

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



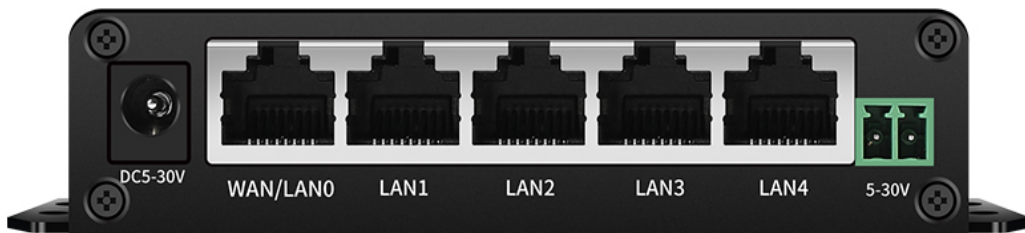
- WIFI
- Serial port (RS232/RS485)
- WEB-based configuration

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

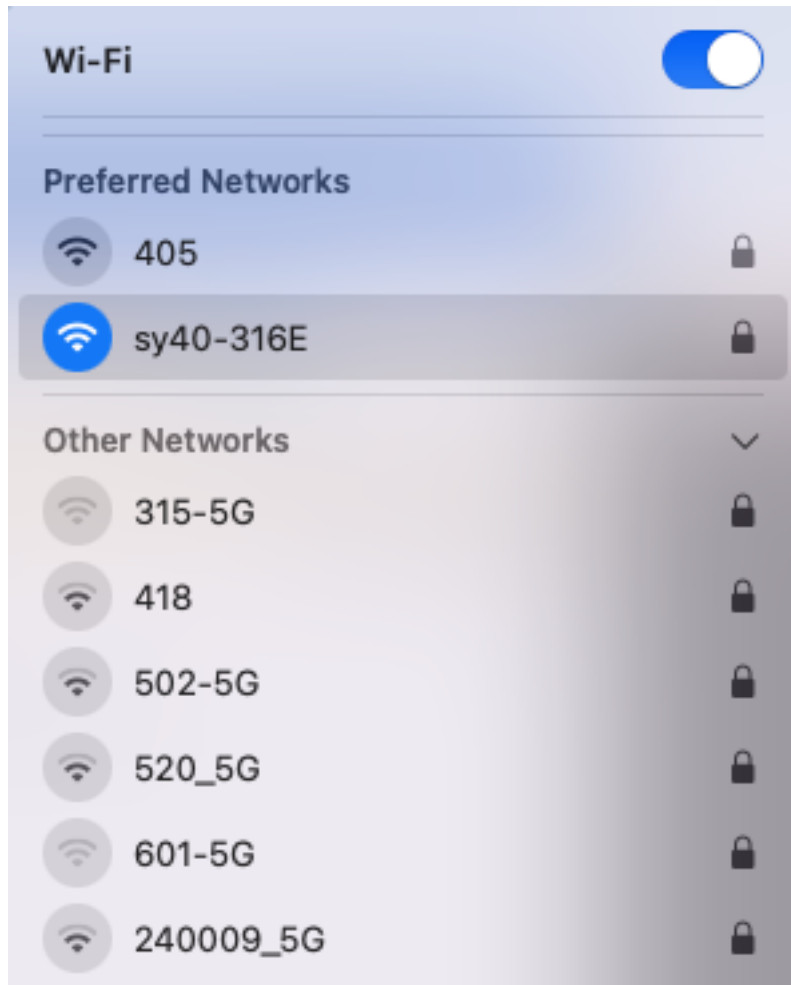
Default router LAN IP: 192.168.1.1

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

M2M
4G Industrial Router

Load Avg: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.34 MB / 60.15 MB
Uptime: 0d 00H 33m

ISP: China CMCC
Signal strength: 100 % (-51dBm / 31)
Firmware: V2.5.8
ZH EN Logout

Home Status WAN 3G/4G WiFi Firewall VPN Cloud System

Internet Status

Connection Control: Reconnect Disconnect Flight Mode

WAN Priority: 3G/4G Modem, always

Connection Status: Connected

Connection Type: 3G/4G/5G Modem

Session Uptime: 0d 00H 32m

Traffic During The Session: ↓ 219.28 MiB ↑ 8.09 MiB

Current Data Rate: ↓ 0 Kbps ↑ 0 Kbps

IPv4 Address WAN: 10.43.8.226

Gateway WAN: 10.43.8.29

DNS: 120.196.165.7
221.179.38.7

WAN MAC Address: 3E:7C:9D:20:5E:30

More Config...

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



M2M
4G Industrial Router

Load Avg: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.04 MB / 60.15 MB
Uptime: 0d 01H 05m

ISP: China CMCC
Signal strength: 100 % (-51dBm / 31)
Firmware: V2.5.8
ZH EN Logout

Home **Status** WAN 3G/4G WiFi Firewall VPN Cloud System

Log Traffic Interface System Log DHCP info Port Forwarding Routing table Network Session Table

System Time: Thu, Aug 14 11:06:36 2025 GMT+0800

```
Aug 14 10:01:13 syslogd started: BusyBox v1.24.2
Aug 14 10:01:13 sy40: The system current version: V2.5.8 <Aug 1 2025 14:26:09>.
Aug 14 10:01:13 kernel: klogd started: BusyBox v1.24.2 (2025-08-01 14:25:39 CST)
Aug 14 10:01:13 kernel: Linux version 3.4.113 (IoT@Iot-Wrt) (gcc version 4.4.7 (GCC) ) #655 Fri Aug
Aug 14 10:01:13 kernel: MediaTek SoC: MT7628A, RevID: 0102, RAM: DDR2, XTAL: 40MHz
Aug 14 10:01:13 kernel: CPU/OCF/SYS frequency: 580/193/193 MHz
Aug 14 10:01:13 kernel: CPU revision is: 00019655 (MIPS 24Kec)
Aug 14 10:01:13 kernel: Determined physical RAM map:
Aug 14 10:01:13 kernel: memory: 04000000 @ 00000000 (usable)
Aug 14 10:01:13 kernel: Zone PFN ranges:
Aug 14 10:01:13 kernel: Normal 0x00000000 -> 0x000004000
Aug 14 10:01:13 kernel: Movable zone start PFN for each node
Aug 14 10:01:13 kernel: Early memory PFN ranges
Aug 14 10:01:13 kernel: 0: 0x00000000 -> 0x000004000
Aug 14 10:01:13 kernel: On node 0 totalpages: 16384
Aug 14 10:01:13 kernel: free_area_init_node: node 0, pgdat 8032b8d0, node_mem_map 81000000
Aug 14 10:01:13 kernel: Normal zone: 128 pages used for memmap
Aug 14 10:01:13 kernel: Normal zone: 0 pages reserved
Aug 14 10:01:13 kernel: Normal zone: 16256 pages, LIFO batch:3
Aug 14 10:01:13 kernel: Primary instruction cache 64kB. VIPT. 4-wav. linesize 32 bytes.
```

Clear **Save** Refresh

Copyright 2010-2025 All Rights Reserved.

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)

The screenshot displays the WAN configuration interface. At the top, there are navigation tabs: Home, Status, WAN (selected), 3G/4G, WiFi, Firewall, VPN, Cloud, and System. Below these are sub-tabs: WAN (selected), LAN, WAN (selected), Port forward (UPnP), DMZ, and DDNS. A blue informational box states: "sy40D supports several connection types to WAN. These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected." The main configuration area includes: WAN Connection Type: IPoE: Static IP; Enable shortcut-fe?: Enable for IPv4/IPv6; WAN IP Settings: IP Address: 0.0.0.0; Subnet Mask: 255.255.255.0; Default Gateway: 0.0.0.0; MTU: 1500 [1300..1500]; WAN DNS Settings: DNS Server 1: (empty); DNS Server 2: (empty); DNS Server 3: (empty); Special Requirement from ISP: Authentication: No; MAC Address: (empty) with a plus button; Don't Decrement the TTL after Routing: No, Always Decrement (*); Ports Isolation and VLAN Filtering: WAN to LAN: No set.

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).



Home Status **WAN** 3G/4G WiFi Firewall VPN Cloud System

WAN LAN **WAN** Port forward (UPnP) DMZ DDNS

sy40D supports several connection types to WAN. These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

WAN Connection Type: IPoE: Automatic IP

Enable shortcut-fe?: Enable for IPv4/IPv6

ARP Ping Alive of Remote Gateway?

WAN DNS Settings

Get the DNS Server Address Automatically?

Special Requirement from ISP

Authentication: No

Host Name: sy40

Vendor Class Identifier:

MAC Address: +

Don't Decrement the TTL after Routing: No, Always Decrement (*)

Ports Isolation and VLAN Filtering

WAN to LAN: No set

Choose IPTV STB Port: No

VLAN Tagged Traffic Filter?

Apply

C. PPPoE (Broadband Dial-Up)

Requires **username & password** for authentication.

Note: Credentials are **case-sensitive**—enter them carefully.



Home Status WAN 3G/4G WiFi Firewall VPN Cloud System

WAN LAN WAN Port forward (UPnP) DMZ DDNS

sy40D supports several connection types to WAN. These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

WAN Connection Type: PPPoE

PPPoE & MAN access: No

Enable shortcut-fe? Enable for IPv4/IPv6

WAN DNS Settings

Get the DNS Server Address Automatically?

PPP VPN Client Setting

User Name:

Password:

Authentication Algorithm: Auto

MTU: 1492 [1000..1492]

MRU: 1492 [1000..1492]

Automatically send LCP requests? Yes No

Adaptive LCP Echo Interval: Yes No

PPPoE Service Name:

Access Concentrator Name:

Idle Disconnect Time in Seconds: 0 [0..86400]

Additional pppd Options:

3.1.2 Port Forward(UPnP)

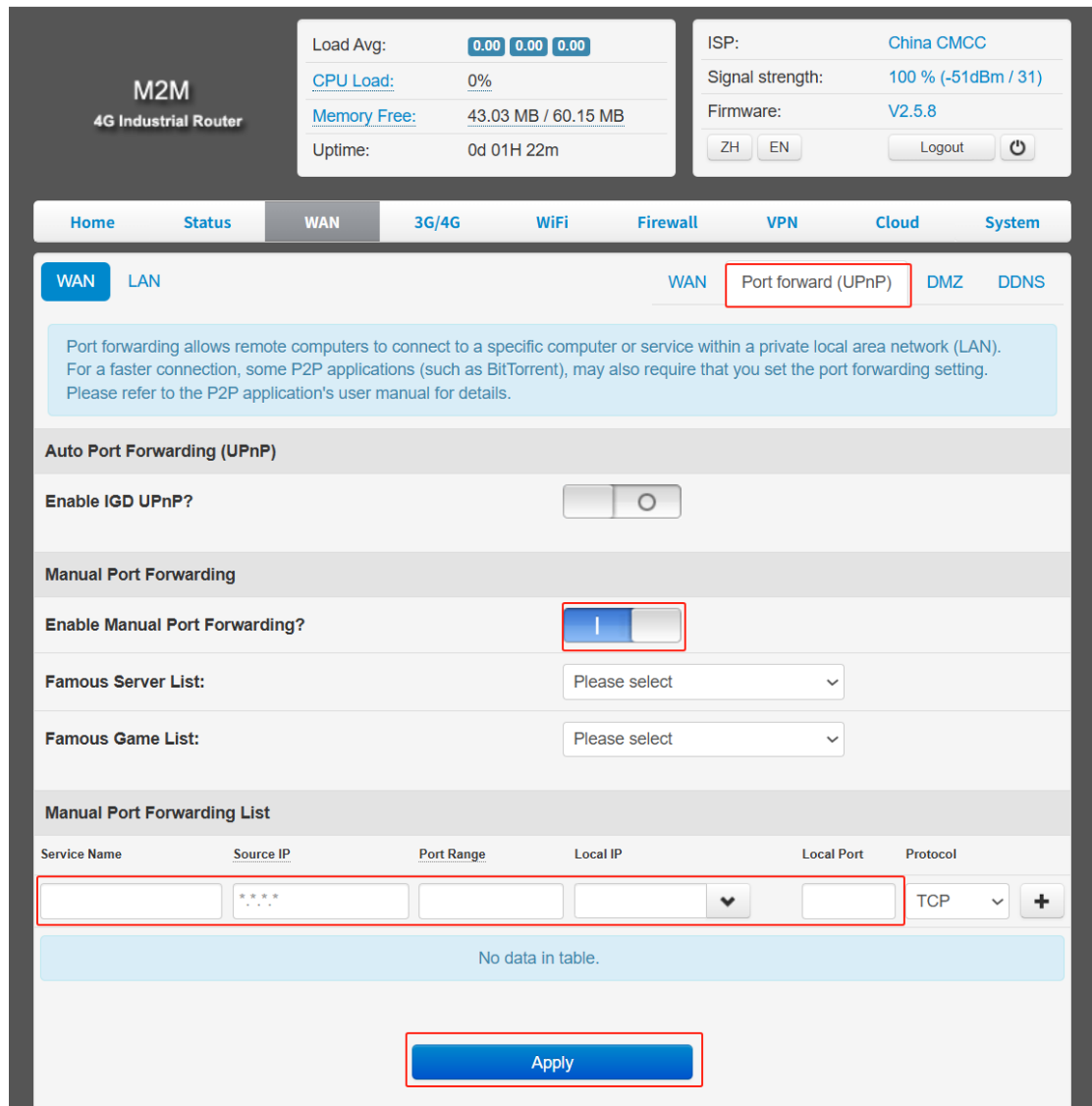
Port forwarding maps internal service ports to the external network, allowing remote access via: Public IP + Port number

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.

Dynamic DNS (DDNS) allows you to assign an Internet domain name to a computer with a dynamic IP Address. Currently, several DDNS services are embedded in sy40D.

The wireless router currently uses a private WAN IP Address (192.168.x.x, 10.x.x.x or 172.16.x.x). This router may be in the multiple-NAT environment and DDNS service will use the external IP from ISP!

Enable the DDNS Client?

Service Profile: [DDNS link](#)

Host Name:

Please fill in the right blanks according to your specific situation

Host Name:

Host Name:

DDNS User Name or E-mail Address or Token:

DDNS Password:

Use Secure HTTPS Connection?

Enable Wildcard?

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



M2M
4G Industrial Router

Load Avg: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.00 MB / 60.15 MB
Uptime: 0d 01H 29m

ISP: China CMCC
Signal strength: 100 % (-51dBm / 31)
Firmware: V2.5.8
ZH EN Logout

Home Status WAN 3G/4G WiFi Firewall VPN Cloud System

WAN LAN LAN DHCP Server Route Switch

Configure the LAN IP of sy40D. The DHCP Server dynamically changes the IP pool when you change the LAN IP.

IP Address: 192.168.1.1 192.168.1.1
Subnet Mask: 255.255.255.0 255.255.255.0

Enable Spanning Tree Protocol (STP)?

Apply

3.2.2 DHCP Server

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

Home Status WAN 3G/4G WiFi Firewall VPN Cloud System

WAN LAN LAN DHCP Server Route Switch

sy40D supports up to 253 IP Addresses for your local network. The IP Address of a local machine can be assigned manually by the network administrator or obtained automatically from sy40D if the DHCP Server is enabled.

Enable DHCP Server?

Domain Name: lan

IP Pool Starting Address: 192.168.1.100

IP Pool Ending Address: 192.168.1.200

DHCP Lease Time (sec): 86400 [120..604800]

Default Gateway:

DNS and WINS Server Setting

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.

The screenshot displays the '3G/4G' configuration page. At the top, there are tabs for Home, Status, WAN, 3G/4G, WiFi, Firewall, VPN, Cloud, and System. Below the tabs, there are sub-tabs for cellular, 3G/4G, vpdn, and AT. A blue banner at the top contains the text: "When using a VPDN dedicated network card or directional card, please set 'WAN disconnection detection': System Service - Wan Detect".

Under the 'cellular' sub-tab, there is a section for 'Enable 3G/3G Modem' with a toggle switch turned on. A red annotation points to this toggle with the text: "If you need a secondary card for backup, please turn on it." Below this is the 'SIM card backup' section, which includes a dropdown for 'initial SIM card' (set to SIM0), a 'dial failure count (switch)' set to 3, and an 'On/Off' toggle switch. A red annotation points to the 'On/Off' toggle with the text: "Using: SIM0".

The '3G/4G Modem Base Settings' section is divided into two columns for SIM0 and SIM1. For SIM0, the 'Auto ISP' toggle is turned off, with a red annotation: "Turn off the automatic carrier matching service if you need an APN private network." The 'Modem Type' is 'NDIS/xCM/QMI: LTE', 'Location' is 'China', 'ISP' is 'China Unicom', 'APN Service' is '3gnet', 'PIN Code' is empty, 'Username' is empty, 'Password' is empty, 'authentication protocol' is 'CHAP', 'PDP' is 'IP', and 'Preferred Network' is 'Auto'. For SIM1, the 'Auto ISP' toggle is turned on, 'Modem Type' is 'NDIS/xCM/QMI: LTE', 'Location' is 'China', 'ISP' is 'China Unicom', 'APN Service' is '3gnet', 'PIN Code' is empty, 'Username' is empty, 'Password' is empty, 'authentication protocol' is 'PAP/CHAP (auto)', 'PDP' is 'IP', and 'Preferred Network' is 'Auto'.

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.

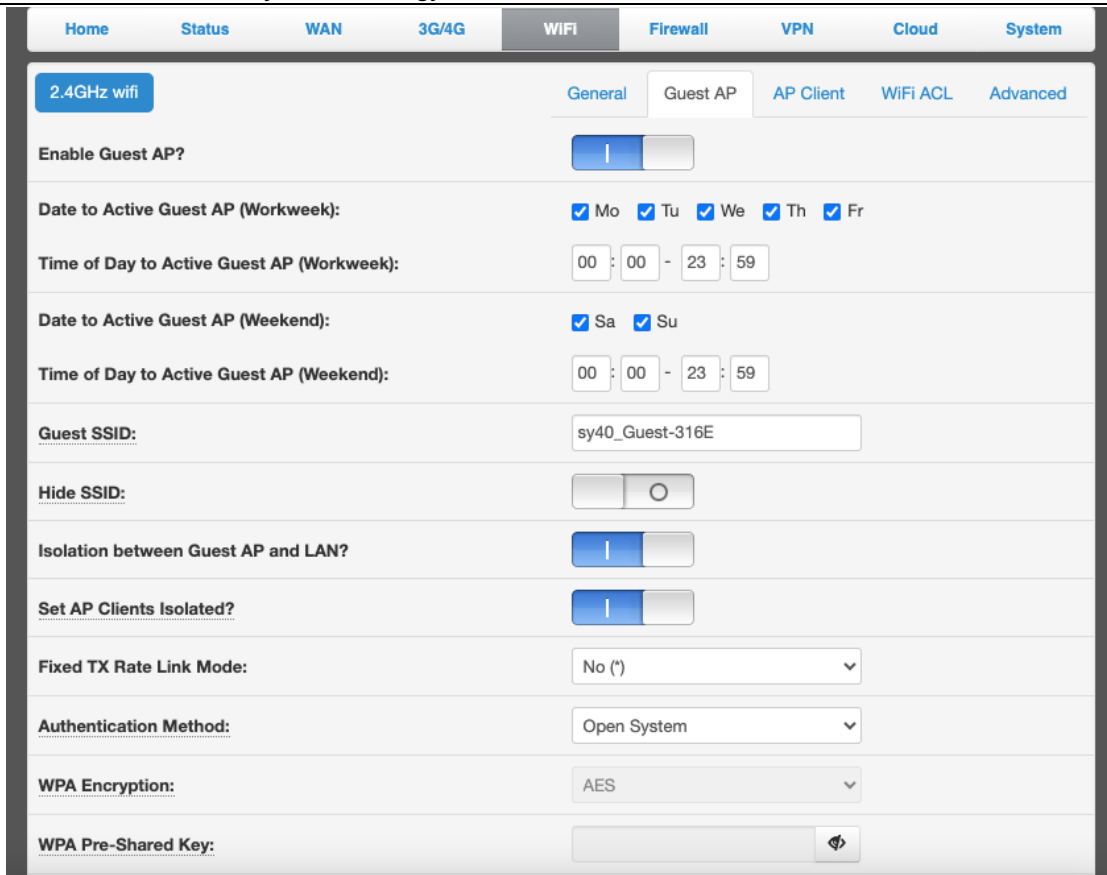


Home	Status	WAN	3G/4G	WiFi	Firewall	VPN	Cloud	System
2.4GHz wifi		General Guest AP AP Client WiFi ACL Advanced						
Enable Radio?	<input type="checkbox"/>							
Date to Enable Radio (workweek):	<input checked="" type="checkbox"/> Mo <input checked="" type="checkbox"/> Tu <input checked="" type="checkbox"/> We <input checked="" type="checkbox"/> Th <input checked="" type="checkbox"/> Fr							
Time of Day to Enable Radio (workweek):	00 : 00 - 23 : 59							
Date to Enable Radio (weekend):	<input checked="" type="checkbox"/> Sa <input checked="" type="checkbox"/> Su							
Time of Day to Enable Radio (weekend):	00 : 00 - 23 : 59							
SSID:	sy40-316E							
Hide SSID:	<input type="checkbox"/>							
Auto Hide SSID:	0 [0..100 min] - 0:disabled							
Wireless Mode:	g/n Mixed (*)							
Channel Bandwidth:	20/40 MHz							
Radio Channel:	Autoselect							
Extension Channel:	Above (+4)							
Fixed TX Rate Link Mode:	No (*)							
Authentication Method:	WPA2-Personal							
WPA Encryption:	AES							
WPA Pre-Shared Key: <input type="checkbox"/>							
Network Key Rotation Interval:	3600 [0..2592000]							
TX Power Adjustment (%):	100 [0..100] - 0:disabled							
Region Code:	China (channels 1-13)							

5.2 Guest AP

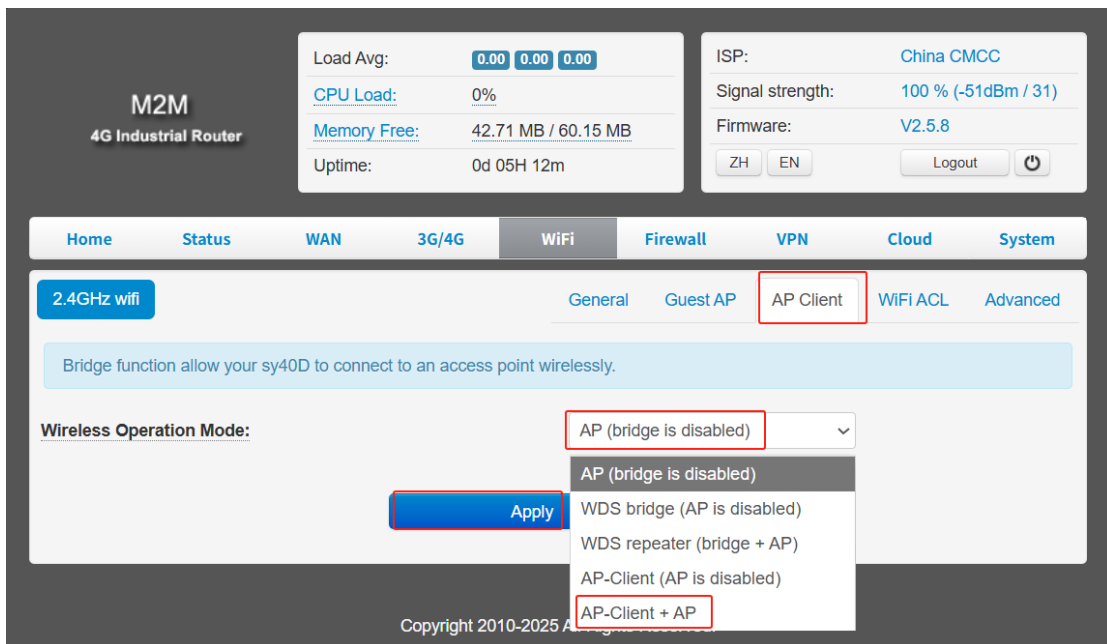
Create isolated WIFI for visitors with separate management

- 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

The screenshot shows the configuration page for the 2.4GHz wifi interface. At the top, there are system status metrics: Load Avg (0.00, 0.03, 0.00), CPU Load (0%), Memory Free (43.73 MB / 60.15 MB), and Uptime (0d 00H 04m). The ISP is China CMCC with a signal strength of 87% (-59dBm / 27) and firmware version V2.5.8. The navigation menu includes Home, Status, WAN, 3G/4G, WiFi (selected), Firewall, VPN, Cloud, and System. Under the WiFi section, there are tabs for General, Guest AP, AP Client (selected), WiFi ACL, and Advanced. A blue box contains instructions for the bridge function. The main configuration area includes: Wireless Operation Mode (AP-Client + AP), Wireless AP-Client Role (WAN (Wireless ISP)), Radio Channel (Channel track checked), STA SSID (m2m), Authentication Method (WPA2-Personal), WPA Encryption (AES), and WPA Pre-Shared Key (masked). An Apply button is at the bottom.

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==>>**
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA Pre-Shared Key:

Apply

click here to enter

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
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA Pre-Shared Key:

Apply

- 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%



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

The screenshot shows the M2M 4G Industrial Router web interface. The top navigation bar includes Home, Status, WAN, 3G/4G, WiFi, Firewall, VPN, Cloud, and System. The WiFi section is active, and the '2.4GHz wifi' tab is selected. The 'WPA Pre-Shared Key' field is highlighted with a red box, and the 'Apply' button is also highlighted with a red box.

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: 8 Channel track

STA SSID: 405

Authentication Method: WPA2-Personal

WPA Encryption: AES

WPA Pre-Shared Key:

Apply

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.



M2M
4G Industrial Router

Load Avg: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.64 MB / 60.15 MB
Uptime: 0d 00H 25m

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

Wireless MAC Filter allows you to control packets from devices with specified MAC Address in your Wireless LAN.

MAC Filter Mode: Disabled
Disabled
Accept
Reject

Apply

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: 0.00 0.00 0.00
CPU Load: 0%
Memory Free: 43.56 MB / 60.15 MB
Uptime: 0d 00H 28m

ISP: China CMCC
Signal strength: 80 % (-63dBm / 25)
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? click here if to enable

Apply

Copyright 2010-2025 All Rights Reserved.



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?

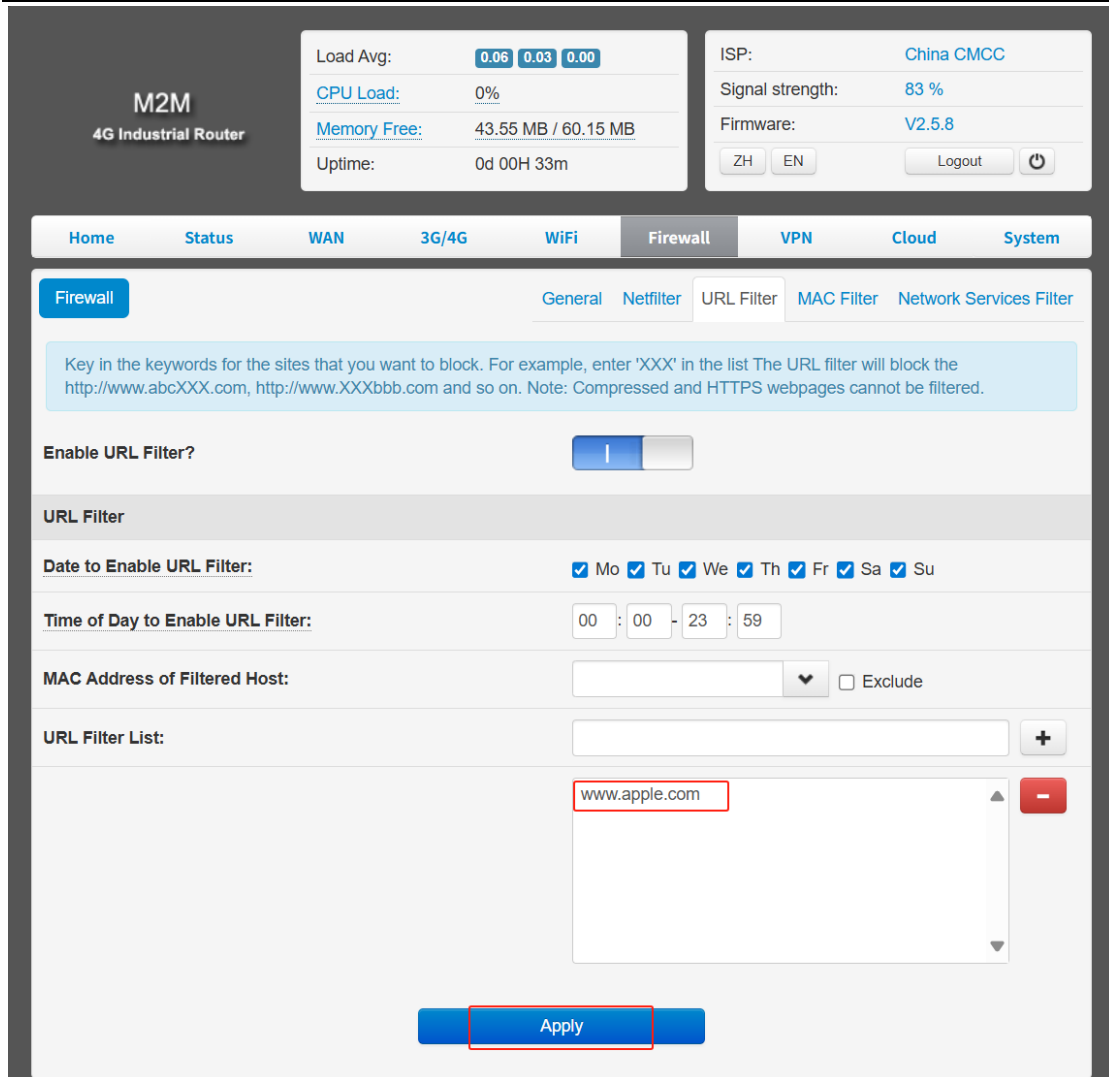
URL Filter

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:



6.2 MAC Filter

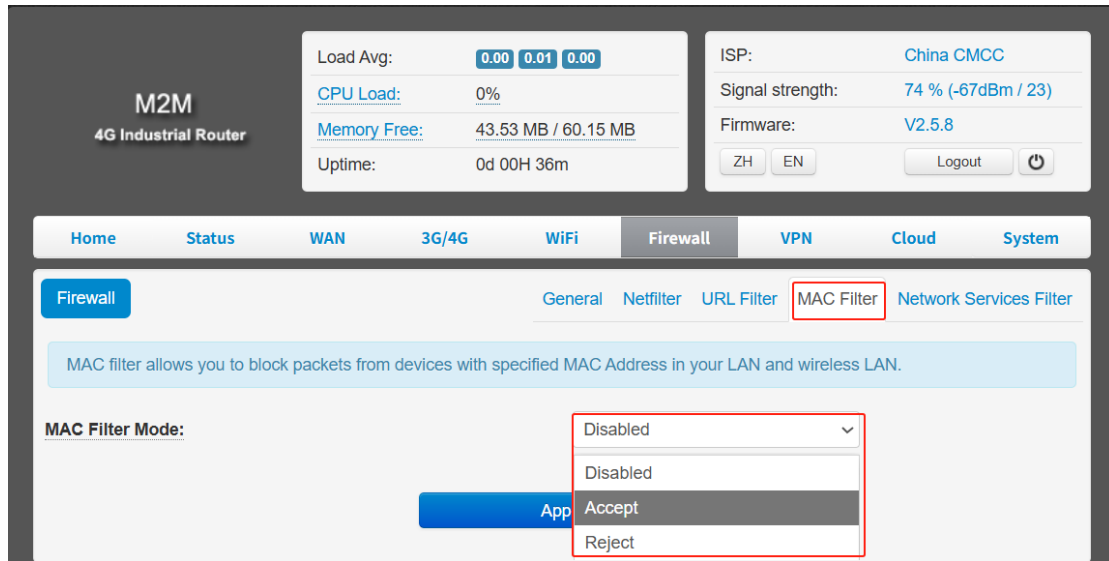
This feature restricts network access based on device MAC addresses, operating in two modes:

1. Accept(Whitelist)

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

2. Reject(Blacklist)

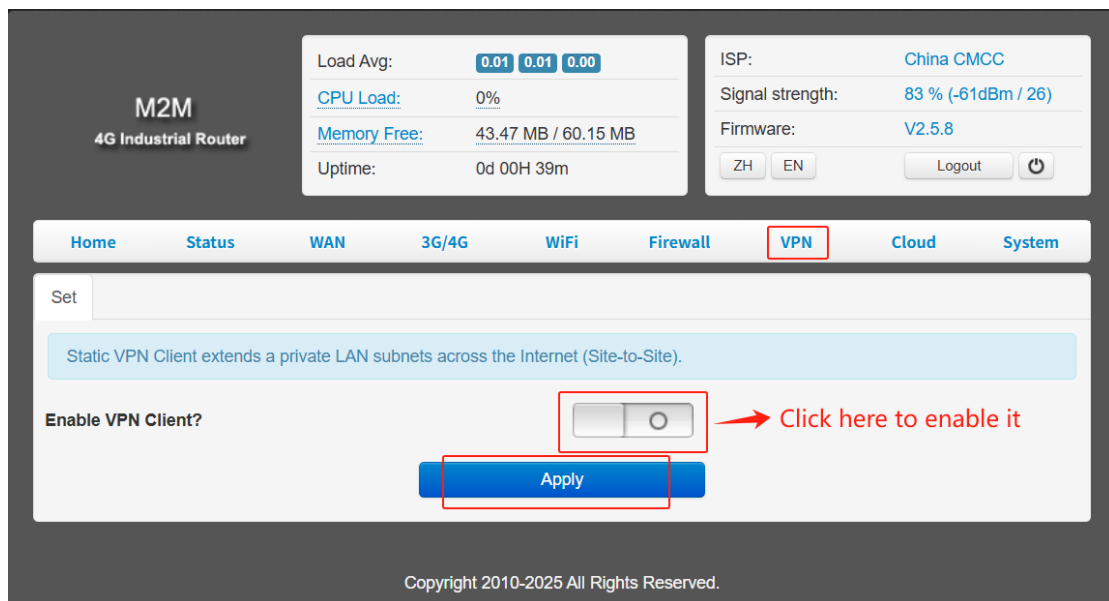
Blocks specific MAC addresses while allowing all others
Useful for banning unauthorized devices



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”

Home Status WAN 3G/4G WiFi Firewall Log 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: PPTP

Remote VPN Server (IP or DNS host):

Login: vpntest

Password:

Authentication Algorithm: Auto

Encryption Cipher Algorithm: Auto

MTU: 1450 [1000..1460]

MRU: 1450 [1000..1460]

Automatically send LCP requests?

Adaptive LCP Echo Interval:

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 F

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

If your server settings include these two, they must be set.

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:	PPTP
Remote VPN Server (IP or DNS host):	PPTP L2TP (w/o IPSec) OpenVPN
Login:	
Password:	*****
Authentication Algorithm:	Auto
Encryption Cipher Algorithm:	Auto
MTU:	1450 [1000..1460]
MRU:	1450 [1000..1460]



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:

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 I2tp 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: Reconnect/VPN

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

These two must be set if your server settings include them.



8. System

8.1.1 Base

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

The screenshot shows the 'Base' configuration page in the SY40 web interface. The 'System' tab is selected, and the 'Base' sub-tab is active. The page contains the following sections and fields:

- System Identification:**
 - Device Name: sy40
 - Administrator Login: admin
 - New Password: (empty)
 - Retype New Password: (empty)
- System Time:**
 - Time Zone: (GMT+08:00) Beijing, Hong Kong
 - NTP Synchronization Period: 12 hours
 - NTP Server 1: pool.ntp.org (Find NTP button)
 - NTP Server 2: ntp1.aliyun.com
- Miscellaneous:**
 - Remote Log Server: (empty) : 514
 - store log: (radio button)
 - Enable Syslog Floating Toolbar? Yes (*)
 - Select WebUI Language: English
 - Enable Context Help? (checkbox)

An 'Apply' button is located at the bottom of the 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

Internet Detector monitors access to the Internet and allows to perform the required actions when the state of Internet access changes.

If you have a private network or a corporate intranet, you must change either Remote...Port 1 or Remote...Port 2 to the address of your private network server or to a consistently online and pingable address.

Internet Detector Poll Mode: Continuous polling

List of Internet Hosts for Check TCP Connection

Remote Server Address and Port 1:	Remote Server Address and Port 2:	Remote Server Address and Port 3:	Remote Server Address and Port 4:	Remote Server Address and Port 5:	Remote Server Address and Port 6:
baidu.com : 80 [ip or domain]	qq.com : 80 [ip or domain]	114.114.114.114 : 53 [ip]	223.5.5.5 : 53 [ip]	208.67.220.220 : 53 [ip]	208.67.222.222 : 53 [ip]

Internet Hosts Polling Settings

Poll Interval After Connection Success/Failed (s): 55 / 5 [55 / 5]

Connection Timeout (s): 3 [1..10]

Events when the State of Internet Access is Changed

Delay Before Raise [Internet Lost] Event (s): 5 [0..600]

Perform Action on [Internet Lost] Event: Reconnect WAN

Pause Before Run New WAN Connection (s): 2 [0..600]

Run the Script When the State of Internet Access is Changed:

Network failure:

Check count:	Router reboot	Reboot 4G module	Reboot 4G module by power off
3 [1..100]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

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.

The screenshot displays the M2M 4G Industrial Router web interface. At the top, there are system status widgets: 'Load Avg' (0.00, 0.00, 0.00), 'CPU Load' (3%), 'Memory Free' (42.24 MB / 60.15 MB), and 'Uptime' (0d 00H 53m). On the right, 'ISP' is China Unicom, 'Signal strength' is 90% (-57dBm / 28), and 'Firmware' is V2.5.8. The main navigation bar includes Home, Status, WAN, 3G/4G, WIFI, Firewall, VPN, Cloud, and System (highlighted). Under the System tab, 'Upgrade/Backup' and 'Firmware Upgrade' are highlighted. The 'Firmware Upgrade' section contains instructions: 1. Specify the path of and name of the downloaded file in the [New Firmware File]. 2. Click [Upload] to upload the file to router. Uploading process takes about 2-3 minutes. 3. After receiving a correct firmware file, router will automatically start the upgrade process. The system reboots after the upgrading process is finished. Below the instructions, there are input fields for 'Product ID' (sy40D), 'MAC' (0C117F05316E), and 'Firmware Version' (V2.5.8 - Aug 1 2025 14:26:08). The 'New Firmware File' field has a 'Choose File' button and 'No file chosen' text. The 'Factory Default' field has a radio button. At the bottom, there is a large blue 'Upload' button.

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.

The screenshot shows the M2M 4G Industrial Router web interface. At the top, there are system status metrics: Load Avg (0.00, 0.00, 0.00), CPU Load (1%), Memory Free (42.99 MB / 60.15 MB), and Uptime (0d 01H 01m). On the right, ISP information is shown: China Unicom, Signal strength (74 % (-67dBm / 23)), and Firmware (V2.5.8). The navigation menu includes Home, Status, WAN, 3G/4G, WiFi, Firewall, VPN, Cloud, and System. The System menu is expanded, showing sub-menus for sys service, Work Mode, Upgrade/Backup, Firmware Upgrade, and Configuration. The Upgrade/Backup sub-menu is selected, displaying a description: "This function allows you to save current router settings to a file or load settings from a file." Below this, the Router Settings (NVRAM) section is visible, containing several options: Factory Default (with a highlighted Reset button), Save Setting to a File (with a Save button), Restore Settings from a File (with a Choose File button and No file chosen text, and an Upload button), NVRAM to Flash Memory Committing Mode (set to Always after changes (*)), and Commit NVRAM Content to Flash Memory Now (with a Commit button).

B. Export Settings

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

Rapidly configure multiple devices with identical settings.

This screenshot is identical to the one above, showing the same web interface. In this instance, the 'Save' button in the 'Save Setting to a File' section is highlighted with a red box.



C. Upload Settings

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

The screenshot displays the router's web interface. At the top, there is a navigation menu with tabs for Home, Status, WAN, 3G/4G, WiFi, Firewall, VPN, Cloud, and System. The System tab is active. Below the navigation, there are sub-tabs for sys service, Work Mode, Upgrade/Backup, Firmware Upgrade, and Configuration. The Upgrade/Backup sub-tab is selected. A light blue box contains the text: "This function allows you to save current router settings to a file or load settings from a file." Below this, the "Router Settings (NVRAM)" section is visible. It includes several options: "Factory Default:" with a "Reset" button; "Save Setting to a File:" with a "Save" button; "Restore Settings from a File:" with a "Choose File" button (highlighted with a red box) and the text "No file chosen", and an "Upload" button (also highlighted with a red box); "NVRAM to Flash Memory Committing Mode:" with a dropdown menu set to "Always after changes (*)"; and "Commit NVRAM Content to Flash Memory Now:" with a "Commit" button.