



# COMMANDO RoutePRO R100-PRO Multi-Functional Router Web Configuration Guide



## INTRODUCTION

COMMANDO R100-PRO Cloud Base Multi-Functional Wired Router with 5\*10/100/1000M configurable LAN/WAN Ports, with functions like Router, 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 Multi WAN Load Balance, 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 and medium enterprise, Commercial set up where no down time affordable due to network issue, hotels and communities with 100+ volumes of users demanding a efficient and always UP network with high security. It is basically 5 in 1 Multi-functional 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, Wireless Controller for COMMANDO PRO Series AP, Cloud based authentication Configuration and monitoring, Enterprise Wired Router with features like static, Default and Dynamic connected route.

COMMANDO R100 PRO is multi-functional router 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 100 APs & unlimited 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 AirPRO 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.

R100 Functions can be broadly classified as follows:

### **Cloud Base Wired Router**

It is 5\* 10/100/1000M configurable and interchangeable LAN/WAN Port which support 100 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 4 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 Access Point Controller for COMMANDO PRO based AP, Support COMMANDO's PRO AP 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 IP-MAC 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.

### **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.

### **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 router connected to internet.

### **How to take access of COMMANDO R100?**

Connect any port of LAN (1-4) 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 any IP address from 192.168.1.2 to 254 to as shown below.

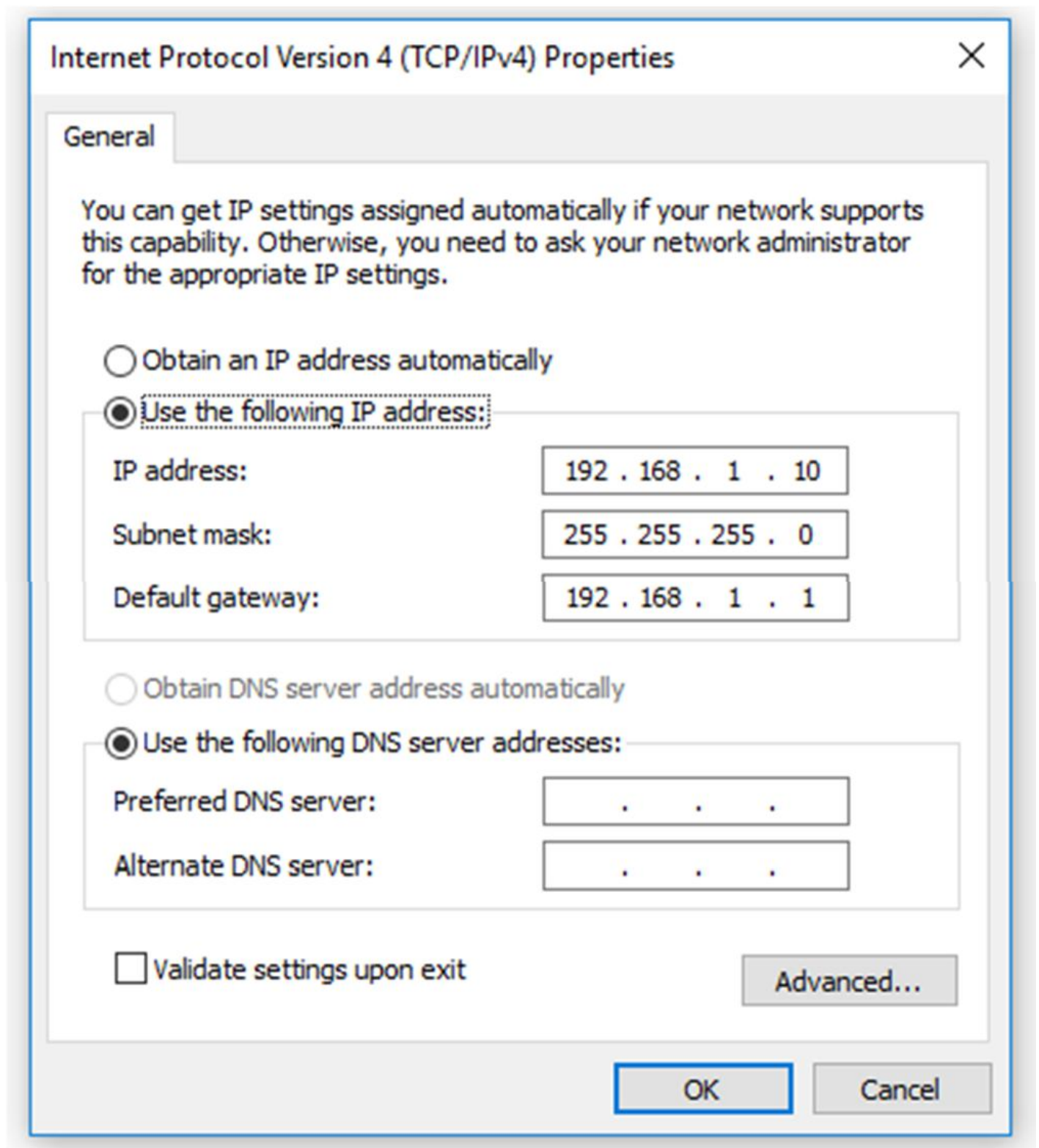
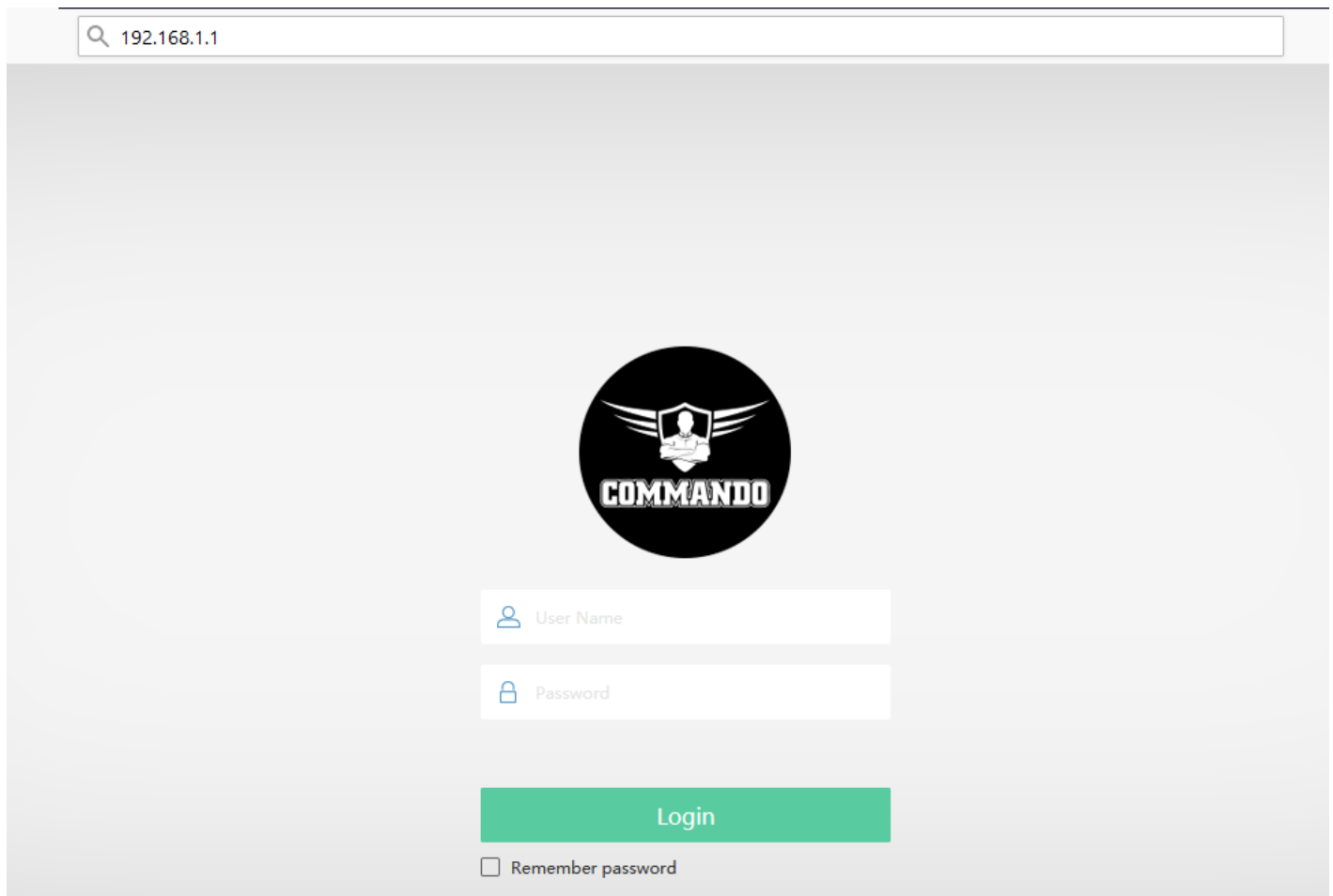


Fig 1. IP setting in PC connected to COMMANDO R100

Open any web browser like Chrome/Firefox/Internet Explorer/Opera etc. and enter default IP address 192.168.1.1 in address field.



**Fig 2. Login page for R100**

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.

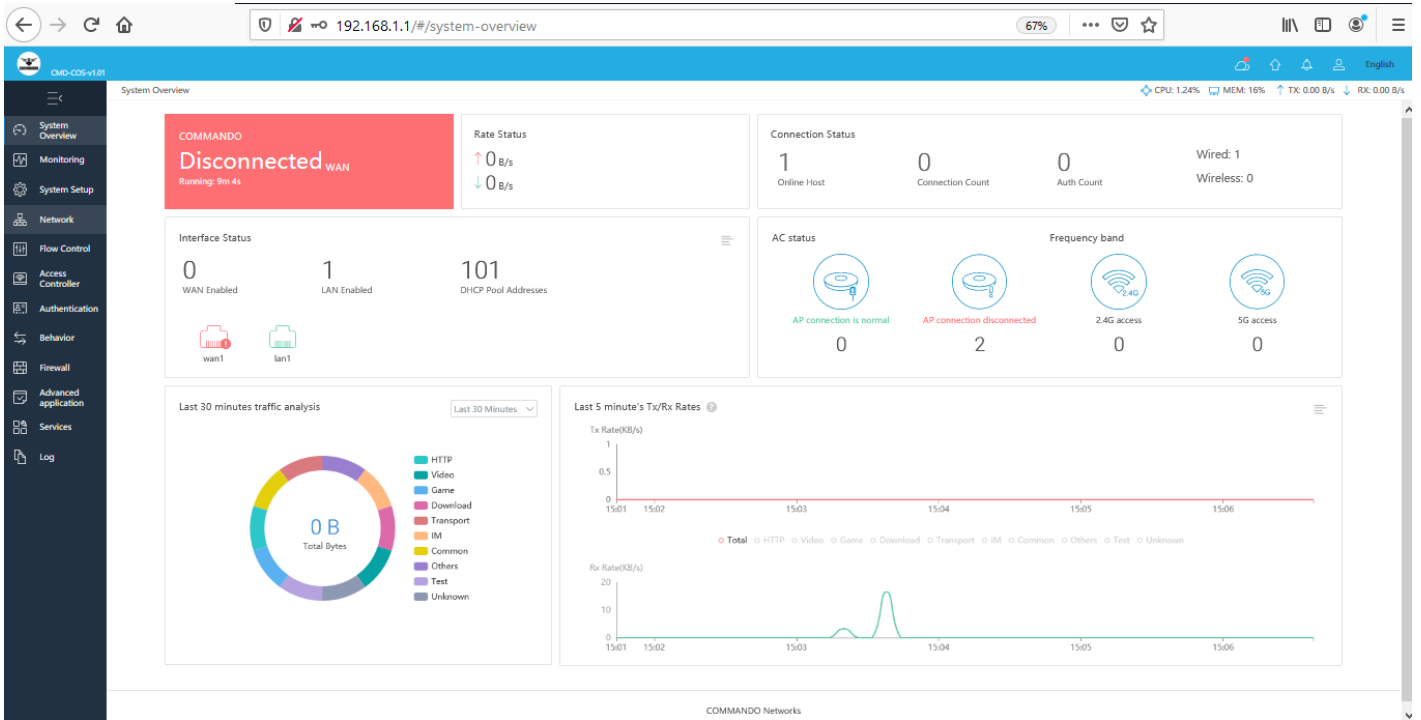


Fig 3. Default System Overview page

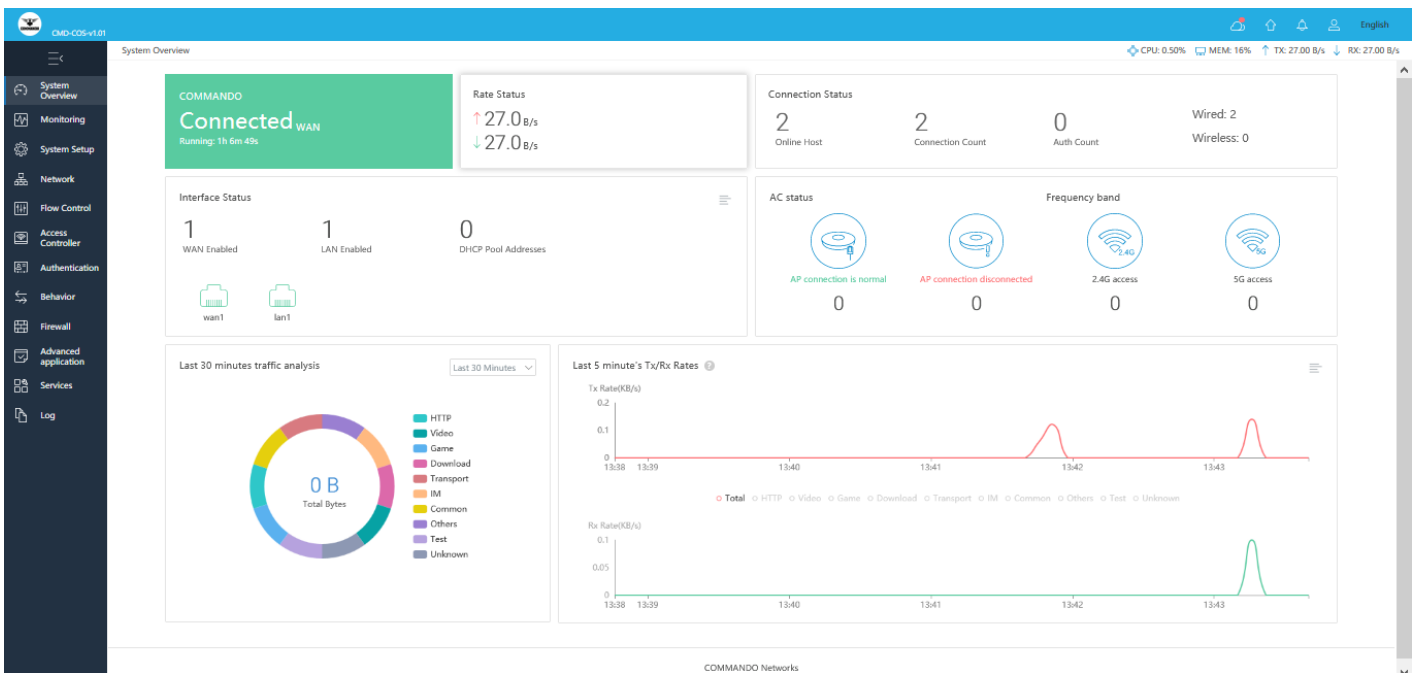
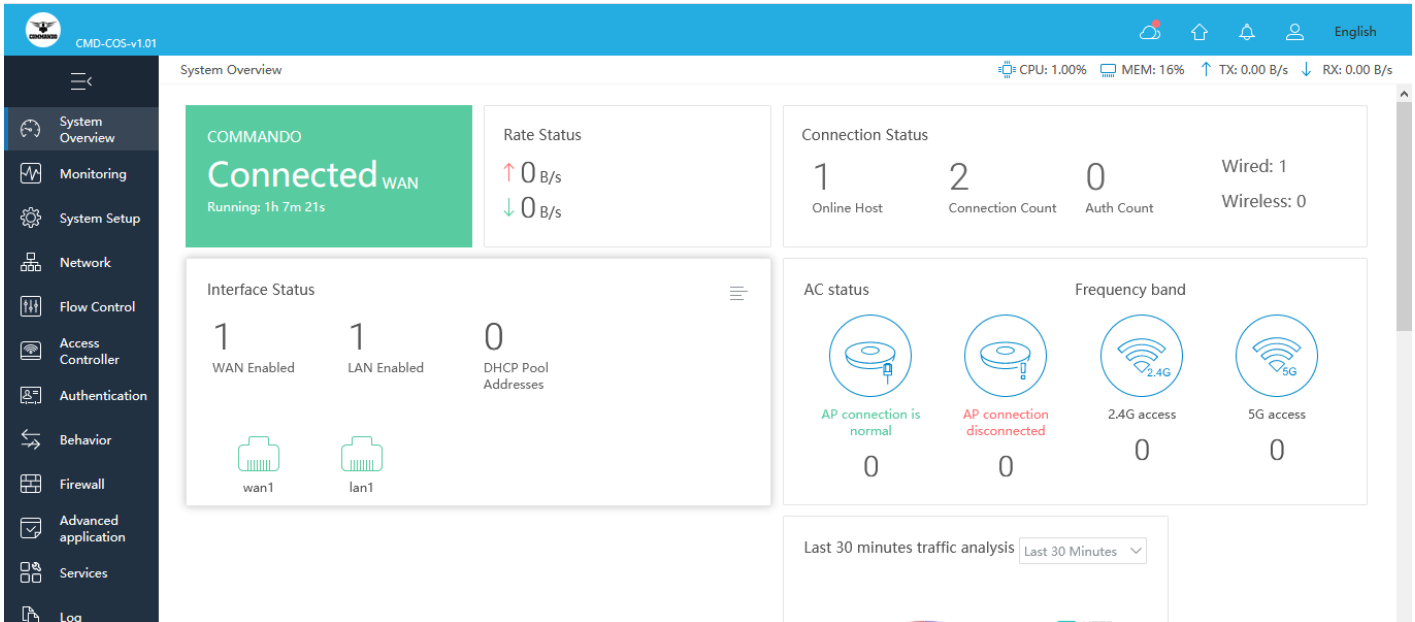


Fig 4. System Overview page after connecting LAN and WAN ports





**Fig 5. Connection status LAN and WAN ports**

I. 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.

## wan1 Default Gateway

---

Connection **Connected** 1052d 15h 9m  
Status:

Type: DHCP

IP: 192.168.1.38

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 192.168.1.1

MAC: 08:24:7c:e0:63:33

Remarks:

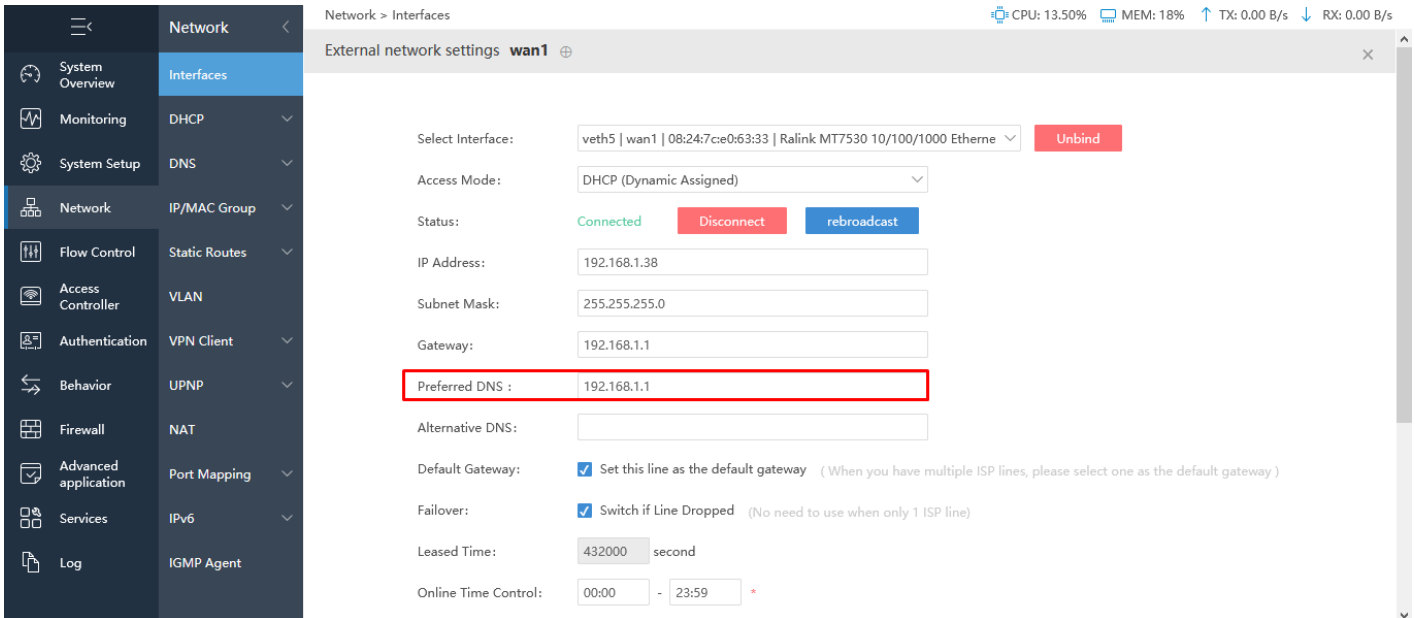
---

Bind Device: veth5/**Connected**/100Mbps/Full-Duplex

---

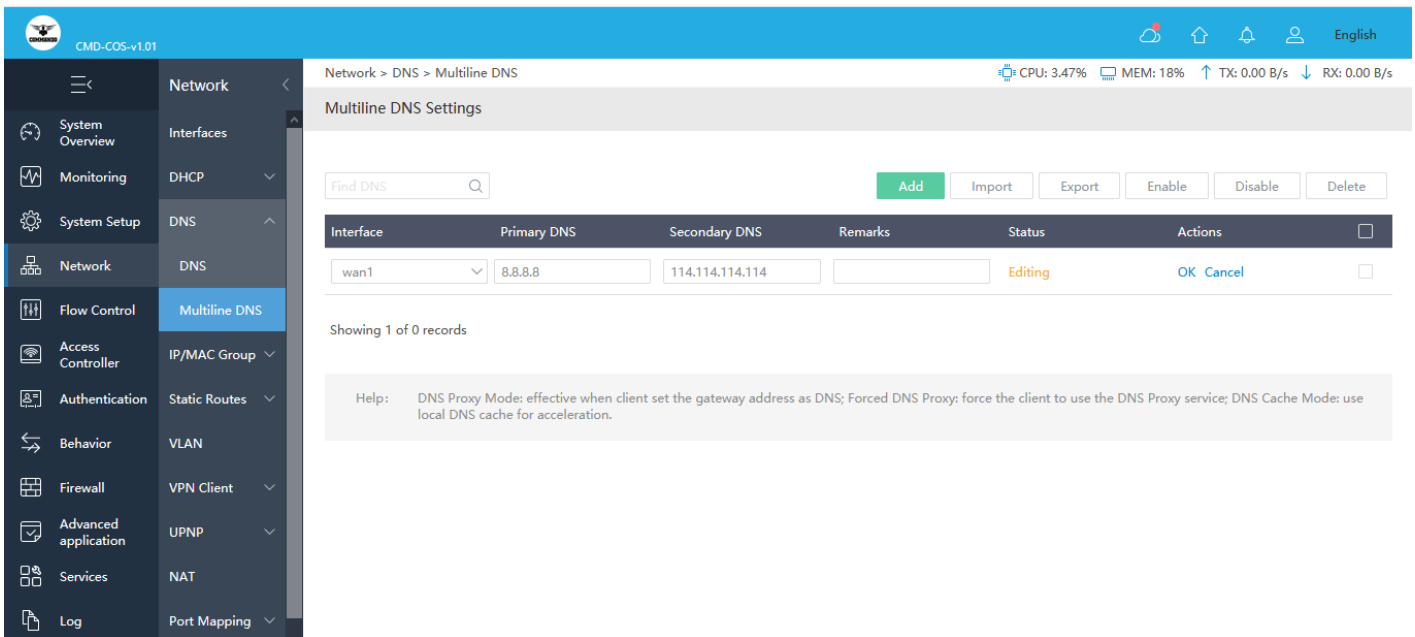
### Fig 6. Non-Proper DNS via DHCP Server

**Note:** Changed LAN IP and taken access of R100 via new set LAN IP as DHCP server in WAN is set as 192.168.1.0/24 network.



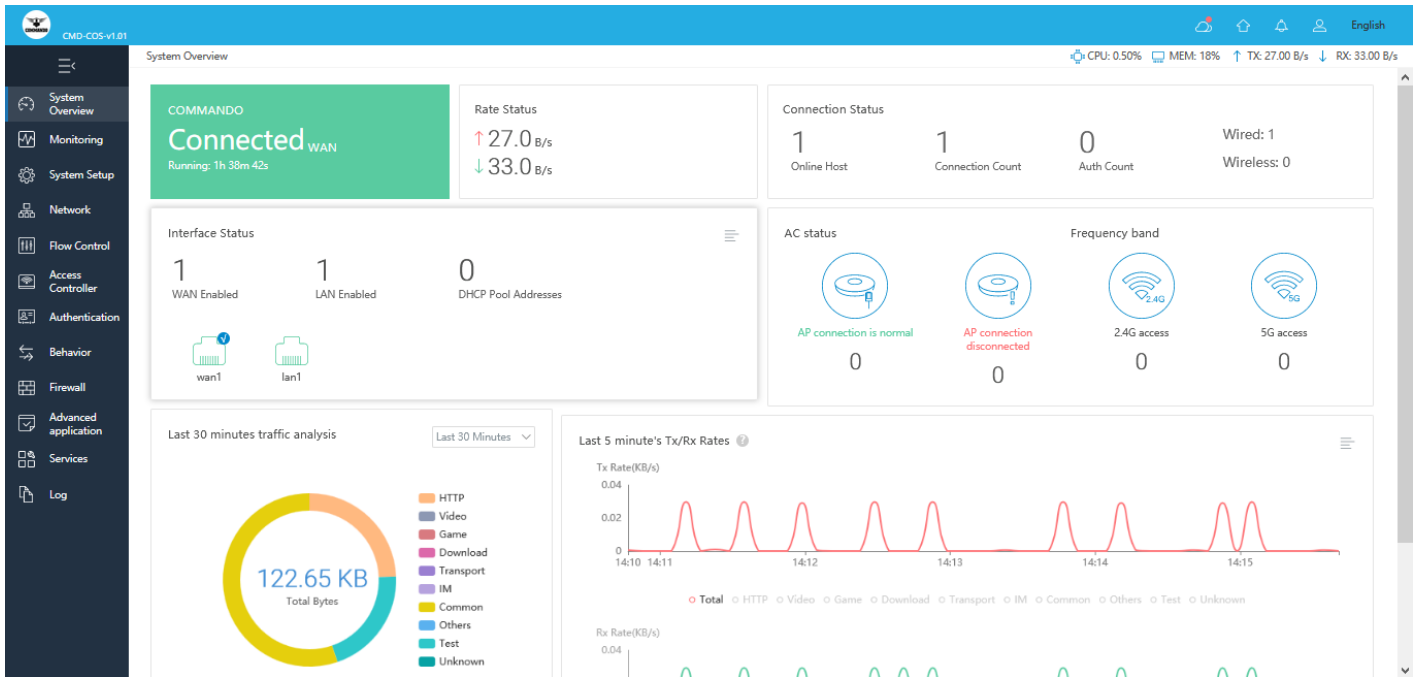
**Fig 7. WAN-1 Getting 192.168.1.1 as preferred DNS server IP automatically**

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



**Fig 8. Multi DNS server Setting in R100.**

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.

Last 30 minutes traffic analysis

Last 30 Minutes

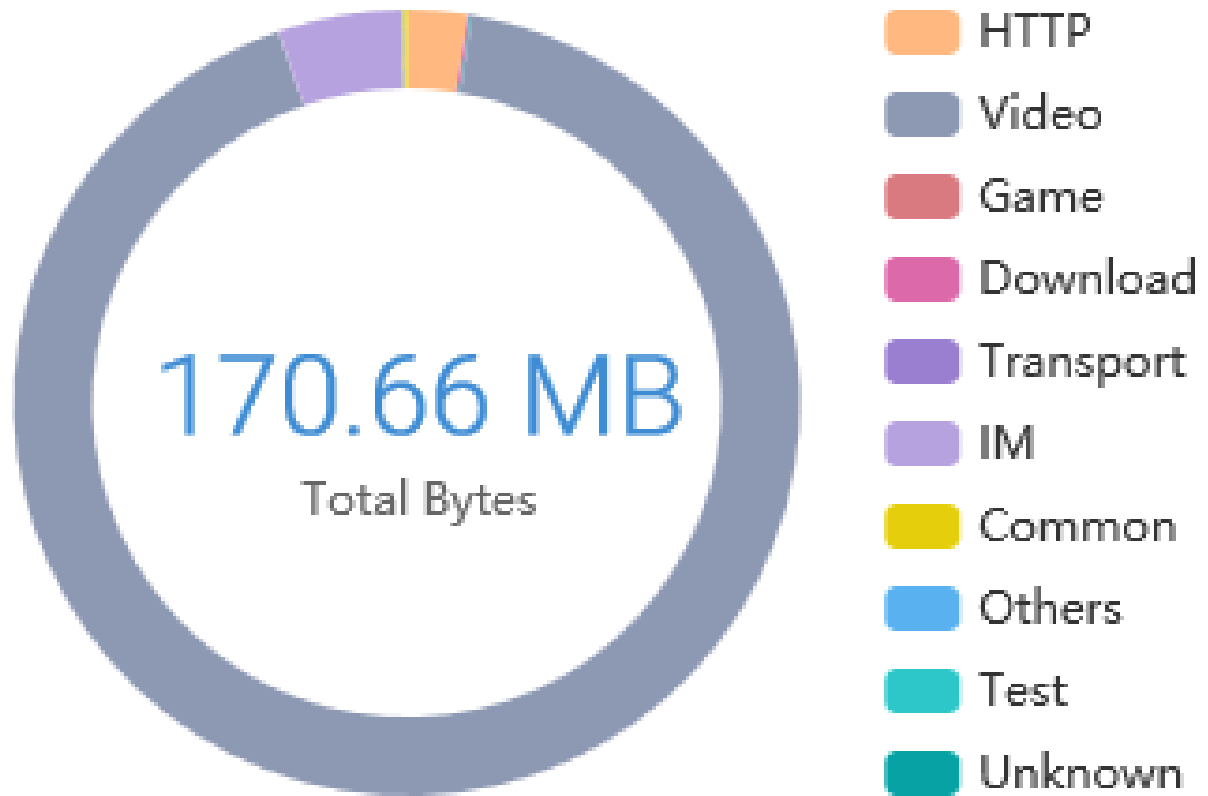


Fig 10. Traffic analysis for all application from last 30 minutes.

# Last 1 day protocol flow distribution

Last 1 Day ▼



- HTTP
- Video
- Game
- Download
- Transport
- IM
- Common
- Others
- Test
- Unknown

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.

A red rectangular border containing the text "Account Settings" in a blue, pixelated font.

Account  
Settings

Remote Access

Actions Logs

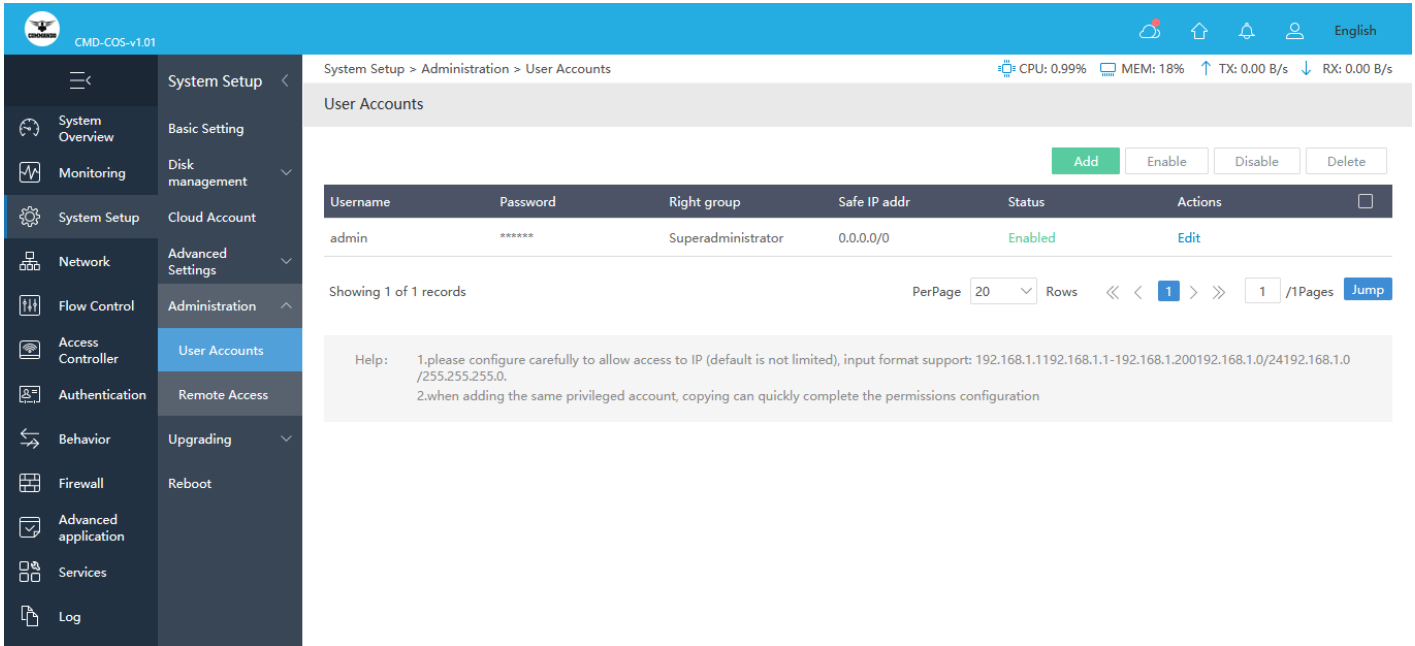
---

Logout

**Fig 13. Account setting icon**

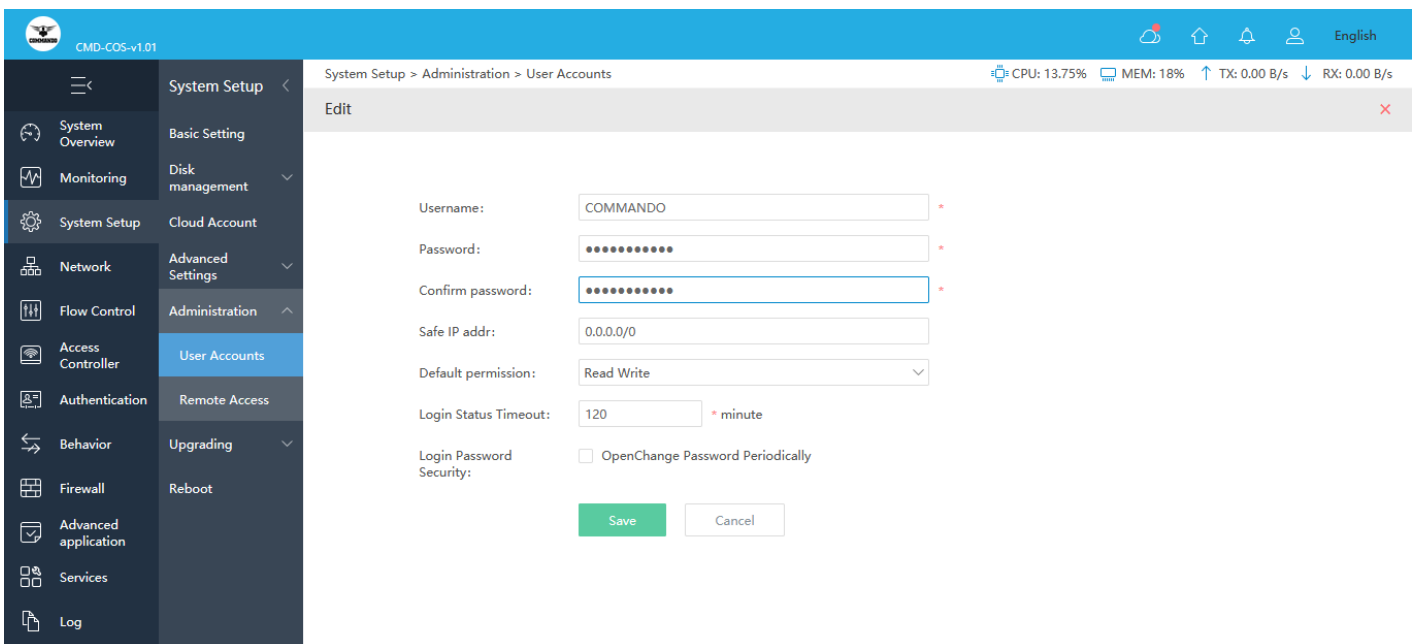
After clicking on account setting Icon user will be redirected to page System Setup > Administration > User Accounts





**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**



 COMMANDO

 ●●●●●●●●●●|

Login

Remember password

Fig 16. Logging with New account

System Setup > Administration > User Accounts

CPU: 0.75% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

User Accounts

Buttons: Add, Enable, Disable, Delete

Username	Password	Right group	Safe IP addr	Status	Actions
COMMANDO	*****	Superadministrator	0.0.0.0/0	Enabled	Edit

Showing 1 of 1 records

PerPage: 20 Rows: 1 / 1Pages: Jump

Help: 1.please configure carefully to allow access to IP (default is not limited), input format support: 192.168.1.1192.168.1.1-192.168.1.200192.168.1.0/24192.168.1.0/255.255.255.0.  
2.when adding the same privileged account, copying can quickly complete the permissions configuration

**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.

Account  
Settings

Remote Access

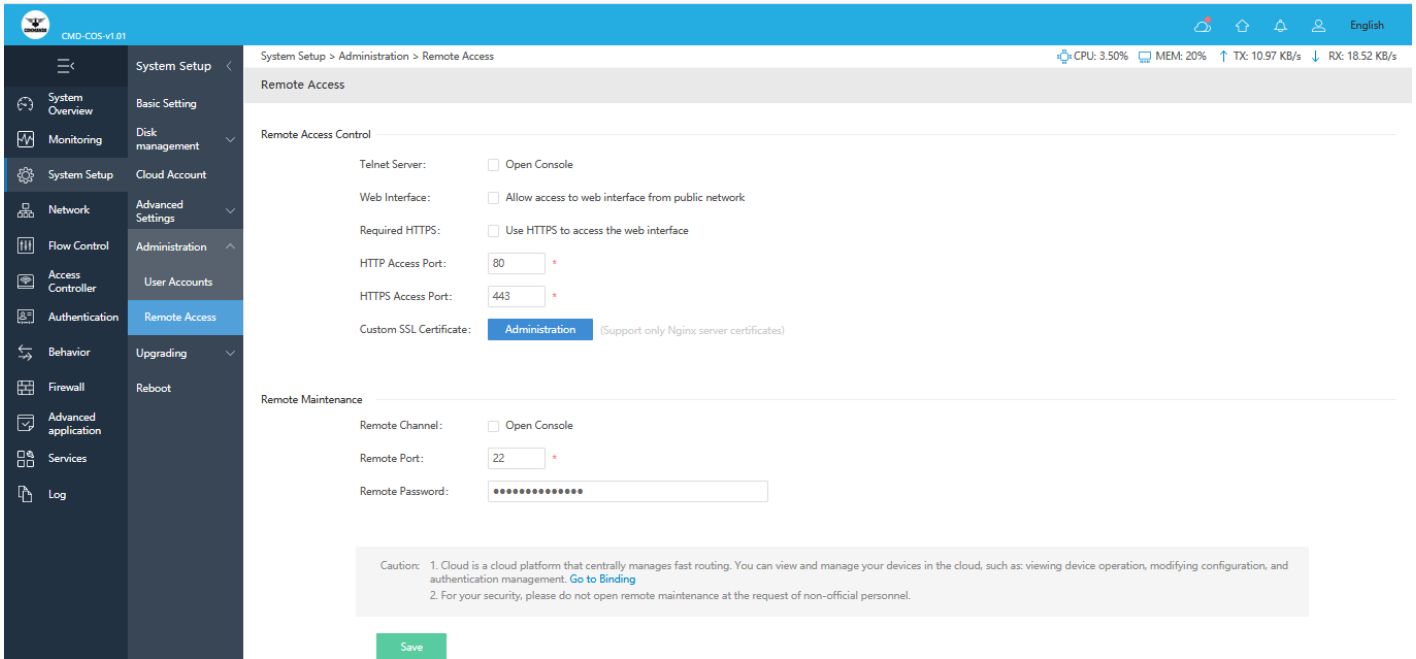
Actions Logs

---

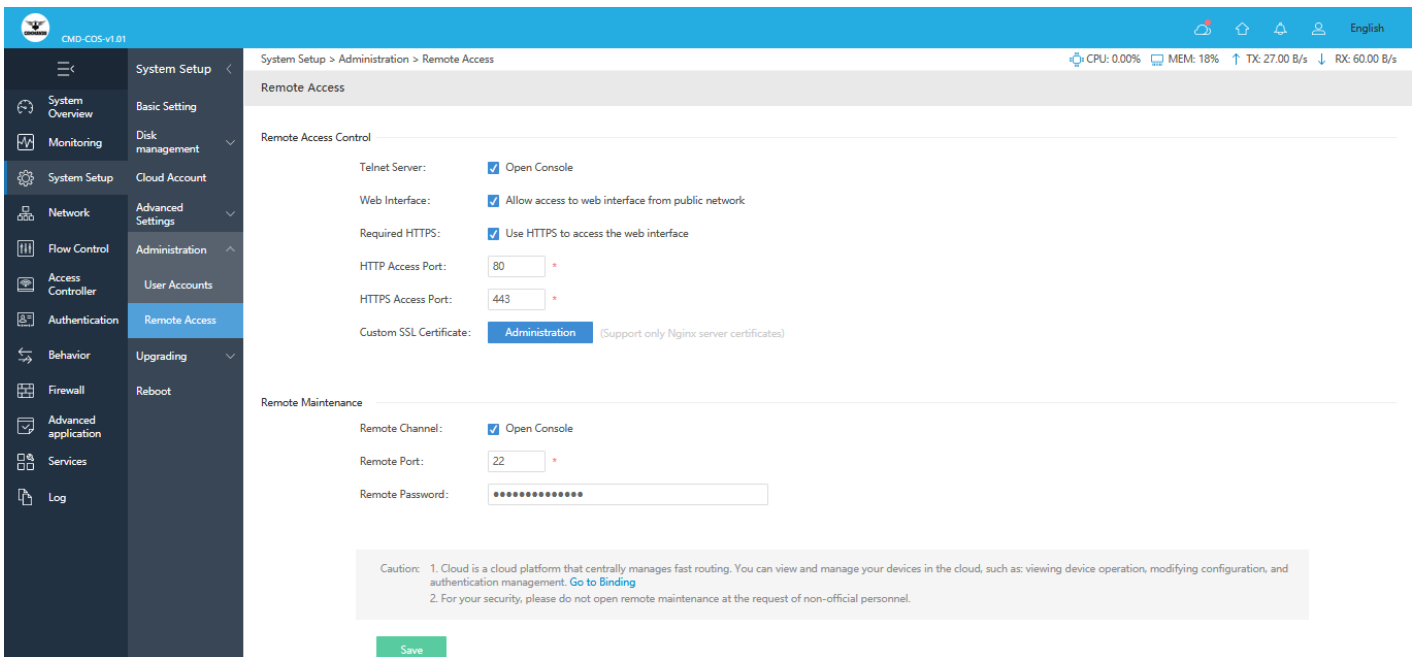
Logout

**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://192.168.0.1:8
0
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 |

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 R100**

**Action Logs:**

The Log system of Router can record, classify and manage the system information effectively.



# Account Settings

## Remote Access



### Actions Logs

---

## Logout

**Fig 22. Action Logs shortcut**

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

Log > System Logs > Action Logs

CPU: 0.75% MEM: 20% TX: 4.92 KB/s RX: 53.00 KB/s

**Action Logs**

Begin Time End Time IP/Username Export Clean All

Time	Username	IP Address	Function	Event
2021-04-12 18:08:52	admin	192.168.1.41	--	Login
2021-04-12 17:55:13	admin	192.168.1.13	Interfaces	exec action for save
2021-04-12 17:55:04	admin	192.168.1.13	Interfaces	exec action for dhcp up
2021-04-12 17:54:46	admin	192.168.1.13	Interfaces	exec action for dhcp down
2021-04-12 17:53:21	admin	192.168.1.13	--	Login
2021-04-12 17:40:43	admin	192.168.1.13	--	Login
2021-04-12 17:40:24	admin	192.168.1.41	--	Login
2021-04-12 17:40:09	admin	192.168.1.41	--	Login
2021-04-08 18:46:37	admin	192.168.1.41	--	Login
2021-04-08 17:47:03	admin	192.168.1.41	--	Login
2021-04-07 18:51:08	admin	192.168.1.41	--	Login

**Fig 23. Action Logs in system logs to show the date, time, users, IP and interface to login in R100**

### Logout:

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



Account  
Settings

Remote Access

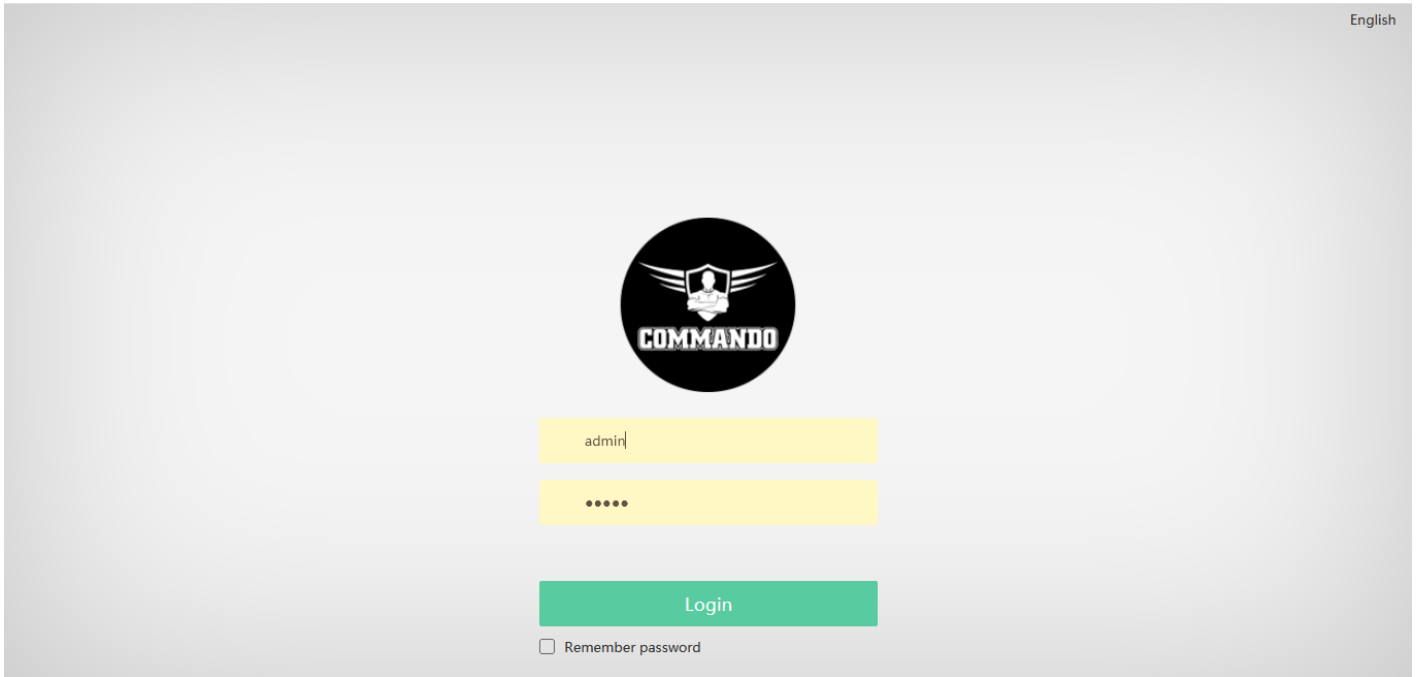
Actions Logs

---

Logout

**Fig 24. Logout shortcut**

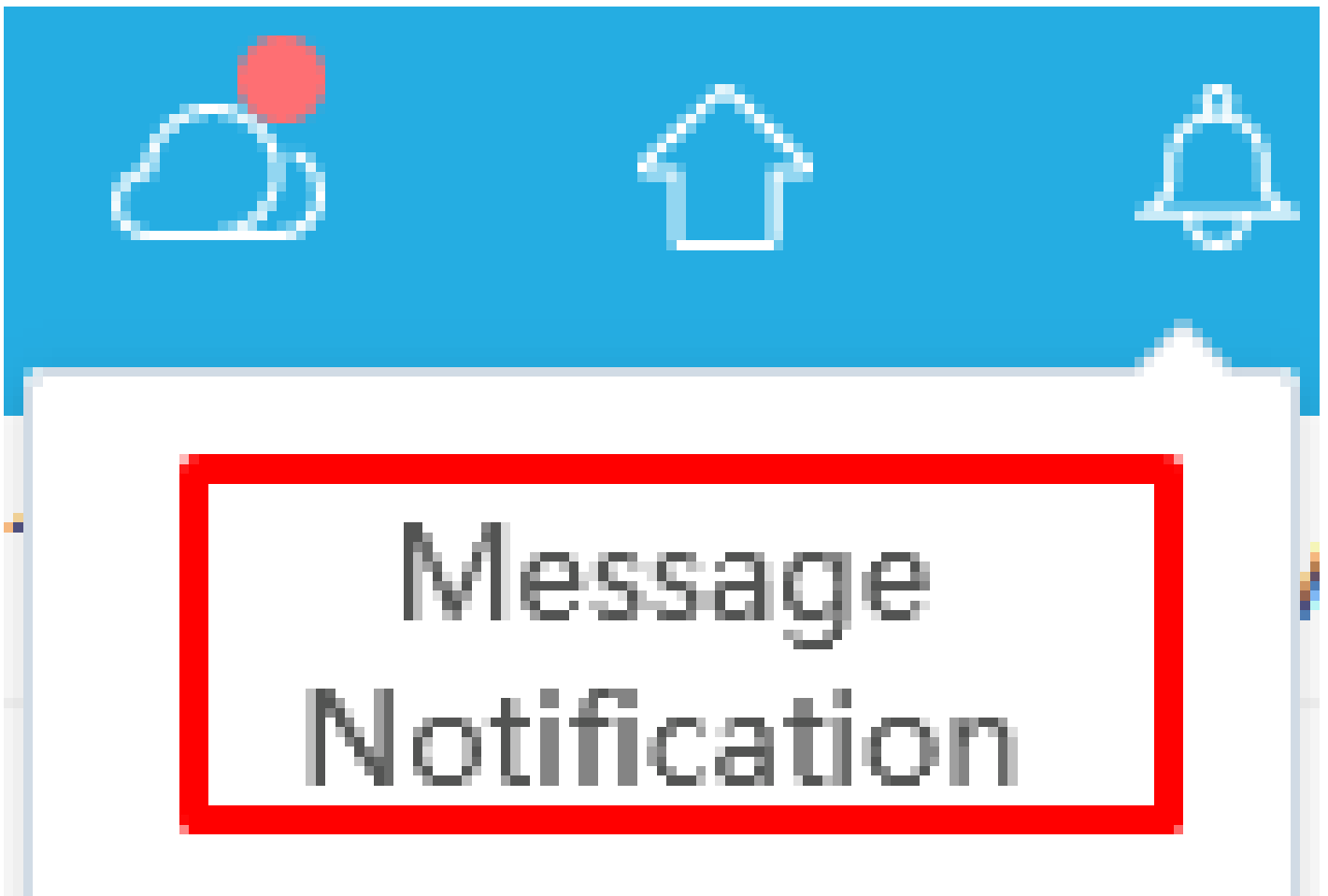
After Clicking Logout, it will be directed to Login page.



**Fig 25. Login page after Logout**

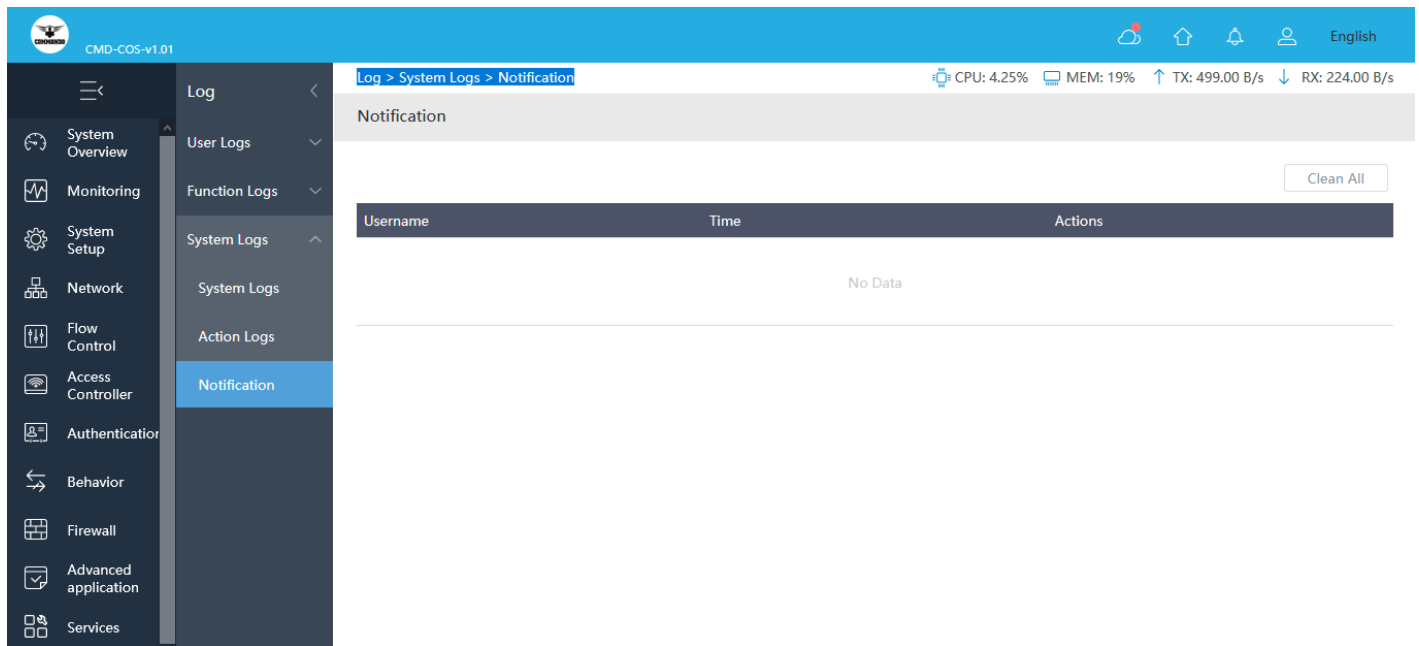
Message Notification:

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



## Fig 26. Message notifications Shortcut

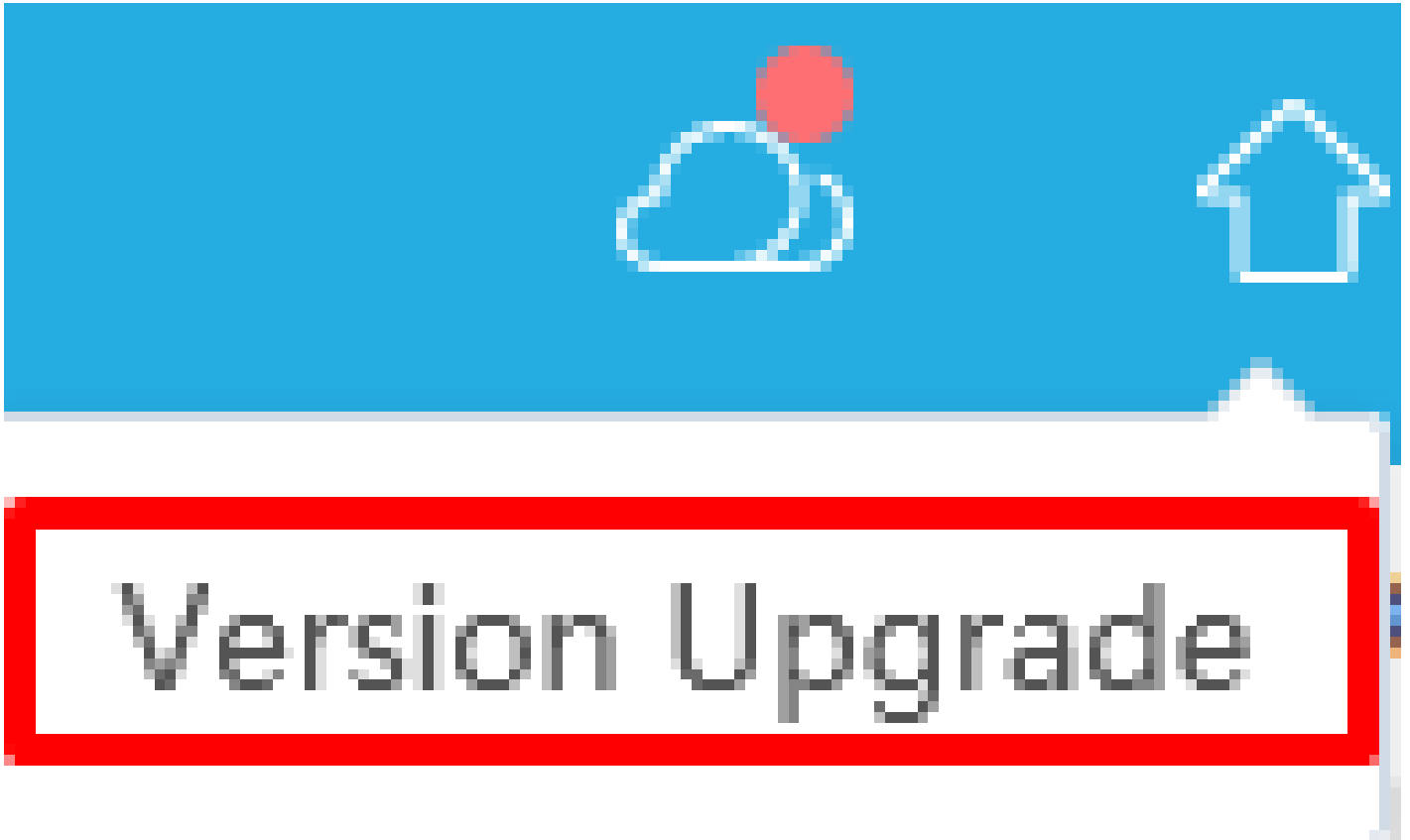
After clicking Message Notification, Log > System Logs > Notification page will be opened.



## Fig 27. Default Message notifications page

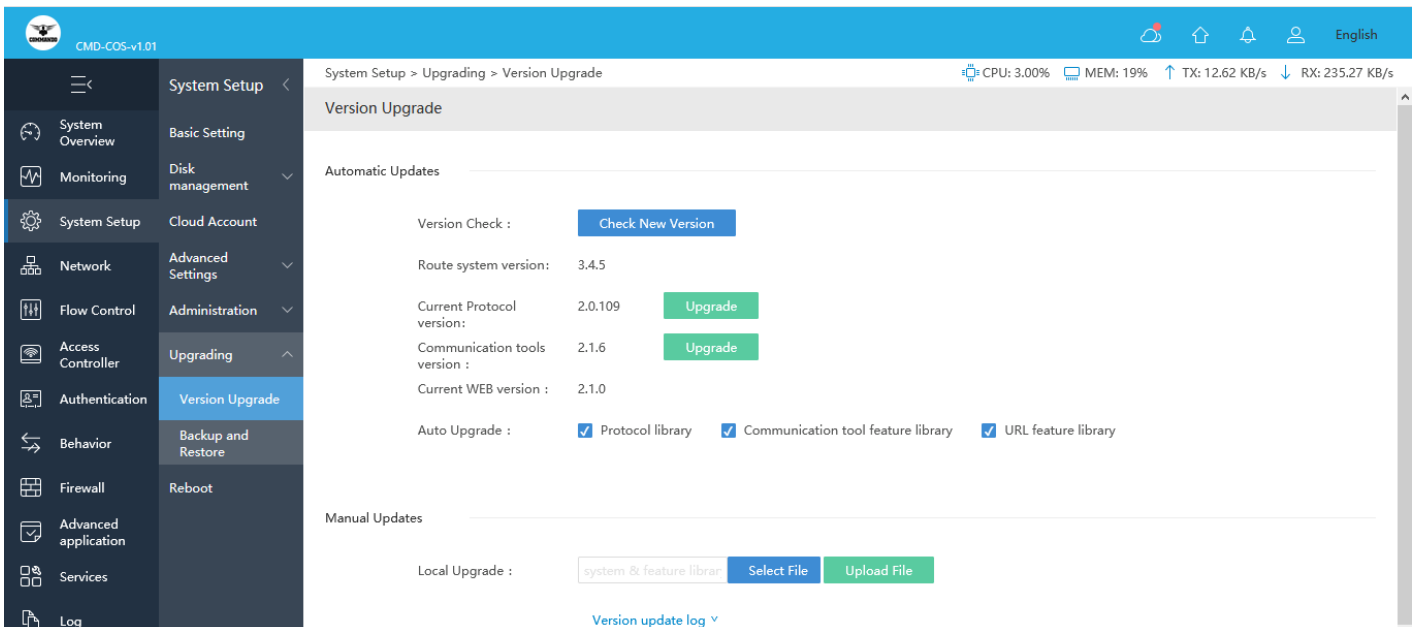
Version Upgrade:

Displays the current configuration version of the Router and allows Automatic or manual Updates.



**Fig 28. Version Upgrade page**

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

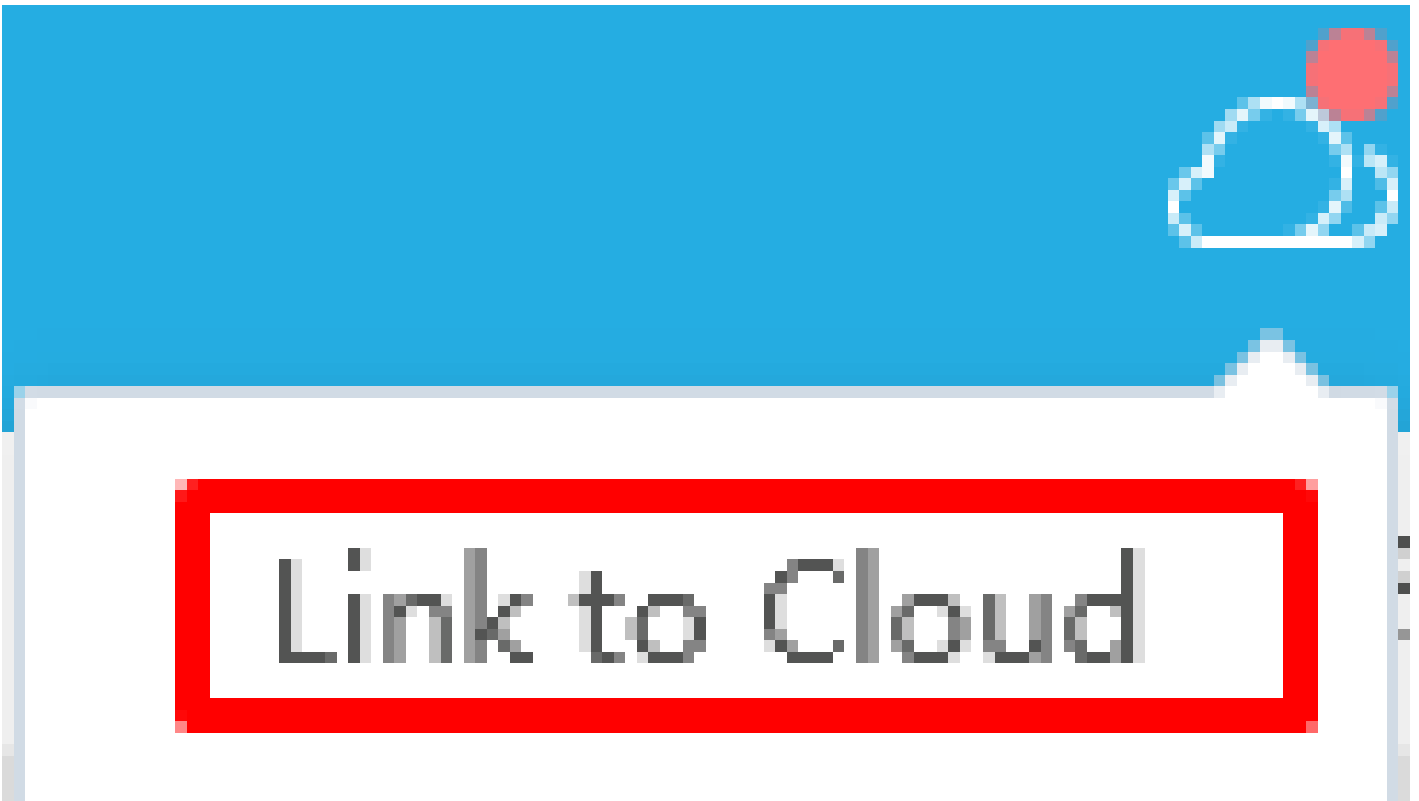


**Fig 29. Default Version Upgrade page**

**Link to Cloud:**

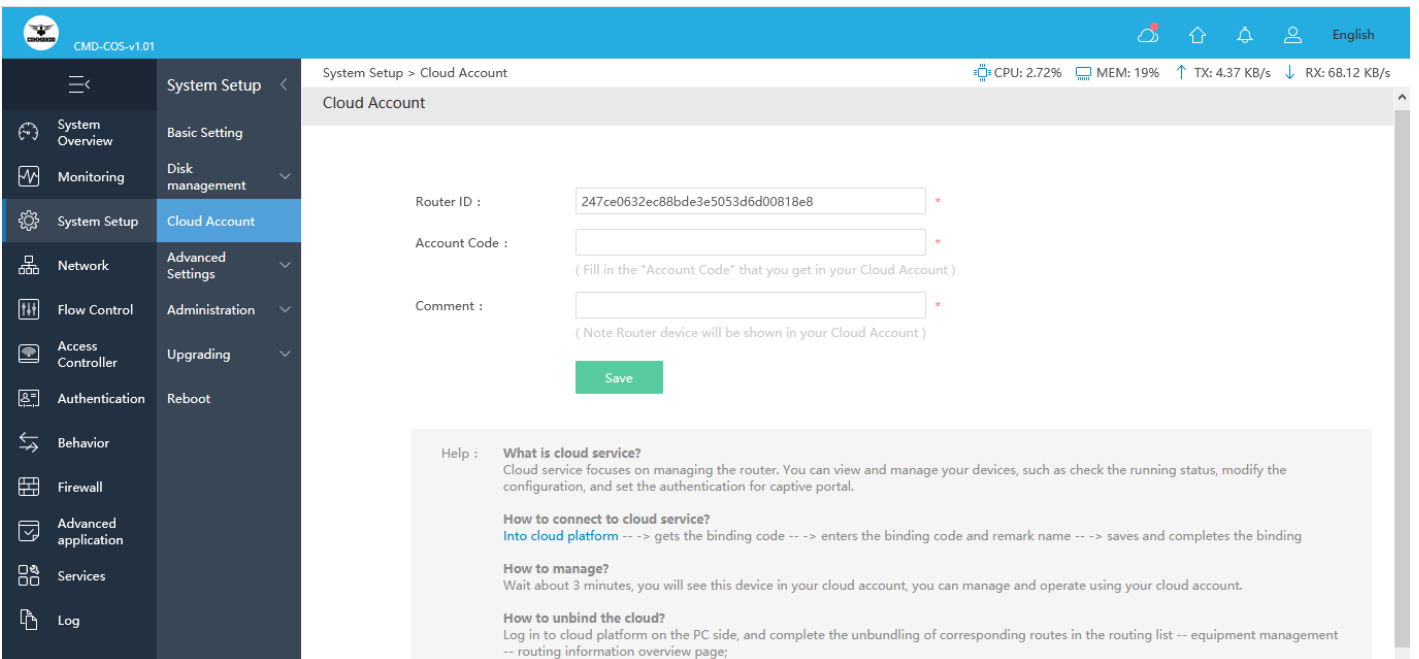
Cloud service helps users to log ON online for managing the router. You can view and

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.



**Fig 31. Link to Cloud account page**

CPU, Memory, Trans and receive icons:

These help us to know running status of router.



The image shows a status bar with four icons and their corresponding values: a CPU icon for 'CPU: 3.22%', a memory icon for 'MEM: 16%', an upward arrow for 'TX: 0.00 B/s', and a downward arrow for 'RX: 0.00 B/s'. Below this bar is a solid grey horizontal line.

CPU: 3.22%   MEM: 16%   ↑ TX: 0.00 B/s   ↓ RX: 0.00 B/s

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



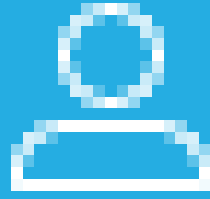
The image shows a status bar with four icons and their corresponding values: a CPU icon for 'CPU: 0.25%', a memory icon for 'MEM: 19%', an upward arrow for 'TX: 6.50 KB/s', and a downward arrow for 'RX: 130.03 KB/s'. Below this bar is a solid grey horizontal line.

CPU: 0.25%   MEM: 19%   ↑ TX: 6.50 KB/s   ↓ RX: 130.03 KB/s

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

### **Language Options:**

Helps to select language as per choice of user.



English

简体中文

繁體中文

English

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 router for configuration and management purposes.

USB interface are data transmission interface.

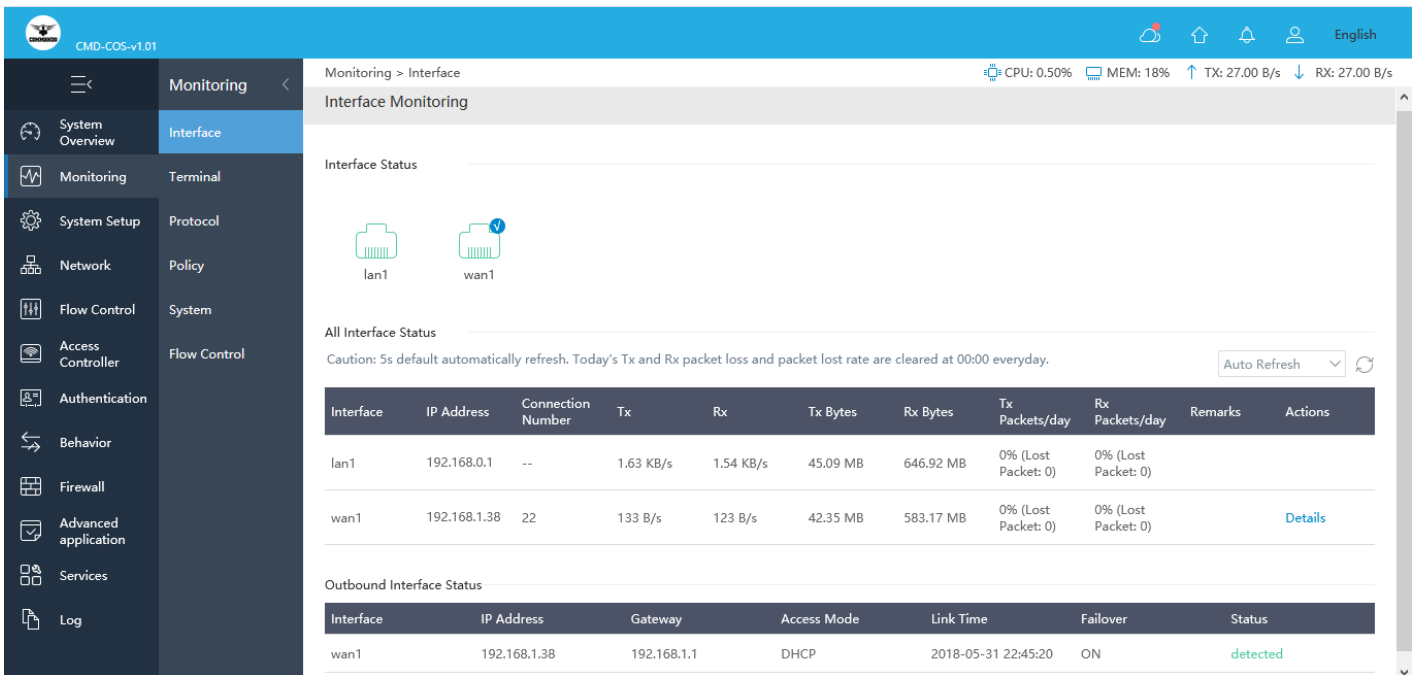
By clicking on Monitoring > Interface we can view the Interface Monitoring

The screenshot shows the 'Interface Monitoring' page in the CMD-COS-v1.01 web interface. The page is titled 'Monitoring > Interface' and 'Interface Monitoring'. It displays the status of two interfaces: lan1 and wan1. The lan1 interface is shown with a green icon and the wan1 interface with a red icon. Below the interface status, there is a table titled 'All Interface Status' which provides detailed statistics for each interface. The table includes columns for Interface, IP Address, Connection Number, Tx, Rx, Tx Bytes, Rx Bytes, Tx Packets/day, Rx Packets/day, Remarks, and Actions. The lan1 interface has an IP address of 192.168.1.1 and is connected. The wan1 interface is not connected. Below the table, there is a section for 'Outbound Interface Status' which shows the wan1 interface with a status of 'dhcp'.

Interface	IP Address	Connection Number	Tx	Rx	Tx Bytes	Rx Bytes	Tx Packets/day	Rx Packets/day	Remarks	Actions
lan1	192.168.1.1	--	51 B/s	92 B/s	307.84 KB	3.56 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		
wan1	--	0	0 B/s	0 B/s	24.38 KB	0 B	0% (Lost Packet: 0)	0% (Lost Packet: 0)		<a href="#">Details</a>

Interface	IP Address	Gateway	Access Mode	Link Time	Failover	Status
wan1	--	--	DHCP	--	ON	dhcp

Fig 1.1.1 Default interface monitoring page



**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.

## Interface Status



### lan1

Connection **Connected**  
Status:

IP: 192.168.0.1

Subnet Mask: 255.255.255.0

MAC: 08:9b:4b:50:1c:bc

Remarks:

Bind Device: veth1/**Connected**/1000Mbps/Full-Duplex

Bind Device: veth2/**Connected**/100Mbps/Full-Duplex

Bind Device: veth3/**Connected**/100Mbps/Full-Duplex

Bind Device: veth4/**Not Connected**/10Mbps/Unknown

**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.

## Interface Status



lan1



wan1

### All Interface Status

Caution: 5s default

#### Interface

lan1

wan1

### Outbound Interface

#### Interface

### wan1 Default Gateway

Connection **Connected** 1052d 18h 14m

Status:

Type: DHCP

IP: 192.168.1.38

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 192.168.1.1

MAC: 08:24:7c:e0:63:33

Remarks:

Bind Device: veth5/**Connected**/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

Monitoring > Terminal

Terminal Monitoring

Comment/IP/MAC  All access types  All  shut down autor  Auto Refresh

IP/MAC	Connection Number	Tx Rate	Rx Rate	Tx Bytes	Rx Bytes	Uptime	Remarks	Actions
192.168.1.100 e0:db:55:be:35:5b	8	0 B/s	0 B/s	0 B	60.78 KB	9m 20s		<a href="#">Details</a> <a href="#">Networking prohibited</a> <a href="#">Limit</a> <a href="#">Modify comment</a>

Showing 1 of 1 records

PerPage  Rows  /1Pages

**Fig 1.2.1 Default Terminal Monitoring page**

Monitoring > Terminal

Terminal Monitoring

Comment/IP/MAC  All access types  All  shut down autor  Auto Refresh

IP/MAC	Connection Number	Tx Rate	Rx Rate	Tx Bytes	Rx Bytes	Uptime	Remarks	Actions
192.168.0.10 e0:db:55:be:35:5b	5	0 B/s	0 B/s	14.52 KB	26.24 KB	24m 22s		<a href="#">Details</a> <a href="#">Networking prohibited</a> <a href="#">Limit</a> <a href="#">Modify comment</a>
192.168.0.11 08:9b:4b:9e:f4:e3	2	0 B/s	0 B/s	720 B	630 B	23m 58s	AP	<a href="#">Details</a> <a href="#">Networking prohibited</a> <a href="#">Limit</a> <a href="#">Modify comment</a>
192.168.0.12 08:9b:4b:99:a3:94	2	0 B/s	0 B/s	720 B	720 B	23m 37s	AP	<a href="#">Details</a> <a href="#">Networking prohibited</a> <a href="#">Limit</a> <a href="#">Modify comment</a>
192.168.0.14 c4:d9:87:a7:ad:d6	15	397 B/s	156 B/s	2.93 MB	40.26 MB	8m 22s	DESKTOP-70API5S	<a href="#">Details</a> <a href="#">Networking prohibited</a> <a href="#">Limit</a> <a href="#">Modify comment</a>

Showing 1-4 of 4 records

PerPage  Rows  /1Pages

**Fig 1.2.2 Terminal Monitoring after connecting devices page**

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

Monitoring > Terminal

Terminal Monitoring

Comment/IP/MAC  All access types  All  shut down autor  Auto Refresh

IP/MAC	Connection Number	Tx Rate	Rx Rate	Tx Bytes	Rx Bytes	Uptime	Remarks	Actions
192.168.0.10 e0:db:55:be:35:5b	14	27 B/s	27 B/s	15.16 KB	26.91 KB	26m 2s		Details Networking prohibited Limit Modify comment
192.168.0.11 08:9b:4b:9ef4:e3	1	0 B/s	0 B/s	720 B	630 B	25m 38s	AP	Details Networking prohibited Limit Modify comment
192.168.0.12 08:9b:4b:99:a3:94	2	0 B/s	0 B/s	720 B	720 B	25m 17s	AP	Details Networking prohibited Limit Modify comment
192.168.0.14 c4:d9:87:a7:ad:46	13	9.62 KB/s	163.16 KB/s	3.52 MB	48.25 MB	10m 2s	DESKTOP-70API55	Details Networking prohibited Limit Modify comment

Showing 1-4 of 4 records

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

**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.

Monitoring > Terminal

Terminal Details - DESKTOP-70API55 ( IP:192.168.0.14 )

Basic Information | Connection Details | Flow Details | History Logs

Basic Information

IP Address: 192.168.0.14 System/Terminal Type: Unknown / Intel

MAC Address: c4:d9:87:a7:ad:46 Uptime: 12m 14s

Remarks: DESKTOP-70API55

Access Information:

Access mode: Wireless Connect SSID: 5G.COMMAND001\_5G

Connect AP:

Account Information

Auth Type : Account Status:

Username: Password:

Affiliation Package: Custom Valid Date: Permanent

Bind to MAC Method : Manual Share:

User Details

Username : phone:

ID Card: Address:

**Fig 1.2.4 Terminal Monitoring details Basic information page**

Monitoring > Terminal

Terminal Details - DESKTOP-70API5S ( IP:192.168.0.14 )

Basic Information | Connection Details | Flow Details | History Logs

Auto Refresh

App Name	Protocol	Interface	WAN Address	Src.Port	Dst.Address	Dst.Port	Tx Bytes	Rx Bytes	Link Status
HTTPS	tcp	wan1	192.168.1.38	56985	44.238.116.130	443	1.75 KB	4.09 KB	ESTABLISHED
OtherHttp	tcp	wan1	192.168.1.38	57367	203.94.209.18	80	564 B	380 B	ESTABLISHED
SSL	tcp	wan1	192.168.1.38	57409	35.247.185.126	443	2.4 KB	3.73 KB	ESTABLISHED
SSL	tcp	wan1	192.168.1.38	56781	74.125.200.188	5228	1.94 KB	5.78 KB	ESTABLISHED
HTTPS	tcp	wan1	192.168.1.38	57438	172.217.160.214	443	1.44 KB	0.99 KB	ESTABLISHED
Oray_Sunlogin	tcp	wan1	192.168.1.38	56864	121.40.255.86	443	6.24 KB	8.73 KB	ESTABLISHED
SSL	tcp	wan1	192.168.1.38	56822	40.119.211.203	443	2.72 KB	4.91 KB	ESTABLISHED
YOUTUBE	udp	wan1	192.168.1.38	62821	142.250.192.22	443	31.33 KB	547.23 KB	--
YOUTUBE	udp	wan1	192.168.1.38	62859	216.239.32.116	443	2.9 KB	5.14 KB	--
YOUTUBE	udp	wan1	192.168.1.38	62861	172.217.160.195	443	3.47 KB	4.9 KB	--
YOUTUBE	udp	wan1	192.168.1.38	62858	8.8.4.4	443	4.35 KB	6.86 KB	--
YOUTUBE	udp	wan1	192.168.1.38	62867	172.217.160.214	443	8.04 KB	126.74 KB	--
YOUTUBE	udp	wan1	192.168.1.38	61844	216.58.203.46	443	197.05 KB	155.96 KB	--
YOUTUBE	udp	wan1	192.168.1.38	62826	203.94.229.79	443	511.88 KB	11.3 MB	--

Fig 1.2.5 Terminal Monitoring connection details page

Monitoring > Terminal

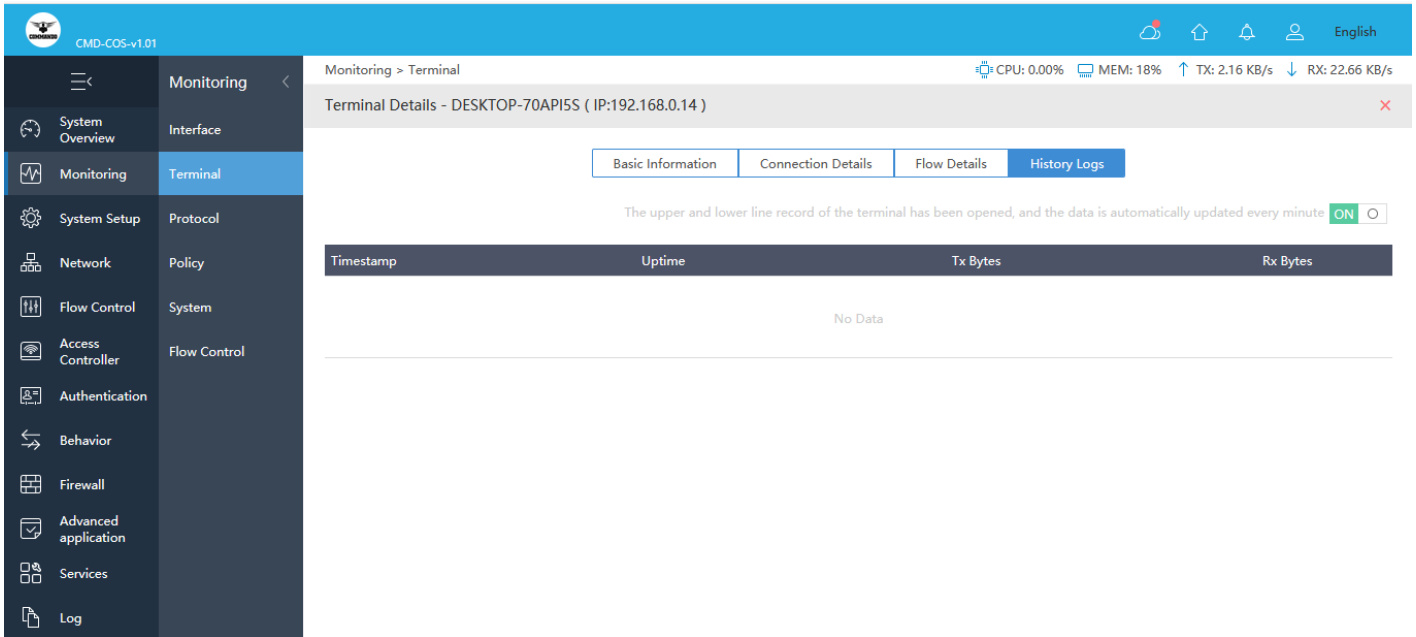
Terminal Details - DESKTOP-70API5S ( IP:192.168.0.14 )

Basic Information | Connection Details | Flow Details | History Logs

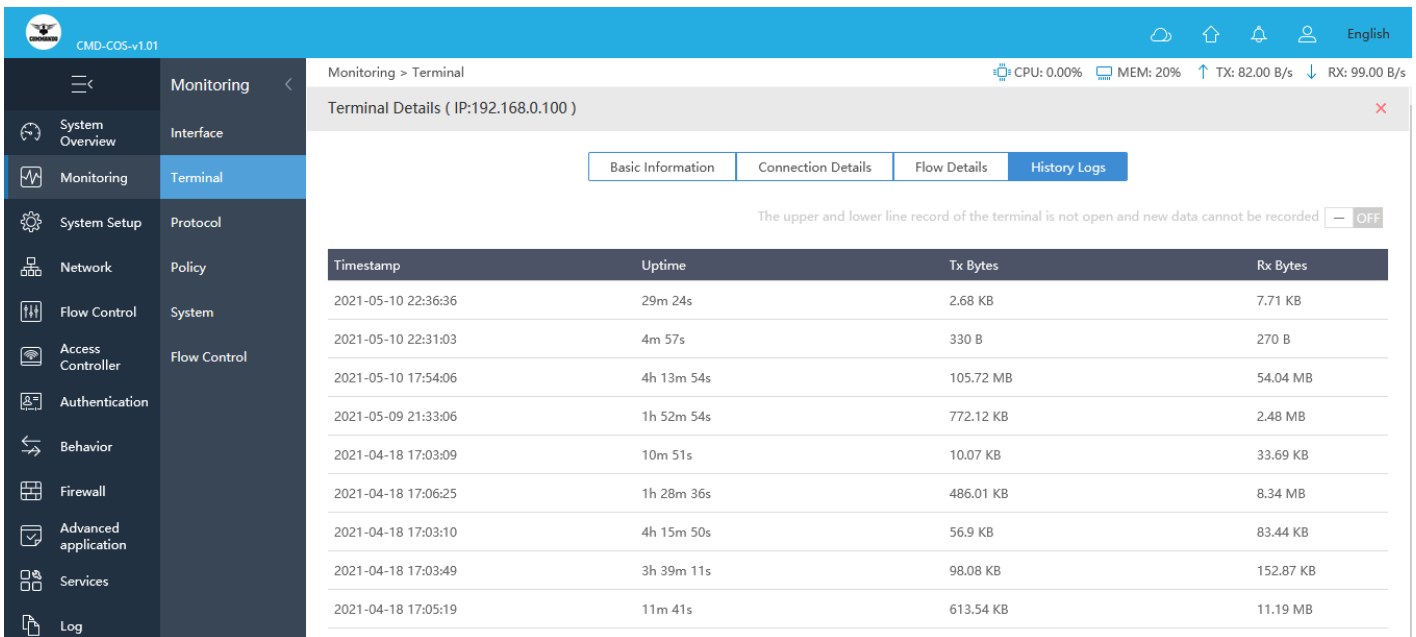
Auto Refresh

App Name	Tx Rate	Total Tx(%)	Rx Rate	Total Rx(%)
Unknown	0 B/s	4.23 KB 0.07%	0 B/s	48.75 KB 0.06%
HttpProtocol	0 B/s	130.88 KB 2.20%	0 B/s	308.93 KB 0.36%
NetDownload	0 B/s	151.65 KB 2.55%	0 B/s	9.85 KB 0.01%
FileTransfer	0 B/s	0 B 0.00%	0 B/s	0 B 0.00%
NetMessage	0 B/s	1.36 KB 0.02%	0 B/s	0 B 0.00%
NetVideo	5.48 KB/s	5.47 MB 94.35%	98.69 KB/s	82.91 MB 99.49%
CommonProtocol	0 B/s	47.52 KB 0.80%	0 B/s	64.52 KB 0.08%
NetGame	0 B/s	0 B 0.00%	0 B/s	0 B 0.00%
OtherSoft	0 B/s	0 B 0.00%	0 B/s	0 B 0.00%
SpeedTool	0 B/s	0 B 0.00%	0 B/s	0 B 0.00%

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



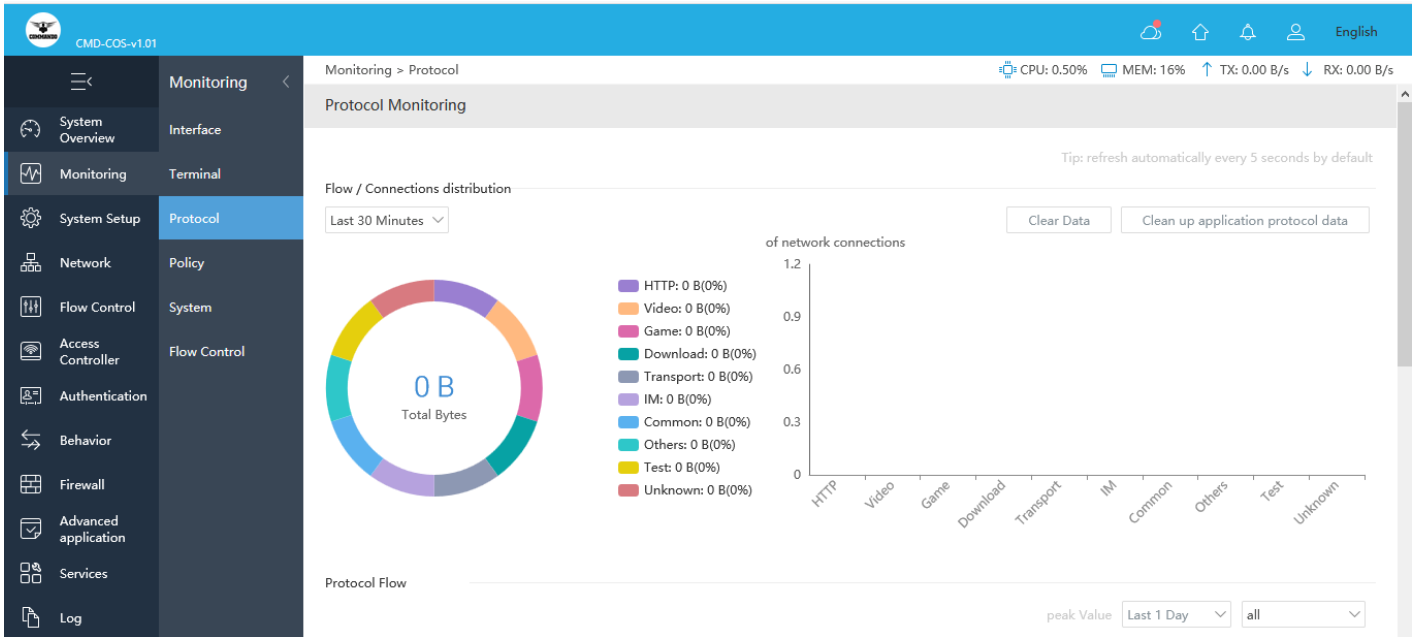


Fig 1.3.1 Protocol Monitoring flow/connections distribution default page

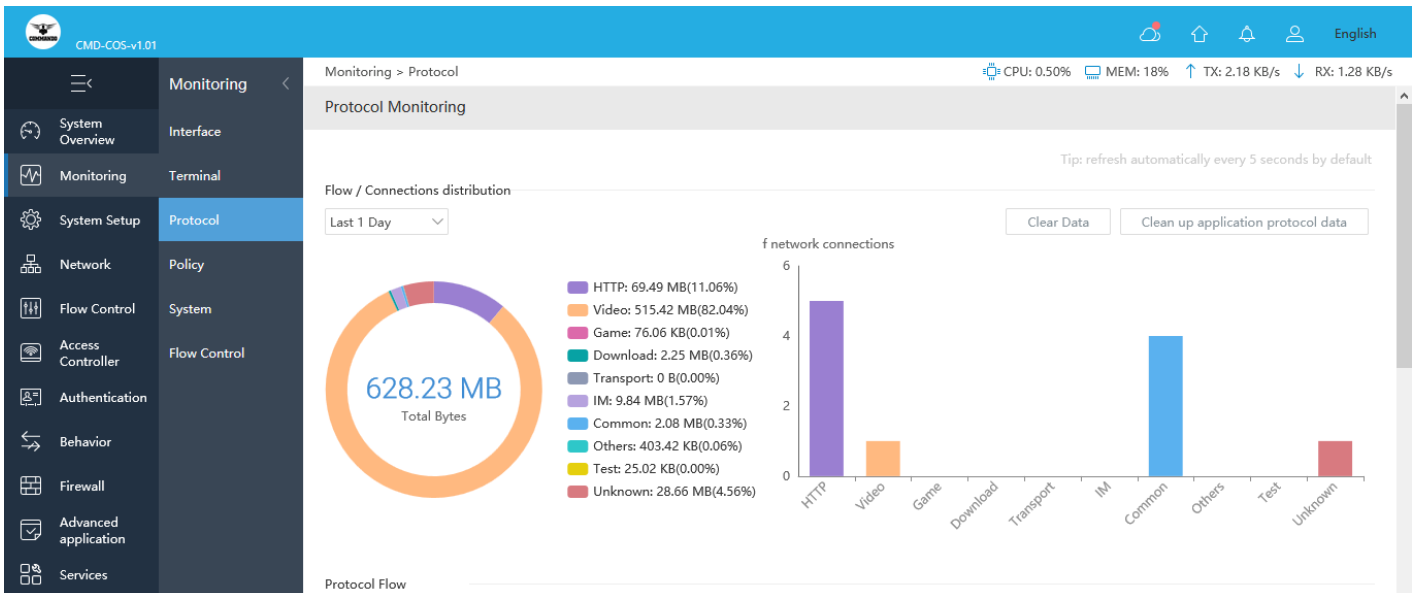
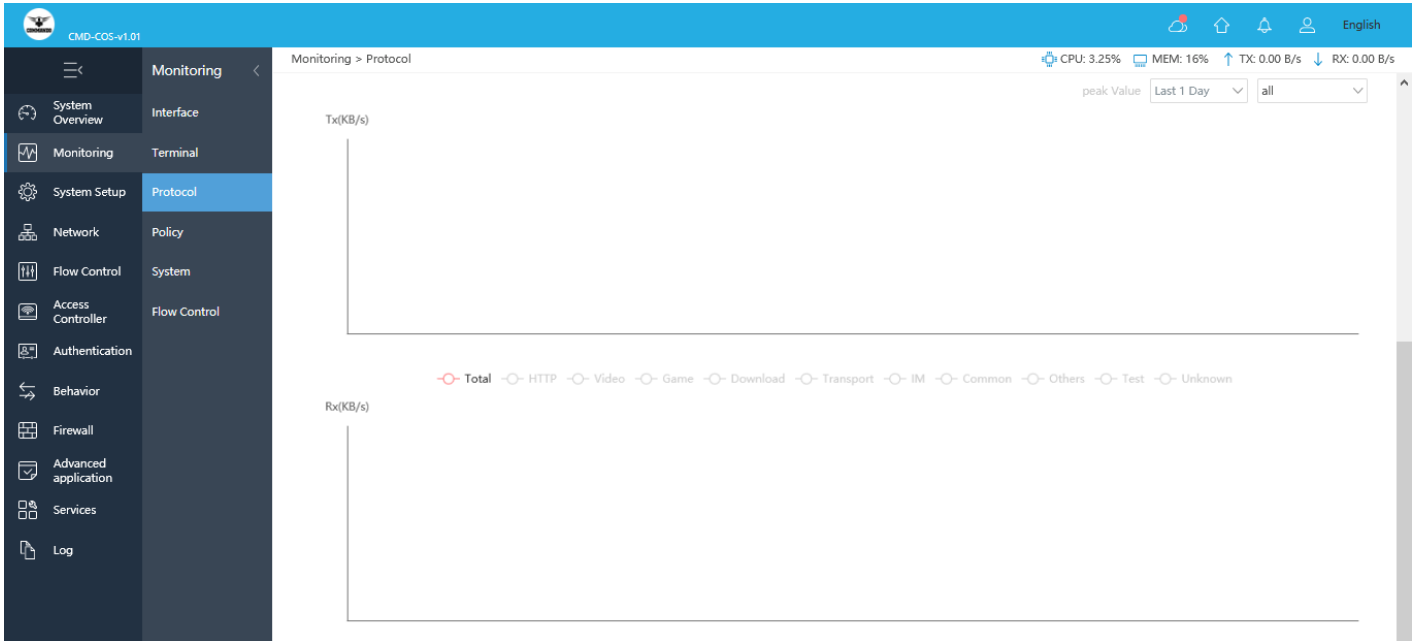
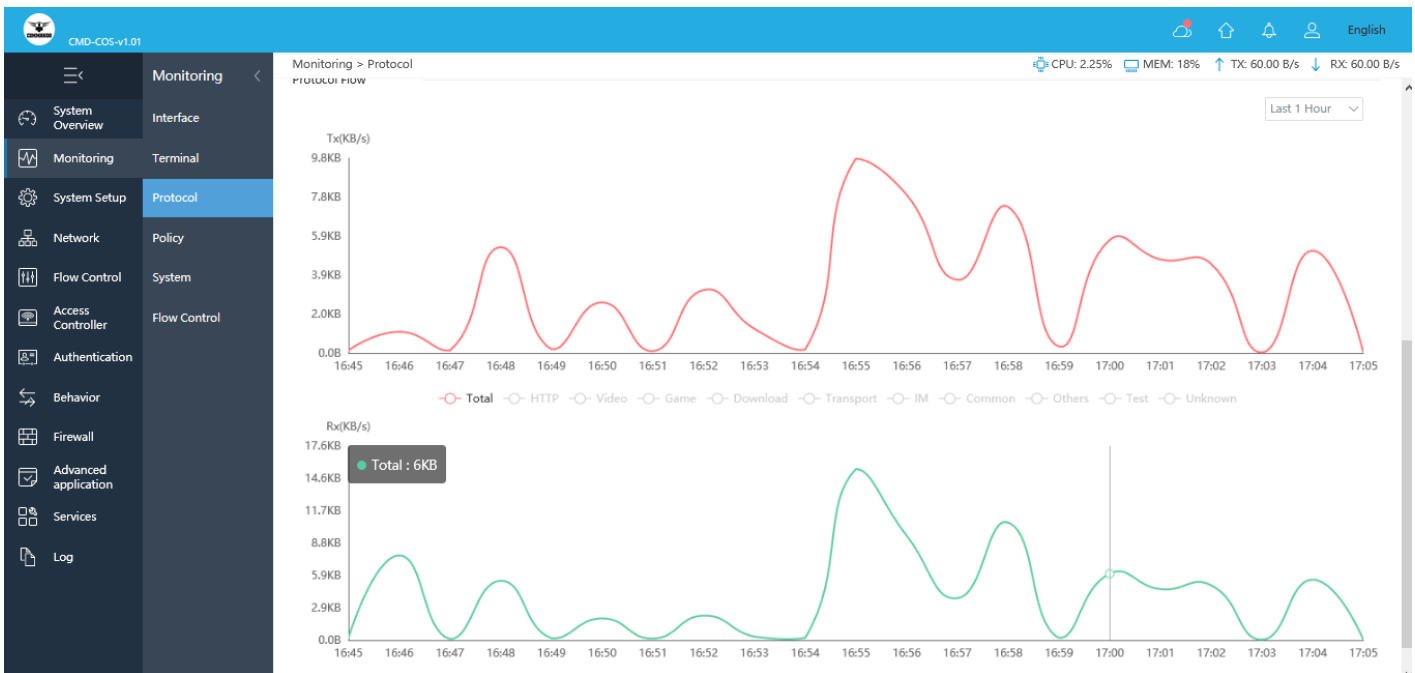


Fig 1.3.2 Protocol Monitoring flow/connections distribution for 1 day page



**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

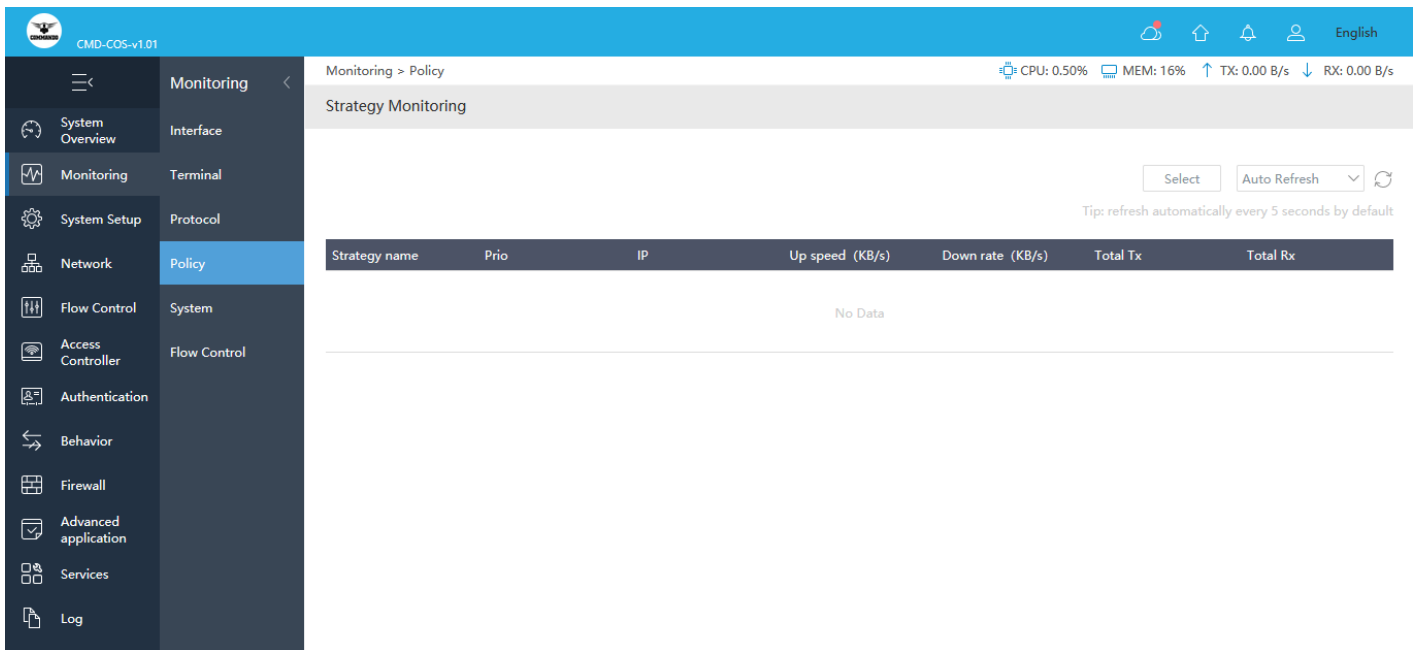


Fig 1.4.1 Default Policy Monitoring page

## 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**

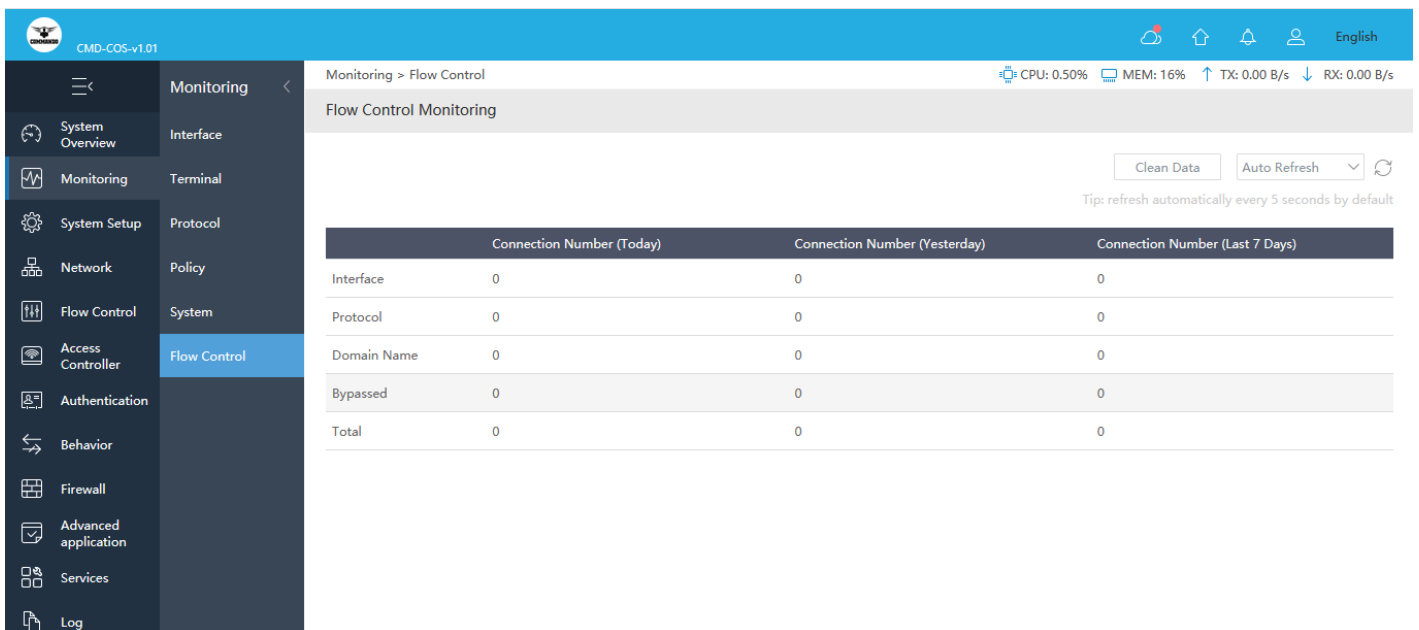


**Fig 1.5.2 System Monitoring for 1hour page**

## 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**

CMD-COS-v1.01 English

CPU: 0.25% MEM: 18% TX: 0.00 B/s RX: 0.00 B/s

Monitoring > Flow Control

### Flow Control Monitoring

Clean Data Auto Refresh ⌂

Tip: refresh automatically every 5 seconds by default

	Connection Number (Today)	Connection Number (Yesterday)	Connection Number (Last 7 Days)
Interface	0	0	0
Protocol	0	0	0
Domain Name	0	0	0
Bypassed	34	0	34
<b>Total</b>	<b>34</b>	<b>0</b>	<b>34</b>

**Fig 1.6.2 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 router 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 Router 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 router.

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

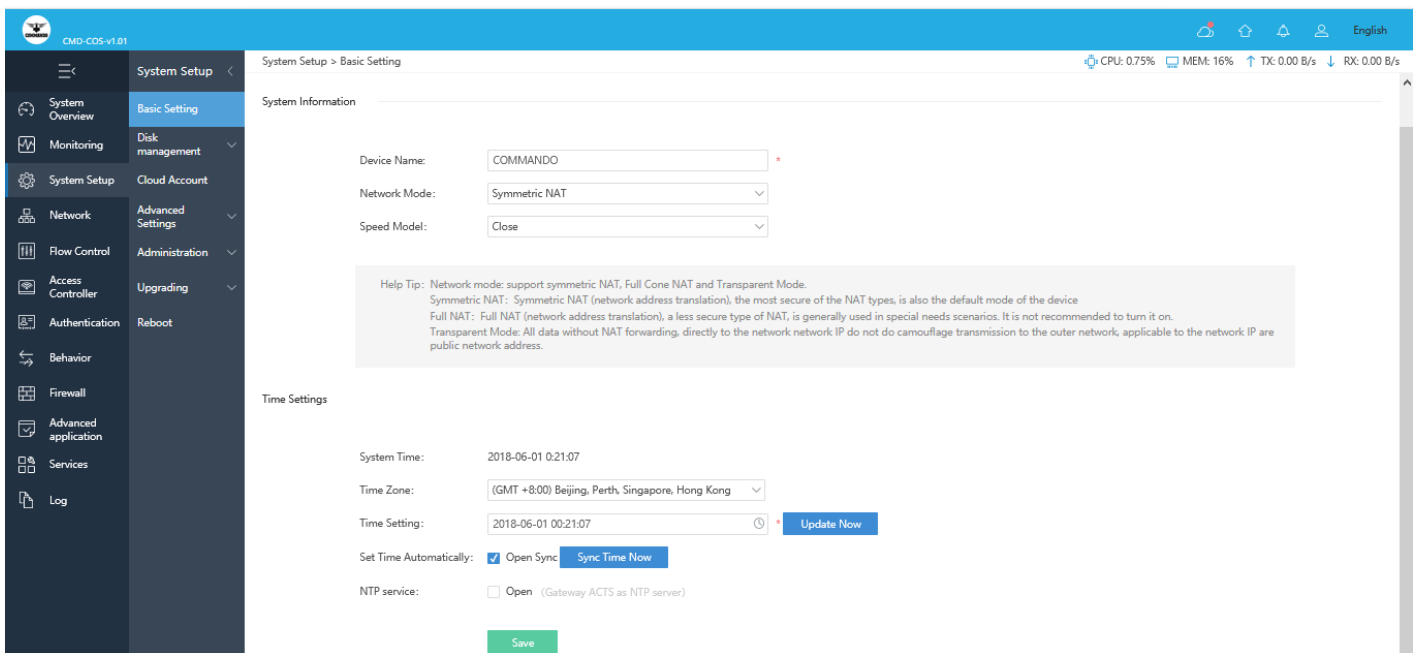


Fig 2.1.1 Default Basic setting page

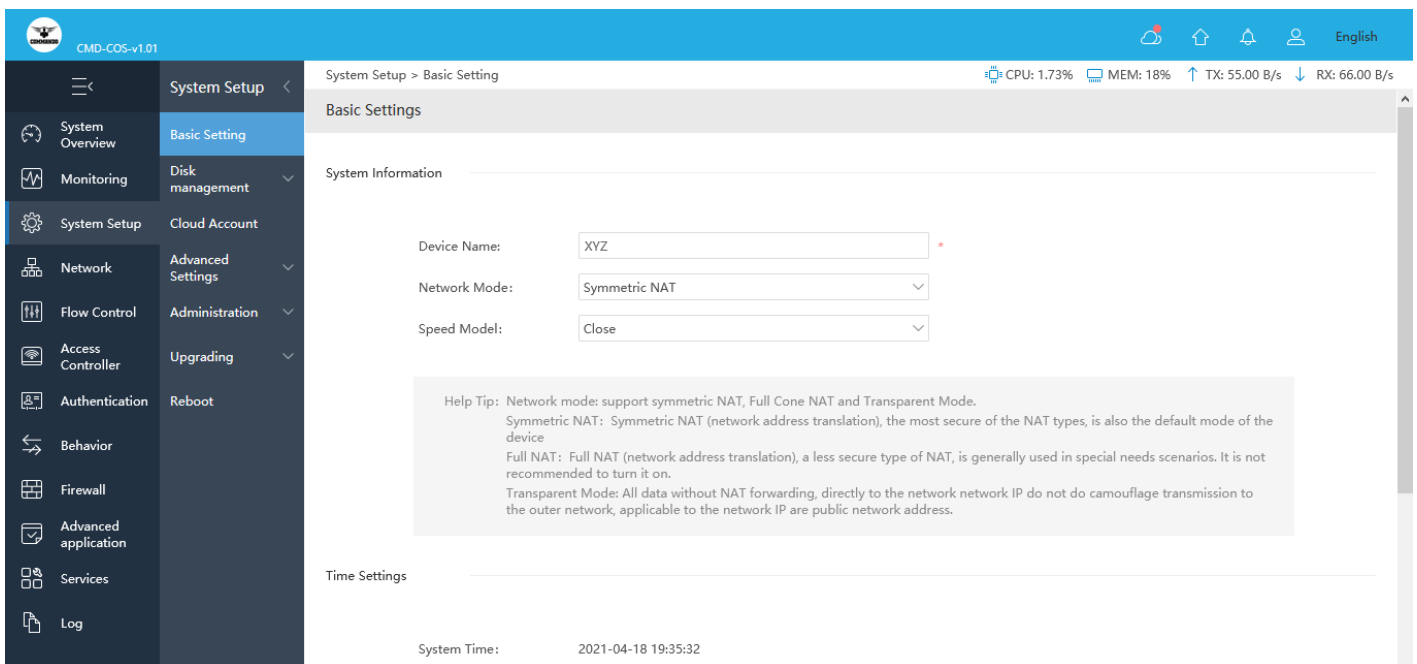
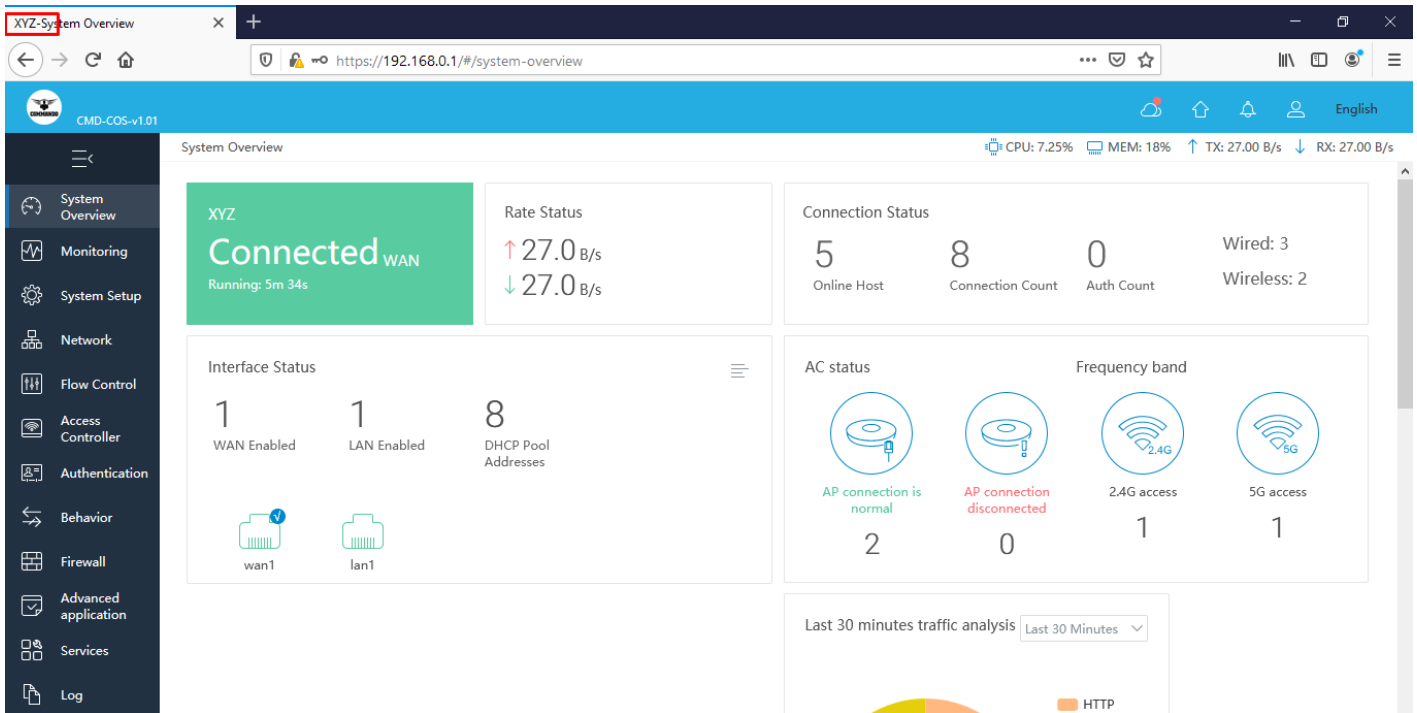


Fig 2.1.2 Basic setting for changing device name page

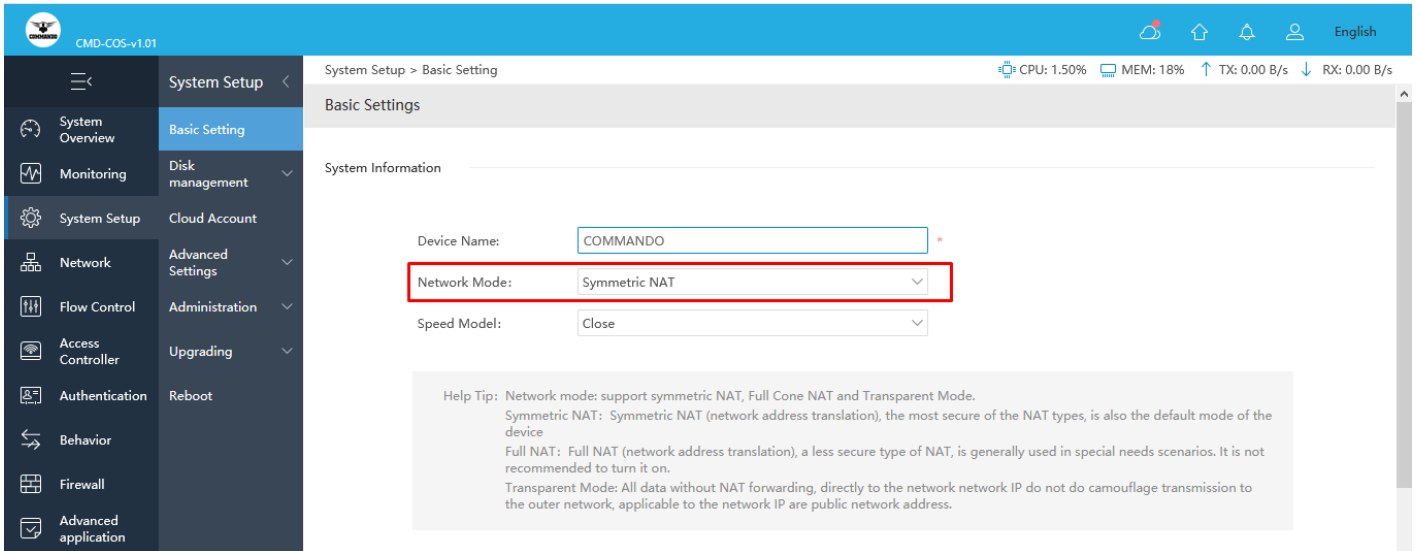


**Fig 2.1.3 XYZ Device name page**

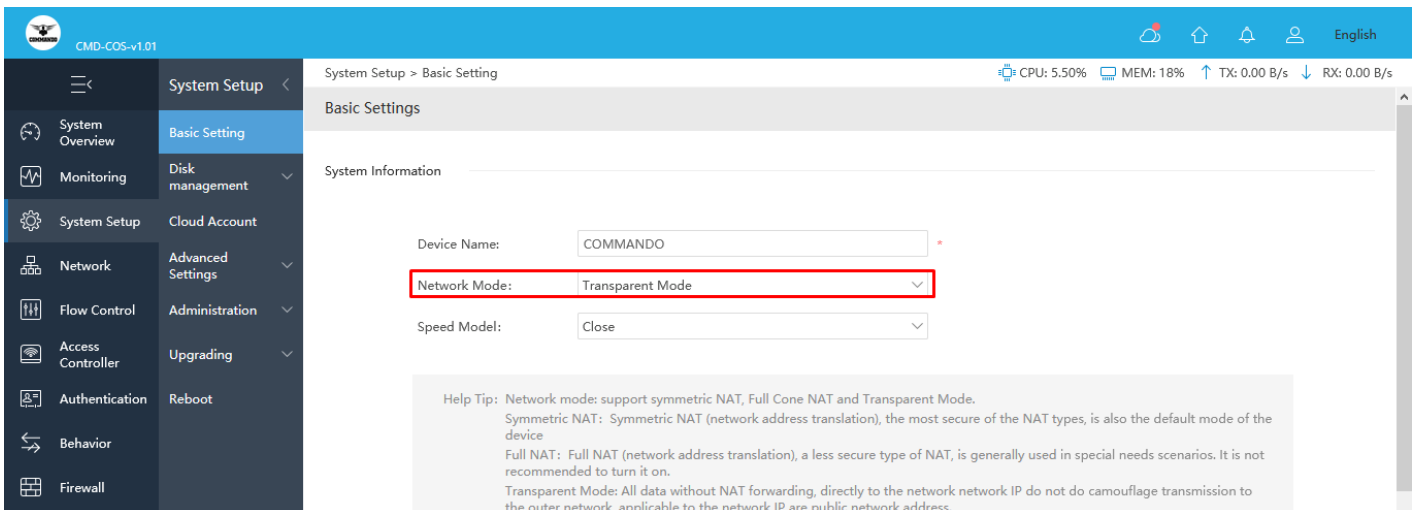
### **Network Address Translation (NAT):**

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 router 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**

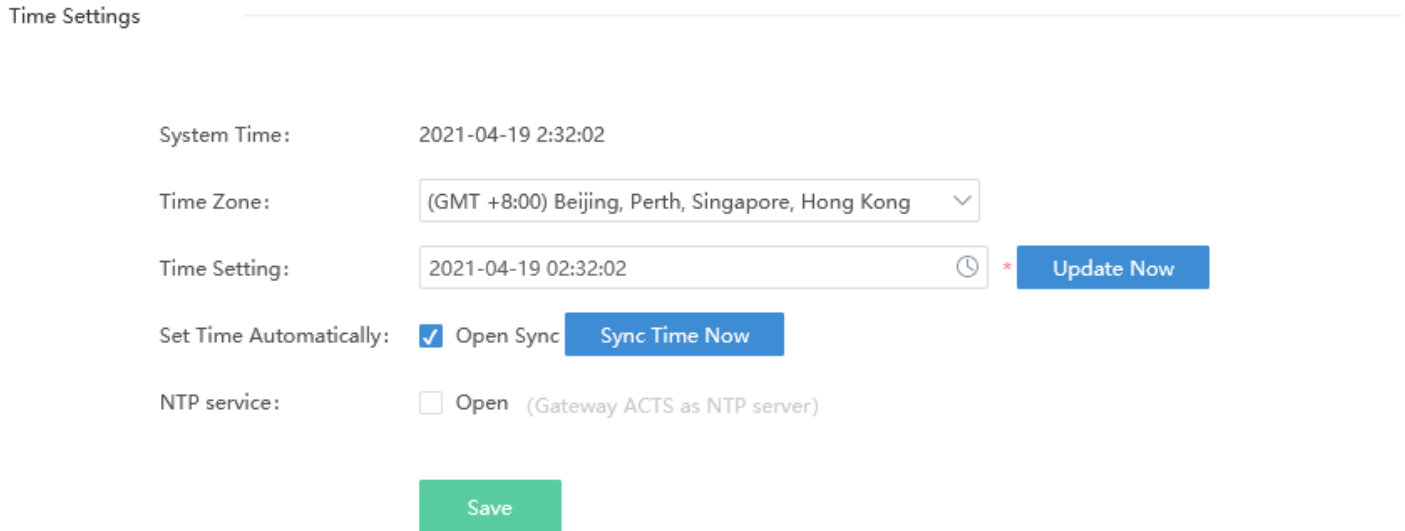
## Time setting:

System Time is the time displayed while the Router 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 Router. Time Zone displays the current time zone of the Router. You can configure the time zone and NTP Server. The Router 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.

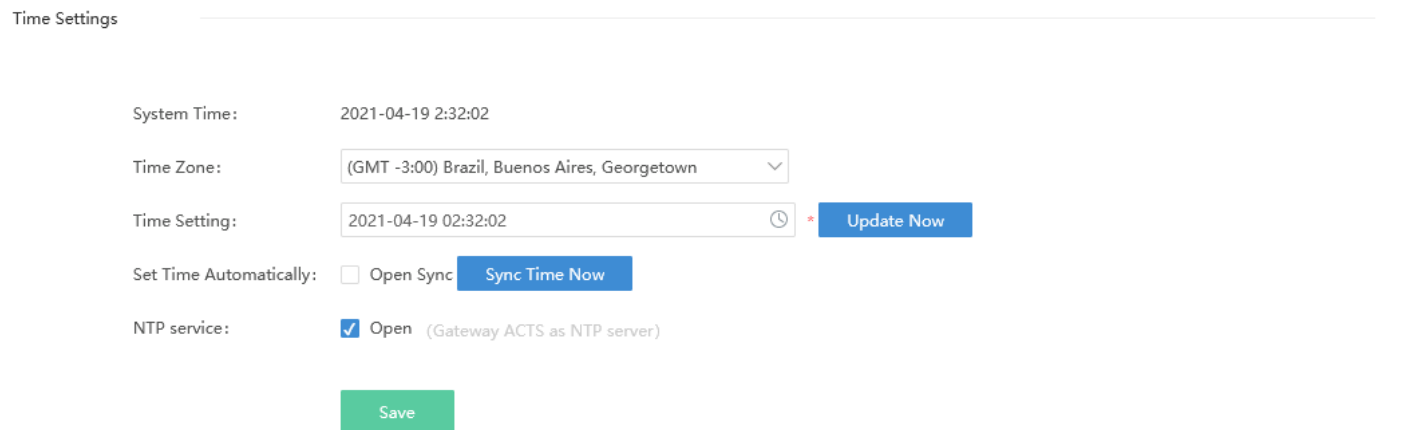


The screenshot shows the 'Time Settings' page. At the top left, it says 'Time Settings'. Below this, there are several settings:

- System Time:** 2021-04-19 2:32:02
- Time Zone:** A dropdown menu showing '(GMT +8:00) Beijing, Perth, Singapore, Hong Kong'.
- Time Setting:** A text input field containing '2021-04-19 02:32:02' with a clock icon and an asterisk. To its right is a blue button labeled 'Update Now'.
- Set Time Automatically:** A checked checkbox followed by 'Open Sync' and a blue button labeled 'Sync Time Now'.
- NTP service:** An unchecked checkbox followed by 'Open (Gateway ACTS as NTP server)'.

At the bottom center, there is a green button labeled 'Save'.

**Fig 2.1.6 Time Settings with Sync time now option page**



The screenshot shows the 'Time Settings' page. At the top left, it says 'Time Settings'. Below this, there are several settings:

- System Time:** 2021-04-19 2:32:02
- Time Zone:** A dropdown menu showing '(GMT -3:00) Brazil, Buenos Aires, Georgetown'.
- Time Setting:** A text input field containing '2021-04-19 02:32:02' with a clock icon and an asterisk. To its right is a blue button labeled 'Update Now'.
- Set Time Automatically:** An unchecked checkbox followed by 'Open Sync' and a blue button labeled 'Sync Time Now'.
- NTP service:** A checked checkbox followed by 'Open (Gateway ACTS as NTP server)'.

At the bottom center, there is a green button labeled 'Save'.

**Fig 2.1.7 Time Settings with NTP service and changing Time zone page**

## 2. Disk management

Router 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 Router supports up to 8 zoning quantity. To access to this page click on System

## Setup > Disk management > Disk partition

The screenshot shows the 'Disk partition' page in the system setup interface. The top navigation bar includes the system logo, version 'CMD-COS-v1.01', and system status indicators: CPU: 0.00%, MEM: 16%, TX: 0.00 B/s, and RX: 0.00 B/s. The left sidebar contains a menu with 'System Setup' selected, and 'Disk partition' highlighted. The main content area displays a table with columns: disk, Mount path, Partition name, Partition type, Partition size, Utilization rate, Binding business, and Actions. The table is currently empty, showing 'No Data'. A 'Quick zoning' button is visible in the top right corner. Below the table, a description box contains the following text:

Description: 1. Each hard disk can support up to 8 partitions, and the system disk can be divided into 4 additional partitions;  
2. External hard disks must be formatted or partitioned after binding services, otherwise related services will use system disk space by default;  
3. Disk partitions support bundled functional services including: ordinary storage, behavior records, Cache Service (partition size 10G and above)

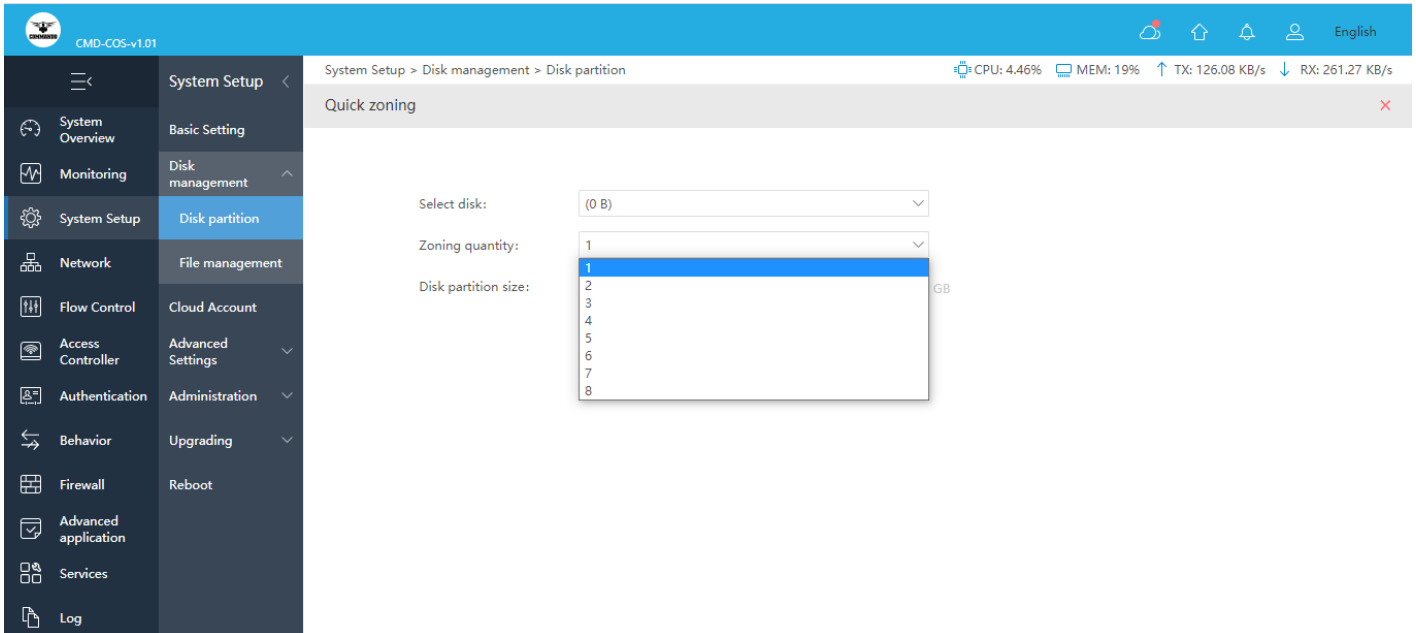
Fig 2.2.1 Disk partition page

The screenshot shows the 'Quick zoning' page in the system setup interface. The top navigation bar includes the system logo, version 'CMD-COS-v1.01', and system status indicators: CPU: 11.50%, MEM: 19%, TX: 64.53 KB/s, and RX: 292.15 KB/s. The left sidebar contains a menu with 'System Setup' selected, and 'Disk partition' highlighted. The main content area displays a 'Quick zoning' form with the following fields:

- Select disk: (0 B)
- Zoning quantity: 1
- Disk partition size: 0 GB

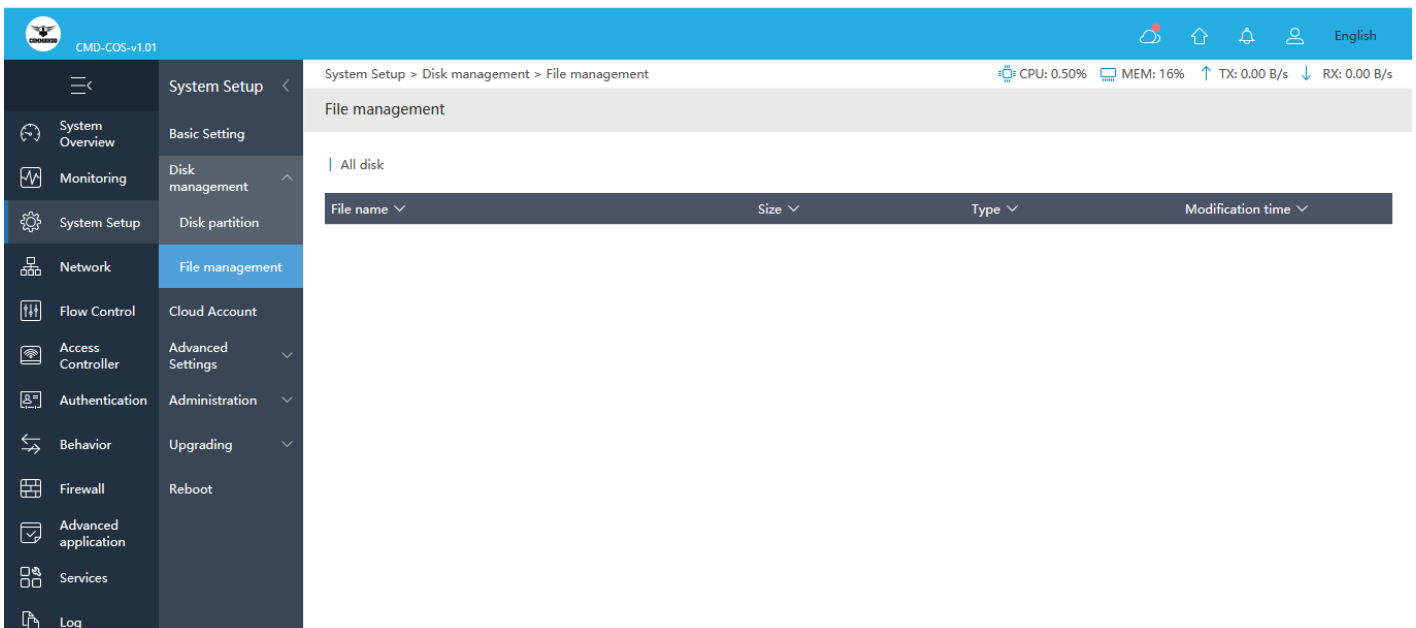
At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Fig 2.2.2 Disk partition quick zoning page



**Fig 2.2.3 Disk partition quick zoning quantity page**

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

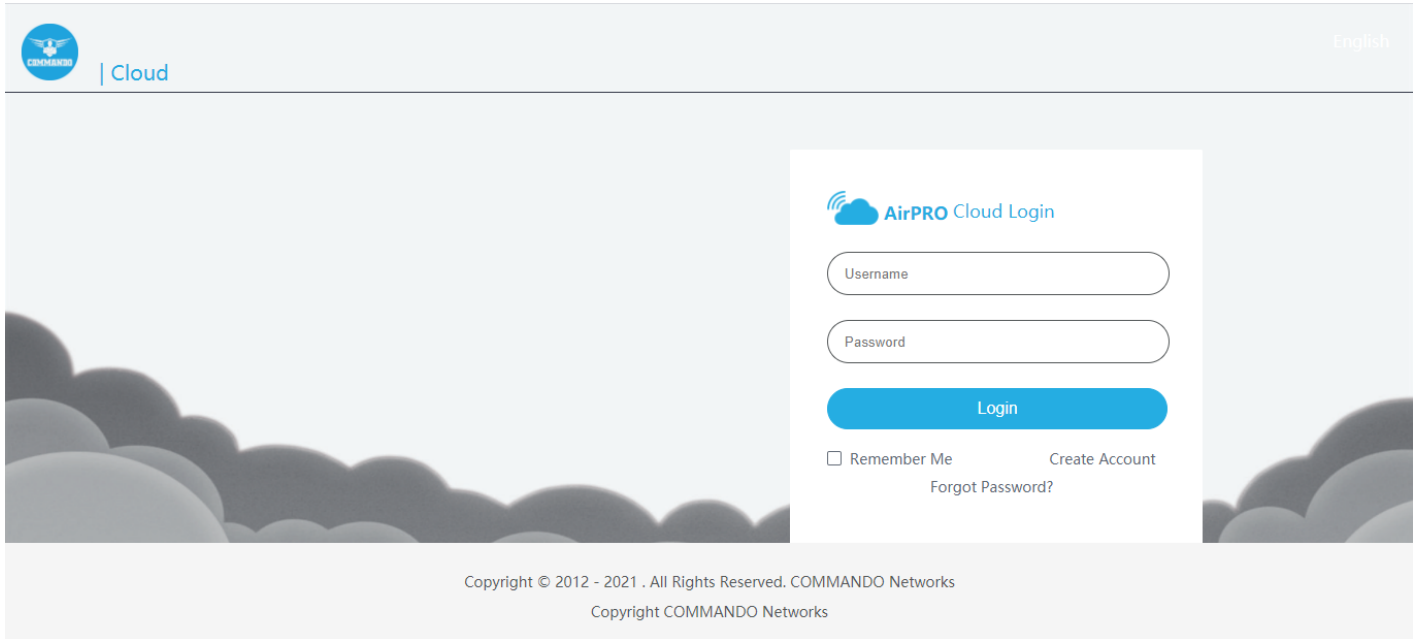


**Fig 2.2.4 Default file Management page**

### 3. Cloud Account

#### 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. 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



Username

Password

Login

Remember Me

[Create Account](#)

[Forgot Password?](#)

---

Fig 2.3.2 Create Cloud Login account page

# Register

---

abcd@gmail.com

.....

.....

Verification Code

Get Email Verification Code

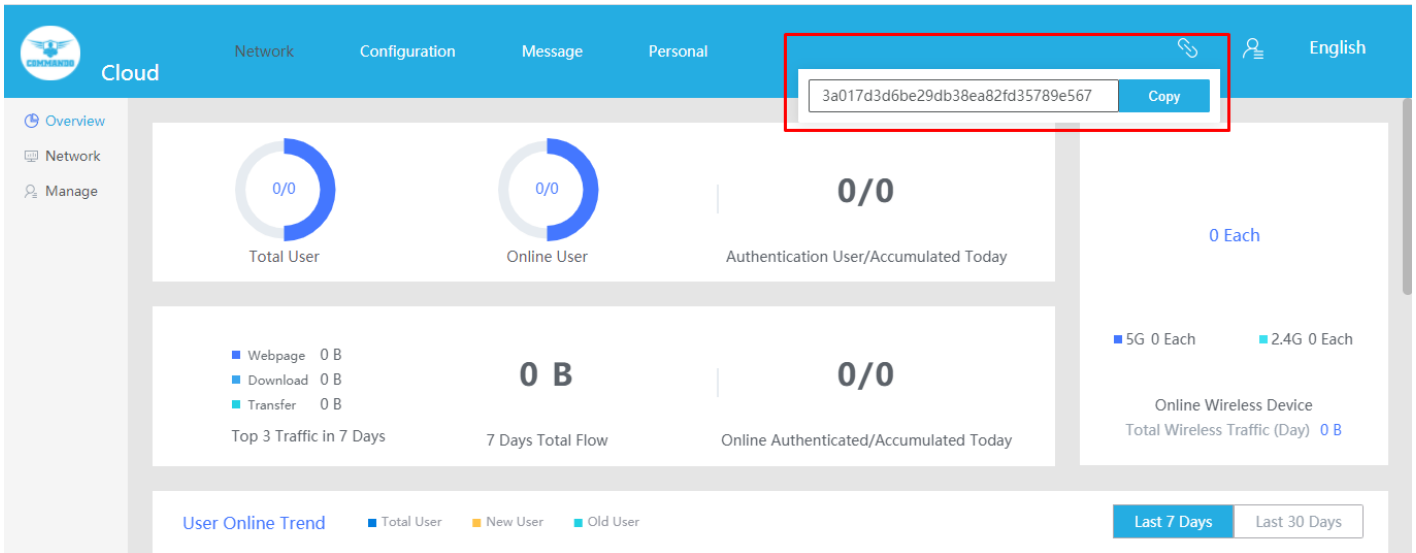
The Repeat Password confirmation does not match.

Register

I agree to [use this agreement](#) [Return to Login](#)

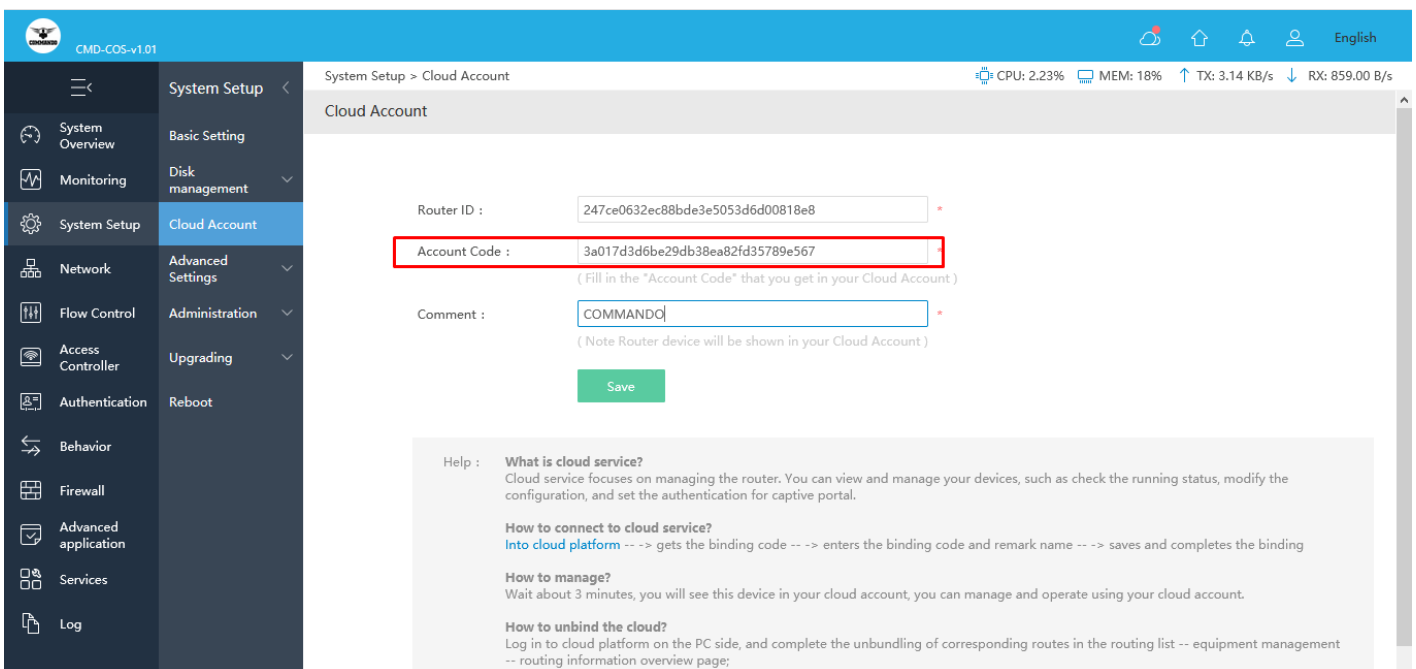
**Fig 2.3.3 Register Cloud Login account page**

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 R100 router with cloud portal page**



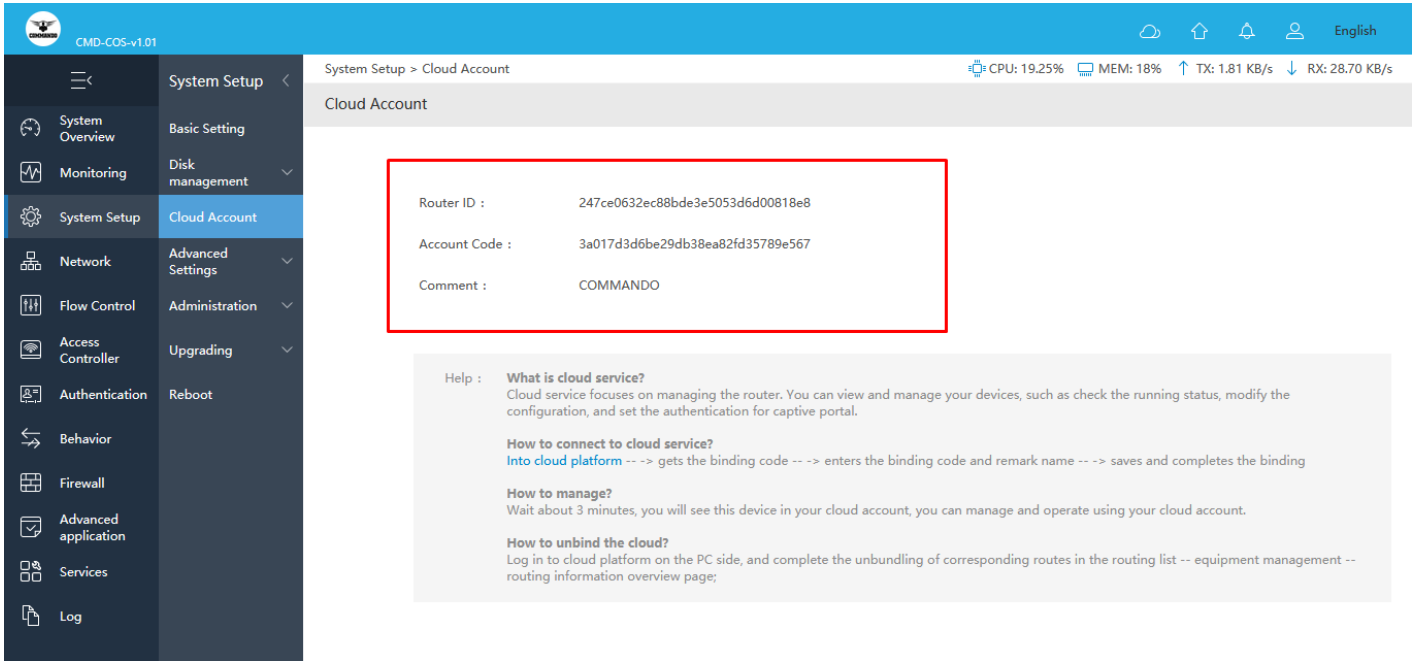


Fig 2.3.6 After Binding R100 router with cloud page

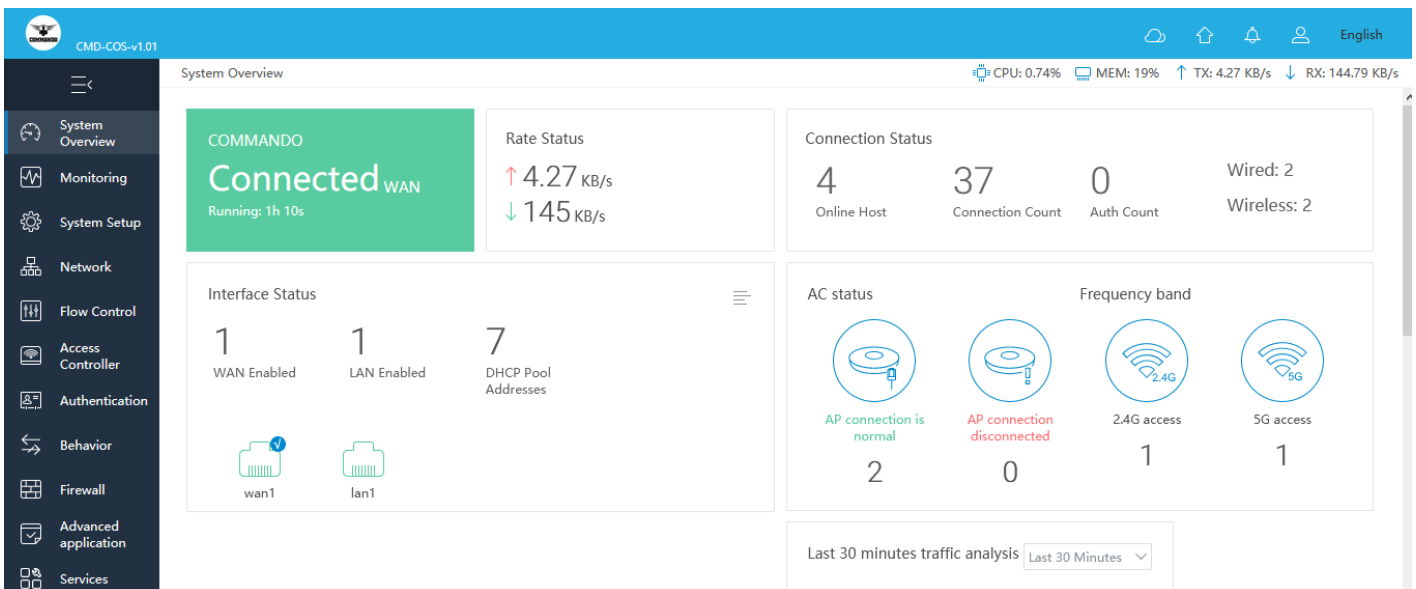
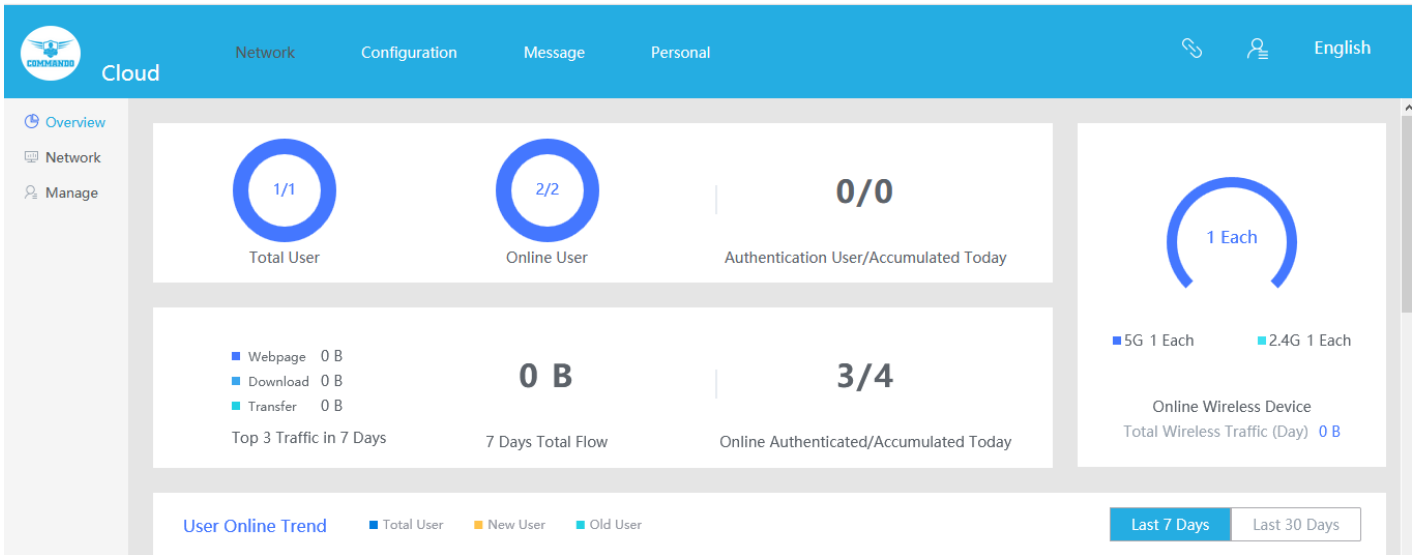
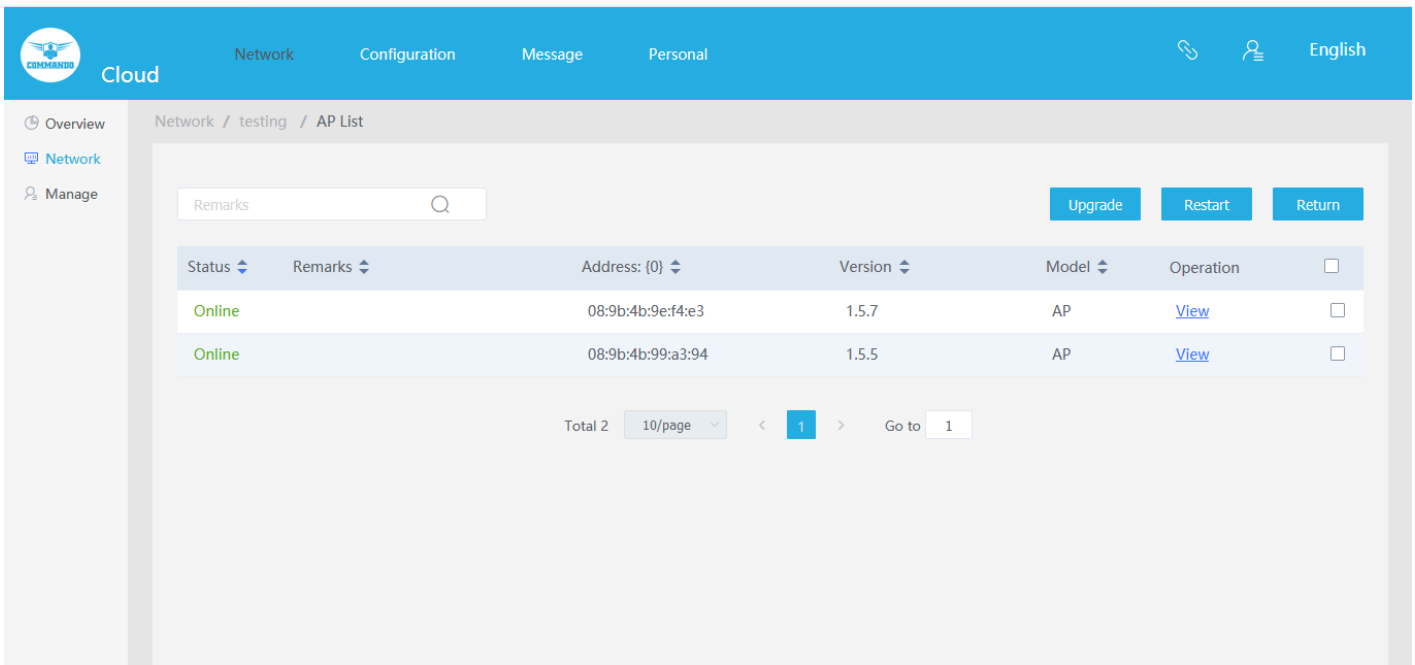


Fig 2.3.7 Normal R100 router system overview page



**Fig 2.3.8 Cloud access of R100 router with cloud page**



**Fig 2.3.9 Cloud access of R100 router 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.

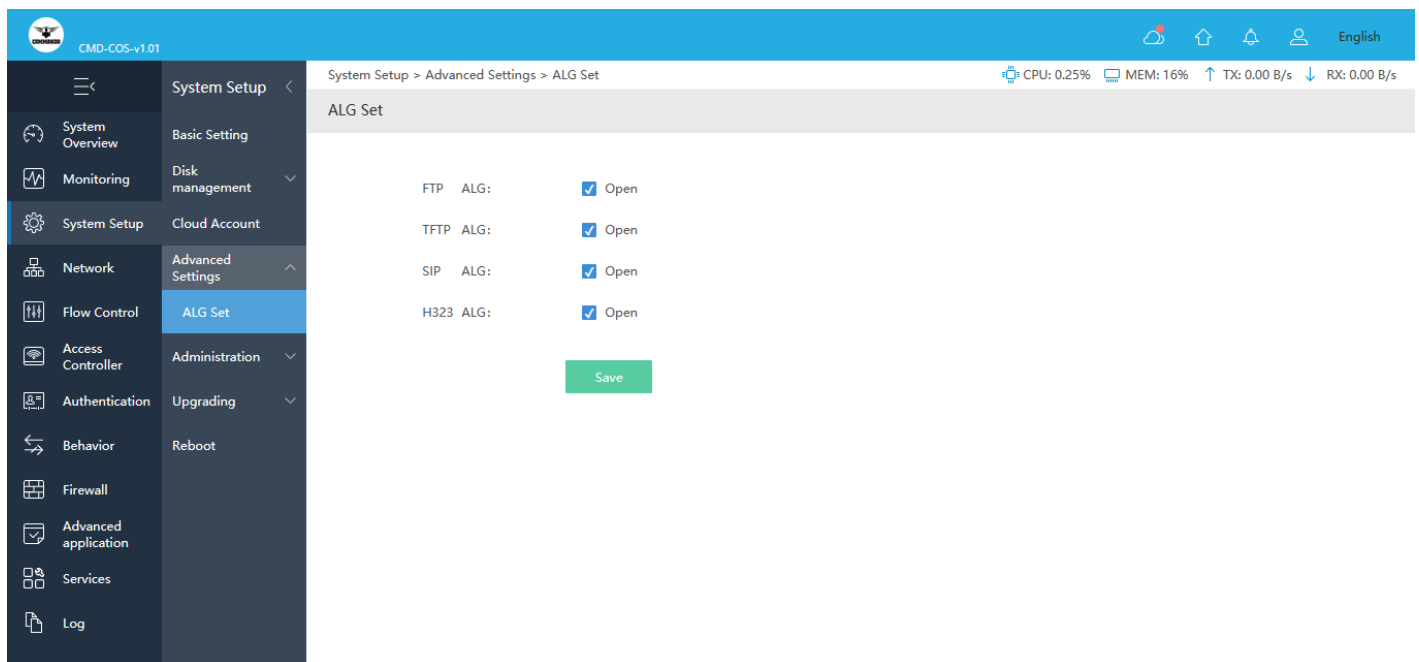
### How to unbind the cloud?

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 like 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**

## 5. Administration

On this page, you can modify the factory default username and password of the Router 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

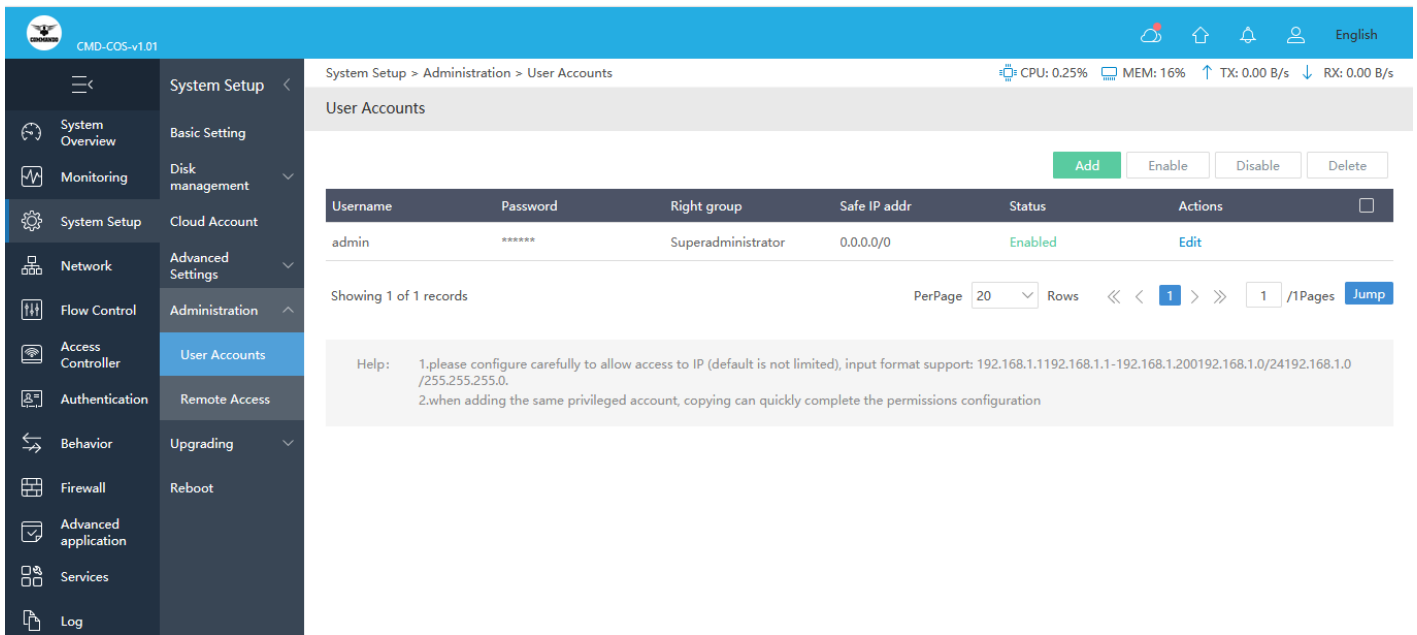


Fig 2.5.1 Default User Accounts page

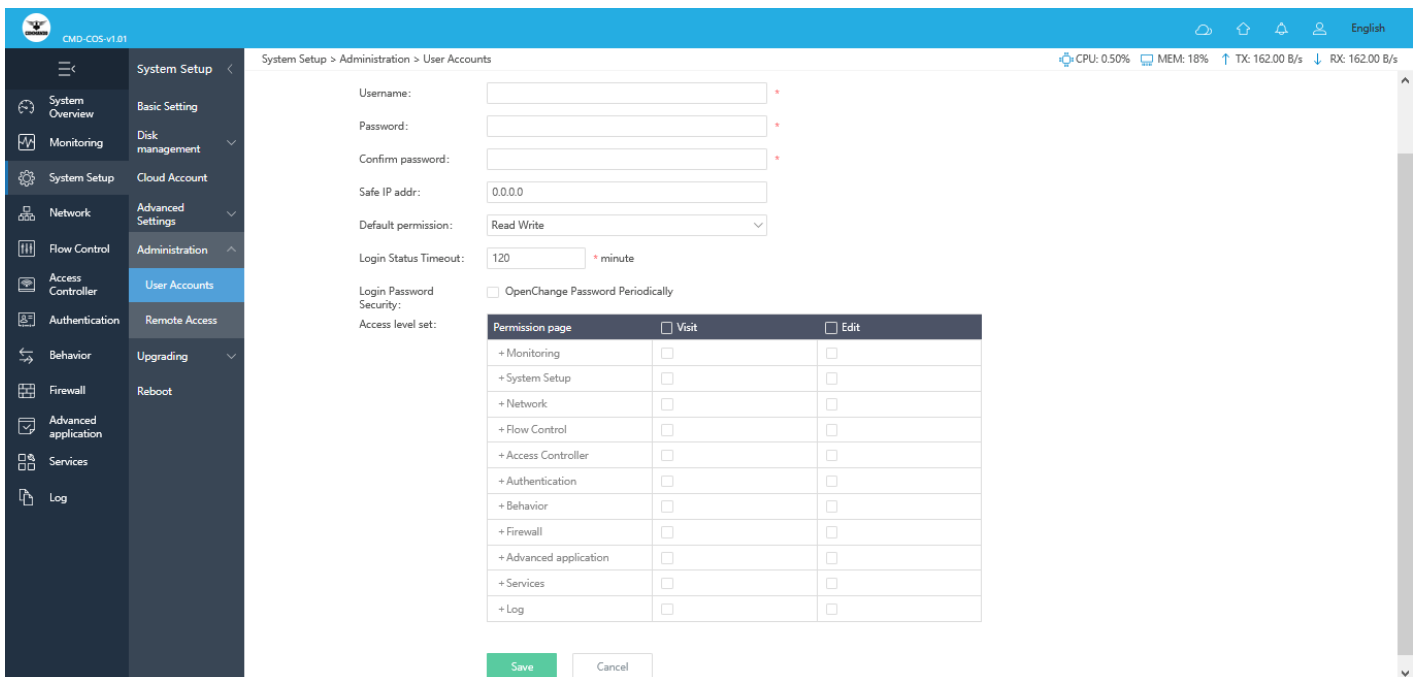
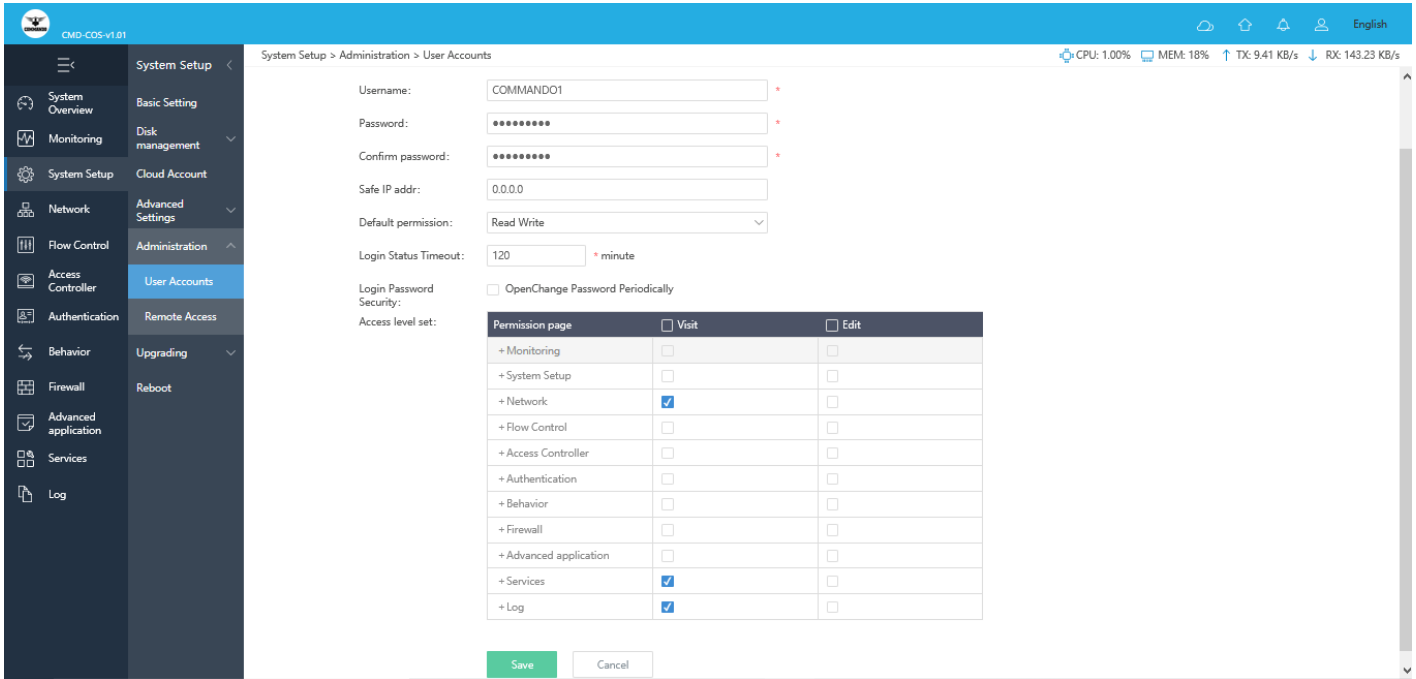
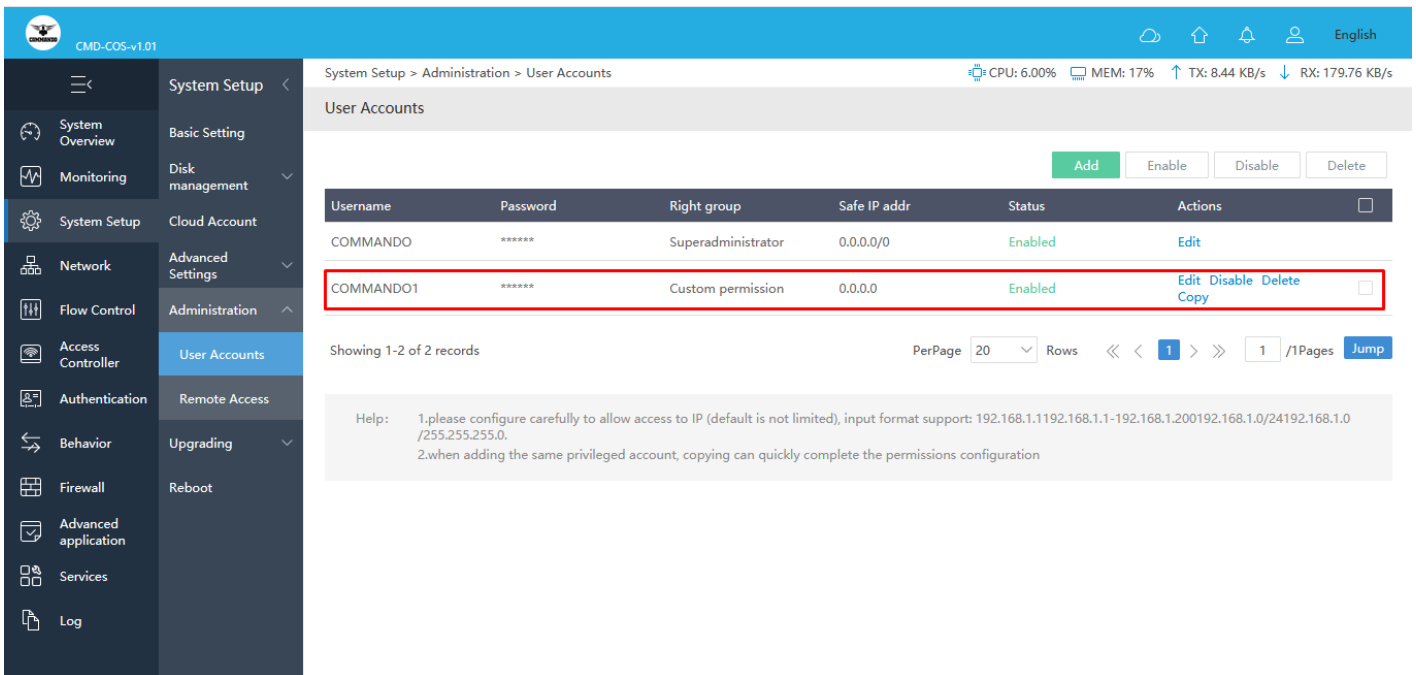


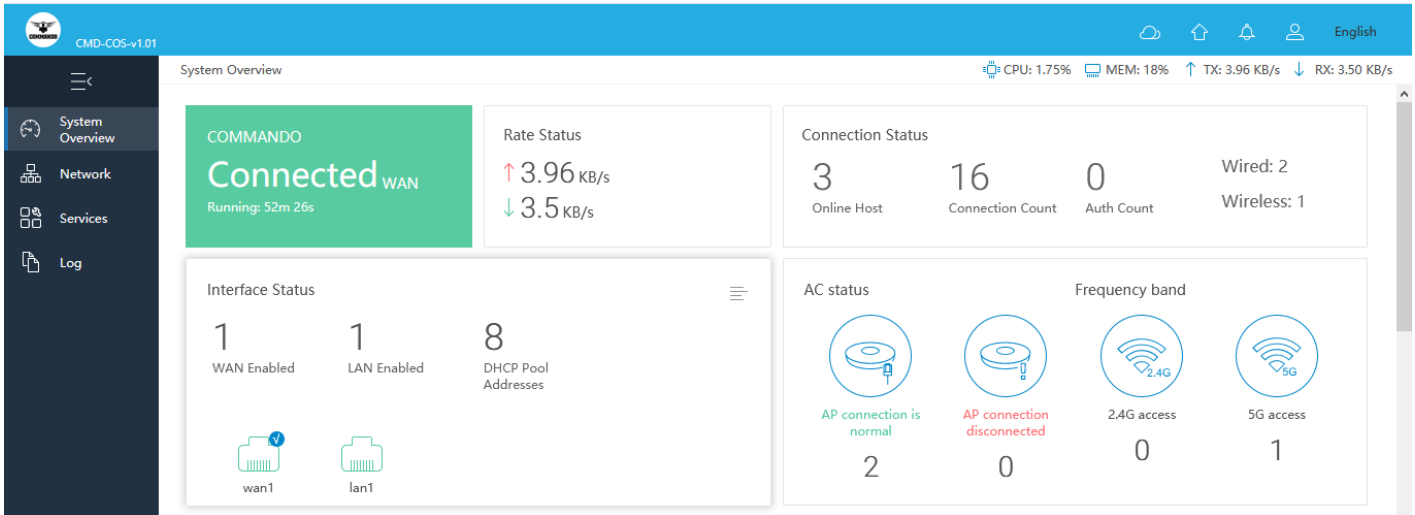
Fig 2.5.2 Add User Accounts page



**Fig 2.5.3 Add User Account with visit permission page**



**Fig 2.5.4 User Account COMMANDO1 with visit permission page**

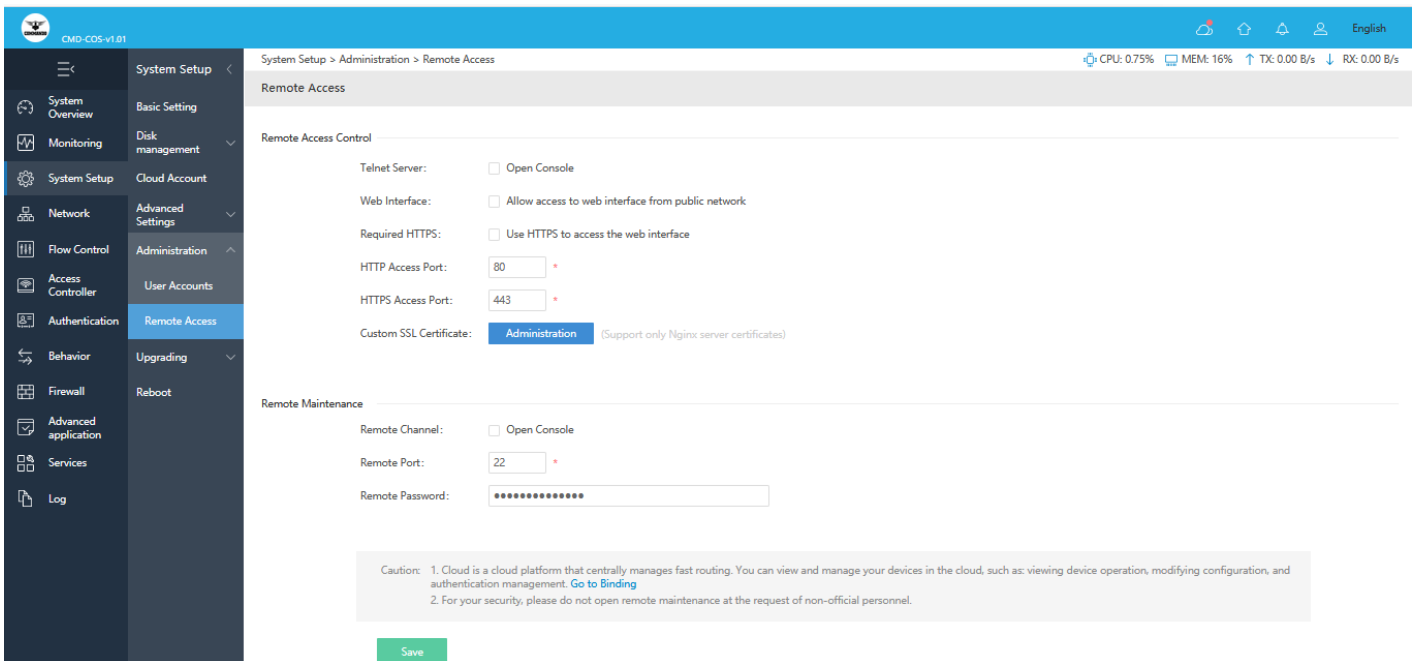


**Fig 2.5.6 Customized access as per User Account COMMANDO1 with visit permission page**

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**

## Remote Access

### Remote Access Control

Telnet Server:	<input checked="" type="checkbox"/> Open Console
Web Interface:	<input checked="" type="checkbox"/> Allow access to web interface from public network
Required HTTPS:	<input checked="" type="checkbox"/> Use HTTPS to access the web interface
HTTP Access Port:	<input type="text" value="80"/> *
HTTPS Access Port:	<input type="text" value="443"/> *
Custom SSL Certificate:	<input type="text" value="Administration"/> (Support only Nginx server certificates)

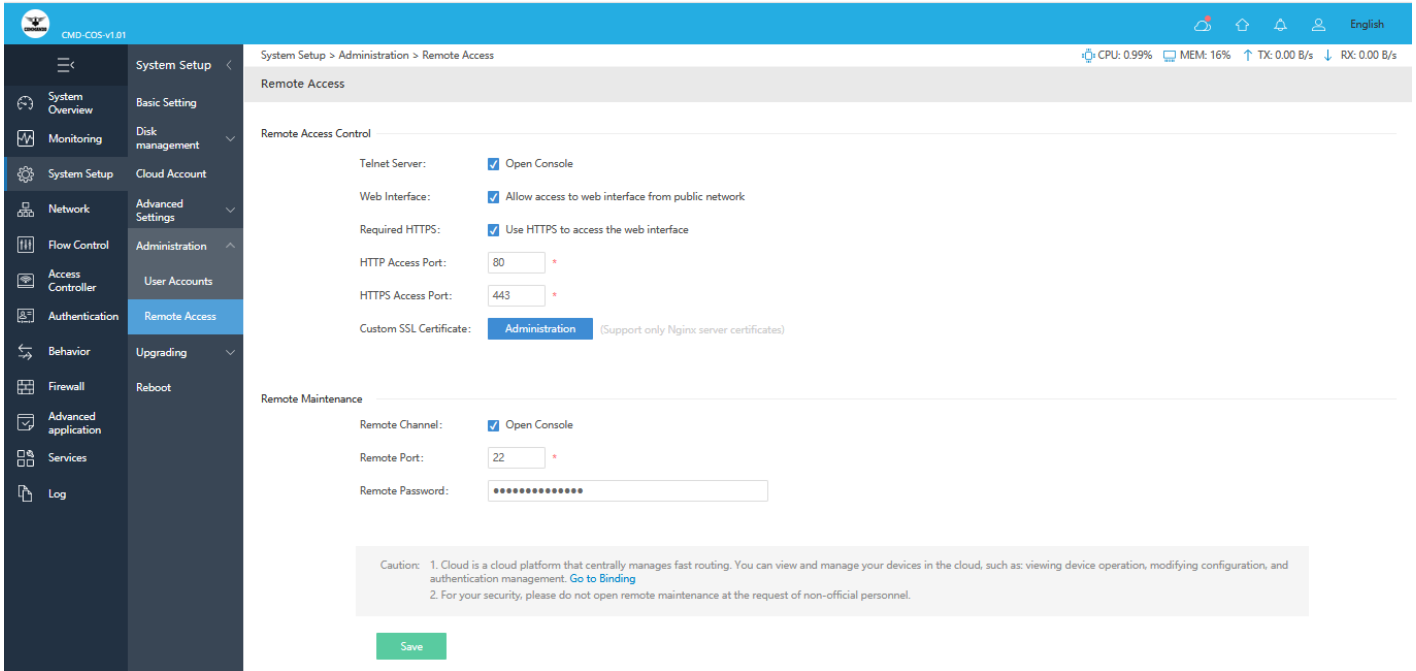
**Fig 2.5.8 Enabling Remote Access control page**

### Remote Maintenance

Remote Channel:	<input checked="" type="checkbox"/> Open Console
Remote Port:	<input type="text" value="22"/> *
Remote Password:	<input type="password" value="••••••••••"/>

Caution: 1. Cloud is a cloud platform that centrally manages fast routing. You can view and manage your devices in the cloud, such as: viewing device operation, modifying configuration, and authentication management. [Go to Binding](#)  
2. For your security, please do not open remote maintenance at the request of non-official personnel.

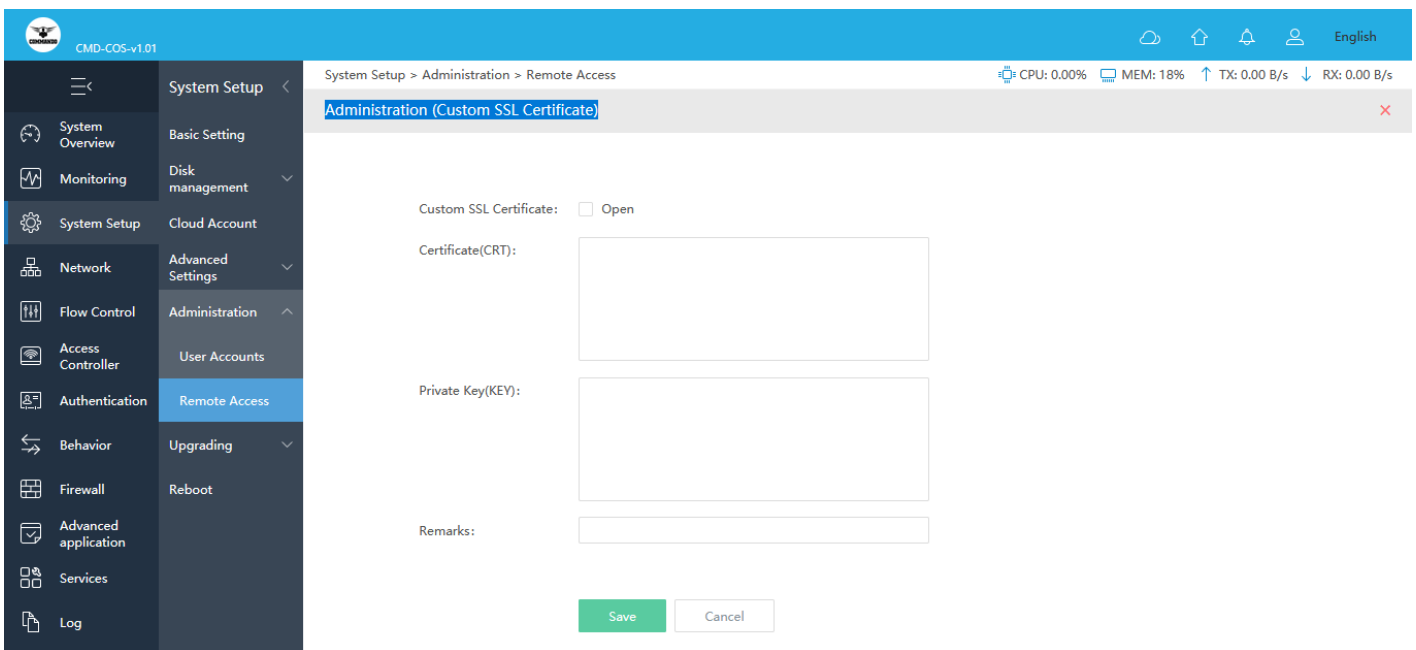
**Fig 2.5.9 Setting password for Remote Access page**



**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**



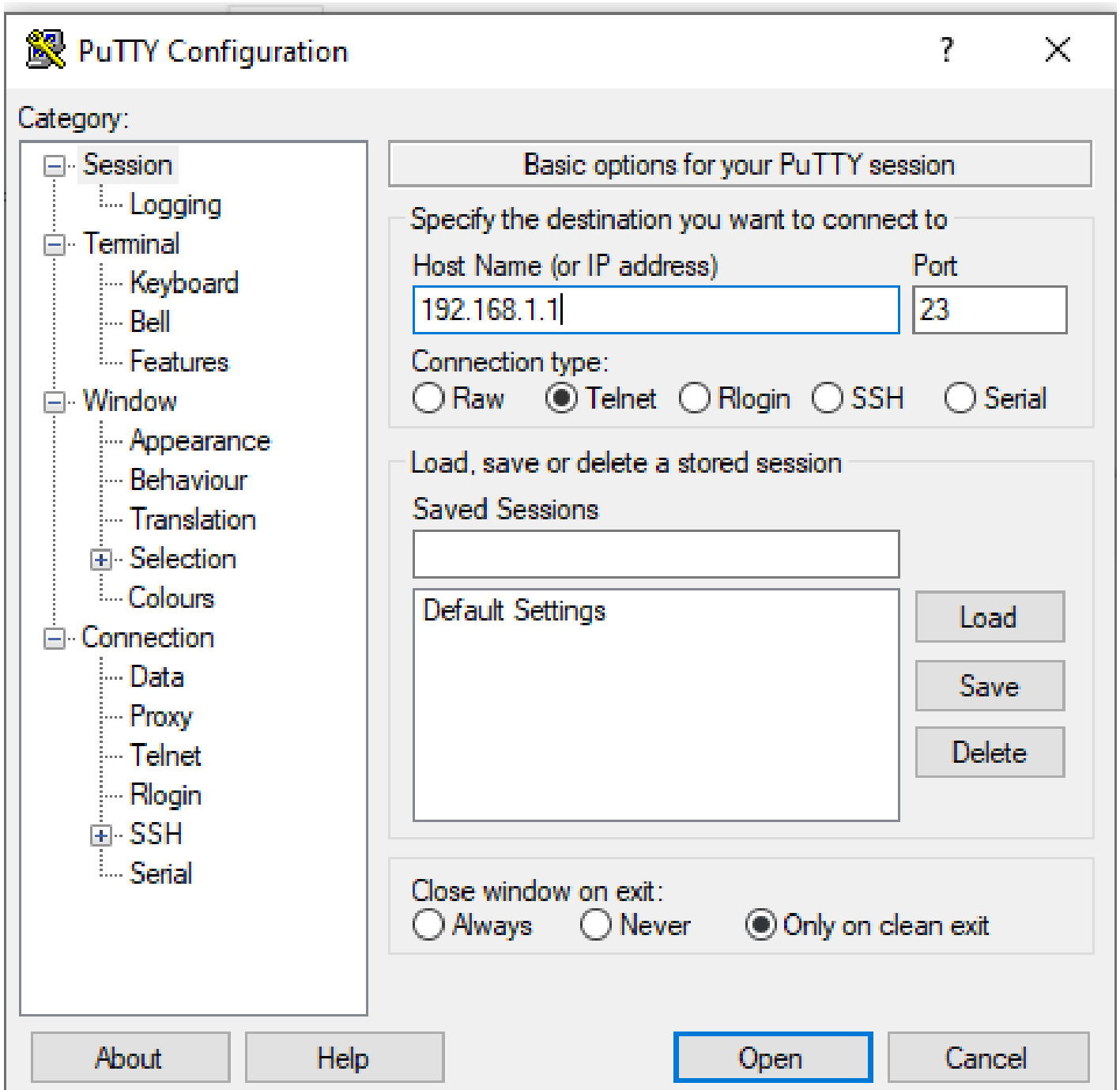


Fig 2.5.12 Putty for Telnet access of device page

```

192.168.1.1 - PuTTY
username: admin
passwd:
  console for English                               Version:
  CMD-COS-v1.01
-----
0. System status | WEB Address -> http://192.168.1.1:8
0
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:
  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 Router

To upgrade the Router is to get more functions and better performance.

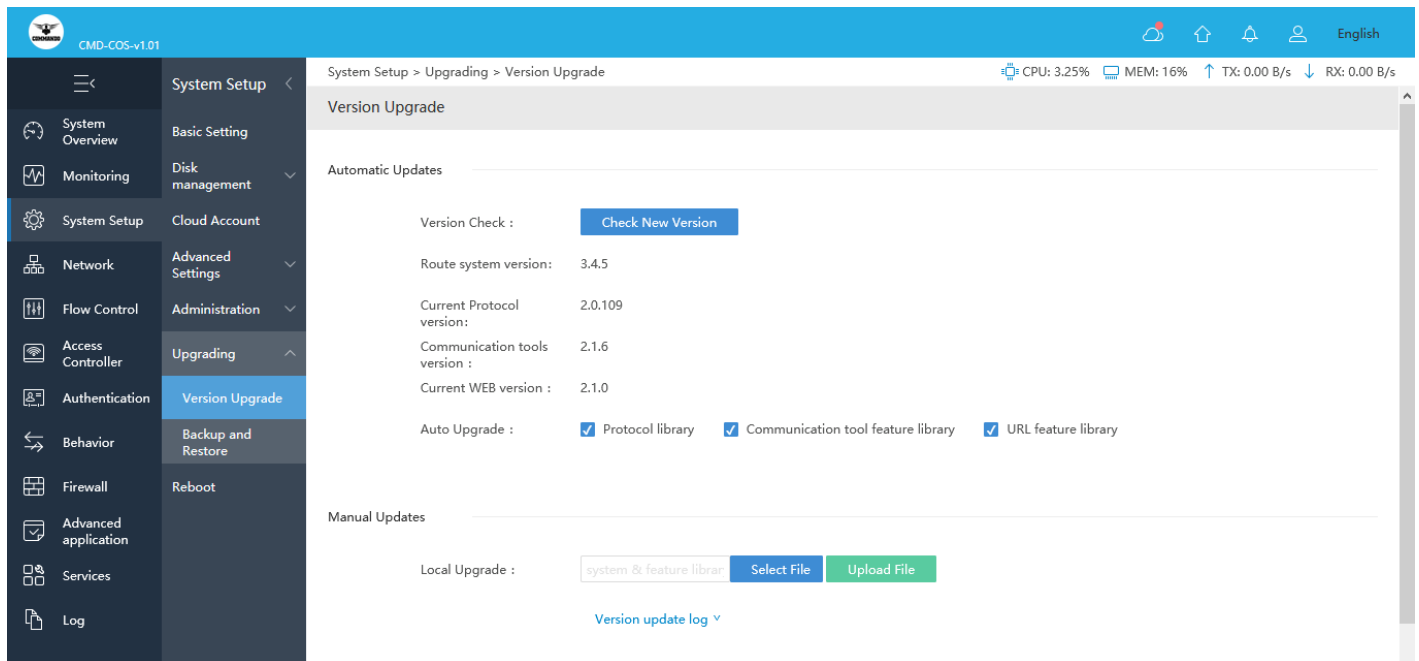
Note:

- 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.



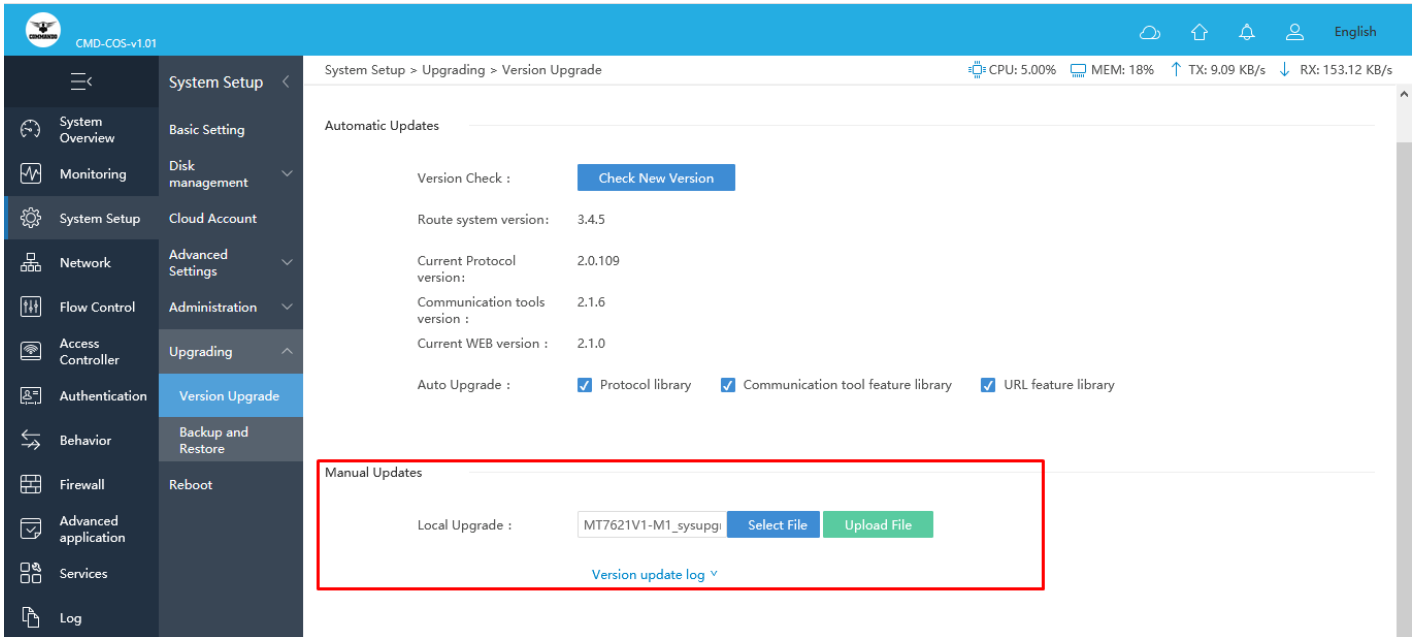
**Fig 2.6.1 Version Upgrade page**

### **Step 1:**

For Manual firmware update to version 3.4.5 COMMANDO Series R100 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.

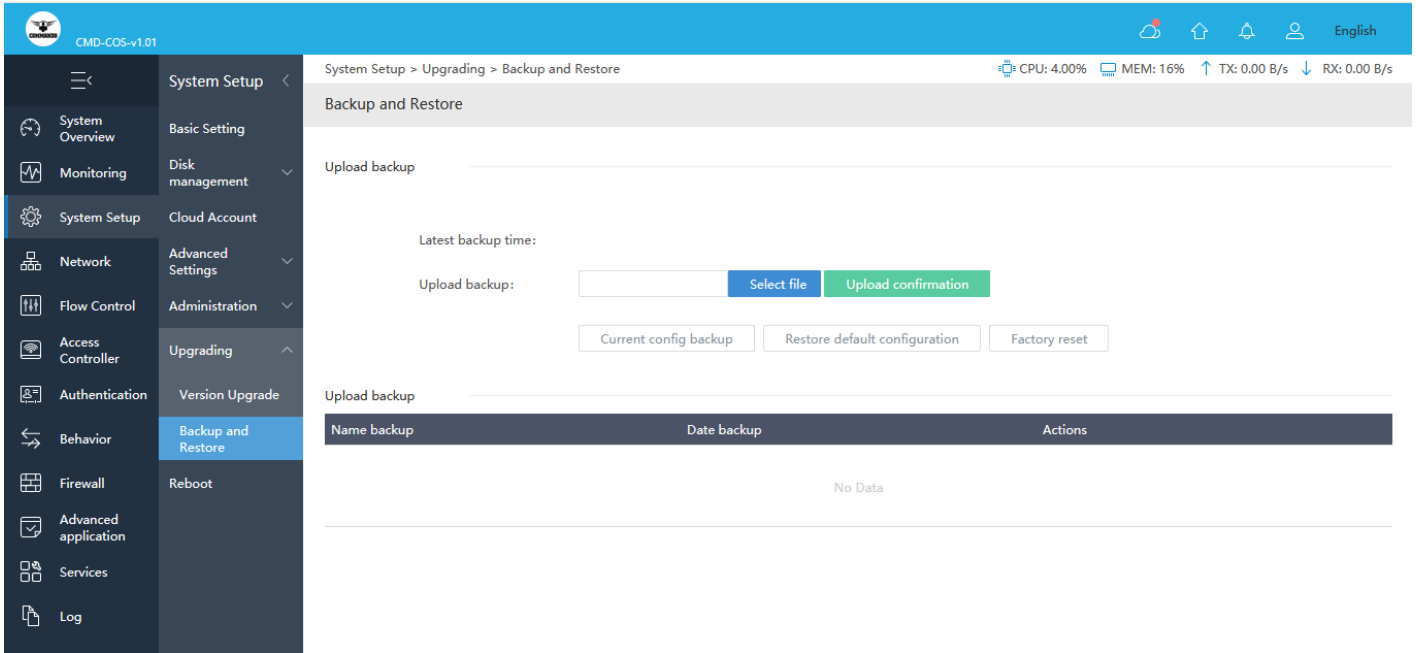


**Fig 2.6.2 Manual Version Upgrade page**

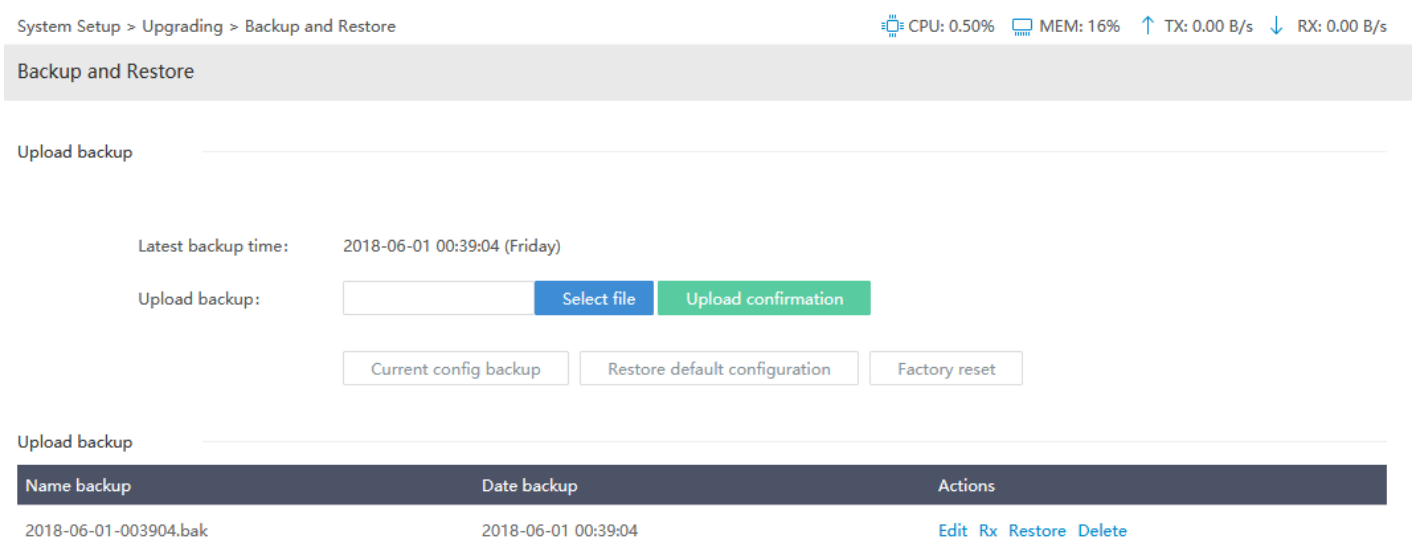
### **Backup and Restore:**

The Backup and Restore configuration feature allow end users to backup all configurations made to the router. In cases when you need to reset the router 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 router manually.

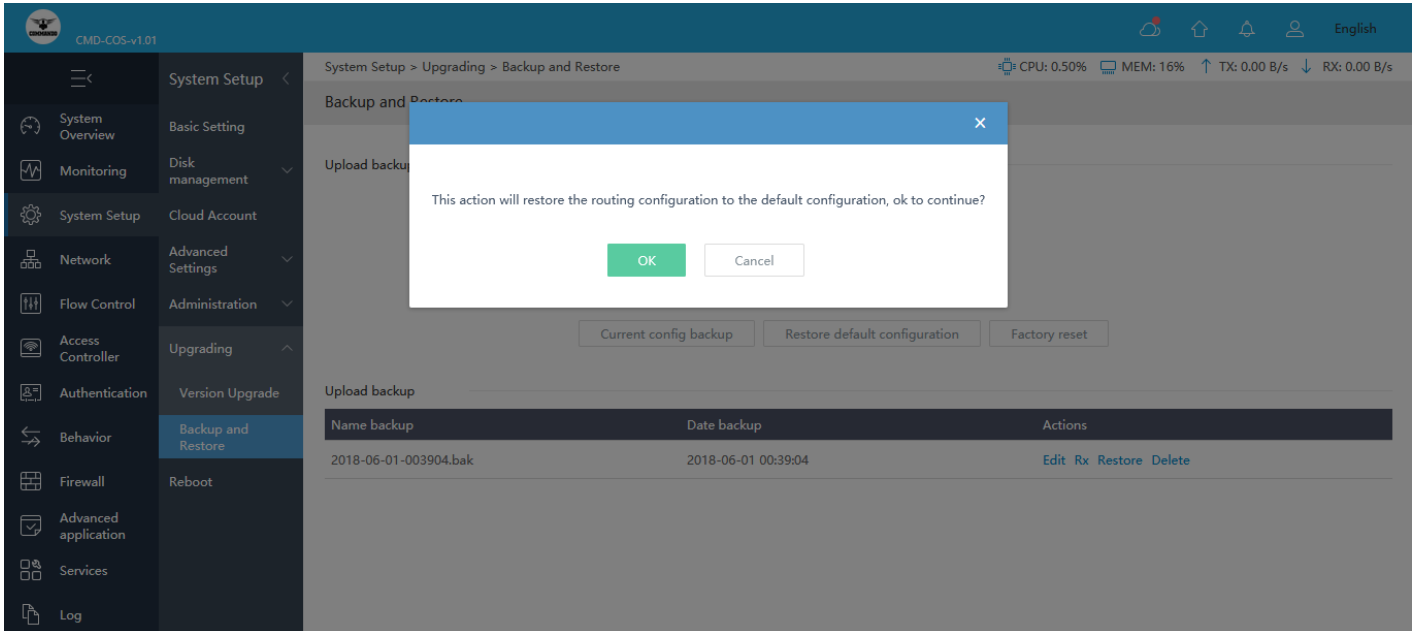
You can restore the router to its factory default settings by the Reset button or by factory reset option in this page. It must be noted that once the Router is reset, all the current configuration settings will be lost. If you want old config files which is backup already then can use option upload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



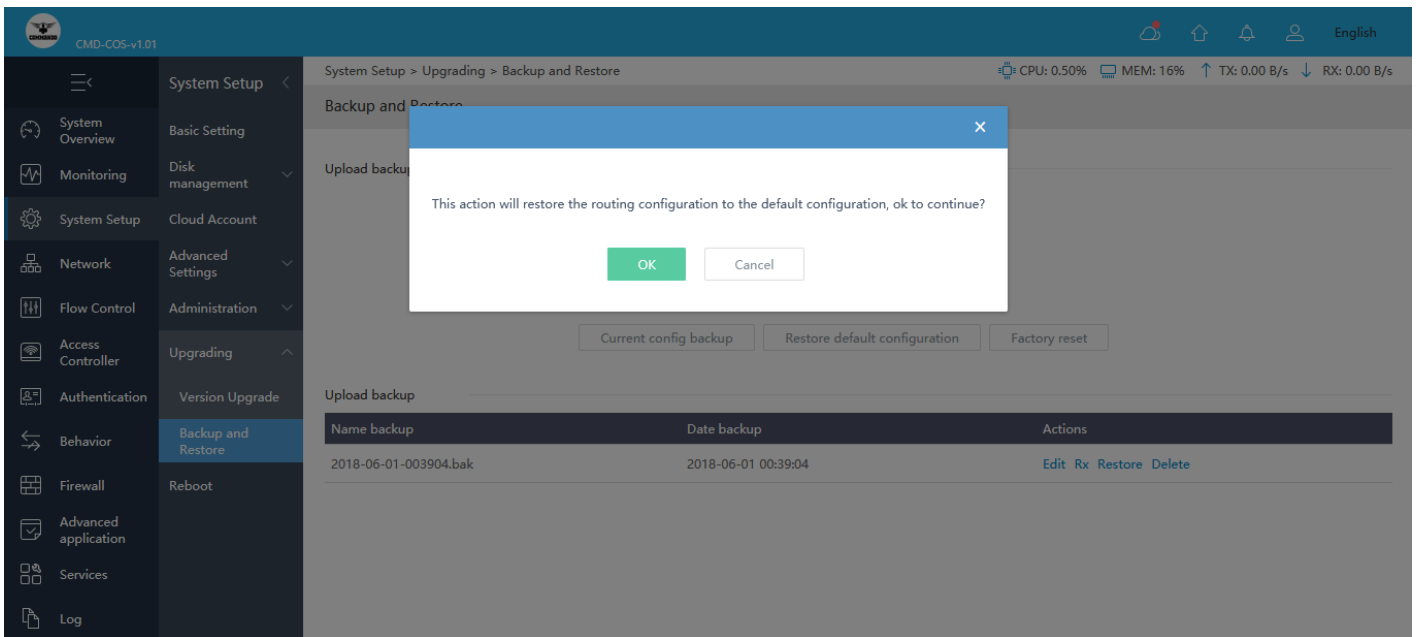
**Fig 2.6.3 Default Backup and Restore page**



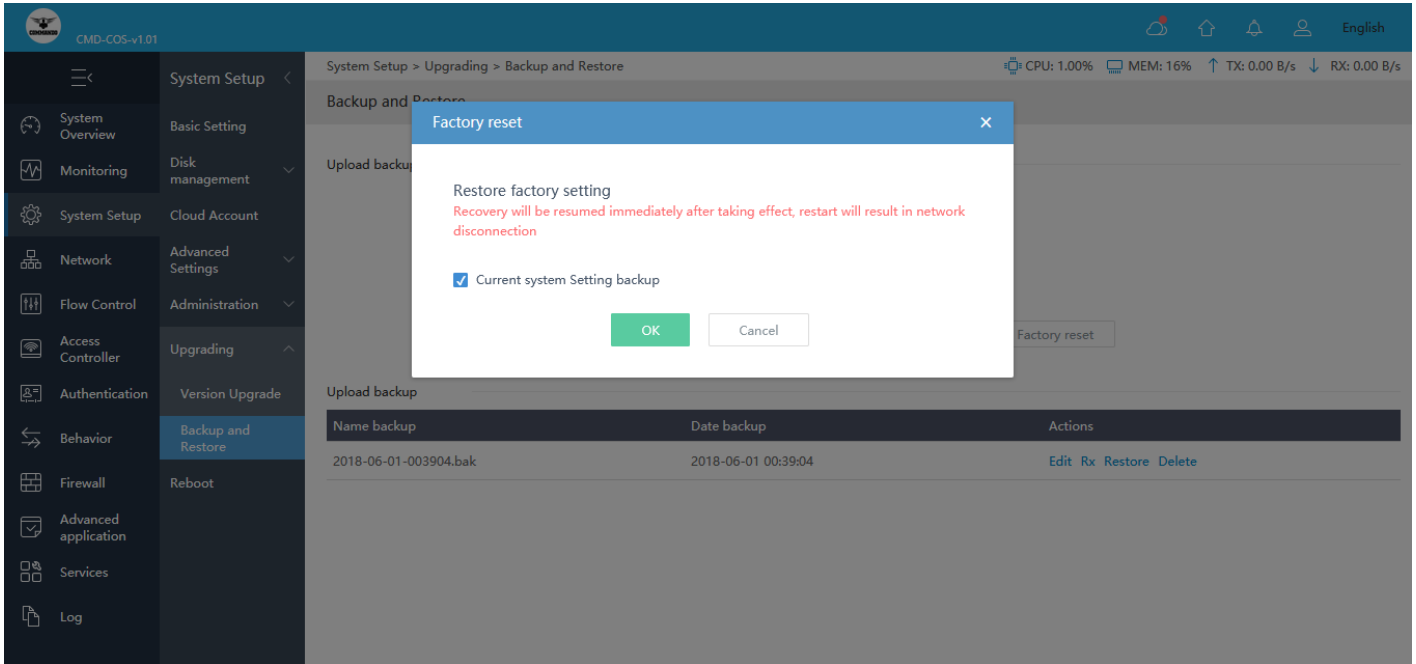
**Fig 2.6.4 Options Backup and Restore page**



**Fig 2.6.5 Backup the current configuration page**



**Fig 2.6.6 Restoring default configuration page**

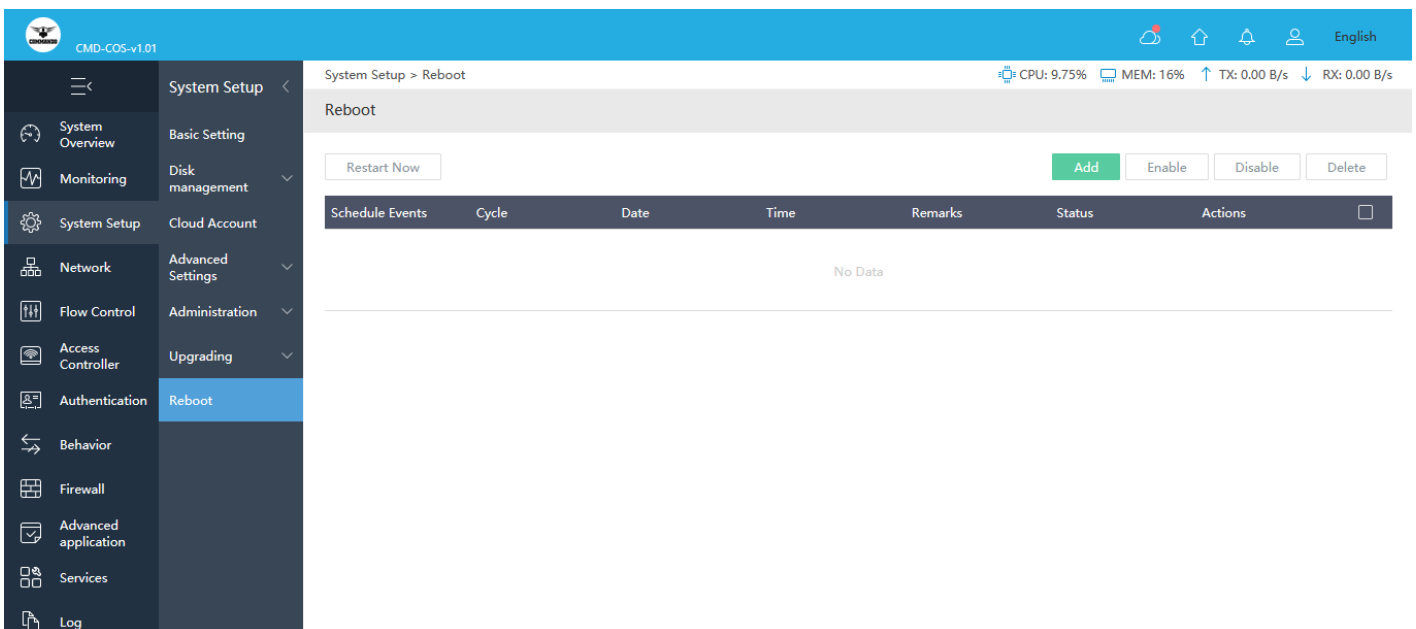


**Fig 2.6.7 Restore Factory setting page**

## 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**

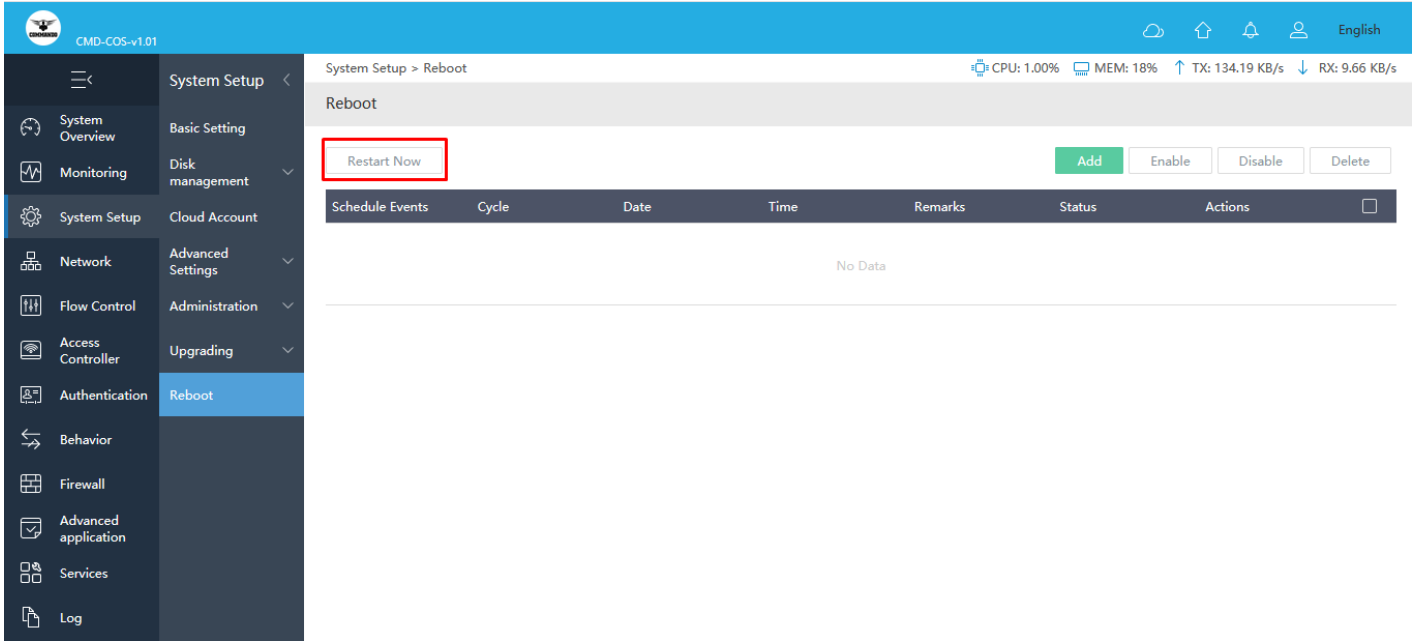


Fig 2.7.2 Restart Now page

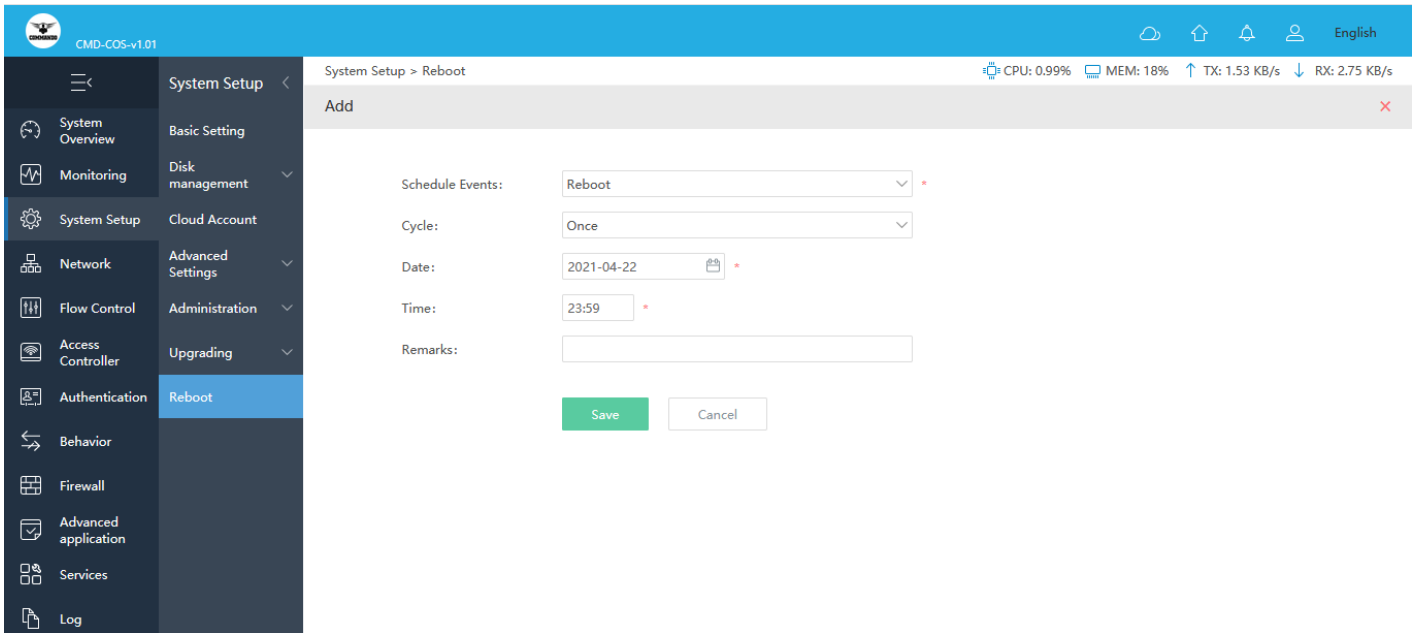
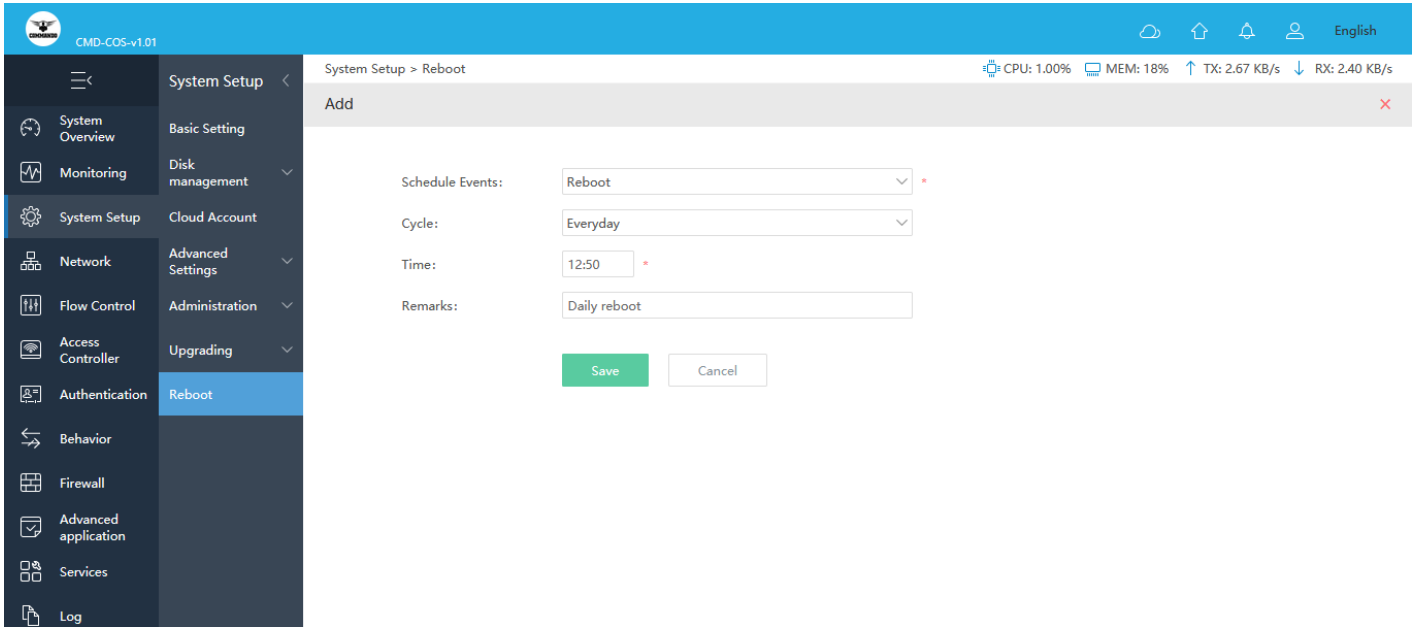
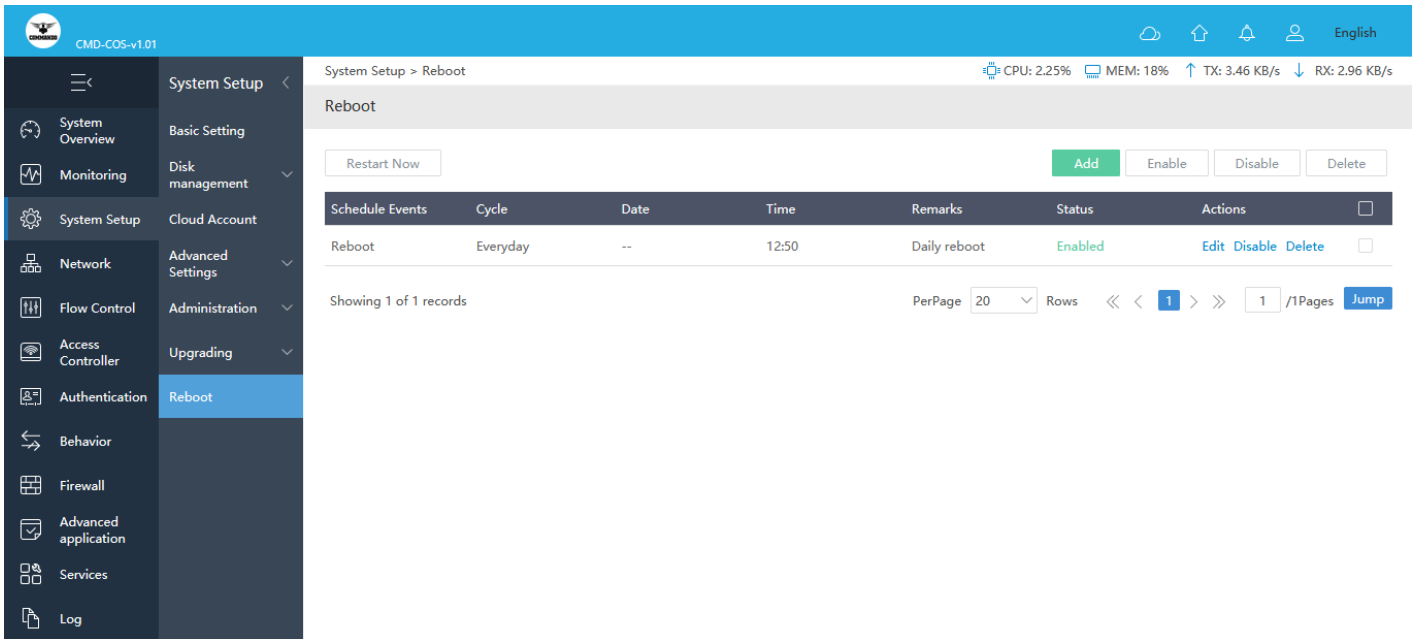


Fig 2.7.3 Default Schedule Restart page





**Fig 2.7.4 Add Schedule Restart page**



**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 router 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 router 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 router to forward all incoming traffic from the internet to the device specified, virtually disabling the routers "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 router 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:

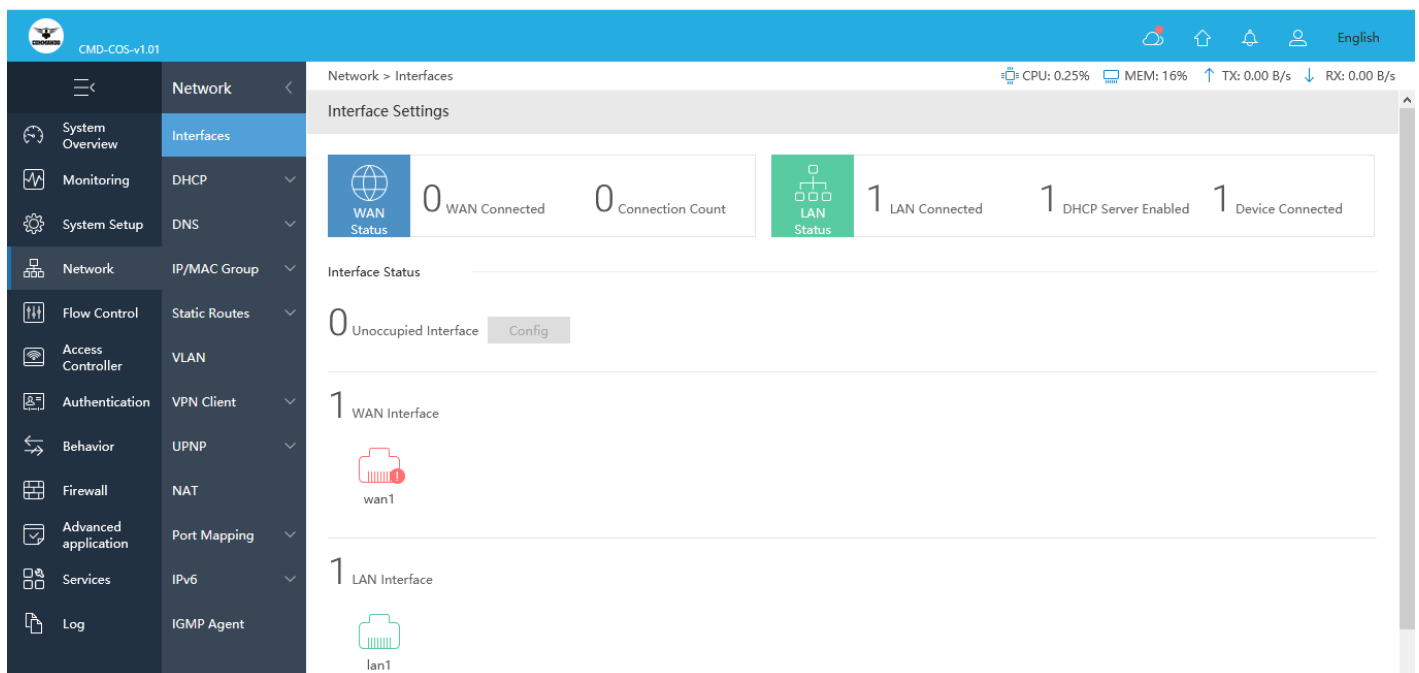
The IGMP Agent is responsible for forwarding multicast messages only to VMs that are registered to that multicast group, while respecting the filtering fields that are defined in IGMPv3. VM registration is detected by processing IGMP Join packets that all subscribed VMs send.

**Fig 3.1 Network Tab options page**

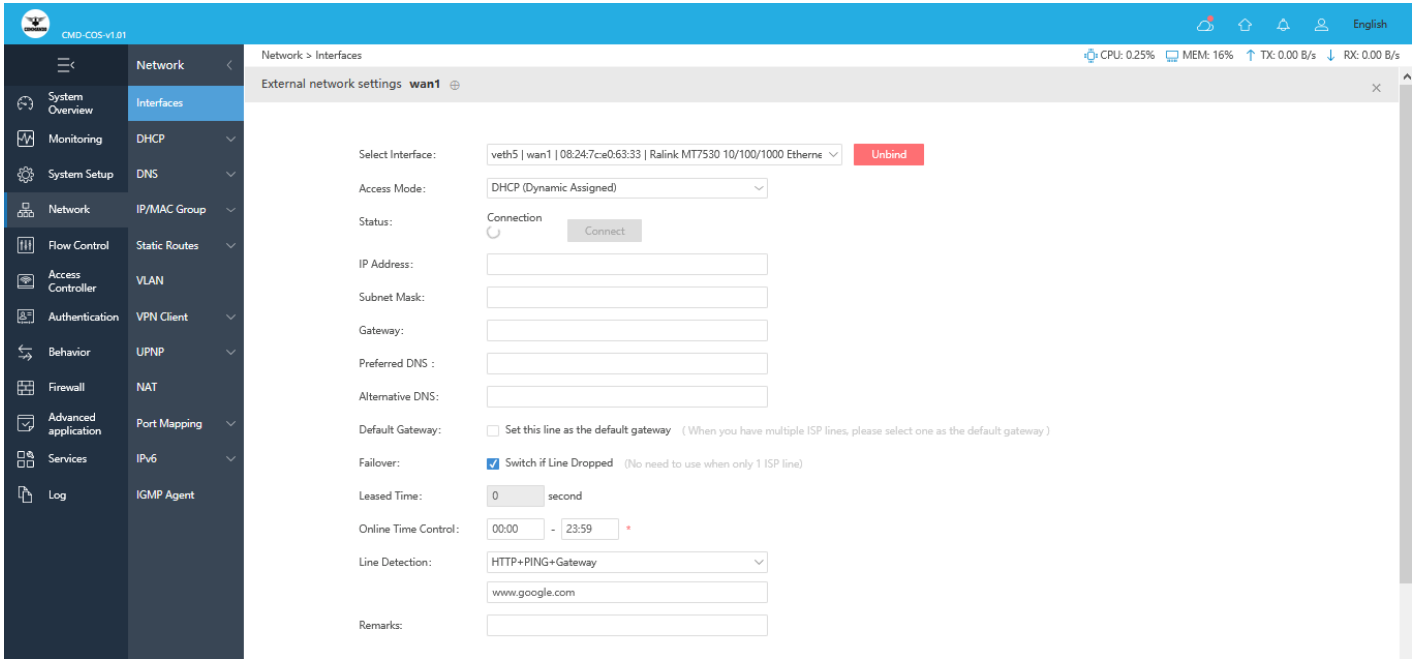
### 1. Interfaces

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.

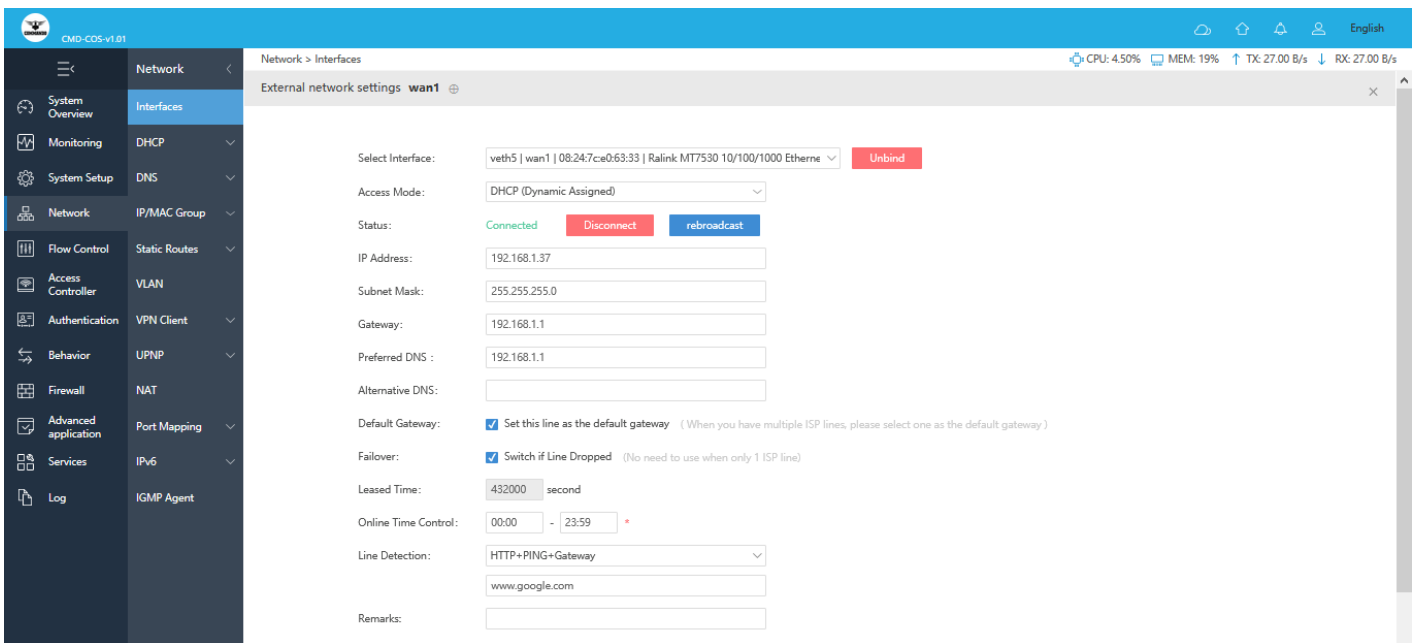
You can create and access all ports parameter of interfaces by clicking Network > Interfaces



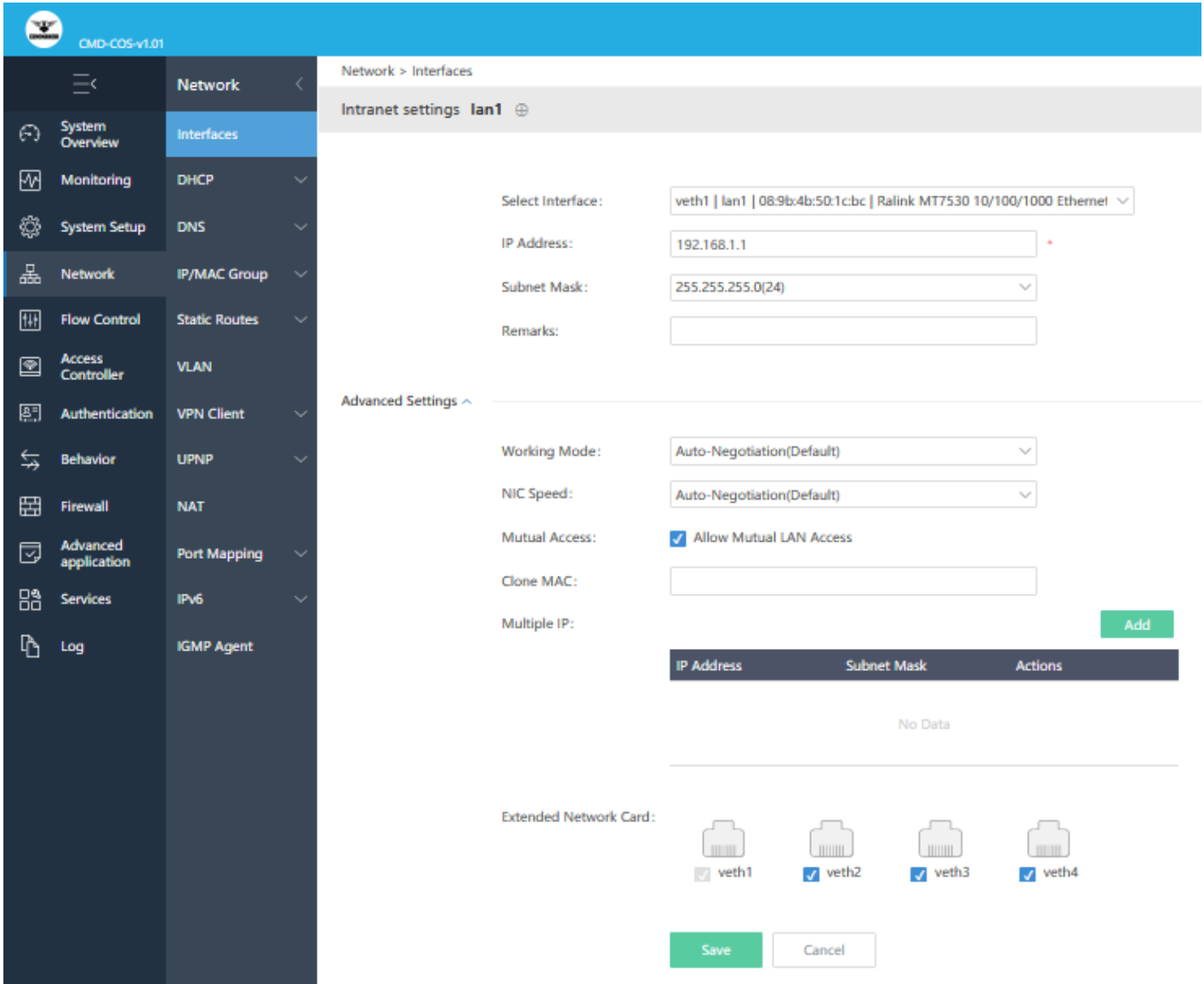
**Fig 3.1.1 Default interface setting page**



**Fig 3.1.2 Default External Network setting options**

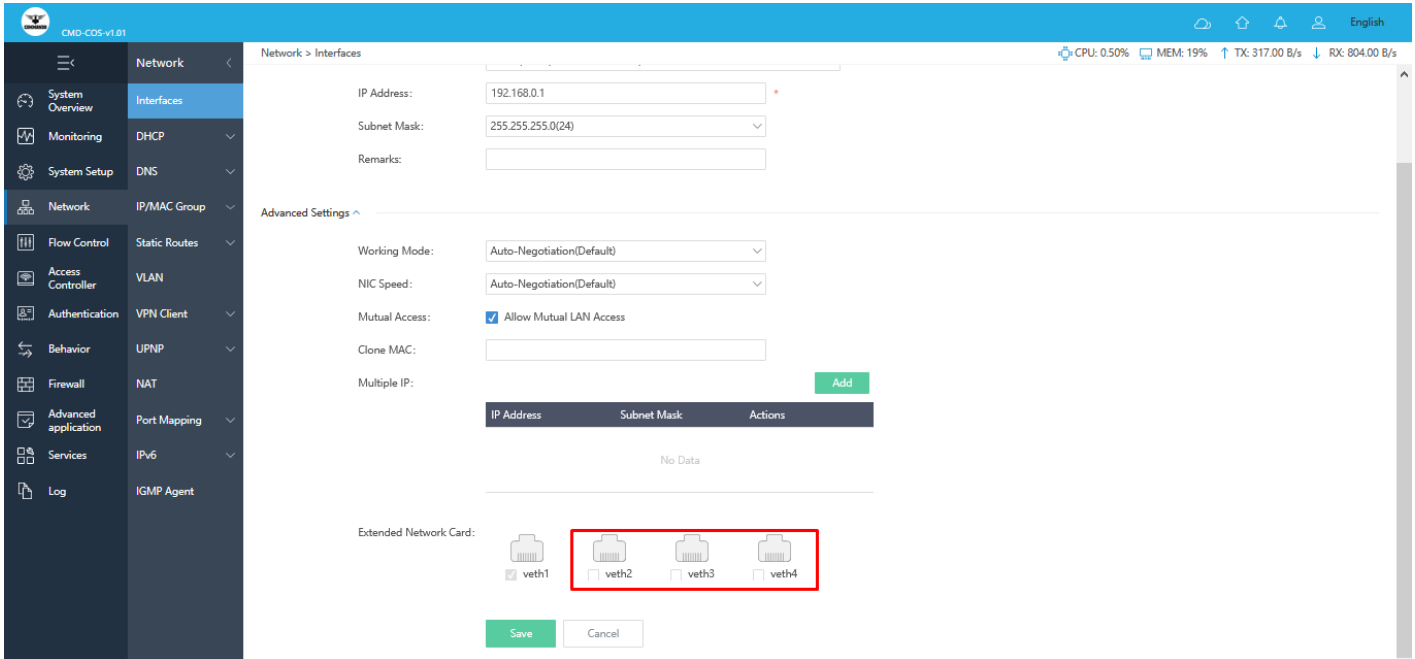


**Fig 3.1.3 Setting External Network setting for WAN1 interface page**



**Fig 3.1.5 Default intranet Network setting for LAN1 interface page**

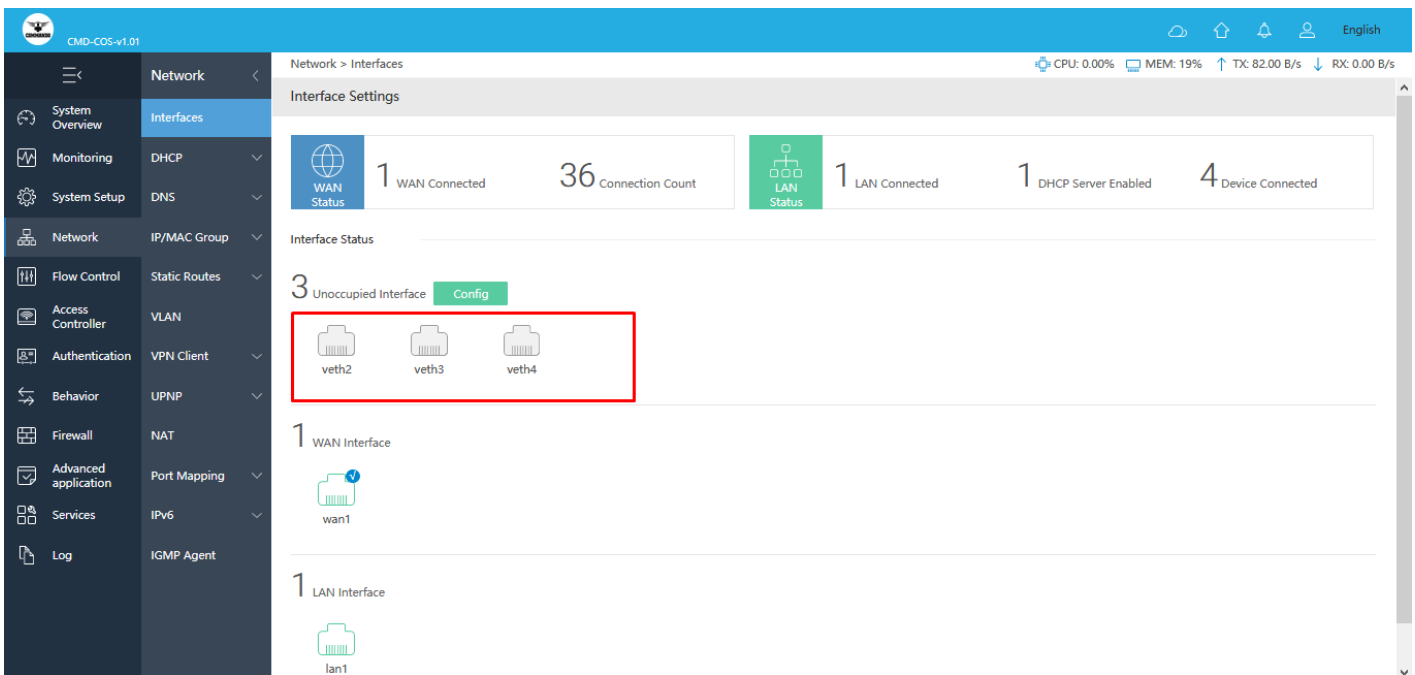
**Note:** By default all 4 LAN ports are mapped and activated namely veth 1,2,3,4 in LAN1.



**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**

NIC Usage:  LAN (Private)  WAN (Public)

Select Interface:  Bind

veth2 | free | 08:24:7c:e0:63:30 | Ralink MT7530 10/100/1000 Ethernet Controller

veth3 | free | 08:24:7c:e0:63:31 | Ralink MT7530 10/100/1000 Ethernet Controller

veth4 | free | 08:24:7c:e0:63:32 | Ralink MT7530 10/100/1000 Ethernet Controller

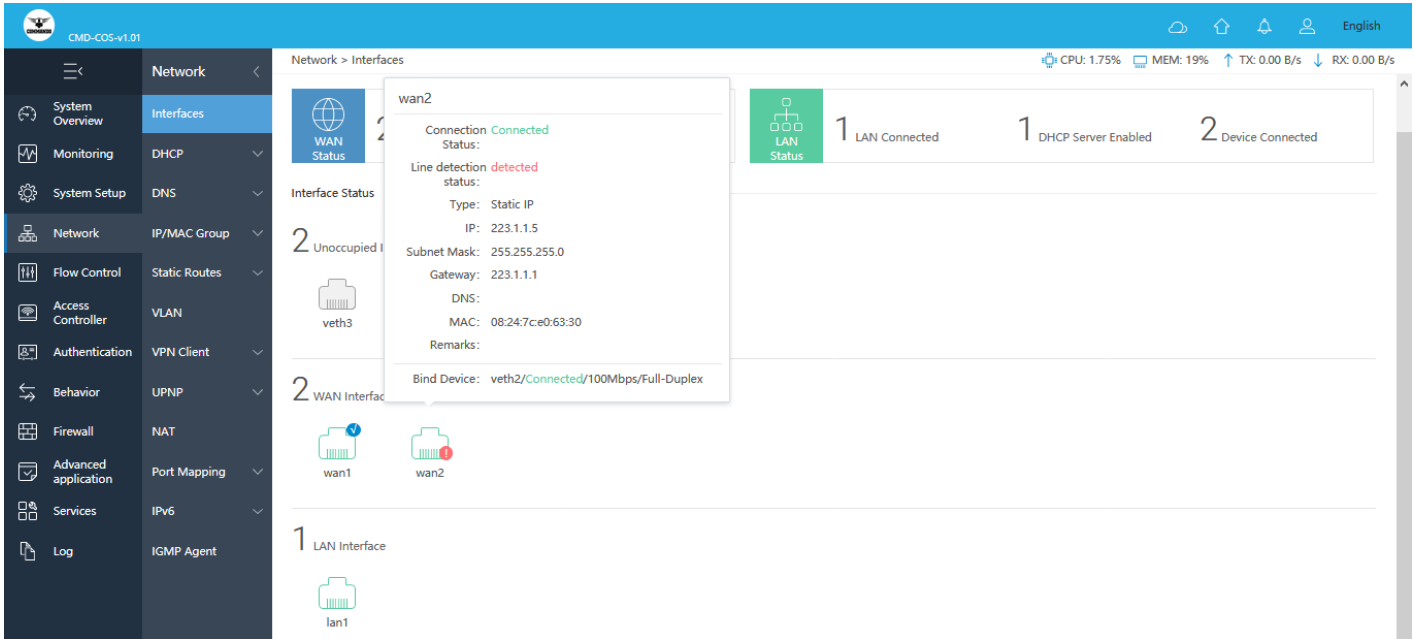
**Fig 3.1.8 Select Interface setting for LAN and WAN interface page**

The screenshot shows the 'External network settings' page for the 'wan2' interface. The interface is currently selected in the dropdown menu. The configuration includes:

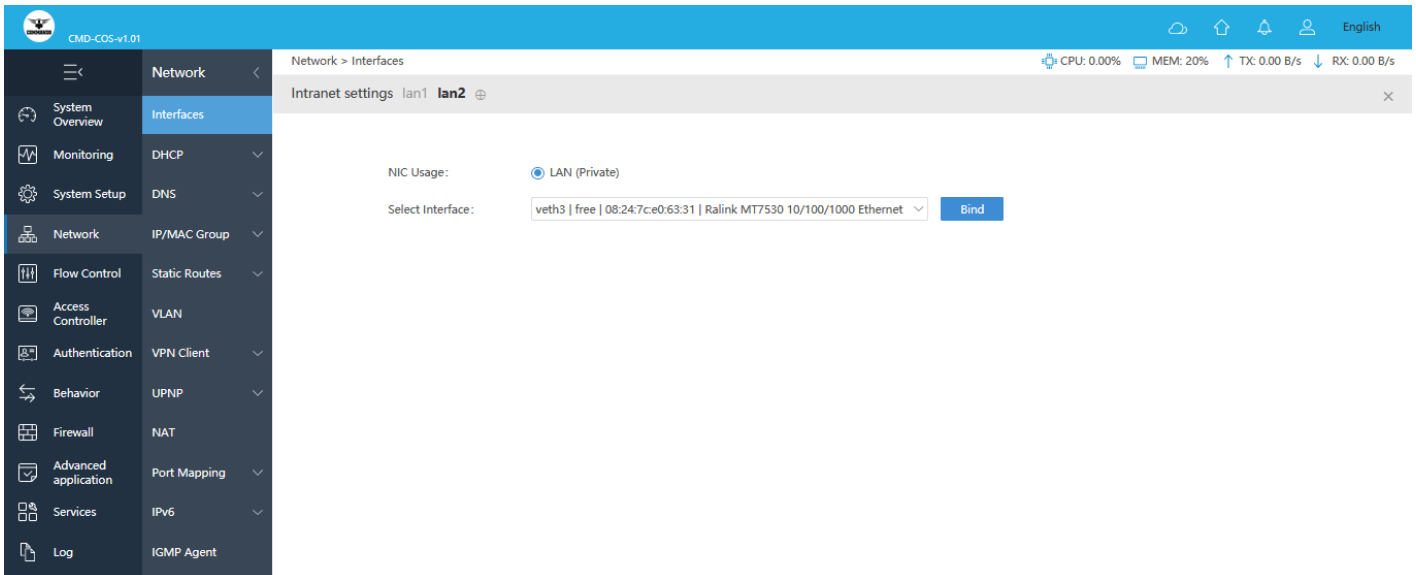
- Select Interface:** veth2 | wan2 | 08:24:7c:e0:63:30 | Ralink MT7530 10/100/1000 Ethernet Controller (with an 'Unbind' button)
- Access Mode:** Static IP (Fixed IP)
- IP Address:** 223.1.1.5
- Subnet Mask:** 255.255.255.0(24)
- Gateway:** 223.1.1.1
- Multiple IP:** A table with columns for IP Address, Subnet Mask, and Actions. An 'Add' button is present above the table.
- Default Gateway:**  Set this line as the default gateway (When you have multiple ISP lines, please select one as the default gateway)
- Failover:**  Switch if Line Dropped (No need to use when only 1 ISP line)

**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**

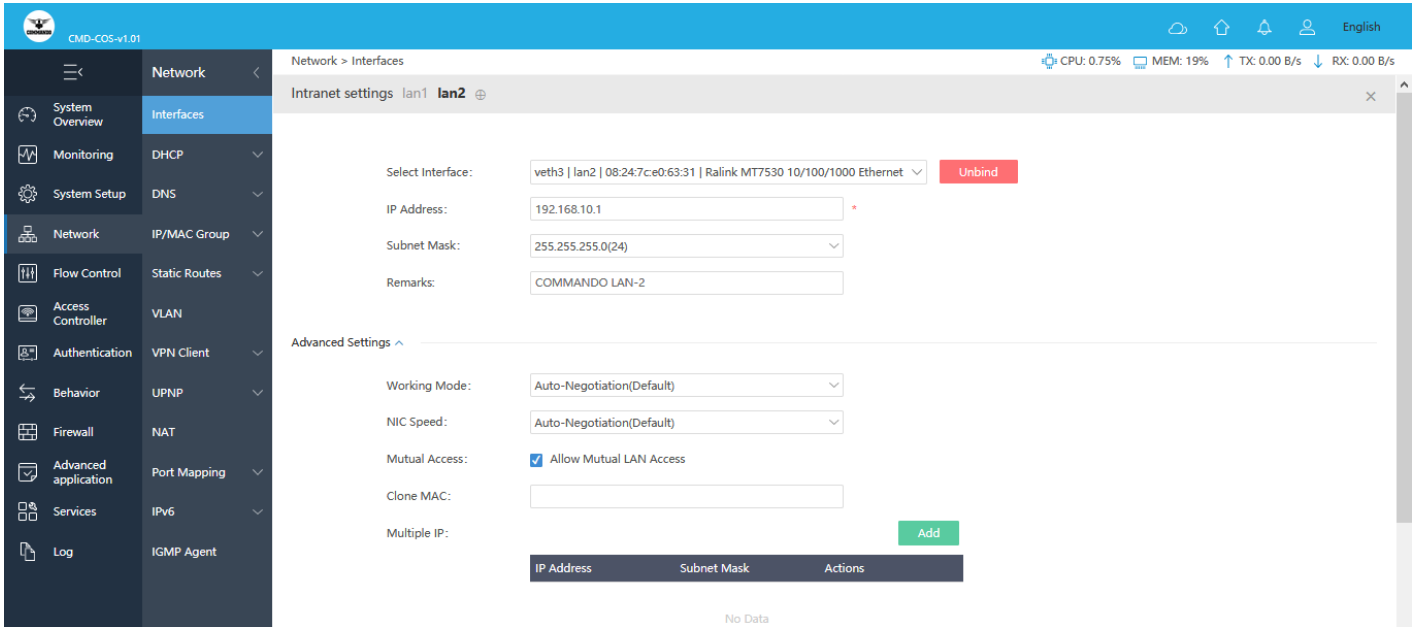


Fig 3.1.12 Setting LAN2 interface parameter page

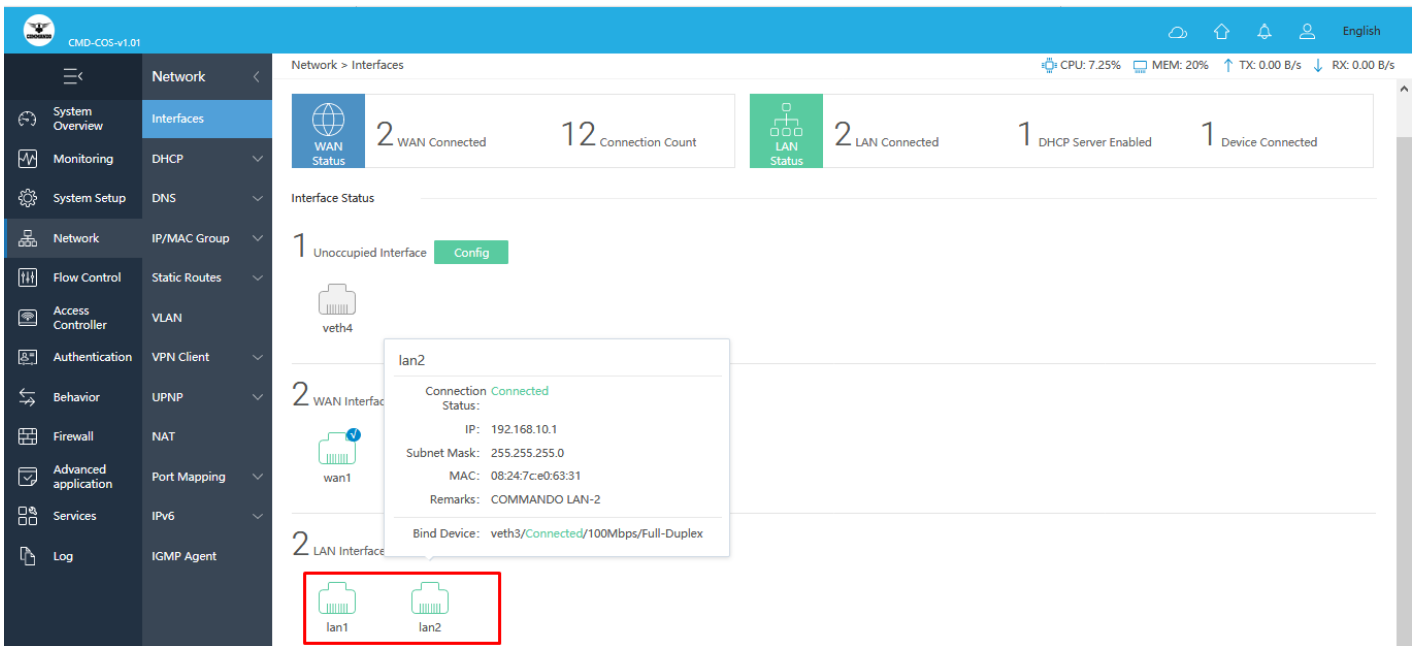
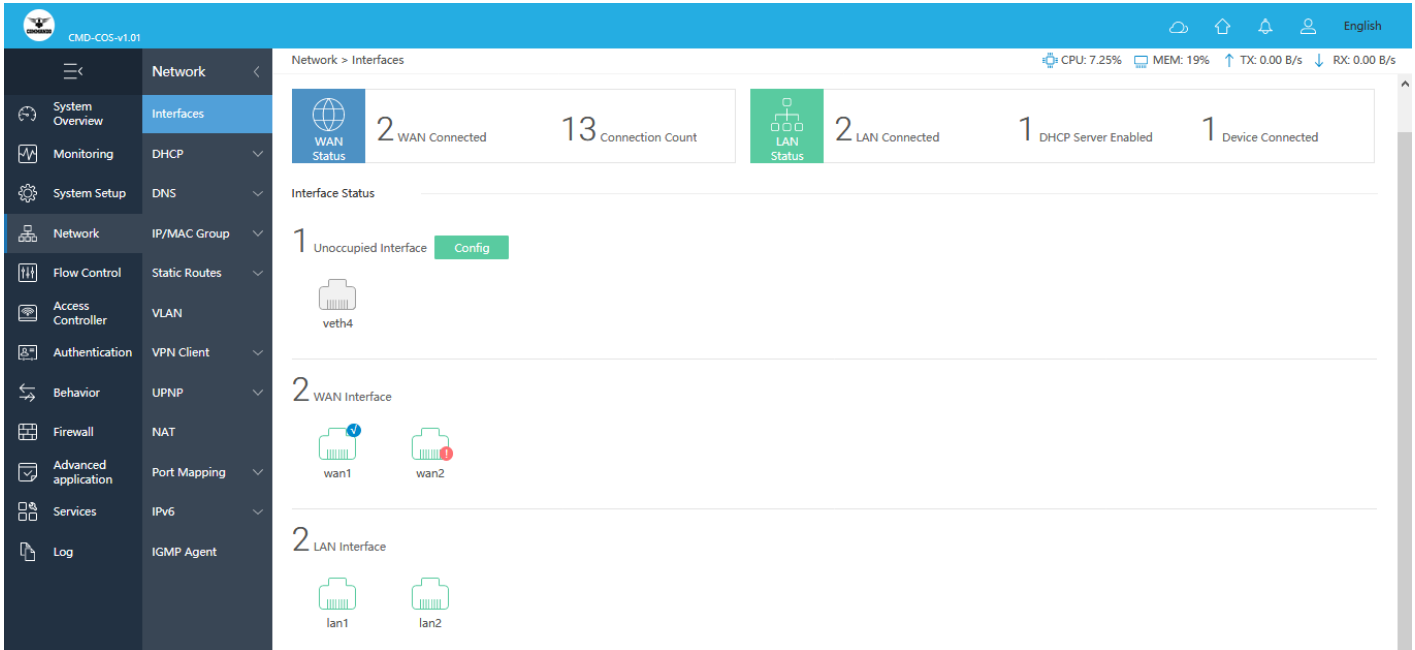


Fig 3.1.13 Network interface page after creating LAN2 interface page

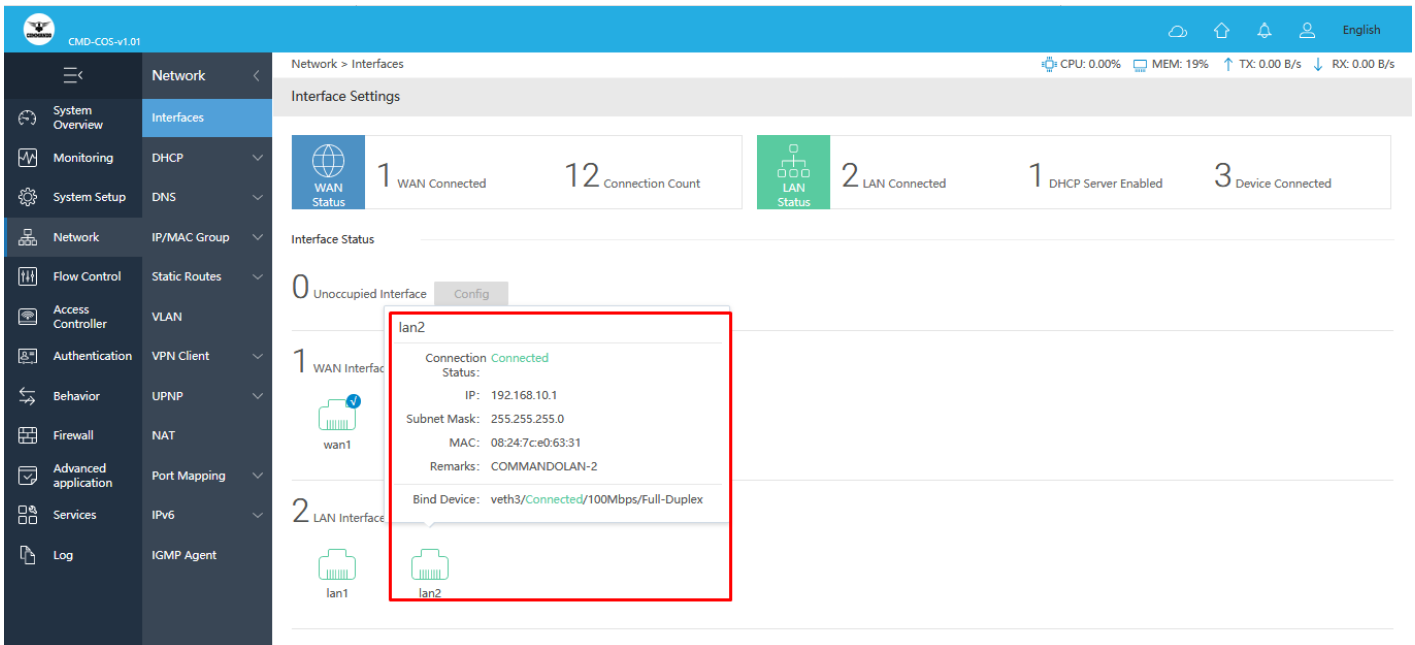


**Fig 3.1.14 Network interface page after creating user defined interfaces page**

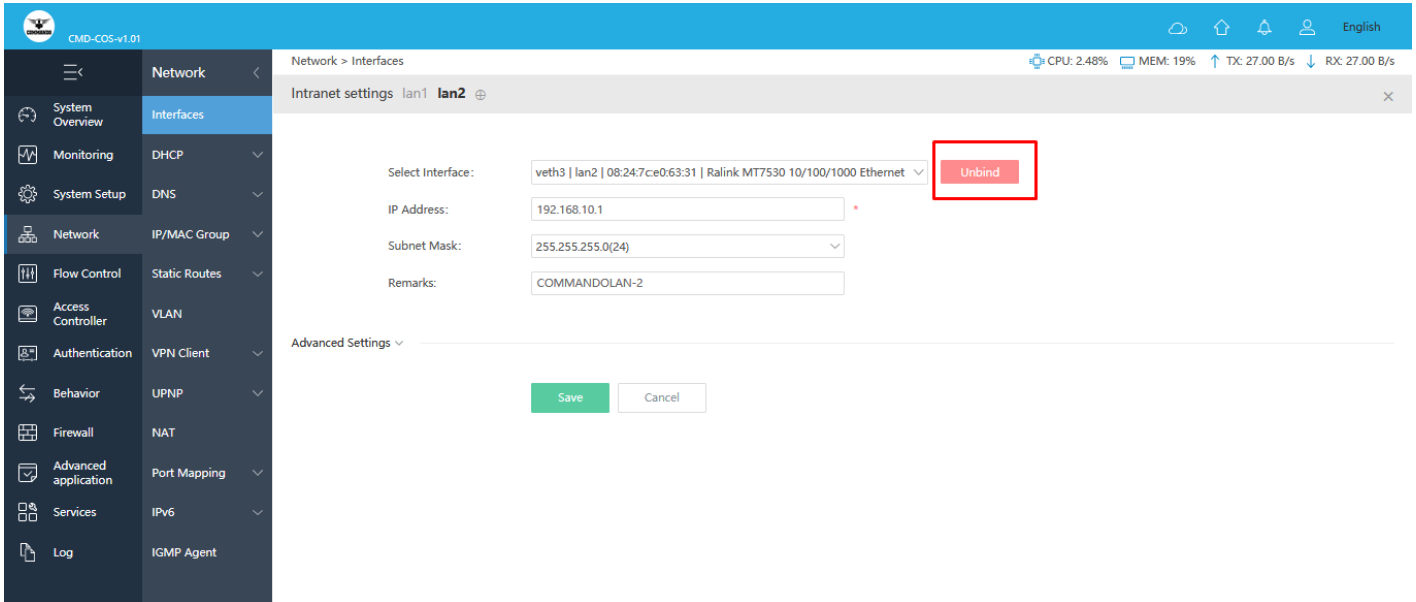
### How to delete unwanted interfaces?

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

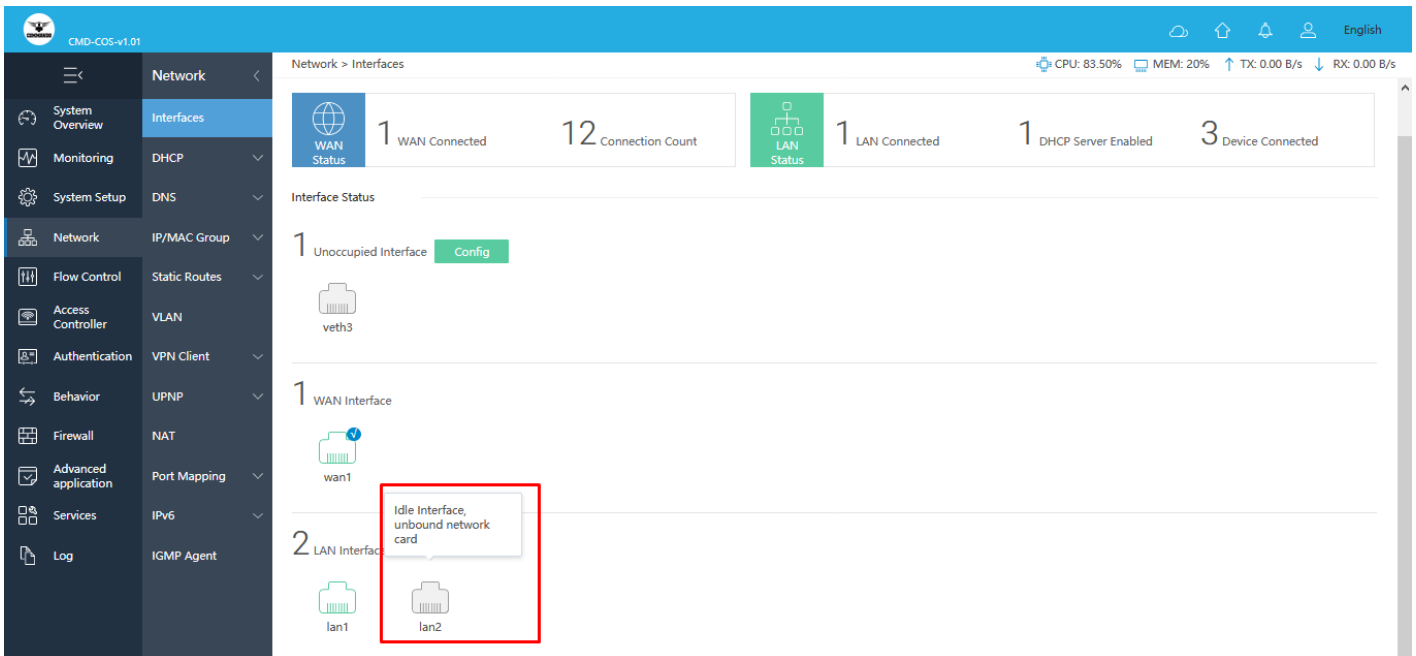
Example: If you want to delete LAN2 port



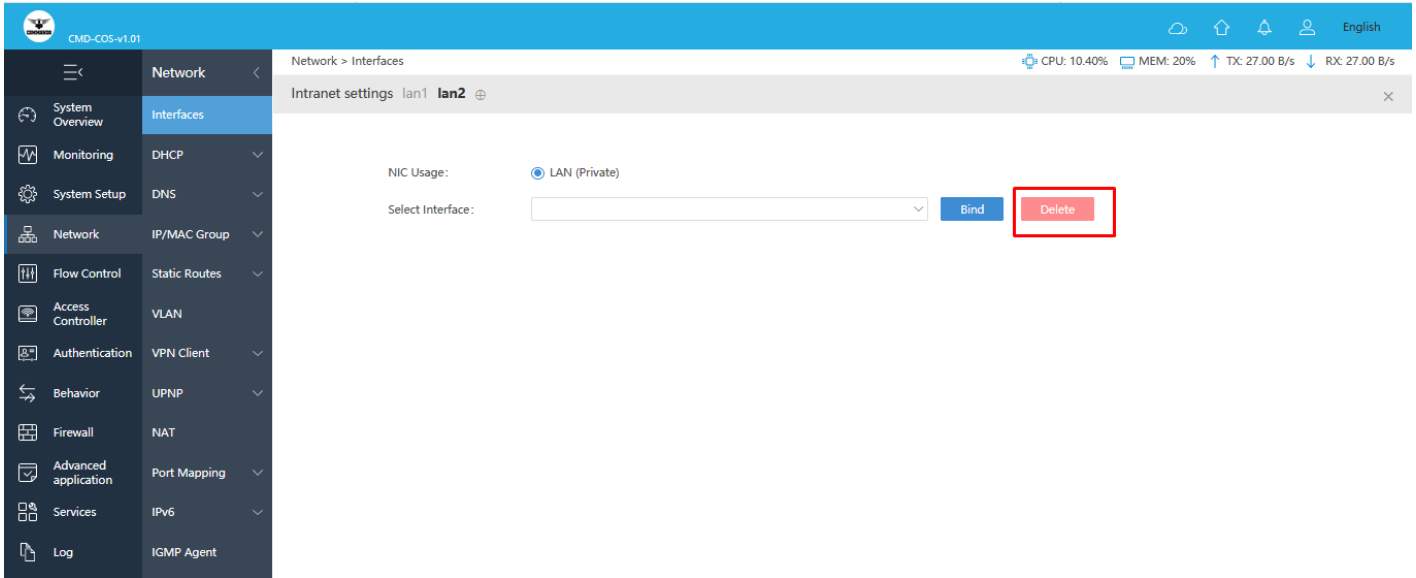
**Fig 3.1.15 Deleting interface after creating user defined LAN2 interface page**



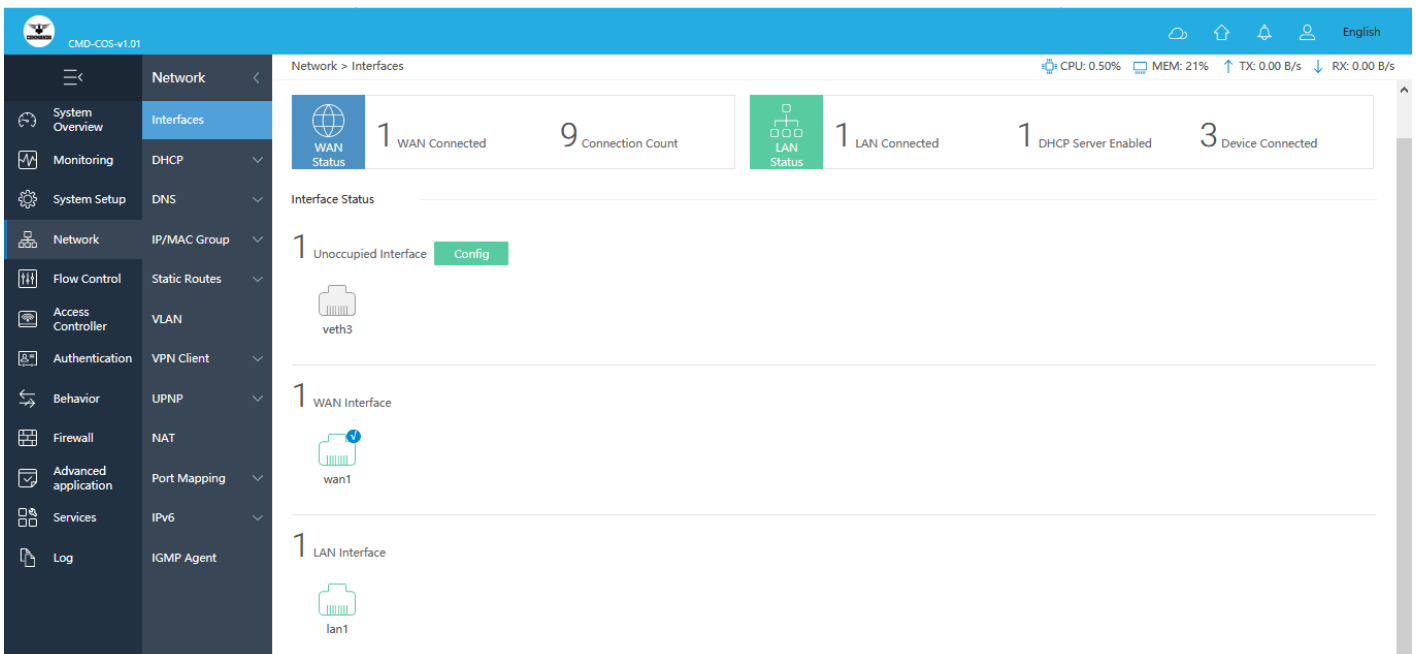
**Fig 3.1.16 Unbinding port from LAN2 interface page**



**Fig 3.1.16 Network interface page after unbinding port from LAN2 interface page**



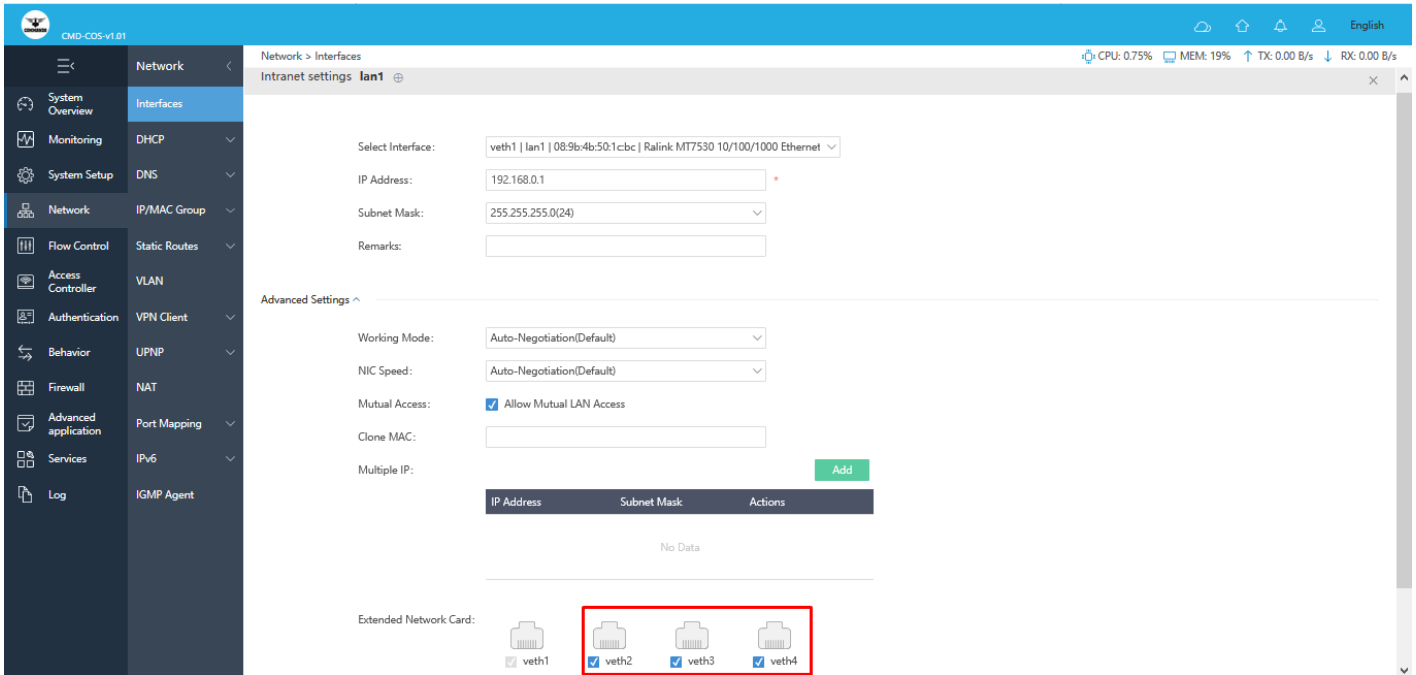
**Fig 3.1.17 Deleting port from LAN2 interface page**



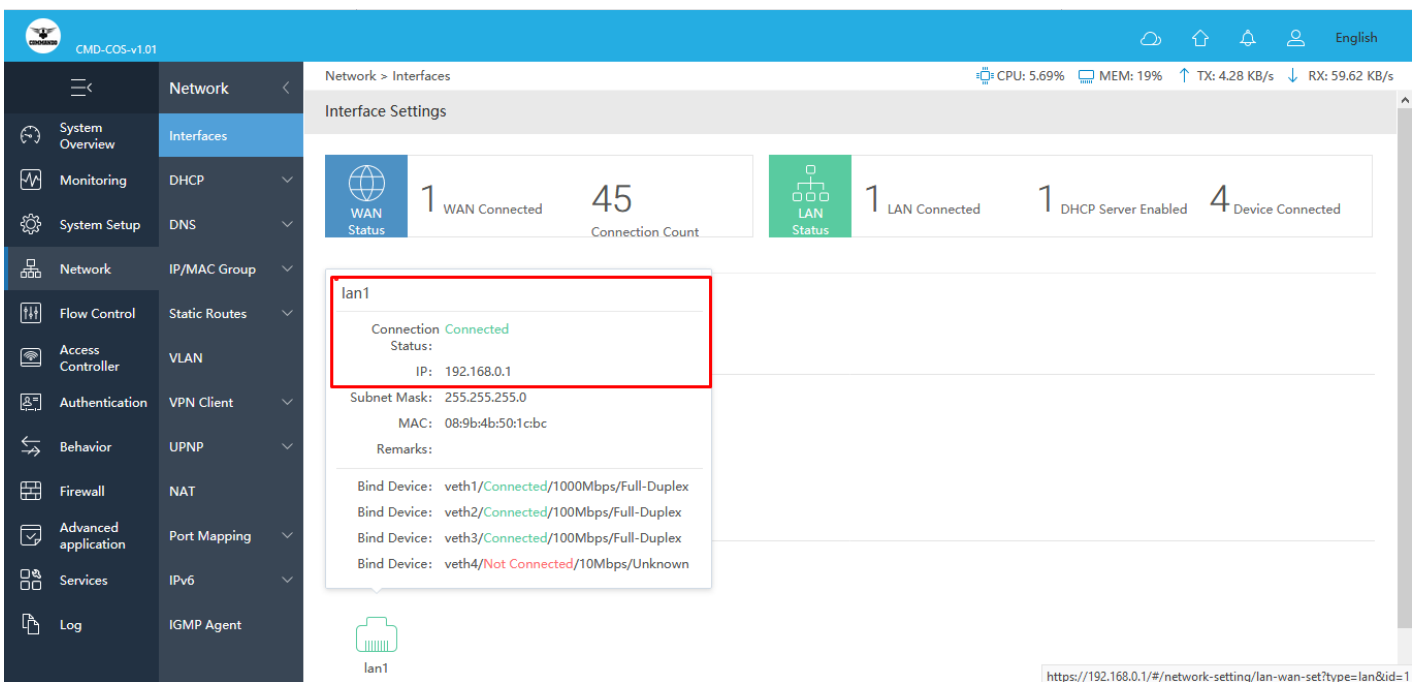
**Fig 3.1.18 Network interface page after deleting LAN2 interface page**

### 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 3.1.19 Binding ports 2,3,4 to LAN1 interface page**



**Fig 3.1.19 Interface setting of LAN1 interface page**

## 2. DHCP

The Router 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 Router'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 Router'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

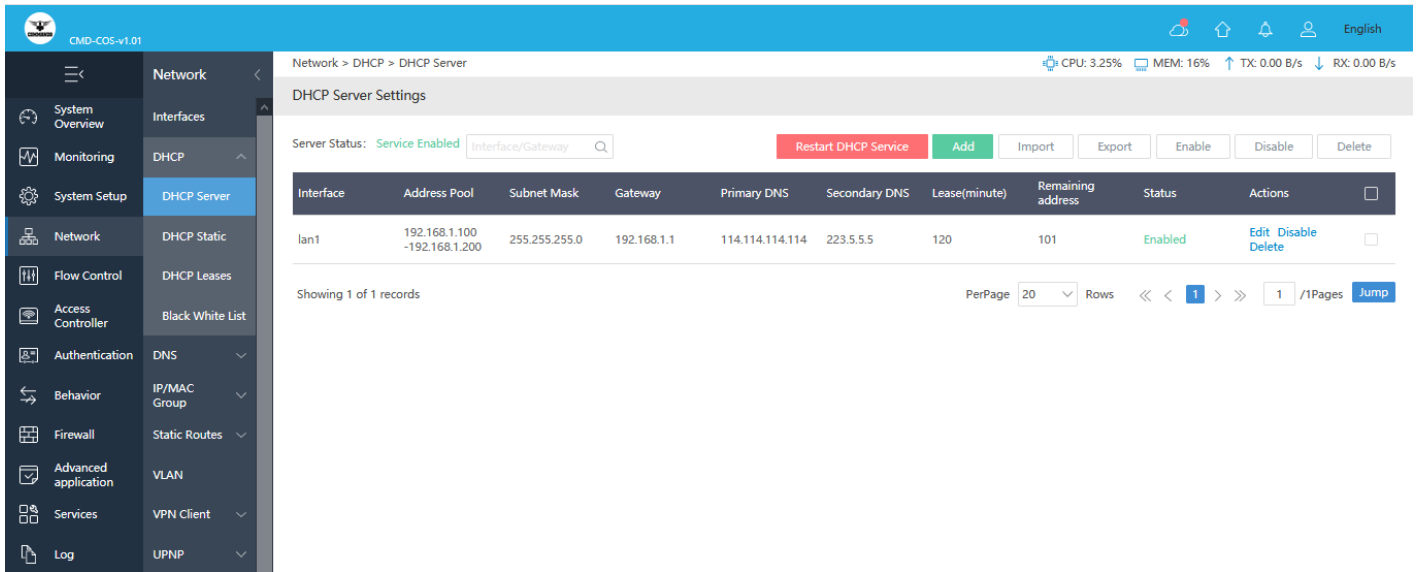


Fig 3.2.1 Default DHCP Server Settings of LAN1 interface page

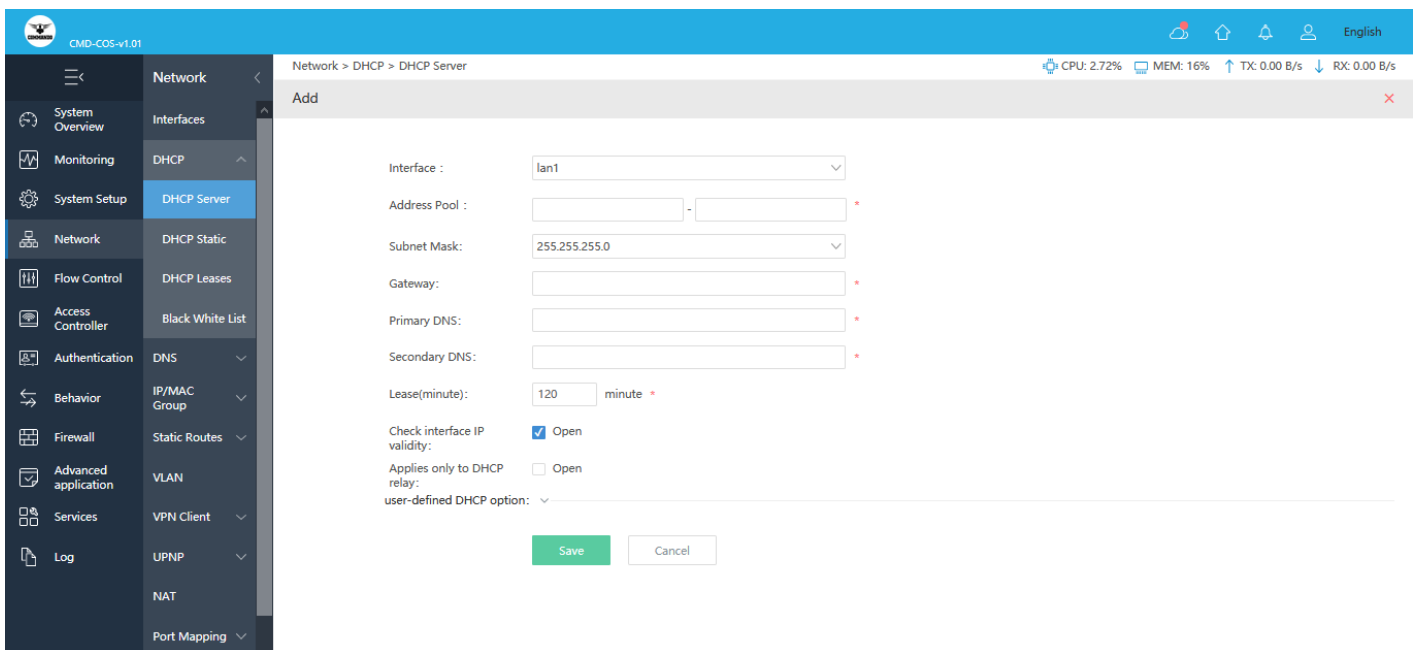
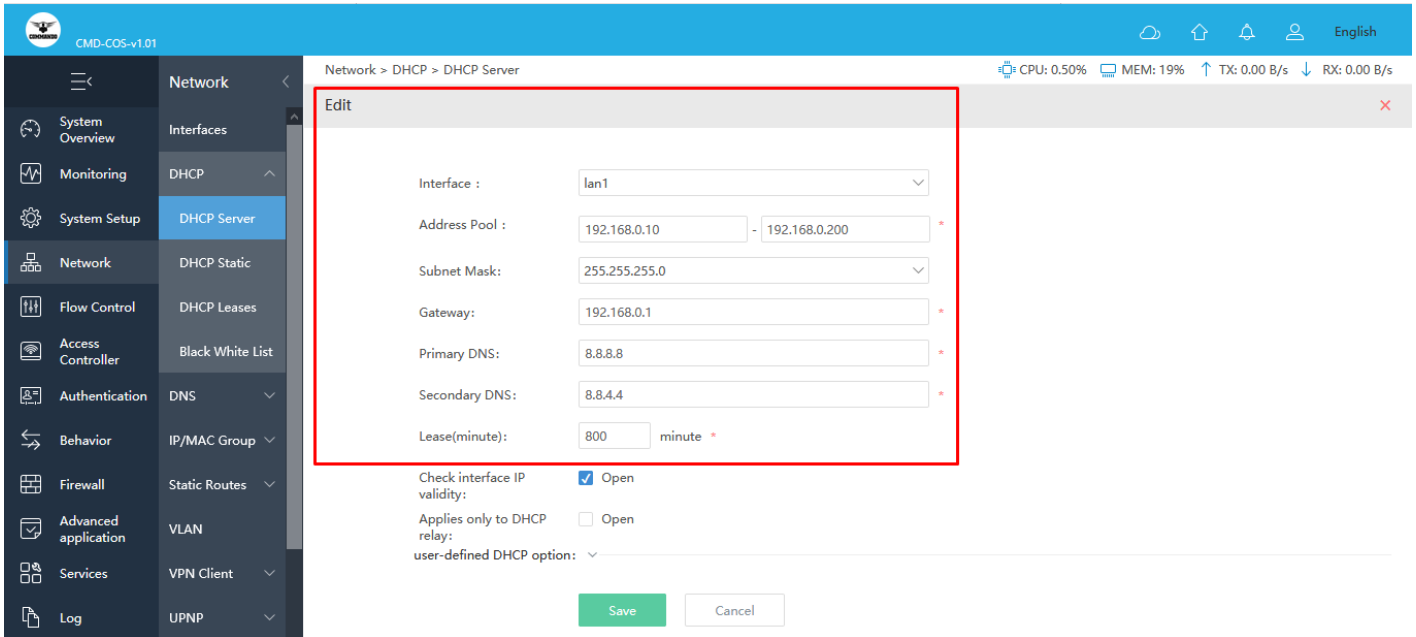
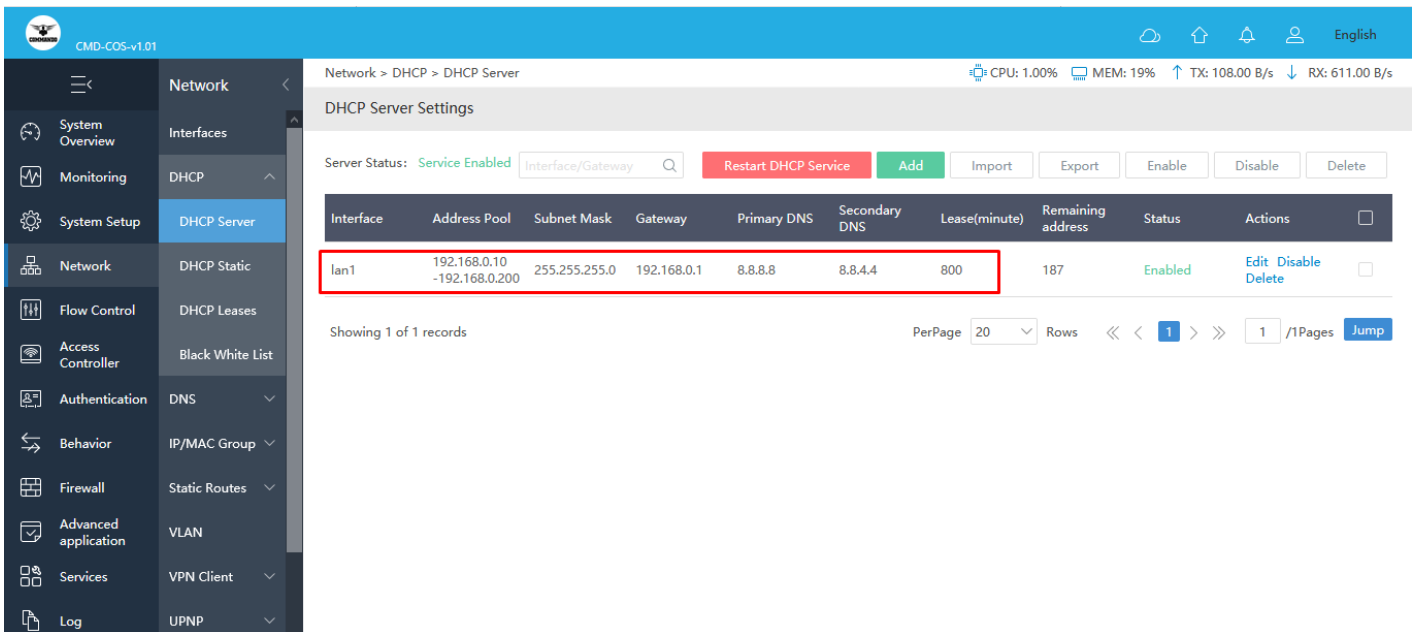


Fig 3.2.2 Add DHCP Server Settings of LAN1 interface page





**Fig 3.2.3 Editing DHCP Server Settings of LAN1 interface page**

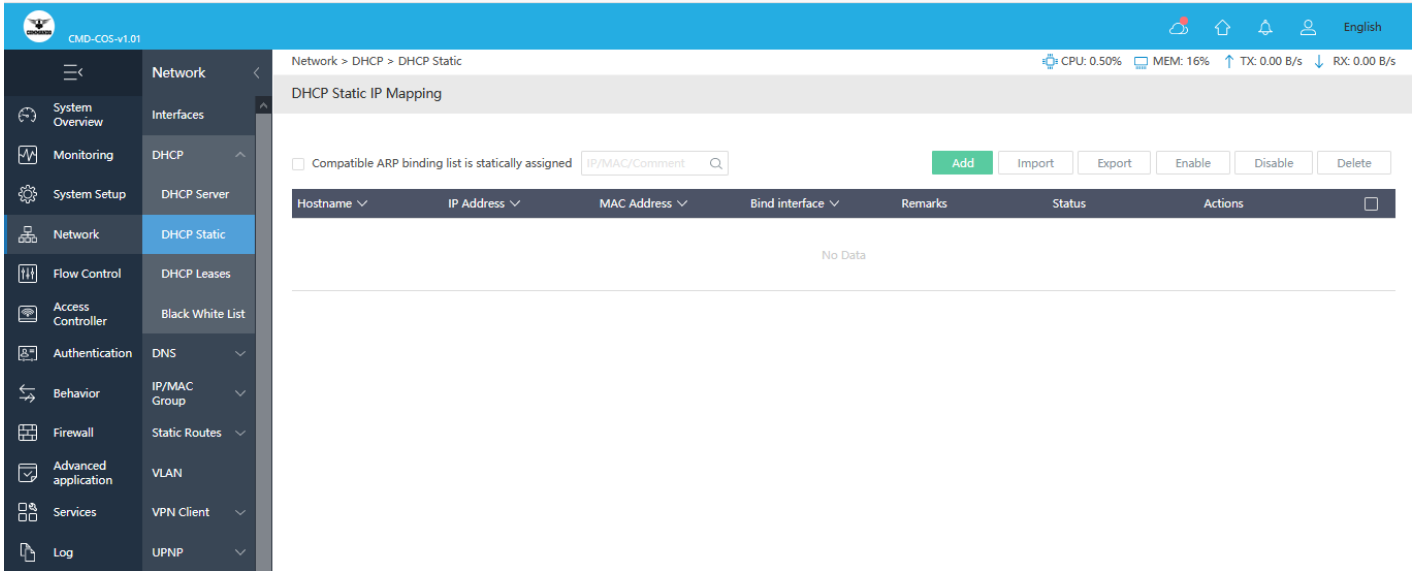


**Fig 3.2.4 DHCP Server Settings of LAN1 interface page**

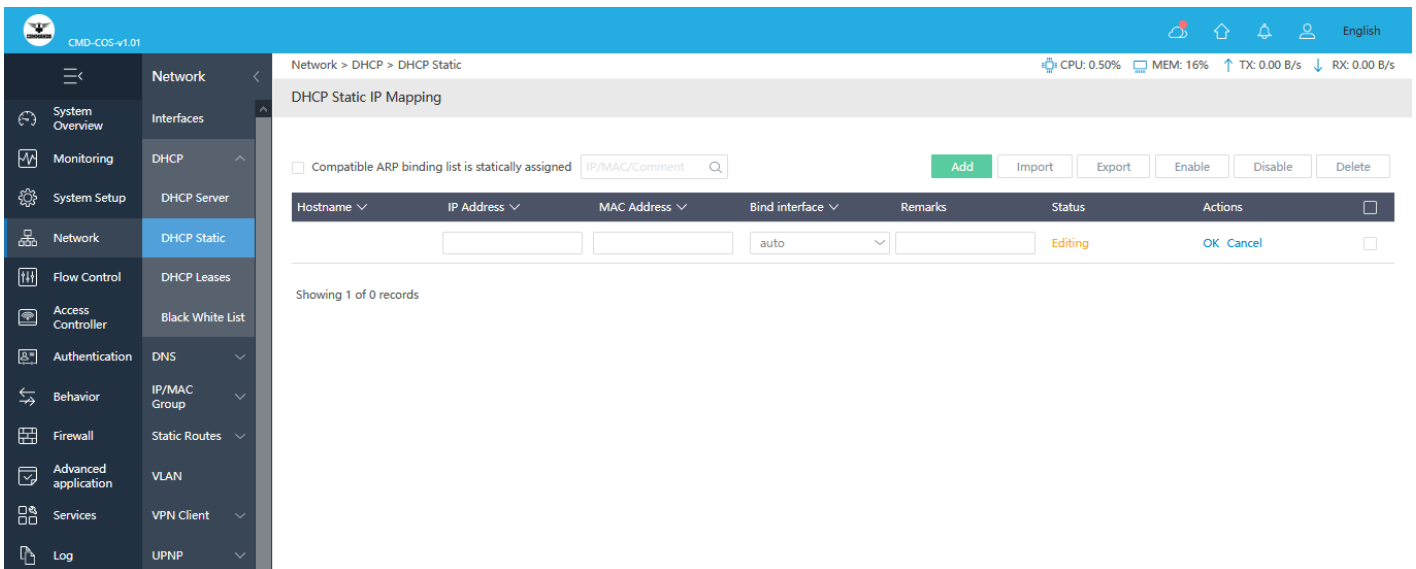
### DHCP static binding:

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.

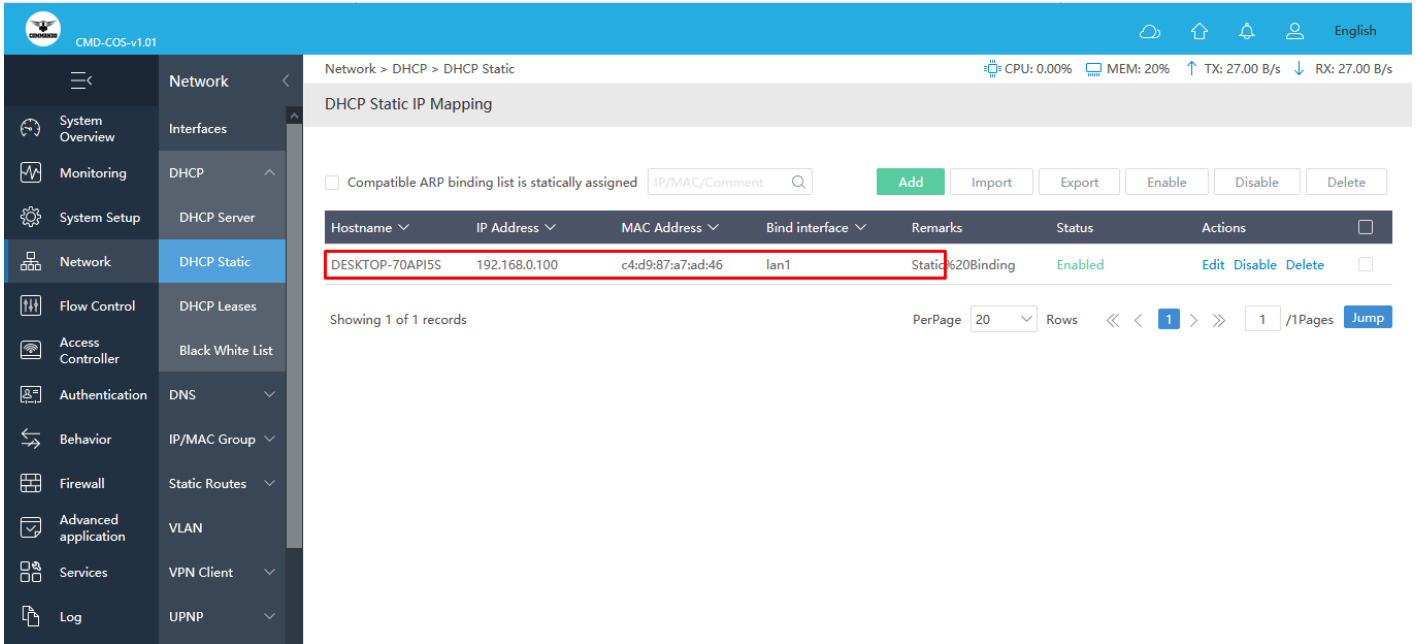
To configure DHCP Static IP Mapping, Click on Network > DHCP > DHCP Static.



**Fig 3.2.5 Default DHCP Static IP Mapping page**



**Fig 3.2.6 Default DHCP Static IP Mapping Add page**

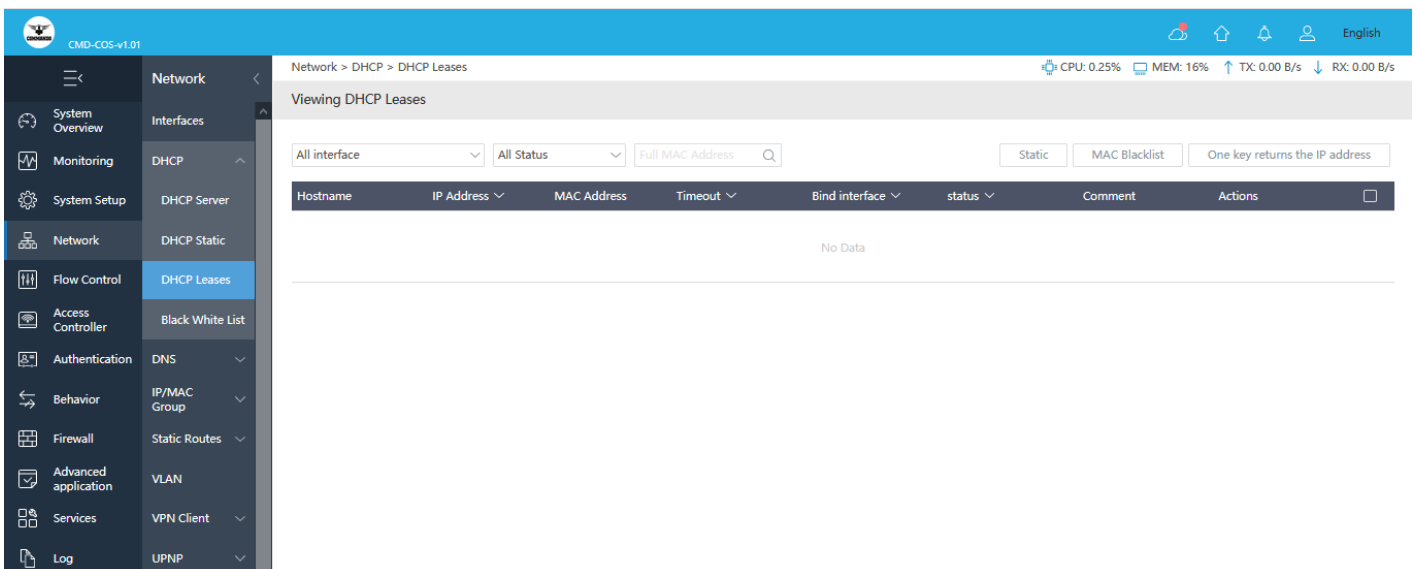


**Fig 3.2.7 DHCP Static IP Mapping Add page**

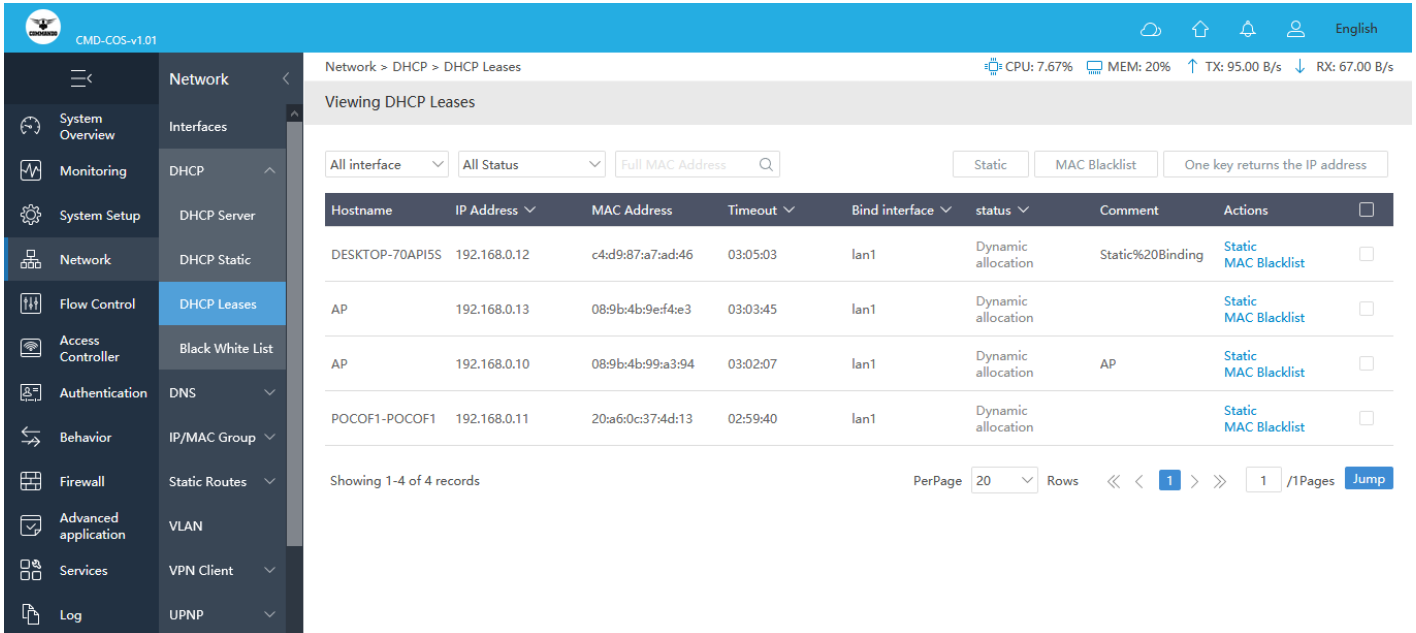
### Viewing DHCP Leases:

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



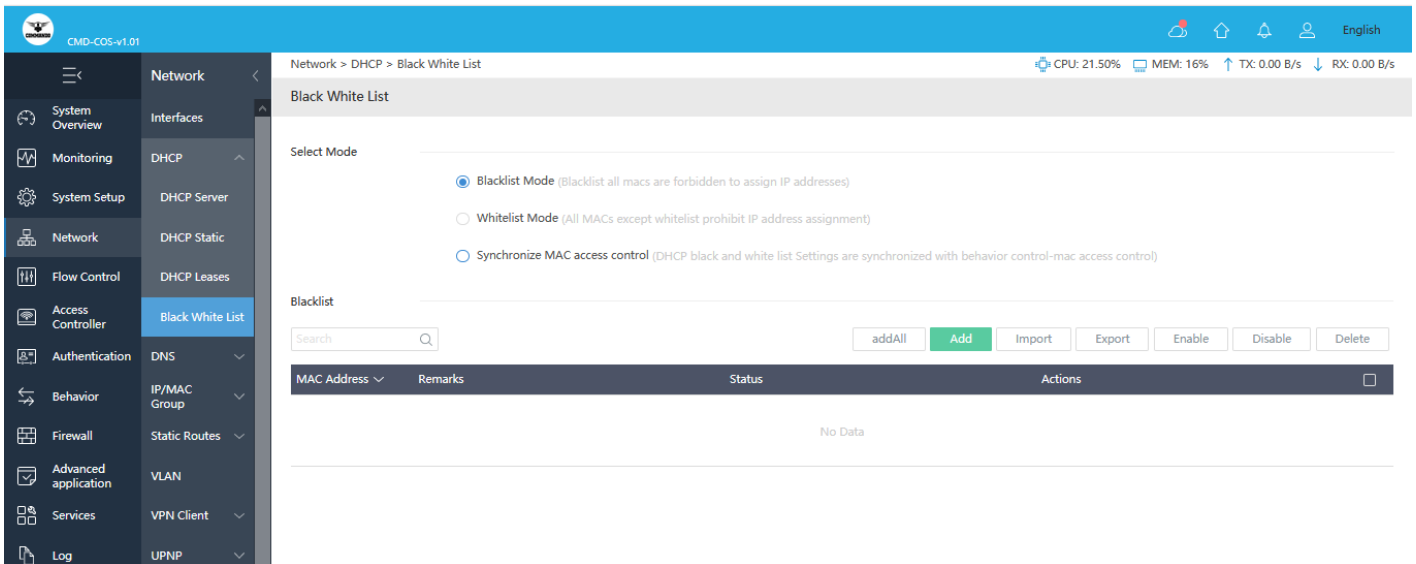
**Fig 3.2.8 Default Viewing DHCP Leases page**



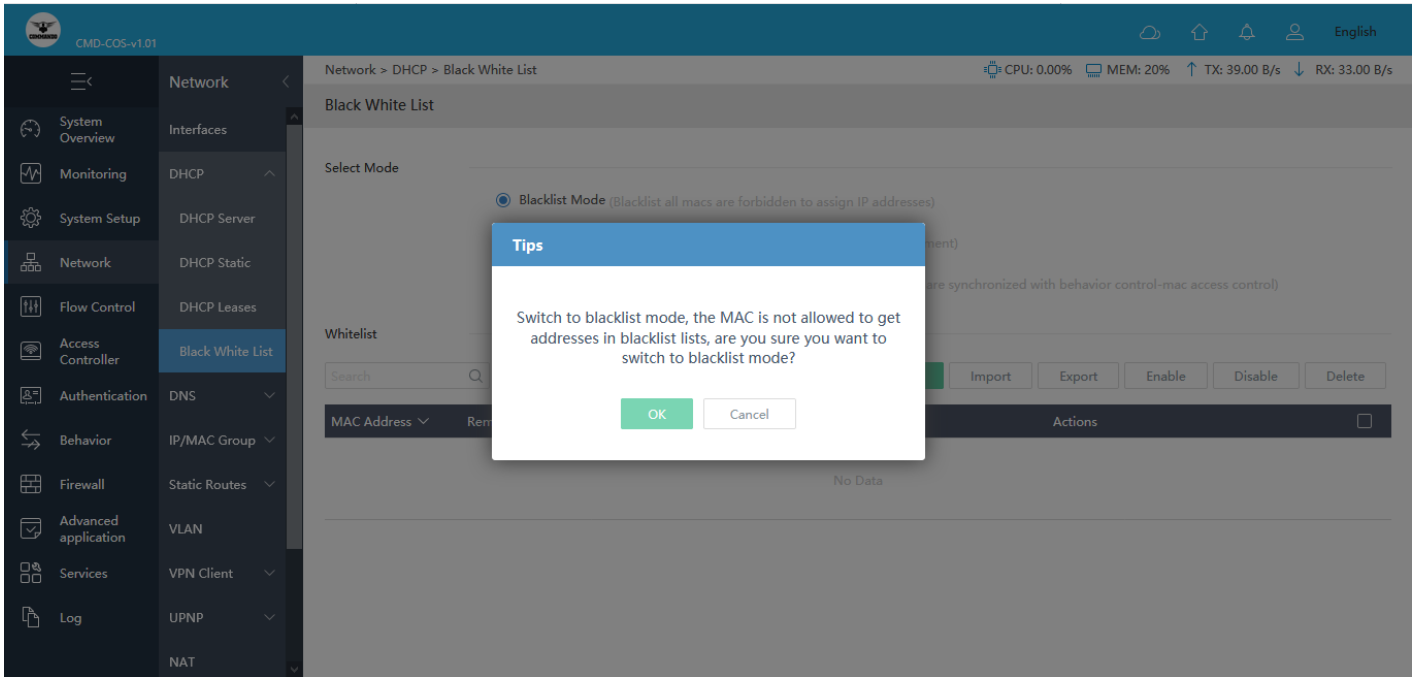
**Fig 3.2.9 Viewing DHCP Leases page**

**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).

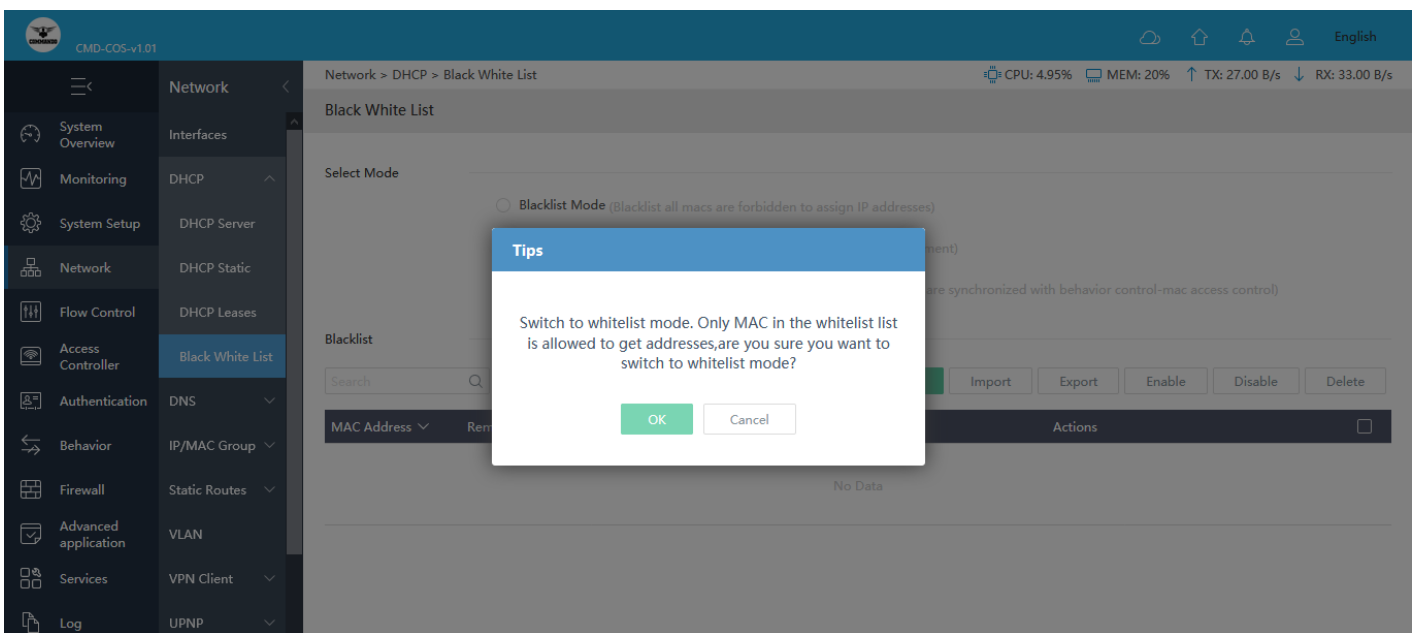
For Black White List users in network, Click on Network > DHCP > Black White List



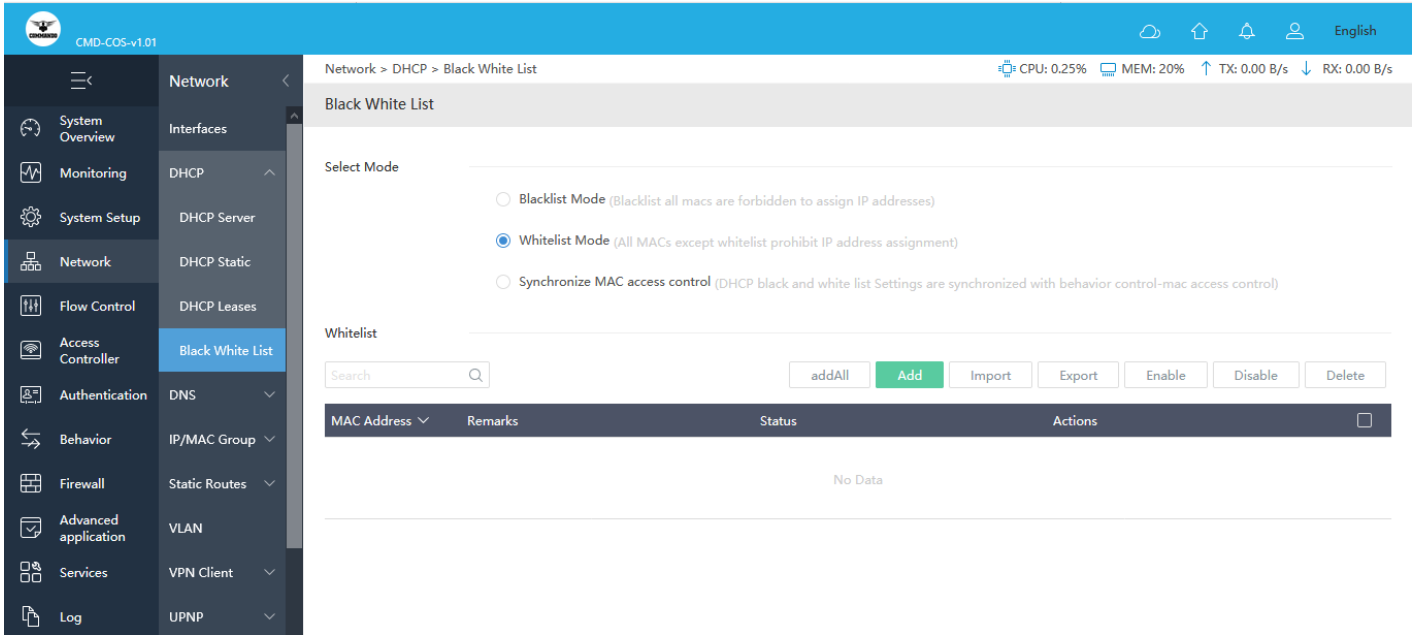
**Fig 3.2.10 Default Blacklist Mode setting in device page**



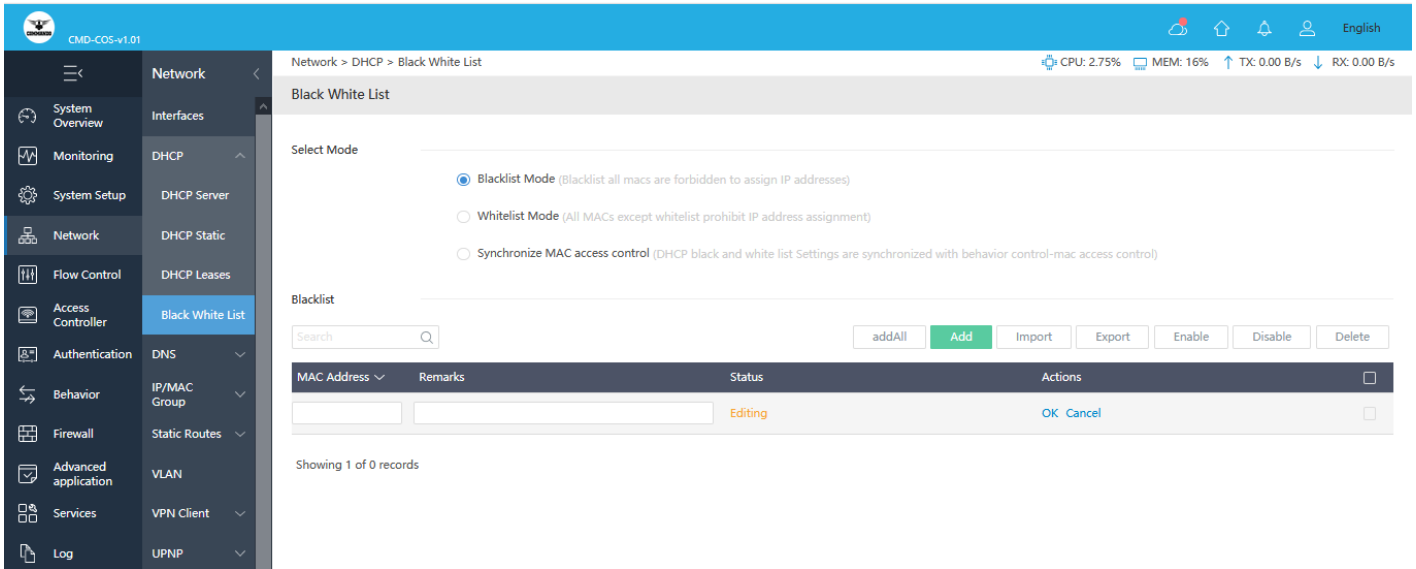
**Fig 3.2.11 Blacklist Mode setting in device page**



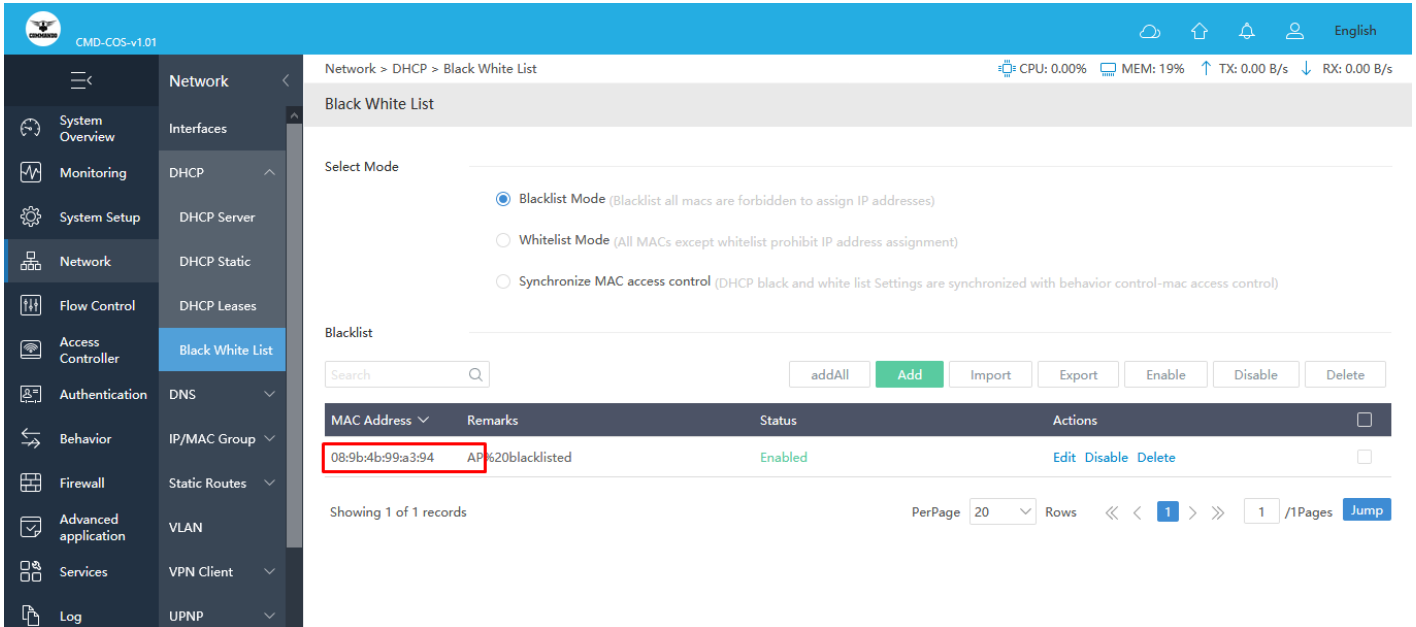
**Fig 3.2.12 Changing mode to Whitelist Mode setting in device page**



**Fig 3.2.13 White list Mode setting in device page**



**Fig 3.2.14 Blacklist mode add page**



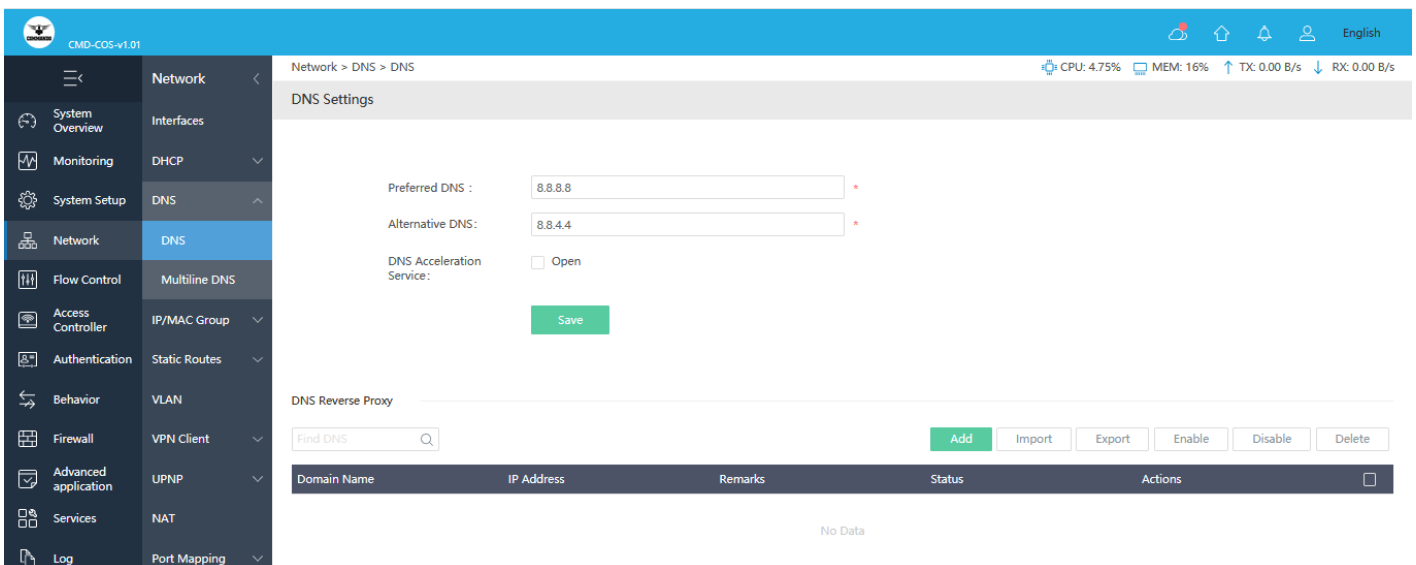
**Fig 3.2.14 Blacklist mode MAC address page**

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

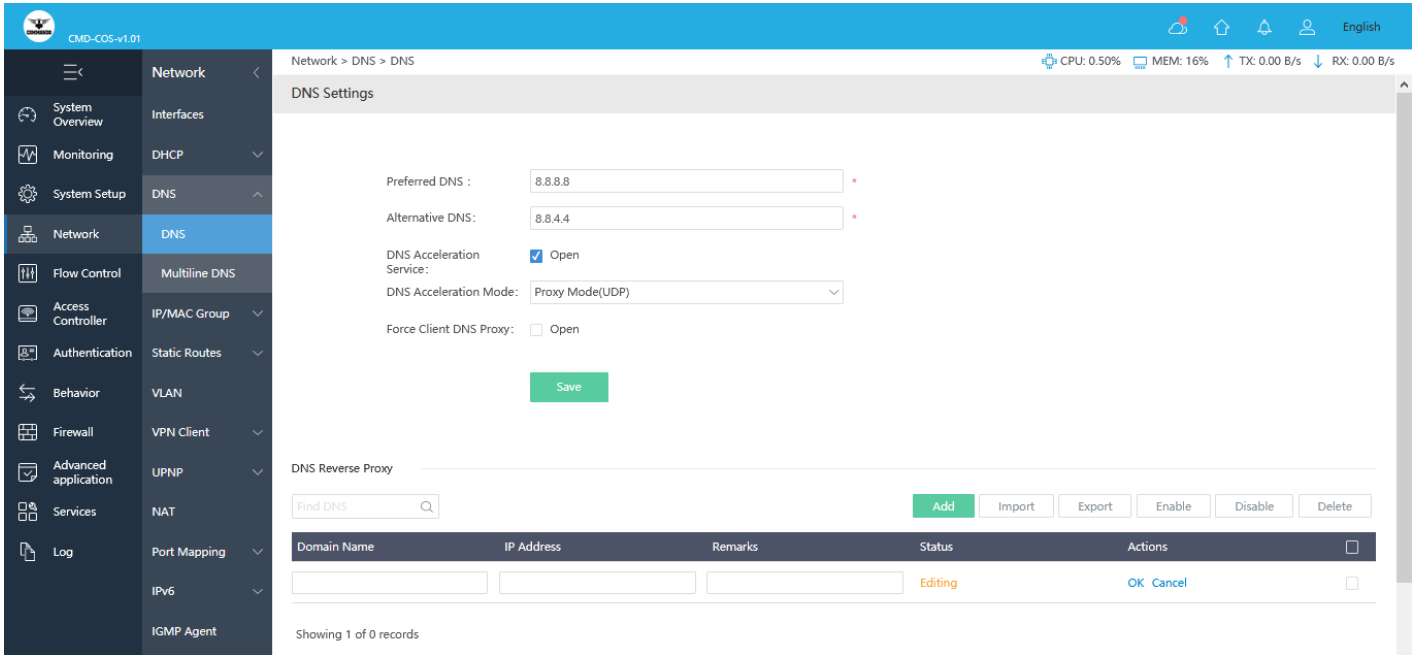
### 3. DNS

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**

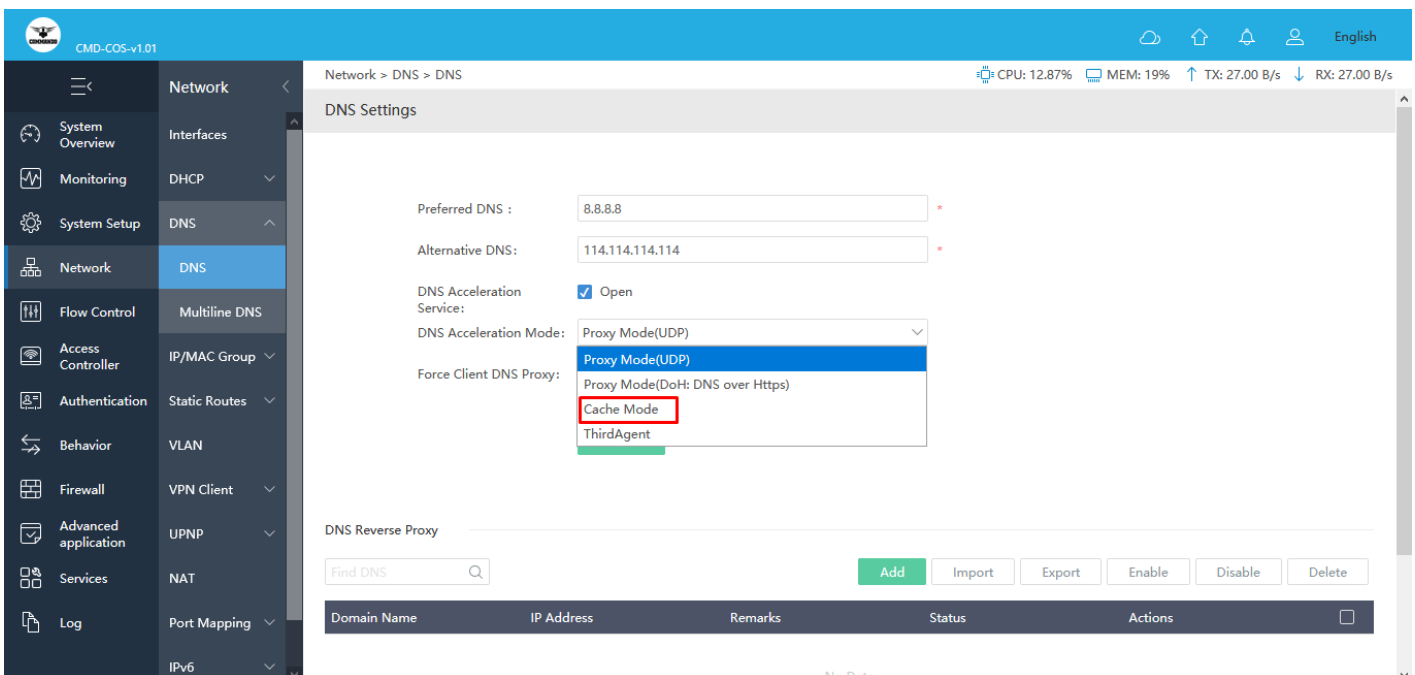


**Fig 3.3.2 Default DNS Settings after opening page**

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.

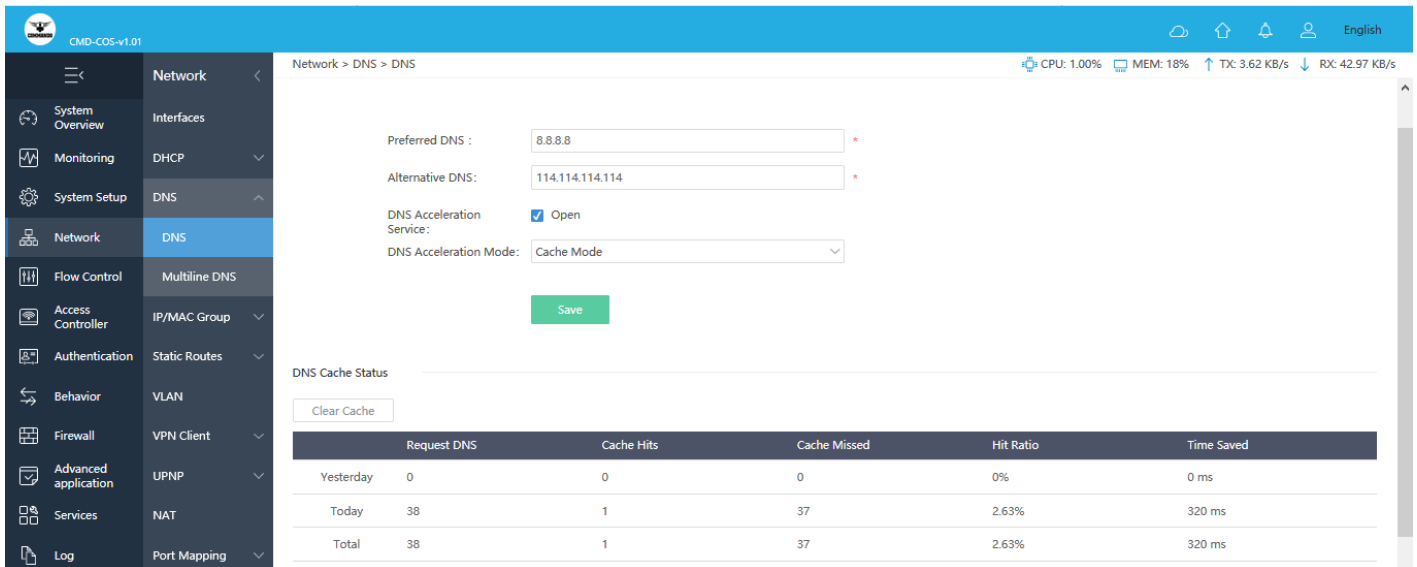
### How to change the DNS Acceleration Mode?

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



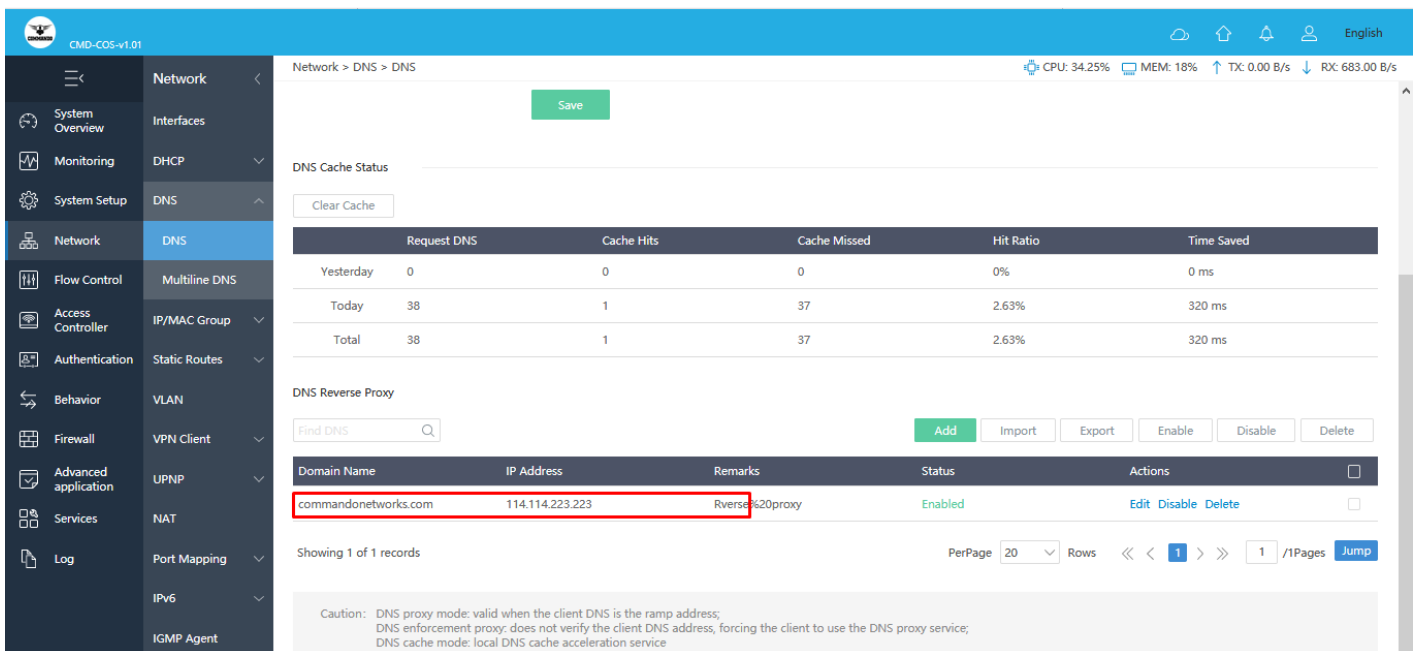


**Fig 3.3.3 Changing DNS acceleration mode to cache page**



**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.



**Fig 3.3.5 DNS Reverse Proxy page**

**Multiline DNS Settings:**

When multiple WAN connected to your router 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

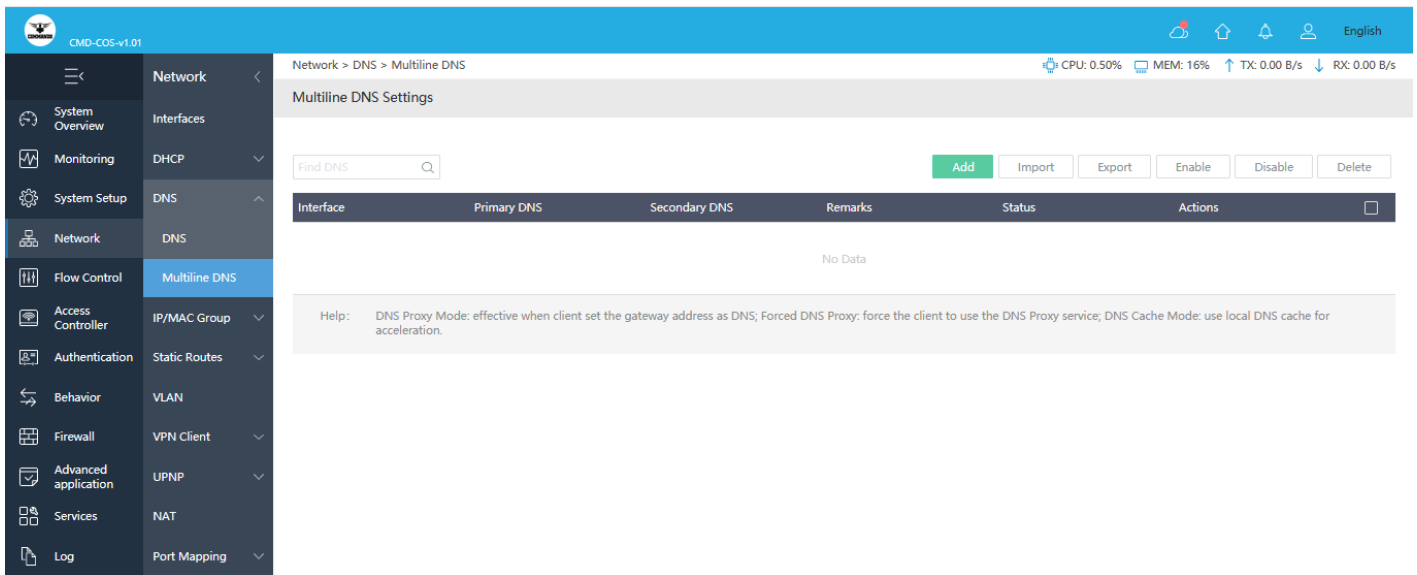


Fig 3.3.6 Default Multiline DNS Settings page

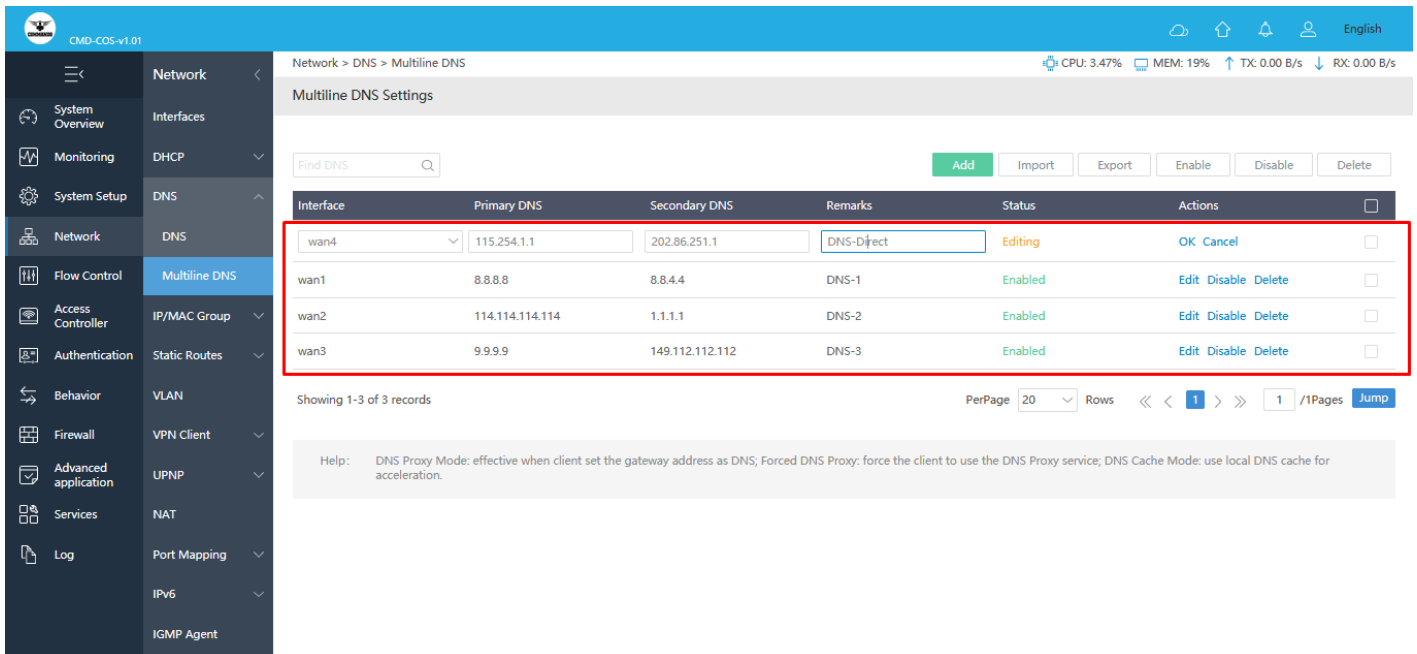
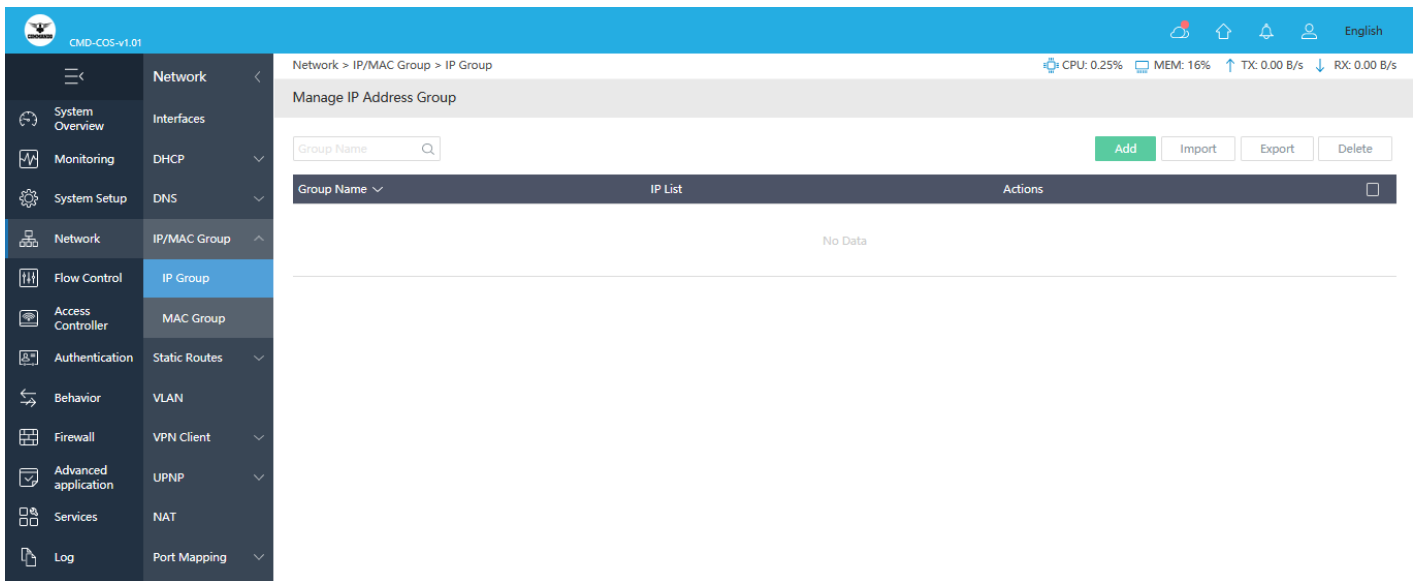


Fig 3.3.7 Multiline DNS Settings page

#### 4. IP/MAC Group

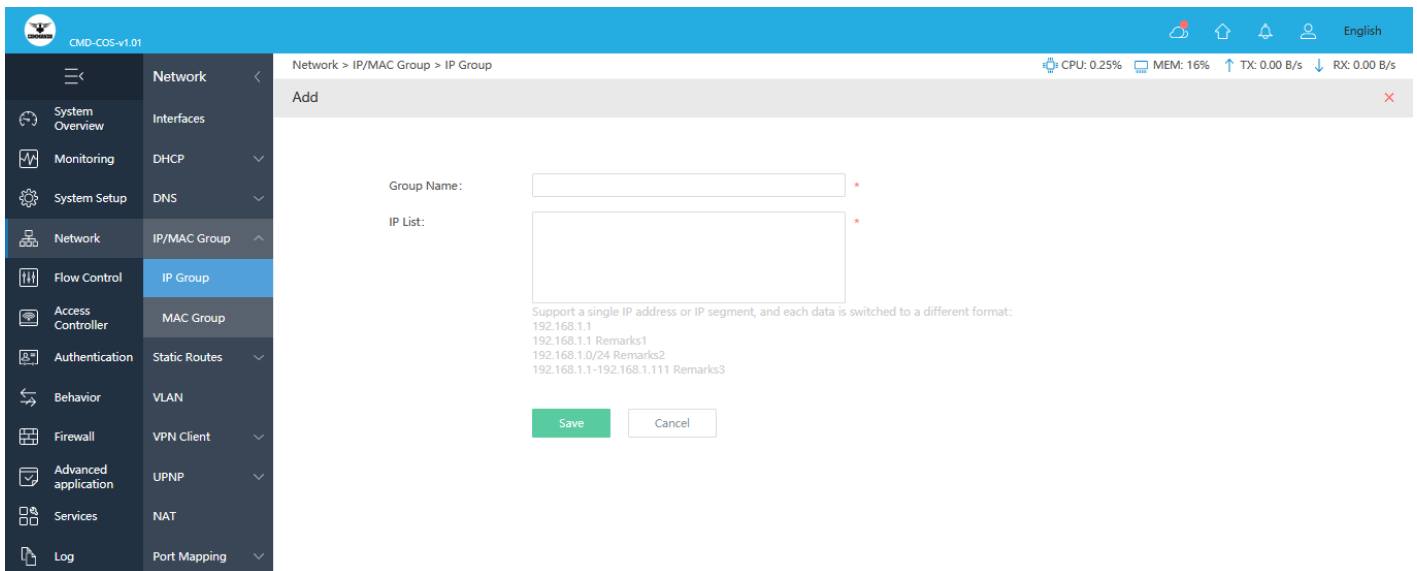
A single IP address divides into two sections: Network ID and Host ID. The Network ID defines the logical group where devices belong. Similarly, we can define IP group which tells routers what groups the users are defined.

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

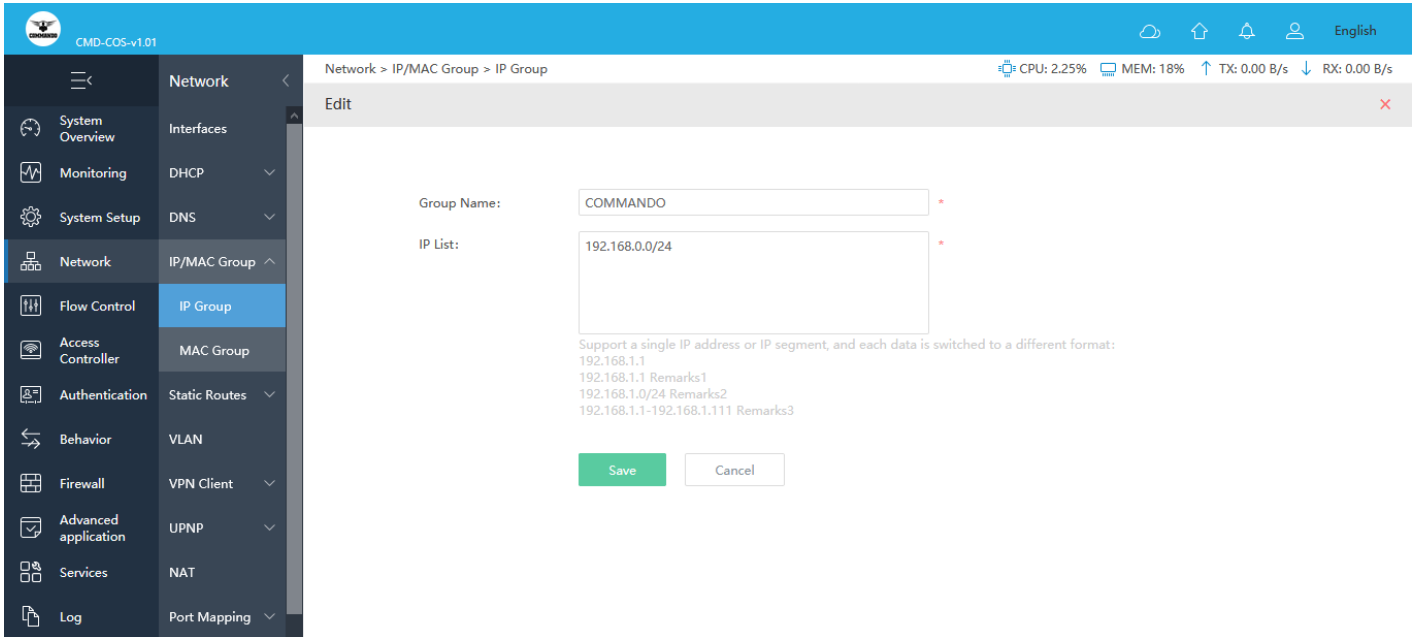


**Fig 3.4.1 Manage IP Address Group page**

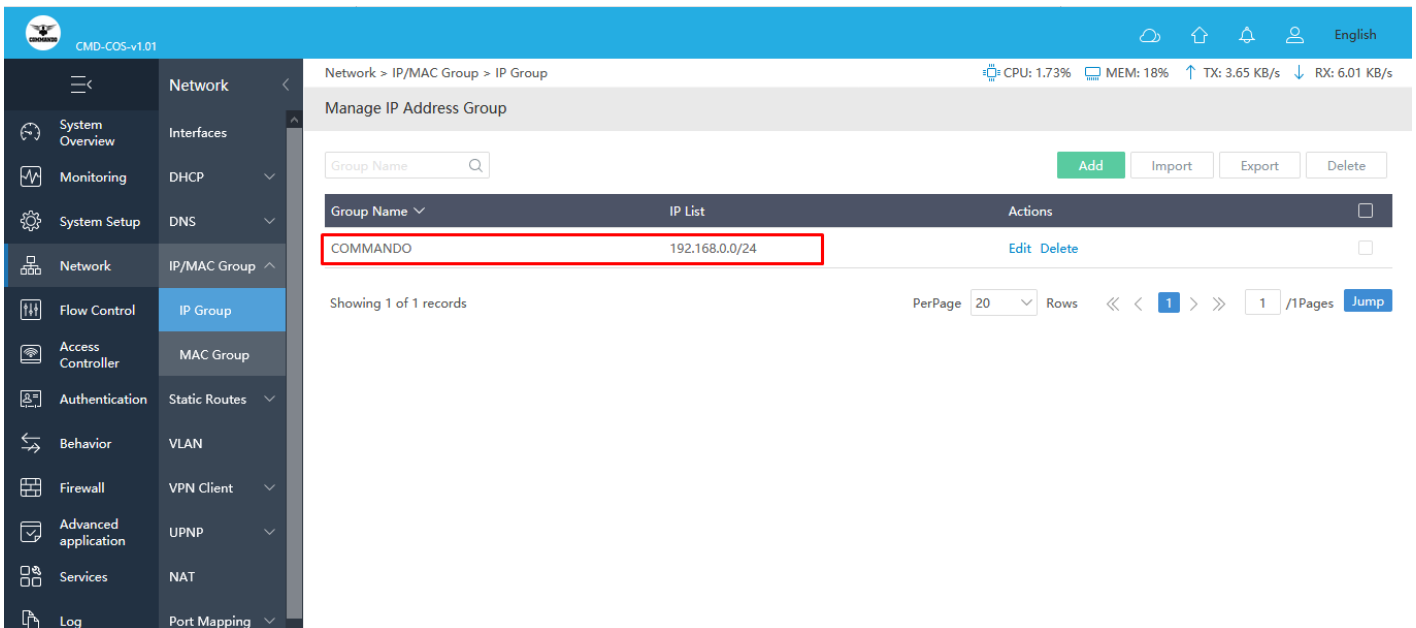
You can add Group Name and IP List. It supports a single IP address or IP segment, and each data is switched to a different format as follows. 192.168.1.1, 192.168.1.1 Remarks1, 192.168.1.0/24 Remarks2, 192.168.1.1-192.168.1.111 Remarks3.



**Fig 3.4.2 Default Add IP Address Group page**



**Fig 3.4.3 Edit IP Address Group page**



**Fig 3.4.4 Manage IP 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 routers 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

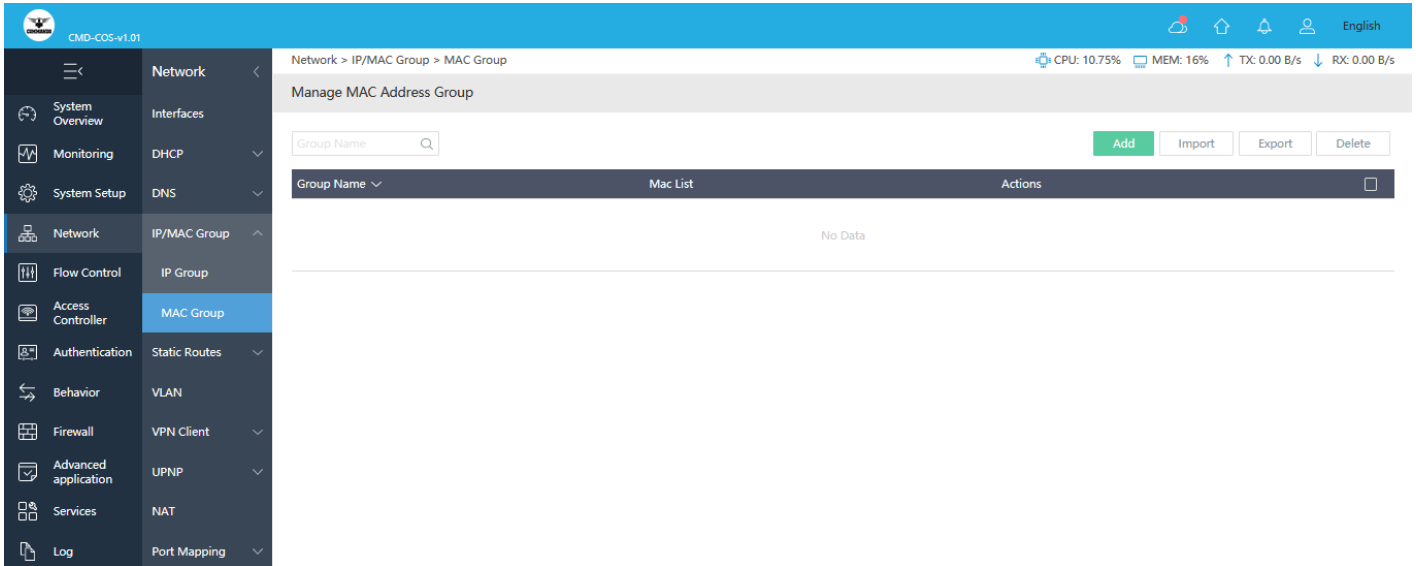


Fig 3.4.5 Default Manage MAC Address Group page

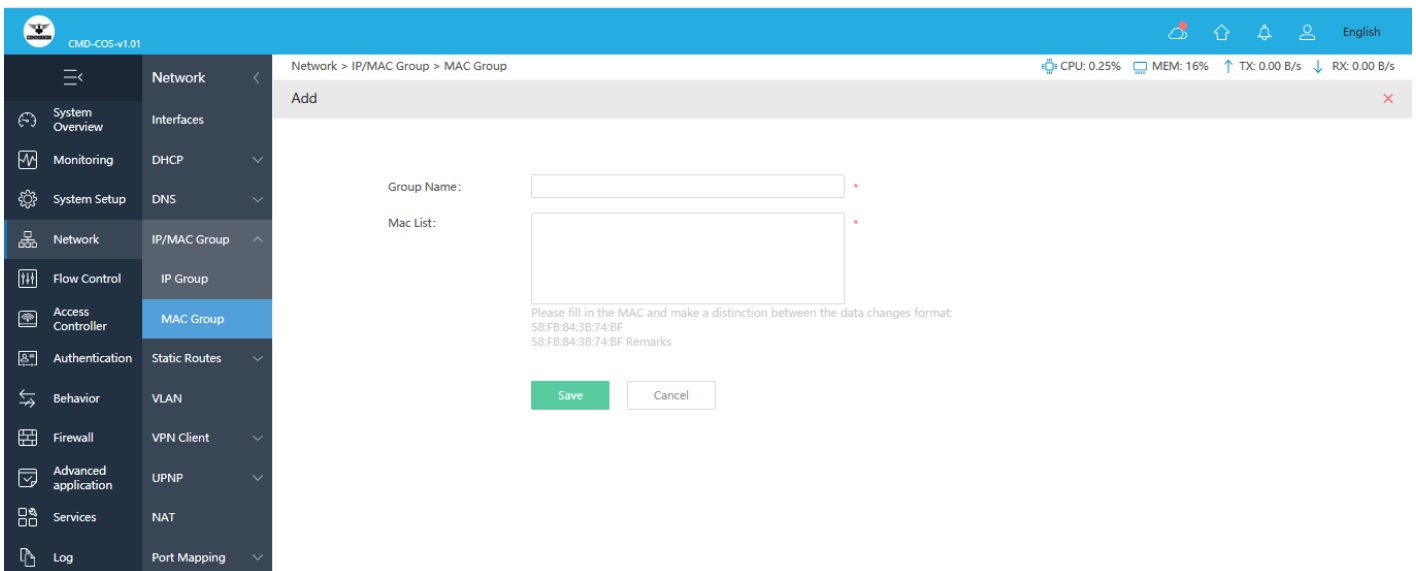
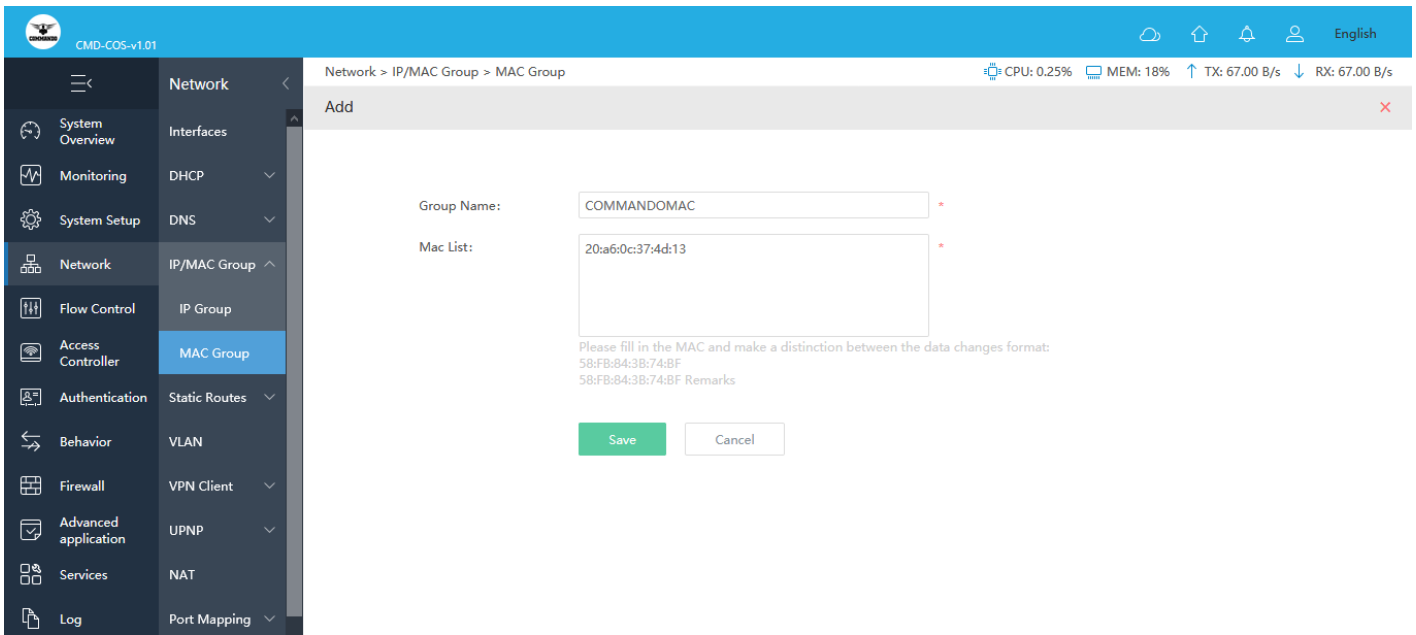
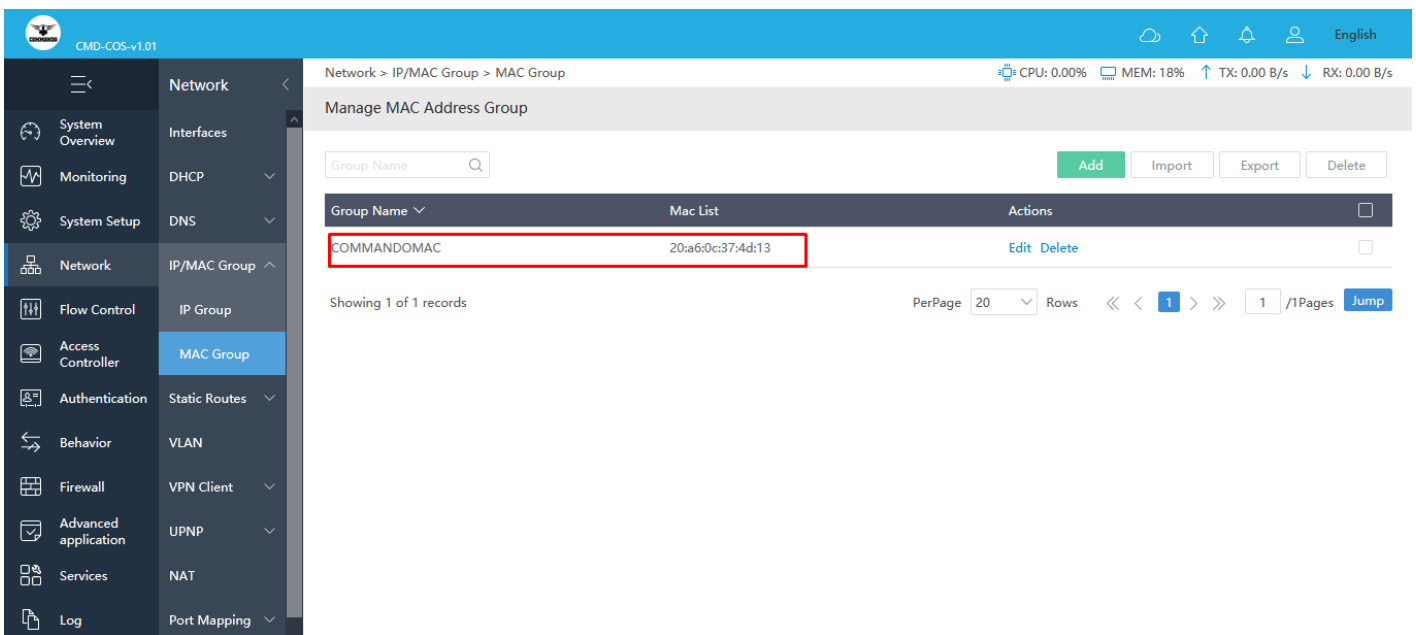


Fig 3.4.6 Add MAC Address Group page



**Fig 3.4.6 Adding specific MAC page**



**Fig 3.4.7 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 mainly 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 router 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 router learned from connected interfaces. The router 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.

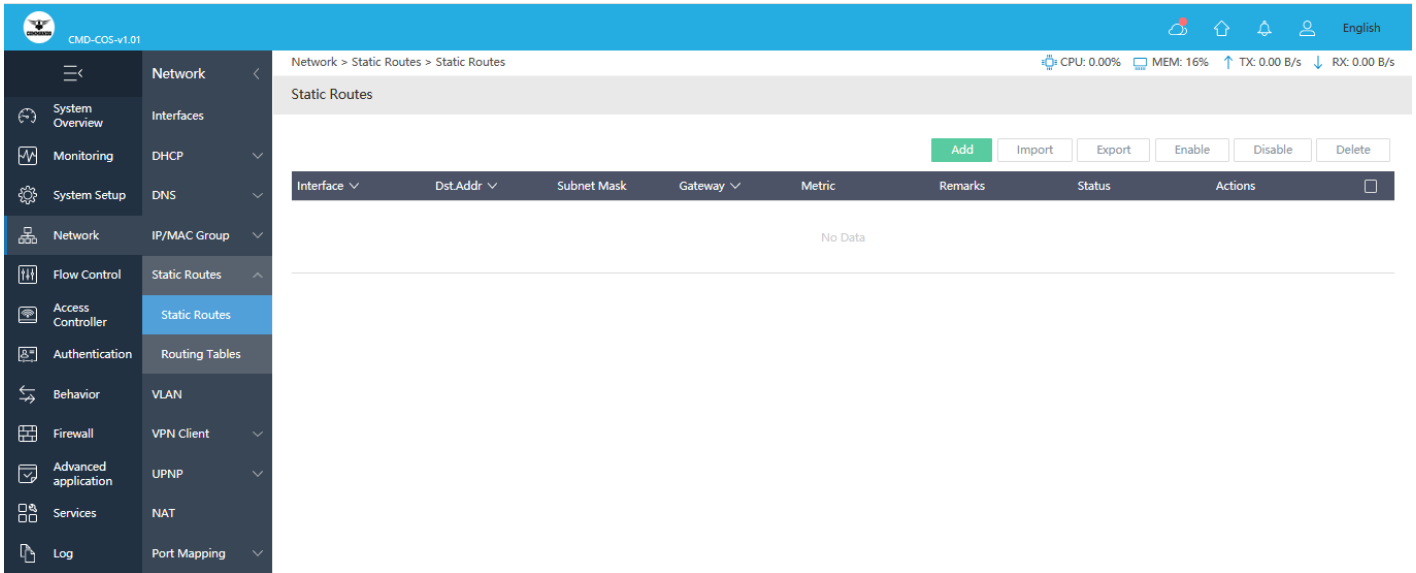


Fig 3.5.1 Default static route page

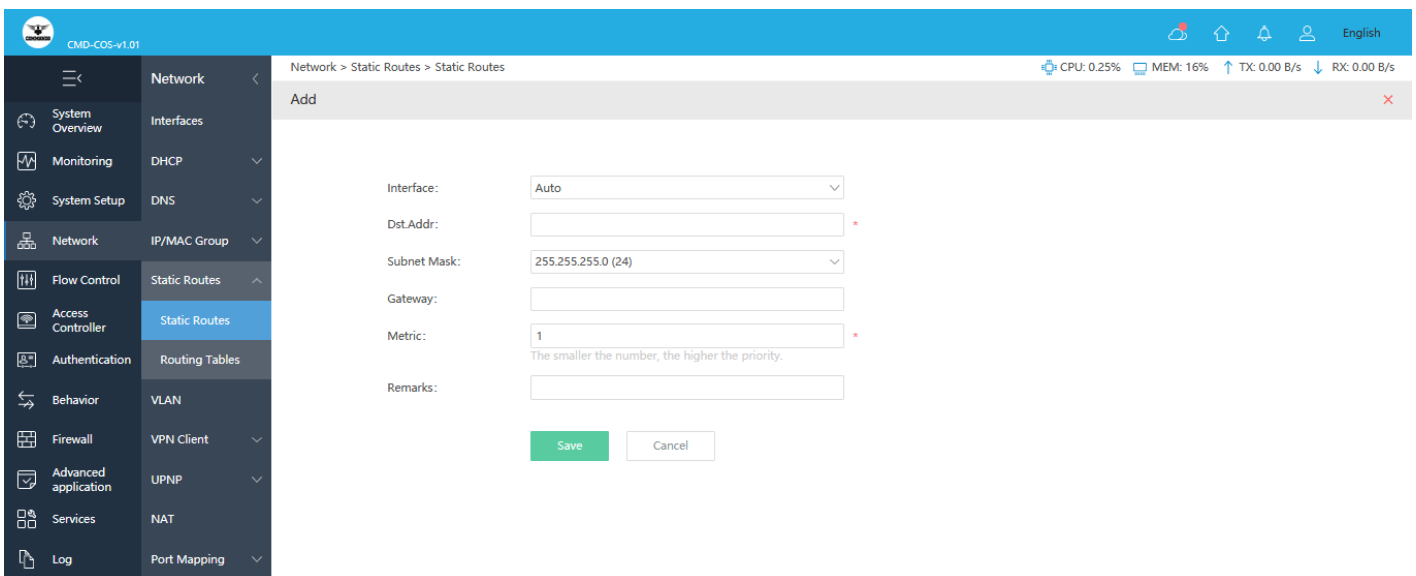
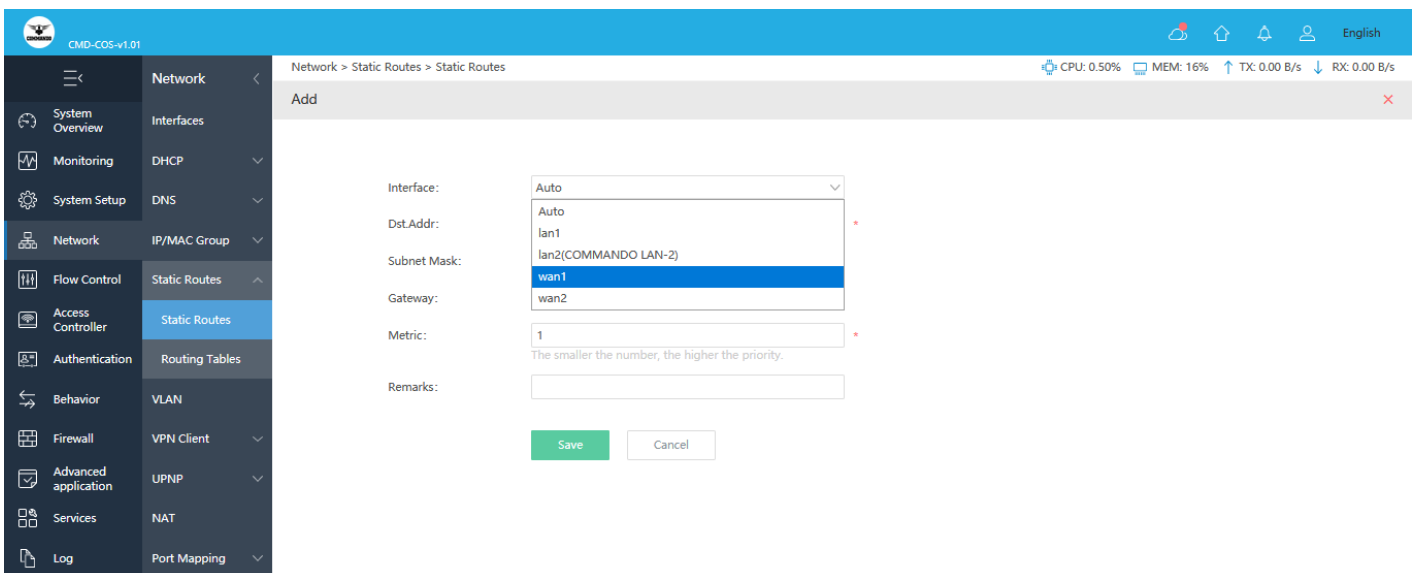
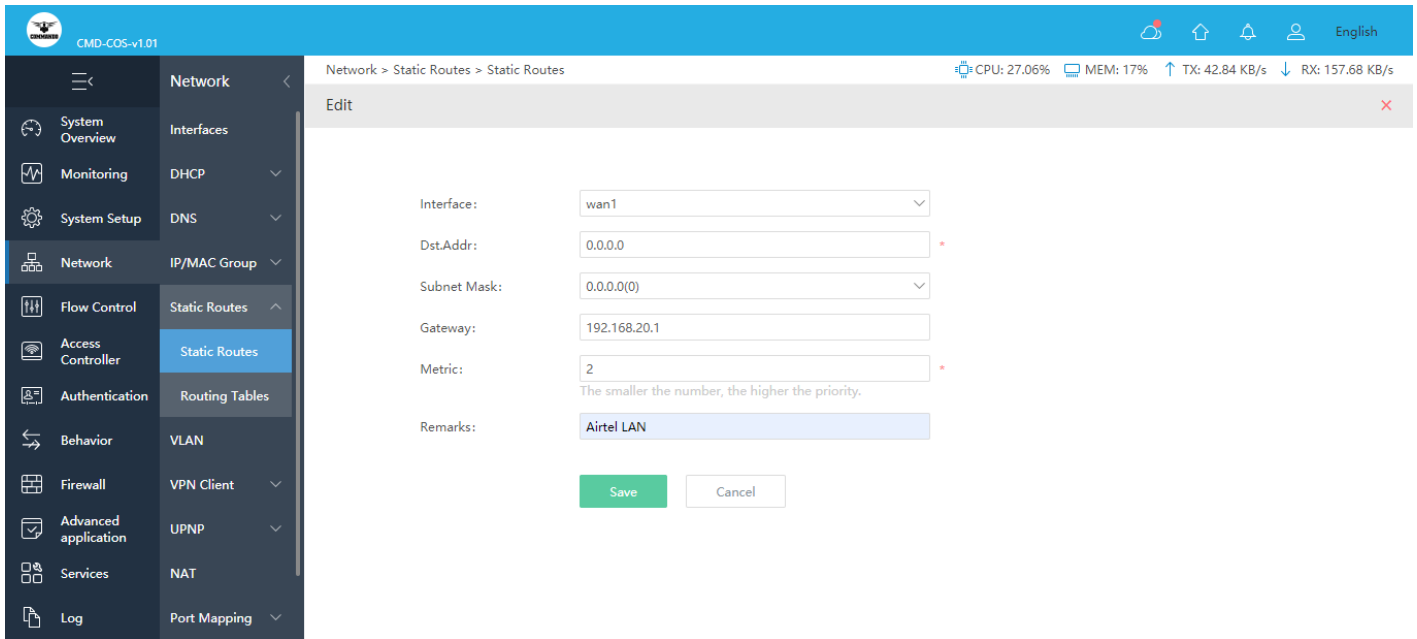


Fig 3.5.2 Default Add static route page





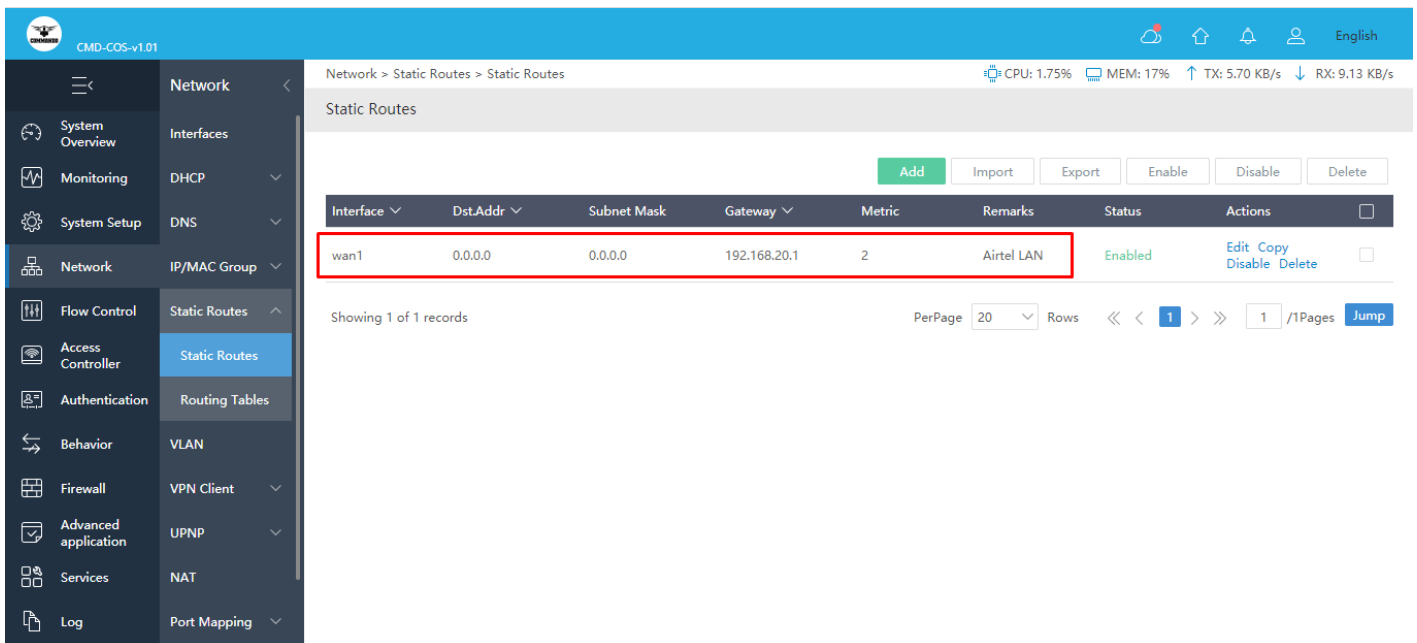
**Fig 3.5.3 Selecting interface in static route page**



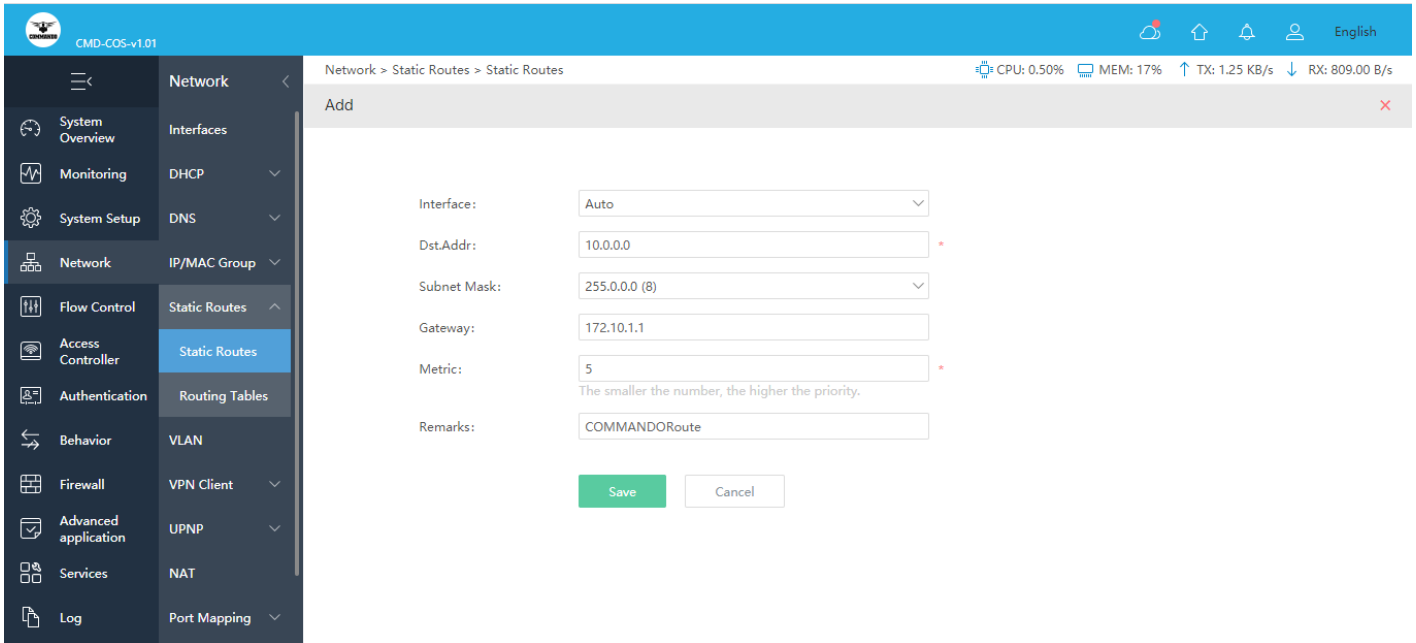
**Fig 3.5.4 Adding Default route (Gateway of last resort) page**

**Note:**

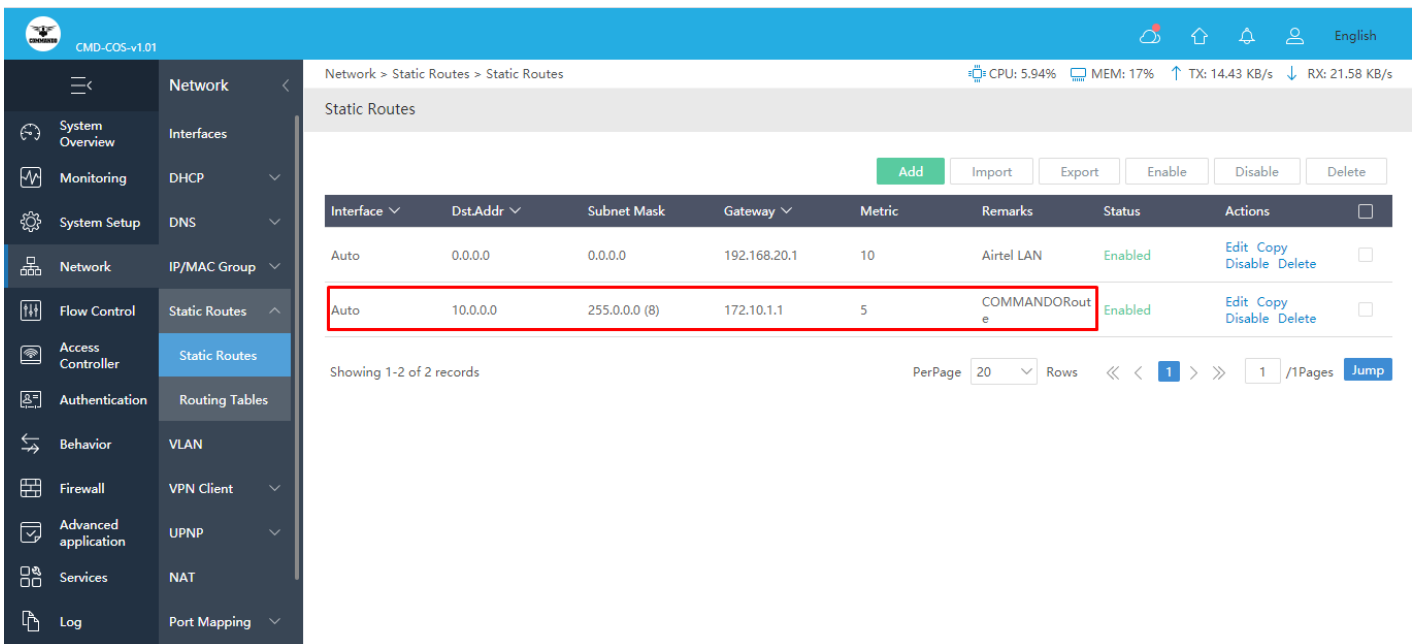
You can add multiple gateways of last resort by changing administrative distance.



**Fig 3.5.5 Default route page**



**Fig 3.5.6 Adding a Specific Static route page**

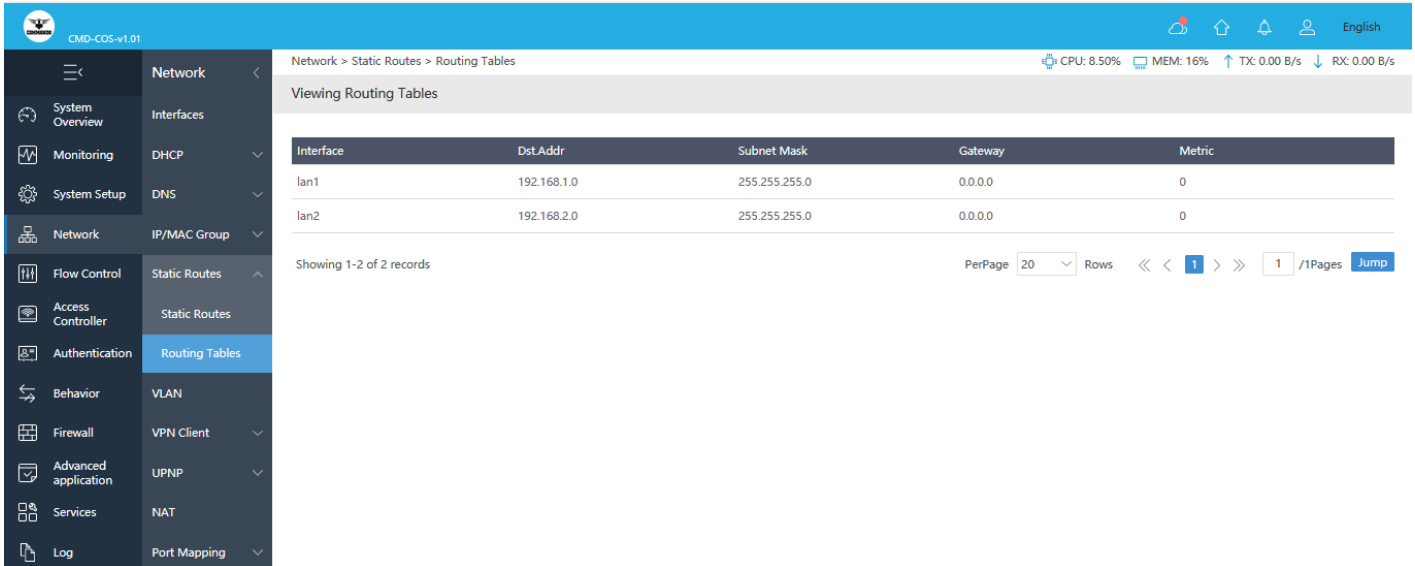


**Fig 3.5.7 Specific Static route page**

### Routing Tables:

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

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



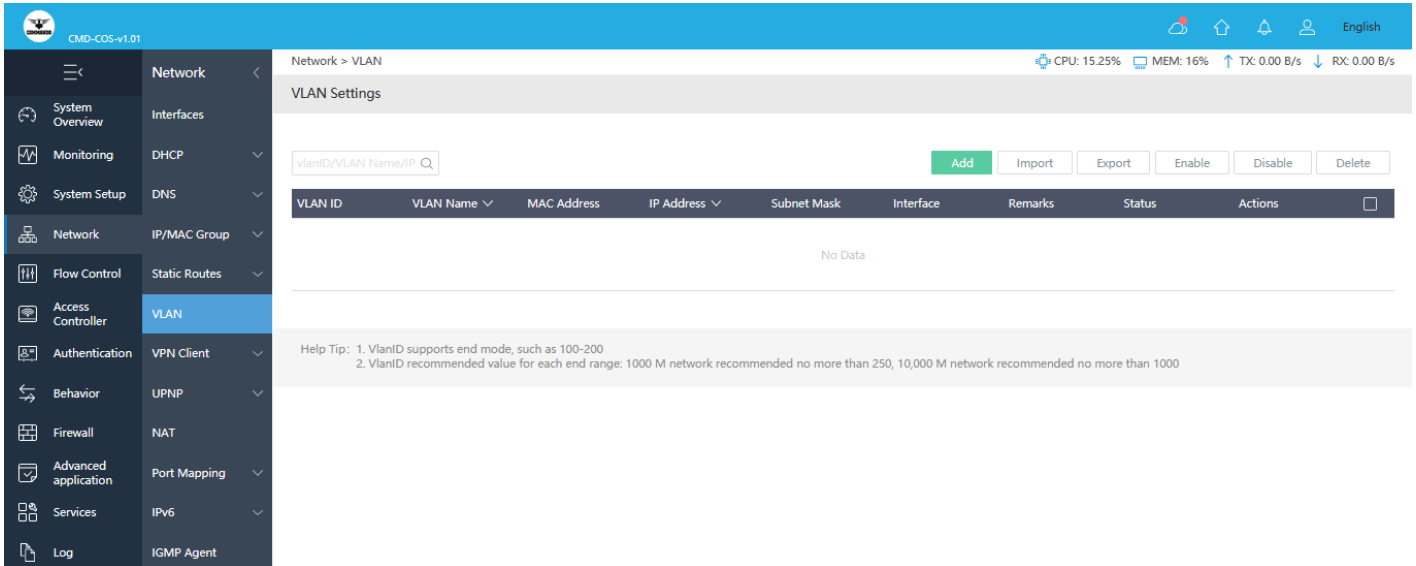
**Fig 3.5.8 Routing Tables page**

## 6. VLAN

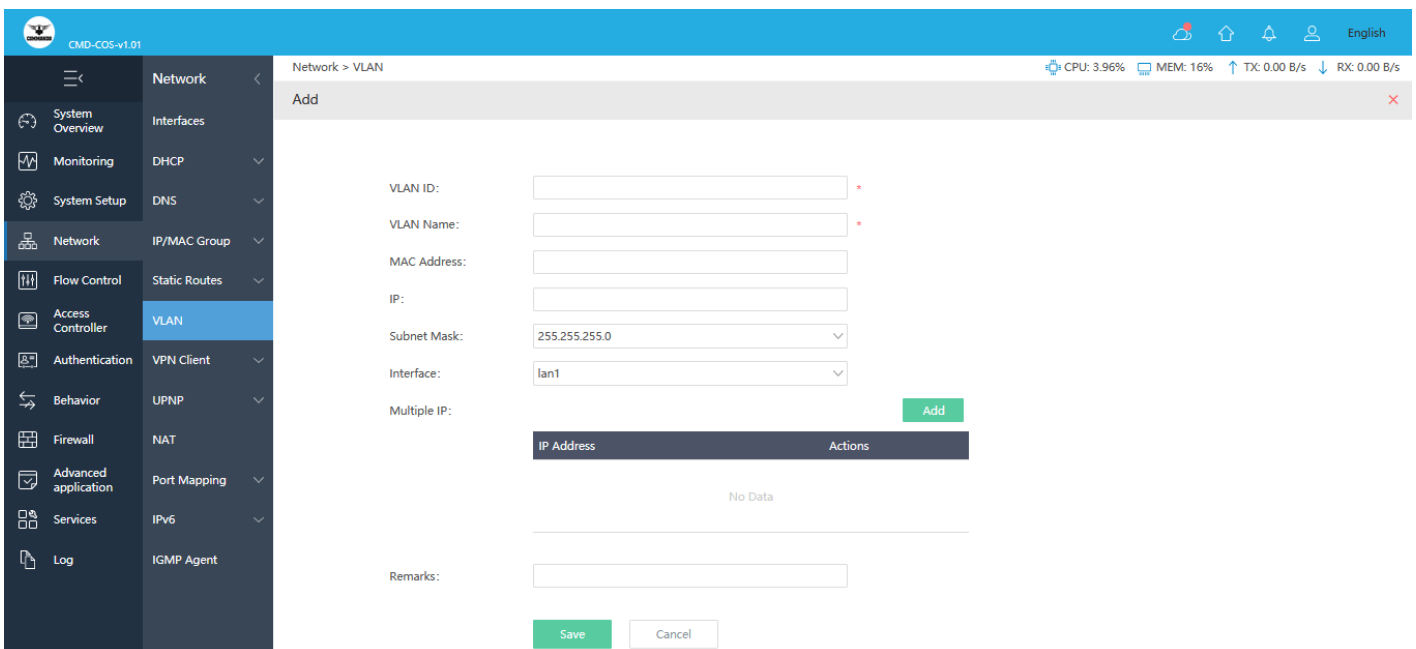
A VLAN (Virtual Local Area Network) allows you to divide the physical LAN into multiple logical LANs so as to control the communication among the ports. The VLAN function can prevent the broadcast storm in LANs and enhance the network security. By creating VLANs, you can divide the LAN into multiple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

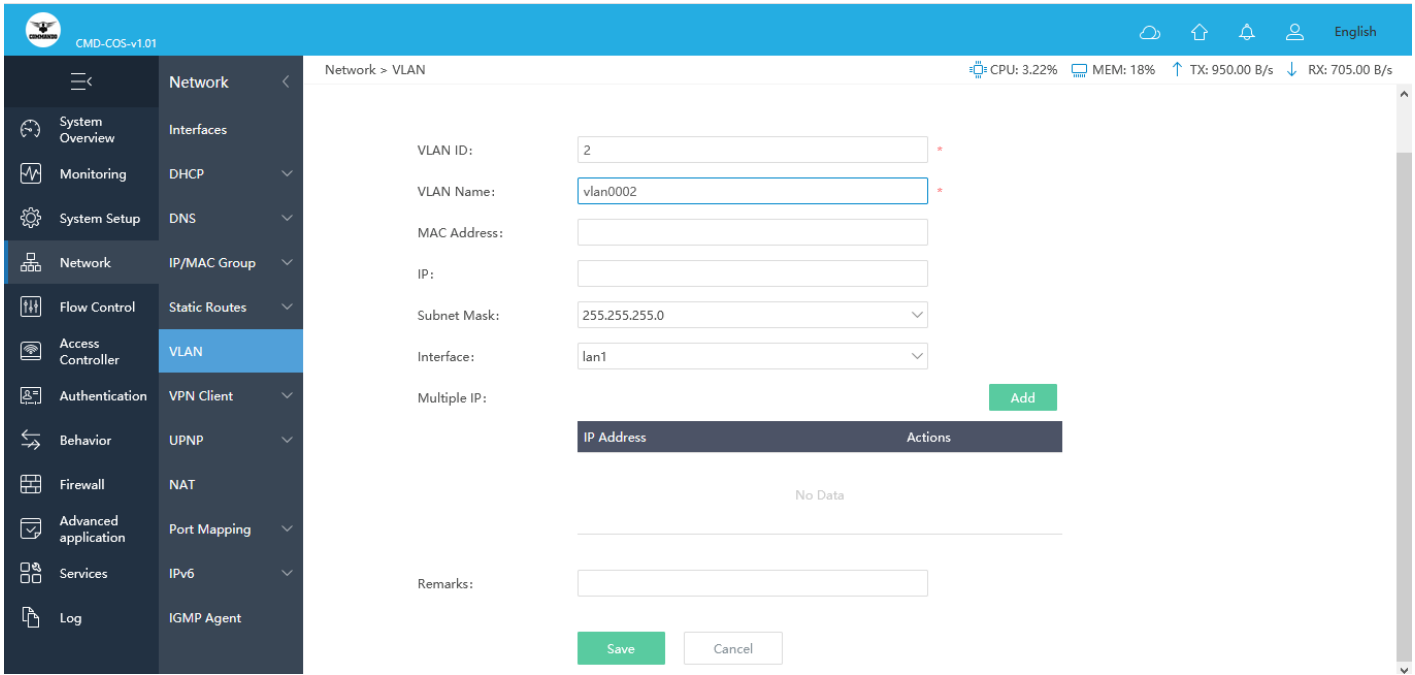
To access VLAN Settings page, Click on Network > VLAN



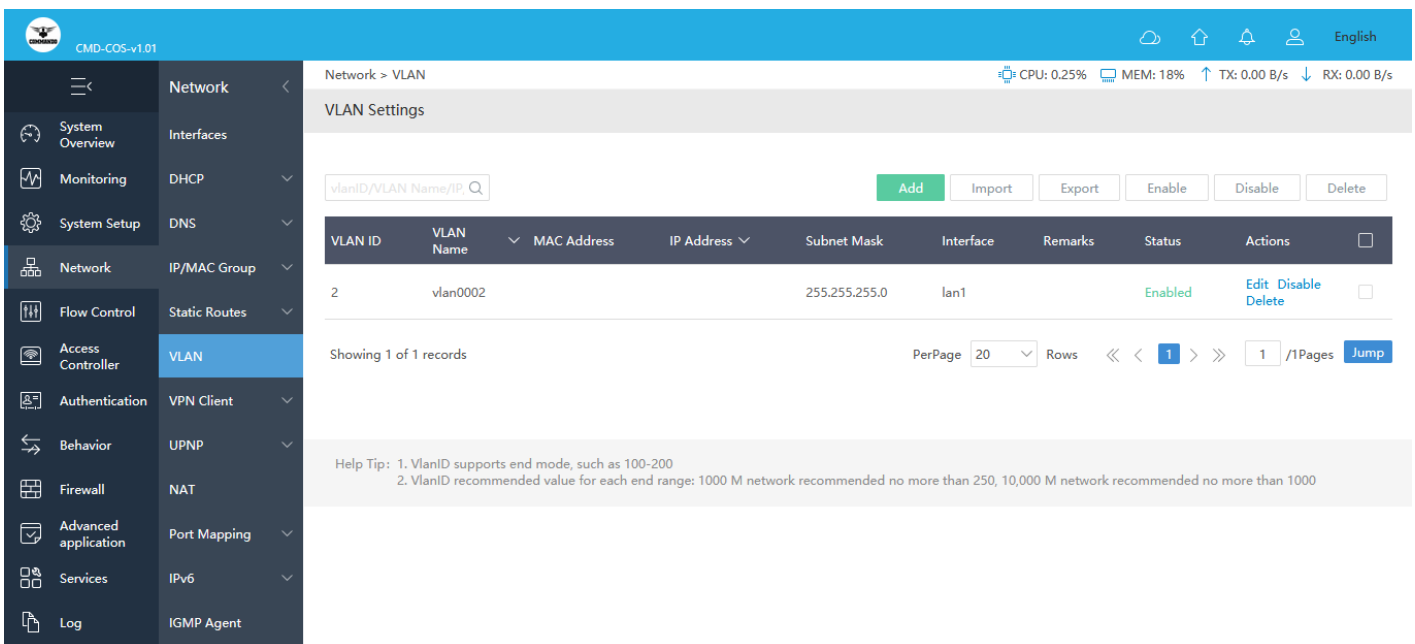
**Fig 3.6.1 Default VLAN Setting page**



**Fig 3.6.2 Add VLAN Setting page**



**Fig 3.6.3 Add VLAN2 Setting on lan1 interface page**

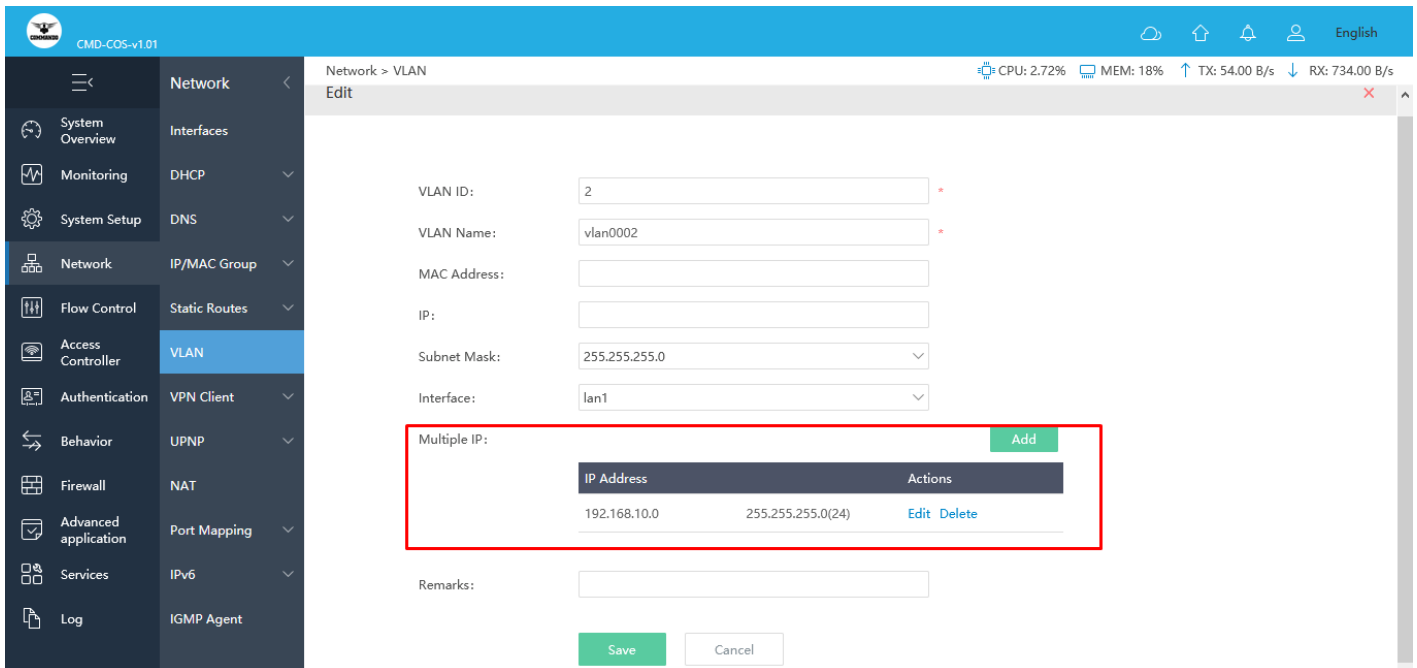


**Fig 3.6.4 VLAN2 Setting on lan1 interface page**

### 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 routers 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, router-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.



**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

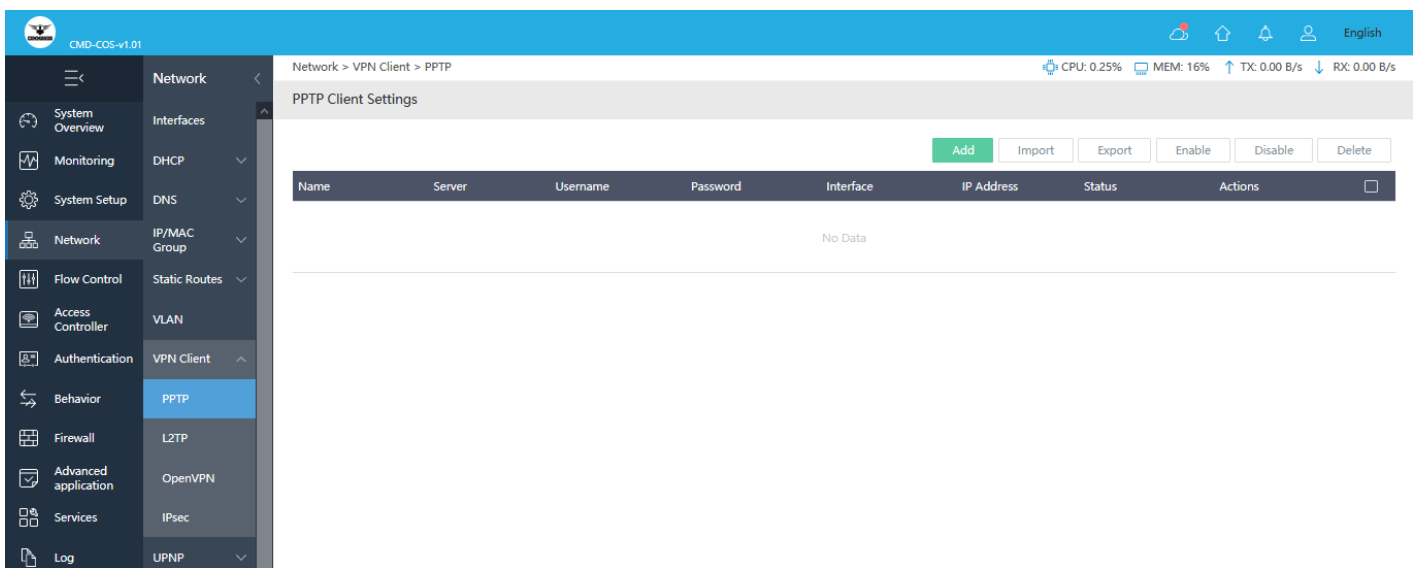
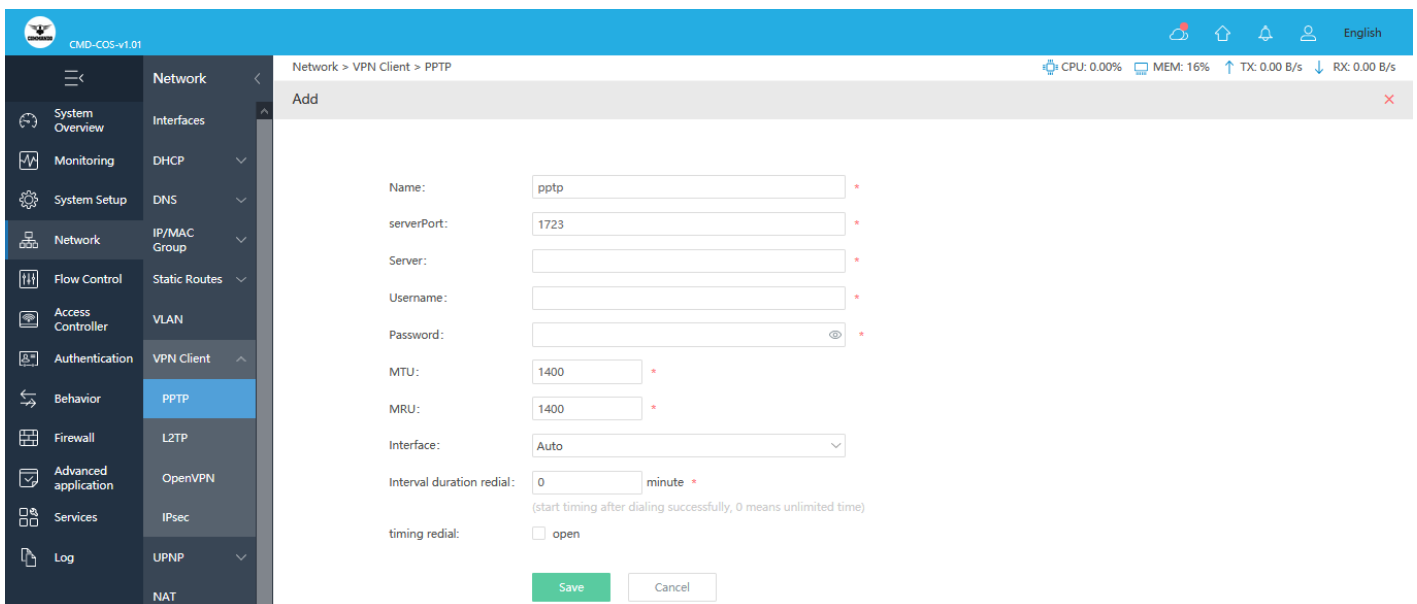
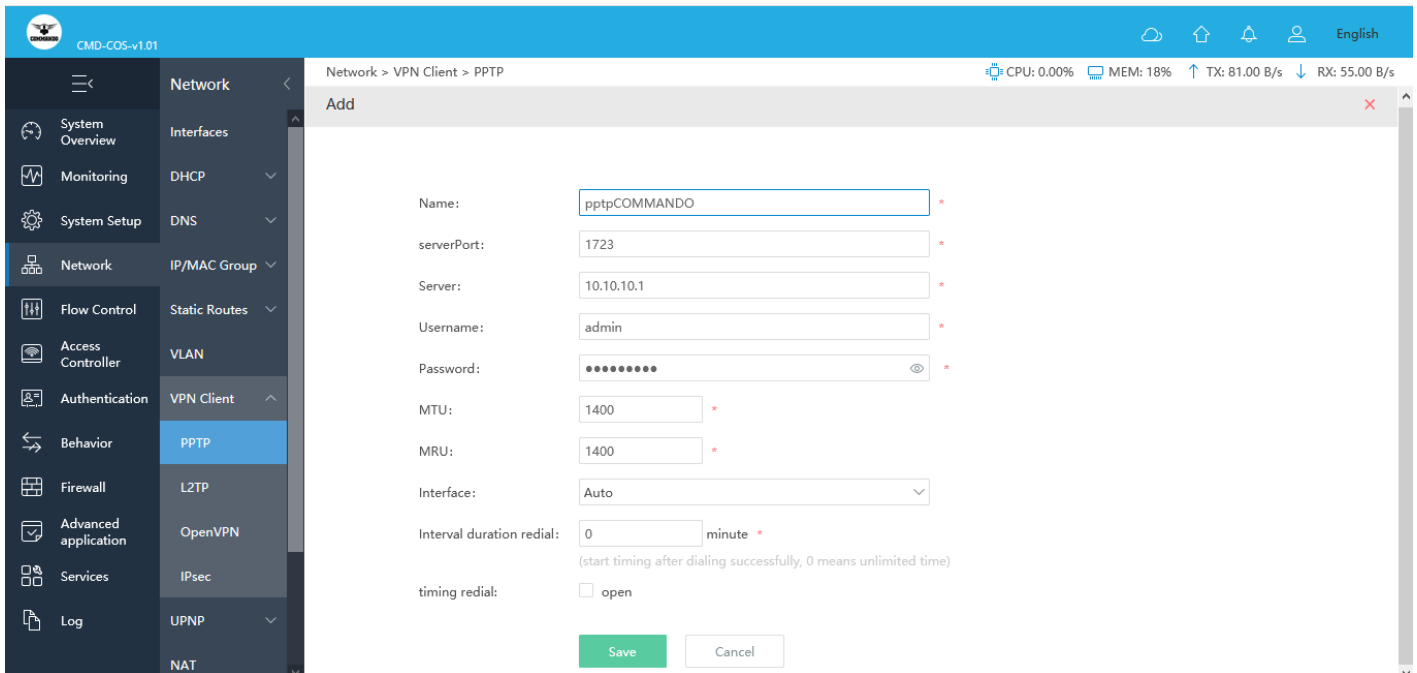


Fig 3.7.1 Default PPTP Setting page



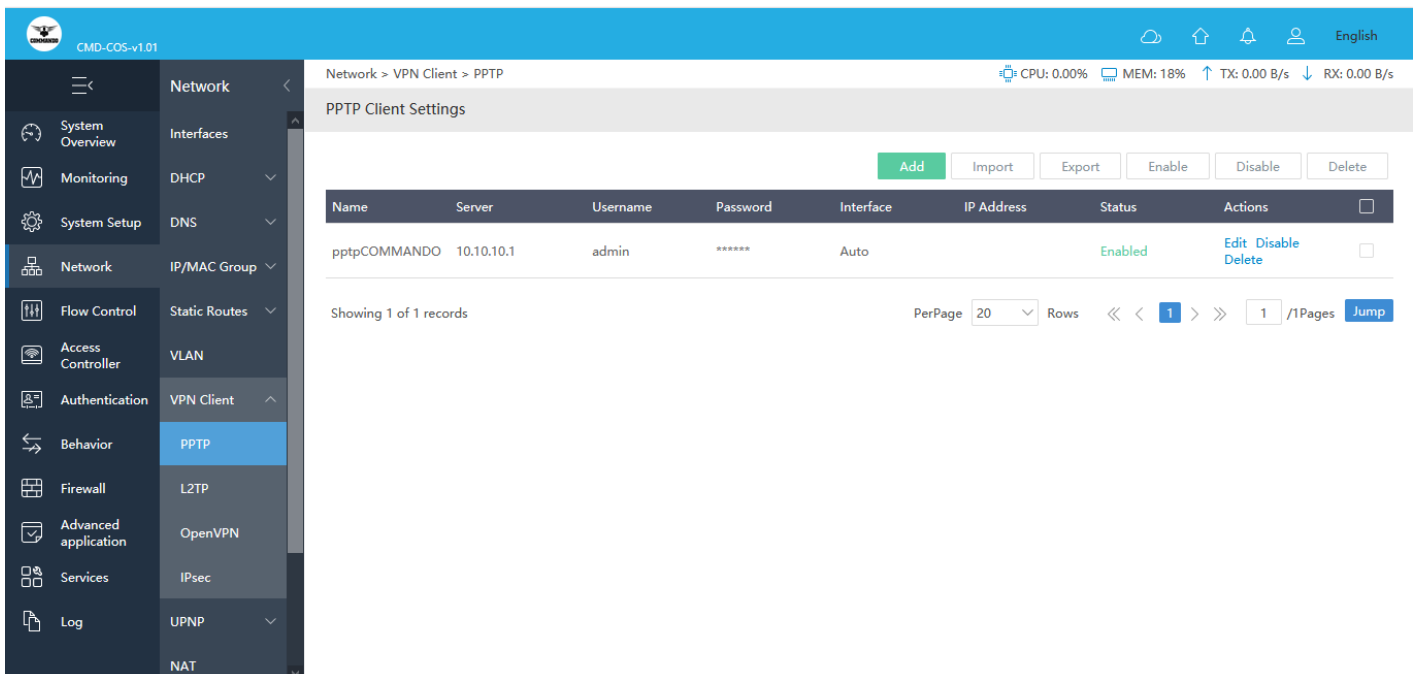
**Fig 3.7.2 Add PPTP Setting page**



**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



**Fig 3.7.4 PPTP Client setting page**

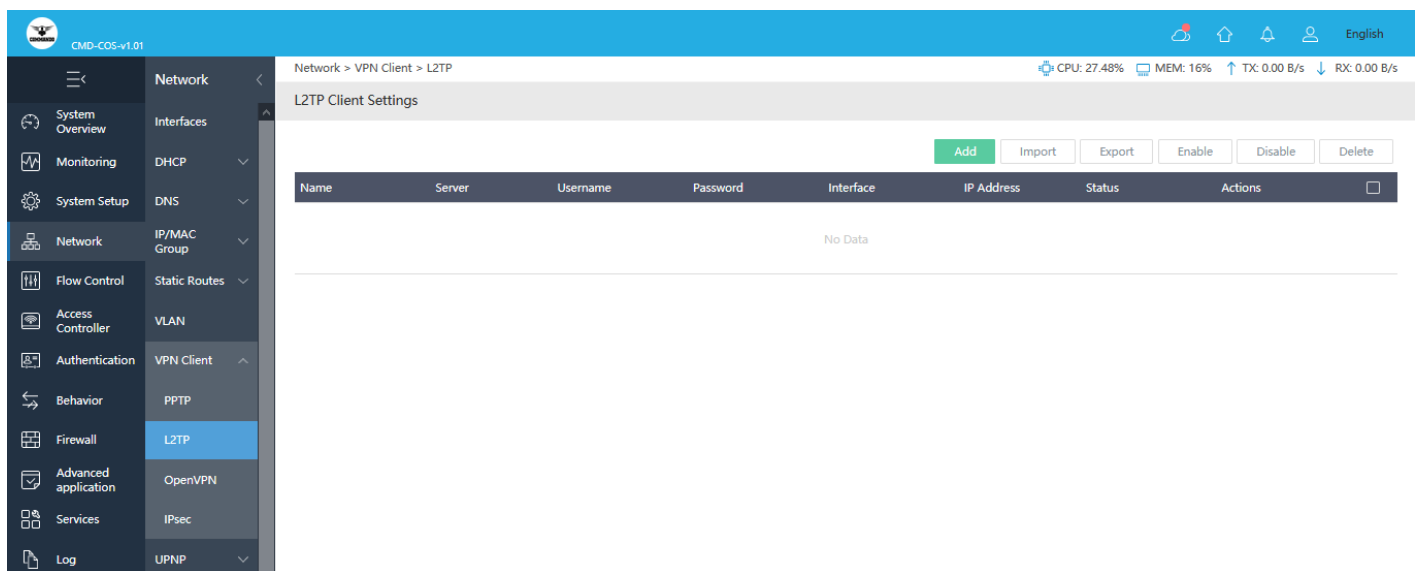
**L2TP:**

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

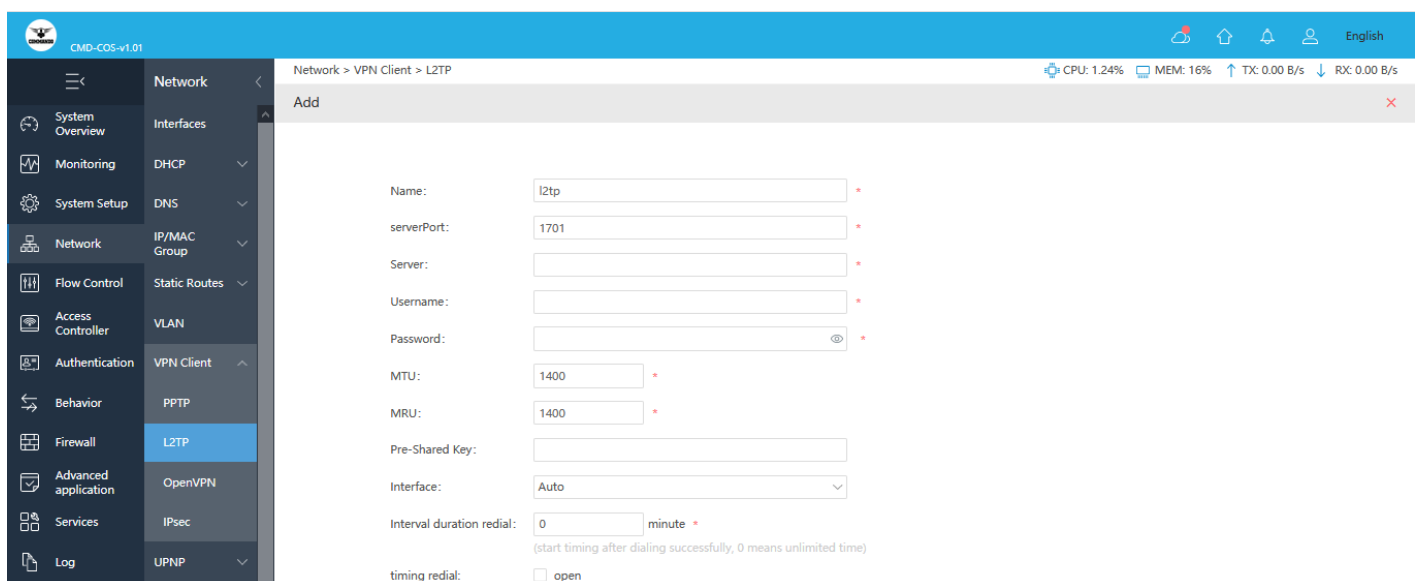


links with a remote LAN. Its ability to carry almost any L2 data format over IP or other L3 networks makes it particularly useful. PPTP (Point-to-Point Tunneling Protocol) is a lower-level encryption method compared to L2TP and OpenVPN. L2TP (Layer Two Tunneling Protocol) is considered a bit more secure 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 (LCCEs) 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.

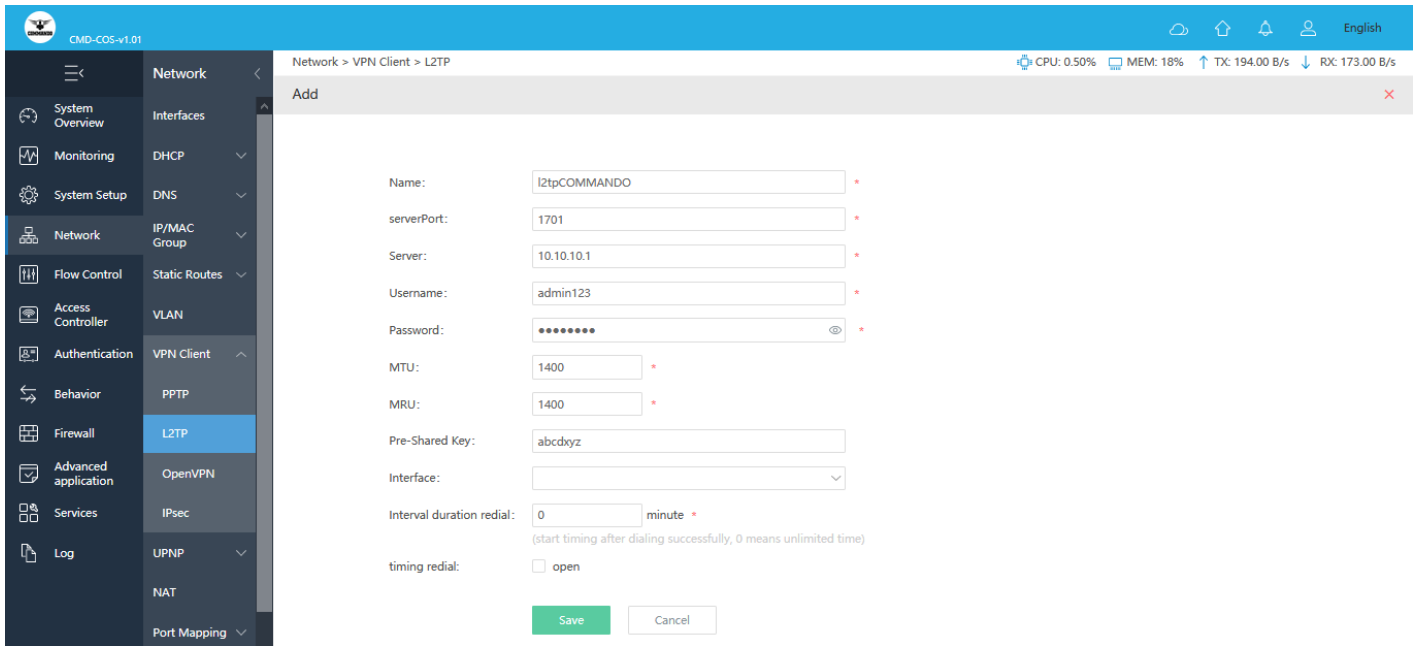
To configure L2TP Client Setting, Click on Network>VPN Client>L2TP



**Fig 3.7.5 Default L2TP Client setting page**



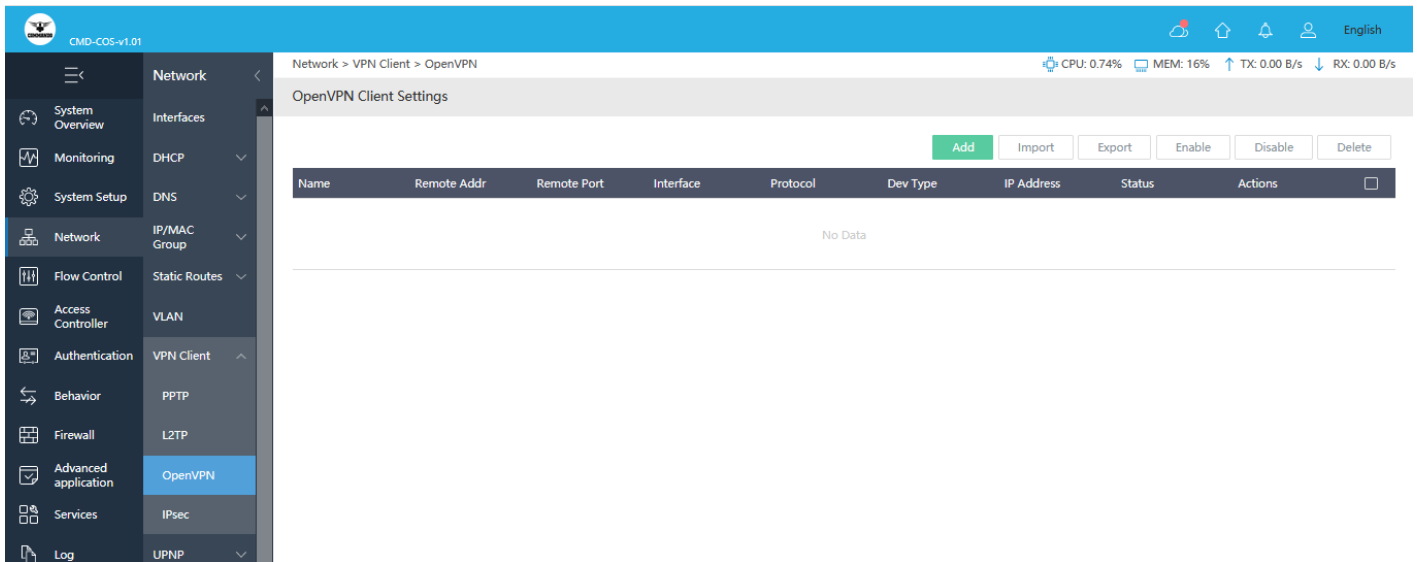
**Fig 3.7.6 Add L2TP Client setting page**



**Fig 3.7.6 L2TP Client setting with details page**

**Note:**

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



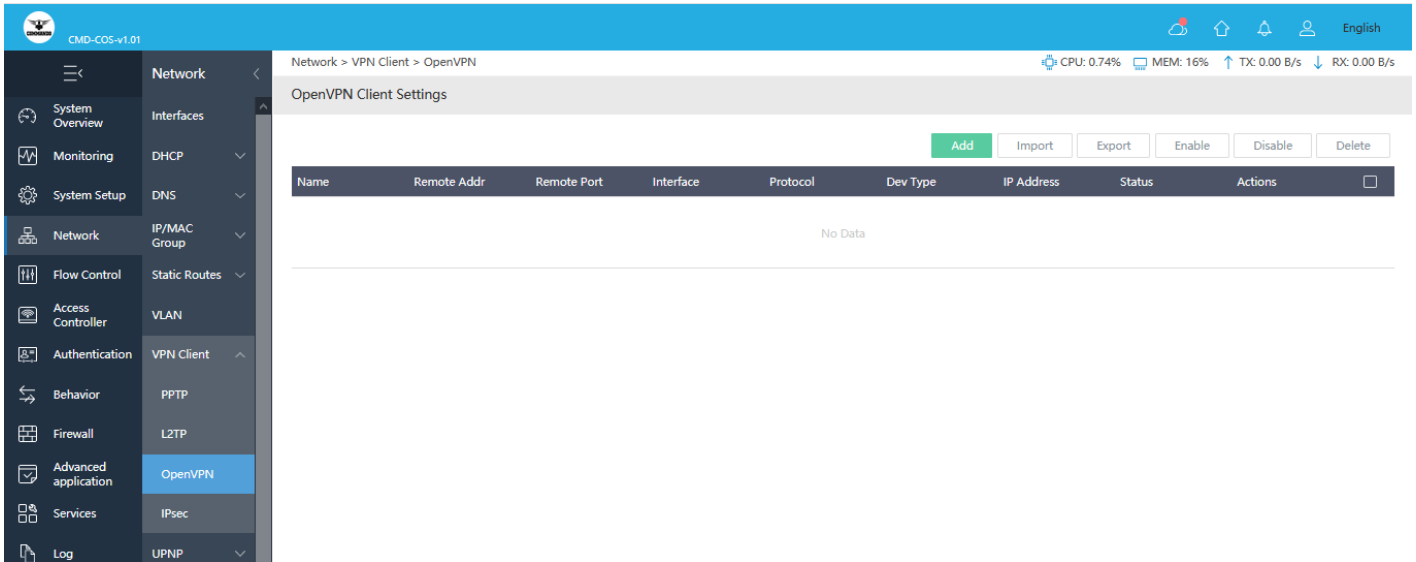
**Fig 3.7.7 L2TP Client setting page**

**OpenVPN:**

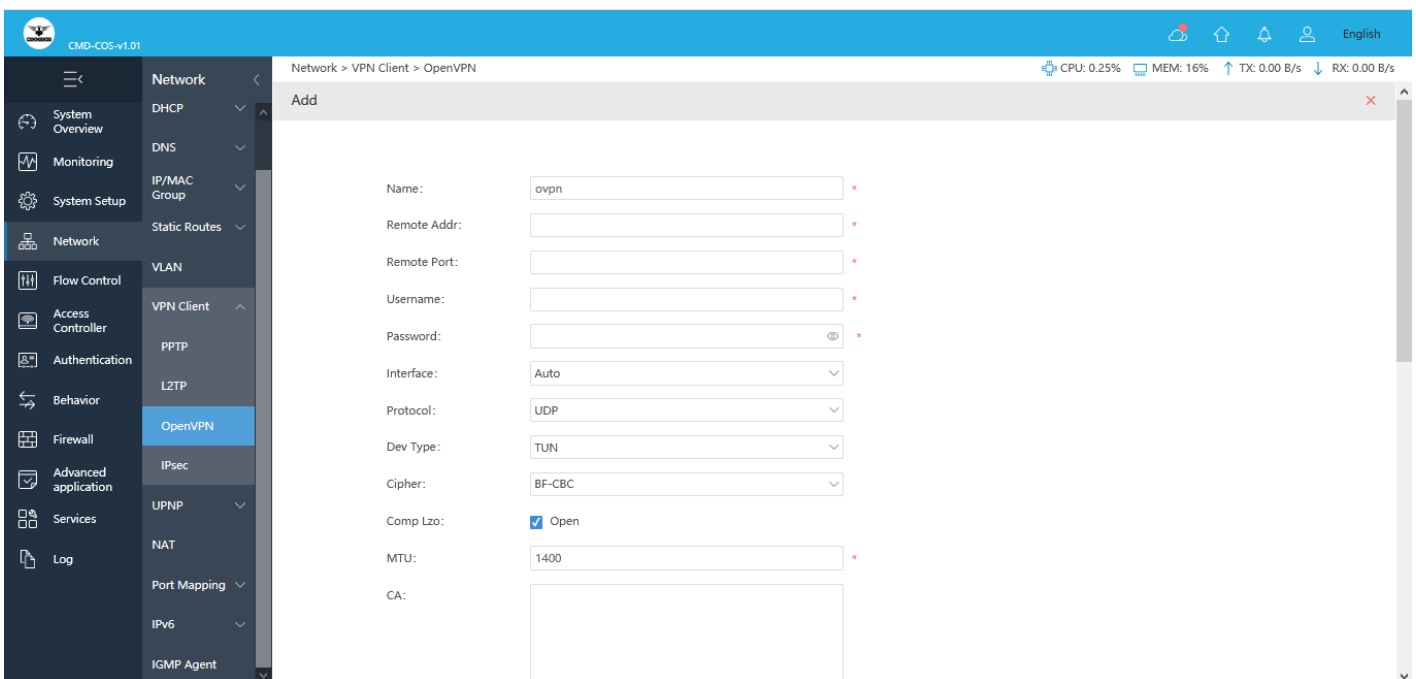
OpenVPN is short for open-source VPN. A router running OpenVPN in client mode, for example, facilitates users within that network to access their VPN without having to install OpenVPN on each computer on that network. A router running OpenVPN in client mode, for example, allows any device on a network 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



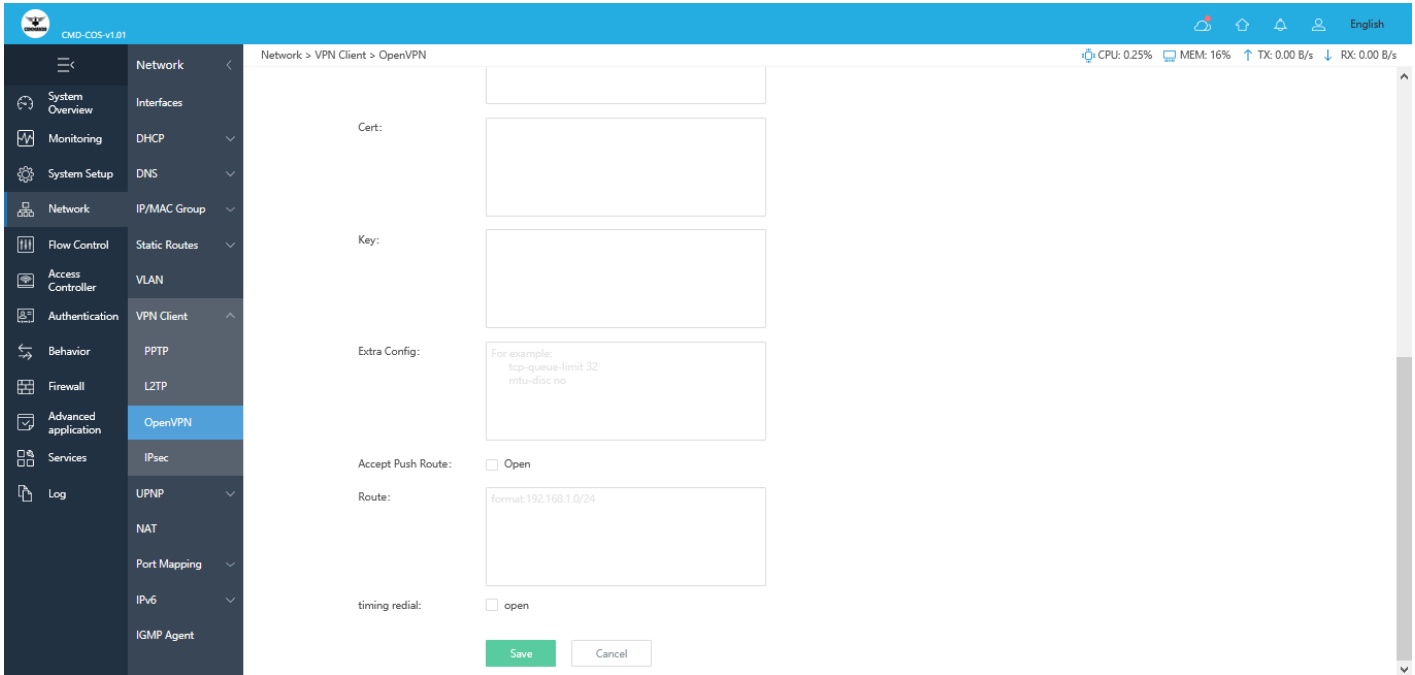
**Fig 3.7.8 Default OpenVPN Client setting page**



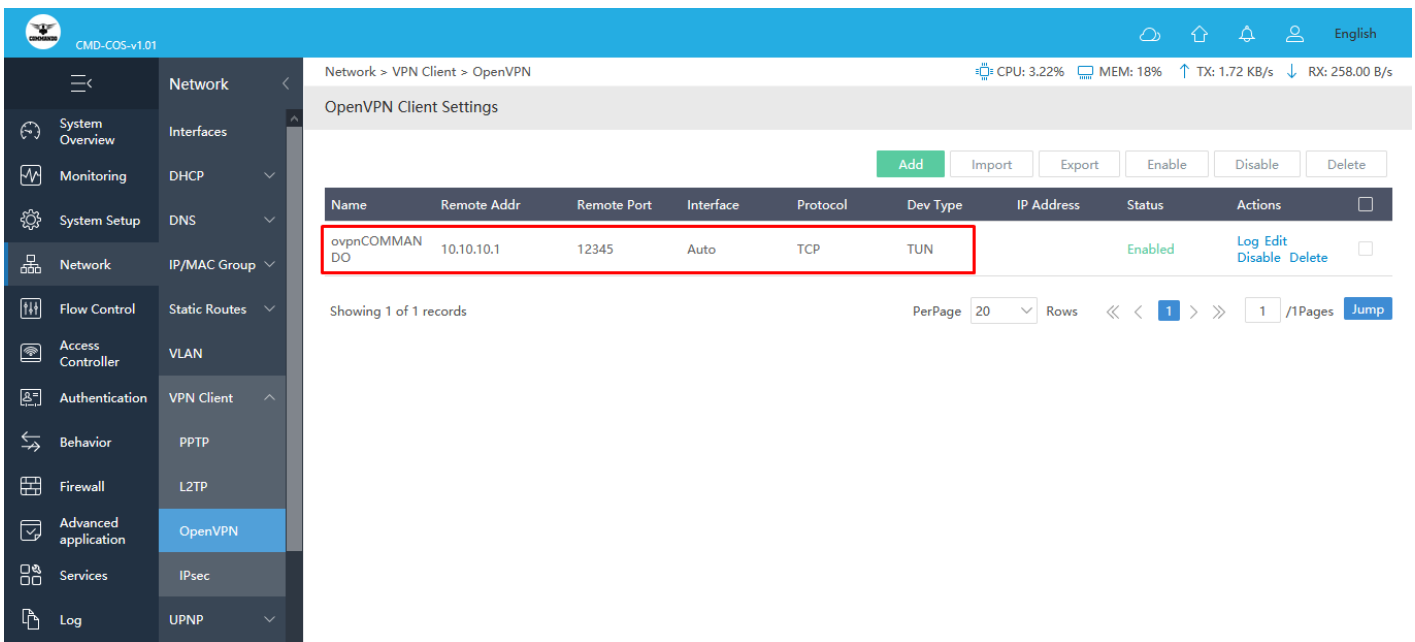
**Fig 3.7.9 Add OpenVPN Client setting page**

**Note:**

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



**Fig 3.7.10 OpenVPN Client details setting page**



**Fig 3.7.11 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?**

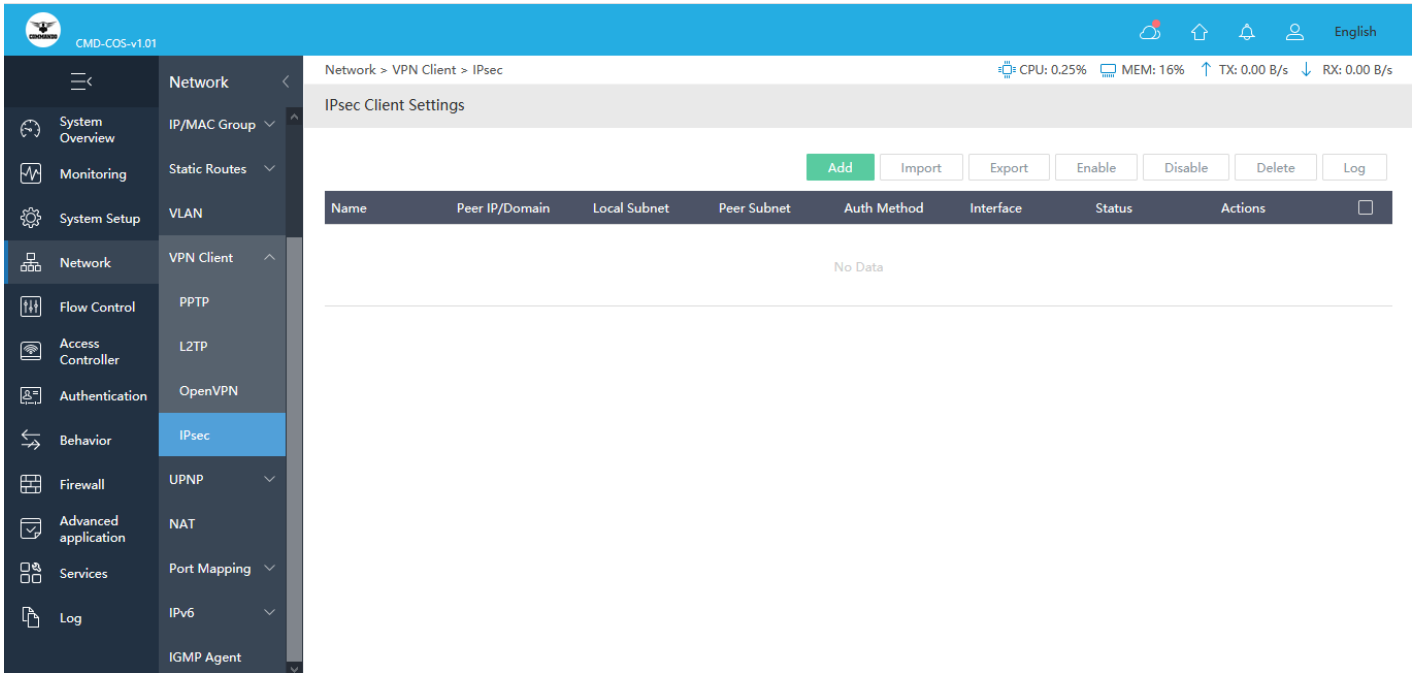
Users can access an IPsec VPN by logging into a VPN application, or "client." This typically requires the user to have installed the application on their device. VPN logins are usually password-based. While data sent over a VPN is encrypted, if user passwords are compromised, attackers can log into the VPN and steal this encrypted data. Using two-factor 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?**

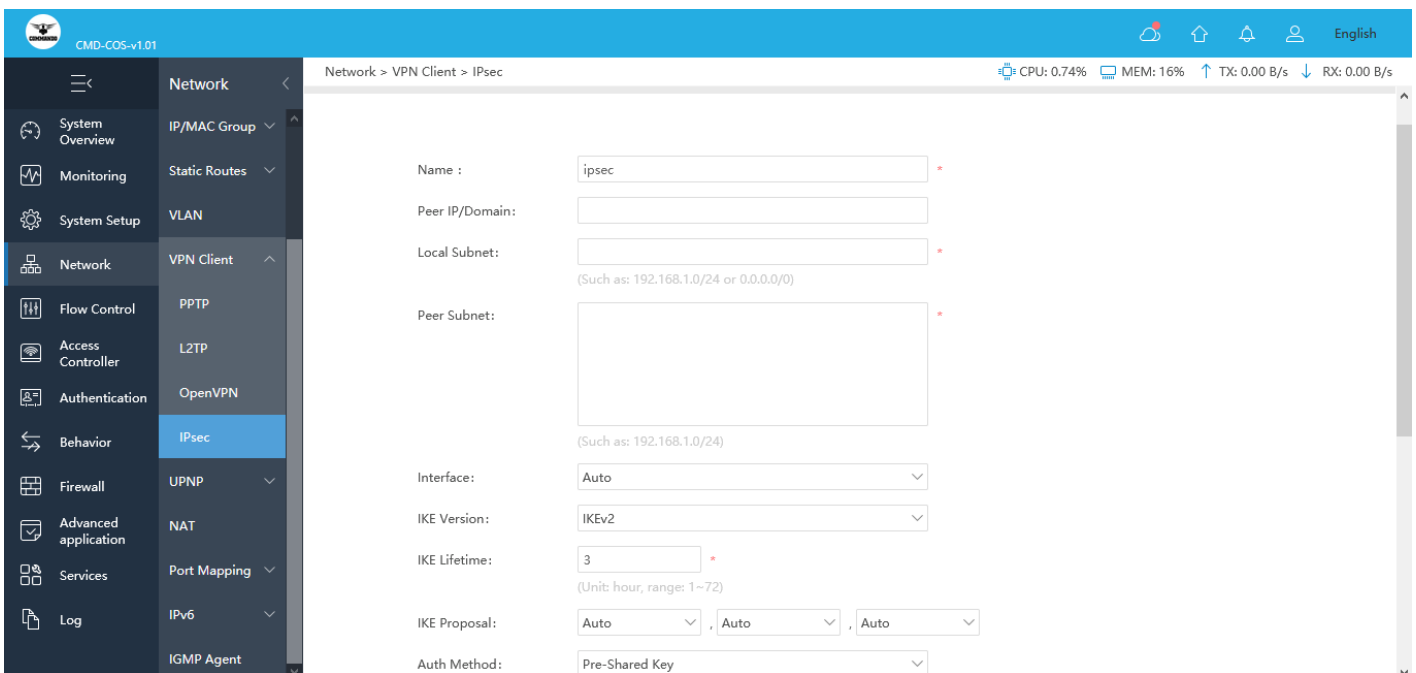
IPsec tunnel mode is used between two dedicated routers, with each router acting as one end of a virtual "tunnel" through a public network. In IPsec tunnel mode, the original IP header containing the final destination of the packet is encrypted, in addition to the packet payload. To tell intermediary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

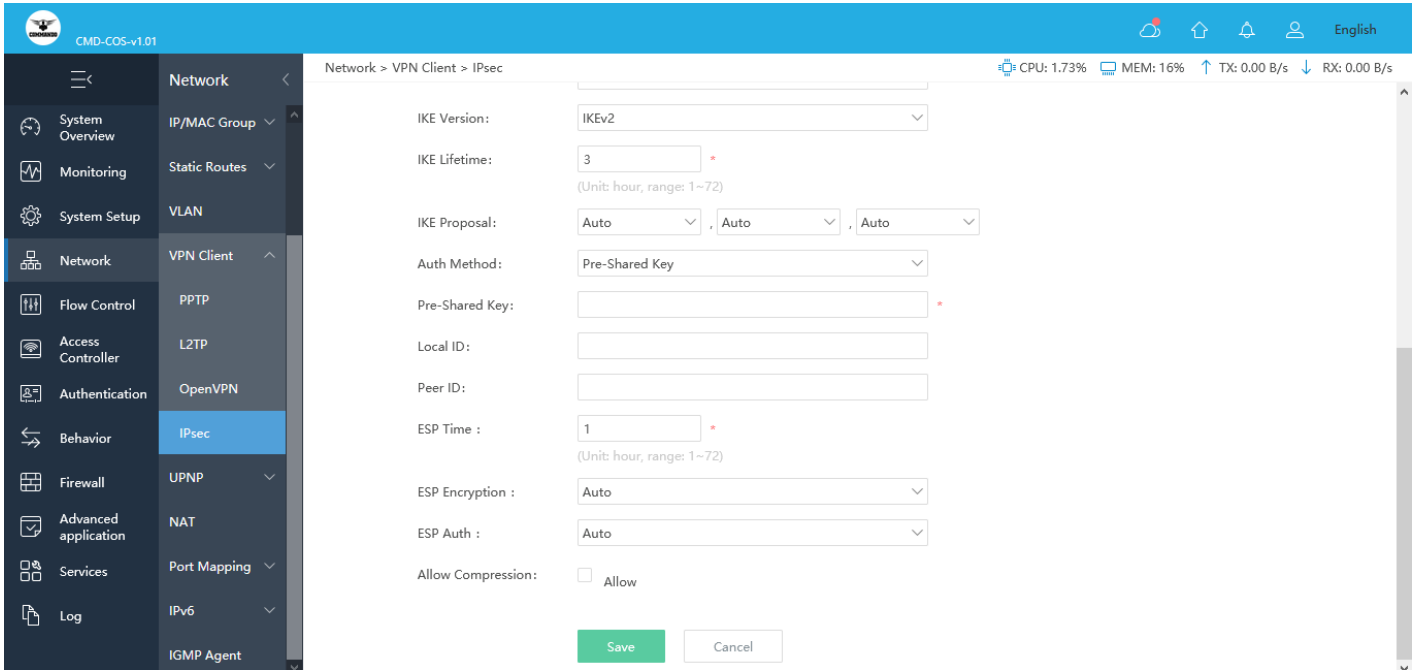
In transport mode, the payload of each packet is encrypted, but the original IP header is not. Intermediary routers are thus able to view the final destination of each packet — unless a separate tunneling protocol (such as GRE) is used.

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

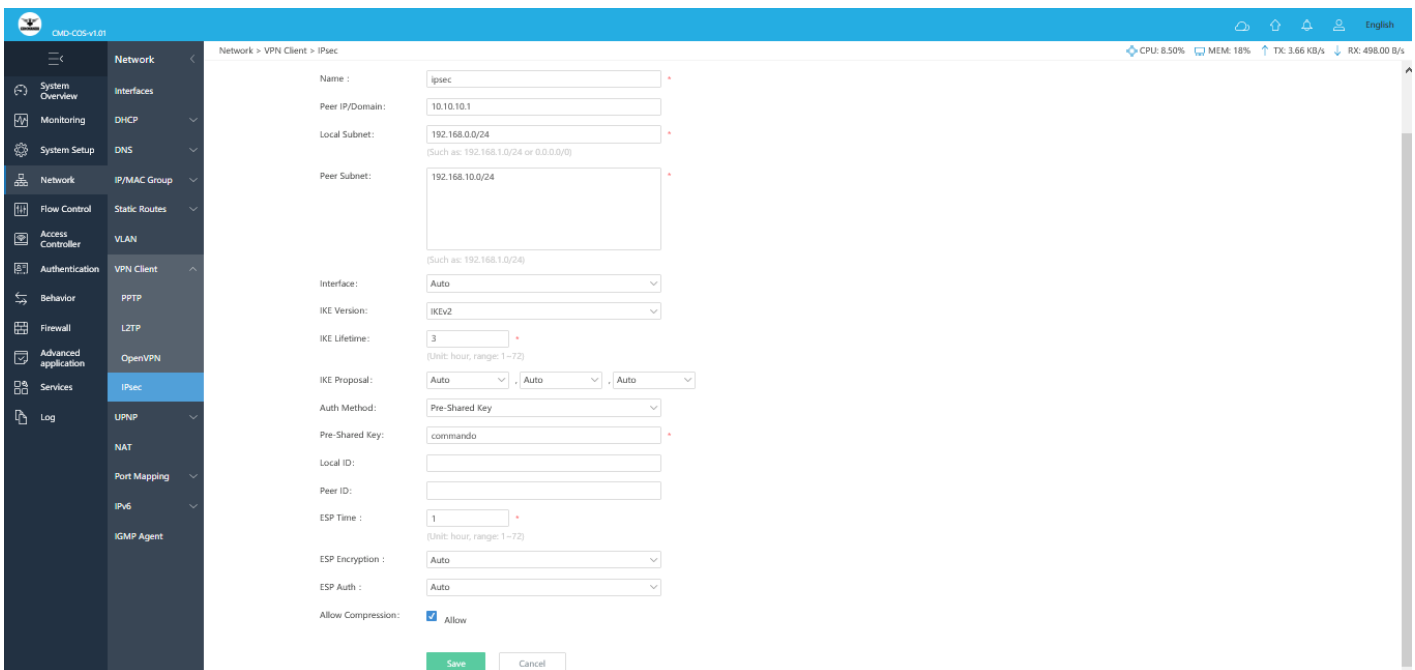


**Fig 3.7.12 Default IPsec Client setting page**

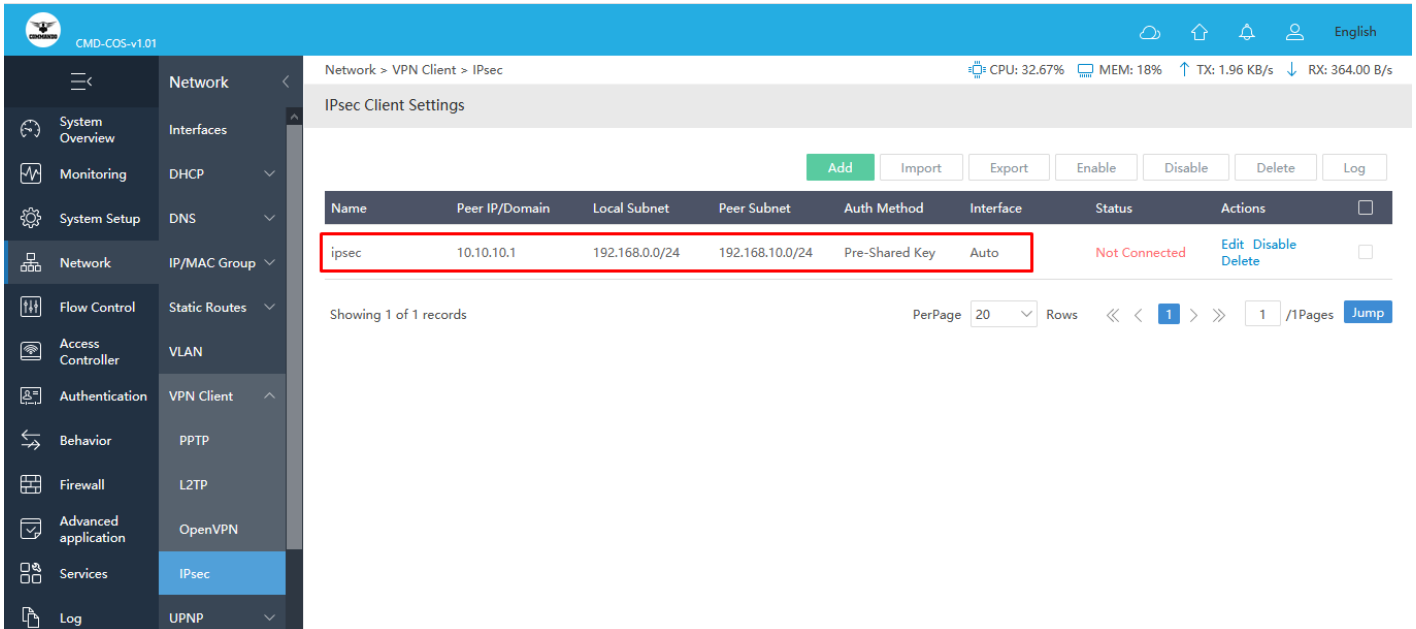




**Fig 3.7.13 Add IPsec Client setting page**



**Fig 3.7.14 IPsec Client details setting page**



**Fig 3.7.15 IPsec Client setting 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

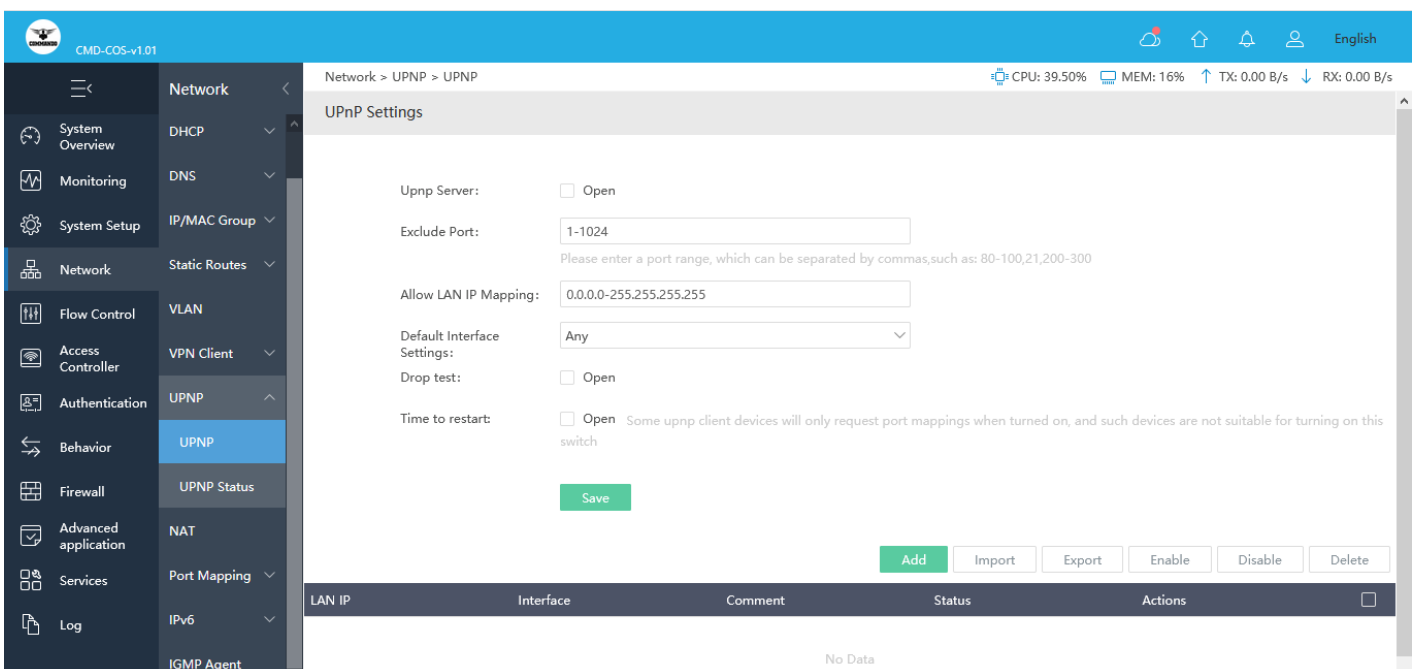




Fig 3.8.1 Default UPnP setting page

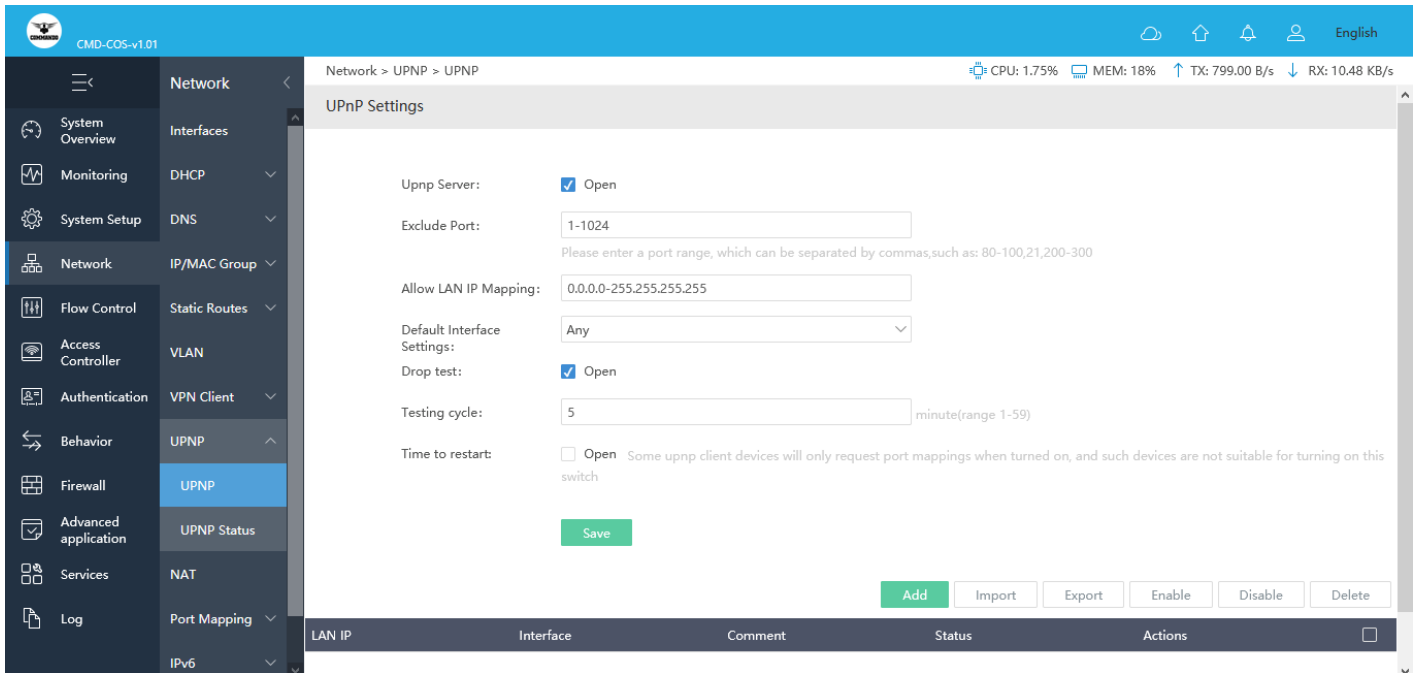


Fig 3.8.2 Enabling UPnP setting page

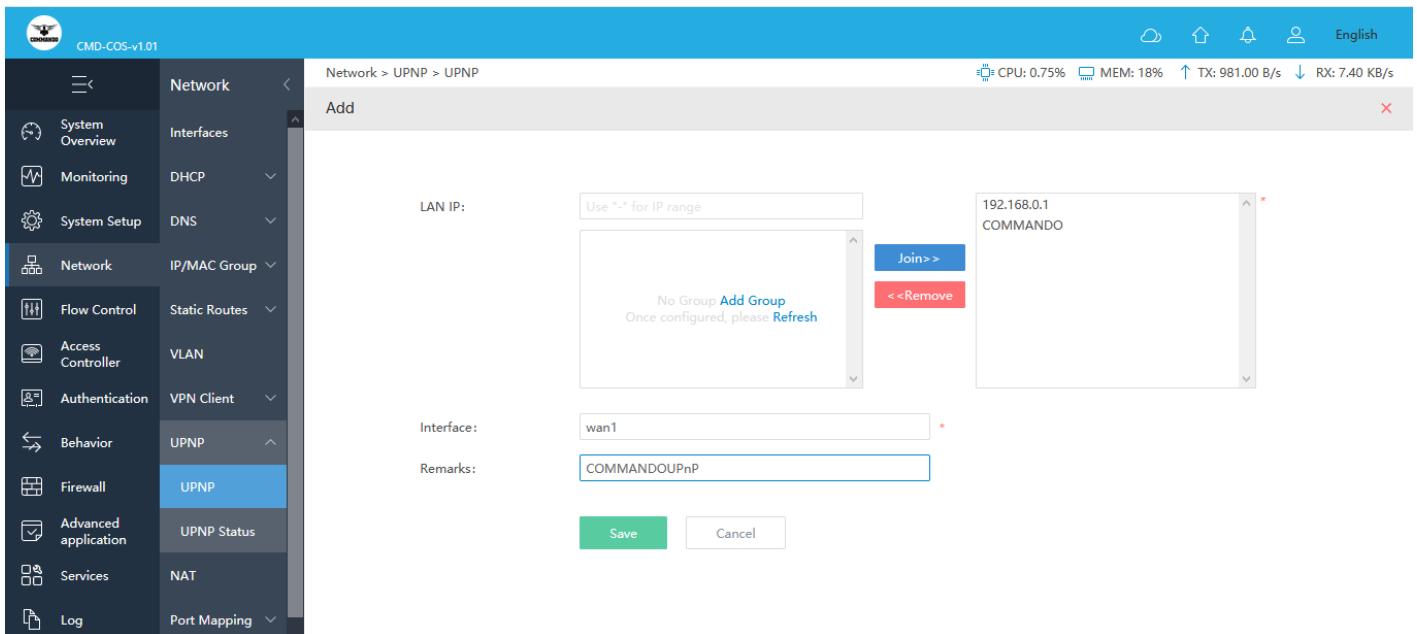


Fig 3.8.3 Add UPnP setting page

The screenshot shows the 'UPnP Settings' page in the CMD-COS v1.01 web interface. The left sidebar contains a navigation menu with categories like System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Network' section is expanded, and 'UPnP' is selected. The main content area displays the following settings:

- Upnp Server:  Open
- Exclude Port:  (Note: 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 (Note: Some upnp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch)

At the bottom of the settings area, there is a 'Save' button and a row of action buttons: Add, Import, Export, Enable, Disable, and Delete. Below this is a table with the following data:

LAN IP	Interface	Comment	Status	Actions
192.168.0.1,COMMANDO	wan1	COMMANDOUPnP	Enabled	Edit Disable Delete

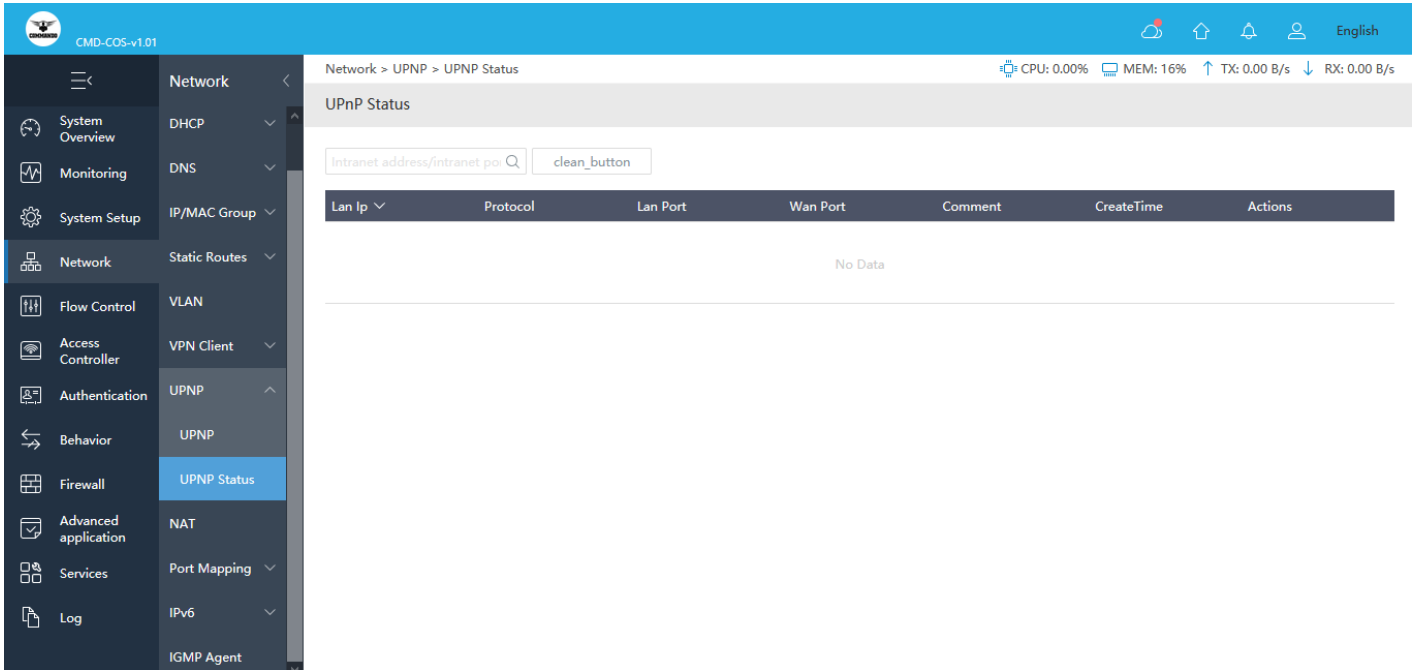
The table shows 1 of 1 records. At the bottom right, there are pagination controls: PerPage 20, Rows, and a 'Jump' button.

**Fig 3.8.4 UPnP setting page**

### UPnP Status:

Conceptually, UPnP extends plug and play—a technology for dynamically attaching devices directly to router 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, NAT 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**

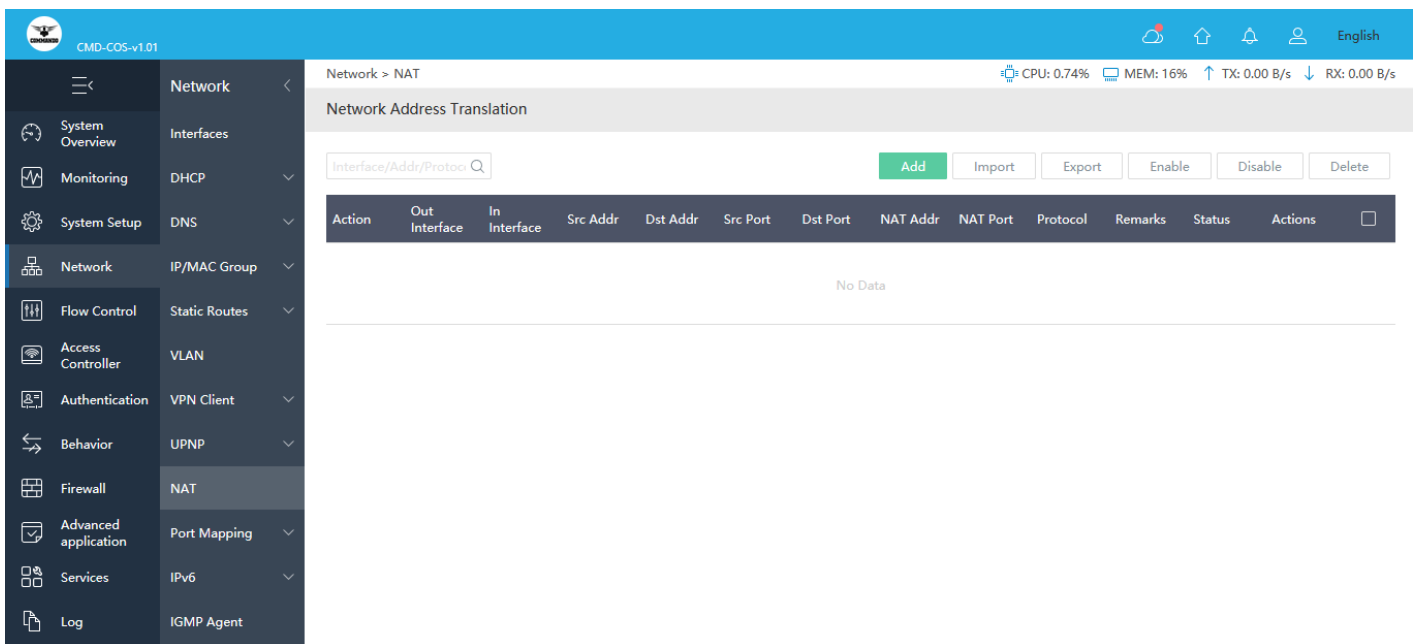
NAT and NAPT can translate only IP addresses in IP datagram headers and port numbers in TCP/UDP headers. For some special protocols such as FTP, IP addresses or port numbers may be contained in the Data field of the protocol packets. Therefore, NAT cannot translate the IP addresses or port numbers. A 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**

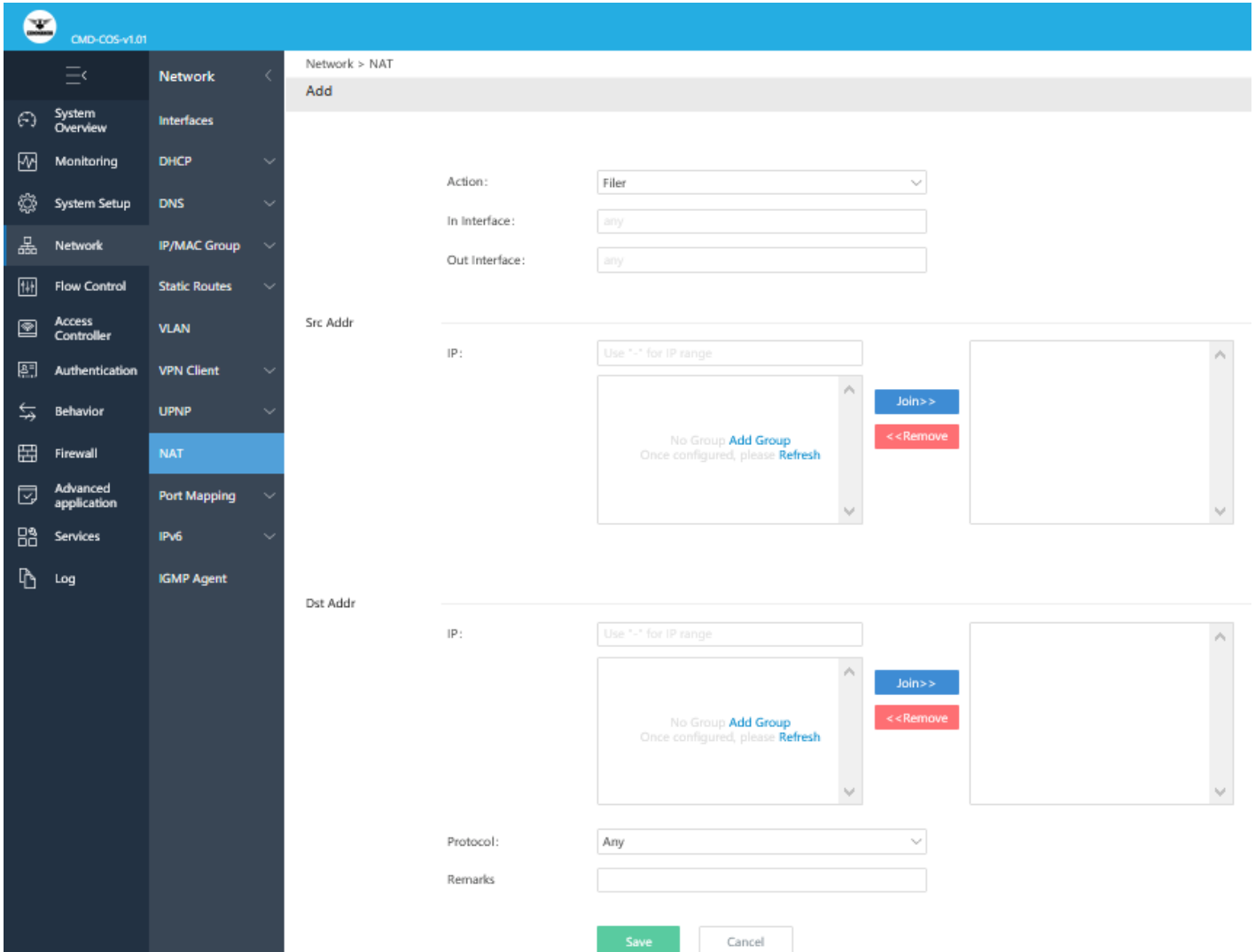


Fig 3.9.2 Default Add Network Address Translation page

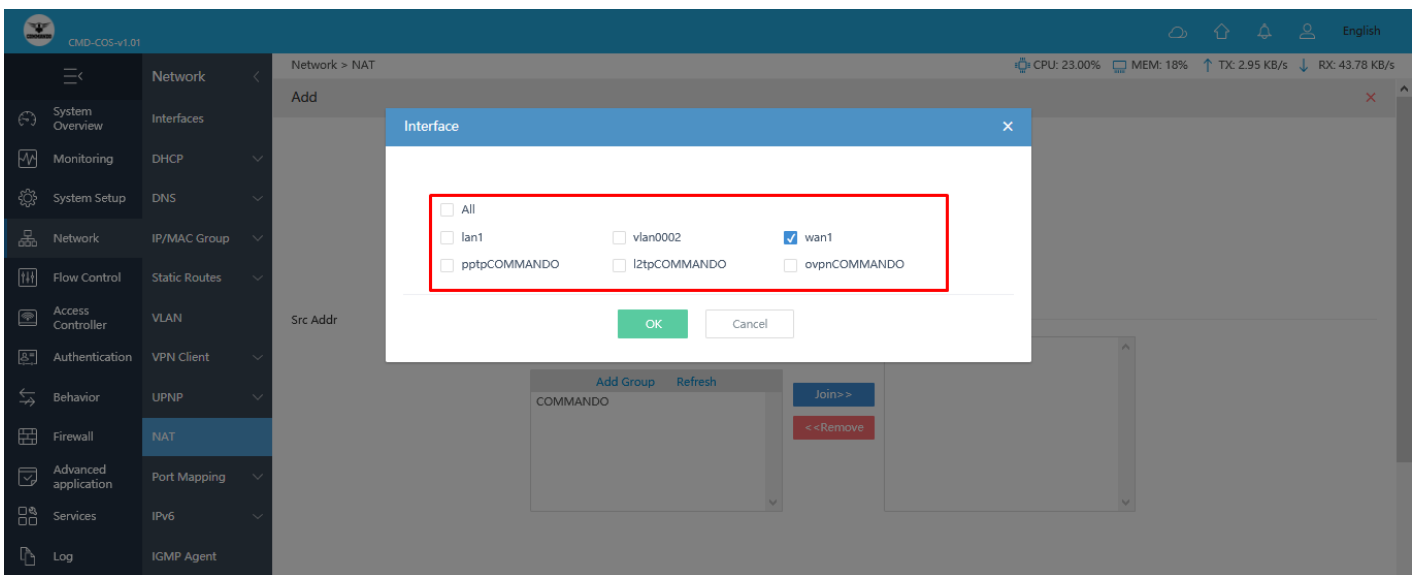
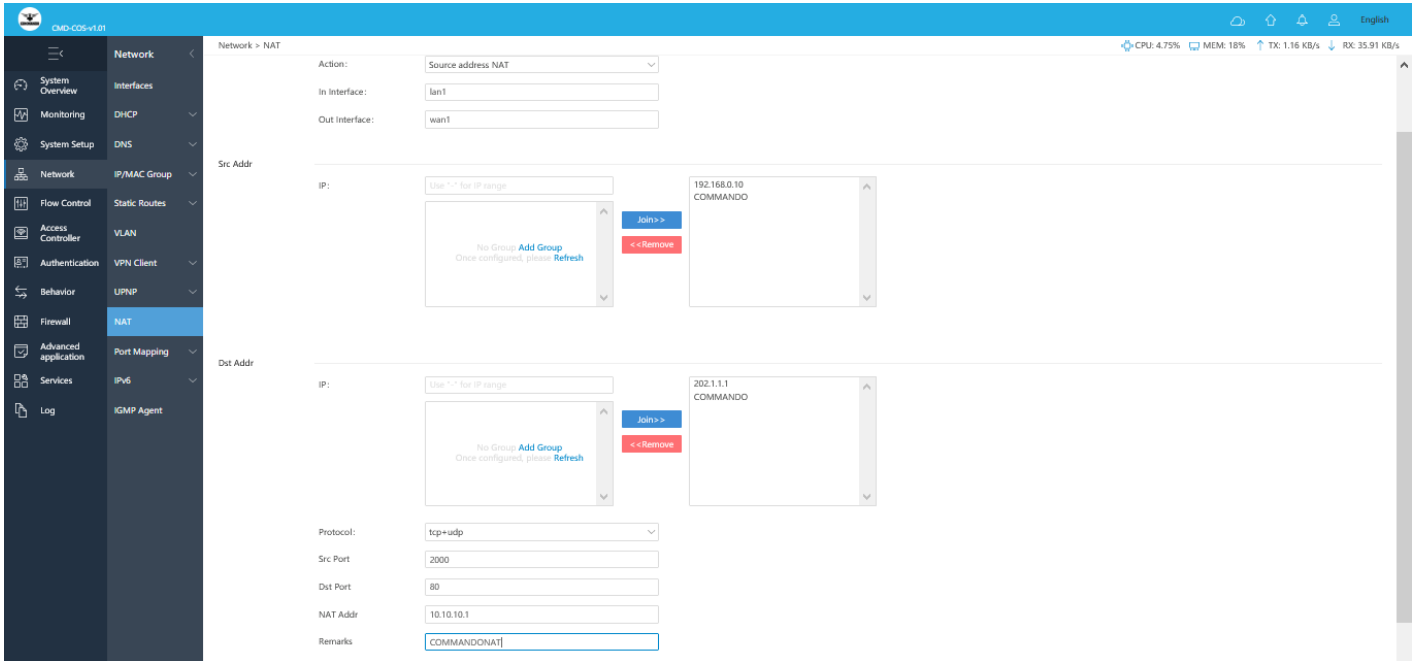
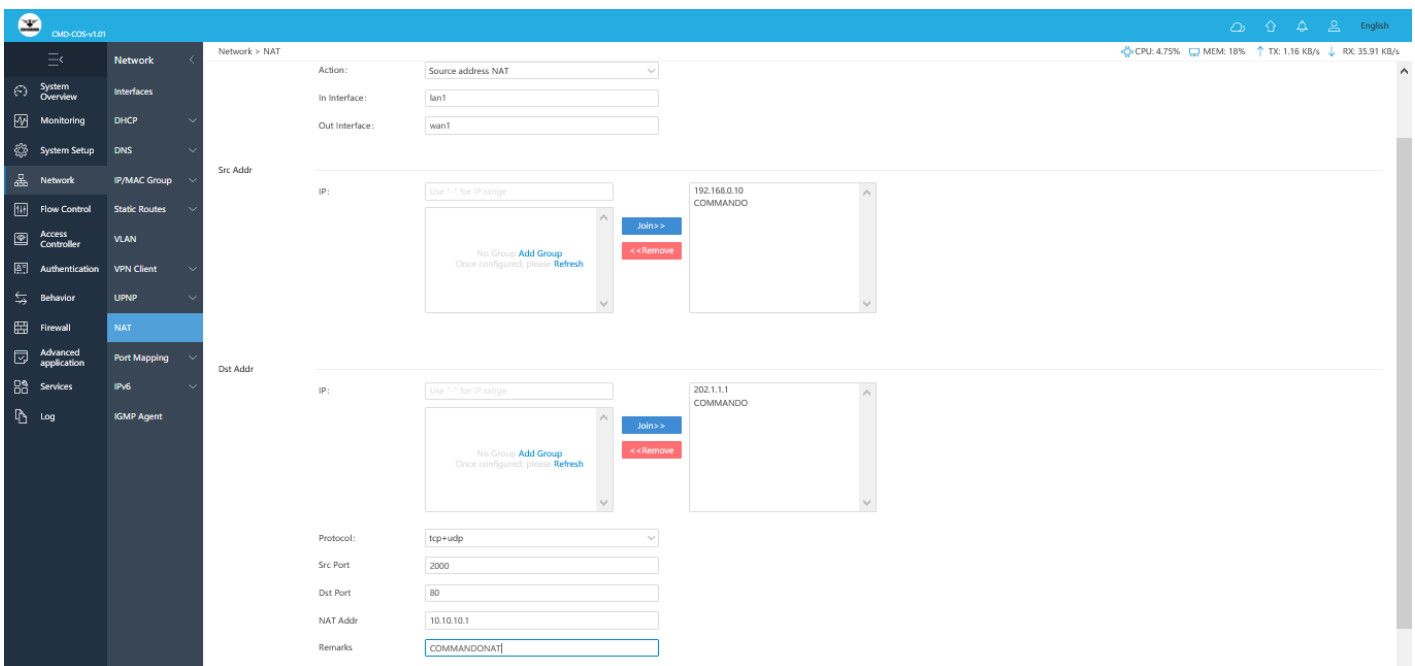


Fig 3.9.3 Add Network Address Translation for specific or all created interfaces page



**Fig 3.9.4 Network Address Translation details page**



**Fig 3.9.5 Network Address Translation 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 router. 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 router 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:

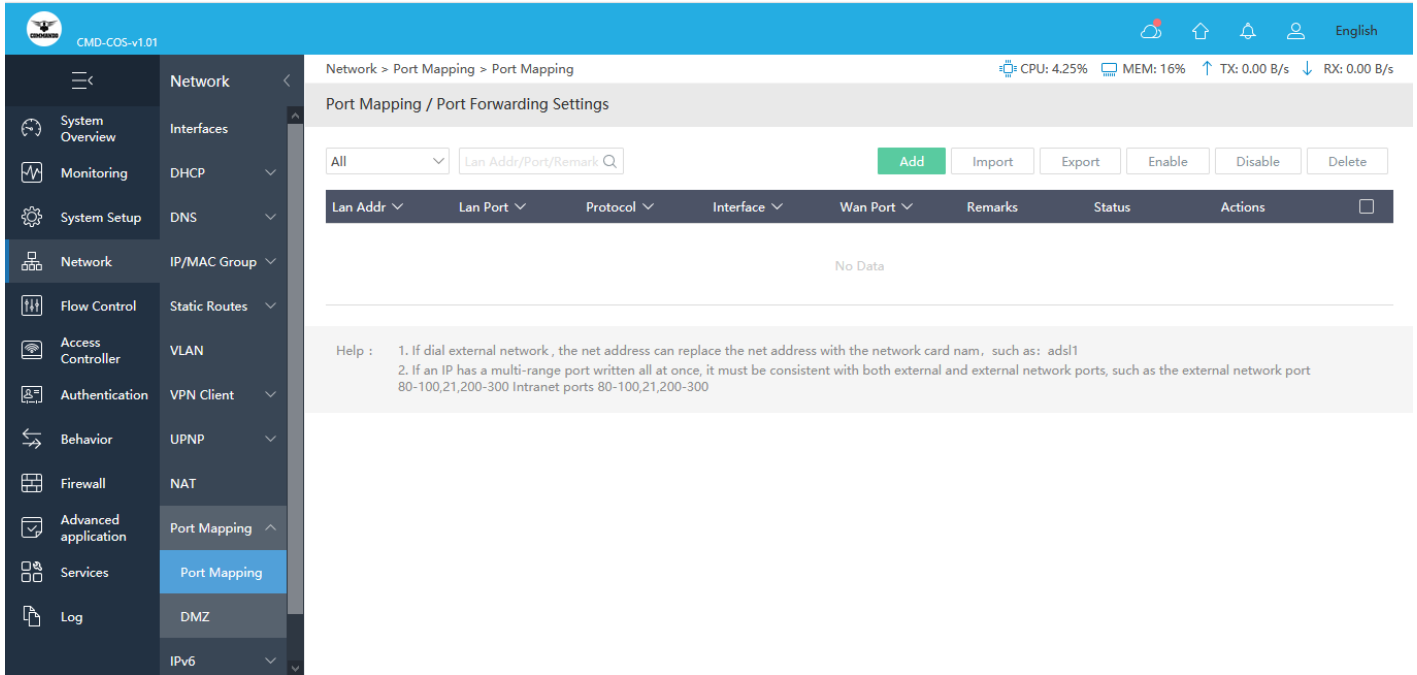
Remote port forwarding of port enables applications on the server side of a Secure Shell (SSH) connection to access services residing on the SSH's client side. Remote port forwarding lets users connect from the server side of a tunnel, SSH or another, to a remote network service located at the tunnel's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

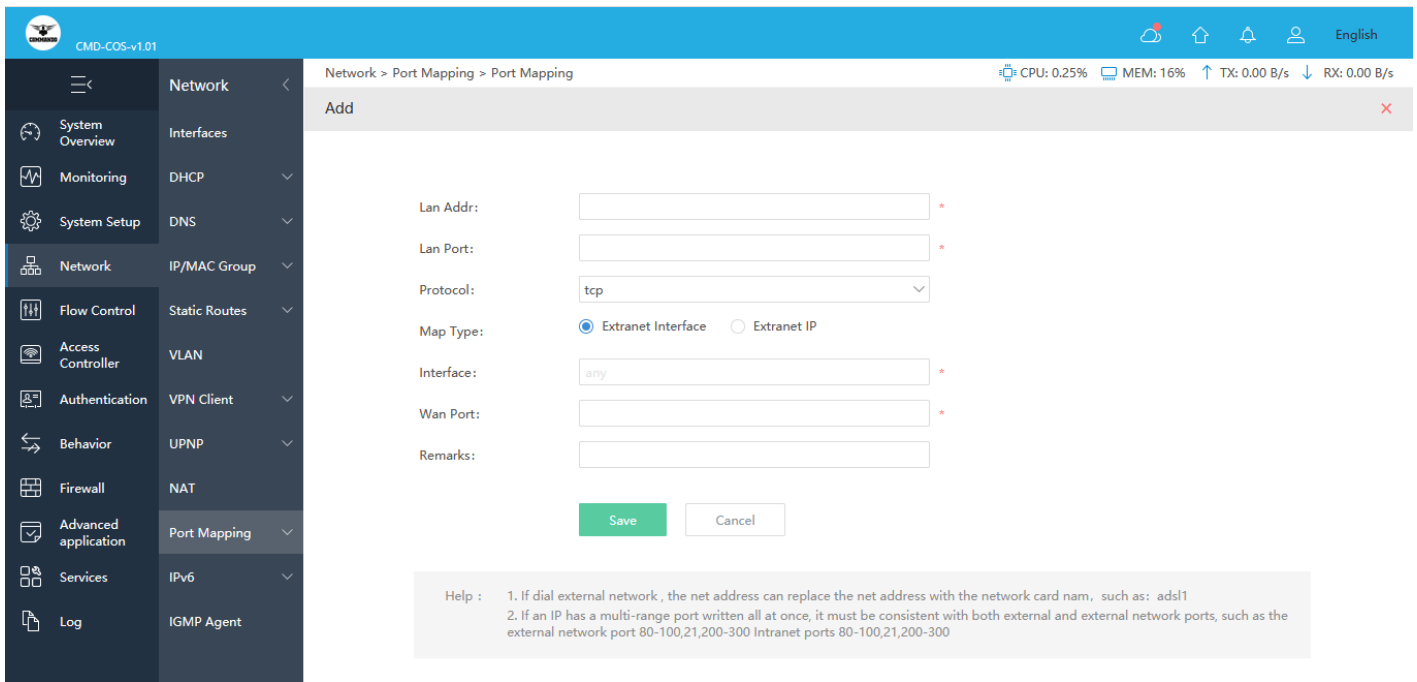
To configure Port Mapping / Port Forwarding Settings, Click on Network > Port Mapping >



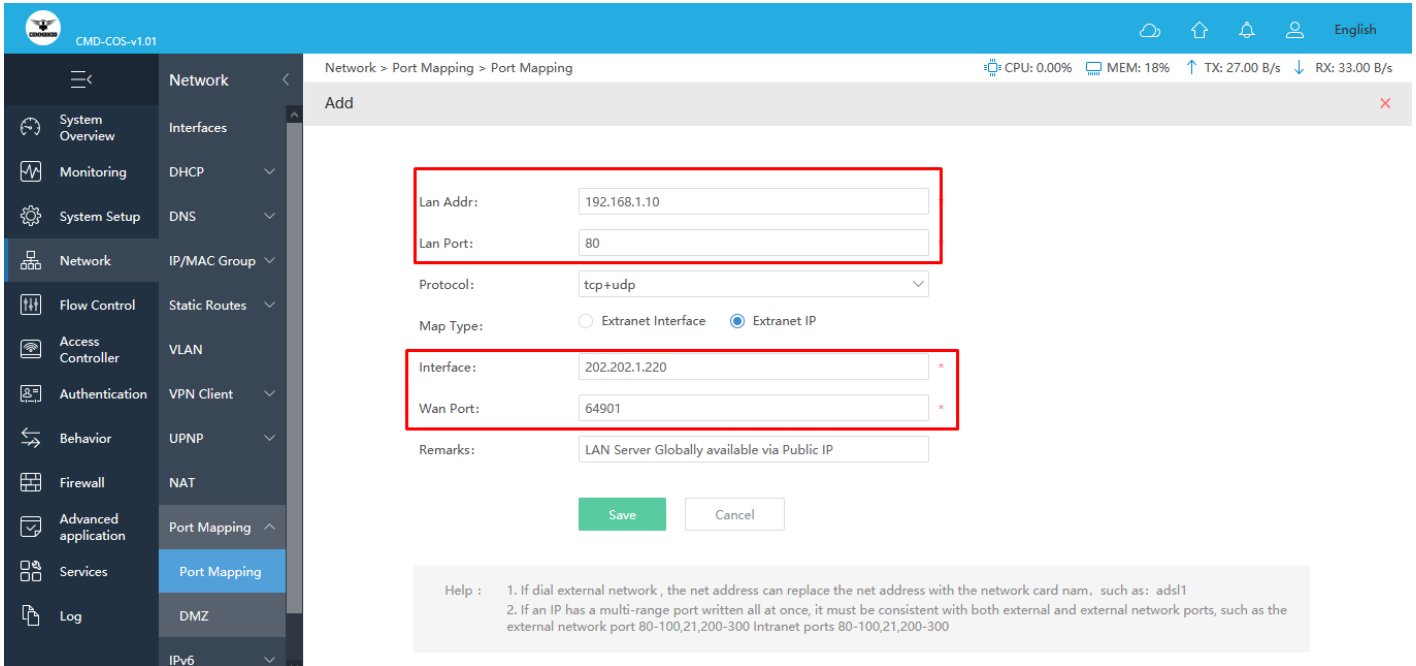
# Port Mapping



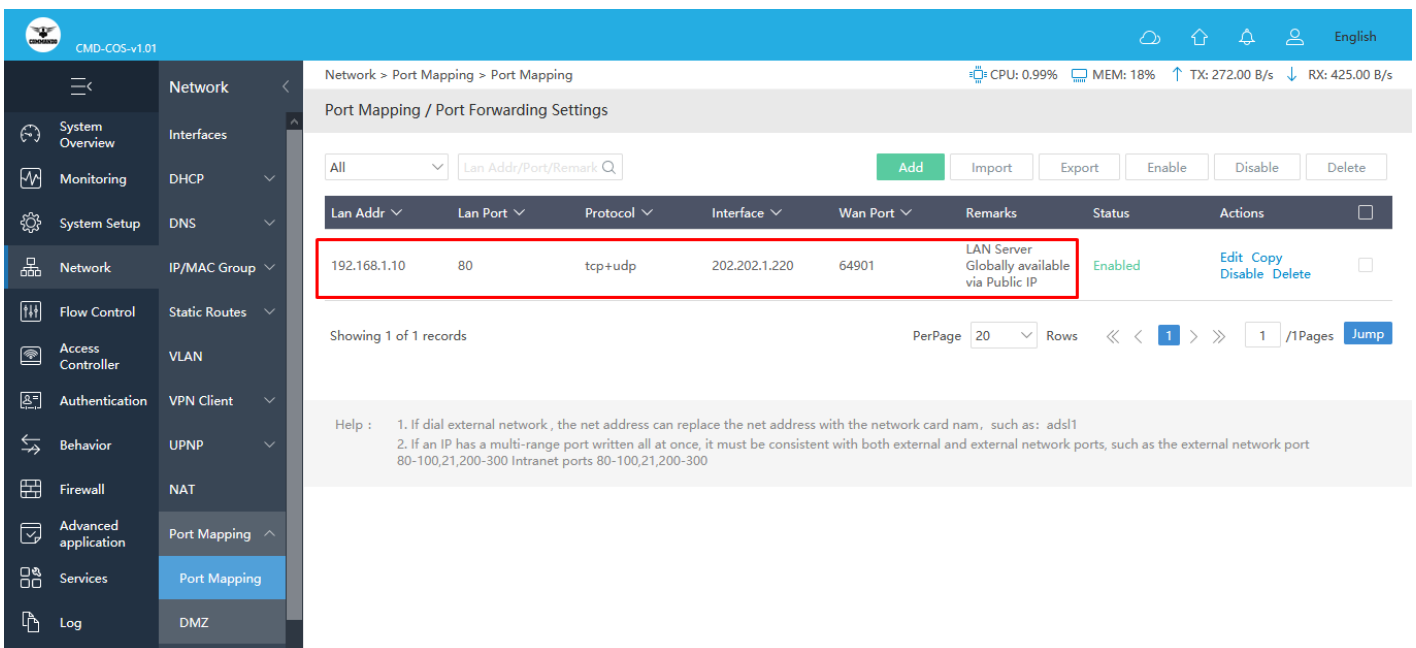
**Fig 3.10.1 Default Port Mapping / Port Forwarding Settings page**



**Fig 3.10.2 Add Port Mapping / Port Forwarding Settings page**



**Fig 3.10.3 Port Mapping / Port Forwarding Detail Settings page**



**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

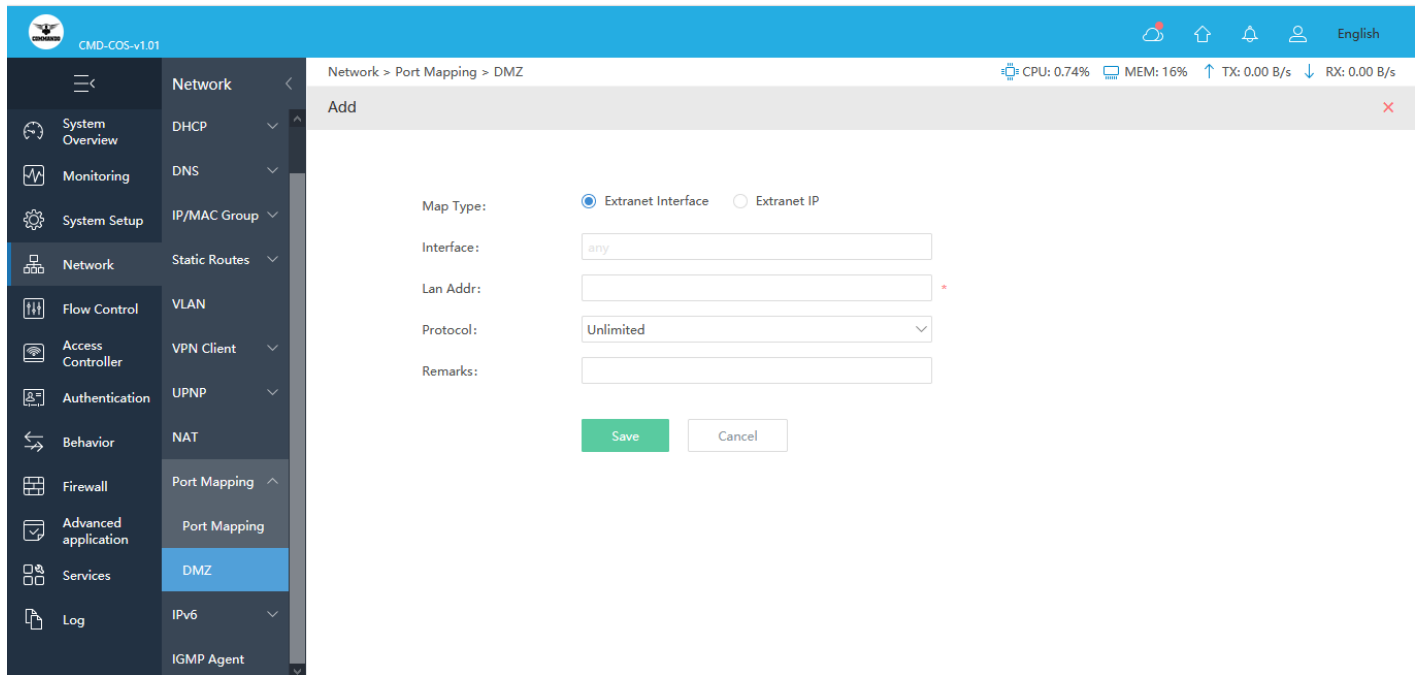
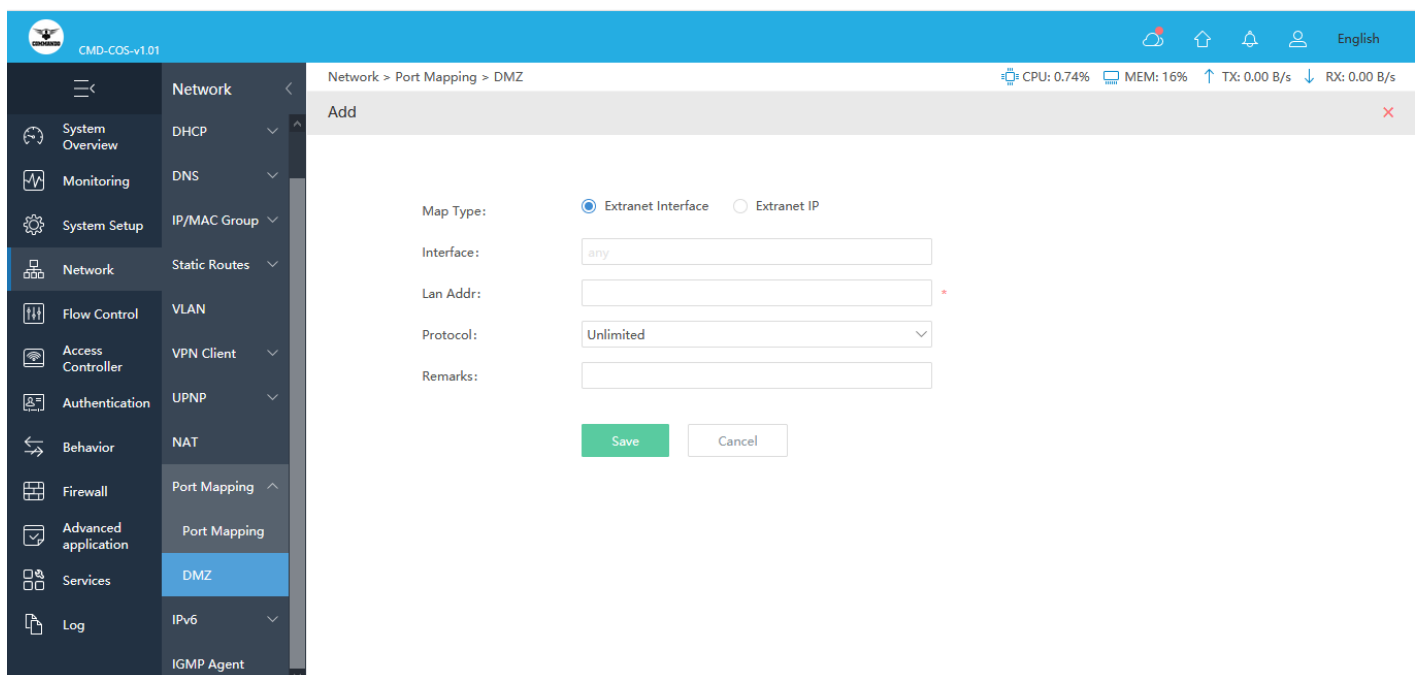
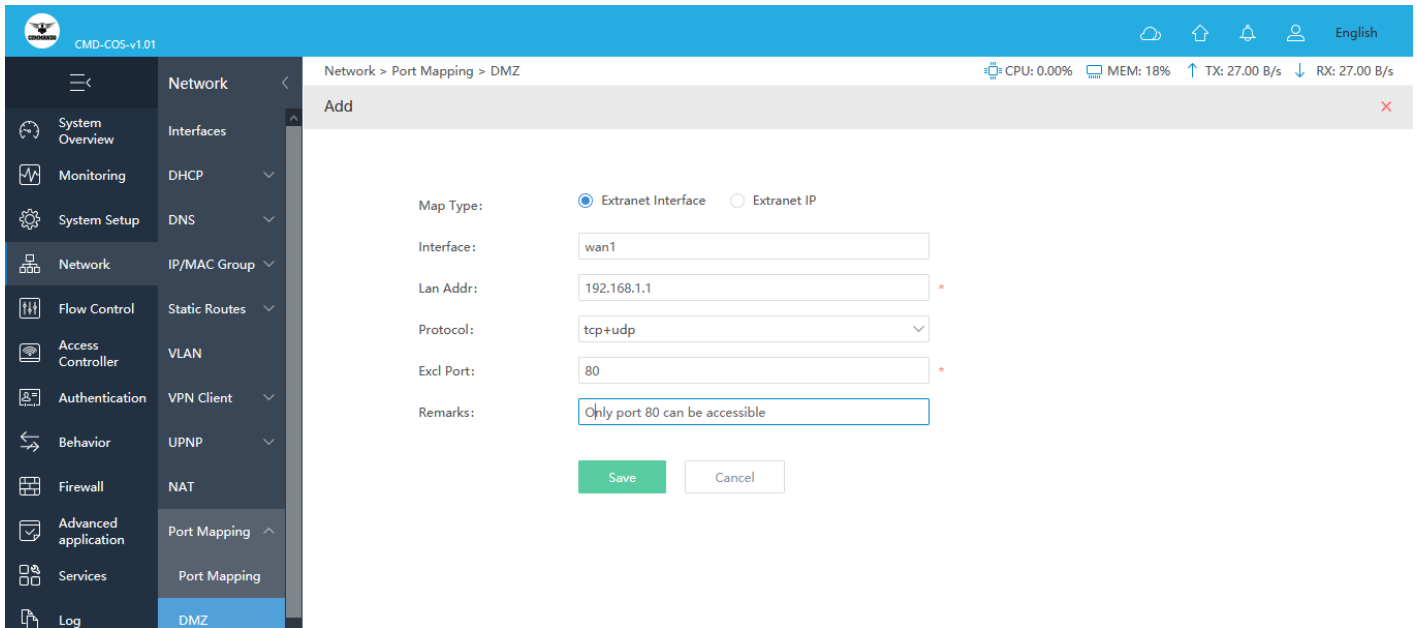


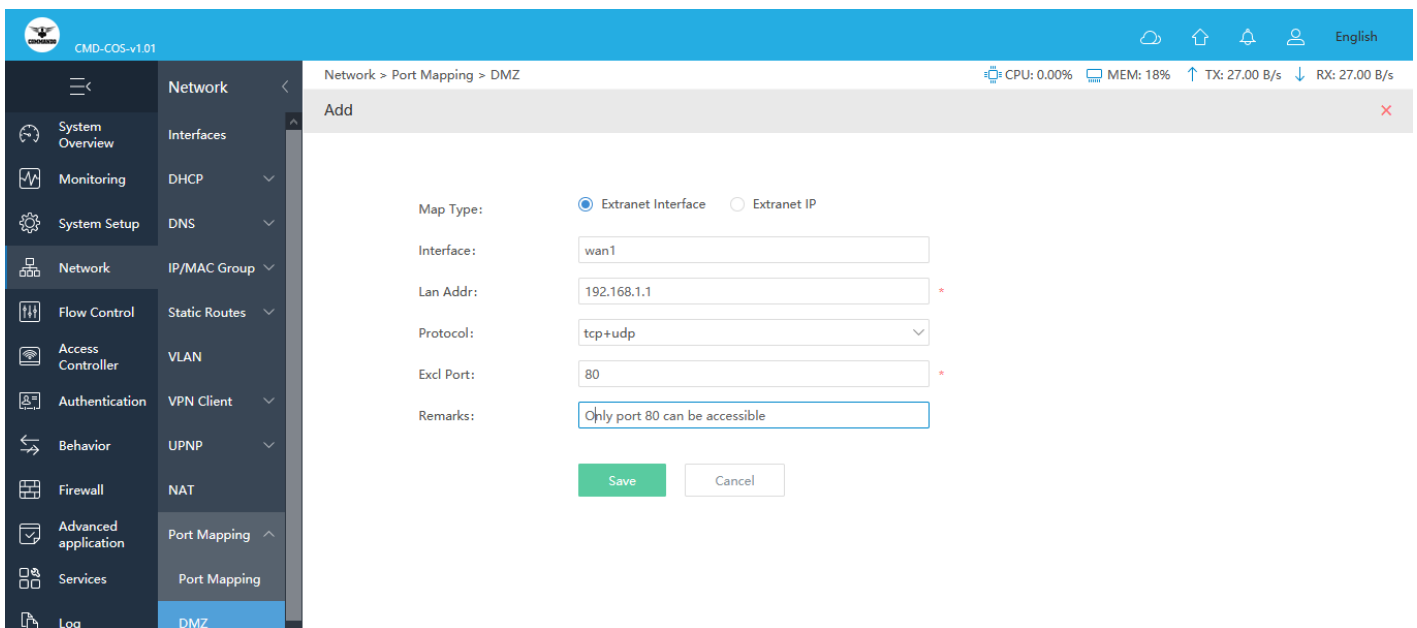
Fig 3.10.5 Default DMZ Settings page



**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

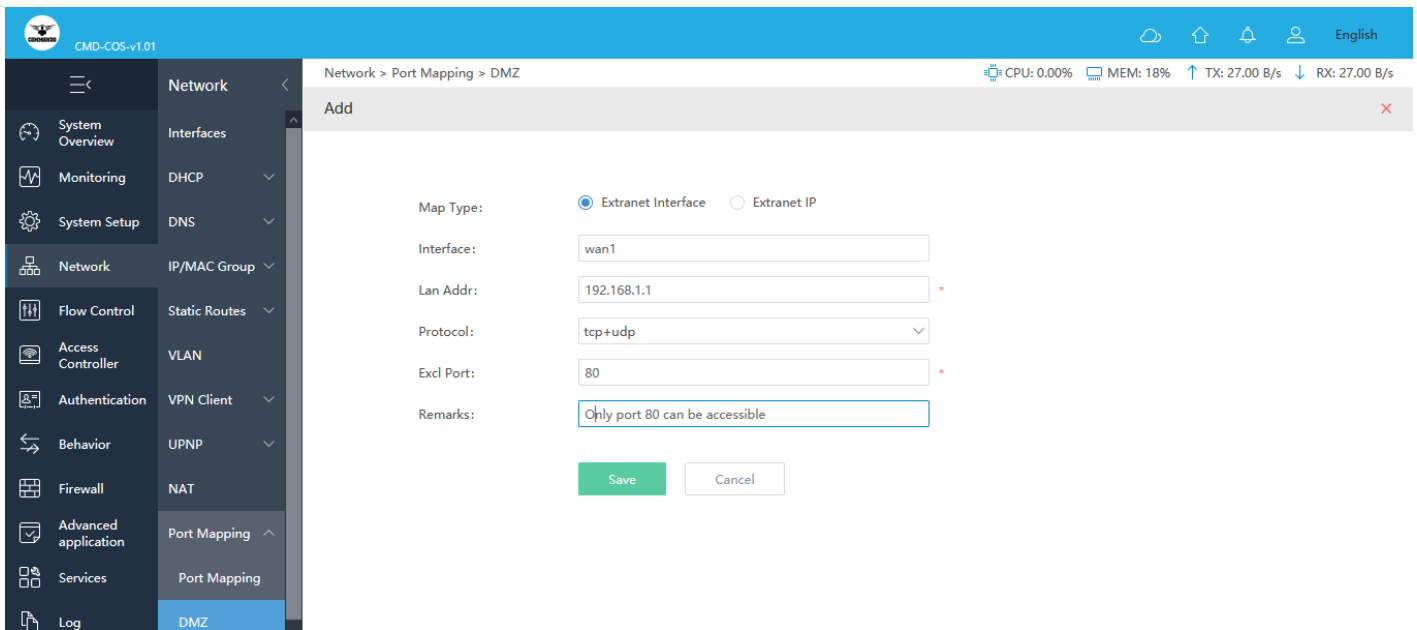


Fig 3.11.1 Default IPv6 Page

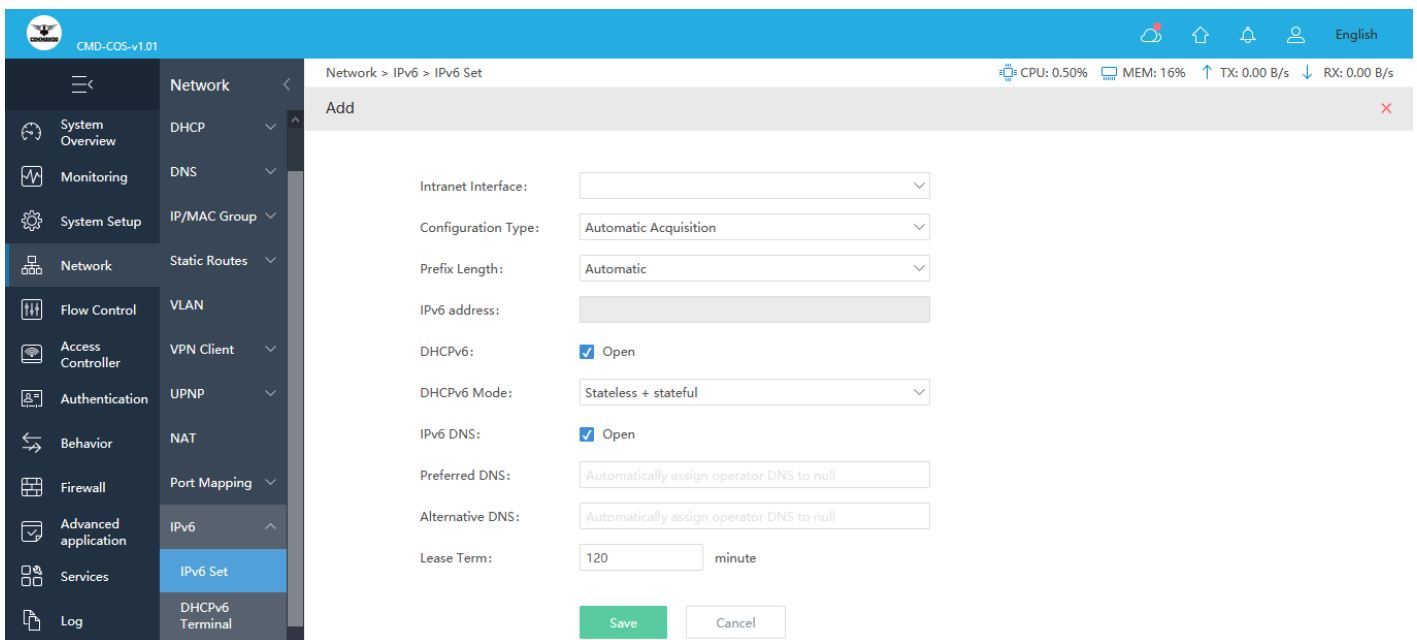
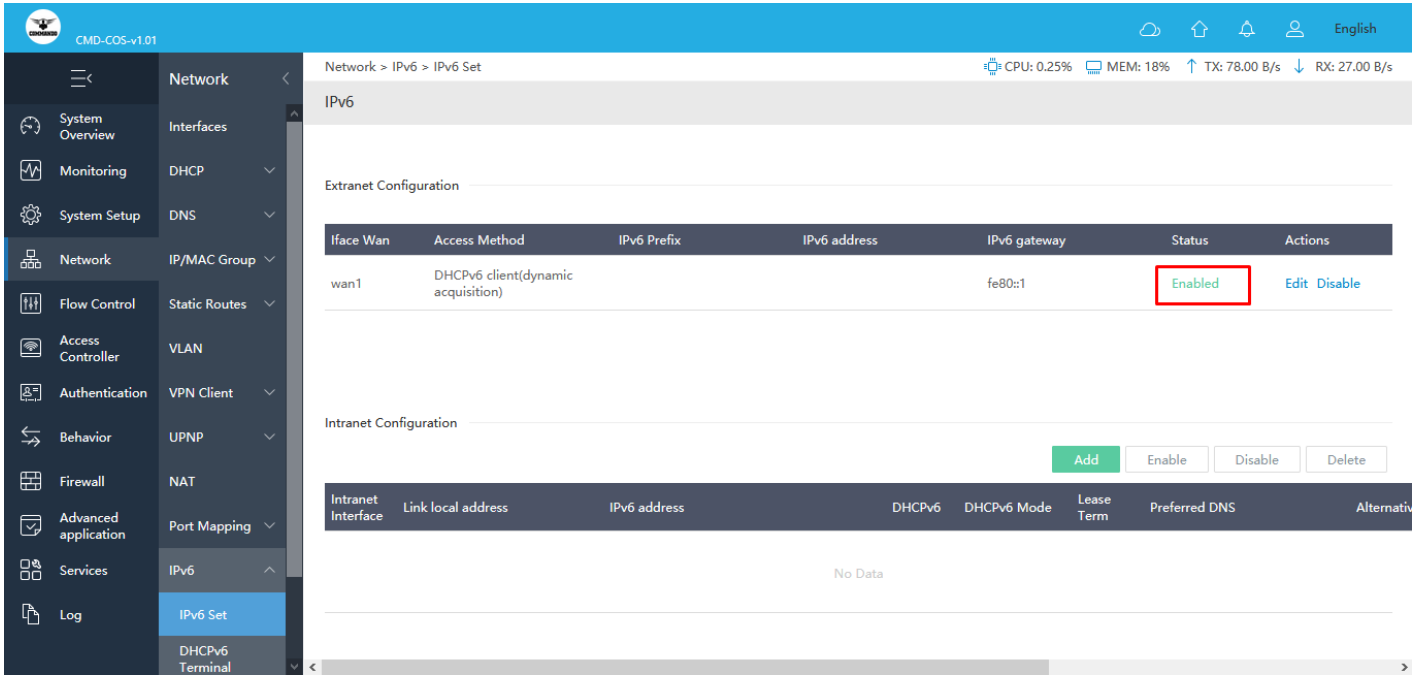
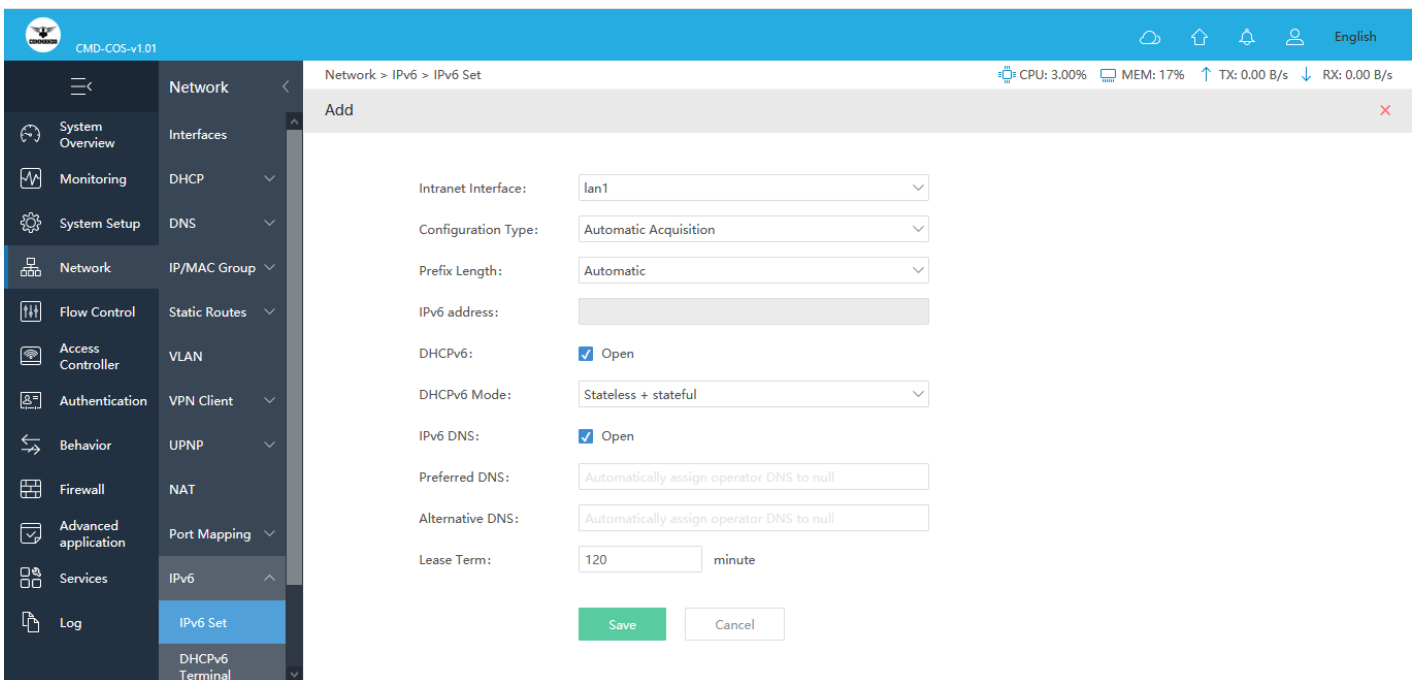


Fig 3.11.2 Add IPv6 Page

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



**Fig 3.11.3 Enabling DHCPv6 Page**



**Fig 3.11.4 Automatic Acquisition of IPv6 address for LAN1 interface Page**



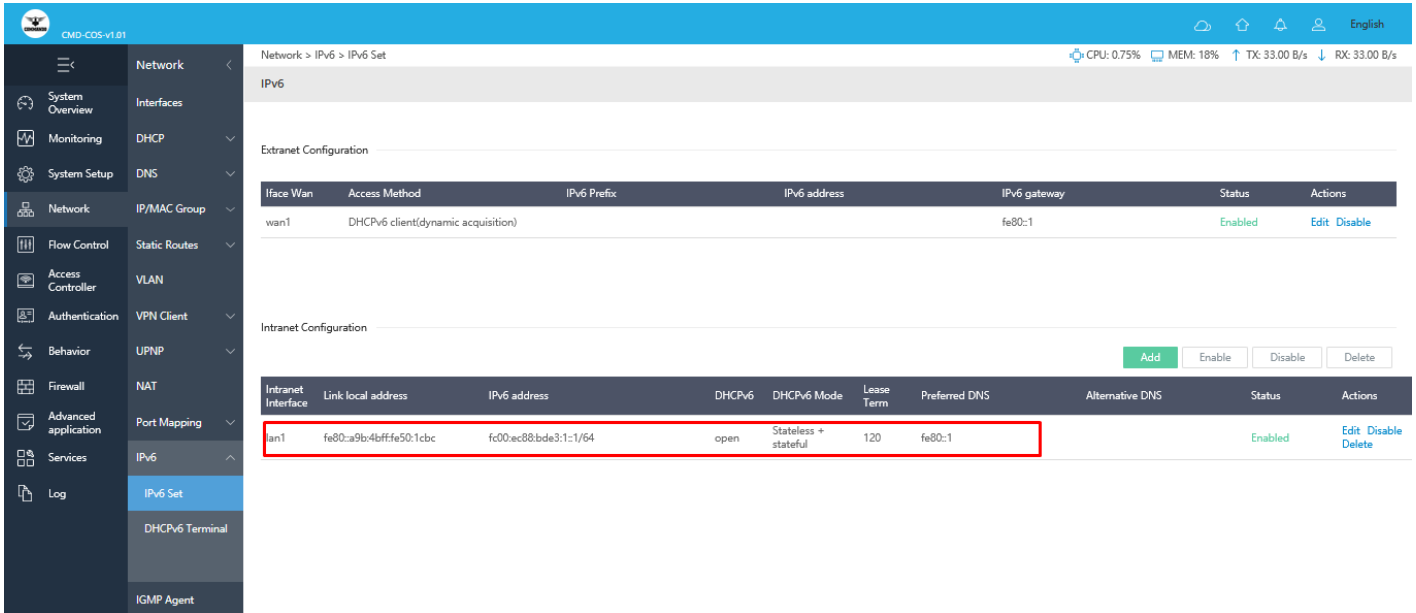


Fig 3.11.5 Automatic IPv6 address for LAN1 interface Page

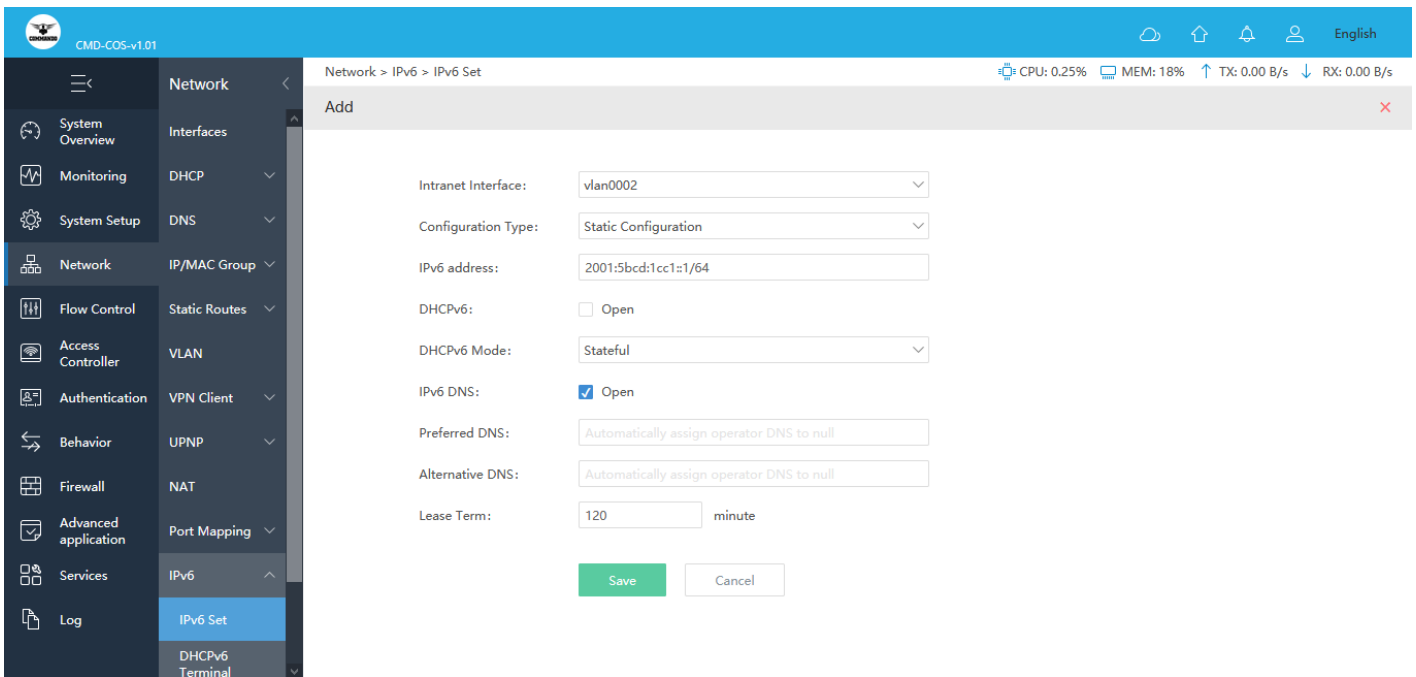
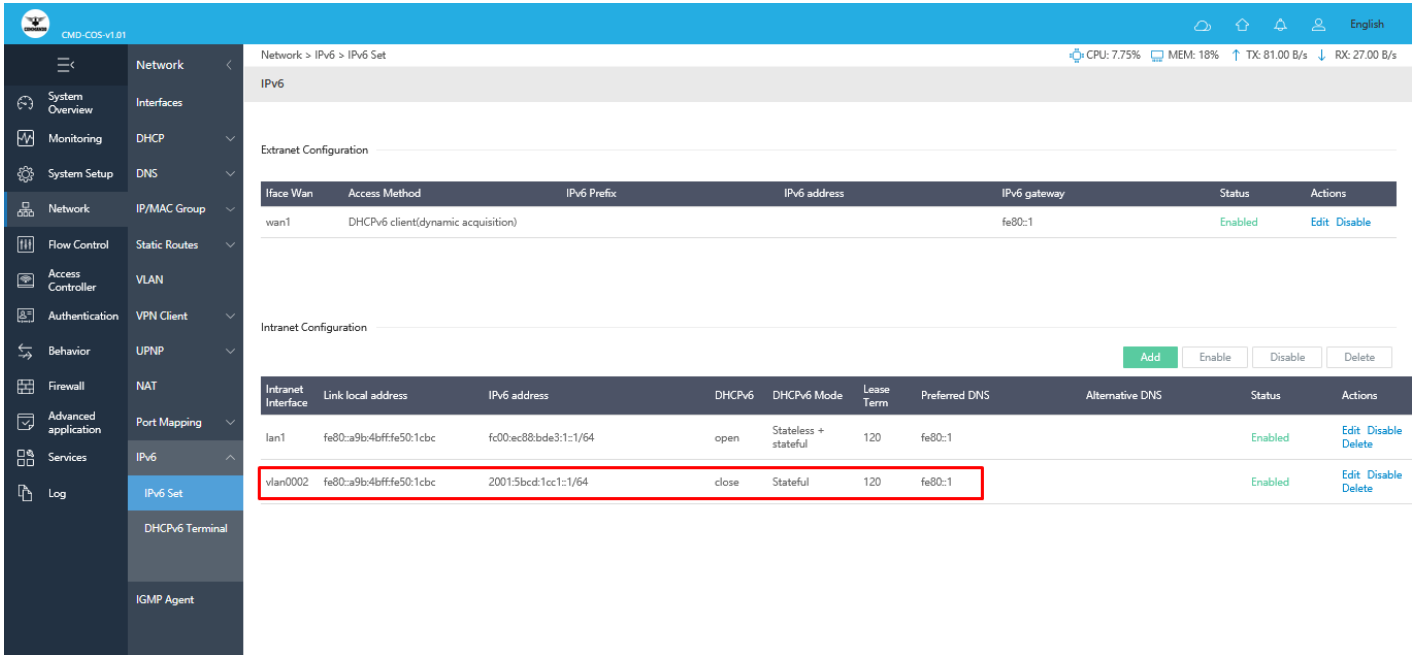


Fig 3.11.6 Manual IPv6 address for vlan0002 interface Page

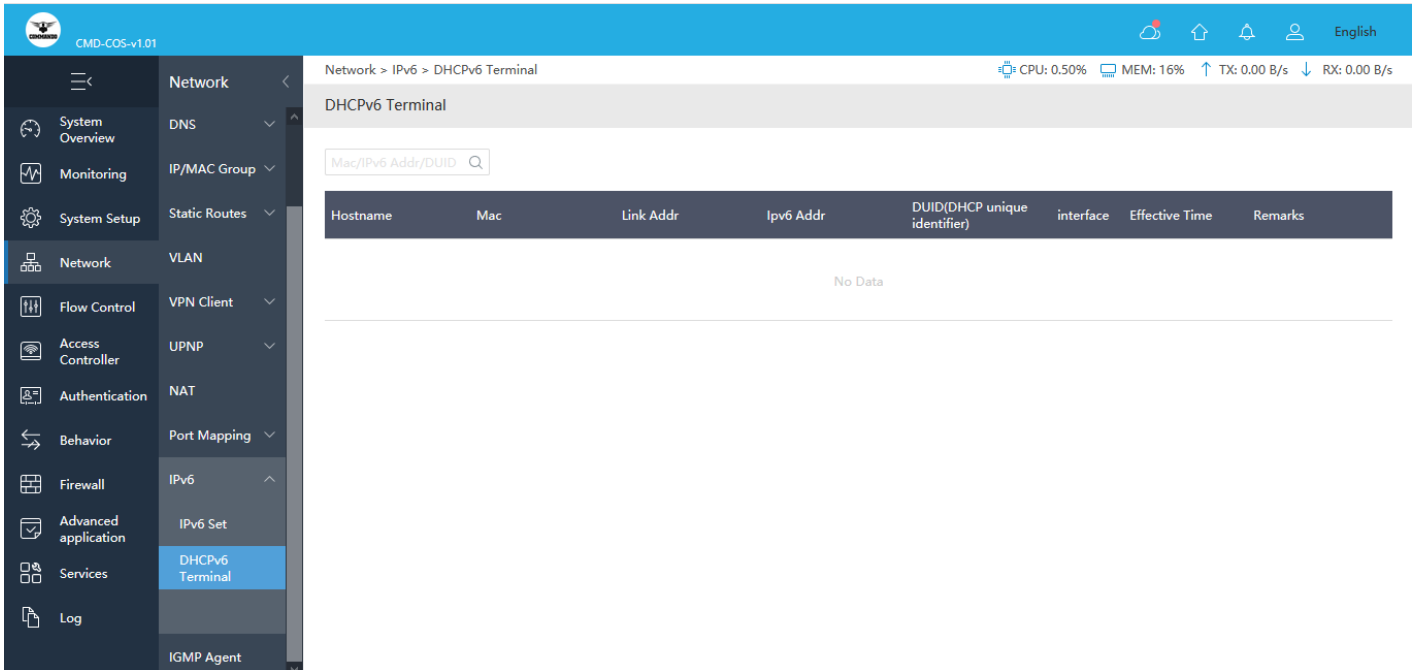


**Fig 3.11.7 Manual IPv6 address for vlan0002 interface Page**

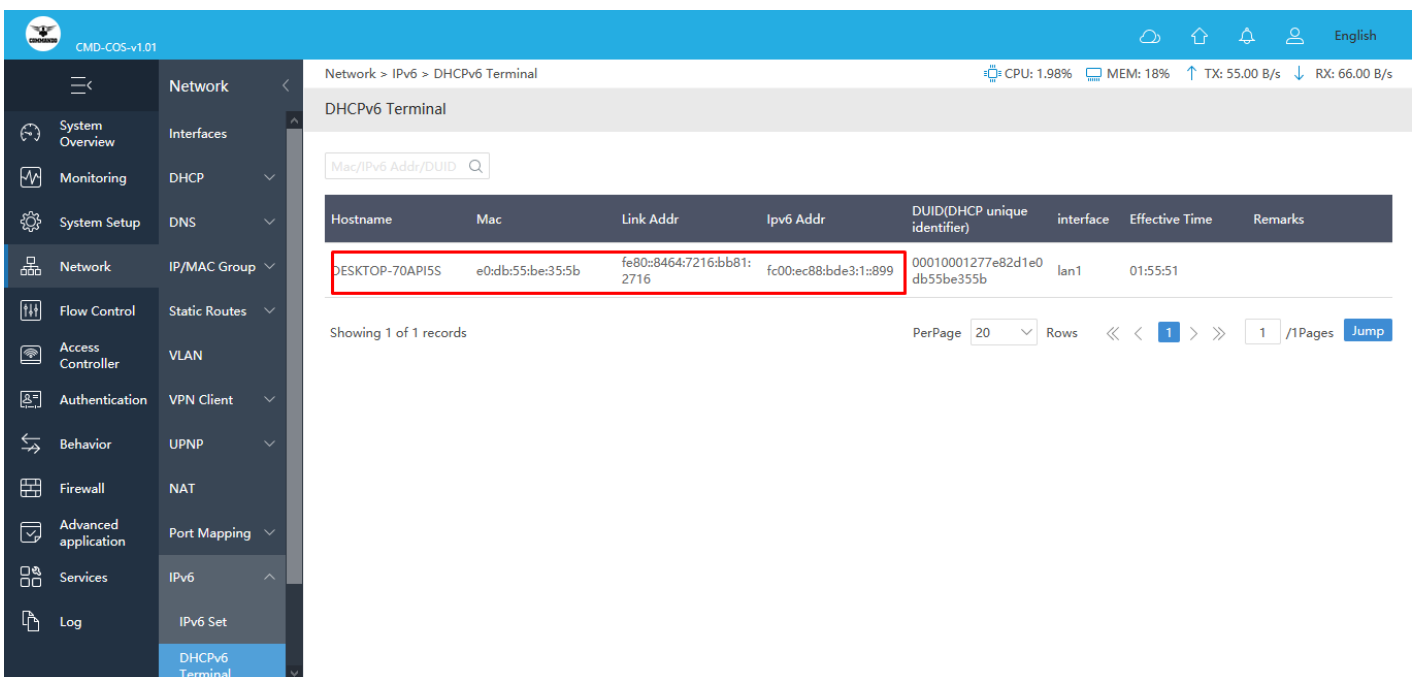
### DHCPv6 Terminal:

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 router exchanges IPv6 packets.

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

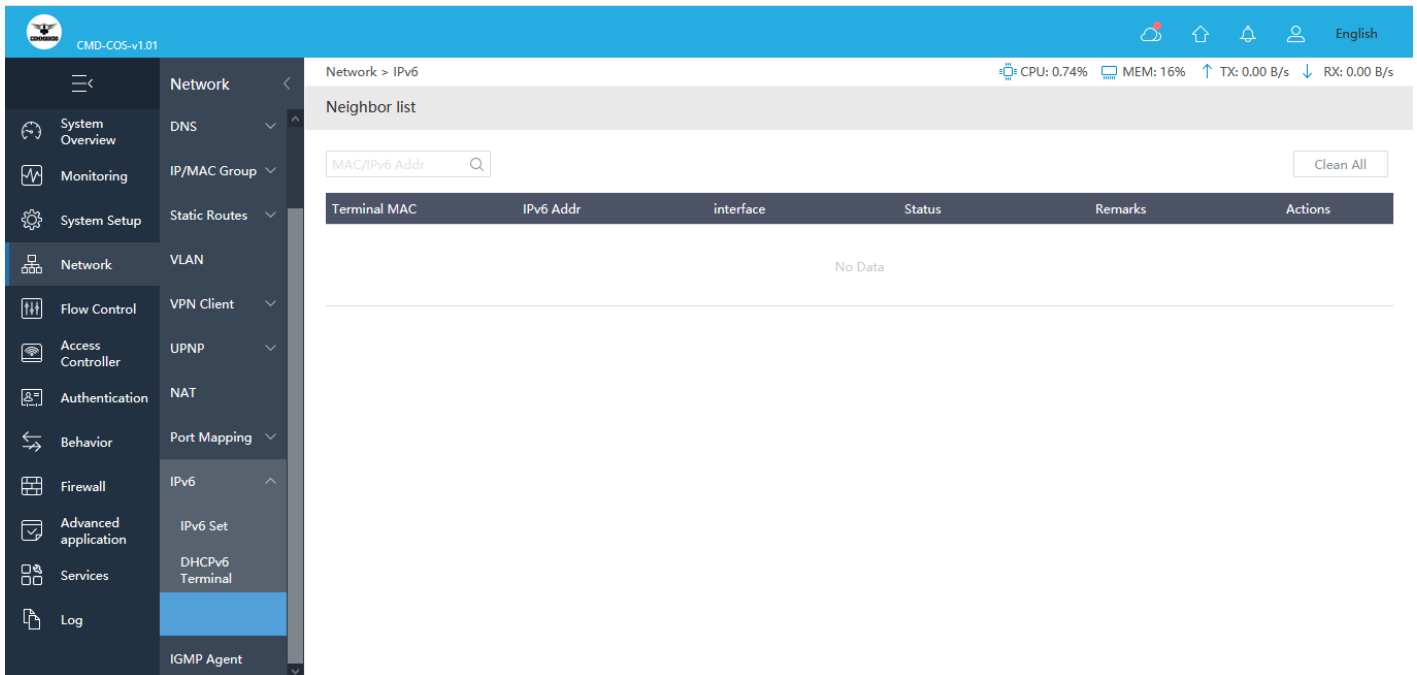


Fig 3.11.10 Default IPv6 Neighbor List Page

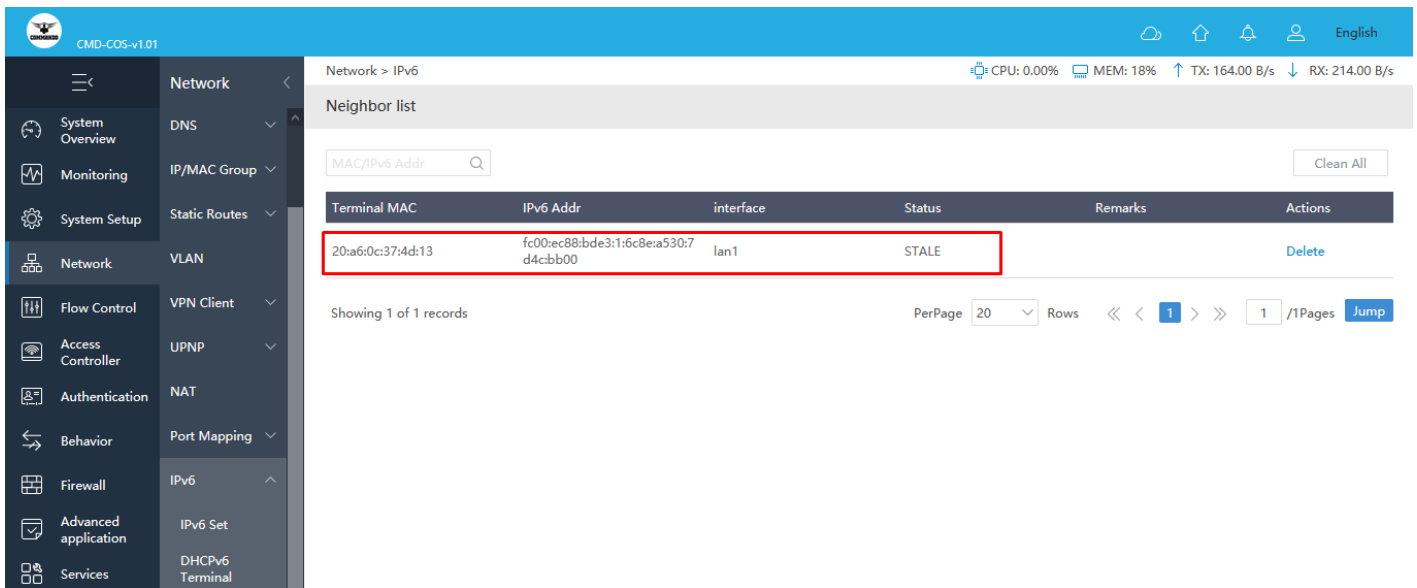
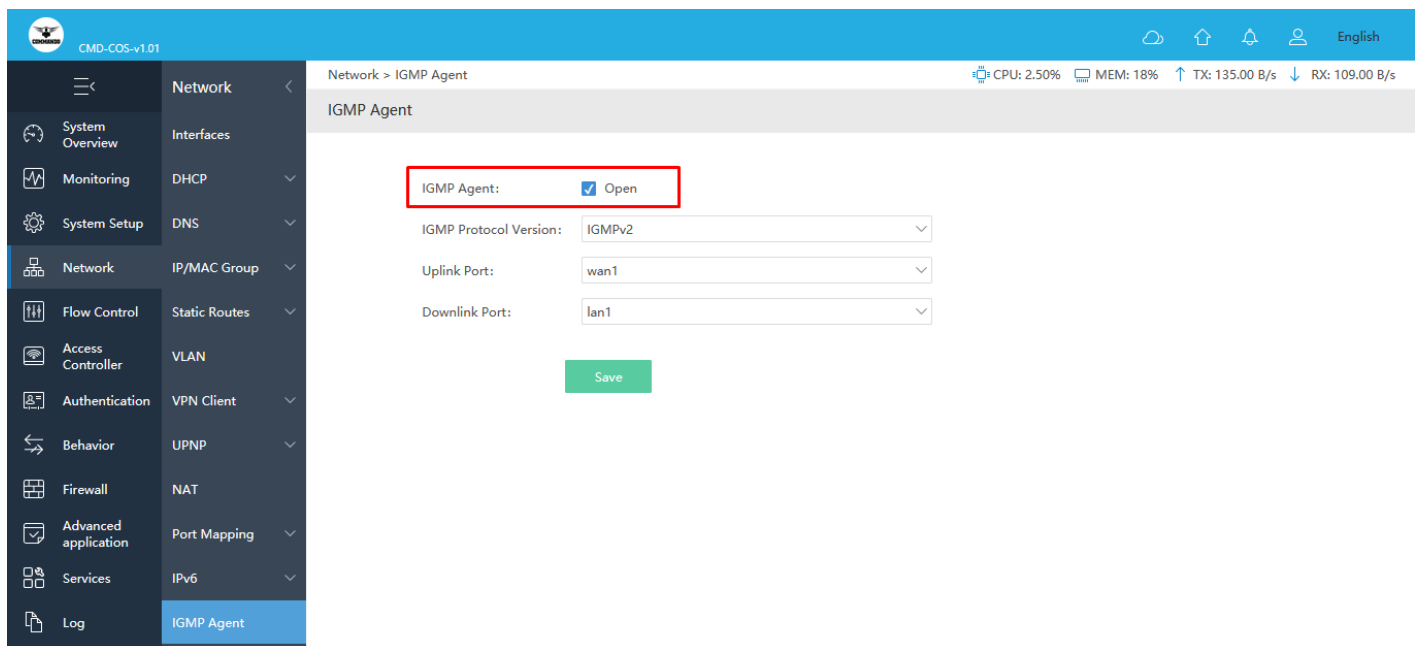


Fig 3.11.11 IPv6 Neighbor List Page

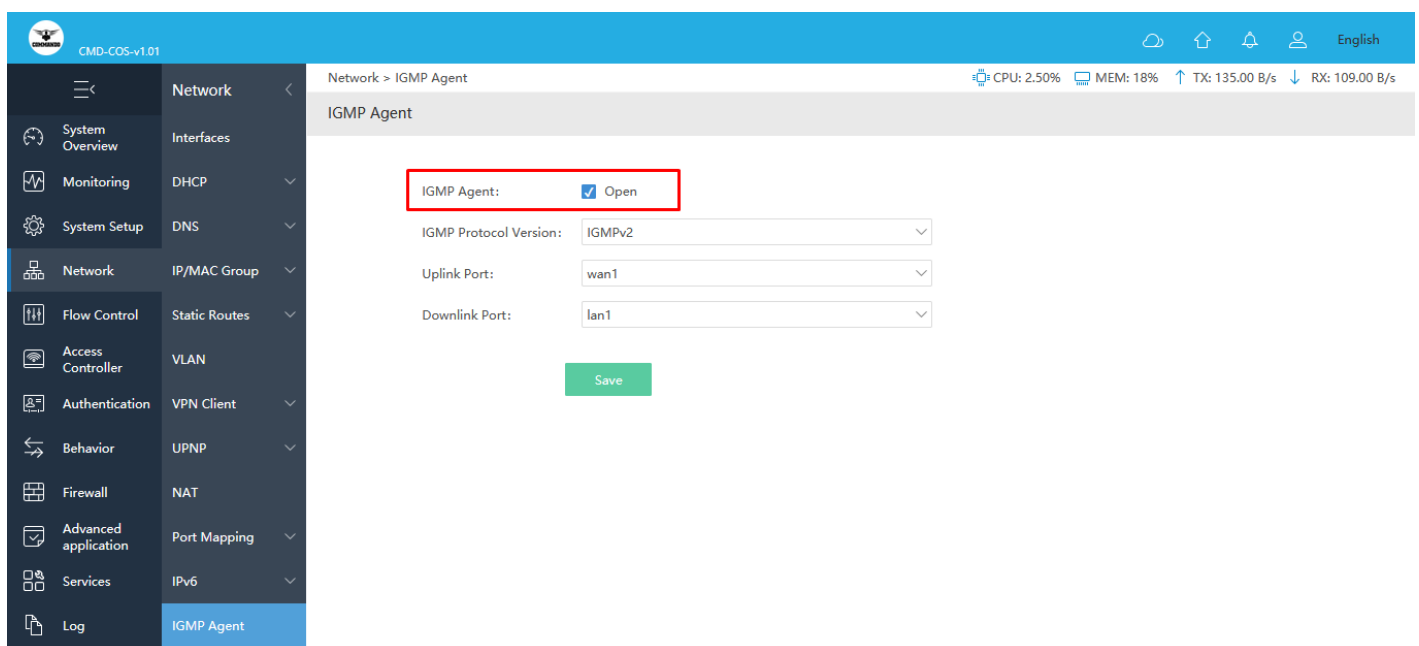
## 3.12 IGMP Agent

The Internet Group Management Protocol (IGMP) used by hosts and multicast routers 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**

## **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.



CMD-COS-v1.01



Flow Control



System  
Overview

Multi-WAN



Monitoring

Smart Flow  
Control



System Setup

IP/MAC Limiters

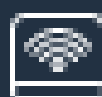


Network

Protocol Library



Flow Control



Access  
Controller



Authentication



Behavior

## **Fig 4.1 Flow control configuration page**

### **Failover and backup**

Multi-WAN routers 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 routers, 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 routers 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 router setup. But with multi-WAN routers, 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



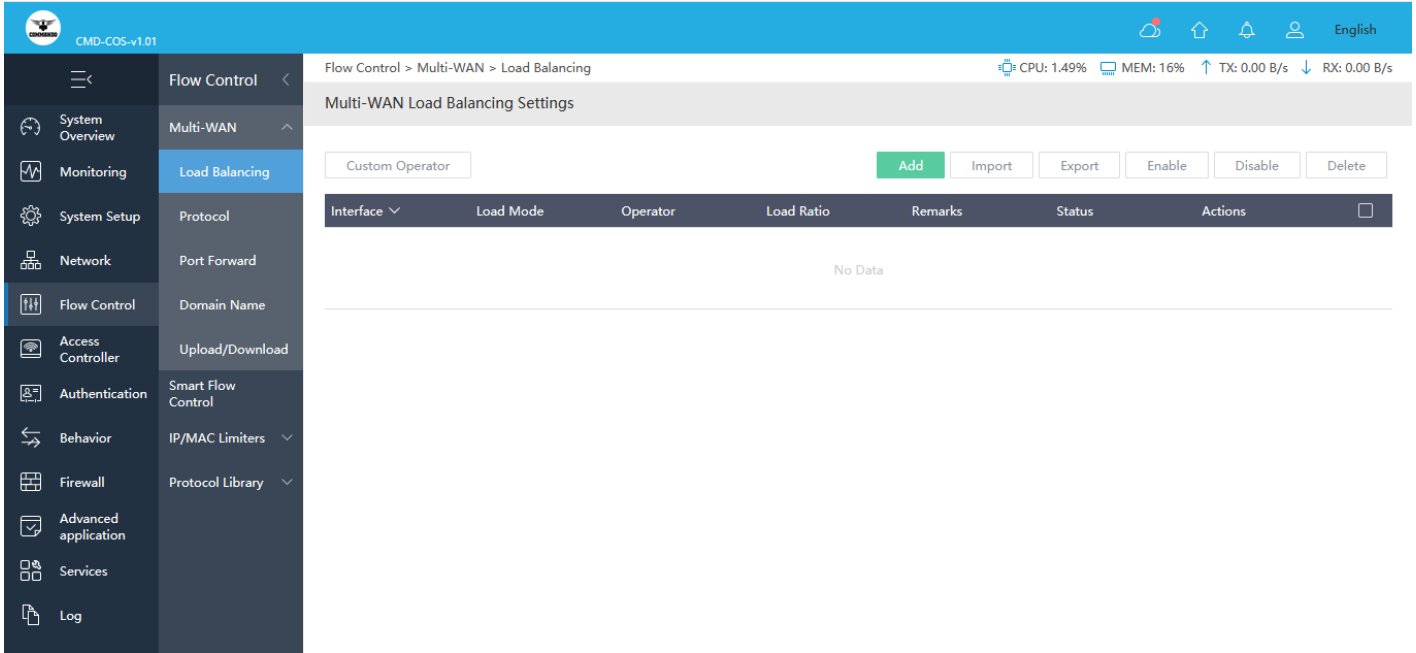
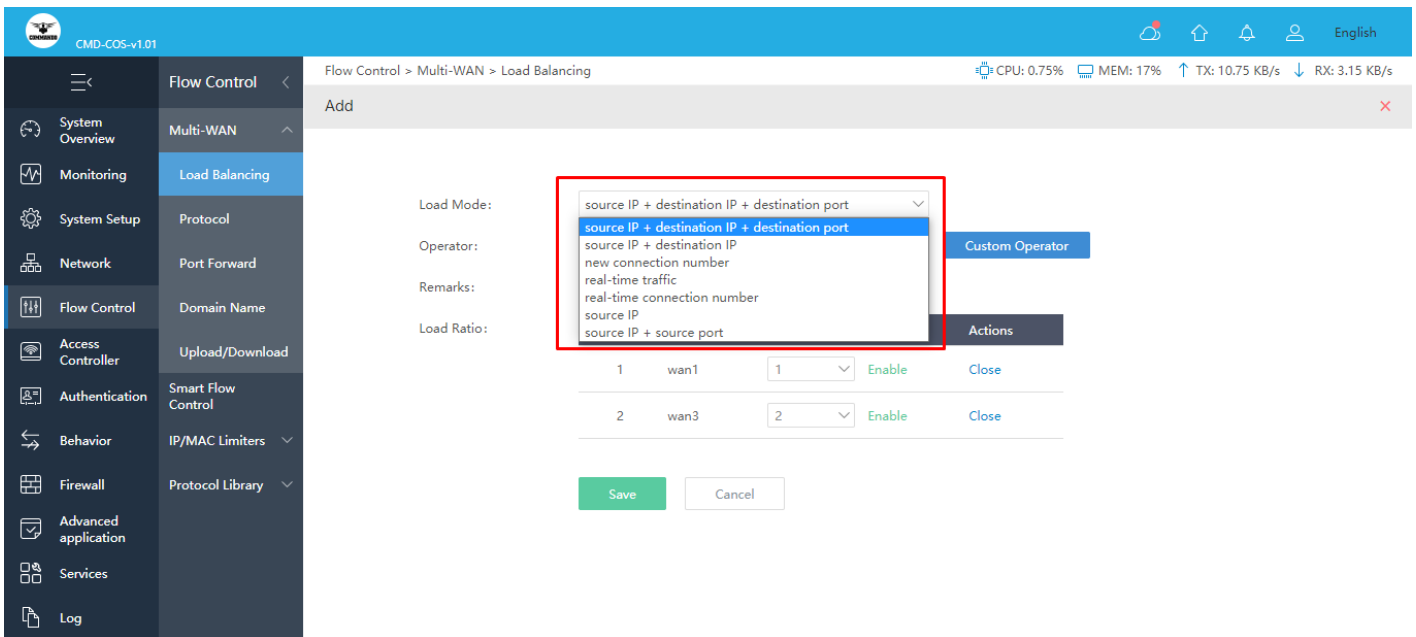
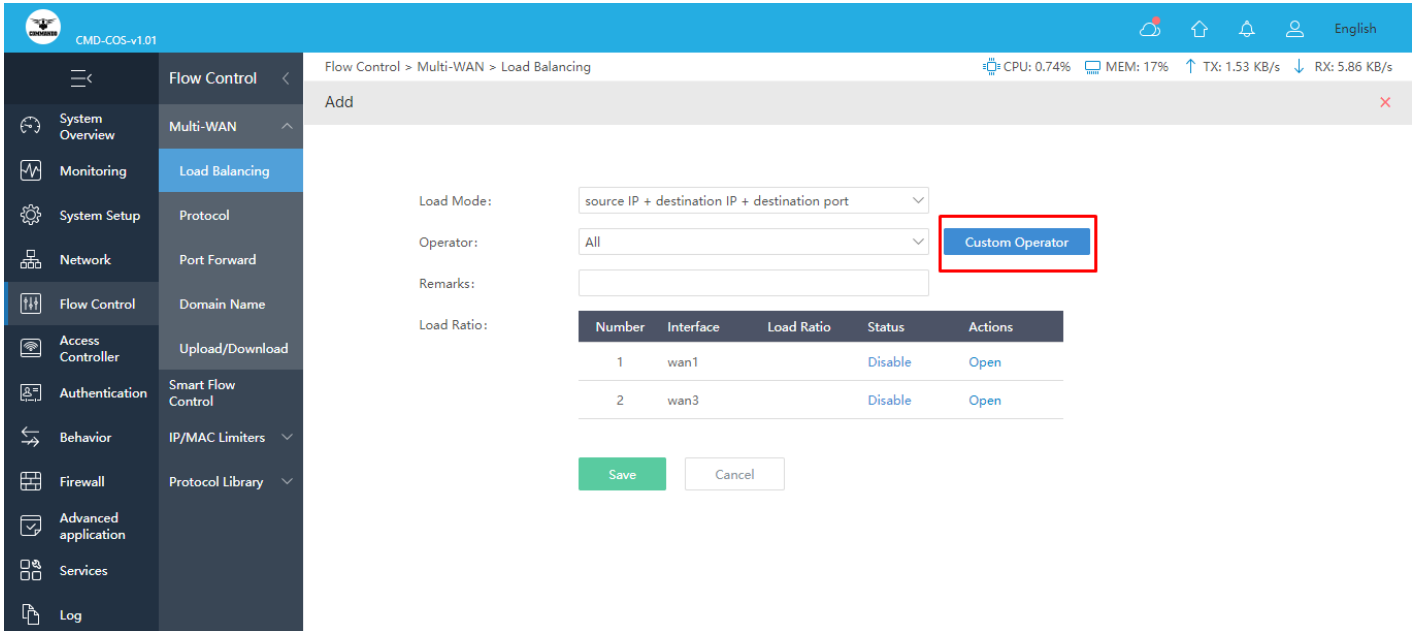
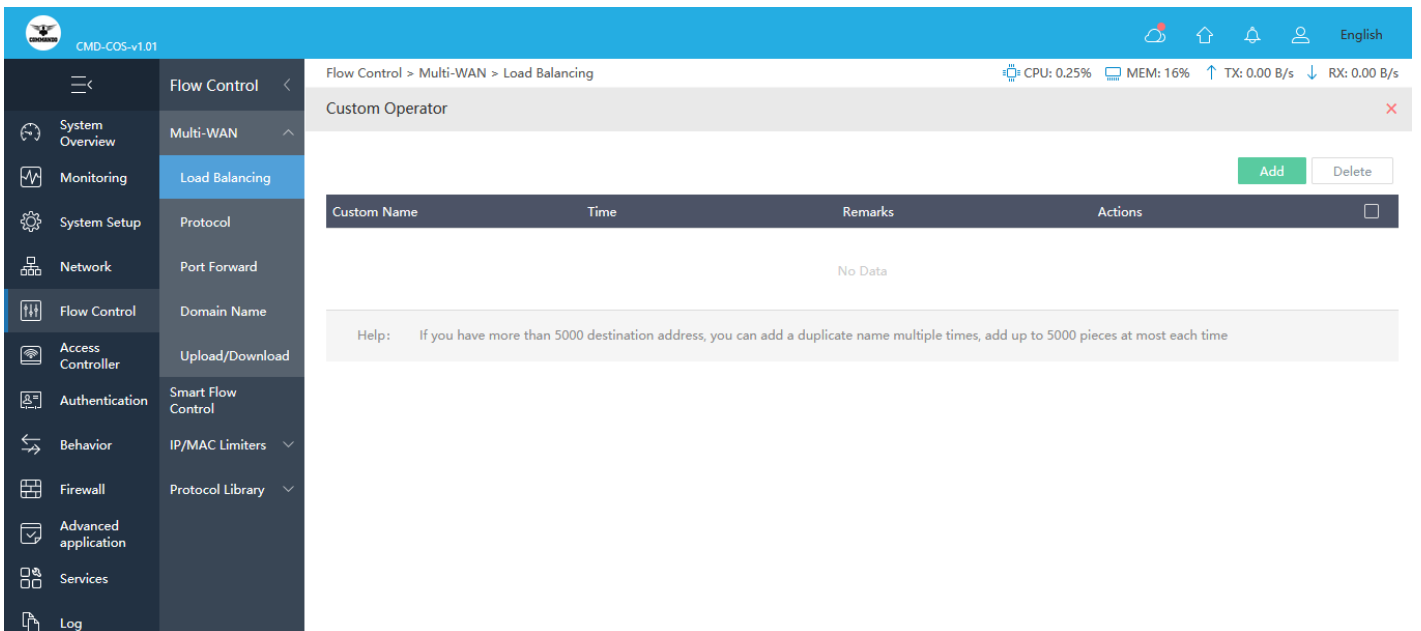


Fig 4.1.1 Default Multi-WAN Load Balancing Settings page

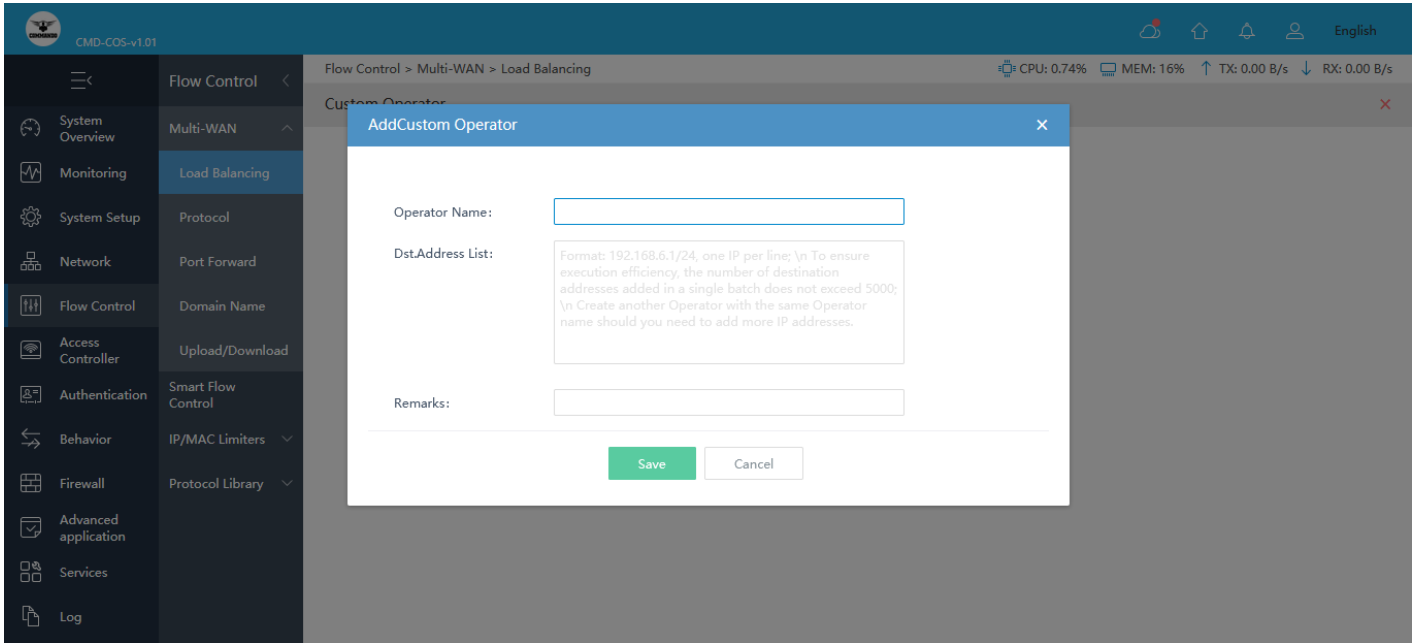




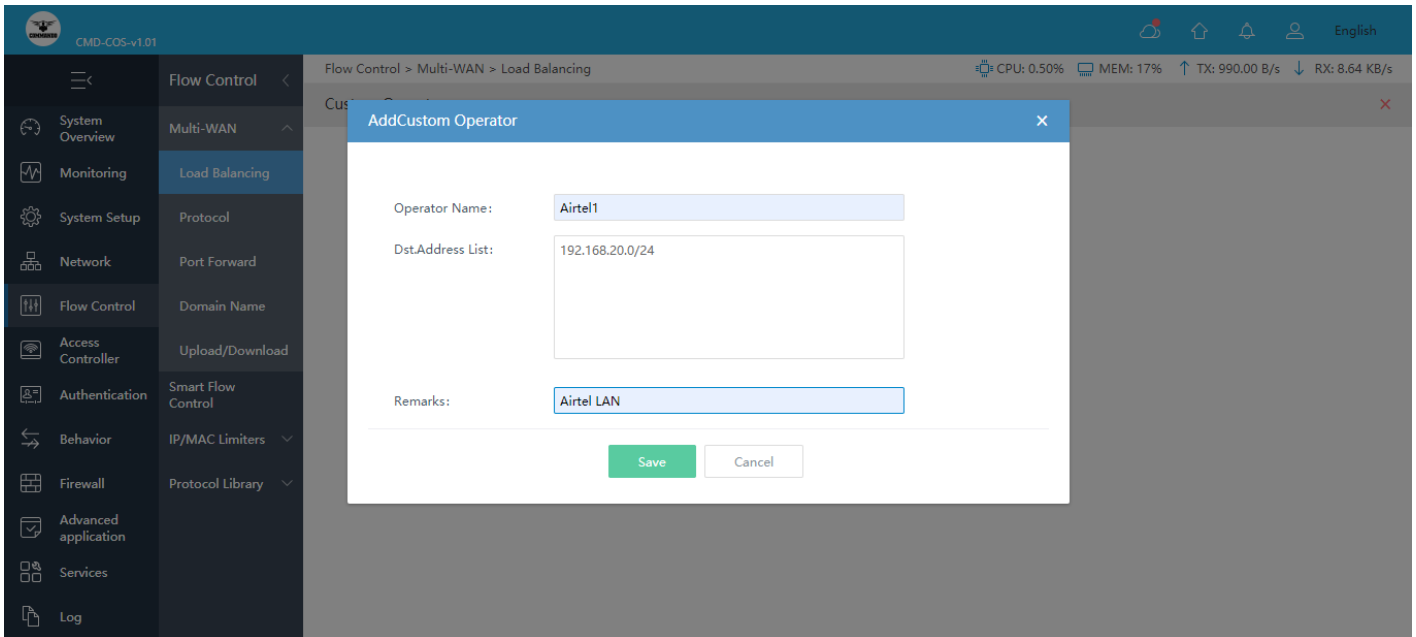
**Fig 4.1.2 Add Multi-WAN Load Balancing Settings page**



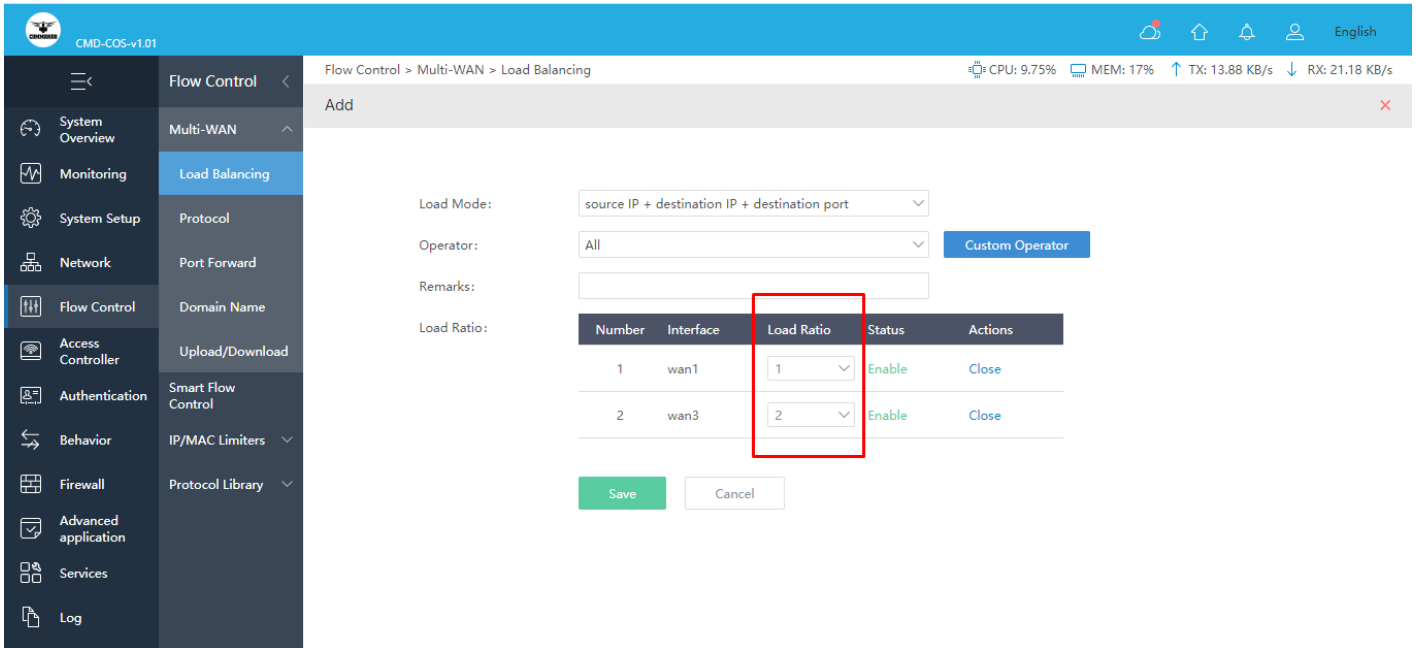
**Fig 4.1.3 Default Custom operator page**



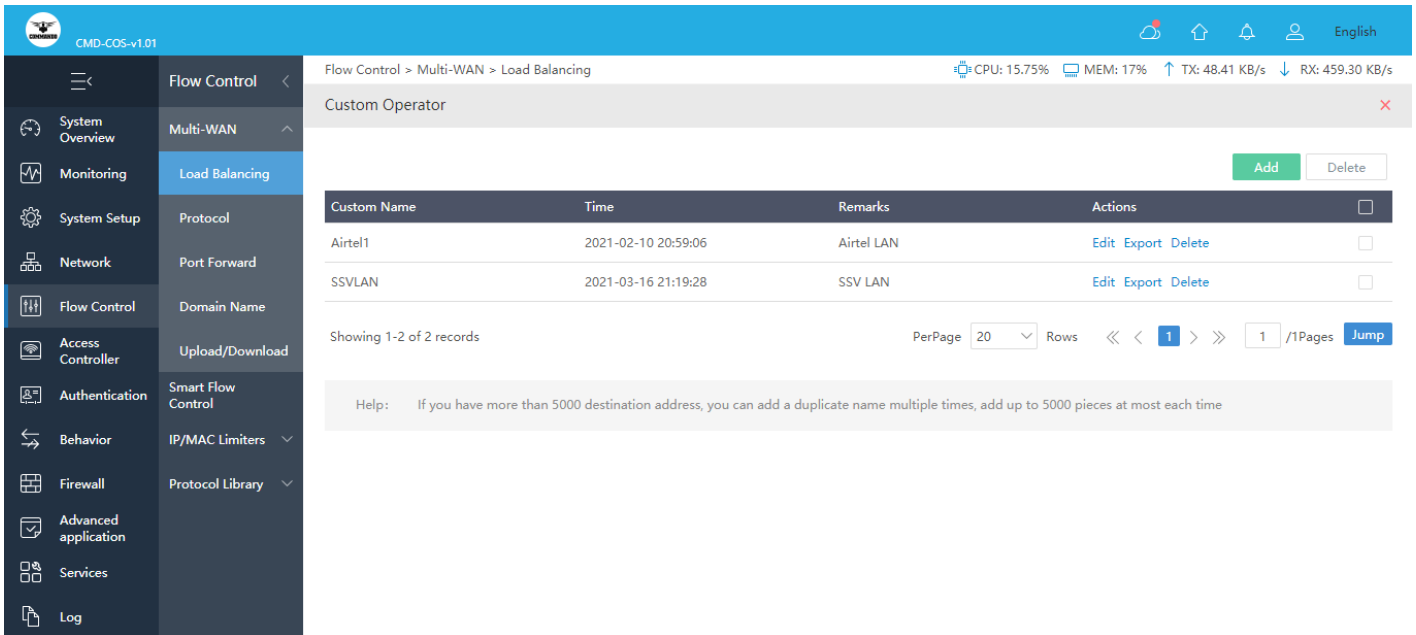
**Fig 4.1.4 Add Custom operator page**



**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

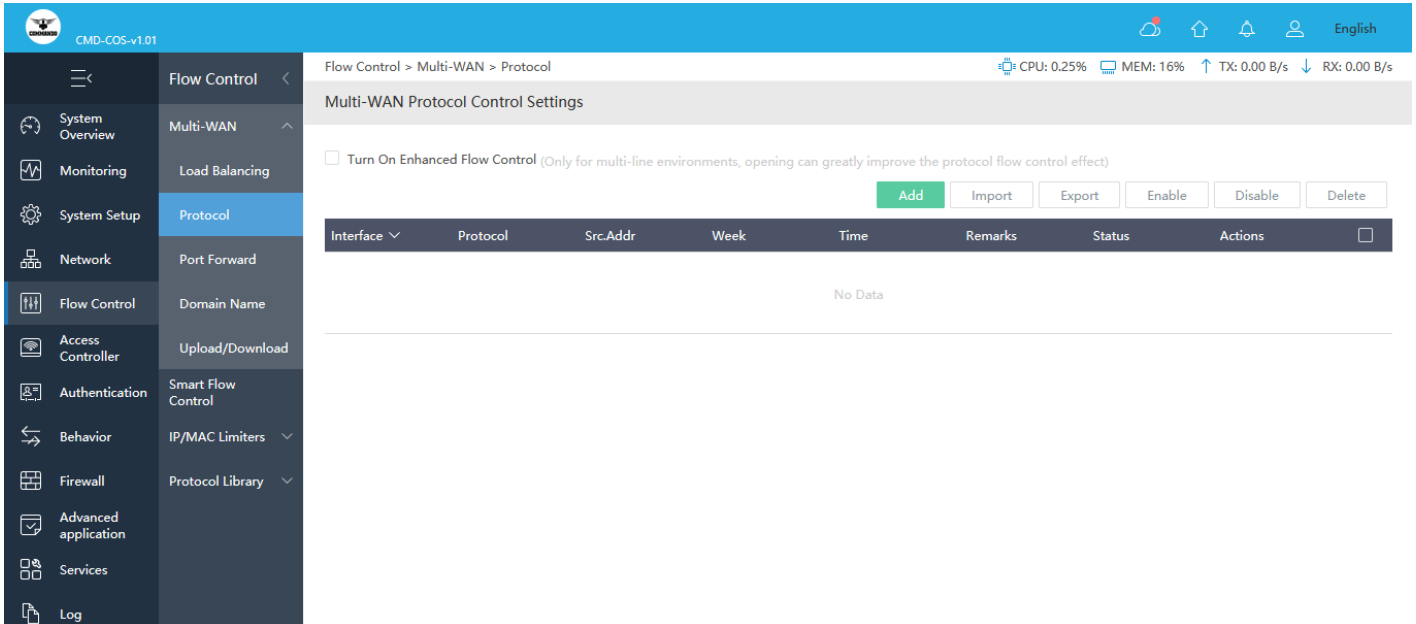


Fig 4.1.8 Default Multi-WAN Protocol Control Settings page

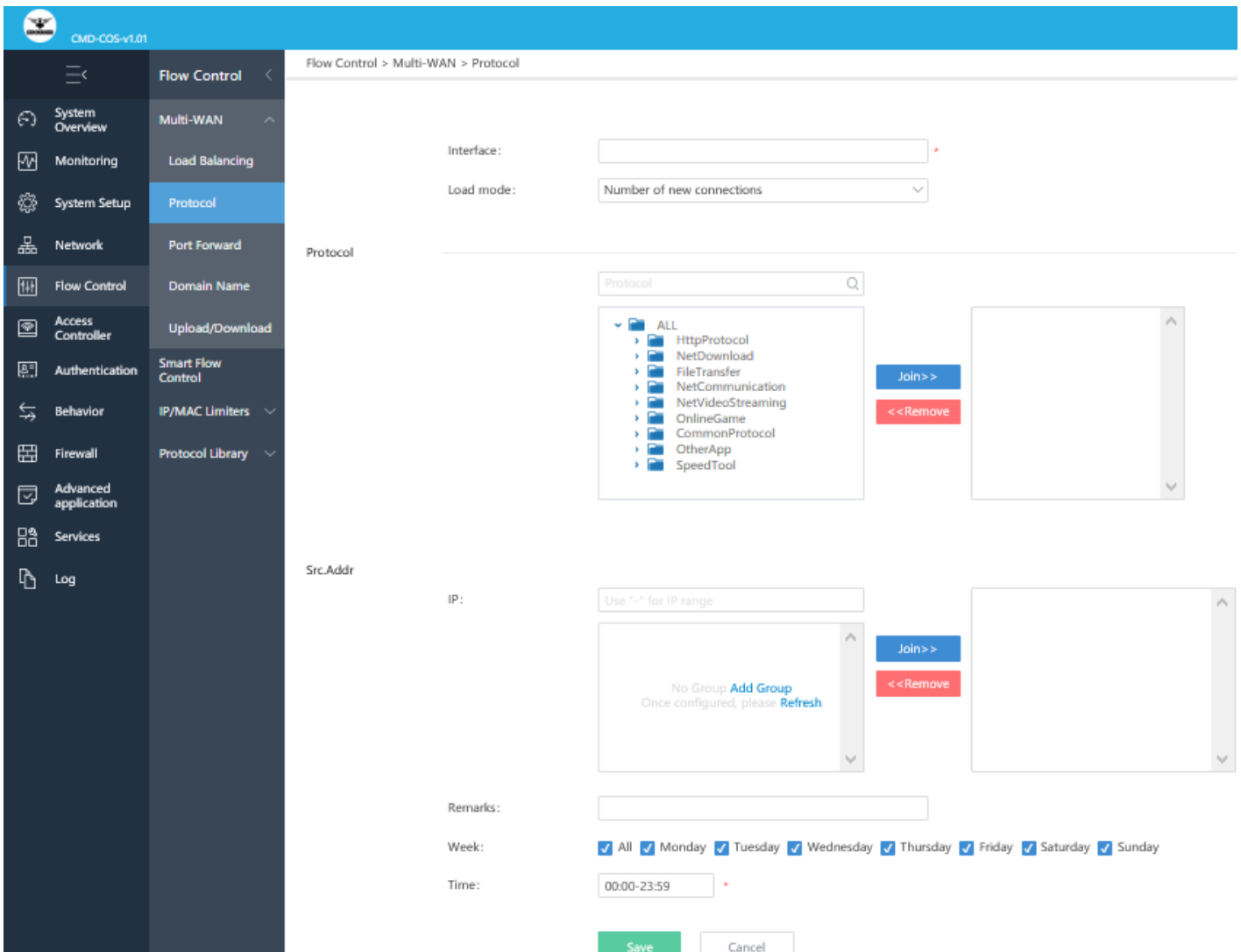
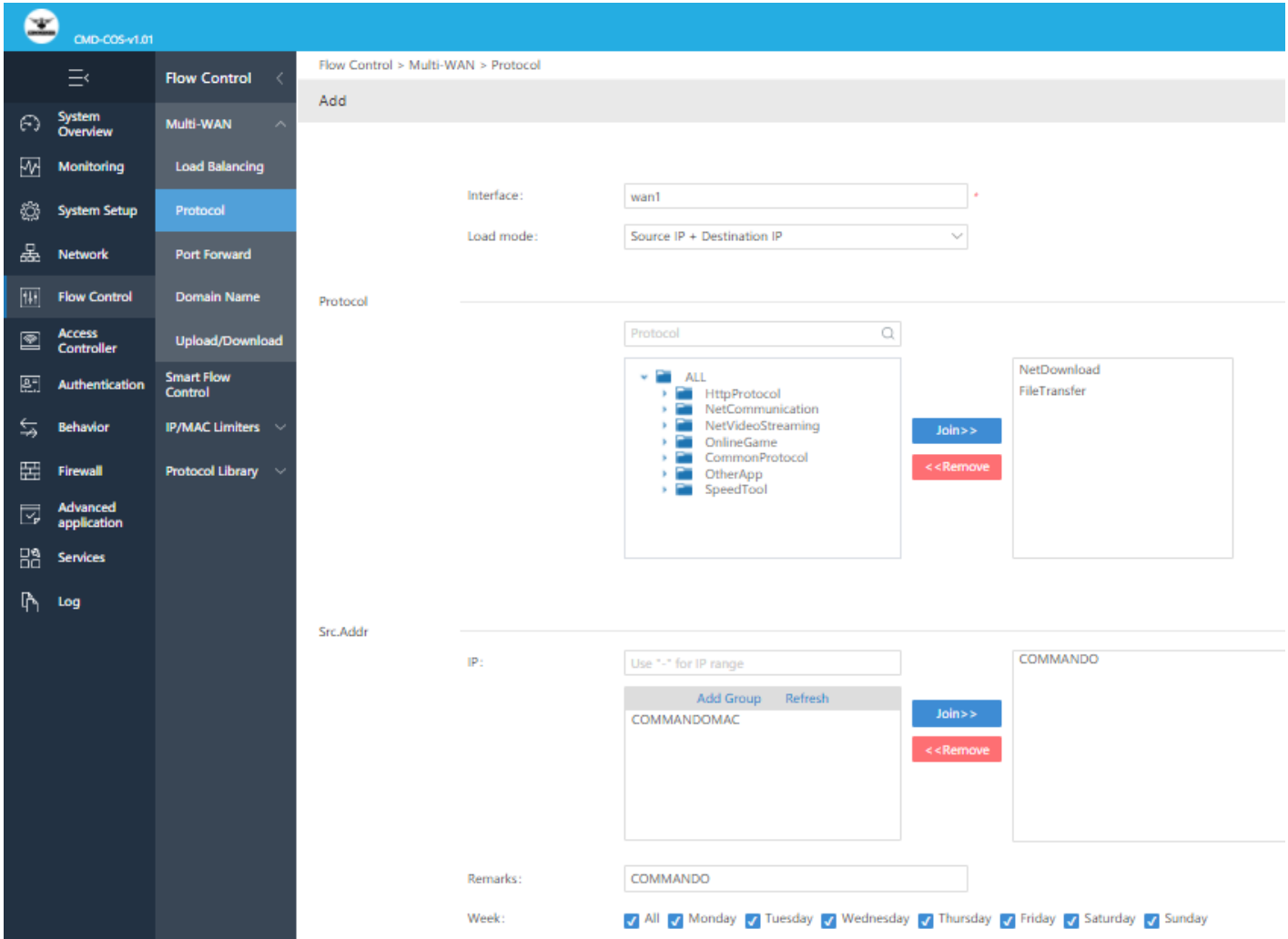
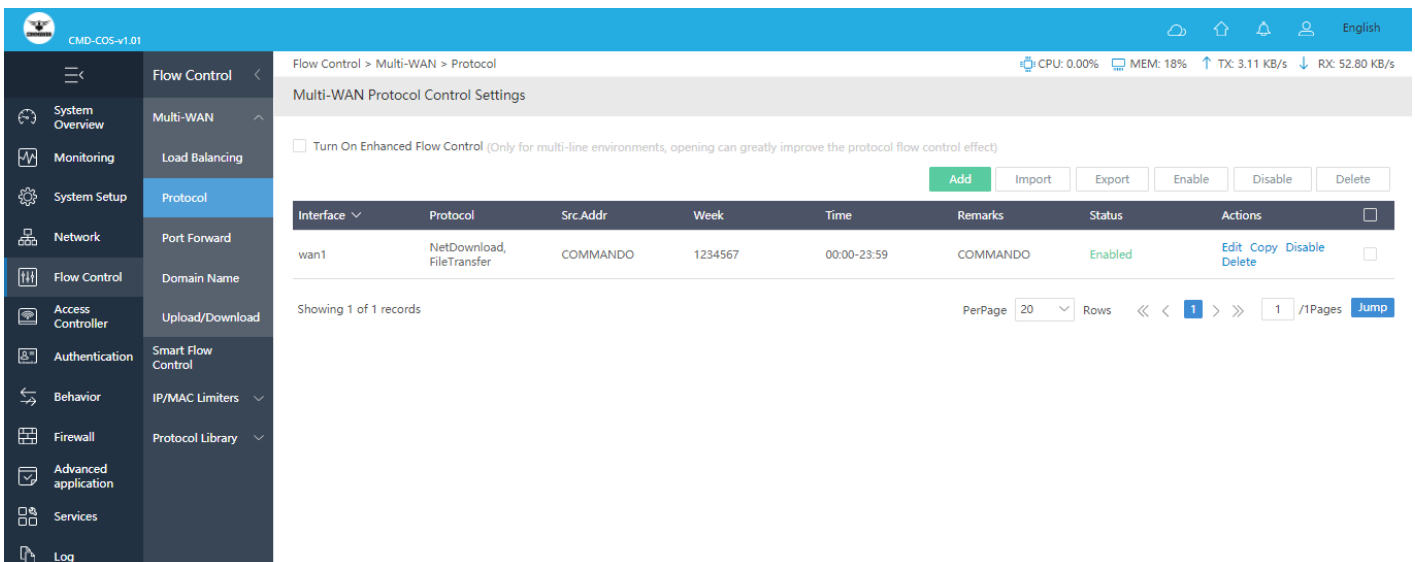


Fig 4.1.9 Add Multi-WAN Protocol Control Settings page



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



**Fig 4.1.11 Multi-WAN Protocol Control Settings page**

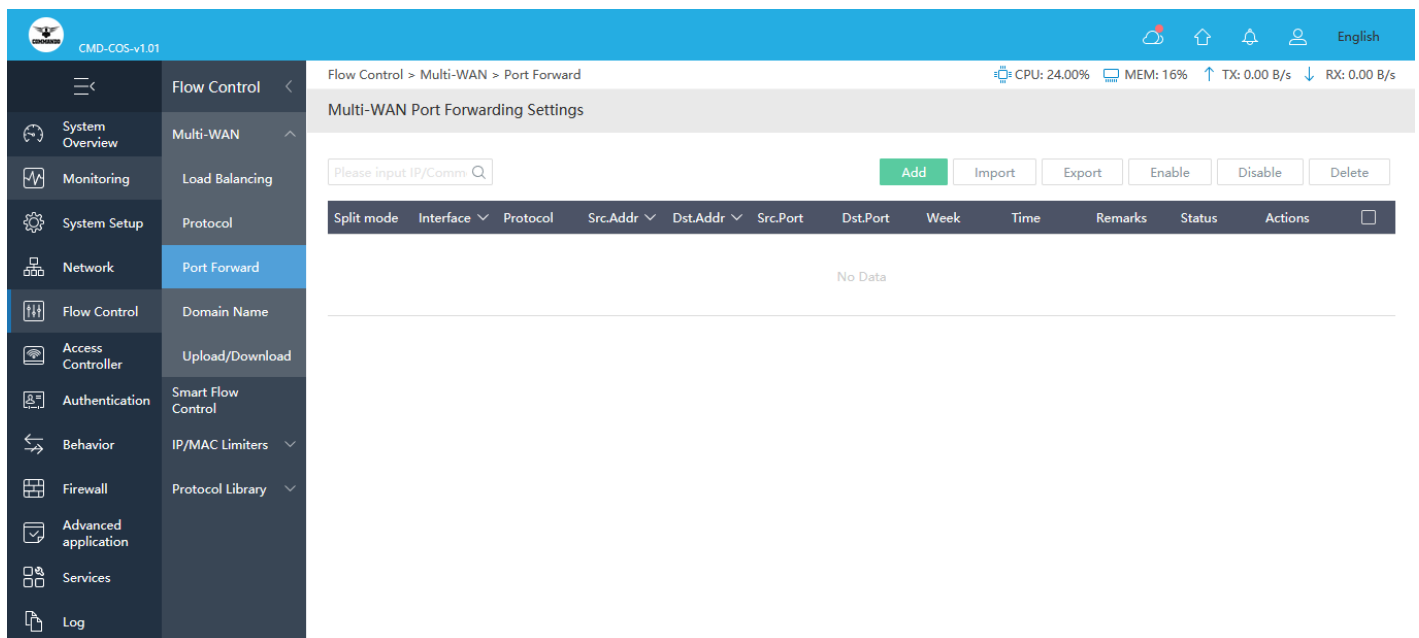
**Multi-WAN Port Forwarding Settings:**

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**

CMD-COS-v1.01

Flow Control > Multi-WAN > Port Forward

CPU: 1.24% MEM: 16% 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: Use \*.\* for IP range

No Group Add Group  
Once configured, please Refresh

Join->>

<<Remove

CMD-COS-v1.01

Flow Control > Multi-WAN > Port Forward

CPU: 0.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Dst.Addr

IP: Use \*.\* for IP range

No Group Add Group  
Once configured, please Refresh

Join->>

<<Remove

Src.Port: \*

Dst.Port: \*

Remarks: \*

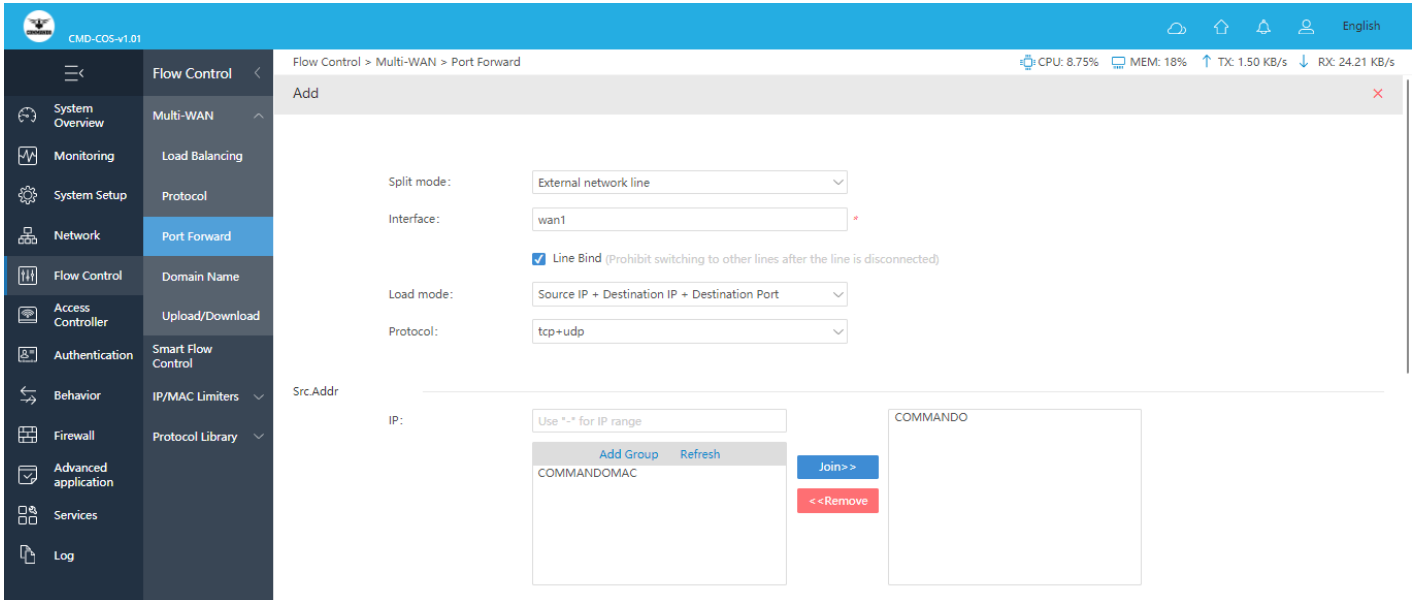
Week:  All  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Time: 00:00-23:59 \*

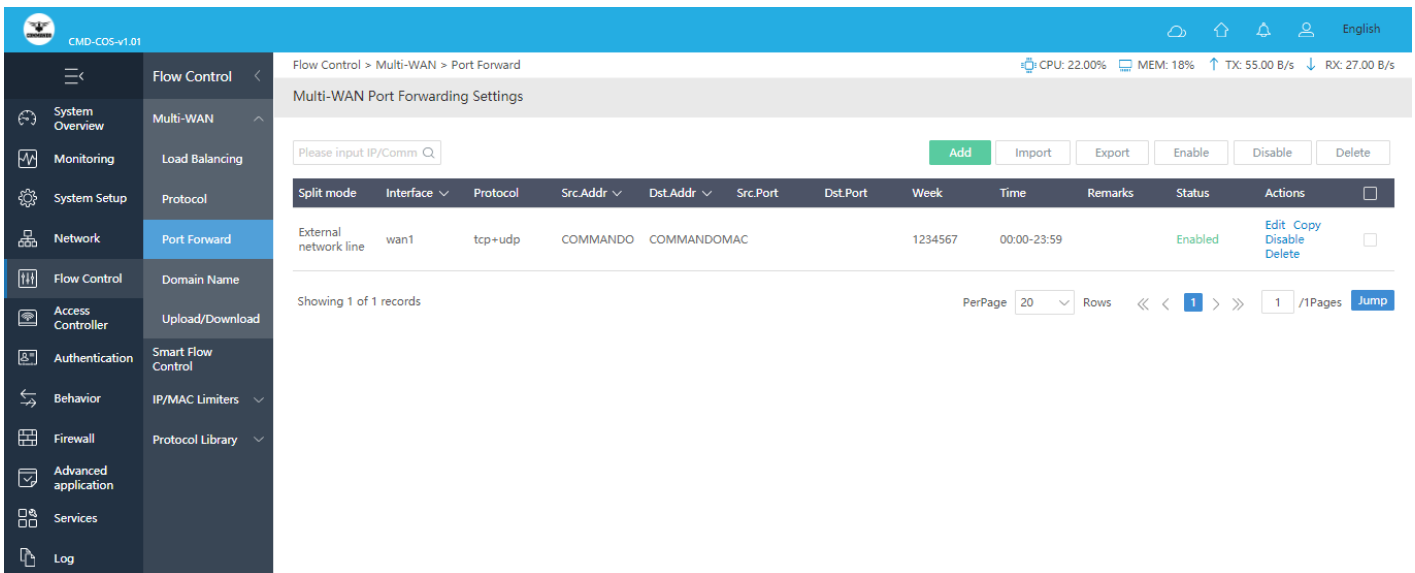
Save Cancel

Fig 4.1.13 Add Multi-WAN Port Forwarding Settings page





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

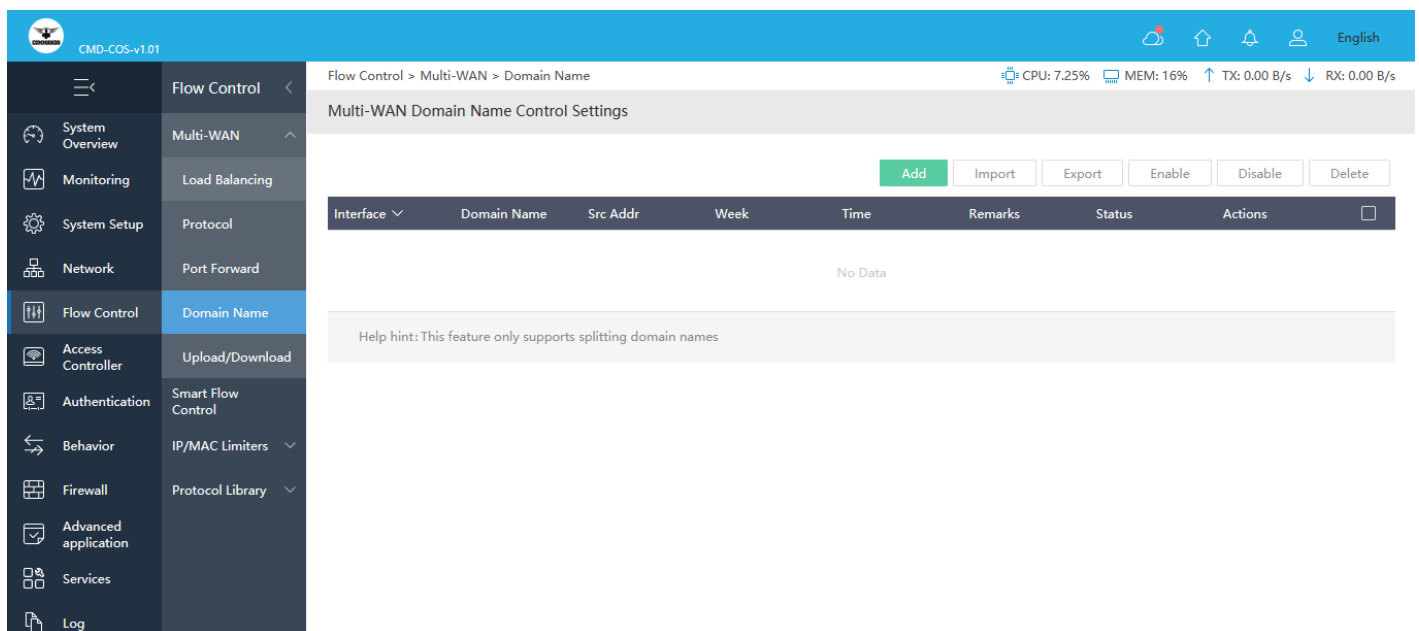


**Fig 4.1.15 Multi-WAN Port Forwarding Settings page**

**Multi-WAN Domain Name Control Settings:**

Basically, our LAN is connected over the Internet through a multi-WAN router, which will route local hosts over WAN1 to WAN4 depending on line overflow/fail and load setting you provided to router. 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 > Multi-WAN > Domain Name



**Fig 4.1.16 Default Multi-WAN Domain Name Control Settings page**

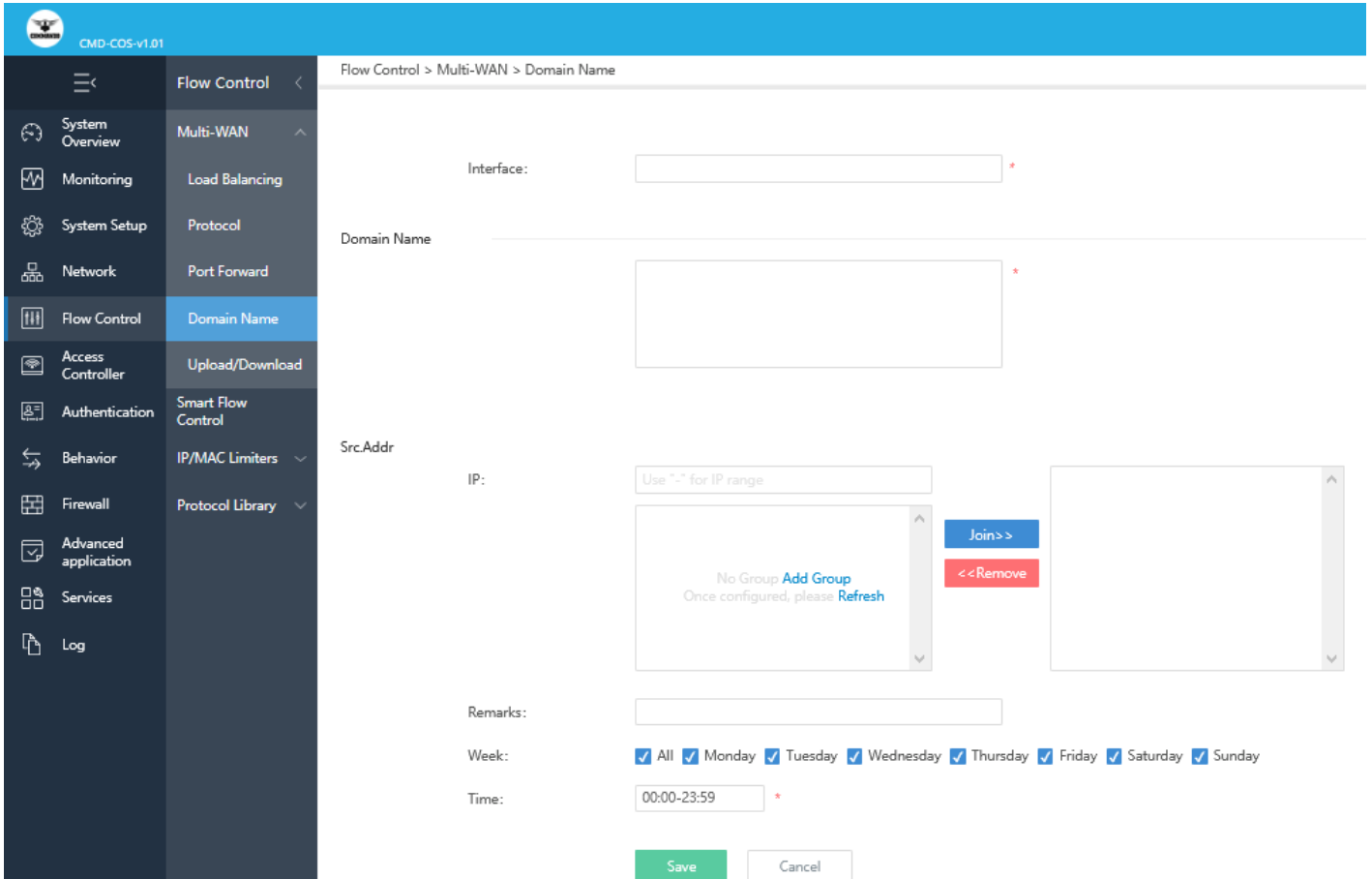


Fig 4.1.17 Add Multi-WAN Domain Name Control Settings page

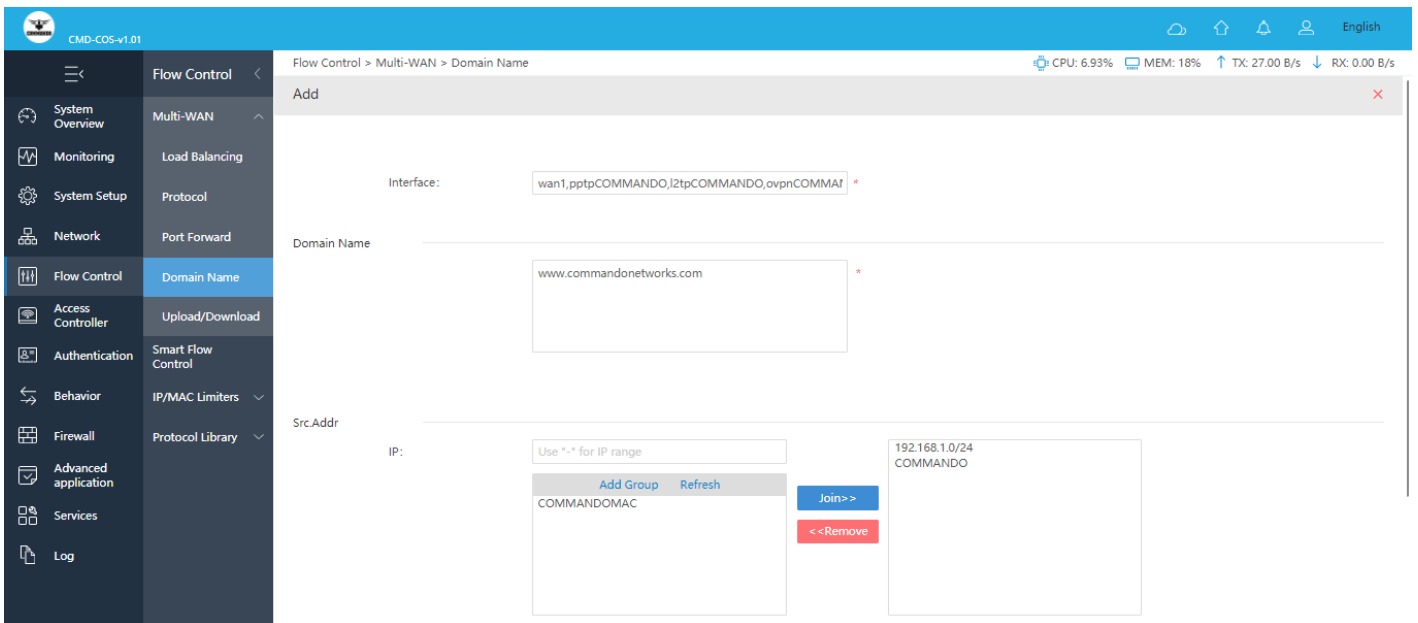
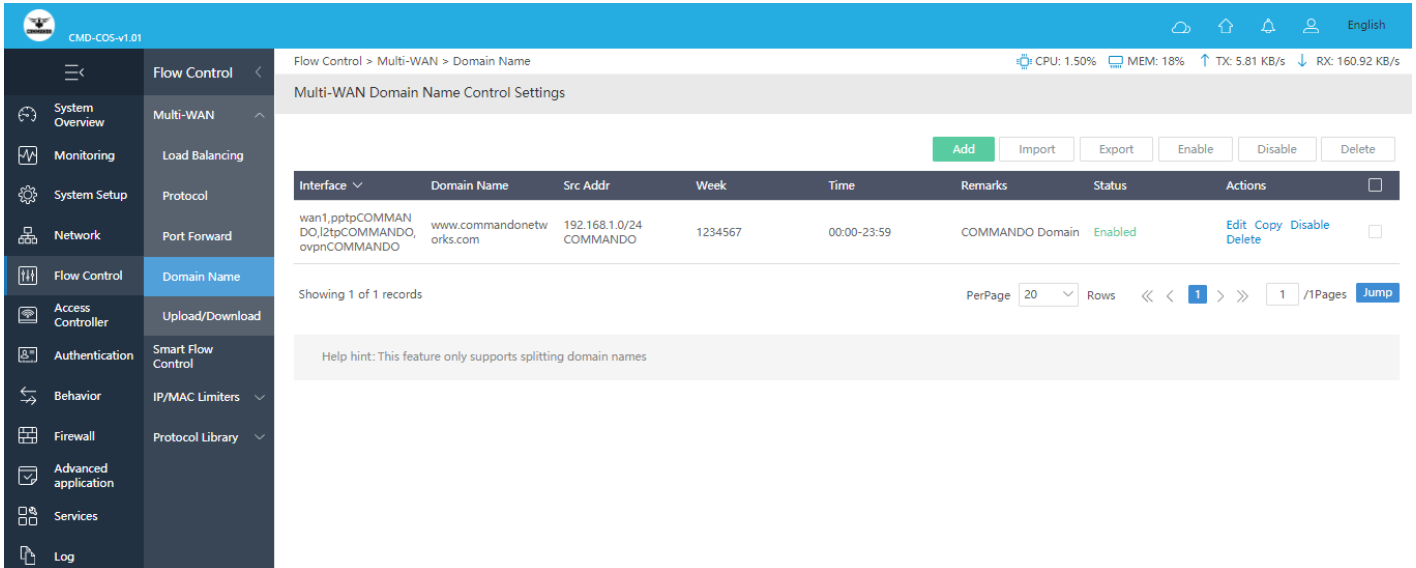


Fig 4.1.18 Details of Multi-WAN Domain Name Control Settings page



**Fig 4.1.19 Multi-WAN Domain Name Control Settings page**

### 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

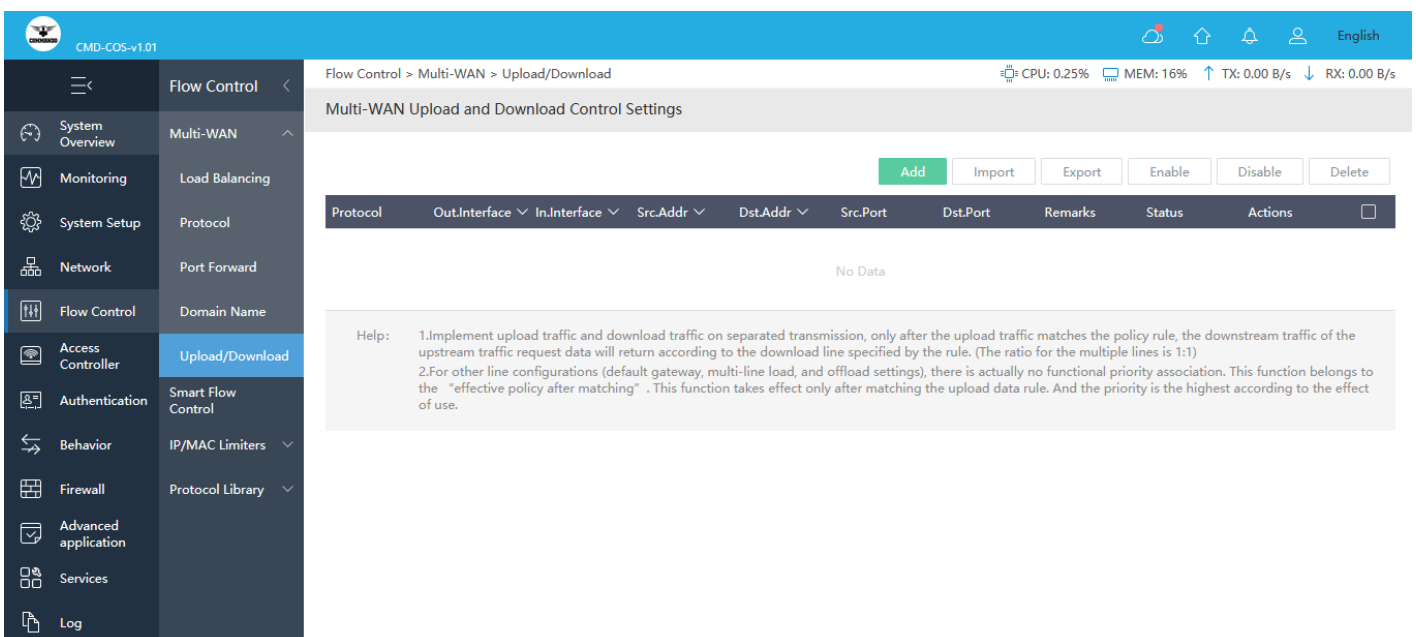


Fig 4.1.20 Multi-WAN Upload and Download Control Settings page

The screenshot shows the 'Multi-WAN > Upload/Download' configuration page. The left sidebar contains a navigation menu with categories like System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Flow Control' section is expanded to show 'Upload/Download' as the active option.

The main configuration area is titled 'Flow Control > Multi-WAN > Upload/Download'. It includes the following fields and controls:

- Protocol:** A dropdown menu currently set to 'any'.
- Out.Interface:** An empty text input field with a red asterisk indicating it is required.
- In.Interface:** An empty text input field with a red asterisk indicating it is required.
- Src.Addr:** A section for source address configuration. It features an 'IP:' input field with a placeholder 'Use "\*" for IP range'. Below it is a list area showing 'No Group' with an 'Add Group' link and a note 'Once configured, please Refresh'. To the right of the list are 'Join >>' and '<< Remove' buttons.
- Dst.Addr:** A section for destination address configuration, identical in structure to the Src.Addr section.
- Src.Port:** A disabled text input field.
- Dst.Port:** A disabled text input field.
- Remarks:** An empty text input field.

At the bottom of the page, there are 'Save' and 'Cancel' buttons.

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

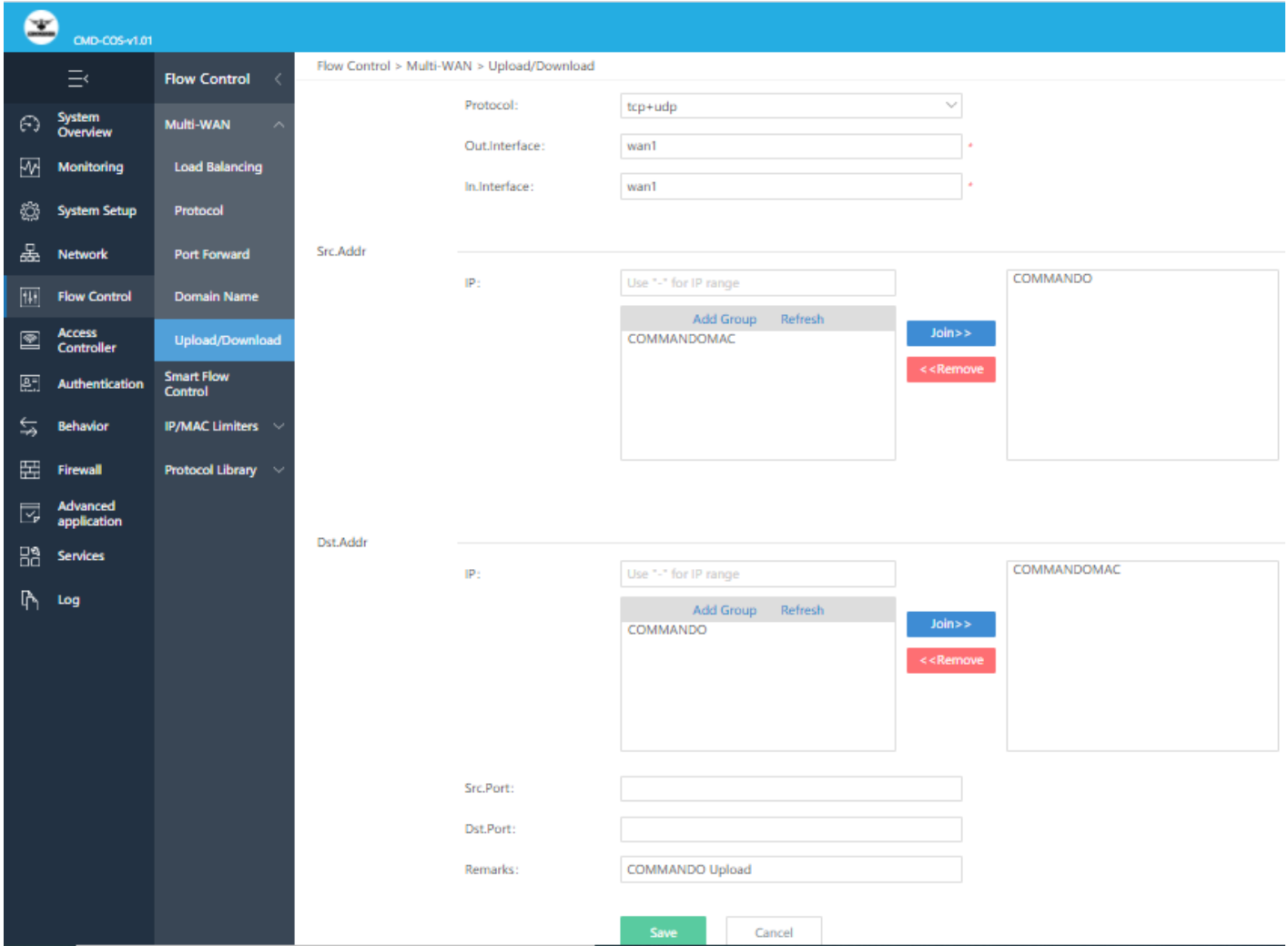


Fig 4.1.22 Details for Multi-WAN Upload and Download Control Settings page

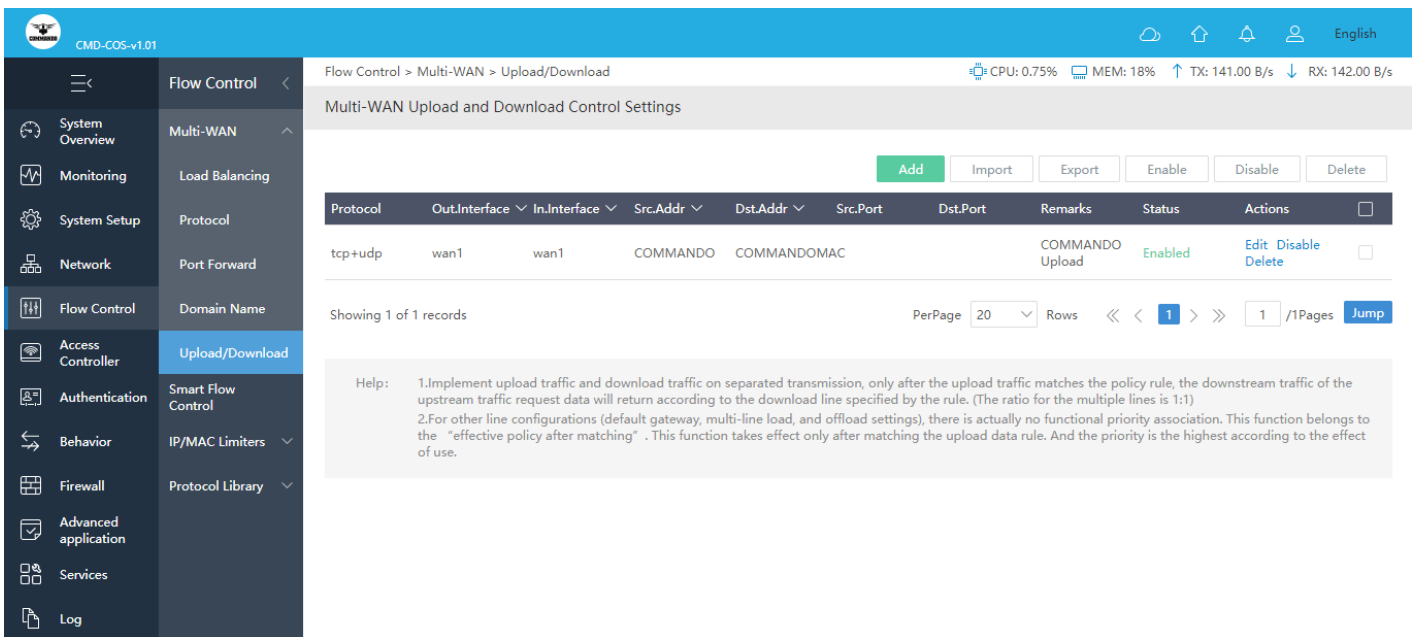


Fig 4.1.23 Multi-WAN Upload and Download Control Settings page

## 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.

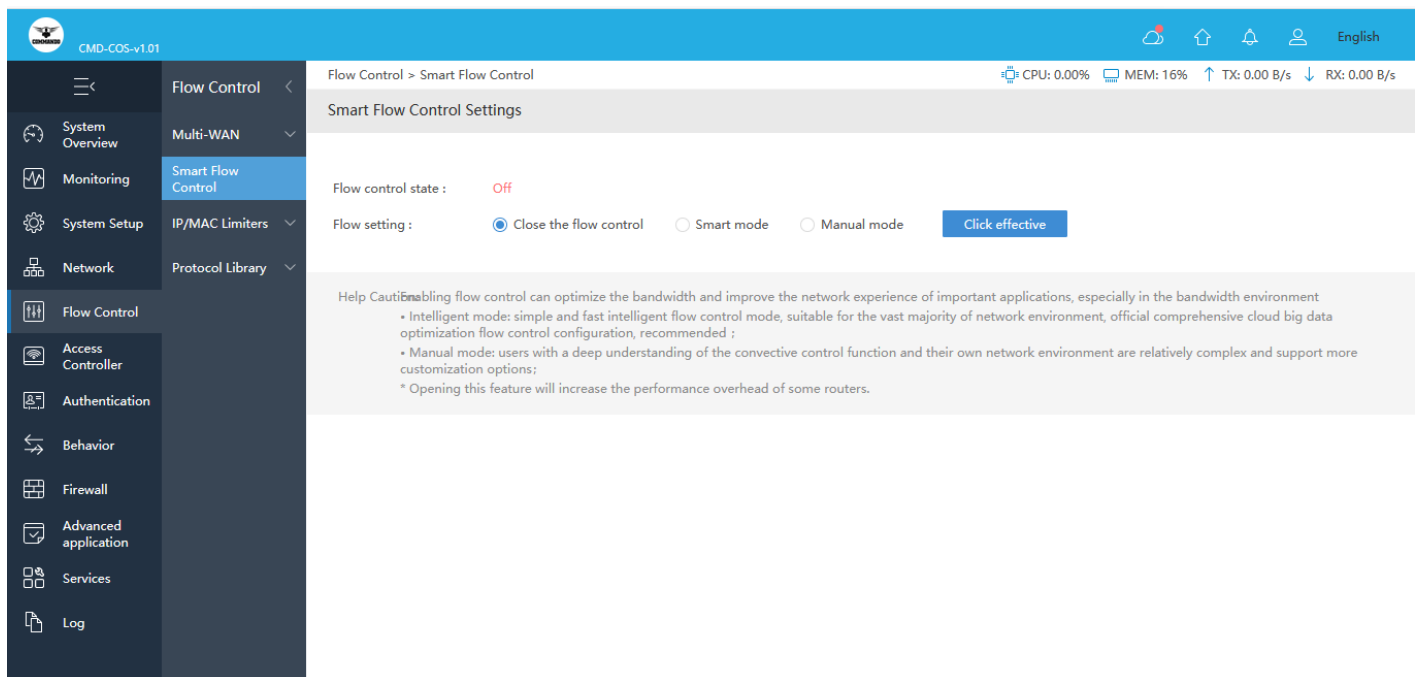
### Manual mode:

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 router for specific applications.

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



CMD-COS-v1.01

Flow Control > Smart Flow Control

Smart Flow Control Settings

Flow control state : Off

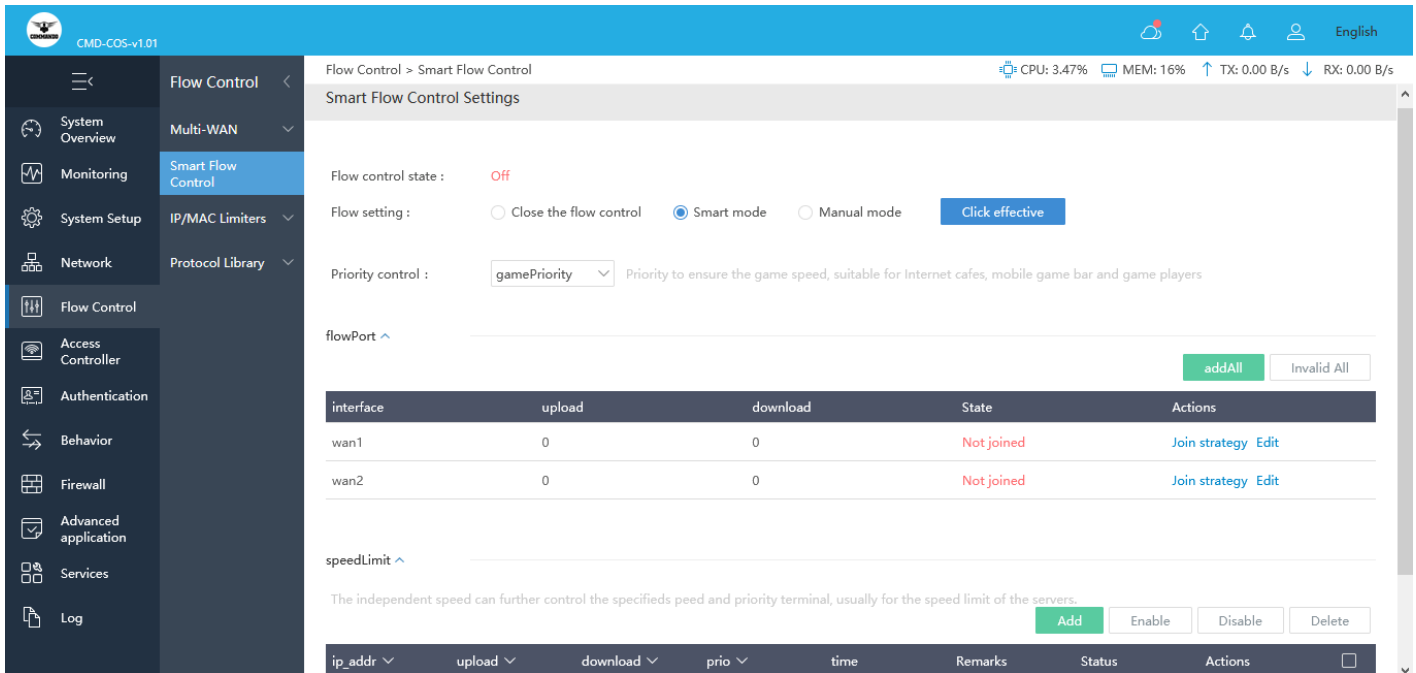
Flow setting :  Close the flow control  Smart mode  Manual mode [Click effective](#)

Help Caution: 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;

\* Opening this feature will increase the performance overhead of some routers.

**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.



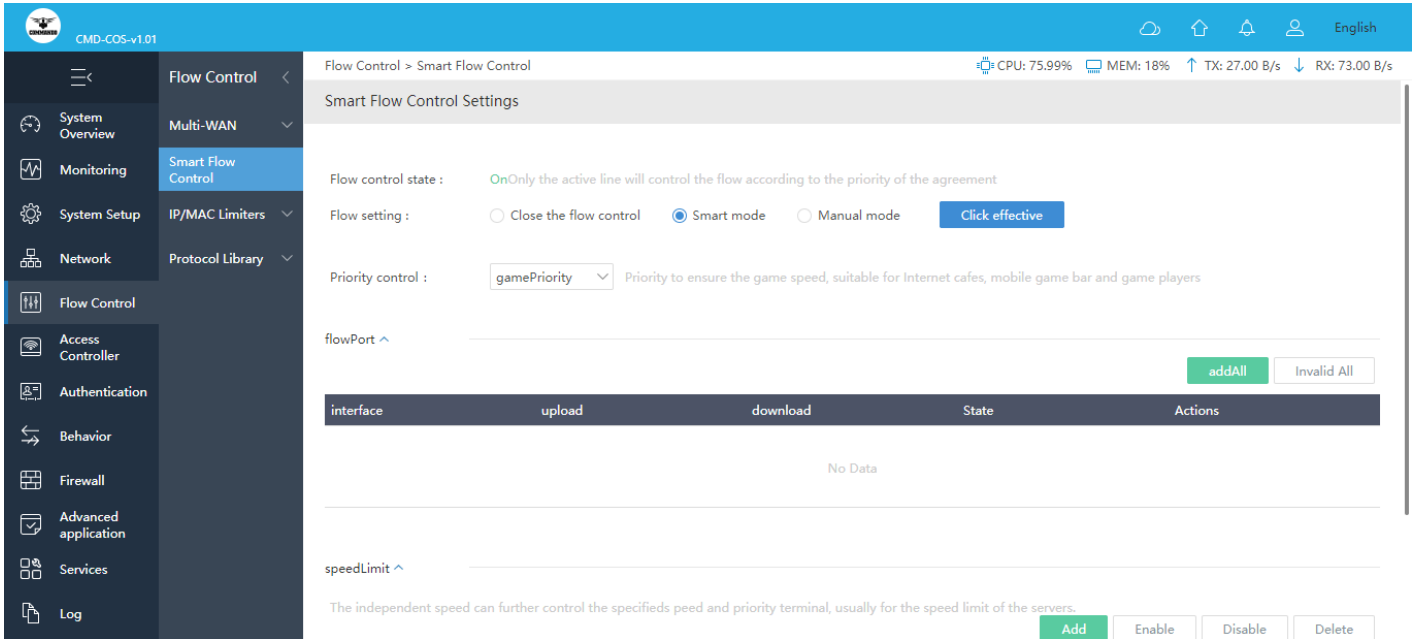


Fig 4.2.3 Default game Priority in Smart Flow Control Settings page

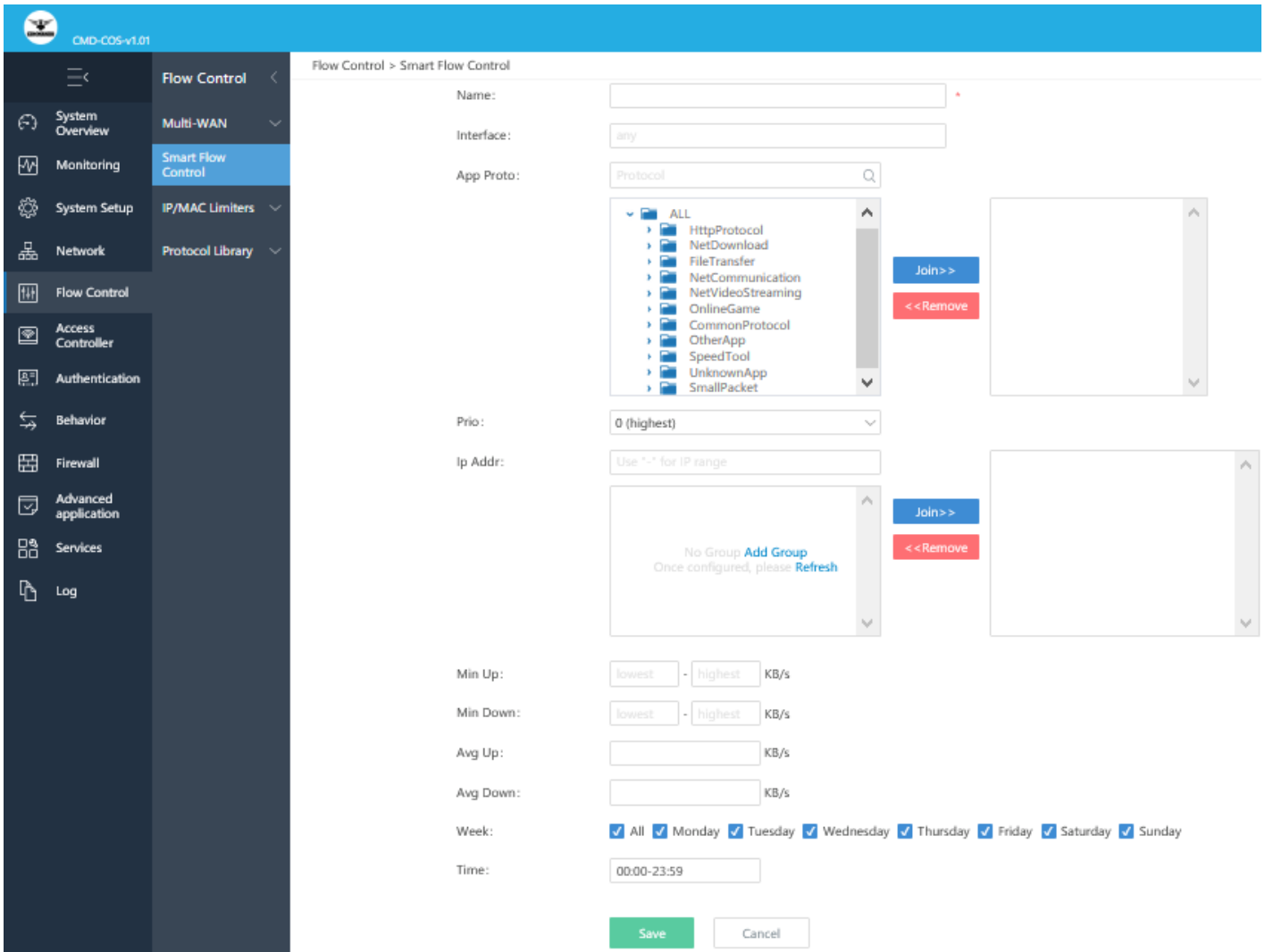
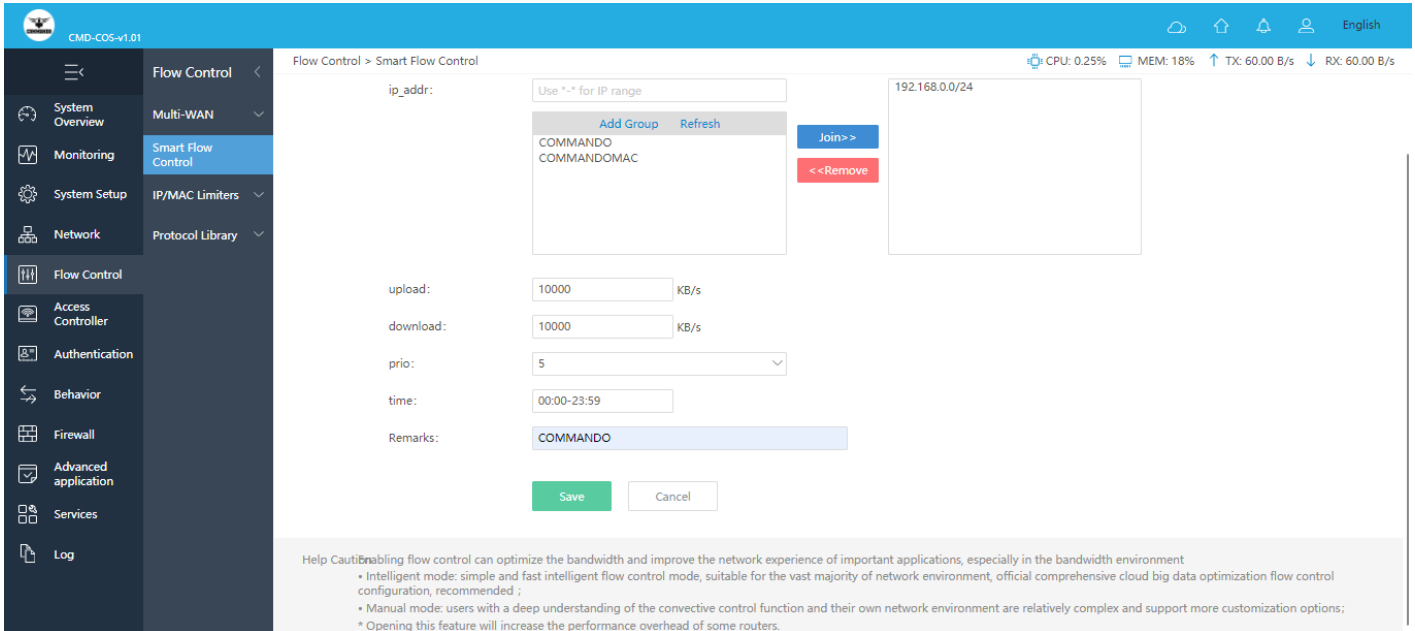
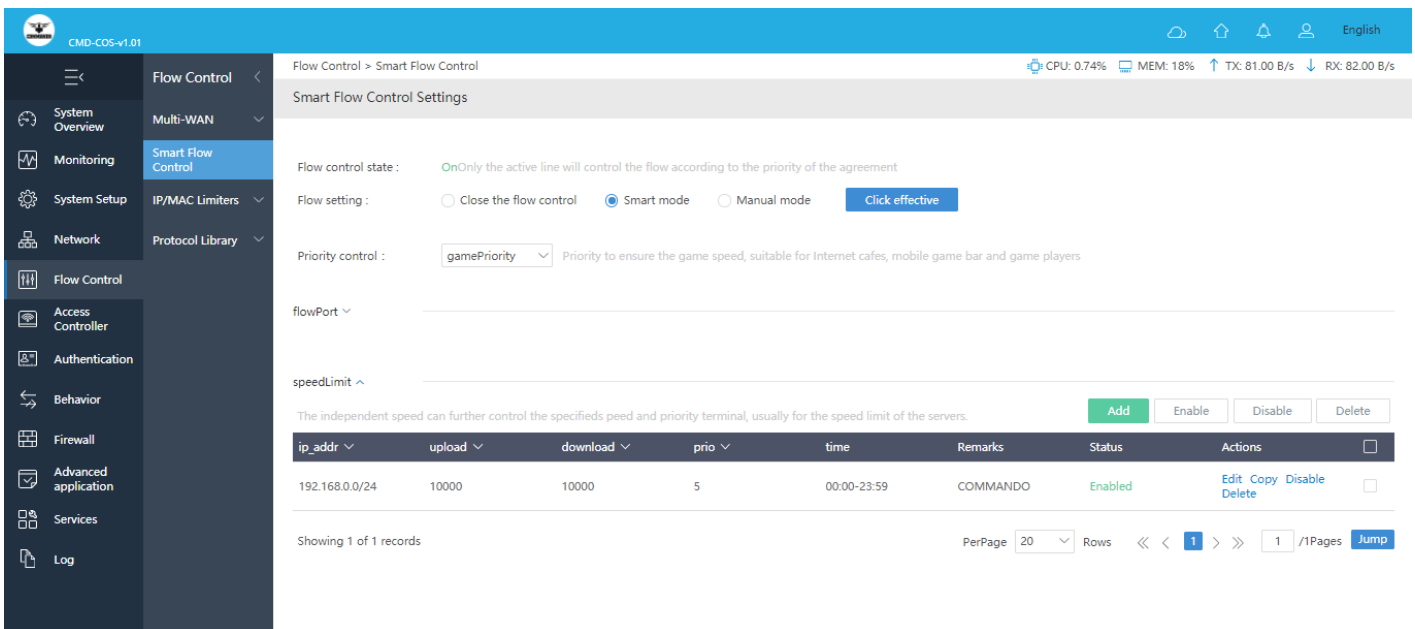


Fig 4.2.4 Add Smart Flow Control Settings page



**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 router 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

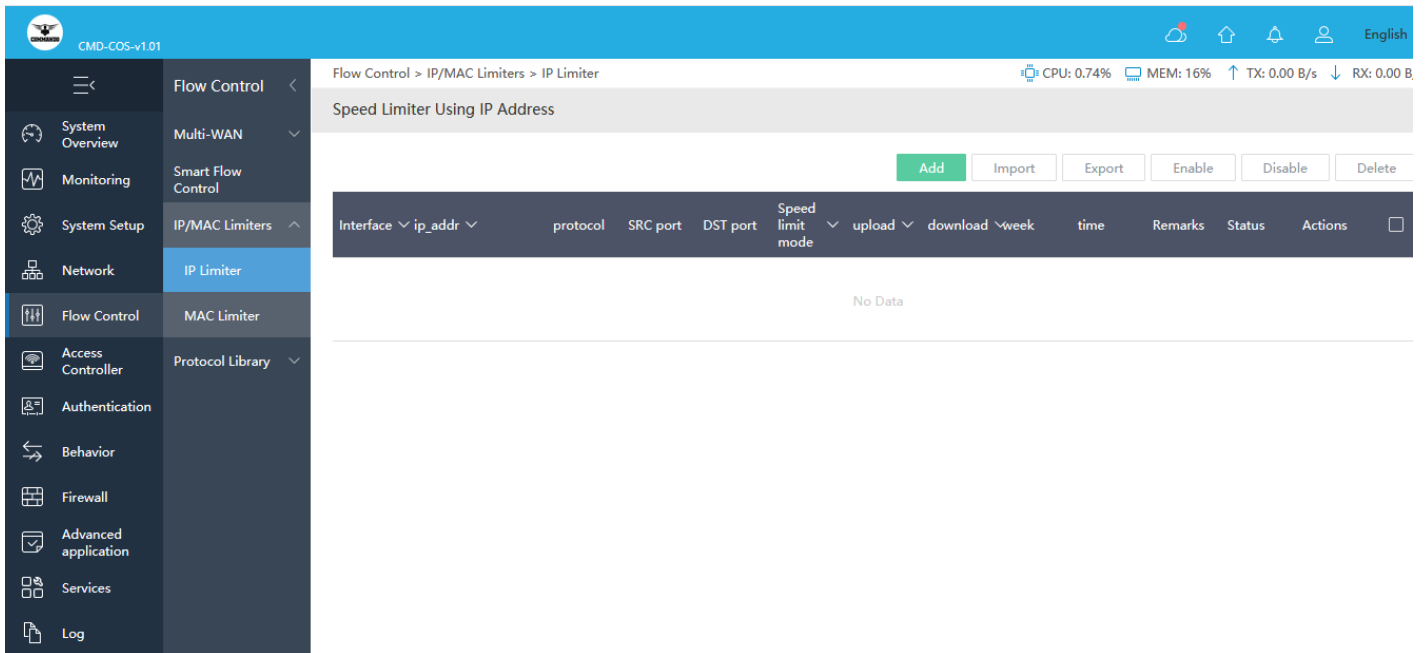
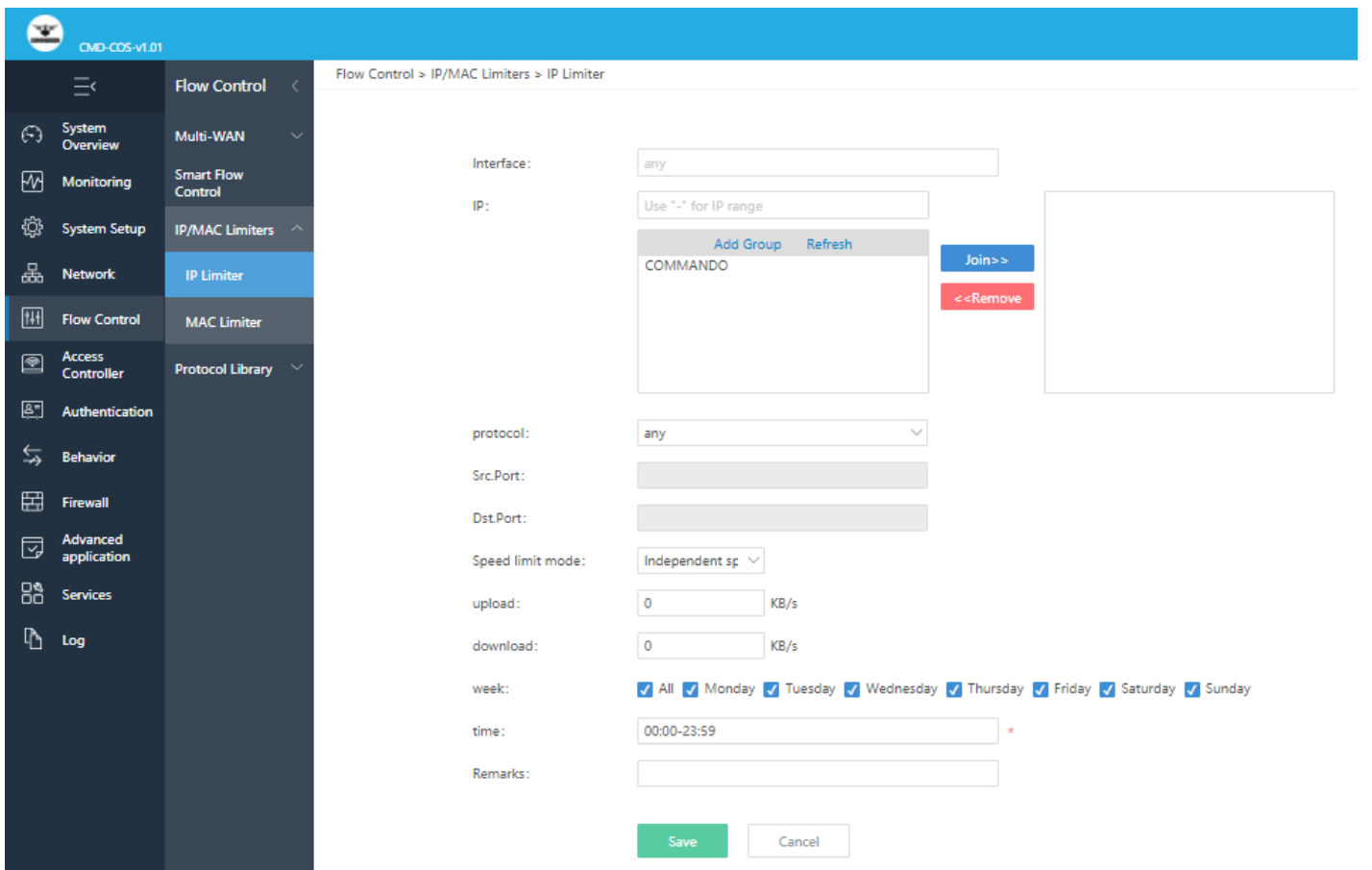
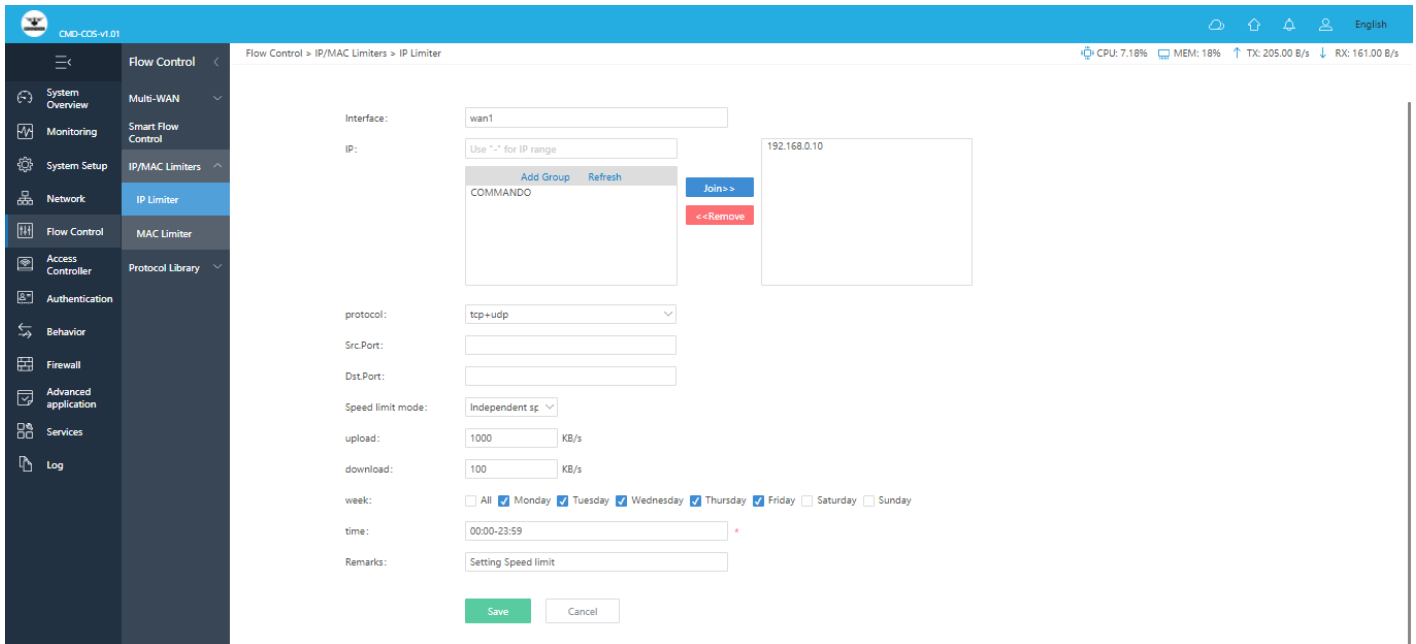


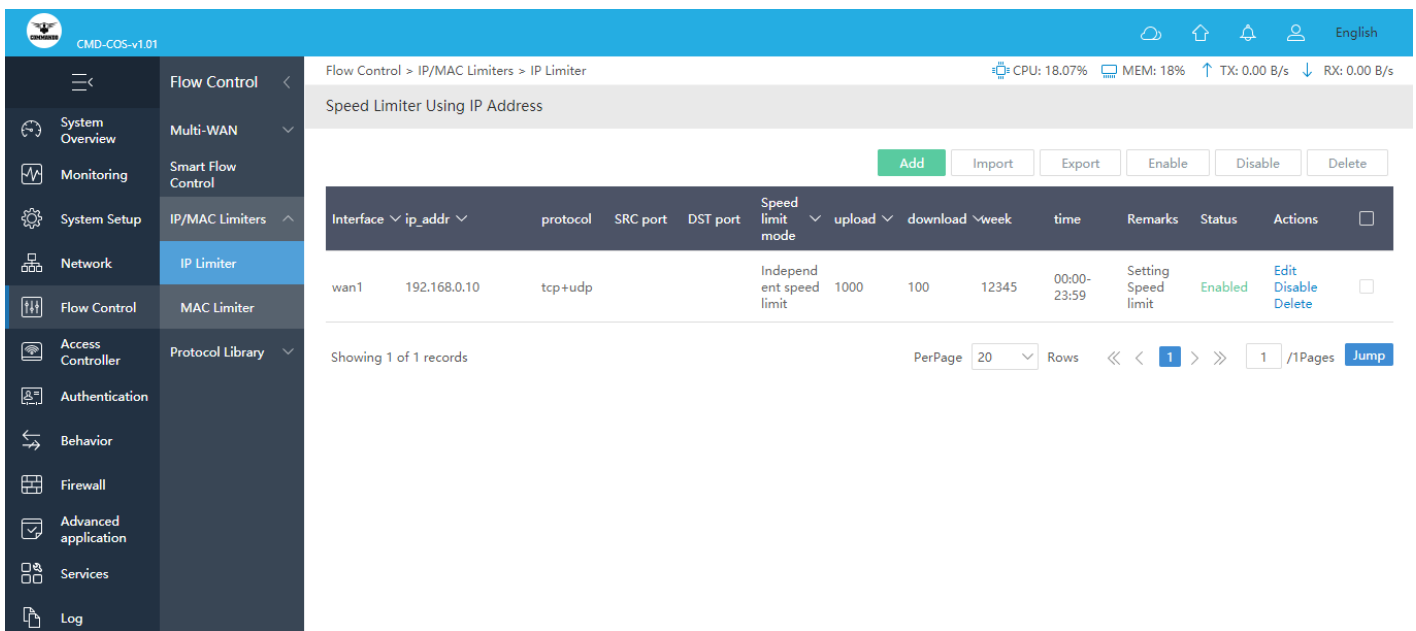
Fig 4.3.1 Default Speed Limiter Using IP Address page



**Fig 4.3.2 Add Speed Limiter Using IP Address page**



**Fig 4.3.3 Speed Limiter for Particular IP Address Page**



**Fig 4.3.4 Speed Limiter Using IP Address Page**

**Speed Limiter Using MAC Address:**

Limit bandwidth on your router 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

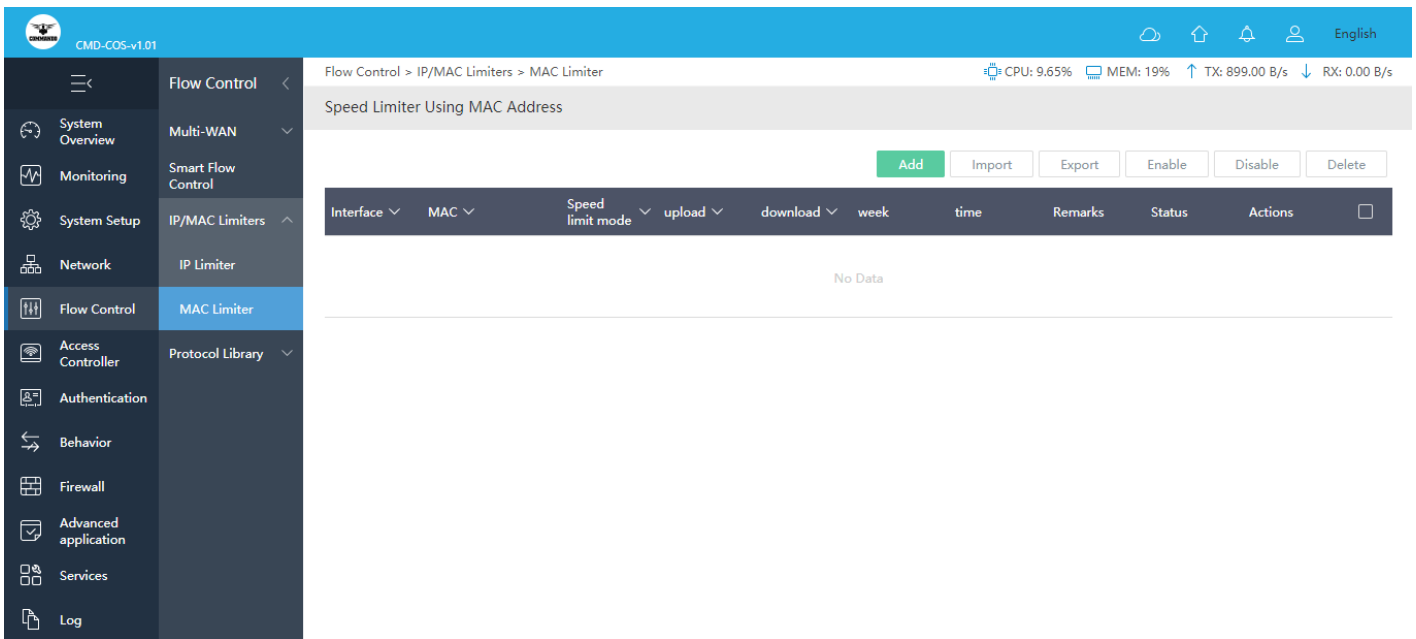


Fig 4.3.5 Default Speed Limiter Using MAC Address page

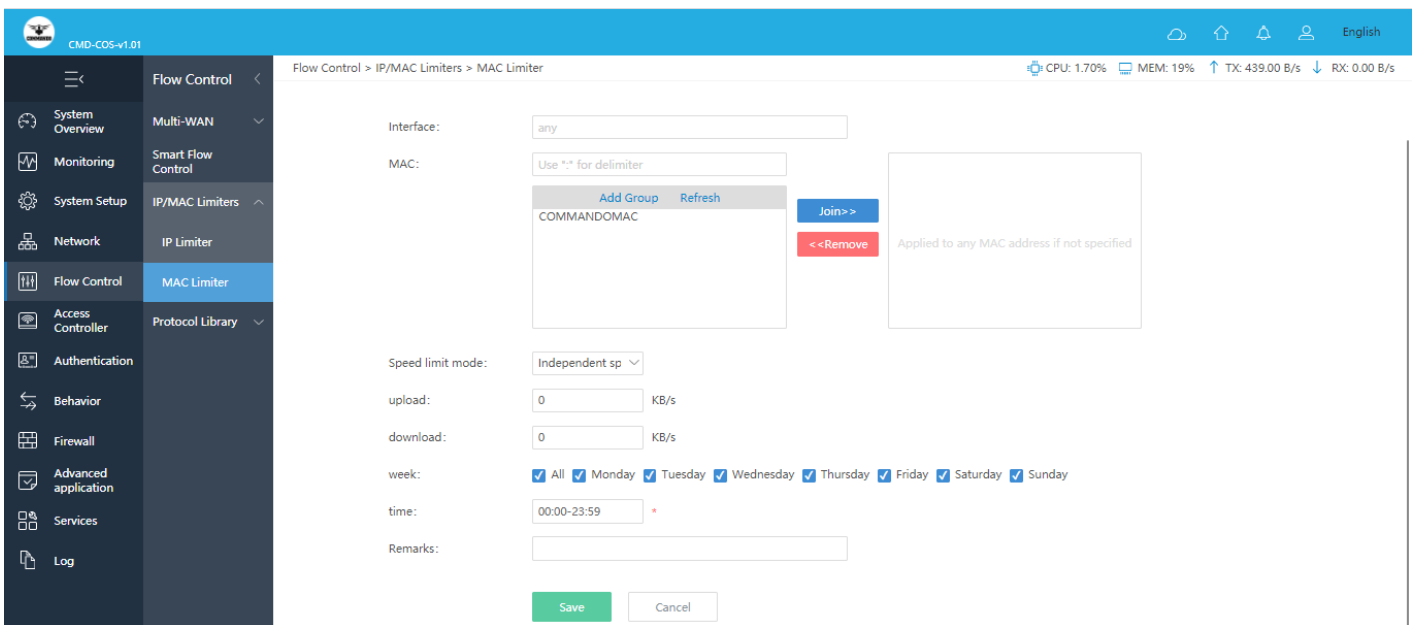
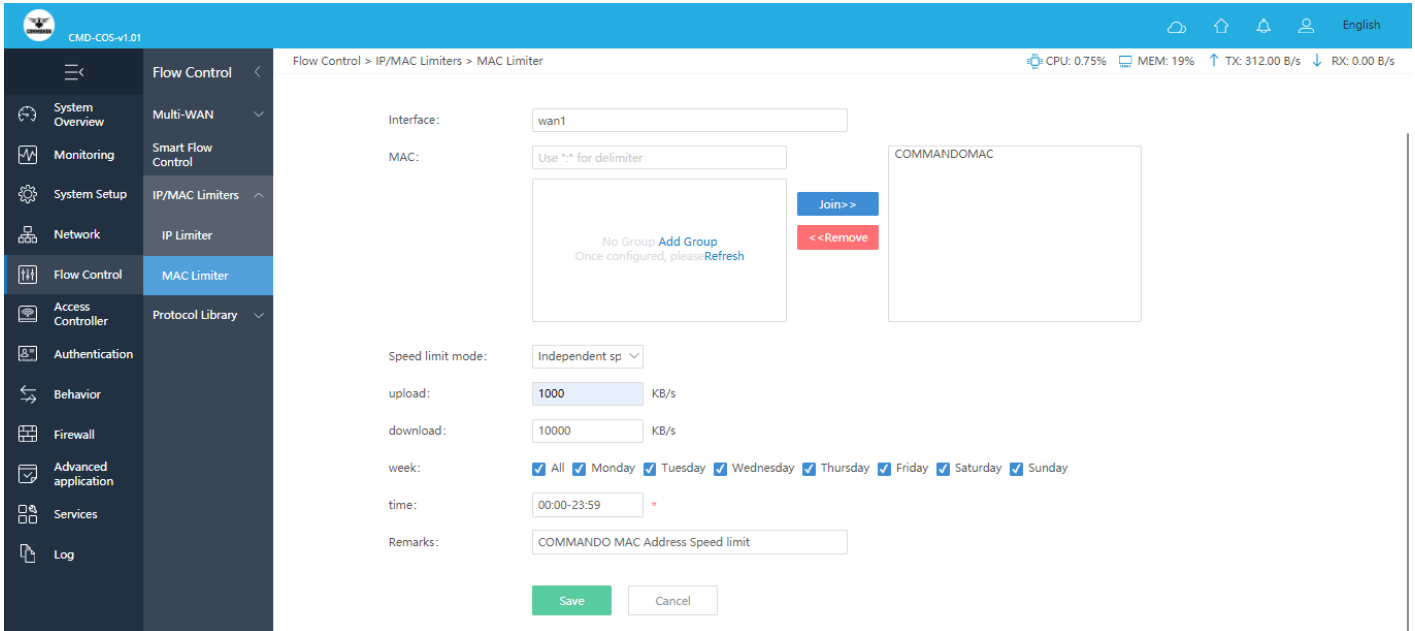
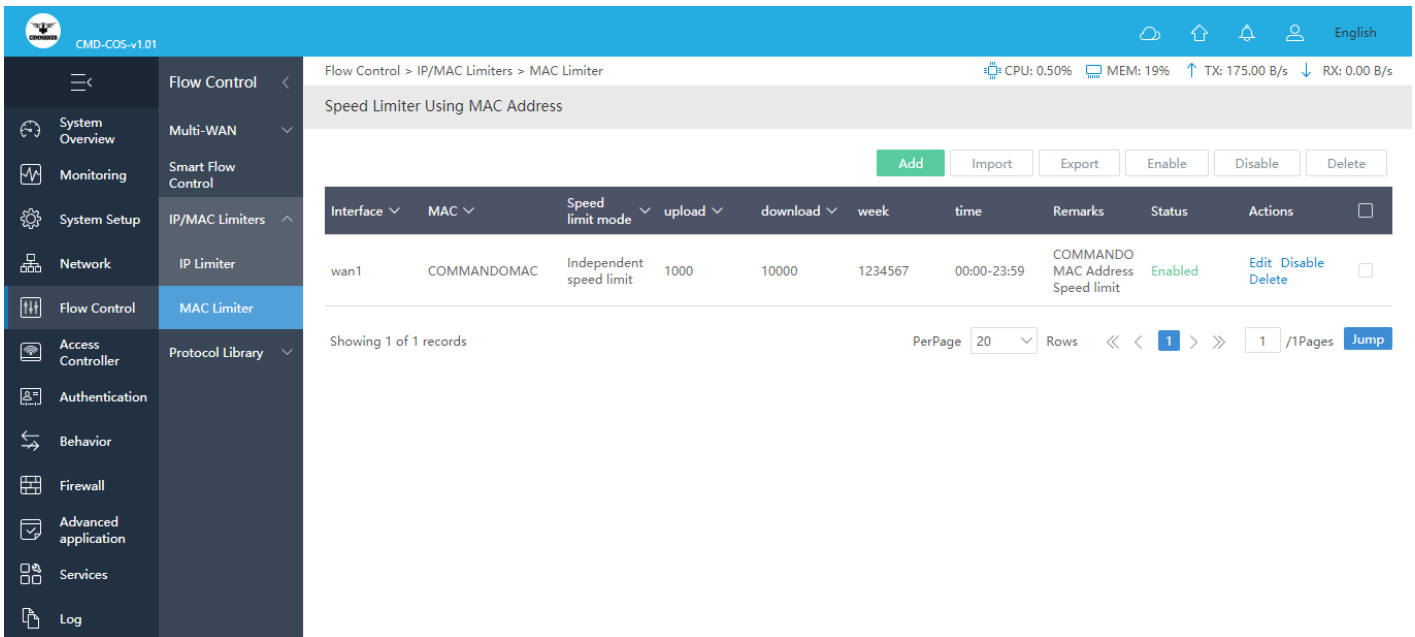


Fig 4.3.6 Add Speed Limiter Using MAC Address page



**Fig 4.3.7 Speed Limiter For COMMANDOMAC Group MAC Address**



**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

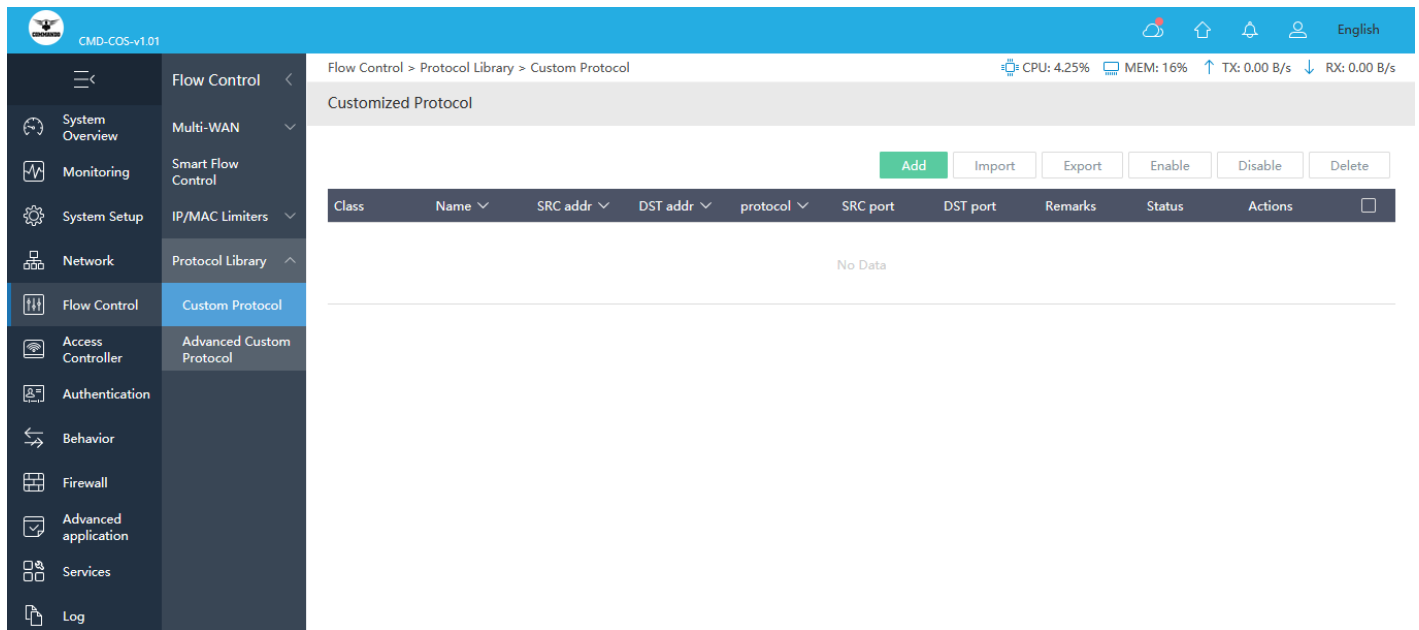


Fig 4.4.1 Default Customized Protocol page

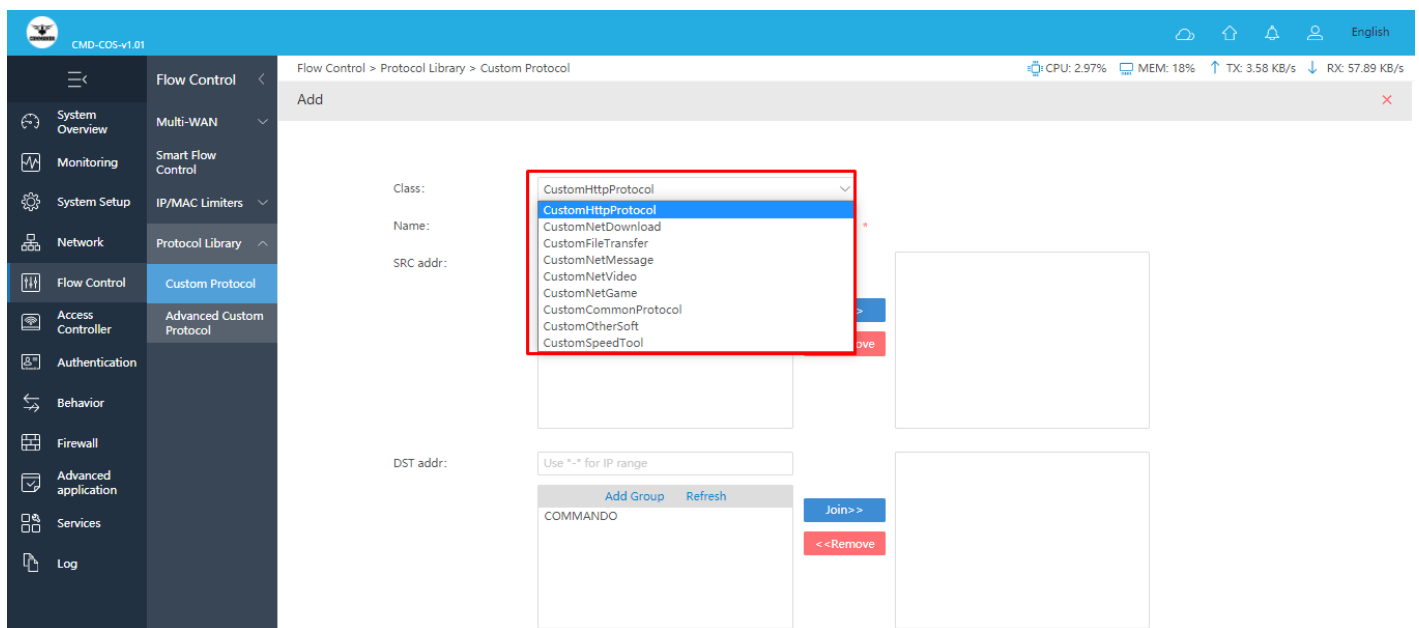
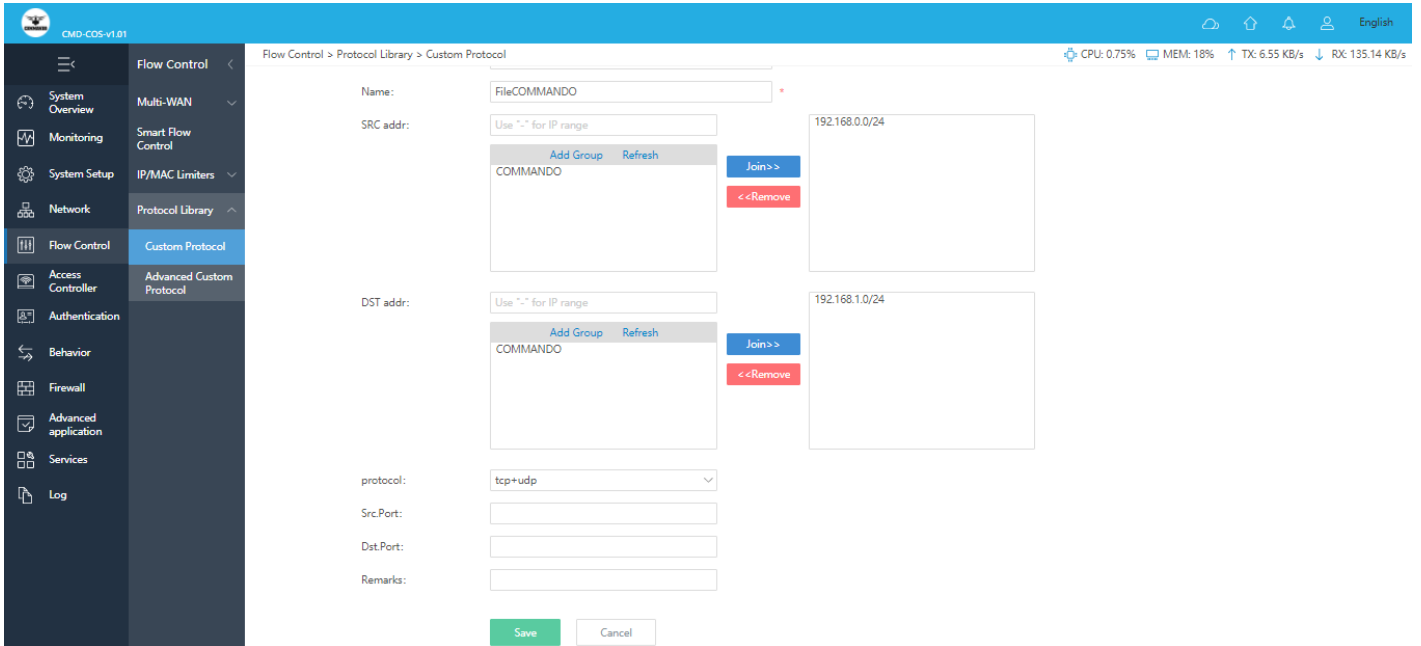
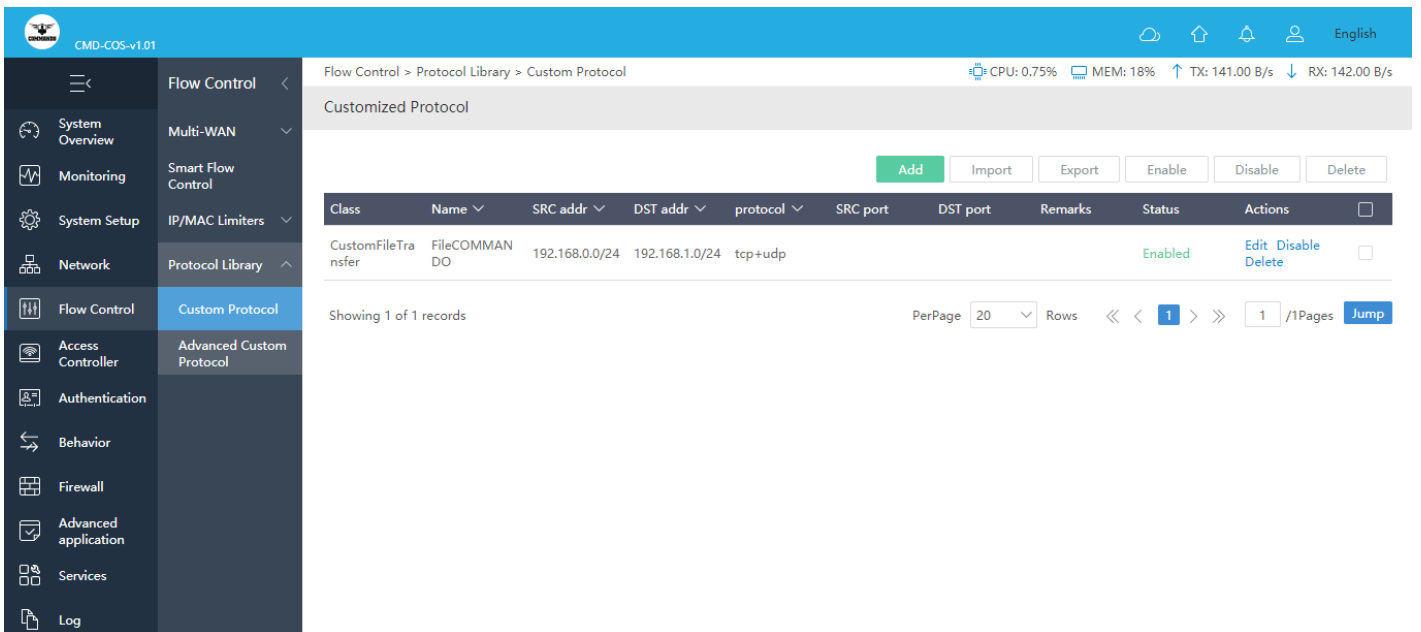


Fig 4.4.2 Add Customized Protocol page



**Fig 4.4.3 Customized Protocol for particular source and destination address page**



**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



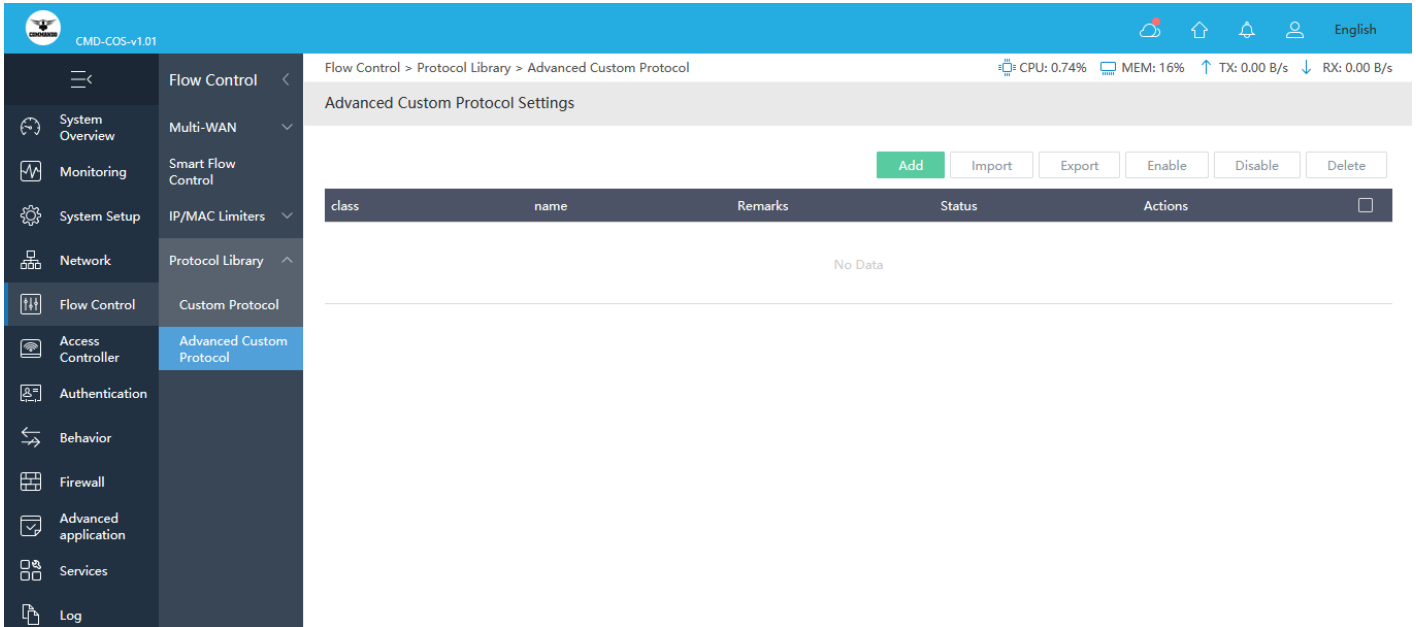


Fig 4.4.5 Default Advanced Custom Protocol page

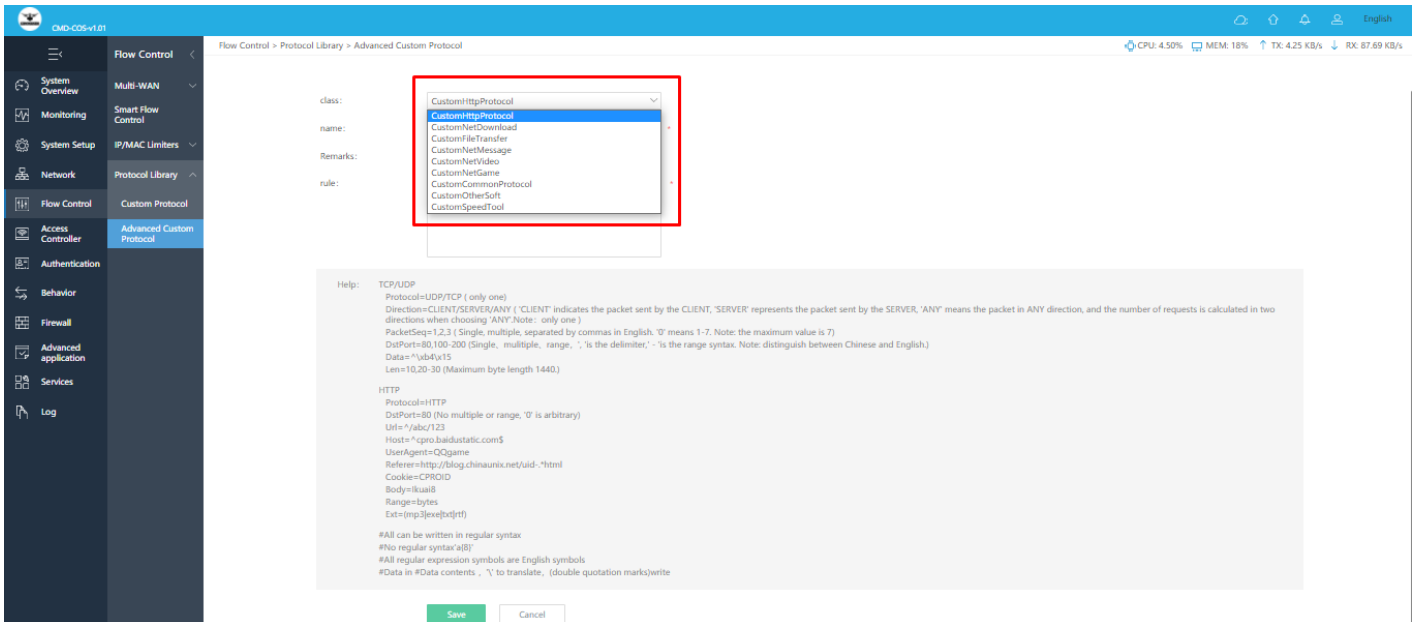


Fig 4.4.5 Add Advanced Custom Protocol page

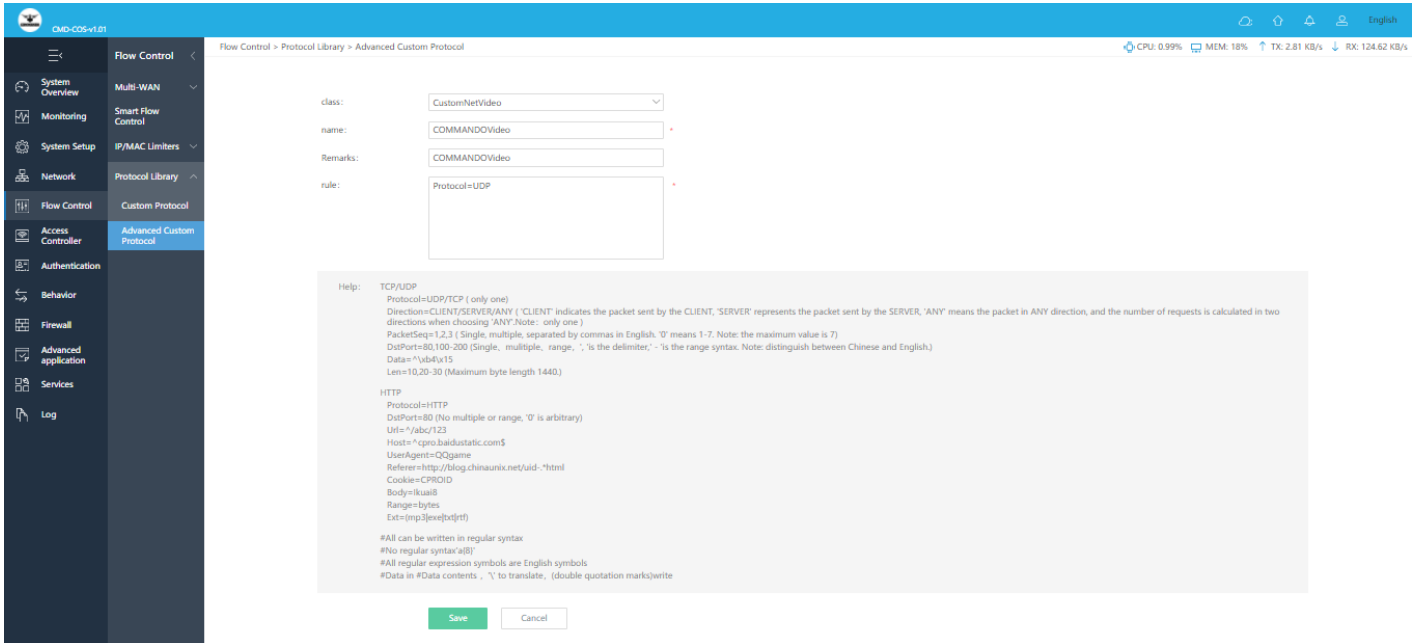


Fig 4.4.6 Advanced Custom Protocol setting for video page

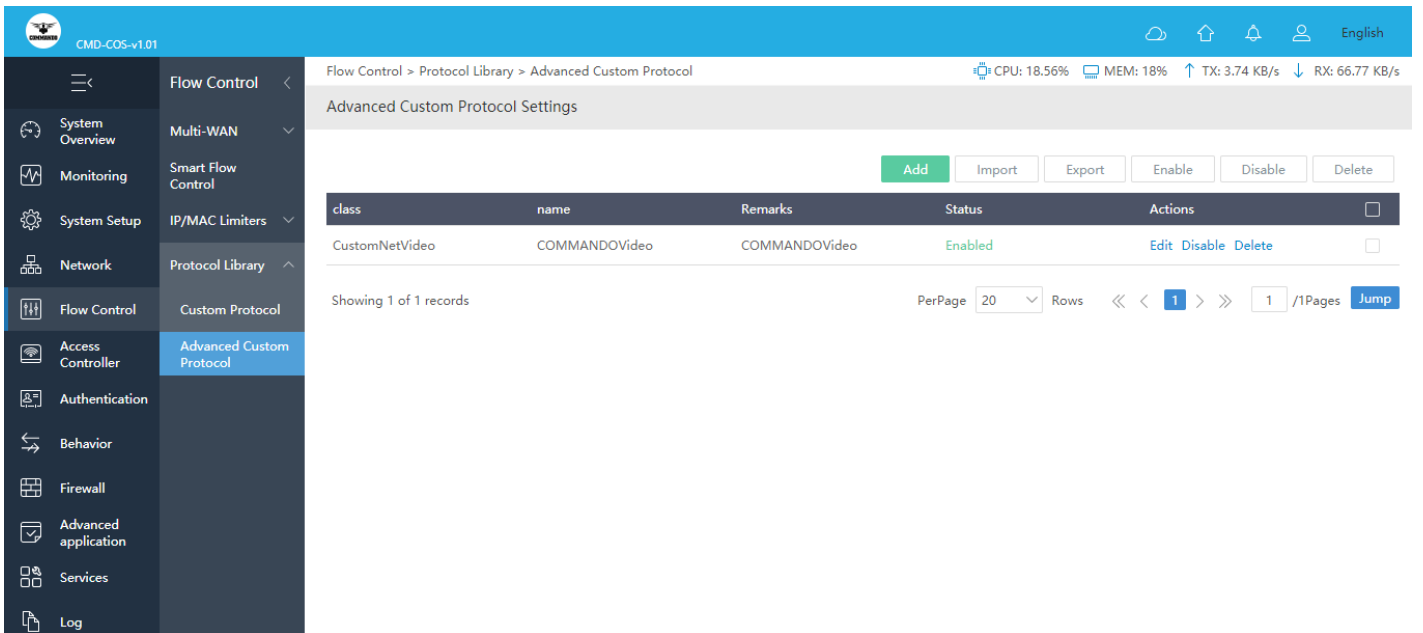


Fig 4.4.7 Advanced Custom Protocol page

## **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.

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

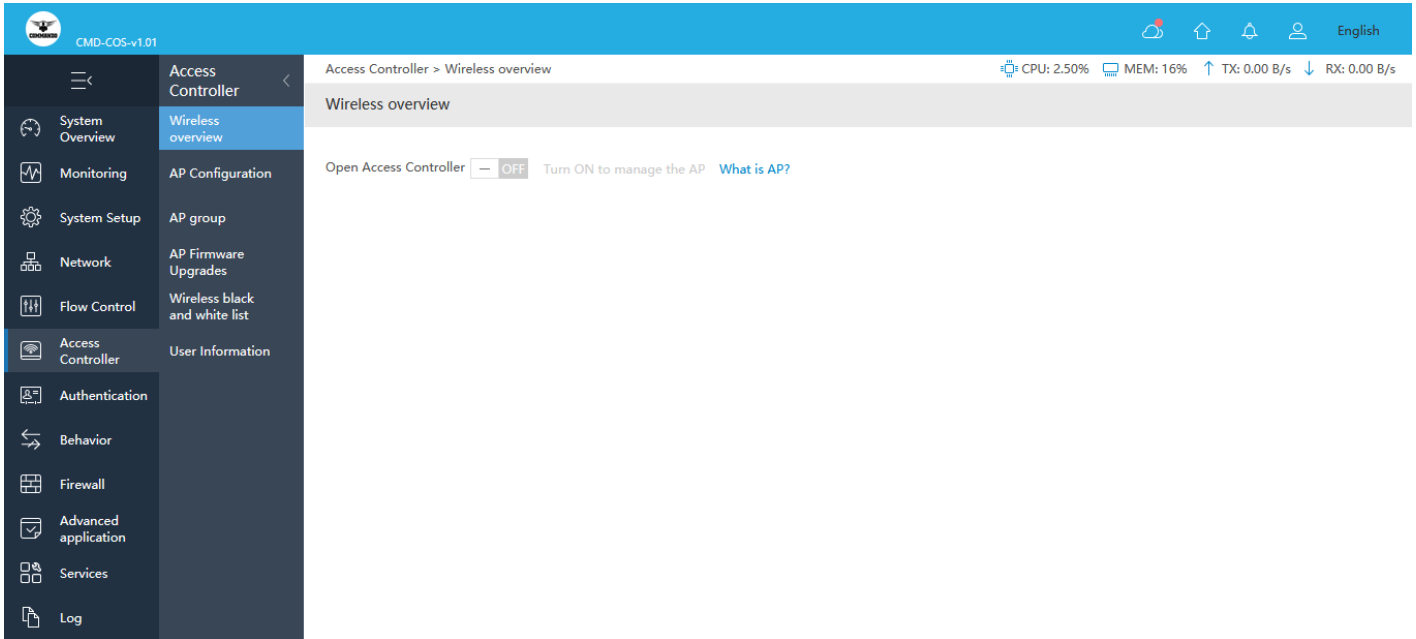
**Black White List:** AP Mac address can be Black/white List to allow/ block access to respective AP's and all users associated with it.

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

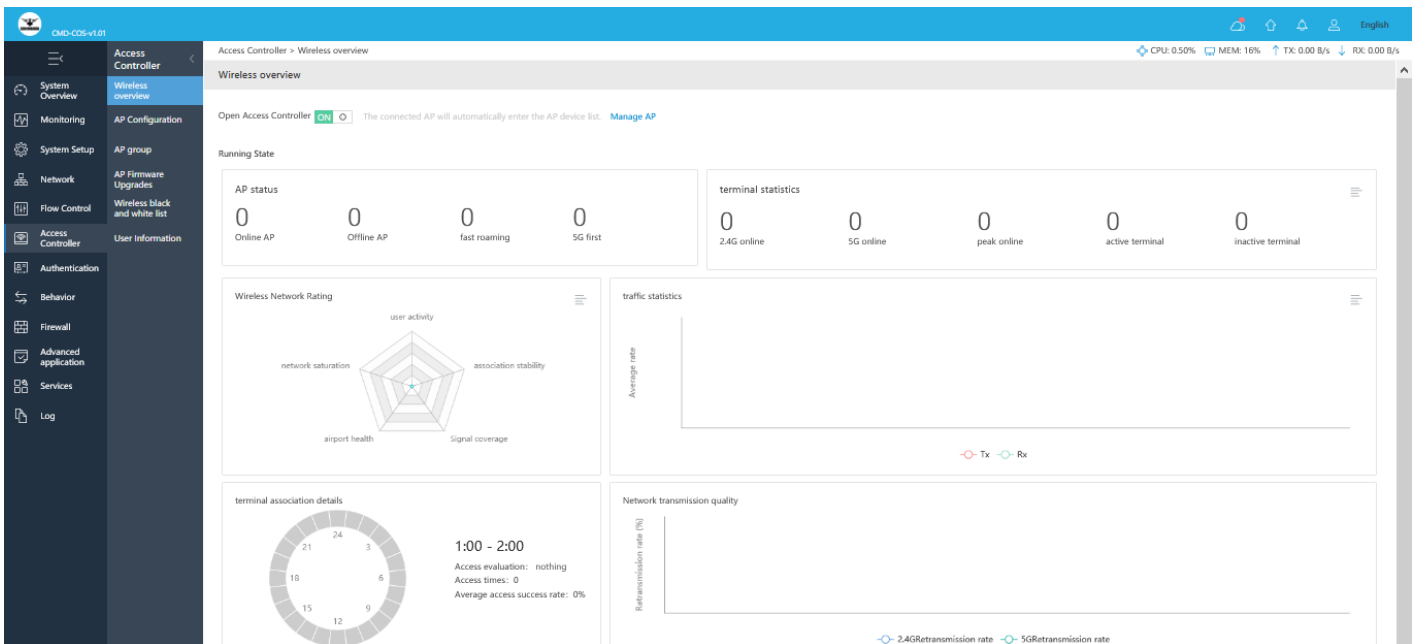
## **5.1 Wireless overview**

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.

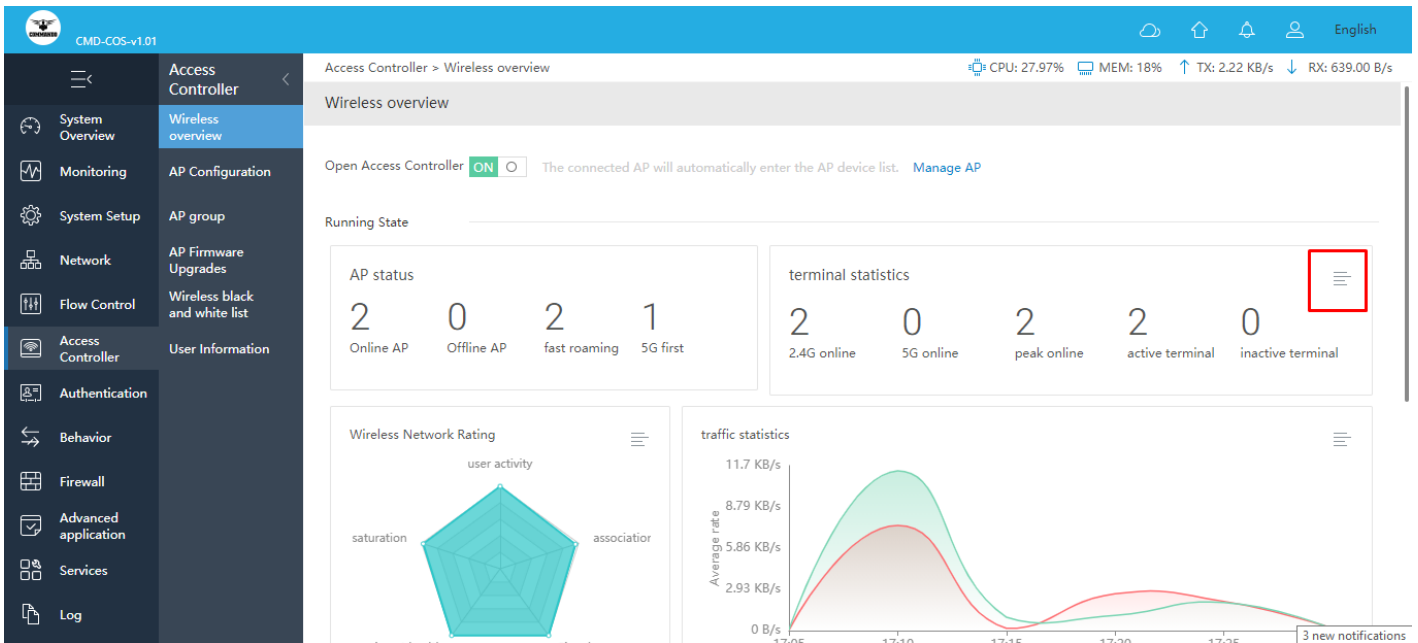
To view Wireless overview, Click on **Access Controller > Wireless overview**



**Fig 5.1.1 Default Wireless overview OFF page**

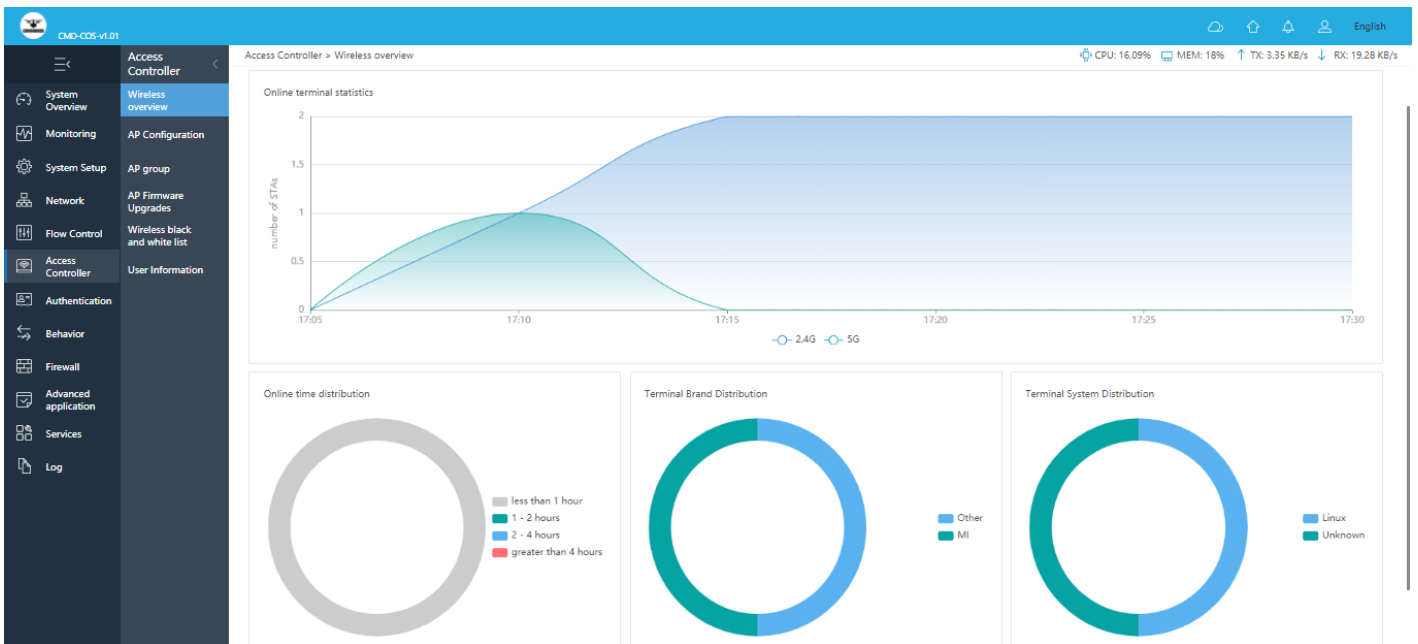


**Fig 5.1.2 Default Wireless overview ON page**

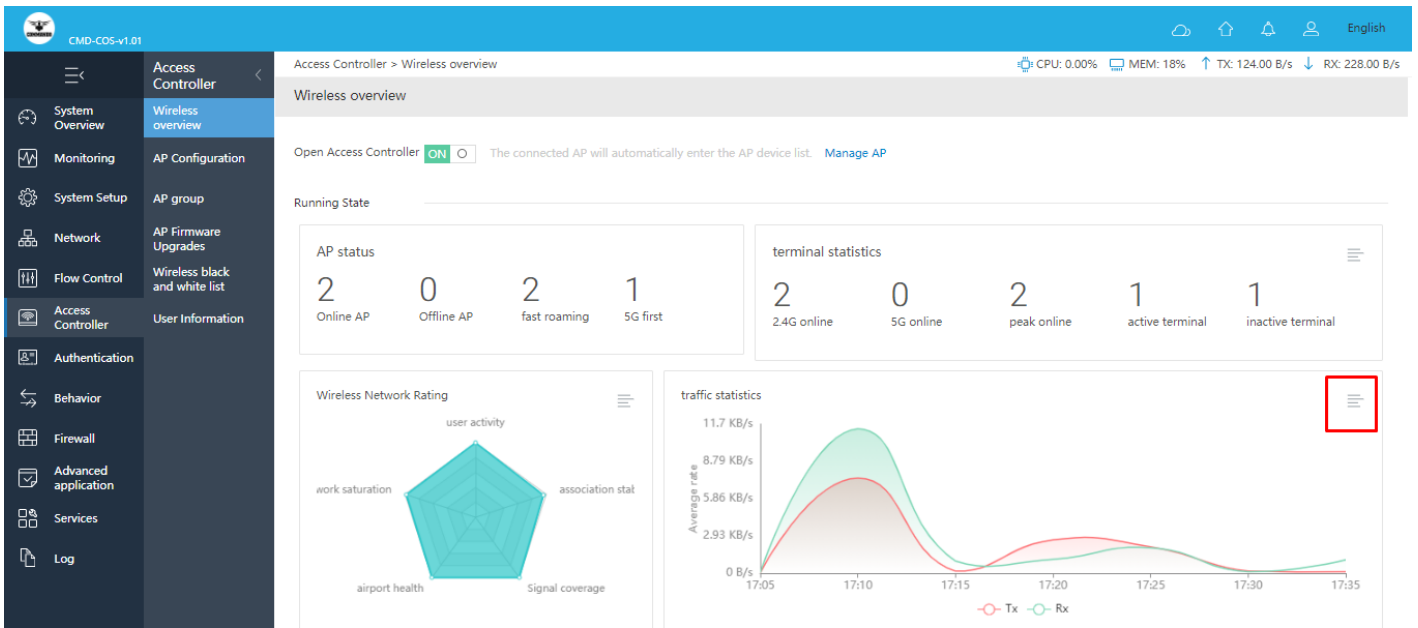


**Fig 5.1.3 Wireless overview after connecting AP and users' page**

After clicking above highlighted icon following page will be displayed

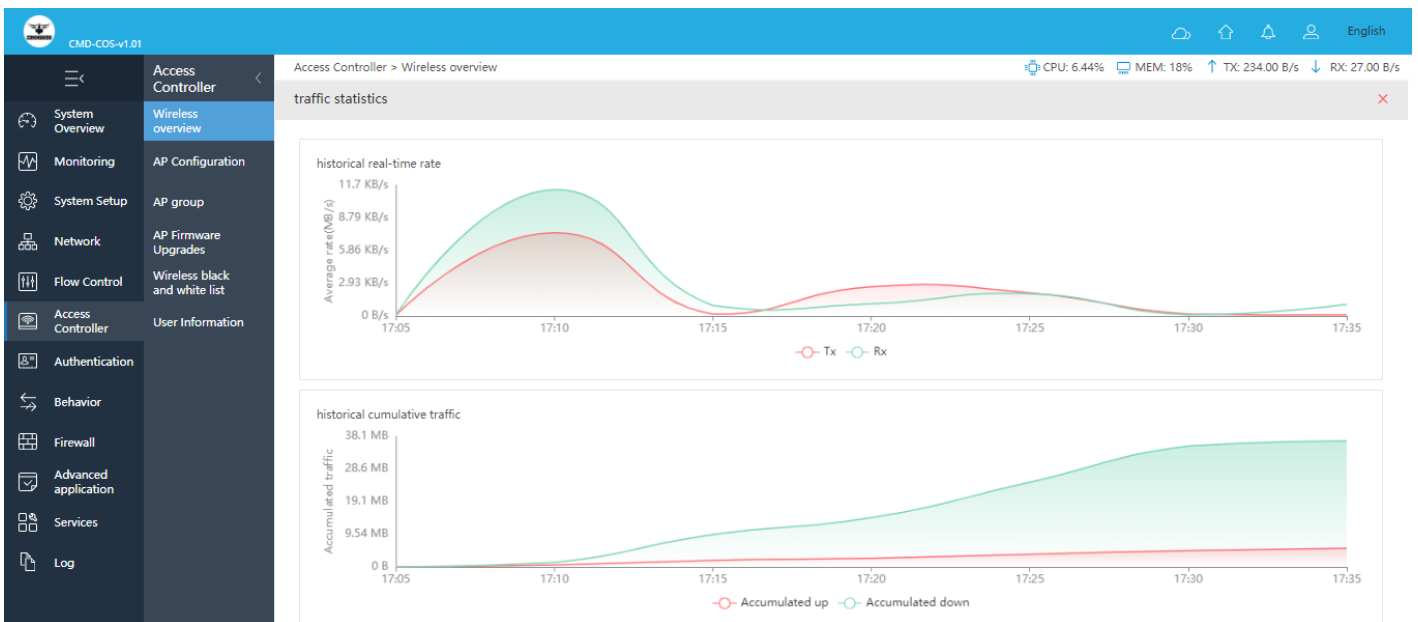


**Fig 5.1.4 Online terminal statistics, distribution, System page**

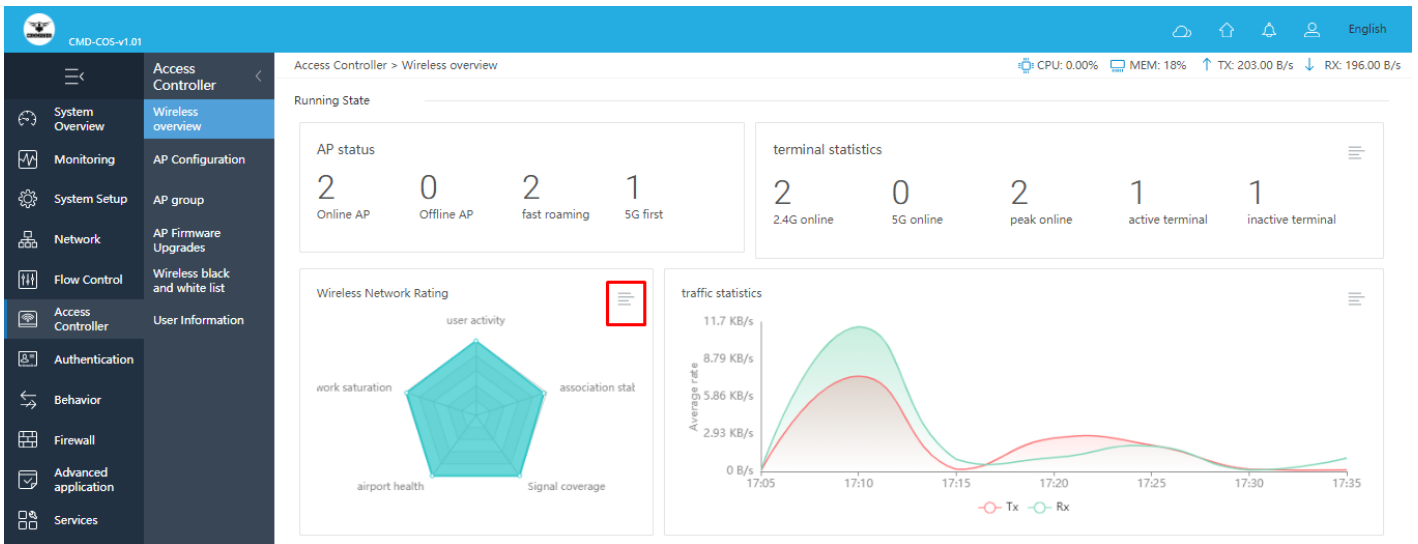


**Fig 5.1.5 Traffic statistics page**

After clicking above highlighted icon following page will be displayed



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



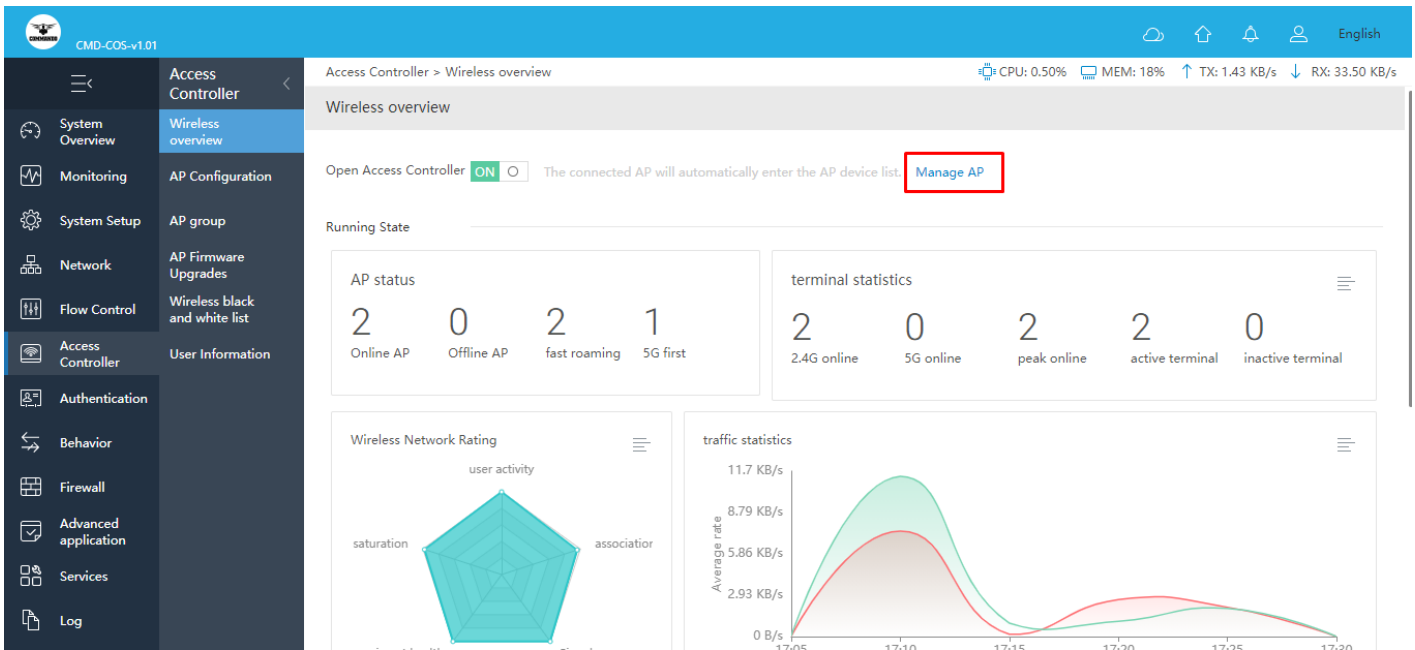
**Fig 5.1.7 Wireless Network Rating page**

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.

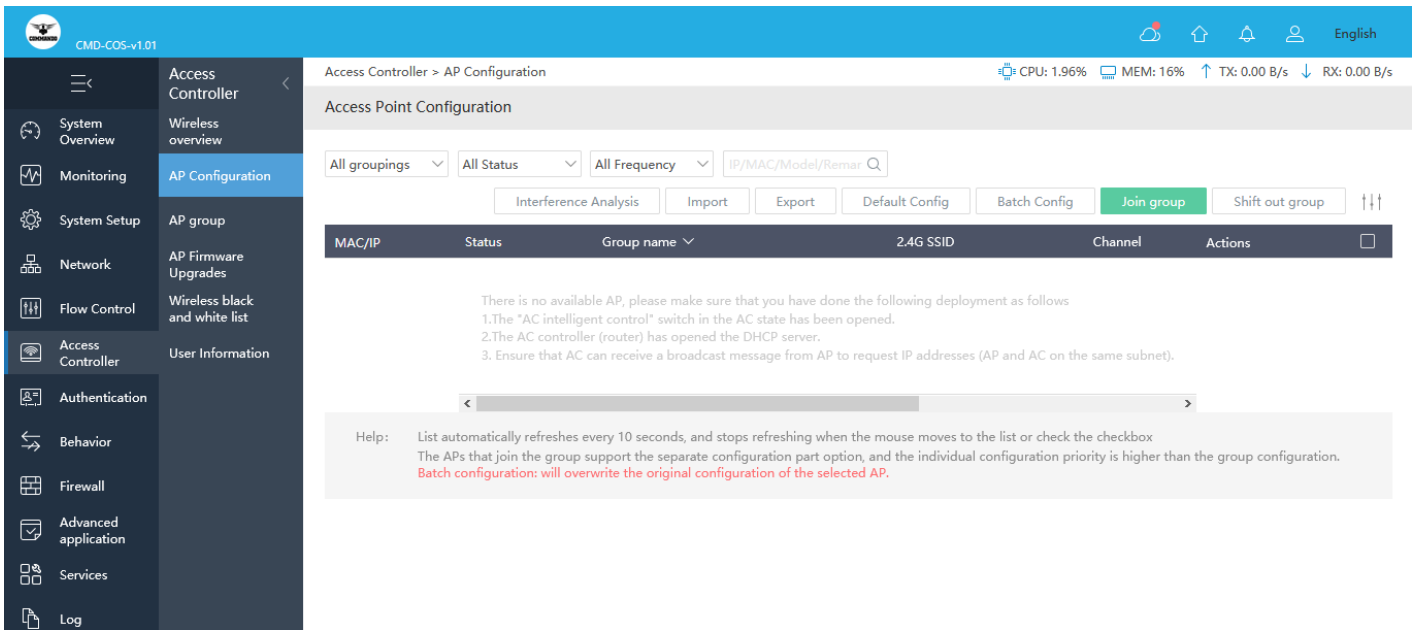


Fig 5.2.1 Default Access Point Configuration page

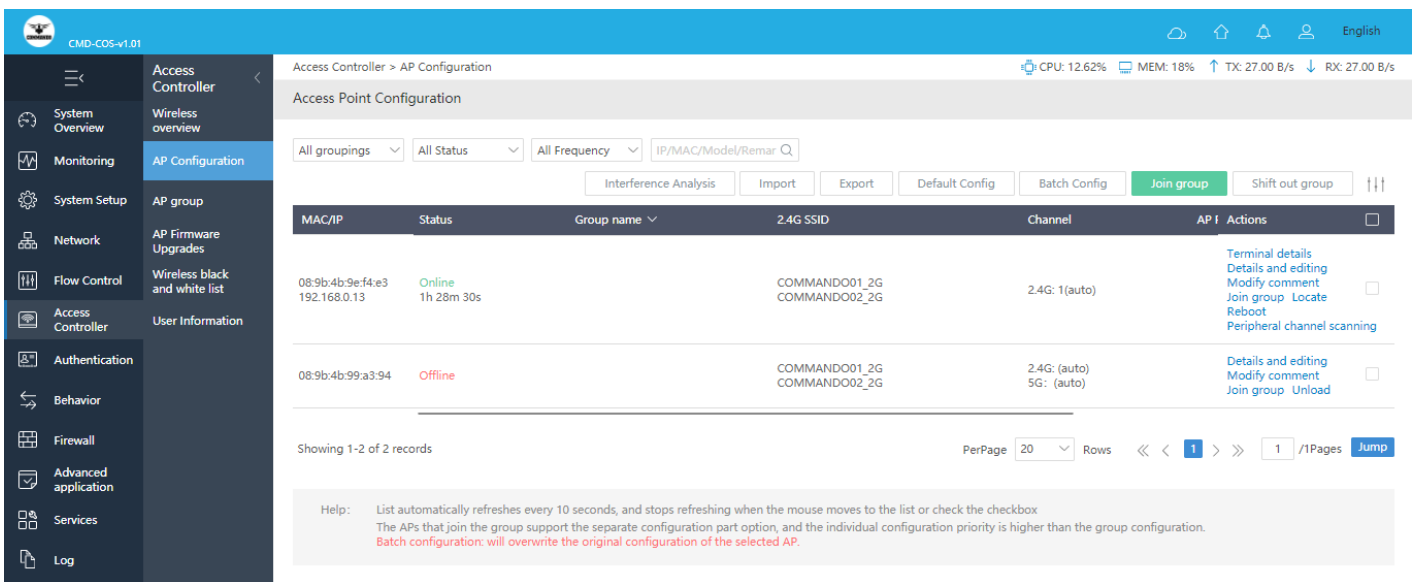
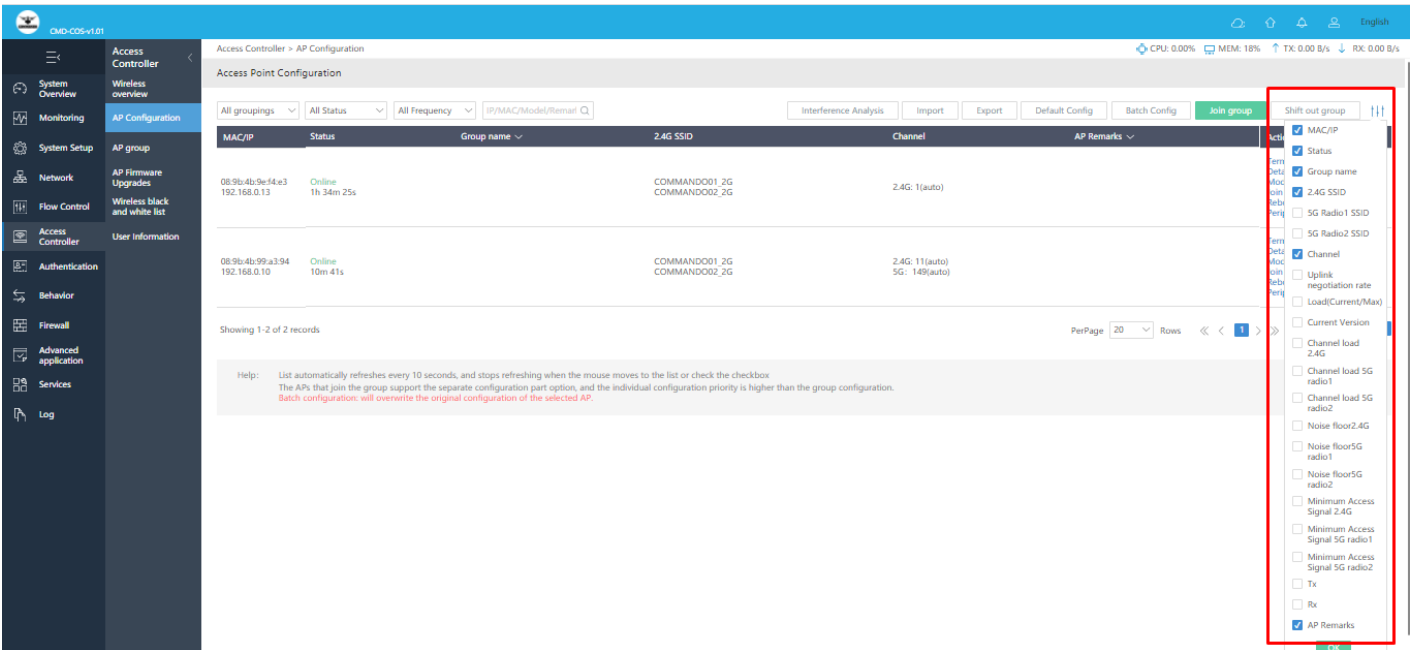


Fig 5.2.2 Access Point Configuration Online/Offline AP page



5.2.3 Access Point Configuration Default AP page

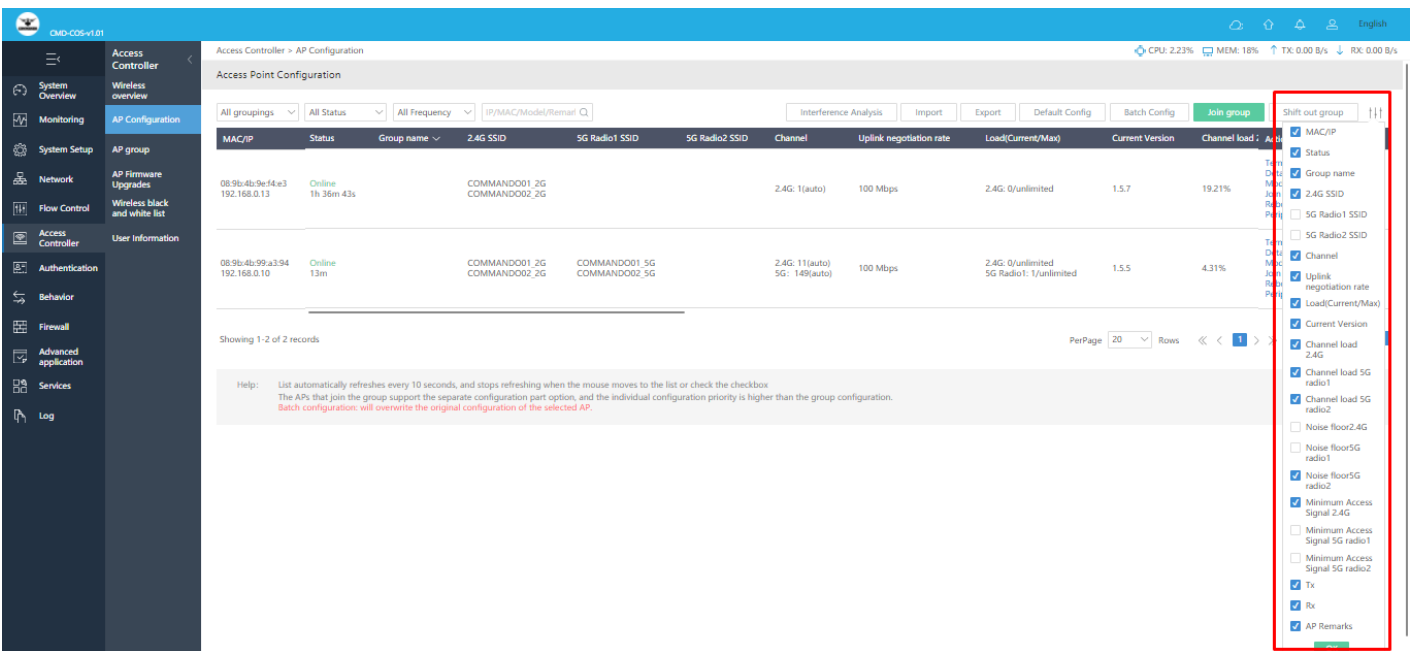
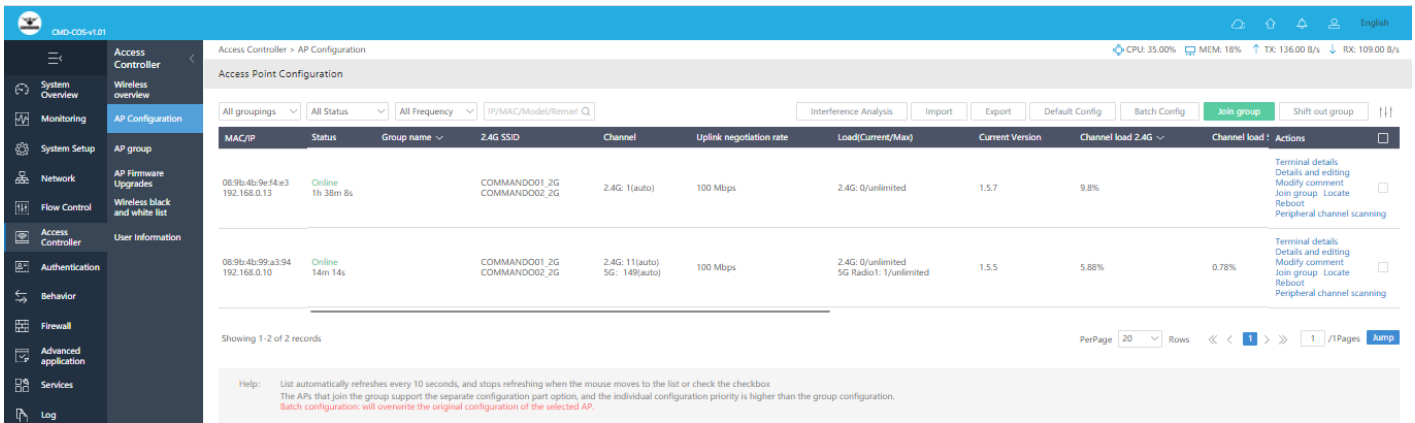
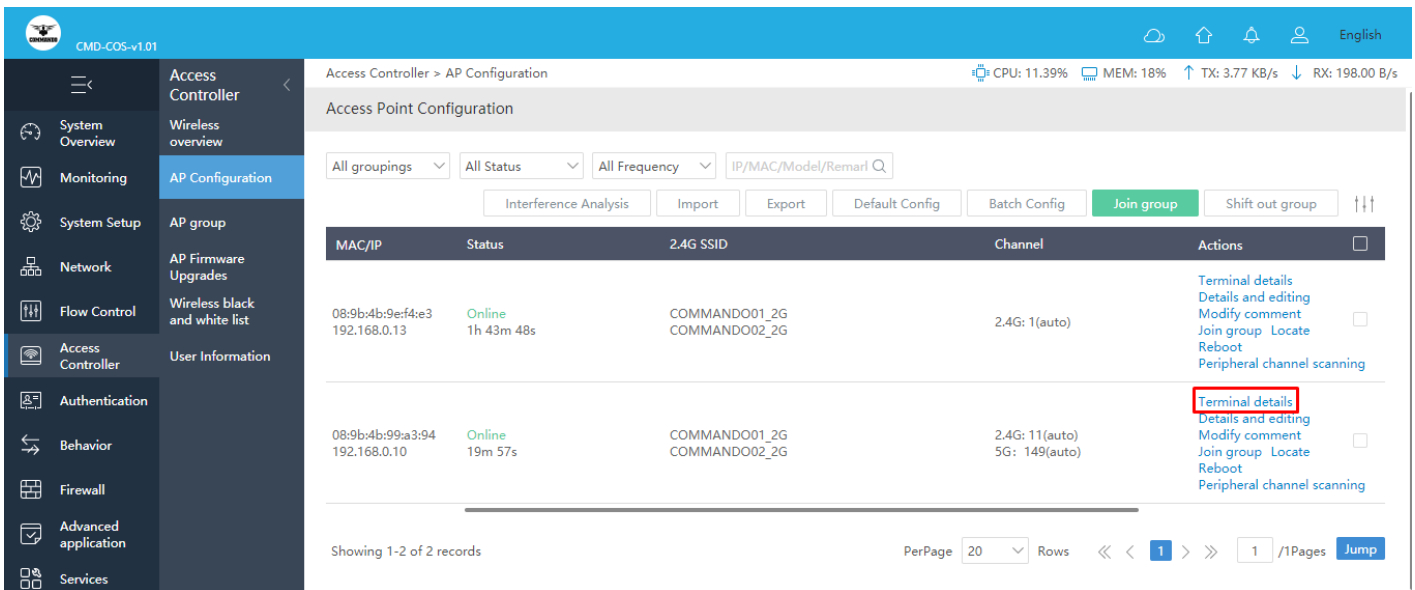


Fig 5.2.4 Access Point Configuration Customize display page

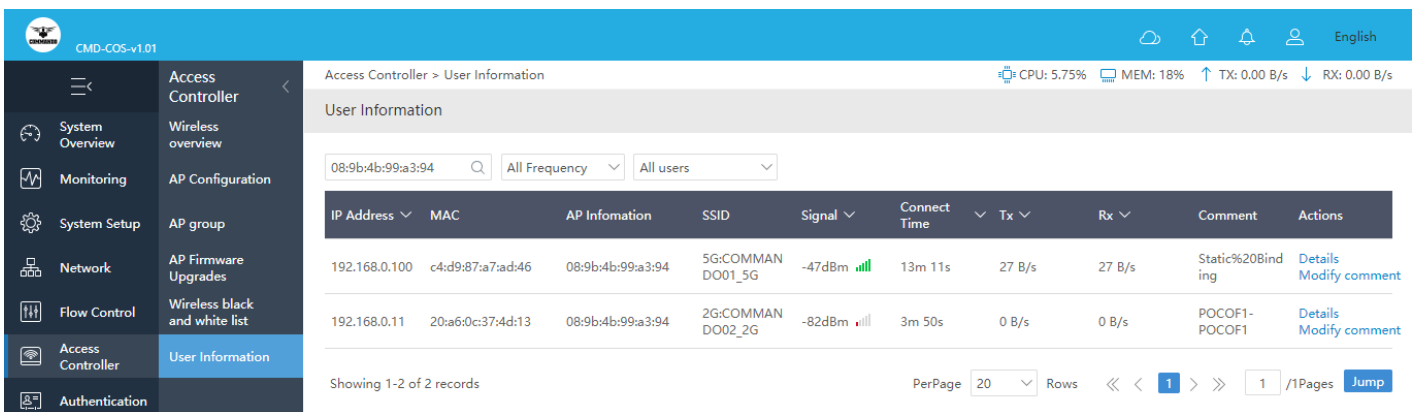


**Fig 5.2.5 Access Point Configuration Customized AP page**

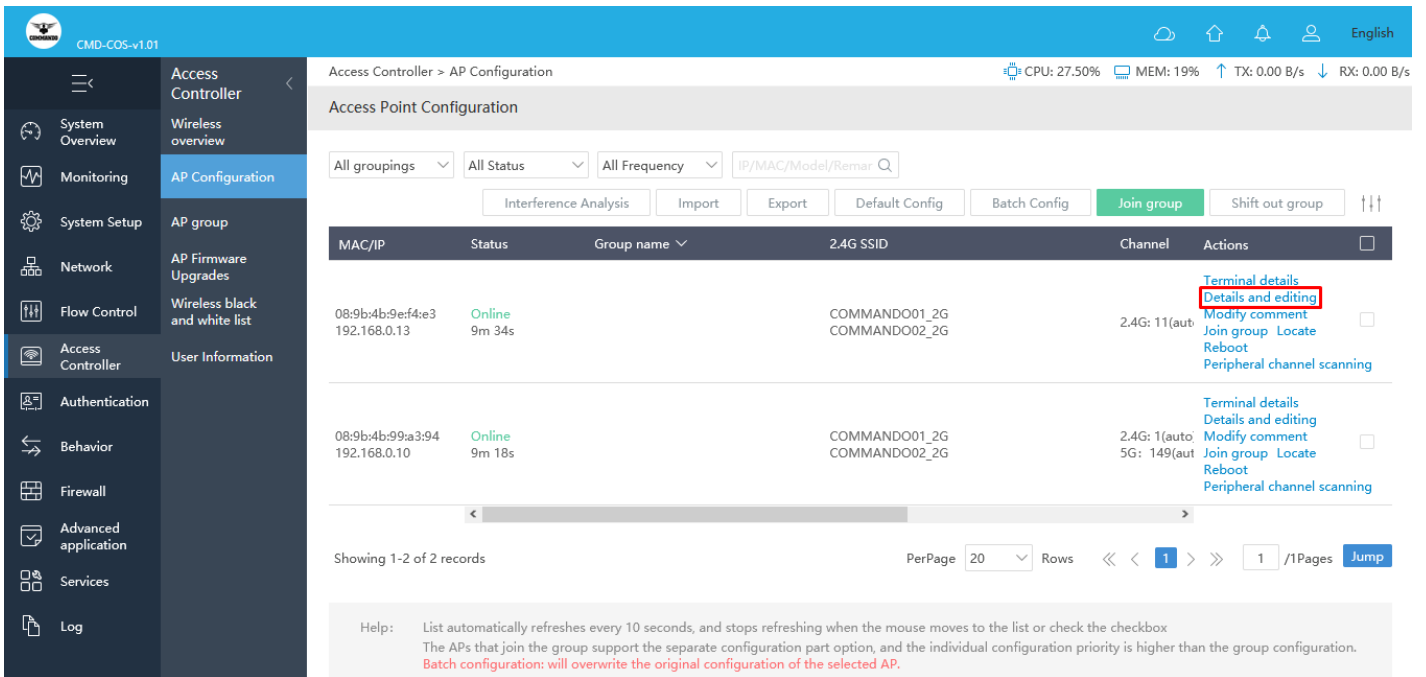


**Fig 5.2.6 Access Point Configuration Terminal Details page**

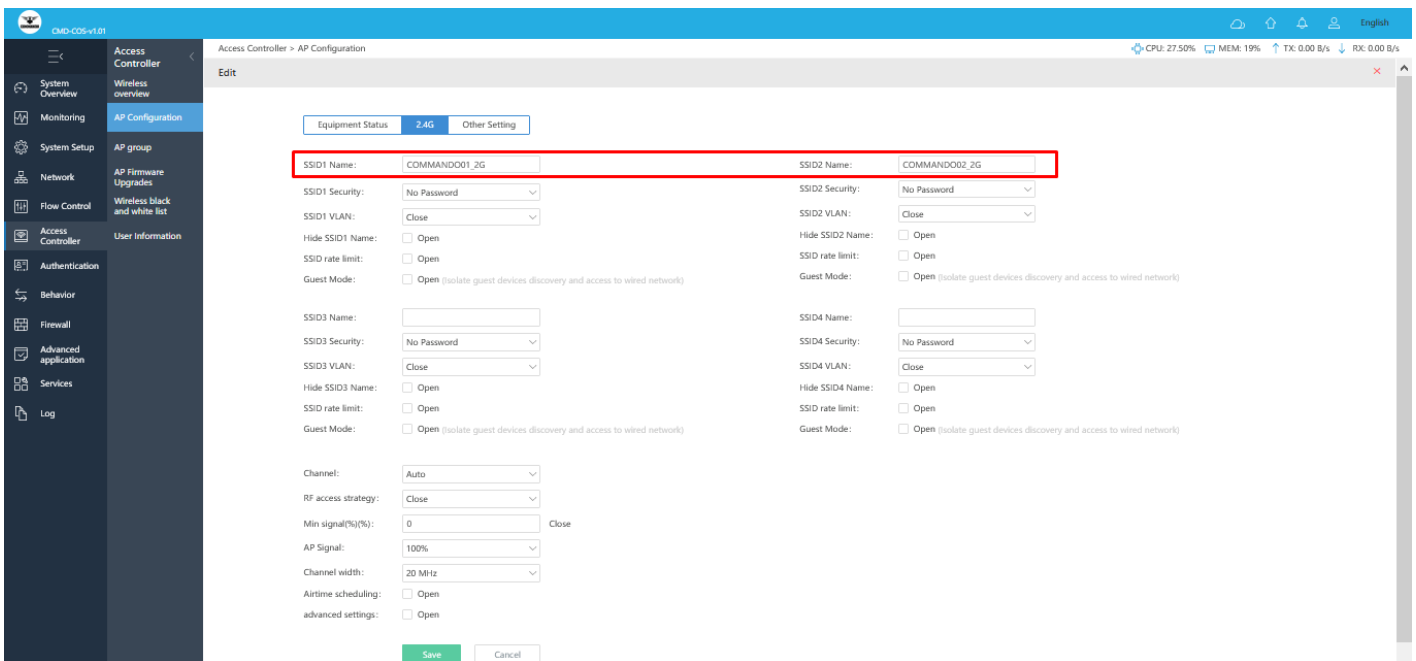
After clicking above highlighted icon you will be directed to User Information page as if you clicked Access Controller > User Information for particular AP page will be displayed.



**Fig 5.2.7 Access Point Configuration Terminal Details page**



**Fig 5.2.8 Details and editing AP Configuration page**



**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.

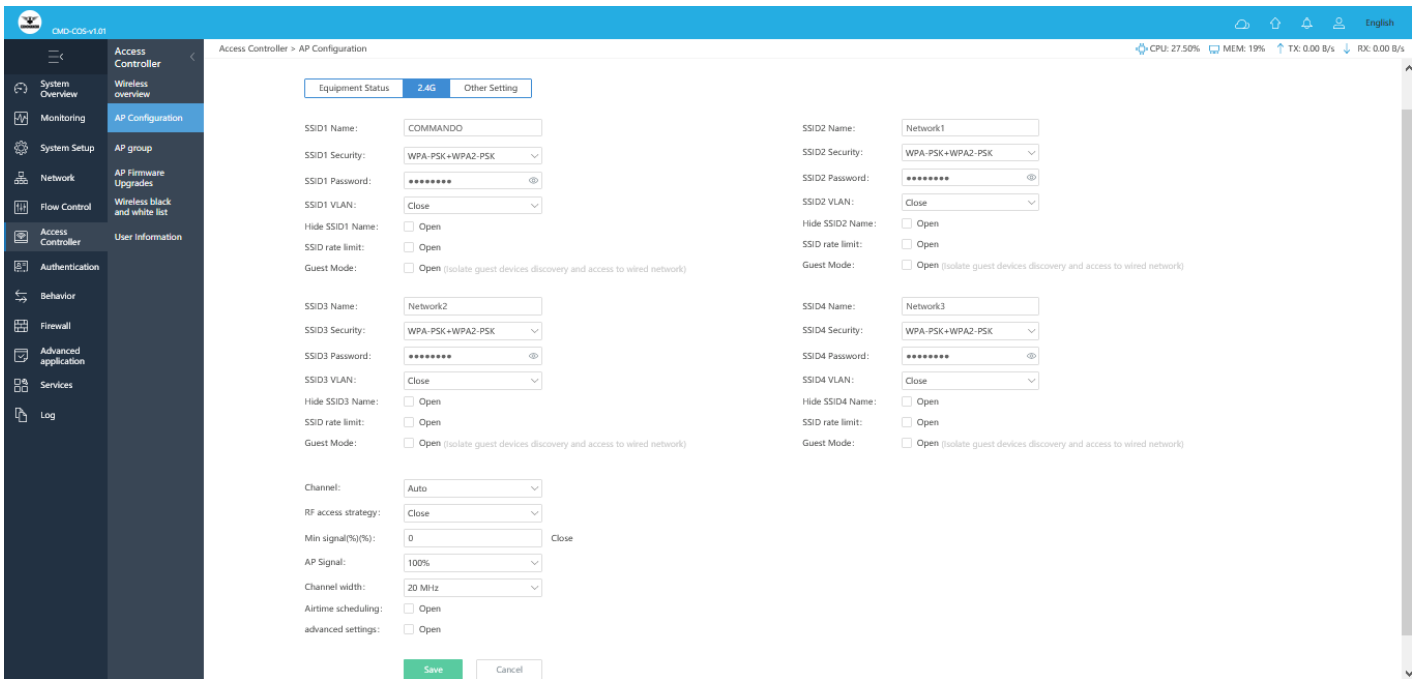


Fig 5.2.10 Changing SSID Configuration page

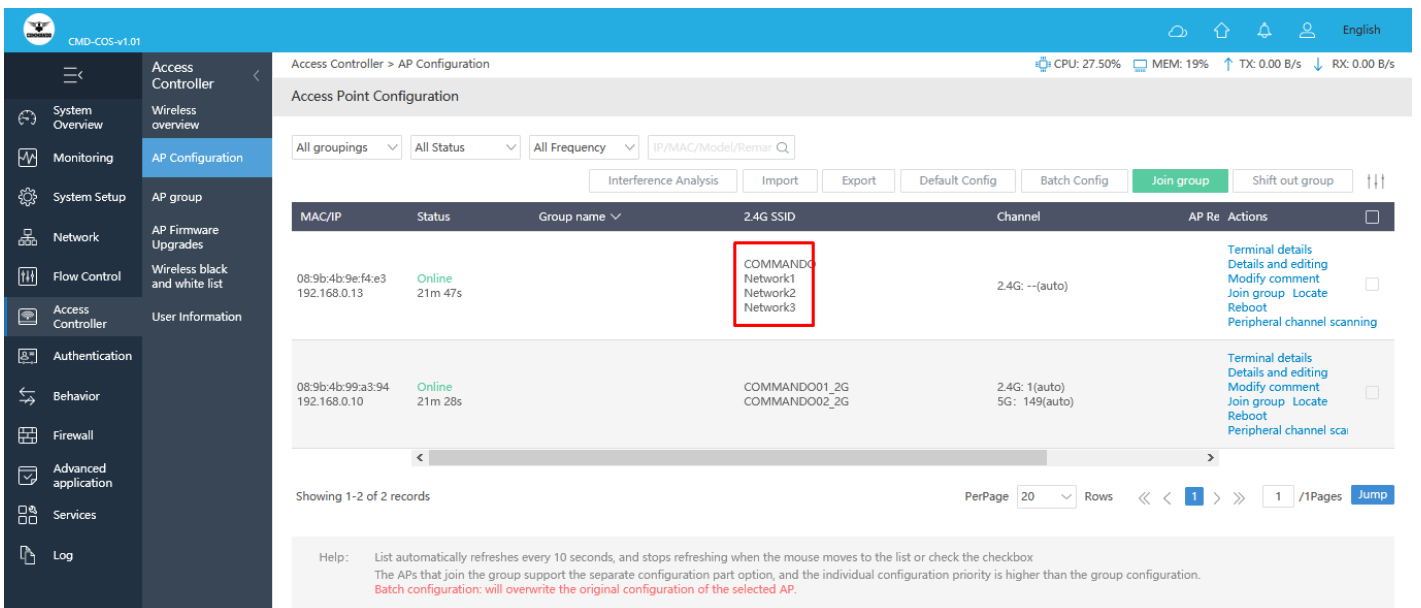
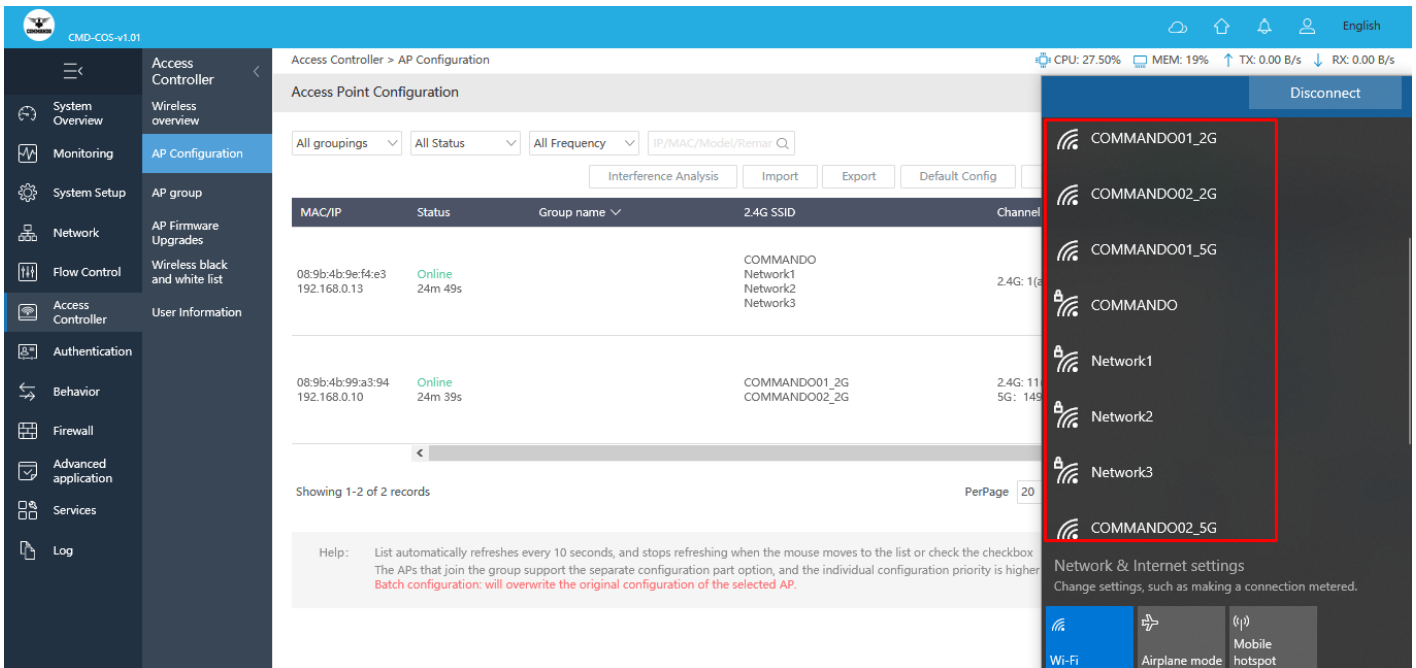


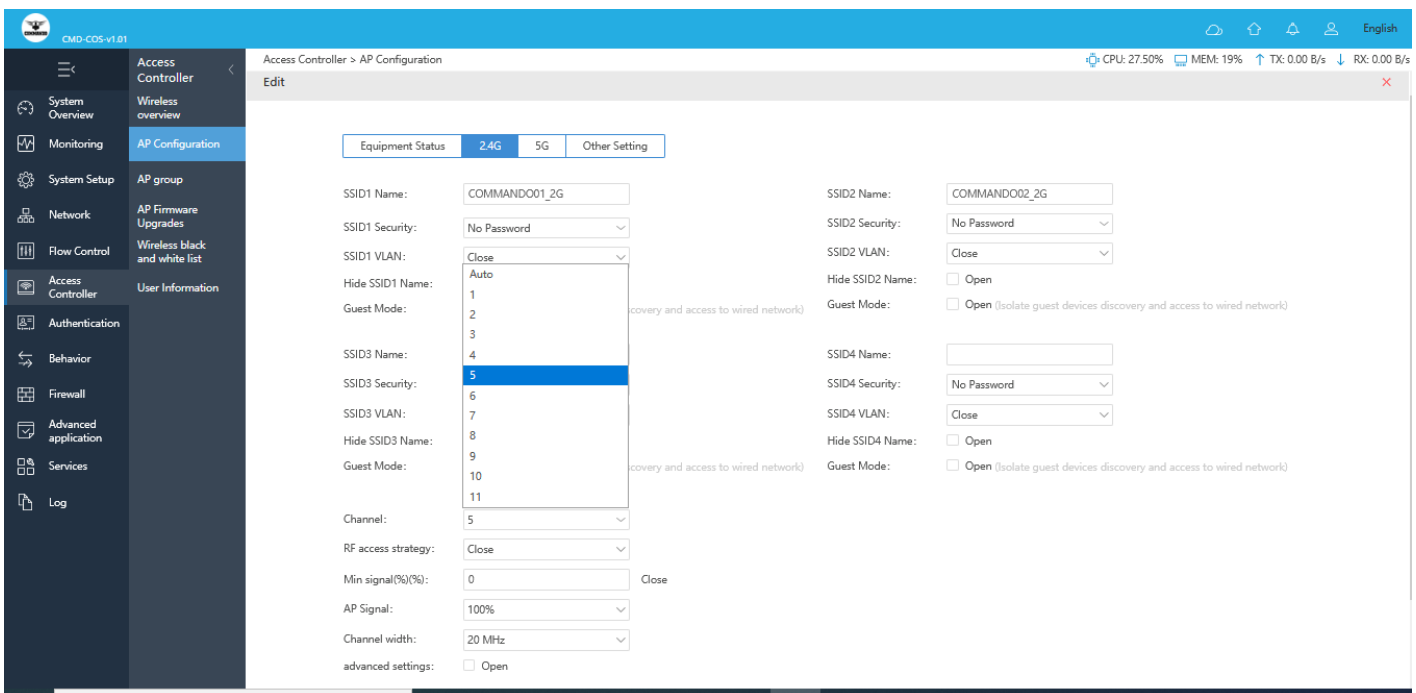
Fig 5.2.11 AP configuration after Changing SSID Configuration page



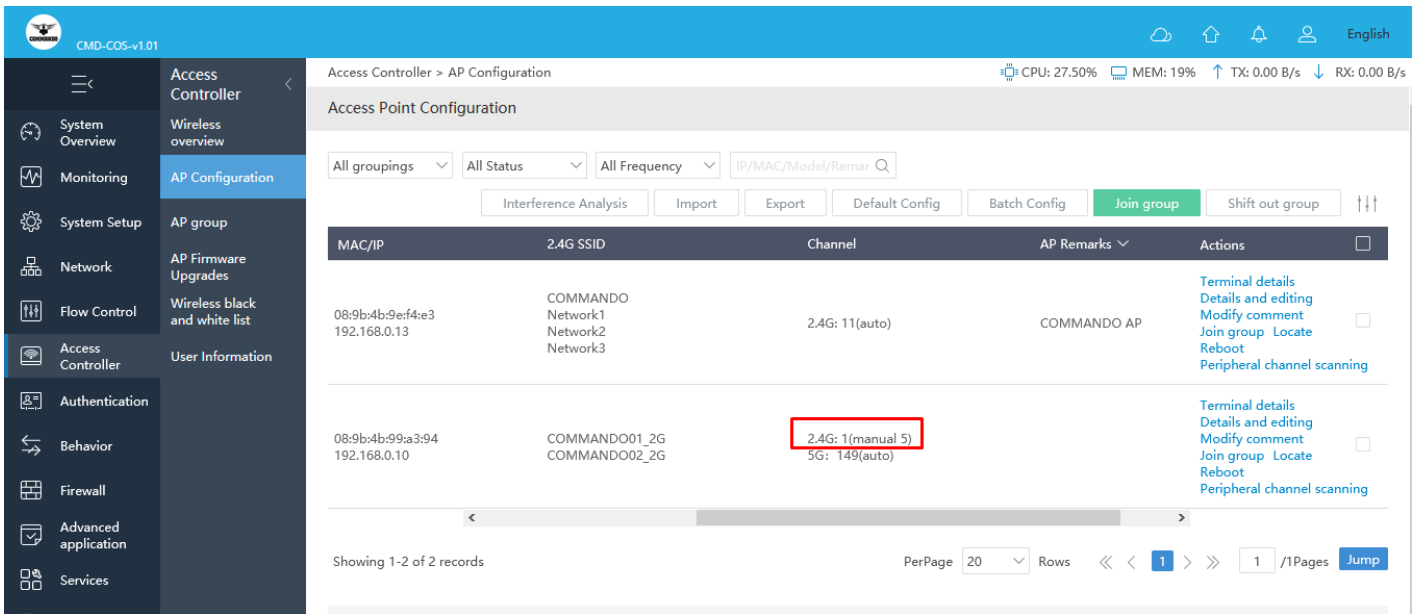
**Fig 5.2.12 SSID available for users page**

### 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 5.2.12 Changing Channel for SSID page**



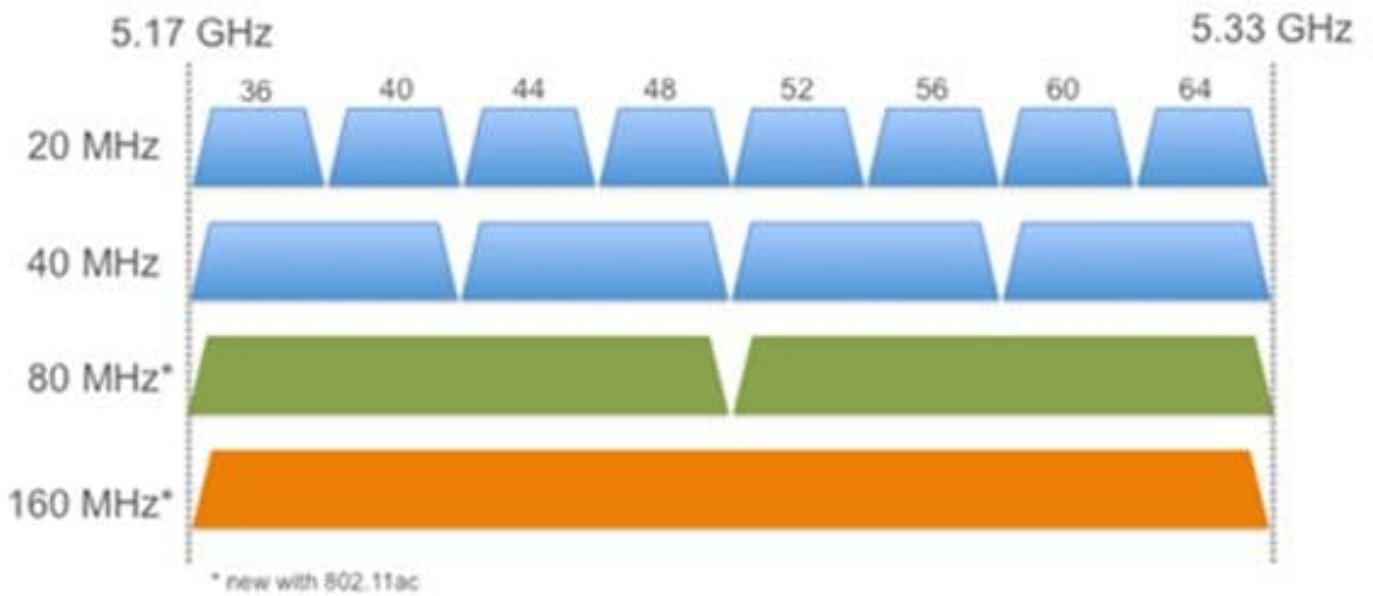
**Fig 5.2.13 Manual Channel for AP configuration page**

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

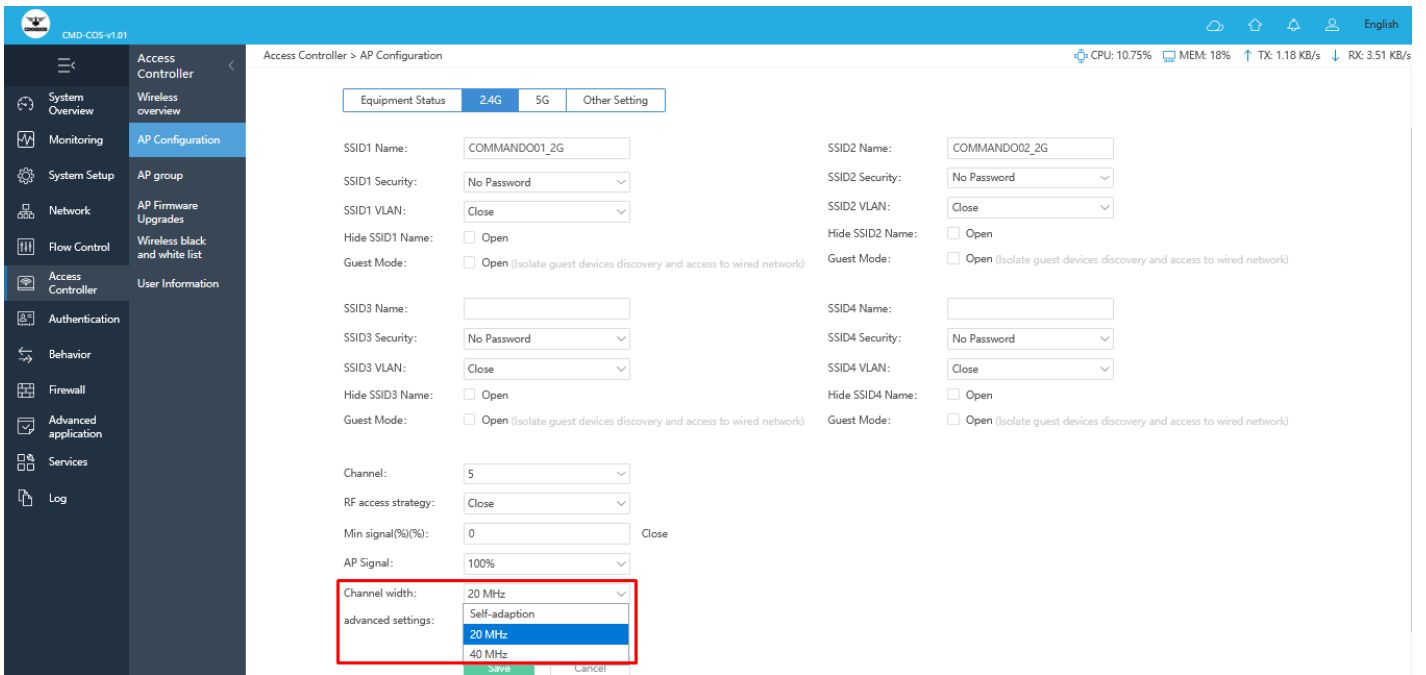


## 5 GHz Channelization

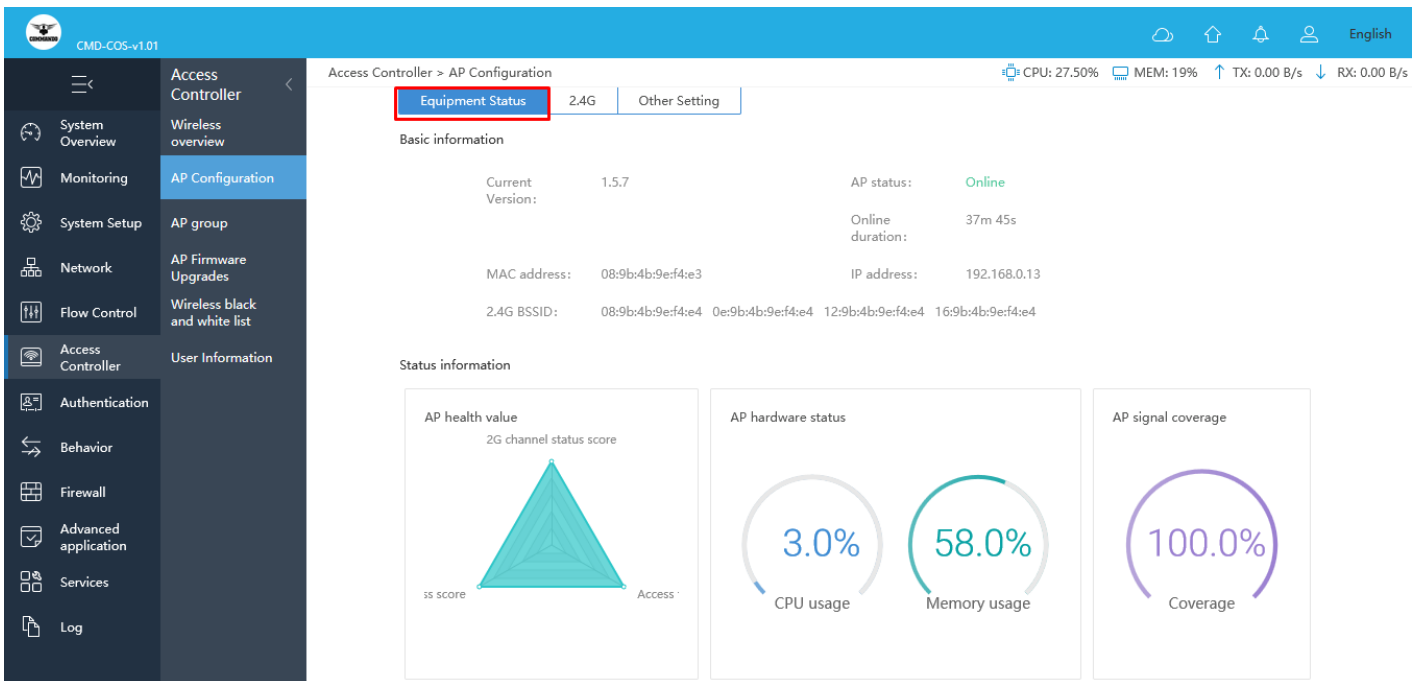


# Spatial Streams	Channel Width			
	20 MHz	40 MHz	80 MHz	160 MHz
1	86 Mbps	200 Mbps	433 Mbps	866 Mbps
2	173 Mbps	400 Mbps	866 Mbps	1.73 Gbps
3	288.9 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps
4	346.7 Mbps	800 Mbps	1.73 Gbps	3.46 Gbps

**Fig 5.2.14 Channel Width and Max. Data rate relation**



**Fig 5.2.15 Changing Channel Width for AP configuration page**

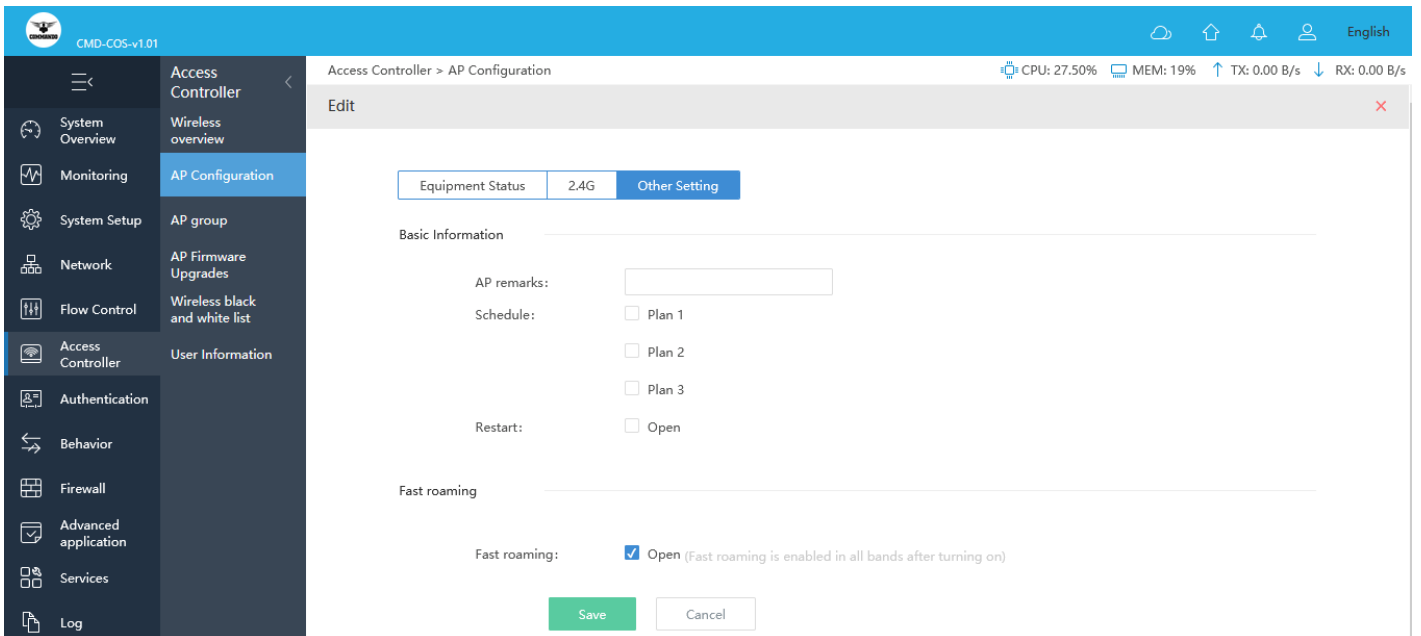




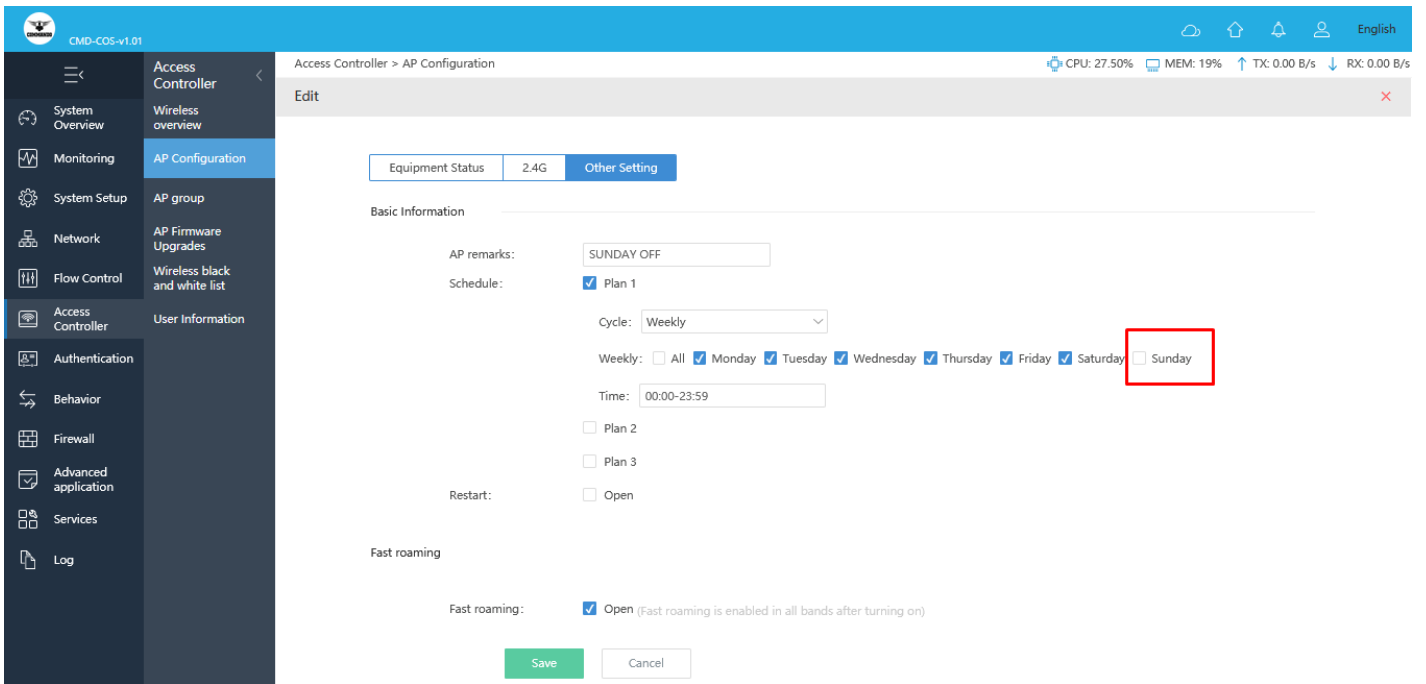
**Fig 5.2.16 Equipment Status of AP page**

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

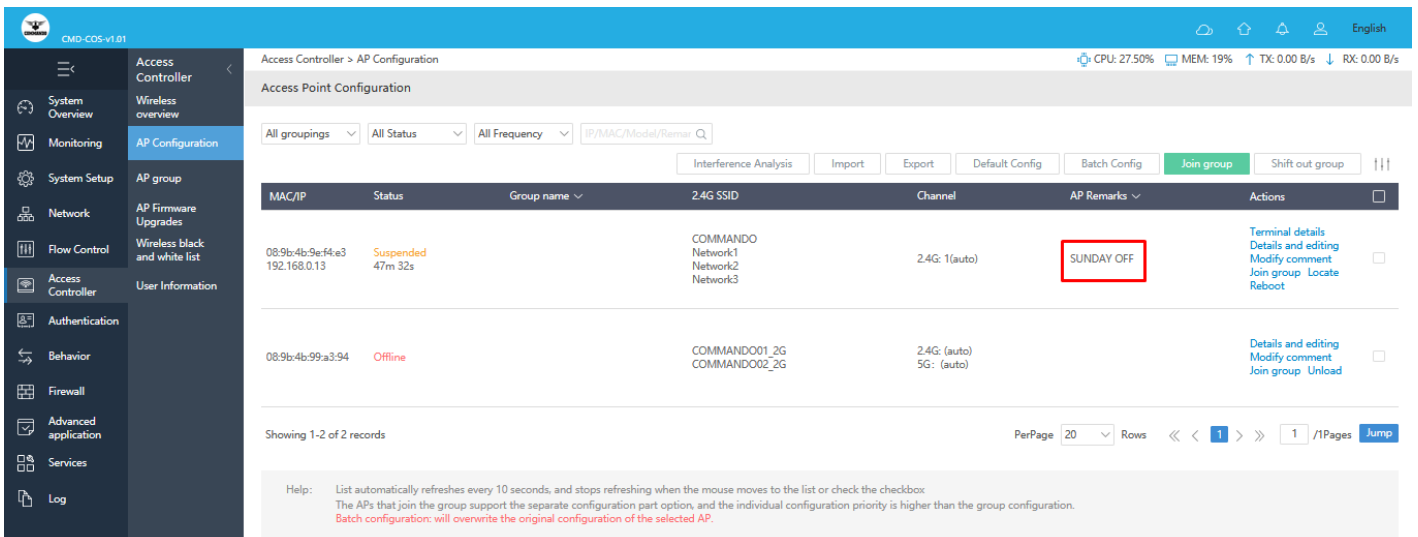
For changing Schedule timing of AP from all time to restricted timing and secure Wi-Fi network from unauthorized access, click on Access Controller > AP Configuration click other setting and Edit Plan as per requirement.



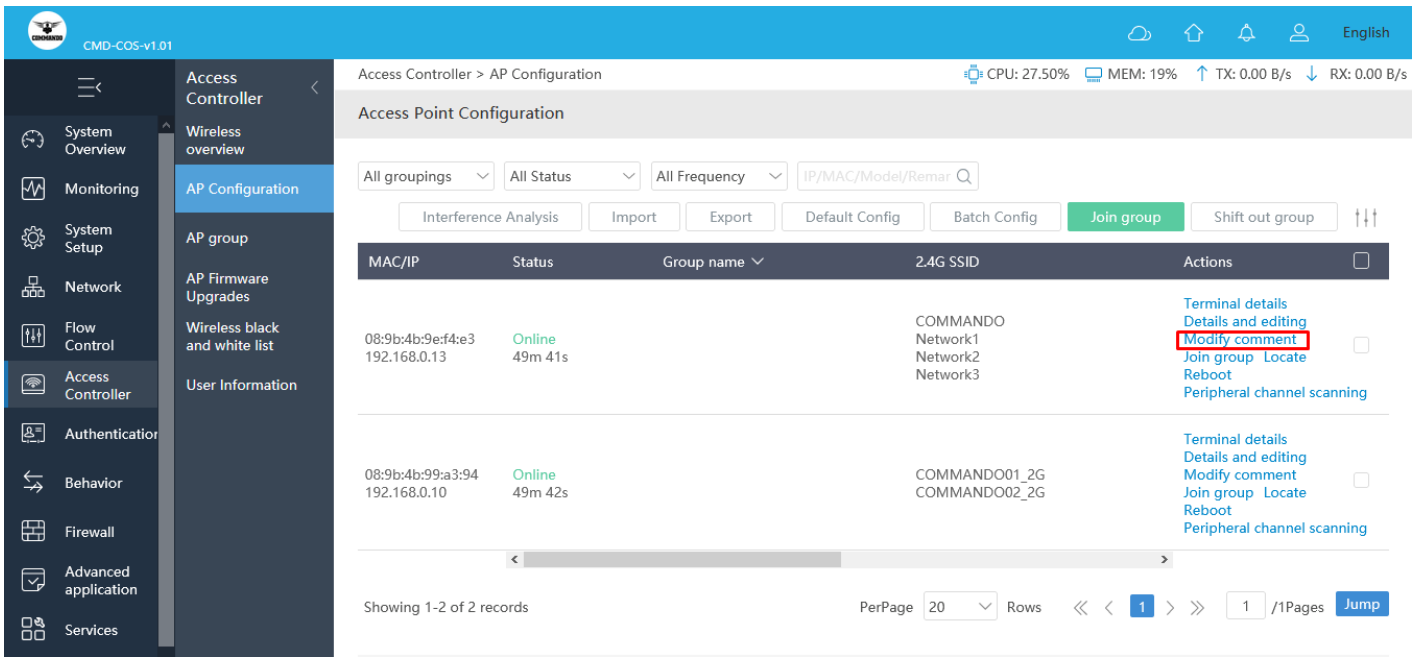
**Fig 5.2.17 Default Other Setting of AP configuration page**



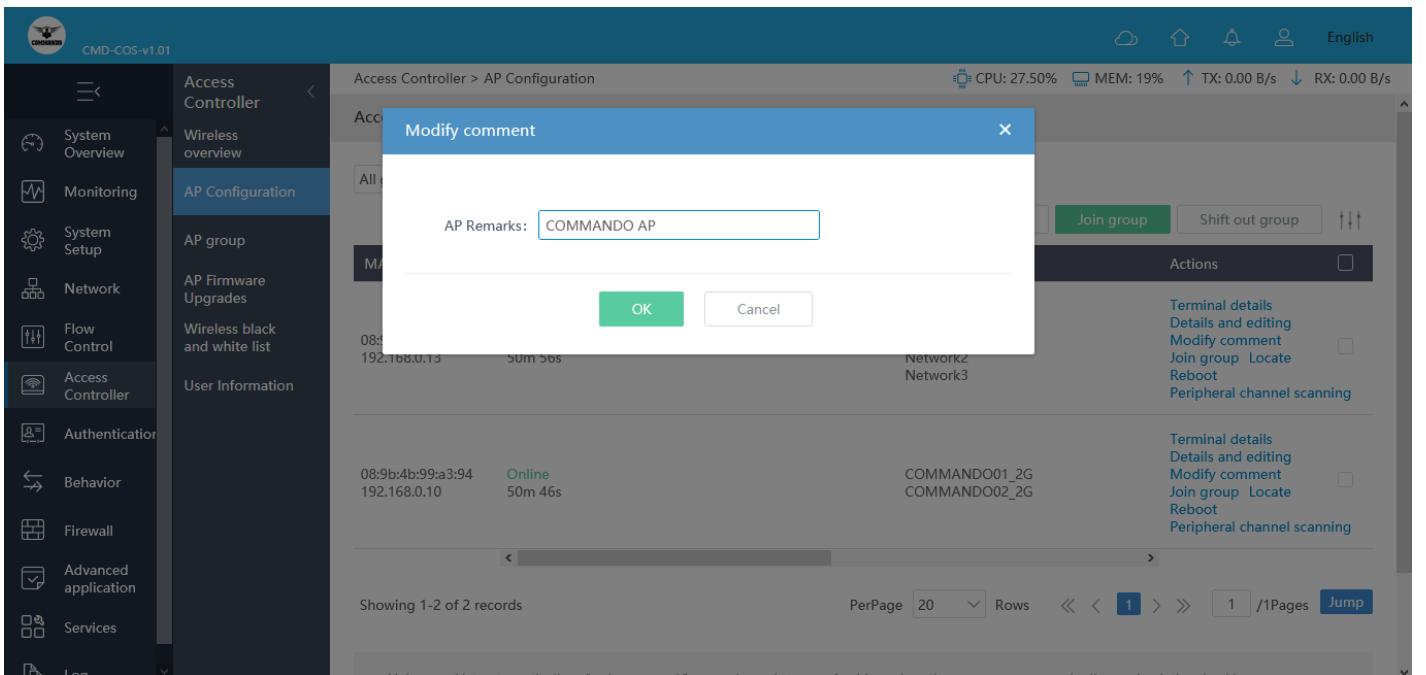
**Fig 5.2.18 Other Setting of AP configuration to turn OFF Wi-Fi on Sunday page**



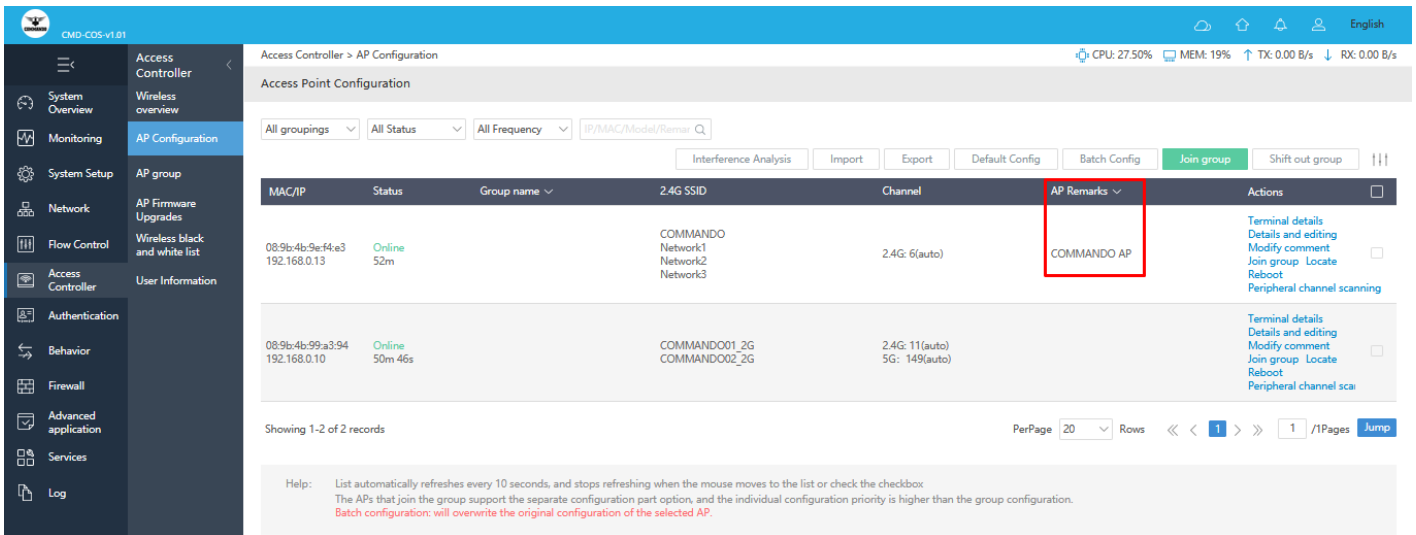
**Fig 5.2.19 AP configuration to turn OFF Wi-Fi on Sunday page**



**Fig 5.2.20 Modify Comment page**

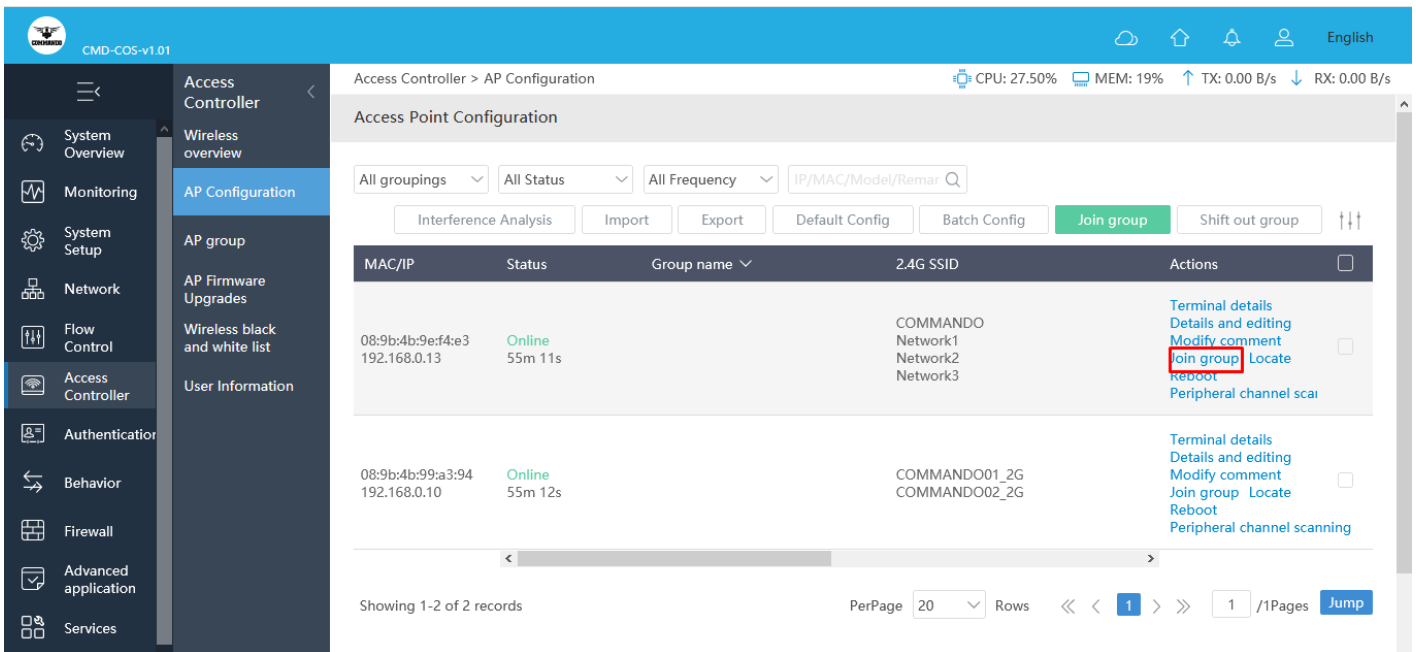


**Fig 5.2.21 Changing Modify Comment page**



**Fig 5.2.22 AP Remark after Modify Comment page**

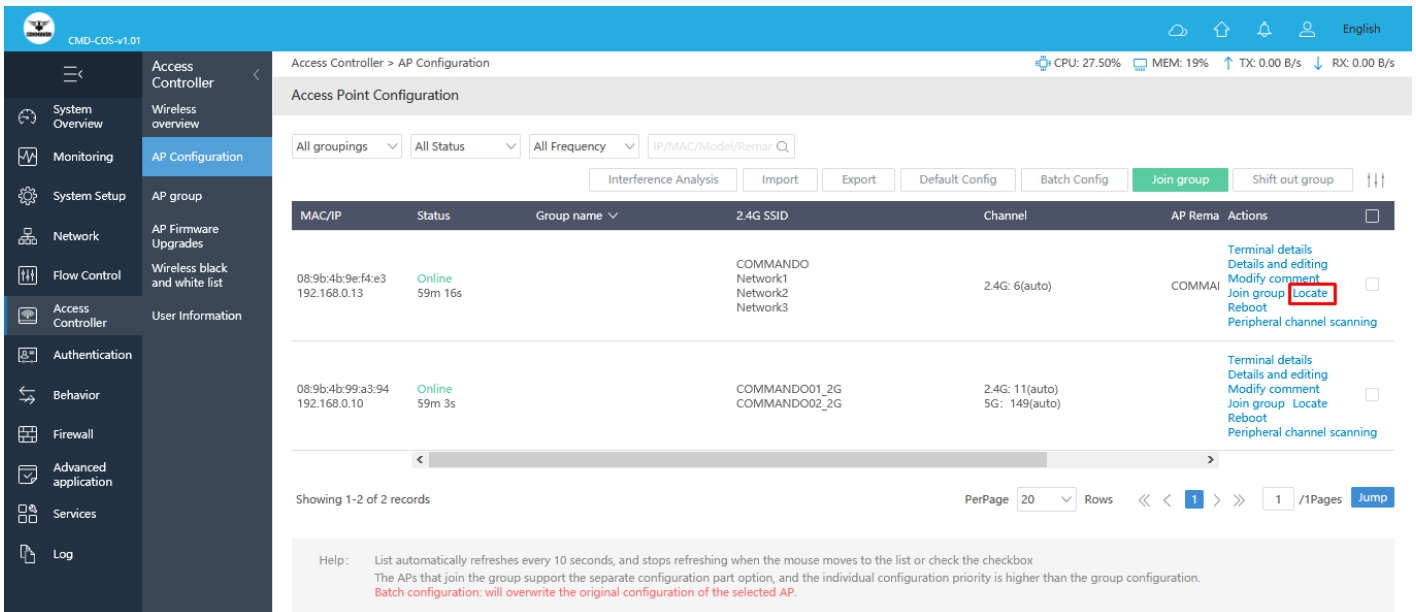
After joining the group, the group configuration will be used, and the AP original configuration will be restored after the group is removed.



**Fig 5.2.23 Default Join group page**

**Note:**

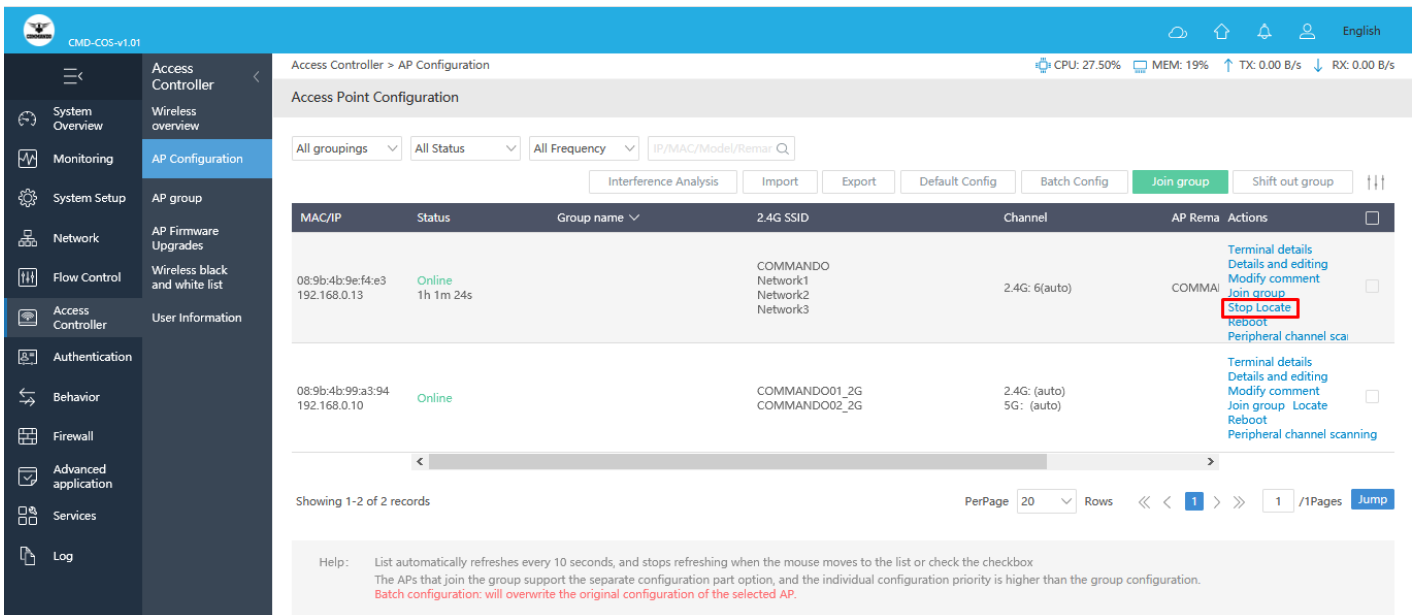
Above page will be Editable after creating AP Group only



**Fig 5.2.24 Default Locate AP page**

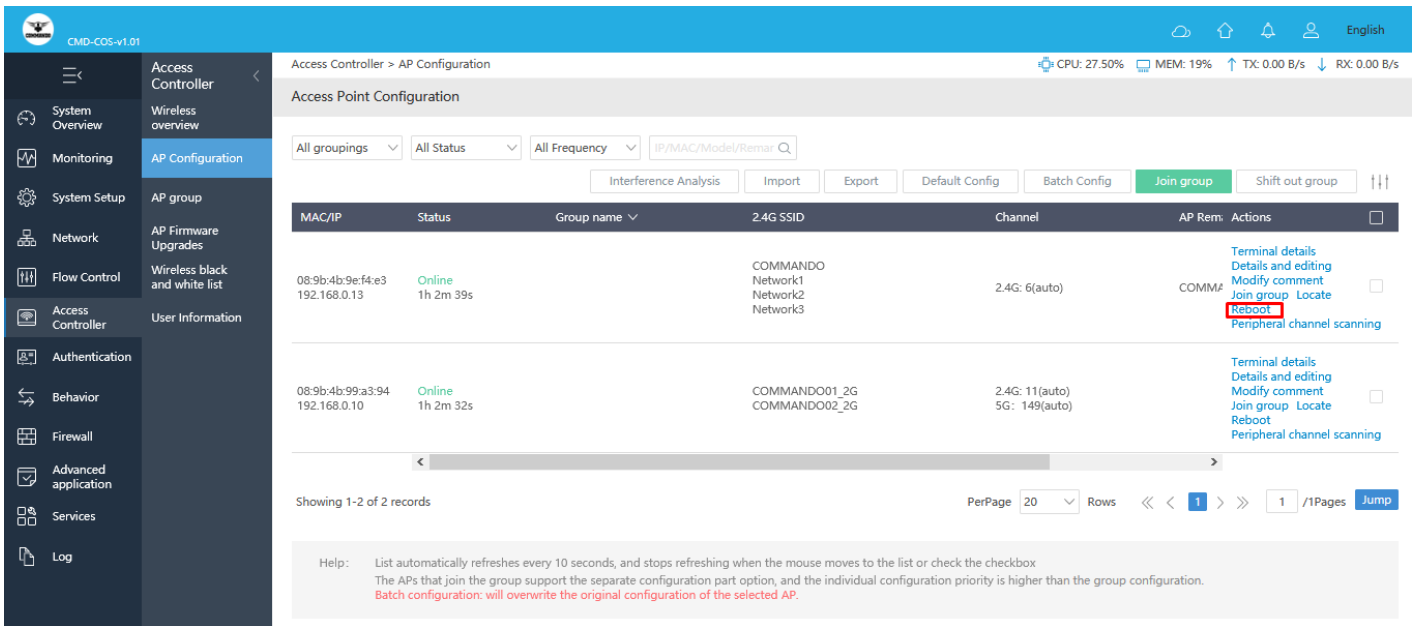
**Note:**

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.

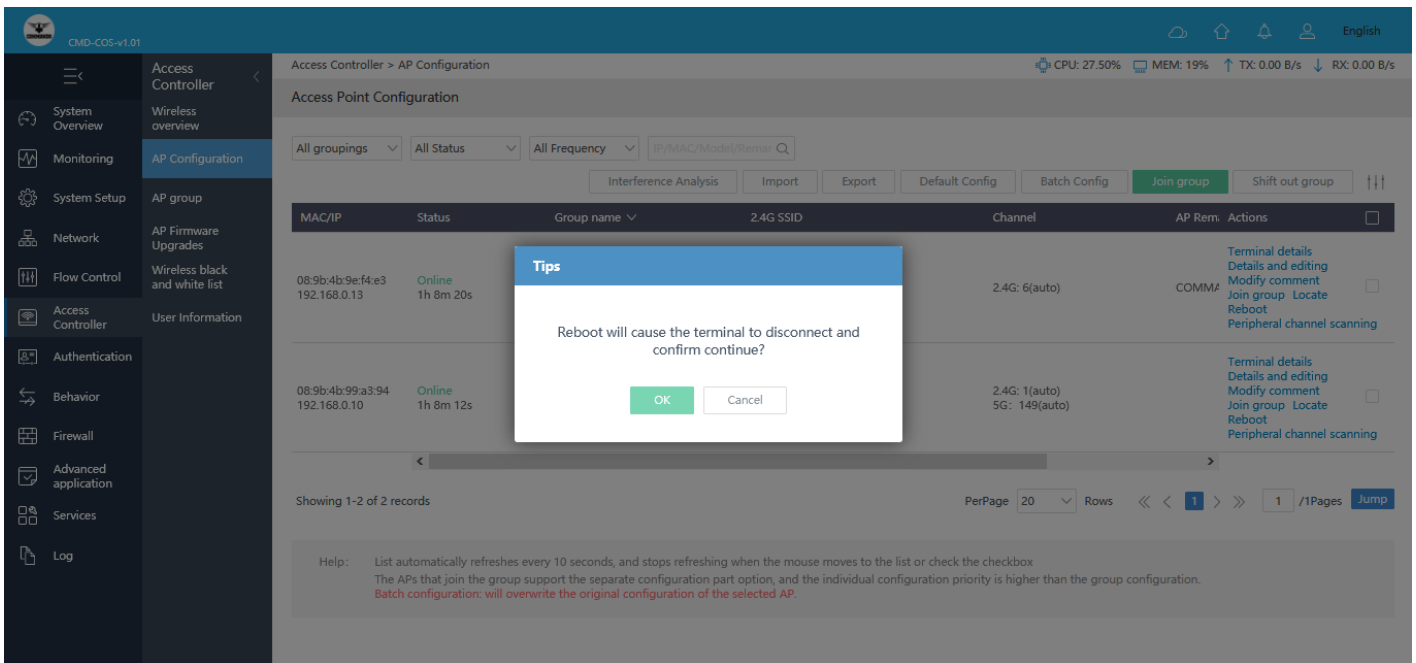


**Fig 5.2.25 For Locate particular AP page**

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:**

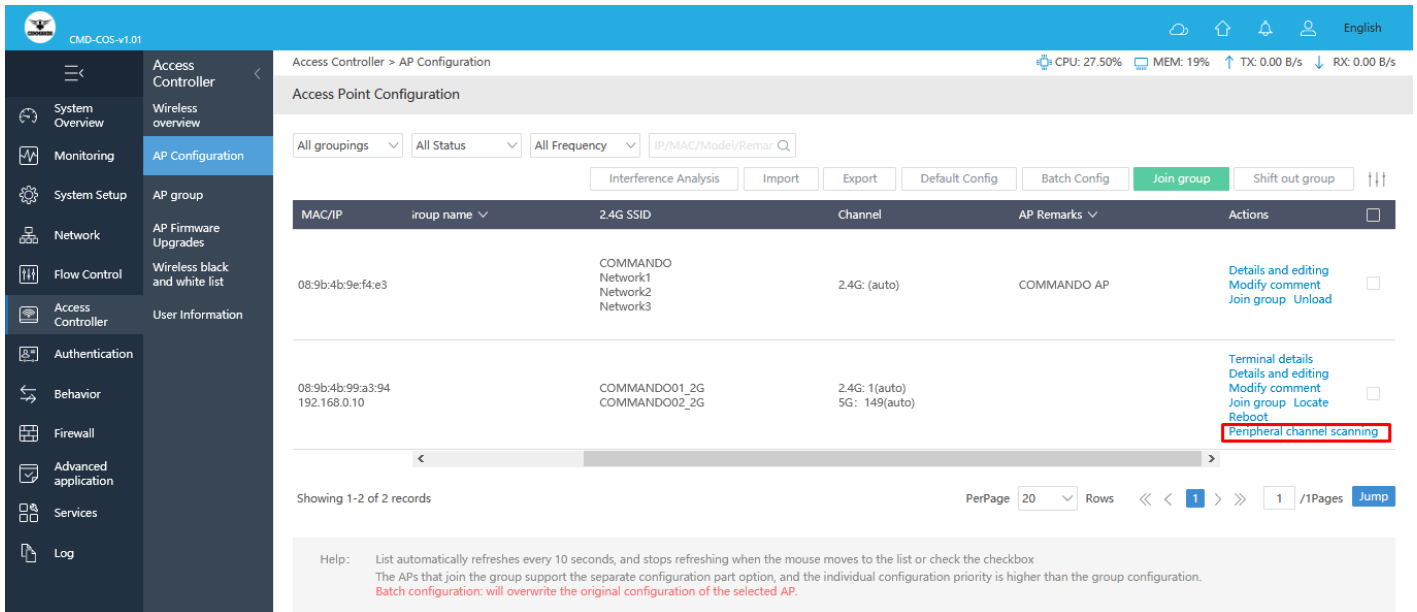
The scanning process consists in actively probing the radio channels to gather access points information.

**Note:**

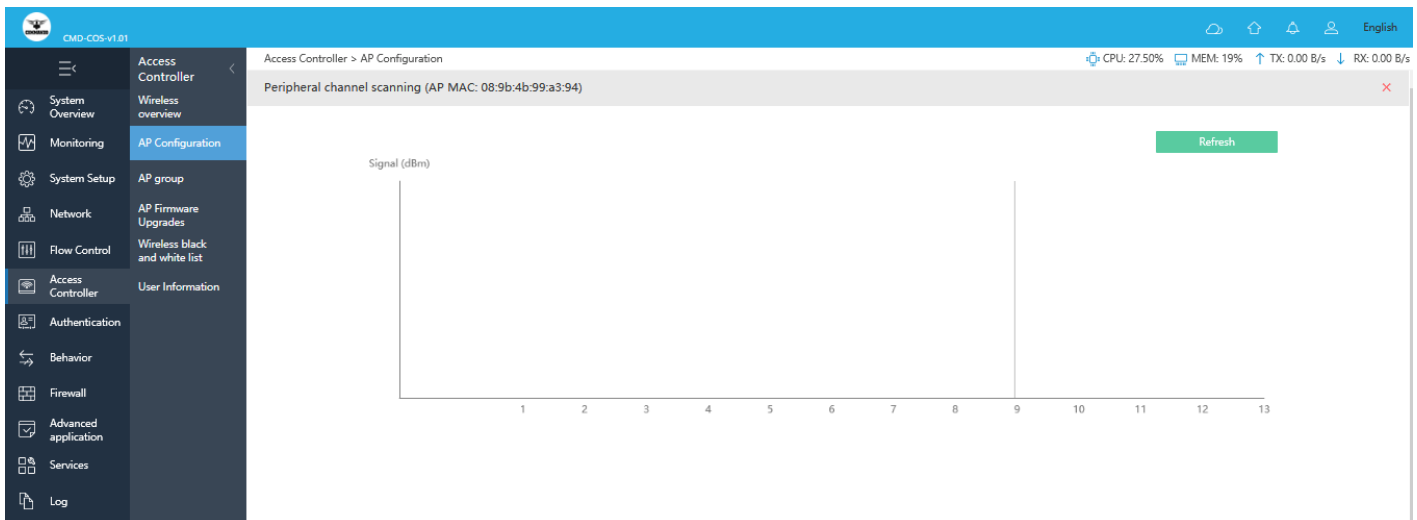
1. Please select AP for signal scanning.
2. The signal strength is negative, the larger the value, the stronger the signal



3. 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

Access Controller > AP group

CPU: 2.75% MEM: 16% 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
No Data					

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

### 5.3.1 Default AP Group page

Access Controller > AP group

Edit

Group name:

Follow group configuration:  Open

2.4G 5G Radio 1 5G Radio 2 Other Setting

2.4G Control state

SSID1 Name:

SSID1 Security:

SSID1 VLAN:

Hide SSID1 Name:  Open

SSID rate limit:  Open

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

SSID2 Name:

SSID2 Security:

SSID2 VLAN:

Hide SSID2 Name:  Open

SSID rate limit:  Open

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

SSID3 Name:

SSID3 Security:

SSID3 VLAN:

Hide SSID3 Name:  Open

SSID rate limit:  Open

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

SSID4 Name:

SSID4 Security:

SSID4 VLAN:

Hide SSID4 Name:  Open

SSID rate limit:  Open

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

Channel:  (1.5.6 and above versions support 12 and 13 channels)

RF access strategy:

Min signal(%)(N):  Close

AP Signal:

Channel width:

Airtime scheduling:  Open

advanced settings:  Open

Save Cancel

### 5.3.2 Default Edit AP Group page

CMD-COS-v1.01

Access Controller > AP group

CPU: 0.50% MEM: 17% TX: 3.89 KB/s RX: 9.23 KB/s

Group name:

Follow group configuration:  Open

2.4G 5G Radio 1 5G Radio 2 Other Setting

2.4G Control state

SSID1 Name: <input type="text" value="Net1"/>	SSID2 Name: <input type="text" value="Net2"/>
SSID1 Security: <input type="text" value="WPA-PSK+WPA2-PSK"/>	SSID2 Security: <input type="text" value="WPA-PSK+WPA2-PSK"/>
SSID1 Password: <input type="password" value="*****"/>	SSID2 Password: <input type="password" value="*****"/>
SSID1 VLAN: <input type="text" value="Open"/>	SSID2 VLAN: <input type="text" value="Open"/>
SSID1 VLAN_ID: <input type="text" value="1"/>	SSID2 VLAN_ID: <input type="text" value="3"/>
Hide SSID1 Name: <input type="checkbox"/> Open	Hide SSID2 Name: <input type="checkbox"/> Open
SSID rate limit: <input type="checkbox"/> Open	SSID rate limit: <input type="checkbox"/> Open
Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>	Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>

CMD-COS-v1.01

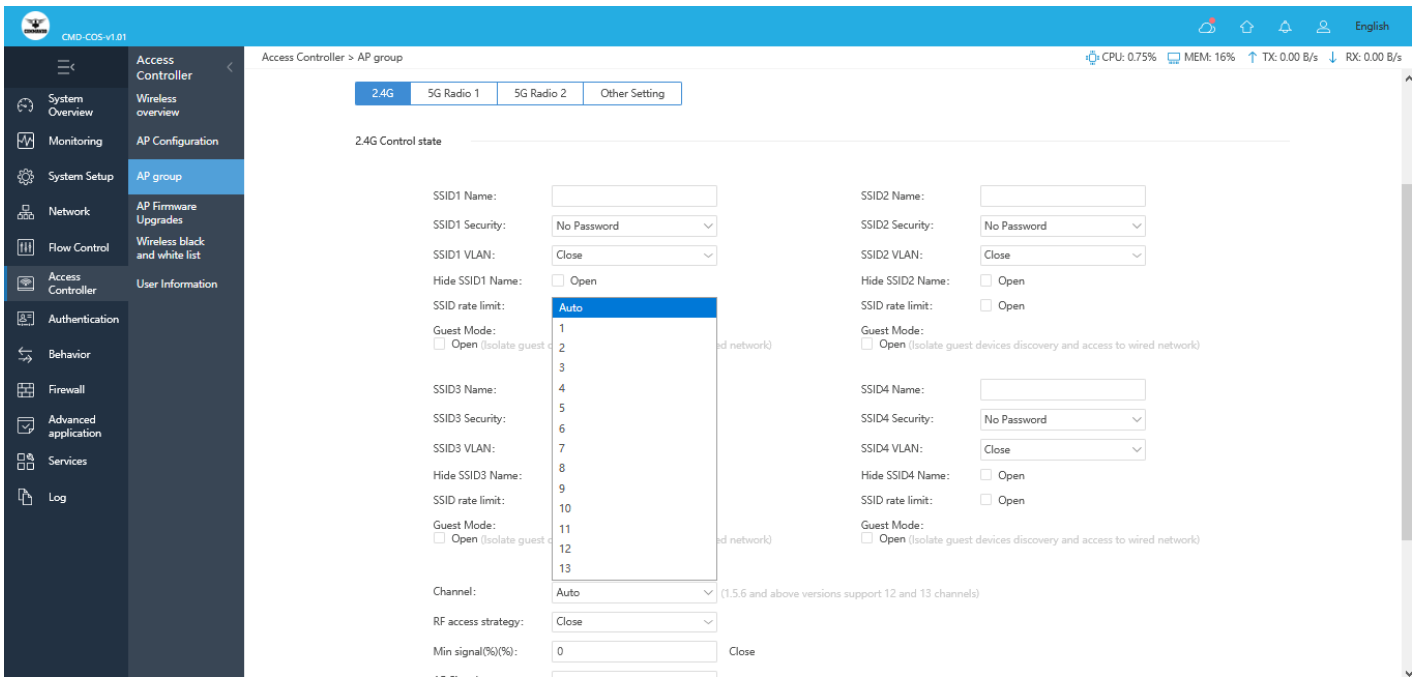
Access Controller > AP group

CPU: 0.99% MEM: 17% TX: 60.00 B/s RX: 60.00 B/s

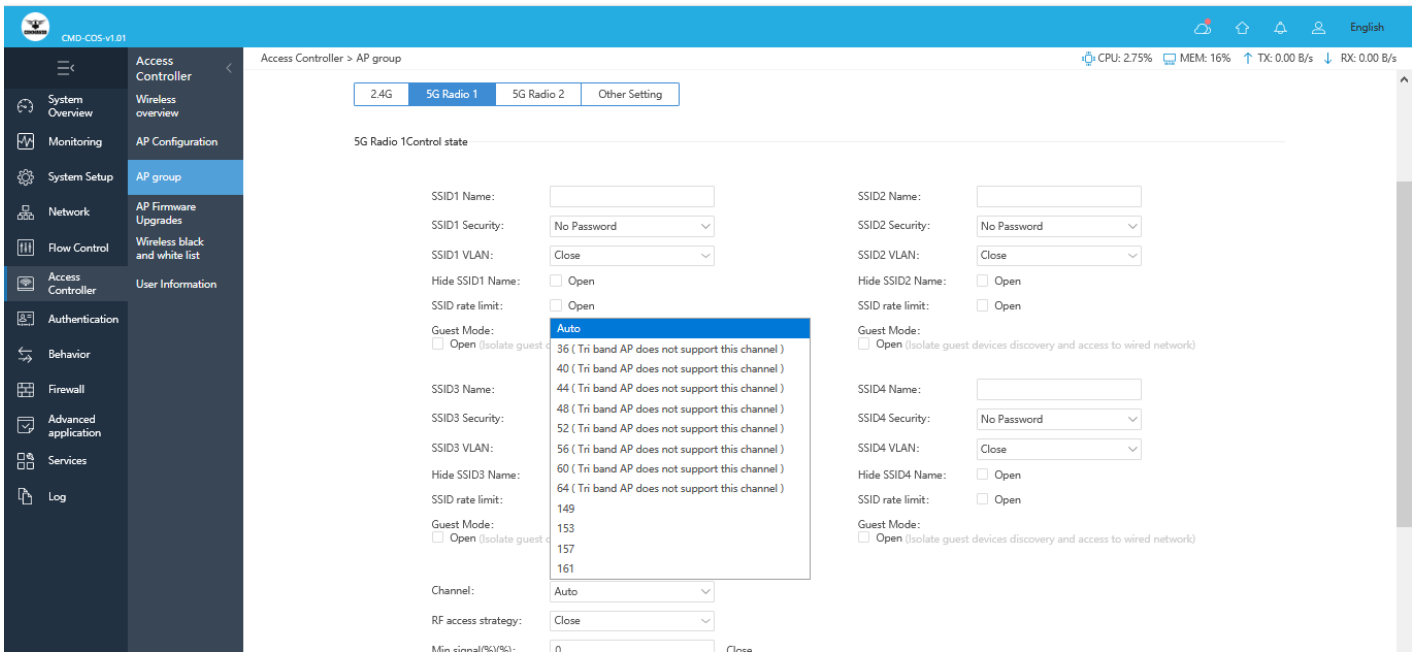
SSID1 Name: <input type="text" value="Net1"/>	SSID2 Name: <input type="text" value="Net2"/>
SSID1 Security: <input type="text" value="WPA-PSK+WPA2-PSK"/>	SSID2 Security: <input type="text" value="WPA-PSK+WPA2-PSK"/>
SSID1 Password: <input type="password" value="*****"/>	SSID2 Password: <input type="password" value="*****"/>
SSID1 VLAN: <input type="text" value="Open"/>	SSID2 VLAN: <input type="text" value="Open"/>
SSID1 VLAN_ID: <input type="text" value="1"/>	SSID2 VLAN_ID: <input type="text" value="3"/>
Hide SSID1 Name: <input type="checkbox"/> Open	Hide SSID2 Name: <input type="checkbox"/> Open
SSID rate limit: <input type="checkbox"/> Open	SSID rate limit: <input type="checkbox"/> Open
Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>	Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>
SSID3 Name: <input type="text"/>	SSID4 Name: <input type="text"/>
SSID3 Security: <input type="text" value="No Password"/>	SSID4 Security: <input type="text" value="No Password"/>
SSID3 VLAN: <input type="text" value="Close"/>	SSID4 VLAN: <input type="text" value="Close"/>
Hide SSID3 Name: <input type="checkbox"/> Open	Hide SSID4 Name: <input type="checkbox"/> Open
SSID rate limit: <input type="checkbox"/> Open	SSID rate limit: <input type="checkbox"/> Open
Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>	Guest Mode: <input type="checkbox"/> Open <small>(Isolate guest devices discovery and access to wired network)</small>
Channel: <input type="text" value="11"/> <small>(1.5.6 and above versions support 12 and 13 channels)</small>	
RF access strategy: <input type="text" value="Close"/>	
Min signal(%): <input type="text" value="0"/> <small>Close</small>	
AP Signal: <input type="text" value="100%"/>	
Channel width: <input type="text" value="40 MHz"/>	
Airtime scheduling: <input type="checkbox"/> Open	
advanced settings: <input type="checkbox"/> Open	

Save Cancel

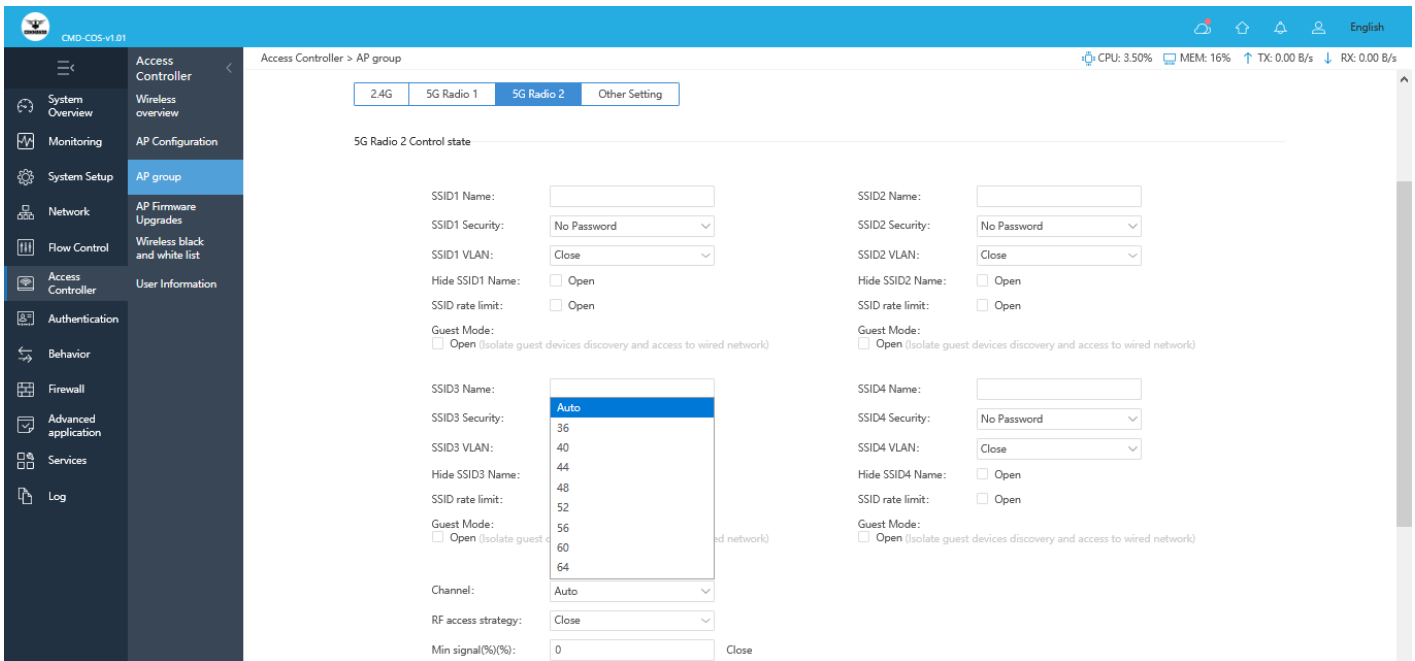
### 5.3.3 Edit AP Group page



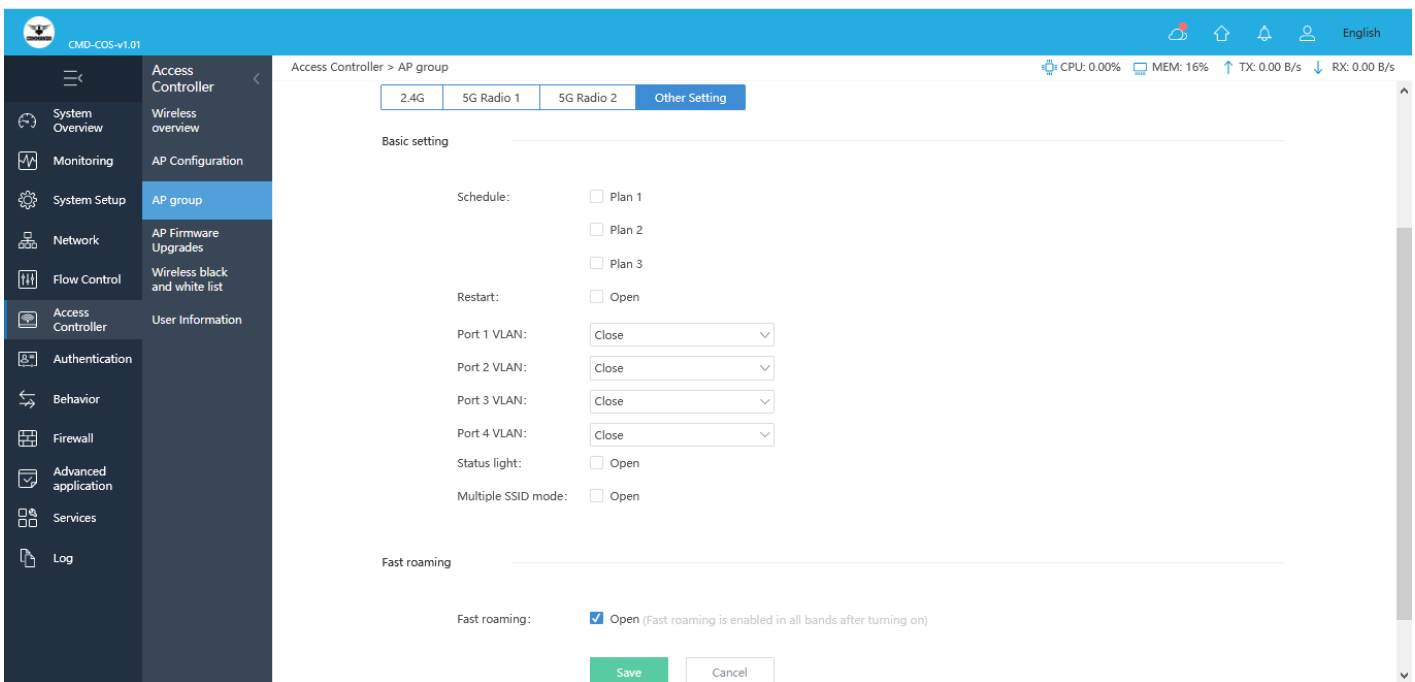
### 5.3.4 Group AP Channel selection in 2.4GHz page



### 5.3.5 Group AP Channel selection in 5GHz Radio1 page



### 5.3.6 Group AP Channel selection in 5GHz Radio2 page



### 5.3.7 Group AP Default Other setting page

The screenshot shows the 'Access Controller > AP group' page. 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 to show 'AP group'. The main content area displays a table with the following data:

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

Below the table, it shows 'Showing 1 of 1 records' and pagination controls. A help message states: 'The APs that join the group use the group configuration uniformly. After the packets are removed, the original AP configuration is restored.'

### 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.

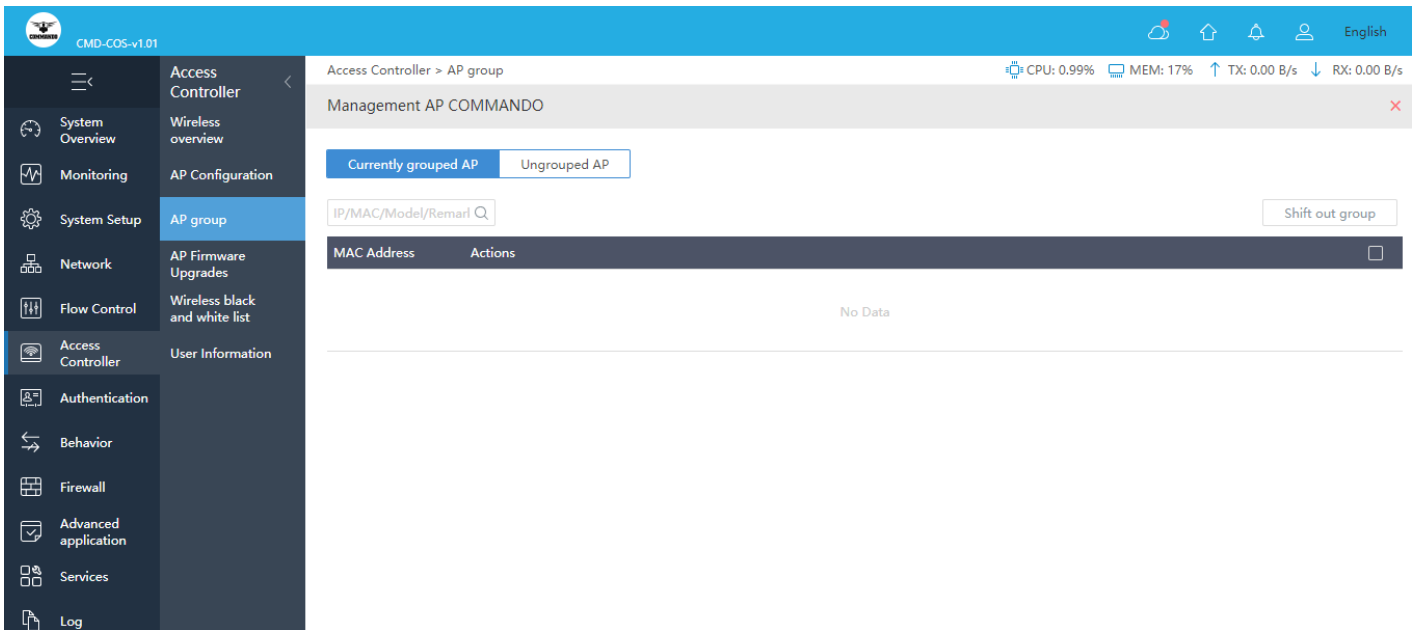
The screenshot shows the 'Access Controller > AP group' page after adding an AP. The table now shows 1 AP in the COMMANDO group. The 'Management AP' link in the Actions column is highlighted with a red box.

Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions
COMMANDO	1	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

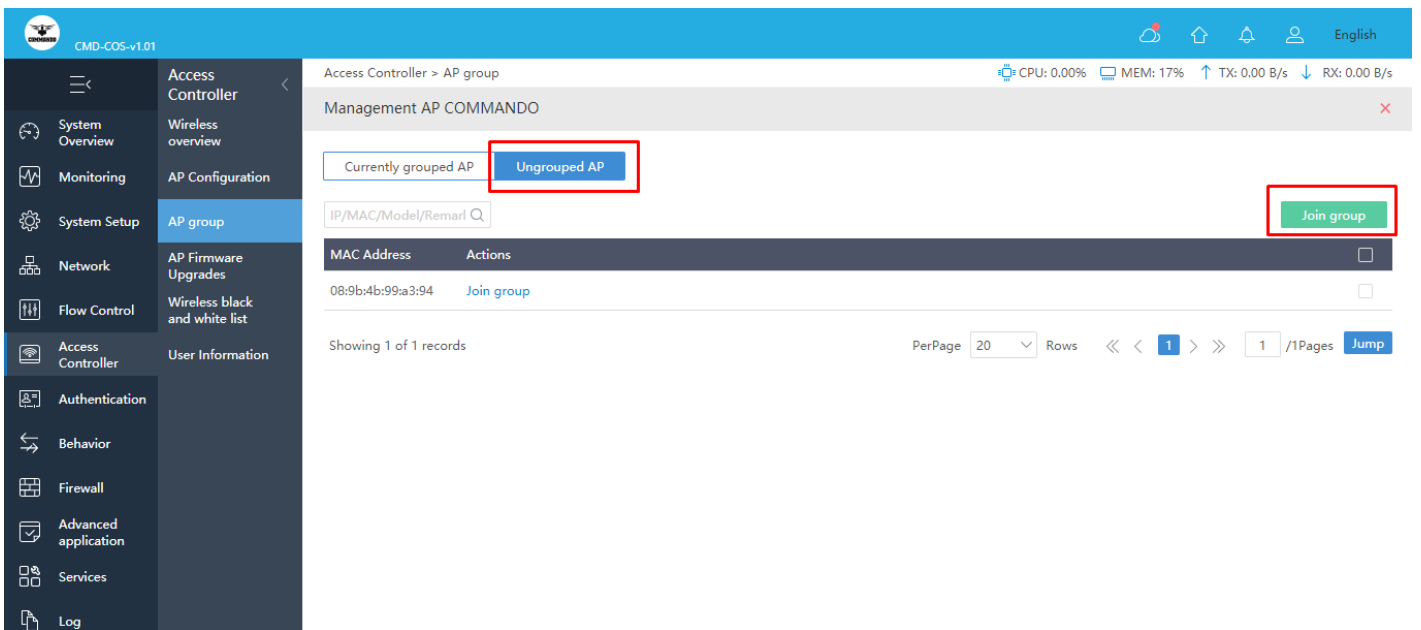
The rest of the page, including the sidebar and help message, remains the same as in the previous screenshot.

### 5.3.9 Management AP Group page

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



### 5.3.10 Default Management AP Group page



### 5.3.11 Join Management AP Group page

### 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



## 5.4.1 Default Upgrade firmware of Access Point page

Access Controller > AP Firmware Upgrades

CPU: 5.25% MEM: 17% TX: 27.00 B/s RX: 27.00 B/s

Access Point Upgrades

MAC/Model

Upgrade All Batch Upgrade

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions
08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade

Showing 1 of 1 records

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

## 5.4.2 Upgrade firmware of Access Point page

Access Controller > AP Firmware Upgrades

CPU: 0.50% MEM: 17% TX: 33.00 B/s RX: 33.00 B/s

Access Point Upgrades

MAC/Model

Upgrade All Batch Upgrade

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions
08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade

Showing 1 of 1 records

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

**Tips**

Are you sure to upgrade the firmware version of AP {0}?

OK Cancel

## 5.4.3 Upgrade firmware of selected Access Point page

CMD-COS-v1.01

Access Controller > AP Firmware Upgrades

CPU: 8.42% MEM: 18% TX: 27.00 B/s RX: 0.00 B/s

Access Point Upgrades

MAC/Model

Upgrade All Batch Upgrade

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions
08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade

Showing 1 of 1 records

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

**Upgrading.**

downloading (IK-X2) firmware: 1%

In the process of upgrading, please ensure that the power is kept and stop any other operations on AP!

[Hide](#)

## 5.4.4 Upgrading firmware of selected Access Point page

**Note:** After Upgrade AP will be restarted automatically.

CMD-COS-v1.01

Access Controller > AP Firmware Upgrades

CPU: 19.10% MEM: 21% TX: 27.00 B/s RX: 162.00 B/s

Access Point Upgrades

MAC/Model

Upgrade All Batch Upgrade

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions
No Data					

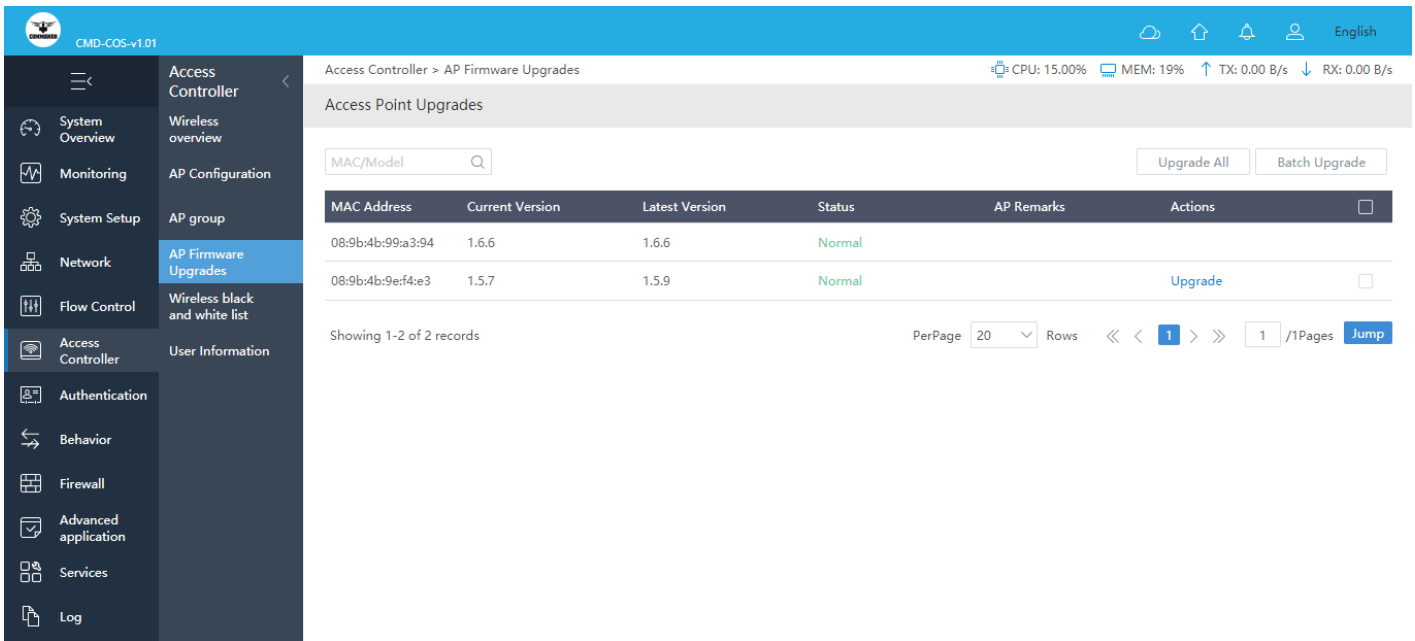
**Upgrading.**

Restart AP: 08:9b:4b:99:a3:94

In the process of upgrading, please ensure that the power is kept and stop any other operations on AP!

[Hide](#)

## 5.4.5 Upgrading firmware restarting Access Point page



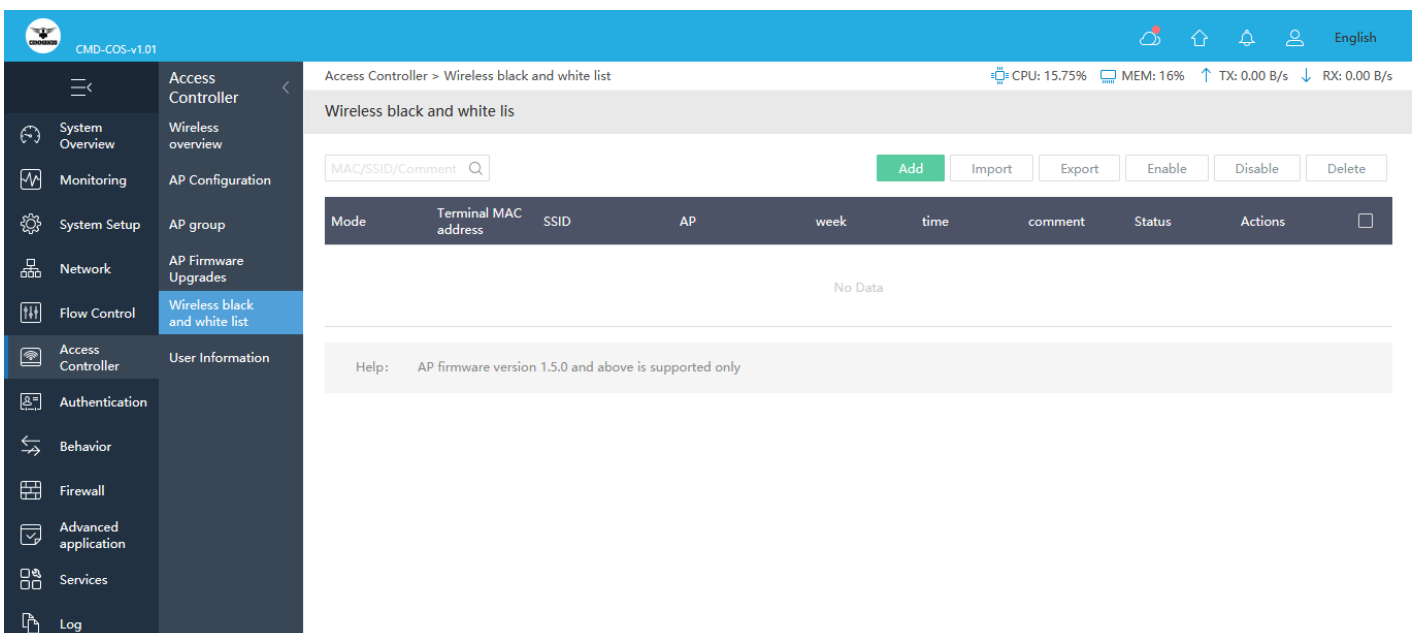
## 5.4.6 After Upgrading firmware Access Point Upgrade page

## 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



## 5.5.1 Default Wireless black and white list page

CMD-COS-v1.01

Access Controller > Wireless black and white list

**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:

SSID: 

- all
- COMMAND001\_2G
- COMMAND001\_5G
- COMMAND002\_2G
- COMMAND002\_5G

AP: 

- all

Week:  All  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Time:

Remarks:

## 5.5.2 Add Wireless black and white list page

CMD-COS-v1.01

Access Controller > Wireless black and white list

CPU: 0.00% MEM: 17% TX: 384.00 B/s RX: 0.00 B/s

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:

SSID: 

- all
- COMMAND001\_2G
- COMMAND001\_5G
- COMMAND002\_5G

AP: 

- all
- 08:9b:4b:99:a3:94

Week:  All  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Time:

Remarks:

### 5.5.3 Wireless blacklisting for particular MAC page

The screenshot shows the 'Wireless black and white list' page. The left sidebar contains a navigation menu with 'Access Controller' selected. The main content area has a search bar for 'MAC/SSID/Comment' and buttons for 'Add', 'Import', 'Export', 'Enable', 'Disable', and 'Delete'. A table lists the blacklisted entries:

Mode	Terminal MAC address	SSID	AP	week	time	comment	Status	Actions
BlackList	08:9b:4b:9e:f4...	COMMAND002_2G	08:9b:4b:9e:f4:e3	12345	00:00-23:59	MAC blacklisting from SSID	Enabled	Edit Disable Delete

Below the table, it indicates 'Showing 1 of 1 records' and provides pagination controls (PerPage: 20, Rows, 1 / 1Pages, Jump). A help message states: 'Help: AP firmware version 1.5.0 and above is supported only'.

### 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

The screenshot shows the 'User Information' page. The left sidebar has 'Access Controller' selected. The main content area has a search bar for 'IP/MAC/SSID' and filters for 'All Frequency' and 'All users'. A table header is visible with columns: IP Address, MAC, AP Information, SSID, Signal, Connect Time, Tx, Rx, Comment, and Actions. The table content is currently empty, displaying 'No Data'.

### 5.6.1 Default User Information page

CMD-COS-v1.01 English

CPU: 0.00% MEM: 19% TX: 443.00 B/s RX: 0.00 B/s

Access Controller > User Information

User Information

IP/MAC/SSID  All Frequency  All users

IP Address	MAC	AP Infomation	SSID	Signal	Connect Time	Tx	Rx	Comment	Actions
192.168.0.102	c4:d9:87:a7:ad:46	08:9b:4b:99:a3:94	5G:COMMAN DO02_5G	-56dBm	1m 21s	70 B/s	0 B/s	DESKTOP-70API5S	<a href="#">Details</a> <a href="#">Modify comment</a>
192.168.0.50	20:a6:0c:37:4d:13	08:9b:4b:99:a3:94	5G:COMMAN DO01_5G	-43dBm	1m 13s	0 B/s	0 B/s	POCOF1-POCOF1	<a href="#">Details</a> <a href="#">Modify comment</a>

Showing 1-2 of 2 records PerPage  Rows  /1Pages [Jump](#)

## 5.6.2 User Information after connecting users' 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.

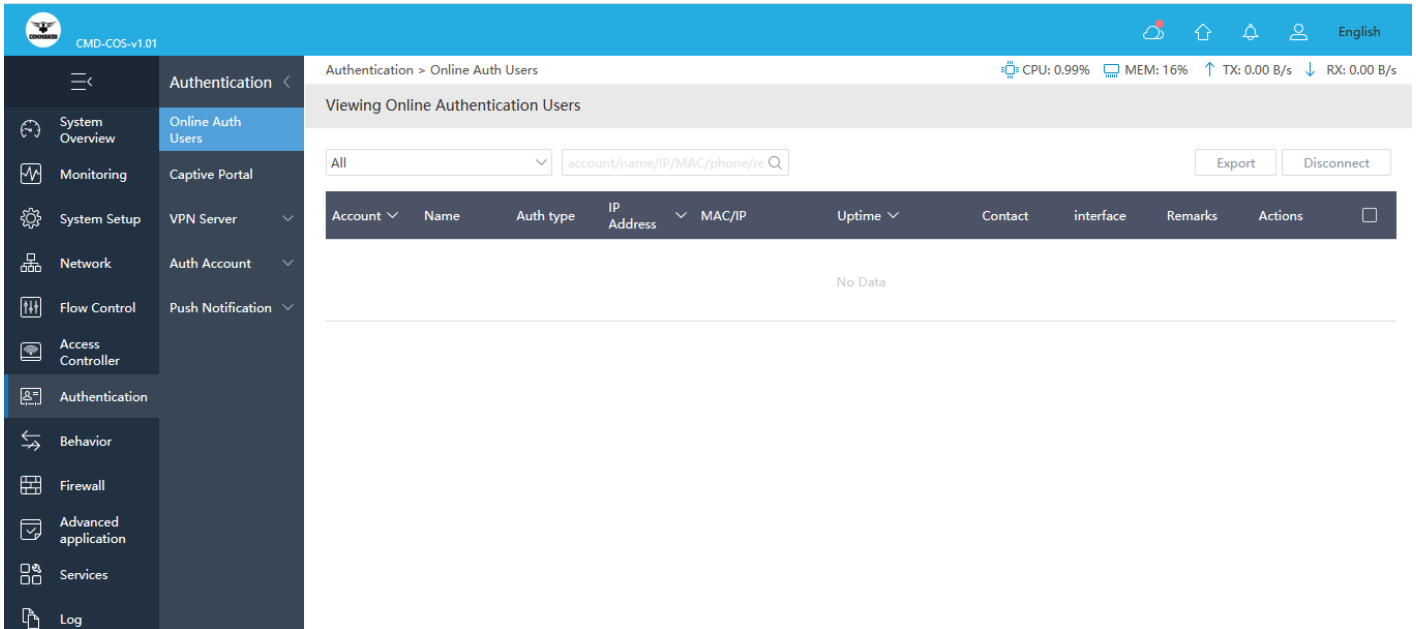
## **Push Notification:**

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

## **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**

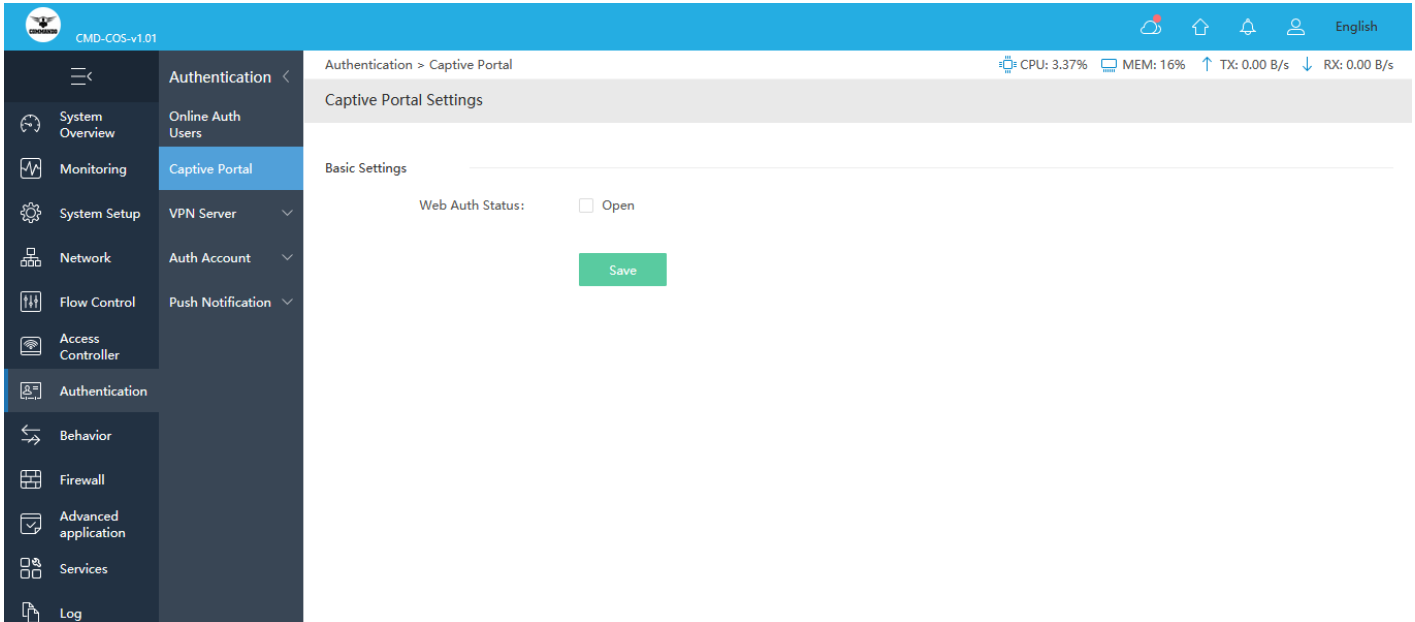
## 6.2 Captive Portal

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

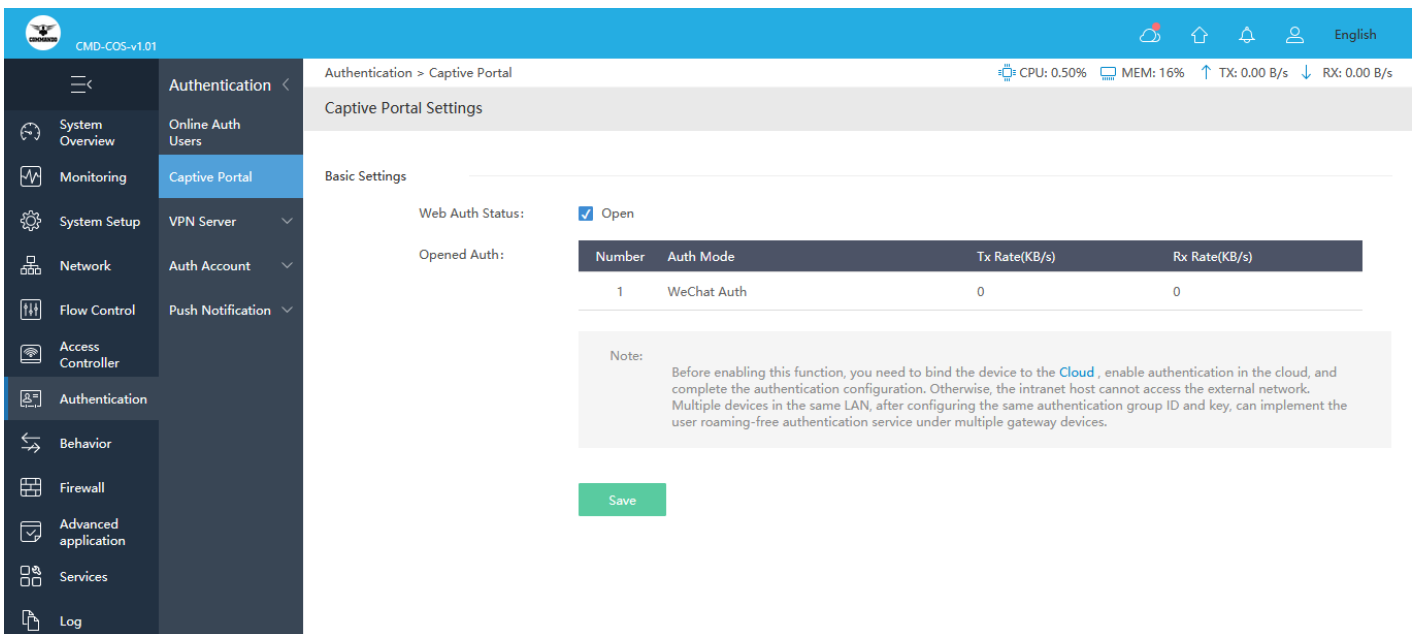




**Fig 6.2.1 Default Captive Portal Settings page**

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**

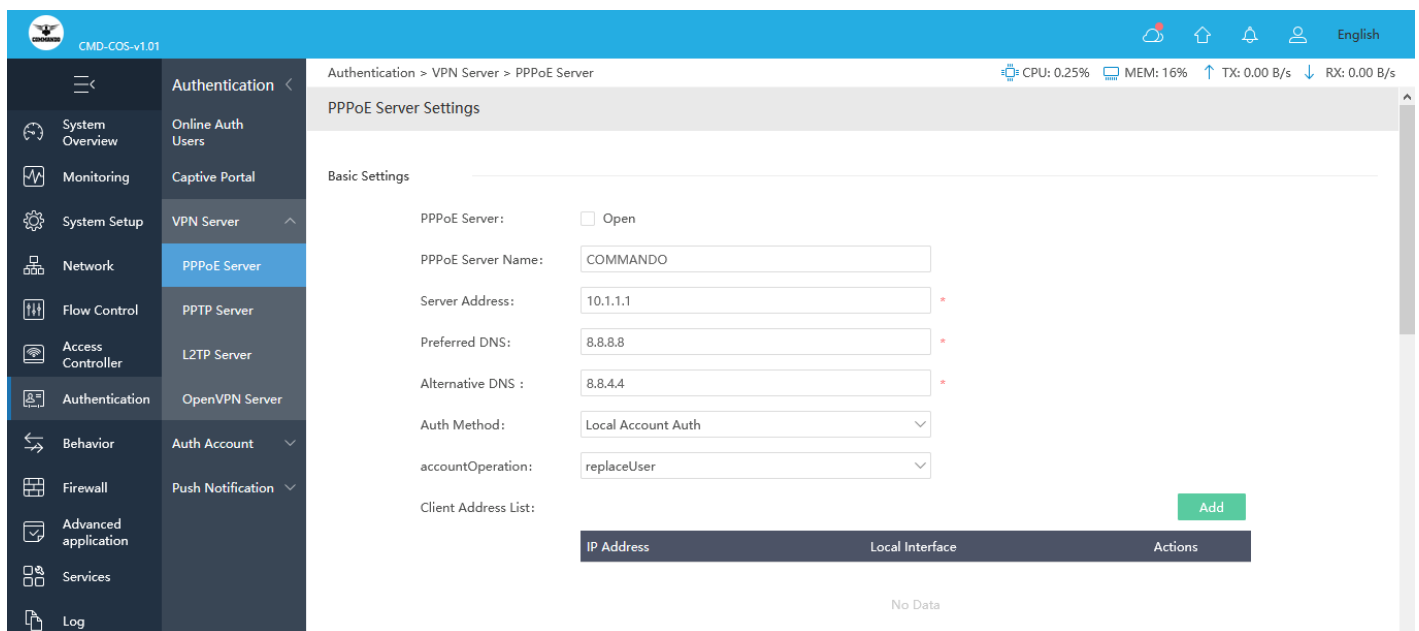
### 6.3 VPN Server

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**

The screenshot displays the 'PPPoE Server Settings' page in the H3C web management interface. The breadcrumb trail is 'Authentication > VPN Server > PPPoE Server'. The page title is 'PPPoE Server Settings'. Under 'Basic Settings', the 'PPPoE Server' checkbox is checked and labeled 'Open'. The 'PPPoE Server Name' is 'COMMANDOPPPoE'. The 'Server Address' is '192.168.200.1'. The 'Preferred DNS' is '8.8.8.8' and the 'Alternative DNS' is '8.8.4.4'. The 'Auth Method' is 'Local Account Auth' and 'accountOperation' is 'replaceUser'. Below these settings is a table for 'Client Address List' with an 'Add' button. The table has three columns: 'IP Address', 'Local Interface', and 'Actions'. One entry is shown with IP '10.1.1.2-10.1.1.254' and interface 'lan1', with 'Edit' and 'Delete' actions available. A note at the bottom states: 'Note: If there is no need to change, please do not set the same IP address as the LAN port'.

**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 router.

**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

Authentication > VPN Server > PPTP Server

Basic Settings

PPTP Server:  Open

serverPort:  \*

Preferred DNS:  \*

Alternative DNS :  \*

Client IP Address List:

Advanced Settings ^

MPPE Data Encryption:  v

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

Server Address:  \*

MTU:  \*

MRU:  \*

### 6.3.3 Default PPTP Server Settings page

Authentication > VPN Server > PPTP Server

PPTP Server Settings

Basic Settings

PPTP Server:  Open

serverPort:  \*

Preferred DNS:  \*

Alternative DNS :  \*

Client IP Address List:

Advanced Settings ^

MPPE Data Encryption:  v

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

Server Address:  \*

MTU:  \*

MRU:  \*

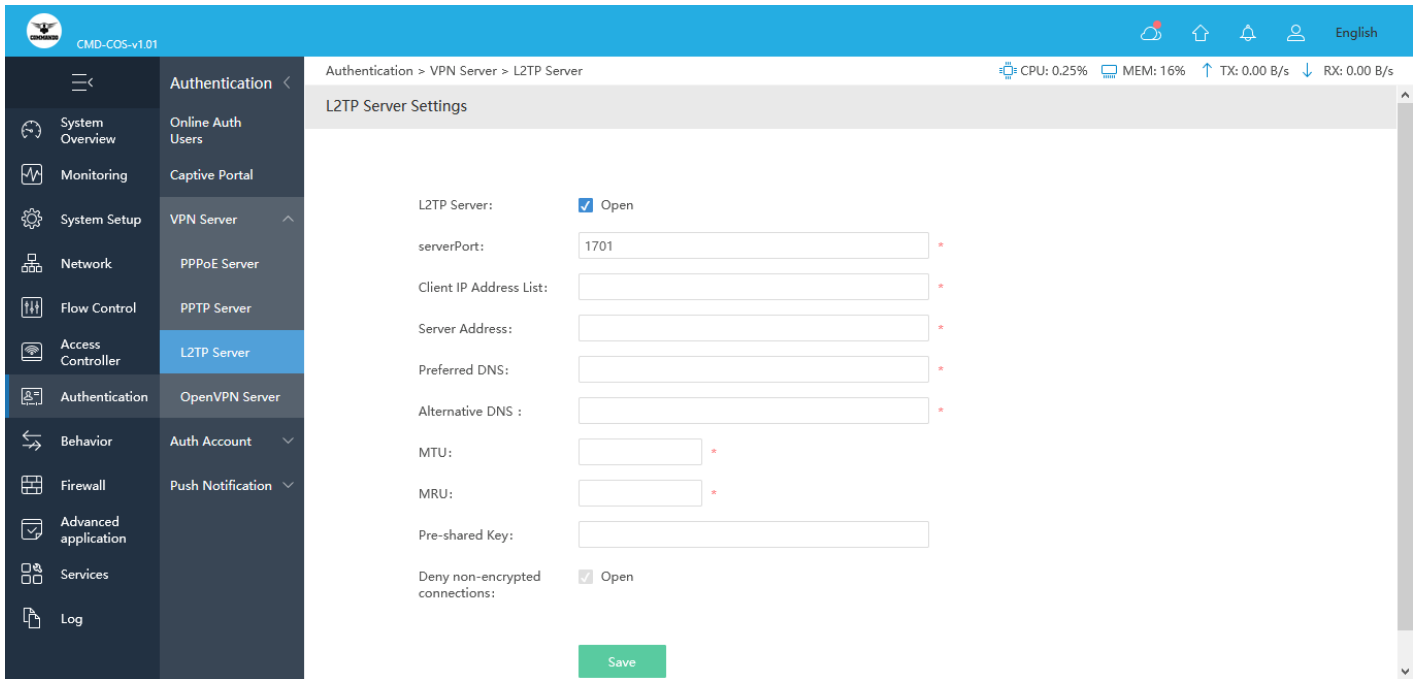
### 6.3.4 PPTP Server Settings after configuration page

#### L2TP Server Settings:

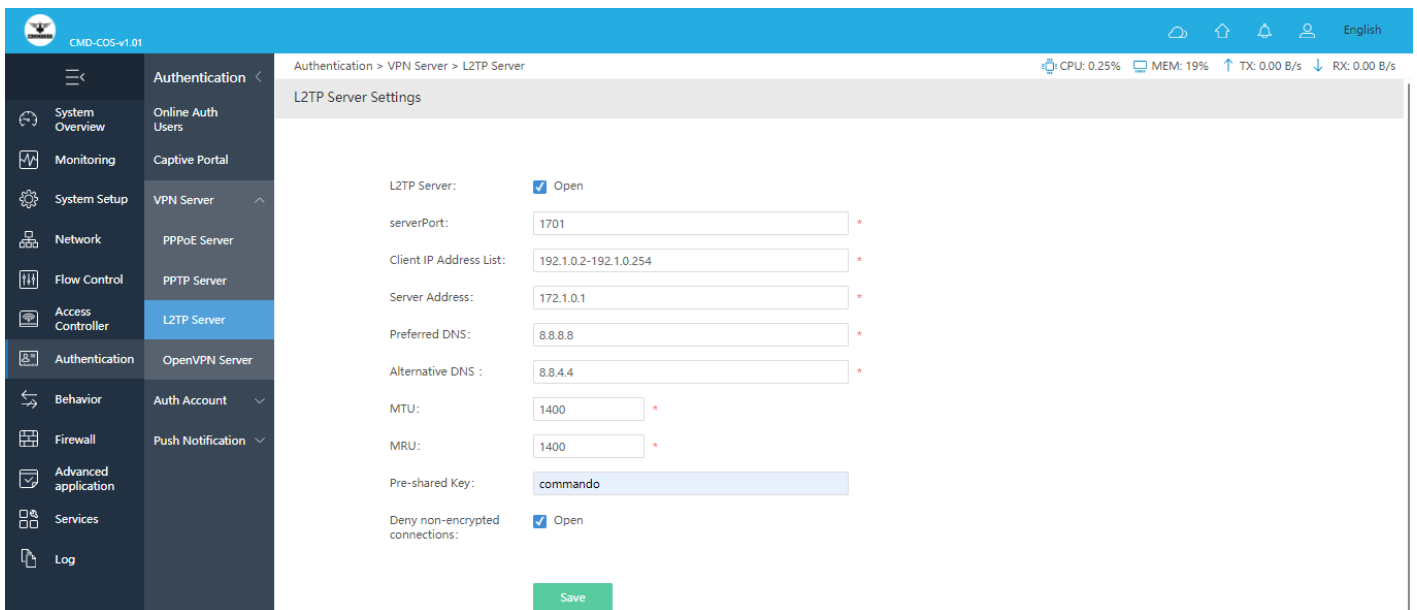
Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP protocol is based on the client and server model. L2TP (Layer 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



**Fig 6.3.5 Default L2TP Server Settings page**



**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 configuration page for an OpenVPN Server. The interface includes a sidebar menu, a breadcrumb trail, and a main configuration area with various settings and a table of push routes.

**Sidebar Menu:**

- System Overview
- Monitoring
- System Setup
- Network
- Flow Control
- Access Controller
- Authentication
  - OpenVPN Server (selected)
  - Auth Account
  - Push Notification
- Behavior
- Firewall
- Advanced application
- Services
- Log

**Breadcrumb:** Authentication > VPN Server > OpenVPN Server

**Configuration Fields:**

- OpenVPN Server:  Open
- Server Port:
- VPN Segment:
- Subnet Mask:
- Tunnel Protocol:
- Tunnel Type:
- Topology type:
- Encryption Algorithm:
- LZO Compression:  Open
- MTU:
- CA Certificate: 

```
-----BEGIN CERTIFICATE-----
MIIDQTCcAimgAwIBAgUAOrD5EkbB39uMA0GCSq
GSIs3DQEBChUAMDCsCzAJBgNV
BAYTAkNOMQ4wDAYDVQQKDAVpS3VhaTEYMBY
GA1UEAwwPaU11YWkgRlV2wWNIENB
MB4XDTE4MDUuMTEzMDAyMFoXDTE4MDUyODE
ZMDAyMFowNjEwMAkGA1UEBmCCO04x
-----
```
- Server Certificate: 

```
-----BEGIN CERTIFICATE-----
MIICGjCCAdICBFvQHBQwDQYJKoZIhvcNAQELBQA
wNjEwMAkGA1UEBmCCO04wDjAM
BgNVBAoMBWludWFpMgRqYDlVQQA9pS3V
haSBEZkZpY2UgQ0EwHhcNMjgwNTMx
MTYwMDIwMjEzMDUyMTYwMDUyMTYwMDUy
wCQYDlVQQA9pS3VhaSBEZkZpY2UgQ0E
-----
```
- Server Private Key: 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAiNSLulFww8YvqQF62m6Cx
Upx0NhwAhoheC957eSjP9sgU
9pZWwXORBBylwe3lh8qr0W/L9c6SmTPXkdAwV4
/SJGQ2icopaj2Rki7ySPVNM4d
j9kVJHHI+CKoodyY3HS+TQU7XIM0AabDqPLHidB
QYorF326iqWX06/vBNuaAQI2
-----
```
- Push Route:

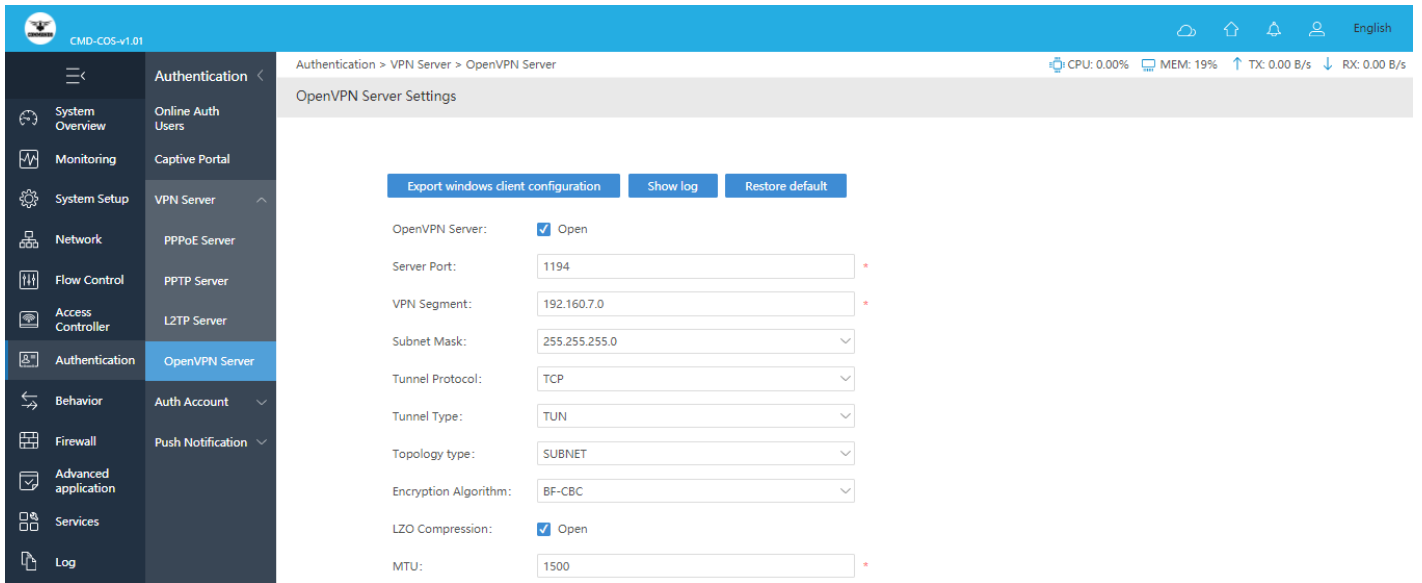
**Push Route Table:**

IP Address	Subnet Mask	Actions
10.7.0.0	255.255.0.0(16)	<a href="#">Edit</a> <a href="#">Delete</a>

**Additional Configuration:**

Additional configuration example: `tcp-queue-limit 32`  
`mtu-disc no`

**Fig 6.3.7 Default OpenVPN Server Settings page**

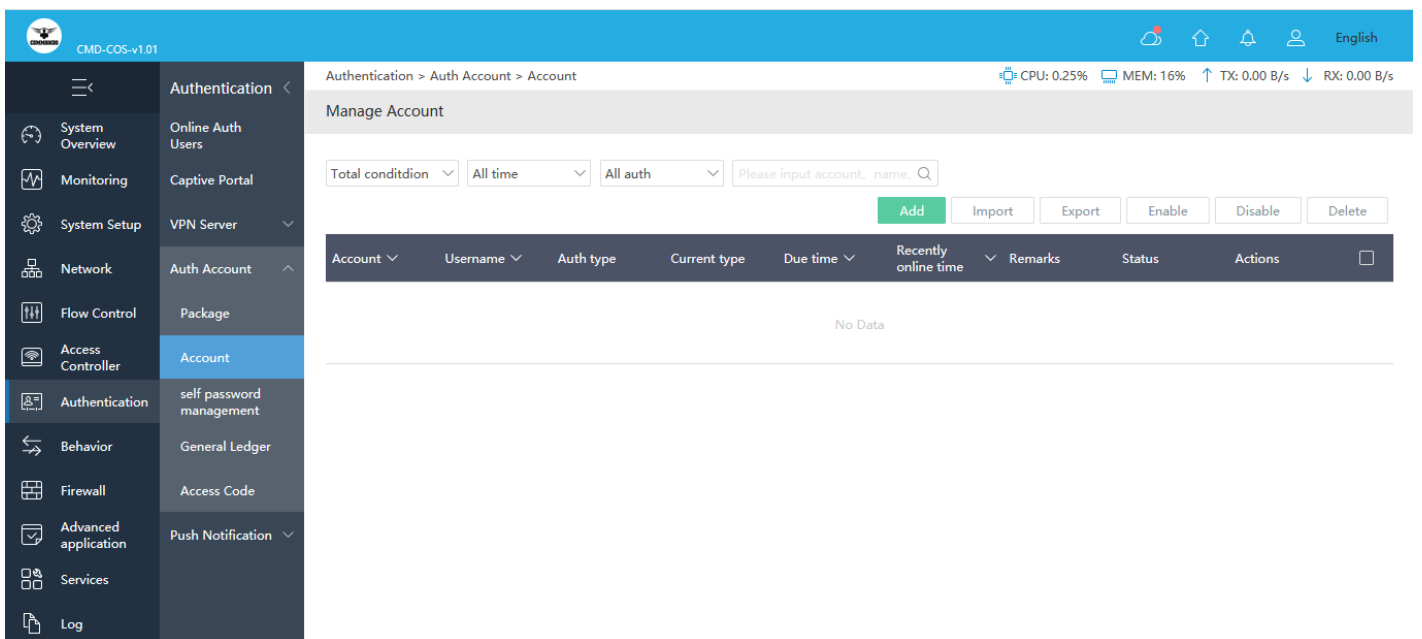


**Fig 6.3.8 Setting OpenVPN Server Settings page**

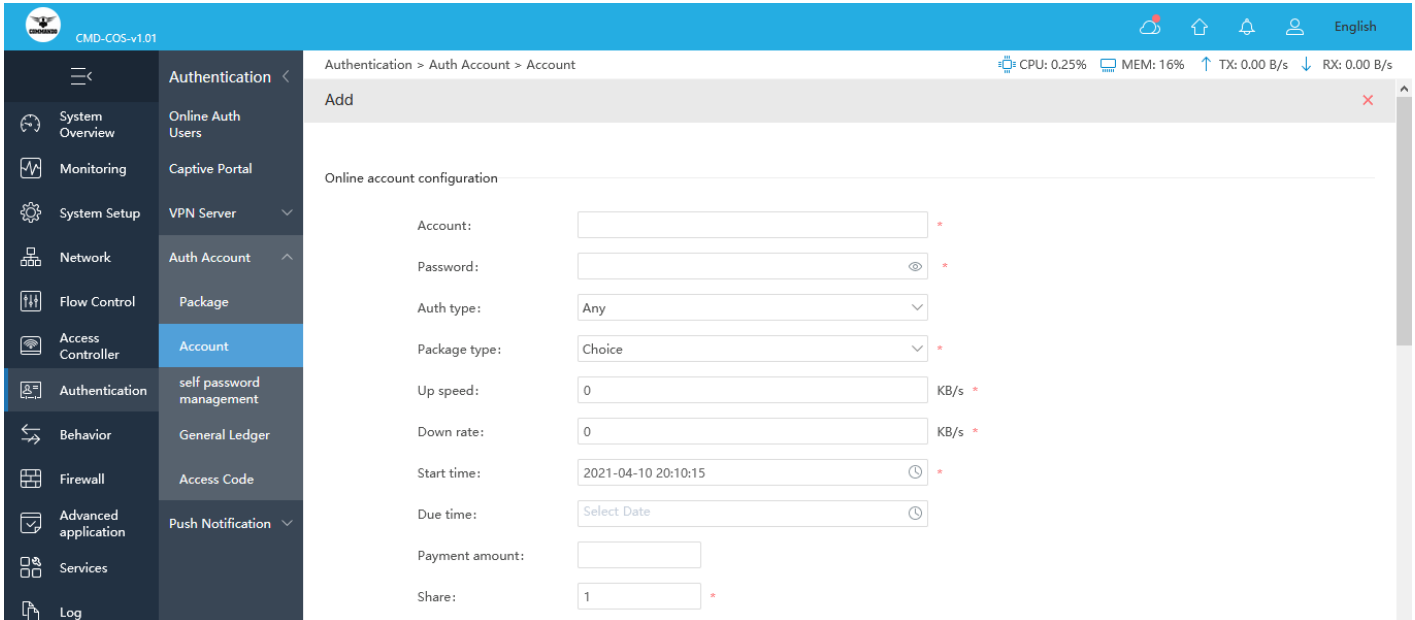
## 6.4 Authentication Account

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.

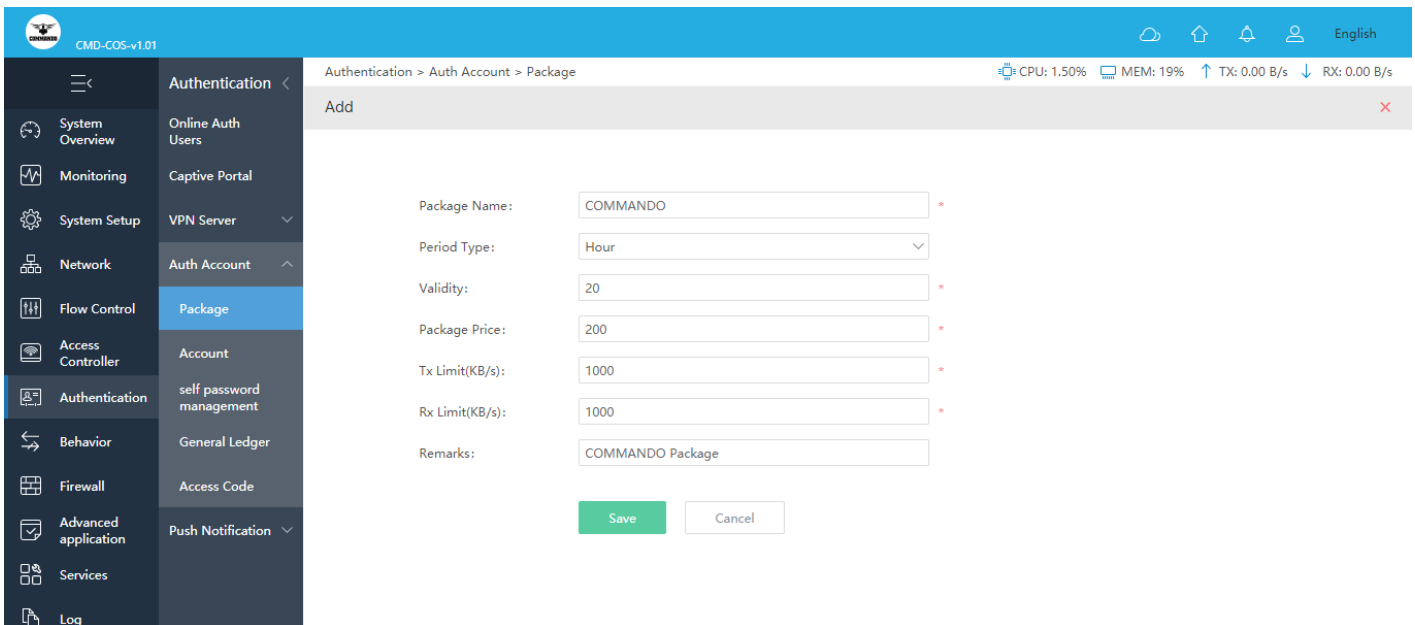
To Manage Package, Click on Authentication > Auth Account > Package



**Fig 6.4.1 Default Manage Package Account page**



**Fig 6.4.2 Add Online Account configuration page**



**Fig 6.4.3 Add particular Online Account configuration page**



Authentication > Auth Account > Package

Manage Package

Buttons: 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 / 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

Authentication > Auth Account > Account

Manage Account

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

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

Account	Username	Auth type	Current type	Due time	Recently online time	Remarks	Status	Actions
No Data								

**Fig 6.4.5 Default Mange Account page**

CMD-COS-v1.01

Authentication > Auth Account > Account

CPU: 0.25% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Add

Online account configuration

Account:

Password:

Auth type: Any

Package type: Choice

Up speed: 0 KB/s

Down rate: 0 KB/s

Start time: 2021-05-08 23:19:35

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 6.4.5 Add Manage Account page**

CMD-COS-v1.01

Authentication > Auth Account > Account

CPU: 0.25% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Binding NIC:

Only support PPPoE

Binding MAC: Manual

MAC addr:

Add a MAC, enter a MAC every line

Fixed IP:

Online customer information

Username:

ID number:

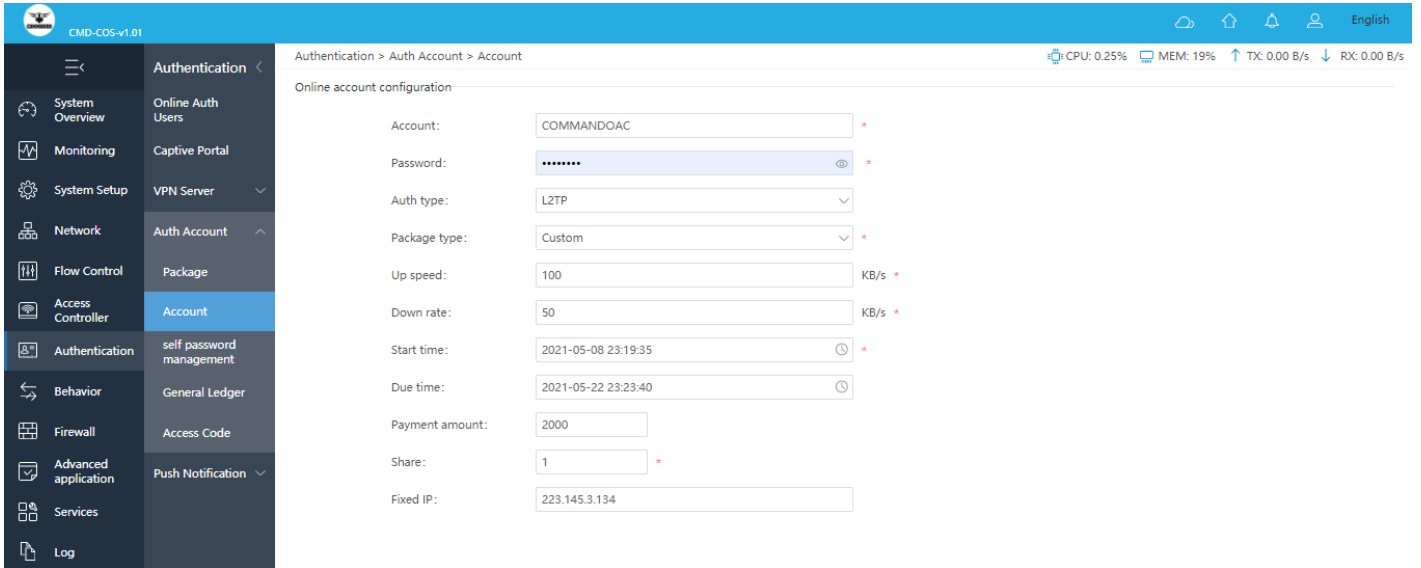
Telephone:

Addr:

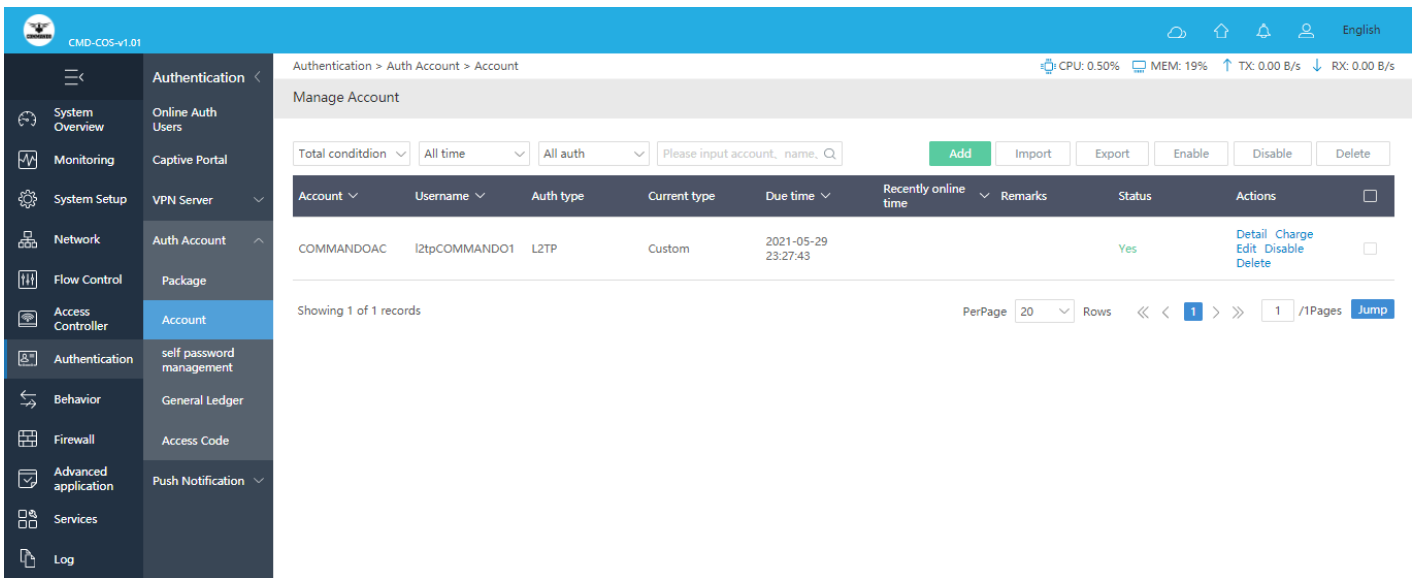
Remarks:

Save Cancel

**Fig 6.4.6 Add Online account configuration page**



**Fig 6.4.7 Add particular Online account configuration page**

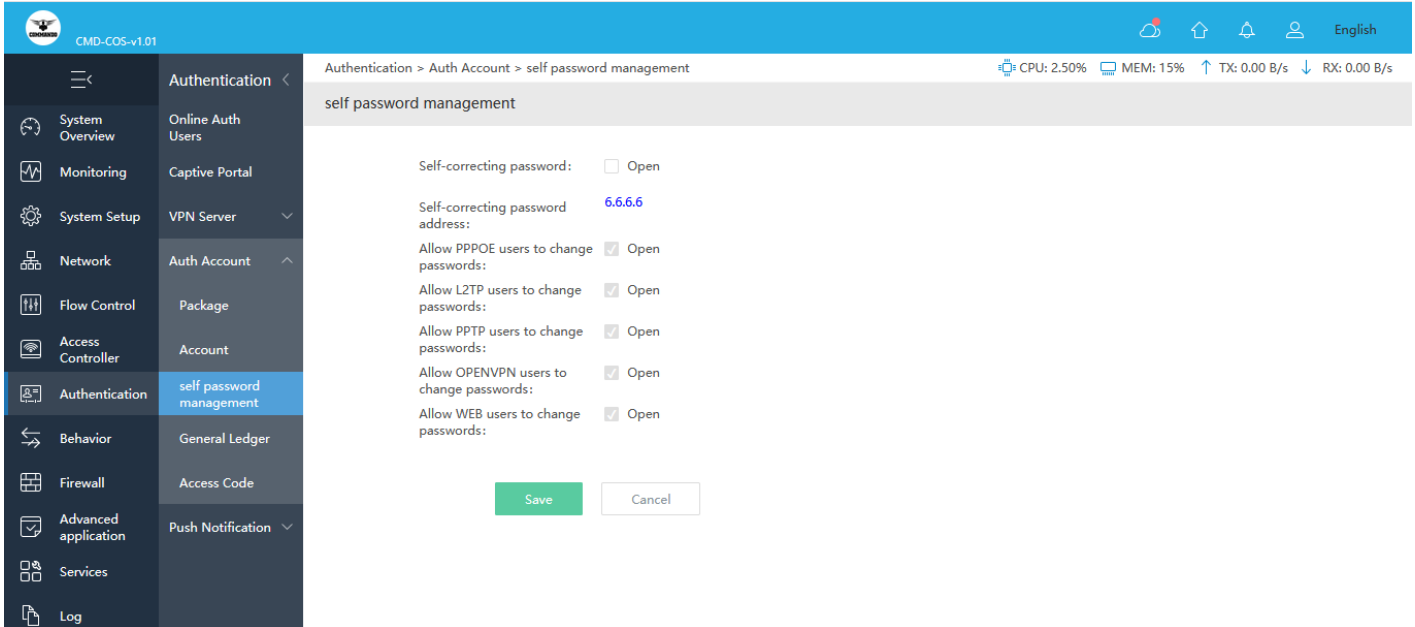


**Fig 6.4.8 Manage Online account page**

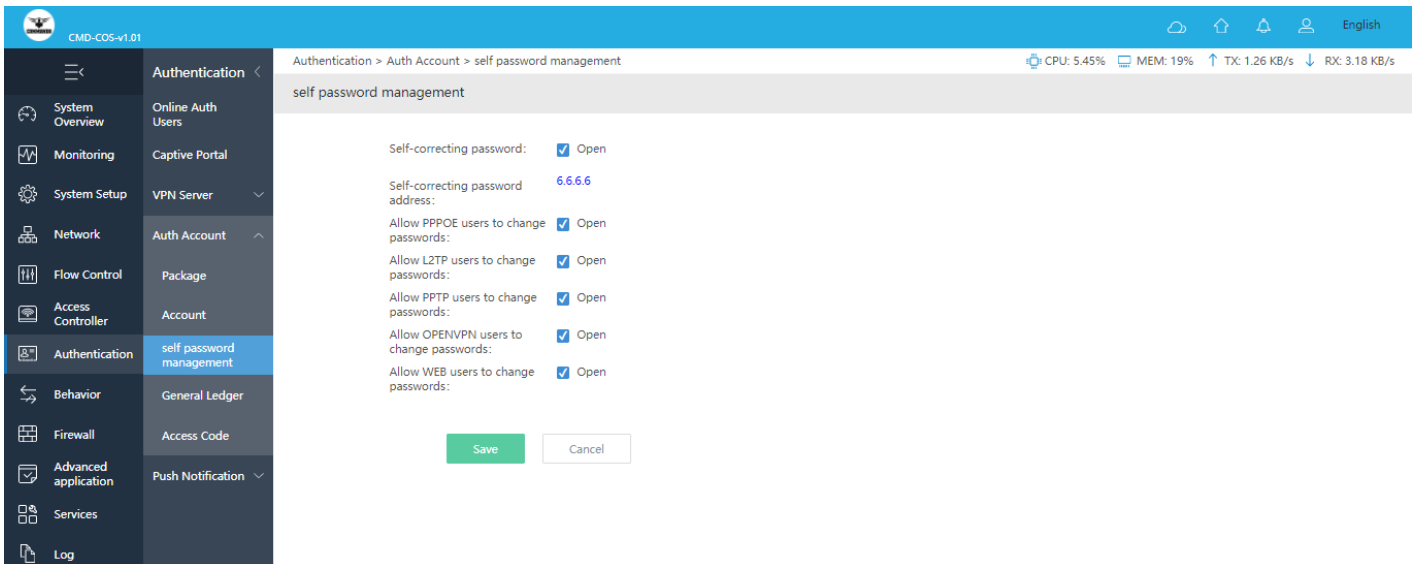
**Self password management:**

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 6.4.9 Default self password management page**

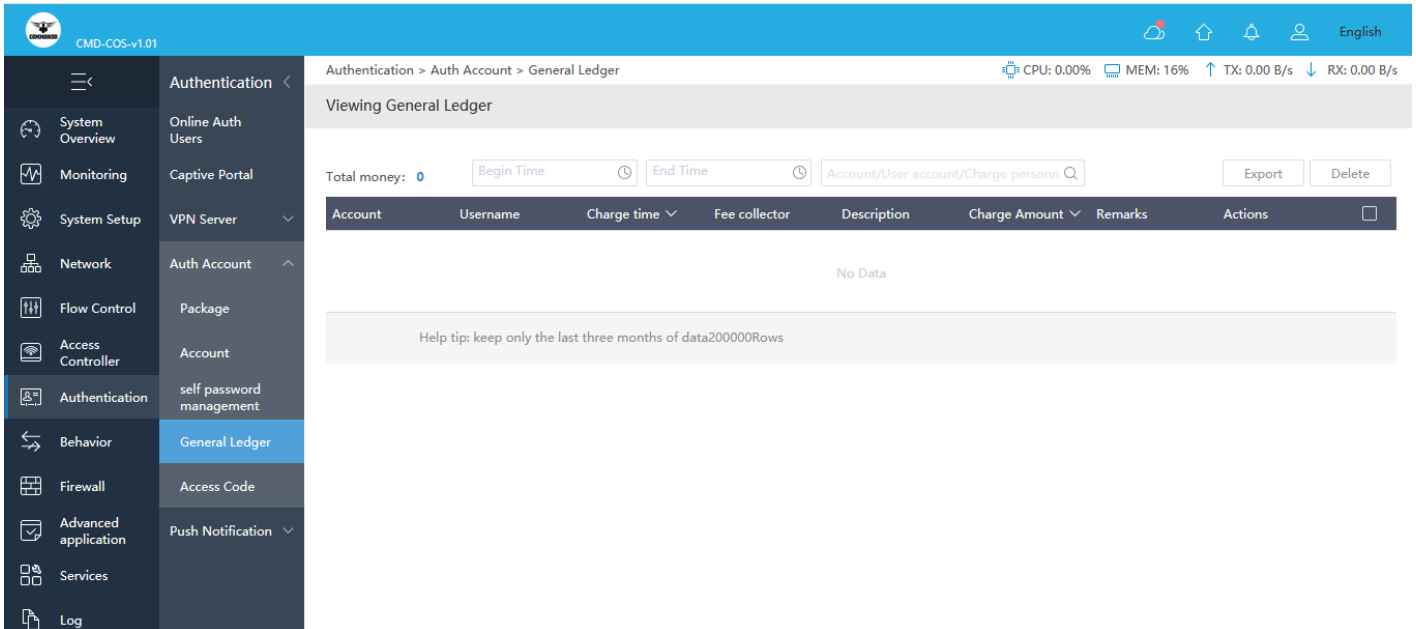


**Fig 6.4.10 Enabling self password management page**

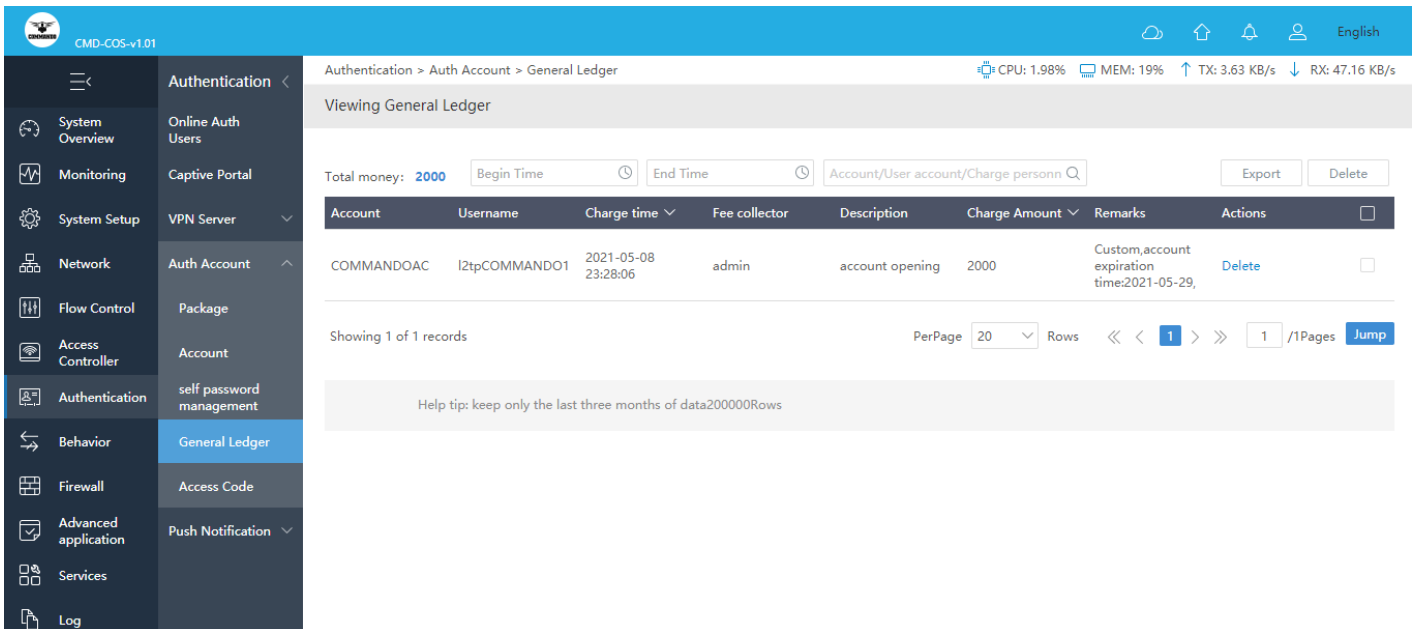
**General Ledger:**

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 6.4.11 Default General Ledger page**



**Fig 6.4.12 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

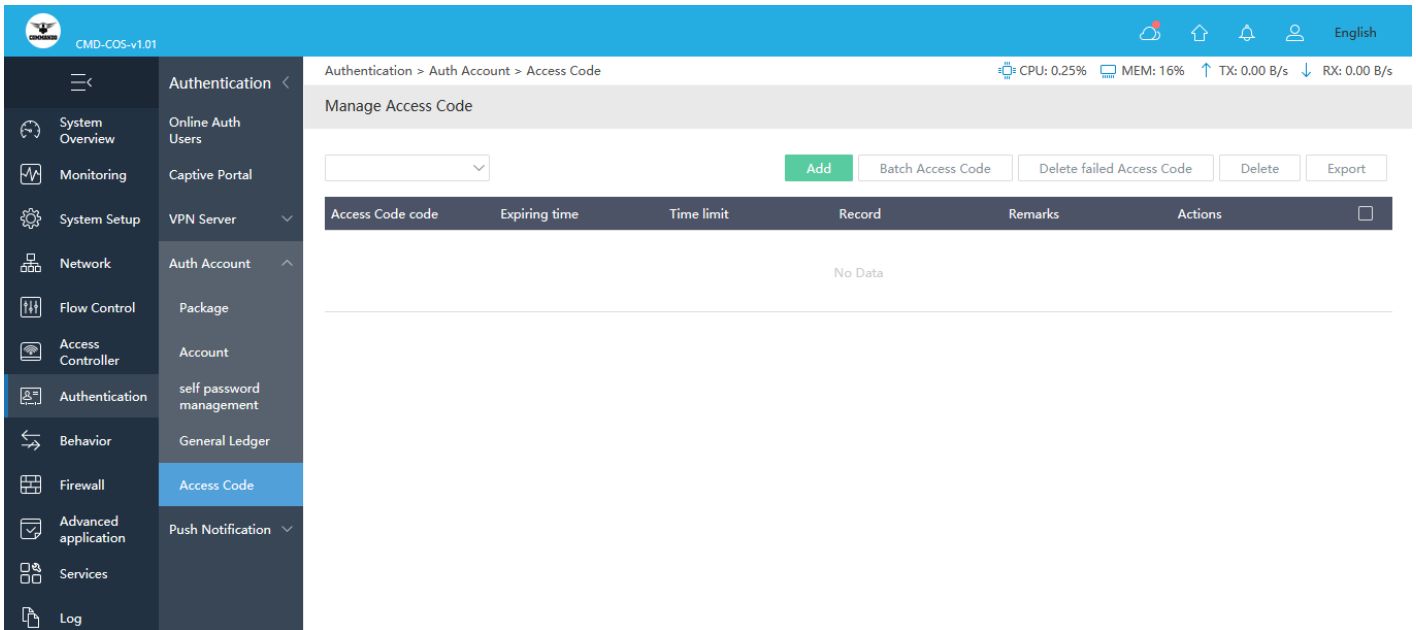


Fig 6.4.13 Default Manage Access Code page

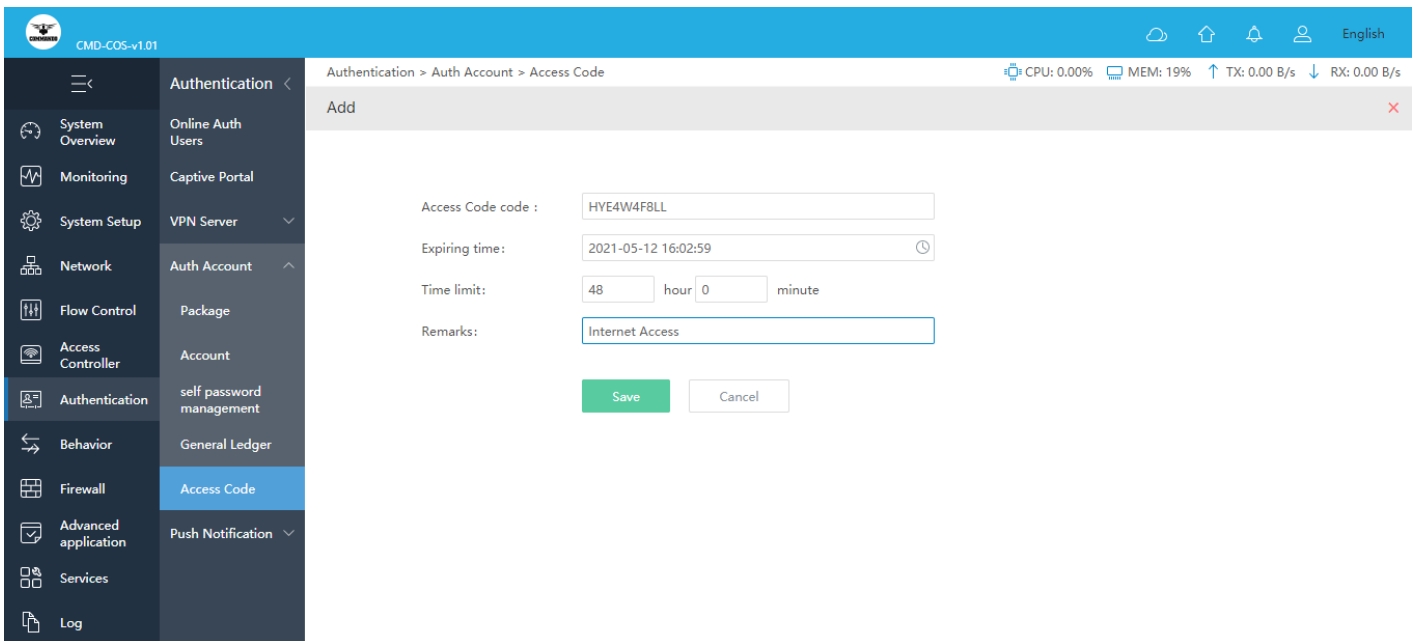


Fig 6.4.14 Add Manage Access Code page

The screenshot displays the 'Manage Access Code' page. At the top, there are system performance indicators: CPU: 1.75%, MEM: 19%, TX: 52.08 KB/s, and RX: 4.86 KB/s. The breadcrumb navigation is 'Authentication > Auth Account > Access Code'. Below the breadcrumb, there are buttons for 'Add', 'Batch Access Code', 'Delete failed Access Code', 'Delete', and 'Export'. A table lists the access codes with columns for 'Access Code code', 'Expiring time', 'Time limit', 'Record', 'Remarks', and 'Actions'. One record is shown with the code 'HYE4W4F8LL', expiring on '2021-05-12 16:02:59', a time limit of '48Hour0Minute', a status of 'Unused', and remarks of 'Internet Access'. The 'Actions' column for this record contains 'Edit' and 'Delete' links. At the bottom of the table, it says 'Showing 1 of 1 records' and 'PerPage 20 Rows 1 /1Pages'. A 'Jump' button is also present.

**Fig 6.4.15 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

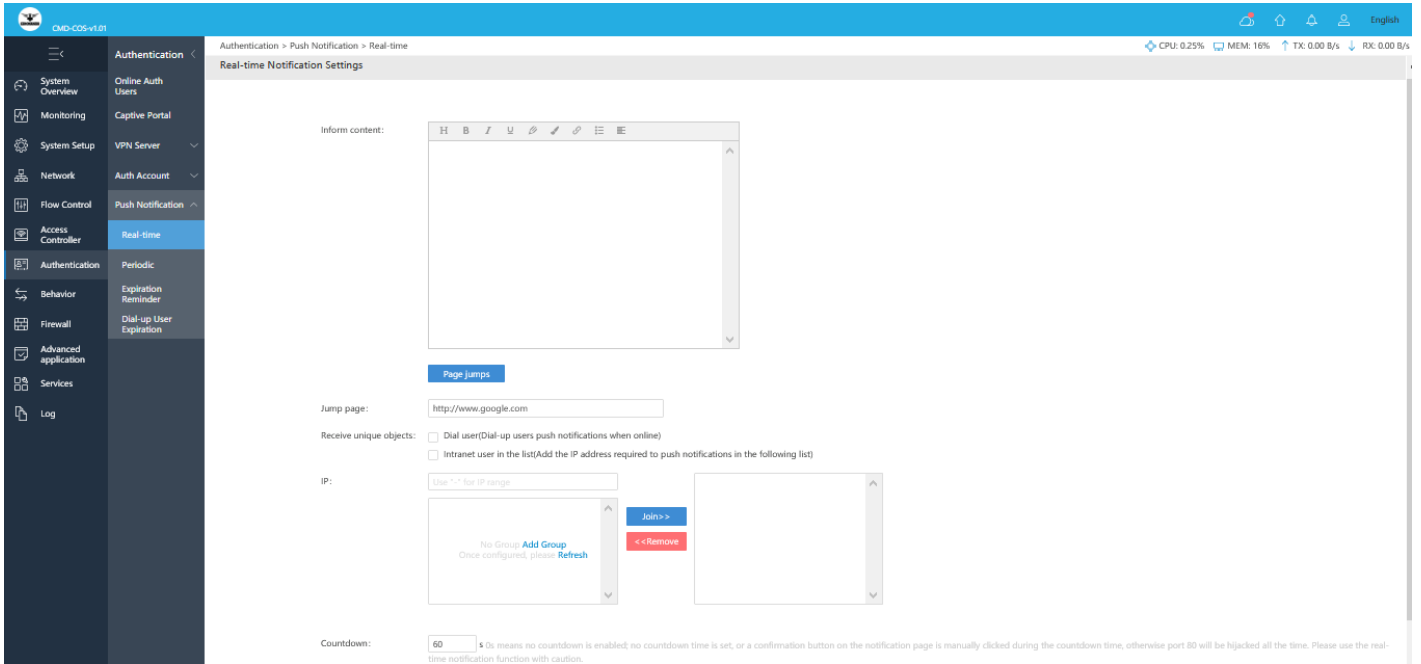
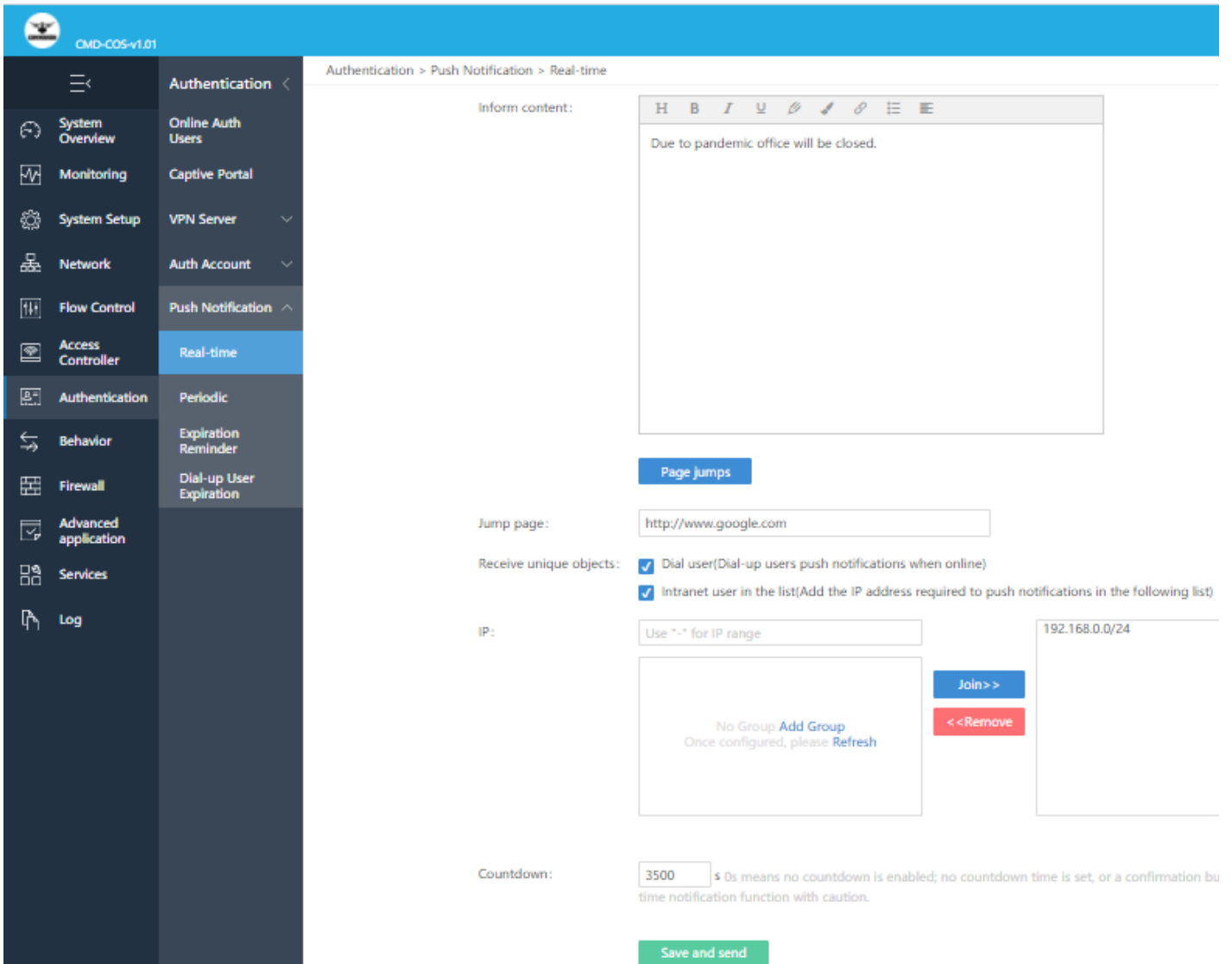


Fig 6.5.1 Default Real-time Notification Settings page



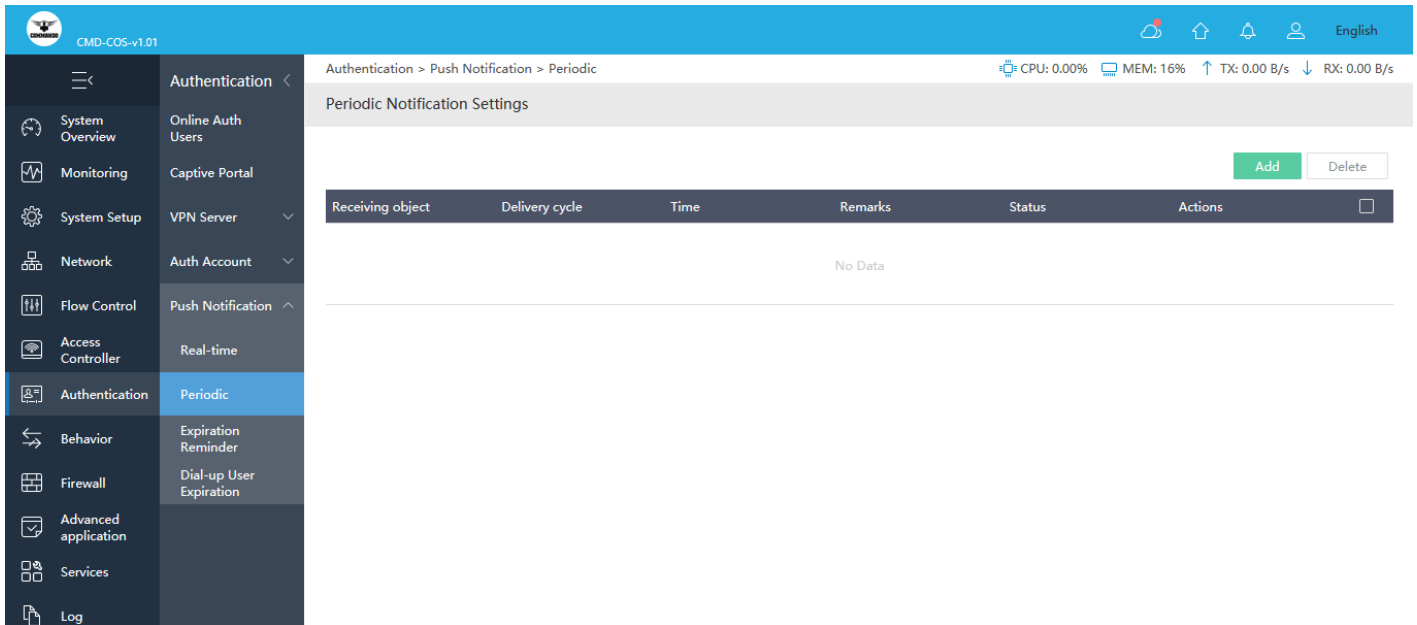


## Fig 6.5.2 Real-time Notification Settings page

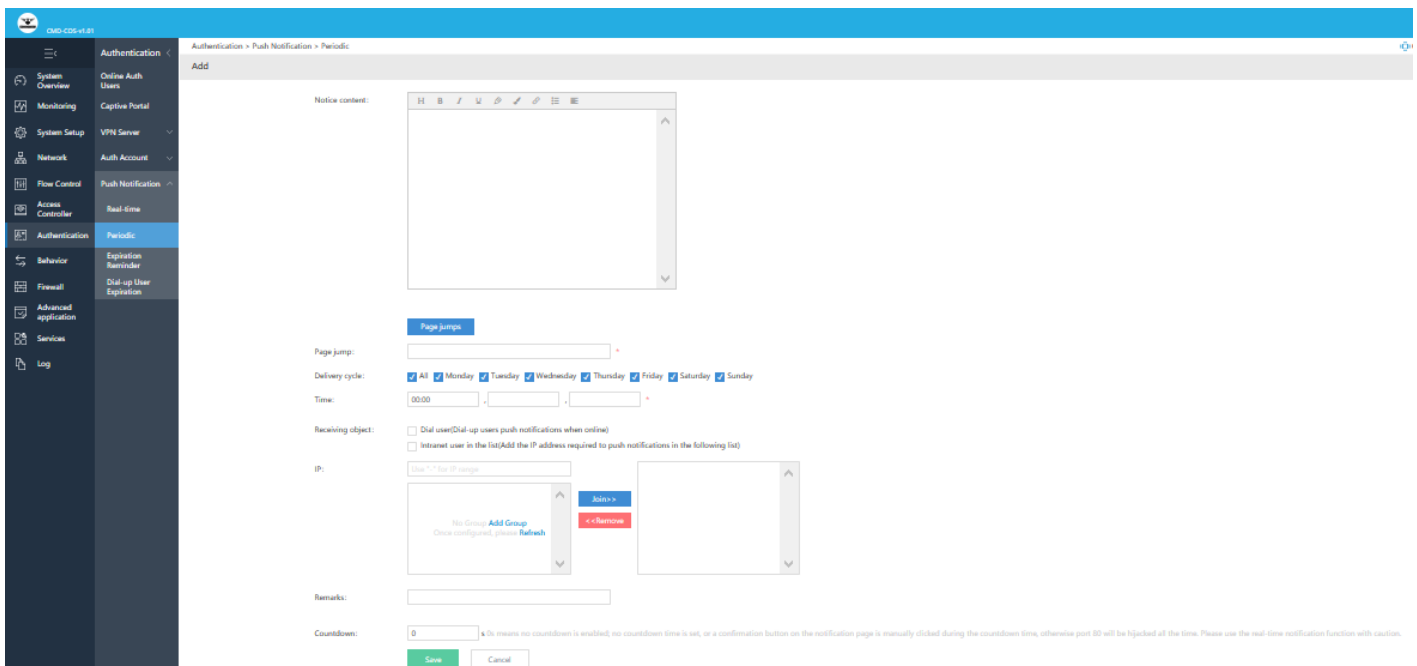
### Periodic Notification Settings:

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.

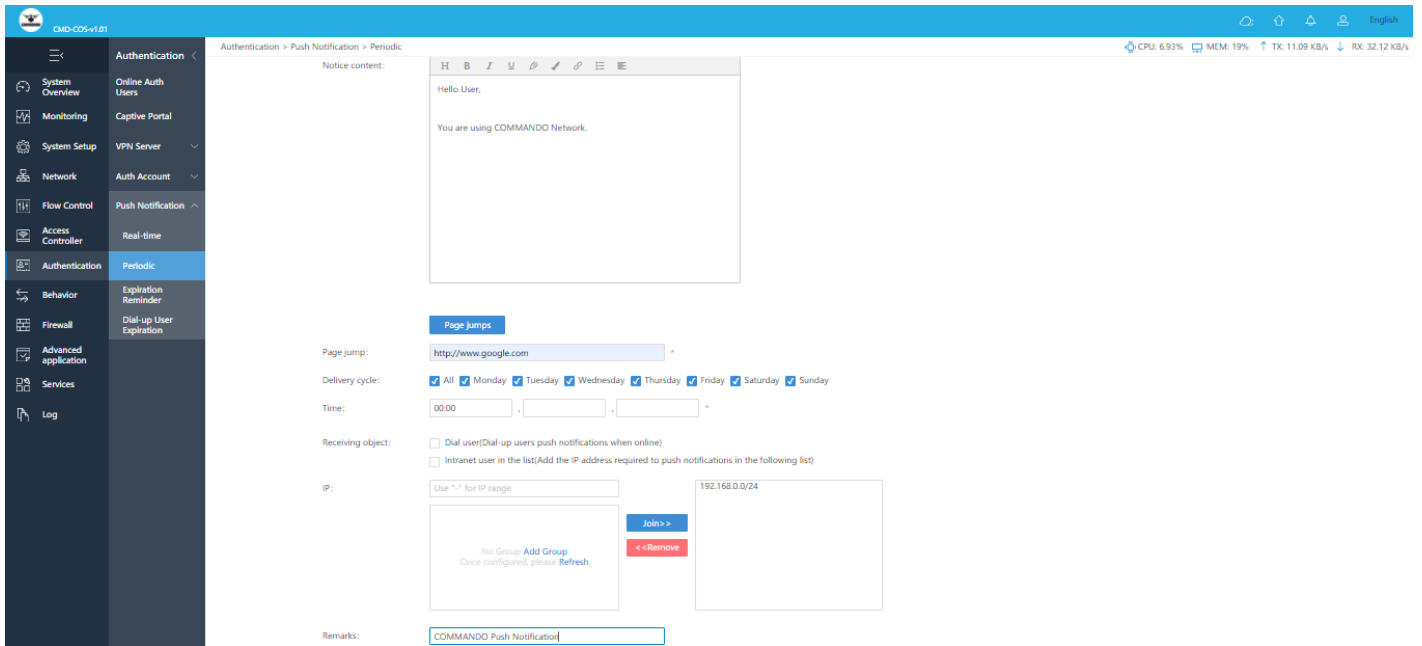
To configure Periodic Notification Settings, Click on Authentication > Push Notification > Periodic



## Fig 6.5.3 Default Periodic Notification Settings page



**Fig 6.5.4 Add Periodic Notification Settings page**

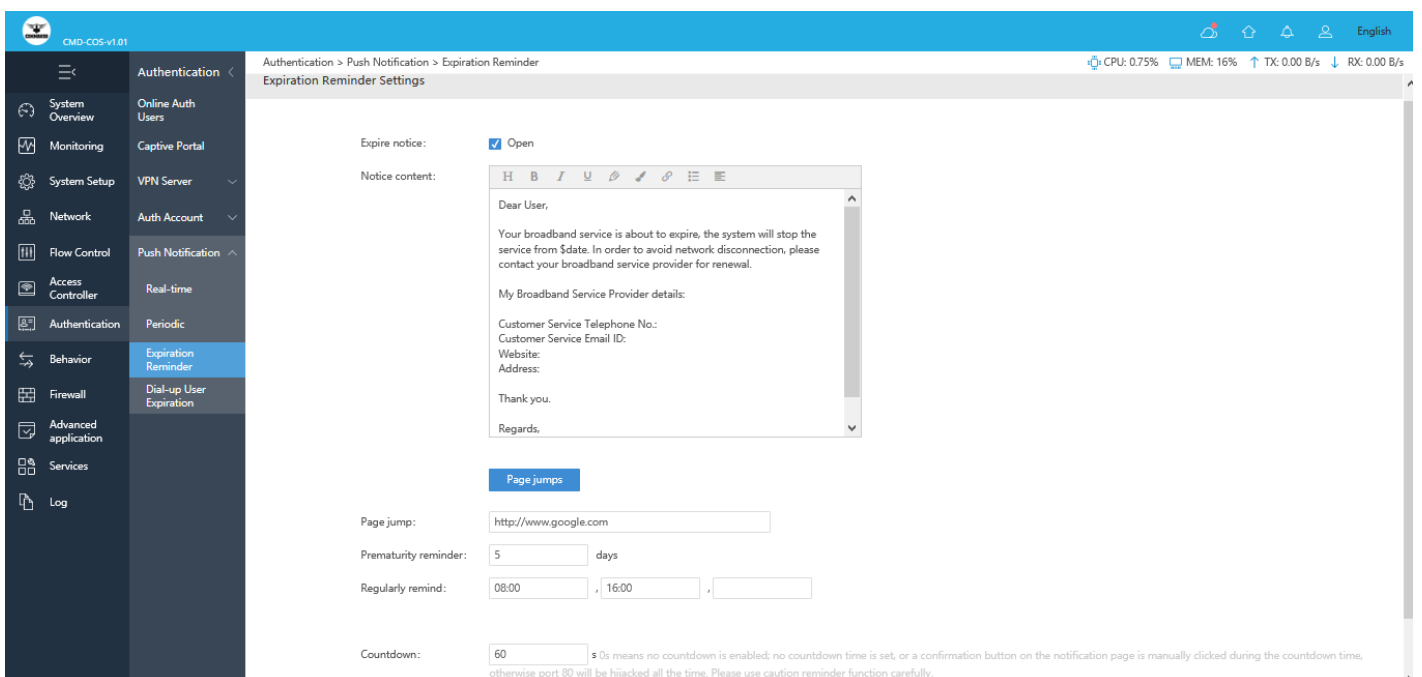


**Fig 6.5.5 Periodic Notification Settings page**

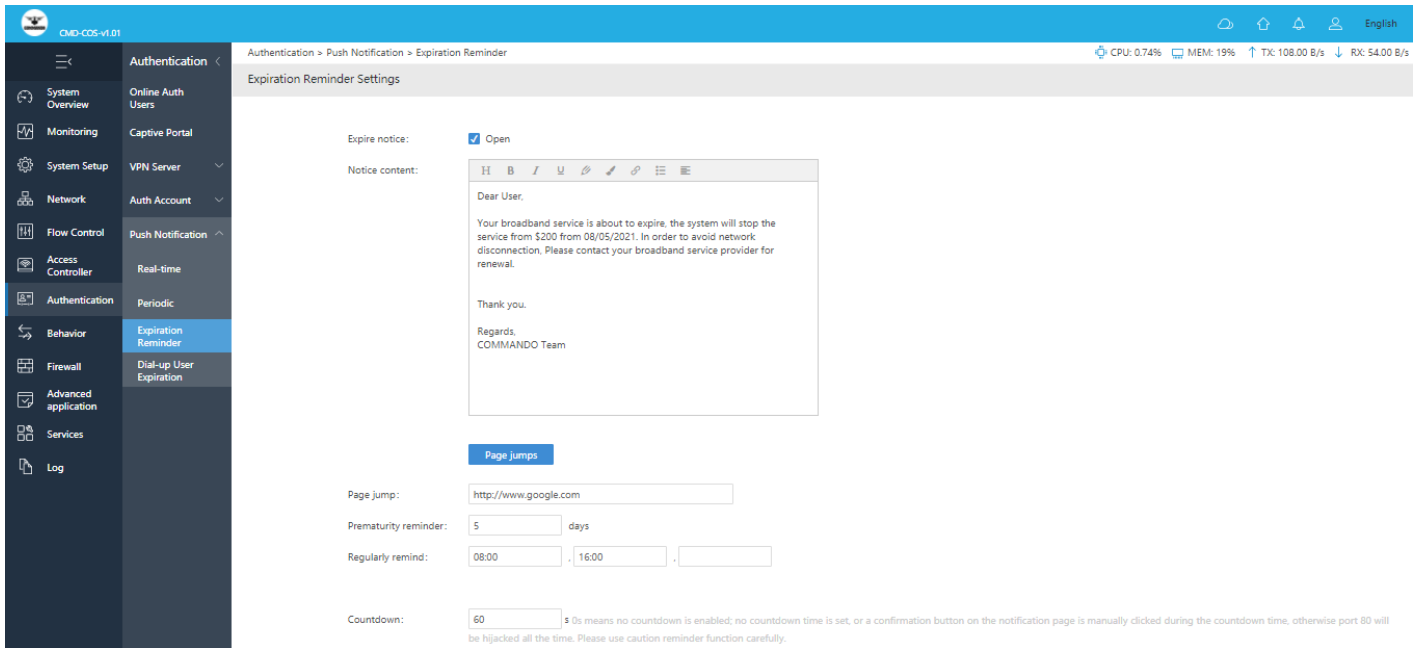
**Expiration Reminder Settings:**

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

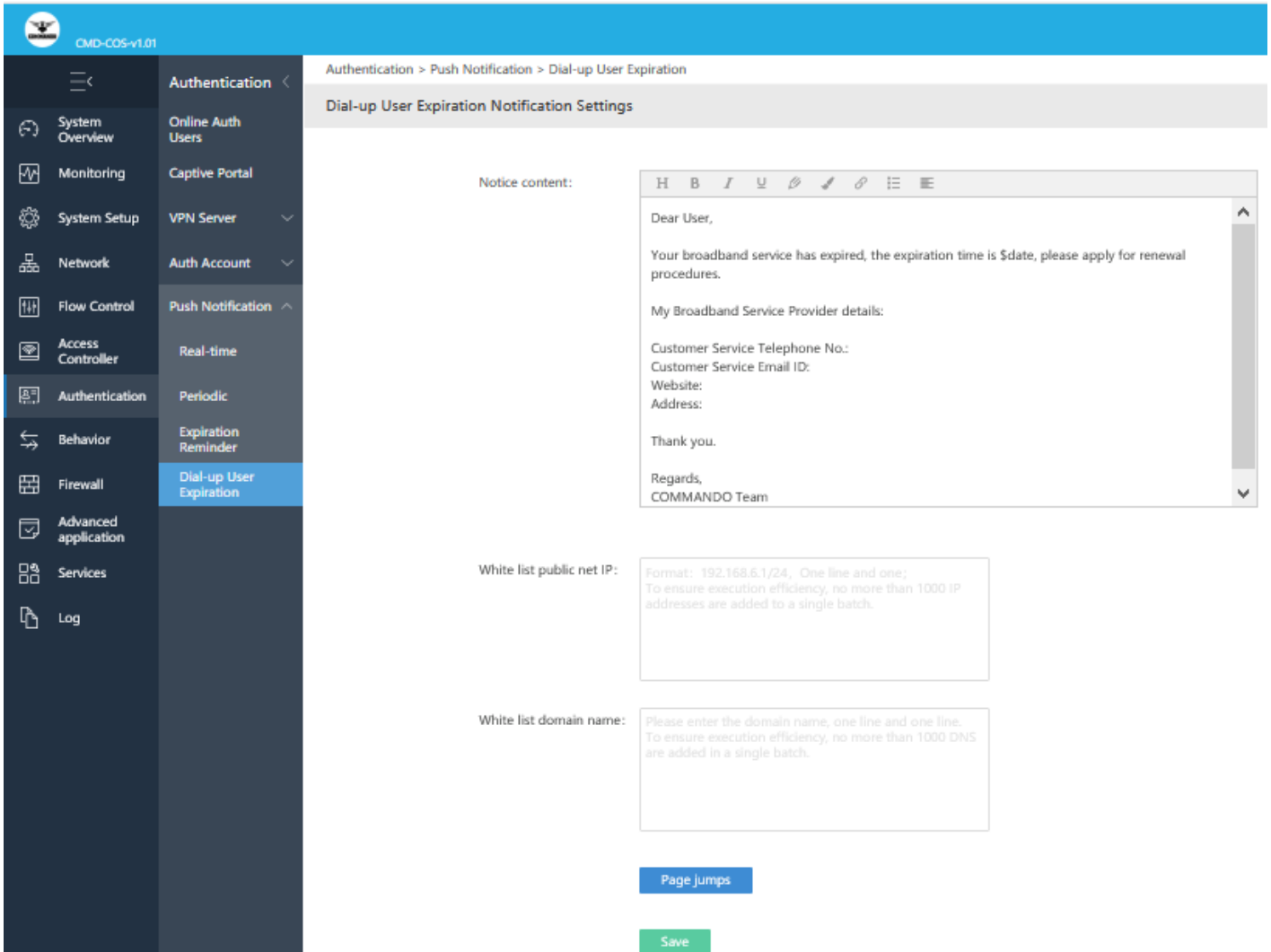


Fig 6.5.8 Default Dial-up User Expiration Notification page

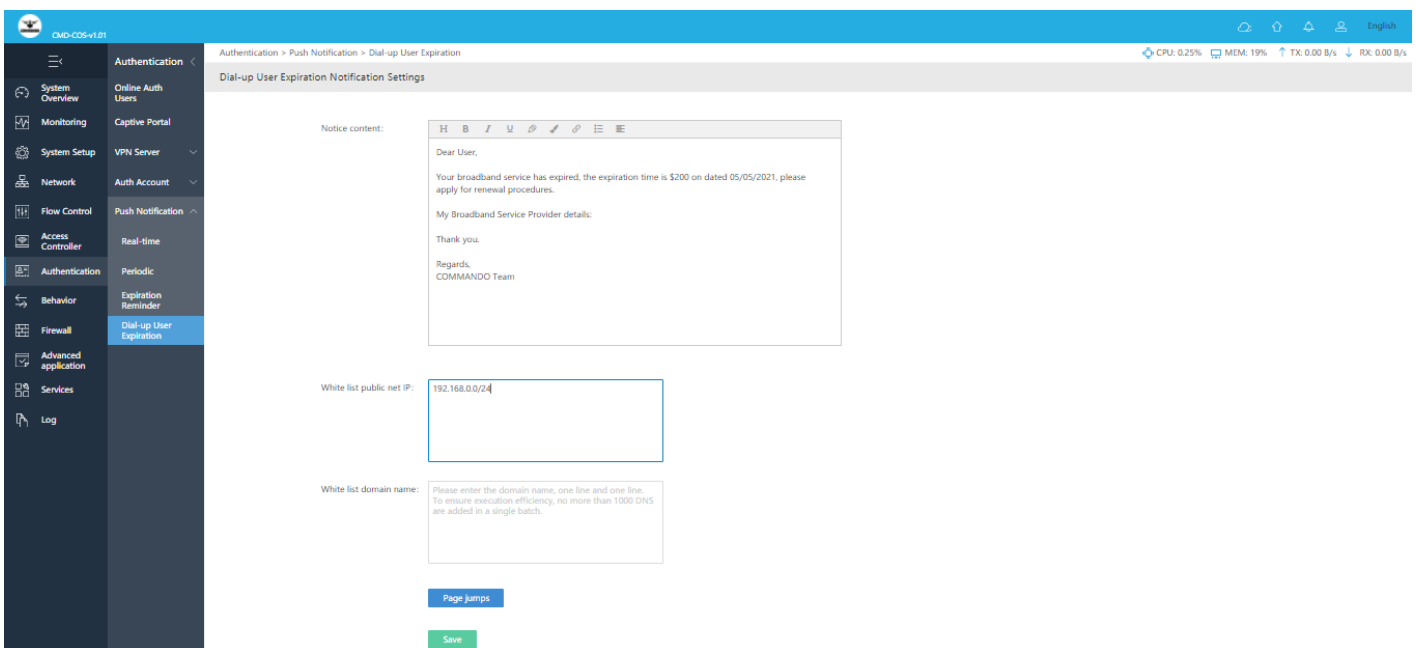


Fig 6.5.9 Dial-up User Expiration Notification page

# 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 routers 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 router on a network segment uses a secondary address, all other routers 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

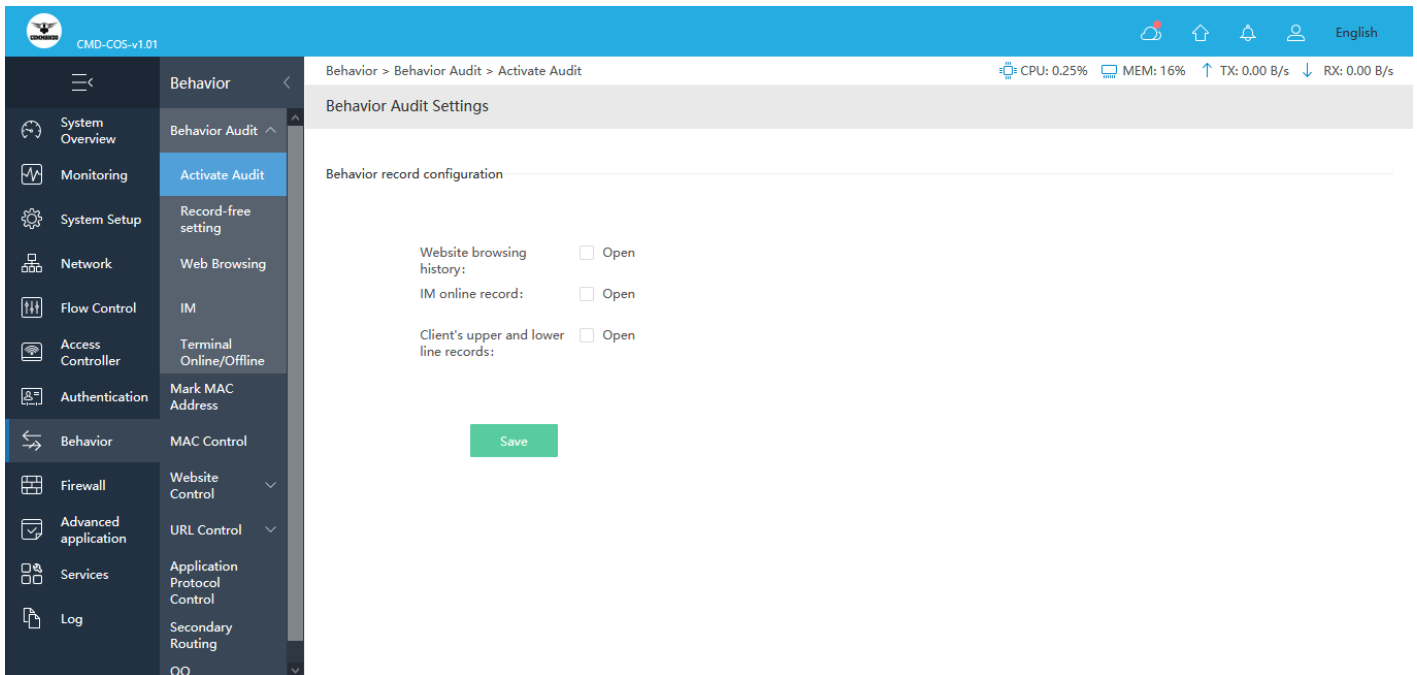


Fig 7.1.1 Default Behavior Audit Settings page

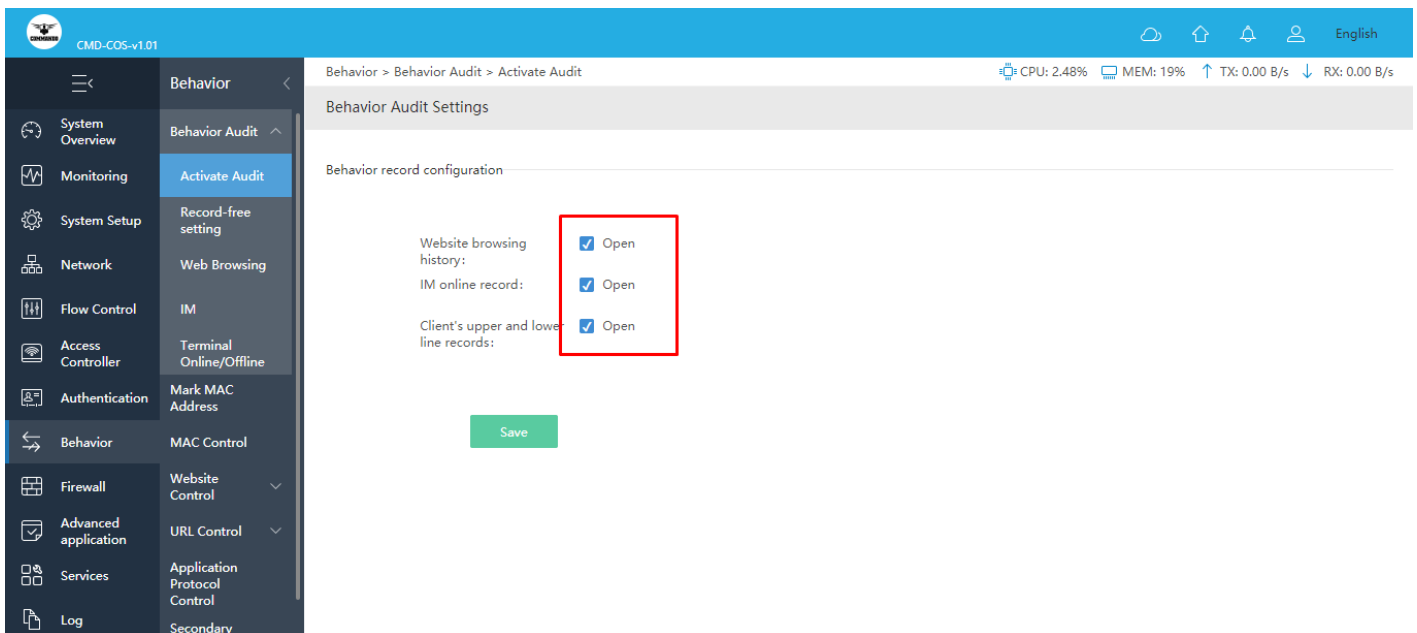


Fig 7.1.2 Enable Behavior Audit Settings page

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

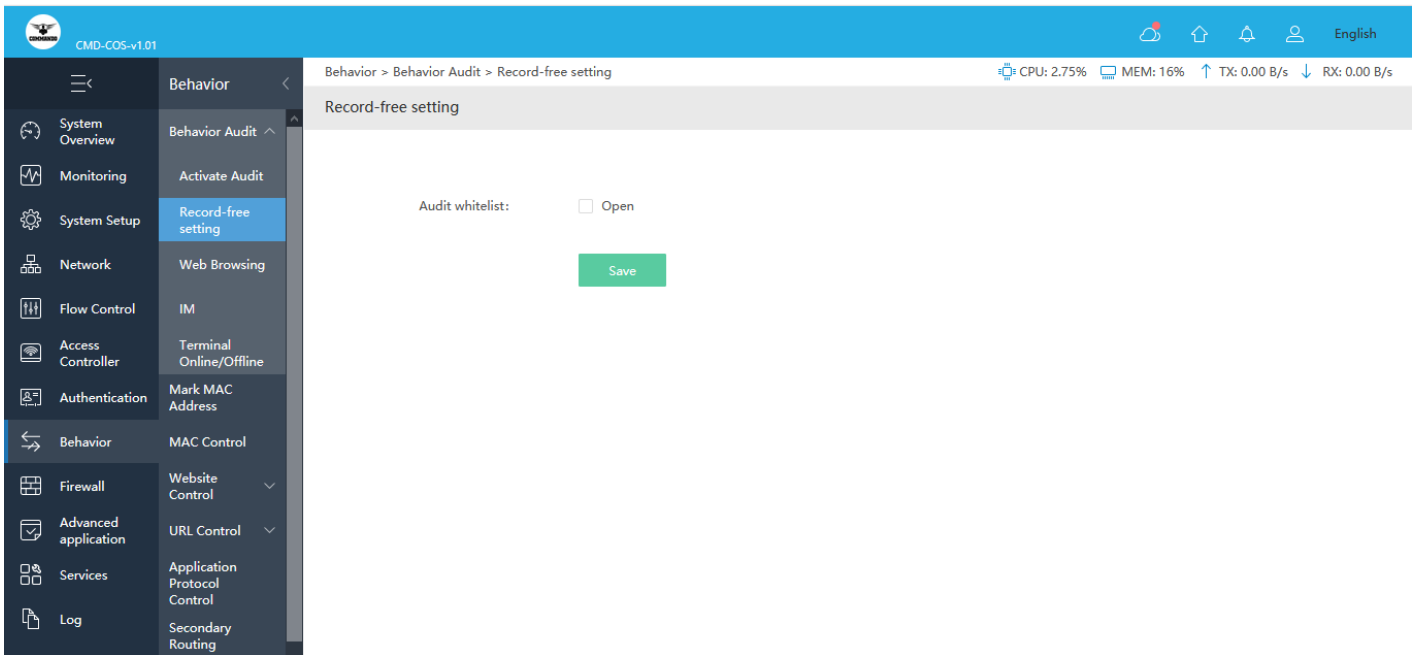


Fig 7.1.3 Default Record-free setting page

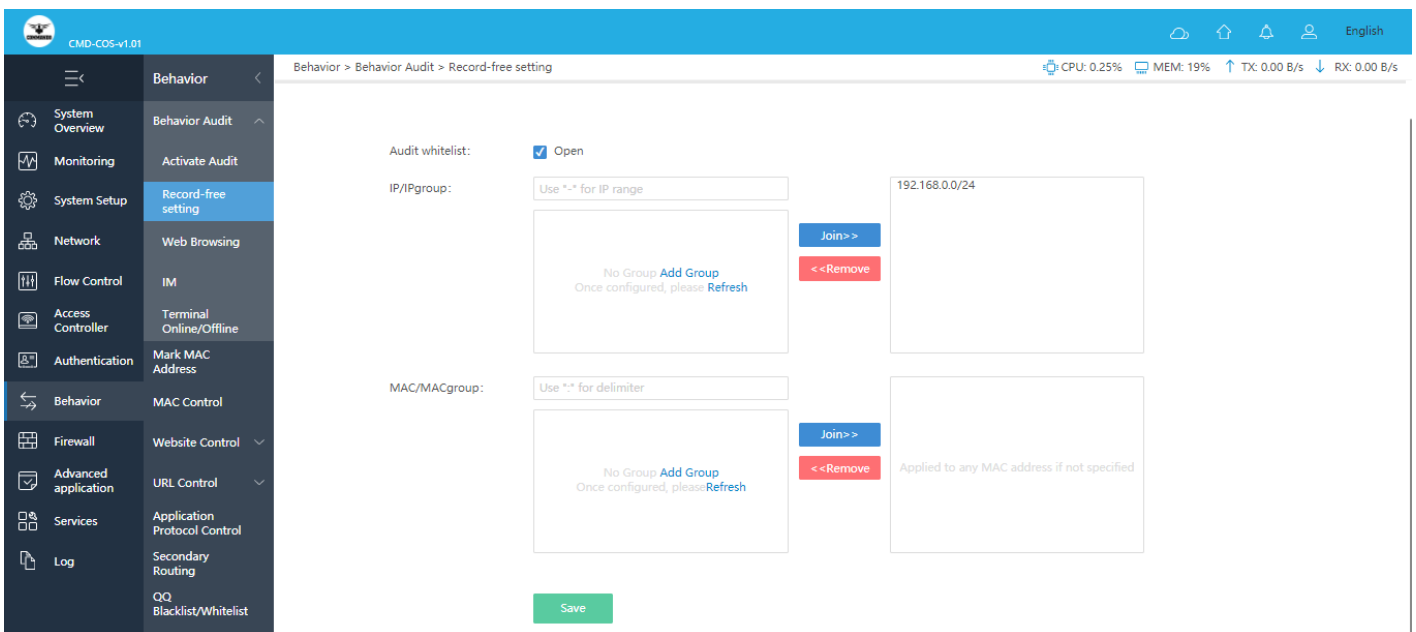


Fig 7.1.4 Enabling Record-free setting page

## 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

The screenshot shows the 'Viewing Web Browsing History' page in the CMD-COS-v1.01 interface. The left sidebar contains a navigation menu with 'Web Browsing' selected under the 'Behavior' category. The main content area features search filters for 'Begin Time', 'End Time', and 'IP/MAC/Web Browsing'. Below the filters is a table with columns 'Time', 'Ip Addr', 'MAC', 'Site Record', and 'Remarks', which currently displays 'No Data'.

Fig 7.1.5 Default Viewing Web Browsing History page

The screenshot shows the 'Viewing Web Browsing History' page in the CMD-COS-v1.01 interface. The left sidebar contains a navigation menu with 'Web Browsing' selected under the 'Behavior' category. The main content area features search filters for 'Begin Time', 'End Time', and 'IP/MAC/Web Browsing'. Below the filters is a table with columns 'Time', 'Ip Addr', 'MAC', 'Site Record', and 'Remarks'. The table contains the following data:

Time	Ip Addr	MAC	Site Record	Remarks
2021-05-09 21:54:24	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons2.gvt2.com/	
2021-05-09 21:53:53	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gvt2.com/	
2021-05-09 21:53:41	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-05-09 21:53:35	192.168.0.103	c4:d9:87:a7:ad:46	https://google.com/	
2021-05-09 21:52:53	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons2.gvt2.com/	
2021-05-09 21:52:35	192.168.0.103	c4:d9:87:a7:ad:46	https://sl-log.oray.net/	
2021-05-09 21:52:32	192.168.0.103	c4:d9:87:a7:ad:46	https://rc10-fc04.oray.com/	
2021-05-09 21:52:31	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-05-09 21:52:30	192.168.0.103	c4:d9:87:a7:ad:46	https://slapi.oray.net/	
2021-05-09 21:52:17	192.168.0.103	c4:d9:87:a7:ad:46	https://play.google.com/	

At the bottom of the table, there is a pagination control showing 'PerPage 10', 'Rows 1 2 3 4 5', and a 'Jump' button.

Fig 7.1.6 Viewing Web Browsing History page



The screenshot shows the CMD-COS-v1.01 interface. The left sidebar contains a navigation menu with categories like System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Behavior' category is expanded, showing sub-items like Behavior Audit, Activate Audit, Record-free setting, Web Browsing (highlighted), IM, Terminal Online/Offline, Mark MAC Address, MAC Control, Website Control, URL Control, Application Protocol Control, and Secondary Routing.

The main content area is titled 'Behavior > Behavior Audit > Web Browsing' and 'Viewing Web Browsing History'. It features a search bar with 'Begin Time', 'End Time', and 'IP/MAC/Web Browsing Q' fields. There are 'export' and 'Clean All' buttons. Below the search bar is a table with the following data:

Time	Ip Addr	MAC	Site Record	Remarks
2021-04-18 17:37:07	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-04-18 17:36:50	192.168.0.14	c4:d9:87:a7:ad:46	https://dmp100dmpprodstorage.table.core.windows.net/	
2021-04-18 17:36:06	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-04-18 17:36:04	192.168.0.14	c4:d9:87:a7:ad:46	https://i.ytimg.com/	
2021-04-18 17:35:58	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-04-18 17:35:58	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons3.gvt2.com/	
2021-04-18 17:35:54	192.168.0.14	c4:d9:87:a7:ad:46	https://android.clients.google.com/	
2021-04-18 17:35:54	192.168.0.14	c4:d9:87:a7:ad:46	https://dns.google/	
2021-04-18 17:35:16	192.168.0.14	c4:d9:87:a7:ad:46	https://i.ytimg.com/	
2021-04-18 17:34:59	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gvt2.com/	

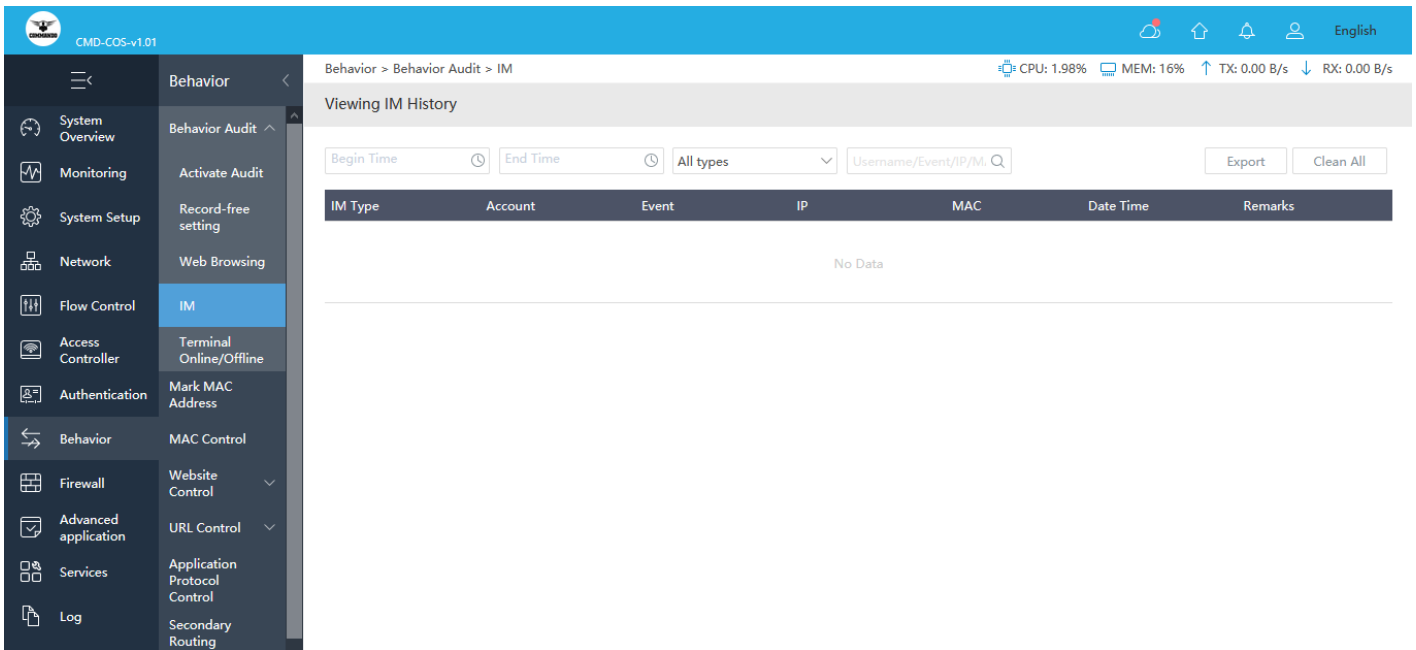
At the bottom, there is a pagination control showing 'PerPage 10', 'Rows', and page numbers 1, 2, 3, 4, 5, with a 'Jump' button.

**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.

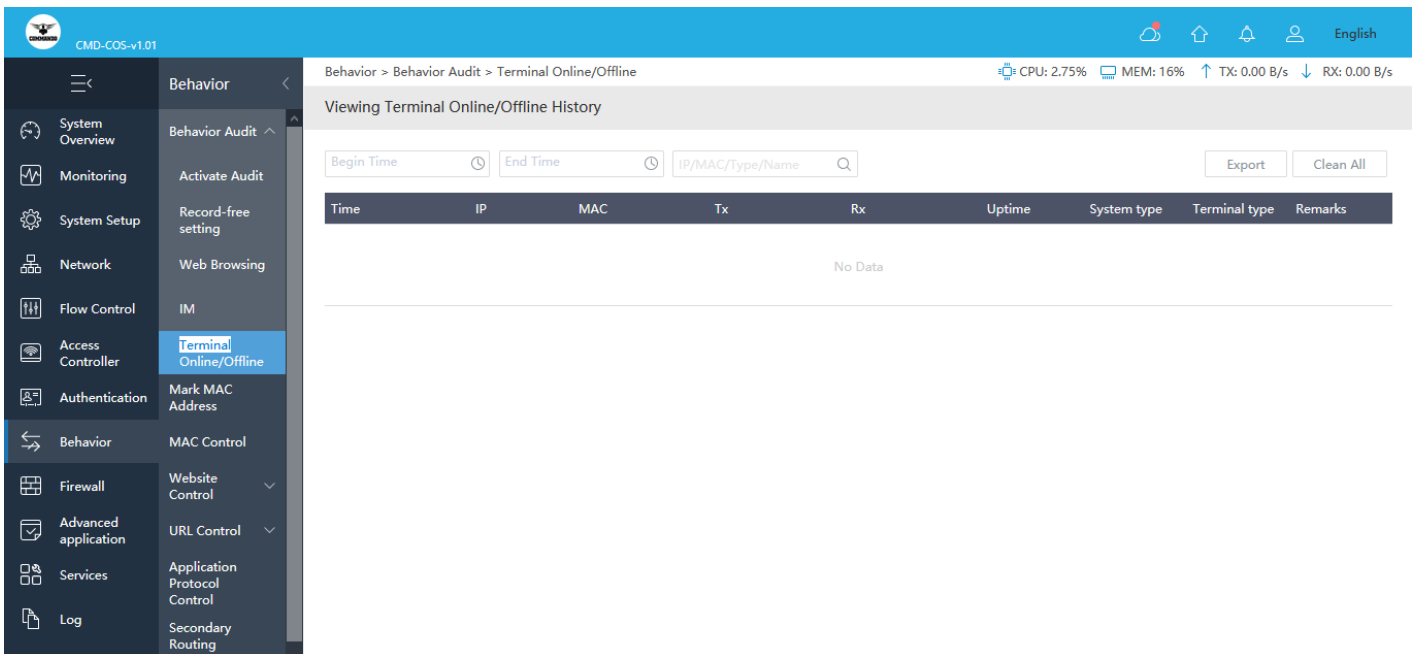
For Viewing IM History, Click on Behavior > Behavior Audit > IM



**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**

Time	IP	MAC	Tx	Rx	Uptime	System type	Terminal type	Remarks
2021-04-18 22:01:37	192.168.0.11	20:a6:0c:37:4d:13	106.53 KB	152.41 KB	1m 23s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:56:15	192.168.0.11	20:a6:0c:37:4d:13	873.68 KB	2.38 MB	17m 45s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:52:42	192.168.0.11	20:a6:0c:37:4d:13	163.92 KB	1.22 MB	3m 18s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:46:00	192.168.0.11	20:a6:0c:37:4d:13	13.52 KB	13.11 KB	2m	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:44:57	192.168.0.100	c4:d9:87:a7:ad:46	245.02 KB	37.57 KB	7m 3s	Unknown	Intel	Static%20Binding
2021-04-18 21:39:46	192.168.0.12	00:6f:64:f9:6e:a8	5.24 KB	3.76 KB	1m 15s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:37:06	192.168.0.12	00:6f:64:f9:6e:a8	3.38 KB	5.96 KB	1m 55s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:34:57	192.168.0.12	00:6f:64:f9:6e:a8	21.17 KB	35.64 KB	1m 4s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:34:29	192.168.0.100	c4:d9:87:a7:ad:46	4.2 MB	26.29 MB	58m 31s	Unknown	Intel	Static%20Binding
2021-04-18 21:33:00	192.168.0.12	00:6f:64:f9:6e:a8	10.19 KB	17.49 KB	1m 1s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:31:58	192.168.0.11	20:a6:0c:37:4d:13	14.03 MB	47.52 MB	1h 31m 3s	Android	Xiaomi	POCOF1-POCOF1
2021-04-18 21:29:51	192.168.0.12	00:6f:64:f9:6e:a8	49.49 KB	165.6 KB	2m 13s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:30:48	192.168.0.12	00:6f:64:f9:6e:a8	214 B	148 B	10s	Android	Samsung	android-3a03a33fd50a61c5
2021-04-18 21:24:14	192.168.0.11	20:a6:0c:37:4d:13	736.15 KB	1.4 MB	27m 46s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:17:35	192.168.0.11	20:a6:0c:37:4d:13	10.51 MB	190.52 MB	28m 25s	Android	Xiaomi	POCOF1-POCOF1
2021-04-18 21:16:56	192.168.0.11	20:a6:0c:37:4d:13	1.55 MB	6.77 MB	4m 4s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:09:31	192.168.0.11	20:a6:0c:37:4d:13	822.48 KB	1.65 MB	7m 29s	Linux	Xiaomi	POCOF1-POCOF1
2021-04-18 21:07:37	192.168.0.100	c4:d9:87:a7:ad:46	1.29 MB	7.58 MB	21m 23s	Windows10	Intel	Static%20Binding
2021-04-18 21:06:40	192.168.0.10	08:9b:4b:99:a3:94	2.22 KB	2.74 KB	22m 20s	Unknown	iKuai	AP%20blacklisted
2021-04-18 21:01:52	192.168.0.100	c4:d9:87:a7:ad:46	169.61 KB	294.86 KB	5m 8s	Windows10	Intel	Static%20Binding

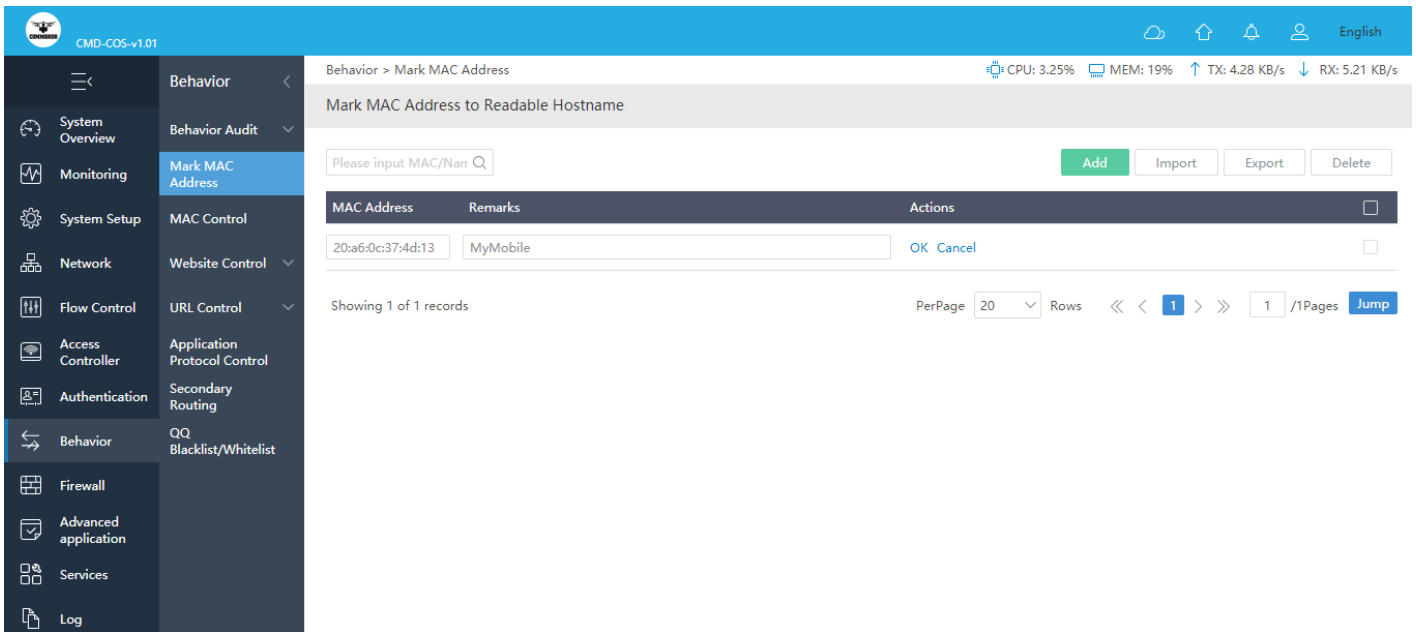
**Fig 7.1.10 Viewing Terminal Online/Offline History page**

## 7.2 Mark MAC Address

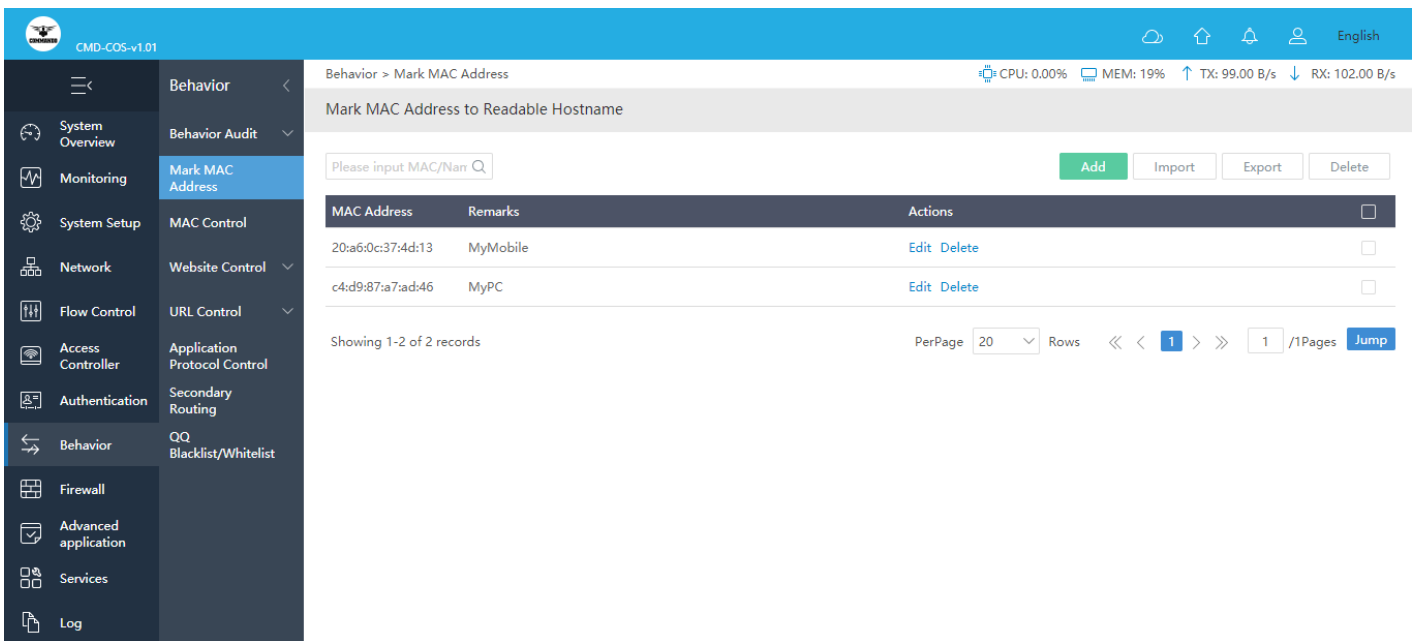
The MAC address is the physical address of a network interface can be marked to local hostname so to identify mac easily by human understandable names.

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**

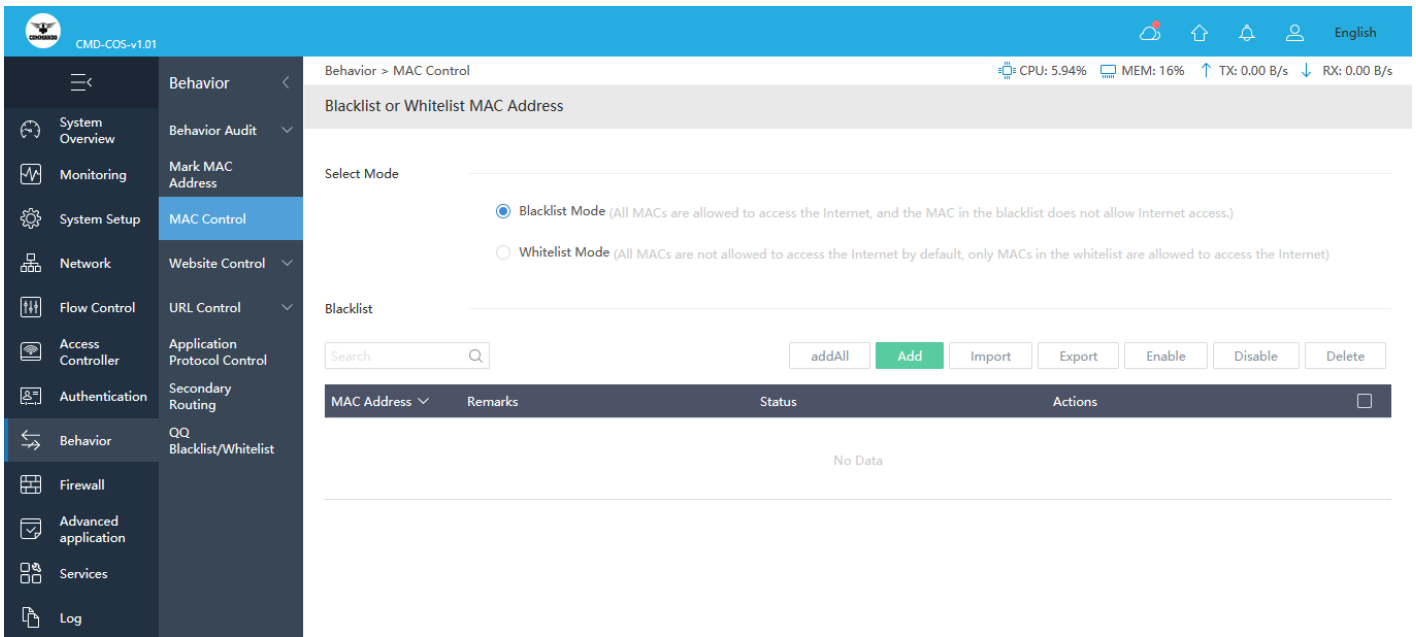


**Fig 7.2.3 Mark MAC Address to Readable Hostname page**

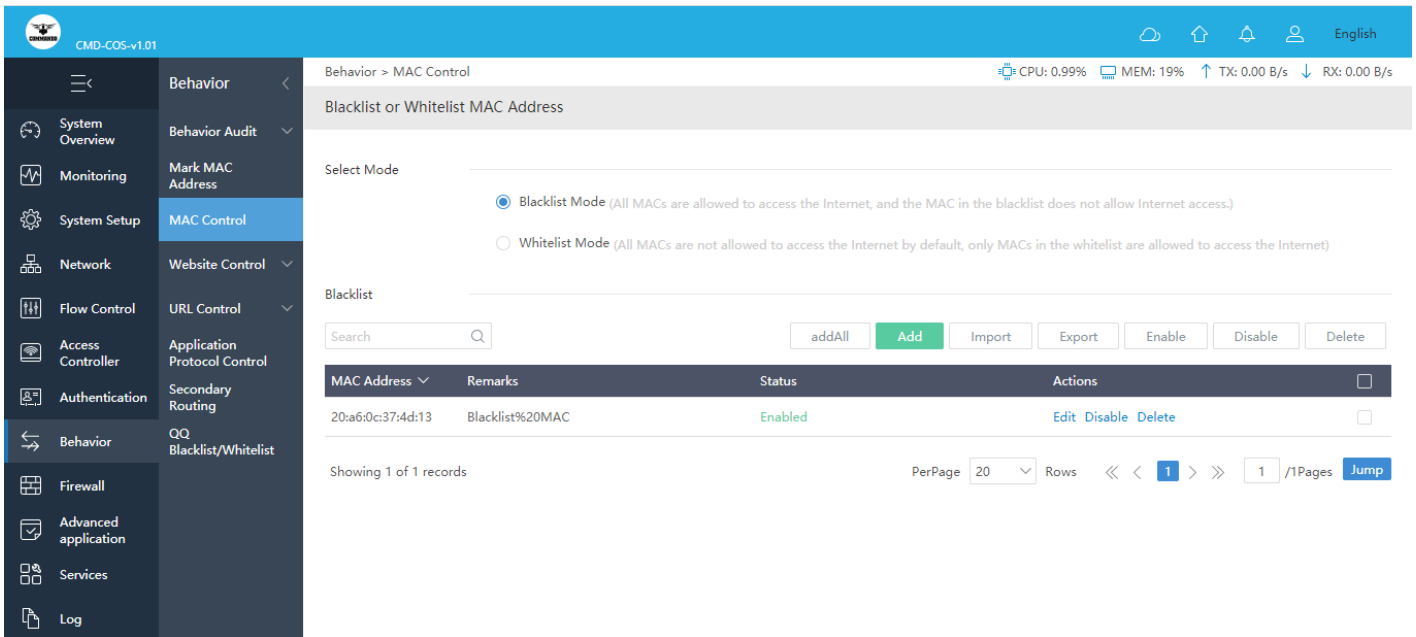
## 7.3 MAC Control

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**



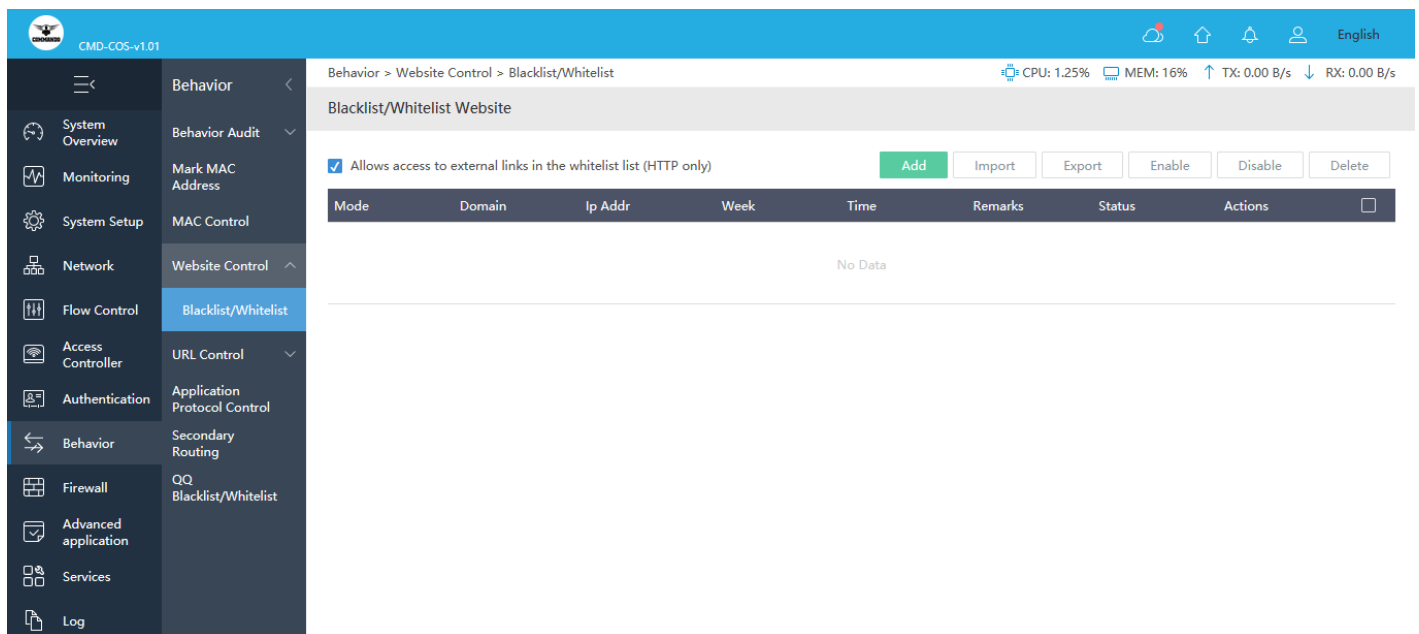
**Fig 7.3.2 Blacklist MAC Address page**

## 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**

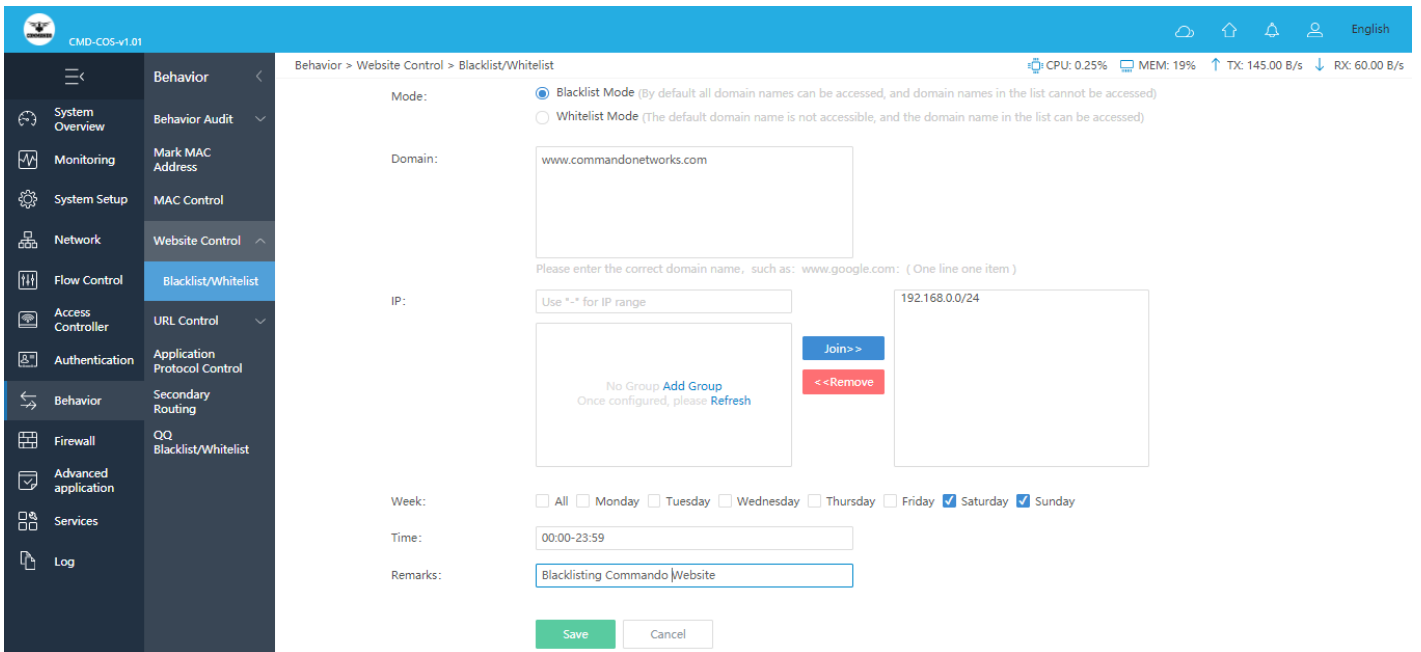


Fig 7.4.2 Blacklist particular Website page

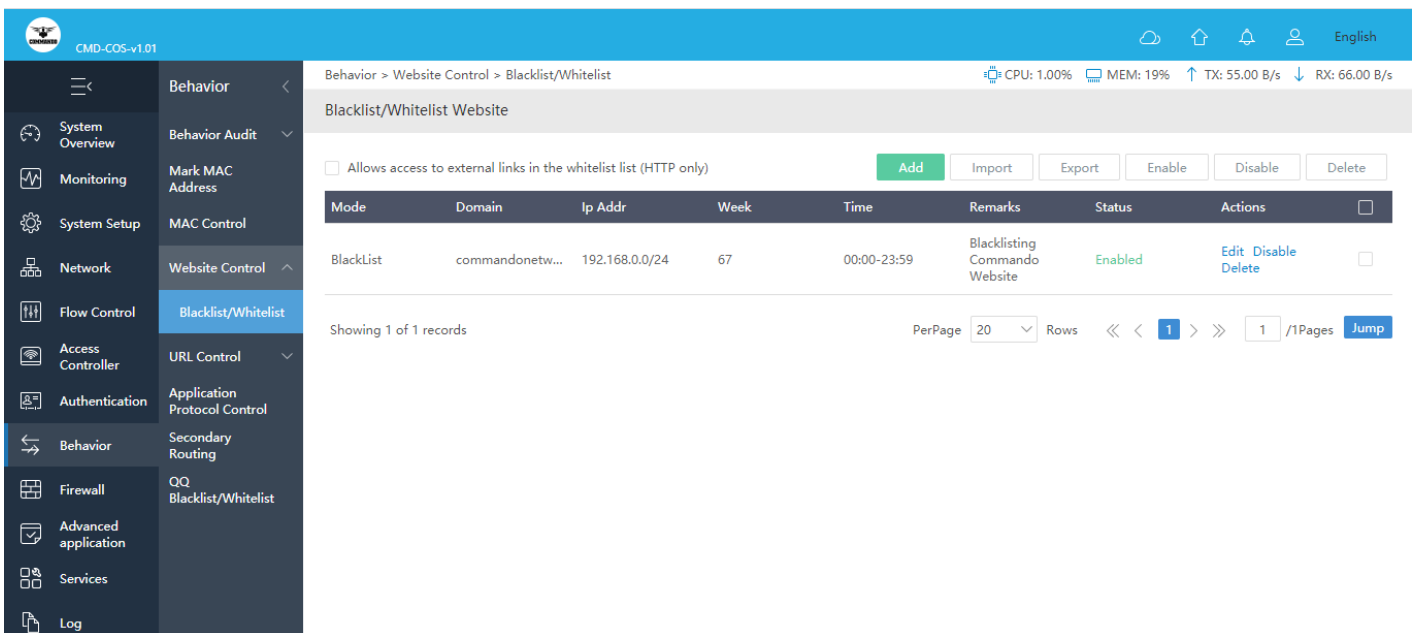


Fig 7.4.3 Blacklist Website page

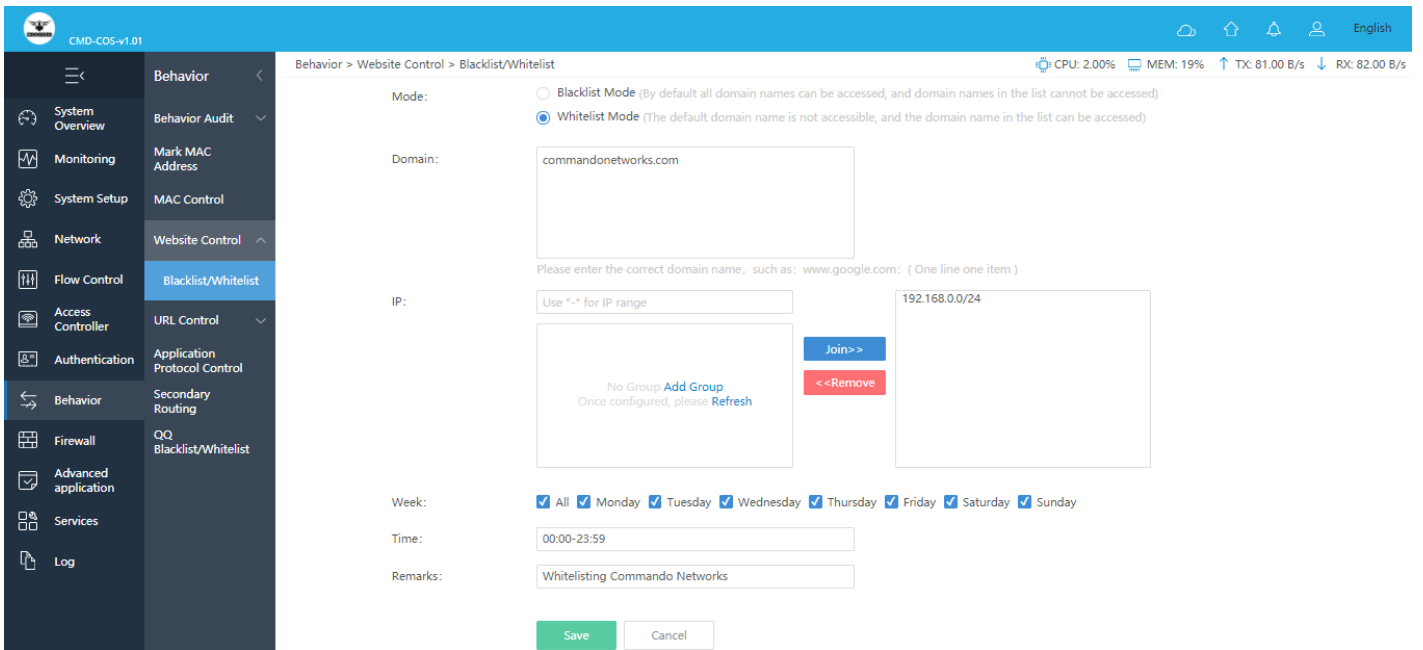


Fig 7.4.4 Whitelisting particular Website page



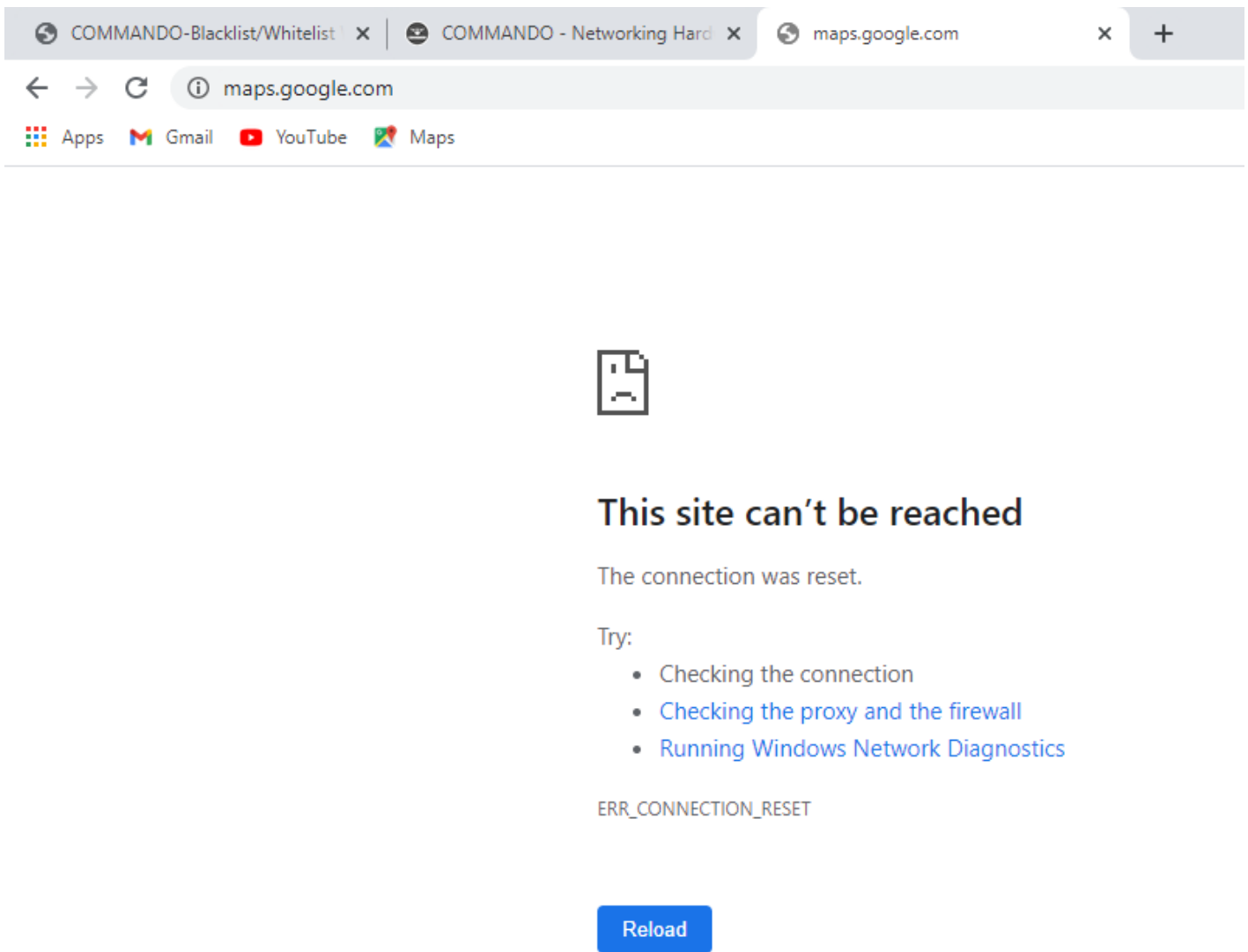


SCOUT E1000-LR: COMMANDO Scout E1000-LR Series I

# Fiber Media Converters

COMMANDO Copper Fast Ethernet/Gigabit To Fiber Converter, Single Mode Single/Dual Fiber, Multi Mode Single/Dual Fiber, 850nm To 1550nm, 550m To 60km. Ideal For Long Distance Transmission In Broadband, Campus Network, Cable TV, Intelligent Broadband And FTTB/FTTH Networks.





**Fig 7.4.5 Result of Whitelisting 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

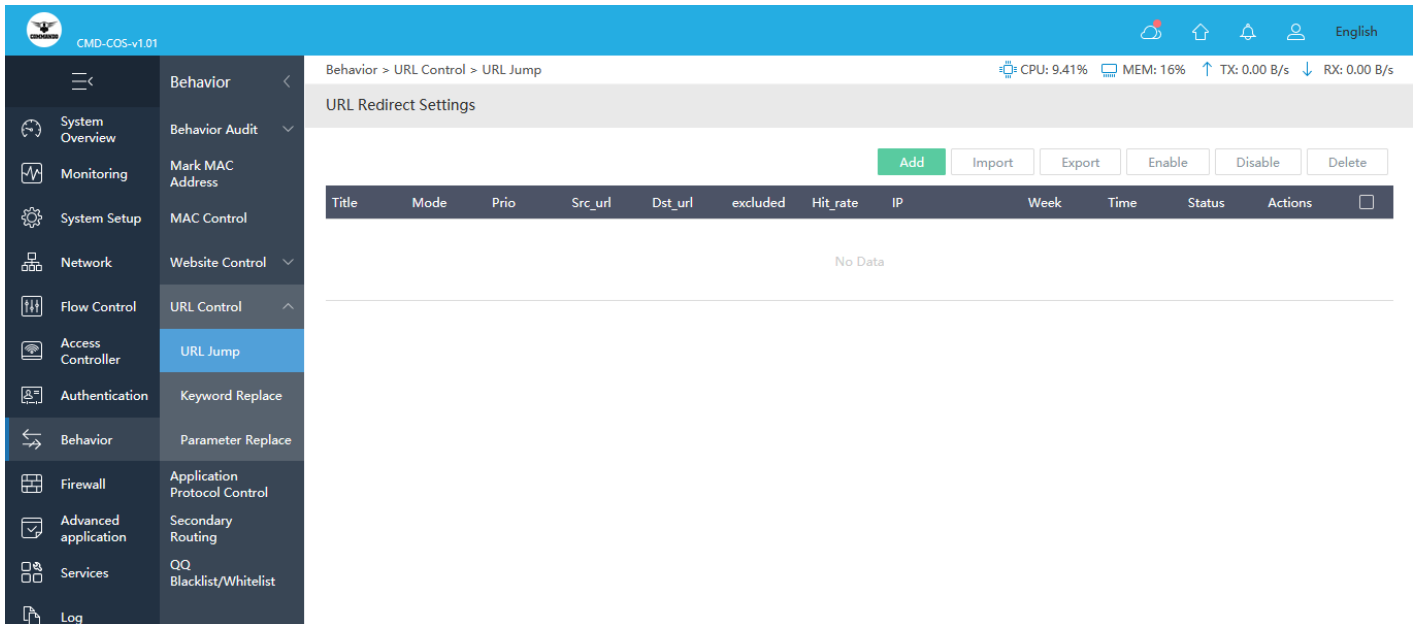


Fig 7.5.1 Default URL Redirect Settings page

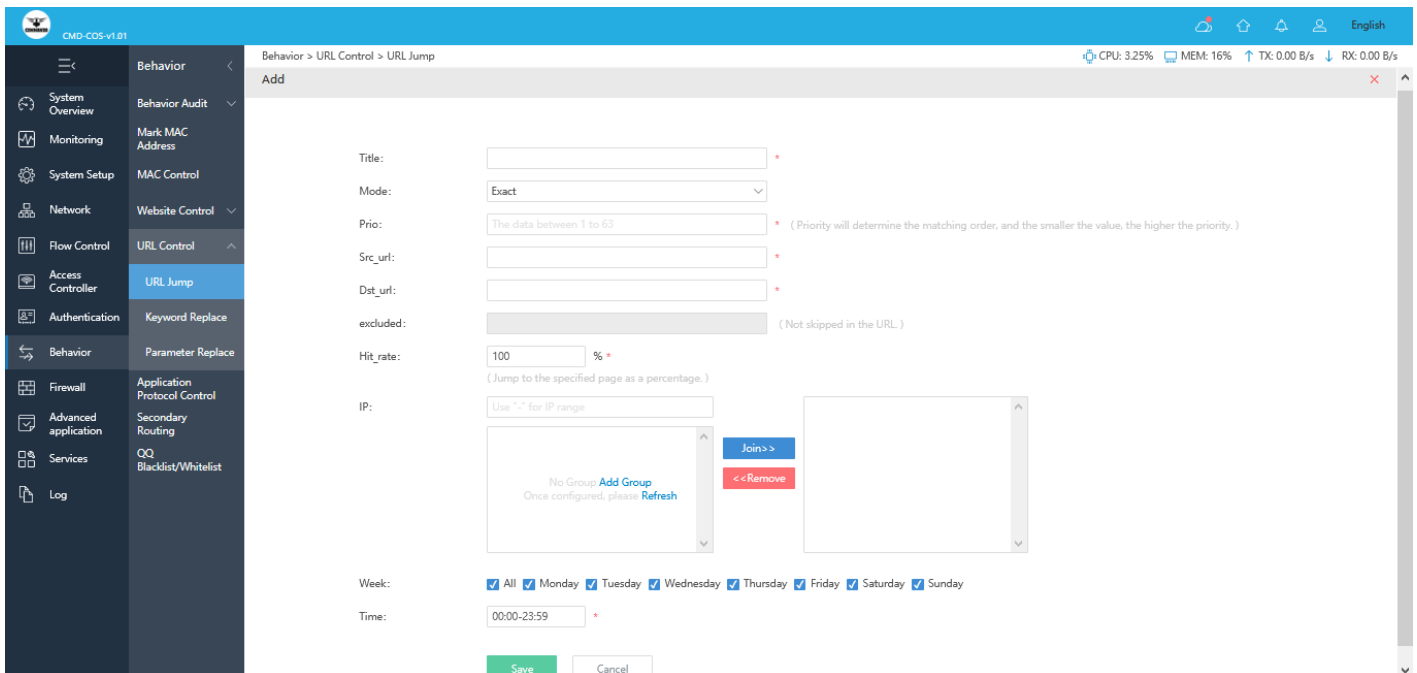
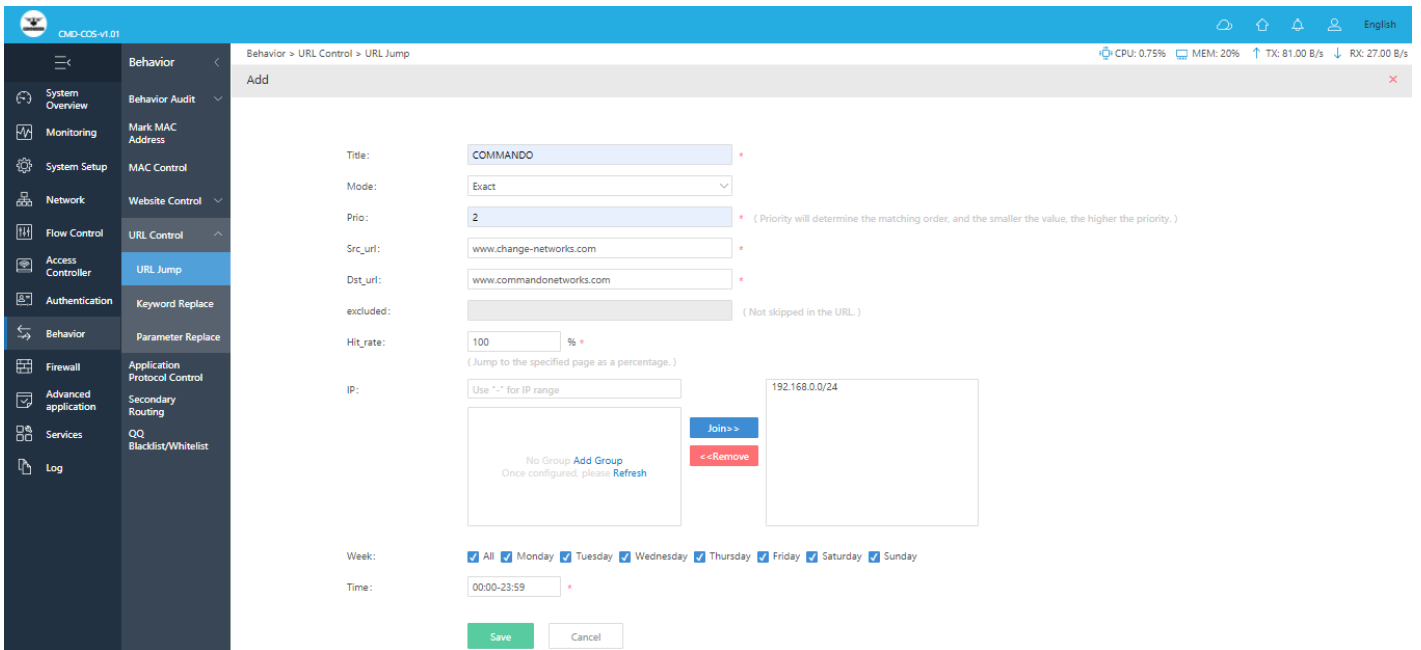
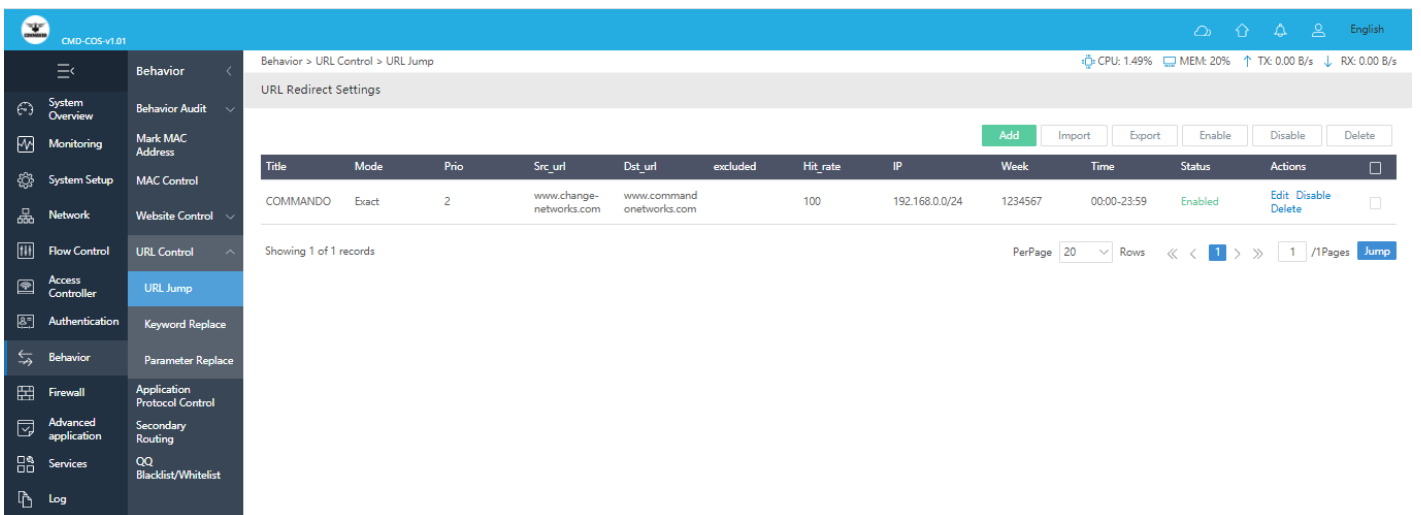


Fig 7.5.2 Add URL Redirect Settings page



**Fig 7.5.3 Add particular URL Redirect Settings page**



**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

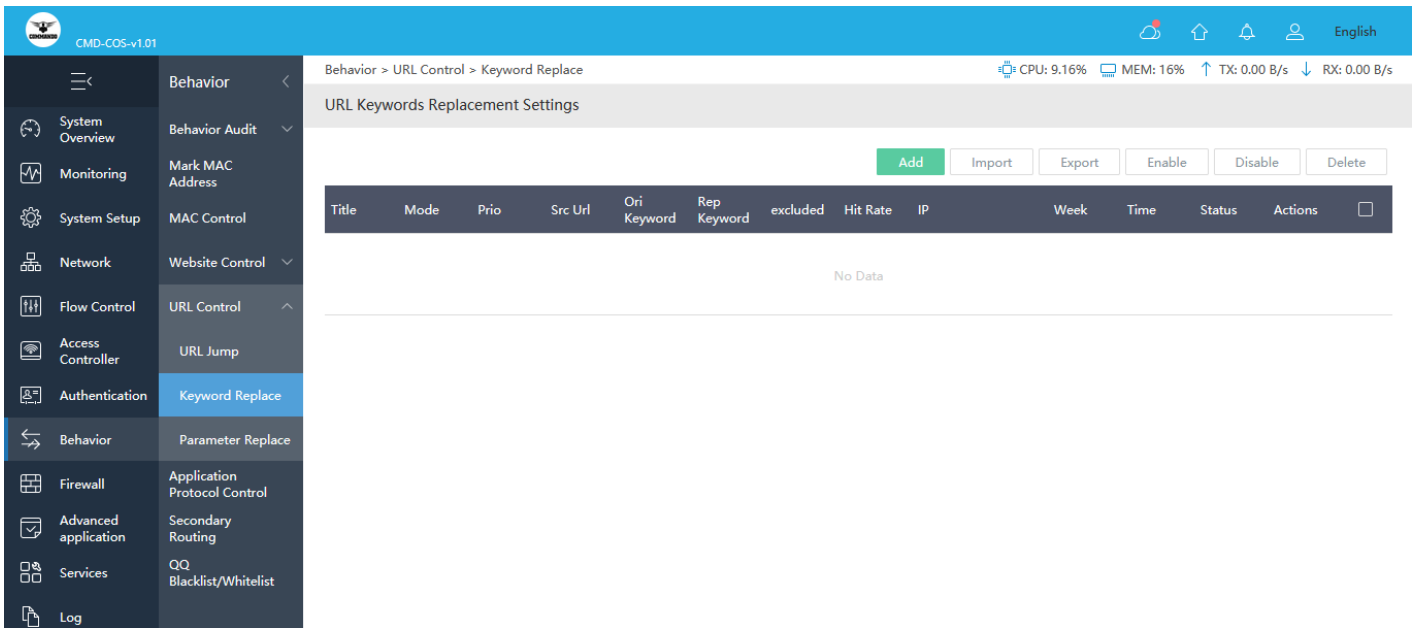


Fig 7.5.5 Default URL Keywords Replacement Settings page

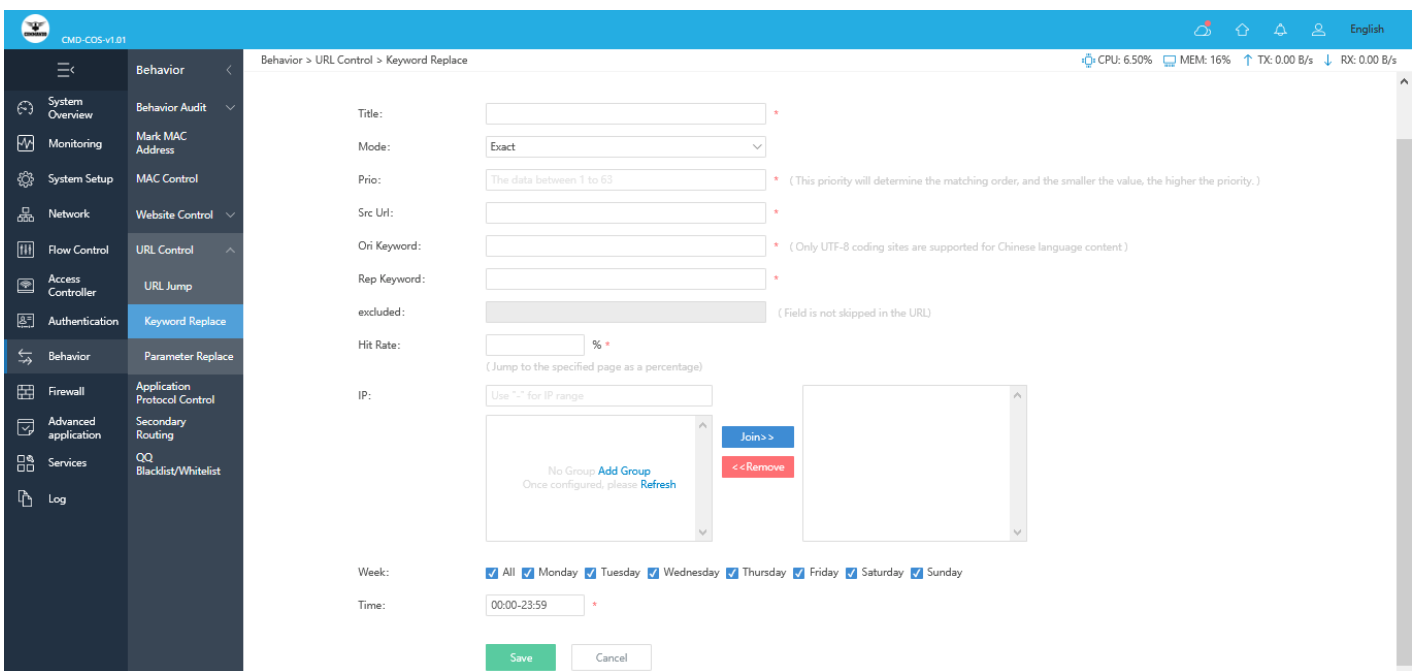
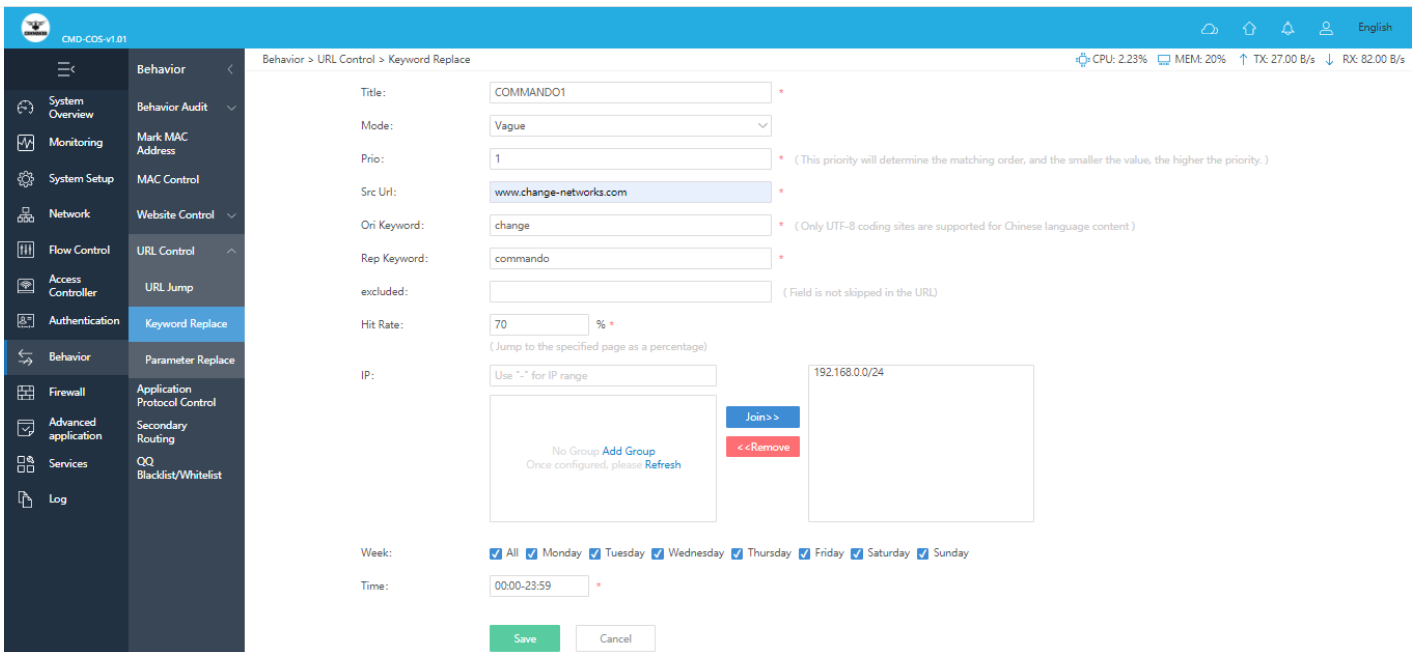
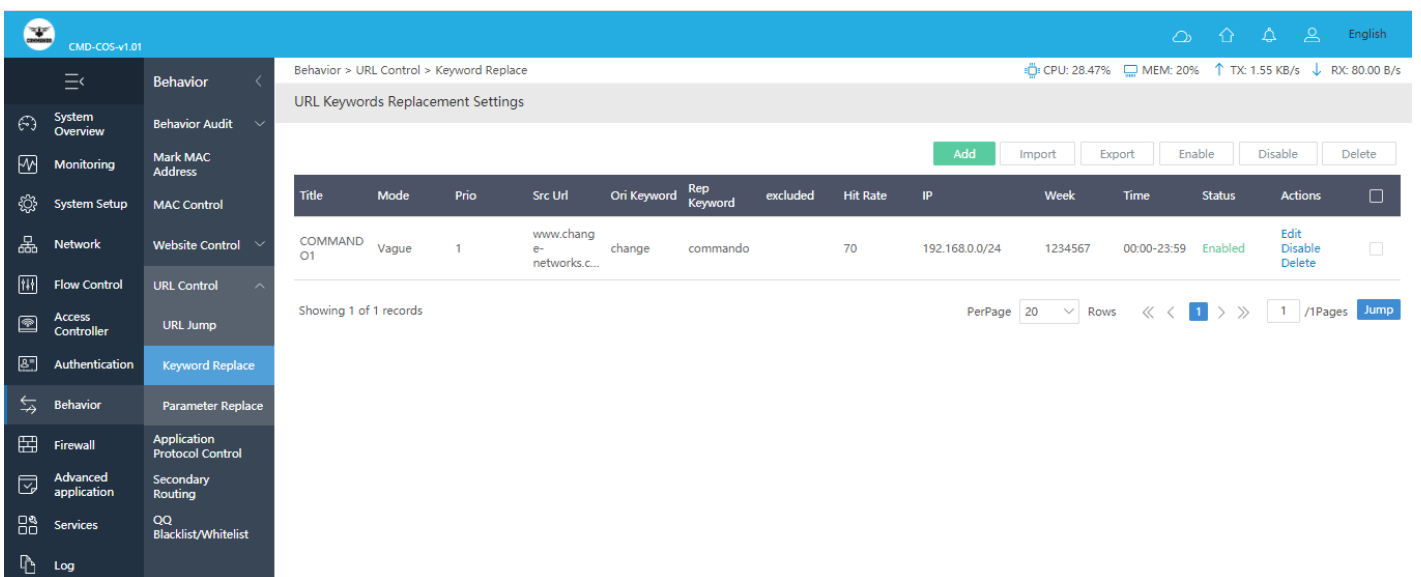


Fig 7.5.6 Add Keywords Replacement Settings page



**Fig 7.5.7 Keywords Replacement Settings with keyword page**



**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

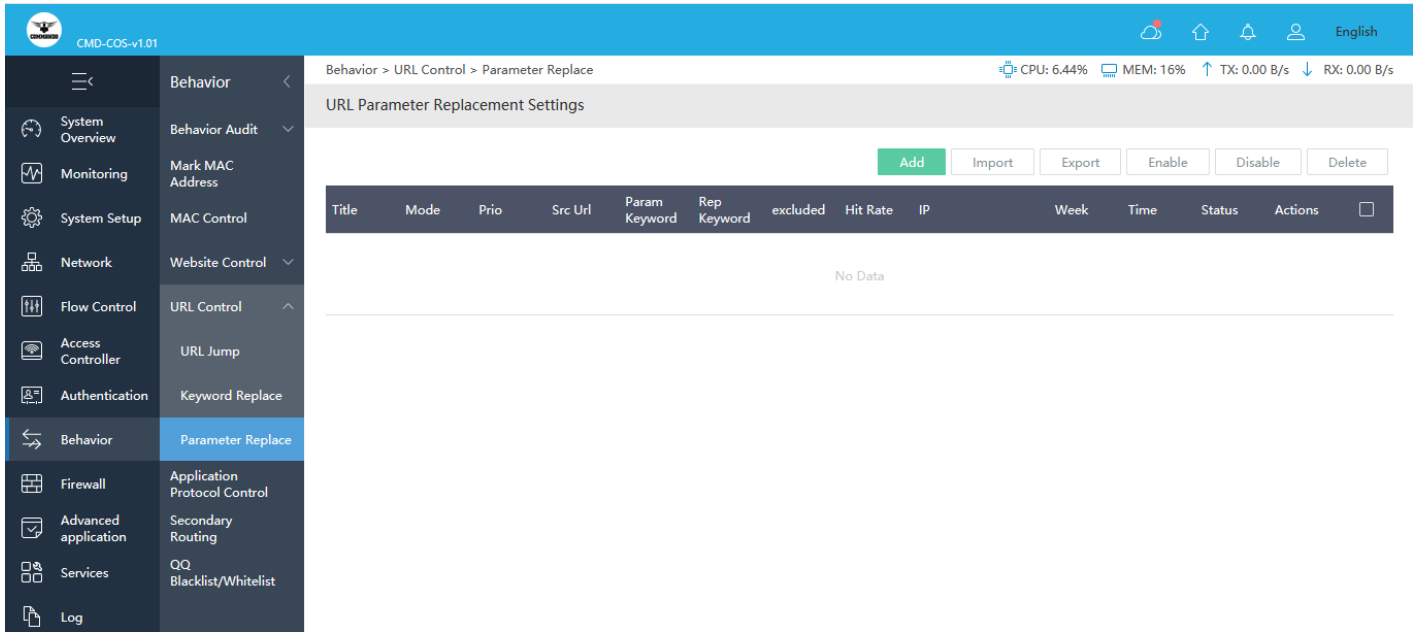


Fig 7.5.9 Default URL Parameter Replacement Settings page

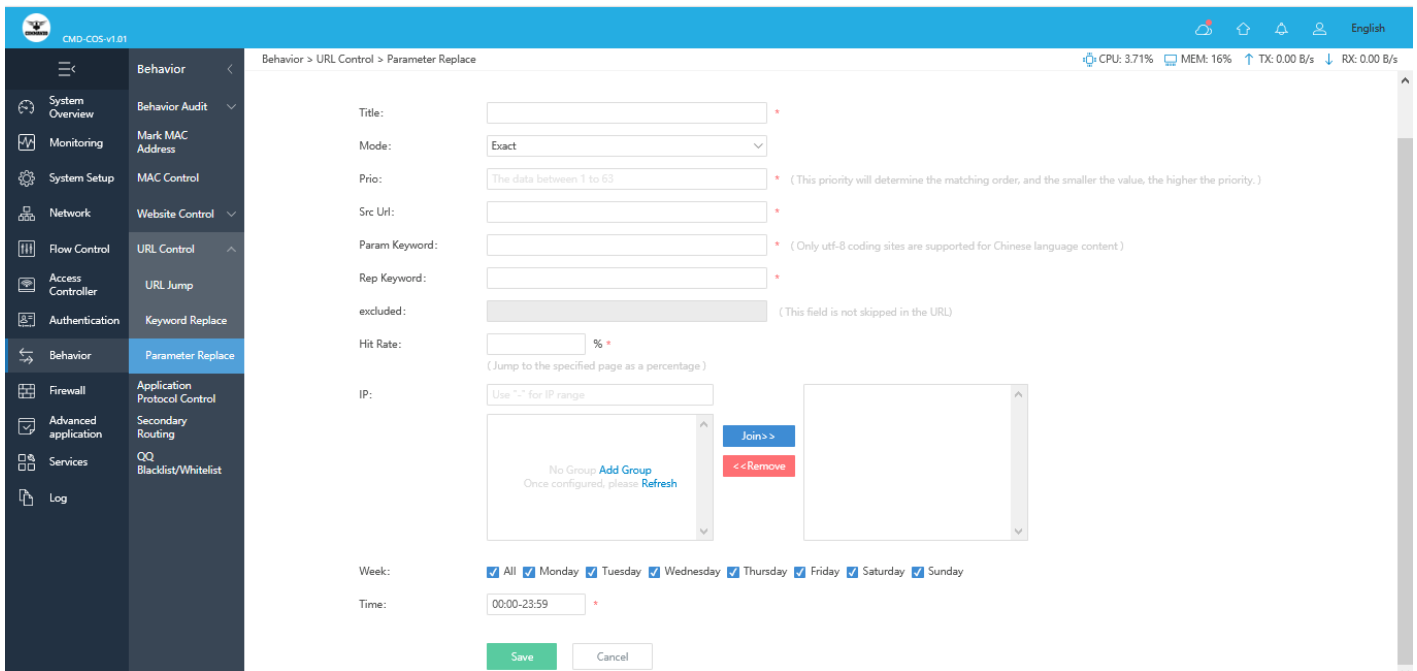
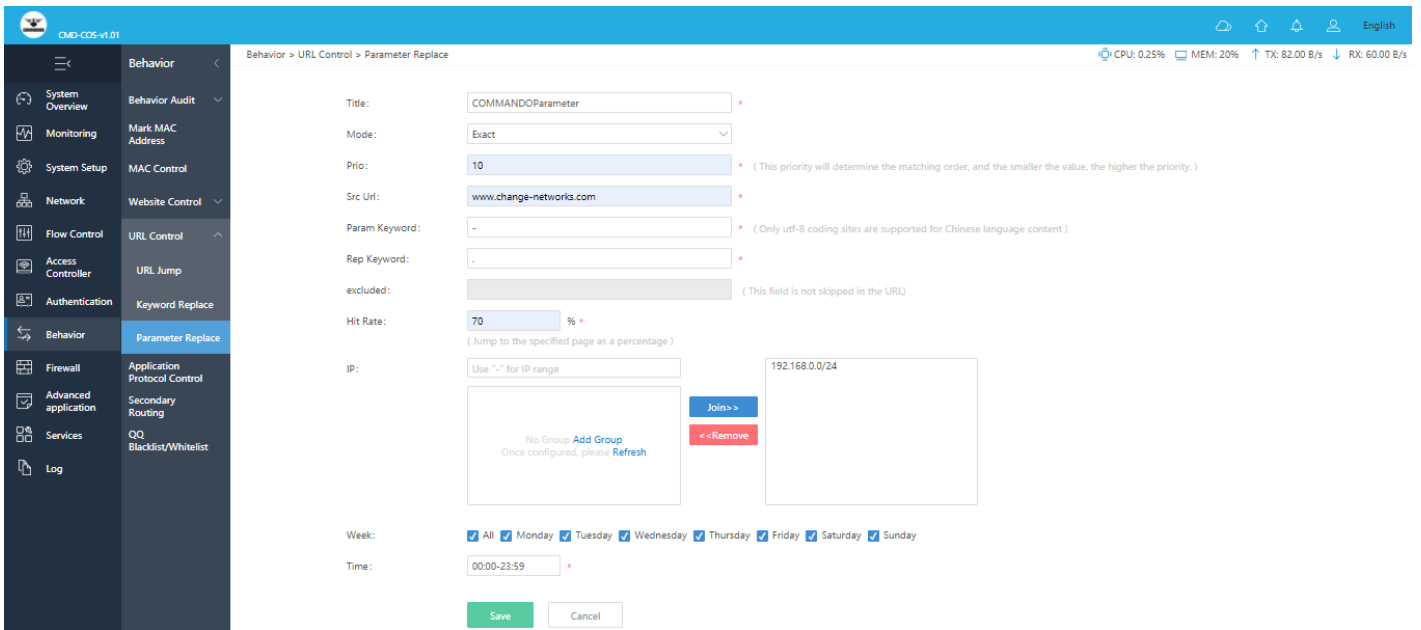
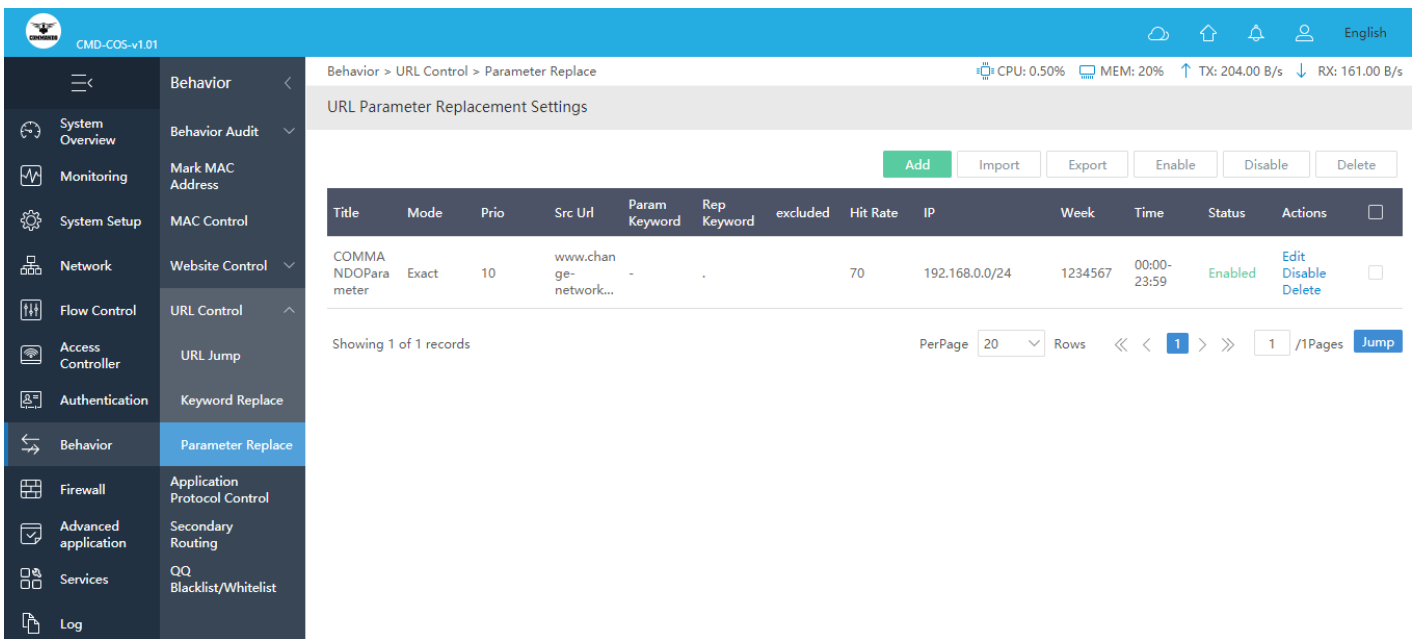


Fig 7.5.10 Add URL Parameter Replacement Settings page



**Fig 7.5.11 URL Parameter Replacement Settings add particular keyword page**



**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

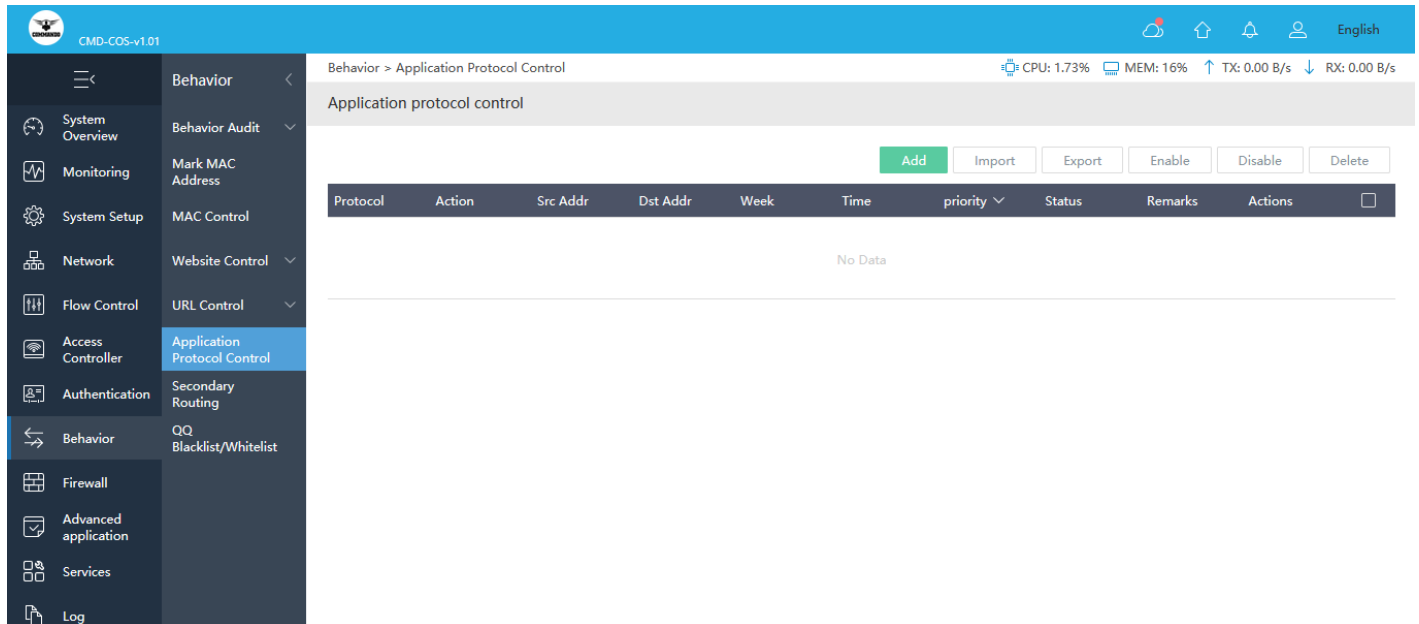


between 10 and 50.

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**

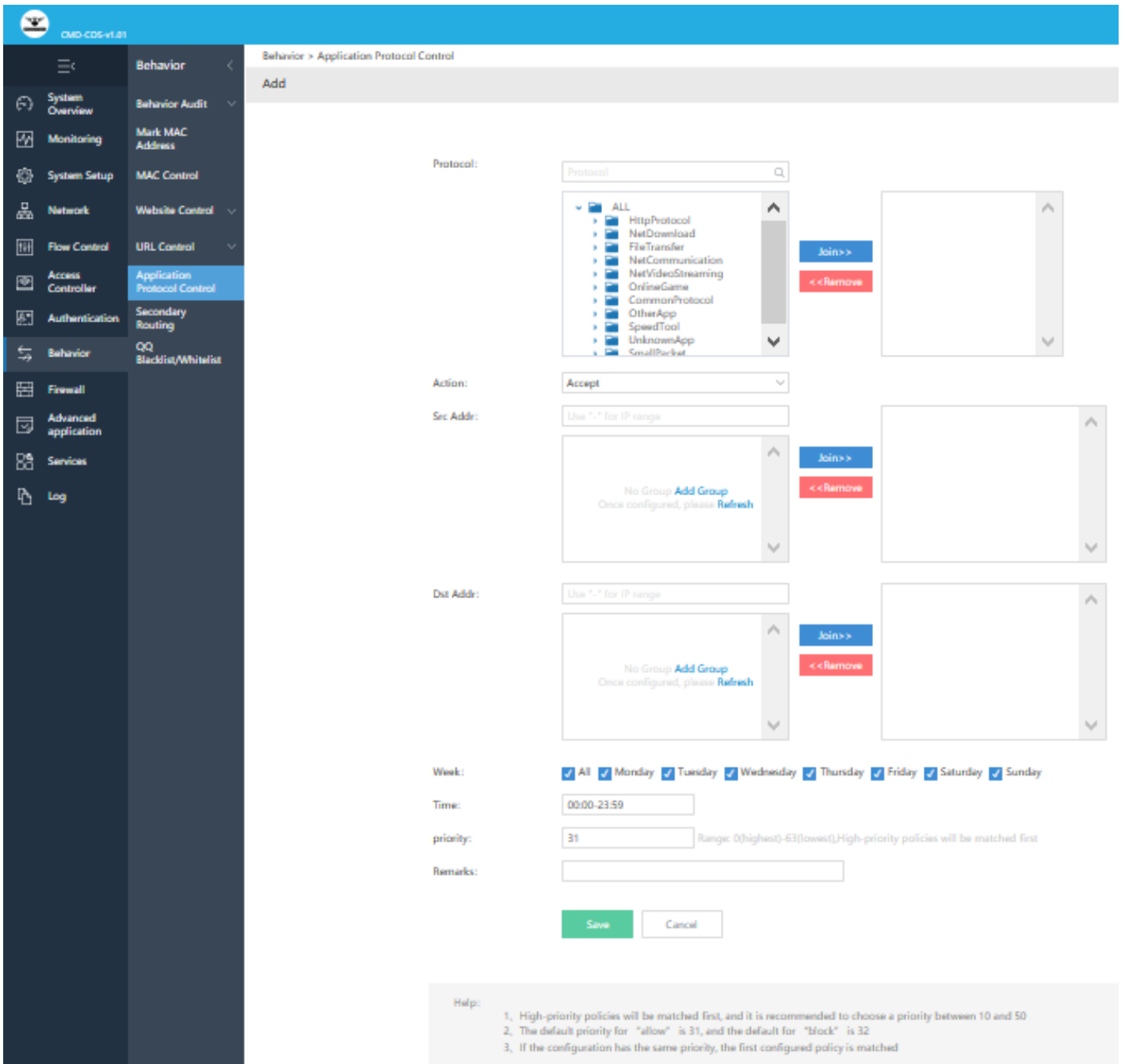
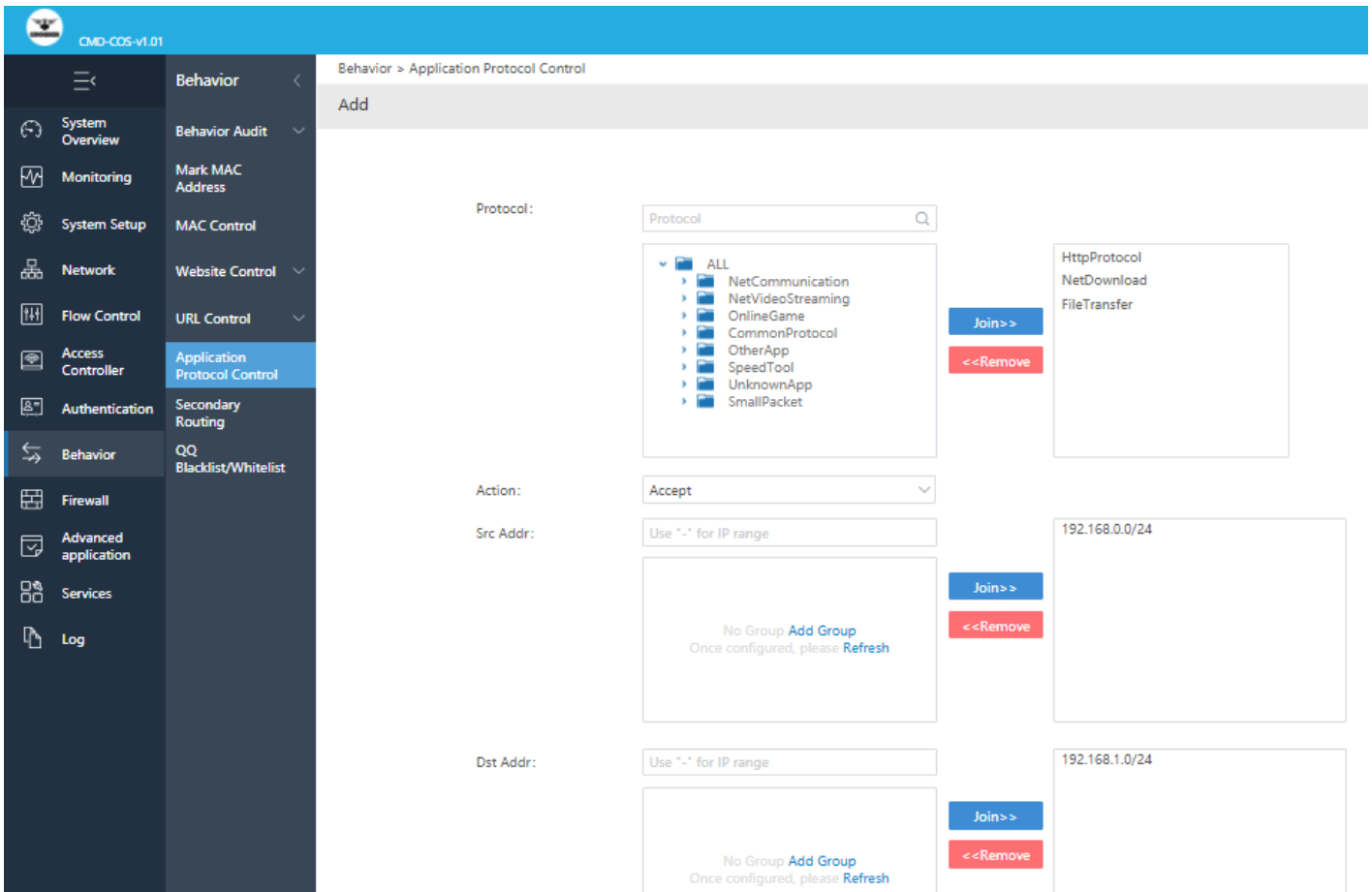
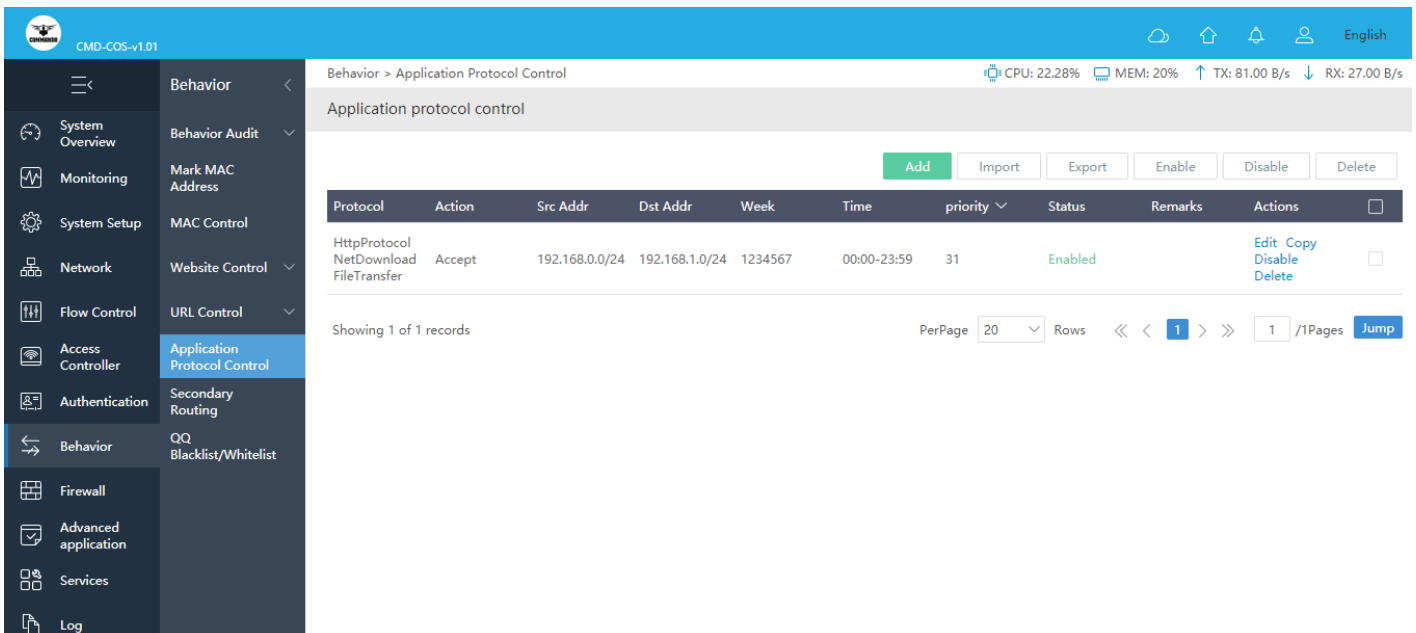


Fig 7.6.2 Add Application protocol control page



**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 routers, 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

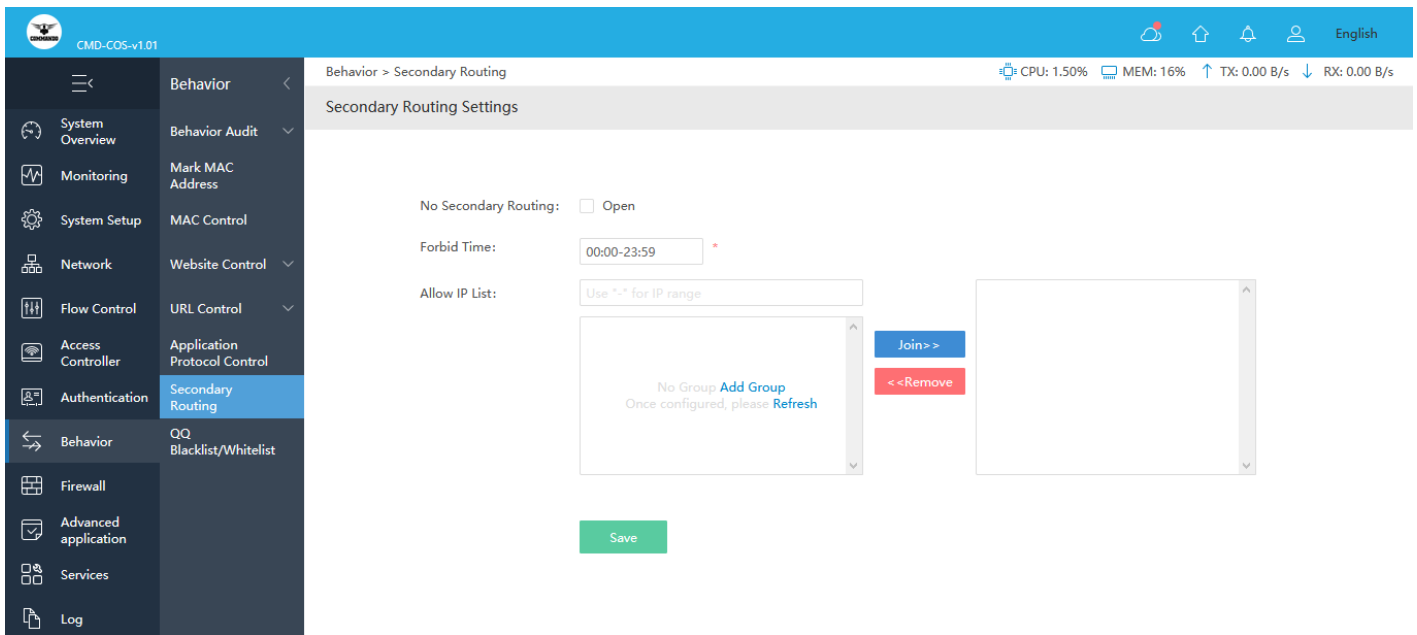


Fig 7.7.1 Default Secondary Routing Settings page

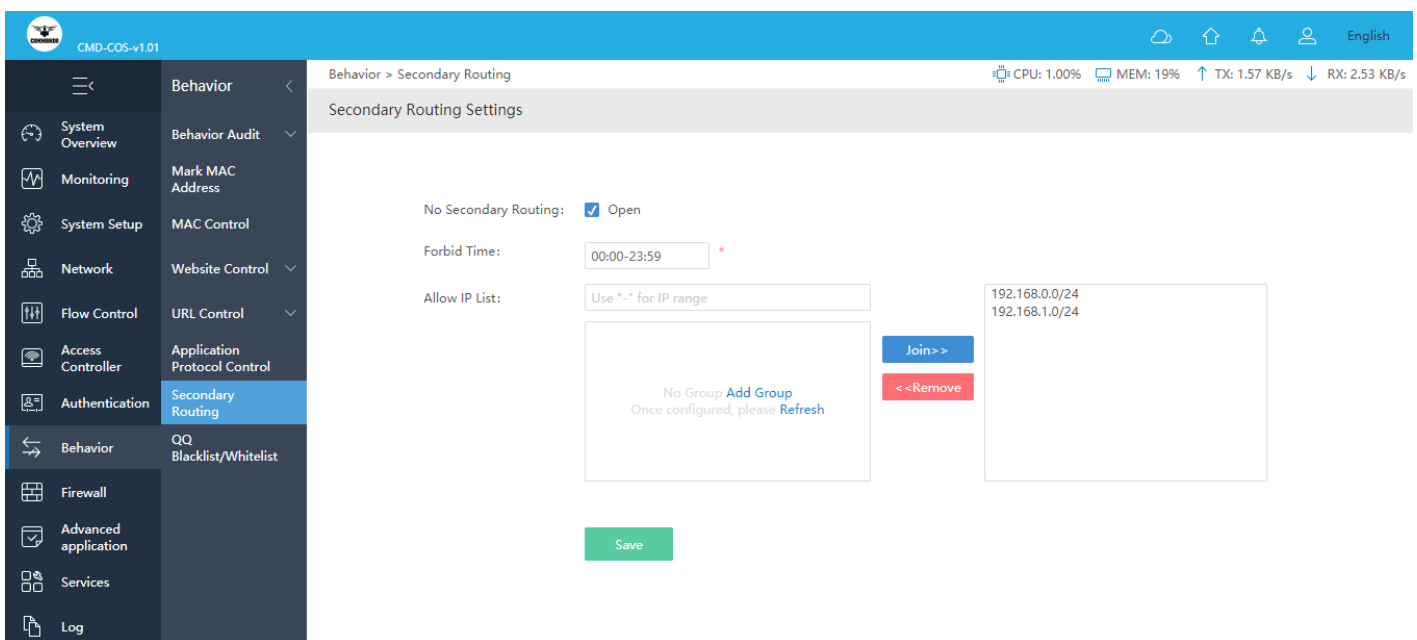
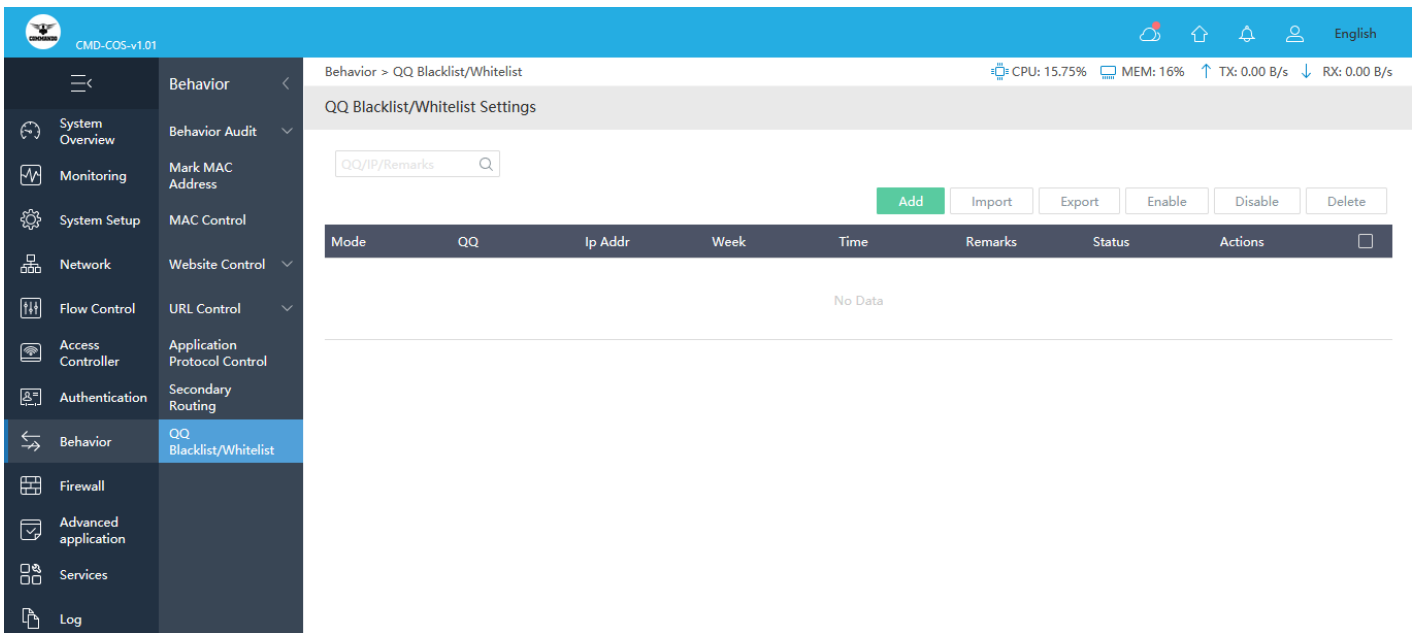


Fig 7.7.2 Secondary Routing Settings page

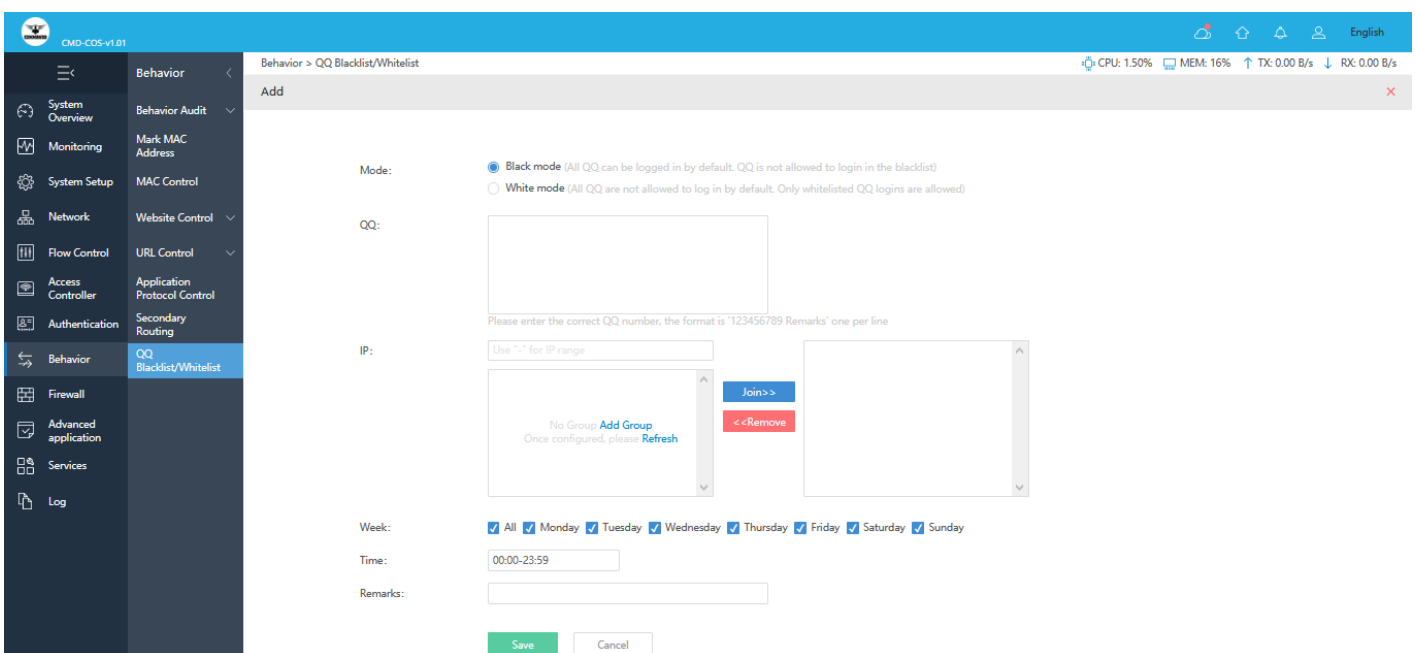
## 7.8 QQ Blacklist/Whitelist

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.

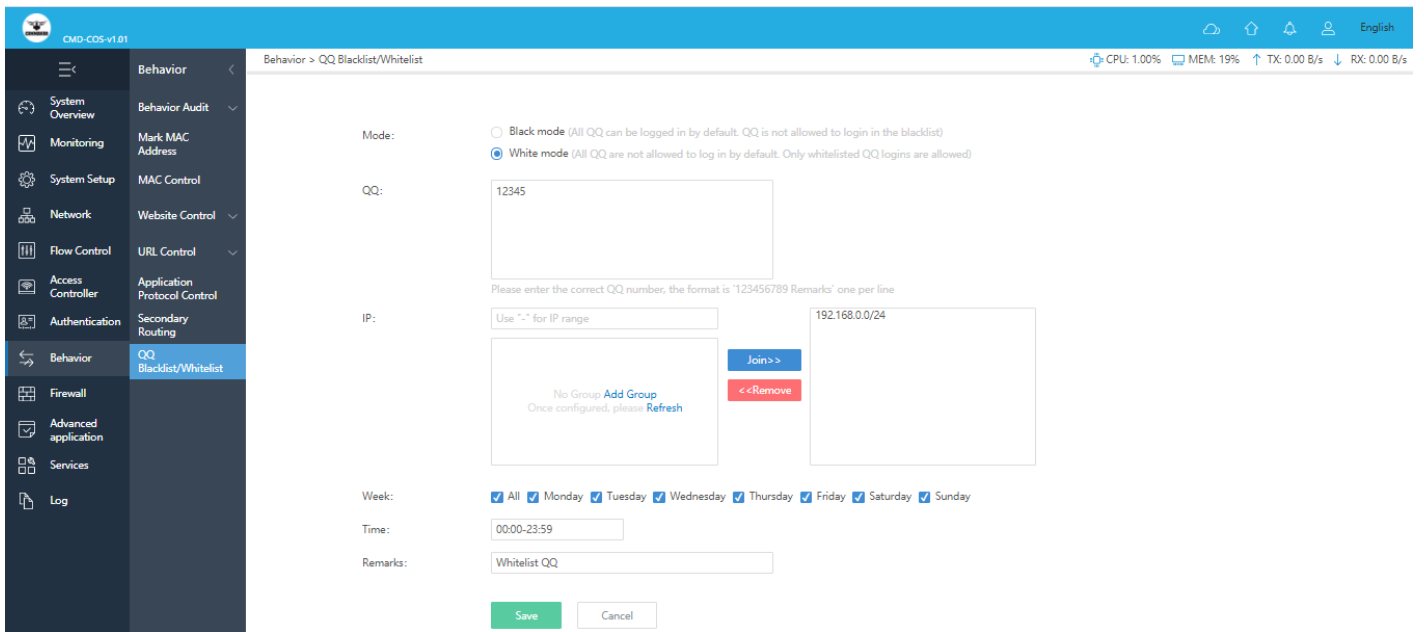
To configure QQ Blacklist/Whitelist Settings, Click on Behavior > QQ Blacklist/Whitelist



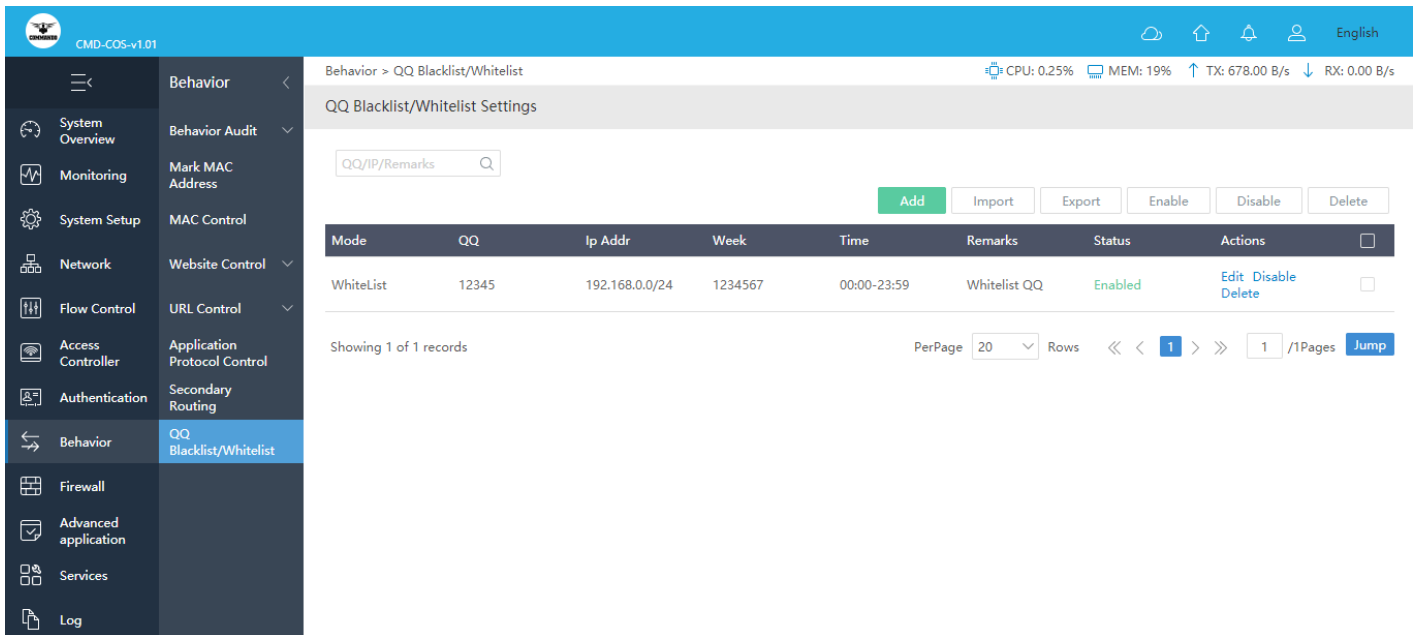
**Fig 7.8.1 Default QQ Blacklist/Whitelist Settings page**



**Fig 7.8.2 Add QQ Blacklist/Whitelist Settings page**



**Fig 7.8.3 QQ Blacklist/Whitelist Settings for particular Network page**



**Fig 7.8.4 QQ Blacklist/Whitelist Settings page**

# 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

CMD-COS-v1.01 English

CPU: 3.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Firewall > ACL Rules

### Access Control List Rules Settings

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

Protocol	Action	Direction	Src.Addr	Dst.Addr	Src.Port	Dst.Port	In.Interface	Out.Interface	Cycle	Period	Remarks	Status	Actions
No Data													

**Fig 8.1.1 Default Access Control List Rules page**



OMD-CDS-v1.01

Firewall > ACL Rules

Add

Protocol: any

Action: accept

Direction: forward

Connection direction matching: close

Src.Addr

IP: Use "\*" for IP range

No Group Add Group  
Once configured, please Refresh

Join >>

<< Remove

Dst.Addr

IP: 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

CMD-COS-v1.01

Firewall > ACL Rules

Protocol: icmp

Action: drop

Direction: forward

Connection direction matching: Original direction

Src.Addr

IP: Use "\*" for IP range 192.168.0.0/24

No Group Add Group  
Once configured, please Refresh

Join > << Remove

Dst.Addr

IP: Use "\*" for IP range 192.168.1.0/24

No Group Add Group  
Once configured, please Refresh

Join > << Remove

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

CMD-COS-v1.01

Firewall > ACL Rules

CPU: 5.00% MEM: 19% TX: 397.00 B/s RX: 0.00 B/s

Access Control List Rules Settings

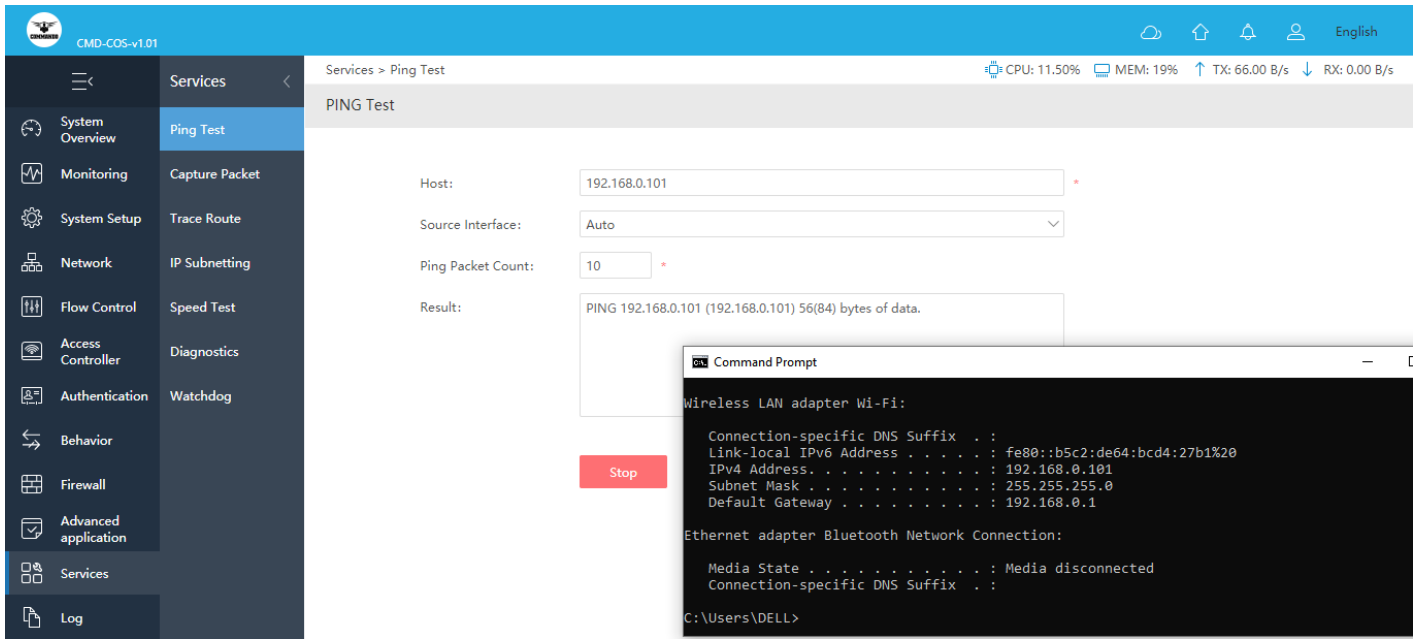
Add Import Export Enable Disable Delete

Protocol	Action	Direction	Src.Addr	Dst.Addr	Src.Port	Dst.Port	In.Interface	Out.Interface	Cycle	Period	Remarks	Status	Actions
icmp	drop	forward	192.168.0.0/24	192.168.1.0/24			lan1_wan1	lan1_wan1	1234567	00:00-23:59	Blocking ping	Enabled	Edit Copy Disable Delete

Showing 1 of 1 records

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

**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

The screenshot displays the 'Firewall > ARP binding' configuration page in the CMD-COS-v1.01 interface. The page features a sidebar with navigation options like System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The main content area shows the 'ARP Binding' configuration, including a search bar for IP/MAC/Name, a table of binding entries, and a help section. The 'Bind state' column for all entries is 'Unbinding', which is highlighted with a red box. The table also includes columns for IP Address, MAC Address, NIC belongs, Bind type, Remarks, and Actions (Bind, Edit, Delete). The page also shows system statistics like CPU, MEM, TX, and RX, and a footer with a help section.

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.100	e0:db:55:be:35:5b	lan1	General		Unbinding	Bind Edit Delete
192.168.0.102	08:9b:4b:9ef4:e3	lan1	General		Unbinding	Bind Edit Delete
192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Unbinding	Bind Edit Delete
192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete
192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete

Fig 8.2.1 Default ARP Binding page

Firewall > ARP binding

ARP Binding

Unbound MAC is not allowed to surf the Internet  Compatibility has been bound to DHCP static allocation

IP/MAC/Name

Add Import Export Bind Clean Delete

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.100	e0:db:55:be:35:5b	lan1	General		Binding	Edit Delete
192.168.0.102	08:9b:4b:9e:f4:e3	lan1	General		Binding	Edit Delete
192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Binding	Edit Delete
192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete
192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete

Showing 1-5 of 5 records

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

Help : General: between IP and MAC(default)  
 Only: IP and MAC , if not correctly matched, can't surf the Internet; The only binding advice is to statically assign the checked and compatible ARP list to the DHCP client  
 Exports and imports: exports or imports the list of arps in the bound state

Fig 8.2.2 After Binding ARP page

Firewall > ARP binding

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

Firewall > ARP binding

ARP Binding

Unbound MAC is not allowed to surf the Internet  Compatibility has been bound to DHCP static allocation

IP/MAC/Name

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions
192.168.0.100	e0:db:55:be:35:5b	lan1	General		Binding	Edit Delete
192.168.0.102	08:9b:4b:9e:f4:e3	lan1	General		Binding	Edit Delete
192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Binding	Edit Delete
192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete
192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete
192.168.10.1	44:99:87:77:ad:46	lan1	General	IP and MAC Static binding	Binding	Edit Delete

Showing 1-6 of 6 records

PerPage  Rows  /1Pages

**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

Firewall > Connection Limiter

Connection Limiter Settings

IP Address	Protocol	WAN Port	Limit	Cycle	Period	Remarks	Status	Actions
No Data								

**Fig 8.3.1 Default Connection Limiter Settings page**

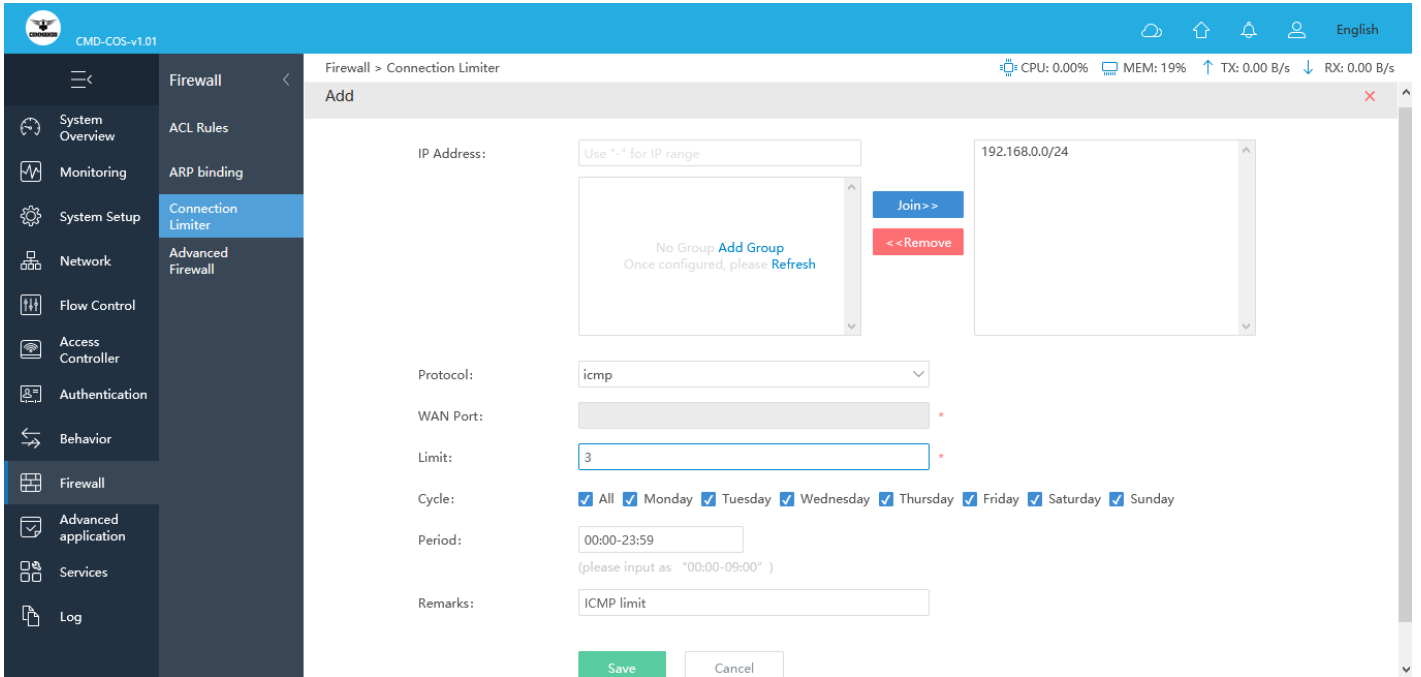


Fig 8.3.2 Add Connection Limiter Settings page

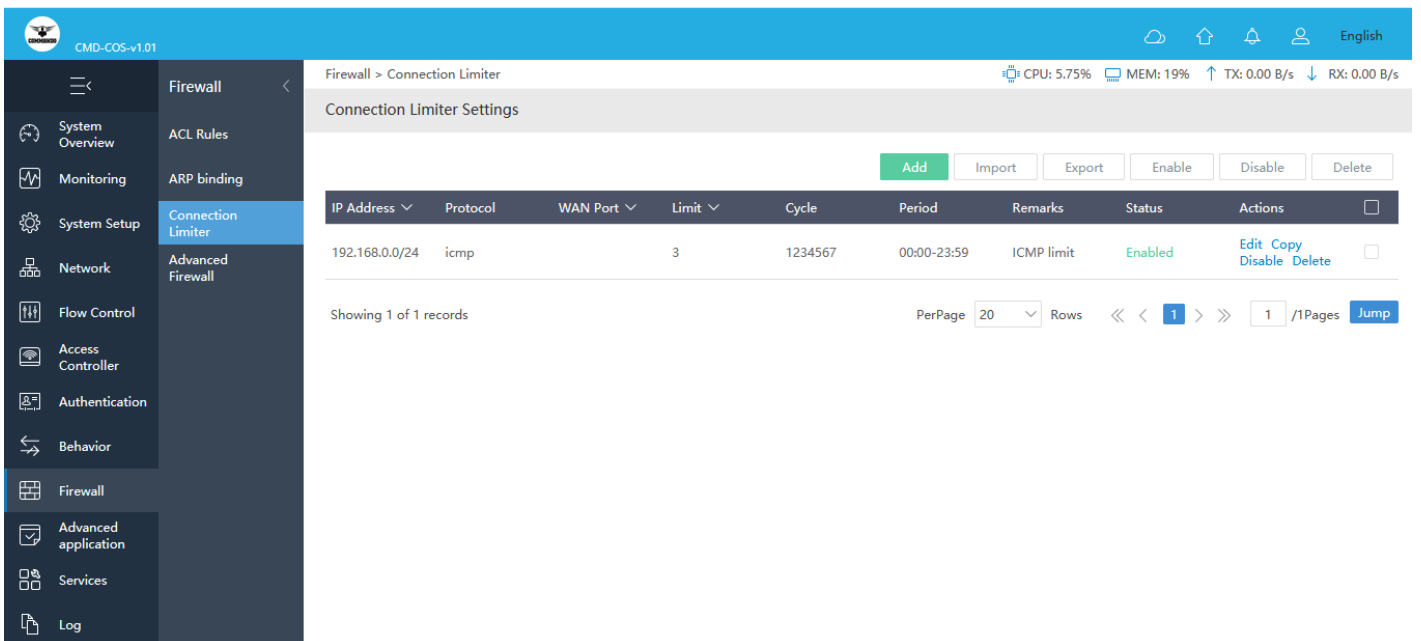
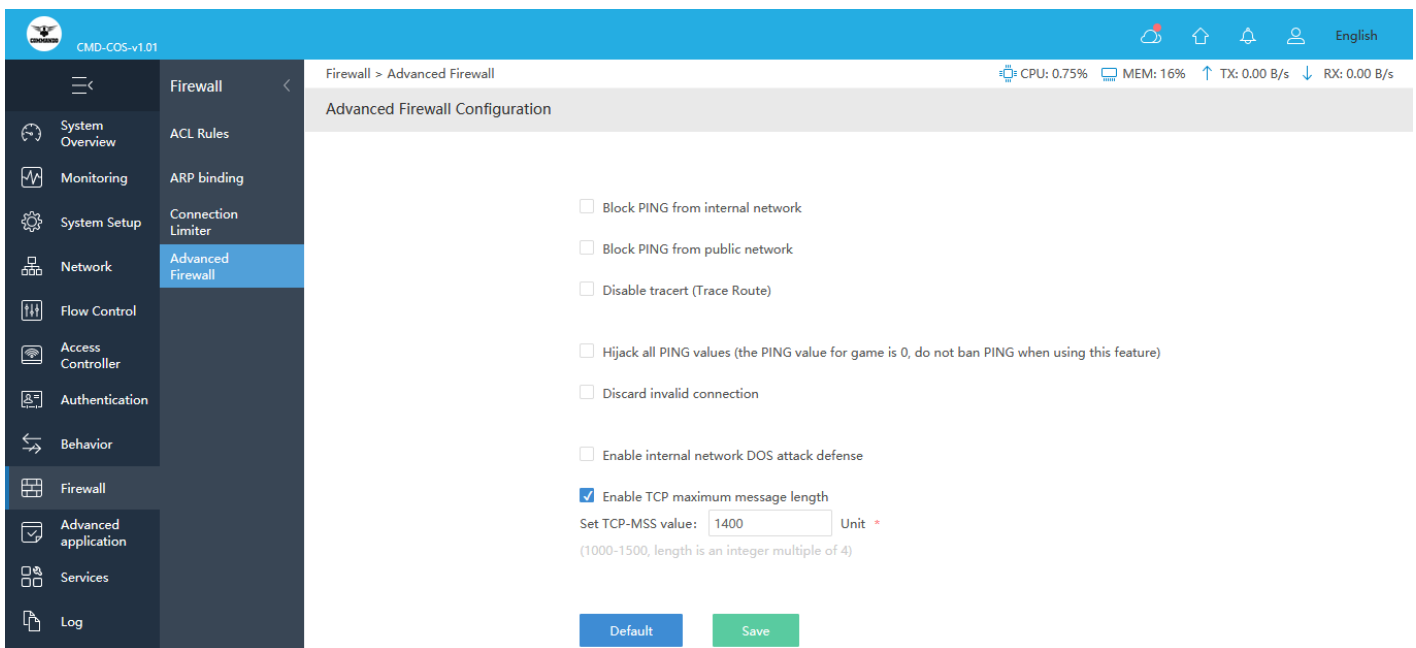


Fig 8.3.3 Connection Limiter Settings page

## 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**



The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes the device name 'CMD-COS-v1.01', system status (CPU: 0.00%, MEM: 19%, TX: 0.00 B/s, RX: 0.00 B/s), and a language selector set to 'English'. The left sidebar contains a menu with categories: System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Firewall' category is expanded, showing sub-items: ACL Rules, ARP binding, Connection Limiter, and 'Advanced Firewall' (which is highlighted). The main content area is titled 'Firewall > Advanced Firewall' and 'Advanced Firewall Configuration'. It features a list of configuration options with checkboxes and a text input field:

- Block PING from internal network
- Block PING from public network
- Disable tracert (Trace Route)
- Hijack all PING values (the PING value for game is 0, do not ban PING when using this feature)
- Discard invalid connection
- Enable internal network DOS attack defense
- Enable TCP maximum message length

Below the 'Enable TCP maximum message length' option, there is a text input field with the value '1500' and a 'Unit \*' label. A note below the input field reads: '(1000-1500, length is an integer multiple of 4)'. At the bottom of the configuration area, there are two buttons: 'Default' and 'Save'.

**Fig 8.4.2 Advanced Firewall Configuration page**

## **ADVANCED APPLICATION**

### **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.

**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.

### **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. 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 router 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

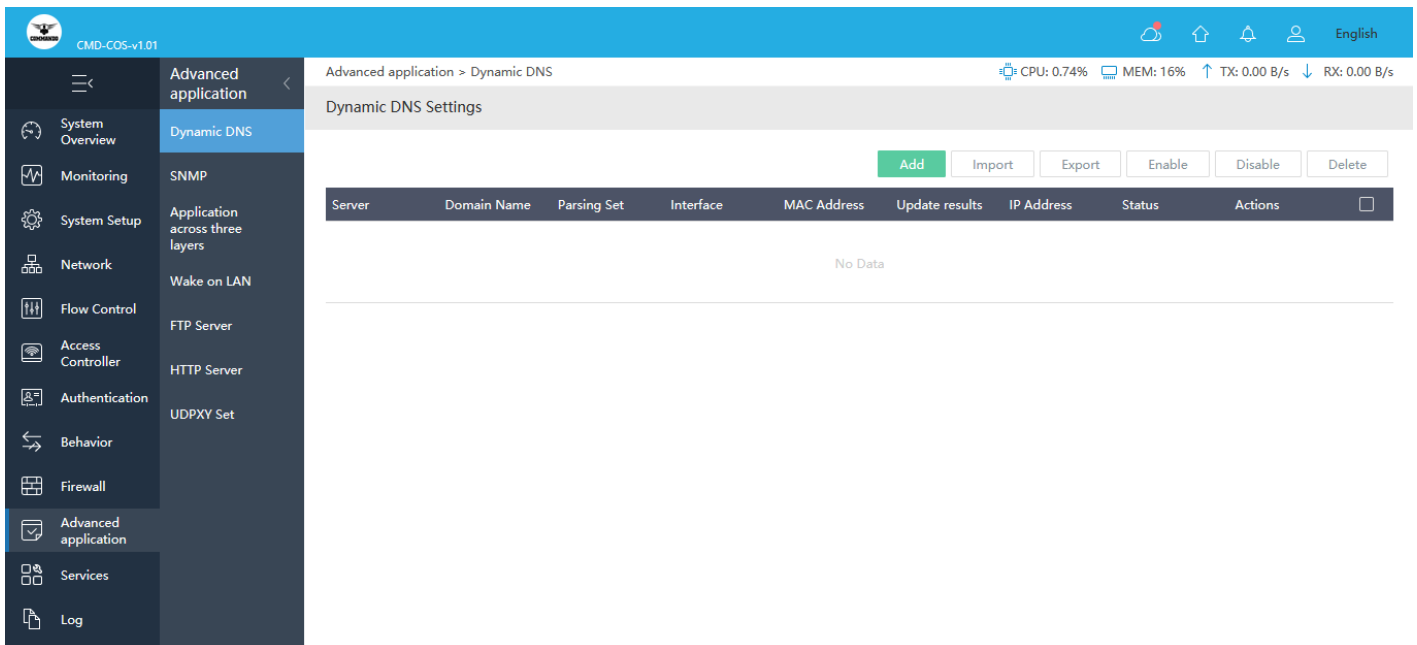


Fig 9.1.1 Default Dynamic DNS Settings page

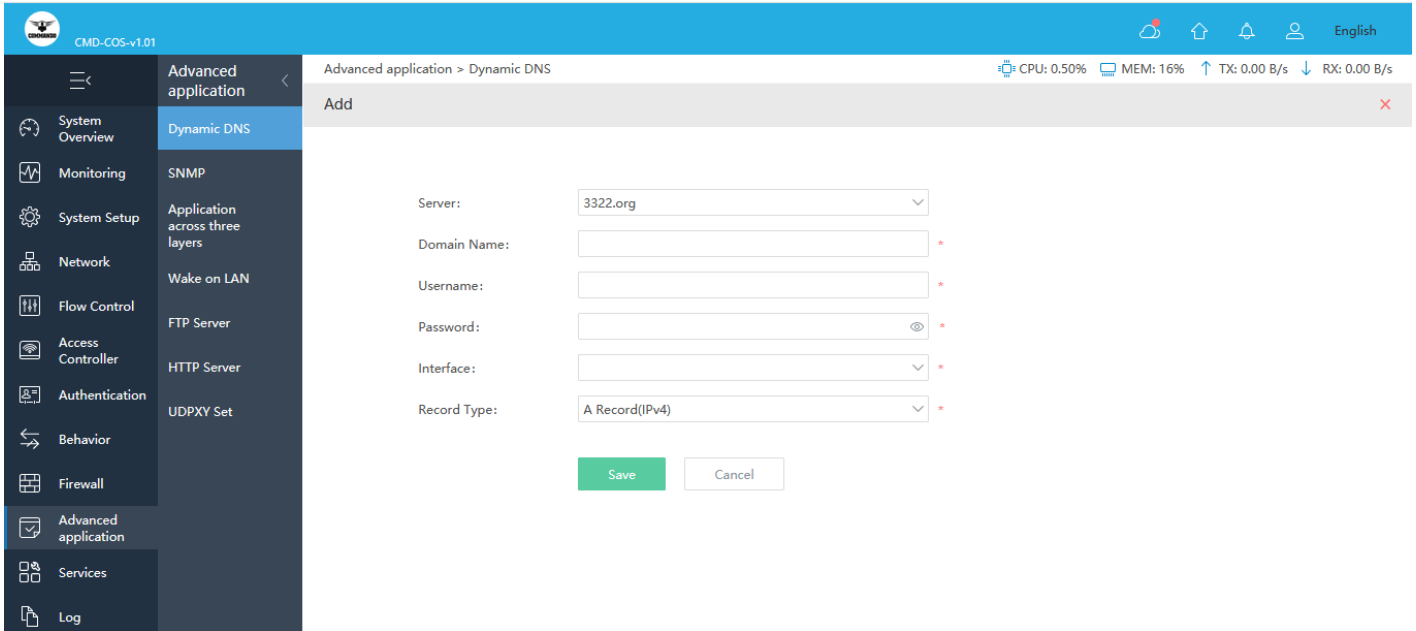


Fig 9.1.2 Add Dynamic DNS Settings page

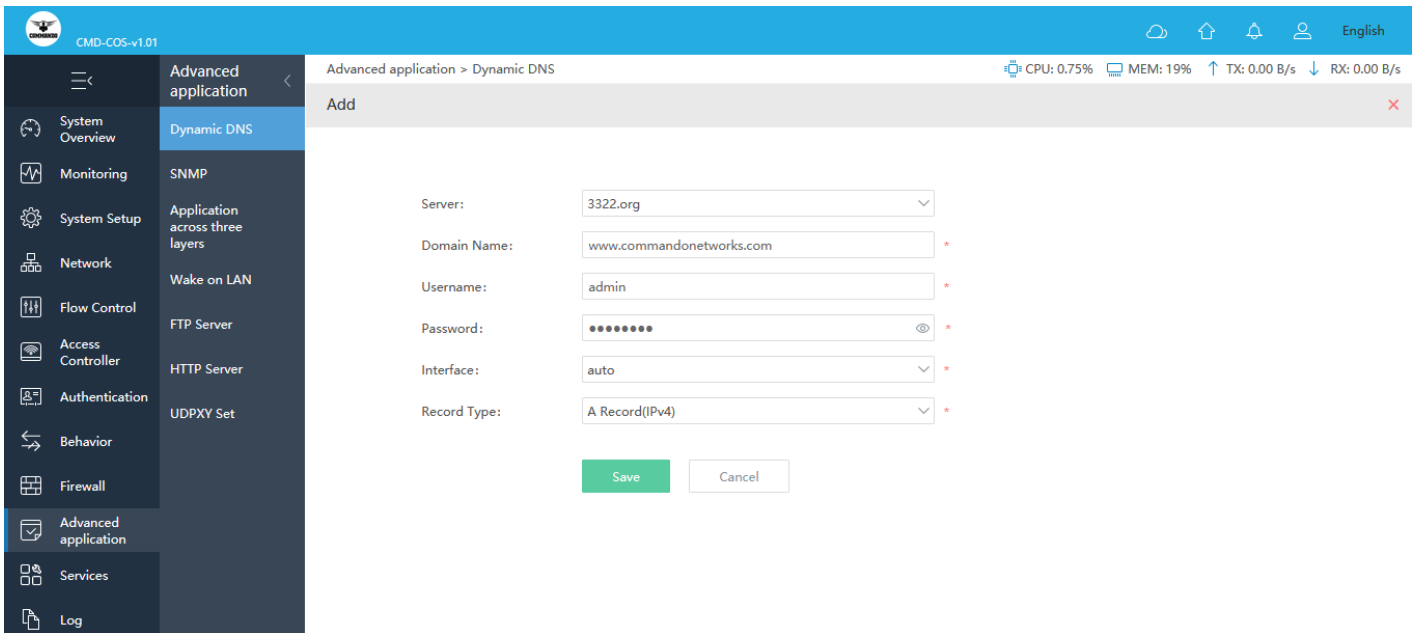


Fig 9.1.3 Add Particular Dynamic DNS Settings page

The screenshot displays the 'Dynamic DNS Settings' page within the 'Advanced application'. The interface includes a top navigation bar with system statistics (CPU: 0.74%, MEM: 19%, TX: 0.00 B/s, RX: 0.00 B/s) and a left sidebar with various configuration categories. The main content area features a table of Dynamic DNS servers. One server is listed with the following details:

Server	Domain Name	Parsing Set	Interface	MAC Address	Update results	IP Address	Status	Actions
3322.org	www.commando-networks.com		auto			--	Enabled	Edit Disable Delete

Below the table, it indicates 'Showing 1 of 1 records' and provides pagination controls (PerPage: 20, Rows, 1 / 1Pages, Jump).

**Fig 9.1.4 Dynamic DNS Settings page**

## 2. 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.

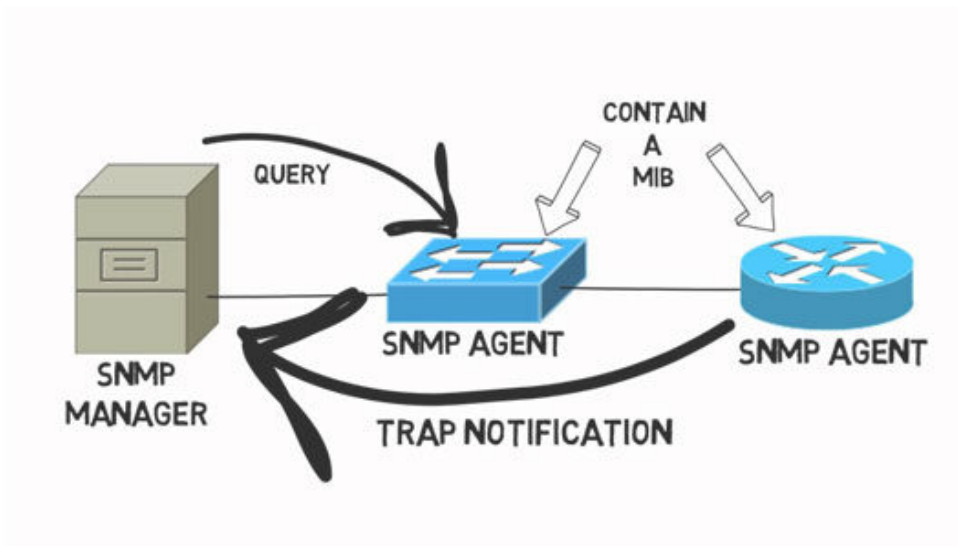
### **Protocols:**

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



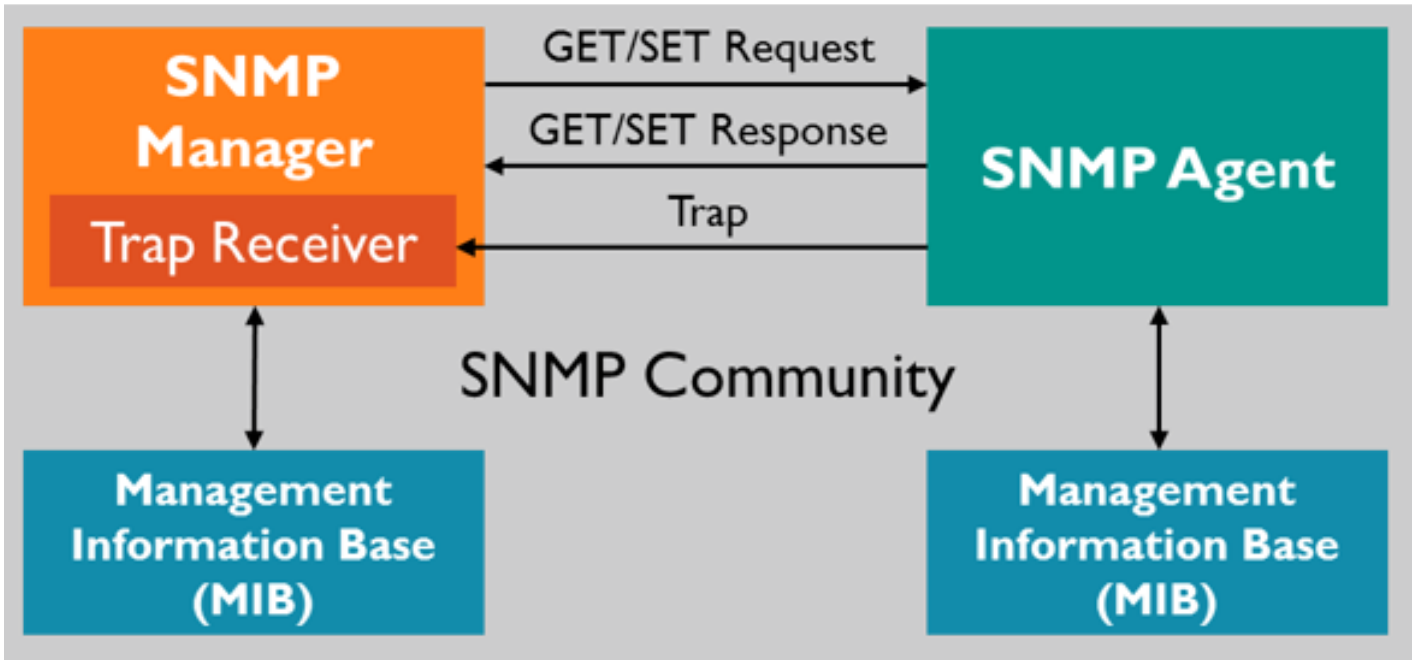
**Fig 9.2.1 SNMP Community concept**

## **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.

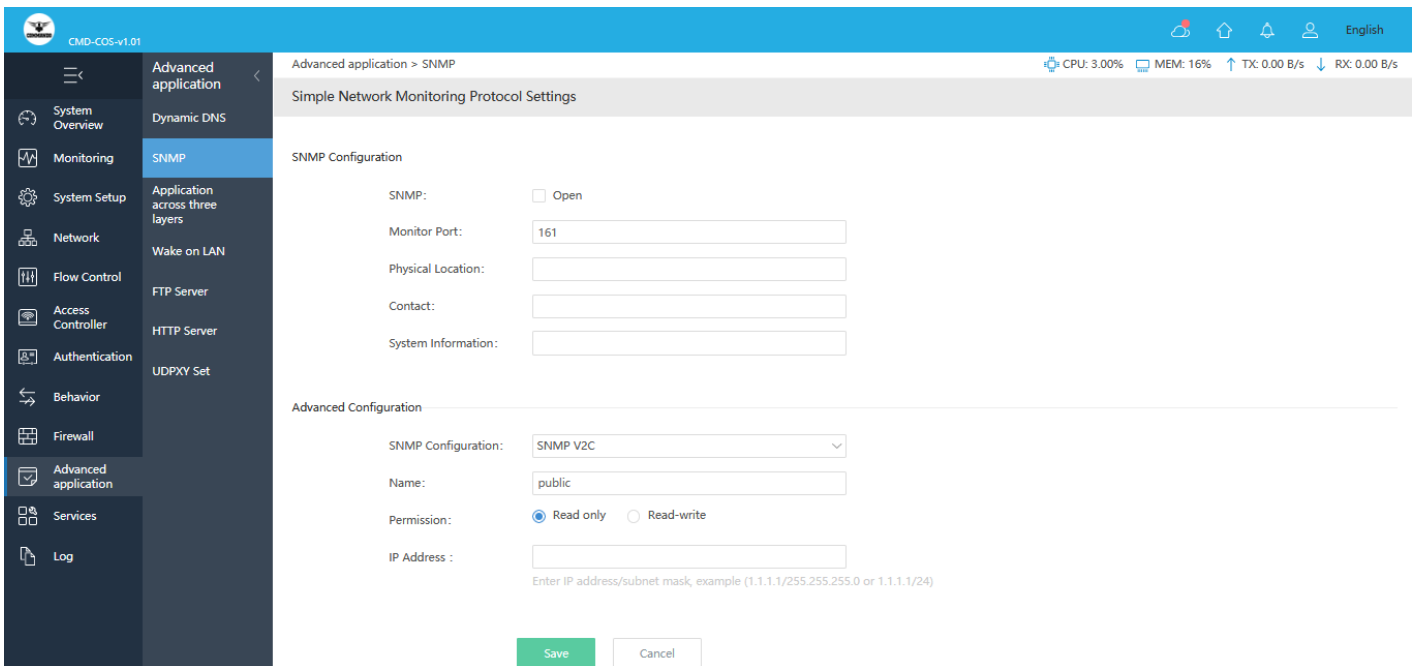
v3 - Mostly identical to SNMPv2, but adds significantly better security, although it supports communities for backward compatibility. Uses MIB-II.



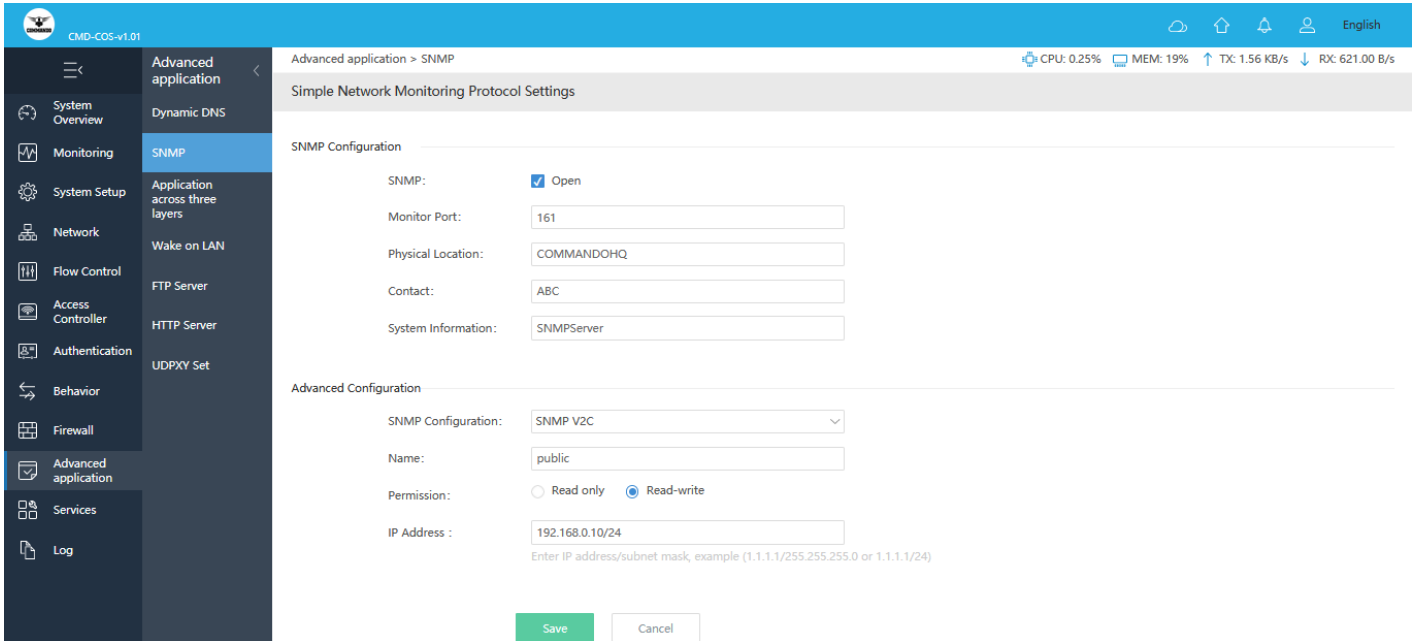
**Fig 9.2.2 SNMP Community concept**

### How to enable Simple Network Monitoring Protocol?

To configure and enable Simple Network Monitoring Protocol Settings, Click on Advanced application > SNMP



**Fig 9.2.3 Default Simple Network Monitoring Protocol Settings page**

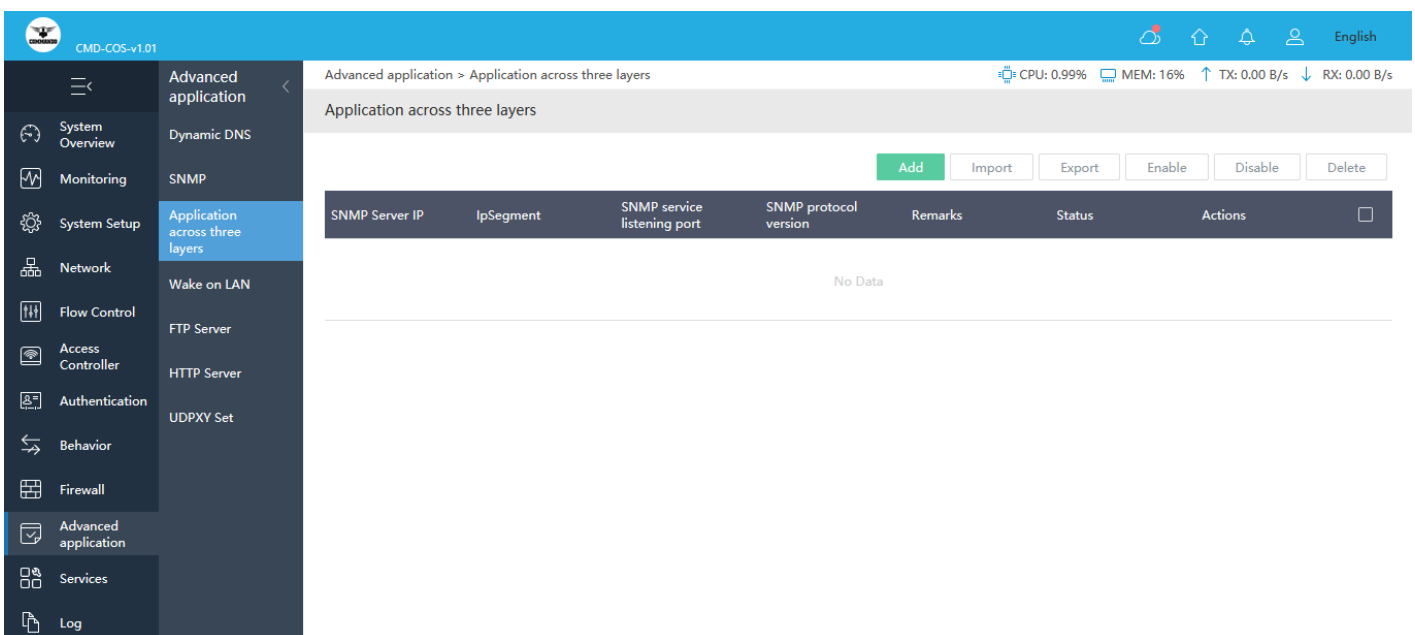


**Fig 9.2.4 Simple Network Monitoring Protocol Settings page**

### 9.3 Application across three layers

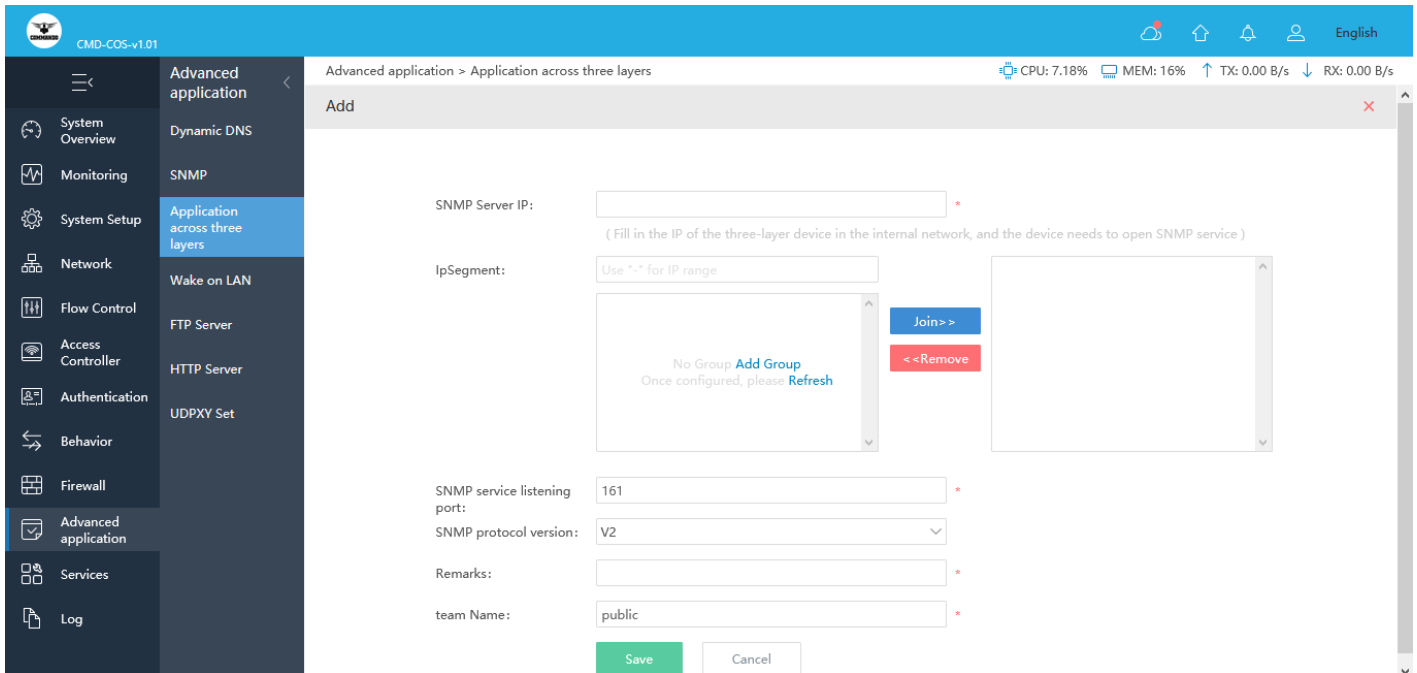
The protocol's client/server architecture has three components SNMP Manager, SNMP Agent and Management Information Base (MIB). The SNMP Manager acts as the client, the SNMP Agent acts as the server and the Management Information Base acts as the server's database. When the SNMP Manager asks the Agent a query, the Agent uses the MIB provide reply.

To configure Application across three layers, Click on Advanced application > Application across three layers

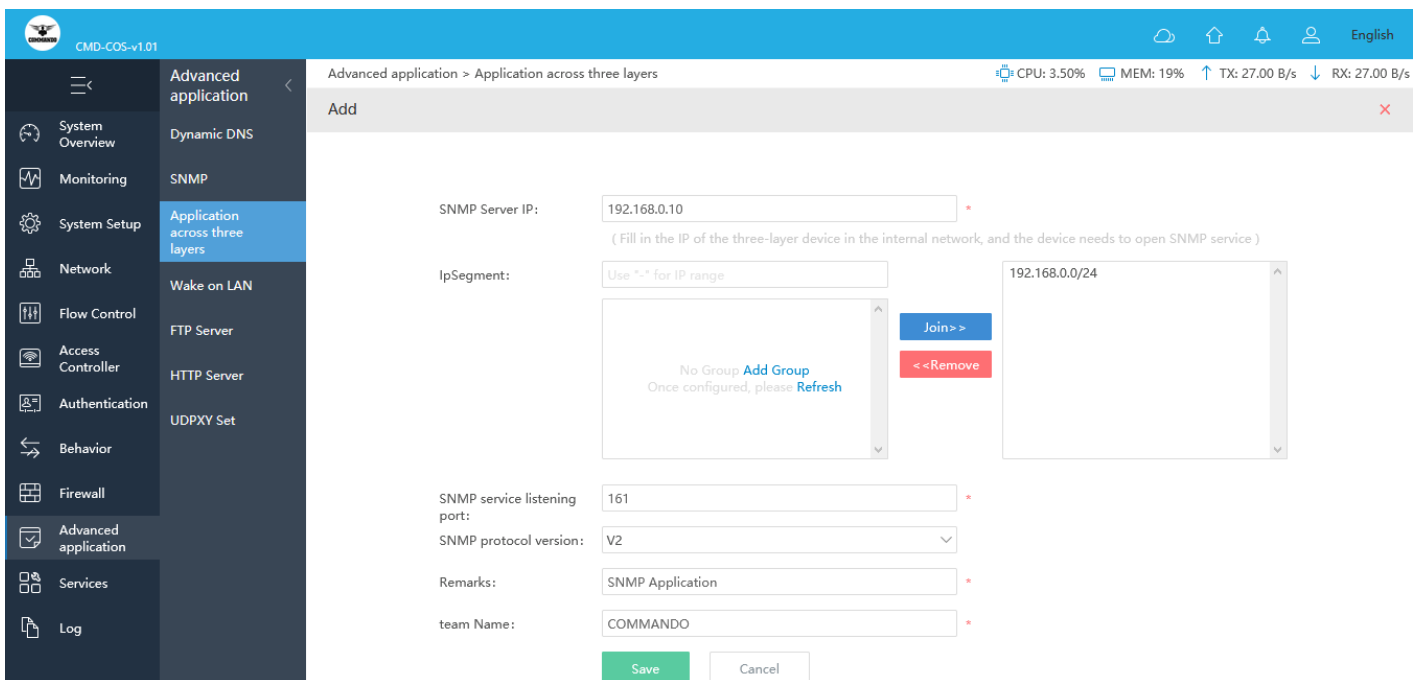




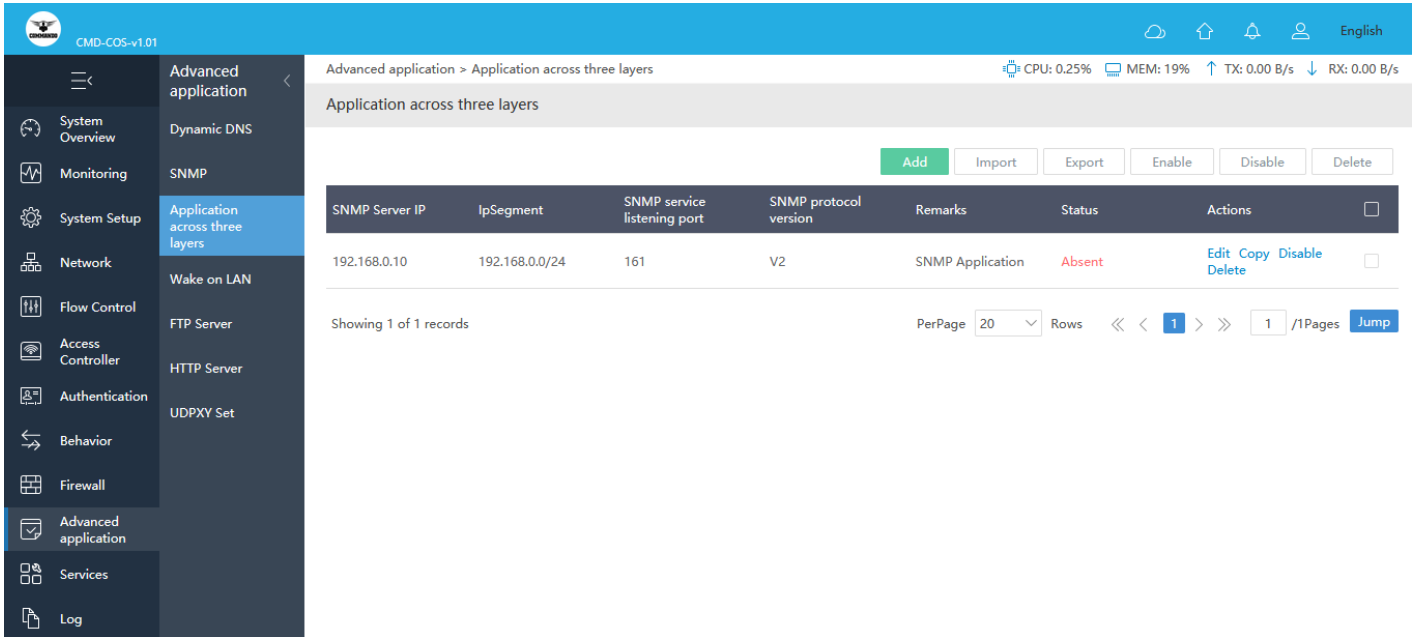
**Fig 9.3.1 Default Application across three layers page**



**Fig 9.3.2 Add Application across three layers page**



**Fig 9.3.3 Application across three layers for particular SNMP server page**



**Fig 9.3.4 Application across three layers page**

## 9.4 Wake on LAN

This utility allows you to easily turn on one or more computers remotely by sending Wake-on-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

CMD-COS-v1.01

Advanced application > Wake on LAN

CPU: 0.50% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Wake-on-LAN Settings

Immediate Wake-up

MAC Address:

Regular Wake-up List

MAC Address	Terminal Status	Cycle	Date	Time	Remarks	Planned Task	Actions
No Data							

**Fig 9.4.1 Default Wake-on-LAN Settings page**

CMD-COS-v1.01

Advanced application > Wake on LAN

CPU: 0.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Add

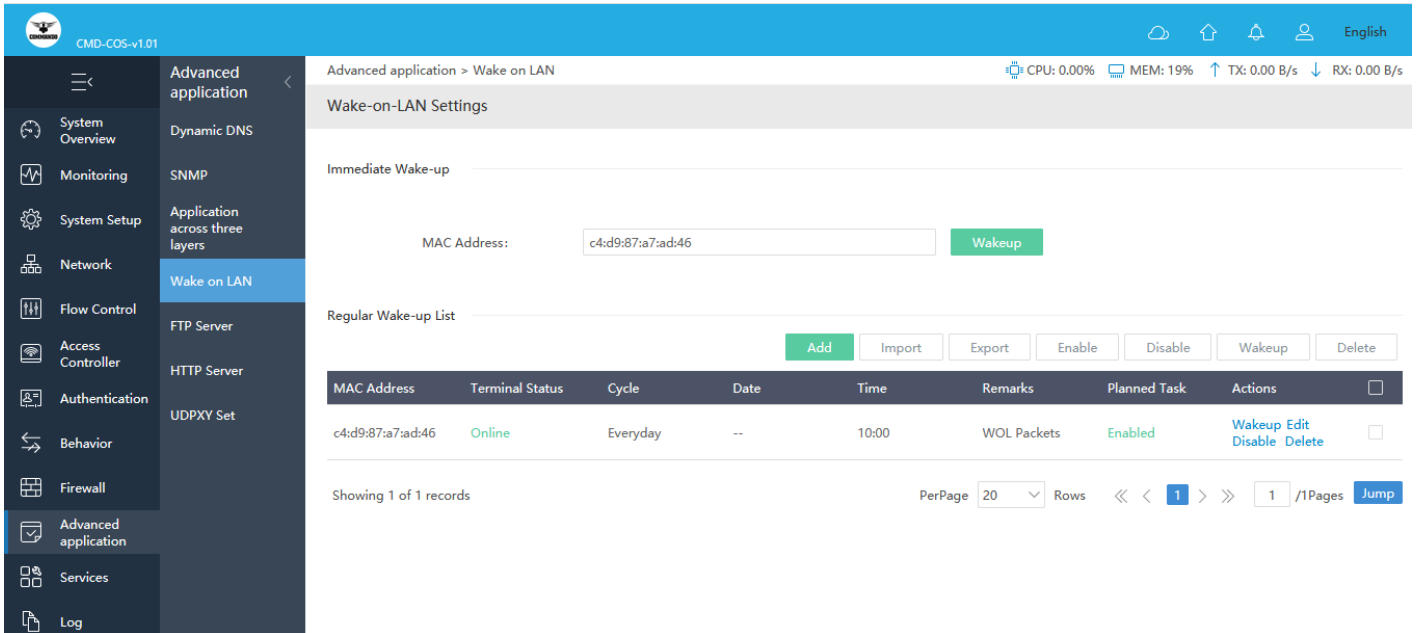
MAC:

Cycle:

Time:

Remarks:

**Fig 9.4.2 Add Wake-on-LAN Settings page**

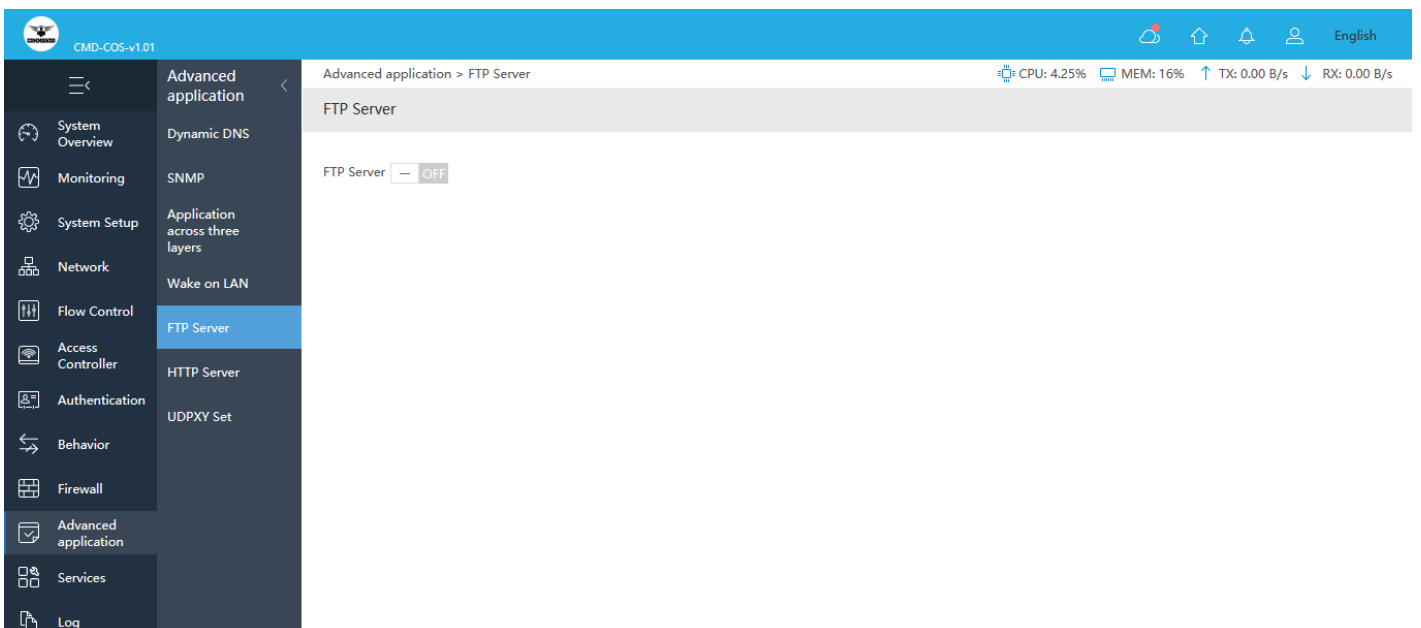


**Fig 9.4.3 Wake-on-LAN Settings page**

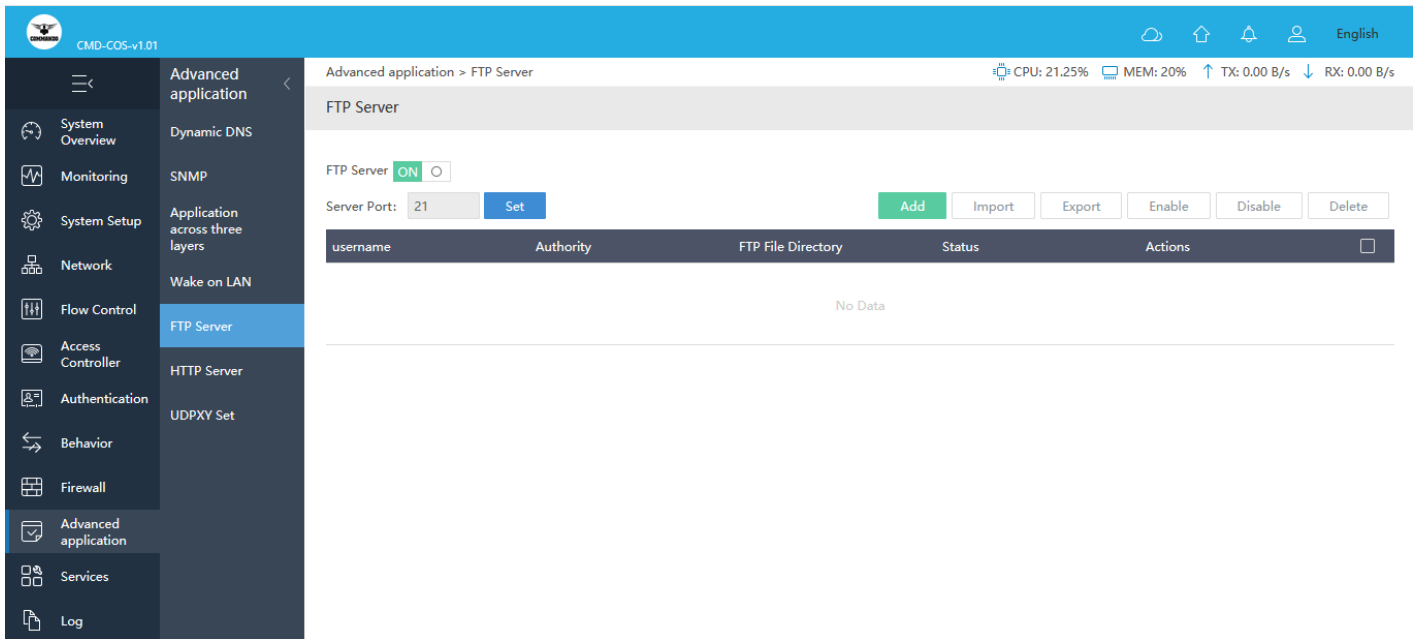
## 9.5 FTP Server

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 9.5.1 Default FTP Server page**

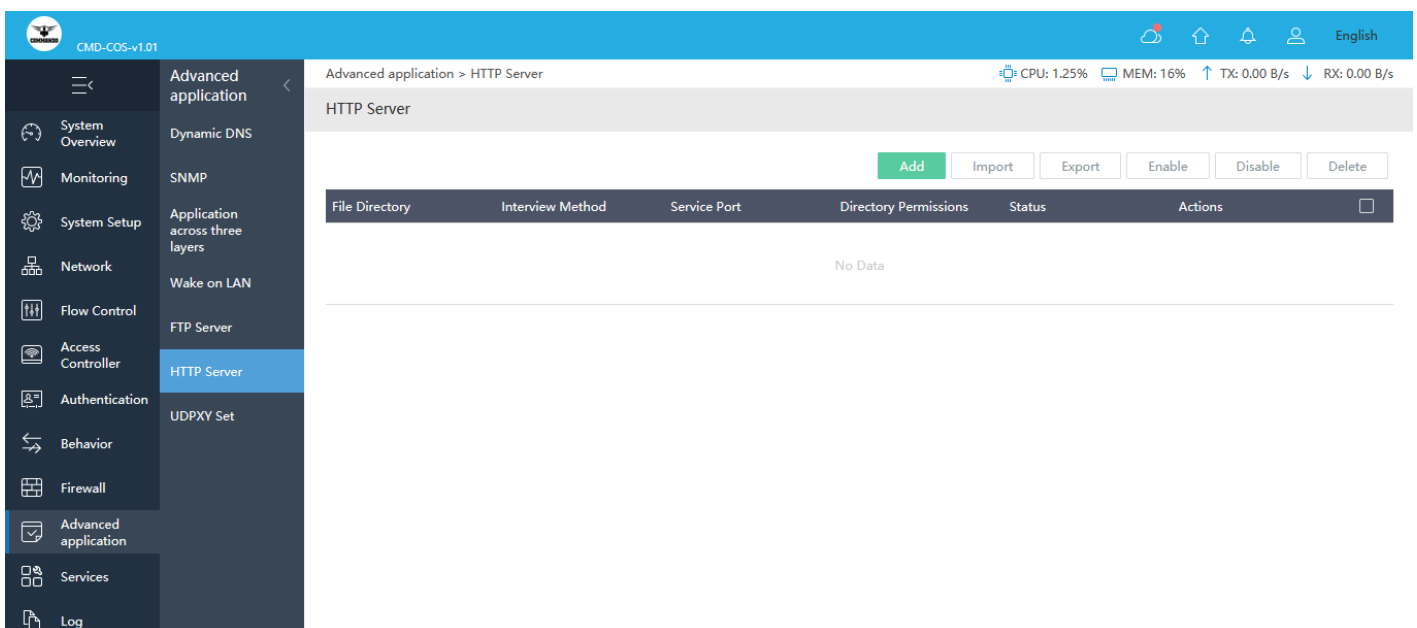


**Fig 9.5.2 Enabling FTP Server page**

## 9.6 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

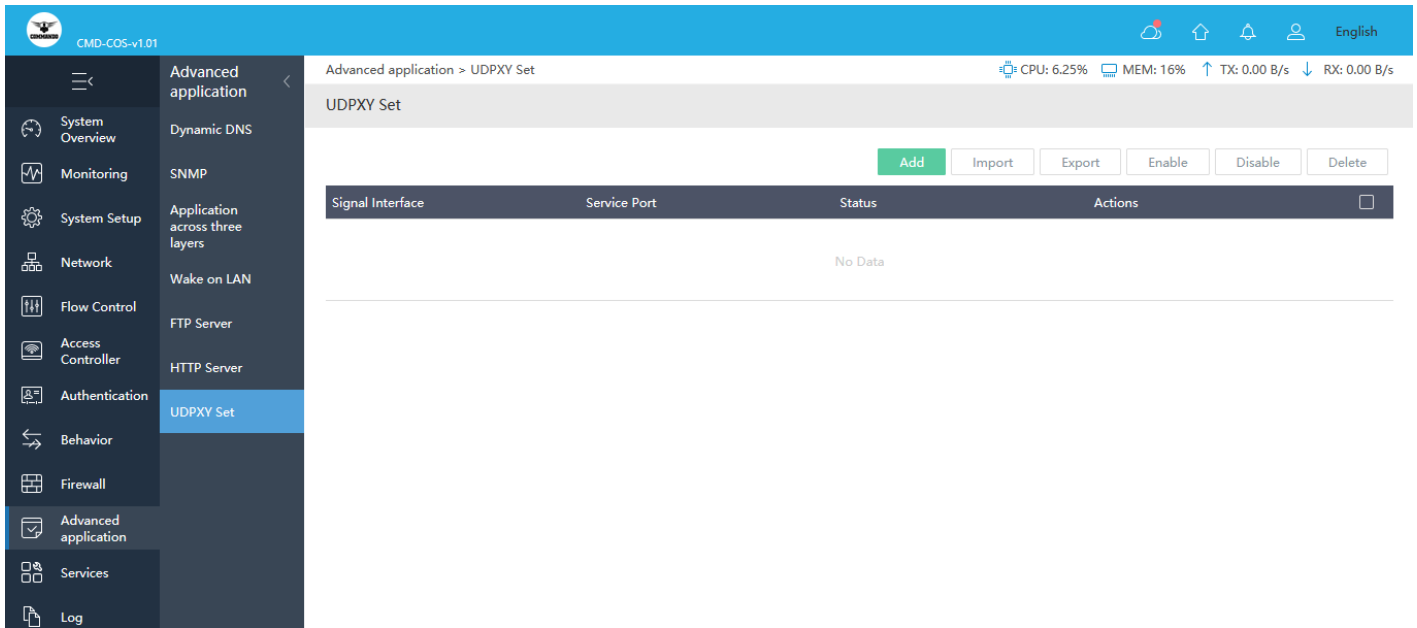


**Fig 9.6.1 Default HTTP Server page**

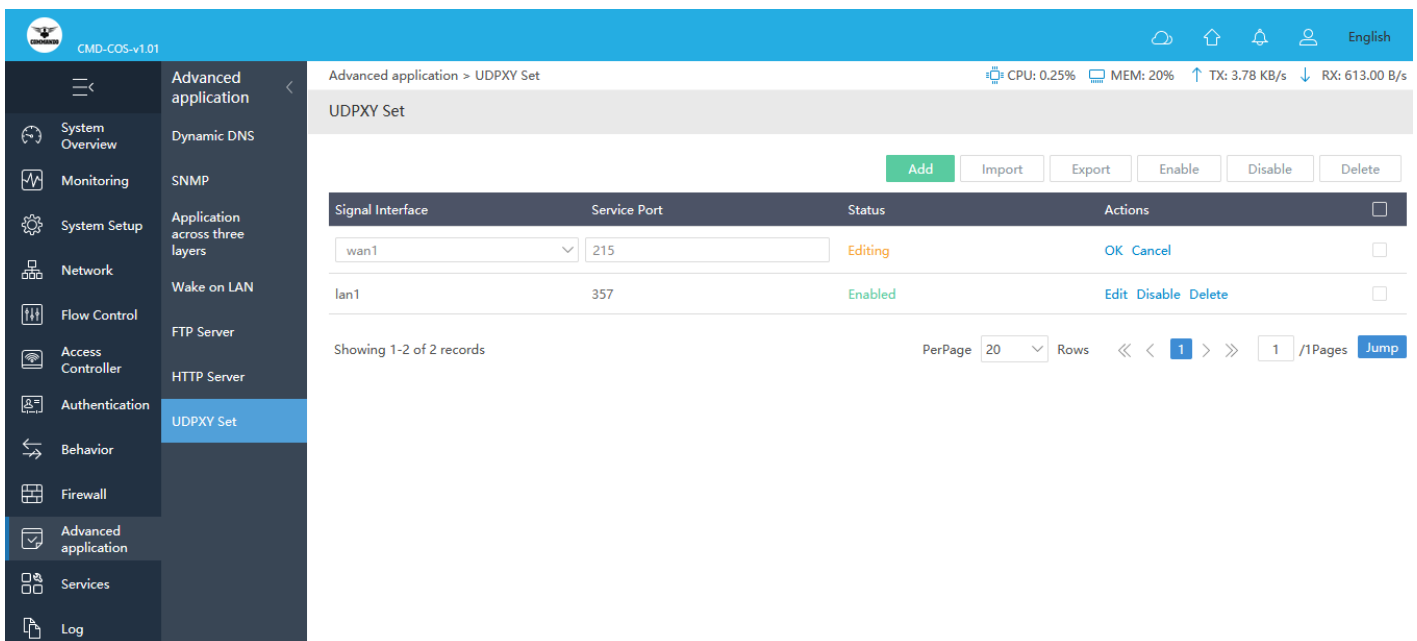
## 9.7 UDPXY Set

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 9.7.1 Default UDPXY Set page**



**Fig 9.7.2 UDPXY 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.

## **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

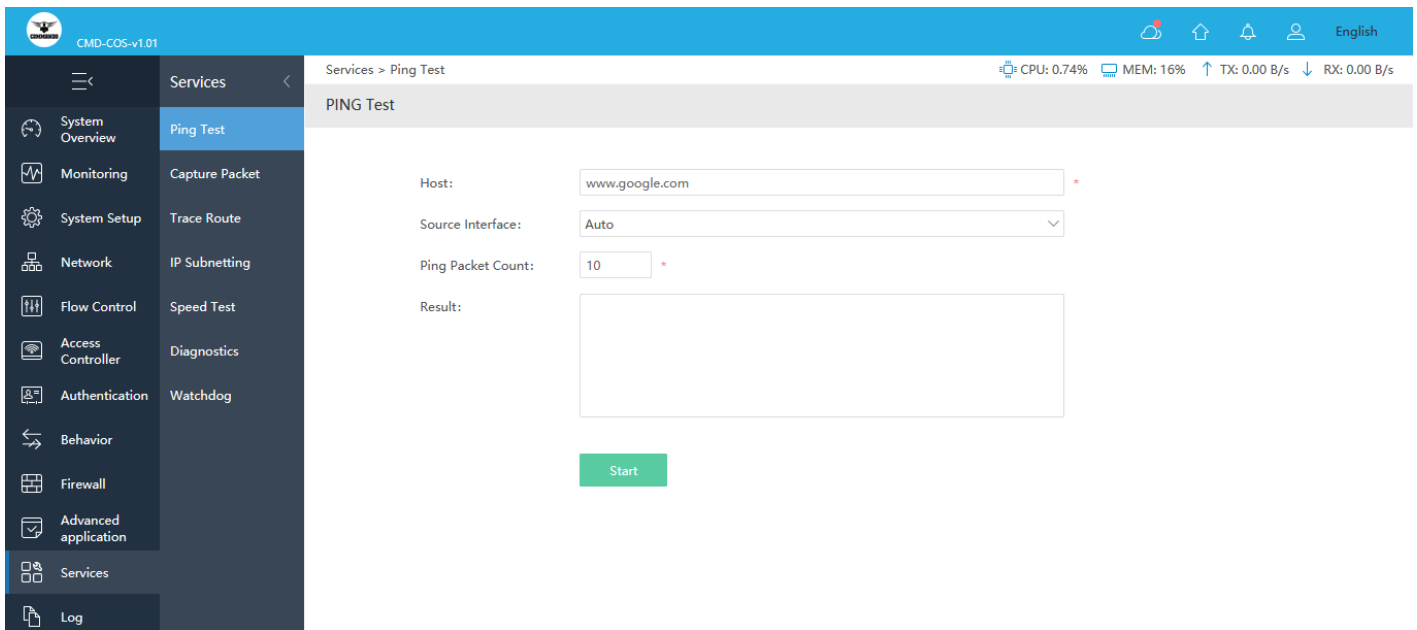


Fig 10.1.1 Default PING Test page

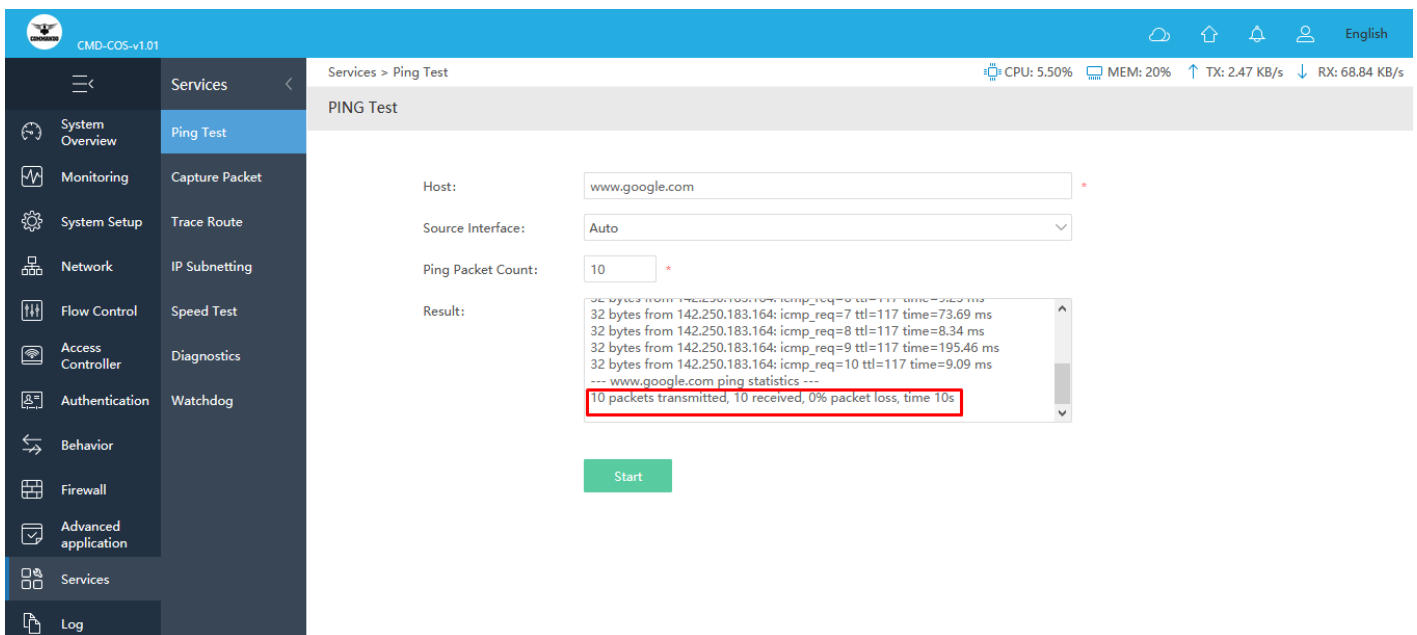
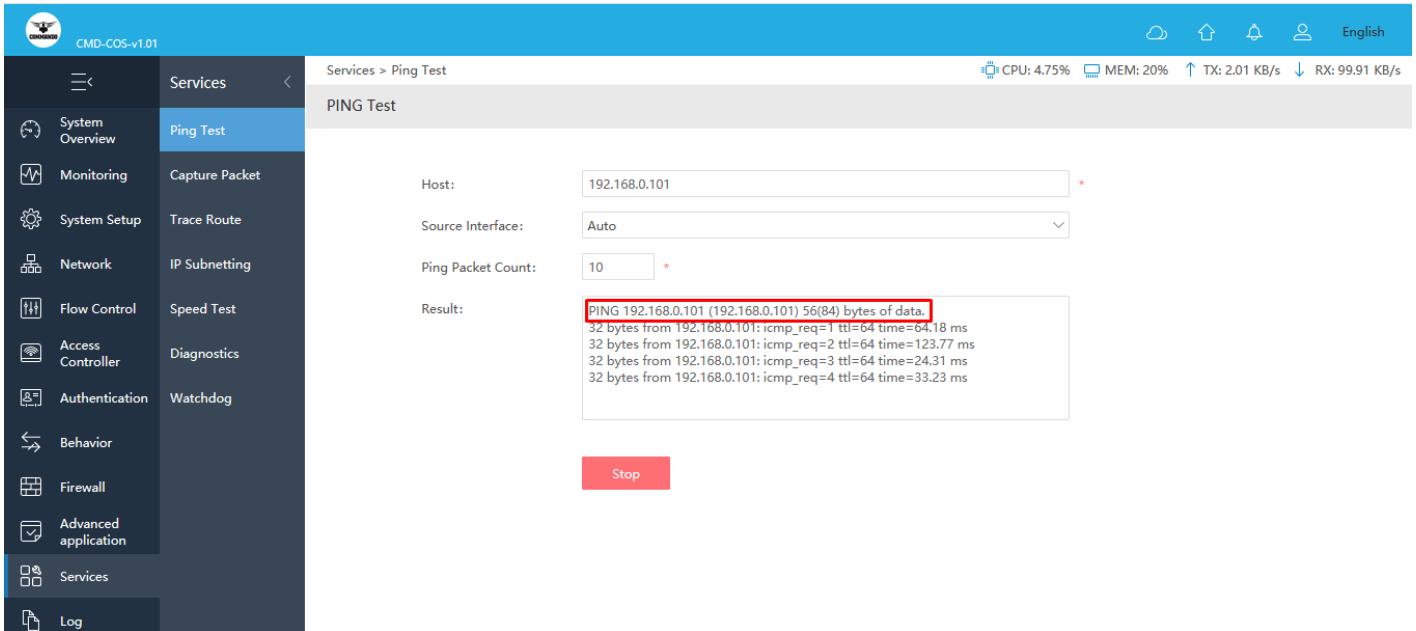


Fig 10.1.2 PING to particular website page





**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

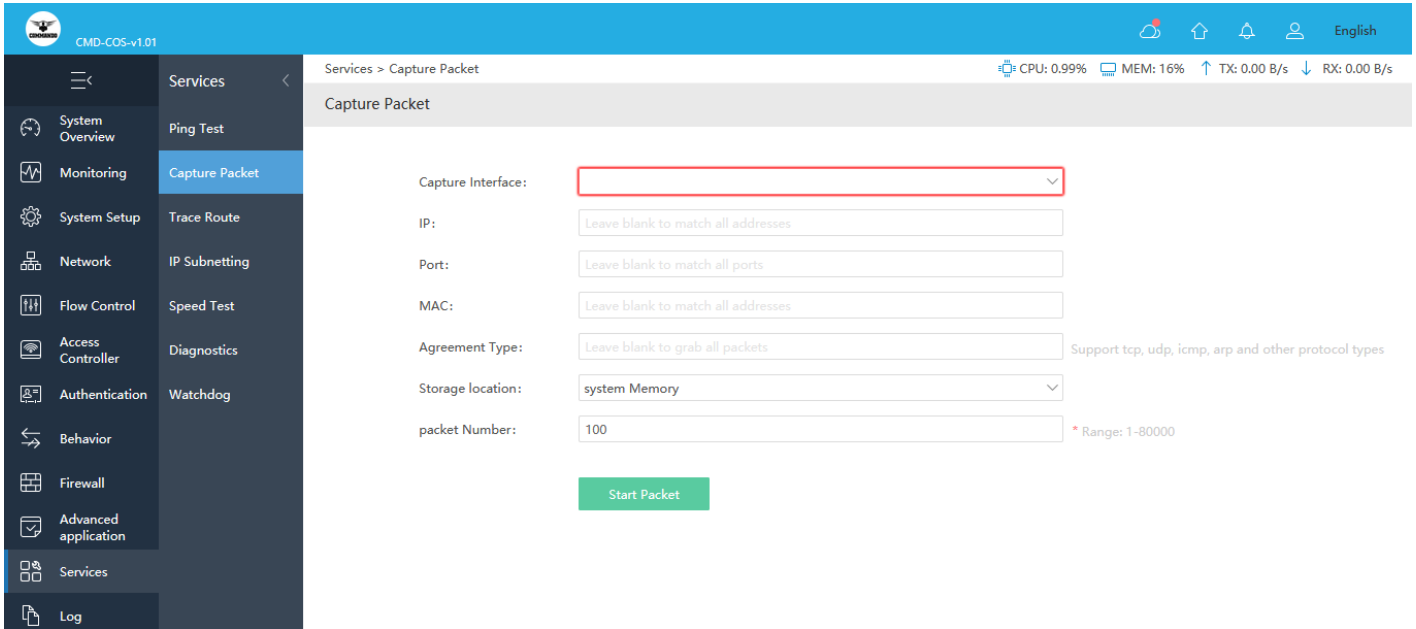


Fig 10.2.1 Default Capture Packet page

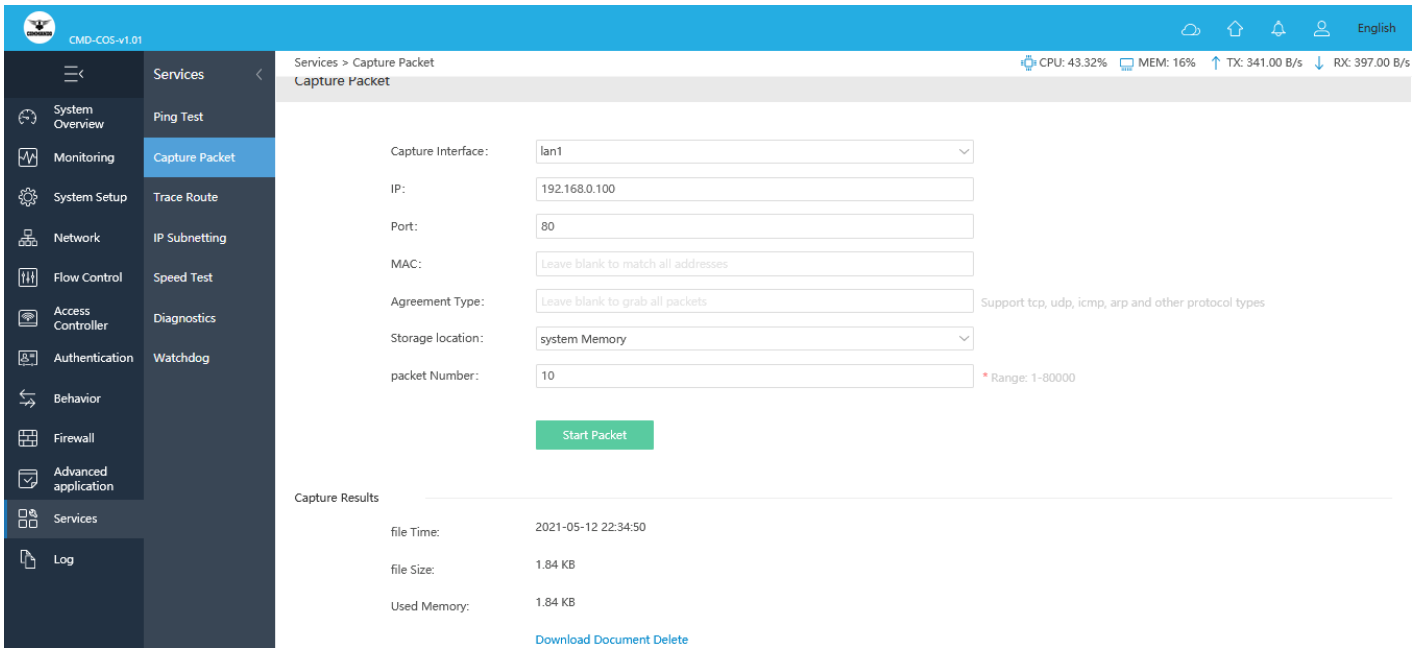
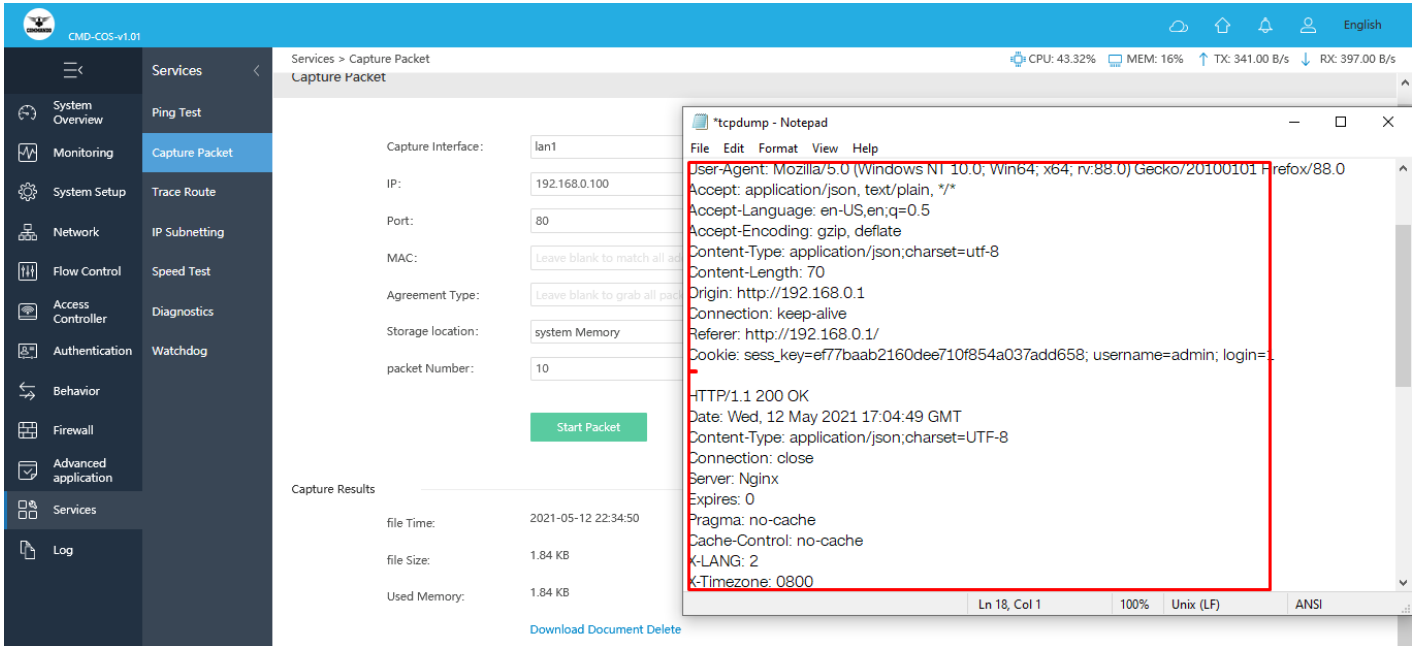


Fig 10.2.2 Capture Packet result page

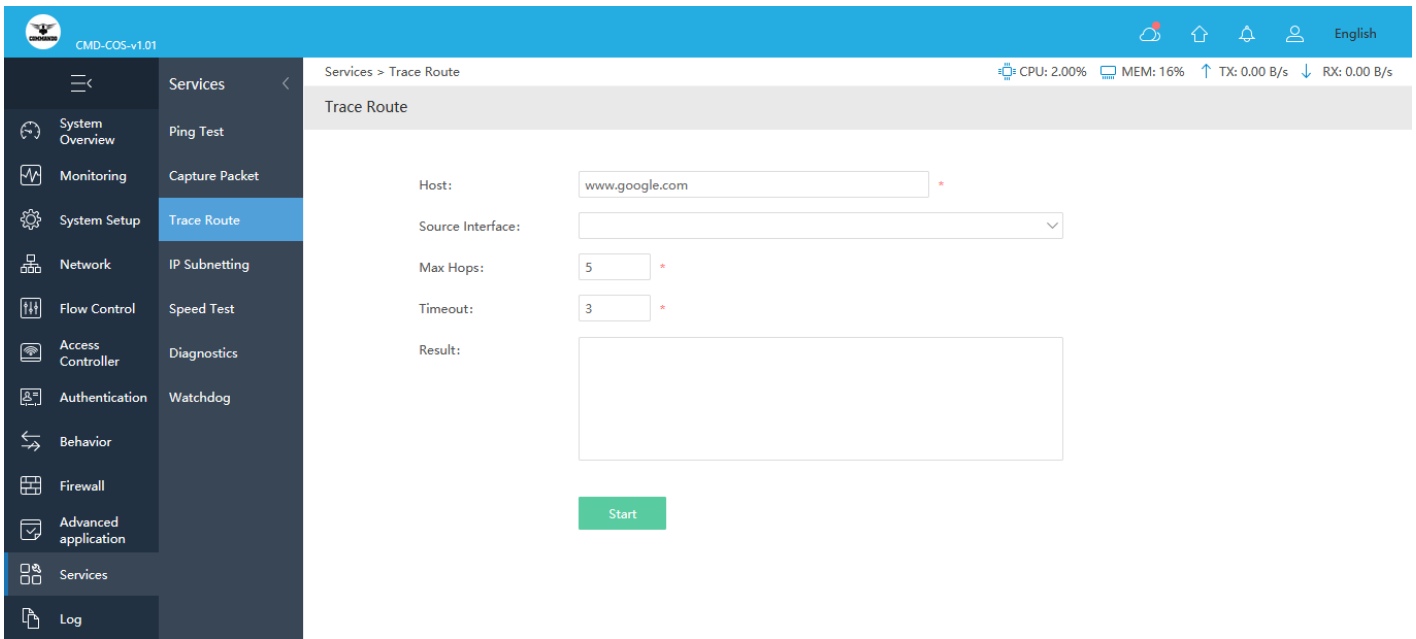


**Fig 10.2.3 Capture Packet download document page**

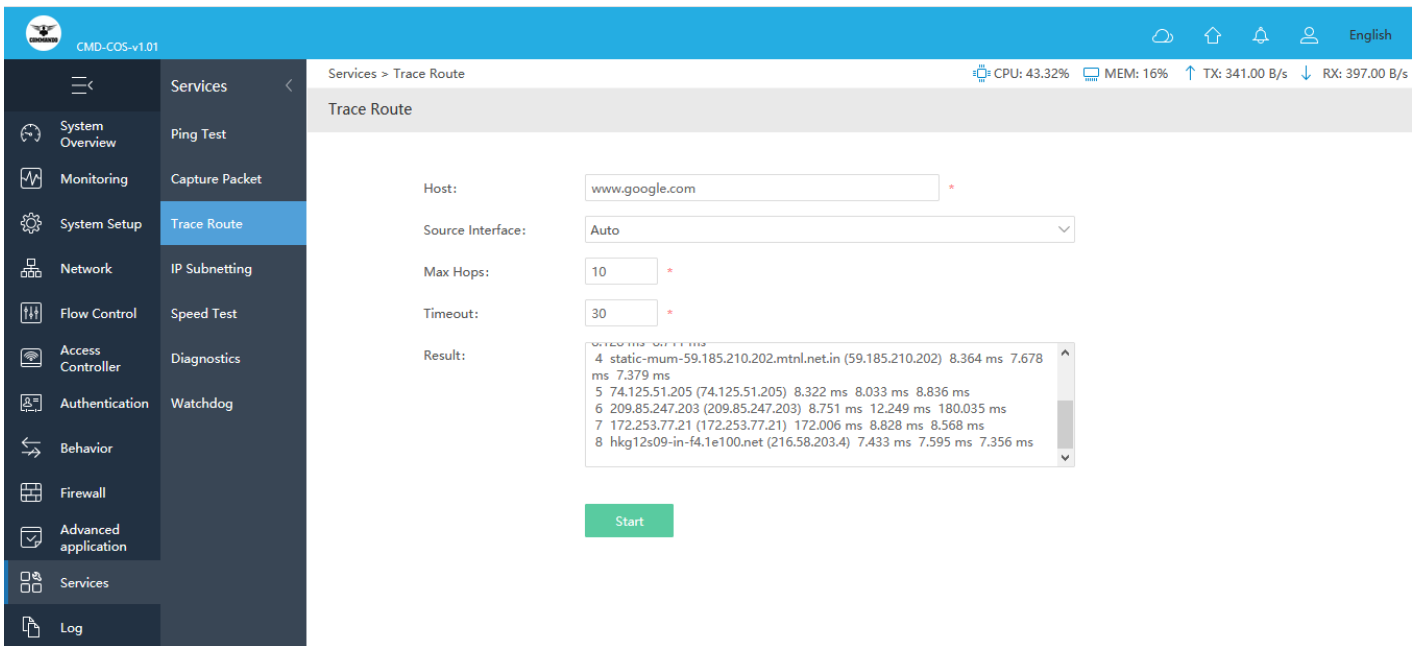
### 10.3 Trace Route

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 routers 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 routers in the path from the source host to destination host and it can be useful when troubleshooting network problems.

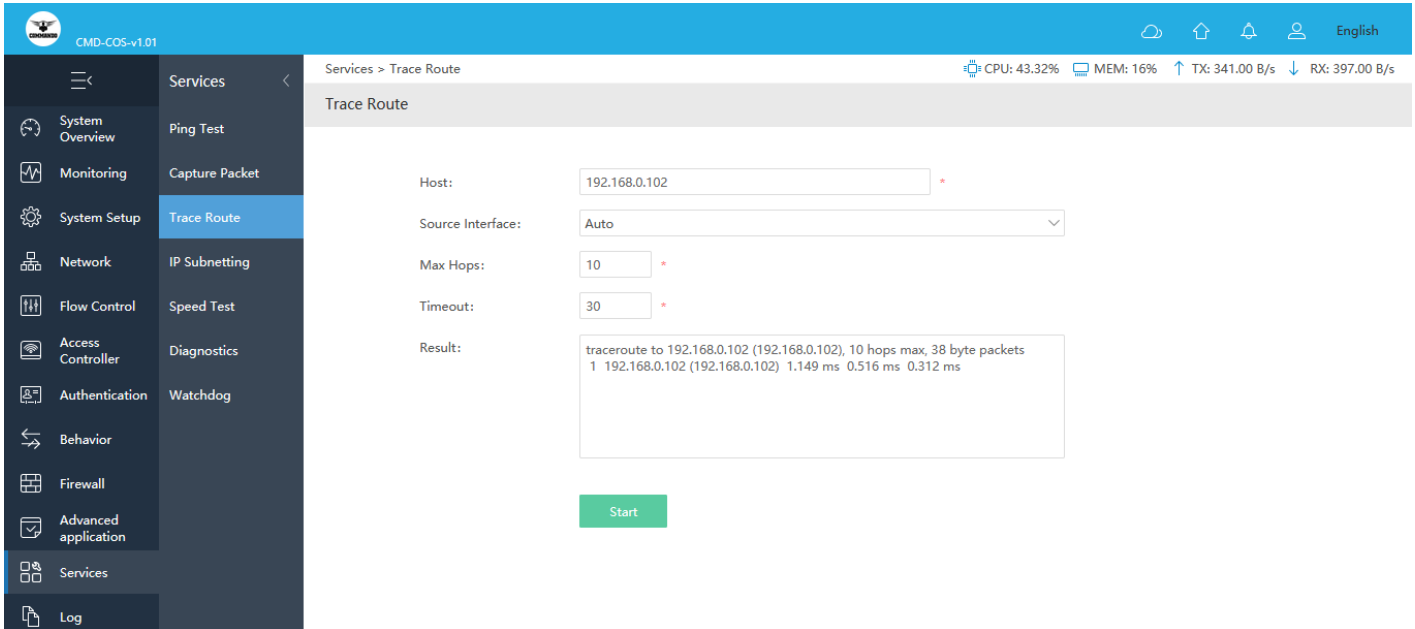
For Trace Route, Click on Services > Trace Route



**Fig 10.3.1 Default Trace Route page**



**Fig 10.3.2 Trace Route particular website page**



**Fig 10.3.3 Trace Route particular IP address page**

## 10.4 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

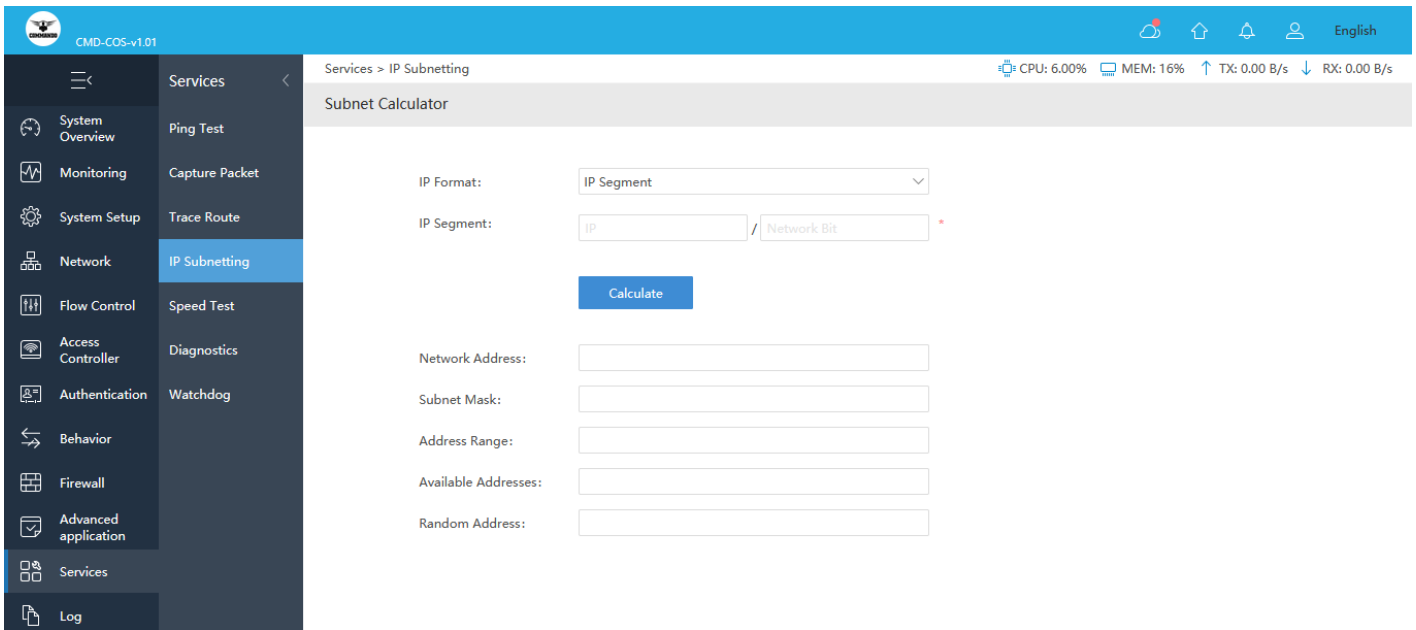


Fig 10.4.1 Default Subnet Calculator page

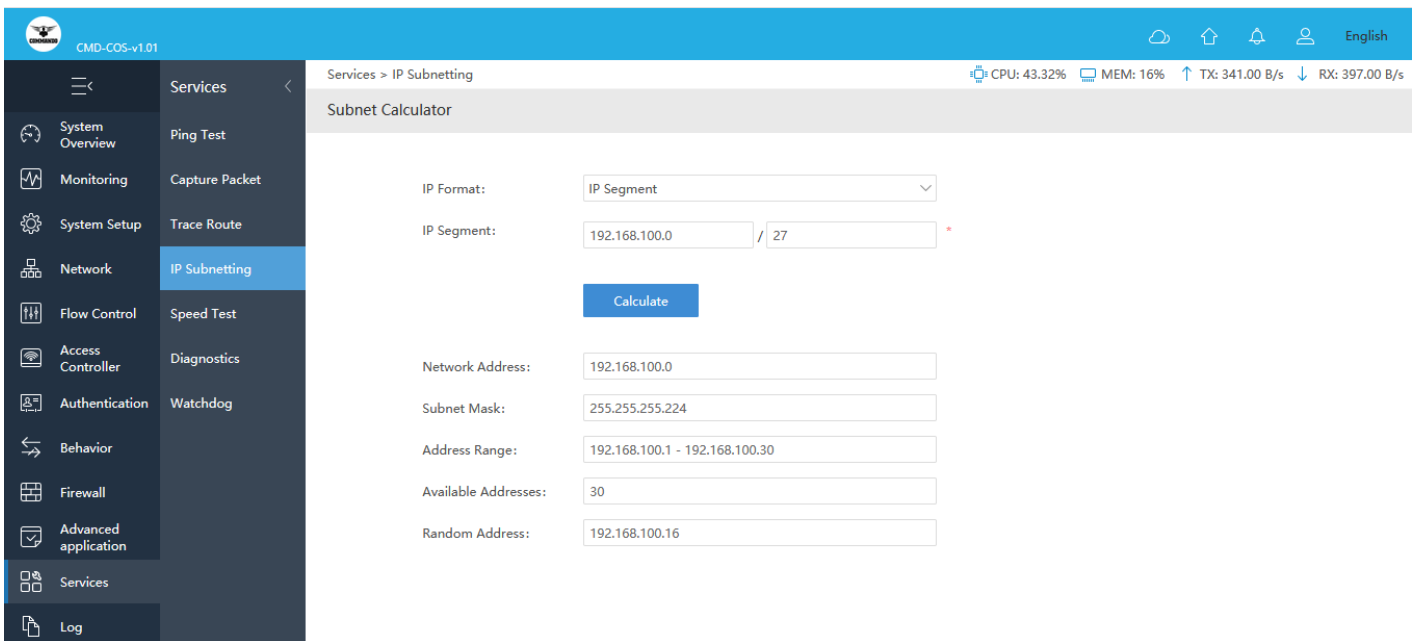
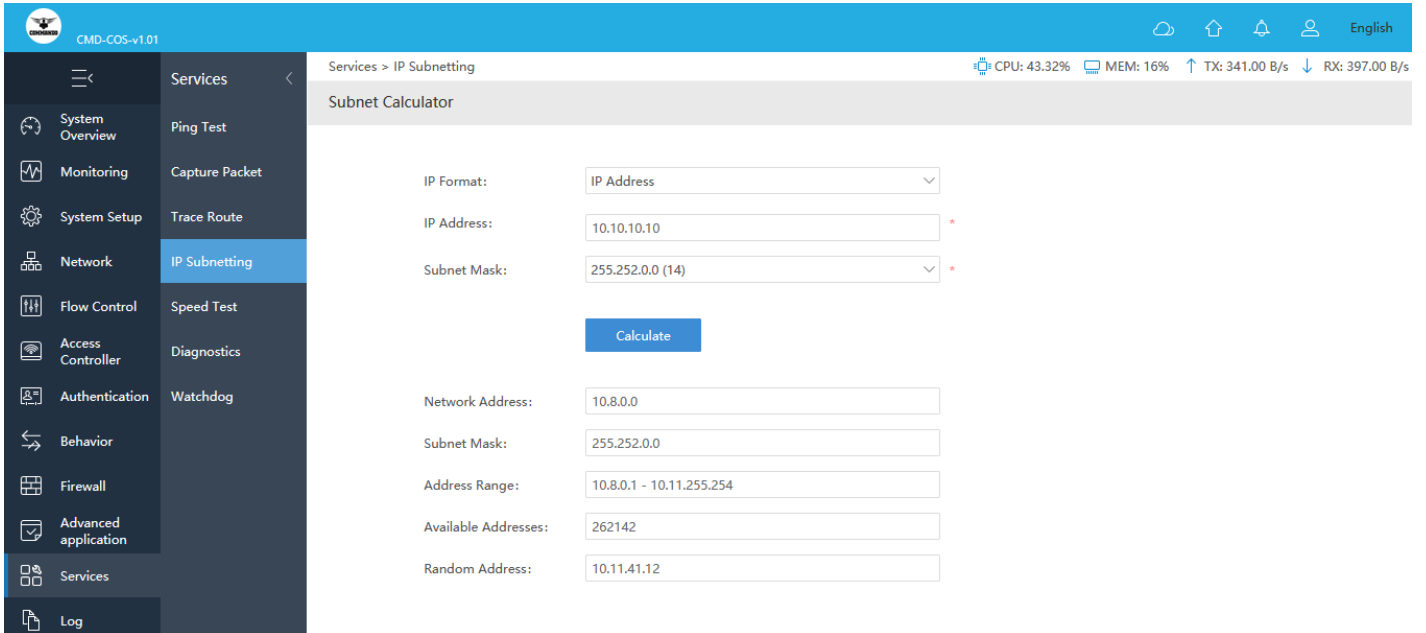


Fig 10.4.2 IP Segment Subnet Calculator page

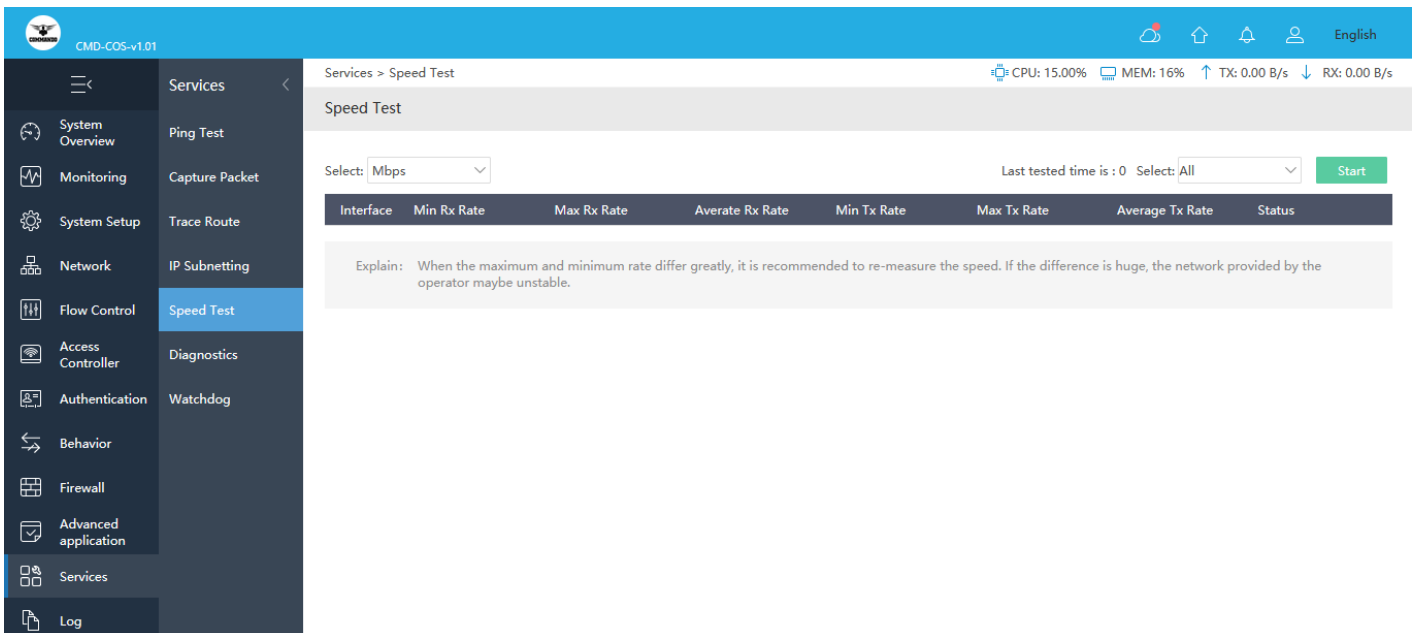


**Fig 10.4.3 IP address Subnet Calculator page**

## 10.5 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 10.5.1 Default Speed Test page**

Services > Speed Test

CPU: 43.32% MEM: 16% TX: 341.00 B/s RX: 397.00 B/s

Select: Mbps Last tested time is : 2021-05-11 23:46:30 Select: All Start

Interface	Min Rx Rate	Max Rx Rate	Average Rx Rate	Min Tx Rate	Max Tx Rate	Average Tx Rate	Status
wan1	1.14 Mbps	1.58 Mbps	1.4 Mbps	0.29 Mbps	0.48 Mbps	0.36 Mbps	speedtest done

Explain: 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 maybe unstable.

**Fig 10.5.2 Speed Test page**

## 10.6 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

Services > Diagnostics

CPU: 43.32% MEM: 16% TX: 341.00 B/s RX: 397.00 B/s

Device Diagnostic

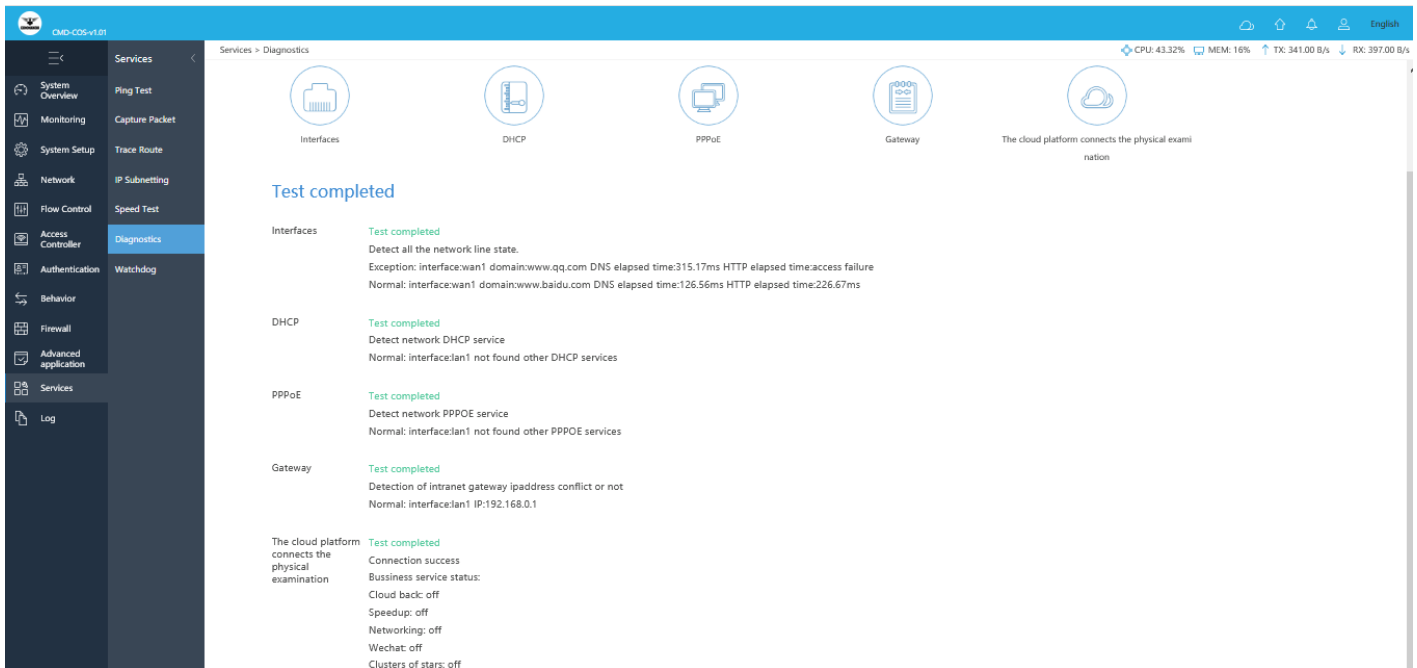
Total Diagnostic  
Diagnostic Your Device

Quick Diagnostic

- Interfaces
- DHCP
- PPPoE
- Gateway
- The cloud platform connects the physical examination



**Fig 10.6.1 Default Device Diagnostic page**

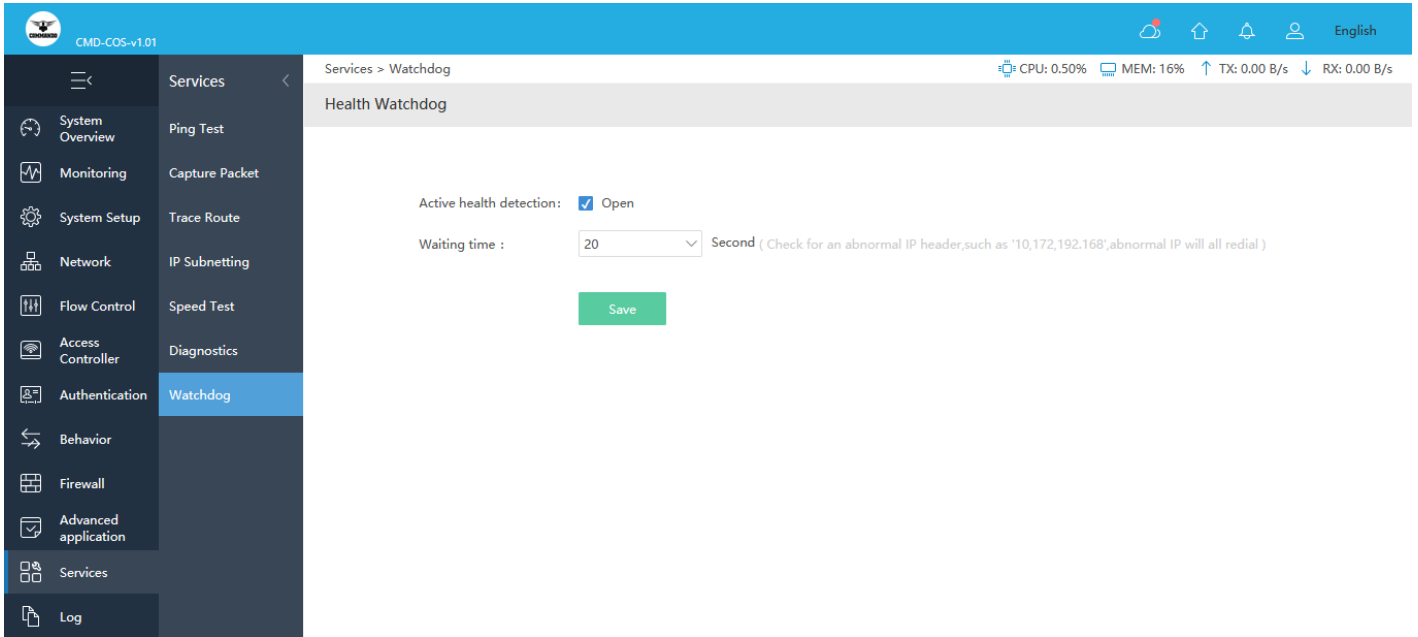


**Fig 10.6.2 Device Diagnostic page**

## 10.7 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 10.7.1 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

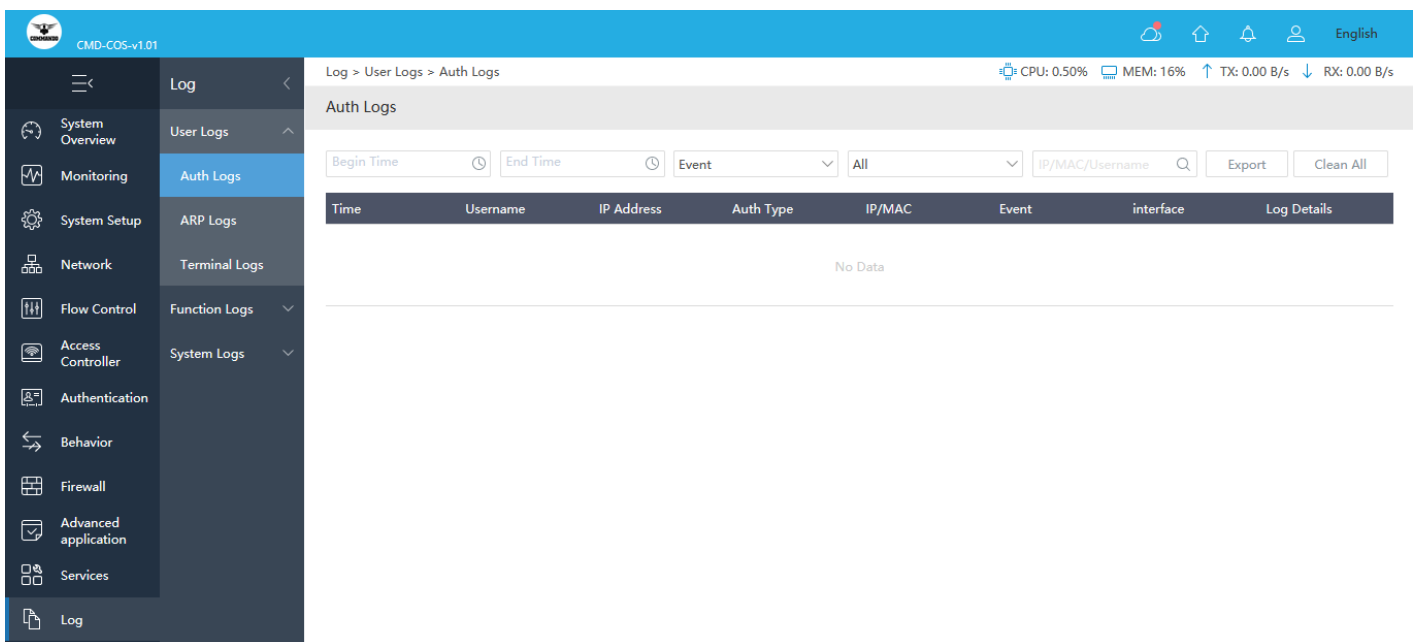
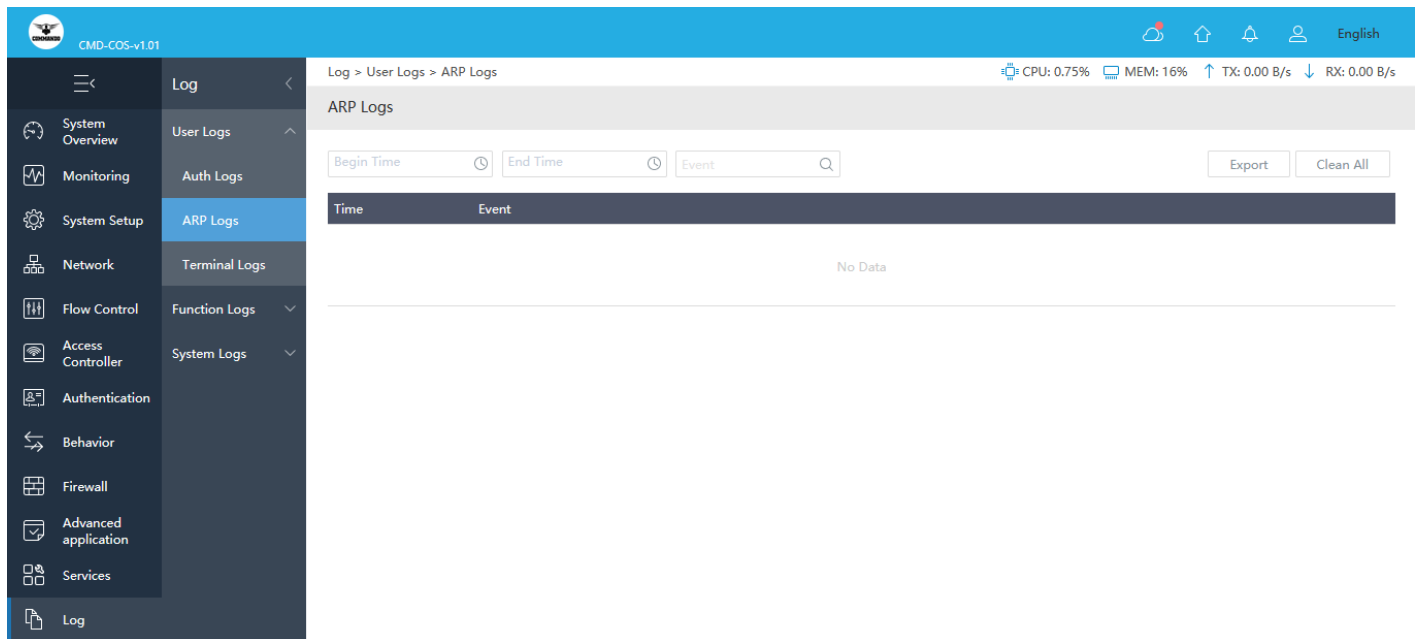


Fig 11.1.1 Default Auth Logs page

## 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

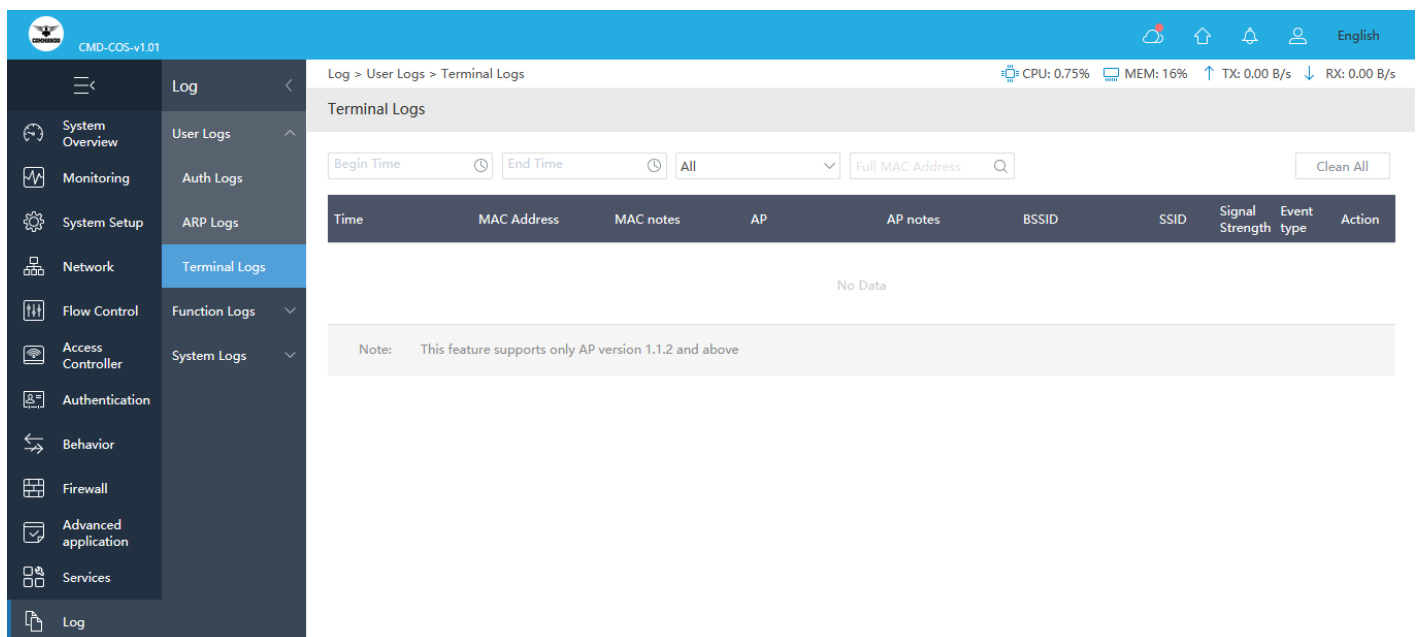


**Fig 11.1.2 Default ARP Logs page**

### 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



**Fig 11.1.3 Default Terminal Logs page**

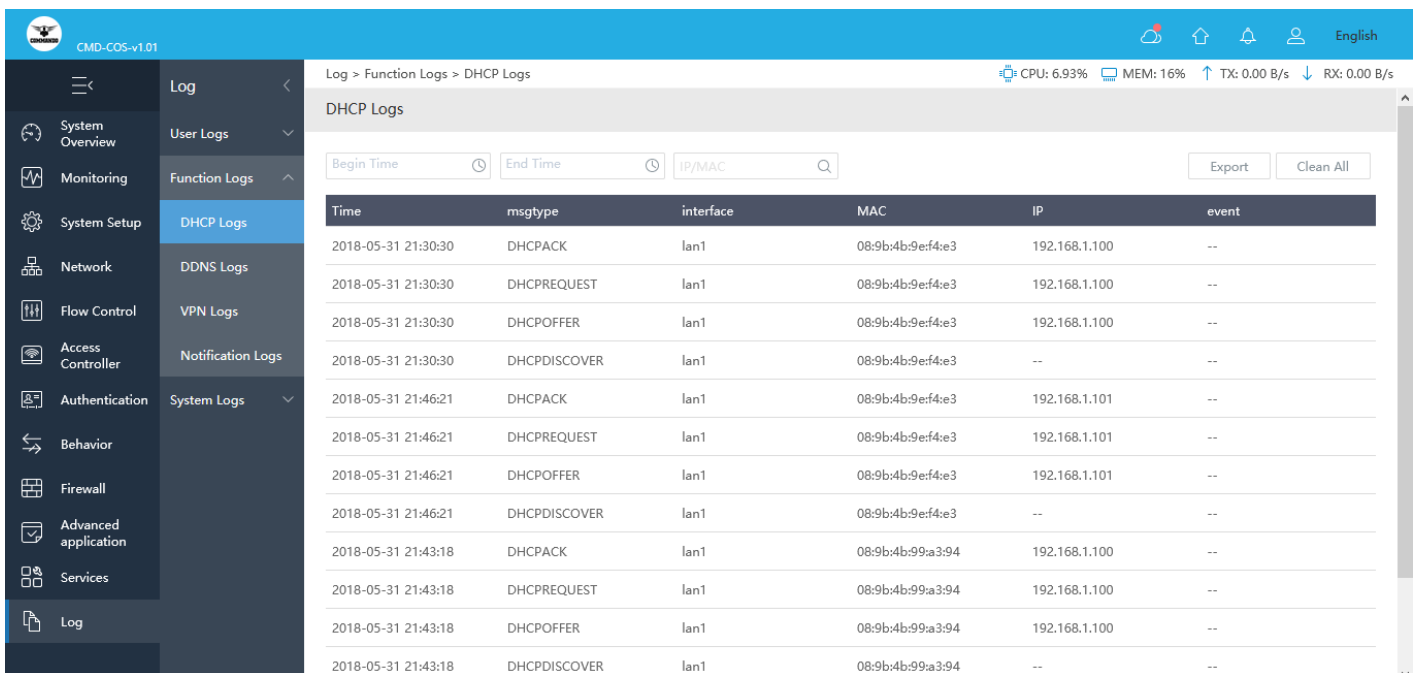
## 11.2 Function Logs

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



The screenshot shows the web interface for CMD-COS-v1.01. The top navigation bar includes a home icon, a notification bell, a user profile icon, and the language 'English'. The left sidebar contains a menu with categories like System Overview, Monitoring, System Setup, Network, Flow Control, Access Controller, Authentication, Behavior, Firewall, Advanced application, Services, and Log. The 'Log' menu is expanded, showing 'User Logs', 'Function Logs', 'DHCP Logs', 'DDNS Logs', 'VPN Logs', 'Notification Logs', and 'System Logs'. The 'DHCP Logs' page is active, displaying a table of logs. The table has columns for Time, msgtype, interface, MAC, IP, and event. The logs show various DHCP messages like DHCPACK, DHCPREQUEST, DHCPPOFFER, and DHCPDISCOVER. The interface also includes search filters for Begin Time, End Time, and IP/MAC, along with 'Export' and 'Clean All' buttons. System status indicators at the top right show CPU: 6.93%, MEM: 16%, TX: 0.00 B/s, and RX: 0.00 B/s.

Time	msgtype	interface	MAC	IP	event
2018-05-31 21:30:30	DHCPACK	lan1	08:9b:4b:9ef4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPREQUEST	lan1	08:9b:4b:9ef4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPOFFER	lan1	08:9b:4b:9ef4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPDISCOVER	lan1	08:9b:4b:9ef4:e3	--	--
2018-05-31 21:46:21	DHCPACK	lan1	08:9b:4b:9ef4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPREQUEST	lan1	08:9b:4b:9ef4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPOFFER	lan1	08:9b:4b:9ef4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPDISCOVER	lan1	08:9b:4b:9ef4:e3	--	--
2018-05-31 21:43:18	DHCPACK	lan1	08:9b:4b:99a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPREQUEST	lan1	08:9b:4b:99a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPOFFER	lan1	08:9b:4b:99a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPDISCOVER	lan1	08:9b:4b:99a3:94	--	--

Fig 11.2.1 Default DHCP Logs page

Log > Function Logs > DHCP Logs

CPU: 0.25% MEM: 20% TX: 0.00 B/s RX: 0.00 B/s

Begin Time [ ] End Time [ ] IP/MAC [ ] Export Clean All

Time	msgtype	interface	MAC	IP	event
2021-05-13 18:54:24	DHCPACK	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 18:54:24	DHCPREQUEST	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 18:43:27	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.0.105	--
2021-05-13 18:43:27	DHCPREQUEST	lan1	08:9b:4b:99:a3:94	192.168.0.105	--
2021-05-13 18:43:12	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.0.102	--
2021-05-13 18:43:12	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.0.102	--
2021-05-13 17:54:24	DHCPACK	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 17:54:24	DHCPREQUEST	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 17:54:24	DHCP OFFER	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 17:54:24	DHCPDISCOVER	lan1	c4:d9:87:a7:ad:46	--	--
2021-05-13 17:43:25	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.0.105	--

**Fig 11.2.2 DHCP Logs page**

### DDNS Logs:

It contains IP Address, Domain Name and Interface along with Log details and time.

For DDNS Logs, Click on Log > Function Logs > DDNS Logs

Log > Function Logs > DDNS Logs

CPU: 9.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Begin Time [ ] End Time [ ] Export Clean All

Time	IP Address	Domain Name	Interface	Result	Log Details
No Data					

**Fig 11.2.3 Default DDNS Logs page**

Log > Function Logs > DDNS Logs

CPU: 0.00% MEM: 20% TX: 69.00 B/s RX: 73.00 B/s

DDNS Logs

Begin Time [ ] End Time [ ] Export Clean All

Time	IP Address	Domain Name	Interface	Result	Log Details
2021-05-13 19:10:13	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 19:05:03	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 19:00:05	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:55:07	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:50:08	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:45:17	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:40:04	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:35:02	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:30:08	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:25:03	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 18:20:09	--	www.commandonetworks.com	Auto	fail	Error: domain errors

**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

Log > Function Logs > VPN Logs

CPU: 0.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

VPN Logs

All [ ] Begin Time [ ] End Time [ ] Log Details [ ] Export Clean All

Time	Interface	Log Details
No Data		

**Fig 11.2.5 Default VPN Logs page**

Log > Function Logs > VPN Logs

CPU: 0.50% MEM: 20% TX: 0.00 B/s RX: 0.00 B/s

VPN Logs

All Begin Time End Time Log Details Export Clean All

Time	Interface	Log Details
2021-04-18 17:12:41	pptpCOMMANDO	Call manager exited with error 256
2021-04-18 17:12:41	pptpCOMMANDO	Exit.
2021-04-18 17:12:41	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2021-04-18 17:12:41	pptpCOMMANDO	connect: Connection timed out
2021-04-18 17:10:23	pptpCOMMANDO	Call manager exited with error 256
2021-04-18 17:10:23	pptpCOMMANDO	Exit.
2021-04-18 17:10:23	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2021-04-18 17:10:23	pptpCOMMANDO	connect: Connection timed out
2021-04-18 17:08:06	pptpCOMMANDO	Call manager exited with error 256
2021-04-18 17:08:06	pptpCOMMANDO	Exit.
2021-04-18 17:08:06	pptpCOMMANDO	Could not open control connection to 10.10.10.1

**Fig 11.2.6 VPN Logs page**

### Notification Logs:

It shows Severity Normal but significant conditions.

For Notification Logs, Log > Function Logs > Notification Logs.

Log > Function Logs > Notification Logs

CPU: 2.23% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Notification Logs

Begin Time End Time Type IP Export Clean All

Time	IP Address	Event	Type
No Data			

**Fig 11.2.7 Default Notification Logs page**

## 11.3 System Logs

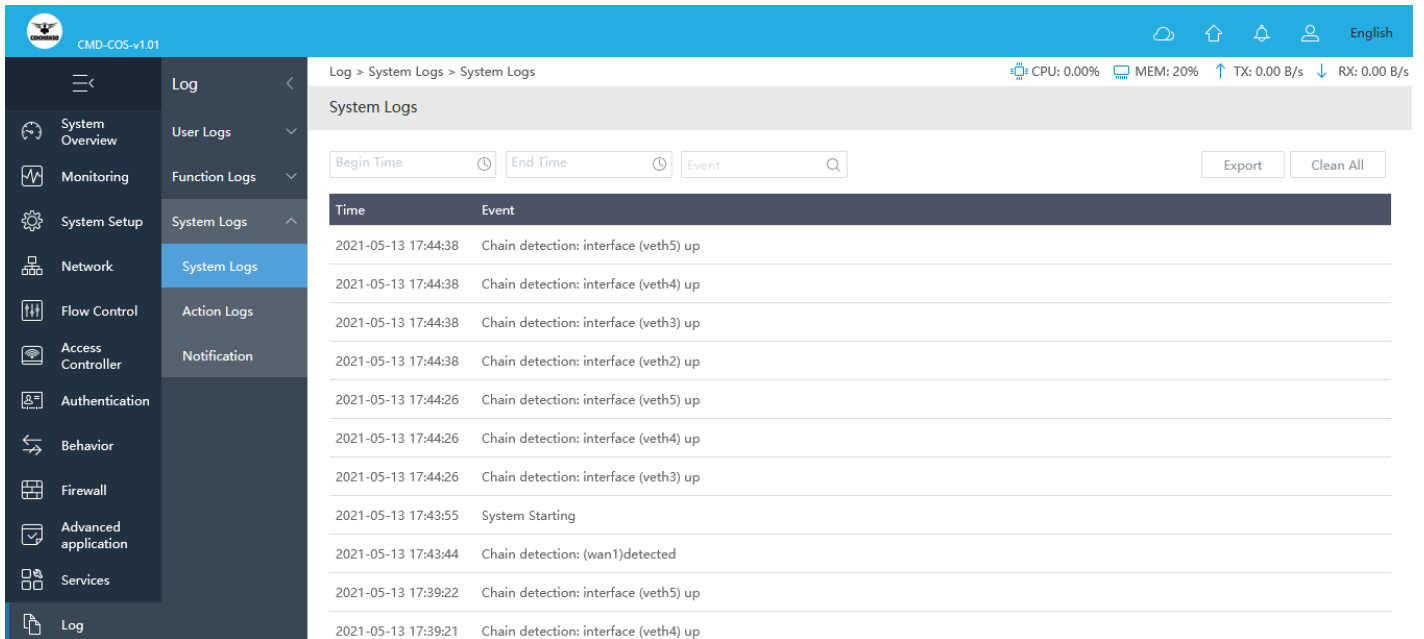
The System Logs provides a variety of logs that you can use to troubleshoot and debug transactions and events that take place within the instance Action and Notification Logs.

### System Logs:



These logs are invaluable for monitoring and troubleshooting your system.

For configure System Logs, Click on Log > System Logs > System Logs.

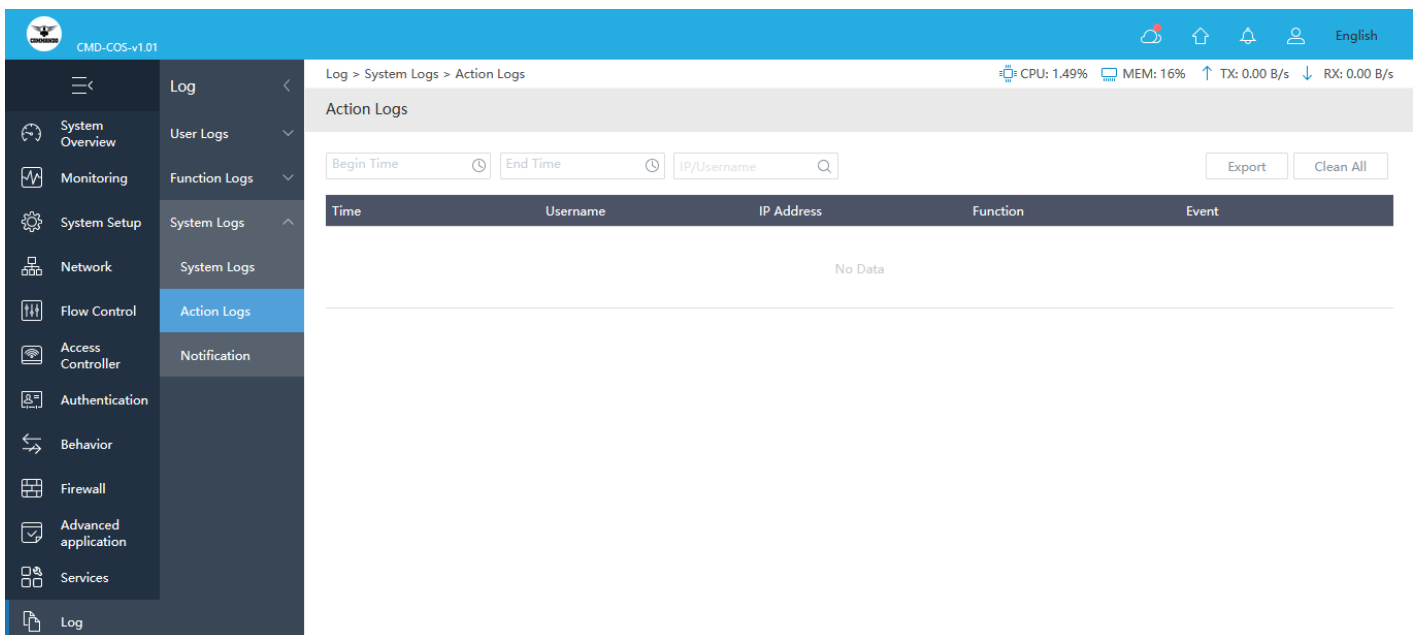


**Fig 11.3.1 Default System Logs page**

### 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**

Log > System Logs > Action Logs

CPU: 1.49% MEM: 20% TX: 0.00 B/s RX: 0.00 B/s

Begin Time End Time IP/Username Export Clean All

Time	Username	IP Address	Function	Event
2021-05-13 18:01:52	admin	192.168.0.100	--	Login
2021-05-12 23:04:34	admin	192.168.0.100	Speed	Test exec action for clean
2021-05-12 21:06:19	admin	192.168.0.100	--	Login
2021-05-12 20:10:29	admin	192.168.0.100	--	Login
2021-05-12 20:10:29	admin	192.168.0.100	--	Login
2021-05-12 20:07:44	admin	192.168.0.100	--	Login
2021-05-11 23:45:04	admin	192.168.0.100	Speed	Test exec action for clean
2021-05-11 23:26:50	admin	192.168.0.100	UDPHY	Set exec action for edit
2021-05-11 23:26:33	admin	192.168.0.100	UDPHY	Set add a rule
2021-05-11 23:26:17	admin	192.168.0.100	UDPHY	Set exec action for edit
2021-05-11 23:26:11	admin	192.168.0.100	UDPHY	Set add a rule

**Fig 11.3.3 Action Logs page**

**Notification:**

For viewing Username, Time and Actions.

For viewing Notification, Click on Log > System Logs > Notification.

Log > System Logs > Notification

CPU: 1.73% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Clean All

Username	Time	Actions
No Data		

**Fig 11.3.4 Notification page**

# COMMANDO CLOUD

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.

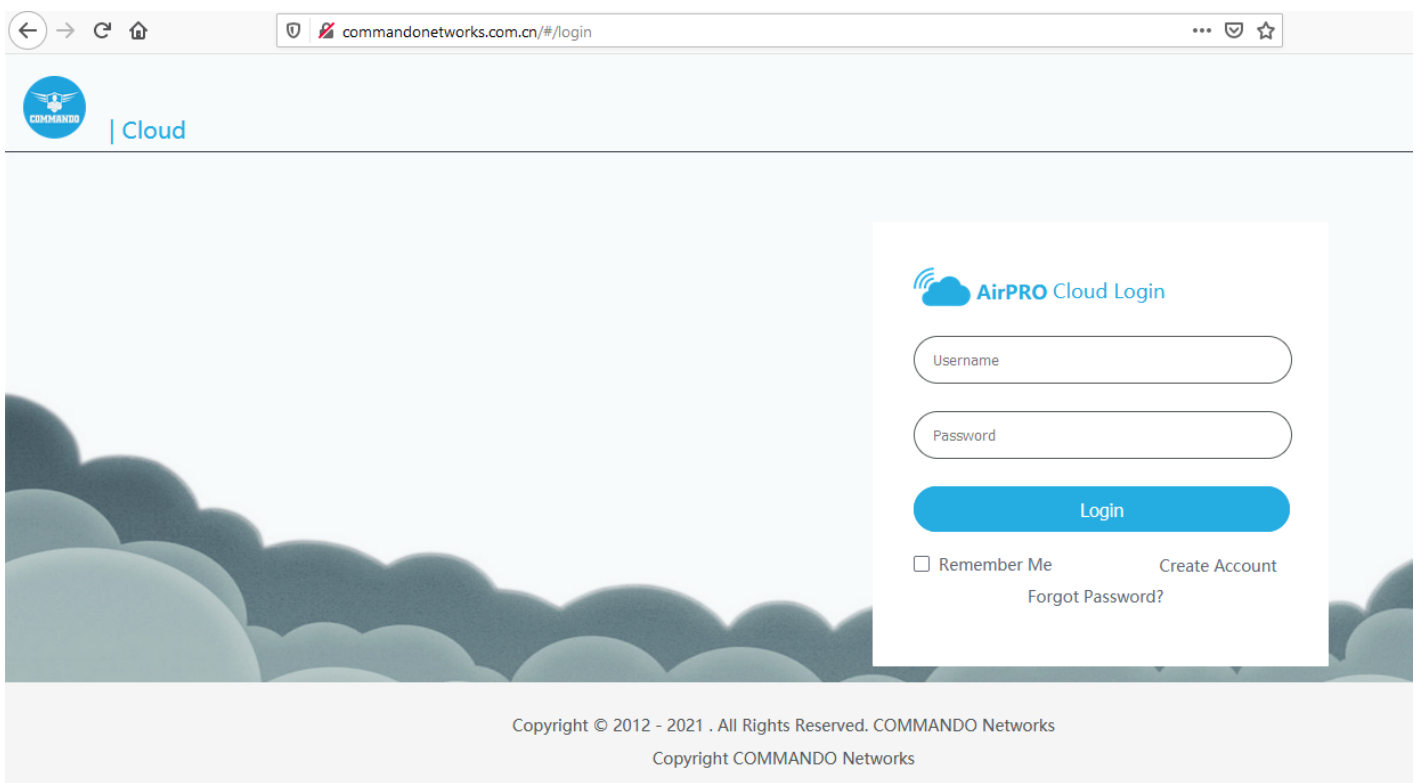


Fig 12.1 Cloud Login page

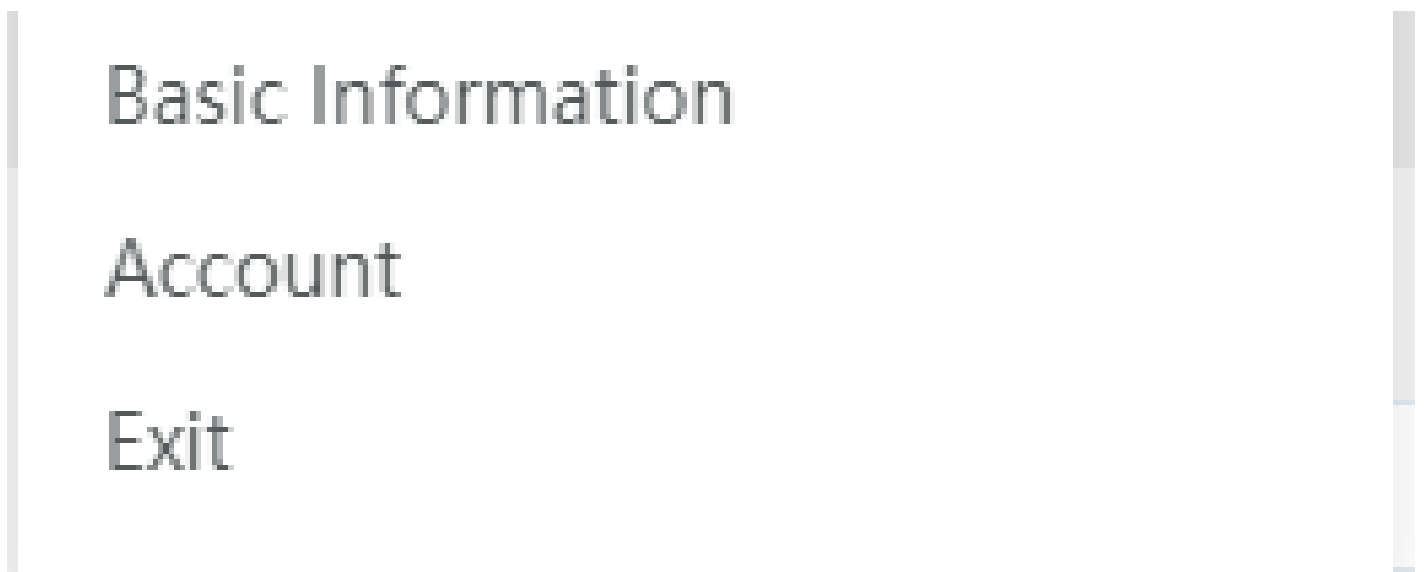
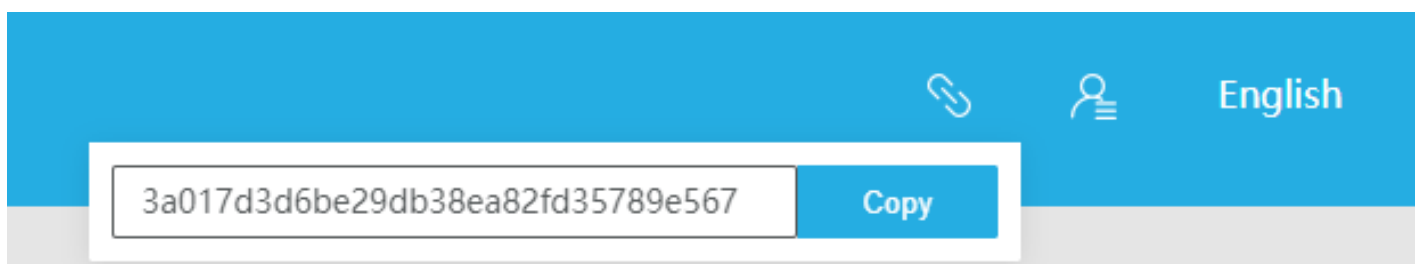


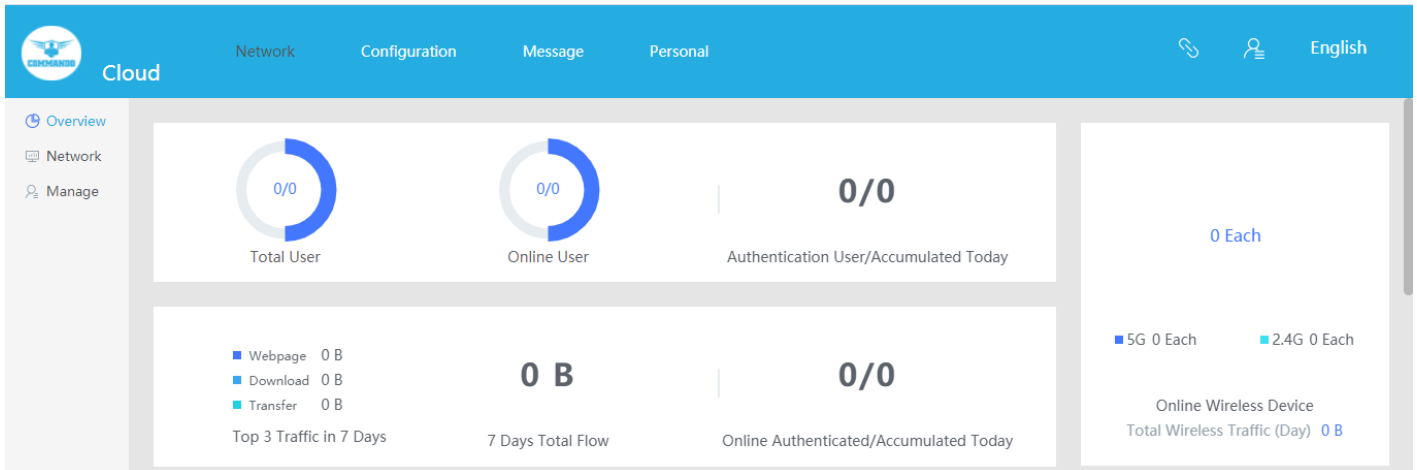
Fig 12.2 Cloud User Language setting page



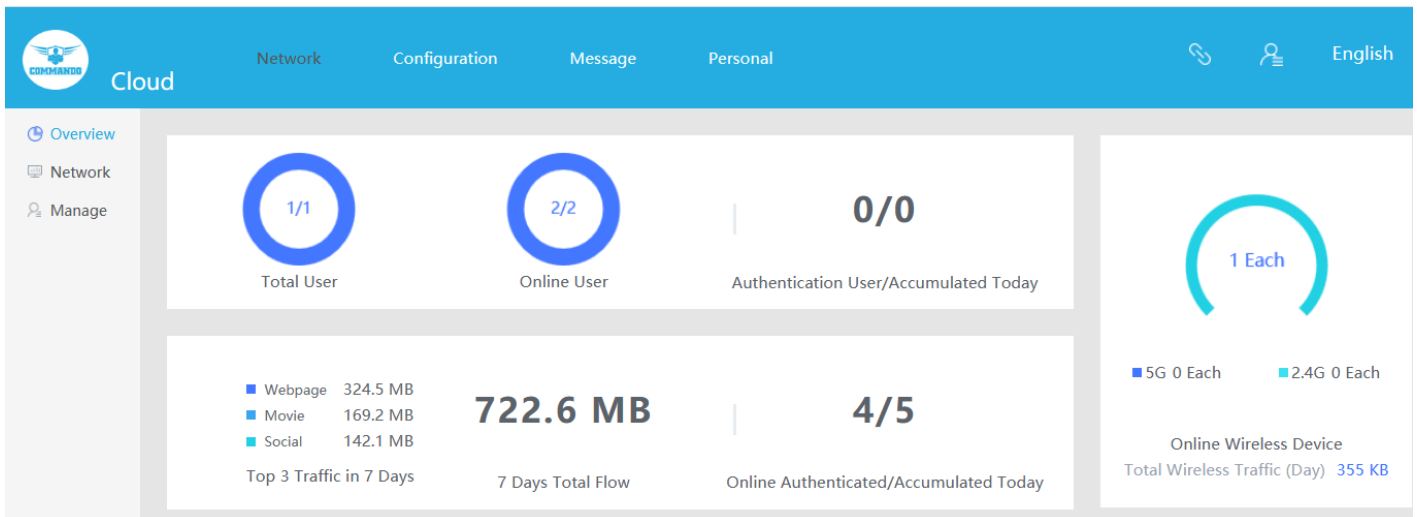
**Fig 12.3 Cloud Binding page**

**12.1 AirPRO Cloud Overview**

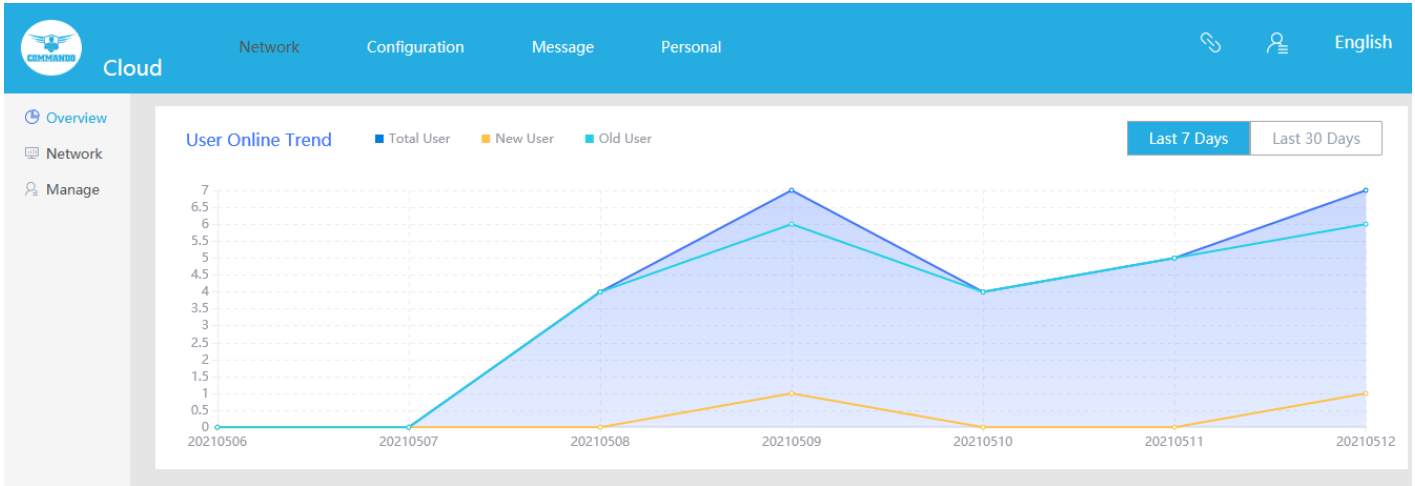
A cloud-managed access point or networking solution allows business owners to manage Wi-Fi and network infrastructure over the cloud with zero maintenance charges, centralize control painlessly. This means businesses can connect to the cloud by subscribing to a pay-as-you-go, on-demand model.



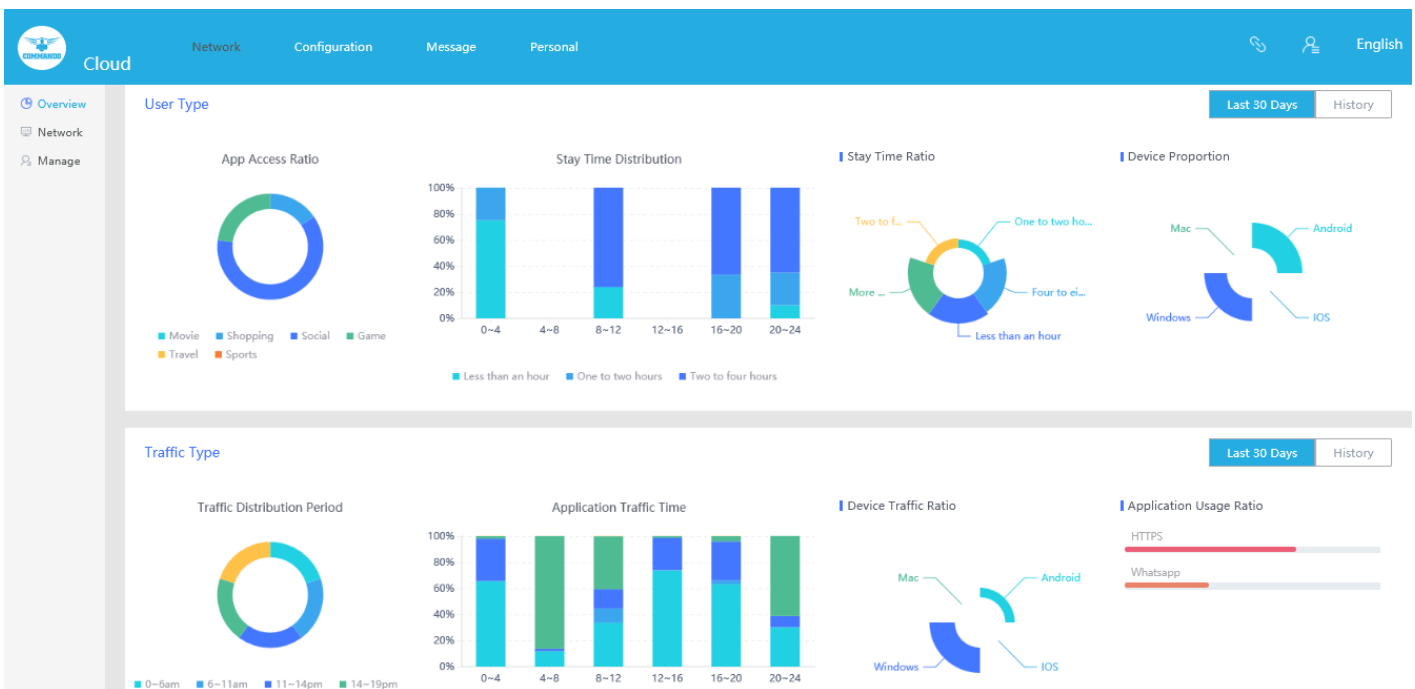
**Fig 12.1.1 Default Cloud Overview page**



**Fig 12.1.2 Cloud Overview page**



**Fig 12.1.3 Cloud User online trend page**



**Fig 12.1.4 Cloud User Type page**

## 12.2 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.

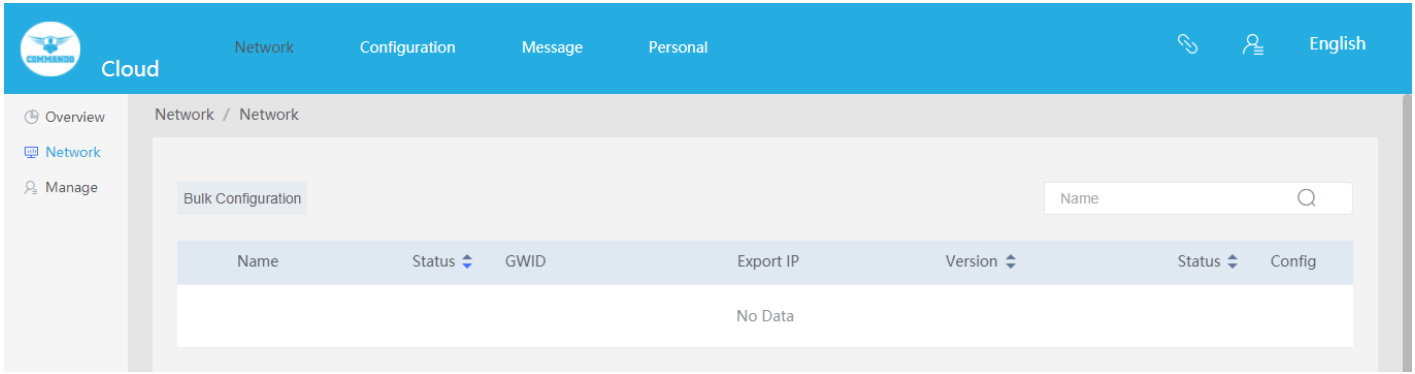


Fig 12.2.1 Default Bulk configuration page

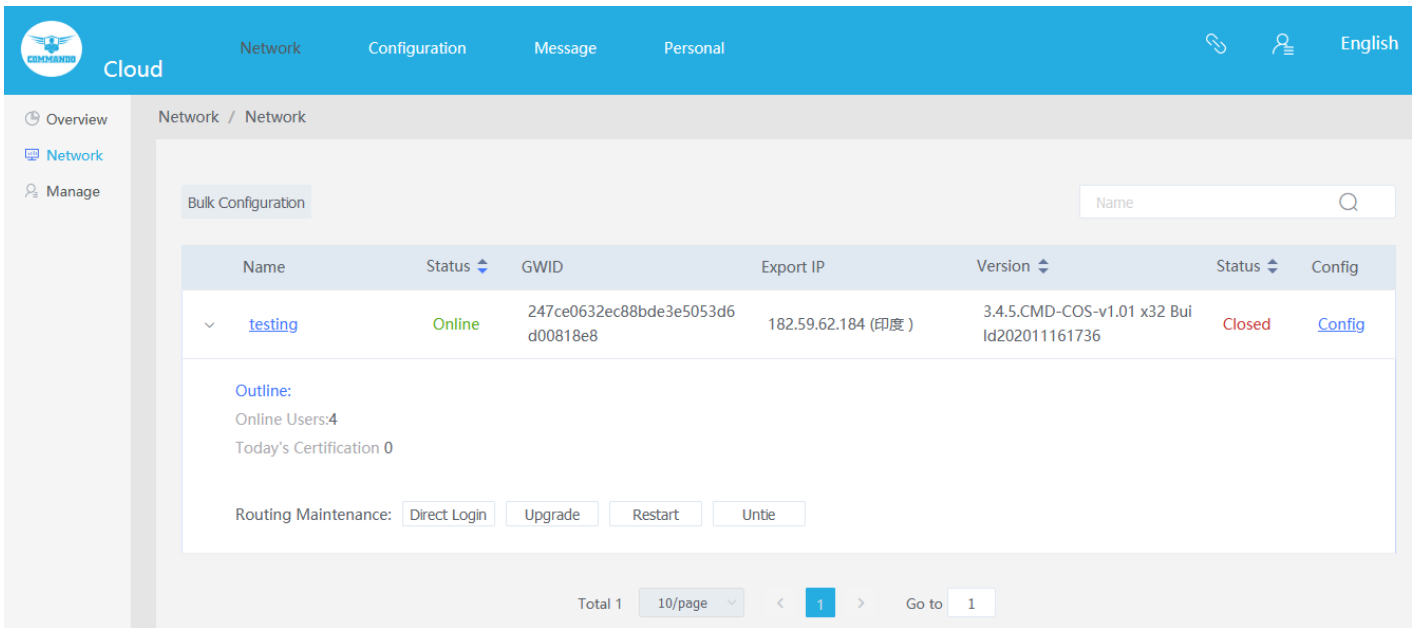
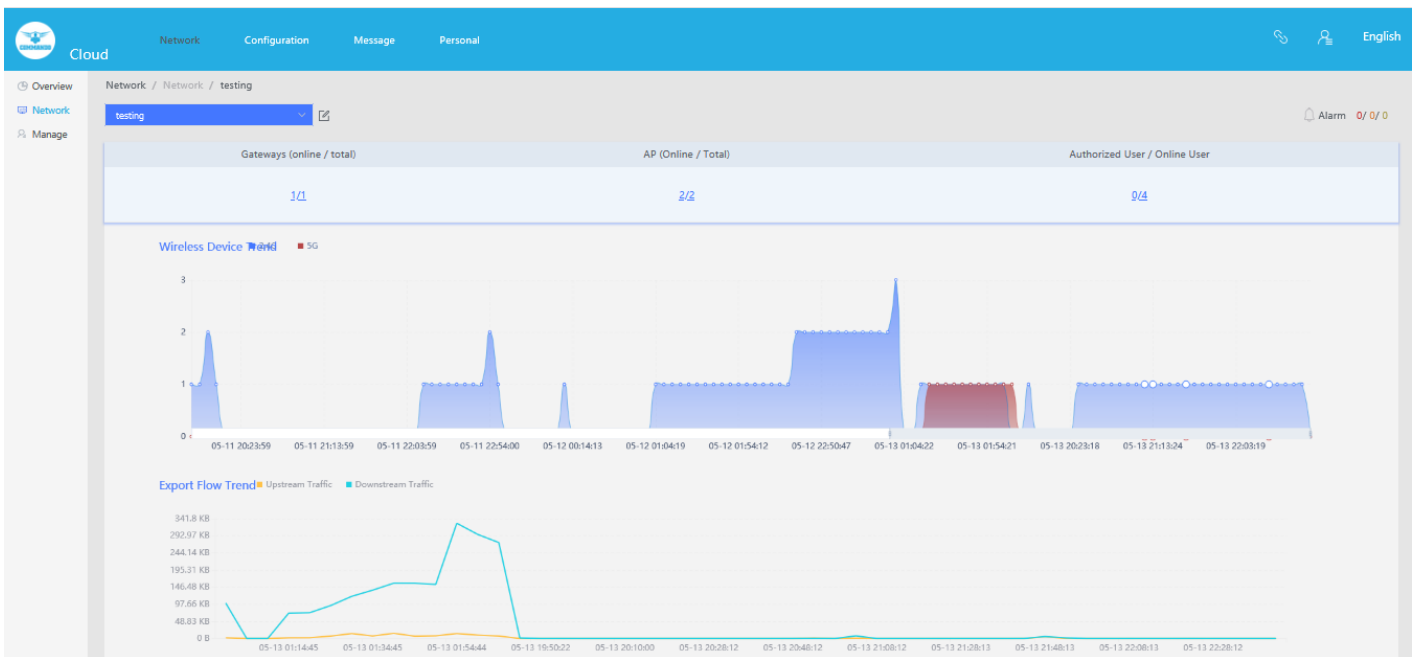
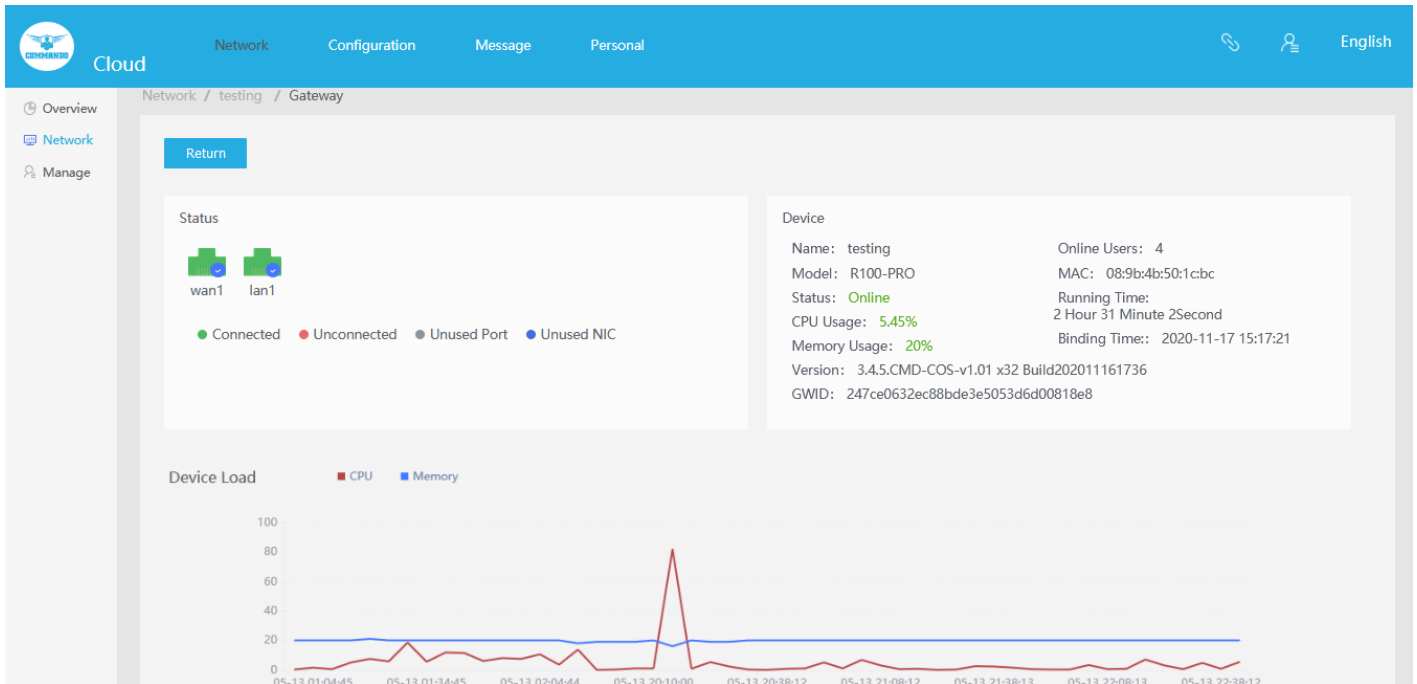


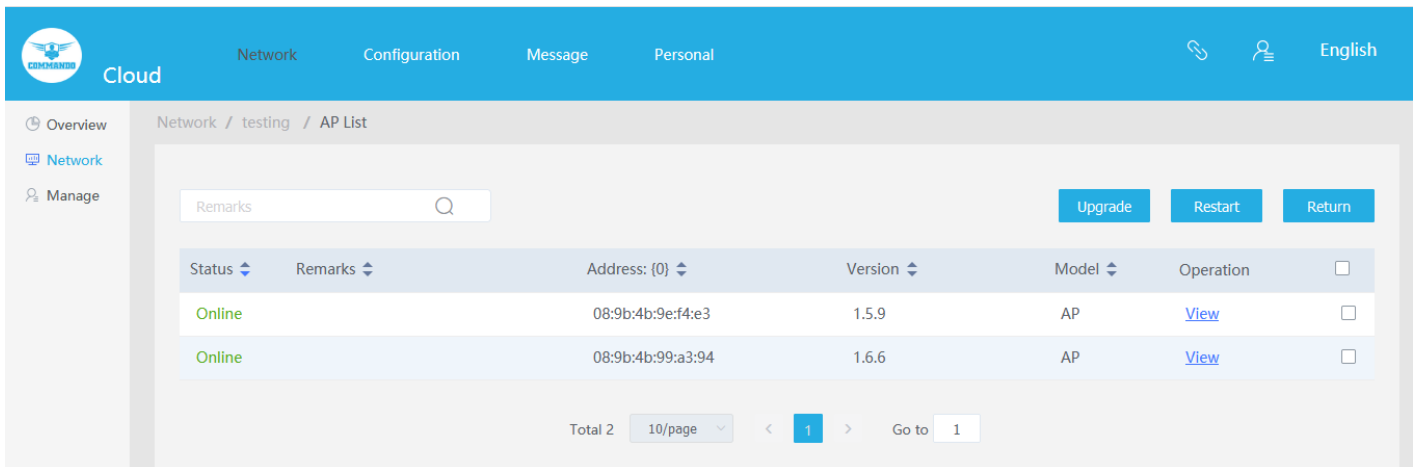
Fig 12.2.2 Bulk configuration page



**Fig 12.2.3 Network Devices listed in Cloud page**

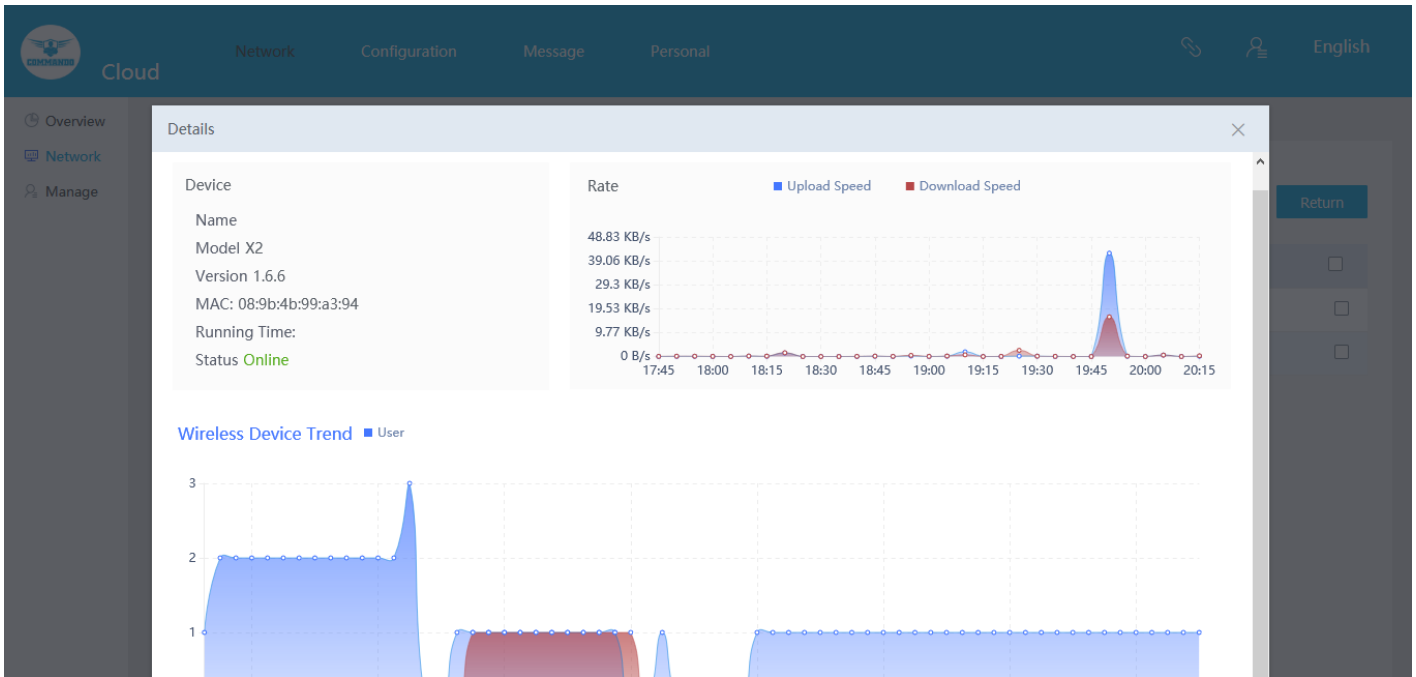


**Fig 12.2.4 Gateway page**



**Fig 12.2.5 AP List page**





**Fig 12.2.5 Bulk configuration for particular AP Device page**

Device	IP	MAC	AP_MAC	Total Tx	Total Rx	Total Time	Online time	Operation
DESKTOP-70API55	192.168.0.10	c4:d9:87:a7:d:46	c4:d9:87:a7:d:46	6.14 MB	61.47 MB	2 Hour 19 Minute 11Second	2021-05-13 17:54	
	192.168.0.10	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	192.168.0.10	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	192.168.0.10	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	

**Fig 12.2.6 Network Management for all users' page**

## 12.3 Configuration

The route controller is responsible for configuring routes in the cloud appropriately. Cloud networking allows users to build networks using cloud-based services. 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.

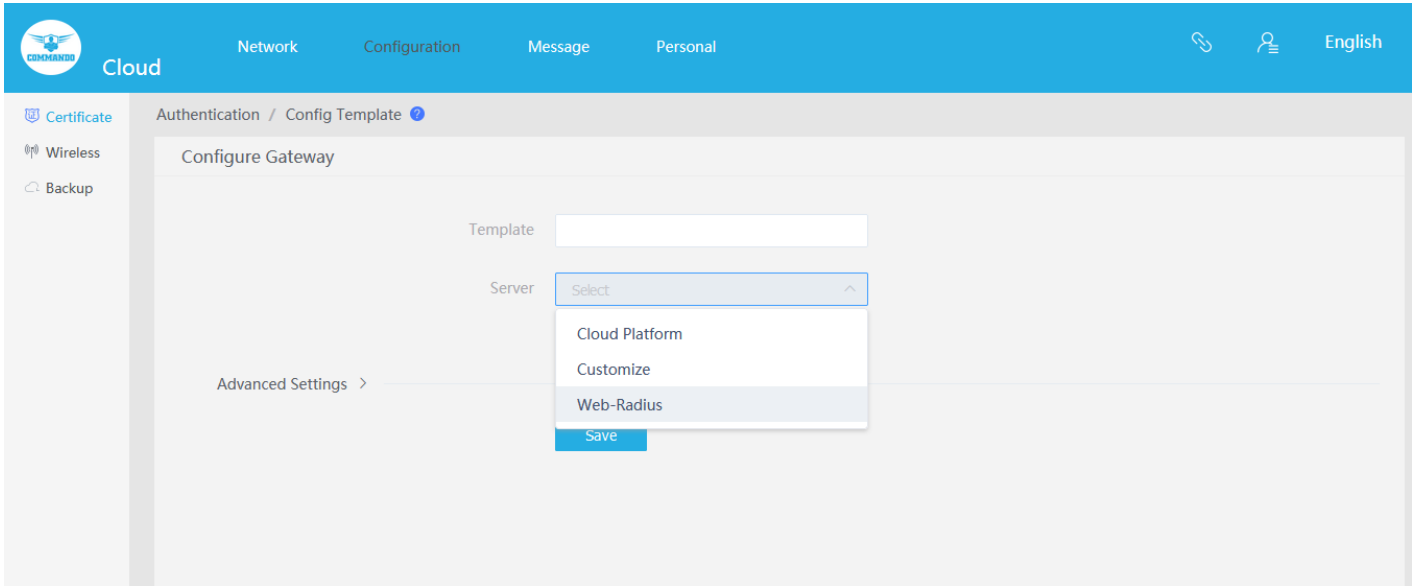


Fig 12.3.1 Default Authentication page

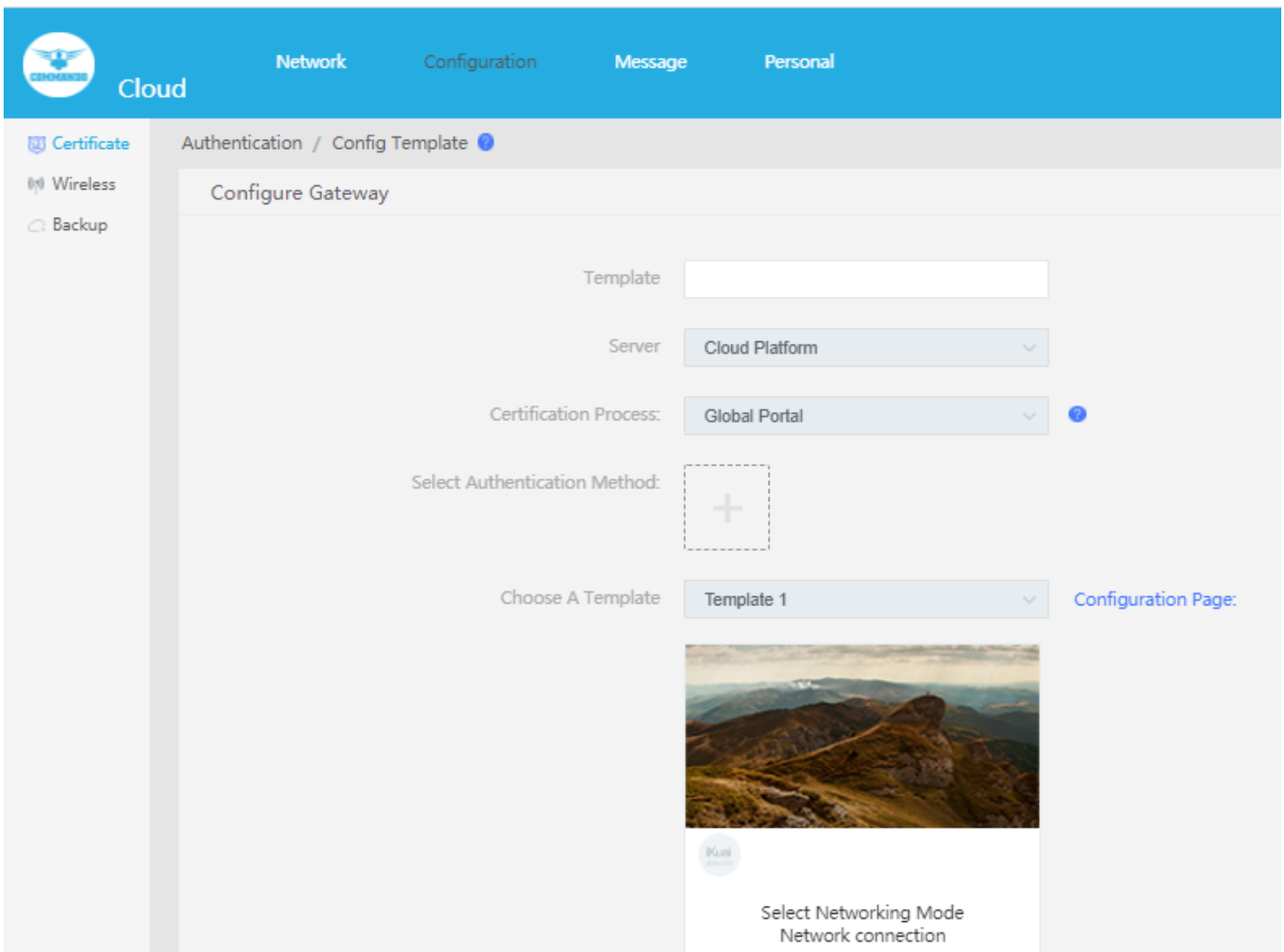


Fig 12.3.2 Default Cloud platform configure gateway page

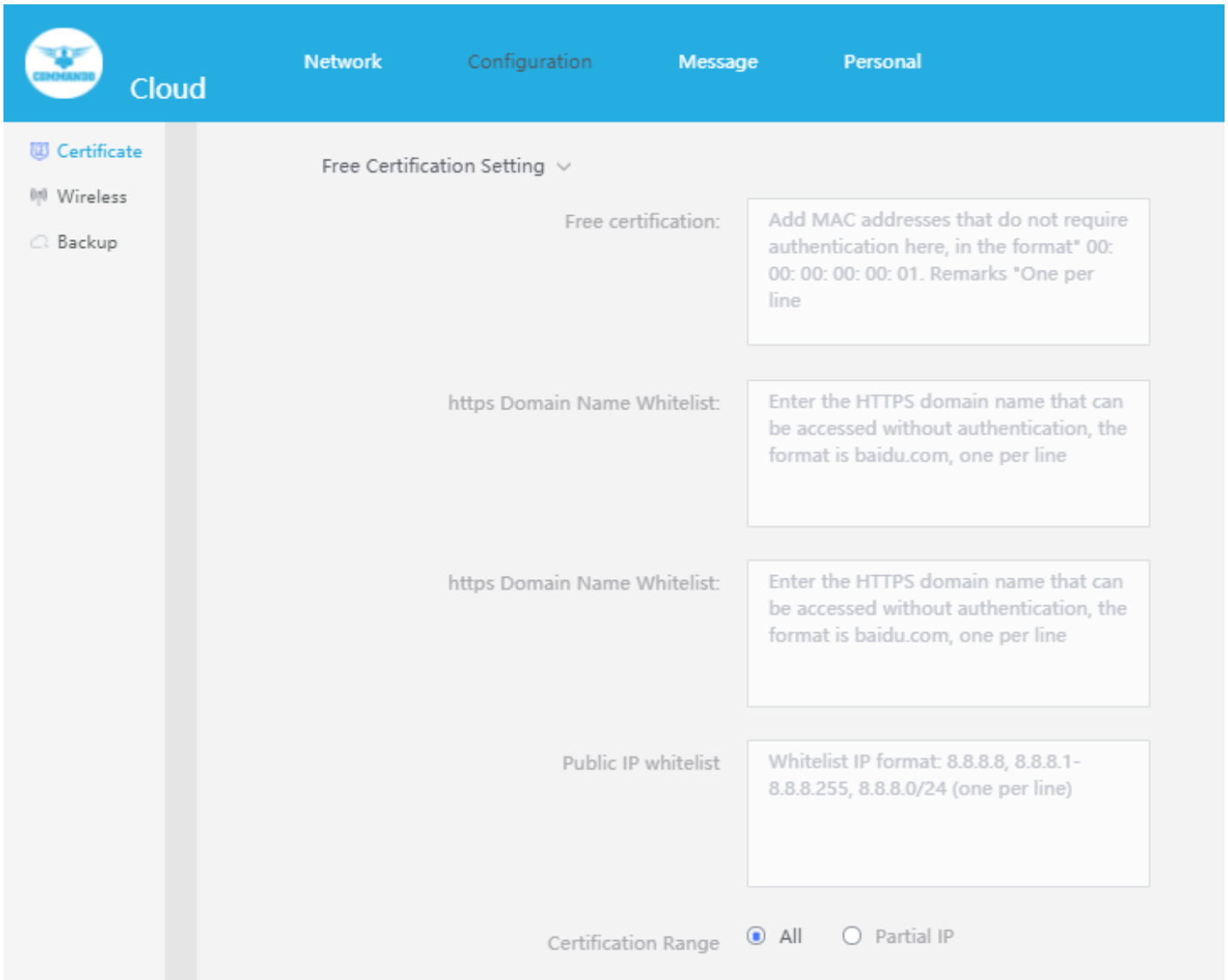


Fig 12.3.3 Default Authentication Free certification setting page

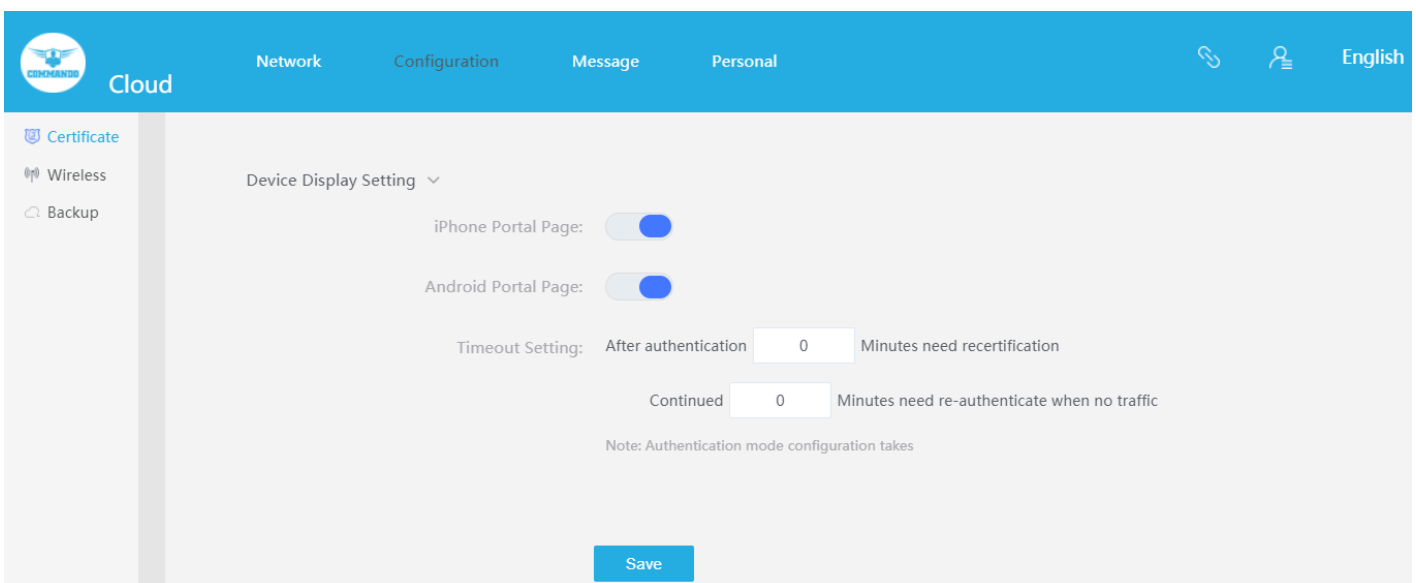
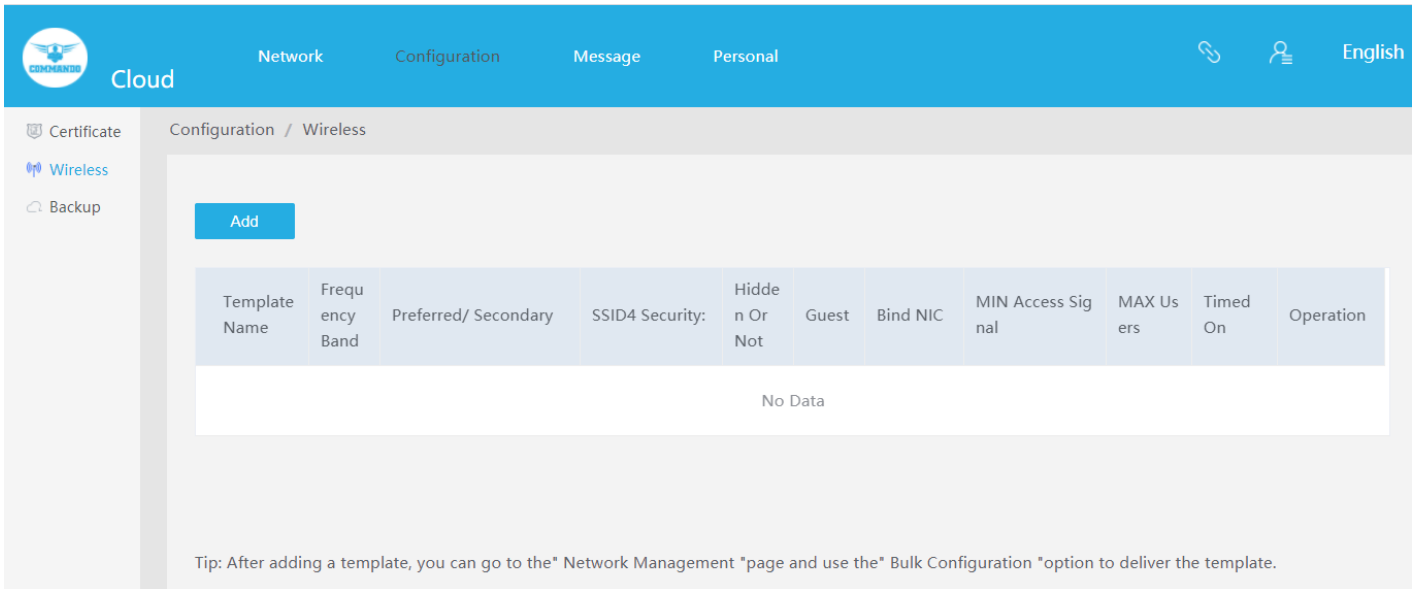
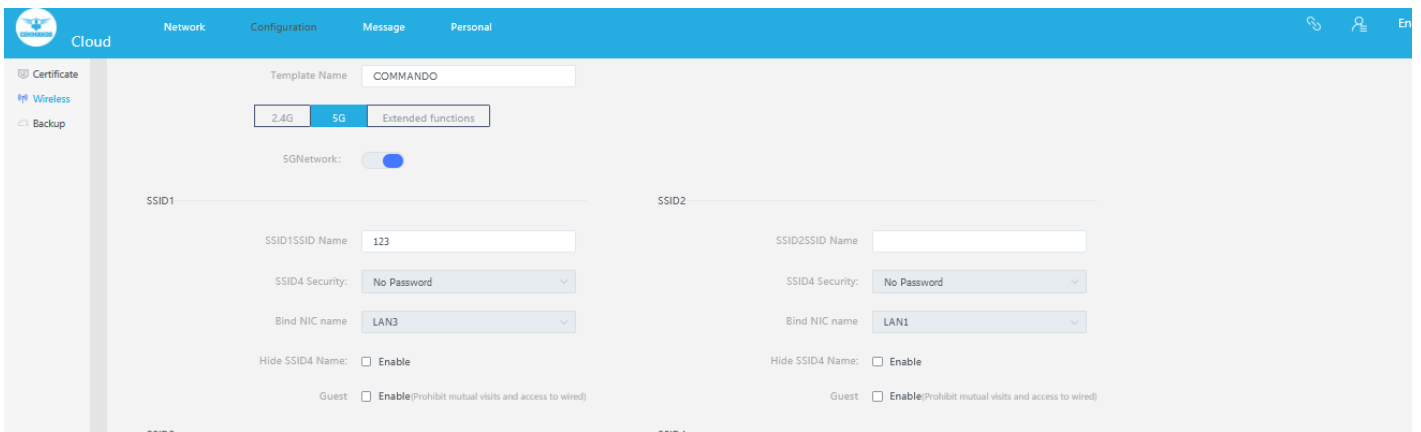


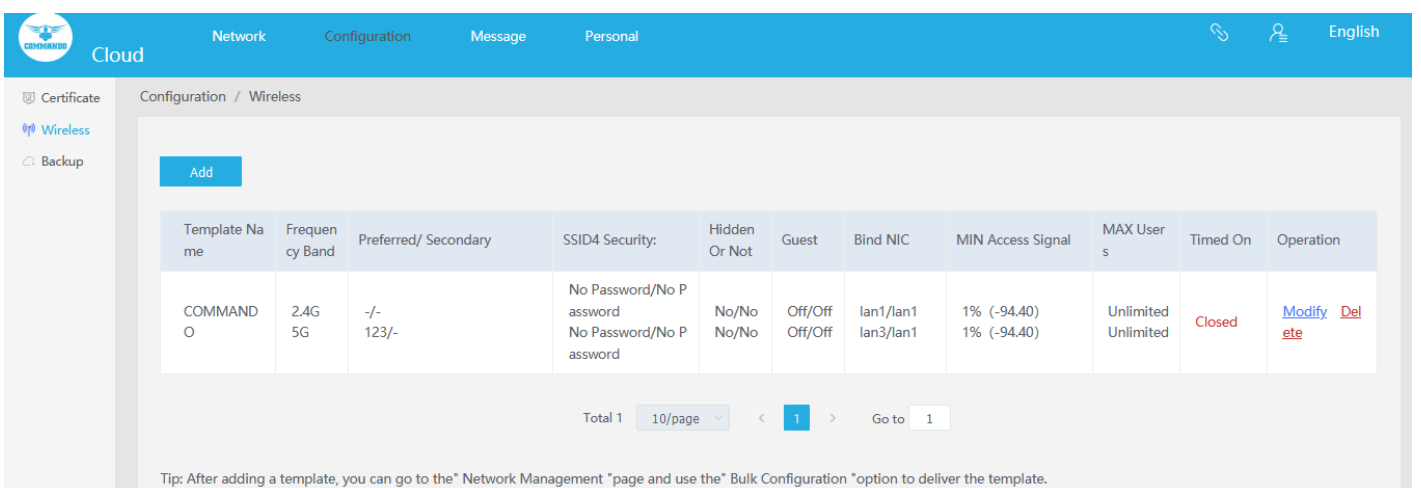
Fig 12.3.4 Default Authentication Device Display setting page



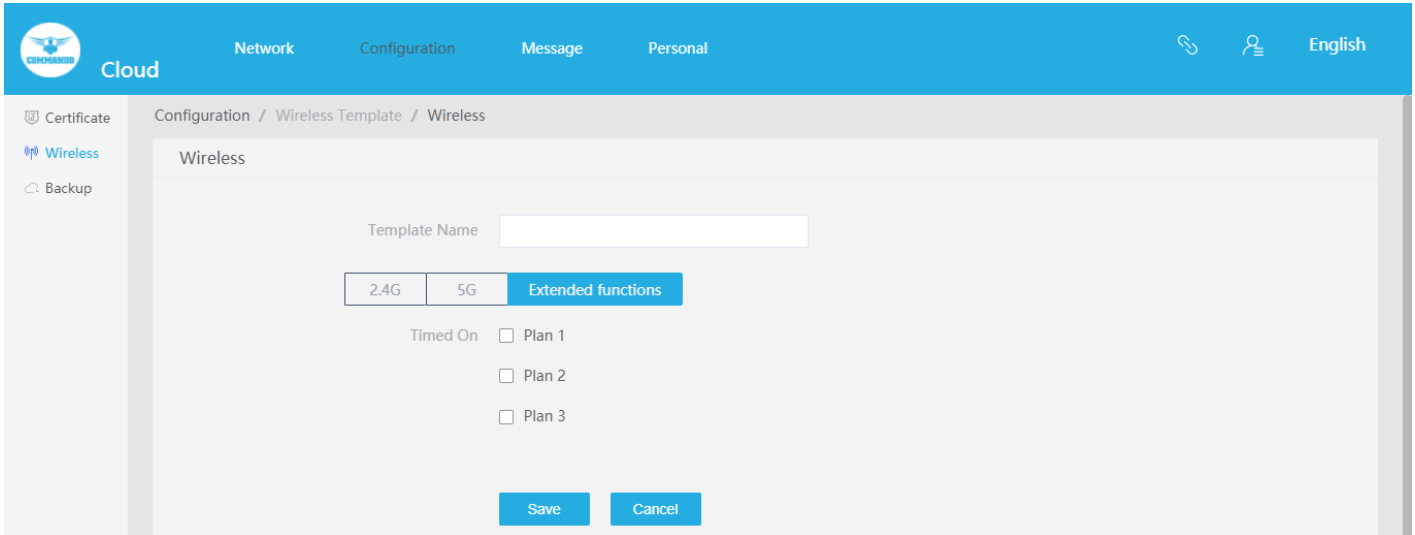
**Fig 12.3.5 Default Wireless add setting page**



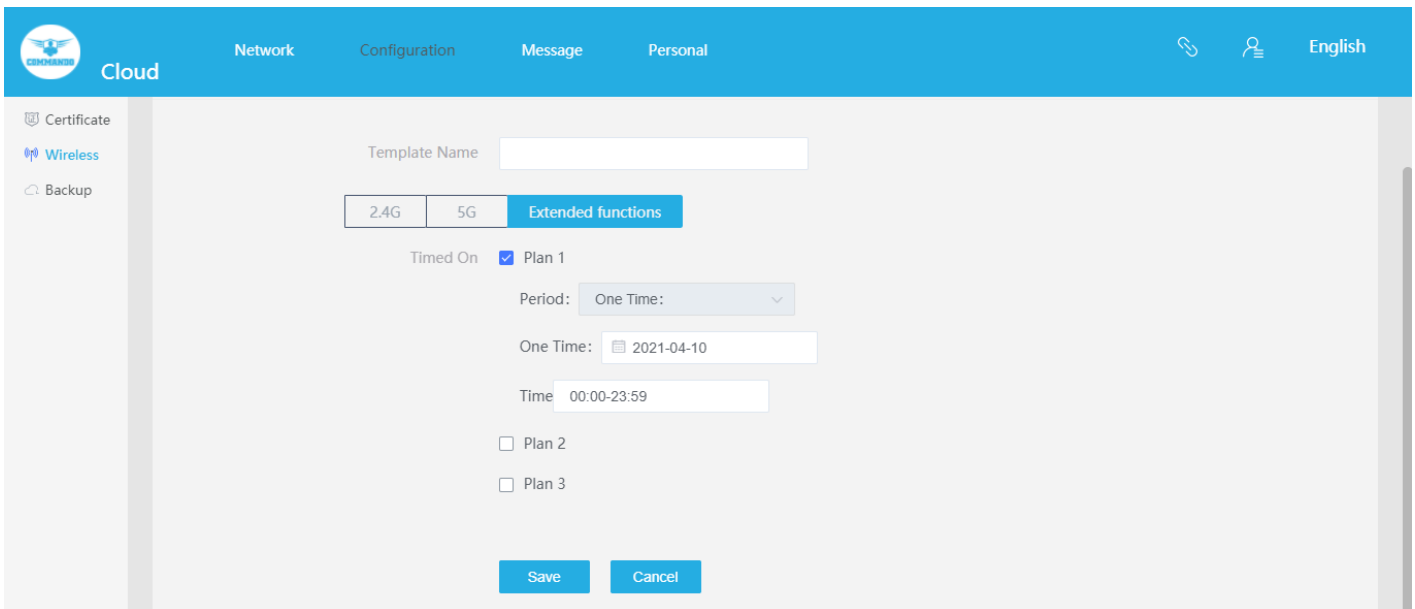
**Fig 12.3.6 Add 5G Wireless setting page**



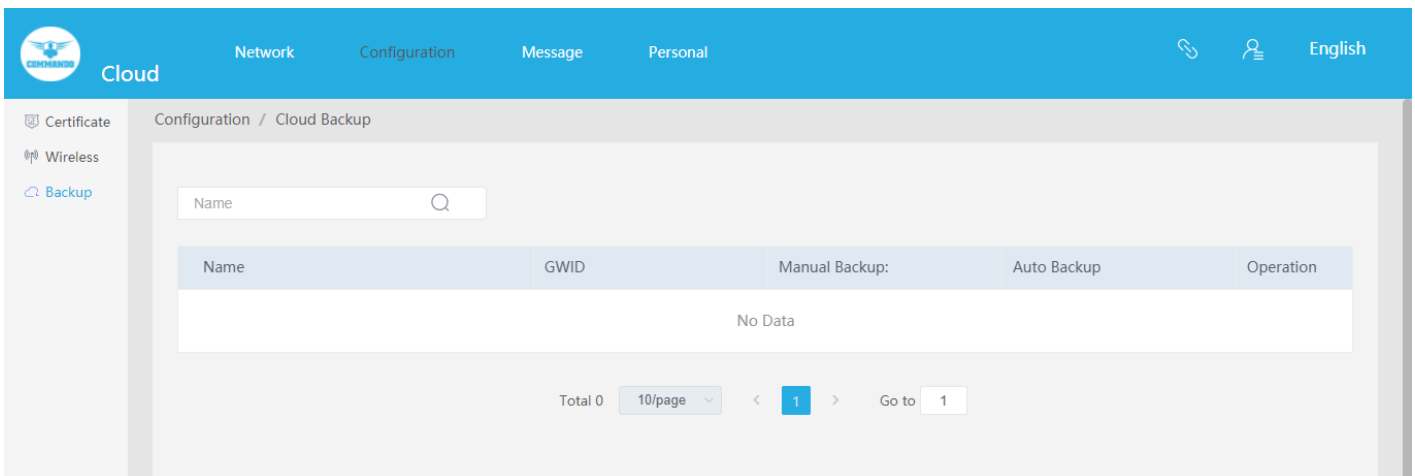
**Fig 12.3.6 Wireless Configuration setting page**



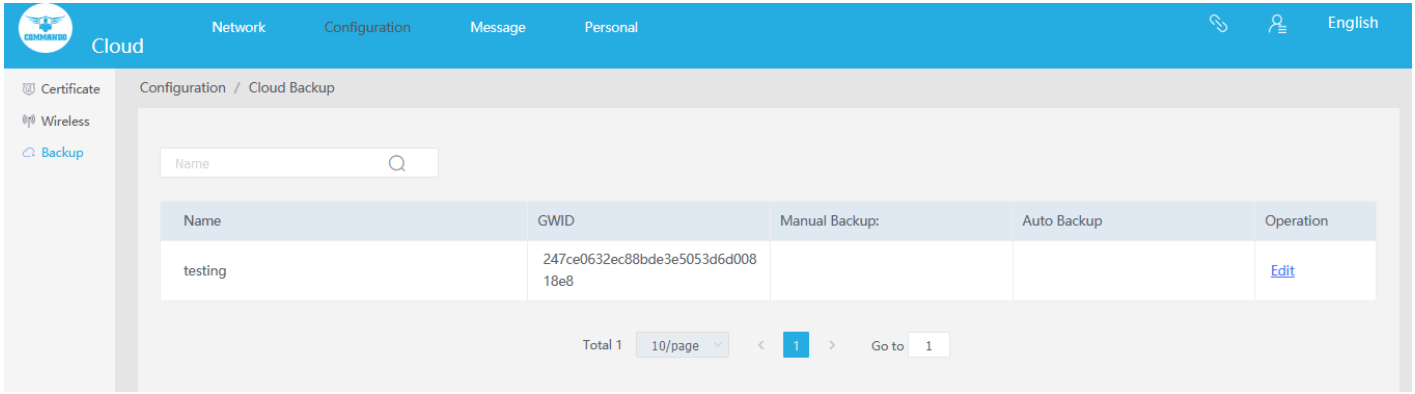
**Fig 12.3.7 Default Wireless Configuration Extended function setting page**



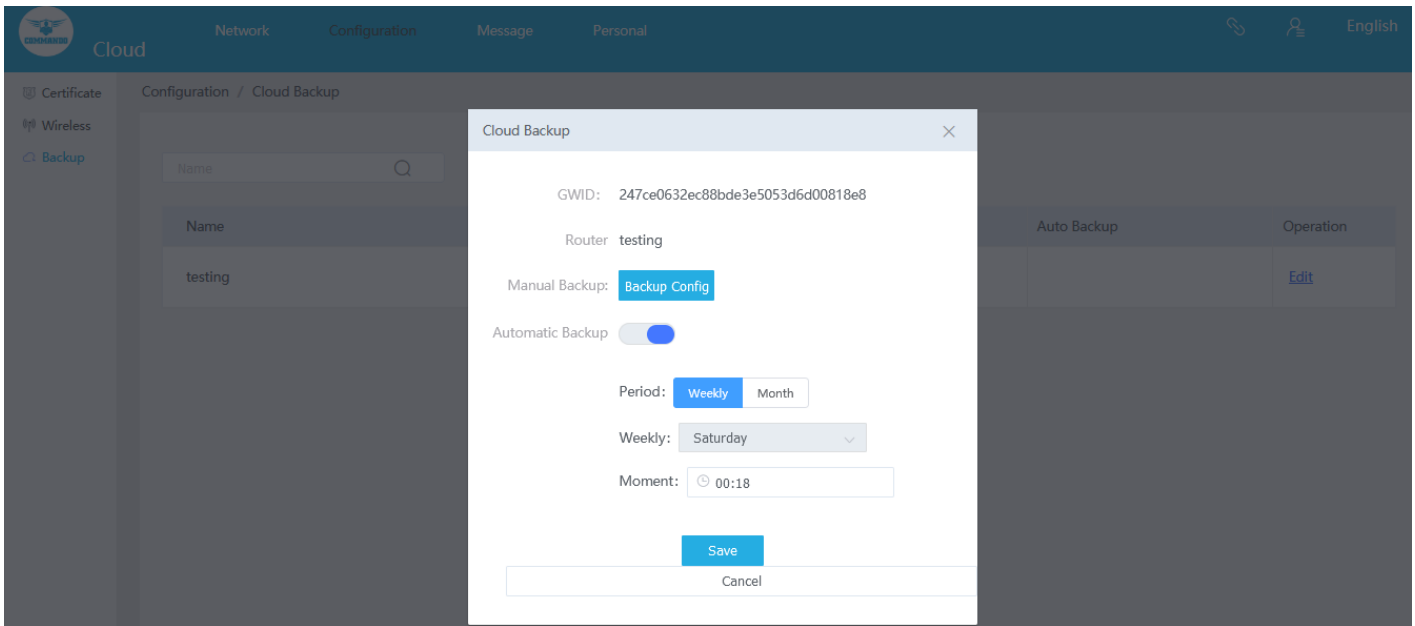
**Fig 12.3.8 Wireless Configuration Extended function for Plan 1 setting page**



**Fig 12.3.9 Default Configuration backup setting page**



**Fig 12.3.10 Backup Configuration setting page**



**Fig 12.3.11 Cloud Backup Configuration setting page**

## 12.4 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 12.4.1 Default Login and Logout page**

Action	IP	Time
No Data		

Total 0   10/page   < 1 >   Go to 1

**Fig 12.4.2 Default Upgrade and Restart page**

Action	IP	Time
No Data		

Total 0   10/page   < 1 >   Go to 1

**Fig 12.4.3 Default Configuration and operation page**

The screenshot displays the 'Configuration / Operation' page in a cloud management interface. At the top, there are navigation tabs for 'Login / logout', 'Upgrade / Restart', and 'Configuration / Operation'. A search bar with 'Start Date', 'To', 'End Date', and a 'Filter' button is present. Below this is a table with the following data:

Action	IP	Time
> Delete template successfully	10.172.128.196	2021-05-14 01:39:04
> Add template successfully	10.172.128.196	2021-05-14 01:35:10
> Open authentication	10.172.128.196	2021-05-13 22:53:02
> Close authentication	10.172.128.196	2020-11-17 19:21:59
> Open authentication	10.172.128.196	2020-11-17 19:02:25

At the bottom, there are pagination controls showing 'Total 5', '10/page', and 'Go to 1'.

**Fig 12.4.4 Configuration and operation page**

## 12.5 Personal

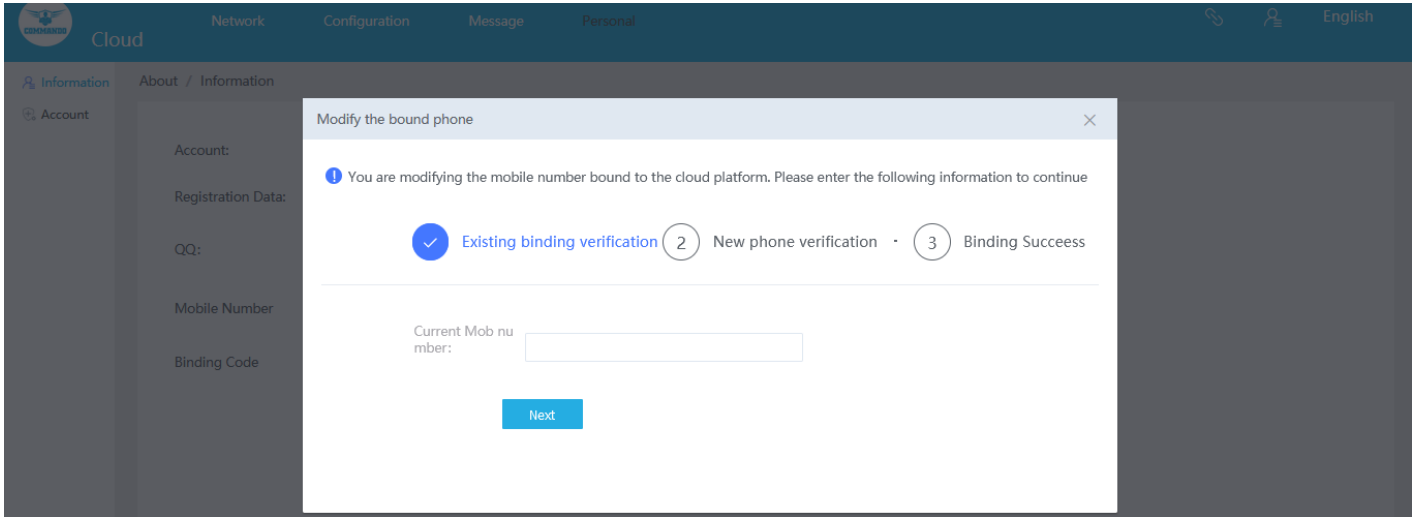
Personal Information is available on this page.

The screenshot shows the 'Personal Information' page with the following details:

- Registration Data: 2021-03-17 23:24:42
- QQ: [Modify]
- Mobile Number: 999\*\*\*\*9326 [Modify]
- Binding Code: 3a017d3d6be29db38ea82fd35789e567

**Fig 12.5.1 Default Personal Information page**





**Fig 12.5.2 Modify Personal Information page**