SY40-4G Industrial Router

USER MANUAL

V1.0

1. Product Description

The SY40 Industrial-Grade Wireless Router is a high-performance communication device developed by Shenzhen Shiyun Technology for 4G network applications. It is designed for industrial data transmission, supporting:

- Transparent data transfer
- Image transmission
- Equipment monitoring
- Wireless routing

Key Features:

- 32-bit high-speed processor
- Multi-mode 4G support (WCDMA/EVDO/TD-SCDMA/TD-LTE/FDD-LTE)
- Interfaces:
    - 10/100M Ethernet

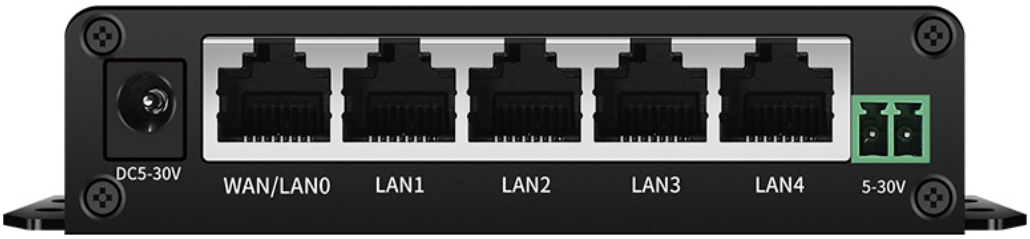
- WIFI
- Serial port (RS232/RS485)

- WEB-based configuration

1.1 Physical Appearance

1.2 Interface Specifications

Panel A:



Panel B:

Panel A:

1. LAN0-LAN4 Ports

- Standard RJ45 connectors with LED indicators
- Functionality: LAN0 configurable as WAN port in standard router mode

2. DC Power Input

- 2.1mm barrel jack (center-positive polarity)
- Voltage range: 5-30V DC

3. Terminal Block Power Input

- 3.81mm pitch 2-pin terminal (left=positive)
- Voltage range: 5-40V DC

Panel B:

1. Antenna Connectors

SMA female (reverse polarity) for:

- 3G/4G cellular
- WIFI

2. LED Indicators

LED	State	Status Description
SYS	Solid ON	Power supplied
	Fast blink	Reset activated (8-second hold)
LINK	Fast blink	Dialing (3G/4G/WIFI bridging)
	Solid ON	Network connected

3. Reset (R) Button

- Press and hold for 8 seconds to trigger factory reset
- Visual confirmation: SYS LED fast blink → reboot

4. SIM Card Slot

- Push-pull mechanism (press yellow button to eject tray)
- Optional: Industrial SMD SIM with:
  - Extended temperature tolerance
  - Vibration/water resistance
  - Pre-programmed ICCID (activation required)

LED Status Indicators

Name	State	Description
SYS (System)	Solid ON	Indicates normal power supply (activated upon boot).
	Slow Blink	System operational (activates ≈10 seconds after power-on).
	Fast Blink	Reset triggered (hold reset button for 5 seconds). System will reboot automatically.
LINK	Solid ON	Network connection established (3G/4G/Wi-Fi).
	Slow Blink	Connected with active data transmission.
	Off	No network connection.
LAN	Solid ON	Ethernet link active (RJ45 port connected).
	Off	No Ethernet connection detected.

Reset Button Operation

1. Activation

Press and hold the **RESET** button for **8 seconds** until:

- The **SYS LED** blinks rapidly (2Hz)
- The router initiates an automatic reboot

2. Completion

Successful reset is confirmed when:

a) SYS LED returns to **slow blink (0.5Hz)**
b) All network interfaces reinitialize

Power Supply

- **Connector:** 2.1mm DC jack (center-positive)
- **Voltage Range:** 5-30V DC (12V recommended for optimal performance)

Antenna Ports

Type: SMA female (reverse polarity)
Configuration:
Port 1&2: 3G/4G cellular (recommended gain: 3-5dBi)
Port 3&4: WIFI (supports up to 15dBi gain)

Users may select appropriate antennas based on application requirements. Higher antenna gain (measured in dBi) generally improves wireless transmission range and reception quality.

2. Connection Preparation

2.1 Connect the equipment

To connect your computer to the router, follow these steps:

2.1.1 Configuring the Computer's IP Address

Before accessing the web configuration interface, it is recommended to configure your computer to:

- "Obtain an IP address automatically"
- "Obtain DNS server address automatically"

This allows the router to assign IP addresses via DHCP.

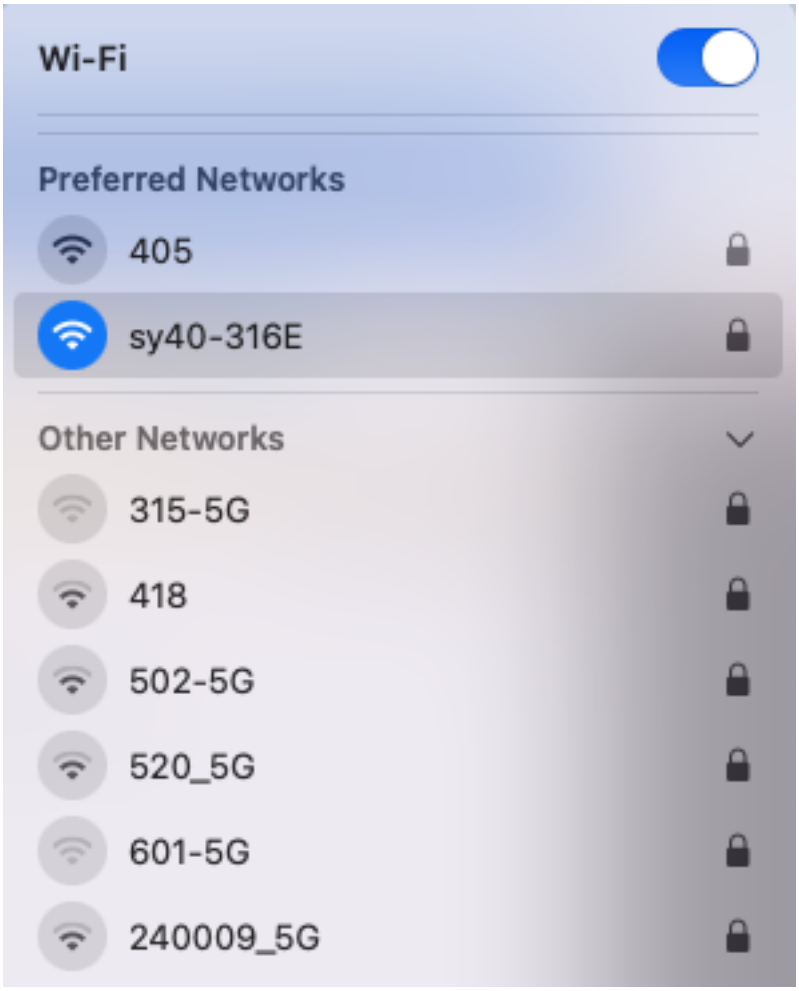
For static IP configuration:

The computer's IP address must reside in the same subnet as the router's LAN interface
Default router LAN IP: 192.168.1.1
Subnet mask: 255.255.255.0

2.1.2 Wi-Fi Connection Setup

To establish WIFI connectivity:

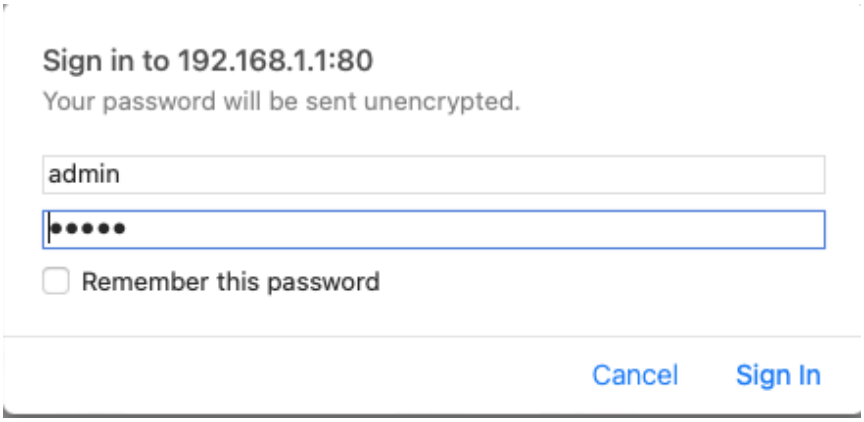
- Detect and select the wireless network broadcast by your router
- Initiate connection by clicking the '**Join**' button
- Enter the Password: 12345678



2.2 Accessing the Router

To access the web interface:

1. Open a browser and enter: **http://192.168.1.1**
2. At the login prompt:
   - **Username**: admin (default)
   - **Password**: admin (default)

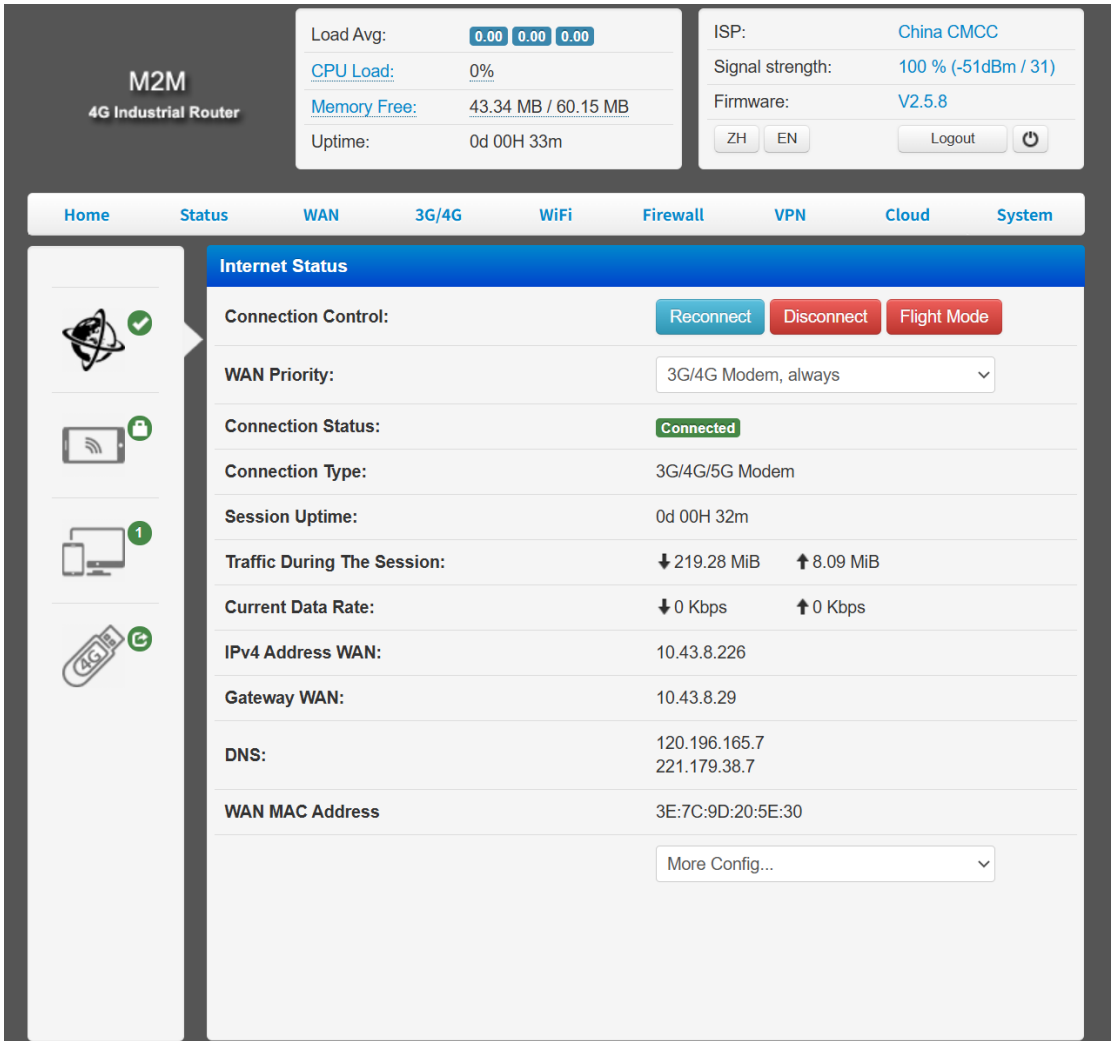


2.3 Router Web Interface

After successful login:

1. Home

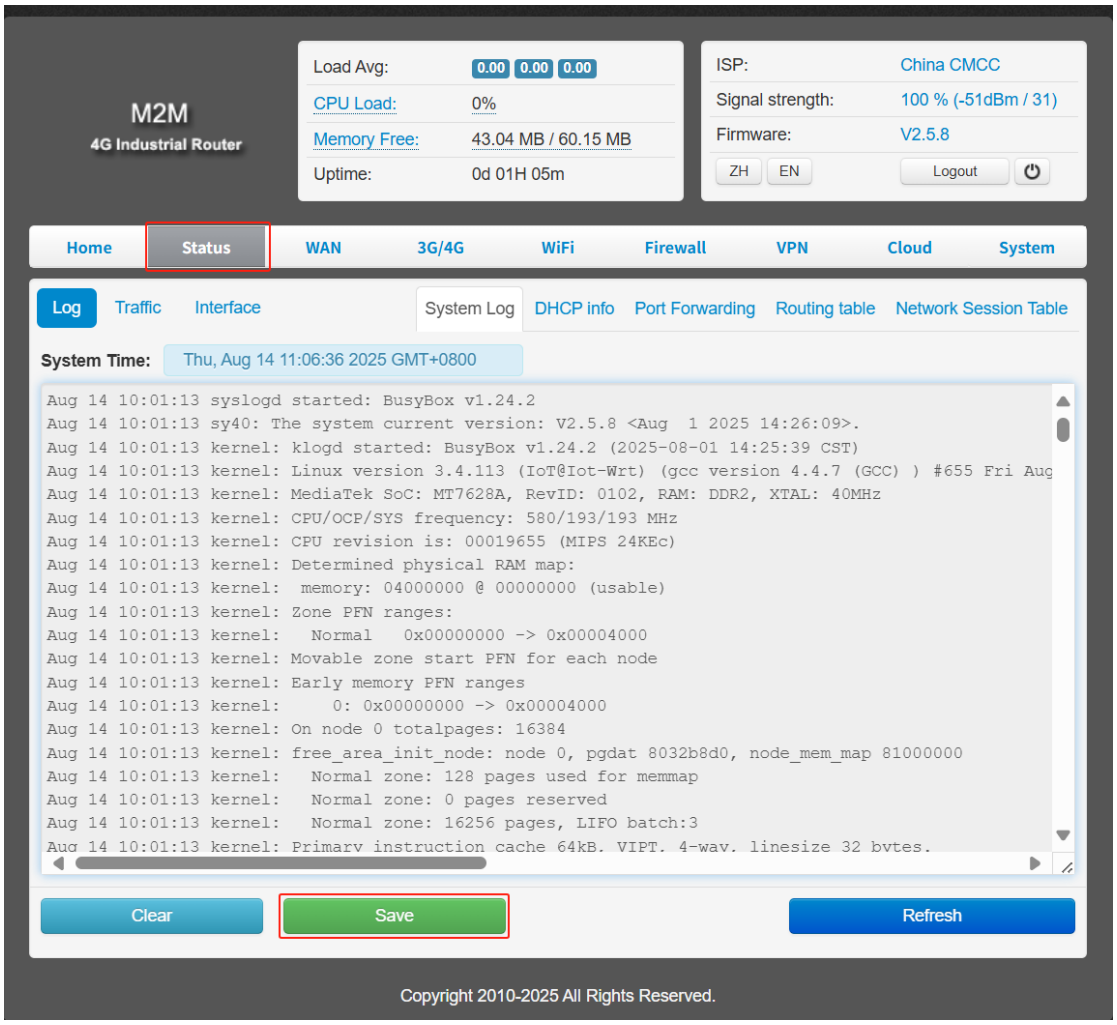
The configuration dashboard will appear for router setup and management



2. Status

System Log (Troubleshooting):

- If you encounter any issues with the router during use, please provide us with a system log for analysis.
- To copy logs:
  a. Navigate to Status Log section
  b. Click “Save” to copy all log texts



3. WAN

This section comprises two functional modules: WAN (External Network) and LAN (Internal Network).

3.1 WAN(External Network)

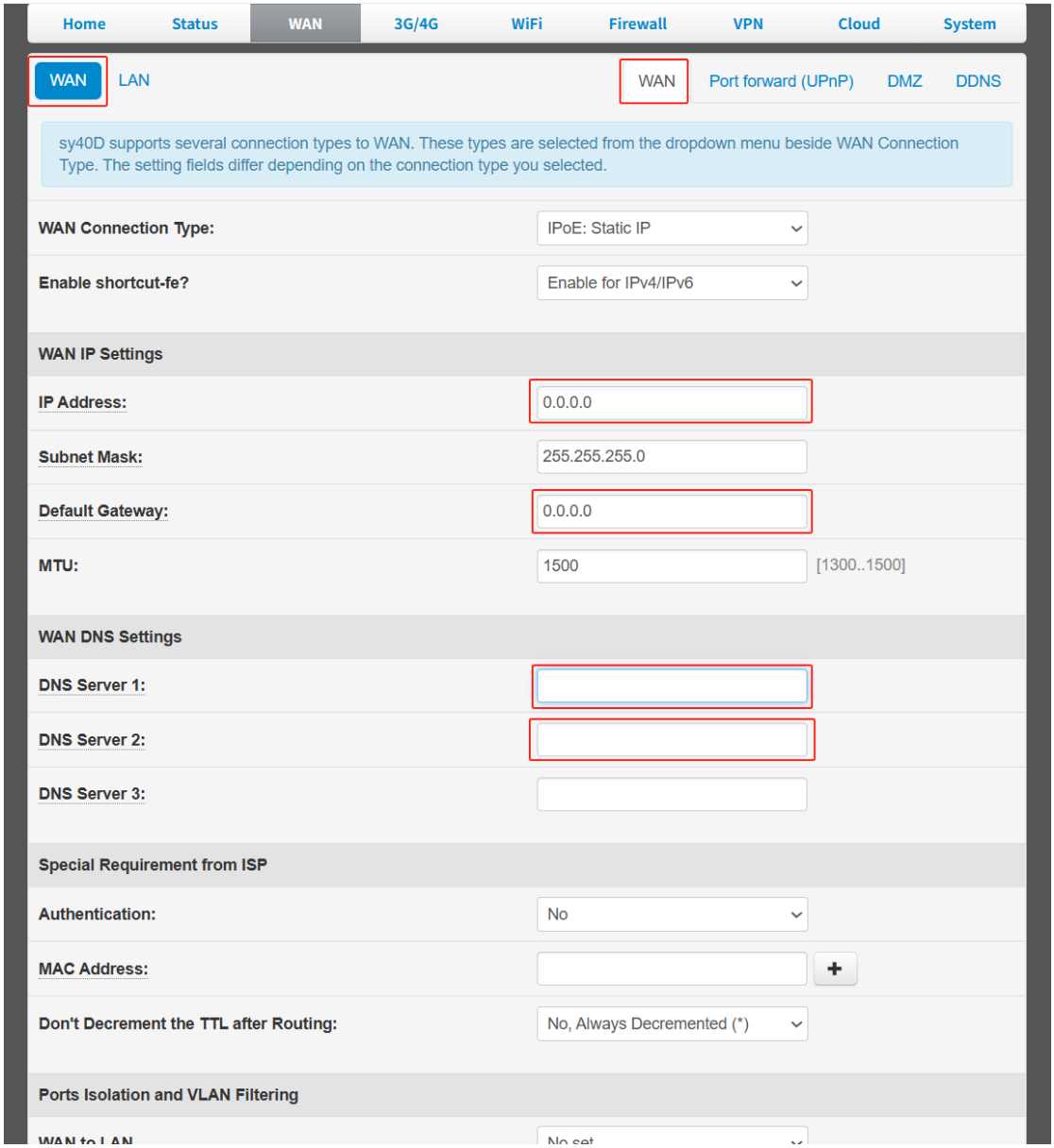
3.1.1 WAN

The SY40 industrial router supports multiple WAN connection types:

A. IPoE: Static IP

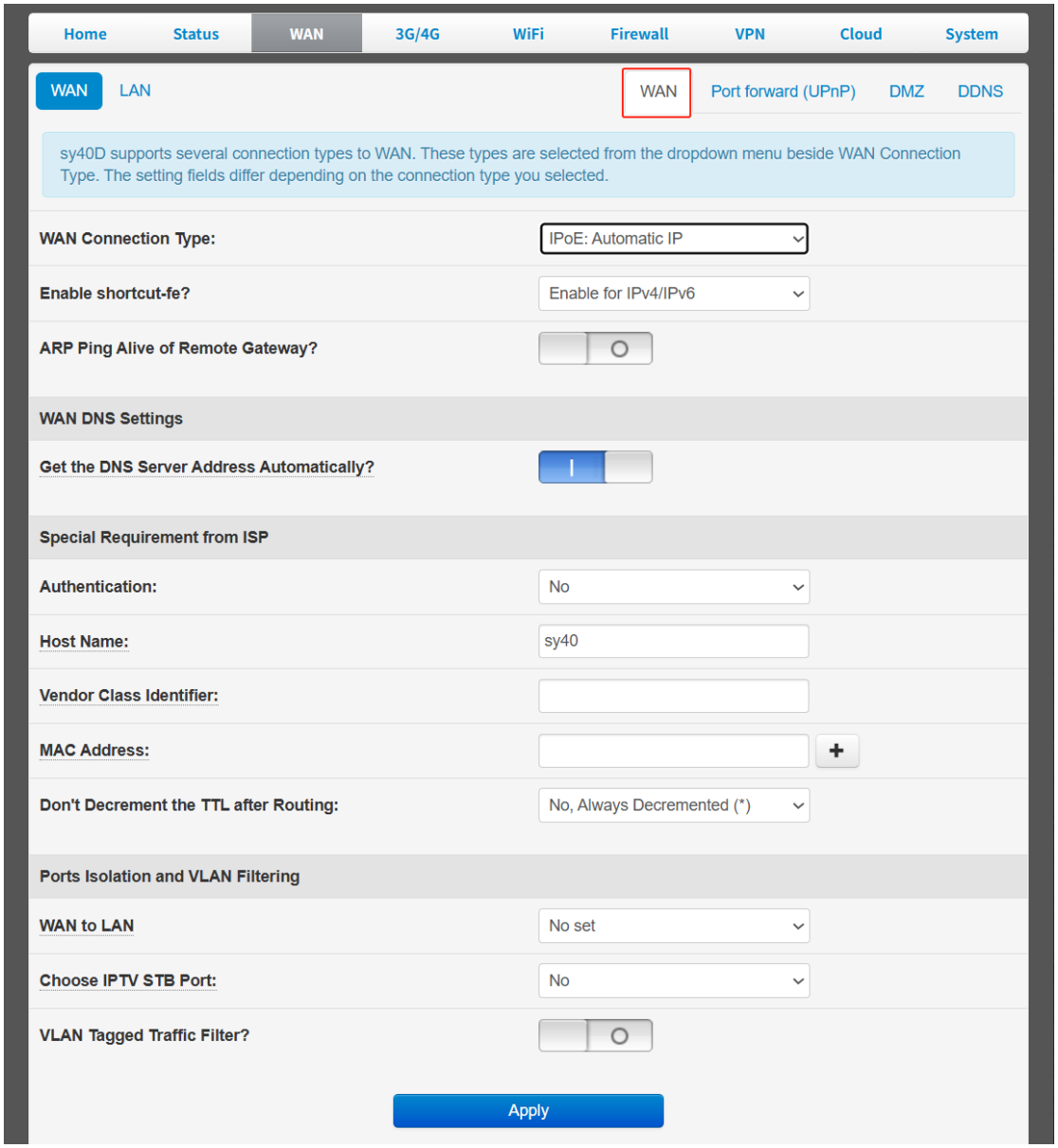
- Configure a fixed IP address manually
- **Critical fields:**
  - **IP Address** (Must match subnet)

- **Subnet Mask** (e.g., 255.255.255.0)
- **Default Gateway** (Verify with your ISP)
- **DNS Service 1 or DNS Service 1 and DNS Service 2**(e.g., 8.8.8.8)



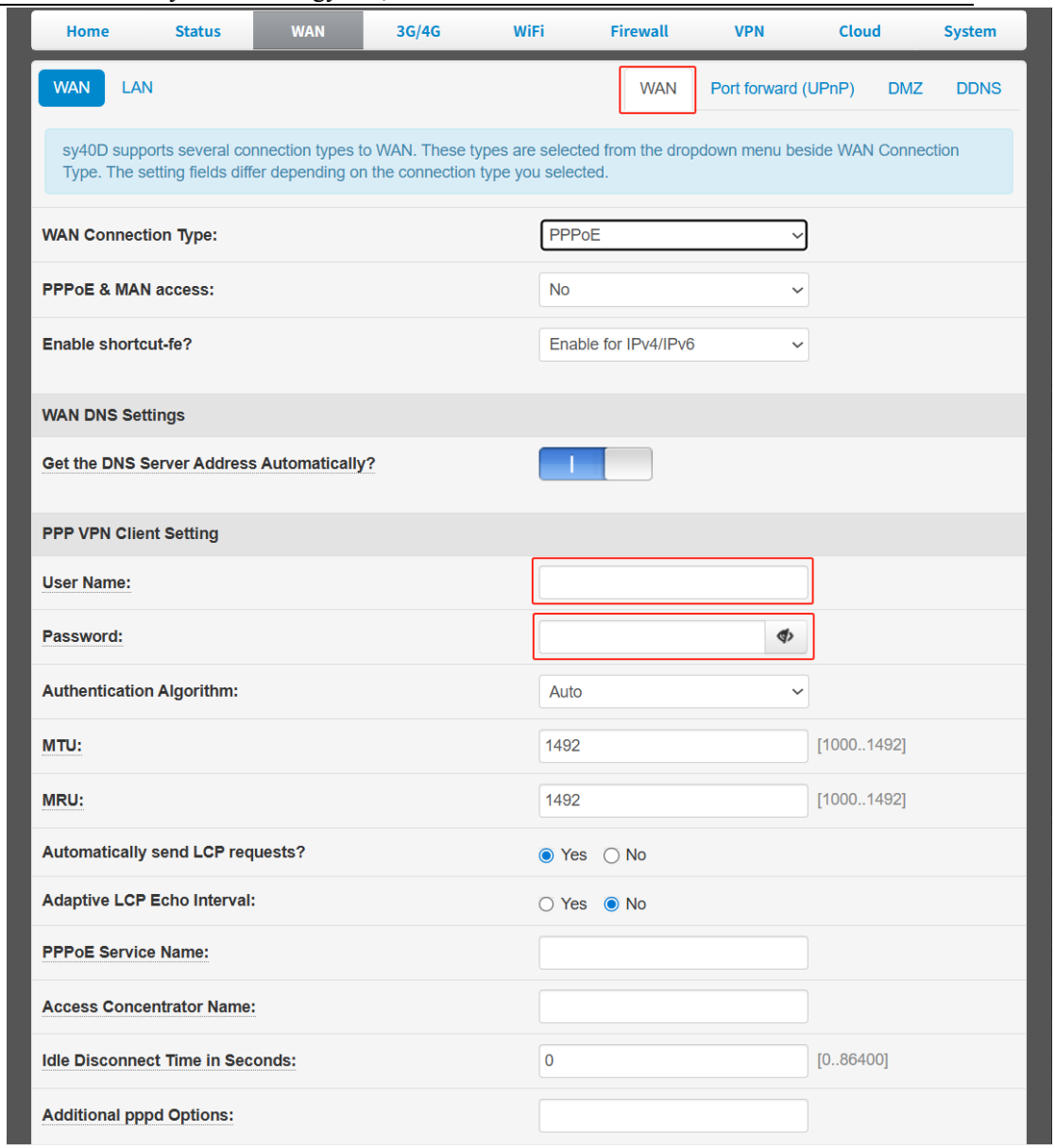
B. IPoE: Automatic IP

• Connect the upstream network device to the **WAN/LAN0 port** via Ethernet.
• The router will **automatically obtain an IP address** (no manual configuration required).



C. PPPoE (Broadband Dial-Up)

Requires **username & password** for authentication.
Note: Credentials are **case-sensitive**—enter them carefully.



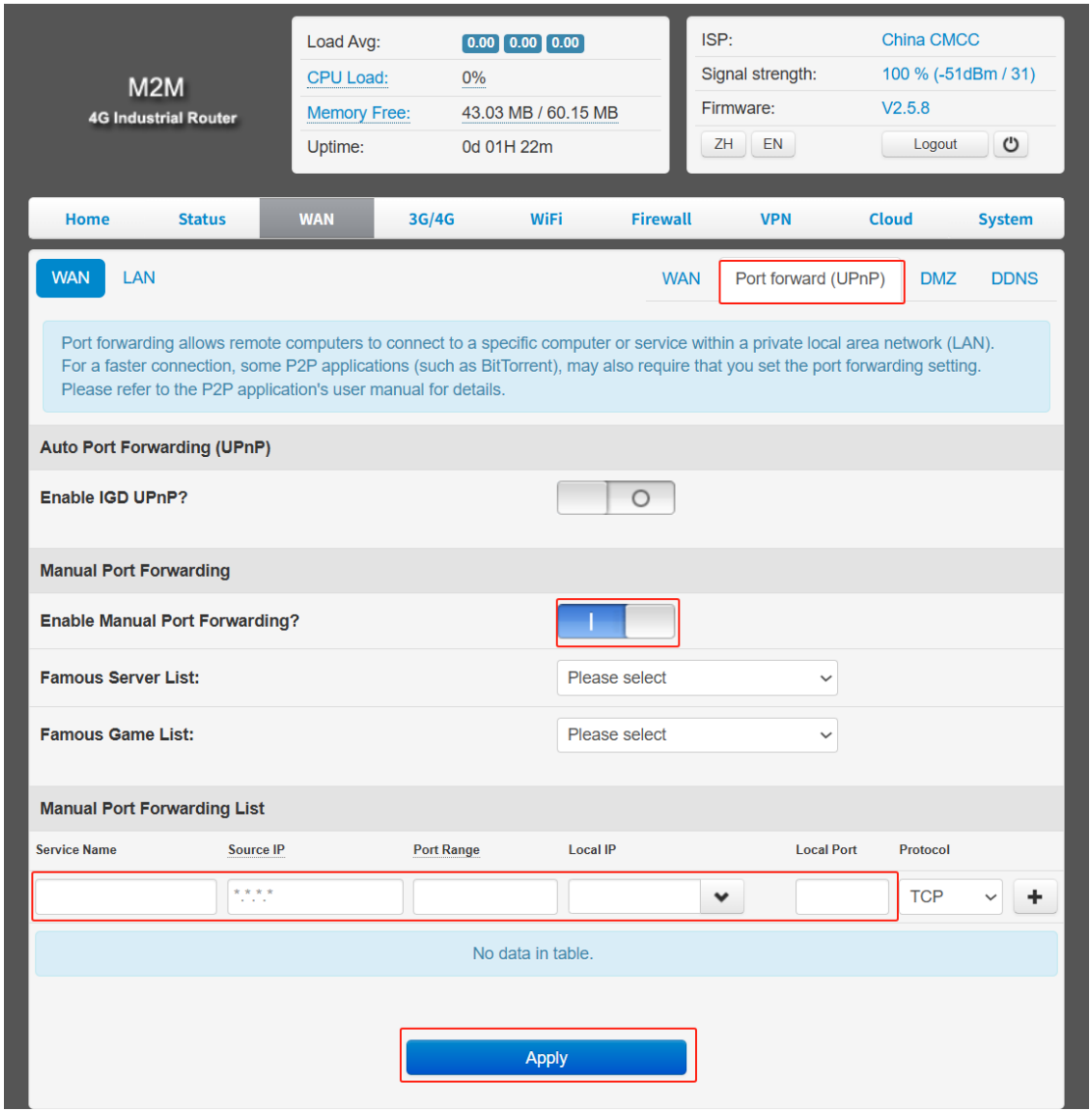
3.1.2 Port Forward(UPnP)

Port forwarding maps internal service ports to the external network, allowing remote access via: Public IP + Port number

Configuration steps:

1. Enable **Manual Port Forwarding.**
2. Fill in the **Manual Port Forwarding List**:
   - Service Name (e.g., "Web Server")
   - Source IP (Optional filtering)
   - Port Range (External ports)
   - Local IP (LAN device IP)
   - Local Port (Internal service port)

3. After modifying settings, click "**Apply**" to save and activate the configuration.



3.13 DMZ

When the router connects to only **one device**, or when you need to expose **a specific device** among multiple connected devices, you can use the **DMZ Host** function instead of port forwarding.

How to Configure

Enter the **target device's IP address** in the **"IP Address of Exposed Station"** field. Click ”**Apply**” to enable DMZ Host.

Effect

All ports on the specified device will be **exposed to the external network.**

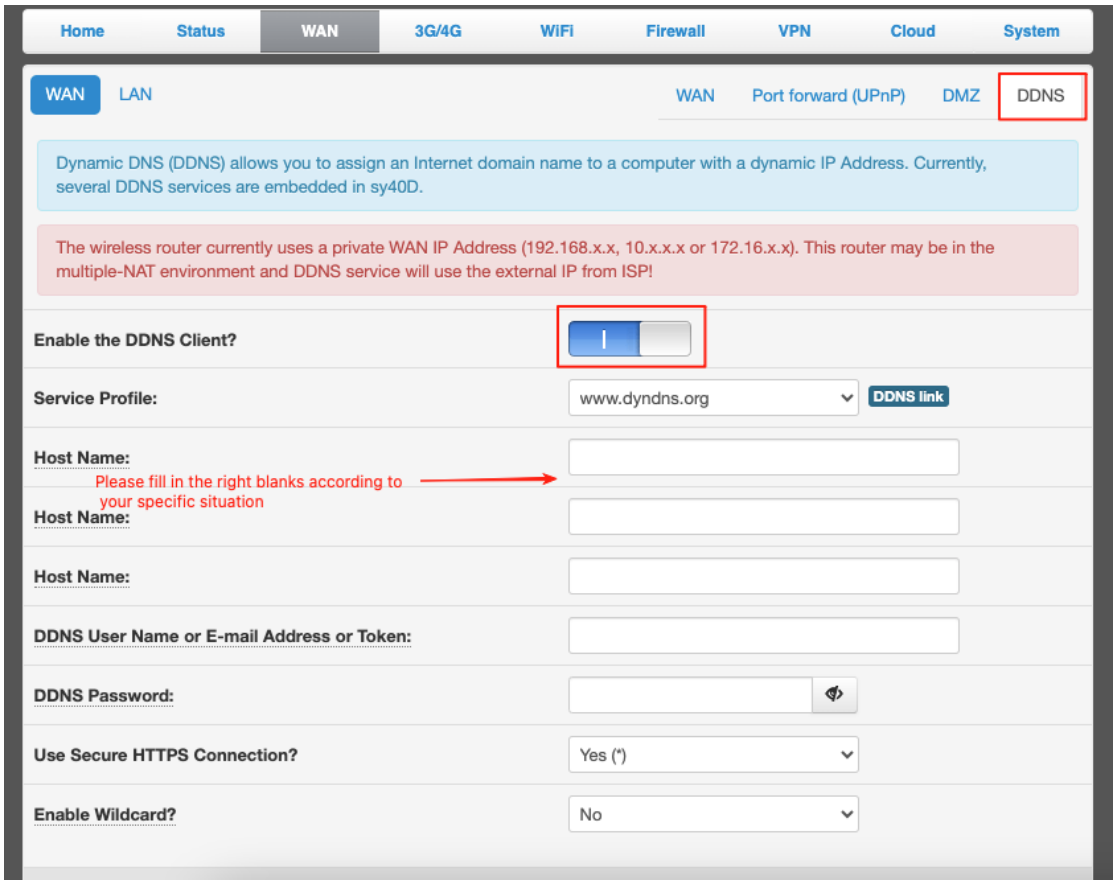
No need for individual port forwarding rules.

3.1.4 DDNS (Dynamic DNS)

DDNS allows accessing the internal network via a domain name, even with a dynamic public IP.

Setup:

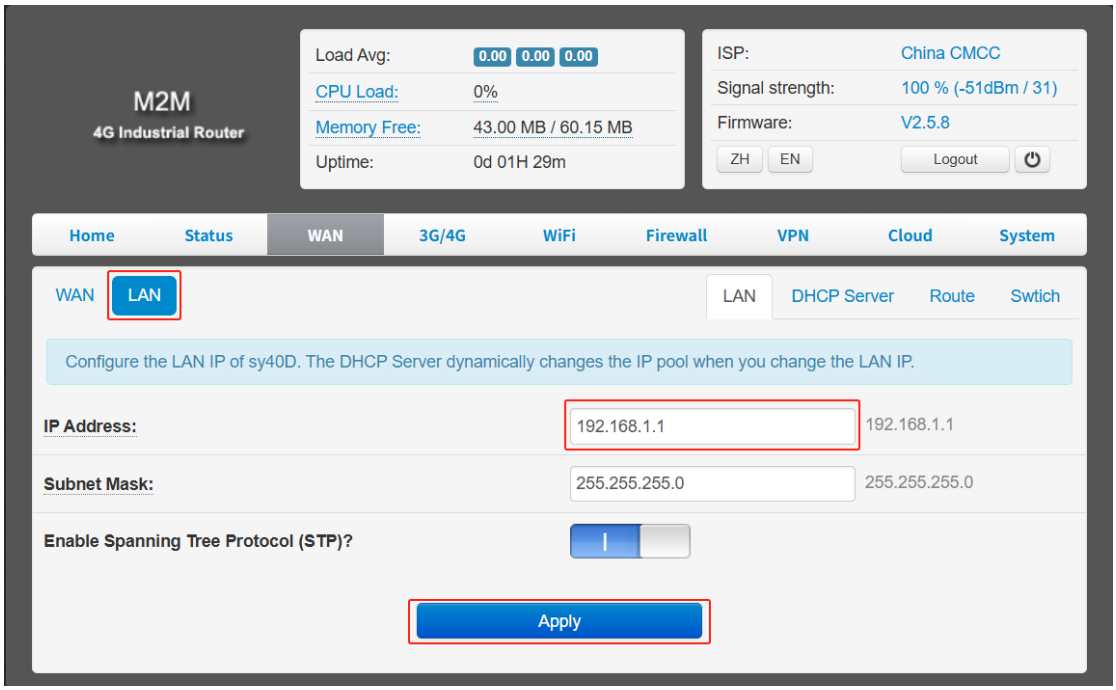
1. Select a **DDNS service provider** when pulling down the **Service Profile menu**(e.g., No-IP, DynDNS).
2. Enter the required account & domain information per your specific situation.



3.2 LAN (Internal Network)

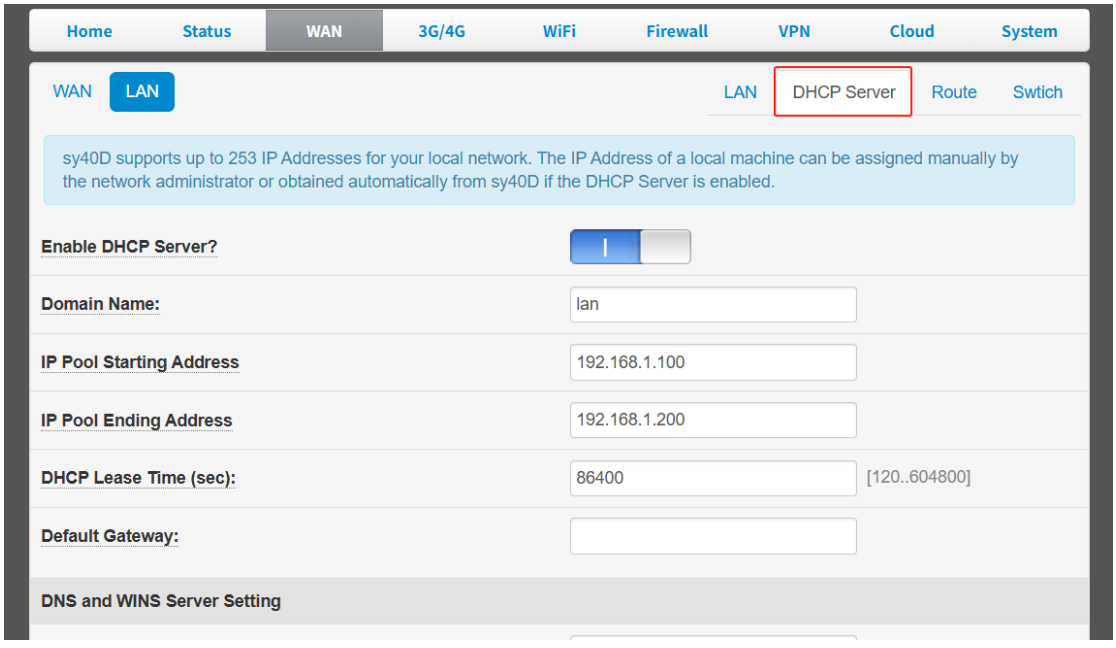
3.2.1 LAN

- You could modify the “**IP Address**” (e.g., 192.168.1.1).
- Note: Changing the gateway IP automatically updates DHCP settings.
- If modification, click "**Apply**" to save and activate the configuration



3.2.2 DHCP Server

- Default: Enabled (automatically assigns IPs to LAN devices).
- If disabled, all devices must use static IPs within the subnet.



4. 3G/4G Cellular Connectivity

3G/4G

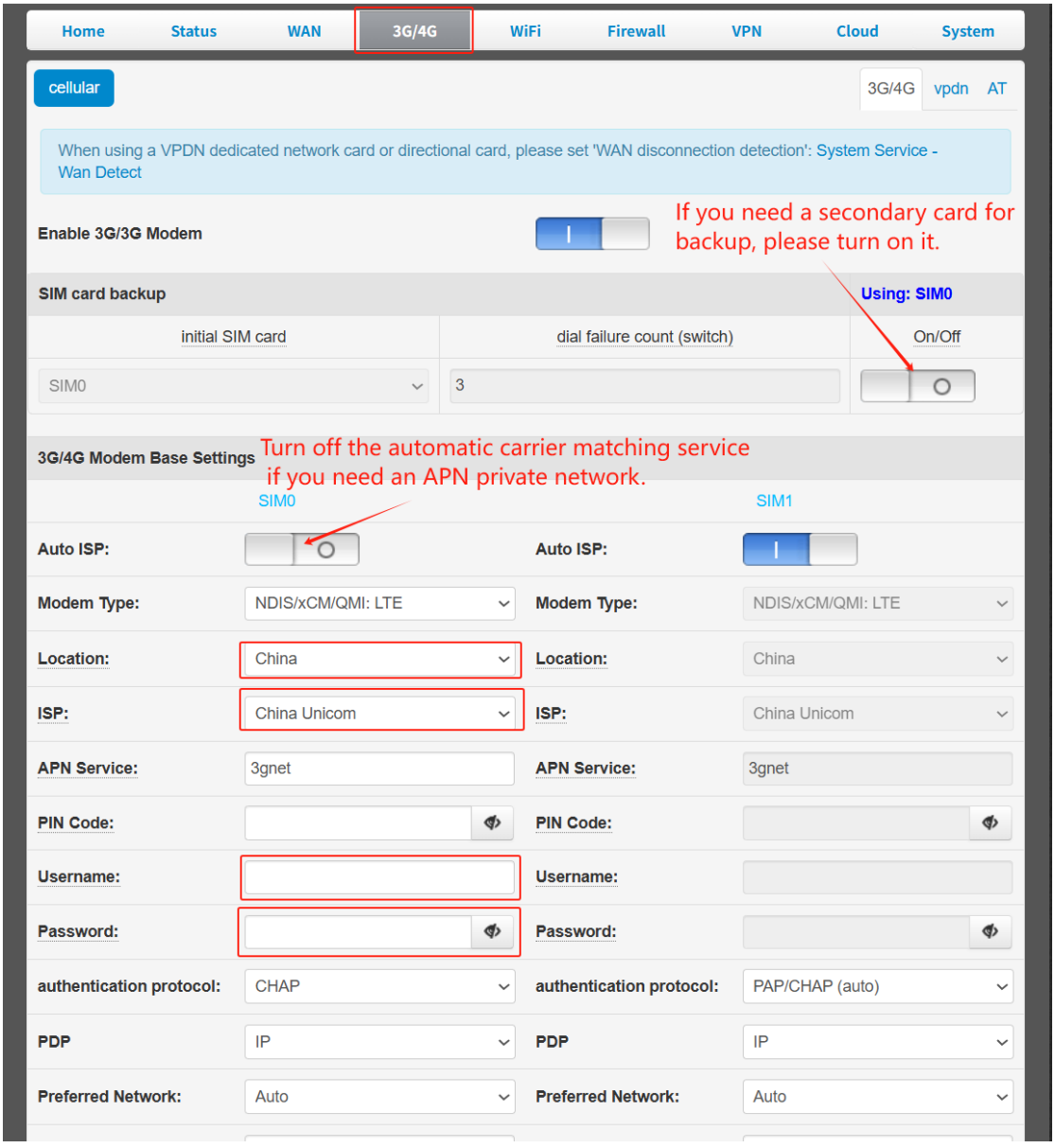
The SY40 industrial router operates in **3G/4G wireless router mode** by default.

- Insert a **3G/4G SIM card**, and the router will automatically detect and connect to the available cellular network.
- Optionally, you can manually select a **specific network operator**.

APN/VPDN Configuration

For specialized SIM cards (e.g., enterprise or VPN-connected cards):
Configure the Access Point Name (APN) to match your carrier's requirements.

For VPDN (Virtual Private Dial-Up Network) cards, enter the designated authentication settings.



5. WiFi

5.1 General

A. Enable/Disable Radio:

Turn the **WIFI radio** ON or OFF.

B. SSID (Network Name)

- Modify the WIFI name if needed
- **Default SSID:** sy40-316E

C. Hide SSID (Stealth Mode)

When enabled:

- The network becomes **invisible** to scans.
- Only **previously connected devices** can auto-join.
- New devices must **manually enter the SSID.**

D. Radio Channel

- **13 selectable channels** (2.4GHz band).
- **Default:** Auto-selection (recommended).
- **Advanced:** Manually lock a channel

E. Authentication Method

Supported **encryption methods:**

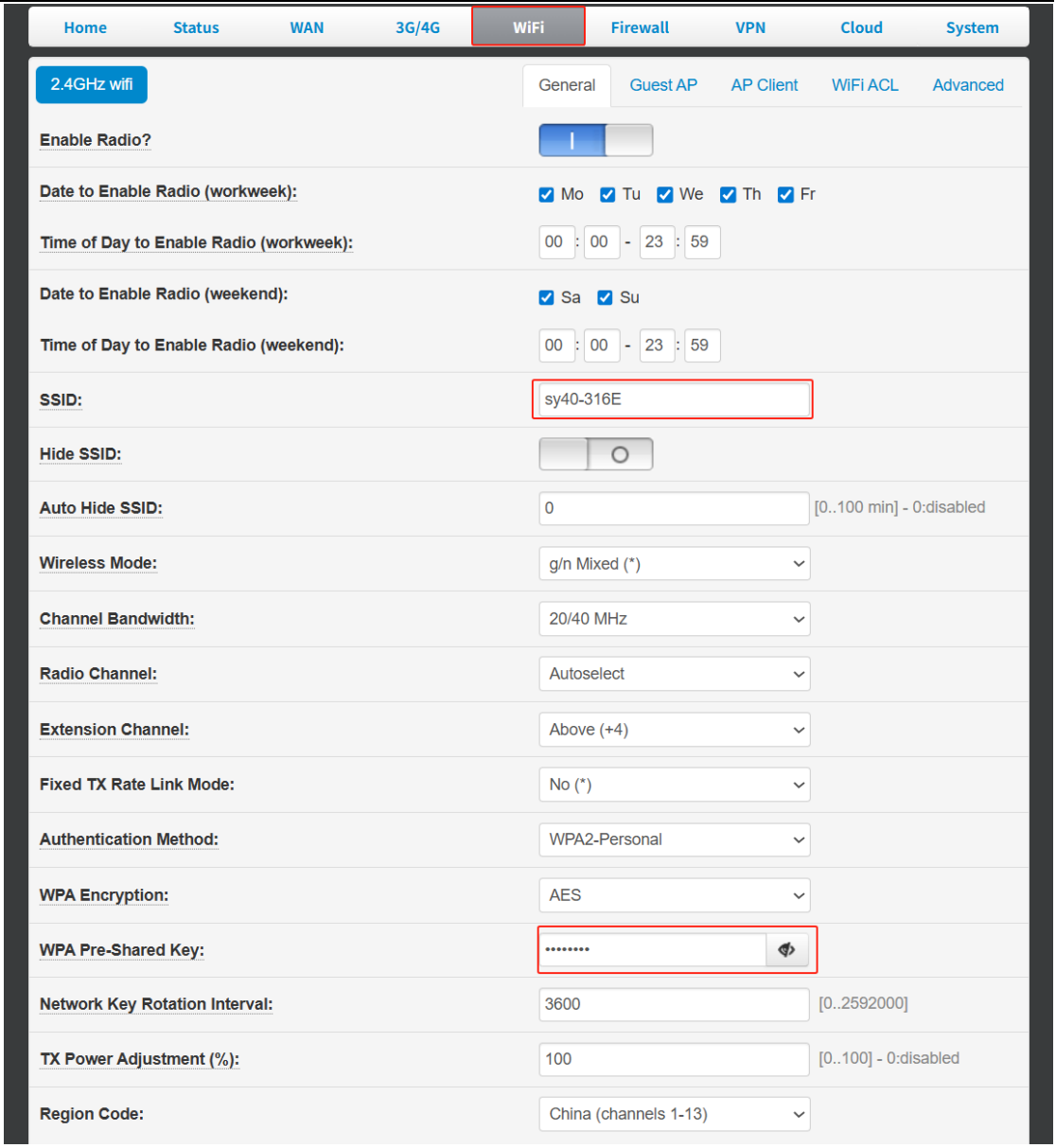
- **WPA2-Personal**(Recommended for industrial use)
- **Open System** (No encryption – high risk!)

F. WPA Pre-shared Key (WIFI Password)

- Set a **strong passphrase**
- **Default:** 12345678

G. Apply Changes

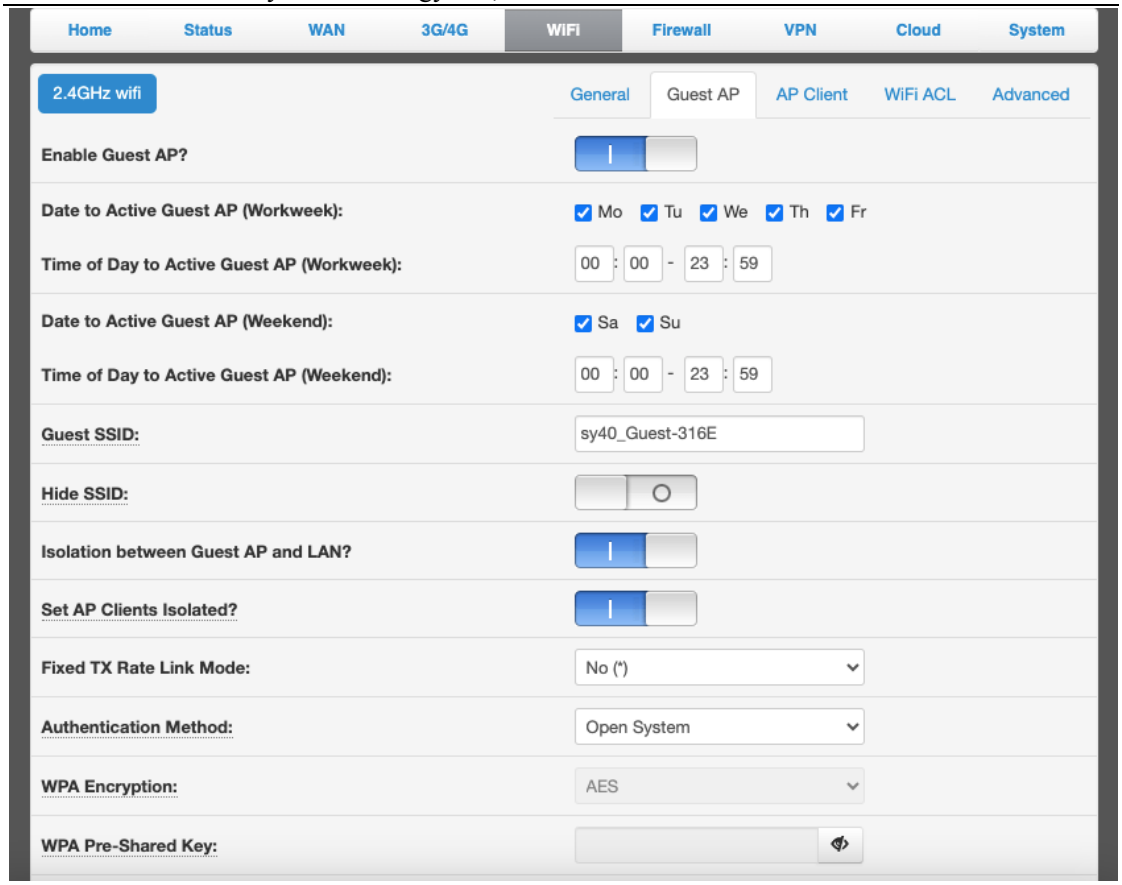
After modifying settings, click "**Apply**" to save and activate the configuration.



5.2 Guest AP

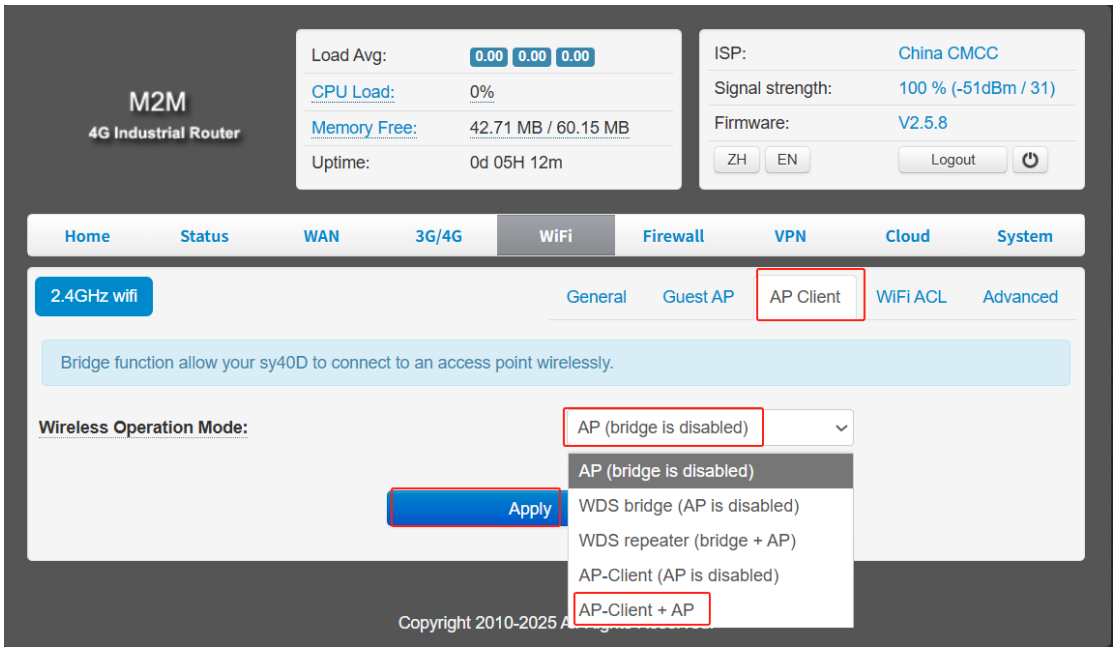
Create isolated WIFI for visitors with separate management

- Configuration follows standard WIFI setup procedure



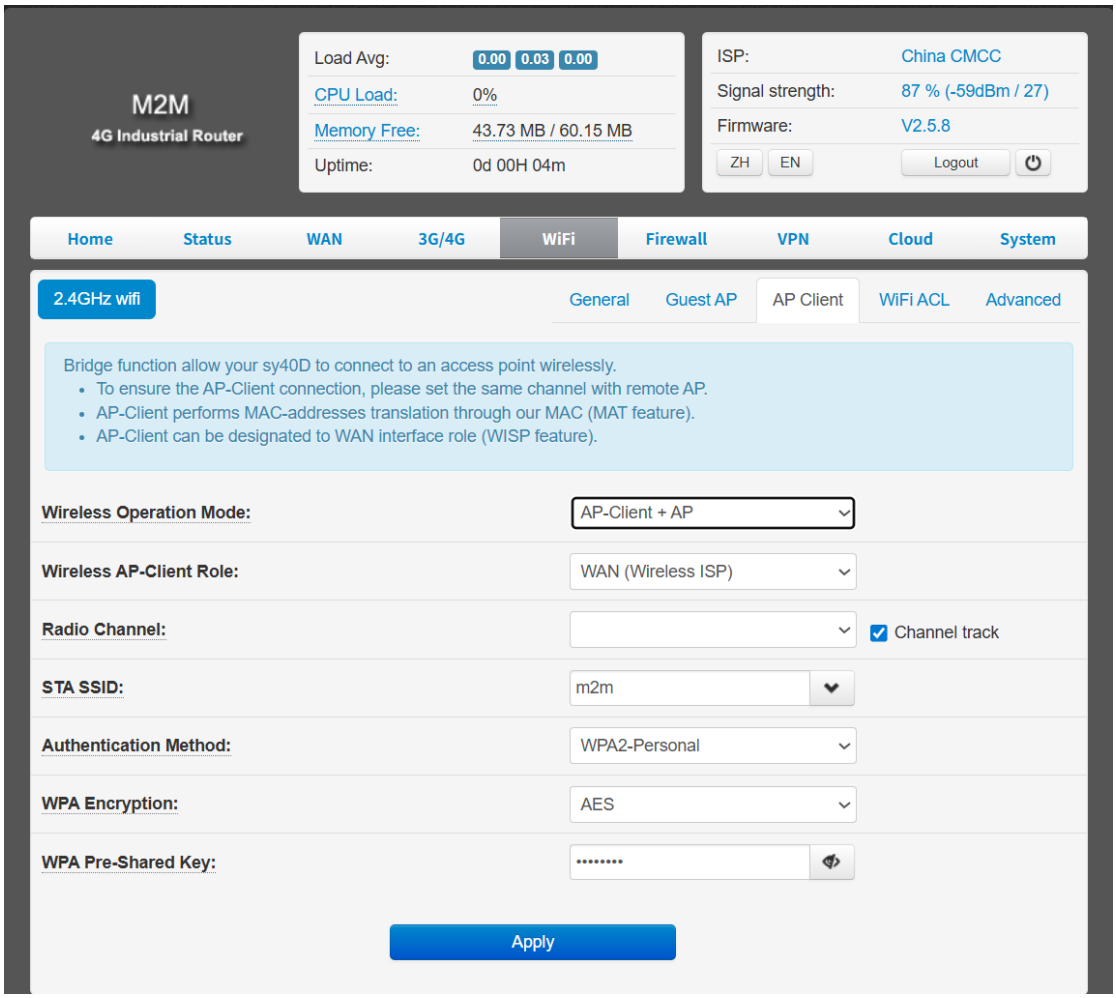
5.3 AP Client

The AP Client feature is disabled by default. When enabled, select AP-Client+AP mode to configure the SY40 as a bridging access point, connecting to an upstream wireless router. Click "**Apply**" to save and activate the configuration.

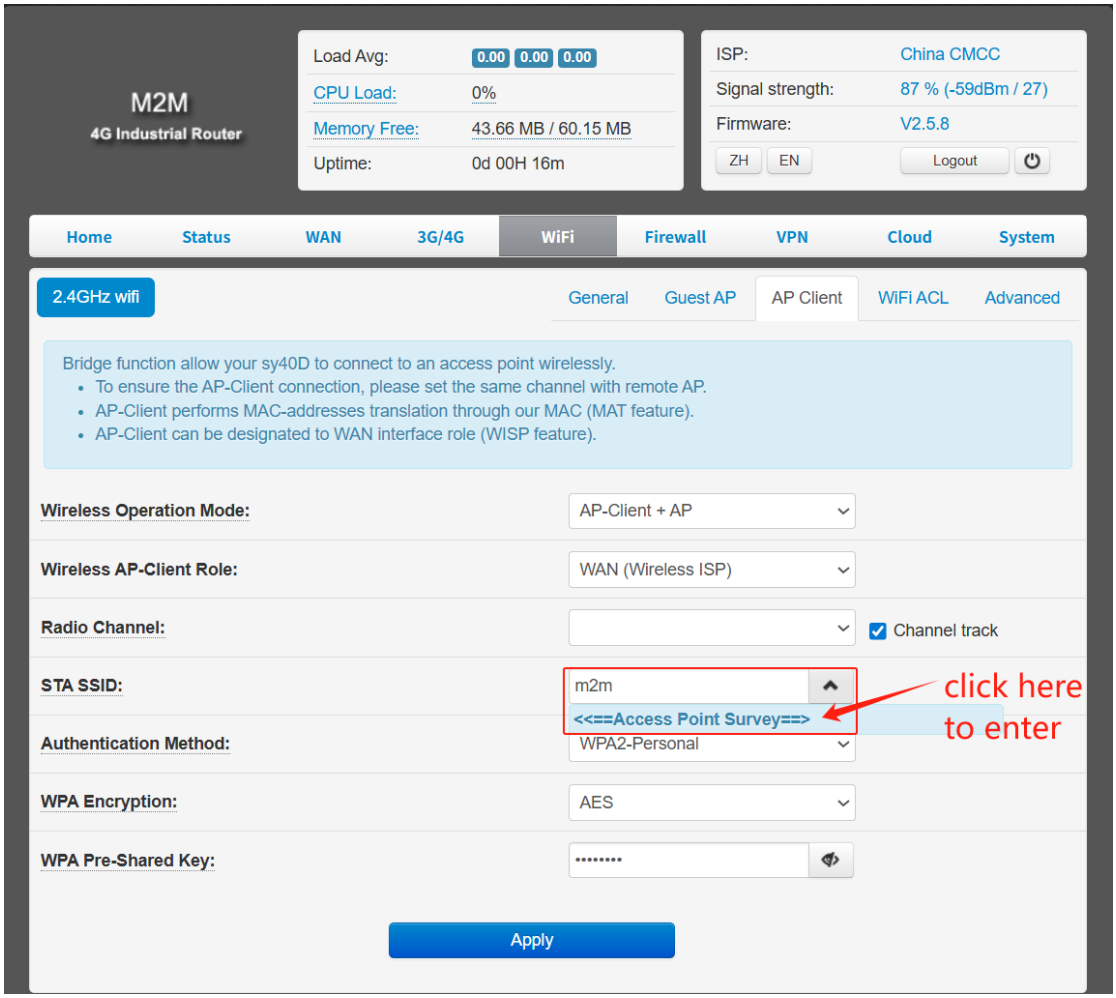


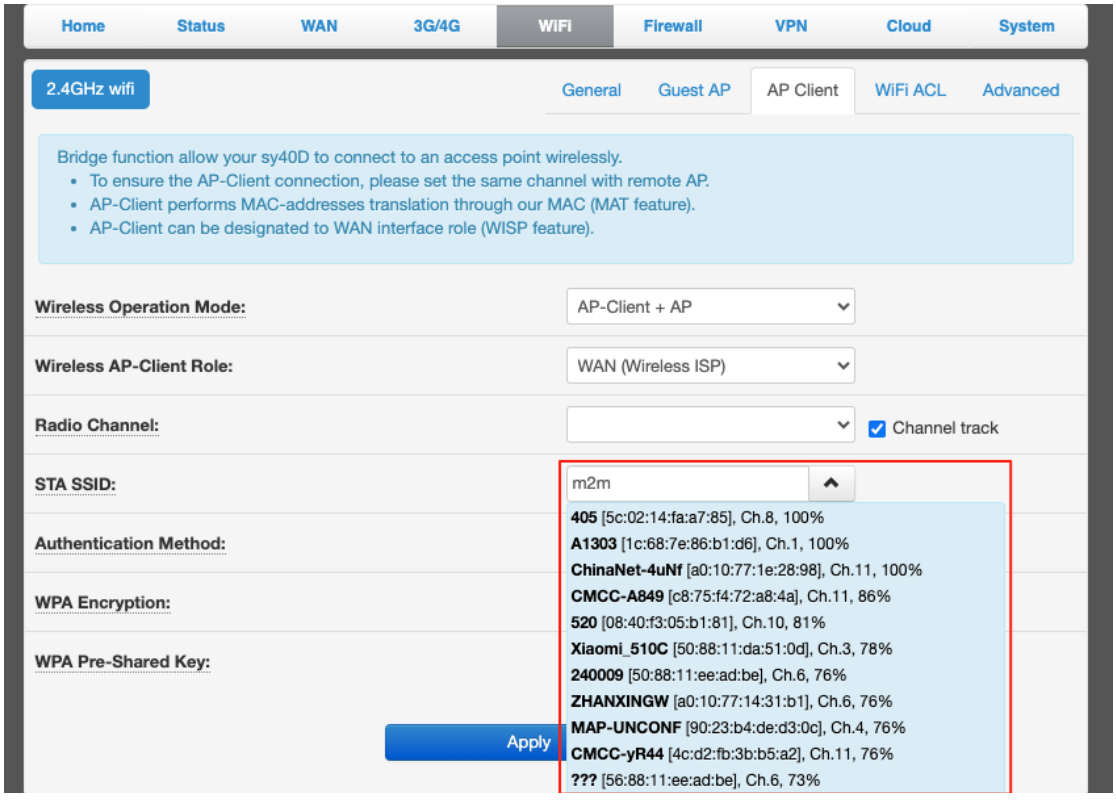
Configuration Steps:

1. Connect via LAN port → **Wireless Operation Mode**→ Select "**AP-Client+AP**" mode

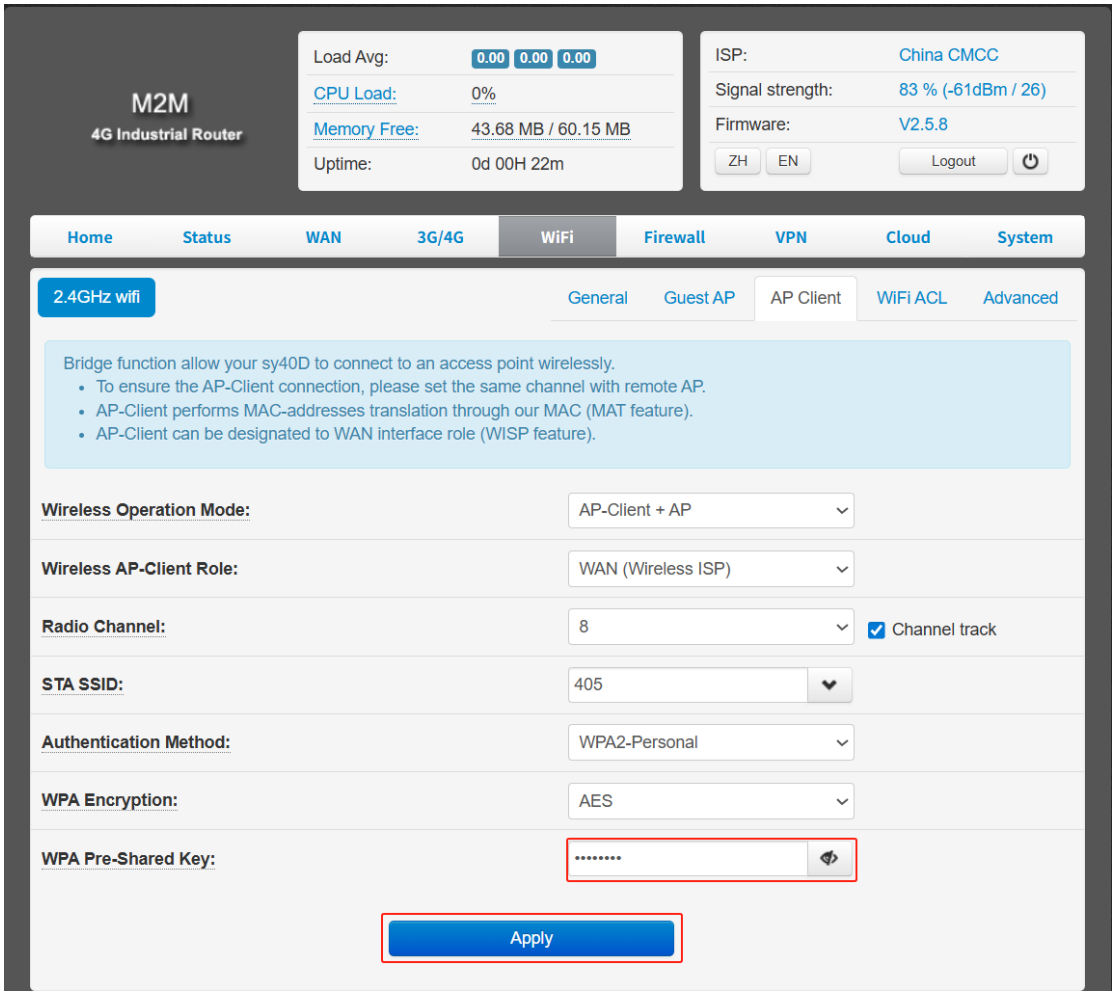


2. Keep "**Wireless AP-Client role**" and "**Radio Channel**" as the default setting
3. Scan and select target AP's SSID from pulling down "**STA SSID**"


M2M
4G Industrial Router
Load Avg: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.66 MB / 60.15 MB
Uptime: 0d 00H 16m
ISP: China CMCC
Signal strength: 87 % (-59dBm / 27)
Firmware: V2.5.8
ZH EN
Logout
Home Status WAN 3G/4G WiFi Firewall VPN Cloud System
2.4GHz wifi
General Guest AP AP Client WiFi ACL Advanced
Bridge function allow your sy40D to connect to an access point wirelessly.
To ensure the AP-Client connection, please set the same channel with remote AP.
AP-Client performs MAC-addresses translation through our MAC (MAT feature).
AP-Client can be designated to WAN interface role (WISP feature).
Wireless Operation Mode: AP-Client + AP
Wireless AP-Client Role: WAN (Wireless ISP)
Radio Channel:
Channel track
STA SSID: m2m
<<==Access Point Survey==>
click here to enter
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA Pre-Shared Key:
Apply


Home Status WAN 3G/4G WiFi Firewall VPN Cloud System
2.4GHz wifi
General Guest AP AP Client WiFi ACL Advanced
Bridge function allow your sy40D to connect to an access point wirelessly.
To ensure the AP-Client connection, please set the same channel with remote AP.
AP-Client performs MAC-addresses translation through our MAC (MAT feature).
AP-Client can be designated to WAN interface role (WISP feature).
Wireless Operation Mode: AP-Client + AP
Wireless AP-Client Role: WAN (Wireless ISP)
Radio Channel:
Channel track
STA SSID: m2m
405 [5c:02:14:fa:a7:85], Ch.8, 100%
A1303 [1c:68:7e:86:b1:d6], Ch.1, 100%
ChinaNet-4uNf [a0:10:77:1e:28:98], Ch.11, 100%
CMCC-A849 [c8:75:f4:72:a8:4a], Ch.11, 86%
520 [08:40:f3:05:b1:81], Ch.10, 81%
Xiaomi_510C [50:88:11:da:51:0d], Ch.3, 78%
240009 [50:88:11:ee:ad:be], Ch.6, 76%
ZHANXINGW [a0:10:77:14:31:b1], Ch.6, 76%
MAP-UNCONF [90:23:b4:de:d3:0c], Ch.4, 76%
CMCC-yR44 [4c:d2:fb:3b:b5:a2], Ch.11, 76%
??? [56:88:11:ee:ad:be], Ch.6, 73%
Authentication Method:
WPA Encryption:
WPA Pre-Shared Key:
Apply

4. Enter **“WPA Pre-Shared Key”** to complete bridging



5.4 WiFi ACL

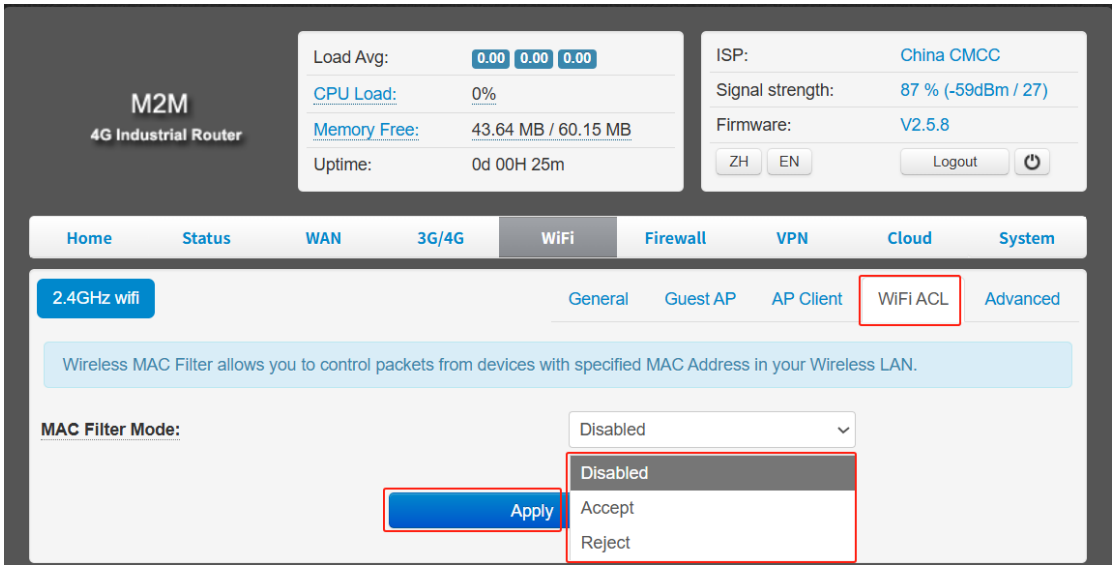
The **MAC Filter Mode** feature allows network access management through two modes: **Accept** and **Reject**(disabled by default).

A. Accept(Whitelist)

Only devices with **pre-authorized MAC addresses** can connect to the network.

B. Reject(Blacklist)

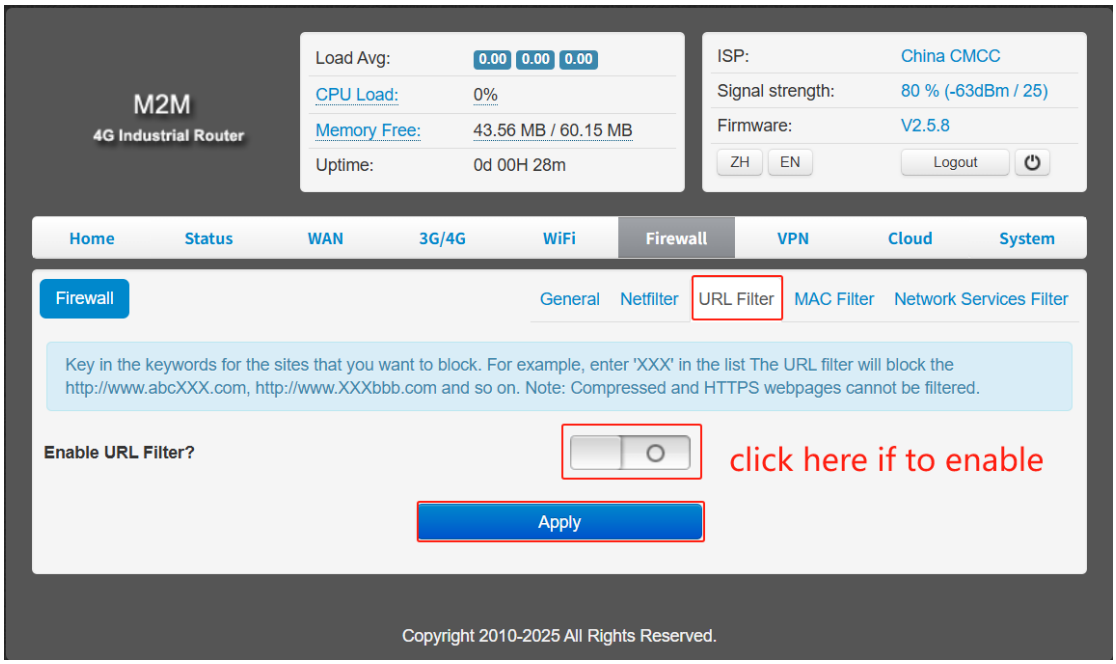
Blocks specified MAC addresses while permitting all others.

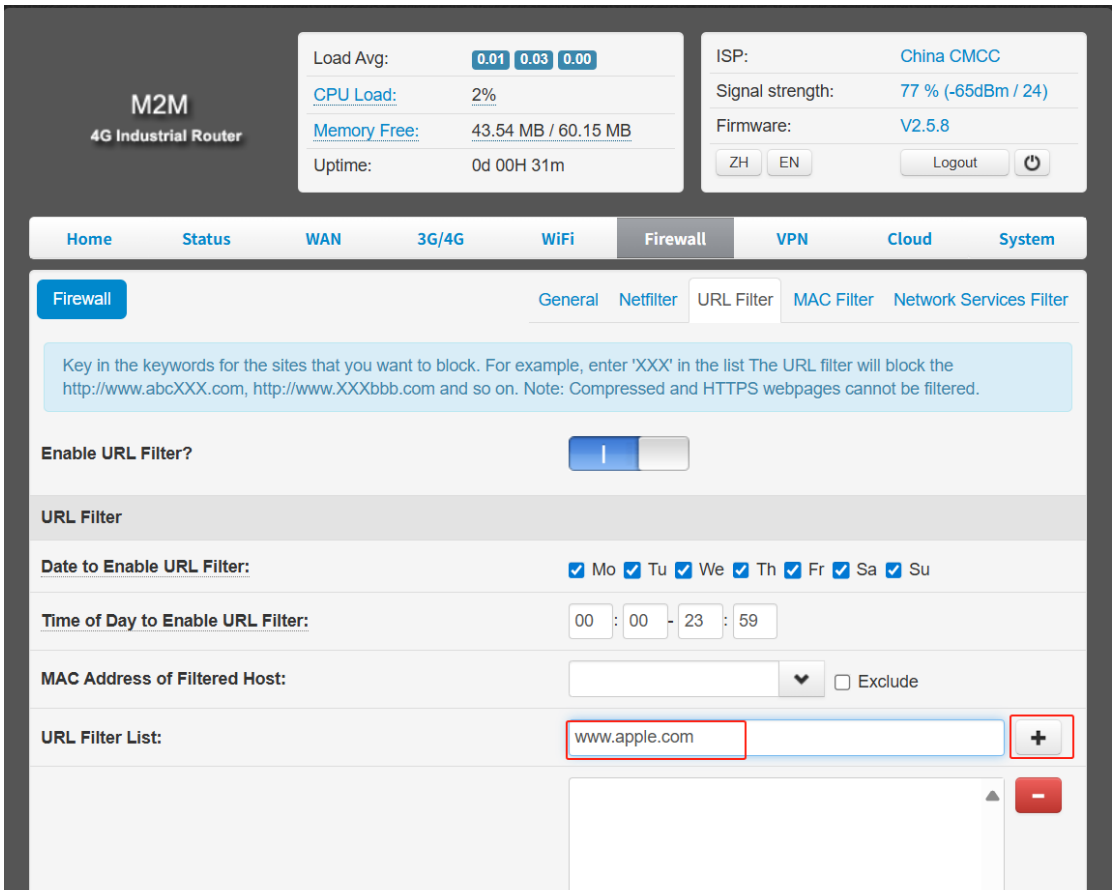


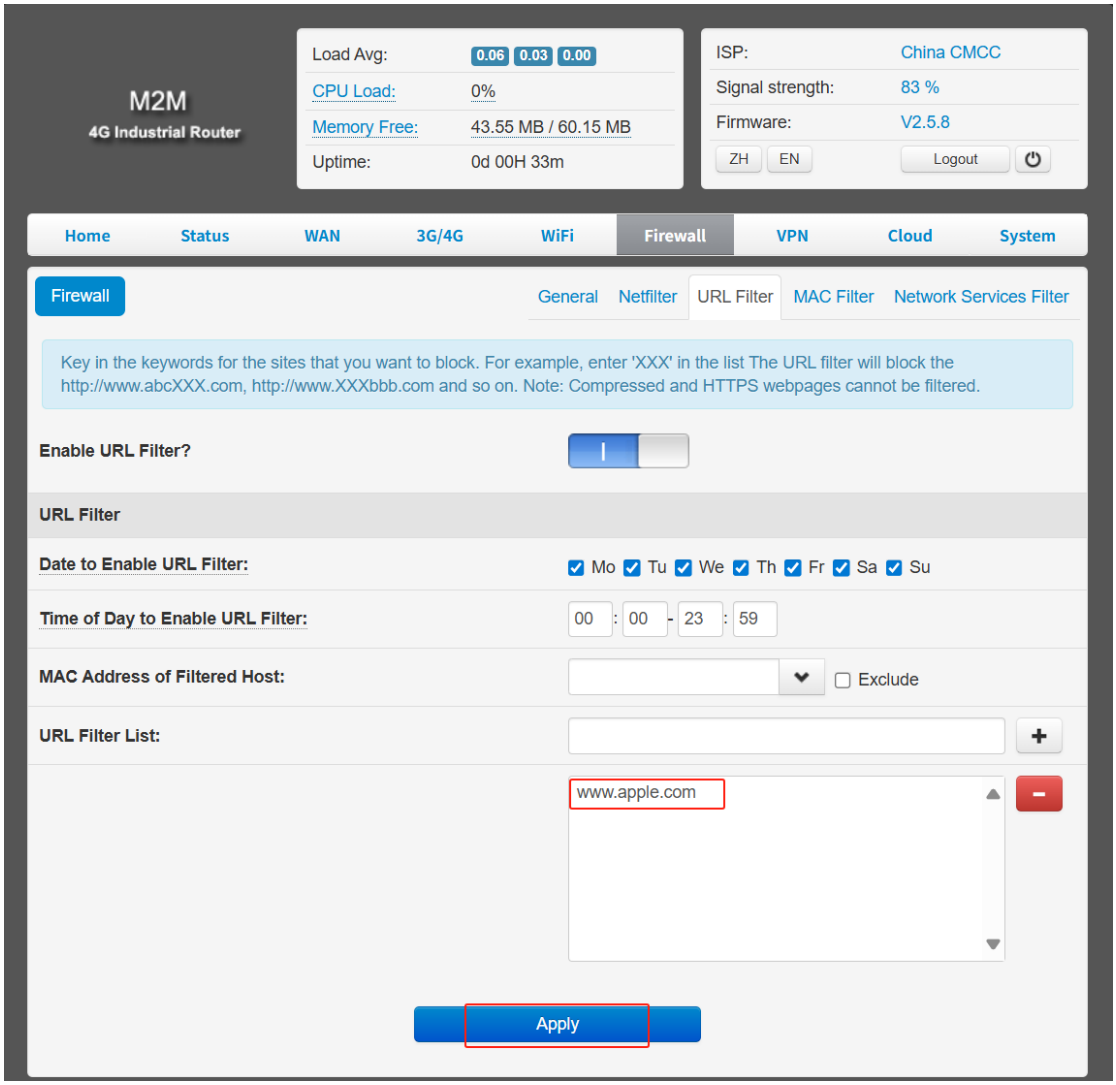
6. Firewall

6.1 URL Filter

When enabled, it features blocks access to websites listed in the "**URL filter List**" (e.g., www.apple.com), while allowing exceptions for specified host addresses.




M2M
4G Industrial Router
Load Avg: 0.01 0.03 0.00
CPU Load: 2%
Memory Free: 43.54 MB / 60.15 MB
Uptime: 0d 00H 31m
ISP: China CMCC
Signal strength: 77 % (-65dBm / 24)
Firmware: V2.5.8
ZH EN
Logout
Home Status WAN 3G/4G WiFi Firewall VPN Cloud System
Firewall
General Netfilter URL Filter MAC Filter Network Services Filter
Key in the keywords for the sites that you want to block. For example, enter 'XXX' in the list The URL filter will block the http://www.abcXXX.com, http://www.XXXbbb.com and so on. Note: Compressed and HTTPS webpages cannot be filtered.
Enable URL Filter?
URL Filter
Date to Enable URL Filter: Mo Tu We Th Fr Sa Su
Time of Day to Enable URL Filter: 00 : 00 - 23 : 59
MAC Address of Filtered Host: Exclude
URL Filter List: www.apple.com



6.2 MAC Filter

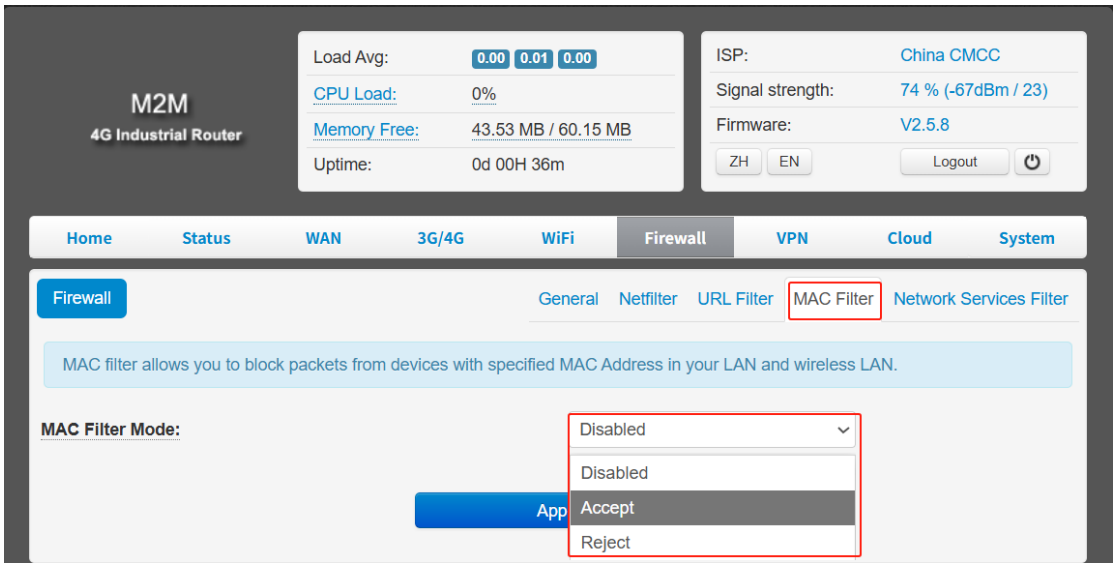
This feature restricts network access based on device MAC addresses, operating in two modes:

1. Accept(Whitelist)

Only devices with pre-registered MAC addresses can connect
Ideal for high-security industrial networks

2. Reject(Blacklist)

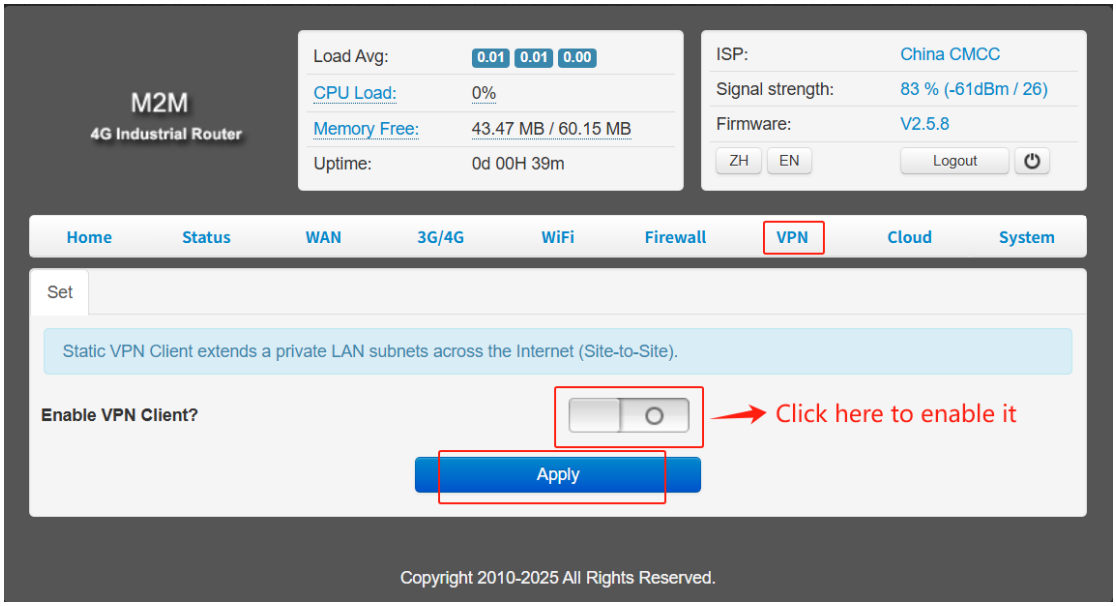
Blocks specific MAC addresses while allowing all others
Useful for banning unauthorized devices



7. VPN

The VPN function supports three protocols: PPTP, L2TP, and Open VPN, operating in both VPN server and VPN client modes.

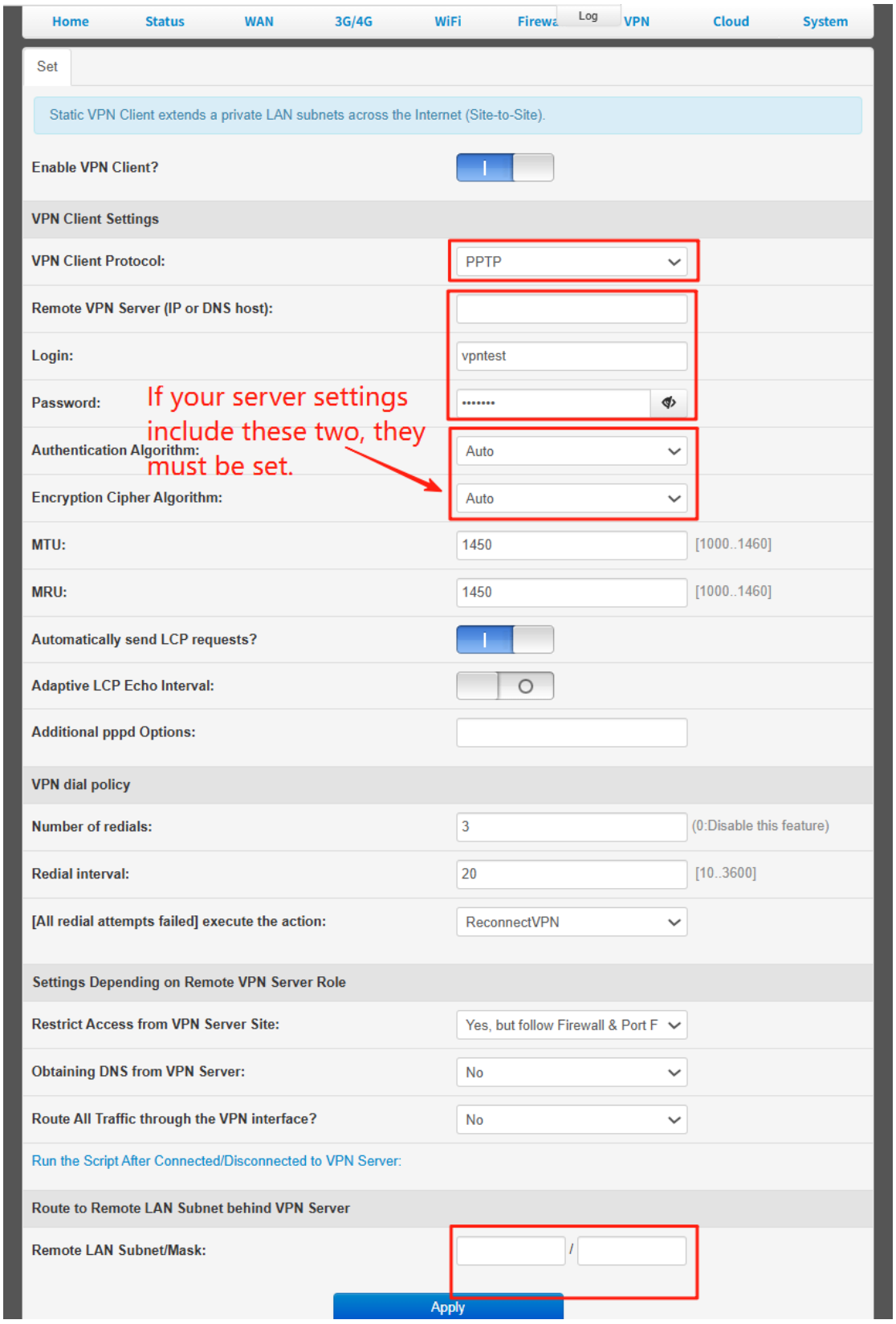
- **Enable VPN Client**
- Click "**Apply**" to save and activate the configuration



7.1 PPTP(Universal VPN Client)

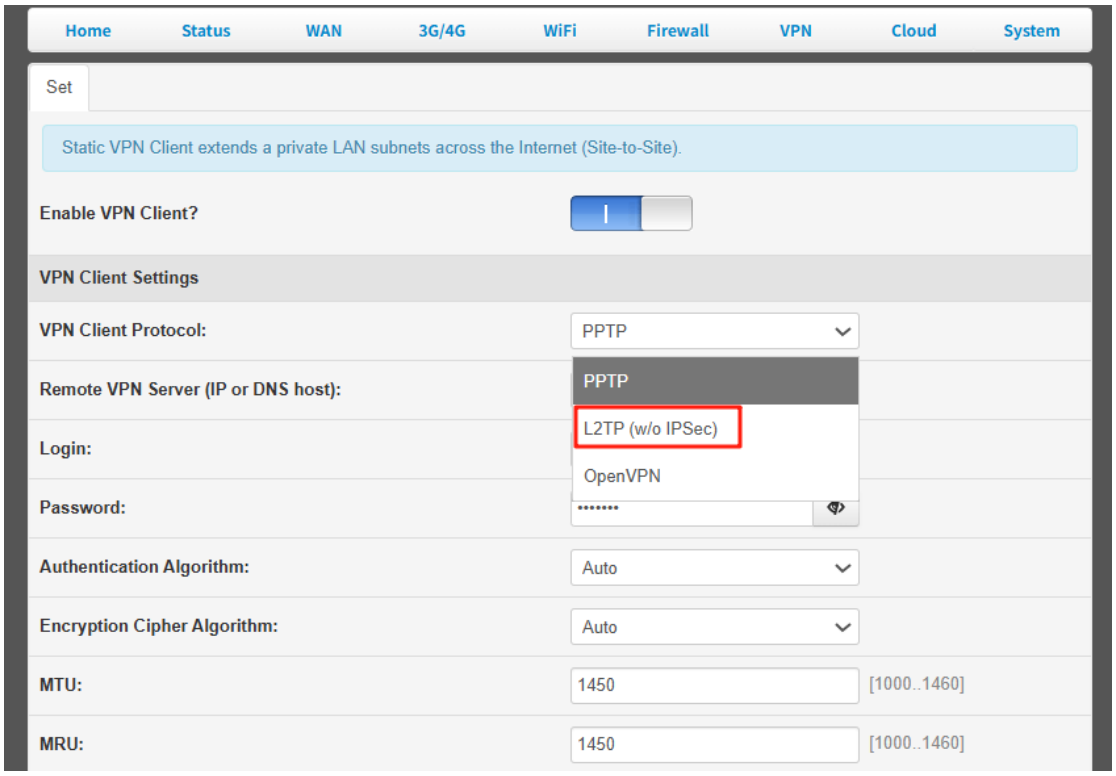
1. Select PPTP as the **"VPN Client Protocol"**.
2. Enter the "**Remote VPN Server(IP or DNS host)**", "**Login(username)**", and "**Password**" in the corresponding fields
3. Choose the appropriate "**Authentication Algorithms**" and "**Encryption Cipher Algorithms**" if your server settings include these two.(Optional)

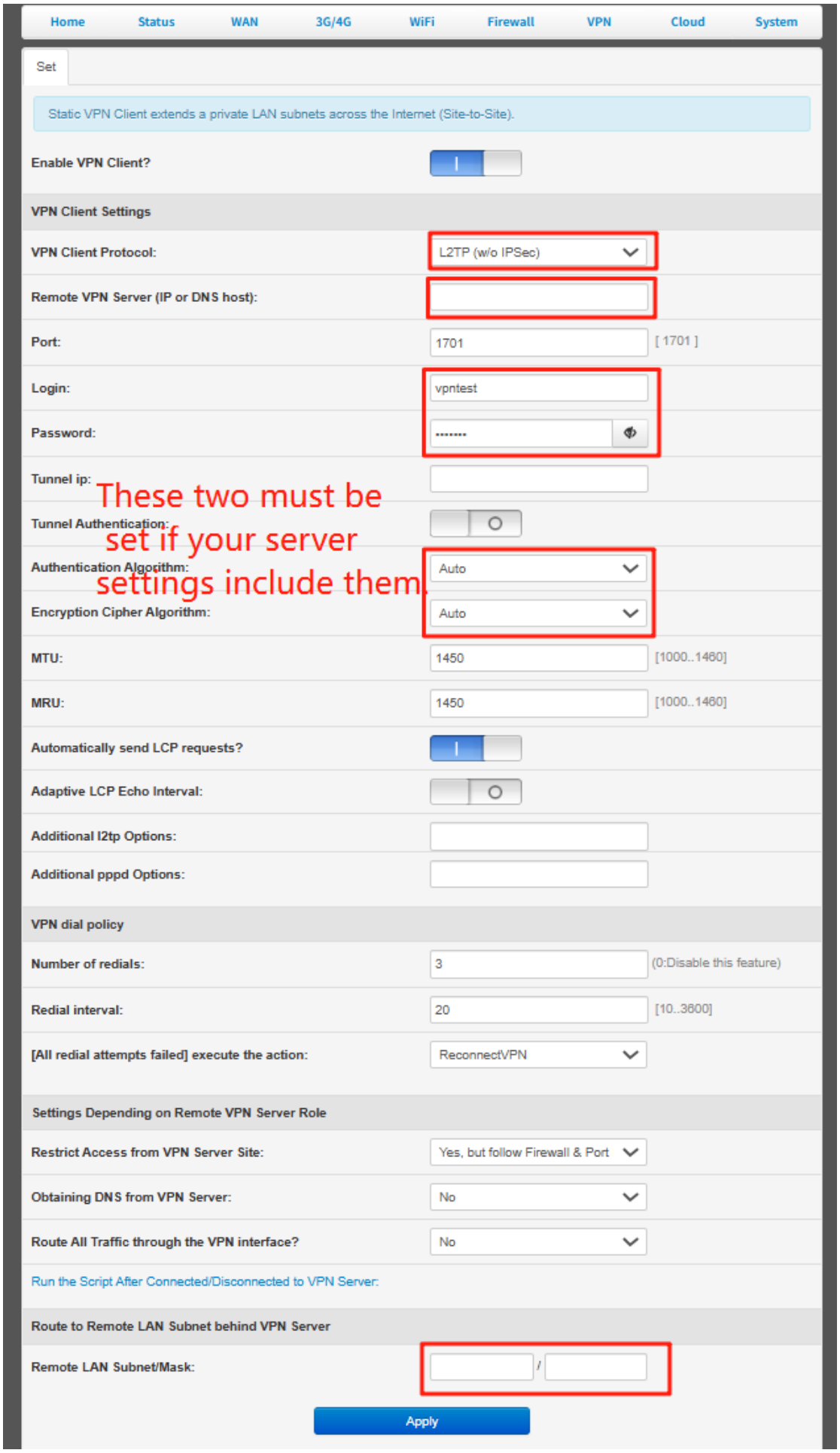
4. Enter "**Remote LAN Subnet/Mask**"



7.2 L2TP

- Select L2TP as the **"VPN Client Protocol"**.
- Refer to the PPTP setup method for configuration procedures.

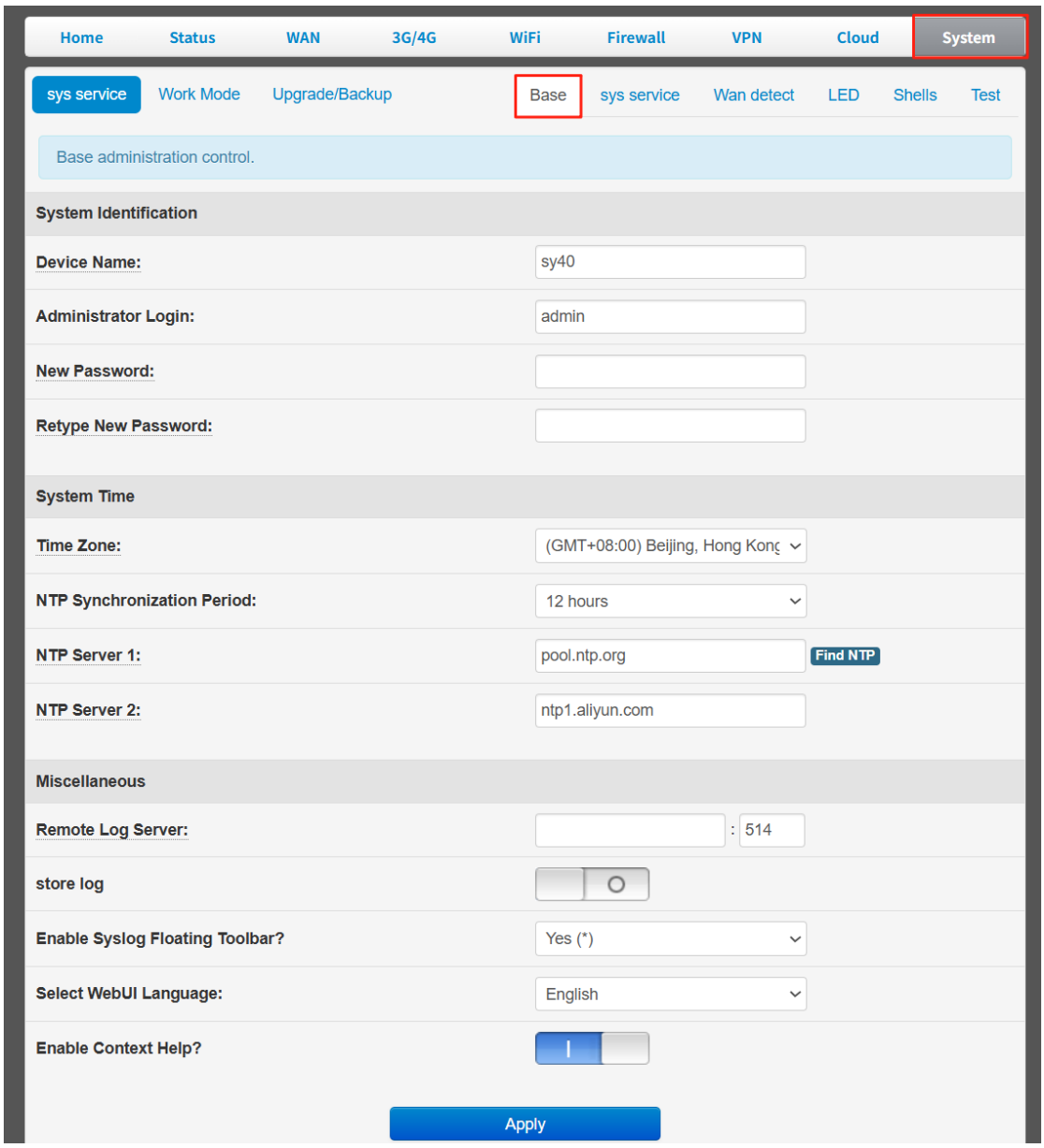



Home
Status
WAN
3G/4G
WiFi
Firewall
VPN
Cloud
System
Set
Static VPN Client extends a private LAN subnets across the Internet (Site-to-Site).
Enable VPN Client?
VPN Client Settings
VPN Client Protocol:
L2TP (w/o IPSec)
Remote VPN Server (IP or DNS host):
Port:
1701
[1701]
Login:
vpntest
Password:
Tunnel ip:
These two must be set if your server settings include them.
Tunnel Authentication:
Authentication Algorithm:
Auto
Encryption Cipher Algorithm:
Auto
MTU:
1450
[1000..1460]
MRU:
1450
[1000..1460]
Automatically send LCP requests?
Adaptive LCP Echo Interval:
Additional l2tp Options:
Additional pppd Options:
VPN dial policy
Number of redials:
3
(0:Disable this feature)
Redial interval:
20
[10..3600]
[All redial attempts failed] execute the action:
ReconnectVPN
Settings Depending on Remote VPN Server Role
Restrict Access from VPN Server Site:
Yes, but follow Firewall & Port
Obtaining DNS from VPN Server:
No
Route All Traffic through the VPN interface?
No
Run the Script After Connected/Disconnected to VPN Server:
Route to Remote LAN Subnet behind VPN Server
Remote LAN Subnet/Mask:
Apply

8. System

8.1.1 Base

Configure the “**Device Name**”, “**Administrator Login**”, and “**Password**” on this page.



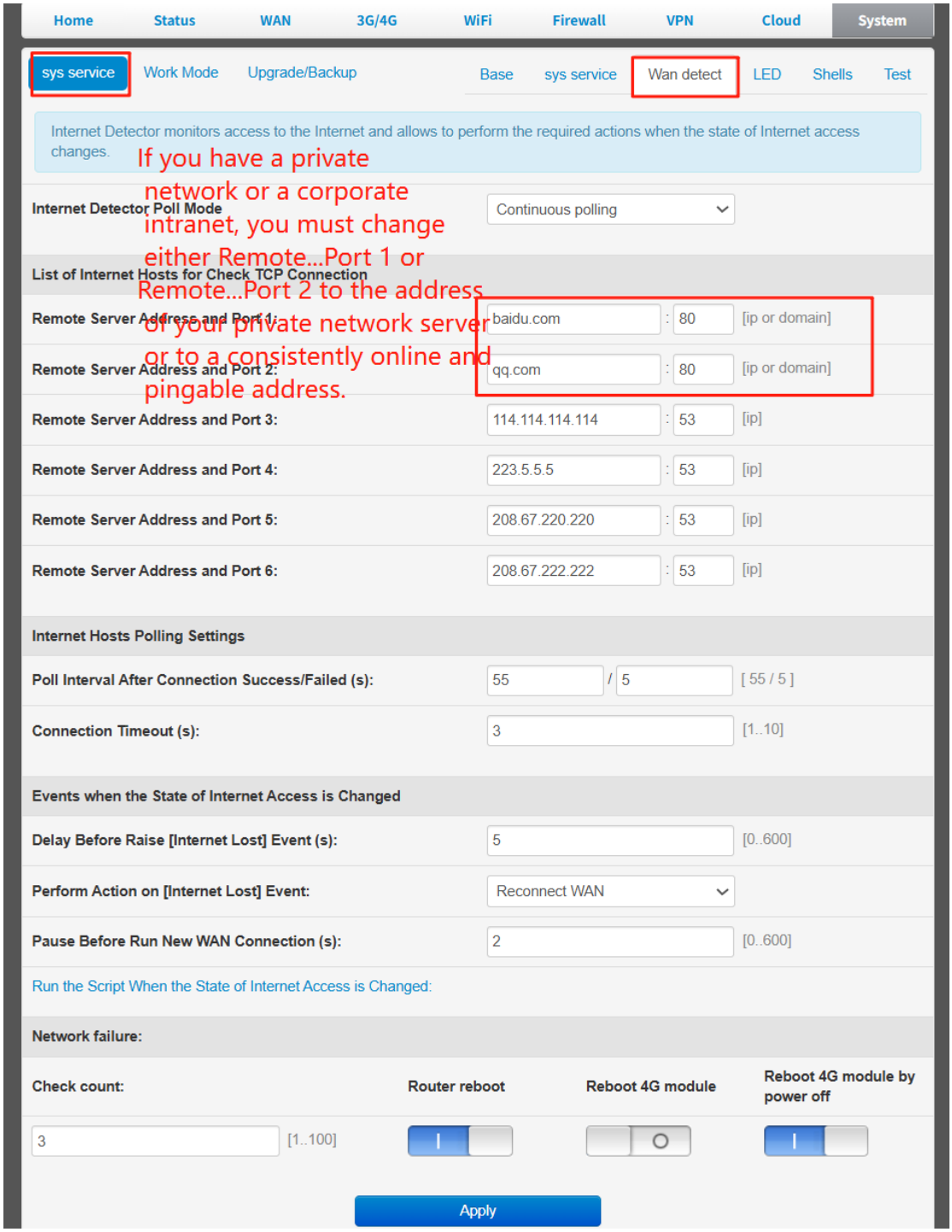
8.1.2 Wan Detect

Functionality:

The system performs connection monitoring by sending ping packets to a specified IP address/domain. Under normal network conditions, ping responses will be received from the target host.

Failure Detection:

- If no response is received after 5 consecutive attempts, the system will determine the connection as dropped
- Automatic reconnection will be initiated



8.2 Upgrade/Backup

8.2.1 Firmware Upgrade

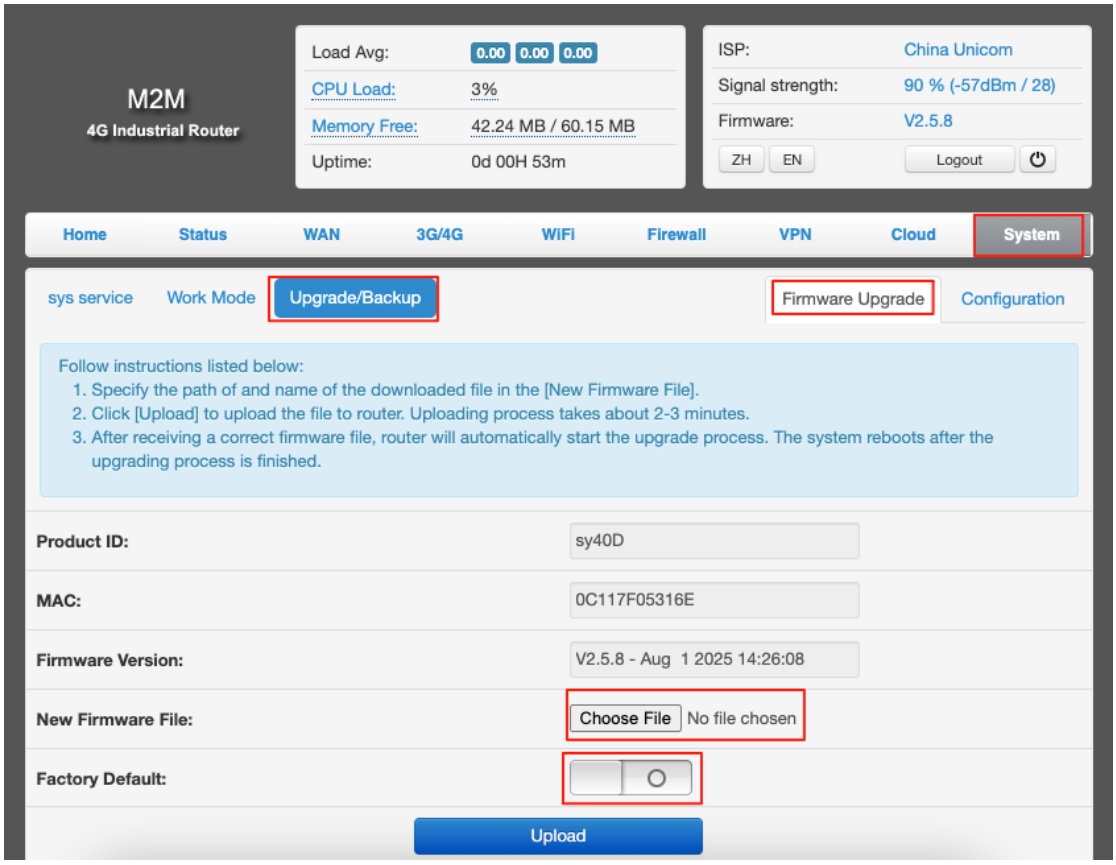
The firmware upgrade feature allows you to load the latest software version to the router for additional functionality and improved stability.

Upgrade Procedure:

1. Save the router upgrade file to your local computer.
2. Click the **<Choose File>** button and select the firmware file.
3. Enable "**Factory Default**"(recommended)
4. Click the **<Upload>** button to start the upgrade.

Important Notes:

- **Do not power off** the router during the upgrade process.
- **A factory reset** is required after the upgrade is complete.



8.2.2 Configuration

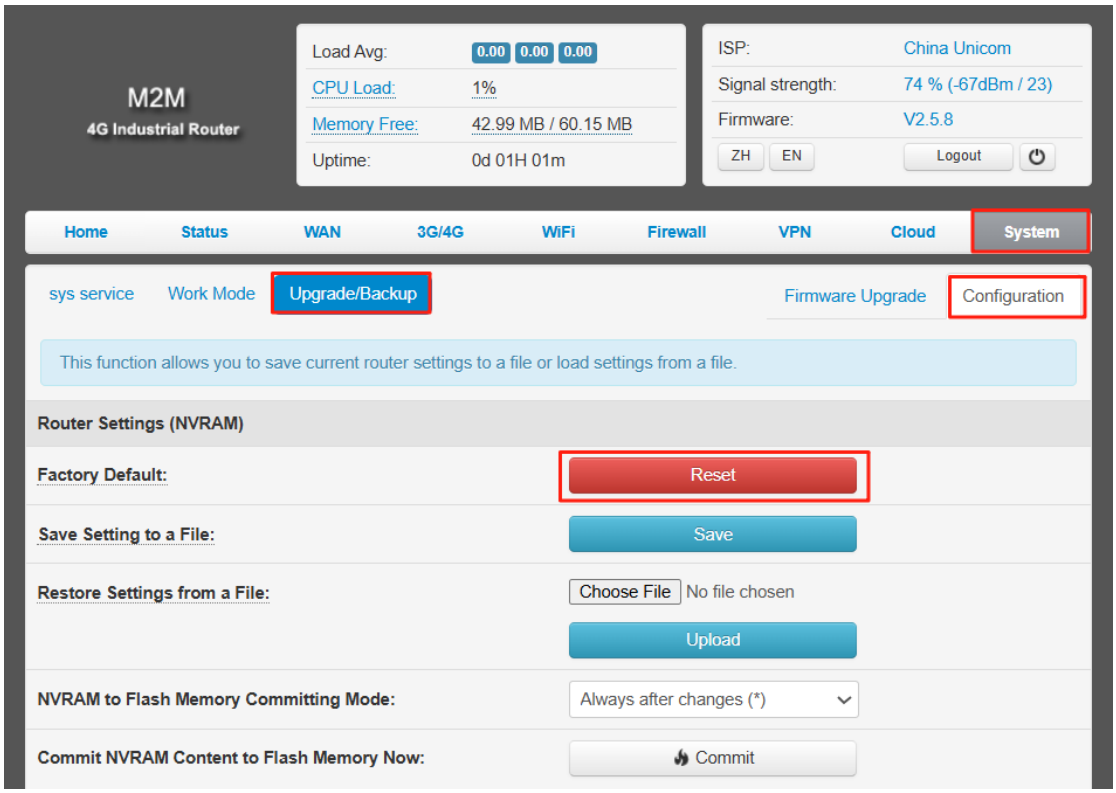
Restore/Export/Upload Settings

A. Factory Default

- The wireless router will reboot automatically during the reset process.
- **All configurations will be erased** and restored to initial defaults.
- **Typical use case:**
  Prepare the device for redeployment in a new network environment.

Operation:

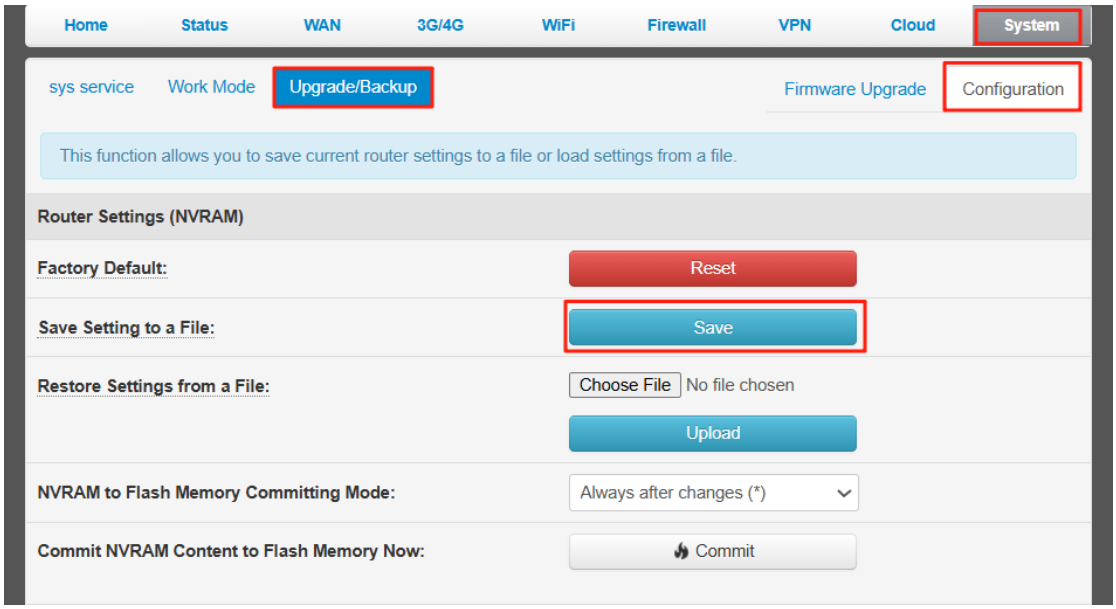
1. Click the **<Reset>** button.
2. Confirm to execute factory reset.



B. Export Settings

- Export current router parameters to a local file as a backup.
- **Application scenario:**

Rapidly configure multiple devices with identical settings.



C. Upload Settings

1. Click **<Choose File>** and select the configuration file.
2. Click **<Upload>** to update router parameters.