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 Could 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.

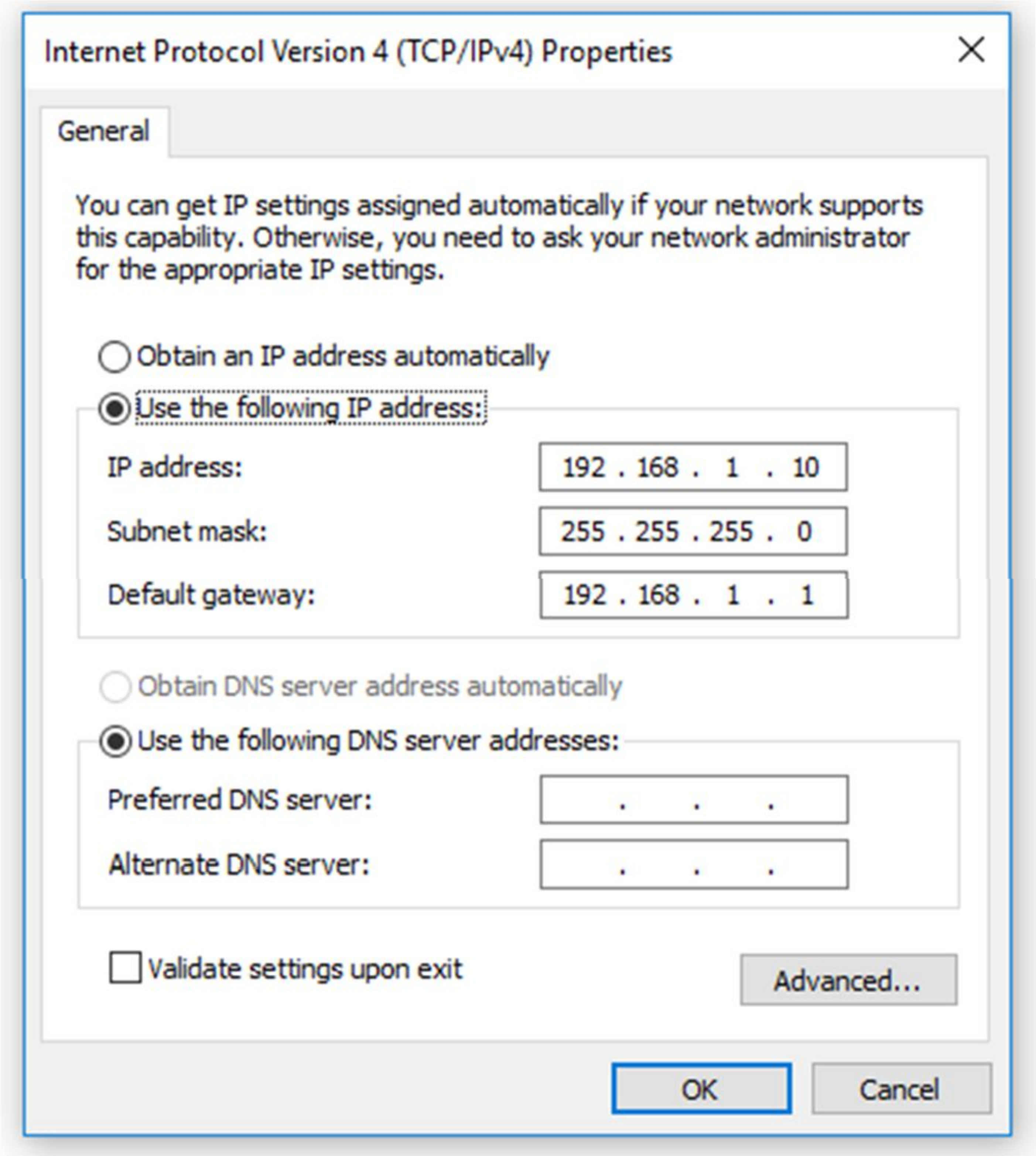
Built-in application identification server
Supports Layer 4 to Layer 7 application identification and can identify over 3200+ applications and application-based policy control technologies, including traffic blocking, traffic limit, and priority adjustment policies.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

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.

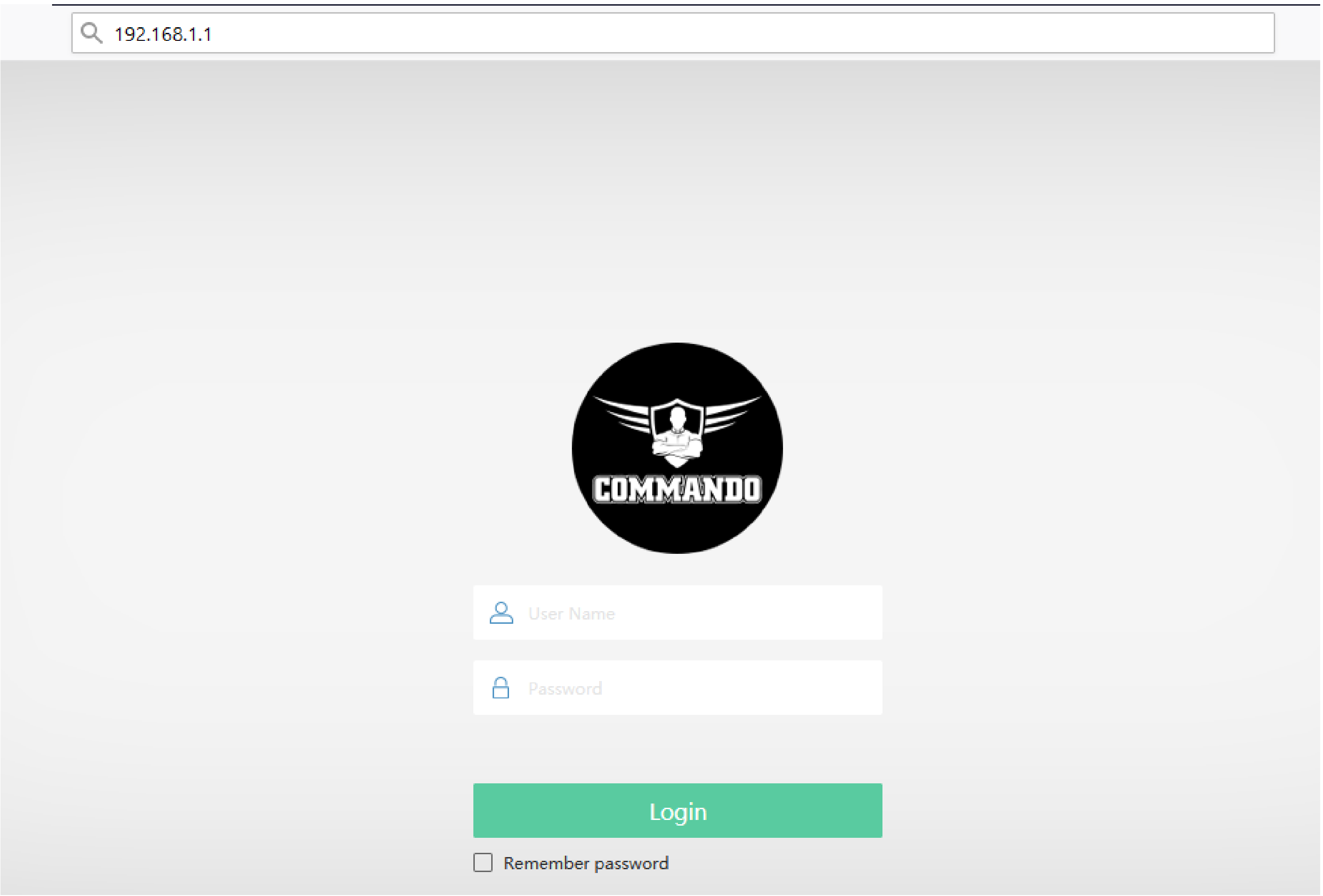
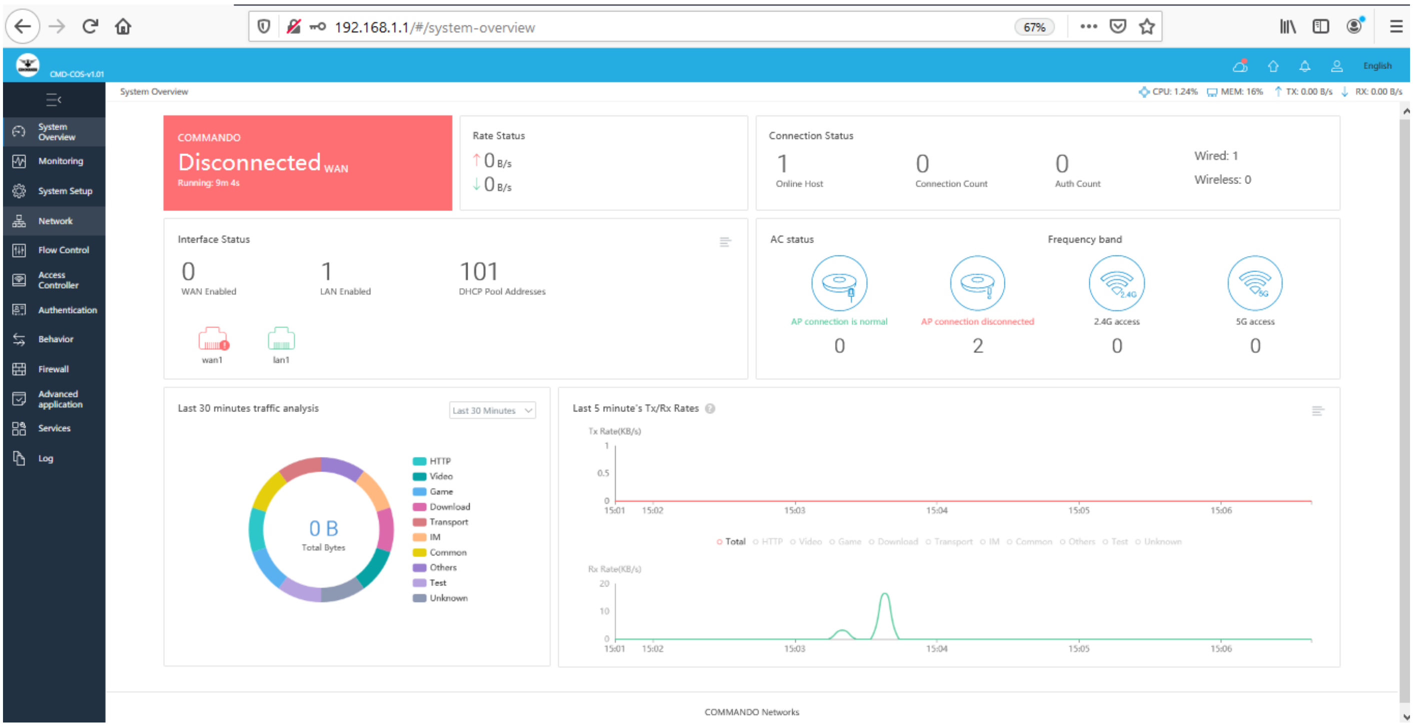


Fig 2. Login page for R100

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.



System Overview

CPU: 1.24% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

COMMANDO
Disconnected WAN
Running: 9m 4s

Rate Status
↑ 0 B/s
↓ 0 B/s

Connection Status
1 Online Host
0 Connection Count
0 Auth Count
Wired: 1
Wireless: 0

Interface Status
0 WAN Enabled
1 LAN Enabled
101 DHCP Pool Addresses
wan1 lan1

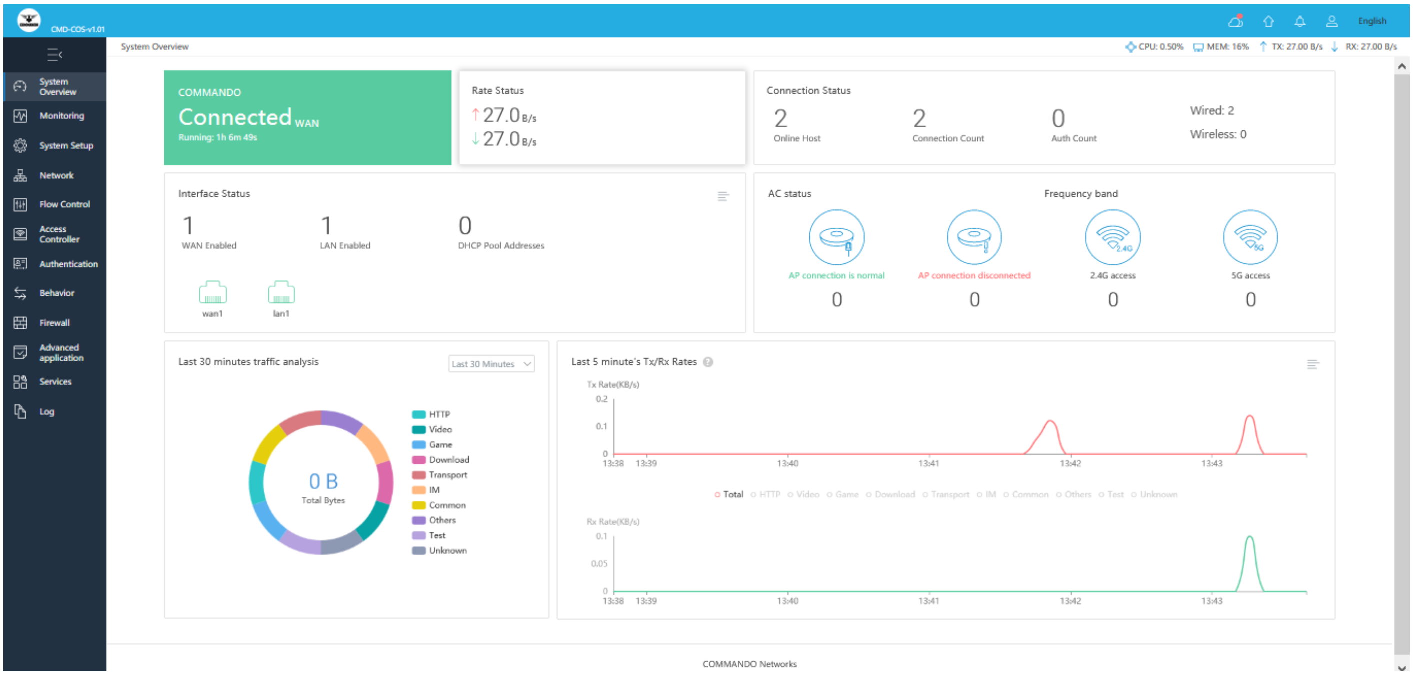
AC status
AP connection is normal: 0
AP connection disconnected: 2

Frequency band
2.4G access: 0
5G access: 0

Last 30 minutes traffic analysis
0 B Total Bytes

Last 5 minute's Tx/Rx Rates

Fig 3. Default System Overview page



System Overview

CPU: 0.50% MEM: 16% TX: 27.00 B/s RX: 27.00 B/s

COMMANDO
Connected WAN
Running: 1h 6m 49s

Rate Status
↑ 27.0 B/s
↓ 27.0 B/s

Connection Status
2 Online Host
2 Connection Count
0 Auth Count
Wired: 2
Wireless: 0

Interface Status
1 WAN Enabled
1 LAN Enabled
0 DHCP Pool Addresses
wan1 lan1

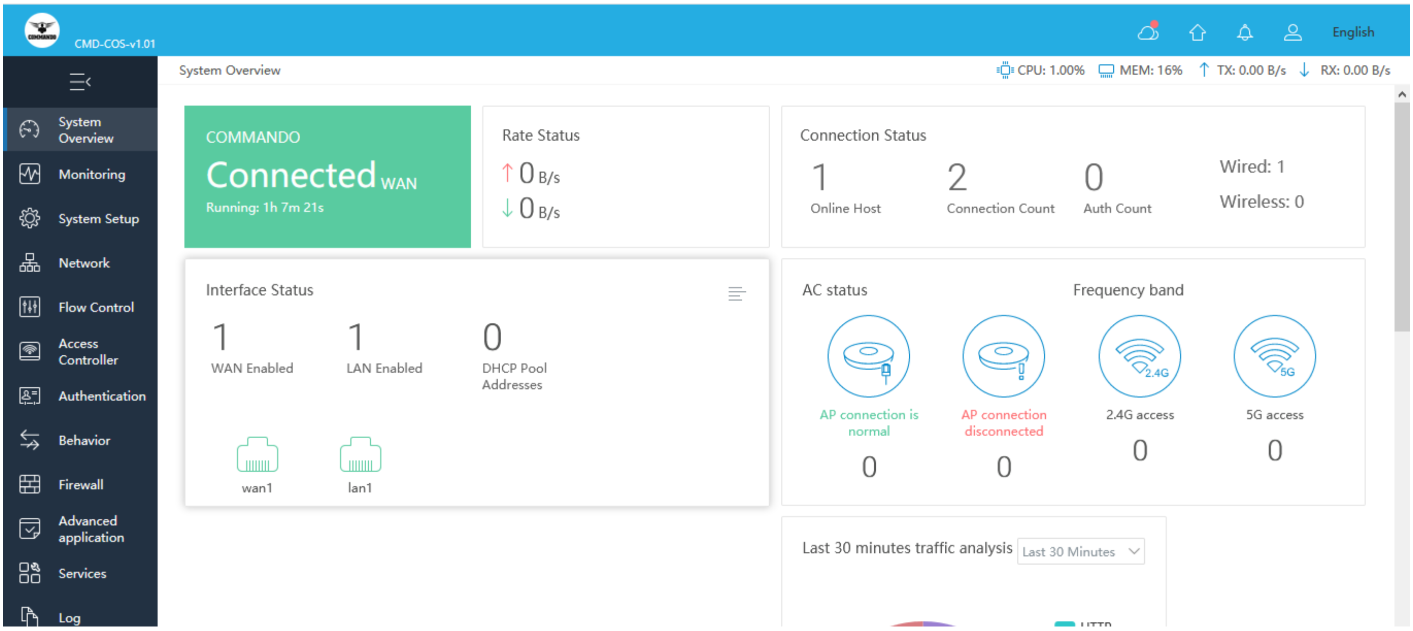
AC status
AP connection is normal: 0
AP connection disconnected: 0

Frequency band
2.4G access: 0
5G access: 0

Last 30 minutes traffic analysis
0 B Total Bytes

Last 5 minute's Tx/Rx Rates

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



System Overview

CPU: 1.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

COMMANDO
Connected WAN
Running: 1h 7m 21s

Rate Status
↑ 0 B/s
↓ 0 B/s

Connection Status
1 Online Host
2 Connection Count
0 Auth Count
Wired: 1
Wireless: 0

Interface Status
1 WAN Enabled
1 LAN Enabled
0 DHCP Pool Addresses
wan1
lan1

AC status
AP connection is normal 0
AP connection disconnected 0

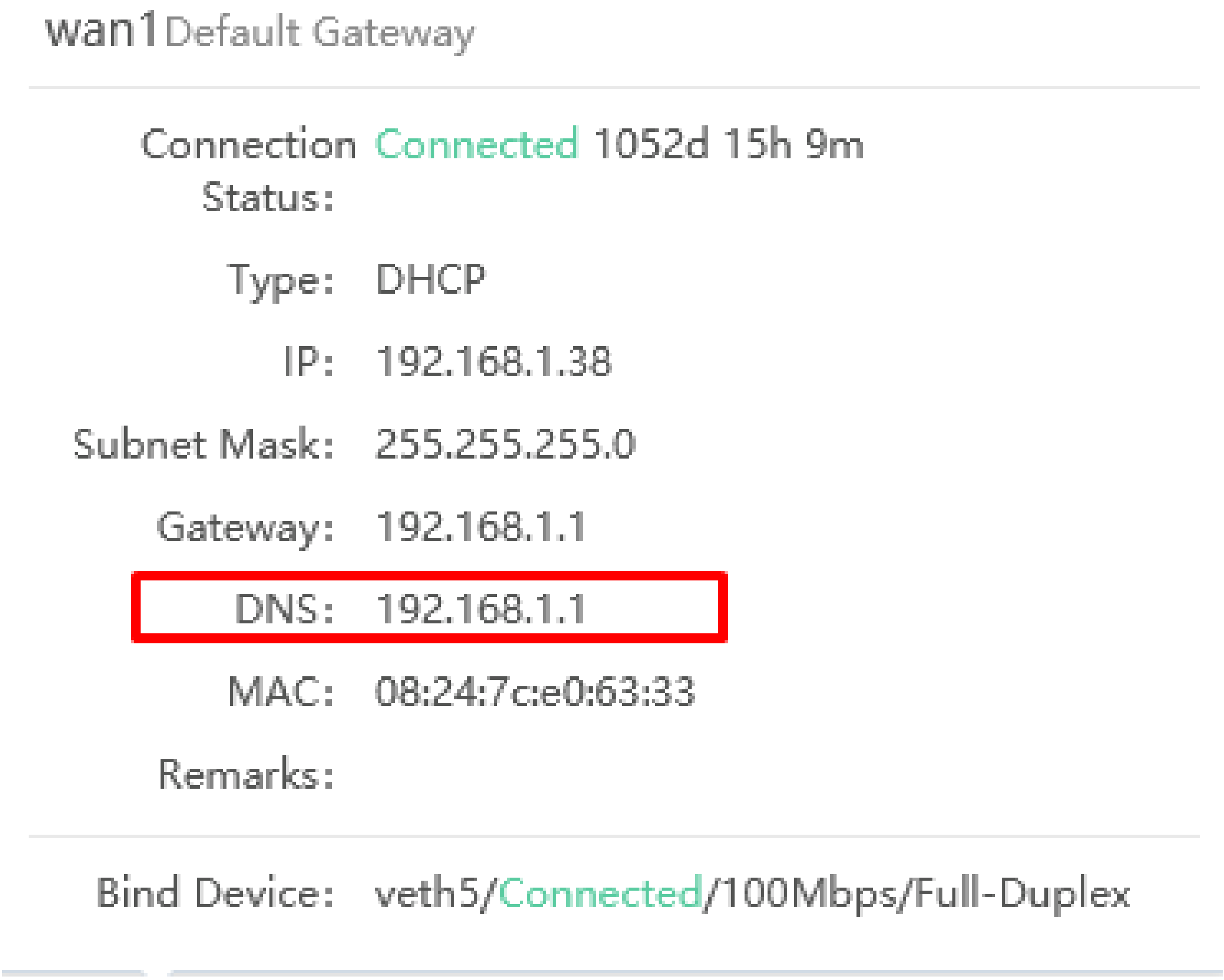
Frequency band
2.4G access 0
5G access 0

Last 30 minutes traffic analysis

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 Status: Connected 1052d 15h 9m

Type: DHCP

IP: 192.168.1.38

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 192.168.1.1

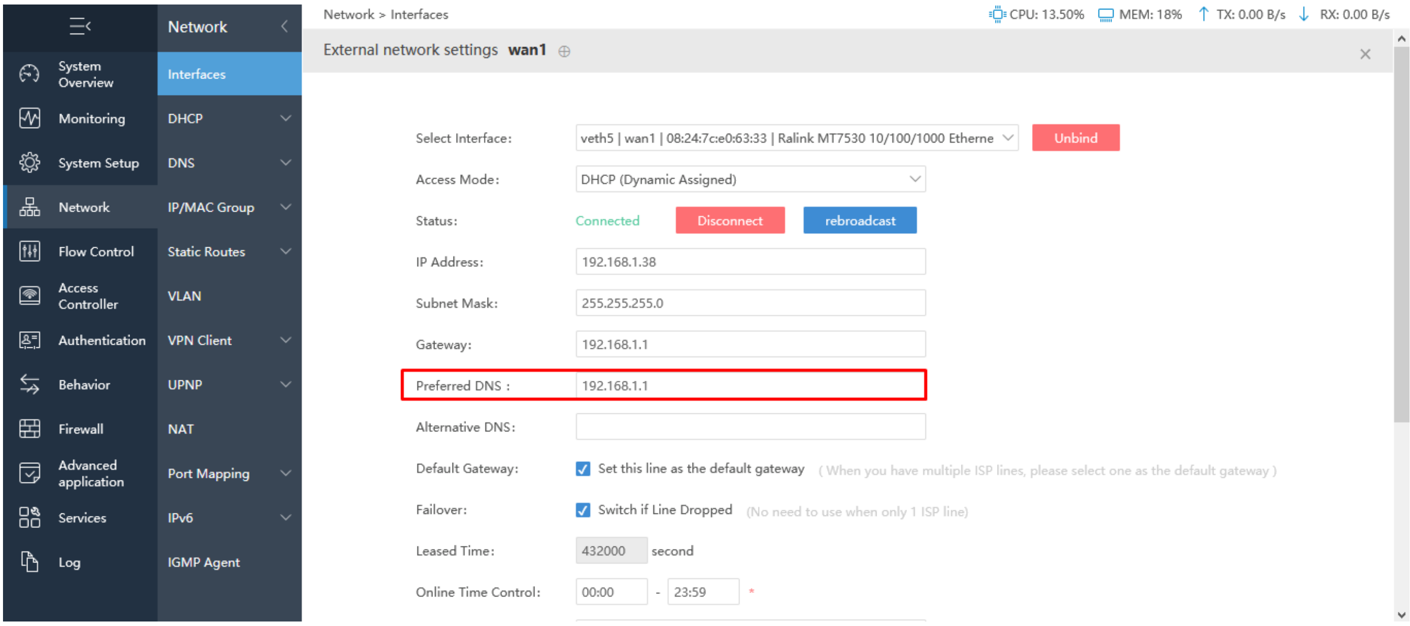
MAC: 08:24:7c:e0:63:33

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.



Network > Interfaces

CPU: 13.50% MEM: 18% TX: 0.00 B/s RX: 0.00 B/s

External network settings **wan1**

Select Interface: veth5 | wan1 | 08:24:7c:e0:63:33 | Ralink MT7530 10/100/1000 Etherne

Access Mode: DHCP (Dynamic Assigned)

Status: Connected

IP Address: 192.168.1.38

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Preferred DNS : 192.168.1.1

Alternative DNS:

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

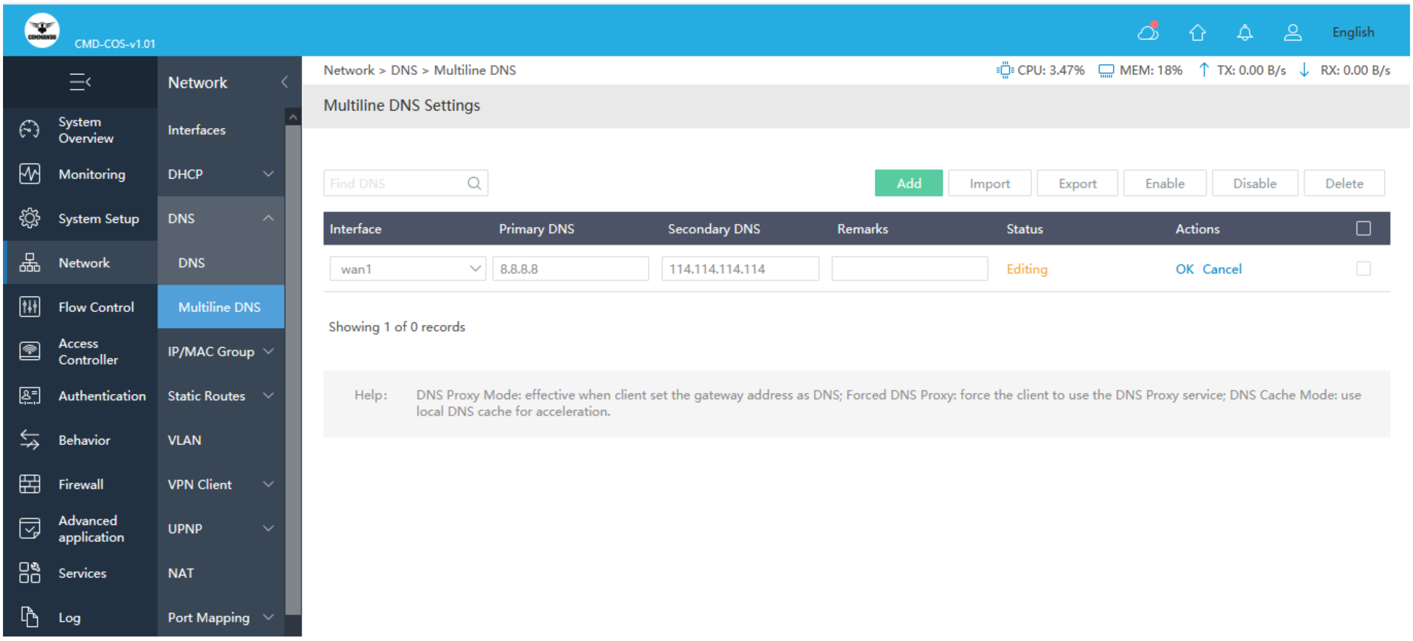
Failover: ☑ Switch if Line Dropped (No need to use when only 1 ISP line)

Leased Time: 432000 second

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

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



Network > DNS > Multiline DNS

CPU: 3.47% MEM: 18% TX: 0.00 B/s RX: 0.00 B/s

Multiline DNS Settings

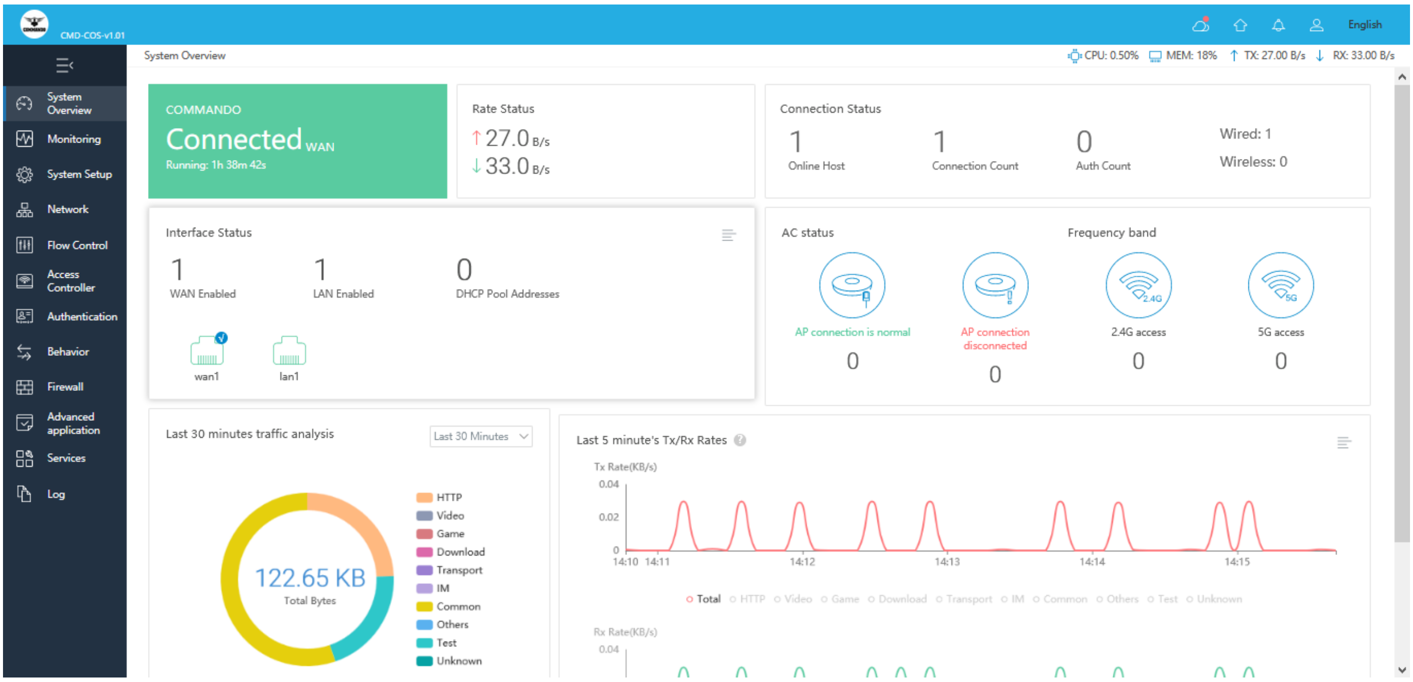
Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions	□
wan1	8.8.8.8	114.114.114.114		Editing	OK Cancel	□

Showing 1 of 0 records

Help: DNS Proxy Mode: effective when client set the gateway address as DNS; Forced DNS Proxy: force the client to use the DNS Proxy service; DNS Cache Mode: use local DNS cache for acceleration.

Fig 8. Multi DNS server Setting in R100.

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



System Overview

CPU: 0.50% MEM: 18% TX: 27.00 B/s RX: 33.00 B/s

COMMANDO
Connected WAN
Running: 1h 38m 42s

Rate Status
↑27.0 B/s
↓33.0 B/s

Connection Status
1 Online Host
1 Connection Count
0 Auth Count
Wired: 1
Wireless: 0

Interface Status
1 WAN Enabled
1 LAN Enabled
0 DHCP Pool Addresses
wan1 lan1

AC status
AP connection is normal 0
AP connection disconnected 0

Frequency band
2.4G access 0
5G access 0

Last 30 minutes traffic analysis
122.65 KB
Total Bytes
HTTP
Video
Game
Download
Transport
IM
Common
Others
Test
Unknown

Last 5 minute's Tx/Rx Rates

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

Traffic Analysis

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

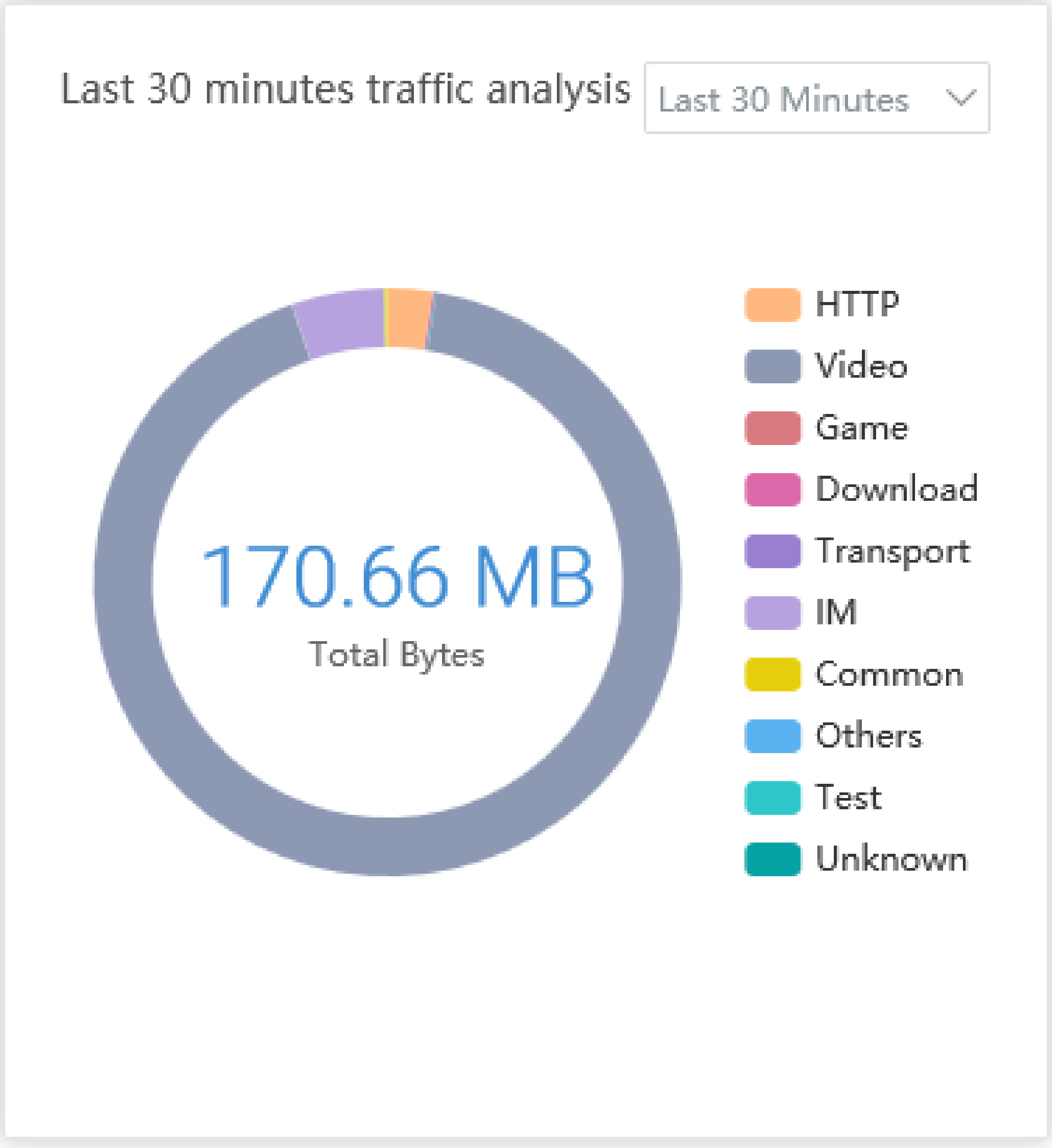
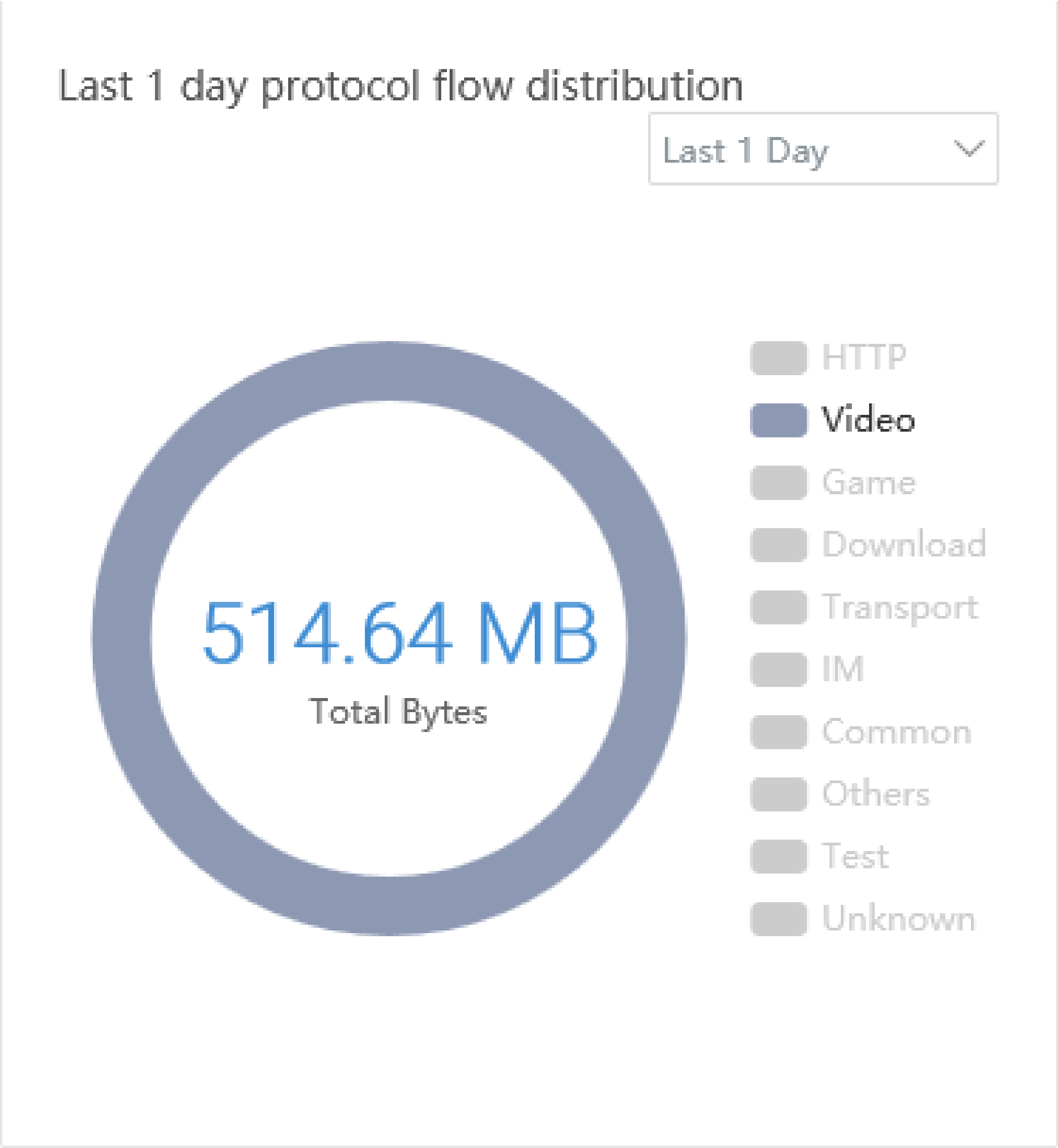


Fig 10. Traffic analysis for all application from last 30 minutes.



Last 1 day protocol flow distribution

Last 1 Day

514.64 MB

Total Bytes

Fig 11. Traffic analysis for video application for 1 day

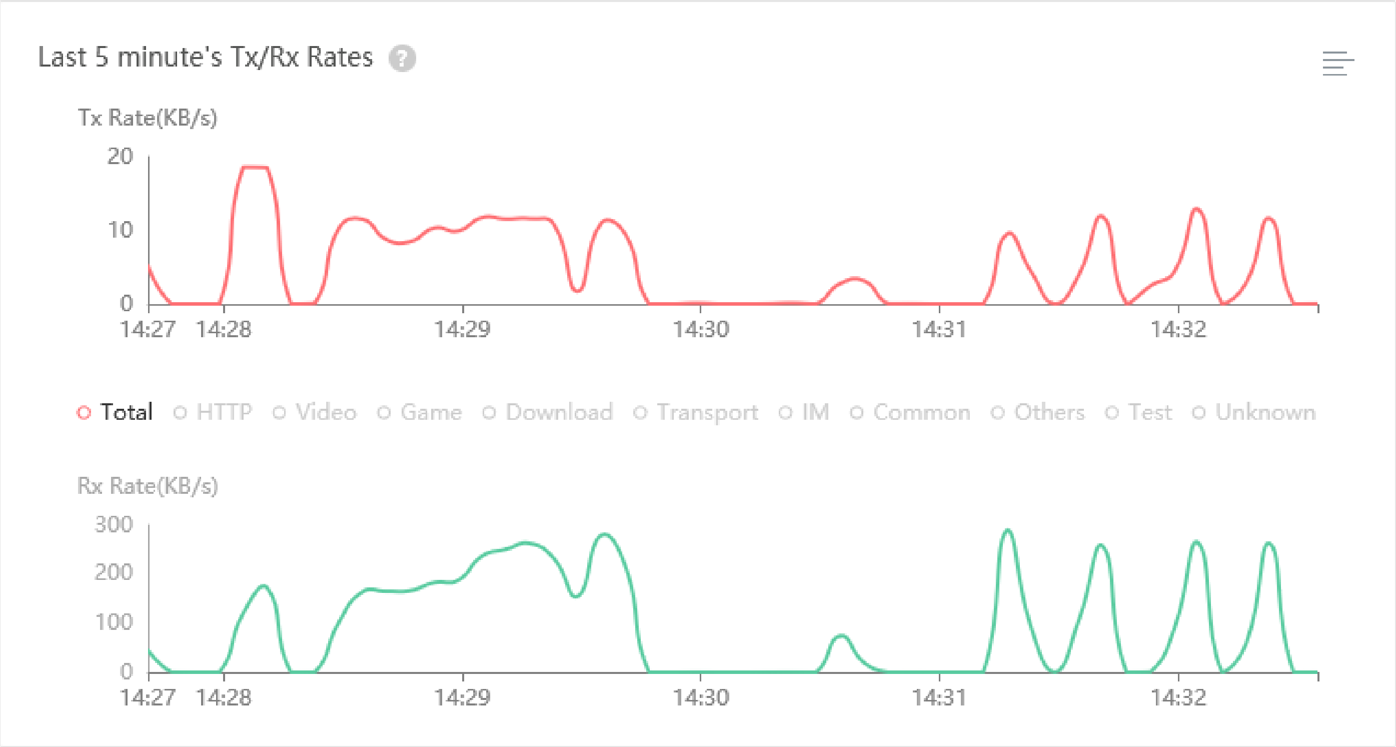
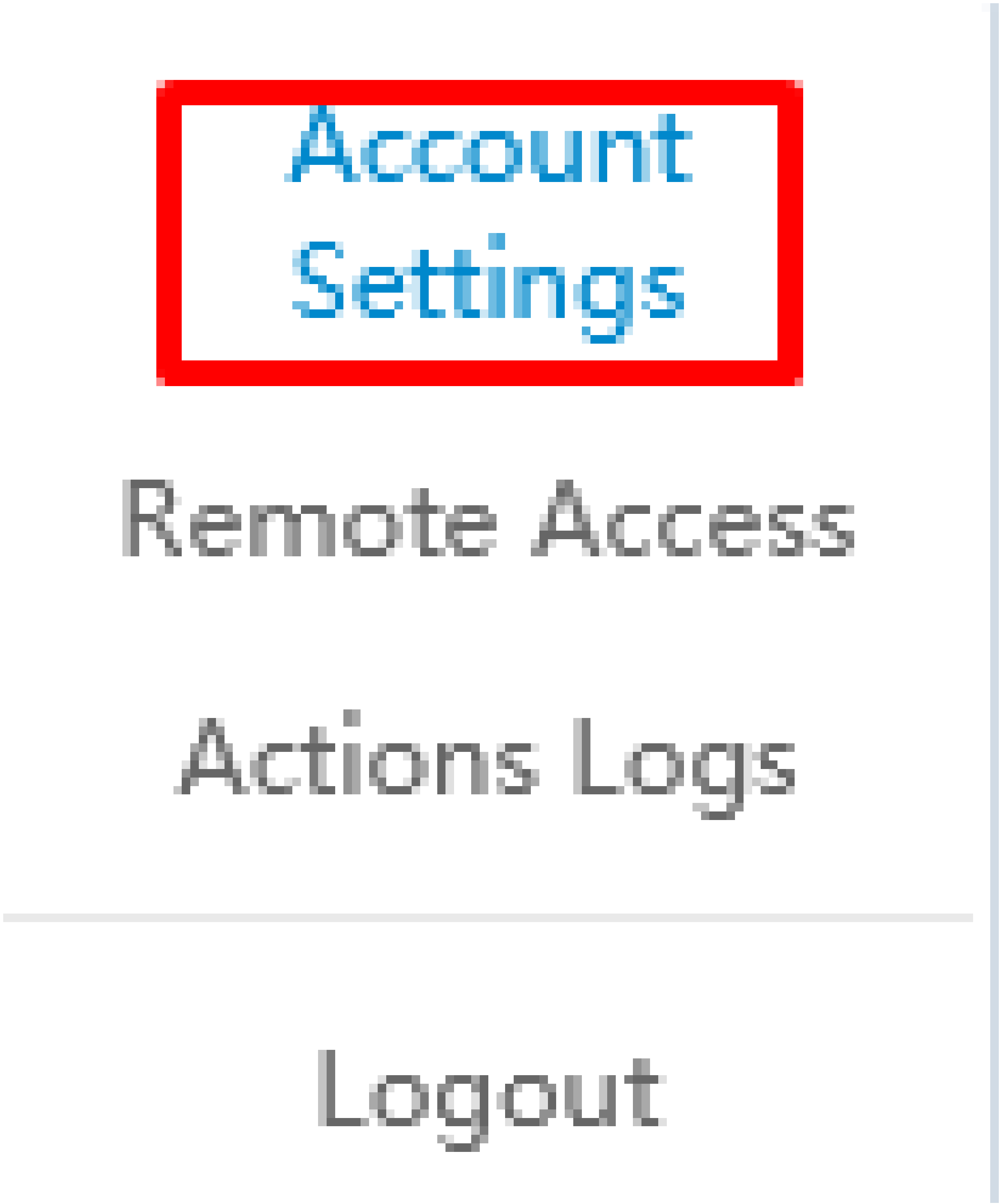


Fig 12. Transmission and Receiving Rate Graphs

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.



Account Settings

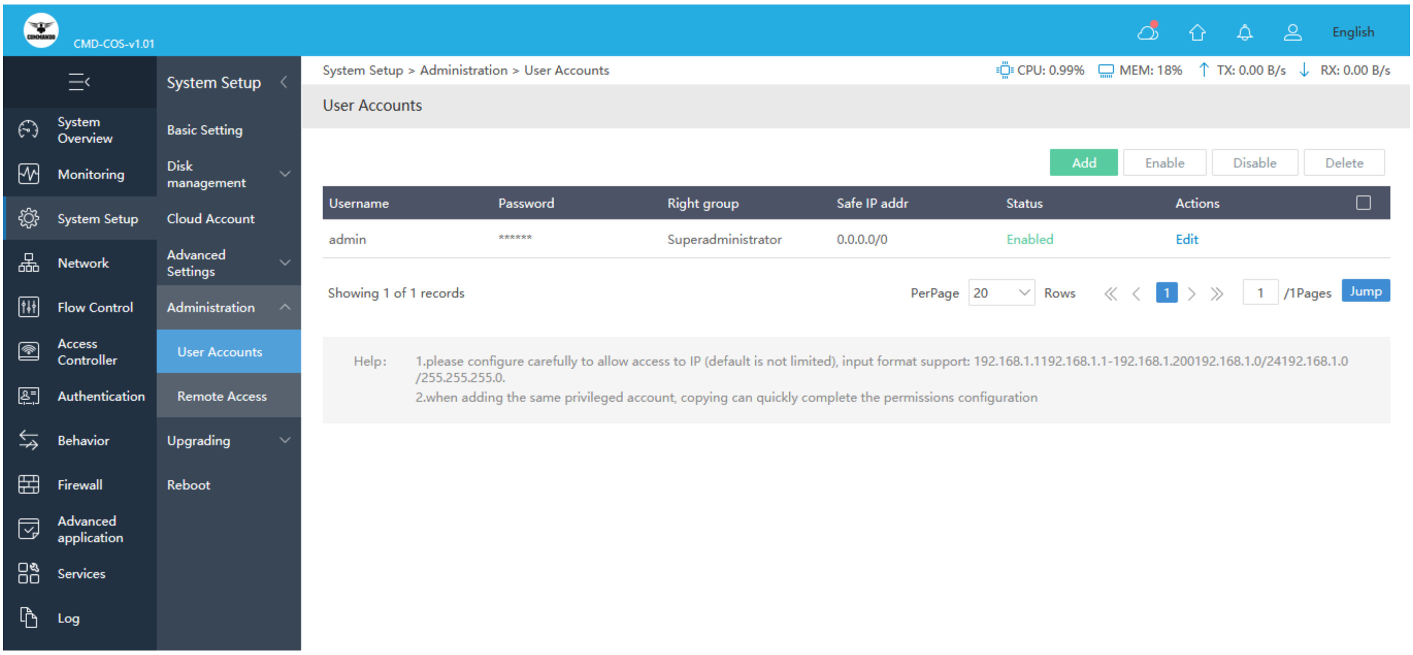
Remote Access

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



User Accounts

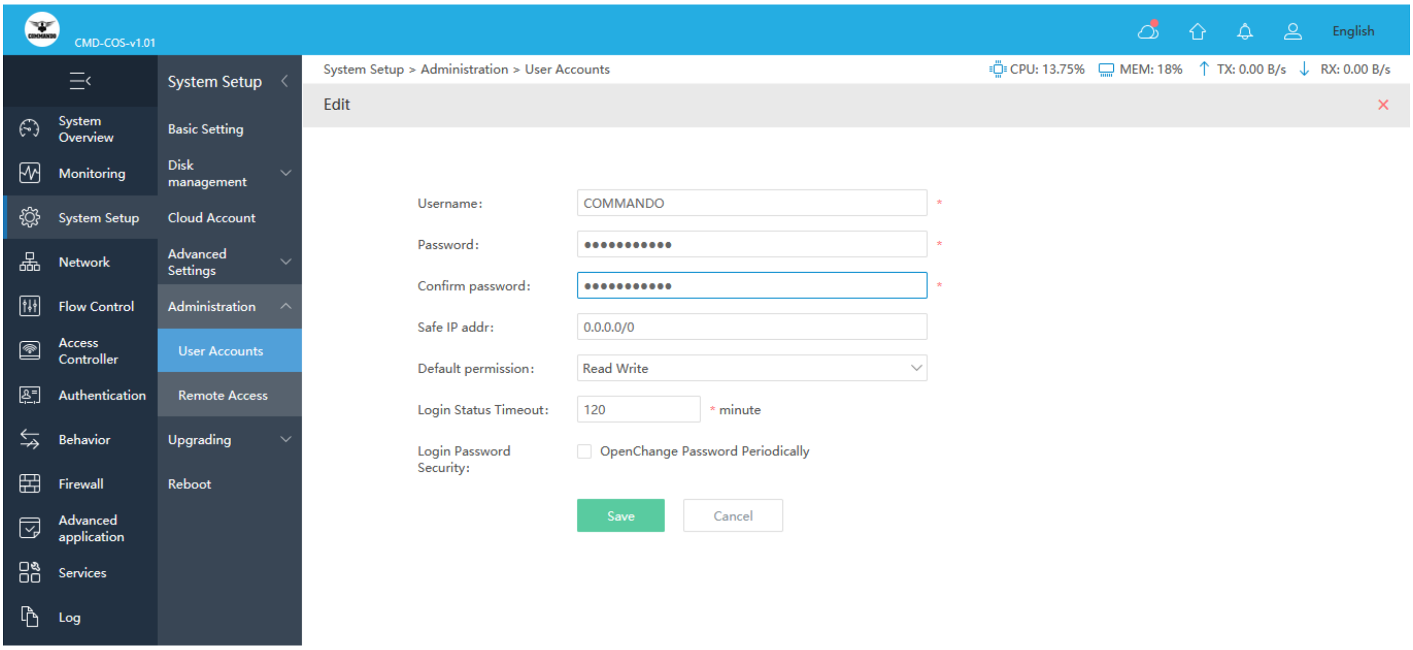
Username	Password	Right group	Safe IP addr	Status	Actions	□
admin	******	Superadministrator	0.0.0.0/0	Enabled	Edit	

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

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 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.



Edit

Username: COMMANDO *

Password: ●●●●●●●●●●● *

Confirm password: ●●●●●●●●●●● *

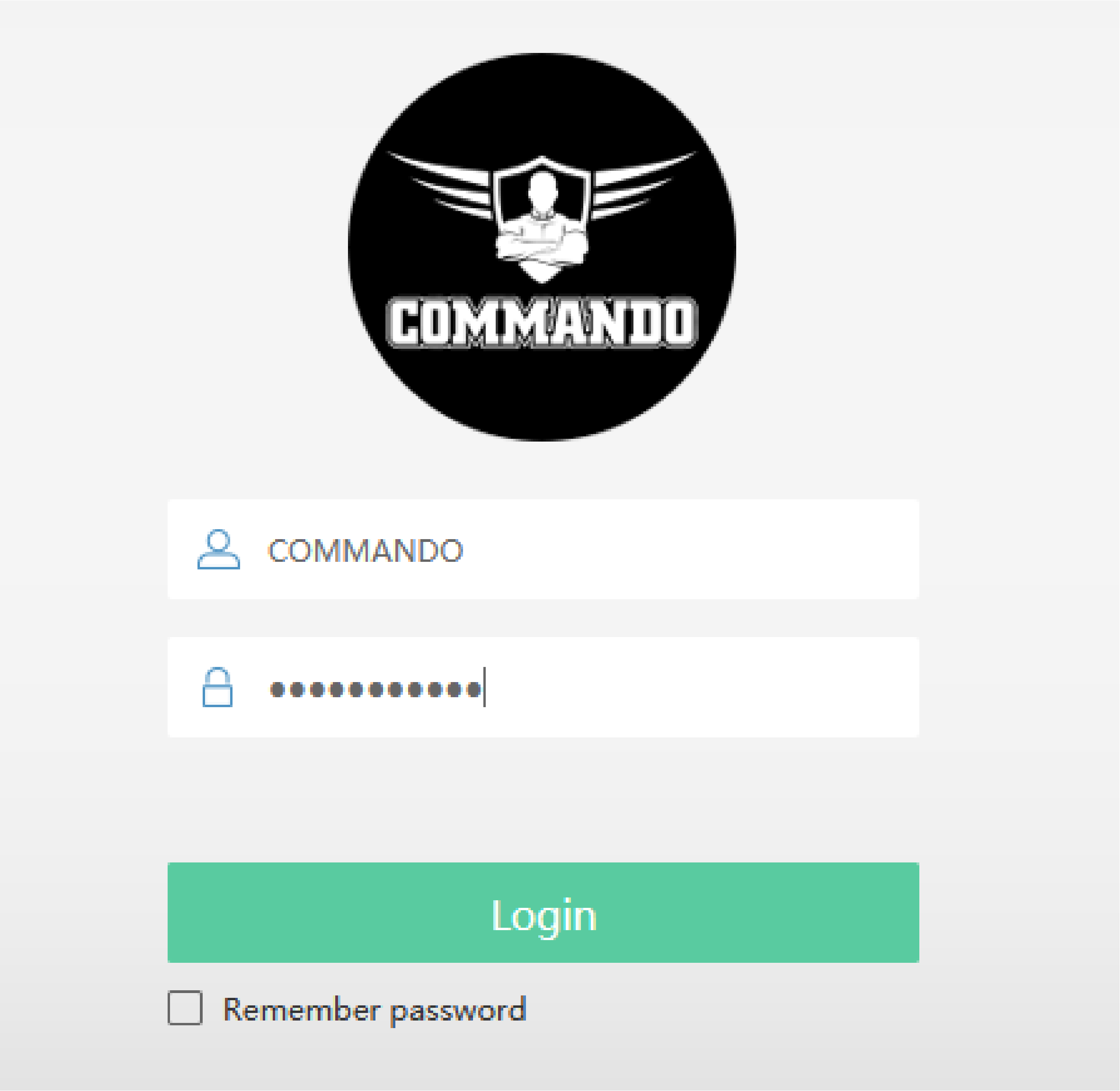
Safe IP addr: 0.0.0.0/0

Default permission: Read Write

Login Status Timeout: 120 * minute

Login Password Security: □ OpenChange Password Periodically

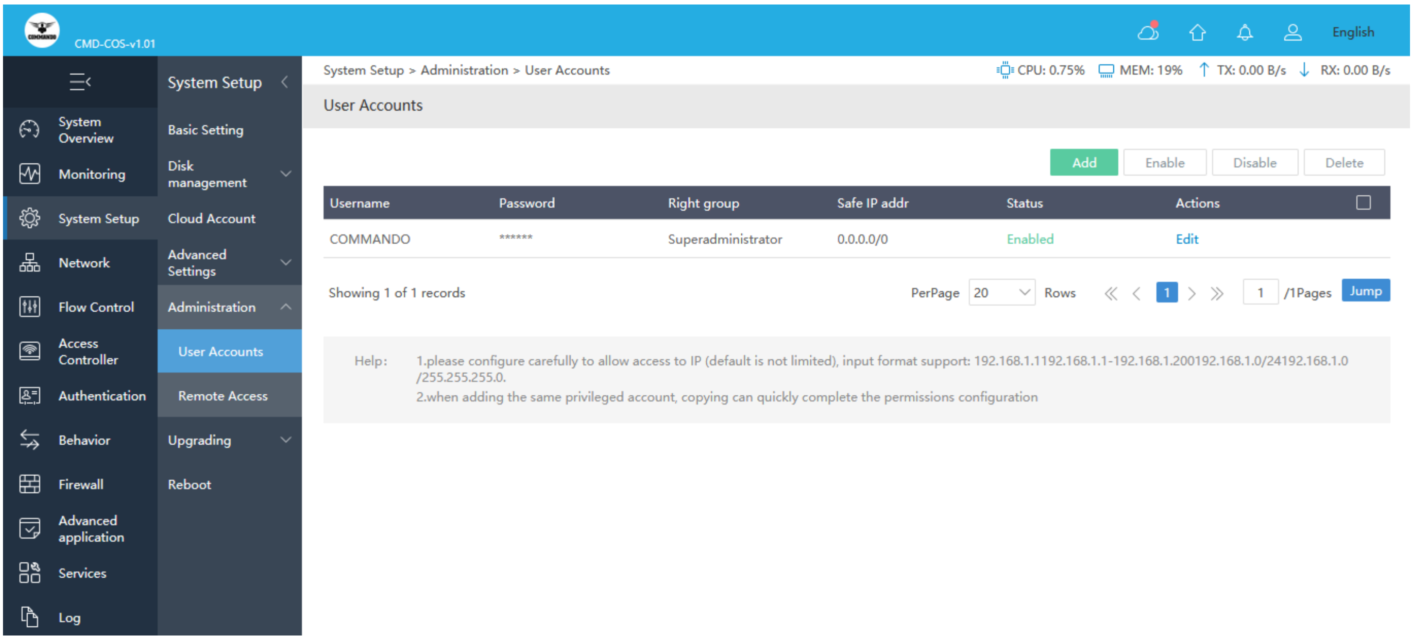
Fig 15. Editing User Account setting



COMMANDO

●●●●●●●●●●●

Fig 16. Logging with New account



User Accounts

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 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.

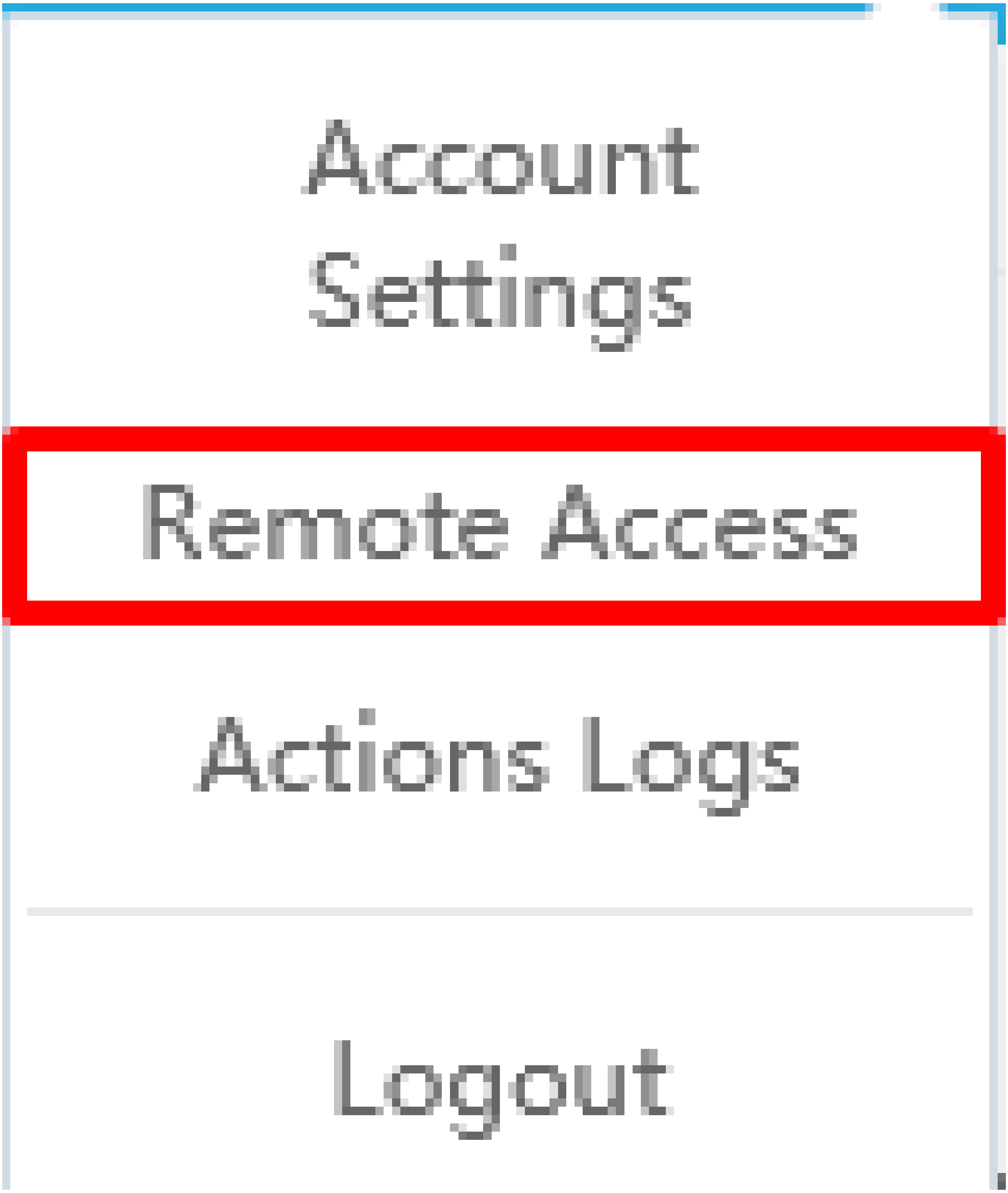
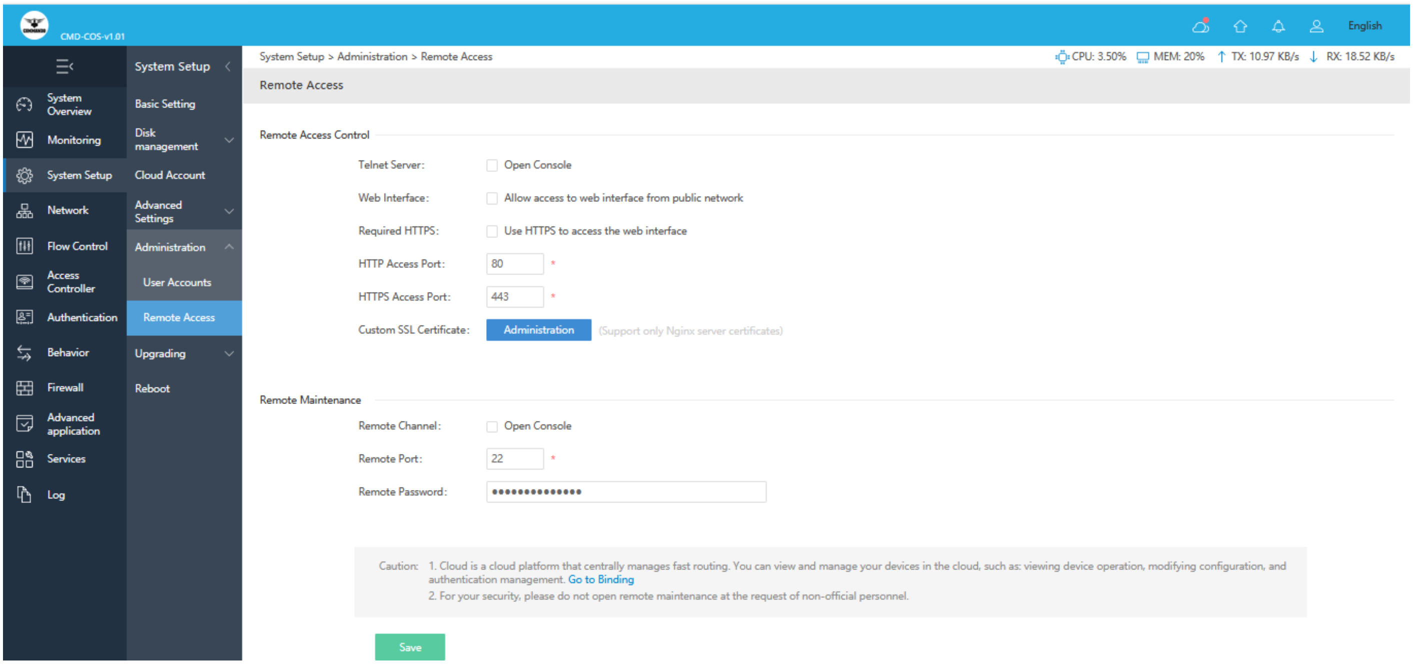


Fig 18. Remote access shortcut

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



System Setup > Administration > Remote Access

Remote Access

Remote Access Control

Telnet Server: □ Open Console

Web Interface: □ Allow access to web interface from public network

Required HTTPS: □ Use HTTPS to access the web interface

HTTP Access Port: 80 *

HTTPS Access Port: 443 *

Custom SSL Certificate: Administration (Support only Nginx server certificates)

Remote Maintenance

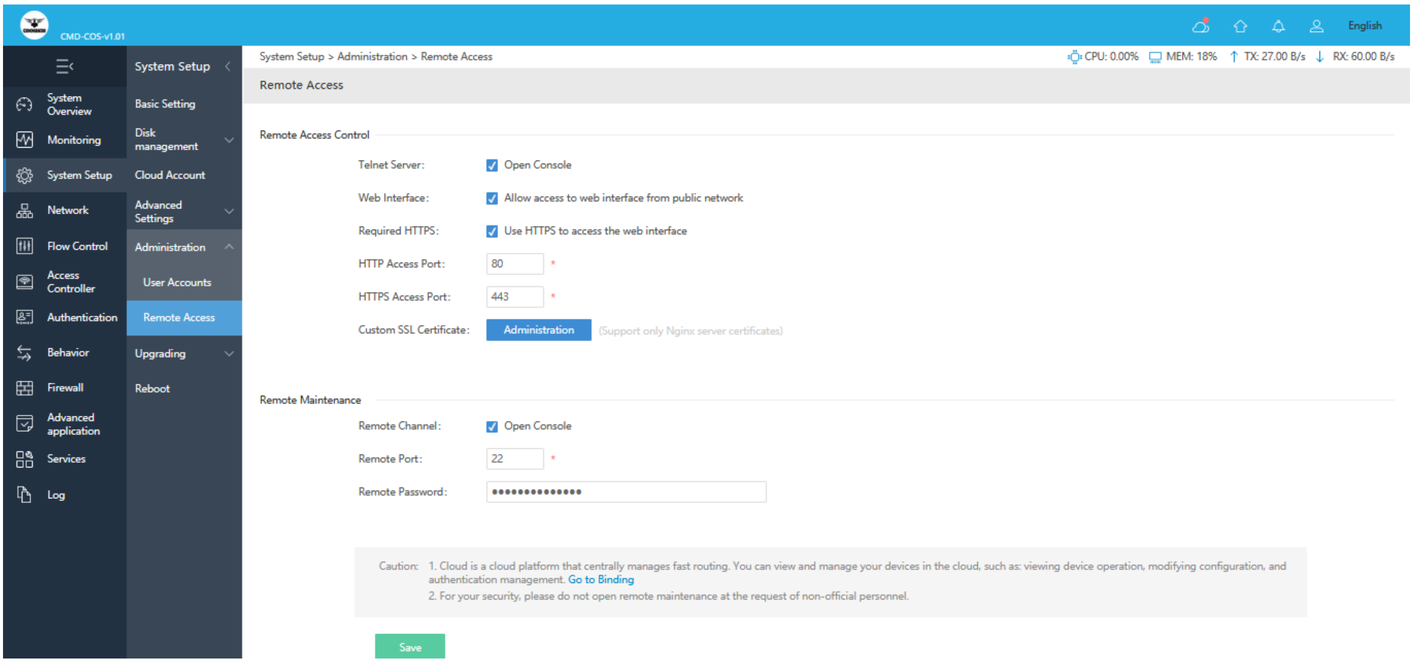
Remote Channel: □ Open Console

Remote Port: 22 *

Remote Password: ••••••••••••••

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 19. Default Remote access control.



System Setup > Administration > Remote Access

Remote Access

Remote Access Control

Telnet Server: ☑ Open Console

Web Interface: ☑ Allow access to web interface from public network

Required HTTPS: ☑ Use HTTPS to access the web interface

HTTP Access Port: 80 *

HTTPS Access Port: 443 *

Custom SSL Certificate: Administration (Support only Nginx server certificates)

Remote Maintenance

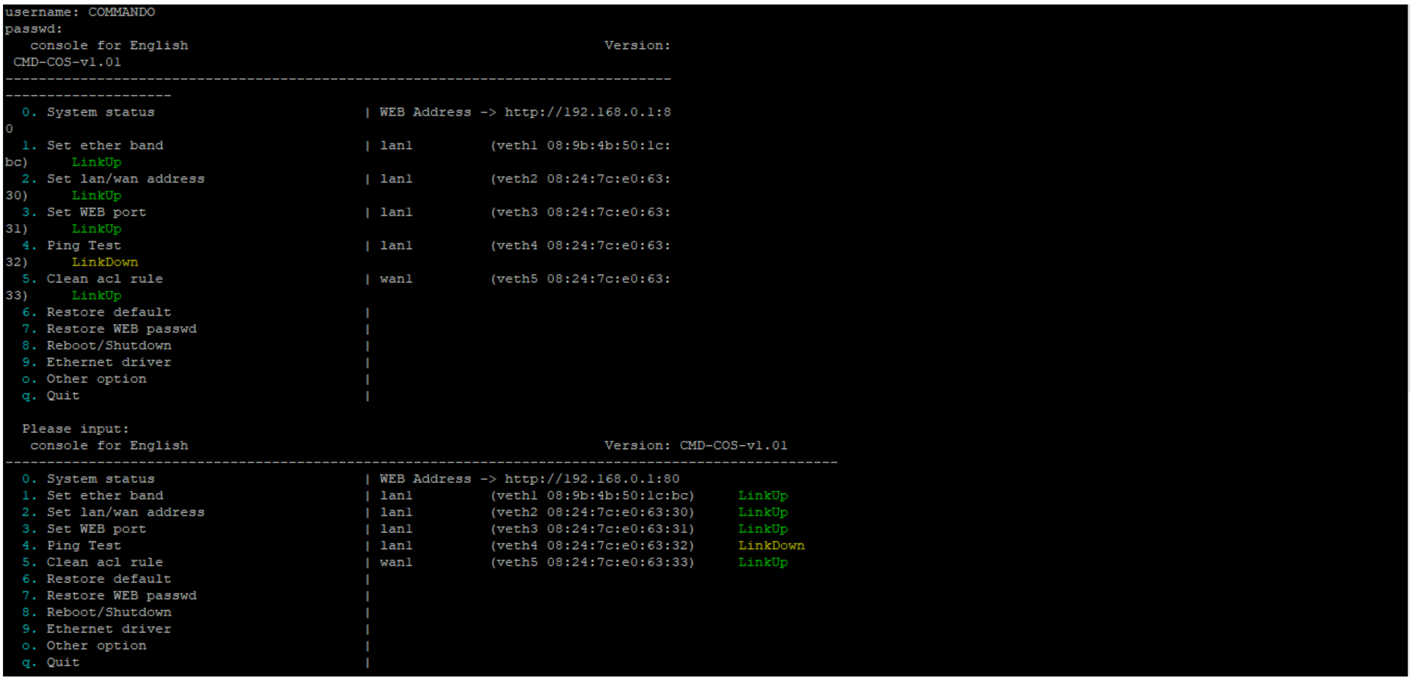
Remote Channel: ☑ Open Console

Remote Port: 22 *

Remote Password: ••••••••••••••

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 20. Changing Remote access control setting.

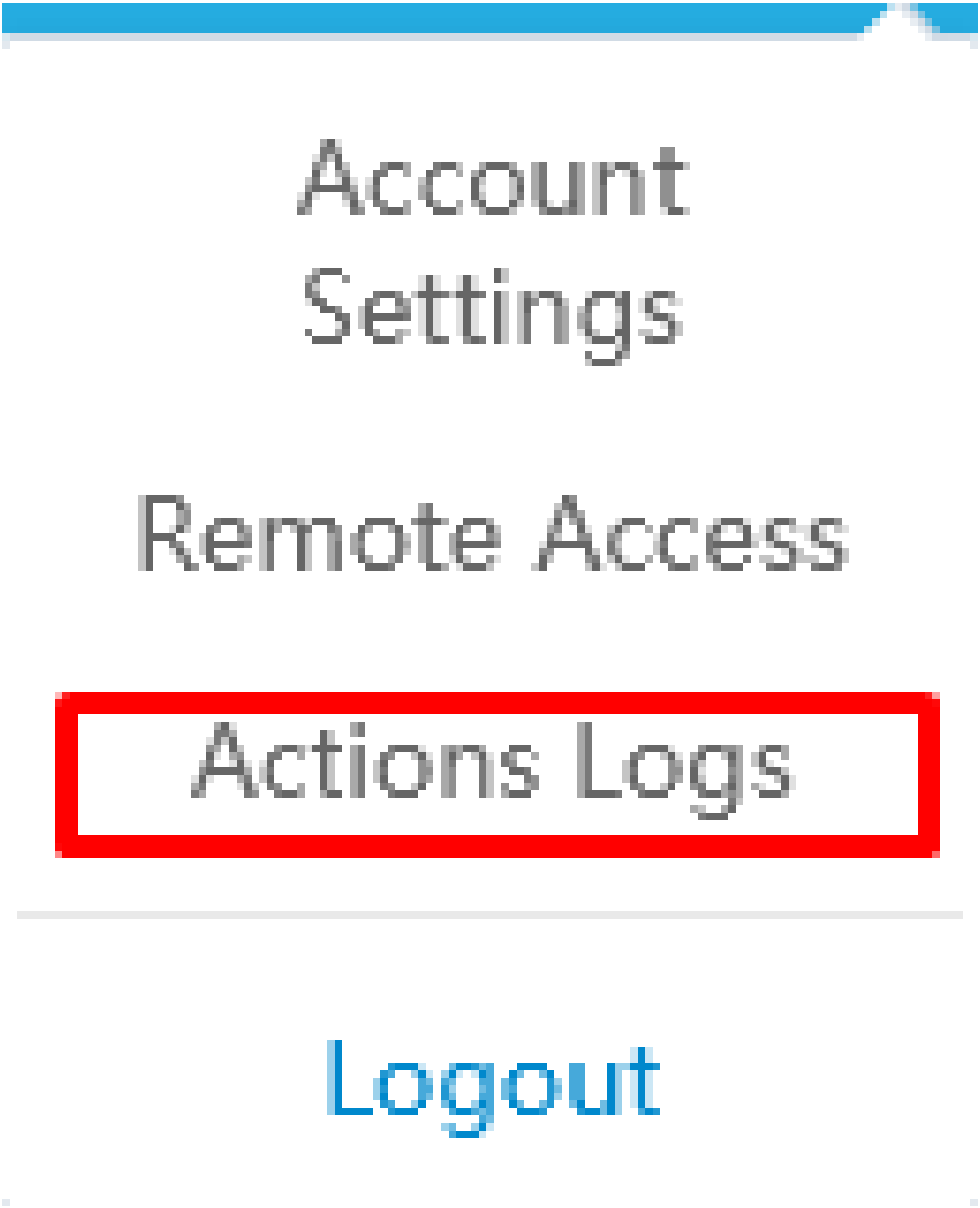


```
username: COMMANDO
passwd:
   console for English                                                  Version:
 CMD-COS-v1.01
--------------------------------------------------------------------------------
--------------------
  0. System status                         | WEB Address -> http://192.168.0.1:8
0
  1. Set ether band                        | lanl         (vethl 08:9b:4b:50:1c:
bc)      LinkUp
  2. Set lan/wan address                   | lanl         (veth2 08:24:7c:e0:63:
30)      LinkUp
  3. Set WEB port                          | lanl         (veth3 08:24:7c:e0:63:
31)      LinkUp
  4. Ping Test                             | lanl         (veth4 08:24:7c:e0:63:
32)      LinkDown
  5. Clean acl rule                        | wanl         (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                        | lanl         (vethl 08:9b:4b:50:1c:bc)     LinkUp
  2. Set lan/wan address                   | lanl         (veth2 08:24:7c:e0:63:30)     LinkUp
  3. Set WEB port                          | lanl         (veth3 08:24:7c:e0:63:31)     LinkUp
  4. Ping Test                             | lanl         (veth4 08:24:7c:e0:63:32)     LinkDown
  5. Clean acl rule                        | wanl         (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

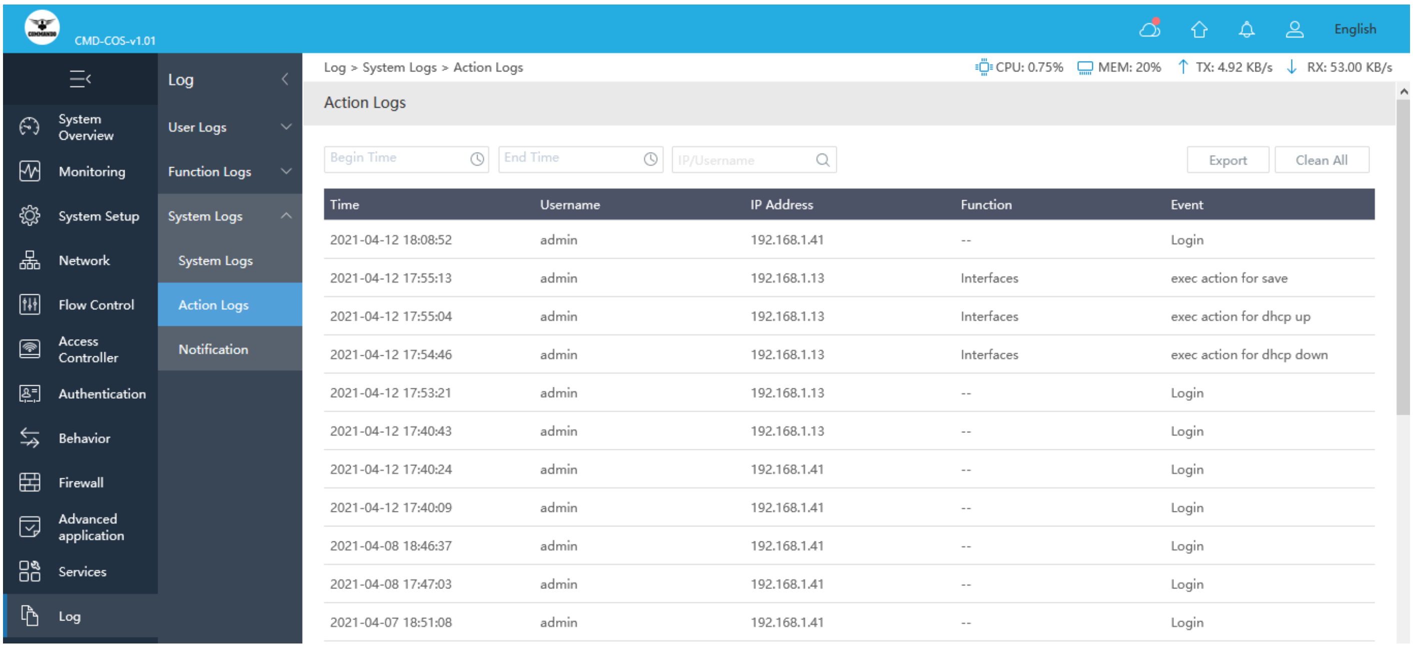
Remote Access

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

Action Logs

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.

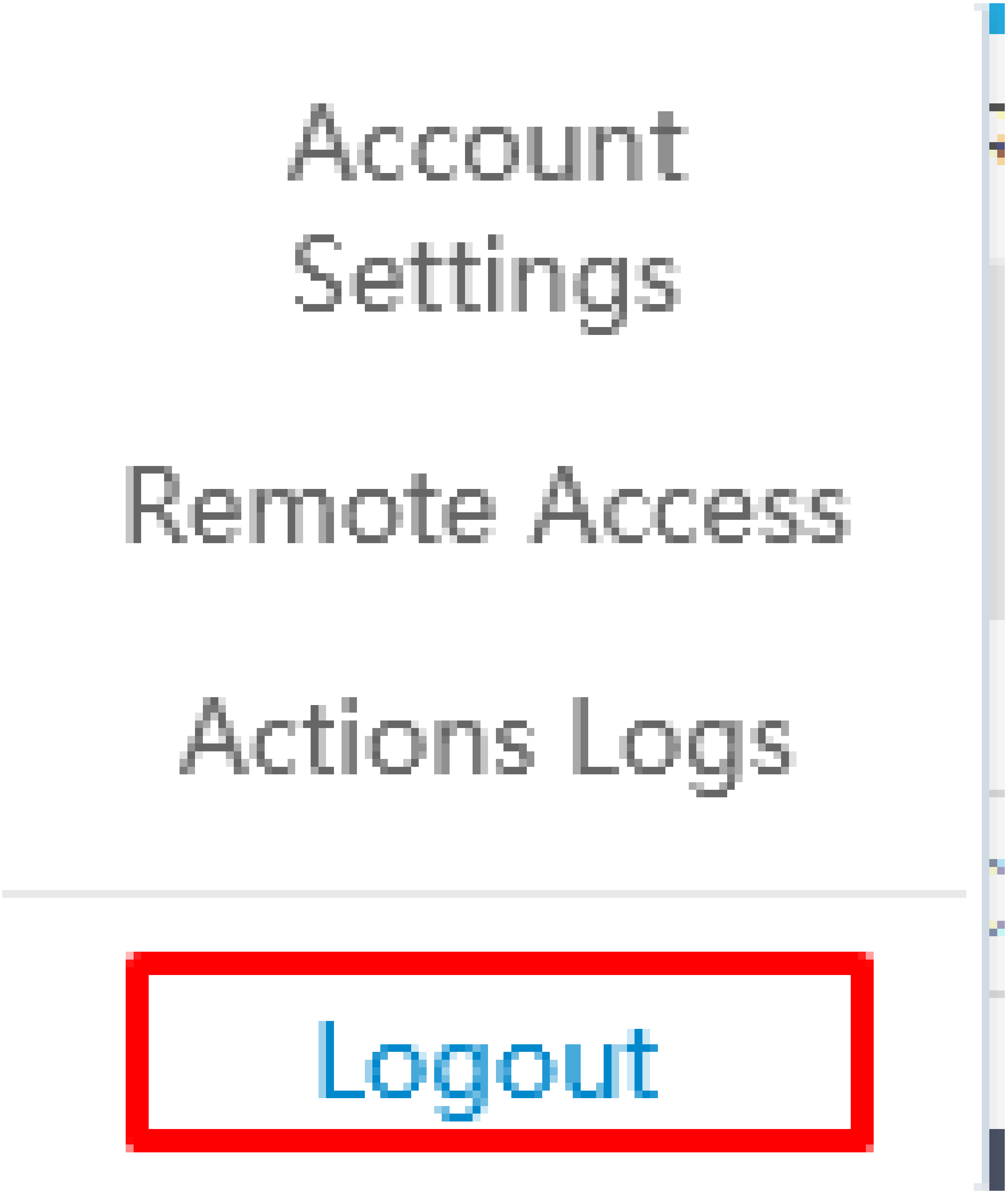


Fig 24. Logout shortcut

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

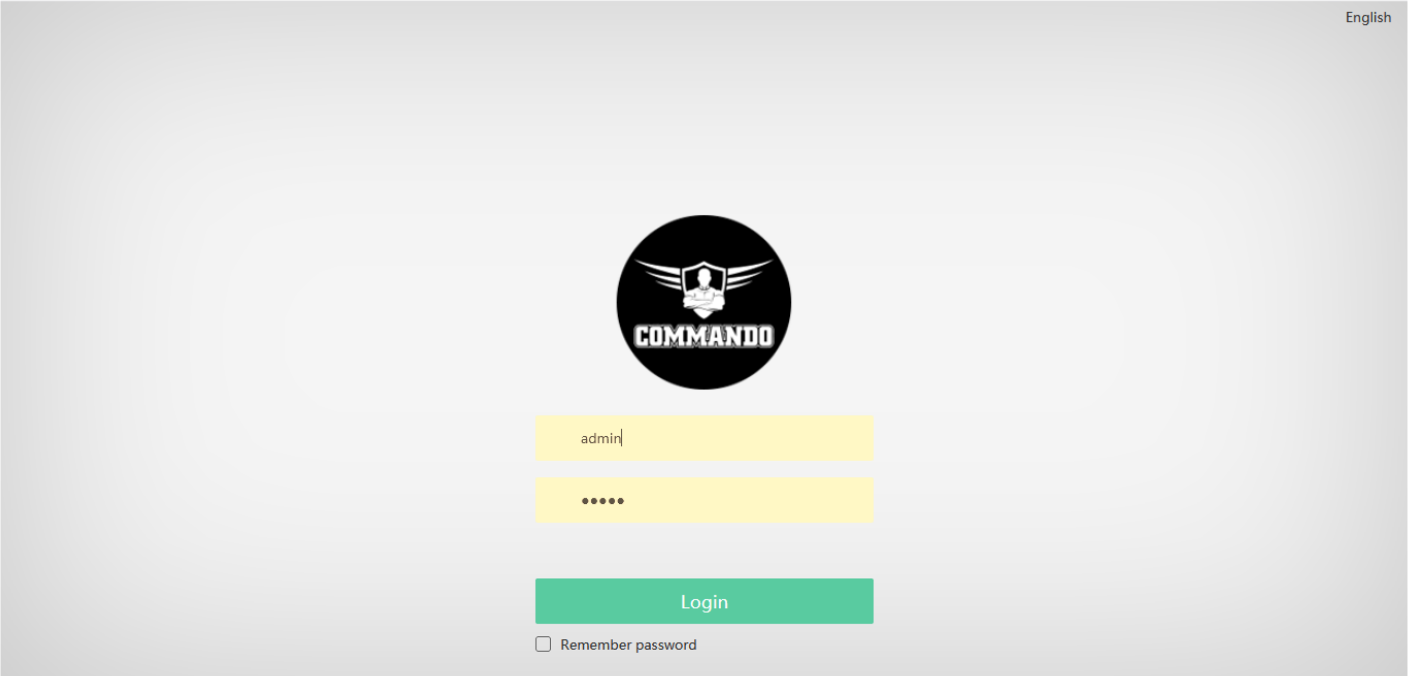


Fig 25. Login page after Logout

Message Notification:

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

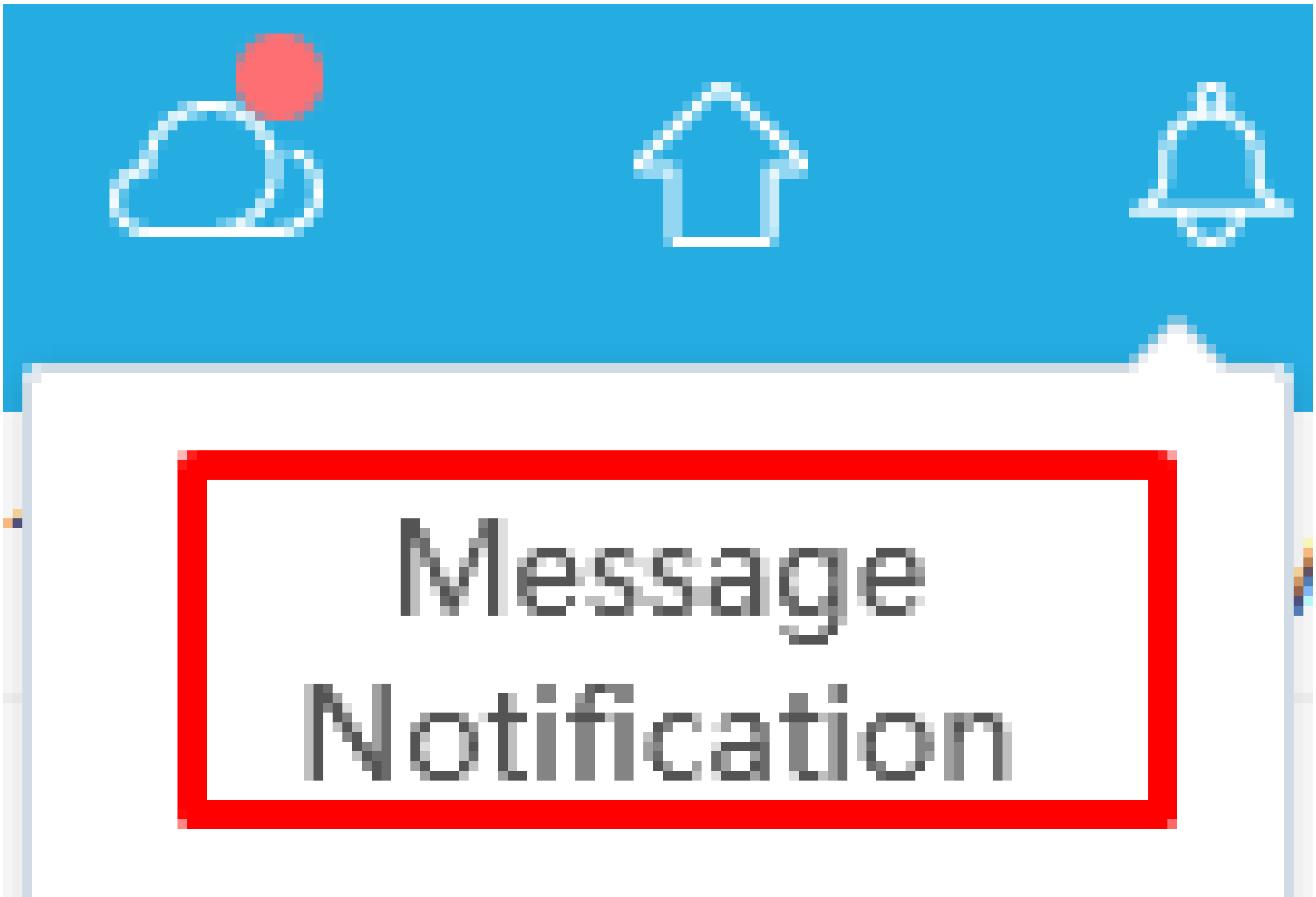


Fig 26. Message notifications Shortcut

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

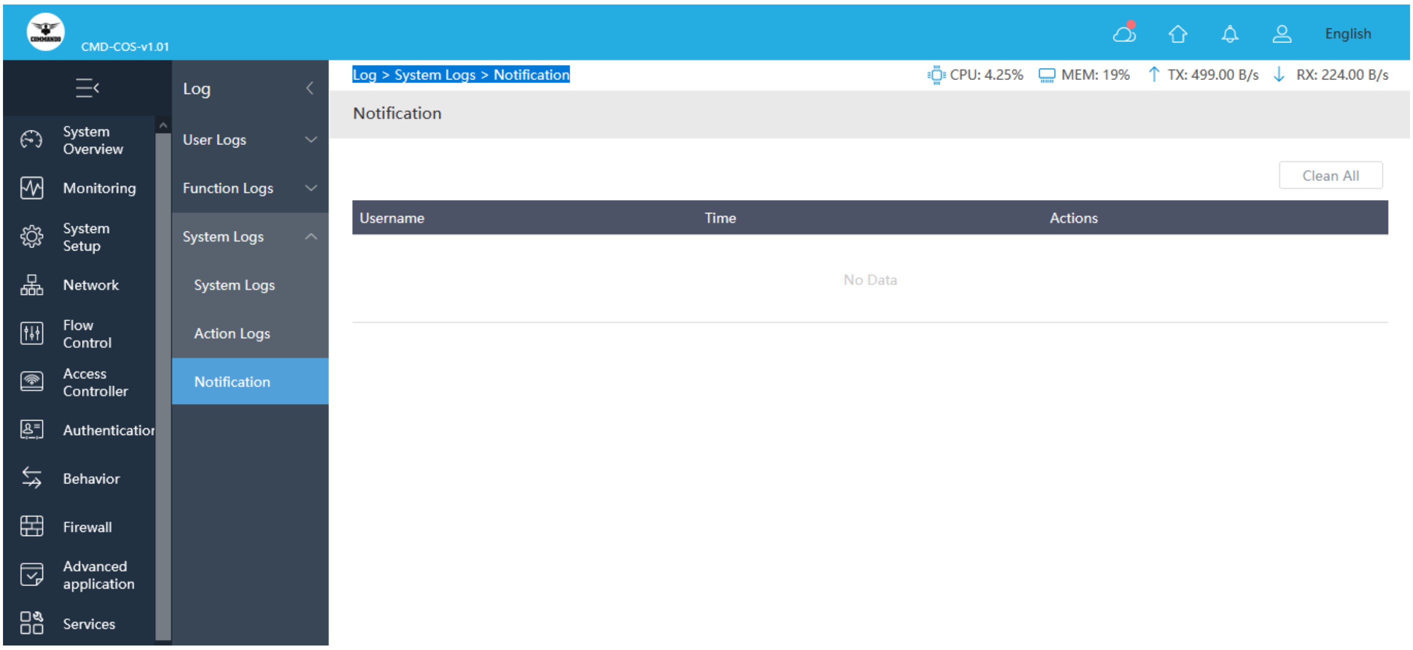
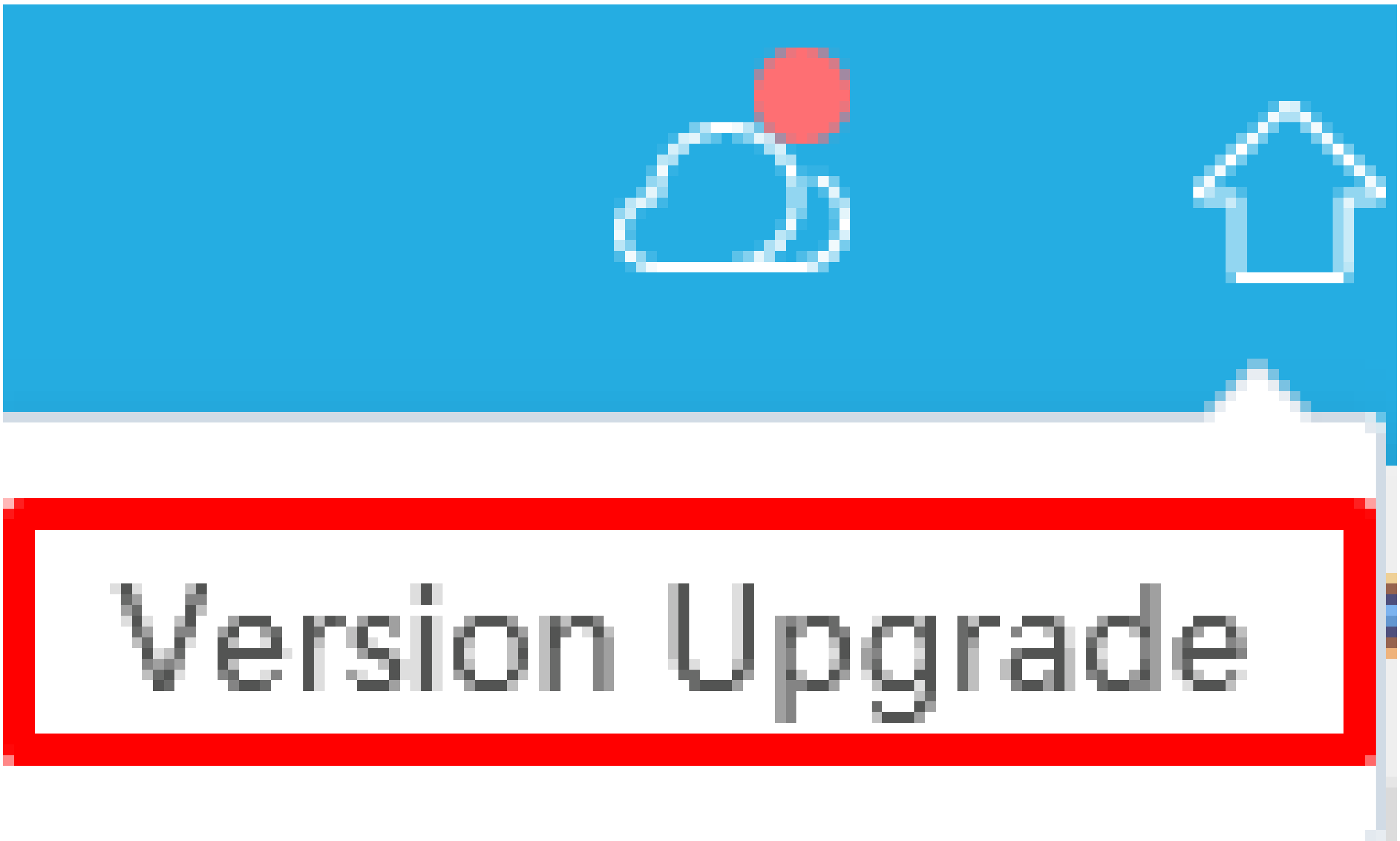


Fig 27. Default Message notifications page

Version Upgrade:

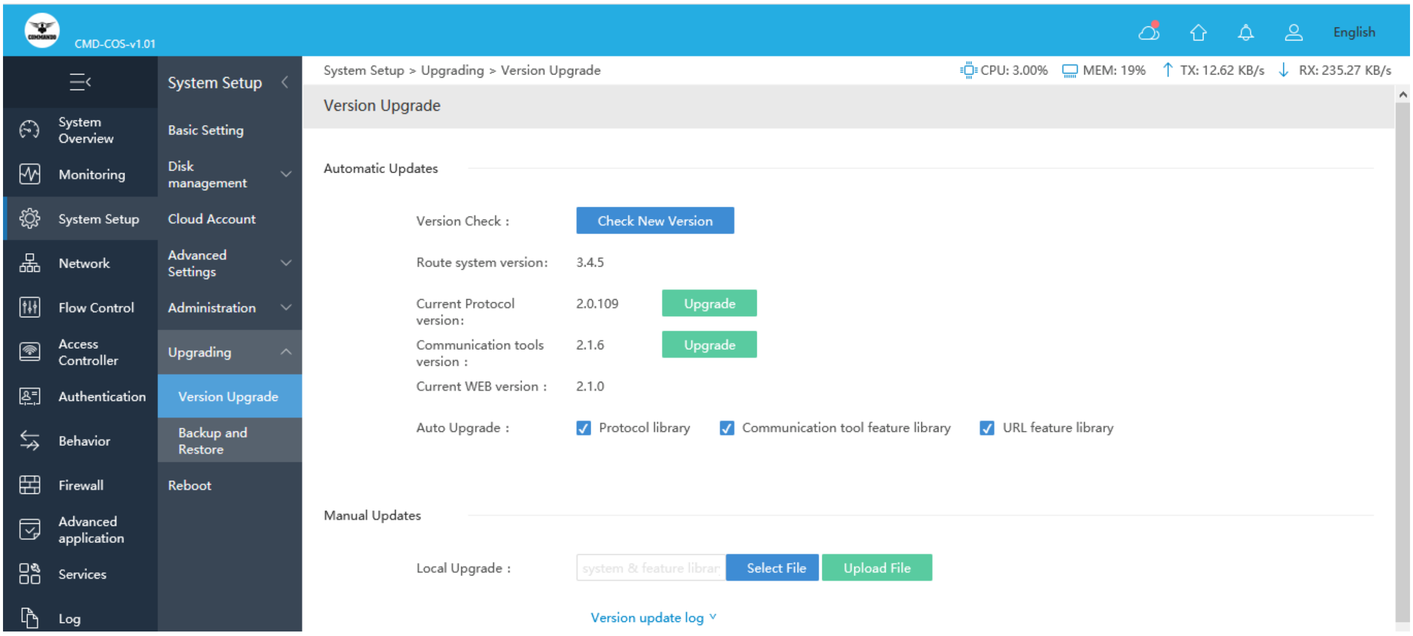
Displays the current configuration version of the Router and allows Automatic or manual Updates.



Version Upgrade

Fig 28. Version Upgrade page

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



System Setup > Upgrading > Version Upgrade

CPU: 3.00% MEM: 19% TX: 12.62 KB/s RX: 235.27 KB/s

Version Upgrade

Automatic Updates

Version Check : Check New Version

Route system version: 3.4.5

Current Protocol version: 2.0.109 Upgrade

Communication tools version : 2.1.6 Upgrade

Current WEB version : 2.1.0

Auto Upgrade : ☑ Protocol library ☑ Communication tool feature library ☑ URL feature library

Manual Updates

Local Upgrade : system & feature librar Select File Upload File

Version update log ˅

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.

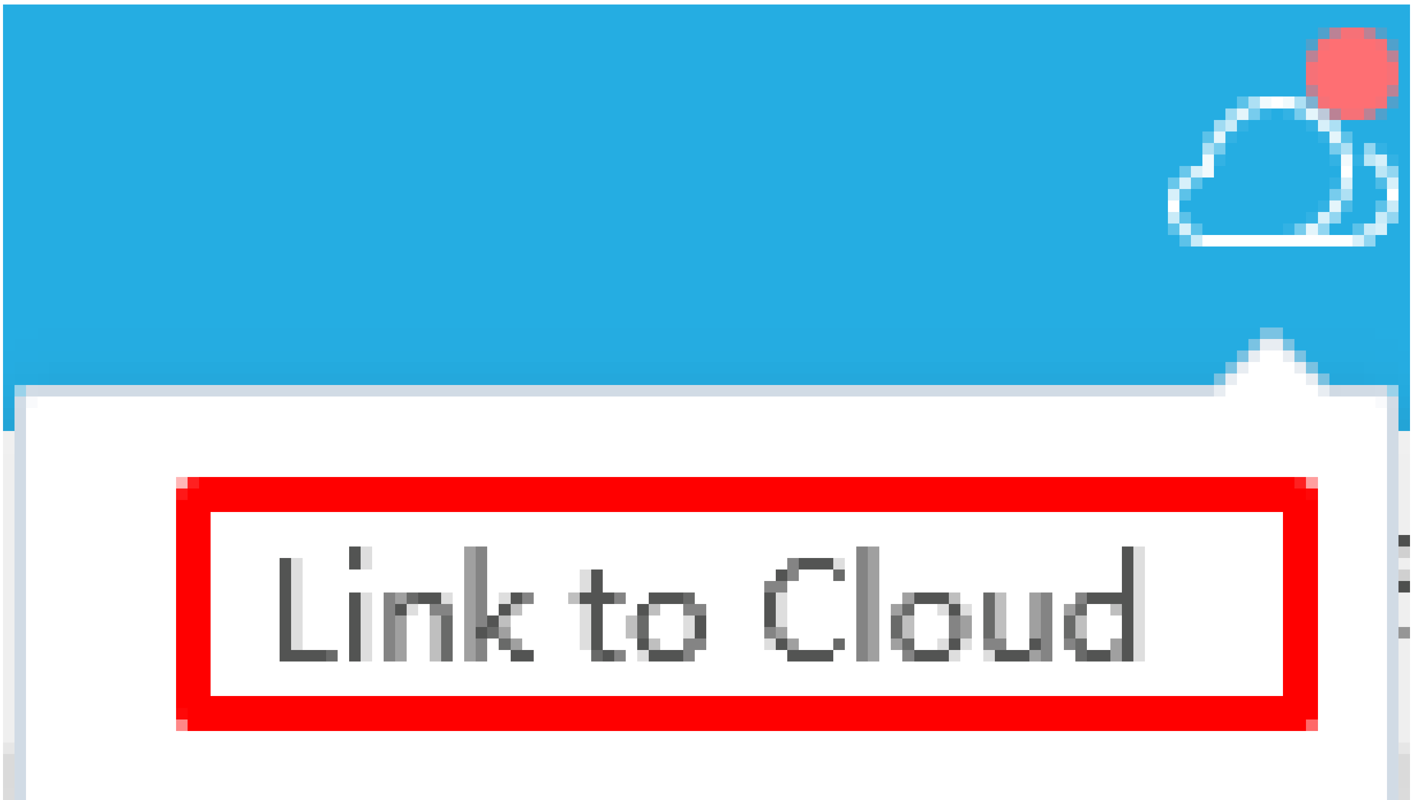
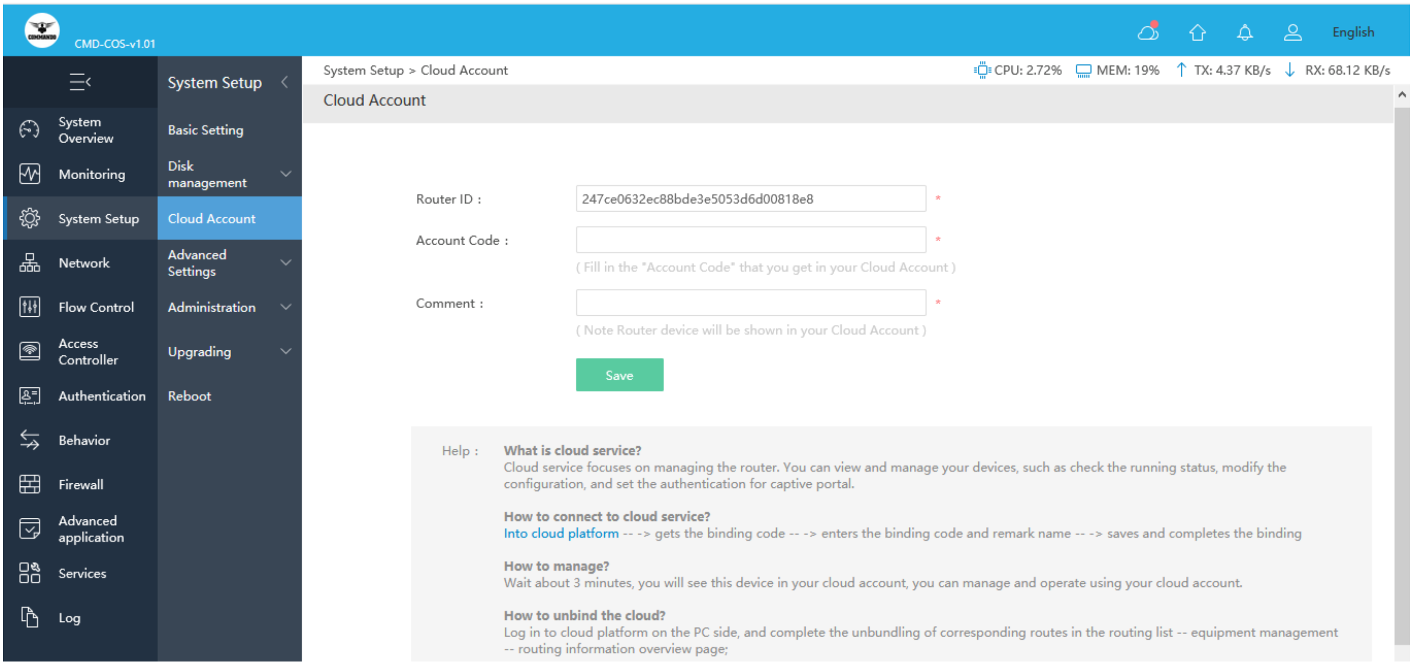


Fig 30. Link to Cloud shortcut

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



Cloud Account

Router ID : 247ce0632ec88bde3e5053d6d00818e8 *

Account Code : *

(Fill in the "Account Code" that you get in your Cloud Account)

Comment : *

(Note Router device will be shown in your Cloud Account)

Save

Help :

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 -- -> gets the binding code -- -> enters the binding code and remark name -- -> saves and completes the binding

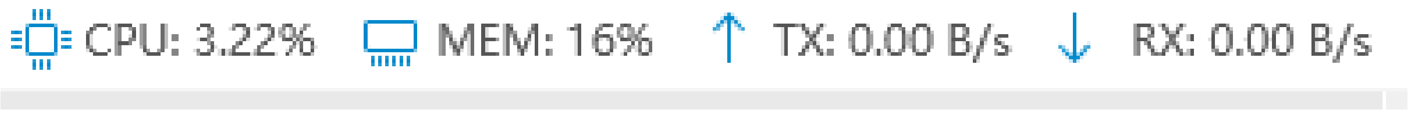
How to manage?
Wait about 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.

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 31. Link to Cloud account page

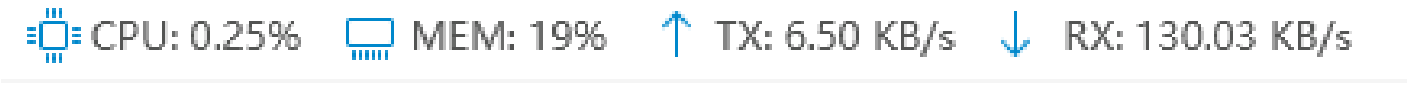
CPU, Memory, Trans and receive icons:

These help us to know running status of router.



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



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.

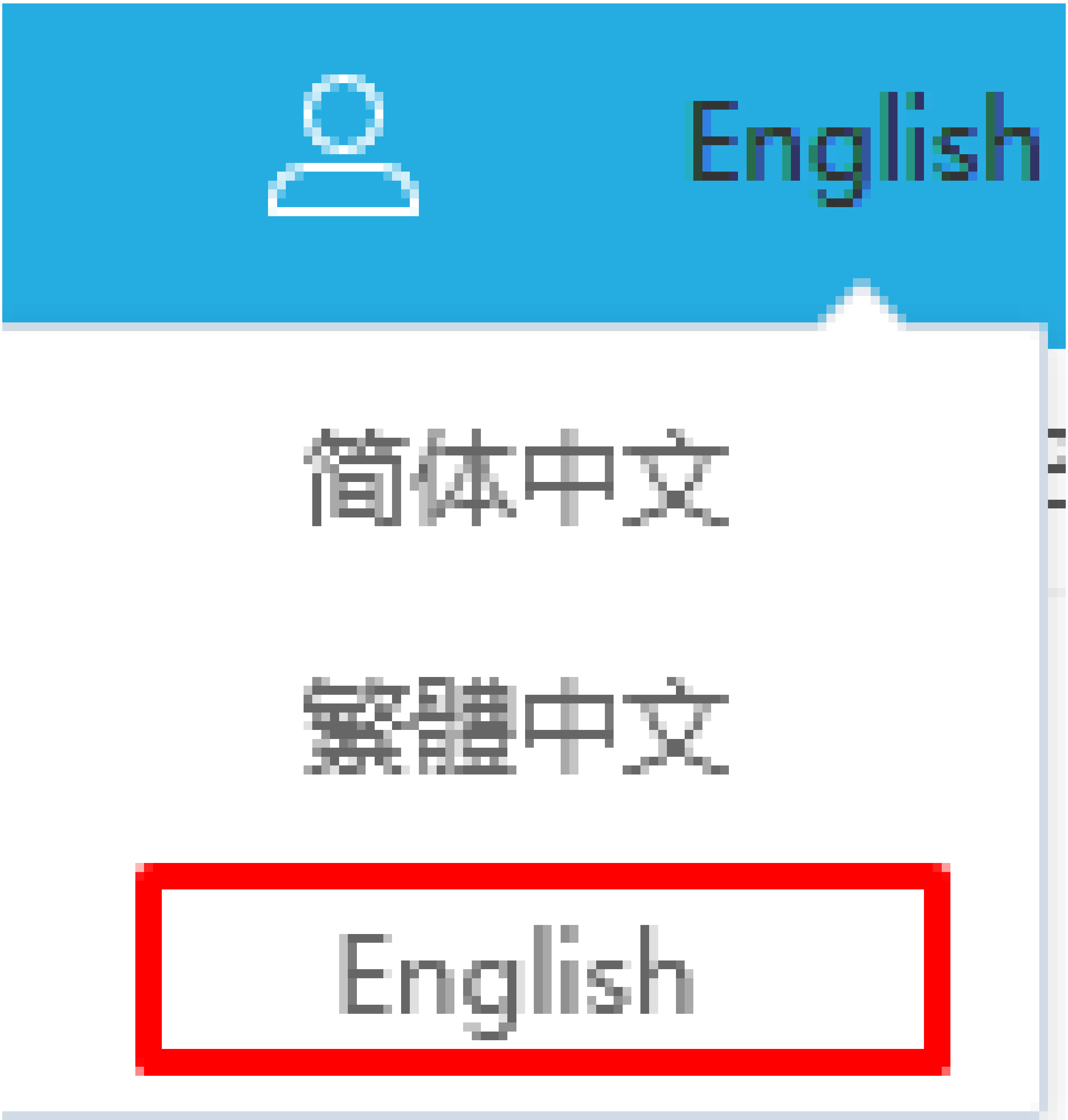


Fig 34. Language selection icon

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

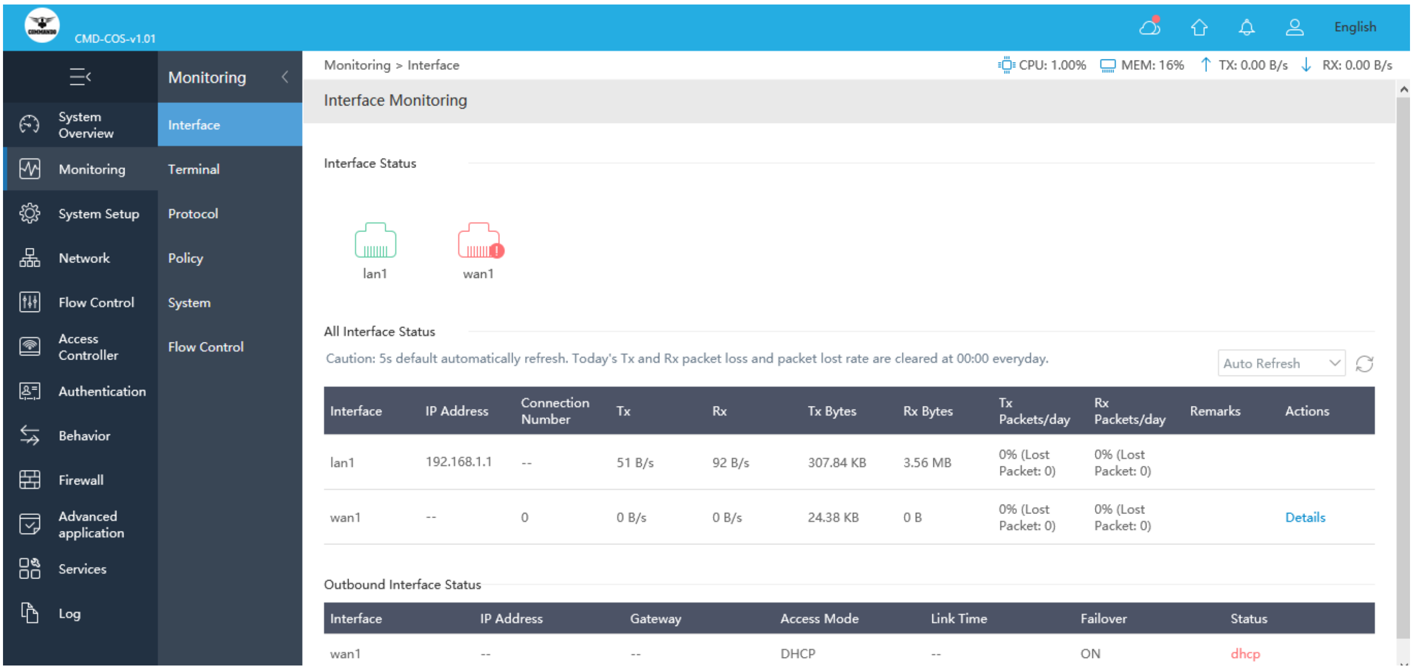
Physical interfaces exist on interface cards and transmit service data. Physical interfaces are classified into the following types:

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

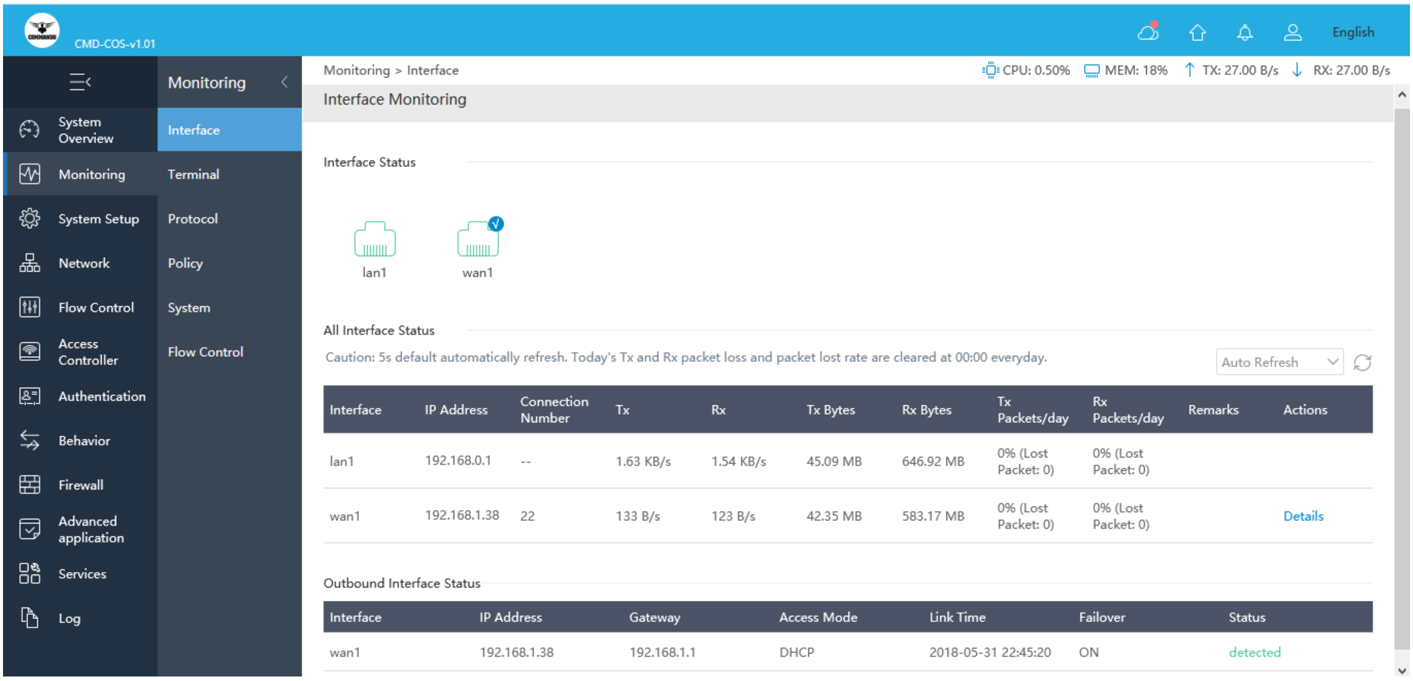


Caution: 5s default automatically refresh. Today's Tx and Rx packet loss and packet lost rate are cleared at 00:00 everyday.

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)		Details

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

Fig 1.1.1 Default interface monitoring page



CPU: 0.50% MEM: 18% TX: 27.00 B/s RX: 27.00 B/s

Interface Monitoring

Interface Status

All Interface Status

Caution: 5s default automatically refresh. Today's Tx and Rx packet loss and packet lost rate are cleared at 00:00 everyday.

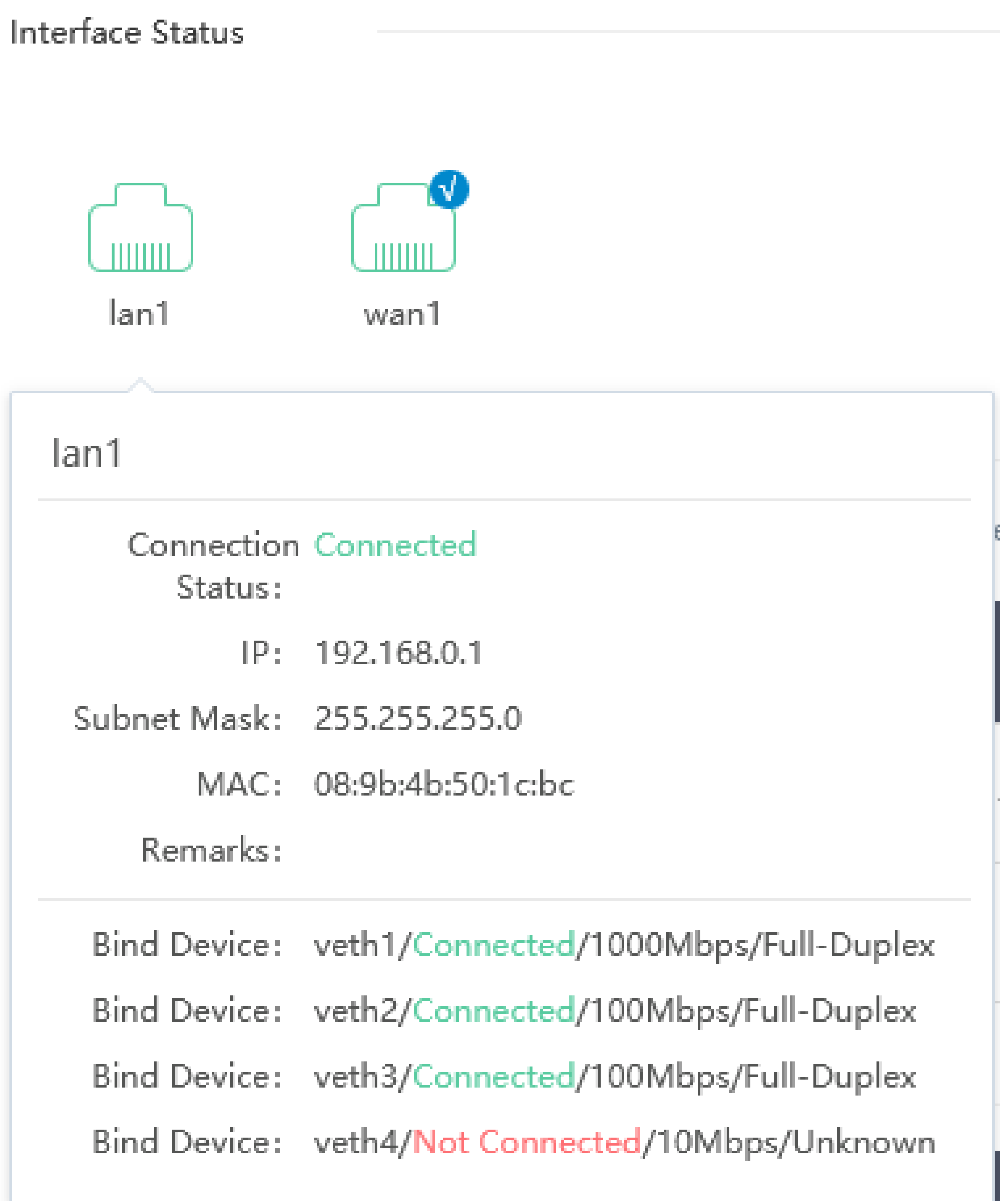
Interface	IP Address	Connection Number	Tx	Rx	Tx Bytes	Rx Bytes	Tx Packets/day	Rx Packets/day	Remarks	Actions
lan1	192.168.0.1	--	1.63 KB/s	1.54 KB/s	45.09 MB	646.92 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		
wan1	192.168.1.38	22	133 B/s	123 B/s	42.35 MB	583.17 MB	0% (Lost Packet: 0)	0% (Lost Packet: 0)		Details

Outbound Interface Status

Interface	IP Address	Gateway	Access Mode	Link Time	Failover	Status
wan1	192.168.1.38	192.168.1.1	DHCP	2018-05-31 22:45:20	ON	detected

Fig 1.1.2 Interface monitoring page after changing LAN and WAN IP

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



Interface Status

lan1

Connection Status: Connected

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

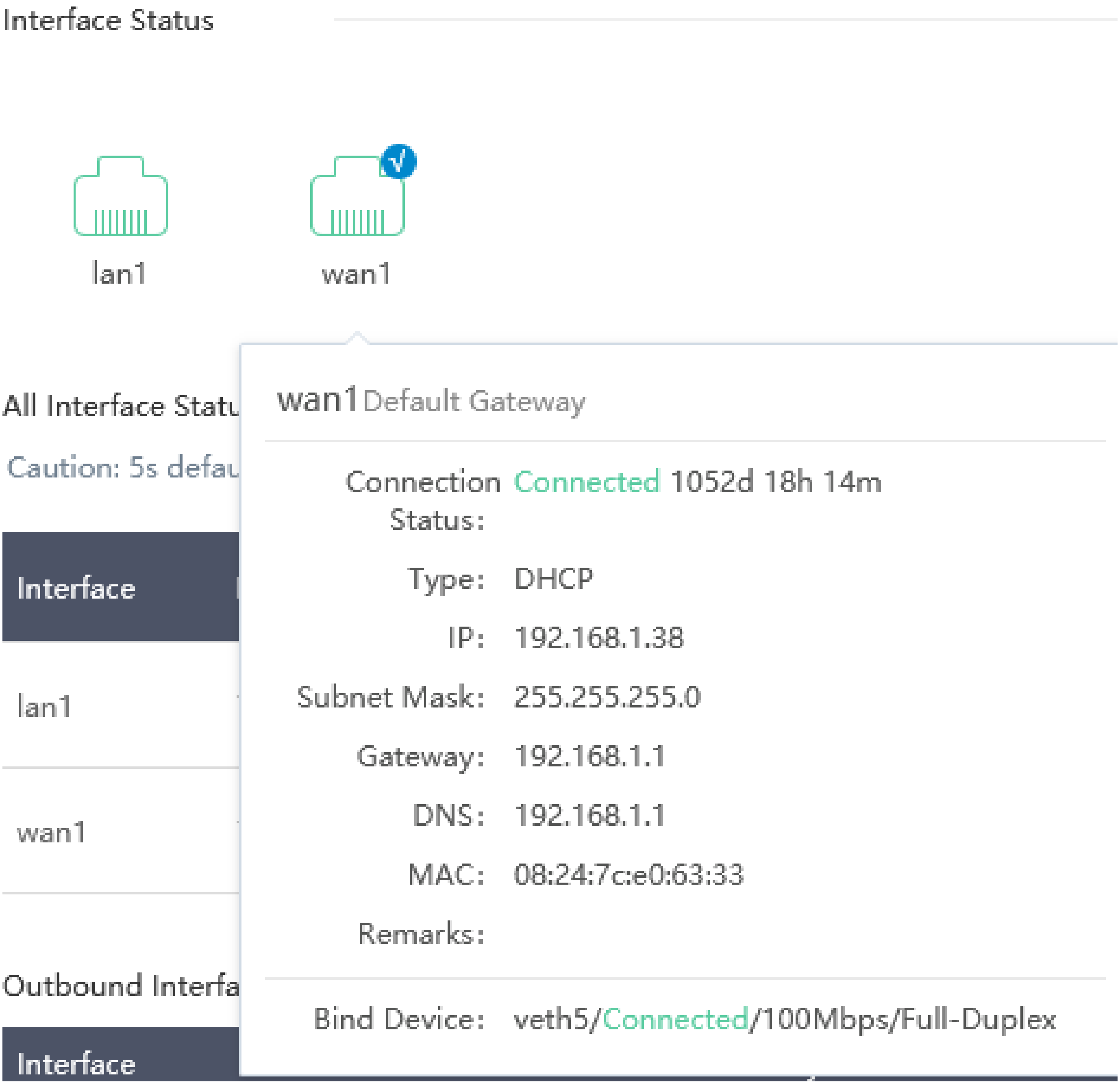
Bind Device: veth2/Connected/100Mbps/Full-Duplex

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

All Interface Statu

Caution: 5s defau

Interface
lan1
wan1

Outbound Interfa

Interface

wan1 Default Gateway

Connection Status: Connected 1052d 18h 14m

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:

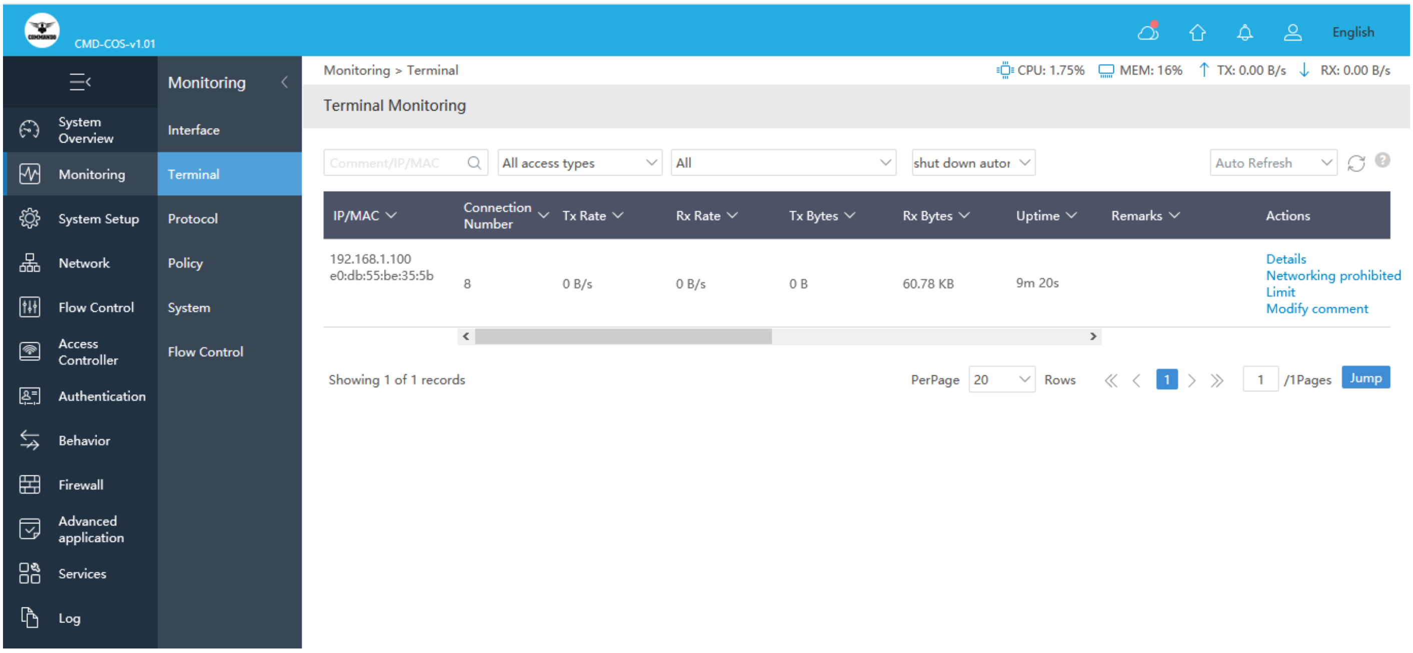
Bind Device: veth5/Connected/100Mbps/Full-Duplex

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



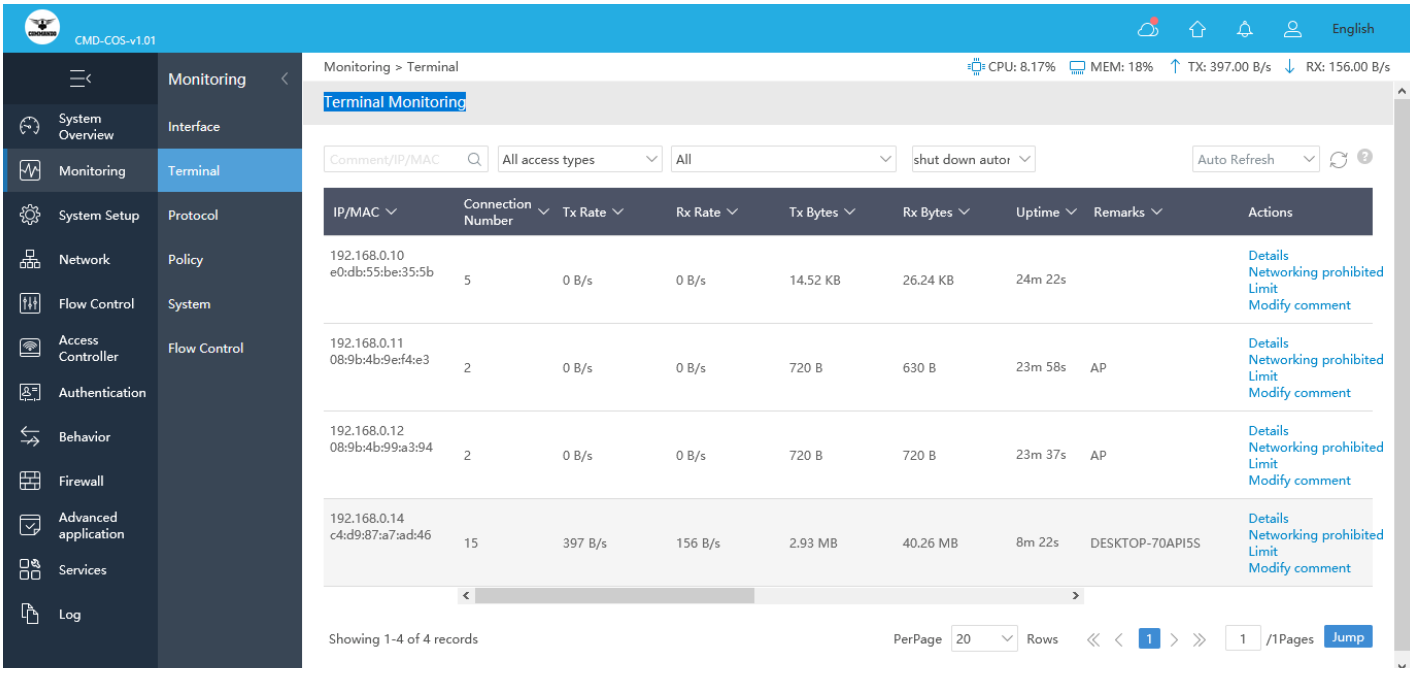
CPU: 1.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Terminal Monitoring

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		Details Networking prohibited Limit Modify comment

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

Fig 1.2.1 Default Terminal Monitoring page



CPU: 8.17% MEM: 18% TX: 397.00 B/s RX: 156.00 B/s

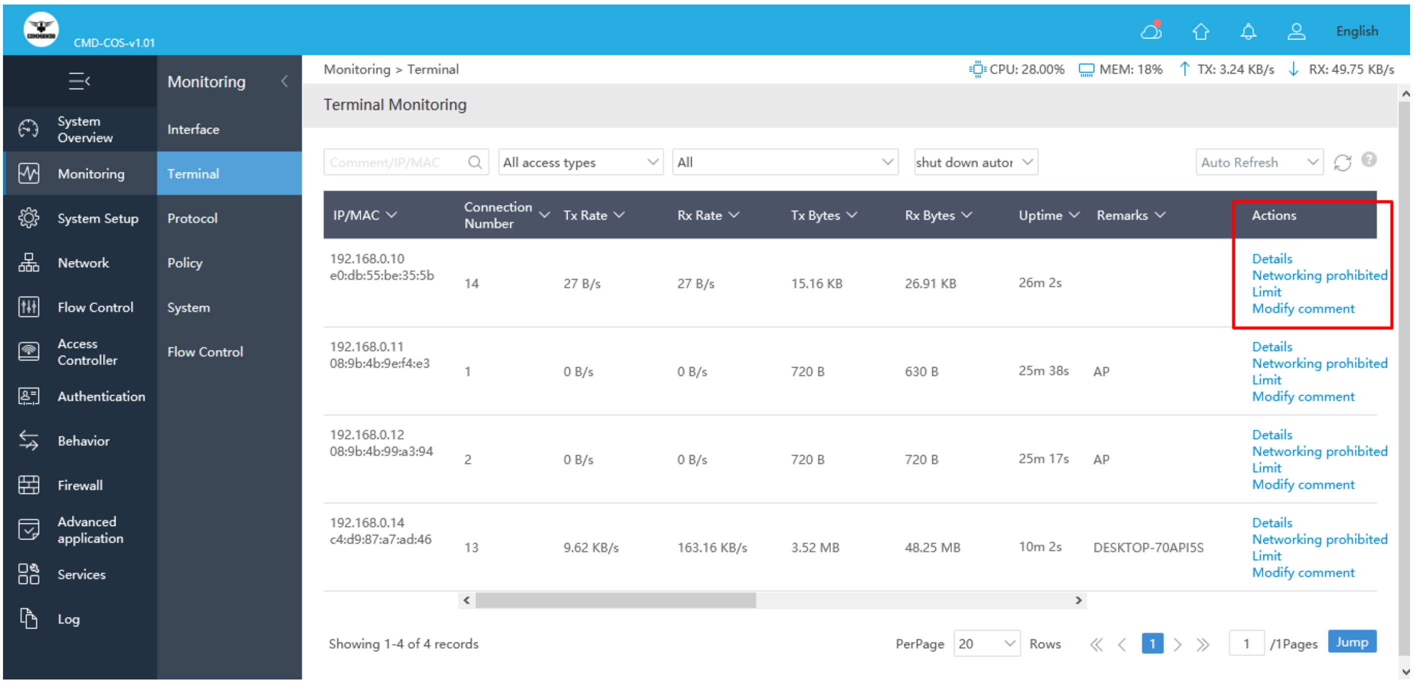
Terminal Monitoring

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		Details Networking prohibited Limit Modify comment
192.168.0.11 08:9b:4b:9e:f4:e3	2	0 B/s	0 B/s	720 B	630 B	23m 58s	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	23m 37s	AP	Details Networking prohibited Limit Modify comment
192.168.0.14 c4:d9:87:a7:ad:46	15	397 B/s	156 B/s	2.93 MB	40.26 MB	8m 22s	DESKTOP-70API5S	Details Networking prohibited Limit Modify comment

Showing 1-4 of 4 records PerPage 20 Rows 1 1 /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

CPU: 28.00% MEM: 18% TX: 3.24 KB/s RX: 49.75 KB/s

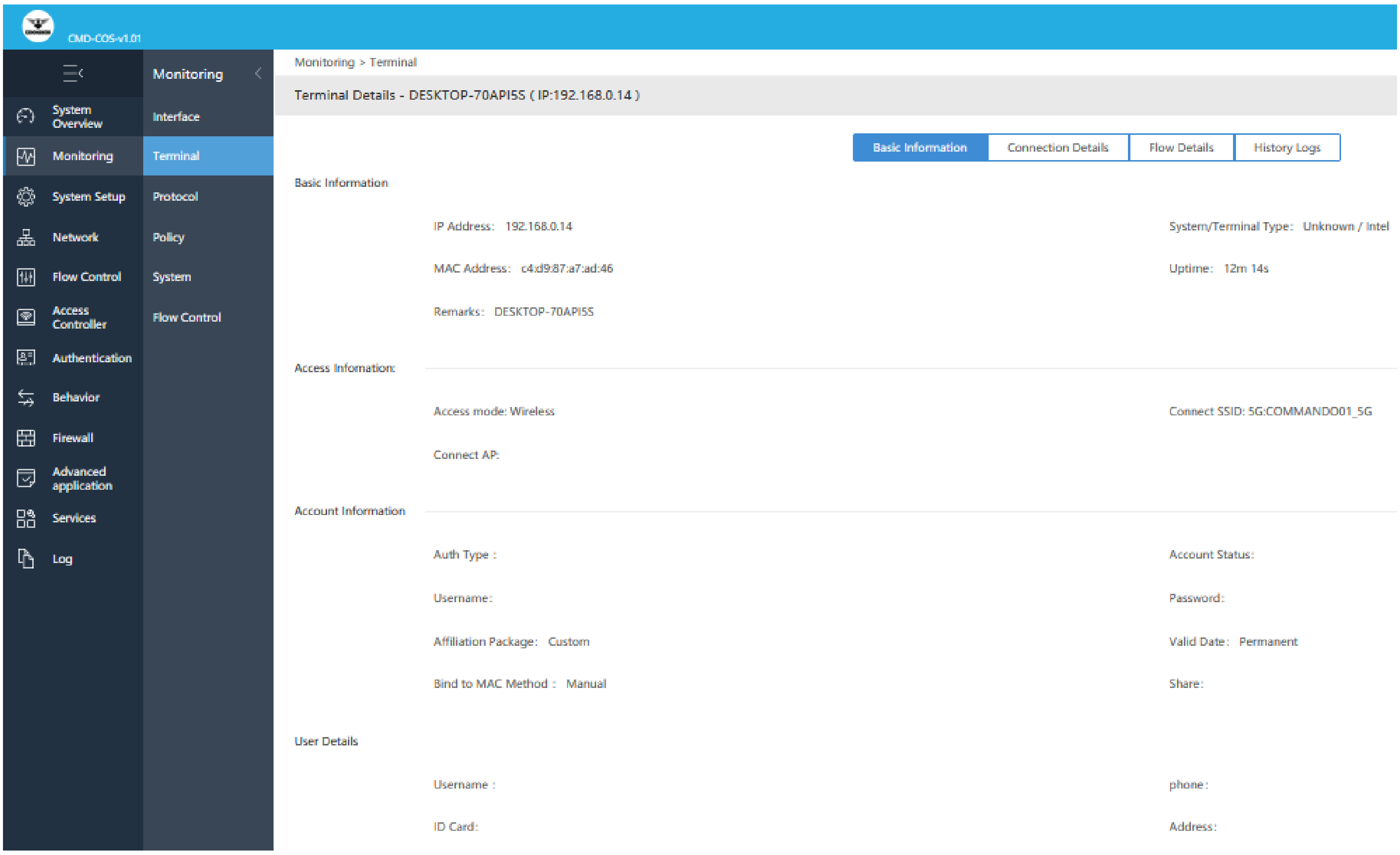
Terminal Monitoring

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:9e:f4: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-70API5S	Details Networking prohibited Limit Modify comment

Showing 1-4 of 4 records   PerPage 20 Rows   1   1 /1Pages

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-70API5S (IP:192.168.0.14)

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-70API5S

Access Information:

Access mode: Wireless   Connect SSID: 5G:COMMANDO01_5G

Connect AP:

Account Information

Auth Type :   Account Status:

Username: Password:

Affiliation Package: Custom   Valid Date: Permanent

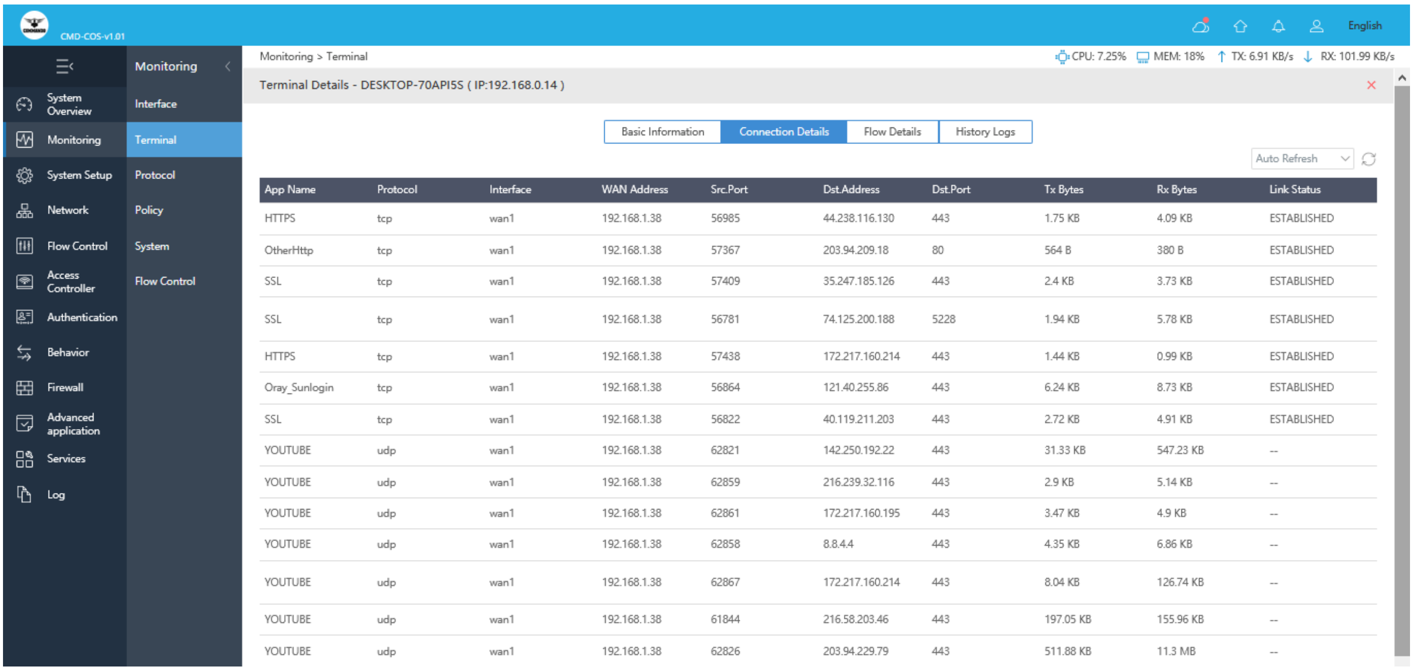
Bind to MAC Method : Manual   Share:

User Details

Username :   phone:

ID Card: Address:

Fig 1.2.4 Terminal Monitoring details Basic information page



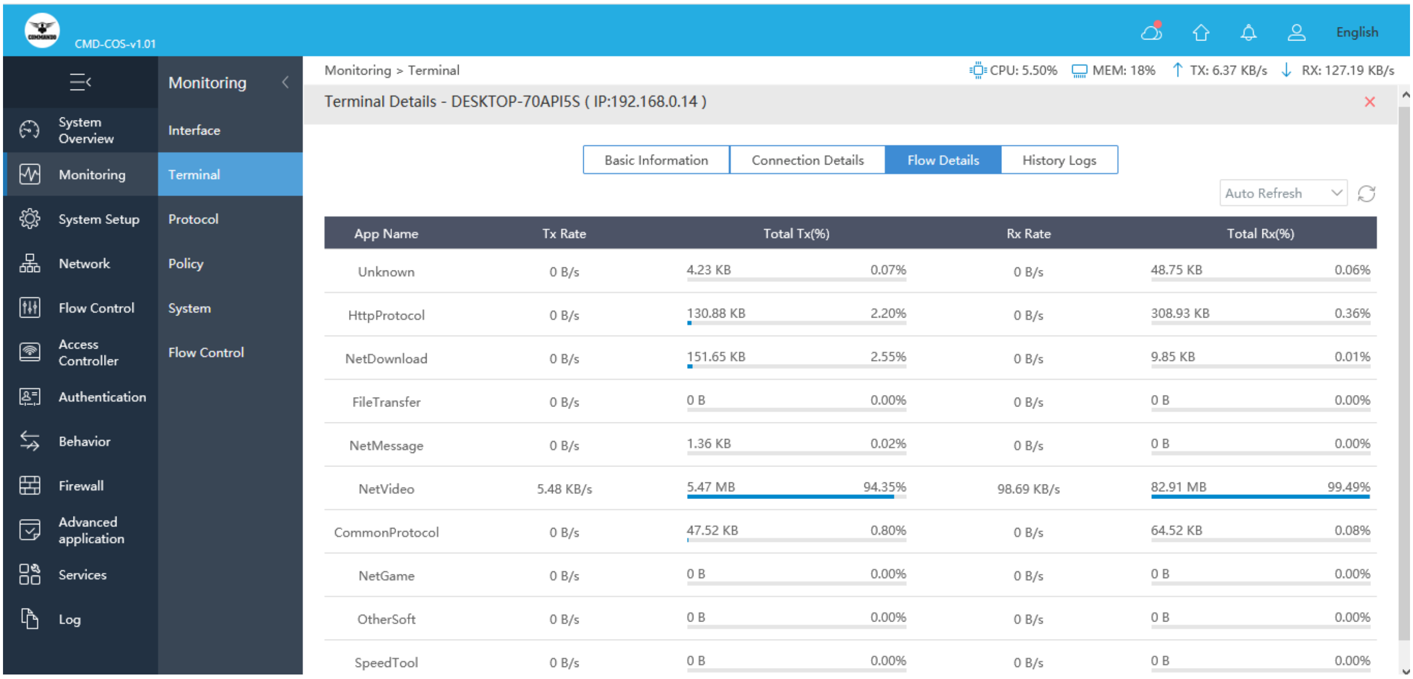
Monitoring > Terminal

CPU: 7.25% MEM: 18% TX: 6.91 KB/s RX: 101.99 KB/s

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

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



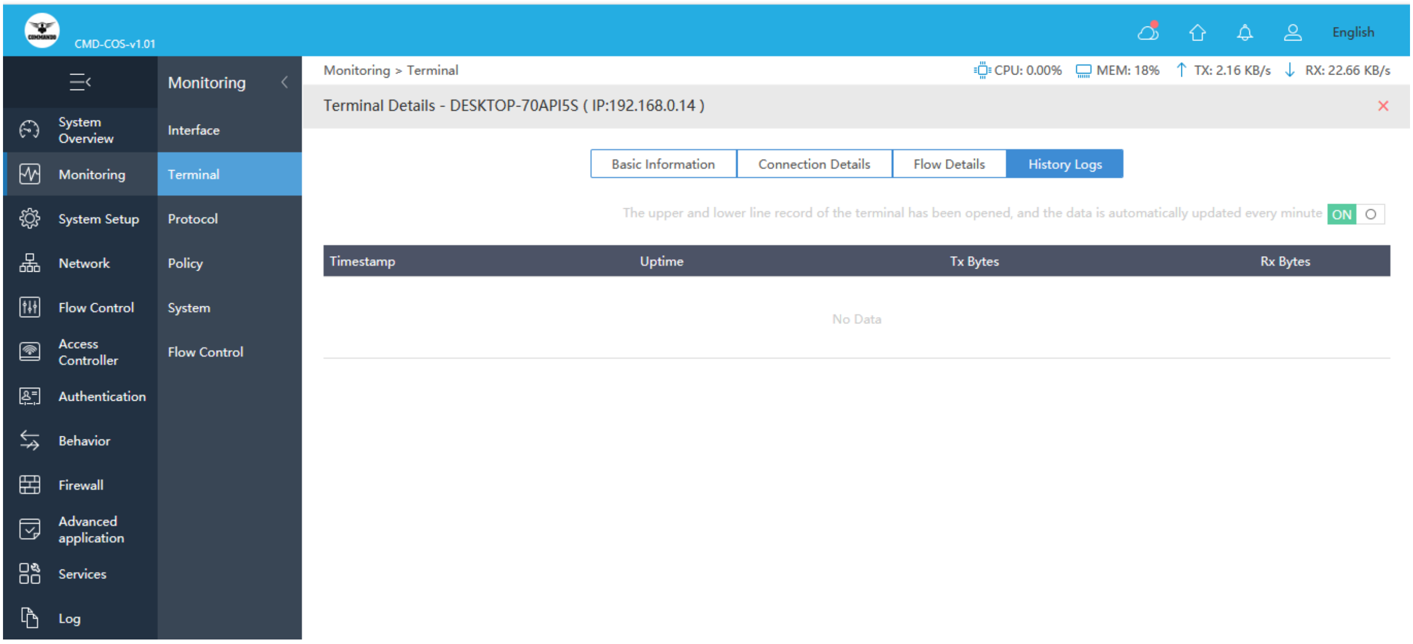
Monitoring > Terminal

CPU: 5.50% MEM: 18% TX: 6.37 KB/s RX: 127.19 KB/s

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

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



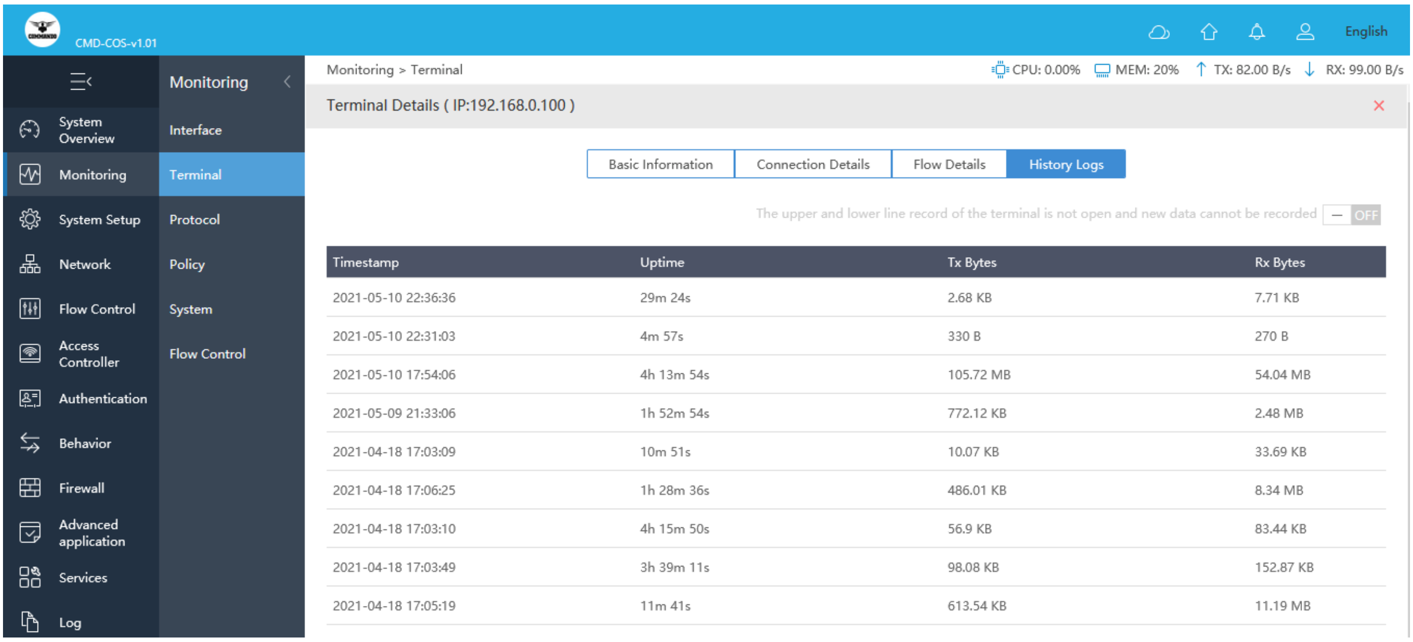
Terminal Details - DESKTOP-70API5S (IP:192.168.0.14)

The upper and lower line record of the terminal has been opened, and the data is automatically updated every minute

Timestamp	Uptime	Tx Bytes	Rx Bytes

No Data

Fig 1.2.7 Default Terminal Monitoring History Logs page



Terminal Details (IP:192.168.0.100)

The upper and lower line record of the terminal is not open and new data cannot be recorded

Timestamp	Uptime	Tx Bytes	Rx Bytes
2021-05-10 22:36:36	29m 24s	2.68 KB	7.71 KB
2021-05-10 22:31:03	4m 57s	330 B	270 B
2021-05-10 17:54:06	4h 13m 54s	105.72 MB	54.04 MB
2021-05-09 21:33:06	1h 52m 54s	772.12 KB	2.48 MB
2021-04-18 17:03:09	10m 51s	10.07 KB	33.69 KB
2021-04-18 17:06:25	1h 28m 36s	486.01 KB	8.34 MB
2021-04-18 17:03:10	4h 15m 50s	56.9 KB	83.44 KB
2021-04-18 17:03:49	3h 39m 11s	98.08 KB	152.87 KB
2021-04-18 17:05:19	11m 41s	613.54 KB	11.19 MB

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

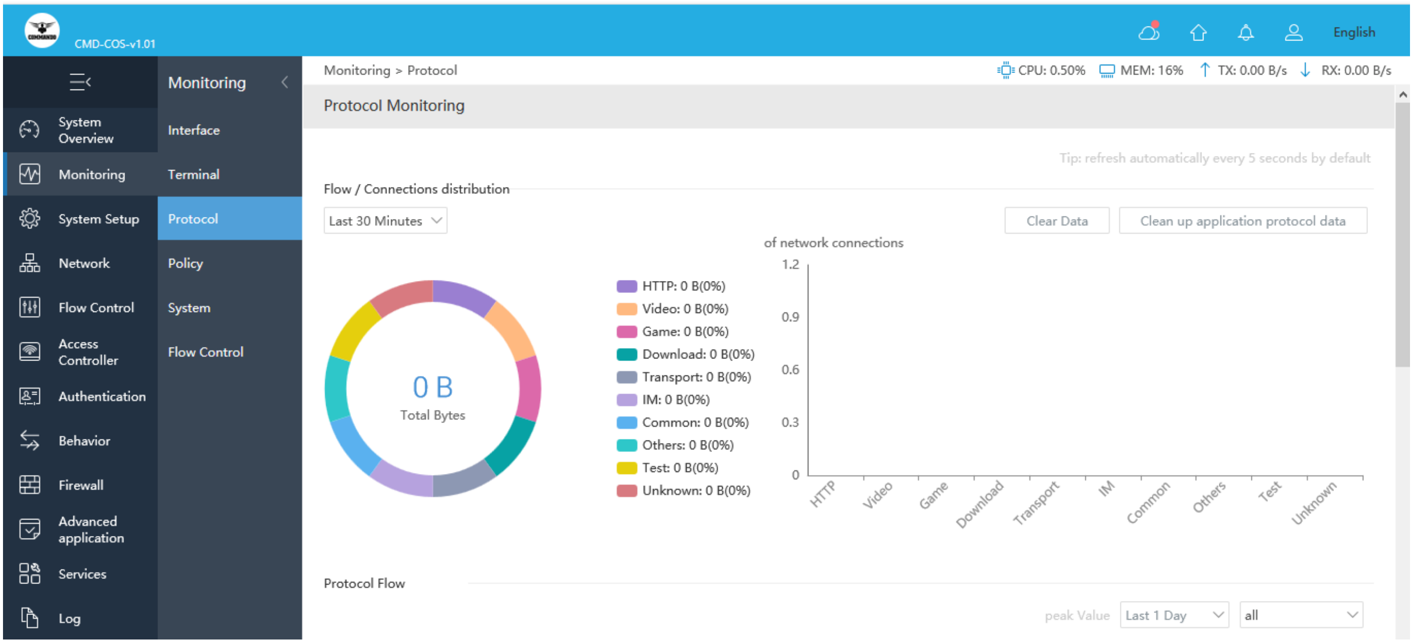


Fig 1.3.1 Protocol Monitoring flow/connections distribution default page

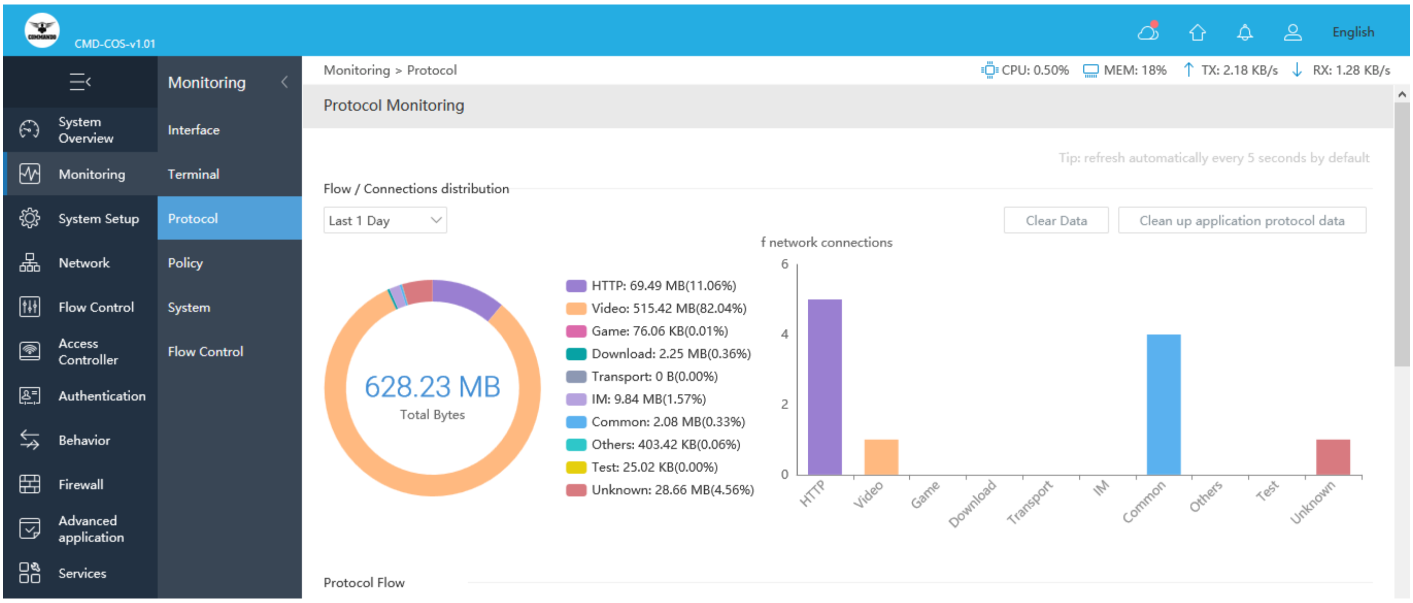


Fig 1.3.2 Protocol Monitoring flow/connections distribution for 1 day page

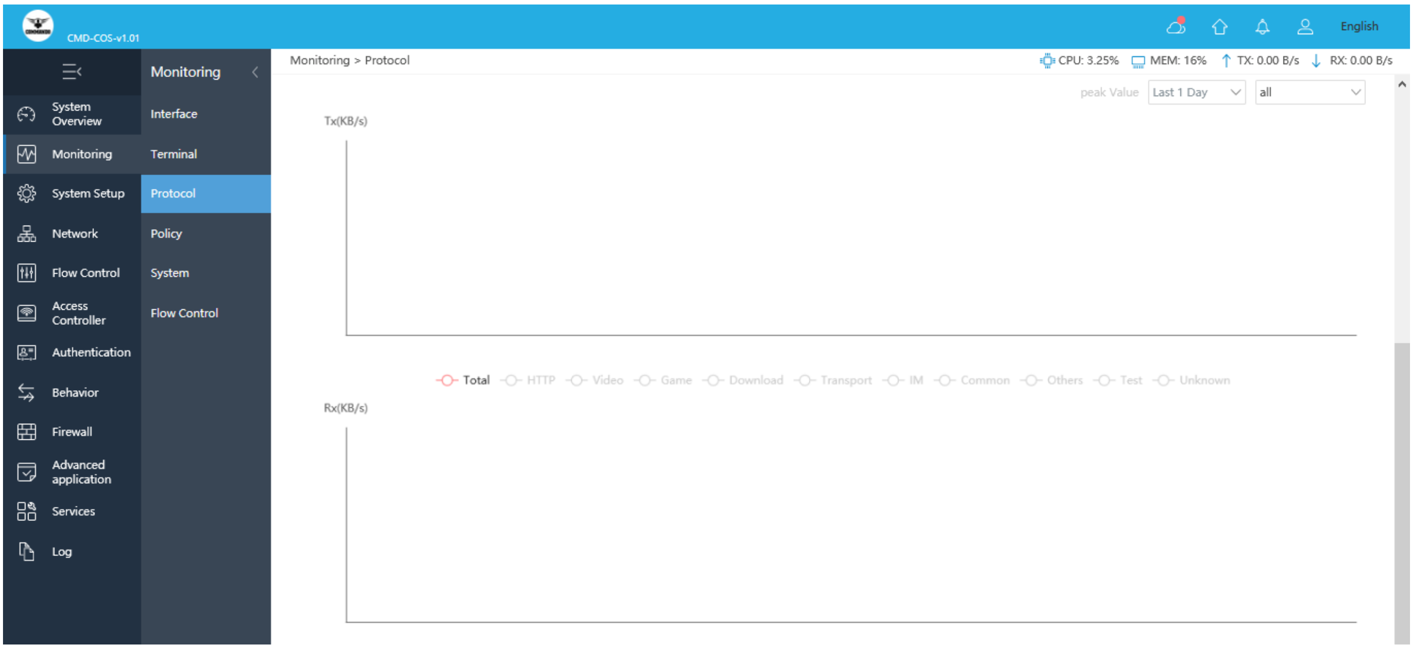


Fig 1.3.3 Default Protocol Monitoring Graphs default page

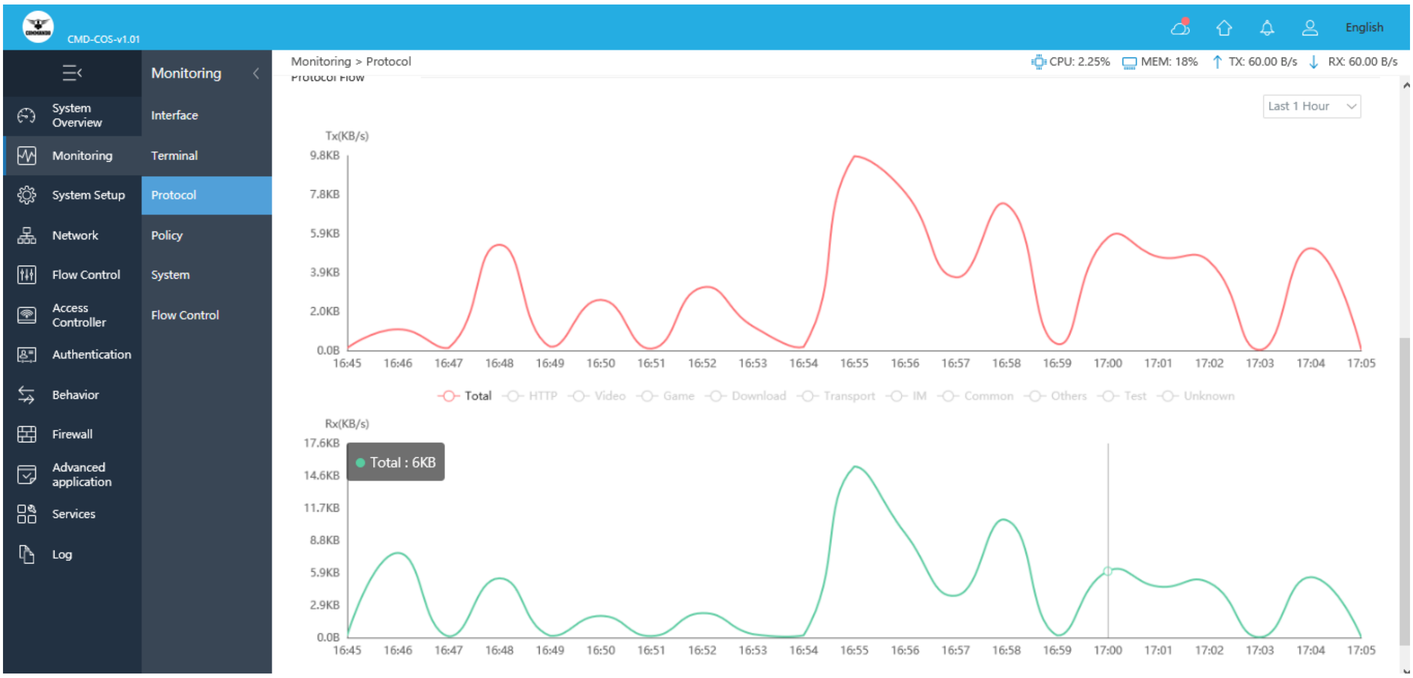
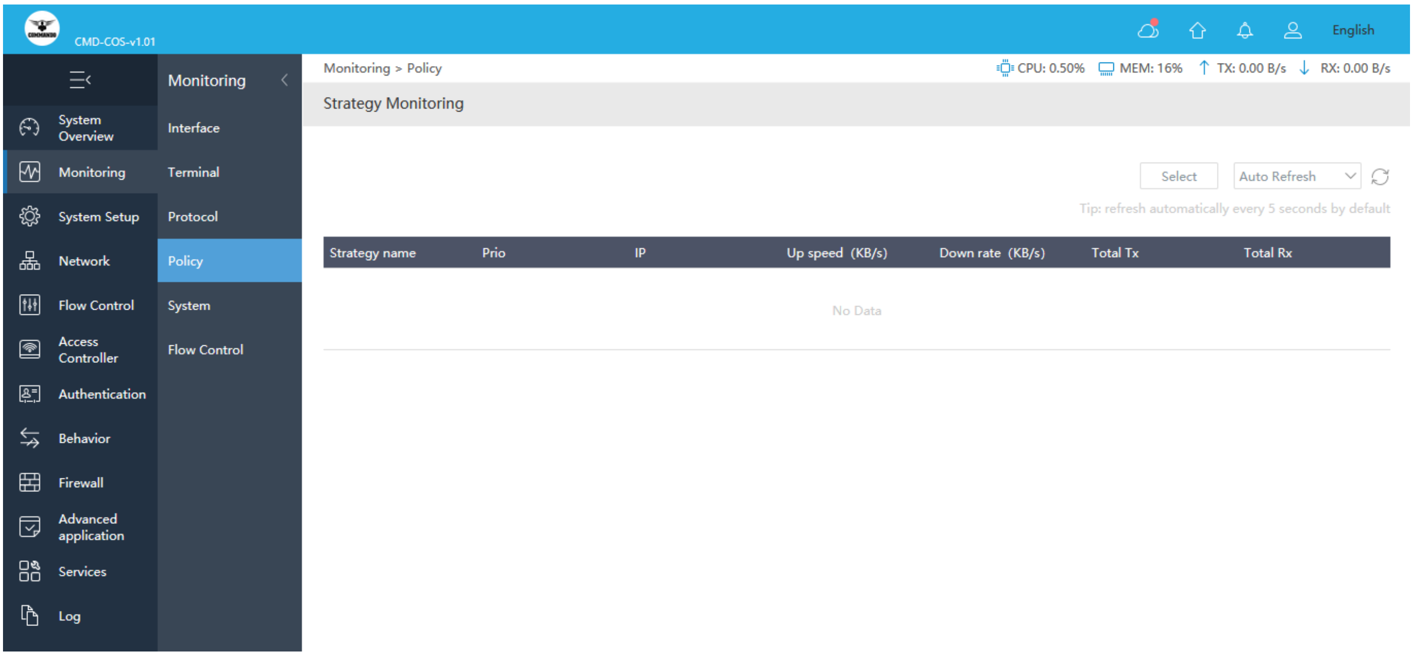


Fig 1.3.4 Protocol Monitoring Graphs for last 1 hour page

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



Monitoring > Policy

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

Strategy Monitoring

Tip: refresh automatically every 5 seconds by default

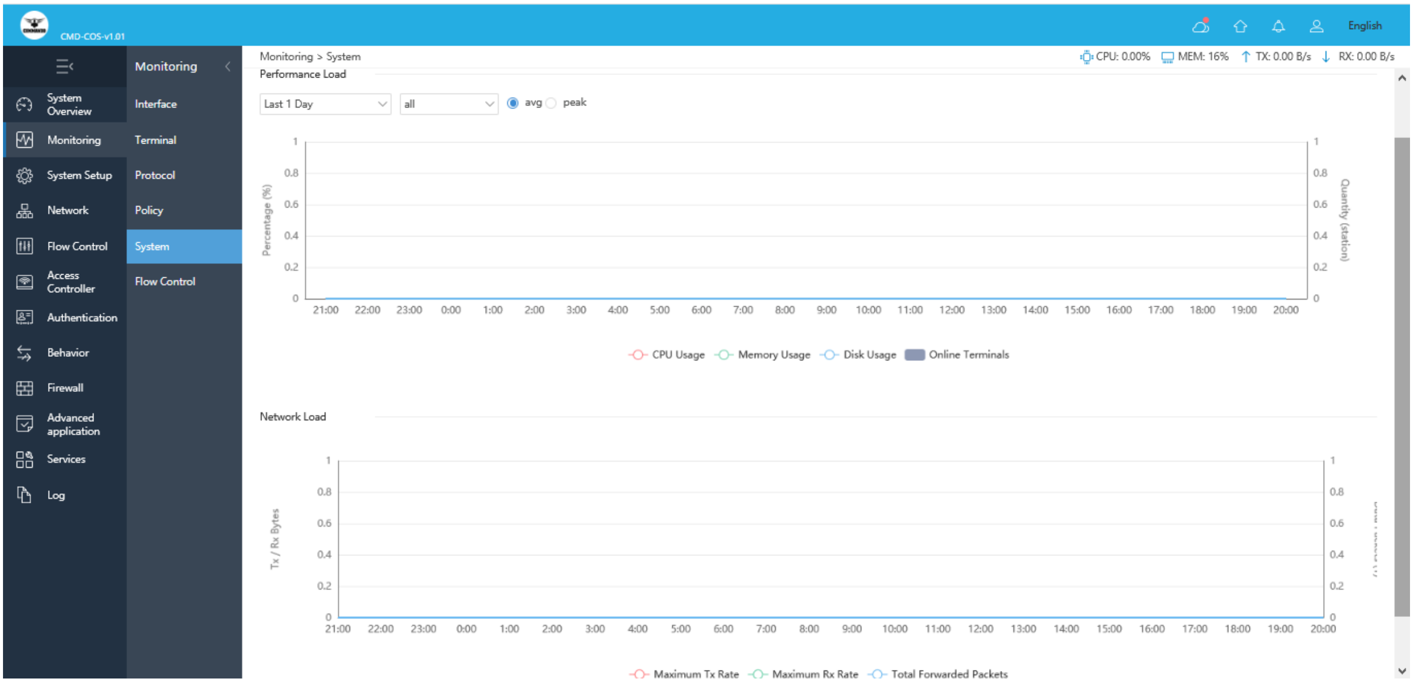
Strategy name	Prio	IP	Up speed (KB/s)	Down rate (KB/s)	Total Tx	Total Rx
No Data						

Fig 1.4.1 Default Policy Monitoring page

5. System

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

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

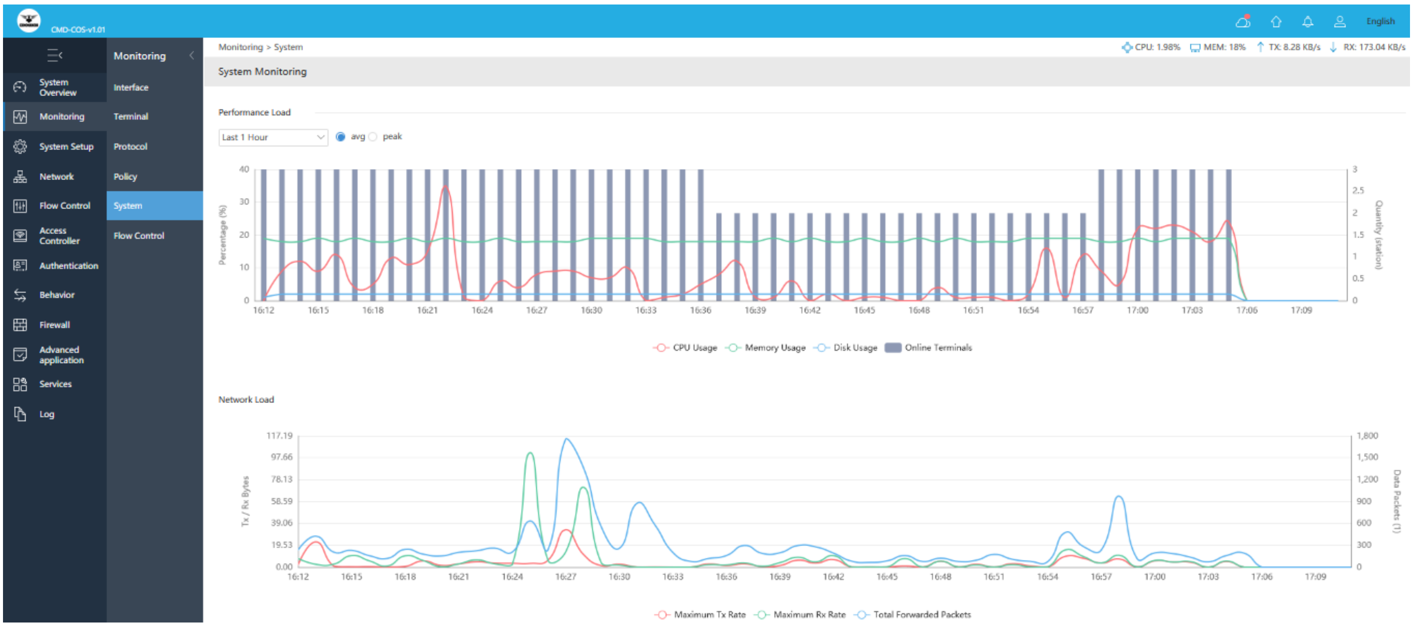


Monitoring > System

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

Last 1 Day | all | ● avg ○ peak

Fig 1.5.1 Default System Monitoring page



Monitoring > System

CPU: 1.98% MEM: 18% TX: 8.28 KB/s RX: 173.04 KB/s

System Monitoring

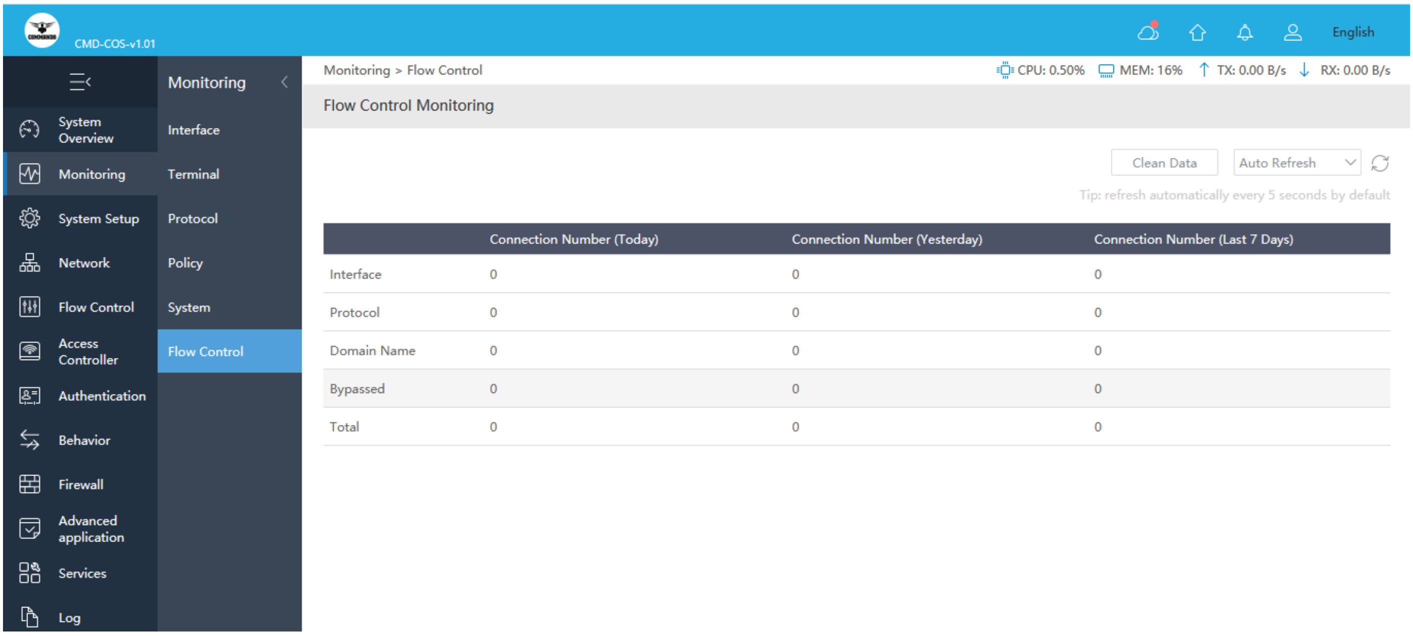
Last 1 Hour ● avg ○ peak

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



Monitoring > Flow Control

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

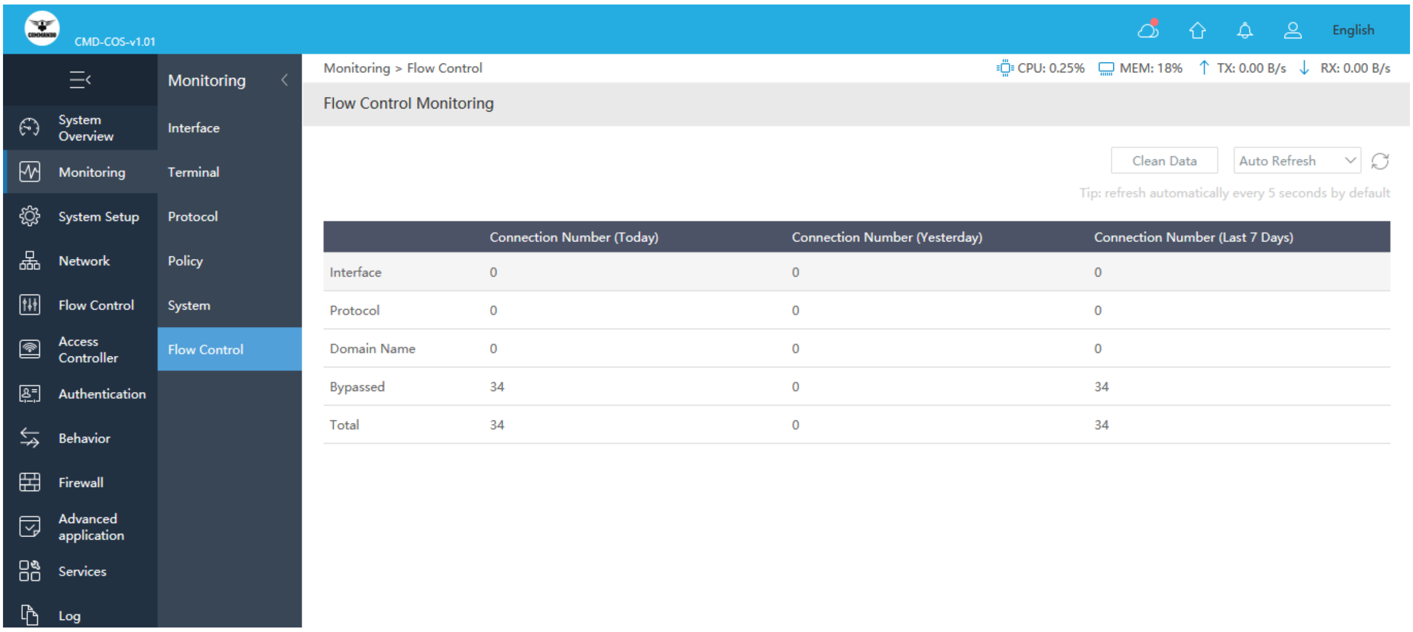
Flow Control Monitoring

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	0	0	0
Total	0	0	0

Fig 1.6.1 Default Flow Control page



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
Total	34	0	34

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.

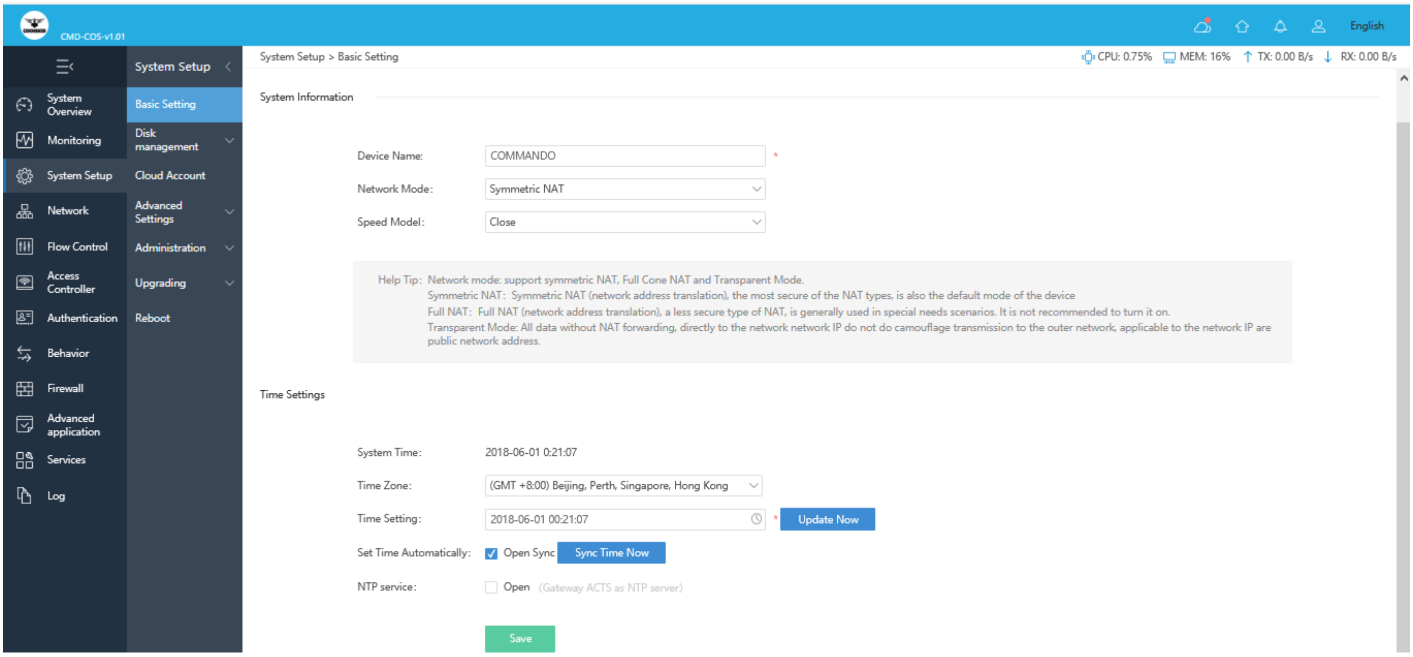
Reboot:

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



System Setup > Basic Setting

CPU: 0.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

System Information

Device Name: COMMANDO *

Network Mode: Symmetric NAT

Speed Model: Close

Help Tip: Network mode: support symmetric NAT, Full Cone NAT and Transparent Mode.
Symmetric NAT: Symmetric NAT (network address translation), the most secure of the NAT types, is also the default mode of the device
Full NAT: Full NAT (network address translation), a less secure type of NAT, is generally used in special needs scenarios. It is not recommended to turn it on.
Transparent Mode: All data without NAT forwarding, directly to the network network IP do not do camouflage transmission to the outer network, applicable to the network IP are public network address.

Time Settings

System Time: 2018-06-01 0:21:07

Time Zone: (GMT +8:00) Beijing, Perth, Singapore, Hong Kong

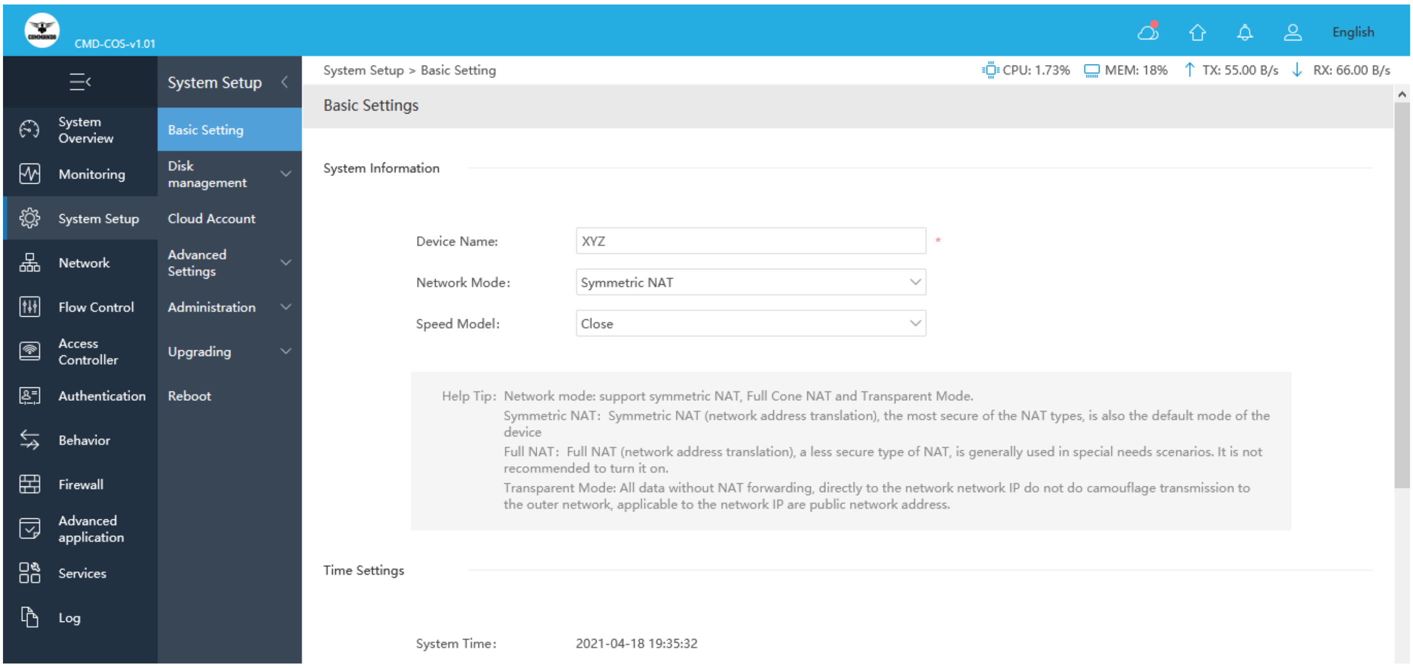
Time Setting: 2018-06-01 00:21:07 * Update Now

Set Time Automatically: ☑ Open Sync Sync Time Now

NTP service: □ Open (Gateway ACTS as NTP server)

Save

Fig 2.1.1 Default Basic setting page



System Setup > Basic Setting

CPU: 1.73% MEM: 18% TX: 55.00 B/s RX: 66.00 B/s

Basic Settings

System Information

Device Name: XYZ *

Network Mode: Symmetric NAT

Speed Model: Close

Help Tip: Network mode: support symmetric NAT, Full Cone NAT and Transparent Mode.
Symmetric NAT: Symmetric NAT (network address translation), the most secure of the NAT types, is also the default mode of the device
Full NAT: Full NAT (network address translation), a less secure type of NAT, is generally used in special needs scenarios. It is not recommended to turn it on.
Transparent Mode: All data without NAT forwarding, directly to the network network IP do not do camouflage transmission to the outer network, applicable to the network IP are public network address.

Time Settings

System Time: 2021-04-18 19:35:32

Fig 2.1.2 Basic setting for changing device name page

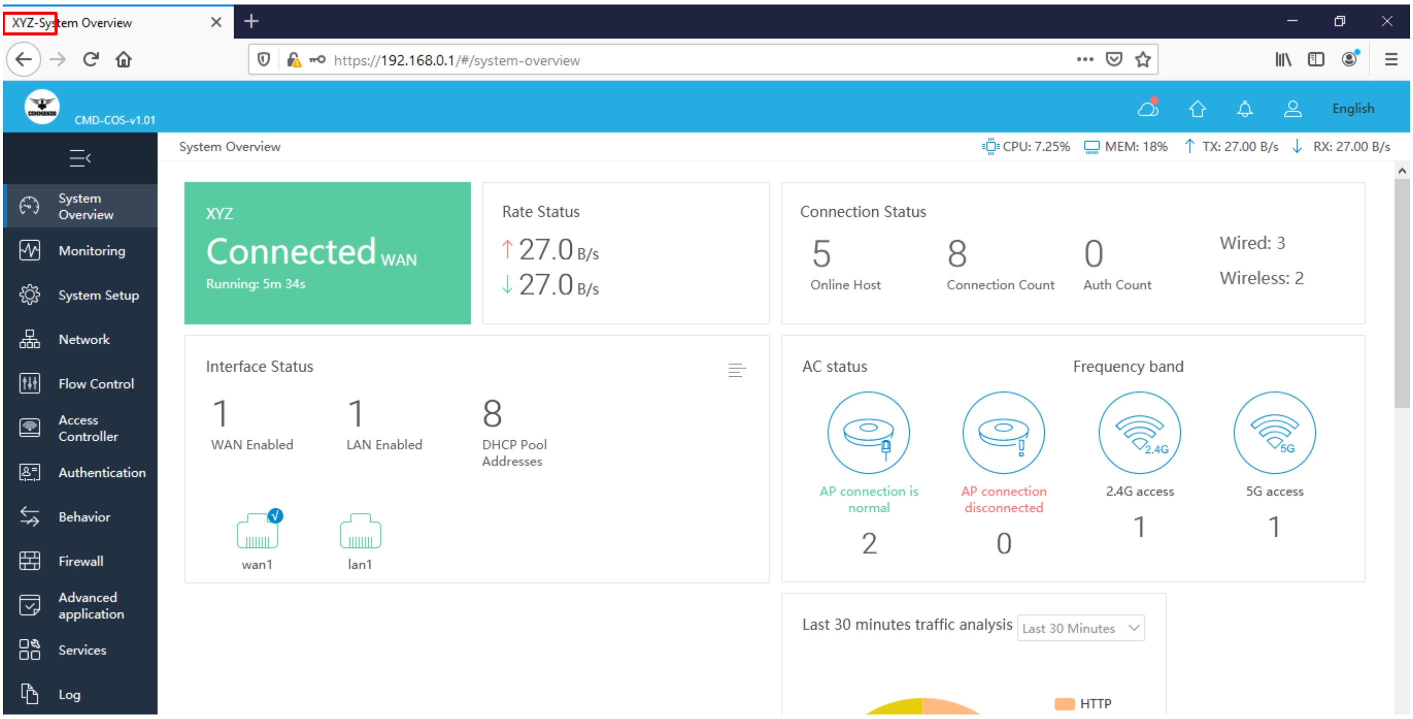
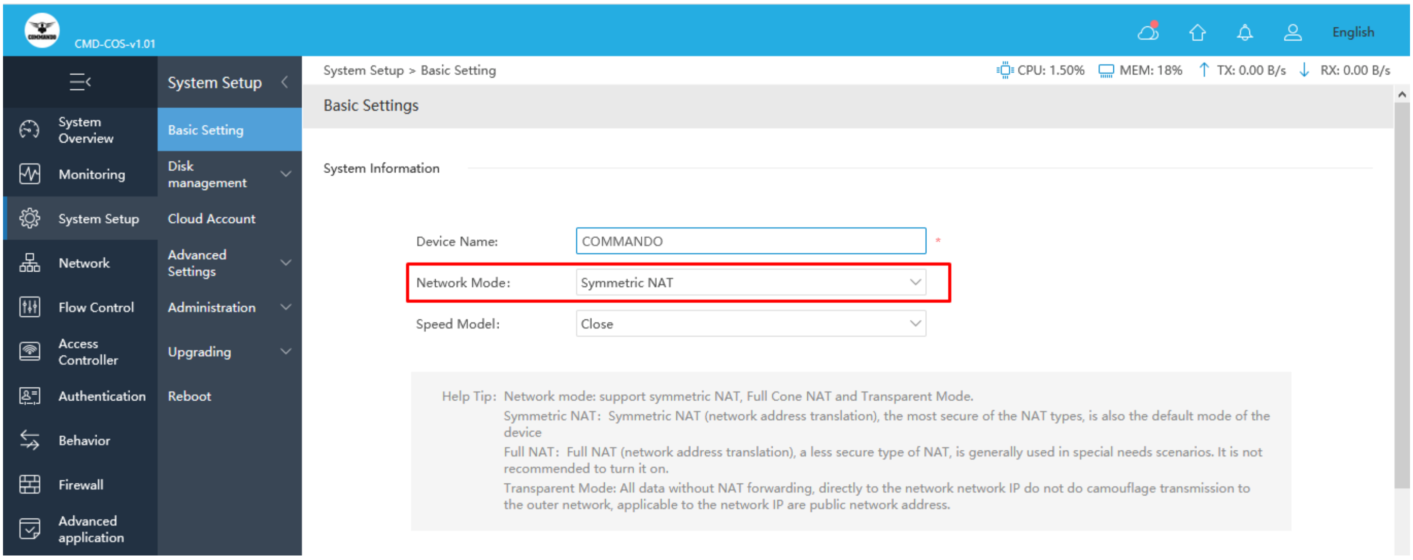


Fig 2.1.3 XYZ Device name page

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.



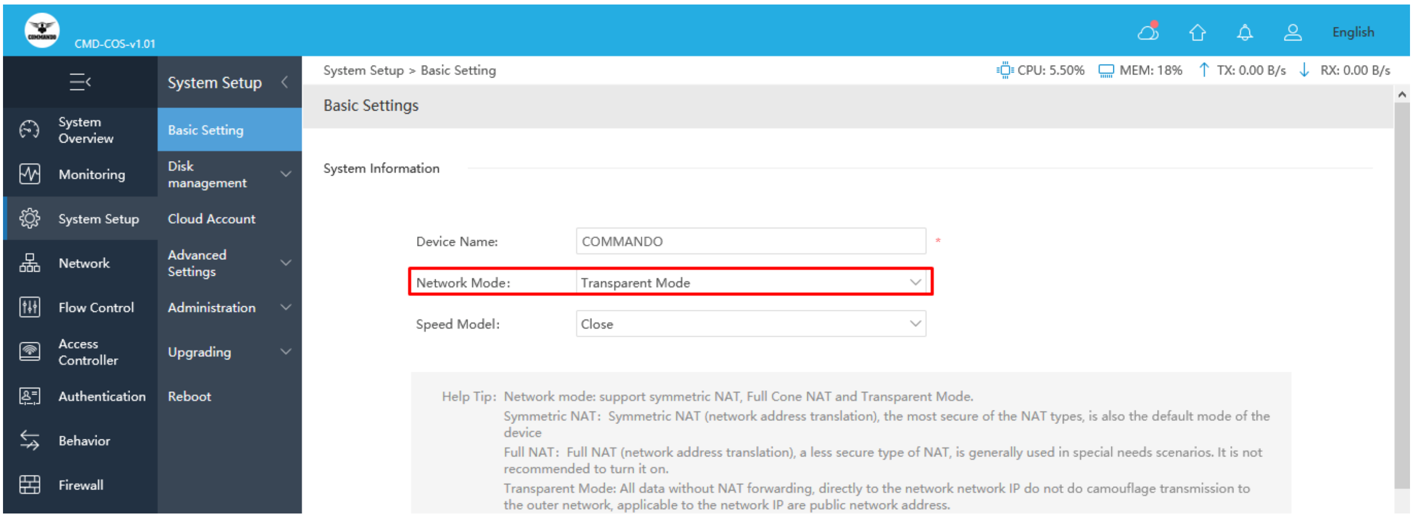
Device Name: COMMANDO *

Network Mode: Symmetric NAT

Speed Model: Close

Help Tip: Network mode: support symmetric NAT, Full Cone NAT and Transparent Mode.
Symmetric NAT: Symmetric NAT (network address translation), the most secure of the NAT types, is also the default mode of the device
Full NAT: Full NAT (network address translation), a less secure type of NAT, is generally used in special needs scenarios. It is not recommended to turn it on.
Transparent Mode: All data without NAT forwarding, directly to the network 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



Device Name: COMMANDO *

Network Mode: Transparent Mode

Speed Model: Close

Help Tip: Network mode: support symmetric NAT, Full Cone NAT and Transparent Mode.
Symmetric NAT: Symmetric NAT (network address translation), the most secure of the NAT types, is also the default mode of the device
Full NAT: Full NAT (network address translation), a less secure type of NAT, is generally used in special needs scenarios. It is not recommended to turn it on.
Transparent Mode: All data without NAT forwarding, directly to the network network IP do not do camouflage transmission to the outer network, applicable to the network IP are public network address.

Fig 2.1.5 Changing network mode Symmetric mode to Transparent mode page

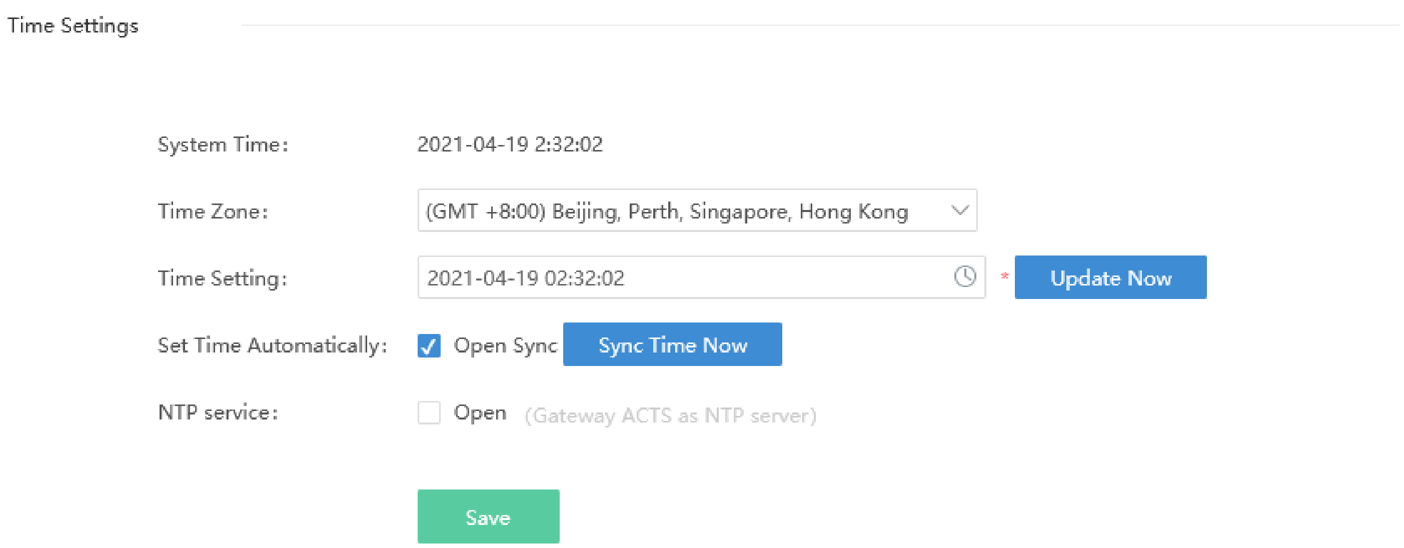
Time setting:

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.



Time Settings

System Time: 2021-04-19 2:32:02

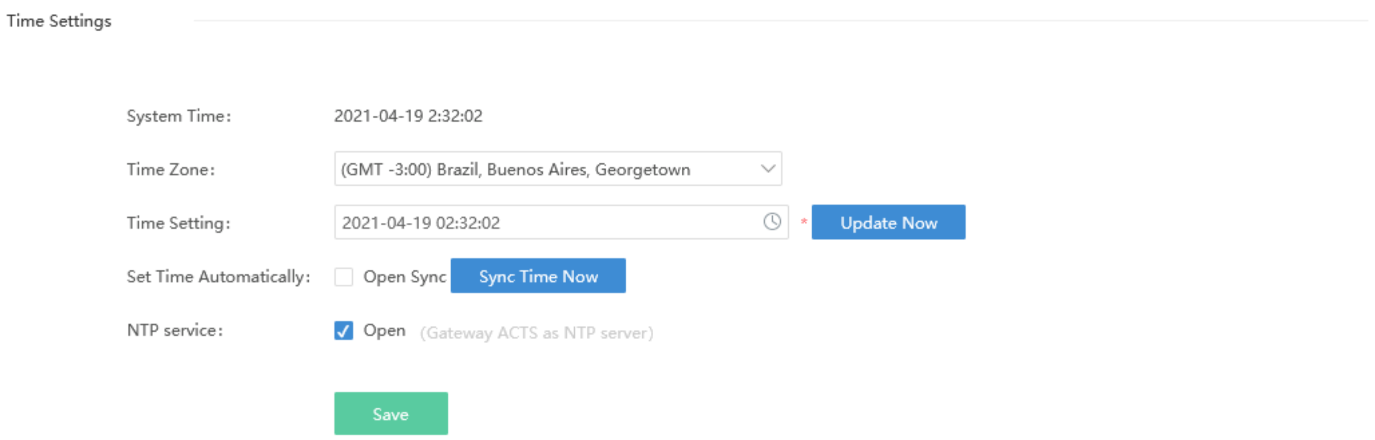
Time Zone: (GMT +8:00) Beijing, Perth, Singapore, Hong Kong

Time Setting: 2021-04-19 02:32:02 *

Set Time Automatically: ☑ Open Sync

NTP service: □ Open (Gateway ACTS as NTP server)

Fig 2.1.6 Time Settings with Sync time now option page



Time Settings

System Time: 2021-04-19 2:32:02

Time Zone: (GMT -3:00) Brazil, Buenos Aires, Georgetown

Time Setting: 2021-04-19 02:32:02 *

Set Time Automatically: □ Open Sync

NTP service: ☑ Open (Gateway ACTS as NTP server)

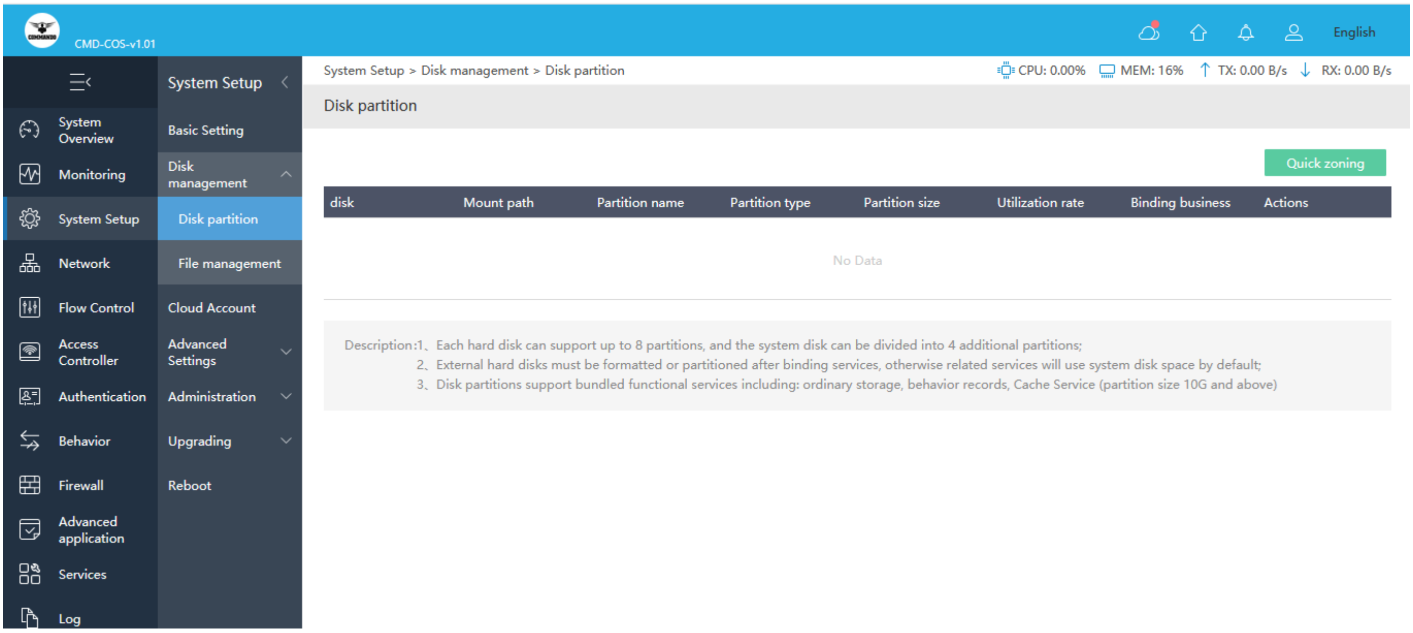
Fig 2.1.7 Time Settings with NTP service and changing Time zone page

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

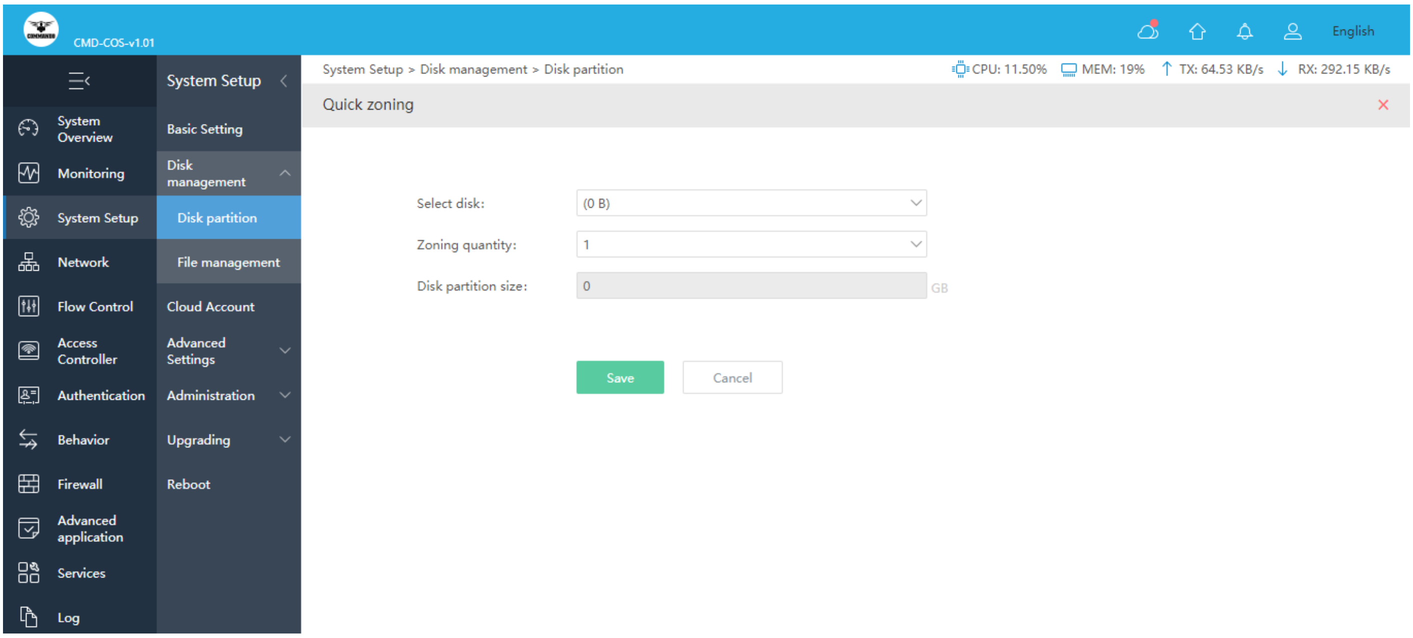


disk	Mount path	Partition name	Partition type	Partition size	Utilization rate	Binding business	Actions

No Data

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

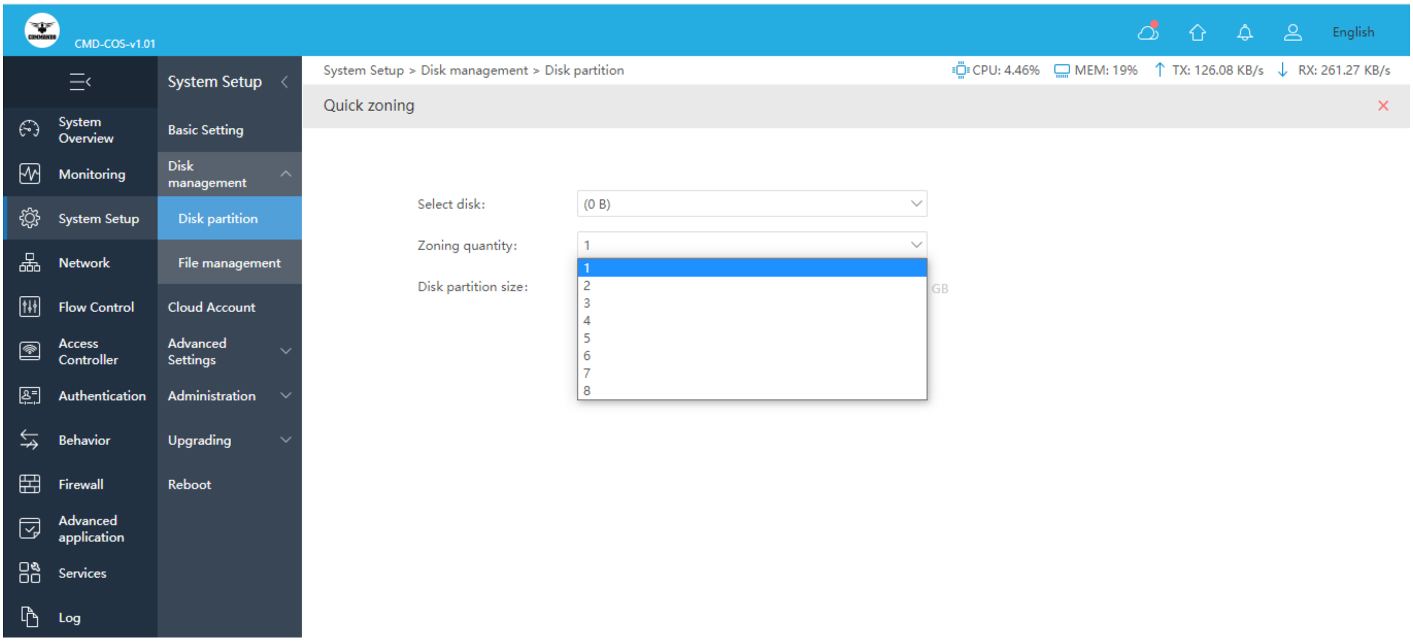


Select disk: (0 B)

Zoning quantity: 1

Disk partition size: 0 GB

Fig 2.2.2 Disk partition quick zoning page



System Setup > Disk management > Disk partition

CPU: 4.46% MEM: 19% TX: 126.08 KB/s RX: 261.27 KB/s

Quick zoning

Select disk: (0 B)

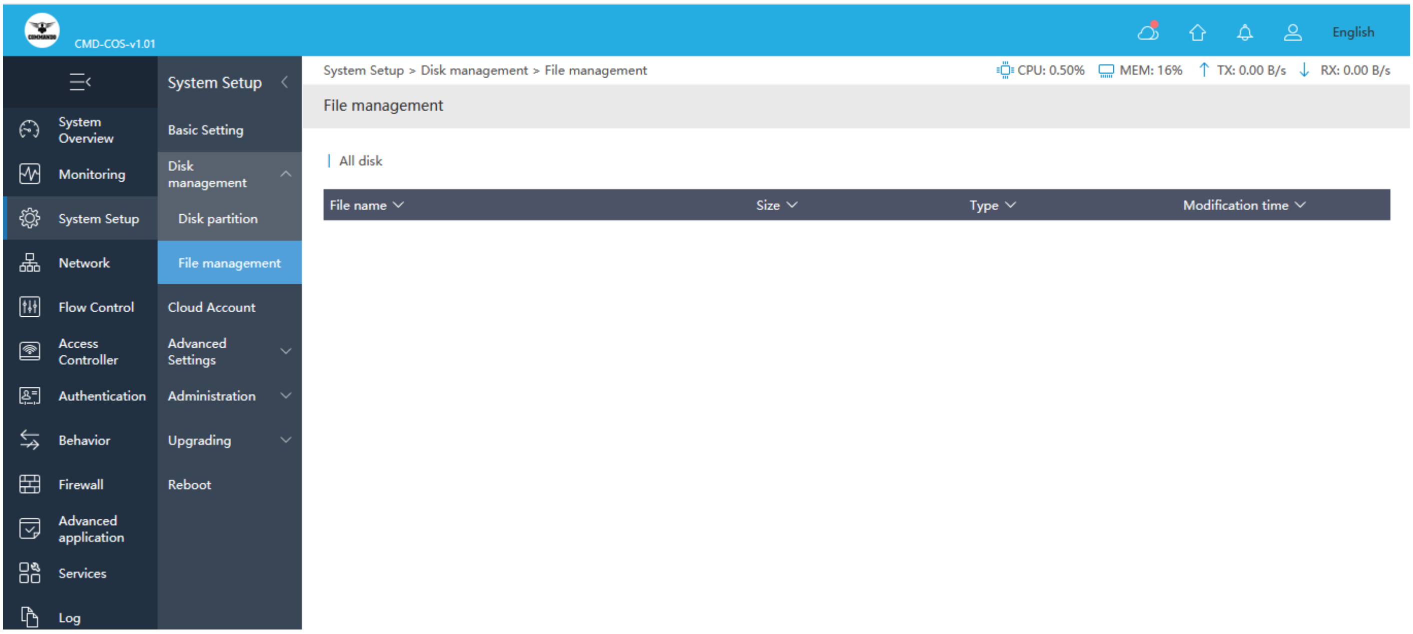
Zoning quantity: 1

Disk partition size:

1
2
3
4
5
6
7
8

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



System Setup > Disk management > File management

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

File management

All disk

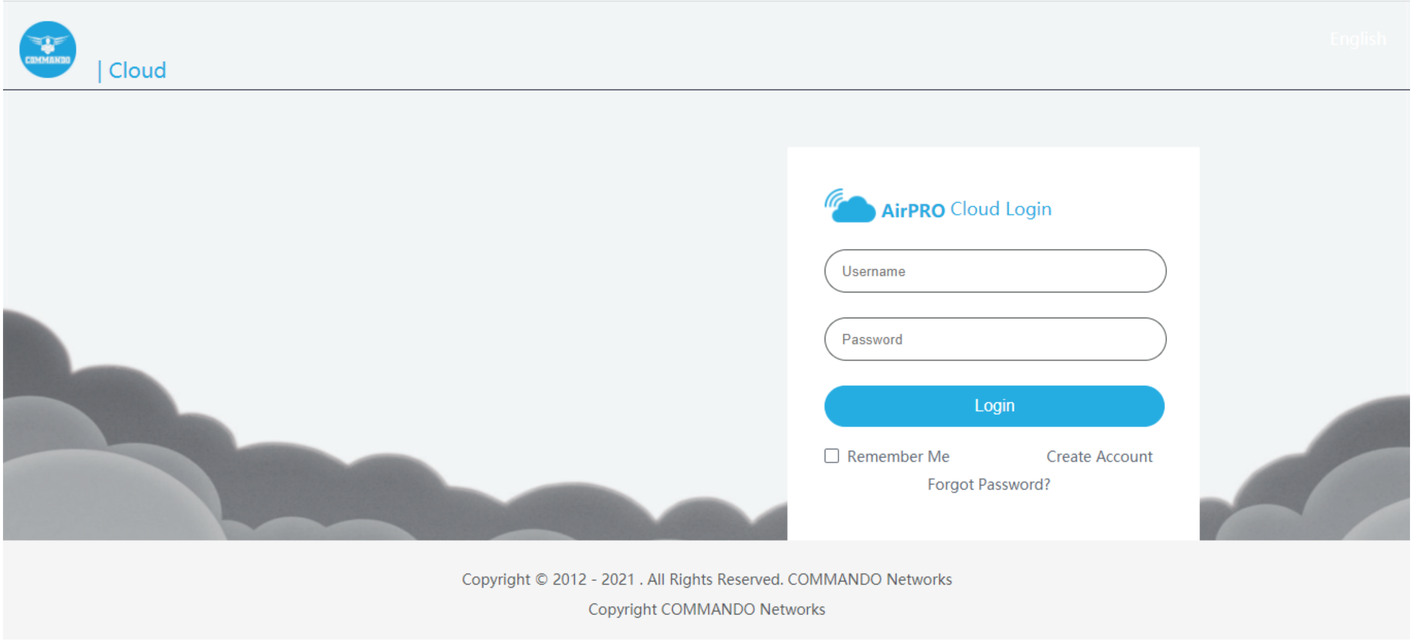
File name	Size	Type	Modification time

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 word.



Copyright © 2012 - 2021 . All Rights Reserved. COMMANDO Networks

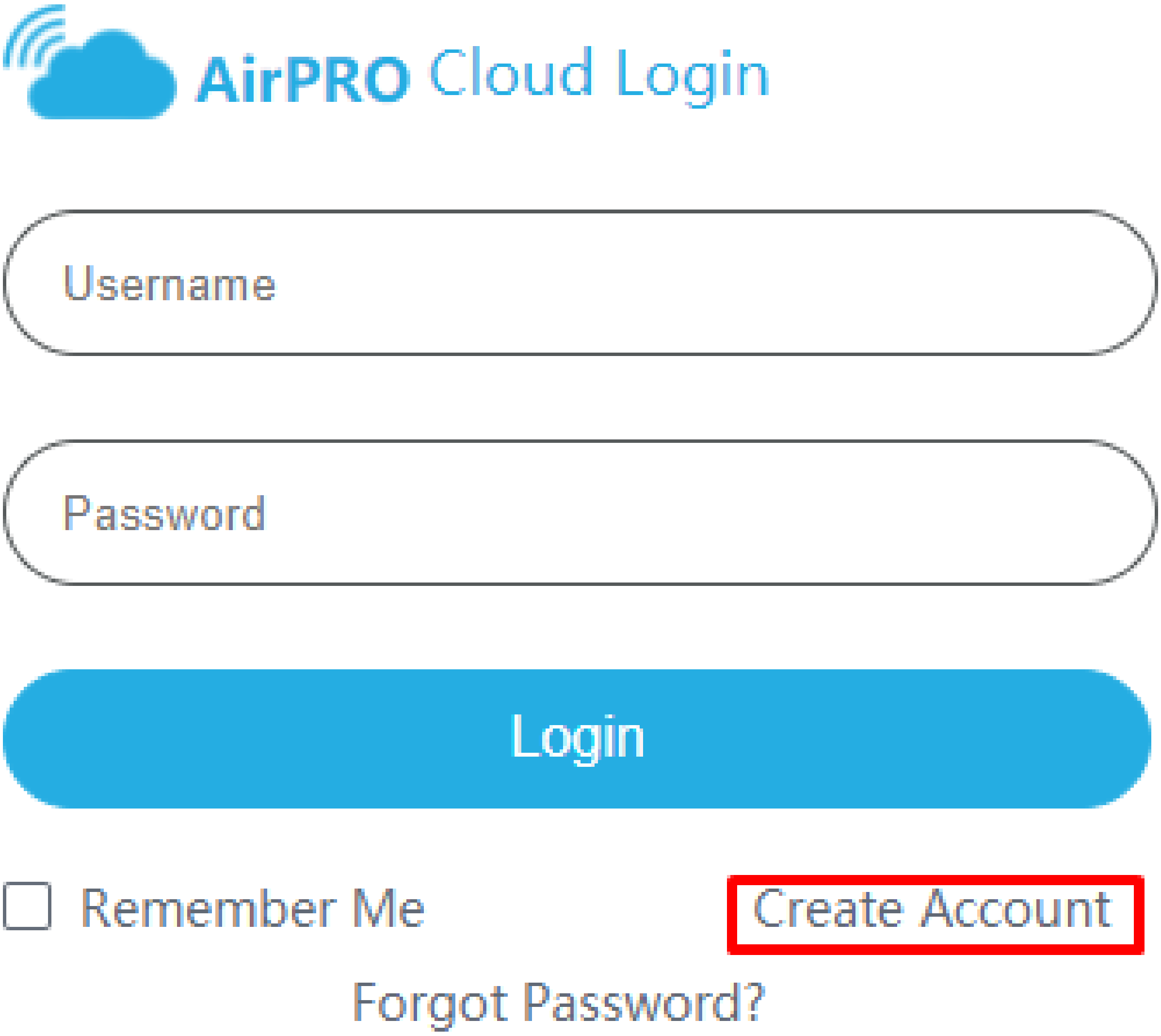
Copyright COMMANDO Networks

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



AirPRO Cloud Login

Username

Password

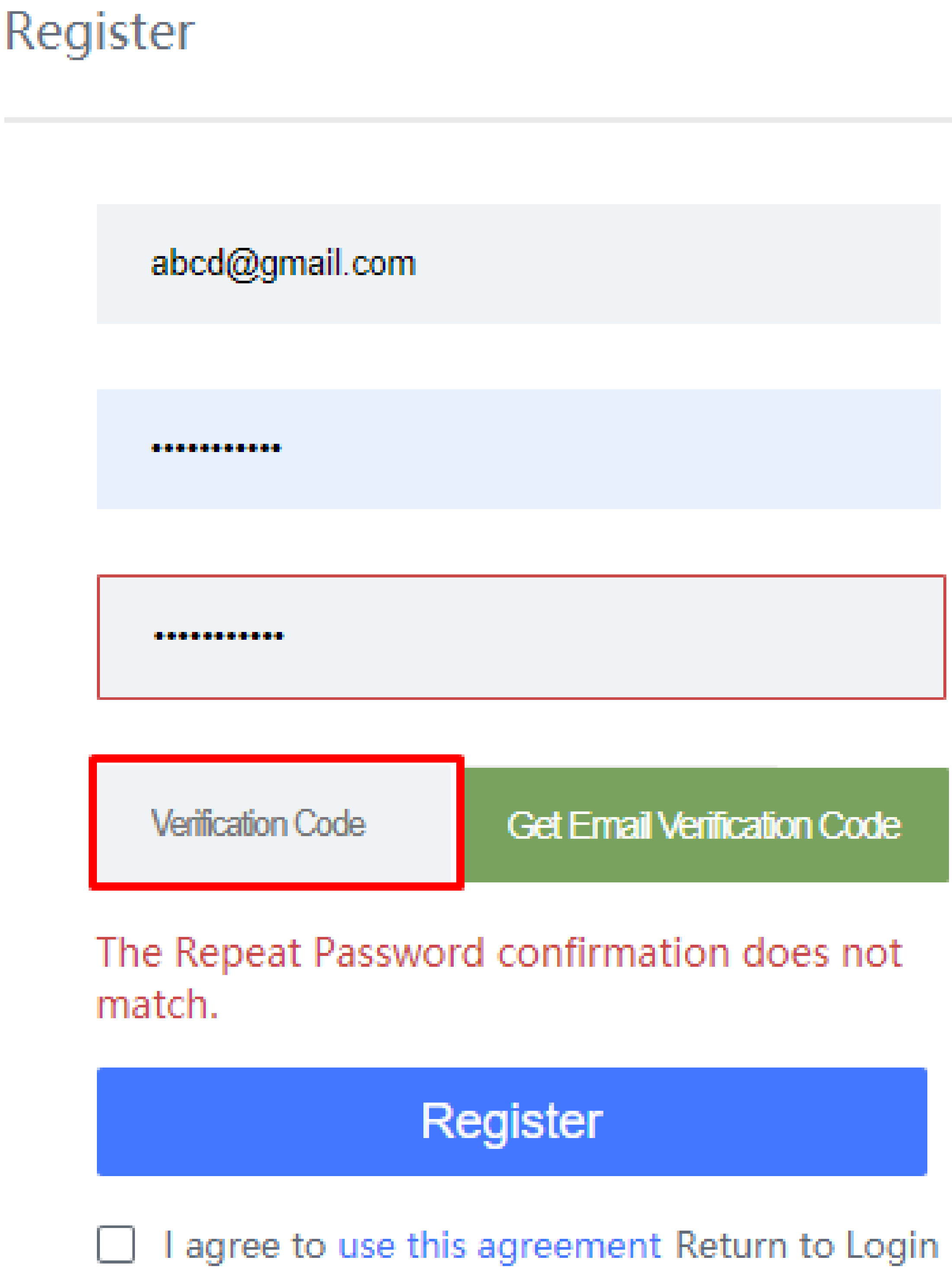
Login

□ Remember Me

Create Account

Forgot Password?

Fig 2.3.2 Create Cloud Login account page



Register

abcd@gmail.com

••••••••••••

••••••••••••

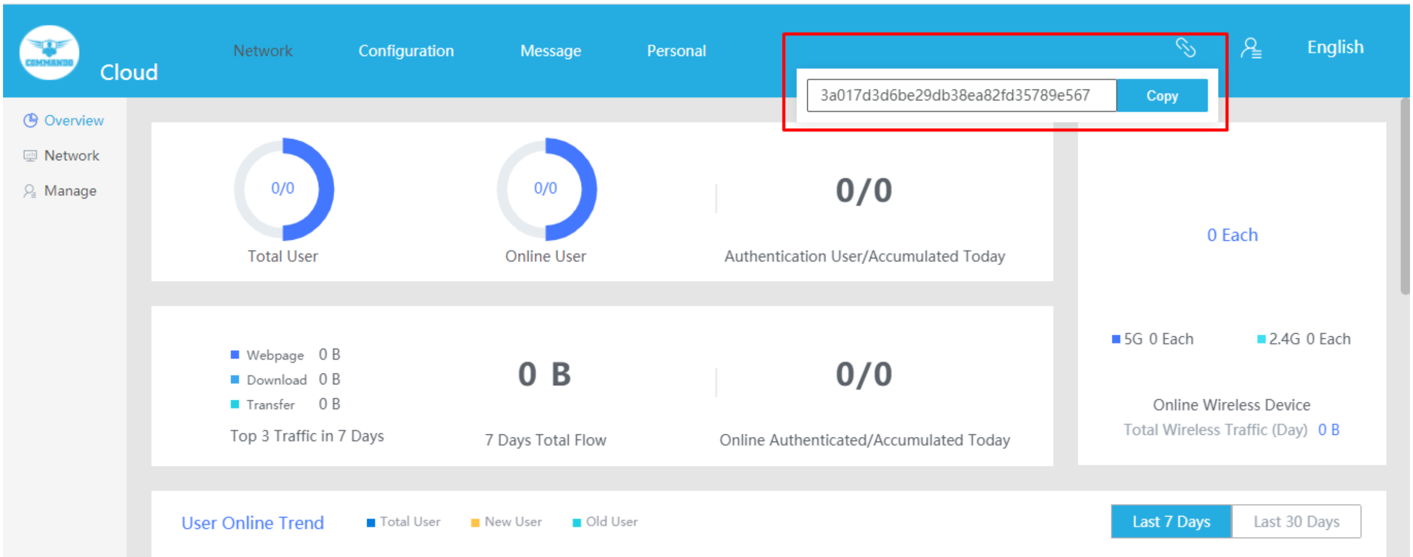
Verification Code
Get Email Verification Code

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

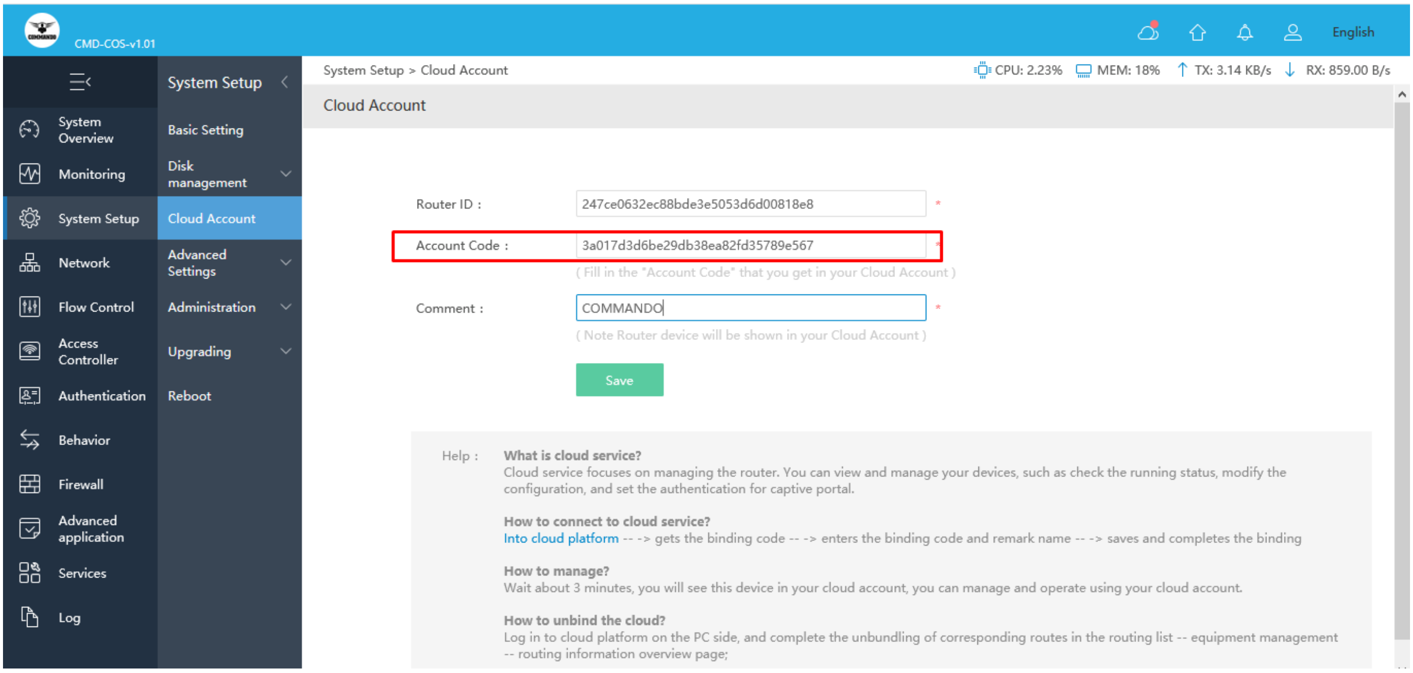
Provide Email ID, password as per your choice and get the verification code either in inbox or spam folder of Email which you submitted.



3a017d3d6be29db38ea82fd35789e567 Copy

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



System Setup > Cloud Account

Cloud Account

Router ID : 247ce0632ec88bde3e5053d6d00818e8 *

Account Code : 3a017d3d6be29db38ea82fd35789e567 *

(Fill in the "Account Code" that you get in your Cloud Account)

Comment : COMMANDO *

(Note Router device will be shown in your Cloud Account)

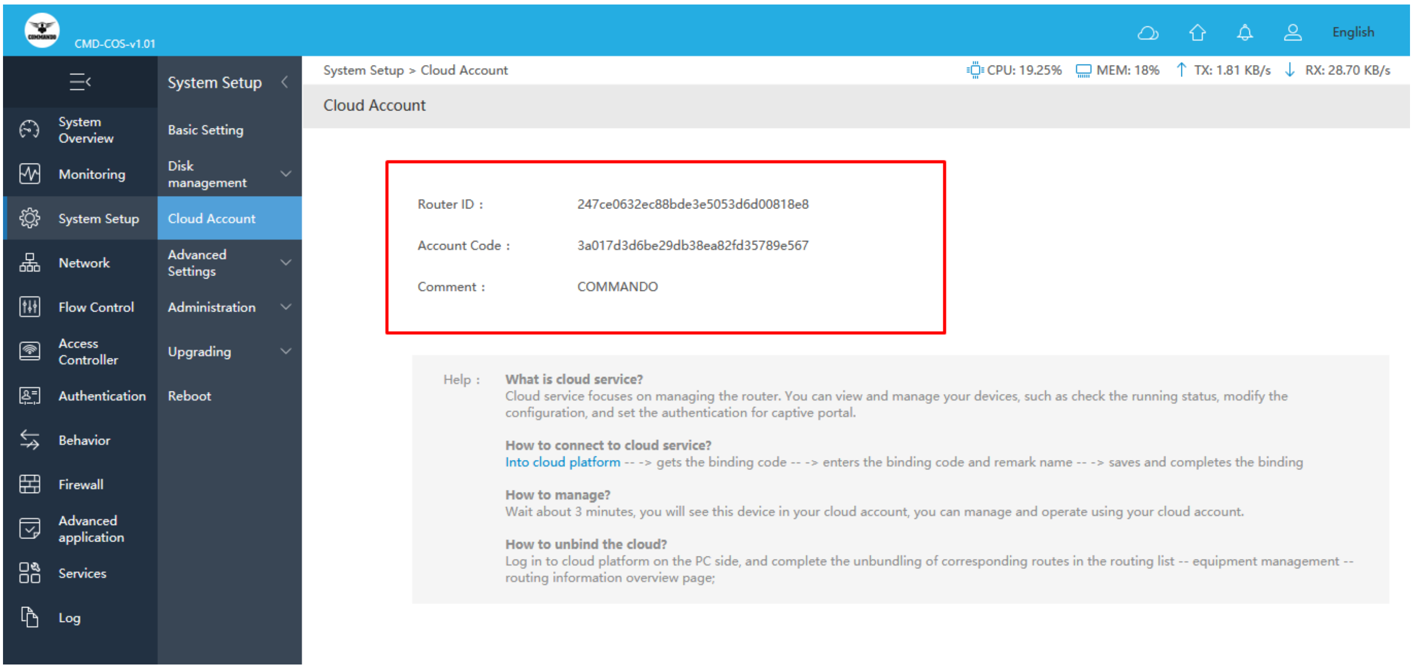
Help : **What is cloud service?**
Cloud service focuses on managing the router. You can view and manage your devices, such as check the running status, modify the configuration, and set the authentication for captive portal.

How to connect to cloud service?
Into cloud platform -- -> gets the binding code -- -> enters the binding code 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 2.3.5 Binding code R100 router with cloud portal page



Cloud Account

Router ID : 247ce0632ec88bde3e5053d6d00818e8

Account Code : 3a017d3d6be29db38ea82fd35789e567

Comment : COMMANDO

Help :

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 -- -> gets the binding code -- -> enters the binding code 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 2.3.6 After Binding R100 router with cloud page

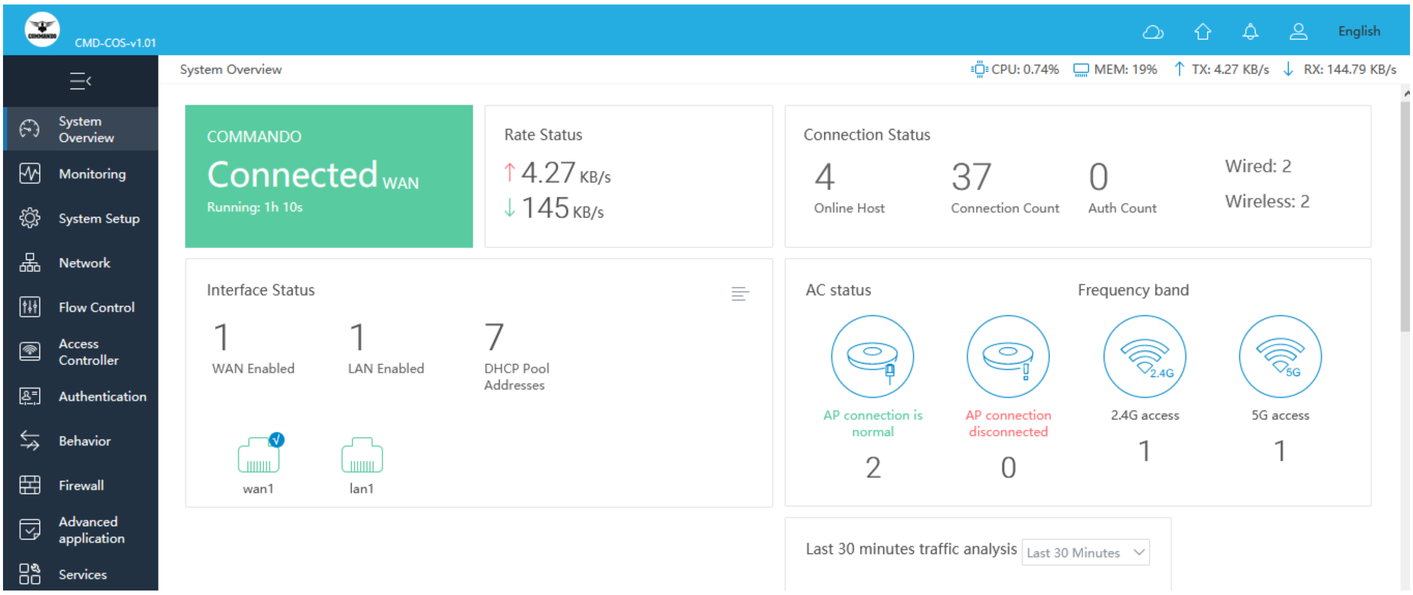


Fig 2.3.7 Normal R100 router system overview page

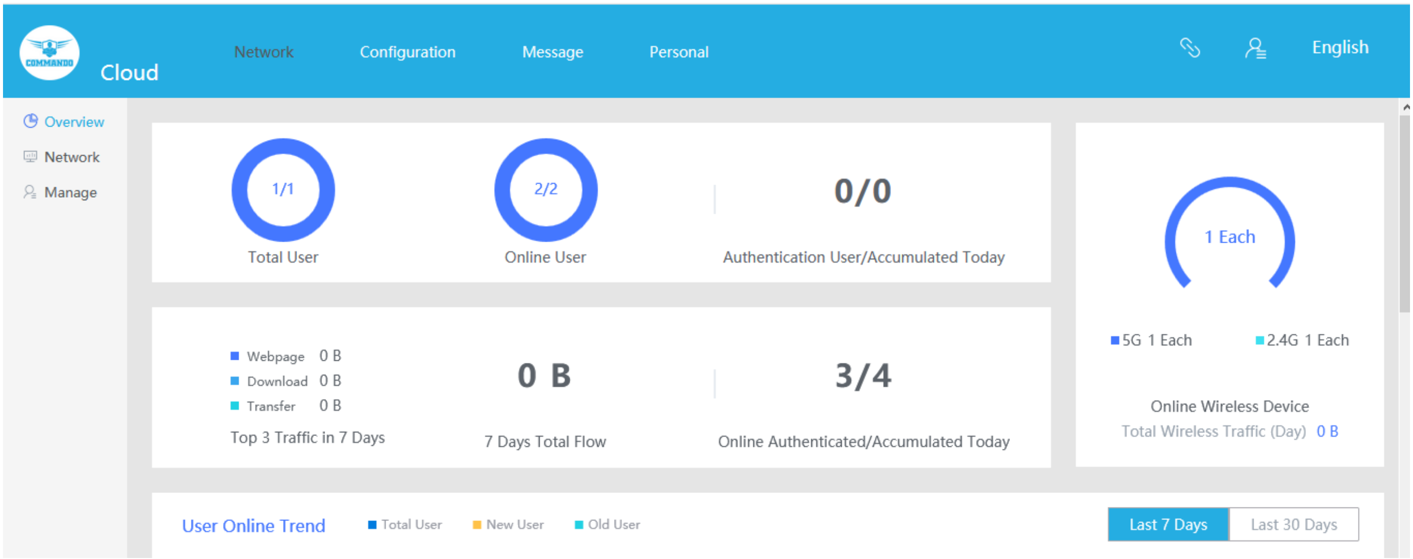
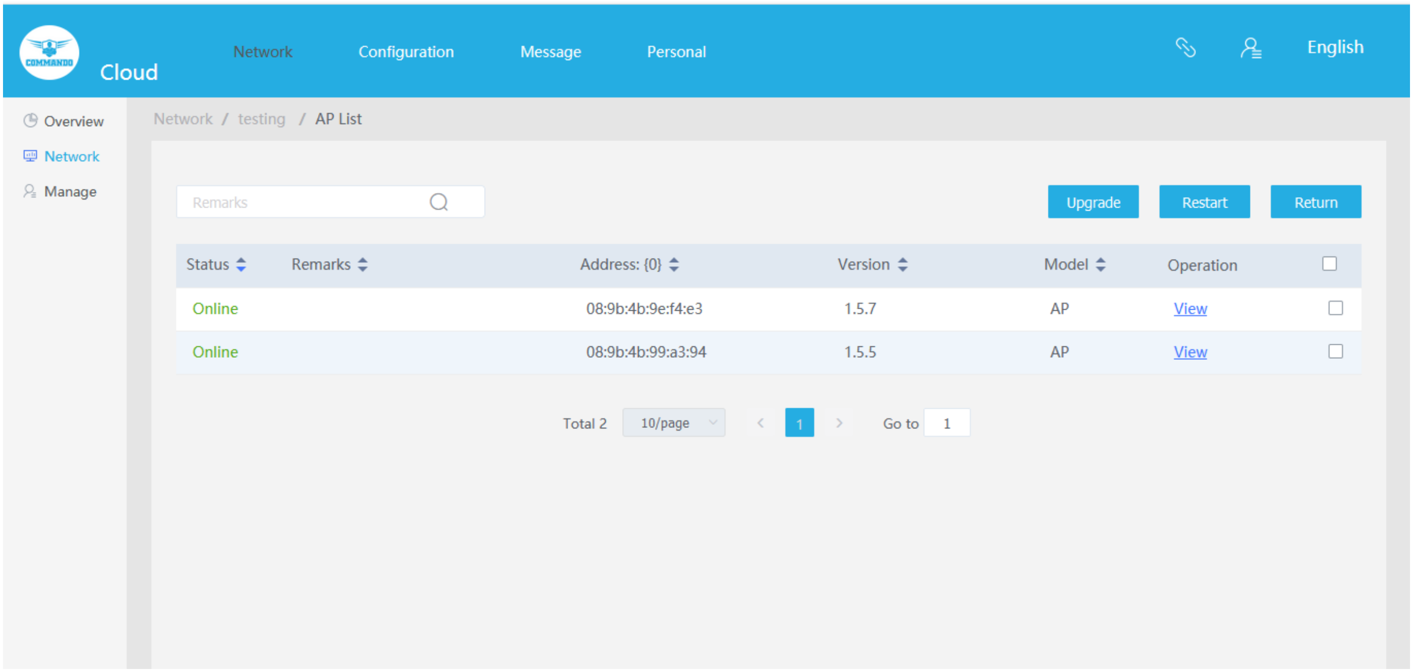


Fig 2.3.8 Cloud access of R100 router with cloud page



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

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.

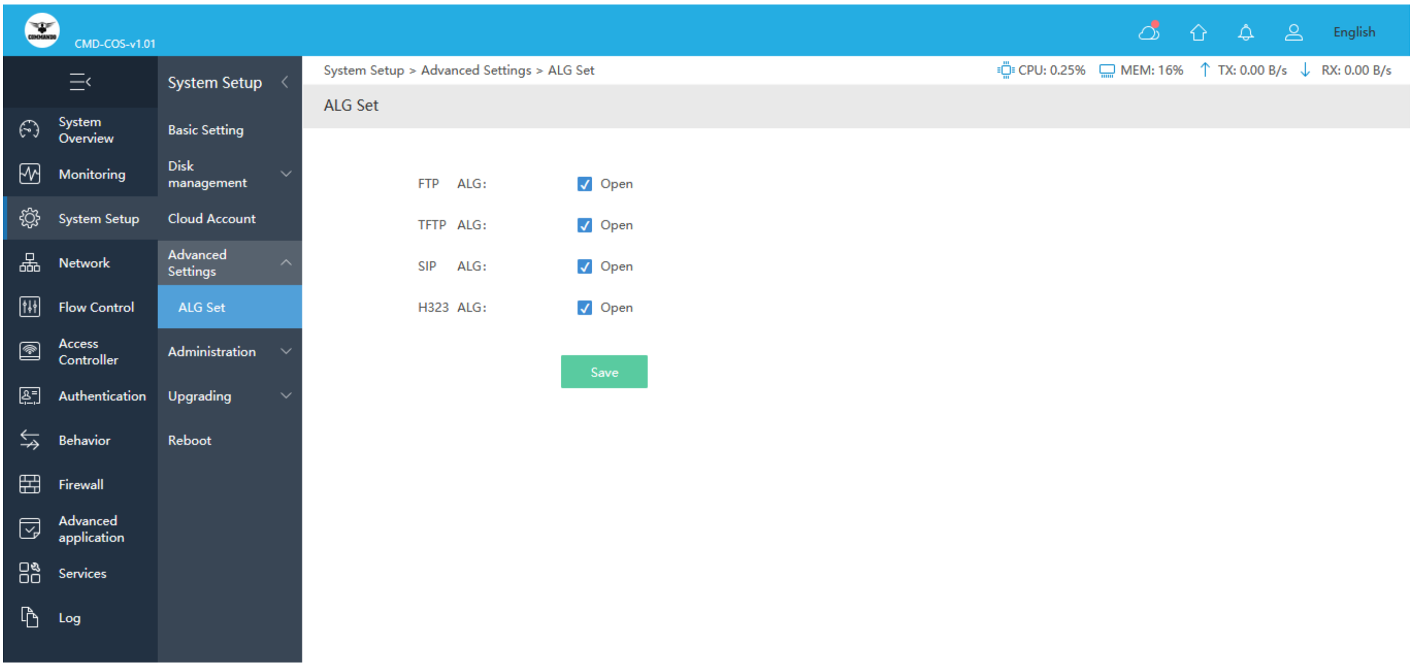
How to unbind the cloud?

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



ALG Set

FTP ALG: ☑ Open

TFTP ALG: ☑ Open

SIP ALG: ☑ Open

H323 ALG: ☑ Open

Fig 2.4.1 ALG set page

5. Administration

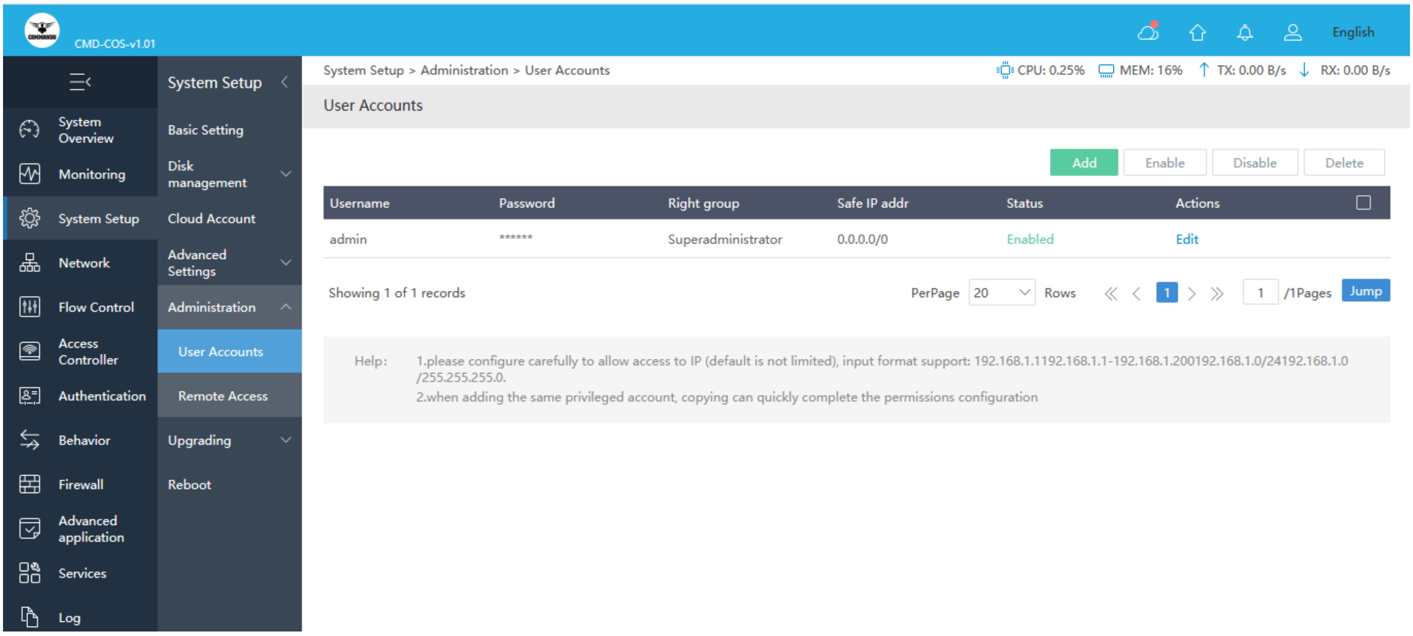
On this page, you can modify the factory default username and password of the Router and create multiple new users and passwords with specific access profiles and rights to manage the device. You can also allow telnet or remote WEB access of device.

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



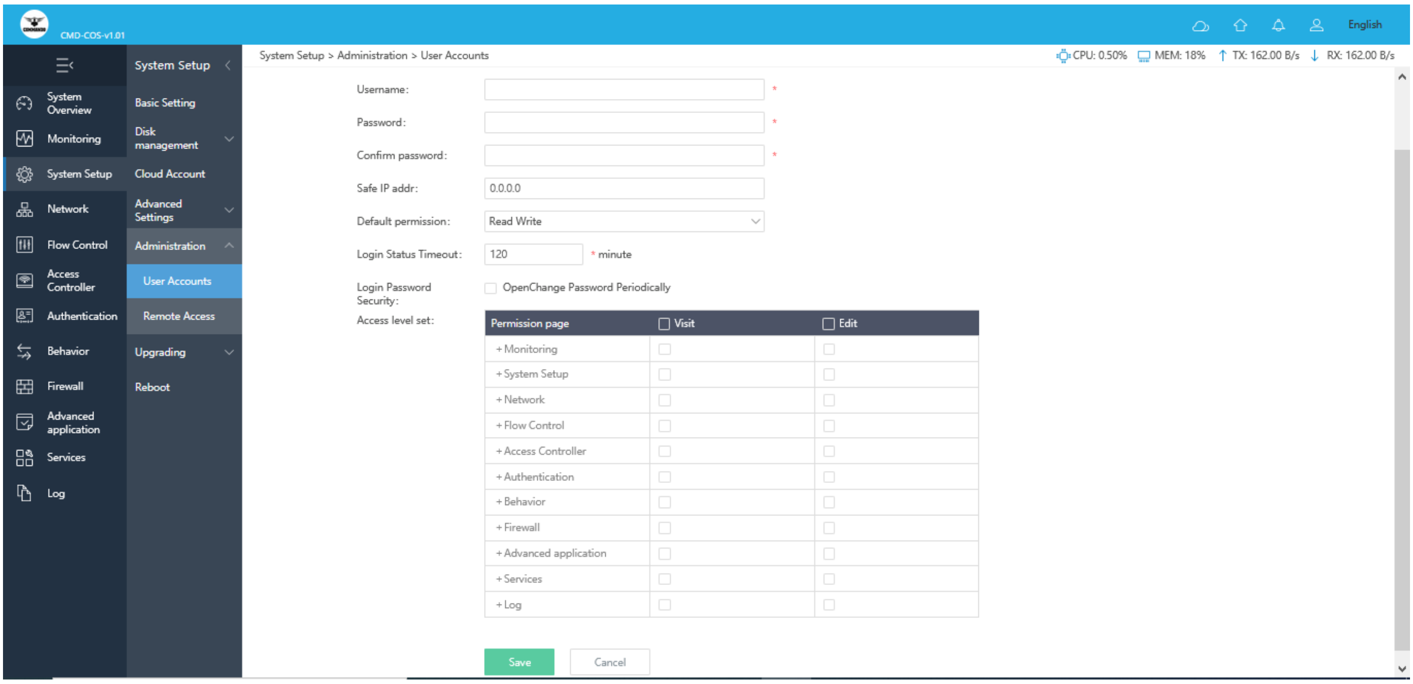
User Accounts

Username	Password	Right group	Safe IP addr	Status	Actions	□
admin	******	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 2.5.1 Default User Accounts page



Username: *

Password: *

Confirm password: *

Safe IP addr: 0.0.0.0

Default permission: Read Write

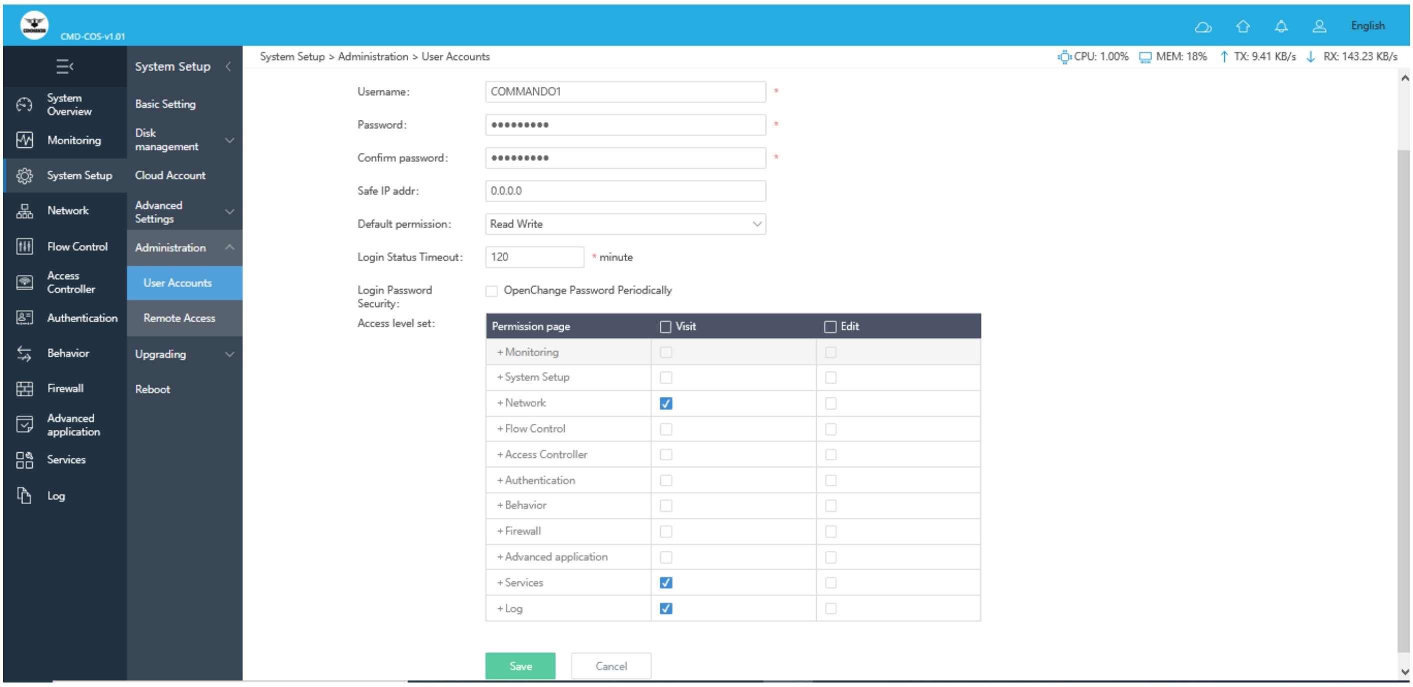
Login Status Timeout: 120 * minute

Login Password Security: □ OpenChange Password Periodically

Access level set:

Permission page	□ Visit	□ Edit
+ Monitoring	□	□
+ System Setup	□	□
+ Network	□	□
+ Flow Control	□	□
+ Access Controller	□	□
+ Authentication	□	□
+ Behavior	□	□
+ Firewall	□	□
+ Advanced application	□	□
+ Services	□	□
+ Log	□	□

Fig 2.5.2 Add User Accounts page



Username: COMMANDO1 *

Password: ●●●●●●●●● *

Confirm password: ●●●●●●●●● *

Safe IP addr: 0.0.0.0

Default permission: Read Write

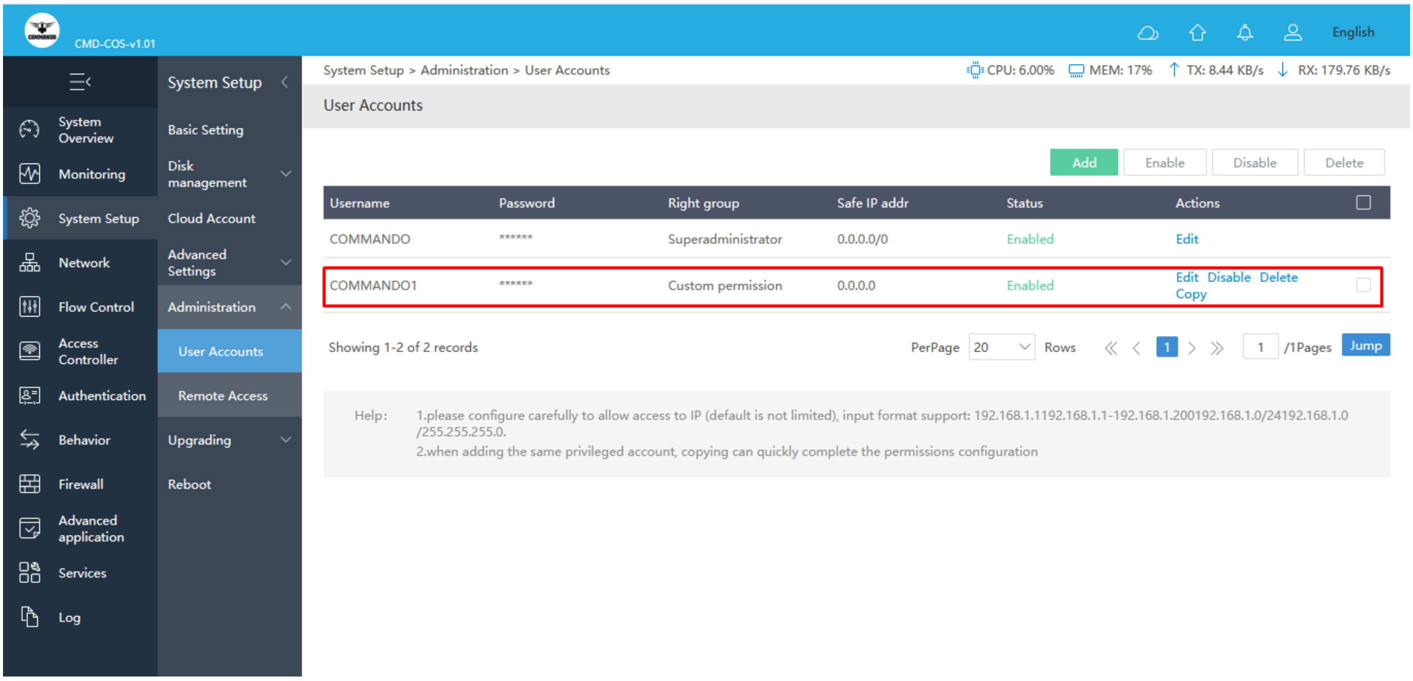
Login Status Timeout: 120 * minute

Login Password Security: □ OpenChange Password Periodically

Access level set:

Permission page	□ Visit	□ Edit
+Monitoring	□	□
+System Setup	□	□
+Network	☑	□
+Flow Control	□	□
+Access Controller	□	□
+Authentication	□	□
+Behavior	□	□
+Firewall	□	□
+Advanced application	□	□
+Services	☑	□
+Log	☑	□

Fig 2.5.3 Add User Account with visit permission page



Username	Password	Right group	Safe IP addr	Status	Actions	□
COMMANDO	******	Superadministrator	0.0.0.0/0	Enabled	Edit	
COMMANDO1	******	Custom permission	0.0.0.0	Enabled	Edit Disable Delete Copy	□

Showing 1-2 of 2 records PerPage 20 Rows 1 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 2.5.4 User Account COMMANDO1 with visit permission page

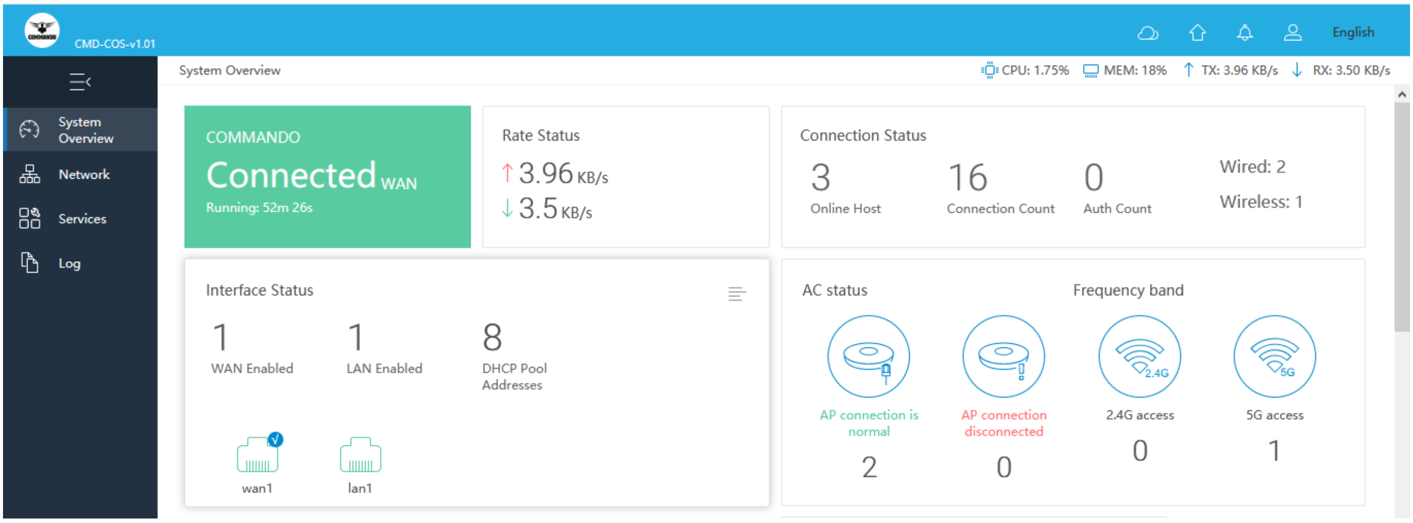
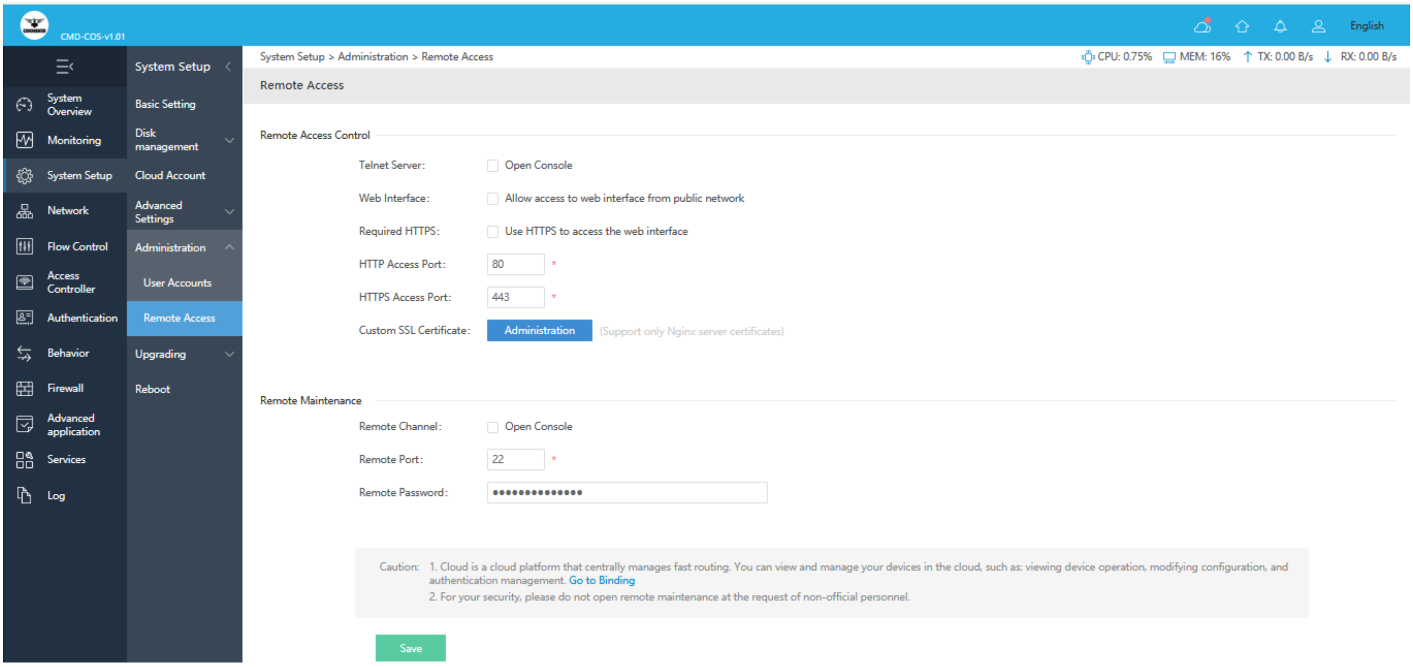


Fig 2.5.6 Customized access as per User Account COMMANDO1 with visit permission page

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



System Setup > Administration > Remote Access

Remote Access

Remote Access Control

Telnet Server: □ Open Console

Web Interface: □ Allow access to web interface from public network

Required HTTPS: □ Use HTTPS to access the web interface

HTTP Access Port: 80 *

HTTPS Access Port: 443 *

Custom SSL Certificate: (Support only Nginx server certificates)

Remote Maintenance

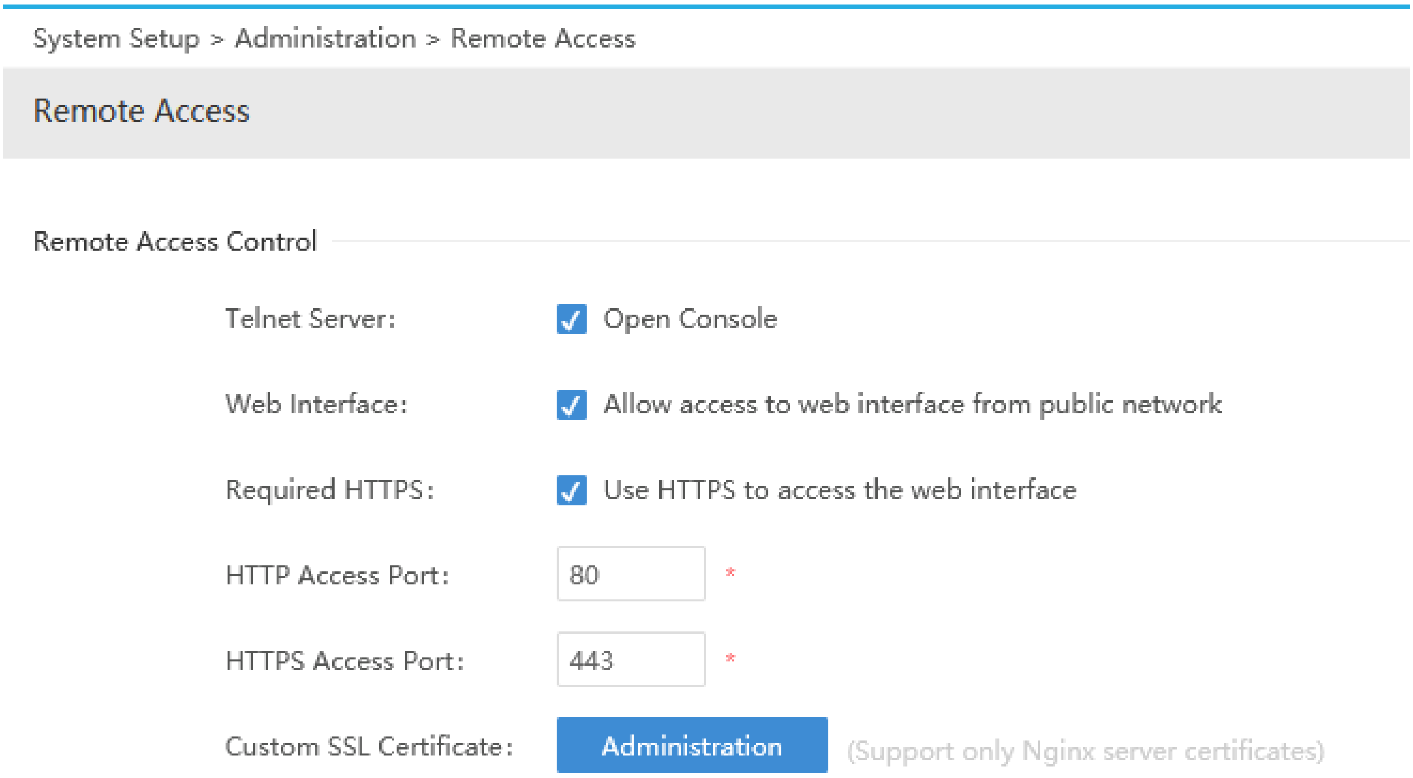
Remote Channel: □ Open Console

Remote Port: 22 *

Remote Password: ••••••••••••••

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 2.5.7 Remote Access control page



System Setup > Administration > Remote Access

Remote Access

Remote Access Control

Telnet Server: ☑ Open Console

Web Interface: ☑ Allow access to web interface from public network

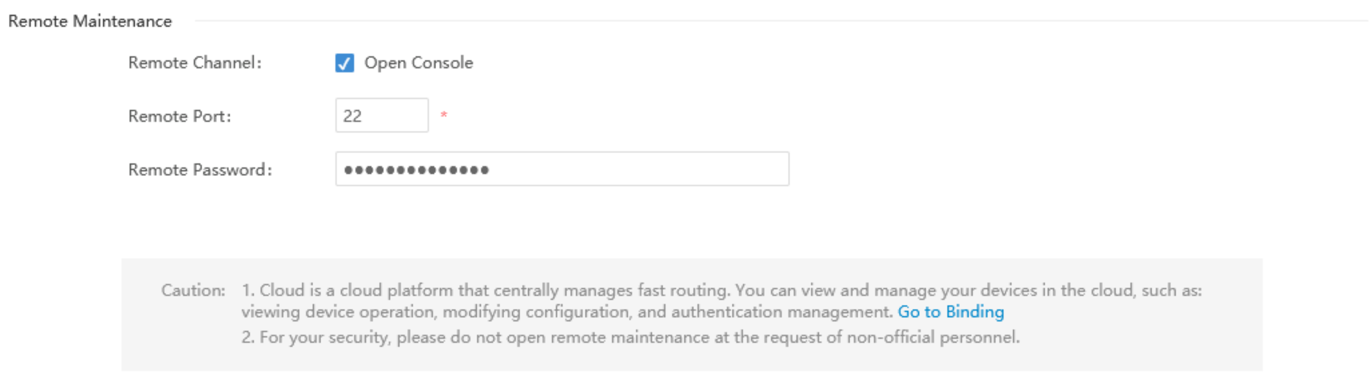
Required HTTPS: ☑ Use HTTPS to access the web interface

HTTP Access Port: 80 *

HTTPS Access Port: 443 *

Custom SSL Certificate: Administration (Support only Nginx server certificates)

Fig 2.5.8 Enabling Remote Access control page



Remote Maintenance

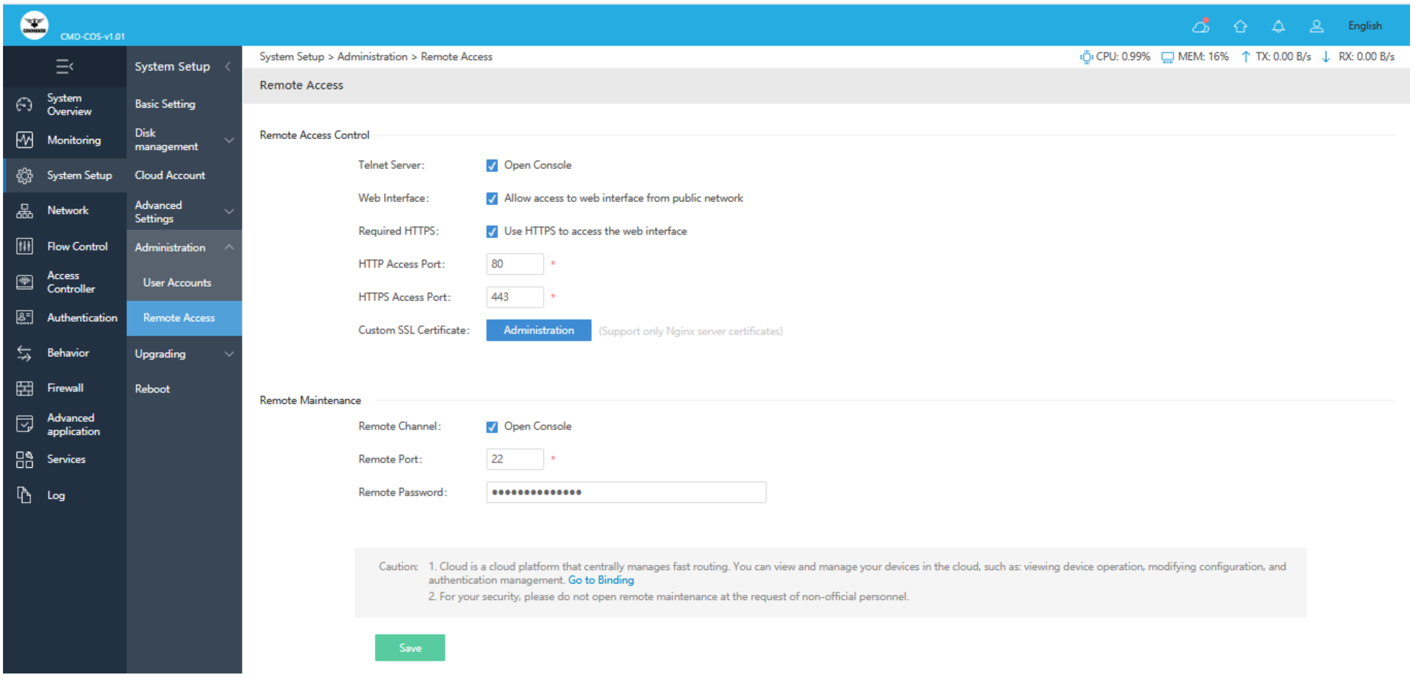
Remote Channel: ☑ Open Console

Remote Port: 22 *

Remote Password: ●●●●●●●●●●●●●●

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



System Setup > Administration > Remote Access

CPU: 0.99% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Remote Access

Remote Access Control

Telnet Server: ☑ Open Console

Web Interface: ☑ Allow access to web interface from public network

Required HTTPS: ☑ Use HTTPS to access the web interface

HTTP Access Port: 80 *

HTTPS Access Port: 443 *

Custom SSL Certificate: Administration (Support only Nginx server certificates)

Remote Maintenance

Remote Channel: ☑ Open Console

Remote Port: 22 *

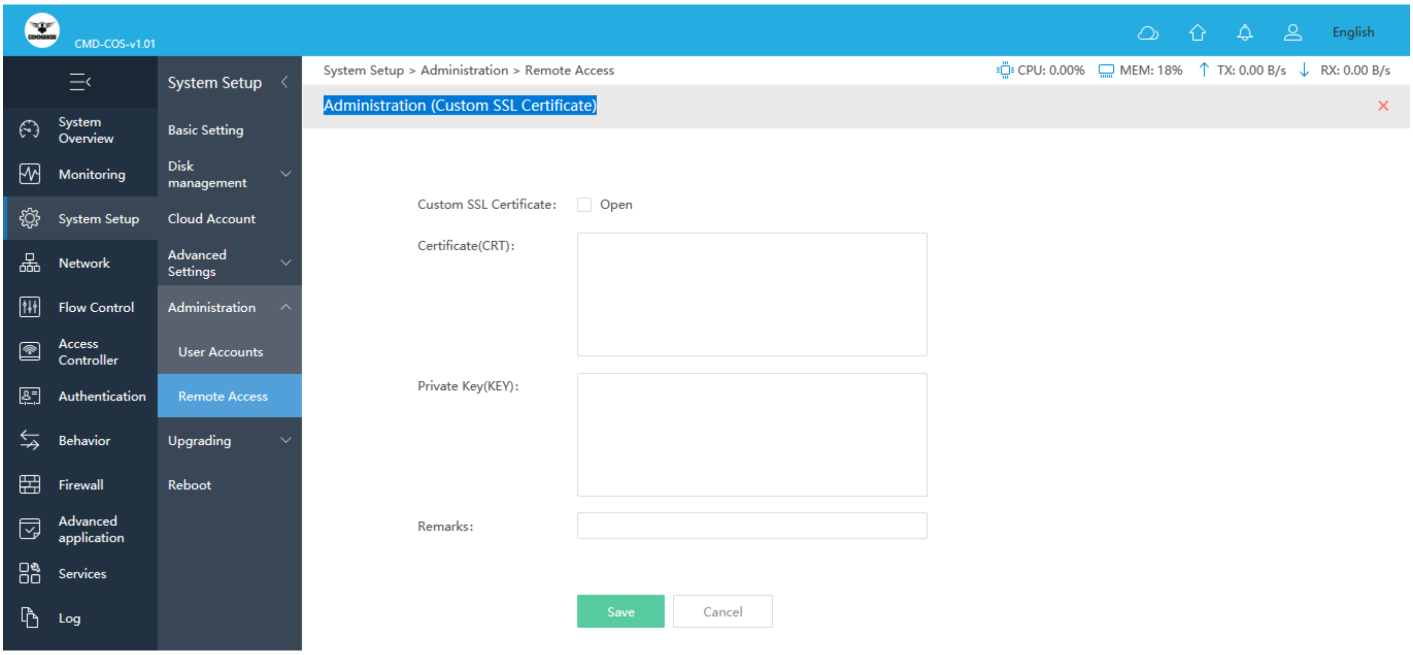
Remote Password: ••••••••••••••

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 2.5.10 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.



System Setup > Administration > Remote Access

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

Administration (Custom SSL Certificate)

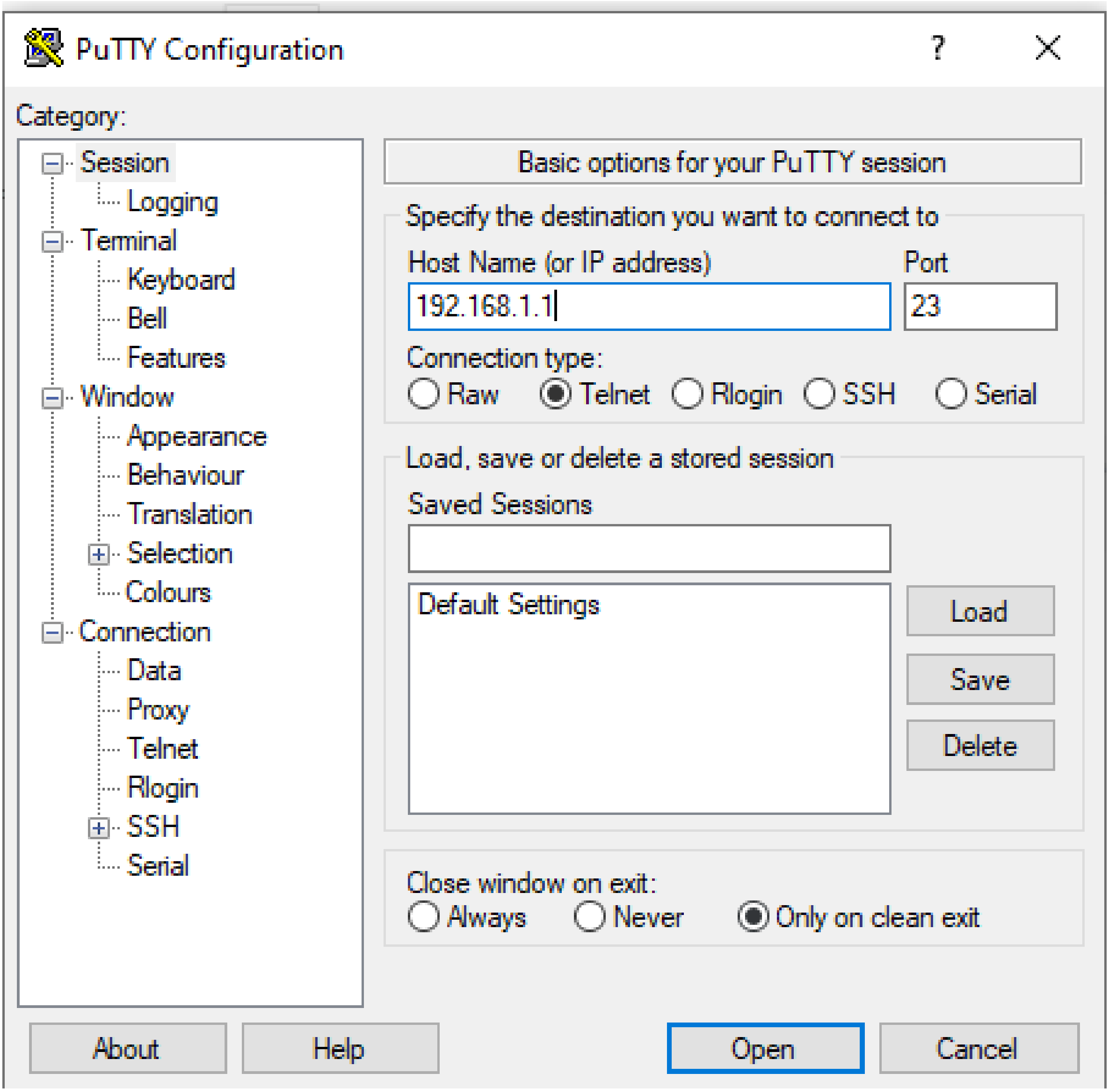
Custom SSL Certificate: □ Open

Certificate(CRT):

Private Key(KEY):

Remarks:

Fig 2.5.11 Administration (Custom SSL Certificate) page



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

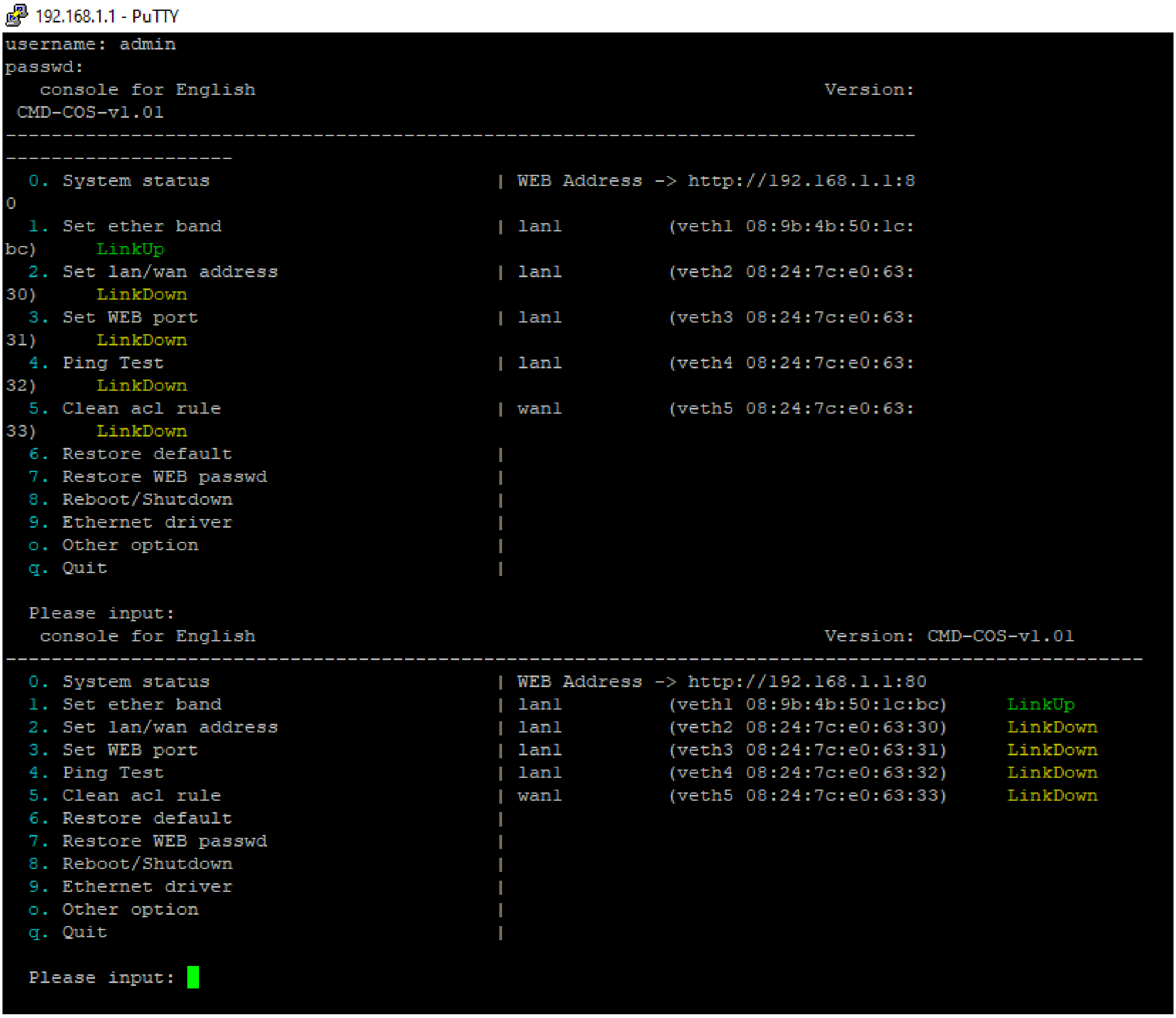
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Fig 2.5.12 Putty for Telnet access of device page



```
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.

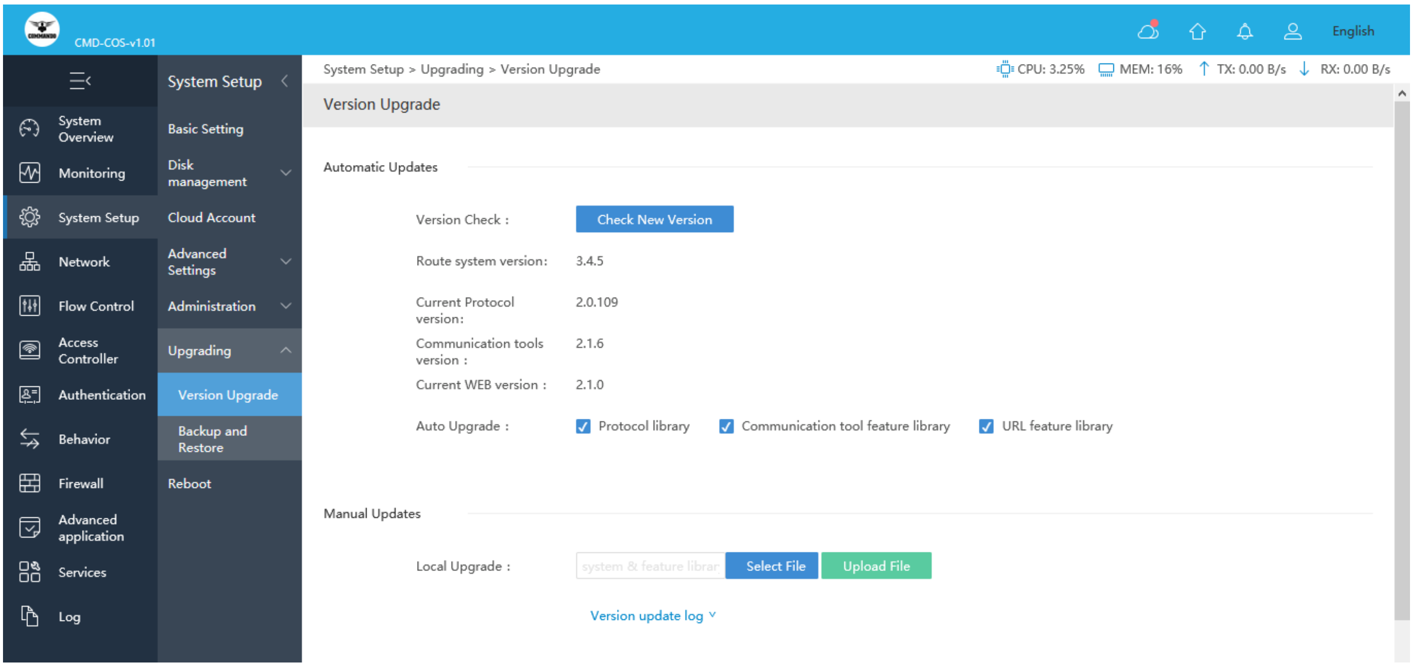
Note:

- 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.



Version Upgrade

Automatic Updates

Version Check :

Route system version: 3.4.5

Current Protocol version: 2.0.109

Communication tools version : 2.1.6

Current WEB version : 2.1.0

Auto Upgrade : ☑ Protocol library ☑ Communication tool feature library ☑ URL feature library

Manual Updates

Local Upgrade : system & feature librar

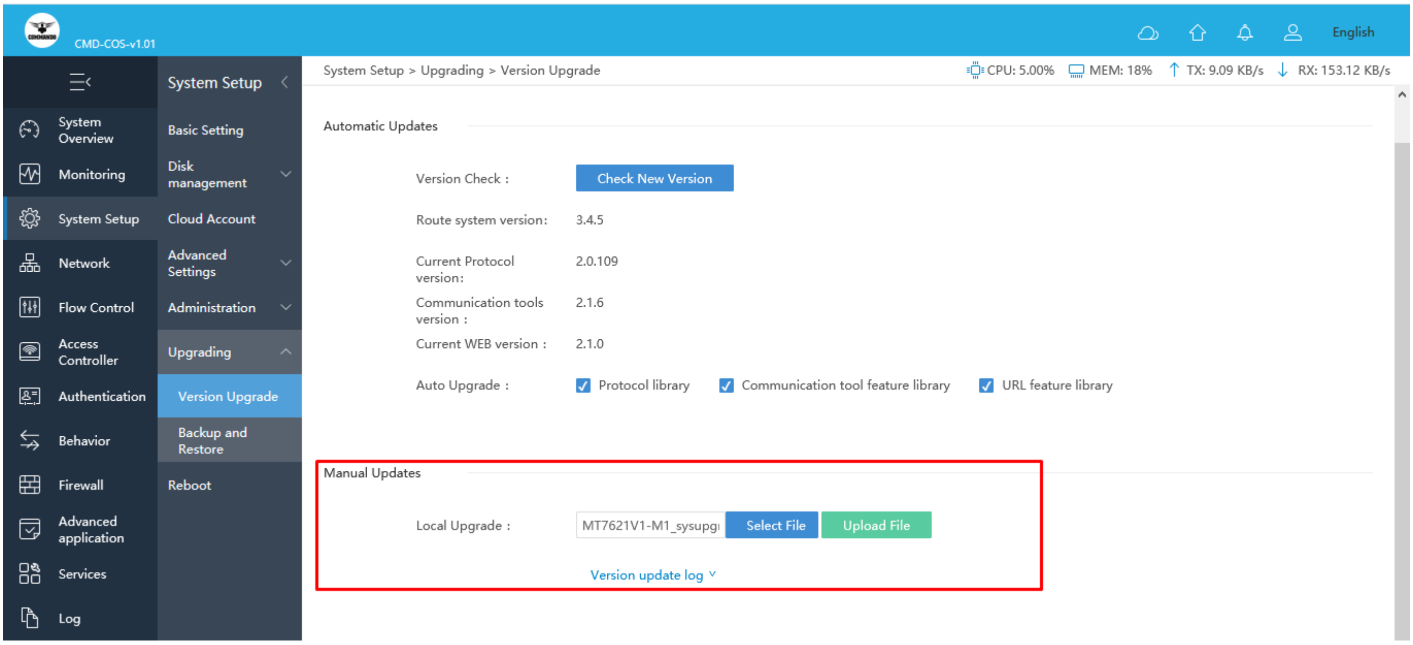
Fig 2.6.1 Version Upgrade page

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.



System Setup > Upgrading > Version Upgrade

CPU: 5.00% MEM: 18% TX: 9.09 KB/s RX: 153.12 KB/s

Automatic Updates

Version Check :

Route system version: 3.4.5

Current Protocol version: 2.0.109

Communication tools version : 2.1.6

Current WEB version : 2.1.0

Auto Upgrade : ☑ Protocol library ☑ Communication tool feature library ☑ URL feature library

Manual Updates

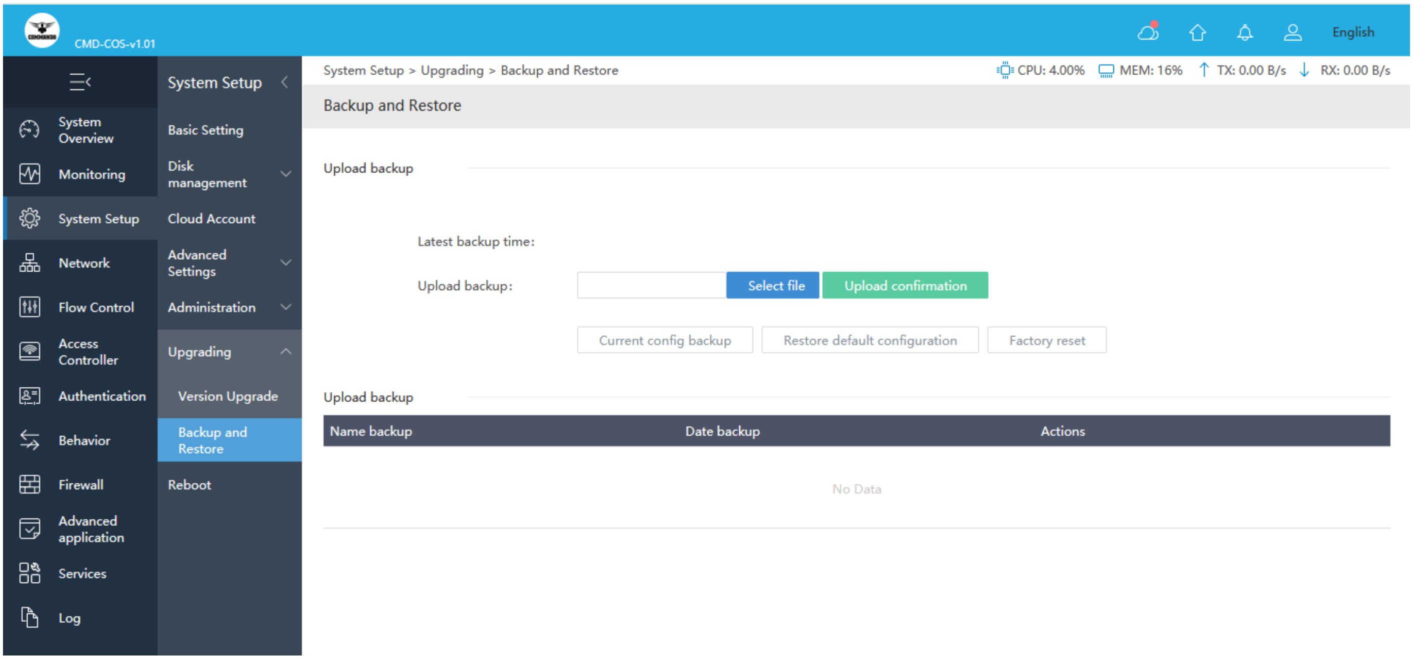
Local Upgrade : MT7621V1-M1_sysupgı

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.



System Setup > Upgrading > Backup and Restore

CPU: 4.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Backup and Restore

Upload backup

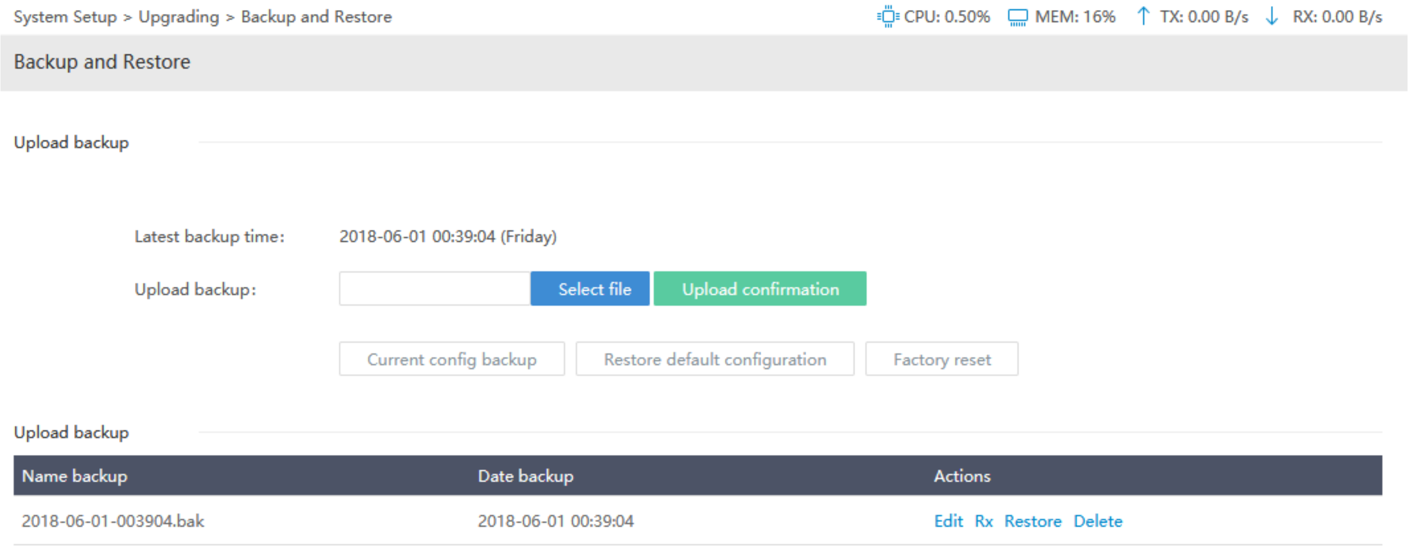
Latest backup time:

Upload backup:

Upload backup

Name backup	Date backup	Actions
No Data		

Fig 2.6.3 Default Backup and Restore page



System Setup > Upgrading > Backup and Restore

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

Backup and Restore

Upload backup

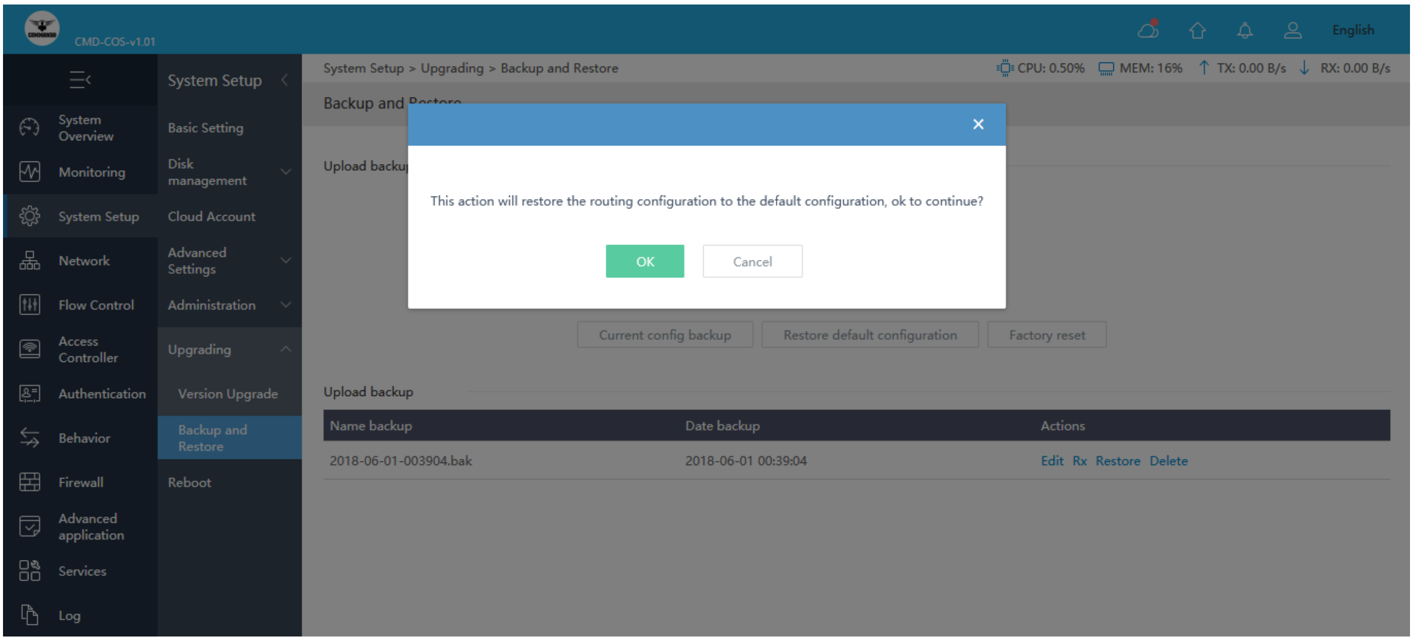
Latest backup time: 2018-06-01 00:39:04 (Friday)

Upload backup:

Upload backup

Name backup	Date backup	Actions
2018-06-01-003904.bak	2018-06-01 00:39:04	Edit Rx Restore Delete

Fig 2.6.4 Options Backup and Restore page



System Setup > Upgrading > Backup and Restore

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

Backup and Restore

Upload backup

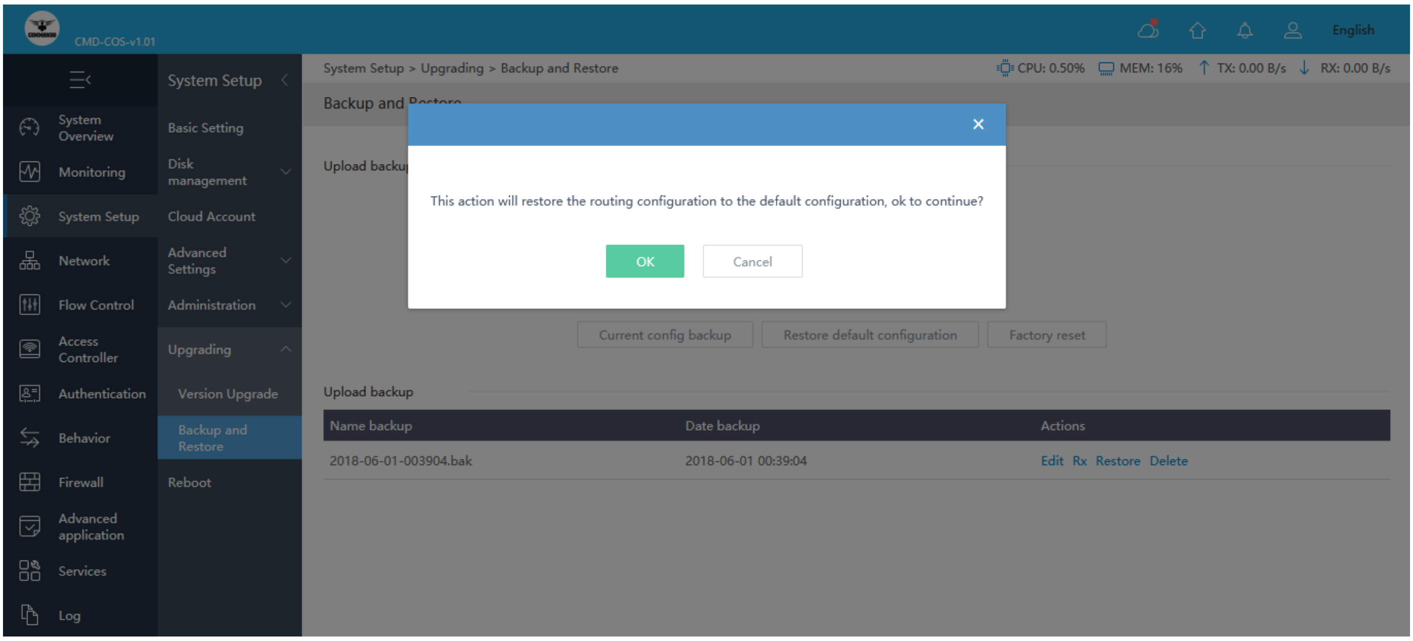
This action will restore the routing configuration to the default configuration, ok to continue?

OK Cancel

Upload backup

Name backup	Date backup	Actions
2018-06-01-003904.bak	2018-06-01 00:39:04	Edit Rx Restore Delete

Fig 2.6.5 Backup the current configuration page



System Setup > Upgrading > Backup and Restore

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

Backup and Restore

Upload backup

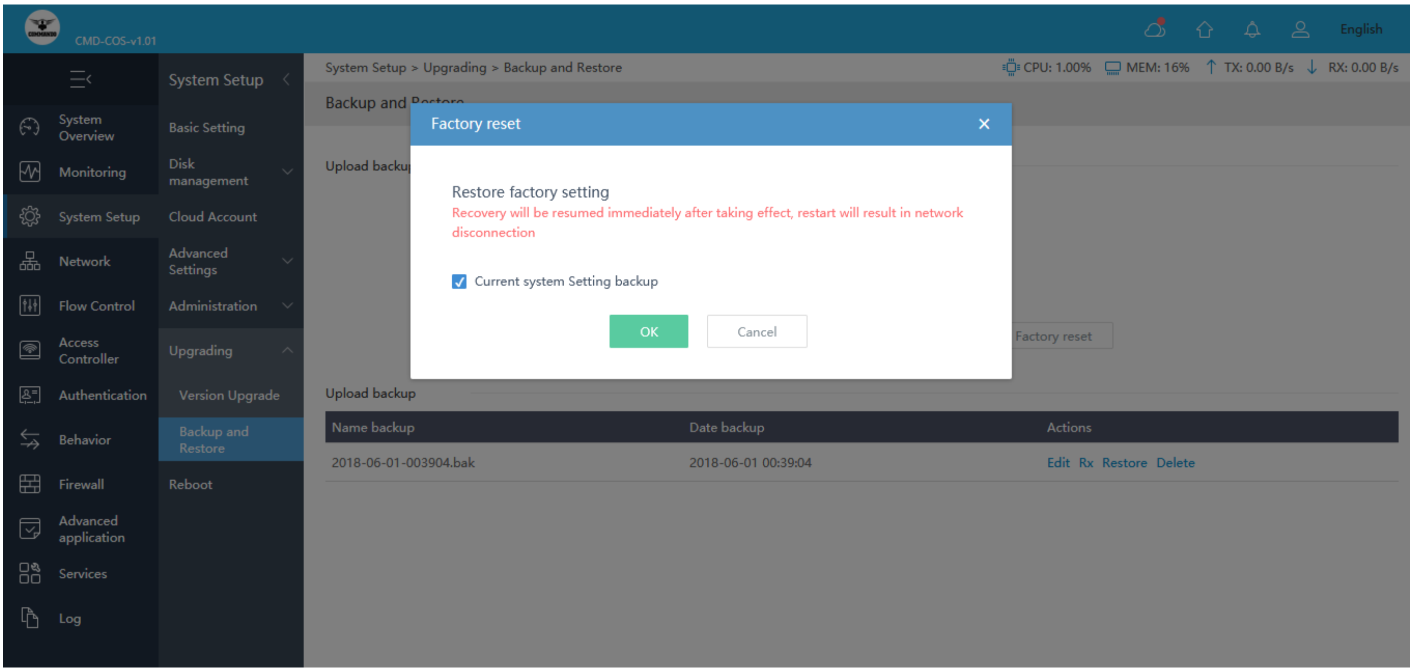
This action will restore the routing configuration to the default configuration, ok to continue?

OK Cancel

Upload backup

Name backup	Date backup	Actions
2018-06-01-003904.bak	2018-06-01 00:39:04	Edit Rx Restore Delete

Fig 2.6.6 Restoring default configuration page



Factory reset ×

Restore factory setting

Recovery will be resumed immediately after taking effect, restart will result in network disconnection

☑ Current system Setting backup

Upload backup

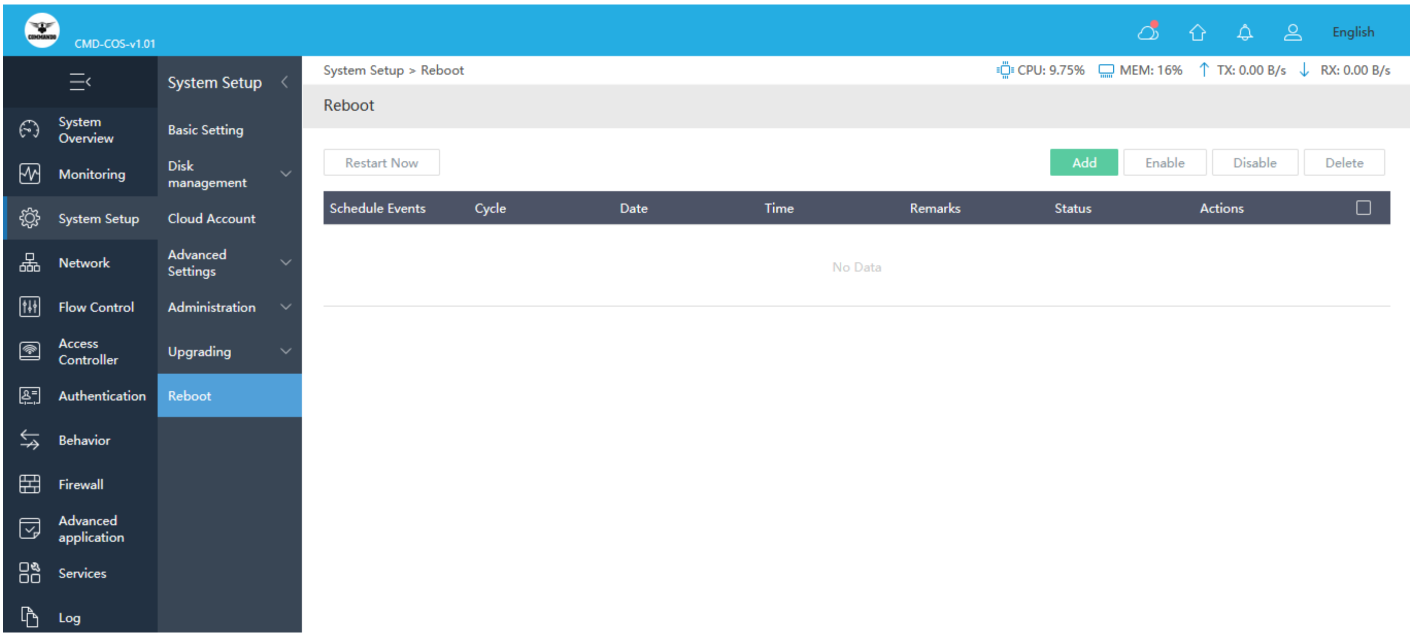
Name backup	Date backup	Actions
2018-06-01-003904.bak	2018-06-01 00:39:04	Edit Rx Restore Delete

Fig 2.6.7 Restore Factory setting page

7. Reboot

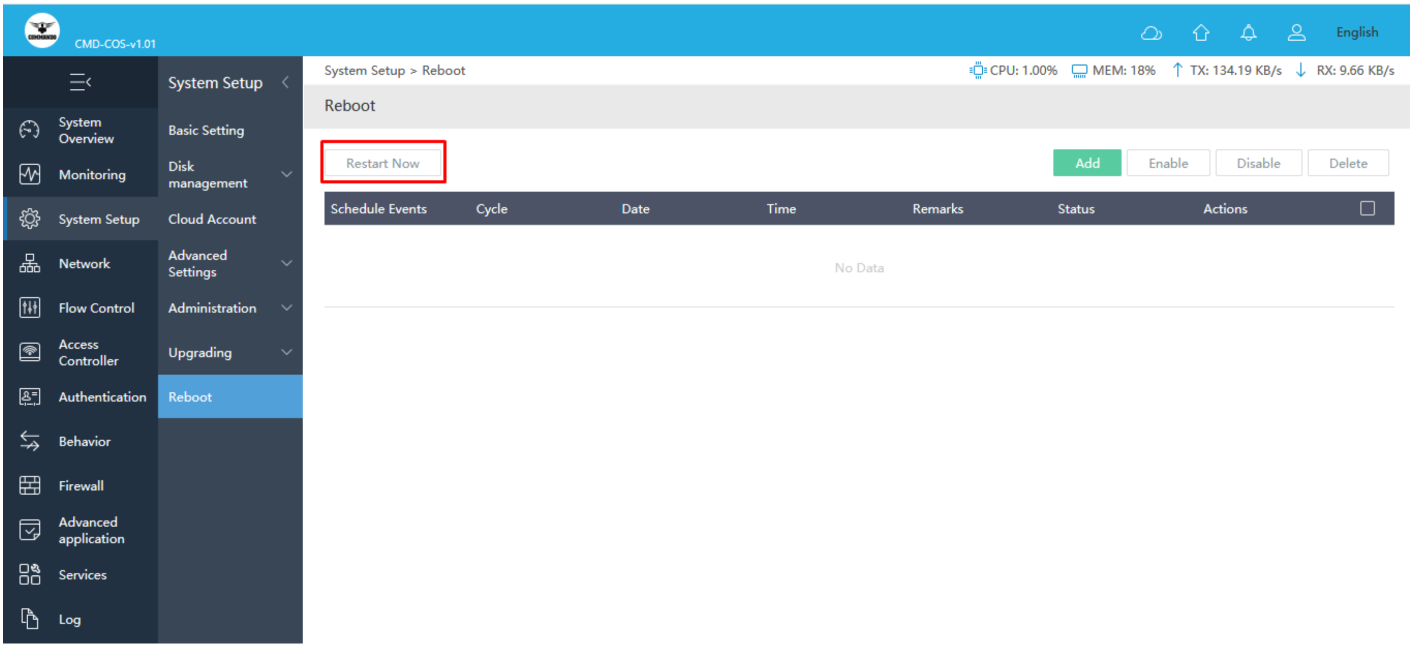
The configuration will not be lost after rebooting. The Internet connection will be temporarily interrupted while rebooting.

For Reboot, Click on System Setup > Reboot



Schedule Events	Cycle	Date	Time	Remarks	Status	Actions	□
No Data							

Fig 2.7.1 Default Reboot page



System Setup > Reboot

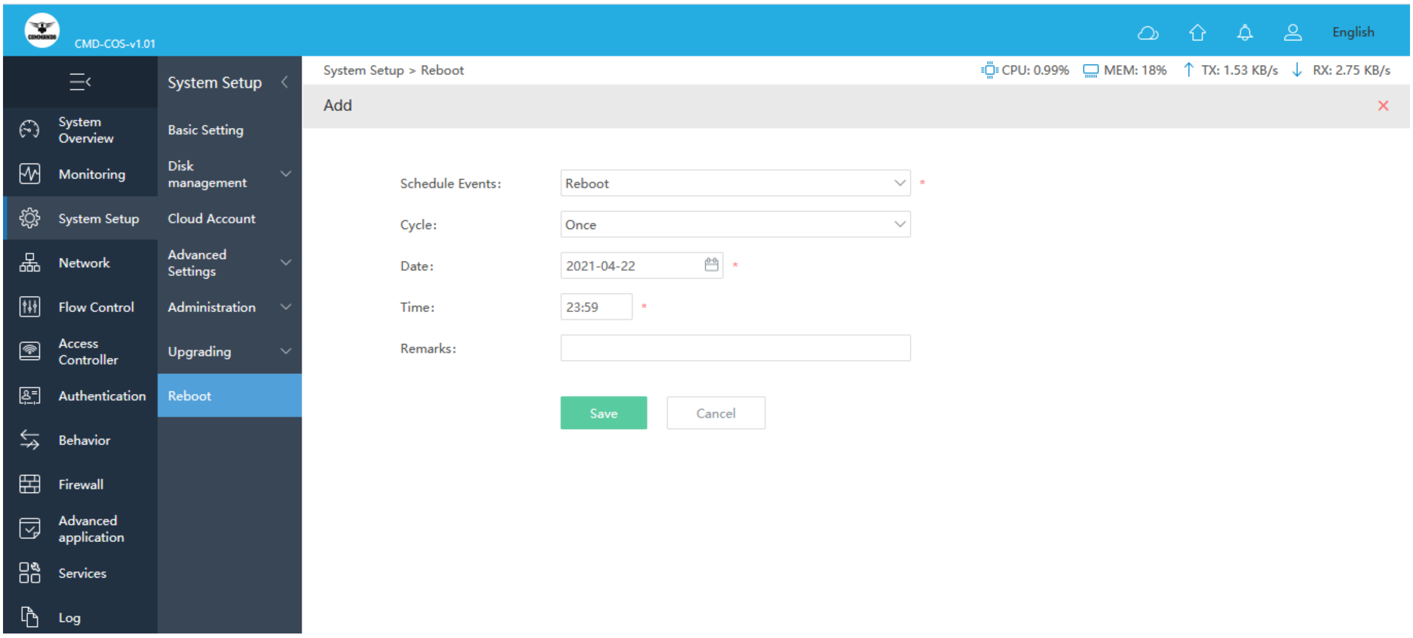
CPU: 1.00% MEM: 18% TX: 134.19 KB/s RX: 9.66 KB/s

Reboot

Schedule Events	Cycle	Date	Time	Remarks	Status	Actions ☐

No Data

Fig 2.7.2 Restart Now page



System Setup > Reboot

CPU: 0.99% MEM: 18% TX: 1.53 KB/s RX: 2.75 KB/s

Add

Schedule Events: Reboot *

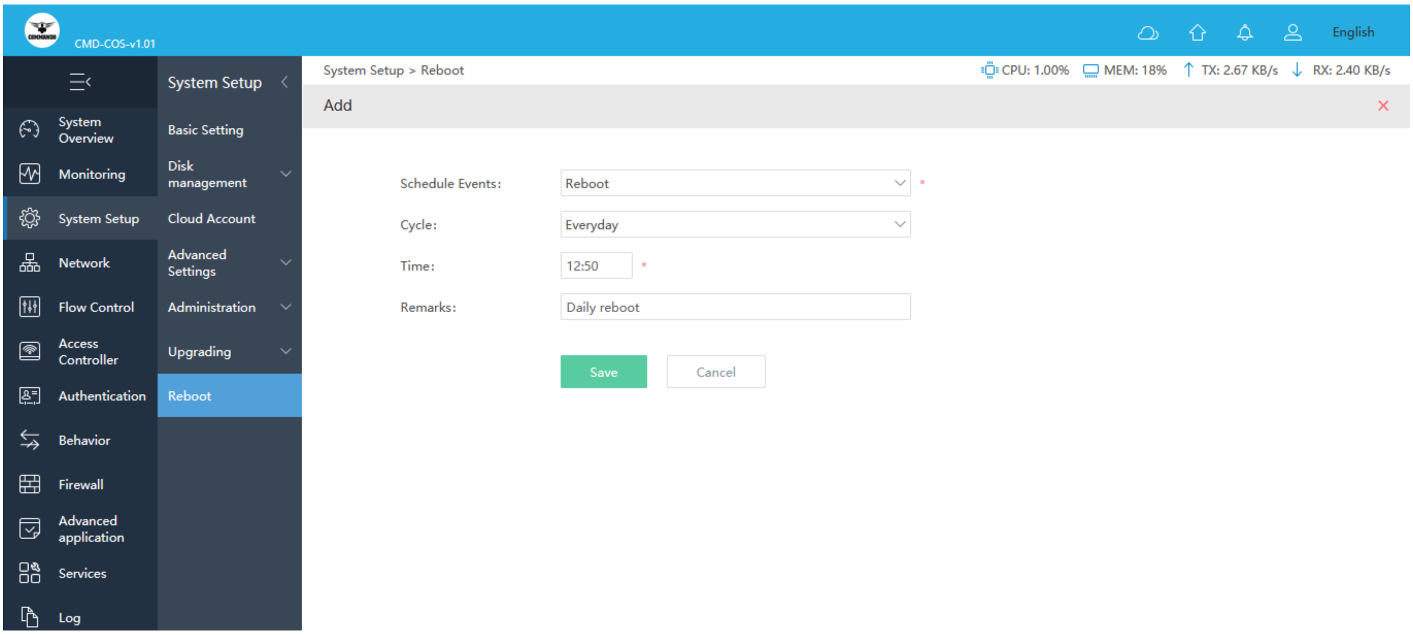
Cycle: Once

Date: 2021-04-22 *

Time: 23:59 *

Remarks:

Fig 2.7.3 Default Schedule Restart page



System Setup > Reboot

CPU: 1.00% MEM: 18% TX: 2.67 KB/s RX: 2.40 KB/s

Add

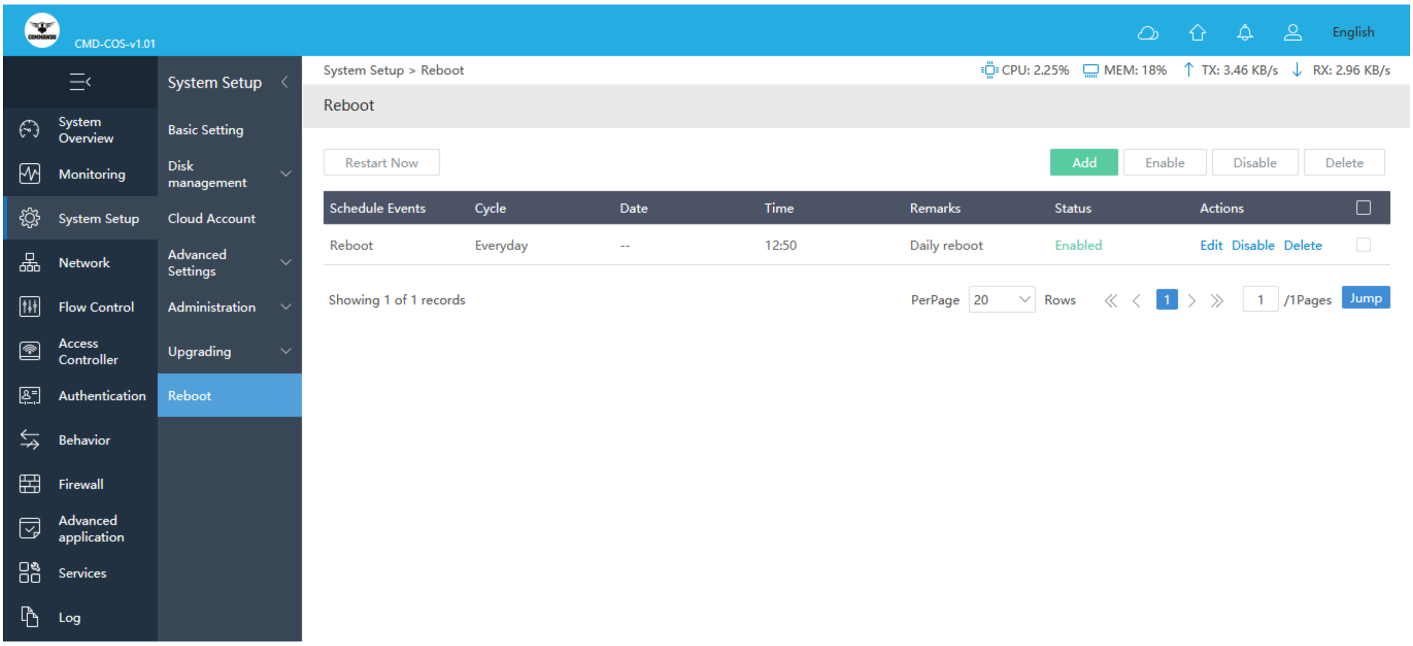
Schedule Events: Reboot *

Cycle: Everyday

Time: 12:50 *

Remarks: Daily reboot

Fig 2.7.4 Add Schedule Restart page



System Setup > Reboot

CPU: 2.25% MEM: 18% TX: 3.46 KB/s RX: 2.96 KB/s

Reboot

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

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

Fig 2.7.5 Schedule Restart everyday page

NETWORK

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

DHCP:

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

DNS:

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

IP/MAC Group:

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

Static Routes:

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

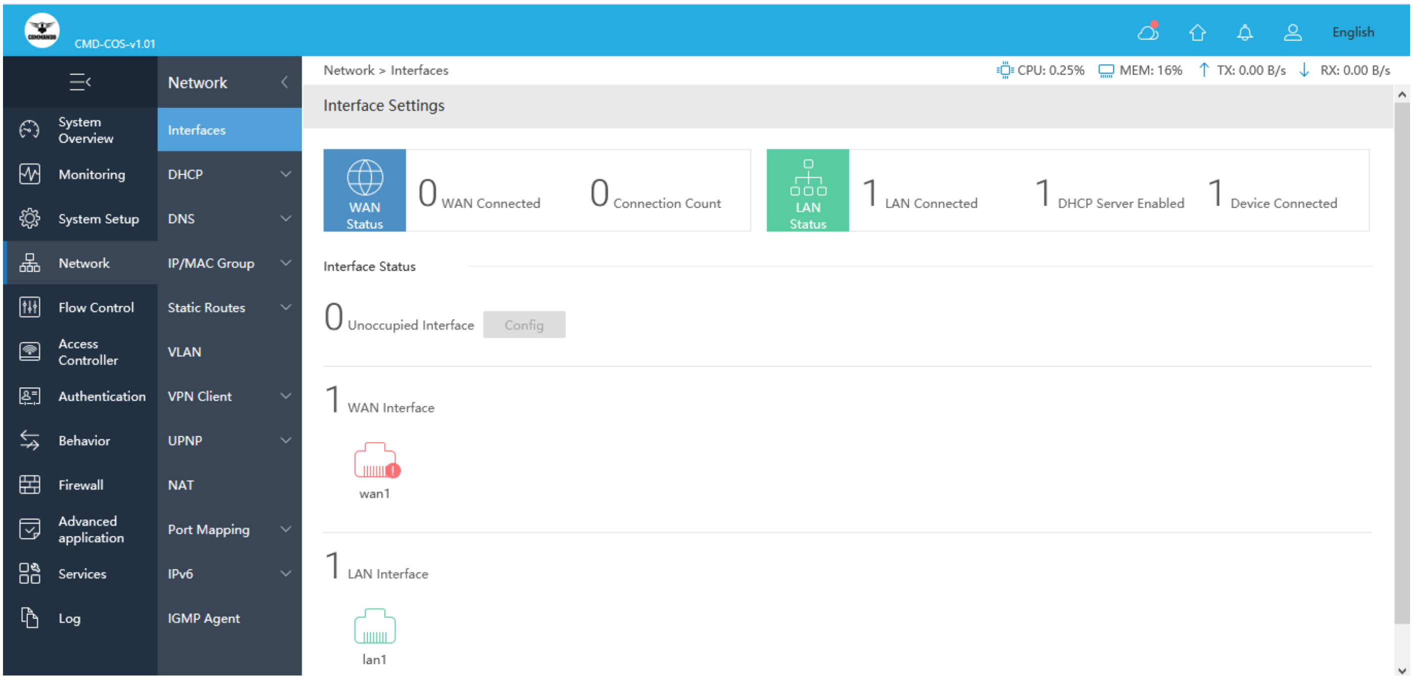
The IGMP Agent is responsible for forwarding multicast messages only to VMs that are registered to that multicast group, while respecting the filtering fields that are defined in IGMPv3. VM registration is detected by processing IGMP Join packets that all subscribed VMs send.

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



Network > Interfaces

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

Interface Settings

WAN Status 0 WAN Connected 0 Connection Count

LAN Status 1 LAN Connected 1 DHCP Server Enabled 1 Device Connected

Interface Status

0 Unoccupied Interface

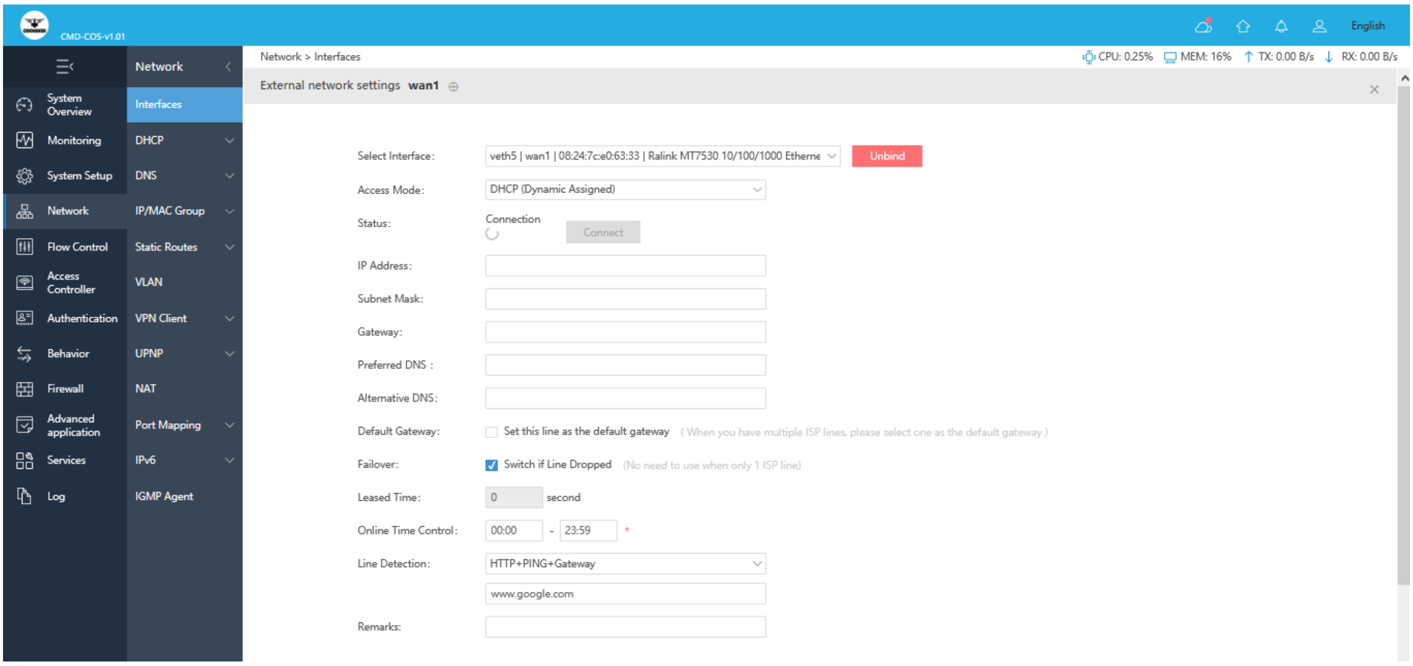
1 WAN Interface

wan1

1 LAN Interface

lan1

Fig 3.1.1 Default interface setting page



External network settings **wan1**

Select Interface: veth5 | wan1 | 08:24:7c:e0:63:33 | Ralink MT7530 10/100/1000 Etherne   Unbind

Access Mode: DHCP (Dynamic Assigned)

Status: Connection   Connect

IP Address:

Subnet Mask:

Gateway:

Preferred DNS :

Alternative DNS:

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)

Leased Time: 0 second

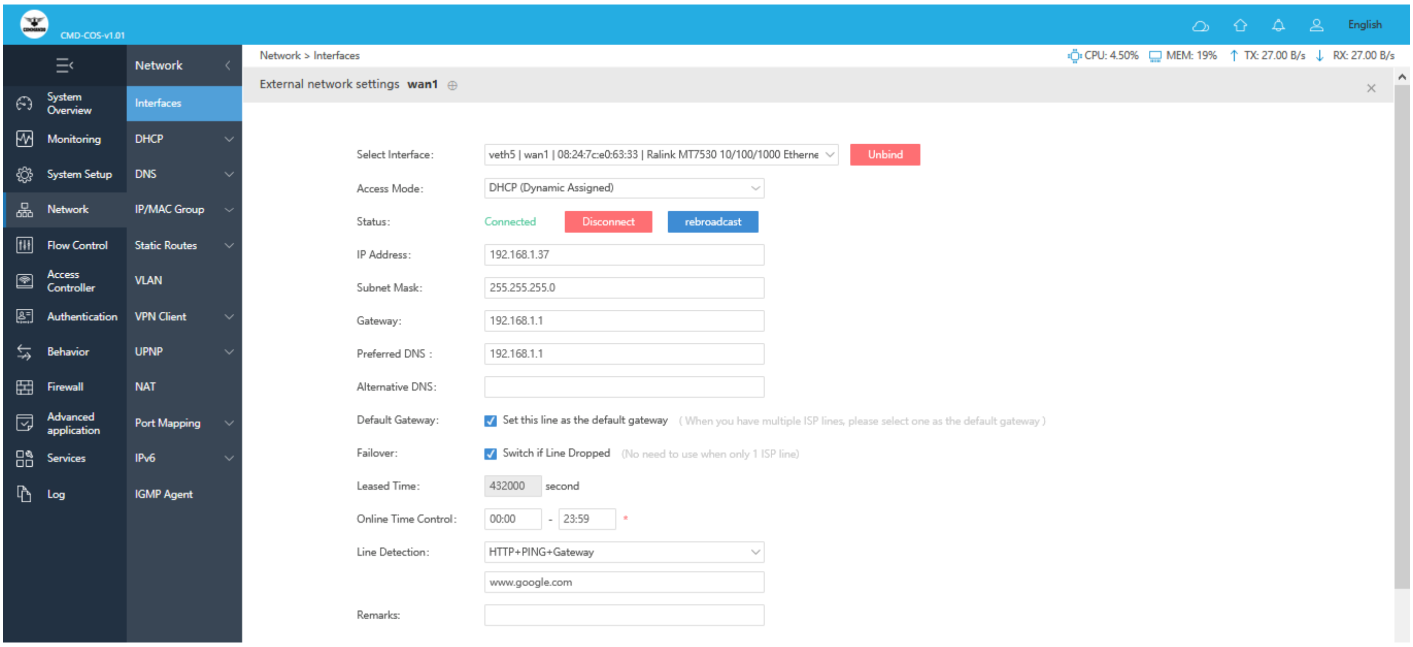
Online Time Control: 00:00 - 23:59 *

Line Detection: HTTP+PING+Gateway

www.google.com

Remarks:

Fig 3.1.2 Default External Network setting options



External network settings **wan1**

Select Interface: veth5 | wan1 | 08:24:7c:e0:63:33 | Ralink MT7530 10/100/1000 Etherne   Unbind

Access Mode: DHCP (Dynamic Assigned)

Status: Connected   Disconnect   rebroadcast

IP Address: 192.168.1.37

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Preferred DNS : 192.168.1.1

Alternative DNS:

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)

Leased Time: 432000 second

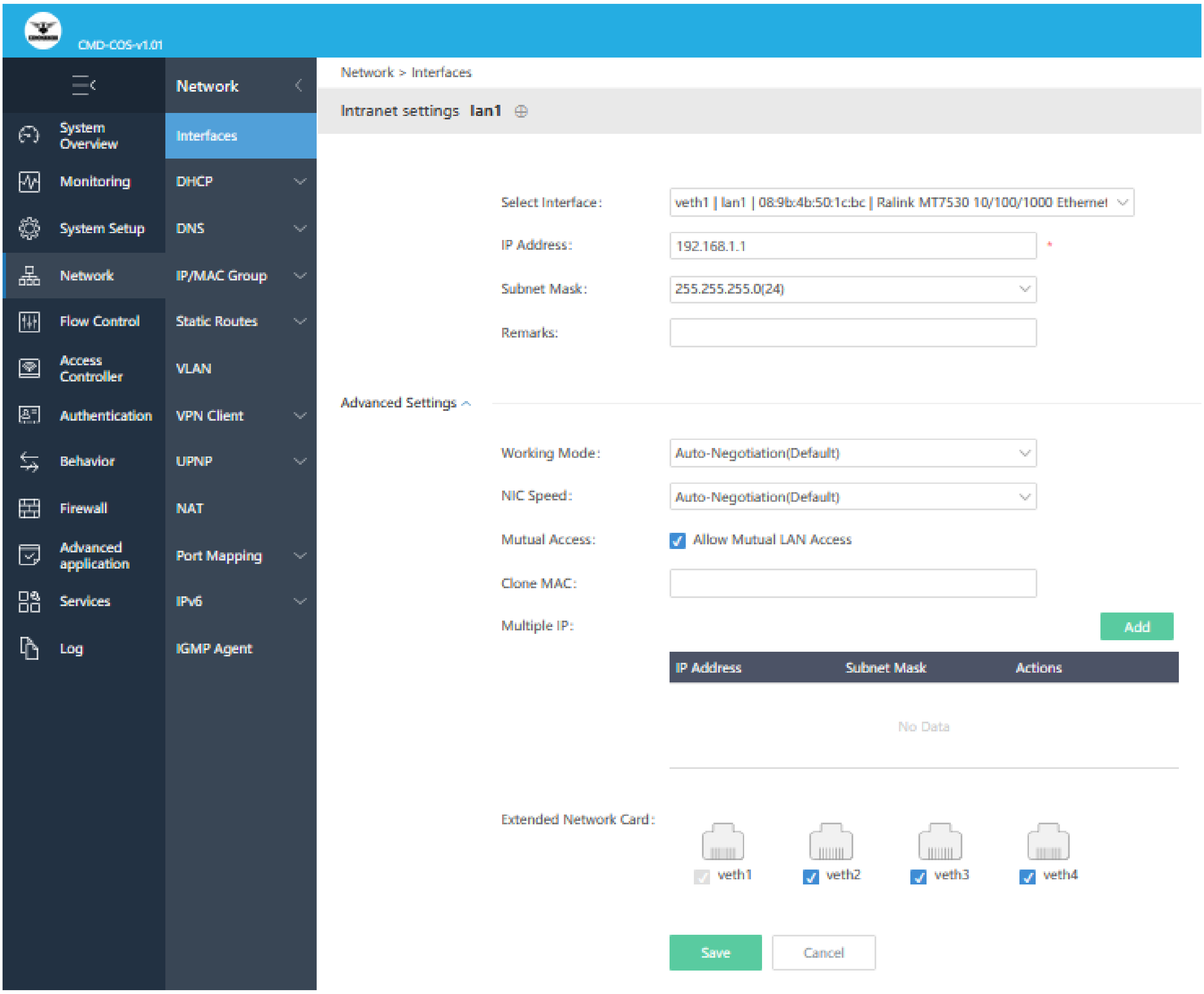
Online Time Control: 00:00 - 23:59 *

Line Detection: HTTP+PING+Gateway

www.google.com

Remarks:

Fig 3.1.3 Setting External Network setting for WAN1 interface page



Intranet settings **lan1**

Select Interface: veth1 | lan1 | 08:9b:4b:50:1c:bc | Ralink MT7530 10/100/1000 Ethernet

IP Address: 192.168.1.1 *

Subnet Mask: 255.255.255.0(24)

Remarks:

Advanced Settings

Working Mode: Auto-Negotiation(Default)

NIC Speed: Auto-Negotiation(Default)

Mutual Access: ☑ Allow Mutual LAN Access

Clone MAC:

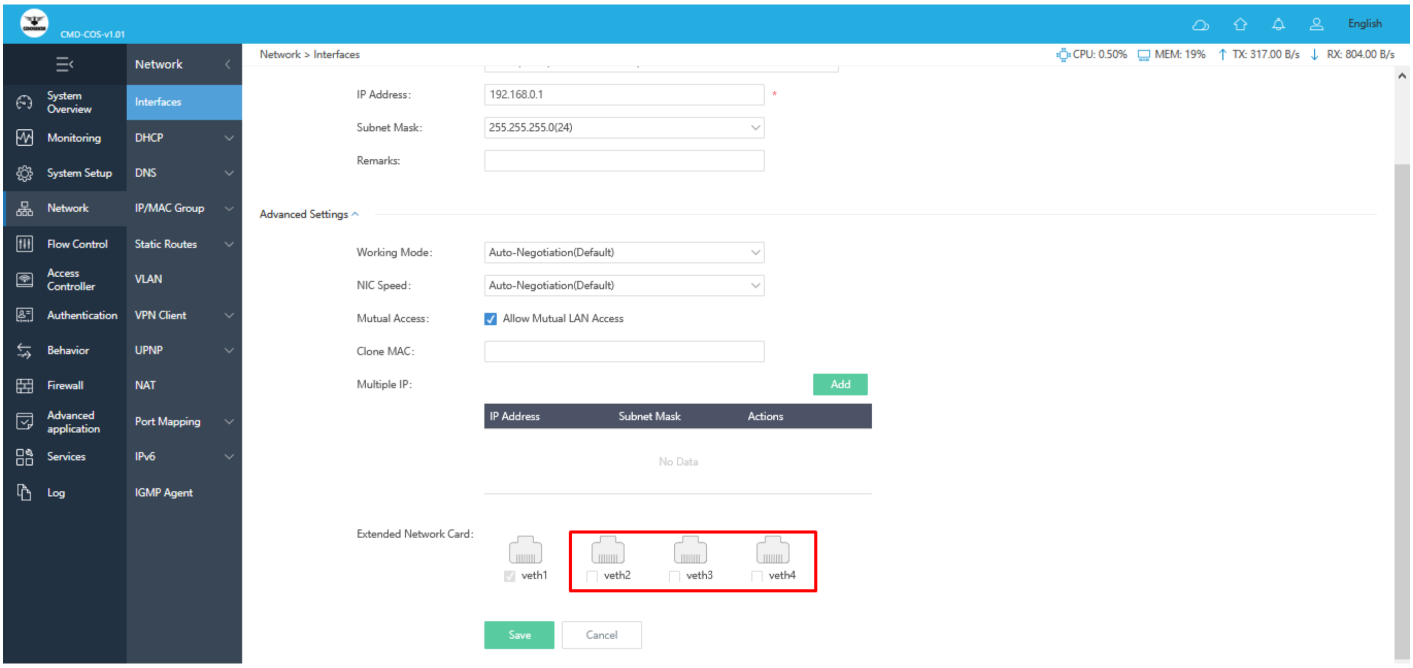
Multiple IP:

IP Address	Subnet Mask	Actions
No Data		

Extended Network Card: ☑ veth1 ☑ veth2 ☑ veth3 ☑ veth4

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**.**



IP Address: 192.168.0.1 *

Subnet Mask: 255.255.255.0(24)

Remarks:

Advanced Settings

Working Mode: Auto-Negotiation(Default)

NIC Speed: Auto-Negotiation(Default)

Mutual Access: ☑ Allow Mutual LAN Access

Clone MAC:

Multiple IP: Add

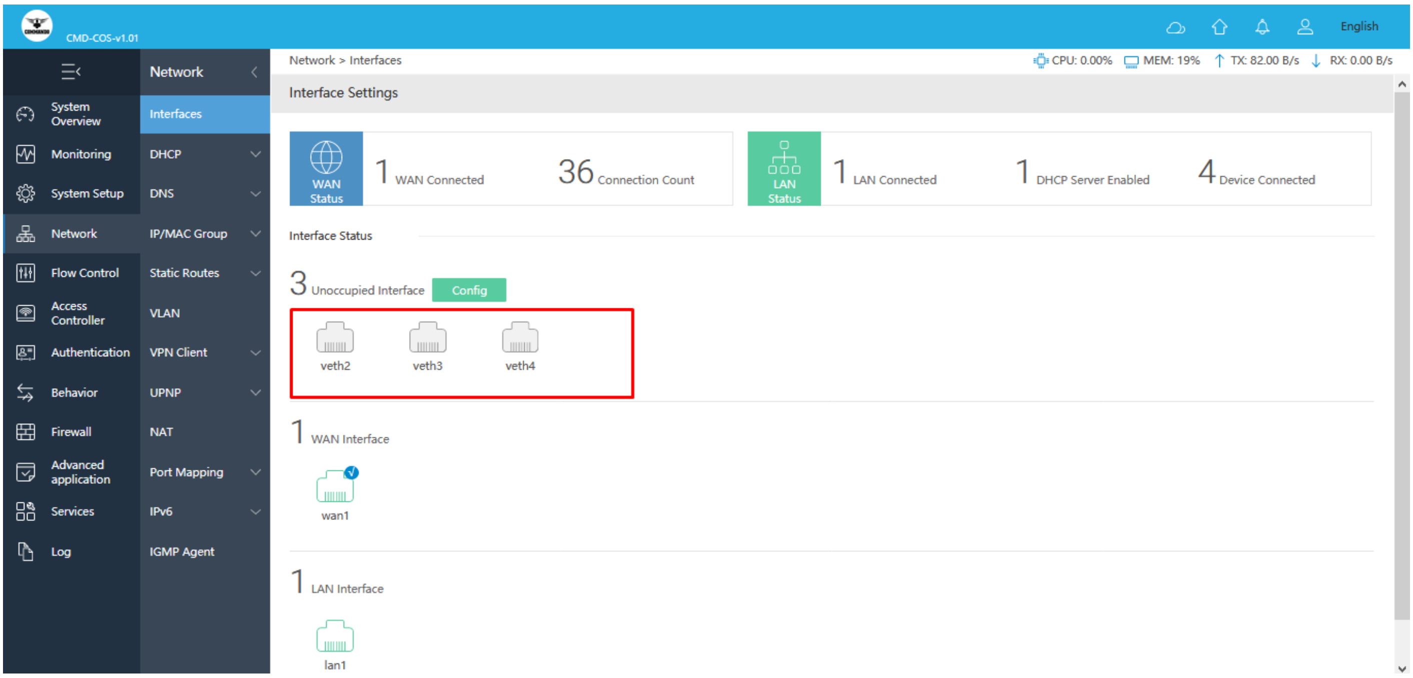
IP Address	Subnet Mask	Actions
No Data		

Extended Network Card: ☑ veth1 □ veth2 □ veth3 □ veth4

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.



Interface Settings

WAN Status: 1 WAN Connected, 36 Connection Count

LAN Status: 1 LAN Connected, 1 DHCP Server Enabled, 4 Device Connected

Interface Status

3 Unoccupied Interface Config

veth2 veth3 veth4

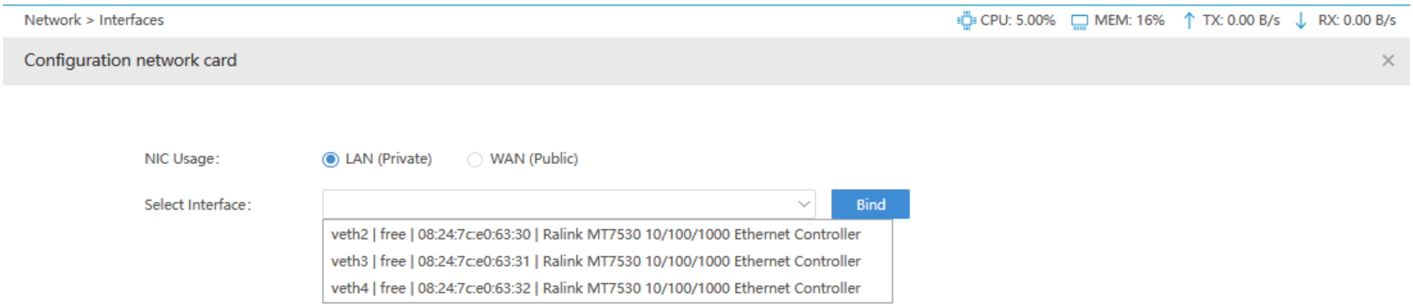
1 WAN Interface

wan1

1 LAN Interface

lan1

Fig 3.1.7 Interface setting after releasing ports form LAN1 interface page



Network > Interfaces

CPU: 5.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

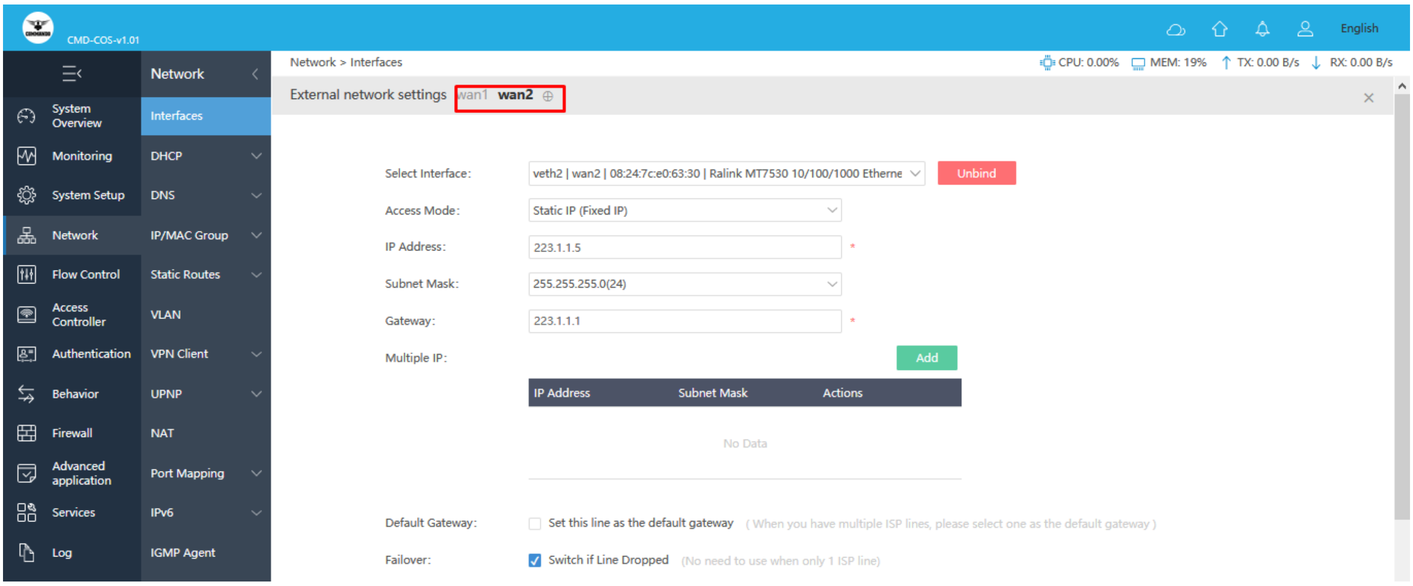
Configuration network card

NIC Usage: ● LAN (Private) ○ WAN (Public)

Select Interface:

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



Network > Interfaces

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

External network settings wan1 **wan2**

Select Interface: veth2 | wan2 | 08:24:7c:e0:63:30 | Ralink MT7530 10/100/1000 Etherne

Access Mode: Static IP (Fixed IP)

IP Address: 223.1.1.5 *

Subnet Mask: 255.255.255.0(24)

Gateway: 223.1.1.1 *

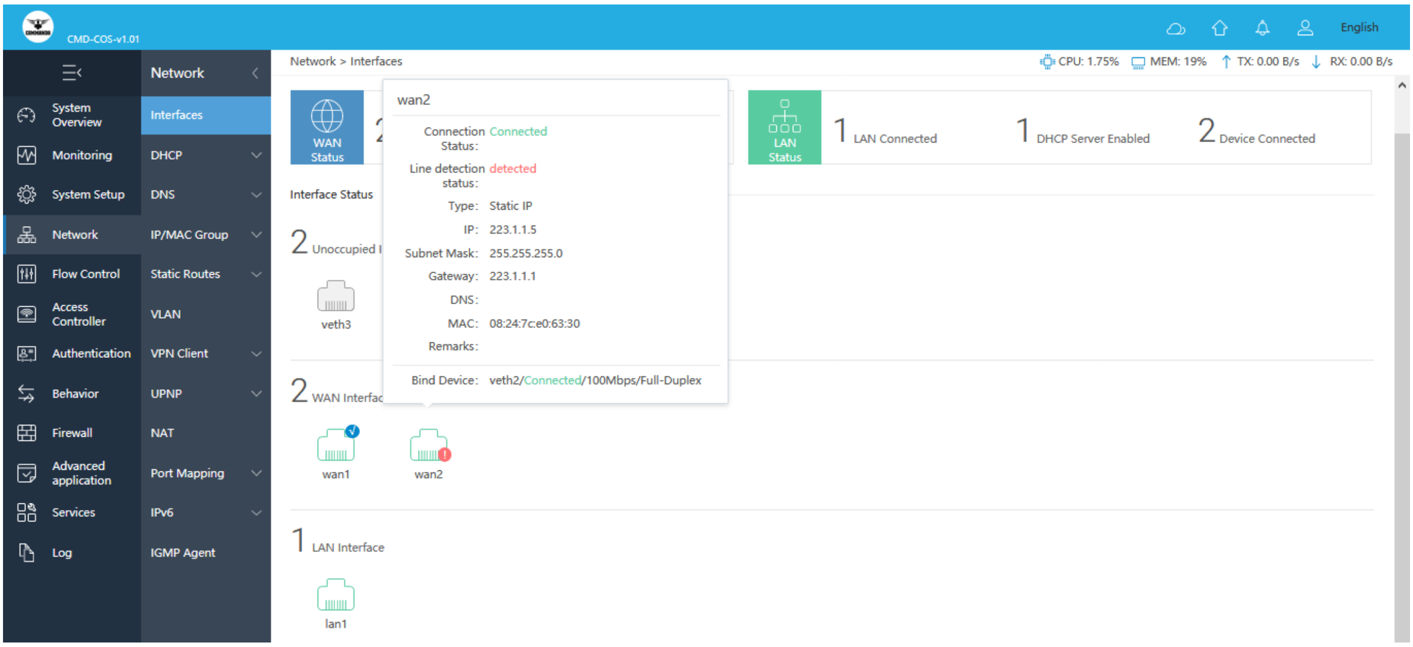
Multiple IP:

IP Address	Subnet Mask	Actions
No Data		

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



wan2

Connection Status: Connected

Line detection status: detected

Type: Static IP

IP: 223.1.1.5

Subnet Mask: 255.255.255.0

Gateway: 223.1.1.1

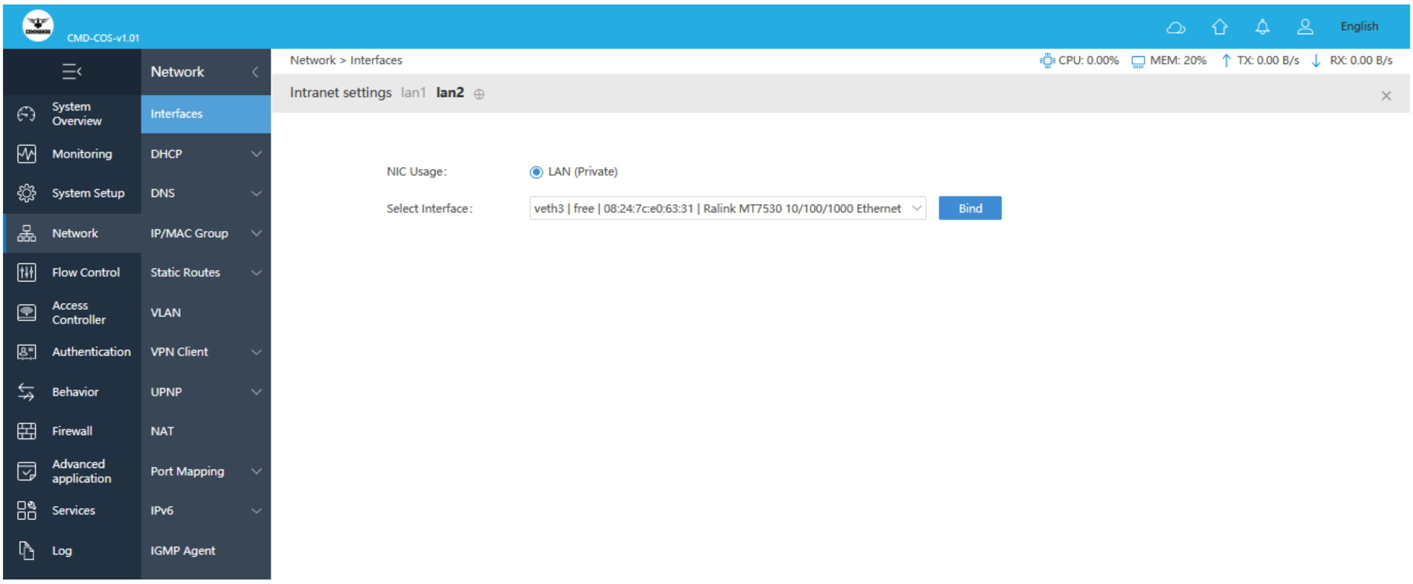
DNS:

MAC: 08:24:7c:e0:63:30

Remarks:

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

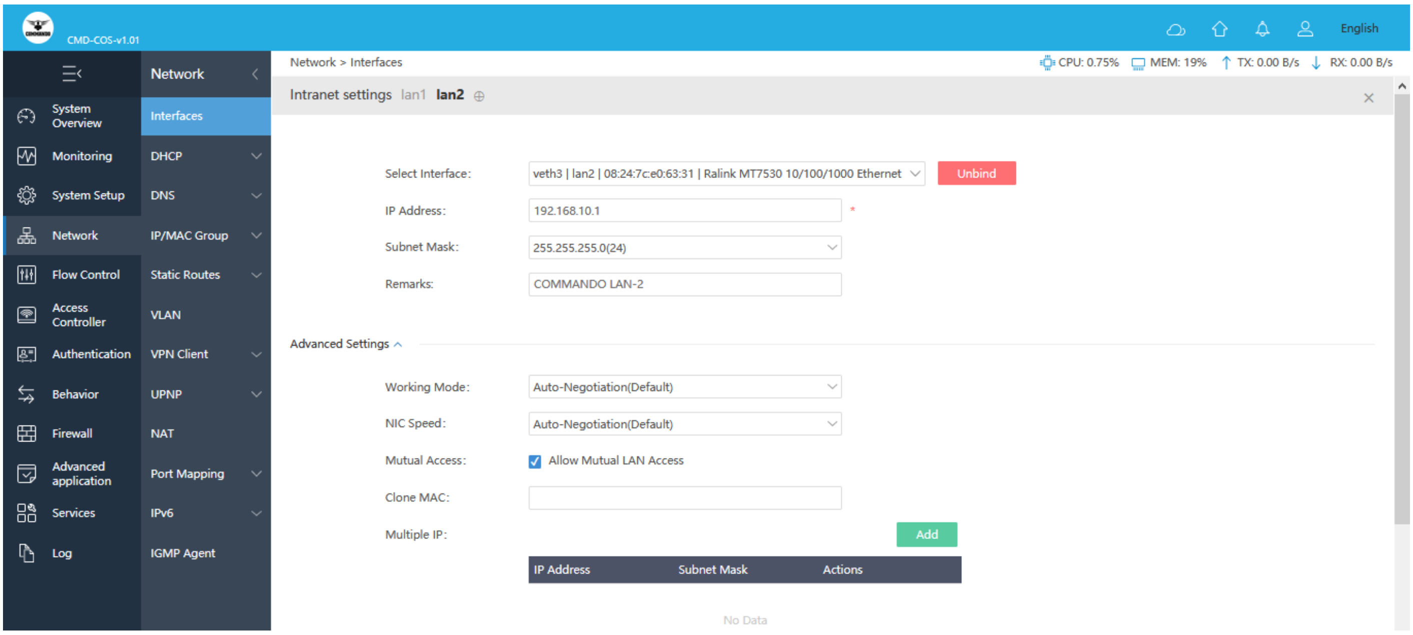
Fig 3.1.10 Network interface page after creating WAN2 interface page



NIC Usage: ● LAN (Private)

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

Fig 3.1.11 Creating LAN2 interface page



Network > Interfaces

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

Intranet settings lan1 **lan2**

Select Interface: veth3 | lan2 | 08:24:7c:e0:63:31 | Ralink MT7530 10/100/1000 Ethernet [Unbind]

IP Address: 192.168.10.1 *

Subnet Mask: 255.255.255.0(24)

Remarks: COMMANDO LAN-2

Advanced Settings

Working Mode: Auto-Negotiation(Default)

NIC Speed: Auto-Negotiation(Default)

Mutual Access: ☑ Allow Mutual LAN Access

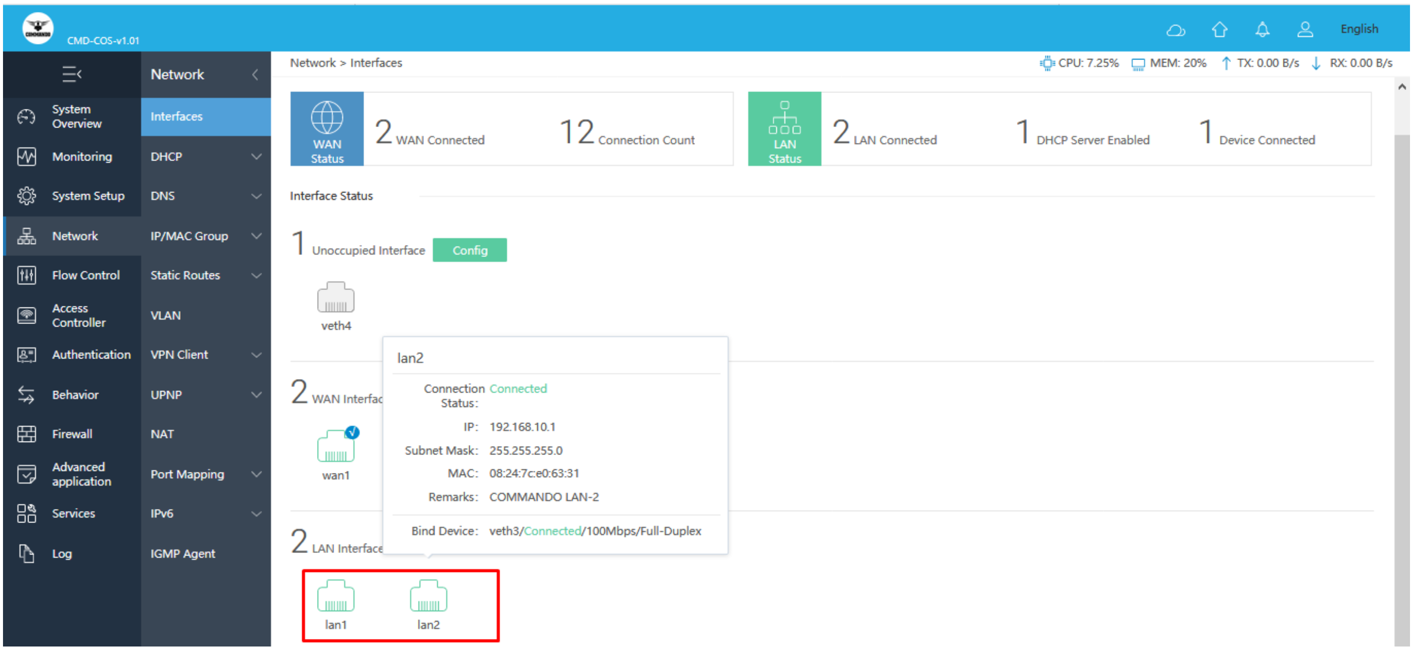
Clone MAC:

Multiple IP: [Add]

IP Address	Subnet Mask	Actions

No Data

Fig 3.1.12 Setting LAN2 interface parameter page



Network > Interfaces

CPU: 7.25% MEM: 20% TX: 0.00 B/s RX: 0.00 B/s

2 WAN Connected 12 Connection Count

2 LAN Connected 1 DHCP Server Enabled 1 Device Connected

Interface Status

1 Unoccupied Interface [Config]

2 WAN Interfac

2 LAN Interface

lan2

Connection Status: Connected

IP: 192.168.10.1

Subnet Mask: 255.255.255.0

MAC: 08:24:7c:e0:63:31

Remarks: COMMANDO LAN-2

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

Fig 3.1.13 Network interface page after creating LAN2 interface page

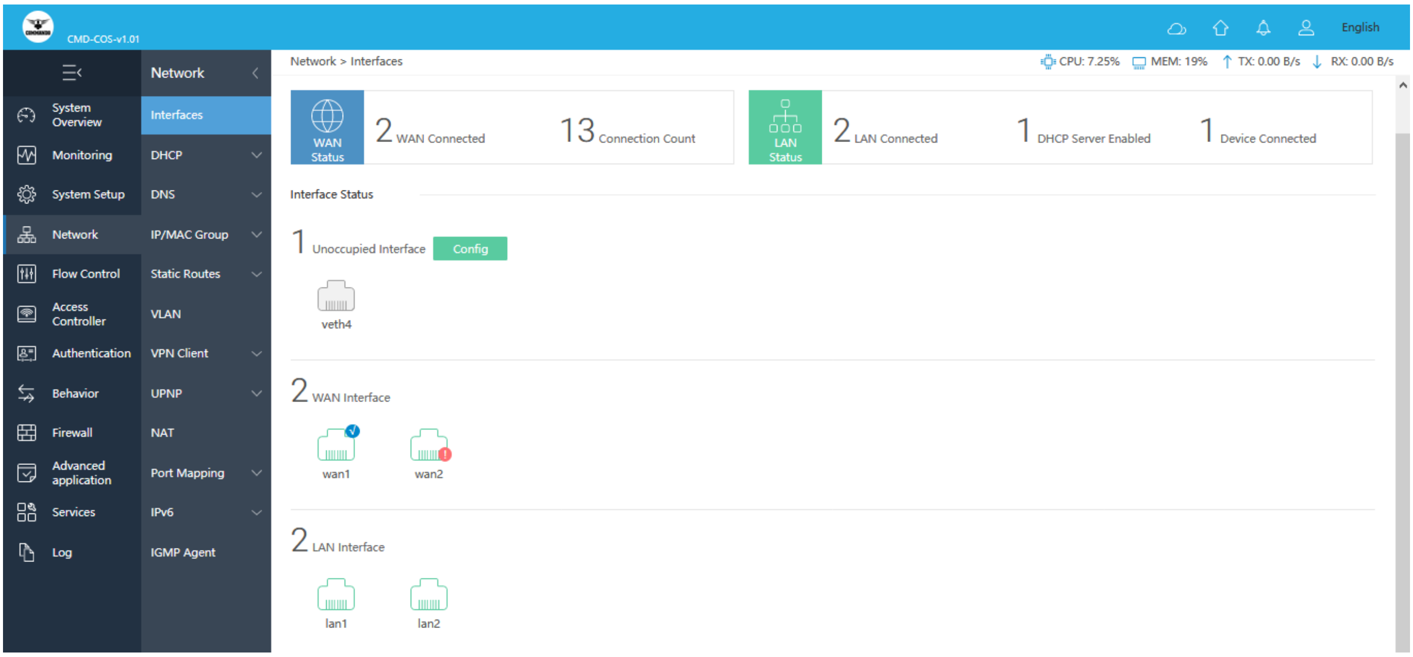
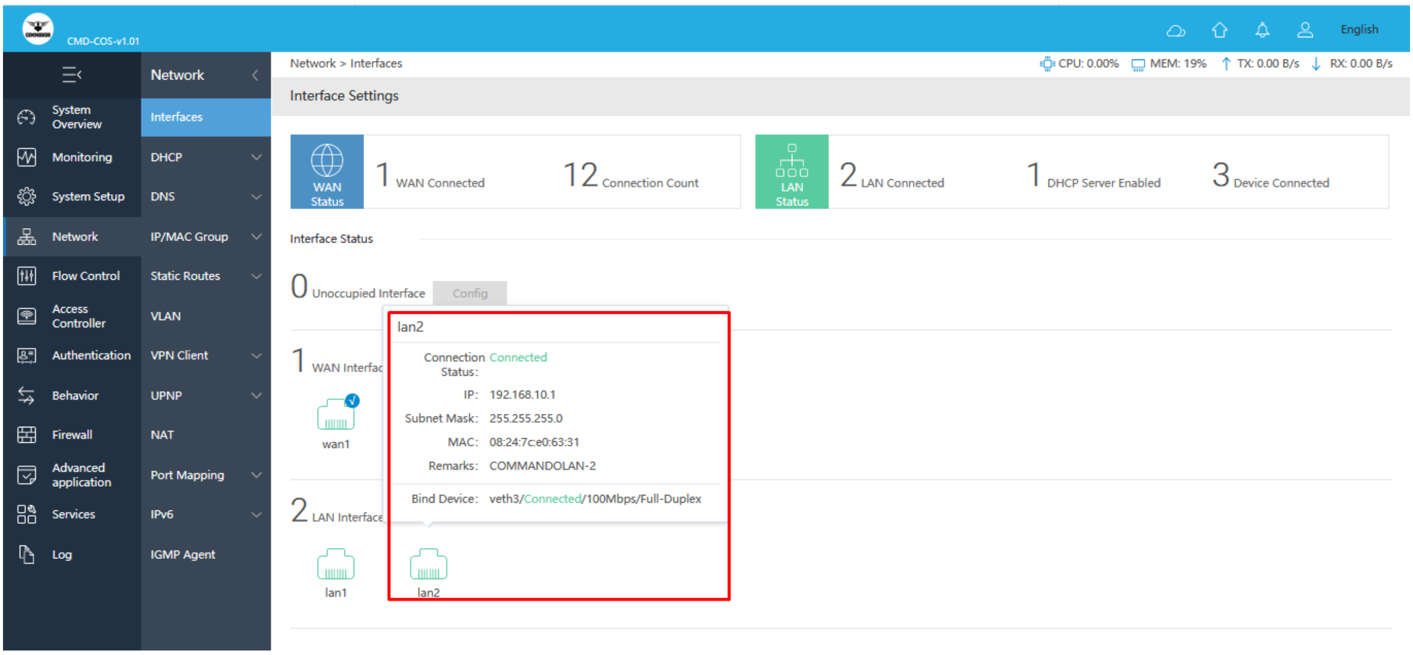


Fig 3.1.14 Network interface page after creating user defined interfaces page

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



lan2

Connection Status: Connected

IP: 192.168.10.1

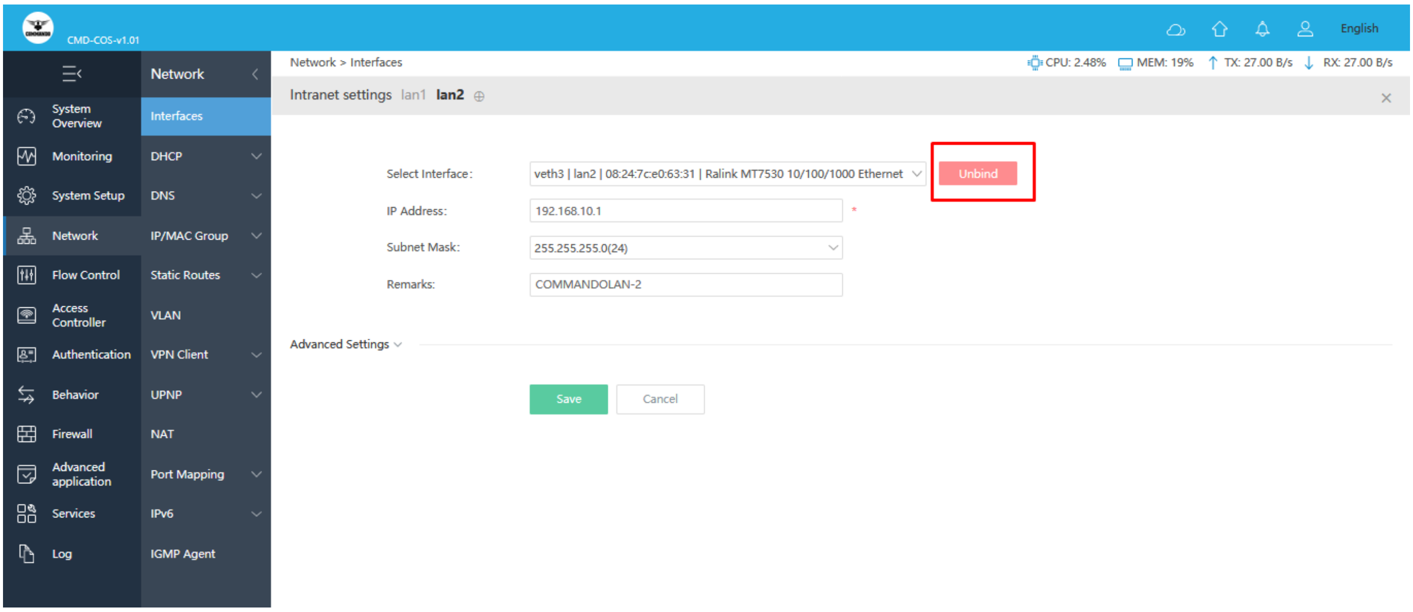
Subnet Mask: 255.255.255.0

MAC: 08:24:7c:e0:63:31

Remarks: COMMANDOLAN-2

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

Fig 3.1.15 Deleting interface after creating user defined LAN2 interface page



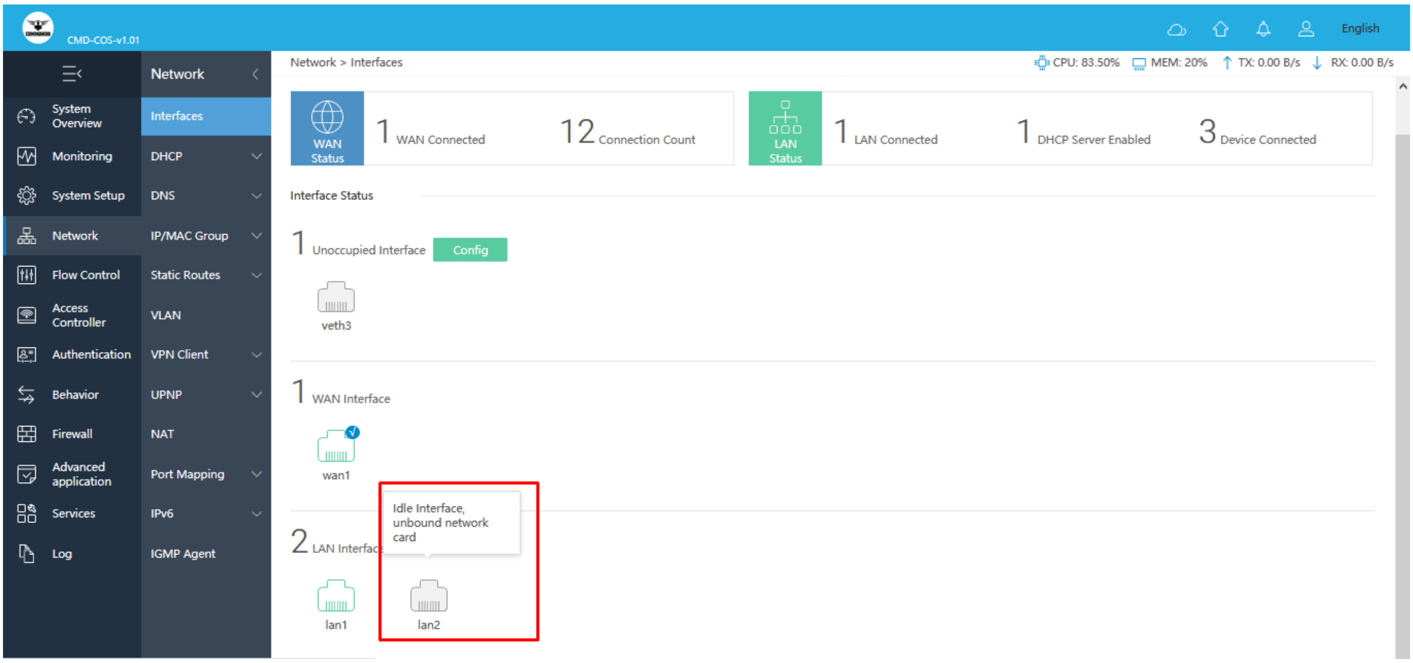
Select Interface: veth3 | lan2 | 08:24:7c:e0:63:31 | Ralink MT7530 10/100/1000 Ethernet

IP Address: 192.168.10.1 *

Subnet Mask: 255.255.255.0(24)

Remarks: COMMANDOLAN-2

Fig 3.1.16 Unbinding port from LAN2 interface page



1 WAN Connected 12 Connection Count

1 LAN Connected 1 DHCP Server Enabled 3 Device Connected

1 Unoccupied Interface

1 WAN Interface

2 LAN Interface

Idle Interface, unbound network card

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

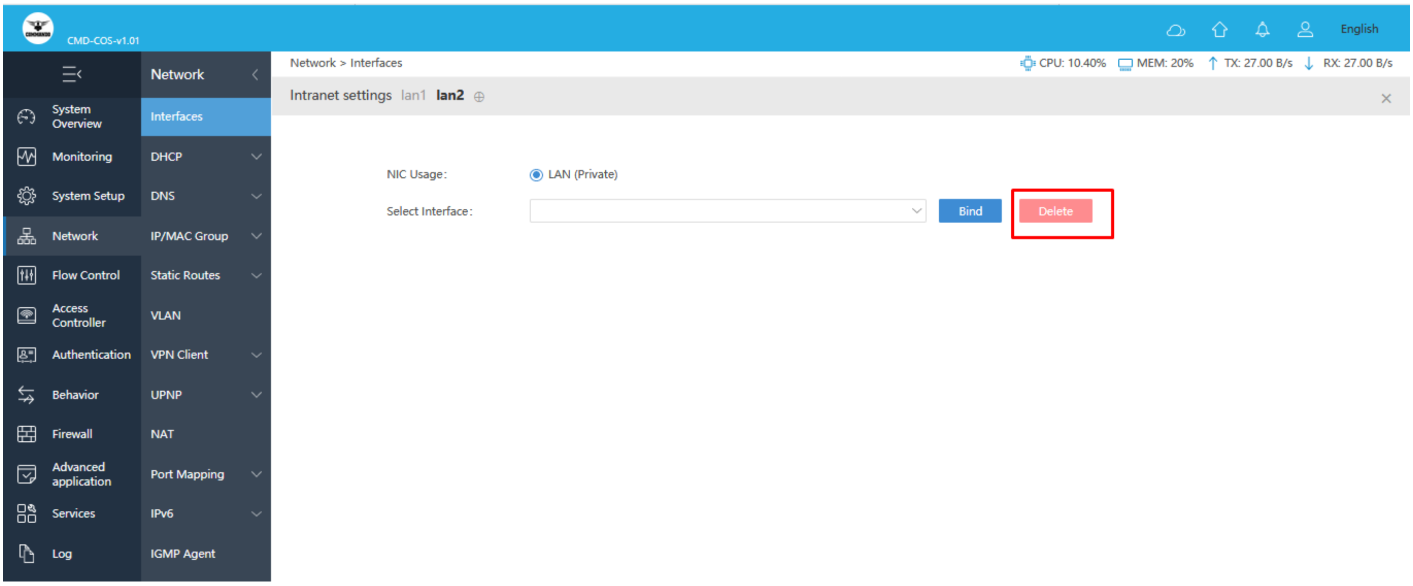


Fig 3.1.17 Deleting port from LAN2 interface page

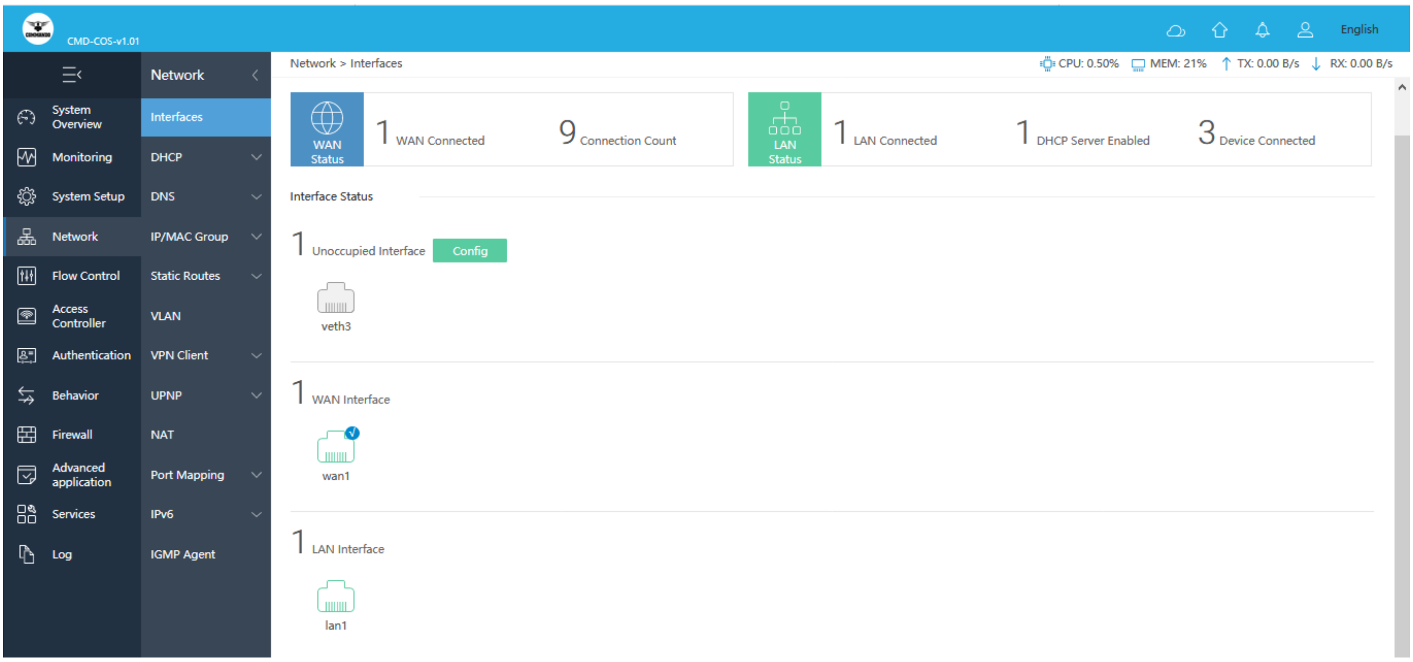
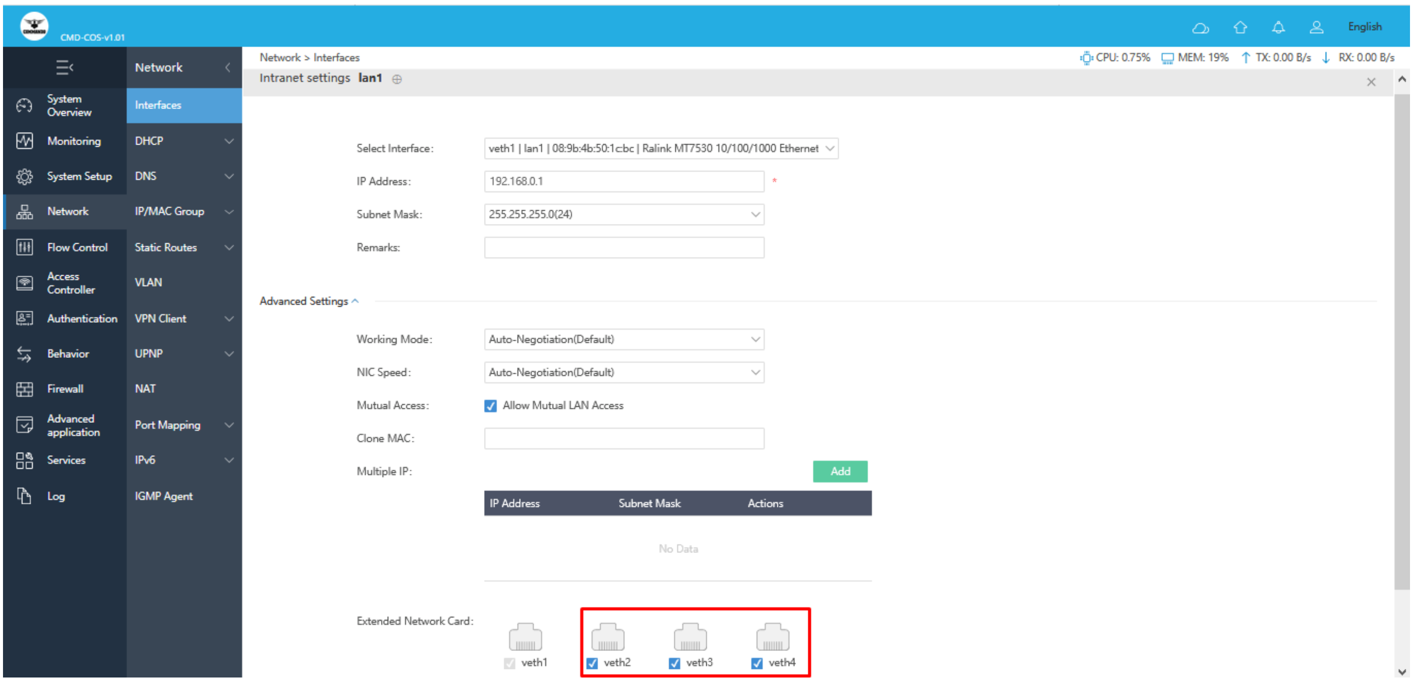


Fig 3.1.18 Network interface page after deleting LAN2 interface page

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.



Network > Interfaces

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

Intranet settings **lan1**

Select Interface: veth1 | lan1 | 08:9b:4b:50:1c:bc | Ralink MT7530 10/100/1000 Ethernet

IP Address: 192.168.0.1 *

Subnet Mask: 255.255.255.0(24)

Remarks:

Advanced Settings

Working Mode: Auto-Negotiation(Default)

NIC Speed: Auto-Negotiation(Default)

Mutual Access: ☑ Allow Mutual LAN Access

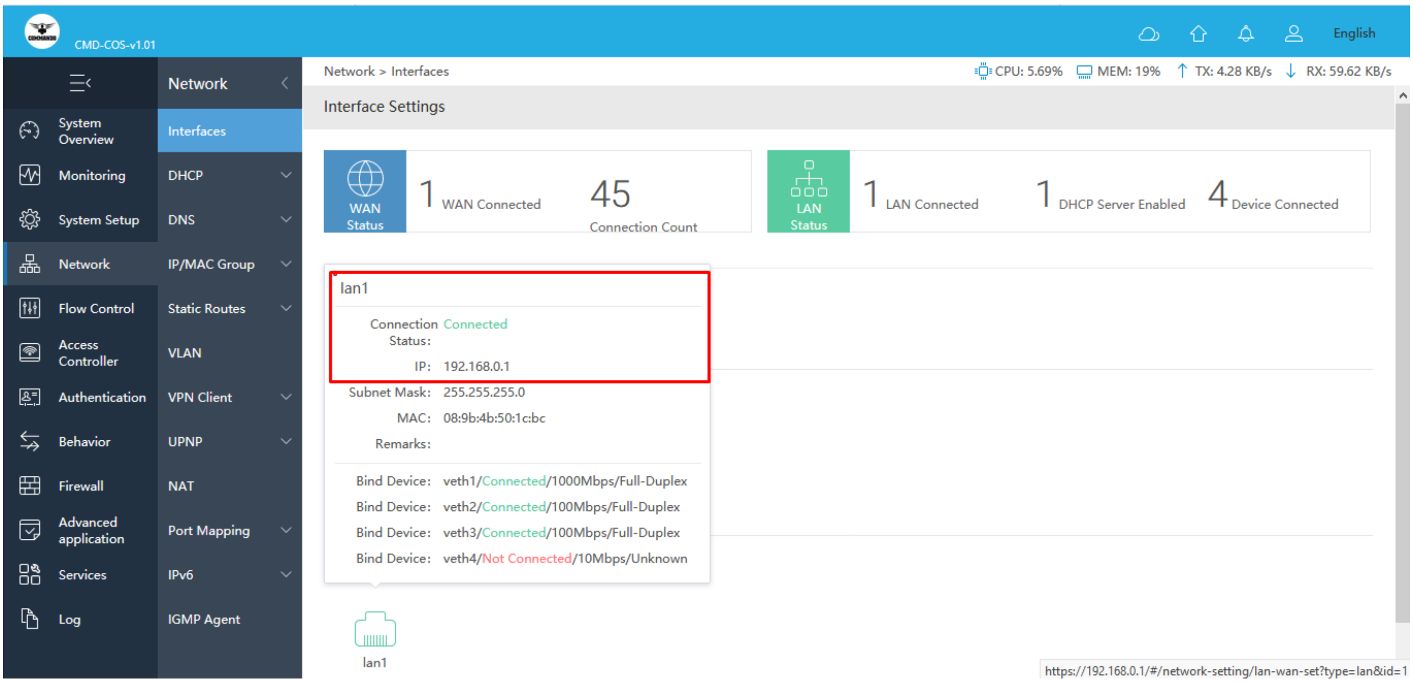
Clone MAC:

Multiple IP: Add

IP Address	Subnet Mask	Actions
No Data		

Extended Network Card: ☑ veth1 ☑ veth2 ☑ veth3 ☑ veth4

Fig 3.1.19 Binding ports 2,3,4 to LAN1 interface page



Network > Interfaces

CPU: 5.69% MEM: 19% TX: 4.28 KB/s RX: 59.62 KB/s

Interface Settings

1 WAN Connected 45 Connection Count

1 LAN Connected 1 DHCP Server Enabled 4 Device Connected

lan1

Connection Status: Connected

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

https://192.168.0.1/#/network-setting/lan-wan-set?type=lan&id=1

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 DNSA 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.

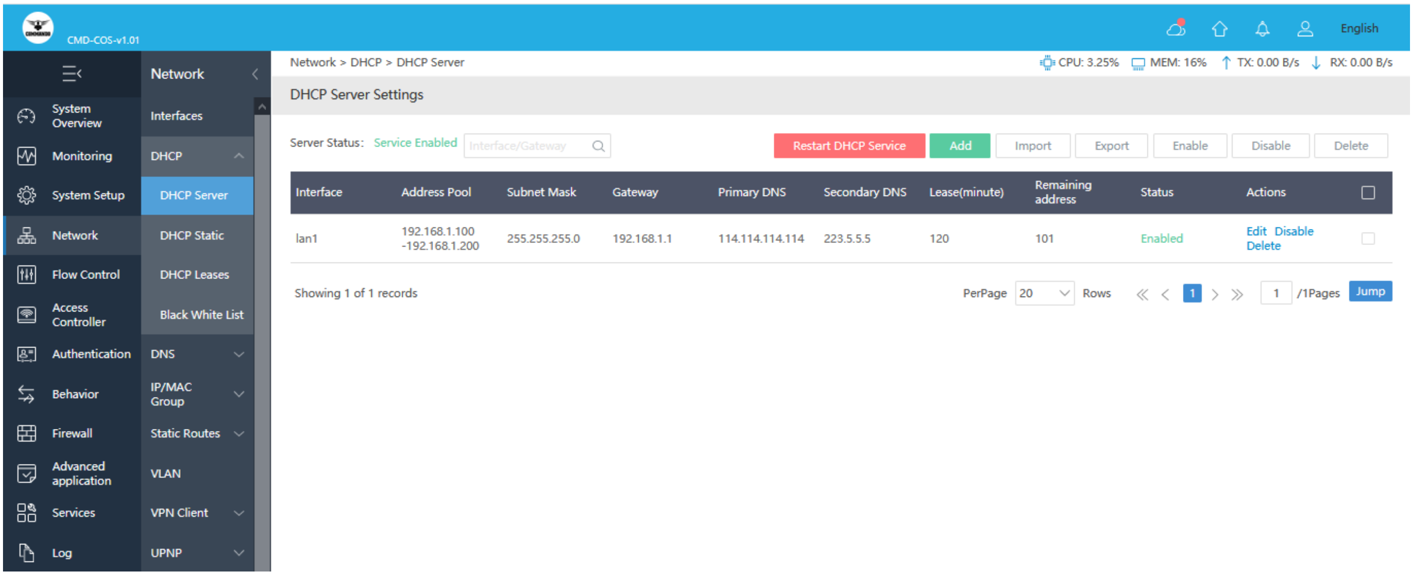
Domain Name:

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



Network > DHCP > DHCP Server

DHCP Server Settings

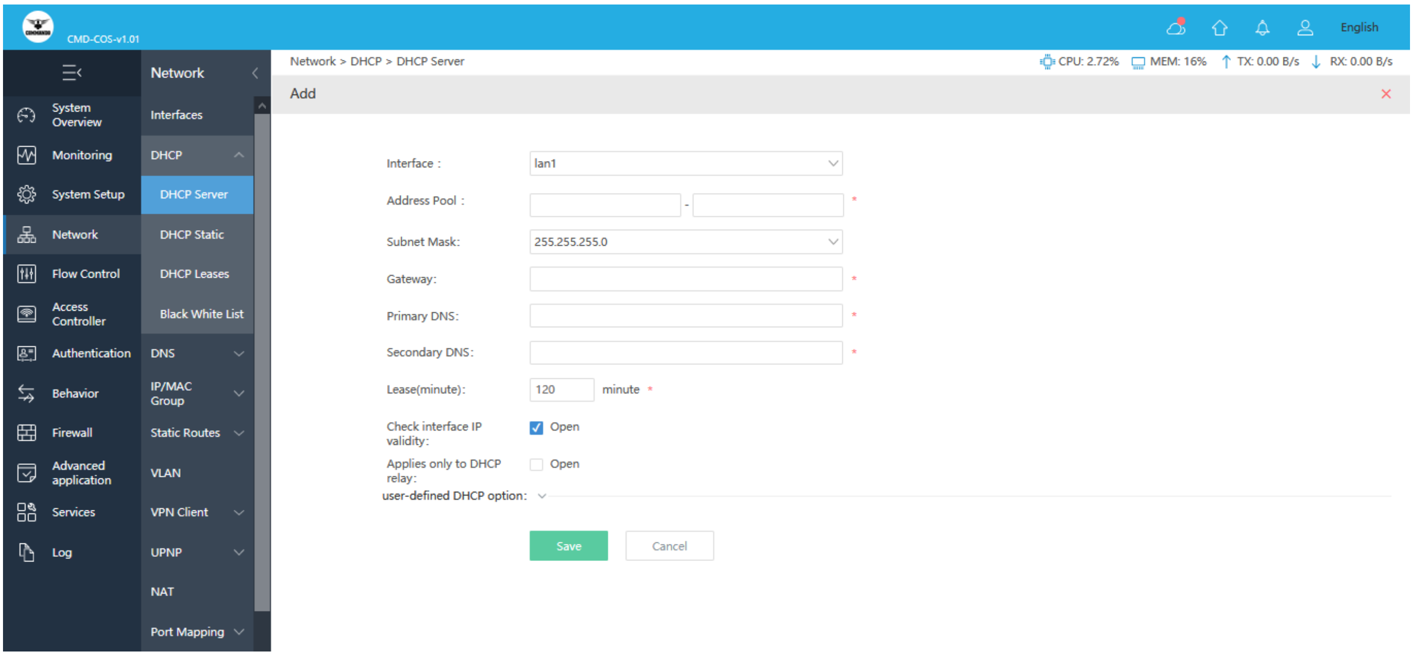
Server Status: Service Enabled

Interface	Address Pool	Subnet Mask	Gateway	Primary DNS	Secondary DNS	Lease(minute)	Remaining address	Status	Actions	□
lan1	192.168.1.100 -192.168.1.200	255.255.255.0	192.168.1.1	114.114.114.114	223.5.5.5	120	101	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows 1 /1Pages Jump

Fig 3.2.1 Default DHCP Server Settings of LAN1 interface page



Network > DHCP > DHCP Server

Add

Interface : lan1

Address Pool : -

Subnet Mask: 255.255.255.0

Gateway:

Primary DNS:

Secondary DNS:

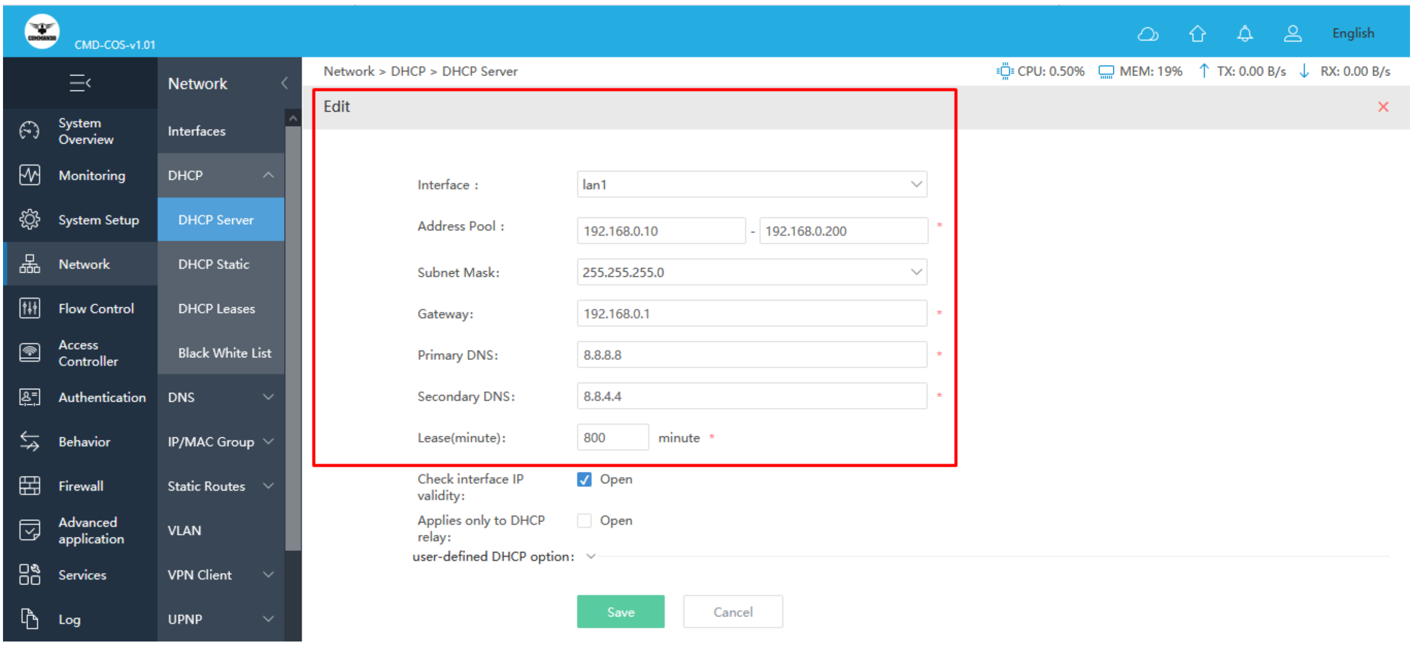
Lease(minute): 120 minute

Check interface IP validity: ☑ Open

Applies only to DHCP relay: □ Open

user-defined DHCP option:

Fig 3.2.2 Add DHCP Server Settings of LAN1 interface page



Edit

Interface : lan1

Address Pool : 192.168.0.10 - 192.168.0.200 *

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1 *

Primary DNS: 8.8.8.8 *

Secondary DNS: 8.8.4.4 *

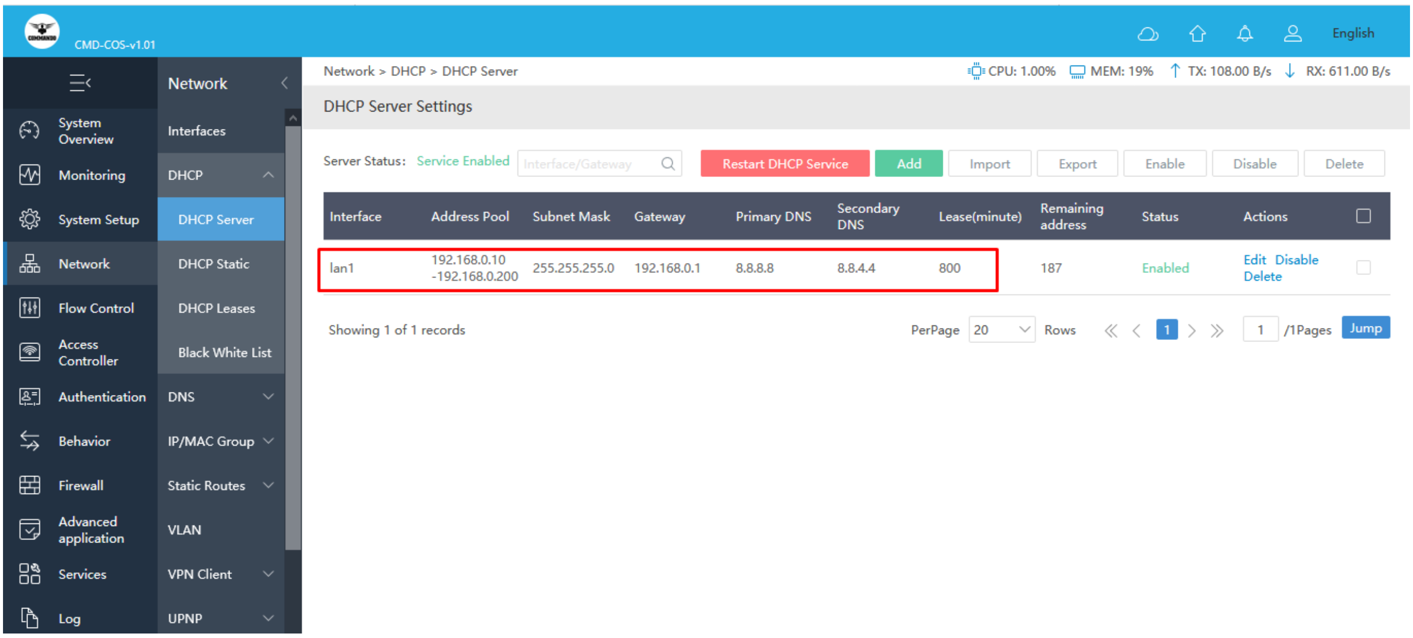
Lease(minute): 800 minute *

Check interface IP validity: ☑ Open

Applies only to DHCP relay: □ Open

user-defined DHCP option:

Fig 3.2.3 Editing DHCP Server Settings of LAN1 interface page



DHCP Server Settings

Server Status: Service Enabled

Interface	Address Pool	Subnet Mask	Gateway	Primary DNS	Secondary DNS	Lease(minute)	Remaining address	Status	Actions	□
lan1	192.168.0.10 -192.168.0.200	255.255.255.0	192.168.0.1	8.8.8.8	8.8.4.4	800	187	Enabled	Edit Disable Delete	□

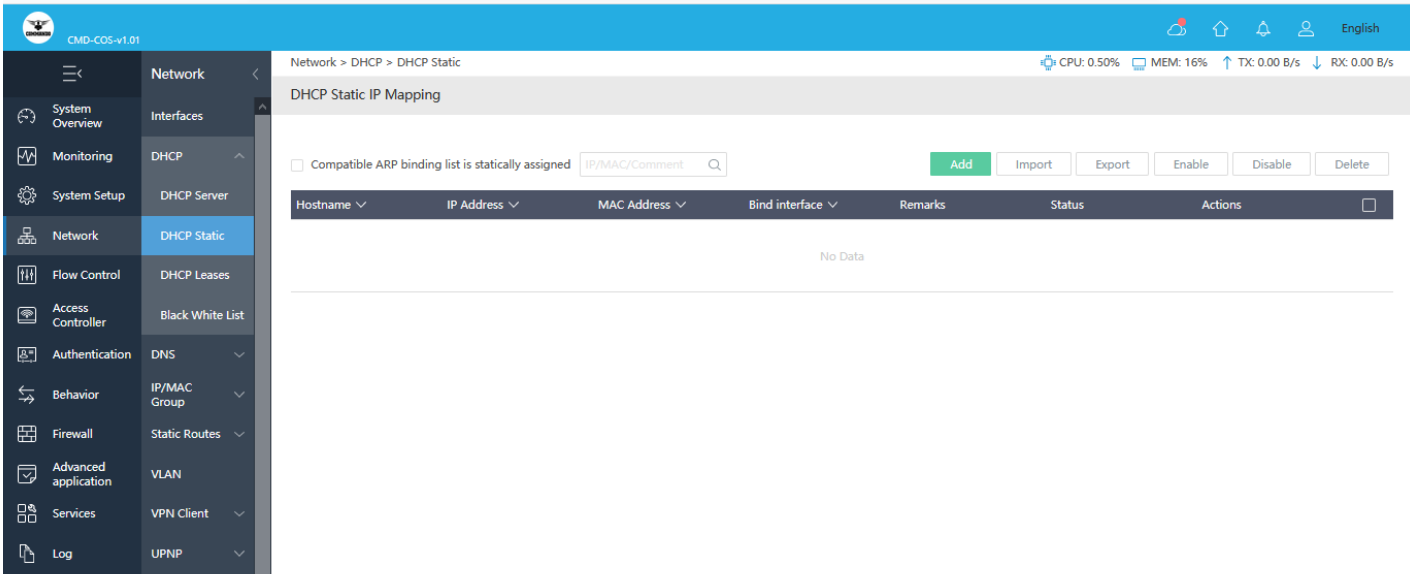
Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

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.



Network > DHCP > DHCP Static

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

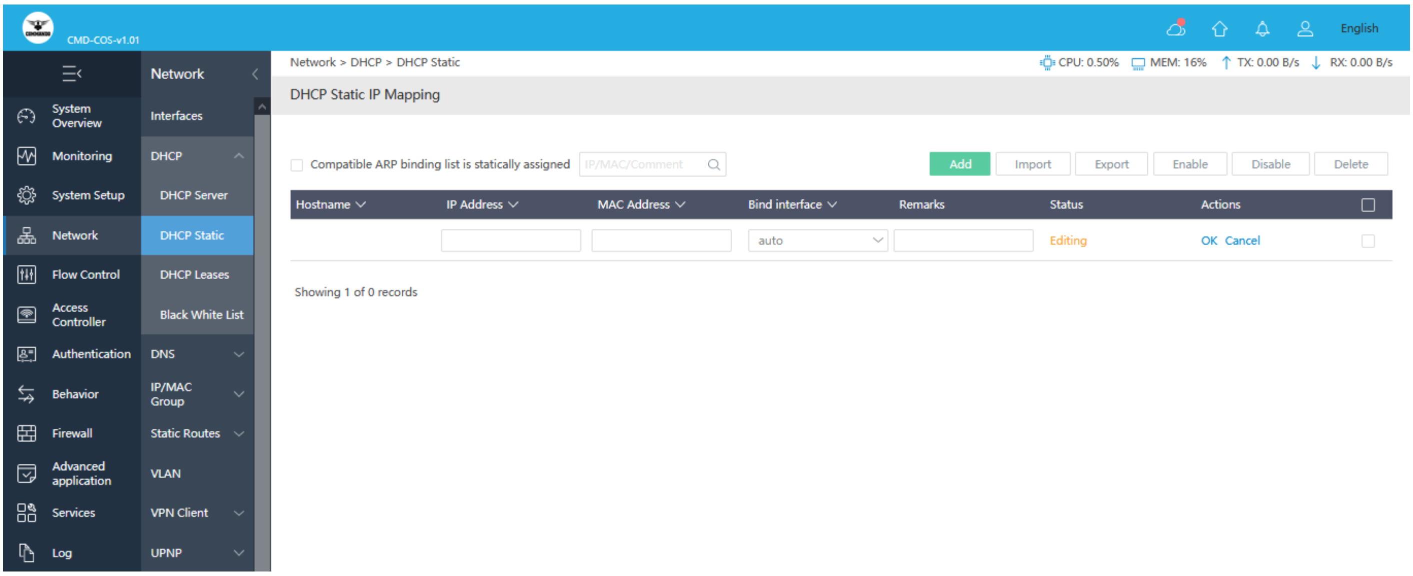
DHCP Static IP Mapping

□ Compatible ARP binding list is statically assigned [IP/MAC/Comment]

Hostname	IP Address	MAC Address	Bind interface	Remarks	Status	Actions □

No Data

Fig 3.2.5 Default DHCP Static IP Mapping page



Network > DHCP > DHCP Static

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

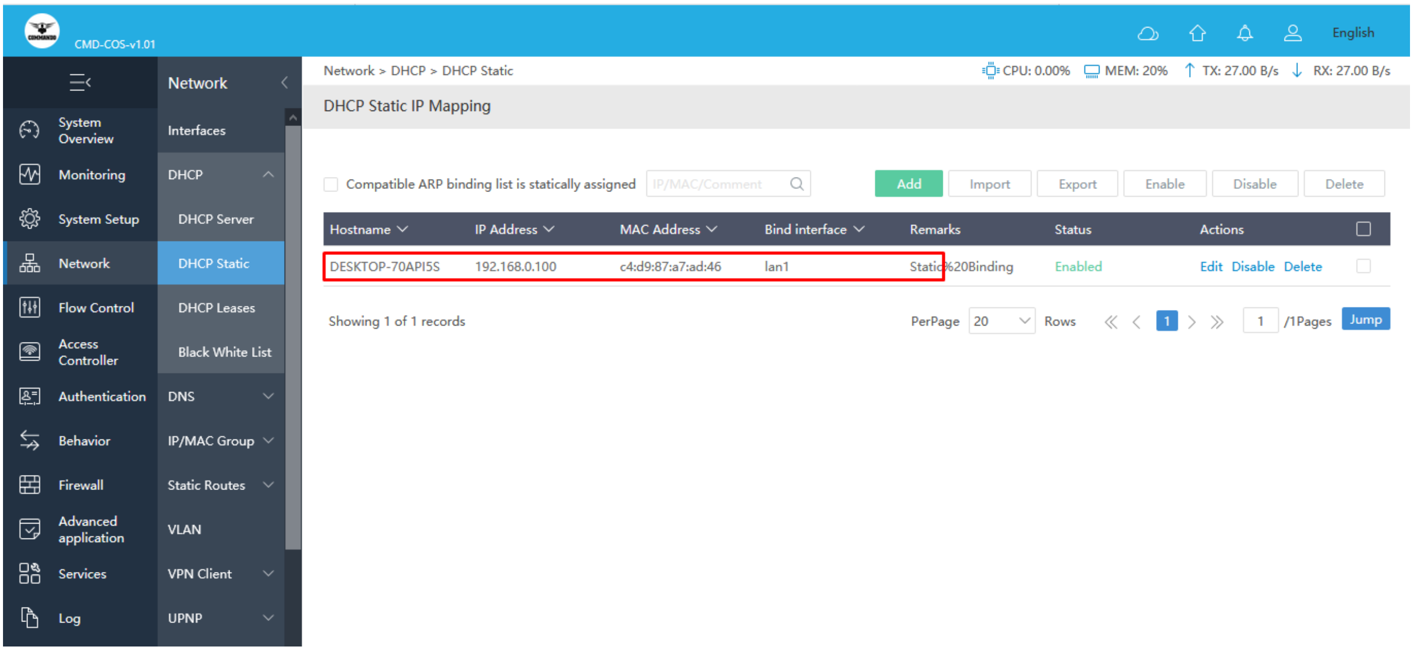
DHCP Static IP Mapping

□ Compatible ARP binding list is statically assigned [IP/MAC/Comment]

Hostname	IP Address	MAC Address	Bind interface	Remarks	Status	Actions □
			auto		Editing	OK Cancel □

Showing 1 of 0 records

Fig 3.2.6 Default DHCP Static IP Mapping Add page



Network > DHCP > DHCP Static

CPU: 0.00% MEM: 20% TX: 27.00 B/s RX: 27.00 B/s

DHCP Static IP Mapping

□ Compatible ARP binding list is statically assigned   IP/MAC/Comment

Hostname	IP Address	MAC Address	Bind interface	Remarks	Status	Actions	□
DESKTOP-70API5S	192.168.0.100	c4:d9:87:a7:ad:46	lan1	Static%20Binding	Enabled	Edit Disable Delete	□

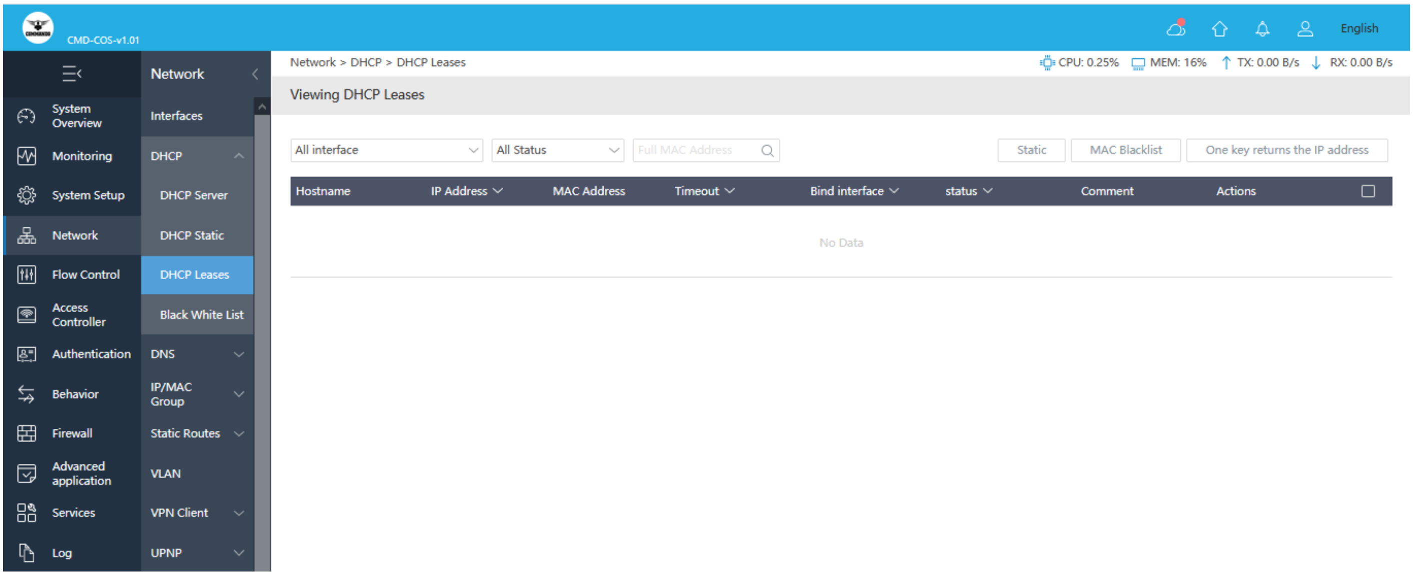
Showing 1 of 1 records   PerPage 20 Rows   1   1 /1Pages Jump

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



Network > DHCP > DHCP Leases

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

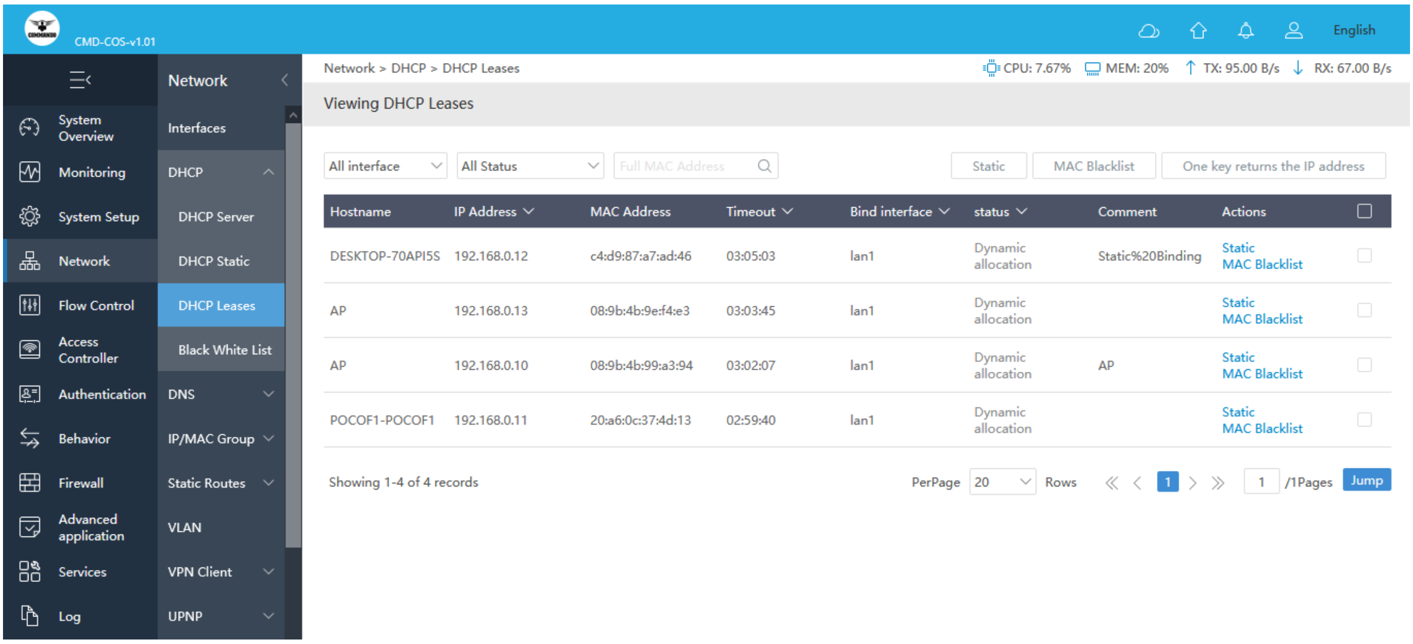
Viewing DHCP Leases

All interface   All Status   Full MAC Address

Hostname	IP Address	MAC Address	Timeout	Bind interface	status	Comment	Actions	□

No Data

Fig 3.2.8 Default Viewing DHCP Leases page



Network > DHCP > DHCP Leases

CPU: 7.67% MEM: 20% TX: 95.00 B/s RX: 67.00 B/s

Viewing DHCP Leases

Hostname	IP Address	MAC Address	Timeout	Bind interface	status	Comment	Actions	□
DESKTOP-70API5S	192.168.0.12	c4:d9:87:a7:ad:46	03:05:03	lan1	Dynamic allocation	Static%20Binding	Static MAC Blacklist	□
AP	192.168.0.13	08:9b:4b:9e:f4:e3	03:03:45	lan1	Dynamic allocation		Static MAC Blacklist	□
AP	192.168.0.10	08:9b:4b:99:a3:94	03:02:07	lan1	Dynamic allocation	AP	Static MAC Blacklist	□
POCOF1-POCOF1	192.168.0.11	20:a6:0c:37:4d:13	02:59:40	lan1	Dynamic allocation		Static MAC Blacklist	□

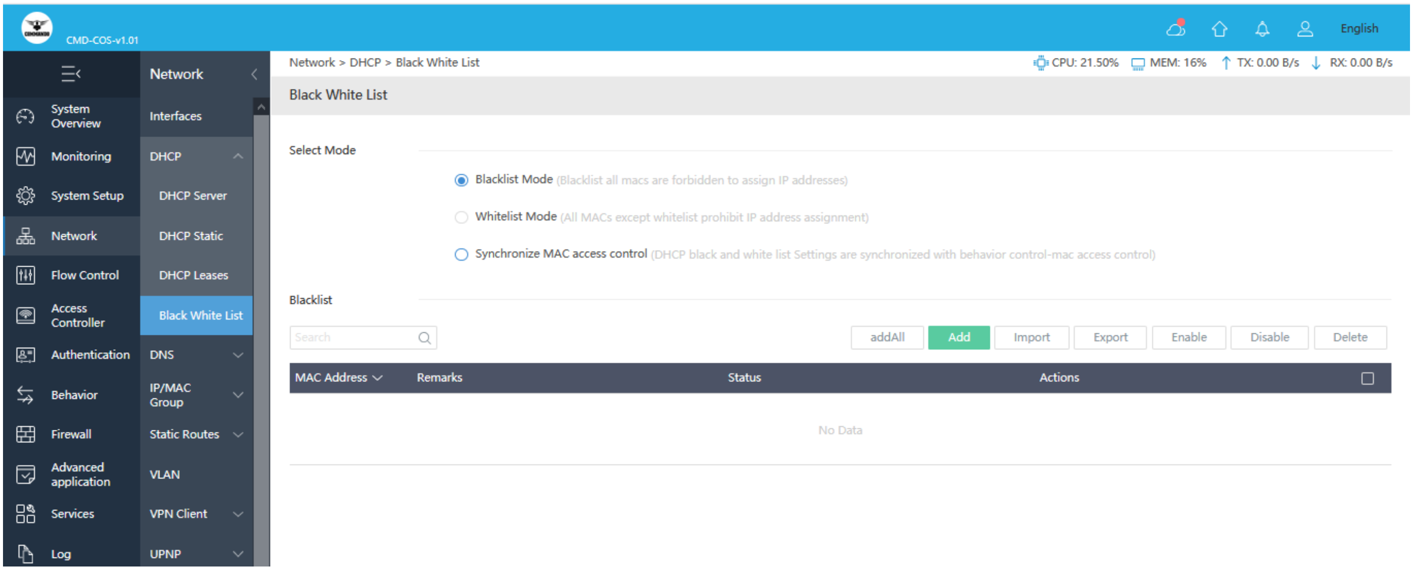
Showing 1-4 of 4 records

PerPage 20 Rows 1 1 /1Pages

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



Network > DHCP > Black White List

CPU: 21.50% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Black White List

Select Mode

● Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses)

○ Whitelist Mode (All MACs except whitelist prohibit IP address assignment)

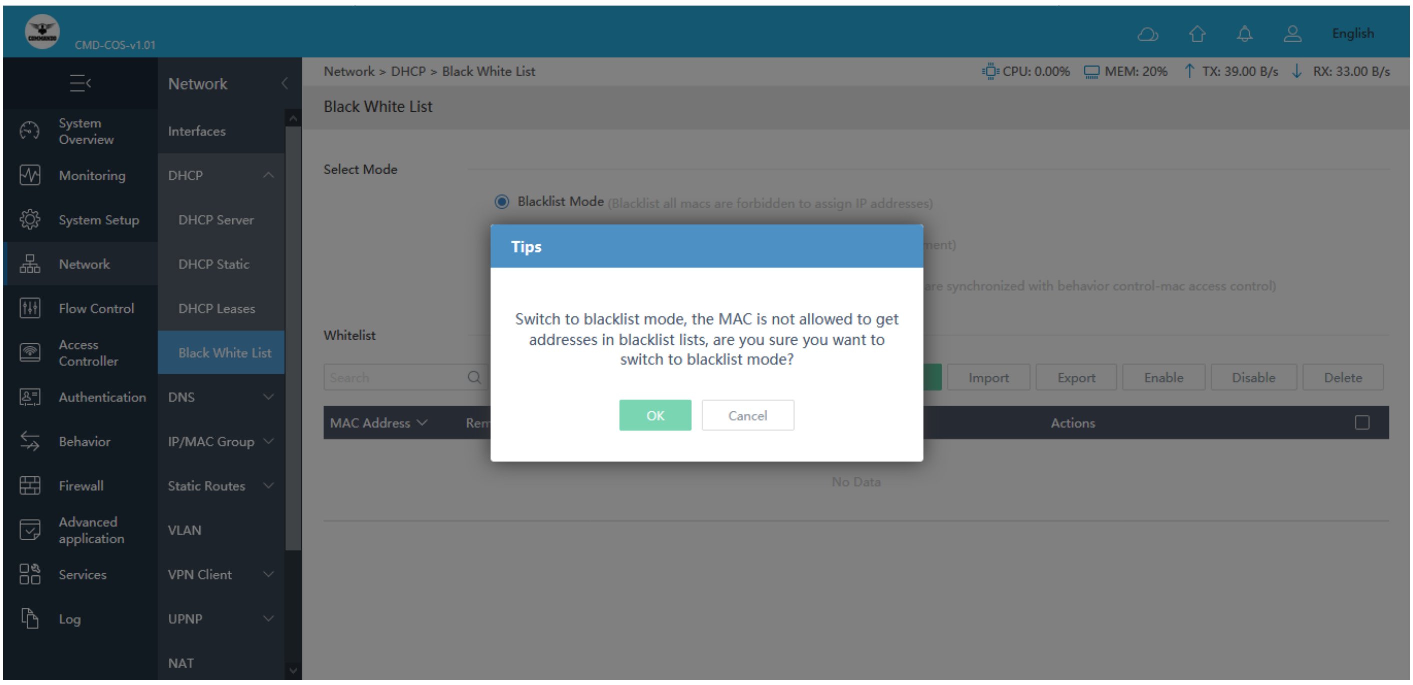
○ Synchronize MAC access control (DHCP black and white list Settings are synchronized with behavior control-mac access control)

Blacklist

MAC Address	Remarks	Status	Actions	□

No Data

Fig 3.2.10 Default Blacklist Mode setting in device page



Black White List

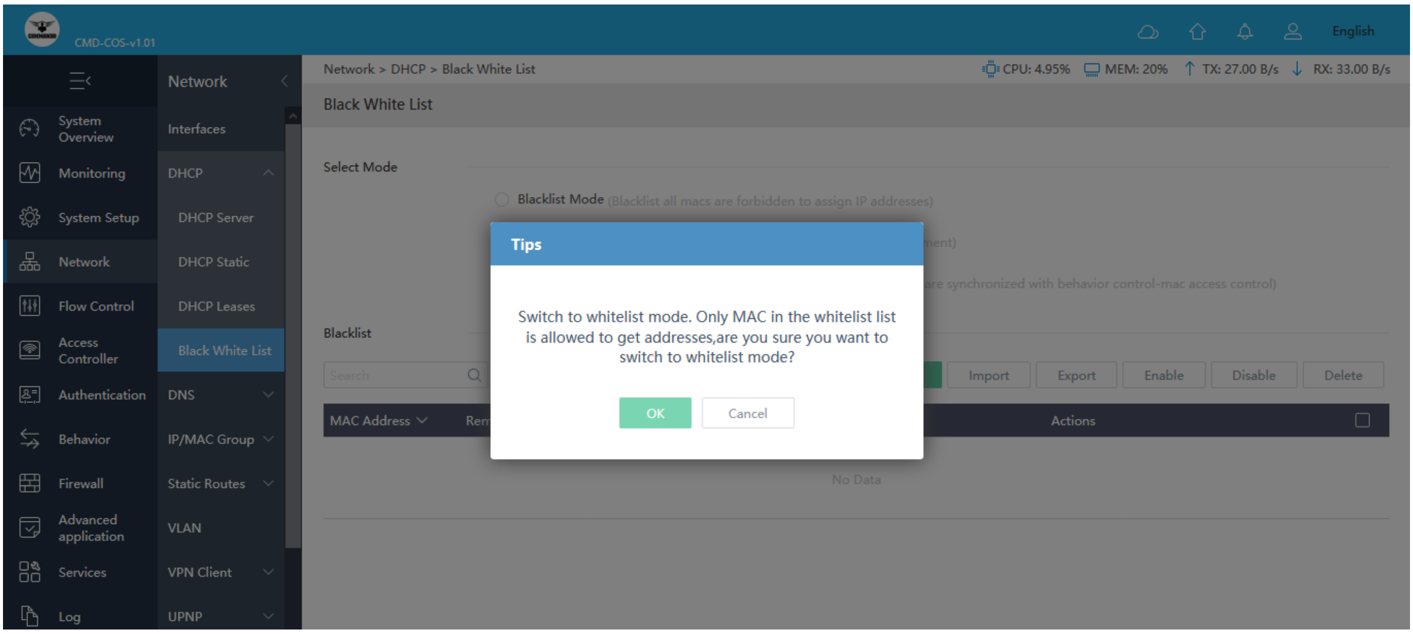
Select Mode

● Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses)

Tips

Switch to blacklist mode, the MAC is not allowed to get addresses in blacklist lists, are you sure you want to switch to blacklist mode?

Fig 3.2.11 Blacklist Mode setting in device page



Black White List

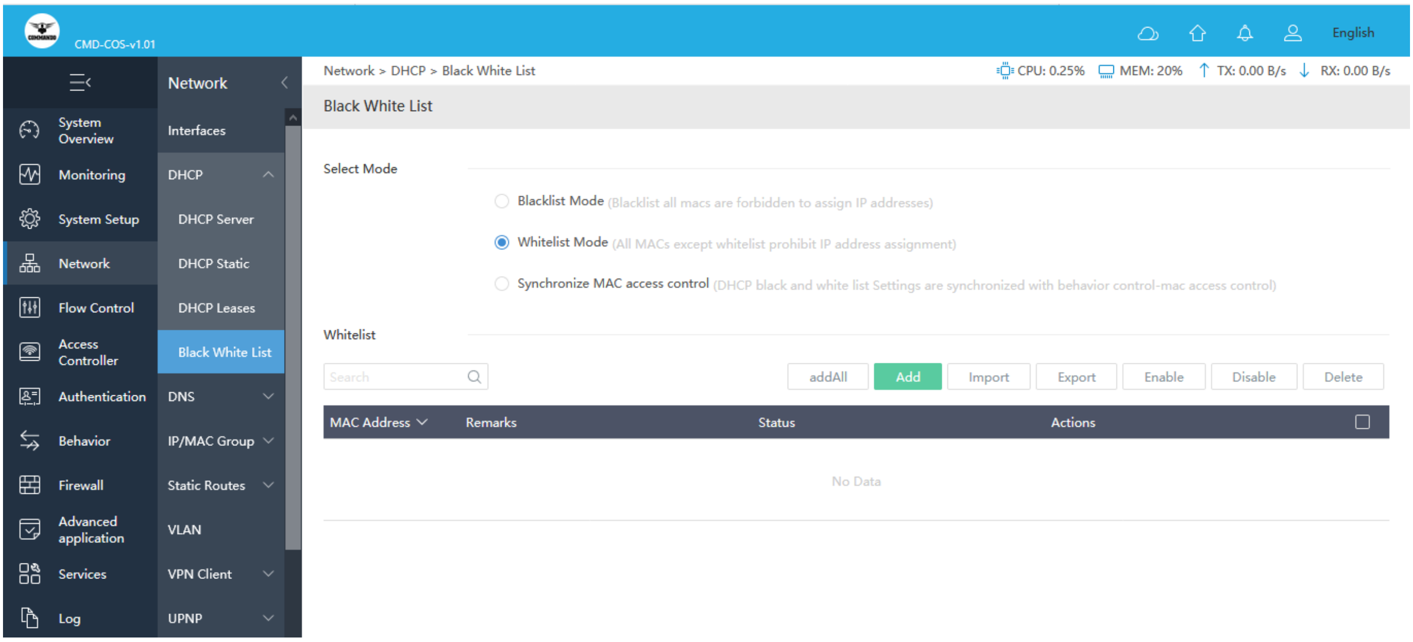
Select Mode

○ Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses)

Tips

Switch to whitelist mode. Only MAC in the whitelist list is allowed to get addresses,are you sure you want to switch to whitelist mode?

Fig 3.2.12 Changing mode to Whitelist Mode setting in device page



Black White List

Select Mode

○ Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses)

● Whitelist Mode (All MACs except whitelist prohibit IP address assignment)

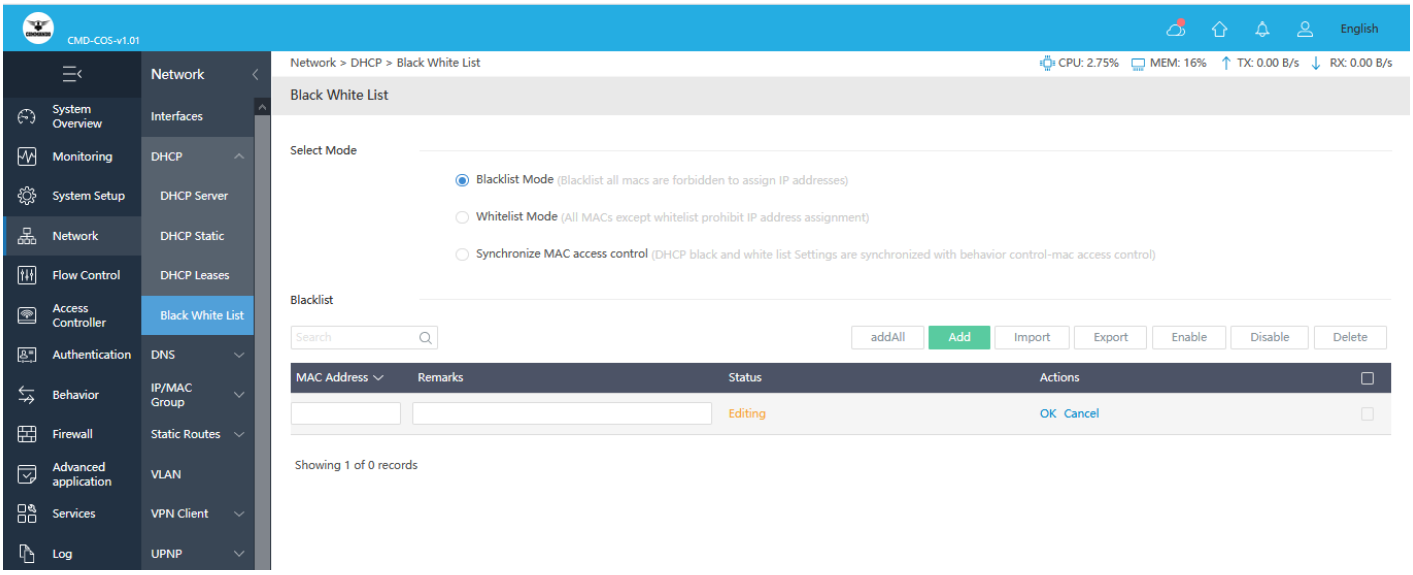
○ Synchronize MAC access control (DHCP black and white list Settings are synchronized with behavior control-mac access control)

Whitelist

MAC Address	Remarks	Status	Actions	□

No Data

Fig 3.2.13 White list Mode setting in device page



Black White List

Select Mode

● Blacklist Mode (Blacklist all macs are forbidden to assign IP addresses)

○ Whitelist Mode (All MACs except whitelist prohibit IP address assignment)

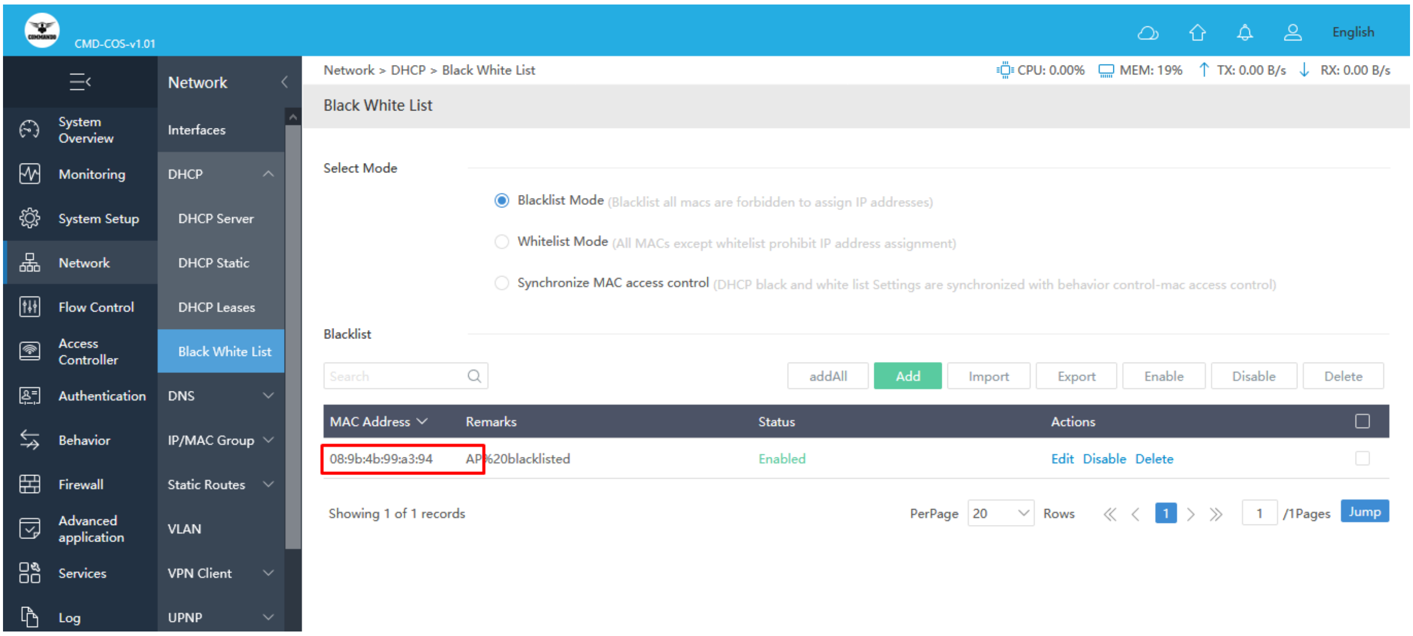
○ Synchronize MAC access control (DHCP black and white list Settings are synchronized with behavior control-mac access control)

Blacklist

MAC Address	Remarks	Status	Actions	□
		Editing	OK Cancel	□

Showing 1 of 0 records

Fig 3.2.14 Blacklist mode add page



Network > DHCP > Black White List

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

Black White List

Select Mode

● 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)

Blacklist

Search | addAll | Add | Import | Export | Enable | Disable | Delete

MAC Address	Remarks	Status	Actions	□
08:9b:4b:99:a3:94	AP%20blacklisted	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

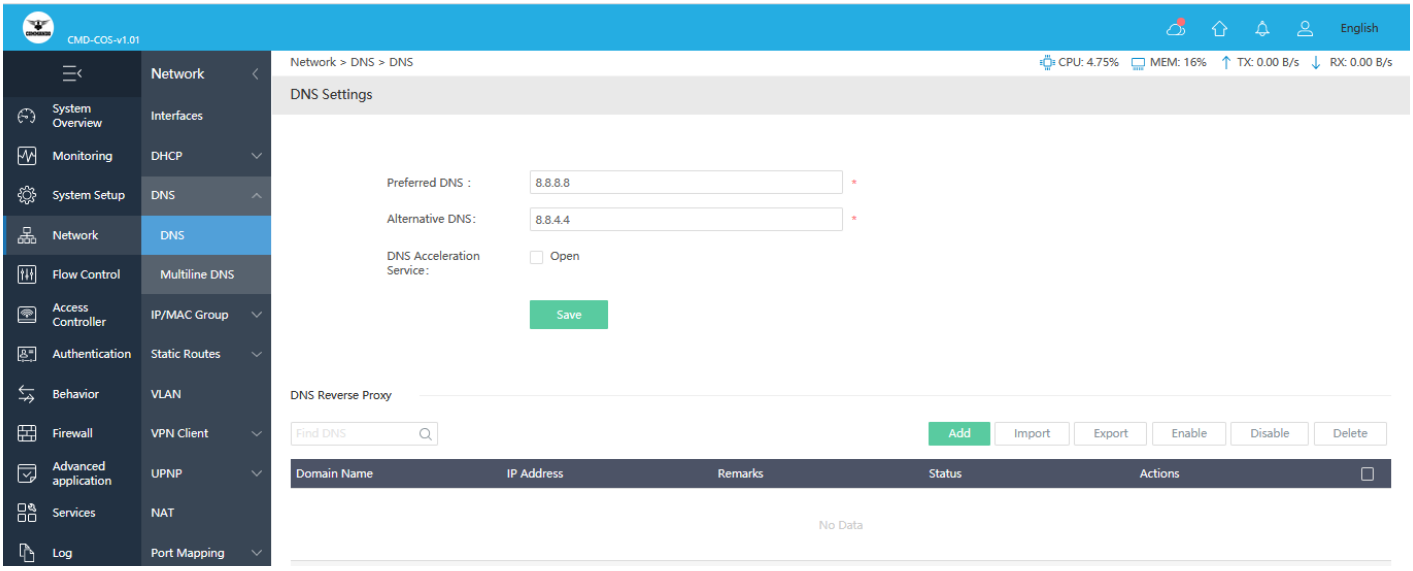
Fig 3.2.14 Blacklist mode MAC address page

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



Network > DNS > DNS

CPU: 4.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

DNS Settings

Preferred DNS : 8.8.8.8 *

Alternative DNS: 8.8.4.4 *

DNS Acceleration Service: □ Open

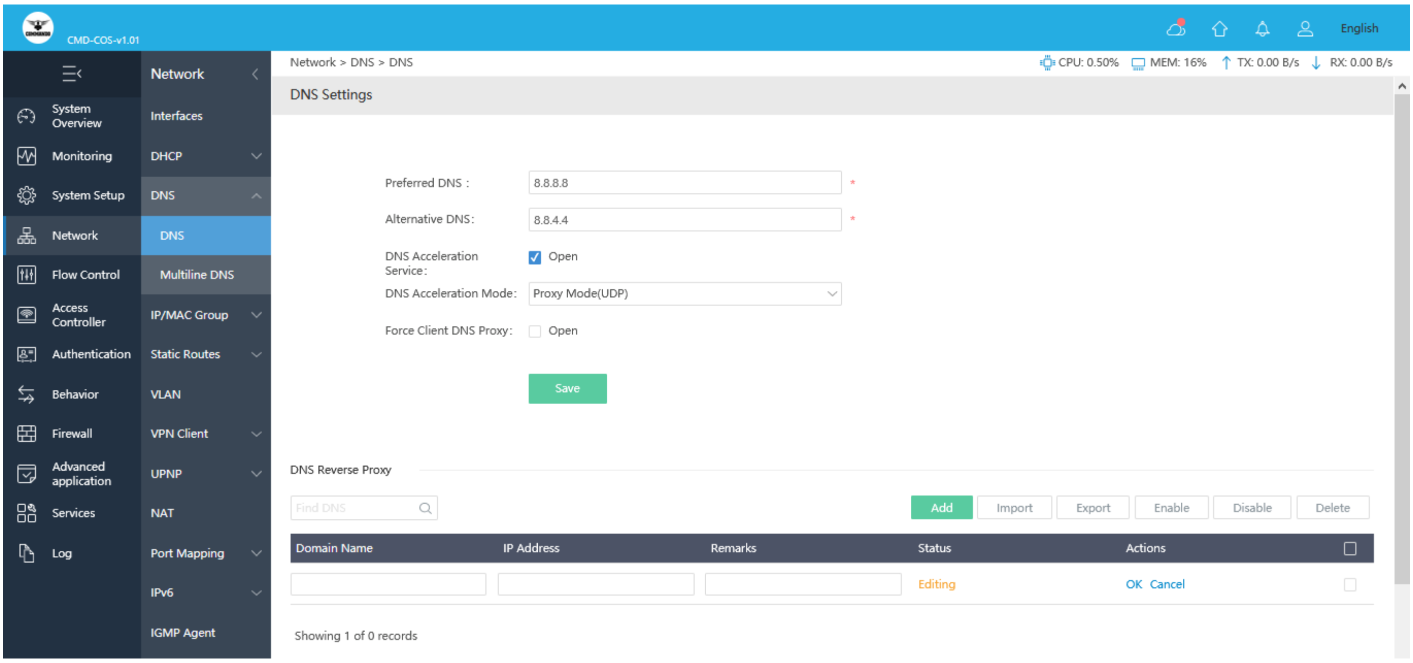
Save

DNS Reverse Proxy

Find DNS | Add | Import | Export | Enable | Disable | Delete

Domain Name	IP Address	Remarks	Status	Actions	□
No Data					

Fig 3.3.1 Default DNS Settings page



DNS Settings

Preferred DNS : 8.8.8.8 *

Alternative DNS: 8.8.4.4 *

DNS Acceleration Service: ☑ Open

DNS Acceleration Mode: Proxy Mode(UDP)

Force Client DNS Proxy: □ Open

DNS Reverse Proxy

Domain Name	IP Address	Remarks	Status	Actions	□
			Editing	OK Cancel	□

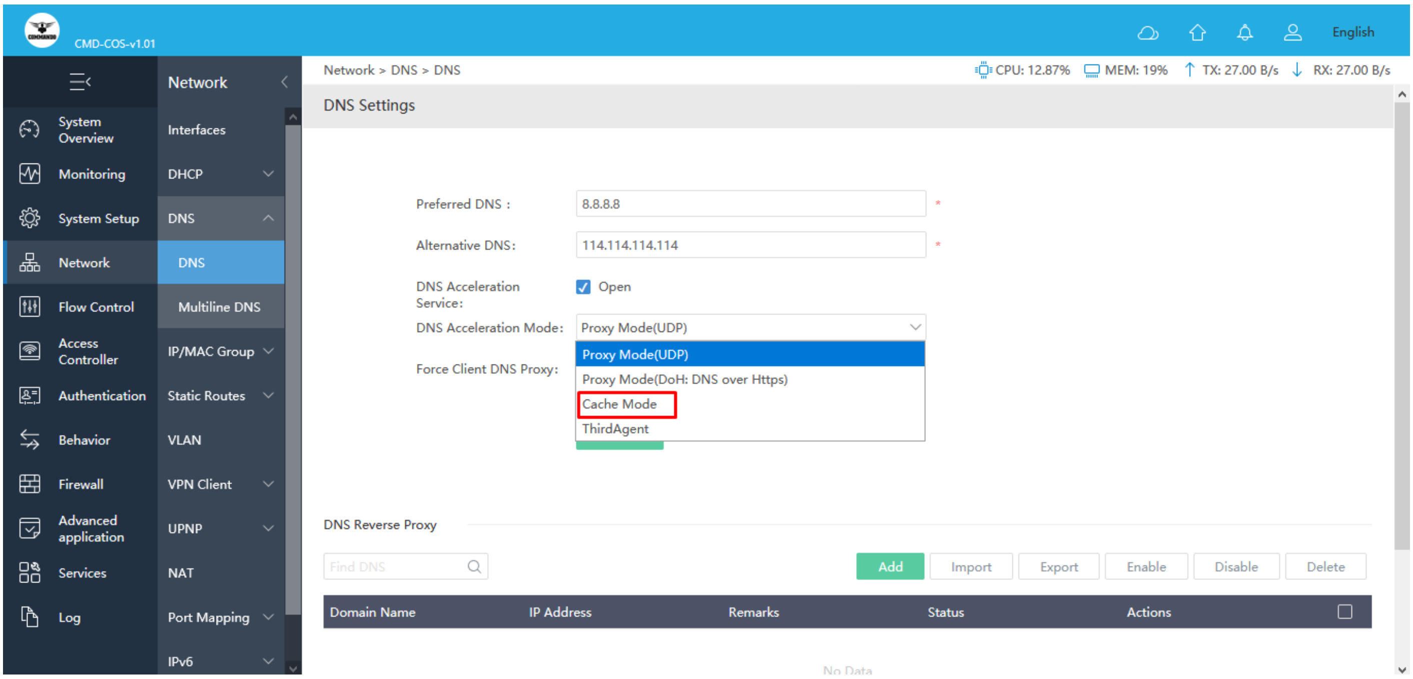
Showing 1 of 0 records

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.



DNS Settings

Preferred DNS : 8.8.8.8 *

Alternative DNS: 114.114.114.114 *

DNS Acceleration Service: ☑ Open

DNS Acceleration Mode: Proxy Mode(UDP)

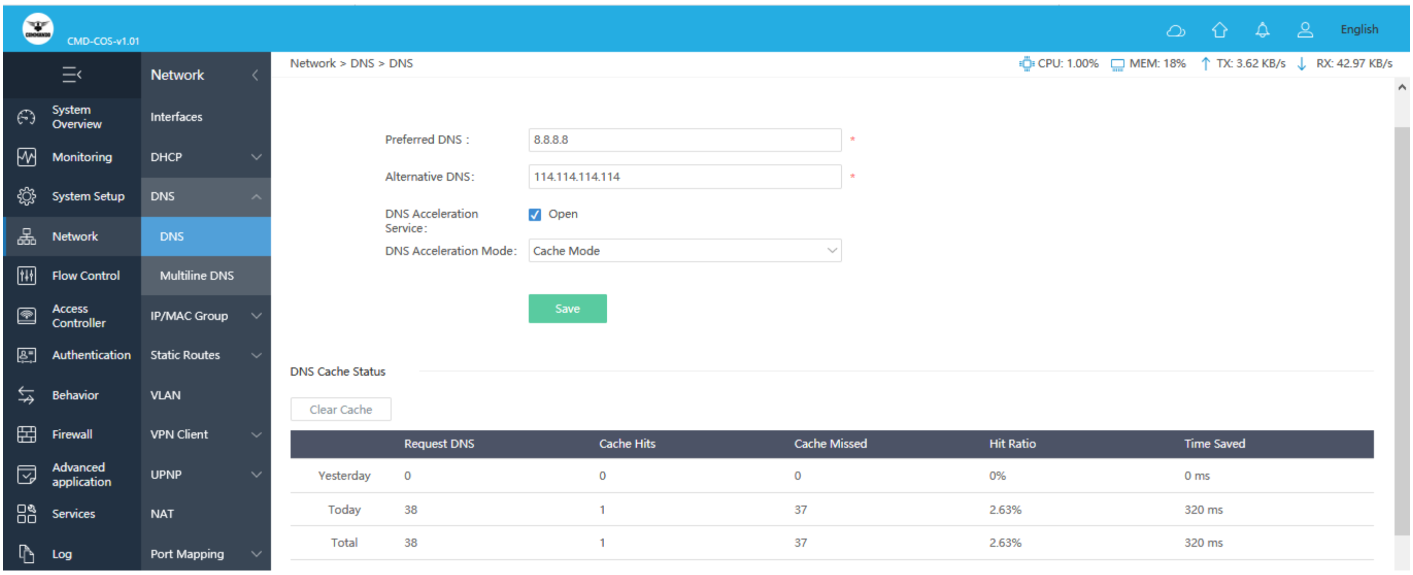
Force Client DNS Proxy:

DNS Reverse Proxy

Domain Name	IP Address	Remarks	Status	Actions	□

No Data

Fig 3.3.3 Changing DNS acceleration mode to cache page



Preferred DNS : 8.8.8.8 *

Alternative DNS: 114.114.114.114 *

DNS Acceleration Service: ☑ Open

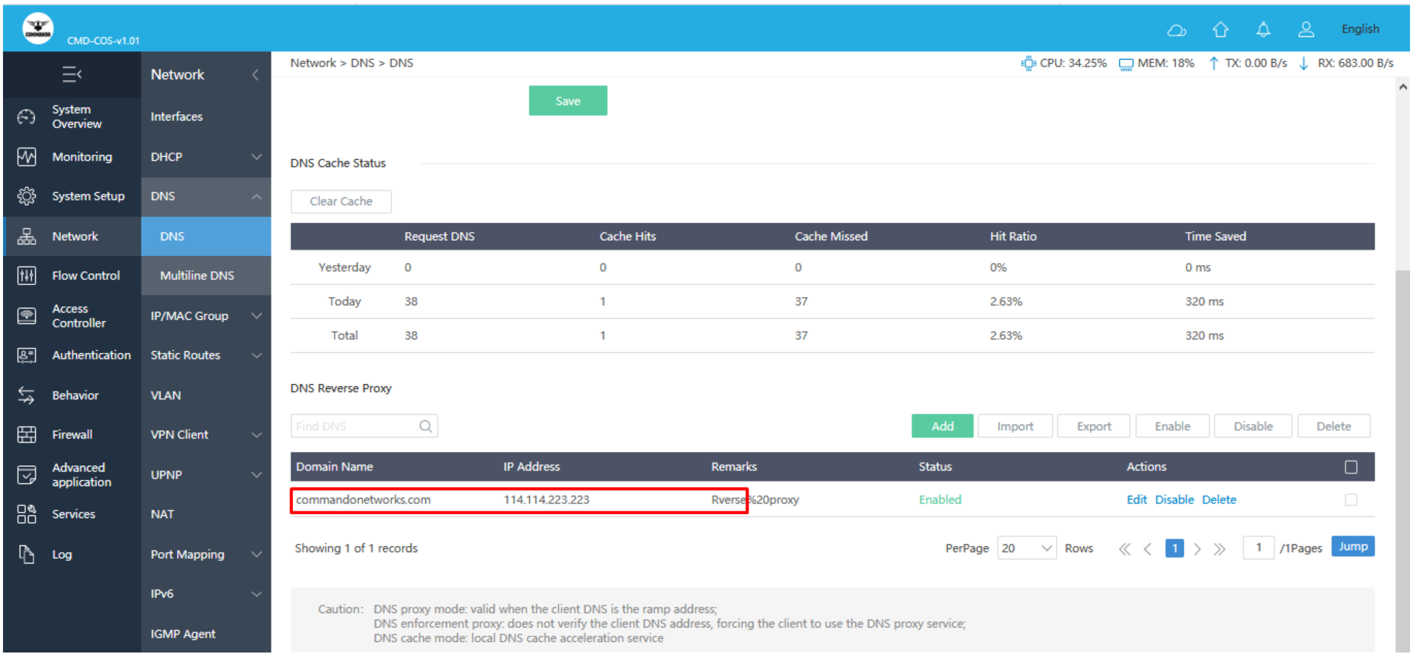
DNS Acceleration Mode: Cache Mode

DNS Cache Status

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

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.



DNS Cache Status

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

DNS Reverse Proxy

Domain Name	IP Address	Remarks	Status	Actions	□
commandonetworks.com	114.114.223.223	Rverse%20proxy	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

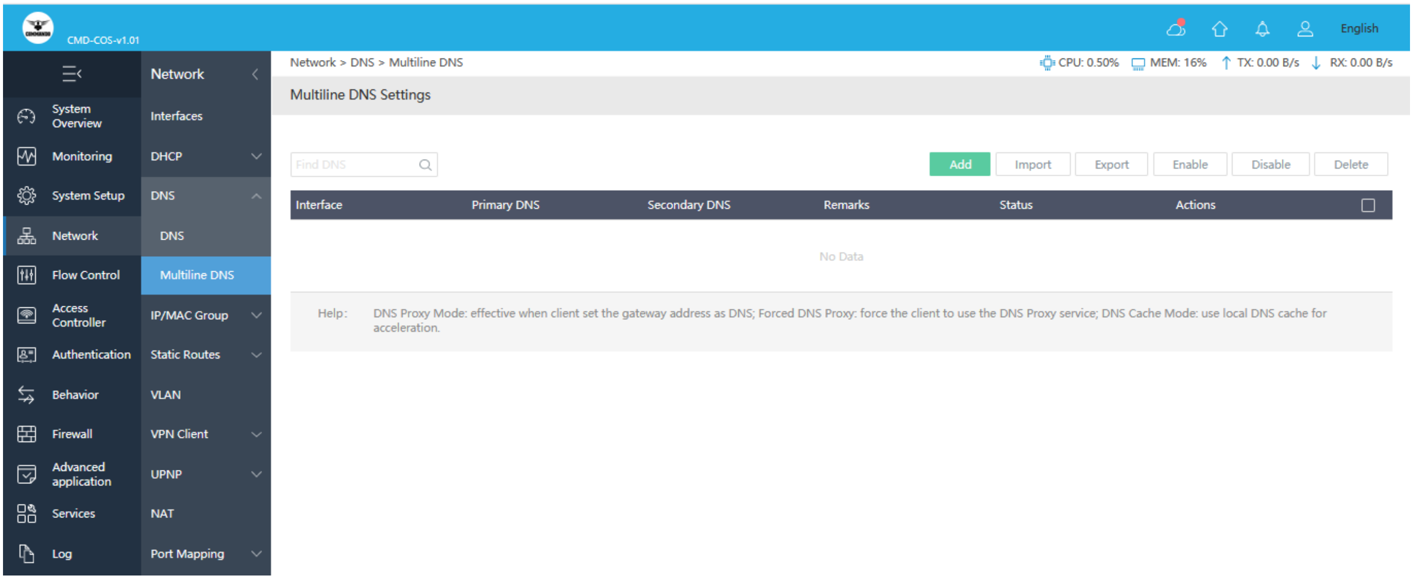
Caution: DNS proxy mode: valid when the client DNS is the ramp address;
DNS enforcement proxy: does not verify the client DNS address, forcing the client to use the DNS proxy service;
DNS cache mode: local DNS cache acceleration service

Fig 3.3.5 DNS Reverse Proxy page

Multiline DNS Settings:

When multiple WAN connected to your 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



Network > DNS > Multiline DNS

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

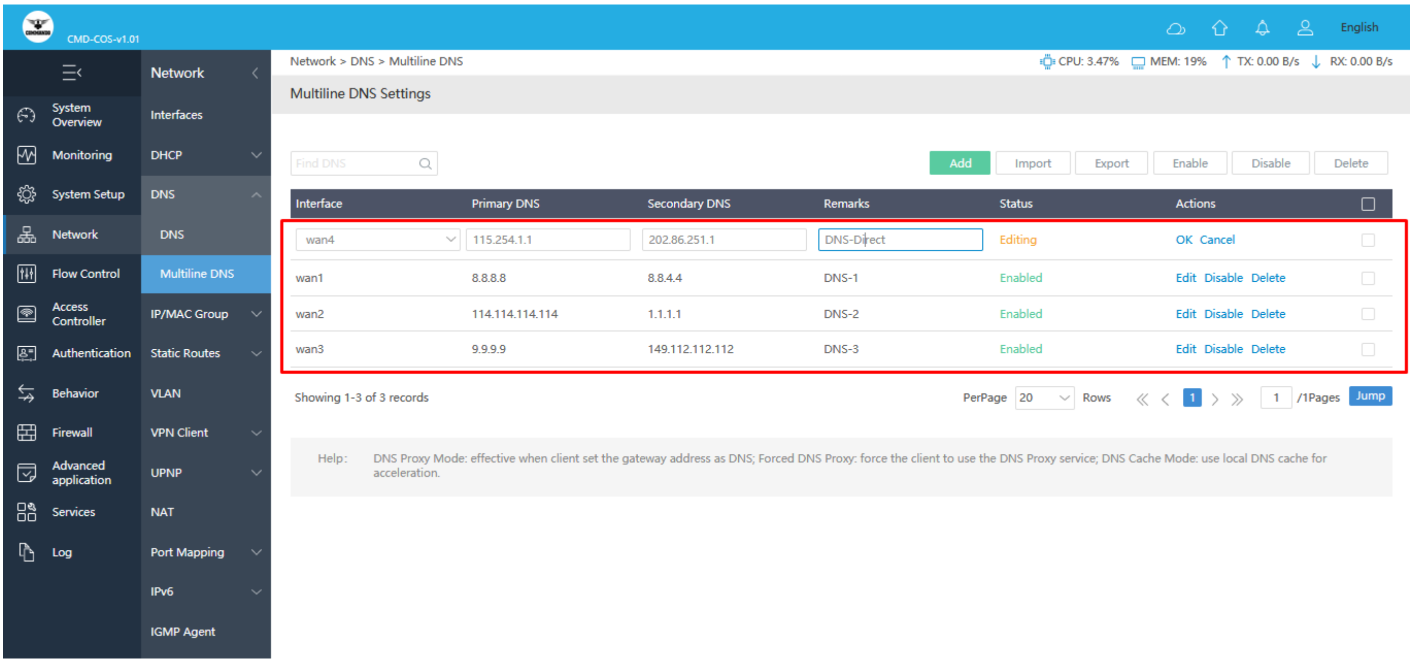
Multiline DNS Settings

Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions □

No Data

Help: DNS Proxy Mode: effective when client set the gateway address as DNS; Forced DNS Proxy: force the client to use the DNS Proxy service; DNS Cache Mode: use local DNS cache for acceleration.

Fig 3.3.6 Default Multiline DNS Settings page



Network > DNS > Multiline DNS

CPU: 3.47% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Multiline DNS Settings

Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions □
wan4	115.254.1.1	202.86.251.1	DNS-Direct	Editing	OK Cancel □
wan1	8.8.8.8	8.8.4.4	DNS-1	Enabled	Edit Disable Delete □
wan2	114.114.114.114	1.1.1.1	DNS-2	Enabled	Edit Disable Delete □
wan3	9.9.9.9	149.112.112.112	DNS-3	Enabled	Edit Disable Delete □

Showing 1-3 of 3 records PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

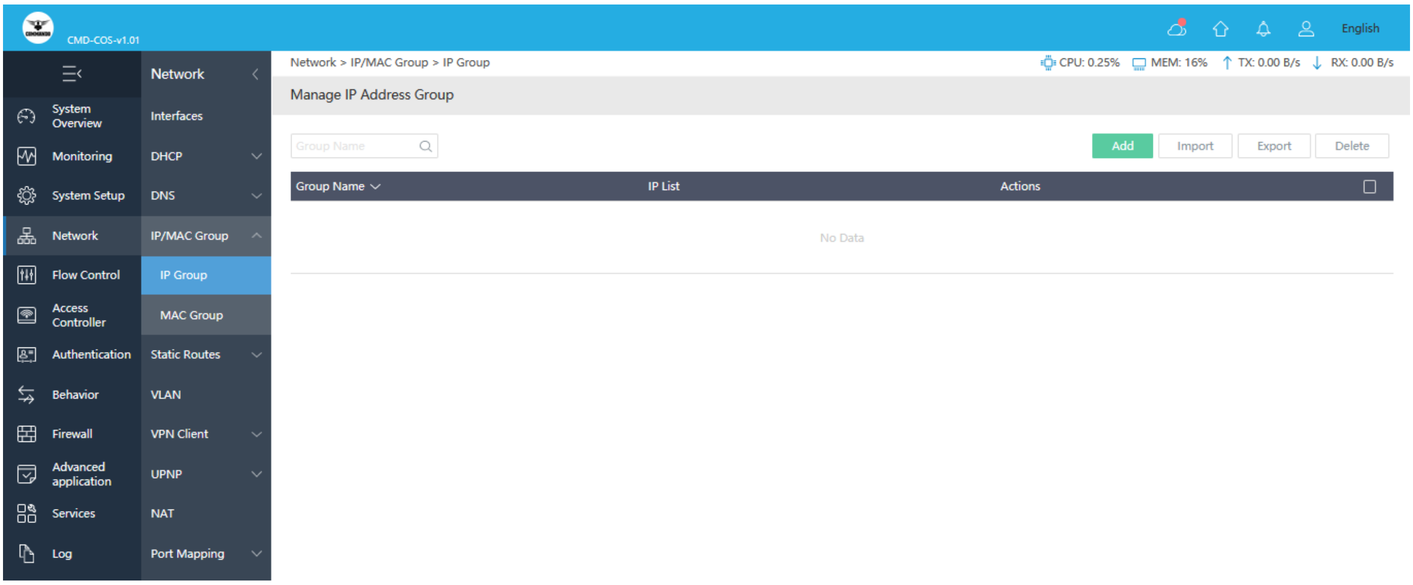
Help: DNS Proxy Mode: effective when client set the gateway address as DNS; Forced DNS Proxy: force the client to use the DNS Proxy service; DNS Cache Mode: use local DNS cache for acceleration.

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



Network > IP/MAC Group > IP Group

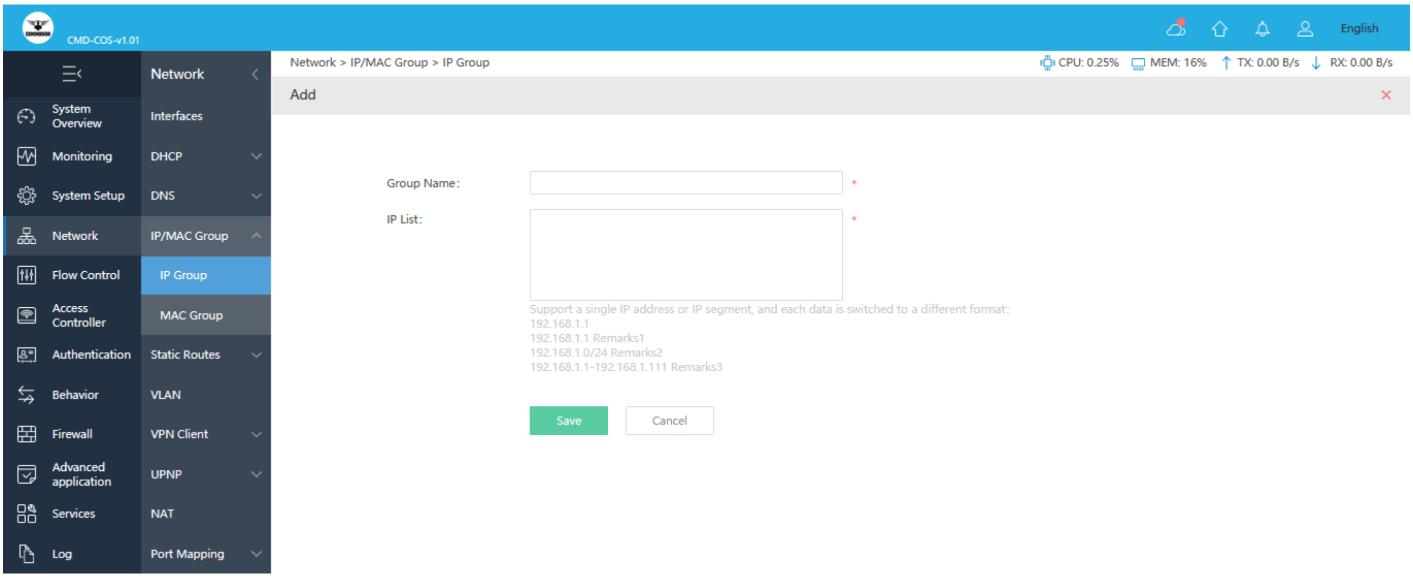
Manage IP Address Group

Group Name	IP List	Actions

No Data

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.



Network > IP/MAC Group > IP Group

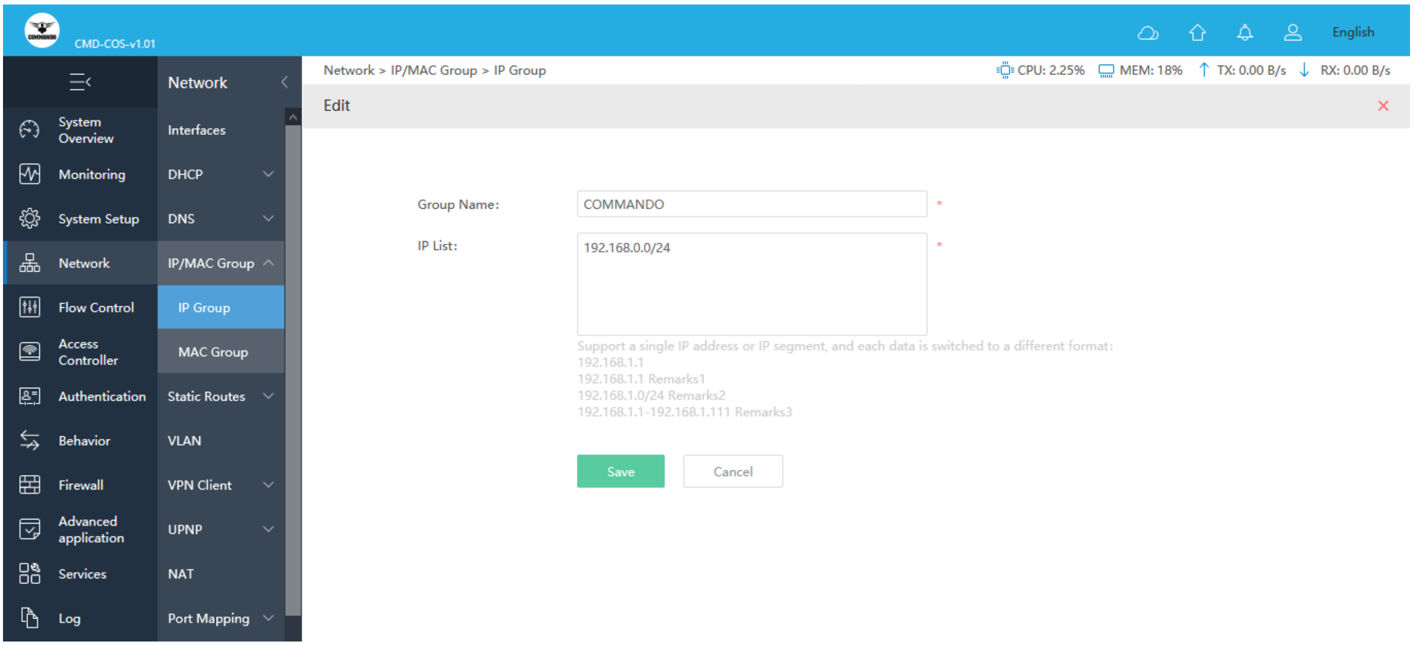
Add

Group Name: *

IP List: *

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

Fig 3.4.2 Default Add IP Address Group page



Network > IP/MAC Group > IP Group

CPU: 2.25% MEM: 18% TX: 0.00 B/s RX: 0.00 B/s

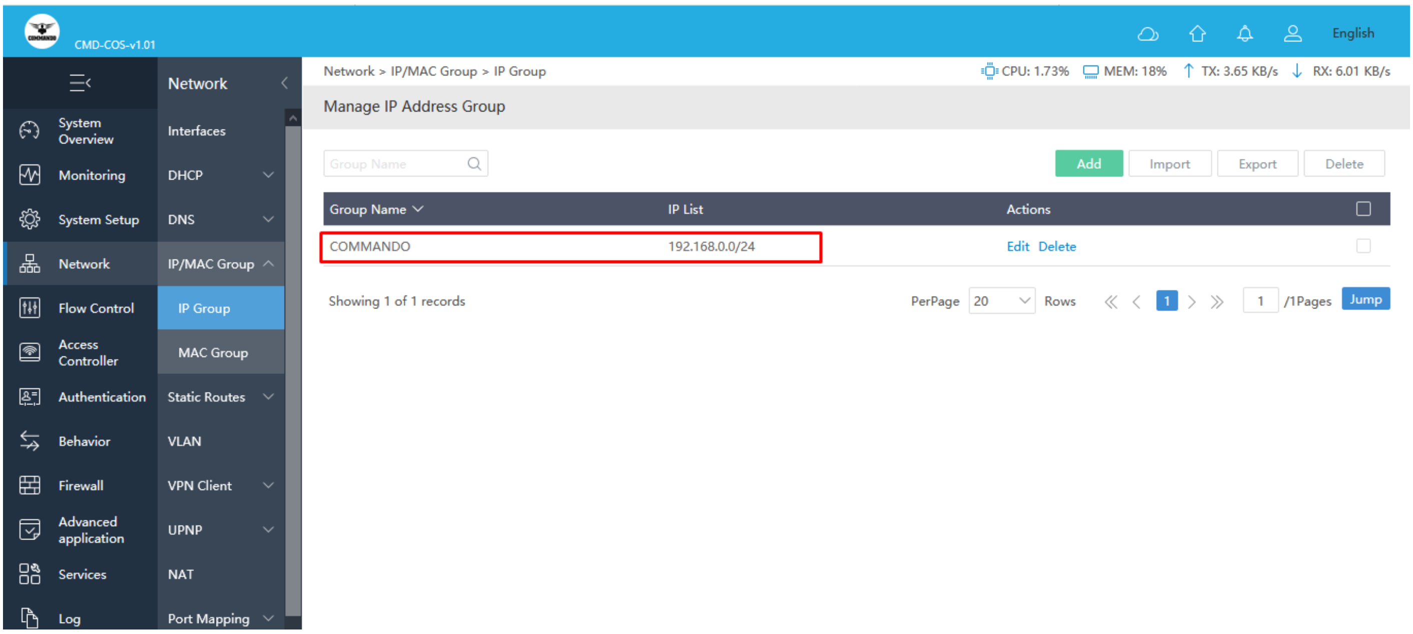
Edit

Group Name: COMMANDO *

IP List: 192.168.0.0/24 *

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

Fig 3.4.3 Edit IP Address Group page



Network > IP/MAC Group > IP Group

CPU: 1.73% MEM: 18% TX: 3.65 KB/s RX: 6.01 KB/s

Manage IP Address Group

Group Name	IP List	Actions	□
COMMANDO	192.168.0.0/24	Edit Delete	□

Showing 1 of 1 records PerPage 20 Rows 1 /1Pages

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

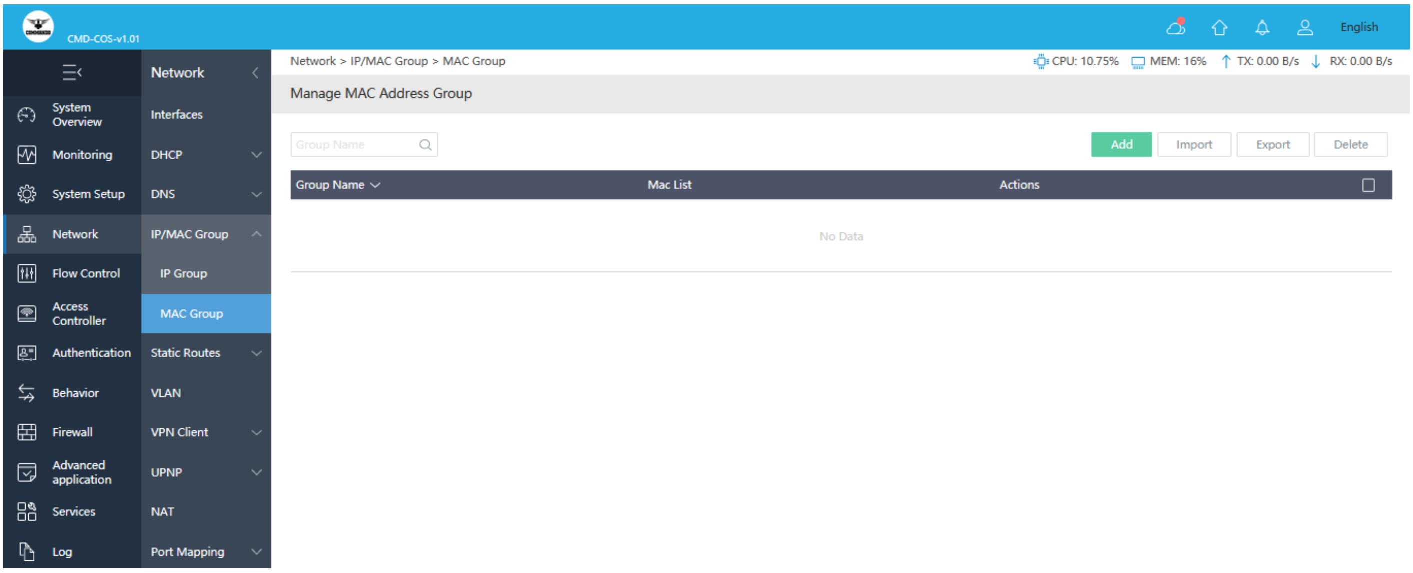
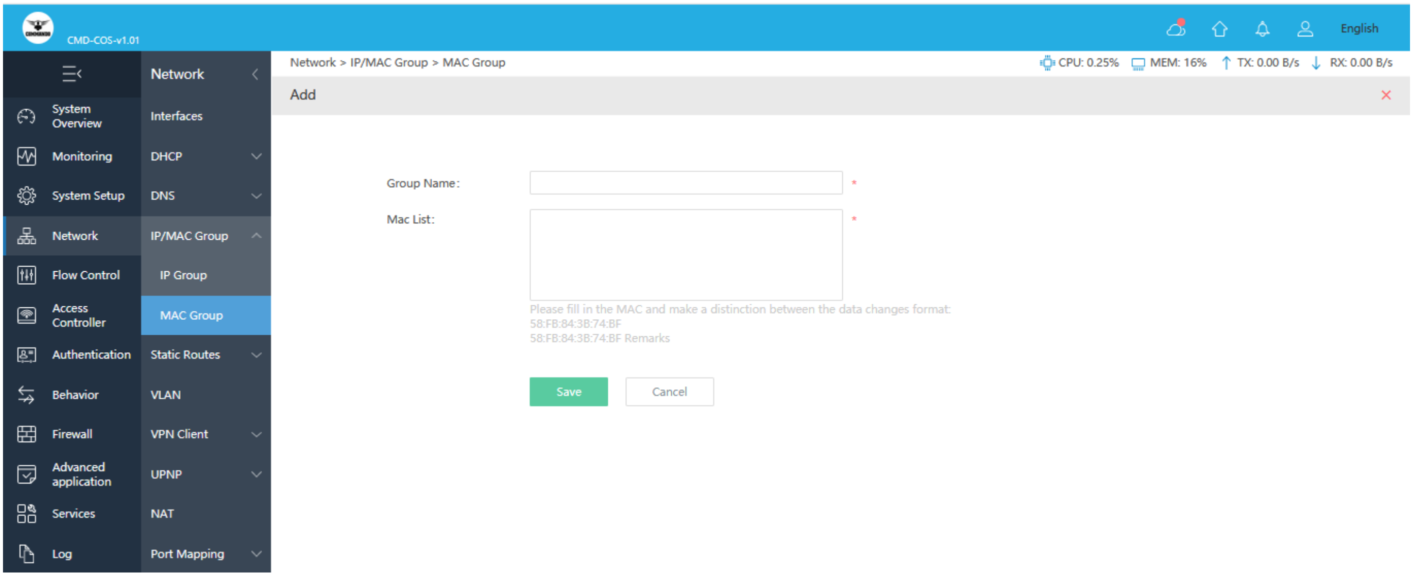
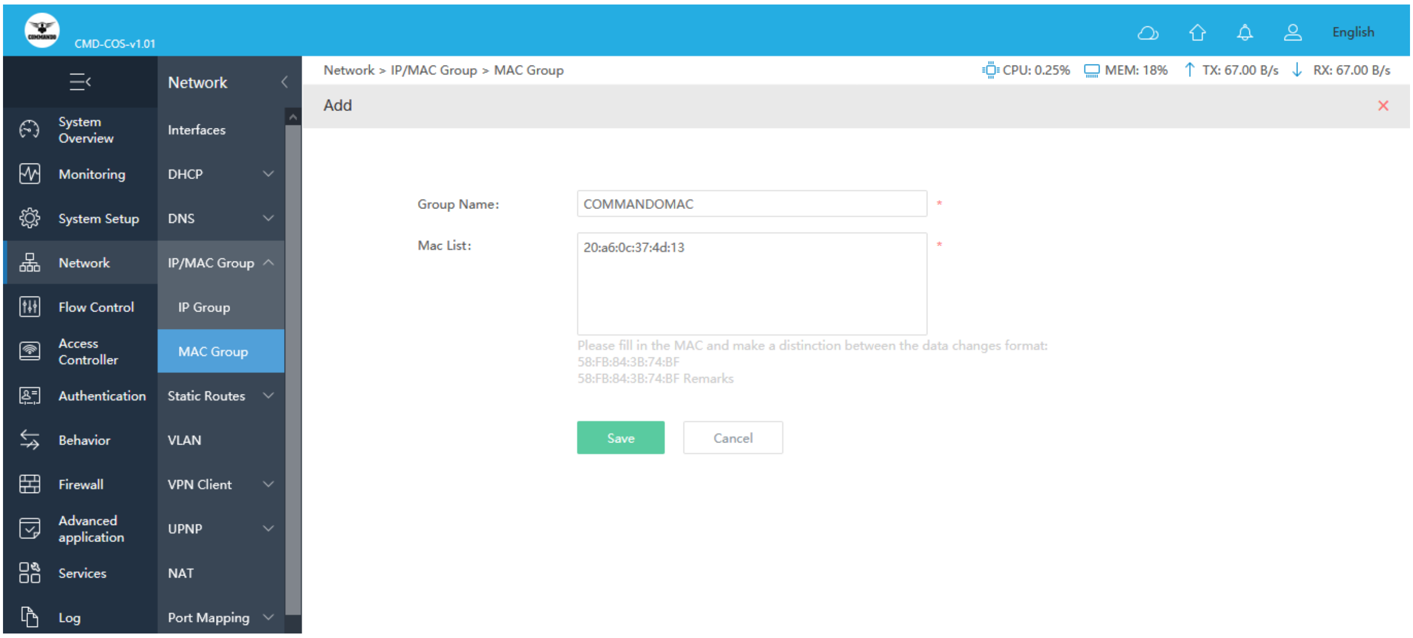


Fig 3.4.5 Default Manage MAC Address Group page



Please fill in the MAC and make a distinction between the data changes format:
58:FB:84:3B:74:BF
58:FB:84:3B:74:BF Remarks

Fig 3.4.6 Add MAC Address Group page

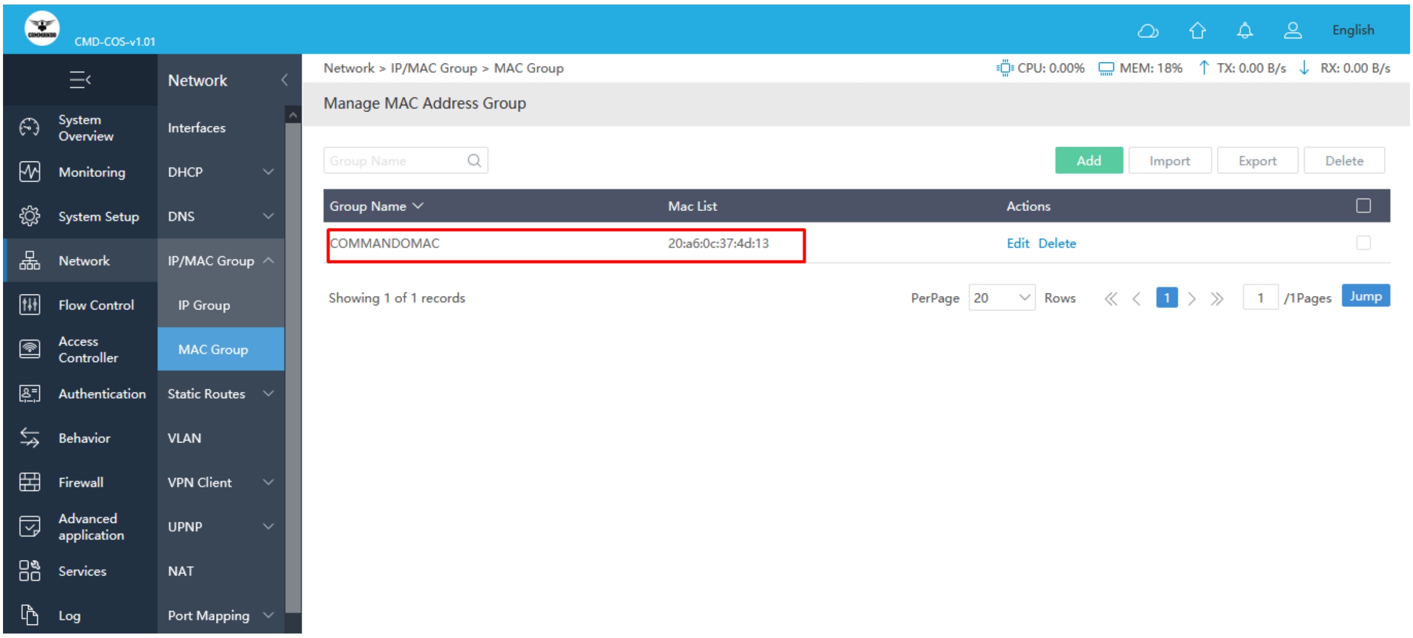


Group Name: COMMANDOMAC *

Mac List: 20:a6:0c:37:4d:13 *

Please fill in the MAC and make a distinction between the data changes format:
58:FB:84:3B:74:BF
58:FB:84:3B:74:BF Remarks

Fig 3.4.6 Adding specific MAC page



Group Name	Mac List	Actions	□
COMMANDOMAC	20:a6:0c:37:4d:13	Edit Delete	□

Showing 1 of 1 records   PerPage 20 Rows   1   1 /1Pages Jump

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 manly Destination, Subnet Mask and Next Hop (Gateway). The destination and subnet mask are both the fixed value 0.0.0.0, which means arbitrary destination IP addresses that are not matched by other route entries.

Routing table is used for a Layer 3 device to forward packets to the correct destination. When the 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.

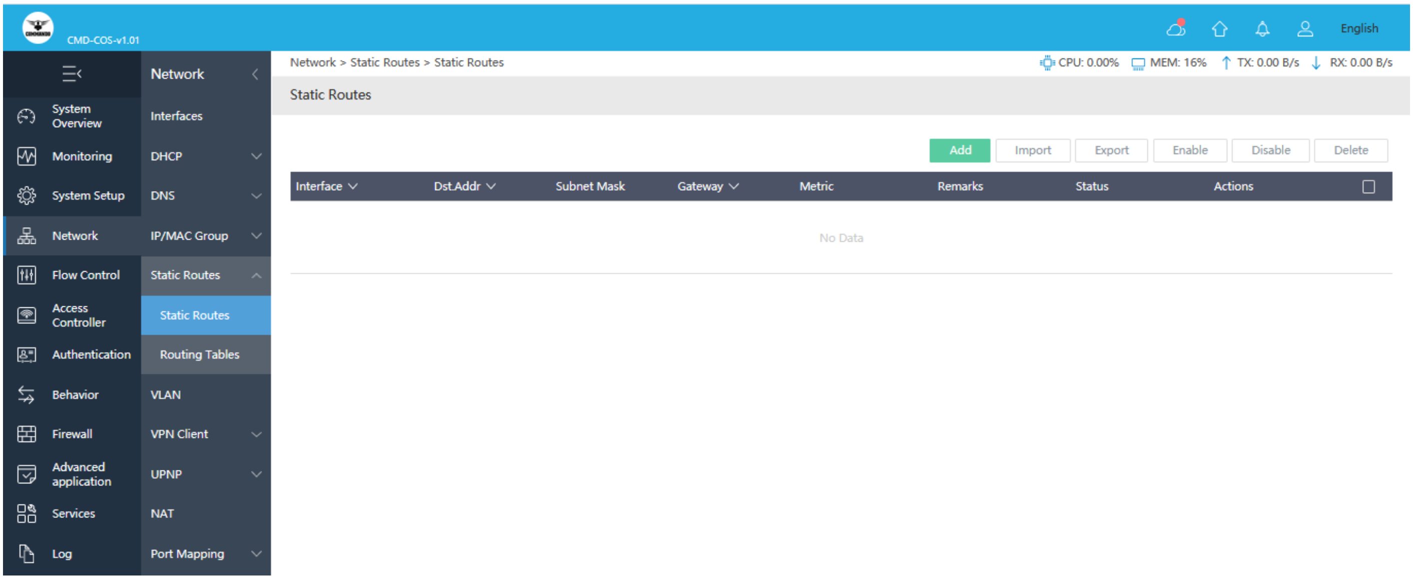
Dynamic routing entries:

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:

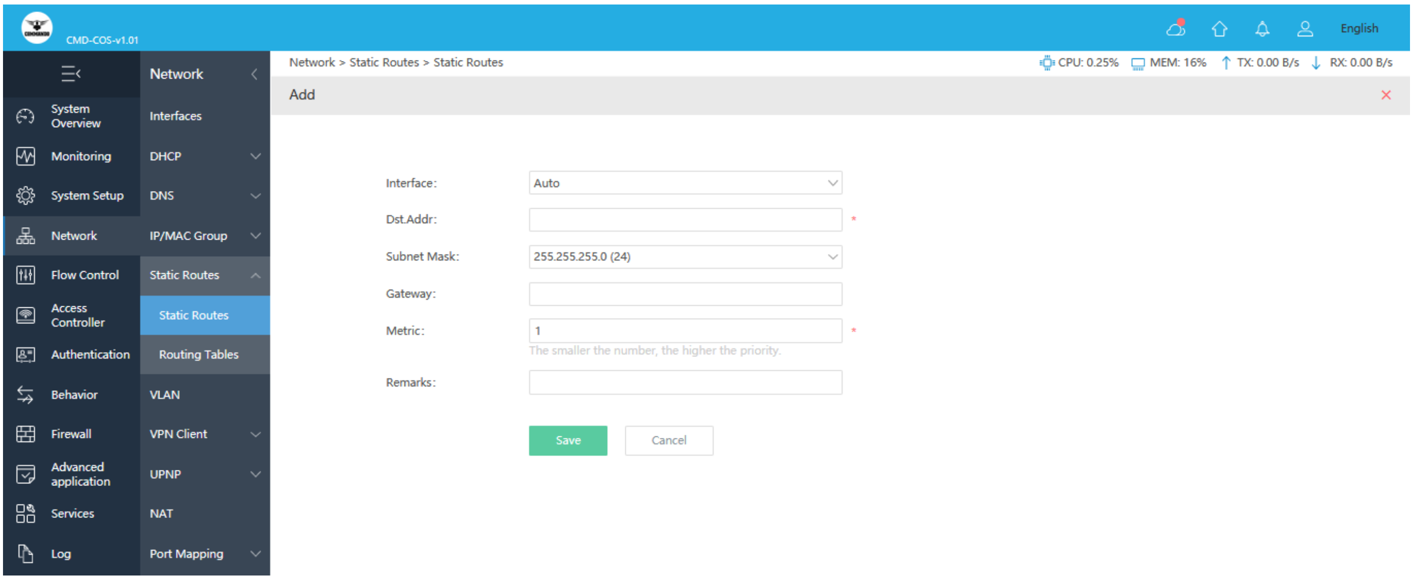
Static routing entries are manually added non-aging routing entries. In a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable 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.



Interface	Dst.Addr	Subnet Mask	Gateway	Metric	Remarks	Status	Actions	□
No Data								

Fig 3.5.1 Default static route page



Interface: Auto

Dst.Addr: *

Subnet Mask: 255.255.255.0 (24)

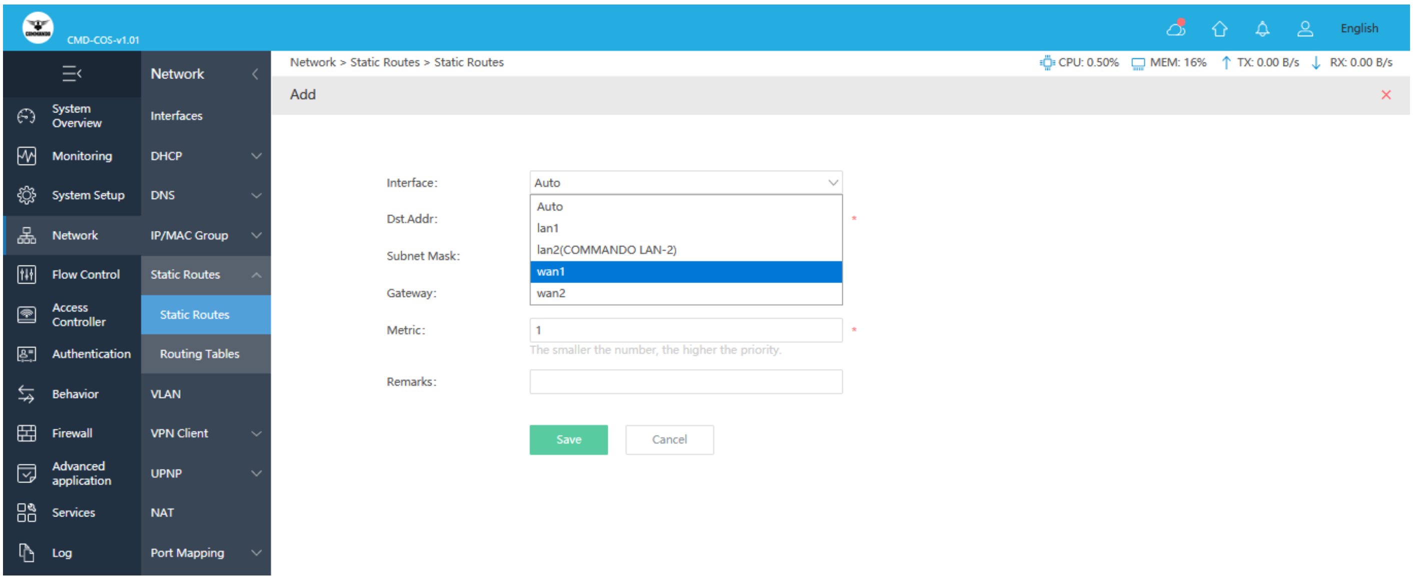
Gateway:

Metric: 1 *

The smaller the number, the higher the priority.

Remarks:

Fig 3.5.2 Default Add static route page



Interface: Auto

Dst.Addr: *

Subnet Mask:

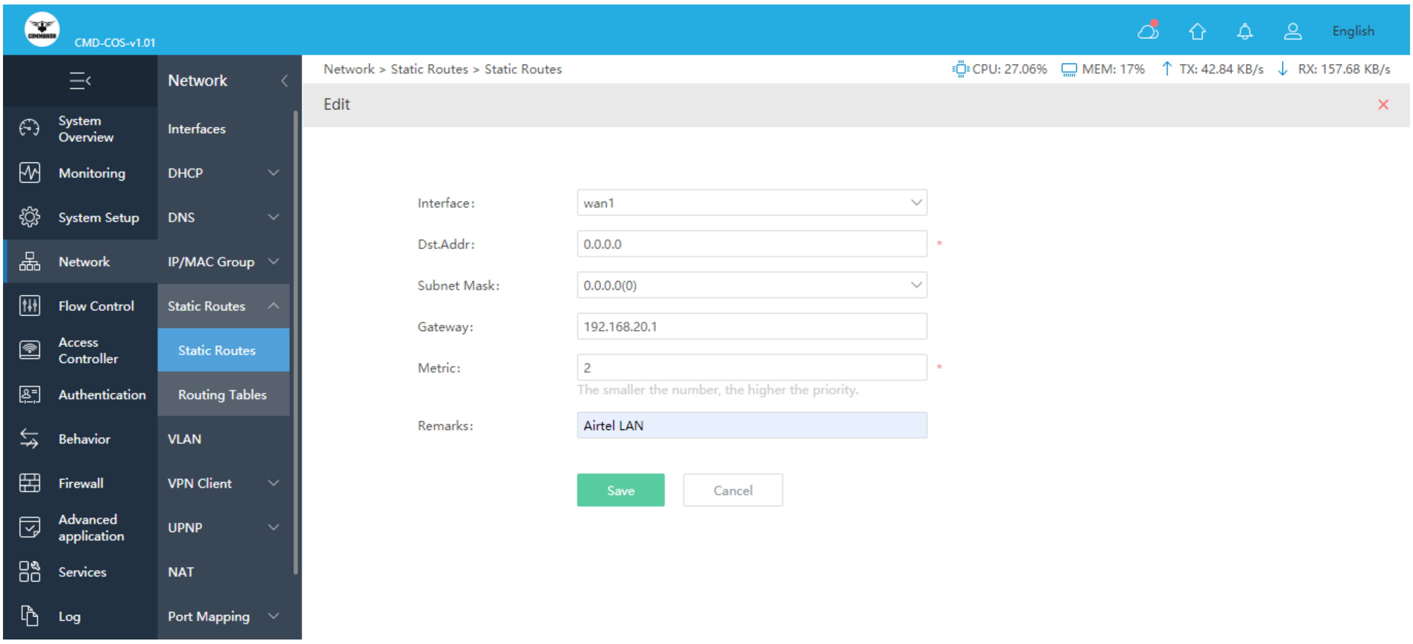
Gateway:

Metric: 1 *

The smaller the number, the higher the priority.

Remarks:

Fig 3.5.3 Selecting interface in static route page



Interface: wan1

Dst.Addr: 0.0.0.0 *

Subnet Mask: 0.0.0.0(0)

Gateway: 192.168.20.1

Metric: 2 *

The smaller the number, the higher the priority.

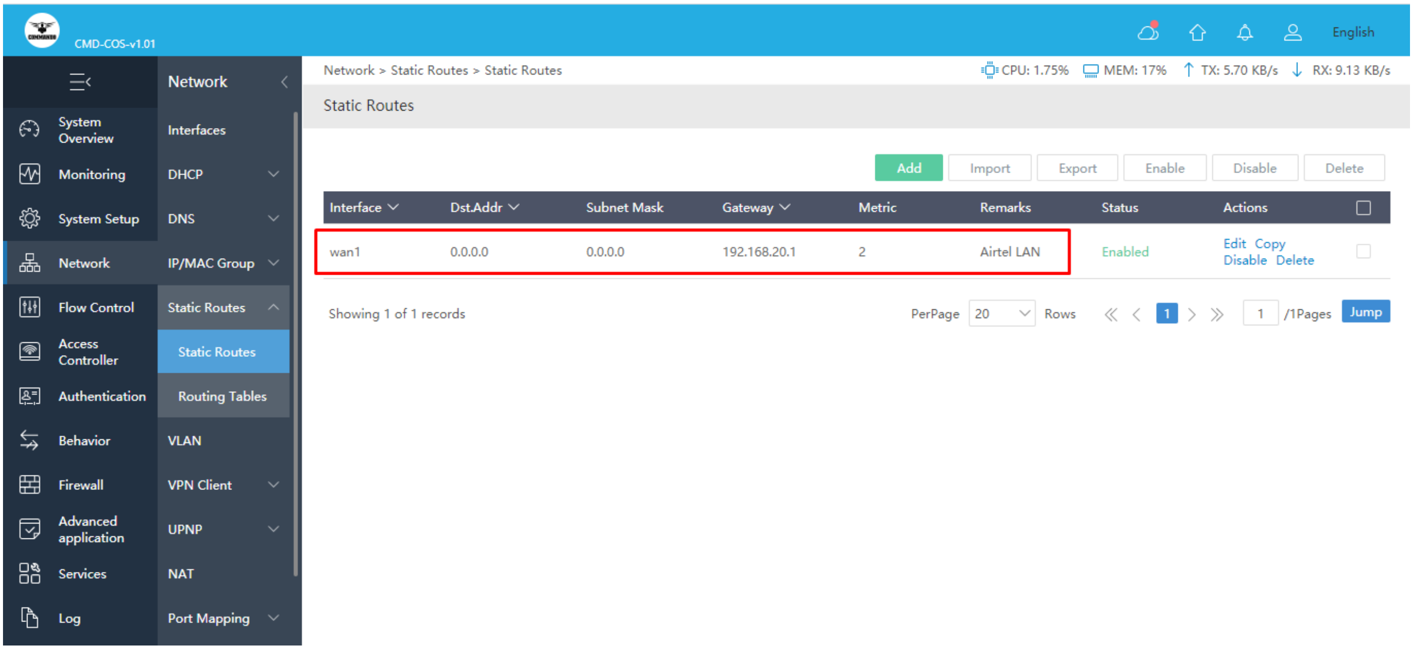
Remarks: Airtel LAN

Save Cancel

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

Note:

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

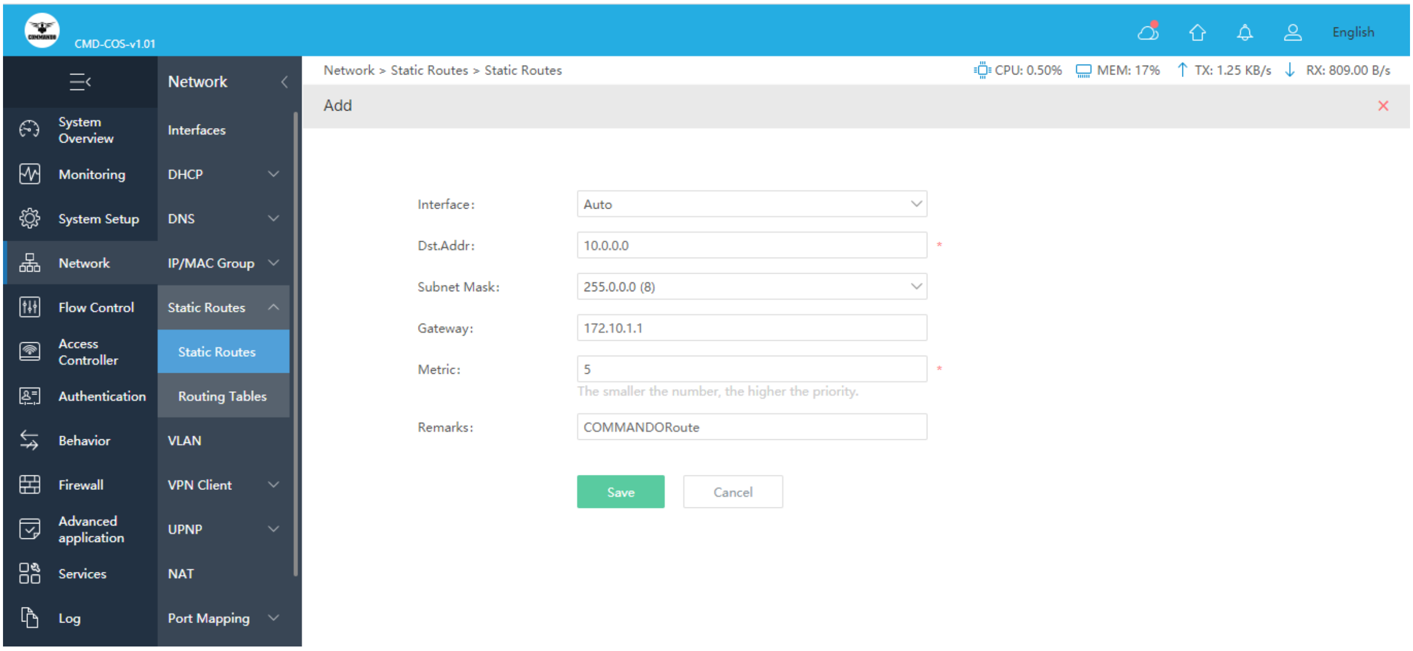


Interface	Dst.Addr	Subnet Mask	Gateway	Metric	Remarks	Status	Actions	□
wan1	0.0.0.0	0.0.0.0	192.168.20.1	2	Airtel LAN	Enabled	Edit Copy Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows 1 1 /1Pages Jump

Fig 3.5.5 Default route page



Add

Interface: Auto

Dst.Addr: 10.0.0.0 *

Subnet Mask: 255.0.0.0 (8)

Gateway: 172.10.1.1

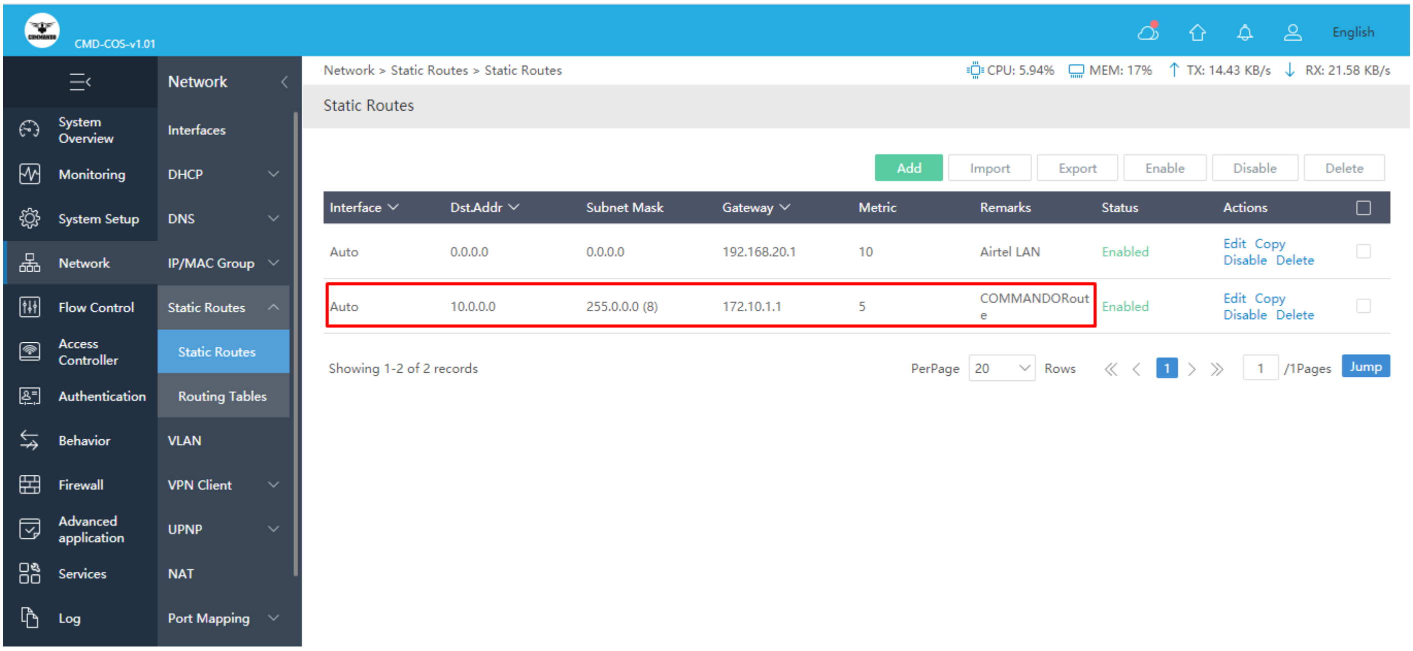
Metric: 5 *

The smaller the number, the higher the priority.

Remarks: COMMANDORoute

Save Cancel

Fig 3.5.6 Adding a Specific Static route page



Static Routes

Interface	Dst.Addr	Subnet Mask	Gateway	Metric	Remarks	Status	Actions	□
Auto	0.0.0.0	0.0.0.0	192.168.20.1	10	Airtel LAN	Enabled	Edit Copy Disable Delete	□
Auto	10.0.0.0	255.0.0.0 (8)	172.10.1.1	5	COMMANDORoute	Enabled	Edit Copy Disable Delete	□

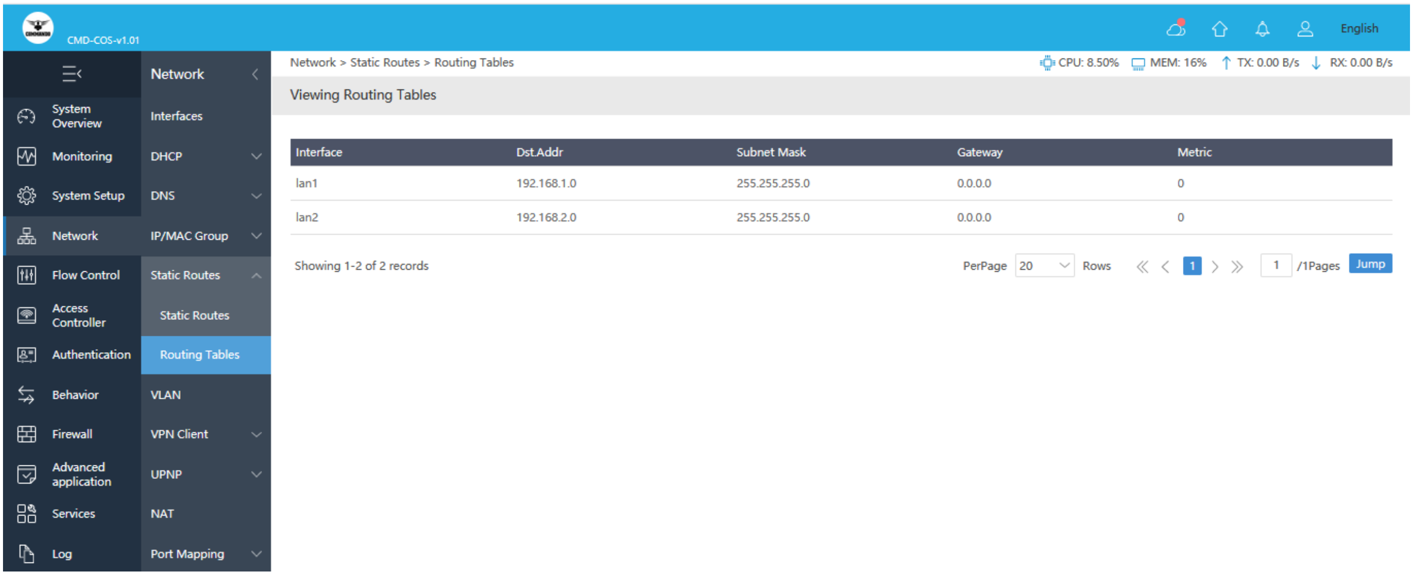
Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

Fig 3.5.7 Specific Static route page

Routing Tables:

The routing table contains network/next hop associations. These associations tell a 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



Viewing Routing Tables

Interface	Dst.Addr	Subnet Mask	Gateway	Metric
lan1	192.168.1.0	255.255.255.0	0.0.0.0	0
lan2	192.168.2.0	255.255.255.0	0.0.0.0	0

Showing 1-2 of 2 records

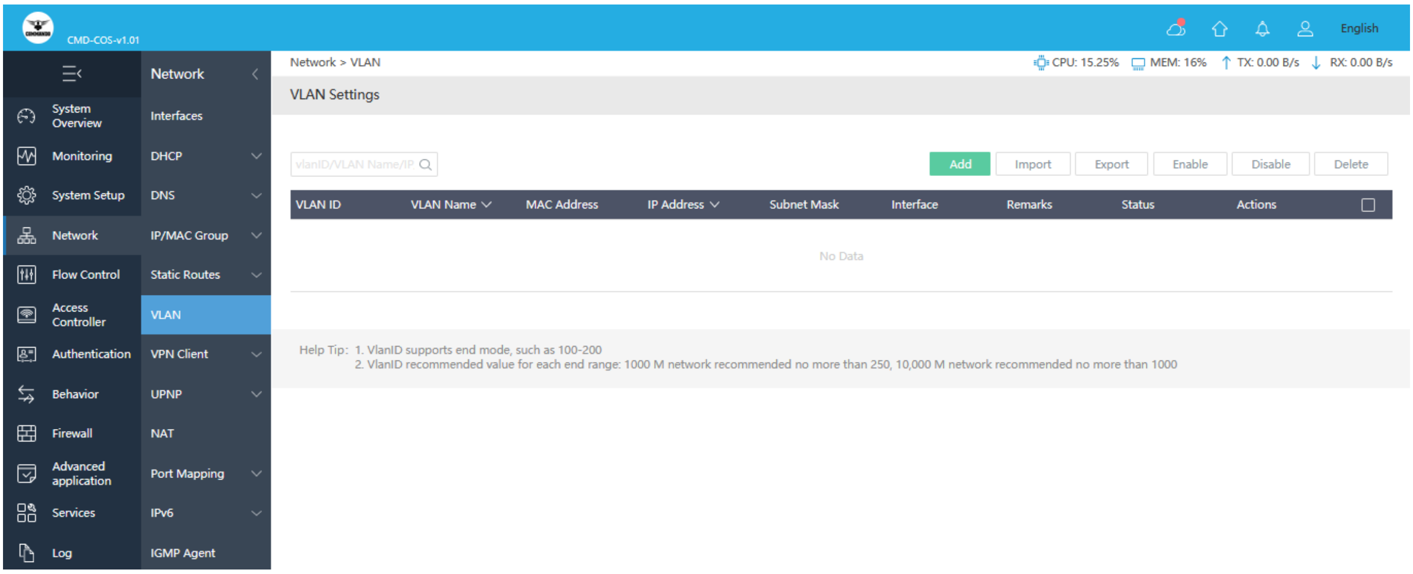
Fig 3.5.8 Routing Tables page

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



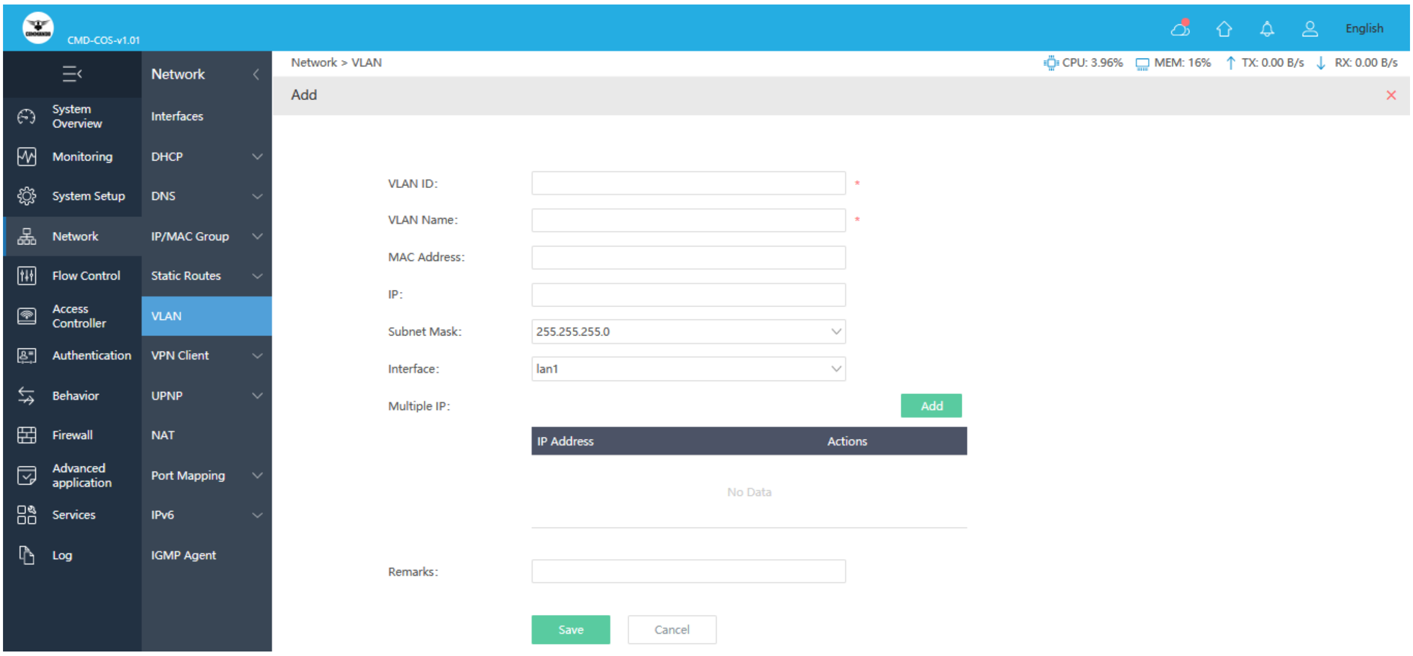
VLAN Settings

VLAN ID	VLAN Name	MAC Address	IP Address	Subnet Mask	Interface	Remarks	Status	Actions	□

No Data

Help Tip: 1. VlanID supports end mode, such as 100-200
2. VlanID recommended value for each end range: 1000 M network recommended no more than 250, 10,000 M network recommended no more than 1000

Fig 3.6.1 Default VLAN Setting page



Add

VLAN ID: *

VLAN Name: *

MAC Address:

IP:

Subnet Mask: 255.255.255.0

Interface: lan1

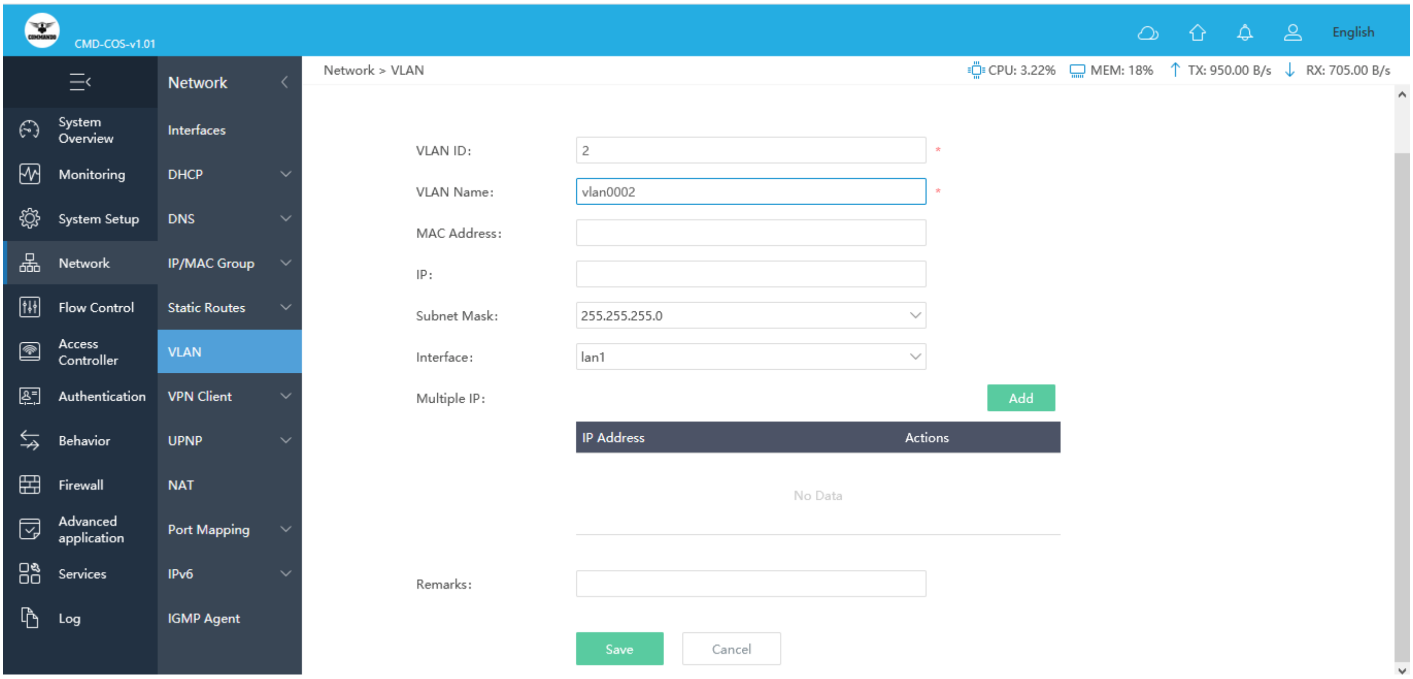
Multiple IP:

IP Address	Actions

No Data

Remarks:

Fig 3.6.2 Add VLAN Setting page



VLAN ID: 2 *

VLAN Name: vlan0002 *

MAC Address:

IP:

Subnet Mask: 255.255.255.0

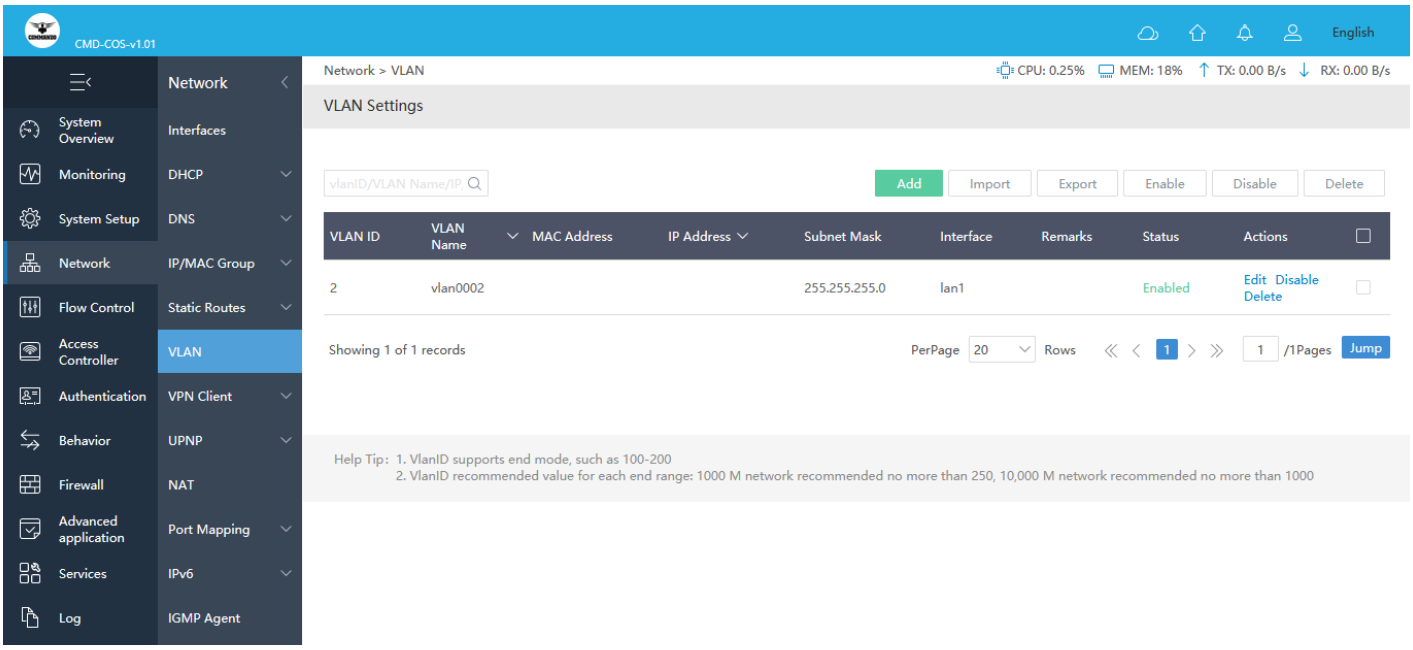
Interface: lan1

Multiple IP:

IP Address	Actions
No Data	

Remarks:

Fig 3.6.3 Add VLAN2 Setting on lan1 interface page



VLAN Settings

VLAN ID	VLAN Name	MAC Address	IP Address	Subnet Mask	Interface	Remarks	Status	Actions	□
2	vlan0002			255.255.255.0	lan1		Enabled	Edit Disable Delete	□

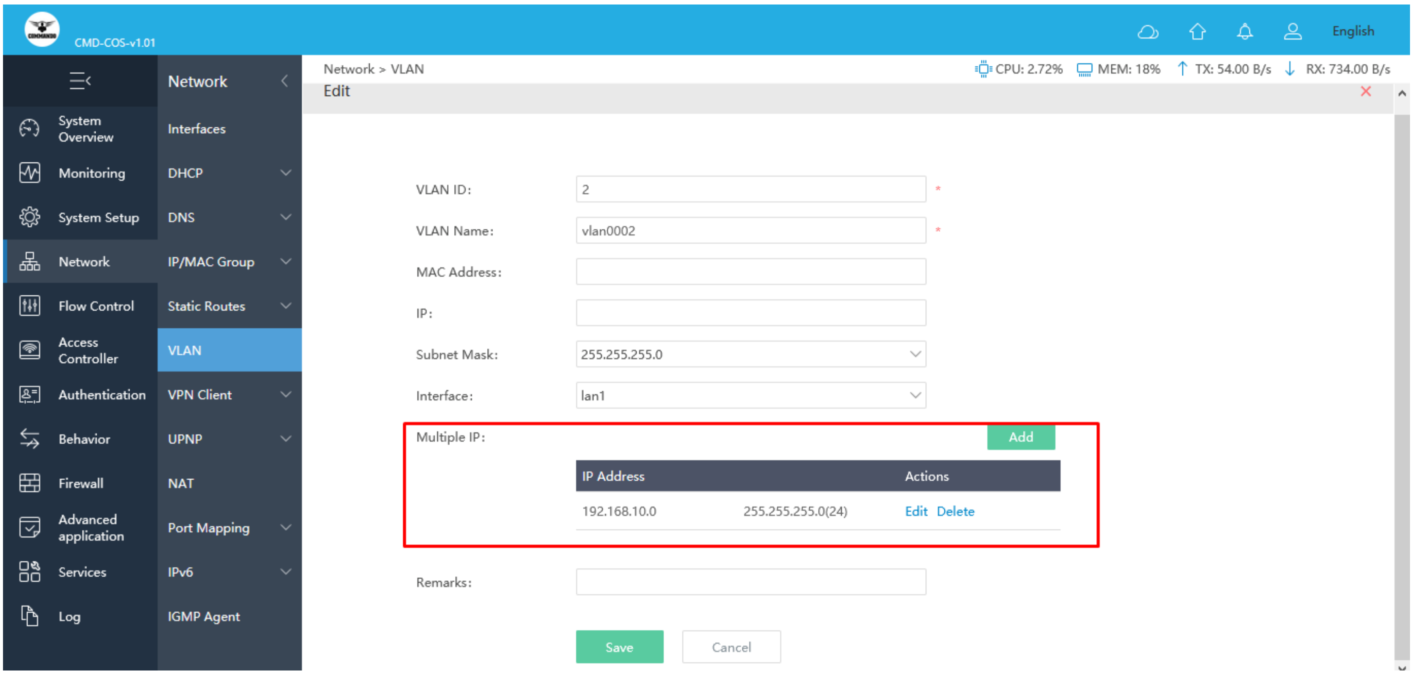
Showing 1 of 1 records

Help Tip: 1. VlanID supports end mode, such as 100-200
2. VlanID recommended value for each end range: 1000 M network recommended no more than 250, 10,000 M network recommended no more than 1000

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.



VLAN ID: 2 *

VLAN Name: vlan0002 *

MAC Address:

IP:

Subnet Mask: 255.255.255.0

Interface: lan1

Multiple IP:

IP Address		Actions
192.168.10.0	255.255.255.0(24)	Edit Delete

Remarks:

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.

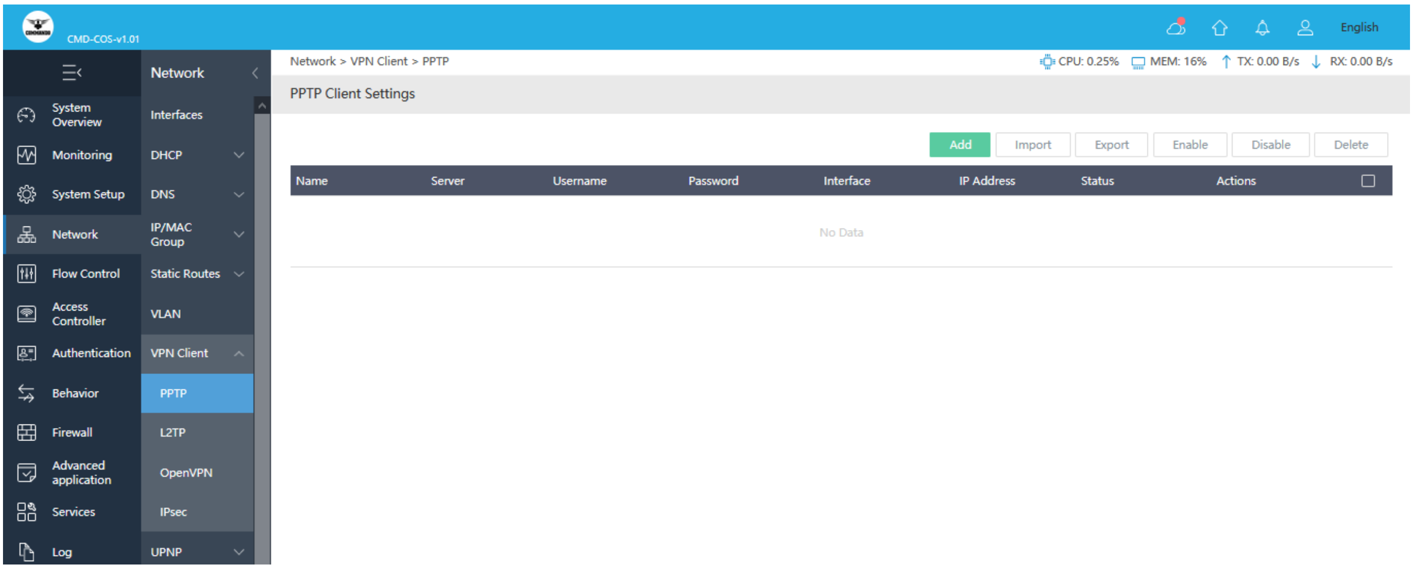
Note:

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

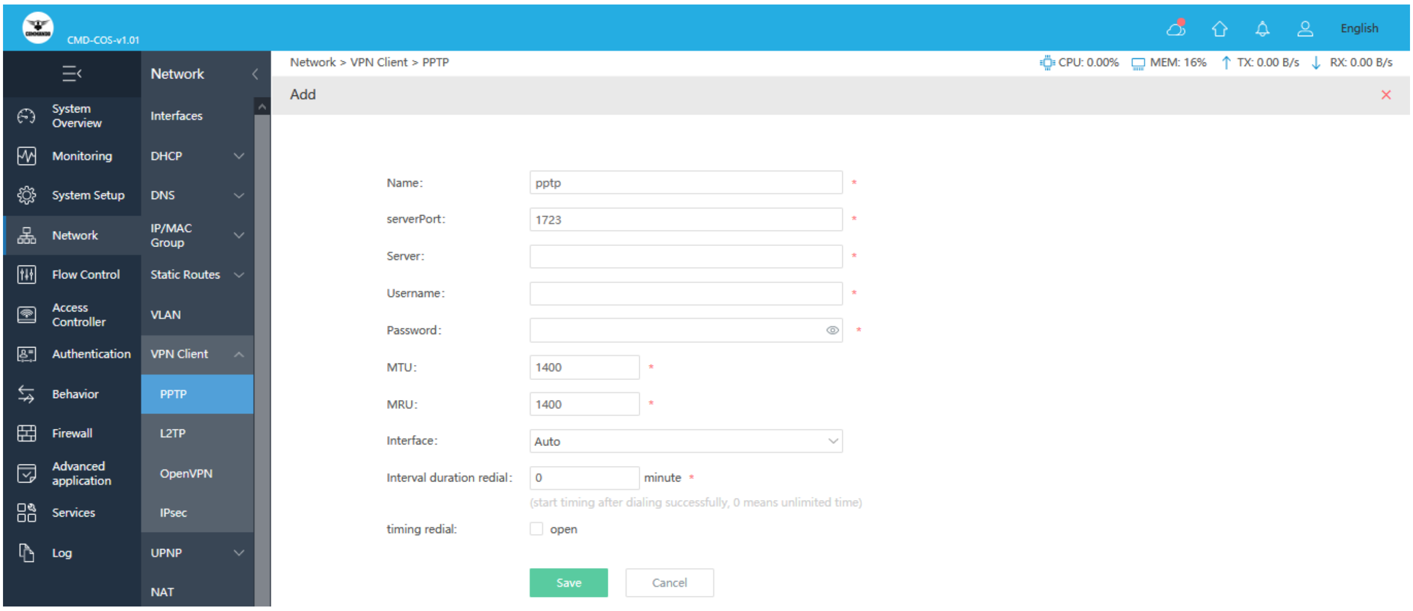


PPTP Client Settings

Name	Server	Username	Password	Interface	IP Address	Status	Actions	□

No Data

Fig 3.7.1 Default PPTP Setting page



Add

Name: pptp *

serverPort: 1723 *

Server: *

Username: *

Password: *

MTU: 1400 *

MRU: 1400 *

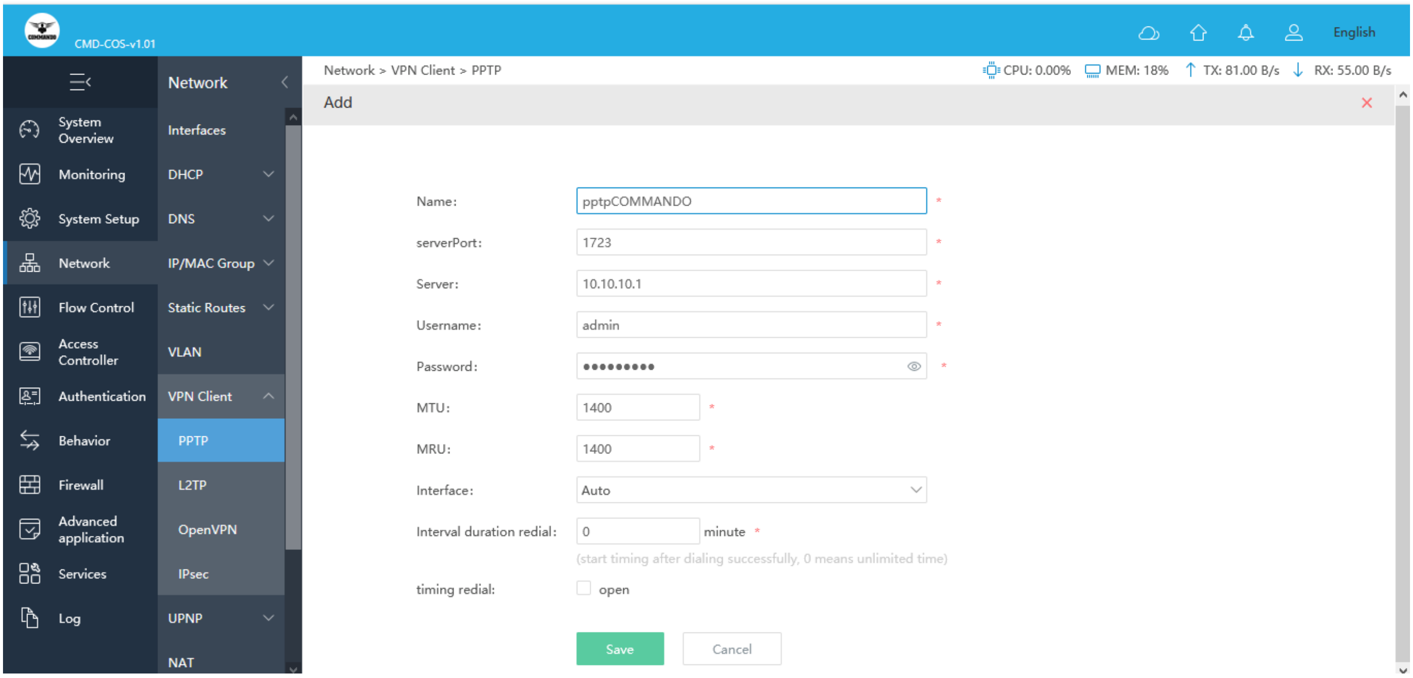
Interface: Auto

Interval duration redial: 0 minute *

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

timing redial: □ open

Fig 3.7.2 Add PPTP Setting page



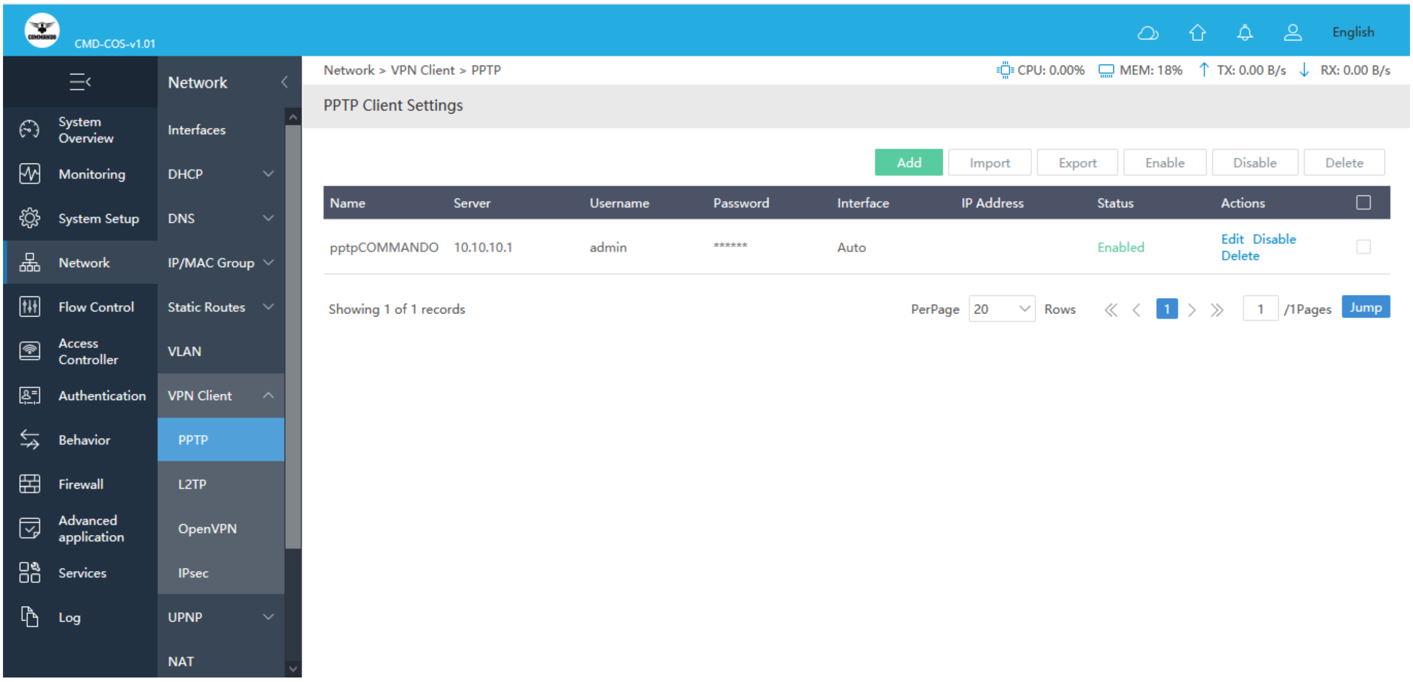
Add

Name:	pptpCOMMANDO *
serverPort:	1723 *
Server:	10.10.10.1 *
Username:	admin *
Password:	••••••••• *
MTU:	1400 *
MRU:	1400 *
Interface:	Auto
Interval duration redial:	0 minute * (start timing after dialing successfully, 0 means unlimited time)
timing redial:	□ open

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



PPTP Client Settings

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

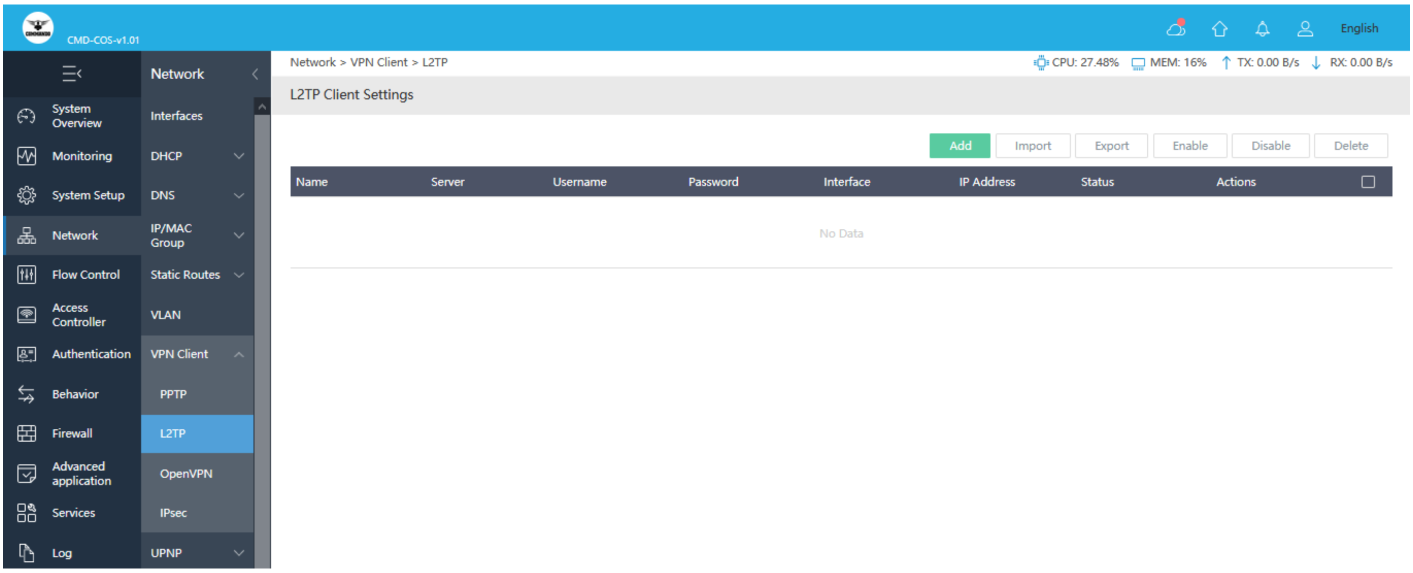
Showing 1 of 1 records

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

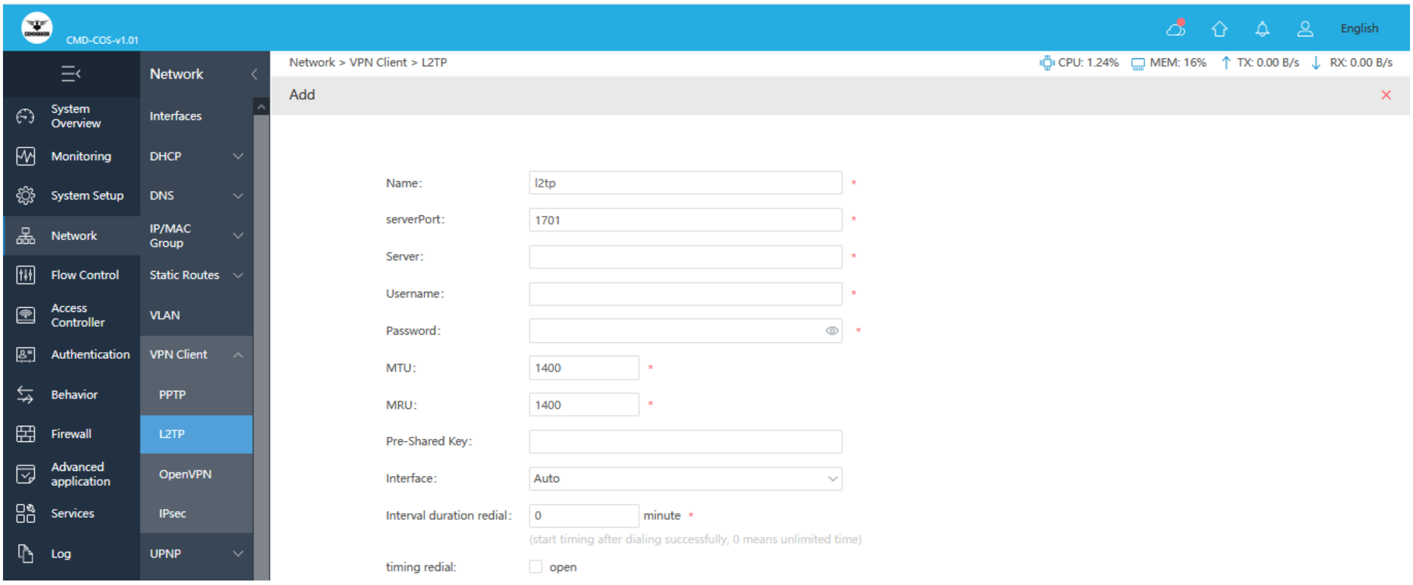


L2TP Client Settings

Name	Server	Username	Password	Interface	IP Address	Status	Actions	□

No Data

Fig 3.7.5 Default L2TP Client setting page



Add

Name: l2tp *

serverPort: 1701 *

Server: *

Username: *

Password: *

MTU: 1400 *

MRU: 1400 *

Pre-Shared Key:

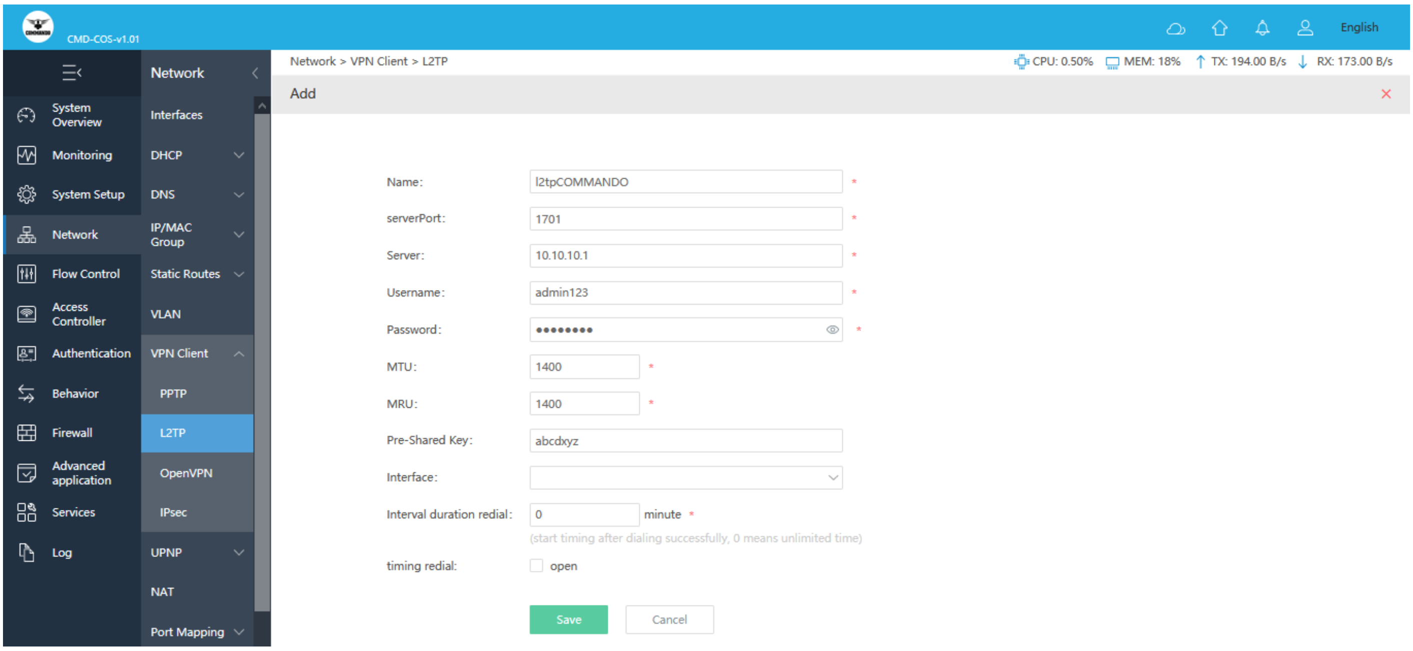
Interface: Auto

Interval duration redial: 0 minute *

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

timing redial: □ open

Fig 3.7.6 Add L2TP Client setting page



Name: l2tpCOMMANDO *

serverPort: 1701 *

Server: 10.10.10.1 *

Username: admin123 *

Password: •••••••• *

MTU: 1400 *

MRU: 1400 *

Pre-Shared Key: abcdxyz

Interface:

Interval duration redial: 0 minute *

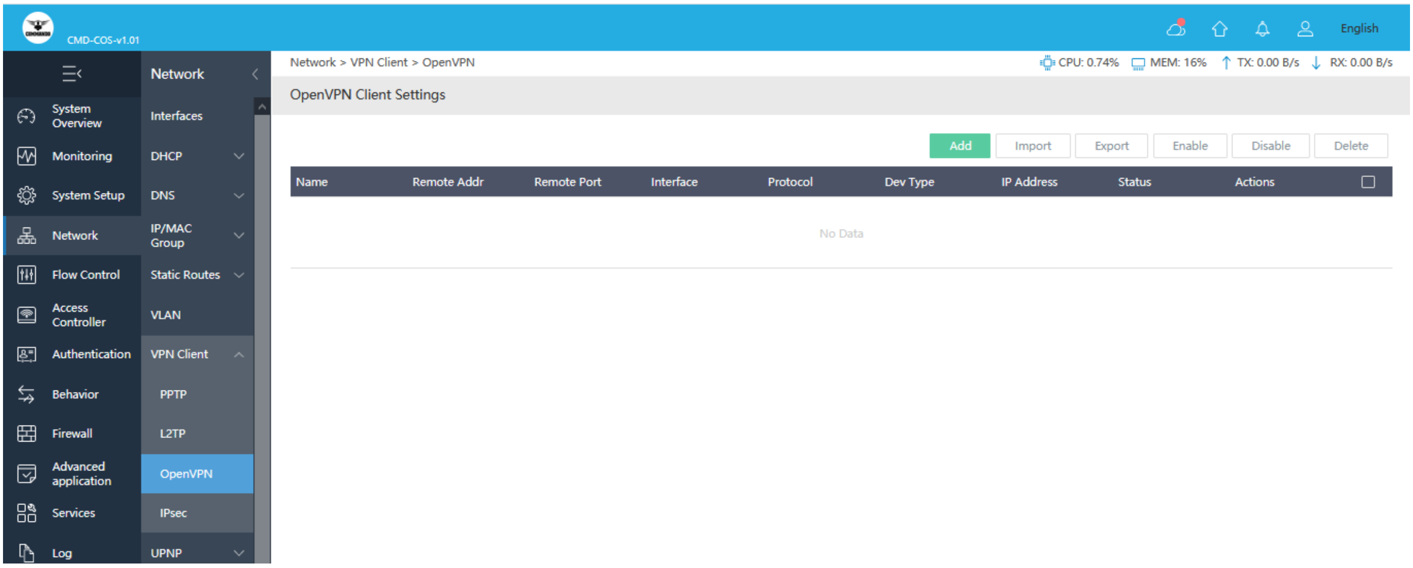
(start timing after dialing successfully, 0 means unlimited time)

timing redial: □ open

Fig 3.7.6 L2TP Client setting with details page

Note:

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



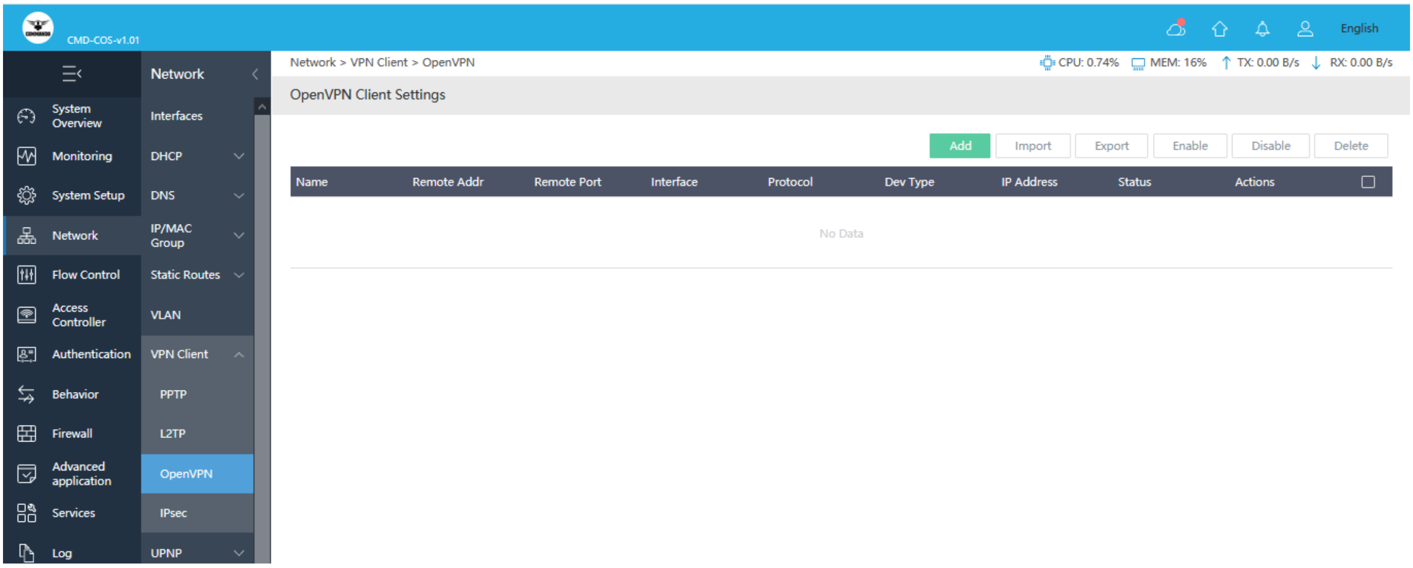
Name	Remote Addr	Remote Port	Interface	Protocol	Dev Type	IP Address	Status	Actions	□
No Data									

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



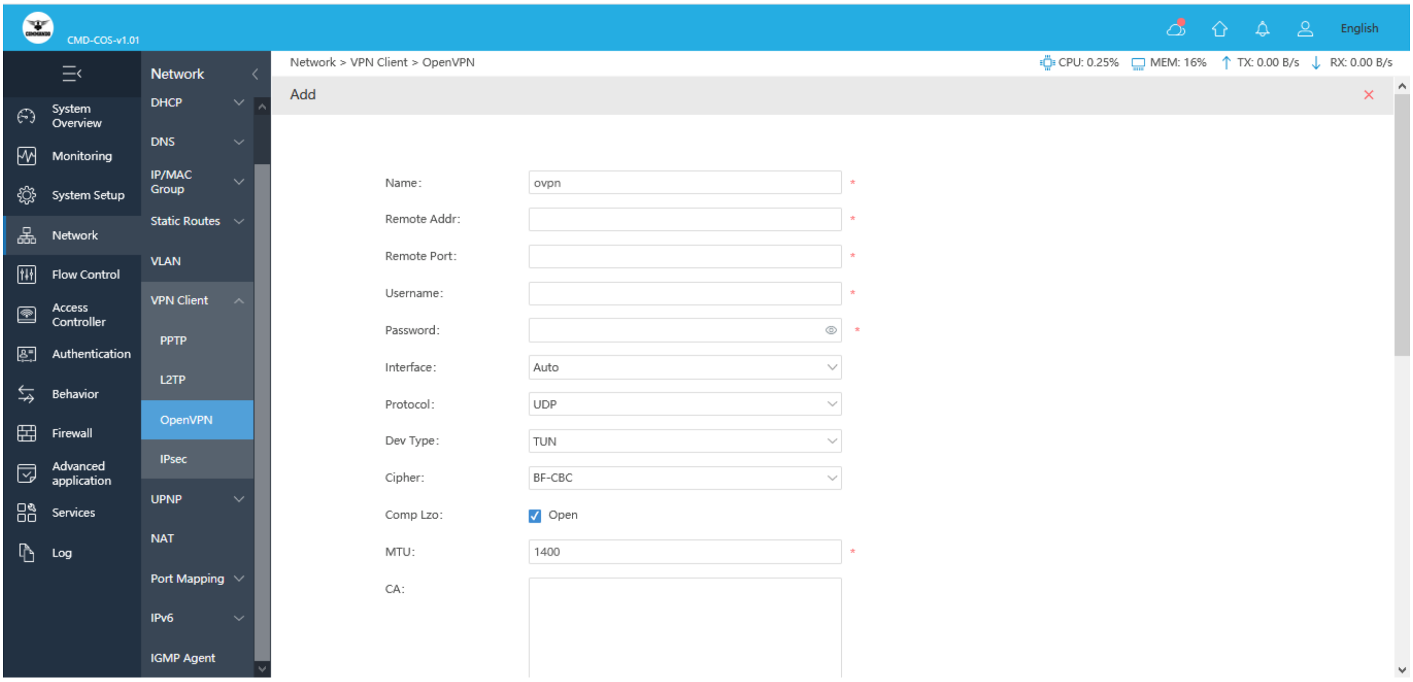
Network > VPN Client > OpenVPN

OpenVPN Client Settings

Name	Remote Addr	Remote Port	Interface	Protocol	Dev Type	IP Address	Status	Actions	□

No Data

Fig 3.7.8 Default OpenVPN Client setting page



Network > VPN Client > OpenVPN

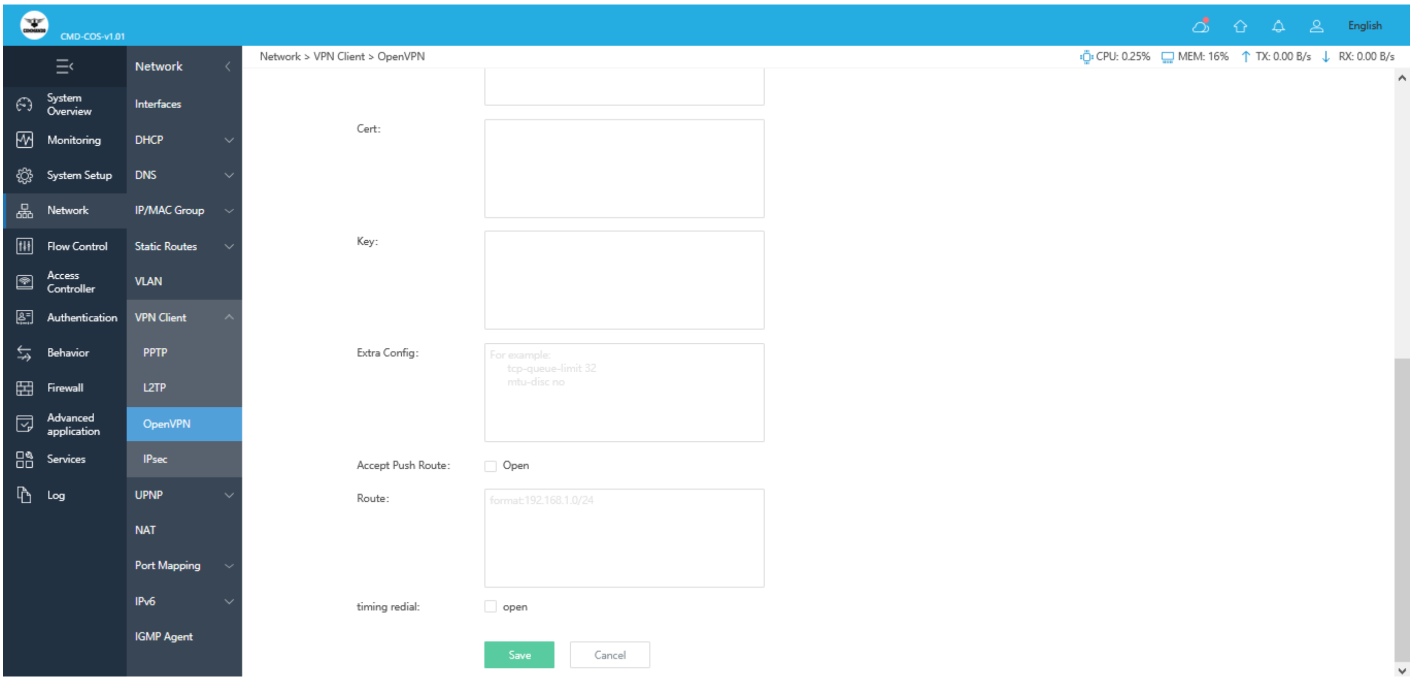
Add

Name:	ovpn *
Remote Addr:	*
Remote Port:	*
Username:	*
Password:	*
Interface:	Auto
Protocol:	UDP
Dev Type:	TUN
Cipher:	BF-CBC
Comp Lzo:	☑ Open
MTU:	1400 *
CA:	

Fig 3.7.9 Add OpenVPN Client setting page

Note:

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



Cert:

Key:

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

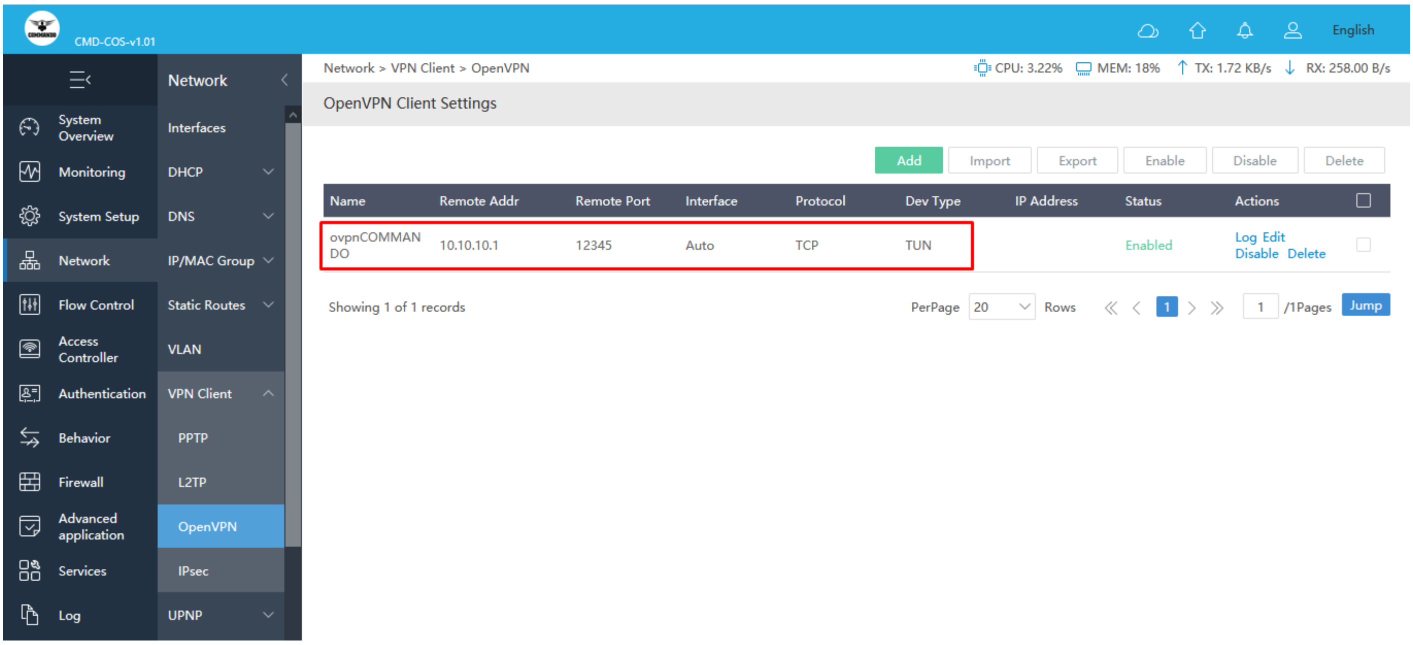
Accept Push Route: □ Open

Route: format:192.168.1.0/24

timing redial: □ open

Save Cancel

Fig 3.7.10 OpenVPN Client details setting page



OpenVPN Client Settings

Add Import Export Enable Disable Delete

Name	Remote Addr	Remote Port	Interface	Protocol	Dev Type	IP Address	Status	Actions	□
ovpnCOMMANDO	10.10.10.1	12345	Auto	TCP	TUN		Enabled	Log Edit Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

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?

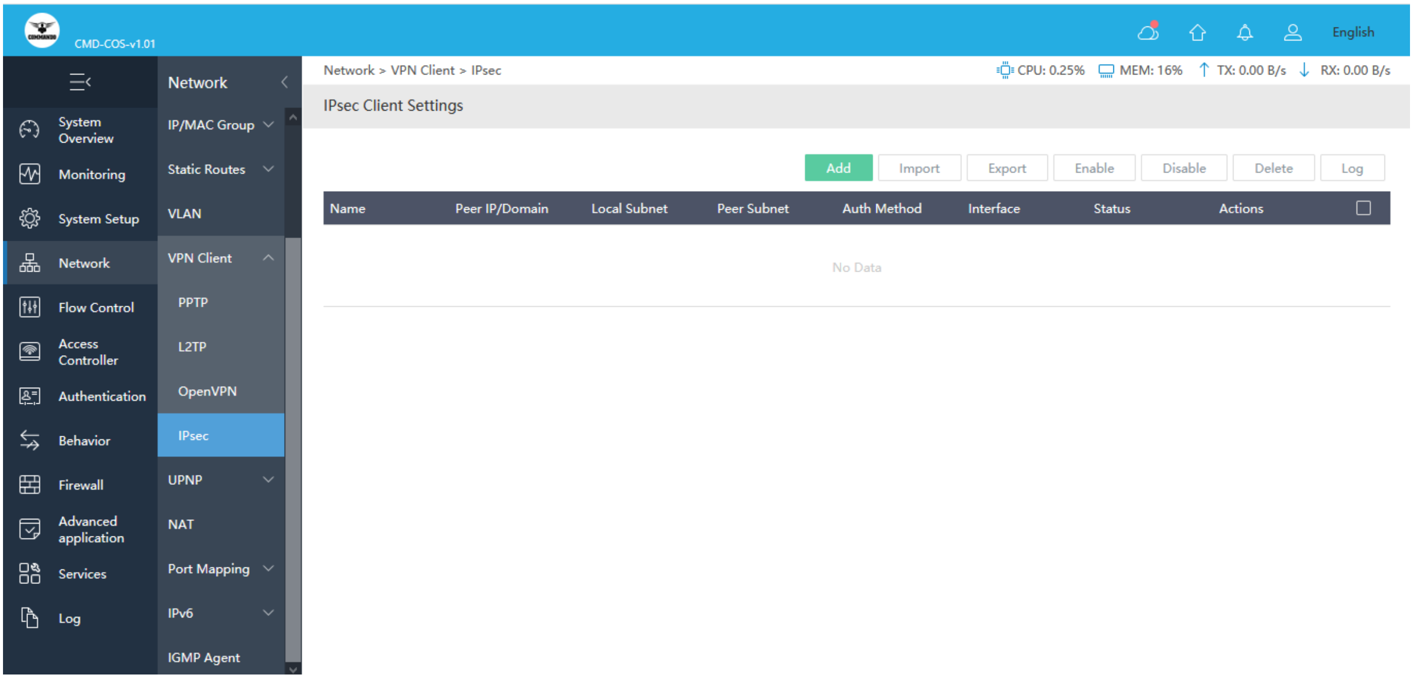
Users can access an IPsec VPN by logging into a VPN application, or "client." This typically requires the user to have installed the application on their device. VPN logins are usually password-based. While data sent over a VPN is encrypted, if user passwords are compromised, attackers can log into the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



Network > VPN Client > IPsec

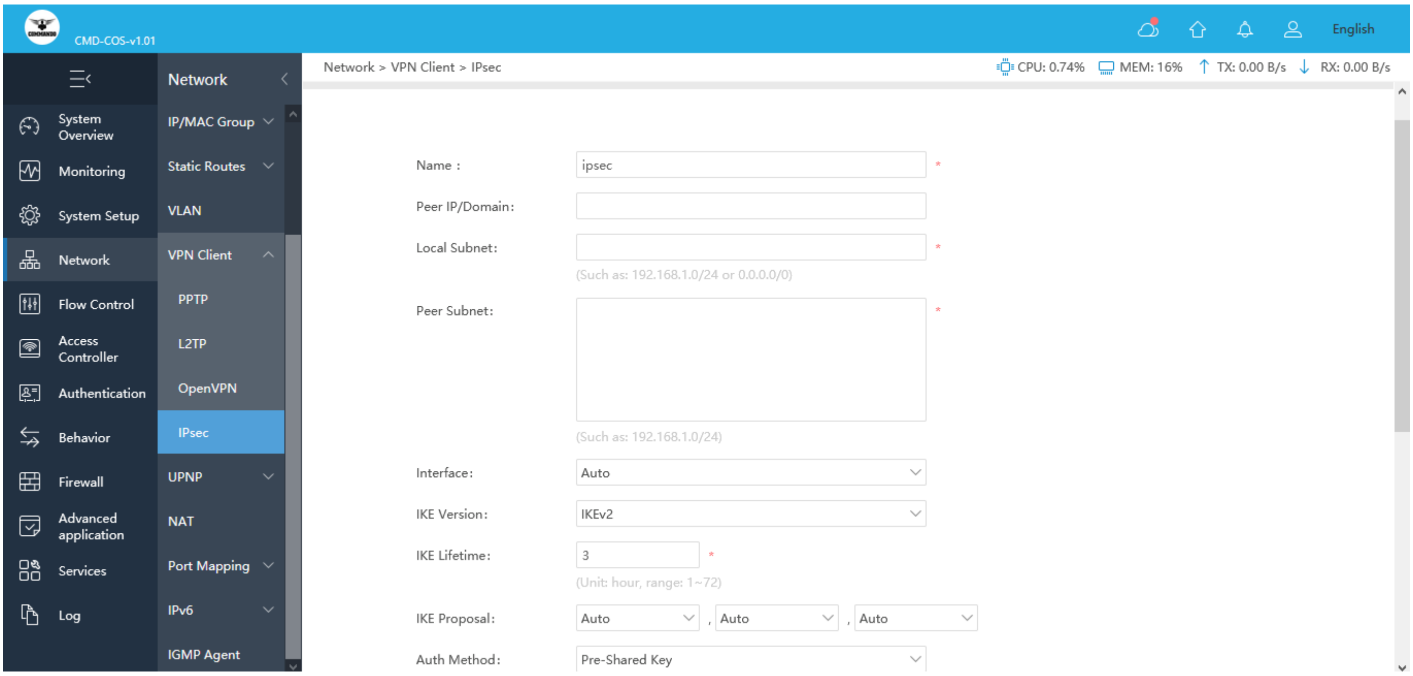
CPU: 0.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

IPsec Client Settings

Name	Peer IP/Domain	Local Subnet	Peer Subnet	Auth Method	Interface	Status	Actions	□

No Data

Fig 3.7.12 Default IPsec Client setting page



Network > VPN Client > IPsec

CPU: 0.74% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Name : ipsec *

Peer IP/Domain:

Local Subnet: *

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

Peer Subnet: *

(Such as: 192.168.1.0/24)

Interface: Auto

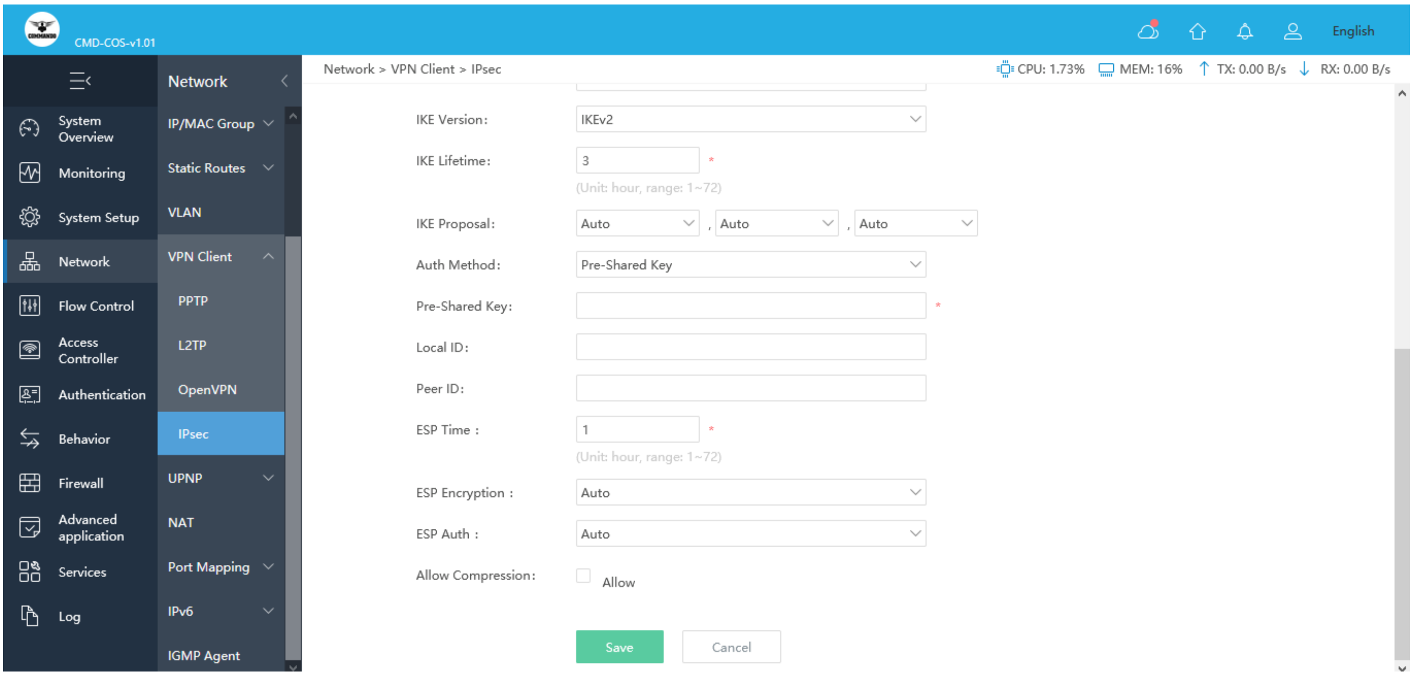
IKE Version: IKEv2

IKE Lifetime: 3 *

(Unit: hour, range: 1~72)

IKE Proposal: Auto , Auto , Auto

Auth Method: Pre-Shared Key



IKE Version: IKEv2

IKE Lifetime: 3 *
(Unit: hour, range: 1~72)

IKE Proposal: Auto , Auto , Auto

Auth Method: Pre-Shared Key

Pre-Shared Key: *

Local ID:

Peer ID:

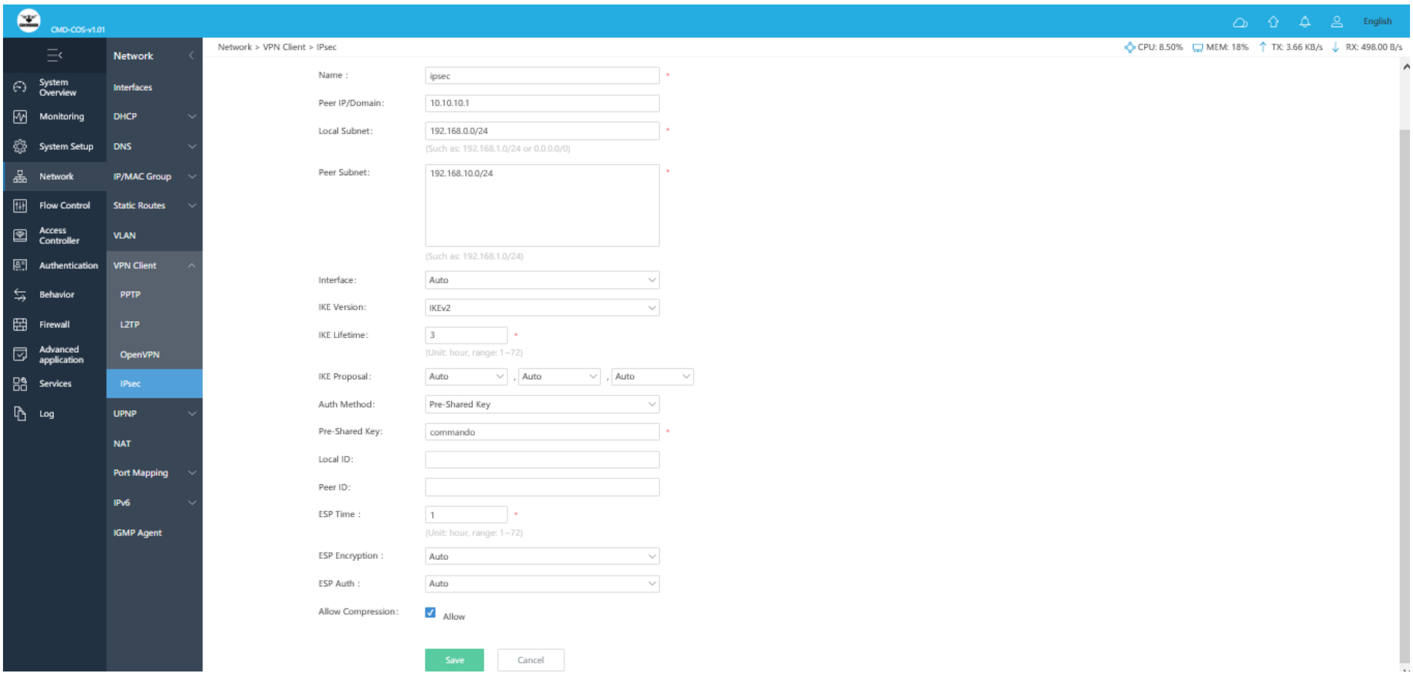
ESP Time : 1 *
(Unit: hour, range: 1~72)

ESP Encryption : Auto

ESP Auth : Auto

Allow Compression: □ Allow

Fig 3.7.13 Add IPsec Client setting page



Name : ipsec *

Peer IP/Domain: 10.10.10.1

Local Subnet: 192.168.0.0/24 *
(Such as: 192.168.1.0/24 or 0.0.0.0/0)

Peer Subnet: 192.168.10.0/24 *
(Such as: 192.168.1.0/24)

Interface: Auto

IKE Version: IKEv2

IKE Lifetime: 3 *
(Unit: hour, range: 1~72)

IKE Proposal: Auto , Auto , Auto

Auth Method: Pre-Shared Key

Pre-Shared Key: commando *

Local ID:

Peer ID:

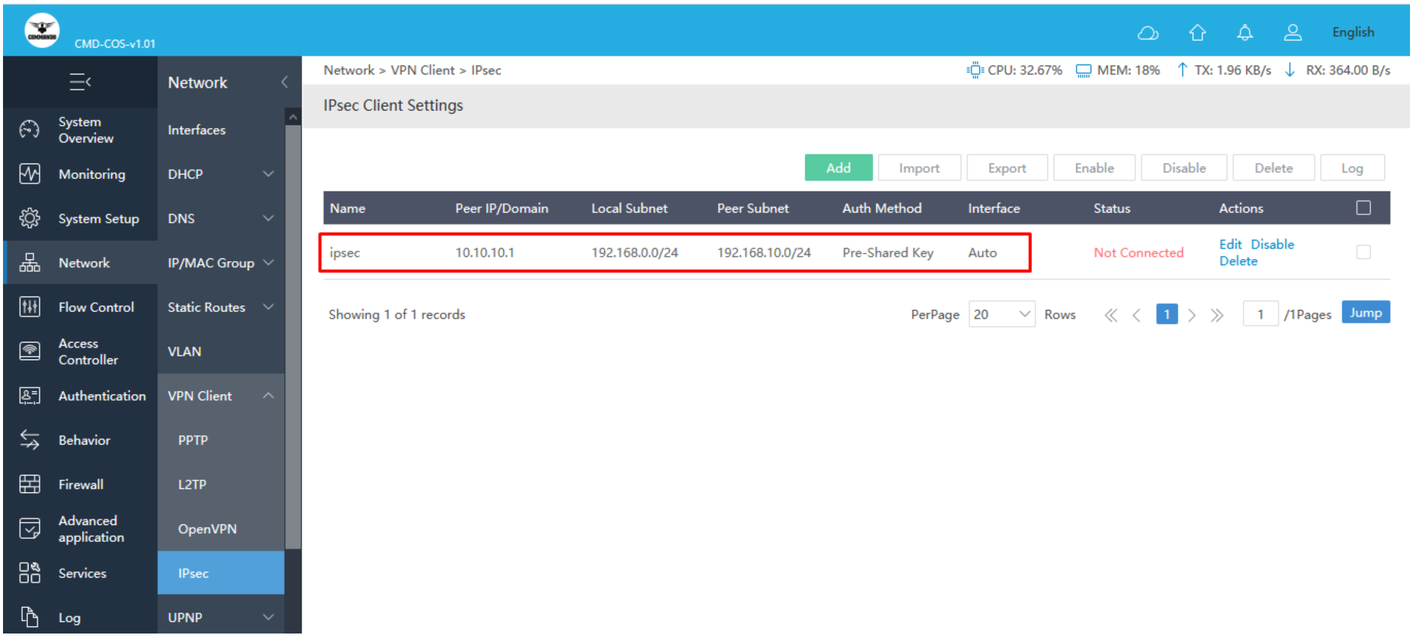
ESP Time : 1 *
(Unit: hour, range: 1~72)

ESP Encryption : Auto

ESP Auth : Auto

Allow Compression: ☑ Allow

Fig 3.7.14 IPsec Client details setting page



Network > VPN Client > IPsec CPU: 32.67% MEM: 18% TX: 1.96 KB/s RX: 364.00 B/s

IPsec Client Settings

Name	Peer IP/Domain	Local Subnet	Peer Subnet	Auth Method	Interface	Status	Actions	□
ipsec	10.10.10.1	192.168.0.0/24	192.168.10.0/24	Pre-Shared Key	Auto	Not Connected	Edit Disable Delete	□

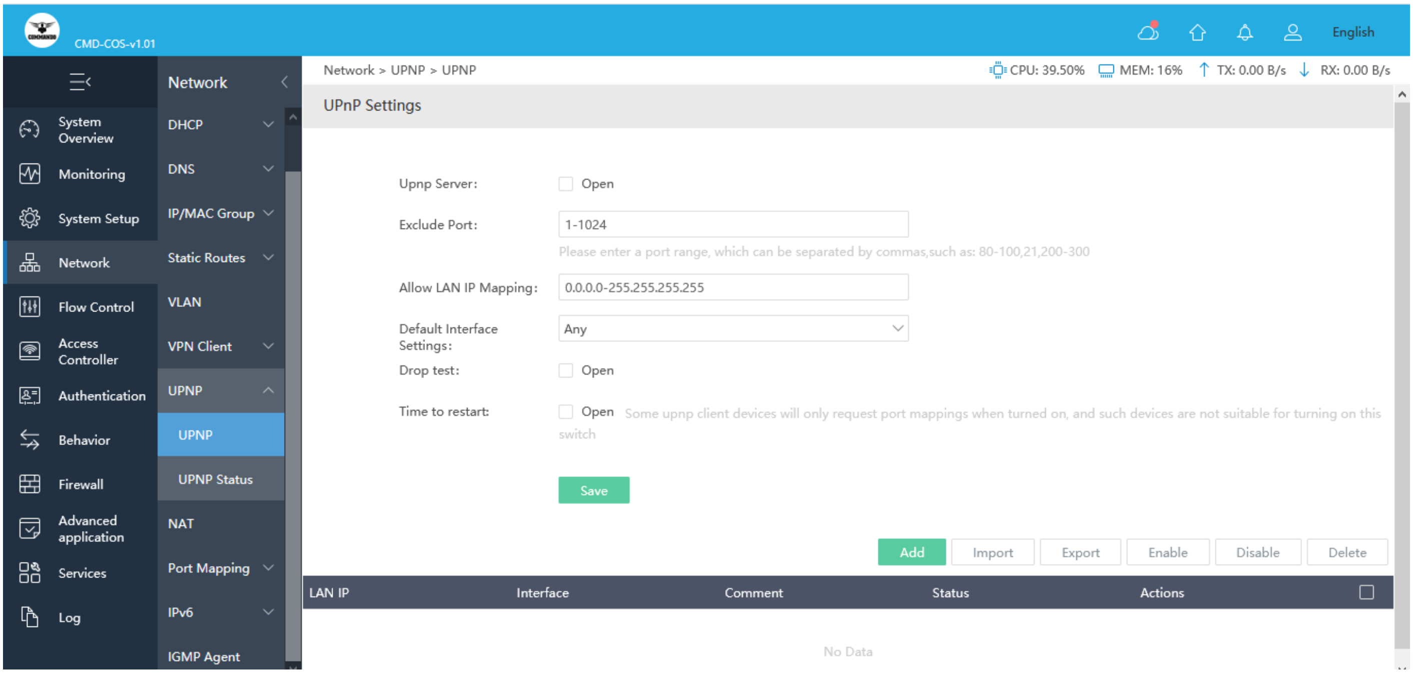
Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

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



Network > UPNP > UPNP CPU: 39.50% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

UPnP Settings

Upnp Server: □ Open

Exclude Port: 1-1024

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

Allow LAN IP Mapping: 0.0.0.0-255.255.255.255

Default Interface Settings: Any

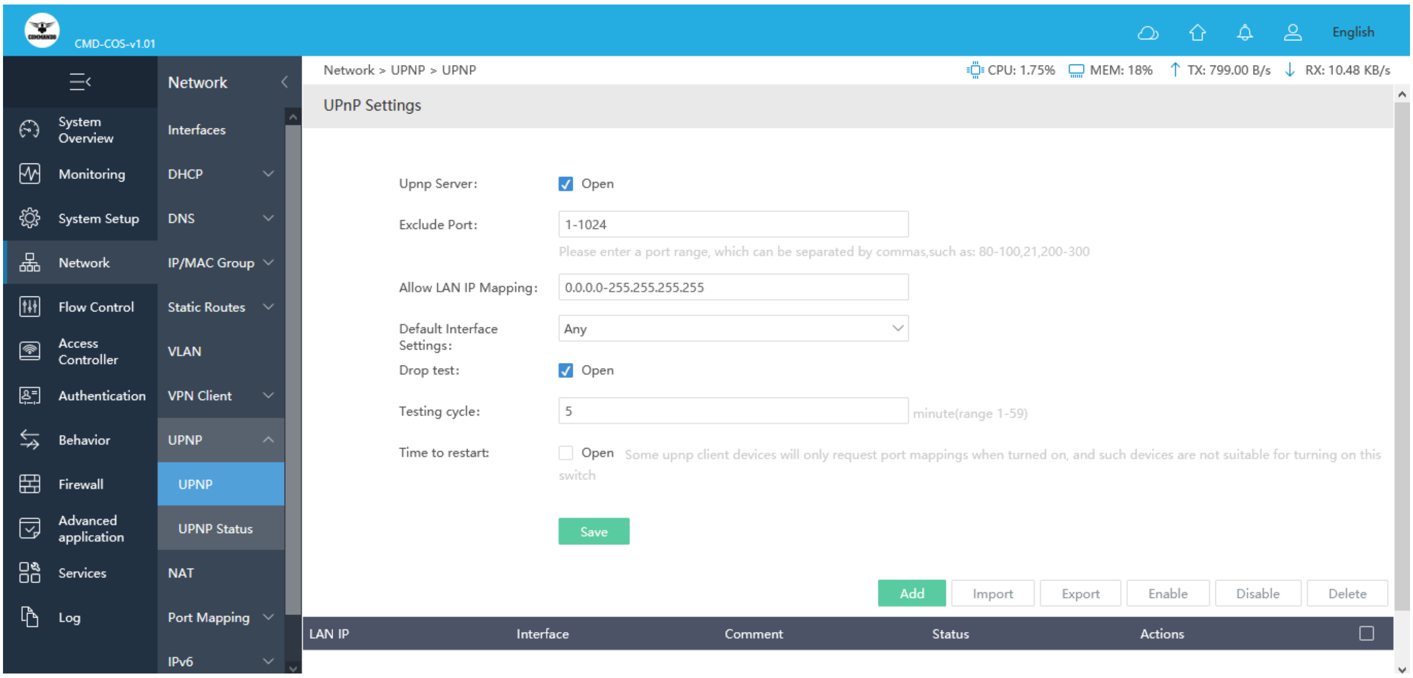
Drop test: □ Open

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

LAN IP	Interface	Comment	Status	Actions	□

No Data

Fig 3.8.1 Default UPnP setting page



UPnP Settings

Upnp Server: ☑ Open

Exclude Port: 1-1024

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

Allow LAN IP Mapping: 0.0.0.0-255.255.255.255

Default Interface Settings: Any

Drop test: ☑ Open

Testing cycle: 5 minute(range 1-59)

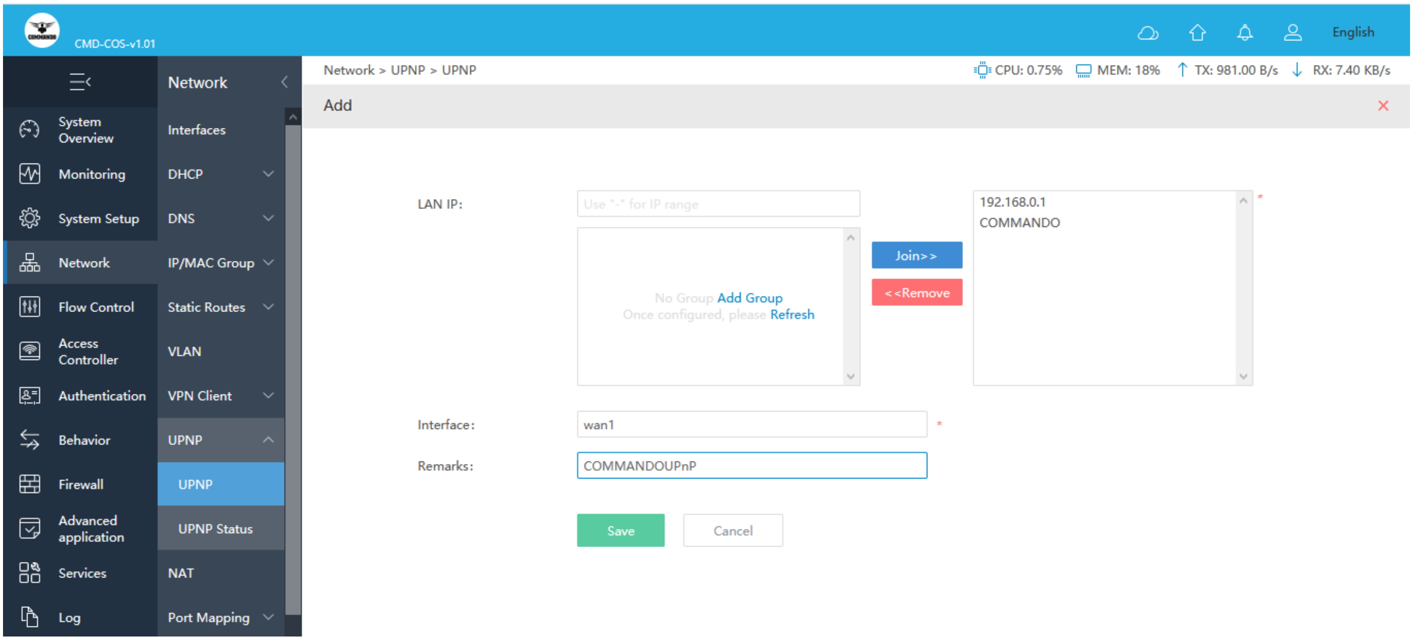
Time to restart: ☐ Open Some upnp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch

Save

Add Import Export Enable Disable Delete

LAN IP	Interface	Comment	Status	Actions	□

Fig 3.8.2 Enabling UPnP setting page



Add ×

LAN IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Join>>
<<Remove

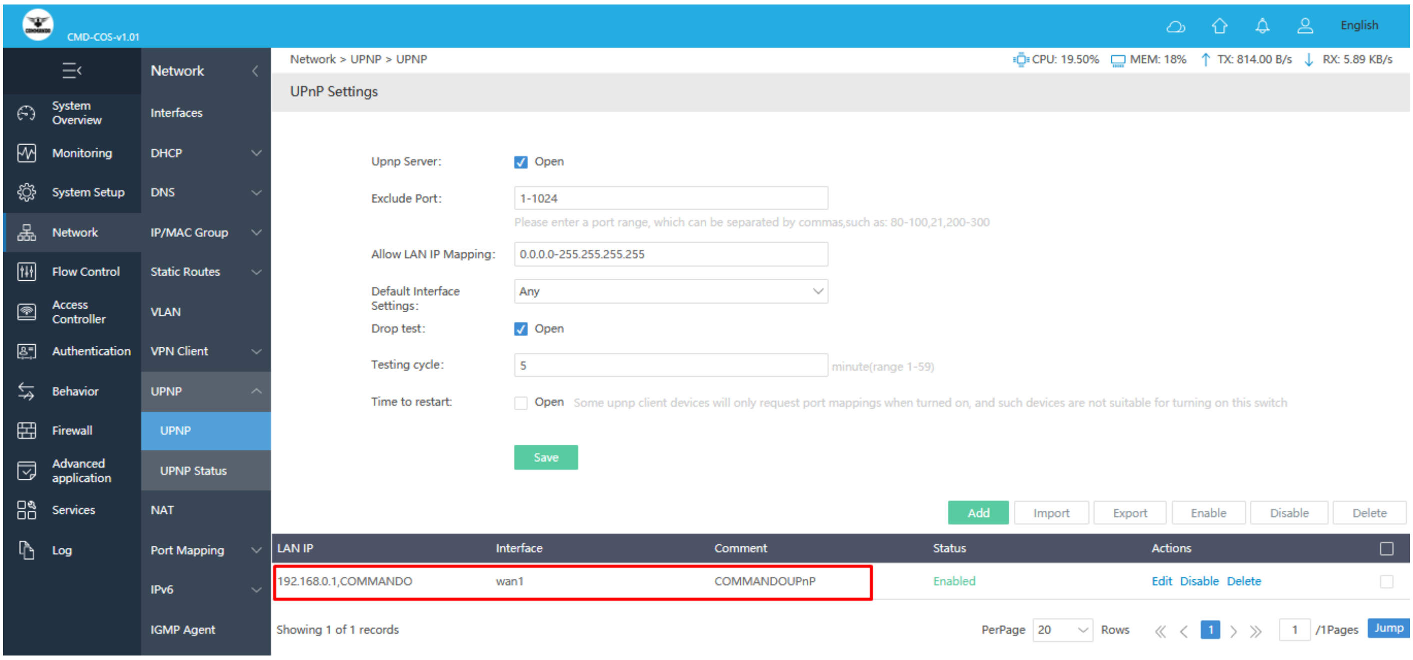
192.168.0.1
COMMANDO

Interface: wan1 *

Remarks: COMMANDOUPnP

Save Cancel

Fig 3.8.3 Add UPnP setting page



UPnP Settings

Upnp Server: ☑ Open

Exclude Port: 1-1024

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

Allow LAN IP Mapping: 0.0.0.0-255.255.255.255

Default Interface Settings: Any

Drop test: ☑ Open

Testing cycle: 5 minute(range 1-59)

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

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

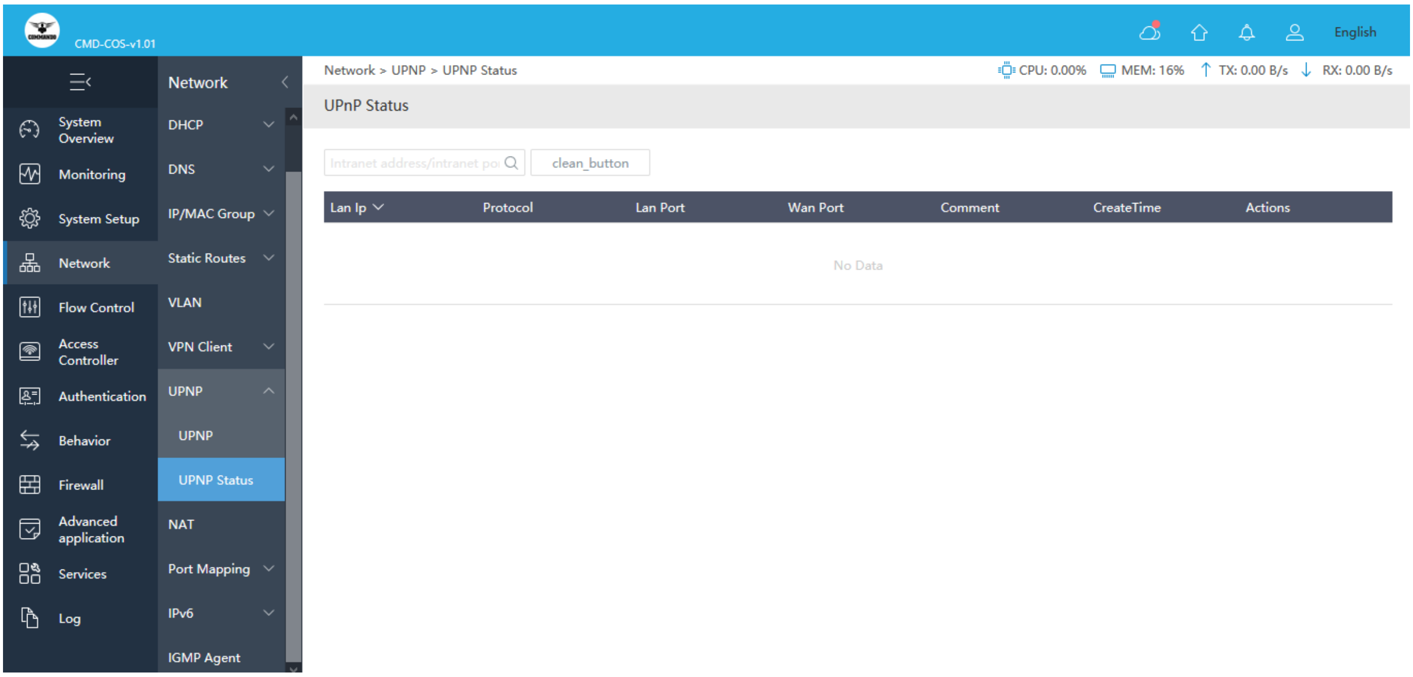
Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

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 f. 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



Lan Ip	Protocol	Lan Port	Wan Port	Comment	CreateTime	Actions
			No Data			

Fig 3.8.5 UPnP Status page

3.9 NAT

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

It translates the IP address in an IP datagram header to another IP address, allowing users on private networks to access public networks. Basic NAT implements one-to-one translation between one private IP address and one public IP address, whereas Network Address and Port Translation (NAPT) implements one-to-many translation between one public IP address and multiple private IP addresses. The Exhaustion of IPv4 addresses has become a bottleneck for the network development. IPv6 can solve the problem of IPv4 address shortage, but numerous network devices and applications are based on IPv4. Major transitional technologies such as classless inter-domain routing (CIDR) and private network addresses are used before the wide use of IPv6 addresses. NAT enables users on private networks to access public networks. When a host on a private network accesses a public network, NAT translates the host's private IP address to a public IP address. Multiple hosts on a private network can share one public IP address. This implements network communication while saving public IP addresses. In addition to one-to-one address translation, NAPT allows multiple private IP addresses to be mapped to the same public IP address. It is also called many-to-one address translation or address reuse.

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

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

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

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

NAT ALG

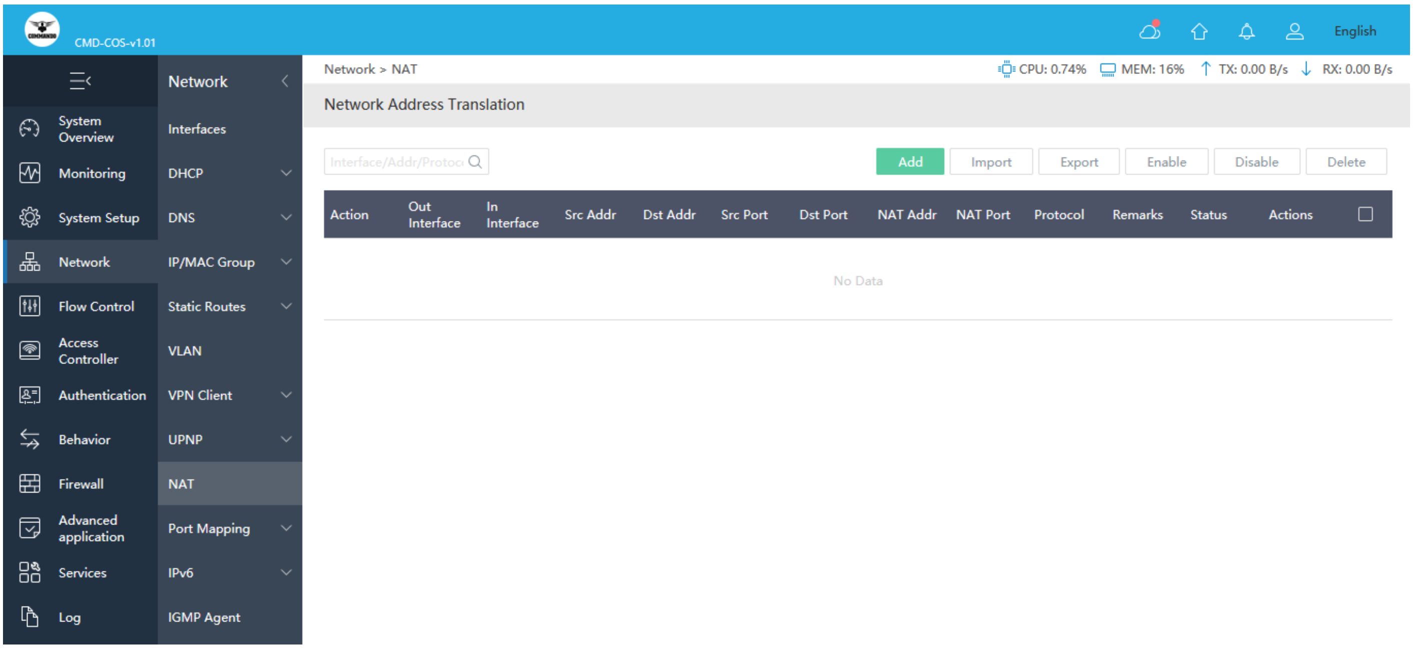
NAT and NAPT can translate only IP addresses in IP datagram headers and port numbers in TCP/UDP headers. For some special protocols such as FTP, IP addresses or port numbers may be contained in the Data field of the protocol packets. Therefore, NAT cannot translate the IP addresses or port numbers. A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

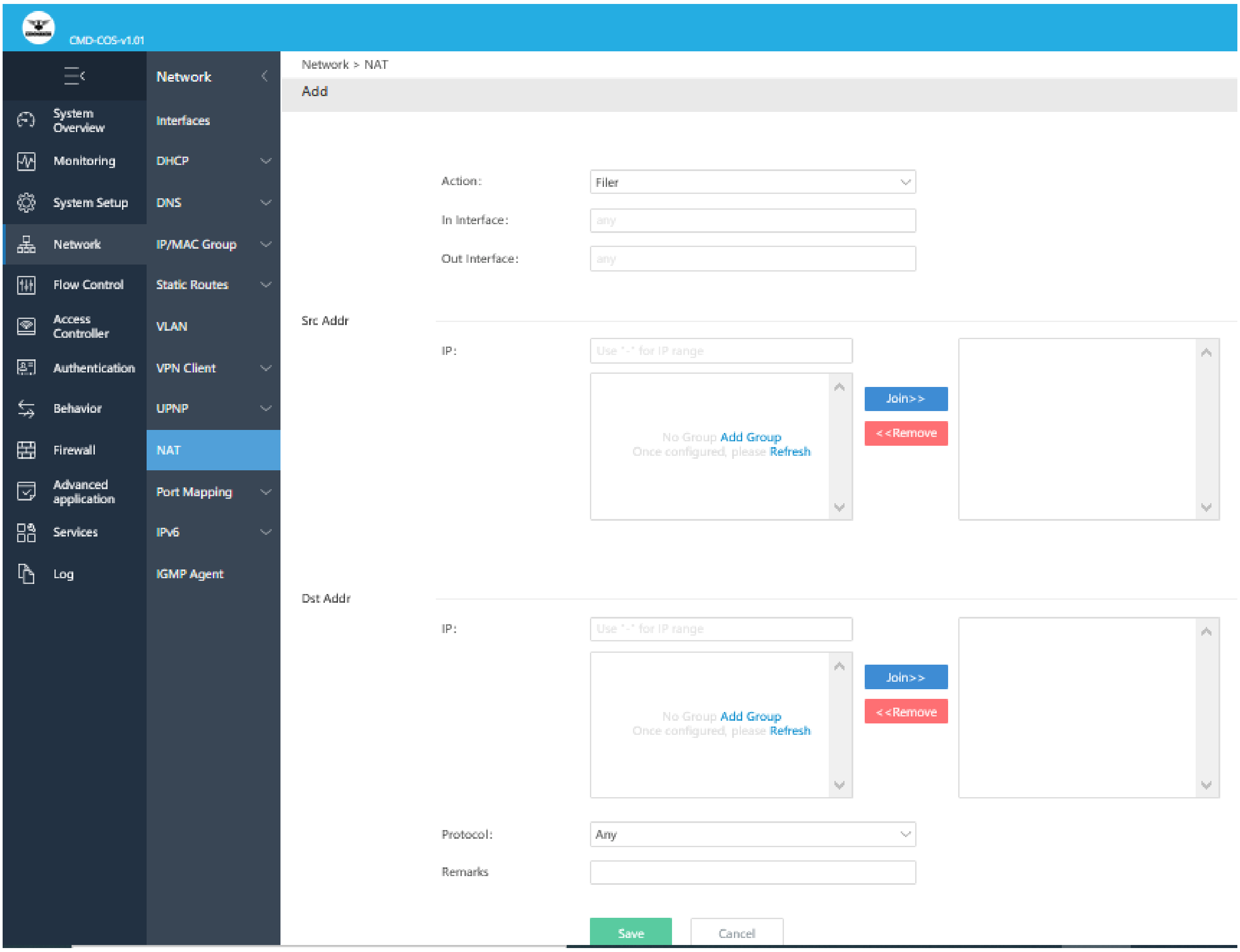
To configure Network Address Translation, Click on Network > NAT



Action	Out Interface	In Interface	Src Addr	Dst Addr	Src Port	Dst Port	NAT Addr	NAT Port	Protocol	Remarks	Status	Actions	□

No Data

Fig 3.9.1 Default Network Address Translation page



Action: Filer

In Interface: any

Out Interface: any

Src Addr

IP: Use '-' for IP range

No Group Add Group
Once configured, please Refresh

Dst Addr

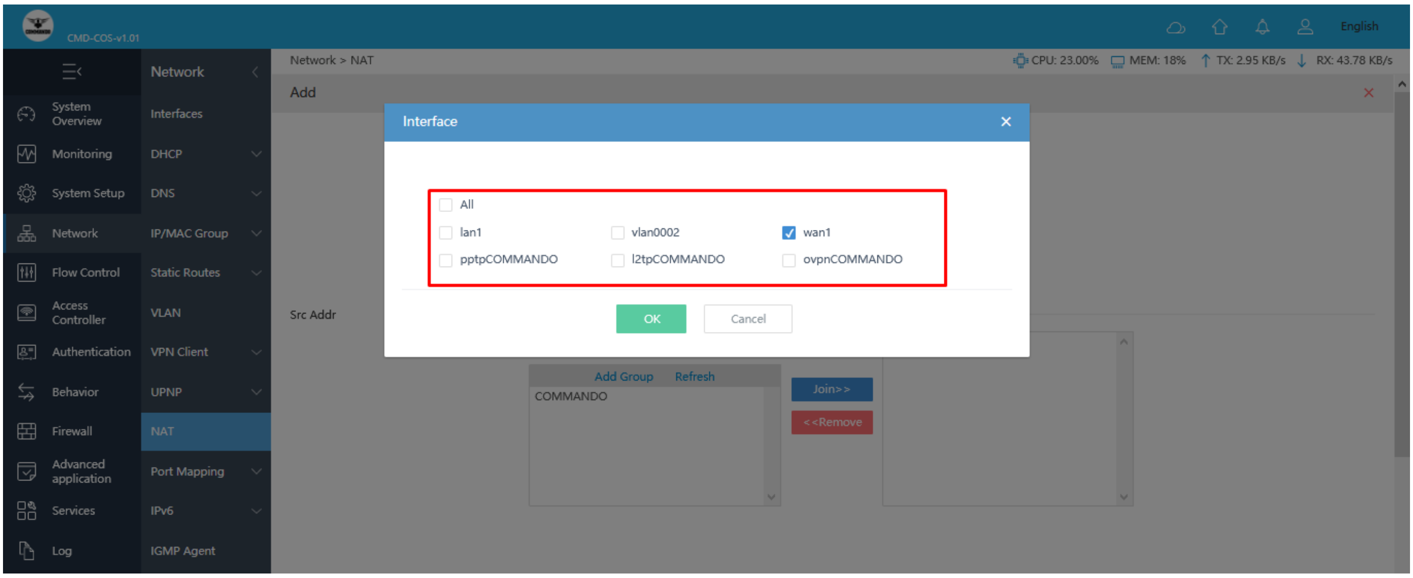
IP: Use '-' for IP range

No Group Add Group
Once configured, please Refresh

Protocol: Any

Remarks

Fig 3.9.2 Default Add Network Address Translation page

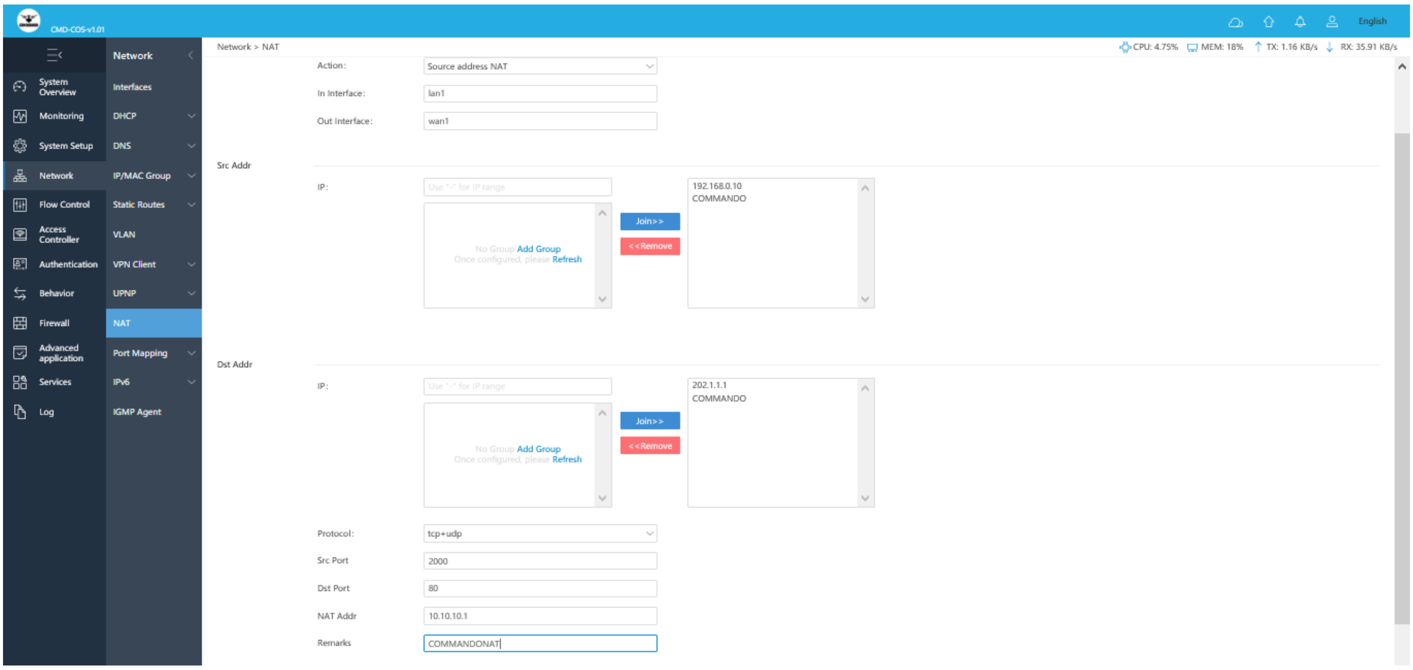


CPU: 23.00% MEM: 18% TX: 2.95 KB/s RX: 43.78 KB/s

Interface

□ All
□ lan1 □ vlan0002 ☑ wan1
□ pptpCOMMANDO □ l2tpCOMMANDO □ ovpnCOMMANDO

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



Action: Source address NAT

In Interface: lan1

Out Interface: wan1

Src Addr

IP: 192.168.0.10 COMMANDO

Dst Addr

IP: 202.1.1.1 COMMANDO

Protocol: tcp+udp

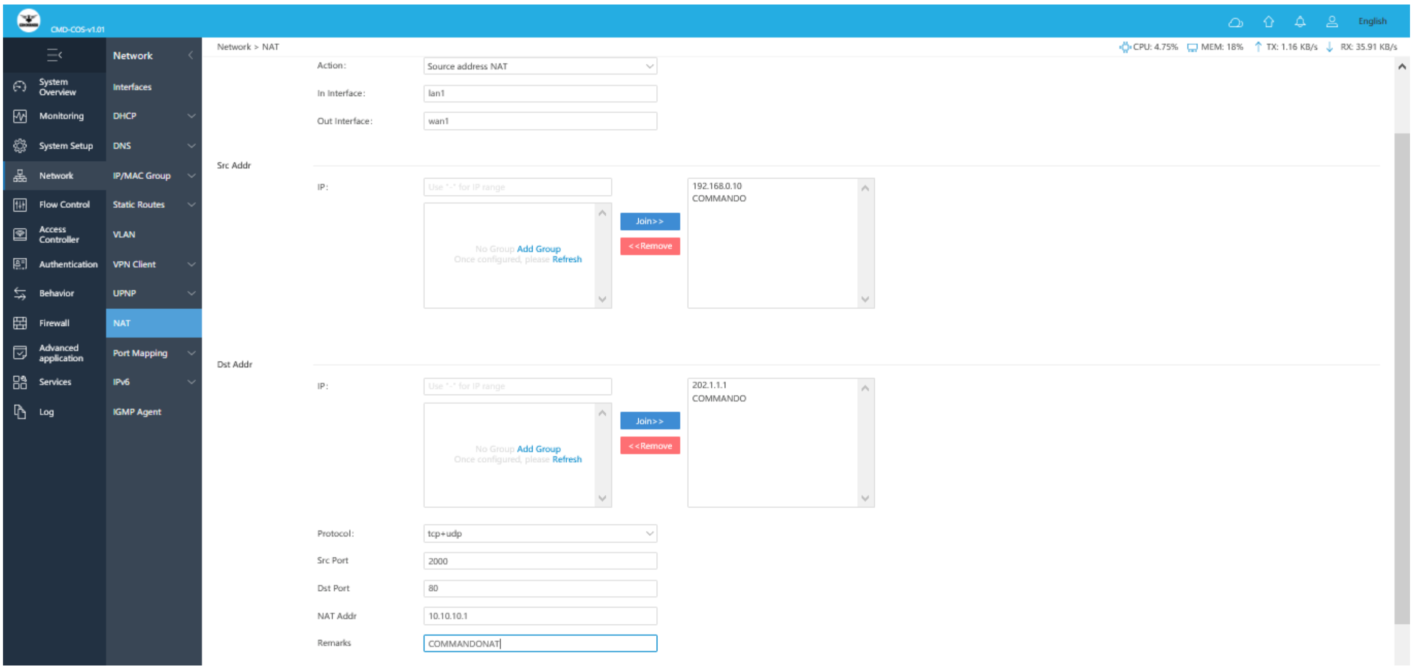
Src Port 2000

Dst Port 80

NAT Addr 10.10.10.1

Remarks COMMANDONAT

Fig 3.9.4 Network Address Translation details page



Action: Source address NAT

In Interface: lan1

Out Interface: wan1

Src Addr

IP: 192.168.0.10 COMMANDO

Dst Addr

IP: 202.1.1.1 COMMANDO

Protocol: tcp+udp

Src Port 2000

Dst Port 80

NAT Addr 10.10.10.1

Remarks COMMANDONAT

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.

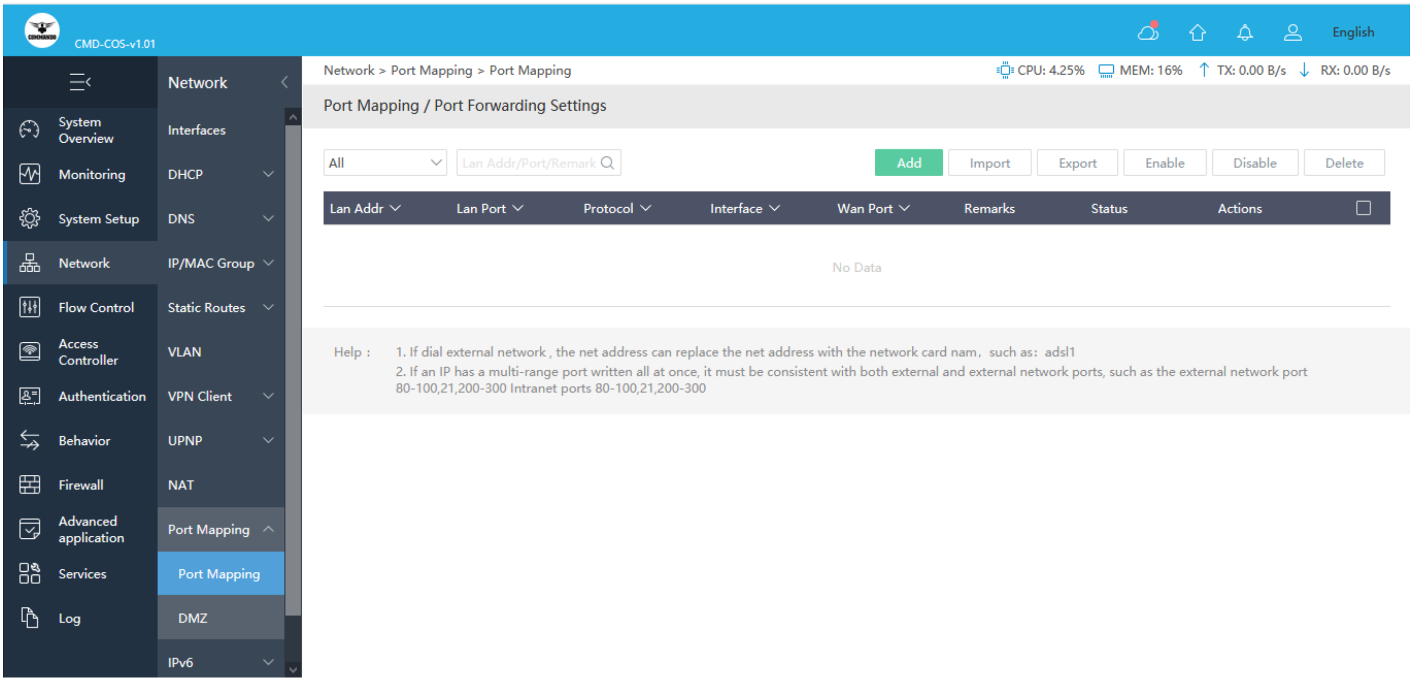
Local port forwarding is the most common type of port forwarding. It is used to let a user connect from the local computer to another server, ie. forward data securely from another client application running on the same computer as a Secure Shell (SSH) client. Some uses of local port forwarding:

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



Network > Port Mapping > Port Mapping

CPU: 4.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Port Mapping / Port Forwarding Settings

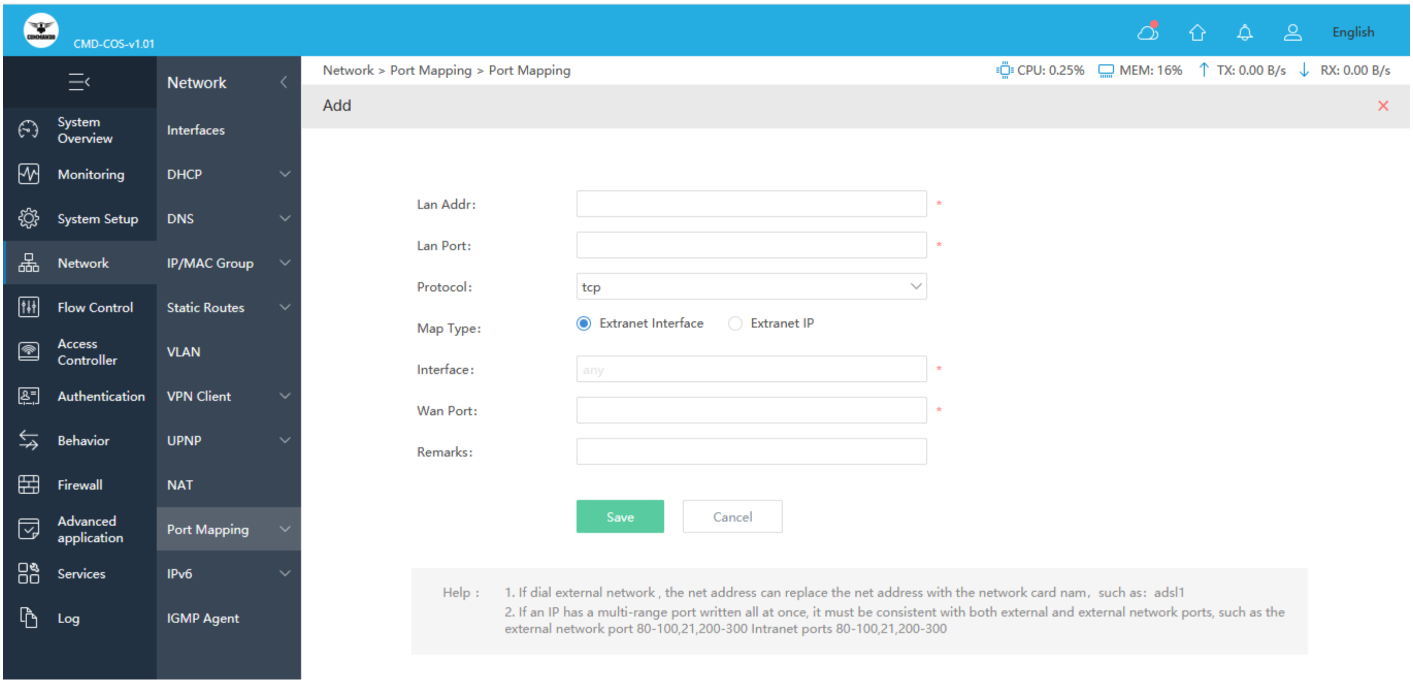
All | Lan Addr/Port/Remark

Lan Addr	Lan Port	Protocol	Interface	Wan Port	Remarks	Status	Actions	□

No Data

Help : 1. If dial external network , the net address can replace the net address with the network card nam, such as: adsl1
2. If an IP has a multi-range port written all at once, it must be consistent with both external and external network ports, such as the external network port 80-100,21,200-300 Intranet ports 80-100,21,200-300

Fig 3.10.1 Default Port Mapping / Port Forwarding Settings page



Network > Port Mapping > Port Mapping

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

Add

Lan Addr: *

Lan Port: *

Protocol: tcp

Map Type: ● Extranet Interface ○ Extranet IP

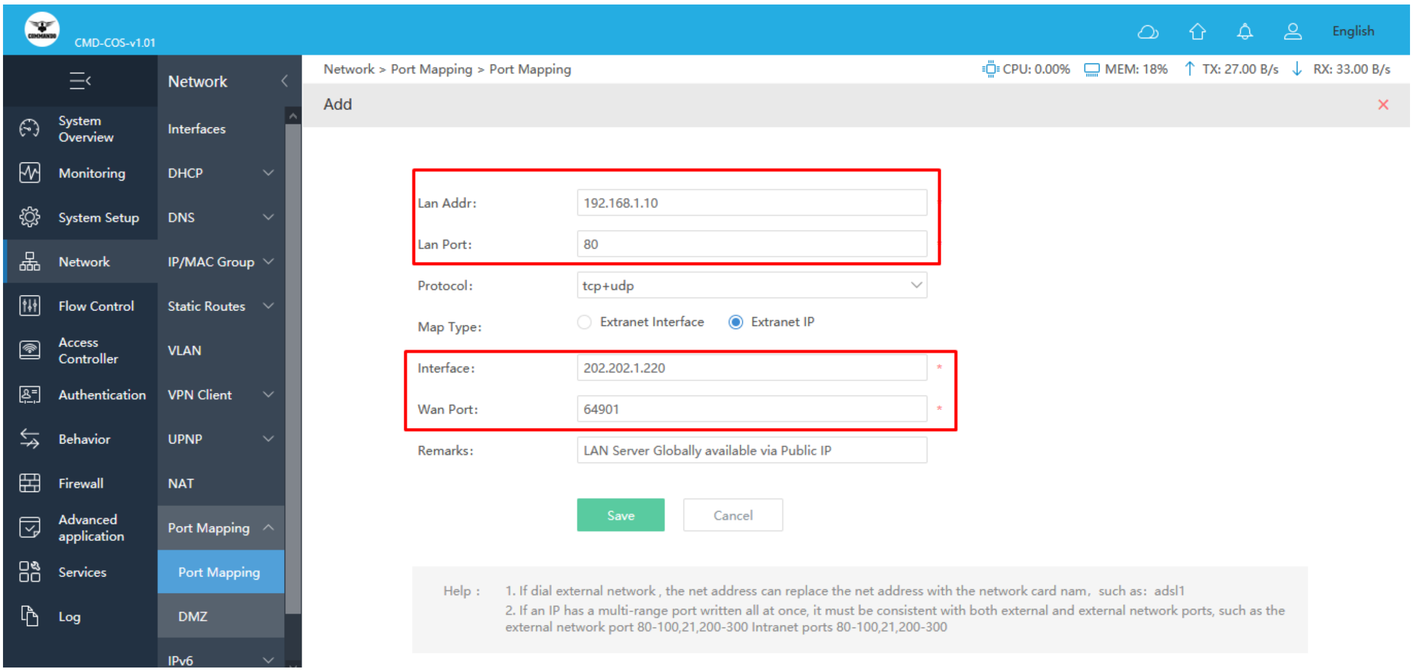
Interface: any *

Wan Port: *

Remarks:

Help : 1. If dial external network , the net address can replace the net address with the network card nam, such as: adsl1
2. If an IP has a multi-range port written all at once, it must be consistent with both external and external network ports, such as the external network port 80-100,21,200-300 Intranet ports 80-100,21,200-300

Fig 3.10.2 Add Port Mapping / Port Forwarding Settings page



Lan Addr: 192.168.1.10

Lan Port: 80

Protocol: tcp+udp

Map Type: ○ Extranet Interface ● Extranet IP

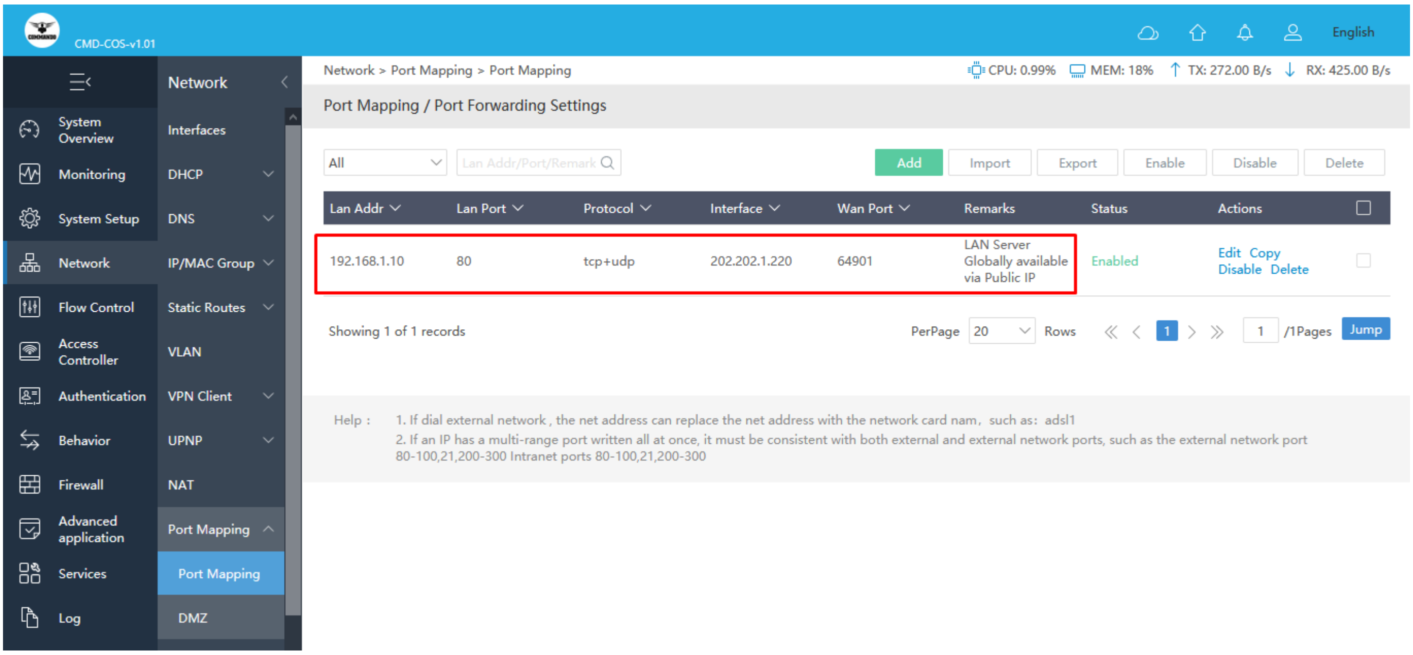
Interface: 202.202.1.220 *

Wan Port: 64901 *

Remarks: LAN Server Globally available via Public IP

Help : 1. If dial external network , the net address can replace the net address with the network card nam，such as：adsl1
2. If an IP has a multi-range port written all at once, it must be consistent with both external and external network ports, such as the external network port 80-100,21,200-300 Intranet ports 80-100,21,200-300

Fig 3.10.3 Port Mapping / Port Forwarding Detail Settings page



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

Showing 1 of 1 records PerPage 20 Rows 1 /1Pages Jump

Help : 1. If dial external network , the net address can replace the net address with the network card nam，such as：adsl1
2. If an IP has a multi-range port written all at once, it must be consistent with both external and external network ports, such as the external network port 80-100,21,200-300 Intranet ports 80-100,21,200-300

Fig 3.10.4 Port Mapping / Port Forwarding page

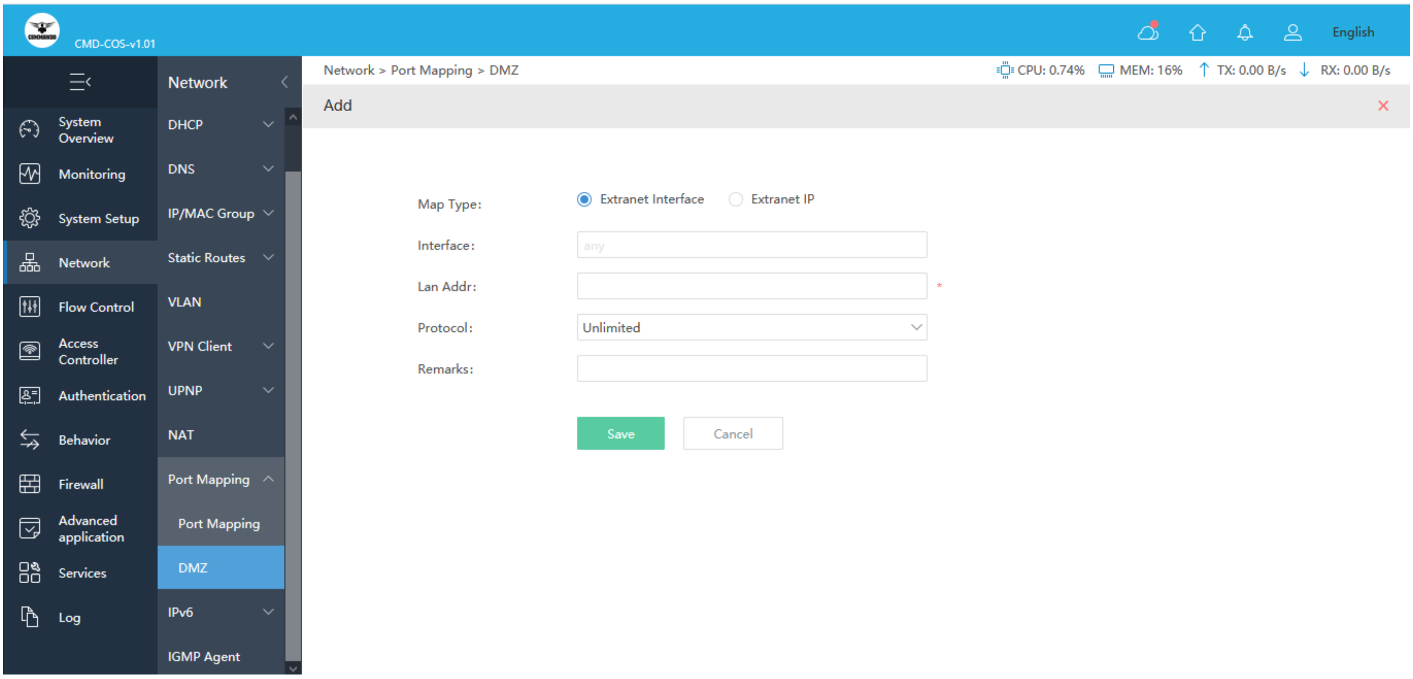
Now with public IP (created on WAN port generally) and port number in example 202.202.1.220:64901 you can access internal server 192.168.1.10:80.

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



Network > Port Mapping > DMZ

Add

Map Type: ● Extranet Interface ○ Extranet IP

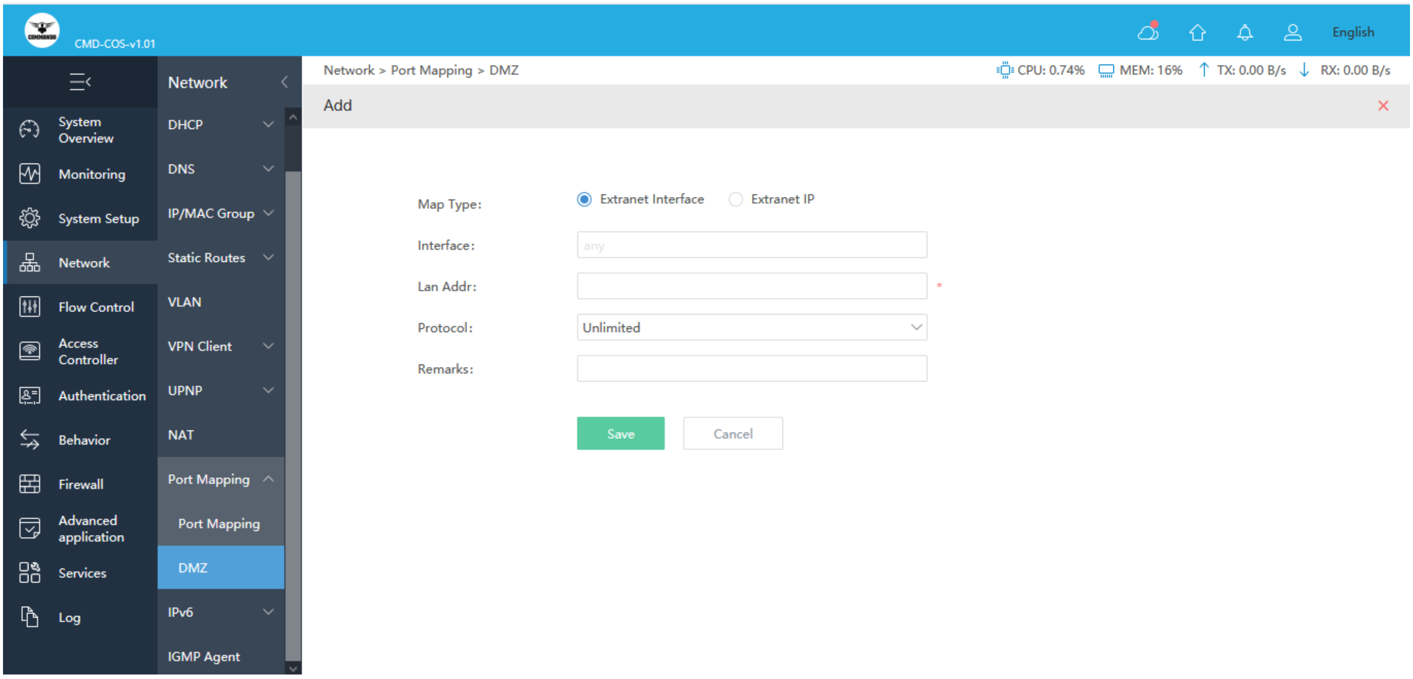
Interface: any

Lan Addr: *

Protocol: Unlimited

Remarks:

Fig 3.10.5 Default DMZ Settings page


Network > Port Mapping > DMZ

Add

Map Type: ● Extranet Interface ○ Extranet IP

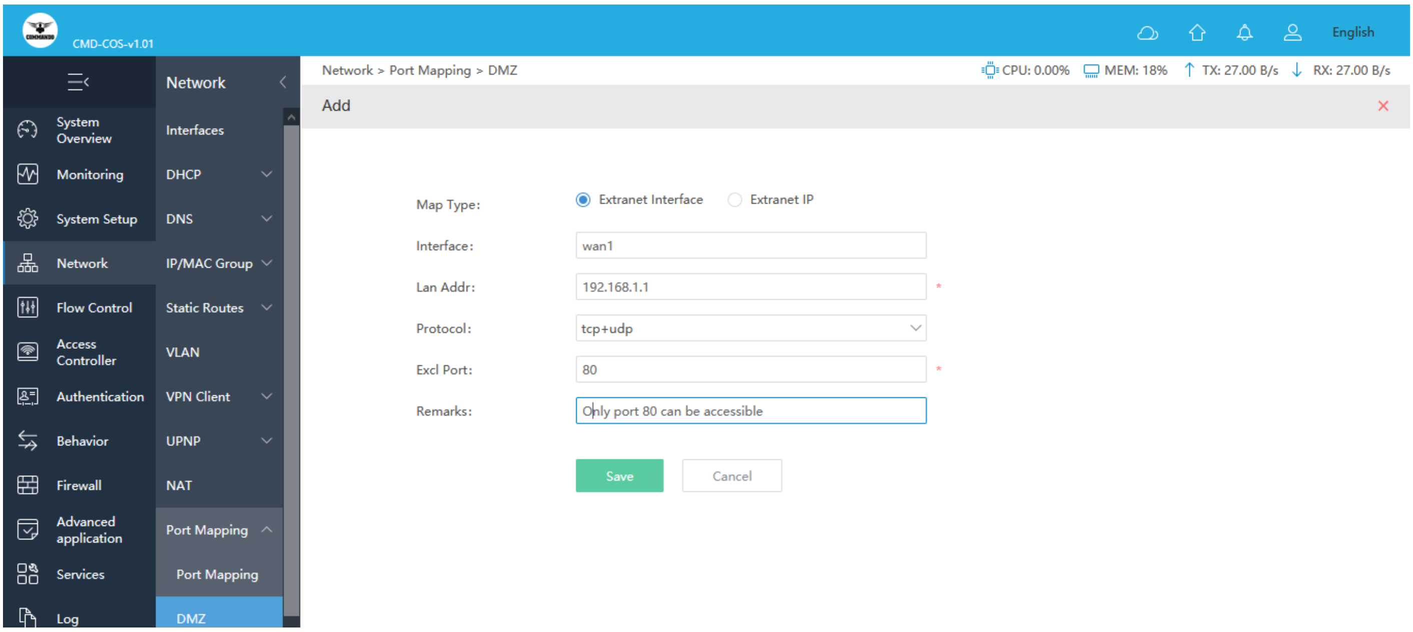
Interface: any

Lan Addr: *

Protocol: Unlimited

Remarks:

Fig 3.10.6 Add DMZ Settings page



Map Type: ● Extranet Interface ○ Extranet IP

Interface: wan1

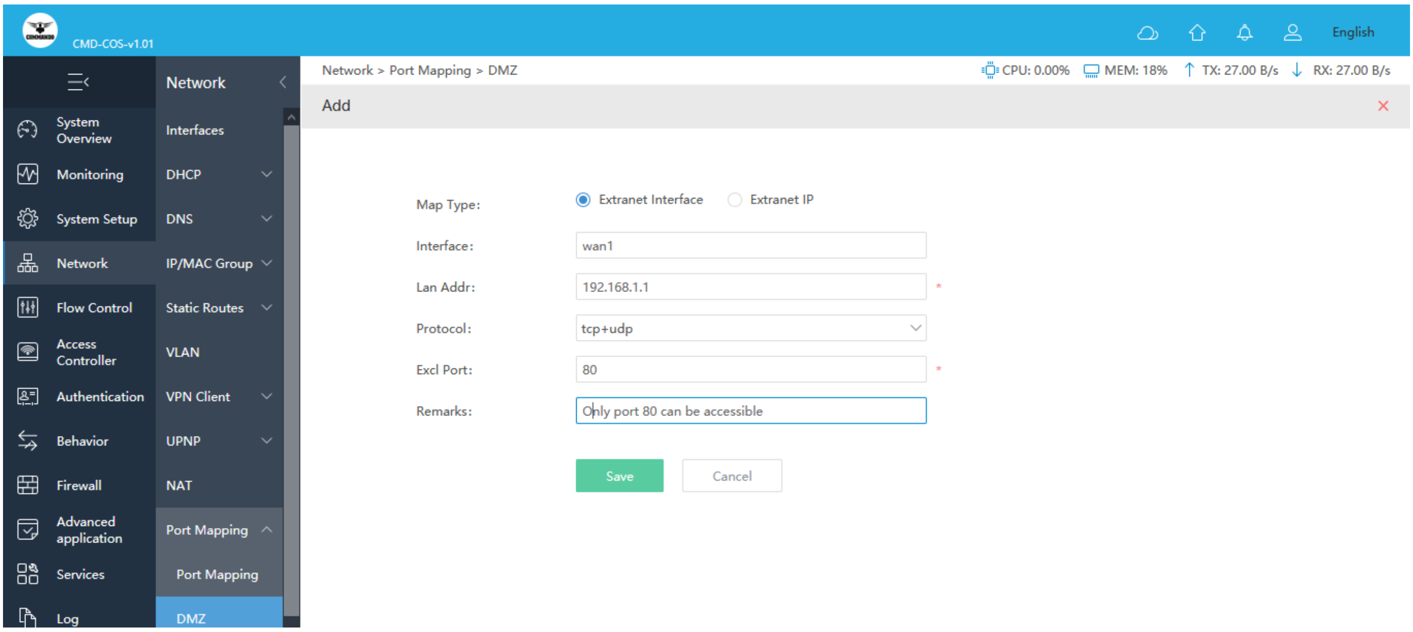
Lan Addr: 192.168.1.1 *

Protocol: tcp+udp

Excl Port: 80 *

Remarks: Only port 80 can be accessible

Fig 3.10.7 DMZ detail Settings page



Map Type: ● Extranet Interface ○ Extranet IP

Interface: wan1

Lan Addr: 192.168.1.1 *

Protocol: tcp+udp

Excl Port: 80 *

Remarks: Only port 80 can be accessible

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).

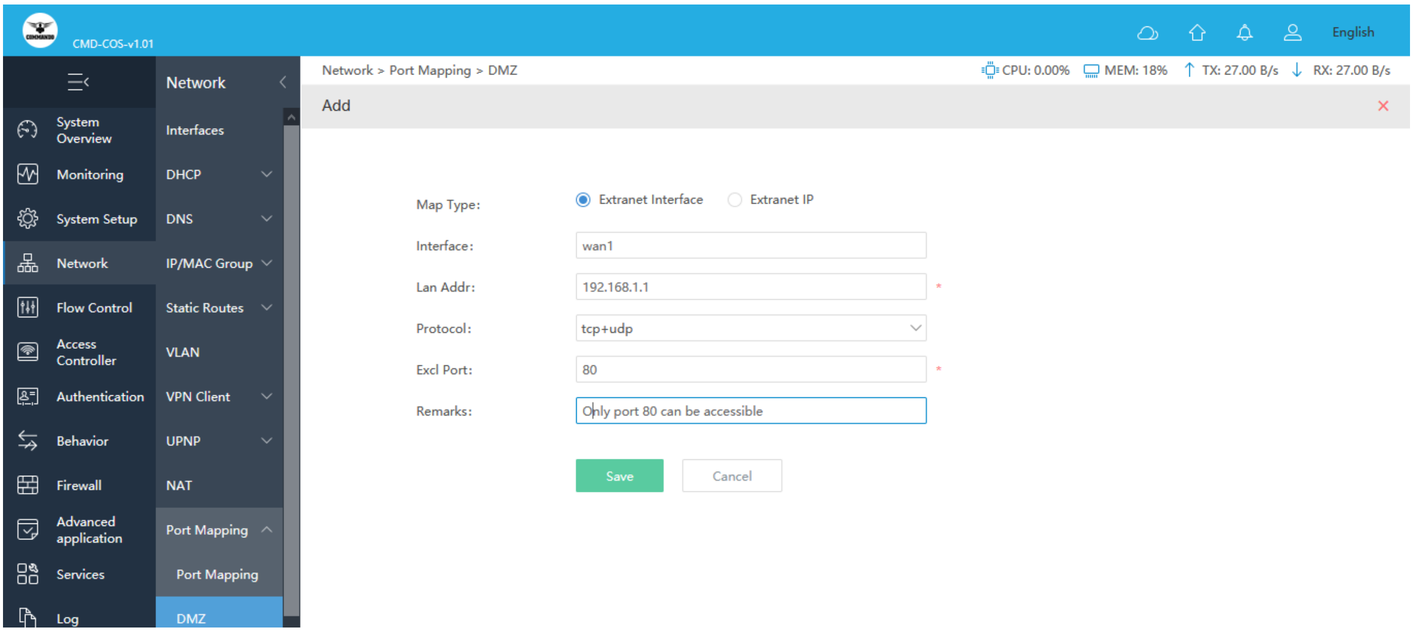
When IPv6 runs on a node, a link-local address that consists of a fixed prefix and an interface ID in EUI-64 format is automatically assigned to each interface of the node. This mechanism enables two IPv6 nodes on the same link to communicate without any configuration, making link-local addresses widely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



Map Type: ● Extranet Interface ○ Extranet IP

Interface: wan1

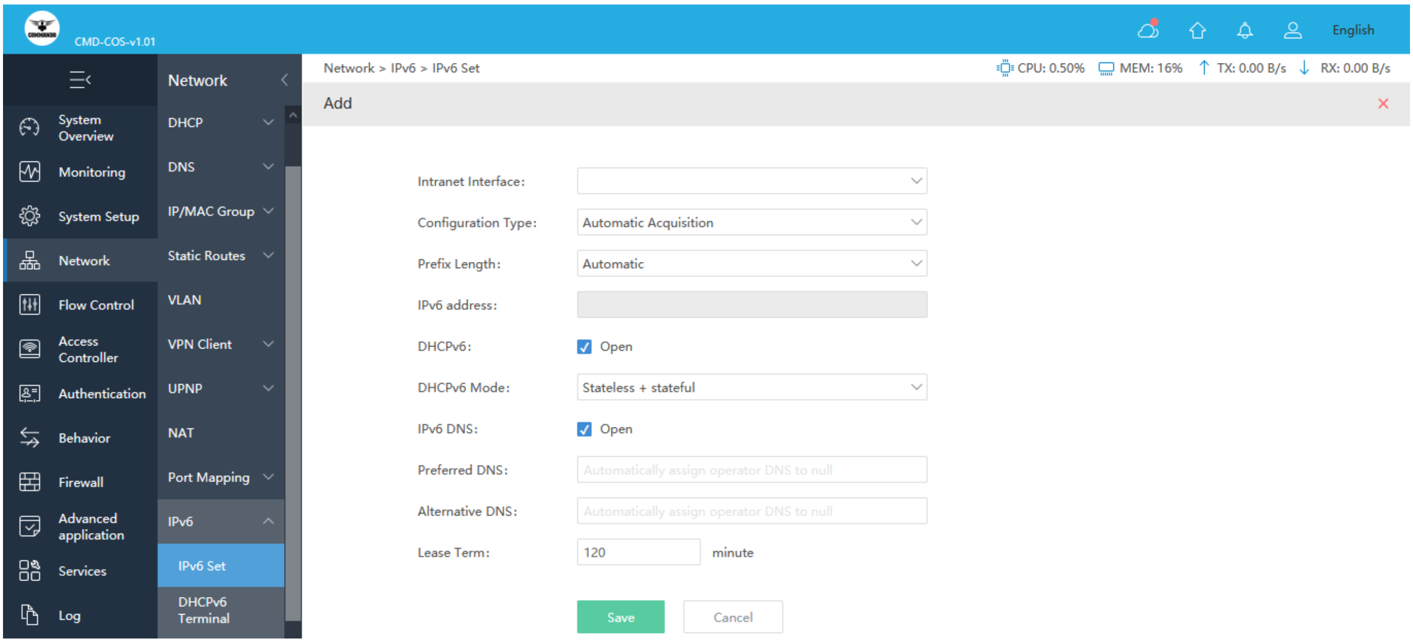
Lan Addr: 192.168.1.1 *

Protocol: tcp+udp

Excl Port: 80 *

Remarks: Only port 80 can be accessible

Fig 3.11.1 Default IPv6 Page



Intranet Interface:

Configuration Type: Automatic Acquisition

Prefix Length: Automatic

IPv6 address:

DHCPv6: ☑ Open

DHCPv6 Mode: Stateless + stateful

IPv6 DNS: ☑ Open

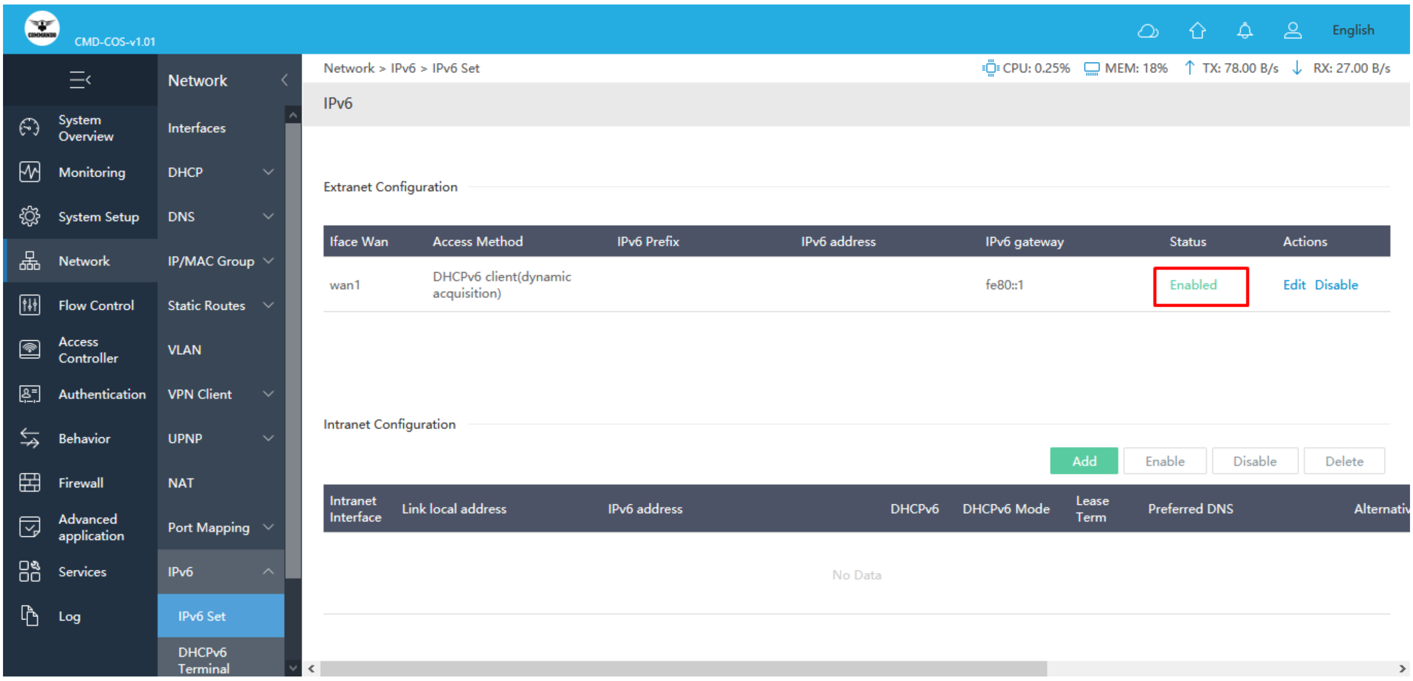
Preferred DNS: Automatically assign operator DNS to null

Alternative DNS: Automatically assign operator DNS to null

Lease Term: 120 minute

Fig 3.11.2 Add IPv6 Page

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



Network > IPv6 > IPv6 Set

CPU: 0.25% MEM: 18% TX: 78.00 B/s RX: 27.00 B/s

IPv6

Extranet Configuration

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

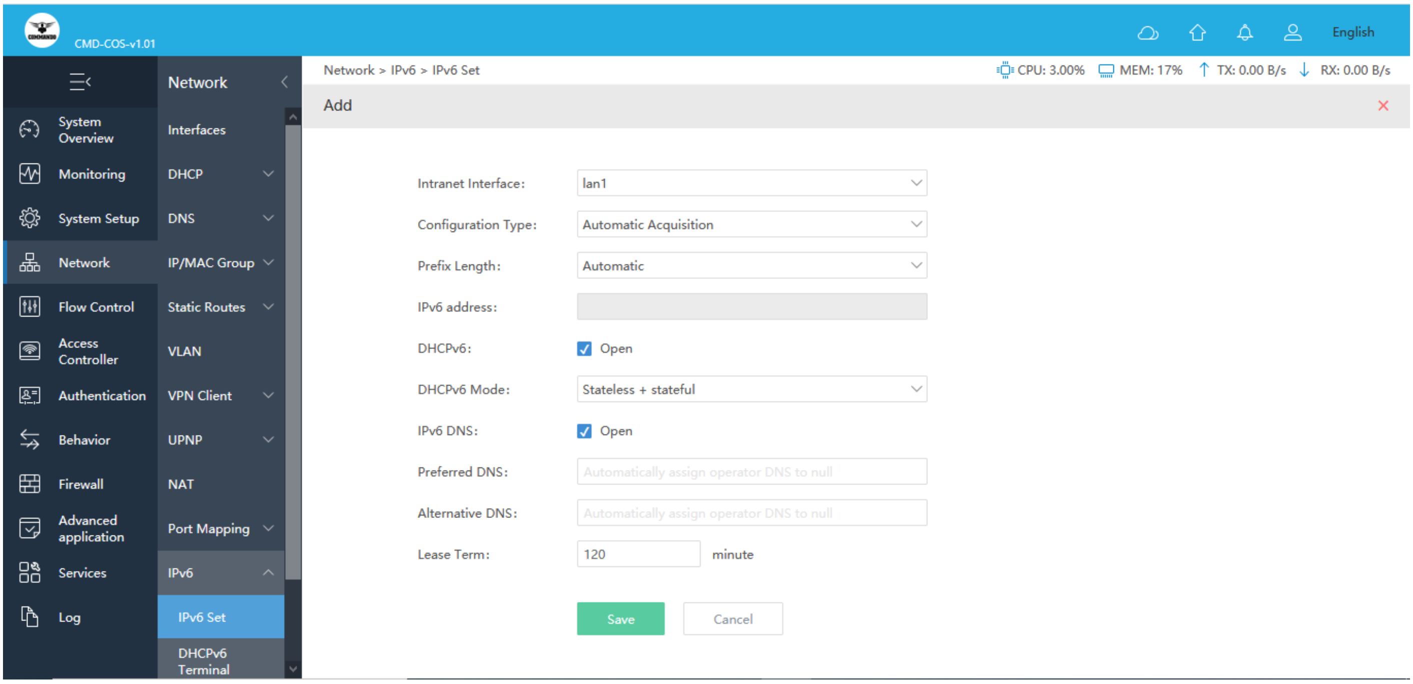
Intranet Configuration

Add Enable Disable Delete

Intranet Interface	Link local address	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term	Preferred DNS	Alternativ

No Data

Fig 3.11.3 Enabling DHCPv6 Page



Network > IPv6 > IPv6 Set

CPU: 3.00% MEM: 17% TX: 0.00 B/s RX: 0.00 B/s

Add ×

Intranet Interface: lan1

Configuration Type: Automatic Acquisition

Prefix Length: Automatic

IPv6 address:

DHCPv6: ☑ Open

DHCPv6 Mode: Stateless + stateful

IPv6 DNS: ☑ Open

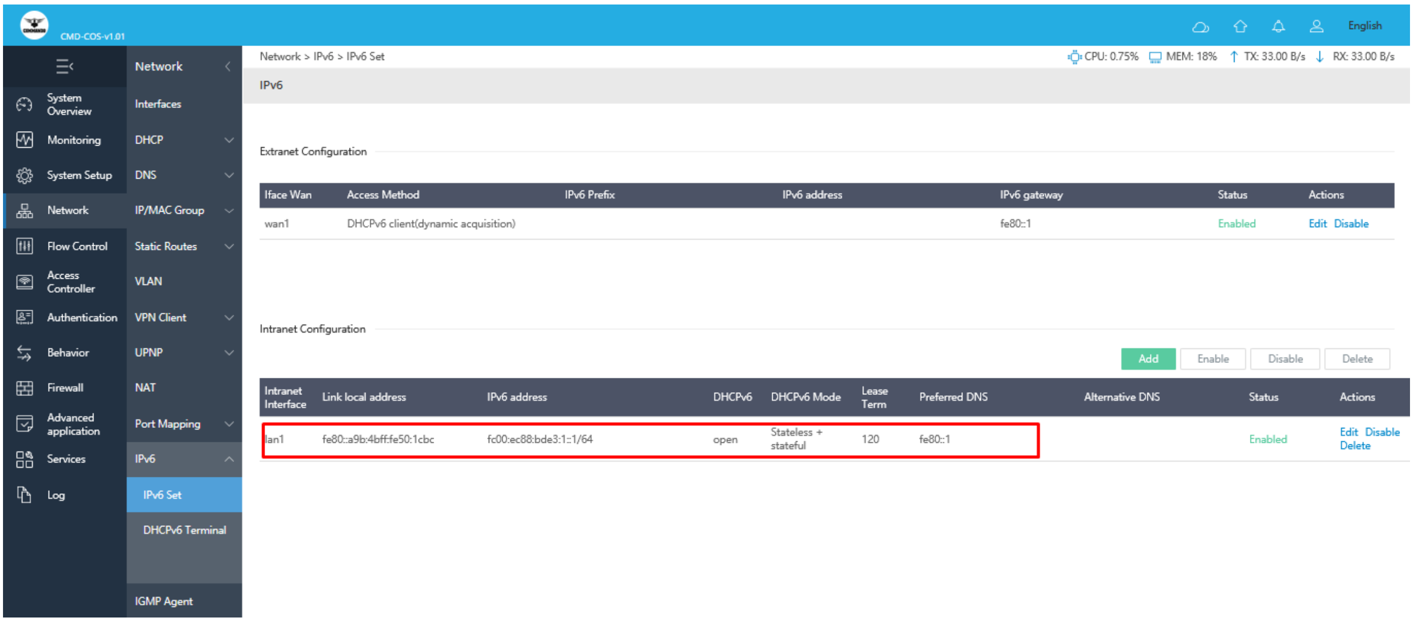
Preferred DNS: Automatically assign operator DNS to null

Alternative DNS: Automatically assign operator DNS to null

Lease Term: 120 minute

Save Cancel

Fig 3.11.4 Automatic Acquisition of IPv6 address for LAN1 interface Page



Network > IPv6 > IPv6 Set

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

IPv6

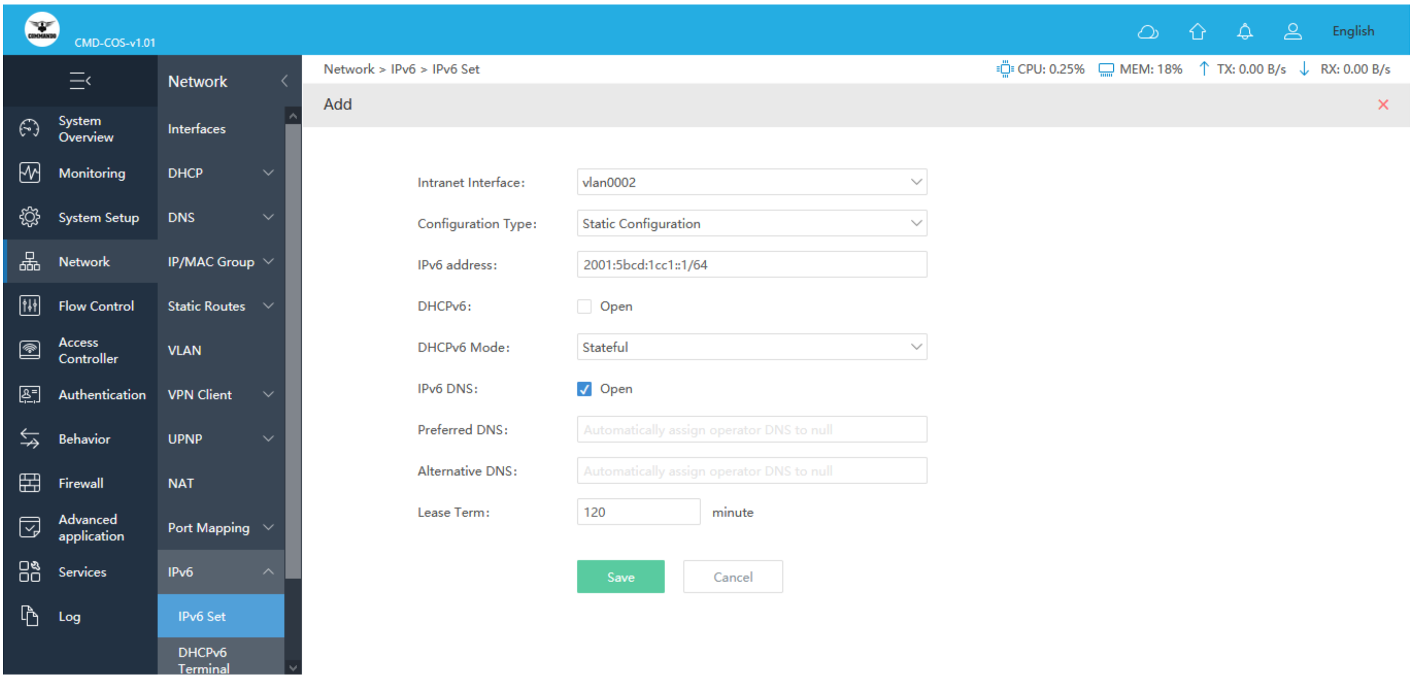
Extranet Configuration

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

Intranet Configuration

Intranet Interface	Link local address	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term	Preferred DNS	Alternative DNS	Status	Actions
lan1	fe80::a9b:4bff:fe50:1cbc	fc00:ec88:bde3:1::1/64	open	Stateless + stateful	120	fe80::1		Enabled	Edit Disable Delete

Fig 3.11.5 Automatic IPv6 address for LAN1 interface Page



Network > IPv6 > IPv6 Set

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

Add

Intranet Interface: vlan0002

Configuration Type: Static Configuration

IPv6 address: 2001:5bcd:1cc1::1/64

DHCPv6: □ Open

DHCPv6 Mode: Stateful

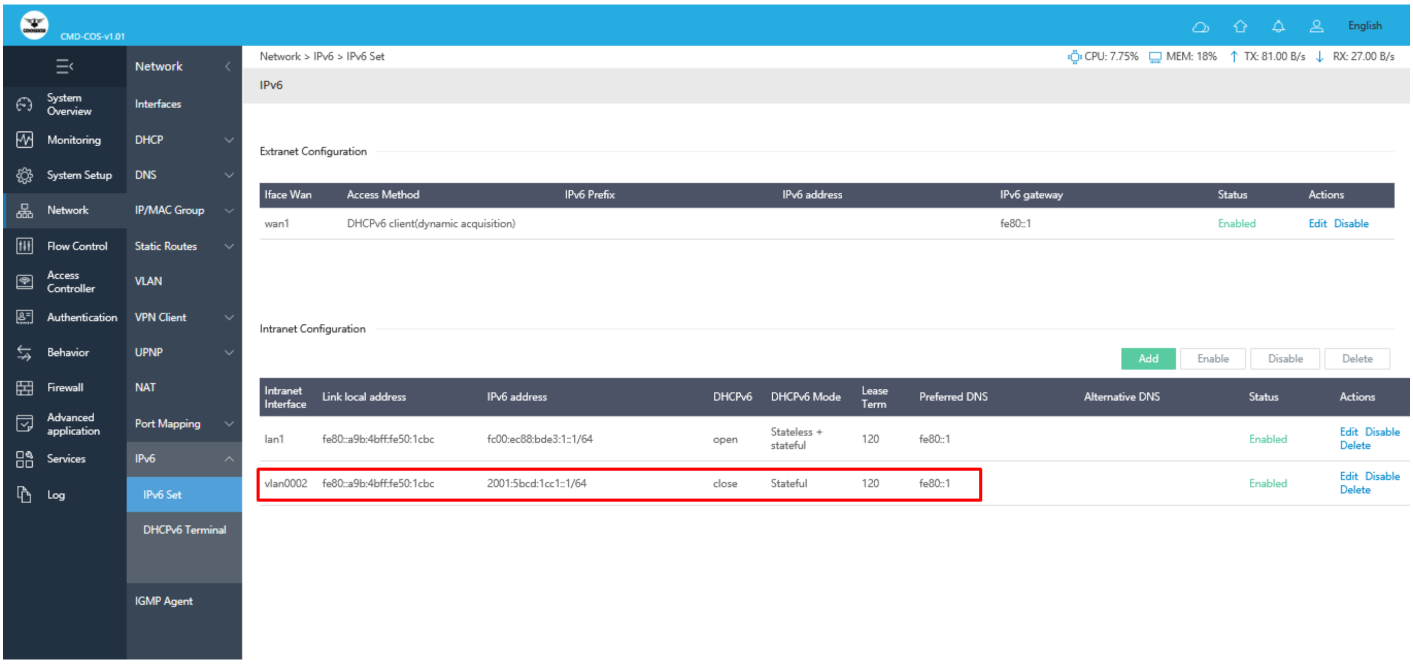
IPv6 DNS: ☑ Open

Preferred DNS: Automatically assign operator DNS to null

Alternative DNS: Automatically assign operator DNS to null

Lease Term: 120 minute

Fig 3.11.6 Manual IPv6 address for vlan0002 interface Page



Extranet Configuration

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

Intranet Configuration

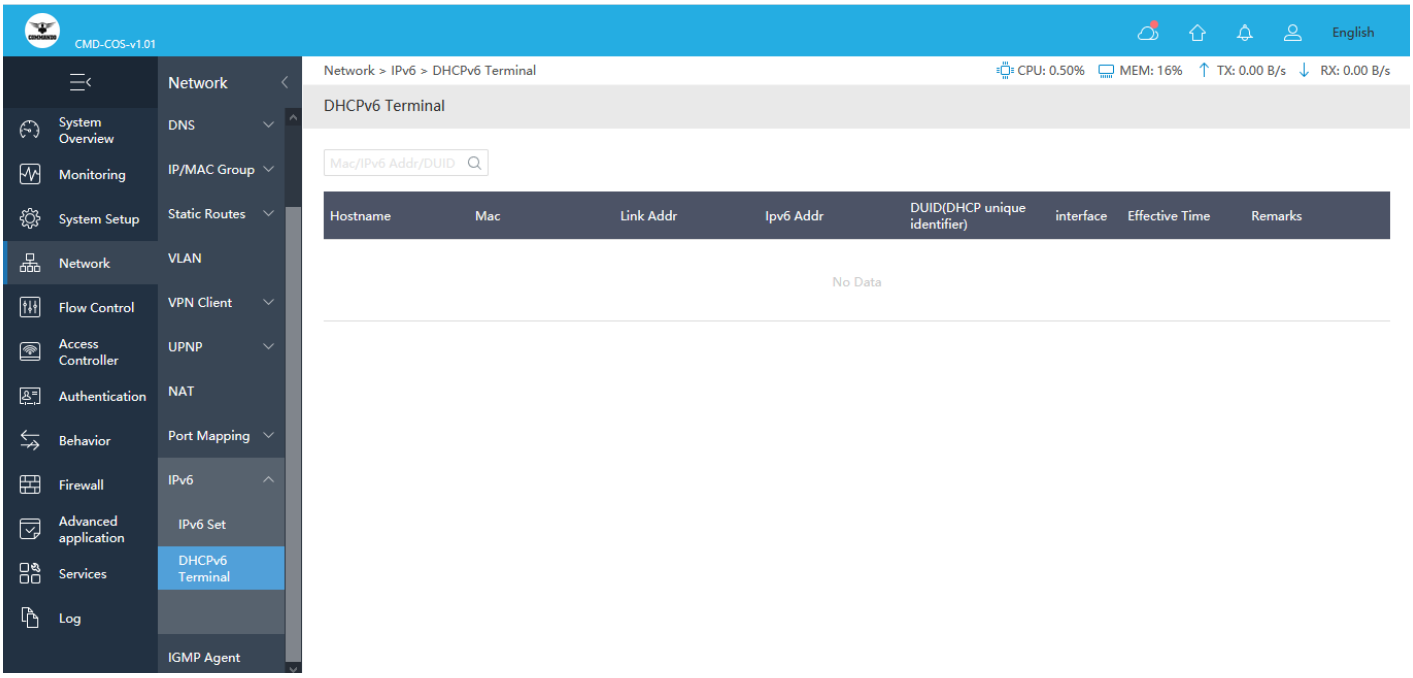
Intranet Interface	Link local address	IPv6 address	DHCPv6	DHCPv6 Mode	Lease Term	Preferred DNS	Alternative DNS	Status	Actions
lan1	fe80::a9b:4bff:fe50:1cbc	fc00:ec88:bde3:1::1/64	open	Stateless + stateful	120	fe80::1		Enabled	Edit Disable Delete
vlan0002	fe80::a9b:4bff:fe50:1cbc	2001:5bcd:1cc1::1/64	close	Stateful	120	fe80::1		Enabled	Edit Disable Delete

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.

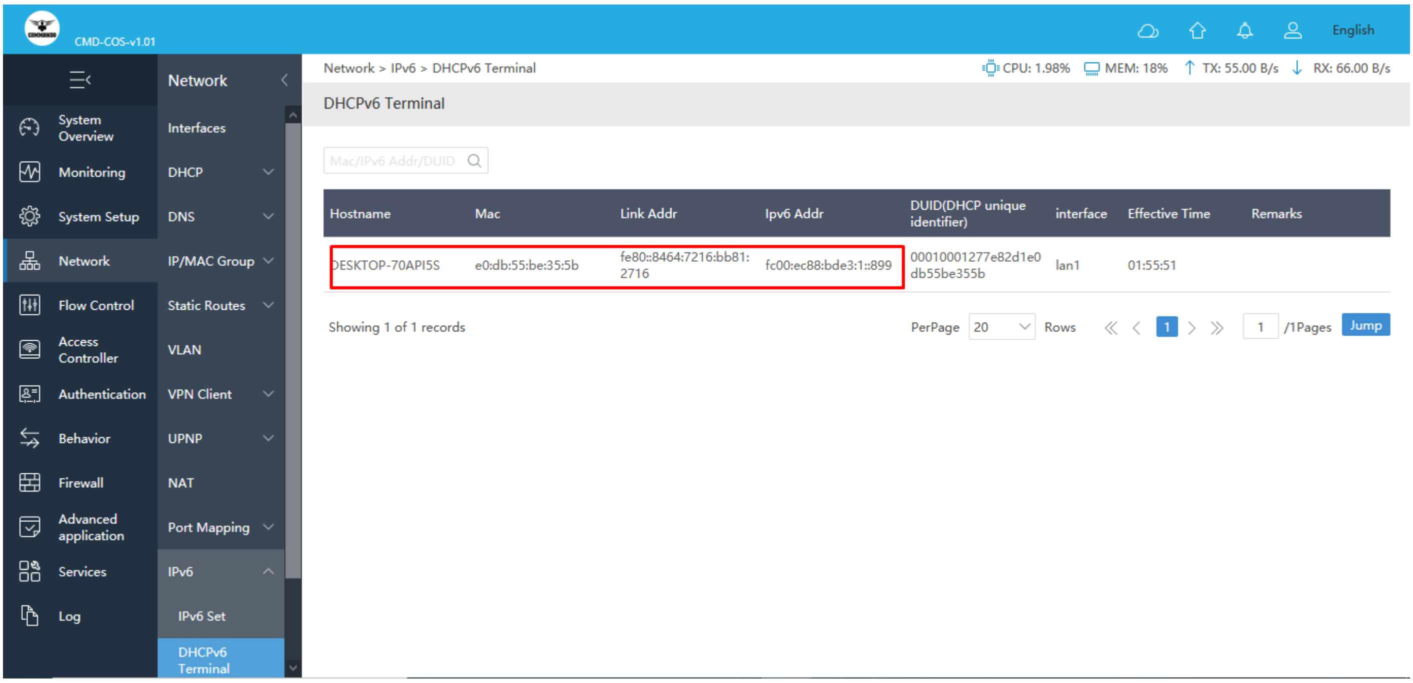
To view DHCPv6 Terminal, Click on Network > IPv6 > DHCPv6 Terminal



DHCPv6 Terminal

Hostname	Mac	Link Addr	Ipv6 Addr	DUID(DHCP unique identifier)	interface	Effective Time	Remarks
No Data							

Fig 3.11.8 Default DHCPv6 Terminal Page



DHCPv6 Terminal

Hostname	Mac	Link Addr	Ipv6 Addr	DUID(DHCP unique identifier)	interface	Effective Time	Remarks
DESKTOP-70API5S	e0:db:55:be:35:5b	fe80::8464:7216:bb81:2716	fc00:ec88:bde3:1::899	00010001277e82d1e0db55be355b	lan1	01:55:51	

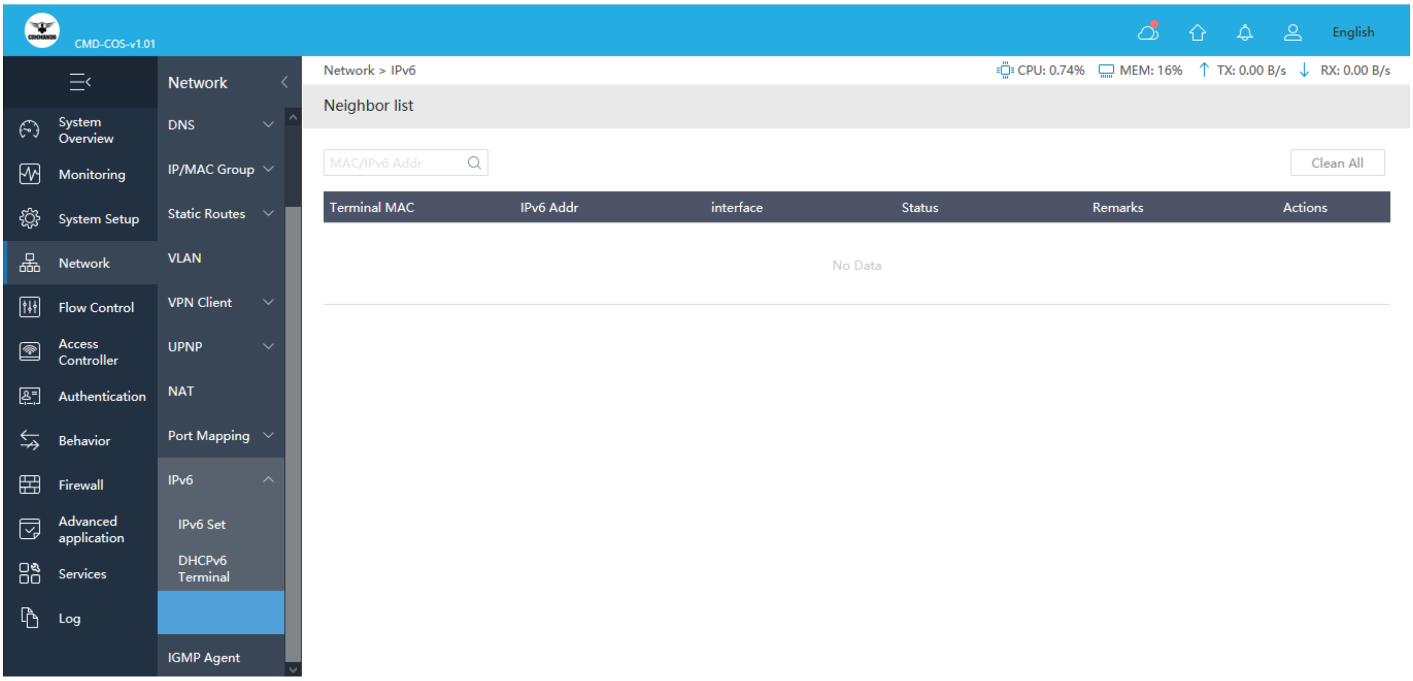
Showing 1 of 1 records

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

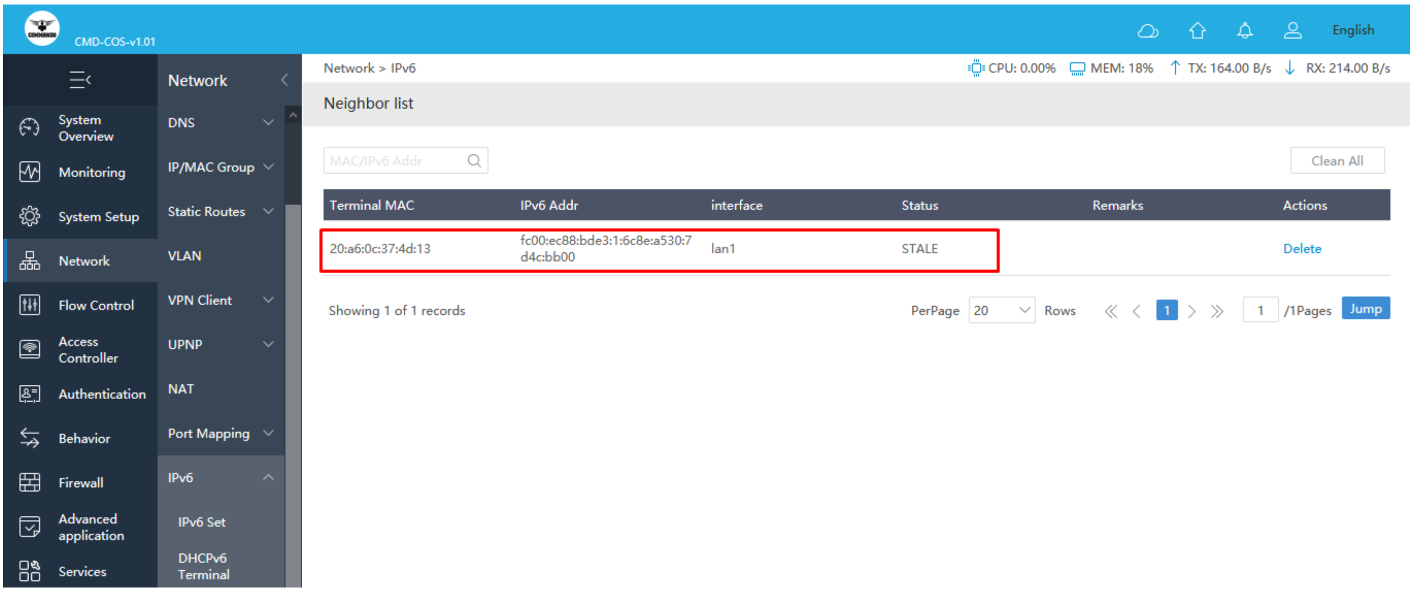


Neighbor list

Terminal MAC	IPv6 Addr	interface	Status	Remarks	Actions

No Data

Fig 3.11.10 Default IPv6 Neighbor List Page



Neighbor list

Terminal MAC	IPv6 Addr	interface	Status	Remarks	Actions
20:a6:0c:37:4d:13	fc00:ec88:bde3:1:6c8e:a530:7d4c:bb00	lan1	STALE		Delete

Showing 1 of 1 records

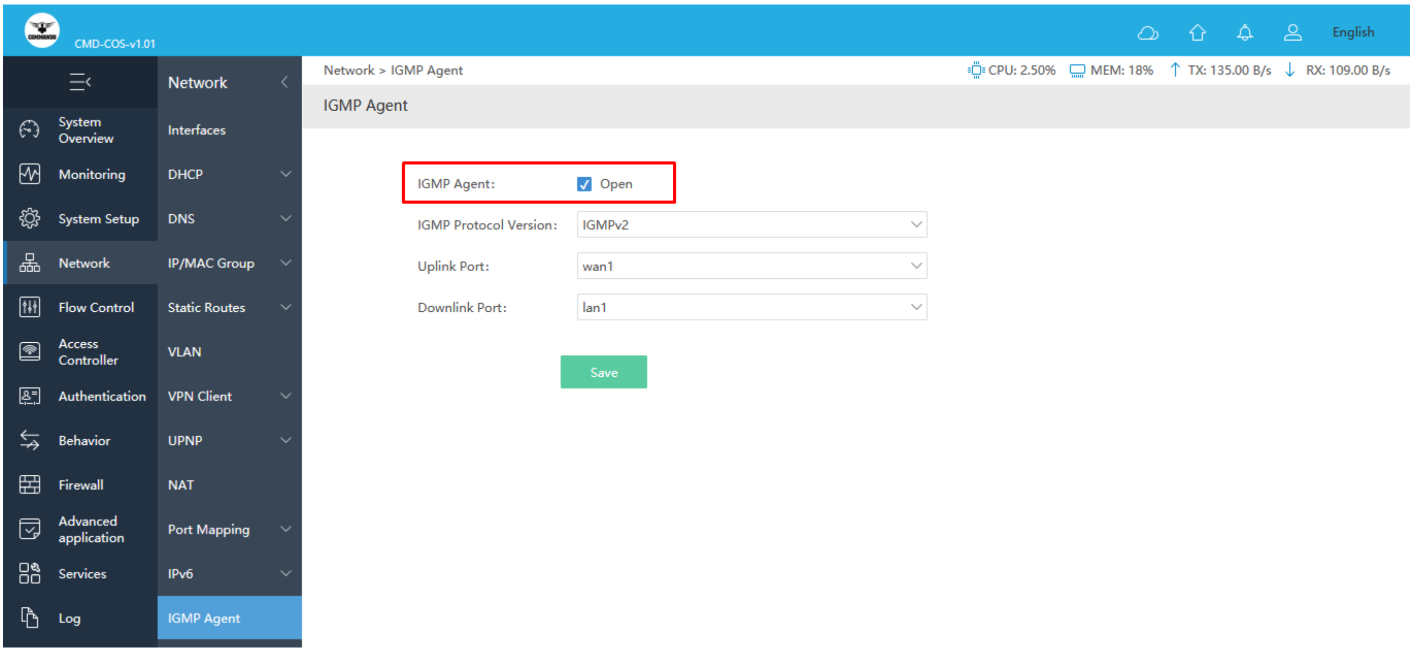
PerPage 20 Rows 1 1 /1Pages Jump

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



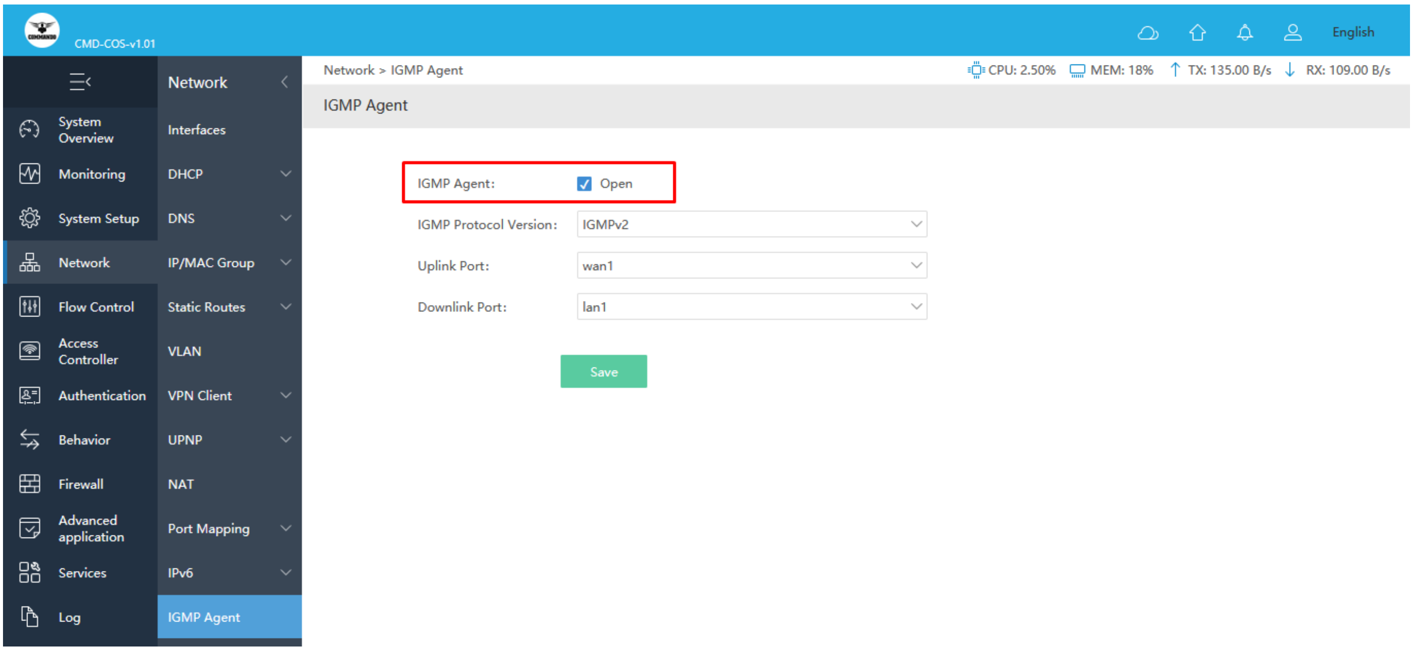
IGMP Agent: ☑ Open

IGMP Protocol Version: IGMPv2

Uplink Port: wan1

Downlink Port: lan1

Fig 3.12.1 Default IGMP Agent Page



IGMP Agent: ☑ Open

IGMP Protocol Version: IGMPv2

Uplink Port: wan1

Downlink Port: lan1

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.

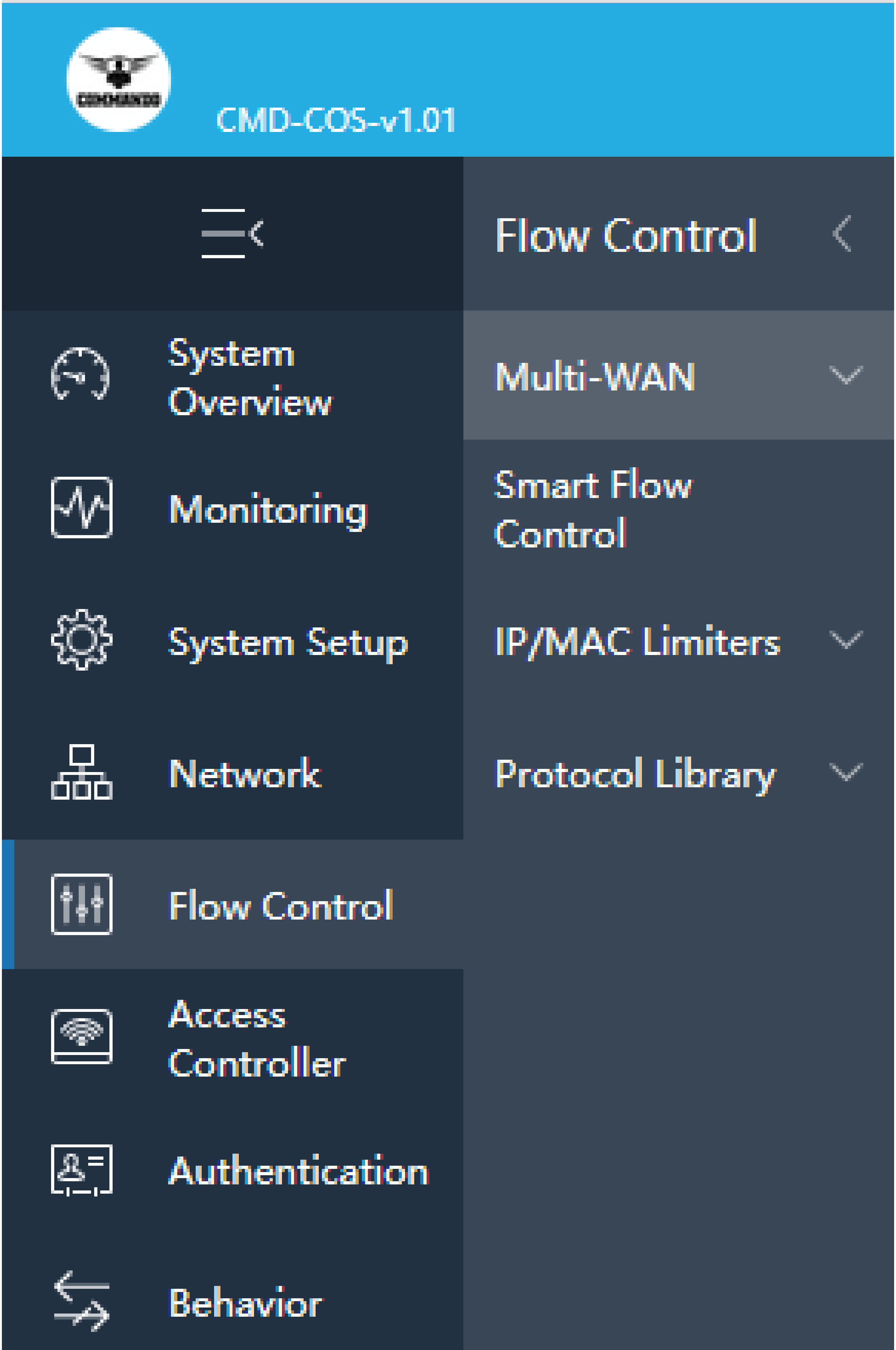

CMD-COS-v1.01
Flow Control
System Overview
Multi-WAN
Monitoring
Smart Flow Control
System Setup
IP/MAC Limiters
Network
Protocol Library
Flow Control
Access Controller
Authentication
Behavior

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.

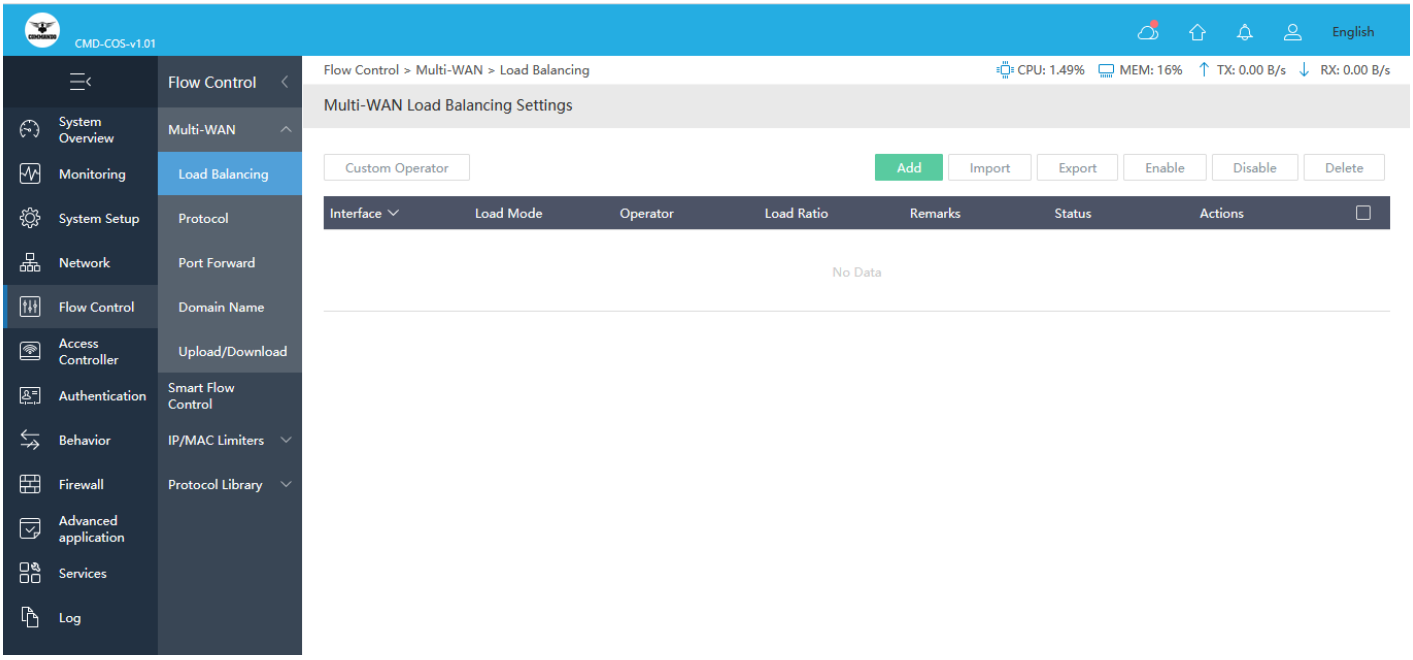
Load balancing

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



Flow Control > Multi-WAN > Load Balancing

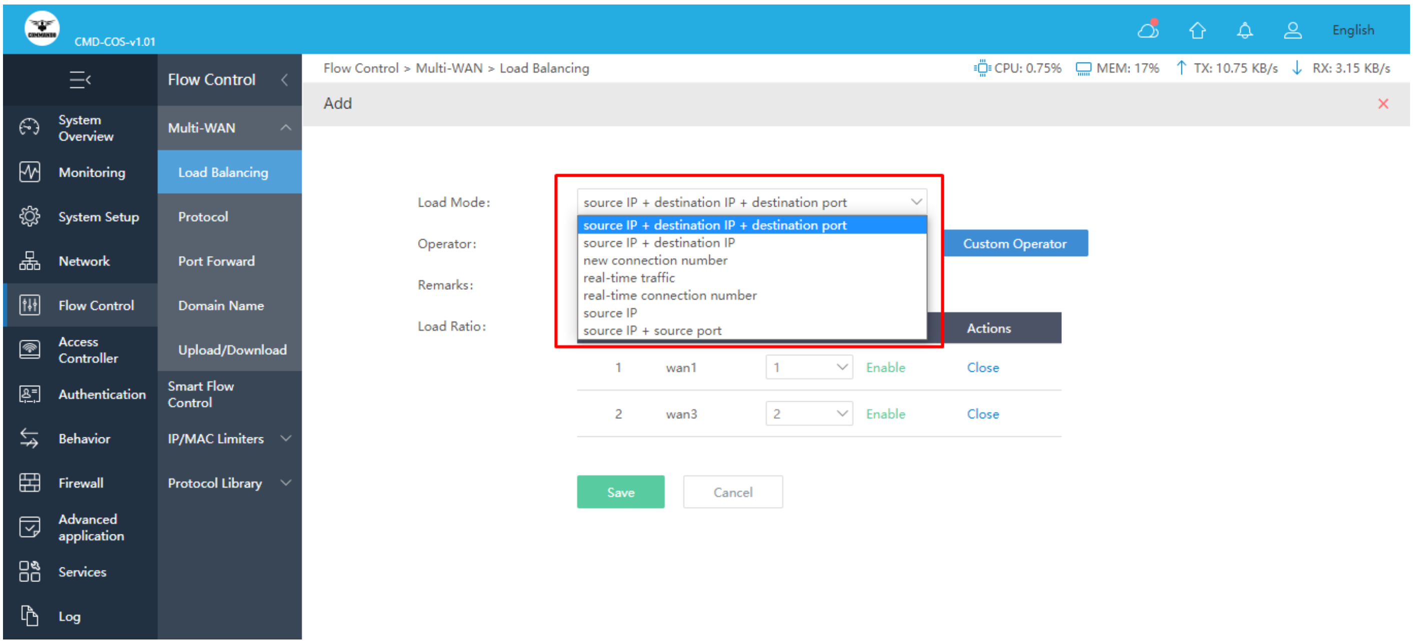
CPU: 1.49% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Multi-WAN Load Balancing Settings

Interface	Load Mode	Operator	Load Ratio	Remarks	Status	Actions	□

No Data

Fig 4.1.1 Default Multi-WAN Load Balancing Settings page



Flow Control > Multi-WAN > Load Balancing

CPU: 0.75% MEM: 17% TX: 10.75 KB/s RX: 3.15 KB/s

Add

Load Mode: source IP + destination IP + destination port

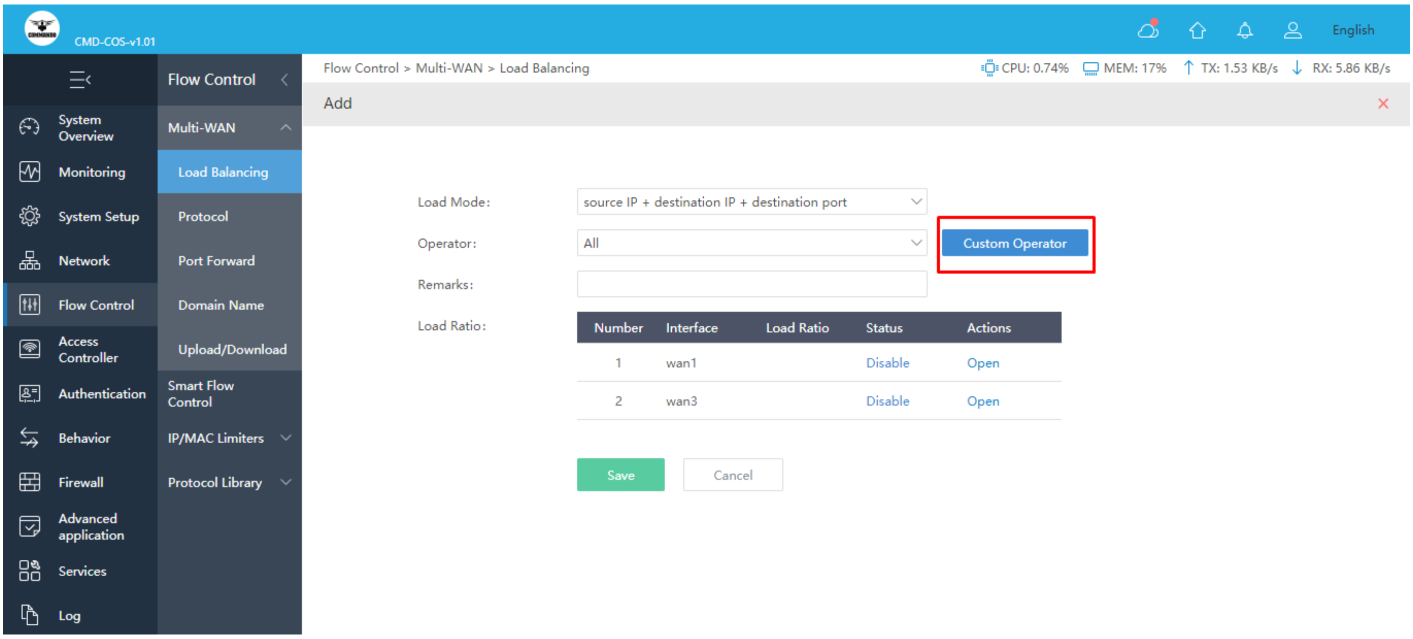
- source IP + destination IP + destination port
- source IP + destination IP
- new connection number
- real-time traffic
- real-time connection number
- source IP
- source IP + source port

Operator:

Remarks:

Load Ratio:

				Actions
1	wan1	1	Enable	Close
2	wan3	2	Enable	Close



Flow Control > Multi-WAN > Load Balancing

CPU: 0.74% MEM: 17% TX: 1.53 KB/s RX: 5.86 KB/s

Add

Load Mode: source IP + destination IP + destination port

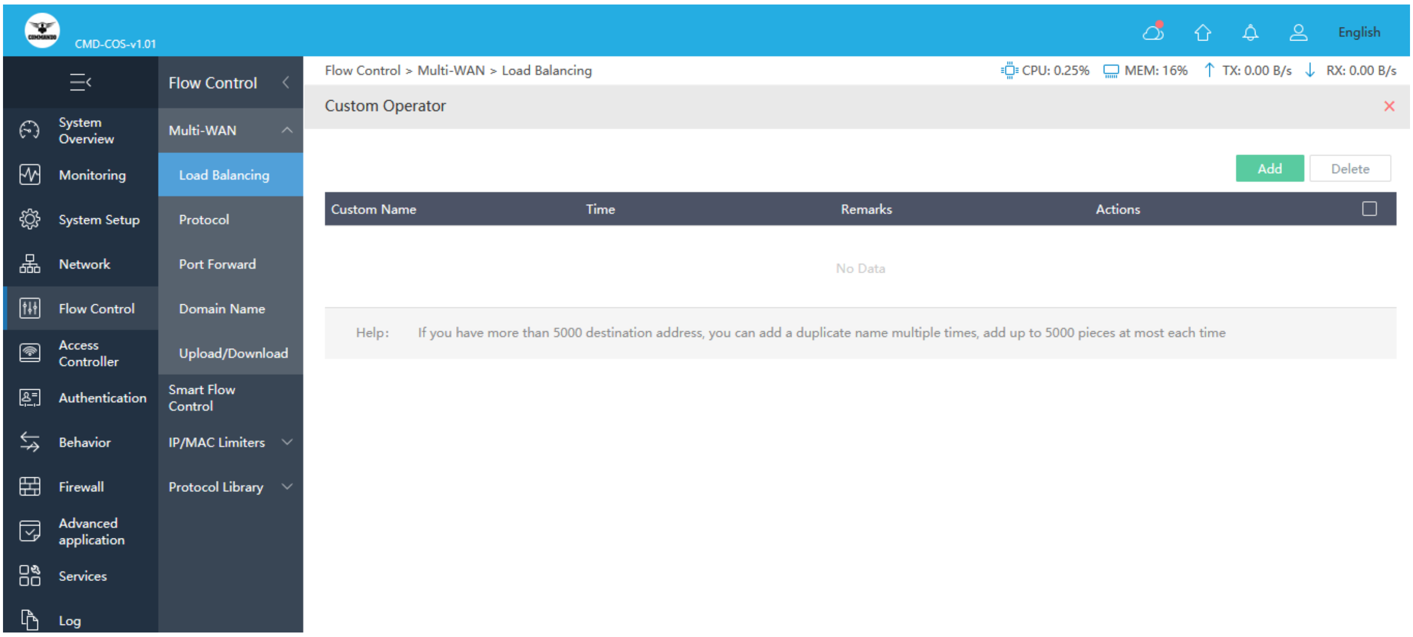
Operator: All

Remarks:

Load Ratio:

Number	Interface	Load Ratio	Status	Actions
1	wan1		Disable	Open
2	wan3		Disable	Open

Fig 4.1.2 Add Multi-WAN Load Balancing Settings page



Flow Control > Multi-WAN > Load Balancing

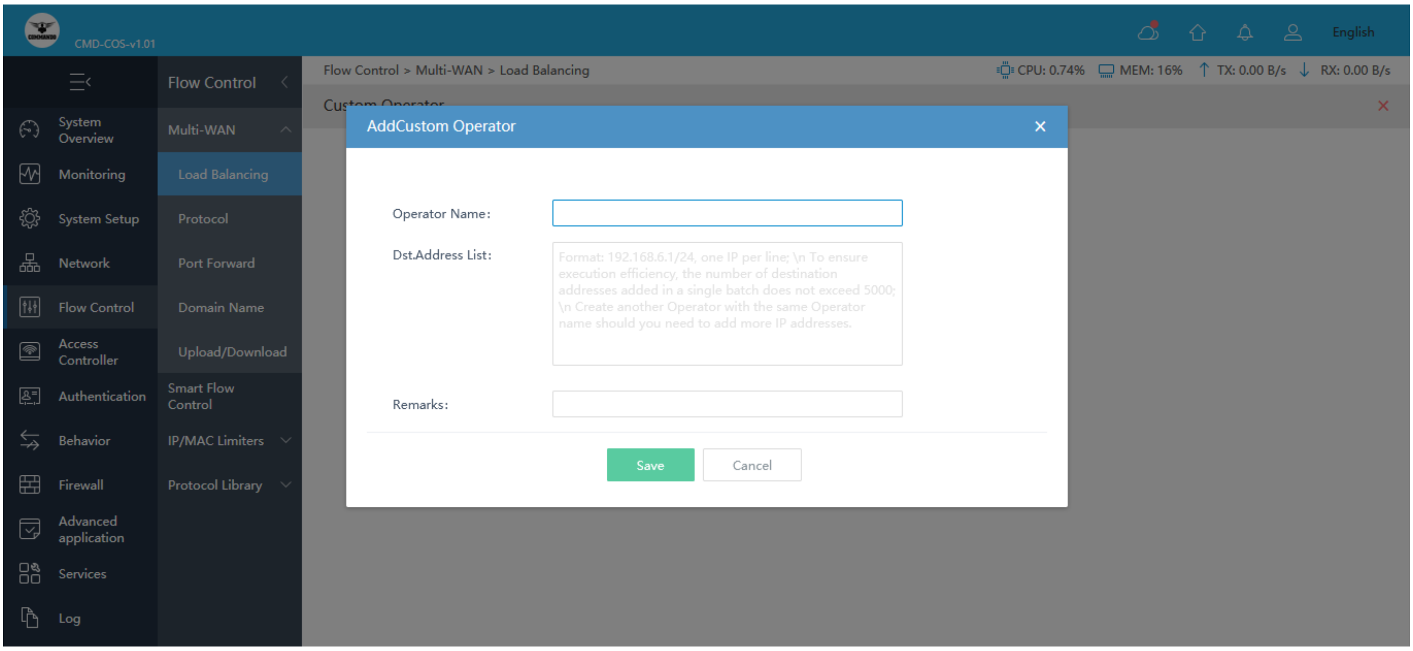
CPU: 0.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Custom Operator

Custom Name	Time	Remarks	Actions	□
		No Data		

Help: If you have more than 5000 destination address, you can add a duplicate name multiple times, add up to 5000 pieces at most each time

Fig 4.1.3 Default Custom operator page

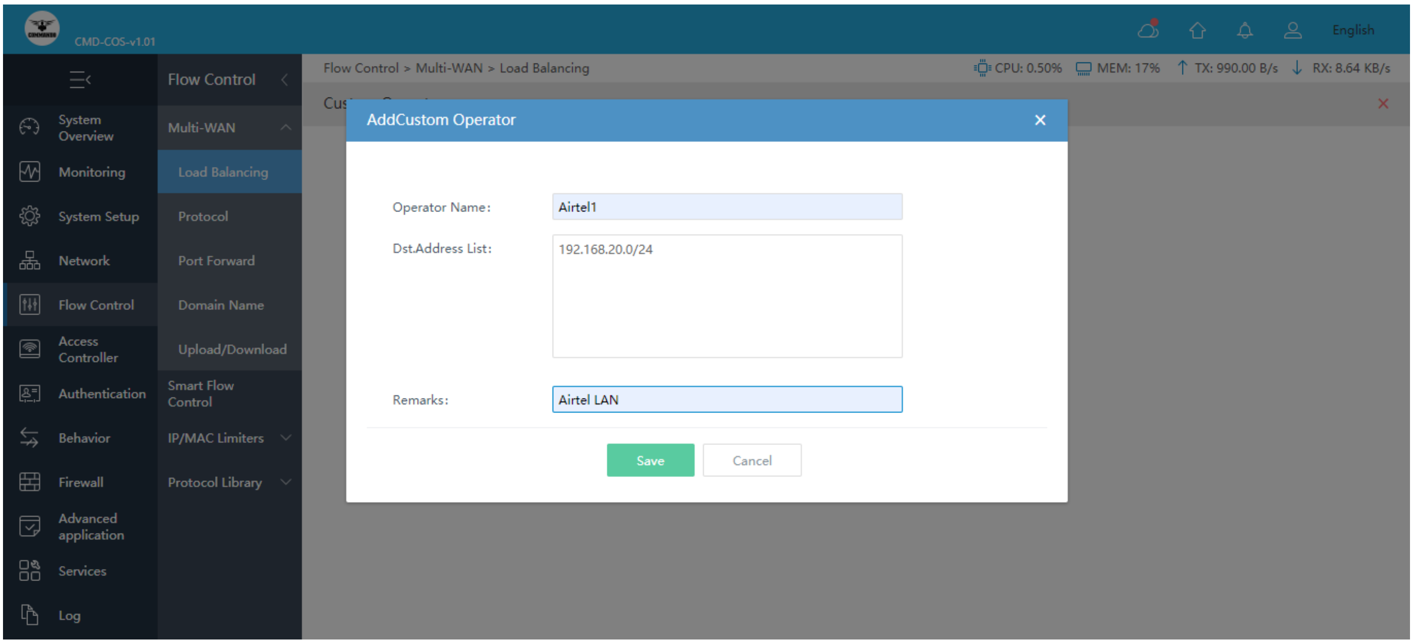


Operator Name:

Dst.Address List: Format: 192.168.6.1/24, one IP per line; \n To ensure execution efficiency, the number of destination addresses added in a single batch does not exceed 5000; \n Create another Operator with the same Operator name should you need to add more IP addresses.

Remarks:

Fig 4.1.4 Add Custom operator page

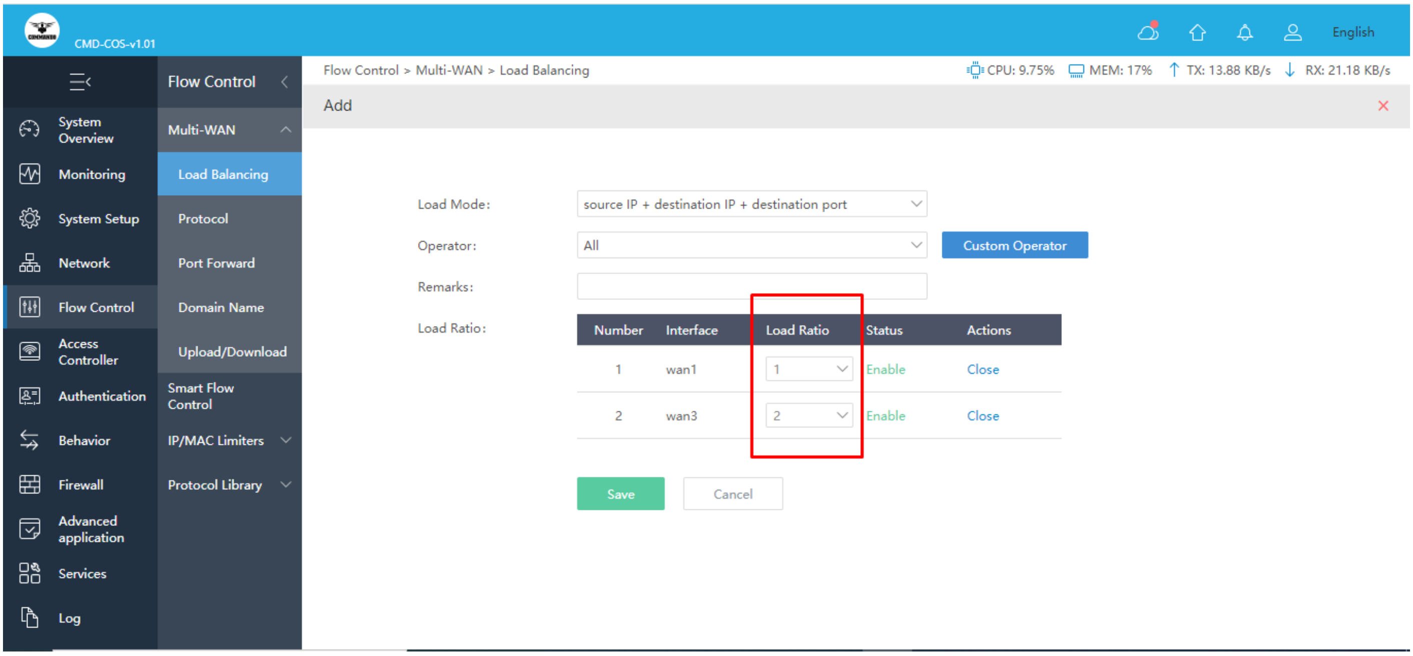


Operator Name: Airtel1

Dst.Address List: 192.168.20.0/24

Remarks: Airtel LAN

Fig 4.1.5 Setting Custom operator page



Flow Control > Multi-WAN > Load Balancing   CPU: 9.75% MEM: 17% TX: 13.88 KB/s RX: 21.18 KB/s

Add

Load Mode: source IP + destination IP + destination port

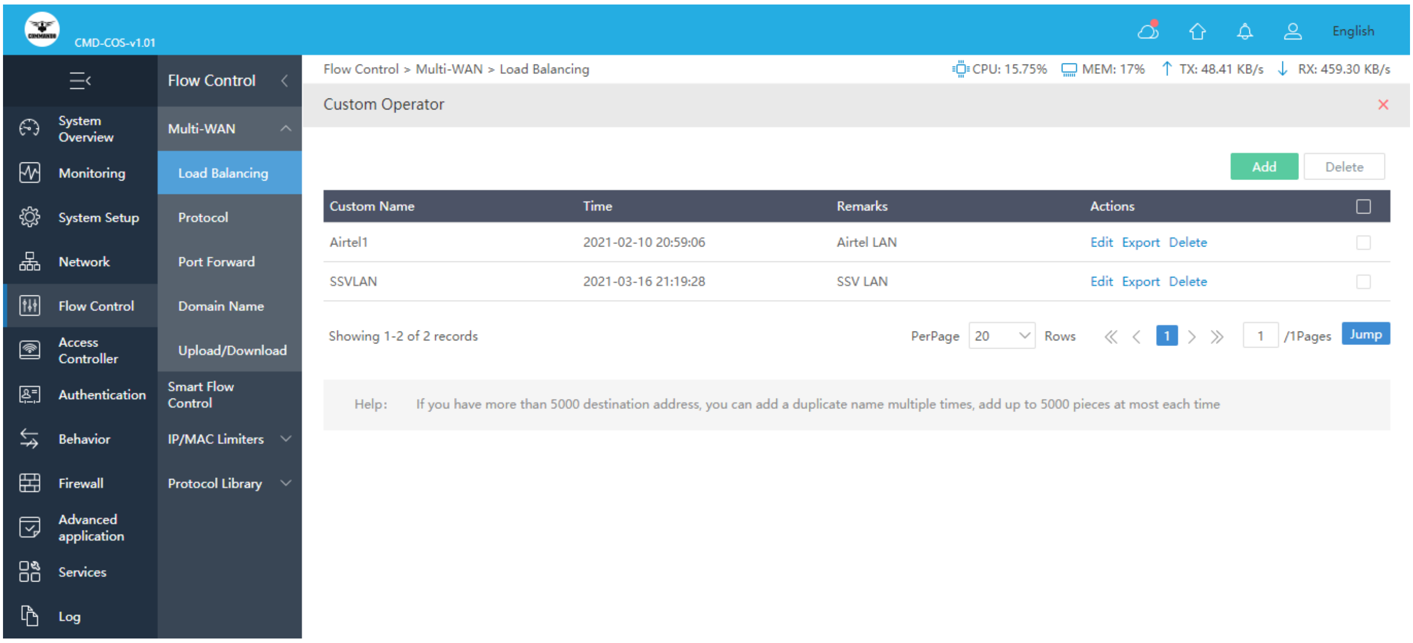
Operator: All

Remarks:

Load Ratio:

Number	Interface	Load Ratio	Status	Actions
1	wan1	1	Enable	Close
2	wan3	2	Enable	Close

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



Flow Control > Multi-WAN > Load Balancing   CPU: 15.75% MEM: 17% TX: 48.41 KB/s RX: 459.30 KB/s

Custom Operator

Custom Name	Time	Remarks	Actions	□
Airtel1	2021-02-10 20:59:06	Airtel LAN	Edit Export Delete	□
SSVLAN	2021-03-16 21:19:28	SSV LAN	Edit Export Delete	□

Showing 1-2 of 2 records   PerPage 20 Rows   1   1 /1Pages

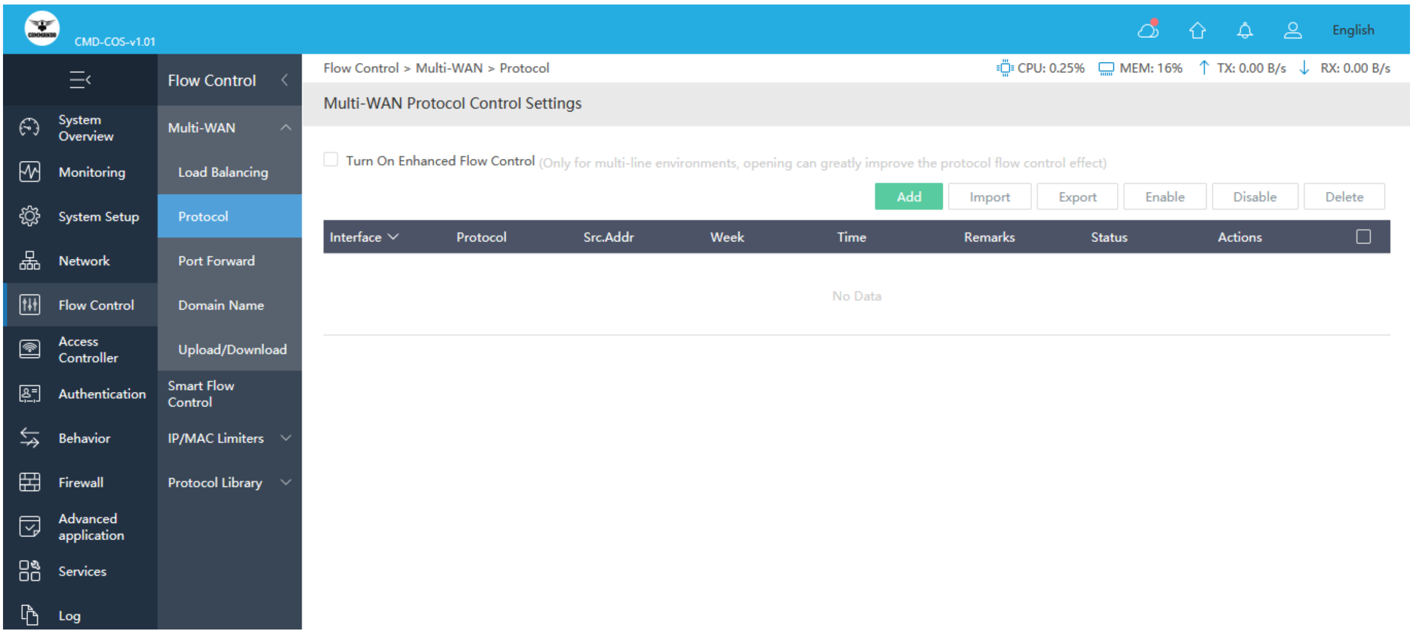
Help: If you have more than 5000 destination address, you can add a duplicate name multiple times, add up to 5000 pieces at most each time

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



Flow Control > Multi-WAN > Protocol

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

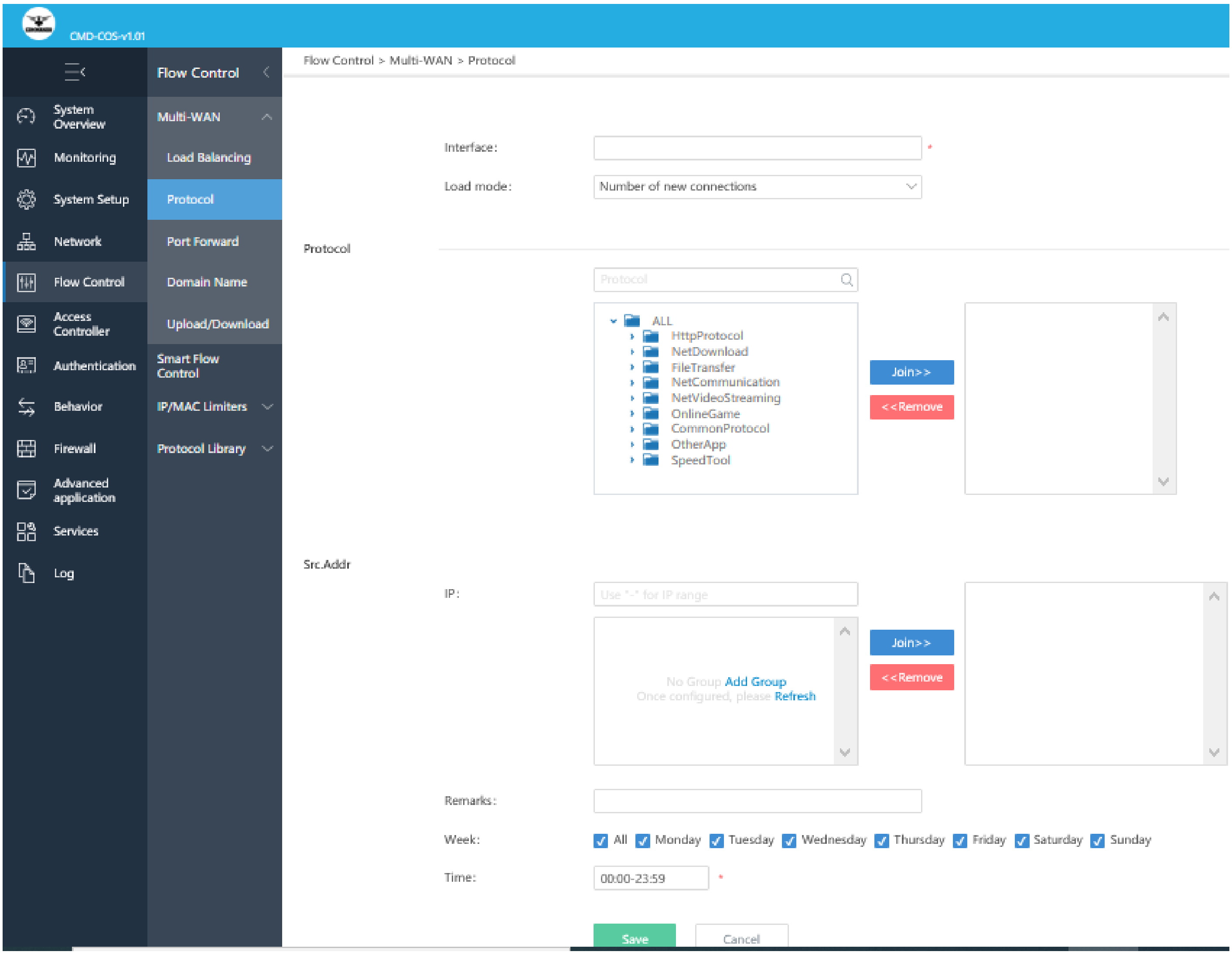
Multi-WAN Protocol Control Settings

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

Interface	Protocol	Src.Addr	Week	Time	Remarks	Status	Actions	□

No Data

Fig 4.1.8 Default Multi-WAN Protocol Control Settings page



Flow Control > Multi-WAN > Protocol

Interface: *

Load mode: Number of new connections

Protocol

Protocol

Src.Addr

IP: Use "-" for IP range

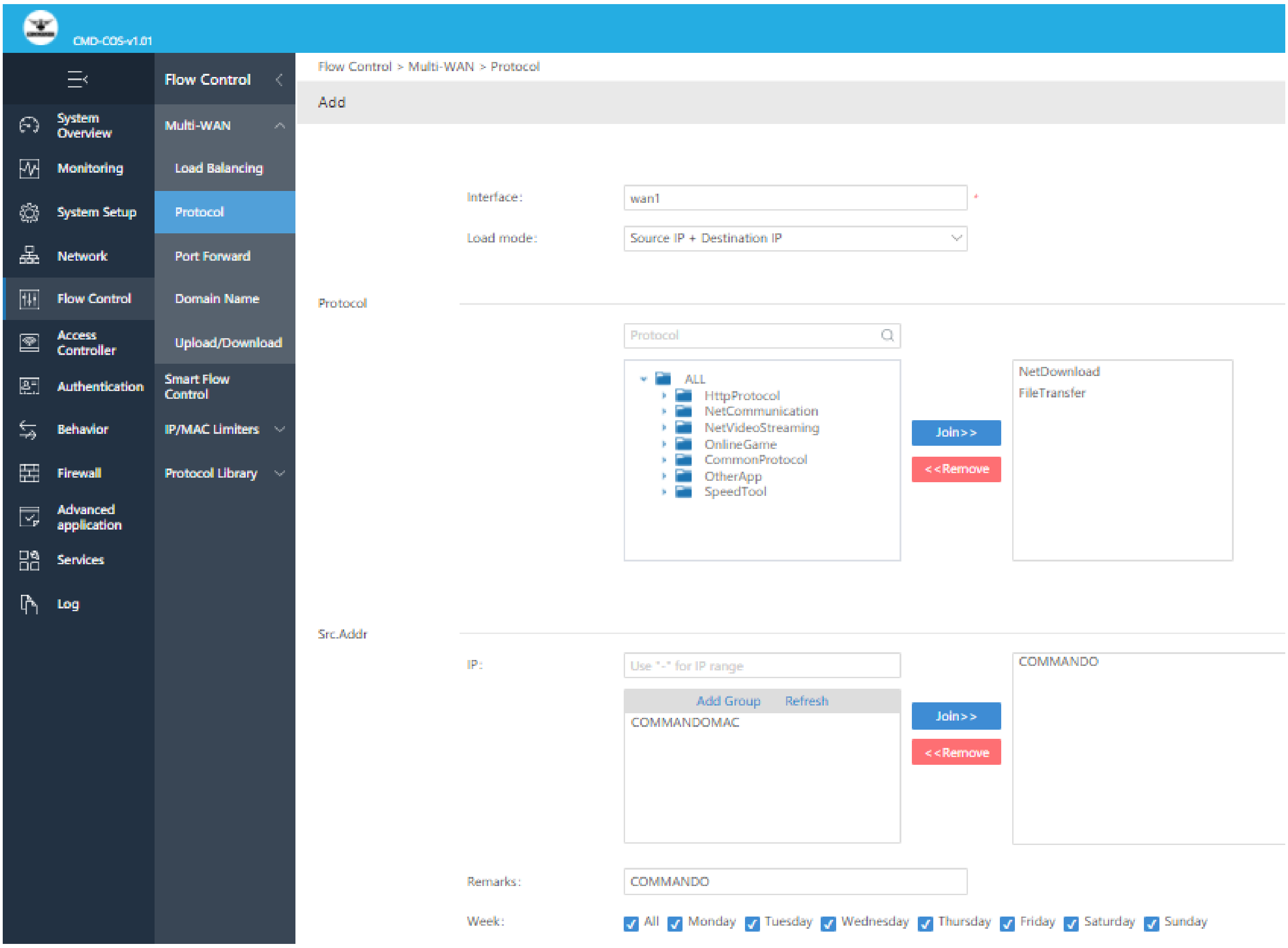
No Group Add Group
Once configured, please Refresh

Remarks:

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

Time: 00:00-23:59 *

Fig 4.1.9 Add Multi-WAN Protocol Control Settings page



Interface: wan1 *

Load mode: Source IP + Destination IP

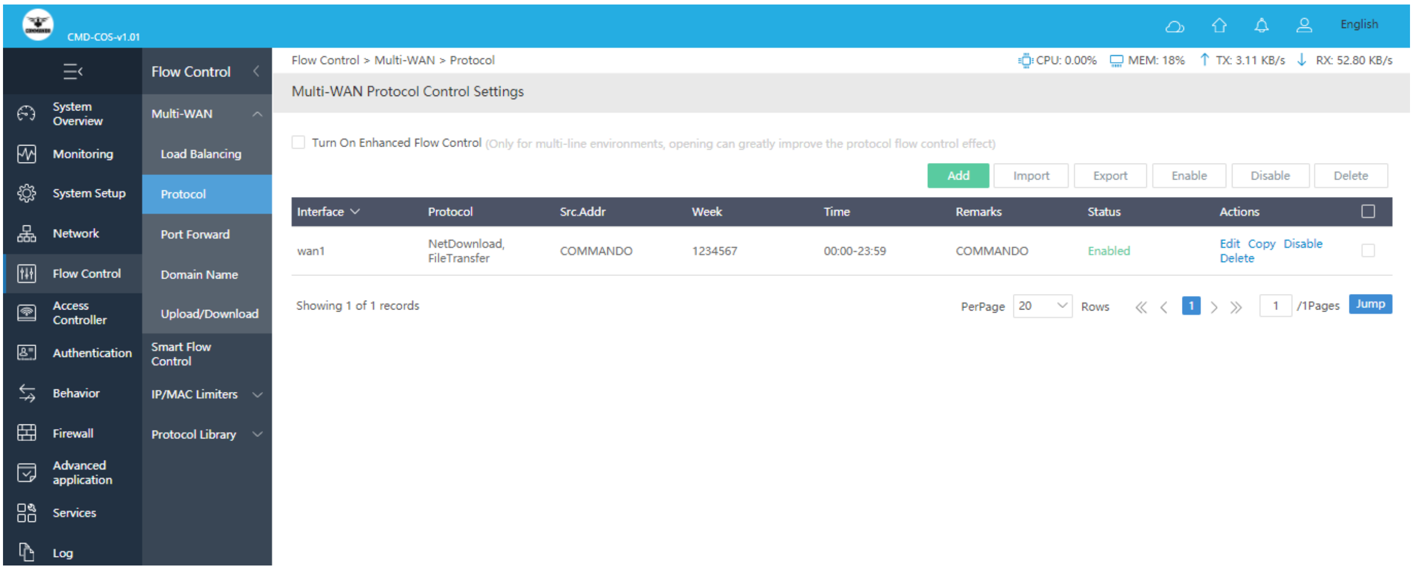
Protocol: NetDownload, FileTransfer

IP: COMMANDO

Remarks: COMMANDO

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

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



CPU: 0.00% MEM: 18% TX: 3.11 KB/s RX: 52.80 KB/s

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

Interface	Protocol	Src.Addr	Week	Time	Remarks	Status	Actions	□
wan1	NetDownload, FileTransfer	COMMANDO	1234567	00:00-23:59	COMMANDO	Enabled	Edit Copy Disable Delete	□

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

Fig 4.1.11 Multi-WAN Protocol Control Settings page

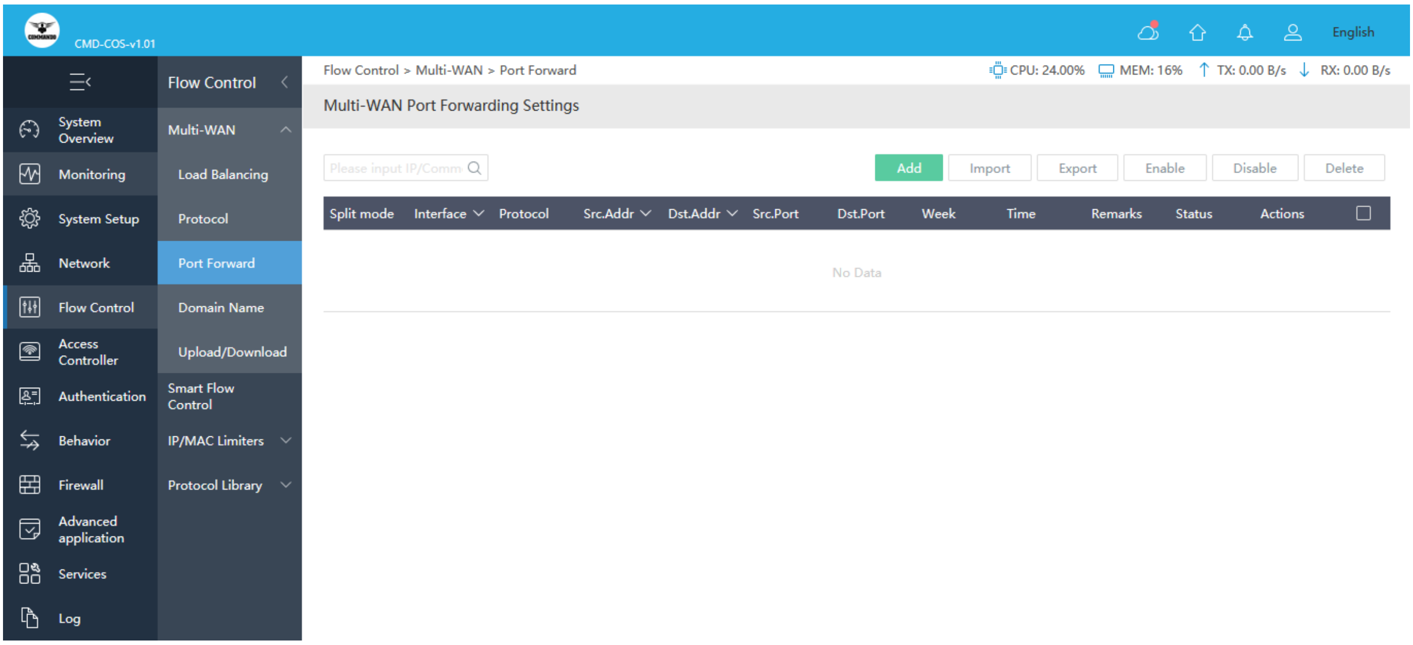
Multi-WAN Port Forwarding Settings:

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



Flow Control > Multi-WAN > Port Forward

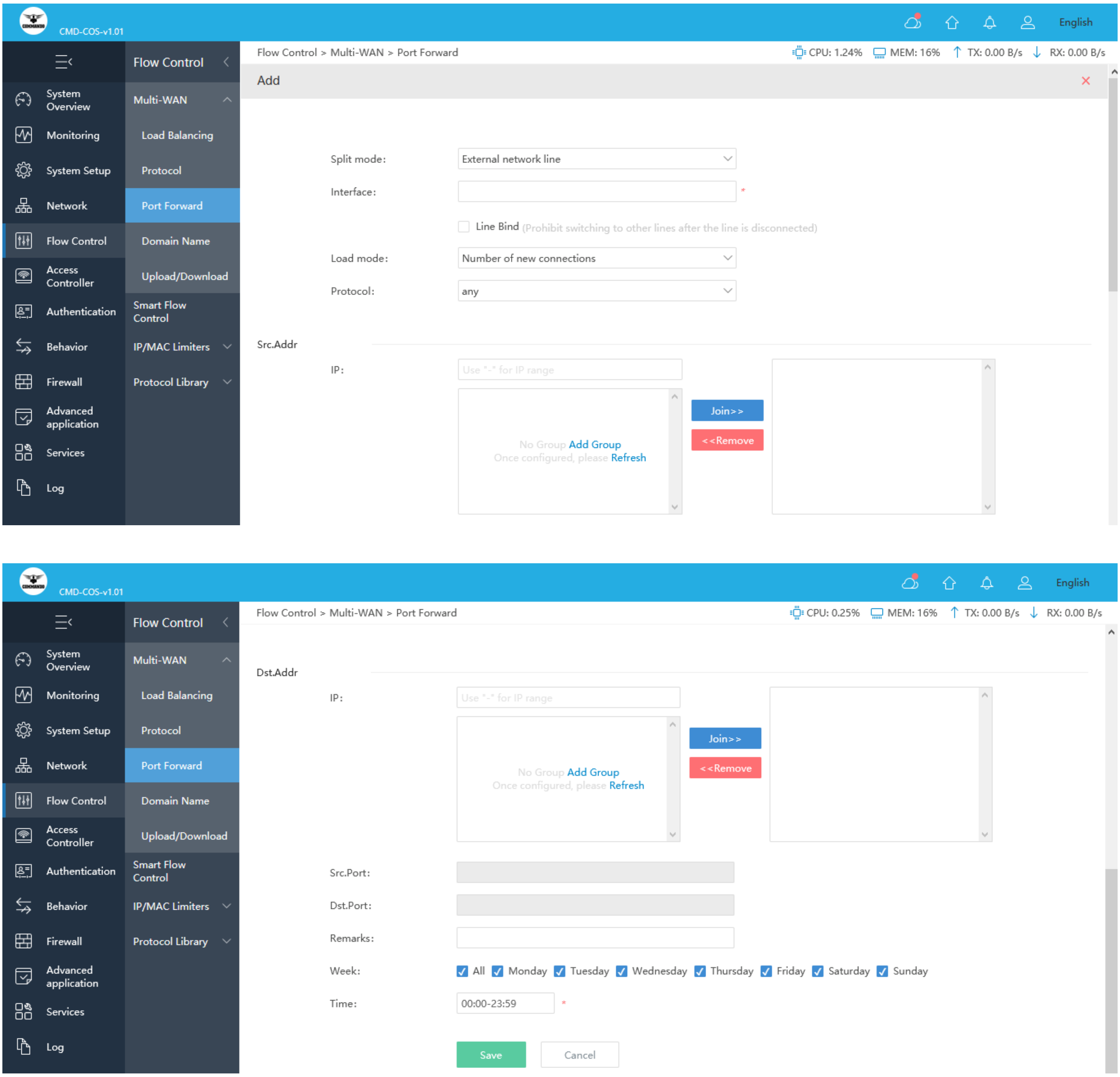
CPU: 24.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Multi-WAN Port Forwarding Settings

Split mode	Interface	Protocol	Src.Addr	Dst.Addr	Src.Port	Dst.Port	Week	Time	Remarks	Status	Actions	□

No Data

Fig 4.1.12 Default Multi-WAN Port Forwarding Settings page



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

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:

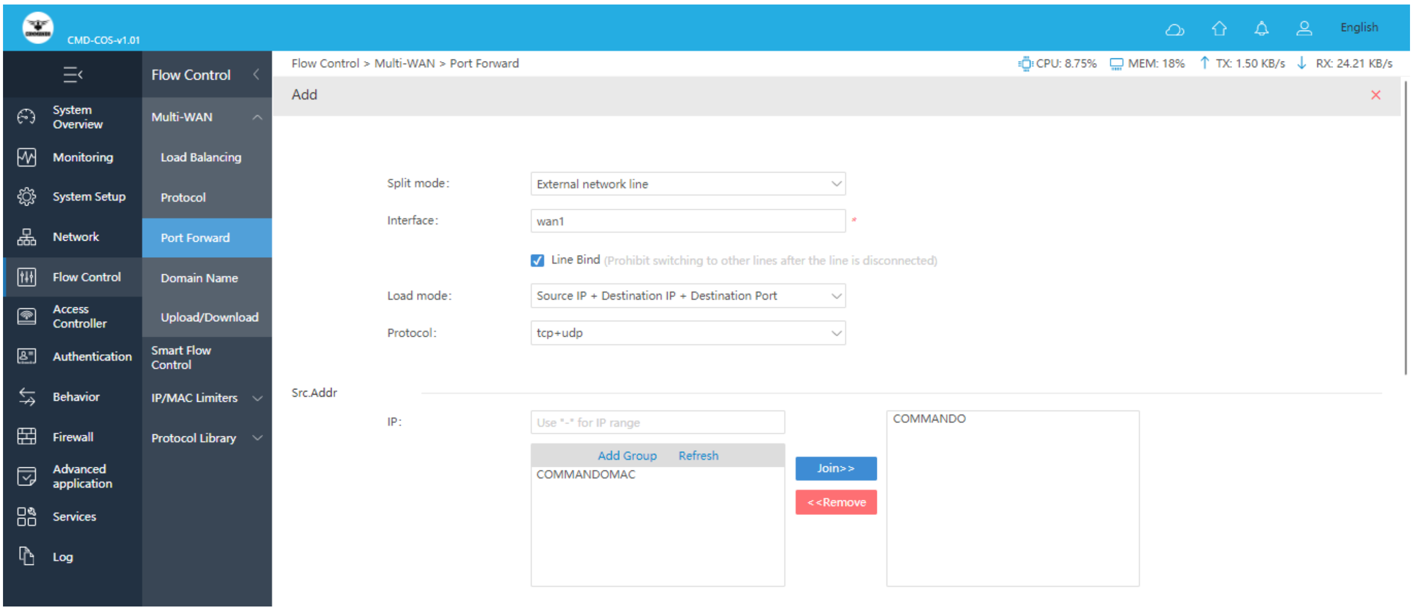
Remarks:

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



Flow Control > Multi-WAN > Port Forward

Add

Split mode: External network line

Interface: wan1 *

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

Load mode: Source IP + Destination IP + Destination Port

Protocol: tcp+udp

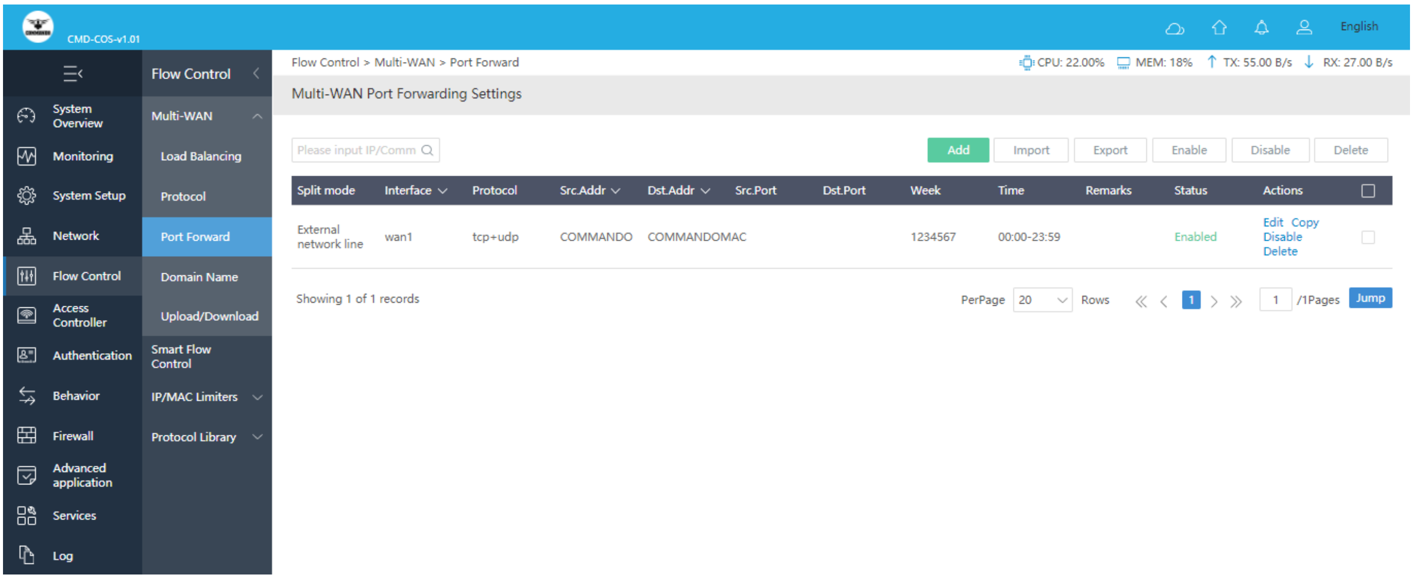
Src.Addr

IP: Use "-" for IP range

COMMANDOMAC

COMMANDO

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



Flow Control > Multi-WAN > Port Forward

Multi-WAN Port Forwarding Settings

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

Showing 1 of 1 records

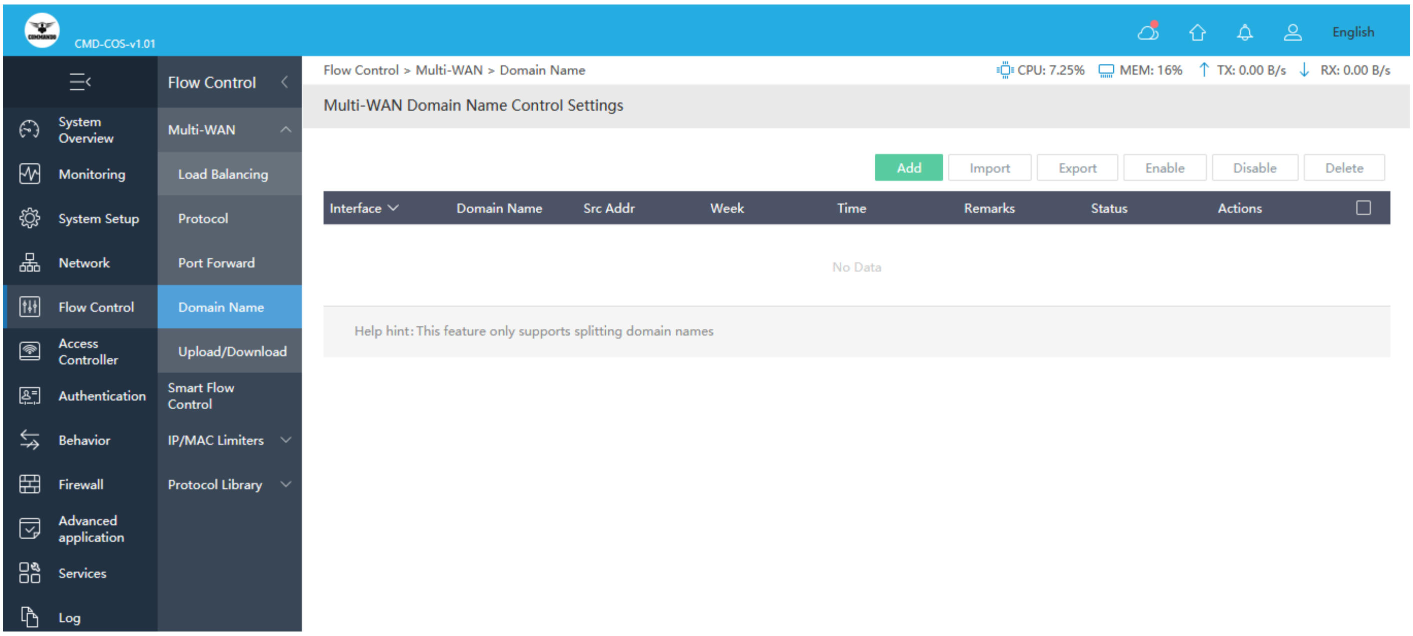
PerPage 20 Rows 1 1 /1Pages

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



Flow Control > Multi-WAN > Domain Name

CPU: 7.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

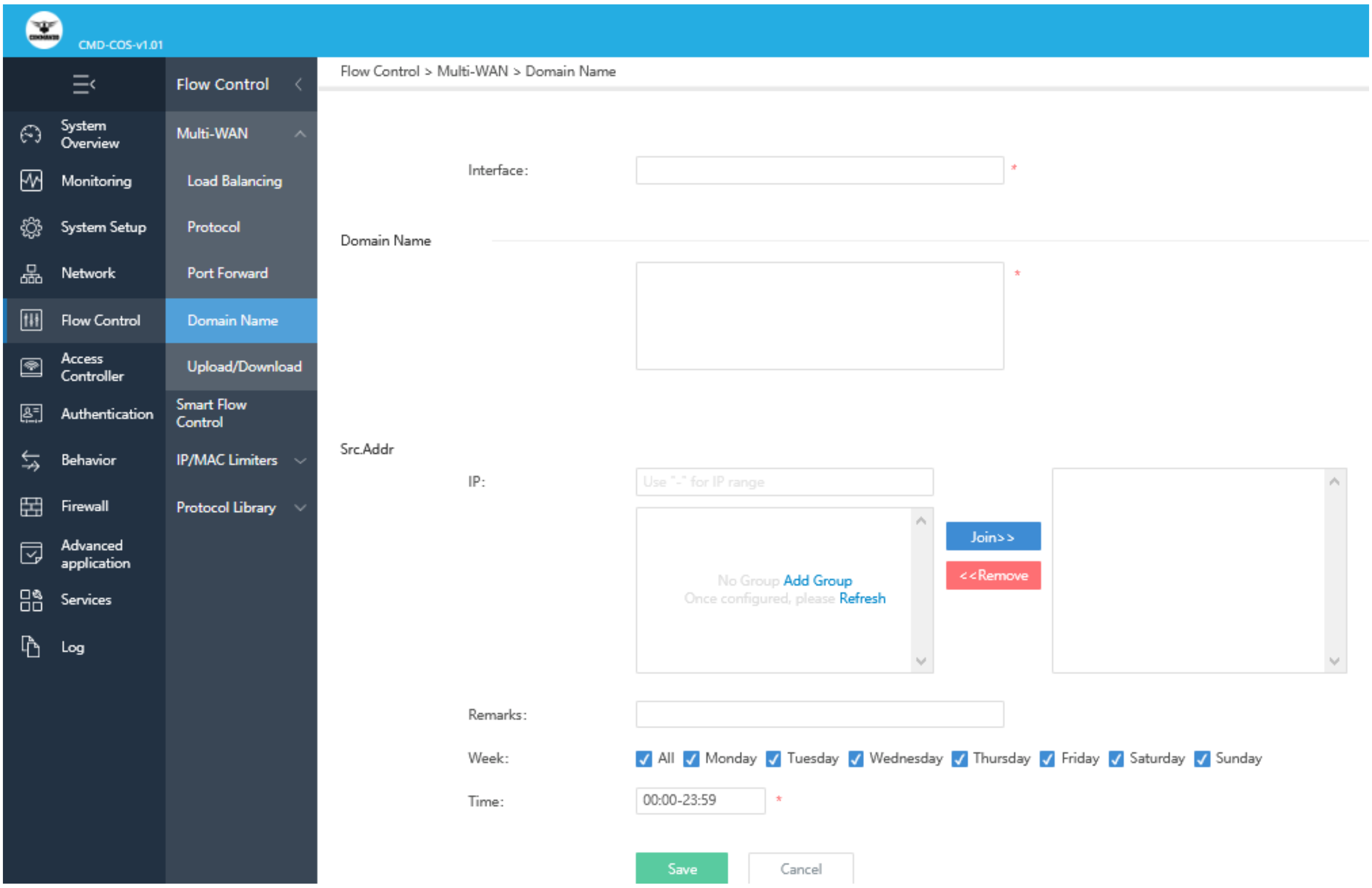
Multi-WAN Domain Name Control Settings

Interface	Domain Name	Src Addr	Week	Time	Remarks	Status	Actions	□

No Data

Help hint: This feature only supports splitting domain names

Fig 4.1.16 Default Multi-WAN Domain Name Control Settings page



Flow Control > Multi-WAN > Domain Name

Interface: *

Domain Name *

Src.Addr

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Join>>
<<Remove

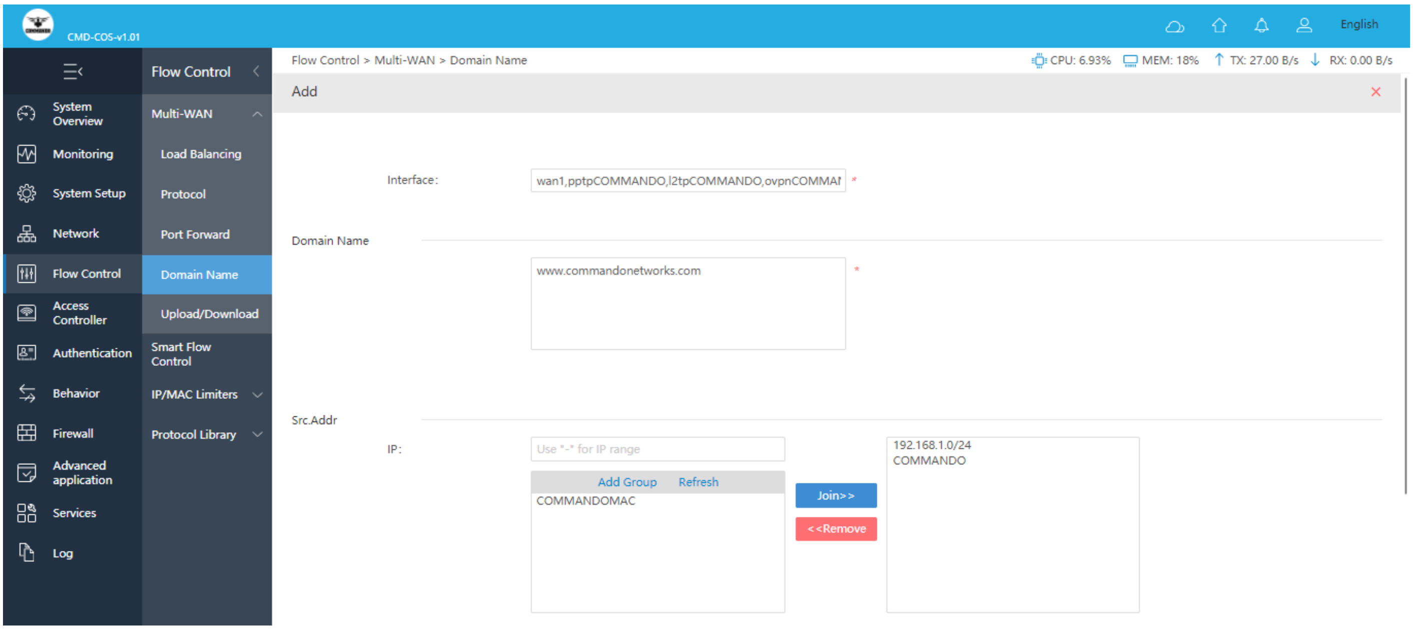
Remarks:

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

Time: 00:00-23:59 *

Save Cancel

Fig 4.1.17 Add Multi-WAN Domain Name Control Settings page



Flow Control > Multi-WAN > Domain Name

CPU: 6.93% MEM: 18% TX: 27.00 B/s RX: 0.00 B/s

Add

Interface: wan1,pptpCOMMANDO,l2tpCOMMANDO,ovpnCOMMAI *

Domain Name www.commandonetworks.com *

Src.Addr

IP: Use "-" for IP range

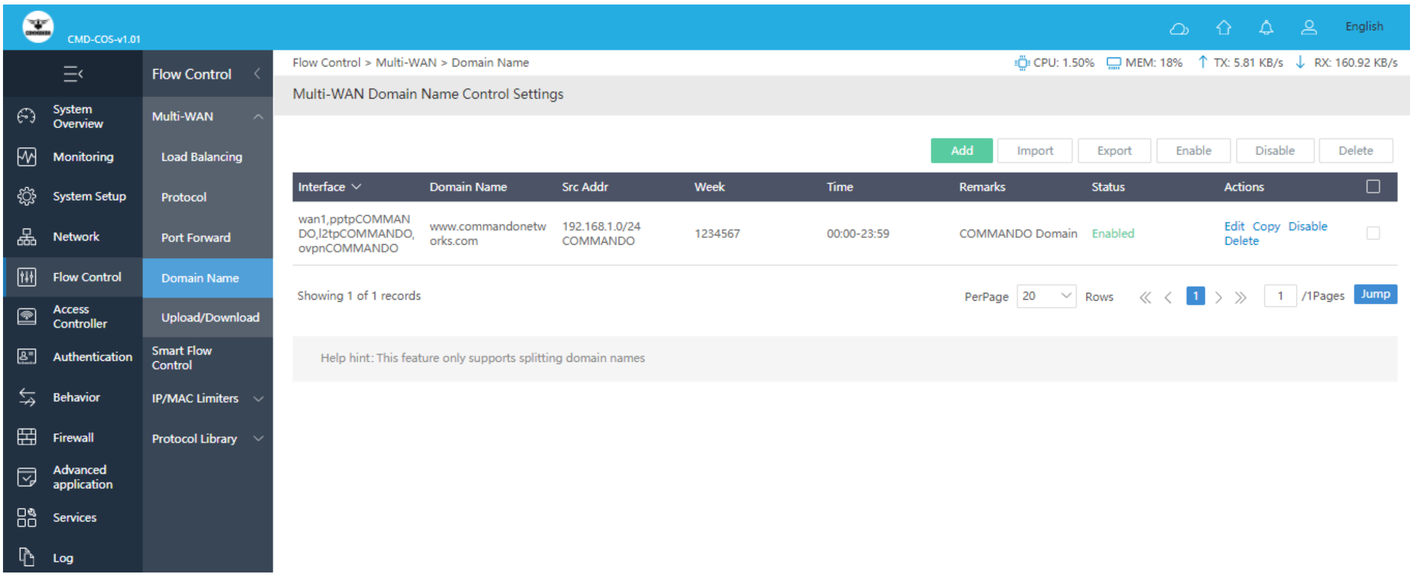
Add Group Refresh

COMMANDOMAC

Join>>
<<Remove

192.168.1.0/24
COMMANDO

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



Flow Control > Multi-WAN > Domain Name

CPU: 1.50% MEM: 18% TX: 5.81 KB/s RX: 160.92 KB/s

Multi-WAN Domain Name Control Settings

Interface	Domain Name	Src Addr	Week	Time	Remarks	Status	Actions	□
wan1,pptpCOMMANDO,l2tpCOMMANDO,ovpnCOMMANDO	www.commandonetworks.com	192.168.1.0/24 COMMANDO	1234567	00:00-23:59	COMMANDO Domain	Enabled	Edit Copy Disable Delete	□

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

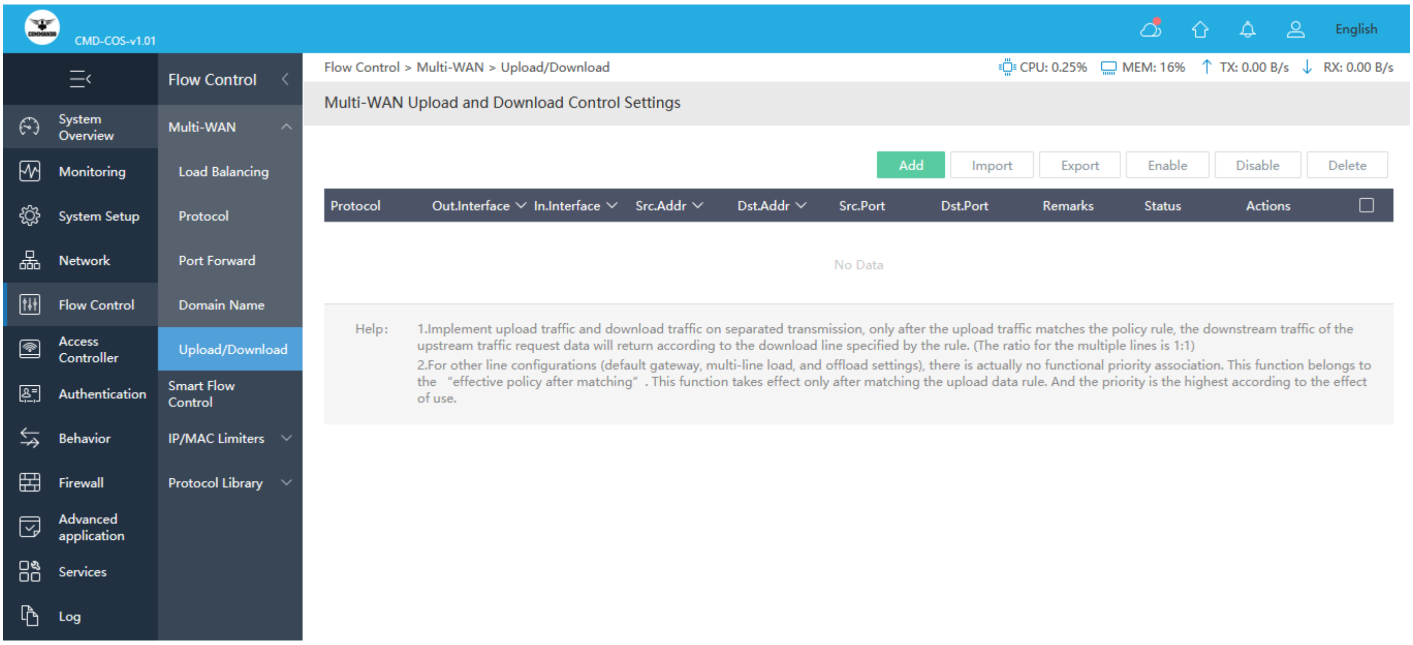
Help hint: This feature only supports splitting domain names

Fig 4.1.19 Multi-WAN Domain Name Control Settings pagestrong>

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



Flow Control > Multi-WAN > Upload/Download

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

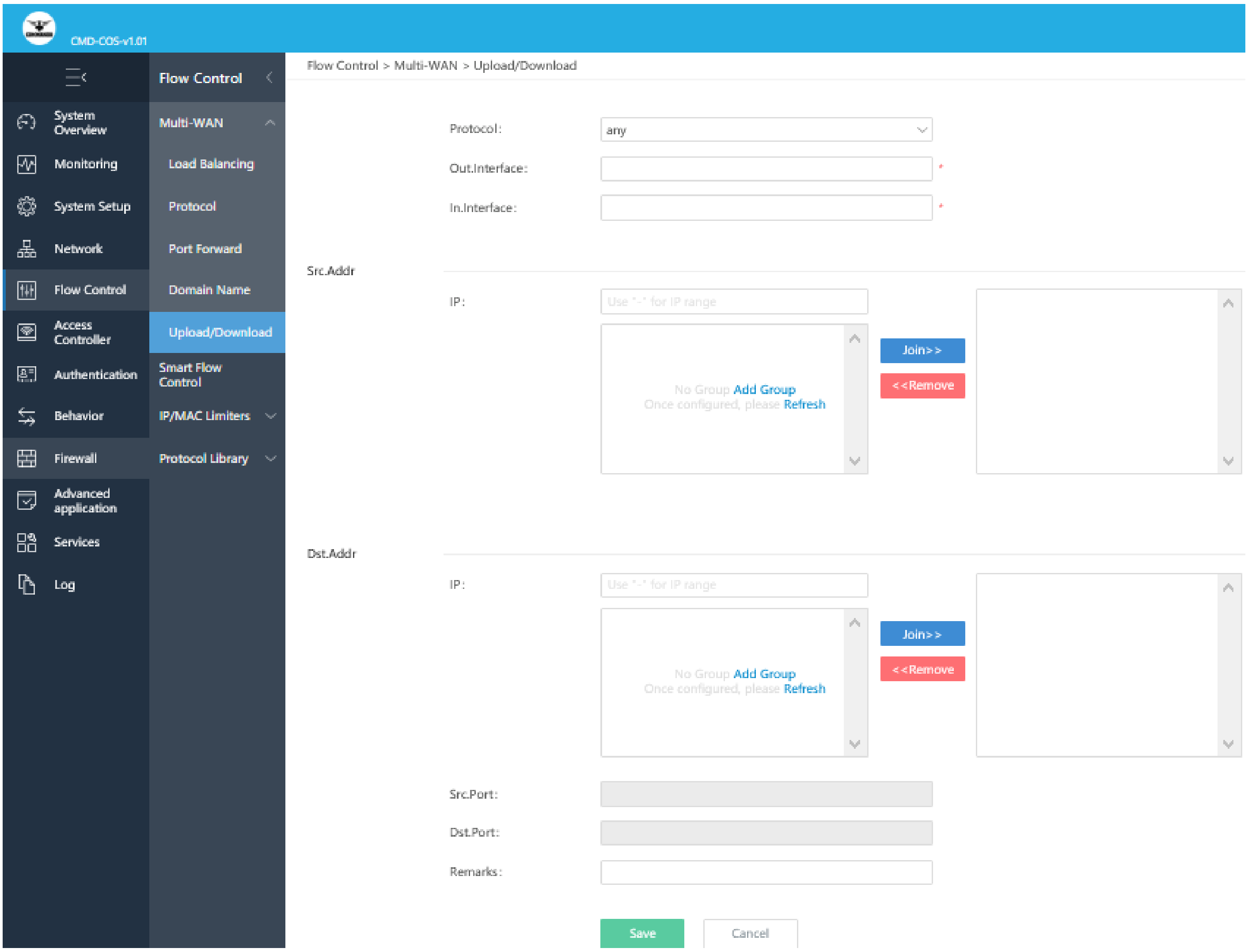
Multi-WAN Upload and Download Control Settings

Protocol	Out.Interface	In.Interface	Src.Addr	Dst.Addr	Src.Port	Dst.Port	Remarks	Status	Actions	□

No Data

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

Fig 4.1.20 Multi-WAN Upload and Download Control Settings page



Flow Control > Multi-WAN > Upload/Download

Protocol: any

Out.Interface: *

In.Interface: *

Src.Addr

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Dst.Addr

IP: Use "-" for IP range

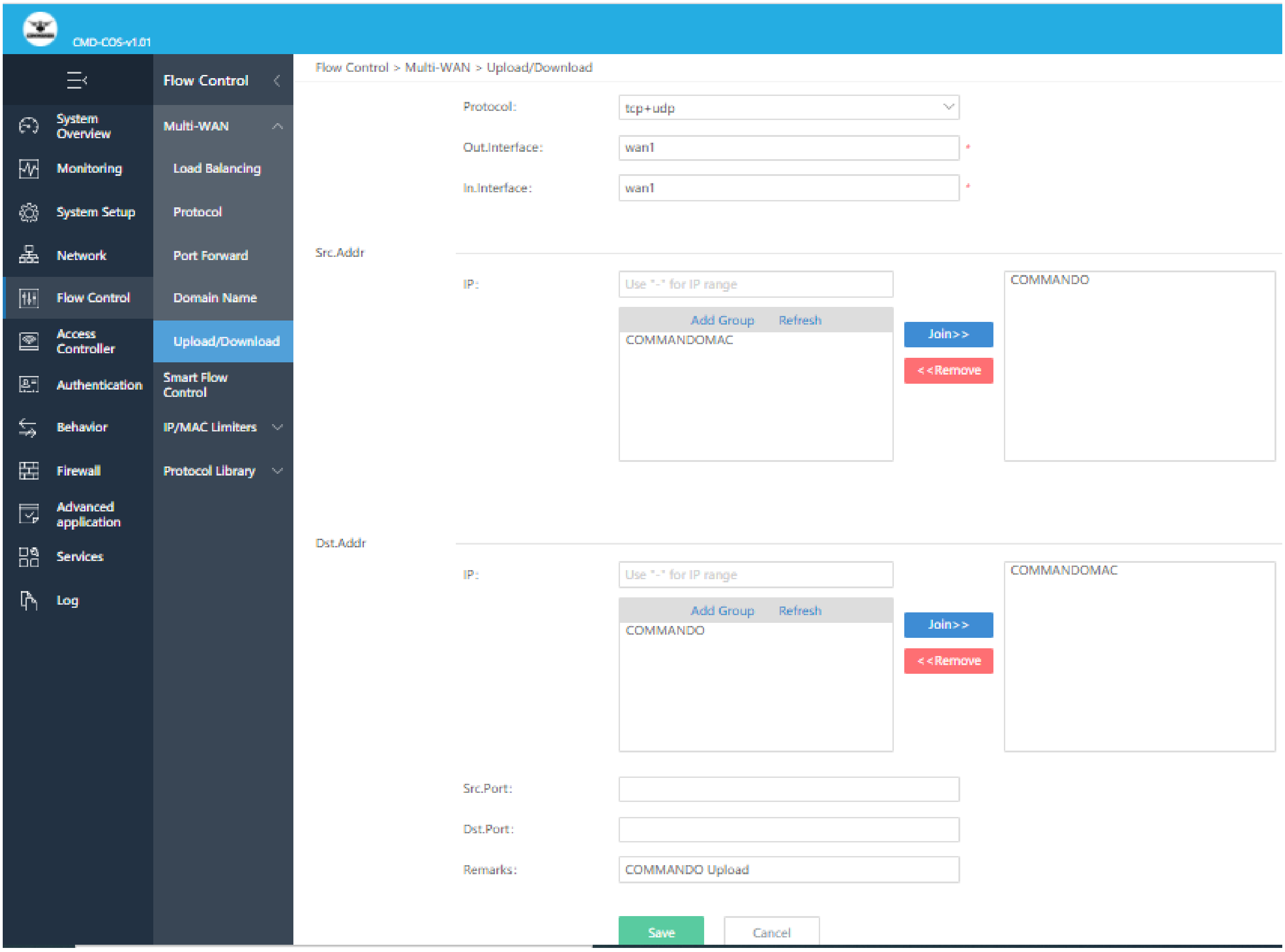
No Group Add Group
Once configured, please Refresh

Src.Port:

Dst.Port:

Remarks:

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



Flow Control > Multi-WAN > Upload/Download

Protocol: tcp+udp

Out.Interface: wan1 *

In.Interface: wan1 *

Src.Addr

IP: Use "-" for IP range

COMMANDOMAC

COMMANDO

Dst.Addr

IP: Use "-" for IP range

COMMANDO

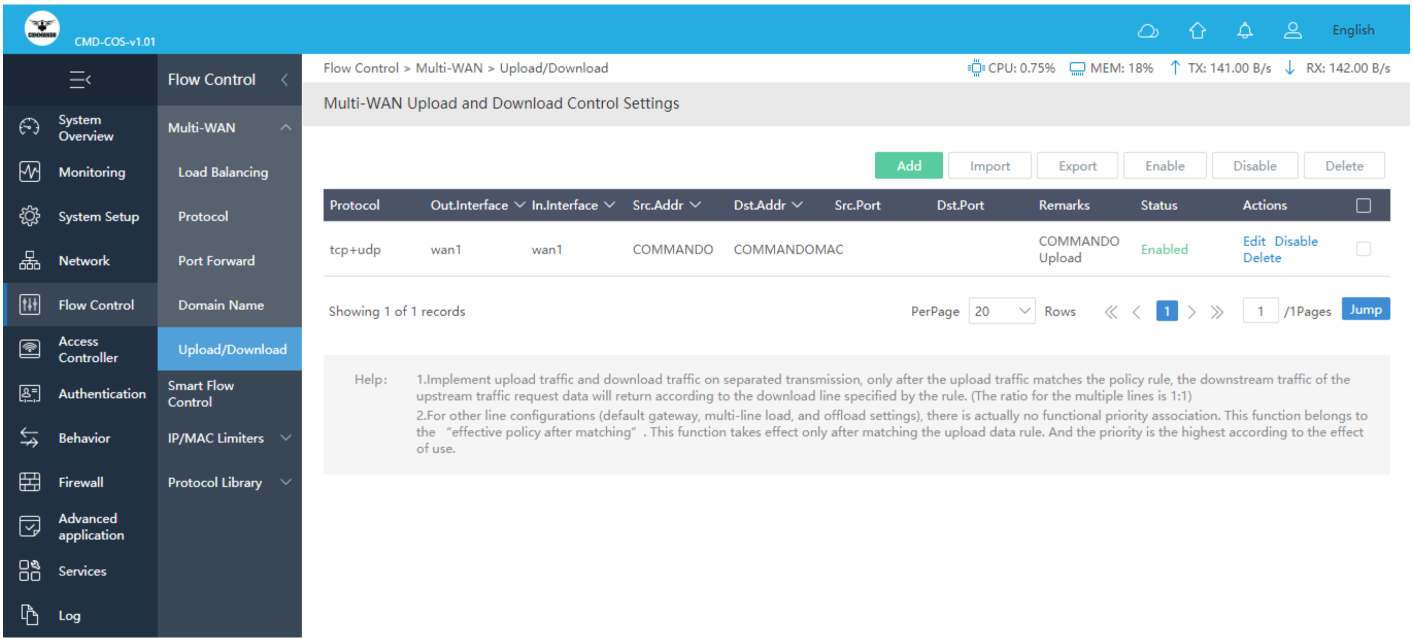
COMMANDOMAC

Src.Port:

Dst.Port:

Remarks: COMMANDO Upload

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



Flow Control > Multi-WAN > Upload/Download

CPU: 0.75% MEM: 18% TX: 141.00 B/s RX: 142.00 B/s

Multi-WAN Upload and Download Control Settings

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

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

Help: 1.Implement upload traffic and download traffic on separated transmission, only after the upload traffic matches the policy rule, the downstream traffic of the upstream traffic request data will return according to the download line specified by the rule. (The ratio for the multiple lines is 1:1)

2.For other line configurations (default gateway, multi-line load, and offload settings), there is actually no functional priority association. This function belongs to the "effective policy after matching" . This function takes effect only after matching the upload data rule. And the priority is the highest according to the effect of use.

Fig 4.1.23 Multi-WAN Upload and Download Control Settings page

4.2 Smart Flow Control

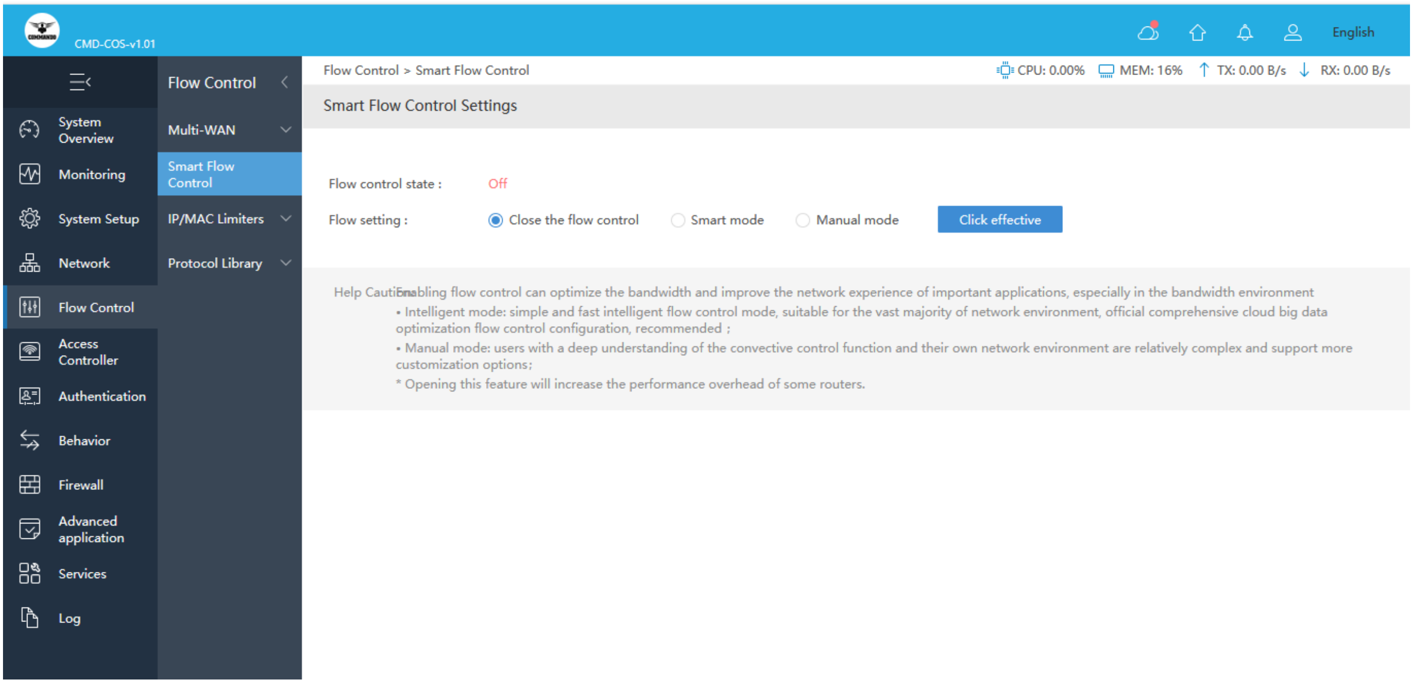
Smart Flow Control Settings is an appropriate flow control strategy can improve network performance by using the available resources efficiently and by alleviate congestion and to obtain an efficient network performance. Head‑of‑line (HOL) blocking problem can occur in the FIFO queue and Round‑Robin (RR)‑based scheduling mechanism. In the HOL blocking, when the first packet in buffer queues is blocked, the other packets behind them cannot pass through the lines even if there are enough resources. Therefore, network performance is reduced severely in the presence of HOL blocking. Enabling flow control can optimize the bandwidth and improve the network experience of important applications, especially in the bandwidth environment

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

Manual mode:
Ssers 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



Flow control state : Off

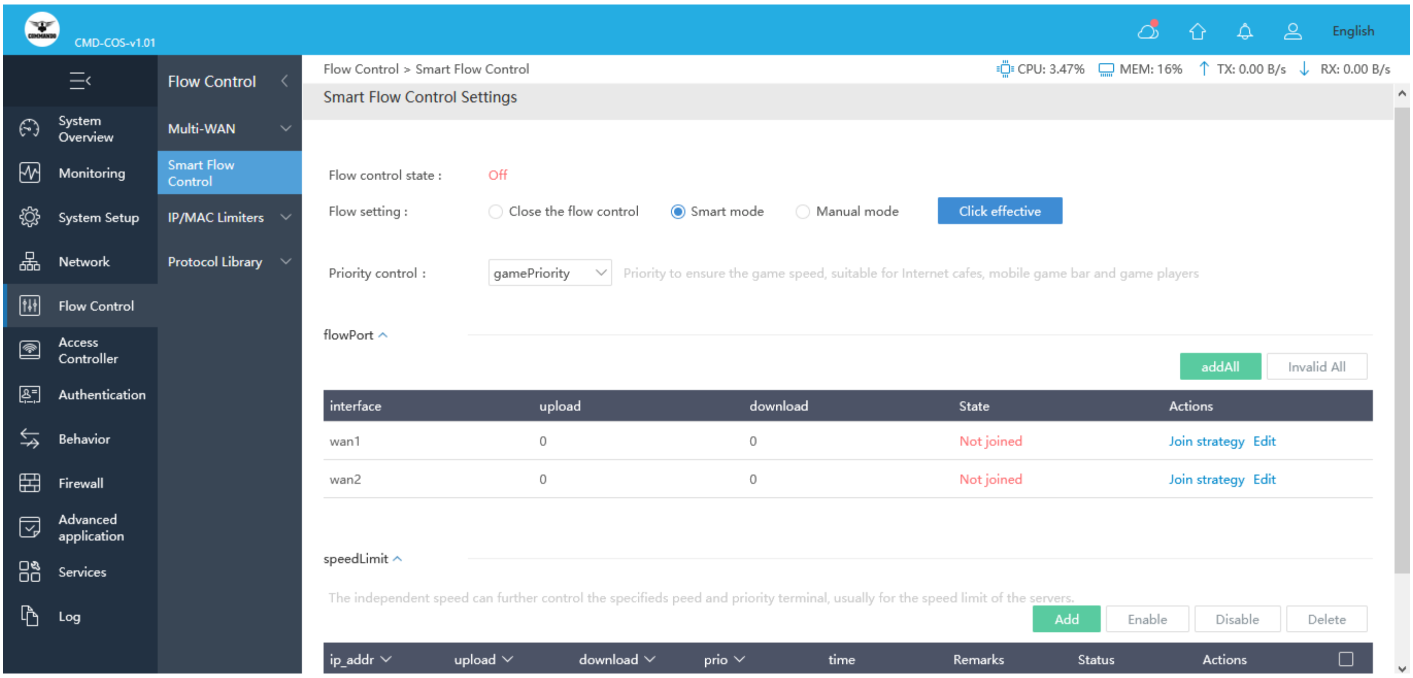
Flow setting : ● Close the flow control ○ Smart mode ○ Manual mode [Click effective]

Help CautiEnabling 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



Flow Control > Smart Flow Control

CPU: 3.47% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Smart Flow Control Settings

Flow control state : Off

Flow setting : ○ Close the flow control ● Smart mode ○ Manual mode [Click effective]

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

flowPort

[addAll] [Invalid All]

interface	upload	download	State	Actions
wan1	0	0	Not joined	Join strategy Edit
wan2	0	0	Not joined	Join strategy Edit

speedLimit

The independent speed can further control the specifieds peed and priority terminal, usually for the speed limit of the servers.

[Add] [Enable] [Disable] [Delete]

ip_addr	upload	download	prio	time	Remarks	Status	Actions	□

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:

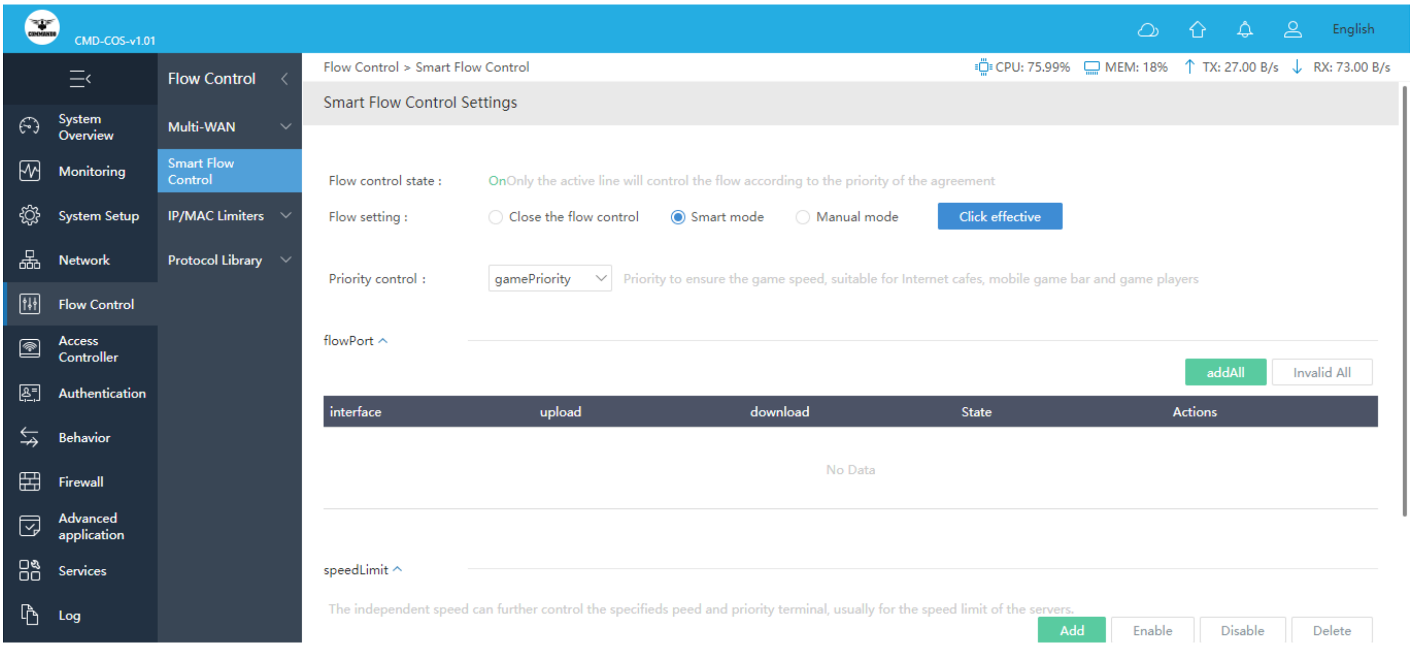
Priority to ensure the game speed, suitable for Internet cafes, mobile game bar and game players.

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.



Flow Control > Smart Flow Control

CPU: 75.99% MEM: 18% TX: 27.00 B/s RX: 73.00 B/s

Smart Flow Control Settings

Flow control state : OnOnly the active line will control the flow according to the priority of the agreement

Flow setting : ○ Close the flow control ● Smart mode ○ Manual mode Click effective

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

flowPort

addAll Invalid All

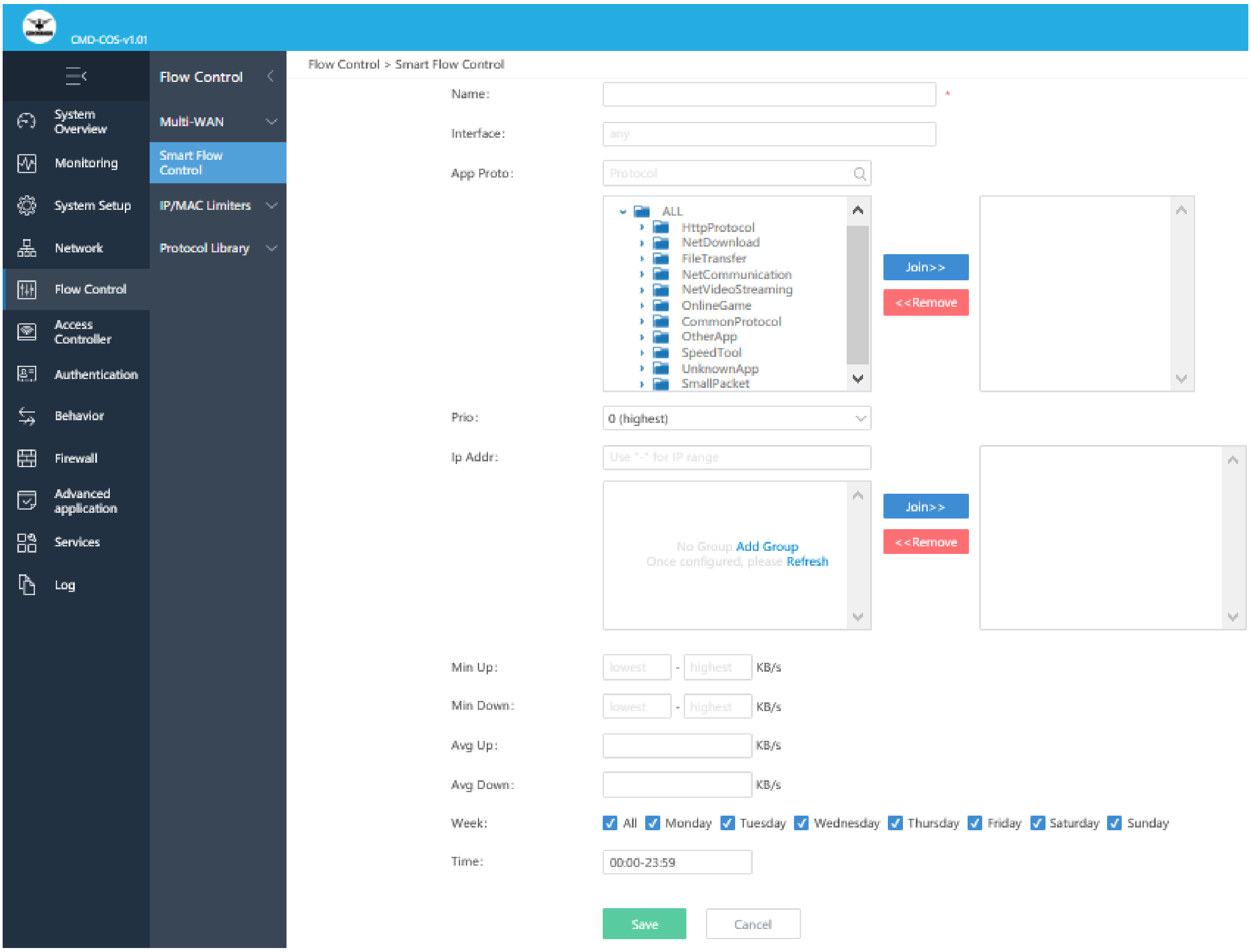
interface	upload	download	State	Actions
No Data				

speedLimit

The independent speed can further control the specifieds peed and priority terminal, usually for the speed limit of the servers.

Add Enable Disable Delete

Fig 4.2.3 Default game Priority in Smart Flow Control Settings page



Flow Control > Smart Flow Control

Name: *

Interface: any

App Proto: Protocol

Prio: 0 (highest)

Ip Addr: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Min Up: lowest - highest KB/s

Min Down: lowest - highest KB/s

Avg Up: KB/s

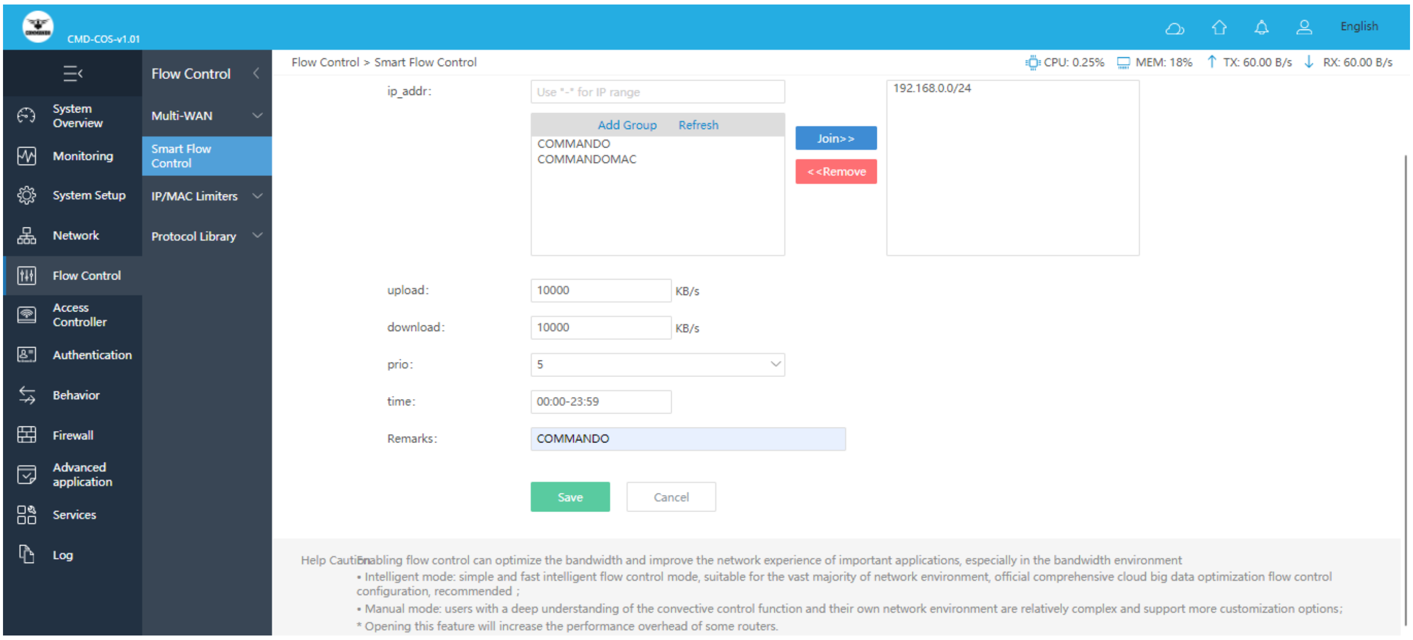
Avg Down: KB/s

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

Time: 00:00-23:59

Save Cancel

Fig 4.2.4 Add Smart Flow Control Settings page



Flow Control > Smart Flow Control

CPU: 0.25% MEM: 18% TX: 60.00 B/s RX: 60.00 B/s

ip_addr: Use "-" for IP range

COMMANDO
COMMANDOMAC

192.168.0.0/24

upload: 10000 KB/s

download: 10000 KB/s

prio: 5

time: 00:00-23:59

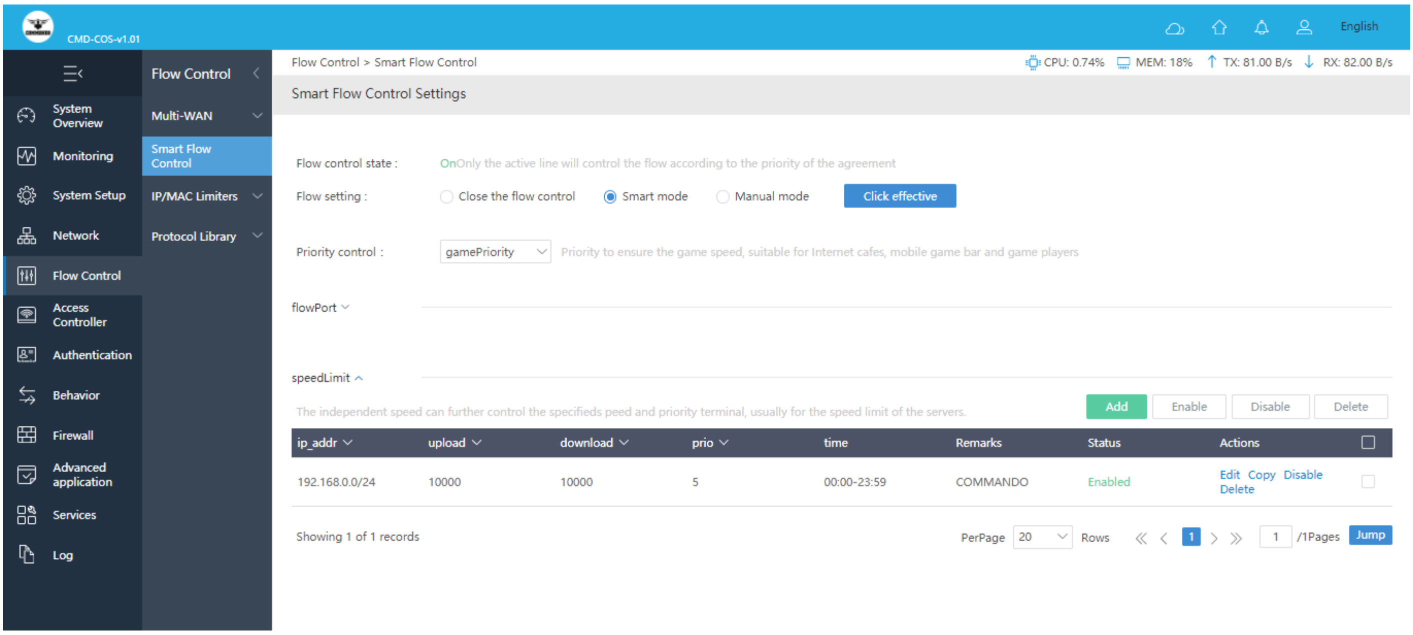
Remarks: COMMANDO

Help CautiEnabling 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 4.2.5 Changing Smart Flow Control Settings page



Flow Control > Smart Flow Control

CPU: 0.74% MEM: 18% TX: 81.00 B/s RX: 82.00 B/s

Smart Flow Control Settings

Flow control state : OnOnly the active line will control the flow according to the priority of the agreement

Flow setting : ○ Close the flow control ● Smart mode ○ Manual mode

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

flowPort

speedLimit

The independent speed can further control the specifieds peed and priority terminal, usually for the speed limit of the servers.

ip_addr	upload	download	prio	time	Remarks	Status	Actions	□
192.168.0.0/24	10000	10000	5	00:00-23:59	COMMANDO	Enabled	Edit Copy Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages

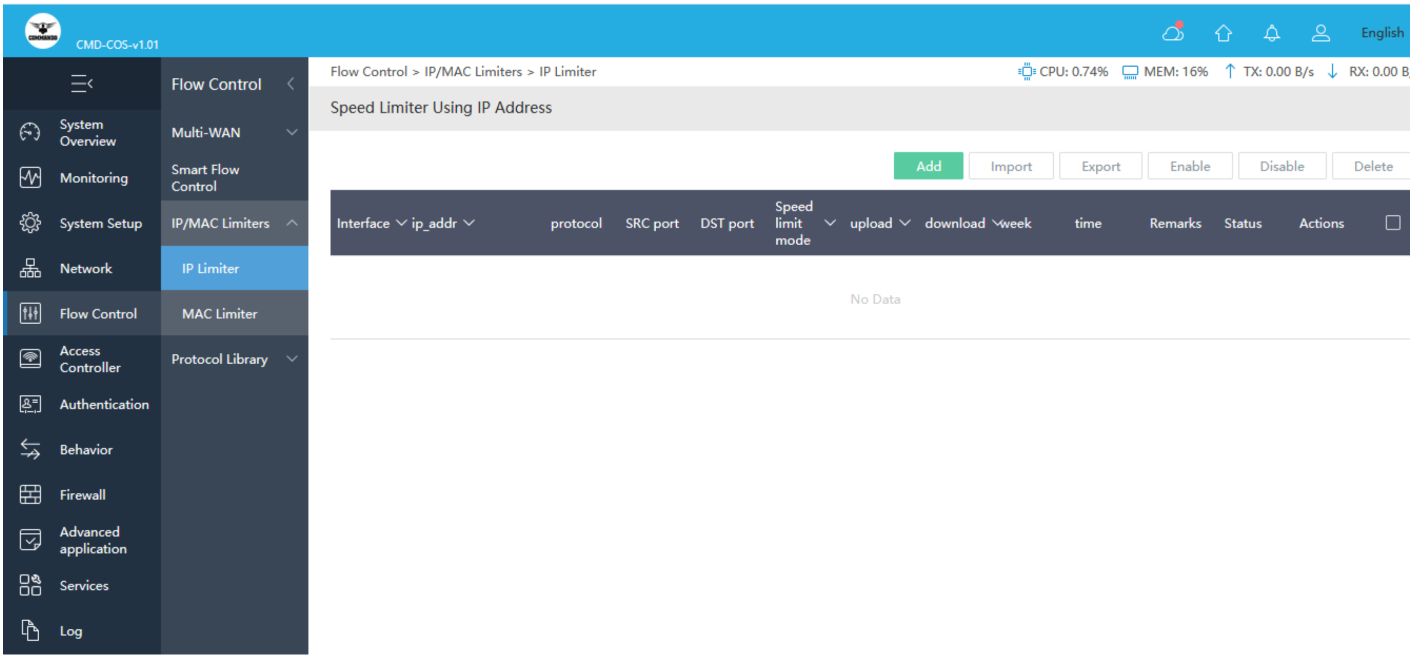
Fig 4.2.6 Smart Flow Control Settings page

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



Flow Control > IP/MAC Limiters > IP Limiter

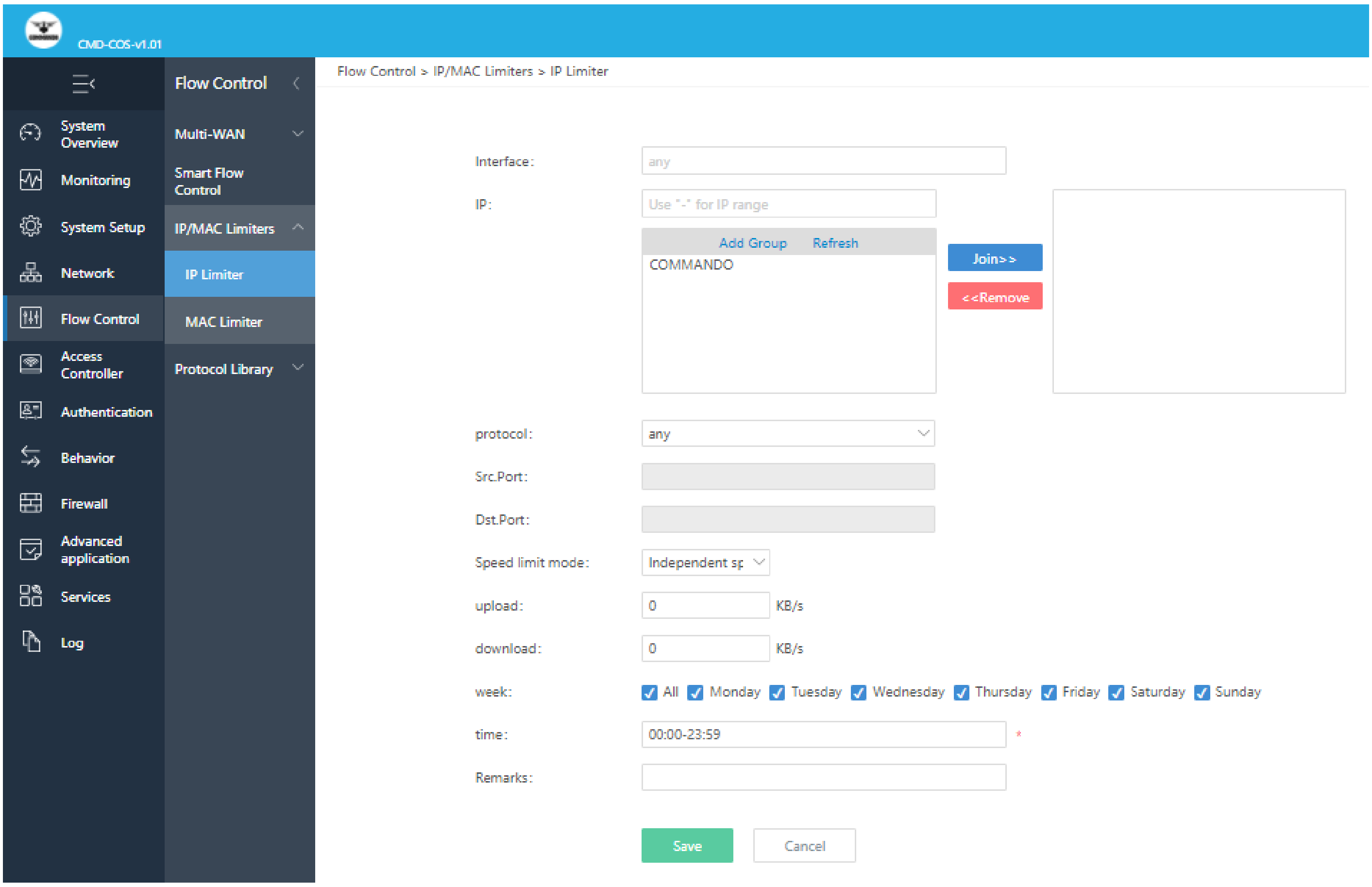
CPU: 0.74% MEM: 16% TX: 0.00 B/s RX: 0.00 B

Speed Limiter Using IP Address

Interface	ip_addr	protocol	SRC port	DST port	Speed limit mode	upload	download	week	time	Remarks	Status	Actions	□

No Data

Fig 4.3.1 Default Speed Limiter Using IP Address page



Flow Control > IP/MAC Limiters > IP Limiter

Interface: any

IP: Use "-" for IP range

COMMANDO

protocol: any

Src.Port:

Dst.Port:

Speed limit mode: Independent sp

upload: 0 KB/s

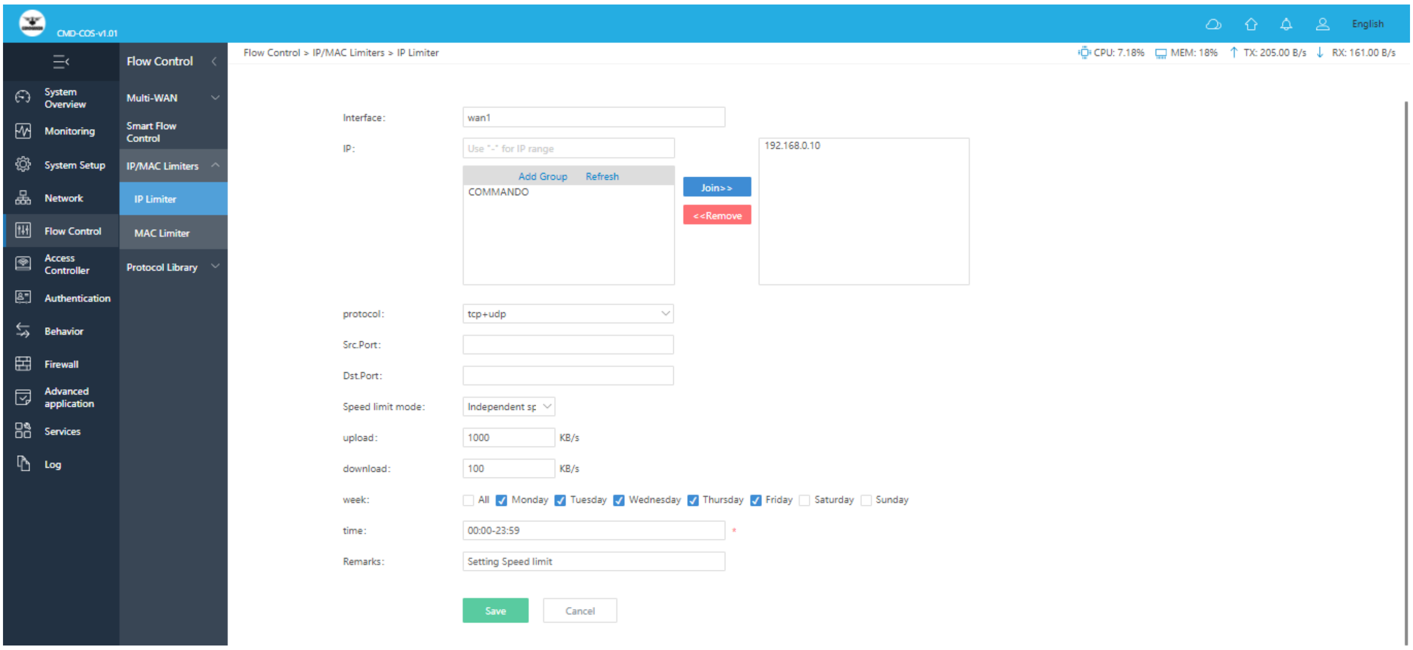
download: 0 KB/s

week: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

time: 00:00-23:59 *

Remarks:

Fig 4.3.2 Add Speed Limiter Using IP Address page



Flow Control > IP/MAC Limiters > IP Limiter

Interface: wan1

IP: Use "-" for IP range

COMMANDO

192.168.0.10

protocol: tcp+udp

Src.Port:

Dst.Port:

Speed limit mode: Independent sp

upload: 1000 KB/s

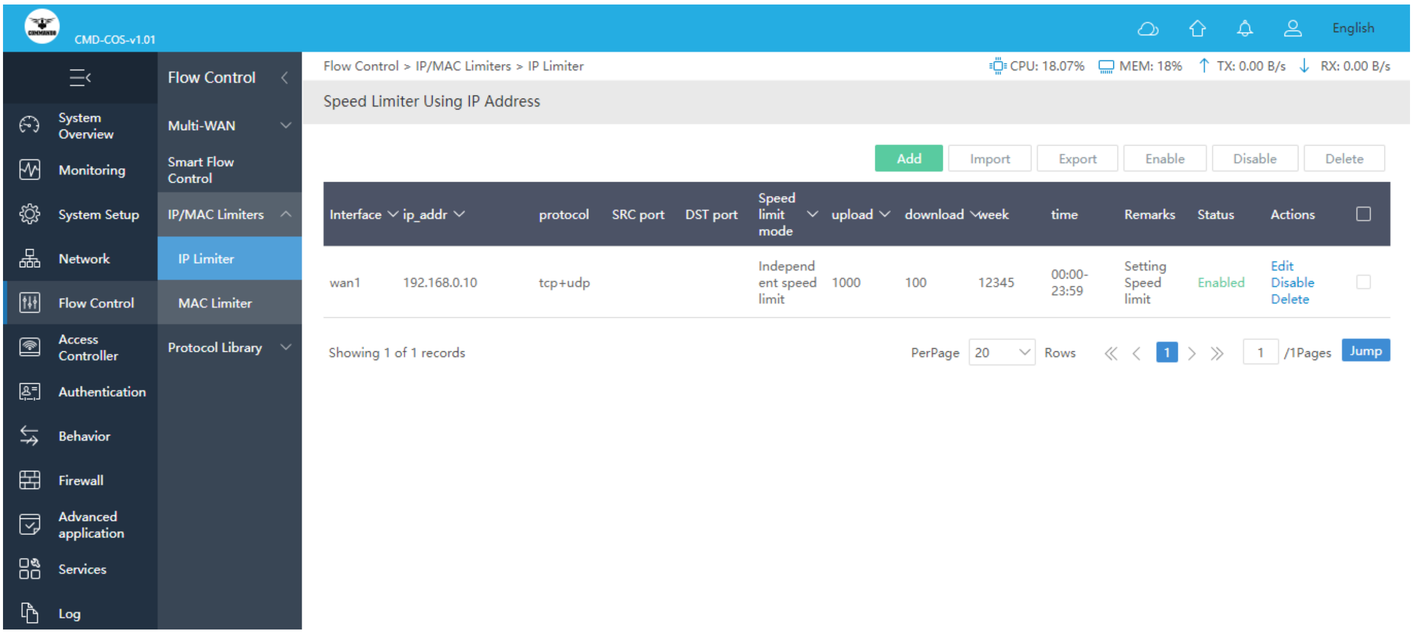
download: 100 KB/s

week: □ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

time: 00:00-23:59 *

Remarks: Setting Speed limit

Fig 4.3.3 Speed Limiter for Particular IP Address Page



Flow Control > IP/MAC Limiters > IP Limiter

Speed Limiter Using IP Address

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

Showing 1 of 1 records

PerPage 20 Rows 1 /1Pages

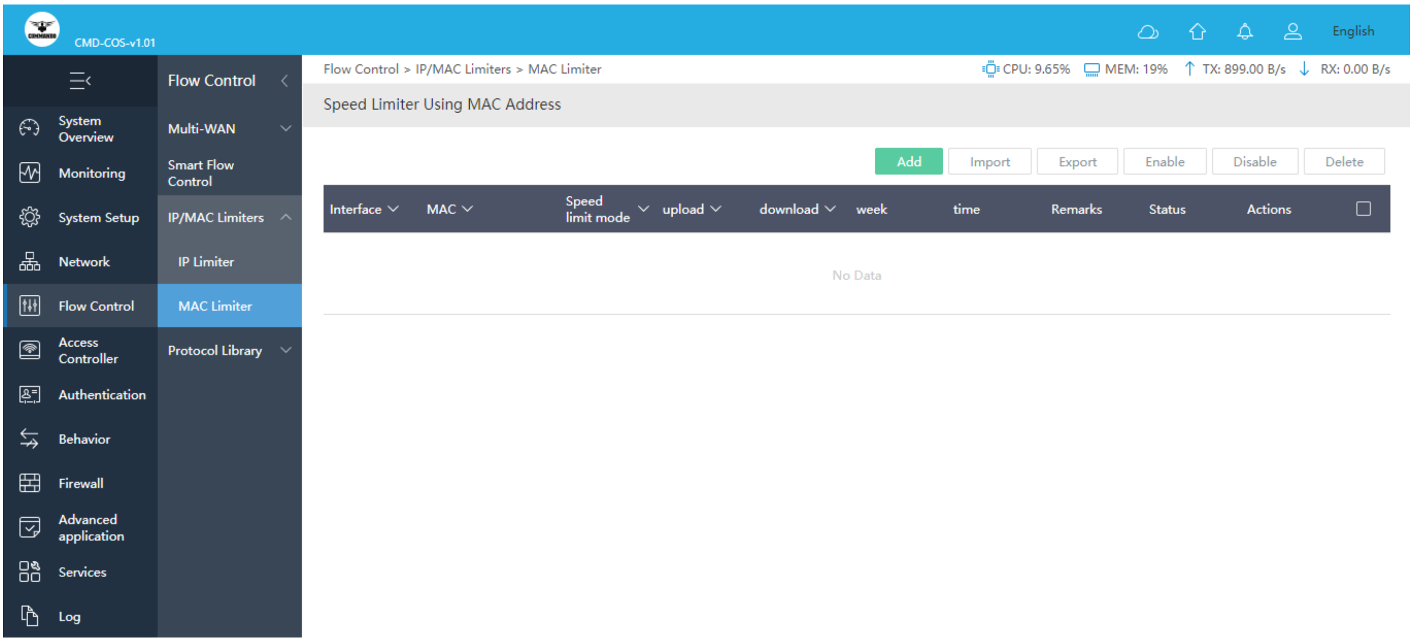
Fig 4.3.4 Speed Limiter Using IP Address Page

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



Flow Control > IP/MAC Limiters > MAC Limiter

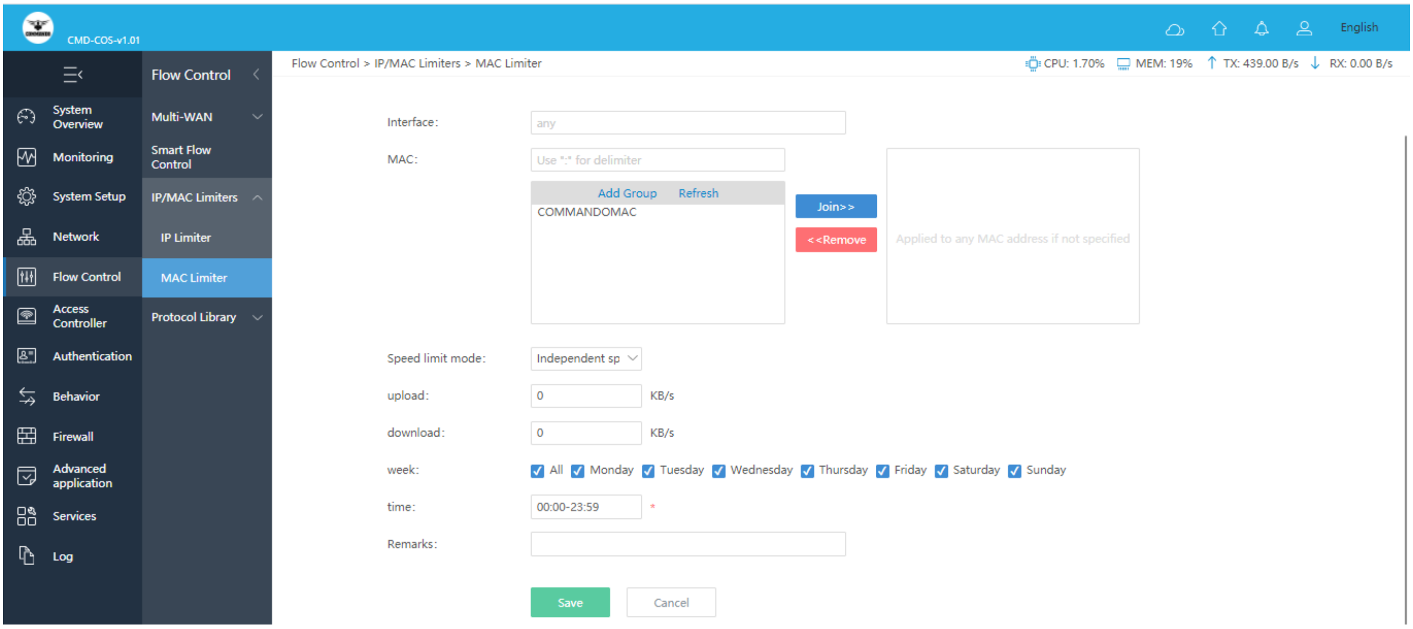
CPU: 9.65% MEM: 19% TX: 899.00 B/s RX: 0.00 B/s

Speed Limiter Using MAC Address

Interface	MAC	Speed limit mode	upload	download	week	time	Remarks	Status	Actions	□

No Data

Fig 4.3.5 Default Speed Limiter Using MAC Address page



Flow Control > IP/MAC Limiters > MAC Limiter

CPU: 1.70% MEM: 19% TX: 439.00 B/s RX: 0.00 B/s

Interface: any

MAC: Use ":" for delimiter

COMMANDOMAC

Applied to any MAC address if not specified

Speed limit mode: Independent sp

upload: 0 KB/s

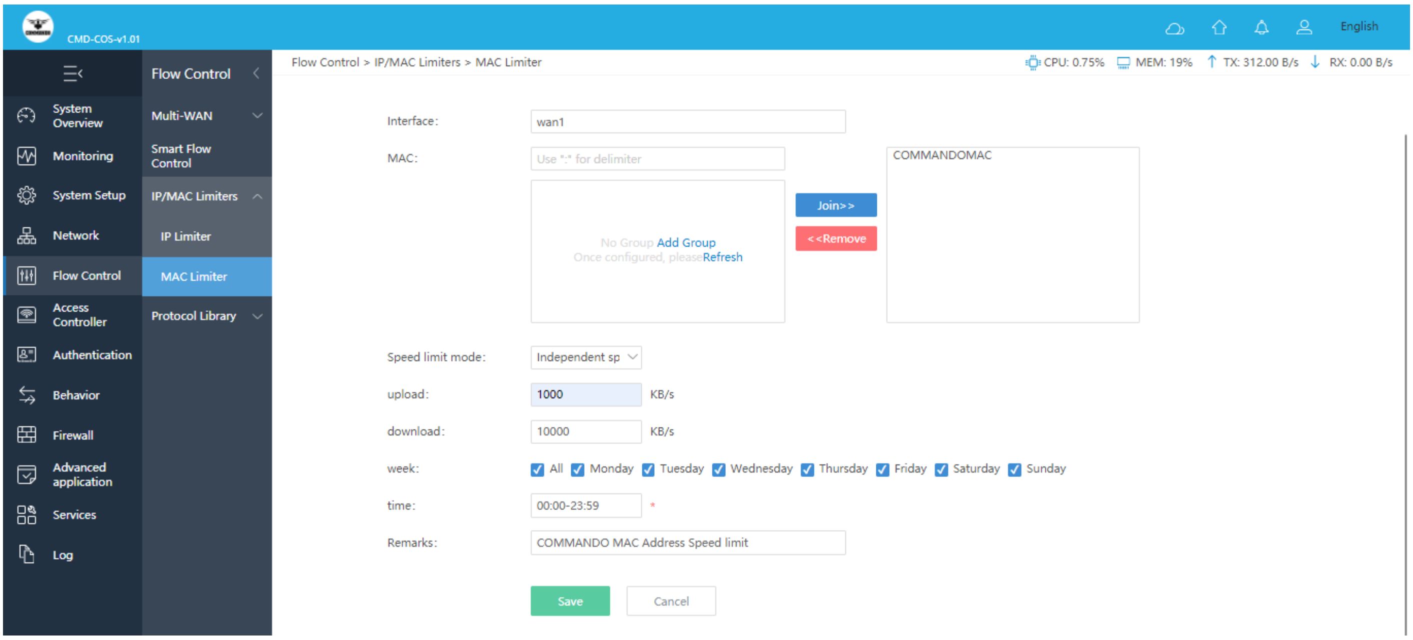
download: 0 KB/s

week: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

time: 00:00-23:59 *

Remarks:

Fig 4.3.6 Add Speed Limiter Using MAC Address page



Interface: wan1

MAC: Use ":" for delimiter

No Group Add Group
Once configured, please Refresh

Join>>
<<Remove

COMMANDOMAC

Speed limit mode: Independent sp

upload: 1000 KB/s

download: 10000 KB/s

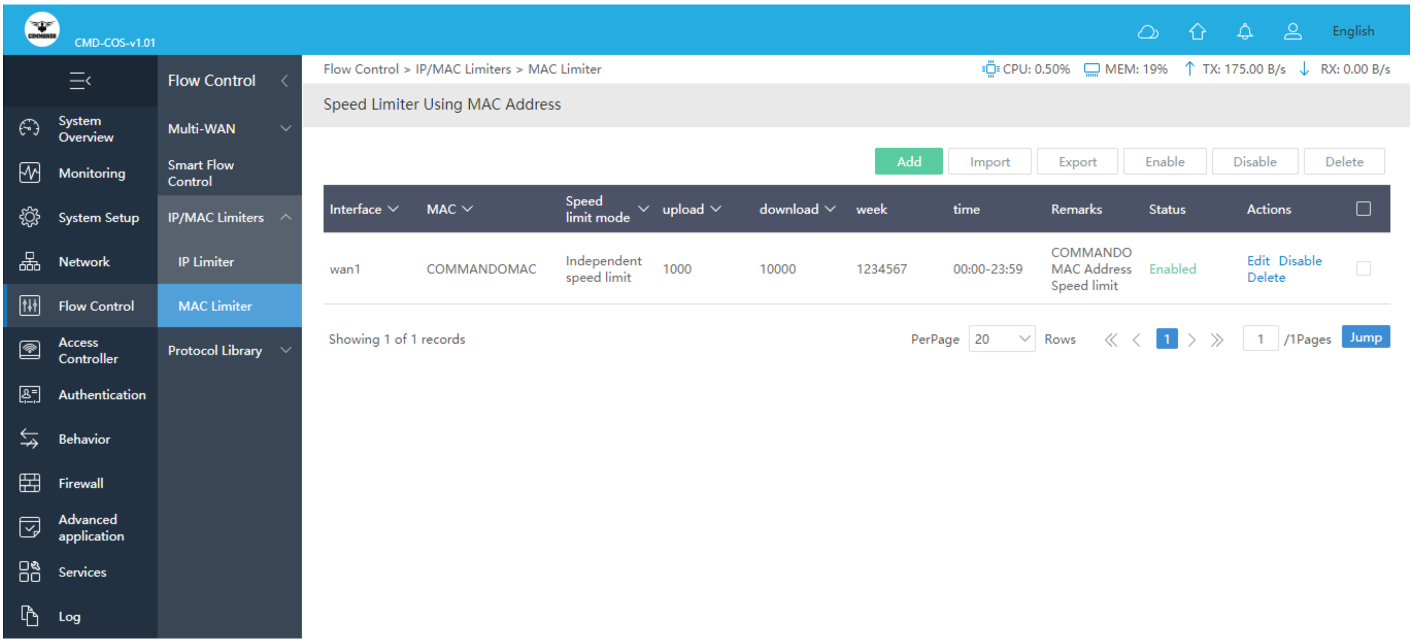
week: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

time: 00:00-23:59 *

Remarks: COMMANDO MAC Address Speed limit

Save Cancel

Fig 4.3.7 Speed Limiter For COMMANDOMAC Group MAC Address



Speed Limiter Using MAC Address

Add Import Export Enable Disable Delete

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

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

Fig 4.3.8 Speed Limiter for COMMANDOMAC Group page

4.4 Protocol Library

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

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

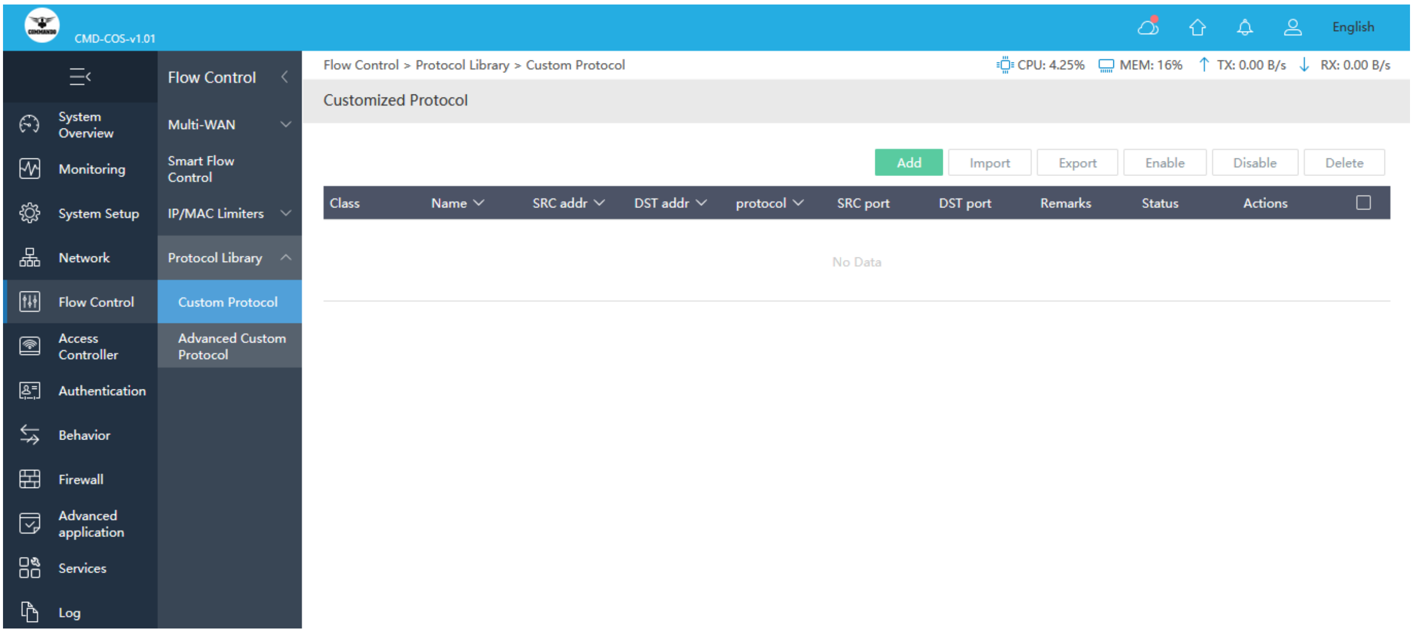
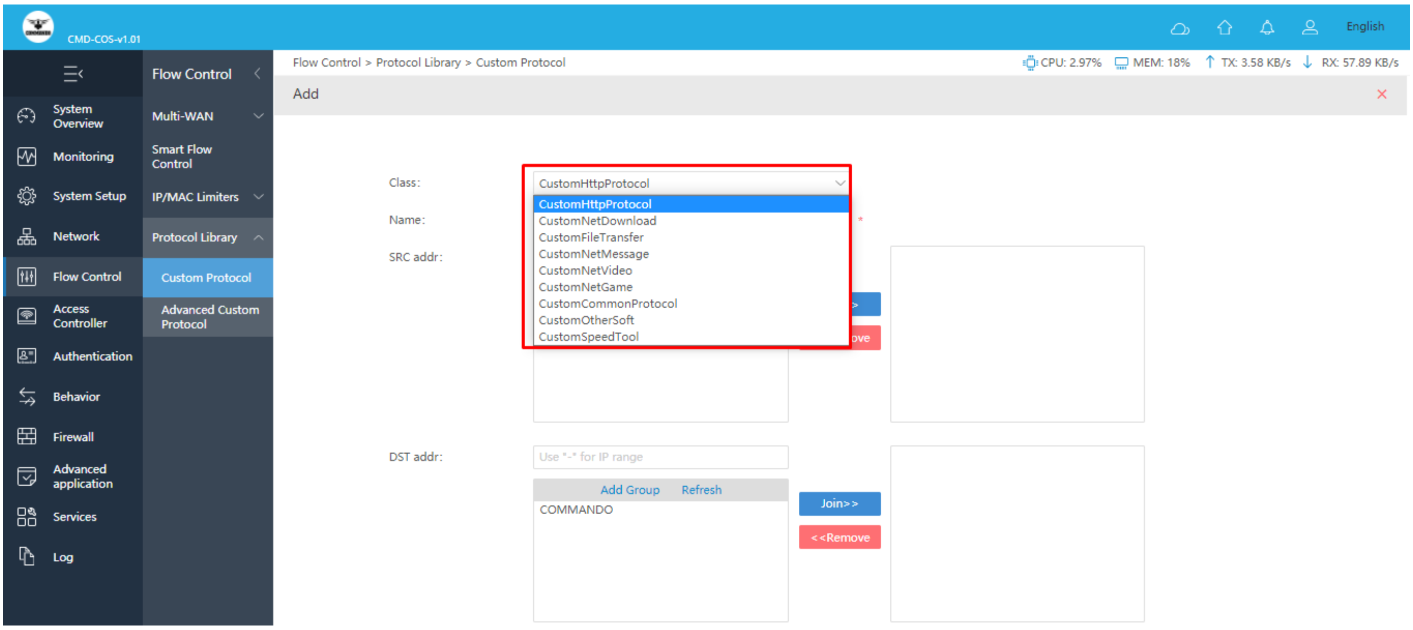
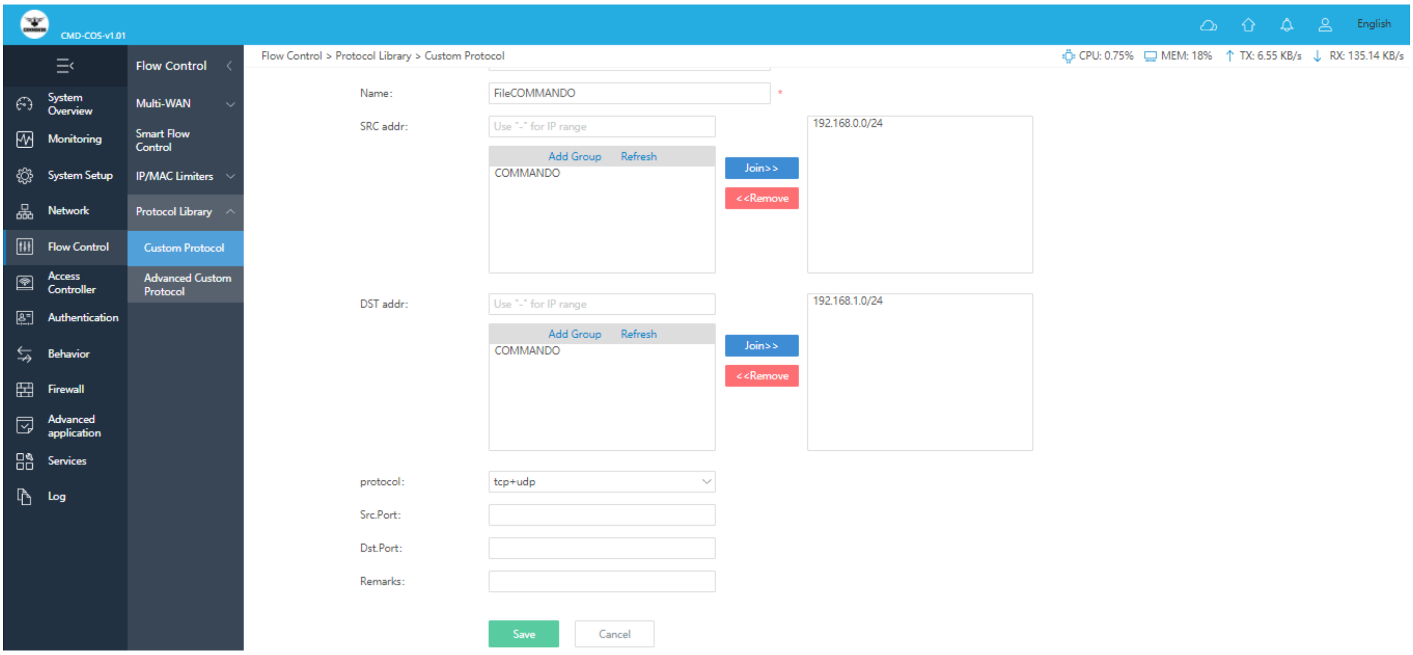


Fig 4.4.1 Default Customized Protocol page



Class: CustomHttpProtocol

Fig 4.4.2 Add Customized Protocol page



Name: FileCOMMANDO *

SRC addr: Use "-" for IP range

Add Group Refresh

COMMANDO

Join>>

<<Remove

192.168.0.0/24

DST addr: Use "-" for IP range

Add Group Refresh

COMMANDO

Join>>

<<Remove

192.168.1.0/24

protocol: tcp+udp

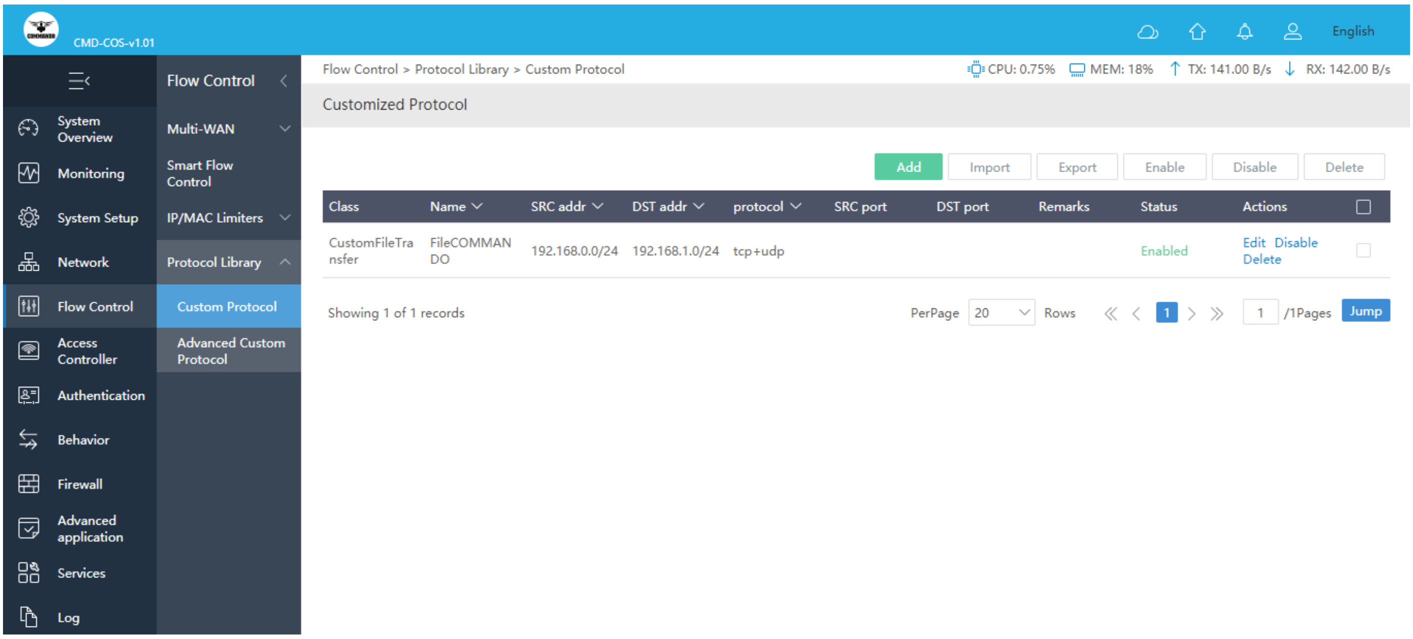
Src.Port:

Dst.Port:

Remarks:

Save Cancel

Fig 4.4.3 Customized Protocol for particular source and destination address page



Customized Protocol

Add Import Export Enable Disable Delete

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

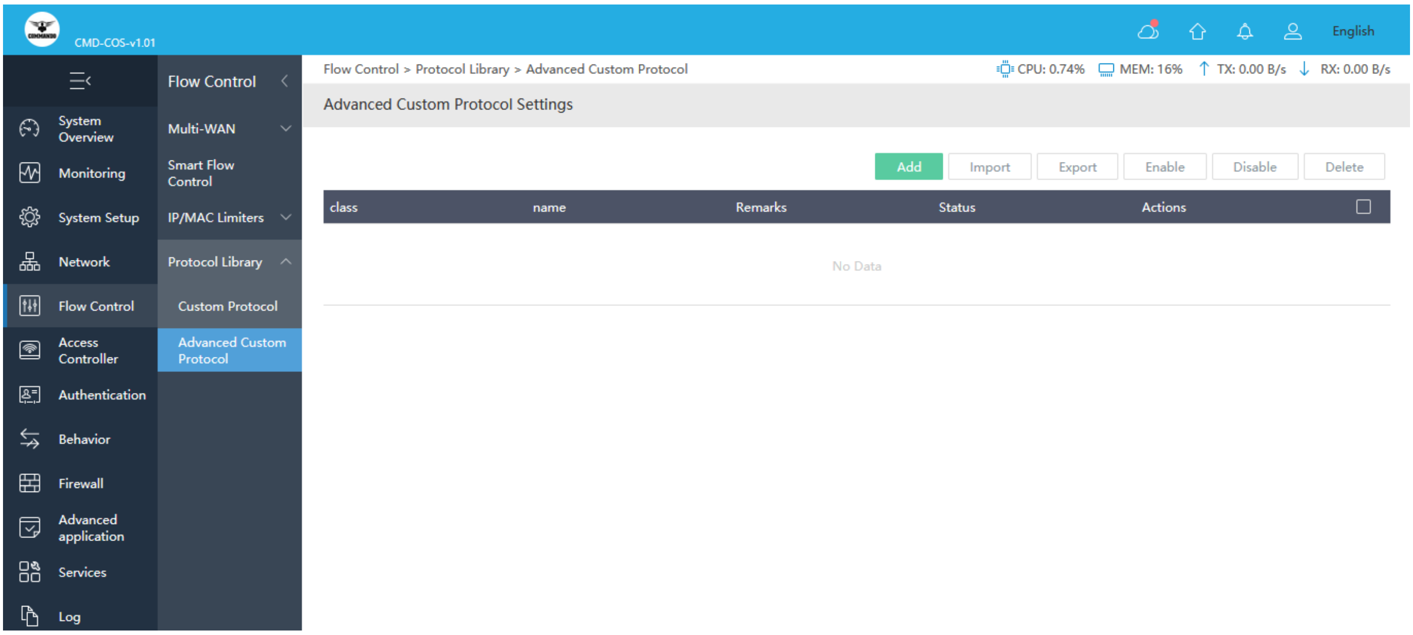
Showing 1 of 1 records PerPage 20 Rows 1 /1Pages Jump

Fig 4.4.4 Customized Protocol page

Advanced Custom Protocol Settings:

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

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



Flow Control > Protocol Library > Advanced Custom Protocol

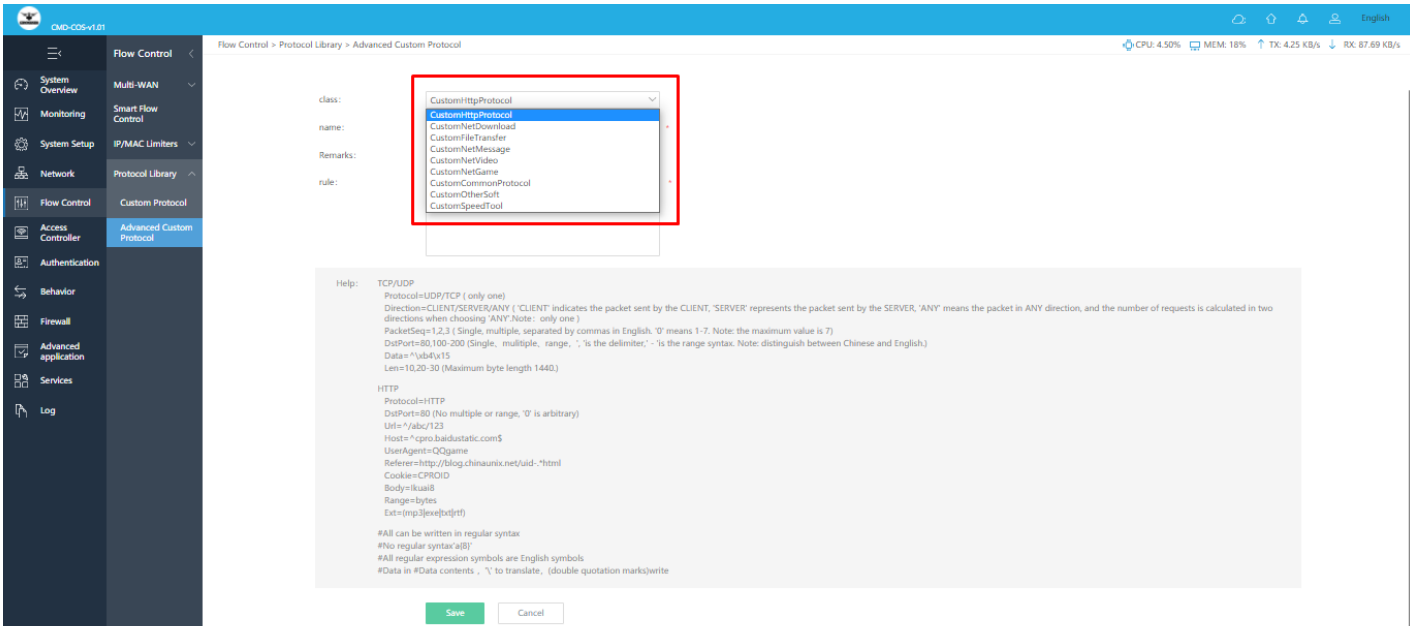
CPU: 0.74% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Advanced Custom Protocol Settings

class	name	Remarks	Status	Actions

No Data

Fig 4.4.5 Default Advanced Custom Protocol page



Flow Control > Protocol Library > Advanced Custom Protocol

CPU: 4.50% MEM: 18% TX: 4.25 KB/s RX: 87.69 KB/s

class: CustomHttpProtocol

name:

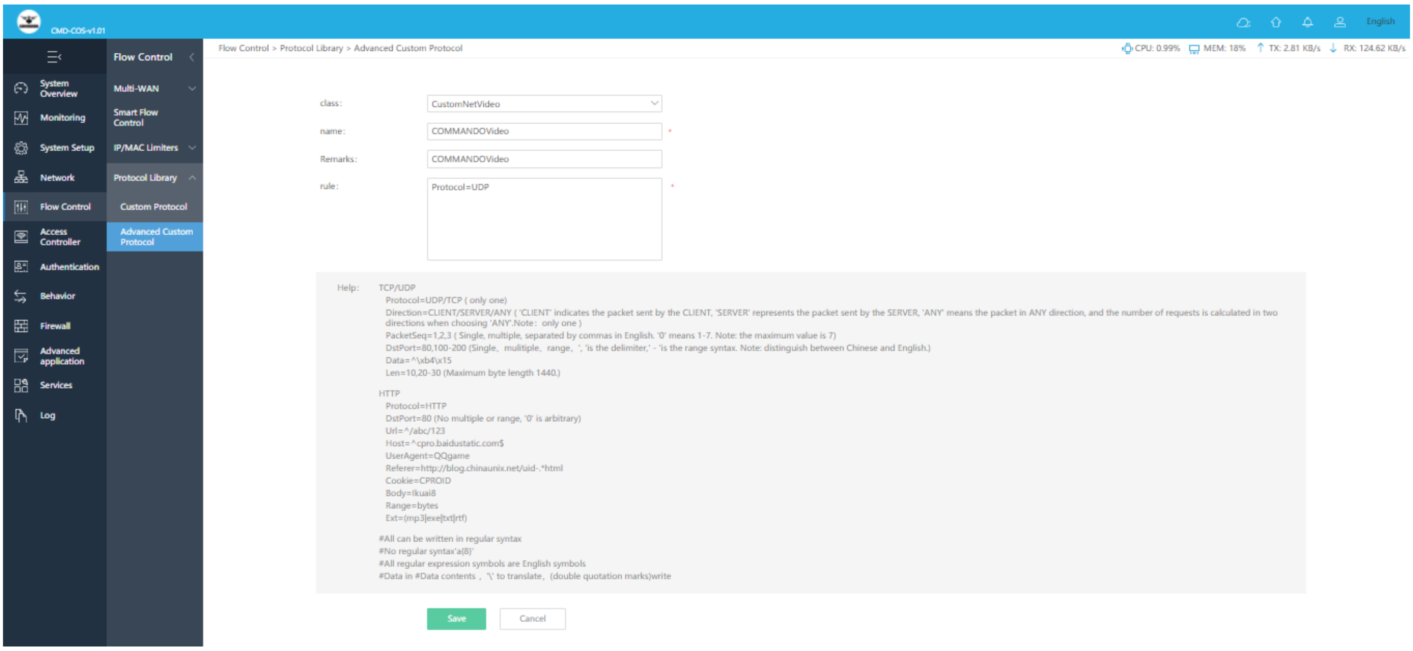
Remarks:

rule:

Help: TCP/UDP

```
Protocol=UDP/TCP ( only one)
Direction=CLIENT/SERVER/ANY ( 'CLIENT' indicates the packet sent by the CLIENT, 'SERVER' represents the packet sent by the SERVER, 'ANY' means the packet in ANY direction, and the number of requests is calculated in two directions when choosing 'ANY'.Note:  only one )
PacketSeq=1,2,3 ( Single, multiple, separated by commas in English. '0' means 1-7. Note: the maximum value is 7)
DstPort=80,100-200 (Single、mulitiple、range，', 'is the delimiter,' - 'is the range syntax. Note: distinguish between Chinese and English.)
Data=^\xb4\x15
Len=10,20-30 (Maximum byte length 1440.)

HTTP
Protocol=HTTP
DstPort=80 (No multiple or range, '0' is arbitrary)
Url=^/abc/123
Host=^cpro.baidustatic.com$
UserAgent=QQgame
Referer=http://blog.chinaunix.net/uid-.*html
Cookie=CPROID
Body=Ikuai8
Range=bytes
Ext=(mp3|exe|txt|rtf)

#All can be written in regular syntax
#No regular syntax'a{8}'
#All regular expression symbols are English symbols
#Data in #Data contents， '\' to translate，(double quotation marks)write
```

Fig 4.4.5 Add Advanced Custom Protocol page



Flow Control > Protocol Library > Advanced Custom Protocol

CPU: 0.99% MEM: 18% TX: 2.81 KB/s RX: 124.62 KB/s

class: CustomNetVideo

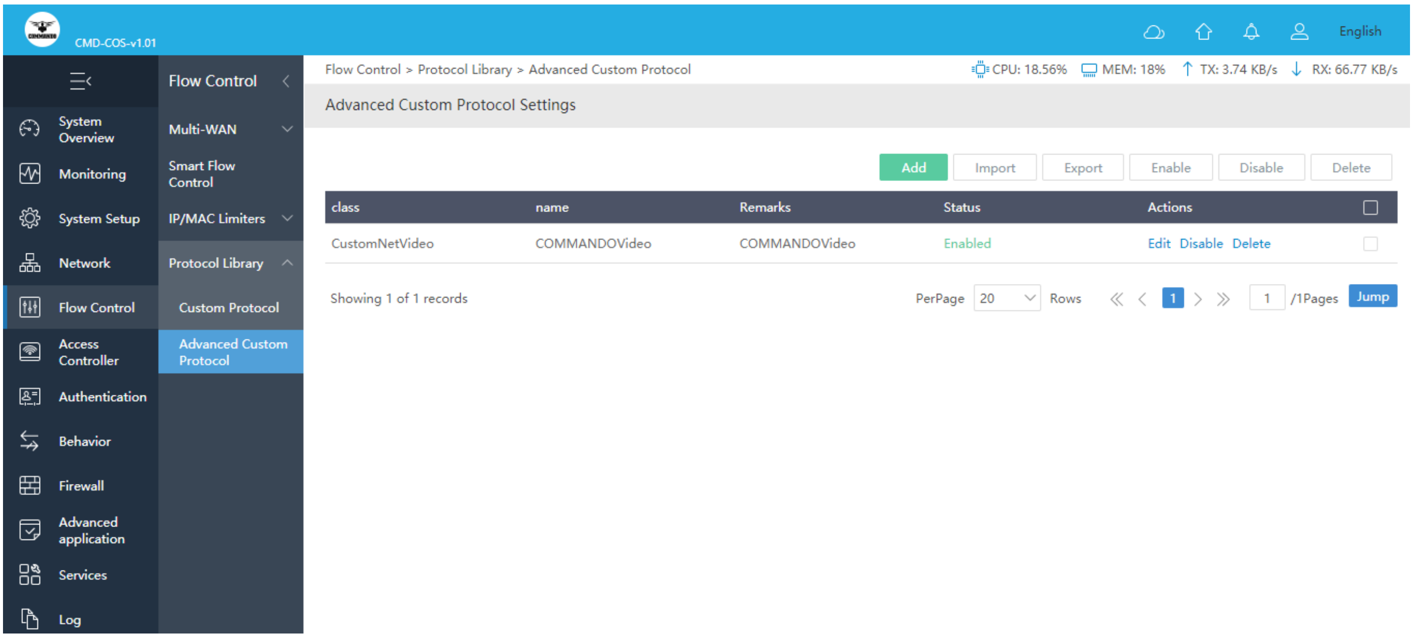
name: COMMANDOVideo *

Remarks: COMMANDOVideo

rule: Protocol=UDP *

```
Help:  TCP/UDP
         Protocol=UDP/TCP ( only one)
         Direction=CLIENT/SERVER/ANY ( 'CLIENT' indicates the packet sent by the CLIENT, 'SERVER' represents the packet sent by the SERVER, 'ANY' means the packet in ANY direction, and the number of requests is calculated in two
         directions when choosing 'ANY'.Note:  only one )
         PacketSeq=1,2,3 ( Single, multiple, separated by commas in English. '0' means 1-7. Note: the maximum value is 7)
         DstPort=80,100-200 (Single、mulitiple、range，', 'is the delimiter,' - 'is the range syntax. Note: distinguish between Chinese and English.)
         Data=^\xb4\x15
         Len=10,20-30 (Maximum byte length 1440.)

       HTTP
         Protocol=HTTP
         DstPort=80 (No multiple or range, '0' is arbitrary)
         Url=^/abc/123
         Host=^cpro.baidustatic.com$
         UserAgent=QQgame
         Referer=http://blog.chinaunix.net/uid-.*html
         Cookie=CPROID
         Body=Ikuai8
         Range=bytes
         Ext=(mp3|exe|txt|rtf)

       #All can be written in regular syntax
       #No regular syntax'a{8}'
       #All regular expression symbols are English symbols
       #Data in #Data contents，'\' to translate，(double quotation marks)write
```

Fig 4.4.6 Advanced Custom Protocol setting for video page



Flow Control > Protocol Library > Advanced Custom Protocol

CPU: 18.56% MEM: 18% TX: 3.74 KB/s RX: 66.77 KB/s

Advanced Custom Protocol Settings

class	name	Remarks	Status	Actions	□
CustomNetVideo	COMMANDOVideo	COMMANDOVideo	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages

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**

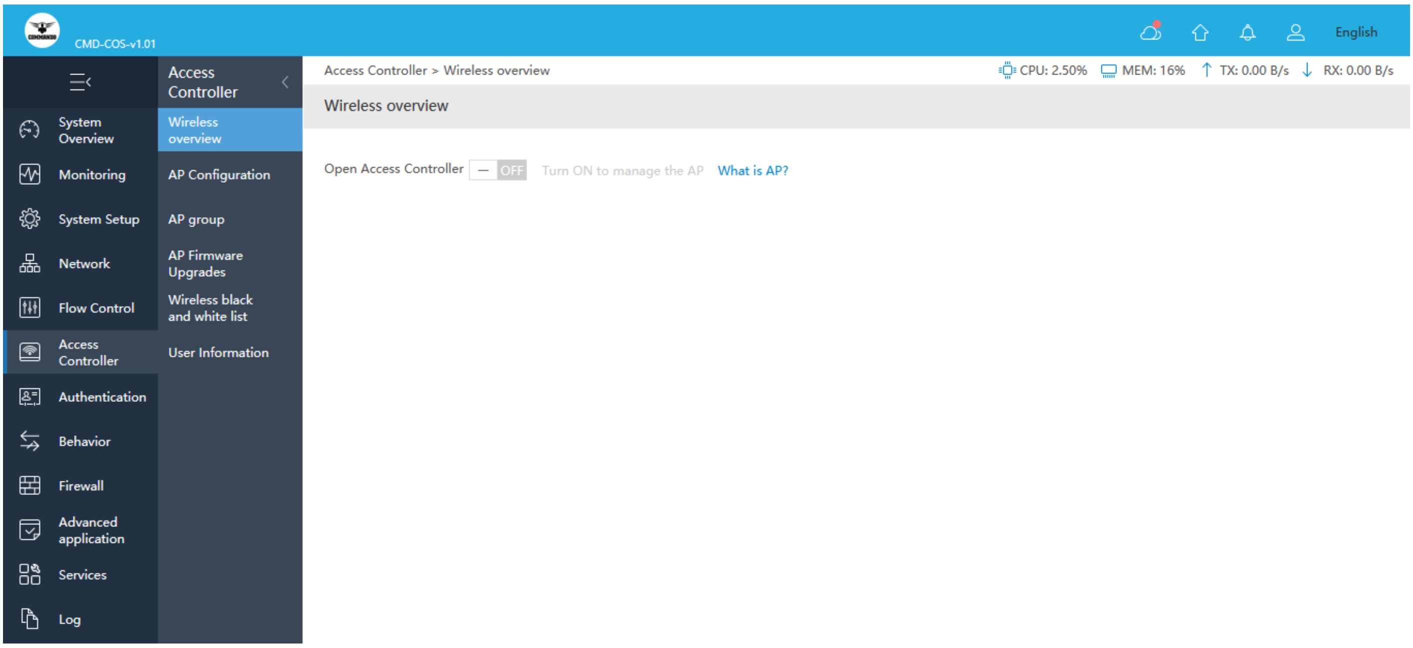


Fig 5.1.1 Default Wireless overview OFF page

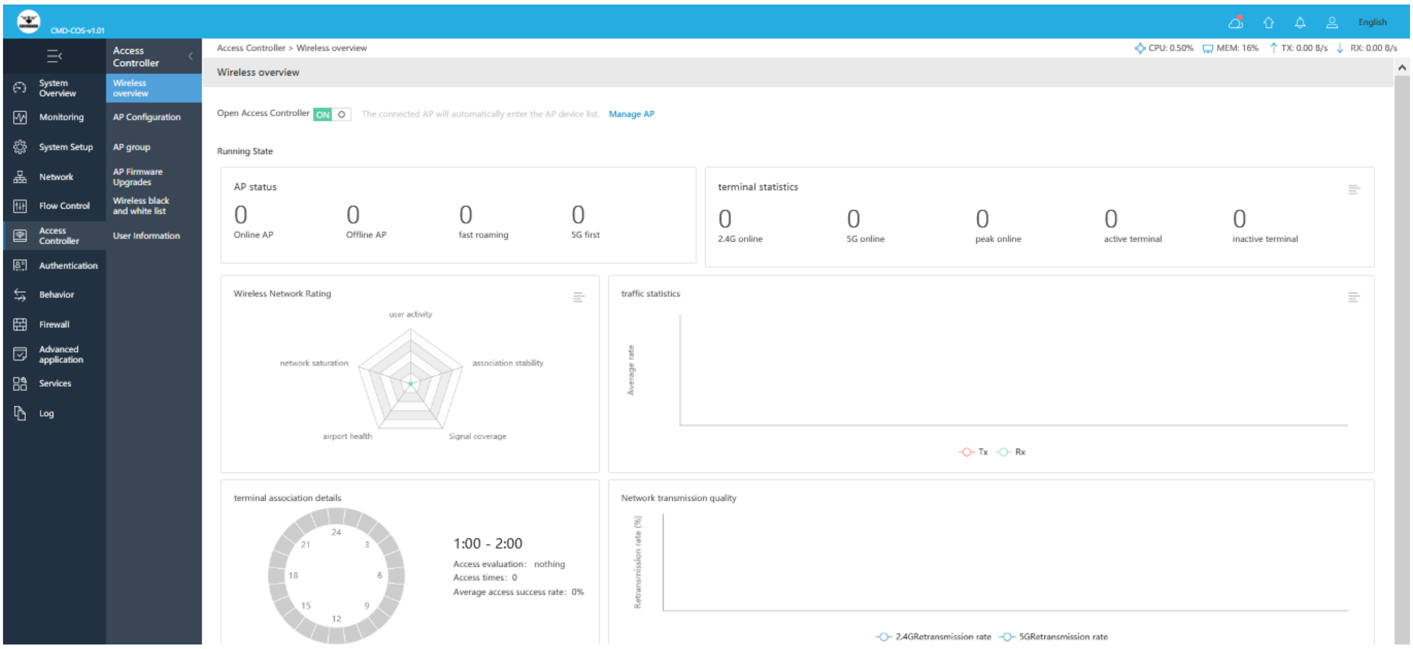
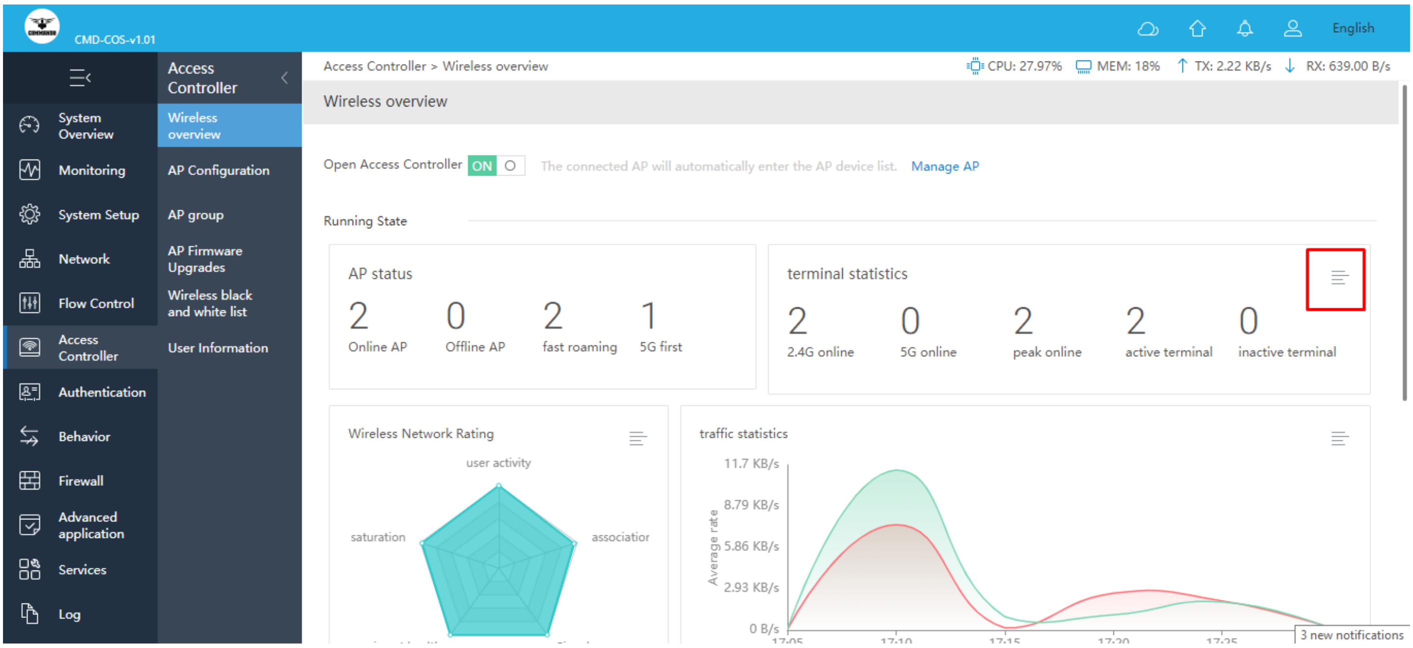


Fig 5.1.2 Default Wireless overview ON page



AP status

2	0	2	1
Online AP	Offline AP	fast roaming	5G first

terminal statistics

2	0	2	2	0
2.4G online	5G online	peak online	active terminal	inactive terminal

Fig 5.1.3 Wireless overview after connecting AP and users' page

After clicking above highlighted icon following page will be displayed

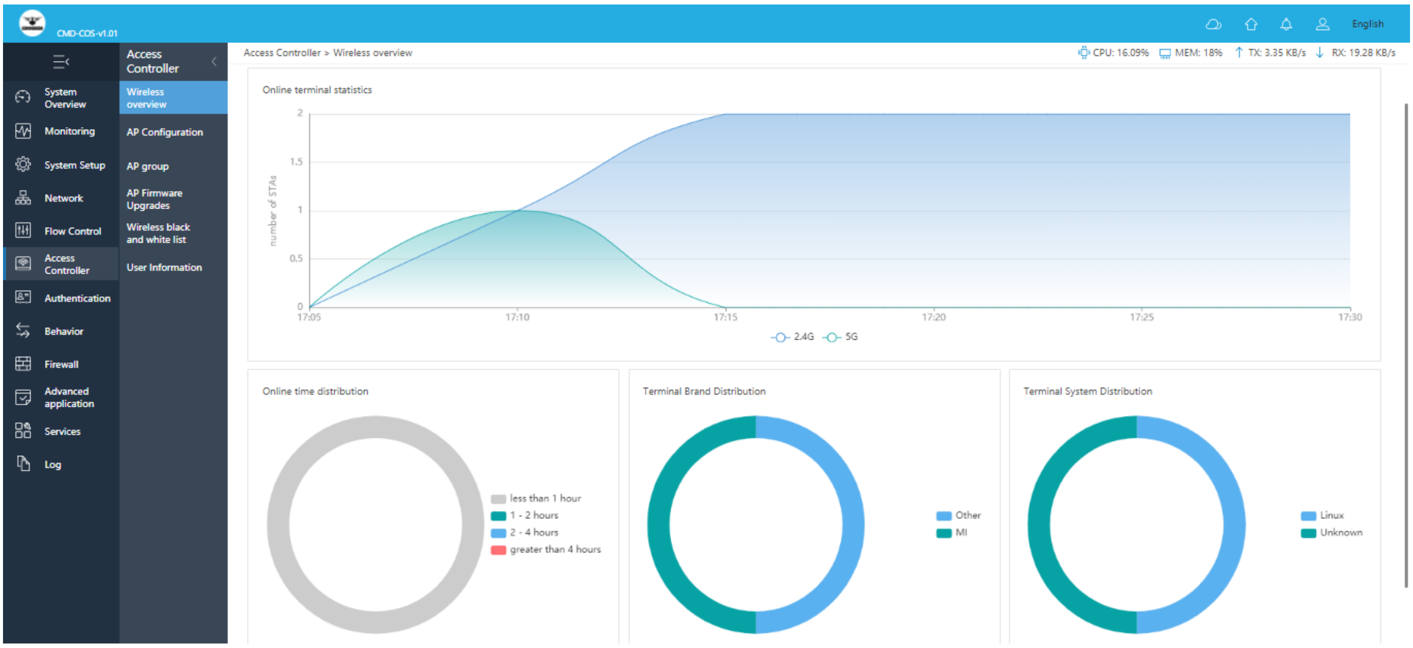


Fig 5.1.4 Online terminal statistics, distribution, System page

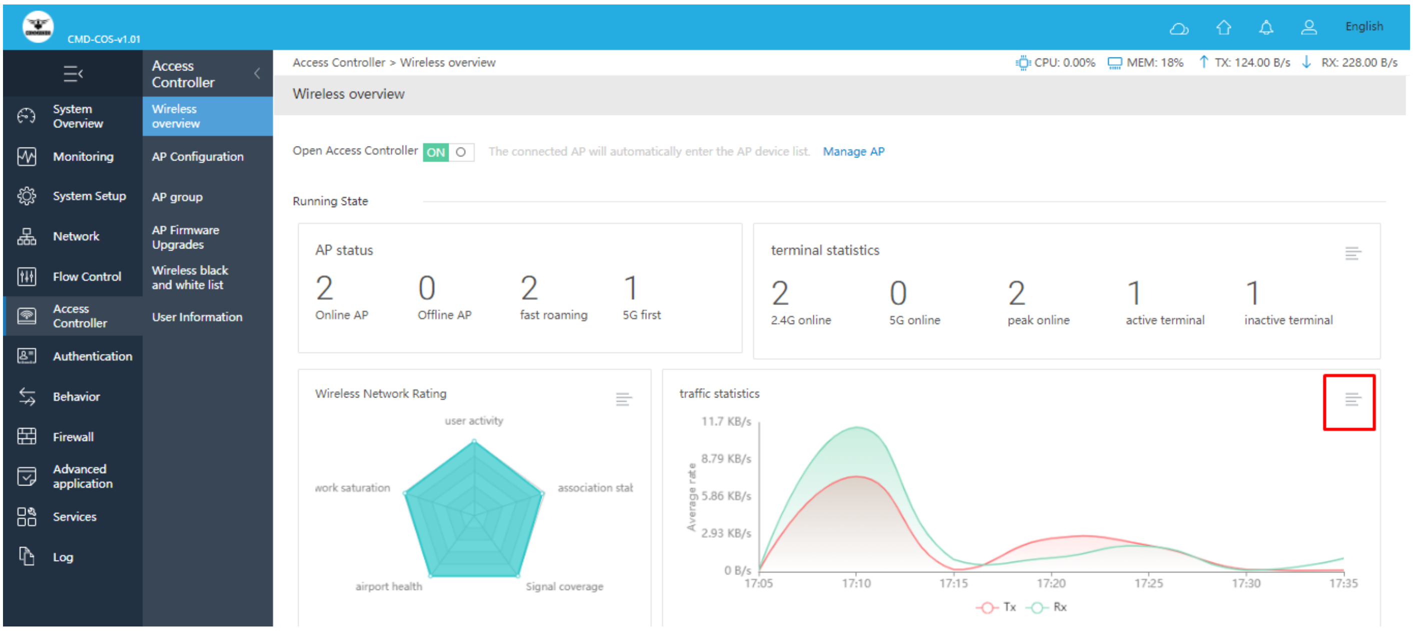


Fig 5.1.5 Traffic statistics page

After clicking above highlighted icon following page will be displayed

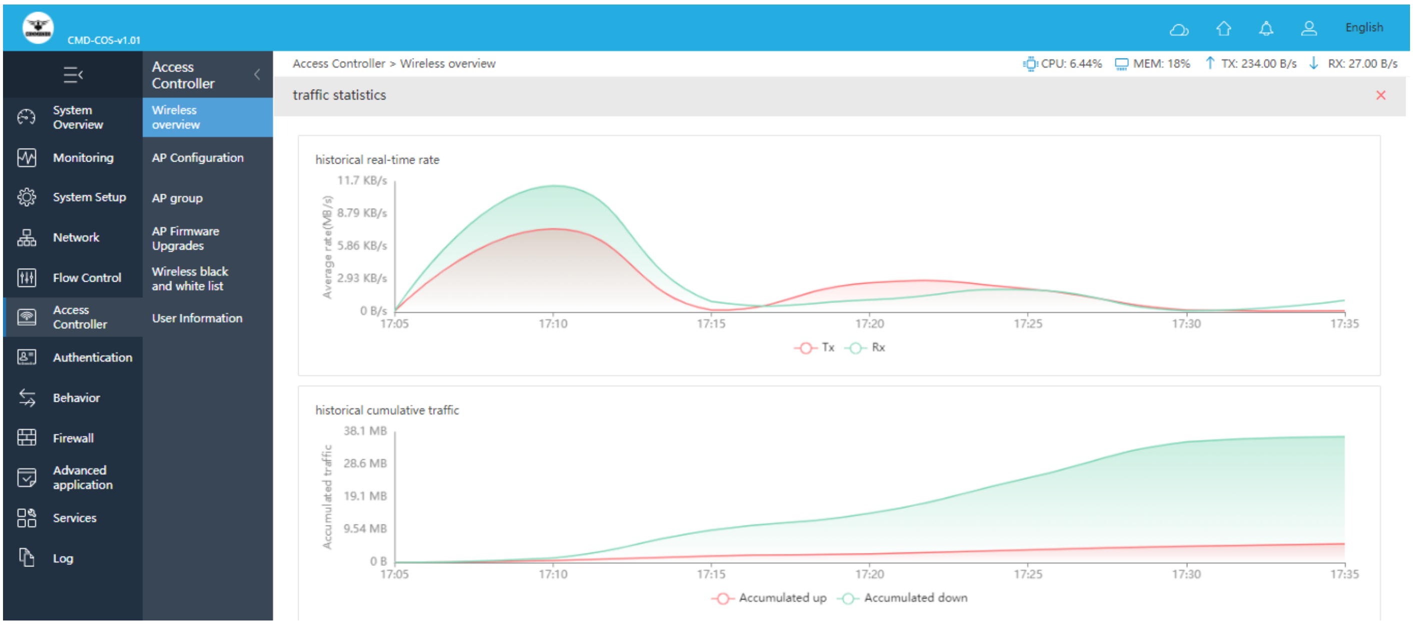


Fig 5.1.6 Traffic statistics with historical real-time rate, cumulative traffic page

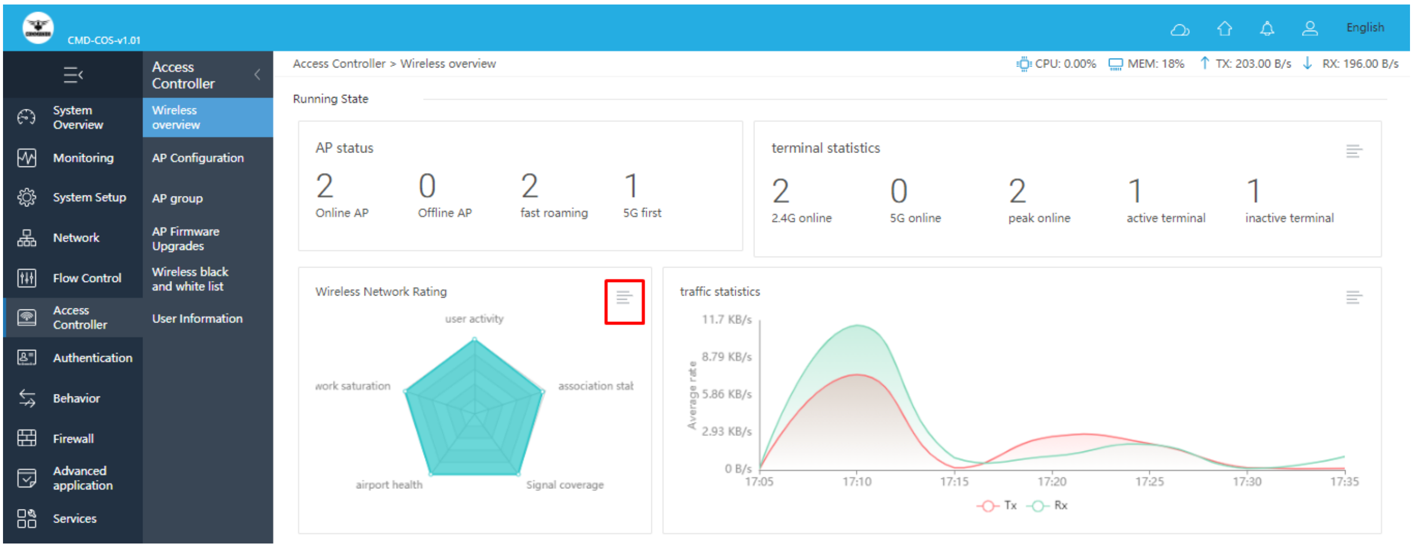


Fig 5.1.7 Wireless Network Rating page

After clicking above highlighted icon following page will be displayed

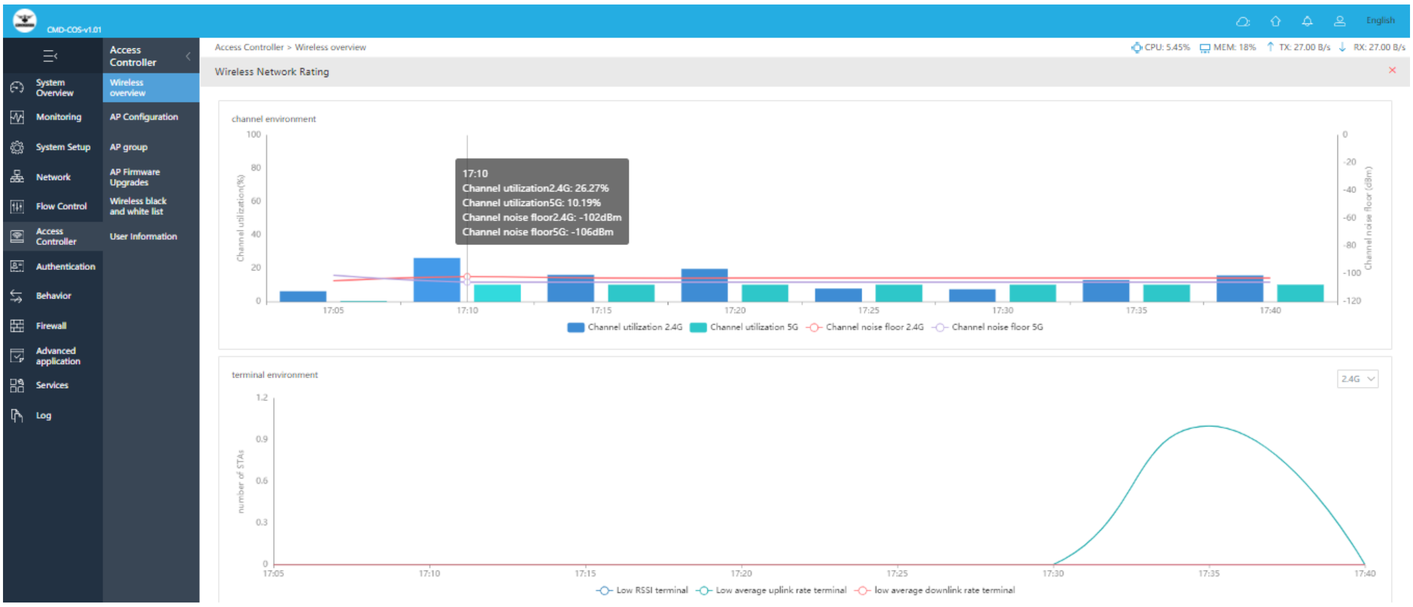
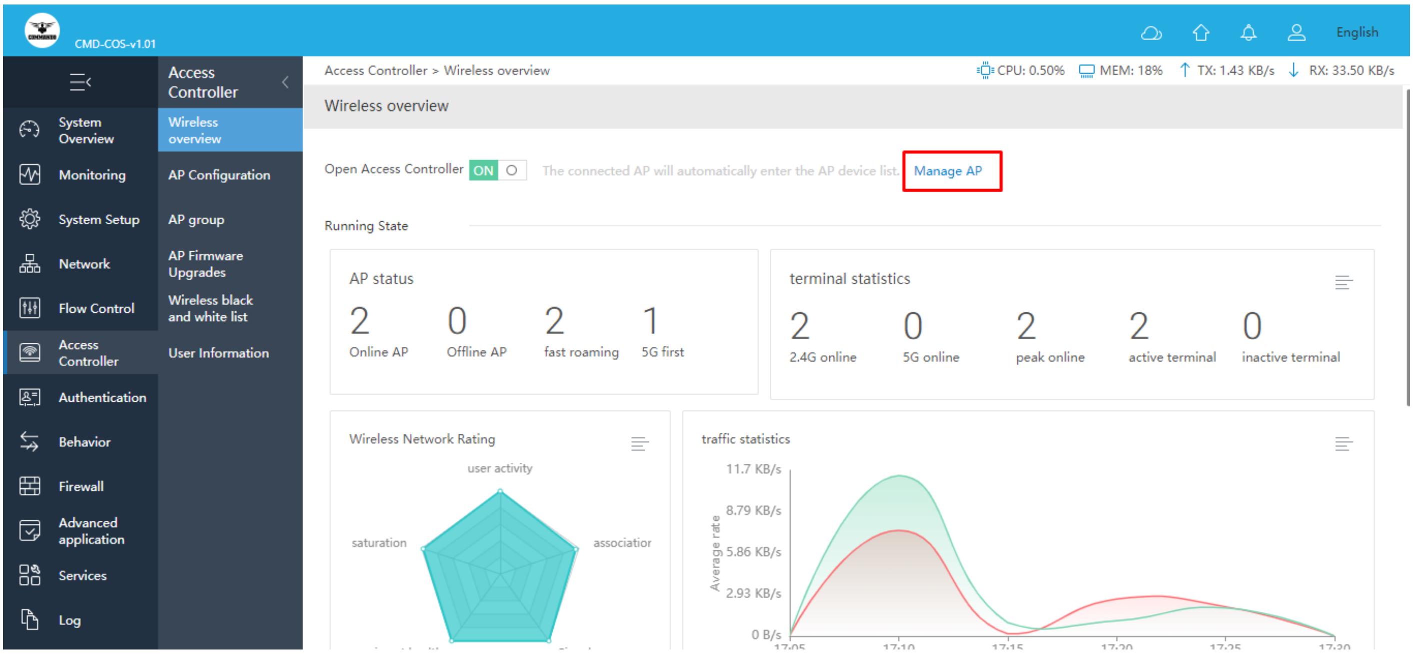


Fig 5.1.8 Wireless Network Rating channel and terminal environment page



The connected AP will automatically enter the AP device list.

Fig 5.1.9 Open Access Controller Manage AP page

It will direct with Access Controller > AP Configuration page.

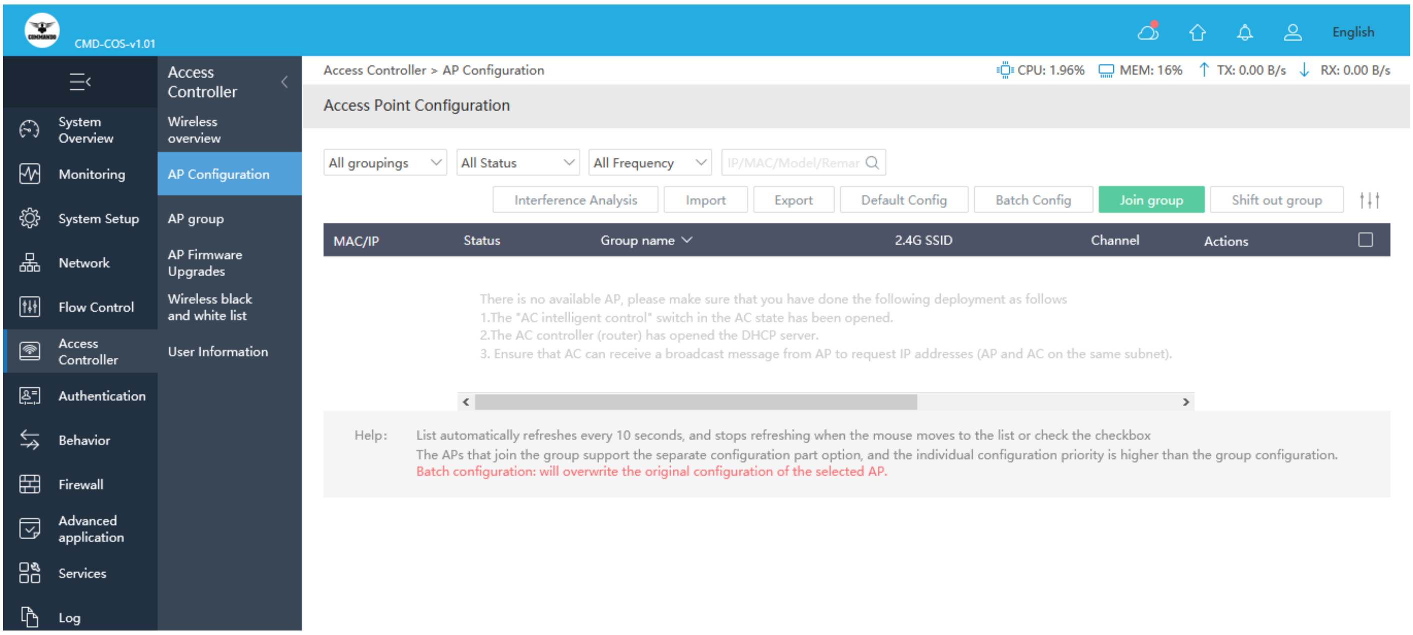
5.2 AP Configuration

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

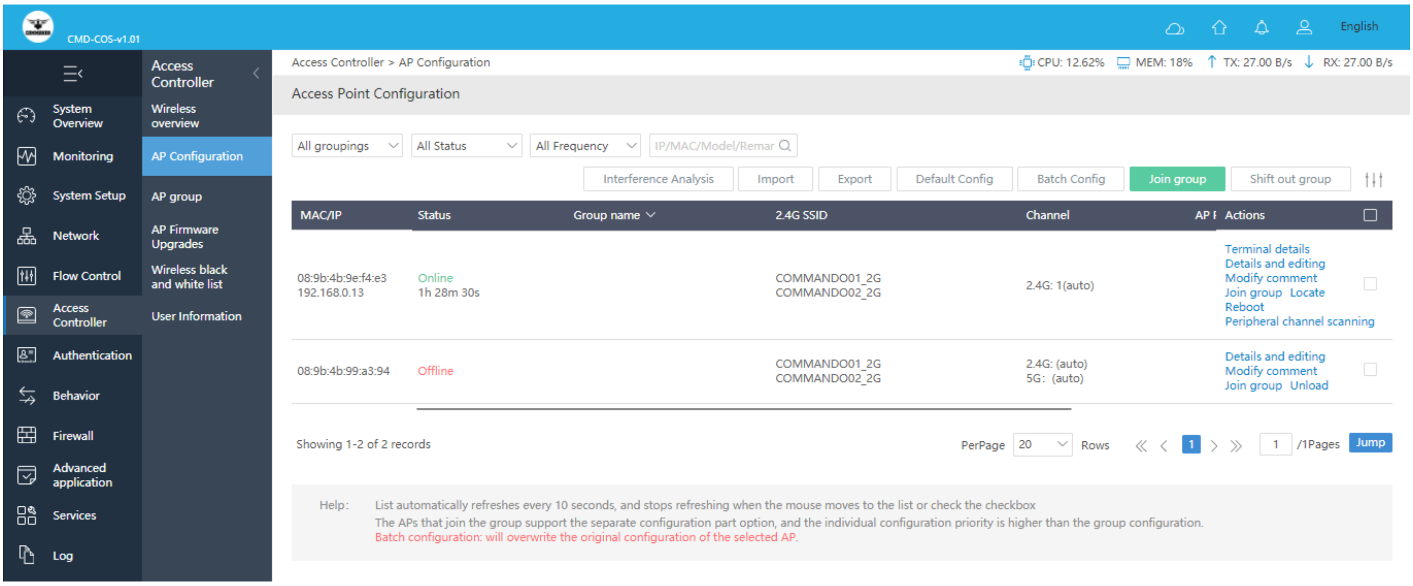
Note: List automatically refreshes every 10 seconds and stops refreshing when the mouse moves to the list or check the checkbox. The APs that join the group support the separate configuration part option, and the individual configuration priority is higher than the group configuration. Batch configuration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



There is no available AP, please make sure that you have done the following deployment as follows
1.The "AC intelligent control" switch in the AC state has been opened.
2.The AC controller (router) has opened the DHCP server.
3. Ensure that AC can receive a broadcast message from AP to request IP addresses (AP and AC on the same subnet).

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

Fig 5.2.1 Default Access Point Configuration page

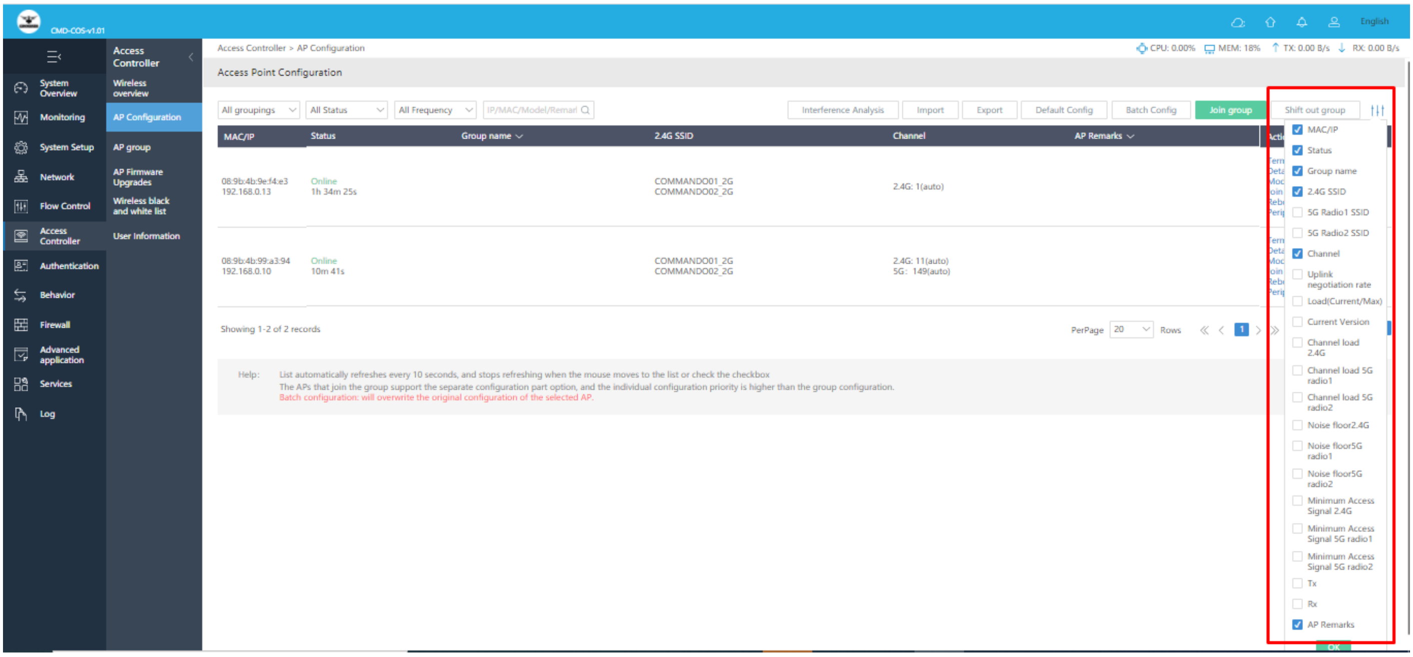


MAC/IP	Status	Group name	2.4G SSID	Channel	AP F	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 28m 30s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94	Offline		COMMANDO01_2G COMMANDO02_2G	2.4G: (auto) 5G: (auto)		Details and editing Modify comment Join group Unload	□

Showing 1-2 of 2 records

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

Fig 5.2.2 Access Point Configuration Online/Offline AP page



Access Controller > AP Configuration

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

Access Point Configuration

All groupings | All Status | All Frequency | IP/MAC/Model/Remarl

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

MAC/IP	Status	Group name	2.4G SSID	Channel	AP Remarks
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 34m 25s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto)	
08:9b:4b:99:a3:94 192.168.0.10	Online 10m 41s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)	

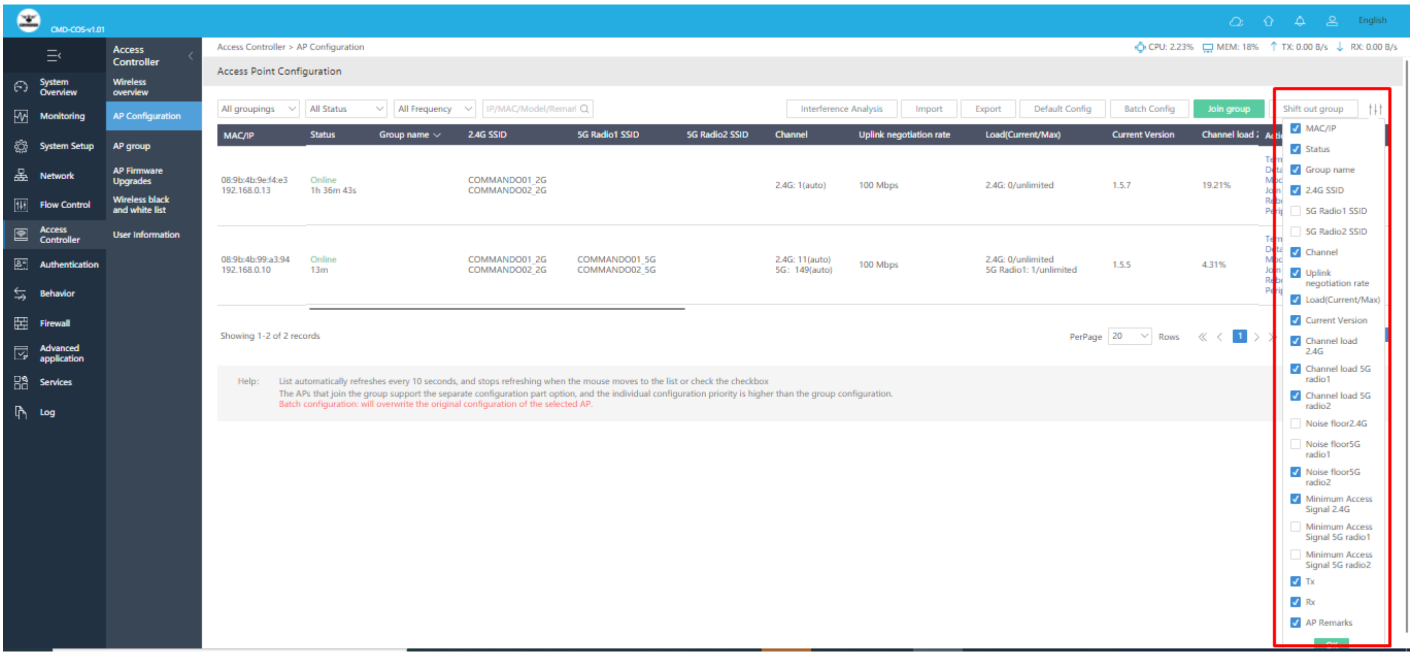
Showing 1-2 of 2 records

PerPage 20 Rows 1

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

- ☑ MAC/IP
- ☑ Status
- ☑ Group name
- ☑ 2.4G SSID
- □ 5G Radio1 SSID
- □ 5G Radio2 SSID
- ☑ Channel
- □ Uplink negotiation rate
- □ Load(Current/Max)
- □ Current Version
- □ Channel load 2.4G
- □ Channel load 5G radio1
- □ Channel load 5G radio2
- □ Noise floor2.4G
- □ Noise floor5G radio1
- □ Noise floor5G radio2
- □ Minimum Access Signal 2.4G
- □ Minimum Access Signal 5G radio1
- □ Minimum Access Signal 5G radio2
- □ Tx
- □ Rx
- ☑ AP Remarks

5.2.3 Access Point Configuration Default AP page



Access Controller > AP Configuration

CPU: 2.23% MEM: 18% TX: 0.00 B/s RX: 0.00 B/s

Access Point Configuration

All groupings | All Status | All Frequency | IP/MAC/Model/Remarl

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

MAC/IP	Status	Group name	2.4G SSID	5G Radio1 SSID	5G Radio2 SSID	Channel	Uplink negotiation rate	Load(Current/Max)	Current Version	Channel load 2
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 36m 43s		COMMANDO01_2G COMMANDO02_2G			2.4G: 1(auto)	100 Mbps	2.4G: 0/unlimited	1.5.7	19.21%
08:9b:4b:99:a3:94 192.168.0.10	Online 13m		COMMANDO01_2G COMMANDO02_2G	COMMANDO01_5G COMMANDO02_5G		2.4G: 11(auto) 5G: 149(auto)	100 Mbps	2.4G: 0/unlimited 5G Radio1: 1/unlimited	1.5.5	4.31%

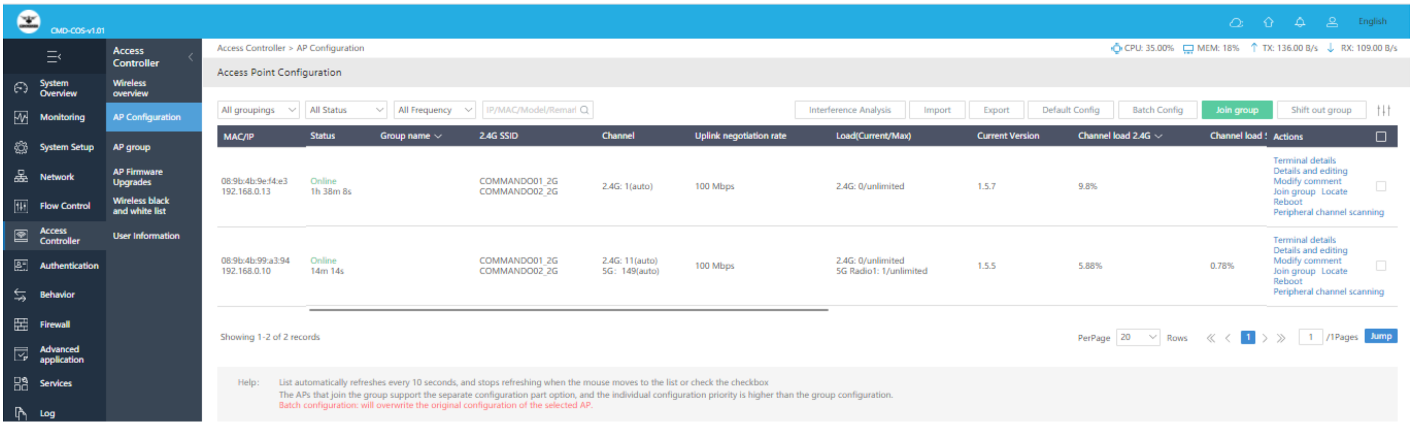
Showing 1-2 of 2 records

PerPage 20 Rows 1

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

- ☑ MAC/IP
- ☑ Status
- ☑ Group name
- ☑ 2.4G SSID
- □ 5G Radio1 SSID
- □ 5G Radio2 SSID
- ☑ Channel
- ☑ Uplink negotiation rate
- ☑ Load(Current/Max)
- ☑ Current Version
- ☑ Channel load 2.4G
- ☑ Channel load 5G radio1
- ☑ Channel load 5G radio2
- □ Noise floor2.4G
- □ Noise floor5G radio1
- ☑ Noise floor5G radio2
- ☑ Minimum Access Signal 2.4G
- □ Minimum Access Signal 5G radio1
- □ Minimum Access Signal 5G radio2
- ☑ Tx
- ☑ Rx
- ☑ AP Remarks

Fig 5.2.4 Access Point Configuration Customize display page

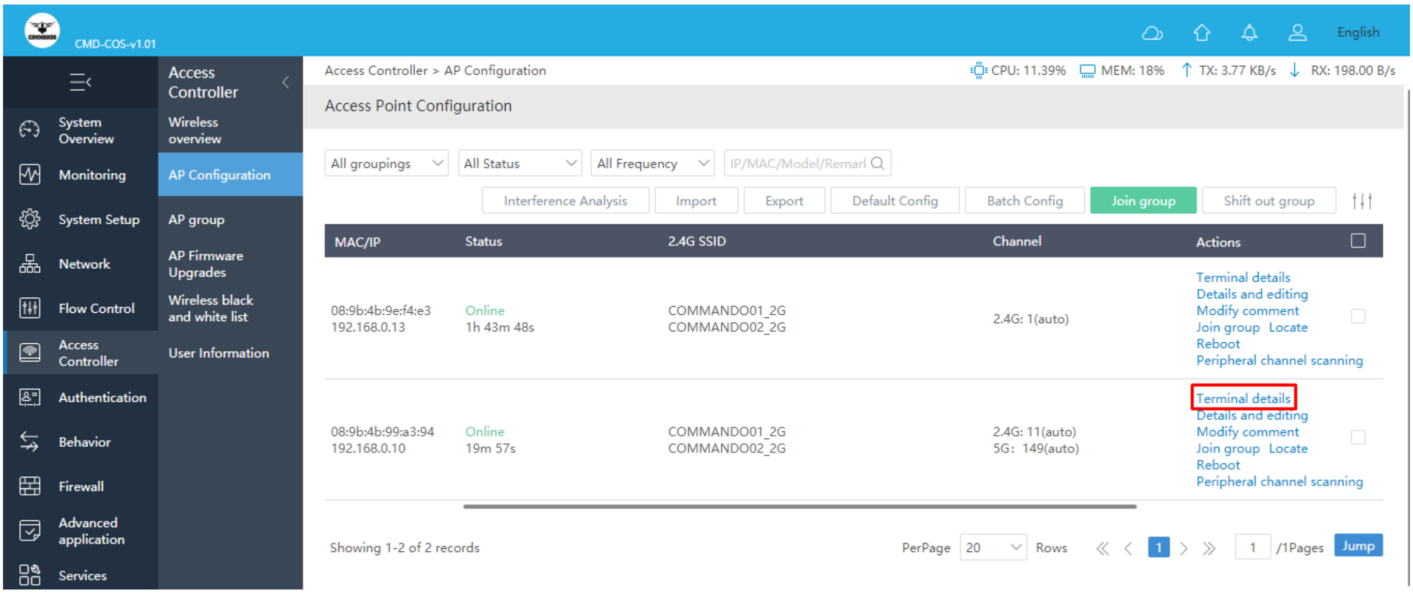


MAC/IP	Status	Group name	2.4G SSID	Channel	Uplink negotiation rate	Load(Current/Max)	Current Version	Channel load 2.4G	Channel load !	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 38m 8s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto)	100 Mbps	2.4G: 0/unlimited	1.5.7	9.8%		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 14m 14s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)	100 Mbps	2.4G: 0/unlimited 5G Radio1: 1/unlimited	1.5.5	5.88%	0.78%	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

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

Fig 5.2.5 Access Point Configuration Customized AP page

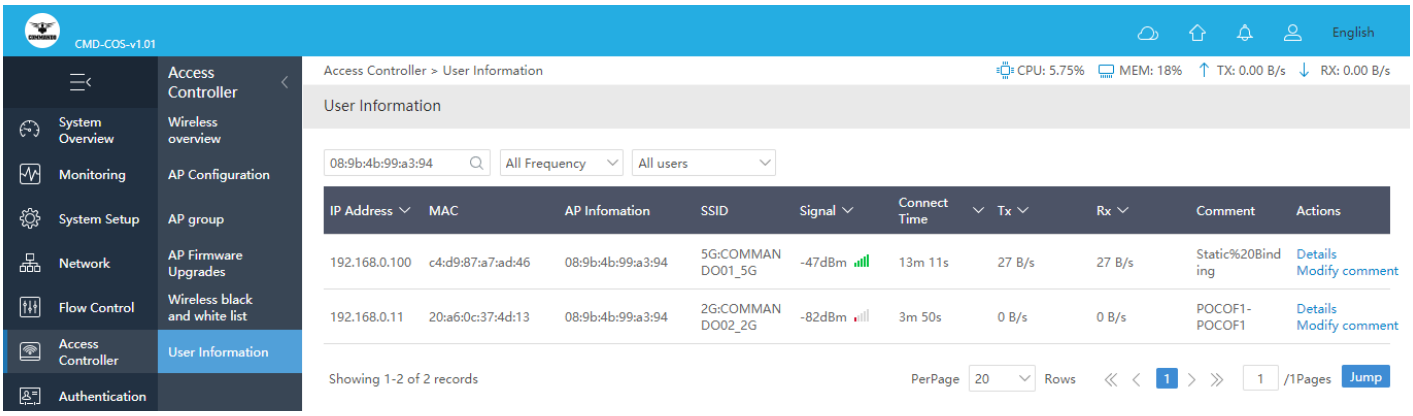


MAC/IP	Status	2.4G SSID	Channel	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 43m 48s	COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto)	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 19m 57s	COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

Fig 5.2.6 Access Point Configuration Terminal Details page

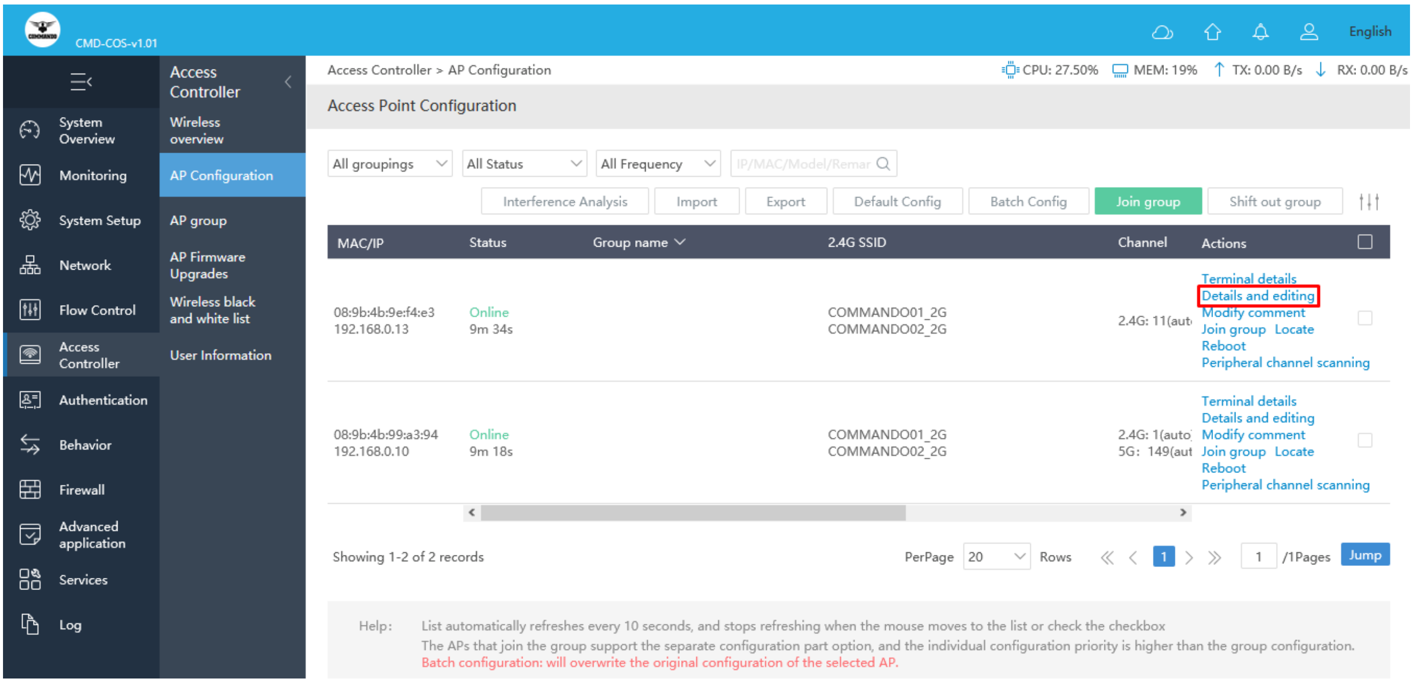
After clicking above highlighted icon you will be directed to User Information page as if you clicked Access Controller > User Information for particular AP page will be displayed.



IP Address	MAC	AP Infomation	SSID	Signal	Connect Time	Tx	Rx	Comment	Actions
192.168.0.100	c4:d9:87:a7:ad:46	08:9b:4b:99:a3:94	5G:COMMANDO01_5G	-47dBm	13m 11s	27 B/s	27 B/s	Static%20Binding	Details Modify comment
192.168.0.11	20:a6:0c:37:4d:13	08:9b:4b:99:a3:94	2G:COMMANDO02_2G	-82dBm	3m 50s	0 B/s	0 B/s	POCOF1-POCOF1	Details Modify comment

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

Fig 5.2.7 Access Point Configuration Terminal Details page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

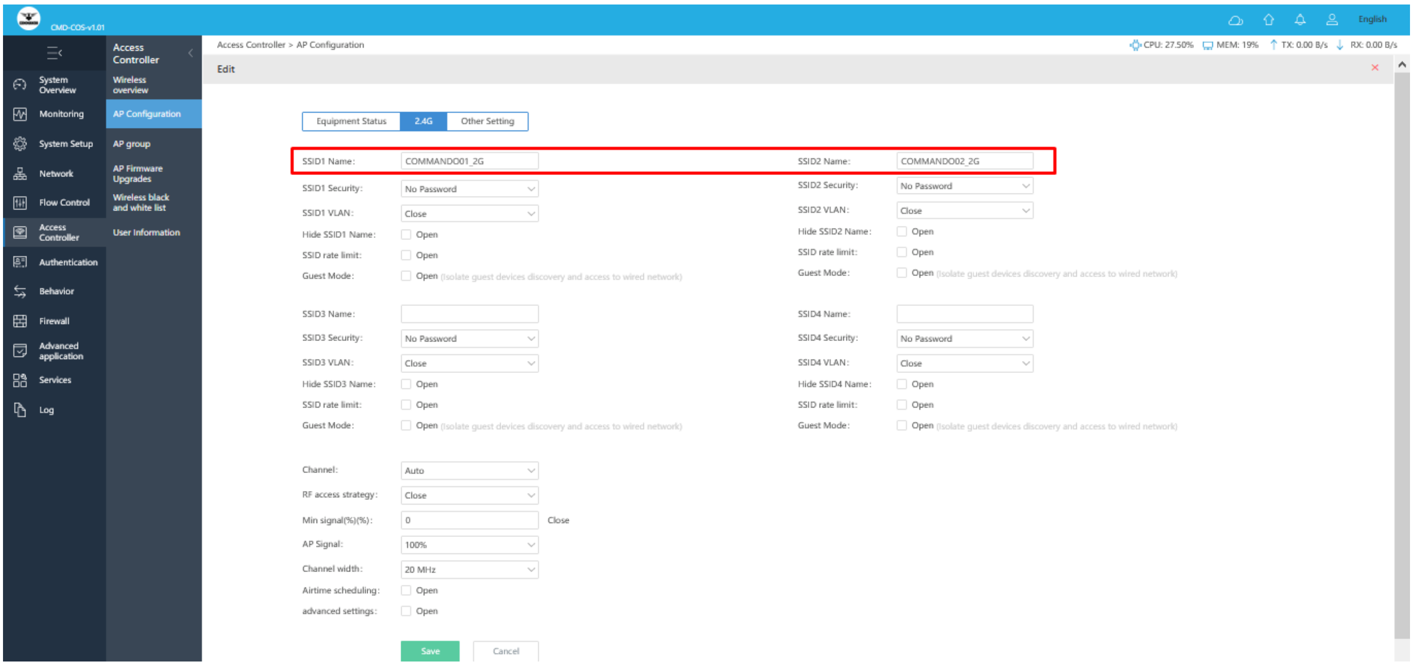
Access Point Configuration

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

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages

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

Fig 5.2.8 Details and editing AP Configuration page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Edit

SSID1 Name: COMMANDO01_2G
SSID1 Security: No Password
SSID1 VLAN: Close
Hide SSID1 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID2 Name: COMMANDO02_2G
SSID2 Security: No Password
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID3 Name:
SSID3 Security: No Password
SSID3 VLAN: Close
Hide SSID3 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

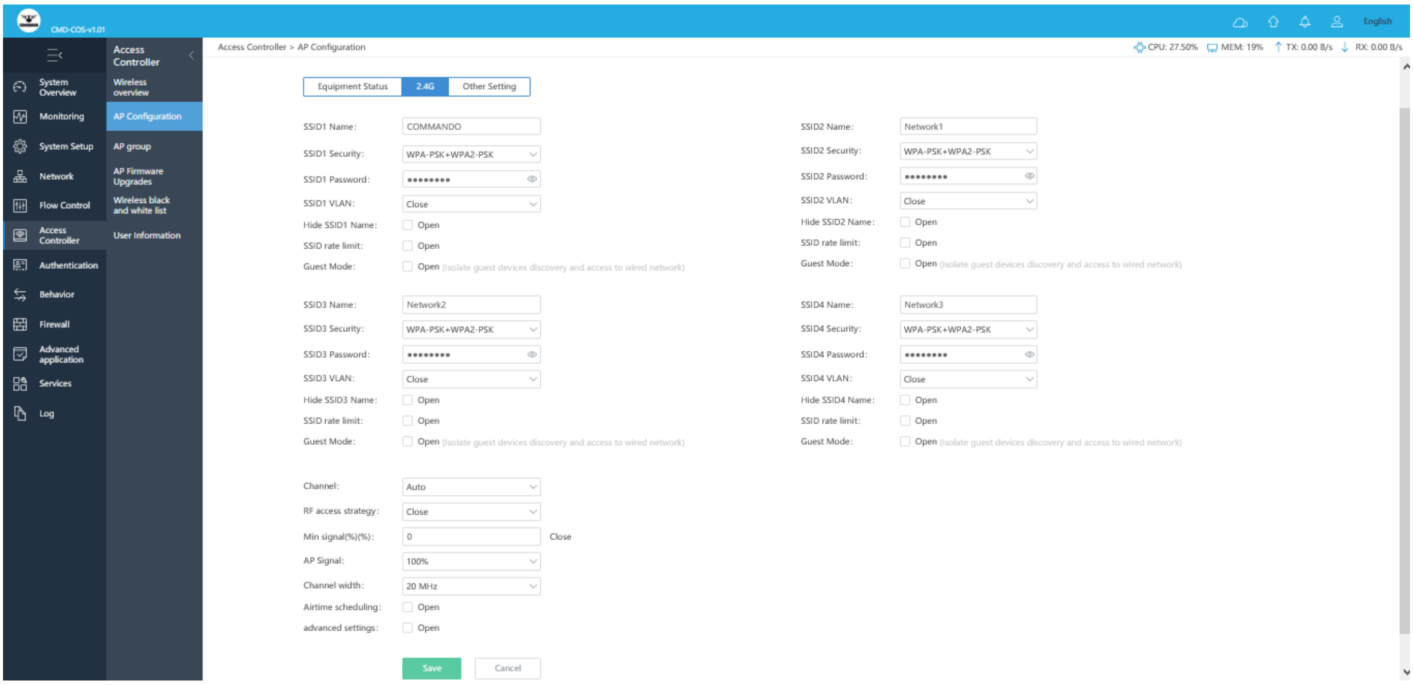
SSID4 Name:
SSID4 Security: No Password
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

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

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.



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

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

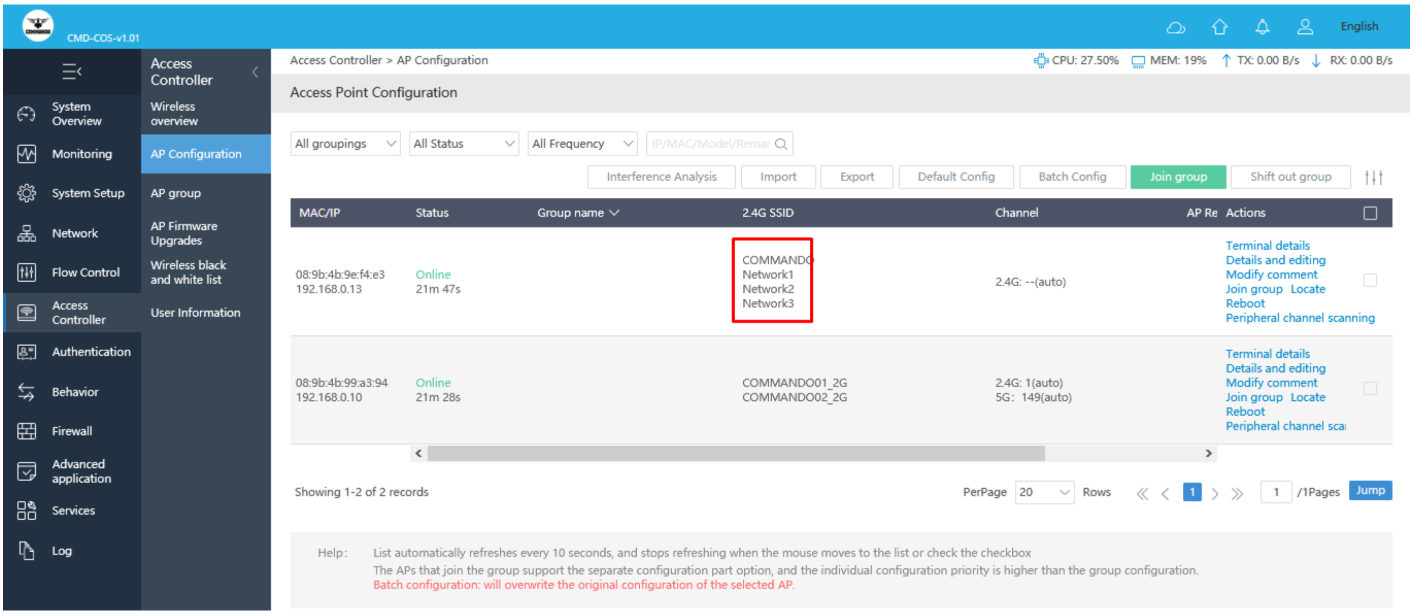
SSID2 Name: Network1
SSID2 Security: WPA-PSK+WPA2-PSK
SSID2 Password: ••••••••
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID3 Name: Network2
SSID3 Security: WPA-PSK+WPA2-PSK
SSID3 Password: ••••••••
SSID3 VLAN: Close
Hide SSID3 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID4 Name: Network3
SSID4 Security: WPA-PSK+WPA2-PSK
SSID4 Password: ••••••••
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

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

Fig 5.2.10 Changing SSID Configuration page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Access Point Configuration

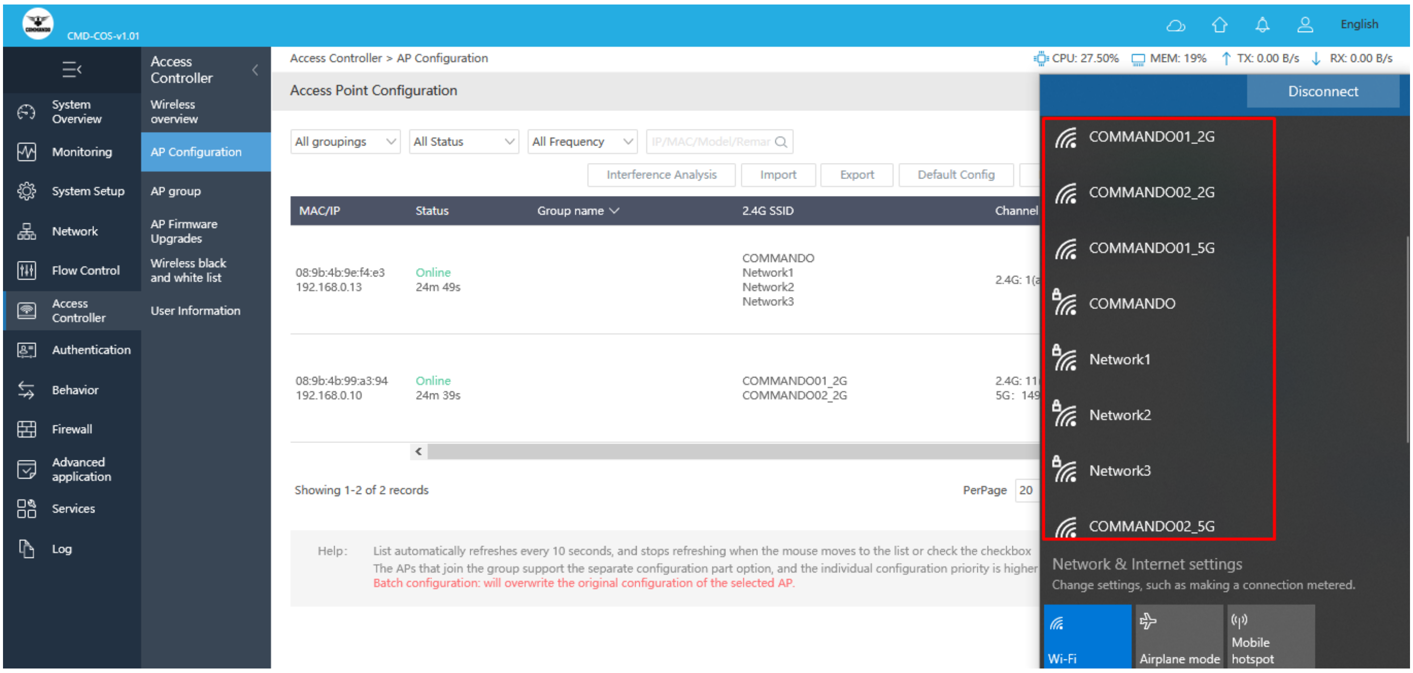
MAC/IP	Status	Group name	2.4G SSID	Channel	AP Re	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 21m 47s		COMMANDO Network1 Network2 Network3	2.4G: --(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 21m 28s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scai	□

Showing 1-2 of 2 records

1 /1Pages

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

Fig 5.2.11 AP configuration after Changing SSID Configuration page



MAC/IP	Status	Group name	2.4G SSID	Channel
08:9b:4b:9e:f4:e3 192.168.0.13	Online 24m 49s		COMMANDO Network1 Network2 Network3	2.4G: 1(a
08:9b:4b:99:a3:94 192.168.0.10	Online 24m 39s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11 5G: 149

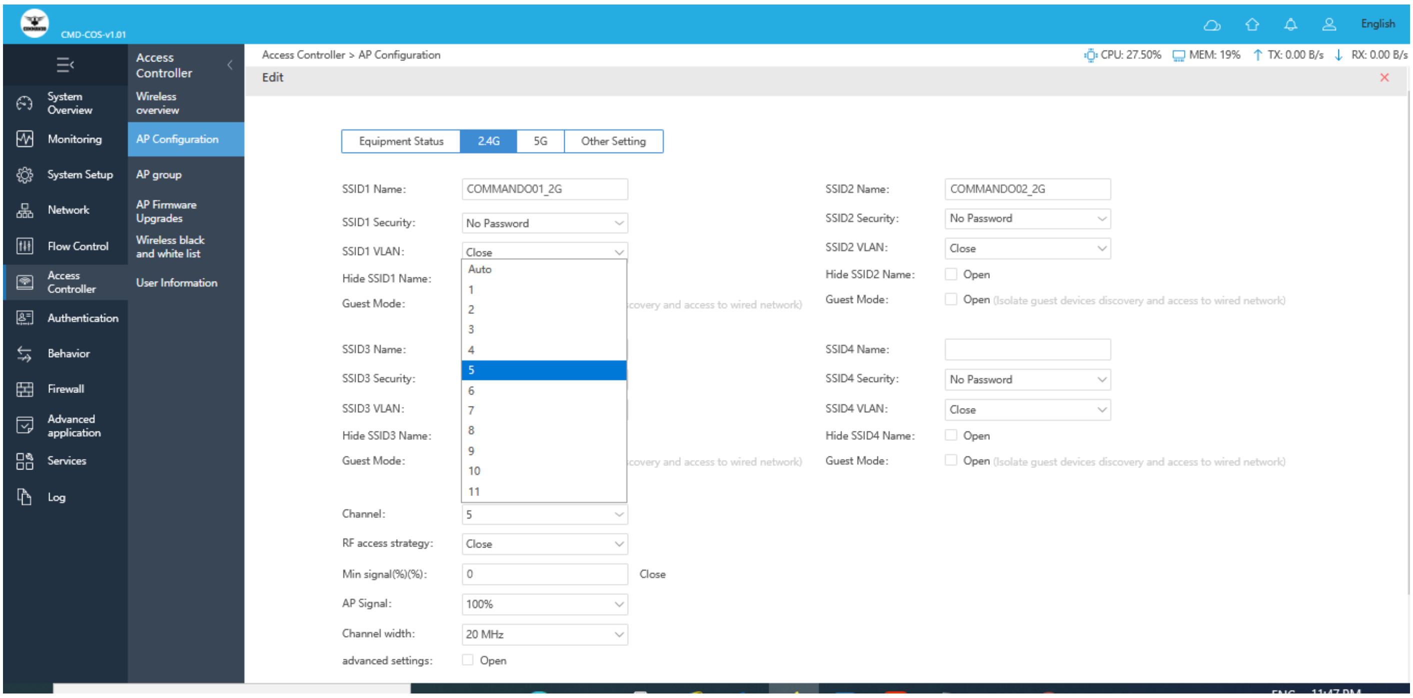
Showing 1-2 of 2 records PerPage 20

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

Fig 5.2.12 SSID available for users page

How to set up manually Selected channel?

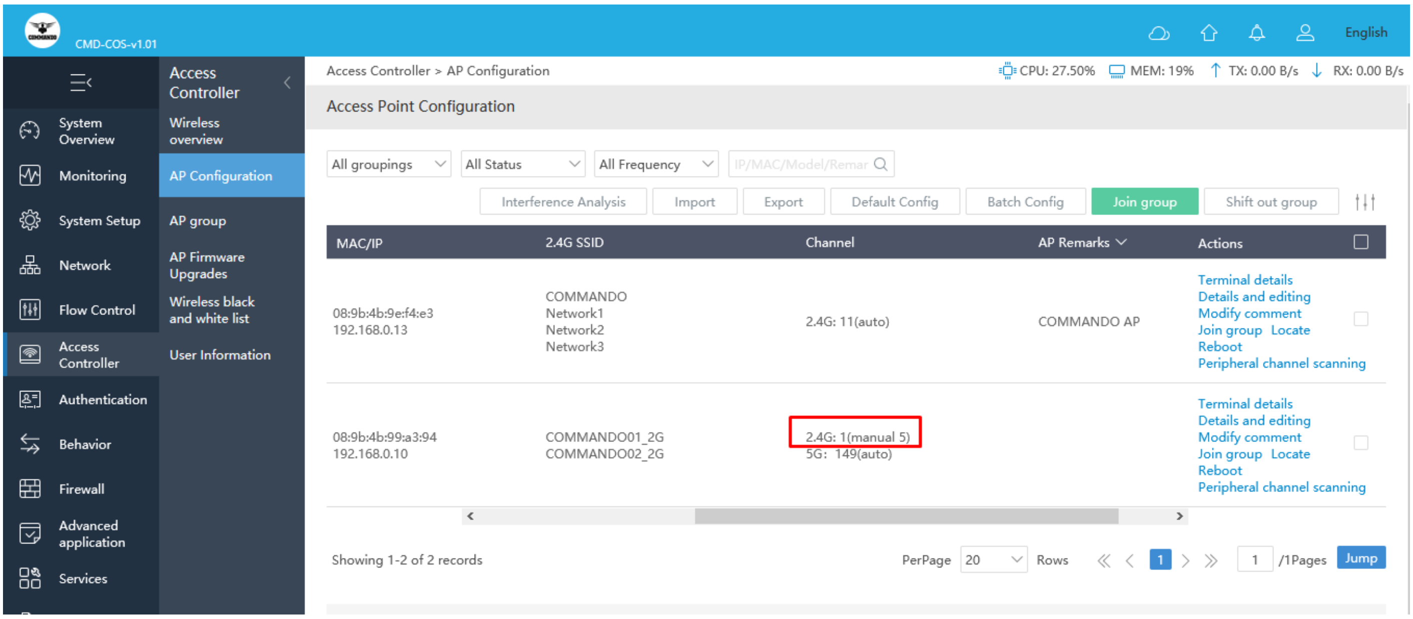
Direct communication between an 802.11 client radio and an access point occurs over a common ISM Band channel frequency. You set the channel manually or auto in the access point, if you set radio card automatically tunes its transceiver to the frequency of the access point having the strongest signal.



SSID1 Name: COMMANDO01_2G
SSID1 Security: No Password
SSID1 VLAN: Close
Hide SSID1 Name:
Guest Mode: covery and access to wired network)
SSID3 Name:
SSID3 Security:
SSID3 VLAN:
Hide SSID3 Name:
Guest Mode: covery and access to wired network)
Channel: 5
RF access strategy: Close
Min signal(%)(%): 0 Close
AP Signal: 100%
Channel width: 20 MHz
advanced settings: □ Open

SSID2 Name: COMMANDO02_2G
SSID2 Security: No Password
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)
SSID4 Name:
SSID4 Security: No Password
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

Fig 5.2.12 Changing Channel for SSID page

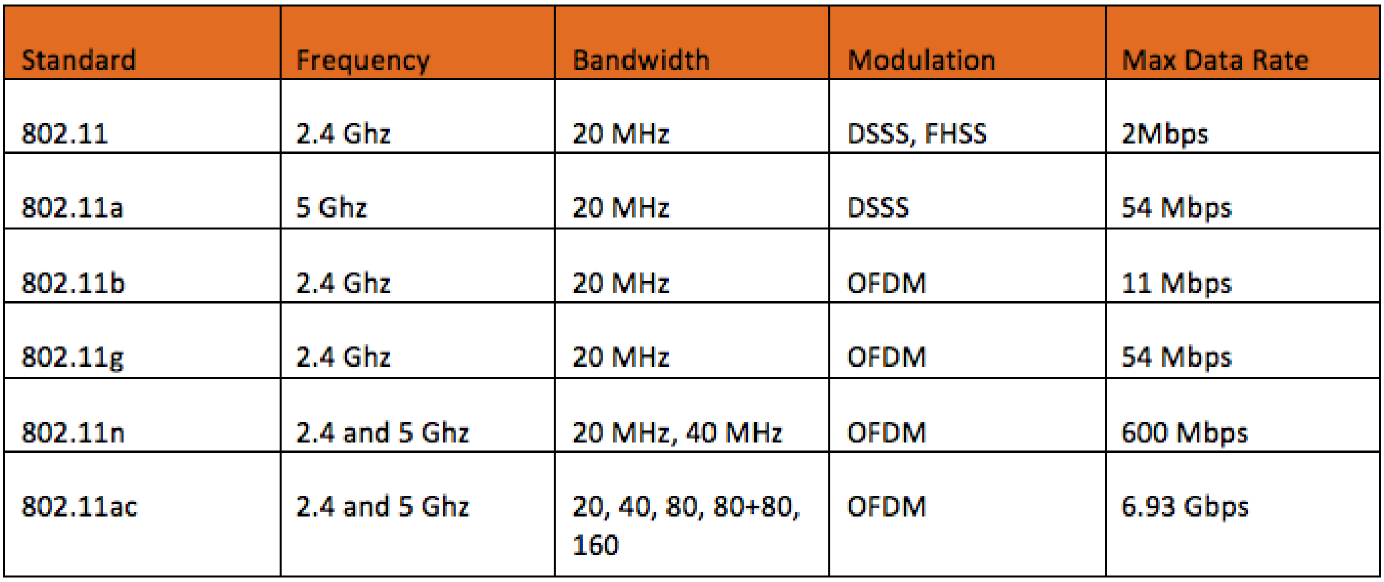


MAC/IP	2.4G SSID	Channel	AP Remarks	Actions
08:9b:4b:9e:f4:e3 192.168.0.13	COMMANDO Network1 Network2 Network3	2.4G: 11(auto)	COMMANDO AP	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning
08:9b:4b:99:a3:94 192.168.0.10	COMMANDO01_2G COMMANDO02_2G	2.4G: 1(manual 5) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

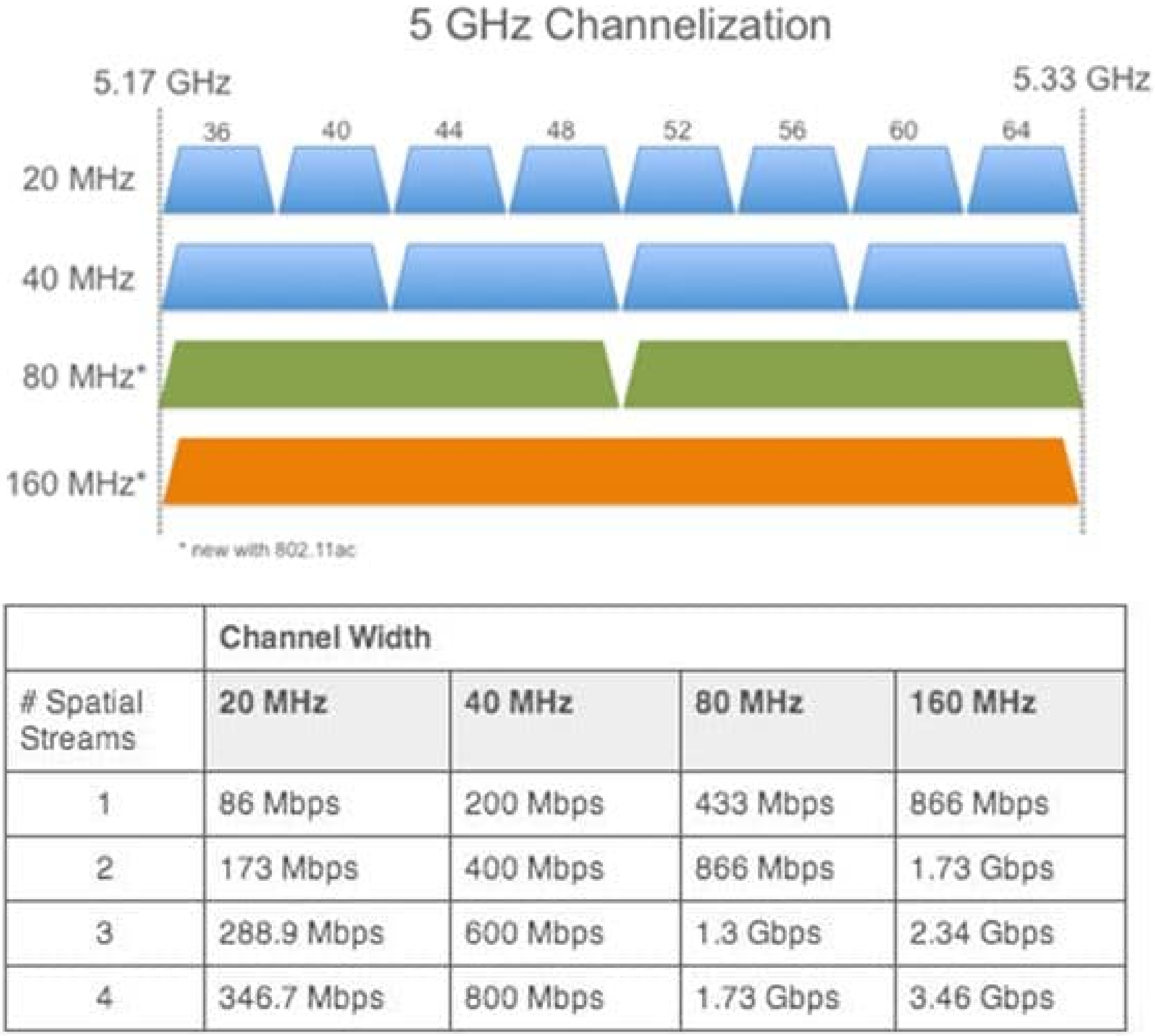
Showing 1-2 of 2 records

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.

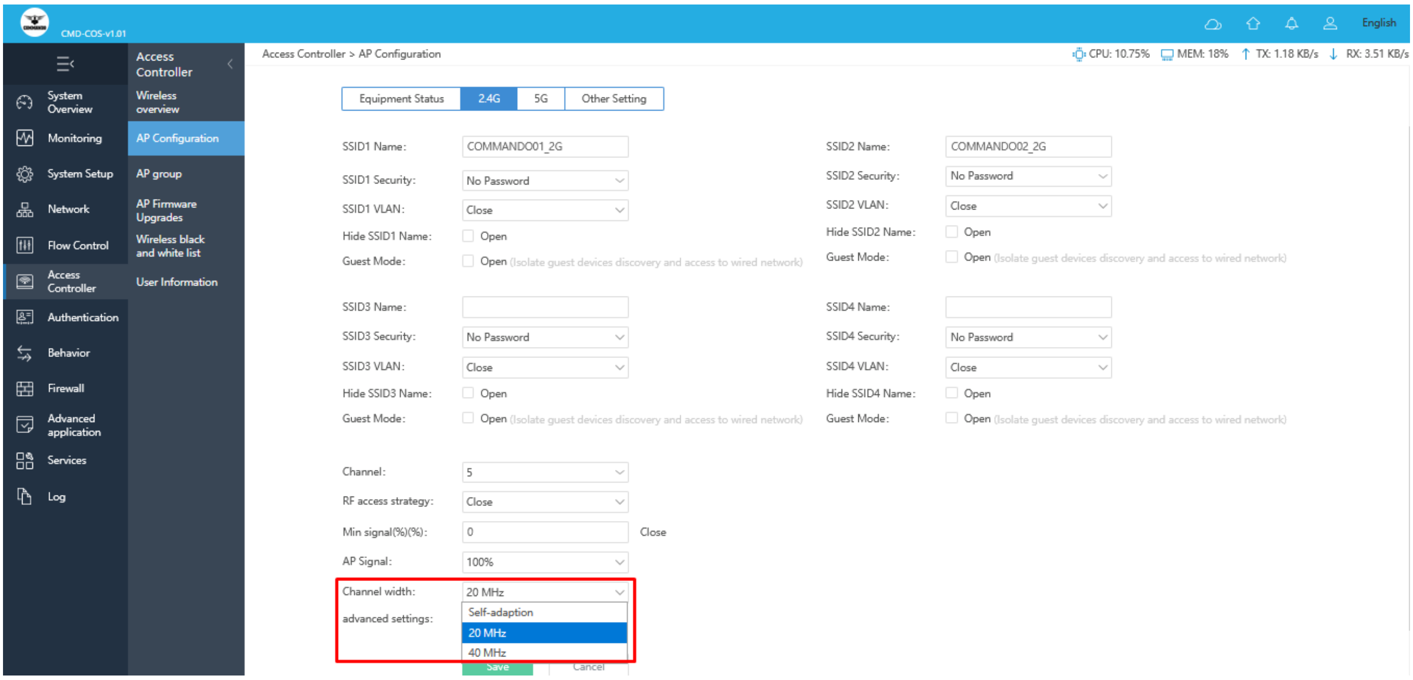


Standard	Frequency	Bandwidth	Modulation	Max Data Rate
802.11	2.4 Ghz	20 MHz	DSSS, FHSS	2Mbps
802.11a	5 Ghz	20 MHz	DSSS	54 Mbps
802.11b	2.4 Ghz	20 MHz	OFDM	11 Mbps
802.11g	2.4 Ghz	20 MHz	OFDM	54 Mbps
802.11n	2.4 and 5 Ghz	20 MHz, 40 MHz	OFDM	600 Mbps
802.11ac	2.4 and 5 Ghz	20, 40, 80, 80+80, 160	OFDM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



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

Fig 5.2.14 Channel Width and Max. Data rate relation



Access Controller > AP Configuration

CPU: 10.75% MEM: 18% TX: 1.18 KB/s RX: 3.51 KB/s

SSID1 Name: COMMANDO01_2G

SSID1 Security: No Password

SSID1 VLAN: Close

Hide SSID1 Name: □ Open

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

SSID2 Name: COMMANDO02_2G

SSID2 Security: No Password

SSID2 VLAN: Close

Hide SSID2 Name: □ Open

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

SSID3 Name:

SSID3 Security: No Password

SSID3 VLAN: Close

Hide SSID3 Name: □ Open

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

SSID4 Name:

SSID4 Security: No Password

SSID4 VLAN: Close

Hide SSID4 Name: □ Open

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

Channel: 5

RF access strategy: Close

Min signal(%)(%): 0 Close

AP Signal: 100%

Channel width: 20 MHz

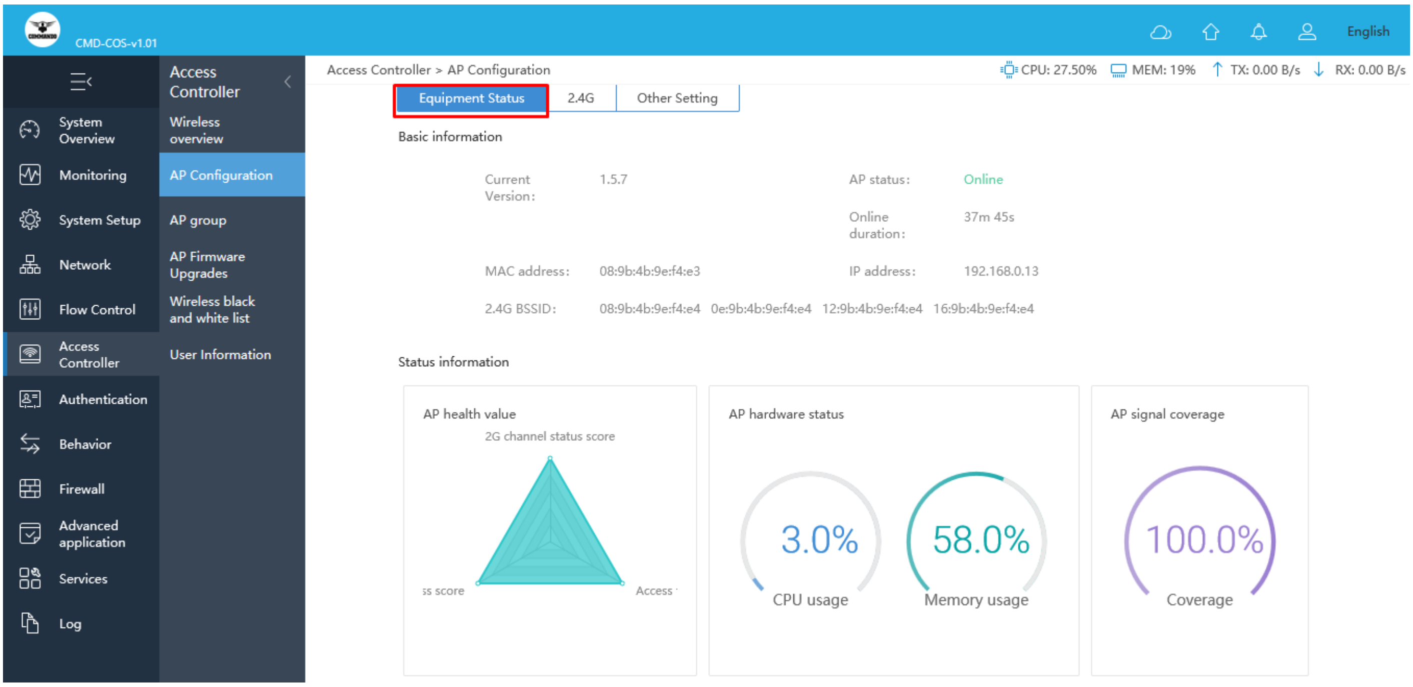
advanced settings:

Self-adaption

20 MHz

40 MHz

Fig 5.2.15 Changing Channel Width for AP configuration page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Basic information

Current Version: 1.5.7

AP status: Online

Online duration: 37m 45s

MAC address: 08:9b:4b:9e:f4:e3

IP address: 192.168.0.13

2.4G BSSID: 08:9b:4b:9e:f4:e4 0e:9b:4b:9e:f4:e4 12:9b:4b:9e:f4:e4 16:9b:4b:9e:f4:e4

Status information

AP health value

AP hardware status

AP signal coverage

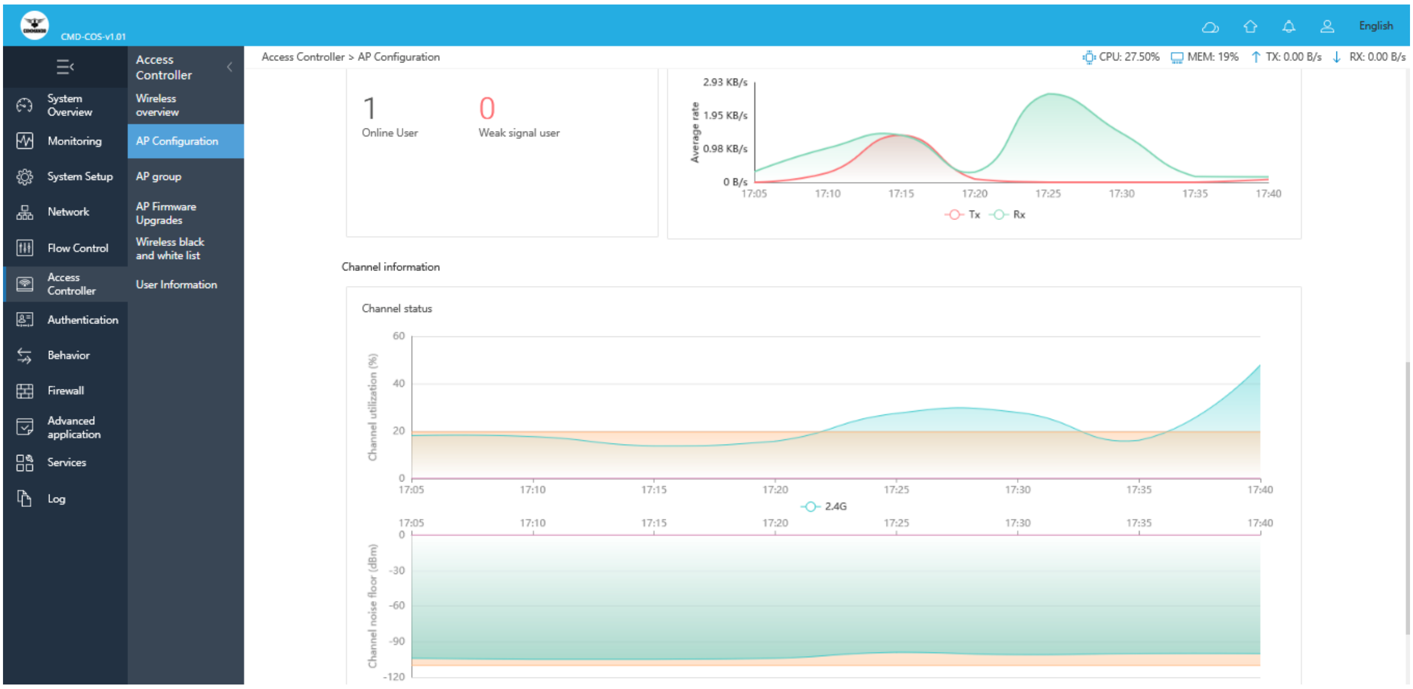
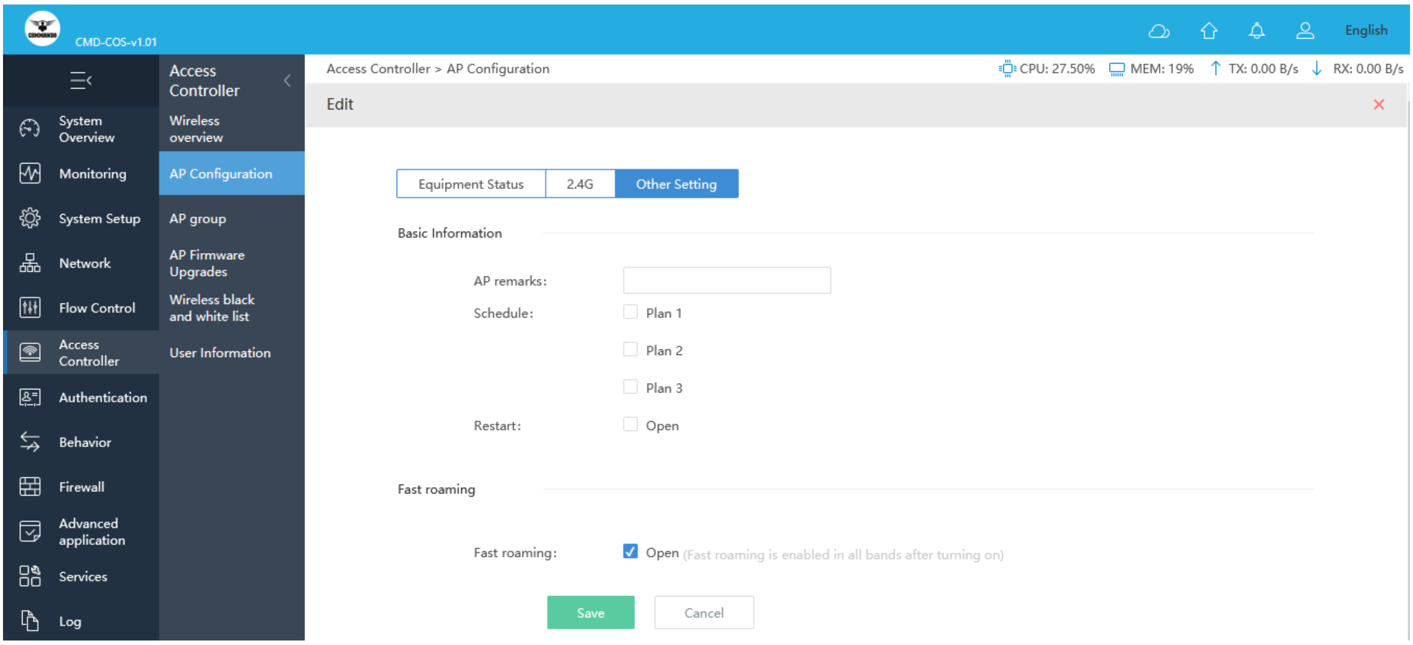


Fig 5.2.16 Equipment Status of AP page

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.



Basic Information

AP remarks:

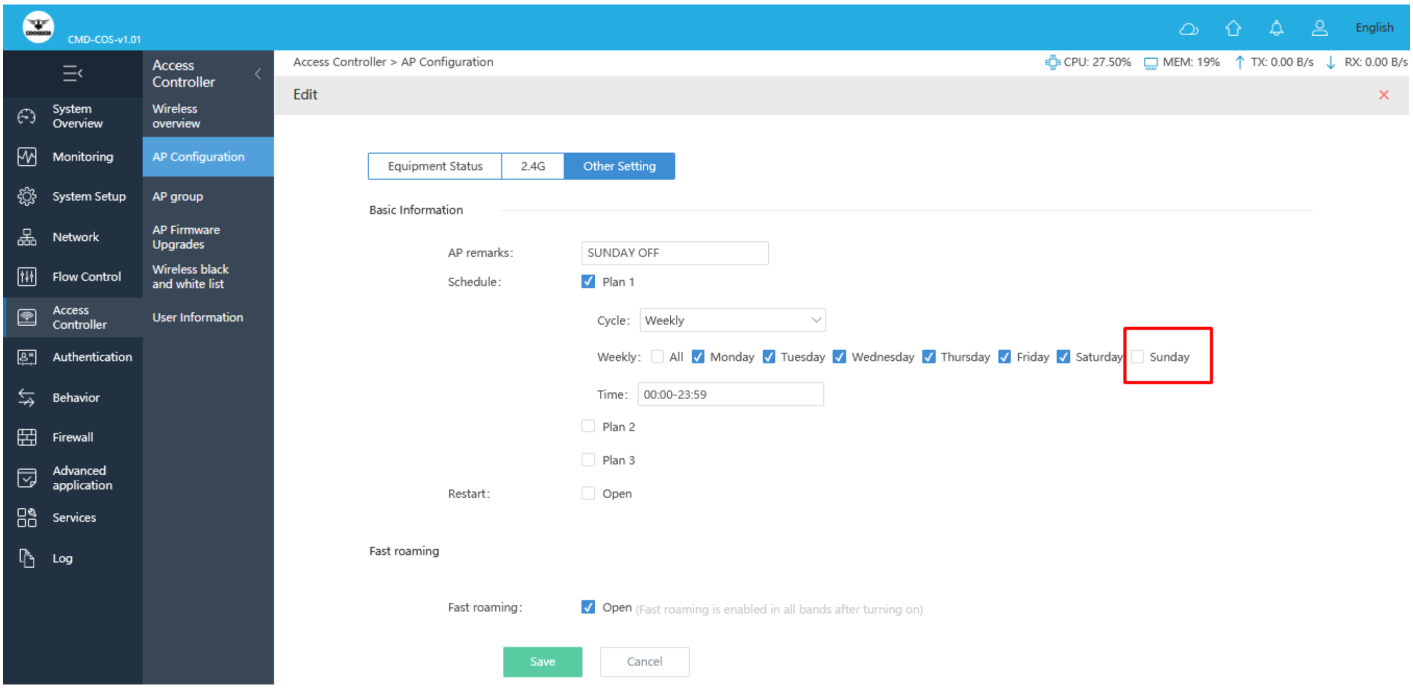
Schedule: □ Plan 1 □ Plan 2 □ Plan 3

Restart: □ Open

Fast roaming

Fast roaming: ☑ Open (Fast roaming is enabled in all bands after turning on)

Fig 5.2.17 Default Other Setting of AP configuration page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Edit

Basic Information

AP remarks: SUNDAY OFF

Schedule: ☑ Plan 1

Cycle: Weekly

Weekly: □ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday □ Sunday

Time: 00:00-23:59

□ Plan 2

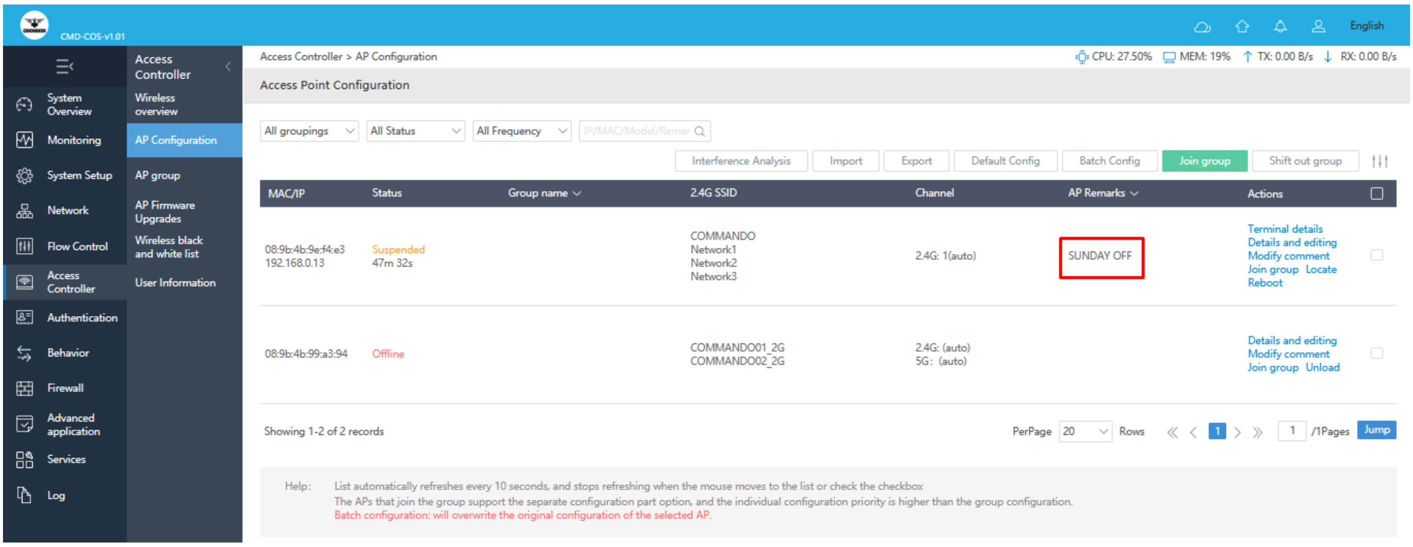
□ Plan 3

Restart: □ Open

Fast roaming

Fast roaming: ☑ Open (Fast roaming is enabled in all bands after turning on)

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



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

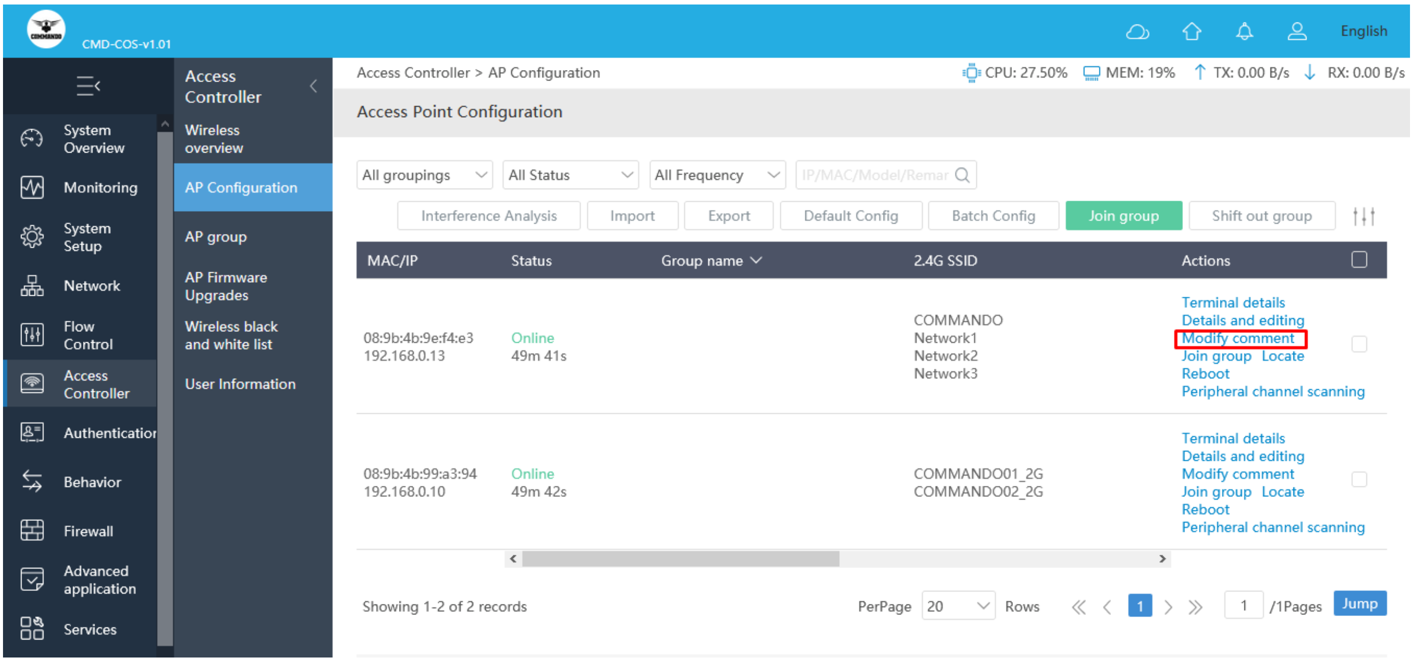
Access Point Configuration

MAC/IP	Status	Group name	2.4G SSID	Channel	AP Remarks	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Suspended 47m 32s		COMMANDO Network1 Network2 Network3	2.4G: 1(auto)	SUNDAY OFF	Terminal details Details and editing Modify comment Join group Locate Reboot	□
08:9b:4b:99:a3:94	Offline		COMMANDO01_2G COMMANDO02_2G	2.4G: (auto) 5G: (auto)		Details and editing Modify comment Join group Unload	□

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages

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

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



Access Controller > AP Configuration

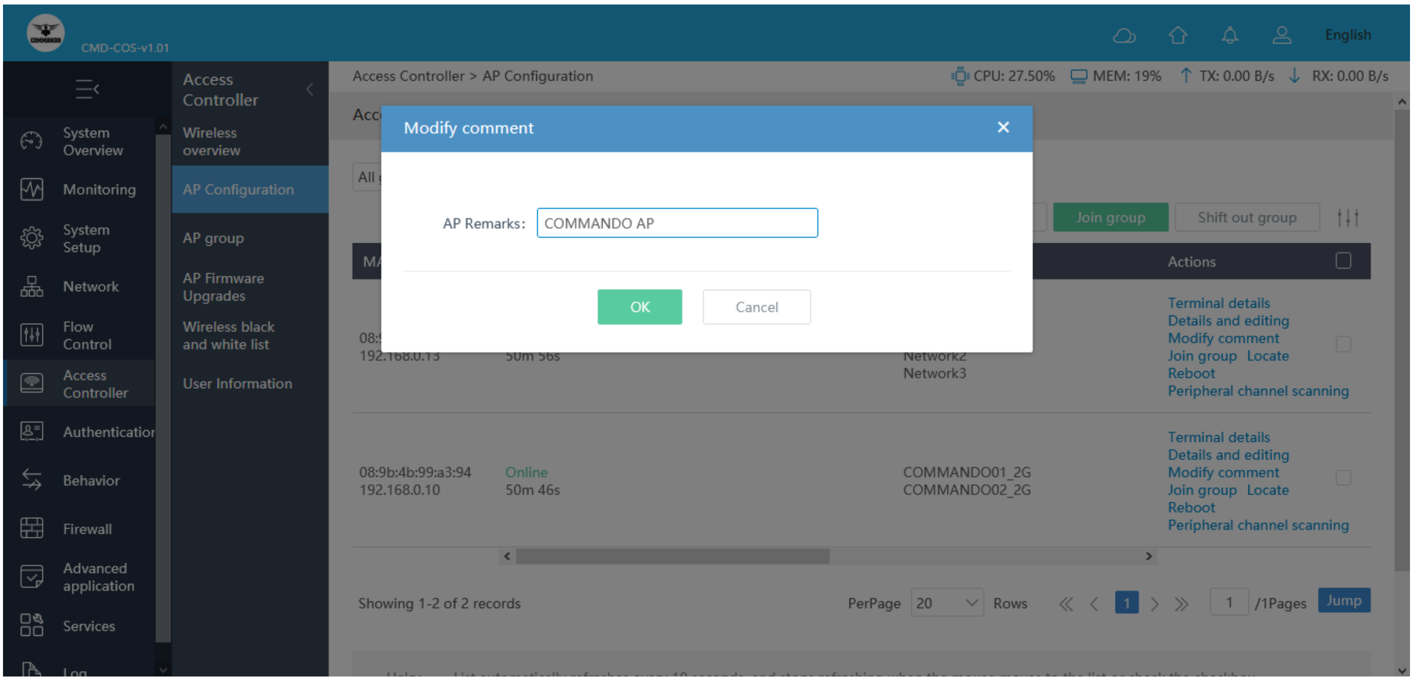
CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Access Point Configuration

MAC/IP	Status	Group name	2.4G SSID	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 49m 41s		COMMANDO Network1 Network2 Network3	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 49m 42s		COMMANDO01_2G COMMANDO02_2G	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

Showing 1-2 of 2 records PerPage 20 Rows 1 /1Pages

Fig 5.2.20 Modify Comment page



Modify comment

AP Remarks: COMMANDO AP

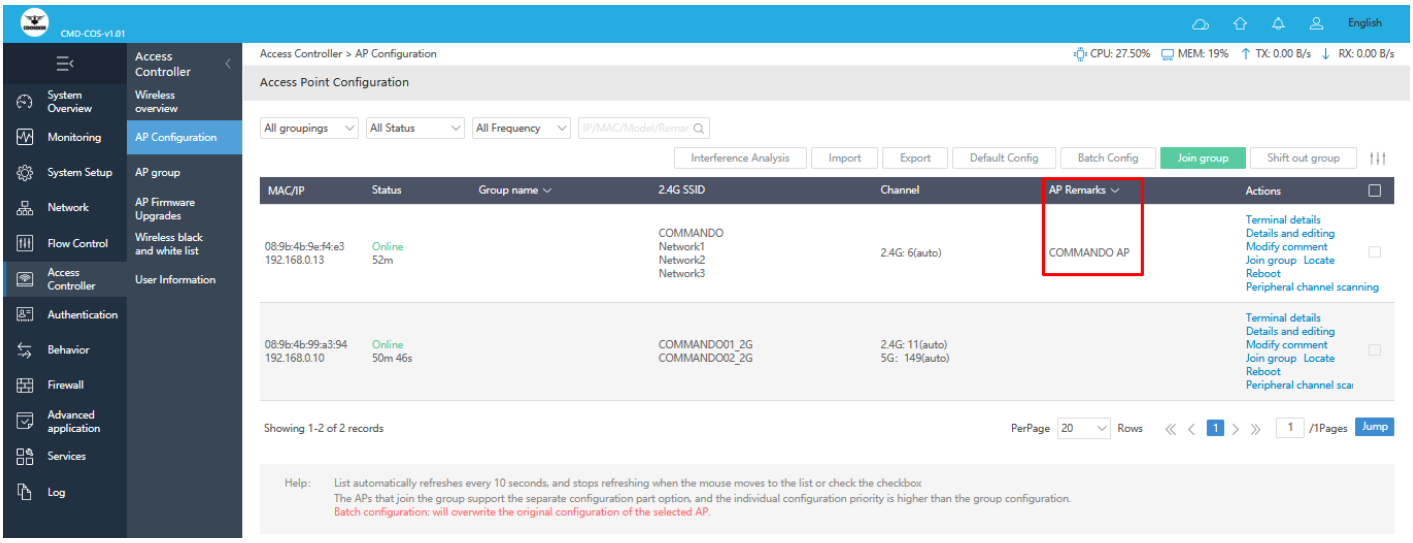
Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

MAC/IP	Status	2.4G SSID	Actions
08:9b:4b:9e:f4:e3 192.168.0.13	50m 56s	Network2 Network3	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning
08:9b:4b:99:a3:94 192.168.0.10	Online 50m 46s	COMMANDO01_2G COMMANDO02_2G	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

Showing 1-2 of 2 records PerPage 20 Rows 1 /1Pages

Fig 5.2.21 Changing Modify Comment page



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Access Point Configuration

MAC/IP	Status	Group name	2.4G SSID	Channel	AP Remarks	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 52m		COMMANDO Network1 Network2 Network3	2.4G: 6(auto)	COMMANDO AP	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 50m 46s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scai	□

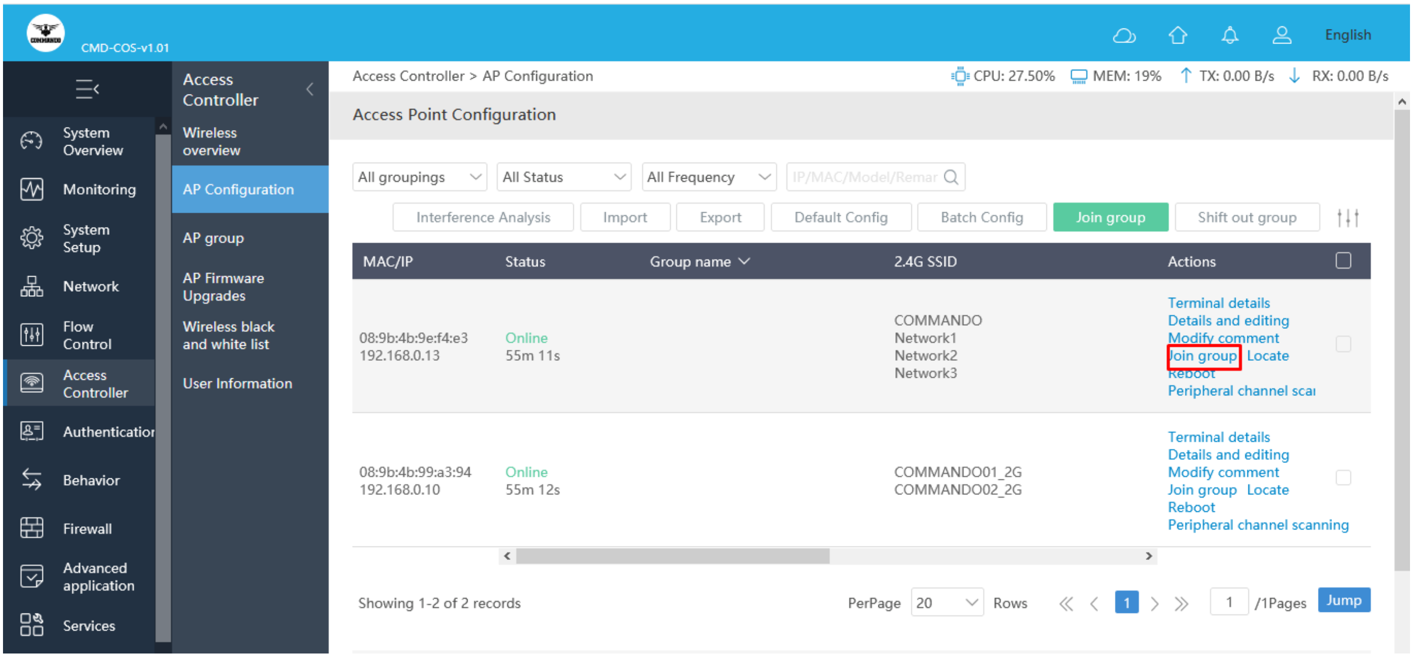
Showing 1-2 of 2 records

PerPage 20 Rows 1 1 /1Pages Jump

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

Fig 5.2.22 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.



Access Controller > AP Configuration

CPU: 27.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Access Point Configuration

MAC/IP	Status	Group name	2.4G SSID	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 55m 11s		COMMANDO Network1 Network2 Network3	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scai	□
08:9b:4b:99:a3:94 192.168.0.10	Online 55m 12s		COMMANDO01_2G COMMANDO02_2G	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

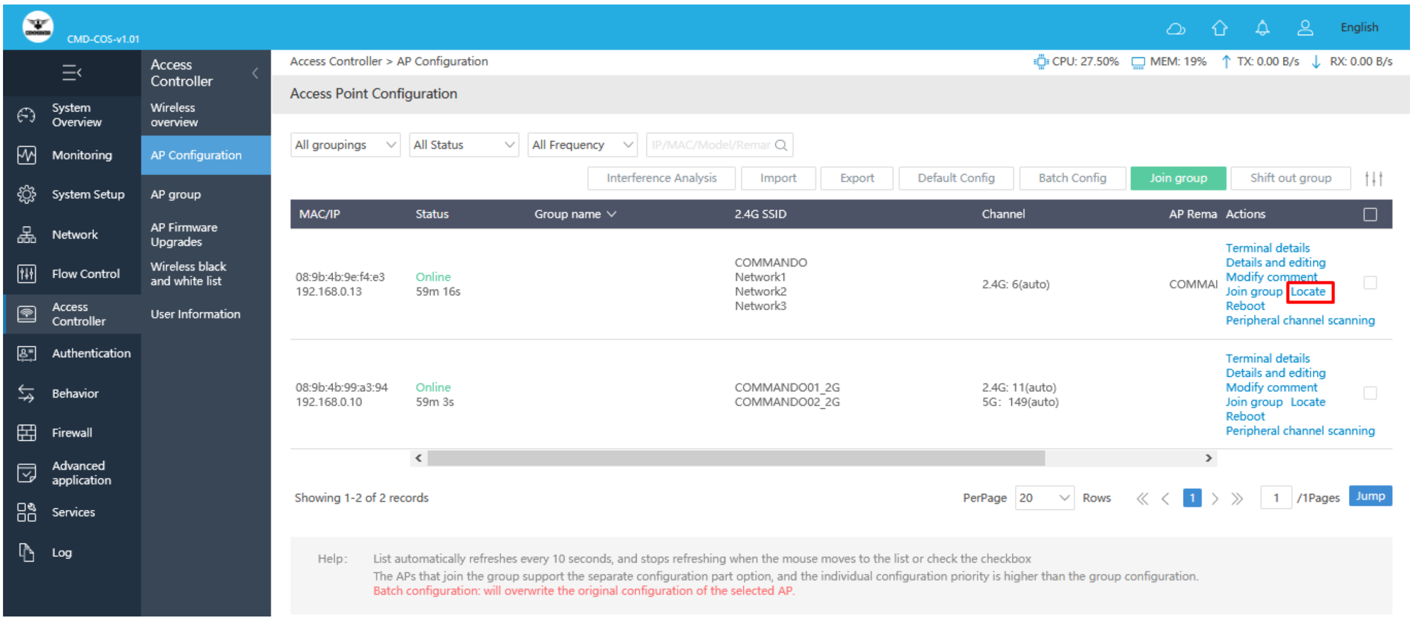
Showing 1-2 of 2 records

PerPage 20 Rows 1 1 /1Pages Jump

Fig 5.2.23 Default Join group page

Note:

Above page will be Editable after creating AP Group only



MAC/IP	Status	Group name	2.4G SSID	Channel	AP Rema	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 59m 16s		COMMANDO Network1 Network2 Network3	2.4G: 6(auto)	COMMAI	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□
08:9b:4b:99:a3:94 192.168.0.10	Online 59m 3s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

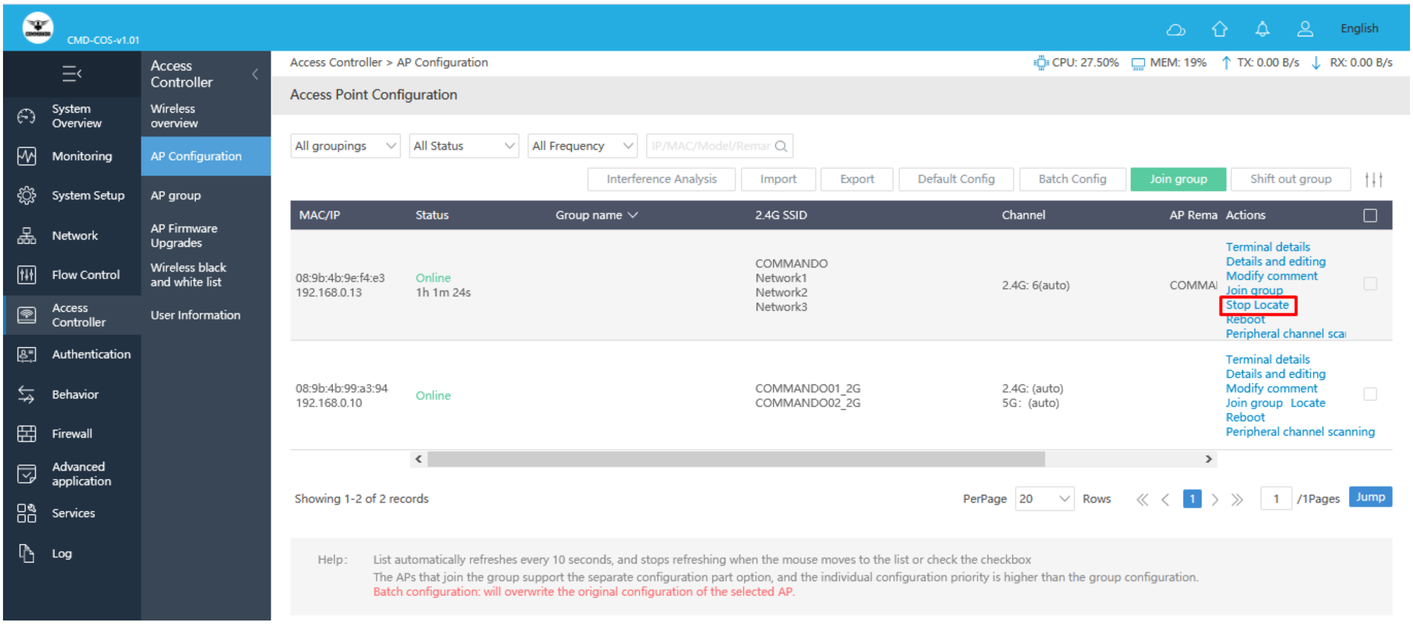
Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

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

Fig 5.2.24 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.



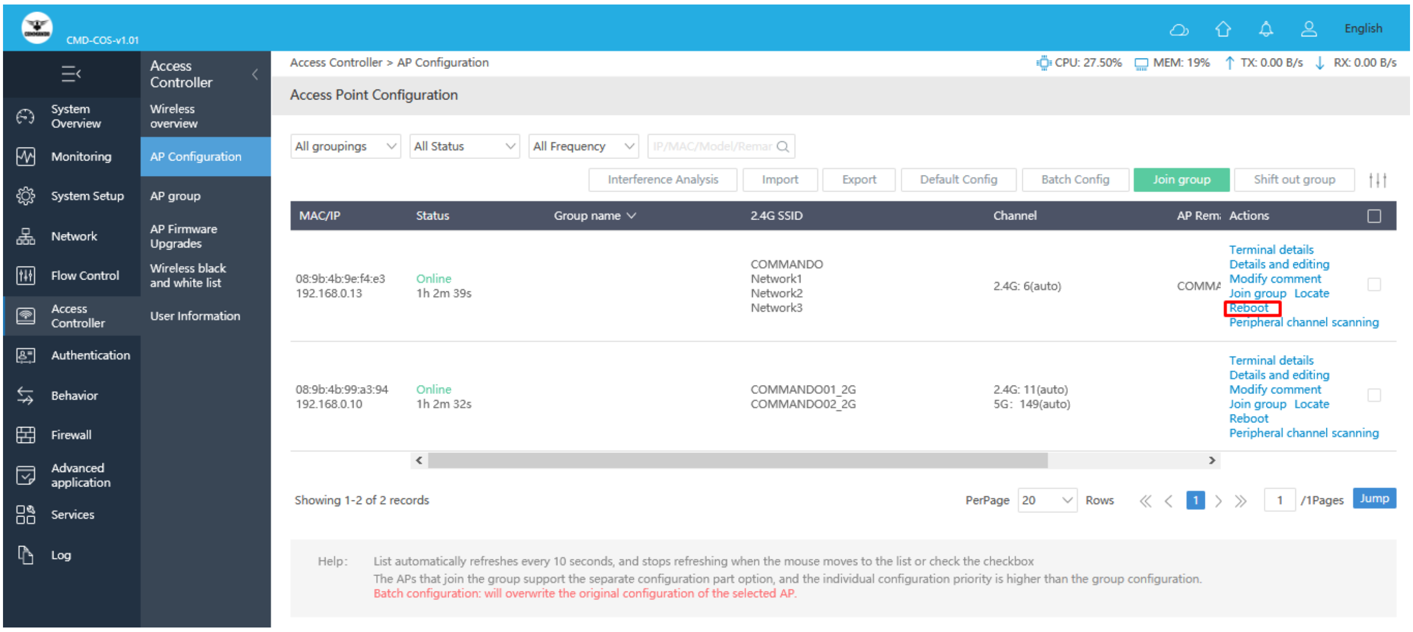
MAC/IP	Status	Group name	2.4G SSID	Channel	AP Rema	Actions	□
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 1m 24s		COMMANDO Network1 Network2 Network3	2.4G: 6(auto)	COMMAI	Terminal details Details and editing Modify comment Join group Stop Locate Reboot Peripheral channel scai	□
08:9b:4b:99:a3:94 192.168.0.10	Online		COMMANDO01_2G COMMANDO02_2G	2.4G: (auto) 5G: (auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

Showing 1-2 of 2 records PerPage 20 Rows 1 1 /1Pages Jump

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

Fig 5.2.25 For Locate particular AP page

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

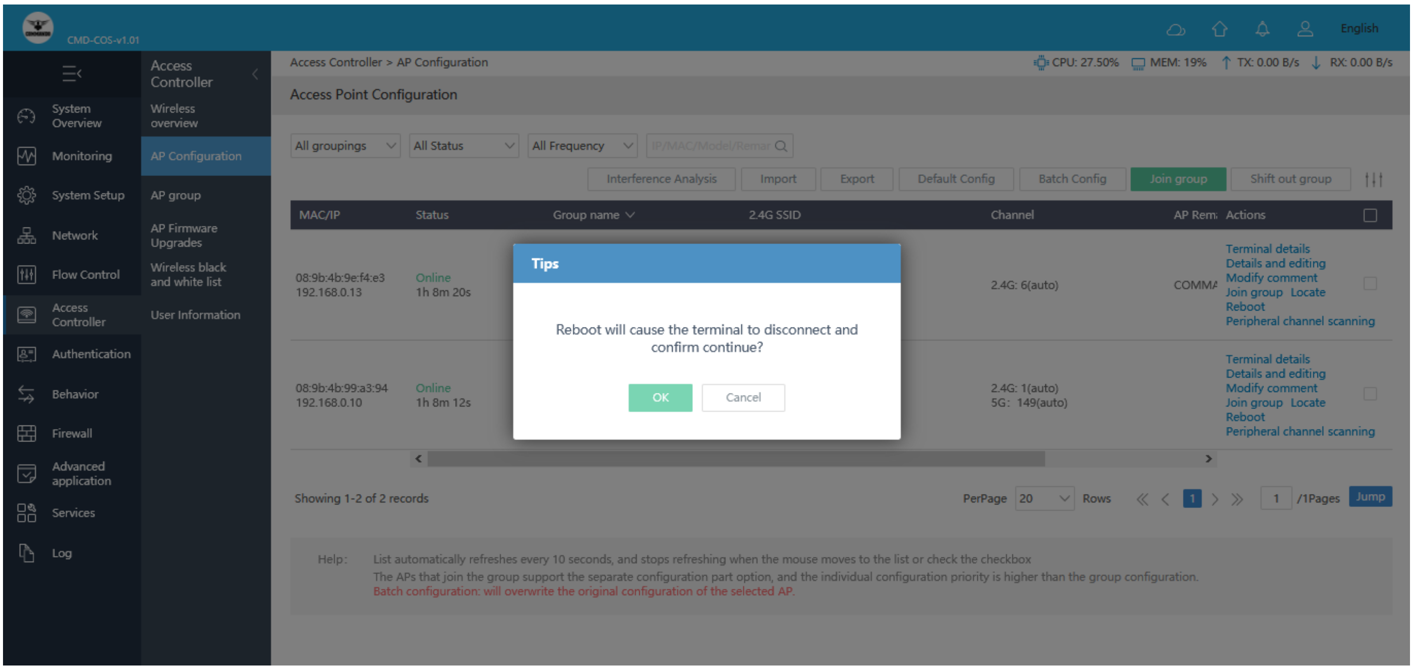


MAC/IP	Status	Group name	2.4G SSID	Channel	AP Rem:	Actions
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 2m 39s		COMMANDO Network1 Network2 Network3	2.4G: 6(auto)	COMMA	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning
08:9b:4b:99:a3:94 192.168.0.10	Online 1h 2m 32s		COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

Showing 1-2 of 2 records PerPage 20 Rows 1 /1Pages Jump

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

Fig 5.2.26 Reboot option in AP configuration page



MAC/IP	Status	Group name	2.4G SSID	Channel	AP Rem:	Actions
08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 8m 20s			2.4G: 6(auto)	COMMA	Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning
08:9b:4b:99:a3:94 192.168.0.10	Online 1h 8m 12s			2.4G: 1(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning

Tips

Reboot will cause the terminal to disconnect and confirm continue?

OK Cancel

Showing 1-2 of 2 records PerPage 20 Rows 1 /1Pages Jump

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

Fig 5.2.27 Reboot AP page

Peripheral channel scanning:

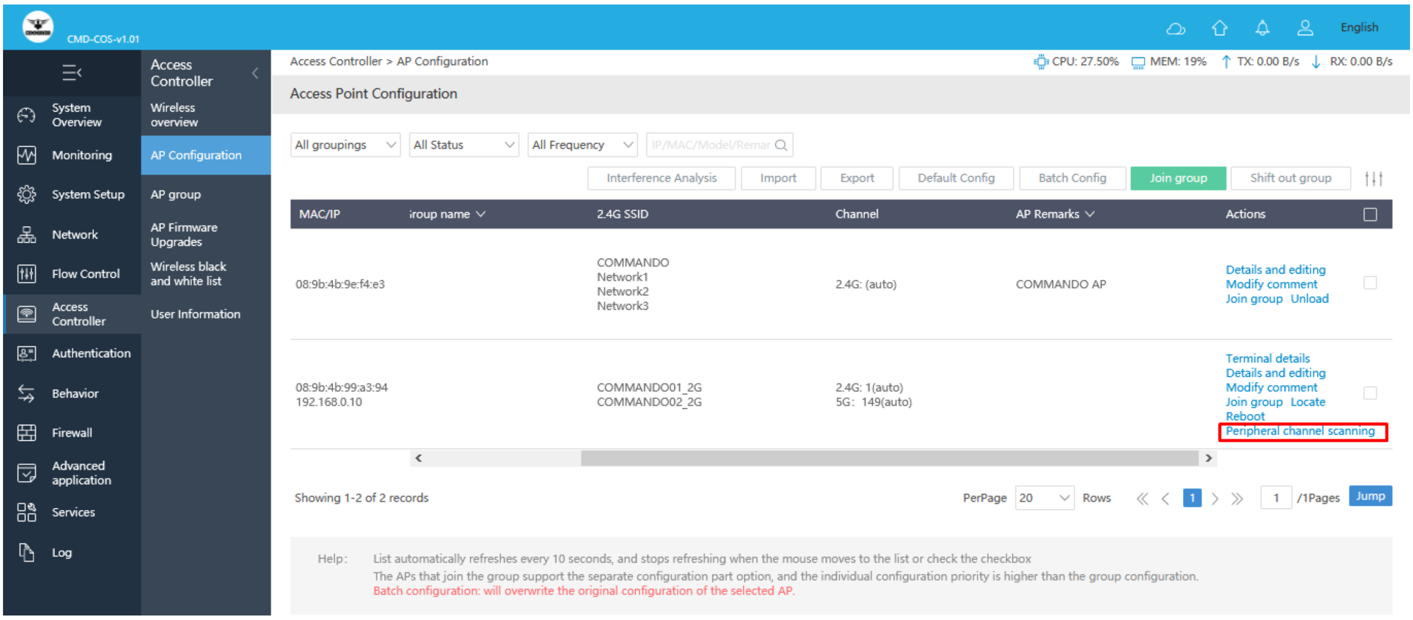
The scanning process consists in actively probing the radio channels to gather access points information.

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



Access Controller > AP Configuration   CPU: 27.50%   MEM: 19%   TX: 0.00 B/s   RX: 0.00 B/s

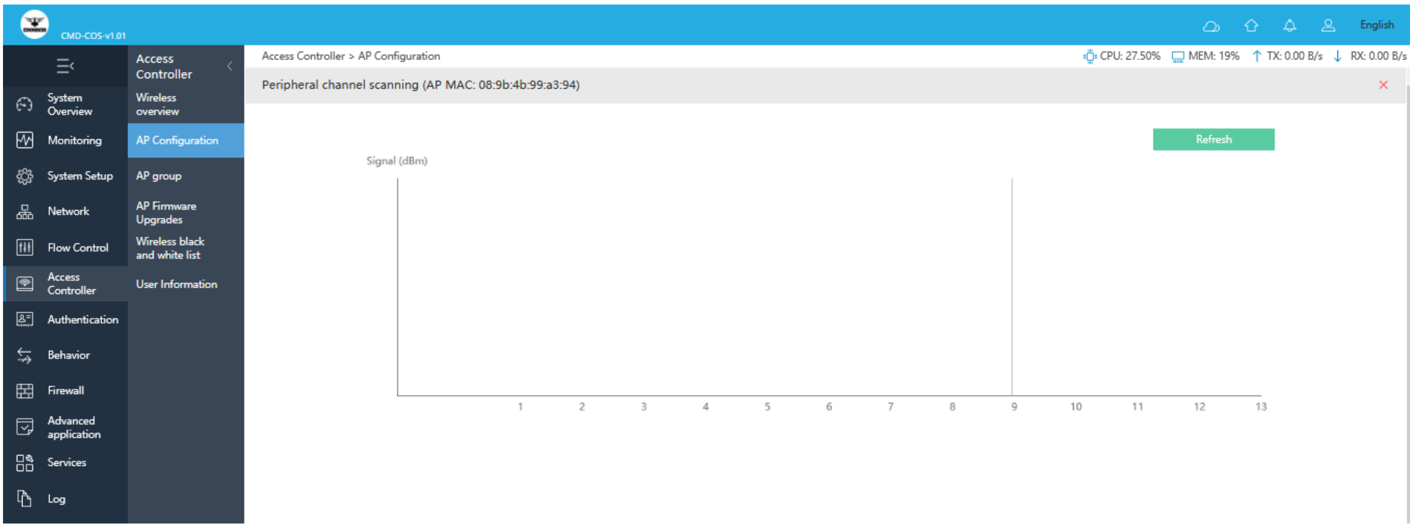
Access Point Configuration

MAC/IP	ɹroup name	2.4G SSID	Channel	AP Remarks	Actions	□
08:9b:4b:9e:f4:e3		COMMANDO Network1 Network2 Network3	2.4G: (auto)	COMMANDO AP	Details and editing Modify comment Join group Unload	□
08:9b:4b:99:a3:94 192.168.0.10		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto) 5G: 149(auto)		Terminal details Details and editing Modify comment Join group Locate Reboot Peripheral channel scanning	□

Showing 1-2 of 2 records   PerPage 20 Rows   1   1 /1Pages   Jump

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

Fig 5.2.28 Default Peripheral channel scanning option page



Access Controller > AP Configuration   CPU: 27.50%   MEM: 19%   TX: 0.00 B/s   RX: 0.00 B/s

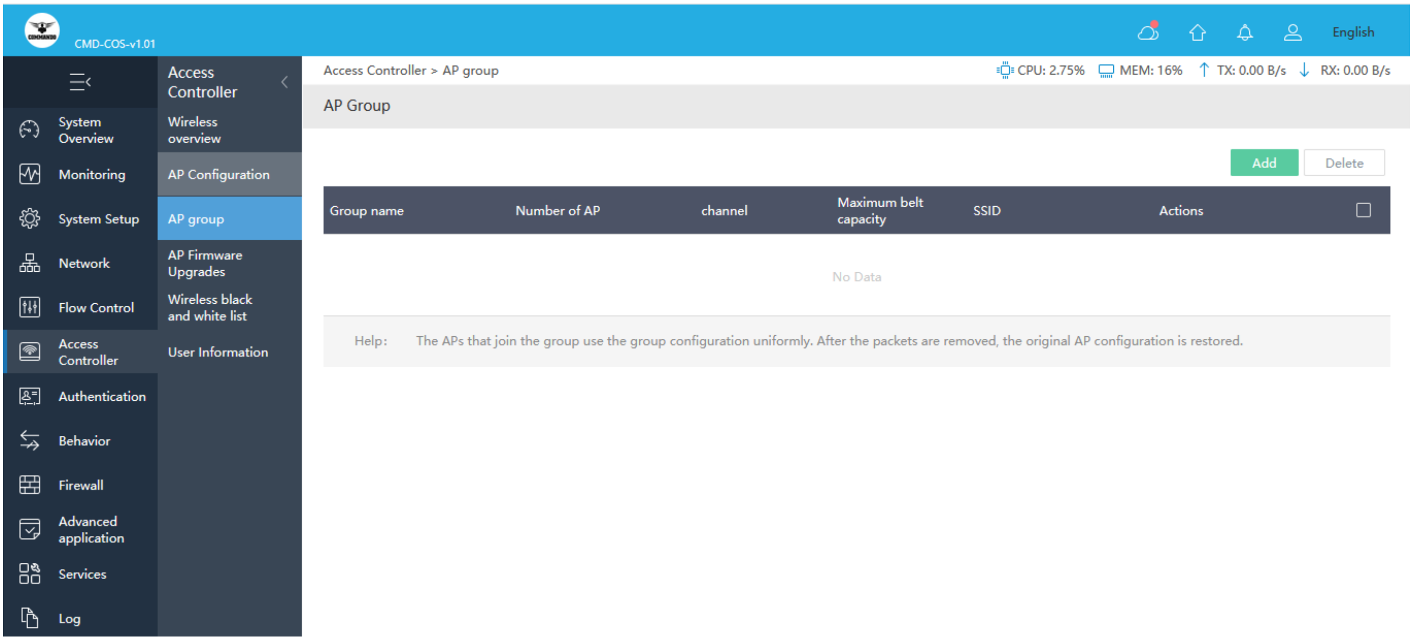
Peripheral channel scanning (AP MAC: 08:9b:4b:99:a3:94)

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

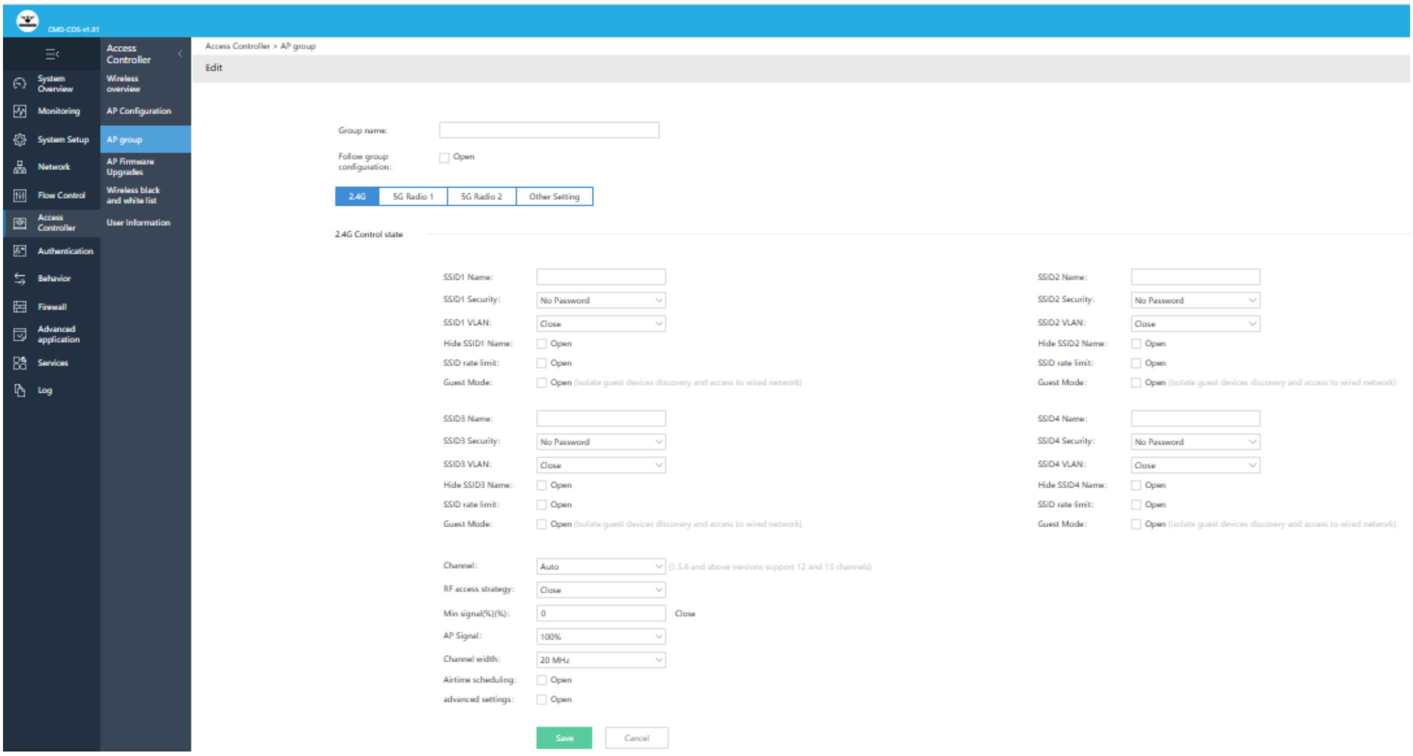
CPU: 2.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

AP Group

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 Control state

SSID1 Name:

SSID1 Security: No Password

SSID1 VLAN: Close

Hide SSID1 Name: □ Open

SSID rate limit: □ Open

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

SSID2 Name:

SSID2 Security: No Password

SSID2 VLAN: Close

Hide SSID2 Name: □ Open

SSID rate limit: □ Open

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

SSID3 Name:

SSID3 Security: No Password

SSID3 VLAN: Close

Hide SSID3 Name: □ Open

SSID rate limit: □ Open

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

SSID4 Name:

SSID4 Security: No Password

SSID4 VLAN: Close

Hide SSID4 Name: □ Open

SSID rate limit: □ Open

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

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

RF access strategy: Close

Min signal(%)(%): 0 Close

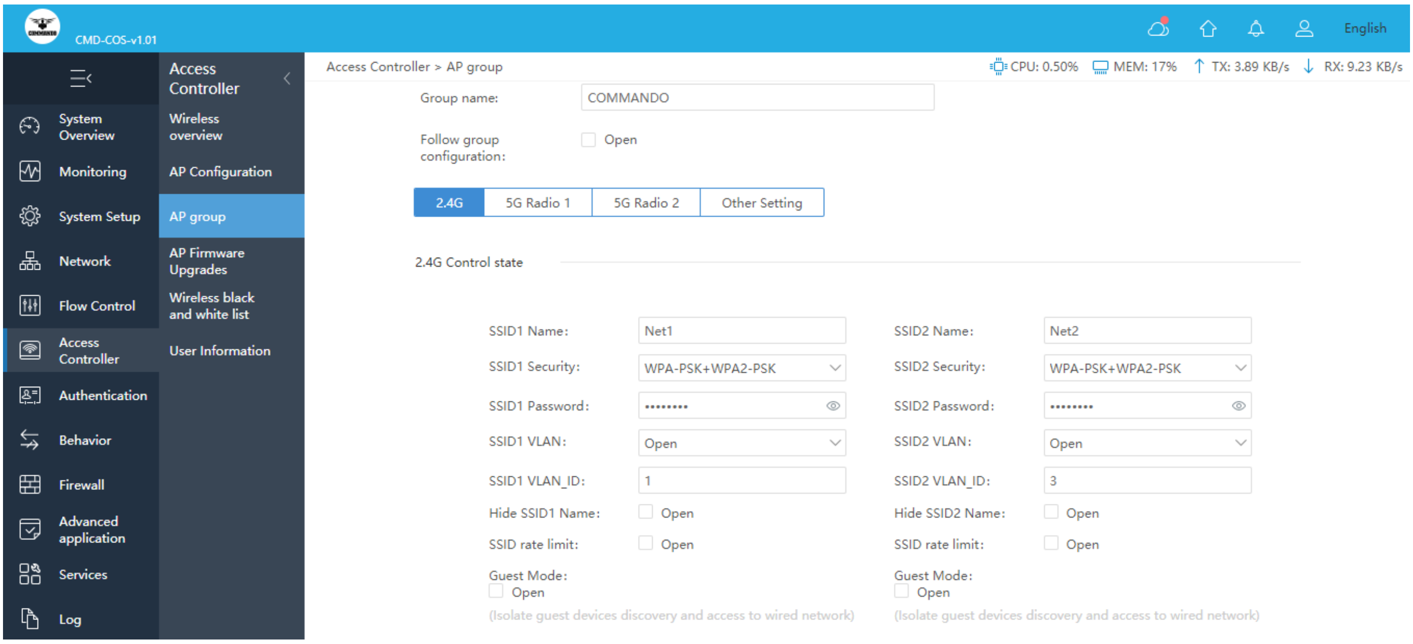
AP Signal: 100%

Channel width: 20 MHz

Airtime scheduling: □ Open

advanced settings: □ Open

5.3.2 Default Edit AP Group page



Access Controller > AP group

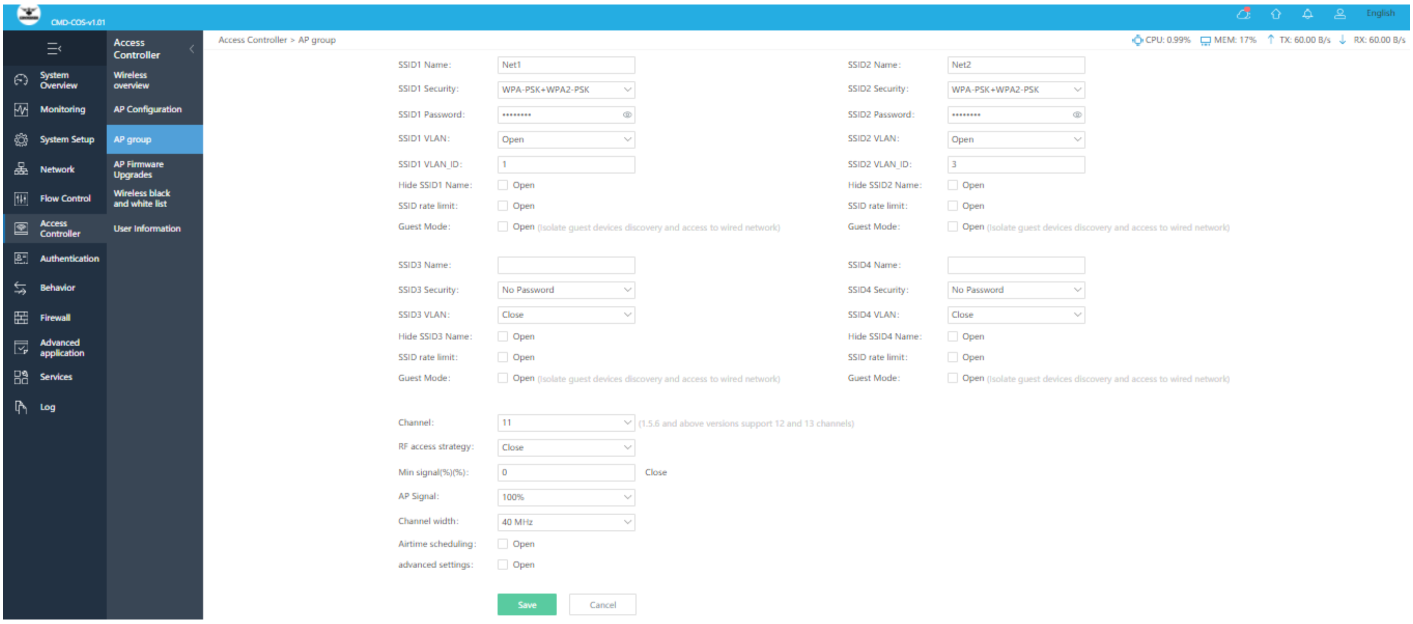
CPU: 0.50% MEM: 17% TX: 3.89 KB/s RX: 9.23 KB/s

Group name: COMMANDO

Follow group configuration: □ Open

2.4G Control state

SSID1 Name:	Net1	SSID2 Name:	Net2
SSID1 Security:	WPA-PSK+WPA2-PSK	SSID2 Security:	WPA-PSK+WPA2-PSK
SSID1 Password:	••••••••	SSID2 Password:	••••••••
SSID1 VLAN:	Open	SSID2 VLAN:	Open
SSID1 VLAN_ID:	1	SSID2 VLAN_ID:	3
Hide SSID1 Name:	□ Open	Hide SSID2 Name:	□ Open
SSID rate limit:	□ Open	SSID rate limit:	□ Open
Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)	Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)



Access Controller > AP group

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

SSID1 Name:	Net1	SSID2 Name:	Net2
SSID1 Security:	WPA-PSK+WPA2-PSK	SSID2 Security:	WPA-PSK+WPA2-PSK
SSID1 Password:	••••••••	SSID2 Password:	••••••••
SSID1 VLAN:	Open	SSID2 VLAN:	Open
SSID1 VLAN_ID:	1	SSID2 VLAN_ID:	3
Hide SSID1 Name:	□ Open	Hide SSID2 Name:	□ Open
SSID rate limit:	□ Open	SSID rate limit:	□ Open
Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)	Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)
SSID3 Name:		SSID4 Name:	
SSID3 Security:	No Password	SSID4 Security:	No Password
SSID3 VLAN:	Close	SSID4 VLAN:	Close
Hide SSID3 Name:	□ Open	Hide SSID4 Name:	□ Open
SSID rate limit:	□ Open	SSID rate limit:	□ Open
Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)	Guest Mode:	□ Open (Isolate guest devices discovery and access to wired network)

Channel: 11 (1.5.6 and above versions support 12 and 13 channels)

RF access strategy: Close

Min signal(%)(%): 0 Close

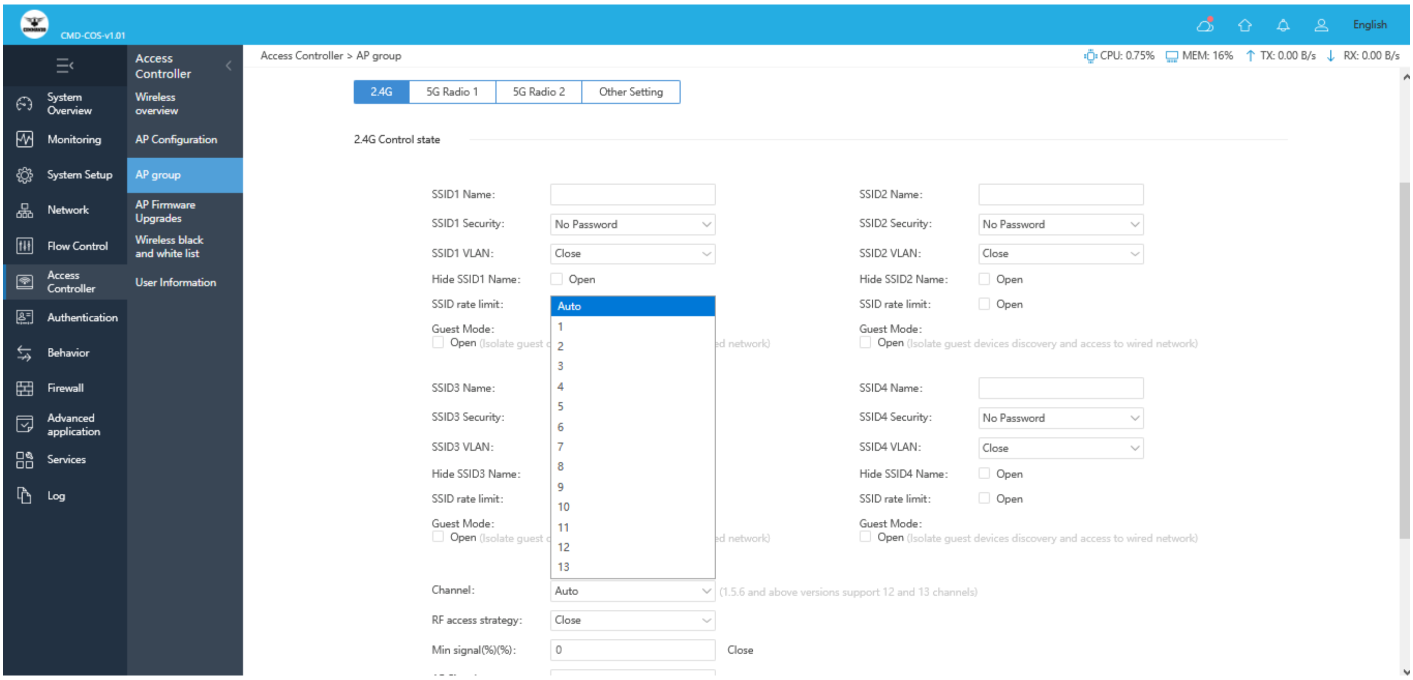
AP Signal: 100%

Channel width: 40 MHz

Airtime scheduling: □ Open

advanced settings: □ Open

5.3.3 Edit AP Group page



CMD-COS-v1.01

English

Access Controller > AP group

CPU: 0.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

2.4G Control state

SSID1 Name:
SSID1 Security: No Password
SSID1 VLAN: Close
Hide SSID1 Name: □ Open
SSID rate limit: Auto
Guest Mode: □ Open (Isolate guest … network)

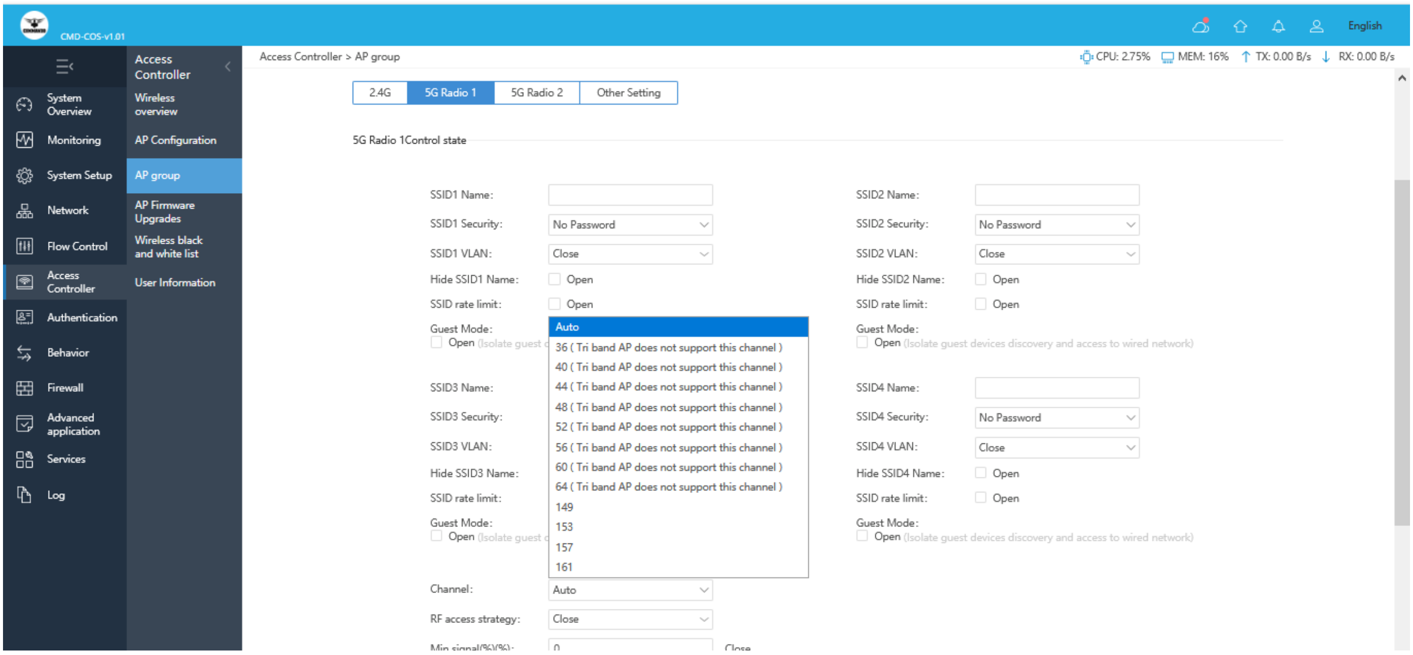
SSID3 Name:
SSID3 Security:
SSID3 VLAN:
Hide SSID3 Name:
SSID rate limit:
Guest Mode: □ Open (Isolate guest … network)

SSID2 Name:
SSID2 Security: No Password
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID4 Name:
SSID4 Security: No Password
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

Channel: Auto (1.5.6 and above versions support 12 and 13 channels)
RF access strategy: Close
Min signal(%)(%): 0 Close

5.3.4 Group AP Channel selection in 2.4GHz page



CMD-COS-v1.01

English

Access Controller > AP group

CPU: 2.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

5G Radio 1Control state

SSID1 Name:
SSID1 Security: No Password
SSID1 VLAN: Close
Hide SSID1 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest …

SSID3 Name:
SSID3 Security:
SSID3 VLAN:
Hide SSID3 Name:
SSID rate limit:
Guest Mode: □ Open (Isolate guest …

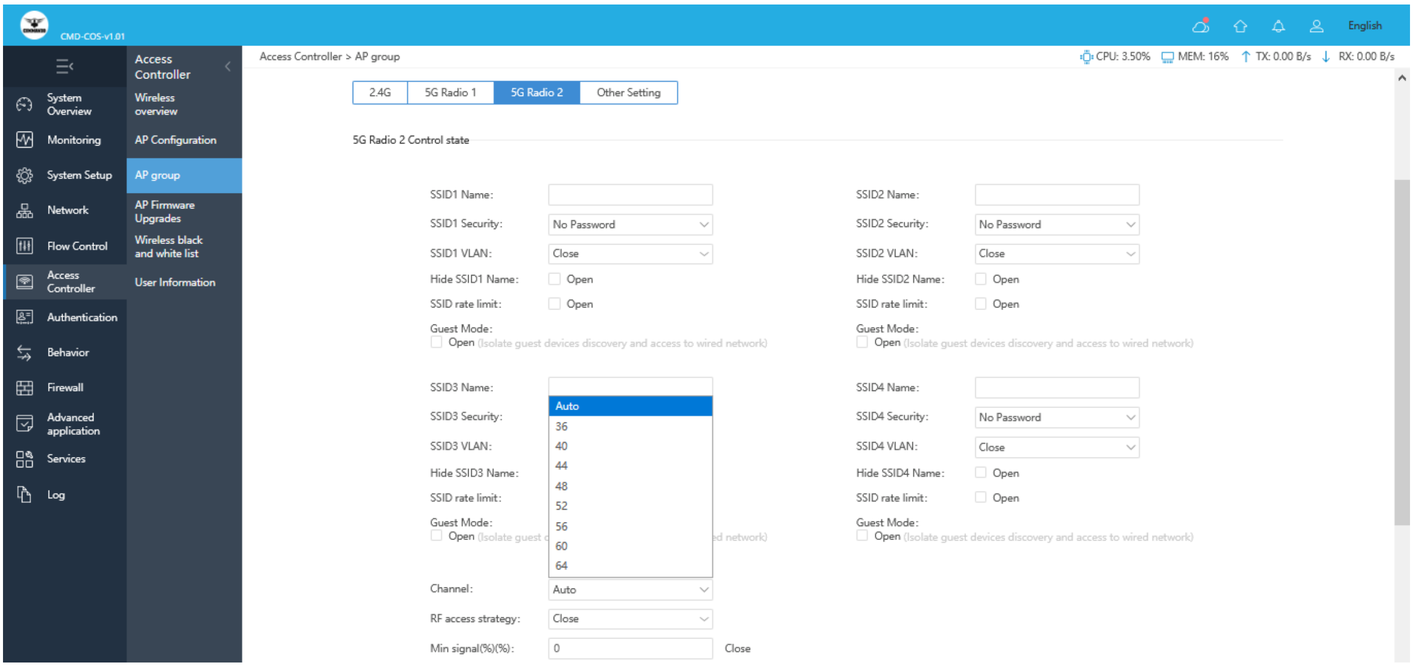
SSID2 Name:
SSID2 Security: No Password
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

SSID4 Name:
SSID4 Security: No Password
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
SSID rate limit: □ Open
Guest Mode: □ Open (Isolate guest devices discovery and access to wired network)

Auto
36 (Tri band AP does not support this channel)
40 (Tri band AP does not support this channel)
44 (Tri band AP does not support this channel)
48 (Tri band AP does not support this channel)
52 (Tri band AP does not support this channel)
56 (Tri band AP does not support this channel)
60 (Tri band AP does not support this channel)
64 (Tri band AP does not support this channel)
149
153
157
161

Channel: Auto
RF access strategy: Close
Min signal(%)(%): 0 Close

5.3.5 Group AP Channel selection in 5GHz Radio1 page



Access Controller > AP group

5G Radio 2 Control state

SSID1 Name:
SSID1 Security: No Password
SSID1 VLAN: Close
Hide SSID1 Name: □ Open
SSID rate limit: □ Open
Guest Mode:
□ Open (Isolate guest devices discovery and access to wired network)

SSID2 Name:
SSID2 Security: No Password
SSID2 VLAN: Close
Hide SSID2 Name: □ Open
SSID rate limit: □ Open
Guest Mode:
□ Open (Isolate guest devices discovery and access to wired network)

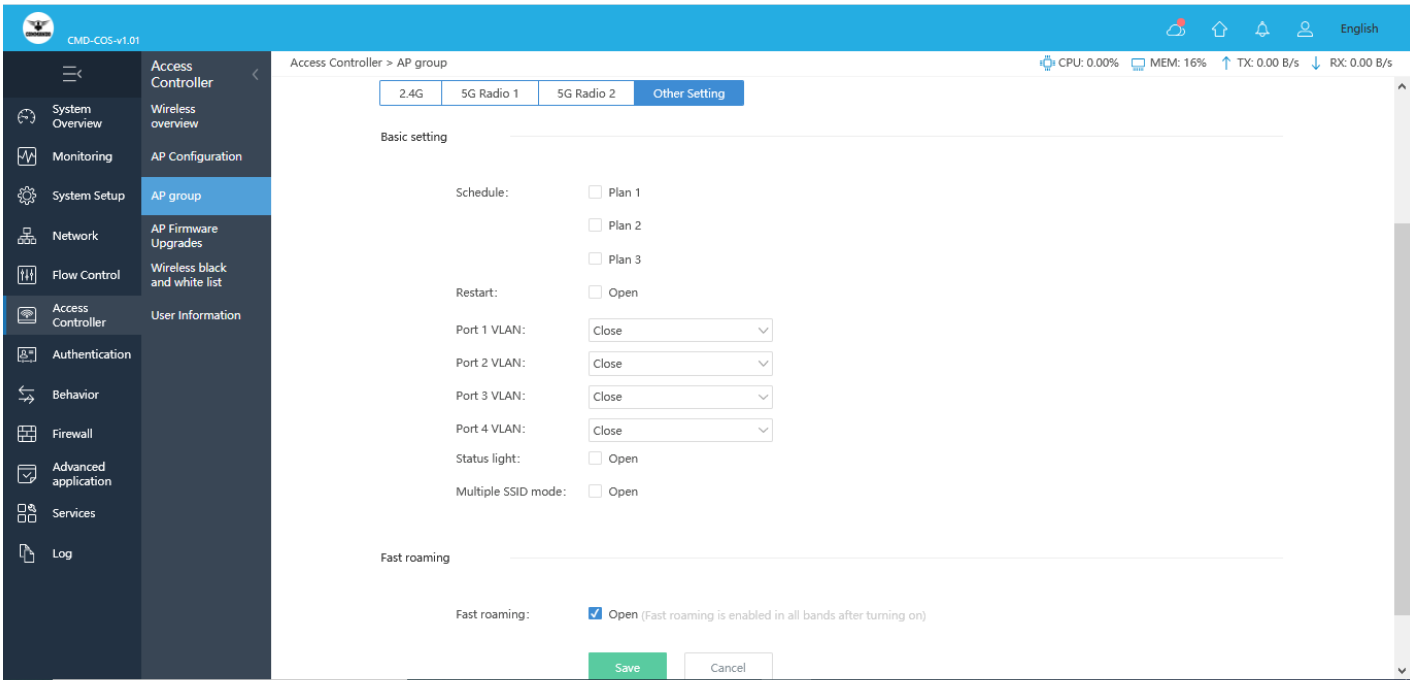
SSID3 Name:
SSID3 Security:
SSID3 VLAN:
Hide SSID3 Name:
SSID rate limit:
Guest Mode:
□ Open (Isolate guest d…d network)

Auto
36
40
44
48
52
56
60
64

SSID4 Name:
SSID4 Security: No Password
SSID4 VLAN: Close
Hide SSID4 Name: □ Open
SSID rate limit: □ Open
Guest Mode:
□ Open (Isolate guest devices discovery and access to wired network)

Channel: Auto
RF access strategy: Close
Min signal(%)(%): 0 Close

5.3.6 Group AP Channel selection in 5GHz Radio2 page



Access Controller > AP group

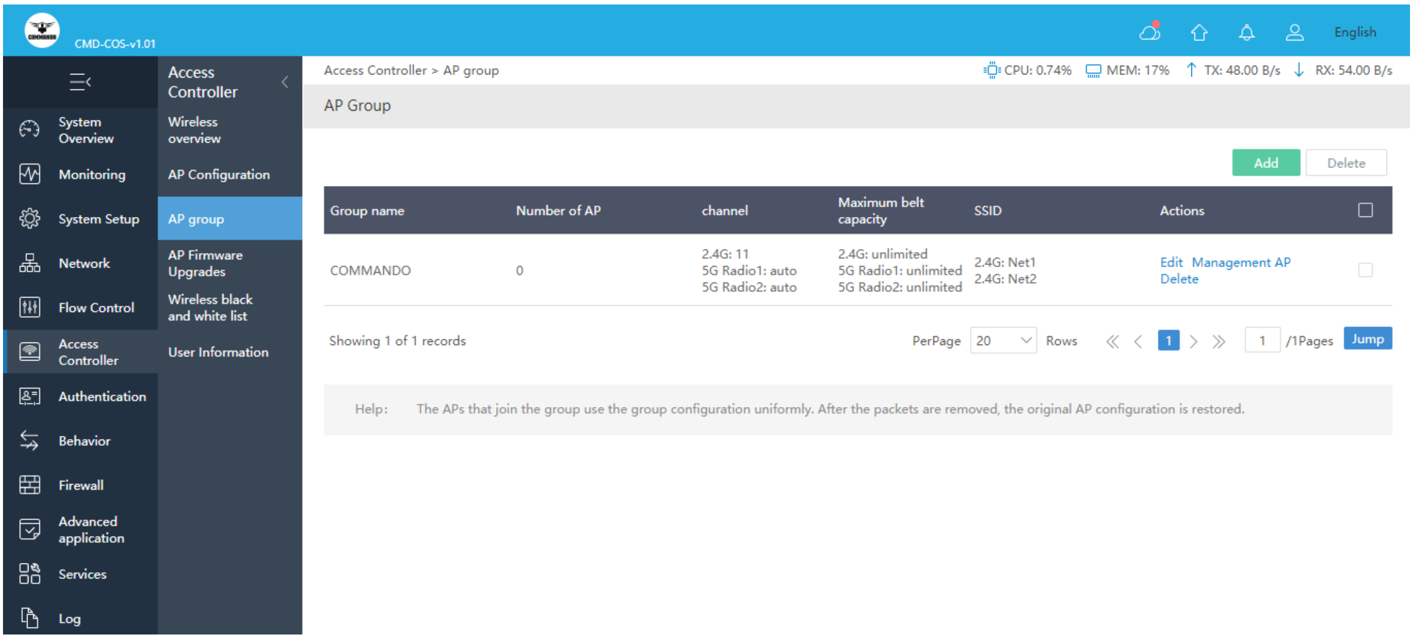
Basic setting

Schedule: □ Plan 1
□ Plan 2
□ Plan 3
Restart: □ Open
Port 1 VLAN: Close
Port 2 VLAN: Close
Port 3 VLAN: Close
Port 4 VLAN: Close
Status light: □ Open
Multiple SSID mode: □ Open

Fast roaming

Fast roaming: ☑ Open (Fast roaming is enabled in all bands after turning on)

5.3.7 Group AP Default Other setting page



Access Controller > AP group

CPU: 0.74% MEM: 17% TX: 48.00 B/s RX: 54.00 B/s

AP Group

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

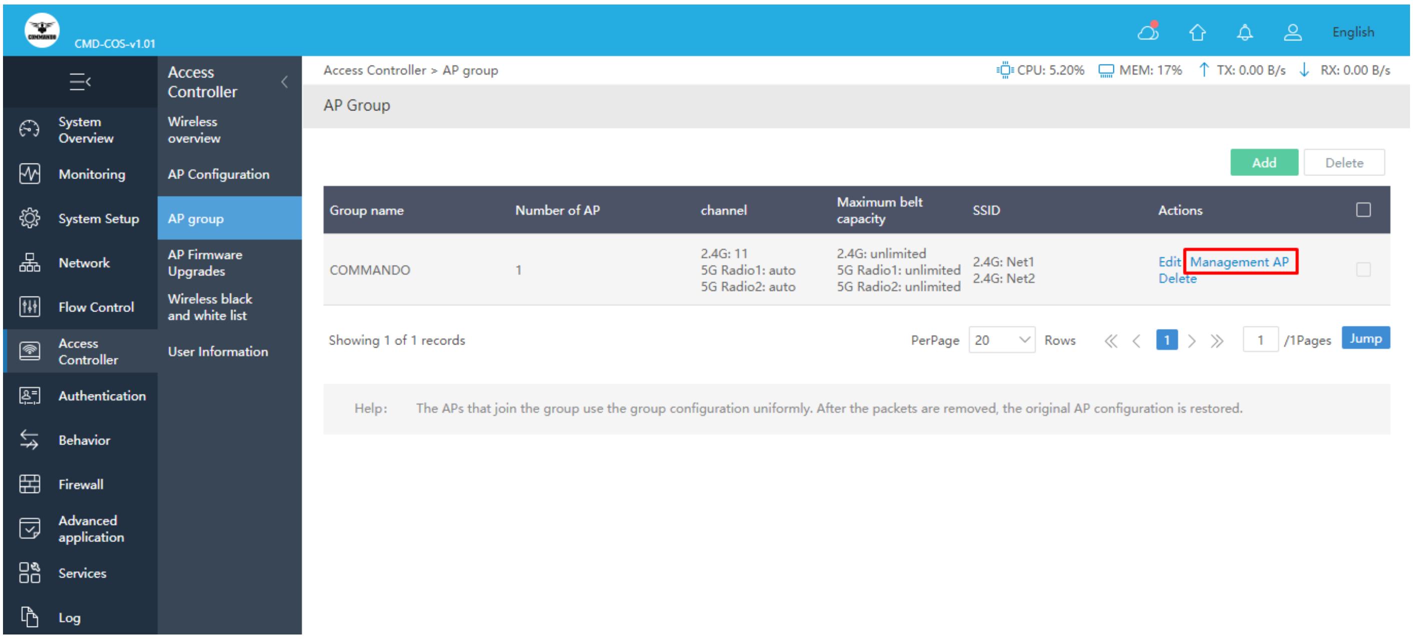
Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

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

5.3.8 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.



Access Controller > AP group

CPU: 5.20% MEM: 17% TX: 0.00 B/s RX: 0.00 B/s

AP Group

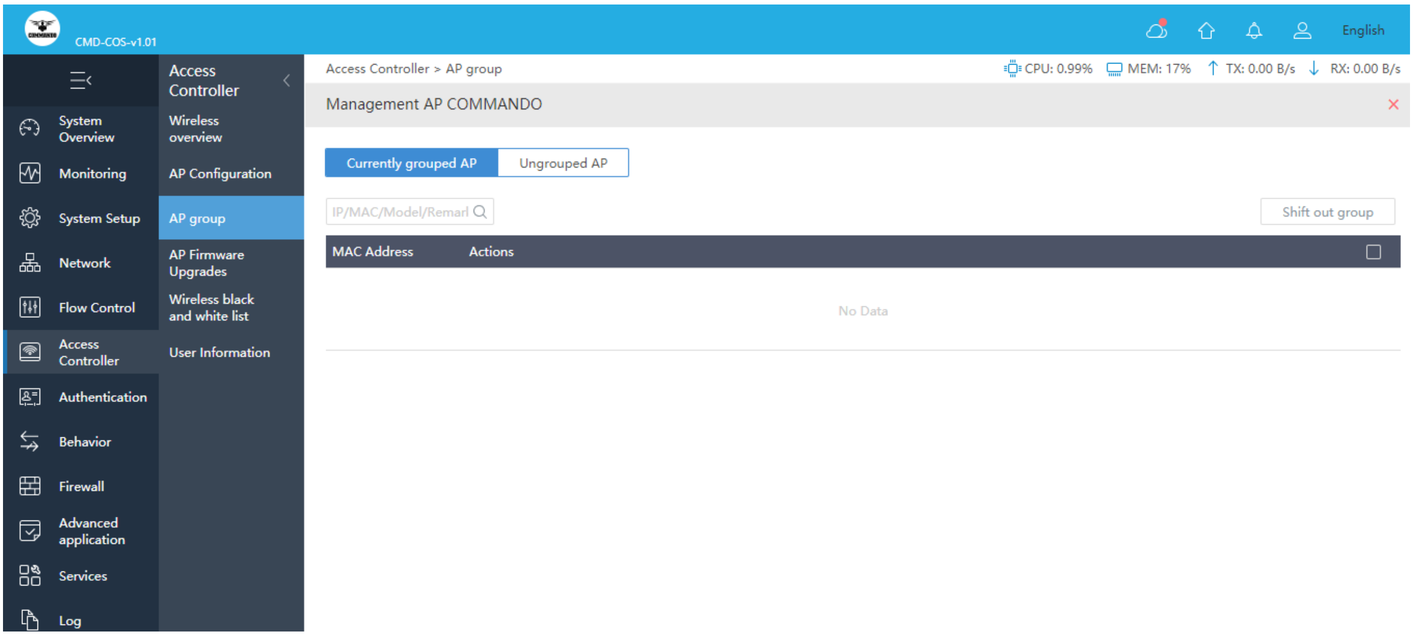
Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions	□
COMMANDO	1	2.4G: 11 5G Radio1: auto 5G Radio2: auto	2.4G: unlimited 5G Radio1: unlimited 5G Radio2: unlimited	2.4G: Net1 2.4G: Net2	Edit Management AP Delete	□

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

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

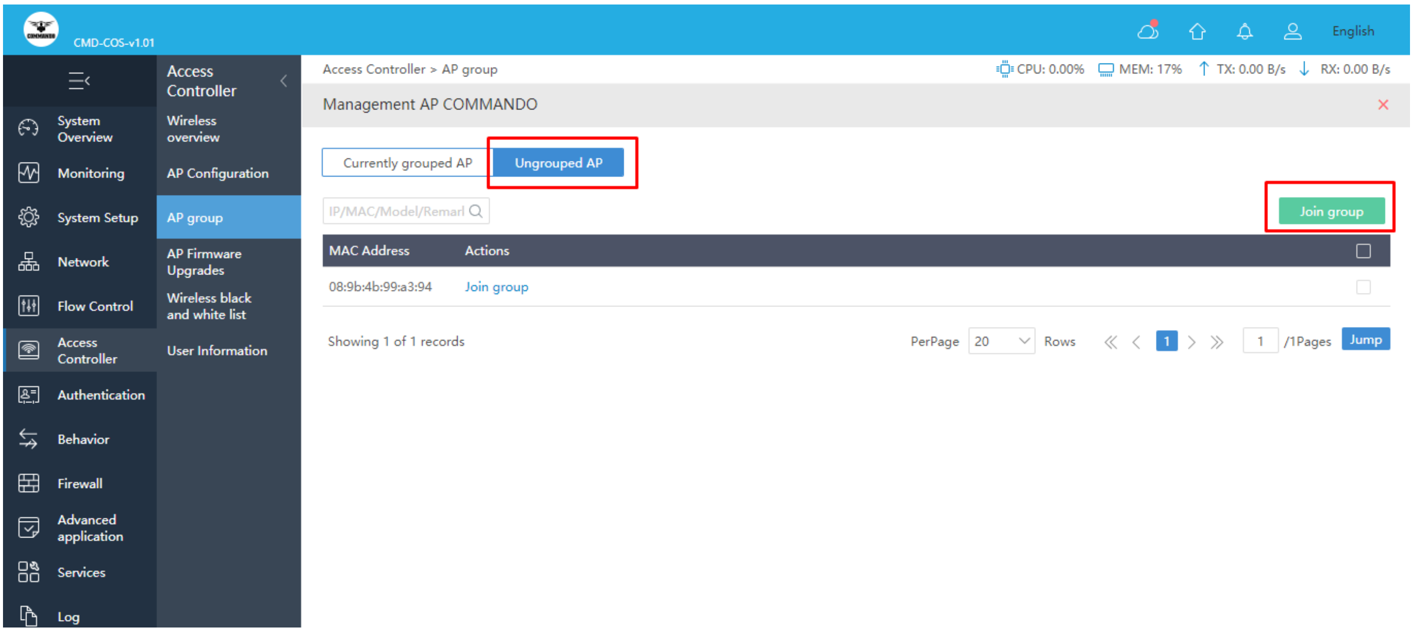
5.3.9 Management AP Group page

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



MAC Address	Actions	□
No Data		

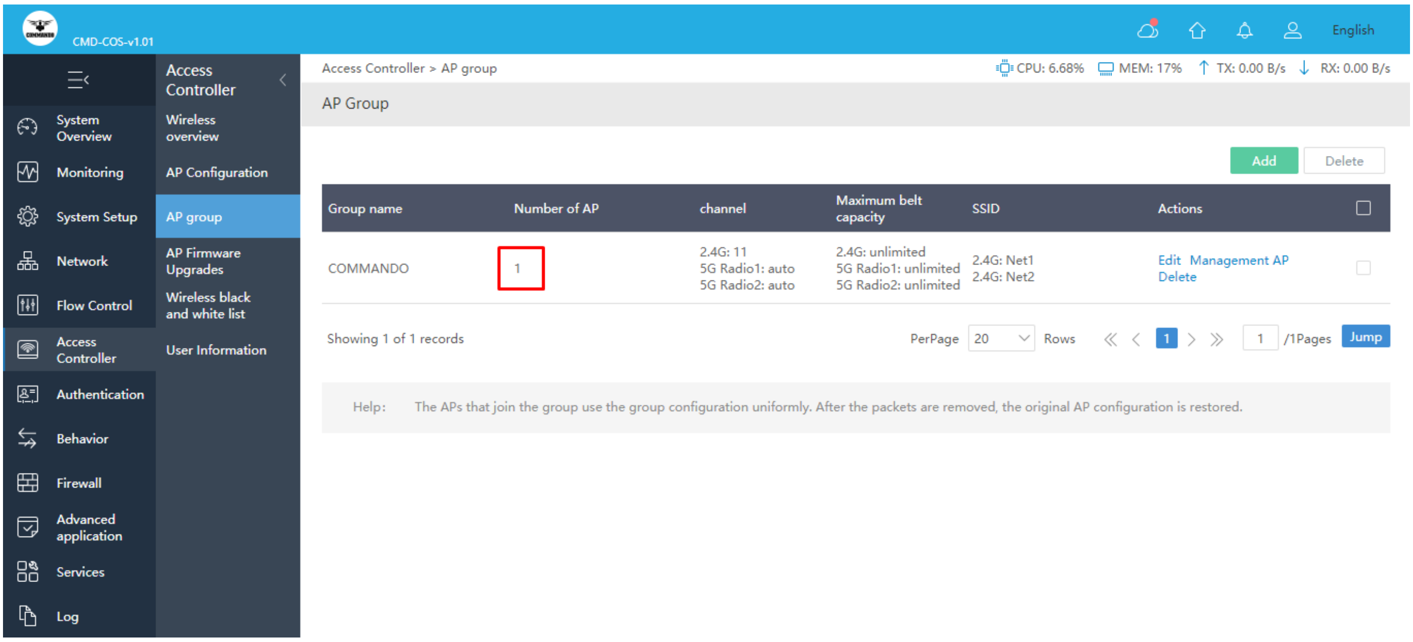
5.3.10 Default Management AP Group page



MAC Address	Actions	□
08:9b:4b:99:a3:94	Join group	□

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages Jump

5.3.11 Join Management AP Group page



Access Controller > AP group

CPU: 6.68% MEM: 17% TX: 0.00 B/s RX: 0.00 B/s

AP Group

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	□

Showing 1 of 1 records

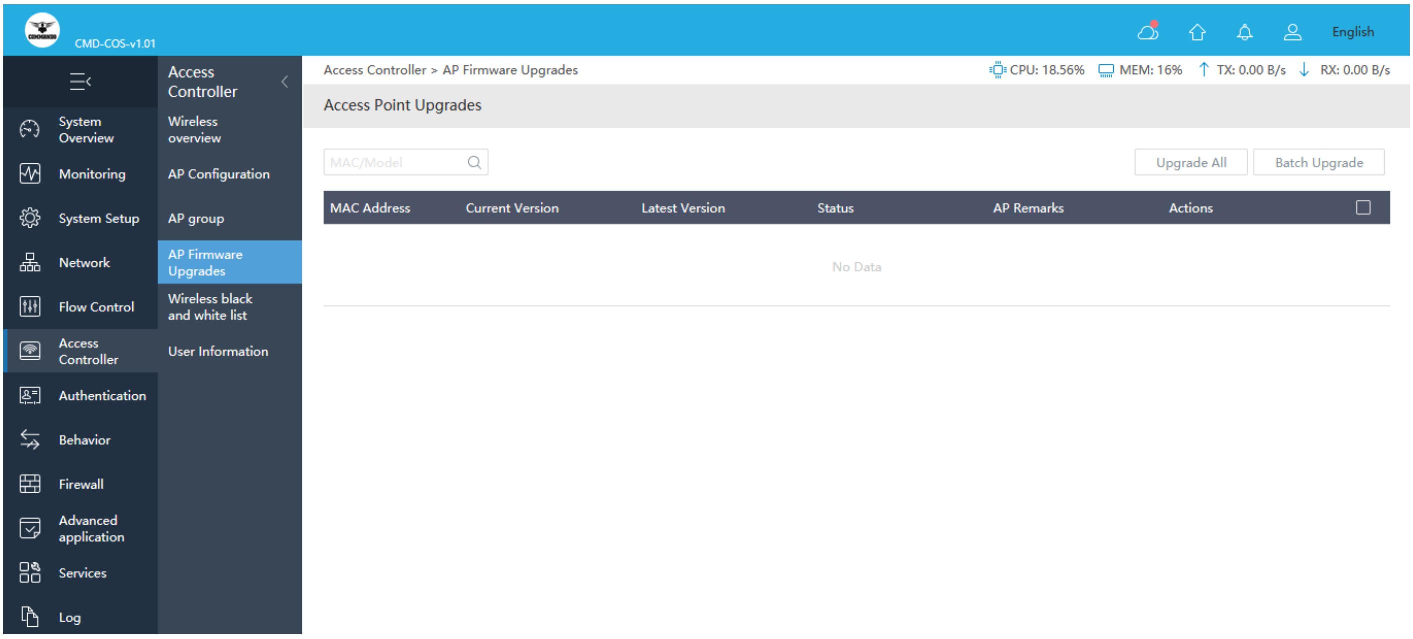
Help: The APs that join the group use the group configuration uniformly. After the packets are removed, the original AP configuration is restored.

5.3.12 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



Access Controller > AP Firmware Upgrades

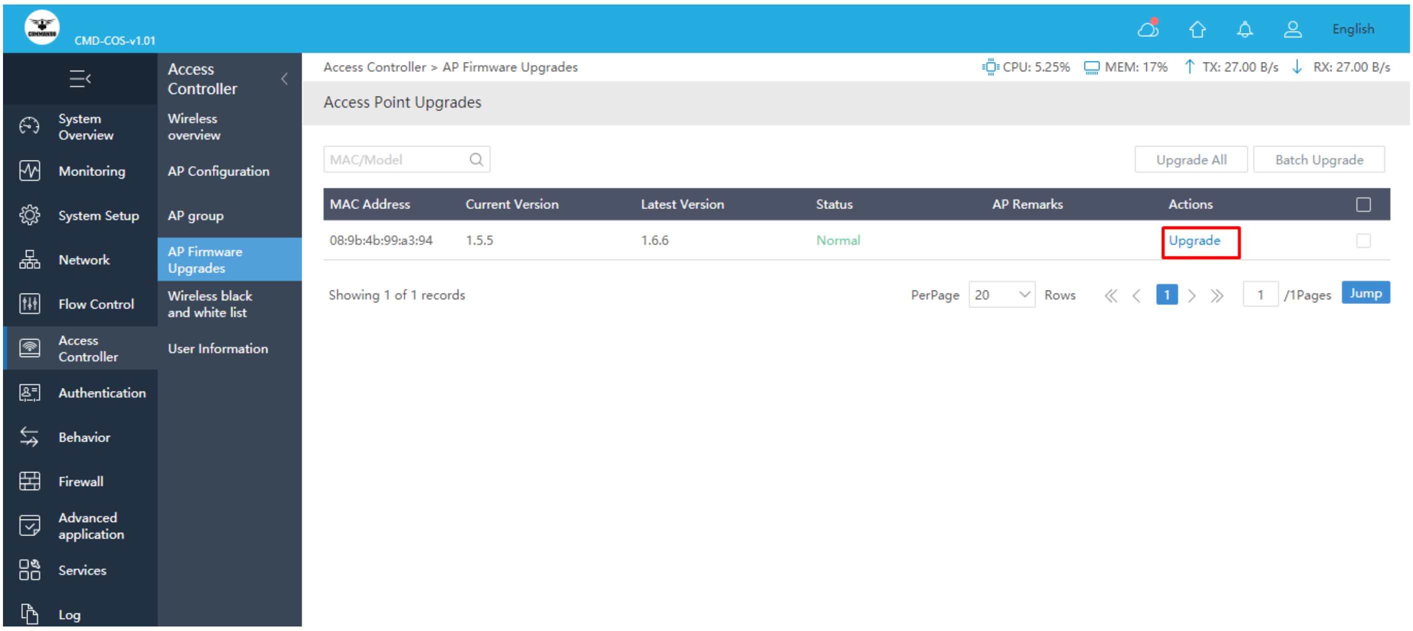
CPU: 18.56% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Access Point Upgrades

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	□

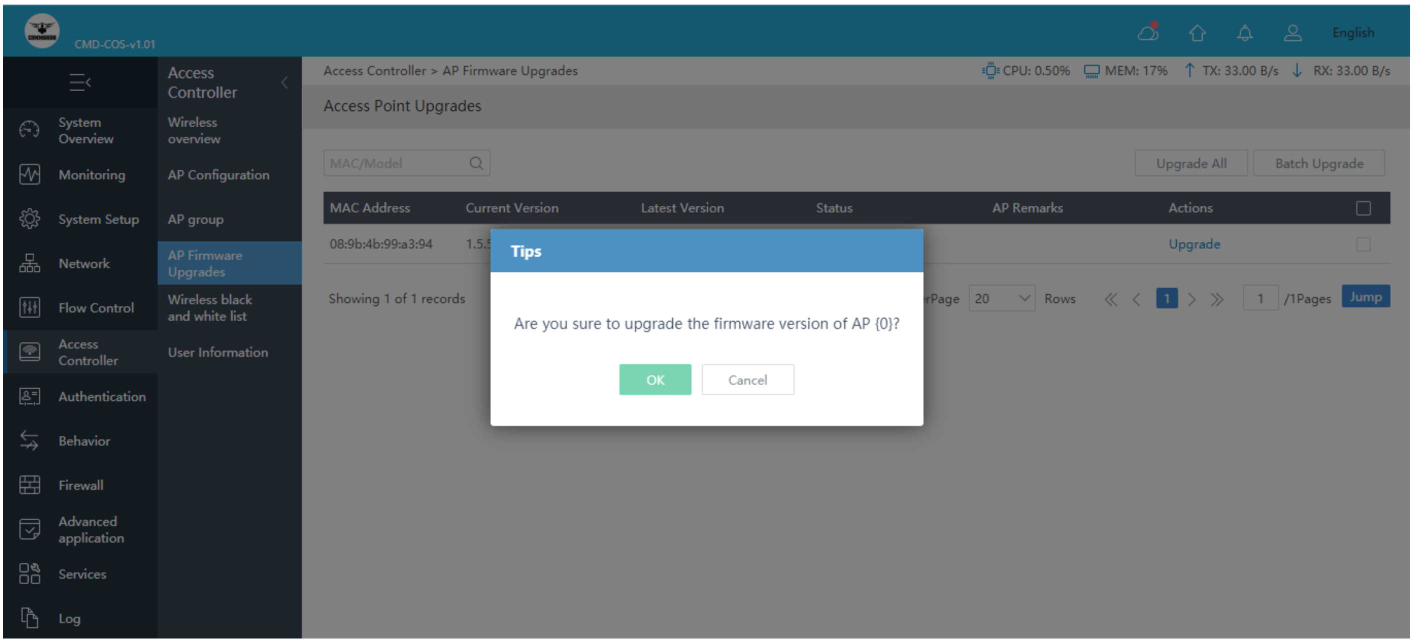
No Data

5.4.1 Default Upgrade firmware of Access Point page



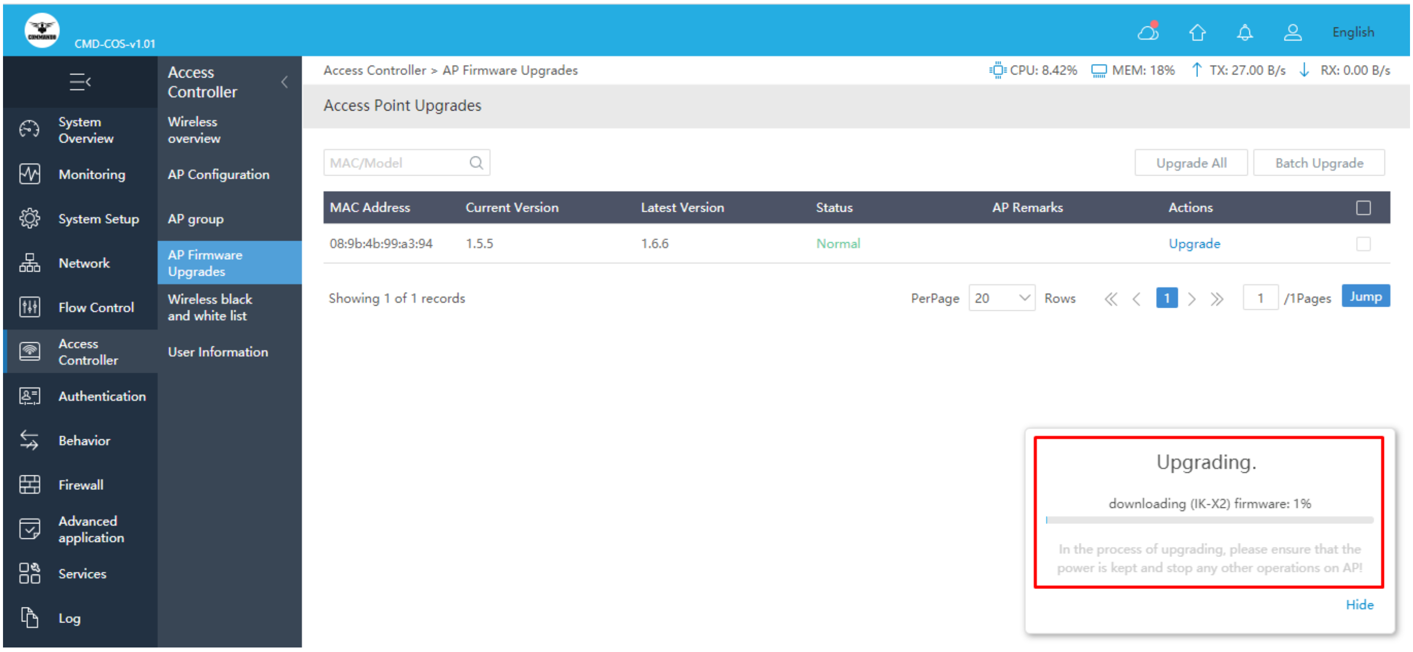
MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	□
08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade	□

5.4.2 Upgrade firmware of Access Point page



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

5.4.3 Upgrade firmware of selected Access Point page



Access Controller > AP Firmware Upgrades

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

Access Point Upgrades

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

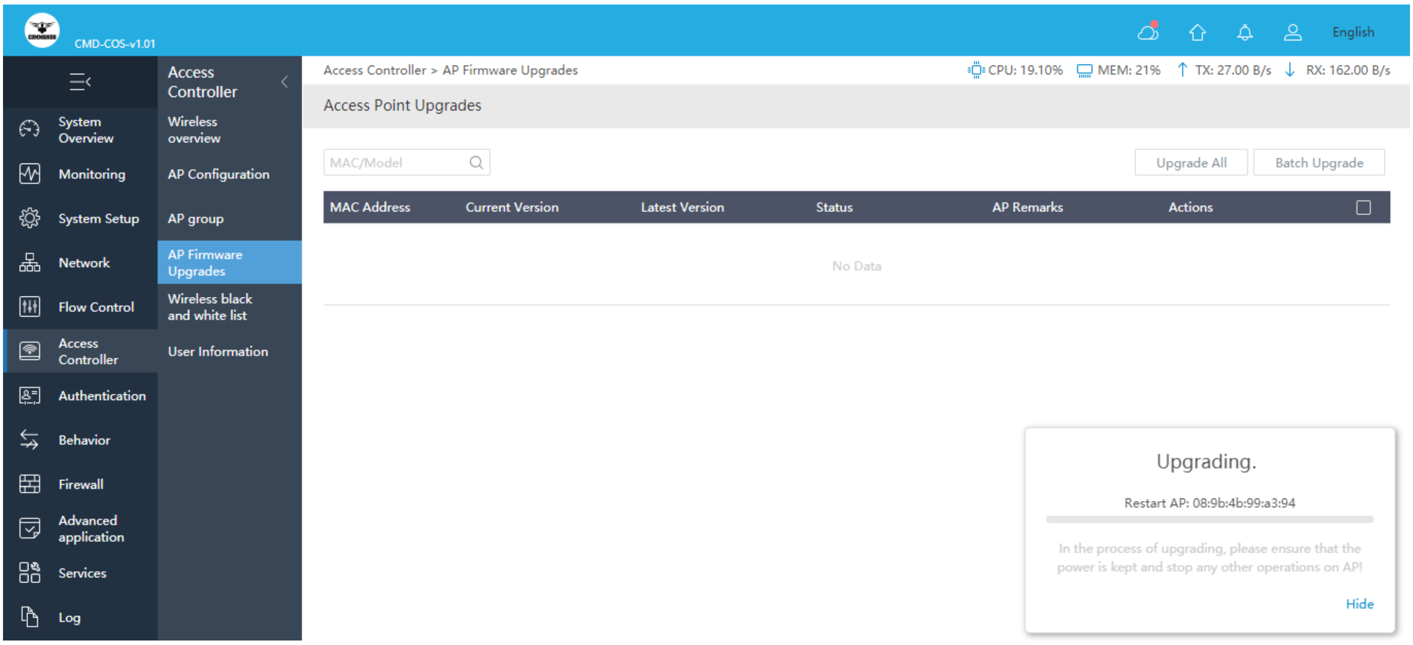
Upgrading.

downloading (IK-X2) firmware: 1%

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

5.4.4 Upgrading firmware of selected Access Point page

Note: After Upgrade AP will be restarted automatically.



Access Controller > AP Firmware Upgrades

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

Access Point Upgrades

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	□

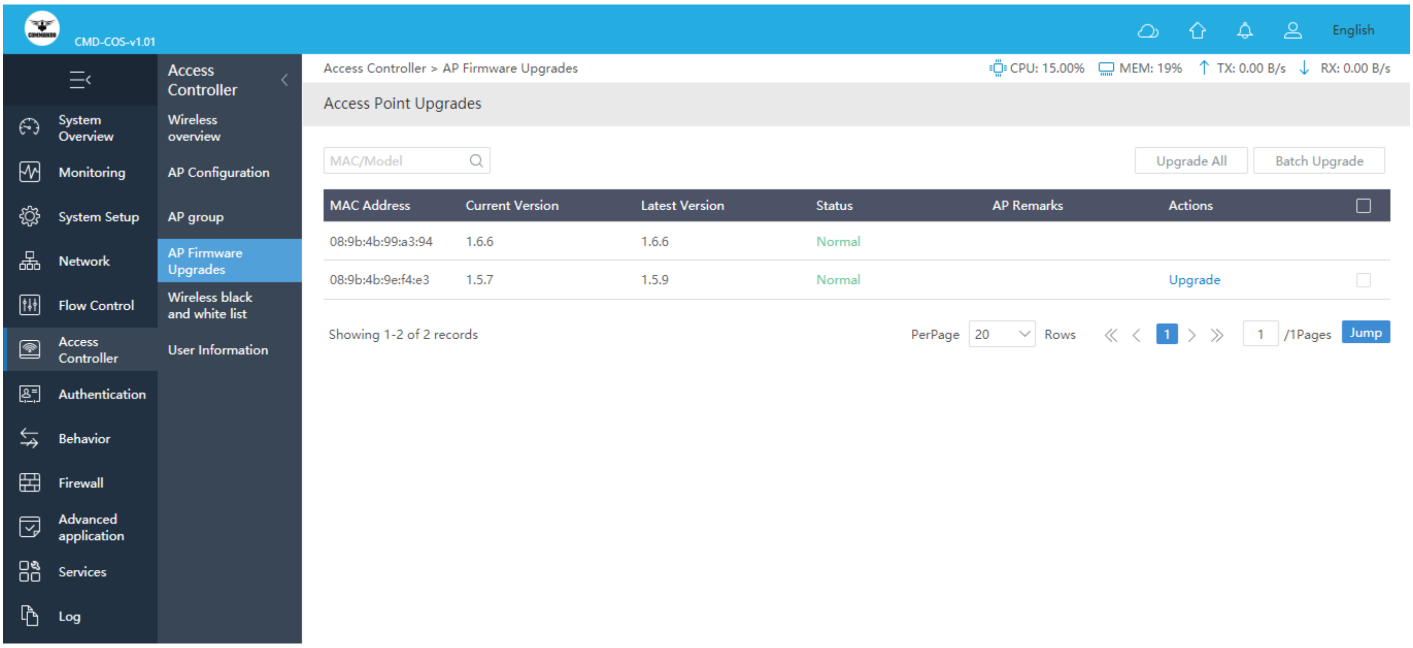
No Data

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!

5.4.5 Upgrading firmware restarting Access Point page



Access Controller > AP Firmware Upgrades

CPU: 15.00% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Access Point Upgrades

MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	□
08:9b:4b:99:a3:94	1.6.6	1.6.6	Normal			
08:9b:4b:9e:f4:e3	1.5.7	1.5.9	Normal		Upgrade	□

Showing 1-2 of 2 records

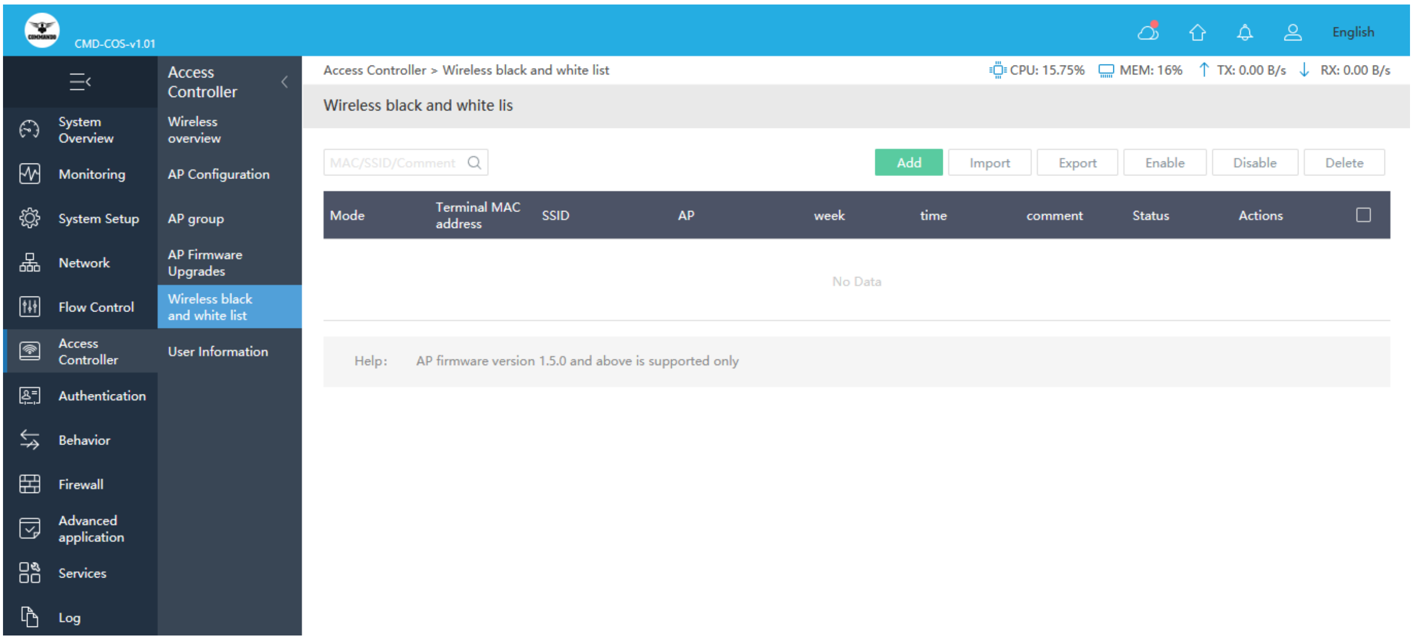
5.4.6 After Upgrading firmware Access Point Upgrade page

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



Access Controller > Wireless black and white list

CPU: 15.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

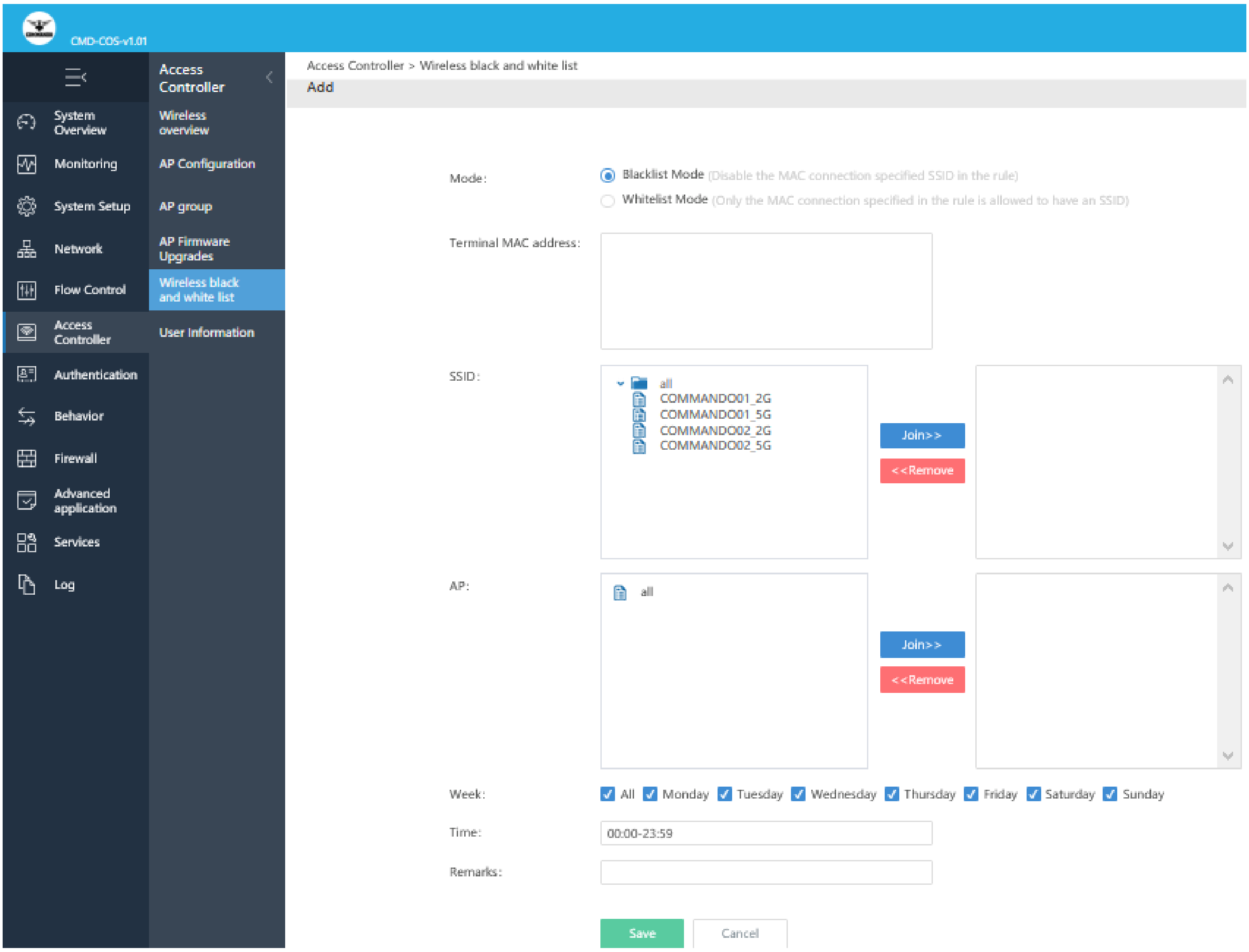
Wireless black and white lis

Mode	Terminal MAC address	SSID	AP	week	time	comment	Status	Actions	□

No Data

Help: AP firmware version 1.5.0 and above is supported only

5.5.1 Default Wireless black and white list page



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
COMMANDO01_2G
COMMANDO01_5G
COMMANDO02_2G
COMMANDO02_5G

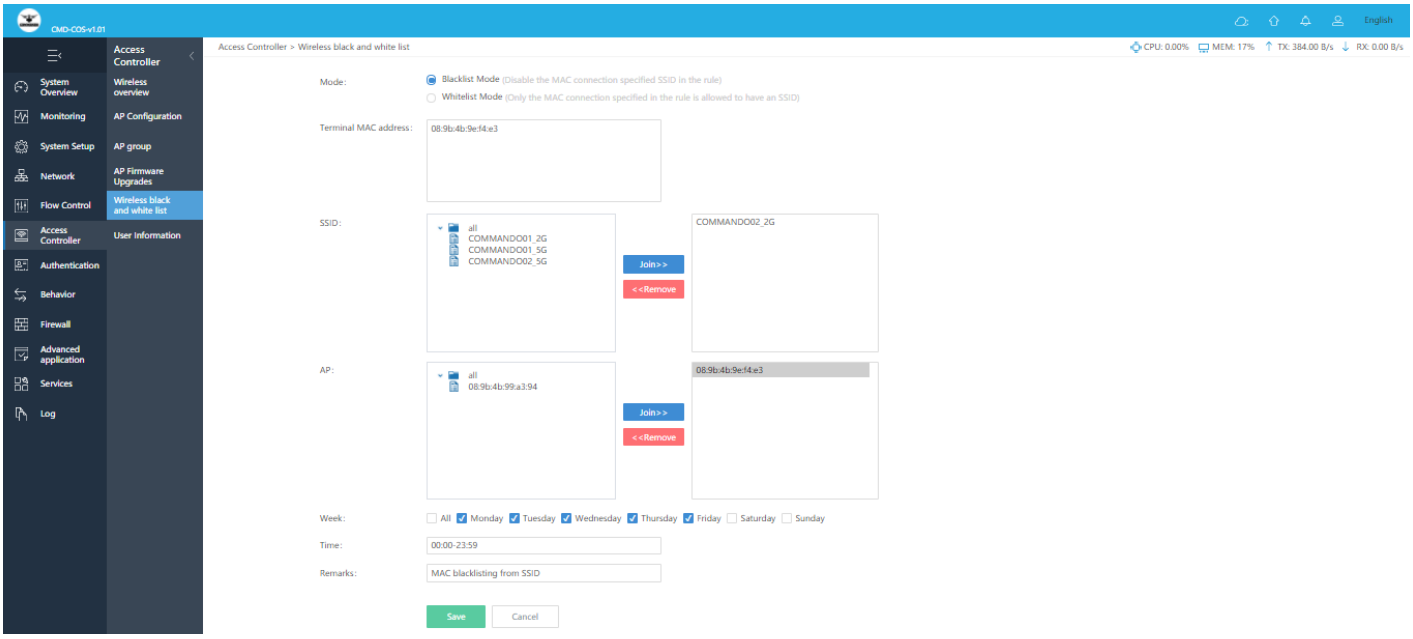
AP:
all

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

Time: 00:00-23:59

Remarks:

5.5.2 Add Wireless black and white list page



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: 08:9b:4b:9e:f4:e3

SSID:
all
COMMANDO01_2G
COMMANDO01_5G
COMMANDO02_5G

COMMANDO02_2G

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

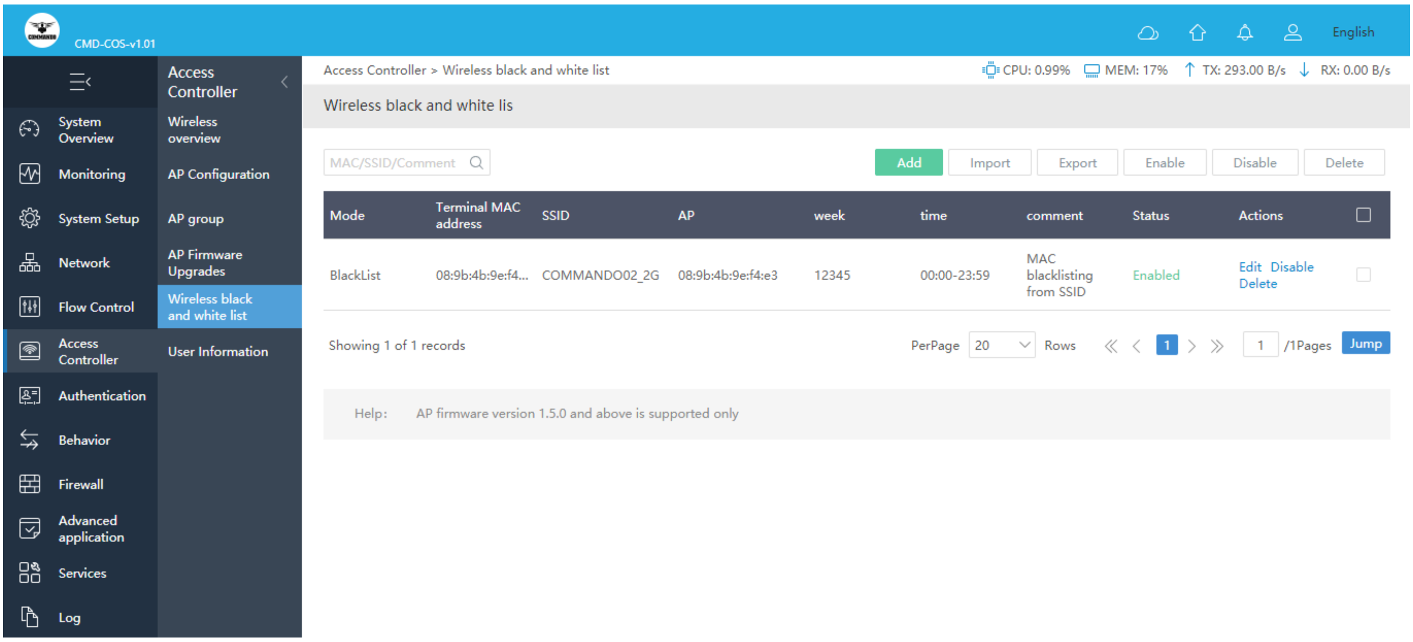
08:9b:4b:9e:f4:e3

Week: □ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Time: 00:00-23:59

Remarks: MAC blacklisting from SSID

5.5.3 Wireless blacklisting for particular MAC page



Access Controller > Wireless black and white list

Wireless black and white lis

Mode	Terminal MAC address	SSID	AP	week	time	comment	Status	Actions	□
BlackList	08:9b:4b:9e:f4...	COMMANDO02_2G	08:9b:4b:9e:f4:e3	12345	00:00-23:59	MAC blacklisting from SSID	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

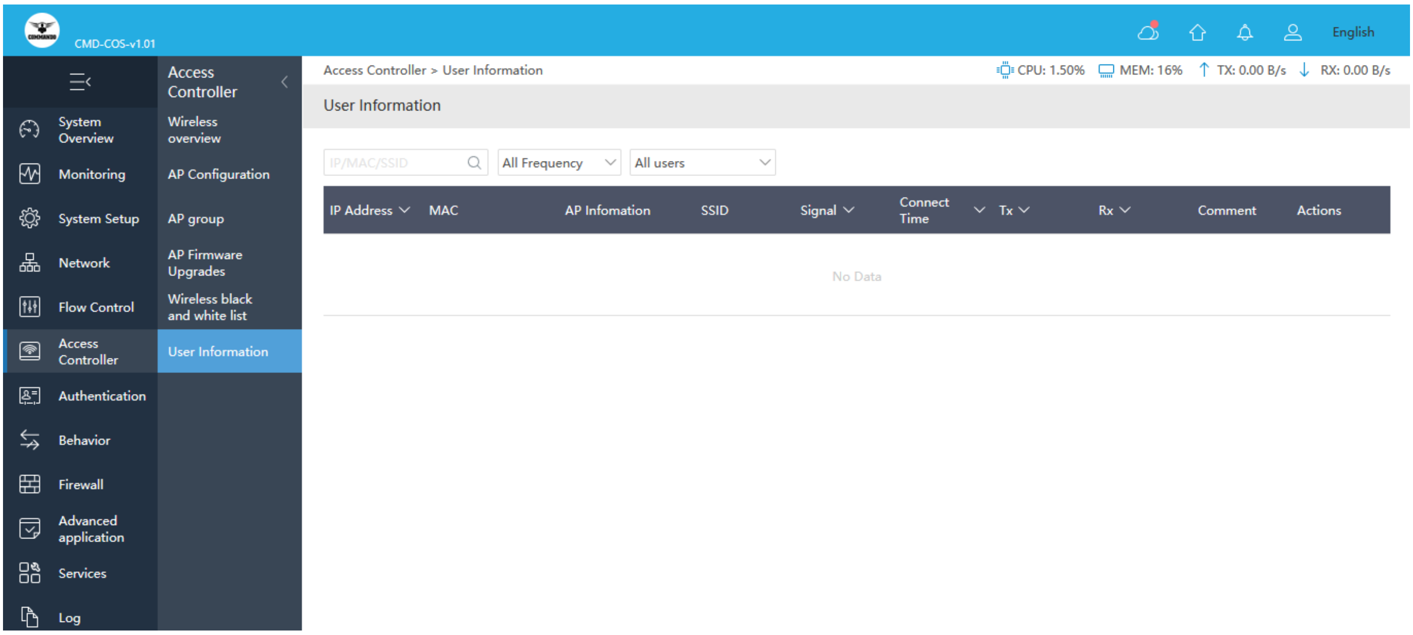
Help: AP firmware version 1.5.0 and above is supported only

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



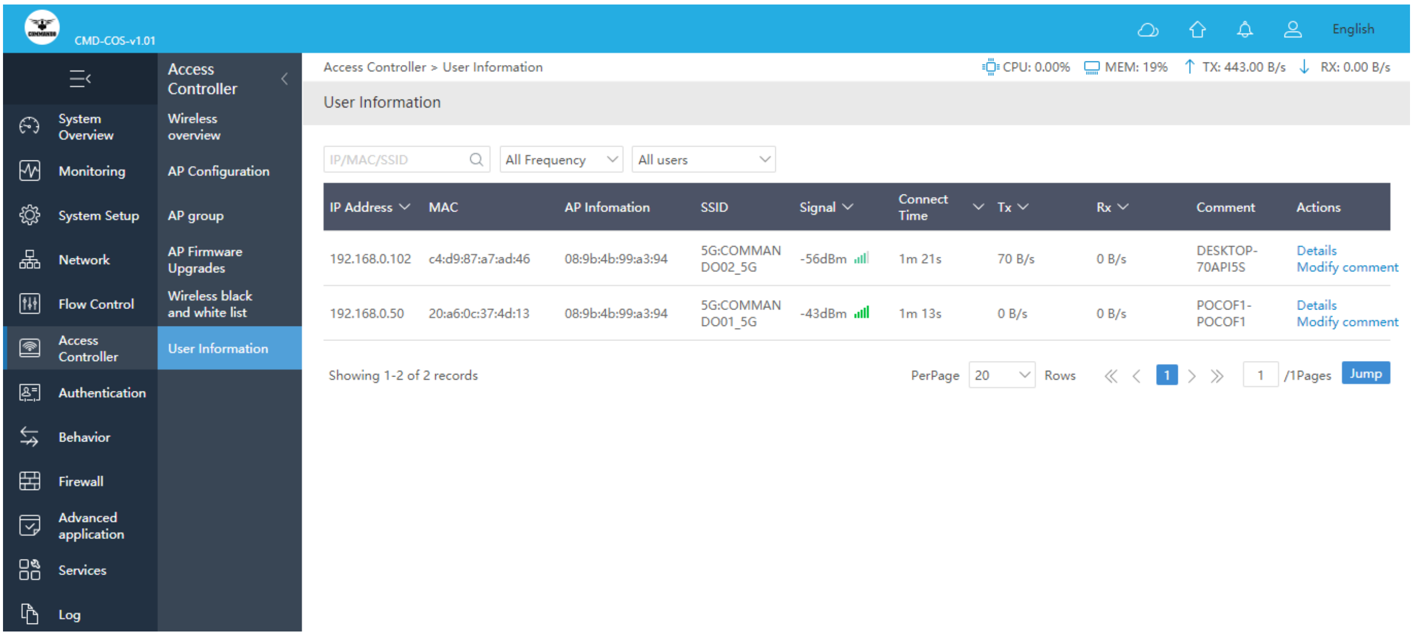
Access Controller > User Information

User Information

IP Address	MAC	AP Infomation	SSID	Signal	Connect Time	Tx	Rx	Comment	Actions

No Data

5.6.1 Default User Information page



Access Controller > User Information

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

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:COMMANDO02_5G	-56dBm	1m 21s	70 B/s	0 B/s	DESKTOP-70API5S	Details Modify comment
192.168.0.50	20:a6:0c:37:4d:13	08:9b:4b:99:a3:94	5G:COMMANDO01_5G	-43dBm	1m 13s	0 B/s	0 B/s	POCOF1-POCOF1	Details Modify comment

Showing 1-2 of 2 records

PerPage 20 Rows « ‹ 1 › » 1 /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

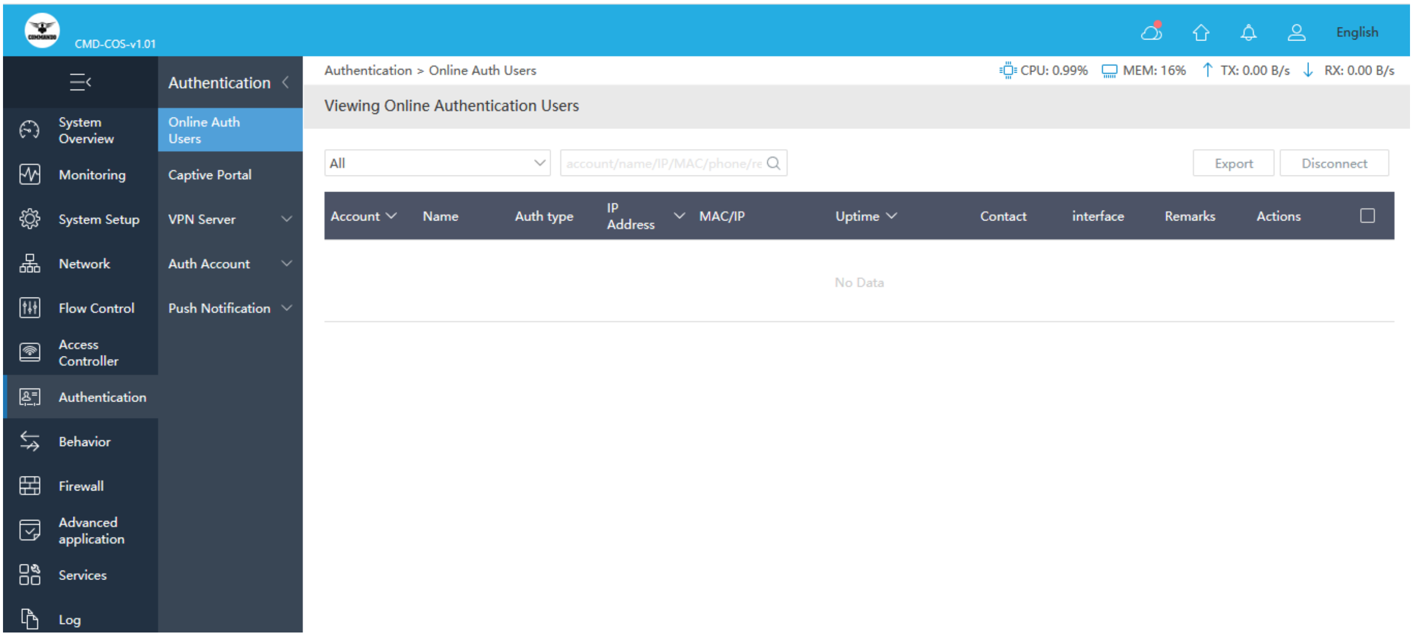


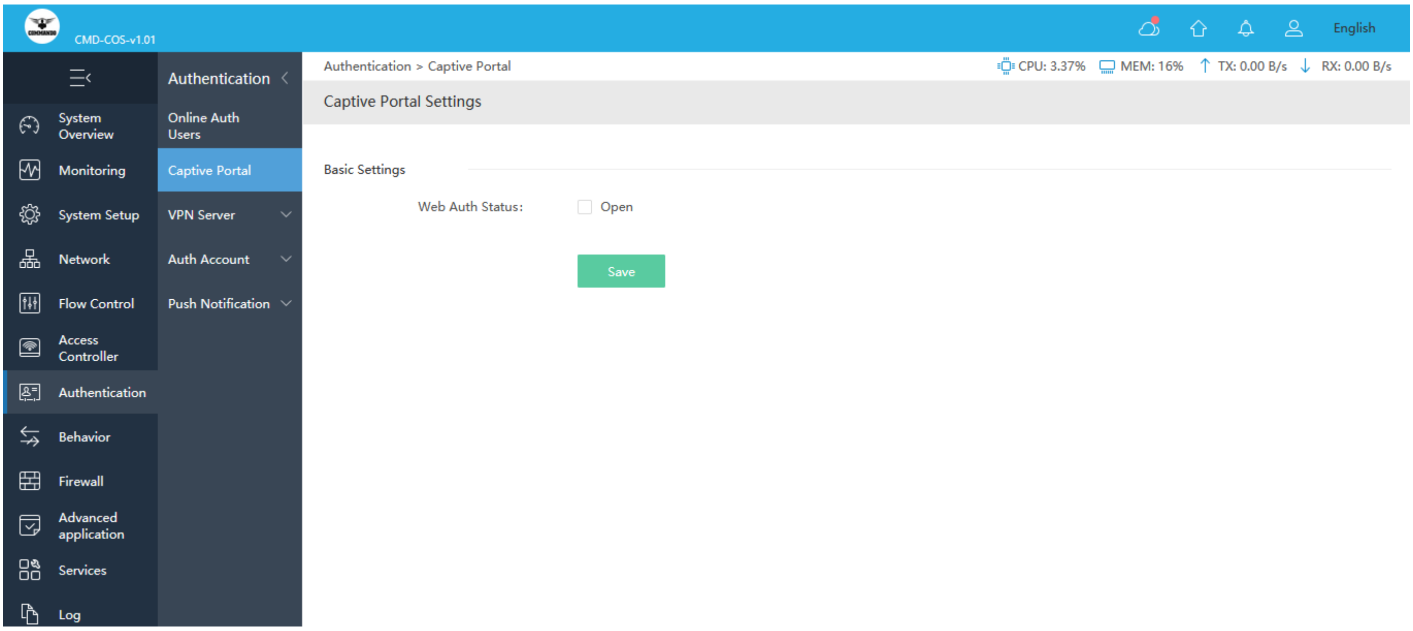
Fig 6.1.1 Default Online Authentication Users page

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



Captive Portal Settings

Basic Settings

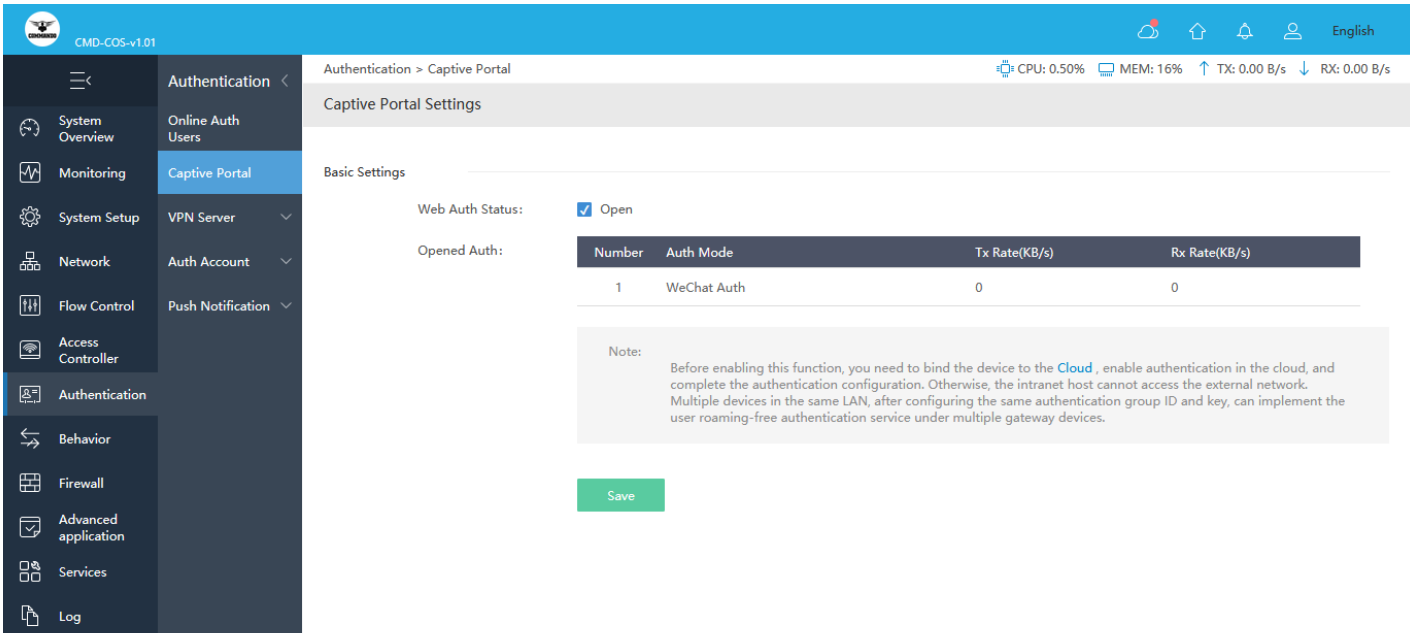
Web Auth Status: □ Open

Save

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.



Captive Portal Settings

Basic Settings

Web Auth Status: ☑ Open

Opened Auth:

Number	Auth Mode	Tx Rate(KB/s)	Rx Rate(KB/s)
1	WeChat Auth	0	0

Note:

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.

Save

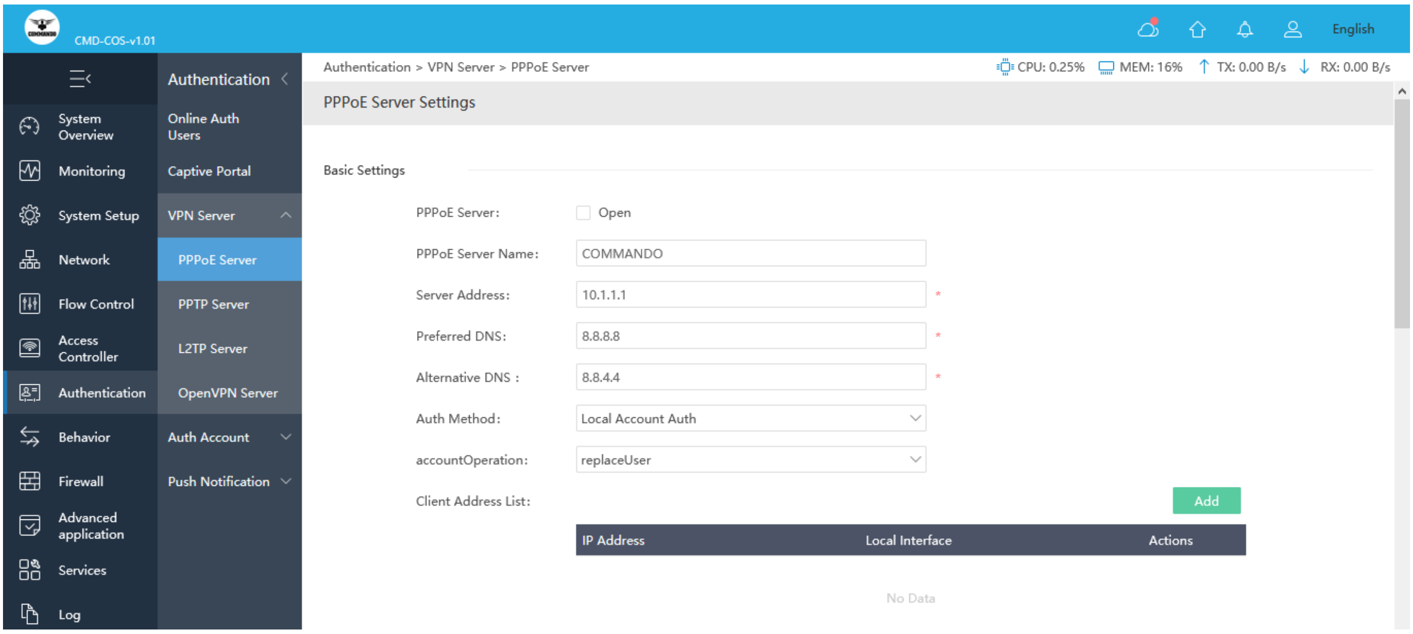
Fig 6.2.2. Enabling Captive Portal Settings page

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



PPPoE Server Settings

Basic Settings

PPPoE Server: □ Open

PPPoE Server Name: COMMANDO

Server Address: 10.1.1.1 *

Preferred DNS: 8.8.8.8 *

Alternative DNS : 8.8.4.4 *

Auth Method: Local Account Auth

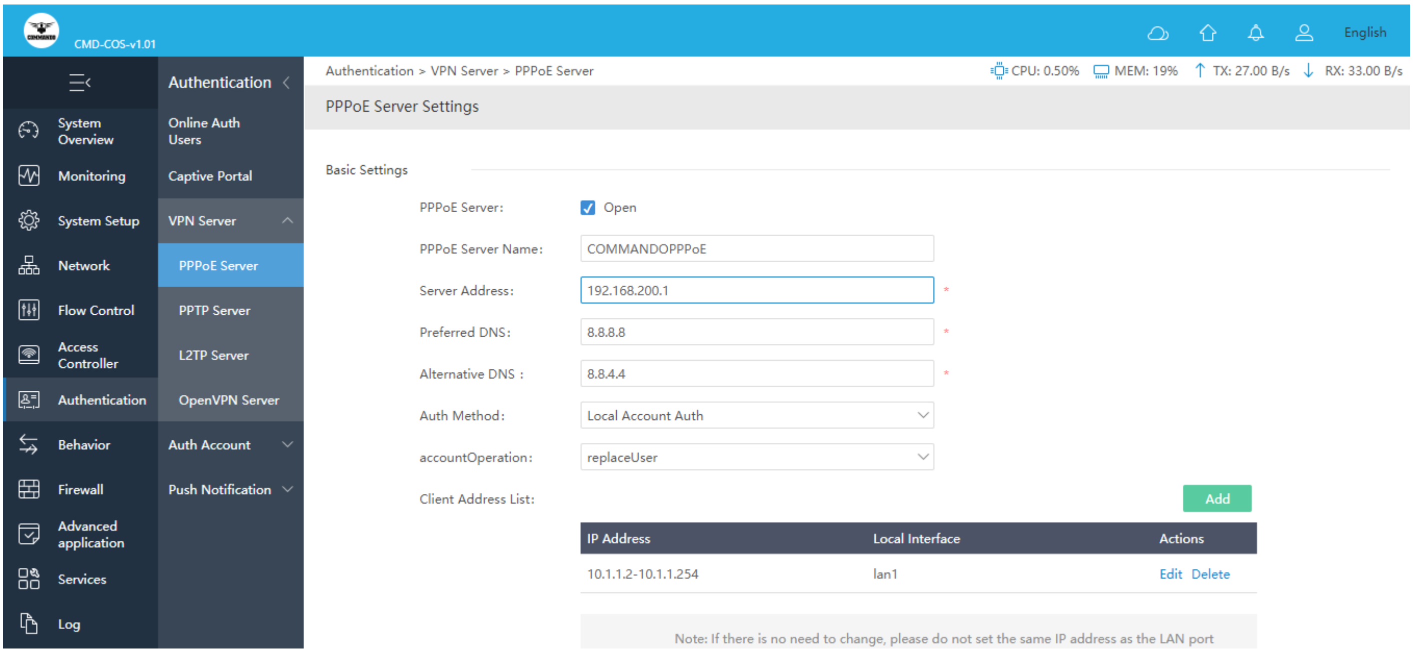
accountOperation: replaceUser

Client Address List: Add

IP Address	Local Interface	Actions

No Data

Fig 6.3.1 Default PPPoE Server Settings page



PPPoE Server Settings

Basic Settings

PPPoE Server: ☑ Open

PPPoE Server Name: COMMANDOPPPoE

Server Address: 192.168.200.1 *

Preferred DNS: 8.8.8.8 *

Alternative DNS : 8.8.4.4 *

Auth Method: Local Account Auth

accountOperation: replaceUser

Client Address List:

IP Address	Local Interface	Actions
10.1.1.2-10.1.1.254	lan1	Edit Delete

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**.**

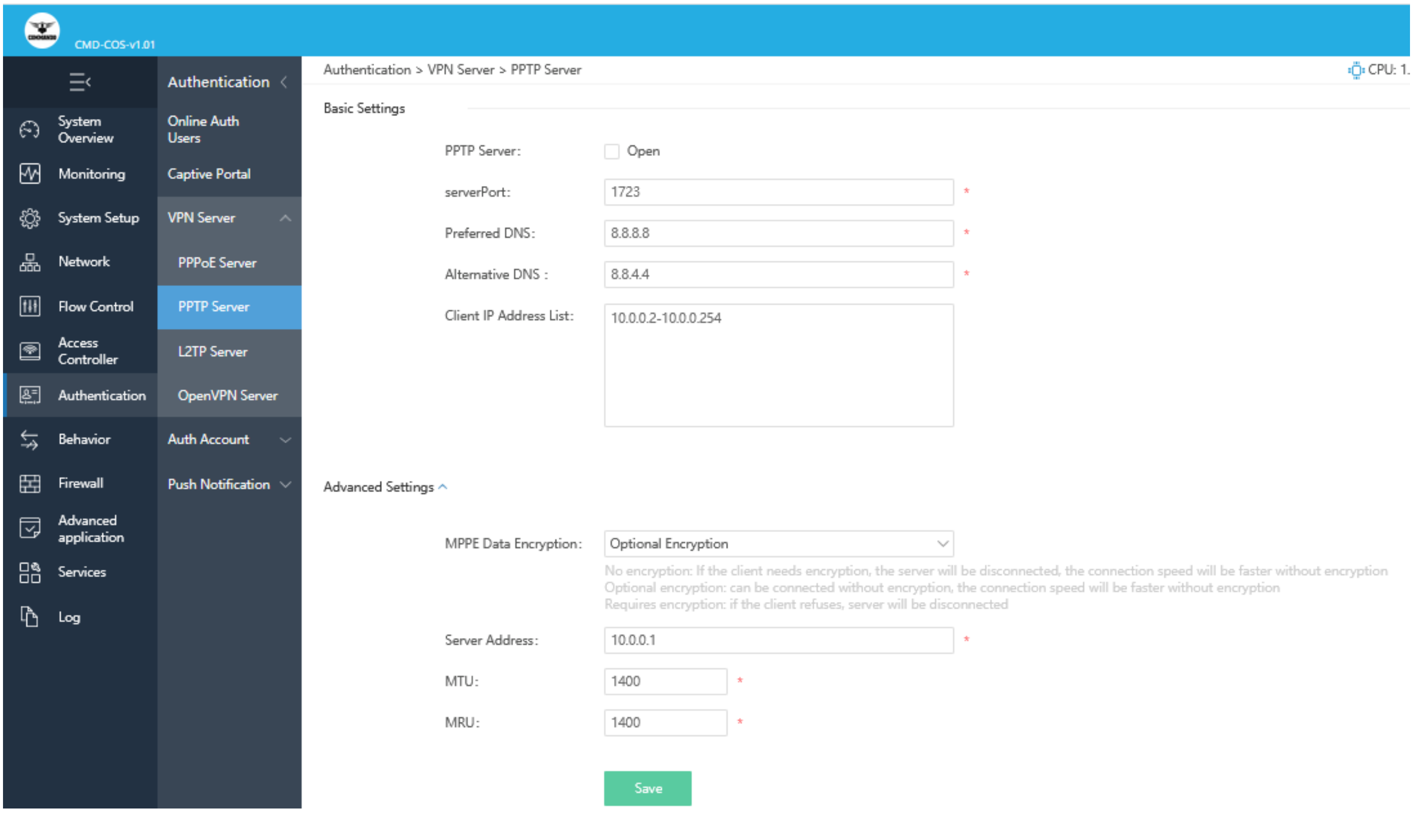
Note:

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: 1723 *

Preferred DNS: 8.8.8.8 *

Alternative DNS : 8.8.4.4 *

Client IP Address List: 10.0.0.2-10.0.0.254

Advanced Settings

MPPE Data Encryption: Optional Encryption

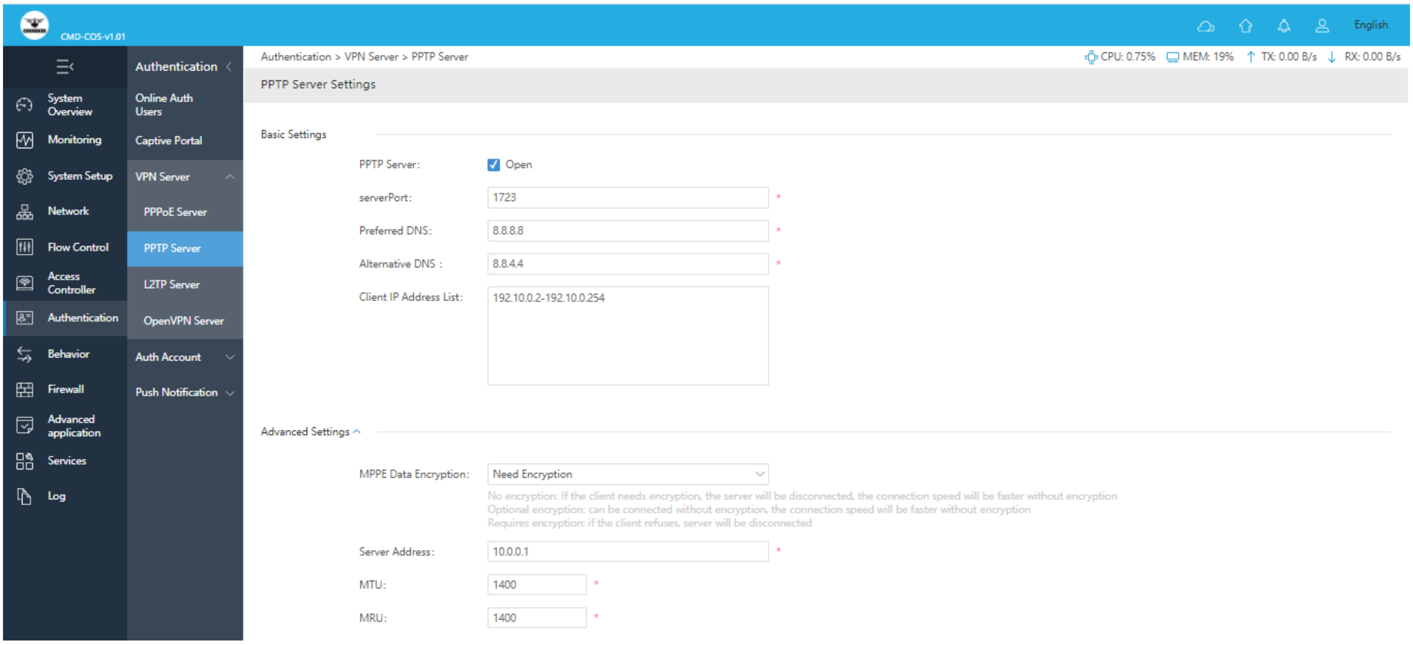
No encryption: If the client needs encryption, the server will be disconnected, the connection speed will be faster without encryption
Optional encryption: can be connected without encryption, the connection speed will be faster without encryption
Requires encryption: if the client refuses, server will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

Server Address: 10.0.0.1 *

MTU: 1400 *

MRU: 1400 *

6.3.3 Default PPTP Server Settings page



Authentication > VPN Server > PPTP Server

PPTP Server Settings

Basic Settings

PPTP Server: ☑ Open

serverPort: 1723 *

Preferred DNS: 8.8.8.8 *

Alternative DNS : 8.8.4.4 *

Client IP Address List: 192.10.0.2-192.10.0.254

Advanced Settings

MPPE Data Encryption: Need Encryption

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: 10.0.0.1 *

MTU: 1400 *

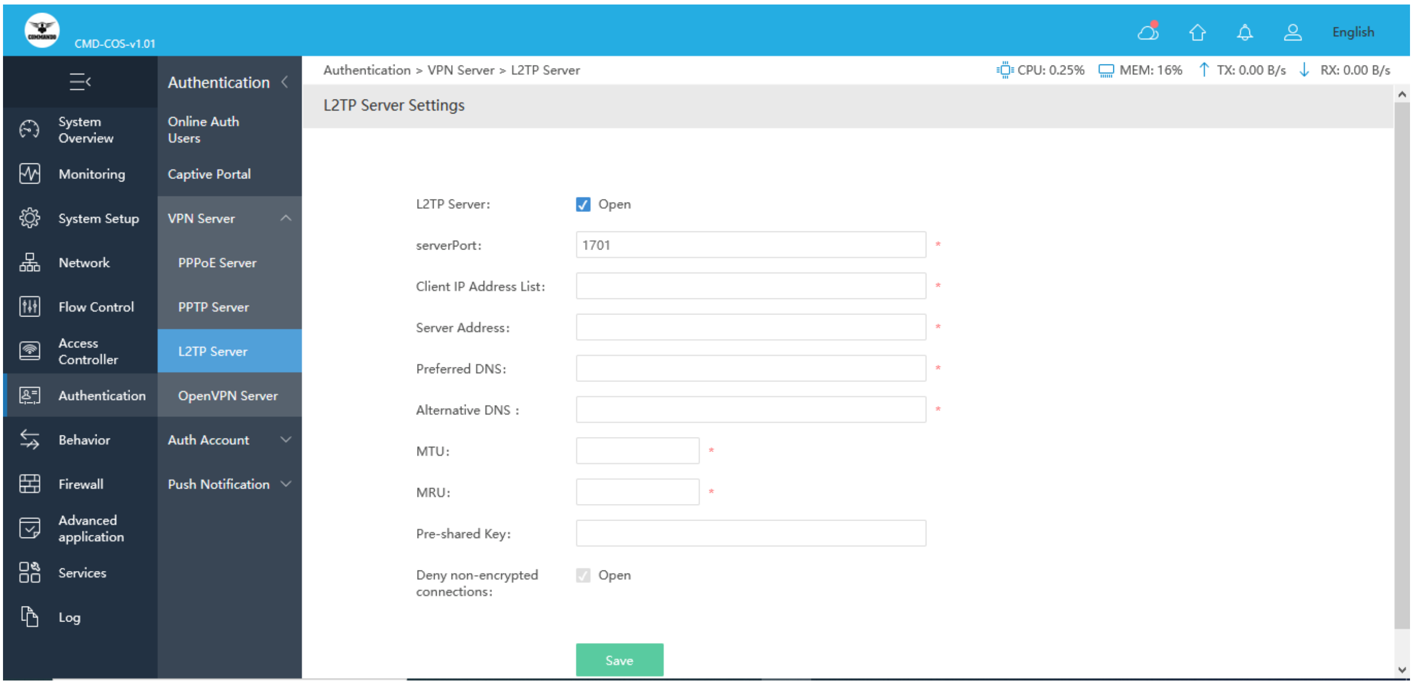
MRU: 1400 *

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



L2TP Server Settings

L2TP Server: ☑ Open

serverPort: 1701 *

Client IP Address List: *

Server Address: *

Preferred DNS: *

Alternative DNS : *

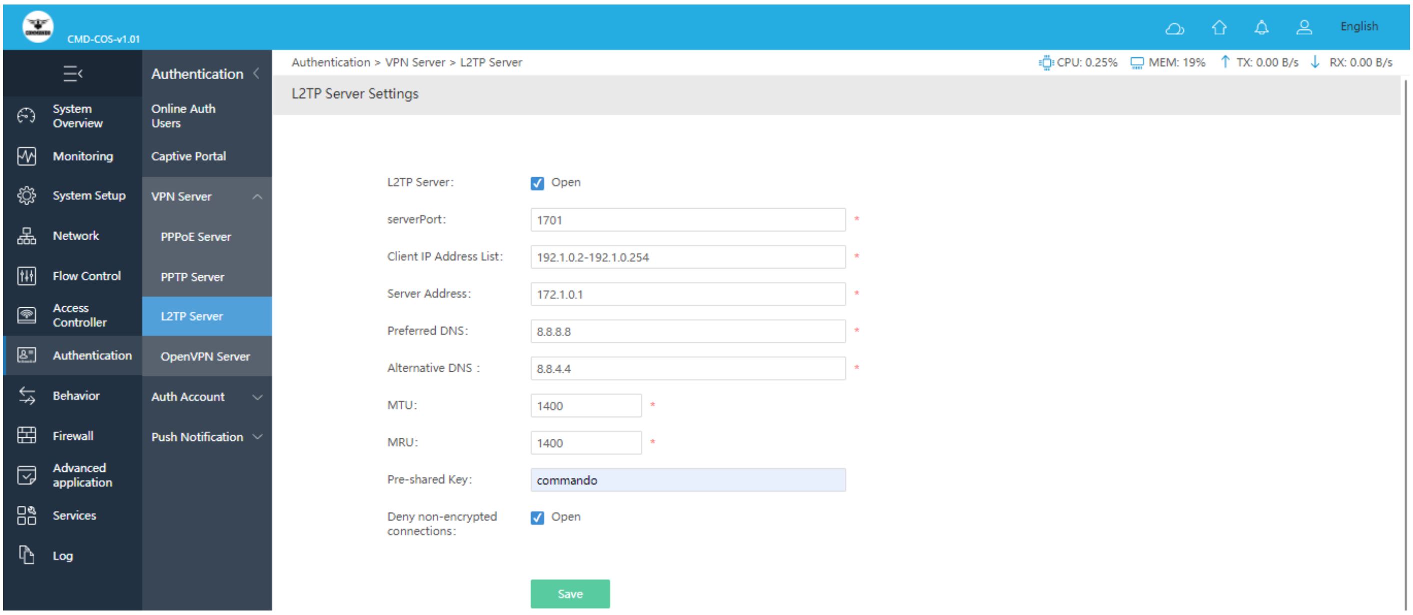
MTU: *

MRU: *

Pre-shared Key:

Deny non-encrypted connections: ☐ Open

Fig 6.3.5 Default L2TP Server Settings page



L2TP Server Settings

L2TP Server: ☑ Open

serverPort: 1701 *

Client IP Address List: 192.1.0.2-192.1.0.254 *

Server Address: 172.1.0.1 *

Preferred DNS: 8.8.8.8 *

Alternative DNS : 8.8.4.4 *

MTU: 1400 *

MRU: 1400 *

Pre-shared Key: commando

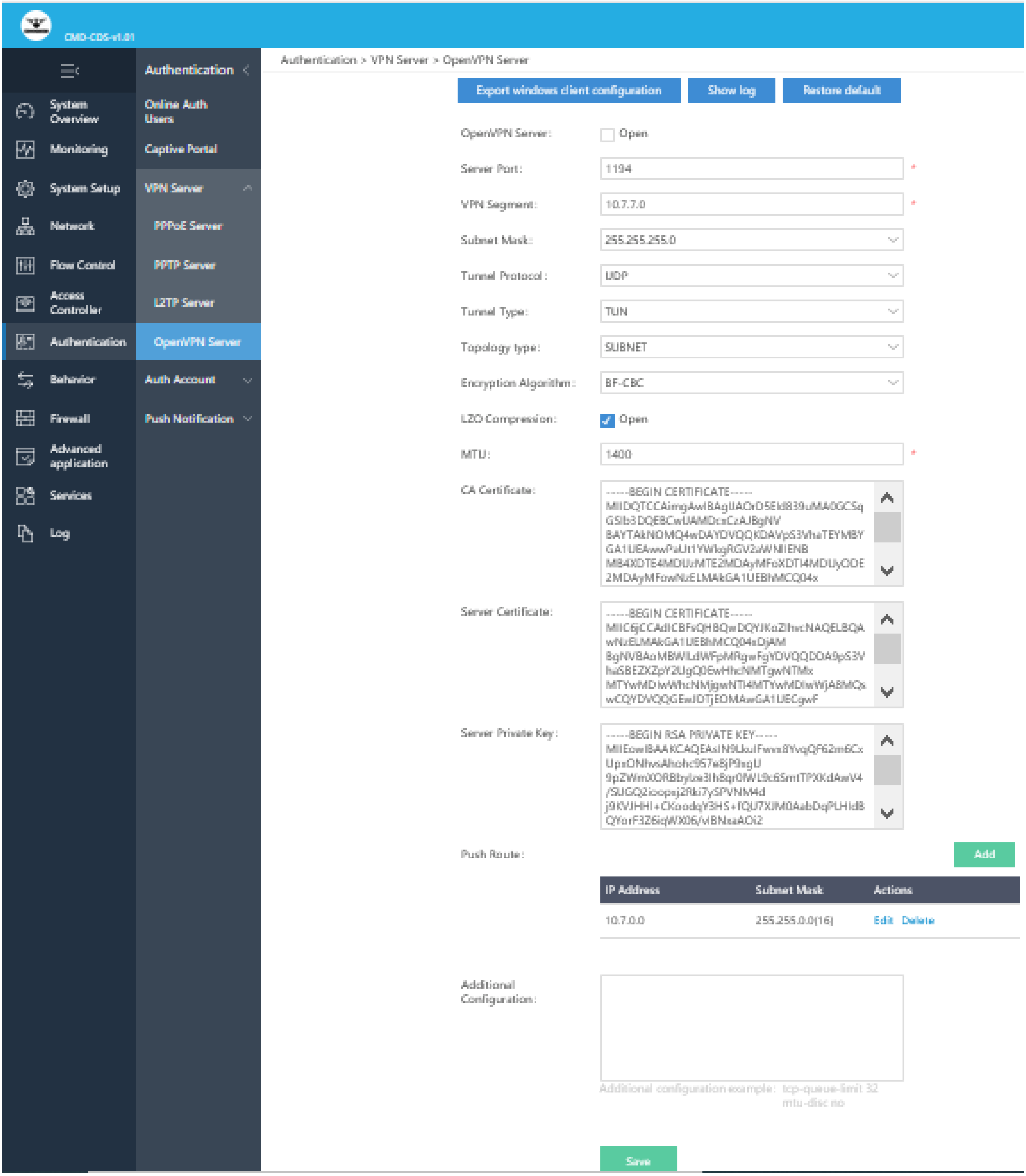
Deny non-encrypted connections: ☑ Open

Fig 6.3.6 Setting L2TP Server Settings page

OpenVPN Server Settings:

OpenVPN Access Server is a set of installation and configuration tools that come in one package that simplifies the rapid deployment of a VPN remote access solution. Thus, OpenVPN Access Server streamlines the configuration and management of an OpenVPN based secure remote access deployment. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

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



Authentication > VPN Server > OpenVPN Server

OpenVPN Server: □ Open

Server Port: 1194 *

VPN Segment: 10.7.7.0 *

Subnet Mask: 255.255.255.0

Tunnel Protocol: UDP

Tunnel Type: TUN

Topology type: SUBNET

Encryption Algorithm: BF-CBC

LZO Compression: ☑ Open

MTU: 1400 *

CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgIJAOrD5Ekl839uMA0GCSq
GSIb3DQEBCwUAMDcxCzAJBgNV
BAYTAkNOMQ4wDAYDVQQKDAVpS3VhaTEYMBY
GA1UEAwwPaUt1YWkgRGV2aWNlIENB
MB4XDTE4MDUxMTE2MDAyMFoXDTI4MDUyODE
2MDAyMFowNzELMAkGA1UEBhMCQ04x
```

Server Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC6jCCAdICBFxQHBQwDQYJKoZIhvcNAQELBQA
wNzELMAkGA1UEBhMCQ04xDjAM
BgNVBAoMBWlLdWFpMRgwFgYDVQQDDA9pS3V
haSBEZXZpY2UgQ0EwHhcNMTgwNTMx
MTYwMDIwWhcNMjgwNTI4MTYwMDIwWjA8MQs
wCQYDVQQGEwJDTjEOMAwGA1UECgwF
```

Server Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxIN9LkuIFwrx8YvqQF62m6Cx
UpxONlwsAhohc957e8jP9sgU
9pZWmXORBbyLw3lh8qr0fWL9c6SmTPXKdAwV4
/SUGQ2ioopsj2Rki7ySPVNM4d
j9KVJHHl+CKoodqY3HS+fQU7XJM0AabDqPLHIdB
QYorF3Z6iqWX06/vBNsaAOi2
```

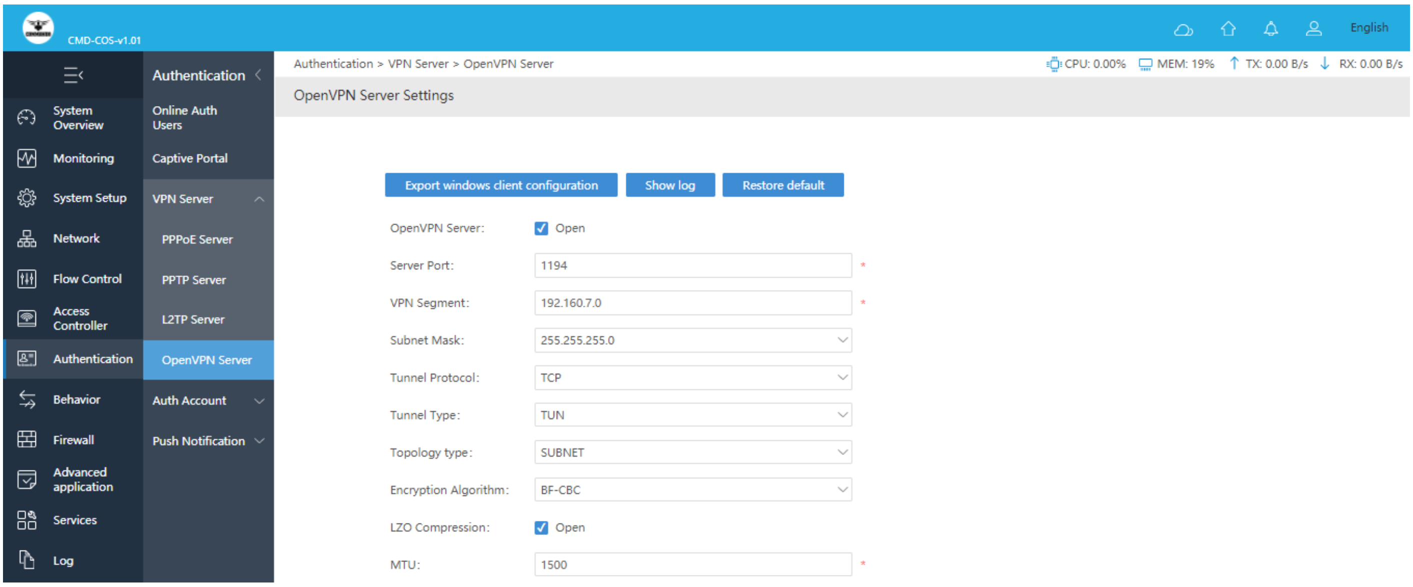
Push Route:

IP Address	Subnet Mask	Actions
10.7.0.0	255.255.0.0(16)	Edit Delete

Additional Configuration:

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

Fig 6.3.7 Default OpenVPN Server Settings page



Authentication > VPN Server > OpenVPN Server

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

OpenVPN Server Settings

OpenVPN Server: ☑ Open

Server Port: 1194 *

VPN Segment: 192.160.7.0 *

Subnet Mask: 255.255.255.0

Tunnel Protocol: TCP

Tunnel Type: TUN

Topology type: SUBNET

Encryption Algorithm: BF-CBC

LZO Compression: ☑ Open

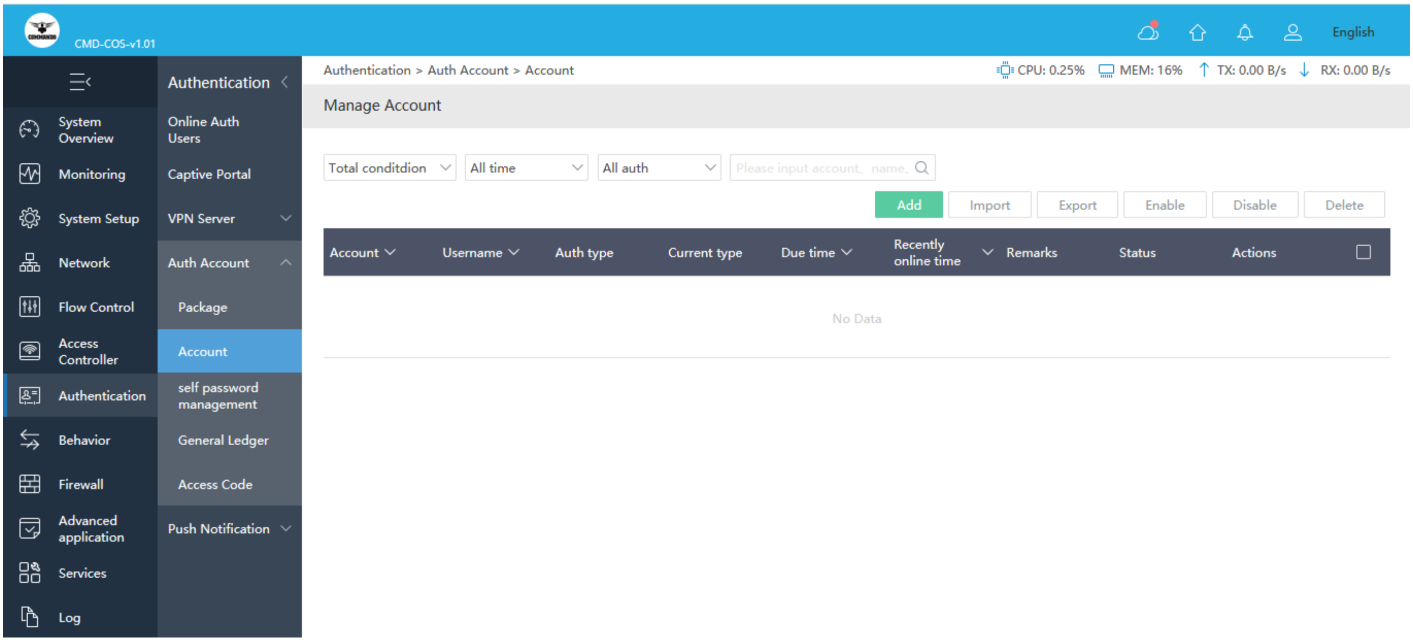
MTU: 1500 *

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



Authentication > Auth Account > Account

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

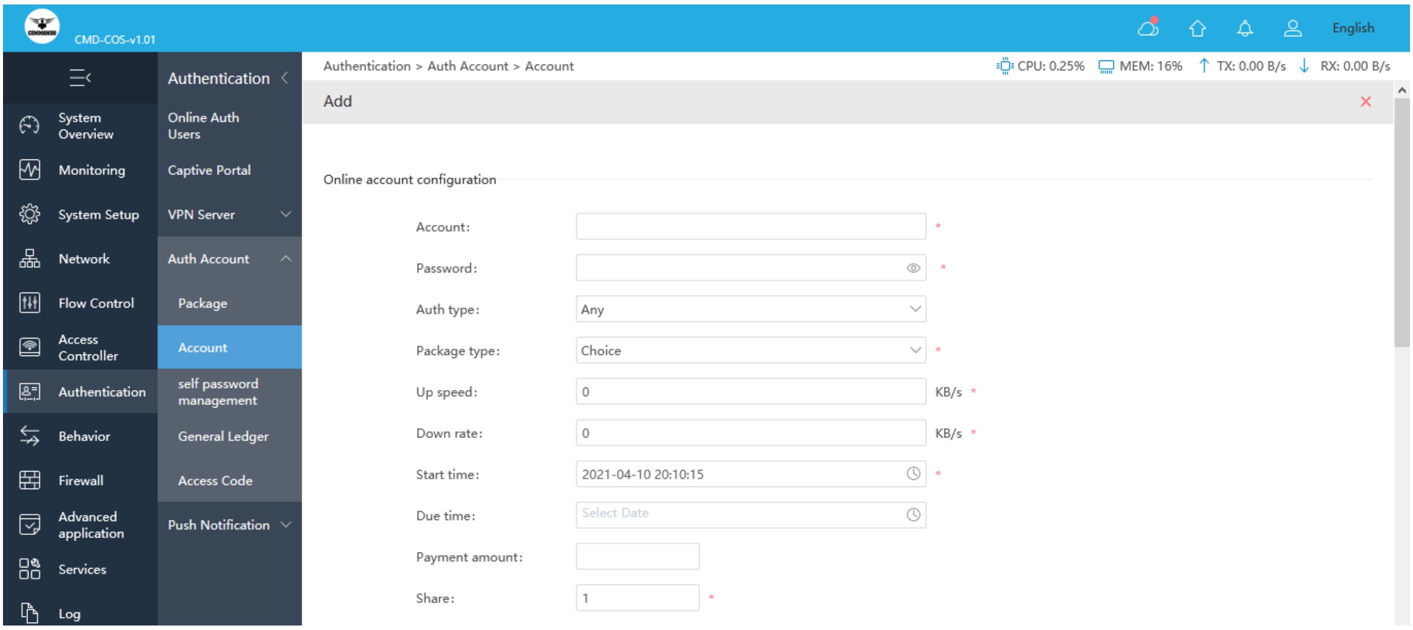
Manage Account

Total conditdion | All time | All auth | Please input account, name,

Account	Username	Auth type	Current type	Due time	Recently online time	Remarks	Status	Actions	□

No Data

Fig 6.4.1 Default Manage Package Account page



Add

Online account configuration

Account: *

Password: *

Auth type: Any

Package type: Choice *

Up speed: 0 KB/s *

Down rate: 0 KB/s *

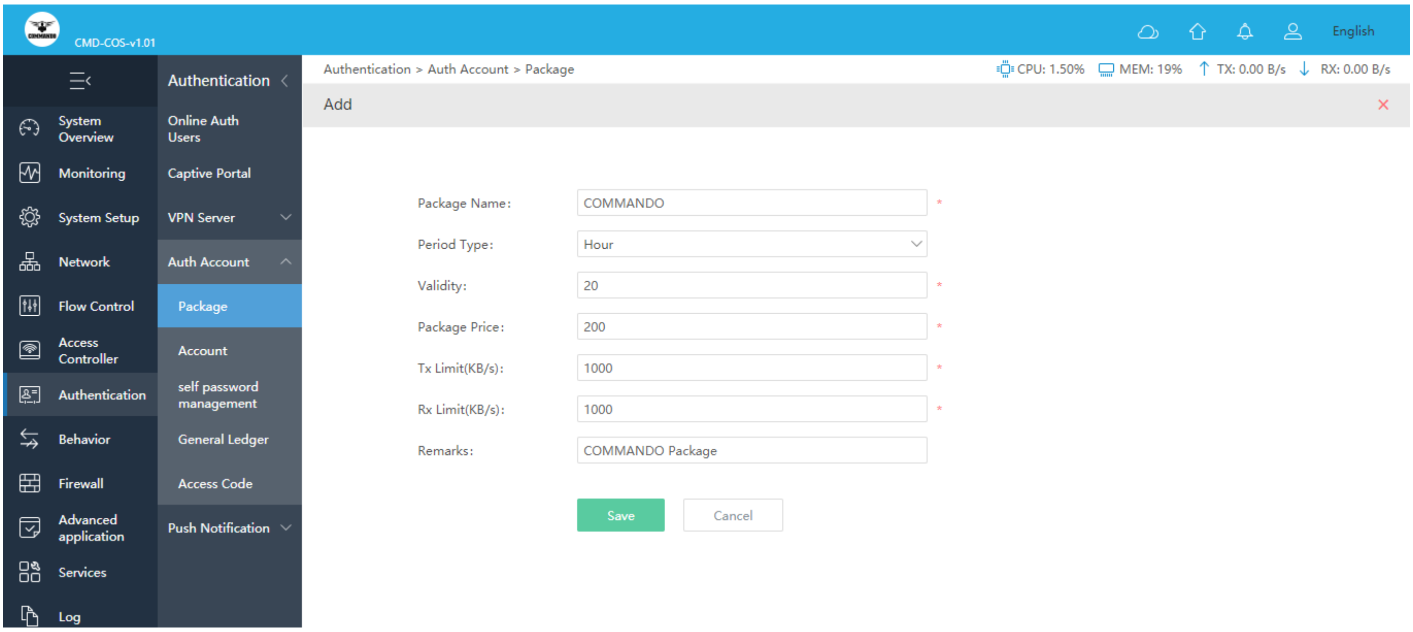
Start time: 2021-04-10 20:10:15 *

Due time: Select Date

Payment amount:

Share: 1 *

Fig 6.4.2 Add Online Account configuration page



Add

Package Name: COMMANDO *

Period Type: Hour

Validity: 20 *

Package Price: 200 *

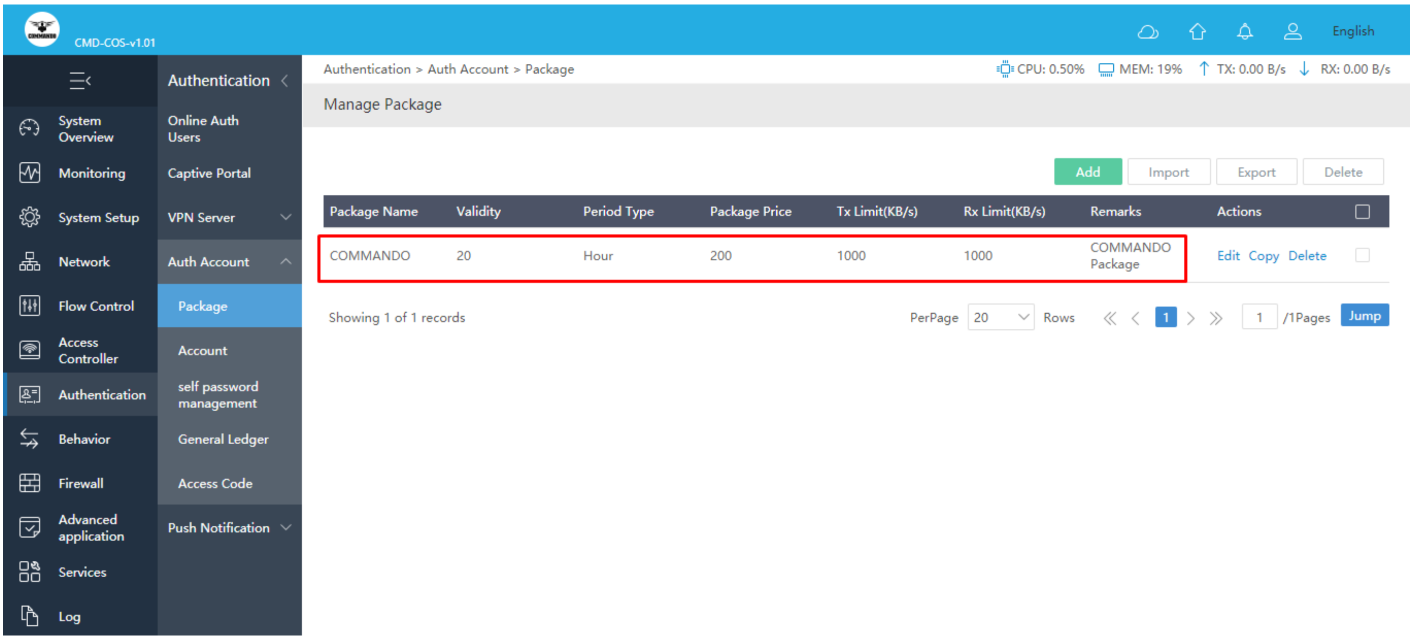
Tx Limit(KB/s): 1000 *

Rx Limit(KB/s): 1000 *

Remarks: COMMANDO Package

Save Cancel

Fig 6.4.3 Add particular Online Account configuration page



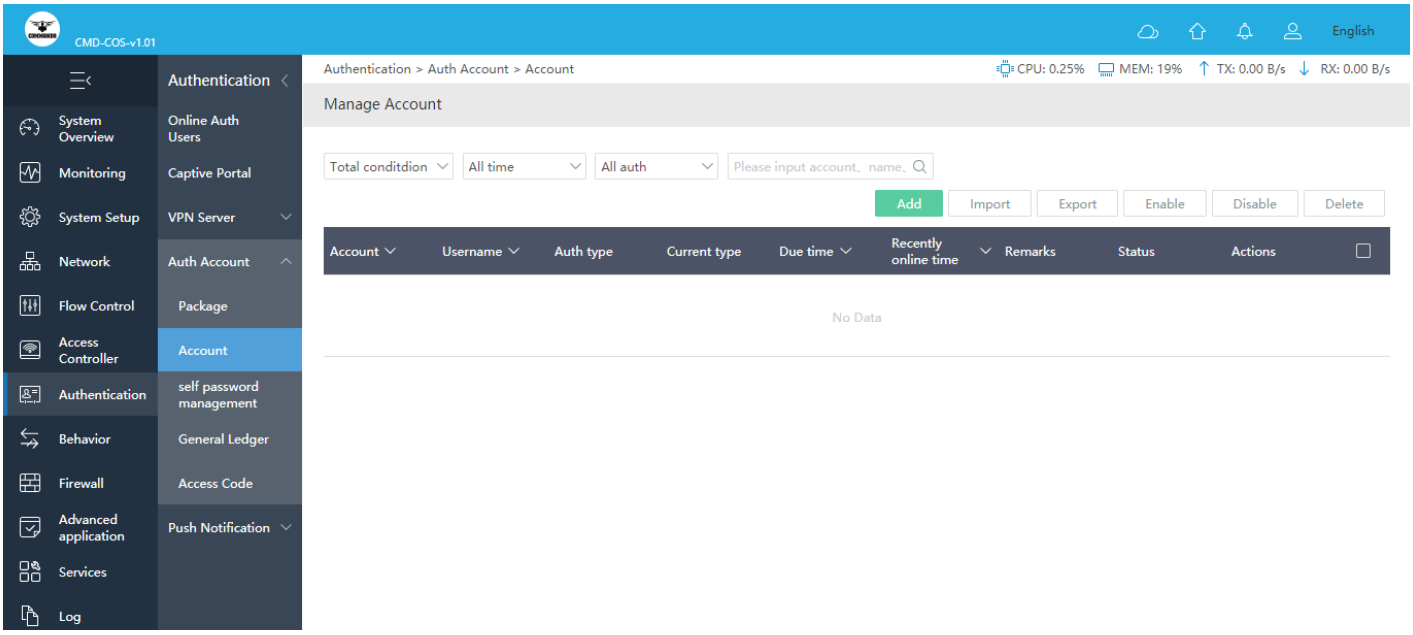
Package Name	Validity	Period Type	Package Price	Tx Limit(KB/s)	Rx Limit(KB/s)	Remarks	Actions	□
COMMANDO	20	Hour	200	1000	1000	COMMANDO Package	Edit Copy Delete	□

Fig 6.4.4 Manage package page

Manage Account:

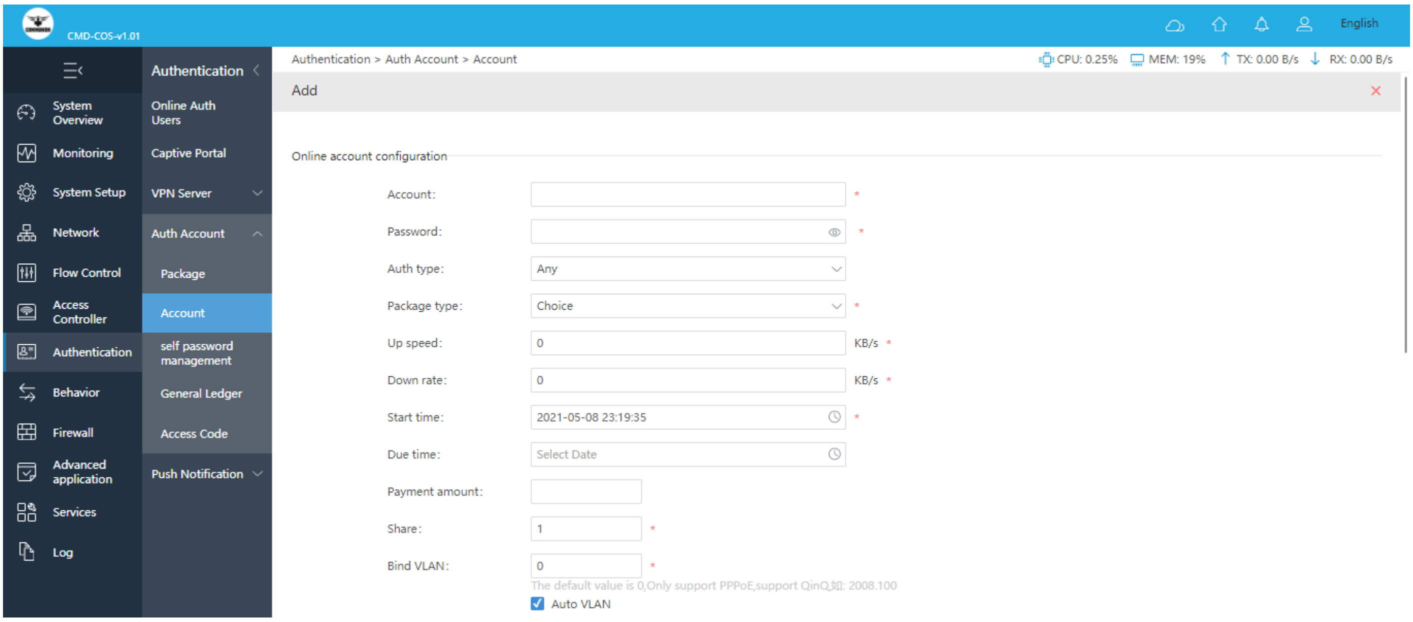
For creating and managing account use the following tabs.

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



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

Fig 6.4.5 Default Mange Account page



Authentication > Auth Account > Account

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:

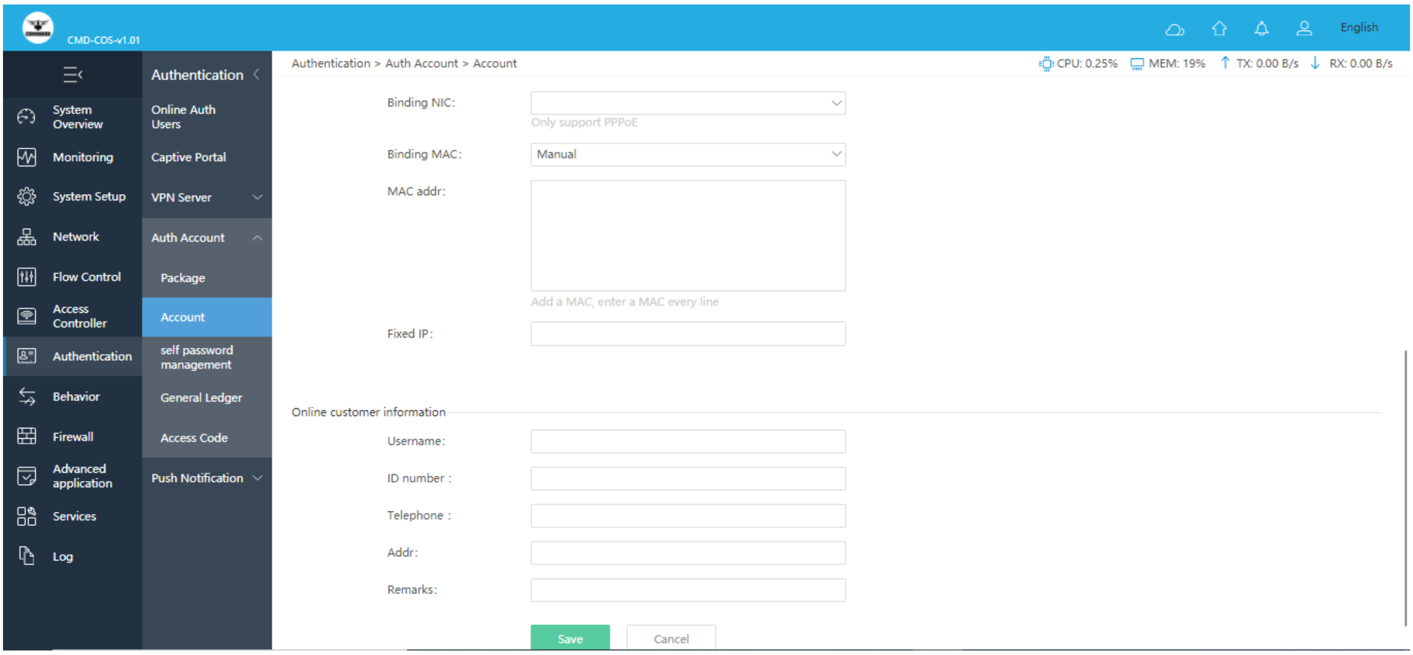
Share: 1 *

Bind VLAN: 0 *

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

☑ Auto VLAN

Fig 6.4.5 Add Manage Account page



Authentication > Auth Account > Account

Binding NIC:

Only support PPPoE

Binding MAC: Manual

MAC addr:

Add a MAC, enter a MAC every line

Fixed IP:

Online customer information

Username:

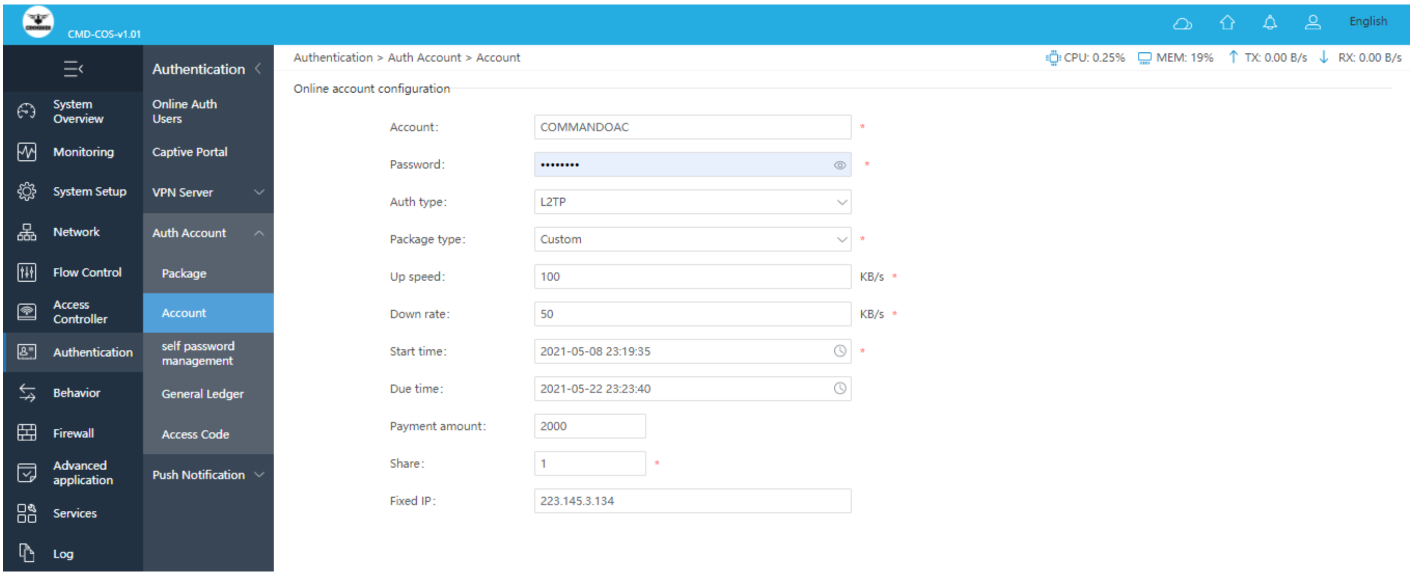
ID number :

Telephone :

Addr:

Remarks:

Fig 6.4.6 Add Online account configuration page

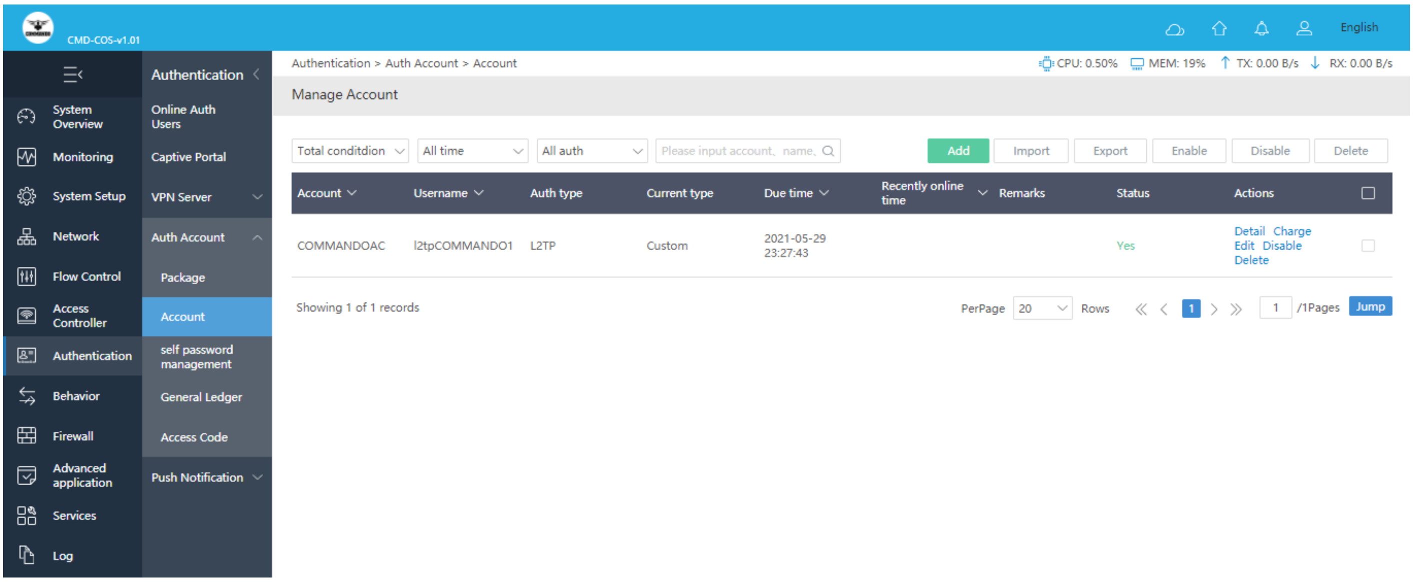


Authentication > Auth Account > Account

Online account configuration

Account:	COMMANDOAC *
Password:	•••••••• *
Auth type:	L2TP
Package type:	Custom *
Up speed:	100 KB/s *
Down rate:	50 KB/s *
Start time:	2021-05-08 23:19:35 *
Due time:	2021-05-22 23:23:40
Payment amount:	2000
Share:	1 *
Fixed IP:	223.145.3.134

Fig 6.4.7 Add particular Online account configuration page



Authentication > Auth Account > Account

Manage Account

Account	Username	Auth type	Current type	Due time	Recently online time	Remarks	Status	Actions	□
COMMANDOAC	l2tpCOMMANDO1	L2TP	Custom	2021-05-29 23:27:43			Yes	Detail Charge Edit Disable Delete	□

Showing 1 of 1 records

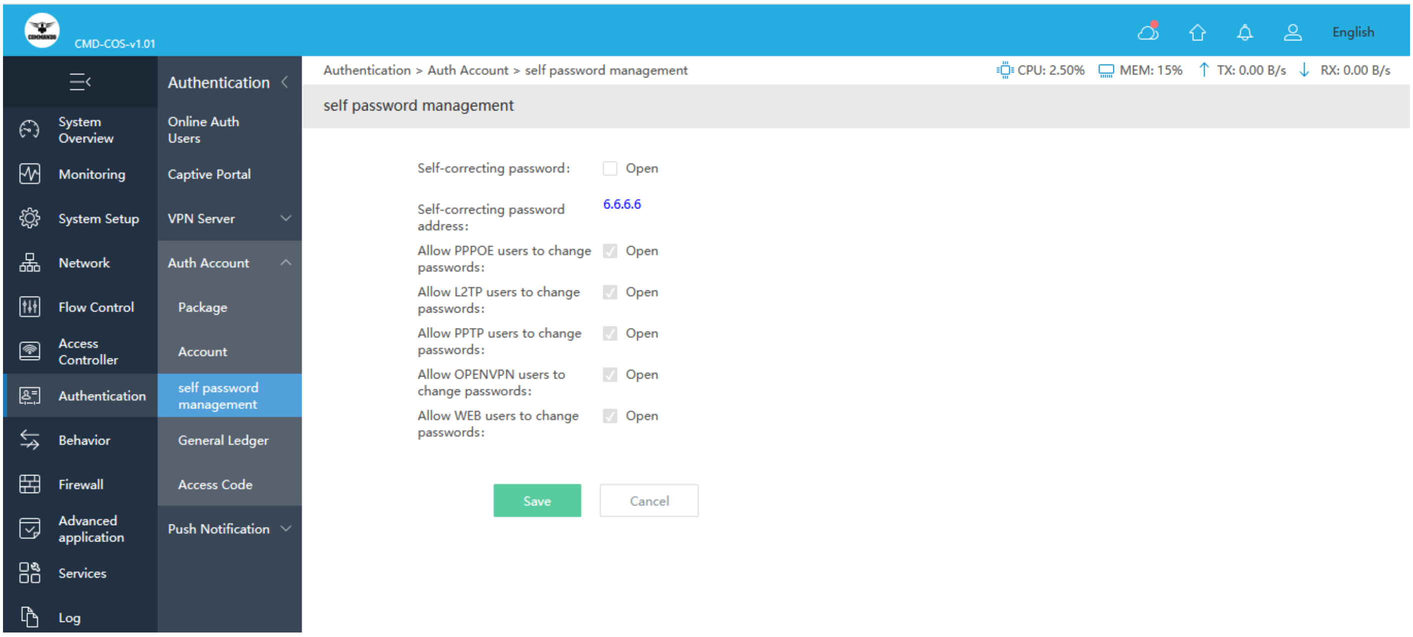
PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

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



self password management

Self-correcting password: □ Open

Self-correcting password address: 6.6.6.6

Allow PPPOE users to change passwords: ☑ Open

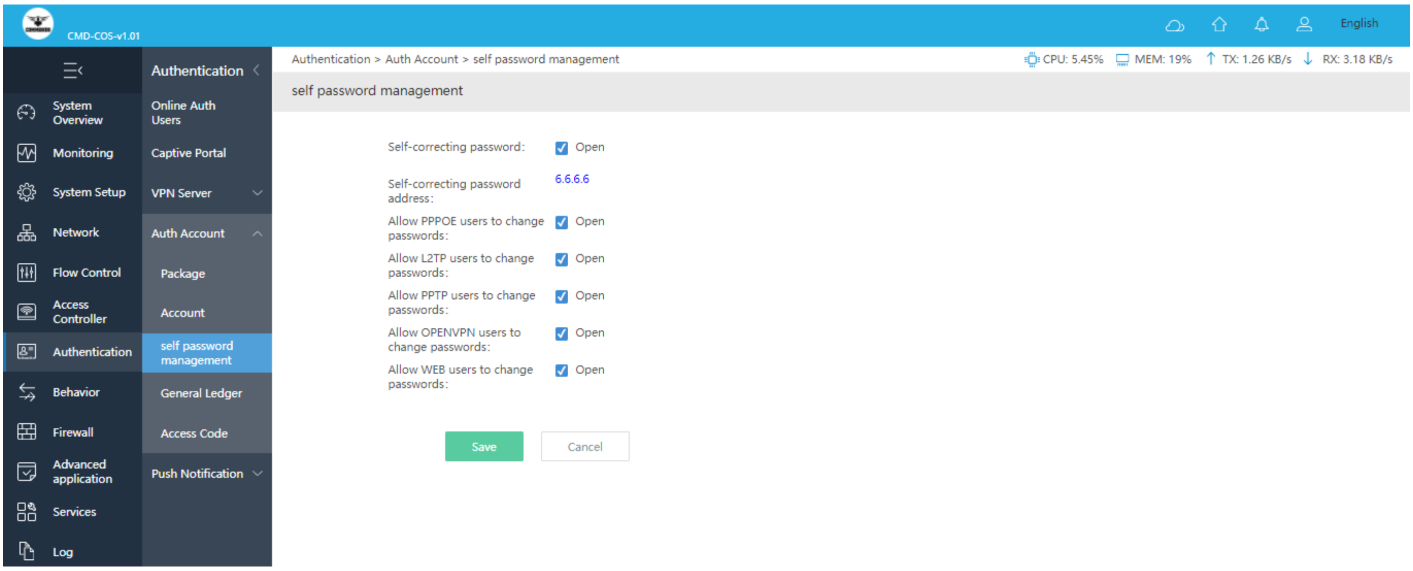
Allow L2TP users to change passwords: ☑ Open

Allow PPTP users to change passwords: ☑ Open

Allow OPENVPN users to change passwords: ☑ Open

Allow WEB users to change passwords: ☑ Open

Fig 6.4.9 Default self password management page



self password management

Self-correcting password: ☑ Open

Self-correcting password address: 6.6.6.6

Allow PPPOE users to change passwords: ☑ Open

Allow L2TP users to change passwords: ☑ Open

Allow PPTP users to change passwords: ☑ Open

Allow OPENVPN users to change passwords: ☑ Open

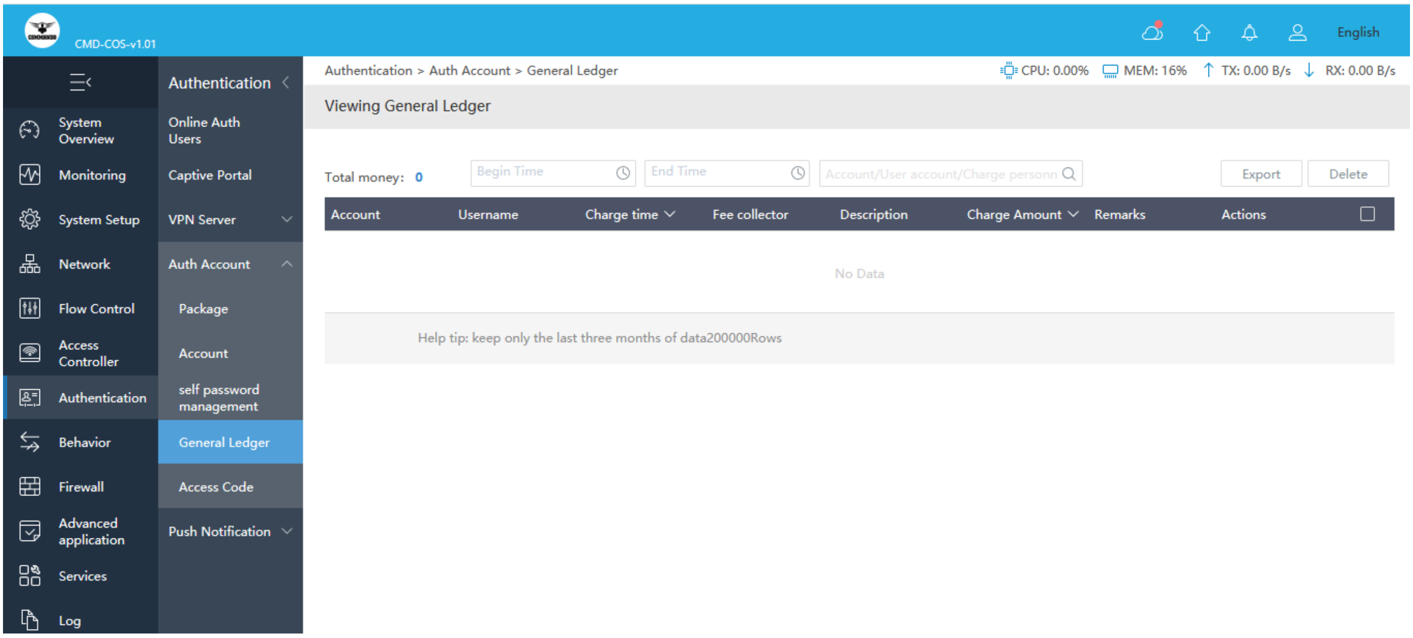
Allow WEB users to change passwords: ☑ Open

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



Viewing General Ledger

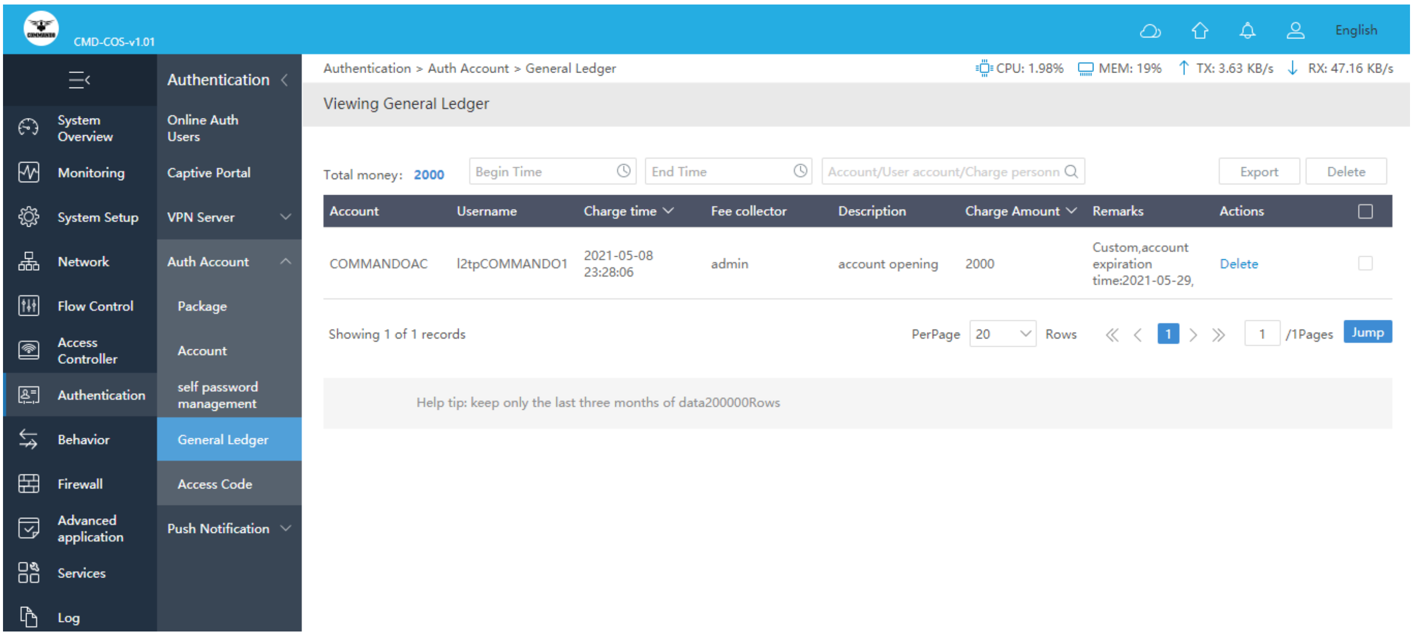
Total money: 0

Account	Username	Charge time	Fee collector	Description	Charge Amount	Remarks	Actions	□

No Data

Help tip: keep only the last three months of data200000Rows

Fig 6.4.11 Default General Ledger page



Viewing General Ledger

Total money: 2000

Account	Username	Charge time	Fee collector	Description	Charge Amount	Remarks	Actions	□
COMMANDOAC	l2tpCOMMANDO1	2021-05-08 23:28:06	admin	account opening	2000	Custom,account expiration time:2021-05-29,	Delete	□

Showing 1 of 1 records PerPage 20 Rows 1 1 /1Pages

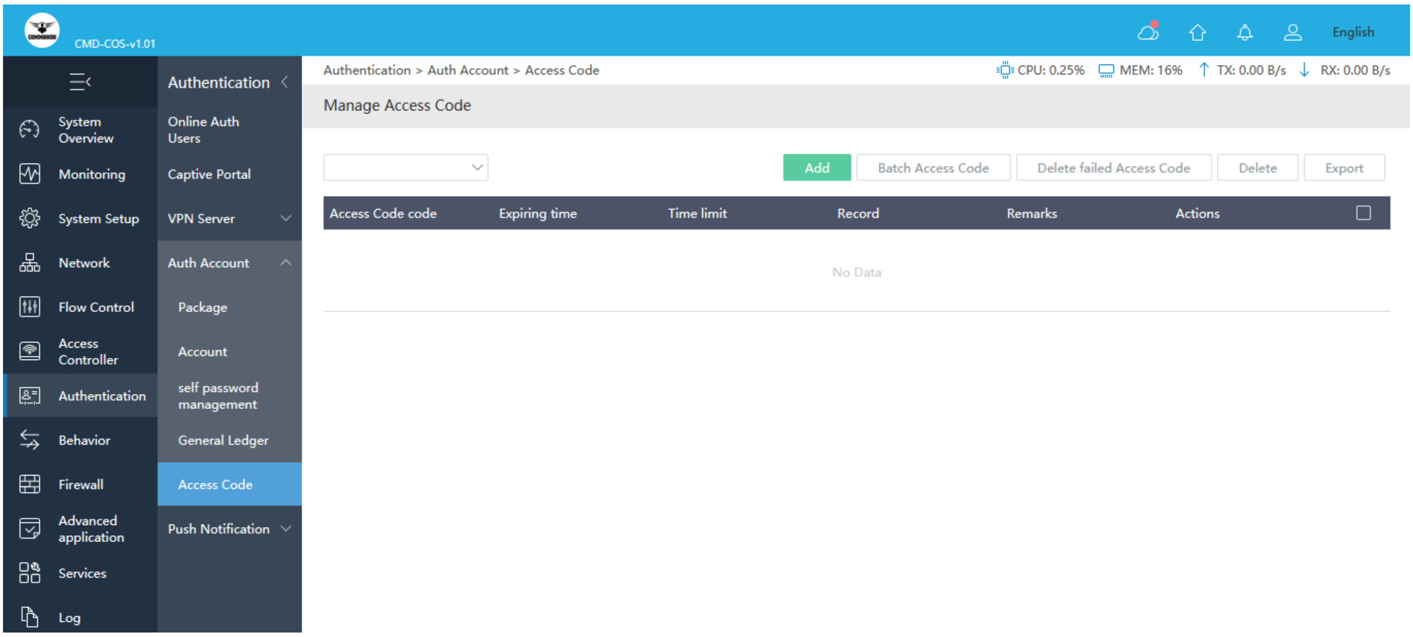
Help tip: keep only the last three months of data200000Rows

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



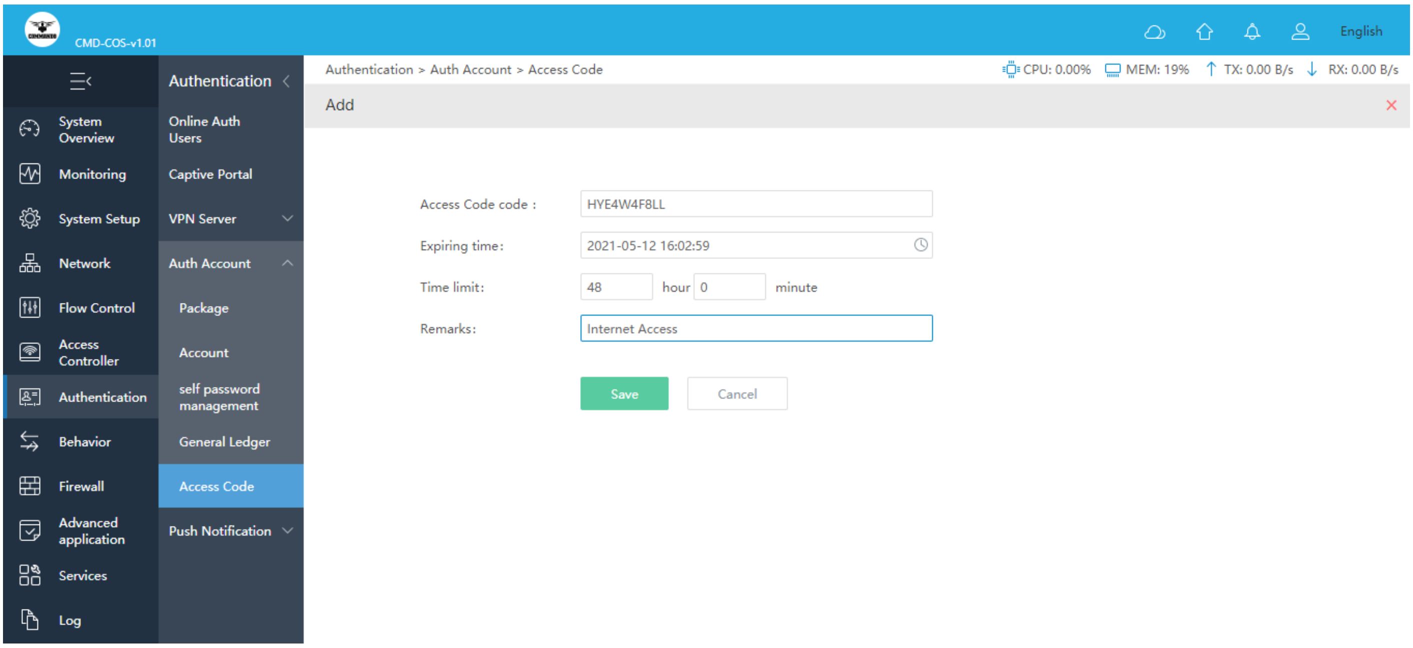
Authentication > Auth Account > Access Code

Manage Access Code

Access Code code	Expiring time	Time limit	Record	Remarks	Actions	□

No Data

Fig 6.4.13 Default Manage Access Code page



Authentication > Auth Account > Access Code

Add

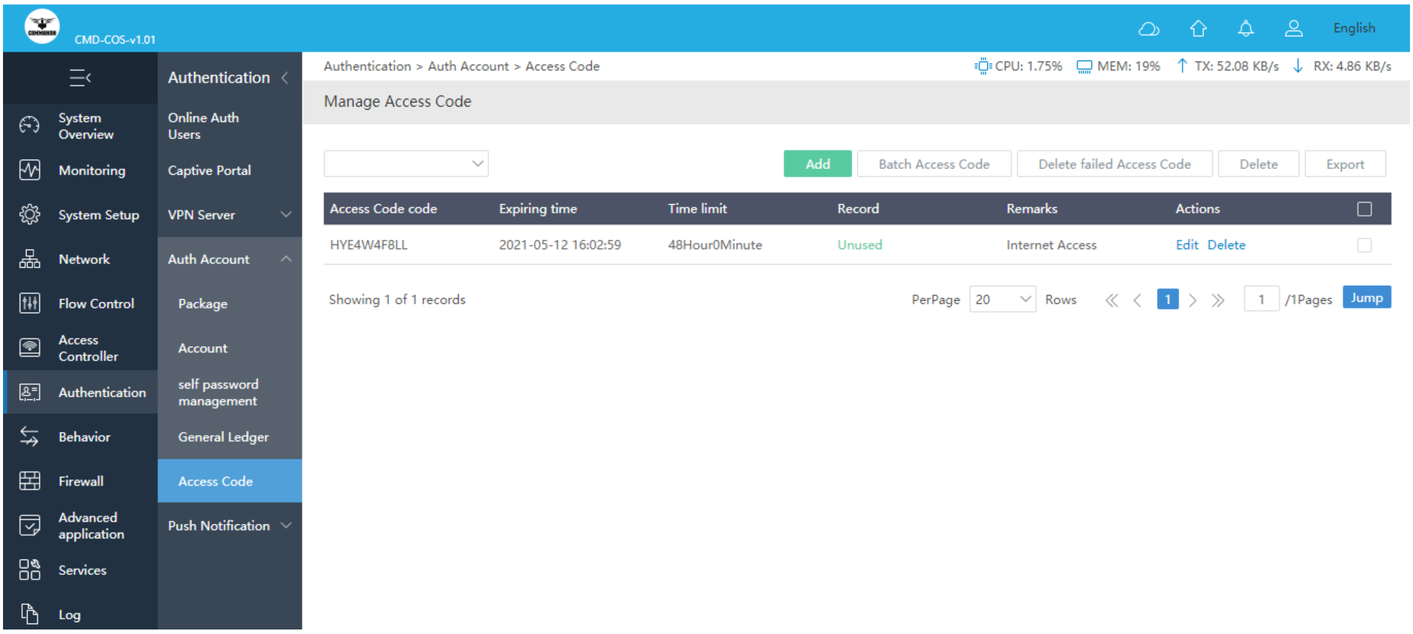
Access Code code : HYE4W4F8LL

Expiring time: 2021-05-12 16:02:59

Time limit: 48 hour 0 minute

Remarks: Internet Access

Fig 6.4.14 Add Manage Access Code page



Authentication > Auth Account > Access Code

CPU: 1.75% MEM: 19% TX: 52.08 KB/s RX: 4.86 KB/s

Manage Access Code

Access Code code	Expiring time	Time limit	Record	Remarks	Actions	□
HYE4W4F8LL	2021-05-12 16:02:59	48Hour0Minute	Unused	Internet Access	Edit Delete	□

Showing 1 of 1 records

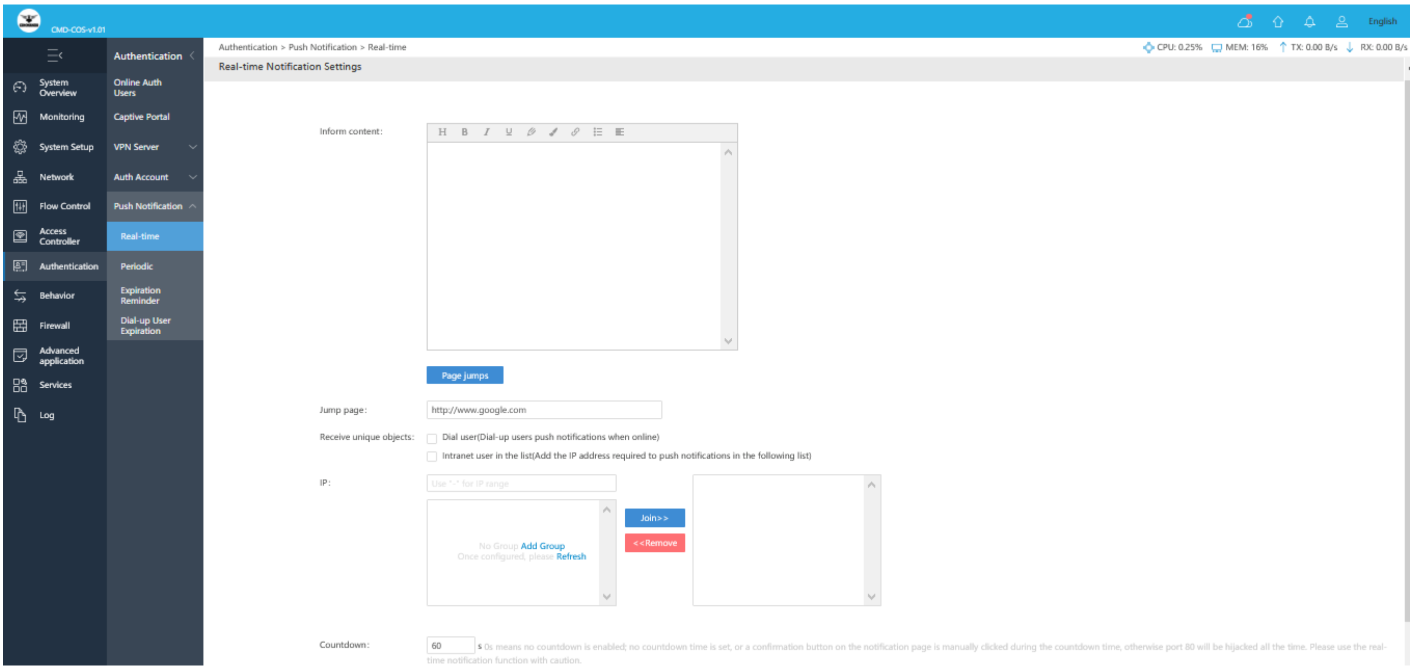
Fig 6.4.15 Manage Access Code page

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



Authentication > Push Notification > Real-time

Real-time Notification Settings

Inform content:

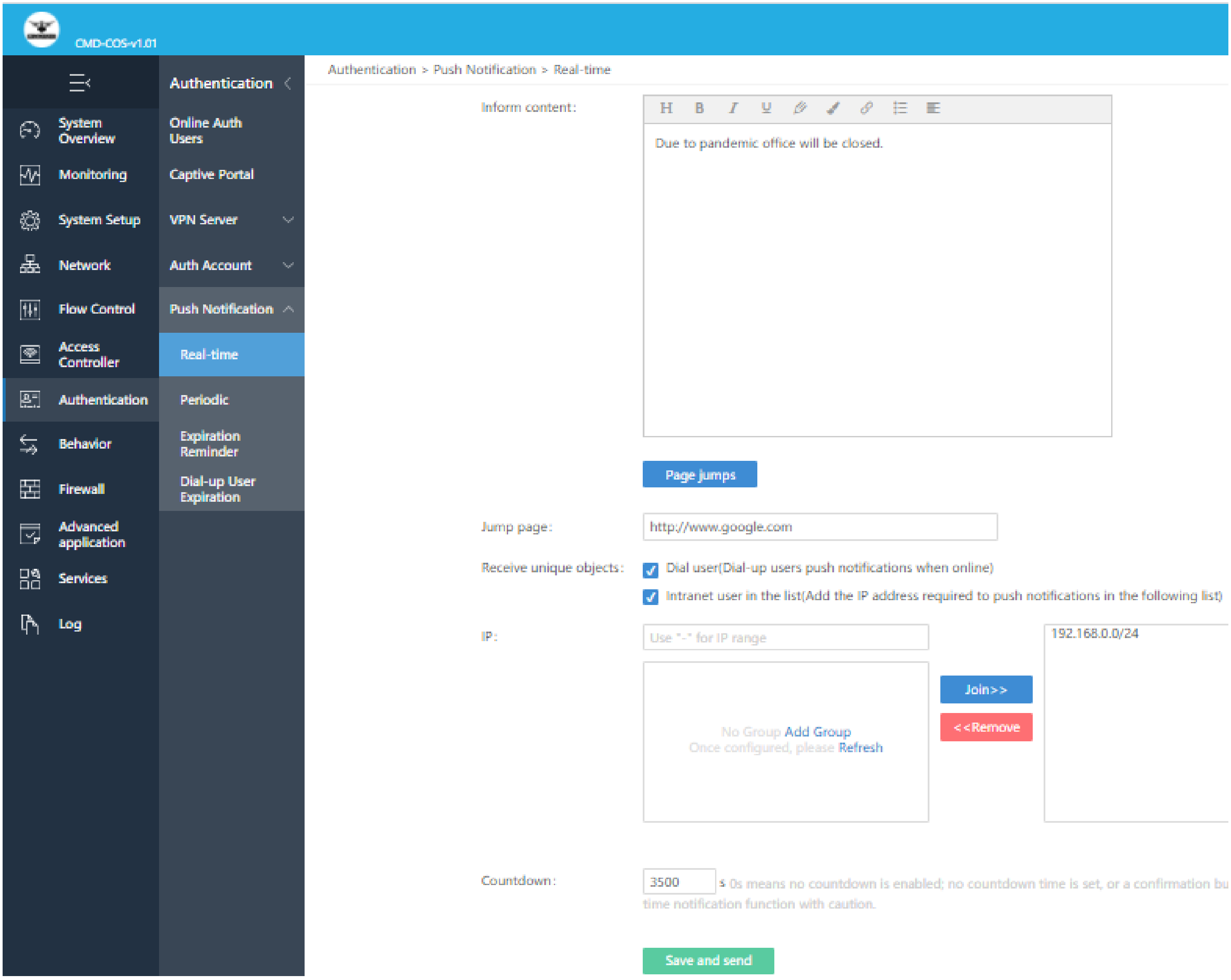
Jump page: http://www.google.com

Receive unique objects:
□ Dial user(Dial-up users push notifications when online)
□ Intranet user in the list(Add the IP address required to push notifications in the following list)

IP: Use "-" for IP range

Countdown: 60 s 0s means no countdown is enabled; no countdown time is set, or a confirmation button on the notification page is manually clicked during the countdown time, otherwise port 80 will be hijacked all the time. Please use the real-time notification function with caution.

Fig 6.5.1 Default Real-time Notification Settings page



Authentication > Push Notification > Real-time

Inform content: Due to pandemic office will be closed.

Jump page: http://www.google.com

Receive unique objects:
☑ Dial user(Dial-up users push notifications when online)
☑ Intranet user in the list(Add the IP address required to push notifications in the following list)

IP: Use "-" for IP range

192.168.0.0/24

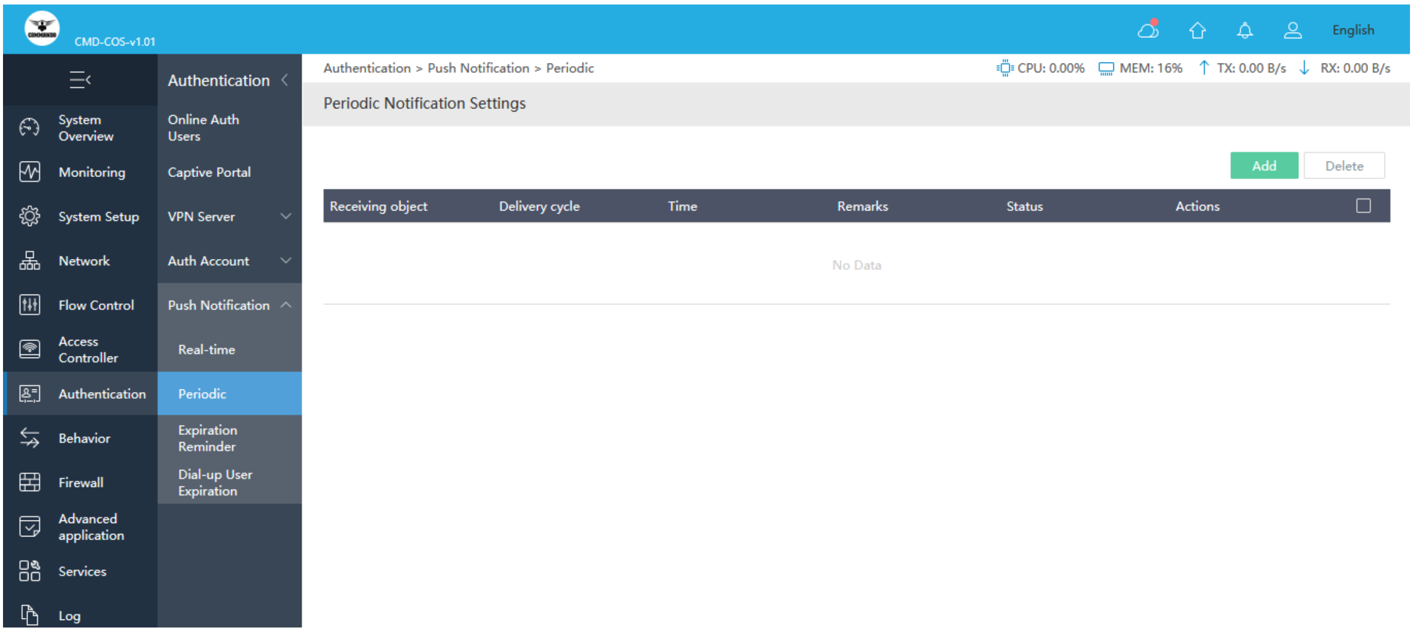
Countdown: 3500 s 0s means no countdown is enabled; no countdown time is set, or a confirmation bu
time notification function with caution.

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



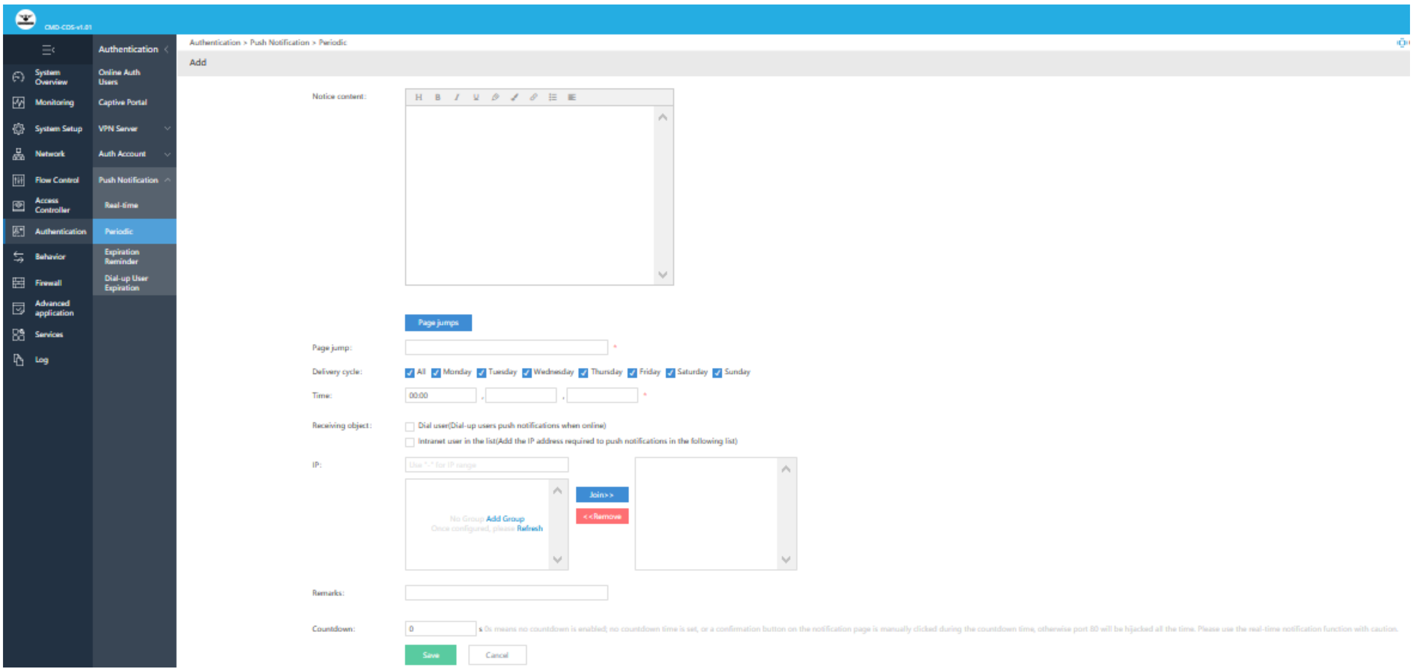
Authentication > Push Notification > Periodic

Periodic Notification Settings

Receiving object	Delivery cycle	Time	Remarks	Status	Actions	□

No Data

Fig 6.5.3 Default Periodic Notification Settings page



Authentication > Push Notification > Periodic

Add

Notice content:

Page jump: *

Delivery cycle: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Time: 00:00 , , *

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

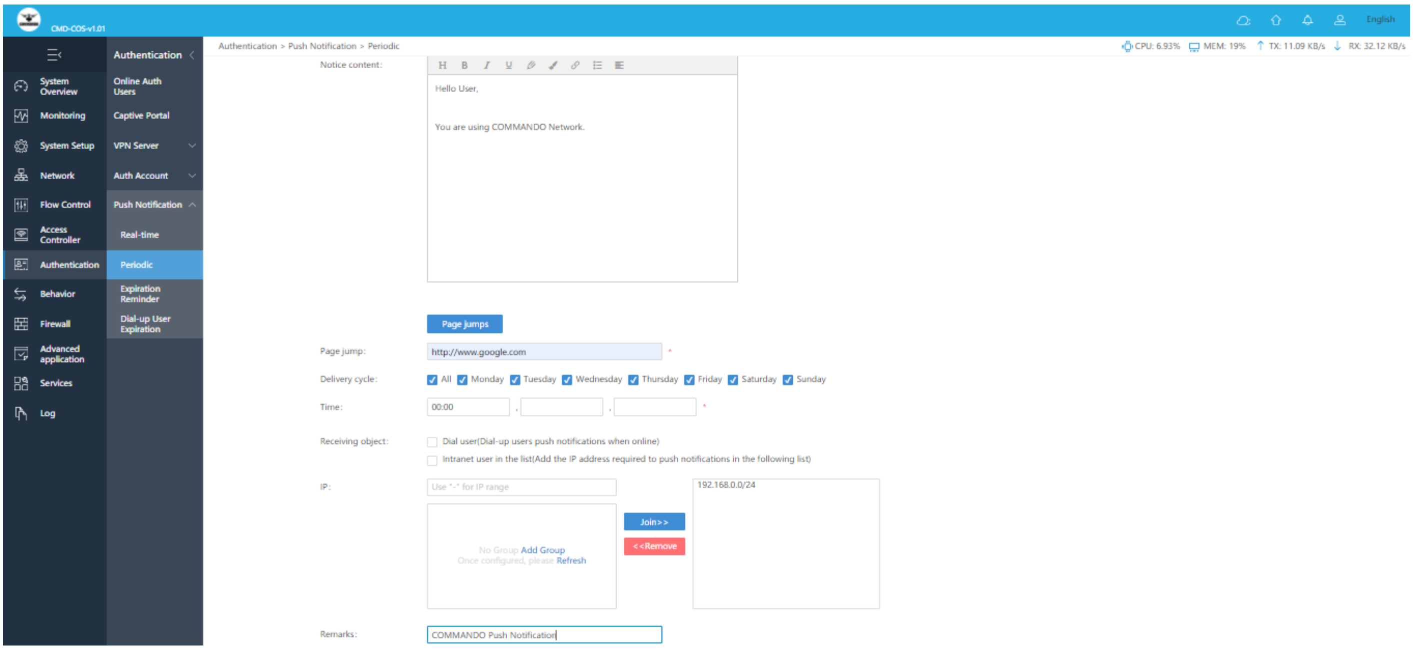
IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Remarks:

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

Fig 6.5.4 Add Periodic Notification Settings page



Authentication > Push Notification > Periodic

Notice content:

Hello User,

You are using COMMANDO Network.

Page jumps

Page jump: http://www.google.com *

Delivery cycle: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Time: 00:00 , , *

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

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Join>>
<<Remove

192.168.0.0/24

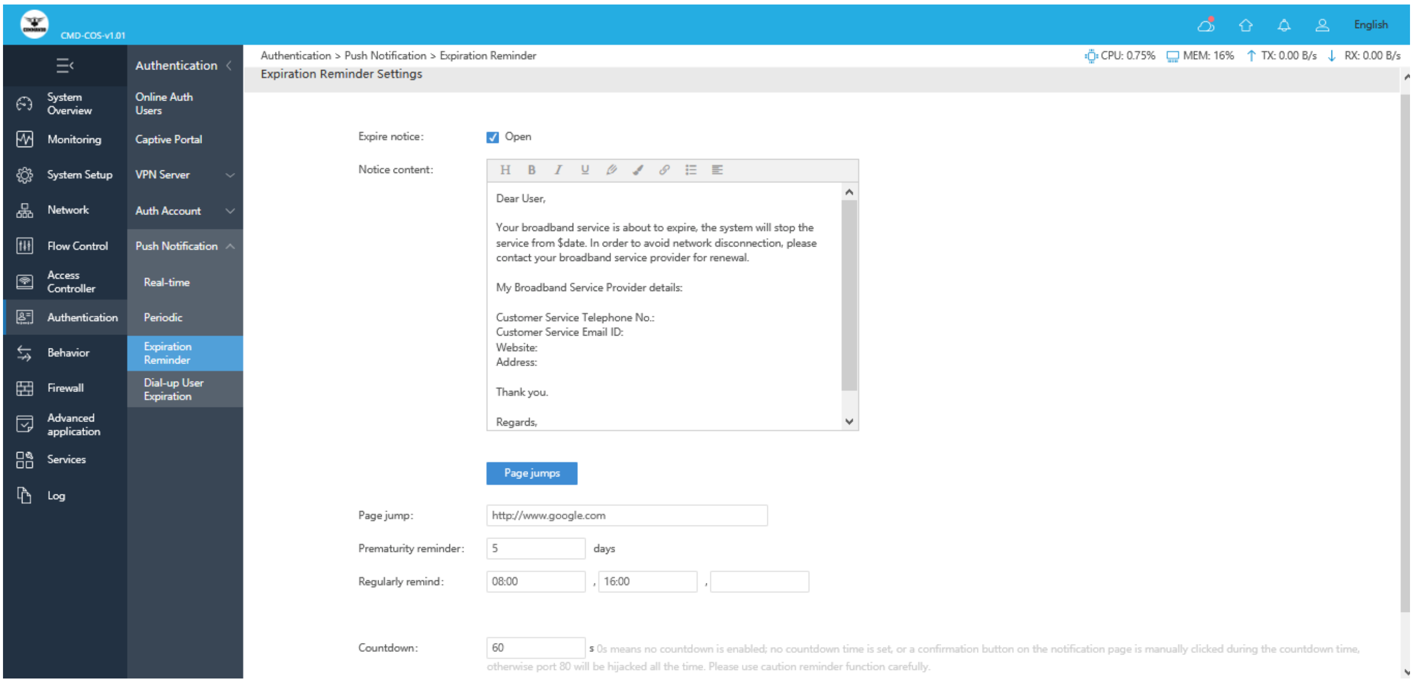
Remarks: COMMANDO Push Notification

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



Authentication > Push Notification > Expiration Reminder

Expiration Reminder Settings

Expire notice: ☑ Open

Notice content:

Dear User,

Your broadband service is about to expire, the system will stop the service from $date. In order to avoid network disconnection, please contact your broadband service provider for renewal.

My Broadband Service Provider details:

Customer Service Telephone No.:
Customer Service Email ID:
Website:
Address:

Thank you.

Regards,

Page jumps

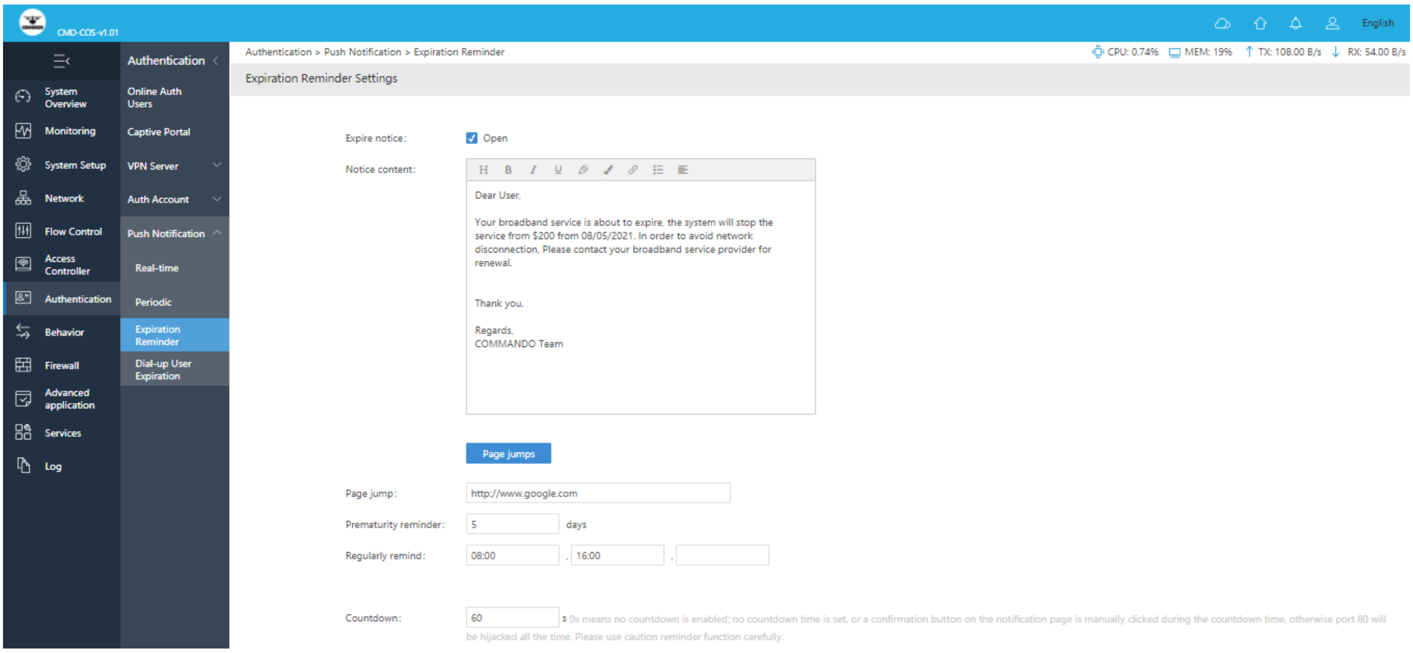
Page jump: http://www.google.com

Prematurity reminder: 5 days

Regularly remind: 08:00 , 16:00 ,

Countdown: 60 s 0s means no countdown is enabled; no countdown time is set, or a confirmation button on the notification page is manually clicked during the countdown time, otherwise port 80 will be hijacked all the time. Please use caution reminder function carefully.

Fig 6.5.6 Default Expiration Reminder Settings page



Authentication > Push Notification > Expiration Reminder

Expiration Reminder Settings

Expire notice: ☑ Open

Notice content:

Dear User,

Your broadband service is about to expire, the system will stop the service from $200 from 08/05/2021. In order to avoid network disconnection, Please contact your broadband service provider for renewal.

Thank you.

Regards,
COMMANDO Team

Page jump: http://www.google.com

Prematurity reminder: 5 days

Regularly remind: 08:00 , 16:00 ,

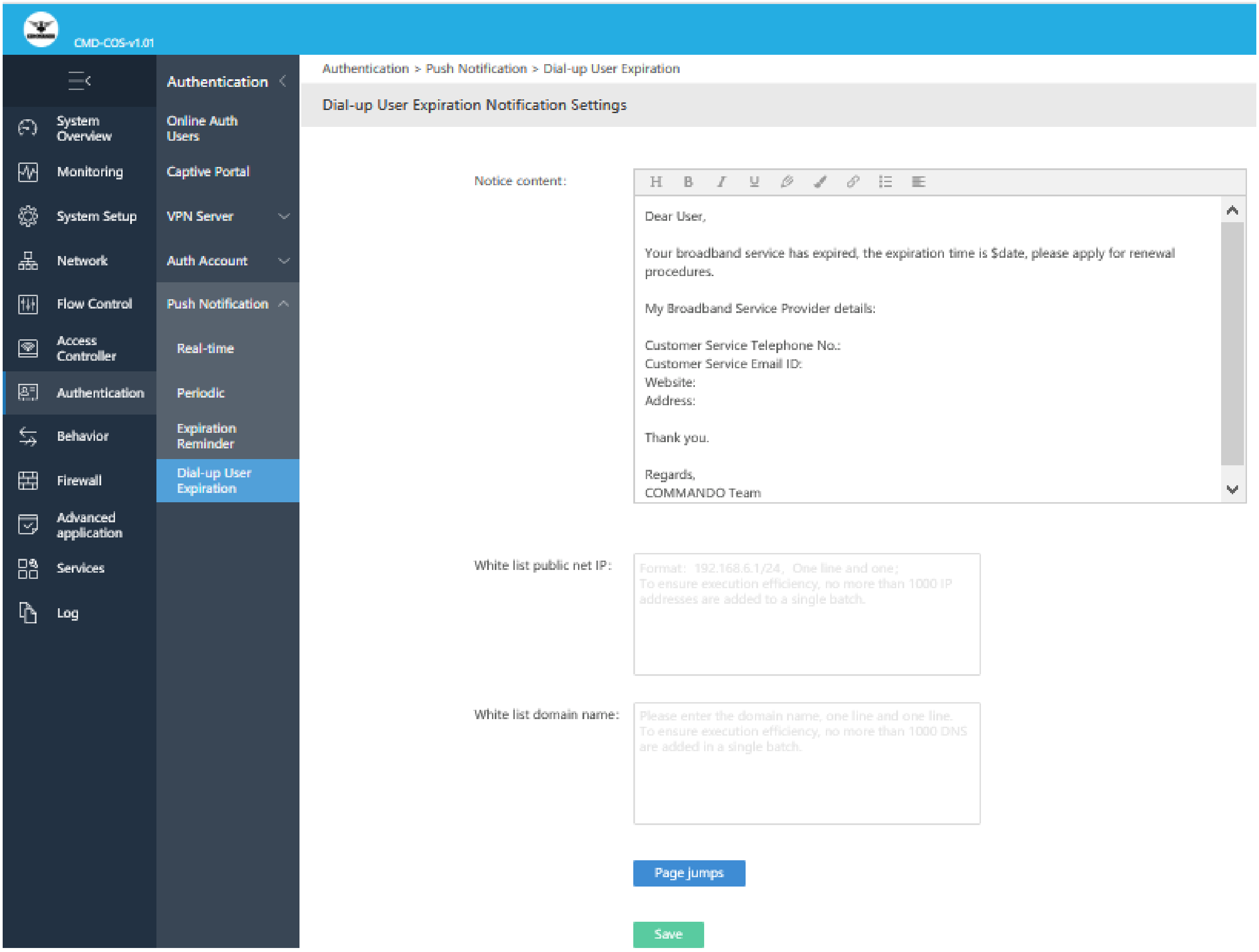
Countdown: 60 s 0s means no countdown is enabled; no countdown time is set, or a confirmation button on the notification page is manually clicked during the countdown time, otherwise port 80 will be hijacked all the time. Please use caution reminder function carefully.

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



Authentication > Push Notification > Dial-up User Expiration

Dial-up User Expiration Notification Settings

Notice content:

Dear User,

Your broadband service has expired, the expiration time is $date, please apply for renewal procedures.

My Broadband Service Provider details:

Customer Service Telephone No.:
Customer Service Email ID:
Website:
Address:

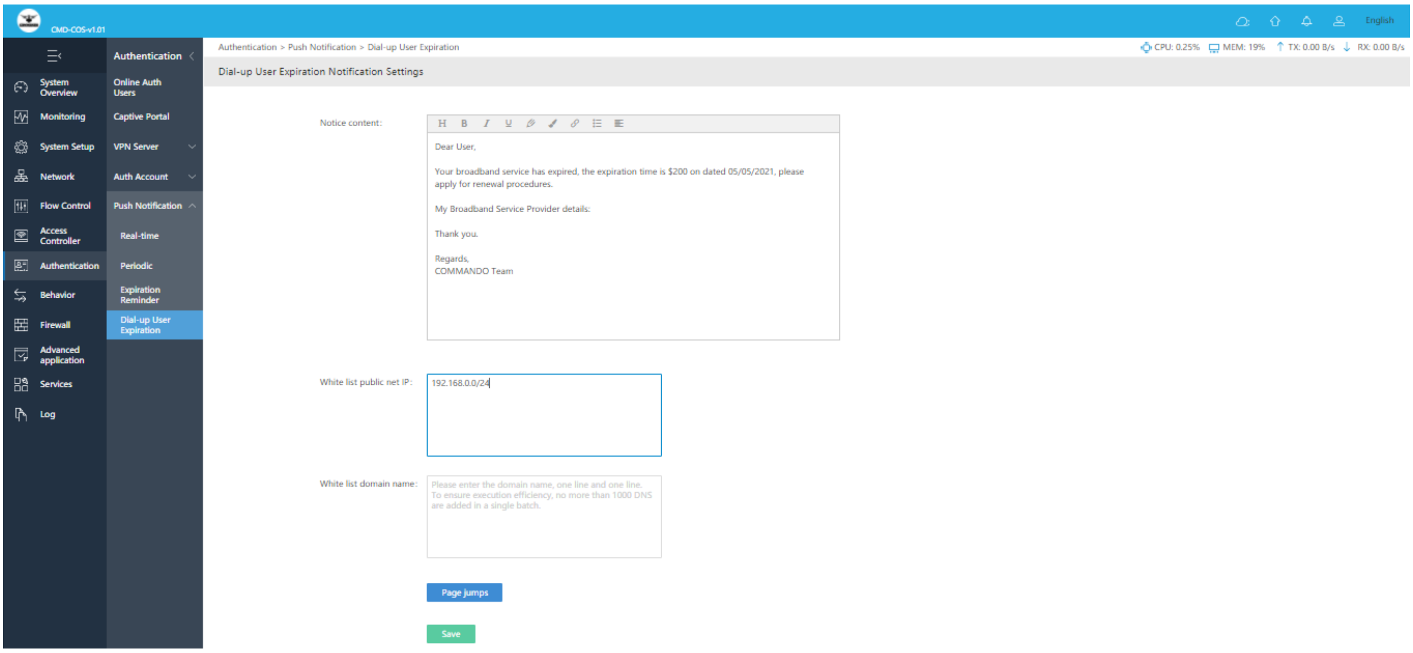
Thank you.

Regards,
COMMANDO Team

White list public net IP: Format: 192.168.6.1/24, One line and one; To ensure execution efficiency, no more than 1000 IP addresses are added to a single batch.

White list domain name: Please enter the domain name, one line and one line. To ensure execution efficiency, no more than 1000 DNS are added in a single batch.

Fig 6.5.8 Default Dial-up User Expiration Notification page



Authentication > Push Notification > Dial-up User Expiration

Dial-up User Expiration Notification Settings

Notice content:

Dear User,

Your broadband service has expired, the expiration time is $200 on dated 05/05/2021, please apply for renewal procedures.

My Broadband Service Provider details:

Thank you.

Regards,
COMMANDO Team

White list public net IP: 192.168.0.0/24

White list domain name: Please enter the domain name, one line and one line. To ensure execution efficiency, no more than 1000 DNS are added in a single batch.

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.

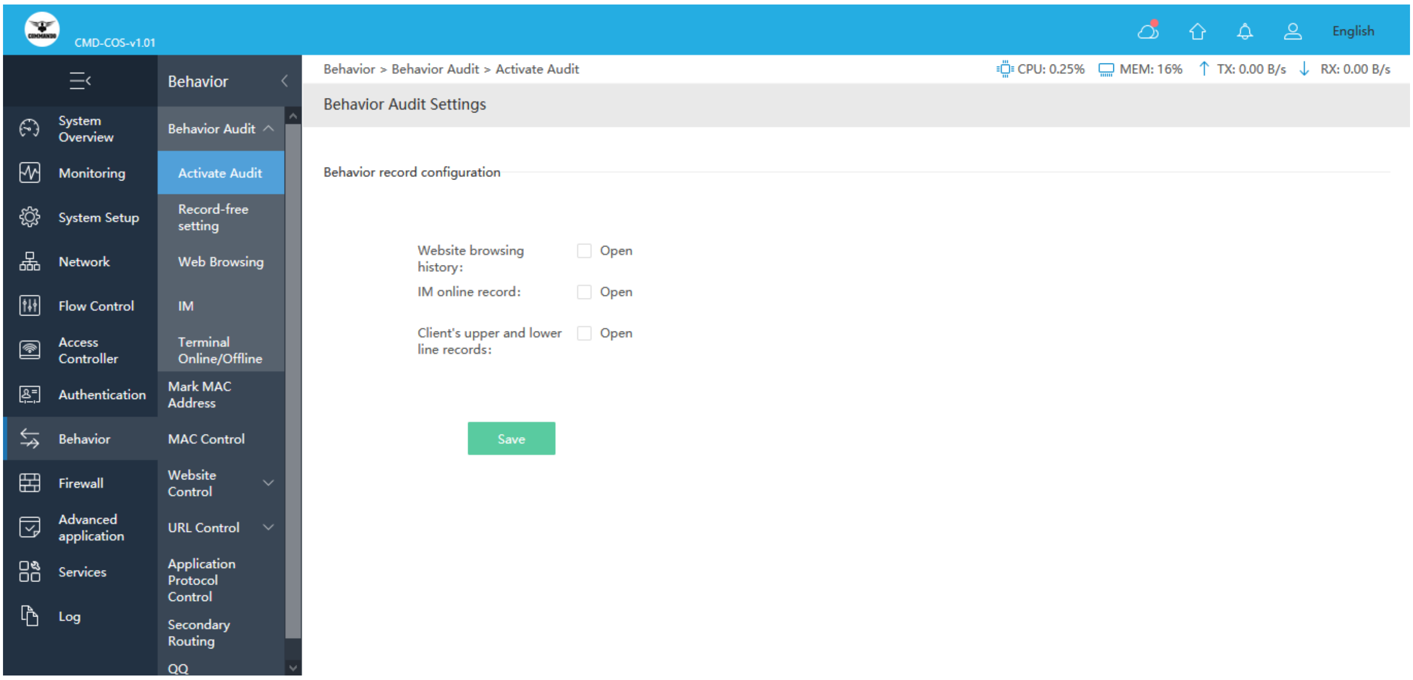
Secondary Routing: Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet. To create a single network from subnets that are physically separated by another network by using a secondary address first network is extended or layered 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



Behavior Audit Settings

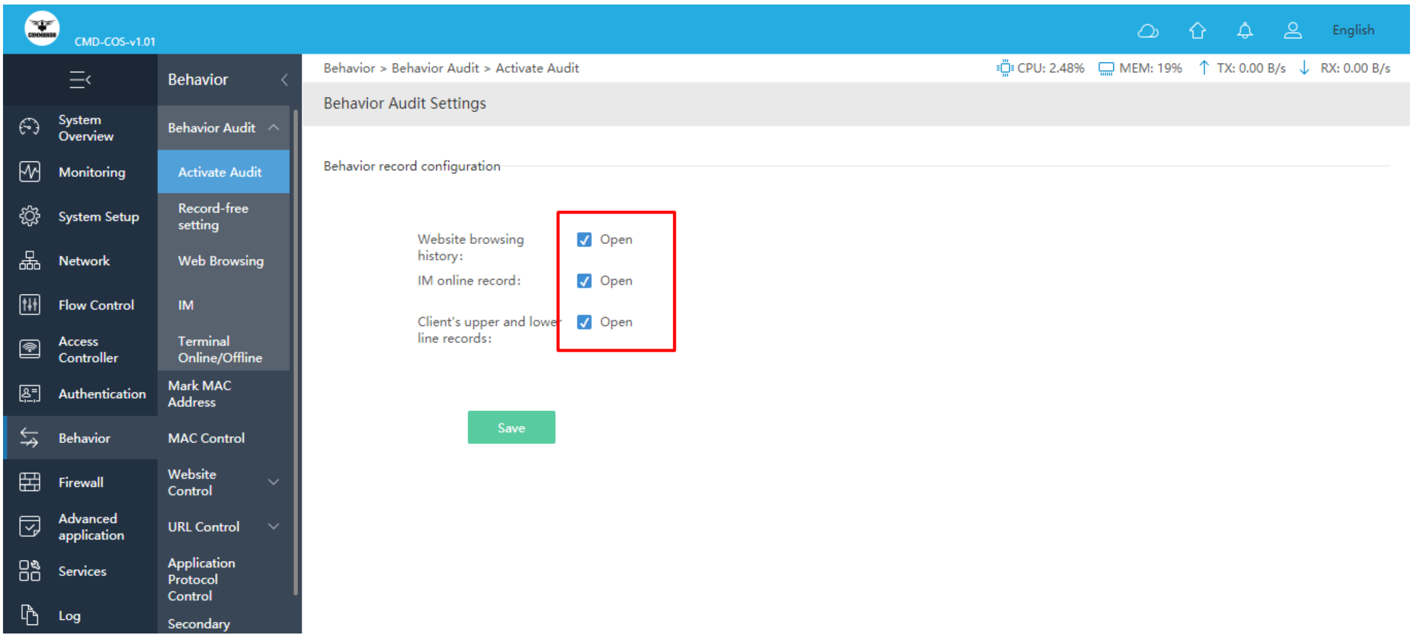
Behavior record configuration

Website browsing history: □ Open

IM online record: □ Open

Client's upper and lower line records: □ Open

Fig 7.1.1 Default Behavior Audit Settings page



Behavior Audit Settings

Behavior record configuration

Website browsing history: ☑ Open

IM online record: ☑ Open

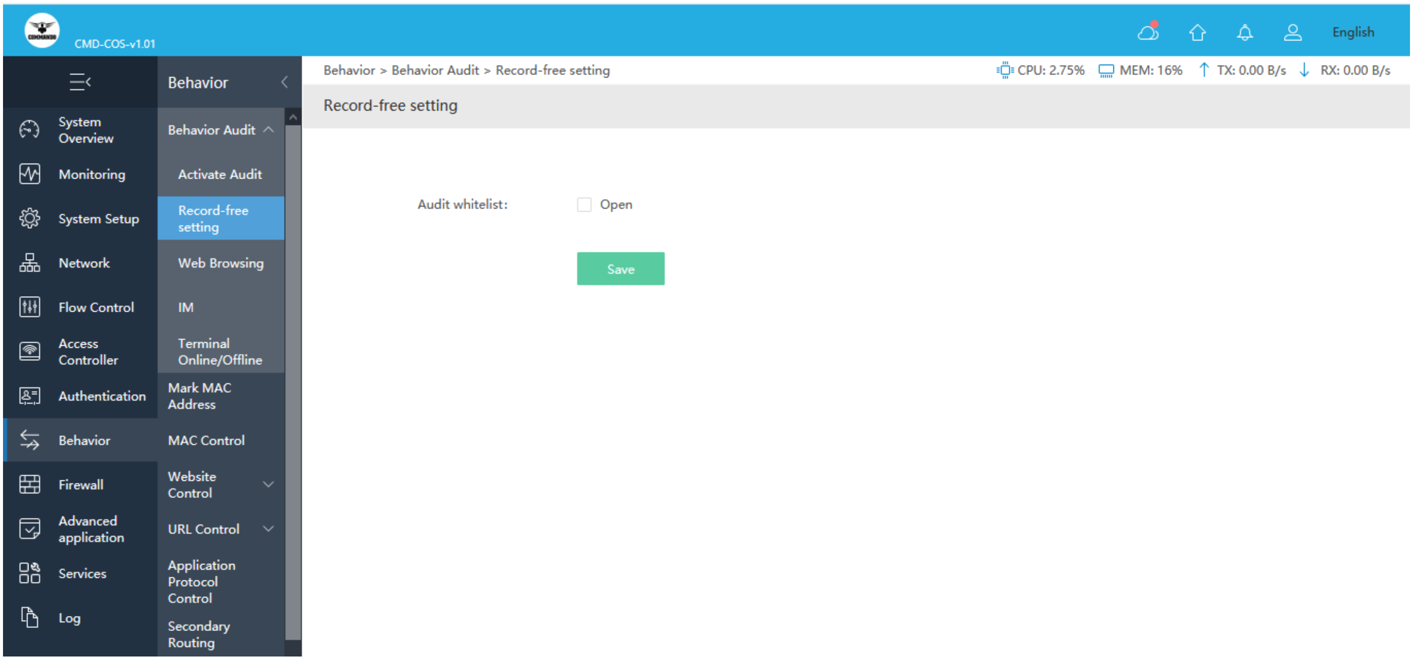
Client's upper and lower line records: ☑ Open

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.

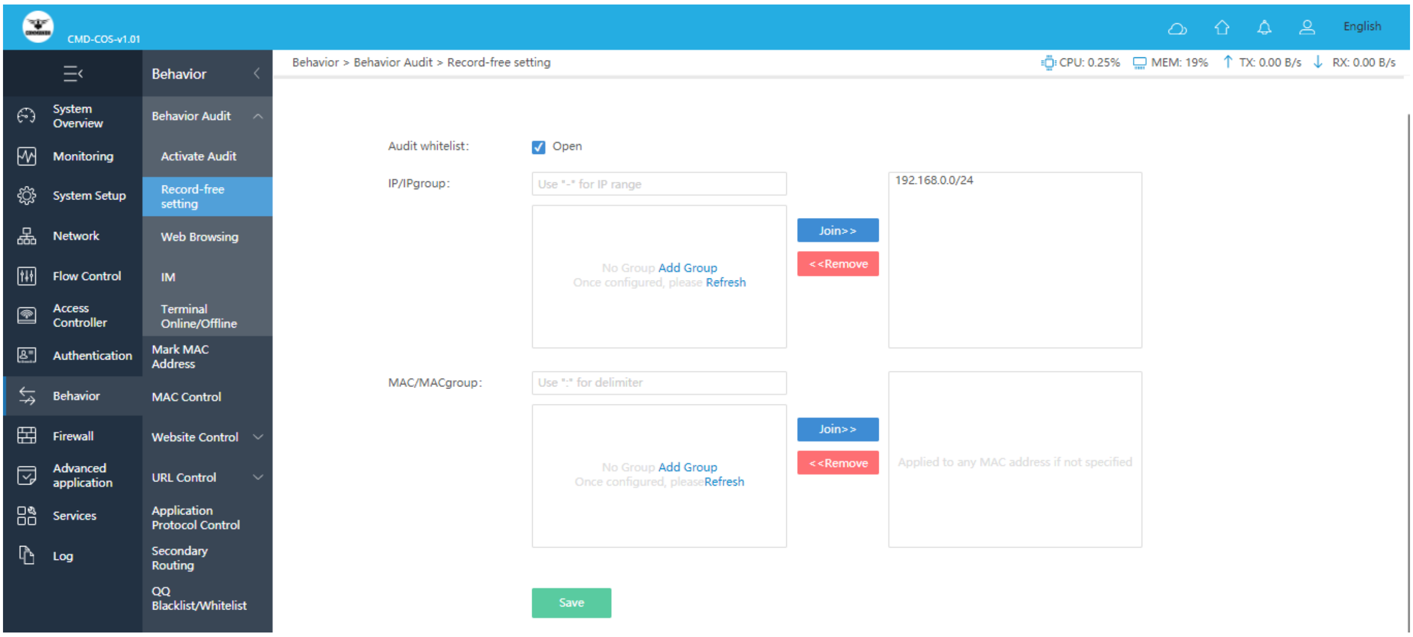
To enable Record-free setting, Click on Behavior > Behavior Audit > Record-free setting



Record-free setting

Audit whitelist: □ Open

Fig 7.1.3 Default Record-free setting page



Audit whitelist: ☑ Open

IP/IPgroup: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

192.168.0.0/24

MAC/MACgroup: Use ":" for delimiter

No Group Add Group
Once configured, pleaseRefresh

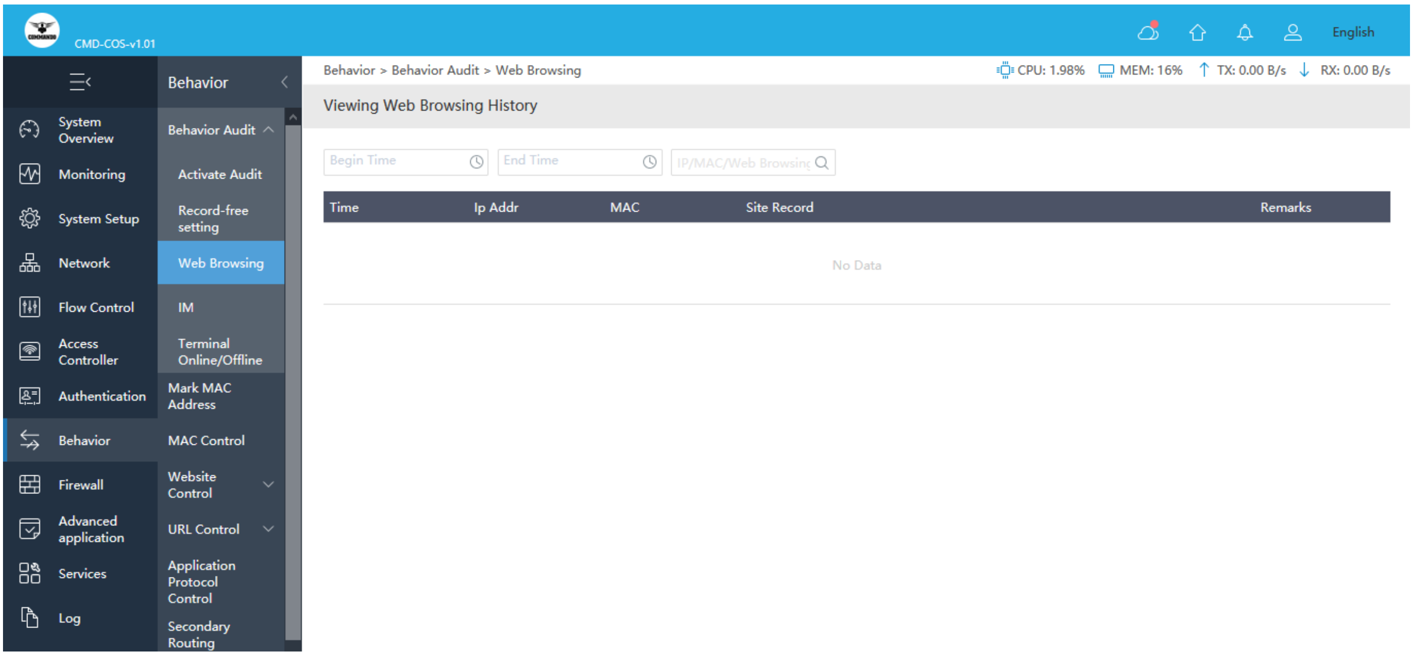
Applied to any MAC address if not specified

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



Behavior > Behavior Audit > Web Browsing

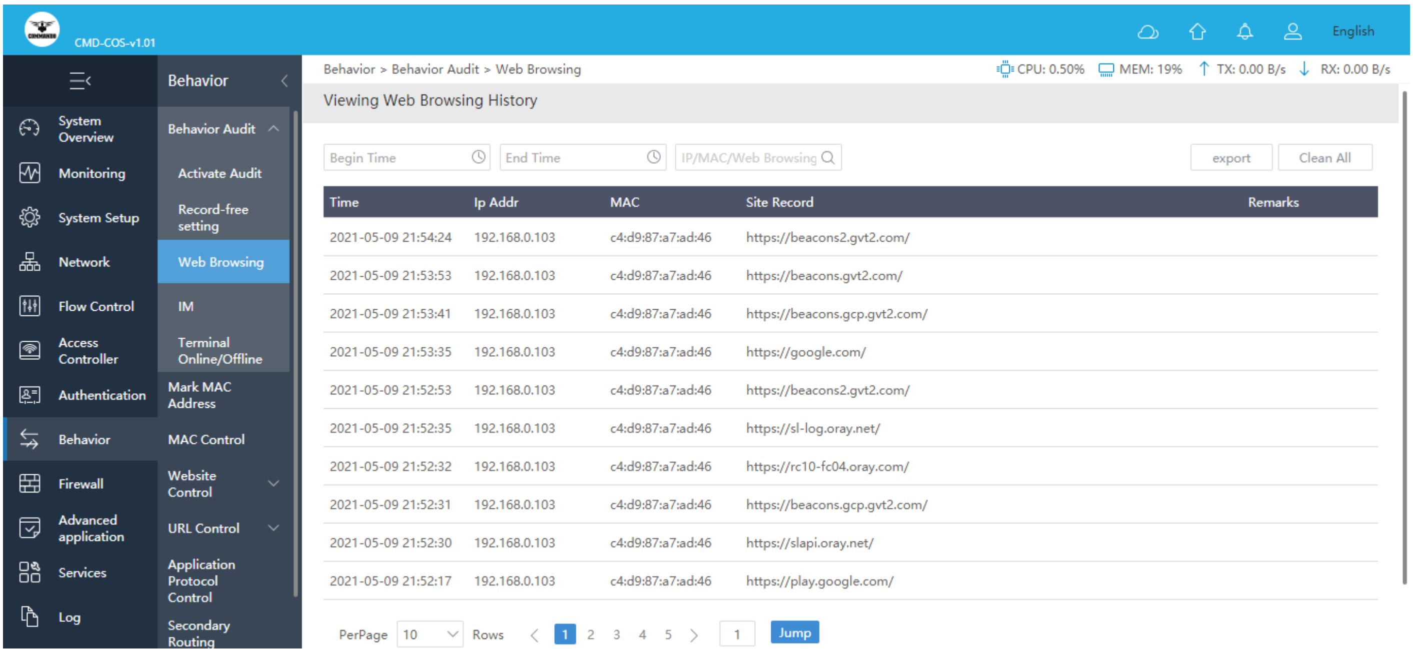
CPU: 1.98% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Viewing Web Browsing History

Time	Ip Addr	MAC	Site Record	Remarks

No Data

Fig 7.1.5 Default Viewing Web Browsing History page



Behavior > Behavior Audit > Web Browsing

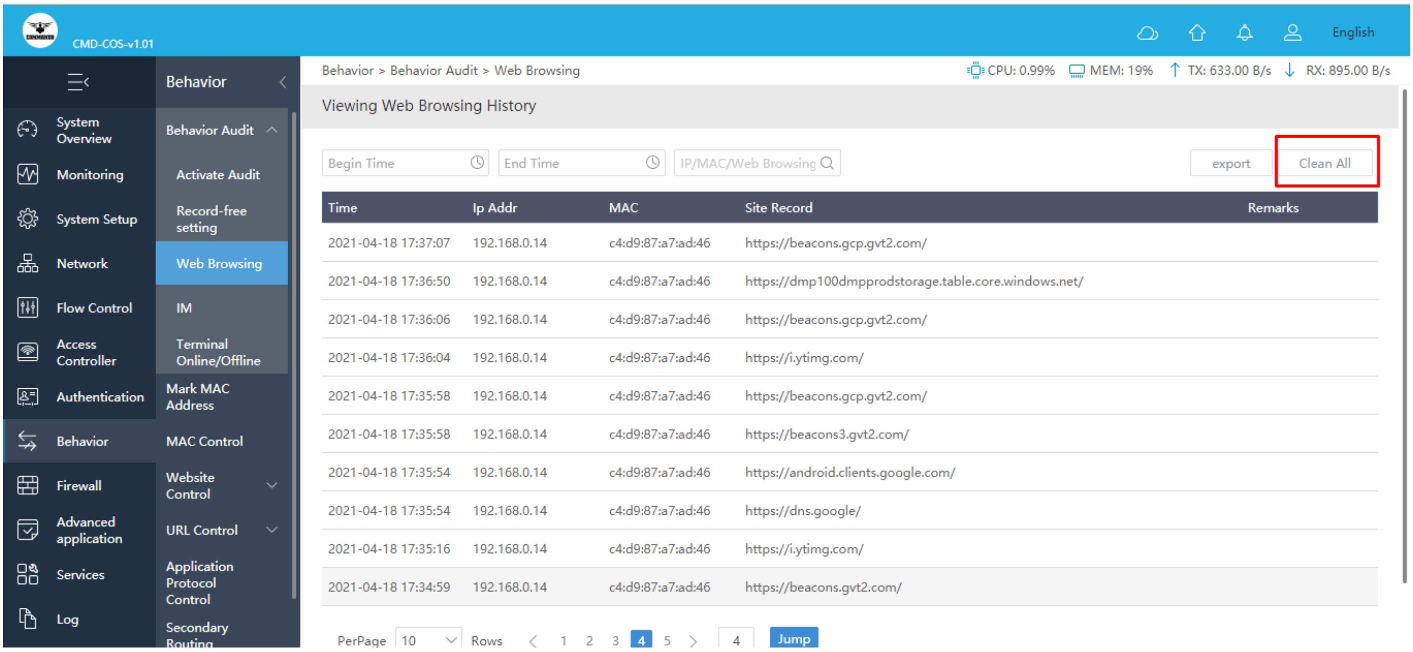
CPU: 0.50% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Viewing Web Browsing History

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/	

PerPage 10 Rows

Fig 7.1.6 Viewing Web Browsing History page



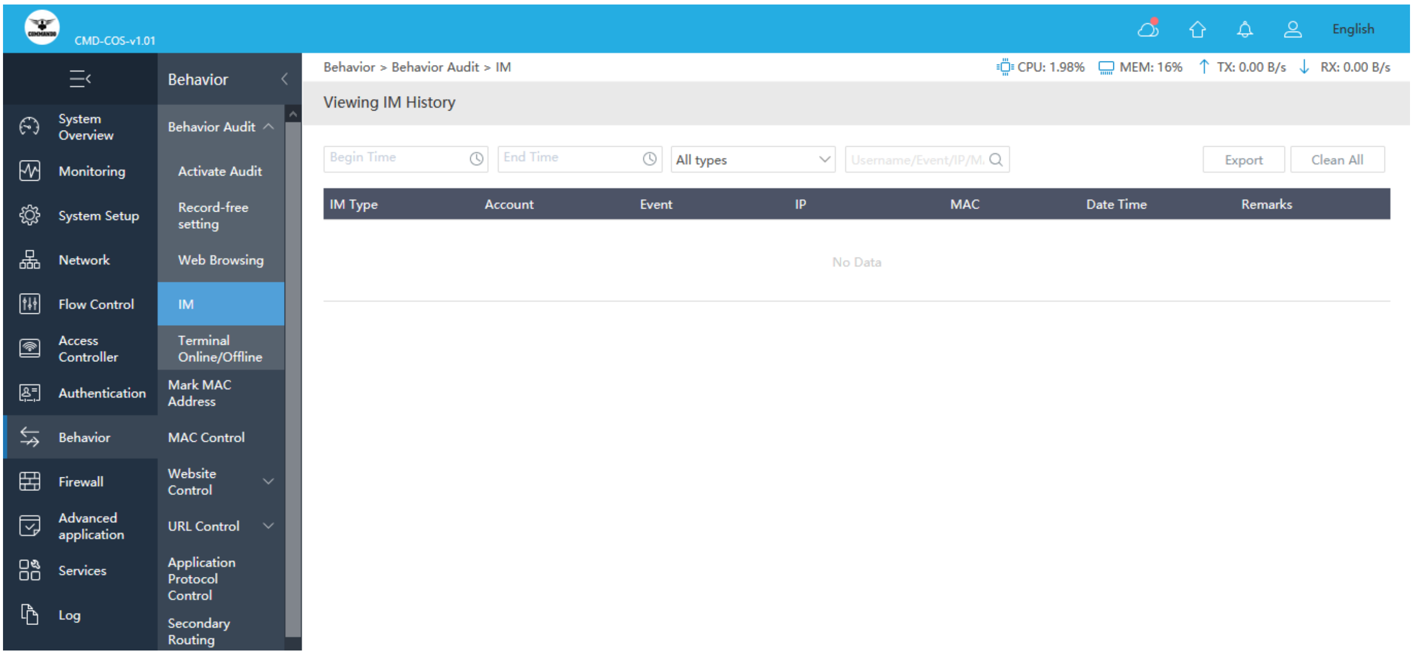
Time	Ip Addr	MAC	Site Record	Remarks
2021-04-18 17:37:07	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
2021-04-18 17:36:50	192.168.0.14	c4:d9:87:a7:ad:46	https://dmp100dmpprodstorage.table.core.windows.net/	
2021-04-18 17:36:06	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
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/	

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

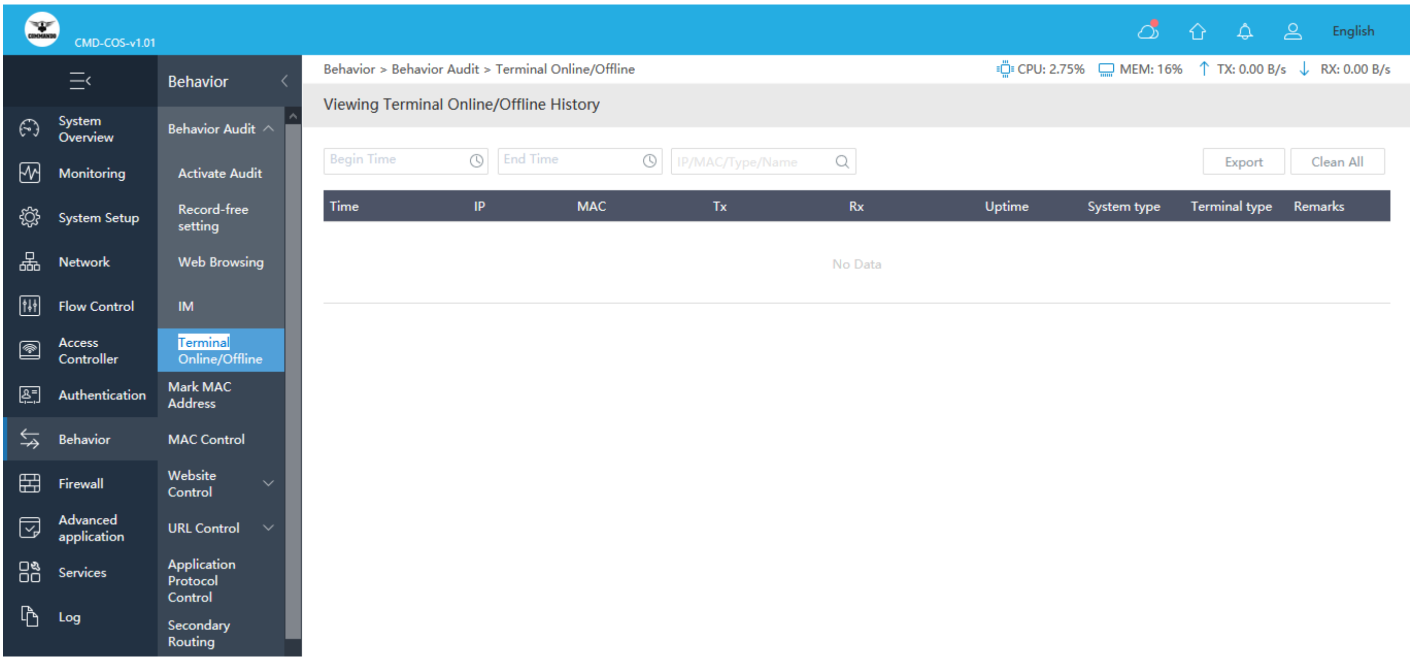


IM Type	Account	Event	IP	MAC	Date Time	Remarks

Fig 7.1.8 Viewing IM History page

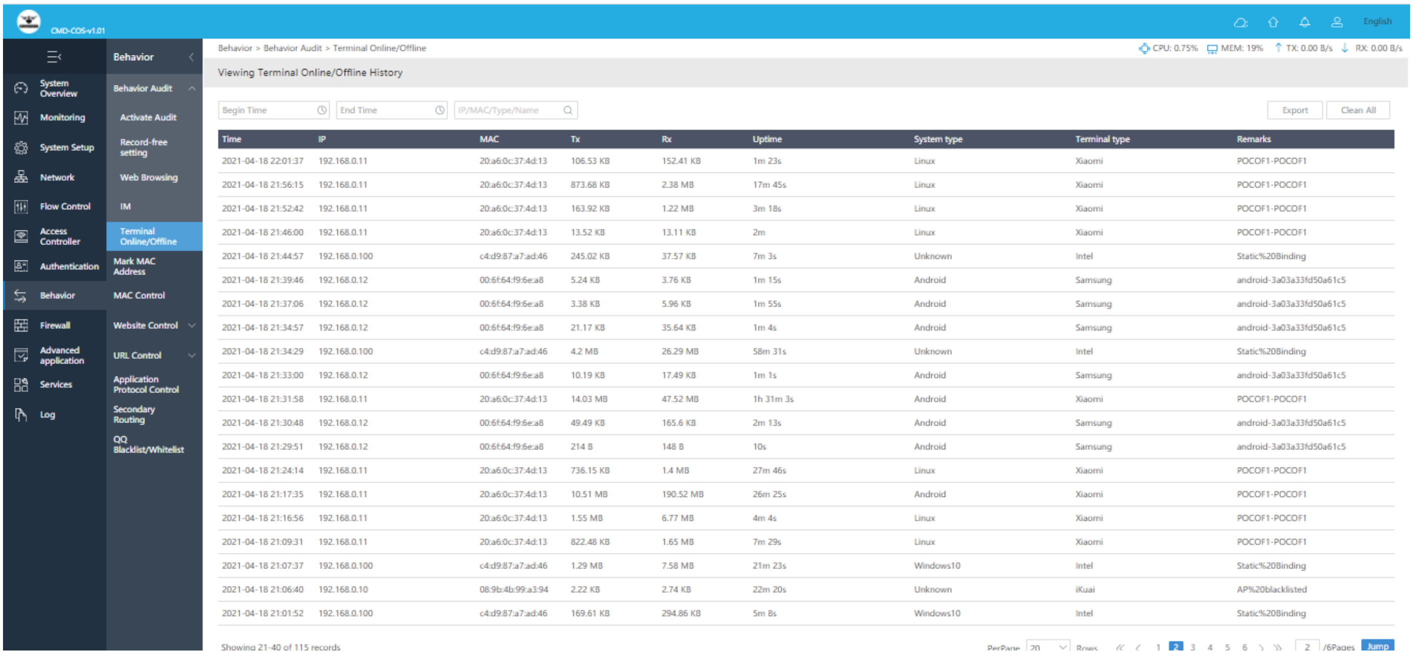
Terminal Online/Offline History:

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



Time	IP	MAC	Tx	Rx	Uptime	System type	Terminal type	Remarks

Fig 7.1.9 Default Viewing Terminal Online/Offline History page



Behavior > Behavior Audit > Terminal Online/Offline

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

Viewing Terminal Online/Offline History

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 21:30:48	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 21:29:51	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	26m 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

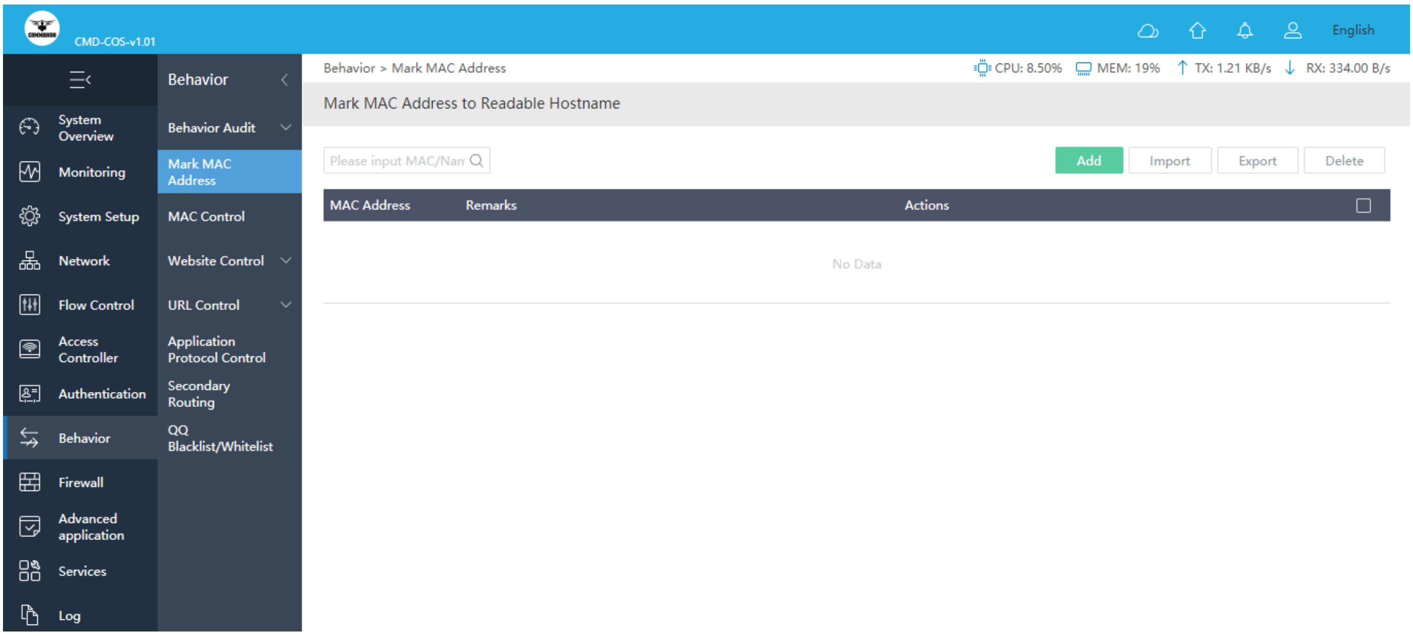
Showing 21-40 of 115 records

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



Behavior > Mark MAC Address

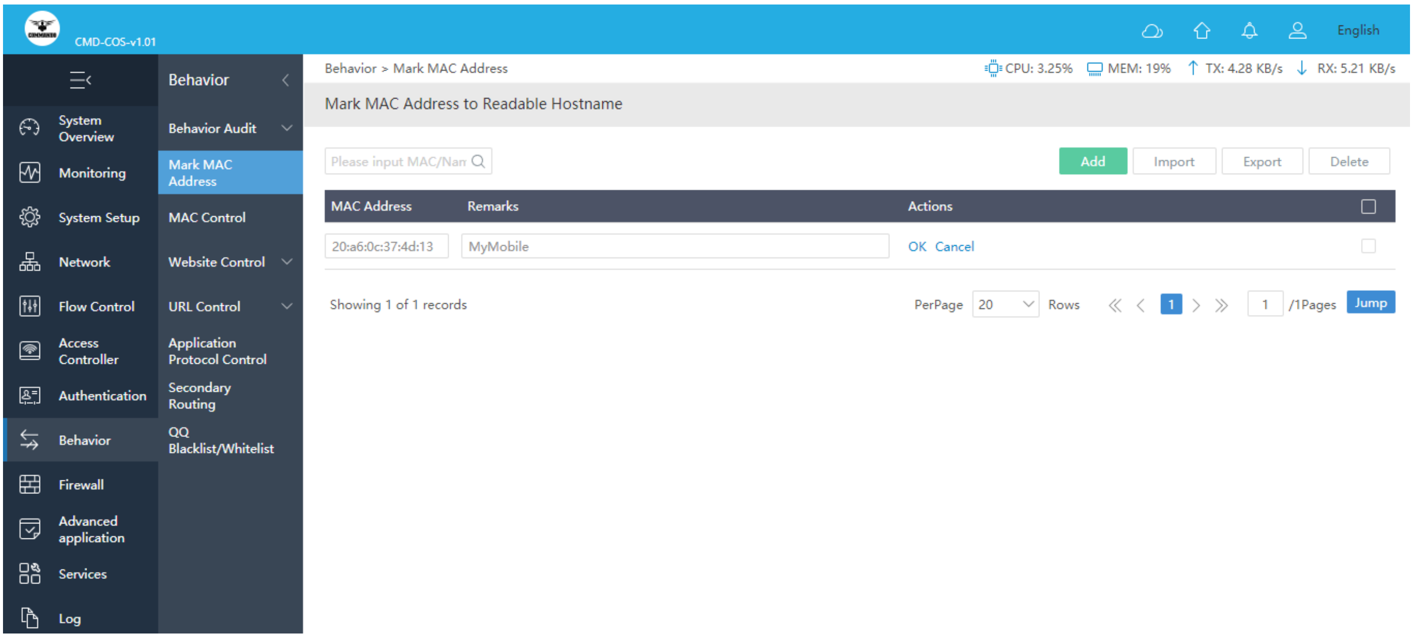
CPU: 8.50% MEM: 19% TX: 1.21 KB/s RX: 334.00 B/s

Mark MAC Address to Readable Hostname

MAC Address	Remarks	Actions	□

No Data

Fig 7.2.1 Default Mark MAC Address to Readable Hostname page



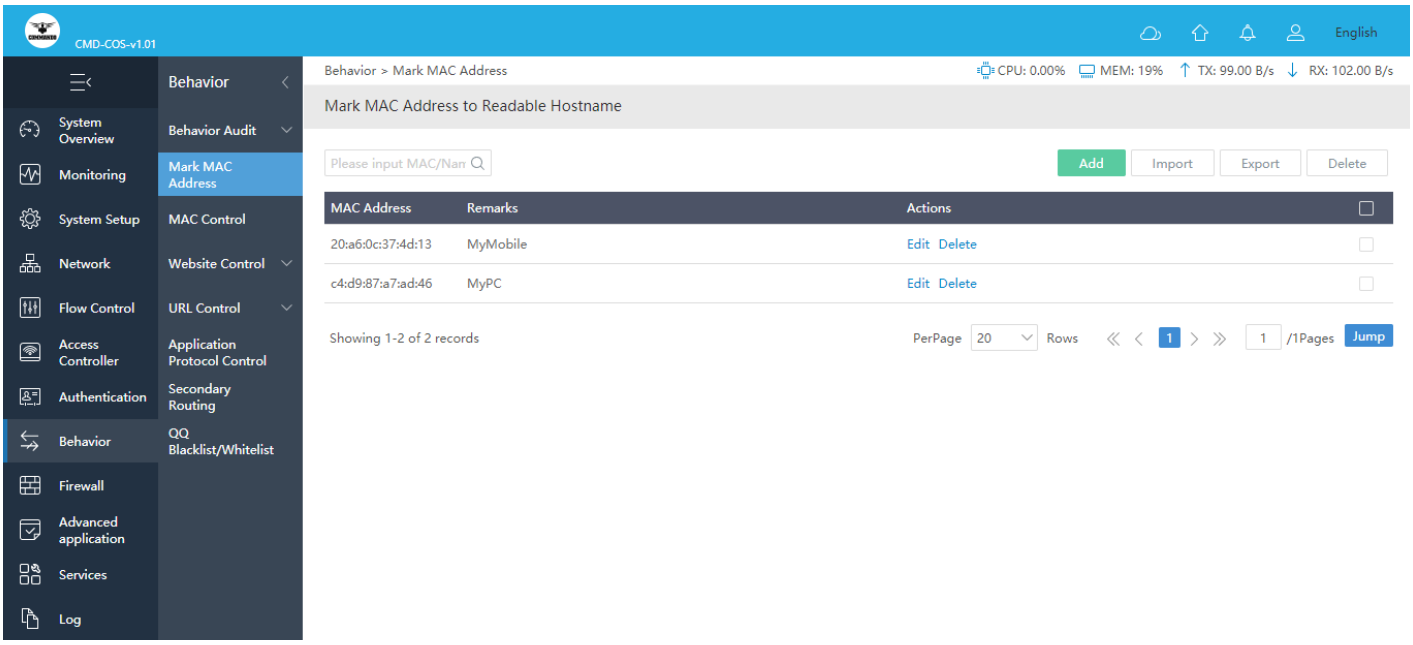
Behavior > Mark MAC Address CPU: 3.25% MEM: 19% TX: 4.28 KB/s RX: 5.21 KB/s

Mark MAC Address to Readable Hostname

MAC Address	Remarks	Actions	□
20:a6:0c:37:4d:13	MyMobile	OK Cancel	□

Showing 1 of 1 records PerPage 20 Rows 1 /1Pages

Fig 7.2.2 Adding Mark MAC Address to Readable Hostname page



Behavior > Mark MAC Address CPU: 0.00% MEM: 19% TX: 99.00 B/s RX: 102.00 B/s

Mark MAC Address to Readable Hostname

MAC Address	Remarks	Actions	□
20:a6:0c:37:4d:13	MyMobile	Edit Delete	□
c4:d9:87:a7:ad:46	MyPC	Edit Delete	□

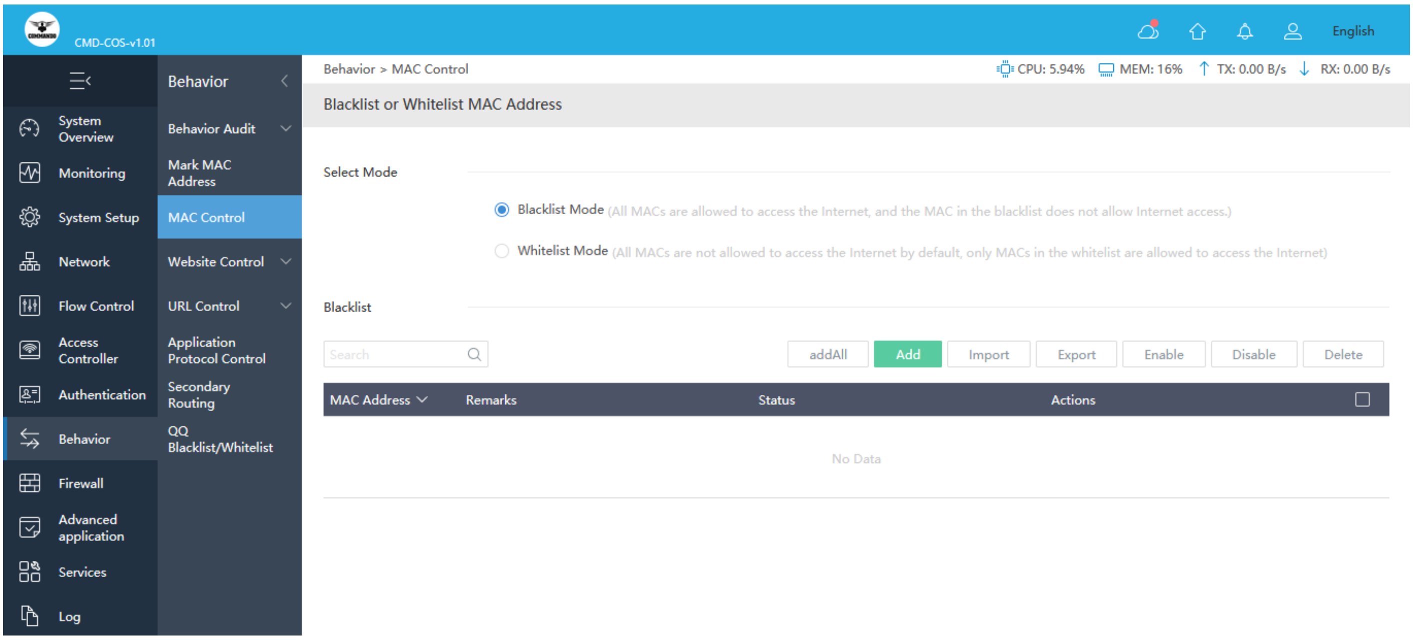
Showing 1-2 of 2 records PerPage 20 Rows 1 /1Pages

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



Behavior > MAC Control

CPU: 5.94% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Blacklist or Whitelist MAC Address

Select Mode

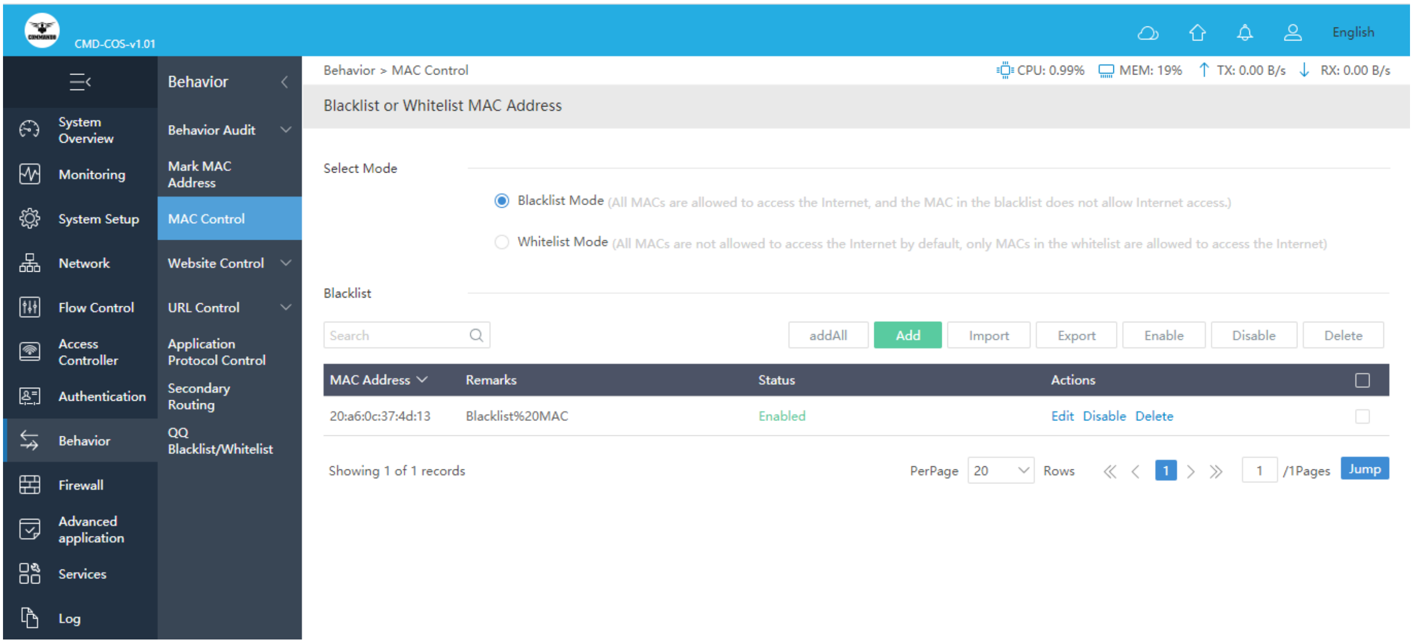
● Blacklist Mode (All MACs are allowed to access the Internet, and the MAC in the blacklist does not allow Internet access.)

○ Whitelist Mode (All MACs are not allowed to access the Internet by default, only MACs in the whitelist are allowed to access the Internet)

Blacklist

MAC Address	Remarks	Status	Actions	□
		No Data		

Fig 7.3.1 Default Blacklist or Whitelist MAC Address page



Behavior > MAC Control

CPU: 0.99% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Blacklist or Whitelist MAC Address

Select Mode

● Blacklist Mode (All MACs are allowed to access the Internet, and the MAC in the blacklist does not allow Internet access.)

○ Whitelist Mode (All MACs are not allowed to access the Internet by default, only MACs in the whitelist are allowed to access the Internet)

Blacklist

MAC Address	Remarks	Status	Actions	□
20:a6:0c:37:4d:13	Blacklist%20MAC	Enabled	Edit Disable Delete	□

Showing 1 of 1 records PerPage 20 Rows « ‹ 1 › » 1 /1Pages

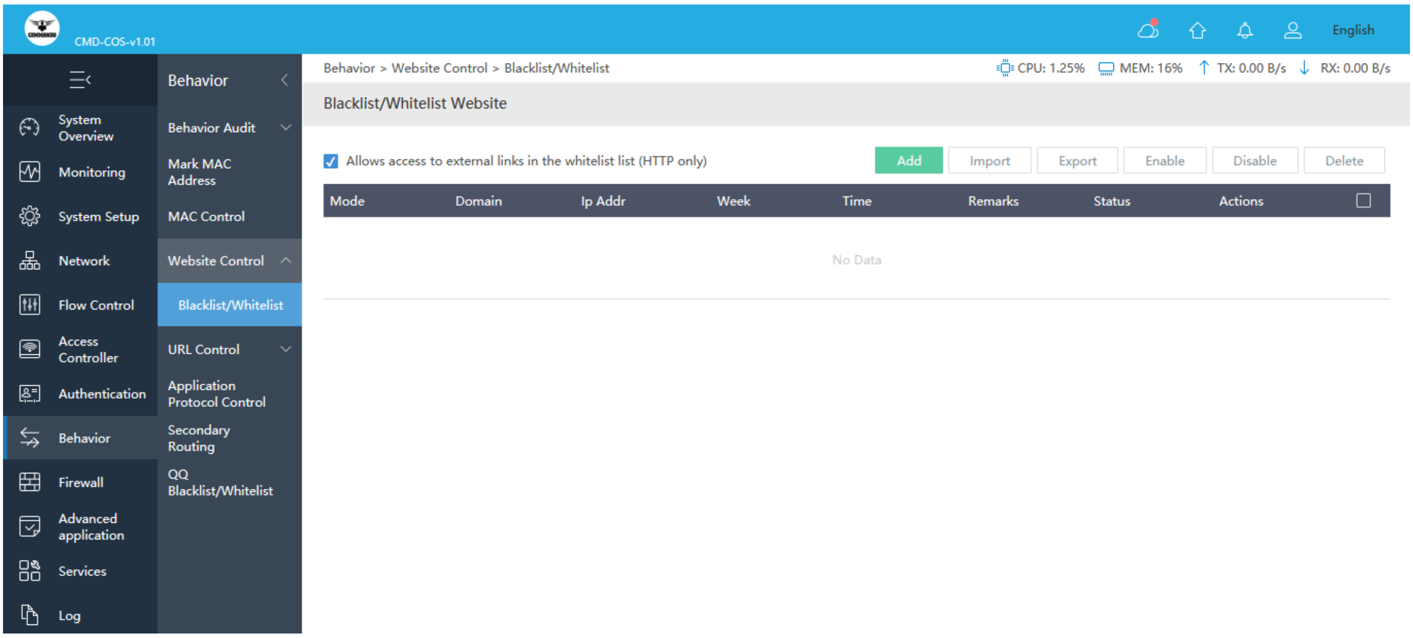
Fig 7.3.2 Blacklist MAC Address page

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)



Behavior > Website Control > Blacklist/Whitelist

CPU: 1.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

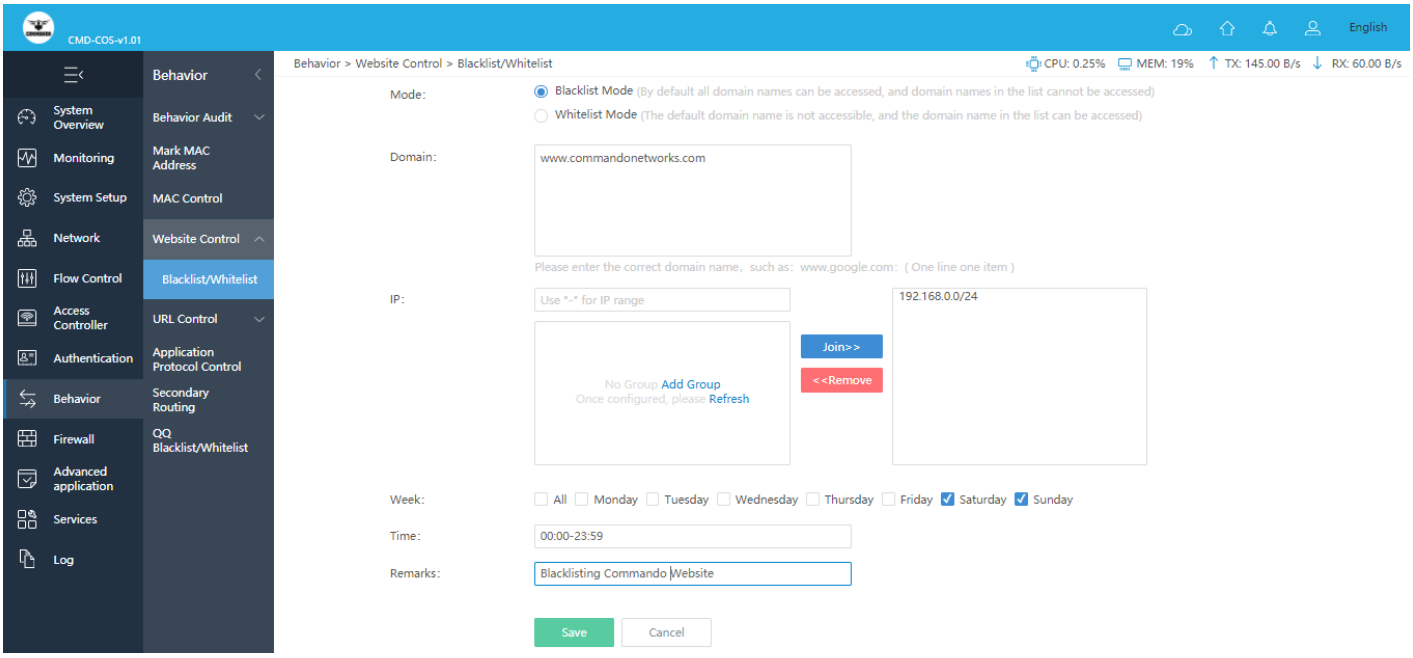
Blacklist/Whitelist Website

☑ Allows access to external links in the whitelist list (HTTP only)

Mode	Domain	Ip Addr	Week	Time	Remarks	Status	Actions	□

No Data

Fig 7.4.1 Default Blacklist/Whitelist Website page



Behavior > Website Control > Blacklist/Whitelist

CPU: 0.25% MEM: 19% TX: 145.00 B/s RX: 60.00 B/s

Mode: ● Blacklist Mode (By default all domain names can be accessed, and domain names in the list cannot be accessed)
○ Whitelist Mode (The default domain name is not accessible, and the domain name in the list can be accessed)

Domain: www.commandonetworks.com

Please enter the correct domain name, such as: www.google.com; (One line one item)

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

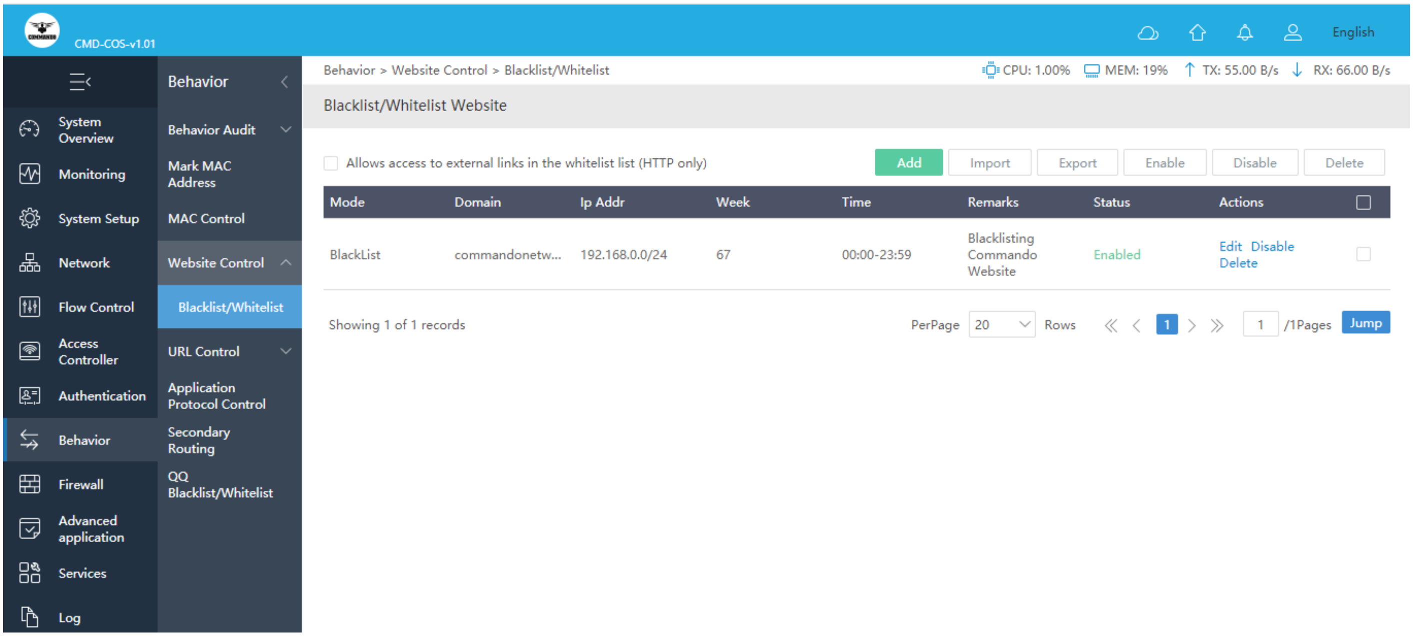
192.168.0.0/24

Week: □ All □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday ☑ Saturday ☑ Sunday

Time: 00:00-23:59

Remarks: Blacklisting Commando Website

Fig 7.4.2 Blacklist particular Website page



Behavior > Website Control > Blacklist/Whitelist

CPU: 1.00% MEM: 19% TX: 55.00 B/s RX: 66.00 B/s

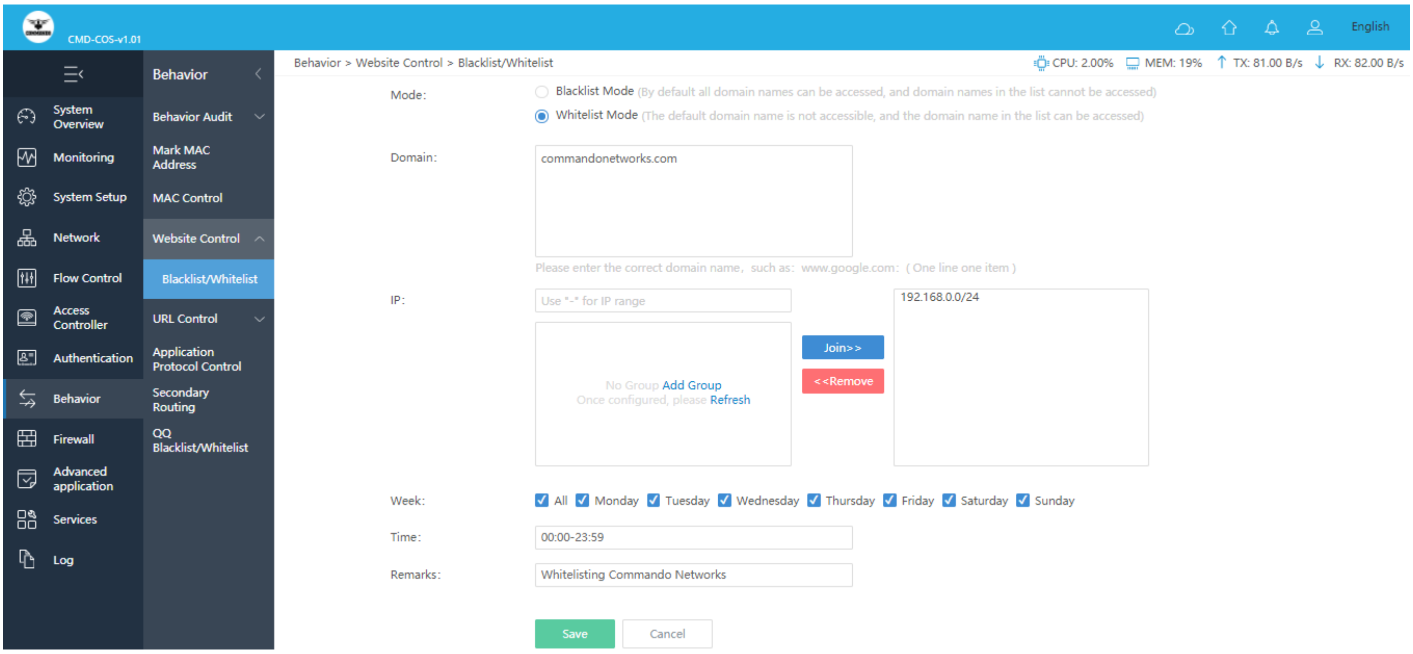
Blacklist/Whitelist Website

□ Allows access to external links in the whitelist list (HTTP only)

Mode	Domain	Ip Addr	Week	Time	Remarks	Status	Actions	□
BlackList	commandonetw...	192.168.0.0/24	67	00:00-23:59	Blacklisting Commando Website	Enabled	Edit Disable Delete	□

Showing 1 of 1 records PerPage 20 Rows « ‹ 1 › » 1 /1Pages

Fig 7.4.3 Blacklist Website page



Mode:
○ Blacklist Mode (By default all domain names can be accessed, and domain names in the list cannot be accessed)
● Whitelist Mode (The default domain name is not accessible, and the domain name in the list can be accessed)

Domain: commandonetworks.com

Please enter the correct domain name, such as: www.google.com; (One line one item)

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Join>>

<<Remove

192.168.0.0/24

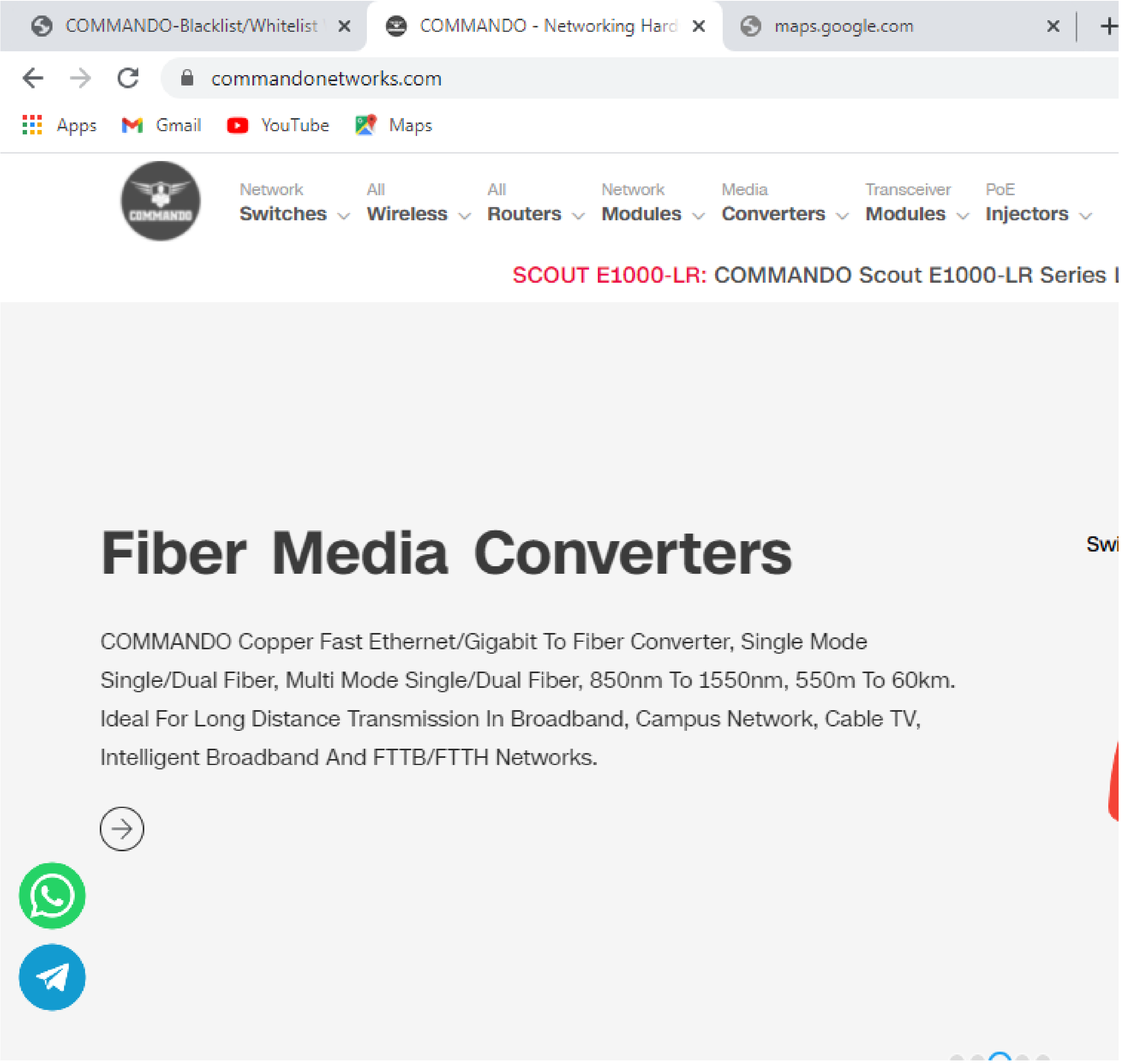
Week: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Time: 00:00-23:59

Remarks: Whitelisting Commando Networks

Save Cancel

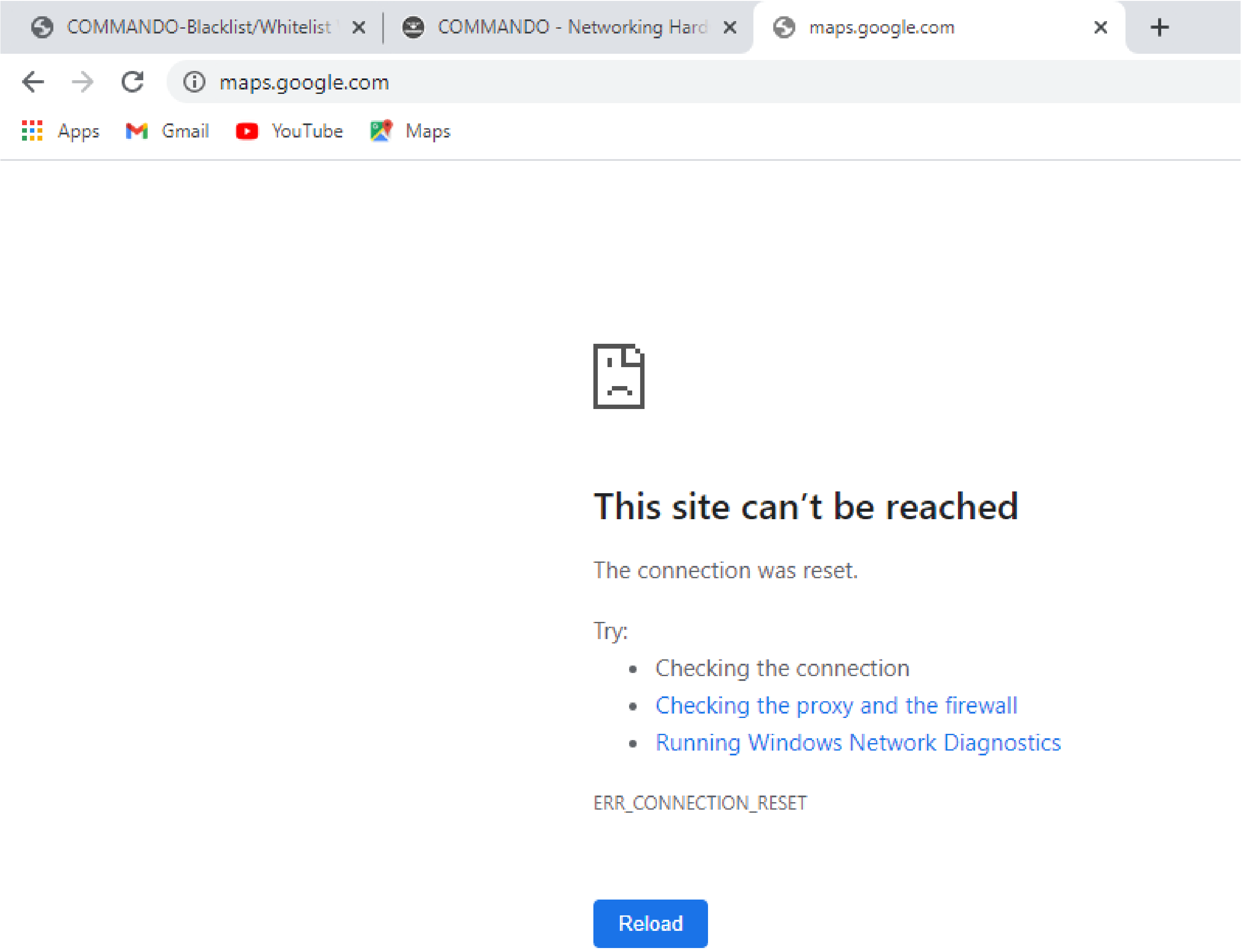
Fig 7.4.4 Whitelisting particular Website page



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.



This site can’t be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

Fig 7.4.5 Result of Whitelisting particular Website page

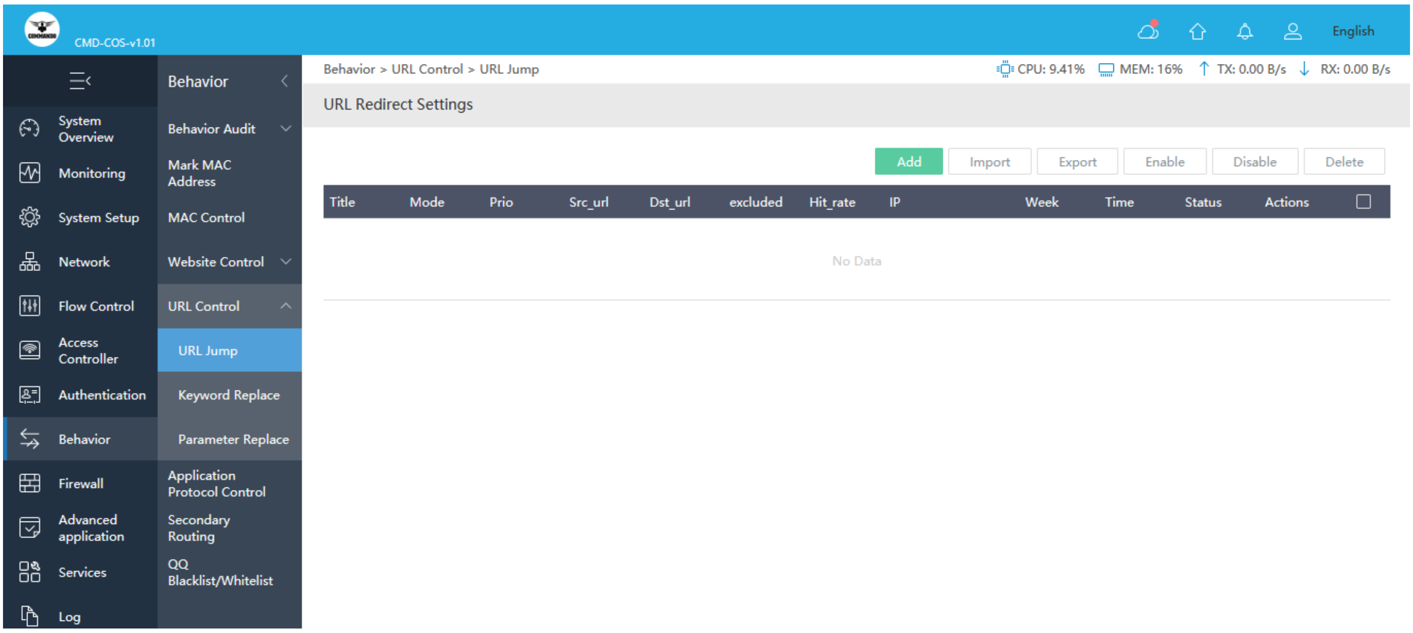
7.5 URL Control

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



Behavior > URL Control > URL Jump

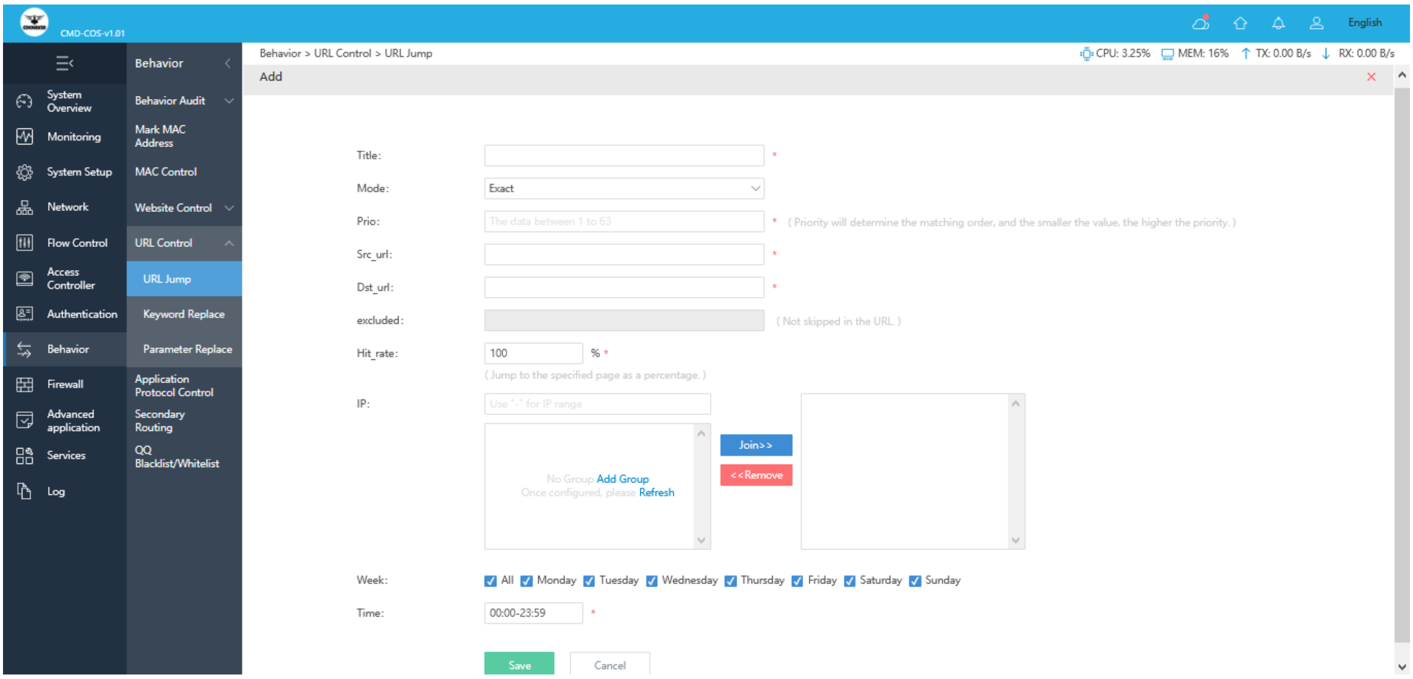
CPU: 9.41% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

URL Redirect Settings

Title	Mode	Prio	Src_url	Dst_url	excluded	Hit_rate	IP	Week	Time	Status	Actions	□

No Data

Fig 7.5.1 Default URL Redirect Settings page



Behavior > URL Control > URL Jump

CPU: 3.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Add

Title: *

Mode: Exact

Prio: The data between 1 to 63 * (Priority will determine the matching order, and the smaller the value, the higher the priority.)

Src_url: *

Dst_url: *

excluded: (Not skipped in the URL.)

Hit_rate: 100 % *
(Jump to the specified page as a percentage.)

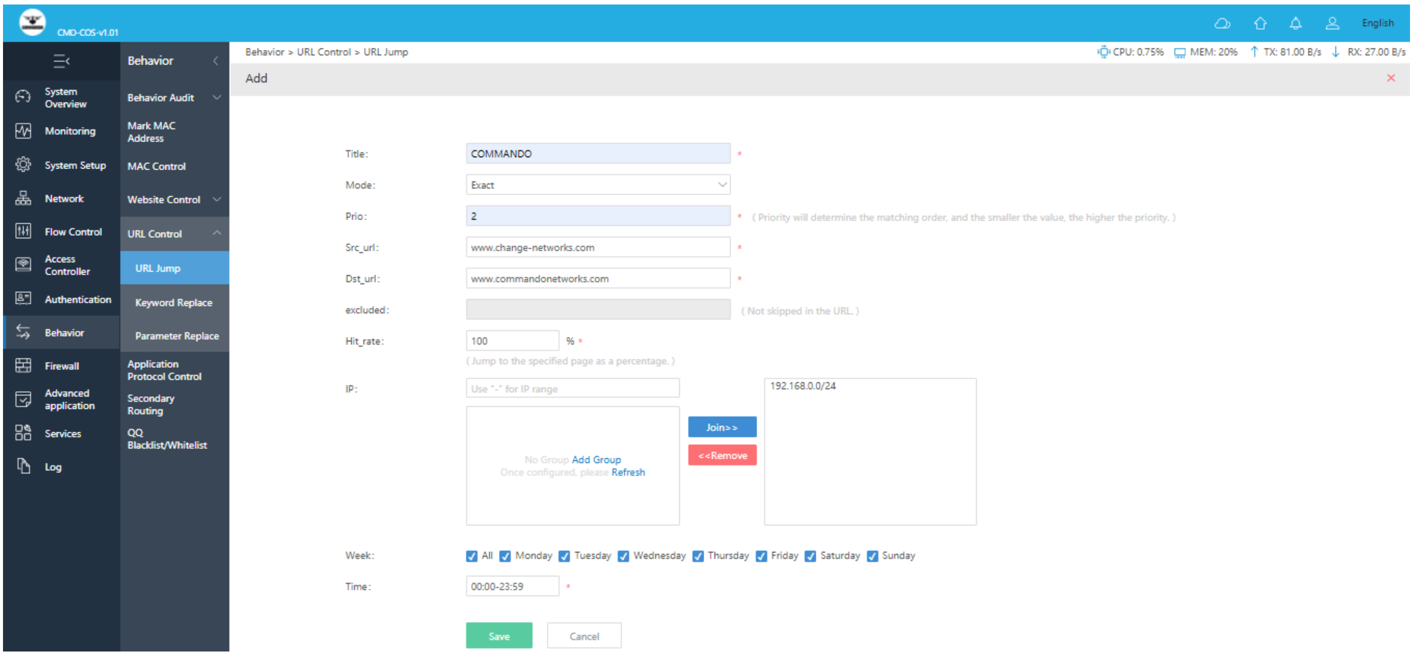
IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

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

Time: 00:00-23:59 *

Fig 7.5.2 Add URL Redirect Settings page



Behavior > URL Control > URL Jump

CPU: 0.75% MEM: 20% TX: 81.00 B/s RX: 27.00 B/s

Add

Title: COMMANDO *

Mode: Exact

Prio: 2 * (Priority will determine the matching order, and the smaller the value, the higher the priority.)

Src_url: www.change-networks.com *

Dst_url: www.commandonetworks.com *

excluded: (Not skipped in the URL.)

Hit_rate: 100 % *

(Jump to the specified page as a percentage.)

IP: Use "-" for IP range

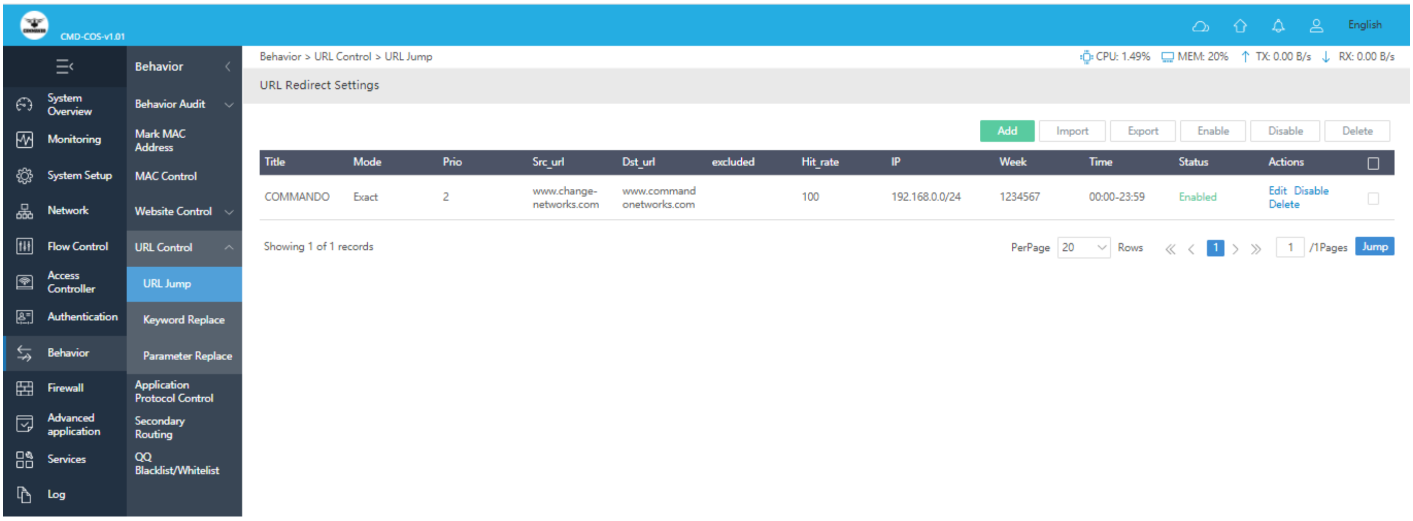
No Group Add Group
Once configured, please Refresh

192.168.0.0/24

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

Time: 00:00-23:59 *

Fig 7.5.3 Add particular URL Redirect Settings page



Behavior > URL Control > URL Jump

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

URL Redirect Settings

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

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

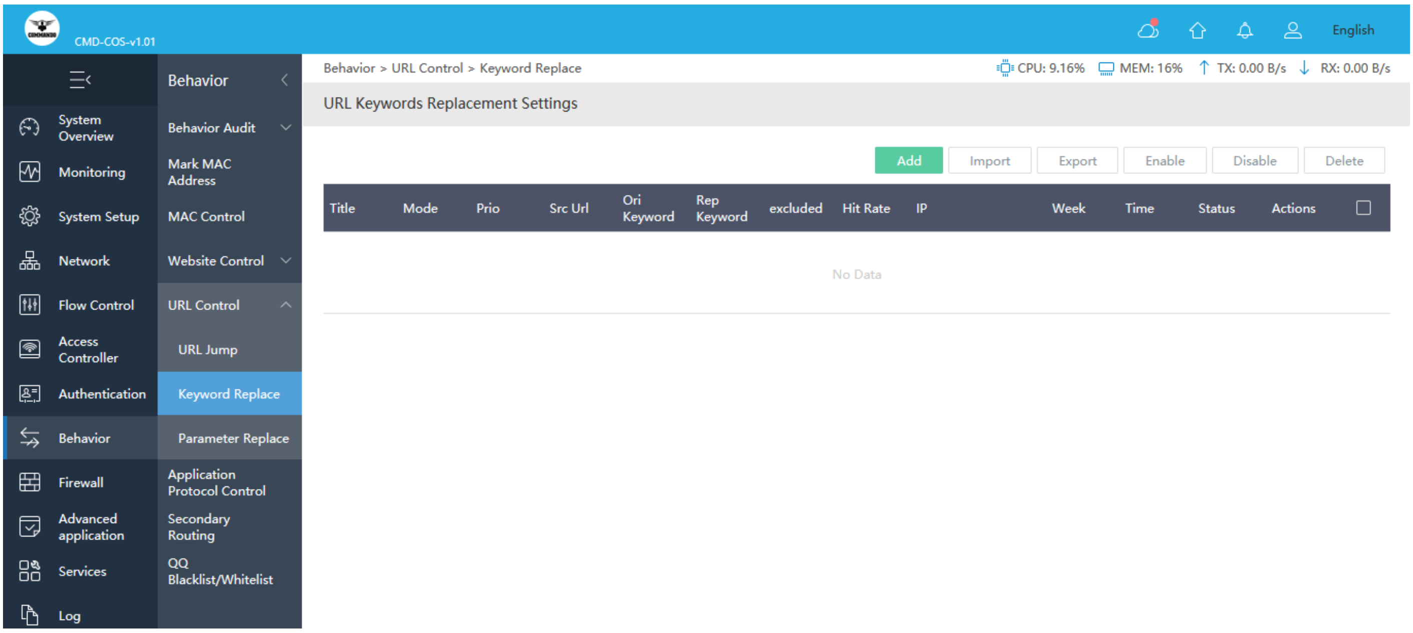
Fig 7.5.4 URL Redirect Settings page

URL Keywords Replacement Settings:

You can replace URL for a selected group of keywords with a single new URL or Search and replace all or part of the URLs for a group of keywords or

Append to the end of the URL for a group of keywords.

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



Behavior > URL Control > Keyword Replace

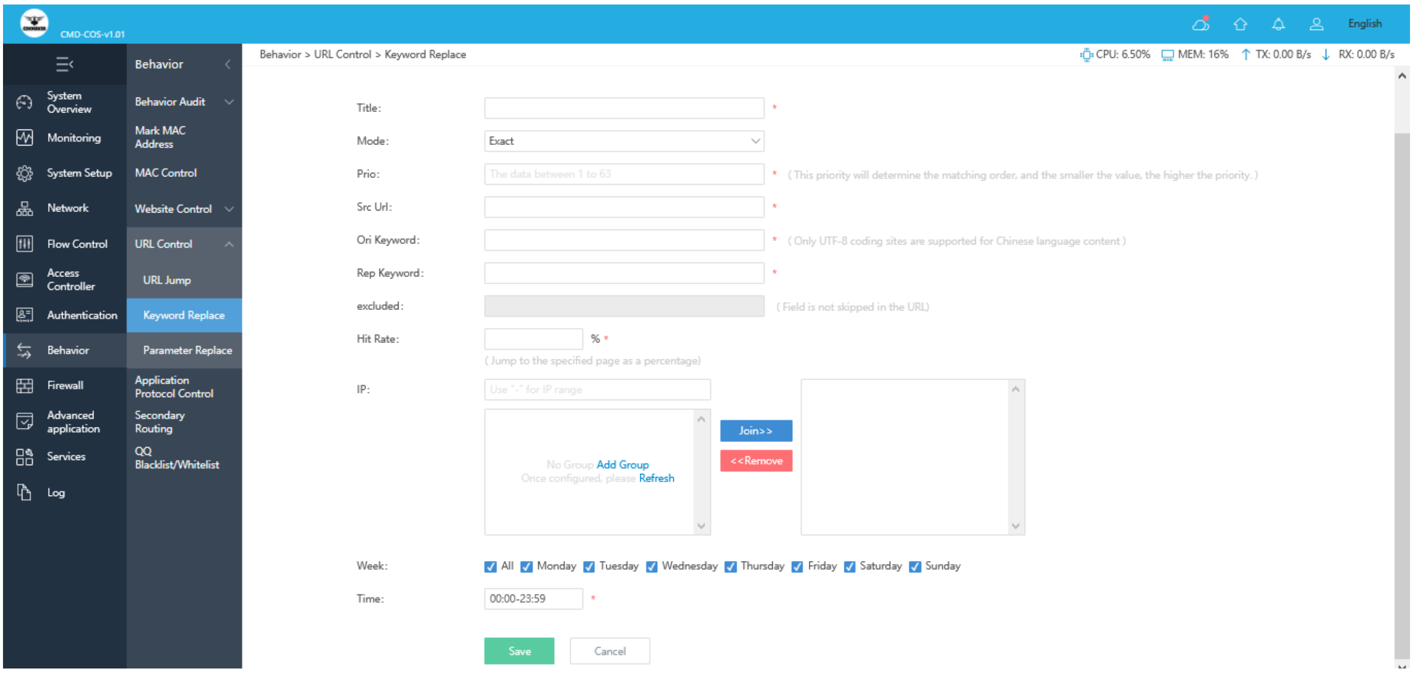
CPU: 9.16% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

URL Keywords Replacement Settings

Title	Mode	Prio	Src Url	Ori Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions	□

No Data

Fig 7.5.5 Default URL Keywords Replacement Settings page



Behavior > URL Control > Keyword Replace

CPU: 6.50% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Title: *

Mode: Exact

Prio: The data between 1 to 63 * (This priority will determine the matching order, and the smaller the value, the higher the priority.)

Src Url: *

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

Rep Keyword: *

excluded: (Field is not skipped in the URL)

Hit Rate: % *

(Jump to the specified page as a percentage)

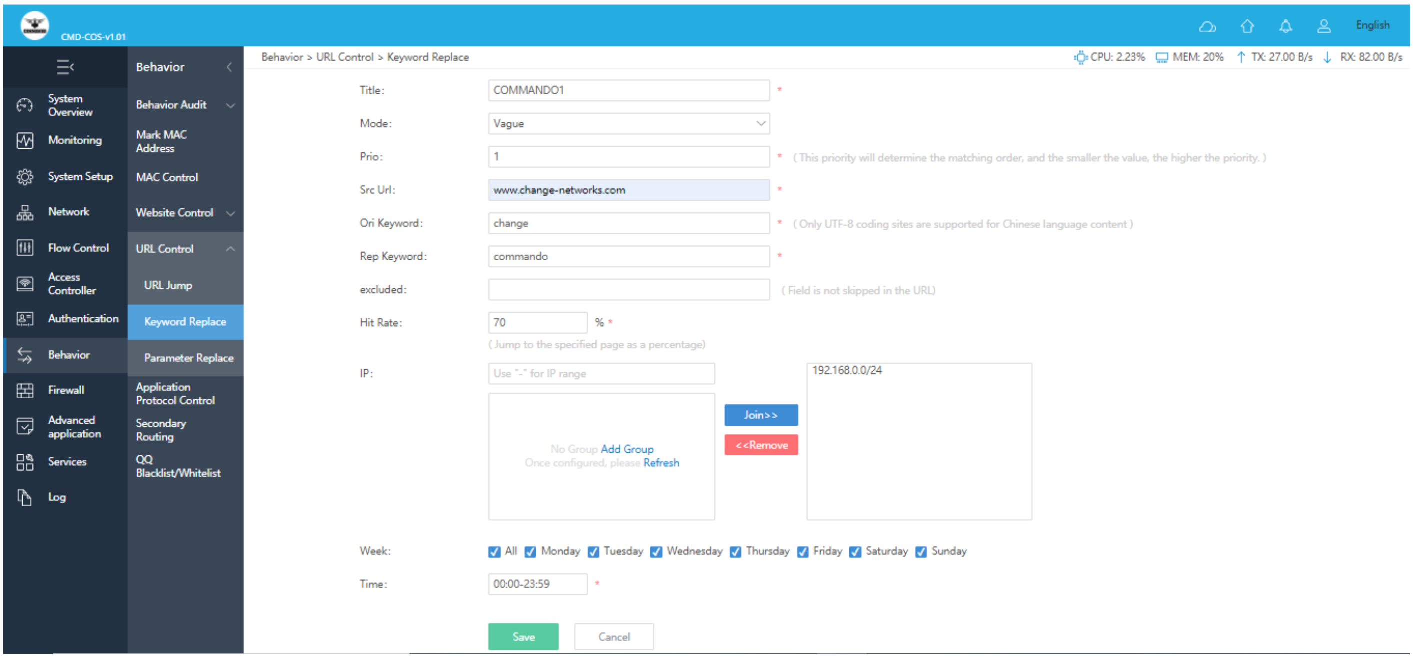
IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

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

Time: 00:00-23:59 *

Fig 7.5.6 Add Keywords Replacement Settings page



Behavior > URL Control > Keyword Replace

CPU: 2.23% MEM: 20% TX: 27.00 B/s RX: 82.00 B/s

Title: COMMANDO1 *

Mode: Vague

Prio: 1 * (This priority will determine the matching order, and the smaller the value, the higher the priority.)

Src Url: www.change-networks.com *

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

Rep Keyword: commando *

excluded: (Field is not skipped in the URL)

Hit Rate: 70 % *
(Jump to the specified page as a percentage)

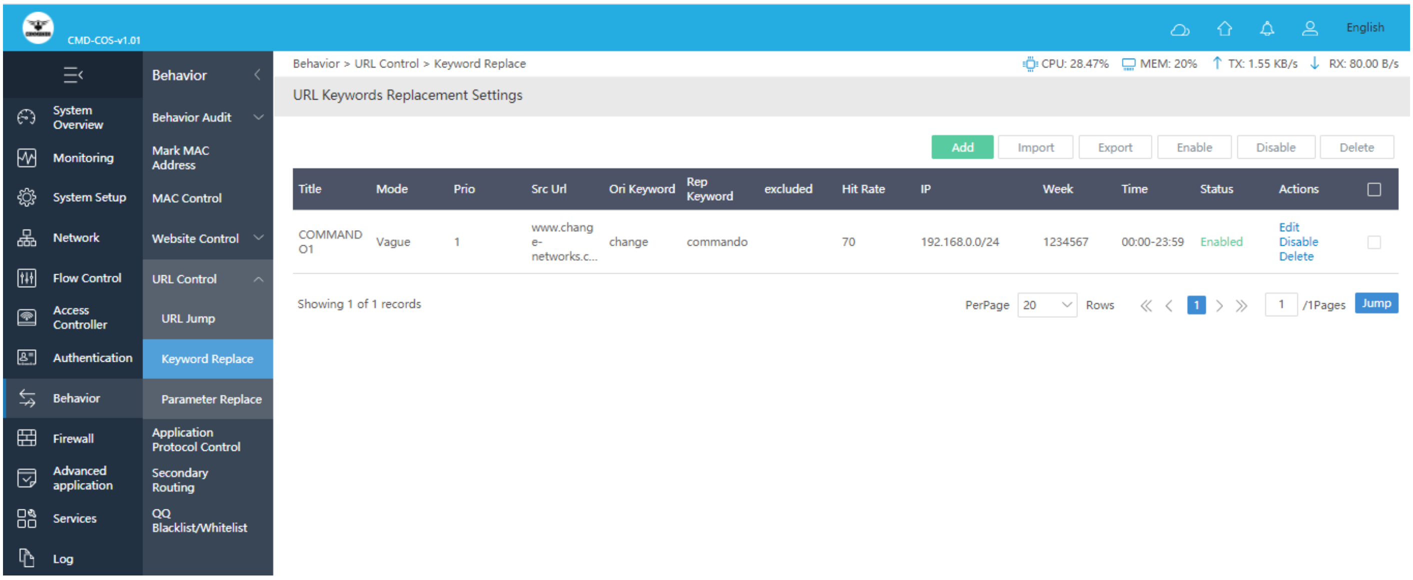
IP: Use "-" for IP range
No Group Add Group
Once configured, please Refresh
Join>>
<<Remove
192.168.0.0/24

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

Time: 00:00-23:59 *

Save Cancel

Fig 7.5.7 Keywords Replacement Settings with keyword page



Behavior > URL Control > Keyword Replace

CPU: 28.47% MEM: 20% TX: 1.55 KB/s RX: 80.00 B/s

URL Keywords Replacement Settings

Title	Mode	Prio	Src Url	Ori Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions	□
COMMANDO1	Vague	1	www.change-networks.c...	change	commando		70	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete	□

Showing 1 of 1 records

PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

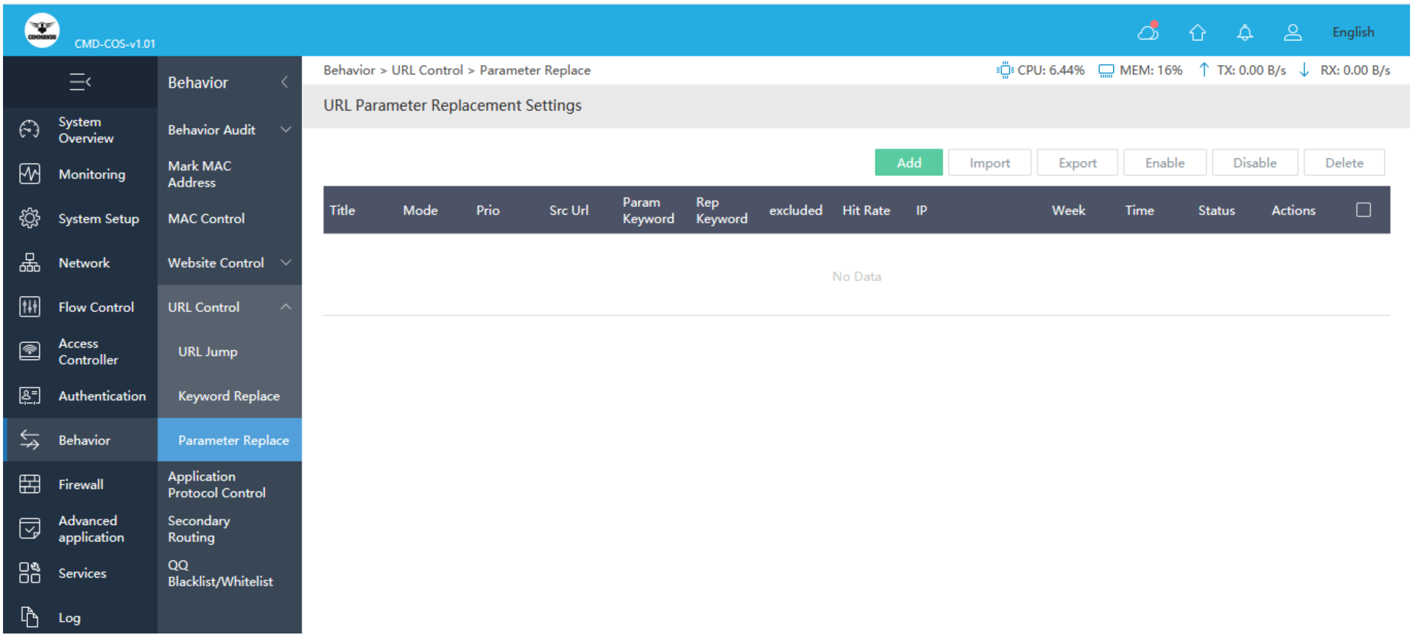
Fig 7.5.8 URL Keywords Replacement Settings page

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



Behavior > URL Control > Parameter Replace

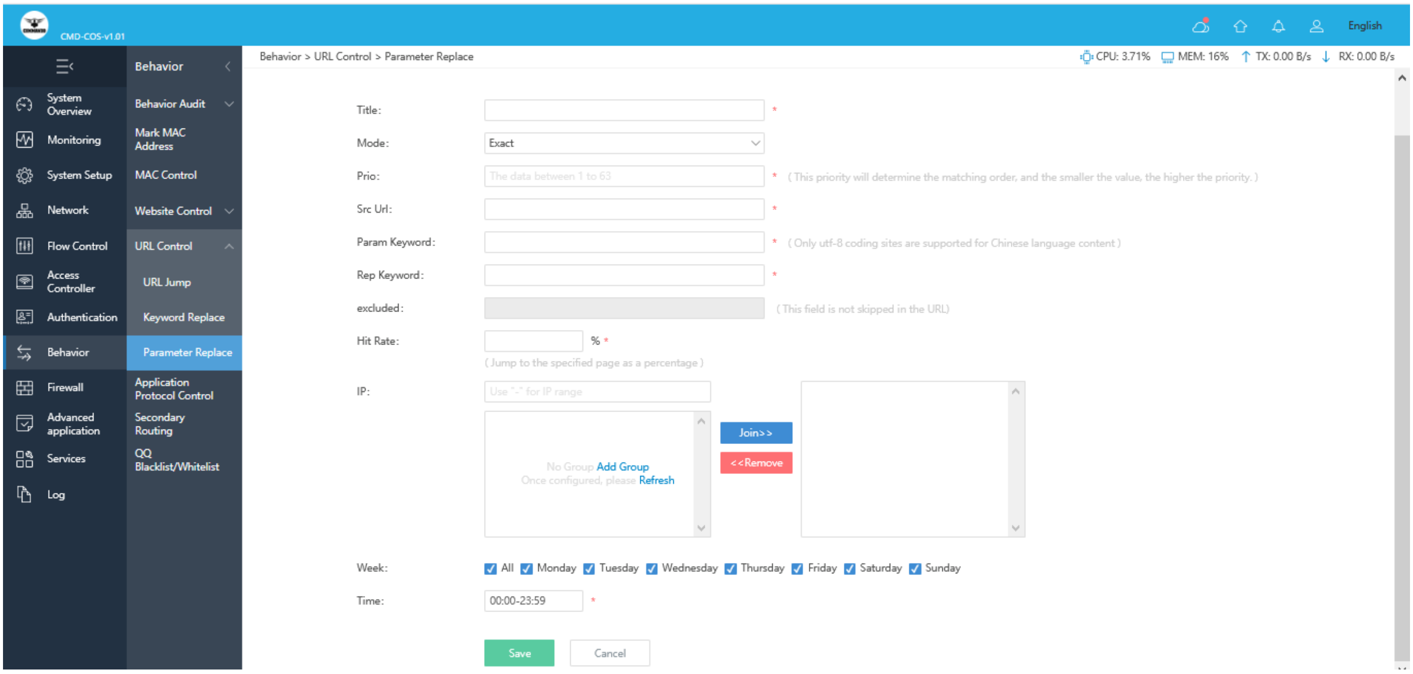
CPU: 6.44% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

URL Parameter Replacement Settings

Title	Mode	Prio	Src Url	Param Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions	□

No Data

Fig 7.5.9 Default URL Parameter Replacement Settings page



Behavior > URL Control > Parameter Replace

CPU: 3.71% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Title: *

Mode: Exact

Prio: The data between 1 to 63 * (This priority will determine the matching order, and the smaller the value, the higher the priority.)

Src Url: *

Param Keyword: * (Only utf-8 coding sites are supported for Chinese language content)

Rep Keyword: *

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

Hit Rate: % *

(Jump to the specified page as a percentage)

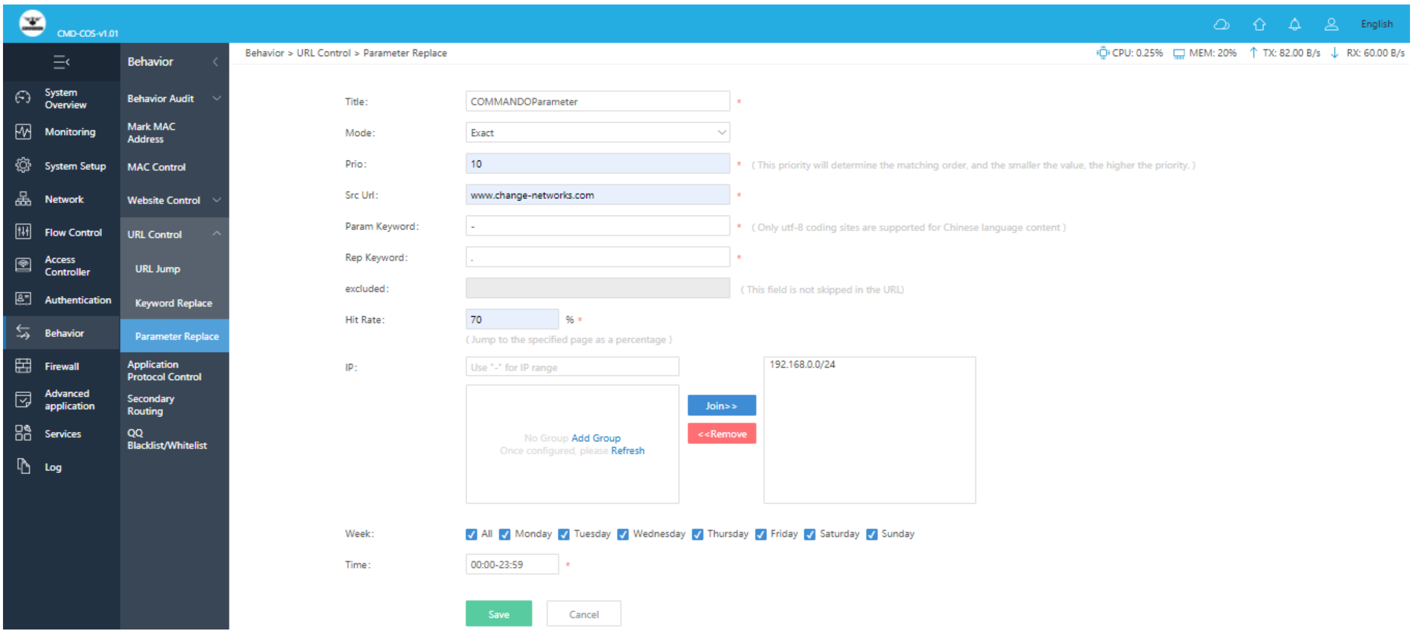
IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

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

Time: 00:00-23:59 *

Fig 7.5.10 Add URL Parameter Replacement Settings page



Behavior > URL Control > Parameter Replace

Title: COMMANDOParameter *

Mode: Exact

Prio: 10 * (This priority will determine the matching order, and the smaller the value, the higher the priority.)

Src Url: www.change-networks.com *

Param Keyword: - * (Only utf-8 coding sites are supported for Chinese language content)

Rep Keyword: . *

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

Hit Rate: 70 % *
(Jump to the specified page as a percentage)

IP: Use "-" for IP range

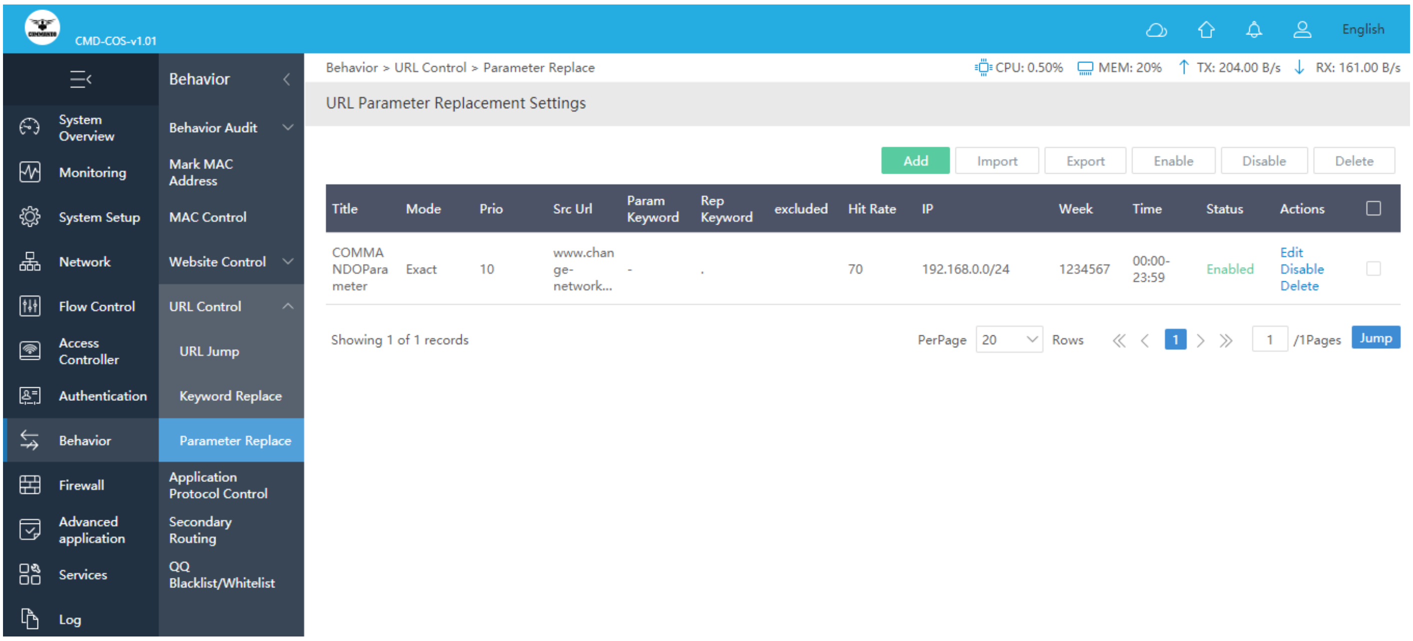
No Group Add Group
Once configured, please Refresh

192.168.0.0/24

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

Time: 00:00-23:59 *

Fig 7.5.11 URL Parameter Replacement Settings add particular keyword page



Behavior > URL Control > Parameter Replace

URL Parameter Replacement Settings

Title	Mode	Prio	Src Url	Param Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions	□
COMMANDOParameter	Exact	10	www.change-network...	-	.		70	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete	□

Showing 1 of 1 records   PerPage 20 Rows   1   1 /1Pages

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

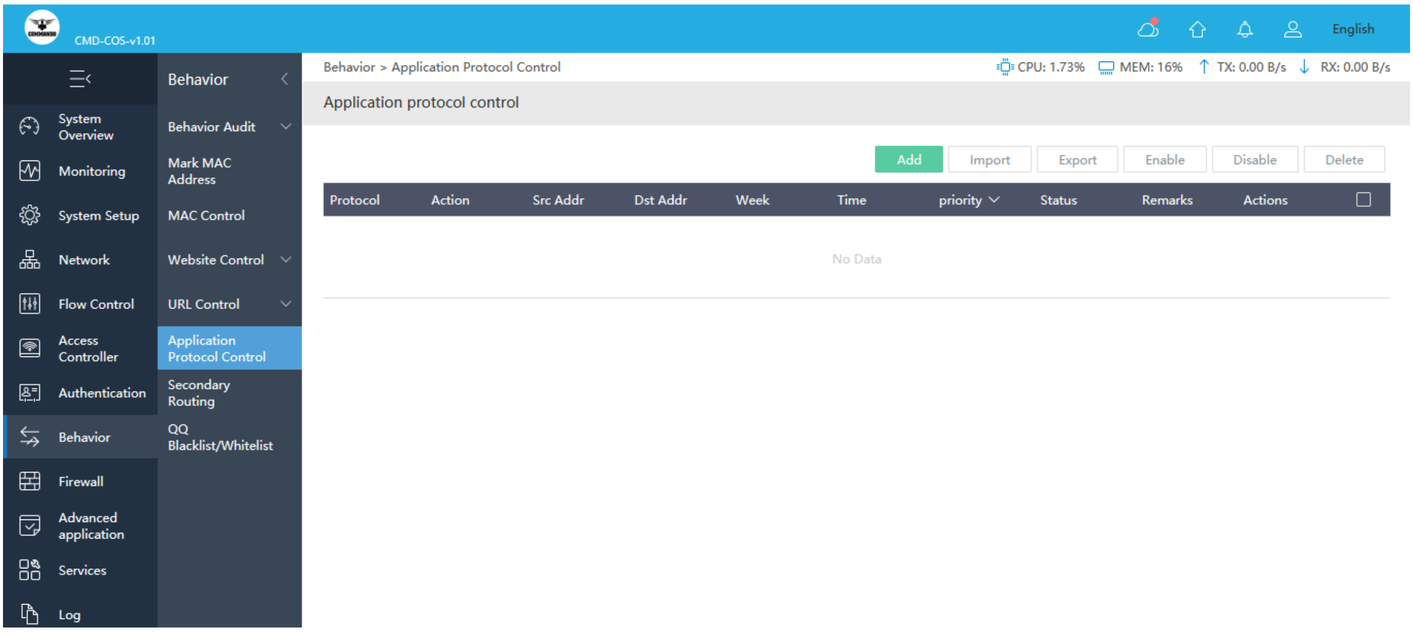
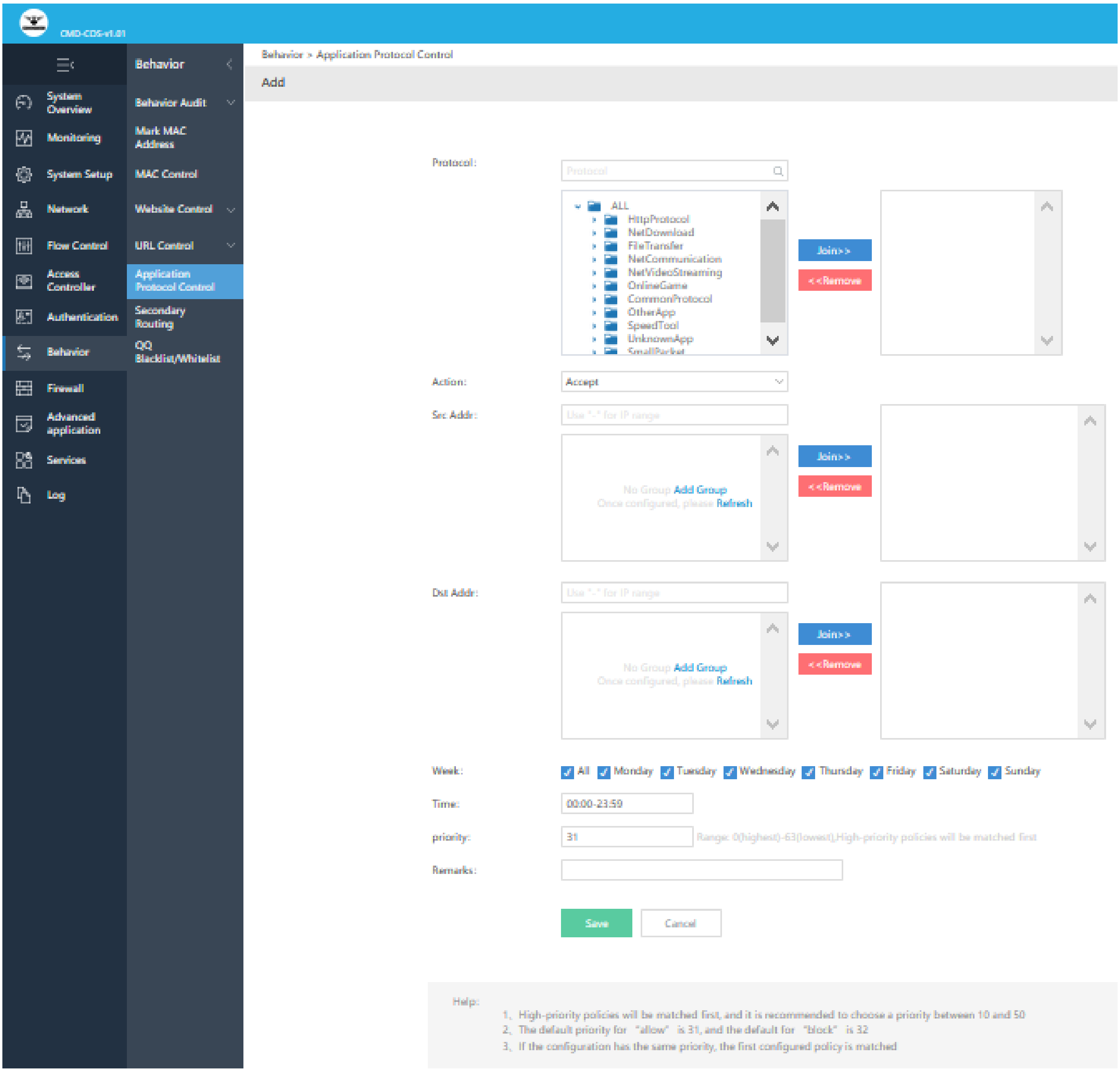


Fig 7.6.1 Default Application protocol control page



Behavior > Application Protocol Control

Add

Protocol: Protocol

ALL
HttpProtocol
NetDownload
FileTransfer
NetCommunication
NetVideoStreaming
OnlineGame
CommonProtocol
OtherApp
SpeedTool
UnknownApp
SmallPacket

Action: Accept

Src Addr: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Dst Addr: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

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

Time: 00:00-23:59

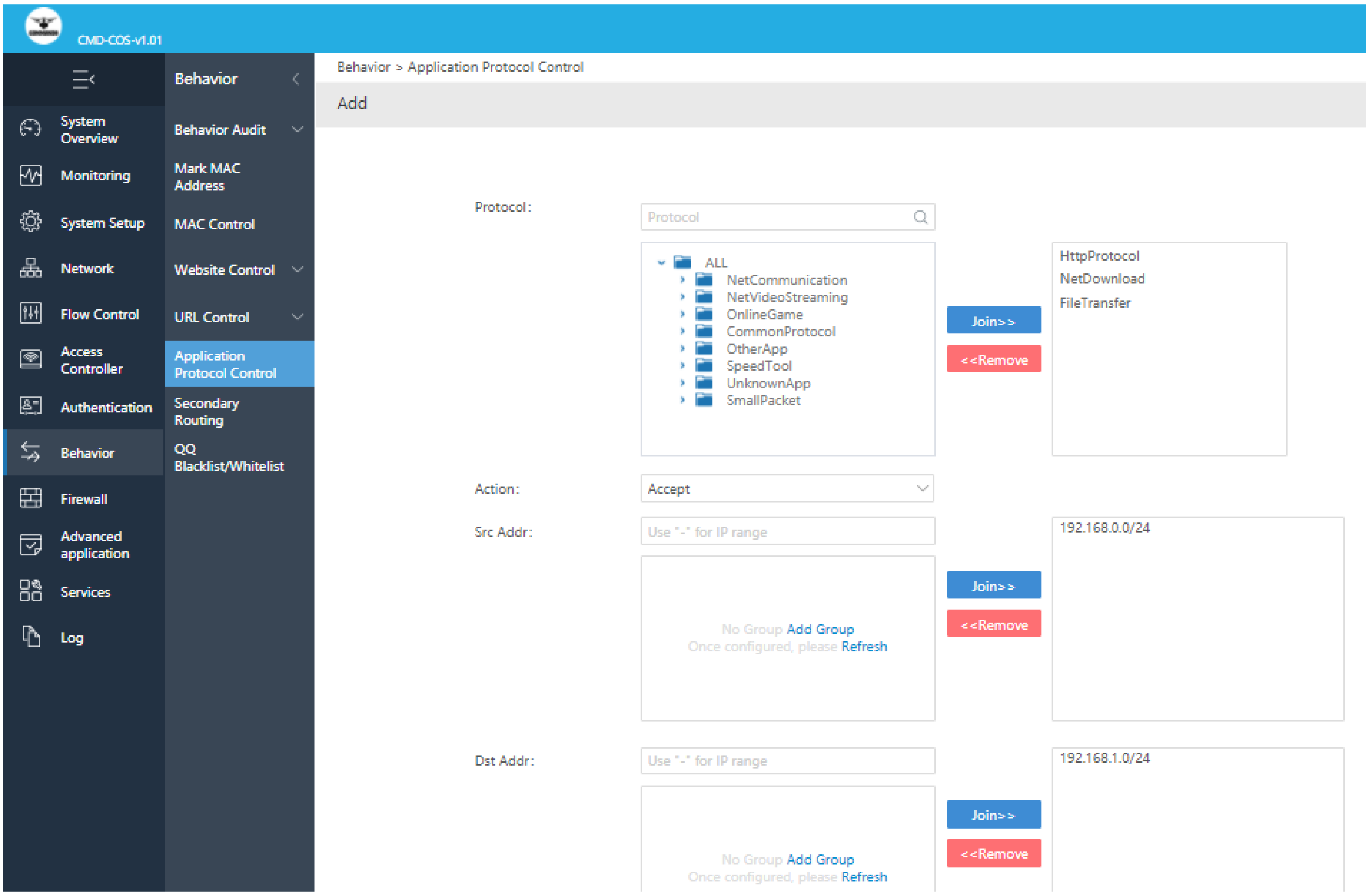
priority: 31 Range: 0(highest)-63(lowest),High-priority policies will be matched first

Remarks:

Help:

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

Fig 7.6.2 Add Application protocol control page



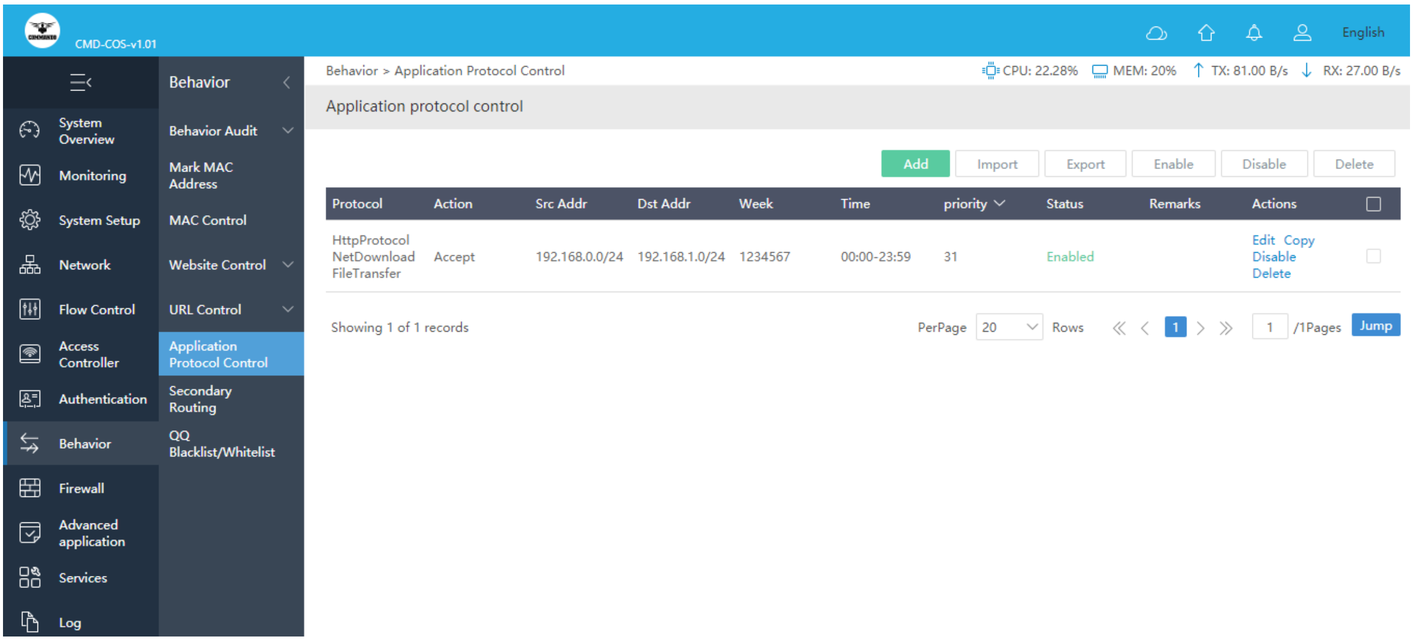
Protocol: HttpProtocol, NetDownload, FileTransfer

Action: Accept

Src Addr: 192.168.0.0/24

Dst Addr: 192.168.1.0/24

Fig 7.6.3 Application protocol control add particular action page



Protocol	Action	Src Addr	Dst Addr	Week	Time	priority	Status	Remarks	Actions	□
HttpProtocol NetDownload FileTransfer	Accept	192.168.0.0/24	192.168.1.0/24	1234567	00:00-23:59	31	Enabled		Edit Copy Disable Delete	□

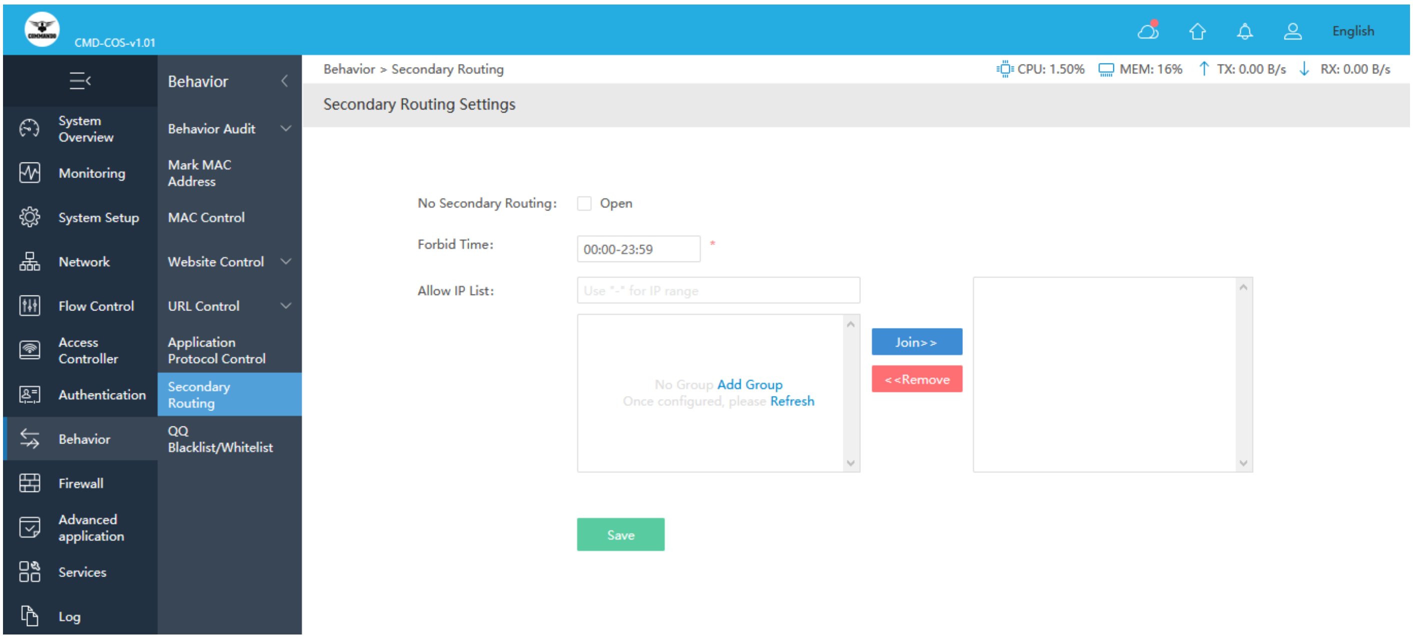
Showing 1 of 1 records PerPage 20 Rows 1 /1Pages Jump

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



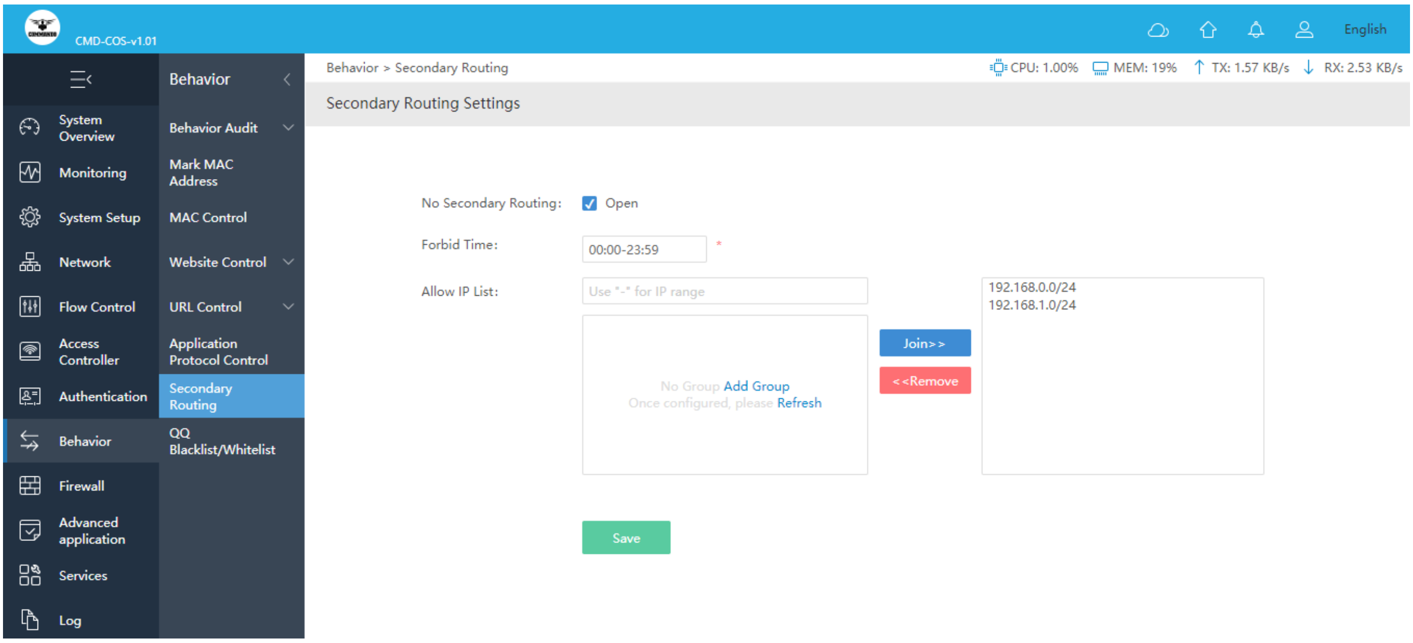
Secondary Routing Settings

No Secondary Routing: □ Open

Forbid Time: 00:00-23:59 *

Allow IP List: Use "-" for IP range

Fig 7.7.1 Default Secondary Routing Settings page



Secondary Routing Settings

No Secondary Routing: ☑ Open

Forbid Time: 00:00-23:59 *

Allow IP List: Use "-" for IP range

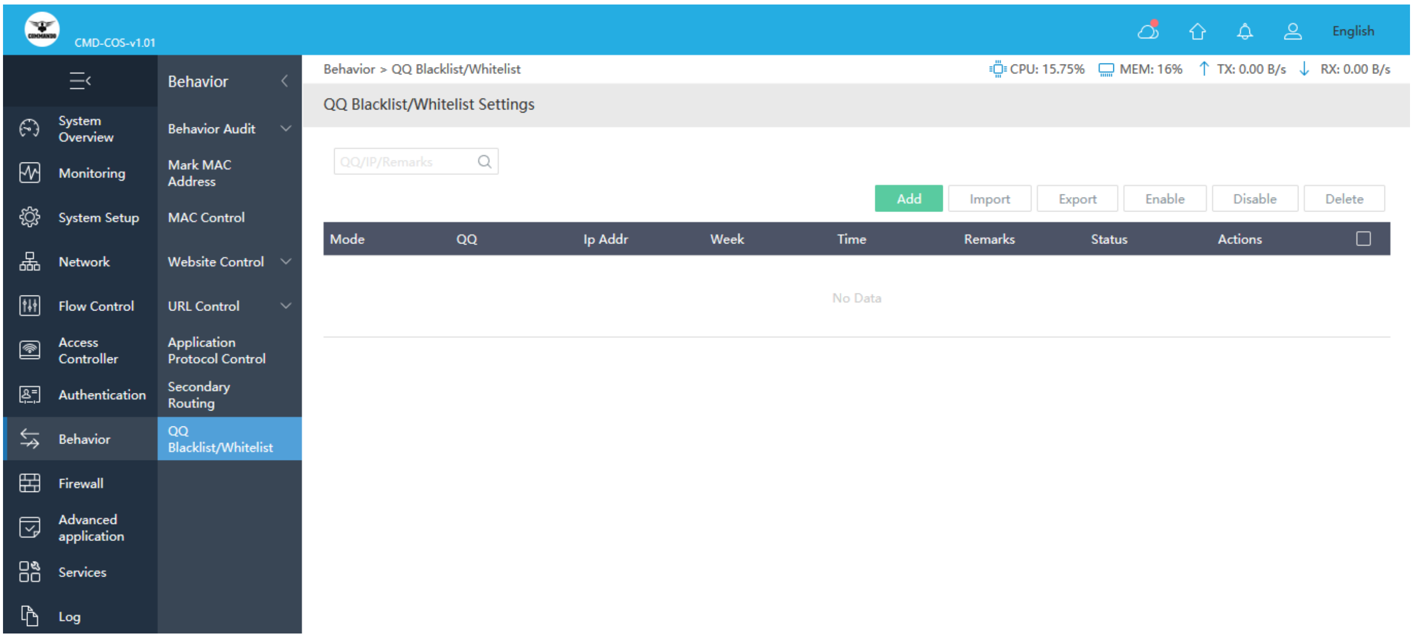
192.168.0.0/24
192.168.1.0/24

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



Behavior > QQ Blacklist/Whitelist

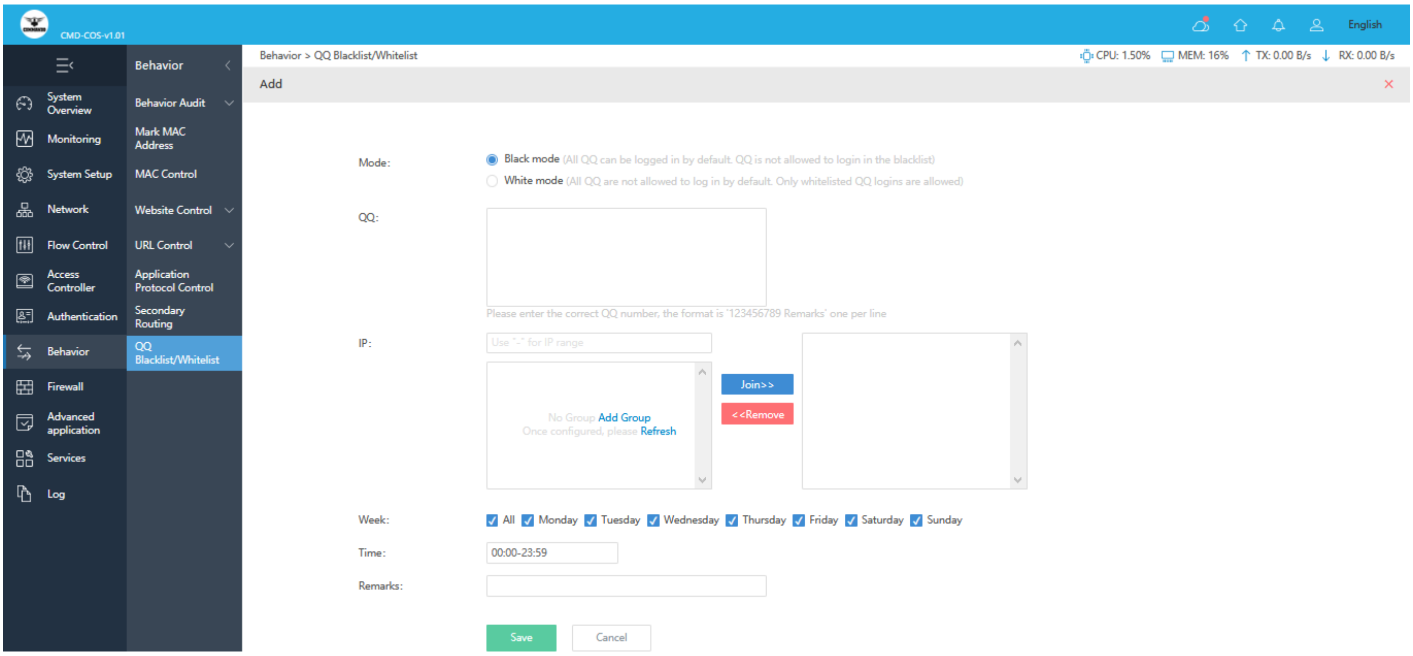
CPU: 15.75% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

QQ Blacklist/Whitelist Settings

Mode	QQ	Ip Addr	Week	Time	Remarks	Status	Actions	□

No Data

Fig 7.8.1 Default QQ Blacklist/Whitelist Settings page



Behavior > QQ Blacklist/Whitelist

CPU: 1.50% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Add

Mode: ● Black mode (All QQ can be logged in by default. QQ is not allowed to login in the blacklist)
○ White mode (All QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed)

QQ:

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

IP: Use "-" for IP range

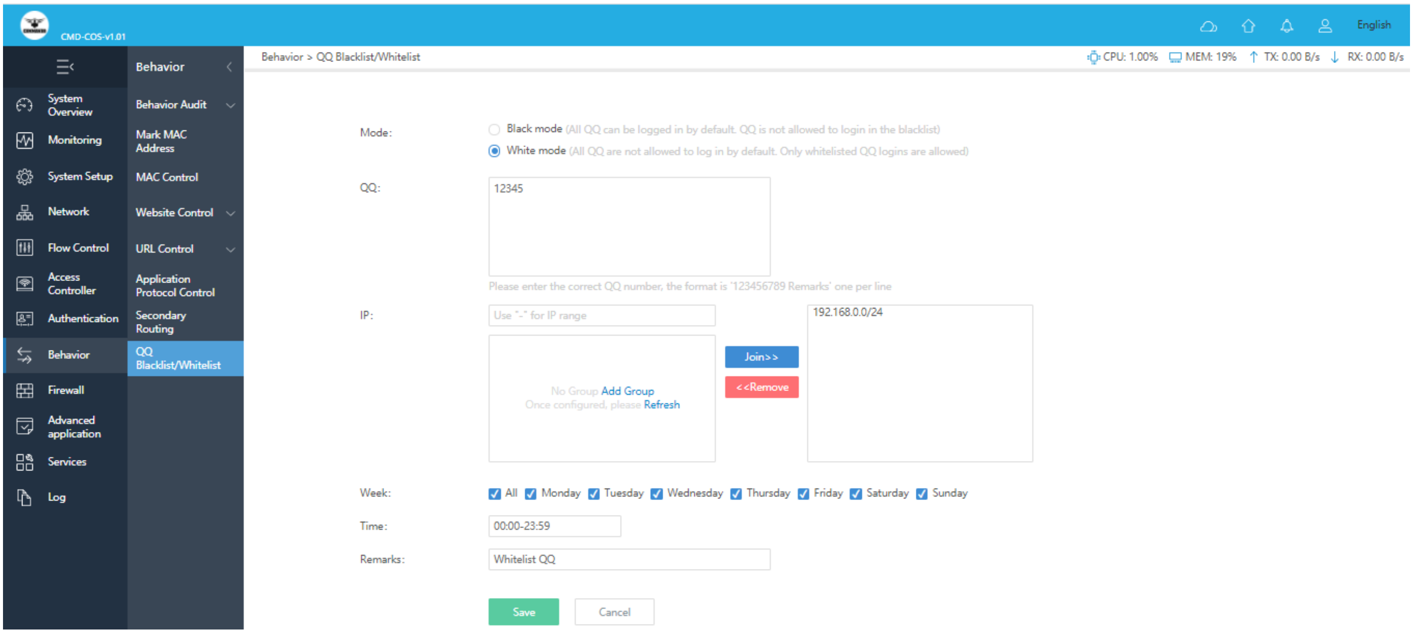
No Group Add Group
Once configured, please Refresh

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

Time: 00:00-23:59

Remarks:

Fig 7.8.2 Add QQ Blacklist/Whitelist Settings page



Mode: ○ Black mode (All QQ can be logged in by default. QQ is not allowed to login in the blacklist)
● White mode (All QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed)

QQ: 12345

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

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Join>>
<<Remove

192.168.0.0/24

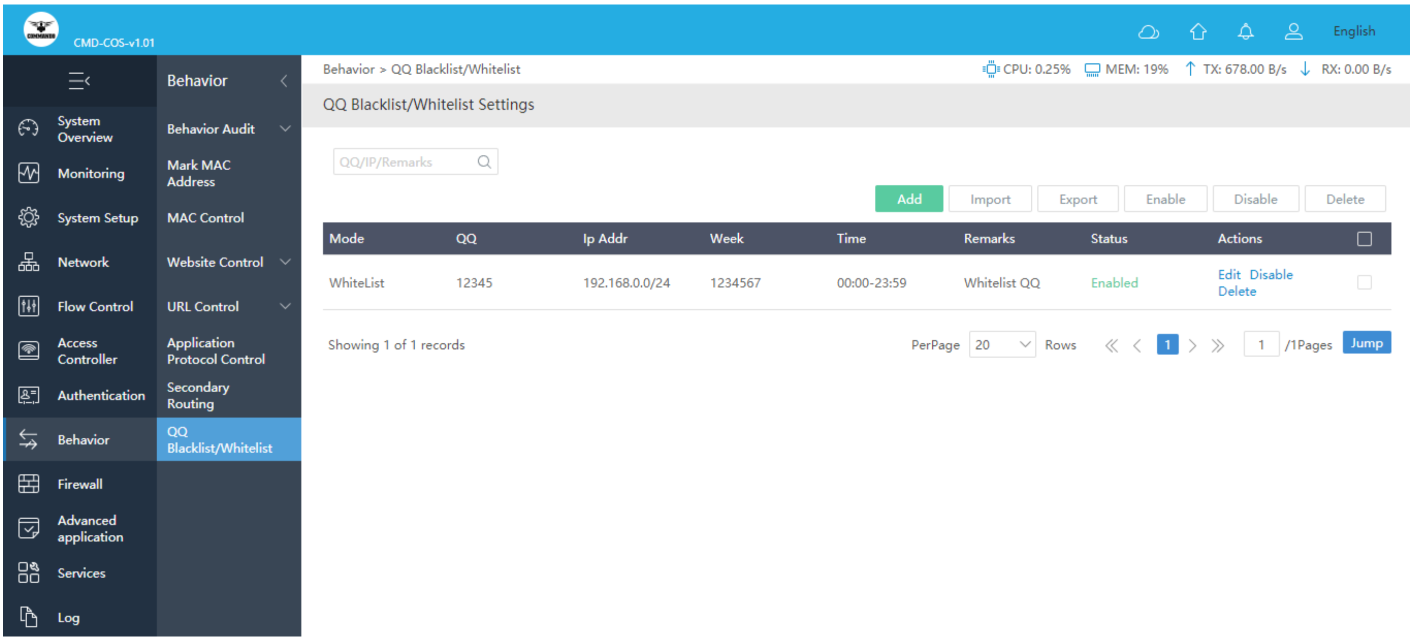
Week: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Time: 00:00-23:59

Remarks: Whitelist QQ

Save Cancel

Fig 7.8.3 QQ Blacklist/Whitelist Settings for particular Network page



QQ Blacklist/Whitelist Settings

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

Showing 1 of 1 records PerPage 20 Rows 1 /1Pages Jump

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.

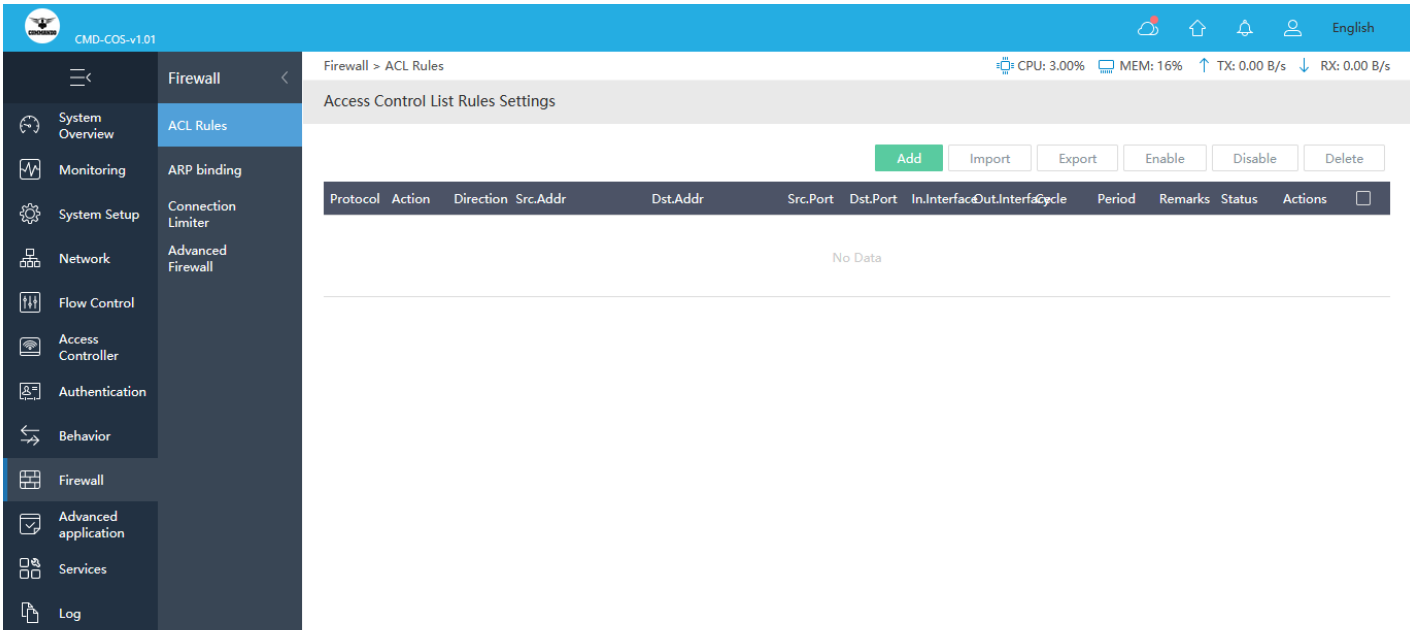
Advanced Firewall:
This advance firewall to Block PING from internal network, Block PING from public network, Disable tracert (Trace Route), Hijack all PING values, Discard invalid connection,

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



Firewall > ACL Rules

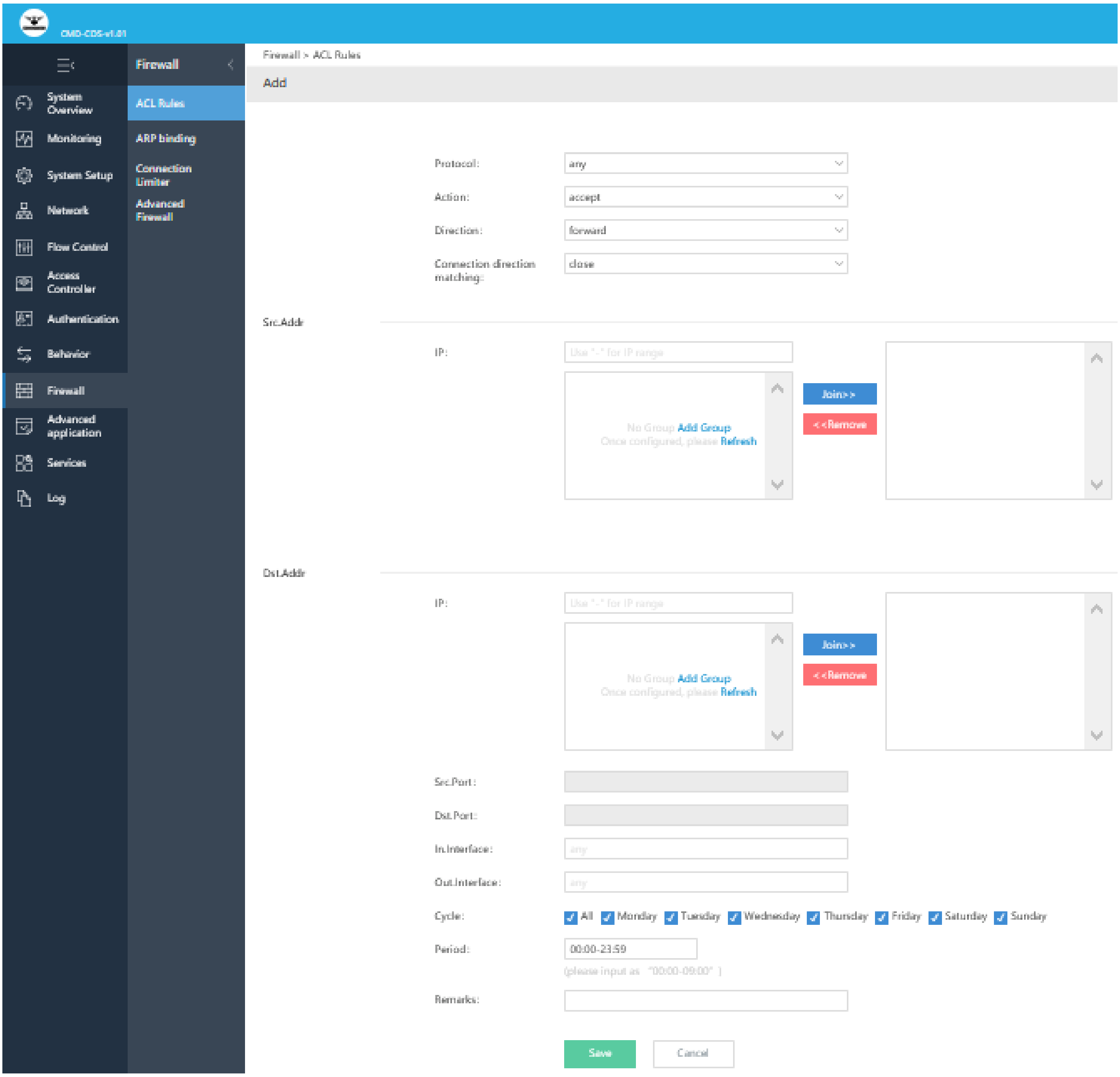
CPU: 3.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Access Control List Rules Settings

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



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

Dst.Addr

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

Src.Port:

Dst.Port:

In.Interface: any

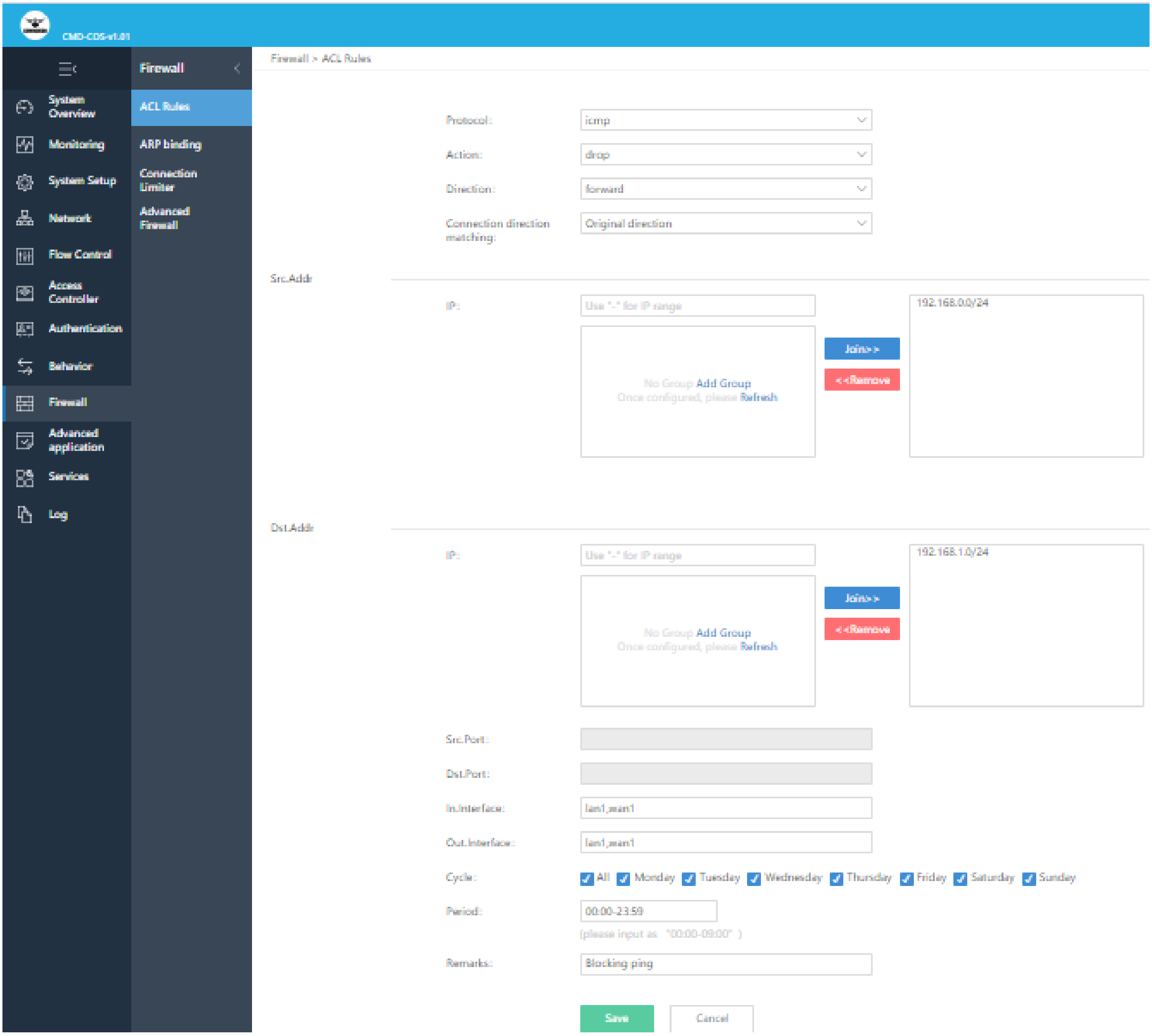
Out.Interface: any

Cycle: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Period: 00:00-23:59
(please input as "00:00-09:00")

Remarks:

Fig 8.1.2 Add Access Control List Rules page



Firewall > ACL Rules

Protocol: icmp

Action: drop

Direction: forward

Connection direction matching: Original direction

Src.Addr

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

192.168.0.0/24

Dst.Addr

IP: Use "-" for IP range

No Group Add Group
Once configured, please Refresh

192.168.1.0/24

Src.Port:

Dst.Port:

In.Interface: lan1,wan1

Out.Interface: lan1,wan1

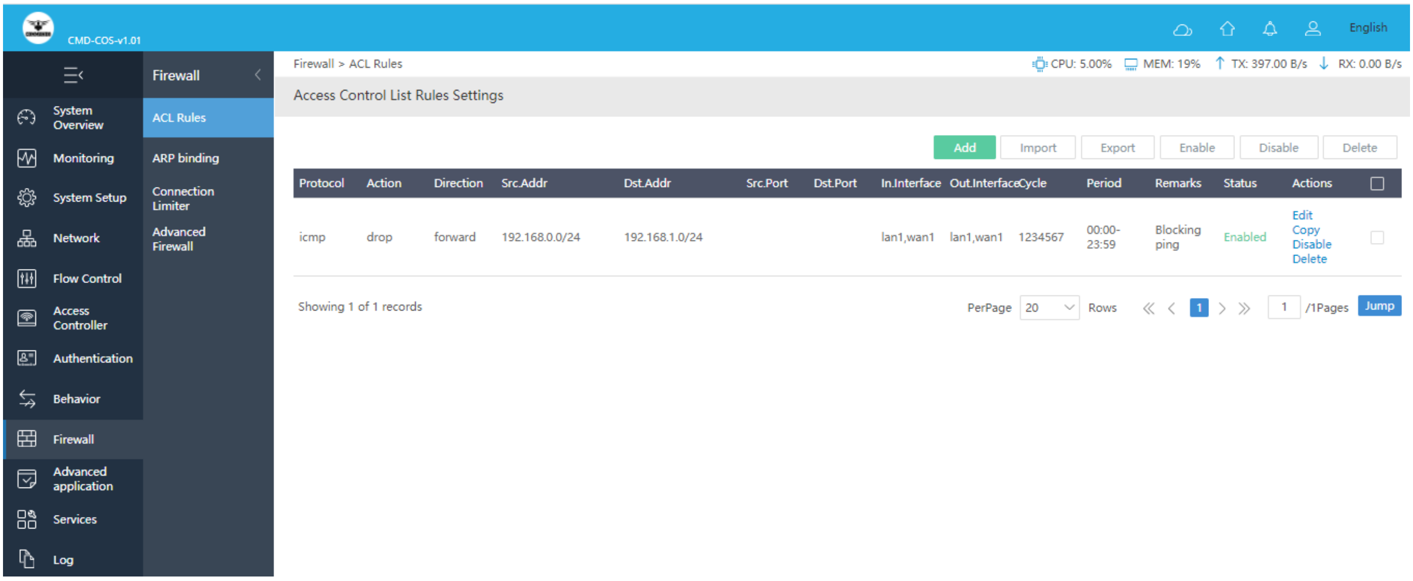
Cycle: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Period: 00:00-23:59

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

Remarks: Blocking ping

Fig 8.1.3 Add particular Access Control List Rules page



Firewall > ACL Rules

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

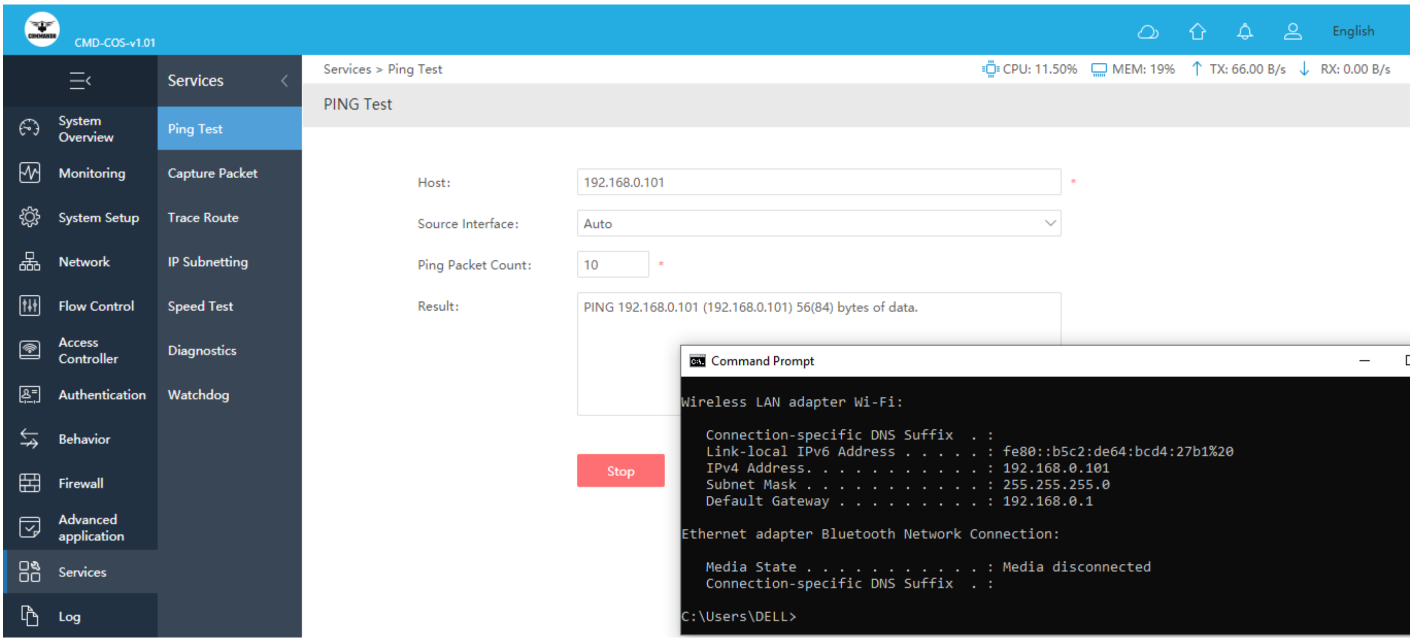
Access Control List Rules Settings

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

Fig 8.1.4 Access Control List Rules setting page



PING Test

Host: 192.168.0.101 *

Source Interface: Auto

Ping Packet Count: 10 *

Result: PING 192.168.0.101 (192.168.0.101) 56(84) bytes of data.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b5c2:de64:bcd4:27b1%20
   IPv4 Address. . . . . . . . . . . : 192.168.0.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\DELL>
```

Fig 8.1.5 Impact of Access Control List Rules page

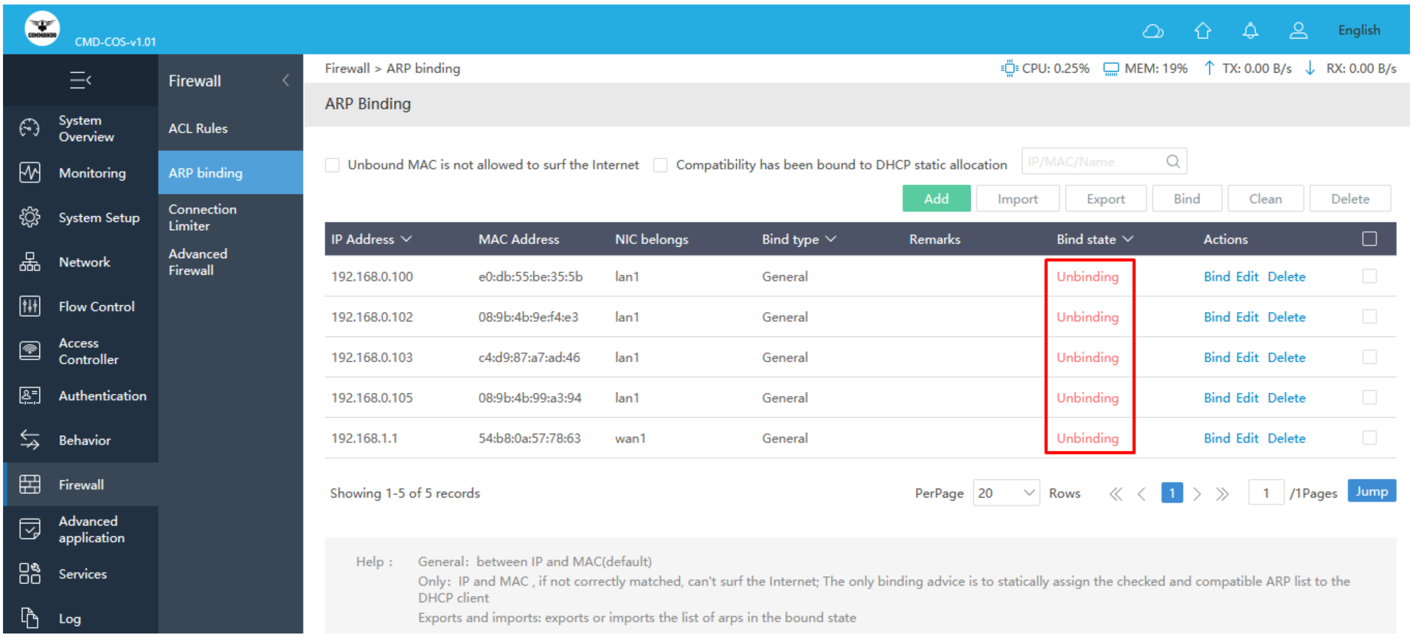
8.2 Arp Binding

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



Firewall > ARP binding   CPU: 0.25% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

ARP Binding

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

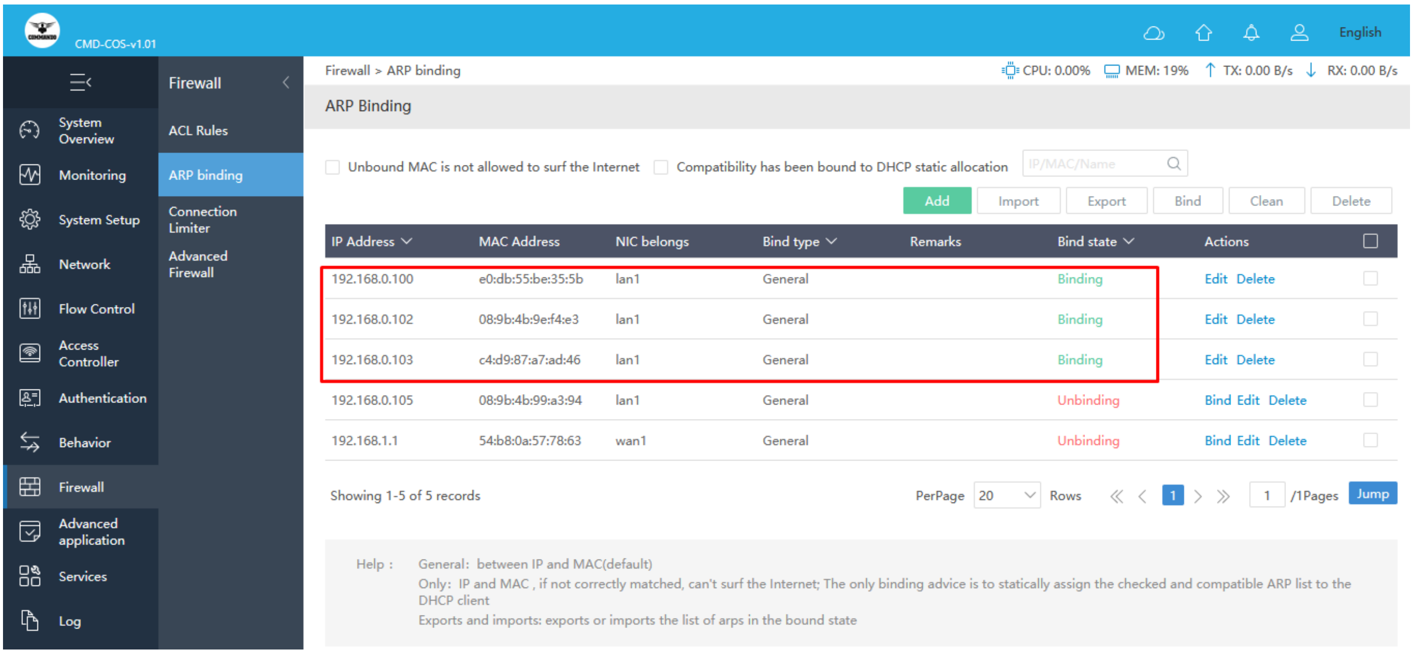
Add Import Export Bind Clean Delete

IP Address	MAC Address	NIC belongs	Bind type	Remarks	Bind state	Actions	□
192.168.0.100	e0:db:55:be:35:5b	lan1	General		Unbinding	Bind Edit Delete	□
192.168.0.102	08:9b:4b:9e:f4: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	□

Showing 1-5 of 5 records   PerPage 20 Rows 1 1 /1Pages 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 8.2.1 Default ARP Binding page



Firewall > ARP binding

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

ARP Binding

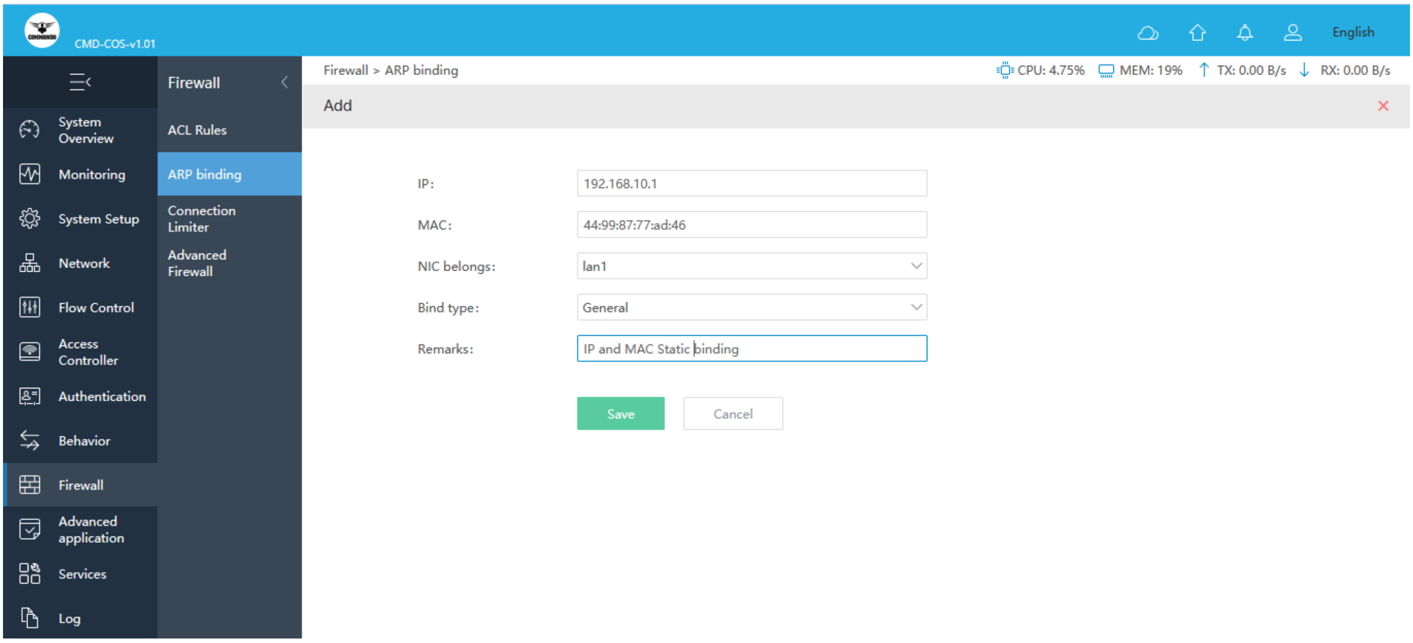
□ Unbound MAC is not allowed to surf the Internet □ Compatibility has been bound to DHCP static allocation

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 /1Pages

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

CPU: 4.75% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

Add

IP: 192.168.10.1

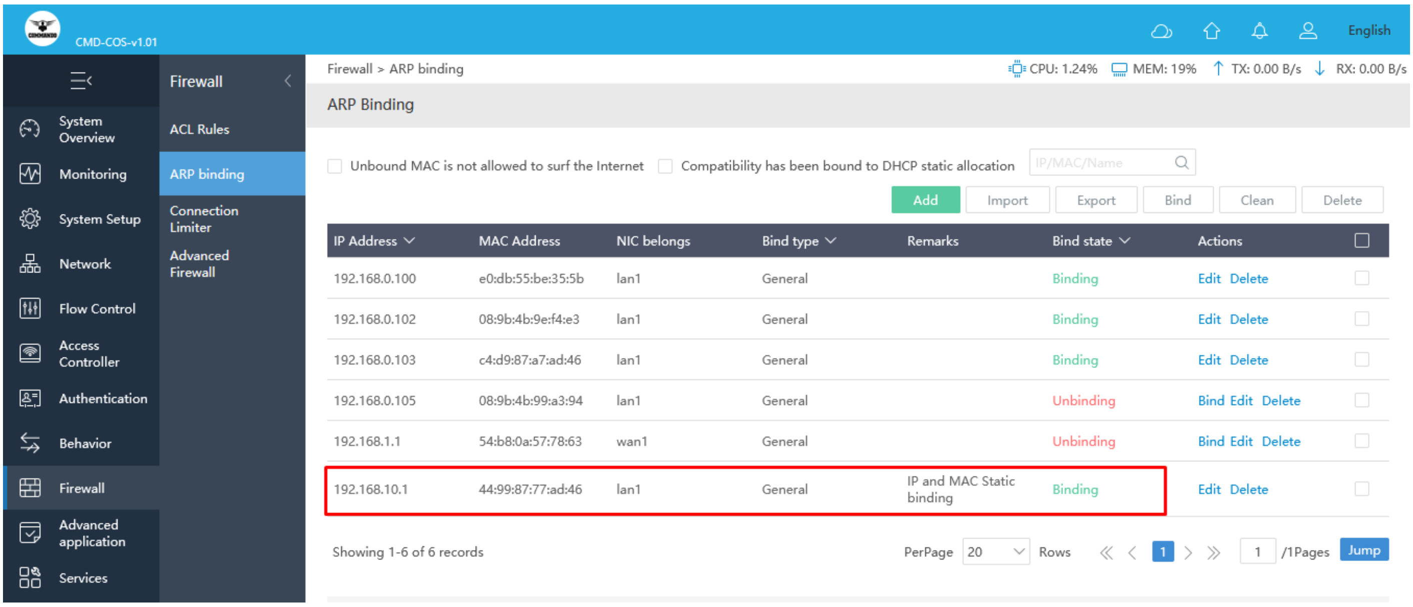
MAC: 44:99:87:77:ad:46

NIC belongs: lan1

Bind type: General

Remarks: IP and MAC Static binding

Fig 8.2.3 Add ARP Binding page



Firewall > ARP binding

CPU: 1.24% MEM: 19% TX: 0.00 B/s RX: 0.00 B/s

ARP Binding

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

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	□

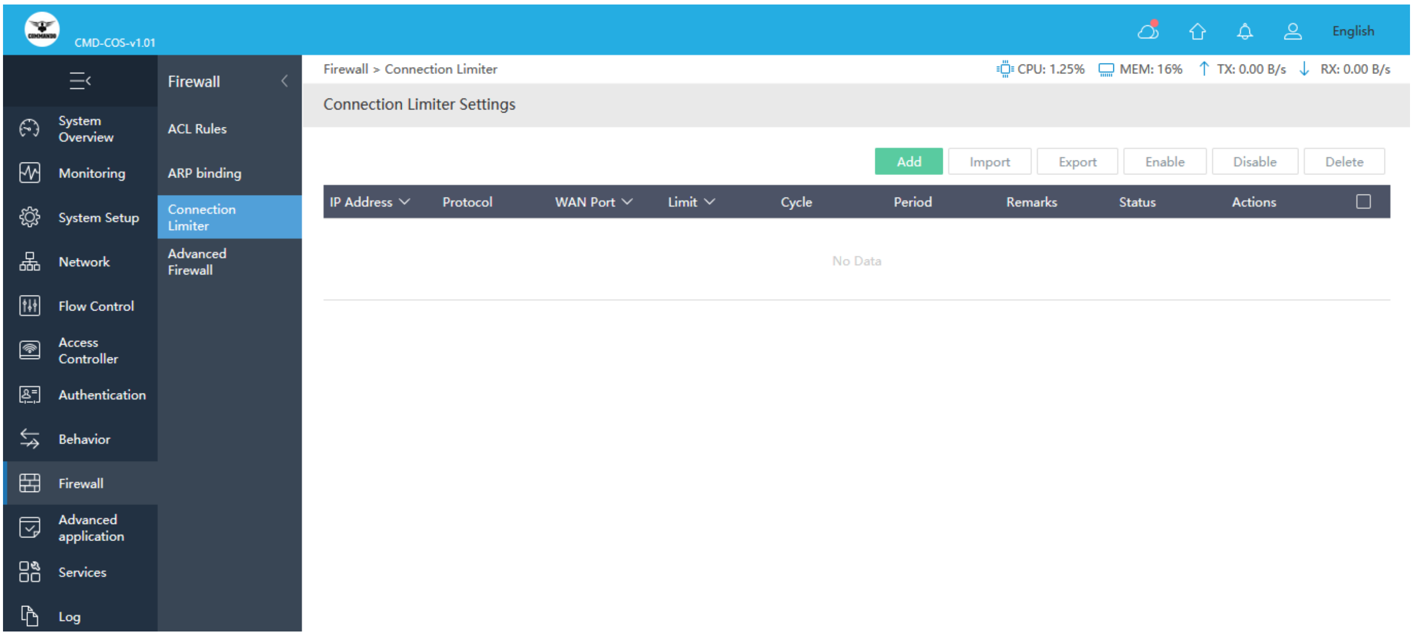
Showing 1-6 of 6 records PerPage 20 Rows 1 /1Pages

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

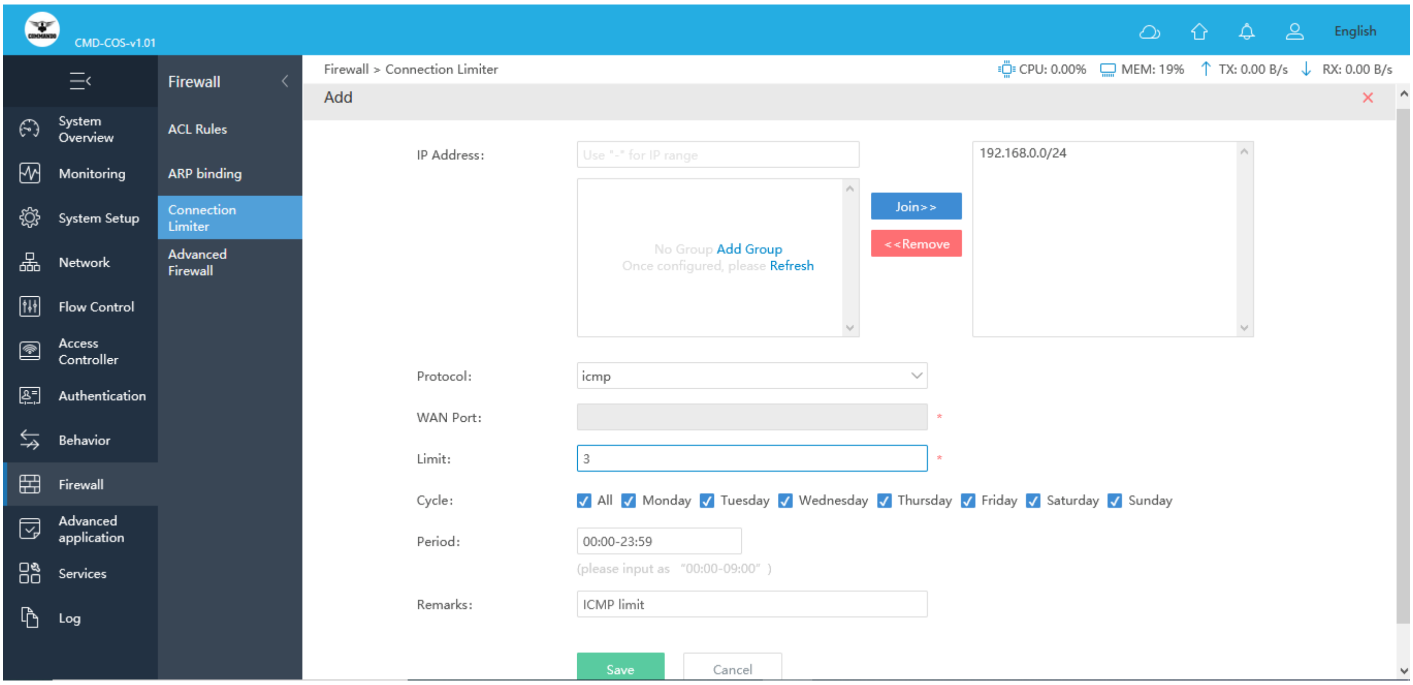
CPU: 1.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

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



Add

IP Address: Use "-" for IP range

192.168.0.0/24

Protocol: icmp

WAN Port: *

Limit: 3 *

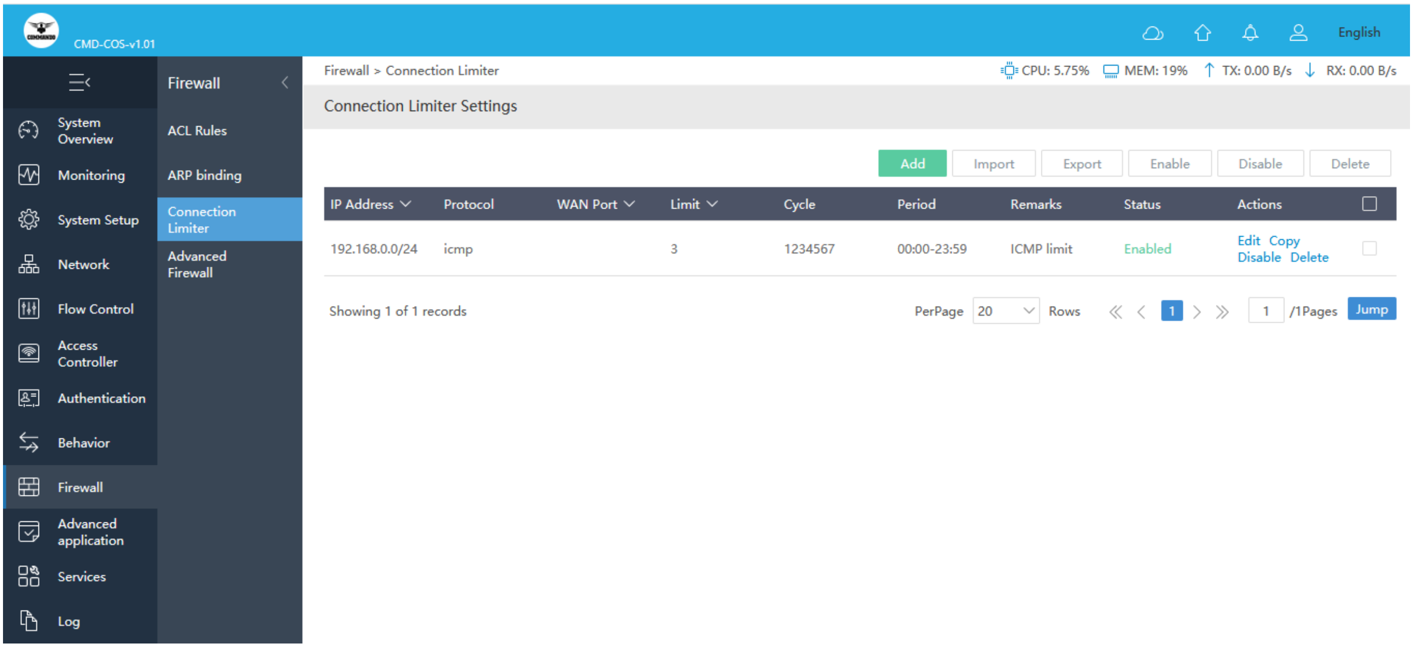
Cycle: ☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Period: 00:00-23:59

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

Remarks: ICMP limit

Fig 8.3.2 Add Connection Limiter Settings page



Connection Limiter Settings

IP Address	Protocol	WAN Port	Limit	Cycle	Period	Remarks	Status	Actions	□
192.168.0.0/24	icmp		3	1234567	00:00-23:59	ICMP limit	Enabled	Edit Copy Disable Delete	□

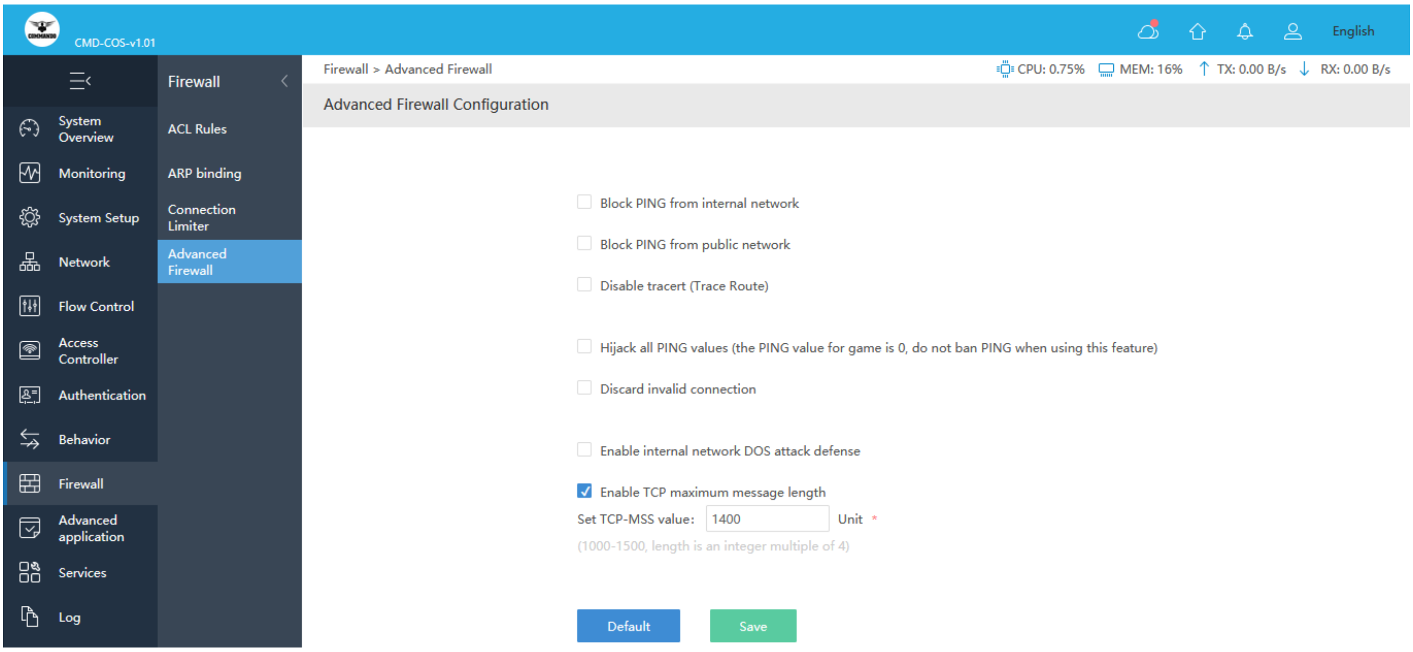
Showing 1 of 1 records PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

Fig 8.3.3 Connection Limiter Settings page

8.4 Advanced Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Generally, Firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall is a security device in network that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access. A firewall is an essential part of security system. Without it, your network is open to threats and attacks. A firewall keeps destructive and disruptive forces out and controls the incoming and outgoing network traffic based on security parameters that you can control and define. Advance firewall to Block PING from internal network, Block PING from public network, Disable tracert (Trace Route), Hijack all PING values, Discard invalid connection and also enable internal network DOS attack defense and TCP maximum message length.

To configure Advanced Firewall Configuration, Click on Firewall > Advanced Firewall



Advanced Firewall Configuration

□ 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

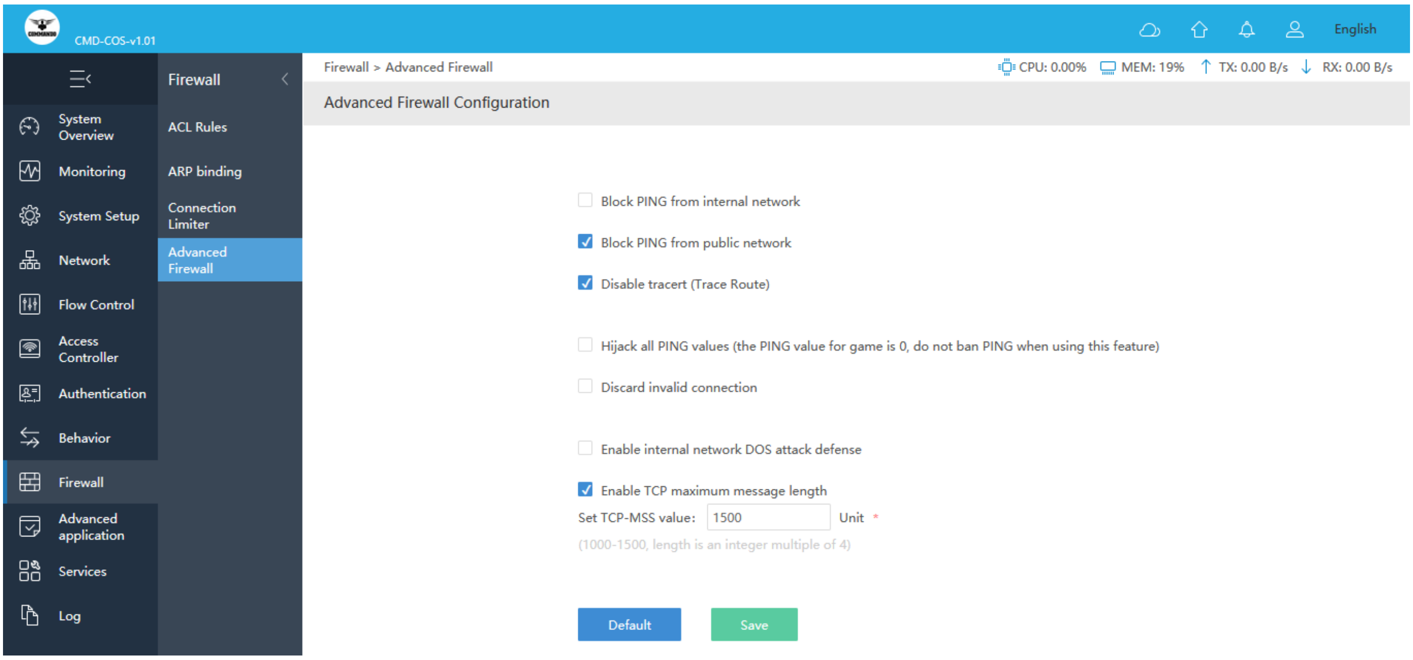
□ Enable internal network DOS attack defense

☑ Enable TCP maximum message length

Set TCP-MSS value: 1400 Unit *

(1000-1500, length is an integer multiple of 4)

Fig 8.4.1 Default Advanced Firewall Configuration page



Advanced Firewall Configuration

□ 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

Set TCP-MSS value: 1500 Unit *

(1000-1500, length is an integer multiple of 4)

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:

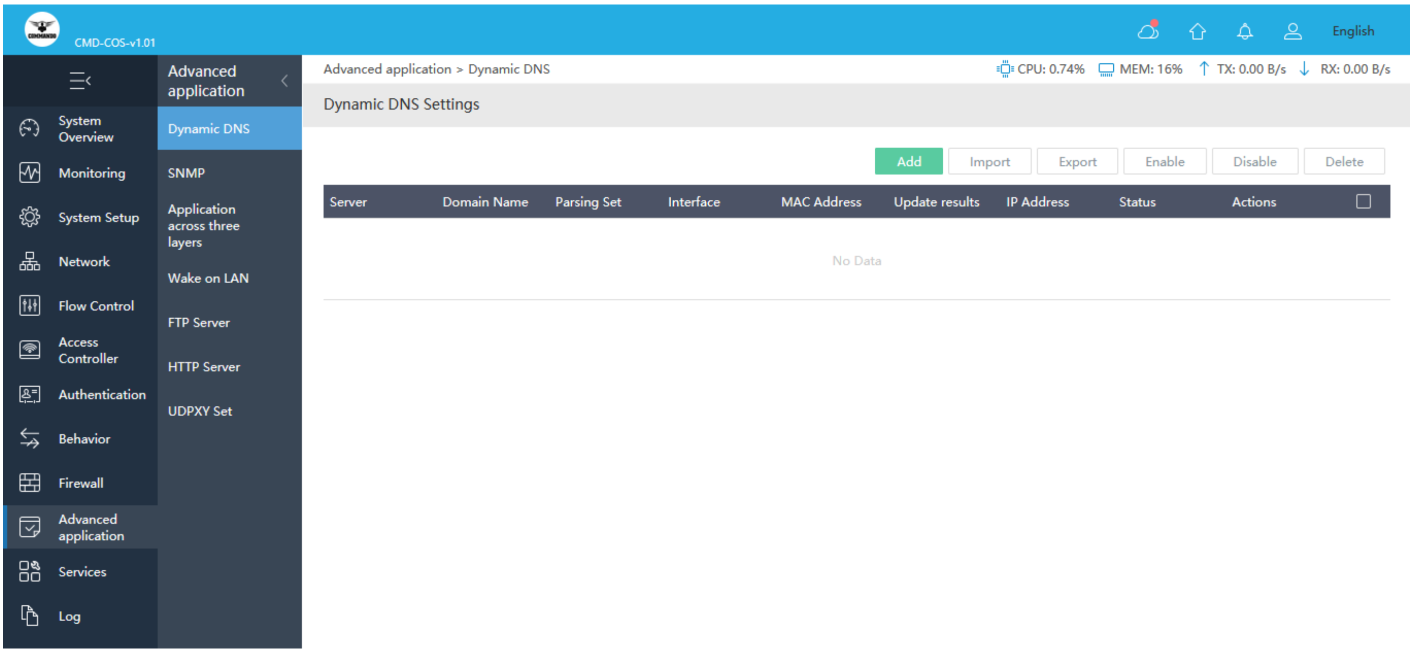
UDPXY is a UDP-to-HTTP multicast traffic relay daemon it forwards UDP traffic from a given multicast subscription to the requesting HTTP client. UDPXY listens (on a dedicated address/port) for HTTP requests issued by clients.

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.

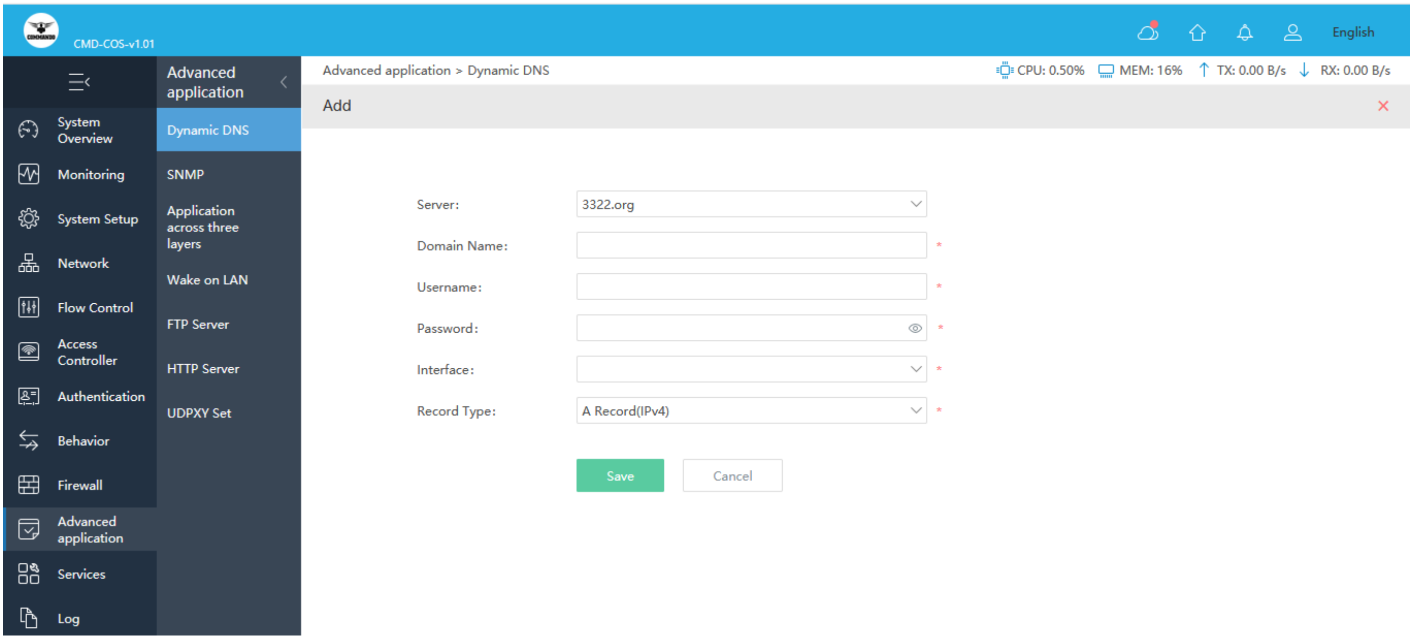
To configure Dynamic DNS Settings, Click on Advanced application > Dynamic DNS



Dynamic DNS Settings

Server	Domain Name	Parsing Set	Interface	MAC Address	Update results	IP Address	Status	Actions	□
				No Data					

Fig 9.1.1 Default Dynamic DNS Settings page



Server: 3322.org

Domain Name: *

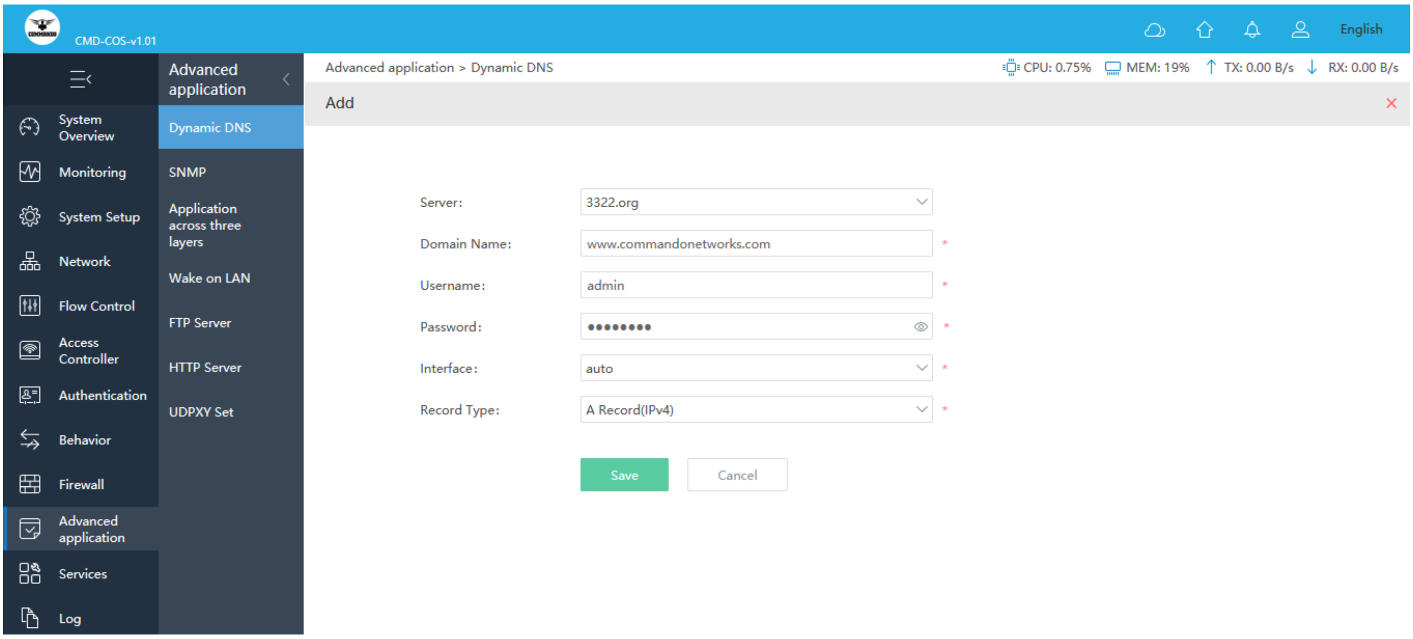
Username: *

Password: *

Interface: *

Record Type: A Record(IPv4) *

Fig 9.1.2 Add Dynamic DNS Settings page



Server: 3322.org

Domain Name: www.commandonetworks.com *

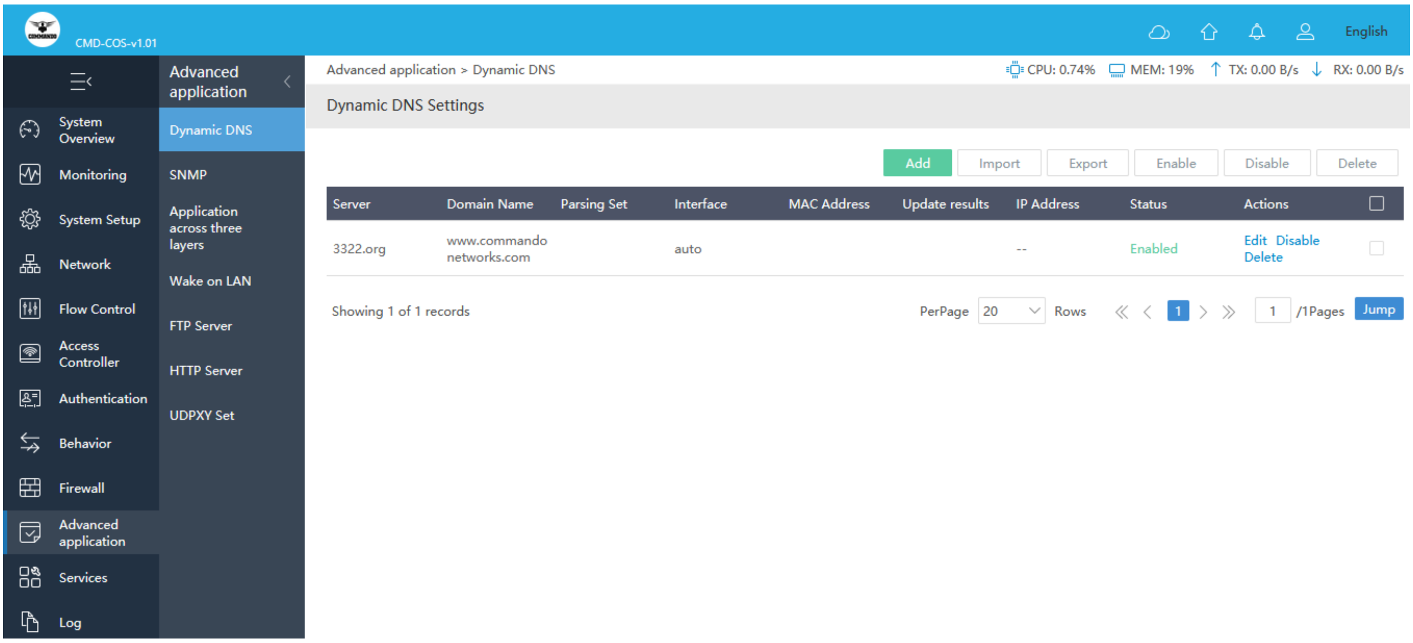
Username: admin *

Password: •••••••• *

Interface: auto *

Record Type: A Record(IPv4) *

Fig 9.1.3 Add Particular Dynamic DNS Settings page



Advanced application > Dynamic DNS

Dynamic DNS Settings

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

Showing 1 of 1 records

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

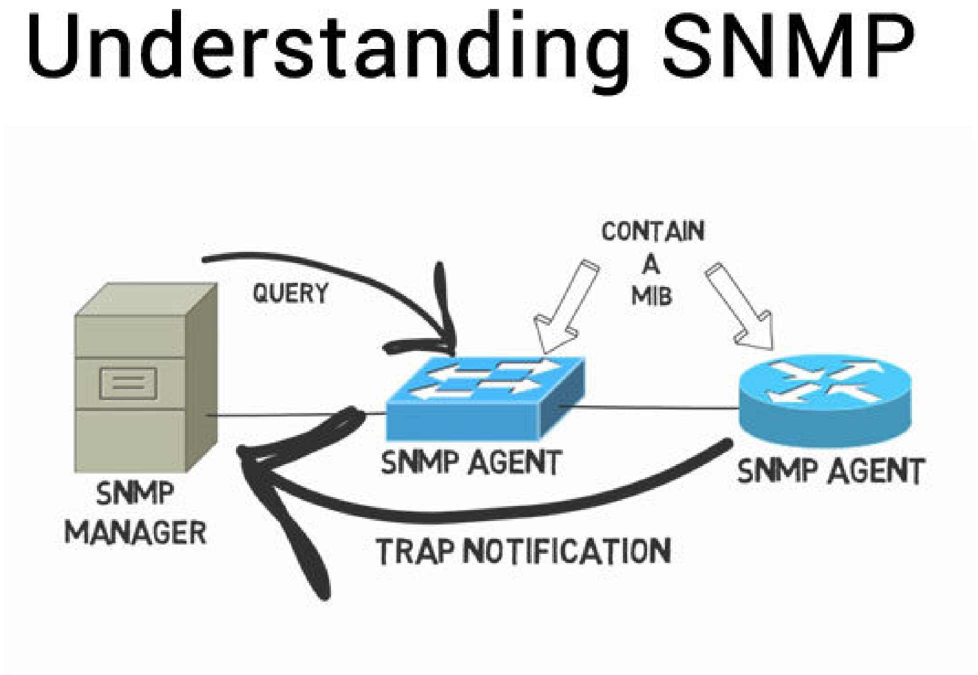


Fig 9.2.1 SNMP Community concept

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.

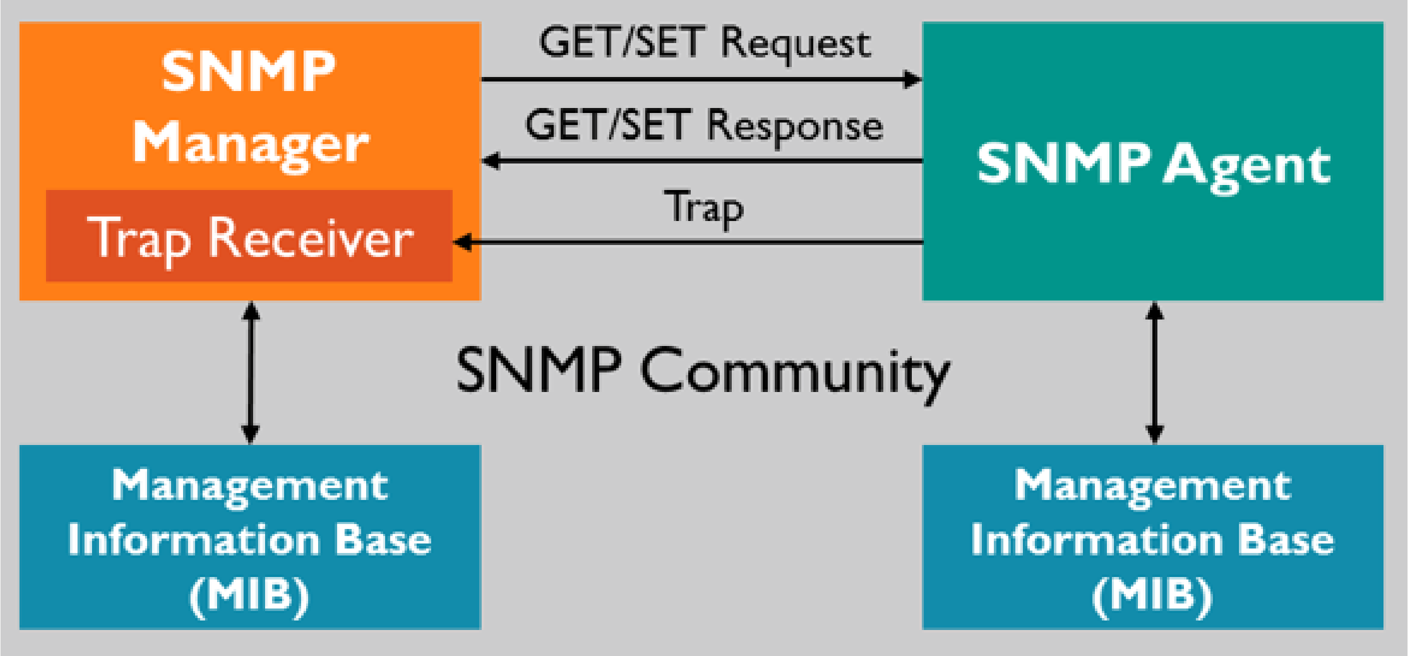
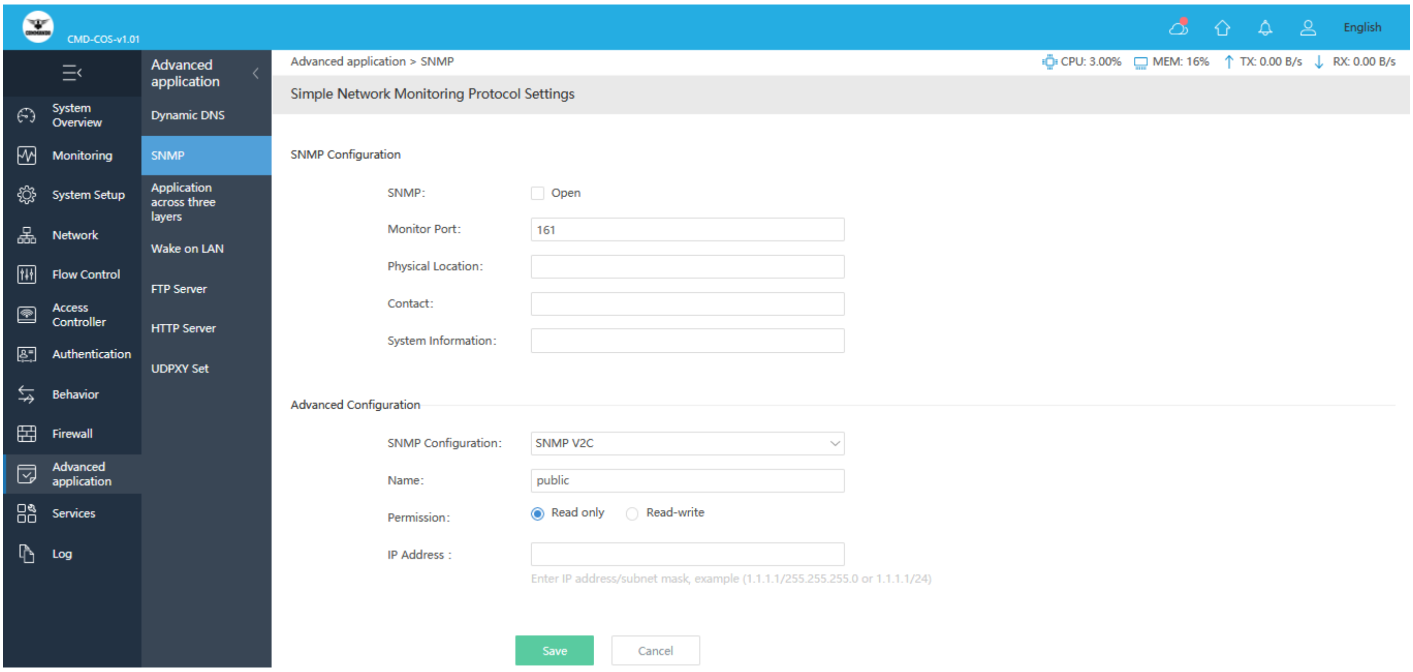


Fig 9.2.2 SNMP Community concept

How to enable Simple Network Monitoring Protocol?

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



Advanced application > SNMP

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

Simple Network Monitoring Protocol Settings

SNMP Configuration

SNMP: □ Open

Monitor Port: 161

Physical Location:

Contact:

System Information:

Advanced Configuration

SNMP Configuration: SNMP V2C

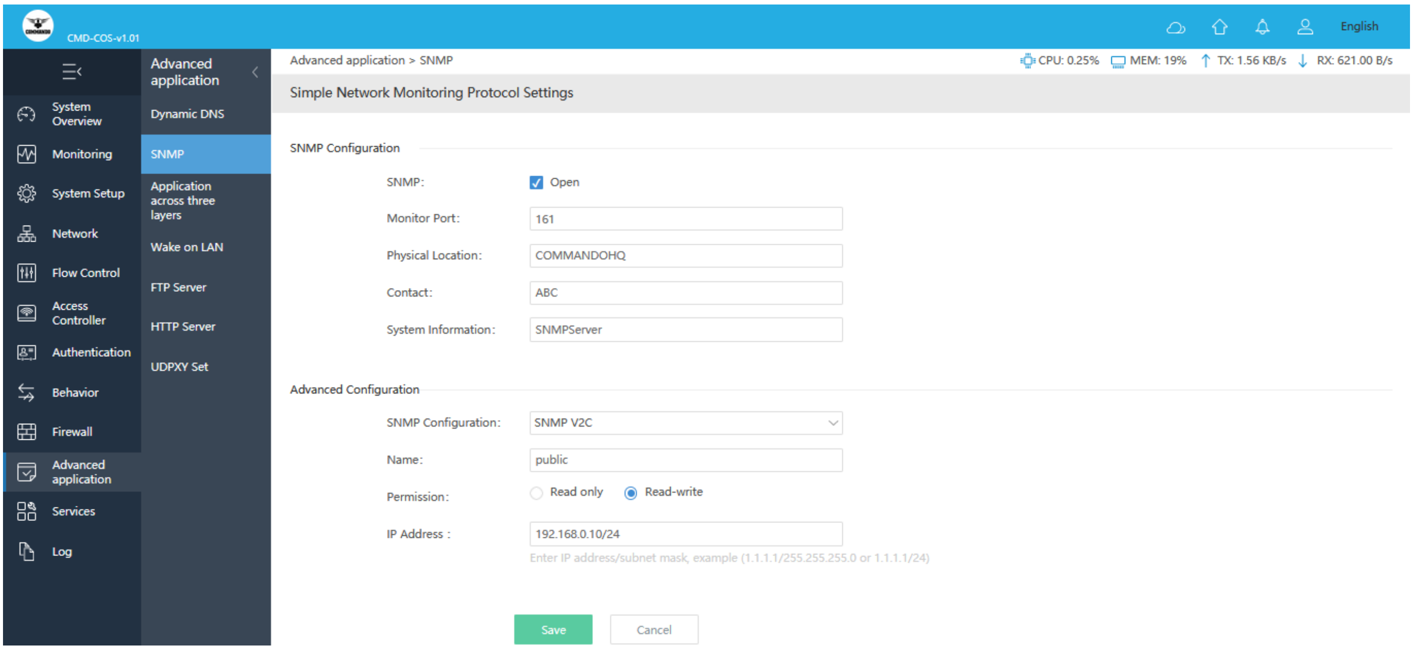
Name: public

Permission: ● Read only ○ Read-write

IP Address :

Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)

Fig 9.2.3 Default Simple Network Monitoring Protocol Settings page



Advanced application > SNMP

CPU: 0.25% MEM: 19% TX: 1.56 KB/s RX: 621.00 B/s

Simple Network Monitoring Protocol Settings

SNMP Configuration

SNMP: ☑ Open

Monitor Port: 161

Physical Location: COMMANDOHQ

Contact: ABC

System Information: SNMPServer

Advanced Configuration

SNMP Configuration: SNMP V2C

Name: public

Permission: ○ Read only ● Read-write

IP Address : 192.168.0.10/24

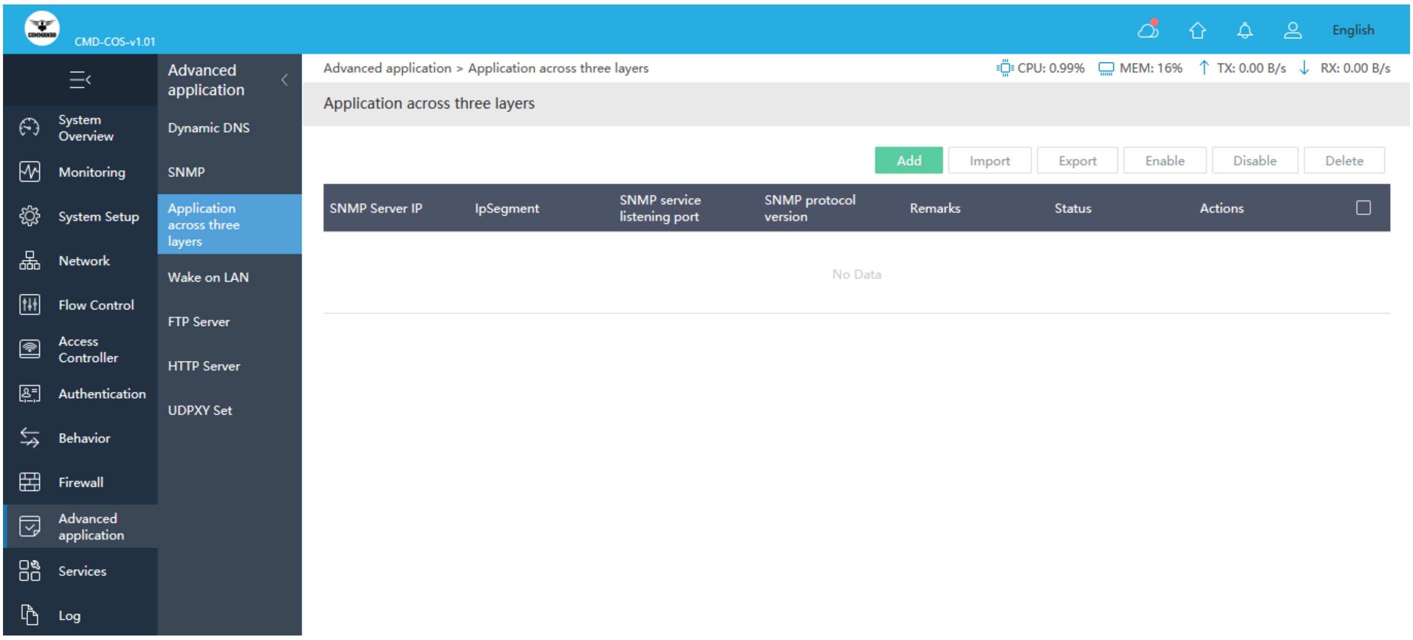
Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)

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



Advanced application > Application across three layers

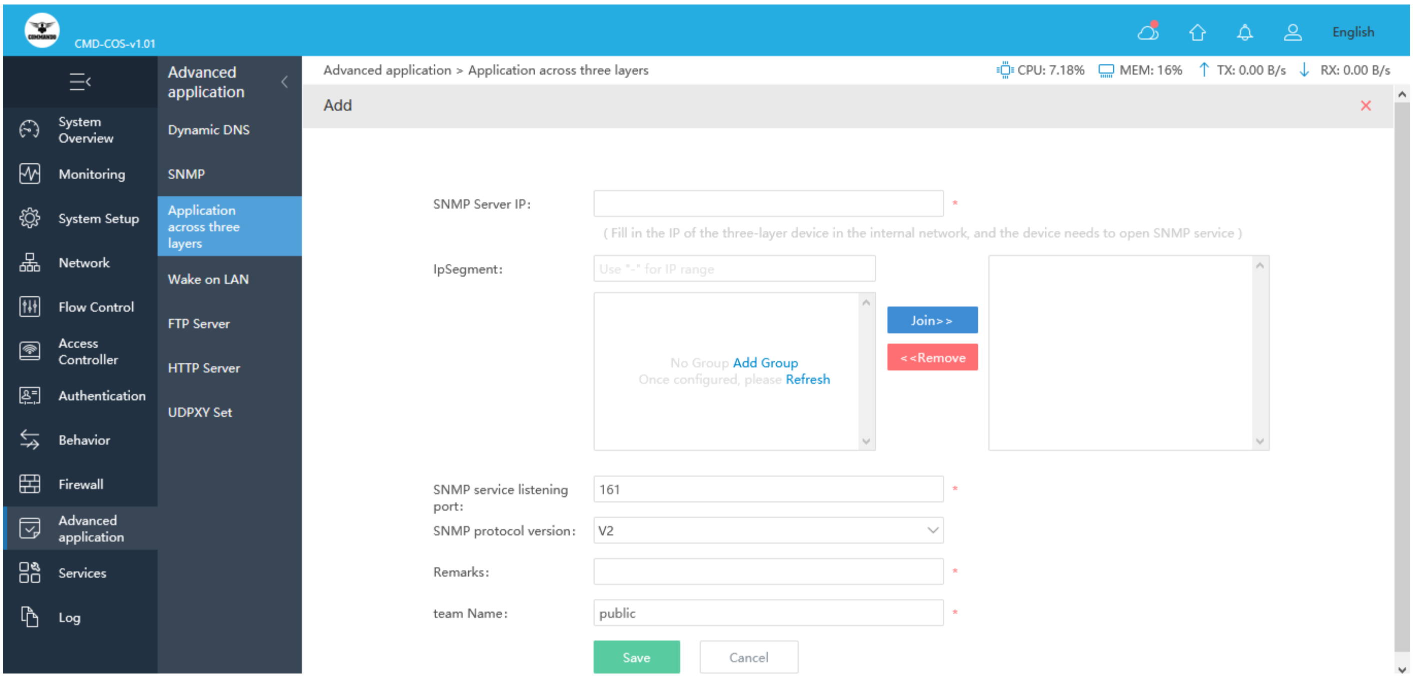
CPU: 0.99% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Application across three layers

SNMP Server IP	IpSegment	SNMP service listening port	SNMP protocol version	Remarks	Status	Actions	□

No Data

Fig 9.3.1 Default Application across three layers page



Advanced application > Application across three layers

CPU: 7.18% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

SNMP Server IP: *

(Fill in the IP of the three-layer device in the internal network, and the device needs to open SNMP service)

IpSegment: Use "-" for IP range

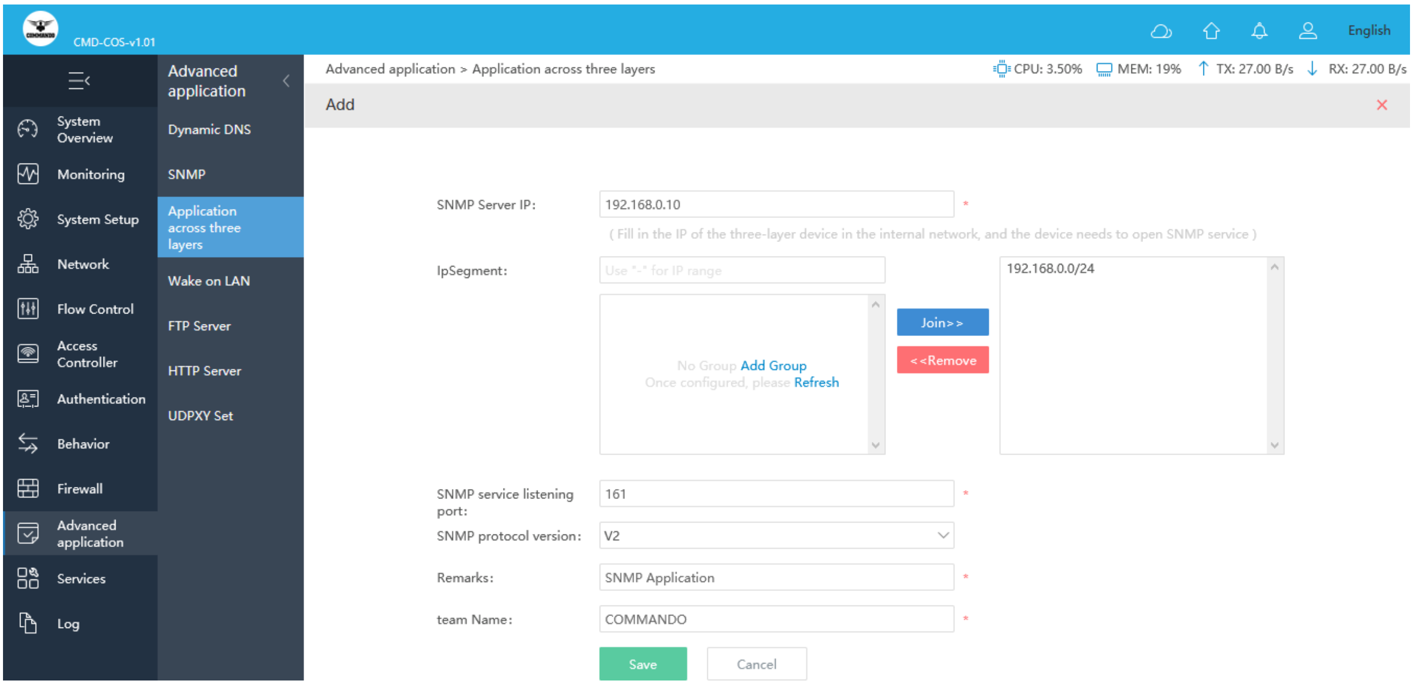
SNMP service listening port: 161 *

SNMP protocol version: V2

Remarks: *

team Name: public *

Fig 9.3.2 Add Application across three layers page



Advanced application > Application across three layers

CPU: 3.50% MEM: 19% TX: 27.00 B/s RX: 27.00 B/s

SNMP Server IP: 192.168.0.10 *

(Fill in the IP of the three-layer device in the internal network, and the device needs to open SNMP service)

IpSegment: Use "-" for IP range

192.168.0.0/24

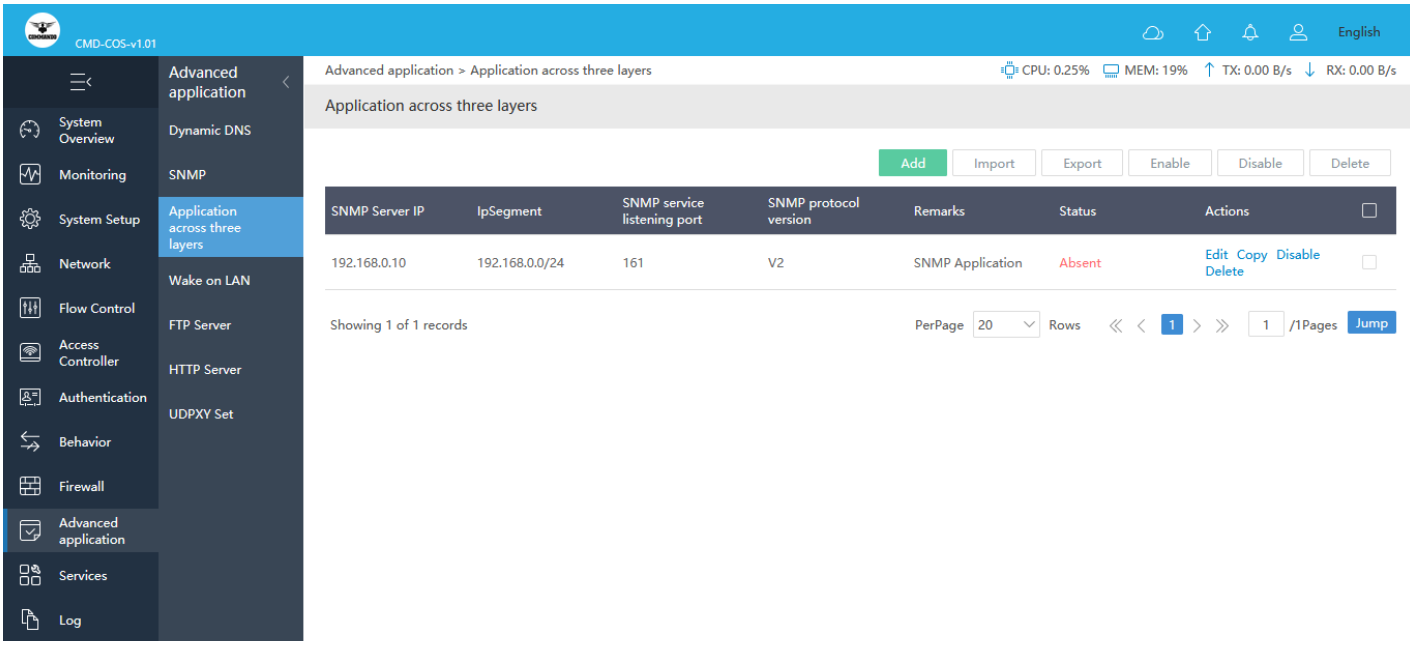
SNMP service listening port: 161 *

SNMP protocol version: V2

Remarks: SNMP Application *

team Name: COMMANDO *

Fig 9.3.3 Application across three layers for particular SNMP server page



Advanced application > Application across three layers

Application across three layers

SNMP Server IP	IpSegment	SNMP service listening port	SNMP protocol version	Remarks	Status	Actions	□
192.168.0.10	192.168.0.0/24	161	V2	SNMP Application	Absent	Edit Copy Disable Delete	□

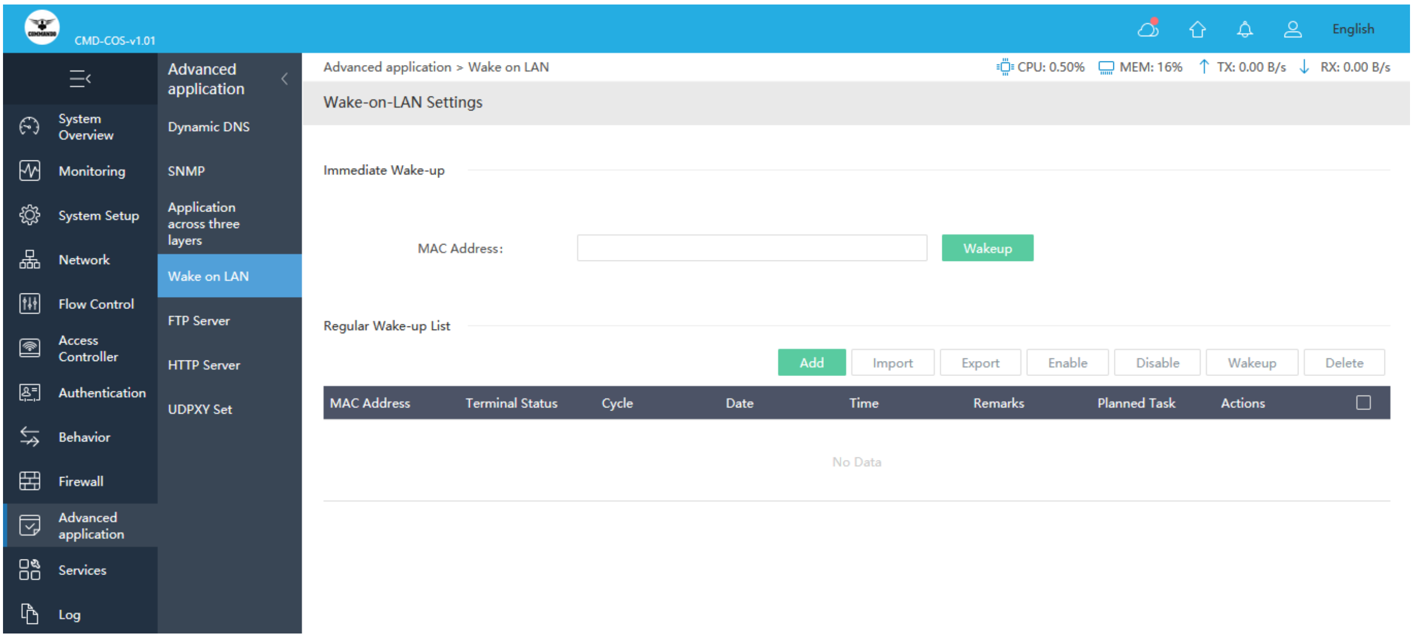
Showing 1 of 1 records

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



Wake-on-LAN Settings

Immediate Wake-up

MAC Address: Wakeup

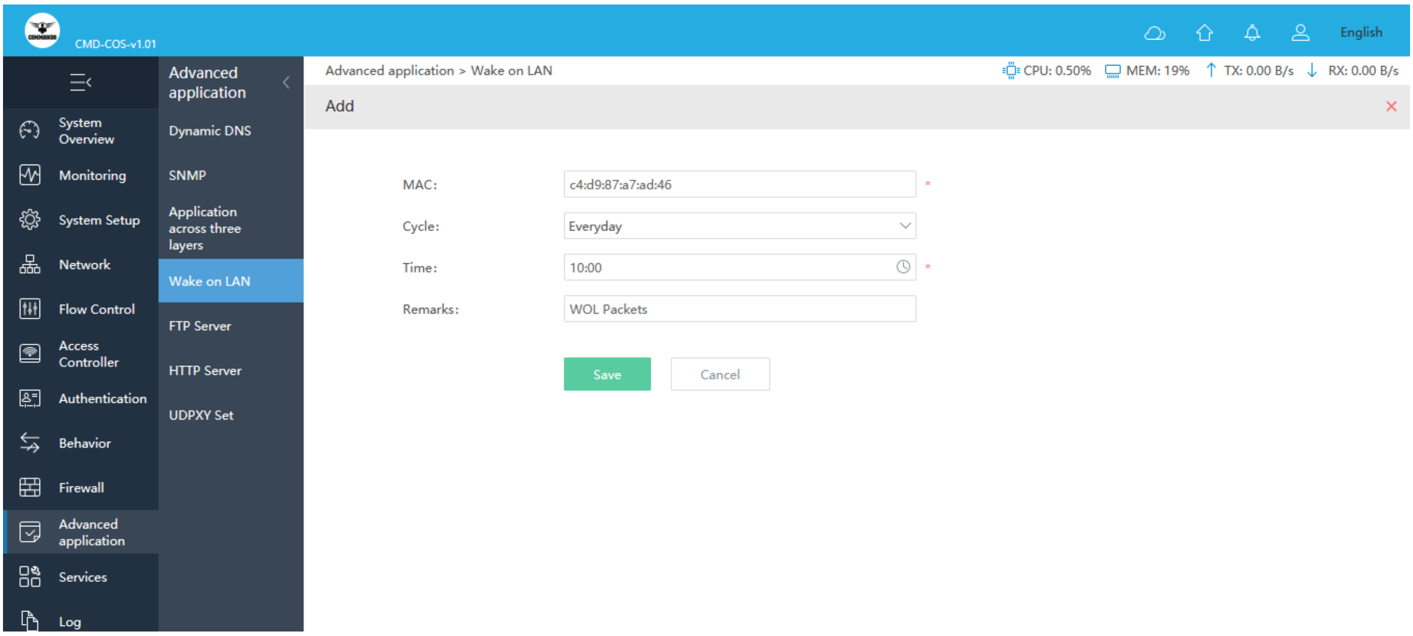
Regular Wake-up List

Add Import Export Enable Disable Wakeup Delete

MAC Address	Terminal Status	Cycle	Date	Time	Remarks	Planned Task	Actions	□

No Data

Fig 9.4.1 Default Wake-on-LAN Settings page



Add

MAC: c4:d9:87:a7:ad:46 *

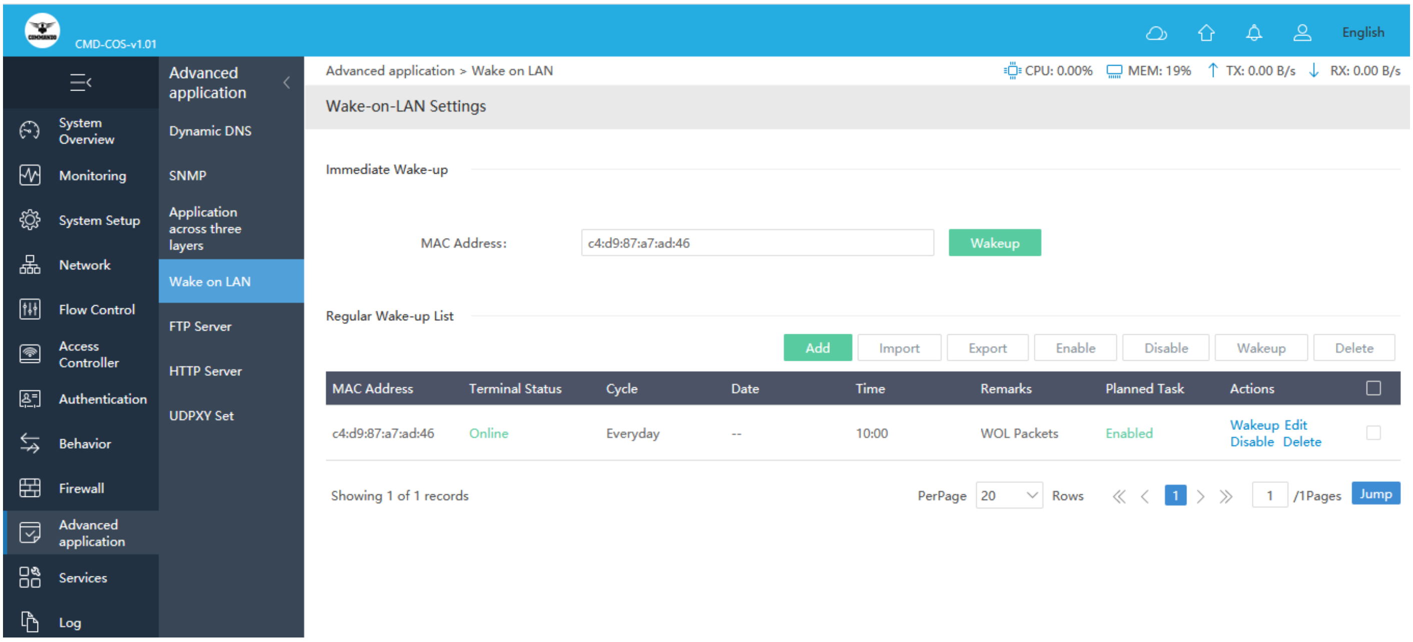
Cycle: Everyday

Time: 10:00 *

Remarks: WOL Packets

Save Cancel

Fig 9.4.2 Add Wake-on-LAN Settings page



Advanced application > Wake on LAN

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

Wake-on-LAN Settings

Immediate Wake-up

MAC Address: c4:d9:87:a7:ad:46

Regular Wake-up List

MAC Address	Terminal Status	Cycle	Date	Time	Remarks	Planned Task	Actions	□
c4:d9:87:a7:ad:46	Online	Everyday	--	10:00	WOL Packets	Enabled	Wakeup Edit Disable Delete	□

Showing 1 of 1 records

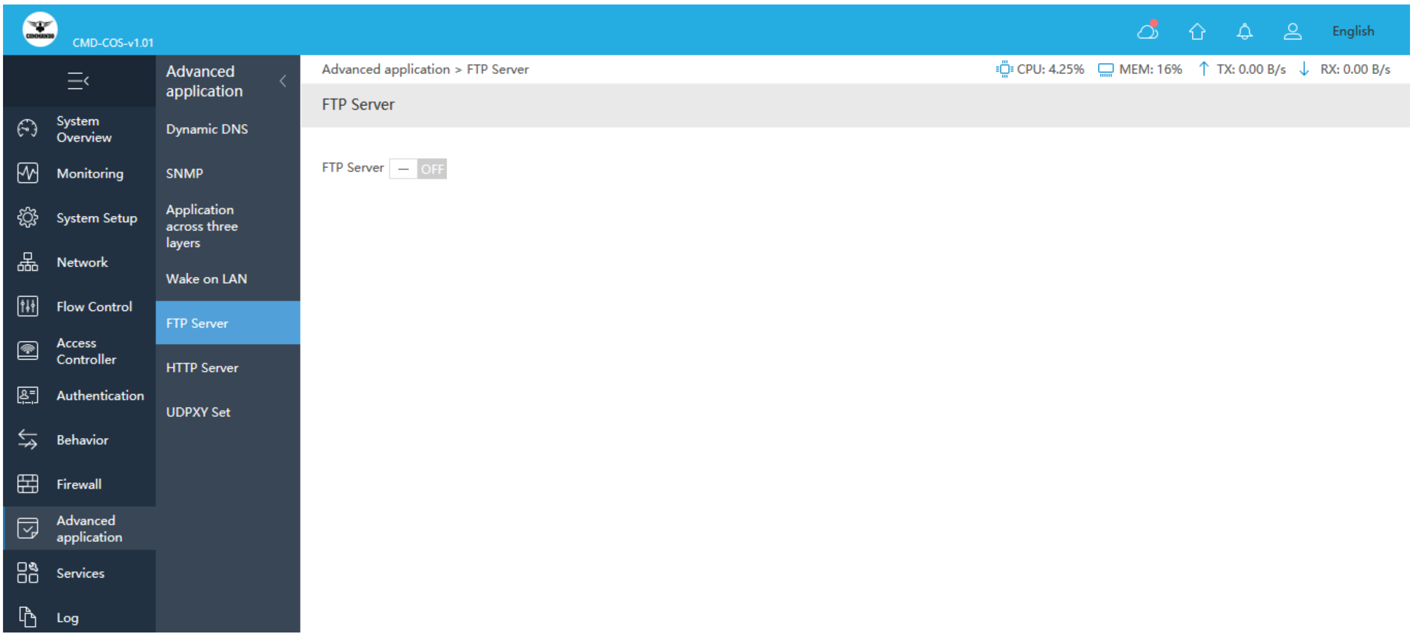
PerPage 20 Rows « ‹ 1 › » 1 /1Pages

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



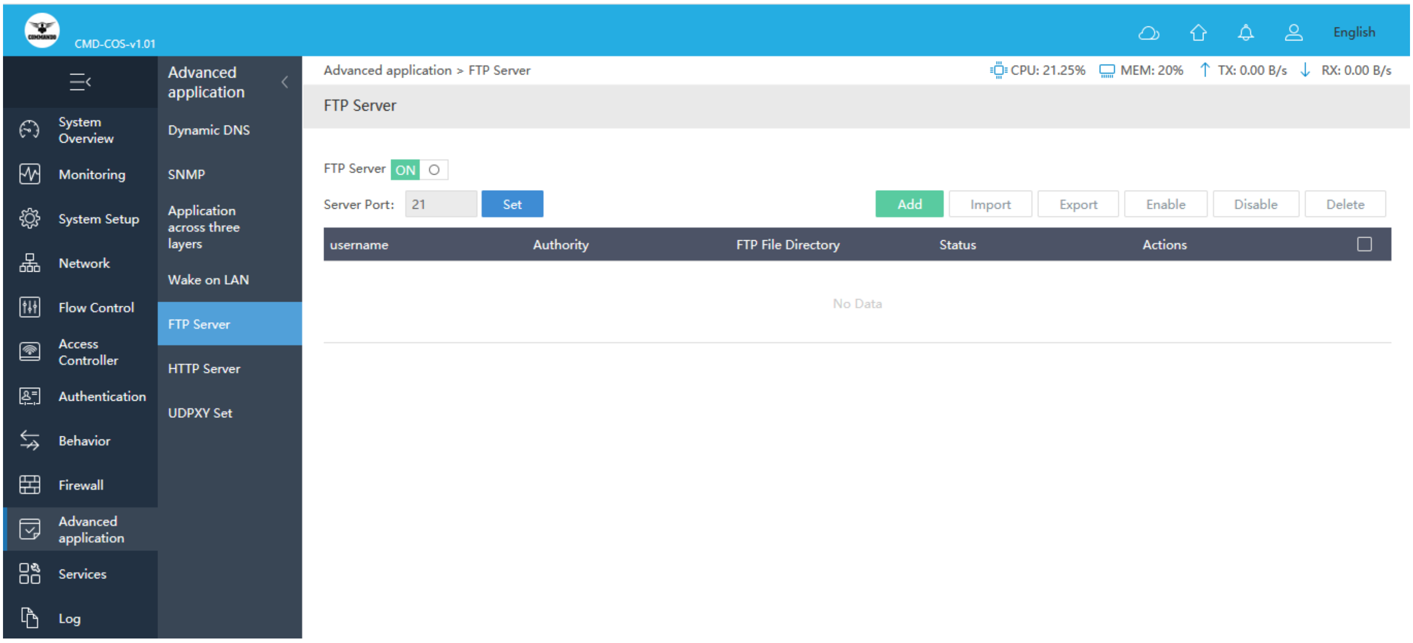
Advanced application > FTP Server

CPU: 4.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

FTP Server

FTP Server — OFF

Fig 9.5.1 Default FTP Server page



Advanced application > FTP Server

CPU: 21.25% MEM: 20% TX: 0.00 B/s RX: 0.00 B/s

FTP Server

FTP Server ON

Server Port: 21

username	Authority	FTP File Directory	Status	Actions	□

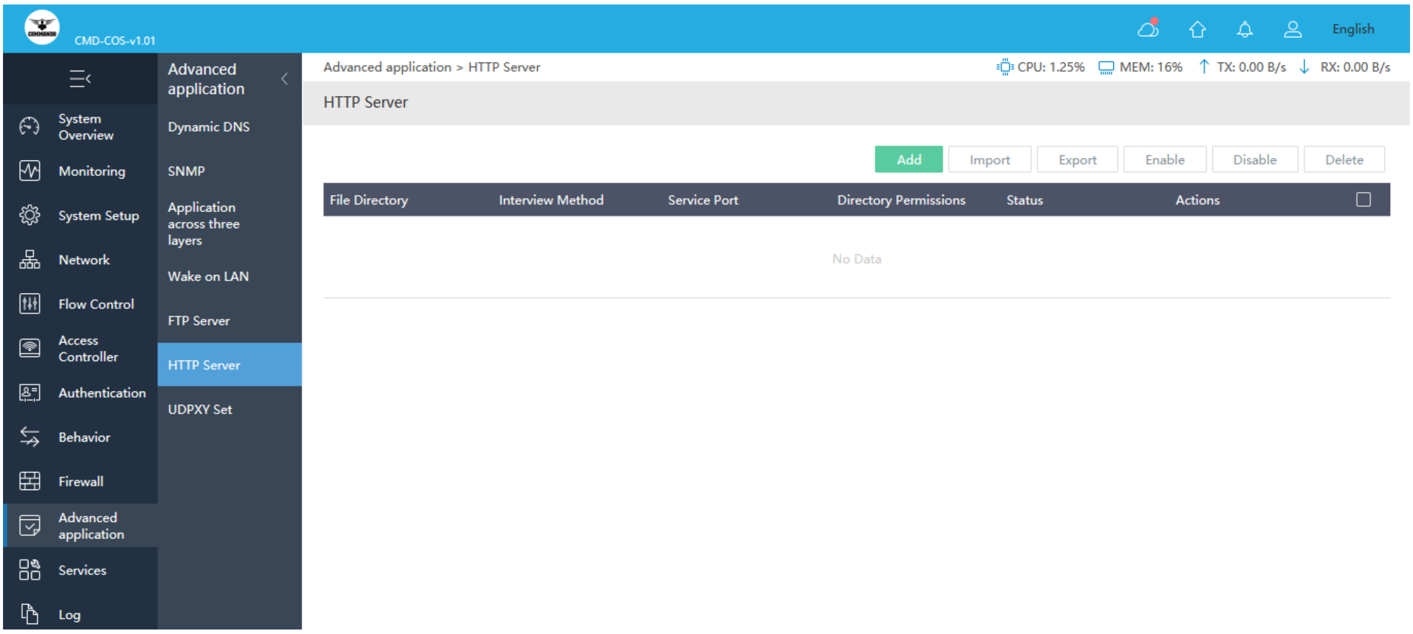
No Data

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



Advanced application > HTTP Server

CPU: 1.25% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

HTTP Server

File Directory	Interview Method	Service Port	Directory Permissions	Status	Actions	□

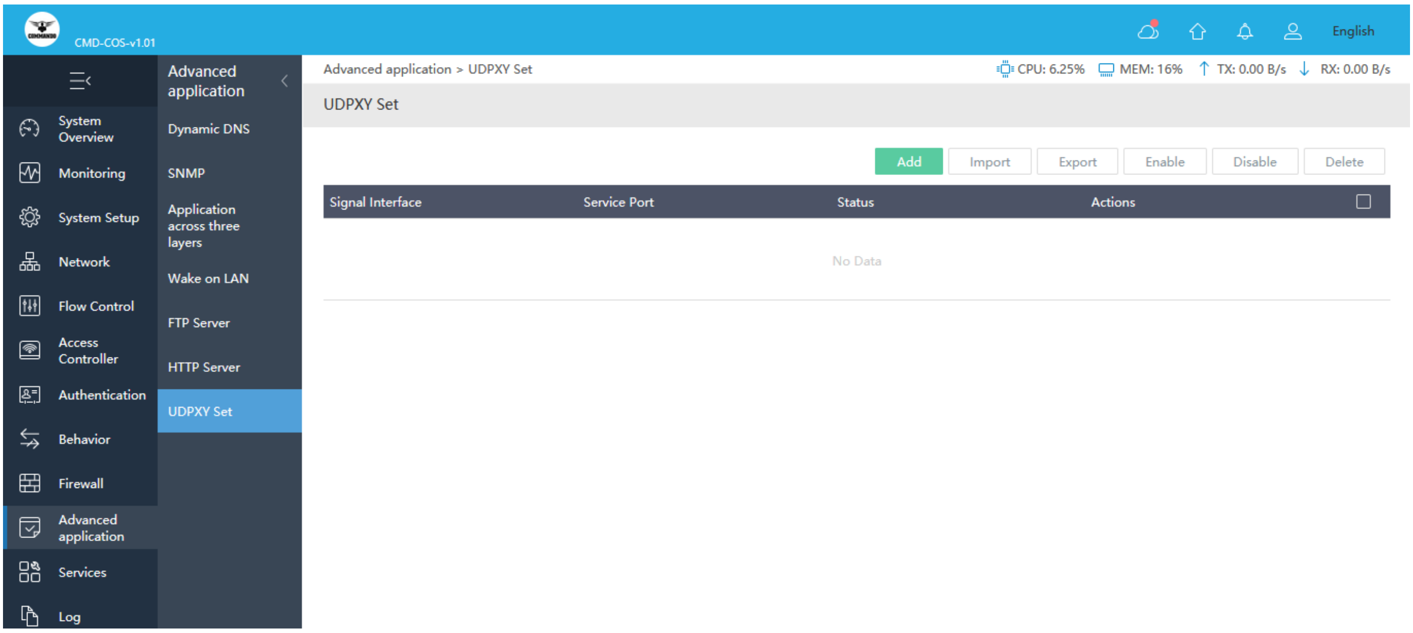
No Data

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

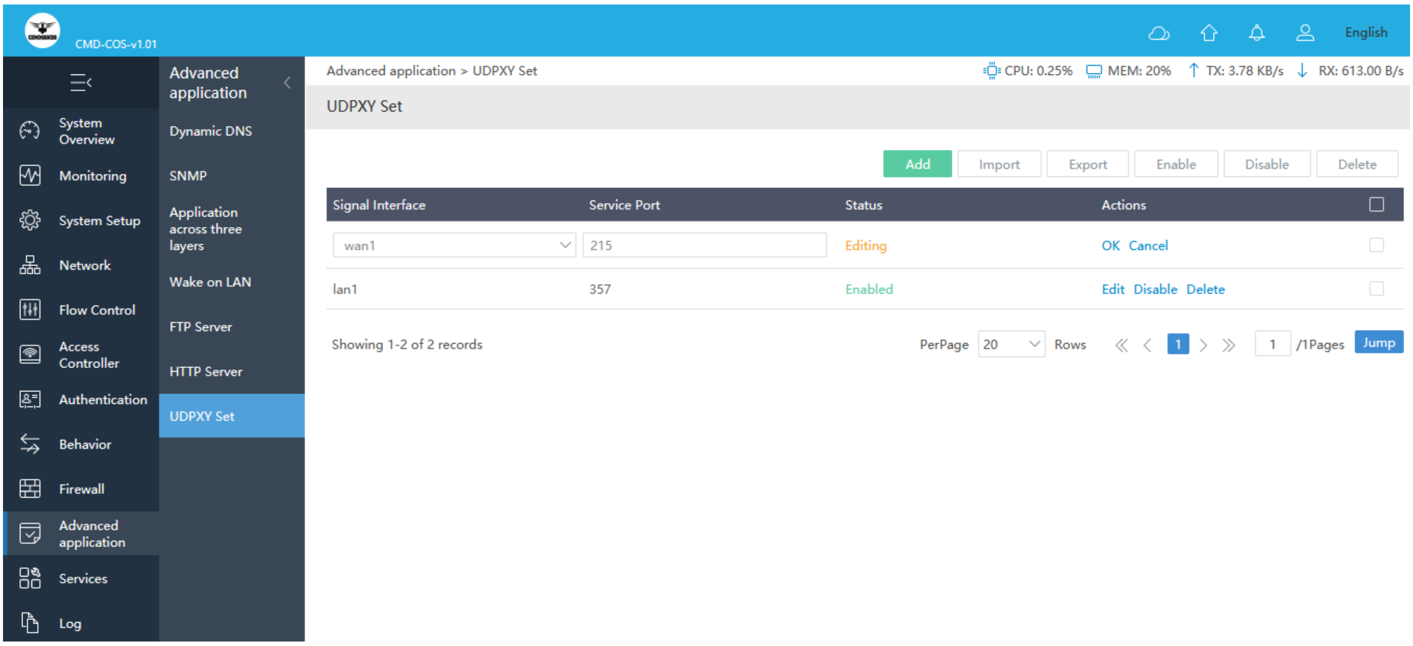


UDPXY Set

Signal Interface	Service Port	Status	Actions	□

No Data

Fig 9.7.1 Default UDPXY Set page



UDPXY Set

Signal Interface	Service Port	Status	Actions	□
wan1	215	Editing	OK Cancel	□
lan1	357	Enabled	Edit Disable Delete	□

Showing 1-2 of 2 records PerPage 20 Rows « ‹ 1 › » 1 /1Pages Jump

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:

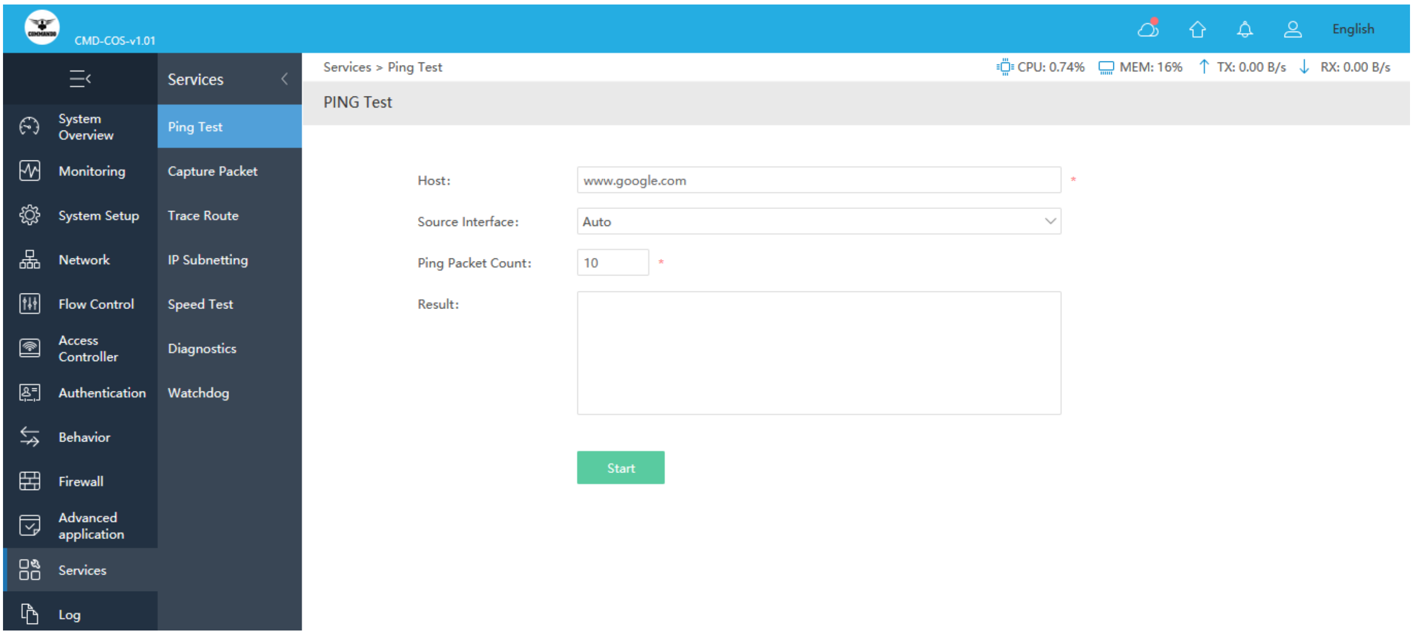
Health Watchdog for physical hardware Active health detection.

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



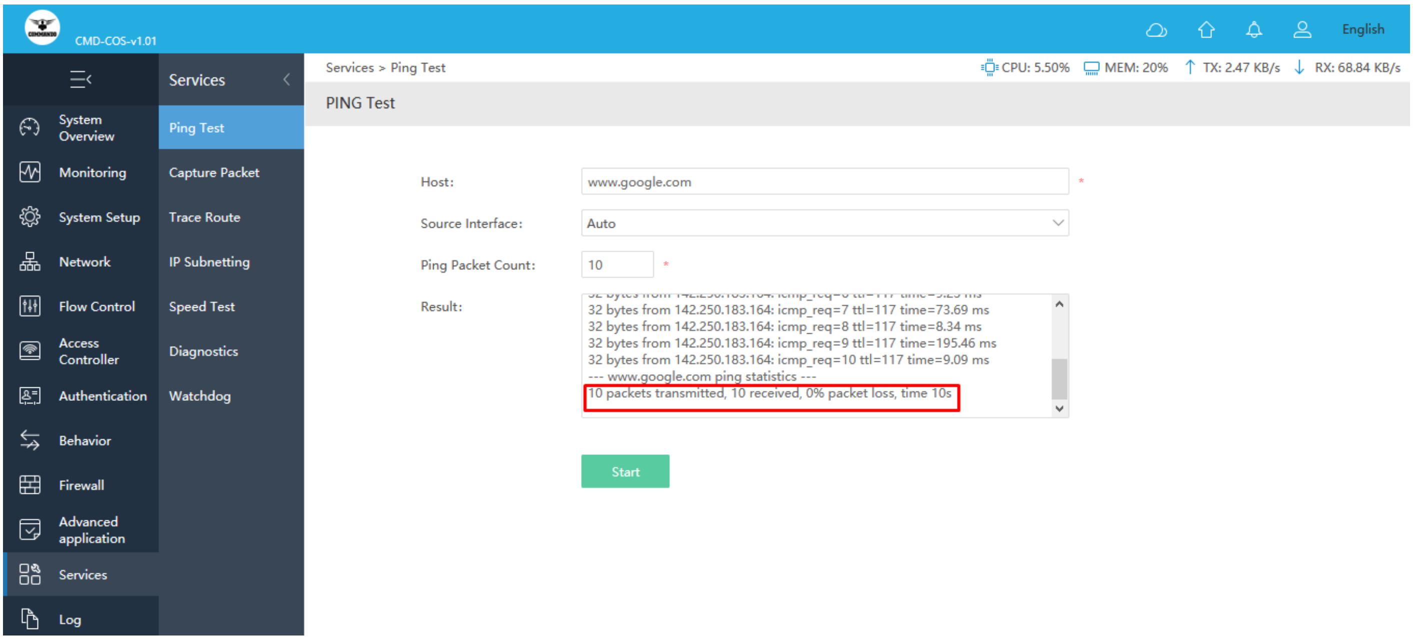
Host: www.google.com *

Source Interface: Auto

Ping Packet Count: 10 *

Result:

Fig 10.1.1 Default PING Test page



Host: www.google.com *

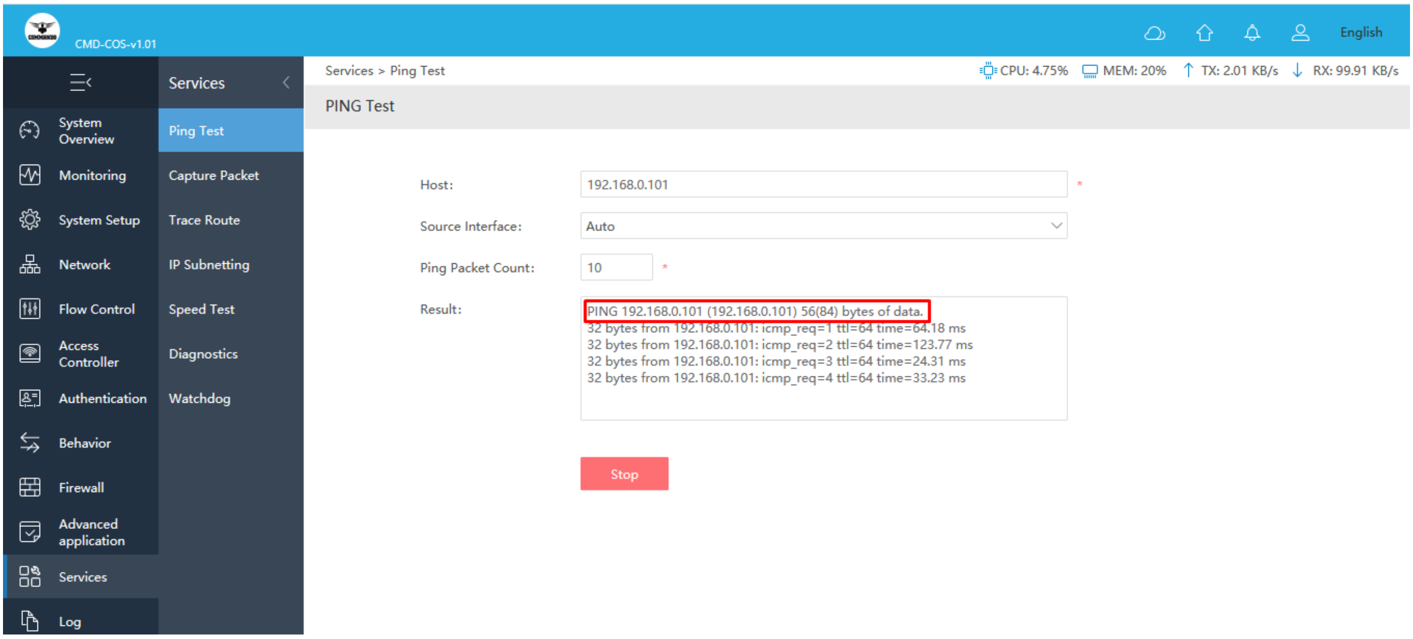
Source Interface: Auto

Ping Packet Count: 10 *

Result:

```
32 bytes from 142.250.183.164: icmp_req=6 ttl=117 time=9.25 ms
32 bytes from 142.250.183.164: icmp_req=7 ttl=117 time=73.69 ms
32 bytes from 142.250.183.164: icmp_req=8 ttl=117 time=8.34 ms
32 bytes from 142.250.183.164: icmp_req=9 ttl=117 time=195.46 ms
32 bytes from 142.250.183.164: icmp_req=10 ttl=117 time=9.09 ms
--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 10s
```

Fig 10.1.2 PING to particular website page



Host: 192.168.0.101 *

Source Interface: Auto

Ping Packet Count: 10 *

Result:

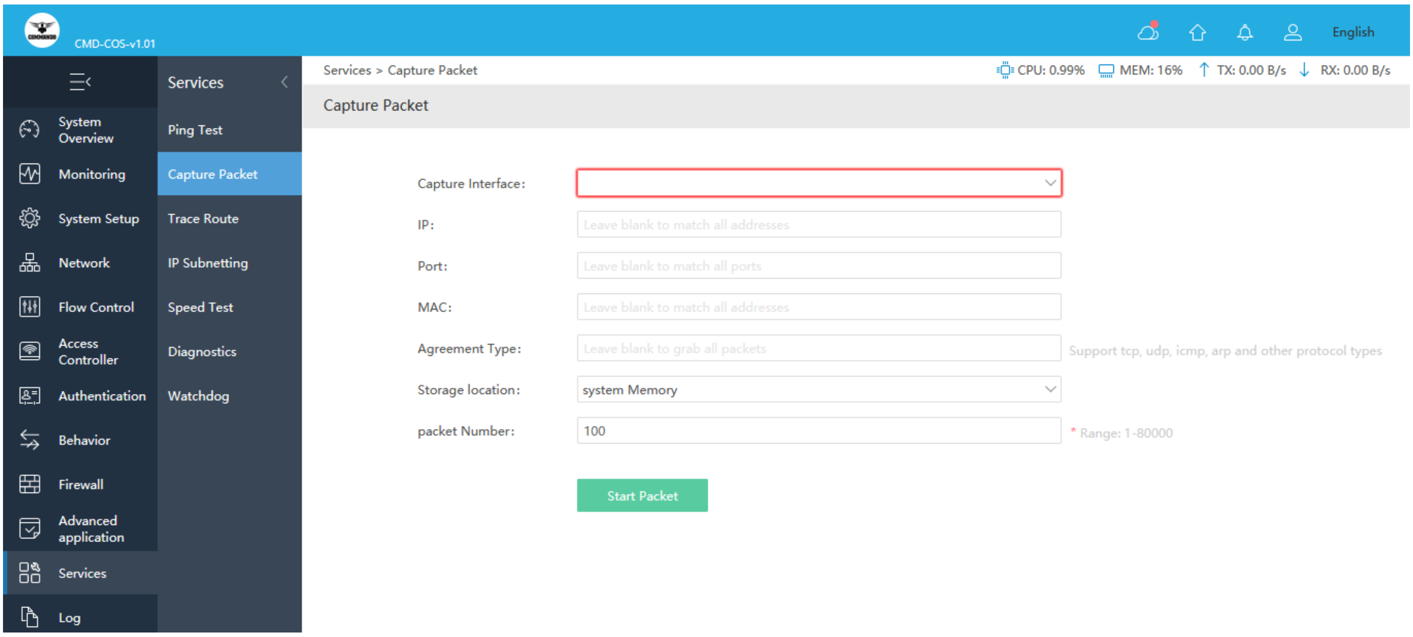
```
PING 192.168.0.101 (192.168.0.101) 56(84) bytes of data.
32 bytes from 192.168.0.101: icmp_req=1 ttl=64 time=64.18 ms
32 bytes from 192.168.0.101: icmp_req=2 ttl=64 time=123.77 ms
32 bytes from 192.168.0.101: icmp_req=3 ttl=64 time=24.31 ms
32 bytes from 192.168.0.101: icmp_req=4 ttl=64 time=33.23 ms
```

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



Capture Packet

Capture Interface:

IP: Leave blank to match all addresses

Port: Leave blank to match all ports

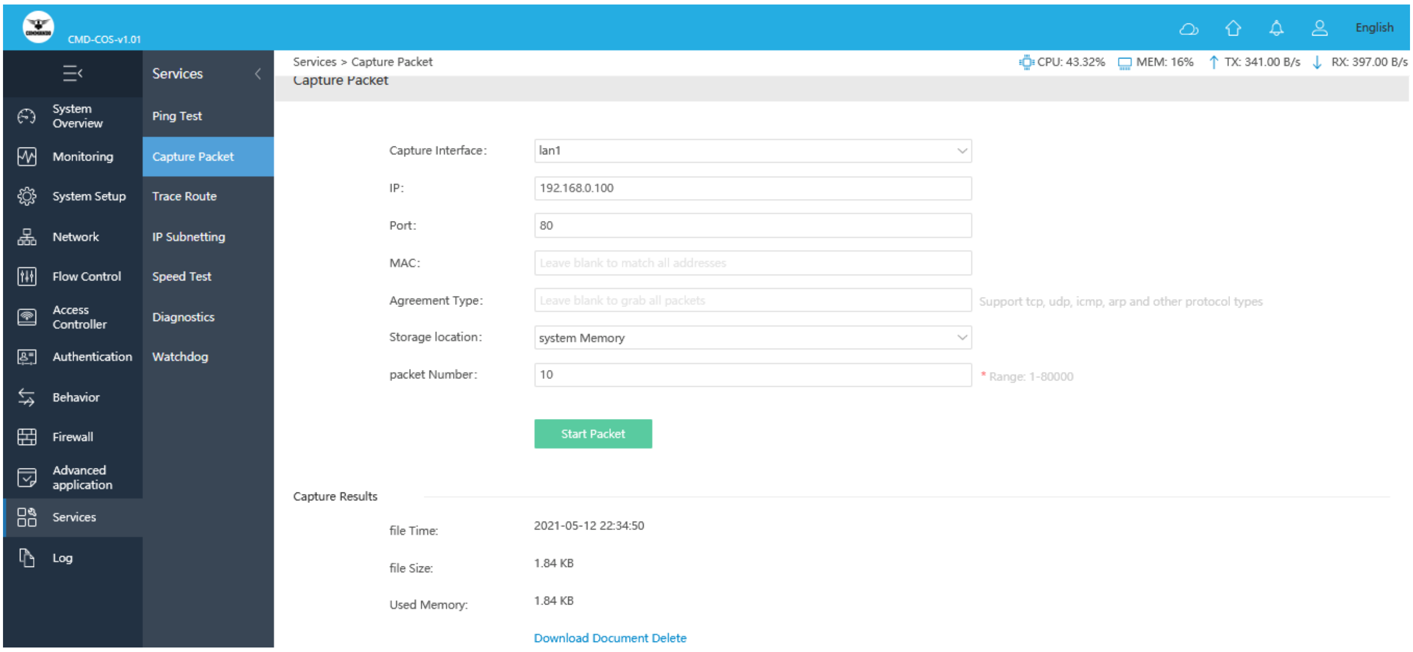
MAC: Leave blank to match all addresses

Agreement Type: Leave blank to grab all packets Support tcp, udp, icmp, arp and other protocol types

Storage location: system Memory

packet Number: 100 * Range: 1-80000

Fig 10.2.1 Default Capture Packet page



Capture Packet

Capture Interface: lan1

IP: 192.168.0.100

Port: 80

MAC: Leave blank to match all addresses

Agreement Type: Leave blank to grab all packets Support tcp, udp, icmp, arp and other protocol types

Storage location: system Memory

packet Number: 10 * Range: 1-80000

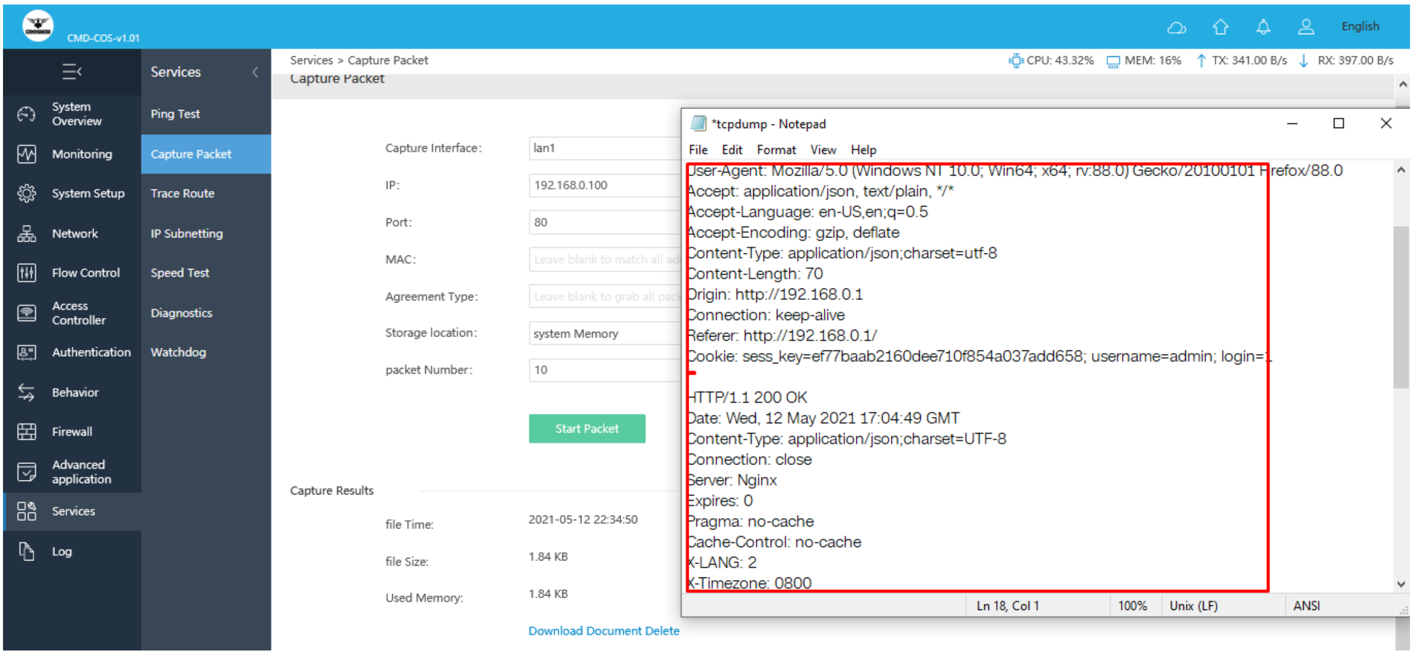
Capture Results

file Time: 2021-05-12 22:34:50

file Size: 1.84 KB

Used Memory: 1.84 KB

Fig 10.2.2 Capture Packet result page



Capture Interface: lan1

IP: 192.168.0.100

Port: 80

MAC: Leave blank to match all ad

Agreement Type: Leave blank to grab all pac

Storage location: system Memory

packet Number: 10

Start Packet

Capture Results

file Time: 2021-05-12 22:34:50

file Size: 1.84 KB

Used Memory: 1.84 KB

Download Document Delete

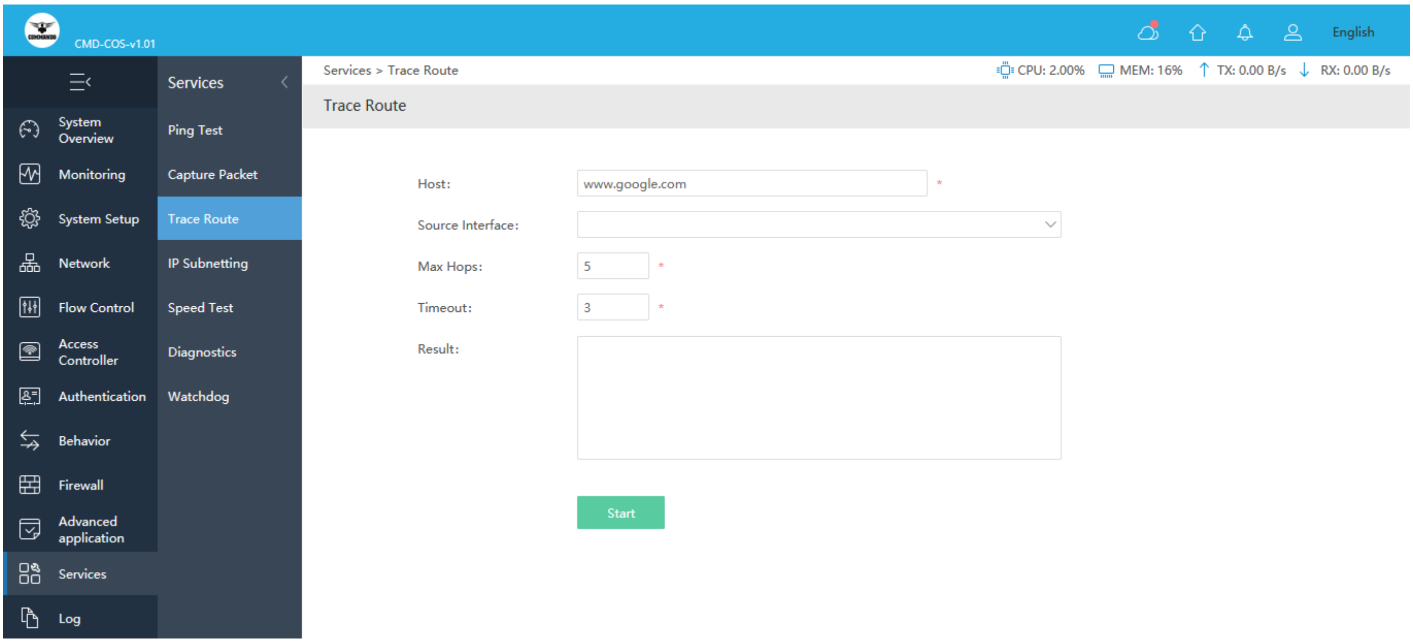
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 70
Origin: http://192.168.0.1
Connection: keep-alive
Referer: http://192.168.0.1/
Cookie: sess_key=ef77baab2160dee710f854a037add658; username=admin; login=1

HTTP/1.1 200 OK
Date: Wed, 12 May 2021 17:04:49 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Server: Nginx
Expires: 0
Pragma: no-cache
Cache-Control: no-cache
X-LANG: 2
X-Timezone: 0800
```

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



Services > Trace Route

CPU: 2.00% MEM: 16% TX: 0.00 B/s RX: 0.00 B/s

Trace Route

Host: www.google.com *

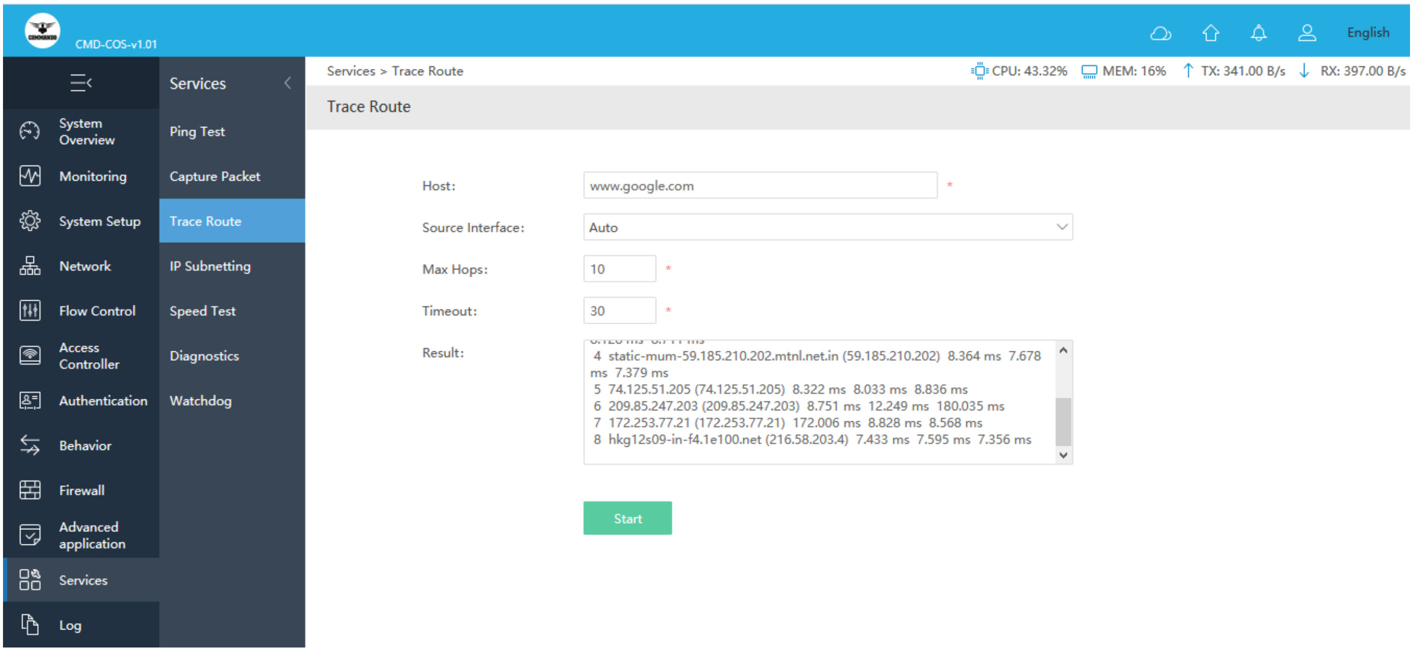
Source Interface:

Max Hops: 5 *

Timeout: 3 *

Result:

Fig 10.3.1 Default Trace Route page



Services > Trace Route

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

Trace Route

Host: www.google.com *

Source Interface: Auto

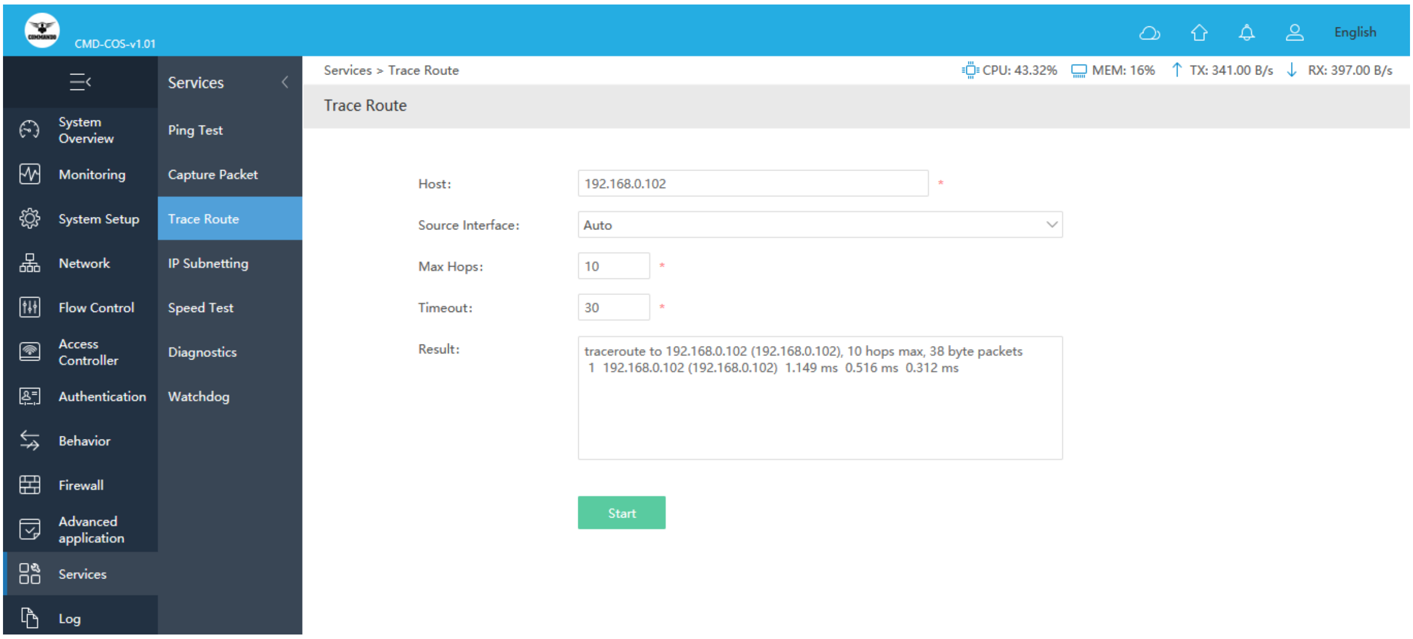
Max Hops: 10 *

Timeout: 30 *

Result:

```
 4  static-mum-59.185.210.202.mtnl.net.in (59.185.210.202)  8.364 ms  7.678
ms  7.379 ms
 5  74.125.51.205 (74.125.51.205)  8.322 ms  8.033 ms  8.836 ms
 6  209.85.247.203 (209.85.247.203)  8.751 ms  12.249 ms  180.035 ms
 7  172.253.77.21 (172.253.77.21)  172.006 ms  8.828 ms  8.568 ms
 8  hkg12s09-in-f4.1e100.net (216.58.203.4)  7.433 ms  7.595 ms  7.356 ms
```

Fig 10.3.2 Trace Route particular website page



Host: 192.168.0.102 *

Source Interface: Auto

Max Hops: 10 *

Timeout: 30 *

Result:

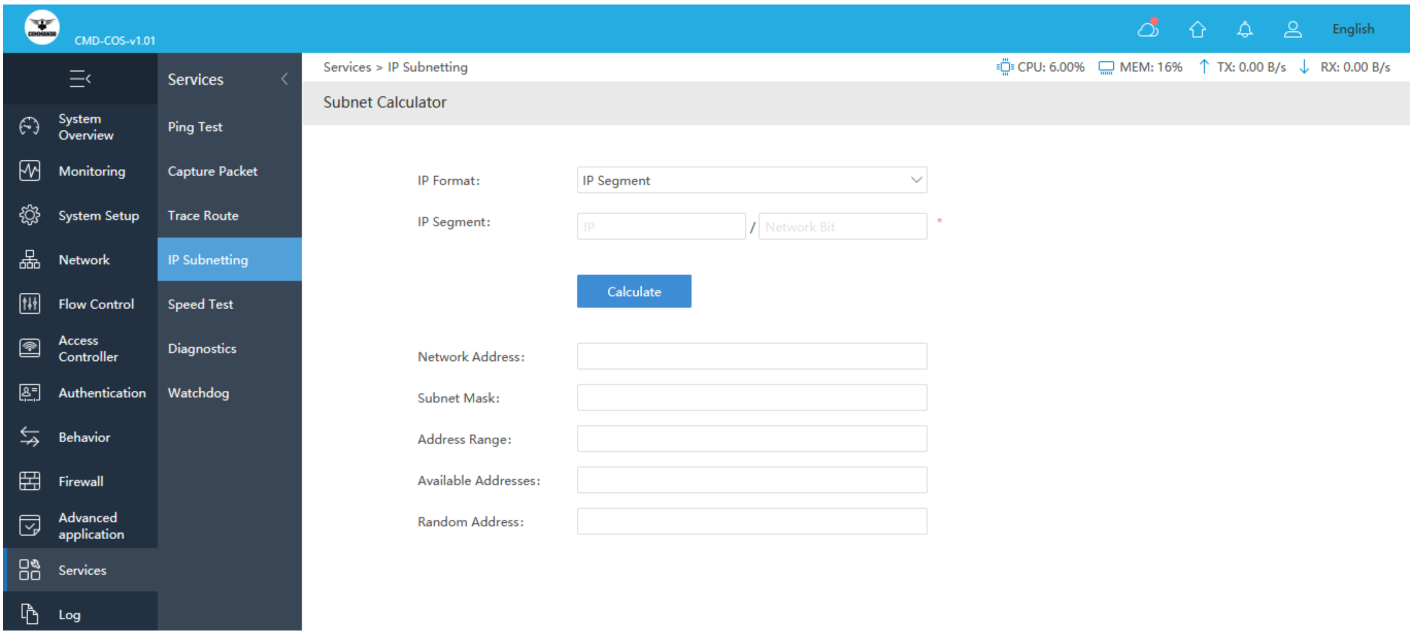
```
traceroute to 192.168.0.102 (192.168.0.102), 10 hops max, 38 byte packets
 1  192.168.0.102 (192.168.0.102)  1.149 ms  0.516 ms  0.312 ms
```

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



IP Format: IP Segment

IP Segment: /

Network Address:

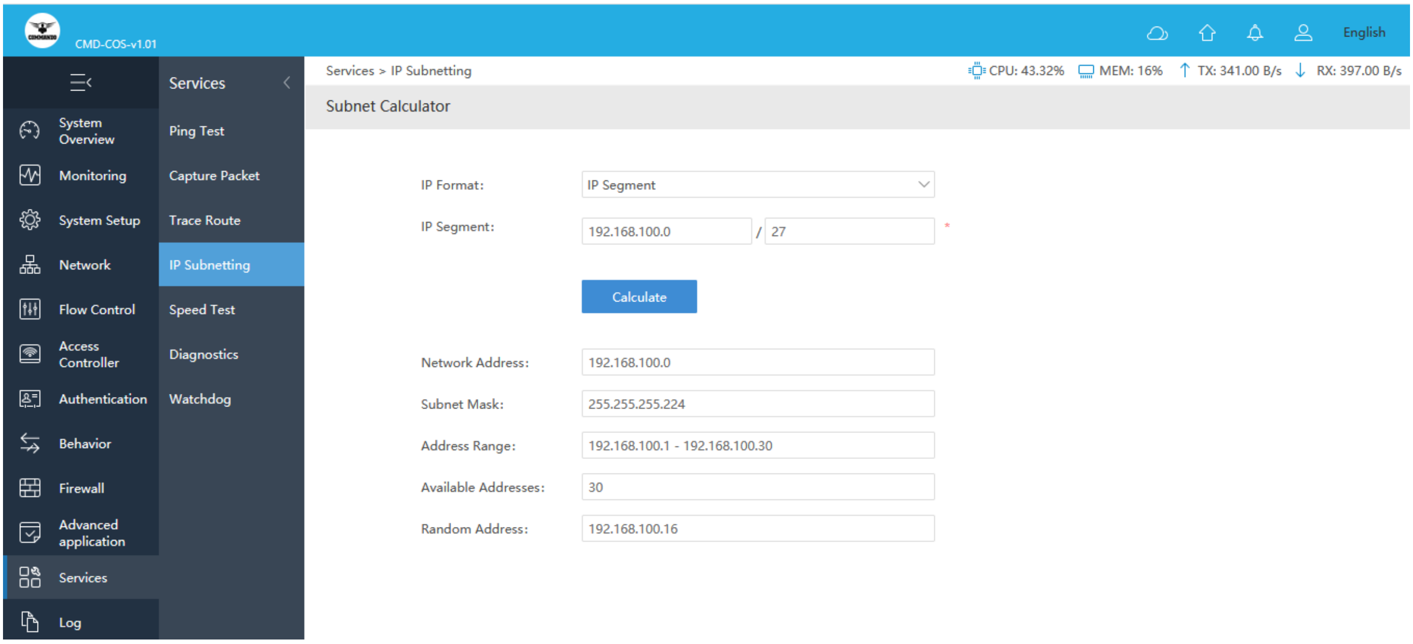
Subnet Mask:

Address Range:

Available Addresses:

Random Address:

Fig 10.4.1 Default Subnet Calculator page



IP Format: IP Segment

IP Segment: 192.168.100.0 / 27

Network Address: 192.168.100.0

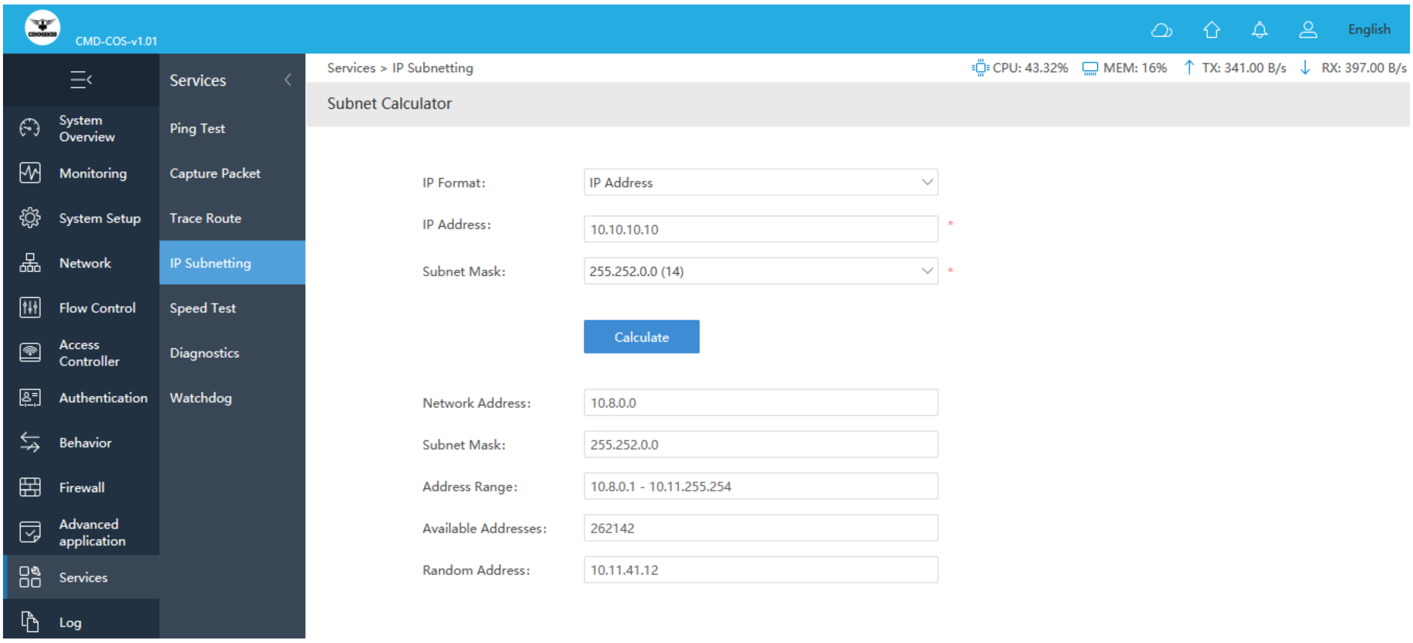
Subnet Mask: 255.255.255.224

Address Range: 192.168.100.1 - 192.168.100.30

Available Addresses: 30

Random Address: 192.168.100.16

Fig 10.4.2 IP Segment Subnet Calculator page



Subnet Calculator

IP Format: IP Address

IP Address: 10.10.10.10 *

Subnet Mask: 255.252.0.0 (14) *

Network Address: 10.8.0.0

Subnet Mask: 255.252.0.0

Address Range: 10.8.0.1 - 10.11.255.254

Available Addresses: 262142

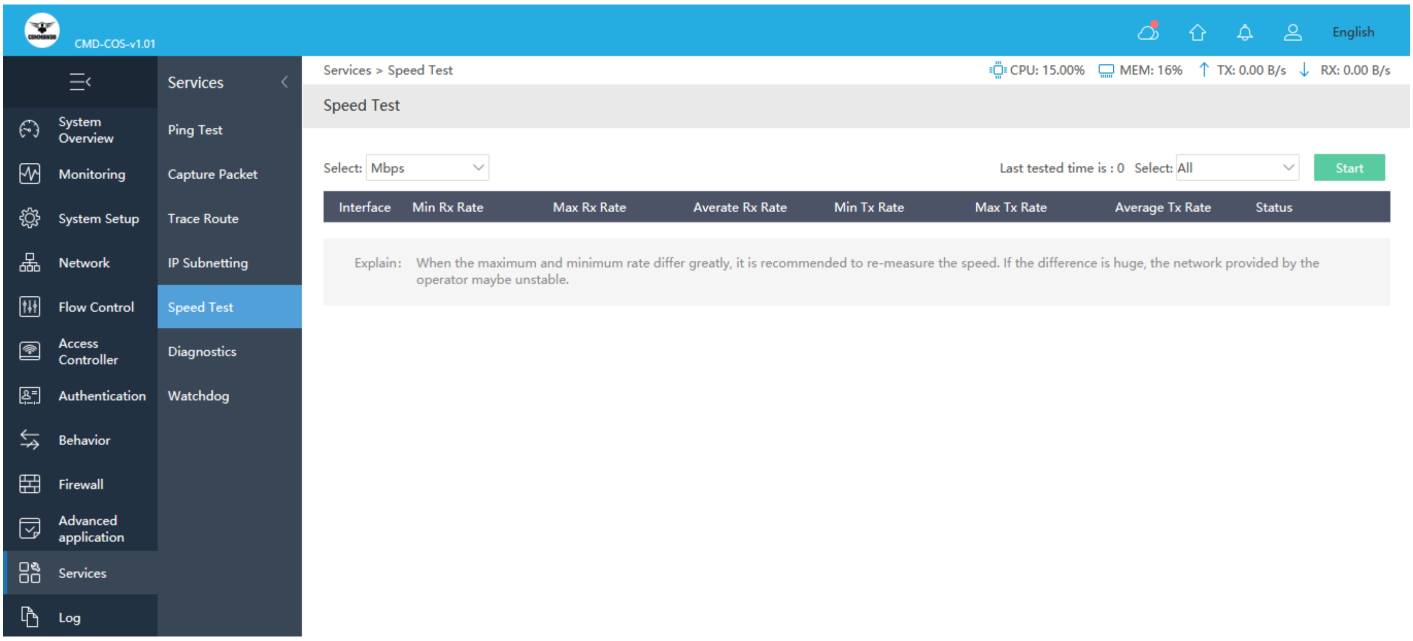
Random Address: 10.11.41.12

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



Speed Test

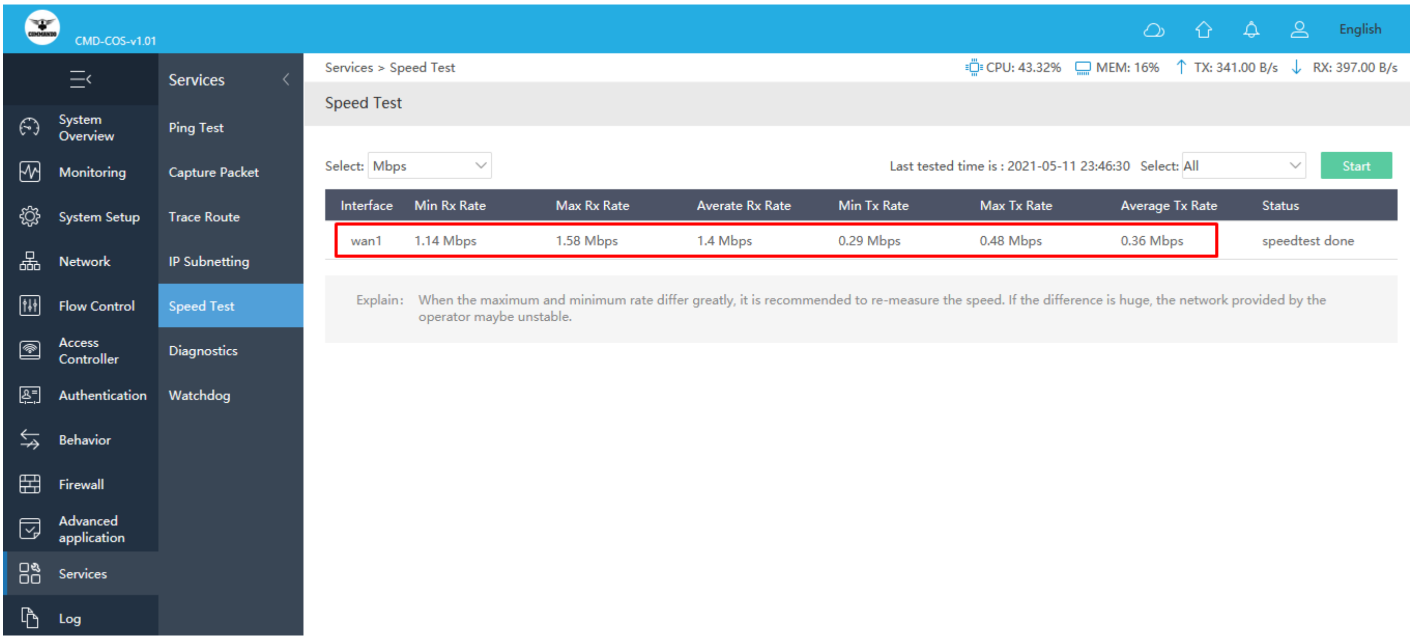
Select: Mbps

Last tested time is : 0 Select: All

Interface	Min Rx Rate	Max Rx Rate	Averate Rx Rate	Min Tx Rate	Max Tx Rate	Average Tx Rate	Status

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 10.5.1 Default Speed Test page



Speed Test

Select: Mbps

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

Interface	Min Rx Rate	Max Rx Rate	Averate 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

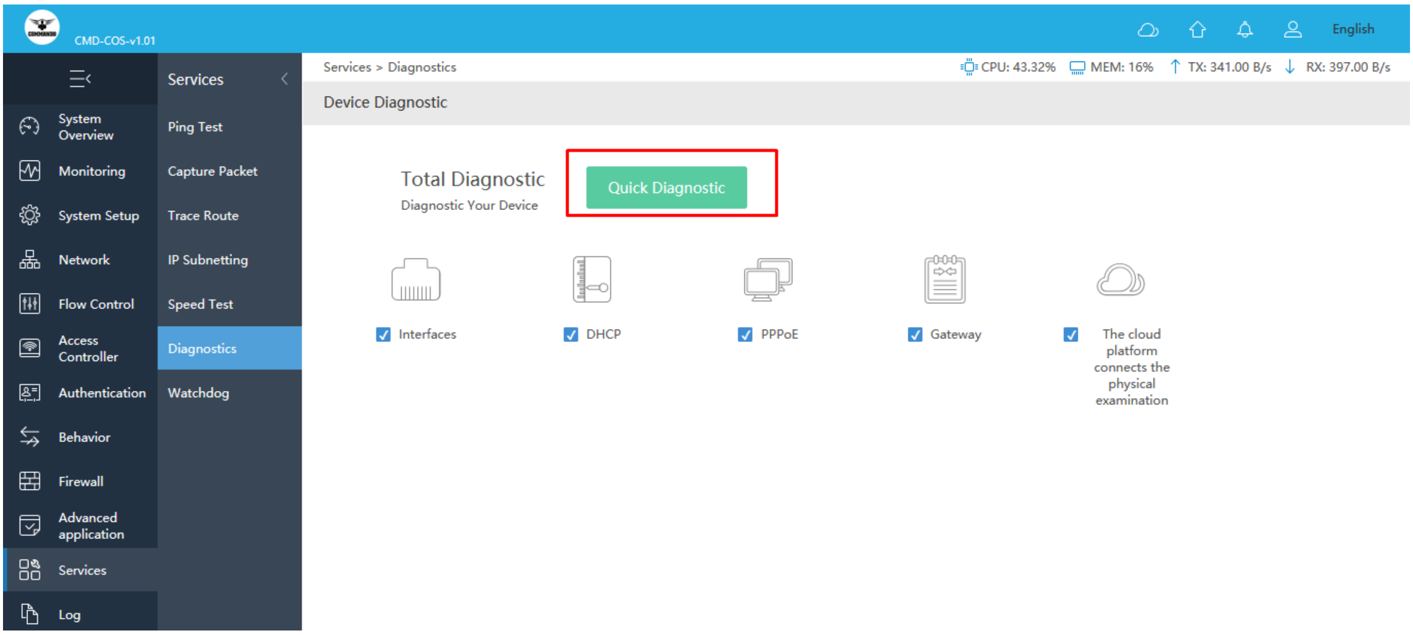
Explain: When the maximum and minimum rate differ greatly, it is recommended to re-measure the speed. If the difference is huge, the network provided by the operator maybe unstable.

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



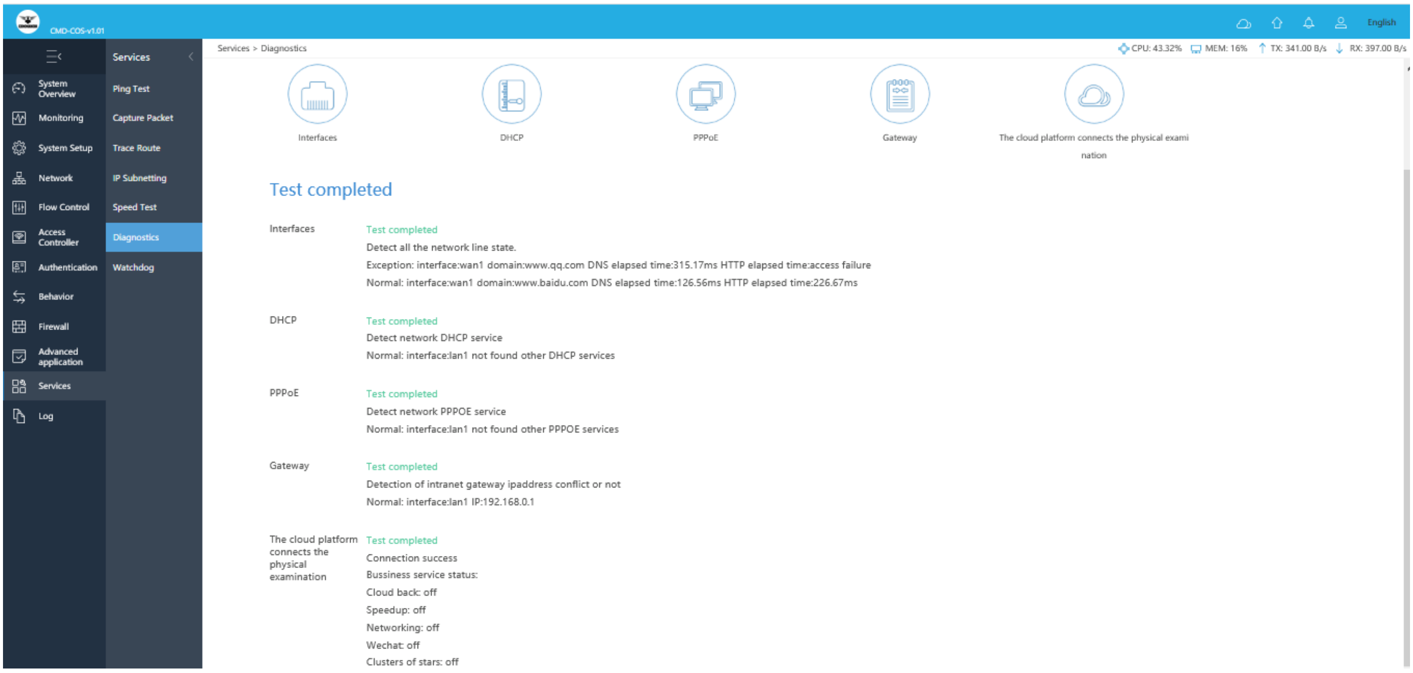
Device Diagnostic

Total Diagnostic

Diagnostic Your Device

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

Fig 10.6.1 Default Device Diagnostic page



Test completed

Interfaces
Test completed
Detect all the network line state.
Exception: interface:wan1 domain:www.qq.com DNS elapsed time:315.17ms HTTP elapsed time:access failure
Normal: interface:wan1 domain:www.baidu.com DNS elapsed time:126.56ms HTTP elapsed time:226.67ms

DHCP
Test completed
Detect network DHCP service
Normal: interface:lan1 not found other DHCP services

PPPoE
Test completed
Detect network PPPOE service
Normal: interface:lan1 not found other PPPOE services

Gateway
Test completed
Detection of intranet gateway ipaddress conflict or not
Normal: interface:lan1 IP:192.168.0.1

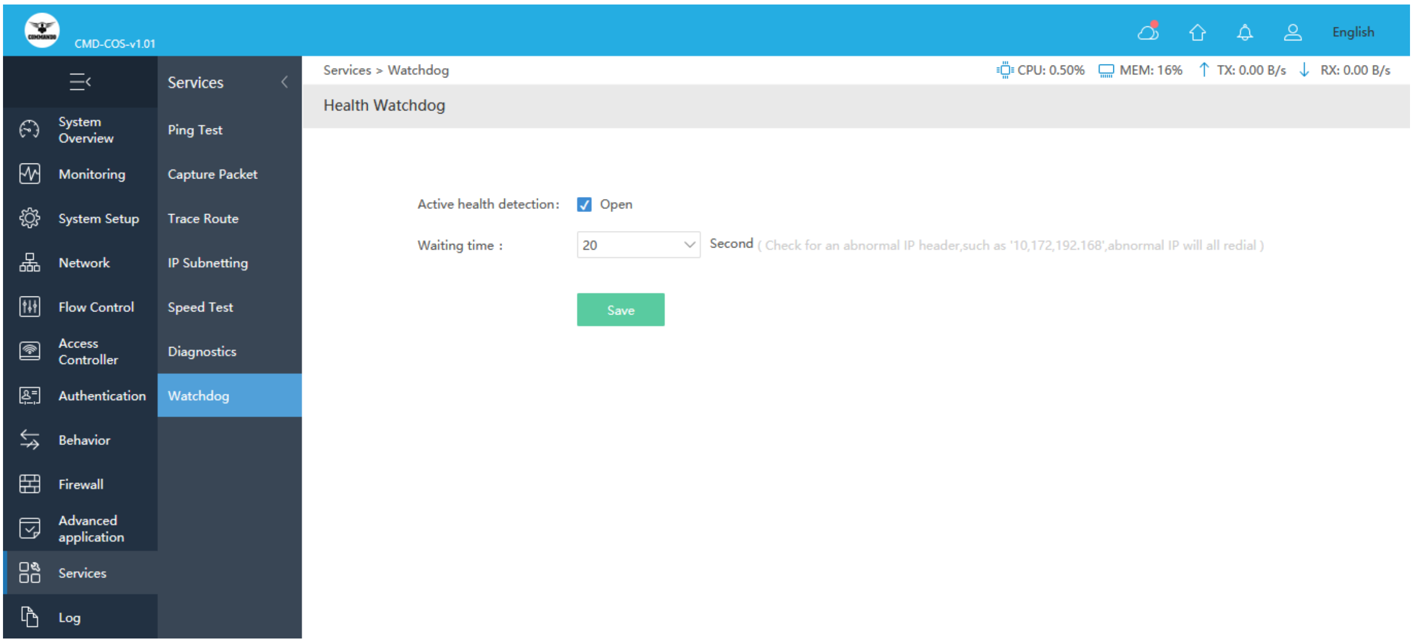
The cloud platform connects the physical examination
Test completed
Connection success
Bussiness service status:
Cloud back: off
Speedup: off
Networking: off
Wechat: off
Clusters of stars: off

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



Health Watchdog

Active health detection: ☑ Open

Waiting time : 20 Second (Check for an abnormal IP header,such as '10,172,192.168',abnormal IP will all redial)

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.

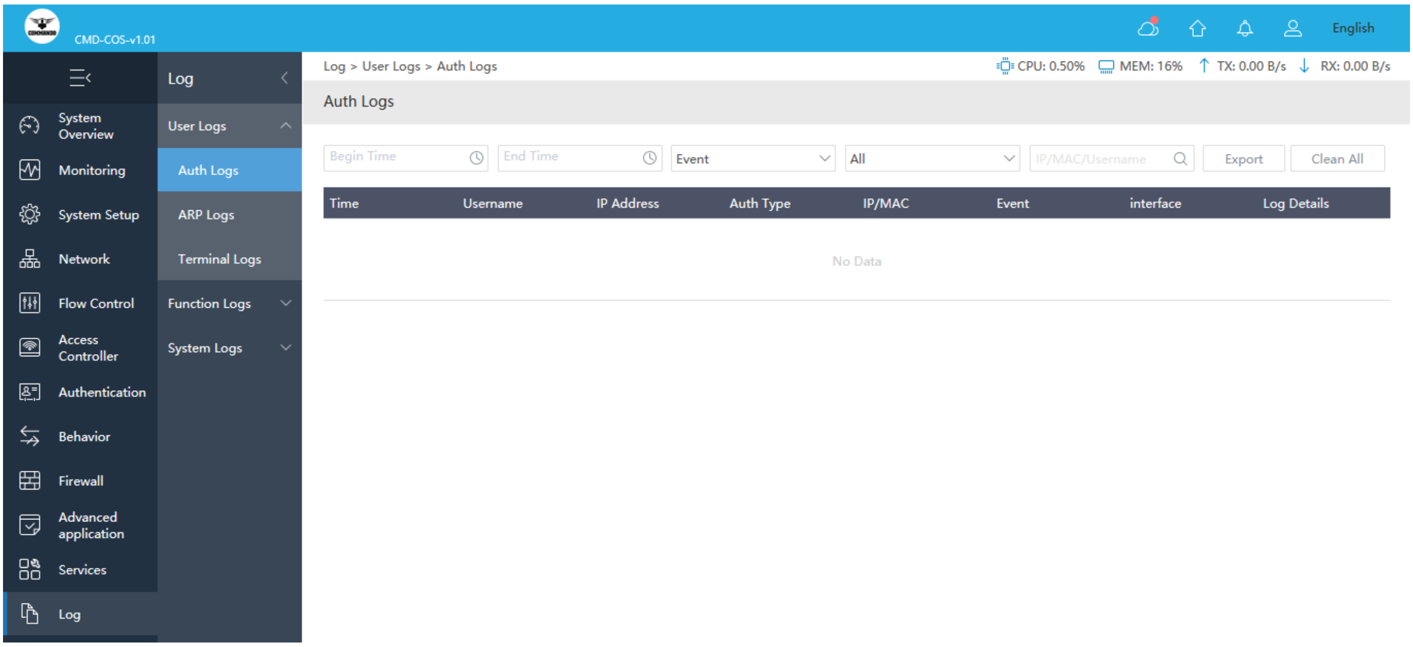
System Logs:
This is for viewing System Logs, Action Logs, Notification.

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



Log > User Logs > Auth Logs

Auth Logs

Time	Username	IP Address	Auth Type	IP/MAC	Event	interface	Log Details

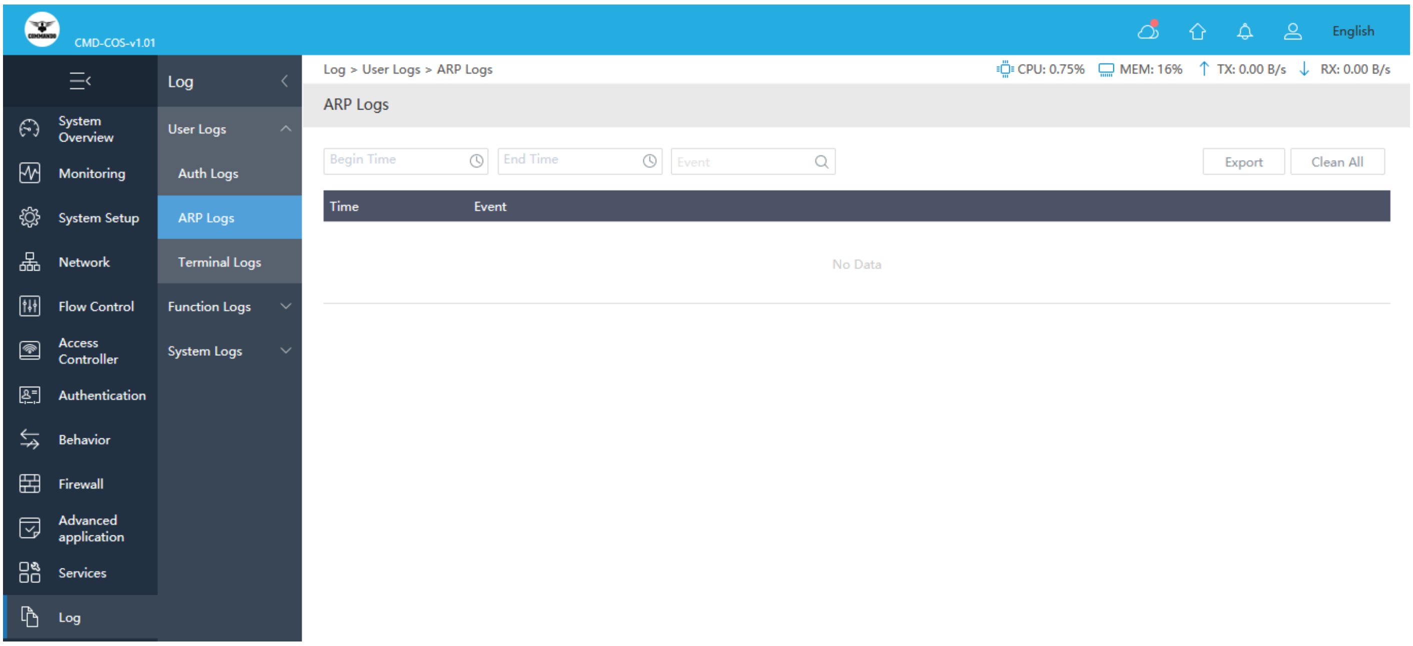
No Data

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



ARP Logs

Time	Event

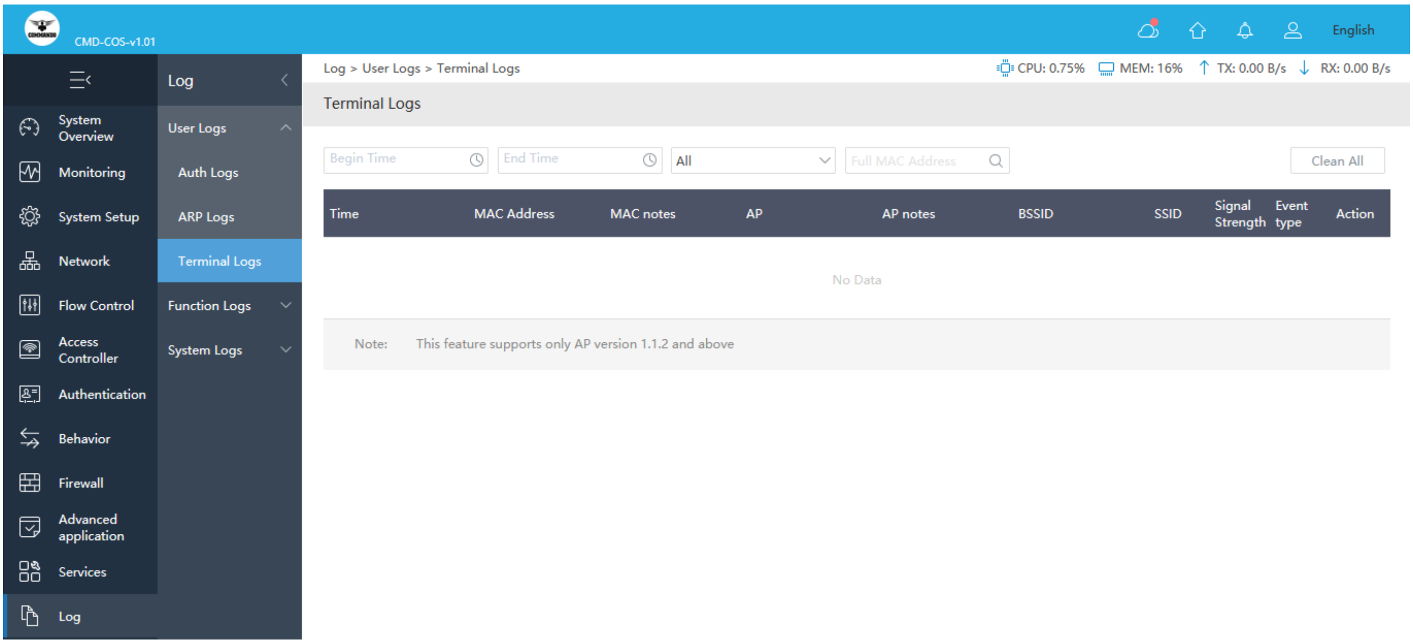
No Data

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



Terminal Logs

Time	MAC Address	MAC notes	AP	AP notes	BSSID	SSID	Signal Strength	Event type	Action

No Data

Note: This feature supports only AP version 1.1.2 and above

Fig 11.1.3 Default Terminal Logs page

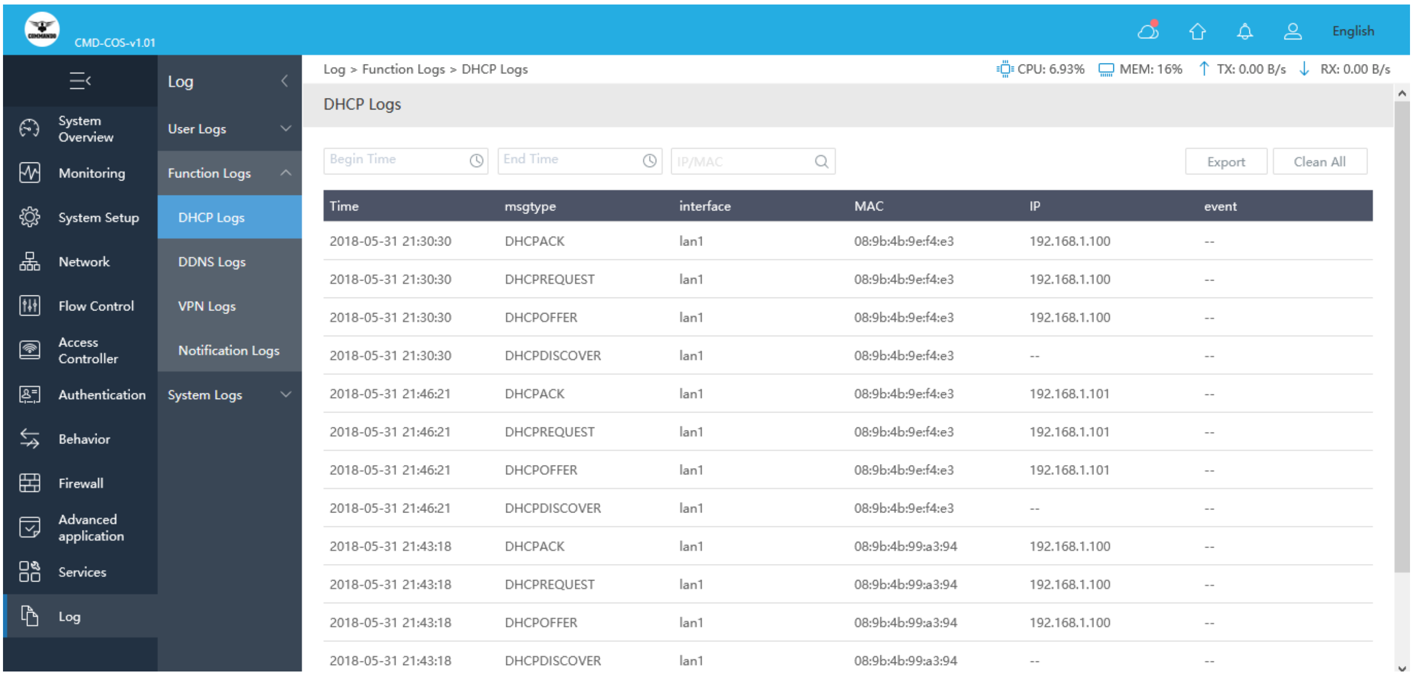
11.2 Function Logs

You Can monitor function Logs like DHCP Logs, DDNS Logs and VPN Logs.

DHCP Logs:

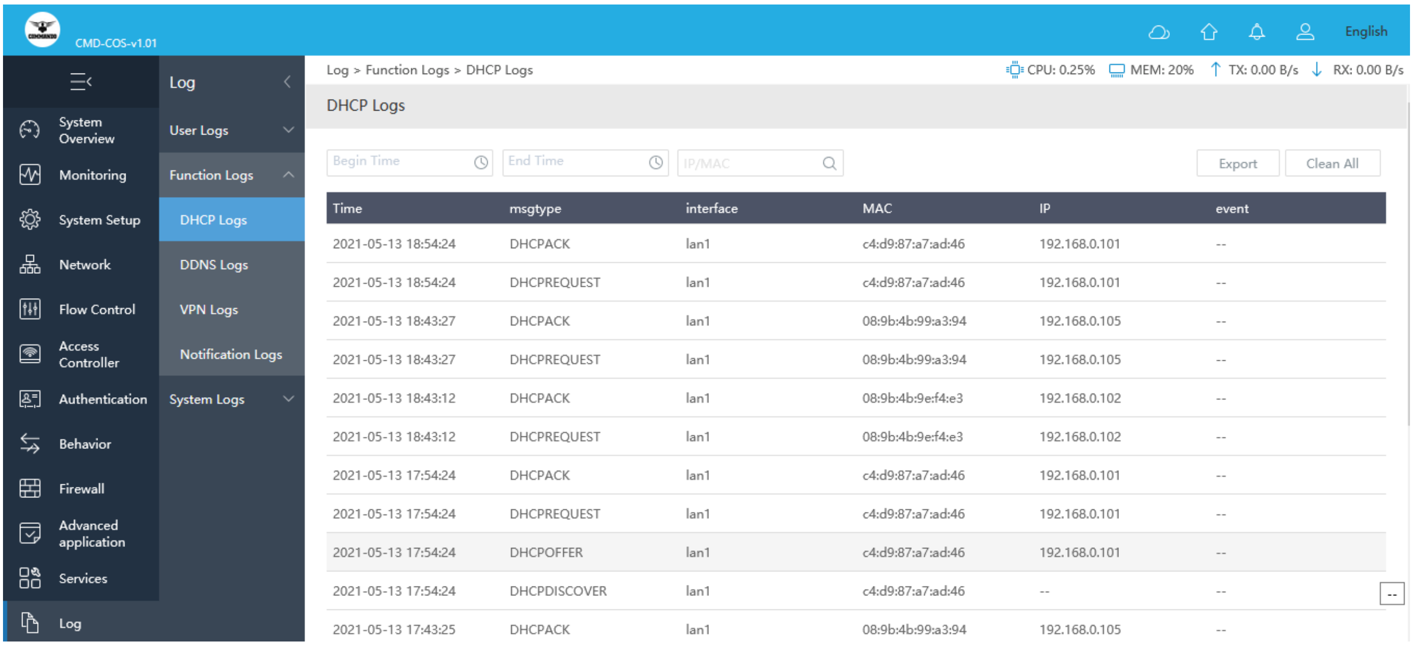
DHCP logs contains MAC address, associated IP, message type and connected interface which can be crucial for identifying connected user. Monitoring and alerting to unknown and unrecognized users are also important for most of organizations.

To monitor DHCP Logs, Click on Log > Function Logs > DHCP Logs



Time	msgtype	interface	MAC	IP	event
2018-05-31 21:30:30	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPOFFER	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	--
2018-05-31 21:30:30	DHCPDISCOVER	lan1	08:9b:4b:9e:f4:e3	--	--
2018-05-31 21:46:21	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPOFFER	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	--
2018-05-31 21:46:21	DHCPDISCOVER	lan1	08:9b:4b:9e:f4:e3	--	--
2018-05-31 21:43:18	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPREQUEST	lan1	08:9b:4b:99:a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPOFFER	lan1	08:9b:4b:99:a3:94	192.168.1.100	--
2018-05-31 21:43:18	DHCPDISCOVER	lan1	08:9b:4b:99:a3:94	--	--

Fig 11.2.1 Default DHCP Logs page



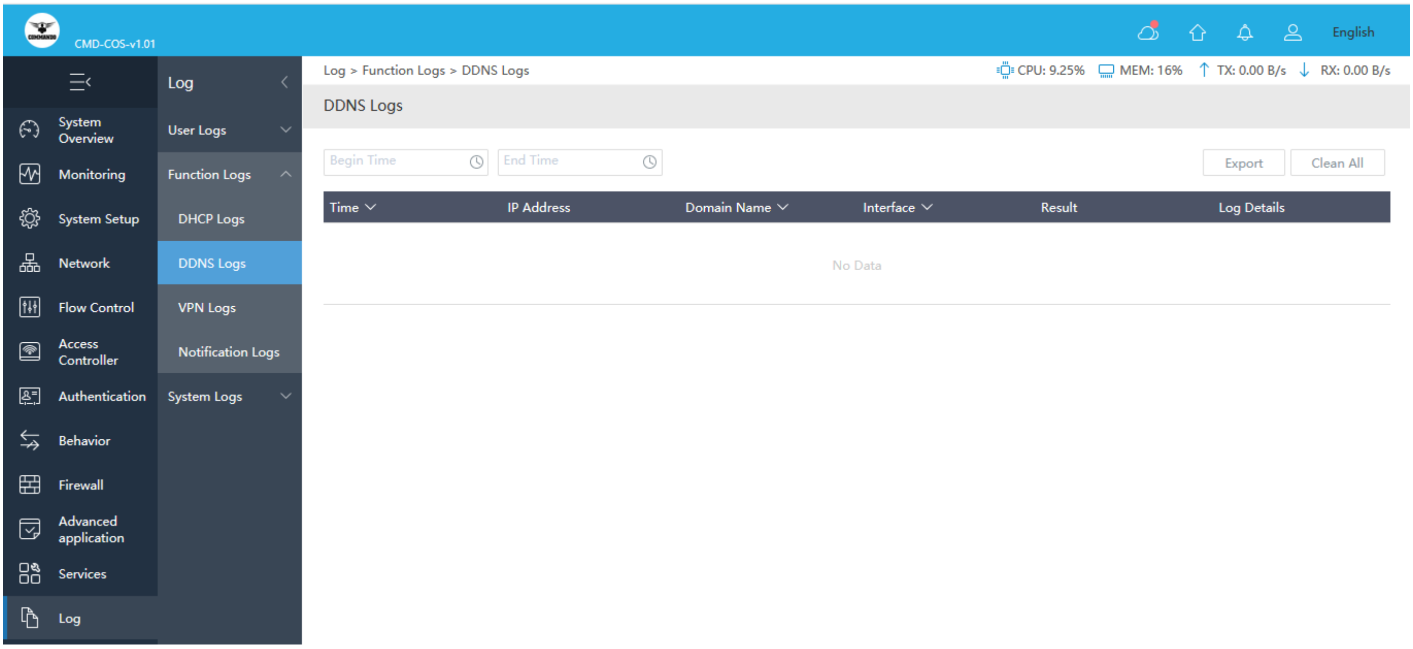
Time	msgtype	interface	MAC	IP	event
2021-05-13 18:54:24	DHCPACK	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 18:54:24	DHCPREQUEST	lan1	c4:d9:87:a7:ad:46	192.168.0.101	--
2021-05-13 18:43:27	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.0.105	--
2021-05-13 18:43:27	DHCPREQUEST	lan1	08:9b:4b:99:a3:94	192.168.0.105	--
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	DHCPOFFER	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:

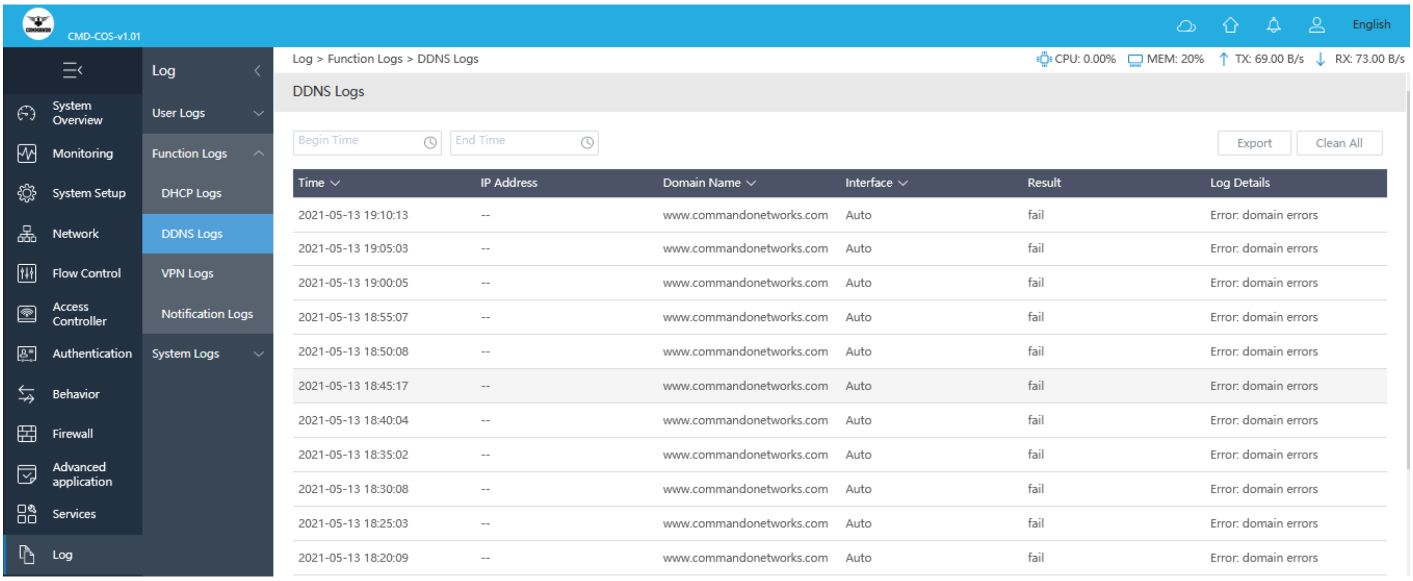
It contains IP Address, Domain Name and Interface along with Log details and time.

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



Time	IP Address	Domain Name	Interface	Result	Log Details
No Data					

Fig 11.2.3 Default DDNS Logs page



Log > Function Logs > DDNS Logs

DDNS Logs

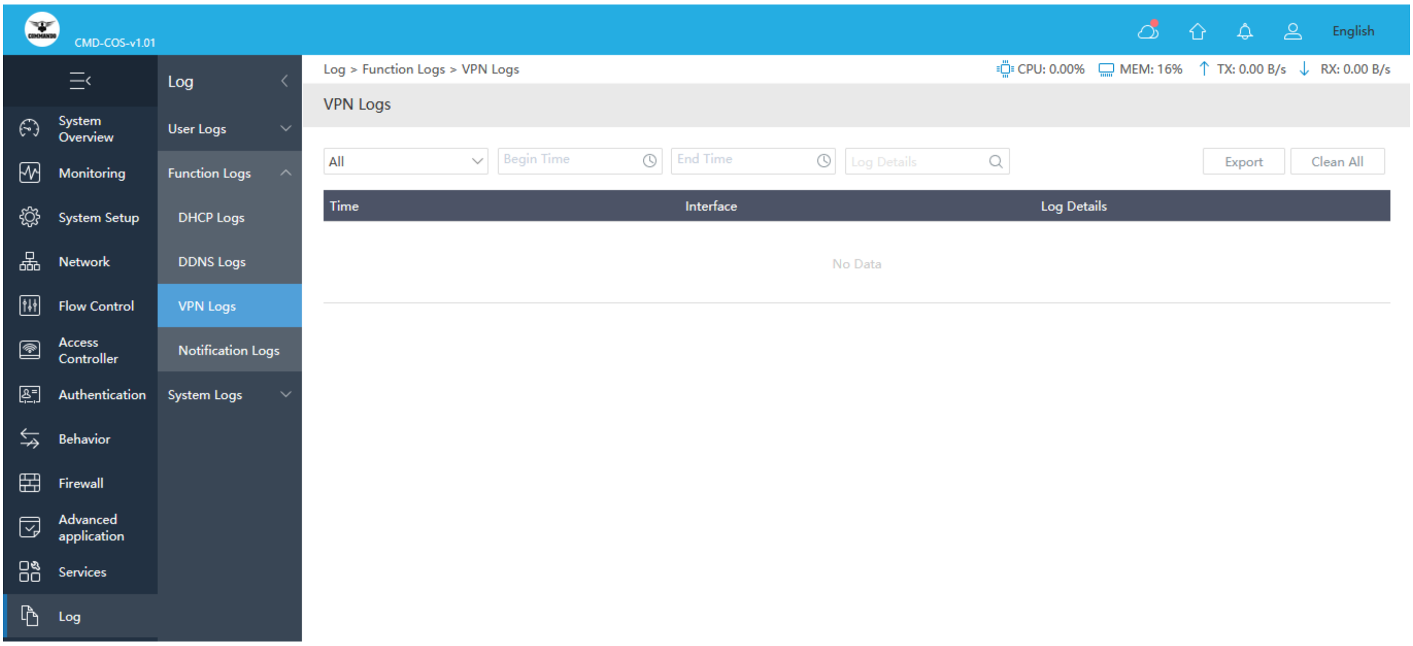
Time	IP Address	Domain Name	Interface	Result	Log Details
2021-05-13 19:10:13	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 19:05:03	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 19:00:05	--	www.commandonetworks.com	Auto	fail	Error: domain errors
2021-05-13 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



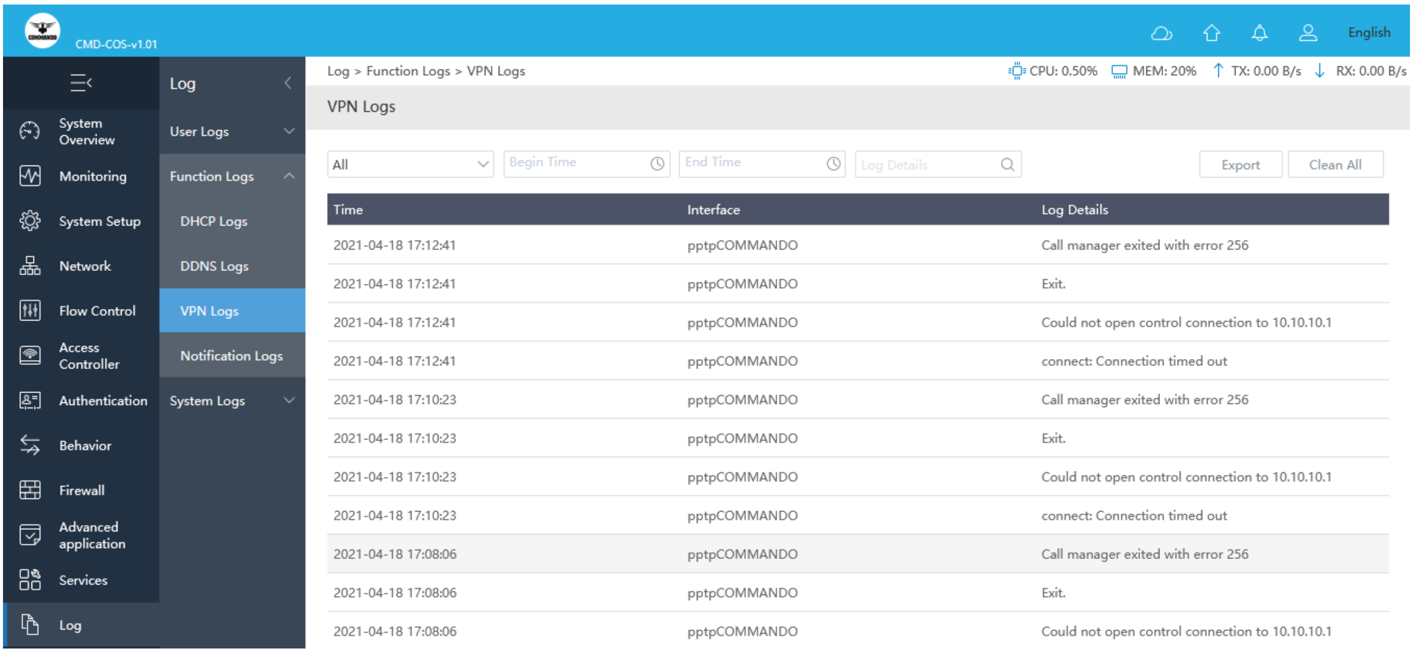
Log > Function Logs > VPN Logs

VPN Logs

Time	Interface	Log Details

No Data

Fig 11.2.5 Default VPN Logs page



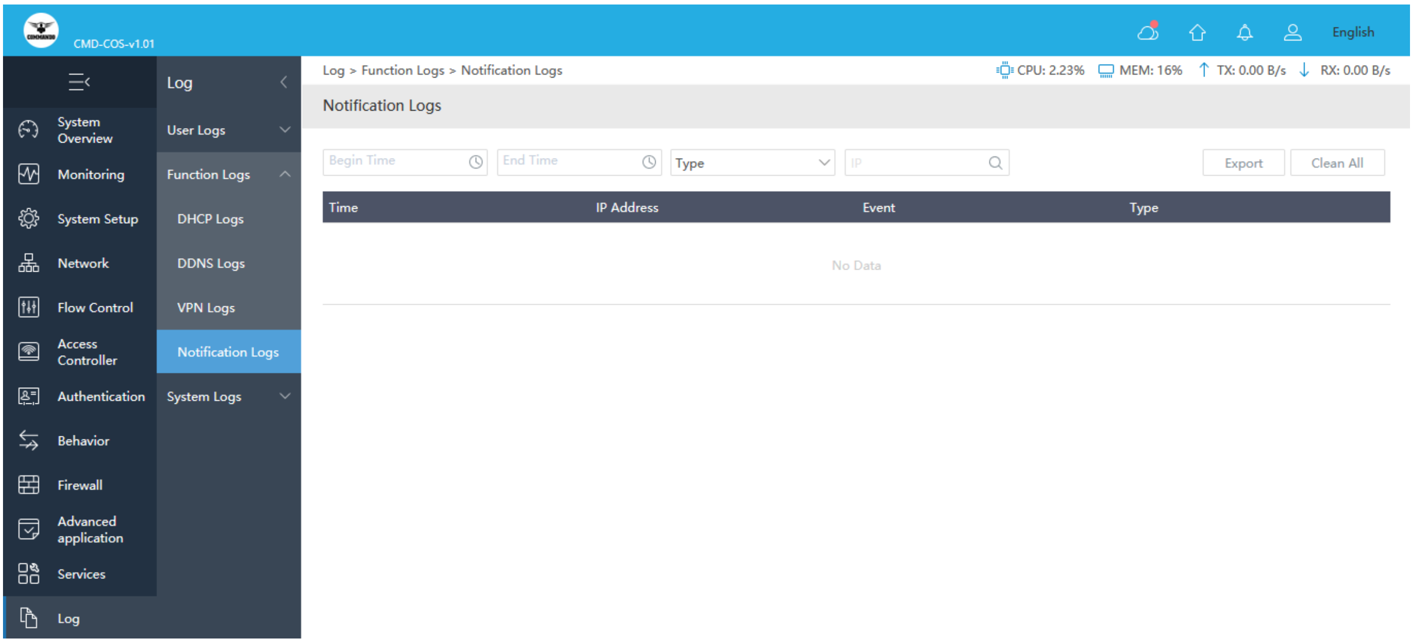
Time	Interface	Log Details
2021-04-18 17:12:41	pptpCOMMANDO	Call manager exited with error 256
2021-04-18 17:12:41	pptpCOMMANDO	Exit.
2021-04-18 17:12:41	pptpCOMMANDO	Could not open control connection to 10.10.10.1
2021-04-18 17:12:41	pptpCOMMANDO	connect: Connection timed out
2021-04-18 17:10:23	pptpCOMMANDO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



Time	IP Address	Event	Type
		No Data	

Fig 11.2.7 Default Notification Logs page

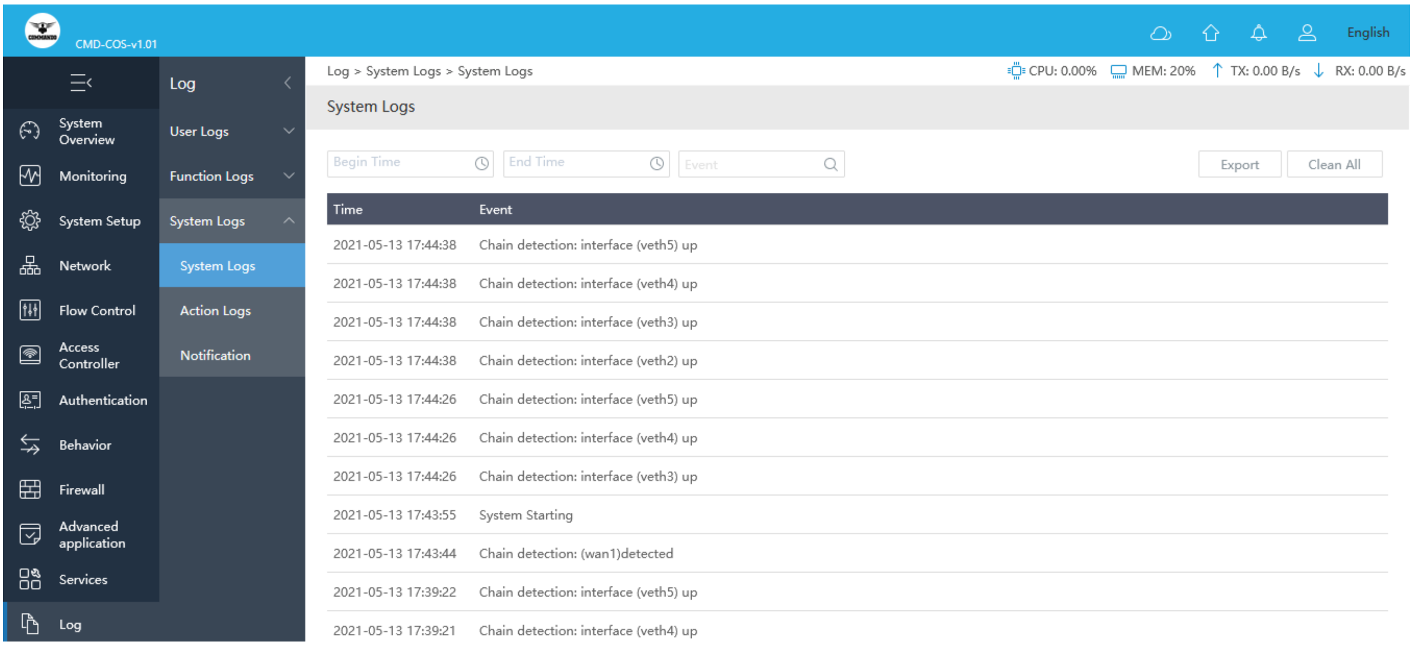
11.3 System Logs

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.



System Logs

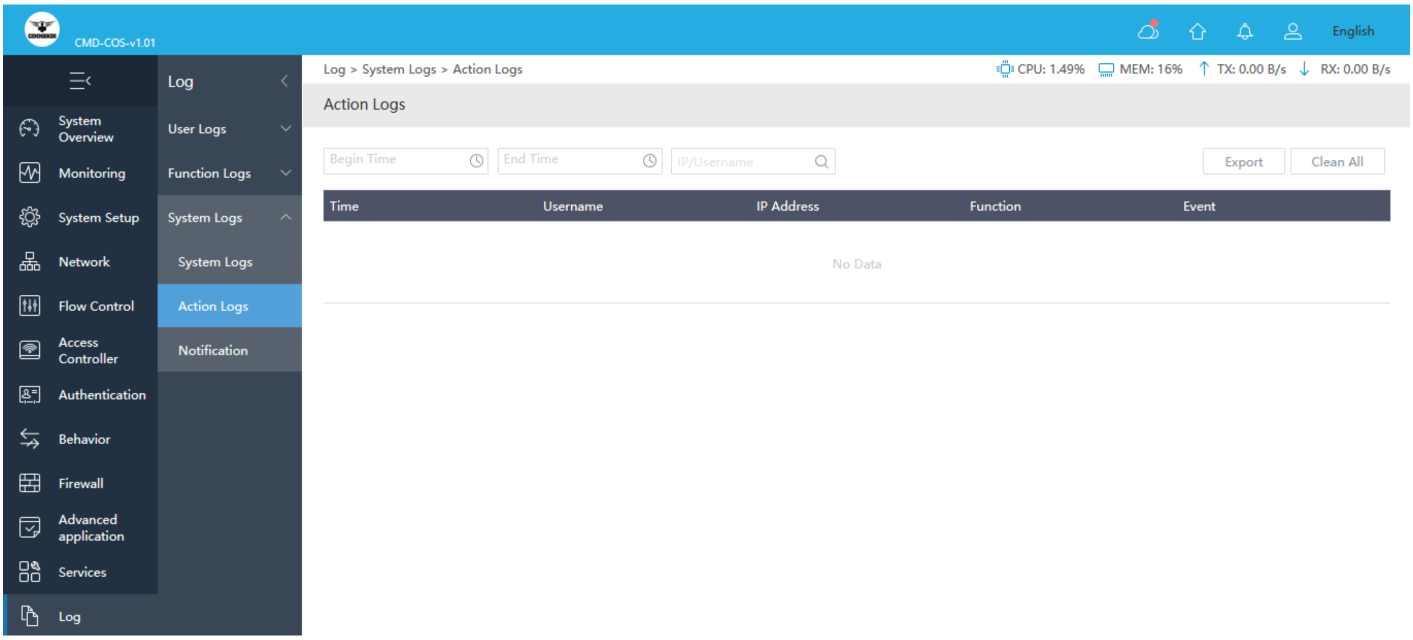
Time	Event
2021-05-13 17:44:38	Chain detection: interface (veth5) up
2021-05-13 17:44:38	Chain detection: interface (veth4) up
2021-05-13 17:44:38	Chain detection: interface (veth3) up
2021-05-13 17:44:38	Chain detection: interface (veth2) up
2021-05-13 17:44:26	Chain detection: interface (veth5) up
2021-05-13 17:44:26	Chain detection: interface (veth4) up
2021-05-13 17:44:26	Chain detection: interface (veth3) up
2021-05-13 17:43:55	System Starting
2021-05-13 17:43:44	Chain detection: (wan1)detected
2021-05-13 17:39:22	Chain detection: interface (veth5) up
2021-05-13 17:39:21	Chain detection: interface (veth4) up

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.

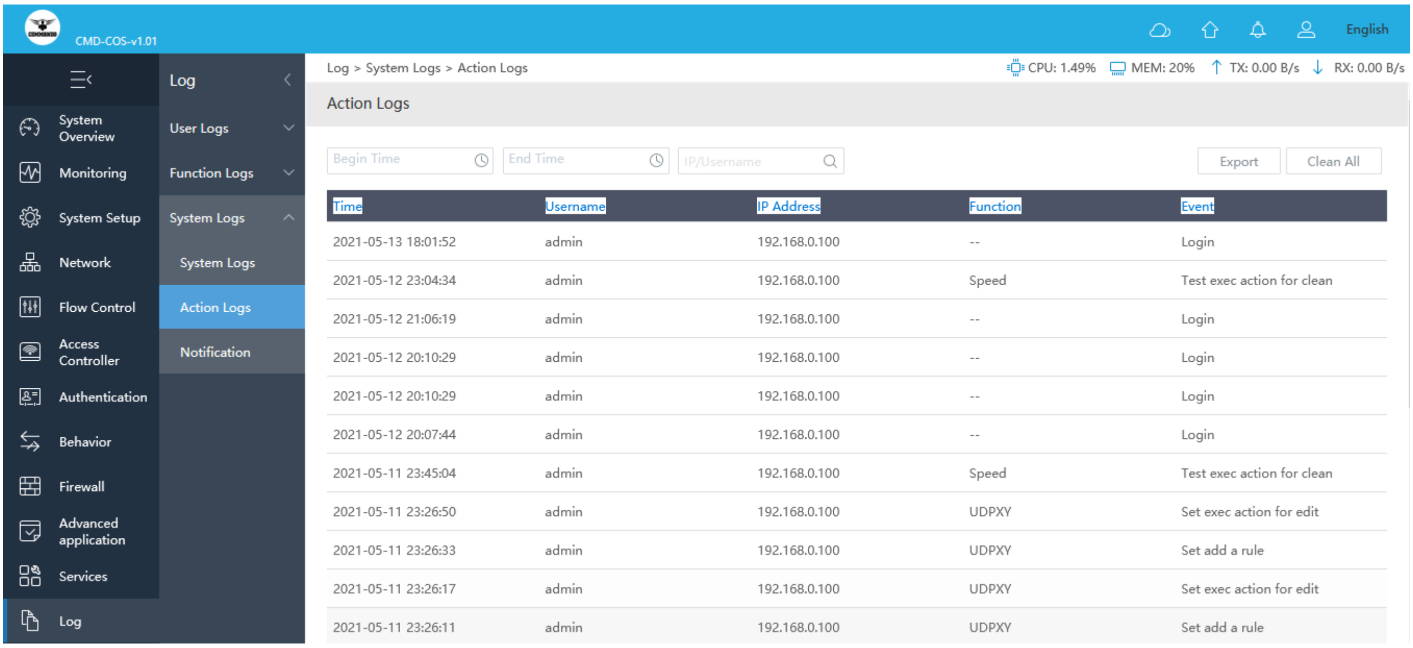
To configure Action Logs, Click on Log > System Logs > Action Logs.



Action Logs

Time	Username	IP Address	Function	Event
		No Data		

Fig 11.3.2 Default Action Logs page



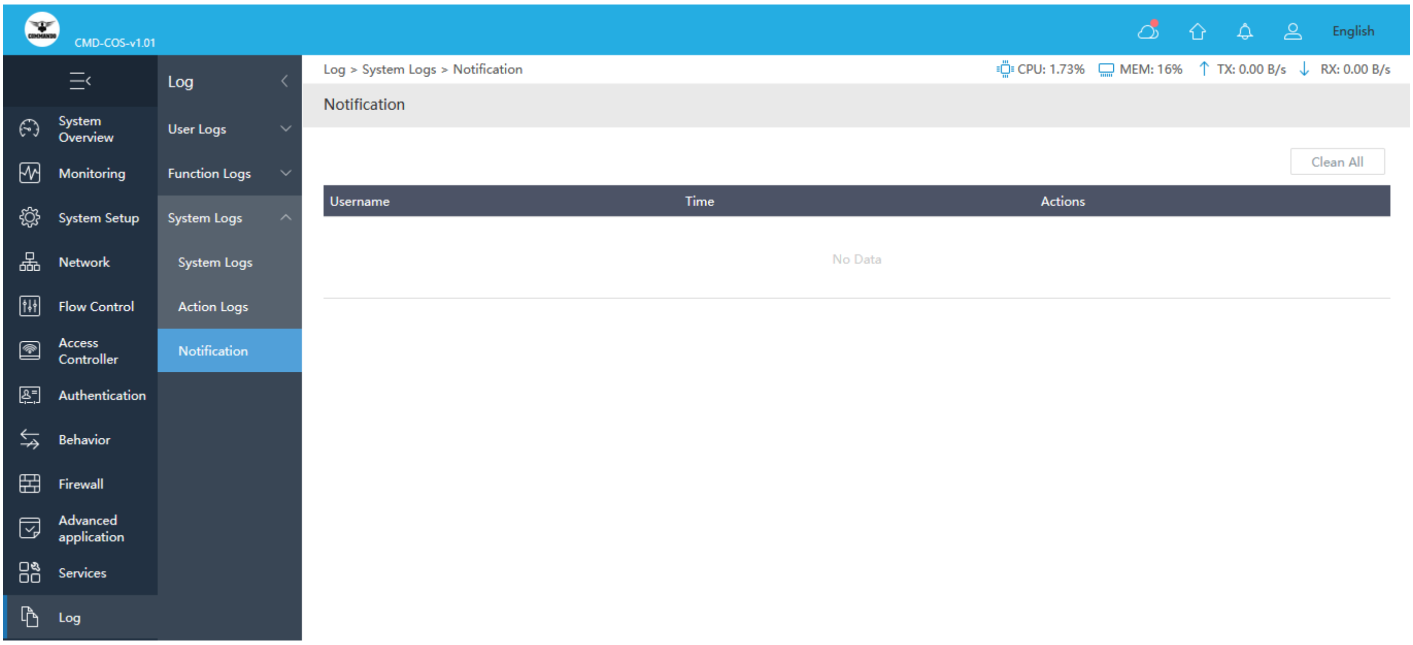
Time	Username	IP Address	Function	Event
2021-05-13 18:01:52	admin	192.168.0.100	--	Login
2021-05-12 23:04:34	admin	192.168.0.100	Speed	Test exec action for clean
2021-05-12 21:06:19	admin	192.168.0.100	--	Login
2021-05-12 20:10:29	admin	192.168.0.100	--	Login
2021-05-12 20:10:29	admin	192.168.0.100	--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



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?

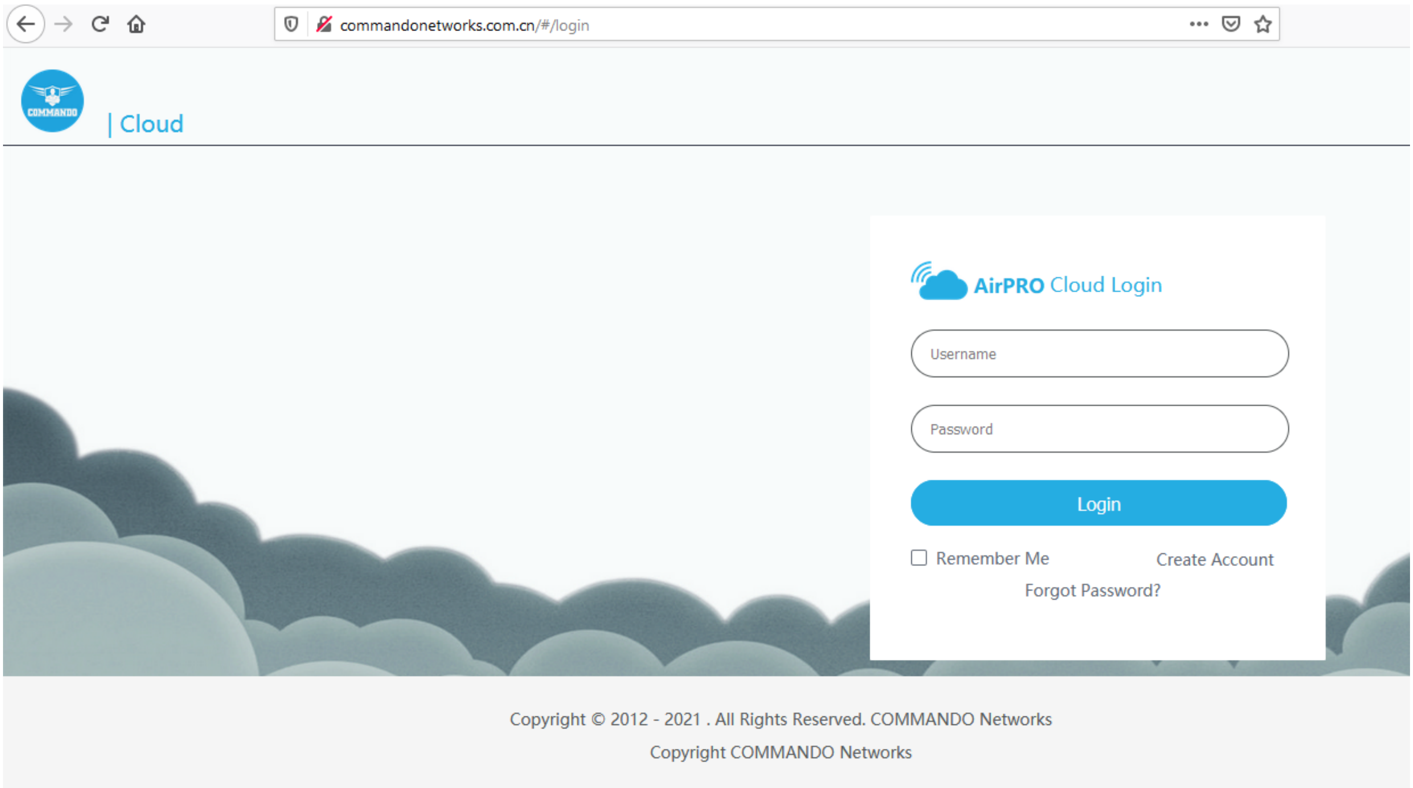
Into cloud platform http://commandonetworks.com.cn/ ---> gets the binding code ---> enters the binding code in router and remark name ---> saves and completes the binding.

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?

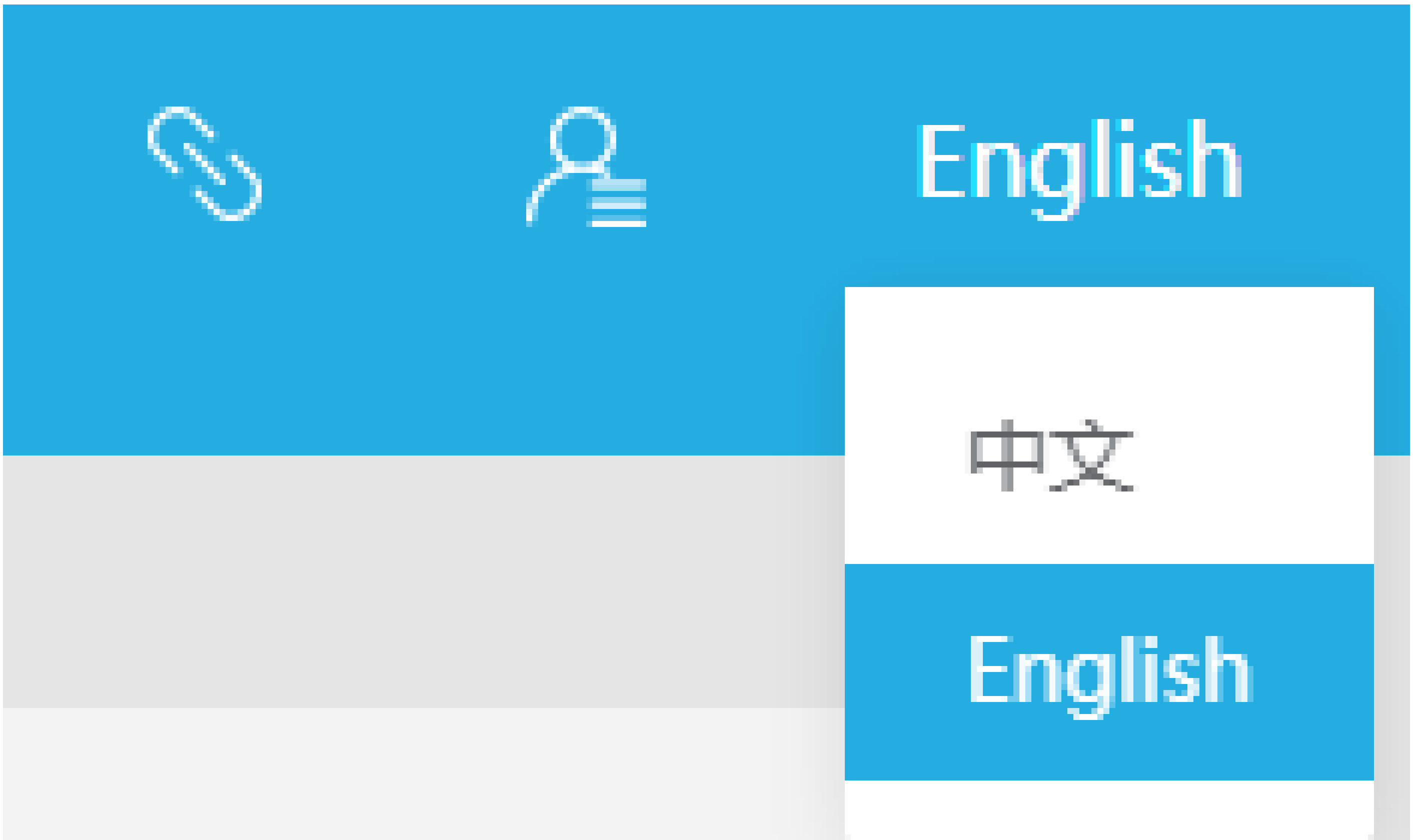
Log in to cloud platform on the PC side and complete the unbundling of corresponding routes in the routing list -- equipment management -- routing information overview page.



Copyright © 2012 - 2021 . All Rights Reserved. COMMANDO Networks

Copyright COMMANDO Networks

Fig 12.1 Cloud Login page



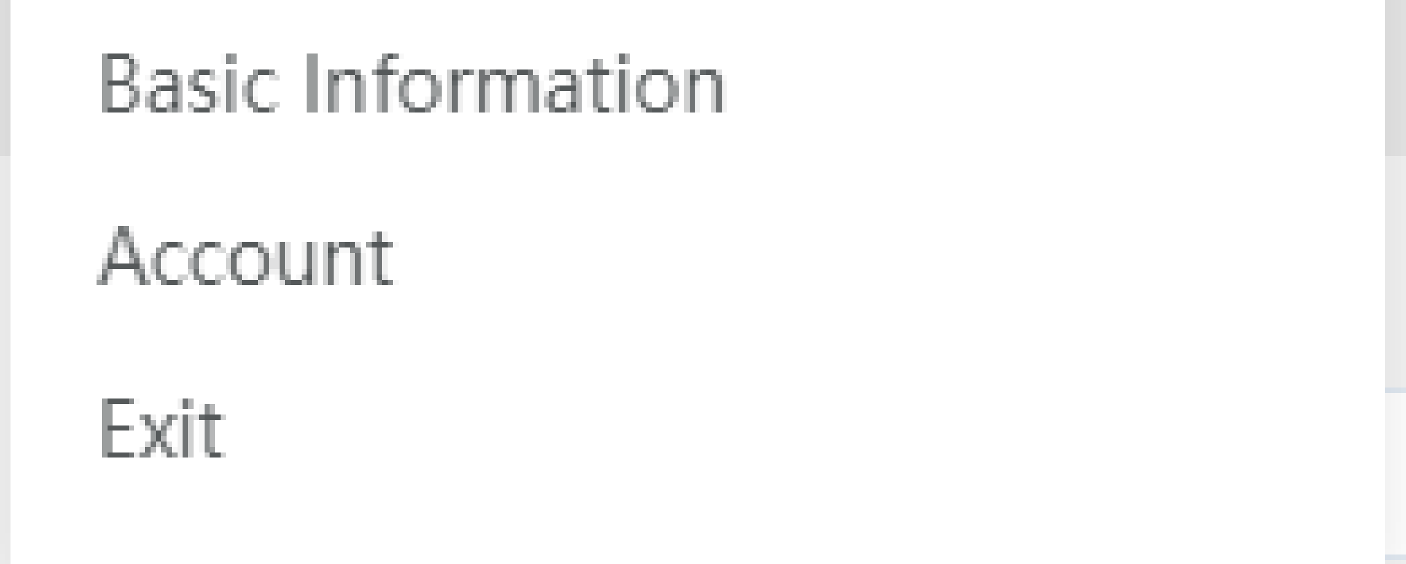
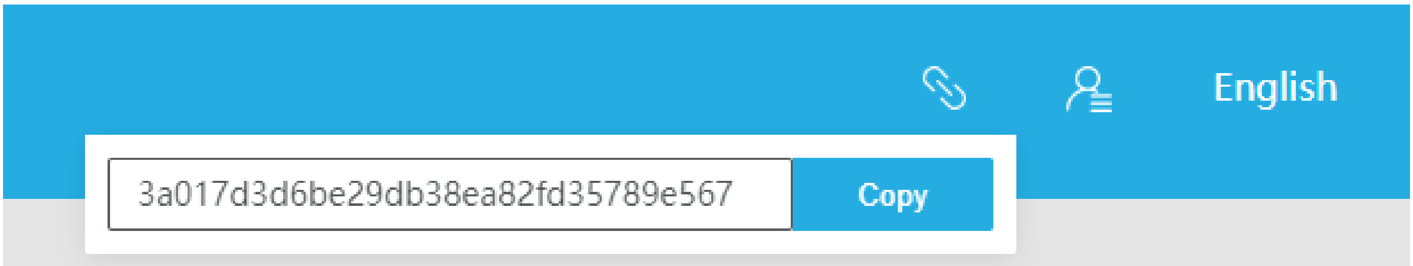


Fig 12.2 Cloud User Language setting page

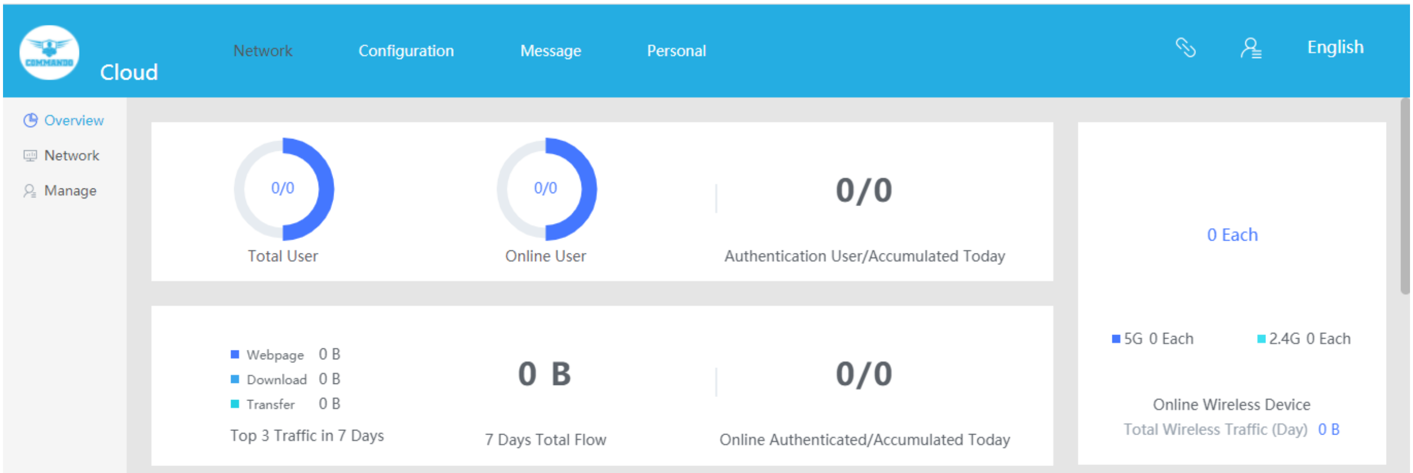


3a017d3d6be29db38ea82fd35789e567

Fig 12.3 Cloud Binding page

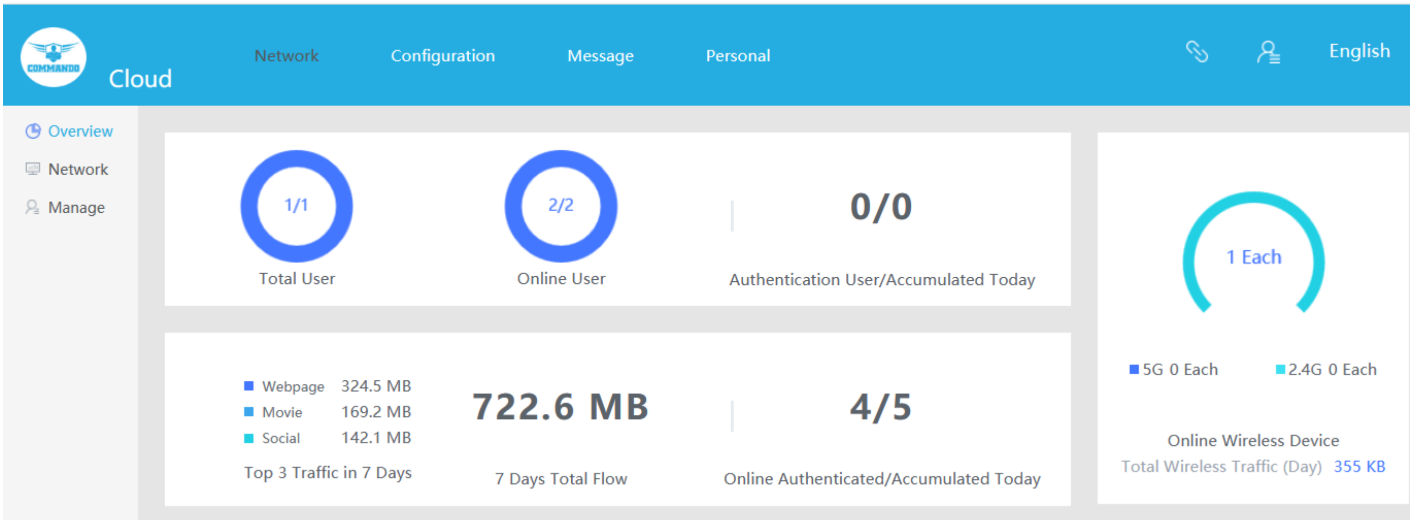
12.1 AirPRO Cloud Overview

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.



0/0 Total User
0/0 Online User
0/0 Authentication User/Accumulated Today
0 Each
Webpage 0 B
Download 0 B
Transfer 0 B
Top 3 Traffic in 7 Days
0 B 7 Days Total Flow
0/0 Online Authenticated/Accumulated Today
5G 0 Each
2.4G 0 Each
Online Wireless Device
Total Wireless Traffic (Day) 0 B

Fig 12.1.1 Default Cloud Overview page



1/1 Total User
2/2 Online User
0/0 Authentication User/Accumulated Today
1 Each
Webpage 324.5 MB
Movie 169.2 MB
Social 142.1 MB
Top 3 Traffic in 7 Days
722.6 MB 7 Days Total Flow
4/5 Online Authenticated/Accumulated Today
5G 0 Each
2.4G 0 Each
Online Wireless Device
Total Wireless Traffic (Day) 355 KB

Fig 12.1.2 Cloud Overview page

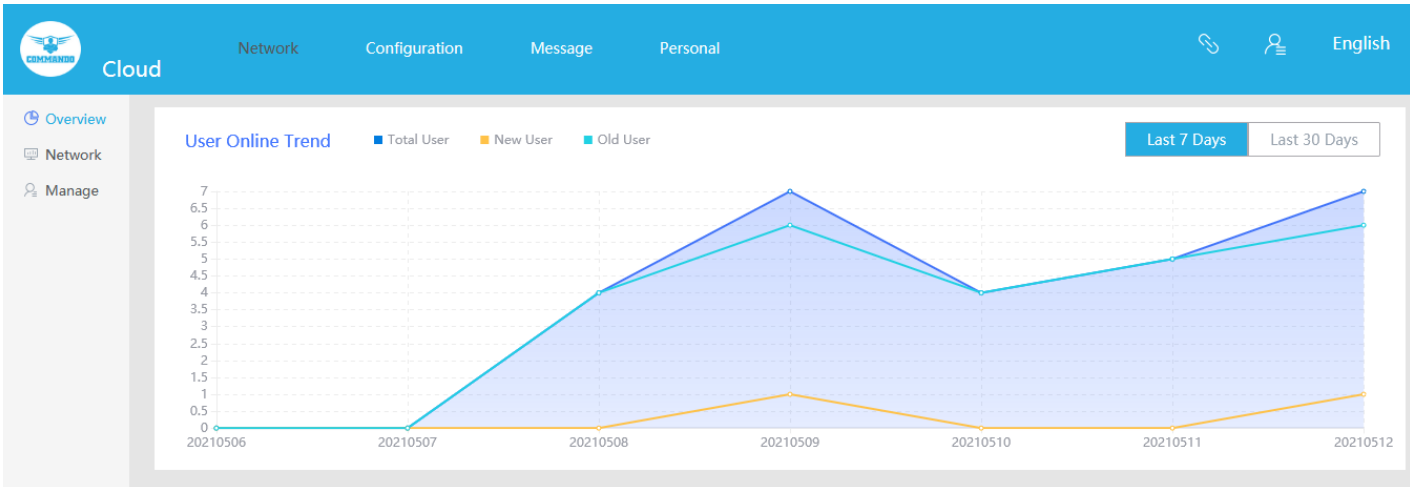


Fig 12.1.3 Cloud User online trend page

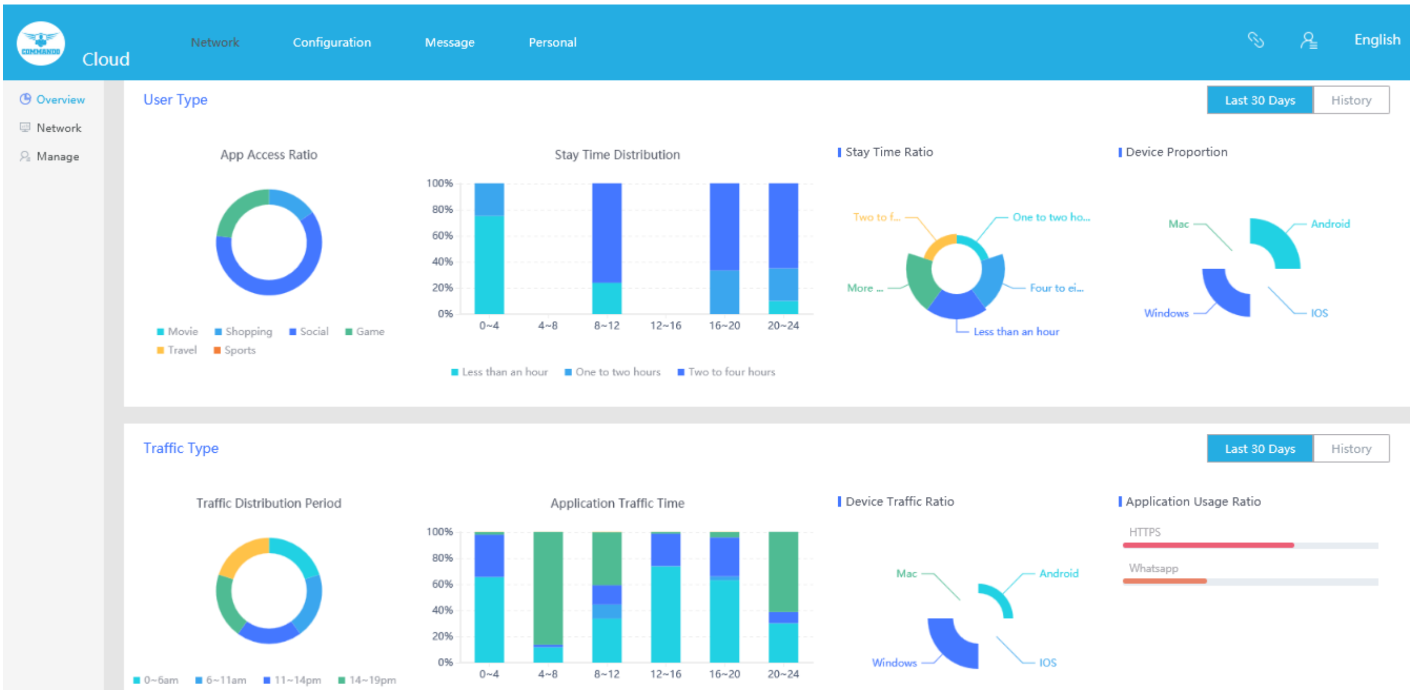
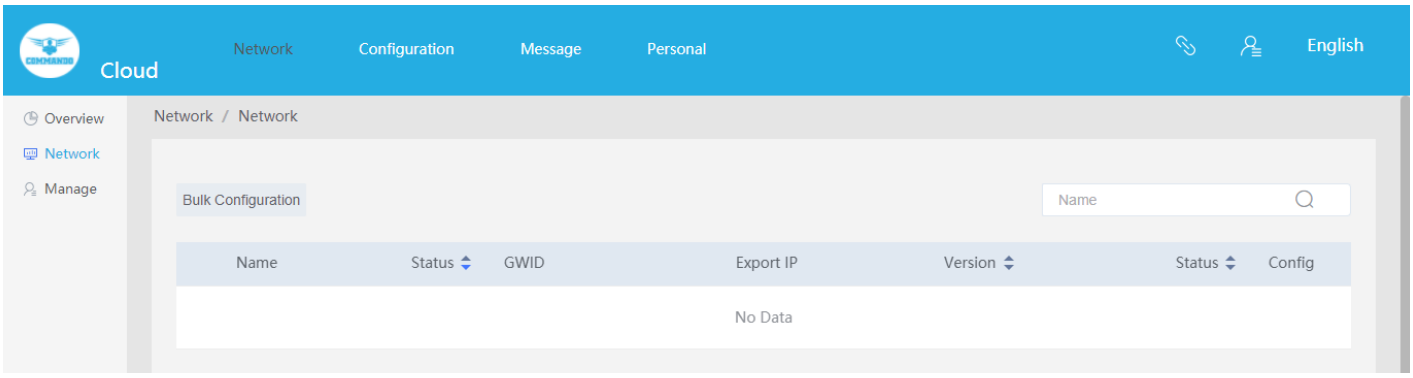


Fig 12.1.4 Cloud User Type page

12.2 Network

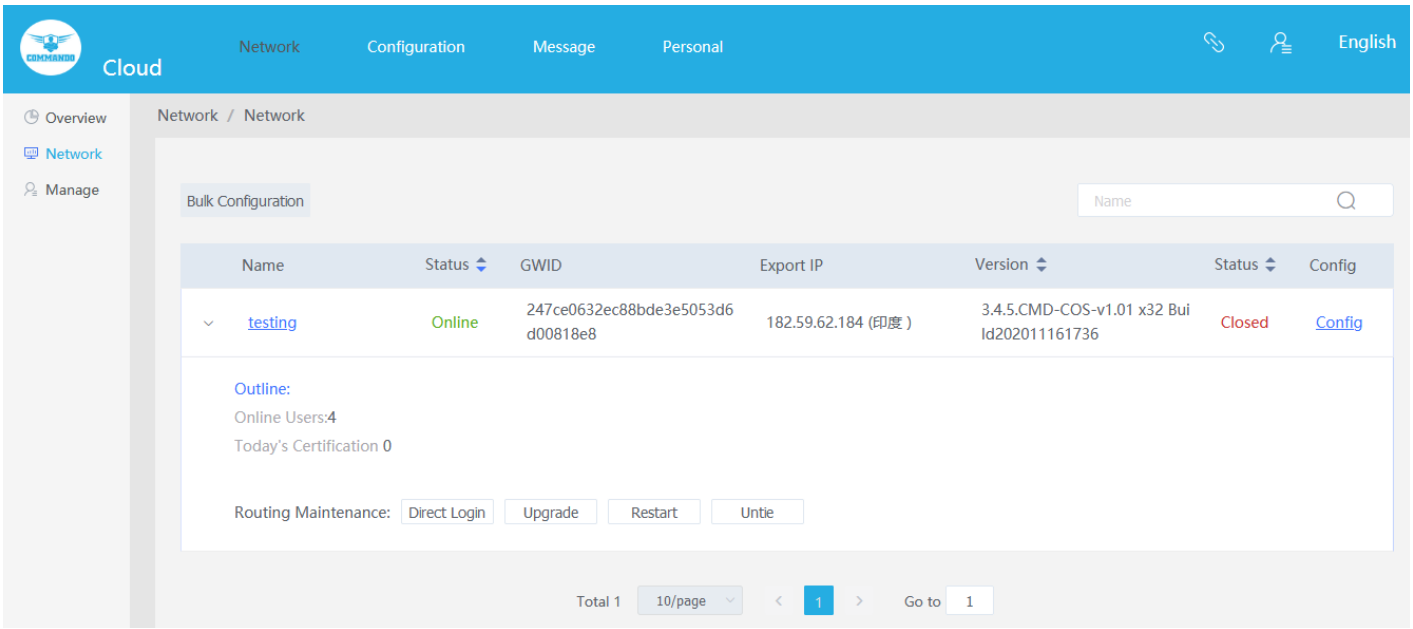
Cloud Networking Solutions are Designed to Enhance Your access and IT infrastructure in which some or all of an organization's network capabilities and resources are hosted cloud account.



Network / Network

Name	Status	GWID	Export IP	Version	Status	Config
No Data						

Fig 12.2.1 Default Bulk configuration page



Network / Network

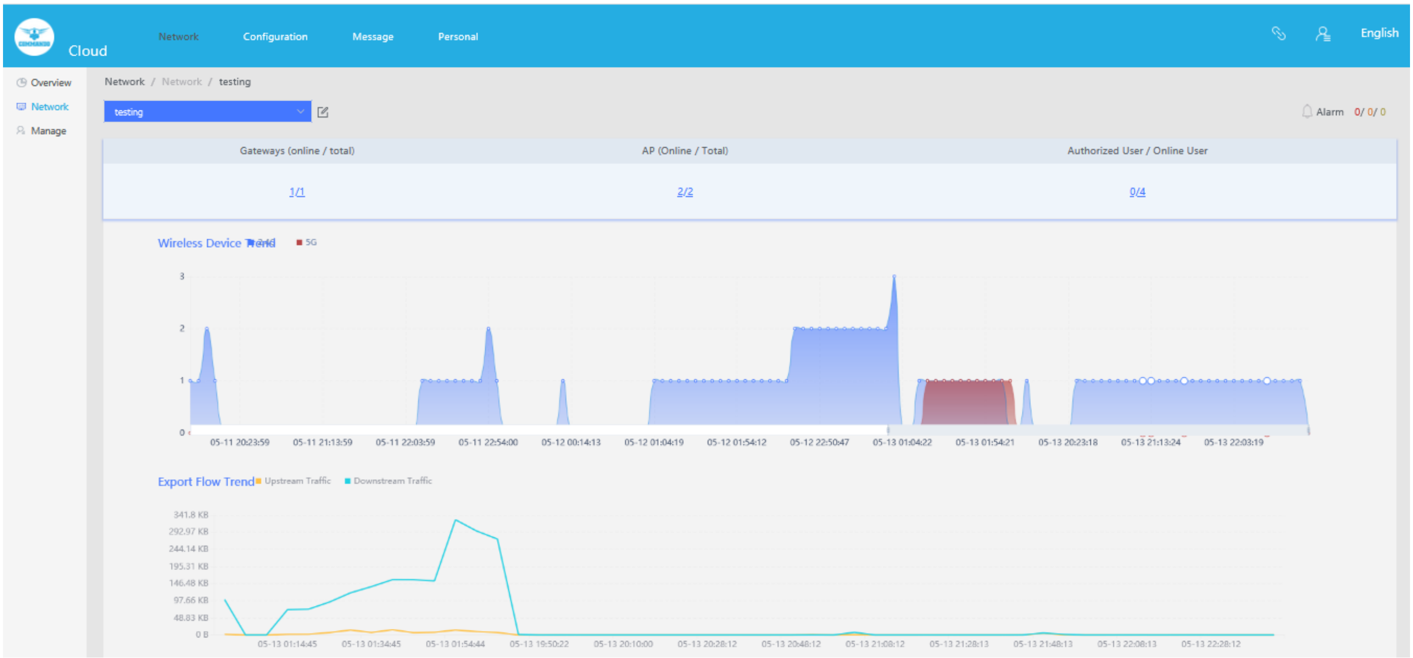
	Name	Status	GWID	Export IP	Version	Status	Config
⌄	testing	Online	247ce0632ec88bde3e5053d6d00818e8	182.59.62.184 (印度)	3.4.5.CMD-COS-v1.01 x32 Build202011161736	Closed	Config

Outline:
Online Users:4
Today's Certification 0

Routing Maintenance: Direct Login Upgrade Restart Untie

Total 1 10/page ‹ 1 › Go to 1

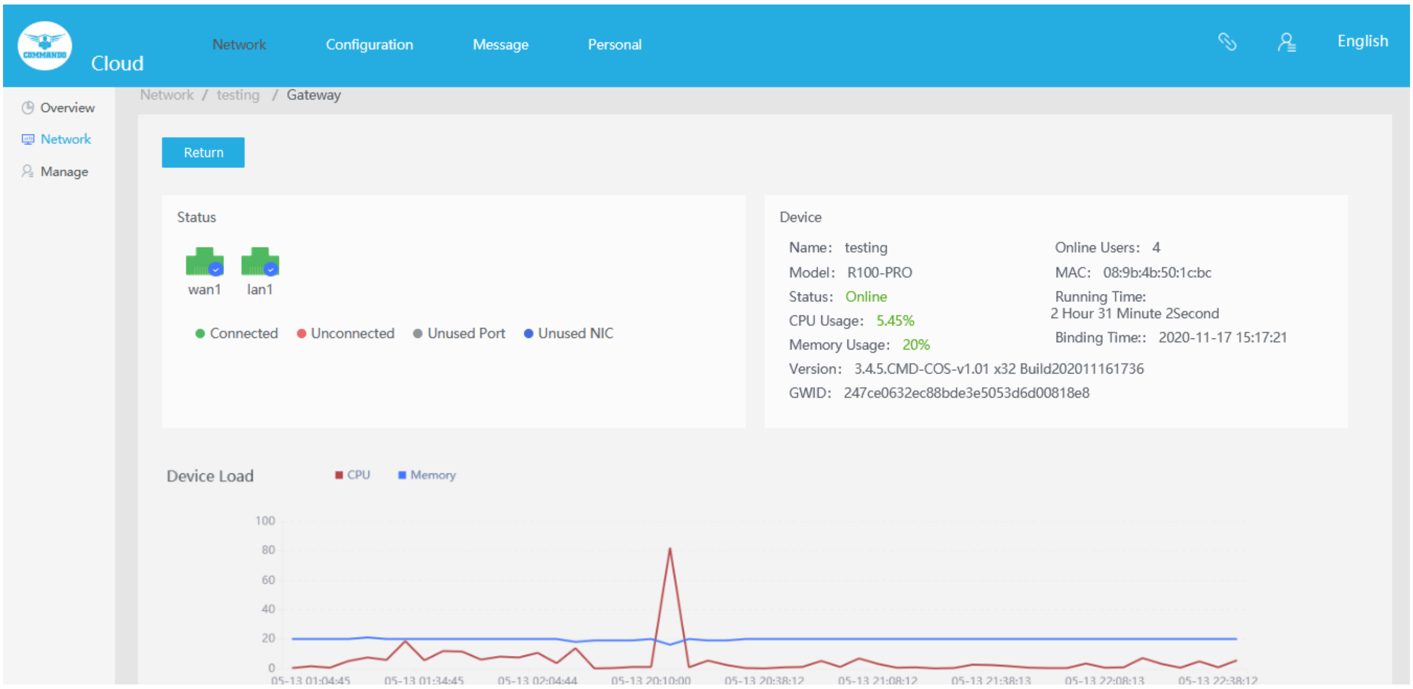
Fig 12.2.2 Bulk configuration page



Network / Network / testing

Gateways (online / total)	AP (Online / Total)	Authorized User / Online User
1/1	2/2	0/4

Fig 12.2.3 Network Devices listed in Cloud page



Status

wan1 lan1

● Connected ● Unconnected ● Unused Port ● Unused NIC

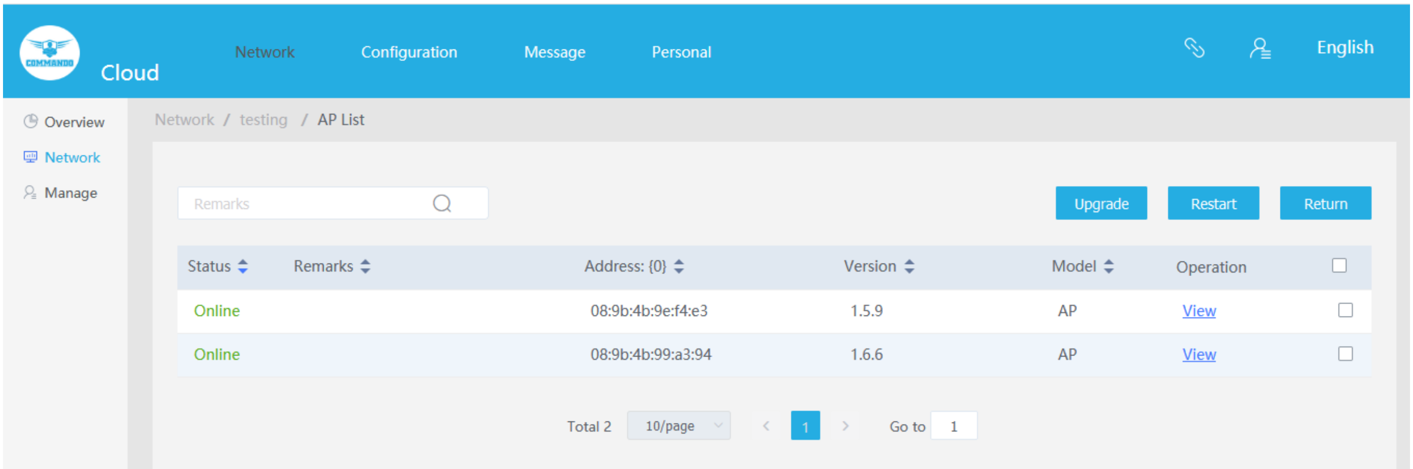
Device

Name: testing
Model: R100-PRO
Status: Online
CPU Usage: 5.45%
Memory Usage: 20%
Version: 3.4.5.CMD-COS-v1.01 x32 Build202011161736
GWID: 247ce0632ec88bde3e5053d6d00818e8

Online Users: 4
MAC: 08:9b:4b:50:1c:bc
Running Time:
2 Hour 31 Minute 2Second
Binding Time:: 2020-11-17 15:17:21

Device Load

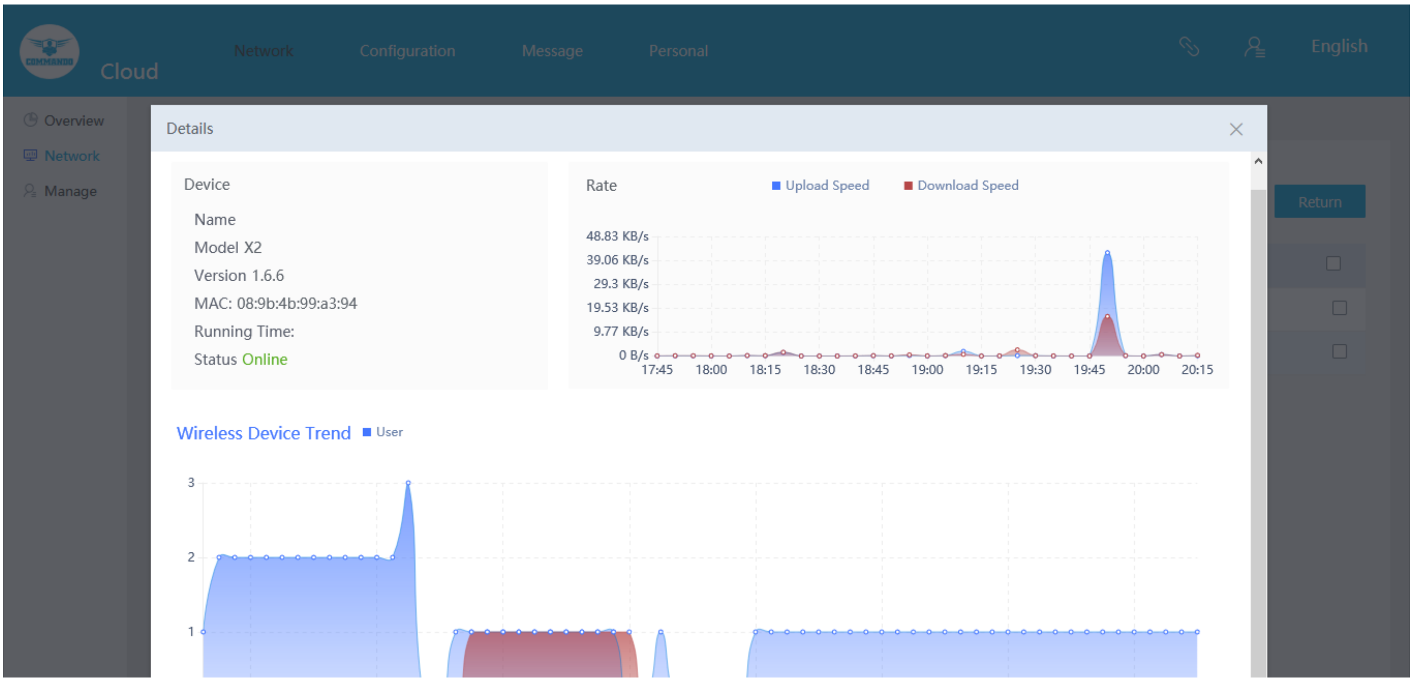
Fig 12.2.4 Gateway page



Status	Remarks	Address: {0}	Version	Model	Operation	□
Online		08:9b:4b:9e:f4:e3	1.5.9	AP	View	□
Online		08:9b:4b:99:a3:94	1.6.6	AP	View	□

Total 2 10/page < 1 > Go to 1

Fig 12.2.5 AP List page



Details

Device

Name

Model X2

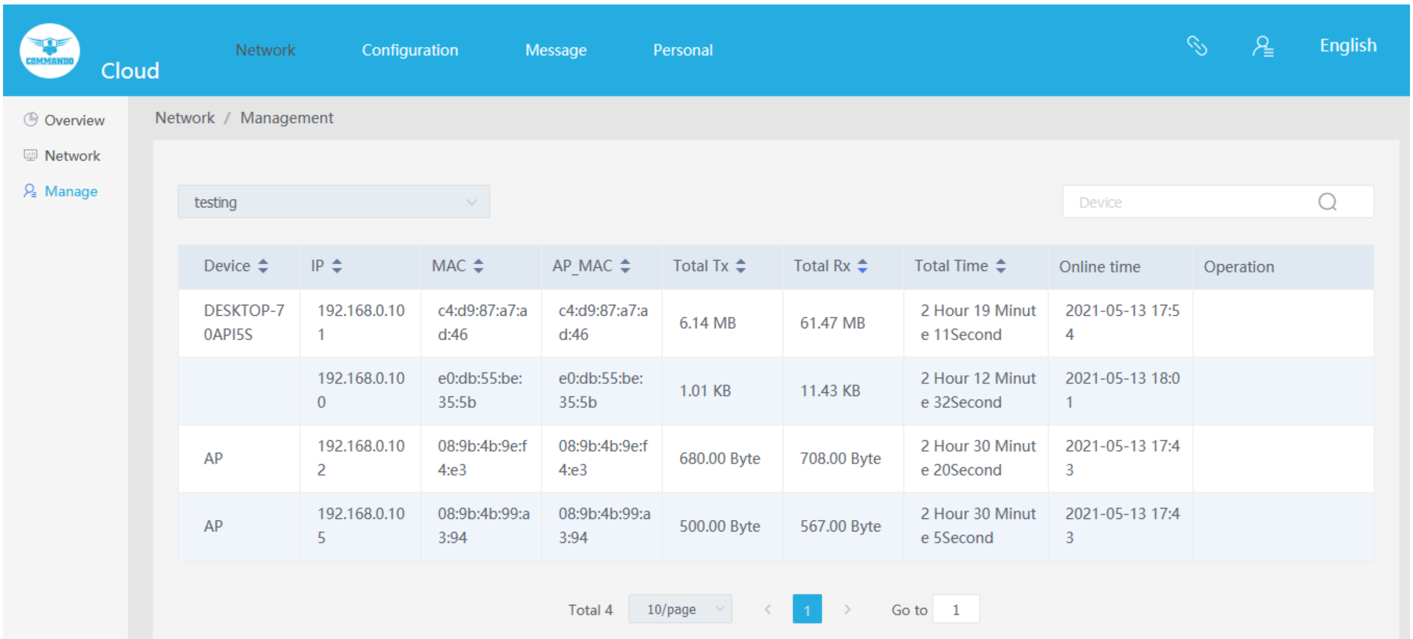
Version 1.6.6

MAC: 08:9b:4b:99:a3:94

Running Time:

Status Online

Fig 12.2.5 Bulk configuration for particular AP Device page



Network / Management

testing

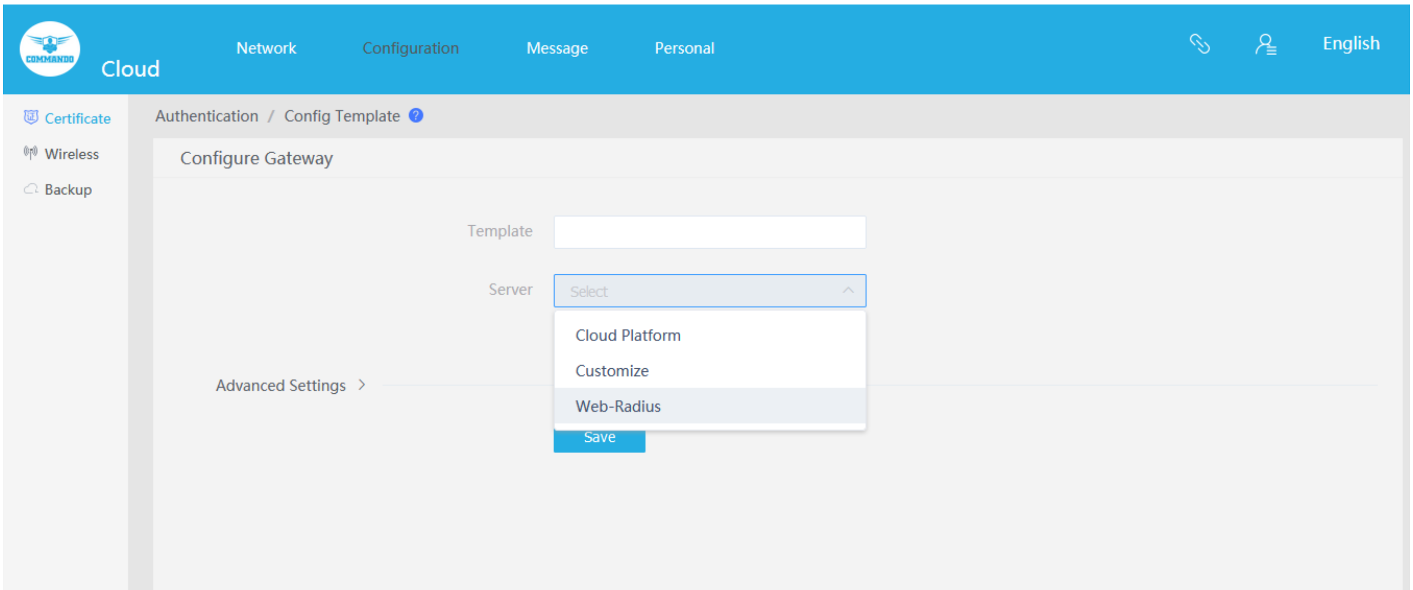
Device	IP	MAC	AP_MAC	Total Tx	Total Rx	Total Time	Online time	Operation
DESKTOP-70API5S	192.168.0.101	c4:d9:87:a7:ad:46	c4:d9:87:a7:ad:46	6.14 MB	61.47 MB	2 Hour 19 Minute 11Second	2021-05-13 17:54	
	192.168.0.100	e0:db:55:be:35:5b	e0:db:55:be:35:5b	1.01 KB	11.43 KB	2 Hour 12 Minute 32Second	2021-05-13 18:01	
AP	192.168.0.102	08:9b:4b:9e:f4:e3	08:9b:4b:9e:f4:e3	680.00 Byte	708.00 Byte	2 Hour 30 Minute 20Second	2021-05-13 17:43	
AP	192.168.0.105	08:9b:4b:99:a3:94	08:9b:4b:99:a3:94	500.00 Byte	567.00 Byte	2 Hour 30 Minute 5Second	2021-05-13 17:43	

Total 4 10/page < 1 > Go to 1

Fig 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.



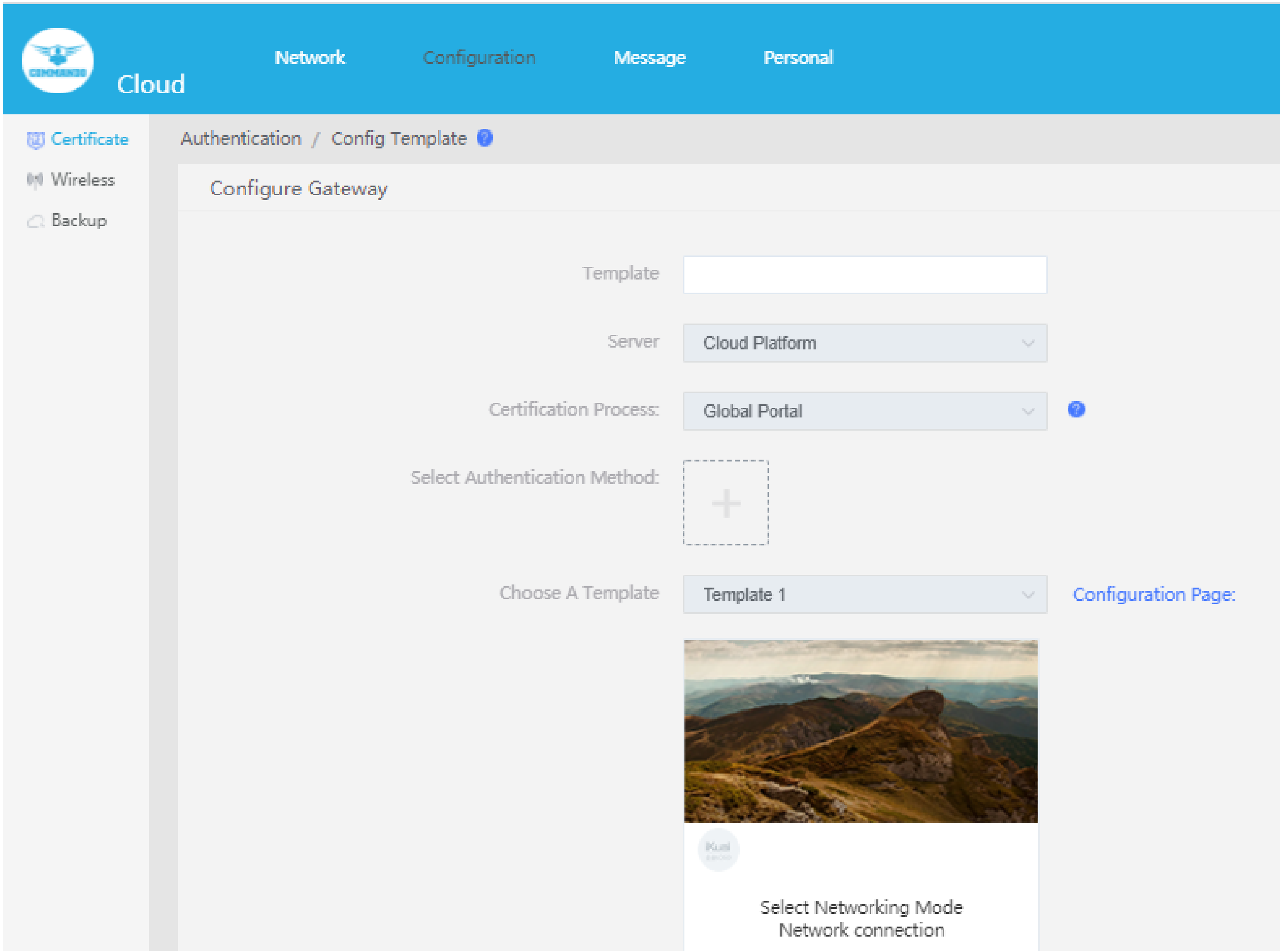
Authentication / Config Template

Configure Gateway

Template

Server: Select

Fig 12.3.1 Default Authentication page



Authentication / Config Template

Configure Gateway

Template

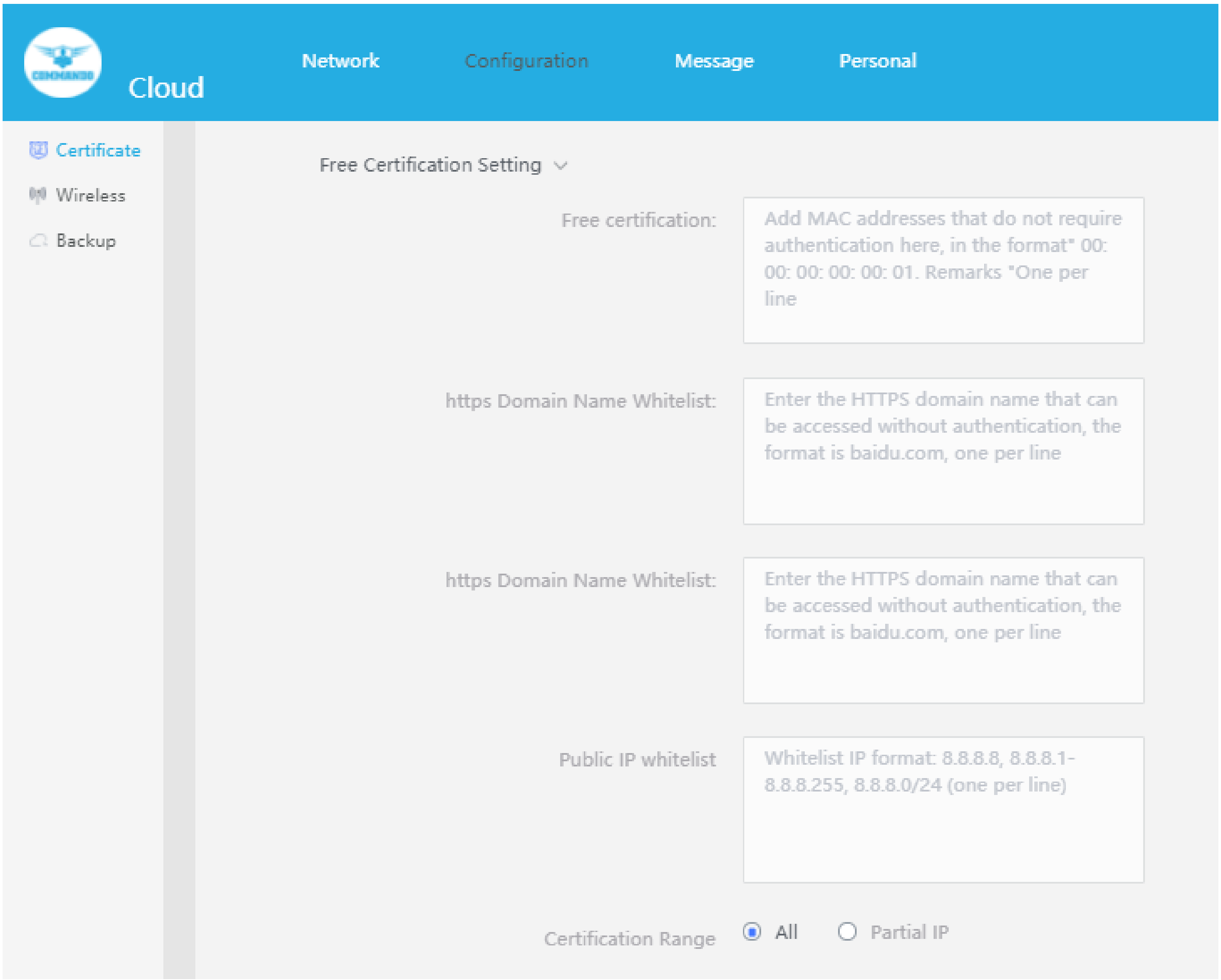
Server: Cloud Platform

Certification Process: Global Portal

Select Authentication Method:

Choose A Template: Template 1

Fig 12.3.2 Default Cloud platform configure gateway page



Free Certification Setting

Free certification: Add MAC addresses that do not require authentication here, in the format" 00: 00: 00: 00: 00: 01. Remarks "One per line

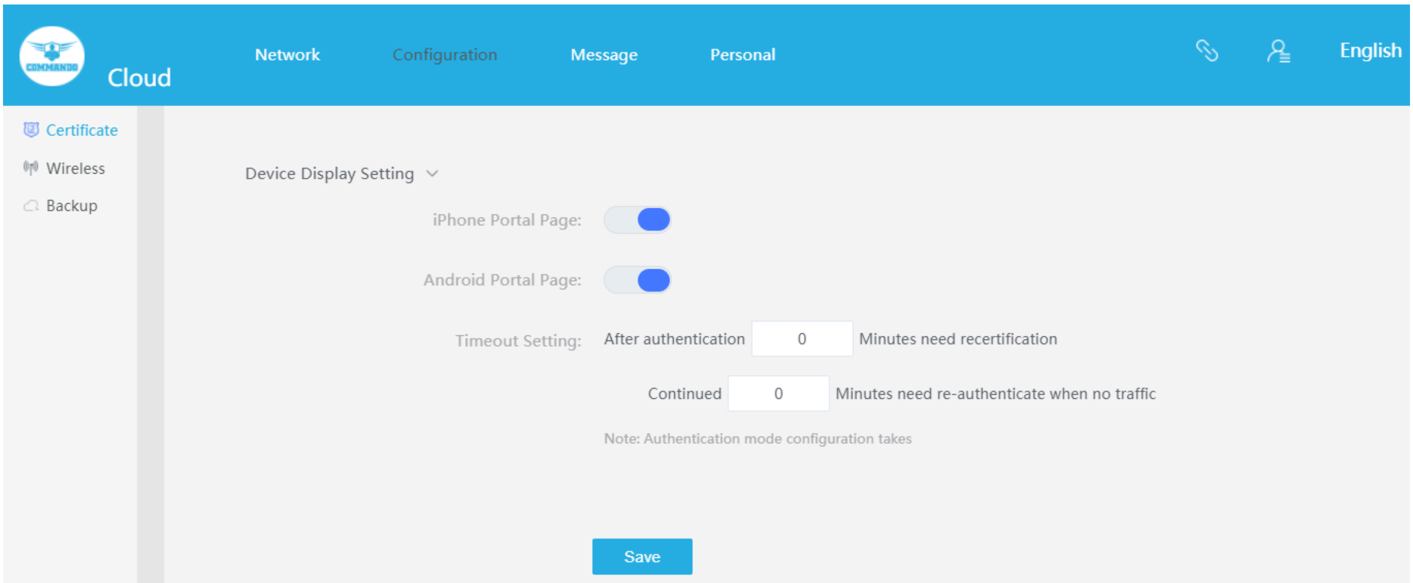
https Domain Name Whitelist: Enter the HTTPS domain name that can be accessed without authentication, the format is baidu.com, one per line

https Domain Name Whitelist: Enter the HTTPS domain name that can be accessed without authentication, the format is baidu.com, one per line

Public IP whitelist Whitelist IP format: 8.8.8.8, 8.8.8.1-8.8.8.255, 8.8.8.0/24 (one per line)

Certification Range ● All ○ Partial IP

Fig 12.3.3 Default Authentication Free certification setting page



Device Display Setting

iPhone Portal Page: on

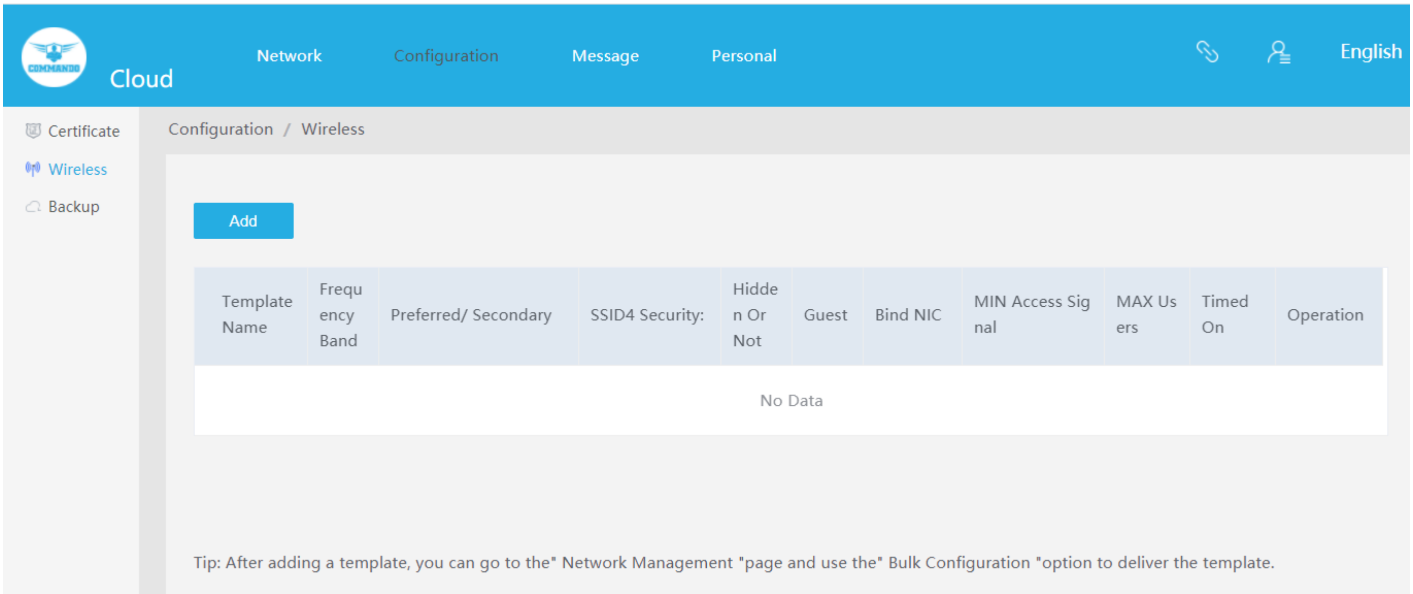
Android Portal Page: on

Timeout Setting: After authentication 0 Minutes need recertification

Continued 0 Minutes need re-authenticate when no traffic

Note: Authentication mode configuration takes

Fig 12.3.4 Default Authentication Device Display setting page

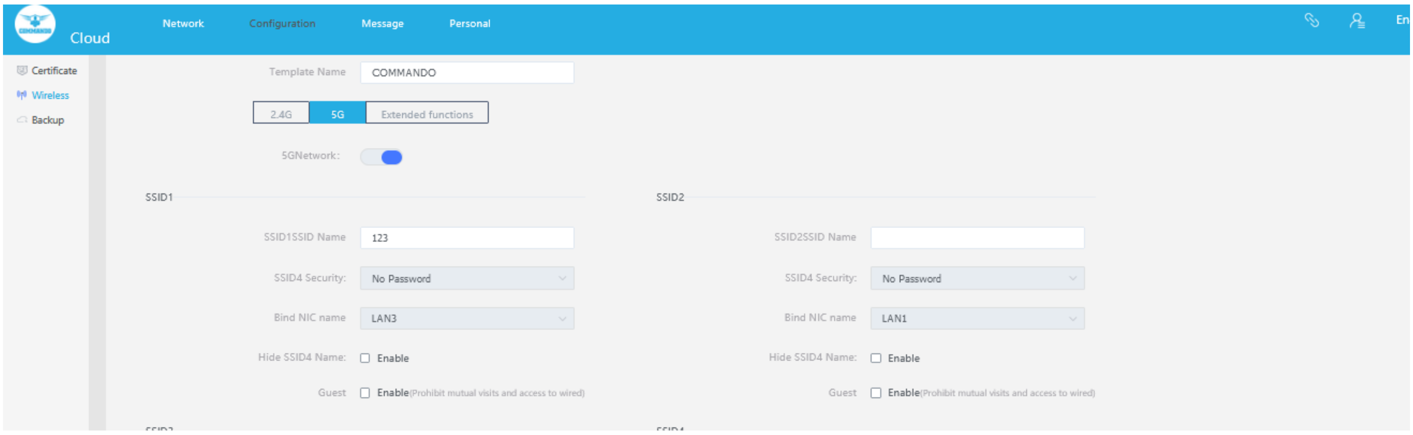


Configuration / Wireless

Template Name	Frequency Band	Preferred/ Secondary	SSID4 Security:	Hidden Or Not	Guest	Bind NIC	MIN Access Signal	MAX Users	Timed On	Operation
No Data										

Tip: After adding a template, you can go to the" Network Management "page and use the" Bulk Configuration "option to deliver the template.

Fig 12.3.5 Default Wireless add setting page



Template Name: COMMANDO

5GNetwork: on

SSID1

SSID1SSID Name: 123

SSID4 Security: No Password

Bind NIC name: LAN3

Hide SSID4 Name: □ Enable

Guest: □ Enable(Prohibit mutual visits and access to wired)

SSID2

SSID2SSID Name:

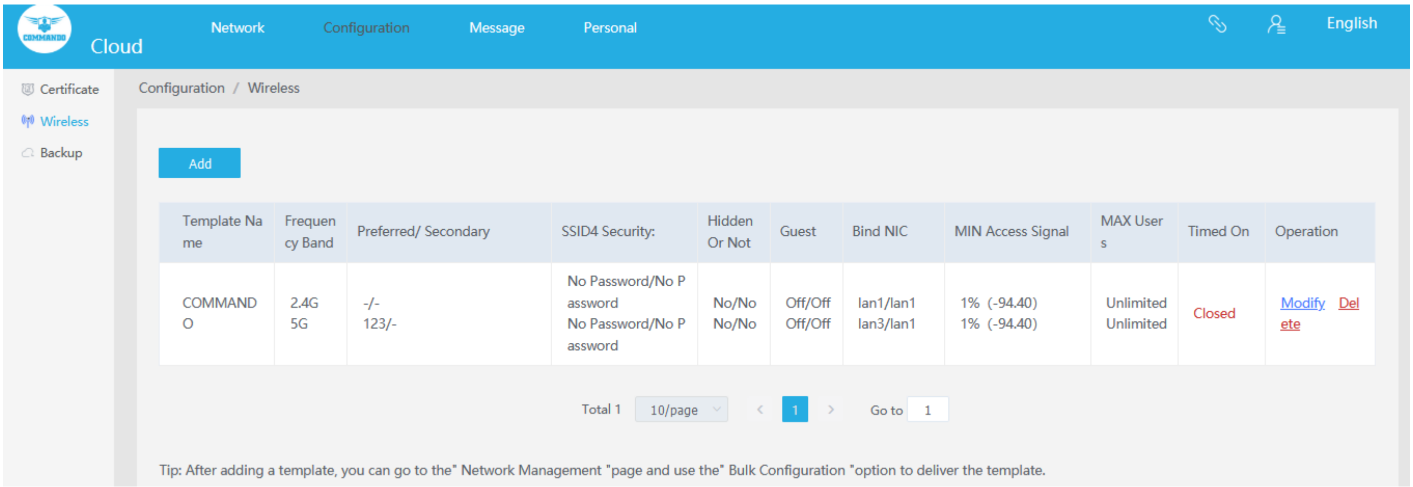
SSID4 Security: No Password

Bind NIC name: LAN1

Hide SSID4 Name: □ Enable

Guest: □ Enable(Prohibit mutual visits and access to wired)

Fig 12.3.6 Add 5G Wireless setting page



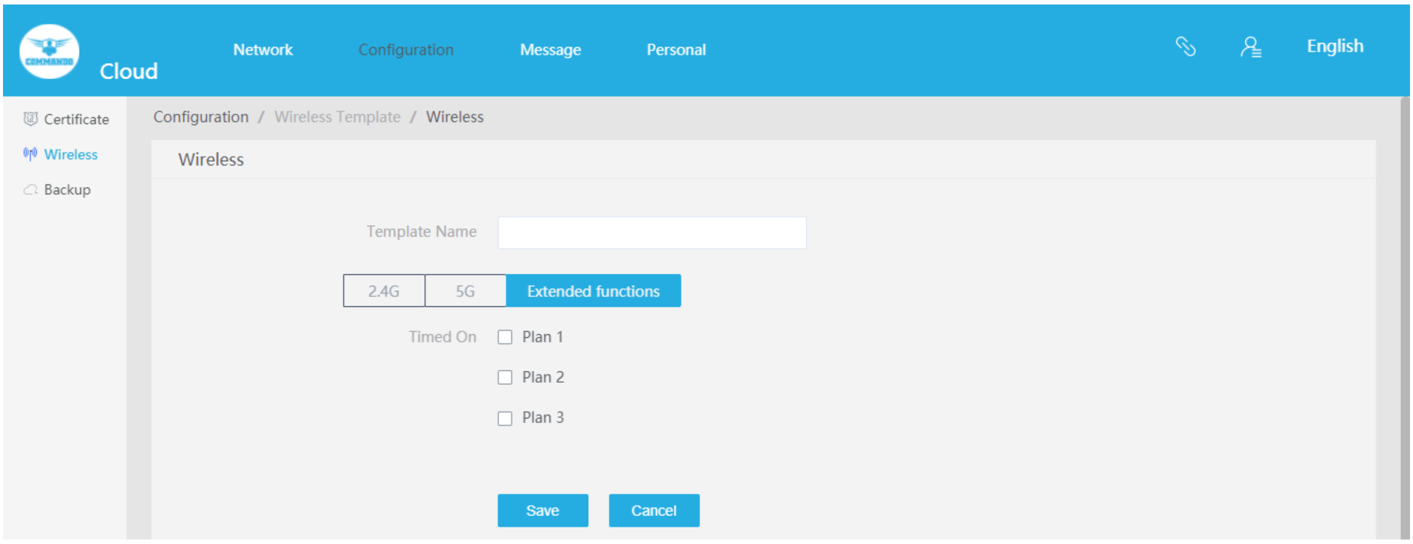
Configuration / Wireless

Template Name	Frequency Band	Preferred/ Secondary	SSID4 Security:	Hidden Or Not	Guest	Bind NIC	MIN Access Signal	MAX Users	Timed On	Operation
COMMANDO	2.4G 5G	-/- 123/-	No Password/No Password No Password/No Password	No/No No/No	Off/Off Off/Off	lan1/lan1 lan3/lan1	1% (-94.40) 1% (-94.40)	Unlimited Unlimited	Closed	Modify Delete

Total 1 10/page < 1 > Go to 1

Tip: After adding a template, you can go to the" Network Management "page and use the" Bulk Configuration "option to deliver the template.

Fig 12.3.6 Wireless Configuration setting page



Configuration / Wireless Template / Wireless

Wireless

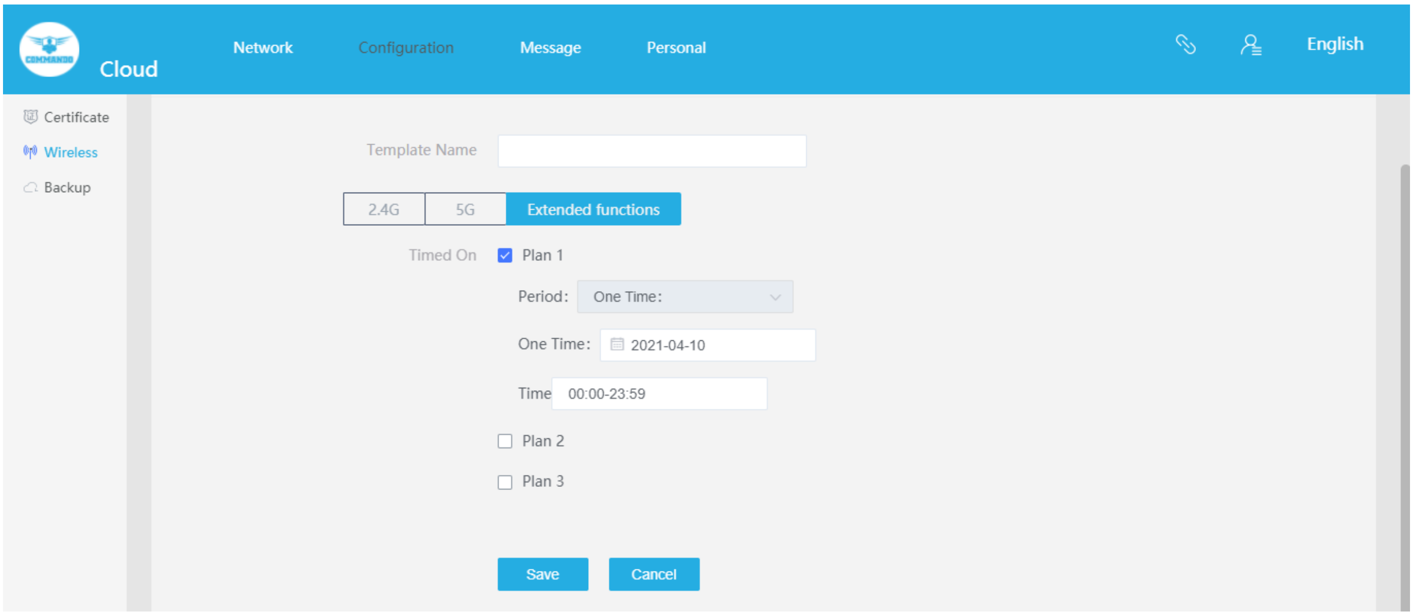
Template Name

Timed On □ Plan 1

□ Plan 2

□ Plan 3

Fig 12.3.7 Default Wireless Configuration Extended function setting page



Template Name

Timed On ☑ Plan 1

Period: One Time:

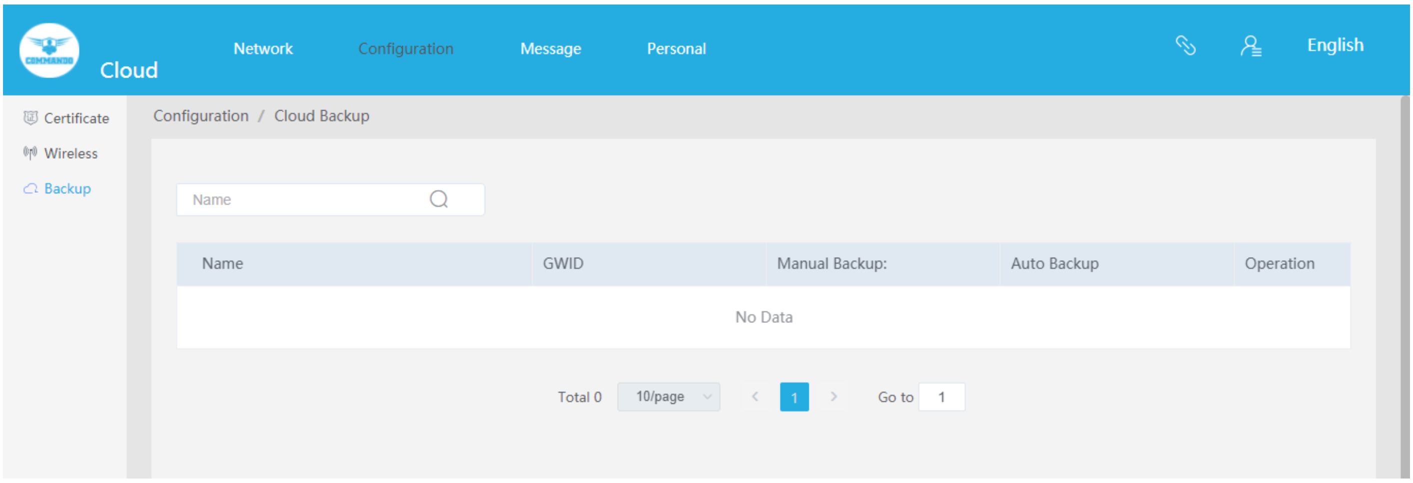
One Time: 2021-04-10

Time 00:00-23:59

□ Plan 2

□ Plan 3

Fig 12.3.8 Wireless Configuration Extended function for Plan 1 setting page

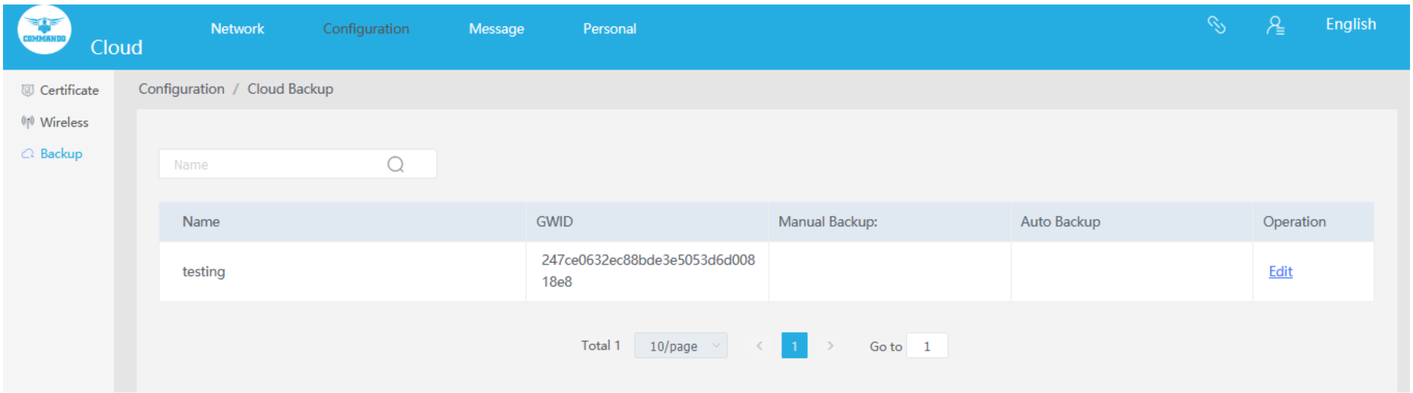


Configuration / Cloud Backup

Name	GWID	Manual Backup:	Auto Backup	Operation
No Data				

Total 0 10/page ‹ 1 › Go to 1

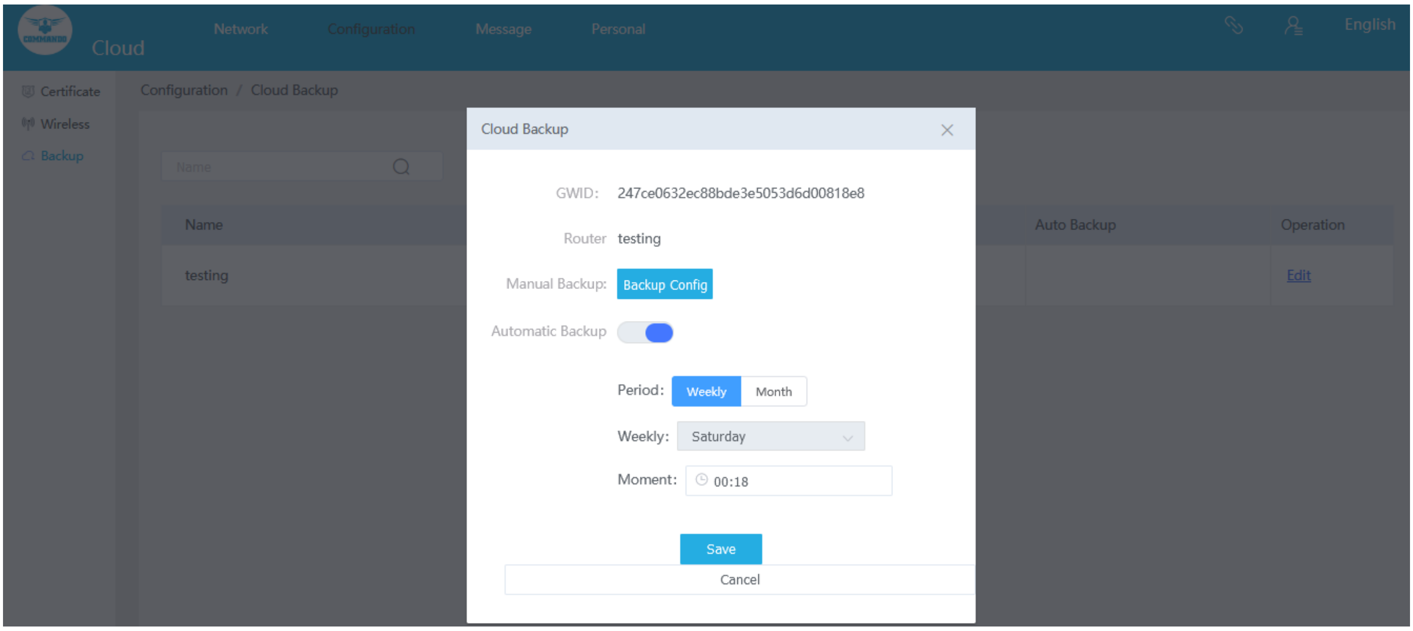
Fig 12.3.9 Default Configuration backup setting page



Name	GWID	Manual Backup:	Auto Backup	Operation
testing	247ce0632ec88bde3e5053d6d00818e8			Edit

Total 1 10/page 1 Go to 1

Fig 12.3.10 Backup Configuration setting page



GWID: 247ce0632ec88bde3e5053d6d00818e8

Router testing

Manual Backup: Backup Config

Automatic Backup

Period: Weekly Month

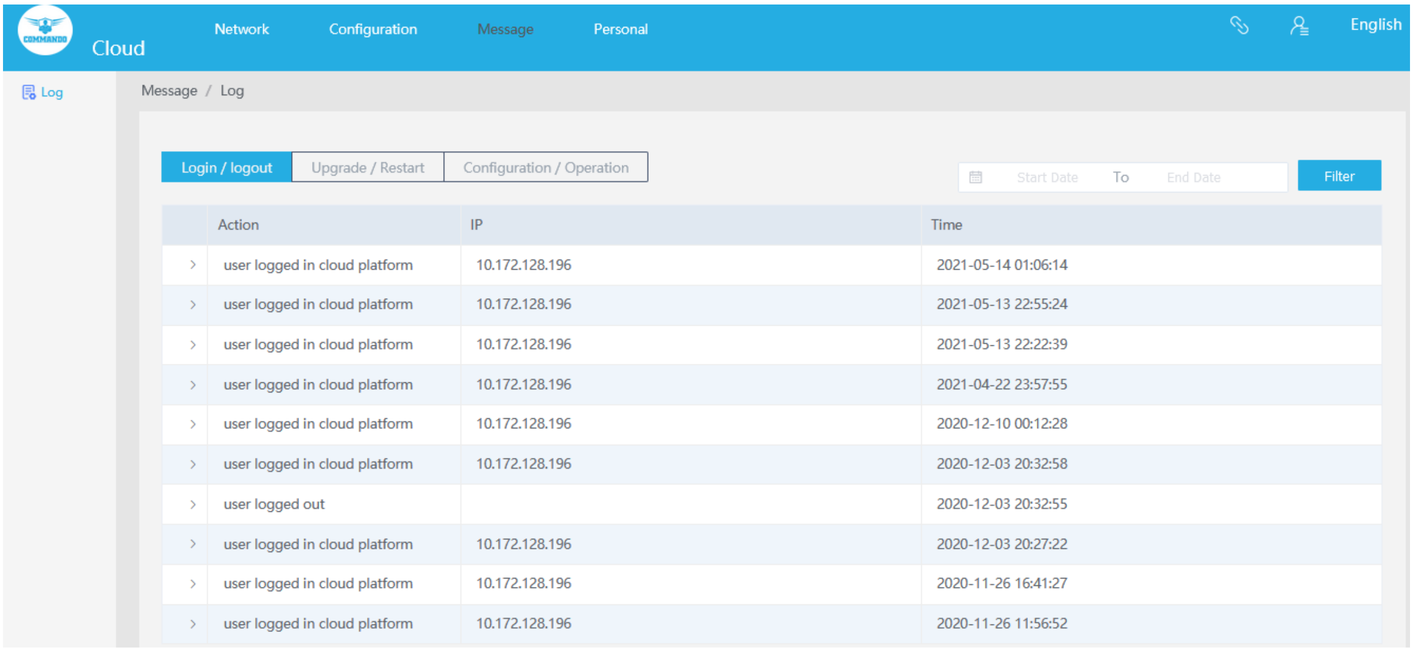
Weekly: Saturday

Moment: 00:18

Fig 12.3.11 Cloud Backup Configuration setting page

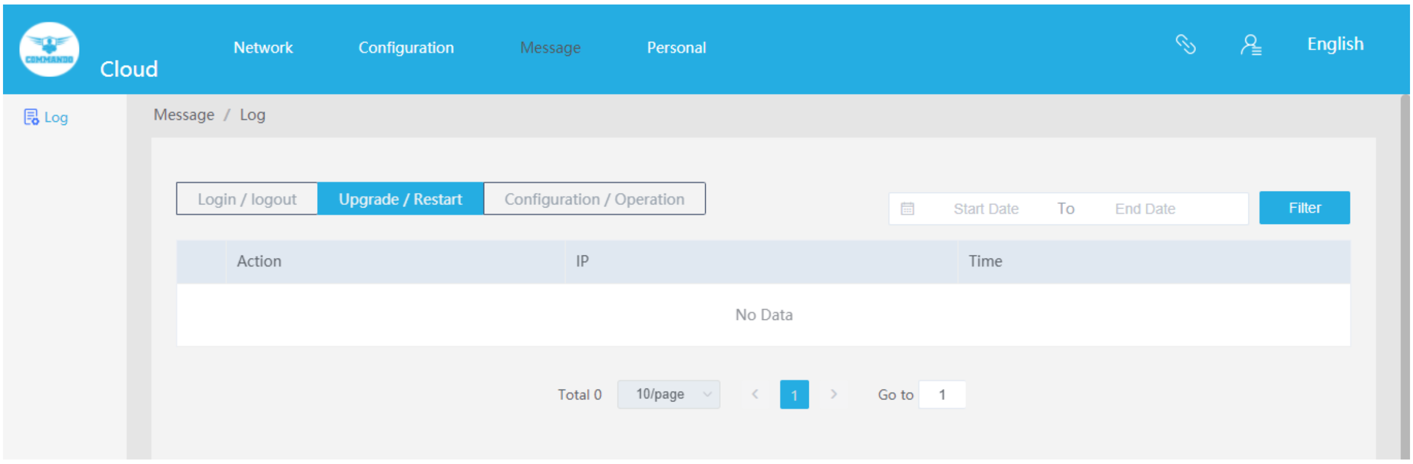
12.4 Message

Messages can be Log, Login or logout, Upgrade or Restart and Configuration or Operation.



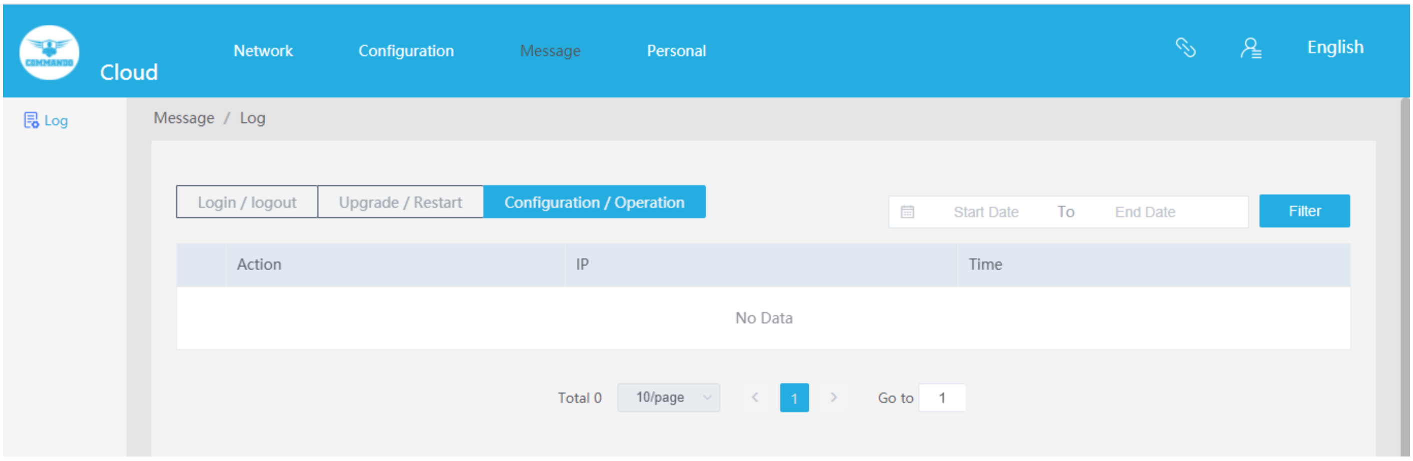
	Action	IP	Time
›	user logged in cloud platform	10.172.128.196	2021-05-14 01:06:14
›	user logged in cloud platform	10.172.128.196	2021-05-13 22:55:24
›	user logged in cloud platform	10.172.128.196	2021-05-13 22:22:39
›	user logged in cloud platform	10.172.128.196	2021-04-22 23:57:55
›	user logged in cloud 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



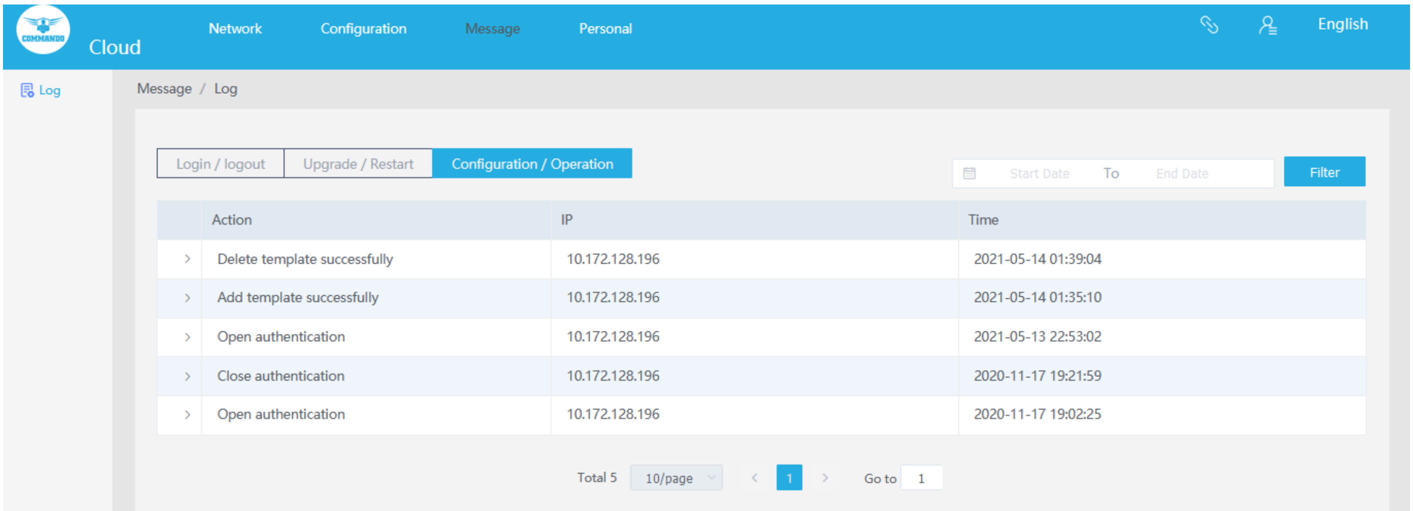
	Action	IP	Time
		No Data	

Fig 12.4.2 Default Upgrade and Restart page



	Action	IP	Time
		No Data	

Fig 12.4.3 Default Configuration and operation page



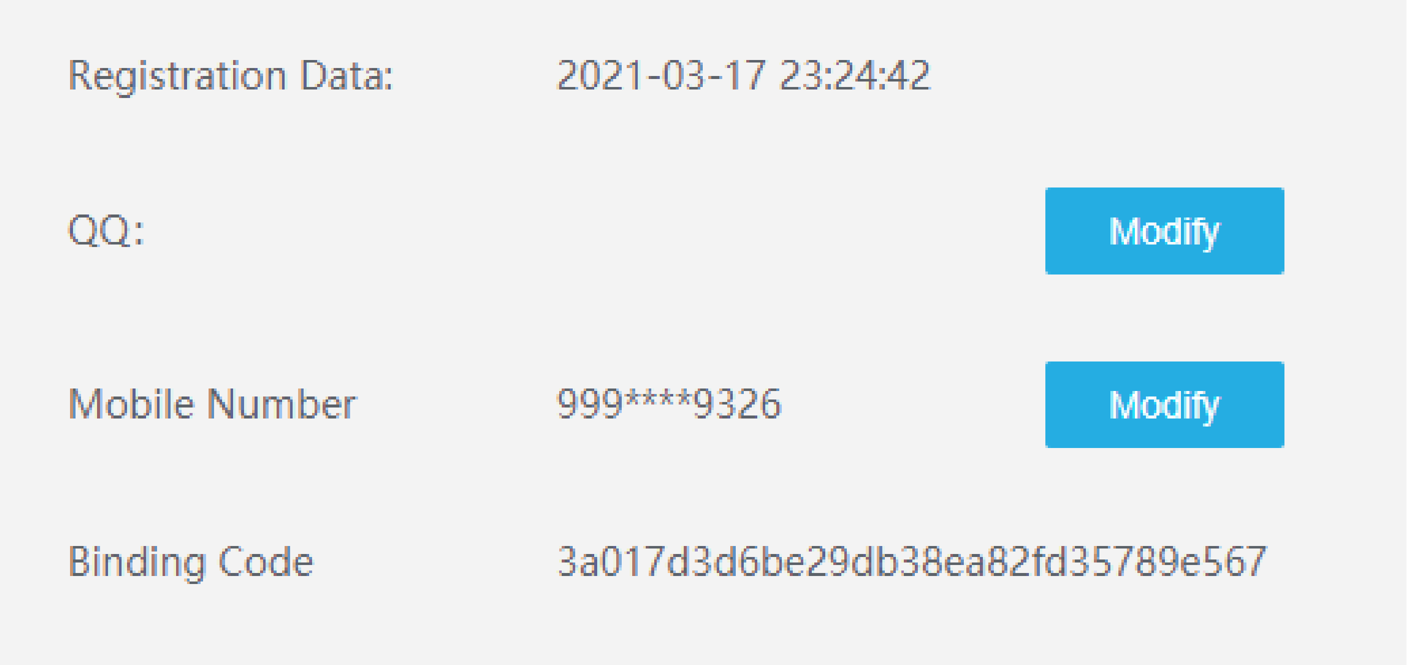
Action	IP	Time
Delete template successfully	10.172.128.196	2021-05-14 01:39:04
Add template successfully	10.172.128.196	2021-05-14 01:35:10
Open authentication	10.172.128.196	2021-05-13 22:53:02
Close authentication	10.172.128.196	2020-11-17 19:21:59
Open authentication	10.172.128.196	2020-11-17 19:02:25

Total 5 10/page 1 Go to 1

Fig 12.4.4 Configuration and operation page

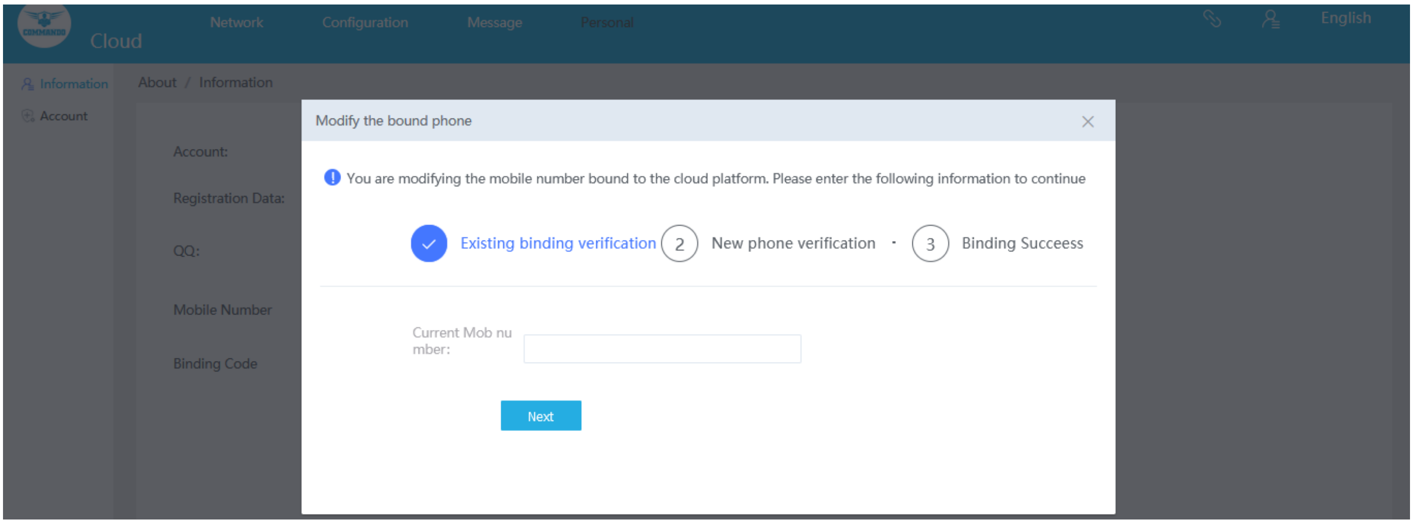
12.5 Personal

Personal Information is available on this page.



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



Modify the bound phone

You are modifying the mobile number bound to the cloud platform. Please enter the following information to continue

✓ Existing binding verification ② New phone verification ③ Binding Succeess

Current Mob number:

Next

Fig 12.5.2 Modify Personal Information page