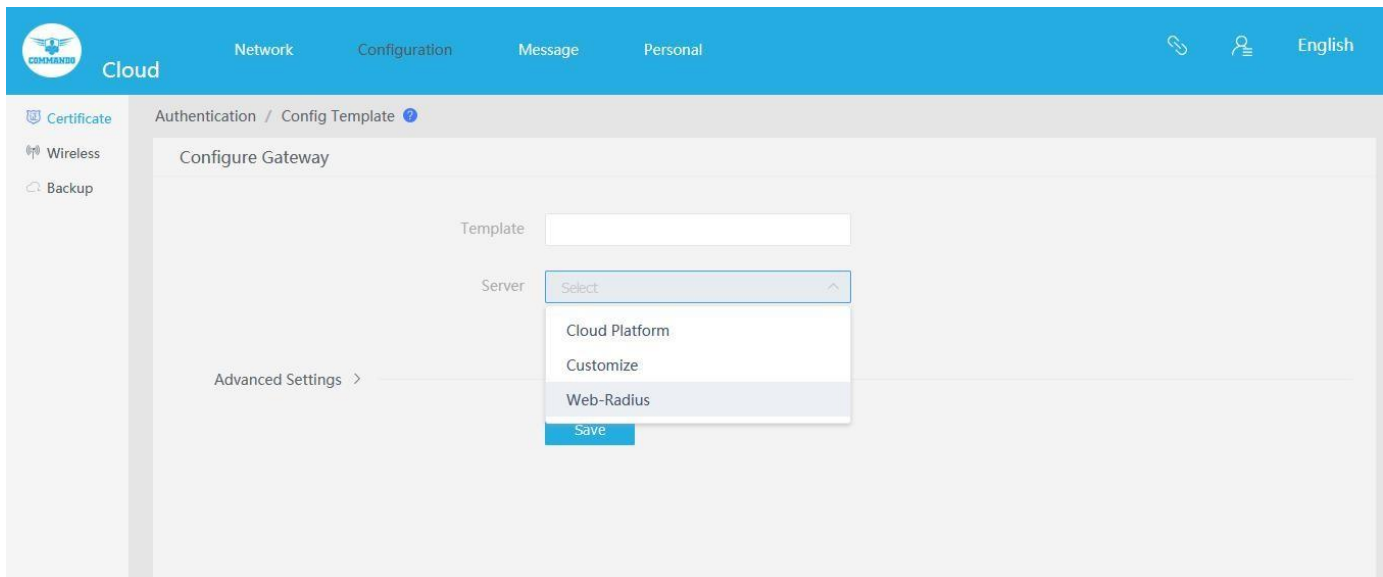


Fig 6.3.1 Default Server Authentication selection page

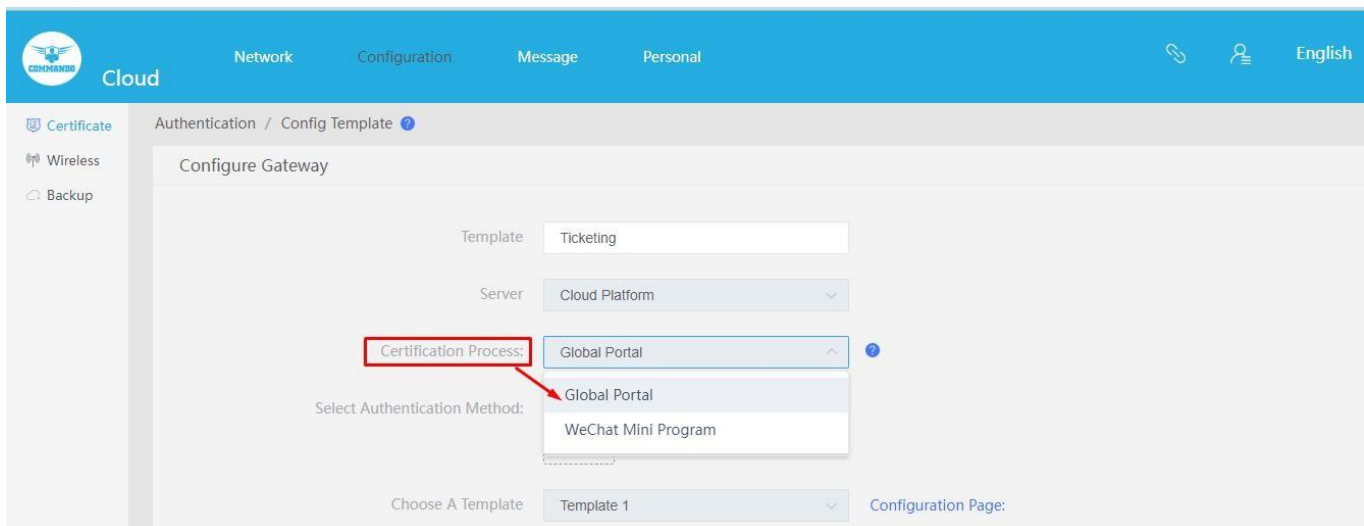


Fig 6.3.2 Certification Process selection option page

User can select various Authentication Method as per choice/requirement. You can choose multiple methods of authentication simultaneously.

Add Authentication Method

☐ WeChat Link Wi-Fi

☐ Mobile Authentication

☐ User Authentication

☐ One-click Authentication

☐ Fixed Password

☐ Countdown Authentication


☐ QQ Authentication

☐ MicroBlog Authentication

☐ Code Authentication

☐ Trial

Fig 6.3.3 Authentication Method selection option page

Cloud

Network

Configuration

Message

Personal

Certificate

Wireless

Backup

Authentication / Config Template

Configure Gateway

Template

Server

Certification Process:

Select Authentication Method:

Choose A Template


Configuration Page:

Cloud Platform

Global Portal

+

Template 1

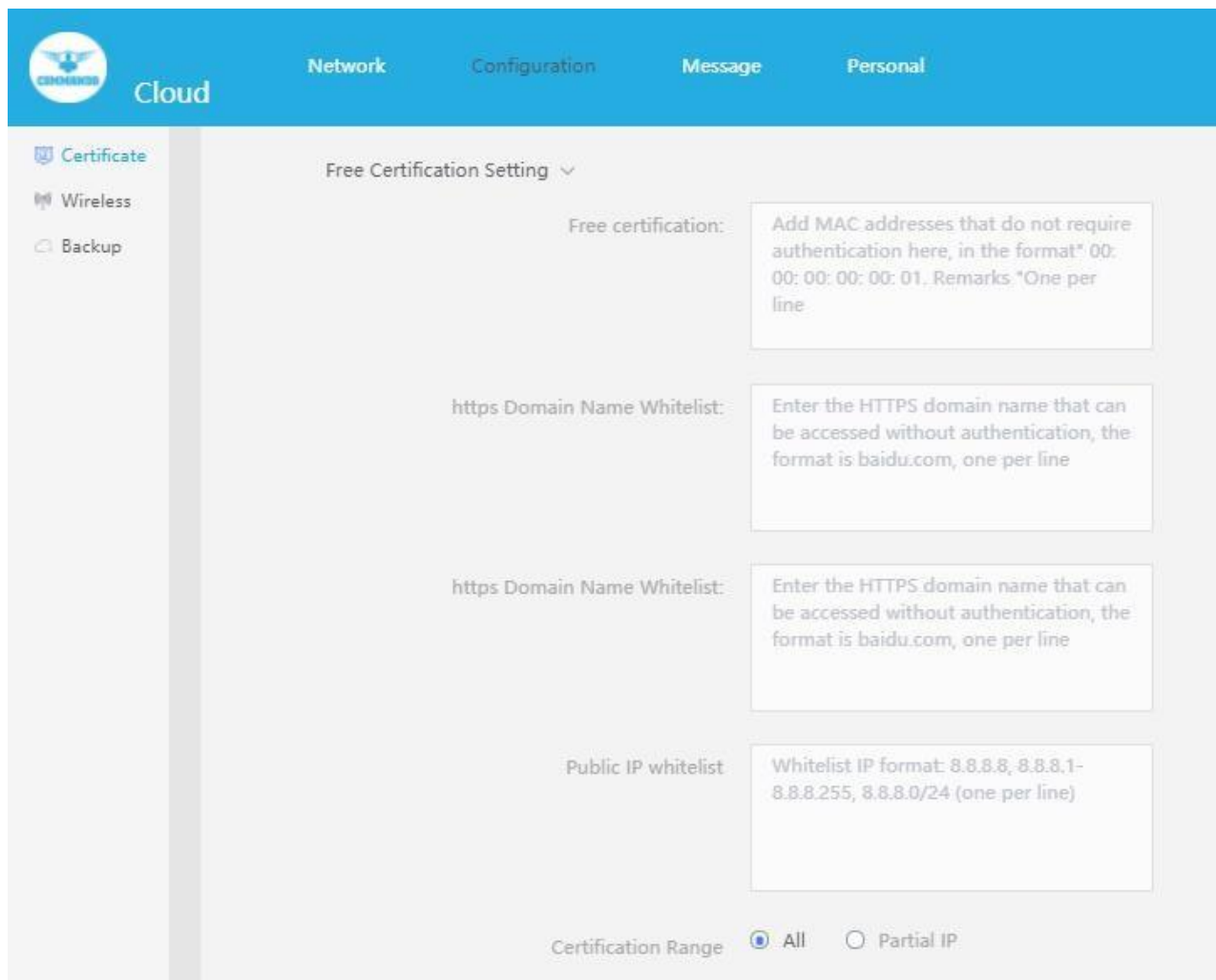


Pool

Select Networking Mode

Network connection

Fig 6.3.4 Default Cloud platform configure gateway page

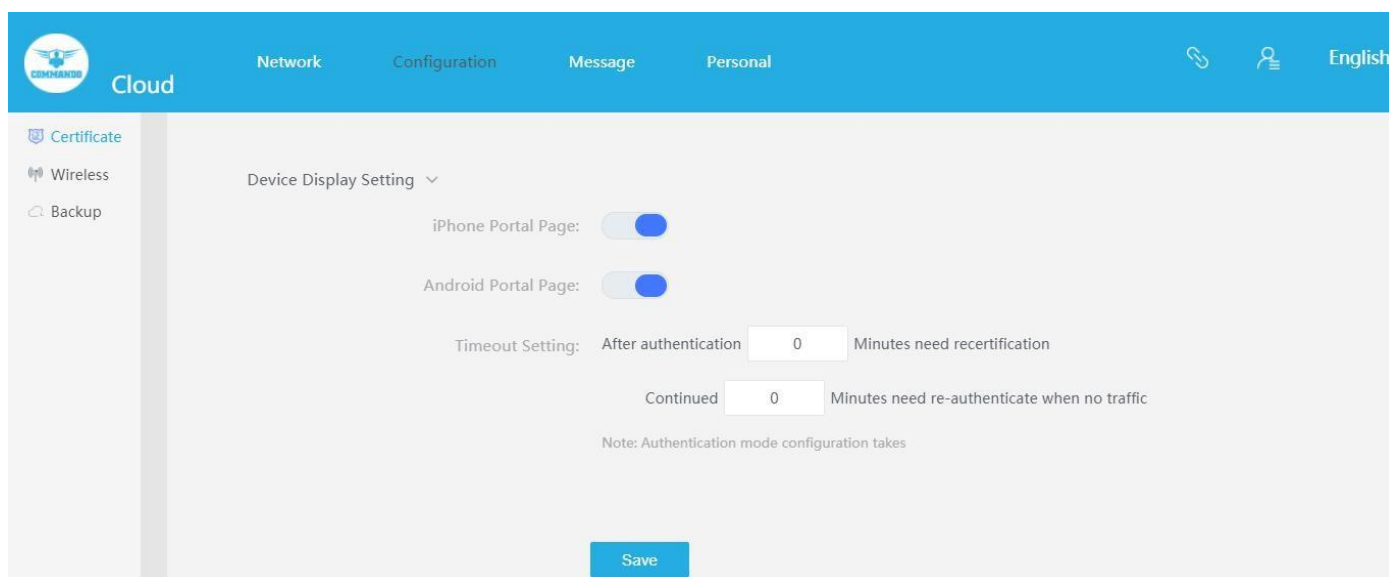


The screenshot shows the 'Free Certification Setting' page. The left sidebar contains 'Certificate', 'Wireless', and 'Backup' options. The main content area has a title 'Free Certification Setting' with a dropdown arrow. Below the title are four configuration sections, each with a label and a text input box:

- Free certification:** Add MAC addresses that do not require authentication here, in the format "00:00:00:00:00:01, Remarks "One per line"
- https Domain Name Whitelist:** Enter the HTTPS domain name that can be accessed without authentication, the format is baidu.com, one per line
- https Domain Name Whitelist:** Enter the HTTPS domain name that can be accessed without authentication, the format is baidu.com, one per line
- Public IP whitelist** Whitelist IP format: 8.8.8.8, 8.8.8.1-8.8.8.255, 8.8.8.0/24 (one per line)

At the bottom, there is a 'Certification Range' section with two radio buttons: 'All' (selected) and 'Partial IP'.

Fig 6.3.5 Default Authentication Free certification setting page



The screenshot shows the 'Device Display Setting' page. The left sidebar contains 'Certificate', 'Wireless', and 'Backup' options. The main content area has a title 'Device Display Setting' with a dropdown arrow. Below the title are three configuration sections:

- iPhone Portal Page:** A toggle switch that is currently turned on (blue).
- Android Portal Page:** A toggle switch that is currently turned on (blue).
- Timeout Setting:** This section includes two input fields for 'Minutes need recertification' and 'Minutes need re-authenticate when no traffic', both set to '0'.

Below the input fields is a note: 'Note: Authentication mode configuration takes'. At the bottom center, there is a blue 'Save' button.

Fig 6.3.6 Default Authentication Device Display setting page

Example 1:

Let us set Authentication/Config Template for Configure Gateway with Template named Ticketing with authentication Server platform as Cloud Platform with Certification Process as Global Portal along with Authentication Method as One-click Authentication.

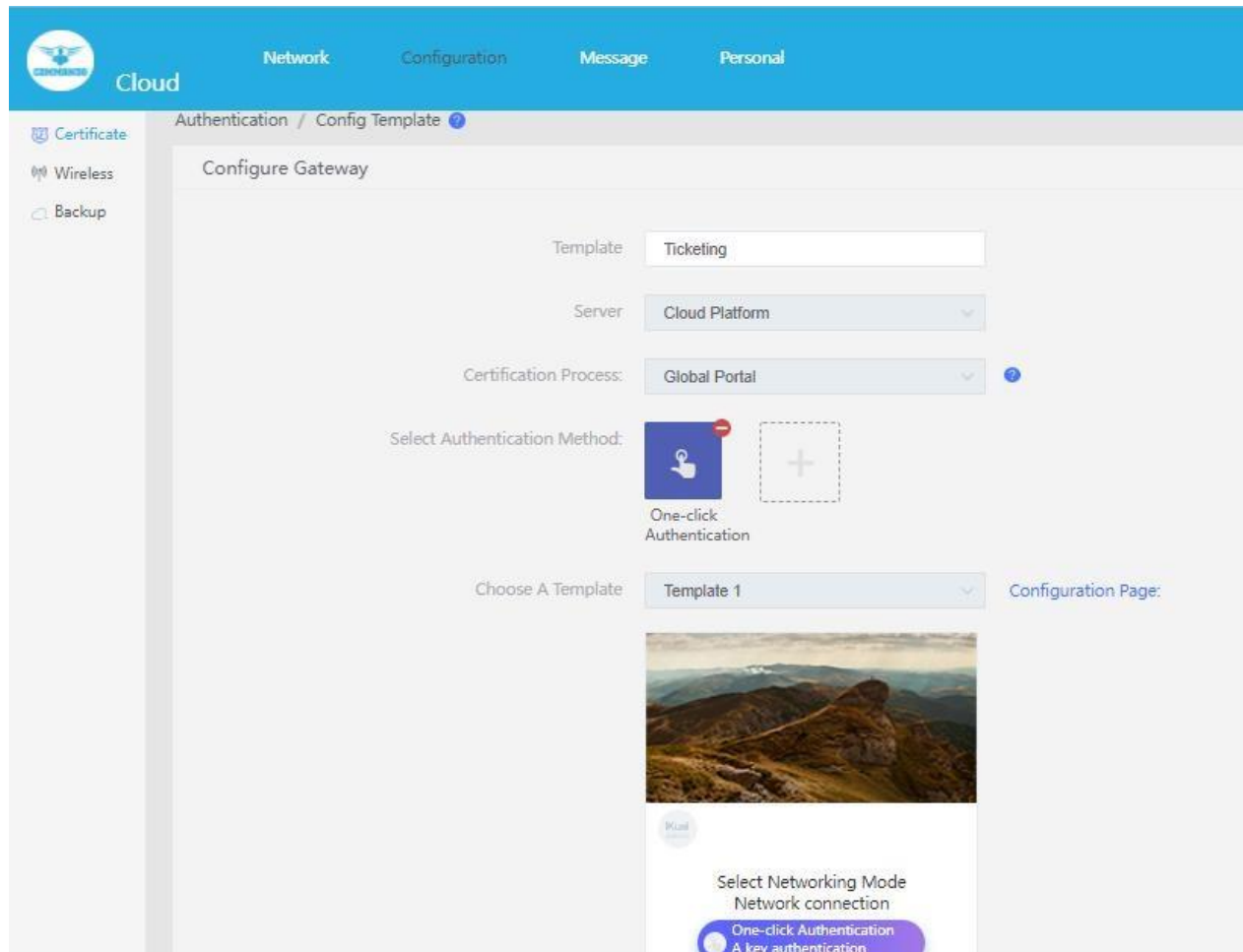


Fig 6.3.7 Authentication Config Template setting for example 1 page

Note: After adding a template, you can go to the " Network Management "page and use the" Bulk Configuration "option to deliver the template.

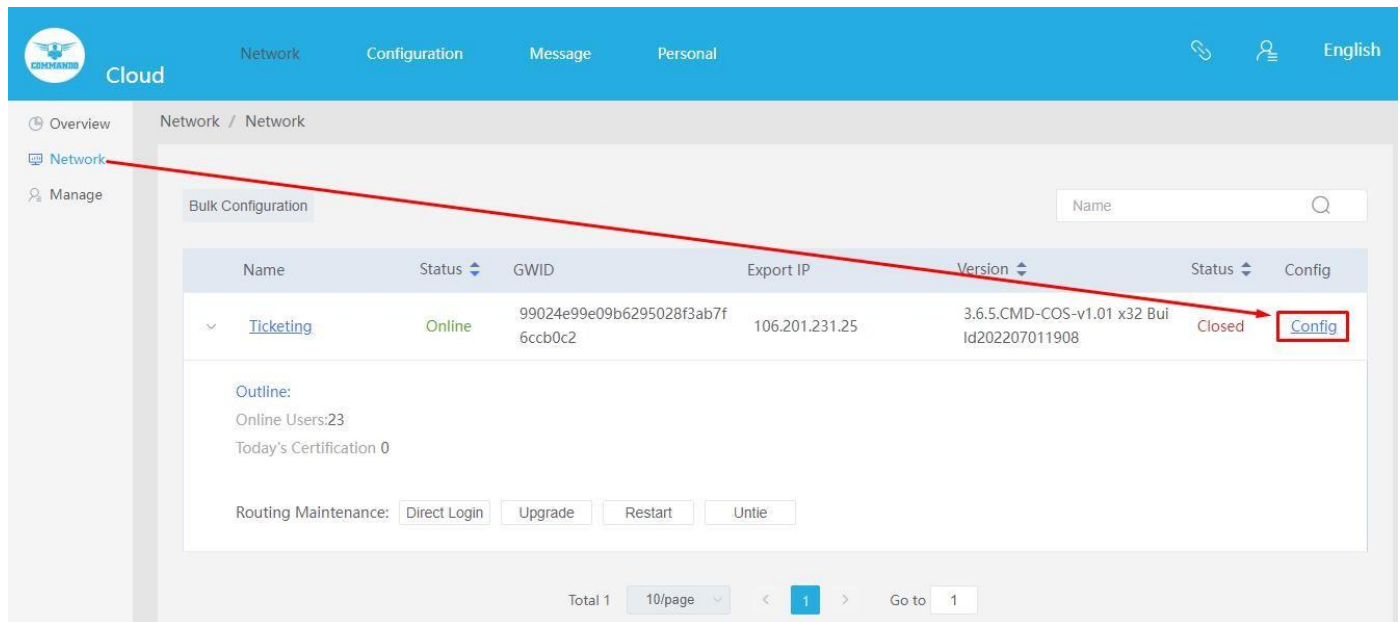


Fig 6.3.8 Authentication Configuration in network setting for example 1 page



Fig 6.3.9 Authentication web page for example 1 page

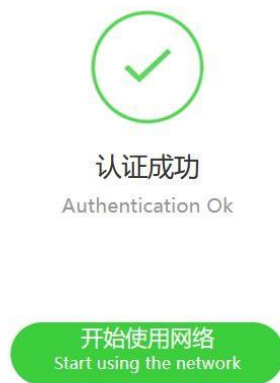


Fig 6.3.10 Authentication Successful web page for example 1 page



Fig 6.3.11 Wi-Fi connected after Authentication Successful for example 1 page

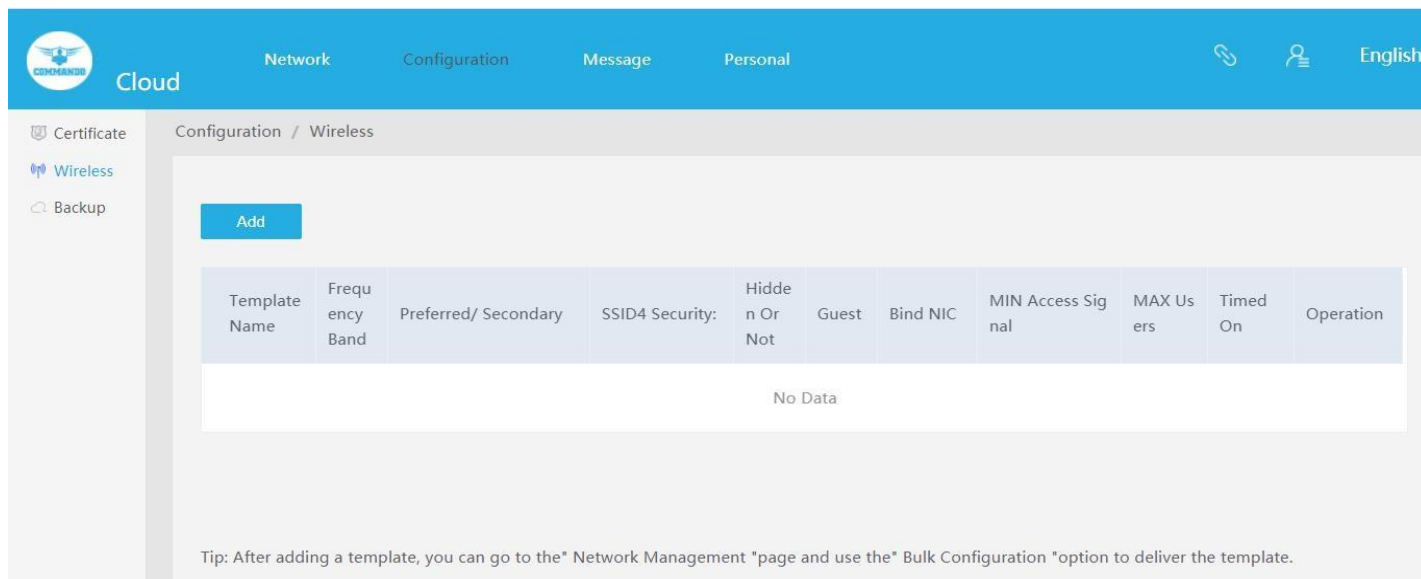


Fig 6.3.12 Default Wireless add setting page

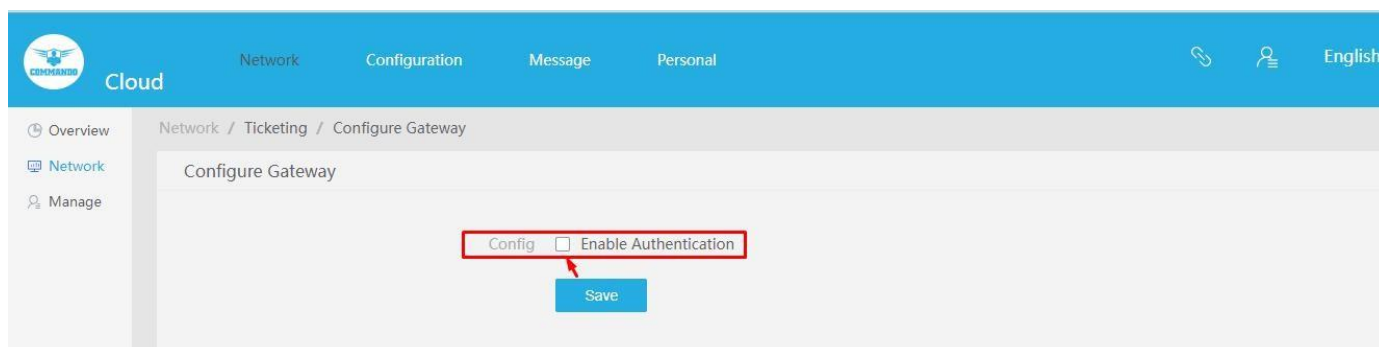


Fig 6.3.13 Default configure gateway setting page

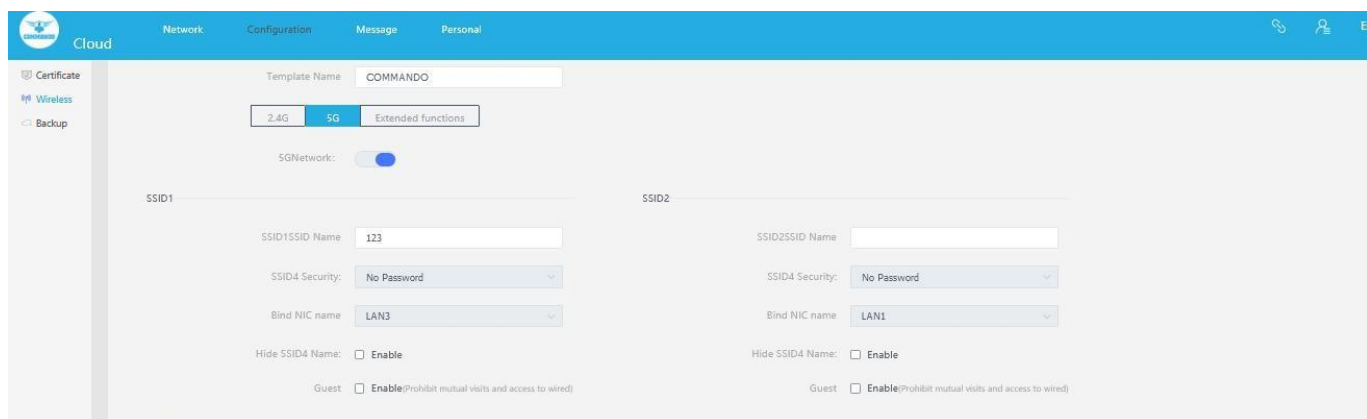


Fig 6.3.14 Default Add 5G Wireless setting page

Cloud

Network Configuration Message Personal

Configuration / Wireless Template / Wireless

Wireless

Template Name

2.4G 5G Extended functions

Timed On ☐ Plan 1
☐ Plan 2
☐ Plan 3

Save Cancel

Fig 6.3.15 Default Wireless Configuration Extended function setting page

Cloud

Network Configuration Message Personal

Configuration / Wireless Template / Wireless

Wireless

Template Name

2.4G 5G Extended functions

Timed On ☒ Plan 1
☐ Plan 2
☐ Plan 3

Period: One Time:

One Time:

Time:

Save Cancel

Fig 6.3.16 Default Wireless Configuration Extended function for Plan 1 setting page

Cloud

Network Configuration Message Personal

Configuration / Cloud Backup

Name

Name	GWID	Manual Backup:	Auto Backup	Operation
No Data				

Total 0 10/page < 1 > Go to 1

Fig 6.3.17 Default Configuration backup setting page

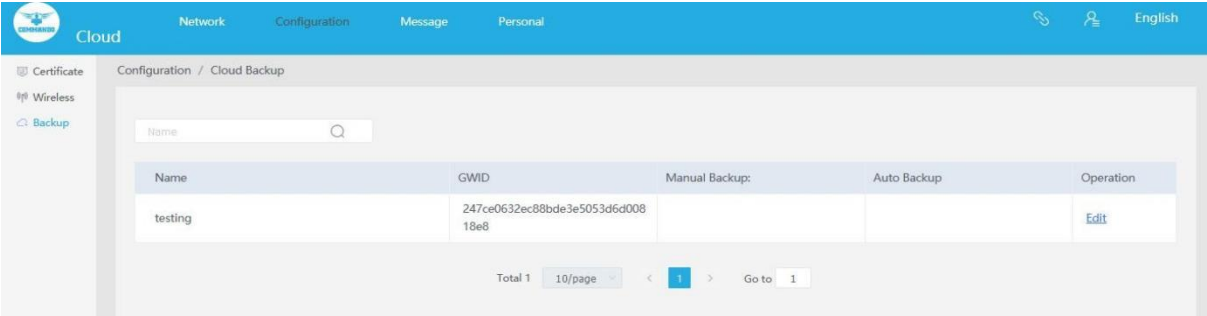


Fig 6.3.18 Default Backup Configuration setting page

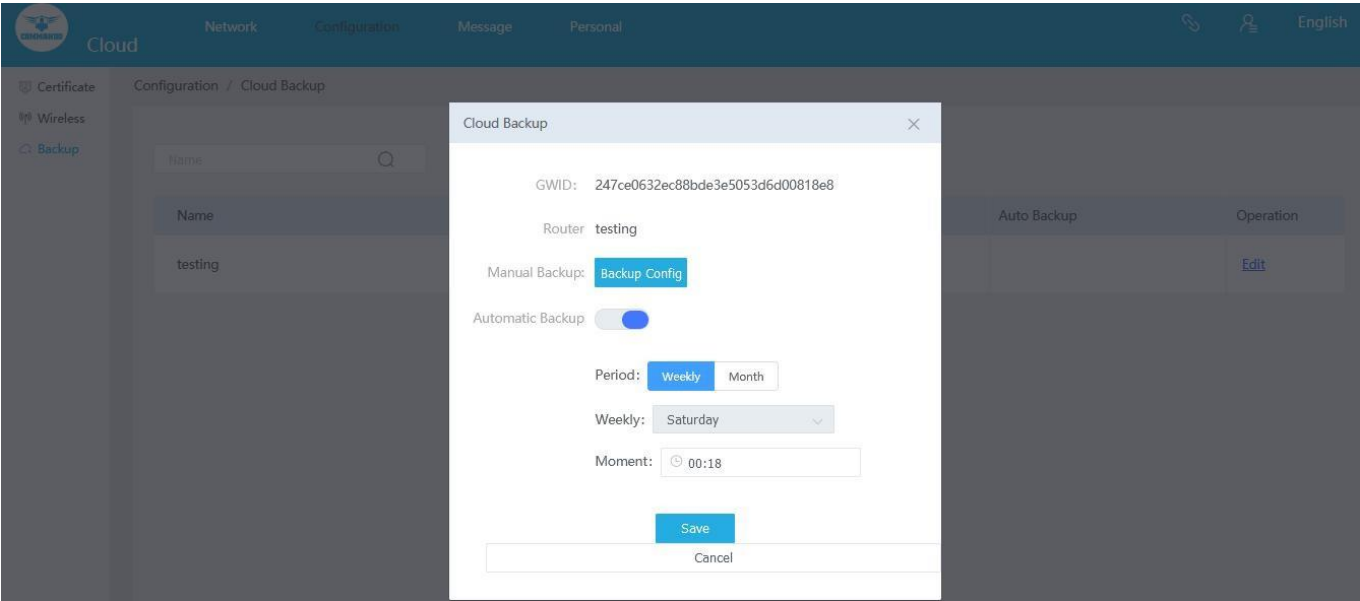
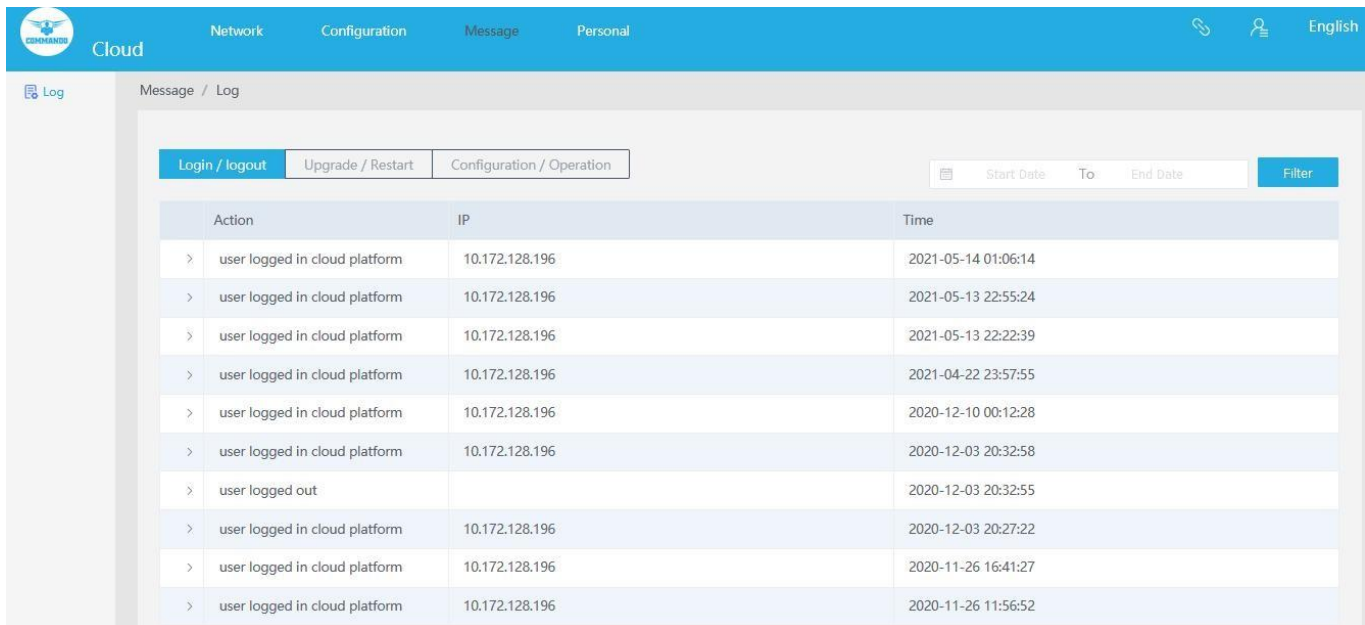


Fig 6.3.19 Default Cloud Backup Configuration setting page

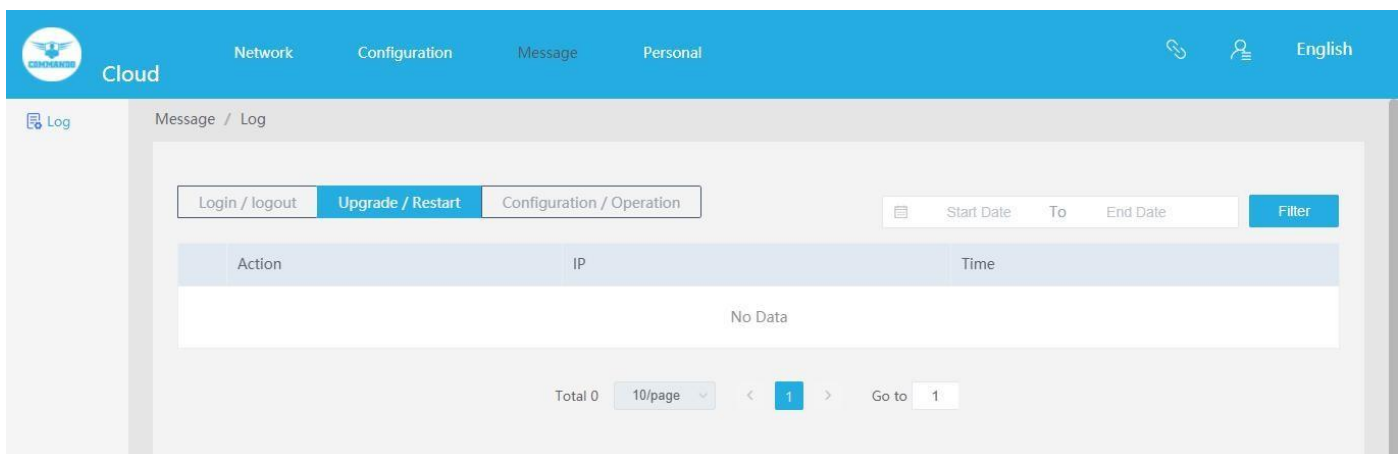
1.4 Message

Messages can be Log, Login or logout, Upgrade or Restart and Configuration or Operation.



Action	IP	Time
> user logged in cloud platform	10.172.128.196	2021-05-14 01:06:14
> user logged in cloud platform	10.172.128.196	2021-05-13 22:55:24
> user logged in cloud platform	10.172.128.196	2021-05-13 22:22:39
> user logged in cloud platform	10.172.128.196	2021-04-22 23:57:55
> user logged in cloud platform	10.172.128.196	2020-12-10 00:12:28
> user logged in cloud platform	10.172.128.196	2020-12-03 20:32:58
> user logged out		2020-12-03 20:32:55
> user logged in cloud platform	10.172.128.196	2020-12-03 20:27:22
> user logged in cloud platform	10.172.128.196	2020-11-26 16:41:27
> user logged in cloud platform	10.172.128.196	2020-11-26 11:56:52

Fig 6.4.1 Default Login and Logout page



Action	IP	Time
No Data		

Total 0 10/page < 1 > Go to 1

Fig 6.4.2 Default Upgrade and Restart page

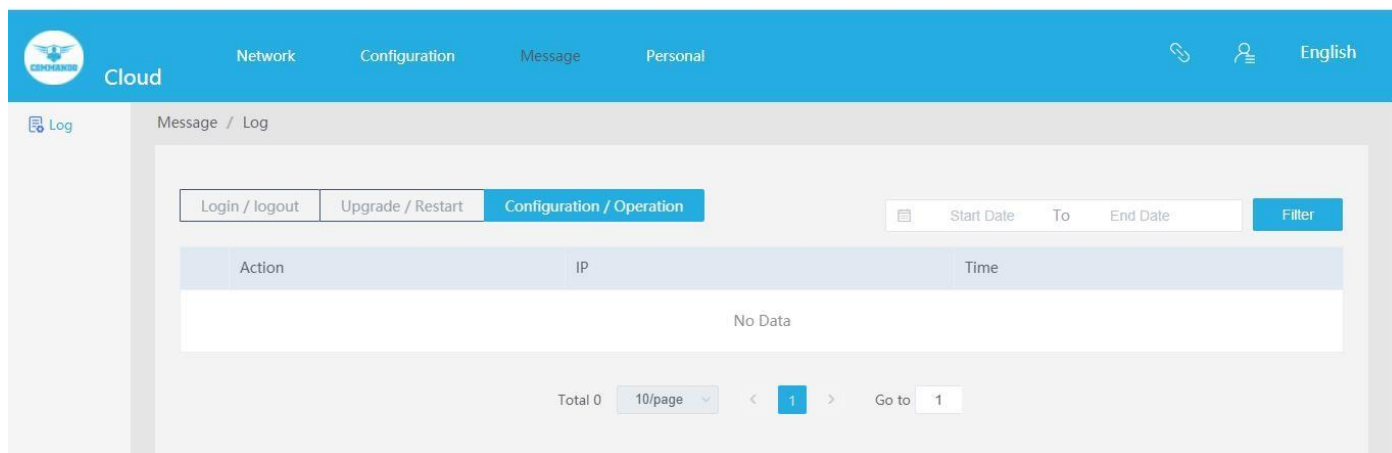


Fig 6.4.3 Default Configuration and operation page

Cloud Management Interface - Configuration / Operation

Navigation: Network, Configuration, Message, Personal

Filter: Start Date To End Date

Action	IP	Time
> Close authentication	10.172.128.196	2022-09-15 13:31:26
> Open authentication	10.172.128.196	2022-09-15 13:27:12
> Delete template successfully	10.172.128.196	2022-09-14 22:58:54
> Close authentication	10.172.128.196	2022-09-14 22:58:49
> Open authentication	10.172.128.196	2022-09-14 22:54:49
> Close authentication	10.172.128.196	2022-09-14 22:54:24
> Modify the template successfully	10.172.128.196	2022-09-14 22:51:40
> Delete template successfully	10.172.128.196	2022-09-14 22:51:31
> Add template successfully	10.172.128.196	2022-09-14 22:51:21
> Save certification	10.172.128.196	2022-09-14 22:50:50

Fig 6.4.4 Configuration and operation page

1.5 Personal

Personal Information is available on this page.

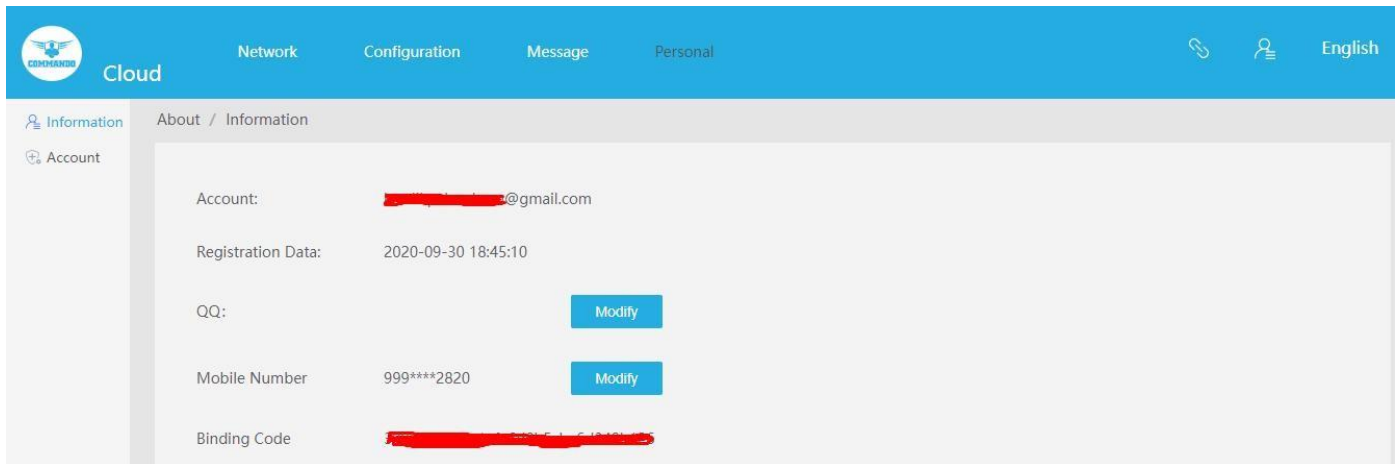


Fig 6.5.1 Default Personal Information page

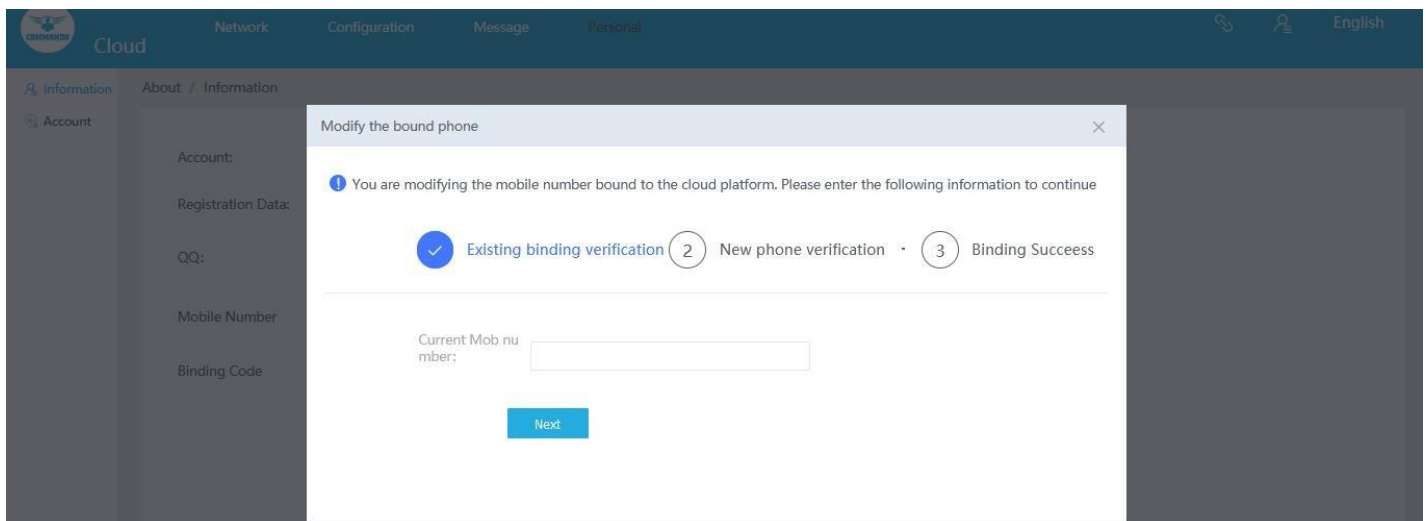


Fig 6.5.2 Modify Personal Information page

Frequently asked questions.

1. What are the differences between 802.11a/b/g/n/ac Standards?

Protocol	Frequency Band	Compatibility	Theoretical Rate	Actual Rate
802.11a	5 GHz	N/A	54 Mbit/s	About 22 Mbit/s
802.11b	2.4 GHz	N/A	11 Mbit/s	About 5 Mbit/s
802.11g	2.4 GHz	Compatible with 802.11b	54 Mbit/s	About 22 Mbit/s
802.11n	2.4 GHz, 5 GHz	Compatible with 802.11a/b/g	450 Mbit/s (three spatial flows)	About 80 to 220 Mbit/s
802.11ac	5 GHz	Compatible with 802.11a/n	1300 Mbit/s	250 Mbit/s to 400 Mbit/s

2. What is the category of copper cable?

The different categories denote the frequency at which the cable will pass or fail at a number of parameter tests. In theory, the higher the frequency, the more data (megabits per second/Mbps) you can transmit. The word Category is often abbreviated as Cat. The common network cables include Category 5 cable (Cat 5), Category 5 enhanced (Cat 5e), & Category 6 cable (Cat 6). These are twisted pair cables that use RJ45 connectors, with a maximum transmission distance of up to 250 meters. Network cables also include Category 1 cable (Cat 1), Category 2 cable (Cat 2), Category 3 cable (Cat 3), Category 4 cable (Cat 4), Category 6a (Cat 6a), and Category 7 cable (Cat 7). Generally, a higher category indicates a later version, more advanced technology, and higher bandwidth and cost.

Also, depending on whether the shield layer is available, the network category of cable cables changes. There are two types of cables namely, Shielded twisted pair (STP) and unshielded twisted pair (UTP). STP cables can reduce radiation and prevent information from being intercepted and external electromagnetic interference from entering. Compared with the same type of UTP cables, STP cables boast higher transmission rate, but they are more expensive and more difficult to install. UTP cables feature low cost, light weight, and are easy to bend.

They rarely cause great impact on common networks. UTP cables are more widely used. To practically implement a full-duplex transmission rate of up to 10 Gbps, recommended Category 7 with STP.

Category of cable	Transmission frequency	Distance Covered
Cat5e	Up to 100Mhz	Supports 1GE (Gigabit Ethernet/1000Mbps) up to 100m
Cat6	Up to 250Mhz	Supports 10GE up to 5-10m
Cat6a	Up to 500Mhz	Supports 10GE up to 30m
Cat7	Up to 600Mhz	Supports 10GE up to 100m
Cat7a	Up to 1000Mhz	Supports 10GE up to 250m

1. What is MIMO?

MIMO (Multiple-Input Multiple-Output) to multiply the capacity of radio links which consists of multiple trans and receive antennas to forward data at the simultaneously generates multiple spatial streams, The receiving antennas can take out the signal from different spatial paths and reconstruct the original signal which ultimately increases transfer rates of up to 600Mbps.

2. What Is Beamforming Technology?

Beamforming processes the signals sent by multiple antennas to generate a directional signal radiation pattern to boost signal from the transmitter helping to increase distance to receiver with improving in signal to noise ratio and ultimately increase signal coverage.

3. What are Beacon Interval, RTS Threshold?

Beacon Interval is the time between beacon frames transmitted by an access point. The AP radio will transmit one beacon for each SSID it has enabled at each beacon interval.. Beacon Interval determines the time interval of the beacon frames sent by the AP device. RTS Threshold is the packet size, in bytes, that requires the

AP to check the transmitting frames to determine if an RTS/Clear to Send (CTS) handshake is required with the receiving client.

4. What physical interfaces are generally used in networks?

Physical interfaces exist on interface cards and transmit service data. Physical interfaces are classified into the following types:

LAN Interface: They are 10/100/1000 Mbps ports to exchange data with network devices on LANs. The following are the common LAN interfaces used worldwide.

1. Fast Ethernet interface

A FE interface works at the data link layer, provides a maximum transmission rate of 100 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

2. Gigabit Ethernet interface

A GE interface works at the data link layer, provides a maximum transmission rate of 1000 Mbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

3. 10 Gigabit Ethernet interface

A 10GE interface works at the data link layer, provides a maximum transmission rate of 10 Gbit/s, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

4. Multi-GigE interface

It is an Ethernet electrical interface that can work at the rate of 1000 Mbps, 2500 Mbps, 5000 Mbps, or 10000 Mbps.

5. 40 Gigabit Ethernet interface

A 40GE interface works at the data link layer, provides a maximum transmission rate of 40 Gbps, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

Management interface: Management interfaces are used to log in to switches for

configuration and management purposes.

USB interface: It is generally data transmission interface. You can perform USB based deployment on a switch through this interface.

Mini USB interface: It is a data transmission interface as well as management interface. You can perform basic configuration and management on a switch through this interface.

Monitoring Interface: Monitoring interfaces are used to monitor a switch's components, including the cabinet door, power supply, and backup power supply.

Console interface: The console interface is connected to the COM serial interface of a configuration terminal to set up an on-site configuration environment. This interface can be connected to a network interface of a configuration terminal or network management workstation to set up an onsite or remote configuration environment.

Out of band Eth interface: This interface can be connected to a network interface with RJ45 cable of a configuration terminal or network management workstation to set up an onsite or remote configuration environment.

Optical Interfaces: In a fiber optic communications link, a point at which an optical signal is passed from one equipment or medium to another without conversion to an electrical signal. Depending on transmission rates, optical modules are classified into 100G, 40G, 10G, and 1G optical modules.

7. What logical interfaces are generally used in networks?

Logical interfaces do not physically exist. They are manually configured and can be used to exchange data and transmit service data.

Trunk Interface: A Trunk has Layer 2 and Layer 3 features and is formed by binding multiple Ethernet interfaces to provide more bandwidth and higher transmission

reliability.

Tunnel interface: A tunnel interface has Layer 3 features, transmits packets, & identifies and processes packets transmitted over a tunnel.

VLAN interface: A VLAN interface has Layer 3 features and enables VLANs to have gateway IP.

Ethernet Sub interface: An Ethernet sub-interface is configured on a main interface to allow the local L3 device to communicate with multiple L2 devices.

Loopback interface: A loopback interface is always UP and can be configured with a 32-bit subnet mask.

NULL interface: A null interface is used to filter routes because any data packets received by the null interface are discarded

NVE interface: An NVE interface is the logical interface to establish VXLAN tunnels with other NVE devices.

VBD interface: A VBD interface is the virtual interface based on a BD to support Layer 3 features and implement communication between different BDs, between BD and non- BD networks, and between BDs and Layer 3 networks.

Virtual Ethernet (VE) interface: A VE interface is used when other data link layer protocols need to be carried by the Ethernet protocol. A VE sub-interface can be created to allow an L2VPN to access an L3VPN.

Layer 2 Interface: A L2 interface can act a switchport decides how to forward data based on the MAC address. They can only forward the received packets in Layer 2 switching mode or join VLANs to forward the packets in Layer 3 routing mode through VLAN interfaces.

Layer 3 Interface: Layer 3 interfaces forward packets to another device using static or

dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter VLAN routing of Layer 2 traffic. IP addresses can be configured for these interfaces. They can forward the received packets in Layer 3 routing mode. That is, they can send and receive packets whose source and destination IP addresses are located in different segments.

8. What are different types of VLAN within a private VLAN?

Primary VLAN: It can forward the traffic from the promiscuous ports to isolated ports, community ports and other promiscuous ports in the same private VLAN.

Community VLAN: It is a secondary VLAN. It forwards traffic between ports which belong to the same community and to the promiscuous ports. There can be multiple community VLANs per private VLAN.

Isolated VLAN: It is a secondary VLAN. It carries traffic from isolated ports to promiscuous ports.

9. What is ARP & how it works?

The basic purpose of the Address Resolution Protocol (ARP) is to resolve IP addresses to Ethernet mac addresses. It is the method by which any node or interface on a LAN can dynamically learn the MAC address of another IP host or router on the same LAN. The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

ARP Request, is a message that makes the simple request “if this is your IP address, please reply with your MAC address.” ARP also defines the ARP Reply message, which indeed lists both the original IP address and the matching MAC address. It is used to dynamically map layer-3 network addresses to data-link addresses. The ARP cache is vulnerable to ARP cache poisoning and ARP spoofing attacks. ARP table for all devices connected to it. The ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The device creates dynamic addresses from the ARP packets it receives.

10. How does DHCP Server work?

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. DHCP (dynamic host configuration protocol) allows a server to assign an IP address to a computer from a preselected range of numbers configured for a particular network. Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring IP addresses, gateways and other IP related things automatically to connected hosts. DHCP Host/client generally require four IPv4 settings namely IP address, Subnet mask, Default Gateway IP and optional DNS server IP addresses. You can customize the DHCP pool subnet and address range to provide simultaneous access to a greater number of clients. DHCP allows the permanent assignment of host addresses, but more commonly, DHCP assigns a temporary lease of IP addresses. With these leases, the DHCP server can reclaim IP addresses when a device is removed from the network, making better use of the available addresses. DHCP also enables mobility by mac to IP binding.

GLOSSARY

ACL: Access Control List can limit network traffic and restrict access to certain users, ports or mac by allowing and disallowing based on L2/L3/L4 information.

ALG: Application Level Gateway (ALG) is an application specific translation agent that allows an application on a host in one address domain to connect to its receiver port running on a host in different address domain. It allows client applications to use dynamic TCP/UDP ports to communicate with known ports used by server applications.

AH: Authentication Header provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality.

ARP: Address Resolution Protocol used to map an IP address to a MAC address in short converts between IP addresses and MAC addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP: Boot Protocol is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CFM: Connectivity Fault Management provides fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

COS: Class of Service is supported by prioritizing packets based on the required level of service and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence

bit, or DSCP priority bit.

DDNS: DDNS (Dynamic Domain Name Server) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DDNS

configuration of its configured hostnames, addresses capability of assigning a fixed host and domain name to a dynamic Internet IP address.

DHCP: Dynamic Host Control Protocol provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP SNOOPING: It is used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DIFFSERV: Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS: Domain Name Service used for translating host names for network nodes into IP addresses.

DMZ: DMZ (Demilitarized Zone) allows local hosts exposed to the Internet (untrusted Networks) additional protection and adds an extra layer of security to an organization's

internal local-area network from untrusted traffic. The main goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure.

DSCP: Differentiated Services Code Point Service uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

DSL: Digital Subscriber Line that allows data to be sent or received over existing traditional phone lines that use existing telephone lines to transport high-bandwidth data, Voice and video, to service subscribers. DSL provides dedicated, point-to-point, public network access.

EAPOL: Extensible Authentication Protocol over LAN is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A username and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

ERPS: Ethernet Ring Protection Switching can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.

ESP: Encapsulating Security Payload provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

EUI: Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is

based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

FTP: File Transfer Protocol is a application layer protocol, is a way to download, upload, and transfer files on the internet or privet networks between computer systems. It allows transfer of files back and forth between VPN's, cloud or public networks.

GARP: Generic Attribute Registration Protocol is a protocol that can be used by end stations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered end stations.

GMRP: Generic Multicast Registration Protocol allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GMT: Greenwich Mean Time also World Time, UTC nominally reflects the mean solar time along the Earth's prime meridian. Network Time Protocol (NTP) is a protocol that allows the synchronization of system clocks which is very convenient for log and troubleshooting purposes for events in networks.

GVRP: GARP VLAN Registration Protocol is a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

H.323: H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. It defines a common set of CODECs, call setup, negotiating procedures, and basic data transport methods.

HTTP: Hypertext Transfer Protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

ICMP: Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feedback information about better routing choices.

IEEE 802.1D: Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q: VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P: An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1S: An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1W: An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard now incorporated in IEEE 802.1D-2004.

IEEE 802.1X: Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC: Defines frame extensions for VLAN tagging.

IEEE 802.3X: Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP: Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

IGMP QUERY: On each subnetwork, one IGMP-capable device will act as the querier that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP PROXY: Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in a simple tree that uses IGMP Proxy.

IGMP SNOOPING: Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT: Management of the network from a station attached directly to the network.

Internet: INTERNET stands for Interconnected Network systems that connects millions of web servers which provides a variety of information and communication facilities

with standardized communication protocols.

IP MULTICAST FILTERING: A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE: The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default but may be configured differently to suit the requirements for specific network applications.

ISP: Internet Service Provider provides individuals or organizations access to the internet and other telecom related services. An ISP has the equipment to have a point of presence on the internet for the geographic area served.

LACP: Link Aggregation Control Protocol allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2: Data Link layer in the ISO OSI 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LAN: Local Area Network is a collection of devices connected in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

LINK AGGREGATION: Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. It provides network redundancy by load-balancing traffic across all available trunk links.

LLDP: Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MAC address: Media Access Control address is a hardware identifier that uniquely identifies each device on a network.

MD5: Message-Digest 5 is an algorithm that is used to create digital signatures. It is intended for use with 32-bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB: Management Information Base is an acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MSTP: Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

MRD: Multicast Router Discovery is used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

Multicast Switching: A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR: Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-

demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

MTU: Maximum Transmission Unit is the largest-size frame or packet. MTU is the largest packet or frame size, specified in octets, Standard Ethernet supports an MTU of 1500 bytes and Ethernet implementation supporting jumbo frames, allowing for an MTU up to 10000 bytes.

NAT: Network Address Translator conserves IP addresses that are legally registered and prevents their depletion and provides security to access the internet with privacy by hiding the device IP address from the public network, even when sending and receiving traffic. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable addresses space.

NTP: Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical master slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio. NTP Server NTP Server is used for synchronizing the time across computer networks.

OAM: Operation, Administration, and Maintenance provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

OSPF: Open Shortest Path First (OSPF) is an open link state routing protocol. OSPF routers learn the entire network topology for their "area" (the portion of the network they maintain routes for, usually the entire network for small networks). OSPF routers send event driven updates. If a network is converged for a week, the OSPF routers will send no updates. OSPF has far faster convergence than distance vector protocols

such as RIP.

OUT-OF-BAND Management: The device can be accessed from a station not attached to the network.

PORT MIRRORING: A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be monitored.

PORT TRUNK: Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower speed physical links.

PRIVATE VLANs: Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QINQ Tunneling: It is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QOS: Quality of Service refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS: Remote Authentication Dial-in User Service is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP: Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol that has an AD value of 120 uses port number 520.

RMON: Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP and can set alarms on a variety of traffic conditions, including specific error types.

RSTP: Rapid Spanning Tree Protocol reduces the convergence time for network topology changes.

SMTP: Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP: Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP: Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server or can be received via broadcasts sent by NTP servers.

SSH: Secure Shell is a secure replacement for remote access functions, including the Telnet. SSH can authenticate users with a cryptographic key and encrypt data connections between management clients and the switch.

STA: Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+: Terminal Access Controller Access Control System Plus is a logon authentication protocol that uses software running on a central server to control access to TACACS compliant devices on the network.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET: It is a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP: Trivial File Transfer Protocol used for software/firmware downloads.

UDP: User Datagram Protocol provides a datagram mode for packet switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC: Universal Time Coordinate is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN: Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers and allows users to share information and resources as though located on the same LAN.

XMODEM: A protocol used to transfer files between devices. Data is grouped in 128- byte blocks and error-corrected.