

### 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 Passthrough, 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/IPv-	4) Properties
General	
You can get IP settings assigned auto this capability. Otherwise, you need for the appropriate IP settings.	omatically if your network supports to ask your network administrator
Obtain an IP address automatic	ally
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 auto	omatically
Use the following DNS server ac	dresses:
Preferred DNS server:	
Alternate DNS server:	· · · ·
Validate settings upon exit	Advanced
	OK Cancel

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.

Q 192.168.1.1		
	COMIMANDO	
	🛆 User Name	
	Password	
	Login	
	Remember password	

### 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.

$\overleftarrow{\leftarrow}$ $\rightarrow$ $\overleftarrow{C}$ $\overleftarrow{\omega}$	0 🖉 🗝 192.168.1.1/#/system-overview			679	6) ⊠ ☆	III\ E	) 🔹 =
2 CMD-COS-V1.01						🗗 û 🗛	🚊 English
Er System Ov	rview				🔷 CPU: 1	1.24% 🔛 MEM: 16% ↑ TX: 0.00 E	3/s 🤳 RX: 0.00 B/s
System     Overview	COMMANDO Rate Status		Connection Status	0	0	Wired: 1	
🔅 System Setup	Running: 9m 4s		Online Host	U Connection Count	U Auth Count	Wireless: 0	
Image: Network         Network           Ital:         Flow Control	Interface Status		AC status	_	Frequency band	~	
Controller	0 1 101 WAN Enabled LAN Enabled DHCP Pool Addresses			(P)	(R)		
Behavior Eirewall	want kant		AP connection is normal O	AP connected	2.4G access	5G access	
Advanced application	Last 30 minutes traffic analysis	Last 5 minute's Tx/Rx Rates ③				=	
(h) Log	OB Total Bytes	0 0 1501 1502 0 Total Re Rate(X8/s) 20	1503 O HTTP O Video O Game O Down	1504 load o Transport o IM o Comm	1505 ion O Others O Test O Unknow	15:06	
		0	15:03	15:04	15:05	15:06	

Fig 3. Default System Overview page

2	CMD-COS-v1.01							🕹 û 🌩 2	2 English
	≡<	System Overview					🔷 CPU: 0.5	0% 🛄 MEM: 16% ↑ TX: 27.00 B/s ,	RX: 27.00 B/s
ଚ	System Overview	COMMANDO	Rate Status		Connection Status				Â
<b>6</b> 2	Monitoring	Connected wan	↑27.0 <sub>B/s</sub>		2	2	0	Wired: 2 Wireless: 0	
÷	System Setup	Kuming, mom 495	↓ ∠ / .U B/s		Unine Host	Connection Count	Auth Count		
몲	Network	Interface Status		_	AC status		Frequency band		
<u>111</u>	Flow Control	1 1	0			$\frown$		$\frown$	
2	Access Controller	WAN Enabled LAN Enabled	DHCP Pool Addresses			(@)	( 🛜 )	( 🛜 )	
8.	Authentication				AP connection is normal	AP connection disconnected	2 4G access	5G arress	
₩	Behavior				0	0	0	0	
⊞	Firewall	wan1 lan1							
☑	Advanced application	Last 30 minutes traffic analysis	Last 30 Minutes	Last 5 minute's Tx/Rx Rates 😰					
8	Services			Tx Rate(KB/s)					
ß	Log	ОВ	HTTP Video Game Download Transport	0.1	13;40	13:41	13:42	13:43	
		Total Bytes	Common Others Test Unknown	o 1 Rx Rate(KI/d) 0.05 0 13:38 13:39	otan o HTP o Video o Game o Dowr 13:40	nicear o transport o IM o Commi	on o others o test o Unknow	m 1343	
				COMP	/ANDO Networks				

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

CMD-COS-	101	් 🗘 🗘 ළ English
≡́	System Overview	=☐: CPU: 1.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
System Overview     Monitoring     System Setu	COMMANDO Connected WAN Running: 1h 7m 21s  Rate Status $0 B/s$ $0 B/s$	Connection Status 1 2 0 Wired: 1 Online Host Connection Count Auth Count Wireless: 0
Hit Flow Control Controller	Interface Status Enabled LAN Enabled DHCP Pool Addresses	AC status Frequency band
∽ Behavior ⊞ Firewall	wan1 lan1	AP connection is AP connection 2.4G access 5G access normal disconnected 0 0
Advanced application		Last 30 minutes traffic analysis Last 30 Minutes V
ြို Log		

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.

	Connection Status:	Connected 1052d	15h	9m
	Type:	DHCP		
	IP:	192.168.1.38		
Sub	onet 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 <	Network > Interfaces	± CPU: 13.50% 🖵 MEM: 18% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
			External network settings wan1	• ×
63	Overview	Interfaces		
<u>-</u>	Monitoring	рнср 🗸		
ැරිූ	System Setup	DNS V	Select Interface:	veth5   wan1   08:24:7c:e0:63:33   Ralink MT7530 10/100/1000 Etherne V Unbind
چە 1	ojstem cetap		Access Mode:	DHCP (Dynamic Assigned) $\checkmark$
品	Network	IP/MAC Group 🗸 🗸	Status:	Connected Disconnect rebroadcast
†∔†	Flow Control	Static Routes 🛛 🗸	IP Address:	192.168.1.38
<b>P</b>	Access	VLAN		
	Controller		Subnet Mask:	255.255.255.0
<u>8</u> =	Authentication	VPN Client 🗸 🗸	Gateway:	192.168.1.1
⇆	Behavior	UPNP 🗸	Preferred DNS :	192.168.1.1
臣	Firewall	NAT	Alternative DNS:	
Ţ	Advanced application	Port Mapping $\sim$	Default Gateway:	Set this line as the default gateway (When you have multiple ISP lines, please select one as the default gateway)
0%	Services	IPv6 V	Failover:	Switch if Line Dropped (No need to use when only 1 ISP line)
ſĿ	Log	IGMP Agent	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

СВИОНАЯ	CMD-COS-v1.01							<u>ර් ර                                  </u>	English
	≡<	Network <	Network > D	NS > Multiline DNS			≣ <mark>0</mark> ≣ CPU: 3.47%	MEM: 18% ↑ TX: 0.00 B/s 🤳	RX: 0.00 B/s
6	System	Interfaces	Multiline D	NS Settings					
<u>,</u>	Overview	interfaces							
₩	Monitoring	DHCP 🗸 🗸		Q		Add	Import Export	Enable Disable	Delete
ţĊ	System Setup	DNS ^	Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions	
品	Network	DNS	wan1	< 8.8.8.8	114.114.114.114		Editing	OK Cancel	
†∔†	Flow Control	Multiline DNS	Chowing 1 o	f 0 records					
<b></b>	Access Controller	IP/MAC Group \vee	Showing 10	i o records					
<u>8</u>	Authentication	Static Routes 🛛 🗸	Help:	DNS Proxy Mode: effective when local DNS cache for acceleration.	client set the gateway address as	s DNS; Forced DNS Proxy	y: force the client to use the	DNS Proxy service; DNS Cache N	Node: use
₩	Behavior	VLAN							
田	Firewall	VPN Client $$							
Ţ	Advanced application	UPNP 🗸							
0%	Services	NAT							
ſð	Log	Port Mapping $$							

Fig 8. Multi DNS server Setting in R100.

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



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

### **Traffic Analysis**

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



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



Fig 11. Traffic analysis for video application for 1 day



### Fig 12. Transmission and Receiving Rate Graphs

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

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



### 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

	CMD-COS-v1.01							් ර ර	၌ <u>၉</u> English
	=<	System Setup	System Setup	> Administration > User Accounts			≣ <b>∷</b> CPU: 0.99% 🛄	MEM: 18% ↑ TX: 0	0.00 B/s \downarrow RX: 0.00 B/s
•	Sustem		User Accou	nts					
69	Overview	Basic Setting							
₩	Monitoring	Disk management					Add	Enable D	isable Delete
ŝ	System Setup	Cloud Account	Username	Password	Right group	Safe IP addr	Status	Actions	
-0-		Advanced	admin	***	Superadministrator	0.0.0/0	Enabled	Edit	
葩	Network	Settings	Showing 1 o	f 1 records		DerDa	a 20 × Rows		1 /1Pages Jump
ţţţ	Flow Control	Administration ^	showing ro	rrecords		reiray	Je 20 + Nows //	. 🗙 📫 / //	1 / Trages 2000p
<b></b>	Access Controller	User Accounts	Help:	1.please configure carefully to allov	w access to IP (default is not limi	ted), input format supp	port: 192.168.1.1192.168.1.1-1	192.168.1.200192.168.	1.0/24192.168.1.0
<u>&amp;=</u>	Authentication	Remote Access		2.when adding the same privileged	account, copying can quickly co	omplete the permission	s configuration		
<b>↓</b> ≯	Behavior	Upgrading 🗸 🗸							
Ħ	Firewall	Reboot							
Ţ	Advanced application								
0% 00	Services								
ß	Log								

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.

	د در									
	=<	System Setup	System Setup > Administration > User Ad	counts	📮 CPU: 13.75% 🛄 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s					
~	Sustem	· ·	Edit		×					
6-3	Overview	Basic Setting								
₩	Monitoring	Disk management								
ţĊ}	System Setup	Cloud Account	Username:	COMMANDO	*					
品	Network	Advanced 🗸 🗸	Password :	*****						
<b>+1</b> 4	Flow Control		Confirm password:	•••••	*					
		Automistration	Safe IP addr:	0.0.0/0						
<b></b>	Access Controller	User Accounts	Default permission:	Read Write ~						
& <u>-</u>	Authentication	Remote Access	Login Status Timeout:	120 * minute						
⇒	Behavior	Upgrading 🗸 🗸	Login Password	OpenChange Password Periodically						
臣	Firewall	Reboot	Security:							
Ţ	Advanced application			Save Cancel						
0%	Services									
ſð	Log									

Fig 15. Editing User Account setting

COMMANDO	
COMMANDO	
<u>A</u> •••••••••	
Login	
Remember password	

Fig 16. Logging with New account

	>								0 5 5
санона	CMD-COS-v1.01								English
	=<	System Setup	System Setup	> Administration > User Accounts			📲 CPU: 0.75%	MEM: 19% ↑ TX: 0.	00 B/s \downarrow RX: 0.00 B/s
	-	-)	User Accour	nts					
(	System Overview	Basic Setting							
₩	Monitoring	Disk management					Add	Enable Dis	able Delete
ŝ	System Setup	Cloud Account	Username	Password	Right group	Safe IP addr	Status	Actions	
品	Network	Advanced 🗸 🗸	COMMANDO	) *****	Superadministrator	0.0.0/0	Enabled	Edit	
†∔†	Flow Control	Administration ^	Showing 1 of	f 1 records		PerPa	ige 20 🗸 Rows ≪	( < 1 > »	1 /1Pages Jump
<b>(</b>	Access Controller	User Accounts	Help:	1.please configure carefully to allo /255.255.255.0	w access to IP (default is not limi	ited), input format sup	port: 192.168.1.1192.168.1.1-	192.168.1.200192.168.1	.0/24192.168.1.0
<u>&amp;</u> =	Authentication	Remote Access		2.when adding the same privileged	d account, copying can quickly c	omplete the permission	ns configuration		
ţ	Behavior	Upgrading 🗸 🗸							
田	Firewall	Reboot							
Ţ	Advanced application								
0% 00	Services								
ſð	Log								

Fig 17. User Account setting after changing accounts

### **Remote Access:**

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

# Account Settings

### Remote Access

# Actions Logs

# Logout

### Fig 18. Remote access shortcut

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

_				
	CMD-COS-v1.01			Engli
		System Setup <	System Setup > Administration > Remote Access	8.52
A	System	Basic Setting	Remote Access	
	Overview	Disk	Remote Access Control	
<u>2</u>	Monitoring	management	Telnet Server: Open Console	
ţĊ;	System Setup	Cloud Account		
品	Network	Advanced Settings	vieb interface. Allow access to web interface irom public network	
111	Flow Control	Administration ^	Required HTIPS: Use HTIPS to access the web interface	
۲	Access	User Accounts	HTTP Access Port: 80 *	
8=	Authentication	Remote Access	HTTPS Access Port: 443 *	
			Custom SSL Certificate: Administration (Support only Nginx server certificates)	
⇒	Behavior	Upgrading 🗸		
臣	Firewall	Reboot	Remote Maintenance	
Ţ	Advanced application		Remote Channel: Open Console	
0% 00	Services		Remote Port: 22 *	
ቡ	Log		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.	
			Save	

Fig 19. Default Remote access control.

	CMD-COS-v1.01			් රු 👃 ළි English
	≡<	System Setup <	System Setup > Administration > Remote Ac	çess © CPU: 0.00% 및 MEM: 18% ↑ TX: 27.00 B/s ↓ RX: 60.00 B/s
Ð	System Overview	Basic Setting	Remote Access	
5	Monitoring	Disk $\checkmark$ management $\checkmark$	Remote Access Control	
ŝ	System Setup	Cloud Account	Telnet Server:	Open Console
品	Network	Advanced 🗸 🗸	Web Interface:	Allow access to web interface from public network
111	Flow Control	Administration ^	Required HTTPS:	Use HTTPS to access the web interface
۲	Access	User Accounts	HTTP Access Port:	80 *
æ	Authentication	Remote Access	HTTPS Access Port:	443 *
ريت ح			Custom SSL Certificate:	Administration (Support only Nginx server certificates)
→ _	benavior	Upgrading V		
臣	Firewall	Reboot	Remote Maintenance	
Ţ	Advanced application		Remote Channel:	✓ Open Console
	Services		Remote Port:	22 *
ß	Log		Remote Password:	*****
			Caution: 1. Cloud authentic 2. For you	s 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 ation management. Ge to Binding Ir security, please do not open remote maintenance at the request of non-official personnel.
			Save	

Fig 20. Changing Remote access control setting.

NGOTTO TO COMMANDO					
naserid.					
console for English		Version			
CMD-COS-v1.01		version.			
01D 00D 41.01					
0. System status	WEB Address ->	http://192.168.0.1:8			
1. Set ether band	lanl (v	ethl 08:9b:4b:50:1c:			
bc) LinkUp					
<ol><li>Set lan/wan address</li></ol>	lanl (V	eth2 08:24:7c:e0:63:			
30) LinkUp					
3. Set WEB port	lanl (v	eth3 08:24:7c:e0:63:			
31) LinkUp					
4. Ping Test	lanl (v	eth4 08:24:7c:e0:63:			
32) LinkDown					
5. Clean acl rule	wanl (v	eth5 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: CMI	-cos - v1.01		
0. System status	WEB Address ->	http://192.168.0.1:80			
1. Set ether band	lanl (v	ethl 08:9b:4b:50:1c:bc)			
<ol><li>Set lan/wan address</li></ol>	lanl (v	eth2 08:24:7c:e0:63:30)			
3. Set WEB port	lanl (v	eth3 08:24:7c:e0:63:31)			
4. Ping Test	lanl (v	eth4 08:24:7c:e0:63:32)	LinkDown		
5. Clean acl rule	wanl (v	eth5 08:24:7c:e0:63:33)			
<ol> <li>Restore default</li> </ol>					
<ol><li>Restore WEB passwd</li></ol>					
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



### Logout

### Fig 22. Action Logs shortcut

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

_								
	CMD-COS-v1.01							한 슈 은 English
	=	log	<	Log > System Logs > A	ction Logs		📮 CPU: 0.75%	% ↑ TX: 4.92 KB/s ↓ RX: 53.00 KB/s
		209		Action Logs				
$(\mathbf{x})$	System Overview	User Logs	$\sim$					
				Begin Time	S End Time	() IP/Username Q		Export Clean All
<u>~v</u>	Monitoring	Function Logs	<u> </u>					
ţĈ	System Setup	System Logs	^	Time	Username	IP Address	Function	Event
-				2021-04-12 18:08:52	admin	192.168.1.41		Login
ൽ	Network	System Logs		2021-04-12 17:55:13	admin	192.168.1.13	Interfaces	exec action for save
ţţţ	Flow Control	Action Logs		2021-04-12 17:55:04	admin	192.168.1.13	Interfaces	exec action for dhcp up
<b></b>	Access Controller	Notification		2021-04-12 17:54:46	admin	192.168.1.13	Interfaces	exec action for dhcp down
<u>&amp;=</u>	Authentication			2021-04-12 17:53:21	admin	192.168.1.13		Login
₩	Behavior			2021-04-12 17:40:43	admin	192.168.1.13		Login
田	Firewall			2021-04-12 17:40:24	admin	192.168.1.41		Login
	Advanced			2021-04-12 17:40:09	admin	192.168.1.41		Login
	application			2021-04-08 18:46:37	admin	192.168.1.41		Login
	Services			2021-04-08 17:47:03	admin	192.168.1.41		Login
ſð	Log			2021-04-07 18:51:08	admin	192.168.1.41		Login

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

### Logout:

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

# Account Settings Remote Access Actions Logs



### Fig 24. Logout shortcut

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

Eng COMIMANDO	lish
admin	
•••••	
Login	

### 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.

	CMD-COS-v1.0					්	습 수	. 2	English
	<u></u> ,	Log	Log > System Logs > Notification		📮 CPU: 4.25%	MEM: 19% 1	TX: 499.00	B/s ↓ RX:	224.00 B/s
Ð	System Overview	Vser Logs	Notification						
₩	Monitoring	Function Logs						Cle	ean All
ŝ	System Setup	System Logs	Username	Time		Actions			
品	Network	System Logs			No Data				
ţ†	Flow Control	Action Logs							
ŕ	Access Controller	Notification							
<u>ه</u> =	Authenticatior								
∽	Behavior								
Ħ	Firewall								
Ţ	Advanced application								
00	Services								

Fig 27. Default Message notifications page

Version Upgrade:

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



### Fig 28. Version Upgrade page

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

	CMD-COS-v1.01					2	Ŷ	٥		English
	=<	System Setup	System Setup > Upgrading > Version L	lpgrade	∎ CPU: 3.00%	MEM: 19%	12.0 TX: 12.0	52 KB/s	↓ RX:2	235.27 KB/s
	_		Version Upgrade							
6	System Overview	Basic Setting								
₩	Monitoring	Disk management	Automatic Updates							
ţĊ	System Setup	Cloud Account	Version Check :	Check New Version						
뮯	Network	Advanced $\checkmark$ Settings	Route system version:	3.4.5						
ţţţ	Flow Control	Administration $\lor$	Current Protocol version:	2.0.109 Upgrade						
<b></b>	Access Controller	Upgrading ^	Communication tools version :	2.1.6 Upgrade						
<u>8</u> =	Authentication	Version Upgrade	Current WEB version :	2.1.0						
<b>↓</b> ≱	Behavior	Backup and Restore	Auto Upgrade :	✓ Protocol library ✓ Communication tool feature library	✓ URL feature li	brary				
Ħ	Firewall	Reboot								
Ţ	Advanced application		Manual Updates							
0% 00	Services		Local Upgrade :	system & feature librar Select File Upload File						
ĥ	Log			Version update log Y						

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.

	CMD-COS-v1.01			🔿 🗘 🕰 English							
	=<	System Setup	System Setup > Cloud Account	aĢ≣ CPU: 2.72% 🛄 MEM: 19% ↑ TX: 4.37 KB/s ↓ RX: 68.12 KB/s							
	-	-,	Cloud Account								
A	System Overview	Basic Setting									
₩	Monitoring	Disk management									
ţĊ	System Setup	Cloud Account	Router ID :	247ce0632ec88bde3e5053d6d00818e8 *							
品	Network	Advanced	Account Code :	(Fill in the "Account Code" that you get in your Cloud Account )							
[†↓†	Flow Control	Administration V	Comment :	•							
	Access			( Note Router device will be shown in your Cloud Account )							
	Controller	Upgrading 🗸 🗸		Save							
&= ;;	Authentication	Reboot									
₩	Behavior		Help: W	nat is cloud service?							
田	Firewall		Clo	d service focuses on managing the router. You can view and manage your devices, such as check the running status, modify the iguration, and set the authentication for captive portal.							
Ţ	Advanced application		Ho	w <b>to connect to cloud service?</b> o cloud platform> gets the binding code> enters the binding code and remark name> saves and completes the binding							
0% 00	Services		Ho Wa	w to manage? it about 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.							
ß	Log		Ho Loy	w to unbind the cloud? y in to cloud platform on the PC side, and complete the unbundling of corresponding routes in the routing list equipment management outing 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.



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



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

#### Language Options:

Helps to select language as per choice of user.



Fig 34. Language selection icon

### MONITORING

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

### Interface:

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

### Terminal:

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

#### Protocol:

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

### **Policy:**

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

#### System:

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

#### Flow Control:

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

#### 1. Interface

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

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

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

USB interface are data transmission interface.

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

	CMD-COS-v1.01										්	☆ \$		English
	=<	Monitoring <	Monitoring > In	terface						= CPU: 1.009	6 🛄 MEM: 16%	↑ TX: 0.0	DB/s ↓	RX: 0.00 P
~	Sustem	J	Interface Mon	itoring										
6-9	Overview	Interface												
₩	Monitoring	Terminal	Interface Status											
ţĊ	System Setup	Protocol	<u> </u>	<u> </u>										
츎	Network	Policy	lan1	wan1										
†∔†	Flow Control	System												
<b>R</b>	Access Controller	Flow Control	All Interface Stat Caution: 5s defa	t <b>us</b> ult automatica	lly refresh. Toda	ıy's Tx and Rx pa	icket loss and	d packet lost rate ar	e cleared at 00:00	) everyday.		Auto	Refresh	× Ø
<u>8</u> =	Authentication		Interface	IP Address	Connection Number	Tx	Rx	Tx Bytes	Rx Bytes	Tx Packets/day	Rx Packets/day	Remarks	Actio	ons
	Behavior									0% (Lost	0% (Lost			
Ħ	Firewall		lan1	192.168.1.1		51 B/s	92 B/s	307.84 KB	3.56 MB	Packet: 0)	Packet: 0)			
Ţ	Advanced application		wan1		0	0 B/s	0 B/s	24.38 KB	0 B	0% (Lost Packet: 0)	0% (Lost Packet: 0)		Deta	ils
0%	Services		Outbound Inter	ace Status										
ſð	Log		Interface	IP Ac	dress	Gateway		Access Mode	Link Time	•	Failover	Statu	IS	
			wan1					DHCP			ON	dhcp		

Fig 1.1.1 Default interface monitoring page

	CMD-COS-v1.01										්	û	¢	<u>e</u> Eng	lisł
	=	Monitoring	Monitoring > I	nterface						© CPU: 0.50%	🛄 MEM: 18%	↑ TX: 2	27.00 B/s	↓ RX: 27.	00
		Wontohing	Interface Mo	nitoring											
Ð	System Overview	Interface													
₩	Monitoring	Terminal	Interface Statu	S											
ŝ	System Setup	Protocol													
品	Network	Policy	lan1	wan1											
ţţţ	Flow Control	System	All Interferen Ch	-											
<b>₩</b>	Flow Control Access Controller	System Flow Control	All Interface St Caution: 5s de	atus fault automatical	ly refresh. Toda	ay's Tx and Rx pa	cket loss and p	acket lost rate ar	re cleared at 00:00	) everyday.		A	uto Refre	sh ∨	G
₩	Flow Control Access Controller Authentication	System Flow Control	All Interface St Caution: 5s de Interface	atus fault automatical IP Address	ly refresh. Toda Connection Number	ay's Tx and Rx pa	cket loss and p Rx	acket lost rate ar Tx Bytes	re cleared at 00:00 Rx Bytes	) everyday. Tx Packets/day	Rx Packets/day	A	uto Refre	sh ∨ Actions	S
₹ \$\ \$	Flow Control Access Controller Authentication Behavior	System Flow Control	All Interface St Caution: 5s de Interface lan1	atus fault automatical IP Address 192.168.0.1	ly refresh. Toda Connection Number 	ay's Tx and Rx par Tx 1.63 KB/s	cket loss and p Rx 1.54 KB/s	acket lost rate ar Tx Bytes 45.09 MB	re cleared at 00:00 Rx Bytes 646.92 MB	) everyday. Tx Packets/day 0% (Lost	Rx Packets/day 0% (Lost	A	uto Refre	esh 🗸	S
	Flow Control Access Controller Authentication Behavior Firewall	System Flow Control	All Interface St Caution: 5s de Interface Ian1	atus fault automatical IP Address 192.168.0.1	ly refresh. Toda Connection Number 	ay's Tx and Rx par Tx 1.63 KB/s	cket loss and p Rx 1.54 KB/s	acket lost rate ar Tx Bytes 45.09 MB	re cleared at 00:00 Rx Bytes 646.92 MB	0 everyday. Tx Packets/day 0% (Lost Packet: 0)	Rx Packets/day 0% (Lost Packet: 0)	Remark	uto Refre	Actions	S
	Flow Control Access Controller Authentication Behavior Firewall Advanced application	System Flow Control	All Interface St Caution: 5s de Interface Ian1 wan1	atus fault automatical IP Address 192.168.0.1 192.168.1.38	ly refresh. Toda Connection Number  22	ay's Tx and Rx pa Tx 1.63 KB/s 133 B/s	Rx Rx 1.54 KB/s 123 B/s	acket lost rate ar Tx Bytes 45.09 MB 42.35 MB	re cleared at 00:00 Rx Bytes 646.92 MB 583.17 MB	D everyday. Tx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0)	Rx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0)	Remark	uto Refre	Actions Details	
	Flow Control Access Controller Authentication Behavior Firewall Advanced application Services	System Flow Control	All Interface St Caution: 5s de Interface Ian1 wan1 Outbound Inte	atus fault automatical IP Address 192.168.0.1 192.168.1.38 rface Status	ly refresh. Toda Connection Number  22	ay's Tx and Rx par Tx 1.63 KB/s 133 B/s	Rx 1.54 KB/s 123 B/s	acket lost rate ar Tx Bytes 45.09 MB 42.35 MB	re cleared at 00:00 Rx Bytes 646.92 MB 583.17 MB	) everyday. Tx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0)	Rx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0)	Remarl	ks .	Actions Details	2
우 18 (기 태 사 톱 🔊 🗐	Flow Control Access Controller Authentication Behavior Firewall Advanced application Services Log	System Flow Control	All Interface St Caution: 5s de Interface Ian 1 wan 1 Outbound Inte Interface	atus fault automatical IP Address 192.168.0.1 192.168.1.38 rface Status IP Ad	ly refresh. Toda Connection Number  22 dress	ay's Tx and Rx par Tx 1.63 KB/s 133 B/s Gateway	Rx 1.54 KB/s 123 B/s	Tx Bytes Tx Bytes 45.09 MB 42.35 MB	re cleared at 00:00 Rx Bytes 646.92 MB 583.17 MB Link Time	D everyday. Tx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0)	Rx Packets/day 0% (Lost Packet: 0) 0% (Lost Packet: 0) Failover	Remarl	uto Refre	Actions Details	

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.

lan1	wan1
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/ <mark>Not Connected</mark> /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

Interface Status		
_		
lan1	wan1	
-		
All Interface Statu	wan1Default Ga	teway
Caution: 5s defau	Connection Status:	Connected 1052d 18h 14m
Interface	Type:	DHCP
	IP:	192.168.1.38
lan1	Subnet Mask:	255.255.255.0
	Gateway:	192.168.1.1
wan1	DNS:	192.168.1.1
	MAC:	08:24:7c:e0:63:33
	Remarks:	
Outbound Interfa Interface	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
	CMD-COS-v1.01									් (	) <del>(</del> 2	English
	=<	Monitoring <	Monitoring > Termin	al					📮 CPU: 1.75%	🛄 MEM: 16%	↑ TX: 0.00 B/s ↓ R)	(: 0.00 B/s
-			Terminal Monitori	ng								
6-3	Overview	Interface										
₩	Monitoring	Terminal	Comment/IP/MAC	Q All acce	ss types	<ul><li>✓ All</li></ul>		<ul> <li>✓ shut down aut</li> </ul>	tor 🗸		Auto Refresh ∨	S 🛛
ţĊţ	System Setup	Protocol	IP/MAC 🗸	Connection Number	∕ Tx Rate ∨	Rx Rate ∨	Tx Bytes 🗸	Rx Bytes 🗸	Uptime 🗸	Remarks 🗸	Actions	
	Network	Policy	192.168.1.100 e0:db:55:be:35:5b	0	0.04	0.0/-	0.0	60.70 KB	0 20-		Details Networking	prohibited
†∔†	Flow Control	System		8	U B/S	U B/S	0.8	00.78 KB	9111 205		Limit Modify con	nment
r	Access Controller	Flow Control		<						>		_
<u>&amp;=</u>	Authentication		Showing 1 of 1 recor	rds				PerPage 20	✓ Rows	《 〈 1 〉	≫ 1 /1Pages	Jump
\$	Behavior											
臣	Firewall											
Ţ	Advanced application											
00	Services											
ß	Log											

# Fig 1.2.1 Default Terminal Monitoring page

	CMD-CO5-v1.01									් ර	수 은 English
	≡<	Monitoring <	Monitoring > Termin	al				: <b>.</b>	:PU: 8.17% 📮	🛄 MEM: 18%  ↑ TX: 39	7.00 B/s \downarrow RX: 156.00 B/s
~	System		Terminal Monitori	ing							
6.)	Óverview	Interface									
₩	Monitoring	Terminal	Comment/IP/MAC	Q All acce	ess types	All		✓ shut down au	tor ∨	Auto	Refresh 🗸 💭 🔮
ţĊţ	System Setup	Protocol	IP/MAC $\sim$	Connection Number	∕ Tx Rate ∽	Rx Rate ∽	Tx Bytes $\checkmark$	Rx Bytes ∨	Uptime $\sim$	✓ Remarks ∨	Actions
品	Network	Policy	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
†∔†	Flow Control	System			0.0/0	0.070	THE RE	LUILTING			Limit Modify comment
<b></b>	Access Controller	Flow Control	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
<u>&amp;</u>	Authentication										Modify comment
$\downarrow$	Behavior		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
Ħ	Firewall										Limit Modify comment
y	Advanced application		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
0 <b>%</b> 00	Services										Modify comment
R	Log			<					3	>	
			Showing 1-4 of 4 re	cords				PerPage 20	$\checkmark$ Rows	« < <u>1</u> > »	1 /1Pages Jump

# Fig 1.2.2 Terminal Monitoring after connecting devices page

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

	CMD-COS-v1.01									්	٢	۵	<u>ڪ</u> E	nglish
	⊒<	Monitoring <	Monitoring > Termina	al				i 🛱 E CP	PU: 28.00% (	MEM: 18%	↑ TX: 3.2	4 KB/s	↓ RX: 4	9.75 KB/s
~	System	Ŭ	Terminal Monitorir	ng										
6-9	Overview	Interface												
₩	Monitoring	Terminal	Comment/IP/MAC	Q All acces	ss types 🛛 🗸	All	``	∽ shut down auto	√ 10		Auto F	lefresh	$\sim$	30
ţĊ	System Setup	Protocol	IP/MAC 🗸	Connection _ Number	⊤x Rate ∨	Rx Rate ∽	Tx Bytes ∨	Rx Bytes $\checkmark$	Uptime $\checkmark$	Remarks $\checkmark$	[	Action	IS	
÷	Network	Policy	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 Netwo	s orking pro	ohibited
†∔†	Flow Control	System										Limit	y comme	int
۲	Access Controller	Flow Control	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 Netwo	s orking pro	ohibited
<u>&amp;</u> =	Authentication											Modify	y comme	int
₩	Behavior		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 Netwo	s orking pro	ohibited
臣	Firewall											Modif	y comme	nt
Ţ	Advanced application		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-70A	PI5S	Details Netwo	s orking pro	ohibited
0% 00	Services											Modif	y comme	nt
ſħ	Log			<					>					
			Showing 1-4 of 4 rec	ords				PerPage 20	∨ Rows	《 < 1 >	> >>	1 /1P	ages 🛛	ump

#### 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.

	CMD-COS-v1.01					
	=,	Monitoring <	Monitoring > Terminal			
~	System		Terminal Details - D	ESKTOP-70API5S ( IP:192.168.0.14 )		
6-)	Overview	Interface				The Bat III
₩	Monitoring	Terminal			Basic Information Connection Details	How Details History Logs
<i>ф</i>	System Setup	Protocol	Basic Information			
몲	Network	Policy		IP Address: 192.168.0.14		System/Terminal Type: Unknown / Intel
<b>11</b>	Flow Control	System		MAC Address: c4:d9:87:a7:ad:46		Uptime: 12m 14s
9	Access Controller	Flow Control		Remarks: DESKTOP-70API5S		
<u>8</u> "	Authentication		Access Information:			
⇔	Behavior			Access mode: Wireless		Connect SSID: 5G:COMMANDO01 5G
臣	Firewall					
Ø	Advanced			Connect AP:		
	Services		Account Information			
R.	loa			Auth Type :		Account Status:
-11	cog					
				Username:		Password:
				Affiliation Package: Custom		Valid Date: Permanent
				Bind to MAC Method : Manual		Share:
			User Details			
			Carl Could			
				Username :		phone:
				ID Card:		Address:

Fig 1.2.4 Terminal Monitoring details Basic information page

	CMD-COS-v1.01										් ර	🗘 🔔 English
	=,	Monitorina <	Monitoring > Termin	al						🧔: CPU: 7.25% 🛛	🛄 MEM: 18% ↑ TX:	6.91 KB/s 👃 RX: 101.99 KB/s
~			Terminal Details -	DESKTOP-70API5S	(IP:192.168.0.14)							×
6-3	Overview	Interface								-		
<u>64</u>	Monitoring	Terminal				Basic Information	on Connection D	etails How Detail	s History Logs	]		
ţ	System Setup	Protocol										Auto Refresh
무	Network	Policy	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
tit	Flow Control	System	OtherHttp	tcp	wan1	192.168.1.38	57367	203.94.209.18	80	564 B	380 B	ESTABLISHED
۲	Access Controller	Flow Control	SSL	tcp	wan1	192.168.1.38	57409	35.247.185.126	443	2.4 KB	3.73 KB	ESTABLISHED
<u>&amp;</u> =	Authentication		SSL	tcp	wan1	192.168.1.38	56781	74.125.200.188	5228	1.94 KB	5.78 KB	ESTABLISHED
¢‡	Behavior		HTTPS	tcp	wan1	192.168.1.38	57438	172.217.160.214	443	1.44 KB	0.99 KB	ESTABLISHED
臣	Firewall		Oray_Sunlogin	tcp	wan1	192.168.1.38	56864	121.40.255.86	443	6.24 KB	8.73 KB	ESTABLISHED
Ţ	Advanced application		SSL	tcp	wan1	192.168.1.38	56822	40.119.211.203	443	2.72 KB	4.91 KB	ESTABLISHED
	Services		YOUTUBE	udp	wan1	192.168.1.38	62821	142.250.192.22	443	31.33 KB	547.23 KB	
R	Log		YOUTUBE	udp	wan1	192.168.1.38	62859	216.239.32.116	443	2.9 KB	5.14 KB	
-	3		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

	CMD-COS-v1.01							් ර ද	A English
	=<	Monitoring <	Monitoring > Terminal				📮 CPU: 5.50%	1: 18% ↑ TX: 6.37 KB/s	, ↓ RX: 127.19 KB/s
			Terminal Details - DESK	TOP-70API5S ( IP:192.	.168.0.14 )				×
6	System Overview	Interface							
FM	Monitoring	Terminal		Basic	Information Connection	on Details Flow De	tails History Logs		
~								Auto R	efresh $\checkmark$ $\mathcal{O}$
÷Ċż	System Setup	Protocol	App Name	Tx Rate	Total Tx	:(%)	Rx Rate	Total F	kx(%)
矗	Network	Policy	Unknown	0 B/s	4.23 KB	0.07%	0 B/s	48.75 KB	0.06%
†∔†	Flow Control	System	HttpProtocol	0 B/s	130.88 KB	2.20%	0 B/s	308.93 KB	0.36%
<b></b>	Access Controller	Flow Control	NetDownload	0 B/s	151.65 KB	2.55%	0 B/s	9.85 KB	0.01%
<u>&amp;=</u>	Authentication		FileTransfer	0 B/s	0 B	0.00%	0 B/s	0 B	0.00%
<b>↓</b> ≯	Behavior		NetMessage	0 B/s	1.36 KB	0.02%	0 B/s	0 B	0.00%
田	Firewall		NetVideo	5.48 KB/s	5.47 MB	94.35%	98.69 KB/s	82.91 MB	99.49%
Ţ	Advanced application		CommonProtocol	0 B/s	47.52 KB	0.80%	0 B/s	64.52 KB	0.08%
0%	Services		NetGame	0 B/s	0 B	0.00%	0 B/s	0 B	0.00%
ſЪ	Log		OtherSoft	0 B/s	0 B	0.00%	0 B/s	0 B	0.00%
	<sup>11</sup>		SpeedTool	0 B/s	0 B	0.00%	0 B/s	0 B	0.00%

Fig 1.2.6 Terminal Monitoring flow details page

	CMD-COS-v1.01							්	<u>ۍ</u> ۲	2 2	English
	=,	Monitoring	Monitoring > Terminal			≡Ös CPU:	: 0.00% 🛄 MEM:	18%	TX: 2.16	KB/s ↓ R	X: 22.66 KB/s
-		monitoring	Terminal Details - DESKTOP-70API5S (	IP:192.168.0.14)							×
6)	Overview	Interface									
₩	Monitoring	Terminal		Basic Information	Connection Details	Flow Details	History Logs				
ţĊjł	System Setup	Protocol		The upper and low	er line record of the termir	nal has been opened, a	and the data is auto	omatical	ly updated	every minu	te ON O
品	Network	Policy	Timestamp	Uptime		Tx Bytes				Rx Bytes	
†∔†	Flow Control	System			No Data						
<b></b>	Access Controller	Flow Control									
<u>&amp;=</u>	Authentication										
₩	Behavior										
臣	Firewall										
Ţ	Advanced application										
0%	Services										
Ŀ	Log										

### Fig 1.2.7 Default Terminal Monitoring History Logs page

	CMD-COS-v1.01							۵	企	٩	2	English
	=<	Monitorina <	Monitoring > Terminal			÷Ö	CPU: 0.00% 🛄 N	/IEM: 20%	↑ TX:	82.00 B/	s ↓	RX: 99.00 B/s
	-	g	Terminal Details (IP:192.168.0.100)									×
$\mathbb{C}$	System Overview	Interface										
M	Monitoring	Terminal		Basic Information	Connection Details	Flow Details	History Logs					
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					The upper and lower li				ta canno			OFF
ւ;	System Setup	Protocol										
品	Network	Policy	Timestamp	Uptime		Tx Bytes				Rx By	rtes	
(†14)	Flow Control	System	2021-05-10 22:36:36	29m 24s		2.68 KB				7.71	KB	
	Access	,	2021-05-10 22:31:03	4m 57s		330 B				270 8	3	
<b>P</b>	Controller	Flow Control	2021-05-10 17:54:06	4h 13m 54s		105.72 MI	3			54.04	MB	
<u>&amp;</u> =)	Authentication		2021-05-00 21-22-06	1h 52m 54r		772 12 40				2.40	MR	
÷	Behavior		2021-03-03-21.33.00	111 J2111 J45		112.12 ND				2,40	IVID	
>	benavior		2021-04-18 17:03:09	10m 51s		10.07 KB				33.69	KB	
臣	Firewall		2021-04-18 17:06:25	1h 28m 36s		486.01 KB				8.34	MB	
Ţ	Advanced application		2021-04-18 17:03:10	4h 15m 50s		56.9 KB				83.44	KB	
0%	Services		2021-04-18 17:03:49	3h 39m 11s		98.08 KB				152.8	7 KB	
			2021-04-18 17:05:19	11m 41s		613.54 KB				11.19	MB	
L)	Log											

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

	CMD-COS-v1.01								්	û	¢	2	English	
	=<	Monitoring <	Monitoring > Protocol				≡(	ECPU: 0.50%	MEM: 1	6% 1	TX: 0.00	B/s 🦊	RX: 0.00 E	3/s
-	—		Protocol Monitoring											í
6	Overview	Interface												
₩	Monitoring	Terminal	Flow / Connections distribution					Tip: r	efresh autor	natically	every 5 s	econds b	y default	
ţĊţ	System Setup	Protocol	Last 30 Minutes $\checkmark$					Clear Data	Clea	in up ap	plication	protocol	data	
뮮	Network	Policy			of netw 1.2	ork connections								
t+t	Flow Control	System		HTTP: 0 B(0%)	0.9									
<b></b>	Access Controller	Flow Control		Game: 0 B(0%)										
<u>&amp;</u> =	Authentication		0 B	Transport: 0 B(0%)	0.6									
			Total Bytes	Common: 0 B(0%)	0.3									
$\rightarrow$	Behavior			Others: 0 B(0%)										
Ħ	Firewall			Unknown: 0 B(0%)	0 1	with wide (2	ame hoad	- Rolt	IN and		let's r	jë .	ONNE	
Ţ	Advanced application						Donn	Trans	Cour	0.		Unk		
0%	Services		Protocol Flow											
ß	Log							peak Va	Last 1	Day	$\checkmark$ all		$\sim$	

# Fig 1.3.1 Protocol Monitoring flow/connections distribution default page

	CMD-COS-v1.01			් රා 🗘 ළ English	
	=,	Monitoring <	Monitoring > Protocol	= □ □ □ □ □ □ □ □ □ □ □ □ □ □ MEM: 18% ↑ TX: 2.18 KB/s ↓ RX: 1.28 KB/s	
Ð	 System Overview	Interface	Protocol Monitoring		^
₩	Monitoring	Terminal	Flow / Connections distribution	Tip: refresh automatically every 5 seconds by default	
ţĊţ	System Setup	Protocol	Last 1 Day 🛛 🗸	Clear Data Clean up application protocol data	
品	Network	Policy			
ţţţ	Flow Control	System		Video: 515.42 MB(82.04%)	
<b></b>	Access Controller	Flow Control		Game: 76.06 KB(0.01%) 4 Download: 2.25 MB(0.36%)	
<u>&amp;=</u>	Authentication		628.23 MB	Transport: 0 B(0.00%) IM: 9.84 MB(1.57%) 2	
<del>√</del> ≱	Behavior			Common: 2.08 MB(0.33%) Others: 403.42 KB(0.06%)	
臣	Firewall			Test: 25.02 KB(0.00%)     Unknown: 28.66 MB(4.56%)     Tr <sup>Q</sup> Jid <sup>6D</sup>	
Ţ	Advanced application			Dogu Light Cop. Roge	
0% 00	Services		Protocol Flow		

# 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

	CMD-COS-v1.01							් (	) 4 2	English
	=,	Monitoring <	Monitoring > Policy	,			≡ <b>□</b> ≡ CPU: 0.5	i0% 🛄 MEM: 16%	↑ TX: 0.00 B/s 🗸	RX: 0.00 B/s
~	Surtem	,	Strategy Monitor	ing						
6-3	Overview	Interface								
₽₽	Monitoring	Terminal						Select	Auto Refre	sh $\checkmark \mathcal{O}$
ţĊţ	System Setup	Protocol						Tip: refresh automat	ically every 5 seco	onds by default
品	Network	Policy	Strategy name	Prio	IP	Up speed (KB/s)	Down rate(KB/s)	Total Tx	Total Rx	
†∔†	Flow Control	System				No Data				
<b></b>	Access Controller	Flow Control								
&= 	Authentication									
<b>↓</b>	Behavior									
Ħ	Firewall									
Ţ	Advanced application									
0%	Services									
ß	Log									

Fig 1.4.1 Default Policy Monitoring page

#### 5. System

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

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



#### Fig 1.5.1 Default System Monitoring page



Fig 1.5.2 System Monitoring for 1hour page

#### 6. Flow Control

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

For Flow Control Monitoring, Click on Monitoring > Flow Control

	CMD-COS-v1.01					👌 🔂 🙏 🖴 English
	=<	Monitoring <	Monitoring > Flow Contr	ol	≡ <mark>□</mark> ≣ CPU:	0.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
-		g	Flow Control Monitor	ing		
63	Overview	Interface				
<u>-</u>	Monitoring	Terminal				Clean Data 🛛 Auto Refresh 🗸 🃿
ැරිූ	System Setup	Protocol				Tip: refresh automatically every 5 seconds by default
5				Connection Number (Today)	Connection Number (Yesterday)	Connection Number (Last 7 Days)
品	Network	Policy	Interface	0	0	0
ţţţ	Flow Control	System	Protocol	0	0	0
<b></b>	Access Controller	Flow Control	Domain Name	0	0	0
<u>&amp;</u> =	Authentication		Bypassed	0	0	0
<del>⊊</del> ≯	Behavior		Total	0	0	0
臣	Firewall					
Ţ	Advanced application					
0%	Services					
<b>F</b> A						

Fig 1.6.1 Default Flow Control page

	-					
CONHED	CMD-COS-v1.01					
	=<	Monitoring <	Monitoring > Flow Contr	ol	= <mark>□</mark> = CPU: 0	.25% 🛄 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
	_	, j	Flow Control Monitor	ing		
$\mathfrak{S}$	System Overview	Interface				
	Monitoring	Terminal				Clean Data 🛛 Auto Refresh 🗸 💭
<u>بن</u>	Worlitoring	Terrinia				Tip: refresh automatically every 5 seconds by default
ţĊ	System Setup	Protocol				
모	Network	Deller		Connection Number (Today)	Connection Number (Yesterday)	Connection Number (Last 7 Days)
666	Network	Policy	Interface	0	0	0
ţţţ	Flow Control	System	Protocol	0	0	0
<b></b>	Access Controller	Flow Control	Domain Name	0	0	0
<u>&amp;</u> =	Authentication		Bypassed	34	0	34
<b>↓</b>	Behavior		Total	34	0	34
臣	Firewall					
Ţ	Advanced application					
0%	Services					
ſð	Log					

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 or	ר Svstem Setup >	<b>Basic Setting</b>

	CMD-COS-v1.01				් දා 👃 🕹 English
	≡<	System Setup	<	System Setup > Basic Setting	
ଚ	System Overview	Basic Setting		System Information	^
	Monitoring	Disk management	~	Device Name:	COMMANDO .
¢;	System Setup	Cloud Account		Network Mode	
뮮	Network	Advanced Settings	~	Speed Model:	Close V
t#t	Flow Control	Administration	~		
<b>®</b>	Access Controller	Upgrading	~	Help Tip: Network n Symmetric	node: support symmetric NAT, Full Cone NAT and Transparent Mode. . NAT: Symmetric NAT (network address translation), the most secure of the NAT types, is also the default mode of the device
<u>8</u> =	Authentication	Reboot		Full NAT: Transparer	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. nt Mode: All data without NAT forwarding, directly to the network IP do not do carnouflage transmission to the outer network, applicable to the network IP are
₩	Behavior			public net	work address.
臣	Firewall			Time Settings	
Ţ	Advanced application				
	Services			System Time:	2018-06-01 0.21:07
Ъ	Log			Time Zone:	(GMT +8:00) Beijing, Perth, Singapore, Hong Kong 🛛 🗸
				Time Setting:	2018-06-01 00-21:07 (0) * Update Now
				Set Time Automatically:	✓ Open Sync Time Now
				NTP service:	Open (Gateway ACTS as NTP server)
					Save

#### Fig 2.1.1 Default Basic setting page

	CMD-COS-v1.01				ය් ර අ ළ	English
	⊒<	System Setup <	System Setup > Basic Setting		≣⊑ CPU: 1.73% 🛄 MEM: 18% ↑ TX: 55.00 B/s ↓	RX: 66.00 B/s
~	System		Basic Settings			
(~)	Overview	Basic Setting				
<u>-</u>	Monitoring	Disk 🗸 🗸	System Information			
ţĊ	System Setup	Cloud Account				
品	Network	Advanced 🗸 🗸 🗸	Device Name:	XYZ	] * 7	
t†	Flow Control	Administration $\checkmark$	Network Mode:	Symmetric NAI	]	
<b></b>	Access Controller	Upgrading 🗸 🗸	Speed Model:	Close ~		
8 <u>-</u>	Authentication	Reboot	Help Tip: Network Symmetr	mode: support symmetric NAT, Full Cone NAT and Transparer ric NAT: Symmetric NAT (network address translation), the mo	nt Mode. ost secure of the NAT types, is also the default mode of the	
₩	Behavior		device Full NAT	: Full NAT (network address translation), a less secure type of	NAT, is generally used in special needs scenarios. It is not	
Ħ	Firewall		recomm Transpar the oute	ended to turn it on. ent Mode: All data without NAT forwarding, directly to the net entwork and isolate to the network IB are public network add	twork network IP do not do camouflage transmission to	_
Ţ	Advanced application			r network, applicable to the network in are public network add	II 035.	
0% 00	Services		Time Settings			
Ռ	Log					
_			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 are public network address.

	CMD-COS-v1.01							්	6 ¢	2	Englis
	=<	System Setup	System Setup	> Basic Setting			📲 CPU: 1.50%	🛄 MEM: 18%	1 TX: 0.0	10 B/s 🤳	RX: 0.00
6	 System		Basic Settin	gs							
63	Overview	Basic Setting									
5	Monitoring	Disk 🗸 🗸	System Inforr	nation							
ţĊţ	System Setup	Cloud Account			00000000						
曓	Network	Advanced 🗸		Device Name:	COMMANDO	^					
000		Settings		Network Mode:	Symmetric NAT	$\sim$					
tłt	Flow Control	Administration $\checkmark$		Speed Model:	Close	$\sim$					
<b></b>	Access Controller	Upgrading 🗸 🗸									
<u>&amp;=</u>	Authentication	Reboot		Help Tip: Network	node: support symmetric NAT, Full Cone NAT a	nd Transparent Mo	de.				
¢↓	Behavior			Symmetri device Full NAT	NAT: Symmetric NAT (network address transl	ation), the most sec	cure of the NAT types,	is also the default	t mode of t	the	
臣	Firewall			recomme	ided to turn it on. ht Mode: All data without NAT forwarding, direct	ctlv to the network	network IP do not do	camouflage trans	mission to		
<u> </u>				the outer	network, applicable to the network IP are public	network address.		announage a uno			
Ţ	Advanced application										

#### Fig 2.1.4 Default network mode Symmetric mode page

	CMD-COS-v1.01					් ර 4		
	=,	System Setun	System Setup	> Basic Setting		🛱 CPU: 5.50% 🛄 MEM: 18% ↑ TX: 0	.00 B/s 🔱	
			Basic Settin	gs				
$(\mathbf{r})$	System Overview	Basic Setting						
₩	Monitoring	Disk management	System Inform	nation				
ţĊ	System Setup	Cloud Account						
品	Network	Advanced		Device Name:	COMMANDO	*		
		Settings		Network Mode:	Transparent Mode	$\sim$		
tłł	Flow Control	Administration $\checkmark$		Speed Model:	Close	$\checkmark$		
<b></b>	Access Controller	Upgrading $\lor$						
<u>&amp;</u> =	Authentication	Reboot		Help Tip: Network m	ode: support symmetric NAT, Full Cone NAT and Tra	ransparent Mode.		
¢	Behavior			Symmetric device	NAT: Symmetric NAT (network address translation)	a), the most secure of the NAT types, is also the default mode of	the	
				Full NAT: I recommend	Full NAT (network address translation), a less secure ded to turn it on.	e type of NAT, is generally used in special needs scenarios. It is i	ot	
Ħ	Firewall			Transparen the outer n	t Mode: All data without NAT forwarding, directly to etwork, applicable to the network IP are public netw	o the network network IP do not do camouflage transmission to work 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	$\sim$			
	Time Setting:	2021-04-19 02:32:02	0	*	Update Now	
	Set Time Automatically:	✓ Open Sync Sync Time Now				
	NTP service:	Open (Gateway ACTS as NTP server)				
		Save				

#### 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	$\sim$		
	Time Setting:	2021-04-19 02:32:02	0	* Update Now	
	Set Time Automatically:	Open Sync Sync Time Now			
	NTP service:	✔ Open (Gateway ACTS as NTP server)			
		Save			

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

#### 2. Disk management

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

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

# Setup > Disk management > Disk partition

	CMD-COS-v1.01								් ර 4	) <u> </u>
	=<	System Setup	System Setup > D	)isk management > Disk	partition			≣ CPU: 0.00%	🖵 MEM: 16% ↑ TX: 0	.00 B/s ↓ RX: 0.00 B/s
-			Disk partition							
63	Overview	Basic Setting								
₩	Monitoring	Disk ^ management								Quick zoning
ţĊ	System Setup	Disk partition	disk	Mount path	Partition name	Partition type	Partition size	Utilization rate	Binding business	Actions
品	Network	File management					No Data			
†∔†	Flow Control	Cloud Account								
<b></b>	Access Controller	Advanced $\checkmark$ Settings	Description:1, 2,	Each hard disk can sup External hard disks mu	oport up to 8 partitions, ist be formatted or part	and the system disk o itioned after binding s	an be divided into 4 a services, otherwise rela	dditional partitions; ted services will use sys	tem disk space by defau	ult;
<u>&amp;</u> =	Authentication	Administration $\vee$	3,	Disk partitions support	t bundled functional se	vices including: ordin	ary storage, behavior r	ecords, Cache Service (p	partition size 10G and al	bove)
\$	Behavior	Upgrading 🗸 🗸								
臣	Firewall	Reboot								
Ţ	Advanced application									
0% 00	Services									
ſð	Log									

Fig 2.2.1 Disk partition page

	CMD-COS-v1.01				් 🗘 🗘 English
	⊒<	System Setup <	System Setup > Disk management > Disk	partition	≣⊑ CPU: 11.50% 🛄 MEM: 19% ↑ TX: 64.53 KB/s ↓ RX: 292.15 KB/s
6	System	Pasic Satting	Quick zoning		×
E A	Overview Monitoring	Disk ^			
_ ۲	System Setup	Disk partition	Select disk:	(0 B)	~
뮯	Network	File management	Zoning quantity:	1	~
tŧŧ	Flow Control	Cloud Account	Disk partition size:	0	
<b></b>	Access Controller	Advanced $\checkmark$ Settings			
<u>&amp;</u> =	Authentication	Administration $\checkmark$		Save Cancel	
⇆	Behavior	Upgrading $\vee$			
田	Firewall	Reboot			
Ţ	Advanced application				
0%	Services				
ſð	Log				

Fig 2.2.2 Disk partition quick zoning page

	CMD-COS-v1.01					C	<mark>ኔ</mark> ጉ .	¢ 2	English
	≡<	System Setup <	System Setup > Disk management > Disk	k partition	≣ <mark>0</mark> ≣ CPU: 4.46%	🛄 MEM: 19%	↑ TX: 126.08	KB/s ↓ RX:	261.27 KB/s
6)	System Overview	Basic Setting	Quick zoning						×
₩	Monitoring	Disk ^ management							
ţĊ	System Setup	Disk partition	Select disk:	(0 B)	·				
뮯	Network	File management	Zoning quantity:	1 ~ ~ 1 2	<i>,</i>				
t+t	Flow Control	Cloud Account	Disk partition size:	3	GB				
<b>R</b>	Access Controller	Advanced $\checkmark$ Settings		5 6 7					
<u>&amp;</u> =	Authentication	Administration $\checkmark$		8					
↓ \$	Behavior	Upgrading 🗸 🗸							
田	Firewall	Reboot							
Ţ	Advanced application								
0%	Services								
ſð	Log								

#### 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

	CMD-COS-v1.01				්	습 수 온 English
	=<	System Setup	System Setup > Disk management > File management		📲 CPU: 0.50% 🔛 MEM: 16	% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
-			File management			
6	System Overview	Basic Setting				
₩	Monitoring	Disk ^ management	All disk			
ţ	System Setup	Disk partition	File name 🗸	Size 🗸	Туре 🗸	Modification time $\checkmark$
品	Network	File management				
†∔†	Flow Control	Cloud Account				
<b></b>	Access Controller	Advanced 🗸 🗸 🗸				
<u>&amp;</u> =	Authentication	Administration $\lor$				
₩	Behavior	Upgrading $\vee$				
臣	Firewall	Reboot				
Ţ	Advanced application					
0% 00	Services					
ľð	Log					

#### 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.

Cloud	English
Image: Create Account   Create Account   Forgot Password?	
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





Fig 2.3.2 Create Cloud Login account page

# Register



#### 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.

Cloud	Network Configura d	ition Message	Personal	3a017d3d6be29db38ea82fd35785	S A English		
Wetwork       Manage	0/0 Total User	0/0 Online User	Authent	<b>0/0</b> ication User/Accumulated Today	0 Each		
	<ul> <li>Webpage 0 B</li> <li>Download 0 B</li> <li>Transfer 0 B</li> <li>Top 3 Traffic in 7 Days</li> </ul>	<b>D B</b> 7 Days Total Flow	Online A	<b>0/0</b> uthenticated/Accumulated Today	<ul> <li>5G 0 Each</li> <li>2.4G 0 Each</li> <li>Online Wireless Device</li> <li>Total Wireless Traffic (Day)</li> <li>0 B</li> </ul>		
	User Online Trend Total U	ser 🗧 New User 🔳 Old Us	ser		Last 7 Days Last 30 Days		

#### 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

	CMD-COS-v1.01					් ර ද ද	English
	=<	System Setup	System Setu	p > Cloud Accou	int	ធ្វើ៖ CPU: 2.23% 🛄 MEM: 18% ↑ TX: 3.14 KB/s 🤳 R	X: 859.00 B/s
-		,	Cloud Acc	ount			
6)	Overview	Basic Setting					
₩	Monitoring	Disk management					
ţĈ	System Setup	Cloud Account		Router ID :		247ce0632ec88bde3e5053d6d00818e8 *	
品	Network	Advanced		Account Code	e :	3a017d3d6be29db38ea82fd35789e567	
		Settings				( Hill in the "Account Code" that you get in your Cloud Account )	
†‡†	Flow Control	Administration 🗸		Comment :		COMMANDO *	
<b></b>	Access Controller	Upgrading 🗸 🗸				( Note Router device will be shown in your Cloud Account )	
<u>&amp;</u> =	Authentication	Reboot				Save	
⇆	Behavior						
Ħ	Firewall			Help :	What is clo Cloud servi configuration	cloud service? price focuses on managing the router. You can view and manage your devices, such as check the running status, modify the ation, and set the authentication for captive portal.	
Ţ	Advanced application				How to co Into cloud	connect to cloud service? ud platform> gets the binding code> enters the binding code and remark name> saves and completes the binding	
0% 00	Services				manage? out 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.		
ſ	Log				How to un Log in to cl routing i	unbind the cloud? o cloud platform on the PC side, and complete the unbundling of corresponding routes in the routing list equipment managem g information overview page;	nent

Fig 2.3.5 Binding code R100 router with cloud portal page

	CMD-COS-v1.01		🛆 û 🌲 English	
	≡<	System Setup <	System Setup > Cloud Account 📮 CPU: 19.25% 🛄 MEM: 18% ↑ TX: 1.81 KB/s 🤳 RX: 28.70 KB	/s
0	System	Basic Setting	Cloud Account	
<u></u>	Overview Monitoring	Disk management		
ŝ	System Setup	Cloud Account	Router ID : 247ce0632ec88bde3e5053d6d00818e8	
品	Network	Advanced	Account Code : 3a017d3d6be29db38ea82fd35789e567	
ţ†	Flow Control	Administration $\checkmark$	comment : COMMANDO	
۲	Access Controller	Upgrading 🗸 🗸		
<u>&amp;=</u>	Authentication	Reboot	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.	
<b>↓</b> ≯	Behavior		How to connect to cloud service?	
臣	Firewall		How to manage?	
Ţ	Advanced application		Wait about 3 minutes, you will see this device in your cloud account, you can manage and operate using your cloud account.	
0% 00	Services		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;	
ĥ	Log			

# Fig 2.3.6 After Binding R100 router with cloud page

CHONE	CMD-COS-v1.01						උ ර	) ¢ 2	English
	≡<	System Overview				≡Щ́≡ CPU: 0.74%	🛄 MEM: 19% ↑ TX	(: 4.27 KB/s ↓ RX: 14	14.79 KB/s
Ð	System Overview	COMMANDO	Rate Status		Connection Status				
₩	Monitoring	<b>Connected</b> <sub>WAN</sub>	↑ 4.27 кв/s		4	37	0	Wired: 2	
ţĊţ	System Setup	Running: 1h 10s	↓145 кв/s		Online Host	Connection Count	Auth Count	Wireless: 2	
品	Network								
†∔†	Flow Control	Interface Status	7	=	AC status	$\frown$	Frequency band	$\frown$	
<b>P</b>	Access Controller	WAN Enabled LAN Enabled	/ DHCP Pool		$(\bigcirc)$	$(\bigcirc)$			
&= ;;	Authentication		Addresses		AP connection is	AP connection	2.4G access	5G access	
₩	Behavior				normal	disconnected	1	1	
Ħ	Firewall	wan1 lan1			Z	0			
Ţ	Advanced application				Last 30 minutes tra	ffic analysis	Minutes		
0%	Services				Last so minutes tru	Last 30	winutes 🗸		

Fig 2.3.7 Normal R100 router system overview page

Cloud	Network Configur	ation Message	Personal	ି ନୁ English
(9) Overview				
Network A Manage	1/1	2/2	0/0	
	Total User	Online User	Authentication User/Accumulated Today	T Edci
	Webpage 0 B Download 0 B	0 B	3/4	■5G 1 Each ■2.4G 1 Each
	Top 3 Traffic in 7 Days	7 Days Total Flow	Online Authenticated/Accumulated Today	Total Wireless Traffic (Day) 0 B
	User Online Trend Total U	Jser 🗧 New User 🔳 Old U	lser	Last 7 Days Last 30 Days

Fig 2.3.8 Cloud access of R100 router with cloud page

Clou	Network Configu ud	uration Message	Personal			% ନ୍ଧୁ	English
() Overview	Network / testing / AP List						
🖳 Network							
A Manage	Remarks	Q			Upgrade	Restart	Return
	Status 🗢 Remarks 🜩	Add	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	
		Total 2	10/page V K	> Go to 1			

#### 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

	CMD-COS-v1.01				<u>්</u> ර අ ළ ම
	≡<	System Setup	System Setup > Advanced Settings > A	ALG Set	ដ្ឋើ៖ CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX:
$\sim$	System		ALG Set		
(~)	Overview	Basic Setting			
<u>-</u>	Monitoring	Disk management	FTP ALG:	Open	
ţĊ	System Setup	Cloud Account	TFTP ALG:	✓ Open	
₼	Network	Advanced Settings	SIP ALG:	✓ Open	
tłt	Flow Control		H323 ALG:	✓ Open	
<b></b>	Access Controller	Administration $$		Save	
<u>&amp;</u> =	Authentication	Upgrading 🗸 🗸		Save	
₩	Behavior	Reboot			
Ħ	Firewall				
Ţ	Advanced application				
0% 00	Services				
ŀð	Log				

#### 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

	CMD-COS-v1.01							<u>ර් ර ද</u>	English	
	=,	System Setup	System Setup	> Administration > User Accounts		🛱 CPU: 0.25% 📮 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s				
<b>•</b>	Sustem	· ·	User Accou	ints						
(~)	Overview	Basic Setting								
₩	Monitoring	Disk management					Add	Enable Disable	Delete	
ţĊ	System Setup	Cloud Account	Username	Password	Right group	Safe IP addr	Status	Actions		
品	Network	Advanced 🗸 🗸	admin	<b>朱黄</b> 虎天 <b>向</b> 代	Superadministrator	0.0.0/0	Enabled	Edit	_	
†∔†	Flow Control	Administration ^	Showing 1 o	f 1 records		PerPage 20 V Rows 《 1 > 》 1 //Pages Jump				
<b>(</b>	Access Controller	User Accounts	Help:	1.please configure carefully to allo	w access to IP (default is not lim	ited), input format supp	port: 192.168.1.1192.168.1.1-	192.168.1.200192.168.1.0/2419	92.168.1.0	
<u>&amp;</u> =	Authentication	Remote Access		2.when adding the same privilege	d account, copying can quickly c	omplete the permission	s configuration			
₩	Behavior	Upgrading 🗸 🗸 🗸								
臣	Firewall	Reboot								
Ţ	Advanced application									
0% 00	Services									
ľð	Log									

Fig 2.5.1 Default User Accounts page

CMD-COS-V						
≡<	System Setup 〈	System Setup > Administration > User Accou	nts			ାଙ୍ଭୁଁ CPU: 0.50% 🛄 MEM: 18% ↑ TX: 162.00 B/s ↓ F
System	Basic Setting	Username:		*		
C <sup>2</sup> Overview	Disk	Password:		*		
안 Monitoring	management	Confirm password:		*		
ුරි System Setup	Cloud Account	Safe IP addr:	0.0.0.0			
Retwork	Advanced $\checkmark$	Default permission:	Read Write	$\checkmark$		
111 Flow Control	Administration ^	Login Status Timeout	120 * minute			
Access	User Accounts	Login Status Hineout.	Open Change Bernus d Durin	dia lla		
Controller	n	Login Password Security:	UpenChange Password Perio	dically		
e.j Authenticatio	n Remote Access	Access level set:	Permission page	🗌 Visit	🗌 Edit	
🕁 Behavior	Upgrading $\vee$		+ Monitoring			
🖽 Firewall	Reboot		+ System Setup			
			+ Network			
Advanced application			+ Flow Control			
Services			+ Access Controller			
_			+ Authentication			
ևը՝ լաց			+ Behavior			
			+ Firewall			
			+ Advanced application			
			+ Services			
			+ Log			

Fig 2.5.2 Add User Accounts page

CMD-COS- <u>v1.01</u>						
≡'	System Setup	System Setup > Administration > User Accou	unts			
System	Basic Setting	Username:	COMMANDO1		*	
Overview	Disk	Password:	******		*	
Monitoring	management	Confirm password:	******		*	
System Setup	Cloud Account	Safe IP addr:	0.0.0.0			
Network	Advanced Settings	Default permission :	Read Write	~		
Flow Control	Administration	Login Status Timeout:	120 * minut	e		
Access Controller	User Accounts	Login Password	OpenChange Password Pe	riodically		
Authentication	Remote Acc <u>ess</u>	Security:		,		
R-L		Access level set:	Permission page	U Visit		
benavior	Upgrading		+ System Setup			
Firewall	Reboot		+ Network	<b>V</b>		
Advanced application			+ Flow Control			
Services			+ Access Controller			
lon			+ Authentication			
			+ Behavior			
			+ Firewall			
			+ Advanced application			
			+ Services	<b>V</b>		
			+ Log	<b>v</b>		
	CND-COS-V101	CMC-COS-VIAT       CMC-COS-VIAT       System       Systemice       Systemice       Monitoring       Disk       Systemice       Monitoring       Systemice       Systemice       Systemice       Systemice       Systemice       Systemice       Courd Could Account       Administration       Access       Behavior       Serrices       Advanced       Log	CMCACCGANAL       System Setup       System Setup > Administration > User Accord         System Setup > Outer Setup > Administration > User Accord       Basic Setting Password:       Password:         Nonitoring System Setup > Cloud Accourt       Confirm password:       Safe IP addr:         Network   Administration >       Conduct Court       Safe IP addr:       Default permission:         Row Control   Administration >       Controller       Default permission:       Login Status Timeout:         Authentication   Remote Access       Services       Login Password Scrifty;       Access level aet:         Services   Log       Reboot       Heboot       Heboot       Heboot         Ing       Image Accourts       Heboot       Heboot         Services   Log       Image Acceurts       Heboot         Services   Log       Image Acceurts       Heboot         Log       Image Acceurts       Heboot         Services   Log       Image Acceurts       Heboot         Log       I	CMC/CCC/+101       System Setup <       System Setup >> Administration > User Accounts         System       Basic Setting       Username:       COMMANDO1         System Setup       Cox       Password:       e=======         System Setup       Coud Account       Safe IP addr:       0.0.0         Row Control       Advanced       Default permission:       Read Write         Authentication       Remote Access       Default permission:       Read Write         Behavior       Upgrading       OpenChange Password Password       OpenChange Password Password Password         Advanced       Advanced       OpenChange Password       OpenChange Password Password Password         Services       Login Password       OpenChange Password       Services         Log       Reboot       Heboarie       Heboarie       Heboarie         Log       Services       Services       Services       Services         Log       Log       Services       Services       Services       Services <tr< th=""><th>CMC-CCS-101       System Setup        System Setup &gt; Administration &gt; User Accounts         System Netup        Basic Setting       Username:       COMMANDO1         Monitoring Disk management        Confirm password:       ************************************</th><th>Concorrel   System   System Setup   System Setup   Control   Advanced   Services   Behavior   Authentication   Services   Log     Retoot   Advanced   Application   Services   Log     Services   Log     Services   Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log                                                                                                                                    &lt;</th></tr<>	CMC-CCS-101       System Setup        System Setup > Administration > User Accounts         System Netup        Basic Setting       Username:       COMMANDO1         Monitoring Disk management        Confirm password:       ************************************	Concorrel   System   System Setup   System Setup   Control   Advanced   Services   Behavior   Authentication   Services   Log     Retoot   Advanced   Application   Services   Log     Services   Log     Services   Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log     Services     Log                                                                                                                                    <

Fig 2.5.3 Add User Account with visit permission page

	CMD-COS-v1.01								⊃ û ¢	🛆 English
	≡<	System Setup	System Setup	> Administra	ation > User Accounts			EPU: 6.00% EMEM: 17	% ↑ TX: 8.44 KB/s	↓ RX: 179.76 KB/s
	System		User Accou	nts						
(~)	Overview	Basic Setting								
∽	Monitoring	Disk 🗸 🗸						Add	Enable Disable	Delete
ţĈţ	System Setup	Cloud Account	Username		Password	Right group	Safe IP addr	Status	Actions	
0		Advanced	COMMANDO	0	*****	Superadministrator	0.0.0/0	Enabled	Edit	
666	Network	Settings	COMMAND	01	****	Custom permission	0.0.0.0	Enabled	Edit Disable De	iete
ţţţ	Flow Control	Administration ^							Сору	
<b></b>	Access Controller	User Accounts	Showing 1-2	of 2 records			PerPag	e 20 V Rows « <	1 > > 1	/1Pages Jump
8= ;	Authentication	Remote Access	Hele -	1	-6	anna an 10 (dafaula is nat linsi			169 1 200102 169 1 0/2	4103 169 1 0
<b>↓</b>	Behavior	Upgrading 🗸 🗸	Help:	/255.255.25 2.when add	ingure carefully to allow a 55.0. ling the same privileged ac	count, copying can quickly co	mplete the permission	s configuration	00.1.200192.100.1.0/22	192.100.1.0
Ħ	Firewall	Reboot								
y	Advanced application									
00	Services									
ß	Log									

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

	CMD-COS-v1.01				🔿 🕁 👃 English						
	=,	System Setup	System Setup > Adm	ninistration > Remote Acc	ess 🔂 CPU: 0.75% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s						
	-		Remote Access								
ଚ	Overview	Basic Setting									
<u>-</u>	Monitoring	Disk management	Remote Access Contr	trol							
ţې:	System Setup	Cloud Account		Telnet Server:	Open Console						
	Matural	Advanced		Web Interface:	Allow access to web interface from public network						
670	INETWORK	Settings	_	Required HTTPS:	Use HTTPS to access the web interface						
tłł	Flow Control	Administration	<ul> <li>.</li> </ul>								
	Access	User Accounts		HTTP Access Port:							
6-1				HTTPS Access Port:	443 •						
( <u>8</u> .)	Authentication	Remote Access		Custom SSL Certificate:	Administration (Support only Nginx server certificates)						
\$	Behavior	Upgrading	/								
臣	Firewall	Reboot	<b>N</b>								
	Advanced		Remote Maintenance	Provente Channels							
7	application			Remote Channel:	Open Console						
	Services			Remote Port:	22 *						
ሌ	Log			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.							
				Save							
			_								

Fig 2.5.7 Remote Access control page

System Setup > Administration > Remote Access

Remote Access

# Remote Access Control Telnet Server: Image: Open Console Web Interface: Image: Allow access to web interface from public network Required HTTPS: Image: 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 Main	tenance	
	Remote Channel:	✓ Open Console
	Remote Port:	22 *
	Remote Password :	•••••
	Caution: 1. Cloud is viewing de 2. For your	a cloud platform that centrally manages fast routing. You can view and manage your devices in the cloud, such as: vice operation, modifying configuration, and authentication management. Go to Binding security, please do not open remote maintenance at the request of non-official personnel.

Fig 2.5.9 Setting password for Remote Access page

	CMD-COS-v1.01			් දා ද English							
		System Setup	System Setup > Administration > Remot								
~	System	Paula Cambra	Remote Access								
63	Overview	Dasic Setting									
<u>w</u>	Monitoring	Disk management	, Remote Access Control								
ţ.	System Setup	Cloud Account	Telnet Server:	Open Console							
品	Network	Advanced Settings	Web Interface:	Allow access to web interface from public network							
t#	Flow Control	Administration	Required HTTPS:	V Use HTTPS to access the web interface							
۲	Access Controller	User Accounts	HTTPS Access Port:	443 *							
<u>8</u> =	Authentication		Custom SSL Certific	ste: Administration (Support only Noinx server certificates)							
₩	Behavior	Upgrading									
臣	Firewall	Reboot									
	Advanced		Remote Maintenance	Deve Counte							
	application		Remote Channel:	V open Console							
	Services		Remote Port:	22 •							
Ъ	Log		Remote Password:	•••••							
			Caution: 1. Cl. auth 2. Fo	ud 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 infication management. Go to Binding your security, please do not open remote maintenance at the request of non-official personnel.							
			Save								

#### 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.

	CMD-COS-v1.01				스) 샵 슈 온 English
	$\equiv$	System Setup <	System Setup > Administration > Remote Access		🚦 CPU: 0.00% 🛄 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
Ð	System Overview	Basic Setting	Administration (Custom SSL Certificate)		X
~	Monitoring	Disk management			
ţ	System Setup	Cloud Account	Custom SSL Certificate: Ope	'n	
뮮	Network	Advanced $\checkmark$ Settings	Certificate(CRT):		
t+t	Flow Control	Administration ^			
۴	Access Controller	User Accounts			
<u>&amp;</u> =]	Authentication	Remote Access	Private Key(KEY):		
$\stackrel{\checkmark}{\Rightarrow}$	Behavior	Upgrading 🗸 🗸			
臣	Firewall	Reboot			
Ţ	Advanced application		Remarks:		
0%	Services				
ſĿ	Log		Sa	ve Cancel	

Fig 2.5.11 Administration (Custom SSL Certificate) page

RuTTY Configuration		?	×
Category:			
<ul> <li>Session</li> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> <li>Colours</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	Basic options for your PuTTY se         Specify the destination you want to conne         Host Name (or IP address)         192.168.1.1         Connection type:         Raw         Raw         Telnet         Raw         Saved Sessions         Default Settings         Close window on exit:         Always         Never         Only on cl	ssion ct to Port 23 C C C C C C C C C C C C C C C C C C	Serial ad ve ete
About Help	Open	Can	icel

Fig 2.5.12 Putty for Telnet access of device page

19 🚰	ም 192.168.1.1 - PuTTY												
user	name: admin												
pass	wd:												
C	onsole for English				Version:								
CMD	-COS-V1.01												
0.	System status		WEB Address	-> http	//192.168.1.1.8								
0 .	System Status		HED Address	> 1100p	,,,152.100.1.110								
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)	LinkDown												
з.	Set WEB port		lanl	(veth3	08:24:7c:e0:63:								
31)	LinkDown												
4.	Ping Test	L	lanl	(veth4	08:24:7c:e0:63:								
32)	LinkDown												
	Clean acl rule	1	wanl	(veth5	08:24:7c:e0:63:								
33)	LinkDown												
	Restore default	1											
7.	Restore WEB passwd												
8.	Reboot/Shutdown												
9.	Ethernet driver												
ο.	Other option												
q.	Quit												
PI	ease input:												
c	onsole for English				Version: CMD-CO	5-v1.01							
Ο.	System status		WEB Address -	-> http	://192.168.1.1:80								
	Set ether band	L	lanl	(vethl	08:9b:4b:50:1c:bc)	LinkUp							
2.	Set lan/wan address	I	lanl	(veth2	08:24:7c:e0:63:30)	LinkDown							
з.	Set WEB port	I.	lanl	(veth3	08:24:7c:e0:63:31)	LinkDown							
4.	Ping Test	l	lanl	(veth4	08:24:7c:e0:63:32)	LinkDown							
	Clean acl rule		wanl	(veth5	08:24:7c:e0:63:33)	LinkDown							
	Restore default												
	Restore WEB passwd												
8.	Reboot/Shutdown												
9.	Ethernet driver												
ο.	Other option												
q.	Quit												
Pl	ease 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.

	CMD-COS-v1.01			් 🗘 🗘 L English	
	_<	System Setup	System Setup > Upgrading > Version U	n Upgrade 📮 CPU: 3.25% 🖵 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s	s
~	Sustem		Version Upgrade		^
(-)	Overview	Basic Setting			
₩	Monitoring	Disk management	Automatic Updates		
ţĊ	System Setup	Cloud Account	Version Check :	Check New Version	
₽	Network	Advanced 🗸 🗸 🗸	Route system version:	n: 3.4.5	
ţţţ	Flow Control	Administration $\checkmark$	Current Protocol version:	2.0.109	
<b></b>	Access Controller	Upgrading ^	Communication tools version :	s 2.1.6	
<u>&amp;=</u>	Authentication	Version Upgrade	Current WEB version :	: 2.1.0	
₩	Behavior	Backup and Restore	Auto Upgrade:	🗹 Protocol library 🛛 🧭 Communication tool feature library 🔄 URL feature library	
Ħ	Firewall	Reboot			
Ţ	Advanced application		Manual Updates		
0%	Services		Local Upgrade :	system & feature librar Select File Upload File	
ß	Log			Version update log Y	ľ

#### 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 mt7621v1m1\_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.

					C		۵	0	English
		System Setup <	System Setup > Upgrading > Version U	pgrade	: CPU: 5.00% ☐ MEM: 18%	6 ↑ TX: 9	.09 KB/s	↓ RX: 1	53.12 KB/s
Ð	System Overview	Basic Setting	Automatic Updates						
₩	Monitoring	Disk management	Version Check :	Check New Version					
ţĊ	System Setup	Cloud Account	Route system version:	3.4.5					
뮮	Network	Advanced ~ Settings	Current Protocol version:	2.0.109					
t+t	Flow Control	Administration $\checkmark$	Communication tools version :	2.1.6					
<b></b>	Access Controller	Upgrading ^	Current WEB version :	2.1.0					
<u>&amp;</u> =	Authentication	Version Upgrade	Auto Upgrade :	✓ Protocol library ✓ Communication tool feature library	✓ URL feature library				
, ¢	Behavior	Backup and Restore							
田	Firewall	Reboot	Manual Updates						
Ţ	Advanced application		Local Upgrade :	MT7621V1-M1_sysupgi Select File Upload File					
0% 00	Services			Version update log Y					
ſĿ	Log								

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.

	CMD-COS-v1.01						්	Û	¢ 2	English
	=<	System Setup	System Setup > Upgrading > Backup and	Restore		∎ <mark>⊒</mark> ≣ CPU: 4.00%	EMEM: 16%	↑тх	: 0.00 B/s 🗸	RX: 0.00 B/s
6	System	Basic Setting	Backup and Restore							
<u>6</u>	Overview Monitoring	Disk v management	Upload backup							
ţŷł	System Setup	Cloud Account								
品	Network	Advanced 🗸 🗸	Latest backup time:							
tit	Flow Control	Administration 🗸	Орюад Баскир:	Se	Upload confirmation					
r	Access Controller	Upgrading ^		Current config backup	Restore default configuration	Factory reset				
<u>&amp;</u> =	Authentication	Version Upgrade	Upload backup							
<b>↓</b> ≯	Behavior	Backup and Restore	Name backup	Date backup		Actions				
Ħ	Firewall	Reboot			No Data					
Ţ	Advanced application									
00	Services									
Ъ	Log									

# Fig 2.6.3 Default Backup and Restore page

System Setup > Upgrading > Backup and	Restore		≣ ☐ ☐ E C P U: 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:	Select file	Upload confirmation							
	Current config backup Restore	default configuration	Factory reset						
Upload backup									
Name backup	Date backup		Actions						
2018-06-01-003904.bak	2018-06-01 00:39:04		Edit Rx I	Restore Delete					

# Fig 2.6.4 Options Backup and Restore page

	CMD-COS-v1.01									
	_<	System Setup	System Setup >	Upgrading > Backup and Restore		≡ <u></u> ≣ CPU: 0.50%	🛄 MEM: 16%	↑ TX: 0.00 I	B/s ↓ RX	: 0.00 B/s
0			Backup and	lectoro						
(~)	Overview	Basic Setting				×				
~~		Disk management	Upload backuj							
ţĊ		Cloud Account		This action will restore the routing co	This action will restore the routing configuration to the default configuration, ok to continue?	ontinue?				
쁆	Network	Advanced $\checkmark$ Settings		ОК	Cancel					
<b>†</b> ↓†		Administration $\vee$								
<b></b>	Access Controller	Upgrading ^		Current o	onfig backup Restore default configurat	tion Factory reset				
<u>&amp;</u> =		Version Upgrade	Upload backup							
$\Leftrightarrow$	Behavior	or Backup and	Name backup		Date backup	Actions				
			2018-06-01-00	)3904.bak	2018-06-01 00:39:04	Edit Ra	Restore Delete			
Ē		Reboot								
Ţ	Advanced application									
0%										
ß	Log									

Fig 2.6.5 Backup the current configuration page

	CMD-COS-v1.01							්	) ¢	2	English
		System Setup	System Setup >	Upgrading > Backup and	Restore		ECPU: 0.50%	🛄 MEM: 16%	↑ TX: 0.00 I	B∕s ↓ R	X: 0.00 B/s
		System setup	Backup and P	octoro							
Ð	System Overview	Basic Setting				×					
~		Disk 🗸 🗸	Upload backu								
ţĊ}		Cloud Account		This action will restore t	he routing configuration to the d	efault configuration, ok to continue?					
₼	Network	Advanced $\checkmark$ Settings			OK	I					
<b>†</b> ↓†		Administration $\sim$									
	Access Controller	Upgrading ^			Current config backup	Restore default configuration	Factory reset				
&= ;;-		Version Upgrade	Upload backup								
$\leq$	Behavior	Backup and	Name backup		Date backup		Actions				
		Kestore	2018-06-01-00	3904.bak	2018-06-01 00	):39:04	Edit Rx	Restore Delete			
Ħ	Firewall	Reboot									
∽	Advanced application										
0 <i>%</i> 00											
ſ	Log										

Fig 2.6.6 Restoring default configuration page

	CMD-COS-v1.01							්	Û	¢ 2	English
	=<	System Setup	System Setup > Upgrading > Backup and Restore				l: 1.00%	🛄 MEM: 16%	↑ т	X: 0.00 B/s	↓ RX: 0.00 B/s
		· ·	Backup and P	octoro							
$( \cap $	System Overview	Basic Setting		Factory reset X							
~~		Disk management	Upload backuj	Restore factory setting							
ţĊţ		Cloud Account		Recovery will be resumed immediately a disconnection	ly after taking effect, restart will result in network						
	Network	Advanced $\checkmark$ Settings	✓ Current system Setting backup								
		Administration $\vee$									
<b></b>	Access Controller	Upgrading ^		OK	Cancel	Facto	ry reset				
&= 	Authentication	Version Upgrade	Upload backup								
$\Leftrightarrow$	Behavior	Backup and	Name backup		Date backup		Actions				
		Kestore	2018-06-01-003904.bak		2018-06-01 00:39:04		Edit Rx Restore Delete				
Ħ	Firewall	Reboot									
y	Advanced application										
0%											
ß											

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

	CMD-COS-v1.01								6 4 2	English
	=<	System Setup	System Setup > Rebo	oot				"	16% ↑ TX: 0.00 B/s 🗸	RX: 0.00 B/s
		,	Reboot							
Ð	System Overview	Basic Setting								
₩	Monitoring	Disk management	Restart Now					Add Er	able Disable	Delete
ţĊ	System Setup	Cloud Account	Schedule Events	Cycle	Date	Time	Remarks	Status	Actions	
뮯	Network	Advanced ~ Settings				N	o Data			
ţţţ	Flow Control	Administration $\checkmark$								
<b></b>	Access Controller	Upgrading 🗸 🗸								
<u>&amp;=</u>	Authentication	Reboot								
₩	Behavior									
臣	Firewall									
Ţ	Advanced application									
0%	Services									
Ռ	Log									

Fig 2.7.1 Default Reboot page

	CMD-COS-v1.01							د	⊃ û ¢ ,	C English
	=<	System Setup <	System Setup > Rebo	ot			≡ <mark></mark> ≣ CPU	: 1.00% 🛄 MEM: 189	% ↑ TX: 134.19 KB/s	↓ RX: 9.66 KB/s
~	System		Reboot							
6-3	Overview	Basic Setting								
₫⁄	Monitoring	Disk management	Restart Now					Add	Enable Disable	Delete
ţĊĵ	System Setup	Cloud Account	Schedule Events	Cycle	Date	Time	Remarks	Status	Actions	
₼	Network	Advanced 🗸 🗸				No	Data			
†∔†	Flow Control	Administration $\sim$								
<b>(</b>	Access Controller	Upgrading 🗸 🗸								
<u>&amp;</u> =	Authentication	Reboot								
₩	Behavior									
臣	Firewall									
Ţ	Advanced application									
0%	Services									
ſð	Log									

# Fig 2.7.2 Restart Now page

	CMD-COS-v1.01				$ riangle _  ightarrow $ $ riangle _  ightarrow $ English
	,≣<	System Setup	System Setup > Reboot		ដើ្ឌ CPU: 0.99% 🛄 MEM: 18% ↑ TX: 1.53 KB/s 🤳 RX: 2.75 KB/s
Ð	System	Basic Setting	Add		×
<u></u>	Monitoring	- Disk management	Schedule Events:	Reboot 🗸 *	
÷	System Setup	Cloud Account	Cycle:	Once ~	
뮮	Network	Advanced Settings	Date:	2021-04-22	
†∔†	Flow Control	Administration	Time:	23:59 *	
<b>R</b>	Access Controller	Upgrading	Remarks:		
<u>&amp;</u> =	Authentication	Reboot		Save	
⇆	Behavior			Caller	
田	Firewall				
Ţ	Advanced application				
0% 00	Services				
Ŀ	Log				

Fig 2.7.3 Default Schedule Restart page
	CMD-COS-v1.01					ථ	û	۵	<u>e</u> Engli	sh
	Ξ·	System Setup	System Setup > Reboot			=∰= CPU: 1.00% 🛄 MEM: 18%	↑ тх:	2.67 KB/s	↓ RX: 2.40	KB/s
ଚ	System Overview	Basic Setting	Add							×
₹	Monitoring	Disk management	Schedule Events:	Reboot	*					
ţĊţ	System Setup	Cloud Account	Cycle:	Everyday	$\sim$					
品	Network	Advanced v Settings	Time:	12:50 *						
ţţţ	Flow Control	Administration $\checkmark$	Remarks:	Daily reboot						
<b></b>	Access Controller	Upgrading $\sim$		Save						
<u>&amp;</u> =	Authentication	Reboot								
₩	Behavior									
Ħ	Firewall									
Ţ	Advanced application									
0%	Services									
լ	Log									

## Fig 2.7.4 Add Schedule Restart page

	CMD-COS-v1.01							۵	습 🗘 🔔 Eng	glish
	—< System Setup <		System Setup > Reboo	ot			E CP	U: 2.25% 🛄 MEM: 189	6 ↑ TX: 3.46 KB/s 🤳 RX: 2.9	96 KB/s
-			Reboot							
63	Overview	Basic Setting								
₩	Monitoring	Disk management	Restart Now					Add Ena	able Disable Dele	ete
ţĈ	System Setup	Cloud Account	Schedule Events	Cycle	Date	Time	Remarks	Status	Actions	
品	Network	Advanced $\checkmark$ Settings	Reboot	Everyday		12:50	Daily reboot	Enabled	Edit Disable Delete	
†∔†	Flow Control	Administration $$	Showing 1 of 1 record	ds			PerPage 20	∨ Rows ≪ <	$1 > \gg 1$ /1Pages	Jump
<b></b>	Access Controller	Upgrading $\lor$								
<u>&amp;</u> =	Authentication	Reboot								
₩	Behavior									
E	Firewall									
Ţ	Advanced application									
0% 00	Services									
ſð	Log									

# Fig 2.7.5 Schedule Restart everyday page

## NETWORK

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

## DHCP:

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

## DNS:

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

## **IP/MAC Group:**

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

## Static Routes:

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

## VLAN:

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

## UPNP:

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

## NAT:

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

## Port Mapping:

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

## IPv6:

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

### **IGMP Agent:**

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

## Fig 3.1 Network Tab options page

## 1. Interfaces

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

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



Fig 3.1.1 Default interface setting page

	CMD-COS-v1.01				<u> ሰ ት ቅ </u> የ	inglish
	=,	Network	<	Network > Interfaces	±0± CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX	: 0.00 B/s
6	System Overview	Interfaces		External network settings $\ \textbf{wan1} \ \oplus \$		×
~	Monitoring	DHCP	~	Select Interface:	08:247c=0.65:33   Ralink MT7530 10/100/1000 Etherns V Unbind	
÷	System Setup	DNS	~	Access Mode DHCP (Dynam	c Assianed)	
品	Network	IP/MAC Group	~	Status: Connection		
tłł	Flow Control	Static Routes	~		Connect	
۴	Access Controller	VLAN		IP Address:		
<u>&amp;</u> =	Authentication	VPN Client	$\sim$	Gateway:		
\$	Behavior	UPNP	~	Preferred DNS :		
臣	Firewall	NAT		Alternative DNS:		
V	Advanced application	Port Mapping	$\sim$	Default Gateway: Set this line	as the default gateway (When you have multiple ISP lines, please select one as the default gateway )	
	Services	IPv6	~	Failover: 🗸 Switch if Li	e Dropped (No need to use when only 1 ISP line)	
Ъ	Log	IGMP Agent		Leased Time: 0 se	ond	
				Online Time Control : 00:00 -	23.59 *	
				Line Detection: HTTP+PING+0	ateway 🗸	
				www.google.c	m	

## Fig 3.1.2 Default External Network setting options

	CMD-COS-v1.01									English
	≡́	Network	<	Network > Interfaces		i CPU: 4.50%	🛄 MEM: 19%	↑ TX: 27.00 B	′s↓	RX: 27.00 B/s
~	System	late from		External network settings wan1 $\oplus$						×
6.3	Overview	interlaces								
22	Monitoring	DHCP		Select Interface:	veth5   wan1   08:24:7c:e0:63:33   Ralink MT7530 10/100/1000 Etherne 🗸 Unbind					
ţ	System Setup	DNS		Access Mode:	DHCP (Dynamic Assigned)					
品	Network	IP/MAC Group		Status:	Connected Disconnect rebroadcast					
tit	Flow Control	Static Routes		IP Address:	192.168.1.37					
۲	Access Controller	VLAN		Subnet Mask:	255.255.255.0					
<u>&amp;=</u>	Authentication	VPN Client		Gateway:	192.168.1.1					
₩	Behavior	UPNP		Preferred DNS :	192.168.1.1					
臣	Firewall	NAT		Alternative DNS:						
Ţ	Advanced application	Port Mapping		Default Gateway:	Set this line as the default gateway (When you have multiple ISP lines, please select one as the default gateway)					
0% 00	Services	IPv6		Failover:	Switch if Line Dropped (No need to use when only 1 ISP line)					
Ъ	Log	IGMP Agent		Leased Time:	432000 second					
				Online Time Control:	00:00 - 23:59 *					
				Line Detection:	HTTP+PING+Gateway $\vee$					
					www.google.com					
				Remarks:						

Fig 3.1.3 Setting External Network setting for WAN1 interface page

	CMD-COS-v1.01							
	⊒<	Network <	Network > Interfaces					
~	System		Intranet settings la	n1 ⊕				
6-3	Overview	Interfaces						
₩	Monitoring	DHCP ~		Select Interface:	veth1   Jan1   0	8:9b:4b:50:1c:bc   Ral	ink MT7530 10/	100/1000 Ethernet 🗸
÷	System Setup	DNS ~		IP Address:	192,168,1,1			•
品	Network	IP/MAC Group		Subnet Mask:	255,255,255,00	24)		~
<u>†∔†</u>	Flow Control	Static Routes V		Remarks:		- ''		
	Access Controller	VLAN						
87	Authentication	VPN Client 🗸 🗸	Advanced Settings ~					
	Pahador			Working Mode:	Auto-Negotiat	ion(Default)		~
÷*)	benavior	Urivr V		NIC Speed	Auto-Negotiat	ion(Default)		~
臣	Firewall	NAT						
Ø	Advanced application	Port Mapping $\sim$		Mutual Access:	Allow Mutu	al LAN Access		
00 00	Services	IPv6 ~		Clone MAC:				
ъ	Log	IGMP Agent		Multiple IP:				Add
					IP Address	Subnet	Mask	Actions
							No Data	
				Extended Network Cords				
				Extended Network Card:				
					veth1	veth2	✓ veth3	✓ veth4
					Save	Cancel		

Fig 3.1.5 Default intranet Network setting for LAN1 interface page

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

CMD-COS-v1.					
=,	Network	<	Network > Interfaces		кÖ́а CPU: 0.50% 🛄 МЕМ: 19% ↑ ТХ: 317.00 В/s ↓ R
System	Interfaces		IP Address:	192.168.0.1	
Monitoring	DHCP	$\sim$	Subnet Mask:	255.255.0(24) 🗸	
— දබූ System Setup	DNS	~	Remarks:		
Retwork	IP/MAC Group	$\sim$	Advanced Settings ^		
How Control	Static Routes	~	Working Mode:	Auto-Negotiation(Default) $\lor$	
Controller	VLAN		NIC Speed:	Auto-Negotiation(Default)	
Authentication	VPN Client	~	Mutual Access:	Allow Mutual LAN Access	
🕁 Behavior	UPNP	~	Clone MAC:		
Firewall	NAT		Multiple IP:	Add	
Advanced application	Port Mapping	~		IP Address Subnet Mask Actions	
Services	IPv6	~		No Data	
Log	IGMP Agent				
			Extended Network Card	veth1 veth2 veth3 veth4	
				Save Cancel	

## 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.

	CMD-COS-v1.01		තා 🟠 🗘 English	
	≡<	Network <	Network > Interfaces 😳 CPU: 0.00% 🛄 MEM: 19% ↑ TX: 82.00 B/s ↓ RX: 0.00 B/s	
ଚ	System Overview	Interfaces	Interface Settings	î
5	Monitoring	DHCP 🗸		
ţĝ;	System Setup	DNS 🗸	WAN         I WAN Connected         J U Connection Count         LAN         I LAN Connected         I DHCP Server Enabled         T Device Connected           Status         Status<	
볾	Network	IP/MAC Group 🗸 🗸	Interface Status	
†∔†	Flow Control	Static Routes $\sim$	3	
	Access Controller	VLAN		
8 <u>.</u>	Authentication	VPN Client $\sim$	veth2 veth3 veth4	
↓	Behavior	UPNP 🗸		
Ħ	Firewall	NAT	1 WAN Interface	
7	Advanced application	Port Mapping $\sim$		
0% 00	Services	IPv6 $\checkmark$	wan1	
ß	Log	IGMP Agent	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) OWAN (Public)		
Select Interface:	✓ Bind		
	veth2   free   08:24:7c:e0:63:30   Ralink MT7530 10/100/1000 Ethernet Controller		
	veth3   free   08:24:7c:e0:63:31   Ralink MT7530 10/100/1000 Ethernet Controller		
	veth4   free   08:24:7c:e0:63:32   Ralink MT7530 10/100/1000 Ethernet Controller		



CMD-COS-v1.0	1		ා රු 🗘 Le English
≡<	Network <	Network > Interfaces	t <sup>©</sup> CPU: 0.00% □ MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
System	Interfaces	External network settings wan1 wan2 ⊕	×
Monitoring	рнср 🗸		
ද්ථූර් System Setup	DNS 🗸	Select Interface: veth2   wan2   08:24:7ce0:53:30   Ralink M17530 10/100/1000 Etherne V On Access Mode: Static IP (Fixed IP) V	bind
品 Network	IP/MAC Group 🗸 🗸	IP Address: 223.1.1.5	
†∔† Flow Control	Static Routes $\sim$	Subnet Mask: 255.255.0(24) 🗸	
Controller	VLAN	Gateway: 223.1.1.1 *	
윤 Authentication	VPN Client $\vee$	Multiple IP: Add	
⇒ Behavior	UPNP 🗸	IP Address Subnet Mask Actions	
Firewall	NAT	No Data	
Advanced application	Port Mapping 🛛 🗸		
Services	IPv6 V	Default Gateway: Set this line as the default gateway (When you have multiple ISP lines, please	select one as the default gateway )
Log	IGMP Agent	Failover: Switch if Line Dropped (No need to use when only 1 ISP line)	

Fig 3.1.9 Creating WAN2 interface page



## Fig 3.1.10 Network interface page after creating WAN2 interface page

	CMD-COS-v1.01			ے 🖒 🖒 🕰 English
	=,	Network	Network > Interfaces	🛱 CPU: 0.00% 🛄 MEM: 20% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
E	System Overview	Interfaces	Intranet settings Ian1 Ian2 ⊕	Х
₩	Monitoring	DHCP	NIC Usage: () LAN (Private)	
÷	System Setup	DNS	Select Interface : veth3   free   08:24:7c:e0:63:31   Ralink MT7530 10/100/1000 Ethernet 🗸	Bind
뮮	Network	IP/MAC Group		
†∔†	Flow Control	Static Routes		
•	Access Controller	VLAN		
<u>8</u> "	Authentication	VPN Client		
₩	Behavior	UPNP		
臣	Firewall	NAT		
Ţ	Advanced application	Port Mapping		
0%	Services	IPv6		
Ъ	Log	IGMP Agent		

Fig 3.1.11 Creating LAN2 interface page

	CMD-COS-v1.01			තා 🕆 👃 Langlish
	=,	Network <	Network > Interfaces	😳 CPU: 0.75% 🔤 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
ଚ	System Overview	Interfaces	Intranet settings lan1 lan2 $\oplus$	×
₩	Monitoring	DHCP 🗸 🗸	6 L 11 L 1	
ţ	System Setup	DNS ~	IP Address:	Veths (Tan2 ) US24:7CEVES:31 ) Rallink M17530 TU/100/1000 Emernet V Unbind
몲	Network	IP/MAC Group 🗸 🗸	Subnet Mask:	255 255 0(24)
tit	Flow Control	Static Routes 🗸 🗸 🗸	Remarks:	COMMANDO LAN-2
•	Access Controller	VLAN		
<u>&amp;</u> "	Authentication	VPN Client $\sim$	Advanced Settings A	
¢↓	Behavior	UPNP 🗸	Working Mode:	Auto-Negotiation(Default)
Ħ	Firewall	NAT	NIC Speed:	Auto-Negotiation(Default)
y	Advanced application	Port Mapping 🛛 🗸	Mutual Access:	Z Allow Mutual LAN Access
0%	Services	IPv6 🗸	Clone MAC:	
Ъ	Log	IGMP Agent	Multiple IP:	Add IP Address Subnet Mask Actions
				No Data

## Fig 3.1.12 Setting LAN2 interface parameter page

×	CMD-CO5-v1.01		ත රු 🗘 දී English
	≡<	Network <	Network > Interfaces
Ð	System Overview	Interfaces	
₩	Monitoring	DHCP 🗸 🗸	WAN         Z WAN Connected         I Z Connected Count         LAN         Z LAN Connected         I Drice Server Enabled         I Device Connected           Status         Status<
ŝ	System Setup	DNS 🗸	Interface Status
놂	Network	IP/MAC Group 🗸 🗸	Unoccupied Interface Config
†#†	Flow Control	Static Routes $\sim$	
•	Access Controller	VLAN	veth4
<b>₽</b> .	Authentication	VPN Client $\sim$	lan2
⇔	Behavior	UPNP 🗸	2 WAN Interfac Connection Connected Status:
臣	Firewall	NAT	IP:         192.168.10.1
Ţ	Advanced application	Port Mapping $\sim$	wan1 MAC: 08:24:7c:e0:63:31
0% 00	Services	IPv6 🗸	Remarks: COMMANDO LAN-2
Ռ	Log	IGMP Agent	
			Ian1     Ian2

Fig 3.1.13 Network interface page after creating LAN2 interface page

	CMD-COS-v1.01		තා රු 🗘 La English
	≡́	Network <	Network > Interfaces
6)	System Overview	Interfaces	2 WAN connected 13 connection Count 2 LAN connected 1 DHCP Server Enabled 1 Device Connected
₽2	Monitoring	DHCP 🗸 🗸	Status Status
ţĊ	System Setup	DNS $\sim$	Interface Status
몲	Network	IP/MAC Group 🗸 🗸	1 Unoccupied Interface Config
tit	Flow Control	Static Routes $\sim$	
•	Access Controller	VLAN	veth4
<u>₿</u> ",	Authentication	VPN Client $\lor$	
\$↓	Behavior	UPNP 🗸	2 WAN Interface
臣	Firewall	NAT	
y	Advanced application	Port Mapping $$	wan1 wan2
0% 00	Services	IPv6 V	
Ъ	Log	IGMP Agent	2 LAN Interface
			lan1 lan2

## 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

	CMD-COS-v1.01		තා රු 🗘 L English
	=<	Network <	Network > Interfaces 📫 CPU: 0.00% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
			Interface Settings
6	Overview	Interfaces	
~~	Monitoring	DHCP 🗸 🗸	
ŝ	System Setup	DNS 🗸	WAN         I WAN Connected         I Z Connection Count         LAN         Z LAN Connected         I DRCP server chapled         O Device Connected           Status         Status<
몲	Network	IP/MAC Group 🗸 🗸	Interface Status
†∔†	Flow Control	Static Routes $\sim$	
٩	Access Controller	VLAN	
<u>8</u> "	Authentication	VPN Client $\checkmark$	1 WAN Interfac Connected Status:
₩	Behavior	UPNP 🗸	<b>0</b> IP: 192.168.10.1
臣	Firewall	NAT	Subnet Mask:         255.255.255.0           wan1         MAC:         08.24.7c.e0r.63.31
Ţ	Advanced application	Port Mapping 🛛 🗸	Remarks: COMMANDOLAN-2
0% 00	Services	IPv6 ~	2 LAN Interface Bind Device: veth3/Connected/100Mbps/Full-Duplex
ß	Log	IGMP Agent	lan1 lan2

Fig 3.1.15 Deleting interface after creating user defined LAN2 interface page

	CMD-COS-v1.01			යා රු 🗛	🛆 English
	=	Network	Network > Interfaces	📮 CPU: 2.48% 🛄 MEM: 19% ↑ TX: 27.00 E	3/s 👃 RX: 27.00 B/s
	Sustam		Intranet settings lan1 lan2		×
63	Overview	Interfaces			
<u>-</u>	Monitoring	DHCP	Select Interface :	veth3   Jan2   08:24:7c:e0:63:31   Ralink MT7530 10/100/1000 Ethernet	
ţĊ	System Setup	DNS	/		
모	Network	IP/MAC Group	IP Address:	192.168.10.1	
000		in y make choup	Subnet Mask:	255.255.255.0(24) ~	
†‡†	Flow Control	Static Routes	Remarks:	COMMANDOLAN-2	
۲	Access Controller	VLAN			
<u>₽</u> ,	Authentication	VPN Client	Advanced Settings ~		
⇆	Behavior	UPNP	/	Save Cancel	
臣	Firewall	NAT			
Ţ	Advanced application	Port Mapping			
0% 00	Services	IPv6			
Ъ	Log	IGMP Agent			

# Fig 3.1.16 Unbinding port from LAN2 interface page

	CMD-COS-v1.01		තා 🗘 🗘 La English
	Ξ·	Network <	Network > Interfaces 👜 CPU: 83.50% 🛄 MEM: 20% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System Overview	Interfaces	
₩	Monitoring	DHCP 🗸 🗸	Status Status
ţĝ	System Setup	DNS ~	Interface Status
몲	Network	IP/MAC Group 🛛 🗸	
t++	Flow Control	Static Routes $\sim$	
¢	Access Controller	VLAN	veth3
<u>8</u> "	Authentication	VPN Client $\sim$	
\$↓	Behavior	UPNP 🗸	1 WAN Interface
臣	Firewall	NAT	
y	Advanced application	Port Mapping $\sim$	wani
0% 00	Services	IPv6 $\vee$	Idle Interface, unbound network
Ъ	Log	IGMP Agent	2 LAN Interface card
			lan1 lan2

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

	CMD-COS-v1.01			스) 슈 슈 온 English
	=<	Network <	Network > Interfaces	n CPU: 10.40% 🛄 MEM: 20% ↑ TX: 27.00 B/s 🤳 RX: 27.00 B/s
6	 System	Interfaces	Intranet settings Ian1 Ian2 🕀	×
~~,	Overview Monitoring	рнср ~		
~			NIC Usage: <ul> <li>LAN (Private)</li> </ul>	
:Ç;	System Setup	DNS ~	Select Interface: V Bind	Delete
놂	Network	IP/MAC Group 🗸 🗸		
†4†	Flow Control	Static Routes $\sim$		
۲	Access Controller	VLAN		
<u>8</u> "	Authentication	VPN Client $\sim$		
₩	Behavior	UPNP ~		
臣	Firewall	NAT		
J	Advanced application	Port Mapping $\sim$		
	Services	IPv6 V		
Ъ	Log	IGMP Agent		

## Fig 3.1.17 Deleting port from LAN2 interface page

смр-соз-		තා 🗘 👃 Langlish
≡<	Network <	Network > Interfaces
System Overview	Interfaces	1 WAN Connected 9 Connection Count 1 LAN Connected 1 DHCP Server Enabled 3 Device Connected
Monitoring	DHCP 🗸	Status
දබූදි System Setu	p DNS 🗸	Interface Status
品 Network	IP/MAC Group 🗸 🗸	Unoccupied Interface Config
111 Flow Contro	Static Routes $\sim$	
Access Controller	VLAN	veth3
올 Authenticati	on VPN Client $\sim$	
∽ Behavior	UPNP $\lor$	1 WAN Interface
Firewall	NAT	
Advanced application	Port Mapping $\sim$	wan1
음악 Services	IPv6 $\checkmark$	
Log	IGMP Agent	1 LAN Interface
		lan1

## 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.

<u>_</u>	<u>}</u>					
CHOMAN	CMD-COS-v1.01					C⊅ Englis
	≡́	Network	<	Network > Interfaces		i៉្មi CPU: 0.75% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00
	System			Intranet settings lan1 🕀		×
6-3	Overview	Interfaces				
5	Monitoring	DHCP	~	Select Interface:	veth1   lan1   08:9b:4b:50:1c:bc   Ralink: MT7530 10/100/1000 Ethernet $\vee$	
÷	System Setup	DNS	~	IP Address:	192.168.0.1	
厵	Network	IP/MAC Group	~	Subnet Mask:	255.255.0(24) 🗸	
tłt	Flow Control	Static Routes	~	Remarks:		
۲	Access Controller	VLAN		Advanced Settings		
8=	Authentication	VPN Client	$\sim$	Advanced Settings		
÷	Behavior	UPNP	$\sim$	Working Mode:	Auto-Negotiation(Default)	
~7				NIC Speed:	Auto-Negotiation(Default)	
Ħ	Firewall	NAT		Mutual Access:	Allow Mutual LAN Access	
y	Advanced application	Port Mapping	$\sim$	Clone MAC:		
	Services	IPv6	$\sim$	Multiple IP:	Add	
Ъ	Log	IGMP Agent			IP Address Subnet Mask Actions	
					No Dete	
				Extended Network Card	weth1 veth2 veth3 v veth4	

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

CHORN	CMD-CO5-v1.01			තා රු 🗘 ළ English
	=<	Network <	Network > Interfaces	📮 CPU: 5.69% 🔛 MEM: 19% ↑ TX: 4.28 KB/s 🤳 RX: 59.62 KB/s
6	System	Interfaces	Interface Settings	
FW	Overview Monitoring	рнср 🗸		
_ چې	System Setup	DNS 🗸	WAN 1 WAN Connected 45	1 LAN Connected 1 DHCP Server Enabled 4 Device Connected
品	Network	IP/MAC Group 🗸 🗸		
ţţţ	Flow Control	Static Routes 🛛 🗸	Connection Connected	
<b></b>	Access Controller	VLAN	Status: IP: 192.168.0.1	
<u>&amp;=</u>	Authentication	VPN Client $\checkmark$	Subnet Mask: 255.255.255.0 MAC: 08:9b:4b:50:1c:bc	
₩	Behavior	UPNP 🗸	Remarks:	
Ħ	Firewall	NAT	Bind Device: veth1/Connected/1000Mbps/Full-Duplex Bind Device: veth2/Connected/100Mbps/Full-Duplex	
Ţ	Advanced application	Port Mapping 🗸 🗸	Bind Device: veth3/Connected/100Mbps/Full-Duplex	
0%	Services	IPv6 V	Bind Device: veth4/Not Connected/10Mbps/Unknown	
ß	Log	IGMP Agent	Lan1	http://102.169.0.1/#/network-ratting/fan.use.cet2tema-Jap.Bit

Fig 3.1.19 Interface setting of LAN1 interface page

## 2. DHCP

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

## **DHCP Server:**

A DHCP Server is a network server that automatically provides and assigns IP addresses,

default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

### Interface:

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

## Address Pool:

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

### Subnet Mask:

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

### Gateway

**Primary DNS** 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

	CMD-COS-v1.01										් ර	4 <u>2</u>	English
	=<	Network	Network > DHCP	> DHCP Server						🛱 CPU: 3.25%	🛄 MEM: 16% 1	TX: 0.00 B/s 🔱 I	RX: 0.00 B/s
			DHCP Server Se	ettings									
E	System Overview	Interfaces	Â										
₽⁄	Monitoring	DHCP ^	Server Status: Se	ervice Enabled Inter	face/Gateway C	۹	Res	tart DHCP Service	Add	Import Expor	t Enable	Disable	Delete
ţĊ	System Setup		Interface	Address Pool	Subnet Mask	Gateway	Primary DNS	Secondary DNS	Lease(minute)	Remaining address	Status	Actions	
놂	Network	DHCP Static	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	
tłt	Flow Control	DHCP Leases	Showing 1 of 1 r	ecords					PerPage	20 × Rows		>> 1 /1Page	Jump
<b>P</b>	Access Controller	Black White List										//	
8 <b>.</b>	Authentication	DNS 🗸											
\$↓	Behavior	IP/MAC V Group											
臣	Firewall	Static Routes 🛛 🗸											
Ī	Advanced application	VLAN											
0%	Services	VPN Client 🗸											
ጭ	Log												

Fig 3.2.1 Default DHCP Server Settings of LAN1 interface page

	CMD-COS-v1.01			ත් රු 👃 English
	Ξ<	Network <	Network > DHCP > DHCP Server	4월 CPU: 2.72% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
6	System Overview	Interfaces	Add	×
₩	Monitoring	DHCP ^	Interface : lan1	~
ţţ	System Setup	DHCP Server	Address Pool :	· · ·
볾	Network	DHCP Static	Subnet Mask: 255.255.255.0	~
†∔†	Flow Control	DHCP Leases	Gateway:	•
۲	Access Controller	Black White List	Primary DNS:	•
<u>&amp;"</u>	Authentication	DNS 🗸	Secondary DNS :	*
⇔	Behavior	IP/MAC v Group	Lease(minute): 120 minute *	
₿	Firewall	Static Routes 🗸 🗸	Check interface IP 🗹 Open validity:	
V	Advanced application	VLAN	Applies only to DHCP Open relay:	
	Services	VPN Client 🗸 🗸	user-defined DHCP option: V	
Δ	Log	UPNP 🗸	Save	
		NAT		
		Port Mapping $\smallsetminus$		

Fig 3.2.2 Add DHCP Server Settings of LAN1 interface page

	CMD-COS-v1.01			스) 슈 슈 온 English
	Ξ<	Network <	Network > DHCP > DHCP Server	≣ CPU: 0.50% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6)	System Overview	Interfaces	Edit	X
₩	Monitoring	рнср 🔷	Interface : Ian1	
ţĊ	System Setup	DHCP Server	Address Pool : 192.168.0.10 - 192.168.0.200 *	
츎	Network	DHCP Static	Subnet Mask: 255.255.255.0 V	
t+t	Flow Control	DHCP Leases	Gateway: 192.168.0.1 *	
<b>R</b>	Access Controller	Black White List	Primary DNS: 8.8.8.8 *	
<u>8</u> =	Authentication	DNS 🗸	Secondary DNS: 8.8.4.4 *	
⇒	Behavior	IP/MAC Group \vee	Lease(minute): 800 minute *	
Ħ	Firewall	Static Routes 🛛 🗸	Check interface IP 🛛 🗹 Open validity:	
Ţ	Advanced application	VLAN	Applies only to DHCP Open relay:	
0% 00	Services	VPN Client $\lor$	user-defined DHCP option: V	
ß	Log	UPNP V	Save	

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

	CMD-COS-v1.01		ධා 🗘 🗘 English	
	=<	Network <	Network > DHCP > DHCP Server	J/s
		<u>^</u>	DHCP Server Settings	
E	Overview	Interfaces		
₩	Monitoring	DHCP ^	Server Status: Service Enabled Interface/Gateway Q Restart DHCP Service Add Import Export Enable Disable Delete	
ţĊ	System Setup	DHCP Server	Interface Address Pool Subnet Mask Gateway Primary DNS Secondary Lease(minute) Remaining Status Actions 🗌 address	
品	Network	DHCP Static	lan1 192.168.0.10 255.255.255.0 192.168.0.1 8.8.8.8 8.8.4.4 800 187 Enabled Edit Disable Delete	
†∔†	Flow Control	DHCP Leases		
<b>R</b>	Access Controller	Black White List	Showing for records	
8= 	Authentication	DNS 🗸		
₩	Behavior	IP/MAC Group ${}^{\checkmark}$		
Ħ	Firewall	Static Routes 🛛 🗸		
Ţ	Advanced application	VLAN		
0% 00	Services	VPN Client 🗸 🗸		
Ъ	Log	UPNP V		

### 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.

CMD-COS	1.01							් ර ද ළ	Englis
=<	Network <	Network > DHCP > DHCP	Static				📫 CPU: 0.50% 🛛	MEM: 16% ↑ TX: 0.00 B/s	↓ RX: 0.00
System Overview	Interfaces	DHCP Static IP Mappin	g						
Monitoring	DHCP ^	Compatible ARP bindir	ng list is statically assigned	IP/MAC/Comment Q		Add	Import Export	Enable Disable	Delete
දිටුර් System Setu	DHCP Server	Hostname $\checkmark$	IP Address $\checkmark$	MAC Address $\checkmark$	Bind interface $\checkmark$	Remarks	Status	Actions	
品 Network	DHCP Static				No Data				
111 Flow Contro	DHCP Leases								
Access Controller	Black White List								
윤. Authenticat	on DNS 🗸								
∽ Behavior	IP/MAC Group								
Firewall	Static Routes 🗸 🗸								
Advanced application	VLAN								
Services	VPN Client 🗸								
Log	UPNP 🗸								

# Fig 3.2.5 Default DHCP Static IP Mapping page

	CMD-COS-v1.01								් ර 4 2	English
	=<	Network	Network > DHCP > DHCP S	Static				🛱 CPU: 0.50%	MEM: 16% ↑ TX: 0.00 B/s 👃	RX: 0.00 B/s
~	 System	Interfaces	DHCP Static IP Mapping	g						
6.3	Overview	interraces								
₩	Monitoring	DHCP ^	Compatible ARP bindin	g list is statically assigned		Q	Add	Import Export	Enable Disable	Delete
<i>ې</i> ې	System Setup	DHCP Server	Hostname $\vee$	IP Address $\checkmark$	MAC Address $\vee$	Bind interface $\lor$	Remarks	Status	Actions	
몲	Network	DHCP Static				auto	~	Editing	OK Cancel	
†4†	Flow Control	DHCP Leases	Showing 1 of 0 records							
۲	Access Controller	Black White List	showing for orecords							
& <b>.</b> "	Authentication	DNS 🗸								
⇔	Behavior	IP/MAC Group								
臣	Firewall	Static Routes $\sim$								
Ø	Advanced application	VLAN								
0%	Services	VPN Client 🗸								
Ъ	Log	UPNP V								

# Fig 3.2.6 Default DHCP Static IP Mapping Add page

	CMD-COS-y1 01							ථා	û 4 ≗	English
	=	Network	Network > DHCP > DH	CP Static			= <u>□</u> = CPU: (	0.00% 🛄 MEM: 20%	o ↑ TX: 27.00 B/s ↓	RX: 27.00 B/s
			DHCP Static IP Map	ping						
$\mathbb{C}$	System Overview	Interfaces								
₩	Monitoring	DHCP ^	Compatible ARP bi	nding list is statically ass	igned IP/MAC/Comm	ent Q	Add Import	Export Ena	ble Disable	Delete
ţĈ	System Setup	DHCP Server	Hostname ∨	IP Address $\checkmark$	MAC Address $\checkmark$	Bind interface $\checkmark$	Remarks	Status	Actions	
品	Network	DHCP Static	DESKTOP-70API5S	192.168.0.100	c4:d9:87:a7:ad:46	lan1	Static%20Binding	Enabled	Edit Disable Dele	te 🗌
tit	Flow Control	DHCP Leases	Showing 1 of 1 record	s			PerPage 20 ∨	Rows 《 〈	Ⅰ > ≫ 1 /1Pa	ges Jump
<b>P</b>	Access Controller	Black White List								
<u>&amp;=</u>	Authentication	DNS 🗸								
₩	Behavior	IP/MAC Group \vee								
Ħ	Firewall	Static Routes 🛛 🗸								
,	Advanced application	VLAN								
04	Services	VPN Client 🗸								
ß	Log	UPNP V								

## 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

	CMD-COS-v1.01								්	☆ ↓ 2	C English
	=<	Network <	Network > DHCP > DH	CP Leases				<	CPU: 0.25% 🛄 MEM: 1	6% ↑ TX: 0.00 B/s	↓ RX: 0.00 B/s
			Viewing DHCP Lease	es							
6	Overview	Interfaces									
<u>-</u>	Monitoring	DHCP ^	All interface	<ul> <li>✓ All Stat</li> </ul>	tus 🗸 Fu	II MAC Address Q		Static	MAC Blacklist	One key returns th	ie IP address
ţĊţ	System Setup	DHCP Server	Hostname	IP Address $\vee$	MAC Address	Timeout $\vee$	Bind interface $\vee$	status $\vee$	Comment	Actions	
윪	Network	DHCP Static					No Data				
†#†	Flow Control	DHCP Leases									
P	Access Controller	Black White List									
<u>₽</u> "	Authentication	DNS $\sim$									
₩	Behavior	IP/MAC Group									
臣	Firewall	Static Routes $$									
Ţ	Advanced application	VLAN									
0% 00	Services	VPN Client 🗸 🗸									
Ъ	Log										

Fig 3.2.8 Default Viewing DHCP Leases page

	CMD-COS-v1.01								û	¢ 2	English
	=<	Network <	Network > DHCP >	DHCP Leases				≣ЩE CPU: 7.67%	🛄 MEM: 20% ↑ 1	'X: 95.00 B/s ↓ RX:	: 67.00 B/s
	_		Viewing DHCP Le	ases							
$\mathfrak{S}$	System Overview	Interfaces									
₩	Monitoring	рнср 🔷	All interface $\checkmark$	All Status	← Full MAC Addre	ess Q		Static MAC	Blacklist One	key returns the IP ad	ldress
ţĊţ	System Setup	DHCP Server	Hostname	IP Address $\checkmark$	MAC Address	Timeout $\checkmark$	Bind interface $\checkmark$	status ∨	Comment	Actions	
品	Network	DHCP Static	DESKTOP-70API5S	192.168.0.12	c4:d9:87:a7:ad:46	03:05:03	lan1	Dynamic allocation	Static%20Binding	Static MAC Blacklist	
ţţţ	Flow Control	DHCP Leases	АР	192.168.0.13	08:9b:4b:9e:f4:e3	03:03:45	lan1	Dynamic allocation		Static MAC Blacklist	
<b></b>	Access Controller	Black White List	AP	192.168.0.10	08:9b:4b:99:a3:94	03:02:07	lan1	Dynamic allocation	AP	Static MAC Blacklist	
<u>8</u> =	Authentication	DNS 🗸						Dynamic		Static	
<b>↓</b>	Behavior	IP/MAC Group ${}^{\checkmark}$	POCOF1-POCOF1	192.168.0.11	20:a6:0c:37:4d:13	02:59:40	lan1	allocation		MAC Blacklist	
Ħ	Firewall	Static Routes 🛛 🗸	Showing 1-4 of 4 re	ecords			PerPage	20 $\checkmark$ Rows	« < <b>1</b> >	≫ 1 /1Pages	Jump
,	Advanced application	VLAN									
0%	Services	VPN Client $\vee$									
ľð	Log	UPNP V									

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

	CMD-COS-v1.01											۵	<u></u>		English
	=,	Network <	Network > DHCP > B	lack White List						😳 CP	U: 21.50%	MEM: 16%	↑ TX: 0.0	0 B/s 🔱	RX: 0.00 B/s
	System		Black White List												
6-3	Overview	Interfaces													
₩	Monitoring	DHCP ^	Select Mode												
ţ	System Setup	DHCP Server		Blacklist Mode (B	lacklist all macs are fo	rbidden to assign IP a	addresses)								
윪	Network	DHCP Static		Whitelist Mode (     Synchronize MAG	All MACs except white	list prohibit IP addres	ss assignmer		d with boboui						
tŧł	Flow Control	DHCP Leases		- Synchronize WAC	access control (DITC)	- black and write list					ic access com				
P	Access Controller	Black White List	Blacklist												
<u>₽</u> "	Authentication	DNS 🗸	Search	Q				addAll	Add	Import	Export	Enable	Disa	ble	Delete
\$.	Behavior	IP/MAC Group	MAC Address ~	Remarks		Status				Actio	ns				
Ħ	Firewall	Static Routes 🗸 🗸					No Data	а							
V	Advanced application	VLAN													
0%	Services	VPN Client 🗸													
٦Ŋ.	Log														



	CMD-COS-v1.01				
		Network <	Network > DHCP > Black W	hite List	🛱 CPU: 0.00% 🛄 MEM: 20% ↑ TX: 39.00 B/s 🤳 RX: 33.00 B/s
6	System		Black White List		
C*3		interlaces			
₩			Select Mode		
ţŷ				<ul> <li>Blacklist Mode (Blacklist all macs are forbidden to assign IP address</li> </ul>	ses)
品				Tips	nent)
ţţţ				Switch to blacklist mode, the MAC is not allowed to get	are synchronized with behavior control-mac access control)
<b></b>	Access Controller	Black White List	Whitelist	addresses in blacklist lists, are you sure you want to switch to blacklist mode?	Innet Frent Field, Dickle Delde
8= 	Authentication		search Q		
$\overleftrightarrow$	Behavior		MAC Address ∨ Rem	OK Cancel	Actions
Ħ					
Ţ	Advanced application	VLAN			
00		VPN Client $\vee$			
ľ		UPNP 🗸			
		NAT			

Fig 3.2.11 Blacklist Mode setting in device page

CENTRE	CMD-COS-v1.01					ے ڈ	4 4	English
		Network <	Network > DHCP > Black W	hite List	ः 🛄 ECPU: 4.95% 🖳	MEM: 20% 个	TX: 27.00 B/s 🔱	RX: 33.00 B/s
			Black White List					
A	System Overview	Interfaces						
<u>-</u>			Select Mode					
ţĊŗ				Blacklist Mode (Blacklist all macs are forbidden to assign IP addresser				
品				Tips	nent)			
ţţţ				Switch to whitelist mode. Only MAC in the whitelist list	are synchronized with behavio			
<b></b>	Access Controller		Blacklist	is allowed to get addresses,are you sure you want to switch to whitelist mode?				
&= 			Search Q		Import Export	Enable	Disable	Delete
⇔	Behavior		MAC Address 🗸 🦷 Rem	CK Canter	Actions			
Ħ				No Data				
Ţ	Advanced application	VLAN						
0%								
ľð	Log	UPNP 🗸						

Fig 3.2.12 Changing mode to Whitelist Mode setting in device page

	CMD-COS-v1.01						<u>උ</u> ර	}	C English
	=,	Network <	Network > DHCP > BI	ack White List		📲 CPU: 0.25% 🔛 I	MEM: 20%	↑ TX: 0.00 B/s	↓ RX: 0.00 B/s
	_		Black White List						
6	Overview	Interfaces							
₽	Monitoring	DHCP ^	Select Mode						
ţÇ	System Setup	DHCP Server		Blacklist Mode (Blacklist all macs are f	orbidden to assign IP addresses)				
品	Network	DHCP Static		Whitelist Mode (All MACs except whit	elist prohibit IP address assignmen	t)			
t††	Flow Control	DHCP Leases		<ul> <li>Synchronize MAC access control (DHC</li> </ul>	CP black and white list Settings are	synchronized with behavior co	ontrol-mac ac	cess control)	
<b>(</b>	Access Controller	Black White List	Whitelist						
<u>&amp;</u> =	Authentication	DNS 🗸	Search	Q	addAll Add	Import Export	Enable	Disable	Delete
\$↓	Behavior	IP/MAC Group \vee	MAC Address $\checkmark$	Remarks	Status	Actions			
⊞	Firewall	Static Routes 🛛 🗸			No Data				
Ţ	Advanced application	VLAN							
0% 00	Services	VPN Client 🗸							
ſ	Log	UPNP V							

# Fig 3.2.13 White list Mode setting in device page

	CMD-COS-v1.01						් ර ද ,	O English
	=<	Network <	Network > DHCP > Black	White List		📫 CPU: 2.75% 🛄 ME	.M: 16% ↑ TX: 0.00 B/s	↓ RX: 0.00 B/s
	- ·		Black White List					
6	Overview	Interfaces						
<u>-</u>	Monitoring	DHCP ^	Select Mode					
ţĊ	System Setup	DHCP Server		Blacklist Mode (Blacklist all macs are forbidd	en to assign IP addresses)			
윪	Network	DHCP Static		Whitelist Mode (All MACs except whitelist pr	ohibit IP address assignment			
†∔†	Flow Control	DHCP Leases		Synchronize MAC access control (DHCP blac	c and white list Settings are s	ynchronized with behavior control-mac access control)		
٩	Access Controller	Black White List	Blacklist				Fachla Dischla	Delete
8 <u>.</u>	Authentication	DNS 🗸	search (				Enable	Delete
Ś	Behavior		MAC Address ~ R	temarks	Status	Actions		
, í		Group			Editing	OK Cancel		
E	Firewall	Static Routes 🗸						
V	Advanced application	VLAN	Showing 1 of 0 records					
0%	Services	VPN Client 🗸						
P	Log							

Fig 3.2.14 Blacklist mode add page

	CMD-COS-v1.01						D & & A	A English
	=,	Network <	Network > DHCP > Bl	ack White List		📲 CPU: 0.00% 🔛 MEM	1: 19% ↑ TX: 0.00 B/	s \downarrow RX: 0.00 B/s
		^	Black White List					
6)	Overview	Interfaces						
₽4	Monitoring	DHCP ^	Select Mode					
ţŷ;	System Setup	DHCP Server		Blacklist Mode (Blacklist all n	nacs are forbidden to assign IP addresses			
品	Network	DHCP Static		Whitelist Mode (All MACs ex	cept whitelist prohibit IP address assignm	ient)		
555				Synchronize MAC access cor	trol (DHCP black and white list Settings a	re synchronized with behavior contro	ol-mac access control)	
T+T	Flow Control	DHCP Leases	Placklist					
<b></b>	Access Controller	Black White List	Diacklist					
<u>&amp;</u> "	Authentication	DNS 🗸	Search	Q	addAll Add	Import Export E	inable Disable	Delete
$\leftarrow$	Behavior		MAC Address $\checkmark$	Remarks	Status	Actions		
	benavior	in yinine croup	08:9b:4b:99:a3:94	AP%20blacklisted	Enabled	Edit Disable De	elete	
E	Firewall	Static Routes 🛛 🗸					_	
Ţ	Advanced application	VLAN	Showing 1 of 1 recor	ds	Per	Page 20 🗸 Rows < <	1 > > 1	/1Pages Jump
0% 00	Services	VPN Client $\vee$						
ቡ	Log	UPNP V						

## 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

	CMD-COS-v1.01						් ර	} 수 온 English
	=<	Network <	Network > DNS > DNS				🛱 CPU: 4.75% 🔛 MEM: 16%	↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
-	Sustem		DNS Settings					
63	Overview	Interfaces						
~~	Monitoring	DHCP $\lor$						
ŝ	System Setup	DNS ^	Preferred DNS :	8.8.8.8		*		
모	Network	DNS	Alternative DNS:	8.8.4.4		*		
000	nothork	BNS	DNS Acceleration	Open				
†‡†	Flow Control	Multiline DNS	Service:					
۹	Access Controller	IP/MAC Group 🗸 🗸		Save				
ê	Authentication	Static Routes 🛛 🗸						
₩	Behavior	VLAN	DNS Reverse Proxy					
臣	Firewall	VPN Client 🗸 🗸	Find DNS Q			Add	Import Export Enable	Disable Delete
Ţ	Advanced application	UPNP 🗸 🗸	Domain Name IP A	ddress I	Remarks	Status	Actions	
0% 00	Services	NAT			No	Data		
Ъ	Log	Port Mapping 🗸 🗸						

Fig 3.3.1 Default DNS Settings page

	CMD-CO5-v1.01		ත් රු 🗘 ළ Eng	ish
	=<	Network <	Network > DNS > DNS 🔤 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.	)0 B,
	 System		DNS Settings	
6-3	Overview	Interfaces		
<u>-</u>	Monitoring	DHCP V		
ţ	System Setup	DNS ^	Preferred DNS : 8.8.8.8 *	
品	Network	DNS	Alternative DNS: 8.8.4.4	
+14	Flow Control	Multiline DNS	DNS Acceleration 🗹 Open Service:	
	Access		DNS Acceleration Mode: Proxy Mode(UDP)	
2	Controller	IP/MAC Group V	Force Client DNS Proxy: 🗌 Open	
ê.	Authentication	Static Routes $\sim$		
₩	Behavior	VLAN	Save	
臣	Firewall	VPN Client $\sim$		
V	Advanced application	UPNP 🗸	DNS Reverse Proxy	
0% 00	Services	NAT	Find DNS     Q       Add     Import       Export     Enable       Disable     Delete	
Ъ	Log	Port Mapping 🛛 🗸	Domain Name IP Address Remarks Status Actions	
		IPv6 ~	Editing OK Cancel	
		IGMP Agent	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.

	CMD-COS-v1.01					ථ	습 수 은 English
	_<	Network <	Network > DNS > DNS			티슈 CPU: 12.87% 🛄 MEM: 199	6 ↑ TX: 27.00 B/s 🤳 RX: 27.00
Ð	System Overview	∧ Interfaces	DNS Settings				
<u>-</u>	Monitoring	рнср 🗸					
ţĊţ	System Setup	DNS ^	Preferred DNS :	8.8.8.8	*		
뷺	Network	DNS	Alternative DNS:	114.114.114.114	*		
†∔†	Flow Control	Multiline DNS	DNS Acceleration Service :	✓ Open Prove Made(UDD)			
<b>@</b>	Access Controller	IP/MAC Group \vee	Force Client DNS Proxy:	Proxy Mode(UDP) Proxy Mode(UDP)	~		
<u>&amp;=</u>	Authentication	Static Routes 🛛 🗸		Proxy Mode(DoH: DNS over Https) Cache Mode			
$\stackrel{\checkmark}{\Rightarrow}$	Behavior	VLAN		ThirdAgent			
Ħ	Firewall	VPN Client $$					
Ţ	Advanced application	UPNP 🗸	DNS Reverse Proxy				
0%	Services	NAT	Find DNS Q		Add	mport Export Enable	e Disable Delete
ß	Log	Port Mapping $\checkmark$	Domain Name IP Ada	dress Remarks	Statu	s Action	ns 🗌
		IPv6 V					

#### ..... 🛆 🟠 🗘 English Network > DNS > DNS CPU: 1.00% MEM: 18% TX: 3.62 KB/s Network System Interfaces Preferred DNS : 8.8.8.8 Monitoring DHCP 114.114.114.114 Alternative DNS: £ System Setup Open DNS Acceleration 몲 DNS Acceleration Mode: Cache Mode 14 Flow Control Multiline DNS Access Controller IP/MAC Group thentication Static Route: DNS Cache Status Behavior VLAN Clear Cache Firewall VPN Client Cache Mi Advanced application UPNP 0 0 0 0% Yesterday 0 ms Today 37 2.63% 320 ms 38 Services Total 37 2.63% 320 ms Port Mapping

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

Fig 3.3.4 DNS cache status page

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

	CMD-COS-v1.01							스> 슈 슈 온 English		
	≡<	Network <	Network > DNS >	DNS			∎ <mark>0</mark> ≣ CPU: 34.25	5% 🛄 MEM: 18% ↑ TX: 0.00 B/s ↓ RX: 683.00 B/		
Ð	System Overview	Interfaces			Save					
₩	Monitoring	DHCP $\vee$	DNS Cache Status							
ŝ	System Setup	DNS ^	Clear Cache							
놂	Network	DNS		Request D	NS Cache Hits	Cache Missed	Hit Ratio	Time Saved		
ttt	Flow Control	Multiline DNS	Yesterday	0	0	0	0%	0 ms		
<b>P</b>	Access	IP/MAC Group 🗸 🗸	Today	38	1	37	2.63%	320 ms		
8"	Authentication	Static Routes 🗸 🗸 🗸	Total	38	1	37	2.63%	320 ms		
	Behavior	VLAN	DNS Reverse Proxy							
E	Firewall	VPN Client $$	Find DNS	Q			Add Import Exp	oort Enable Disable Delete		
V	Advanced	UPNP V	Domain Name		IP Address	Remarks	Status	Actions		
0%	Services	NAT	commandonetwo	rks.com	114.114.223.223	Rverse <sup>9</sup> 620proxy	Enabled	Edit Disable Delete		
Ъ	Log	Port Mapping 🛛 🗸	Showing 1 of 1 re	cords			PerPage 20 $\checkmark$ Rows	$\ll$ $\langle$ 1 $\rangle$ $\gg$ 1 /1Pages Jump		
		IPv6 🗸								
		IGMP Agent	Caution: DN DN DN	S proxy mod S enforceme S cache mod	e: valid when the client DNS is the ramp add nt proxy: does not verify the client DNS addr e: local DNS cache acceleration service	ress; ess, forcing the client to use the DNS pro	client to use the DNS proxy 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



Fig 3.3.6 Default Multiline DNS Settings page

	CMD-COS-v1.01							△ ↔ ♣ ≗	English
	=<	Network <	Network > DNS > Multiline DN	15			📫 CPU: 3.47% 🔛 M	1EM: 19% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	System		Multiline DNS Settings						
6-3	Overview	Interfaces							
₩	Monitoring	DHCP 🗸 🗸	Find DNS Q			Add	Import Export	Enable Disable	Delete
ţ	System Setup	DNS ^	Interface	Primary DNS	Secondary DNS	Remarks	Status	Actions	
뮮	Network	DNS	wan4 ~	/ 115.254.1.1	202.86.251.1	DNS-Direct	Editing	OK Cancel	
tit	Flow Control	Multiline DNS	wan1	8.8.8.8	8.8.4.4	DNS-1	Enabled	Edit Disable Delete	
•	Access Controller	IP/MAC Group 🗸 🗸	wan2	114.114.114.114	1.1.1.1	DNS-2	Enabled	Edit Disable Delete	
<u>&amp;</u> "	Authentication	Static Routes $\sim$	wan3	9.9.9.9	149.112.112.112	DNS-3	Enabled	Edit Disable Delete	
\$ ¢	Behavior	VLAN	Showing 1-3 of 3 records			Per	Page 20 $\sim$ Rows $\ll$	< 1 > » 1 /1Pa	ges Jump
臣	Firewall	VPN Client $\sim$							
y	Advanced application	UPNP 🗸	Help: DNS Proxy Mo acceleration.	de: effective when client set the g	ateway address as DNS; Forced D	NS Proxy: force the client to use	he DNS Proxy service; DNS Cache	e Mode: use local DNS cache fo	r
0% 00	Services	NAT							
Ъ	Log	Port Mapping $\sim$							
		IPv6 ~							
		IGMP Agent							

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

	CMD-COS-v1.01		ත් රු 🗘 උ ළාglish
	=,	Network <	Network > IP/MAC Group > IP Group CPU: 0.25% 📮 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
0	 System	Interforme	Manage IP Address Group
6.3	Overview	interfaces	
~~	Monitoring	DHCP $\lor$	Group Name Q Add Import Export Delete
ŝ	System Setup	DNS 🗸	Group Name V IP List Actions
몲	Network	IP/MAC Group	No Data
†4†	Flow Control		
<b>P</b>	Access Controller	MAC Group	
<u>&amp;</u> "	Authentication	Static Routes $\sim$	
₩	Behavior	VLAN	
臣	Firewall	VPN Client $\vee$	
Ţ	Advanced application	UPNP 🗸	
	Services	NAT	
Ъ	Log	Port Mapping $\vee$	

## 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.

	CMD-COS-v1.01				🛆 🏠 🐥 😤 English
	=,	Network (	Network > IP/MAC Group > IP Group		🛱 CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
			Add		×
Ð	System Overview	Interfaces			
<u>-</u>	Monitoring	DHCP 🗸 🗸			
ŝ	System Setup	DNS 🗸	Group Name:	*	
묘	Network	IP/MAC Group	IP List:	*	
000					
†‡†	Flow Control	IP Group			
P	Access Controller	MAC Group		Support a single IP address or IP segment, and each data is switched to a diff 192.168.1.1	ierent format:
<u>₽</u> ,	Authentication	Static Routes 🛛 🗸		192.168.1.1 Remarks1 192.168.1.0/24 Remarks2 192.168.1.1-192.168.1.111 Remarks3	
₩	Behavior	VLAN			
臣	Firewall	VPN Client 🗸 🗸		Save Cancel	
Ī	Advanced application	UPNP V			
0%	Services	NAT			
Ъ	Log	Port Mapping 🗸 🗸			

Fig 3.4.2 Default Add IP Address Group page

	CMD-COS-v1.01				스) 슈 오 English
	Ξ<	Network <	Network > IP/MAC Group > IP Group		🛱 CPU: 2.25% 🛄 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
Ð	System	Interfaces	Edit		×
₩	Monitoring	рнср 🗸			
ţÇ	System Setup	DNS 🗸	Group Name:	COMMANDO	
品	Network	IP/MAC Group 🔿	IP List:	192.168.0.0/24	
†ŧ†	Flow Control	IP Group			
۴	Access Controller	MAC Group		Support a single IP address or IP segment, and each data i 192.168.1.1	J switched to a different format:
<u>&amp;</u> =	Authentication	Static Routes 🛛 🗸		192.168.1.1 Kemarks1 192.168.1.0/24 Remarks2 192.168.1.1-192.168.1.111 Remarks3	
\$	Behavior	VLAN			
Ħ	Firewall	VPN Client 🗸 🗸		Save Cancel	
Ţ	Advanced application	UPNP 🗸			
0% 00	Services	NAT			
ŀ	Log	Port Mapping 🗸			

### Fig 3.4.3 Edit IP Address Group page

	CMD-COS-v1.01				스 슈 A A	English
	=<	Network <	Network > IP/MAC Group > IP Group		ः🛱 CPU: 1.73% 🛄 MEM: 18% ↑ TX: 3.65 KB/s 🤳 R	X: 6.01 KB/s
-		^	Manage IP Address Group			
63	Overview	Interfaces				
₩	Monitoring	рнср 🗸	Group Name Q		Add Import Export	Delete
ţĊ	System Setup	DNS 🗸	Group Name ∽	IP List	Actions	
品	Network	IP/MAC Group 🔿	COMMANDO	192.168.0.0/24	Edit Delete	
†∔†	Flow Control	IP Group	Showing 1 of 1 records		PerPage 20 ~ Rows 《 < 1 > 》 1 /1Page	es Jump
<b>®</b>	Access Controller	MAC Group				
<u>&amp;=</u>	Authentication	Static Routes 🛛 🗸				
₩	Behavior	VLAN				
臣	Firewall	VPN Client $$				
Ţ	Advanced application	UPNP 🗸				
0% 00	Services	NAT				
ſð	Log	Port Mapping $$				

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

	CMD-COS-v1.01				ත් රු 👃 English
	=,	Network <	Network > IP/MAC Group > MAC Group		n CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
0	System	Interfaces	Add		×
₩	Monitoring	DHCP V			
ţ	System Setup	DNS ~	Group Name:		*
볾	Network	IP/MAC Group	Mac List:		*
tłt	Flow Control	IP Group			
۲	Access Controller	MAC Group		Please fill in the MAC and make a distinction between the di 58:FB:84:38:74:BF	data changes format:
<u>8</u> .	Authentication	Static Routes $\sim$		JULDUM JULMUT RETRAINS	
₩	Behavior	VLAN		Save Cancel	
臣	Firewall	VPN Client $\sim$			
Ţ	Advanced application	UPNP 🗸			
00	Services	NAT			
ľ	Log	Port Mapping 🗸 🗸			

Fig 3.4.6 Add MAC Address Group page

	CMD-COS-v1.01				۵	습 수 은 English
	≡<	Network <	Network > IP/MAC Group > MAC Group		≡ CPU: 0.25% 🛄 MEM: 18%	↑ TX: 67.00 B/s ↓ RX: 67.00 B/s
Ð	System Overview	Interfaces	Add			×
₩	Monitoring	DHCP 🗸				
ţĊŗ	System Setup	DNS 🗸	Group Name:	COMMANDOMAC	*	
品	Network	IP/MAC Group \land	Mac List:	20:a6:0c:37:4d:13	*	
†∔†	Flow Control	IP Group				
<b>P</b>	Access Controller	MAC Group		Please fill in the MAC and make a distinction between the 58:FB:84:3B:74:BF	] data changes format:	
<u>&amp;</u> =	Authentication	Static Routes 🗸 🗸		58:FB:84:38:74:8F Remarks		
⇆	Behavior	VLAN		Save		
臣	Firewall	VPN Client $$				
Ţ	Advanced application	UPNP ~				
0% 00	Services	NAT				
ſð	Log	Port Mapping $\vee$				

Fig 3.4.6 Adding specific MAC page

	CMD-COS-v1.01				스) 습 수 온 Fr	ıglish
	=,	Network <	Network > IP/MAC Group > MAC Group		🛱 CPU: 0.00% 🛄 MEM: 18% ↑ TX: 0.00 B/s ↓ RX:	0.00 B/s
-		^	Manage MAC Address Group			
6)	Overview	Interfaces				
₩	Monitoring	DHCP 🗸 🗸	Group Name Q		Add Import Export Del	ete
ţĊĵ	System Setup	DNS 🗸	Group Name ∨	Mac List	Actions	
몲	Network	IP/MAC Group 🔿	COMMANDOMAC	20:a6:0c:37:4d:13	Edit Delete	
ţţţ	Flow Control	IP Group	Showing 1 of 1 records		PerPage 20 $\checkmark$ Rows $\ll$ $\langle$ 1 $\rangle$ $\gg$ 1 /1Pages	Jump
۲	Access Controller	MAC Group				
<u>&amp;=</u>	Authentication	Static Routes 🗸 🗸				
₩	Behavior	VLAN				
臣	Firewall	VPN Client $$				
Ţ	Advanced application	UPNP V				
0% 00	Services	NAT				
ľð	Log	Port Mapping $$				

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.

	CMD-COS-v1.01									⊿ ☆ 수 ዶ	English
	=<	Network <	Network > Static Ro	outes > Static Routes					📫 CPU: 0.00% 🛛 🛄 M	EM: 16% ↑ TX: 0.00 B/s	RX: 0.00 B/s
~	System		Static Routes								
6-3	Overview	Interfaces									
₩	Monitoring	DHCP 🗸 🗸						Add In	nport Export	Enable Disable	Delete
ţĊ	System Setup	DNS 🗸	Interface $\lor$	Dst.Addr $\vee$	Subnet Mask	Gateway 🗸	Metric	Remarks	Status	Actions	
뮮	Network	IP/MAC Group 🗸 🗸					No Data				
†∔†	Flow Control	Static Routes 🛛 🔿									
	Access Controller	Static Routes									
<u>&amp;</u> =	Authentication	Routing Tables									
\$	Behavior	VLAN									
臣	Firewall	VPN Client $\checkmark$									
I	Advanced application	UPNP V									
	Services	NAT									
Ъ	Log	Port Mapping 🗸 🗸									

# Fig 3.5.1 Default static route page

	CMD-COS-v1.01				් 🗘 🗘 உ English
	≡<	Network <	Network > Static Routes > Static Routes		. CPU: 0.25%
~	System		Add		×
6-3	Overview	Interfaces			
₩	Monitoring	DHCP 🗸 🗸			
ŝ	System Setup	DNS $\sim$	Interface:	Auto	
品	Network	IP/MAC Group	Dst.Addr:		*
			Subnet Mask:	255.255.255.0 (24) 🗸	
T+1	Flow Control	Static Routes A	Gateway:		
•	Access Controller	Static Routes	Metric:	1	*
<u>&amp;</u> "	Authentication	Routing Tables		The smaller the number, the higher the priority.	
¢ ≯	Behavior	VLAN	Remarks:		
Ē	Firewall	VPN Client 🗸			
	Advanced			Save Cancel	
Ţ	application	UPNP V			
0%	Services	NAT			
Ъ	Log	Port Mapping 🗸 🗸			

# Fig 3.5.2 Default Add static route page

	CMD-COS-v1.01				් 🖒 🛆 Lenglish
	=,	Network	Network > Static Routes > Static Routes		📫 CPU: 0.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s 👃 RX: 0.00 B/s
			Add		×
6)	System Overview	Interfaces			
<u>-</u>	Monitoring	DHCP 🗸 🗸			
ŝ	System Setup	DNS 🗸	Interface:	Auto $\checkmark$	
			Dst.Addr:	Auto lan1	*
ക്	Network	IP/MAC Group V	Subnet Mask:	lan2(COMMANDO LAN-2)	
†‡†	Flow Control	Static Routes		wan1	
<b>(</b>	Access	Static Routes	Gateway:	wan2	
	Controller		Metric:	1	*
<u>₿</u> ",	Authentication	Routing Tables		The smaller the number, the higher the priority.	
₩	Behavior	VLAN	Remarks:		
臣	Firewall	VPN Client $\checkmark$		Save Cancel	
Ţ	Advanced application	UPNP 🗸			
0% 00	Services	NAT			
Ъ	Log	Port Mapping 🗸 🗸			

## Fig 3.5.3 Selecting interface in static route page

	CMD-COS-v1.01	l.			් 🗘 🗘 English
	≡<	Network	Network > Static Routes > Static Routes		्रिः CPU: 27.06% 🛄 MEM: 17% ↑ TX: 42.84 KB/s ↓ RX: 157.68 KB/s
A	System Overview	Interfaces	Edit		×
₩	Monitoring	DHCP 🗸			
ţĊţ	System Setup	DNS 🗸	Interface :	wan1 V	
뷺	Network	IP/MAC Group 🗸 🗸	Dst.Addr:	0.0.0.0	*
ţ†	Flow Control	Static Routes 🔷	Subnet Mask:	0.0.0.0(0) ~	
<u></u>	Access	Static Routes	Gateway:	192.168.20.1	
<u>ه</u> =	Authentication	Routing Tables	Metric:	2 The smaller the number, the higher the priority.	-
<u> </u>	Behavior	VLAN	Remarks:	Airtel LAN	
	Firewall	VPN Client V			
	Advanced			Save Cancel	
	application				
őő	Services	NAT			
لگ	Log	Port Mapping $\checkmark$			

## 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.

	د الله در الله من الله الله الله الله الله الله الله الل								English		
	=<	Network <	Network > Stati	Routes > Static Route	25			∎ <b>□</b> = CPU: 1.75%	🛄 MEM: 17% ↑	TX: 5.70 KB/s 🤳 R)	X: 9.13 KB/s
	_		Static Routes								
( )	System Overview	Interfaces									
₩	Monitoring	DHCP 🗸 🗸					Add	Import Exp	oort Enable	Disable	Delete
ţĊţ	System Setup	DNS 🗸	Interface $\checkmark$	Dst.Addr $\checkmark$	Subnet Mask	Gateway ∨	Metric	Remarks	Status	Actions	
矗	Network	IP/MAC Group 🛛 🗸	wan1	0.0.0.0	0.0.0.0	192.168.20.1	2	Airtel LAN	Enabled	Edit Copy Disable Delete	
ţţţ	Flow Control	Static Routes 🔷	Showing 1 of 1	records			PerPa	ge 20 $\checkmark$ Rows	« < <mark>1</mark> >	≫ 1 /1Page	Jump
<b>R</b>	Access Controller	Static Routes									
8= ;	Authentication	Routing Tables									
$\downarrow$	Behavior	VLAN									
臣	Firewall	VPN Client $\vee$									
<b>I</b>	Advanced application	UPNP 🗸									
0%	Services	NAT	I								
ľð	Log	Port Mapping 🗸									

Fig 3.5.5 Default route page

	CMD-COS-v1.01				්	☆ ↓	A English
	Ξ·	Network <	Network > Static Routes > Static Routes		≡ <b>□</b> = CPU: 0.50% □ MEM: 17%	↑ TX: 1.25 KB/s	↓ RX: 809.00 B/s
Ð	System Overview	Interfaces	Add				×
₽2	Monitoring	рнср 🗸					
ţĊ}	System Setup	DNS 🗸	Interface:	Auto			
÷	Network	IP/MAC Group 🛛 🗸	Dst.Addr:	10.0.0.0 *	*		
(†∔†	Flow Control	Static Routes 🔿	Subnet Mask:	255.0.0 (8) ~			
	Access	Static Routes	Gateway:	172.10.1.1			
<u>&amp;=</u>	Authentication	Routing Tables	Metric:	5 The smaller the number, the higher the priority.	*		
¢‡	Behavior	VLAN	Remarks:	COMMANDORoute			
Ħ	Firewall	VPN Client 🗸 🗸		Save Cancel			
Ţ	Advanced application	UPNP 🗸					
0%	Services	NAT					
ľð	Log	Port Mapping 🗸 🗸					

### Fig 3.5.6 Adding a Specific Static route page

	CMD-COS-v1.01								් ර	) <b>4</b> 2	English
	=,	Network <	Network > Static	Routes > Static Route	'S			∎ CPU: 5.94%	🗋 МЕМ: 17% ↑ ТХ	(: 14.43 KB/s 🔱 RX: 3	21.58 KB/s
~	Surtem		Static Routes								
6-3	Overview	Interfaces									
₩	Monitoring	рнср 🗸					Add	Import Exp	oort Enable	Disable	Delete
ţĊţ	System Setup	DNS 🗸	Interface $\checkmark$	Dst.Addr $\checkmark$	Subnet Mask	Gateway 🗸	Metric	Remarks	Status	Actions	
矗	Network	IP/MAC Group 🛛 🗸	Auto	0.0.0.0	0.0.0.0	192.168.20.1	10	Airtel LAN	Enabled	Edit Copy Disable Delete	
†∔†	Flow Control	Static Routes 🔷	Auto	10.0.0.0	255.0.0.0 (8)	172.10.1.1	5	COMMANDORo e	ut Enabled	Edit Copy Disable Delete	
<b></b>	Access Controller	Static Routes	Showing 1-2 of	2 records			PerPa	age 20 V Rows	《 < 1 >	≫ 1 /1Pages	Jump
<u>&amp;</u> =	Authentication	Routing Tables									
₩	Behavior	VLAN									
Ħ	Firewall	VPN Client $\checkmark$									
Ţ	Advanced application	upnp v									
0%	Services	NAT									
ľð	Log	Port Mapping 🗸 🗸									

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

	CMD-COS-v1.01						් 🗘 🗘 🖄 English
	=<	Network <	Network > Static Routes > Routing Tak	les		📮 CPU: 8.50%	MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
	-		Viewing Routing Tables				
6	Overview	Interfaces					
<u>-</u>	Monitoring	DHCP 🗸 🗸	Interface	Dst.Addr	Subnet Mask	Gateway	Metric
łĜ;	System Setup	DNS 🗸	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
ക്	Network	IP/MAC Group V					
tit	Flow Control	Static Routes 🛛 🔿	Showing 1-2 of 2 records			PerPage 20 $\checkmark$ Rows $\ll$	< 1 > >> 1 /1Pages Jump
•	Access Controller	Static Routes					
<u>8</u> .	Authentication	Routing Tables					
₩	Behavior	VLAN					
臣	Firewall	VPN Client $\sim$					
Ţ	Advanced application	UPNP 🗸					
0%	Services	NAT					
Ъ	Log	Port Mapping $\sim$					

## 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

	🛎 CMD-COS-VL01								
	≡<	Network <	Network > VLAN 🔤 CPU: 15.25%  ☐ MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s						
Ð	System Overview	Interfaces	VLAN Settings						
₩	Monitoring	рнср 🗸	VlaniD/VLAN Name/IP Q Add Import Export Enable Disable Delete						
ŝ	System Setup	DNS ~	VLAN ID VLAN Name V MAC Address IP Address V Subnet Mask Interface Remarks Status Actions 🗌						
윪	Network	IP/MAC Group 🗸 🗸							
†∔†	Flow Control	Static Routes 🛛 🗸	No Data						
۲	Access Controller	VLAN							
<b>₽</b> ,	Authentication	VPN Client $\sim$	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						
₩	Behavior								
臣	Firewall	NAT							
V	Advanced application	Port Mapping 🗸 🗸							
0% 00	Services	IPv6 🗸							
Ъ	Log	IGMP Agent							

## Fig 3.6.1 Default VLAN Setting page

	CMD-COS-v1.01					ත් රු 👃 පු English
	≡<	Network <	Network > VLAN			🛱 CPU: 3.96% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
ଚ	System Overview	Interfaces	Add			×
₩	Monitoring	DHCP 🗸				
ŝ	System Setup	DNS 🗸	VLAN ID:		*	
몲	Network	IP/MAC Group 🗸 🗸	VLAN Name:		*	
t††	Flow Control	Static Routes 🗸 🗸 🗸	MAC Address:			
•	Access Controller	VLAN	subnet Mask:	255.255.255.0	~	
<u>8</u> "	Authentication	VPN Client $\sim$	Interface:	lan1	$\sim$	
\$↓	Behavior	UPNP V	Multiple IP:		Add	
臣	Firewall	NAT		IP Address	Actions	
Ţ	Advanced application	Port Mapping 🛛 🗸		No Data		
0% 00	Services	IPv6 🗸				
Ъ	Log	IGMP Agent	Remarks:			
				Save Cancel		

Fig 3.6.2 Add VLAN Setting page
	CMD-COS-v1.01						ධ	ΰ¢	<u>e</u> English
	≡́	Network	Network > VLAN			≣∰: CPU: 3.22%	🛄 MEM: 18%	↑ TX: 950.00 B/s	↓ RX: 705.00 B/s
6)	System Overview	Interfaces							
₩	Monitoring	DHCP	VLAN ID:	2		*			
ţĊţ	System Setup	DNS	MAC Address:	10002					
品	Network	IP/MAC Group	IP:						
ttt	Flow Control	Static Routes	Subnet Mask:	255.255.255.0	$\sim$				
<b></b>	Access Controller	VLAN	Interface:	lan1	$\sim$				
<u>8</u> =	Authentication	VPN Client	Multiple IP:			Add			
₩	Behavior	UPNP		IP Address	Actio	ons			
Ħ	Firewall	NAT			No Data				
Ţ	Advanced application	Port Mapping							
0% 00	Services	IPv6	Remarks:						
ß	Log	IGMP Agent		Save Cancel					

Fig 3.6.3 Add VLAN2 Setting on lan1 interface page

	CMD-COS-v1.01										_ ♪ û	¢ 2	English
	=<	Network	<	Network > VLA	N				: <b>.</b>	CPU: 0.25%	MEM: 18% ↑ 1	TX: 0.00 B/s 🔱 R	X: 0.00 B/s
		Hetholik	Ì	VLAN Setting	s								
Ð	System Overview	Interfaces											
₽	Monitoring	DHCP	~		lame/IP, Q			Ad	ld Import	Export	Enable	Disable	Delete
ţĊ	System Setup	DNS	~	VLAN ID	VLAN	✓ MAC Address	IP Address 🗸	Subnet Mask	Interface	Remarks	Status	Actions	
뷺	Network	IP/MAC Group	$\sim$		Name							Edit Disable	
†∔†	Flow Control	Static Routes	~	2	vlan0002			255.255.255.0	lan1		Enabled	Delete	
<b></b>	Access Controller	VLAN		Showing 1 of 1	records				PerPage 20	🗸 Rows 🔍	< 1 > >	1 /1Page	s Jump
<u>8</u> -	Authentication	VPN Client	~										
₩	Behavior	UPNP	~										
Ħ	Firewall	NAT		Heip Tip: 1. V 2. V	lanID support lanID recomm	s end mode, such as 100 lended value for each er	nd range: 1000 M netwo	ork recommended no r	nore than 250, 10,0	00 M network re	ecommended no	more than 1000	
Ţ	Advanced application	Port Mapping	~										
00	Services	IPv6	~										
ß	Log	IGMP Agent											

## 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.

	CMD-COS-v1.01					<u>م</u>	☆ ♪		Er	١ç
	Ξ·	Network	Network > VLAN Edit		≣ <mark></mark> ≣ CPU: 2.72%	MEM: 18% 1	TX: 54.00 B	/s ↓ RX:	73	4.
6	System Overview	Interfaces	Luit							
₩	Monitoring	DHCP	VLAN ID:	2	×					
ţĊţ	System Setup	DNS	VLAN Name:	vlan0002	*					
뮮	Network	IP/MAC Group	MAC Address:							
†∔†	Flow Control	Static Routes	IP:							
r	Access Controller	VLAN	Subnet Mask:	255.255.255.0	$\checkmark$					
<u>&amp;</u>	Authentication	VPN Client	Interface:	lan1	$\sim$					
⇆	Behavior	UPNP	Multiple IP:		Add					
Ħ	Firewall	NAT		IP Address	Actions					
Ţ	Advanced application	Port Mapping		192.168.10.0 255.255.255.0(24)	Edit Delete					
0%	Services	IPv6	Remarks:							
ß	Log	IGMP Agent								
				Save Cancel						

Fig 3.6.5 Adding Multiple IP address page

## 7. VPN Client

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

#### Note:

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

## PPTP:

PPTP stands for Point-to-Point Tunneling Protocol is a network protocol used to implement Virtual Private Network (VPN) tunnels between public networks. PPTP uses a control channel over Transmission Control Protocol (TCP) and a Generic Routing Encapsulation (GRE) tunnel operating to encapsulate Point-to-Point (PPP) packets. As a tunneling protocol, PPTP encapsulates network protocol datagrams within an IP envelope. PPTP was designed to allow users to connect to a VPN server from any point on the Internet and still have the same authentication, encryption, and corporate LAN access they'd have from connecting directly into it.

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

د المعند من												
	=<	Network	<	Network > VPN C	lient > PPTP				Ö	CPU: 0.25% 🛄 ME	M: 16% ↑ TX: 0.00 B/s ↓	RX: 0.00 E
			Ì	PPTP Client Set	tings							
Ð	Overview	Interfaces										
₩	Monitoring	DHCP	$\sim$						Add Import	Export	Enable Disable	Delete
ţĊ	System Setup	DNS	~	Name	Server	Username	Password	Interface	IP Address	Status	Actions	
몲	Network	IP/MAC	~					No Data				
†∔†	Flow Control	Static Routes	~									
•	Access Controller	VLAN										
<u>8</u> "	Authentication	VPN Client	~									
$\downarrow$	Behavior	РРТР										
Ħ	Firewall	L2TP										
Ţ	Advanced application	OpenVPN										
	Services	IPsec										
Ъ	Log	UPNP	~									

Fig 3.7.1 Default PPTP Setting page

	CMD-COS-v1.01				් 🖒 🗘 🕹 English
	<u></u> _<	Network <	Network > VPN Client > PPTP		4 <sup>™</sup> / <sub>2</sub> # CPU: 0.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	System		Add		×
6-3	Overview	Interfaces			
-24	Monitoring	DHCP 🗸 🗸			
ţĊţ	System Setup	DNS 🗸	Name:	pptp	*
몲	Network		serverPort:	1723	*
	flow Control	Gloup	Server:		*
[]+T	Flow Control	Static Routes V	Username :		*
<b>P</b>	Access Controller	VLAN	Password :		*
<b>₽</b> ,	Authentication	VPN Client	MTU:	1400 *	
₩	Behavior	РРТР	MRU	1400 *	
æ	Firewall	I 2TP	Wite.	1400	
	A damaged	<u></u>	Interface :	Auto	
V	application	OpenVPN	Interval duration redial:	0 minute *	
0%	Services	IPsec	timing radials	(start timing after dialing successfully, 0 means unlimited t	ime)
Ъ	Log		uming redia:	open	
		NAT		Save Cancel	

## Fig 3.7.2 Add PPTP Setting page

	CMD-COS-v1.01				ථ	습 수 은 English
	<u></u>	Network <	Network > VPN Client > PPTP		= CPU: 0.00% 🛄 MEM: 18%	↑ TX: 81.00 B/s ↓ RX: 55.00 B/s
<i>—</i>	Sustem	^	Add			× ^
6-3	Overview	Interfaces				
₩	Monitoring	рнср 🗸				
ţĊţ	System Setup	DNS 🗸	Name:	pptpCOMMANDO *		
모	Network		serverPort:	1723 *		
	Network		Server:	*		
ţţţ	Flow Control	Static Routes \vee	Username:	admin		
<b></b>	Access Controller	VLAN	Password:	••••••		
<u>&amp;=</u>	Authentication	VPN Client 🔷	MTU:	1400 *		
₩	Behavior	РРТР	MRU:	1400 *		
田	Firewall	L2TP	Interface:	Auto		
Ţ	Advanced application	OpenVPN	Interval duration redial:	0 minute *		
0%	Services	IPsec .		(start timing after dialing successfully, 0 means unlimited time)		
ſħ.			timing redial:	open		
-13	Log	NAT		Save Cancel		

#### Fig 3.7.3 Add PPTP with username and password setting page

#### Note:

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

CENORA	CMD-COS-v1.01					스) 습 👃 English
	=	Network	Network > VPN Client > PPTP			🛱 CPU: 0.00% 🔛 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
		Network (	PPTP Client Settings			
$\mathfrak{S}$	System Overview	Interfaces				
	Manifestina					Add Import Export Enable Disable Delete
273	Monitoring	DHCP V	Nama Camura		Deserved	
ţĊ	System Setup	DNS 🗸	Name Server	Osername	Password	interface iP address status actions
	N	ID ALACC	pptpCOMMANDO 10.10.10.1	admin	*****	Auto Enabled Edit Disable Delete
666	INETWORK	IP/MAC Group V				
†∔†	Flow Control	Static Routes 🛛 🗸	Showing 1 of 1 records			PerPage 20 $\checkmark$ Rows $\ll$ $\langle$ 1 $\rangle$ $\gg$ 1 /1Pages Jump
<b>P</b>	Access Controller	VLAN				
& <u>=</u>	Authentication	VPN Client				
₩	Behavior	рртр				
臣	Firewall	L2TP				
Ţ	Advanced application	OpenVPN				
0% 00	Services	IPsec				
ſð	Log	UPNP V				
		NAT				

## 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

	CMD-COS-v1.01										6 6 A A	English
	=<	Network	<	Network > VPN Clier	nt > L2TP				i CF	'U: 27.48% 🛄 MEM:	16% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	-			L2TP Client Settin	gs							
69	System Overview	Interfaces										
₩	Monitoring	DHCP	~						Add Import	Export	nable Disable	Delete
ŝ	System Setup	DNS	~	Name	Server	Username	Password	Interface	IP Address	Status	Actions	
윪	Network	IP/MAC Group	~					No Data				
†‡†	Flow Control	Static Routes	~									
۲	Access Controller	VLAN										
<u>&amp;</u> "	Authentication	VPN Client	^									
\$J	Behavior	РРТР										
臣	Firewall											
ÿ	Advanced application	OpenVPN										
0%	Services	IPsec										
Ъ	Log	UPNP	~									

Fig 3.7.5 Default L2TP Client setting page

	CMD-COS-v1.01						් 🗘 🗘 English
	=<	Network	Netwo	rk > VPN Client > L2TP			📮 CPU: 1.24% 🔛 MEM: 16% ↑ TX: 0.00 B/s 👃 RX: 0.00 B/s
~	 System	1-1-5	Add				×
6-3	Overview	internaces					
₽∿	Monitoring	DHCP	~				
ŝ	System Setup	DNS	~	Name:	l2tp		*
品	Network	IP/MAC	~	serverPort:	1701		
		Group		Server:			•
†‡†	Flow Control	Static Routes	~	licername -			- -
<b>P</b>	Access	VLAN		oscinane.			
	Controller			Password:		۲	D *
<u>&amp;</u> "	Authentication	VPN Client	^	MTU:	1400 *		
¢≯	Behavior	РРТР		MRU:	1400 *		
臣	Firewall			Pre-Shared Key:			
Ţ	Advanced application	OpenVPN		Interface:	Auto	~	2
	Services	IPsec		Interval duration redial:	0 minute *		
DA.	Log				(start timing after dialing success	fully, 0 means unlimited tir	time)
43	Log	OPMP	Ň	timing redial:	open		

### Fig 3.7.6 Add L2TP Client setting page

	CMD-COS-v1.01				rightarrow රු රු 👃 ළ English
	≡́	Network <	Network > VPN Client > L2TP		(亞= CPU: 0.50% 🛄 MEM: 18% 个 TX: 194.00 B/s ↓ RX: 173.00 B/s
6)	System Overview	Interfaces	Add		×
₩	Monitoring	рнср 🗸			
ŝ	System Setup	DNS 🗸	Name:	I2tpCOMMANDO	*
몲	Network	IP/MAC Group	serverPort:	1701	]• 
tit	Flow Control	Static Routes 🗸 🗸	Server:	10.10.10.1	*
	Access Controller	VLAN	Username : Password -	admin123	*
<u>&amp;</u> "	Authentication	VPN Client	MTU:	1400 *	
$\downarrow$	Behavior	РРТР	MRU:	1400 *	
臣	Firewall	L2TP	Pre-Shared Key:	abcdxyz	
y	Advanced application	OpenVPN	Interface:		
0% 00	Services	IPsec	Interval duration redial:	0 minute *	
Ъ	Log	UPNP 🗸	timing redial:	(start timing after dialing successfully, 0 means unlimited open	time)
		NAT			
		Port Mapping $\smallsetminus$		Save Cancel	

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

#### Note:

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

	CMD-COS-v1.01										්	û ↓ ≗	English
	<u></u> ≓<	Network	<	Network > VPN	Client > OpenVPN					i CP	U: 0.74% 🛄 MEM: 16%	↑ TX: 0.00 B/s	, RX: 0.00 B/s
6	System	Interfaces	^	OpenVPN Clie	nt Settings								
 	Monitoring	DHCP	$\sim$						Add	Import	Export Enable	Disable	Delete
 ۲	System Setup	DNS	~	Name	Remote Addr	Remote Port	Interface	Protocol	Dev Туре	IP Address	Status	Actions	
몲	Network	IP/MAC Group	~					No Data					
tłt	Flow Control	Static Routes	~										
•	Access Controller	VLAN											
8 <b>.</b>	Authentication	VPN Client	^										
¢‡	Behavior	РРТР											
臣	Firewall	L2TP											
y	Advanced application	OpenVPN											
00	Services	IPsec											
I٩.	Log	UPNP	$\sim$										

#### 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

	CMD-COS-v1.01									් ර	)	English
	=<	Network	Network > VPN C	client > OpenVPN					E CPI	J: 0.74% 🛄 MEM: 16%	↑ TX: 0.00 B/s	VRX: 0.00 B/s
			OpenVPN Clier	nt Settings								
Ð	System Overview	Interfaces										
₩	Monitoring	DHCP 🗸 🗸						Add	Import	Export Enable	Disable	Delete
ŝ	System Setup	DNS 🗸	Name	Remote Addr	Remote Port	Interface	Protocol	Dev Type	IP Address	Status	Actions	
쯂	Network	IP/MAC v Group					No Data					
†#†	Flow Control	Static Routes 🛛 🗸										
P	Access Controller	VLAN										
ê.,	Authentication	VPN Client										
⇆	Behavior	рртр										
臣	Firewall	L2TP										
V	Advanced application	OpenVPN										
0% 00	Services	IPsec										
Δ	Log	UPNP V										

Fig 3.7.8 Default OpenVPN Client setting page

							් <u>බ</u>		_
	CMD-COS-v1.01		Network > VPN Client > OpenVPN			сри: 0.25% 🗖	MEM: 16% 1 TX: 0.0	,	0 B/
	=	Network <	Add						
6	System Overview	DHCP A							
AN.	Monitorina	DNS 🗸							
~		IP/MAC	Name:	ovpn	*				
ţĊ;	System Setup	Chattin Davitare	Pemote Addr:		*				
몲	Network	Static Roules V	Activity Addr.						
(†4†	Flow Control	VLAN	Remote Port:		*				
	Access	VPN Client	Username:		*				
	Controller	DDTD	Password:		۵ *				
<u>&amp;</u> "	Authentication	FF IF	Interface:	Auto	~				
	Behavior	L2TP							
		OpenVPN	Protocol:	UDP	~				
œ	Firewall	IPsec	Dev Type :	TUN	$\sim$				
Ţ	Advanced application	irsee	Cipher:	BF-CBC	$\sim$				
	Services	UPNP 🗸	Comp Lzo:	✓ Open					
п.		NAT	MTH	1400					
43	Log	Port Mapping	MIU.	1400					
		- In this party of the second s	CA:						
		IPv6 🗸							
		IGMP Agent							

Fig 3.7.9 Add OpenVPN Client setting page

#### Note:

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

CMD-	-COS-v1.01					් 🖒 🗘 🚨 English
≡<		Network	<	Network > VPN Client > OpenVPN		±ਹੁੰ≠ CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
System Overvie	w	Interfaces				Â
Monito	ring	DHCP		Cert:		
ද්ටූ? System	Setup	DNS				
品 Networ	ĸ	IP/MAC Group				
filt Flow Co	ontrol	Static Routes		Key:		
Access Control	ller	VLAN				
온 Authen	tication	VPN Client				
🕁 Behavio	r I	PPTP		Extra Config:		
E Firewall		L2TP				
Advanc	ed tion					
□& Service:	s I	IPsec		Accept Push Route:	Open	
[Ի տայ		UPNP		Route:		
		NAT				
		Port Mapping				
		IPv6		timing redial:	open	
		IGMP Agent			Save	

Fig 3.7.10 OpenVPN Client details setting page

	CMD-COS-v1.01									<u>م</u> ن	¢ 2	English
	=<	Network <	Network > VPN C	lient > OpenVPN				= <b></b>	CPU: 3.22%	MEM: 18% 1 TX:	1.72 KB/s ↓ RX:	258.00 B/s
	_		OpenVPN Clien	nt Settings								
R	System Overview	Interfaces										
₩	Monitoring	DHCP 🗸 🗸						Add Imp	oort Export	t Enable	Disable	Delete
ţĊ	System Setup	DNS 🗸	Name	Remote Addr	Remote Port	Interface	Protocol	Dev Type	IP Address	Status	Actions	
÷	Network	IP/MAC Group \vee	ovpnCOMMAN DO	10.10.10.1	12345	Auto	ТСР	TUN		Enabled	Log Edit Disable Delete	
†∔†	Flow Control	Static Routes 🗸 🗸	Showing 1 of 1 re	ecords				PerPage 20	∨ Rows	« < <b>1</b> > )	≫ 1 /1Page	s Jump
•	Access Controller	VLAN										
<u>&amp;</u> =	Authentication	VPN Client 🔷										
⇒	Behavior	рртр										
臣	Firewall	L2TP										
Ţ	Advanced application	OpenVPN										
0% 00	Services	IPsec										
ſð	Log	UPNP 🗸										

#### 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

	CMD-COS-v1.01								් (	) <b>4</b> 2	English
	=<	Network <	Network > VPN Cl	ient > IPsec				: CPU: 0.	25% 🛄 MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
-			IPsec Client Set	tings							
63	Overview	IP/MAC Group 🗸									
₩	Monitoring	Static Routes 🛛 🗸					Add Import	Export	Enable Disab	e Delete	Log
ţĊţ	System Setup	VLAN	Name	Peer IP/Domain	Local Subnet	Peer Subnet	Auth Method	Interface	Status	Actions	
뮮	Network	VPN Client ^					No Data				
ţţţ	Flow Control	рртр									
<b></b>	Access Controller	L2TP									
<u>&amp;</u> =	Authentication	OpenVPN									
₩	Behavior	IPsec									
E	Firewall	UPNP 🗸									
Ţ	Advanced application	NAT									
0%	Services	Port Mapping \vee									
ß	Log	IPv6 V									
		IGMP Agent									

## Fig 3.7.12 Default IPsec Client setting page

	CMD-COS-v1.01				riangle delta d
	≡<	Network <	Network > VPN Client > IPsec		ig CPU: 0.74%
$\epsilon$	System Overview	IP/MAC Group \vee 🤺			
₩	Monitoring	Static Routes 🛛 🗸	Name :	ipsec	
ţĊ	System Setup	VLAN	Peer IP/Domain:		
品	Network	VPN Client 🔷	Local Subnet:	(0.0.1 cm 102 168 1 0/24 cm 0.0.0.0/0)	•
ţţţ	Flow Control	рртр	Peer Subnet:	(Such as: 152,108,1.0/24 of 0.0.00/0)	
<b></b>	Access Controller	L2TP			
<u>&amp;</u> =	Authentication	OpenVPN			
, ¢	Behavior	IPsec		(Such as: 192.168.1.0/24)	
臣	Firewall	UPNP 🗸	Interface:	Auto	
Ţ	Advanced application	NAT	IKE Version:	IKEv2 ~	
0% 00	Services	Port Mapping \vee	IKE Lifetime:	3 * (Unit: hour, range: 1~72)	
ſð	Log	IPv6 V	IKE Proposal:	Auto	~
		IGMP Agent	Auth Method:	Pre-Shared Key $\checkmark$	~

	CMD-COS-v1.01						<b>5</b>	<u>۵</u>	A Eng	glish
	≡<	Network <	Network > VPN Client > IPsec			📮 CPU: 1.73%	🛄 MEM: 16%	1 TX: 0.00 E	/s \downarrow RX:0	0.00 B/s
6	System Overview	IP/MAC Group \vee 🤺	IKE Version:	IKEv2 ~						
₩	Monitoring	Static Routes 🛛 🗸	IKE Lifetime:	3 * (Unit hour range 1~72)						
ţĊţ	System Setup	VLAN	IKE Proposal:	Auto V, Auto V, Auto	$\sim$					
뮮	Network	VPN Client	Auth Method:	Pre-Shared Key						
t††	Flow Control	рртр	Pre-Shared Key:		*					
<b></b>	Access Controller	L2TP	Local ID:							- 1
<u>8</u> =	Authentication	OpenVPN	Peer ID:							
$\stackrel{\leftarrow}{\downarrow}$	Behavior	IPsec	ESP Time :	1 *						
Ħ	Firewall	UPNP ~	ESP Encryption :	(Unit: hour, range: 1~72)						
Ţ	Advanced application	NAT	ESP Auth :	Auto						
0% 00	Services	Port Mapping 🗸	Allow Compression:	Allow						
ß	Log	IPv6 V								
		IGMP Agent		Save Cancel						v

Fig 3.7.13 Add IPsec Client setting page

1	CMD-COS-v1.01				〇) 介 女 皇 English
		Network	Network > VPN Client > IPsec		♦ СРU: 8.50% П МЕМ: 18% ↑ ТК: 3.66 КВ/з ↓ RX: 498.00 В/
ല	System	Interfaces	Name :	ipsec	
<u>مم</u>	Monitoring	DHCP	Peer IP/Domain:	10.10.10.1	
			Local Subnet:	192.168.0.0/24	
- 22	System Setup	DNS	×	(Such as: 192.168.1.0/24 or 0.0.0.0/0)	
몲	Network	IP/MAC Group	Peer Subnet:	192.168.10.0/24	•
tił:	Flow Control	Static Routes	~		
2	Access Controller	VLAN			
8.	Authentication	VPN Client	^	(Such as: 192.168.1.0/24)	
₩	Behavior	PPTP	Interface:	Auto	
E	Finewall	12TP	IKE Version:	IKEv2 ~	
	Advanced		IKE Lifetime:	3 •	
	application	OpenVPN	IKE Proposal -	Auto	Y
	Services	IPsec	Auth Methods	Pro Charad Kau	
Ъ	Log	UPNP	V Pro Flored Key	Pre-sitared key ·	
		NAT	Pre-Shared Key.	commando	
		Port Mapping	v		
		IPv6	Peer ID:		
		IGMP Agent	ESP Time :	1 Unit: hour. range: 1–72)	
			ESP Encryption :	Auto	
			ESP Auth :	Auto	
			Allow Compression :		
				- PARTIN	
				Save Cancel	

Fig 3.7.14 IPsec Client details setting page

									ධ	6 4 2	English
		Natwork	Network > VPN	Client > IPsec				≣ <b>©</b> ≣ CPU: 32.67%	6 🛄 MEM: 18% ↑	TX: 1.96 KB/s ↓ F	X: 364.00 B/s
	=`	Network	IPsec Client Se	ettings							
$(\cdot)$	System Overview	Interfaces									
~	Monitoring	рнср 🗸					Add Import	Export	Enable Disa	ble Delete	Log
ţĈ	System Setup	DNS 🗸	Name	Peer IP/Domain	Local Subnet	Peer Subnet	Auth Method	Interface	Status	Actions	
品	Network	IP/MAC Group 🗸	ipsec	10.10.10.1	192.168.0.0/24	192.168.10.0/24	Pre-Shared Key	Auto	Not Connected	Edit Disable Delete	
†ŧ†	Flow Control	Static Routes 🗸 🗸	Showing 1 of 1	records			PerPag	e 20 ~ Ro	ows « < 1	> >> 1 /1Pa	ges Jump
<b>P</b>	Access Controller	VLAN									
<u>&amp;</u> =	Authentication	VPN Client 🔷									
⇒	Behavior	рртр									
臣	Firewall	L2TP									
Ţ	Advanced application	OpenVPN									
0% 00	Services	IPsec									
ſð	Log	UPNP V									

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 Play) protocol from different manufacturer can automatically discover and Play.

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

	CMD-COS-v1.01			ත් රු 🗘 ළ English
	⊒<	Network <	Network > UPNP > UPNP	ដើ្ធ⊧CPU: 39.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
S	System	рнср 🗸 ^	UPnP Settings	
₩	Monitoring	DNS 🗸	Upnp Server:	Open
ţĊţ	System Setup	IP/MAC Group $ \smallsetminus $	Exclude Port:	1-1024
品	Network	Static Routes 🛛 🗸		Please enter a port range, which can be separated by commas,such as: 80-100,21,200-300
ţ†	Flow Control	VLAN	Allow LAN IP Mapping:	0.0.0.255.255.255.255
<b></b>	Access Controller	VPN Client $\checkmark$	Default Interface Settings:	Any ~
<u>&amp;=</u>	Authentication	UPNP ^	Drop test:	Open
₩	Behavior	UPNP	Time to restart:	Upen Some uppp client devices will only request port mappings when turned on, and such devices are not suitable for turning on this switch
Ħ	Firewall	UPNP Status		Save
Ţ	Advanced application	NAT		
0% 00	Services	Port Mapping \vee		Add Import Export Enable Delete
ľð	Log	IPv6 V	LAN IP Intern	ace Comment status Actions
		IGMP Agent		No Data

## Fig 3.8.1 Default UPnP setting page

	CMD-COS-v1.01				ථ	습 수 은 English
	_<	Network <	Network > UPNP > UPNP		🛱 CPU: 1.75% 🛄 MEM: 18% ↑	TX: 799.00 B/s ↓ RX: 10.48 KB/s
~	System	· · · · · · · · · · · · · · · · · · ·	UPnP Settings			ŕ
63	Overview	Interfaces				
₩	Monitoring	DHCP 🗸	Upnp Server:	✓ Open		
ţĊţ	System Setup	DNS 🗸	Exclude Port:	1-1024		
品	Network	IP/MAC Group $  imes $		Please enter a port range, which can be separated by comr	nas,such as: 80-100,21,200-300	
†∔†	Flow Control	Static Routes 🗸 🗸	Allow LAN IP Mapping:	0.0.0255.255.255.255		
6	Access	V/LAN	Default Interface Settings:	Any 🗸		
	Controller	<b>VEAN</b>	Drop test:	✔ Open		
<u>8</u> =	Authentication	VPN Client 🗸	Testing cycle:	5	minute(range 1-59)	
⇒	Behavior	UPNP ^	Time to restart:	Open Some upnp client devices will only request port	mappings when turned on, and such devices ar	re not suitable for turning on this
Ħ	Firewall	UPNP		switch		
Ţ	Advanced application	UPNP Status		Save		
0% 00	Services	NAT		_	Lunat Fuent Facili	Disekla Delete
ß	Log	Port Mapping 🗸			Export Enable	Disable Delete
			LAN IP Interf	ace Comment	Status Actions	
		IPv6 🗸 🗸				,

Fig 3.8.2 Enabling UPnP setting page

	CMD-COS-v1.01				ධ	습 🗘 🛆 English
	=<	Network <	Network > UPNP > UPNP		📲 CPU: 0.75% 🔛 MEM: 18%	↑ TX: 981.00 B/s ↓ RX: 7.40 KB/s
-		^	Add			×
6)	Overview	Interfaces				
₫⁄	Monitoring	DHCP 🗸 🗸				
ţĊ	System Setup	DNS 🗸	LAN IP:	Use "-" for IP range	192.168.0.1 COMMANDO	
品	Network	IP/MAC Group $  imes $		<pre>&gt;</pre>		
ţţţ	Flow Control	Static Routes 🛛 🗸		No Group Add Group Once configured, please Refresh		
<b>(</b>	Access Controller	VLAN				
<u>&amp;=</u>	Authentication	VPN Client $$		~		¥
₩	Behavior	UPNP ^	Interface :	*		
Ħ	Firewall	UPNP	Remarks:	COMMANDOUPnP		
Ţ	Advanced application	UPNP Status		Save Cancel		
0% 00	Services	NAT				
ľð	Log	Port Mapping 🗸				

Fig 3.8.3 Add UPnP setting page

	CMD-COS-v1.01						۵	습 수 온	English
	=,	Network <	Network > UPNP > UPNP			iĝi C	CPU: 19.50% 🛄 MEM: 18%	↑ TX: 814.00 B/s ↓	RX: 5.89 KB/s
೯	System Overview	Interfaces	UPnP Settings						
₩	Monitoring	рнср 🗸	Upnp Server:	✓ Open					
ţĊ	System Setup	DNS ~	Exclude Port:	1-1024					
몲	Network	IP/MAC Group 🗸 🗸		Please enter a port range, which car	be separated by commas, such	as: 80-100,21,200-300			
tŧt	Flow Control	Static Routes $\sim$	Allow LAN IP Mapping:	0.0.0.0-255.255.255.255					
•	Access Controller	VLAN	Default Interface Settings:	Any	~				
8.	Authentication	VPN Client 🗸 🗸	Drop test:	Open					
4			Testing cycle:	5	minute(	range 1-59)			
→	Behavior	UPNP ^	Time to restart:	Open Some upnp client device	s will only request port mapping	is when turned on, and such de	evices are not suitable for turni	ng on this switch	
Ħ	Firewall	UPNP							
y	Advanced application	UPNP Status		Save					
0% 00	Services	NAT				Add	Import Export E	nable Disable	Delete
Ъ	Log	Port Mapping $\sim$	LAN IP I	nterface	Comment	Status	Actions		
		IPv6 ~	192.168.0.1,COMMANDO	wan1	COMMANDOUPnP	Enabled	Edit Dis	able Delete	
		IGMP Agent	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



## 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. 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.

	CMD-COS-v1.01		් 🗘 🗘 🕰 English
	⊒<	Network <	Network > NAT = EPU: 0.74% = MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
0	Surtem		Network Address Translation
6-9	Overview	Interfaces	
∽	Monitoring	DHCP 🗸 🗸	Interface/Addr/Protoc/Q Add Import Export Enable Disable Delete
ţĊţ	System Setup	DNS 🗸	Action Out In Src Addr Dst Addr Src Port Dst Port NAT Addr NAT Port Protocol Remarks Status Actions 🗌
矗	Network	IP/MAC Group 🛛 🗸	No Data
†∔†	Flow Control	Static Routes $\sim$	
<b>R</b>	Access Controller	VLAN	
<u>&amp;</u> =	Authentication	VPN Client $\vee$	
\$	Behavior	UPNP ~	
臣	Firewall	NAT	
Ţ	Advanced application	Port Mapping $\sim$	
0% 00	Services	IPv6 V	
ß	Log	IGMP Agent	

To configure Network Address Translation, Click on Network > NAT

Fig 3.9.1 Default Network Address Translation page

	CMD-COS-v1.01				
	⊒<	Network <	Network > NAT		
6	System	Interfaces	Add		
 	Overview				
M	Monitoring	рнср 🗸		Action:	Filer V
÷	System Setup	DNS 🗸		In Interface:	
品	Network	IP/MAC Group 🛛 🗸		Out Interface:	
<b>†</b> ∔†	Flow Control	Static Routes $\sim$			
	Access Controller	VLAN	Src Addr		
87	Authentication	VPN Client $\vee$		IP:	Use "-" for IP range
	Rehavior				<
**	Bellavior	Urinr V			No Group Add Group
臣	Firewall	NAT			Once configured, please <b>Refresh</b>
2	Advanced application	Port Mapping $\sim$			✓
0% 00	Services	IPv6 V			
ъ	Log	IGMP Agent			
			Dst Addr		
				IP:	Use 1-1 for IP range
					A state of the
					No Group Add Group
					Once configured, please Refresh
				Protocol:	Any 🗸
				Remarks	
					Save Cancel

Fig 3.9.2 Default Add Network Address Translation page

					ු රු 🗘 ළ English
		Network 〈	Network > NAT		🖕 CPU: 23.00% 🛄 MEM: 18% ↑ TX: 2.95 KB/s ↓ RX: 43.78 KB/s
~			Add		× ^
6-3	Overview	Interfaces		Interface	
~~					
÷					
놂				□ lan1 □ vlan0002 🗸 wan1	
†∔†				pptpCOMMANDO I2tpCOMMANDO ovpnCOMMANDO	
•	Access Controller		Src Addr	OK Cancel	
<u>&amp;</u> "					^
$\Leftrightarrow$				Add Group Refresh Join>>	
Ħ				< <remove< td=""><td></td></remove<>	
Ţ	Advanced application				
0%					
ß					

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

	GMD-COS-v1.01				Dj 🗘 🗘 🚊 English
	=,	Network <	Network > NAT		©-CPU:4.75% □ MEM-18% ↑ TX:116 KB/4 ↓ RX:35.91 KB/4
~				Action:	Source address NAT
6-3	Overview	Interfaces		In Interface:	Lant
- 64	Monitoring	DHCP 🗸		Out Interface:	vant
¢	System Setup	DNS 🗸			
몲	Network	IP/MAC Group 🗸 🗸	Src Addr	ID:	1921 MAR 0 10
148	Flow Control	Static Routes $\sim$			COMMANDO
9	Access Controller	VLAN			John >>
8	Authentication	VPN Client 🗸 🗸			And Ghos Add Madag
₩	Behavior				v v
Ħ	Firewall	NAT			
	Advanced application	Port Mapping 🛛 🗸			
88	Services	IPv6 ~	Dst Addr	IP:	Use 15 for P more 2021.1.1
ቤ	Log	IGMP Agent			COMMANDO
					No Group Add Group Chee configured, place Refeat
				Protocol:	tcp+udp $\lor$
Γ_				Src Port	2000
				Dst Port	80
				NAT Addr	10.10.10.1
				Remarks	COMMANDONAT

Fig 3.9.4 Network Address Translation details page

2	CMD-C05-4101				🛆 û 🗘 😩 English
	=,	Network <	Network > NAT		♦ CPU: 475% 💭 MEM. 18% ↑ TX: 1.16 KB/s ↓ RX: 3.53 H KB/s
~				Action:	Source address NAT V
63	Overview	Interfaces		In Interface:	lant
5	Monitoring	DHCP 🗸 🗸		Out Interface:	sant
ŵ	System Setup	DNS 🗸			
몲	Network	IP/MAC Group 🔍	Src Addr	10.	192160.00
111	Flow Control	Static Routes $\sim$		1P :	
2	Access Controller	VLAN			<ul> <li></li> </ul>
BT	Authentication	VPN Client 🗸			No Group Add Group Control Con
←	Rehador				
*	Denavior	UPINF V			v v
Ħ	Firewall	NAT			
	application	Port Mapping 🛛 🗸	Dst Addr		
	Services	IPv6 ~		IP:	Une 11 for tP range. 202.1.1.1
Ъ	Log	IGMP Agent			
					No Course Add Groups
					One configured, plaue Refresh
				Protocol:	tçp+udp v
				Src Port	2000
_				Dst Port	80
				NAT Addr	10.10.1
				Remarks	

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

	CMD-COS-v1.01	L							්	û 4 ≗	English
	≡<	Network <	Network >	Port Mapping > Port Mapp	ping			E CPU: 4	4.25% 🛄 MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
~	System		Port Map	oping / Port Forwarding	Settings						
(~)	Overview	Interfaces									
<u>-</u>	Monitoring	DHCP 🗸	All	Lan Addr/Port/	Remark Q		Add	Import	Export Enable	e Disable	Delete
ţ	System Setup	DNS 🗸	Lan Addr	$\checkmark$ Lan Port $\checkmark$	Protocol $\checkmark$	Interface $\checkmark$	Wan Port $\checkmark$	Remarks	Status	Actions	
÷	Network	IP/MAC Group \vee					No Data				
†∔†	Flow Control	Static Routes 🛛 🗸									
<b></b>	Access Controller	VLAN	Help :	<ol> <li>If dial external network ,</li> <li>If an IP has a multi-rang</li> </ol>	, the net address can r je port written all at or	replace the net addres nce, it must be consist	s with the network car ent with both external	d nam, such as: a and external netwo	dsl1 ork ports, such as the e	external network port	
<u>&amp;</u> =	Authentication	VPN Client $$		80-100,21,200-300 Intrane	et ports 80-100,21,200	-300					
\$	Behavior	UPNP 🗸									
Ħ	Firewall	NAT									
Ţ	Advanced application	Port Mapping 🔿									
00	Services	Port Mapping									
ſð	Log	DMZ									
		IPv6 V									

Fig 3.10.1 Default Port Mapping / Port Forwarding Settings page

<u>e</u> Englis	û 4	්්								
) B/s 🤳 RX: 0.00	↑ TX: 0.00	5% 🛄 MEM: 16%	≣⊑ CPU: 0.25%		ng	<ul> <li>Port Mappin</li> </ul>	Network > Port Mapping >	etwork <	=< r	
							Add			-
								terfaces	verview	63
								HCP 🗸 🗸	onitoring [	₩
			*				Lan Addr:	vs v	stem Setup [	ŝ
			*				Lan Port:	/MAC Group 🗸 🗸	etwork I	品
				$\sim$	tcp		Protocol:	atic Routes 🛛 🗸	ow Control S	<b>†</b> ↓†
				anet IP	Extranet Interface  Ext		Мар Туре:	ANI	cess ,	_ _
			*				Interface:	AN	ontroller	-
			*				Wan Port:	'N Client 🗸 🗸	uthentication \	<u>&amp;</u> =
							Remarks:	PNP ~	havior l	₩
								AT	rewall 1	臣
					Save Cancel			rt Mapping 🛛 🗸	dvanced polication	V
		m cuch acu adel1	with the network card nem	n ranlaca tha nat addracs w	wternel network, the net address s	1. If dial or	Hala	<i>r</i> 6 ~	rvices I	0% 00
; the	orts, such as	d external network p	nt with both external and ex 300	once, it must be consistent anet ports 80-100,21,200-30	has a multi-range port written all a network port 80-100,21,200-300 Int	2. If an IP external n	Help :	MP Agent	ig I	ſð
a	orts, such	am, such as: adsl1 d external network pr	• • • • • • • • • • • • • • • • • • •	n replace the net address w once, it must be consistent anet ports 80-100,21,200-30	tcp            • Extranet Interface         • Ext         any          any          Save         Cancel         external network, the net address of has a multi-range port written all a network port 80-100,21,200-300 Int	1. If dial e 2. If an IP external n	Lan Addr: Lan Port: Protocol: Map Type: Interface: Wan Port: Remarks: Help :	NS × MAC Group × atic Routes × AN N Client × NP × NP × AT rt Mapping × r6 ×	stem Setup [ etwork   sw Control   sw Contro	

Fig 3.10.2 Add Port Mapping / Port Forwarding Settings page

	CMD-COS-v1.01						۵	û	¢ 2	<u> </u>	English
	Ξ	Network <	Network > Port Mapping >	Port Mapping		≣ <b>∷</b> ≣ CPU: 0.00%	<b>MEM:</b> 18%	↑ тх: 2	7.00 B/s	↓ RX:	33.00 B
6	System	∧ Interfaces	Add								;
	Overview	interfaces									
Ψ	Monitoring	рнср 🗸		G	102 100 1 10						
ţĊ	System Setup	DNS 🗸	Lan Addr:		192.168.1.10						
品	Network	IP/MAC Group \vee	Lan Port:	8	80						
(†1†	Flow Control	Static Routes 🗸	Protocol:	t	tcp+udp ~						
	Access		Мар Туре:		Extranet Interface						
	Controller	VLAN	Interface:	2	202.202.1.220 *						
<u>8</u> =	Authentication	VPN Client $\checkmark$	Wan Port:	6	64901 *						
⇔	Behavior	UPNP 🗸	Remarks:	L.	LAN Server Globally available via Public IP						
臣	Firewall	NAT									
Ţ	Advanced application	Port Mapping A			Save						
0%	Services	Port Mapping		A. 17 P. L				14			
Ŀ	Log	DMZ	Help :	2. If an IP has external netwo	nai network , the net address can replace the net address with a multi-range port written all at once, it must be consistent wit ork port 80-100 21 200-300 Intranet ports 80-100 21 200-300	the network card nar th both external and	m, such as: ads external network	: ports, su	ch as the		
					, , , , , , , , , , , , , , , , , , , ,						

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

	CMD-COS-v1.01							ද	) \$ & &	English
	=	Network <	Network > Port Mapping > Port Mappi	ng			≣ CPU: 0.99%	🛄 MEM: 18% ↑ T)	K: 272.00 B/s 🔱 RX	: 425.00 B/s
	_	A	Port Mapping / Port Forwarding S	ettings						
Ð	System Overview	Interfaces								
₩	Monitoring	DHCP 🗸	All   Lan Addr/Port/F	lemark Q		Add	Import Exp	oort Enable	Disable	Delete
ŝ	System Setup	DNS 🗸	Lan Addr ∨ Lan Port ∨	Protocol 🗸	Interface 🗸	Wan Port $\checkmark$	Remarks	Status	Actions	
뮯	Network	IP/MAC Group $  imes $	192.168.1.10 80	tcp+udp	202.202.1.220	64901	LAN Server Globally available via Public IP	Enabled	Edit Copy Disable Delete	
†∔†	Flow Control	Static Routes 🛛 🗸	Shawing 1 of 1 seconds			DD	20 N Pauro		1 (10	lump
<b></b>	Access Controller	VLAN	showing For Frecords			PerPag	ge 20 V Kows		// I /TPage	s Jump
<u>&amp;</u> =	Authentication	VPN Client $$								
\$	Behavior	UPNP 🗸	Help: 1. If dial external network , 2. If an IP has a multi-range 80-100,21,200-300 Intranet	the net address can re port written all at one ports 80-100,21,200-3	place the net address e, it must be consiste 300	with the network card nt with both external a	nam, such as: adsl1 nd external network p	ports, such as the ext	ernal network port	
臣	Firewall	NAT								
Ţ	Advanced application	Port Mapping 🔿								
0% 00	Services	Port Mapping								
ſð	Log	DMZ								

#### 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.

	CMD-COS-v1.01				් රු 🗘 English
	⊒<	Network <	Network > Port Mapping > DMZ		📮 CPU: 0.74% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
			Add		×
63	Overview	рнсь 🔨			
-^-	Monitoring	DNS 🗸			
ţ	System Setup	IP/MAC Group $  imes $	Мар Туре:	Extranet Interface Extranet IP	
뷺	Network	Static Routes 🗸 🗸	Interface :		
[†↓+]	Flow Control	VLAN	Lan Addr:		*
	Accore		Protocol:	Unlimited $\checkmark$	
<b></b>	Controller	VPN Client V	Remarks:		
<u>&amp;</u> =	Authentication	UPNP 🗸			
₩	Behavior	NAT		Save Cancel	
⊞	Firewall	Port Mapping \land			
Ţ	Advanced application	Port Mapping			
0%	Services	DMZ			
ſð	Log	IPv6 V			
		IGMP Agent			

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

#### Fig 3.10.5 Default DMZ Settings page

	CMD-COS-v1.01				් 🗘 🛆 English
	⊒<	Network <	Network > Port Mapping > DMZ		🛱 CPU: 0.74% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
ଚ	System Overview	DHCP 🗸 🗖	Add		×
₽	Monitoring	DNS 🗸			
ţĝ	System Setup	IP/MAC Group \vee	Map Type:	Extranet Interface Extranet IP	
<b>—</b>	Network	Static Routes 🗸	Interface:		]
ţţţ	Flow Control	VLAN	Lan Addr:	Helimited	]
R	Access Controller	VPN Client $\checkmark$	Remarks:	•	
& <u>=</u>	Authentication	UPNP 🗸			
₩	Behavior	NAT		Save Cancel	
Ħ	Firewall	Port Mapping \land			
Ţ	Advanced application	Port Mapping			
0% 00	Services	DMZ			
ß	Log	IPv6 V			
		IGMP Agent			

#### Fig 3.10.6 Add DMZ Settings page

	CMD-COS-v1.01				ے 🗘 🏠 🔔 English
	⊒<	Network <	Network > Port Mapping > DMZ		ដើ្ឋ፤ CPU: 0.00% 🛄 MEM: 18% ↑ TX: 27.00 B/s ↓ RX: 27.00 B/s
6)	System Overview	∧ Interfaces	Add		×
₩	Monitoring	рнср 🗸			
ţĊţ	System Setup	DNS 🗸	Мар Туре:	Extranet Interface      Extranet IP	
品	Network	IP/MAC Group \vee	Interface :	wan1	
†4†	Flow Control	Static Routes 🗸 🗸	Lan Addr:	192.168.1.1	
<b>P</b>	Access Controller	VLAN	Protocol: Excl Port:	80 ×	
<u>&amp;</u> =	Authentication	VPN Client 🗸 🗸	Remarks:	Ohly port 80 can be accessible	
⇆	Behavior	UPNP 🗸			
Ħ	Firewall	NAT		Save Cancel	
Ţ	Advanced application	Port Mapping 🔿			
0%	Services	Port Mapping			
ß	Log	DMZ			

#### Fig 3.10.7 DMZ detail Settings page

	CMD-COS-v1.01				스) 슈 욘 English
	≡<	Network <	Network > Port Mapping > DMZ		to B/s ↓ RX: 27.00 B/s to RX: 27.00 B/s
Ð	System Overview	Interfaces	Add		X
~~	Monitoring	рнср 🗸			
ţĝ	System Setup	DNS V	Map Type:	Extranet Interface      Extranet IP	
品	Network	IP/MAC Group \vee	Interface :	wan1	
†∔†	Flow Control	Static Routes 🗸 🗸	Lan Addr:	192.168.1.1	*
<b></b>	Access Controller	VLAN	Protocol:	tcp+udp ~	
<u>&amp;</u> =	Authentication	VPN Client 🗸 🗸	Excl Port: Remarks:	80 Only port 80 can be accessible	*
₩	Behavior	UPNP V			1
Ħ	Firewall	NAT		Save	
Ţ	Advanced application	Port Mapping			
0%	Services	Port Mapping			
R		DMZ			

#### 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 0:0:0:0:0:0:0:0:1/128 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

	CMD-COS-v1.01				스) 슈 스 English
	Ē	Network <	Network > Port Mapping > DMZ		i∰: CPU: 0.00% 🛄 MEM: 18% ↑ TX: 27.00 B/s ↓ RX: 27.00 B/s
Ð	System Overview	A Interfaces	Add		×
<u>-</u>	Monitoring	DHCP 🗸			
ŝ	System Setup	DNS 🗸	Map Type:	Extranet Interface Extranet IP	
品	Network	IP/MAC Group \vee	Interface :	wan1	
†∔†	Flow Control	Static Routes 🗸 🗸	Lan Addr:	192.168.1.1	*
- -	Access	VLAN	Protocol:	tcp+udp ~	
	Controller		Excl Port:	80	*
لقِتْ	Authentication	VPN Client 🗸	Remarks:	Ohly port 80 can be accessible	]
\$↓	Behavior	UPNP 🗸			
臣	Firewall	NAT		Save Cancel	
Ţ	Advanced application	Port Mapping 🔿			
0% 00	Services	Port Mapping			
[ħ	Log	DMZ			

## Fig 3.11.1 Default IPv6 Page

COOM	CMD-COS-v1.01				් 🗘 🗘 ළ English
	≡<	Network <	Network > IPv6 > IPv6 Set		🖆 CPU: 0.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
R	System Overview	DHCP 🗸 🔨	Add		X
₽4	Monitoring	DNS 🗸	Intranet Interface:	~	
ţĊţ	System Setup	IP/MAC Group $  imes $	Configuration Type:	Automatic Acquisition $\checkmark$	
品	Network	Static Routes 🗸 🗸	Prefix Length:	Automatic $\vee$	
†∔†	Flow Control	VLAN	IPv6 address:		
<b></b>	Access Controller	VPN Client $\lor$	DHCPv6:	✔ Open	
8= 	Authentication	UPNP 🗸	DHCPv6 Mode:	Stateless + stateful $\checkmark$	
₩	Behavior	NAT	IPv6 DNS:	✓ Open	
Ħ	Firewall	Port Mapping $$	Preferred DNS:		
Ţ	Advanced application	IPv6 ^	Alternative DNS:		
0%	Services	IPv6 Set	Lease Term:	120 minute	
ß	Log	DHCPv6 Terminal		Save Cancel	

Fig 3.11.2 Add IPv6 Page

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

	CMD-COS-v1.01							△ 습 ♣	English
	≡<	Network <	Network > IPv	6 > IPv6 Set			≣ CPU: 0.25% 🛄 N	MEM: 18% 个 TX: 78.00 B	/s ↓ RX: 27.00 B/s
-	Sustem	^	IPv6						
(-)	Overview	Interfaces							
₩	Monitoring	рнср 🗸	Extranet Confi	guration					
ţĊţ	System Setup	DNS 🗸							
뷺	Network	IP/MAC Group ${}^{\checkmark}$	Iface Wan	Access Method	IPv6 Pretix	IPv6 address	IPv6 gateway	Status	Actions
tłt	Flow Control	Static Routes 🗸 🗸	wan1	acquisition)			fe80::1	Enabled	Edit Disable
<b>P</b>	Access Controller	VLAN							
& <u>=</u>	Authentication	VPN Client $$							
₩	Behavior	UPNP 🗸	Intranet Confi	guration					
Ħ	Firewall	NAT					Add	Enable Disab	e Delete
Ş	Advanced application	Port Mapping 🗸	Intranet Interface	ink local address	IPv6 address	DHCPv6	DHCPv6 Mode Lease Term	Preferred DNS	Alternativ
0% 00	Services	IPv6 ^				No Data			
ß	Log	IPv6 Set							
		DHCPv6 Terminal ∨	<						>

Fig 3.11.3 Enabling DHCPv6 Page

	CMD-COS-v1.01				🛆 🏠 🗘 English
	⊒<	Network <	Network > IPv6 > IPv6 Set		🗓: CPU: 3.00% 🛄 MEM: 17% ↑ TX: 0.00 B/s \downarrow RX: 0.00 B/s
			Add		×
A	System Overview	Interfaces			
₩	Monitoring	рнср 🗸	Intranet Interface:	lan1 ~	
ţĊţ	System Setup	DNS 🗸	Configuration Type:	Automatic Acquisition $\checkmark$	
뮯	Network	IP/MAC Group $ arsigma$	Prefix Length:	Automatic $\checkmark$	
†∔†	Flow Control	Static Routes 🛛 🗸	IPv6 address:		
<b>R</b>	Access Controller	VLAN	DHCPv6:	✓ Open	
8= ;	Authentication	VPN Client $$	DHCPv6 Mode:	Stateless + stateful $\lor$	
\$	Behavior	UPNP 🗸	IPv6 DNS:	✓ Open	
Ħ	Firewall	NAT	Preferred DNS:		
<b>I</b>	Advanced application	Port Mapping 🗸	Alternative DNS:		
0%	Services	IPv6 ^	Lease Term:	120 minute	
ß	Log	IPv6 Set		Save Cancel	
		DHCPv6 Terminal Y			

Fig 3.11.4 Automatic Acquisition of IPv6 address for LAN1 interface Page

×	CMD-COS-v1.01											<u>م</u> ۵ ۵	🖄 English
	<u></u> ,	Network	<	Network > I	IPv6 > IPv6 Set						🤹 CPU: 0.75% 🔛 N	1EM: 18% ↑ TX: 33.00	B/s ↓ RX: 33.00 B/s
ଚ	System Overview	Interfaces		IPv6									
5	Monitoring	DHCP	$\sim$	Eutropot Co	afiguration								
¢;	System Setup	DNS	$\sim$	Extranet Co	iniguration .								
品	Network	IP/MAC Group	~	Itace Wan	Access Method	IPv6 Pretix		IPv6 addres	5	IPv6 gi	ateway	Status	Actions
TH:	Flow Control	Static Routes	~	wan1	DHCPv6 client(dynami	c acquisition)				te80::1		tnabled	Edit Disable
۲	Access Controller	VLAN											
<u>8</u> ,	Authentication	VPN Client	$\sim$	Intranct Cor	afiguration								
¢↓	Behavior	UPNP	~	indanet coi	linguration						Add	Enable Disa	ble Delete
臣	Firewall	NAT		Intranet	Link local address	IPv6 address	DHCP	6 DHCPv6 Mode	Lease	Preferred DNS	Alternative DNS	Status	Actions
Ţ	Advanced application	Port Mapping	$\sim$	Interface	fe80::a9b:4bff:fe50:1cbc	fc00:ec88:bde3:1:1/64	open	Stateless +	120	fe80::1	1	Enabled	Edit Disable
	Services	IPv6	^					statetul			]		Delete
Ъ	Log	IPv6 Set											
		DHCPv6 Termin	al										

Fig 3.11.5 Automatic IPv6 address for LAN1 interface Page

	CMD-COS-v1.01				ා රු 🗘 🚊 English
	≡<	Network <	Network > IPv6 > IPv6 Set		🛱 CPU: 0.25% 🛄 MEM: 18% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
0	System	A Interfaces	Add		×
₩	Monitoring	рнср 🗸	Intranet Interface:	vlan0002 V	
ţĊţ	System Setup	DNS 🗸	Configuration Type:	Static Configuration $\checkmark$	
뮮	Network	IP/MAC Group \vee	IPv6 address:	2001:5bcd:1cc1::1/64	
†∔†	Flow Control	Static Routes 🛛 🗸	DHCPv6:	Open	
<b>R</b>	Access Controller	VLAN	DHCPv6 Mode:	Stateful $\checkmark$	
<u>&amp;</u> =	Authentication	VPN Client $$	IPv6 DNS:	✓ Open	
⇒	Behavior	UPNP 🗸	Preferred DNS:		
Ħ	Firewall	NAT	Alternative DNS:		
Ţ	Advanced application	Port Mapping $$	Lease Term:	120 minute	
0% 00	Services	IPv6 ^		Save Cancel	
ß	Log	IPv6 Set			
		DHCPv6			

Fig 3.11.6 Manual IPv6 address for vlan0002 interface Page

	CMD-COS-v1.01												û ↓	🙇 English
	=,	Network	<	Network >	IPv6 > IPv6 Set							🖕 CPU: 7.75% 🔛 MEI	M: 18% ↑ TX: 81.00 B	3/s 👃 RX: 27.00 B/s
				IPv6										
63	Overview	Interfaces												
₩	Monitoring	DHCP	~	Extranet Co	nfiguration									
ŝ	System Setup	DNS	$\sim$		5									
品	Network	IP/MAC Group	~	Iface Wan	Access Method	IPv6 Prefix		IPv6 address			IPv6 gateway		Status	Actions
				wan1	DHCPv6 client(dynam	ic acquisition)					fe80::1		Enabled	Edit Disable
111	Flow Control	Static Routes	~											
۲	Access Controller	VLAN												
<u>8</u> =	Authentication	VPN Client	$\sim$	Intranot Cor	oficuration									
\$4	Behavior	UPNP	$\sim$	indanet co	Ingulation							Add	Enable Disab	le Delete
臣	Firewall	NAT		Intranet	Link local address	IPv6 address	DHCPv6	DHCPv6 Mode	Lease	Preferred DNS		Alternative DNS	Status	Actions
⊲	Advanced	Port Mapping	$\sim$	Interface					Term					
	application			lan1	fe80::a9b:4bff:fe50:1cbc	fc00:ec88:bde3:1:1/64	open	Stateless + stateful	120	fe80::1			Enabled	Edit Disable Delete
öð	Services	IPvo	^		(-9001-4)-((-C0-1-)	2001.51		Charles I	120	6-90-1			Freddad	Edit Disable
ß	Log	IPv6 Set		Vianuuuz	Teouca9b:4bmteou:Tcbc	2001:50cd:1cc1::1/04	close	Stateful	120	TEOU:: I			chabled	Delete
		DHCPv6 Termin	al											
		IGMP Agent												

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 configuration.

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

	≡<	Network <	Network > IPv6 > DF	ICPv6 Terminal			E CPU	J: 0.50% 🛄	MEM: 16% ↑ TX	(: 0.00 B/s 🔱	RX: 0.00 B/s
~	System		DHCPv6 Terminal								
6.)	Overview	0113									
₩	Monitoring	IP/MAC Group $ \smallsetminus $	Mac/IPv6 Addr/DUI								
ţĊţ	System Setup	Static Routes 🗸 🗸	Hostname	Мас	Link Addr	lpv6 Addr	DUID(DHCP unique identifier)	interface	Effective Time	Remarks	
品	Network	VLAN				No Data					
†∔†	Flow Control	VPN Client $$									
<b></b>	Access Controller	UPNP 🗸									
<u>&amp;</u> =	Authentication	NAT									
⇆	Behavior	Port Mapping $$									
Ħ	Firewall	IPv6 ^									
Ţ	Advanced application	IPv6 Set									
0%	Services	DHCPv6 Terminal									
Ŀ	Log										
		IGMP Agent									

## Fig 3.11.8 Default DHCPv6 Terminal Page

	CMD-COS-v1.01						〇) 슈 오 Englist
	⊒<	Network <	Network > IPv6 > DHC	Pv6 Terminal			≣Ö≣ CPU: 1.98% 🛄 MEM: 18% ↑ TX: 55.00 B/s ↓ RX: 66.00
~	Surtem		DHCPv6 Terminal				
6-3	Overview	Interfaces					
₩	Monitoring	DHCP 🗸	Mac/IPv6 Addr/DUID	Q			
ţĊ	System Setup	dns ~	Hostname	Мас	Link Addr	lpv6 Addr	DUID(DHCP unique interface Effective Time Remarks identifier)
品	Network	IP/MAC Group \vee	DESKTOP-70API5S	e0:db:55:be:35:5b	fe80::8464:7216:bb81: 2716	fc00:ec88:bde3:1::899	00010001277e82d1e0 lan1 01:55:51
†∔†	Flow Control	Static Routes 🛛 🗸					
<b></b>	Access Controller	VLAN	Showing 1 of 1 record	ls			PerPage 20 V Rows 《 〈 1 〉 》 1 /1Pages Jun
& <u>=</u>	Authentication	VPN Client $\checkmark$					
₩	Behavior	UPNP ~					
臣	Firewall	NAT					
Ţ	Advanced application	Port Mapping $$					
0%	Services	IPv6 ^					
ſð	Log	IPv6 Set					
		DHCPv6 Terminal					

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

	CMD-COS-v1.01						් ර	수 은 English
	Ξ<	Network <	Network > IPv6				📮 CPU: 0.74% 🛄 MEM: 16% ↑	TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System	DNS 🗸 🗖	Neighbor list					
FM	Overview	IP/MAC Group \vee	MAC/IPv6 Addr Q					Clean All
 ث	System Setup	Static Routes 🛛 🗸	Terminal MAC	IPv6 Addr	interface	Status	Remarks	Actions
뷺	Network	VLAN				No Data		
ţ†	Flow Control	VPN Client 🗸 🗸						
<b></b>	Access Controller	UPNP 🗸						
<u>&amp;</u> =	Authentication	NAT						
<b>↓</b>	Behavior	Port Mapping $$						
Ħ	Firewall	IPv6 ^						
Ţ	Advanced application	IPv6 Set						
0% 00	Services	DHCPv6 Terminal						
ß	Log							
		IGMP Agent						

Fig 3.11.10 Default IPv6 Neighbor List Page

	CMD-COS-v1.01							English
	=<	Network <	Network > IРvб			≣ <u>□</u> ≣ CPU: 0.00%	MEM: 18% 1X: 164.00 B	/s 🤳 RX: 214.00 B/s
-			Neighbor list					
63	Overview	DNS V						
₩	Monitoring	IP/MAC Group ${}^{\checkmark}$	MAC/IPv6 Addr Q					Clean All
ŝ	System Setup	Static Routes 🛛 🗸	Terminal MAC	IPv6 Addr	interface	Status	Remarks	Actions
品	Network	VLAN	20:a6:0c:37:4d:13	fc00:ec88:bde3:1:6c8e:a530:7 d4c:bb00	lan1	STALE		Delete
ţ†	Flow Control	VPN Client $\vee$	Showing 1 of 1 records			PerPage 20 V Rov	vs « < 1 > » 1	/1Pages Jump
۲	Access Controller	UPNP 🗸						
<u>&amp;</u> =	Authentication	NAT						
\$	Behavior	Port Mapping 🗸						
臣	Firewall	IPv6 ^						
Ţ	Advanced application	IPv6 Set						
0%	Services	DHCPv6 Terminal						

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

	CMD-COS-v1.01					
	,	Network <	Network > IGMP Agent			
~	System		IGMP Agent			
(~)	Overview	Interfaces				
₩	Monitoring	DHCP 🗸 🗸	IGMP Agent: 🗾 Open			
ţĊţ	System Setup	DNS ~	IGMP Protocol Version : IGMPv2 V			
♣	Network	IP/MAC Group 🛛 🗸	Uplink Port: wan1 V			
†∔†	Flow Control	Static Routes 🛛 🗸	Downlink Port: lan1 V			
<b></b>	Access Controller	VLAN				
&= ;,	Authentication	VPN Client 🗸 🗸	Save			
₩	Behavior	UPNP 🗸				
Ħ	Firewall	NAT				
Ţ	Advanced application	Port Mapping 🗸 🗸				
0% 00	Services	IPv6 V				
ß	Log	IGMP Agent				

Fig 3.12.1 Default IGMP Agent Page

	CMD-COS-v1.01				스) 슈 스 English
	⊒<	Network	Network > IGMP Agent		🛱 CPU: 2.50% 🛄 MEM: 18% ↑ TX: 135.00 B/s 🤳 RX: 109.00 B/s
6	System	Interfaces	IGMP Agent		
	Monitoring	DHCP	IGMP Agent:	Open	
ţ	System Setup	DNS	IGMP Protocol Version:	IGMPv2	
品	Network	IP/MAC Group	Uplink Port:	wan1 ~	
†∔†	Flow Control	Static Routes	Downlink Port:	lan1 V	
<b></b>	Access Controller	VLAN		Save	
&= ;;	Authentication	VPN Client	,		
\$	Behavior	UPNP			
Ħ	Firewall	NAT			
Ţ	Advanced application	Port Mapping			
0%	Services	IPv6			
Ŀ	Log	IGMP Agent			

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

	<u> </u> <	Flow Control	<
$(\tilde{\cdot})$	System Overview	Multi-WAN	$\sim$
~~	Monitoring	Smart Flow Control	
Śż	System Setup	IP/MAC Limiters	$\sim$
品	Network	Protocol Library	~
<b>†</b> ↓†	Flow Control		
<b>@</b>	Access Controller		
<u>&amp;=</u>	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
	2							්	6 4 2	English
	CMD-COS-v1.01	Elow Control	Flow Control > Multi-W	AN > Load Balancing	1			CPU: 1.49% 🛄 MEM:	16% ↑ TX: 0.00 B/s	↓ RX: 0.00 B
			Multi-WAN Load Ba	lancing Settings						
6	System Overview	Multi-WAN ^								
₩	Monitoring	Load Balancing	Custom Operator				Add Import	Export En	able Disable	Delete
ţĊjł	System Setup	Protocol	Interface $\checkmark$	Load Mode	Operator	Load Ratio	Remarks	Status	Actions	
	Network	Port Forward				No Da	ata			
†∔†	Flow Control	Domain Name								
۲	Access Controller	Upload/Download								
<u>&amp;</u> =	Authentication	Smart Flow Control								
⇆	Behavior	IP/MAC Limiters 🛛 🗸								
臣	Firewall	Protocol Library 🛛 🗸								
Ţ	Advanced application									
00	Services									
ſð	Log									

## Fig 4.1.1 Default Multi-WAN Load Balancing Settings page



	CMD-COS-v1.01									්	û	¢		English
	<u></u> _<	Flow Control <	Flow Control	> Multi-WAN > Load Bala	ncing				∎ <b>□</b> ≣ CPU: 0.74%	<b>MEM:</b> 17%	↑ тх:	1.53 KB/s	↓ RX	(: 5.86 KB/s
9	System Overview	Multi-WAN ^	Add											×
₽	Monitoring	Load Balancing												
ţĊ	System Setup	Protocol		Load Mode:	source IP +	destination IP	+ destination port	$\sim$	[	_				
	Network	Port Forward		Operator:	All			$\sim$	Custom Operator					
tit	Flow Control	Domain Name		Remarks:										
<b></b>	Access Controller	Upload/Download		Load Ratio:	Number 1	Interface wan1	Load Ratio	Status Disable	Actions Open					
<u>ළ</u> =	Authentication	Smart Flow Control			2	wan3		Disable	Open					
⇒	Behavior	IP/MAC Limiters 🗸 🗸												
Ħ	Firewall	Protocol Library 🗸 🗸			Save	Can	cel							
Ţ	Advanced application													
0%	Services													
ĥ	Log													

# Fig 4.1.2 Add Multi-WAN Load Balancing Settings page

	CMD-COS-v1.01			5	企	۵	2	English
	=,	Flow Control <	Flow Control > Multi-WAN > Load Balancing	1: 16%	ר ↑	(: 0.00 B	/s ↓	RX: 0.00 B/s
-			Custom Operator					×
6)	Overview	Multi-WAN ^						
₩	Monitoring	Load Balancing				Add		Delete
ţĊ	System Setup	Protocol	Custom Name Time Remarks Actions					
品	Network	Port Forward	No Data					
ţţţ	Flow Control	Domain Name						
<b>(</b>	Access Controller	Upload/Download	Help: If you have more than 5000 destination address, you can add a duplicate name multiple times, add up to 5000 pieces at mo	ist eac	n time			
<u>&amp;=</u>	Authentication	Smart Flow Control						
₩	Behavior	IP/MAC Limiters $~~$						
臣	Firewall	Protocol Library 🗸 🗸						
Ţ	Advanced application							
0% 00	Services							
ĥ	Log							

# Fig 4.1.3 Default Custom operator page

					4	6 4 2	E	
	<u></u> ≺	Flow Control <	Flow Control > Multi-WAN > Load	d Balancing	🛱 CPU: 0.74% 🔛 MEM:	16% ↑ TX: 0.00 B/s ↓ R	xx	
€) s	System Overview		Custom Operator AddCustom Operator		×			
- <u>//</u>								
ېژې s			Operator Name:					
	Network		Dst.Address List:					
	Access Controller							
<u>ଛ</u> = ⊿	Authentication	Smart Flow Control	Remarks:					
Ś⇒ B	Behavior							
F				Save Cancel				
	Advanced application							
0% S								
Γbι								

Fig 4.1.4 Add Custom operator page

	CMD-COS-v1.01								
		Flow Control <	Flow Control > Multi-WAN	> Load Balancing	≡Щ"≡ CPU: 0.50%	EMEM: 17%	↑ TX: 9	90.00 B/s 🤳	RX: 8.64 KB/
	System Overview	Multi-WAN ^	Cus AddCustom Oper	ator	×				×
~~		Load Balancing							
ţ		Protocol	Operator Name	Airtel1					
	Network	Port Forward	Dst.Address List	192.168.20.0/24					
		Domain Name							
<b></b>	Access Controller	Upload/Download							
<u>&amp;</u> =	Authentication	Smart Flow Control	Remarks:	Airtel LAN	]				
⇔	Behavior	IP/MAC Limiters $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$							
	Firewall	Protocol Library $~~ \lor~~$		Save					
V	Advanced application								
0%									
ſð	Log								

Fig 4.1.5 Setting Custom operator page

	CMD-COS-v1.01									්	습	۵	<u> </u>	ingl
	≡<	Flow Control <	Flow Control	> Multi-WAN > Load Balanc	ing				≣ <mark>0</mark> ≣ CPU: 9.75% □	MEM: 17%	↑ TX: 13.	88 KB/s	↓ RX: 21	1.18
$\mathfrak{S}$	System Overview	Multi-WAN ^	Add											
₽2	Monitoring	Load Balancing												
ţĊţ	System Setup	Protocol		Load Mode:	source IP +	destination IP +	destination port	$\sim$						
÷	Network	Port Forward		Operator:	All			~	Custom Operator					
tit	Flow Control	Domain Name		Kemarks:										
۲	Access Controller	Upload/Download		Load Ratio:	Number	Interface	Load Ratio	Status	Actions					
&= ;;	Authentication	Smart Flow Control				warri		C	Close					
¢	Behavior	IP/MAC Limiters 🛛 🗸			2	wans	2 ~	Enable	Close					
Ħ	Firewall	Protocol Library 🗸 🗸			Save	Cance	əl							
Ţ	Advanced application													
0%	Services													
ß	Log													

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

	CMD-COS-v1.01					් ර ද ප	English
	=<	Flow Control <	Flow Control > Multi-WAN > Load Balan	icing	≡ <b>⊑</b> ≡ CPU: 15.75%	☐ MEM: 17% ↑ TX: 48.41 KB/s ↓	RX: 459.30 KB/s
~			Custom Operator				×
6-3	Overview	Multi-WAN ^					
₩	Monitoring	Load Balancing				Add	Delete
ŝ	System Setup	Protocol	Custom Name	Time	Remarks	Actions	
品	Network	Port Forward	Airtel1	2021-02-10 20:59:06	Airtel LAN	Edit Export Delete	
ţţţ	Flow Control	Domain Name	SSVLAN	2021-03-16 21:19:28	SSV LAN	Edit Export Delete	
<b></b>	Access Controller	Upload/Download	Showing 1-2 of 2 records		PerPage 20 $\checkmark$ Row	s « < 1 > » 1 /1	IPages Jump
<u>&amp;=</u>	Authentication	Smart Flow Control	Help: If you have more than 50	000 destination address, you can add a dup	licate name multiple times, add up to 5000	pieces at most each time	
₩	Behavior	IP/MAC Limiters 🗸 🗸					
⊞	Firewall	Protocol Library 🛛 🗸					
Ţ	Advanced application						
0% 00	Services						
ſð	Log						

### 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

	CMD-CO5-v1.01								۵	û ¢ ≥	English
	=<	Flow Control	Flow Control > M	ulti-WAN > Protocol				: CPU: (	0.25% 🛄 MEM: 169	6 ↑ TX: 0.00 B/s 🗸	RX: 0.00 B/s
			Multi-WAN Pro	otocol Control Sett	tings						
Ð	System Overview	Multi-WAN ^									
₩	Monitoring	Load Balancing	Turn On Enha	nced Flow Control (C	Only for multi-line env	vironments, opening	can greatly improve the	protocol flow cont	rol effect)		2.1.
ŝ	System Setup	Protocol					Add	Import	Export Enabl	e Disable	Delete
品	Network	Port Forward	Interface ∨	Protocol	Src.Addr	Week	Time	Remarks	Status	Actions	
ţţţ	Flow Control	Domain Name					No Data				
<b></b>	Access Controller	Upload/Download									
<u>&amp;</u> =	Authentication	Smart Flow Control									
₩	Behavior	IP/MAC Limiters $$									
田	Firewall	Protocol Library 🛛 🗸									
Ţ	Advanced application										
0% 00	Services										
ľð	Log										

# Fig 4.1.8 Default Multi-WAN Protocol Control Settings page

2	CMD-COS-v1.01					
	≡<	Flow Control	Flow Control > Multi-V	VAN > Protocol		
ଚ	System Overview	Multi-WAN ^				
₩	Monitoring	Load Balancing		Interface:	· · ·	
¢	System Setup	Protocol		Load mode:	Number of new connections $\checkmark$	
品	Network	Port Forward	Protocol			
<u>†∔†</u>	Flow Control	Domain Name			Protocol Q	
9	Access Controller	Upload/Download			HttpProtocol	
<u>8</u> -	Authentication	Smart Flow Control			NetDownload     FileTransfer     NetCommunication	
₩	Behavior	IP/MAC Limiters 🗸 🗸			NetVideoStreaming     OnlineGame     CommonProtocol	
臣	Firewall	Protocol Library 🗸 🗸			CotherApp     SpeedTool	
J	Advanced application				~	
00	Services					
ъ	Log		Src.Addr			
				IP:		^
					A state of the	
					No Group Add Group	
					¥	$\lor$
				Remarks:		
				Week:	🗸 All 🗹 Monday 🗸 Tuesday 📝 Wednesday 🗹 Thursday 📝 Friday 📝 Saturday 🏹 Sunday	
				Time:	00:00-23:59 *	
					Save Cancel	

Fig 4.1.9 Add Multi-WAN Protocol Control Settings page

	CMD-COS-v1.01						
	≡	Flow Control <	Flow Control > Multi-V	VAN > Protocol			
6	System	Multi-WAN	Add				
	Overview						
ĿМ	Monitoring	Load Balancing		Interface:	wan1		
ţ,	System Setup	Protocol		Load mode:	Source ID + Dectination ID	~	
몵	Network	Port Forward		Lood mode.	Source In + Destination In		
141	Flow Control	Domain Name	Protocol				
	Access Controller	Upload/Download			Protocol Q		
<u>8</u> =	Authentication	Smart Flow Control			ALL		NetDownload FileTransfer
₩	Behavior	IP/MAC Limiters 🗸 🗸			NetCommunication     NetVideoStreaming     OnlineGame	Join>>	
臣	Firewall	Protocol Library 🗸 🗸			CommonProtocol     OtherApp     SpeedTool	< <remove< th=""><th></th></remove<>	
Ţ	Advanced application				spectron		
0 <b>%</b> 00	Services						
ዋ	Log						
			Src.Addr				
				IP:	Use "-" for IP range		COMMANDO
					Add Group Refresh	Join>>	
						< <remove< th=""><th></th></remove<>	
				Remarks:	COMMANDO		
				Week:	🗸 All 🗹 Monday 🗹 Tuesday ✔ Wednesda	ay 🔽 Thursday 🚦	🖌 Friday 🔽 Saturday 🔽 Sunday

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

	смр-соs- <u>v1.01</u>								<u> </u>	6 4 <u>8</u>	English
	=<	Flow Control <	Flow Control > Mult	i-WAN > Protocol				ې: CPU: 0	0.00% 🛄 MEM: 18%	↑ TX: 3.11 KB/s 👃 RX:	52.80 KB/s
~	System		Multi-WAN Proto	col Control Settings							
69	Overview	Multi-WAN ^									
₩	Monitoring	Load Balancing	Turn On Enhance	ed Flow Control (Only for	multi-line environment	s, opening can greatly i	mprove the protocol flow	control effect)			
ŝ	System Setup							Add Import	Export	e Disable I	Delete
品	Network	Port Forward	Interface ∨	Protocol	Src.Addr	Week	Time	Remarks	Status	Actions	
	Flow Control	Damain Mana	wan1	FileTransfer	COMMANDO	1234567	00:00-23:59	COMMANDO	Enabled	Delete	
IIII	Flow Control	Domain Name									
<b></b>	Access Controller	Upload/Download	Showing 1 of 1 reco	ords				PerPage 20 🗸	Rows 《 < 1	> >> 1 /1Page	5 Jump
8"	Authentication	Smart Flow Control									
₩	Behavior	IP/MAC Limiters $\sim$									
臣	Firewall	Protocol Library 🗸 🗸									
Ţ	Advanced application										
0%	Services										
ռ	Log										

## 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

	CMD-COS-v1.01										්	Û	¢ 2	English
	≡<	Flow Control <	Flow Control >	Multi-WAN	> Port Forwar	ď				©: CPU: 24	.00% 🛄 MEM:	16% ↑ T.	X: 0.00 B/s ↓	RX: 0.00 B/s
~	System		Multi-WAN	Port Forwar	ding Setting	gs								
(~)	Overview	Multi-WAN ^						_						
₩	Monitoring	Load Balancing		P/Comm Q				4	Add I	mport	Export Er	able	Disable	Delete
ţĊţ	System Setup	Protocol	Split mode	Interface $\checkmark$	Protocol	Src.Addr ∨	Dst.Addr ∨ Src.Port	Dst.Port	Week	Time	Remarks	Status	Actions	
品	Network	Port Forward						No Data						
ţţţ	Flow Control	Domain Name												
<b></b>	Access Controller	Upload/Download												
<u>&amp;</u> "	Authentication	Smart Flow Control												
₩	Behavior	IP/MAC Limiters 🗸 🗸												
Ħ	Firewall	Protocol Library $\sim$												
Ţ	Advanced application													
0 % 00	Services													
ľð	Log													

Fig 4.1.12 Default Multi-WAN Port Forwarding Settings page

	CMD-COS-v1.01						්	û ↓	<u> </u>
	=<	Flow Control <	Flow Control	> Multi-WAN > Port Forwar	d	CPU: 1.24%	EMEM: 16%	↑ TX: 0.00	B/s 🤳 RX: 0.00 B/s
	_		Add						×
Ð	System Overview	Multi-WAN ^							
₽	Monitoring	Load Balancing							
ţĊţ	System Setup	Protocol		Split mode:	External network line 🗸				
品	Network	Port Forward		Interface:					
†∔†	Flow Control	Domain Name			Line Bind (Prohibit switching to other lines after the line is discor	nnected)			
	Access Controller	Upload/Download		Load mode:	Number of new connections				
8 <u>=</u>	Authentication	Smart Flow Control		Protocol:	any				
⇆	Behavior	IP/MAC Limiters 🗸 🗸	Src.Addr						
Ħ	Firewall	Protocol Library 🛛 🗸		IP:	Use *-* for IP range			^	
Ţ	Advanced application				Join>>				
0%	Services				No Group Add Group Once configured, please Refresh				
ß	Log								
					· · · · · · · · ·			Ψ	

	CMD-COS-v1.01			් 🗘 🗘 English
	≡<	Flow Control <	Flow Control > Multi-WAN > Port Forwa	rd =☐= CPU: 0.25%  ☐ MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System Overview	Multi-WAN ^	Dst.Addr	
₩	Monitoring	Load Balancing	IP:	Use "-" for IP range
ţĈ	System Setup	Protocol		∧ Join>>
뷺	Network	Port Forward		No Group Add Group < <remove< th=""></remove<>
ţţţ	Flow Control	Domain Name		Once configured, please <b>Refresh</b>
<b></b>	Access Controller	Upload/Download		v
&= ;;	Authentication	Smart Flow Control	Src.Port:	
₩	Behavior	IP/MAC Limiters $~~$	Dst.Port:	
Ħ	Firewall	Protocol Library 🗸 🗸	Remarks:	
Ţ	Advanced application		Week:	🗹 All 🗹 Monday 🗹 Tuesday 🗹 Wednesday 🚺 Thursday 🛃 Friday 🚺 Saturday 🚺 Sunday
0% 00	Services		Time:	00:00-23:59 *
ß	Log			Save Cancel

Fig 4.1.13 Add Multi-WAN Port Forwarding Settings page

	CMD-COS-v1.01								ධ			English
	=<	Flow Control <	Flow Control >	Multi-WAN > Port Forward				📮 CPU: 8.75%	M: 18%	TX: 1.50	KB/s 🤳	RX: 24.21 KB/s
	System		Add									×
6-3	Overview	Multi-WAN ^										
<u>-</u>	Monitoring	Load Balancing										
ŝ	System Setup	Protocol		Split mode:	External network line	$\sim$						
	N			Interface:	wan1	*						
663	Network	Port Forward			Line Bind (Prohibit switching to other lines and the second se	fter the line is dis	sconnected)					
<u>t</u> ‡ŧ	Flow Control	Domain Name		Load mode:	Source IP + Destination IP + Destination Port	~						
<b>P</b>	Access Controller	Upload/Download		Loud mode.	· · · · · · · · · · · · · · · · · · ·							
8"	Authentication	Smart Flow		Protocol:	tcp+udp	$\sim$						
· · ·		Control	Cue Andala									
⇒>	Behavior	IP/MAC Limiters 🗸	Src.Addr	10.	11 1 1 1 1 m		COMMANDO					
臣	Firewall	Protocol Library $\sim$		IP.	Use tor IP range		Communitie					
Ţ	Advanced				Add Group Refresh COMMANDOMAC	Join>>						
<u>п</u> е,	application					< <remove< th=""><th></th><th></th><th></th><th></th><th></th><th></th></remove<>						
ōó	Services											
Ъ	Log											

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

	CMD-COS-v1.01			스) 슈 추 온 English
	=<	Flow Control <	Flow Control > Multi-WAN > Port Forward	± CPU: 22.00% 🛄 MEM: 18% ↑ TX: 55.00 B/s ↓ RX: 27.00 B/s
	-		Multi-WAN Port Forwarding Settings	
69	Overview	Multi-WAN ^		
₩	Monitoring	Load Balancing	Please input IP/Comm Q	d Import Export Enable Disable Delete
ţ	System Setup	Protocol	Split mode Interface -> Protocol Src.Addr -> Dst.Addr -> Src.Port Dst.Port Week	Time Remarks Status Actions 🗌
品	Network	Port Forward	External wan1 tcp+udp COMMANDO COMMANDOMAC 1234567	Correct Copy Enabled Disable Delete
t††	Flow Control	Domain Name		
•	Access Controller	Upload/Download	Showing 1 of 1 records	PerPage 20 V Rows 《 < 1 > 》 1 /1Pages Jump
8.	Authentication	Smart Flow Control		
₩	Behavior	IP/MAC Limiters $\sim$		
臣	Firewall	Protocol Library $\sim$		
Ţ	Advanced application			
0% 00	Services			
Ъ	Log			

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

	CMD-COS-v1.01								<b>්</b> 1	<u>م</u> ۵	Engli
	=<	Flow Control <	Flow Control > Mu	ilti-WAN > Domain Na	ame			" CPU: 7.	25% 🛄 MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00
~	System		Multi-WAN Dor	nain Name Control	Settings						
(~)	Overview	Multi-WAN ^									
₩	Monitoring	Load Balancing					Add	Import	Export Enable	Disable	Delete
ţĊ	System Setup	Protocol	Interface $\vee$	Domain Name	Src Addr	Week	Time	Remarks	Status	Actions	
₼	Network	Port Forward					No Data				
†∔†	Flow Control	Domain Name									
۲	Access Controller	Upload/Download	Help hint: Th	is feature only support	ts splitting domain i	names					
<u>8</u> "	Authentication	Smart Flow Control									
₩	Behavior	IP/MAC Limiters $~~$									
臣	Firewall	Protocol Library 🛛 🗸									
Ţ	Advanced application										
0%	Services										
ľð	Log										

Fig 4.1.16 Default Multi-WAN Domain Name Control Settings page

	CMD-COS-v1.01				
	≡<	Flow Control <	Flow Control > Mu	ulti-WAN > Domain Name	
ଚ	System Overview	Multi-WAN ^			
~~	Monitoring	Load Balancing		Interface:	*
ţÇ	System Setup	Protocol	Domain Name		
品	Network	Port Forward			*
tłt	Flow Control	Domain Name			
۲	Access Controller	Upload/Download			
8= ::	Authentication	Smart Flow Control			
⇔	Behavior	IP/MAC Limiters 🗸 🗸	Src.Addr	ID-	Like 1.4 for IP range
臣	Firewall	Protocol Library 🗸 🗸			
Ţ	Advanced application				Join>>
	Services				Once configured, please Refresh
Ъ	Log				· · · · ·
				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

00000	CMD-COS-v1.01							스) 🏠 🗘 Engli	ish
	=,	Flow Control <	Flow Control >	Multi-WAN > Domain Name			📋 CPU: 6.93%	🖵 MEM: 18% ↑ TX: 27.00 B/s 🤳 RX: 0.0	)0 B/s
	-		Add						×
63	Overview	Multi-WAN ^							
<u>-</u>	Monitoring	Load Balancing							
ţĊţ	System Setup	Protocol		Interface:	wan1,pptpCOMMANDO,I2tpCOMMANDO,ovp	* AMMOOn			
墨	Network	Port Forward	Demain Mana						
			Domain Name						
111	Flow Control	Domain Name			www.commandonetworks.com				
<b>?</b>	Access Controller	Upload/Download							
<u>&amp;</u> ".	Authentication	Smart Flow Control							
⇔	Behavior	IP/MAC Limiters $$							
臣	Firewall	Protocol Library $\sim$	Src.Addr				192 168 1 0/24		
	Advanced			IP:	Use "-" for IP range		COMMANDO		
 &	application				COMMANDOMAC	Join>>			
õõ	Services					< <remove< th=""><th></th><th></th><th></th></remove<>			
Ъ	Log								

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

	CMD-COS-v1.01							ධ	습 🗘 🔔 English
	=<	Flow Control <	Flow Control > Multi-W	AN > Domain Name				📫 CPU: 1.50% 🛄 MEM: 18% ↑	° TX: 5.81 KB/s ↓ RX: 160.92 KB/s
			Multi-WAN Domain	Name Control Setting	gs				
e	System Overview	Multi-WAN ^							
<u>-</u>	Monitoring	Load Balancing						Add Import Export Enabl	e Disable Delete
ŝ	System Setup	Protocol	Interface $\checkmark$	Domain Name	Src Addr	Week	Time	Remarks Status	Actions
品	Network	Port Forward	wan1,pptpCOMMAN DO,l2tpCOMMANDO, ovpnCOMMANDO	www.commandonetw orks.com	192.168.1.0/24 COMMANDO	1234567	00:00-23:59	COMMANDO Domain Enabled	Edit Copy Disable Delete
<b>†</b> #†	Flow Control	Domain Name							
•	Access Controller	Upload/Download	Showing 1 of 1 records					PerPage 20 🗸 Rows « < 1	> >> 1 /1Pages Jump
<u>&amp;"</u>	Authentication	Smart Flow Control	Help hint: This feat	ture only supports splittir	ng domain names				
⇒	Behavior	IP/MAC Limiters $$							
田	Firewall	Protocol Library 🗸 🗸							
Ţ	Advanced application								
0% 00	Services								
ሌ	Log								

## 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

	CMD-CO5-v1.01									් ර	¢	<u> </u>	nglish
	=,	Flow Control <	Flow Contro	ol > Multi-WAN > Upload/Download				= <b></b> = (	CPU: 0.25% 🛄	MEM: 16% 1	TX: 0.00 B/	s ↓ RX:	0.00 B/s
			Multi-WA	N Upload and Download Contro	l Settings								
$\mathbb{C}$	System Overview	Multi-WAN ^											
₩	Monitoring	Load Balancing					Add	Import	Export	Enable	Disable	De	elete
ţĊţ	System Setup	Protocol	Protocol	Out.Interface $\checkmark$ In.Interface $\checkmark$	Src.Addr ∨	Dst.Addr $\vee$	Src.Port	Dst.Port	Remarks	Status	Action	s	
츎	Network	Port Forward					No Data						
ţ†	Flow Control	Domain Name			1 1. 19							10 1.1	
<b>P</b>	Access Controller	Upload/Download	Help:	<ol> <li>Implement upload traffic and do upstream traffic request data will</li> <li>2.For other line configurations (de</li> </ol>	ownload traffic or return according efault gateway, m	separated transr to the download ulti-line load, and	nission, only after line specified by th offload settings),	the upload traff ne rule. (The rati there is actually	o for the multiple no functional pr	olicy rule, the c e lines is 1:1) iority associatio	ownstream	ion belon	ne qs to
<u>&amp;=</u>	Authentication	Smart Flow Control		the <i>"effective</i> policy after matchi of use.	ng" . This functio	on takes effect onl	ly after matching t	he upload data	rule. And the prio	ority is the high	nest accordin	g to the ef	ffect
₩	Behavior	IP/MAC Limiters 🛛 🗸											
臣	Firewall	Protocol Library 🛛 🗸											
Ţ	Advanced application												
0%	Services												
ſð	Log												

# Fig 4.1.20 Multi-WAN Upload and Download Control Settings page

2	2					
		Flow Control	Flow Control > Multi-	WAN > Upload/Download		
ଚ	System Overview	Multi-WAN ^		Protocol:	any ~	
₩	Monitoring	Load Balancing		Out.Interface:	•	
<i>‡</i> ‡	System Setup	Protocol		In.Interface:	·	
몲	Network	Port Forward				
1++	Flow Control	Domain Name	Src.Addr	IP:		~
9	Access Controller	Upload/Download			loins 2	
<u>a</u> =]	Authentication	Smart Flow Control			No Group Add Group	
₩	Behavior	IP/MAC Limiters 🗸 🗸			Once configured, please Refresh	
臣	Firewall	Protocol Library $\sim$			~	~
g	Advanced application					
0 <b>%</b>	Services		Dst.Addr			
ъ	Log			IP:		$\sim$
					< <niol< th=""><th></th></niol<>	
					No Group Add Group Once configured, please Refresh	
					~	$\vee$
				Src.Port:		
				Dst.Port:		
				Remarks:		
					Save Cancel	

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

	OMD-COS-v1.01						
	≡	Flow Control <	Flow Control > Multi-W	/AN > Upload/Download			
6	System	Multi-WAN A		Protocol:	tcp+udp	$\sim$	
	Overview	Load Palandan		Out.Interface:	wan1	*	
- 20	Monitoring	Load Balancing		In.Interface:	wan1	*	
÷,	System Setup	Protocol					
몲	Network	Port Forward	Src.Addr				COMMUNICO
111	Flow Control	Domain Name		IP:	Use "-" for IP range		COMMANDO
	Access Controller	Upload/Download			Add Group Refresh COMMANDOMAC	Join>>	
<u>8</u> =	Authentication	Smart Flow Control				< <remove< th=""><th></th></remove<>	
₩	Behavior	IP/MAC Limiters 🗸 🗸					
臣	Firewall	Protocol Library 🗸					
5	Advanced application						
	Services		Dst.Addr	IP:	Use "-" for IP range		COMMANDOMAC
ቡ	Log				Add Group Refresh		
					COMMANDO	Join>>	
						< <remove< th=""><th></th></remove<>	
				Src.Port:			
				Dst.Port:			
				Remarks:	COMMANDO Upload		
					Save Cancel		

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

CENTRE											<b>〇 ①</b>	¢ 2	English
	=<	Flow Control <	Flow Control	> Multi-WAN > U	oload/Download				≡ <b>□</b> ≣ CPU: (	0.75% 🛄 MEN	: 18% ↑ TX: 1	41.00 B/s ↓ RX	: 142.00 B/s
6	System	Multi-MAN	Multi-WAN	Upload and Do	wnload Control	l Settings							
(-)	Overview							A	dd Import	Export	Enable	Disable	Delete
~~	wonitoring	Load Balancing	<b>D</b> • 1	o.u (			<b>B 1 1 1 1 1</b>						
ţÇ	System Setup	Protocol	Protocol	OutInterface	✓ In.Interface ✓	Src.Addr 🗸	Dst.Addr ∨	Src.Port	Dst.Port	Kemarks	Status	Actions	
뮮	Network	Port Forward	tcp+udp	wan1	wan1	COMMANDO	COMMANDO	MAC		COMMANDO Upload	Enabled	Edit Disable Delete	
ţţţ	Flow Control	Domain Name	Showing 1 o	f 1 records					PerPage 20	✓ Rows ≪	< 1 > >	> 1 /1Pag	es Jump
<b>P</b>	Access Controller	Upload/Download											
<u>&amp;=</u>	Authentication	Smart Flow Control	Help:	1.Implement up upstream traffic	oad traffic and do request data will r	wnload traffic on return according f	separated transr to the download	nission, only aft line specified by	ter the upload traffi y the rule. (The ratio	c matches the po o for the multiple	olicy rule, the dov lines is 1:1)	white the traffic of	of the
$\downarrow$	Behavior	IP/MAC Limiters 🗸 🗸		the "effective p of use.	olicy after matching	ng" . This functio	n takes effect onl	y after matchin	g the upload data r	ule. And the price	ority is the highes	according to th	e effect
Ħ	Firewall	Protocol Library 🔍											
Ţ	Advanced application												
0% 00	Services												
ſð	Log												

# 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 I of I ine (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

	CMD-COS-v1.01		ත් රු 👃 🛆 English
	=<	Flow Control <	Flow Control > Smart Flow Control
<i>—</i>	Sustem		Smart Flow Control Settings
6-)	Overview	Multi-WAN 🗸	
<u>-</u>	Monitoring	Smart Flow Control	Flow control state : Off
ţĊţ	System Setup	IP/MAC Limiters 🗸 🗸	Flow setting :      O Close the flow control      Smart mode      Manual mode      Click effective
뷺	Network	Protocol Library 🛛 🗸	
tit	Flow Control		Help Cauti <b>Ens</b> bling 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 configurations encompanded
<b></b>	Access Controller		<ul> <li>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;</li> </ul>
<u>ද</u>	Authentication		* Opening this feature will increase the performance overhead of some routers.
\$J	Behavior		
Ħ	Firewall		
y	Advanced application		
00	Services		
ſ	Log		

## Fig 4.2.1 Default Flow Control Settings page

	CMD-COS-v1.01						් රු 🗘 ළ Engli
	_<	Flow Control <	Flow Control > Smart Flo	w Control		∎ CPU: 3.47%	) MEM: 16% ↑ TX: 0.00 B/s 👃 RX: 0.0
	_		Smart Flow Control S	ettings			
6	System Overview	Multi-WAN 🗸 🗸					
₩	Monitoring	Smart Flow Control	Flow control state :	Off			
ţĊ	System Setup	IP/MAC Limiters 🛛 🗸	Flow setting :	Close the flow control	Smart mode O Manual mode	Click effective	
品	Network	Protocol Library 🗸 🗸	Priority control :	gamePriority 🗸 Priorit	y to ensure the game speed, suitable for I	nternet cafes, mobile game bar and	game players
†∔†	Flow Control						
<b></b>	Access Controller		flowPort ^				addAll Invalid All
<u>8</u> =	Authentication		interface	upload	download	State	Actions
₩	Behavior		wan1	0	0	Not joined	Join strategy Edit
Ħ	Firewall		wan2	0	0	Not joined	Join strategy Edit
,	Advanced application						
0% 00	Services		speedLimit ^				
լ	Log		The independent speed	can further control the specified	is peed and priority terminal, usually for the	he speed limit of the servers. Add	Enable Disable Delete
			ip_addr∨ up	load 🗸 🛛 download 🗸	prio ∽ time	Remarks Status	s 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.

	CMD-COS-v1.01							ථ	☆ ↓	2	English
	=<	Flow Control <	Flow Control > Smart Flo	ow Control			=Щ= CPU: 75.99% 🛄 M	IEM: 18%	↑ TX: 27.00	B/s ↓	RX: 73.00 B/s
			Smart Flow Control S	ettings							
6)	Overview	Multi-WAN 🗸									
₽2	Monitoring	Smart Flow Control	Flow control state :	<b>On</b> Only the active line will c	ontrol the flow accordi	ng to the priority of the a	agreement				
ţĊł	System Setup	IP/MAC Limiters $~~$	Flow setting :	O Close the flow control	Smart mode	O Manual mode	Click effective				
뷺	Network	Protocol Library 🛛 🗸	Priority control :	gamePriority V Prior	ity to ensure the game	speed, suitable for Interr	net cafes, mobile game bar and	game pla	yers		
tit	Flow Control										
<b>R</b>	Access Controller		flowPort ^								
<u>8</u> =	Authentication								addAll	Inv	alid All
4			interface	upload	downl	oad	State		Actions		
$\rightarrow$	Behavior										
Ħ	Firewall					No Data					
Ţ	Advanced application										
0%	Services		speedLimit ^								
ß	Log		The independent speed	can further control the specifie	eds peed and priority te	rminal, usually for the sp	eed limit of the servers.	Enable	Disab	le	Delete

Fig 4.2.3 Default game Priority in Smart Flow Control Settings page

2	CMD-COS-v1.01				
	=,	Flow Control	Flow Control > Smart Flow Control		
		now control	Name:	•	
0	System Overview	Multi-WAN 🗸 🗸	Interface:		
22	Monitoring	Smart Flow Control	Ann Broto i		
	ê		App Proto:	Protocol	
843 1	System Setup	IP/MAC Limiters V		ALL A	
몲	Network	Protocol Library $\sim$		End Section 2      End Sect	
141	Flow Control			NetCommunication     NetVideoStreaming	
ø	Access			CommonProtocol	
	Controller			CtherApp     SpeedTool	
<u>a</u> =	Authentication			> ■ UnknownApp > ■ SmallPacket ✓	
₩	Behavior		Prio :	0 (highest) $\checkmark$	
臣	Firewall		Ip Addr:	Use "-" for IP range	~
J	Advanced				
03	Consisos				
00	Services			Once configured, please Refresh	
Ъ	Log				
				×	Y.
			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

	CMD-COS-v1.01							۵	<u> </u>		English
	=<	Flow Control	Flow Control > Smart Flow Control				: CPU: 0.25%	MEM: 18%	↑ TX: 60.0	0 B/s 🤳	RX: 60.00 B/s
			ip_addr:	Use "-" for IP range			192.168.0.0/24				
Ð	System Overview	Multi-WAN 🗸 🗸		Add Group	Refresh						
<u>-</u>	Monitoring	Smart Flow Control		COMMANDO COMMANDOMAC		< <remove< th=""><th></th><th></th><th></th><th></th><th></th></remove<>					
ţ	System Setup	IP/MAC Limiters $$									
器	Network	Protocol Library $$									
tŧt	Flow Control		upload:	10000	KB /c						
R	Access		upload.	10000	KD/S						
	Controller		download:	10000	KB/s						
8.	Authentication		prio:	5	$\sim$						
₩	Behavior		time:	00:00-23:59							
臣	Firewall		Remarks:	COMMANDO							
Ţ	Advanced application										
0% 00	Services			Save Can	cel						
ß	Log		Help Cauti <b>Ena</b> bling flow control can optim • Intelligent mode: simple and fa configuration, recommended ; • Manual mode: users with a de * Opening this feature will increa	ize the bandwidth and impro ast intelligent flow control m ep understanding of the con ase the performance overhe:	ove the network expe node, suitable for the nvective control functi ad of some routers.	rience of import vast majority of on and their ow	tant applications, especially in the bandwidth en network environment, official comprehensive clu n network environment are relatively complex a	vironment oud big data o nd support m	optimization ore customi:	flow conti zation opti	rol ons;

### Fig 4.2.5 Changing Smart Flow Control Settings page

	CMD-COS-v1.01								۵	☆ ♪ ዶ	English
	=<	Flow Control	Flow Control > Smart Fl	ow Control				CPU:	0.74% 🛄 MEM: 18%	↑ TX: 81.00 B/s 🔱	RX: 82.00 B/s
			Smart Flow Control	Settings							
6	Overview	Multi-WAN 🗸 🗸									
₩	Monitoring	Smart Flow Control	Flow control state :	<b>On</b> Only the active li	ne will control the flow a	ccording to the priority c	f the agreement				
ţĊ	System Setup	IP/MAC Limiters $$	Flow setting :	O Close the flow co	ontrol 💿 Smart mo	de 🔷 Manual mode	Click effective				
品	Network	Protocol Library 🗸 🗸	Priority control :	gamePriority 🗸	Priority to ensure the	game speed, suitable for	Internet cafes, mobile ga	ame bar and game playe	rs		
†∔†	Flow Control										
<b>P</b>	Access Controller		flowPort $\sim$								
8.	Authentication										
÷	Behavior		speedLimit ^								
	benavior		The independent spee	d can further control the	specifieds peed and pri	ority terminal, usually for	the speed limit of the ser	rvers.	Add Enable	Disable	Delete
臣	Firewall		ip_addr $\checkmark$	upload $\checkmark$	download $\vee$	prio 🗸	time	Remarks	Status	Actions	
Ţ	Advanced application		192.168.0.0/24	10000	10000	5	00:00-23:59	COMMANDO	Enabled	Edit Copy Disable Delete	
0%	Services										
R	Log		Showing 1 of 1 records	5				PerPage 20 🗸	Rows « < 1	> >> 1 /1Pag	ges Jump

## Fig 4.2.6 Smart Flow Control Settings page

### 4.3 IP/MAC Limiters

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

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

set.

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



## Fig 4.3.1 Default Speed Limiter Using IP Address page

	CMD-COS-v1.01			
	≡<	Flow Control	Flow Control > IP/MAC Limiters > IP Limiter	
9	System Overview	Multi-WAN 🗸		
₩	Monitoring	Smart Flow Control	Interface :	any
÷	System Setup	IP/MAC Limiters	IP:	Use *-* for IP range
品	Network	IP Limiter		COMMANDO
<b>†</b> ∔†	Flow Control	MAC Limiter		< <remove< th=""></remove<>
۲	Access Controller	Protocol Library 🗸		
&= ;;	Authentication		protocol:	
₩	Behavior		Src Dort:	any
田	Firewall		Dst Port	
g	Advanced application		Speed limit mode:	Independent sp 🗸
00	Services		upload:	0 KB/s
Ъ	Log		download:	0 KB/s
			week:	🗸 All 🗹 Monday 🟹 Tuesday 📝 Wednesday 📝 Thursday 📝 Friday 🟹 Saturday 📝 Sunday
			time:	00:00-23:59 =
			Remarks:	
				Save

#### × 🛆 🟠 🔔 English Flow Control > IP/MAC Limiters > IP Limiter Flow Control (-) System Overview Multi-WAN Interface: wan1 Smart Flow Control 192.168.0.10 ÷Ö IP/MAC Lin Add Group Ref w Control MAC Lim Access Controller protocol tcp+udp Src.Port: Dst.Port: Advanced application Speed limit m Independent sp. 🗸 pload: 1000 KB/s լի տայ 100 KB/s eek: 🗌 All 🔽 Monday 📝 Tuesday 📝 Wednesday 📝 Thursday 🏹 Friday 🗌 Saturday 🗌 Sunday time: 00:00-23:59 Remarks: Setting Speed limit Save Cancel

## Fig 4.3.2 Add Speed Limiter Using IP Address page

Fig 4.3.3 Speed Limiter for Particular IP Address Page

	CMD-COS-v1.01												۵	☆ ↓	2	English
	=<	Flow Control <	Flow Contro	ol > IP/MAC Limiters >	IP Limiter						CPU:	18.07%	MEM: 18%	↑ TX: 0.0	0 B/s 🤳 R)	(: 0.00 B/s
			Speed Lin	ed Limiter Using IP Addres												
Ð	System Overview	Multi-WAN 🗸							_							
₩	Monitoring	Smart Flow Control								Add	Import	Export	Enable	Disa	ble D	elete
ţĊţ	System Setup	IP/MAC Limiters 🔷	Interface `	∽ ip_addr ∽	protocol	SRC port	DST port	Speed limit ∽ mode	upload $\vee$	download	√week	time	Remarks	Status	Actions	
矗	Network	IP Limiter		100100010				Independ	1000	100	10045	00:00-	Setting		Edit	
ţ†	Flow Control	MAC Limiter	wan I	192.168.0.10	tcp+udp			ent speed limit	1000	100	12345	23:59	limit	Enabled	Disable Delete	
<b>P</b>	Access Controller	Protocol Library 🛛 🗸	Showing 1	of 1 records						PerPage	20 ~	Rows	« < 1	> >>	1 /1Pages	Jump
<u>&amp;</u> "	Authentication															
₩	Behavior															
Ħ	Firewall															
Ţ	Advanced application															
0% 00	Services															
Ŀ	Log															

## 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

	CMD-COS-v1.01							<u>م</u>	¢ گ	English
	=,	Flow Control <	Flow Control > IP/MAC Limiters > MA	C Limiter		ECPU: 9	0.65% 🛄 MEN	1:19% ↑ TX:	899.00 B/s 🔱	RX: 0.00 B/s
	_		Speed Limiter Using MAC Addre	ss						
(	System Overview	Multi-WAN 🗸 🗸								
₩	Monitoring	Smart Flow Control			Add	Import	Export	Enable	Disable	Delete
ŝ	System Setup	IP/MAC Limiters 🔿	Interface $\checkmark$ MAC $\checkmark$	Speed limit mode	download 🗸 week	time	Remarks	Status	Actions	
♣	Network	IP Limiter			No Data					
t+t	Flow Control	MAC Limiter								
<b></b>	Access Controller	Protocol Library 🗸 🗸								
<u>&amp;</u> =	Authentication									
⇆	Behavior									
臣	Firewall									
Ţ	Advanced application									
0% 00	Services									
ſð	Log									

Fig 4.3.5 Default Speed Limiter Using MAC Address page

	CMD-COS-v1.01				스) 슈 스 프 English
	≡<	Flow Control <	Flow Control > IP/MAC Limiters > MAC Lim	ter	to CPU: 1.70% 🛄 MEM: 19% ↑ TX: 439.00 B/s ↓ RX: 0.00 B/s
ଳ	System Overview	Multi-WAN 🗸 🗸	Interface:	any	
~~	Monitoring	Smart Flow Control	MAC:	Use ":" for delimiter	
ţĊ	System Setup	IP/MAC Limiters 🗠		Add Group Refresh	
品	Network	IP Limiter		< <remove app<="" th=""><th>olied to any MAC address if not specified</th></remove>	olied to any MAC address if not specified
t+t	Flow Control	MAC Limiter			
<b>.</b>	Access Controller	Protocol Library 🗸 🗸			
8.	Authentication		Speed limit mode:	Independent sp $$	
₩	Behavior		upload:	0 KB/s	
臣	Firewall		download:	0 КВ/з	
V	Advanced application		week:	🗹 All 🗹 Monday 🗹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Frid	ay 🗹 Saturday 🗹 Sunday
0% 00	Services		time:	00:00-23:59	
Ъ	Log		Remarks:		
				Save	

Fig 4.3.6 Add Speed Limiter Using MAC Address page

	CMD-COS-v1.01			තා රු 🗘 🚊 English
	≡<	Flow Control <	Flow Control > IP/MAC Limiters > MAC Lim	iter to CPU: 0.75% □ MEM: 19% ↑ TX: 312.00 B/s ↓ RX: 0.00 B/s
A	System Overview	Multi-WAN 🗸 🗸	Interface:	wan1
₩	Monitoring	Smart Flow Control	MAC:	Use ":" for delimiter COMMANDOMAC
ţĝ	System Setup	IP/MAC Limiters 🗠		Join>>
몲	Network	IP Limiter		No Group Add Group
<u>†∔†</u>	Flow Control	MAC Limiter		Unce conngureo, piease <b>xerresn</b>
P	Access Controller	Protocol Library $\sim$		
8"	Authentication		Speed limit mode:	Independent sp $\vee$
₩	Behavior		upload:	1000 KB/s
臣	Firewall		download:	10000 KB/s
Ţ	Advanced application		week:	🜠 All 💟 Monday 💟 Tuesday 💟 Wednesday 💟 Thursday 💟 Friday 💟 Saturday 💟 Sunday
0% 00	Services		time:	00:00-23:59 *
ሌ	Log		Remarks:	COMMANDO MAC Address Speed limit
				Save

## Fig 4.3.7 Speed Limiter For COMMANDOMAC Group MAC Address

	CMD-COS-v1.01										û	4 L	English
	=,	Flow Control <	Flow Control >	IP/MAC Limiters > MAG	C Limiter				≡ <b>□</b> = CPU: (	0.50% 🛄 MEM	:19% ↑ TX	: 175.00 B/s 🔱	RX: 0.00 B/s
	_		Speed Limite	r Using MAC Addres	s								
Ð	System Overview	Multi-WAN 🗸							_				
₩	Monitoring	Smart Flow Control						Add	Import	Export	Enable	Disable	Delete
ţĊ	System Setup	IP/MAC Limiters 🔷	Interface $\checkmark$	MAC $\checkmark$	Speed limit mode	upload $\checkmark$	download $\vee$	week	time	Remarks	Status	Actions	
₼	Network	IP Limiter	wan1	COMMANDOMAC	Independent speed limit	1000	10000	1234567	00:00-23:59	COMMANDO MAC Address Speed limit	Enabled	Edit Disable Delete	•
†∔†	Flow Control	MAC Limiter								opood mine			
<b></b>	Access Controller	Protocol Library 🗸 🗸	Showing 1 of	l records				PerF	Page 20 ∨	Rows			Jump
<u>&amp;</u> =	Authentication												
⇆	Behavior												
田	Firewall												
Ţ	Advanced application												
0% 00	Services												
Ŀ	Log												

### 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

	CMD-COS-v1.01										් ර	4 e	English
	=<	Flow Control <	Flow Control	> Protocol Library	v > Custom Protoco	əl			: <u></u>	CPU: 4.25%	MEM: 16% 1	` TX: 0.00 B/s 🚽	, RX: 0.00 B/s
	_		Customized	I Protocol									
Ð	System Overview	Multi-WAN 🗸											
₩	Monitoring	Smart Flow Control						Add	Import	Export	Enable	Disable	Delete
ւi	System Setup	IP/MAC Limiters 🗸 🗸	Class	Name 🗸	SRC addr ∨	DST addr $\checkmark$	protocol $\vee$	SRC port	DST port	Remarks	Status	Actions	
厵	Network	Protocol Library 🗠						No Data					
†ŧ†	Flow Control	Custom Protocol											
<b></b>	Access Controller	Advanced Custom Protocol											
<u>&amp;</u> =	Authentication												
⇔	Behavior												
Ħ	Firewall												
Ţ	Advanced application												
0%	Services												
ľð	Log												

Fig 4.4.1 Default Customized Protocol page

	CMD-COS-v1.01						☆ ↓ ▲ ☞	nglish
	=<	Flow Control <	Flow Control > Protocol Library > Custom	Protocol		📮: CPU: 2.97% 🔛 Mi	EM: 18% ↑ TX: 3.58 KB/s 🤳 RX: 57	.89 KB/s
			Add					×
A	Overview	Multi-WAN 🗸 🗸						
₩	Monitoring	Smart Flow Control						
ţĊj	System Setup	IP/MAC Limiters 🗸	Class:	CustomHttpProtocol	~			
			Name:	CustomNetDownload	*			
楍	Network	Protocol Library	SBC addr:	CustomFileTransfer CustomNetMessage				
<u>†</u> ‡†	Flow Control			CustomNetVideo				
a	Access	Advanced Custom		CustomCommonProtocol	>			
	Controller	Protocol		CustomOtherSoft CustomSpeedTool	ove			
<u>&amp;</u> ".	Authentication							
Ś	Behavior							
臣	Firewall		DST addr:	Lice "-" for ID range				
$\Box$	Advanced application		Dor Buur.					
0&	c			COMMANDO	Join>>			
00	Services				< <remove< th=""><th></th><th></th><th></th></remove<>			
Ъ	Log							

Fig 4.4.2 Add Customized Protocol page

	CMD-COS-v1.01						۵	6 A	🛆 English
	≡́	Flow Control 〈	Flow Control > Protocol Library > Custom Prot	iocol			😳 CPU: 0.75% 🛄 MEM: 18%	↑ TX: 6.55 KB/s	↓ RX: 135.14 KB/s
କ	System	Multi-WAN 🗸	Name:	FileCOMMANDO	*				
PM	Monitoring	Smart Flow	SRC addr:	Use "-" for IP range		192.168.0.0/24			
	System Setup	IP/MAC Limiters		Add Group Refresh COMMANDO	Join>>				
灵	Network	Protocol Library			< <remove< th=""><th></th><th></th><th></th><th></th></remove<>				
111	Flow Control	Custom Protocol							
	Access	Advanced Custom							
E	Controller	Protocol	DST addr:	Use *-* for IP range		192.168.1.0/24			
€	Behavior			Add Group Refresh COMMANDO	Join>>				
~> ₽	Firewall				< <remove< th=""><th></th><th></th><th></th><th></th></remove<>				
	Advanced								
 □&	application								
	services		protocol:	tcp+udp 🗸					
Ъ	Log		Src.Port:						
			Dst.Port:						
			Remarks:						
				Save Cancel					

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

	CMD-COS-v1.01										<u></u> ර	4 2	English
	=<	Flow Control <	Flow Control > F	vrotocol Library >	Custom Protoco	I			E CPU:	0.75% 🛄 Me	EM: 18% ↑ TX: 1	41.00 B/s 🤳 RX	3: 142.00 B/s
-			Customized P	rotocol									
<del>(</del> ~)	Overview	Multi-WAN 🗸 🗸											
₩	Monitoring	Smart Flow Control						Add	Import	Export	Enable	Disable	Delete
ţĊ	System Setup	IP/MAC Limiters 🗸 🗸	Class	Name 🗸	SRC addr $\checkmark$	DST addr $\checkmark$	protocol $\vee$	SRC port	DST port	Remarks	Status	Actions	
튧	Network	Protocol Library 🔿	CustomFileTra nsfer	FileCOMMAN DO	192.168.0.0/24	192.168.1.0/24	tcp+udp				Enabled	Edit Disable Delete	
†∔†	Flow Control	Custom Protocol	Showing 1 of 1	records				Pe	rPage 20	∨ Rows	« < <mark>1</mark> > >	> 1 /1Pag	es Jump
2	Access Controller	Advanced Custom Protocol											
<u>&amp;=</u>	Authentication												
₩	Behavior												
田	Firewall												
Ţ	Advanced application												
0% 00	Services												
ſð	Log												

### 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

	CMD-COS-v1.01						⊿ û ¢	A English
	=<	Flow Control	Flow Control > Protocol Library > Advanced Custom Protocol			"□" CPU: 0.74% □ N	IEM: 16% ↑ TX: 0.00	B/s ↓ RX: 0.00 B/s
	_		Advanced Custom Protocol Settings					
R	System Overview	Multi-WAN 🗸 🗸						
<u>-</u>	Monitoring	Smart Flow Control			Add Imp	ort Export	Enable Disabl	le Delete
ţĊ	System Setup	IP/MAC Limiters 🗸 🗸	class name	Remarks	Status		Actions	
品	Network	Protocol Library \land			No Data			
†∔†	Flow Control	Custom Protocol						
<b>P</b>	Access Controller	Advanced Custom Protocol						
<u>&amp;=</u>	Authentication							
⇒	Behavior							
臣	Firewall							
Ţ	Advanced application							
0% 00	Services							
ľð	Log							

Fig 4.4.5 Default Advanced Custom Protocol page



Fig 4.4.5 Add Advanced Custom Protocol page



## Fig 4.4.6 Advanced Custom Protocol setting for video page

	СМД-СО5-v1.01						<u> </u>	<u>e</u> English
	=<	Flow Control <	Flow Control > Protocol Libra	ary > Advanced Custom Protocol		따라 CPU: 18.56%	🖵 MEM: 18% ↑ TX: 3.74 KB/s	↓ RX: 66.77 KB/s
~			Advanced Custom Protoc	col Settings				
6.)	Overview	Multi-WAN 🗸 🗸						
₩	Monitoring	Smart Flow Control				Add Import Exp	ort Enable Disable	e Delete
ţĊţ	System Setup	IP/MAC Limiters $~~$	class	name	Remarks	Status	Actions	
- 	Network	Protocol Library 🔿	CustomNetVideo	COMMANDOVideo	COMMANDOVideo	Enabled	Edit Disable Delete	
ţţţ	Flow Control	Custom Protocol	Showing 1 of 1 records			PerPage 20 $\checkmark$ Rows	$\ll$ $\langle$ 1 $\rangle$ $\gg$ 1	/1Pages Jump
<b></b>	Access Controller	Advanced Custom Protocol						
<u>&amp;</u> =)	Authentication							
₩	Behavior							
臣	Firewall							
Ţ	Advanced application							
0%	Services							
Ŀ	Log							

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** 

	CMD-COS-v1.01			🛆 🖒 🌲 Englis
	=<	Access	Access Controller > Wireless overview	≝Ös CPU: 2.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00
		Controller	Wireless overview	
6)	Overview	overview		
₩	Monitoring	AP Configuration	Open Access Controller _ OFF Turn ON to manage the AP What is AP?	
ţĊ	System Setup	AP group		
品	Network	AP Firmware Upgrades		
ţţţ	Flow Control	Wireless black and white list		
<b>P</b>	Access Controller	User Information		
<u>8</u> -	Authentication			
₩	Behavior			
Ħ	Firewall			
Y	Advanced application			
0%	Services			
ſð	Log			

# Fig 5.1.1 Default Wireless overview OFF page

	CMD-COS-v1.01										은 English
		Access	Access Controller > Wireless overview						🔷 CPU: 0.50% 🕻	💭 MEM: 16% ↑ TX: 0.00 B/:	a 🤳 RX: 0.00 B/s
0	System	Wireless	Wireless overview								í í
en l	Overview	overview	Open Access Controller		Manage AP						
- PM	Monitoring	AP Configuration			in the second						
¢	System Setup	AP group	Running State								
뮯	Network	AP Firmware Upgrades	AP status			terminal statistics					=
111	Flow Control	Wireless black and white list	0 0	0 0		0	0	0	0	0	
2	Access Controller	User Information	Online AP Offline AP	fast roaming 5G first		2.4G online	5G online	peak online	active terminal	inactive terminal	
<u>8</u>	Authentication										
₩	Behavior		Wireless Network Rating	=	traffic statistics						=
田	Firewall		user activity								
	Advanced				ate						
	application		network saturation	association stability	rage r						
ōć	Services				Ave						
ъ	Log			fired another							
			airport neaith	signal coverage							
			terminal association details		Network transmissio	n quality					
			24	1.00 2.00	ate (96)						
			21 3	Access evaluation: nothing	sion						
			18 6	Access times: 0 Average access success rate: 0%	transmi						
			15 9 12		Re						
							-O- 2.4GRetransm	nission rate -O- 5GRetransmis	sion rate		

Fig 5.1.2 Default Wireless overview ON page

<b></b>	CMD-COS-v1.01		C) & A & A	English
	=<	Access	Access Controller > Wireless overview 📫 CPU: 27.97% 🛄 MEM: 18% ↑ TX: 2.22 KB/s ↓ R	X: 639.00 B/s
		Controller	Wireless overview	
Ð	System Overview	Wireless overview		
₩	Monitoring	AP Configuration	Open Access Controller ON O The connected AP will automatically enter the AP device list. Manage AP	
ţŷł	System Setup	AP group	Running State	
品	Network	AP Firmware Upgrades	AP status terminal statistics	=
ţţţ	Flow Control	Wireless black and white list		
<b>P</b>	Access Controller	User Information	Online AP     Offline AP     fast roaming     5G first     2.4G online     5G online     peak online     active terminal     inactive term	inal
<u>&amp;</u> "	Authentication			
$\downarrow$	Behavior		Wireless Network Rating traffic statistics	Ē
Ħ	Firewall			
Ţ	Advanced application		saturation association association	
0%	Services		2.93 KB/s	
ß	Log			new notifications

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

	CMD-COS-v1.01			_ා රු A ≗ Eng	lish
	=,	Access	Access Controller > Wireless overview	💼 CPU: 0.00% 🛄 MEM: 18% ↑ TX: 124.00 B/s ↓ RX: 228.0	)0 B/s
	Surtem	Controller	Wireless overview		
6-3	Overview	overview			
₩	Monitoring	AP Configuration	Open Access Controller ON O The connected AP will automatically enter the AP device	e list. Manage AP	
ŝ	System Setup	AP group	Running State		
品	Network	AP Firmware Upgrades	AP status terr	erminal statistics	
†∔†	Flow Control	Wireless black and white list	2 0 2 1 2	2 0 2 1 1	
<b>P</b>	Access Controller	User Information	Online AP Offline AP fast roaming 5G first 2.40	4G online 5G online peak online active terminal inactive terminal	
8"	Authentication				
⇔	Behavior		Wireless Network Rating		
臣	Firewall		user activity 11.7 KB/s		1
Ţ	Advanced application		work saturation		
0% 00	Services				
Ъ	Log				
			airport health Signal coverage 17:05	17:10 17:15 17:20 17:25 17:30 17:35 -O- Tx -O- Rx	

# 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

	CMD-COS-v1.01										ථ	Δ Δ	<u> </u>
	≡́	Access	Access Controller > 1	Wireless overview						i CPU: 0.00%	🛄 MEM: 18% 1	TX: 203.00 B/s	↓ RX: 196.00 B/
ଚ	System Overview	Wireless overview	Running State										
₩	Monitoring	AP Configuration	AP status					terminal statisti	cs				=
ţ	System Setup	AP group	2 Online AP	O Offline AP	2 fast roaming	1 5G first		2	0	2	1	1	regio al
品	Network	AP Firmware Upgrades			-			2.4G Online	SG online	peak online	active terminal	inactive te	minai
tit	Flow Control	Wireless black and white list	Wireless Networ	k Rating			traffic statistic	;					_
P	Access Controller	User Information		user activity		_	11.7 KB/s						_
<u>&amp;</u> ".	Authentication						8.79 KB/s						
⇔	Behavior		work saturation		associatio	on stał	ອີດ 5.86 KB/s						
臣	Firewall						<sup>∉</sup> 2.93 KB/s						
Ī	Advanced application		airport he	alth	Signal coverage		0 B/s 17	:05 17:10	0 17:15	17:20	17:25	17:30	17:35
0%	Services									Tx Rx			

Fig 5.1.7 Wireless Network Rating page

After clicking above highlighted icon following page will be displayed



Fig 5.1.8 Wireless Network Rating channel and terminal environment page



Fig 5.1.9 Open Access Controller Manage AP page

It will direct with Access Controller > AP Configuration page.

## 5.2 AP Configuration

## **Access Point Configuration:**

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

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

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

	CMD-CO5-v1.01			් 🗘 🕰 English
	=<	Access	Access Controller > AP Configuration	96% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
	-	Controller	Access Point Configuration	
$(\tilde{\cdot})$	Overview	overview		
₩	Monitoring	AP Configuration	All groupings V All Status V All Frequency V IP/MAC/Model/Remar Q	
ţĊţ	System Setup	AP group	Interference Analysis Import Export Default Config Batch Con	ig Join group Shift out group
₼	Network	AP Firmware Upgrades	MAC/IP Status Group name V 2.46 SSIU	Channel Actions
ţţţ	Flow Control	Wireless black and white list	There is no available AP, please make sure that you have done the following deployment as follov 1.The "AC intelligent control" switch in the AC state has been opened.	is
<b>P</b>	Access Controller	User Information	<ol> <li>The AC controller (router) has opened the DHCP server.</li> <li>Ensure that AC can receive a broadcast message from AP to request IP addresses (AP and AC or</li> </ol>	n the same subnet).
<u>&amp;=</u>	Authentication		¢	>
<b>↓</b> ≯	Behavior		Help: List automatically refreshes every 10 seconds, and stops refreshing when the mouse moves to the list or che The APs that join the group support the separate configuration part option, and the individual configuration	k the checkbox priority is higher than the group configuration.
Ħ	Firewall		Batch configuration: will overwrite the original configuration of the selected AP.	
Ţ	Advanced application			
0%	Services			
լ	Log			

Fig 5.2.1 Default Access Point Configuration page

3	СМД-СО5-v1.01						<u> </u>	습 🗘 🛆 English
	=,	Access	Access Controller > A	AP Configuration			📮 CPU: 12.62% 🛄 MEM: 18	% ↑ TX: 27.00 B/s ↓ RX: 27.00 B/s
	-	Controller	Access Point Confi	iguration				
6	Overview	overview						
<u>-</u>	Monitoring	AP Configuration	All groupings $\sim$	All Status 🗸 🗸	Il Frequency V IP/MAC/Mo	del/Remar Q		
<i>.</i> ??s	System Setup	AD group			Interference Analysis	Import Export Defa	ault Config Batch Config Join g	Shift out group
7 <del>,</del> 2,3	system setup	AP group	MAC/IP	Status	Group name $\vee$	2.4G SSID	Channel	AP F Actions
品	Network	AP Firmware Upgrades						Terminal details
<b>†</b> #†	Flow Control	Wireless black	08:9b:4b:9e:f4:e3	Online		COMMANDO01_2G	2.4C+1(auta)	Details and editing Modify comment
a	Access		192.168.0.13	1h 28m 30s		COMMANDO02_2G	2.4G. 1(auto)	Join group Locate Reboot
	Controller	User Information						Peripheral channel scanning
8.	Authentication		08-96-46-99-33-94	Offline		2.4G: (auto)	Details and editing Modify comment	
÷	Behavior		00.50.40.55.00.54	onine	COMMANDO02_2G		5G: (auto)	Join group Unload
- m								
œ	Firewall		Showing 1-2 of 2 red	cords			PerPage 20 $\checkmark$ Rows $\ll$ $<$	1 > >> 1 /1Pages Jump
5	Advanced application							
08	Services		Help: List a	utomatically refreshes eve	ry 10 seconds, and stops refreshir	ng when the mouse moves to the list or c	heck the checkbox	
-00			The A Batch	APs that join the group sup configuration: will overwi	port the separate configuration p ite the original configuration of t	on priority is higher than the group configurat	ion.	
ľЪ	Log							

Fig 5.2.2 Access Point Configuration Online/Offline AP page

*	OMD-COS-v1.01								0 0 4 2	English		
	=,	Access	Access Controller >	AP Configuration				🔷 CPU: 0.00% 🔤	🔉 MEM: 18% ↑ TX: 0.00 B/s 👃	RX: 0.00		
	System	Wireless	Access Point Con	figuration								
F-3	Overview	overview	All arounings	All Status	All Frequency		Interference Analysis Import Evnort	Default Config	loin group			
W	Monitoring	AP Configuration	MAC/IP	Status	Group name ~	246 5510	Channel	AP Remarks ~	MAC/IP			
	System Setup	AP group	mas, ir						Status			
ፌ	Network	AP Firmware Upgrades	08:9b:4b:9e:f4:e3	Online		COMMANDO01_2G	2.4G: 1(auto)		Deta 🗹 Group nam	ie.		
	Flow Control	Wireless black and white list	192.168.0.13	1h 34m 25s		COMMANDOU2_2G			teb teb Peris 56 Radio1	SSID		
•	Access	User Information							5G Radio2	SSID		
<b>R</b> -1	Authentication		08:9b:4b:99:a3:94	Online		COMMANDO01_2G	2.4G: 11(auto)		Deta 🗹 Channel			
<u>د</u>			192.168.0.10	10m 41s		COMMANDO02_2G	5G: 149(auto)		cin Uplink Rebr negotiation	a rate		
	Behavior								Load(Curre	nt/Max)		
Ħ	Firewall		Showing 1-2 of 2 re	ecords				PerPage 20 $\checkmark$ Rows $\ll$	< 1 > > Current Ver	rsion		
	Advanced application								2.4G	ad EC		
	Services		Help: List a The	Hejp: List automatically refreshes every 10 seconds, and stops refreshing when the mouse moves to the list or check the checkbox The APS hat join the group support the sparse configuration part option, and the individual configuration priority is higher than the group configuration.								
ኩ	Log		batc	Batch configurations will overwrite the original configuration of the selected AP.								
									Noise floor	2.4G		
									radio1	56		
									radio2			
									Signal 2.4G	i		
									Signal 5G r	adio1		
									Minimum A Signal 5G r	Access adio2		
									AP Remark	s		

5.2.3 Access Point Configuration Default AP page

2	CMD-COS-v1.01											<u> </u>	ት 👃 🕹 English
		Access	Access Controller > AP Configuration ♦ CPU. 223% 🕁 MIM: 18% ↑ TX:										↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
0	System	Wireless	Access Point Confi	iguration									
	Óverview	overview	All groupings	All Status V All Freque				Interferenc	re Analysis Import	Export Default Config	Batch Config	loin group	Shift out aroun th
Μ	Monitoring	AP Configuration	масля	Status Group name >	2.46 SSID	5G Radio1 SSID	5G Radio2 SSID	Channel	Unlink pegotiation rate	Load(Current/May)	Current Version	Channel load :	масле
Ô	System Setup	AP group	most a										Status
몶	Network	AP Firmware Upgrades	08:9b:4b:9e:f4:e3	Online	COMMANDO01_2G			2.4G: 1(auto)	100 Mixer	2.4G: 0/unlimited	167	10.21%	Deta 🗹 Group name Moc
141	Flow Control	Wireless black	192.168.0.13	1h 36m 43s	COMMAND002_2G			2.40. ((000))	i do mopo	L. Har by animited			Ion de 2.4G SSID Rebi
ন	Access	User Information											5G Radio2 SSID
	Controller		08:9b:4b:99:a3:94	Online	COMMANDO01 2G	COMMANDO01 5G		2.4G: 11(auto)		2.4G: 0/unlimited			Dita Channel
181	Authentication		192.168.0.10	13m	COMMANDO02_2G	COMMANDO02_2G COMMANDO02_5G		5G: 149(auto)	149(auto) 100 Mbps	5G Radio1: 1/unlimited	1.5.5	4.31%	Ion Vplink Reb negotiation rate
÷	Behavior						_						Perij
臣	Firewall		Showing 1-2 of 2 rec	ords						DerDa	ae 20 V Rour	<i>и</i> ( <b>1</b> )	Current Version
5	Advanced application		showing the original							Perra	ge 10 · Rows		Channel load 2.4G
Bå	Services		Help: List au	utomatically refreshes every 10 sec	nds, and stops refreshing wi	en the mouse moves to the li	ist or check the checkb	ж					Channel load 5G radio1
D.	los		The Al Batch	Ps that join the group support the configuration: will overwrite the or	eparate configuration part or ginal configuration of the se	ption, and the individual conf lected AP.	iguration priority is hig	her than the group o	onfiguration.				Channel load 5G radio2
47	uy												Noise floor2.4G
													Noise floor5G radio1
													Noise floor5G radio2
													Minimum Access Signal 2.4G
													Minimum Access
													Minimum Access
													Signat SG radio2
													Rx Rx
													AP Remarks
													or

Fig 5.2.4 Access Point Configuration Customize display page

												0	🗘 🗘 🕰 English
	=	Access	Access Controller > A	P Configuration							🔷 CPU: 35.00% 🛄 1	MEM: 18% ↑ 1	TX: 136.00 B/s 🤳 RX: 109.00 B/s
0	System	Controller `	Access Point Confi	guration									
6-3	Overview	overview	All annunings	All Status	All Frequency - 54				Interference Antholic Import	Execut Defe	ult Config	Join group	Shift out aroun 111
<b>W</b>	Monitoring	AP Configuration	Xil groupings 🔍	All status 🔍	All Frequency V	IP/MAC/Model/Keman Q			Interference Analysis Import	Export	are coming baten coming	Join group	shirt durgroup
ø	System Setup	AP group	MAC/IP	Status G	roup name ~	Z4G SSID	Channel	Uplink negotiation rate	Load(Current/Max)	Current Version	Channel load 2.4G V	Channel load	Actions
윮	Network	AP Firmware Upgrades	08:9b:4b:9e:f4:e3	Online		COMMANDO01_2G	2.4G: 1(auto)	100 Mbps	2.4G: 0/unlimited	1.5.7	9.8%		Terminal details Details and editing Modify comment
111	Flow Control	Wireless black and white list	192.100.0.13	In Join os		COMMANDOU2_2G							Reboot Peripheral channel scanning
2	Access Controller	User Information											Terminal details Details and editing
81	Authentication		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%	Modify comment
∽	Behavior												Peripheral channel scanning
Ħ	Firewall		Showing 1-2 of 2 rec	ords							BarBaras 20 M Barus		1 /IPager Jump
,	Advanced application		showing the origined	ords.							PerPage 20 + Rows		////////
	Services		Help: List au	tomatically refreshes	every 10 seconds, and	d stops refreshing when the me	ouse moves to the list o	r check the checkbox ation priority is higher than t	the group configuration				
ኩ	Log		Batch	configuration: will ov	erwrite the original co	infiguration of the selected AP.	are individual comga	ation priority ta right a faint	are group comganation.				

Fig 5.2.5 Access Point Configuration Customized AP page

<b></b>	смр-со5-у1.01					ථ	습 🗘 🛆 English
	=<	Access	Access Controller > A	P Configuration		🛱 CPU: 11.39% 🔛 MEM: 18%	↑ TX: 3.77 KB/s ↓ RX: 198.00 B/s
	-	Controller	Access Point Confi	guration			
Ð	System Overview	Wireless overview					
<u>M</u>	Monitoring	AP Configuration	All groupings $\sim$	All Status 🗸 All Freque	ncy V IP/MAC/Model/Remarl Q		
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Curtary Catur			Interference Analysis	Import Export Default Config	Batch Config Join group	Shift out group
202	System Setup	AP group	MAC/IP	Status	2.4G SSID	Channel	Actions
品	Network	AP Firmware Upgrades					Terminal details
ţţţ	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 43m 48s	COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto)	Details and editing Modify comment
<b>P</b>	Access Controller	User Information					Reboot Peripheral channel scanning
<u>8</u> -	Authentication						Terminal details Details and editing
₩	Behavior		08:9b:4b:99:a3:94 192.168.0.10	Online 19m 57s	COMMANDO01_2G COMMANDO02_2G	2.4G: 11(auto) 5G: 149(auto)	Modify comment Join group Locate
Ħ	Firewall						Peripheral channel scanning
Y	Advanced application		Showing 1-2 of 2 rec	ords	PerPage	20 ~ Rows « < 1	> >> 1 /1Pages Jump
0%	Services						

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.

<b></b>	CMD-COS-v1.01									۵	φ φ .	<u>e</u> English
	=,	Access	Access Controll	er > User Information					📮 CPU: 5.75%	6 🛄 MEM: 18%	1 TX: 0.00 B/s	; ↓ RX: 0.00 B/s
	_	Controller	User Informat	tion								
6	System	Wireless										
0.0	Overview	overview										
₩	Monitoring	AP Configuration	08:9b:4b:99:a3	08:9b:4b:99:a3:94 Q All Frequency $\checkmark$ All users $\checkmark$								
ţĊţ	System Setup	AP group	IP Address $\vee$	MAC	AP Infomation	SSID	Signal 🗸	Connect Time	✓ Tx <	Rx ∽	Comment	Actions
品	Network	AP Firmware Upgrades	192.168.0.100	c4:d9:87:a7:ad:46	08:9b:4b:99:a3:94	5G:COMMAN DO01_5G	-47dBm ull	13m 11s	27 B/s	27 B/s	Static%20Bind ing	Details Modify comment
ţţţ	Flow Control	Wireless black and white list	192.168.0.11	20:a6:0c:37:4d:13	08:9b:4b:99:a3:94	2G:COMMAN DO02 2G	-82dBm 📶	3m 50s	0 B/s	0 B/s	POCOF1- POCOF1	Details Modify comment
1	Access Controller	User Information										,
8=	Authentication		Showing 1-2 o	f 2 records	ords			PerPage	20 V Rows	《 〈 1	> >> 1	/1Pages Jump

Fig 5.2.7 Access Point Configuration Terminal Details page
CHONAN	CMD-COS-v1.01									Q	☆ ↓	2	English
	=<	Access	Access Controller > A	AP Configuration					∎ <b>Щ</b> ∎ CPU: 27.50%	🛄 MEM: 19%	1 TX: 0.0	00 B/s 🔱	RX: 0.00 B/
		Controller	Access Point Conf	iguration									
$\mathbb{C}$	System Overview	Wireless overview											
₽2	Monitoring	AP Configuration	All groupings $~~ \lor~$	All Status	✓ All Frequen	cy ∨ IP/		/Remar Q					
<i>5</i> 3;	System Setup	AP group		Interfere	nce Analysis	Import	Export	Default Config	Batch Config	Join group	Shift o	ut group	†+†
~~ ~			MAC/IP	Status	Group name			2.4G SSID		Channel	Actions		
品	Network	Upgrades									Terminal d	etails	
ţţţ	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	3 Online COMMANDO01_2G 9m 34s COMMANDO02_2G		COMMANDO01_2G COMMANDO02_2G			2.4G: 11(aut) Join	Details and Modify cor	editing ment		
r	Access Controller	User Information	13En colorito					Reboot Peripheral	channel sc	anning			
8= 	Authentication										Terminal d	etails editing	
$\stackrel{\checkmark}{\Rightarrow}$	Behavior		08:9b:4b:99:a3:94 192.168.0.10	Online 9m 18s			0	COMMANDO01_2G COMMANDO02_2G		2.4G: 1(auto 5G: 149(aut	Modify cor Join group	nment Locate	
臣	Firewall										Reboot Peripheral	channel sc	anning
Ţ	Advanced application		(hi 1, 2, -(, 2,	•				Darbarra	20	<b>,</b>		(1.0	lump
0% 00	Services		Showing 1-2 of 2 red	cords				PerPage	20 V Rows	« < 💶 >	<i>}</i> //	/ TPages	Jump
ß	Log		Help: List a The A Batch	utomatically refre APs that join the g configuration: w	eshes every 10 seco group support the s ill overwrite the ori	nds, and stops eparate config ginal configur	refreshing w juration part ation of the s	when the mouse mov option, and the indiv selected AP.	es to the list or check th ridual configuration prio	e checkbox rity is higher tha	n the group	configura	tion.

Fig 5.2.8 Details and editing AP Configuration page

×	on costan							0 0 4 L	English
	=<	Access	Access Controller > AP Configuration					- CPU: 27.50% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
0	System	Controller Wireless	Edit						× ^
	Overview	overview							
	Monitoring	AP Configuration	Equipment Status	2.4G Other Setting					
ŵ	System Setup	AP group						-	
몶	Network	AP Firmware	SSID1 Name:	COMMAND001_2G		SSID2 Name:	COMMANDO02_2G		
	dam Cartal	Wireless black	SSID1 Security:	No Password $\sim$		SSID2 Security:	No Password $\qquad \checkmark$		
THE	Flow Control	and white list	SSID1 VLAN:	Close $\lor$		SSID2 VLAN:	Close ~		
2	Access Controller	User Information	Hide SSID1 Name:	Open		Hide SSID2 Name:	Open		
8	Authentication		SSID rate limit:	Open		SSID rate limit:	Open		
<del>(_</del>	Behavior		Guest Mode:	Open (Isolate guest devices dis	covery and access to wired network)	Guest Mode:	Open (Isolate guest devices disc)		
~~			SSID3 Name:			SSID4 Name:			
盟	Firewall		SSID3 Security:	No Parouned		SSID4 Security	No Parsword		
☑	Advanced application		CODD IS AN			contraction of the second se			
BB	Services		SSID3 VDAN:	Close V		SSID4 VDAN:	Close V		
р.			SSID rate limit:	Open		SSID rate limit:	Open		
чо	Log		Guest Mode:	Open (Isolate quest devices dis		Guest Mode:	Open (Isolate guest devices disc)		
			Channel:	Auto 🗸					
			RF access strategy:	Close ~					
			Min signal(%)(%):	0	Close				
			AP Signal:	100%					
			Channel width:	20 MHz					
			Airtime scheduling:	Open					
			advanced settings:	Open					
				Save Cancel					

Fig 5.2.9 Default 2.4G AP Configuration page

# How to change SSID (Wi-Fi Name)?

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

*	CMD-COS-v1.01						🛆 🏠 🔔 English
	Ξ·	Access Controller	ss Controller > AP Configuration				- CPU: 27.50% 💭 MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
6	System Overview	Wireless overview	Equipment Status	2.4G Other Setting			
<b>1</b> 2	Monitoring	AP Configuration	SSID1 Name:	COMMANDO		SSID2 Name:	Network1
¢	System Setup	AP group	SSID1 Security:	WPA-PSK+WPA2-PSK ~		SSID2 Security:	WPA-PSK+WPA2-PSK $\lor$
몲	Network	AP Firmware Upgrades	SSID1 Password:	••••••		SSID2 Password:	••••••
111	Flow Control	Wireless black and white list	SSID1 VLAN:	Close ~		SSID2 VLAN:	Close ~
୲ଵ	Access	User Information	Hide SSID1 Name:	Open		Hide SSID2 Name:	Open
	Controller		SSID rate limit:	Open		SSID rate limit:	Open
8	Authentication		Guest Mode:	Open (Isolate guest devices discovery an	nd access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
₩	Behavior		SSID3 Name:	Network2		SSID4 Name:	Network3
田	Firewall		SSID3 Security:	WPA-PSK+WPA2-PSK V		SSID4 Security:	WPA-PSK+WPA2-PSK V
☑	Advanced application		SSID3 Password:	••••••		SSID4 Password:	••••••
명왕	Services		SSID3 VLAN:	Close $\checkmark$		SSID4 VLAN:	Close $\lor$
<u>п</u> ъ			Hide SSID3 Name:	Open		Hide SSID4 Name:	Open
Ю	Log		SSID rate limit:	Open		SSID rate limit:	Open
			Guest Mode:	Open (Isolate guest devices discovery an	nd access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
			Channel:	Auto $\checkmark$			
			RF access strategy:	Close $\vee$			
			Min signal(%)(%):	0 Close			
			AP Signal:	100%			
			Channel width:	20 MHz V			
			Airtime scheduling:	Open			
			advanced settings:	Open			
				Save Cancel			

# Fig 5.2.10 Changing SSID Configuration page

	CMD-COS-v1.01							스 습 수 온 English
	≡<	Access	Access Controller > /	AP Configuration			📮 CPU: 27.50%	1EM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
		Controller	Access Point Conf	figuration				
6	Overview	overview						
<u>-</u>	Monitoring		All groupings $\sim$	All Status	✓ All Frequency ✓ IP/M	IAC/Model/Remar Q		
52	Curtary Catura	AD			Interference /	Analysis Import Export	Default Config Batch Config Jo	bin group Shift out group
2Ç7	system setup	AP group	MAC/IP	Status	Group name 🗸	2.4G SSID	Channel	AP Re Actions
몲	Network	AP Firmware Upgrades						Terminal details
†∔†	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3 192.168.0.13	Online 21m 47s		COMMANDO Network1 Network2	2.4G:(auto)	Details and editing Modify comment Join group Locate
•	Access Controller	User Information				Network3		Reboot Peripheral channel scanning
<u>8</u> "	Authentication							Terminal details
₩	Behavior		08:9b:4b:99:a3:94 192.168.0.10	Online 21m 28s		COMMANDO01_2G COMMANDO02_2G	2.4G: 1(auto) 5G: 149(auto)	Modify comment Join group Locate
田	Firewall							Reboot Peripheral channel sca
	Advanced			<				>
	application		Showing 1-2 of 2 re	cords			PerPage 20 $\sim$ Rows $\ll$	< 1 > > 1 /1Pages Jump
	Services							
ß	Log		Help: List a The A Batch	nutomatically refrest APs that join the gro configuration: will	hes every 10 seconds, and stops r oup support the separate configu overwrite the original configurat	efreshing when the mouse moves to the list ration part option, and the individual config ion of the selected AP.	or check the checkbox uration priority is higher than the group config	uration.

Fig 5.2.11 AP configuration after Changing SSID Configuration page

	CMD-COS-v1.01							ය ර 4	<u> English</u>
	≡<	Access	Access Controller > /	AP Configuration			içi CPU: 2	27.50% 🛄 MEM: 19% ↑ TX: 0.00	B/s 👃 RX: 0.00 B/s
A	System	Wireless	Access Point Cont	figuration					Disconnect
5	Overview		All groupings $\sim$	All Status	All Frequency V	IAC/Model/Remar Q	(a.	COMMANDO01_2G	
~~	Monitoring	AP Conliguiation			Interference	Analysis Import Export I	Default Config		
ţÇ}	System Setup	AP group	MAC/IP	Status	Group name 🗸	2.4G SSID	Channel	COMMANDO02_2G	
몲	Network	AP Firmware Upgrades					G	COMMANDO01 5G	1
tit	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	Online		COMMANDO Network1	2.4G: 1(a		
<b>P</b>	Access Controller	User Information	192.166.0.15	24m 495		Network3	₽ <i>ſſ</i> ċ	COMMANDO	
<u>8</u> ,	Authentication						B <sub>C</sub>	Notwork1	
⇇	Behavior		08:9b:4b:99:a3:94	Online		COMMANDO01_2G	2.4G: 11		
	Firewall		192.166.0.10	2411 395		COMMANDOUZ_2G	5G. 145	Network2	
8	Filewall			<					I
V	Advanced application		Showing 1-2 of 2 re	cords			PerPage 20	Network3	
0% 00	Services		Showing 1 2 01 2 10	cords			Tellage 20	COMMANDOOD FC	
Ռ	Log		Help: List a	utomatically refresh	es every 10 seconds, and stops :	refreshing when the mouse moves to the list o	or check the checkbox	COMIMANDOUZ_5G	
			The Batch	APs that join the gro n configuration: will (	up support the separate configu overwrite the original configurat	ration part option, and the individual configur ion of the selected AP.	ration priority is higher Netv Chang	vork & Internet settings ge settings, such as making a conne	
							(c)	<b>r∱</b> ((j))	
							Wi-Fi	Airplane mode hotspot	

#### 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.

	CMD-COS-v1.01						තා රු 🗘 💄 English
	=/	Access	Access Controller > AP Configuration				:📮: СРU: 27.50% 🛛 🛄 МЕМ: 19% ↑ ТХ: 0.00 В/з 🤳 RX: 0.00 В/з
		Controller	Edit				×
ଚ	System Overview	Wireless overview					
5	Monitoring	AP Configuration	Equipment Status	2.4G 5G Other Se	tting		
÷	System Setup	AP group	SSID1 Name:	COMMANDO01_2G		SSID2 Name:	COMMANDO02_2G
品	Network	AP Firmware Upgrades	SSID1 Security:	No Password ~		SSID2 Security:	No Password ~
tłł	Flow Control	Wireless black and white list	SSID1 VLAN:	Close		SSID2 VLAN:	Close $\vee$
	Access	User Information	Hide SSID1 Name:	Auto		Hide SSID2 Name:	Open
[]]	Authoritien		Guest Mode:	2	covery and access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
( <u>e</u> .)	Authentication			3			
⇔	Behavior		SSID3 Name:	4		SSID4 Name:	
m			SSID3 Security:	5		SSID4 Security:	No Password 🗸
œ	Firewall		SSID3 VI AN-	6		SSID4 VLAN-	(lose V
<b>I</b>	Advanced application		Hide SSID3 Names	8		Hide SSID4 Name:	
<b>п</b> а.			Tide SSIDS Name.	9		Thue SSID4 Name.	
öð	Services		Guest Mode:	10	covery and access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
Γħ	Log			11			
			Channel:	5 ~			
			RF access strategy:	Close ~			
			Min signal(%)(%):	0	Close		
			AP Signal:	100% ~			
			Channel width:	20 MHz V			
			advanced settings:	Open			
100704-007							

Fig 5.2.12 Changing Channel for SSID page

	CMD-COS-v1.01					ධ	습 수 음	English
	=<	Access	Access Controller > Al	P Configuration		📲 CPU: 27.50% 🛄 MEM: 19	% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
$\sim$	 System	Controller Wireless	Access Point Config	guration				
63	Overview	overview						
2	Monitoring	AP Configuration	All groupings 🗸 🗸	All Status V All Frequency	✓ IP/MAC/Model/Remar Q			
***	c . c .			Interference Analysis Imp	ort Export Default Config	Batch Config Join group	Shift out group	111
ις;	System Setup	AP group	MAC/IP	2.4G SSID	Channel	AP Remarks 🗸	Actions	
品	Network	AP Firmware Upgrades					Terminal details	
<u>†</u> ††	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	COMMANDO Network1	2.4G: 11(auto)	COMMANDO AP	Details and editing Modify comment	
<b>P</b>	Access Controller	User Information	192.168.0.13	Network3			Join group Locate Reboot Peripheral channel scar	nning
<u>&amp;=</u>	Authentication						Terminal details	
<del>√</del> ≯	Behavior		08:9b:4b:99:a3:94 192.168.0.10	COMMANDO01_2G COMMANDO02_2G	2.4G: 1(manual 5) 5G: 149(auto)		Modify comment Join group Locate	
田	Firewall						Reboot Peripheral channel scar	nning
	Advanced			<		>		
	application		Showing 1-2 of 2 rec	ords	PerPage	20 🗸 Rows < < 1	> >> 1 /1Pages	Jump
0%	Services		-		-			
_								

# 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	1		
# 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

	CMD-COS-v1.0					රු රු 👃 ළ English
		Access < Controller	Access Controller > AP Configuration			ion CPU: 10.75% 🛄 MEM: 18% ↑ TX: 1.18 KB/s ↓ RX: 3.51 KB/s
A	System Overview	Wireless overview	Equipment Status	2.4G 5G Other Setting		
-24	Monitoring	AP Configuration	SSID1 Name:	COMMANDO01 2G	SSID2 Name:	COMMANDO02 2G
ŝ	System Setup	AP group	SSID1 Security:	No Password 🗸	SSID2 Security:	No Password ~
品	Network	AP Firmware Upgrades	SSID1 VLAN:	Close V	SSID2 VLAN:	Close 🗸
tit	Flow Control	Wireless black and white list	Hide SSID1 Name:	Open	Hide SSID2 Name:	Open
9	Access Controller	User Information	Guest Mode:	Open (Isolate guest devices discovery and access to will be access to will be access to will be accessed as a second s	red network) Guest mode.	Open (solate guest devices accovery and access to writed network)
<u>A</u>	Authentication		SSID3 Name:		SSID4 Name:	
÷	Behavior		SSID3 Security:	No Password 🗸	SSID4 Security:	No Password V
~77			SSID3 VLAN:	Close $\lor$	SSID4 VLAN:	Close $\checkmark$
臣	Firewall		Hide SSID3 Name:	Open	Hide SSID4 Name:	Open
Ţ	Advanced application		Guest Mode:	Open (Isolate guest devices discovery and access to wi	red network) Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
	Services		Channel:	5		
Ъ	Log		RF access strategy:	Close V		
			Min signal(%)(%):	0 Close		
			AP Signal:	100%		
			Channel width:	20 MHz 🗸		
			advanced settings:	Self-adaption		
_				20 MHz		
				40 MHz Save Cancel		

# Fig 5.2.15 Changing Channel Width for AP configuration page

(100	CMD-COS-v1.01					» û 4 2
	=	Access	Access Controller > AP Configuration		📲 CPU: 27.50% 🔛 MEM:	: 19% ↑ TX: 0.00 B/s ↓ I
		Controller	Equipment Status 2.4G Other Sett	ng		
$\mathbb{C}$	System Overview	Wireless overview	Basic information			
<u> </u>	Monitoring	AP Configuration	Current 1.5.7	AP status: C	Inline	
ŝ	System Setup	AP group	version;	Online 3 duration:	7m 45s	
600	Network	AP Firmware Upgrades	MAC address: 08:9b:4b:9e:f4:e3	IP address: 1	92.168.0.13	
ţţţ	Flow Control	Wireless black and white list	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	
<b></b>	Access Controller	User Information	Status information			
<u>&amp;=</u> ]	Authentication		AP health value	AP hardware status	AP signal	coverage
⇆	Behavior		2G channel status score			
臣	Firewall					$\frown$
Ţ	Advanced application			3.0% (58	.0% (1)	00.0%
0%	Services		ss score Access			Coverage
Ŀ	Log			CFO usage Miemol	y usage	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.

	CMD-COS-v1.01			스) 슈 유 온 Eng	lish
	=<	Access	Access Controller > AP Configuration	ដើ្ច CPU: 27.50% 🖵 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.0	00 B/s
	-	Controller	Edit		×
$(\mathbf{r})$	System Overview	Wireless overview			
₩	Monitoring	AP Configuration	Equipment Status 2.4G	Other Setting	
ŝ	System Setup	AP group	Basic Information		
品	Network	AP Firmware Upgrades	AP remarks:		
ţţţ	Flow Control	Wireless black and white list	Schedule:	Plan 1	
<b>P</b>	Access Controller	User Information		Plan 2	
<u>8</u> =)	Authentication			Plan 3	
<b>↓</b> ≯	Behavior		Restart:	Open	
田	Firewall		Fast roaming		
Ţ	Advanced application		Fast roaming:	Open (Fast marring is enabled in all bands after turning on)	
0%	Services		· ·	( and rearining to endored in an edited error tarring 50)	
ß	Log		Save	Cancel	

Fig 5.2.17 Default Other Setting of AP configuration page

	CMD-COS-v1.01					ධ	<u>۵</u>	2	English
	≡<	Access	Access Contro	oller > AP Configuration	ې CPU: 27.50% 📮	DEM: 19%	↑ TX: 0.00	B/s 🤳	RX: 0.00 B/s
Ð	System Overview	Wireless overview	Edit						×
~~	Monitoring	AP Configuration		Equipment Status 2.4G	Other Setting				
ŝ	System Setup	AP group		Basic Information					
윪	Network	AP Firmware Upgrades		AP remarks	SUNDAY OFF				
†∔†	Flow Control	Wireless black and white list		Schedule:	✓ Plan 1				
P	Access Controller	User Information			Cycle: Weekły 🗸				
<u>e</u> ,	Authentication				Weekly: 🗌 All 🗹 Monday 🗹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Friday 🗹 Saturday 📄 :	Sunday			
₩	Behavior				Time: 00:00-23:59				
臣	Firewall				Plan 2				
Ţ	Advanced application			Restart -	Plan 3				
0% 00	Services			NOVAL 2					
Ъ	Log			Fast roaming					
				Fast roaming:	Open (Fast roaming is enabled in all bands after turning on)				
				Save	Cancel				

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

	CMD-COS-v1.01												English
		Access	Access Controller > A	P Configuration						📮 CPU: 27.50%	🛄 MEM: 19%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
		Controller	Access Point Confi	iguration									
$\mathfrak{S}$	System Overview	Wireless overview											
5	Monitoring	AP Configuration	All groupings $\sim$	All Status	V All Frequency V IP/MAC/Model/Re	emar Q							
1 <del>2</del> 2		40				Interference Analysis	Import	Export	Default Config	Batch Config	Join group	Shift out group	111
£53	system setup	AP group	MAC/IP	Status	Group name 🗸	2.4G SSID		Channe		AP Remarks $\vee$		Actions	П
뮮	Network	AP Firmware Upgrades										*	
t#ŧ	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	Suspended		COMMANDO Network1		2.4G; 10	auto)	SUNDAY OFF		Terminal details Details and editing Modify comment	
۹	Access Controller	User Information	192.168.0.13	4/m 32s		Network2 Network3						Join group Locate Reboot	
<u>&amp;</u> =	Authentication												
₩	Behavior		08:9b:4b:99:a3:94	Offline		COMMANDO01_2G COMMANDO02_2G		2.4G: (a 5G: (au	uto) to)			Details and editing Modify comment Join group Unload	
臣	Firewall												
Ţ	Advanced application		Showing 1-2 of 2 rec	ords					PerPage	20 V Rows	« < 1 )	> > 1 /1Pag	es Jump
	Services												
ß	Log		Help: List a The A Batch	utomatically refre Ps that join the g configuration: w	eshes every 10 seconds, and stops refreshing who proup support the separate configuration part op ill overwrite the original configuration of the sele	en the mouse moves to the li ption, and the individual confi acted AP.	at or check the ch guration priority i	eckbox is higher than	the group configura	tion.			

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

	CMD-COS-v1.0								Q	<b>公</b>	2	English
	=,	Access	Access Controller > A	P Configuration	n			📮 CPU: 27.50%	🛄 MEM: 19%	↑ TX: 0.00	)B/s ↓	RX: 0.00 B/
	_	Controller	Access Point Confi	guration								
$\mathbb{C}$	System Overview	overview										
₩	Monitoring	AP Configuration	All groupings $\sim$	All Status	<ul> <li>✓ All Frequencies</li> </ul>	uency 🗸		/Remar Q				
£2	System		Interference	e Analysis	Import	Export	Default Config	Batch Config	Join group	Shift ou	t group	†+†
ŝ	Setup	AP group	MAC/IP	Status	Group	name 🗸		2.4G SSID		Actions		
品	Network	AP Firmware Upgrades								Terminal det	ails	
ſţţŧ	Flow	Wireless black	08·9h·4h·9e·f4·e3	Online				COMMANDO Network1		Details and e	editing	
	Control	and white list	192.168.0.13	49m 41s				Network2		Join group	Locate	
	Controller	User Information						Networks		Peripheral cl	nannel sca	anning
<u>&amp;</u> =	Authenticatior									Terminal det	tails	
÷	Robavior		08:9b:4b:99:a3:94	Online				COMMANDO01_2G		Details and e Modify com	editing ment	
>	Denavior		192.168.0.10	49m 42s				COMMANDO02_2G		Join group Reboot	Locate	
Ħ	Firewall									Peripheral cl	nannel sca	anning
	Advanced			<					>			
	application		Showing 1-2 of 2 red	ords			PerPag	e 20 🗸 Rows	« < 1 >	≫ 1	/1Pages	Jump
	Services											

Fig 5.2.20 Modify Comment page

CONDE	CMD-COS-v1.0				
	_<	Access	Access Controller > AP Configuration	📮 CPU: 27.50% 🖳 MEM: 1	9% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
Ð	System ^ Overview	Wireless overview	Acc Modify comment	×	
~~			All		
ţÇ	System Setup	AP group	AP Remarks: COMMANDO AP	Join group	Shift out group
	Network	AP Firmware Upgrades	OK Cancel		Terminal details
	Flow Control	Wireless black and white list	08: 192-155.0.13 50m 55s	Networkz	Details and editing Modify comment Join group Locate
<b>(</b>				Network3	Reboot Peripheral channel scanning
<u>8</u> =	Authenticatior				Terminal details
⇔	Behavior		08:9b:4b:99:a3:94 Online 192.168.0.10 50m 46s	COMMANDO01_2G COMMANDO02_2G	Modify comment Join group Locate
Ħ					Reboot Peripheral channel scanning
Ţ	Advanced application		c		
0%			Showing 1-2 of 2 records	PerPage 20 V Rows 《 < 1	> > 1 /1Pages Jump
R	log V		Heles		a da da a aba al da ave

Fig 5.2.21 Changing Modify Comment page

	CMD-COS-v1.01								스) 슈 스 English
	=,	Access	Access Controller > /	AP Configuration				i CPU: 27.50% 🔛 ME	:M: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		Controller	Access Point Conf	iguration					
A	System Overview	Wireless overview							
₩	Monitoring	AP Configuration	All groupings $\sim$	All Status $\checkmark$	All Frequency V IP/MAC/Mod	del/Remar Q			
222	Surton Satur	AP aroun				Interference Analysis	Import Export Default	t Config Batch Config Joi	n group Shift out group
252	System Setup	Aigioup	MAC/IP	Status	Group name $\checkmark$	2.4G SSID	Channel	AP Remarks 🗸	Actions 🗌
믋	Network	AP Firmware Upgrades							Terminal details
ti t	Flow Control	Wireless black	08:9b:4b:9e:f4:e3	Online		COMMANDO Network1	2.40-6(+-)	COMMANDO AD	Details and editing Modify comment
_	Access		192.168.0.13	52m		Network2 Network3	2.4G: 0(auto)	COMIMANDO AP	Join group Locate Reboot
	Controller	User Information				Hearding .			Peripheral channel scanning
<u>&amp;</u> =	Authentication								Terminal details
÷	Behavior		08:9b:4b:99:a3:94	Online		COMMANDO01_2G	2.4G: 11(auto)		Details and editing Modify comment
			192.168.0.10	50m 46s		COMMANDO02_2G	5G: 149(auto)		Join group Locate Reboot
E	Firewall								Peripheral channel scar
Ţ	Advanced application		Showing 1-2 of 2 re	cords				PerPage 20 $\checkmark$ Rows $\ll$ 0	( 1 > » 1 /1Pages Jump
	Services								
ሌ	Log		Help: List a The A Batch	utomatically refreshes APs that join the group a configuration: will ov	every 10 seconds, and stops refreshin support the separate configuration p anwrite the original configuration of the	g when the mouse moves to the list or art option, and the individual configura e selected AP.	check the checkbox ation priority is higher than the group	configuration.	

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.

	CMD-COS-v1.0	1					스) 슈 슈 ዶ English	
	=<	Access <	Access Controller > A	P Configuration		📮 CPU: 27.50%	MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00 E	B/s
6)	System	Wireless	Access Point Conf	iguration				ľ
<u>M</u>	Monitoring	AP Configuration	All groupings $\sim$	All Status	✓ All Frequency ✓ IP/M	IAC/Model/Remar Q		
ţŷ;	System Setup	AP group	Interference	e Analysis Im	port Export Defa	ult Config Batch Config Jo	in group Shift out group †‡†	
뮮	Network	AP Firmware Upgrades	MAC/IP	Status	Group name ∨	2.4G SSID	Actions	
ţţţ	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	Online 55m 11s		COMMANDO Network1 Network2	Modify comment	
<b></b>	Access Controller	User Information	152110010110	55		Network3	Reboot Peripheral channel scar	
&= ;_;	Authenticatior						Terminal details Details and editing	
⇒	Behavior		08:9b:4b:99:a3:94 192.168.0.10	Online 55m 12s		COMMANDO01_2G COMMANDO02_2G	Modify comment Join group Locate	
Ħ	Firewall						Peripheral channel scanning	
Ţ	Advanced application			٢			>	
0 % 0 0	Services		Showing 1-2 of 2 red	cords		PerPage 20 🗸 Rows ≪	< 1 > >> 1 /1Pages Jump	1

# Fig 5.2.23 Default Join group page

## Note:

Above page will be Editable after creating AP Group only

	CMD-COS-v1.01							1	} ↓ ▲ En	iglish
	=,	Access 🧹	Access Controller > A	AP Configuration			📮 CPU: 27.50%	MEM: 19%	↑ TX: 0.00 B/s ↓ RX: 0	0.00 B/s
		Controller	Access Point Conf	iguration						
6)	System Overview	Wireless overview								
5	Monitoring	AP Configuration	All groupings $\sim$	All Status $\sim$ All F	requency V IP/MAC/Mod	lel/Remar Q				
~~~~					Interference Analysis	Import Export	Default Config Batch Config	Join group	Shift out group	tŧt
ççş	System Setup	AP group	MAC/IP	Status Gro	up name 🗸	2.4G SSID	Channel	AP Rema	Actions	
몲	Network	AP Firmware Upgrades							Terminal details	
†∔†	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	Online		COMMANDO Network1	2.4C- 6/3(to)	COMMA	Details and editing Modify comment	
	Access		192.168.0.13	59m 16s		Network2 Network3	2.4G. 6(auto)	COMINA	Join group Locate Reboot	
	Controller	User Information							Peripheral channel scan	ning
<u>8</u> "	Authentication								Terminal details	
5	Behavior		08:9b:4b:99:a3:94	Online		COMMANDO01_2G	2.4G: 11(auto)		Details and editing Modify comment	
~~			192.168.0.10	59m 3s		COMMANDO02_2G	5G: 149(auto)		Join group Locate Reboot	
臣	Firewall								Peripheral channel scan	ning
Ţ	Advanced			<				>		
	-		Showing 1-2 of 2 rea	cords			PerPage 20 $\checkmark$ Rows	« < 1 >	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Jump
ŏõ	Services									
Ъ	Log		Help: List a	utomatically refreshes every 1	0 seconds, and stops refreshin	g when the mouse moves to the list o	r check the checkbox			
			The A Batch	Ps that join the group suppo	rt the separate configuration pattern of the	art option, and the individual configur	ration priority is higher than the group	configuration.		
			bacci	comganation, will overwrite	and original configuration of th					

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.

	CMD-COS-v1.01							스 슈 슈 A English
	=	Access	Access Controller > A	AP Configuration			📮 CPU: 27.50%	) MEM: 19% ↑ TX: 0.00 B/s 👃 RX: 0.00 B/s
		Controller	Access Point Conf	iguration				
Ð	System Overview	Wireless overview						
<u>M</u>	Monitoring	AP Configuration	All groupings $\sim$	All Status	✓ All Frequency ✓ IP/MAC/Mod	l/Remar Q		
	Curtary Catura	AD ====			Interference Analysis	Import Export E	Default Config Batch Config	Join group Shift out group
<i>ъ</i> С3	system setup	AP group	MAC/IP	Status	Group name 🗸	2.4G SSID	Channel	AP Rema Actions
뷺	Network	AP Firmware Upgrades						Terminal details
tŧt	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	Online		COMMANDO Network1	2.4G: 6(auto)	Details and editing Modify comment
	Access Controller	User Information	152.100.0.15	111 1111 245		Network3		Stop Locate Reboot
0=	Authoritation							Peripheral channel sca
( <u></u>	Authentication							Terminal details Details and editing
₩	Behavior		08:9b:4b:99:a3:94 192.168.0.10	Online		COMMANDO01_2G COMMANDO02_2G	2.4G: (auto) 5G: (auto)	Modify comment Join group Locate
臣	Firewall							Reboot Peripheral channel scanning
e	Advanced			<				>
12	application		Showing 1-2 of 2 m	cords			PerPage 20 V Power	
0% 00	Services		510Wing 1-2 01 2 16	cords			Feirage 20 + Kows	
Ъ	Log		Help: List a	utomatically refres	hes every 10 seconds, and stops refreshing	when the mouse moves to the list or	check the checkbox	
			The A Batch	APs that join the gro configuration: will	oup support the separate configuration pa overwrite the original configuration of the	rt option, and the individual configura selected AP.	ation priority is higher than the group con	figuration.

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.

2	CMD-COS-v1.01							스> 슈 슈 온 English
	=<	Access	Access Controller > A	AP Configuration			i CPU: 27.50%	☐ MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		Controller	Access Point Conf	figuration				
$\mathfrak{S}$	System Overview	Wireless overview		-				
5	Monitoring	AP Configuration	All groupings $~~ \lor~$	All Status	All Frequency V IP/MAC/Mo	del/Remar Q		
					Interference Analysis	s Import Export	Default Config Batch Config	Join group Shift out group
ŝ	System Setup	AP group	MAC/IP	Statue		246 5510	Channel	
몲	Network	AP Firmware Upgrades	WIAC/II	Status	Gloup name +	2.43.3310	Channel	Terminal details
†‡†	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3 192.168.0.13	Online 1h 2m 39s		COMMANDO Network1 Network2	2.4G: 6(auto)	COMMA Details and editing Modify comment
<b>P</b>	Access Controller	User Information				Network3		Reboot Peripheral channel scanning
<u>&amp;</u> ,	Authentication							Terminal details
↔	Behavior		08:9b:4b:99:a3:94	Online		COMMANDO01_2G	2.4G: 11(auto)	Modify comment
, m			192.100.0.10	111 2111 325		COMIMANDOU2_2G	5G. 149(auto)	Reboot
E	Firewall							Peripheral channel scanning
Ī	Advanced application			<				>
0%	Services		Showing 1-2 of 2 re	cords			PerPage 20 $\checkmark$ Rows	
DA.	1							
43	Log		Help: List a The A Batch	automatically refreshe APs that join the grou b configuration: will c	es every 10 seconds, and stops refreshing up support the separate configuration provervite the original configuration of t	ng when the mouse moves to the part option, and the individual con he selected AP	list or check the checkbox figuration priority is higher than the group (	configuration.

Fig 5.2.26 Reboot option in AP configuration page

	CMD-COS-v1.01											
			Access Controller >	AP Configuration					🛱 CPU: 27.50%	🛄 MEM: 19%	↑ TX: 0.00 B/s ↓ F	XX: 0.00 B/s
6		Wireless	Access Point Con	figuration								
	Overview	overview	All groupings $\sim$	All Status	✓ All Frequency ✓ IP/MA							
ĿМ	Monitoring				Interference Ar	nalysis Import	Export	Default Config	Batch Config	Join group	Shift out group	111
ţÇ			MACOD	Charles	Conversion N.	240.5510		Cha		40.0	Antiner	
몲		AP Firmware Upgrades	MAC/IP	Status	Group name V	2.46 5310		Cha	Inner	AP Kelli	Actions	
†∔†		Wireless black and white list	08:9b:4b:9e:f4:e3	Online	Tips			2.40	i: 6(auto)	COMMA	Terminal details Details and editing Modify comment	
<b>P</b>	Access Controller		132.100.0.13	1110111205	Reboot will cause the	e terminal to disconnect	t and				Reboot Peripheral channel se	canning
<u>8</u> "					confir	m continue?					Terminal details	
$\overleftrightarrow$			08:9b:4b:99:a3:94 192.168.0.10	Online 1h 8m 12s	ОК	Cancel		2.40 5G:	i: 1(auto) 149(auto)		Details and editing Modify comment Join group Locate	
Ħ											Peripheral channel se	canning
y	Advanced application			<						>		_
0% 00			Showing 1-2 of 2 re	ecords				PerPage	20 V Rows	《〈 1 〉	≫ 1 /1Page	s Jump
ß			Help: List The Batc	automatically refres APs that join the gro h configuration: will	hes every 10 seconds, and stops ret oup support the separate configura i overwrite the original configuratio	reshing when the mouse n tion part option, and the ir n of the selected AP.	hoves to the list ndividual configu	or check the check uration priority is hi	box gher than the group	configuration.		

# 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

	CMD-COS-v1.01					ථ	습 수 <u>온</u> English
	=,	Access	Access Controller > AP Configuration			📫 CPU: 27.50% 🛛 🛄 MEM: 19%	↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		Controller	Access Point Configuration				
Ð	System Overview	Wireless overview					
₩	Monitoring	AP Configuration	All groupings $\lor$ All Status $\lor$ All	Frequency V IP/MAC/Model/Remar Q			
- (7)-	System Setup	AP group		Interference Analysis Import	Export Default Config	Batch Config Join group	Shift out group
472			MAC/IP iroup name V	2.4G SSID	Channel	AP Remarks $\checkmark$	Actions
몲	Network	AP Firmware Upgrades					
ţ‡ţ	Flow Control	Wireless black and white list	08:9b:4b:9e:f4:e3	COMMANDO Network1	2.4G: (auto)	COMMANDO AP	Details and editing Modify comment
•	Access Controller	User Information		Network3			Join group Unload
<u>8</u> ,	Authentication						Terminal details
			08-01-41-00-23-04	COMMANDO01 2G	2.4G: 1/auto)		Details and editing
⇒>	Behavior		192.168.0.10	COMMANDO02_2G	5G: 149(auto)		Join group Locate
臣	Firewall						Peripheral channel scanning
	Advanced		<				>
	application		Showing 1-2 of 2 records		PerPa	ge 20 🗸 Rows < < 1	> >> 1 /1Pages Jump
00	Services						
Ъ	Log		Help: List automatically refreshes every	10 seconds and stops refreshing when the mous	e moves to the list or check the ch	eckbox	
			The APs that join the group supp Batch configuration: will overwrite	ort the separate configuration part option, and the the original configuration of the selected AP.	e individual configuration priority	is higher than the group configuration.	

Fig 5.2.28 Default Peripheral channel scanning option page

×	CMD-COS-v1.01													۵			
	=,	Access	Access Controller > AP Config	uration									io: CPU: 27.50	0% 🛄 MEM: 19	% <b>↑</b> ⊺	TX: (	TX: 0.00
	 System	Controller	Peripheral channel scanni	ng (AP MAC: 08:9b:4b	o:99:a3:94)												
6-3	Overview	overview															
₩	Monitoring	AP Configuration		in .										Refresh			
÷Ç÷	System Setup	AP group	Signal (c	(Bm)													
品	Network	AP Firmware Upgrades															
<u>†</u> ‡‡	Flow Control	Wireless black and white list															
۹	Access Controller	User Information															
<u>8</u> =	Authentication																
⇔	Behavior																
臣	Firewall																
Ţ	Advanced application			1	2	3	4	5	6	7	8	9	0 11	12	13		
	Services																
ß	Log																

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

	CMD-COS-v1.01								් ර 4 ප	English
	=<	Access	Access Controll	ler > AP group				" CPU: 2.7	5% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
~	 System	Controller	AP Group							
63	Overview	overview								
₩	Monitoring	AP Configuration							Add	Delete
ţĊł	System Setup	AP group	Group name		Number of AP	channel	Maximum belt capacity	SSID	Actions	
뷺	Network	AP Firmware Upgrades					No Data			
ţţţ	Flow Control	Wireless black and white list								
<b>P</b>	Access Controller	User Information	Help:	The APs that jo	oin the group use the g	roup configuration uniform	nly. After the packets are n	emoved, the origina	l AP configuration is restored.	
<u>&amp;=</u>	Authentication									
<b>↓</b> ≯	Behavior									
Ħ	Firewall									
Ţ	Advanced application									
0%	Services									
ľð	Log									

# 5.3.1 Default AP Group page

	040-005-1141							
	=,	Access ,	Access Controller > AP group					
		Controller	Edit					
ຄ	System Overview	Wireless overview						
22	Monitoring	AP Configuration						
ø	System Setup	AP group		Group name:				
品	Network	AP Firmware Upgrades		Follow group configuration :	Open			
tii)	Flow Control	Wireless black and white list		2.4G 5G Radio 1	5G Radio 2	Other Setting		
1	Access	User Information						
	Authentication			2.4G Control state				
دع ب	Dallar for				CEPA Name:		SEID2 Nume:	
	CHINA				CODA Consultant		6010-2 Councilian	
H	Firewall				and accurry.		and acony.	
⊡	Advanced				SSID1 VLAN:	Close V	SSID2 VLAN:	Close ~
					Hide SSID1 Name:	Open	Hide SSID2 Name:	Open
88	Services				SSID rate limit:	Open	SSID rate limit:	Open
ъ	Log				GDest MDDe:	Cpen (sciente guare devices discovery and access to writed memoric)	GDest Mode:	Com (notate guara devices discovery and access to wred network)
					SSID3 Name:		SSID4 Name:	
					SSID3 Security:	No Password V	SSID4 Security:	No Password 🗸
					SSID3 VLAN:	Close v	SSID4 VLAN:	Close ~
					Hide SSID3 Name:	Open	Hide SSID4 Name:	Open
					SSID rate limit:	Open	SSID rate limit:	Open
					Guest Mode:	Open (Isolate guest devices discovery and access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
					Channel:	Auto V (1.5.6 and above versions support 12 and 13 channels)		
					RF access strategy:	Close v		
					Min signal(%)(%):	0 Close		
					AP Signal:	100% ~		
					Channel width:	20 MHz V		
					Airtime scheduling:	Open		
					advanced settings:	Open		
						Save Canod		



											-				
CINOR	CMD-COS-v1.01										්	û	¢	2	English
	Ξ,	Access	Access Controller > A	9 group						∎ <b>©</b> ≣ CPU: 0.5	0% 🛄 MEM: 17%	↑ тх:	3.89 KB/s	↓ R	X: 9.23 KB/s
		Controller	Group	name:	COMM	IANDO									
Ð	System Overview	Wireless overview	Follow	group	Оре	en									
₩	Monitoring	AP Configuration	config	uration:											
ţĊ	System Setup	AP group	2.40	5 5G Radio 1	5G	G Radio 2	Other Setting	]							
₼	Network	AP Firmware Upgrades	2.4G C	ontrol state											
ţţţ	Flow Control	Wireless black and white list													
	Access	User Information		SSID1 Name:		Net1			SSID2 Name:	N	et2				
	Controller			SSID1 Security:		WPA-PSK+W	PA2-PSK	$\sim$	SSID2 Security:	: W	PA-PSK+WPA2-PSK	(	$\sim$		
8=) ;	Authentication			SSID1 Password	d:	•••••		$\odot$	SSID2 Password	d: ••			0		
₩	Behavior			SSID1 VLAN:		Open		$\sim$	SSID2 VLAN:	0	pen		$\sim$		
Ħ	Firewall			SSID1 VLAN_ID	):	1			SSID2 VLAN_ID	3					
e	Advanced			Hide SSID1 Na	me:	Open			Hide SSID2 Na	me:	Open				
ý	application			SSID rate limit:		Open			SSID rate limit:		Open				
00 00	Services			Guest Mode: Open					Guest Mode:						
ß	Log			(Isolate guest c	levices d	liscovery and acc	cess to wired net	work)	(Isolate guest o	devices discov	very and access to w	rired netv	vork)		

*								A C A L English
	≡,	Access	Access Controller > AP group					🔷 CPU: 0.99% 🛄 MEM: 17% ↑ TX: 60.00 B/s 🤳 RX: 60.00 B/s
~	System	Wireless		SSID1 Name:	Net1		SSID2 Name:	Net2
63	Óverview	overview		SSID1 Security:	WPA-PSK+WPA2-PSK	$\sim$	SSID2 Security:	WPA-PSK+WPA2-PSK V
<u>-</u>	Monitoring	AP Configuration		SSID1 Password:	••••••	۵	SSID2 Password:	••••••
ĝ	System Setup			SSID1 VLAN:	Open	$\sim$	SSID2 VLAN:	Open ~
몳	Network	AP Firmware		SSID1 VLAN_ID:	1		SSID2 VLAN_ID:	3
E.T.	51 C	Wireless black		Hide SSID1 Name:	Open		Hide SSID2 Name:	Open
[1+1]	Flow Control	and white list		SSID rate limit:	Open		SSID rate limit:	Open
9	Access Controller	User Information		Guest Mode:	Open (Isolate guest devices	discovery and access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
<u>8.</u>	Authentication			SSID3 Name:			SSID4 Name-	
÷	Behavior			CCID3 Consider	No Decovered		CODA Consultan	No Bacquired
~?				SSIDS Security:	NO Password		SSID4 Security:	NO Password V
E	Firewall			SSID3 VLAN:	Close	~	SSID4 VLAN:	Close ~
	Advanced			Hide SSID3 Name:	Open		Hide SSID4 Name:	Open
	application			SSID rate limit:	Open		SSID rate limit:	Open
	Services			Guest Mode:	Open (Isolate guest devices	discovery and access to wired network)	Guest Mode:	Open (Isolate guest devices discovery and access to wired network)
Γħ	Log							
				Channel:	11	(1.5.6 and above versions support 12 and 13 channels	iels)	
				RF access strategy:	Close	~		
				Min signal(%)(%):	0	Close		
				AP Signal:	100%	~		
				Channel width:	40 MHz	~		
				Airtime scheduling:	Open			
				advanced settings:	Open			
					Save			

5.3.3 Edit AP Group page

Access Controller     Access Controller > AP group     Image: Controller > AP group       System     Wireless     2.4G     5G Radio 1     5G Radio 2     Other Setting
Controller System Winders 2.4G 5G Radio 1 5G Radio 2 Other Setting
Overview overview
Monitoring AP Configuration 24G Control state
System Setup AP group
Network AP Firmware SSID1 Name: SSID2 Name:
Upgrades SSID1 Security: No Password V SSID2 Security: No Password V
and white list SSID1 VLAN: Close V SSID2 VLAN: Close
Controller User Information Hide SSID1 Name: Open Hide SSID2 Name: Open SSID rate limit: Open SSID rate limit: Open
Authentication Guest Mode: 1 Guest Mode:
Behavior Upen (Isolate guest d 2 Upen (Isolate guest devices discovery and access to
Firewall SSID3 Name: 4 SSID4 Name:
Advanced SSID3 Security: 6 SSID4 Security: No Password
SSID3 VLAN: 7 SSID4 VLAN: Close
Hide SSID3 Name: 8 Hide SSID4 Name: Open
Acg SSID rate limit: 10 SSID rate limit: Open
Guest Mode: 11 Guest Mode: 0 Open (Isolate guest devices discovery and access to 2
13
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					් ද 👃 English
	=,	Access	Access Controller > AP group			: 🛱: CPU: 2.75% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
0	System	Controller Wireless	2.4G 5G Radio 1 5G Rad	lio 2 Other Setting		^
 	Monitoring	AP Configuration	5G Radio 1Control state			
¢;	System Setup	AP group				
品	Network	AP Firmware Upgrades	SSID1 Name: SSID1 Security:	No Password	SSID2 Name:	No Password
111	Flow Control	Wireless black and white list	SSID1 VLAN:	Close ~	SSID2 VLAN:	Close
۲	Access Controller	User Information	Hide SSID1 Name:	Open	Hide SSID2 Name:	Open
æ	Authentication		SSID rate limit:	Open	SSID rate limit:	Open
ţ. \$↓	Behavior		Guest Mode: Open (Isolate guest	Auto G 36 ( Tri band AP does not support this channel ) (0 (Tri band AP does not support this channel )	Guest Mode:	t devices discovery and access to wired network)
EB	Firewall		SSID3 Name:	40 ( In band AP does not support this channel ) 44 ( Tri band AP does not support this channel )	SSID4 Name:	
	Advanced		SSID3 Security:	48 ( Tri band AP does not support this channel ) 52 ( Tri band AP does not support this channel )	SSID4 Security:	No Password 🗸
0%	C		SSID3 VLAN:	56 ( Tri band AP does not support this channel )	SSID4 VLAN:	Close ~
00	Jervices		Hide SSID3 Name:	60 (Tri band AP does not support this channel )	Hide SSID4 Name:	Open
ß	Log		SSID rate limit:	04 ( In band AP does not support this channel ) 149	SSID rate limit:	Open
			Guest Mode: Open (Isolate guest	153	Guest Mode:	t devices discovery and access to wired network)
				161		
			Channel:	Auto 🗸		
			RF access strategy:	Close ~		
			Min signal/96)(96) -	0 Close		

5.3.5 Group AP Channel selection in 5GHz Radio1 page

	•							~ ~		0. En	alish
mois	CMD-COS-v1.01							ى تى	، دچه T	- "	igiisii
		Access Controller	Access Controller > AP group				∎ <mark>0</mark> : CPU: 3.50	6 🛄 MEM: 16%	↑ TX: 0.00 B/s	👃 RX: 0	0.00 B/s
R	System Overview	Wireless overview	2.4G 5G Radio 1 5G Rad	dio 2 Other Setting							
	Monitoring	AP Configuration	5G Radio 2 Control state								
ŝĝ	System Setup	AP group									- 1
愚	Network	AP Firmware	SSID1 Name:			SSID2 Name:					
		Upgrades	SSID1 Security:	No Password $\lor$		SSID2 Security:	No Password 🗸 🗸				
tit	Flow Control	and white list	SSID1 VLAN:	Close $\checkmark$		SSID2 VLAN:	Close $\sim$				
•	Access Controller	User Information	Hide SSID1 Name:	Open		Hide SSID2 Name:	Open				
<u>a</u> =	Authentication		SSID rate limit:	Open		SSID rate limit:	Open				
t ₹↓	Behavior		Guest Mode:	devices discovery and access to win	ed network)	Guest Mode:	t devices discovery and access to wire	l network)			
臣	Firewall		SSID3 Name:			SSID4 Name:					
Ī	Advanced		SSID3 Security:	Auto 36		SSID4 Security:	No Password $\sim$				
<b>—</b> 8			SSID3 VLAN:	40		SSID4 VLAN:	Close $\lor$				
66	Services		Hide SSID3 Name:	44		Hide SSID4 Name:	Open				
ß	Log		SSID rate limit:	48		SSID rate limit:	Open				
			Guest Mode:	56		Guest Mode:					
			Open (Isolate guest	60	ed network)	Upen (Isolate gues	t devices discovery and access to wire	i network)			
				64							
			Channel:	Auto $\checkmark$							
			RF access strategy:	Close $\checkmark$							
			Min signal(%)(%):	0	Close						

# 5.3.6 Group AP Channel selection in 5GHz Radio2 page

											ి	介	۵.	<u>с</u> в	English	
	CMD-COS-v1.01	Access	Access Controller > AP grou	p						© CPU: 0.009	6 🛄 MEM: 16	6 ↑т.	X: 0.00 B/s	↓ RX	(: 0.00 B/	/s
	='	Controller	2.4G	5G Radio 1	5G Radio 2	Other Setting										^
6)	System Overview	Wireless overview	Paris antija													
<u>-</u>	Monitoring	AP Configuration	basic settini	9												
ŝ	System Setup	AP group		Schedule:	Plan	1										
몲	Network	AP Firmware Upgrades			Plan	2										l
†∔†	Flow Control	Wireless black and white list			Plan	3										
<b>?</b>	Access Controller	User Information		Restart:	Ope	1										
<u>8</u> ,	Authentication			Port 2 VLAN:	Close		~									
↔	Behavior			Port 3 VLAN:	Close		~									
臣	Firewall			Port 4 VLAN:	Close		$\sim$									
	Advanced			Status light:	Ope	1										
	Services			Multiple SSID mod	de: Ope	1										
R	Loa		Foot and in	_												
-	Log		Fast roamin	Ig												
				Fast roaming:	V Oper	۱ (Fast roaming is en	abled in all	bands after tur	ming on)							
					Sav	e Cance	el									V

5.3.7 Group AP Default Other setting page

	CMD-COS-v1.01							4	5	} 1	¢ 2	En	iglish
	=<	Access	Access Controller > AP group	5			📲 CPU: 0.74%	🛄 MEM: 17	7% 个	TX: 48.	00 B/s 🚽	RX: 54	4.00 B/s
6	System	Controller ` Wireless	AP Group										
0-0	Overview	overview									٨dd	Dale	oto
₩	Monitoring	AP Configuration									Add	Dele	ette
ţĊţ	System Setup	AP group	Group name	Number of AP	channel	Maximum belt capacity	SSID		Action	s			
矗	Network	AP Firmware Upgrades	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 N Delete	lanager	ment AP		
tit	Flow Control	Wireless black and white list			56 HadioLi dato	56 Hadiozraninika							
<b>R</b>	Access Controller	User Information	Showing 1 of 1 records			PerPage	20 × Rows	« <	1 >	$\gg$	1 /1	ages	Jump
<u>&amp;</u> =	Authentication		Help: The APs that	join the group use the group co	nfiguration uniformly. A	After the packets are ren	noved, the original	AP configurat	tion is re	estored.			
¢ ₽	Behavior												
Ħ	Firewall												
Ţ	Advanced application												
0% 00	Services												
ľð	Log												

#### 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.

	CMD-COS-v1.01							් ර	¢ 2	English
	=<	Access	Access Controller > AP gro	up			: CPU: 5.20%	☐ MEM: 17% ↑ TX:	0.00 B/s 🔱	RX: 0.00 B/s
	_	Controller	AP Group							
Ð	System Overview	overview								
<u>-</u>	Monitoring	AP Configuration							Add	Delete
ţÇł	System Setup	AP group	Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions		
₼	Network	AP Firmware Upgrades	COMMANDO	1	2.4G: 11 5G Radio1: auto	2.4G: unlimited 5G Radio1: unlimited 5G Radio2: unlimited	2.4G: Net1 2.4G: Net2	Edit Manage Delete	ement AP	
ttt	Flow Control	Wireless black and white list			56 Radio2, auto	50 Nauloz, unimited				
r	Access Controller	User Information	Showing 1 of 1 records			PerPage	20 $\checkmark$ Rows	《 〈 1 〉 》	1 /1Pag	es Jump
8= ;;	Authentication		Help: The APs the	at join the group use the group	o configuration uniformly. A	After the packets are rem	noved, the original AP	configuration is restored	ł.	
⇔	Behavior									
Ħ	Firewall									
y	Advanced application									
0%	Services									
ſð	Log									

5.3.9 Management AP Group page

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

	CMD-COS-v1.01			් රු 👃 🛆 English
	=,	Access	Access Controller > AP group	=☐= CPU: 0.99% 🛄 MEM: 17% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	Svstem	Controller	Management AP COMMANDO	×
6.9	Overview	overview		
₩	Monitoring	AP Configuration	Currently grouped AP Ungrouped AP	
ţĊ	System Setup	AP group	IP/MAC/Model/Remark Q	Shift out group
矗	Network	AP Firmware Upgrades	MAC Address Actions	
ţţţ	Flow Control	Wireless black and white list	No Data	
<b>P</b>	Access Controller	User Information		
<u>&amp;</u> =)	Authentication			
<b>↓</b> ≯	Behavior			
臣	Firewall			
Ţ	Advanced application			
0% 00	Services			
ŀ	Log			

# 5.3.10 Default Management AP Group page

	CMD-COS-v1.01			් ර $\Diamond$ English
	=<	Access	Access Controller > AP group	≣⊑ CPU: 0.00% 🛄 MEM: 17% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
	_	Controller	Management AP COMMANDO	×
$( \mathbf{f} )$	System Overview	Wireless overview		
∽	Monitoring	AP Configuration	Currently grouped AP Ungrouped AP	
ţĊ	System Setup	AP group	IP/MAC/Model/Remark Q	Join group
₼	Network	AP Firmware Upgrades	MAC Address Actions	
ţţţ	Flow Control	Wireless black and white list	08:9b:4b:99:a3:94 Join group	
<b>P</b>	Access Controller	User Information	Showing 1 of 1 records	PerPage 20 $\checkmark$ Rows $\ll$ < 1 > $\gg$ 1 /1Pages Jump
<u>&amp; =</u>	Authentication			
₩	Behavior			
田	Firewall			
Ţ	Advanced application			
0%	Services			
ſð	Log			

5.3.11 Join Management AP Group page

	CMD-COS-v1.01							් ර ර ර්	English
	=,	Access	Access Controller > AP gro	oup			≣Щ≣ CPU: 6.68% 🛄 MEN	∕l: 17% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
		Controller	AP Group						
Ð	System Overview	Wireless overview							
₩	Monitoring	AP Configuration						Add	Delete
ţĊţ	System Setup	AP group	Group name	Number of AP	channel	Maximum belt capacity	SSID	Actions	
⇔	Network	AP Firmware Upgrades	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	
ttt	Flow Control	Wireless black and white list							
P	Access Controller	User Information	Showing 1 of 1 records			PerPage	20 ~ Rows 《 <	1 > ≫ 1 /1Pa	iges Jump
<u>&amp;</u> =	Authentication		Help: The APs th	at join the group use the group co	onfiguration uniformly.	After the packets are ren	noved, the original AP configur	ation is restored.	
₩	Behavior								
Ħ	Firewall								
Ţ	Advanced application								
0%	Services								
[Å	Log								

# 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

	CMD-COS-v1.01							් 🗘 🗘 L English
	≡<	Access	Access Controller >	AP Firmware Upgrades			🛱 CPU: 18.56%	D MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
Ð	System	Wireless	Access Point Up	grades				
 [M-]	Monitoring	AP Configuration		Q				Upgrade All Batch Upgrade
 کې	System Setup	AP group	MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions 🗌
	Network	AP Firmware Upgrades				No Data		
†∔†	Flow Control	Wireless black and white list						
<b></b>	Access Controller	User Information						
<u>&amp;</u> =	Authentication							
₩	Behavior							
臣	Firewall							
Ţ	Advanced application							
0%	Services							
ſð	Log							

# 5.4.1 Default Upgrade firmware of Access Point page

	CMD-COS-v1.01							් ර ද ළ	English
	=<	Access	Access Controller > A	AP Firmware Upgrades			≣ CPU: 5.25% 🛄 MI	EM: 17% ↑ TX: 27.00 B/s 👃	RX: 27.00 B/s
	_	Controller	Access Point Upg	rades					
Ð	System Overview	overview							
₩	Monitoring	AP Configuration	MAC/Model	Q				Upgrade All Batc	h Upgrade
ţĊţ	System Setup	AP group	MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	
- 	Network	AP Firmware Upgrades	08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade	
†∔†	Flow Control	Wireless black and white list	Showing 1 of 1 reco	rds			PerPage 20 $\checkmark$ Rows $\ll$	< 1 > > 1 /1F	ages Jump
<b></b>	Access Controller	User Information							
<u>&amp; </u>	Authentication								
₩	Behavior								
田	Firewall								
Ţ	Advanced application								
0% 00	Services								
[ħ	Log								

5.4.2 Upgrade firmware of Access Point page

	CMD-COS-v1.01							⊿ û \$	A English
		Access	Access Controller > AP Fir	mware Upgrades			≣∰≣ CPU: 0.50% 🛄 🛛	MEM: 17% ↑ TX: 33.00 B/s	↓ RX: 33.00 B/s
		Controller	Access Point Upgrade	s					
Ð	System Overview	Wireless overview							
~		AP Configuration	MAC/Model C	2				Upgrade All	atch Upgrade
ţĊţ		AP group	MAC Address Cu	urrent Version	Latest Version	Status	AP Remarks	Actions	
	Network	AP Firmware Upgrades	08:9b:4b:99:a3:94 1.	<sup>5.2</sup> Tips				Upgrade	
ţţţ		Wireless black and white list	Showing 1 of 1 records	Are you sure t	o upgrade the firmware v	ersion of AP {0}?	rPage 20 🗸 Rows	≪ < 1 > ≫ 1	/1Pages Jump
<b></b>	Access Controller	User Information		ĺ ĺ					
&= ;,	Authentication				OK Cancel				
⇔	Behavior								
Ħ	Firewall								
Ţ	Advanced application								
0% 00									
ſð	Log								

5.4.3 Upgrade firmware of selected Access Point page

	CMD-COS-v1.01							් ර ද ළ	English
	=,	Access	Access Controller > A	P Firmware Upgrades			≣ <mark>.</mark> ≣ CPU: 8.42% 🛄 N	/IEM: 18% ↑ TX: 27.00 B/s 🚽	, RX: 0.00 B/s
	-	Controller	Access Point Upgr	ades					
$\mathcal{O}$	System Overview	Wireless overview							
₩	Monitoring	AP Configuration	MAC/Model	Q				Upgrade All Batch	Upgrade
ţĝ	System Setup	AP group	MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions	
÷	Network	AP Firmware Upgrades	08:9b:4b:99:a3:94	1.5.5	1.6.6	Normal		Upgrade	
ţţţ	Flow Control	Wireless black and white list	Showing 1 of 1 reco	rds			PerPage 20 $\checkmark$ Rows $\ll$	< 1 > » 1 /1P	ages Jump
<b>P</b>	Access Controller	User Information							
<u>&amp;=</u>	Authentication								
⇒	Behavior							l la nue din n	
臣	Firewall							Upgrading.	
e	Advanced						de	ownloading (IK-X2) firmware: 19	6
Ľ	application						In the pro	cess of upgrading, please ensur	e that the
00	Services						power is k	ept and stop any other operatio	ns on AP!
ſð	Log								Hide

# 5.4.4 Upgrading firmware of selected Access Point page

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

	CMD-COS-v1.01							් 🗘 🗘 🛆 English
	=<	Access	Access Controller >	AP Firmware Upgrades			≣ <b>□</b> ≣ CPU: 19.10% 🛄	MEM: 21% ↑ TX: 27.00 B/s 🤳 RX: 162.00 B,
•	Sustem	Wireless	Access Point Upg	grades				
()	Overview	overview						
₽	Monitoring	AP Configuration	MAC/Model	Q				Upgrade All Batch Upgrade
ţĊ	System Setup	AP group	MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions
ሑ	Network	AP Firmware Upgrades				No Data		
tłt	Flow Control	Wireless black and white list						
R	Access Controller	User Information						
8 <u>=</u>	Authentication							
¢‡	Behavior							Upgrading.
Ħ	Firewall							Postart AB: 08:0b:4b:00:=2:04
,	Advanced application						In the	restart AP: 00:90:40:99:40:99:40:99
0%	Services						power	is kept and stop any other operations on AP!
ß	Log							Hide

5.4.5 Upgrading firmware restarting Access Point page

	CMD-COS-v1.01							<u>م</u> ن	수 <u>온</u> E	nglish
	=<	Access	Access Controller > A	IP Firmware Upgrades			■ CPU: 15.00%	☐ MEM: 19% ↑ TX:	0.00 B/s \downarrow RX:	0.00 B/s
	-	Controller	Access Point Upgr	ades						
6)	System Overview	Wireless overview								
₩	Monitoring	AP Configuration	MAC/Model	Q				Upgrade All	Batch Upgr	ade
ŝ	System Setup	AP group	MAC Address	Current Version	Latest Version	Status	AP Remarks	Actions		
모	Network	AP Firmware	08:9b:4b:99:a3:94	1.6.6	1.6.6	Normal				
000	HELMOIR	Upgrades	08:9b:4b:9e:f4:e3	1.5.7	1.5.9	Normal		Upgrade		
ţţţ	Flow Control	Wireless black and white list						_		
<b></b>	Access Controller	User Information	Showing 1-2 of 2 re	cords			PerPage 20 $\checkmark$ Rows	$\ll$ $\langle$ 1 $\rangle$ »	1 /1Pages	Jump
<u>&amp;</u> =	Authentication									
₩	Behavior									
田	Firewall									
Ş	Advanced application									
0%	Services									
ſð	Log									

## 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

	CMD-COS-v1.01									් ර	) ¢ 2	English
	=,	Access	Access Contro	ller > Wireless black	and white list				📮 CPU: 15.75%	DEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
6	System	Controller Wireless	Wireless bla	ck and white lis								
<u> </u>	Overview	overview		omment O				Add	mport Export	Enable	Disable	Delete
<u>₩</u>	Monitoring	AP Configuration						, ad	Export	Lindbio	Dibabio	Delete
ţĈ	System Setup	AP group	Mode	Terminal MAC address	SSID	АР	week	time	comment	Status	Actions	
矗	Network	AP Firmware Upgrades					No Data	a				
†∔†	Flow Control	Wireless black and white list										
<b></b>	Access Controller	User Information	Help:	AP firmware versio	on 1.5.0 and abo	ove is supported only						
<u>8</u> =	Authentication											
↓	Behavior											
Ħ	Firewall											
Ţ	Advanced application											
0% 00	Services											
ľð	Log											

#### X Access Controller Access Controller > Wireless black and white list Add System Overview Wireless Monitoring ₩ AP Configuration ( Blacklist Mode (Disable the MAC connection specified SSID in the rule) Mode: Whitelist Mode (Only the MAC connection specified in the rule is allowed to have an SSID) \$ System Setup AP group Terminal MAC address: AP Firmwa Upgrades 몲 Network s black **†**∔† Flow Control Access Controller 9 User Information <u>8</u>= Authentication SSID: ~ ÷ all all COMMANDO01\_2G COMMANDO01\_5G COMMANDO02\_2G COMMANDO02\_5G ⇒ Behavior 臣 Firewall Advanced application ⊡ Services Մի ւօց AP: Α 😭 all 🗹 All 🗹 Monday 🗹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Friday 🗹 Saturday ✔ Sunday Week: Time: 00:00-23:59 Remarks: Cancel

## 5.5.1 Default Wireless black and white list page

5.5.2 Add Wireless black and white list page

2	CMD-COS-v1.01						): 🕜 수 온 English
		Access	Access Controller > Wireless black and white list			🔷 CPU: 0.00% 🛛 💭 MEM: 13	7% ↑ TX: 384.00 B/s 🤳 RX: 0.00 B/s
0	System	Wireless	Mode:	Blacklist Mode (Disable the MAC connection	n specified SSID in the rule)		
6-3	Óverview	overview		O Whitelist Mode (Only the MAC connection	specified in the rule is allowed to have an SSID)		
24	Monitoring	AP Configuration	Terminal MAC address:	08:9b:4b:9e:f4:e3			
ĝ	System Setup	AP group					
몵	Network	AP Firmware Upgrades					
111	Flow Control	Wireless black and white list					
	Access Controller	User Information	SSID :	COMMANDO01_2G	COMMAND002_2G		
87	Authentication			COMMAND001_5G COMMAND002_5G	< <niot< th=""><th></th><th></th></niot<>		
Ş	Behavior				< <remove< th=""><th></th><th></th></remove<>		
田	Firewall						
⊡,	Advanced application						
	Services		AP:	<ul> <li>all</li> <li>08:9b:4b:99:a3:94</li> </ul>	08.9b:4b:9e:14:e3		
ቡ	Log				< <niot< th=""><th></th><th></th></niot<>		
					< <remove< th=""><th></th><th></th></remove<>		
			Week:	🗌 All 🗹 Monday 🗹 Tuesday 🗹 Wednesd	ay 🗸 Thursday 🗸 Friday 🗌 Saturday 🗌 Sunday		
			Time:	00:00-23:59			
			Remarks:	MAC blacklisting from SSID			
				Save			

# 5.5.3 Wireless blacklisting for particular MAC page

	CMD-COS-v1.01									£	¢ 2	English
	$\equiv$	Access	Access Control	ller > Wireless black	and white list			= <u></u> = C	CPU: 0.99% 🛄 N	1EM: 17% ↑ TX:	293.00 B/s 🔱	RX: 0.00 B/s
~	System	Wireless	Wireless blac	ck and white lis								
6-9	Overview	overview										
₩	Monitoring	AP Configuration	MAC/SSID/Co	omment Q				Add Import	t Export	Enable	Disable	Delete
ţĊţ	System Setup	AP group	Mode	Terminal MAC address	SSID	АР	week	time	comment	Status	Actions	
÷	Network	AP Firmware Upgrades	BlackList	08:9b:4b:9e:f4	COMMANDO02_2G	08:9b:4b:9e:f4:e3	12345	00:00-23:59	MAC blacklisting	Enabled	Edit Disable Delete	
†∔†	Flow Control	Wireless black and white list							from SSID			
P	Access Controller	User Information	Showing 1 of	1 records				PerPage 20	∨ Rows ∢	< 1 > »	1 /1Pag	Jump
<u>&amp;</u> =	Authentication		Help:	AP firmware version	n 1.5.0 and above is su	aported only						
₩	Behavior											
田	Firewall											
Ţ	Advanced application											
0% 00	Services											
A	log											

## 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

	CMD-COS-v1.01									්	û 4	<u> </u>
	=,	Access	Access Controlle	er > User Informatio	n				ECPU: 1.509	6 🛄 MEM: 169	% ↑ TX: 0.00 B/	's ↓ RX:
		Controller	User Informat	ion								
6)	Overview	overview										
₩	Monitoring	AP Configuration	IP/MAC/SSID	Q All Fre	equency 🗸 All user	rs 🗸						
ţÇ	System Setup	AP group	IP Address $\checkmark$	MAC	AP Infomation	SSID	Signal 🗸	Connect Time	✓ Tx ✓	Rx ∽	Comment	Actions
品	Network	AP Firmware Upgrades					No Data					
ţţţ	Flow Control	Wireless black and white list										
<b>(</b>	Access Controller	User Information										
<u>&amp;</u> "	Authentication											
₩	Behavior											
Ħ	Firewall											
Ī	Advanced application											
0% 00	Services											
լ	Log											

5.6.1 Default User Information page

	CMD-COS-v1.01									۵	<u>ڼ</u>	은 English
	=<	Access	Access Controlle	er > User Information					≡ <b>⊑</b> ≡ CPU: 0.00%	MEM: 19%	↑ TX: 443.00 B/	s 👃 RX: 0.00 B/s
	_	Controller	User Informat	tion								
6	System Overview	Wireless overview										
₩	Monitoring	AP Configuration	IP/MAC/SSID	Q All Freq	quency 🗸 All users	~						
ţĊţ	System Setup	AP group	IP Address $\vee$	MAC	AP Infomation	SSID	Signal 🗸	Connect Time	✓ Tx <	Rx 🗸	Comment	Actions
÷	Network	AP Firmware Upgrades	192.168.0.102	c4:d9:87:a7:ad:46	08:9b:4b:99:a3:94	5G:COMMAN DO02_5G	-56dBm utl	1m 21s	70 B/s	0 B/s	DESKTOP- 70API5S	Details Modify comment
ţţţ	Flow Control	Wireless black and white list	192.168.0.50	20:a6:0c:37:4d:13	08:9b:4b:99:a3:94	5G:COMMAN DO01_5G	-43dBm all	1m 13s	0 B/s	0 B/s	POCOF1- POCOF1	Details Modify comment
<b>P</b>	Access Controller	User Information		(a)					20 V D			(10
<u>&amp;</u> =	Authentication		Showing 1-2 of	r 2 records				PerPage	20 V Rows	~~ <	> >> 1	/TPages Jump
\$	Behavior											
田	Firewall											
Ţ	Advanced application											
0% 00	Services											
ſð	Log											

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

	CMD-COS-v1.01			් 🗘 🗘 English
	=,	Authentication <	Authentication > Captive Portal	≣ CPU: 3.37% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	System	Online Auth	Captive Portal Settings	
(~)	Overview	Users		
₩	Monitoring	Captive Portal	Basic Settings	
ţĊji	System Setup	VPN Server 🗸 🗸 🗸	Web Auth Status: Open	
뷺	Network	Auth Account $~~$	Save	
†∔†	Flow Control	Push Notification $$		
<b>P</b>	Access Controller			
<u>8</u> "	Authentication			
⇔	Behavior			
臣	Firewall			
Ţ	Advanced application			
0% 00	Services			
R	Log			

#### 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.

	CMD-COS-v1.01						් ৫ ද ≗	Engl
	<u></u> ,	Authentication <	Authentication > Captive Portal			≣⊑≣ CPU: 0.50% 🖳	☐ MEM: 16% ↑ TX: 0.00 B/s ↓	RX: 0.0
6)	System Overview	Online Auth Users	Captive Portal Settings					
₩	Monitoring	Captive Portal	Basic Settings					
ţ	System Setup	VPN Server 🗸 🗸 🗸	Web Auth Status:	Open				
♣	Network	Auth Account 🛛 🗸	Opened Auth:	Number	Auth Mode	Tx Rate(KB/s)	Rx Rate(KB/s)	
tłt	Flow Control	Push Notification $$		1	WeChat Auth	0	0	
r	Access Controller			Note:	Before enabling this function, you	upeed to hind the device to the Cloud	mable authentication in the cloud	and
<u>&amp;</u> =	Authentication				complete the authentication conf Multiple devices in the same LAN	iguration. Otherwise, the intranet host ca , after configuring the same authentication	nnot access the external network. on group ID and key, can implement	nt the
⇆	Behavior				user roaming-free authentication	service under multiple gateway devices.		
Ħ	Firewall			Save				
V	Advanced application				-			
0% 00	Services							
[Å	Loa							



#### 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

	CMD-COS-v1.01						් ර ද	2	English
	=<	Authentication <	Authentication > VPN Server > PPPoE Se	rver		∎ <b>∷</b> CPU: 0.25%	🛄 MEM: 16% ↑ TX: 0.	00 B/s 🔱	RX: 0.00 B/s
-		Opline Auth	PPPoE Server Settings						Â
(~)	Overview	Users							
-44	Monitoring	Captive Portal	Basic Settings						
ţĊţ	System Setup	VPN Server	PPPoE Server:	Open					
₼	Network	PPPoE Server	PPPoE Server Name:	COMMANDO					
†∔†	Flow Control	PPTP Server	Server Address:	10.1.1.1	*				
<b></b>	Access Controller	L2TP Server	Preferred DNS:	8.8.8.8	*				-
<u>&amp;=</u>	Authentication	OpenVPN Server	Alternative DNS :	8.8.4.4	*				
₩	Behavior	Auth Account 🛛 🗸	Auth Method:	Local Account Auth	~				
田	Firewall	Push Notification $$	accountOperation:	replaceUser	$\sim$				
	Advanced		Client Address List:				Add		
Ľ	application			IP Address	Local Interfac	ce	Actions		
0%	Services								
ľð	Log				No Data				

Fig 6.3.1 Default PPPoE Server Settings page

	CMD-COS-v1.01					ධ	<u>ጉ</u>		
	=,	Authentication <	Authentication > VPN Server > PPPoE	Server		🛱 CPU: 0.50%	1 TX: 27.0	)	00 B/
	System	Online Auth	PPPoE Server Settings						
6-)	Overview	Users							
₩	Monitoring	Captive Portal	Basic Settings						
ţĊţ	System Setup	VPN Server	PPPoE Server:	Open					
品	Network	PPPoE Server	PPPoE Server Name:	COMMANDOPPPoE					
 [4].4]	Elour Control	DDTD Conver	Server Address:	192.168.200.1	*				
	A	FFTF Selver	Preferred DNS:	8.8.8.8	*				
2	Controller	L2TP Server	Alternative DNS :	8.8.4.4	*				
<u>&amp;=</u>	Authentication	OpenVPN Server	Auth Method	Local Account Auth	~				
⇆	Behavior	Auth Account 🛛 🗸	Automethou.						
	e 11		accountOperation :	replaceUser	$\checkmark$				
⊞	Firewall	Push Notification V	Client Address List:				Add		
y	Advanced application			IP Address	Local Interface	Acti	ons		
0% 00	Services			10.1.1.2-10.1.1.254	lan1	Edit	Delete		
ß	Log								
				Note: If there is no	o need to change, please do no	ot 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

200	CMD-COS- <u>v1.01</u>						
	≡́	Authentication <	Authentication > VP	N Server > PPTP Server			ېې: CPU
0	System	Online Auth	Basic Settings				
ភា	Overview Manitanian	Users		PPTP Server:	Open		
- 22	wonitoring	Captive Portai	:	serverPort:	1723		*
ţĊř	System Setup	VPN Server 🔨		Preferred DNS:	8.8.8.8		*
뮮	Network	PPPoE Server		Alternative DNS :	8.8.4.4		*
111	Flow Control	PPTP Server		Client IP Address List:	10.0.0.2-10.0.0.254		
۴	Access Controller	L2TP Server					
8= ;	Authentication	OpenVPN Server					
₩	Behavior	Auth Account $\sim$					
臣	Firewall	Push Notification $ arsine{}$	Advanced Settings ^	×			
	Advanced application			MPPE Data Encountion	Ontional Encountion		
0% 00	Services			inite bata energenon.	No encryption: If the	client needs encryption, the server w	] ill be disconnected, the connection speed will be faster without encryption the connection speed will be faster without encryption
ሴ	Log				Requires encryption: i	if the client refuses, server will be dis	connected
_				Server Address:	10.0.0.1		*
				MTU:	1400	*	
				MRU:	1400	*	
					Save		

6.3.3 Default PPTP Server Settings page

3	CMD-COS-v1.01							۵	<u>۵</u>	2	English
	≡<	Authentication <	Authentication > VPN S	Server > PPTP Server			🤹 CPU: 0.75% 🛄 N	1EM: 19%	↑ TX: 0.0	0 B/s ↓	RX: 0.00 B/s
6	System	Online Auth	PPTP Server Setting	gs							
FAA	Monitoring	Users Captive Portal	Basic Settings								
	System Setun	VPN Server	PP	PTP Server:	✔ Open						
응	Network	PPPoF Server	se	erverPort:	1723	•					
600	Flow Control		Pn	referred DNS:	8.8.8.8	]•					
	Access		Alt	Iternative DNS :	8.8.4.4	*					
E E	Controller	LZTP Server	Cli	lient IP Address List:	192.10.0.2-192.10.0.254						
( <u>e</u> .)	Autientication	OpenVPIN Server									
, ₹	Behavior	Auth Account $\sim$									
盟	Firewall	Push Notification $\smallsetminus$									
Ţ	Advanced application		Advanced Settings ^								
	Services		м	IPPE Data Encryption:	Need Encryption						
ß	Log				No encryption: If the client needs encryption, the server w Optional encryption: can be connected without encryption Requires encryption: if the client refuses, server will be dis	) If be disconnected, the connection speed will be faster without enc the connection speed will be faster without encryption onnected	ryption				
			Se	erver Address:	10.0.0.1	*					
			M	ITU:	1400 *						
			м	IRU:	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

	CMD-COS-v1.01				් 🗘 🗘 ළ English
	_<	Authentication <	Authentication > VPN Server > L2TP Serv	/er	📲 CPU: 0.25% 🔛 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
ଚ	System Overview	Online Auth Users	L2TP Server Settings		^
₩	Monitoring	Captive Portal			
ţĊţ	System Setup	VPN Server ^	L2TP Server:	✓ Open	
÷	Network	PPPoE Server	serverPort:	1701	•
tit	Flow Control	PPTP Server	Client IP Address List:		
<b></b>	Access Controller	L2TP Server	Preferred DNS:		) *
&= ;;	Authentication	OpenVPN Server	Alternative DNS :		
\$↓	Behavior	Auth Account 🛛 🗸	MTU:	*	
Ħ	Firewall	Push Notification $$	MRU:	*	
Ţ	Advanced application		Pre-shared Key:		
0% 00	Services		Deny non-encrypted connections:	✓ Open	
ß	Log				
				Save	

Fig 6.3.5 Default L2TP Server Settings page

смд-соз-v1.0	1			රා 🗘 🔔 English
=<	Authentication <	Authentication > VPN Server > L2TP Server		=Ös CPU: 0.25% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
- Suctors	Online Auth	L2TP Server Settings		
Overview	Users			
Monitoring	Captive Portal			
දිාලි System Setup	VPN Server	L2TP Server:	✓ Open	
品 Network	PPPoE Server	serverPort:	1701	
HI Flow Control	PPTP Server	Client IP Address List:	192.1.0.2-192.1.0.254	•
Access		Server Address:	172.1.0.1	*
Controller	LZTP Server	Preferred DNS:	8.8.8	*
Authentication	OpenVPN Server	Alternative DNS :	8.8.4.4	•
🕁 Behavior	Auth Account $\sim$	MTU:	*	
E Firewall	Push Notification $$	MRU:	1400 *	
Advanced application		Pre-shared Key:	commando	
다. Services		Deny non-encrypted connections:	Open	
Log				
			Save	

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

DMD-CDS-v1.01						
≡•	Authentication <	Authentication > VPN Server > 0	penVPN Server			
ystem	Online Auth		Export windows client	configuration	Show log Restore defa	ult
view	Users		Open//PN Server:	Open		
laring	Captive Portal		Server Port:	1194		
Setup	VPN Server		VPN Segment:	10.7.7.0		
Ł	PPPoE Server		Subnet Mask:	255.255.255.0		~
ntrol	PPTP Server		Tunnel Protocol :	NDb		~
ler	L2TP Server		Tunnel Type:	TUN		~
tication	OpenVPN Server		Topology type:	SUBNET		~
ar	Auth Account 🔍		Encryption Algorithm:	BF-CBC		~
	Push Notification $\sim$		LZO Compression:	🗸 Open		
ed ion			MTU:	1400		
			CA Certificate:	8EGIN CERT MIIDQTCCAimg/ GSIb3DQEBCwU BAYTAkNOMQ4	IFICATE WilBagUAOrD5EkIB39uMA0GCSq AMDcsiCzAJBgNV wDAYDVQQKDAVpS3VhaTEYMBY	^
				GA1UEAwwPaUt M84XDTE4MDU 2MDAyMFowNu	1YWkgRGV2xWNIENB zMTE2MDAgMFsXDTI4MDUyODE ELMAkGA1UEBhMCQ04x	~
			Server Certificate:	88GIN CERT MIICGCCAdICBF wNzELMAkGA1L 8gNV8AoMBWIL baSBEZXZoY2Uo	IFICATE iQHBQwDQYJKoZIhwcNAQELBQA IEBINMCQ04xDJAM LdWFpMRgwFgYDVQQDDA9pS3V ;005wHhcNMTowHTMx	^
				MTYwMDiwWho wCQYDVQQGEw	NMjgwNTI4MTYwMDIwWjABMQs JDTjEOMAwGA1UECgwF	$\checkmark$
			Server Private Key:	8EGIN RSA. MILEowIBAAKCA UprONhvsAhoh 9pZWimXORBbyl /SUGQ2ioopij2F j9KVJHH++CKoo OYtorF32GeWXXX	PRIVATE KEY QEAsiN9UcuIFwm8YvqQF62m6Cx QES7W8jPbgU ba3ih8qr0WU9c6SmtTPXKdAwV4 bi7ySPVNN44d dqY3HS+IQU7XJM0AabDqPLHidB 6/VBNcaAO2	< ·
			Push Route:			
				IP Address	Subnet Mask	Actions
				10.7.0.0	255,255,0.0(16)	Edit Dele
			Additional Configuration:	Additional config	uration example: tcp-queue-limit mtu-disc no	22
				Silve		

# Fig 6.3.7 Default OpenVPN Server Settings page

	СМД-СО5-v1.01							۵	<u>ත</u> ර	û ↓	ے û û 4	<u>ර</u> ර 4 ප	ے û 4 ک	스> 슈 슈 ዶ Eng	තා 🖒 🗘 🛎 Engli	스) 슈 스 온 English
	=,	Authentication <	Authentication > VPN Server > OpenVPN S	Server		i CPU: 0.00	%	% 🛄 MEM: 19%	% 🛄 MEM: 19% ↑ TX	% 🛄 MEM: 19% ↑ TX: 0.00 B/s	% 🛄 MEM: 19% ↑ TX: 0.00 B/s 🗸	% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓	% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ R>	% 🛄 MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.	% 🛄 MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00	% 🛄 MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00 F
_		Online Auth	OpenVPN Server Settings													
69	Overview	Users														
₩	Monitoring	Captive Portal														
÷	System Setup	VPN Server 🔷	Export windows client	configuration Show log	Restore default											
品	Network	PPPoE Server	OpenVPN Server:	Open												
(†14	Flow Control	PPTP Server	Server Port:	1194	*											
	Access	1070 5	VPN Segment:	192.160.7.0	*											
<u> </u>	Controller	L2TP Server	Subnet Mask:	255.255.255.0	$\sim$											
8	Authentication	OpenVPN Server	Tunnel Protocol:	ТСР	$\sim$											
₩	Behavior	Auth Account 🤍	Tunnel Type :	TUN	~											
臣	Firewall	Push Notification $\checkmark$	ranner type.		~											
	Advanced		Topology type:	SUBNET	$\sim$											
- 🖓	application		Encryption Algorithm:	BF-CBC	$\sim$											
04	Services		LZO Compression:	Open												
P	Log		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

	CMD-COS-v1.01		් 🗘 🗘 ළ English
	=,	Authentication <	Authentication > Auth Account > Account 🖞 CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System	Online Auth	Manage Account
FAA	Overview Monitoring	Users Captive Portal	Total condition V All time V All auth V Please input account, name, Q
Č	System Setup	VPN Server V	Add Import Export Enable Delete
品	Network	Auth Account 🛛 🔿	Account 🗸 Username Y Auth type Current type Due time Y Recently Y Remarks Status Actions 🗌
†∔†	Flow Control	Package	No Data
<b></b>	Access Controller	Account	
<u>&amp;</u> =)	Authentication	self password management	
\$ \$	Behavior	General Ledger	
Ħ	Firewall	Access Code	
Ţ	Advanced application	Push Notification $$	
0%	Services		
ſð	Log		

Fig 6.4.1 Default Manage Package Account page

COMMAN	CMD-COS-v1.01				
	=<	Authentication <	Authentication > Auth Account > Account	t	📲 CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
~	Sustam	Opline Auth	Add		×
6-9	Overview	Users			
₩	Monitoring	Captive Portal	Online account configuration		
ŝ	System Setup	VPN Server 🛛 🗸	Account:		
튧	Network	Auth Account 🛛 🔿	Password:	©	*
<u>†</u> ††	Flow Control	Package	Auth type:	Any	
۲	Access Controller	Account	Package type:	Choice	•
<u>&amp;</u> =	Authentication	self password management	Up speed:	0	KB/s *
⇆	Behavior	General Ledger	Down rate:	0	KB/s *
臣	Firewall	Access Code	Start time:	2021-04-10 20:10:15	
V	Advanced	Push Notification $$	Due time:	Select Date	
0%	Services		Payment amount:		
ß	Log		Share:	*	

Fig 6.4.2 Add Online Account configuration page

	CMD-COS-v1.01				스) 슈 오 English
	Ξ́	Authentication <	Authentication > Auth Account > Packag	e	📲 CPU: 1.50% 🛄 MEM: 19% ↑ TX: 0.00 B/s \downarrow RX: 0.00 B/s
Ð	System Overview	Online Auth Users	Add		×
₫⁄	Monitoring	Captive Portal			
ţĈ	System Setup	VPN Server 🛛 🗸	Package Name:	COMMANDO	*
Ē	Network	Auth Account 🛛 🔿	Period Type:	Hour	
ţ†	Flow Control	Package	Validity:	20	*
<b></b>	Access Controller	Account	Package Price:	200	
<u>&amp; </u>	Authentication	self password management	Rx Limit(KB/s):	1000	*
$\stackrel{\leftarrow}{\Rightarrow}$	Behavior	General Ledger	Remarks:	COMMANDO Package	
臣	Firewall	Access Code			
Ţ	Advanced application	Push Notification \vee		Save Cancel	
0% 00	Services				
R	Log				

Fig 6.4.3 Add particular Online Account configuration page
	CMD-COS-v1.01								_ ර	) ¢ 2	English
	=<	Authentication <	Authentication > A	uth Account > Packag	le			© CPU: 0.5	0% 🛄 MEM: 19%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
		0-1 4.4	Manage Package	2							
$( \cdot )$	Overview	Users									
∽	Monitoring	Captive Portal							Add Import	Export	Delete
ţĊ	System Setup	VPN Server 🗸 🗸 🗸	Package Name	Validity	Period Type	Package Price	Tx Limit(KB/s)	Rx Limit(KB/s)	Remarks	Actions	
₼	Network	Auth Account 🛛 🔨	COMMANDO	20	Hour	200	1000	1000	COMMANDO Package	Edit Copy Delet	e 🗌
tit	Flow Control	Package	Showing 1 of 1 red	ords			PerPag	ge 20 V Row	s « < 1 >	≫ 1 /1Pag	es Jump
	Access Controller	Account									
8= ;;	Authentication	self password management									
<b>↓</b> ≯	Behavior	General Ledger									
₿	Firewall	Access Code									
Ţ	Advanced application	Push Notification $$									
0%	Services										
ſŊ	Log										

## 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

	CMD-COS-v1.01		스) 샵 🗘 English
	_<	Authentication <	Authentication > Auth Account > Account > Account 🖞 TX: 0.00 B/s \downarrow RX: 0.00 B/s
	System	Online Auth	Manage Account
(~)	Overview	Users	
₩	Monitoring	Captive Portal	Total condition V All time V All auth V Please input account, name, Q
ţĊ	System Setup	VPN Server 🗸 🗸 🗸	Add Import Export Enable Disable Delete
₼	Network	Auth Account 🛛 🔨	Account $\checkmark$ Username $\checkmark$ Auth type Current type Due time $\checkmark$ Recently $\checkmark$ Remarks Status Actions $\Box$
tit	Flow Control	Package	No Data
<b></b>	Access Controller	Account	
<u>8</u> "	Authentication	self password management	
$\downarrow$	Behavior	General Ledger	
Ħ	Firewall	Access Code	
Ţ	Advanced application	Push Notification $$	
0%	Services		
ß	Log		

Fig 6.4.5 Default Mange Account page

	CMD-COS-v1.01					ධ	습 👃 😤 English
	<u></u> _<	Authentication <	Authentication > Auth Account > Account			🛱 CPU: 0.25% 🛄 MEM: 19%	↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
			Add				×
A	System Overview	Online Auth Users					
₩	Monitoring	Captive Portal	Online account configuration				
ţÇ	System Setup	VPN Server 🗸 🗸 🗸	Account:		*		
品	Network	Auth Account 🛛 🔿	Password:		*		
†∔†	Flow Control	Package	Auth type:	Any	~		
۲	Access Controller	Account	Package type:	Choice	*		
<u>8</u> .	Authentication	self password management	Up speed:	0	KB/s *		
₩	Behavior	General Ledger	Down rate:	0	KB/s *		
臣	Firewall	Access Code	Start time:	2021-05-08 23:19:35	*		
V	Advanced application	Push Notification $$	Due time:	Select Date	0		
പര			Payment amount:				
ŏõ	Services		Share -	*			
P.	Log		Share.				
-11	Log		Bind VLAN:	0 *			
				The default value is 0,Only support PPPoE,support QinC	如: 2008.100		
				Auto VLAN			

Fig 6.4.5 Add Manage Account page

X	CMD-COS-v1.01				තා රු 🗘 💄 English
	≡<	Authentication <	Authentication > Auth Account > Account		tin CPU: 0.25% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
Ð	System Overview	Online Auth Users	Binding NIC:	Only support PPPoE	
₩	Monitoring	Captive Portal	Binding MAC:	Manual	
ţĊţ	System Setup	VPN Server 🗸 🗸	MAC addr:		
品	Network	Auth Account			
†∔†	Flow Control	Package			
<b>P</b>	Access Controller		Eived ID -	Add a MAC, enter a MAC every line	
<u>&amp;</u> "	Authentication	self password management	TROUT.		
⇒	Behavior	General Ledger	Online customer information		
Ħ	Firewall	Access Code	Username:		
y	Advanced application	Push Notification $ \smallsetminus $	ID number :		
0% 00	Services		Telephone :		
Ъ	Log		Addr:		
			Remarks:		
				Save Cance	

Fig 6.4.6 Add Online account configuration page

	CMD-COS-v1.01				ත 🗘 🗘 L English
	≡<	Authentication <	Authentication > Auth Account > Account		i CPU: 0.25% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	System	Online Auth	Online account configuration		
6.9	Overview	Users	Account:	COMMANDOAC	•
₩	Monitoring	Captive Portal	Password:		×
ŝ	System Setup	VPN Server 🗸 🗸	Auth type:	12TP	
よ	Network	Auth Account	Designed to an	Ô unha m	
			Package type:	Custom	
111	Flow Control	Package	Up speed:	100	KB/s *
<b>P</b>	Access Controller	Account	Down rate:	50	KB/s *
<u>8</u> "	Authentication	self password management	Start time:	2021-05-08 23:19:35	) *
⇔	Behavior	General Ledger	Due time:	2021-05-22 23:23:40	
臣	Firewall	Access Code	Payment amount:	2000	
V	Advanced application	Push Notification $$	Share :	1 *	
0%	Services		Fixed IP:	223.145.3.134	
Ъ	Log				



	CMD-COS-v1.01								<u> </u>	) <b>4</b> 8	English
	=<	Authentication <	Authentication > A	uth Account > Account	t			: <u>Ö</u> : (	PU: 0.50% 🛄 MEM: 19%	↑ TX: 0.00 B/s 👃	RX: 0.00 B/s
-		Online Auth	Manage Account	t							
69	Overview	Users									
<u>-</u>	Monitoring	Captive Portal	Total conditdion	<ul> <li>✓ All time</li> </ul>	<ul> <li>All auth</li> </ul>	✓ Please input ac	count, name, Q	Add Import	Export Enable	Disable	Delete
ţĊ	System Setup	VPN Server 🗸 🗸	Account $\checkmark$	Username 🗸	Auth type	Current type	Due time $ \smallsetminus $	Recently online $\checkmark$ Remarks time	Status	Actions	
品	Network	Auth Account	COMMANDOAC	2tpCOMMANDO1	L2TP	Custom	2021-05-29 23:27:43		Yes	Detail Charge Edit Disable	
tłt	Flow Control	Package								Delete	
P	Access Controller	Account	Showing 1 of 1 rec	cords				PerPage 20	Rows 《 < 1 〉	>> 1 /1Pag	es Jump
8.	Authentication	self password management									
¢‡	Behavior	General Ledger									
臣	Firewall	Access Code									
y	Advanced application	Push Notification $$									
0% 00	Services										
Ъ	Log										

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

	CMD-COS-v1.01				📩 🖒 🗘 L English
	⊒<	Authentication <	Authentication > Auth Account > self passwor	rd management	🛱 CPU: 2.50% 🛄 MEM: 15% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
6	System	Online Auth	self password management		
₩	Monitoring	Captive Portal	Self-correcting password:	Open	
ţţ	System Setup	VPN Server 🗸 🗸	Self-correcting password address:	6.6.6.6	
÷	Network	Auth Account 🛛 🔿	Allow PPPOE users to change passwords:	Open	
t†	Flow Control	Package	Allow L2TP users to change passwords:	✓ Open	
<b></b>	Access Controller	Account	Allow PPTP users to change passwords:	V Open	
<u>&amp;=</u>	Authentication	self password management	Allow OPENVPN users to change passwords:	Open	
\$	Behavior	General Ledger	Allow WEB users to change passwords:	√ Open	
田	Firewall	Access Code	Cave	Cancel	
Ţ	Advanced application	Push Notification 🗸		Cancer	
0% 00	Services				
ľ	Log				

## Fig 6.4.9 Default self password management page

	CMD-COS-v1.01			
=	<	Authentication <	Authentication > Auth Account > self password	management
S	ystem	Online Auth Users	self password management	
	Monitoring	Captive Portal	Self-correcting password:	Open
	System Setup	VPN Server 🗸 🗸	Self-correcting password address:	6.6.6.6
	Network	Auth Account $\land$	Allow PPPOE users to change passwords:	🗸 Open
ł	Flow Control	Package	Allow L2TP users to change passwords:	Open
	Access Controller	Account	Allow PPTP users to change passwords:	🗸 Open
1	Authentication	self password	Allow OPENVPN users to change passwords:	Open
	Behavior	management General Ledger	Allow WEB users to change passwords:	Open
3	Firewall	Access Code	Save	Cancel
3	Advanced application	Push Notification $$		
	Services			
5	Log			

## 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

000	CMD-COS-v1.01								්	û \$ \$	English
	=<	Authentication <	Authentication > Au	th Account > Genera	l Ledger			© CPU: 0.00%	MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	_		Viewing General I	edger							
6	System Overview	Users									
₩	Monitoring	Captive Portal	Total money: 0	Begin Time	() End Time	e ()		ount/Charge personn Q		Export	Delete
ŝ	System Setup	VPN Server 🗸 🗸 🗸	Account	Username	Charge time 🗸	Fee collector	Description	Charge Amount $\checkmark$	Remarks	Actions	
쁆	Network	Auth Account 🛛 🔿					No Data				
ţţţ	Flow Control	Package									
<b>(</b>	Access Controller	Account	Help	tip: keep only the la	st three months of dat	a200000Rows					
<u>&amp;=</u>	Authentication	self password management									
₩	Behavior	General Ledger									
Ħ	Firewall	Access Code									
Ţ	Advanced application	Push Notification $$									
0% 00	Services										
Ռ	Log										

## Fig 6.4.11 Default General Ledger page

	CMD-COS-v1.01								ය (	¢ (	A English
	=,	Authentication <	Authentication > Aut	th Account > General	Ledger			📮 CPU: 1.98%	🛄 MEM: 19% ↑ 1	TX: 3.63 KB/s	↓ RX: 47.16 KB/s
	_		Viewing General L	edger							
6)	Overview	Users									
₹	Monitoring	Captive Portal	Total money: 2000	Begin Time	() End Tir	me 🕓	Account/User account	t/Charge personn Q		Export	Delete
ţĊţ	System Setup	VPN Server 🛛 🗸	Account	Username	Charge time $\checkmark$	Fee collector	Description	Charge Amount $ imes$	Remarks	Actions	
♣	Network	Auth Account 🛛 🔿	COMMANDOAC	l2tpCOMMANDO1	2021-05-08 23:28:06	admin	account opening	2000	Custom,account expiration time:2021-05-29,	Delete	
tŧŧ	Flow Control	Package									
<b>(</b>	Access Controller	Account	Showing 1 of 1 reco	ords			PerPag	e 20 $\checkmark$ Rows	《 〈 1 〉	≫ 1	/1Pages Jump
<u>&amp;=</u>	Authentication	self password management	Help	tip: keep only the last	t three months of da	ta200000Rows					
₩	Behavior	General Ledger									
Ħ	Firewall	Access Code									
Ţ	Advanced application	Push Notification $$									
0%	Services										
ſð	Log										

## 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

	CMD-COS-v1.01					්	û 4 2	English
	=,	Authentication <	Authentication > Auth Account > Access Code			📮 CPU: 0.25% 🛄 MEM: 1	6% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	_		Manage Access Code					
Ð	System Overview	Users						
₩	Monitoring	Captive Portal	×		Add Batch Access Code	Delete failed Access (	Code Delete	Export
ŝ	System Setup	VPN Server $\sim$	Access Code code Expiring time	Time limit	Record	Remarks	Actions	
品	Network	Auth Account 🛛 🔨			No Data			
ţ†	Flow Control	Package						
۲	Access Controller	Account						
<u>8</u>	Authentication	self password management						
₩	Behavior	General Ledger						
臣	Firewall	Access Code						
Ţ	Advanced application	Push Notification $$						
0% 00	Services							
Ŀ	Log							

Fig 6.4.13 Default Manage Access Code page

	CMD-COS-v1.01				🛆 🟠 🖨 English
	=,	Authentication <	Authentication > Auth Account > Access C	ode	🛱 CPU: 0.00% 🛄 MEM: 19% ↑ TX: 0.00 B/s \downarrow RX: 0.00 B/s
	Surton	Opling Auth	Add		×
6-3	Overview	Users			
₹	Monitoring	Captive Portal			
ţĊţ	System Setup	VPN Server 🗸 🗸 🗸	Access Code code :	HYE4W4F8LL	
뷺	Network	Auth Account	Expiring time :	2021-05-12 16:02:59	
[†∔†]	Flow Control	Package	Time limit:	48 hour 0 minute	
<u></u>	Access Controller	Account	Remarks:	Internet Access	
&= ;;	Authentication	self password management		Save Cancel	
₩	Behavior	General Ledger			
Ħ	Firewall	Access Code			
Ţ	Advanced application	Push Notification $$			
0%	Services				
ß	Log				

Fig 6.4.14 Add Manage Access Code page

	CMD-COS-v1.01						c	⊃ û ¢ ′	C English
	=<	Authentication <	Authentication > Auth Acc	ount > Access Code			📲 CPU: 1.75% 🛛 🛄 MEM: 1	9% ↑ TX: 52.08 KB/s	↓ RX: 4.86 KB/s
		Opling Auth	Manage Access Code						
6)	Overview	Users							
₩	Monitoring	Captive Portal	~			Add Batch Acc	cess Code Delete failed Acce	ess Code Delete	Export
ţĊ	System Setup	VPN Server $\checkmark$	Access Code code	Expiring time	Time limit	Record	Remarks	Actions	
æ	Network	Auth Account 🛛 🔨	HYE4W4F8LL	2021-05-12 16:02:59	48Hour0Minute	Unused	Internet Access	Edit Delete	
†∔†	Flow Control	Package	Showing 1 of 1 records			Per	Page 20 $\checkmark$ Rows $\ll$ <	1 > » 1 /	1Pages Jump
<b></b>	Access Controller	Account							
<u>&amp;</u> =	Authentication	self password management							
⇆	Behavior	General Ledger							
臣	Firewall	Access Code							
Ţ	Advanced application	Push Notification $$							
0%	Services								
ß	Log								

## 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

2	CMD-COS-v1.01			ත් ර 👃 🕹 English
	=<	Authentication <	Authentication > Push Notification > Real-time	♦ CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
	-	Online Auth	Real-time Notification Settings	
ଚ	Overview	Users		
₩	Monitoring	Captive Portal		
ø	System Setup	VPN Server $\sim$	Inform content:	
ᇔ	Network	Auth Account $\sim$		
111	Flow Control	Push Notification		
2	Access Controller	Real-time		
8.	Authentication	Periodic		
⇆	Behavior	Expiration Reminder		
₿	Firewall	Dial-up User Expiration		
	Advanced			~
88	Services			Page jumps
R	Log		Jump page:	http://www.google.com
Ű			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
				kom>>
				No Group Add Group Once configured, plans. Refersh
				v v
			Countdown:	50 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-

Fig 6.5.1 Default Real-time Notification Settings page

-	CMD-COS-v1.01			
	≡<	Authentication <	Authentication > Push Notification > Real-time	
ଚ	System Overview	Online Auth Users	Inform content:	H B $I \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $
~	Monitoring	Captive Portal		
ŝ	System Setup	VPN Server 🗸 🗸		
몲	Network	Auth Account $\sim$		
141	Flow Control	Push Notification		
۹	Access Controller	Real-time		
<u>e</u> .	Authentication	Periodic		
∽	Behavior	Expiration Reminder		
臣	Firewall	Dial-up User Expiration		Page jumps
Ţ	Advanced application		Jump page:	http://www.google.com
	Services		Receive unique objects:	Dial user(Dial-up users push notifications when online)
ሌ	Log			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 < <remove configured,="" once="" please="" refresh<="" th=""></remove>
			Countdown:	3500 \$ 0s means no countdown is enabled; no countdown time is set, or a confirmation bu time notification function with caution.
				Save and send

## 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

	CMD-COS-v1.01							් ර අ ළ	English
	<u> </u>	Authentication <	Authentication > Push	Notification > Periodic			≣ <b>□</b> ≣ CPU: 0.00% □	MEM: 16% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	System	Online Auth	Periodic Notificatio	n Settings					
6-3	Overview	Users							
₩	Monitoring	Captive Portal						Add	Delete
ŝ	System Setup	VPN Server 🗸 🗸 🗸	Receiving object	Delivery cycle	Time	Remarks	Status	Actions	
矗	Network	Auth Account 🛛 🗸				No Data			
ţţţ	Flow Control	Push Notification \land							
<b>?</b>	Access Controller	Real-time							
<u>&amp;</u> =)	Authentication	Periodic							
₩	Behavior	Expiration Reminder							
₿	Firewall	Dial-up User Expiration							
Ţ	Advanced application								
0%	Services								
ቡ	Log								

## Fig 6.5.3 Default Periodic Notification Settings page

2	OMD-CD5-v1.01			
		Authentication <	Authentication > Push Notification > Periodic	ġ.
~	System	Online Auth	Add	
(~)	Overview	Users	Notice contents	
2	Monitoring	Captive Portal	PUBLIC CONTRACT	
٩	System Setup	VPN Server 🗸 🗸		
볿	Network	Auth Account $\sim$		
tit	Flow Control	Push Notification		
1	Access Controller	Real-time		
<u>85</u>	Authentication	Pwiedic		
\$	Behavior	Expiration Reminder		
Ħ	Firewall	Dial-up User Expiration		~
⊲	Advanced			
04	Samiras			Pagajanga
00 N			Page jump:	•
40	Log		Delivery cycle:	🕐 All 💆 Monday 💋 Taeeday 🖉 Wedeweday 💽 Thanday 🔯 Friday 😨 Standay
			Time:	*
			Receiving object:	C Dai particle up over pub rollications when period
				internet user in the list/Add the IP address required to push notifications in the following list)
			IP:	Un 11 for (P range
				In four Address
				Concernentlypered, gives- Fadwah
			Remarks:	
			Countdown:	0 s the means no countidown is unabled, no countidown time is say, or a confirmation bottom on the notification page is measurily clicked suring the countidown time, otherwise port 10 will be bljacked all the time. Please say the read-time notification function with caucitors.
				Som Canad

#### \* Push Notification > Periodi 🖞 (CPU: 6.93%) 🛄 MEM: 19% 个 TX: 11.09 KB/s 🤳 RX: 32.12 KB нв I ⊻ Ø I ∂ ⊟ ≣ 6 3 Hello User You are using COMMANDO N Expiration Reminder Dial-up Us Expiration Page jump: http://www.google.com 🗸 All 🔽 Monday 🗹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Friday 🗹 Saturday 🗹 Sunday Delivery cy Dial user(Dial-up users push notifications when online) Intranet user in the list(Add the IP address required to push notificati 192.168.0.0/24 COMMANDO Push Notification

## Fig 6.5.4 Add Periodic Notification Settings page

## Fig 6.5.5 Periodic Notification Settings page

## **Expiration Reminder Settings:**

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

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

X	CMD-COS-v1.01			ත් 🗘 🛆 🐣 English
			Authentication > Push Notification > Expiratio	n Reminder
		Authentication <	Expiration Reminder Settings	
ଚ	System Overview	Online Auth Users		
<b>6</b> /4	Monitoring	Captive Portal	Expire notice:	🗹 Open
£Ç‡	System Setup	VPN Server 🗸 🗸	Notice content:	$H  B  I  \sqcup  \emptyset  \mathscr{A}  \mathscr{O}  \boxplus  \blacksquare \\$
E	Network	Auth Account $\qquad \lor$		Dear User,
=	Flow Control	Push Notification \land		con toesoen en toe a soot to express one parties and the soot of t
2	Access Controller	Real-time		My Broadband Service Provider details:
<u>8</u> = -	Authentication	Periodic		Customer Service Telephone No.: Customer Service Email ID:
\$	Behavior	Expiration Reminder		Website: Address:
臣	Firewall	Dial-up User Expiration		Thank you.
	Advanced application			Regards, 🗸
	Services			Page jumps
	Log			
			Page jump:	http://www.google.com
			Prematurity reminder:	5 days
			Regularly remind :	08.00 , 16.00 ,
			Countdown:	60 \$ 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

-				
	D-COS-v1.01			
		Authentication <	Authentication > Push Notification > Expiration	Reminder
System	n	Online Auth	Expiration Reminder Settings	
Overvie	iew	Users		
Monito	oring	Captive Portal	Expire notice:	Open
ැටූ System	n Setup	VPN Server $\sim$	Notice content:	H B I ⊻ Ø I ♂ ☷ ☷
品 Networ	ork	Auth Account 🛛 🗸		Dear User,
HI Flow C	Control	Dush Notification		Your broadband service is about to expire, the system will stop the
Arress		Push Notification		disconnection, Please contact your broadband service provider for
Contro	oller	Real-time		renewal.
율 Authen	ntication	Periodic		Thank you.
😓 Behavio	ior	Expiration		Regards,
E Firewal		Dial-up User		COMMANDO Team
	"	Expiration		
applica	ation			
Service	es			
Log				Page jumps
			Page jump:	http://www.google.com
			Prematurity reminder:	5 days
			Regularly remind:	08:00
			Countdown:	60 \$ 0s means no countdown is enabled; no countdown tim

## Fig 6.5.7 Expiration Reminder Settings page

## **Dial-up User Expiration Notification:**

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

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



Fig 6.5.8 Default Dial-up User Expiration Notification page

2	CMD-COS-v1.01				ැ. රු ද ළ English
		Authentication <	Authentication > Push Notification > Dial-up User E	xpiration	🔷 CPU: 0.25% 🔛 MEM: 19% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
0	System	Online Auth	Dial-up User Expiration Notification Settings		
6-3	Overview	Users			
24	Monitoring	Captive Portal	Notice content:	$\mathbb{H}  \mathbb{B}  I  \  \  \  \  \  \  \  \  \  \  \  \  \$	
÷	System Setup	VPN Server 🗸 🗸		Dear User,	
몶	Network	Auth Account $\sim$		Your broadband service has expired, the expiration time is \$200 on dated 05/05/2021, please apply for renewal procedures.	
111	Flow Control	Push Notification		My Broadband Service Provider details:	
8	Access Controller	Real-time		Thank you.	
<u>e</u> .	Authentication	Periodic		Regards, COMMANDO Team	
\$	Behavior	Expiration Reminder			
臣	Firewall	Dial-up User Expiration			
,	Advanced application				
	Services		White list public net IP:	192.168.0.0/24	
۳h	Log				
			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.	
				Page jumps	
				Save	

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

0000	CMD-COS-v1.01			C) T I A English
	≡<	Behavior <	Behavior > Behavior Audit > Activate Audit	≣ CPU: 0.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
-	Sustan	^	Behavior Audit Settings	
63	Overview	Behavior Audit 🔿		
₩	Monitoring	Activate Audit	Behavior record configuration	
ŝ	System Setup	Record-free setting		
÷	Network	Web Browsing	Website browsing Open history:	
†∔†	Flow Control	м	IM online record: Open	
<b></b>	Access Controller	Terminal Online/Offline	Client's upper and lower Open line records:	
8 <u>=</u>	Authentication	Mark MAC Address		
₩	Behavior	MAC Control	Save	
盟	Firewall	Website Control		
Ţ	Advanced application	URL Control 🗸		
0% 00	Services	Application Protocol		
ß	Log	Secondary Routing		
		QQ		

## Fig 7.1.1 Default Behavior Audit Settings page

	CMD-COS-v1.01			ے۔ CD CA CA English
	=,	Behavior <	Behavior > Behavior Audit > Activate Audit	=☐= CPU: 2.48% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
-			Behavior Audit Settings	
()	Overview	Behavior Audit 🔿		
₩	Monitoring	Activate Audit	Behavior record configuration	
ţ	System Setup	Record-free setting	Website browsing	
矗	Network	Web Browsing	history: IM online record:	
†∔†	Flow Control	ІМ	Client's upper and lower 🗹 Open	
<b></b>	Access Controller	Terminal Online/Offline	line records:	
<u>&amp;</u> =	Authentication	Mark MAC Address		
⇆	Behavior	MAC Control	Save	
田	Firewall	Website $\checkmark$ Control		
Ţ	Advanced application	URL Control $$		
0% 00	Services	Application Protocol Control		
ĽĎ	Log	Secondary		

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

	CMD-COS-v1.01			් 🗘 🗘 Linglish
	=<	Behavior <	Behavior > Behavior Audit > Record-free setting	ដើ្ច៖ CPU: 2.75% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
~	System		Record-free setting	
(-)	Overview	Behavior Audit \land		
₩	Monitoring	Activate Audit		
ţĊţ	System Setup	Record-free setting	Audit whitelist: Open	
뮮	Network	Web Browsing	Save	
†∔†	Flow Control	ім		
•	Access Controller	Terminal Online/Offline		
&= ;;	Authentication	Mark MAC Address		
∽	Behavior	MAC Control		
臣	Firewall	Website Control		
y	Advanced application	URL Control 🗸 🗸		
0% 00	Services	Application Protocol Control		
Ġ	Log	Secondary Routing		

## Fig 7.1.3 Default Record-free setting page

CMD-COS-v1.01						තා 🖒 🗘 🛆 Englis
Ξ·	Behavior <	Behavior > Behavior Audit > Record-free set	tting		⊧ <mark>□</mark> : CPU: 0.25% □	☐ MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00
System Overview	Behavior Audit 🔷					
Monitoring	Activate Audit	Audit whitelist:	✔ Open			
දිිූි System Setup	Record-free setting	IP/IPgroup:	Use "-" for IP range		192.168.0.0/24	
品 Network	Web Browsing			Join>>		
fiif Flow Control	ім		No Group Add Group Once configured, please Refresh	< <remove< th=""><th></th><th></th></remove<>		
Access Controller	Terminal Online/Offline					
Authentication	Mark MAC Address					
⇒ Behavior	MAC Control	MAC/MACgroup:	Use ":" for delimiter			
Firewall	Website Control 🛛 🗸			Join>>		
Advanced application	URL Control 🛛 🗸		No Group Add Group Once configured, pleaseRefresh	< <remove< th=""><th></th><th></th></remove<>		
Services	Application Protocol Control					
Log	Secondary Routing					
	QQ Blacklist/Whitelist		Save			

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

	CMD-COS-v1.01						් 🗘 🗘 🐣 English
	=,	Behavior <	Behavior > Behavior	Audit > Web Browsing			📲 CPU: 1.98% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
-		^	Viewing Web Bro	wsing History			
63	Overview	Behavior Audit 🛆					
₩	Monitoring	Activate Audit	Begin Time	C End Time	() IP/MA	C/Web Browsing Q	
ţţ	System Setup	Record-free setting	Time	Ip Addr	MAC	Site Record	Remarks
츎	Network	Web Browsing				No Data	
†∔†	Flow Control	ім					
۲	Access Controller	Terminal Online/Offline					
&= 	Authentication	Mark MAC Address					
⇆	Behavior	MAC Control					
Ħ	Firewall	Website $\checkmark$ Control					
y.	Advanced application	URL Control 🗸					
00	Services	Application Protocol Control					
ľð	Log	Secondary Routing					

## Fig 7.1.5 Default Viewing Web Browsing History page

	کر کے کہ												
	=<	Behavior <	Behavior > Behavior Au	idit > Web Browsing			≣ CPU: 0.50% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s						
			Viewing Web Brows	ing History									
Ð	System Overview	Behavior Audit \land											
₩	Monitoring	Activate Audit	Begin Time	() End Time		Web Browsing Q	export Clean All						
<i>i</i> 03-	System Setup	Record-free	Time	lp Addr	MAC	Site Record	Remarks						
652	oyotoin ootup	setting	2021-05-09 21:54:24	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons2.gvt2.com/							
÷	Network	Web Browsing	2021-05-09 21:53:53	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gvt2.com/							
†∔†	Flow Control	IM	2021-05-09 21:53:41	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/							
<b></b>	Access Controller	Terminal Online/Offline	2021-05-09 21:53:35	192.168.0.103	c4:d9:87:a7:ad:46	https://google.com/							
<u>&amp;</u> =	Authentication	Mark MAC Address	2021-05-09 21:52:53	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons2.gvt2.com/							
₹	Behavior	MAC Control	2021-05-09 21:52:35	192.168.0.103	c4:d9:87:a7:ad:46	https://sl-log.oray.net/							
m		Website	2021-05-09 21:52:32	192.168.0.103	c4:d9:87:a7:ad:46	https://rc10-fc04.oray.com/							
	Firewall	Control	2021-05-09 21:52:31	192.168.0.103	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/							
y	Advanced application	URL Control $$	2021-05-09 21:52:30	192.168.0.103	c4:d9:87:a7:ad:46	https://slapi.oray.net/							
00	Services	Application Protocol Control	2021-05-09 21:52:17	192.168.0.103	c4:d9:87:a7:ad:46	https://play.google.com/							
ß	Log	Secondary Routing	PerPage 10 $\checkmark$	Rows < 1 2	3 4 5 >	1 Jump							

Fig 7.1.6 Viewing Web Browsing History page

	CMD-COS-v1.01					🔿 🏠 🔔 English	
	=,	Behavior <	Behavior > Behavior Au	ıdit > Web Browsing		ः 🛱 CPU: 0.99% 🔛 MEM: 19% ↑ TX: 633.00 B/s ↓ RX: 895.00 B/	s
-	Curture.		Viewing Web Brows	ing History			
Ð	Overview	Behavior Audit \land					
₩	Monitoring	Activate Audit	Begin Time	C End Time	() IP/MAC/	Web Browsing Q export Clean All	
Ś	System Setup	Record-free	Time	lp Addr	MAC	Site Record Remarks	
-0-		setting	2021-04-18 17:37:07	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
楍	Network	Web Browsing	2021-04-18 17:36:50	192.168.0.14	c4:d9:87:a7:ad:46	https://dmp100dmpprodstorage.table.core.windows.net/	
†∔†	Flow Control	IM	2021-04-18 17:36:06	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
<b></b>	Access Controller	Terminal Online/Offline	2021-04-18 17:36:04	192.168.0.14	c4:d9:87:a7:ad:46	https://i.ytimg.com/	
&= ;;	Authentication	Mark MAC Address	2021-04-18 17:35:58	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gcp.gvt2.com/	
₩	Behavior	MAC Control	2021-04-18 17:35:58	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons3.gvt2.com/	
開	Firewall	Website	2021-04-18 17:35:54	192.168.0.14	c4:d9:87:a7:ad:46	https://android.clients.google.com/	
	Advanced	Control	2021-04-18 17:35:54	192.168.0.14	c4:d9:87:a7:ad:46	https://dns.google/	
Ľ₽	application	URL Control 🗸 🗸	2021-04-18 17:35:16	192.168.0.14	c4:d9:87:a7:ad:46	https://i.ytimg.com/	
00	Services	Application Protocol Control	2021-04-18 17:34:59	192.168.0.14	c4:d9:87:a7:ad:46	https://beacons.gvt2.com/	
ß	Log	Secondary					

## 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

	CMD-COS-v1.01							ح ال	습 수 <u>온</u> Eng	glish
	=,	Behavior <	Behavior > Behavio	r Audit > IM			∎ <mark>⊡</mark> ≣ CPU: 1	.98% 🛄 MEM: 16%	↑ TX: 0.00 B/s ↓ RX: 0	.00 B/s
-			Viewing IM Histo	ory						
6)	Overview	Behavior Audit \land								
₩	Monitoring	Activate Audit	Begin Time	C End Time	Ill types	VUsernar	me/Event/IP/M, Q		Export Clean	All
ţĊţ	System Setup	Record-free setting	ІМ Туре	Account	Event	IP	MAC	Date Time	Remarks	
휾	Network	Web Browsing				No Data				
ţţţ	Flow Control	М								
<b>P</b>	Access Controller	Terminal Online/Offline								
<u>&amp;</u> =	Authentication	Mark MAC Address								
₩	Behavior	MAC Control								
Ħ	Firewall	Website $\checkmark$ Control								
V	Advanced application	URL Control 🗸 🗸								
0%	Services	Application Protocol Control								
ß	Log	Secondary Routing								

## 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

	CMD-COS-v1.01								්	<u>ڼ</u>	S English
	=,	Behavior <	Behavior > Behavio	r Audit > Terminal O	nline/Offline			: CPU: 2.7	5% 🛄 MEM: 169	6 ↑ TX: 0.00 B/:	s \downarrow RX: 0.00 B/s
-		A	Viewing Termina	I Online/Offline H	istory						
6)	Overview	Behavior Audit 🛆									
₩	Monitoring	Activate Audit	Begin Time	() End Time		IP/MAC/Type/Name	Q			Export	Clean All
ţĊji	System Setup	Record-free setting	Time	IP	MAC	Тх	Rx	Uptime	System type	Terminal type	Remarks
뷺	Network	Web Browsing					No Data				
ţţţ	Flow Control	ІМ									
۴	Access Controller	<mark>Terminal</mark> Online/Offline									
<u>8</u> -	Authentication	Mark MAC Address									
⇆	Behavior	MAC Control									
臣	Firewall	Website Control									
Ţ	Advanced application	URL Control 🗸 🗸									
0% 00	Services	Application Protocol Control									
ſĿ	Log	Secondary Routing									



6	P										A A A English
	CMD-COS-v1.01	Behavior <	Behavior > Behavior A	udit > Terminal Online/Offline						👌 CPU	2: 0.75%
0	System		Viewing Terminal O	Inline/Offline History							
(F-)	Overview	Behavior Audit 🗠	Begin Time	(3) End Time	() IP/MAC/Type/Name						Export Clean All
	Monitoring	Activate Audit				~	-				
÷	System Setup	Record-free setting	Time 2021-04-18 22:01:37	IP 192 168 0 11	MAC 20:a6:0c:37:4d:13	TX 105.53 KB	Rx 152.41 KB	Uptime	System type	Terminal type	Remarks
몶	Network	Web Browsing	2021-04-18 22:01:37	192.168.0.11	20:46:0:37:46:13	873 68 KB	2 38 MR	17m 45c	Linux	Xiaomi	800011900011
111	Flow Control	м	2021-04-18 21:50:13	192.168.0.11	20:46:0::37:4d:13	163 92 KB	1.22 MR	3m 18c	Linux	Xiaomi	POCOFI-POCOFI
	Access	Terminal	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
	Controller	Online/Offline	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
81	Authentication	Mark MAC Address	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
⇆	Behavior	MAC Control	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
E	Firewall	Website Control $$	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
	Advanced	URI Control 🗸	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
	application	Application	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
ăă	Services	Protocol Control	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
ĥ	Log	Secondary Routing	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
		QQ Blacklist/Whitelist	2021-04-18 21:29:51	192.168.0.12	00:6f:64:f9:5e: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
			Showina 21-40 of 115	5 records					PerPane	20 V Rows & 1	2 3 4 5 6 5 % Z /6Pages Jump

## 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

	CMD-COS-v1.01				🔿 🖒 🗘 🛎 English
	_<	Behavior <	Behavior > Mark MAC Address		≝⊑ CPU: 8.50% 🛄 MEM: 19% ↑ TX: 1.21 KB/s ↓ RX: 334.00 B/s
~	Sustem		Mark MAC Address to Readable Hostname		
6-9	Overview	Behavior Audit 🗸 🗸			
₩	Monitoring	Mark MAC Address	Please input MAC/Narr Q		Add Import Export Delete
ŝ	System Setup	MAC Control	MAC Address Remarks	Actions	
₼	Network	Website Control 🛛 🗸		No Data	
ţţţ	Flow Control	URL Control 🛛 🗸			
<b></b>	Access Controller	Application Protocol Control			
<u>8</u> =	Authentication	Secondary Routing			
∽	Behavior	QQ Blacklist/Whitelist			
臣	Firewall				
Ţ	Advanced application				
0% 00	Services				
ľð	Log				

Fig 7.2.1 Default Mark MAC Address to Readable Hostname page

CHANNE	CMD-COS-v1.01			🛆 🔓 🔔 English
	=,	Behavior <	Behavior > Mark MAC Address	🛱 CPU: 3.25% 🛄 MEM: 19% 个 TX: 4.28 KB/s 🤳 RX: 5.21 KB/s
	_		Mark MAC Address to Readable Hostname	
$\mathcal{O}$	System Overview	Behavior Audit 🛛 🗸		
₩	Monitoring	Mark MAC Address	Please input MAC/Nan Q	Add Import Export Delete
ţĊţ	System Setup	MAC Control	MAC Address Remarks	Actions
- -	Network	Website Control 🛛 🗸	20:a6:0c:37:4d:13 MyMobile	OK Cancel
ţţţ	Flow Control	URL Control 🛛 🗸	Showing 1 of 1 records	PerPage 20 $\checkmark$ Rows $\ll$ $<$ 1 $>$ $\gg$ 1 /1Pages Jump
<b></b>	Access Controller	Application Protocol Control		
<u>&amp;</u> =	Authentication	Secondary Routing		
⇆	Behavior	QQ Blacklist/Whitelist		
臣	Firewall			
Ţ	Advanced application			
0% 00	Services			
ľð	Log			

Fig 7.2.2 Adding Mark MAC Address to Readable Hostname page

	CMD-COS-v1.01			🛆 🟠 🔔 English
	=,	Behavior <	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	
$\mathbb{C}$	Overview	Behavior Audit 🛛 🗸		
₩	Monitoring	Mark MAC Address	Please input MAC/Narr Q	Add Import Export Delete
ţĊţ	System Setup	MAC Control	MAC Address Remarks	Actions
Ģ	NI-town-la	Website Control	20:a6:0c:37:4d:13 MyMobile	Edit Delete
666	Network	website Control V	c4:d9:87:a7:ad:46 MyPC	Edit Delete
ţţţ	Flow Control	URL Control $\checkmark$		
<b></b>	Access Controller	Application Protocol Control	Showing 1-2 of 2 records	PerPage 20 V Rows 《 < 1 > 》 1 /1Pages Jump
<u>&amp;</u> =)	Authentication	Secondary Routing		
₩	Behavior	QQ Blacklist/Whitelist		
臣	Firewall			
y	Advanced application			
00	Services			
ŀ	Log			

## 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

	CMD_COS_v1.01						් ර	\$ \$	English
	=	Behavior (	Behavior > MAC Cont	trol		≣∰≣ CPU: 5.94% 🛄 I	MEM: 16%	1 TX: 0.00 B/	s ↓ RX: 0.00 B/s
		benavior	Blacklist or Whiteli	ist MAC Address					
Ð	System Overview	Behavior Audit 🛛 🗸							
₩	Monitoring	Mark MAC Address	Select Mode						
ŝ	System Setup	MAC Control		Blacklist Mode (All MACs are allow	ed to access the Internet, and the MA	C in the blacklist does not allo	w Internet a	ccess.)	
品	Network	Website Control 🛛 🗸		Whitelist Mode (All MACs are not a	llowed to access the Internet by defai	ult, only MACs in the whitelist	are allowed	to access the l	nternet)
ţţţ	Flow Control	URL Control 🛛 🗸	Blacklist						
<b></b>	Access Controller	Application Protocol Control		Q	addAll Add	Import Export	Enable	Disable	Delete
<u>&amp;</u> =	Authentication	Secondary Routing	MAC Address $\checkmark$	Remarks	Status	Actions			
₩	Behavior	QQ Blacklist/Whitelist			No Data				
臣	Firewall								
Ţ	Advanced application								
0%	Services								
Ŀ	Log								

Fig 7.3.1 Default Blacklist or Whitelist MAC Address page

CENTRE	CMD-COS-v1.01					රු ¢	<u>e</u> English
	=<	Behavior <	Behavior > MAC Cor	itrol		📲 CPU: 0.99% 🛄 MEM: 19% ↑ TX: 0.00	0 B/s 👃 RX: 0.00 B/s
	_		Blacklist or White	list MAC Address			
Ð	System Overview	Behavior Audit 🛛 🗸					
₩	Monitoring	Mark MAC Address	Select Mode				
ŝ	System Setup	MAC Control		Blacklist Mode (All MA     Whitelist Mode (All MA	Cs are allowed to access the Internet, and the M	AC in the blacklist does not allow Internet access.)	
뷺	Network	Website Control 🛛 🗸			Acs are not allowed to access the internet by der	aut, only wates in the writenst are anowed to access t	
†∔†	Flow Control	URL Control 🛛 🗸	Blacklist				
<b></b>	Access Controller	Application Protocol Control	Search	Q	addAll Add	Import Export Enable Disa	ble Delete
<u>&amp;=</u>	Authentication	Secondary	MAC Address $\checkmark$	Remarks	Status	Actions	
			20:a6:0c:37:4d:13	Blacklist%20MAC	Enabled	Edit Disable Delete	
→	Behavior	Blacklist/Whitelist					
₿	Firewall		Showing 1 of 1 reco	rds	PerP	age 20 $\checkmark$ Rows $\ll$ $\langle$ 1 $\rangle$ $\gg$ .	1 /1Pages Jump
Ţ	Advanced application						
0% 00	Services						
ſð	Log						

# 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)

	CMD-COS-v1.01								්	û ↓ ≗	English
	=<	Behavior <	Behavior > We	bsite Control > Blacklis	st/Whitelist			📮 CPU: 1	.25% 🛄 MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
9	System	Pohavior Audit	Blacklist/Wh	itelist Website							
C*3	Overview	benavior Audit V			ika mikitaliat liat (UTTD			laurant	Fundation Fundation	Disable	Delete
₩	Monitoring	Mark MAC Address	Allows accord	ess to external links in t	the whitelist list (HTTP	only)	Add	import	Export	Disable	Delete
ţĊţ	System Setup	MAC Control	Mode	Domain	Ip Addr	Week	Time	Remarks	Status	Actions	
₼	Network	Website Control \land					No Data				
†∔†	Flow Control	Blacklist/Whitelist									
<b></b>	Access Controller	URL Control 🛛 🗸									
<u>&amp;=</u>	Authentication	Application Protocol Control									
⇆	Behavior	Secondary Routing									
田	Firewall	QQ Blacklist/Whitelist									
Ţ	Advanced application										
0% 00	Services										
ľ	Log										

Fig 7.4.1 Default Blacklist/Whitelist Website page

	CMD-COS-v1.01					ථ	合	4 e	English
	=,	Behavior (	Behavior > Website Control > Blacklist/Whit	telist	📋 CPU: 0.25% 🛛 🛄 MEM	Л: 19%	↑ TX: 14	5.00 B/s	RX: 60.00 B/s
		Denavior	Mode:	Blacklist Mode (By default all domain names can be accessed, and domain names in	the list cannot be accessed)				
6	System Overview	Behavior Audit 🛛 🗸		<ul> <li>Whitelist Mode (The default domain name is not accessible, and the domain name in</li> </ul>	n the list can be accessed)				
M	Monitoring	Mark MAC Address	Domain:	www.commandonetworks.com					
ţĊ	System Setup	MAC Control							
品	Network	Website Control 🛛 🔿							
†∔†	Flow Control	Blacklist/Whitelist		Please enter the correct domain name, such as: www.google.com: (One line one item					
<b>P</b>	Access Controller	URL Control 🗸 🗸	IP:	Use "-" for IP range 192.168.0.0/24					
8"	Authentication	Application Protocol Control		Join>>					
⇆	Behavior	Secondary Routing		No Group Add Group Once configured, please Refresh					
臣	Firewall	QQ Blacklist/Whitelist							
Ţ	Advanced application		Weeks	All Manday Tuesday Wednesday Thursday Sciences	Cunday				
0% 00	Services		VVCCK.	Air Monday Tuesday Weunesday Thursday Priday Saturday	Sunday				
D.	Log		Time:	00:00-23:59					
			Remarks:	Blacklisting Commando Website					
				Save Cancel					

# Fig 7.4.2 Blacklist particular Website page

	CMD-COS-v1.01								_ ර	} 4 2	English
	<u> </u>	Behavior <	Behavior > Website	e Control > Blacklist/W	/hitelist			≡ <b>∷</b> ≡ CPU: 1.009	6 🛄 MEM: 19% ↑	TX: 55.00 B/s 🔱	RX: 66.00 B/s
-			Blacklist/Whiteli	st Website							
()	Overview	Behavior Audit 🛛 🗸									
₩	Monitoring	Mark MAC Address	Allows access t	o external links in the	whitelist list (HTTP onl	y)	Add	Import E	xport Enable	Disable	Delete
ې درې	System Setun	MAC Control	Mode	Domain	Ip Addr	Week	Time	Remarks	Status	Actions	
دچه 	ojstem ootap		Ria alsi int		102 168 0 0/24	67	00.00 22.50	Blacklisting	Fachlad	Edit Disable	
ᇔ	Network	Website Control 🔷	DIACKLISE	commandonetw	192.100.0.0/24	07	00:00-23:39	Website	chabled	Delete	
†∔†	Flow Control	Blacklist/Whitelist	Showing 1 of 1 re	cords			PerPag	e 20 V Row	15 (( ( <b>1</b> )	» 1 /1P	ages Jump
<b></b>	Access Controller	URL Control $$								//	.9
<u>8</u> ,	Authentication	Application Protocol Control									
₩	Behavior	Secondary Routing									
臣	Firewall	QQ Blacklist/Whitelist									
V	Advanced application										
0%	Services										
ľð	Log										

Fig 7.4.3 Blacklist Website page

	CMD-COS-v1.01				ු රු 🗘 🛆 English
	=,	Behavior <	Behavior > Website Control > Blacklist/Whi	telist	🛱 CPU: 2.00% 🛄 MEM: 19% ↑ TX: 81.00 B/s 🤳 RX: 82.00 B/s
			Mode:	O Blacklist Mode (By default all domain names can be accessed, and domain names in t	the list cannot be accessed)
Ð	System Overview	Behavior Audit 🛛 🗸		Whitelist Mode (The default domain name is not accessible, and the domain name in	the list can be accessed)
₩	Monitoring	Mark MAC Address	Domain:	commandonetworks.com	
ţÇ	System Setup	MAC Control			
品	Network	Website Control 🛛 🔿			
t++	Flow Control	Blacklist/Whitelist		Please enter the correct domain name, such as: www.google.com: (One line one item)	
<b>(</b>	Access Controller	URL Control 🗸 🗸	IP:	Use *-* for IP range 192.168.0.0/24	
<u>&amp;</u> "	Authentication	Application Protocol Control		<pre>&lt; niot</pre>	
⇆	Behavior	Secondary Routing		No Group Add Group  Conce configured, please Refresh	
臣	Firewall	QQ Blacklist/Whitelist			
I	Advanced application				
0% 00	Services		Week:	🗹 All 💟 Monday 💟 Tuesday 💟 Wednesday 💟 Thursday 💟 Friday 💟 Saturday	Sunday
D.	Los		Time:	00:00-23:59	
-12	Log		Remarks:	Whitelisting Commando Networks	
				Save Cancel	

Fig 7.4.4 Whitelisting particular Website page



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

Swi

# **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.





I		D
I	1	Л
l		•

# 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

Reload

## 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

	CMD-COS-v1.01											ి	<u>ۍ</u> ۲	2 2	English
	=<	Behavior <	Behavior >	<ul> <li>URL Control</li> </ul>	> URL Jump						≡ <b>∷</b> ≣ CPU: 9.41%	🛄 MEM: 16	i% ↑ т <b>х:</b> 0	0.00 B/s 🔱	RX: 0.00 B/s
		benavior	URL Red	irect Setting	s										
Ð	System Overview	Behavior Audit 🛛 🗸													
₩	Monitoring	Mark MAC Address								Add	Import Expo	ort Enal	ble Di	isable	Delete
ŝ	System Setup	MAC Control	Title	Mode	Prio	Src_url	Dst_url	excluded	Hit_rate	IP	Week	Time	Status	Actions	
ᇔ	Network	Website Control 🛛 🗸							No Da	ita					
ţţţ	Flow Control	URL Control ^													
<b></b>	Access Controller	URL Jump													
<u>&amp;=</u>	Authentication	Keyword Replace													
⇒	Behavior	Parameter Replace													
臣	Firewall	Application Protocol Control													
Ţ	Advanced application	Secondary Routing													
0% 00	Services	QQ Blacklist/Whitelist													
ſð	Log														

## Fig 7.5.1 Default URL Redirect Settings page

	CMD-COS-v1.01			් ර 👃 ළ English	
	=,	Behavior <	Behavior > URL Control > URL Jump	+ 📴 CPU: 3.25% 🔛 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s	
-			Add	×	^
ଳ	Overview	Behavior Audit 🗸 🗸 🗸			
~	Monitoring	Mark MAC Address			
ŝ	System Setup	MAC Control	Title:	*	
	N 1		Mode:	Exact 🗸	
650	Network	Website Control V	Prio:	The data between 1 to 63   * (Priority will determine the matching order, and the smaller the value, the higher the priority.)	
<u>tit</u>	Flow Control	URL Control	Src_url:		
۲	Access Controller	URL Jump	Dst_url:	•	
<u>&amp;</u> =)	Authentication	Keyword Replace	excluded :	(Not skipped in the URL.)	
₩	Behavior	Parameter Replace	Hit_rate:	100 % *	
臣	Firewall	Application Protocol Control		(Jump to the specified page as a percentage.)	
	Advanced	Secondary	IP:	Use "-" for IP range	
	application	Routing			
	Services	Blacklist/Whitelist		<th></th>	
ß	Log			Once configured, please Refresh	
				v v	
			Week:	💟 All 💟 Monday 💟 Tuesday 💟 Wednesday 💟 Thursday 💟 Friday 💟 Saturday 💟 Sunday	
			Time:	00:00-23:59 *	
				Save Cancel	~

Fig 7.5.2 Add URL Redirect Settings page

	CMD-C05-VL01						۵	0 4	2	English
	=,	Behavior <	Behavior > URL Control > URL Jump			🧔: CPU: 0.75% 🛄 MEN	A: 2096	TX: 81.00 B/	's ↓ R	RX: 27.00 B/s
~	Surton		Add							×
6-3	Overview	Behavior Audit 🛛 🗸								
5	Monitoring	Mark MAC Address								
ţĝ;	System Setup	MAC Control	Title:	COMMANDO	*					
묘	Network	Website Control	Mode:	Exact						
	Network	website Control •	Prio:	2	* ( Priority will determine the matching order, and the	he smaller the value, the higher the priority. )				
111	Flow Control	URL Control	Src_url:	www.change-networks.com	×					
۲	Access Controller	URL Jump	Dst url:	www.commandonetworks.com	- ] •					
<u>8</u> "	Authentication	Keyword Replace								
Ś	Behavior	Deservation Desile of	excluded:		(Not skipped in the UKL.)					
~7		Parameter Replace	Hit_rate:	100 % *						
B	Firewall	Application Protocol Control	10-	(sump to the specified page as a percentage.)	192.168.0.0/24					
Ţ	Advanced application	Secondary Routing	1 <b>F</b> .	Use - IOLIPTange						
	Services	QQ Disables Alleita Est		Join	ss -					
ቡ	Log	Blacklisty whitelist		No Group Add Group	nove					
-				Once configureo, please <b>kerresn</b>						
			Week:	V All V Monday V Tuesday V Wednesday V Thu	rsday 🗹 Friday 🔽 Saturday 🗹 Sunday					
			Time :	00:00-23:59 *						
				Save						

### Fig 7.5.3 Add particular URL Redirect Settings page

	CMD-COS-v1.01												<b>山</b> 仓	4 2	English
	=,	Behavior <	Behavior > URL (	Control > URL Jum	р							:0: CPU: 1.49%	🛄 MEM: 20% 🕇	TX: 0.00 B/s 👃	, RX: 0.00 B/s
			URL Redirect S	Settings											
6	Overview	Behavior Audit 🗸 🗸 🗸													
<u>w</u>	Monitoring	Mark MAC Address									Add Im	port Export	Enable	Disable	Delete
63	System Setup	MAC Control	Title	Mode	Prio	Src_url	Dst_url	excluded	Hit_rate	IP	Week	Time	Status	Actions	
89 2			COMMANDO	Exact	2	www.change-	www.command		100	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable	
ക്	Network	Website Control 🗸				hetworks.com	one works.com								
<b>tit</b>	Flow Control	URL Control ^	Showing 1 of 1	records							PerPage 20	0 V Rows	« < <mark>1</mark> >	≫ 1 /1Pa	ages Jump
•	Access Controller	URL Jump													
<u>&amp;</u> ,	Authentication	Keyword Replace													
⇒	Behavior	Parameter Replace													
Ħ	Firewall	Application Protocol Control													
Ţ	Advanced application	Secondary Routing													
0% 00	Services	QQ Blacklist/Whitelist													
ß	Log														

### 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

	CMD-COS-v1.01													්	☆ ↓		English
	⊒<	Behavior <	Behavior a	<ul> <li>URL Control</li> </ul>	ol > Keyword	Replace						E CF	U: 9.16% 📮	MEM: 16%	↑ TX: 0.0	)0 B/s \downarrow F	X: 0.00 B/s
•	Sustem		URL Key	words Repl	acement S	ettings											
6-)	Overview	Behavior Audit 🗸 🗸								_							
₽2	Monitoring	Mark MAC Address					- 1			A	Add	Import	Export	Enable	e Dis	able	Delete
ţĊł	System Setup	MAC Control	Title	Mode	Prio	Src Url	Ori Keyword	Rep Keyword	excluded	Hit Rate	IP		Week	Time	Status	Actions	
品	Network	Website Control 🗸 🗸								No Data							
ţţţ	Flow Control	URL Control 🛛 🔿															
<b></b>	Access Controller	URL Jump															
<u>8</u> =	Authentication	Keyword Replace															
∽	Behavior	Parameter Replace															
Ħ	Firewall	Application Protocol Control															
Ţ	Advanced application	Secondary Routing															
0% 00	Services	QQ Blacklist/Whitelist															
ľð	Log																

# Fig 7.5.5 Default URL Keywords Replacement Settings page

	CMD-COS-v1.01			් ර 👃 🖄 English
	≡<	Behavior <	Behavior > URL Control > Keyword Replace	û CPU: 6.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
ଚି	System Overview	Behavior Audit 🛛 🗸	Title:	•
~~ ~~	Monitoring	Mark MAC Address	Mode:	Exact V
ې ۲	System Setup	MAC Control	Prio:	The data between 1 to 63 • (This priority will determine the matching order, and the smaller the value, the higher the priority.)
品「	Network	Website Control $$	Src Url:	•
tit F	Flow Control	URL Control	Ori Keyword:	(Only UTF-8 coding sites are supported for Chinese language content.)
<b>e (</b>	Access Controller	URL Jump	Rep Keyword :	•
<u>8</u> <i>i</i>	Authentication	Keyword Replace	excluded :	(Field is not slipped in the URL)
t, ∎	Behavior	Parameter Replace	Hit Rate:	(Jumn to the specified page as a percentane)
E ·	Firewall	Application Protocol Control	IP:	Use "-" for IP range
, ⊡	Advanced application	Secondary Routing		Joins s
	Services	QQ Blacklist/Whitelist		No Group Add Group
Γbι	Log			Once configured, please <b>Refresh</b>
				v v
			Week:	🜠 All 💟 Monday 💟 Tuesday 💟 Wednesday 💟 Thursday 💟 Friday 💟 Saturday 💟 Sunday
			Time:	00.00-23:59 •
				Save Cancel

Fig 7.5.6 Add Keywords Replacement Settings page

	CMD-COS-v1.01			තා රු 👃 🚊 English
	Ę	Behavior <	Behavior > URL Control > Keyword Replace	🖧 CPU: 2.23% 🛄 MEM: 20% ↑ TX: 27.00 B/s 🤳 RX: 82.00 B/s
6	System	Behavior Audit 🗸 🗸	Title:	COMMANDO1 *
Ē	Overview	Mark MAC	Mode:	Vague
ΡM	Monitoring	Address	Prio:	1 • (This priority will determine the matching order, and the smaller the value, the higher the priority.)
ţĊŗ	System Setup	MAC Control	Src Url:	www.change-networks.com
뮯	Network	Website Control $$	Ori Keyword :	change  * (Only UTF-8 coding sites are supported for Chinese language content)
111	Flow Control	URL Control ^	Rep Keyword:	commando *
•	Access Controller	URL Jump	excluded:	( Field is not slipped in the URL)
<u>&amp;</u> =	Authentication	Keyword Replace	Hit Rate:	70 % *
È	Behavior	Parameter Replace		(Jump to the specified page as a percentage)
ب م	Firmuall	Application	IP:	Use "-" for IP range 192.168.0.0/24
	Adversed	Protocol Control		Join>>
Ţ	application	Secondary Routing		Ke Cours Add Cours
0% 00	Services	QQ Blacklist/Whitelist		No Group Add Group Once configured, please Refresh
Ъ	Log			
			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

	CMD-COS-v1.01														4 2	English
	=,	Behavior <	Behavior > UR	RL Control > K	eyword Replac	e						"OPU: 28.47	% 🛄 MEM: 20	0% ↑ TX: 1	55 KB/s 🤳	RX: 80.00 B/s
			URL Keywor	ds Replacer	ment Settings	5										
ଚ	Overview	Behavior Audit $\sim$														
<u>-</u>	Monitoring	Mark MAC Address									Add	Import	Export E	nable	Disable	Delete
ţĊ	System Setup	MAC Control	Title	Mode	Prio	Src Url	Ori Keyword	Rep Keyword	excluded	Hit Rate	IP	Week	Time	Status	Actions	
品	Network	Website Control 🛛 🗡	COMMAND 01	Vague	1	www.chang e- networks.c	change	commando		70	192.168.0.0/24	1234567	00:00-23:59	Enabled	Edit Disable Delete	
†#†	Flow Control	URL Control														
P	Access Controller	URL Jump	Showing 1 of	1 records							PerPage	20 ~ Ro	ws « <	1 > >>	1 /1Pag	ges Jump
<u>&amp;"</u>	Authentication	Keyword Replace														
⇆	Behavior	Parameter Replace														
臣	Firewall	Application Protocol Control														
Ţ	Advanced application	Secondary Routing														
0%	Services	QQ Blacklist/Whitelist														
Ռ	Log															

## 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

	CMD-COS-v1.01													්	<u></u> ک	2	English
	=,	Behavior <	Behavior	> URL Contro	l > Paramet	er Replace						i 🛱 i CP	'U: 6.44% 🖕	DMEM: 16%	1 TX: 0.0	00 B/s 🤳	RX: 0.00 B/s
-			URL Para	ameter Rep	lacement S	Settings											
63	Overview	Behavior Audit 🛛 🗸								_							
₩	Monitoring	Mark MAC Address	_							4	Add	Import	Export	Enable	Dis	able	Delete
ţĊ	System Setup	MAC Control	Title	Mode	Prio	Src Url	Param Keyword	Rep Keyword	excluded	Hit Rate	IP		Week	Time	Status	Actions	
÷	Network	Website Control 🛛 🗸								No Data							
ţţţ	Flow Control	URL Control 🔷															
<b></b>	Access Controller	URL Jump															
<u>&amp;=</u>	Authentication	Keyword Replace															
⇆	Behavior	Parameter Replace															
臣	Firewall	Application Protocol Control															
Ţ	Advanced application	Secondary Routing															
0%	Services	QQ Blacklist/Whitelist															
Ŀ	Log																

# Fig 7.5.9 Default URL Parameter Replacement Settings page

CMD-COS-V	.01		ත් දා 👃 English
≡<	Behavior <	Behavior > URL Control > Parameter Replace	0 CPU: 3.71% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
System	Dubardan Andra 🗤		^
U <sup>eg</sup> Overview	benavior Audit	Title:	•
Monitoring	Address	Mode:	Exact V
ුරිූි System Setu	MAC Control	Prio:	The data between 1 to 63 • (This priority will determine the matching order, and the smaller the value, the higher the priority.)
🖧 Network	Website Control $$	Src Url:	•
HIII Flow Control	URL Control ^	Param Keyword:	(Only utf-8 coding sites are supported for Chinese language content )
Access Controller	URL Jump	Rep Keyword :	
요리 Authenticatio	n Keyword Replace	excluded :	(This field is not slipped in the URL)
⇒ Behavior	Parameter Replace	Hit Rate:	(Jum to the specified name as a percentane.)
Firewall	Application Protocol Control	IP:	Use *-* for IP range
Advanced application	Secondary Routing		ceniot
□® Services	QQ Blacklist/Whitelist		No Group Add Group
Մը լաց			Once configured, please <b>Refresh</b>
			v
		Week:	🛛 All 💟 Monday 💟 Iuesday 💟 Wednesday 💟 Ihursday 💟 Inday 💟 Saturday 💟 Sunday
		Time:	00:00-23:59 *
			Save

Fig 7.5.10 Add URL Parameter Replacement Settings page

2	CMD-COS-VI.01			D 🗘 🗘 🚨 English
		Behavior <	Behavior > URL Control > Parameter Replace	OPU: 0.25% □ MEM: 20% ↑ TX: 82.00 B/s ↓ RX: 60.00 B/s
6	System Overview	Behavior Audit 🛛 🗸	Title:	COMMANDOParameter .
<u>-</u>	Monitoring	Mark MAC Address	Mode:	East $\vee$
÷	System Setup	MAC Control	Prio:	10 * (This priority will determine the matching order, and the smaller the value, the higher the priority.)
몲	Network	Website Control $$	Src Url:	www.change-networks.com *
tit	Flow Control	URL Control	Param Keyword :	- • (Only utf-8 coding sites are supported for Chinese language content.)
۲	Access Controller	URL Jump	Rep Keyword:	· · · · · · · · · · · · · · · · · · ·
8.	Authentication	Keyword Replace	excluded:	( This field is not skipped in the URL)
\$	Behavior	Parameter Replace	Hit Rate :	70 % *
Ħ	Firewall	Application	IP :	Use "-" for IP range 192.168.0.0/24
L 2	Advanced	Protocol Control Secondary		
	Services	Routing		Via Course And Course
D.	log	Blacklist/Whitelist		Once configured, please Refresh
			Wash	T 10 Nandra Z Taradra D Madazales Z Taradra D Cales Z Canadra
			Week:	Mali 🖉 Monay 🖉 Tuesaay 🛃 Weenesaay 🛃 Inursaay 🛃 Finaay 🛃 Saturaay 🛃 Sunaay
			Time :	0000-23:59 *
				Save

Fig 7.5.11 URL Parameter Replacement Settings add particular keyword page

	CMD-COS-v1.01													ථ	<u>ጉ</u>	2 2	English
	=<	Behavior <	Behavior > l	URL Control	> Paramete	er Replace						"Ö" CPU: 0.	50% 🛄 M	EM: 20% 1	TX: 204.0	0B/s ↓ RX	: 161.00 B/s
			URL Param	neter Repl	acement S	ettings											
6	Overview	Behavior Audit 🛛 🗸								_							
₩	Monitoring	Mark MAC Address	_								Add	Import	Export	Enab	le D	isable	Delete
ŝ	System Setup	MAC Control	Title	Mode	Prio	Src Url	Param Keyword	Rep Keyword	excluded	Hit Rate	IP		Week	Time	Status	Actions	
畾	Network	Website Control 🛛 🗸	COMMA NDOPara	Exact	10	www.chan ge-	-			70	192.168	0.0.0/24	1234567	00:00- 23:59	Enabled	Edit Disable	
ţţţ	Flow Control	URL Control ^	meter			network										Delete	
۴	Access Controller	URL Jump	Showing 1	of 1 records	5						PerPage	20 ~	Rows	《 < 1	> >>	1 /1Page	Jump
<u>&amp;</u> =)	Authentication	Keyword Replace															
₩	Behavior	Parameter Replace															
臣	Firewall	Application Protocol Control															
Ţ	Advanced application	Secondary Routing															
0%	Services	QQ Blacklist/Whitelist															
Ŀ	Log																

## 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

	CMD-COS-v1.01										් ර	¢ 2	English		
	=<	Behavior <	Behavior > Ap	plication Protoco	ol Control			📮 CPU: 1.73% 🔛 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s							
-	-		Application	protocol conti	ol										
R	System Overview	Behavior Audit 🛛 🗸							_						
₩	Monitoring	Mark MAC Address						Add	Import	Export	Enable	Disable	Delete		
ţĊţ	System Setup	MAC Control	Protocol	Action	Src Addr	Dst Addr	Week	Time	priority 🗸	Status	Remarks	Actions			
÷	Network	Website Control 🛛 🗸						No Data							
†∔†	Flow Control	URL Control 🛛 🗸													
<b>(</b>	Access Controller	Application Protocol Control													
<u>&amp;=</u>	Authentication	Secondary Routing													
⇆	Behavior	QQ Blacklist/Whitelist													
₿	Firewall														
Ţ	Advanced application														
0% 00	Services														
Ռ	Log														

Fig 7.6.1 Default Application protocol control page

	OMD-CDS-v1.01				
	≡	Behavior <	Behavior > Application Protocol Control		
0	System	Balandar Andre Sa	Add		
(-)	Óverview	Senavior Audit			
62	Monitoring	Address			
٢	System Setup	MAC Control	Protocol:	Protocol Q	
믋	Network	Website Control 🔍		ALL	
tit	Flow Control	URL Control 🛛 🗸		NetDownload     EleTransfer	
ন্দ	Access	Application		MetCommunication     MetVideoStreaming     < <remove< th=""><th></th></remove<>	
	Authentication	Secondary		CommonProtocol     OtherApp	
653 <del>( .</del>	Rehavior	Routing QQ		SpeedTool     UnknownApp     SeedTool     SeedTool	
~	Concell	Blacklist/Whitelist	Action:	Accept ~	
1	Advanced		Sec Adde:		
9	application				$\cap$
88	Services			A series	
Ъ	Log			No Group Add Group Once configured, please Refresh	
				×	$\sim$
			Dst Addr:		$\mathbf{A}$
				A binx	
				No Course Add Course	
				Once configured, please Refresh	
				~	4
			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:		
				Save Cancel	
			Help:	ob-minitiv militias will be matched first and it is narrowneeded to choose a minite batween 10 and 20	
			2, Th	se default priority preserve with an interaction and the default for "block" is 32 the renformation has the same priority the first profitment endors' is size	
			3, 11	не олинуоленой нек не лете риотку, ите пис сопирател роксу и полстех	

Fig 7.6.2 Add Application protocol control page

-	CMD-COS-v1.01					
	⊒<	Behavior <	Behavior > Application Protocol Control			
~	System		Add			
6-3	Overview	Behavior Audit 🛛 🗸				
₩	Monitoring	Mark MAC Address				
¢	System Setup	MAC Control	Protocol:	Protocol Q		
쯂	Network	Website Control $~~$		ALL     NetCommunication     NetCommunication		HttpProtocol NetDownload
94 <del>1</del>	Flow Control	URL Control 🗸 🗸		OnlineGame     CommonProtocol	Join>>	FileTransfer
•	Access Controller	Application Protocol Control		OtherApp     SpeedTool     OnknownApp	< <remove< th=""><th></th></remove<>	
<u>8</u> .	Authentication	Secondary Routing		> 🚞 SmallPacket		
∽	Behavior	QQ Blacklist/Whitelist				
Ħ	Firewall		Action:	Accept $\lor$		
y	Advanced application		Src Addr:	Use "-" for IP range		192.168.0.0/24
0%	Services				Join>>	
ъ	Log			No Group <b>Add Group</b> Once configured, please <b>Refresh</b>	< <remove< th=""><th></th></remove<>	
			Dst Addr:	Use "-" for IP range		192.168.1.0/24
					Join>>	
				No Group Add Group Once configured, please Refresh	< <remove< th=""><th></th></remove<>	

Fig 7.6.3 Application protocol control add particular action page

	CMD-COS-v1.01										۵	企	\$ 2	English
	=,	Behavior <	Behavior > Appl	ication Protocol (	Control				I 💭 I CPU	J: 22.28% 🛄 M	VEM: 20%	↑ тх: 8	31.00 B/s 🗸	RX: 27.00 B/s
	-		Application pr	otocol control										
Ð	System Overview	Behavior Audit 🛛 🗸												
₩	Monitoring	Mark MAC Address						Add	Import	Export	Enable		Disable	Delete
ţĊţ	System Setup	MAC Control	Protocol	Action	Src Addr	Dst Addr	Week	Time	priority $\checkmark$	Status	Remark	s	Actions	
÷	Network	Website Control 🛛 🗸	NetDownload FileTransfer	Accept	192.168.0.0/24	192.168.1.0/24	1234567	00:00-23:59	31	Enabled			Disable Delete	
ţţţ	Flow Control	URL Control 🛛 🗸	Showing 1 of 1	records				Pe	rPage 20	✓ Rows <	« < 1	> >>	1 /1	Pages Jump
<b></b>	Access Controller	Application Protocol Control									_			
<u>&amp;=</u>	Authentication	Secondary Routing												
⇆	Behavior	QQ Blacklist/Whitelist												
田	Firewall													
Ţ	Advanced application													
00	Services													
ľð	Log													

## 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

	CMD-COS-v1.01					💋 රු 👃 🛆 English	
	=<	Behavior <	Behavior > Secondary Routing			a 📮 CPU: 1.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s	
~	 System		Secondary Routing Settings				
69	Overview	Behavior Audit 🛛 🗸					
₽	Monitoring	Mark MAC Address					
ţĊ	System Setup	MAC Control	No Secondary Routing:	Open			
뮮	Network	Website Control 🛛 🗸	Forbid Time:	00:00-23:59 *			
ţţţ	Flow Control	URL Control 🛛 🗸	Allow IP List:	Use "-" for IP range		^	
<b>(</b>	Access Controller	Application Protocol Control		^	Join>>		
8= 	Authentication	Secondary Routing		No Group <b>Add Group</b> Once configured, please <b>Refresh</b>	< <remove< th=""><th></th><th></th></remove<>		
<b>↓</b> ≯	Behavior	QQ Blacklist/Whitelist					
Ħ	Firewall			×		~	
Ţ	Advanced application			Save			
0%	Services						
ĥ	Log						

## Fig 7.7.1 Default Secondary Routing Settings page

<b></b>	CMD-COS-v1.01						ථා	企	¢	2	English
	=,	Behavior <	Behavior > Secondary Routing			". CPU: 1.00%	🛄 MEM: 19%	↑ тх:	1.57 KB/	s ↓ R	RX: 2.53 KB/
~			Secondary Routing Settings								
$(\cdot)$	Overview	Behavior Audit 🛛 🗸									
₩	Monitoring	Mark MAC Address									
ţĊ}	System Setup	MAC Control	No Secondary Routing:	V Open							
÷	Network	Website Control 🛛 🗸	Forbid Time:	00:00-23:59 *							
ţţţ	Flow Control	URL Control 🛛 🗸	Allow IP List:	Use "-" for IP range		192.168.0.0/24 192.168.1.0/24					
<b></b>	Access Controller	Application Protocol Control			Join>>						
<u>&amp;=</u> )	Authentication	Secondary Routing		No Group Add Group Once configured, please Refresh	< <remove< th=""><th></th><th></th><th></th><th></th><th></th><th></th></remove<>						
⇆	Behavior	QQ Blacklist/Whitelist									
Ħ	Firewall										
Ţ	Advanced application			Save							
0%	Services										
ß	Log										

## 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

	CMD-COS-v1.01								ප්	5 û 4 2	English
	=<	Behavior <	Behavior > QQ B	lacklist/Whitelist				E CPU:	15.75% 🛄 MEM	: 16% ↑ TX: 0.00 B/s	↓ RX: 0.00 B/s
-			QQ Blacklist/W	/hitelist Settings							
6)	Overview	Behavior Audit 🛛 🗸									
₩	Monitoring	Mark MAC Address		us Q				_ turnet _	Format F	Diable Diable	Dila
ţĊţ	System Setup	MAC Control					Add	import	Export	mable Disable	Delete
뮮	Network	Website Control 🛛 🗸	Mode	QQ	lp Addr	Week	Time	Remarks	Status	Actions	
ţţţ	Flow Control	URL Control 🛛 🗸					No Data				
<b></b>	Access Controller	Application Protocol Control									
<u>&amp;=</u>	Authentication	Secondary Routing									
∽	Behavior	QQ Blacklist/Whitelist									
臣	Firewall										
Ţ	Advanced application										
0%	Services										
ß	Log										

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

🗶 смр-с					ත් රා 🗘 Linglish
≡<	в	ehavior <	Behavior > QQ Blacklist/Whitelist		1 <sup>™</sup> / <sub>2</sub> CPU: 1.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
System	в	ehavior Audit 🗸 🗸	Add		×
•• Overview	. N	/lark MAC			
-y Moniton	ang A	ddress	Mode:	Black mode (All QQ can be logged in by default. QQ is not allowed to login in the blacklist)	
ද්ථූදි System S	Setup N	AC Control		O White mode (All QQ are not allowed to log in by default. Only whitelisted QQ logins are allowed)	
品 Network	k V	Vebsite Control $$	QQ:		
fiif Flow Cor	ntrol U	IRL Control $\checkmark$			
Access Controlle	A ler P	pplication rotocol Control			
용특 Authenti	tication R	econdary louting		Please enter the correct QQ number, the format is '123456789 Remarks' one per line	
🕁 Behavior	r C	χQ ilacklist/Whitelist	IP:	Use "-" for IP range	
Firewall				∧ Join>>	
Advance applicati	ed ion			No Group: Add Group Once configured, please Refresh	
□ta Services					
ի եօց				v	
			Week:	🗸 All 🗸 Monday 🏹 Tuesday 🗹 Wednesday 🗹 Thursday 🗹 Friday 🗹 Saturday 🗹 Sunday	
			Time:	00:00-23:59	
			Remarks:		
				Save Cancel	

## Fig 7.8.2 Add QQ Blacklist/Whitelist Settings page

	CMD-COS-v1.01						۵	) ①	۵	2	English
	≡́	Behavior	<	Behavior > QQ Blacklist/Whitelist		😳 CPU: 1.00%	I MEM:	19% ↑	TX: 0.00 E	Vs ↓ I	RX: 0.00 B/s
ଚ	System Overview	Behavior Audit	~								
<b>M</b>	Monitoring	Mark MAC Address		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)						
ţĊł	System Setup	MAC Control		QQ:	12345						
<u> </u>	Network	Website Control	~								
<b>111</b>	Flow Control	URL Control	~								
۹	Access Controller	Application Protocol Control			Please enter the correct QQ number, the format is '123456789 Remarks' one per line						
<u>8</u> .	Authentication	Secondary Routing		IP:	Use "-" for IP range 192.168.0.0/24						
⇆	Behavior	QQ Blacklist/Whitelist			Join>>						
盟	Firewall				No Group Add Group <> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						
V	Advanced application										
	Services										
Β	Log			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

	CMD-COS-v1.01								_ ර	) ¢ 2	English
	=<	Behavior <	Behavior > QQ Bla	cklist/Whitelist				📮 CPU: 0.25%	□ 🛄 MEM: 19% ↑	TX: 678.00 B/s 🔱	RX: 0.00 B/s
	_		QQ Blacklist/Wh	nitelist Settings							
6	Overview	Behavior Audit 🛛 🗸									
<u>-</u>	Monitoring	Mark MAC Address	QQ/IP/Remarks	Q			A.44	Import	ment Enchle	Dirable	Delete
ţĊ	System Setup	MAC Control					Aud	import L	chaple	Disable	Delete
品	Network	Website Control 🗸	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	
ţţţ	Flow Control	URL Control 🛛 🗸									
<b></b>	Access Controller	Application Protocol Control	Showing 1 of 1 re	cords			PerPa	ge 20 $\checkmark$ Row	rs « < <mark>1</mark> >	≫ 1 /1Pag	jes Jump
<u>&amp; </u>	Authentication	Secondary Routing									
⇆	Behavior	QQ Blacklist/Whitelist									
臣	Firewall										
Ţ	Advanced application										
0%	Services										
Ŀ	Log										

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



Fig 8.1.1 Default Access Control List Rules page

2	OMD-CDS-v1.41							
	≡	Firewall <	Firewall > ACL Rules					
Ð	System	ACL Rules	Add					
M	Monitoring	ARP binding						
	Suctam Satura	Connection		Protocol:	any	$\sim$		
- 140 - 140	aynan ang	Limiter Advanced		Action:	accept	$\sim$		
658 	Pre-trecient	Frewall		Direction:	forward	$\sim$		
tet	Flow Control			Connection direction	dase	~		
æ	Controller			matching:				
<b>Æ</b> .	Authentication		Src.Addr					
5	Behavior			IP:				$\wedge$
田	Firewall				^	Jain>>		
3	Advanced application				No Group Add Group	< <remove< th=""><th></th><th></th></remove<>		
88	Services				Citica consigurad, pixana narran			
ъ	Log				~			$\sim$
			Dst.&ddr					
				IP:				
						_		_
						Join>>		
					Once configured, please Refresh	~~~~		
					· · · · · · · · · · · · · · · · · · ·			~
				Sec.Port:				
				Dst. Port:				
				in.interface:				
				Out.Interface:				
				Cycle:	V All V Monday V Tuesday Vedness	day 🖌 Thursday 🚽	🖌 Friday 🖌 Saturday 🖌 Sunday	
				Period:	00:00-23:59 (please input as "00:00-09:00" ]			
				Remarks:				
					Save Cancel			

Fig 8.1.2 Add Access Control List Rules page

2	CMD-CD5+V1.01						
		Firewall <	Firewall > ACL Rules				
Ð	System Overview	ACL Rules		Pentorol	irma	~	
201	Monitoring	ARP binding		Financia.	tanp .		
	System Setup	Connection		Action:	drop	~	
ърг н	-,	Limiter		Direction:	forward	~	
ä	Network	Firewall		Connection direction matching:	Original direction	$\sim$	
tit	Flow Control		See Add.				
Ð	Access Controller		arcadur	IP:	Use "-" for IP range		192.168.0.0/24
<u>e</u> j	Authentication					tatas a	
\$⇒	Behavior				No Group Add Group	< <remove< th=""><th></th></remove<>	
田	Firewall				Once configured, please Refresh		
J	Advanced application						
88	Services						
Ъ	Log						
			DsLAddr	10-	Hee * * for ID mone		192.168.1.0/24
						<ul> <li>«mat.</li> </ul>	
					No Group Add Group Once configured, please Refresh	< <remove< th=""><th></th></remove<>	
				Src.Port:			
				Dst.Port:			
				In.Interface:	lan1,wan1		
				Out.Interface:	lan1,wan1		
				Cycle:	🗸 All 🛃 Monday 🛃 Tuesday 🛃 Wednesda	y 🛃 Thursday	🖌 Friday 📝 Saturday 🛃 Sunday
				Period:	00:00-23:59		
				Remarks	(presseringut as "0200-0200")		
				CONTRACTOR CONTRACT	arriving bing		
					Save Cancel		

Fig 8.1.3 Add particular Access Control List Rules page

	CMD-COS-v1.01													ථ	습 수		English
	=	Firewall <	Firewall >	ACL Rules								Ö CPU	J: 5.00% 🛄	MEM: 19%	↑ TX: 397.	00 B/s 🤳 F	X: 0.00 B/s
			Access Co	ontrol List F	Rules Settin	qs											
A	System Overview	ACL Rules				-				_							
₩	Monitoring	ARP binding									Add	Import	Export	Enable	e Dis	able	Delete
ŝ	System Setup	Connection Limiter	Protocol	Action	Direction	Src.Addr	Dst.Addr	Src.Port	Dst.Port	In.Interface	OutInterfac	ceCycle	Period	Remarks	Status	Actions Edit	
윪	Network	Advanced Firewall	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	Copy Disable Delete	
<u>†</u> ‡†	Flow Control																
۲	Access Controller		Showing 1	l of 1 record:	5						PerPage	20 ~	Rows	« < 1	> >>	1 /1Page	s Jump
8	Authentication																
₩	Behavior																
臣	Firewall																
Ţ	Advanced application																
0%	Services																
Ъ	Log																

#### 🛆 🔂 🙏 🚊 English ≝ CPU: 11.50% 🛄 MEM: 19% ↑ TX: 66.00 B/s ↓ RX: 0.00 B/s Services > Ping Test Services PING Test System Overview Monitoring Capture Packet Host: 192.168.0.101 {ŷ} System Setup Trace Route Source Interface: Auto IP Subnetting Ping Packet Count: 10 Flow Control PING 192.168.0.101 (192.168.0.101) 56(84) bytes of data. Speed Test Result: Access Controller Diagnostics Command Prompt \_ E Authentication Watchdog 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 . . . . . . . . : 255.0 Default Gateway . . . . . . . : 192.168.0.1 ⇒ Behavior Firewall Advanced application Media State . . . . . . . . . . . Media disconnected Connection-specific DNS Suffix . :

#### Fig 8.1.4 Access Control List Rules setting page

Fig 8.1.5 Impact of Access Control List Rules page

#### 8.2 Arp Binding

Static ARP can implement the binding of IP addresses and MAC addresses to prevent ARP entries from being updated by forged ARP packets sent by attackers. Static ARP entries can be implemented when networks contain critical devices such as servers so that network attackers cannot update the ARP entries containing IP addresses of the critical devices on the switch using ARP attack packets, thereby ensuring communication between users and the critical devices. When network administrator wants to prevent an IP address from accessing devices to bind the IP address to an unavailable MAC address. ARP binding fixes an IP address to a MAC address, so packets coming from any other IP/MAC combination won't be accepted. ARP binding essentially means binding together the MAC and IP addresses, so that all requests from that IP address are served only by the PC having that particular MAC address means that if the IP address or the MAC address, the PC having that particular MAC address means that if the IP address or the MAC address, 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

_										
	CMD-COS-v1.01							۵	) û ¢ &	English
	=,	Firewall <	Firewall > ARP bir	nding			≡Ü≕ CF	PU: 0.25% 🛄 MEM	: 19% ↑ TX: 0.00 B/s 👃	RX: 0.00 B/s
	-		ARP Binding							
6	System Overview	ACL Rules								
5	Monitoring	ARP binding	Unbound MA	C is not allowed to surf the I	nternet Comp	atibility has been bound to	DHCP static allocation		Q	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	<b>.</b> . <b>.</b> .	Connection					Add Import	t Export	Bind Clean	Delete
ççş	System Setup	Limiter	IP Address $\checkmark$	MAC Address	NIC belongs	Bind type 🗸	Remarks	Bind state $\checkmark$	Actions	
品	Network	Advanced Firewall	192.168.0.100	e0:db:55:be:35:5b	lan1	General		Unbinding	Bind Edit Delete	
ţţţ	Flow Control		192.168.0.102	08:9b:4b:9e:f4:e3	lan1	General		Unbinding	Bind Edit Delete	
۲	Access Controller		192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Unbinding	Bind Edit Delete	
<u>&amp;=</u>	Authentication		192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete	
⇆	Behavior		192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete	
臣	Firewall		Showing 1-5 of 5	records			PerPage 20 ∨	Rows 《 〈	1 > >> 1 /1Pag	es Jump
Ţ	Advanced application									
0% 00	Services		Help : Go	eneral: between IP and MA nly: IP and MAC , if not corr	C(default) rectly matched, can	't surf the Internet; The only	binding advice is to statica	Ily assign the checke	ed and compatible ARP list to	the
ß	Log		DI Ex	HCP client ports and imports: exports (	or imports the list o	f arps in the bound state				

For ARP Binding, Click on Firewall > ARP binding

Fig 8.2.1 Default ARP Binding page

								0	) A A A	English
	CMD-COS-v1.01	Firewall <	Firewall > ARP bindi	ng			ŧ		:19% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
<i>—</i>	Sustem	· · · · · · · · ·	ARP Binding							
6-9	Overview	ACL Rules							-	
₩	Monitoring	ARP binding	Unbound MAC i	s not allowed to surf the I	nternet Comp	patibility has been bound to I	DHCP static allocation		Q	
ŝ	System Setup	Connection Limiter					Add In	nport Export	Bind Clean	Delete
	N	Advanced	IP Address $\checkmark$	MAC Address	NIC belongs	Bind type $\checkmark$	Remarks	Bind state 🗸	Actions	
660	Network	Firewall	192.168.0.100	e0:db:55:be:35:5b	lan1	General		Binding	Edit Delete	
†‡†	Flow Control		192.168.0.102	08:9b:4b:9e:f4:e3	lan1	General		Binding	Edit Delete	
<b>(</b>	Access Controller		192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Binding	Edit Delete	
&= ;;	Authentication		192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete	
⇆	Behavior		192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete	
田	Firewall		Showing 1-5 of 5 re	ecords			PerPage 20	∼ Rows ≪ <	1 > > 1 /1Pag	es Jump
Ţ	Advanced application									
0% 00	Services		Help : Gen Only	eral: between IP and MAC : IP and MAC , if not corr	C(default) ectly matched, can	't surf the Internet; The only	binding advice is to st	atically assign the checke	d and compatible ARP list to	the
ß	Log		DHC Expo	P client orts and imports: exports o	or imports the list o	of arps in the bound state				

## Fig 8.2.2 After Binding ARP page

	CMD-COS-v1.01				🔿 🖒 🗘 🛆 English
	⊒<	Firewall <	Firewall > ARP binding		≣©E CPU: 4.75% 🔤 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
<b>•</b>	Sustem		Add		×
6-3	Overview	ACL Rules			
₩	Monitoring	ARP binding	IP:	192.168.10.1	
ţĊţ	System Setup	Connection Limiter	MAC:	44:99:87:77:ad:46	
品	Network	Advanced Firewall	NIC belongs:	lan1	<ul> <li></li> </ul>
ţţţ	Flow Control		Bind type:	General	×
<b>(</b>	Access Controller		Remarks:	IP and MAC Static binding	
<u>&amp;</u> "	Authentication			Save Cancel	
₩	Behavior				
臣	Firewall				
Ţ	Advanced application				
0% 00	Services				
ſð	Log				

Fig 8.2.3 Add ARP Binding page

	CMD-COS-v1.01								) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) )	English
	=<	Firewall <	Firewall > ARP bindin	g			: <u></u> :	CPU: 1.24% 🛄 MEM	: 19% ↑ TX: 0.00 B/s 🗸	RX: 0.00 B/
	_		ARP Binding							
6	System Overview	ACL Rules								
FM-	Monitoring	ARP binding	Unbound MAC is	not allowed to surf the	Internet Compati	bility has been bound to	DHCP static allocation		Q	
~		Connection					Add Import	Export	Bind Clean	Delete
÷Çž	System Setup	Limiter	IP Address ∨	MAC Address	NIC belongs	Bind type 🗸	Remarks	Bind state ∨	Actions	
뷺	Network	Advanced Firewall	192 168 0 100	e0:db:55:be:35:5b	lan1	General		Binding	Edit Delete	
(†1†	Flow Control		192.100.0.100	60.00.33.06.33.00	lann	General		binding	Luit Delete	
			192.168.0.102	08:9b:4b:9e:f4:e3	lan1	General		Binding	Edit Delete	
	Access Controller		192.168.0.103	c4:d9:87:a7:ad:46	lan1	General		Binding	Edit Delete	
<u>&amp;</u> =]	Authentication		192.168.0.105	08:9b:4b:99:a3:94	lan1	General		Unbinding	Bind Edit Delete	
¢,	Behavior		192.168.1.1	54:b8:0a:57:78:63	wan1	General		Unbinding	Bind Edit Delete	
田	Firewall		192.168.10.1	44:99:87:77:ad:46	lan1	General	IP and MAC Static binding	Binding	Edit Delete	
Ţ	Advanced application		Showing 1-6 of 6 red	ords			PerPage 20 V	Bows // / 1	> >> 1 /1Page	Jump
0%	Services								, // _ , // age	

### 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

	CMD-COS-v1.01									් ර	¢ 2	English
	=<	Firewall <	Firewall > Connec	tion Limiter					📮 CPU: 1.25%	🛄 MEM: 16% ↑	TX: 0.00 B/s 🔱	RX: 0.00 B/s
			Connection Lin	niter Settings								
6	System Overview	ACL Rules										
₩	Monitoring	ARP binding						Add	Import Export	Enable	Disable	Delete
ţĊ	System Setup	Connection Limiter	IP Address $\checkmark$	Protocol	WAN Port $\vee$	Limit 🗸	Cycle	Period	Remarks	Status	Actions	
品	Network	Advanced Firewall					No	Data				
†∔†	Flow Control											
<b>(</b>	Access Controller											
<u>&amp;</u> =	Authentication											
⇆	Behavior											
臣	Firewall											
Ţ	Advanced application											
0% 00	Services											
ľð	Log											

Fig 8.3.1 Default Connection Limiter Settings page

	CMD-COS-v1.01				스) 슈 슈 온 English
	=,	Firewall <	Firewall > Connection Limiter		≣ё CPU: 0.00% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
	-		Add		×
S	System Overview	ACL Rules			
₩	Monitoring	ARP binding	IP Address:	Use *-* for IP range	192.168.0.0/24
ţĊţ	System Setup	Connection Limiter		< <not< th=""><th></th></not<>	
品	Network	Advanced Firewall		No Group Add Group <pre>&lt;<remove< pre=""></remove<></pre>	
ţţţ	Flow Control			~	
<b></b>	Access Controller		Protocol	irmn	
<u>&amp;=</u>	Authentication				
$\stackrel{\leftarrow}{\Rightarrow}$	Behavior		WAN Port:	*	
Ħ	Firewall		Limit:	3	Eriday 🛛 Seturday 🗖 Sunday
Ţ	Advanced application		Period:	00:00-23:59	V may V Salady V Salady
0% 00	Services			(please input as "00:00-09:00")	
ß	Log		Remarks:	ICMP limit	
				Save	

Fig 8.3.2 Add Connection Limiter Settings page

	CMD-COS-v1.01									ے د	) <b>\$</b> 8	English
	=,	Firewall <	Firewall > Connec	ction Limiter					📮 CPU: 5.75%	🛄 MEM: 19%	↑ TX: 0.00 B/s 🔱	RX: 0.00 B/s
~			Connection Lin	niter Settings								
(-)	Overview	ACL Rules										
<u>-</u>	Monitoring	ARP binding						Add Im	nport Expor	t Enable	Disable	Delete
ţĊ	System Setup	Connection Limiter	IP Address $\vee$	Protocol	WAN Port $\vee$	Limit 🗸	Cycle	Period	Remarks	Status	Actions	
₼	Network	Advanced Firewall	192.168.0.0/24	icmp		3	1234567	00:00-23:59	ICMP limit	Enabled	Disable Delete	, 🗆
ţţţ	Flow Control		Showing 1 of 1 r	ecords				PerPage 2	0 V Rows	« < <mark>1</mark> >	≫ 1 /1Pag	es Jump
<b>P</b>	Access Controller											
<u>&amp;</u> =	Authentication											
↓ \$	Behavior											
臣	Firewall											
Ţ	Advanced application											
0% 00	Services											
Ŀ	Log											

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

	CMD-COS-v1.01		් 🗘 🗘 La English	
	=<	Firewall <	Firewall > Advanced Firewall 😳 CPU: 0.75% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s	ŝ
	_		Advanced Firewall Configuration	
R	System Overview	ACL Rules		
₹	Monitoring	ARP binding		
ŝ	System Setup	Connection Limiter	Block PING from internal network	
æ	Network	Advanced Firewall	Block PING from public network	
†∔†	Flow Control		Disable tracert (Trace Route)	
<b>R</b>	Access Controller		Hijack all PING values (the PING value for game is 0, do not ban PING when using this feature)	
<u>8</u> =	Authentication		Discard invalid connection	
⇆	Behavior		Enable internal network DOS attack defense	
臣	Firewall		✓ Enable TCP maximum message length	
Ţ	Advanced application		Set TCP-MSS value: 1400 Unit *	
0%	Services		(1000-1000, lengur 6 an integer multiple of 4)	
ſð	Log		Default Save	

Fig 8.4.1 Default Advanced Firewall Configuration page



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

	CMD-COS-v1.01									් ර	) ¢ 2	English
	=,	Advanced	Advanced appl	ication > Dynamic DN	S				∎ CPU: 0.74%	MEM: 16%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	_	application	Dynamic DN	S Settings								
R	System Overview	Dynamic DNS										
₩	Monitoring	SNMP						Add Imp	oort Export	Enable	Disable	Delete
ţŷ	System Setup	Application across three	Server	Domain Name	Parsing Set	Interface	MAC Address	Update results	IP Address	Status	Actions	
矗	Network	Wake on LAN					No Dat	a				
†∔†	Flow Control	FTP Server										
<b></b>	Access Controller	HTTP Server										
<u>&amp;=</u>	Authentication	UDPXY Set										
\$ ↓	Behavior											
Ħ	Firewall											
Ţ	Advanced application											
0% 00	Services											
ß	Log											

Fig 9.1.1 Default Dynamic DNS Settings page

-	CMD-COS-v1.01				් රු 🗘 ළ English
	=,	Advanced	Advanced application > Dynamic DNS		📲 CPU: 0.50% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
		application	Add		×
$(\tilde{r})$	Overview	Dynamic DNS			
<u>-</u>	Monitoring	SNMP			
ţĊ}	System Setup	Application across three	Server:	3322.org ~	
品	Network	layers	Domain Name:		•
	nothon	Wake on LAN	Username:		*
ţţţ	Flow Control	FTP Server	Password :		*
<b></b>	Access Controller	HTTP Server	Interface:		*
<u>&amp;</u> =	Authentication		Decod Trees		
⇆	Behavior	UDPXY Set	Record Type:	A Record(IPV4)	<u>^</u>
				Save Cancel	
⊞	Firewall				
Ţ	Advanced application				
0% 00	Services				
ß	Log				

## Fig 9.1.2 Add Dynamic DNS Settings page

	CMD-COS-v1.01					스) 슈 슈 옾 English
	=,	Advanced	Advanced application > Dynamic DNS			= CPU: 0.75% 🛄 MEM: 19% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		application	Add			×
$\mathbb{C}$	System Overview					
₩	Monitoring	SNMP				
Ś	System Setup	Application	Server:	3322.org ~		
		across three layers	Domain Name:	www.commandonetworks.com	*	
品	Network	Wake on LAN	Username	admin	*	
ţţţ	Flow Control	570.0	o seriariei			
<b></b>	Access	FIP Server	Password:	••••••	*	
Ľ	Controller	HTTP Server	Interface :	auto 🗸	*	
<u>8</u> =	Authentication	UDPXY Set	Record Type:	A Record(IPv4)	· *	
₩	Behavior					
臣	Firewall			Save Cancel		
Ţ	Advanced application					
0%	Services					
Ŀ	Log					

Fig 9.1.3 Add Particular Dynamic DNS Settings page

	CMD-COS-v1.01									ධ	企	<u>م</u> 2	English
	=<	Advanced	Advanced applic	ation > Dynamic DN	S				∎ CPU: 0.74%	🛄 MEM: 19%	↑ т	X: 0.00 B/s	RX: 0.00 B/s
		application	Dynamic DNS	Settings									
$\odot$	System Overview	Dynamic DNS											
	Monitoring	SNMP						Add Im	port Expor	t Enable	,	Disable	Delete
ති	System Setup	Application	Server	Domain Name	Parsing Set	Interface	MAC Address	Update results	IP Address	Status		Actions	
~~~ 	-)	across three layers	3322.org	www.commando		auto				Enabled		Edit Disable	e
品	Network	Wake on LAN		networks.com								Delete	
†∔†	Flow Control	FTP Server	Showing 1 of 1	records				PerPage 20	) V Rows	≪ < 1	> >>	1 /1F	ages Jump
<b>P</b>	Access Controller	HTTP Server											
& <u>=</u> ]	Authentication	UDPXY Set											
₩	Behavior												
盟	Firewall												
Ţ	Advanced application												
0% 00	Services												
ĥ	Log												

Fig 9.1.4 Dynamic DNS Settings page

### 2. SNMP

SNMP stands for Simple Network Monitoring Protocol. It is a protocol for management information transfer in networks, for use in LANs especially for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. SNMP has been defined with four major functional areas to support the core function of allowing managers to manage agents:

#### Data Definition:

The syntax conventions for how to define the data to an agent or manager. These specifications are called the Structure of Management Information (SMI).

#### MIBs:

Over 100 Internet standards define different MIBs, each for a different technology area, with countless vendor proprietary MIBs as well. The MIB definitions conform to the appropriate SMI version.

#### Protocols:

The messages used by agents and managers to exchange management data.

#### Security and Administration:

Definitions for how to secure the exchange of data between agents and managers

# **Understanding SNMP**



#### Fig 9.2.1 SNMP Community concept

#### **SNMP** Version

v1 -simple authentication with communities but used MIB-I originally.

v2 - Uses SMIv2, removed requirement for communities, added Get Bulk and Inform messages, but began with MIB-II originally. 2c Pseudo-release (RFC 1905) that allowed SNMPv1-style communities with SNMPv2; otherwise, equivalent to SNMPv2.

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



#### Fig 9.2.2 SNMP Community concept

#### How to enable Simple Network Monitoring Protocol?

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

	CMD-COS-v1.01			් ර ර ද ළ En
	=	Advanced	Advanced application > SNMP	📫 CPU: 3.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0
		application	Simple Network Monitoring Protoco	l Settings
Ð	System Overview	Dynamic DNS		
₩	Monitoring	SNMP	SNMP Configuration	
ţĊ	System Setup	Application across three	SNMP:	Open
놂	Network	Wake on LAN	Monitor Port:	161
tŧt	Flow Control	ETP Server	Physical Location:	
•	Access Controller		Contact:	
	Authentisation	HTTP Server	System Information :	
lę.,	Authentication	UDPXY Set		
₩	Behavior		Advanced Configuration	
臣	Firewall		SNMP Configuration:	SNMP V2C ~
V	Advanced application		Name:	public
0% 00	Services		Permission :	Read only     Read-write
Ъ	Log		IP Address :	
				Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)
				Save Cancel

Fig 9.2.3 Default Simple Network Monitoring Protocol Settings page

	CMD-COS-v1.01			තා 🗘 👃 English
	=<	Advanced	Advanced application > SNMP	n 🔁 CPU: 0.25% 🥅 MEM: 19% ↑ TX: 1.56 KB/s 👃 RX: 621.00 B/
		application	Simple Network Monitoring Protocol	Settings
6)	System Overview	Dynamic DNS		
₩	Monitoring	SNMP	SNMP Configuration	
ŝ	System Setup	Application	SNMP:	✓ Open
모	Network	layers	Monitor Port:	161
000	nothork	Wake on LAN	Physical Location:	COMMANDOHQ
†∔†	Flow Control	ETD Sonior	-	
	Access	FIF Selvel	Contact:	ABC
	Controller	HTTP Server	System Information:	SNMPServer
<u>8</u> .	Authentication	UDPXY Set		
₩	Behavior		Advanced Configuration	
臣	Firewall		SNMP Configuration:	SNMP V2C V
	Advanced		Name:	public
62	application		Permission :	Read only 🔘 Read-write
	Services			
٦N	log		IP Address :	192.168.0.10/24
-0	Log			Enter IP address/subnet mask, example (1.1.1.1/255.255.255.0 or 1.1.1.1/24)
				Save

#### 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

000	CMD-COS-v1.01								5 û ¢ 2	English
	=<	Advanced	Advanced application	Application across	three layers		=	CPU: 0.99% 🛄 MEM	l: 16% ↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
		application	Application across	three layers						
$\epsilon$	System Overview	Dynamic DNS								
₩	Monitoring	SNMP					Add Import	Export	Enable Disable	Delete
ţŷ	System Setup	Application across three	SNMP Server IP	lpSegment	SNMP service listening port	SNMP protocol version	Remarks	Status	Actions	
÷	Network	layers Wake on LAN				No Dat	а			
ţţţ	Flow Control	FTP Server								
<b></b>	Access Controller	HTTP Server								
<u>&amp;</u> =	Authentication	UDPXY Set								
$\stackrel{}{\downarrow}$	Behavior									
Ħ	Firewall									
Ţ	Advanced application									
0% 00	Services									
ſð	Log									

## Fig 9.3.1 Default Application across three layers page

	CMD-COS-v1.01				් 1	) 4 2	English
	=,	Advanced	Advanced application > Application across the	nree layers	📮 CPU: 7.18%	↑ TX: 0.00 B/s ↓	RX: 0.00 B/s
	-	application	Add				× ^
6)	System Overview	Dynamic DNS					
₩	Monitoring	SNMP					
ţĊ	System Setup	Application across three	SNMP Server IP:	<ul> <li>CEU in the ID of the three larger desires in the interval external operation.</li> </ul>	ad also de vice ana de tra ana a CNIMD		
묘	Network	layers	I= C + -	( Fill in the P of the three-layer device in the internal network, and		service )	
		Wake on LAN	ipsegment:	Ose - for iP range			
1+1	Flow Control	FTP Server		Join>>			
<b></b>	Access Controller	HTTP Server		No Group Add Group			
<u>&amp;</u> =	Authentication			Once configured, please <b>Refresh</b>			
$\overleftrightarrow$	Behavior	UDPXY Set		<u>_</u>		>	
, E	Firewall						
±3	r ii ewaii		SNMP service listening port:	161 *			
,	Advanced application		SNMP protocol version:	V2 ~			
0% 00	Services		Remarks:	×			
Ŀ	Log		team Name:	public *			
				Save			Ŷ

Fig 9.3.2 Add Application across three layers page

mote	CMD-COS-v1.01				<u>م</u>	습 수 은 English
	=<	Advanced	Advanced application > Application across th	nree layers	🛄 CPU: 3.50% 🛄 MEM: 19%	↑ TX: 27.00 B/s ↓ RX: 27.00 B/
	_	application	Add			×
$\odot$	System Overview	Dynamic DNS				
~	Monitoring	SNMP				
ŝ	System Setup	Application	SNMP Server IP:	192.168.0.10 *		
П		layers		( Fill in the IP of the three-layer device in the internal network,	and the device needs to open SNN	IP service )
600	Network	Wake on LAN	IpSegment:		192.168.0.0/24	^
ţţţ	Flow Control	FTP Server		<pre> </pre>		
<b></b>	Access Controller	HTTP Server		No Group Add Group		
<u>&amp;=</u>	Authentication	UDPXY Set		Once configured, please <b>Kerresh</b>		
₩	Behavior			v		~
臣	Firewall		SNMP service listening	*		
Ţ	Advanced application		SNMP protocol version:	V2 ~		
0% 00	Services		Remarks:	SNMP Application *		
ß	Log		team Name:	COMMANDO *		
				Save Cancel		

Fig 9.3.3 Application across three layers for particular SNMP server page

	CMD-COS-v1.01							ථ	습 🗘 🛆 English
	=,	Advanced	Advanced application :	<ul> <li>Application across three</li> </ul>	ee layers		: <b>.</b>	PU: 0.25% 🛄 MEM: 19%	↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		application	Application across t	hree layers					
$\mathbb{C}$	System Overview	Dynamic DNS							
~	Monitoring	SNMP					Add Import	Export Enable	e Disable Delete
ŝ	System Setup	Application across three	SNMP Server IP	lpSegment	SNMP service listening port	SNMP protocol version	Remarks	Status	Actions
뷺	Network	layers Wake on LAN	192.168.0.10	192.168.0.0/24	161	V2	SNMP Application	Absent	Edit Copy Disable
ţţţ	Flow Control	FTP Server	Showing 1 of 1 record	s			PerPage 20 ∨	Rows 《 < 1	> >> 1 /1Pages Jump
<b></b>	Access Controller	HTTP Server	-				-		
<u>&amp;</u> =	Authentication	UDPXY Set							
₩	Behavior								
臣	Firewall								
Ø	Advanced application								
00	Services								
ſð	Log								

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 Wakeon-LAN Settings (WOL) packet to the remote computers for waking computers up from a very low power mode remotely. The WOL feature allows the administrator to remotely power up all sleeping machines so that they can receive updates. WOL sends coded network packets, called magic packets, to systems equipped and enabled to respond to these packets. WOL is based on the principle that when the PC shuts down, the NIC still receives power, and keeps listening on the network for the magic packet to arrive. This magic packet can be sent over connectionless protocols (generally UDP).

To configure Wake-on-LAN Settings, Click on Advanced application > Wake on LAN

	CMD-COS-v1.01							් ර	) <del>(</del> 2	English
	=<	Advanced	Advanced application > Wake on LAN	I			≣ <b>□</b> ≣ CPU: 0.50%	MEM: 16%	↑ TX: 0.00 B/s 🔾	, RX: 0.00 B/s
	_	application	Wake-on-LAN Settings							
$\mathbb{C}$	System Overview	Dynamic DNS								
₽2	Monitoring	SNMP	Immediate Wake-up							
ţĊţ	System Setup	Application across three								
₼	Network	Wake on LAN	MAC Address:				Wakeup			
tit	Flow Control	FTP Server	Regular Wake-up List							
<b></b>	Access Controller	HTTP Server	··· 3			Add Import	Export Enable	Disable	Wakeup	Delete
8= ;	Authentication	UDPXY Set	MAC Address Terminal State	us Cycle	Date	Time	Remarks	Planned Task	Actions	
₩	Behavior									
Ħ	Firewall					No Data				
Ş	Advanced application									
0%	Services									
ľð	Log									

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

	CMD-COS-v1.01						ථා	<u>ት</u>	<u> </u>	English
	=,	Advanced	Advanced application > Wake on LAN			i CPU: 0.50%	EMEM: 19%	↑ тх: 0	.00 B/s 🔱	RX: 0.00 B/s
	-	application	Add							×
$\mathbb{C}$	System Overview	Dynamic DNS								
<u>-</u>	Monitoring	SNMP	MAC:	c4:d9:87:a7:ad:46	*					
ţĊţ	System Setup	Application across three lavers	Cycle:	Everyday	$\sim$					
쁆	Network	Wake on LAN	Time:	10:00	3 *					
ţţţ	Flow Control	FTP Server	Remarks:	WOL Packets						
<b>P</b>	Access Controller	HTTP Server		Save						
<u>&amp;</u> =	Authentication	UDPXY Set								
₩	Behavior									
臣	Firewall									
Ø	Advanced application									
0%	Services									
ſð	Log									

Fig 9.4.2 Add Wake-on-LAN Settings page

	CMD-COS-v1.01								<b>D</b>	û ¢	🛆 English
	=<	Advanced	Advanced application	n > Wake on LAN				∎Ö. CPU: 0.00%	🛄 MEM: 19%	↑ TX: 0.00 B/	′s ↓ RX: 0.00 B/s
		application	Wake-on-LAN Set	tings							
$\odot$	System Overview	Dynamic DNS									
₩	Monitoring	SNMP	Immediate Wake-up								
ţĊ	System Setup	Application across three	MAC	Address	c1.d0.87.a7.ad.16			Wakeup			
쁍	Network	Wake on LAN	MAC	Address	04.05.07.07.00.40			Wakeup			
ţţţ	Flow Control	FTP Server	Regular Wake-up List								
<b></b>	Access Controller	HTTP Server					Add Import	Export Enable	Disable	Wakeup	Delete
<u>&amp;=</u>	Authentication		MAC Address	Terminal Status	Cycle	Date	Time	Remarks	Planned Task	Actions	
\$	Behavior	UDPXY Set	c4:d9:87:a7:ad:46	Online	Everyday		10:00	WOL Packets	Enabled	Wakeup E Disable D	Edit 🗌
田	Firewall		Showing 1 of 1 reco	rds			Pe	erPage 20 $\checkmark$ Rows	≪ < 1	> >> 1	/1Pages Jump
Ţ	Advanced application										
0%	Services										
ľð	Log										

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

	CMD-COS-v1.01			් 🖒 🗘 🛆 English
	=,	Advanced	Advanced application > FTP Server	≣ CPU: 4.25% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
		application	FTP Server	
Ð	System Overview	Dynamic DNS		
₩	Monitoring	SNMP	FTP Server - OFF	
ţĊţ	System Setup	Application across three		
品	Network	Wake on LAN		
ţţţ	Flow Control	FTP Server		
<b></b>	Access Controller	HTTP Server		
<u>&amp;</u> =	Authentication	UDPXY Set		
¢‡	Behavior			
Ħ	Firewall			
Ţ	Advanced application			
0%	Services			
ľ	Log			

#### Fig 9.5.1 Default FTP Server page

	CMD-COS-v1.01							<u>e</u> Eng
	=,	Advanced	Advanced application >	FTP Server		≡ <b>□</b> ≣ CPU: 21.25%	🛄 MEM: 20% ↑ TX: 0.00 E	3/s \downarrow RX: 0.0
		application	FTP Server					
6	System Overview	Dynamic DNS						
₩	Monitoring	SNMP	FTP Server ON O					
<i>:</i> ??3	System Setup	Application	Server Port: 21	Set		Add Import Expo	rt Enable Disable	e Delet
2 <u>2</u> 55	System Setup	across three layers	username	Authority	FTP File Directory	Status	Actions	
品	Network	Wake on LAN						
†††	Flow Control				No Data			
<b>(</b>	Access	FIP Server						
	Controller	HTTP Server						
<u>&amp;</u> =)	Authentication	UDPXY Set						
₩	Behavior							
Ē	Firewall							
<u> </u>								
y.	application							
0%	Services							
FA.								

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

	CMD-COS-v1.01						් 🗘 👃 🛆 English
	=<	Advanced	Advanced application :	> HTTP Server		≣ 	MEM: 16% ↑ TX: 0.00 B/s \downarrow RX: 0.00 B/s
		application	HTTP Server				
$\mathfrak{S}$	System Overview	Dynamic DNS					
₩	Monitoring	SNMP				Add Import Export	Enable Disable Delete
ţĊ	System Setup	Application across three	File Directory	Interview Method	Service Port	Directory Permissions Status	Actions 🗌
÷	Network	layers Wake on LAN				No Data	
ţţţ	Flow Control	FTP Server					
<b>P</b>	Access Controller	HTTP Server					
<u>&amp;=</u>	Authentication	UDPXY Set					
₩	Behavior						
臣	Firewall						
Ţ	Advanced application						
0%	Services						
ß	Log						

#### 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

	CMD-COS-v1.01					<u>්</u> ර ද	🛆 English
	=,	Advanced	Advanced application > UDP>	(Y Set		≡ CPU: 6.25%	B/s \downarrow RX: 0.00 B/s
		application	UDPXY Set				
$(\tilde{r})$	System Overview	Dynamic DNS					
₩	Monitoring	SNMP			Add In	nport Export Enable Disab	e Delete
ţĊ}	System Setup	Application across three	Signal Interface	Service Port	Status	Actions	
品	Network	layers			No Data		
		Wake on LAN					
111	Flow Control	FTP Server					
<b>P</b>	Access Controller	HTTP Server					
<u>&amp;</u> =	Authentication	UDPXY Set					
∽	Behavior						
臣	Firewall						
Ţ	Advanced application						
0% 00	Services						
ርъ	Log						

#### Fig 9.7.1 Default UDPXY Set page

	CMD-COS-v1.01					۵ û ¢ 2	C English
	=<	Advanced 🧹	Advanced application > UDPXY Set		:⊑: CPU: 0	.25% 🛄 MEM: 20% ↑ TX: 3.78 KB/s 🔍	RX: 613.00 B/s
		application	UDPXY Set				
$\odot$	System Overview	Dynamic DNS					
~	Monitoring	SNMP			Add Import	Export Enable Disable	Delete
ţĊţ	System Setup	Application across three	Signal Interface	Service Port	Status	Actions	
品	Network	layers	wan1	∨ 215	Editing	OK Cancel	
		Wake on LAN	lan1	357	Enabled	Edit Disable Delete	
T+1	Flow Control	FTP Server					
<b></b>	Access Controller	HTTP Server	Showing 1-2 of 2 records		PerPage 20 🗸	Rows $\langle \langle 1 \rangle \rangle = 1$	1Pages Jump
& <u>=</u> )	Authentication	UDPXY Set					
₩	Behavior						
臣	Firewall						
Ţ	Advanced application						
0% 00	Services						
ſð	Log						

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

	CMD-COS-v1.01				් 🗘 🗘 🚨 English
	⊒<	Services <	Services > Ping Test		≣Ö≝ CPU: 0.74% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
-	Surtem		PING Test		
(-)	Overview	Ping Test			
₩	Monitoring	Capture Packet	Host:	www.google.com	•
ţĊţ	System Setup	Trace Route	Source Interface:	Auto	~
놂	Network	IP Subnetting	Ping Packet Count:	10 *	
ţţţ	Flow Control	Speed Test	Result:		
<b>P</b>	Access Controller	Diagnostics			
<u>&amp;</u> =	Authentication	Watchdog			
₩	Behavior				
Ħ	Firewall			Start	
Ţ	Advanced application				
0%	Services				
լ	Log				

## Fig 10.1.1 Default PING Test page

	CMD-COS-v1.01						企	۵	2	English
	=	Services <	Services > Ping Test	¤∰= CPU: 5.	50%	🛄 MEM: 20%	↑ TX: 2.	47 KB/s	↓ RX:	68.84 KB/s
		Services	PING Test							
$\mathfrak{S}$	System Overview	Ping Test								
~	Monitoring	Capture Packet	Host:	www.google.com	*					
ţĊţ	System Setup	Trace Route	Source Interface:	Auto	$\sim$					
÷	Network	IP Subnetting	Ping Packet Count:	10 *						
†‡†	Flow Control	Speed Test	Result:	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	^					
<b></b>	Access Controller	Diagnostics		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	ł.					
<u>8</u> =)	Authentication	Watchdog		10 packets transmitted, 10 received, 0% packet loss, time 10s	*					
₩	Behavior									
田	Firewall			Start						
Ţ	Advanced application									
0%	Services									
Ŀ	Log									

Fig 10.1.2 PING to particular website page

	CMD-COS-v1.01						ථ	습	¢	2	English
	=,	Services <	Services > Pin	ng Test		CPU: 4.75%	🛄 MEM: 20%	↑ TX: 2.	01 KB/s	↓ RX	: 99.91 KB/s
6	System	Ping Test	PING Test								
_	Overview	, ř									
5	Monitoring	Capture Packet		Host:	192.168.0.101		*				
ţĊţ	System Setup	Trace Route		Source Interface:	Auto	$\sim$					
뮮	Network	IP Subnetting		Ping Packet Count:	10 *						
ţţţ	Flow Control	Speed Test		Result:	PING 192.168.0.101 (192.168.0.101) 56(84) bytes of data. 32 bytes from 192.168.0.101: icmp_reg=1 ttl=64 time=64.18 ms						
<b></b>	Access Controller	Diagnostics			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=3 ttl=64 time=24.32 ms	;					
<u>&amp;</u> =	Authentication	Watchdog			32 bytes non 132,100,0,101, temp_req=4 te=04 time=33,23 ms						
$\stackrel{\leftarrow}{\Rightarrow}$	Behavior										
臣	Firewall				Stop						
Ø	Advanced application										
0% 00	Services										
۲A.	Lon										

#### 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

	CMD-COS-v1.01				් 🗘 🗘 🐣 English
	<u> </u>	Services <	Services > Capture Packet	្មើ៖ CPU: (	).99% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	System		Capture Packet		
(~)	Overview	Ping Test			
₩	Monitoring	Capture Packet	Capture Interface:	×	7
ţ	System Setup	Trace Route	IP:	Leave blank to match all addresses	]
品	Network	IP Subnetting	Port:		
ţţţ	Flow Control	Speed Test	MAC:		
۲	Access Controller	Diagnostics	Agreement Type:		Support tcp, udp, icmp, arp and other protocol types
<u>&amp;=</u>	Authentication	Watchdog	Storage location:	system Memory	•
<b>↓</b> ≯	Behavior		packet Number:	100	* Range: 1-80000
₿	Firewall			Start Packet	
Ţ	Advanced application				
0% 00	Services				
ſ'n	Log				

## Fig 10.2.1 Default Capture Packet page

	CMD-COS-v1.01						ථ	仑	۵	2	English
	≡<	Services <	Services > Captu	ure Packet		i CPU: 43.32%	MEM: 16%	↑ TX: 34	41.00 B/s	↓ RX	: 397.00 B/s
ଚ	System Overview	Ping Test	Capture r acke								
₩	Monitoring	Capture Packet		Capture Interface:	lan1	~					
ţţ	System Setup	Trace Route		IP:	192.168.0.100						
品	Network	IP Subnetting		Port:	80						
<b>111</b>	Flow Control	Speed Test		MAC:							
<b>P</b>	Access Controller	Diagnostics		Agreement Type:		Support tcp, udp, icmp,	, arp and other pro	tocol typ	95		
<u>8</u> "	Authentication	Watchdog		Storage location:	system Memory	~					
\$↓	Behavior			packet Number:	10	* Range: 1-80000					
臣	Firewall				Start Packet						
I	Advanced application										
0% 00	Services		Capture Results	file Time:	2021-05-12 22:34:50						
Ъ	Log			file Size:	1.84 KB						
				Used Memory:	1.84 KB						
					Download Document Delete						

Fig 10.2.2 Capture Packet result page

	CMD-COS-v1.01				තා 🗘 👃 English	
	≡<	Services <	Services > Capture Packet Capture Packet		n CPU: 43.32% 🥅 MEM: 16% ↑ TX: 341.00 B/s 🤳 RX: 397.00 B/	is 🍙
6)	System Overview	Ping Test			Tcpdump - Notepad - X	<
₩	Monitoring	Capture Packet	Capture Interface:	lan1	File Edit Format View Help	
ŝ	System Setup	Trace Route	IP:	192.168.0.100	Accept: application/json, text/plain, */*	^
뮮	Network	IP Subnetting	Port:	80	Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate	ł
†∔†	Flow Control	Speed Test	MAC:		Content-Type: application/json;charset=utf-8 Content-Length: 70	
	Access Controller	Diagnostics	Agreement Type:		Drigin: http://192.168.0.1 Connection: keep-alive	
<u>8</u> ,	Authentication	Watchdog	Storage location:	system Memory	Referer: http://192.168.0.1/ Dookie: sess_key=ef77baab2160dee710f854a037add658; username=admin; login=1	
⇆	Behavior		packet Number:	10	HTTP/1.1 200 OK	ł
臣	Firewall			Start Packet	Date: Wed, 12 May 2021 17:04:49 GMT Content-Type: application/json;charset=UTF-8	
5	Advanced application				Connection: close Server: Nainx	
	Services		Capture Results	2021-05-12 22:34:50	Expires: 0 Praama: no-cache	
Δ	Log		file Size:	1.84 KB	Cache-Control: no-cache K-LANG: 2	
			Used Memory:	1.84 KB	K-Timezone: 0800	¥
				Download Document Delete	e	T

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

	CMD-COS-v1.01				් රු 👃 🛆 English
	≡<	Services <	Services > Trace Route		≣ CPU: 2.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System Overview	Ping Test	Trace Route		
<u>w</u>	Monitoring	Capture Packet	Host:	www.google.com *	
ţĊ	System Setup	Trace Route	Source Interface:		V
뮮	Network	IP Subnetting	Max Hops:	5 *	
ţţţ	Flow Control	Speed Test	Timeout:	3 *	
<b>P</b>	Access Controller	Diagnostics	Result:		
<u>&amp;</u> "	Authentication	Watchdog			
₩	Behavior				
⊞	Firewall				
Ţ	Advanced application			Start	
0% 00	Services				
ቤ	Log				



	CMD-COS-v1.01					ථ	습	¢		English
	=<	Services <	Services > Trace Route	ې د C	PU: 43.32%	🛄 MEM: 16%	↑ TX: 34	1.00 B/s	↓ RX:	397.00 B/s
~			Trace Route							
(~)	Overview	Ping Test								
₩	Monitoring	Capture Packet	Host:	www.google.com *						
ţĊţ	System Setup	Trace Route	Source Interface:	Auto	~					
<u>д</u>	Network	IP Subnetting	Max Hops:	10 *						
ţţţ	Flow Control	Speed Test	Timeout:	30 *						
<b>P</b>	Access Controller	Diagnostics	Result:	4 static-mum-59.185.210.202.mtnl.net.in (59.185.210.202) 8.364 ms ms 7.379 ms	7.678 ^					
<u>8</u> =	Authentication	Watchdog		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 m 7 172 253 77 21 (172 253 77 21 11 172 006 ms 8.828 ms 8.858 ms						
₩	Behavior			8 hkg12s09-in-f4.1e100.net (216.58.203.4) 7.433 ms 7.595 ms 7.35	6 ms ¥					
田	Firewall			_						
Ţ	Advanced application			Start						
0% 00	Services									
ß	Log									

Fig 10.3.2 Trace Route particular website page

	CMD-COS-v1.01			තා 🗘 🗘 English
	<u></u> _<	Services <	Services > Trace Route	a∰≢CPU: 43.32% 🔛 MEM: 16% ↑ TX: 341.00 B/s ↓ RX: 397.00 B/s
$\mathfrak{S}$	System Overview	Ping Test	Trace Route	
₩	Monitoring	Capture Packet	Host:	192.168.0.102
ţ	System Setup	Trace Route	Source Interface:	Auto
뷺	Network	IP Subnetting	Max Hops:	10 *
†∔†	Flow Control	Speed Test	Timeout:	30 *
<b></b>	Access Controller	Diagnostics	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
<u>&amp;</u> =	Authentication	Watchdog		
₩	Behavior			
臣	Firewall			
V	Advanced application			Start
0% 00	Services			
R	Los			

#### 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

	CMD-COS-v1.01				් 🗘 🗘 ළ English
	=,	Services <	Services > IP Subnetting		≣⊑ CPU: 6.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
•			Subnet Calculator		
()	Overview	Ping Test			
₫	Monitoring	Capture Packet	IP Format:	IP Segment $\checkmark$	
ţĊţ	System Setup	Trace Route	IP Segment:	IP / Network Bit *	
品	Network	IP Subnetting			
ţţţ	Flow Control	Speed Test		Calculate	
<b></b>	Access Controller	Diagnostics	Network Address:		
<u>&amp;=</u>	Authentication	Watchdog	Subnet Mask:		
₩	Behavior		Address Range:		
臣	Firewall		Available Addresses:		
Ţ	Advanced application		Random Address:		
0%	Services				
ľð	Log				

Fig 10.4.1 Default Subnet Calculator page

	CMD-COS-v1.01					ධ	습	¢	2	English
	=,	Services <	Services > IP Subnetting		" CPU: 43.32%	🛄 MEM: 16%	↑ TX: 341	.00 B/s	↓ RX:	397.00 B/s
•	Surtem		Subnet Calculator							
(~)	Overview	Ping Test								
₩	Monitoring	Capture Packet	IP Format:	IP Segment $\checkmark$						
ţĊ	System Setup	Trace Route	IP Segment:	192.168.100.0 / 27	*					
品	Network	IP Subnetting								
ţţţ	Flow Control	Speed Test		Calculate						
<b></b>	Access Controller	Diagnostics	Network Address:	192.168.100.0						
<u>&amp;</u> =	Authentication	Watchdog	Subnet Mask:	255.255.255.224						
<del>⊊</del> ≯	Behavior		Address Range:	192.168.100.1 - 192.168.100.30						
臣	Firewall		Available Addresses:	30						
Ţ	Advanced application		Random Address:	192.168.100.16						
0%	Services									
ſð	Log									

Fig 10.4.2 IP Segment Subnet Calculator page

casoa	CMD-COS-v1.01					ථ	企	¢ 2	C English
	<u></u> _<	Services <	Services > IP Subnetting		" CPU: 43.32%	🛄 MEM: 16%	1 TX: 341.0	00 B/s 🚽	, RX: 397.00 B/s
	System		Subnet Calculator						
(~)	Overview	Ping Test							
∽	Monitoring	Capture Packet	IP Format:	IP Address 🗸					
ţĊţ	System Setup	Trace Route	IP Address:	10.10.10.10	*				
品	Network	IP Subnetting	Subnet Mask:	255.252.0.0 (14)	*				
ţţţ	Flow Control	Speed Test							
<b>P</b>	Access Controller	Diagnostics		Calculate					
<u>8</u> =	Authentication	Watchdog	Network Address:	10.8.0.0					
₩	Behavior		Subnet Mask:	255.252.0.0					
Ħ	Firewall		Address Range:	10.8.0.1 - 10.11.255.254					
y	Advanced application		Available Addresses:	262142					
0%	Services		Random Address:	10.11.41.12					
ß	Log								

#### 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

	CMD-COS-v1.01								් ර	4 2	Engl
	=<	Services <	Services > S	peed Test				📮 CPU: 15.009	6 🛄 МЕМ: 16% ↑ ТХ	∷:0.00 B/s 🦊 R	X: 0.0
	System		Speed Test	t							
(~)	Overview	Ping Test									
₽₽	Monitoring	Capture Packet	Select: Mbp	s V				Last tested tir	me is : 0 Select: All		Start
ţĊţ	System Setup	Trace Route	Interface	Min Rx Rate	Max Rx Rate	Averate Rx Rate	Min Tx Rate	Max Tx Rate	Average Tx Rate	Status	
₼	Network	IP Subnetting	Explain	: When the maximu operator maybe u	um and minimum rate c nstable.	liffer greatly, it is recomm	ended to re-measure	the speed. If the differen	nce is huge, the network p	provided by the	
†∔†	Flow Control	Speed Test									
<b></b>	Access Controller	Diagnostics									
<u>&amp;</u> =	Authentication	Watchdog									
₩	Behavior										
₿	Firewall										
Ţ	Advanced application										
0% 00	Services										
ľð	Log										

Fig 10.5.1 Default Speed Test page

-										
	CMD-COS-v1.01								_) û	.¢ _ Eng
	=,	Services <	Services > Sp	eed Test				📮 CPU: 43.32%	🛛 MEM: 16% ↑ TX: 34	1.00 B/s ↓ RX: 397
~			Speed Test							
6)	Overview	Ping Test								
<u>-</u>	Monitoring	Capture Packet	Select: Mbp	s ~			Last test	ed time is : 2021-05-11 2	3:46:30 Select: All	∽ Sta
ţĊţ	System Setup	Trace Route	Interface	Min Rx Rate	Max Rx Rate	Averate Rx Rate	Min Tx Rate	Max Tx Rate	Average Tx Rate	Status
品	Network	IP Subnetting	wan1	1.14 Mbps	1.58 Mbps	1.4 Mbps	0.29 Mbps	0.48 Mbps	0.36 Mbps	speedtest done
ţ₽ŧ	Flow Control	Speed Test	Explain	When the maxim operator maybe (	um and minimum rate o unstable.	differ greatly, it is recomm	ended to re-measure	the speed. If the differer	nce is huge, the network	provided by the
<b></b>	Access Controller	Diagnostics								
<u>8</u> =]	Authentication	Watchdog								
⇔	Behavior									
뀸	Firewall									
Ţ	Advanced application									
3 <b>%</b>	Services									
ſĿ	Log									

#### 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

	CMD-COS-v1.01						ධ	û	۵	<u>e</u> English
	=<	Services <	Services > Diagnostics			∎ CPU: 43.32%	🛄 MEM: 16%	1 TX: 3	41.00 B/s	↓ RX: 397.00
			Device Diagnostic							
(~)	Overview	Ping Test								
₩	Monitoring	Capture Packet	Total Diagnostic	Ouick Diagnostic						
ţĈ	System Setup	Trace Route	Diagnostic Your Device	Quick Diagnostic						
뮯	Network	IP Subnetting		flait						
ţţţ	Flow Control	Speed Test					D			
<b></b>	Access Controller	Diagnostics	Interfaces	JHCP	✓ PPPoE	Gateway	<ul> <li>The clouc platform connects the second seco</li></ul>	e		
<u>&amp;</u> =	Authentication	Watchdog					physical examinatio	n		
₩	Behavior									
Ħ	Firewall									
Ţ	Advanced application									
0% 00	Services									
ſð	Log									
### Fig 10.6.1 Default Device Diagnostic page

æ	CMD-COS-v1.01						۵	b 🟠 🔔 English
	=,	Services <	Services > Diagnostics				🔷 CPU: 43.32% 🔛 MEM: 16%	↑ TX: 341.00 B/s 👃 RX: 397.00 B/s
ର	System Overview	Ping Test						ľ
FAR	Monitoring	Capture Packet						
~			Interfaces	DHCP	PPPoE	Gateway	The cloud platform connects the physical exami	
÷	System Setup	Trace Route					nation	
몲	Network	IP Subnetting	Test comple	atod				
fi.	Flow Control	Speed Test	rest compie	eleu				
_	Access		Interfaces	Test completed				
	Controller	Diagnostics		Detect all the network line state.				
8.	Authentication	Watchdog		Exception: interface:wan1 domain:www.qq.com DNS ela	psed time:315.17ms HTTP elapsed tir	ne:access failure		
£	Behavior			Normal: interface:wan1 domain:www.baidu.com DNS ela	apsed time:126.56ms HTTP elapsed ti	me:226.67ms		
<i></i>			DHCP	Test completed				
Ħ	Firewall			Detect network DHCP service				
☑	Advanced application			Normal: interface:lan1 not found other DHCP services				
	Services		PPPoF	Test completed				
Γ <b>λ</b>	100			Detect network PPPOE service				
-0	cog			Normal: interface:lan1 not found other PPPOE services				
			Gateway	Test completed				
				Detection of intranet gateway ipaddress conflict or not				
				Normal: Interface:Ian   IP:192.166.0.1				
_			The cloud platform	Test completed				
			connects the	Connection success				
			examination	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



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

	CMD-COS-v1.01							් ර	슈 은 English
	≡<	Log <	Log > User Logs > .	Auth Logs			≡ <b>□</b> ≣ CPU: 0.50%	☐ MEM: 16% ↑ TX:	0.00 B/s ↓ RX: 0.00 B/s
Θ	System	User Logs	Auth Logs						
	Overview Monitoring	Auth Logs	Begin Time	() End Time	() Event		V IP/MAC/L	Isername Q Ex	Clean All
 کې	System Setup	ARP Logs	Time	Username	IP Address	Auth Type IP/MAC	Event	interface	Log Details
뷺	Network	Terminal Logs				No Data			
†∔†	Flow Control	Function Logs 🛛 🗸							
<b>P</b>	Access Controller	System Logs 🛛 🗸							
<u>&amp;</u>	Authentication								
₩	Behavior								
臣	Firewall								
,	Advanced application								
0%	Services								
ŀð	Log								

### 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

	CMD-COS-v1.01			් 🗘 🗘 🛆 English
	=,	Log <	Log > User Logs > ARP Logs	0.75% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
			ARP Logs	
(-)	Overview	User Logs 🔷 🔨		
₩	Monitoring	Auth Logs	Begin Time O End Time O Event Q	Export Clean All
ţĊţ	System Setup		Time Event	
品	Network	Terminal Logs	No Data	
ţţţ	Flow Control	Function Logs 🛛 🗸		
<b></b>	Access Controller	System Logs 🛛 🗸		
<u>&amp; -</u>	Authentication			
₩	Behavior			
臣	Firewall			
Ţ	Advanced application			
0% 00	Services			
ſð	Log			

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

	CMD-COS-v1.01								් ර	) ¢ 2	English
	=,	Log <	Log > User Logs >	Terminal Logs				📮 CPU: 0.75%	5 🛄 MEM: 16%	↑ TX: 0.00 B/s 🔱	RX: 0.00 B/s
-	System		Terminal Logs								
69	Overview	User Logs 🛛 🔿	and at								
₩	Monitoring	Auth Logs	Begin Time	C End lime	() All		← Full MAC Address	Q		(	Clean All
ţĊ	System Setup	ARP Logs	Time	MAC Address	MAC notes	АР	AP notes	BSSID	SSID	Signal Event Strength type	Action
뮮	Network	Terminal Logs					No Data				
†∔†	Flow Control	Function Logs $\sim$									
<b>P</b>	Access Controller	System Logs 🛛 🗸	Note: Th	is feature supports only Al	P version 1.1.2 and abo	ve					
<u>8</u> =	Authentication										
₩	Behavior										
Ħ	Firewall										
,	Advanced application										
0% 00	Services										
ſð	Log										

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

	CMD-COS-v1.01						ది	습 수 은 English
	≡<	Log <	Log > Function Logs > DHC	P Logs			📲 CPU: 6.93% 🔛 MEM: 16	% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
~	Sustem	Ŭ	DHCP Logs					^
6-3	Overview	User Logs 🛛 🗸						
₩	Monitoring	Function Logs 🛛 🔿	Begin Time	End Time		Q		Export Clean All
ţŷ;	System Setup	DHCP Logs	Time	msgtype	interface	MAC	IP	event
	N	DDNG	2018-05-31 21:30:30	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	
666	Network	DDNS Logs	2018-05-31 21:30:30	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	
ţţţ	Flow Control	VPN Logs	2018-05-31 21:30:30	DHCPOFFER	lan1	08:9b:4b:9e:f4:e3	192.168.1.100	
<b></b>	Access Controller	Notification Logs	2018-05-31 21:30:30	DHCPDISCOVER	lan1	08:9b:4b:9e:f4:e3		
<u>&amp;</u> =	Authentication	System Logs 🛛 🗸	2018-05-31 21:46:21	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	
<b>↓</b> ≯	Behavior		2018-05-31 21:46:21	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	
臣	Firewall		2018-05-31 21:46:21	DHCPOFFER	lan1	08:9b:4b:9e:f4:e3	192.168.1.101	
	Advanced		2018-05-31 21:46:21	DHCPDISCOVER	lan1	08:9b:4b:9e:f4:e3		
<u></u> ∠_	application		2018-05-31 21:43:18	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.1.100	
00	Services		2018-05-31 21:43:18	DHCPREQUEST	lan1	08:9b:4b:99:a3:94	192.168.1.100	
ŀ	Log		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

	CMD-COS-v1.01						۵	습 수 은 English
	=,	Log <	Log > Function Logs > DHC	P Logs			🛱 CPU: 0.25% 📮 MEM: 20%	↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
6	System	User Loas	DHCP Logs					
ب مم	Overview		Begin Time	End Time 🕓	IP/MAC Q			Export Clean All
-U -63	System Setun	DHCPLogs	Time	msgtype	interface	MAC	IP	event
~~~	Natwork	DDNS Logs	2021-05-13 18:54:24	DHCPACK	lan1	c4:d9:87:a7:ad:46	192.168.0.101	
	INELWOIK	DDNS Logs	2021-05-13 18:54:24	DHCPREQUEST	lan1	c4:d9:87:a7:ad:46	192.168.0.101	
ţţţ	Flow Control	VPN Logs	2021-05-13 18:43:27	DHCPACK	lan1	08:9b:4b:99:a3:94	192.168.0.105	
<b></b>	Access Controller	Notification Logs	2021-05-13 18:43:27	DHCPREQUEST	lan1	08:9b:4b:99:a3:94	192.168.0.105	
<u>8</u> =	Authentication	System Logs 🛛 🗸	2021-05-13 18:43:12	DHCPACK	lan1	08:9b:4b:9e:f4:e3	192.168.0.102	
⇆	Behavior		2021-05-13 18:43:12	DHCPREQUEST	lan1	08:9b:4b:9e:f4:e3	192.168.0.102	
開	Firewall		2021-05-13 17:54:24	DHCPACK	lan1	c4:d9:87:a7:ad:46	192.168.0.101	
	Advanced		2021-05-13 17:54:24	DHCPREQUEST	lan1	c4:d9:87:a7:ad:46	192.168.0.101	
	application		2021-05-13 17:54:24	DHCPOFFER	lan1	c4:d9:87:a7:ad:46	192.168.0.101	
öõ	Services		2021-05-13 17:54:24	DHCPDISCOVER	lan1	c4:d9:87:a7:ad:46		
ſ	Log		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

	CMD-COS-v1.01						٤	Ĵ 습 🗘 은 English
	⊒<	Log <	Log > Function Log	s > DDNS Logs			=☐= CPU: 9.25% 🛄 MEN	/i: 16% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~	System	Ŭ	DDNS Logs					
6-3	Overview	User Logs 🛛 🗸						
₩	Monitoring	Function Logs	Begin Time	C End Time	()			Export Clean All
ţĊţ	System Setup	DHCP Logs	Time ∽	IP Address	Domain Name 🗸	Interface $\checkmark$	Result	Log Details
	Network	DDNS Logs				No Data		
†∔†	Flow Control	VPN Logs						
<b>R</b>	Access Controller	Notification Logs						
8= ;;-	Authentication	System Logs 🛛 🗸						
⇔	Behavior							
Ħ	Firewall							
Ţ	Advanced application							
0% 00	Services							
ß	Log							

# Fig 11.2.3 Default DDNS Logs page

	CMD-CO5-v1.01						ත	습 수
	⊒<	Log <	Log > Function Logs > DDNS	Logs			📫 CPU: 0.00% 🛄 MEM: 209	6 ↑ TX: 69.00 B/s 🤳 RX: 73.00 B/s
-		<b>,</b>	DDNS Logs					
69	Overview	User Logs 🛛 🗸						
22	Monitoring	Function Logs	Begin Time	End Time				Export Clean All
ŝ	System Setup	DHCP Logs	Time $\lor$	IP Address	Domain Name 🗸	Interface $\checkmark$	Result	Log Details
			2021-05-13 19:10:13		www.commandonetworks.com	Auto	fail	Error: domain errors
楍	Network	DDNS Logs	2021-05-13 19:05:03		www.commandonetworks.com	Auto	fail	Error: domain errors
t†	Flow Control	VPN Logs	2021-05-13 19:00:05		www.commandonetworks.com	Auto	fail	Error: domain errors
<b>P</b>	Access Controller	Notification Logs	2021-05-13 18:55:07		www.commandonetworks.com	Auto	fail	Error: domain errors
<u>&amp;</u> "	Authentication	System Logs 🛛 🗸	2021-05-13 18:50:08		www.commandonetworks.com	Auto	fail	Error: domain errors
₩	Behavior		2021-05-13 18:45:17		www.commandonetworks.com	Auto	fail	Error: domain errors
臣	Firewall		2021-05-13 18:40:04		www.commandonetworks.com	Auto	fail	Error: domain errors
1	Advanced		2021-05-13 18:35:02		www.commandonetworks.com	Auto	fail	Error: domain errors
¥.	application		2021-05-13 18:30:08		www.commandonetworks.com	Auto	fail	Error: domain errors
	Services		2021-05-13 18:25:03		www.commandonetworks.com	Auto	fail	Error: domain errors
Ъ	Log		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

	CMD-COS-v1.01		් ර 4 & E	inglish
	_<	Log <	Log > Function Logs > VPN Logs 📫 CPU: 0.00% 🛄 MEM: 16% ↑ TX: 0.00 B/s \downarrow RX:	: 0.00 B/s
~	System	3	VPN Logs	
6-3	Overview	User Logs 🛛 🗸		
₩	Monitoring	Function Logs	All V Begin Time O End Time O Log Details Q Export Clear	n All
ţĊ	System Setup	DHCP Logs	Time Interface Log Details	
 ₽	Network	DDNS Logs	No Data	
ţţţ	Flow Control	VPN Logs		
<b></b>	Access Controller	Notification Logs		
<u>8</u> =	Authentication	System Logs 🛛 🗸		
, ¢	Behavior			
Ħ	Firewall			
Ţ	Advanced application			
0% 00	Services			
ß	Log			

Fig 11.2.5 Default VPN Logs page

	a				ے کے کرے درم
		Log <	Log > Function Logs > VPN Logs		ដ្នោះ CPU: 0.50% 🛄 MEM: 20% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/
6	System	User Logs →	VPN Logs		
ۍ پ	Overview		All 🗸 Begin Time	C End Time C Log Details	Q Export Clean All
ЪM	Monitoring	Function Logs			
ţ	System Setup	DHCP Logs	lime	Interface	Log Details
뷺	Network	DDNS Logs	2021-04-18 17:12:41	pptpCOMMANDO	Call manager exited with error 256
<b>611</b>	Flam Castral		2021-04-18 17:12:41	pptpCOMMANDO	Exit.
IŧŢ	Flow Control	VPIN Logs	2021-04-18 17:12:41	pptpCOMMANDO	Could not open control connection to 10.10.10.1
<b>P</b>	Access Controller	Notification Logs	2021-04-18 17:12:41	pptpCOMMANDO	connect: Connection timed out
<u>8</u> =	Authentication	System Logs 🛛 🗸	2021-04-18 17:10:23	pptpCOMMANDO	Call manager exited with error 256
<b>↓</b> ≯	Behavior		2021-04-18 17:10:23	pptpCOMMANDO	Exit.
田	Firewall		2021-04-18 17:10:23	pptpCOMMANDO	Could not open control connection to 10.10.10.1
	Advanced		2021-04-18 17:10:23	pptpCOMMANDO	connect: Connection timed out
Ľ₽	application		2021-04-18 17:08:06	pptpCOMMANDO	Call manager exited with error 256
00	Services		2021-04-18 17:08:06	pptpCOMMANDO	Exit.
ß	Log		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.

	CMD-COS-v1 01		් රු 🗘 English
	=,	log <	Log > Function Logs > Notification Logs 🕹 TX: 0.00 B/s 🤳 RX: 0.00 B/s
<b>•</b>	System	209	Notification Logs
6-9	Overview	User Logs 🛛 🗸	
₩	Monitoring	Function Logs 🛛 🔿	Begin Time () End Time () Type V IP Q Export Clean All
ţĊ	System Setup	DHCP Logs	Time IP Address Event Type
♣	Network	DDNS Logs	No Data
†∔†	Flow Control	VPN Logs	
<b>P</b>	Access Controller	Notification Logs	
<u>&amp;=</u>	Authentication	System Logs 🛛 🗸	
⇆	Behavior		
Ħ	Firewall		
Ţ	Advanced application		
0% 00	Services		
ſŊ	Log		

#### 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.

	CMD-COS-v1.01			스> 슈 슈 온 English
	⊒<	Log <	Log > System Logs > System Logs	=☐= CPU: 0.00% 🛄 MEM: 20% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
~			System Logs	
(-)	Overview	User Logs 🛛 🗸		
₩	Monitoring	Function Logs	Begin Time O End Time O Event Q	Export Clean All
ŝ	System Setup	System Logs	Time Event	
Д.	Network	System Logs	2021-05-13 17:44:38 Chain detection: interface (veth5) up	
<b>611</b>	FI 6	A 12 - 1	2021-05-13 17:44:38 Chain detection: interface (veth4) up	
[]+T]	Flow Control	Action Logs	2021-05-13 17:44:38 Chain detection: interface (veth3) up	
<b></b>	Access Controller	Notification	2021-05-13 17:44:38 Chain detection: interface (veth2) up	
<u>&amp;</u> =)	Authentication		2021-05-13 17:44:26 Chain detection: interface (veth5) up	
₩	Behavior		2021-05-13 17:44:26 Chain detection: interface (veth4) up	
田	Firewall		2021-05-13 17:44:26 Chain detection: interface (veth3) up	
Ē	Advanced		2021-05-13 17:43:55 System Starting	
Ľ,	application		2021-05-13 17:43:44 Chain detection: (wan1)detected	
04	Services		2021-05-13 17:39:22 Chain detection: interface (veth5) up	
ß	Log		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.

	CMD-COS-v1.01			🛆 රු 👃 🛆 English
	≡<	Log <	Log > System Logs > Action Logs	🛱 CPU: 1.49% 🛄 MEM: 16% ↑ TX: 0.00 B/s 🤳 RX: 0.00 B/s
6	System	_ User Logs ∨	Action Logs	
<u></u>	Monitoring	Function Logs 🗸 🗸	Begin Time         (C)         End Time         (C)         IP/Username         Q	Export Clean All
ţ	System Setup	System Logs 🛛 🔿	Time Username IP Address	Function Event
品	Network	System Logs	No Data	
ţ†ţ	Flow Control			
<b></b>	Access Controller	Notification		
<u>&amp;</u> =	Authentication			
$\stackrel{\downarrow \ast}{\downarrow}$	Behavior			
臣	Firewall			
Ţ	Advanced application			
0% 00	Services			
ſð	Log			

Fig 11.3.2 Default Action Logs page

	CMD-COS-v1.01						스) 습 🗘 🛆 English
	⊒<	Log <	Log > System Logs > A	Action Logs		" CPU: 1.49%	□ MEM: 20% ↑ TX: 0.00 B/s ↓ RX: 0.00 B/s
•	Surtem		Action Logs				
(-)	Overview	User Logs 🛛 🗸					
₽2	Monitoring	Function Logs $\sim$	Begin Time	() End Time	() IP/Username Q		Export Clean All
ţĊţ	System Setup	System Logs	Time	Username	IP Address	Function	Event
모	Naturali	System Logs	2021-05-13 18:01:52	admin	192.168.0.100		Login
666	Network	System Logs	2021-05-12 23:04:34	admin	192.168.0.100	Speed	Test exec action for clean
†∔†	Flow Control	Action Logs	2021-05-12 21:06:19	admin	192.168.0.100		Login
<b></b>	Access Controller	Notification	2021-05-12 20:10:29	admin	192.168.0.100		Login
<u>&amp;</u> =)	Authentication		2021-05-12 20:10:29	admin	192.168.0.100		Login
₩	Behavior		2021-05-12 20:07:44	admin	192.168.0.100		Login
臣	Firewall		2021-05-11 23:45:04	admin	192.168.0.100	Speed	Test exec action for clean
_	Advanced		2021-05-11 23:26:50	admin	192.168.0.100	UDPXY	Set exec action for edit
<u>_</u>	application		2021-05-11 23:26:33	admin	192.168.0.100	UDPXY	Set add a rule
0%	Services		2021-05-11 23:26:17	admin	192.168.0.100	UDPXY	Set exec action for edit
ß	Log		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.

	CMD-COS-v1.01					් ර	수 은 English
	=<	Loa <	Log > System Logs > Notification			🗒 CPU: 1.73% 🛄 MEM: 16% ↑	TX: 0.00 B/s 🔱 RX: 0.00 B/s
-	-		Notification				
6)	Overview	User Logs 🛛 🗸 🗸					
₩	Monitoring	Function Logs $\sim$					Clean All
ţĊţ	System Setup	System Logs 🛛 🔿	Username	Time		Actions	
品	Network	System Logs			No Data		
ţţţ	Flow Control	Action Logs					
<b></b>	Access Controller						
<u>&amp;</u> =	Authentication						
⇆	Behavior						
Ħ	Firewall						
Ţ	Advanced application						
0% 00	Services						
ĥ	Log						

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 <a href="http://commandonetworks.com.cn/">http://commandonetworks.com.cn/</a> ---> gets the binding code ---> enters the binding code in router and remark name ---> saves and completes the binding.

#### How to manage?

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

#### How to unbind the cloud?

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



### Fig 12.1 Cloud Login page





### Fig 12.3 Cloud Binding page

#### 12.1 AirPRO Cloud Overview

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



Fig 12.1.1 Default Cloud Overview page



Fig 12.1.2 Cloud Overview page



Fig 12.1.3 Cloud User online trend page



Fig 12.1.4 Cloud User Type page

### 12.2 Network

Cloud Networking Solutions are Designed to Enhance Your access and IT infrastructure in which some or all of an organization's network capabilities and resources are hosted cloud account.

COMMAND	Cloud	Network	Configuration	Message	Personal			A Englist
() Overviev	v I	Network / Network						
👳 Network								
. P₌ Manage		Bulk Configuration				Na	me	Q
		Name	Chadrup 🔺	CIMID	Event ID	Version A	Chature	Config
		Indiffe	Status 🚽	GWID	Export IP	version 🚽	Status -	, coniig
					No Data			

Fig 12.2.1 Default Bulk configuration page

Clo	ud	Network	Configuration	Message	Personal					Ą	English
() Overview	Networ	k / Network									
Network											
♀ Manage	Bulk	c Configuration						Name			Q
		Name	Status 🗢	GWID		Export IP	Version 韋		Status	÷	Config
	~	<ul> <li>testing</li> </ul>	Online	247ce0632ect d00818e8	38bde3e5053d6	182.59.62.184 (印度 )	3.4.5.CMD-CC Id2020111617	DS-v1.01 x32 Bui 736	Closed	ł	<u>Config</u>
		Outline: Online Users: <b>4</b> Today's Certificat	ion 0								
		Routing Mainten	ance: Direct Login	Upgrade	Restart	Jntie					
				Total 1	10/page $\lor$	< 1 > Go to	1				

Fig 12.2.2 Bulk configuration page

Clo	Network	Configuration	Message	Personal										S	۸	English
Overview	Network / Network /	testing														
Network	testing	~ 🗹													Alarm	<b>0/ 0/</b> 0
8 Manage																
		Gateways (online / tot	tal)		AP (Online / Total)					Authori	zed User / Online U	Jser				
		1/1				<u>2/2</u>	1			9/4						
	Wireless D	evice Trend 5G														
	3											****00***0		• • • • • •		
	0 ¢ 0 Export Flov 341.8 K8	5-11 20:23:59 05-11 21:13: <b>v Trend=</b> Upstream Traffic	59 05-11 22:03: Downstream Traff	59 05-11 22:54:00	05-12 00:14:13	05-12 01:04:19	05-12 01:54:12	05-12 22:50:47	05-13 01:04:22	05-13 01:54:21	05-13 20:23:18	05-13 21:13:24	05-13 22:03	3:19	3	
	292.97 KB 244.14 KB			/												
	195.31 KB															
	146.48 KB															
	48.83 KB 0 B															



# Fig 12.2.3 Network Devices listed in Cloud page

### Fig 12.2.4 Gateway page

	Network oud	Configuration	Message Personal			% ନ୍ୟୁ	English
() Overview	Network / testing / Al	P List					
Pretwork							
🖓 Manage	Remarks	Q			Upgrade	Restart	Return
	Status 🤤 Rema	arks 🤤	Address: {0} 🤤	Version 🤤	Model 🤤	Operation	
	Online		08:9b:4b:9e:f4:e3	1.5.9	AP	<u>View</u>	
	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

Clou				
Overview	Details			×
A Manage	Device Name Model X2 Version 1.6.6 MAC: 08:9b:4b:99:a3:94 Running Time: Status Online	Rate 48.83 KB/s 39.06 KB/s 29.3 KB/s 9.77 KB/s 0 B/s 0000000000000000000000000000000000	Upload Speed     Download Speed     Download Speed     I8:15     I8:30     I8:45     I9:00     I9:15     I9:30     I9:45     20:00	▲ Return
	Wireless Device Trend User		<b>.</b>	

Fig 12.2.5 Bulk configuration for particular AP Device page

Clo	ud	Network	Configu	ration M	essage F	Personal				S A	English
() Overview	Net	twork / Manage	ment								
🖳 Network											
9₌ Manage		testing									Q
		Device ≑	IP 🜲	MAC 🜲	AP_MAC 🜲	Total Tx 韋	Total Rx ≑	Total Time ≑	Online time	Operation	
		DESKTOP-7 0API5S	192.168.0.10 1	c4:d9:87:a7:a d:46	c4:d9:87:a7:a d:46	6.14 MB	61.47 MB	2 Hour 19 Minut e 11Second	2021-05-13 17:5 4		
			192.168.0.10 0	e0:db:55:be: 35:5b	e0:db:55:be: 35:5b	1.01 KB	11.43 KB	2 Hour 12 Minut e 32Second	2021-05-13 18:0 1		
		AP	192.168.0.10 2	08:9b:4b:9e:f 4:e3	08:9b:4b:9e:f 4:e3	680.00 Byte	708.00 Byte	2 Hour 30 Minut e 20Second	2021-05-13 17:4 3		
		AP	192.168.0.10 5	08:9b:4b:99:a 3:94	08:9b:4b:99:a 3:94	500.00 Byte	567.00 Byte	2 Hour 30 Minut e 5Second	2021-05-13 17:4 3		
					Total 4 10	)/page <	1 > G	io 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.

Clo	Network Col ud	nfiguration Mes	sage Personal			Æ	English
Certificate	Authentication / Config Templa	ate 🕐					
®™ Wireless	Configure Gateway						
☐ Backup	Advanced Settings >	Template Server	Select Cloud Platform Customize Web-Radius Save	^			

Fig 12.3.1 Default Authentication page

Clo	Network Configuration Message Personal Id
(2) Certificate	Authentication / Config Template 📀
010 Wireless	Configure Gateway
G Backup	Template
	Server Cloud Platform V
	Certification Process: Global Portal V
	Select Authentication Method:
	Choose A Template 1 Configuration Page:
	Select Networking Mode Network connection

Fig 12.3.2 Default Cloud platform configure gateway page

Cloud	Network	Configuration	Message	e Personal
Certificate Wireless	Free Certifica	ation Setting Free cer	tification:	Add MAC addresses that do not require
Ск раскир				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 IF	• whitelist	Whitelist IP format: 8.8.8.8, 8.8.8.1- 8.8.8.255, 8.8.8.0/24 (one per line)
		Certificati	on Range	All O Partial IP

Fig 12.3.3 Default Authentication Free certification setting page

COMMANDO	Cloud	Network	Configuration	Message	Personal	Æ	English
I Certifica ♥♥ Wireles	ate s	Device Display S	etting ↓ iPhone Portal P Android Portal P Timeout Set	age: age: ting: After authe Cont Note: Authe	ntication 0 Minutes need recertification nued 0 Minutes need re-authenticate when no traffic utication mode configuration takes		
				Save	l		

Fig 12.3.4 Default Authentication Device Display setting page

COMMANDS	Cloud	ł	Netwo	ork	Configuration	Message	Personal						<u></u> ₽	English
🖲 Certifica	te	Conf	iguration /	Wireless										
🕪 Wireless			Add											
			Template Name	Frequ ency Band	Preferred/ Secondary	SSID4 Security:	Hidde n Or Not	Guest	Bind NIC	MIN Access Sig nal	MAX Us ers	Timed On	Oper	ration
							No	Data						
		Т	ip: After addi	ng a temp	plate, you can go to the" I	Network Managem	ent "page	and use t	he" Bulk Con	figuration "option t	o deliver th	ne templat	te.	

# Fig 12.3.5 Default Wireless add setting page

Cloud	Network	Configuration	Message	Personal				
Certificate		Template Name	COMMANDO					
🙌 Wireless		2.4G 5G	Extended fund	ctions				
		5GNetwork:						
	SSID1				SSID	D2		
		SSID1SSID Name	123			SS	ID255ID Name	
		SSID4 Security:	No Password			:	SSID4 Security:	No Password
		Bind NIC name	LAN3				Bind NIC name	LAN1
		Hide SSID4 Name:	Enable			Hid	e SSID4 Name:	Enable
		Guest	Enable(Prohibit	mutual visits and access to wire	i)		Guest	Enable(Prohibit mutual visits and access to v

Fig 12.3.6 Add 5G Wireless setting page

COMMANDO CI	loud	Network	Co	nfiguration	Message	Personal						S	<u></u> ₽	English
🖲 Certificate	Co	onfiguration / Wire	eless											
<b>Wireless</b>														
Backup		Add												
		Template Na me	Frequen cy Band	Preferred/ Sec	ondary	SSID4 Security:	Hidden Or Not	Guest	Bind NIC	MIN Access Signal	MAX User s	Timed On	Operat	tion
		COMMAND O	2.4G 5G	-/- 123/-		No Password/No P assword No Password/No P assword	No/No No/No	Off/Off Off/Off	lan1/lan1 lan3/lan1	1% (-94.40) 1% (-94.40)	Unlimited Unlimited	Closed	<u>Modif</u> <u>ete</u>	<u>y Del</u>
						Total 1 10/page	~ <	1 >	Go to 1					
		Tip: After adding a	template,	you can go to the	* Network Mana	igement "page and use	the" Bulk Co	onfiguration	n "option to deliv	er the template.				

Fig 12.3.6 Wireless Configuration setting page

Clo	Network ud		Message	Personal		Æ	English
💷 Certificate	Configuration / Wireles	s Template / Wireless					
🕅 Wireless	Wireless						
Backup							
		Template Name					
		2.4G 5G	Extended fun	actions			
		Timed On	Plan 1				
			Plan 2				
			Plan 3				
			Save	Cancel			

Fig 12.3.7 Default Wireless Configuration Extended function setting page

Network		Message Personal	<u></u> ₽	English
<ul> <li>☑ Certificate</li> <li>♥ Wireless</li> <li>ᢙ Backup</li> </ul>	Template Name 2.4G 5G Timed On	Extended functions         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

СІо	Network	Configuration	Message	Personal		S	A Eng	glish
🖲 Certificate	Configuration / Cloud	Backup						
0r0 Wireless								
C Backup	Name	Q						
	Name		GWID	Manual Backup:	Auto Backup		Operation	
				No Data				
			Total 0	10/page V < 1 > Go to	1			

Fig 12.3.9 Default Configuration backup setting page



Fig 12.3.10 Backup Configuration setting page

Clo							
Certificate							
(ij) Wireless		Cloud Backup		×			
A Backup		GWID:	247ce0632ec88bde3e5053d6d00818e8				
	Name	Router	testing	_	Auto Backup		
	testing	Manual Backup:	Backup Config				
		Automatic Backup					
			Period: Weekly Month	_			
			Weekly: Saturday $\lor$	_			
			Moment: © 00:18	_			
			Save	_			
			Cancel				

### 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.

COMMAND	Cloud		Network	Configuration	Message	Personal				S	R	English
🖪 Log	Mes	ssage /	Log									
		Logir	n / logout	Upgrade / Restart	Configuration / (	Operation			То			Filter
			Action		IP		Time					
		>	user logged	d in cloud platform	10.172.128.196	5	2021-05-1	4 01:06:14				
		>	user logged	d in cloud platform	10.172.128.196	5	2021-05-1	3 22:55:24				
		>	user logged	d in cloud platform	10.172.128.196	5	2021-05-1	3 22:22:39				
		>	user logged	d in cloud platform	10.172.128.196	5	2021-04-2	2 23:57:55				
		>	user logged	d in cloud platform	10.172.128.196	5	2020-12-1	0 00:12:28				
		>	user logged	d in cloud platform	10.172.128.196	5	2020-12-0	3 20:32:58				
		>	user logged	d out			2020-12-0	3 20:32:55				
		>	user logged	d in cloud platform	10.172.128.196	5	2020-12-0	3 20:27:22				
		>	user logged	d in cloud platform	10.172.128.196	5	2020-11-2	6 16:41:27				
		>	user logged	d in cloud platform	10.172.128.196	5	2020-11-2	6 11:56:52				

Fig 12.4.1 Default Login and Logout page

COMMANDO	Cloud	Network	Configuration	Message	Personal						R	English
🖪 Log		Message / Log										
		Login / logout	Upgrade / Restart	Configuration /	Operation			Start Date	То	End Date		Filter
		Action		IP				Time				
						No Data						
				Total 0	10/page 🗸	< 1 >	Go to 1					

Fig 12.4.2 Default Upgrade and Restart page

COMMANUE	Cloud	Network	Configuration	Message	Personal								Ą	English	
🖪 Log		Message / Log													
		Login / logout	Upgrade / Restart	Configuration /	Operation				Start Date	То	End Date	<u>}</u>		Filter	
		Action		IP					Time						
						No Data									
				Total 0	10/page V	< 1 >	Go	to 1							

Fig 12.4.3 Default Configuration and operation page

COMMANDO	Cloud		Network	Configuration	Message	Personal			Ą	English
🖪 Log	Me	essage /	Log							
		Logi	n / logout	Upgrade / Restart	Configuration / (	Operation		💼 Start Date <b>To</b>		Filter
			Action			IP		Time		
		>	Delete tem	nplate successfully		10.172.128.196		2021-05-14 01:39:04		
		>	Add templa	ate successfully		10.172.128.196		2021-05-14 01:35:10		
		>	Open auth	entication		10.172.128.196		2021-05-13 22:53:02		
		>	Close auth	entication		10.172.128.196		2020-11-17 19:21:59		
		>	Open auth	entication		10.172.128.196		2020-11-17 19:02:25		
						Total 5 10/page V	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

Clou	Network ud	Configuration Message Personal	ି େ ମ୍≧ English
A Information			
🕀 Account		Modify the bound phone X	
	Account: Registration Data:	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	
	Mobile Number	Current Mob nu mber:	
		Next	

Fig 12.5.2 Modify Personal Information page