# YZW280

**Industrial gateway**




# USER MANUAL

**MT7621AT**

**512 MB DDR3**

**DIN rail**

**−30–75 °C**

**Modbus RTU / TCP**

**VPN / m2mCloud**

**MQTT**

**DTU**

V1.3 • Installation, configuration and maintenance • 2026-11-02

# CONTENTS


**1. Gateway introduction** 5
1.1 Product overview 6
1.2 Variants and options 7
1.3 Remote PLC/HMI maintenance 7
1.4 Modbus acquisition and MQTT reporting 8
1.5 Wired/cellular failover 9
1.6 Camera or terminal backhaul 11
1.7 Prerequisites and capability boundaries 12

**2. Interfaces, installation and connections** 13
2.1 Interfaces and indicators 14
2.2 Main specifications 17
2.3 Package and antenna connections 18
2.4 Dimensions and mounting position 19
2.5 SIM installation and power connection 20
2.6 Serial wiring and service ownership 21

**3. Basic operation and status** 22
3.1 PC connection and Web login 23
3.2 Web interface layout 25
3.3 Device, uplink and client status 26

**4. Network settings** 28
4.1 WAN settings 29
4.2 LAN settings 32
4.3 VLAN settings 34
4.4 Wi-Fi settings 36
4.5 Cellular settings 38
4.6 DHCP service 41
4.7 Link Configuration and failover 43
4.8 Load balancing 47
4.9 DDNS 49

**5. Applications** 52
5.1 Choose acquisition and data processing 53
5.2 ICMP monitoring 53
5.3 Scheduled tasks 55
5.4 Network diagnostics 56
5.5 SMS settings and manual sending 58
5.6 DTU transparent transport 59
5.7 Modbus acquisition and reporting 66
5.8 Modbus device connection 69
5.9 Modbus commands and addressing 71
5.10 Modbus cloud writes over MQTT 74
5.11 SNMP 78
5.12 Local MQTT Broker 79
5.13 Alarm notifications 81
5.14 SMTP mail service 83

**6. VPN** 85
6.1 Choose remote access and tunnels 86
6.2 OpenVPN clients 88
6.3 OpenVPN server 91
6.4 WireGuard 94
6.5 ZeroTier 98
6.6 IPsec 99
6.7 L2TP client 101
6.8 L2TP server 103
6.9 GRE 104
6.10 VXLAN 106
6.11 DMVPN 107
6.12 PPTP client and server 110

**7. Forwarding** 112
7.1 NAT and port forwarding 113
7.2 Static routes 115
7.3 MASQ masquerading 116
7.4 QoS rate control 117

**8. Firewall** 120
8.1 Management ports and remote access 121
8.2 SPI filtering 123
8.3 Address filtering 124
8.4 Domain filtering 126

**9. System management** 128
9.1 Local logs 129
9.2 System time 130
9.3 Admin password management 132
9.4 Configuration backup and restore 133
9.5 Firmware upgrade 135
9.6 Reset button and recovery 137

**10. m2mCloud remote management** 139
10.1 Client configuration and networking 140
10.2 Remote PLC/HMI program transfer 144
10.3 Remote serial access 145
10.4 Windows client: remote access 145
10.5 Linux client: login and bridge 146

**11. Troubleshooting** 148
11.1 Locate faults along the service path 149
11.2 Bilingual terms and section mapping 150

YZW280

# Start with your requirements

Choose your problem, enter the table values, save, test and diagnose. M1 uses the supplied 现场测试工具.zip beside this PDF; lab plans differ from factory defaults.

| REQUIREMENT | SECTIONS |
|---|---|
| Cannot open Web / first login | 2.1 Interfaces and indicators • 2.5 SIM installation and power connection • 2.6 Serial wiring and service ownership • 3.1 PC connection and Web login • 3.3 Device, uplink and client status |
| No uplink / recover after failure | 4.1 WAN settings • 4.2 LAN settings • 4.5 Cellular settings • 4.4 Wi-Fi settings • 4.7 Link Configuration and failover • 4.8 Load balancing |
| Connected but no data / M1 read | 5.1 Choose acquisition and data processing • 5.6 DTU transparent transport • 5.7 Modbus acquisition and reporting |
| Remote PLC / prove HTTP first | 6.1 Choose remote access and tunnels • 10.1 Client configuration and networking • 10.2 Remote PLC/HMI program transfer • 10.3 Remote serial access |
| Backup/recovery / first failure | 9.1 Local logs • 9.4 Configuration backup and restore • 9.5 Firmware upgrade • 9.6 Reset button and recovery • 11.1 Locate faults along the service path |

## INSPECTED UNIT REFERENCE

YZW280

Capture address: 192.168.188.214; an existing test-network address, not a factory default.

This model has no GPS, PLC Collect or Node-RED. Only a 2.4 GHz Wi-Fi menu is present. Shell scripting does not imply Python or Node.js. The primary WAN IPv4 selector includes LAN. Retain another local management connection and recheck uplink selection before changing its role.

YZW280

# First use: from wiring to network access

**Wire → Sign in → Uplink → Service → Record**

1. With power disconnected, fit SIM/antennas/serial wiring and confirm this model’ s power and electrical interfaces.
2. Connect the PC to LAN. Defaults use 192.168.8.1/24; configured equipment uses its administrator-provided current address.
3. Sign in, record model/firmware, change the initial password and verify a fresh login.
4. Establish one WAN or cellular uplink and test gateway, external IP, DNS and a LAN client separately.
5. Add project VPN, acquisition and MQTT services. Read one known point before reporting/processing.
6. Export configuration and record service results, recovery behavior and delivery versions.

Examples are not field control instructions. Unsaved form examples are labeled separately from runtime states. Document production did not change service settings, deploy flows or perform field control.

CHAPTER

# 01

# Introduction

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 1. Gateway introduction

## 1.1 Product overview

YZW280 provides industrial site connectivity, serial transport and remote maintenance. Establish local networking first, then add Modbus, VPN, MQTT and the edge functions available on this model.

### FIELD TASK: HOW TO COMPLETE A FIELD TASK USING THIS MANUAL

Choose one task and follow its entries, save order, test, result, diagnosis and recovery. Reproduce it in an isolated network before replacing site-specific values. Screenshots may be read-only references or unsaved forms; follow the field table and delivered UI.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Factory Access | 192.168.8.1/24 | Defaults only; start in Login |
| Lab Gateway / PC | 192.168.10.1 / 192.168.10.10 | Use after the LAN case; mask/24 |
| PLC / Camera | 192.168.10.20 / 192.168.10.30 | Site plan, not factory addresses |
| Upstream / Peer LAN | 192.168.20.0/24 / 192.168.30.0/24 | Only with actual interfaces/peers required by the case |
| Test Package | 现场测试工具.zip | Supplied beside the manual: Python script, flows and bilingual instructions |

### SAVE, TEST AND OBSERVE

1. Export current configuration, record management access and check lab/site/remote subnet overlap.
2. Basic order: Login→LAN→one uplink→M1 read-only acquisition. Add failover/remote/processing only as needed. Cases need not run together; M2/P1 writes require separate permission.
3. Record actual settings, command, observation and time for each test; back up after passing. On failure follow the relevant branch without changing everything at once.

### PASS CRITERIA AND DIAGNOSIS

Simulator success proves only the tested components, not real PLCs, radio coverage, PoE loading or project acceptance. Repeat relevant tests with the actual equipment.

**Finish and restore:** Undo temporary settings as specified for each task and complete the site/acceptance records.

- 2 × Gigabit RJ45; default 1 WAN/LAN + 1 LAN
- Standard 2 × RS485; one port can be ordered as RS232

- Audited unit: 4G; the datasheet also lists ordered Cat 1 / Cat 4 and 5G RedCap variants; MAIN antenna and ordered DIV antenna
- Modbus RTU/TCP → MQTT / TCP / UDP / IEC104
- OpenVPN / WireGuard / ZeroTier / IPsec / m2mCloud

## 1.2 Variants and options

| ITEM | SCOPE FOR THIS MODEL |
|---|---|
| 4G / 5G | Audited unit: 4G; the datasheet also lists ordered Cat 1 / Cat 4 and 5G RedCap variants; MAIN antenna and ordered DIV antenna |
| Wi-Fi | 2.4 GHz |
| CPU / RAM / Flash | MT7621AT / 512 MB DDR3 / 16 MB SPI NOR |
| Node-RED | Not supported |

This model has no GPS, PLC Collect or Node-RED. Only a 2.4 GHz Wi-Fi menu is present. Shell scripting does not imply Python or Node.js. The primary WAN IPv4 selector includes LAN. Retain another local management connection and recheck uplink selection before changing its role.

The datasheet lists ordered Cat 1, Cat 4 and 5G RedCap variants. Screenshots represent the 4G sample, not every order configuration.

## 1.3 Remote PLC/HMI maintenance

Connect local LAN and uplink, then establish an authorized VPN or m2mCloud tunnel. Test the target IP/port before starting vendor tools; broadcast discovery depends on L2/L3 mode.

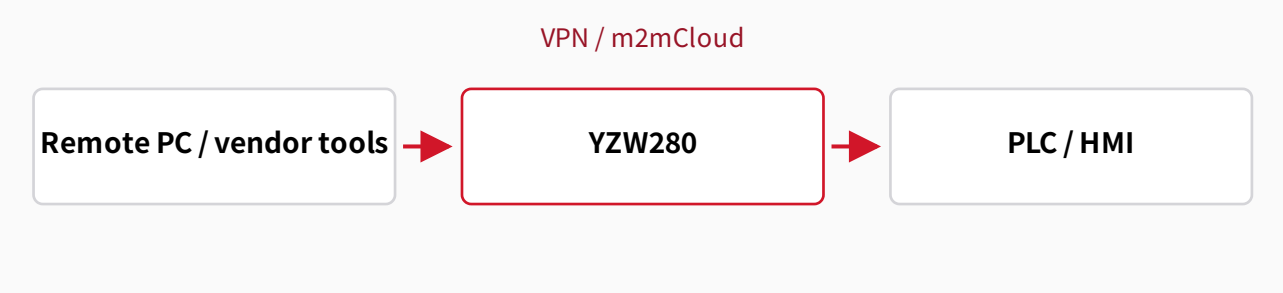



Figure 1-1 Remote PLC/HMI maintenance

### FIELD TASK: USE THE REMOTE-ACCESS CASE TO VERIFY EVERY STAGE

Site LAN192.168.10.0/24 must not overlap the remote PC LAN. Obtain server/port, account authorization, network type, tunnel IPs and allowed subnets from the platform administrator. Validate session, virtual network and site service separately.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Client / Server / Port | On / actual platform server / port | Copy the actual platform endpoint |
| Connection / Tunnel Type | Authorized connection / L3 example | Authorized connection; this L3 case does not imply L2 broadcast |
| M2M IP | Gateway10.44.0.2; remote PC10.44.0.3 | Must actually be assigned/approved by platform |
| Remote Prefix / Peer M2M IP | remote network plan | Do not route the gateway’ s own LAN as remote; PC route to subnet10 goes via gateway tunnel IP |

### SAVE, TEST AND OBSERVE

1. Prove server reachability, save endpoint/authorization/network settings and enable. Inspect session/interface address and authorize both gateway and PC on the platform.
2. Join the same authorized network from the remote PC. Ping the actual gateway tunnel IP and inspect route192.168.10.0/24 via that IP. Do not add conflicting routes if platform manages them.
3. Run bench on LAN PC .10.10. From remote open http://192.168.10.10:8080/ before testing the actual PLC/HMI service.

### PASS CRITERIA AND DIAGNOSIS

Online but no tunnel-IP access: inspect authorization/type/address. Tunnel works but 192.168.10.10 fails: inspect PC route, LAN client gateway 192.168.10.1, firewall and return path.

**Finish and restore:** Leave the test network and revoke temporary routes/authorization; retain approved maintenance scope and local recovery.

## 1.4 Modbus acquisition and MQTT reporting

Start with one instrument and one known read-only point. Verify address, type, scaling and unit before setting publication topics. Compare field, gateway and platform values over repeated samples.




Figure 1-2 Modbus acquisition and MQTT reporting

### FIELD TASK: COMPLETE ACQUISITION/REPORTING WITH M1

On an isolated LAN set the gateway to 192.168.10.1/24 and PC to 192.168.10.10/24, gateway .10.1. Get the Field Test Tools package from Product Documents / Shared Resources. Install Python 3.8+, open its extracted folder and run python site_lab.py bench --bind 192.168.10.10. Keep it open. Allow only the lab LAN to TCP1502/1884/5001/8080 and UDP5002 on the PC firewall.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable / Report Method | On / MQTT | Enable collection and MQTT reporting |
| MQTT Server / Port | 192.168.10.10 / 1884 | PC test broker, separate from the gateway broker |
| Username / Password | field / DemoOnly2026 | Lab credentials for the supplied tool only |
| CA / TLS | TLS off | Plain transport on isolated LAN only; use platform certificates for production |
| Response Timeout | 1000 ms | Enter 1 if the page uses seconds |
| Periodic / Report Interval | On / 5 s | Use the periodic-report option exposed on the page |

### SAVE, TEST AND OBSERVE

1. In a second PC window run python site_lab.py modbus-get --host 192.168.10.10. Expect values [255], proving the mock slave runs.
2. Add a TCP device as in the next section, then the temperature command. Save command, device connection and global settings in order; confirm acquisition is enabled.
3. Run python site_lab.py watch --host 192.168.10.10 --topic plant/site1/plc1/data --seconds 30 --expect temperature=255. The tool prints raw messages and PASS when it observes numeric 255.

### PASS CRITERIA AND DIAGNOSIS

Require successful acquisition and an observed temperature=255. MQTT online alone is insufficient. No message: inspect broker/auth/topic then collection logs. Wrong value: inspect FC, start and type.

For a real instrument replace IP/port/unit/register map individually. 255 is a lab raw value; a 0.1 scale gives 25.5. Do not label raw 255 as 255°C.

**Finish and restore:** Disable the test connection, stop the tool with Ctrl+C and remove temporary firewall rules. Configure production credentials/TLS from the handover sheet.

## 1.5 Wired/cellular failover

Validate wired and cellular uplinks independently. Select WAN / Mobile in Link Configuration and set probes for every actual interface. Test primary failure/recovery and service reconnection during maintenance.

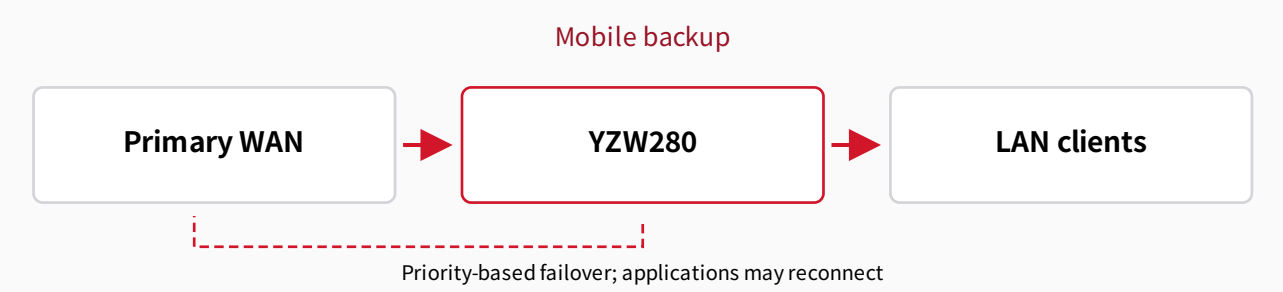



Figure 1-3 Wired/cellular failover

## FIELD TASK: DISCONNECT AND RECOVER USING THE FAILOVER CASE

Prove WAN and cellular applications individually before this test. Disable a conflicting load-balancing plan. WAN test gateway is 192.168.20.1; cellular probes need a real carrier-reachable ICMP target, not the WAN private address.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Link Configuration | WAN / Mobile | Use this combination if present; wired first |
| Keepalive Check | enabled | Configure for multiple actual interfaces as required |
| WAN IPv4 Check Address | 192.168.20.1 | Proves reachability only to upstream gateway; use a reachable end-to-end target to detect upstream outages |
| Cellular IPv4 Check Address | carrier-reachable IP | One literal IPv4 address per interface |

## SAVE, TEST AND OBSERVE

1. Save and record Current, Status and Reason for IPv4/IPv6 plus the LAN application result. A healthy non-current backup is normally expected.
2. At the unit, disconnect only the WAN uplink cable, retaining LAN management. Record fault time, egress change and application reconnection time. Restore WAN, observe recovery and retest.
3. Also test upstream Internet failure with Ethernet still connected. If 192.168.20.1 still answers, that probe cannot detect the upstream outage; choose an end-to-end reachable target and repeat.

## PASS CRITERIA AND DIAGNOSIS

Pass when the application recovers; no fixed switching time is promised. No switch: check backup IP/service. Switched without data: check application reconnect and platform IP allowlists.

**Finish and restore:** Restore the cable and original priority plan; finish only after checking egress and application. For this platform, see Link Configuration for single-interface/cellular keepalive and Mobile bootstrap rules; verify the interfaces actually participating.

## 1.6 Camera or terminal backhaul

This model does not support PoE. Power the camera and gateway separately to their respective ratings and connect the data path through LAN or a switch. Verify camera addressing and stream first, then uplink capacity and platform viewing.

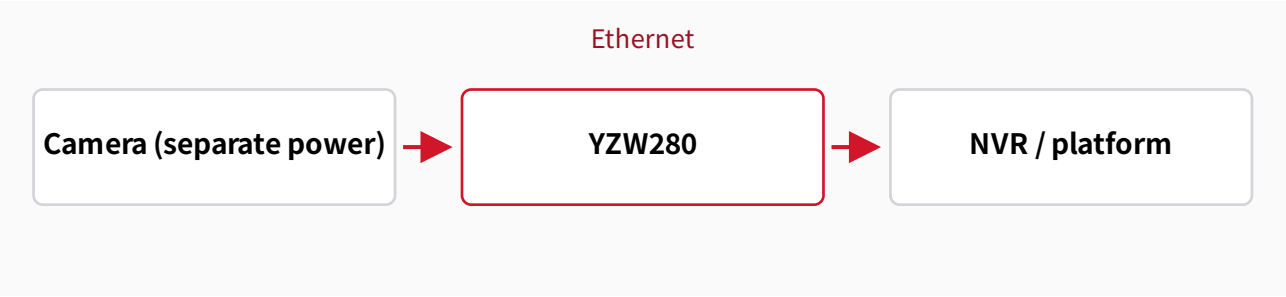



Figure 1-4 Camera or terminal backhaul

### FIELD TASK: PROVE THE LOCAL CAMERA STREAM BEFORE REMOTE VIEWING

Check gateway/camera power against this model’ s instructions; use the PoE chapter only for a model with specified PSE. This case covers network/stream fields.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Camera IP / Mask / Gateway | 192.168.10.30 / 255.255.255.0 / 192.168.10.1 | Set on camera |
| Stream URL / Account | Actual camera RTSP/vendor URL and authorized account | Obtain actual channel URL/credentials from camera management |
| Bitrate | Measure for actual resolution/frame rate | Allow for concurrent streams, overhead and uplink variation |

### SAVE, TEST AND OBSERVE

1. From LAN run ping 192.168.10.30/open its page, then use vendor client or VLC for the actual stream. Observe continuity/bitrate/frame loss.
2. Establish VPN/m2mCloud and routes, then test the same authorized IP stream remotely. Validate cloud device-ID/binding separately.

### PASS CRITERIA AND DIAGNOSIS

No local picture: inspect power/IP/credentials/stream. Remote-only stutter: inspect sustained uplink, concurrency and retransmission. Missing cloud device: inspect binding/platform access.

**Finish and restore:** Close temporary viewers/ports and restore credentials/bitrate/access scope.

## 1.7 Prerequisites and capability boundaries

| BOUNDARY | IMPLEMENTATION REQUIREMENT |
| --- | --- |
| Serial | One owner per physical port; DTU, acquisition and remote serial must not share it concurrently |
| UI | Screenshots use this unit’ s native Chinese/English OEM themes; its current address is not a factory default |
| Validation | Menus, fields, hardware references and relevant implementation checked; no field writes, flow deployment or carrier/RF service acceptance performed |

This model has no GPS, PLC Collect or Node-RED. Only a 2.4 GHz Wi-Fi menu is present. Shell scripting does not imply Python or Node.js. The primary WAN IPv4 selector includes LAN. Retain another local management connection and recheck uplink selection before changing its role.

CHAPTER

02

# Installation

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 2. Interfaces, installation and connections

## 2.1 Interfaces and indicators

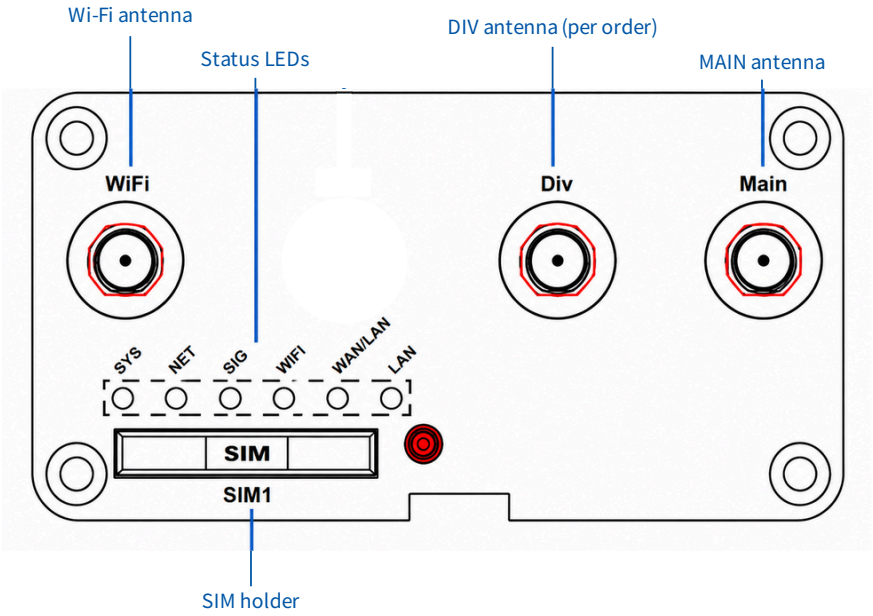



Figure 2-1 Interface panel 1

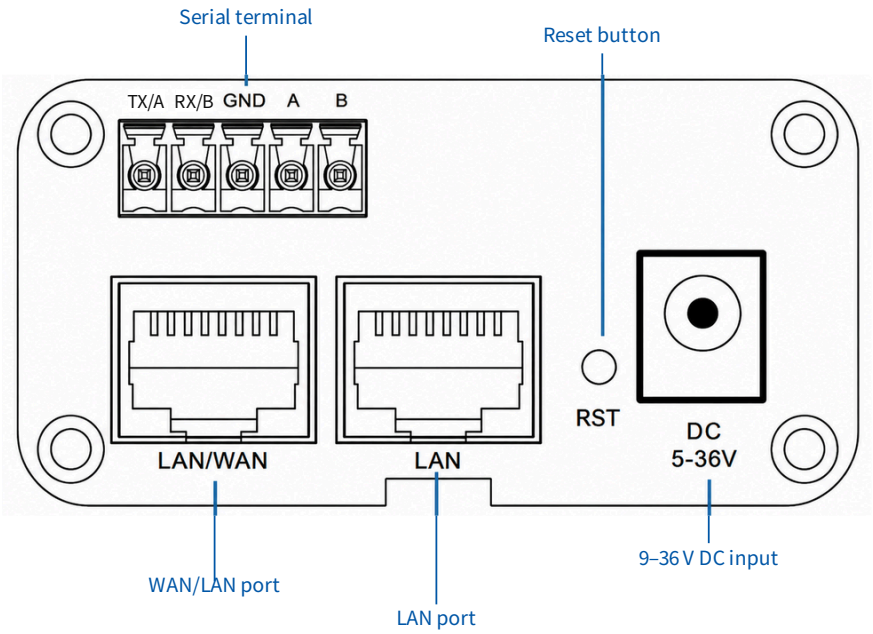



Figure 2-2 Interface panel 2

| INTERFACE | **DESCRIPTION** |
|---|---|
| Ethernet | 2 × Gigabit RJ45; default 1 WAN/LAN + 1 LAN |
| Serial | Standard 2 × RS485; one port can be ordered as RS232 |
| SIM | 1 × pull-out SIM tray, 1.8 / 3 V |
| DC | 9–36 V DC barrel input, nominal 12 V DC |
| LED | SYS, NET, SIG, WIFI, WAN/LAN, LAN |
| Wi-Fi / Cellular | 2.4 GHz / Audited unit: 4G; the datasheet also lists ordered Cat 1 / Cat 4 and 5G RedCap variants; MAIN antenna and ordered DIV antenna |

LEDs assist inspection of power, registration, signal and links. Color/blink indications do not establish service operation; check runtime state and test the service.

### LED STATES AND FIELD DIAGNOSIS

Identify each indicator by its chassis label. Panel, integrated socket and reserved indicators are distinguished; table groups do not add hardware.

This table uses this model’ s inventory, specifications and platform software, not the300L SIG cadence. Software references are distinct from physical acceptance; unconfirmed colors, exact timing or functions are not inferred.

| INDICATOR/GROUP | NORMAL OR REFERENCE STATE | MEANING AND NEXT CHECK |
|---|---|---|
| SYS (system/power) | Normally steady after system startup; do not apply another model’ s RUN blink rule. | If unlit, check supply/wiring, startup and Web access. A lit LED does not prove all applications work. |
| NET (cellular link) | Software reference: blinking during registration/dialing, steady when connected, off when disabled or stopped. | Persistent blink: inspect SIM, registration, APN and session IP. Steady still requires a platform test. |
| SIG (cellular signal) | Corresponding software: CSQ1–10 slow blink,11–20 fast blink,21–31 steady; off without a valid signal value. | These are CSQ ranges, not RSRP dBm thresholds. Signal indication without a steady NET still requires SIM/APN/session checks. |
| WIFI (wireless) | Lights or blinks when the corresponding radio is enabled; a shared LED may encode different band combinations. | Inspect enable, fitted bands, SSID and clients. A lit indicator does not prove a client has an IP or Internet access. |
| WAN/LAN (assigned role) | Link/activity indication follows the actual connected port. | First inspect whether the port is assigned WAN or LAN; light does not identify its role. |
| LAN (link/activity) | On with a detected Ethernet link; blinks with RX/TX traffic. | No light: inspect cable, peer power and role. Light/activity without Web: inspect PC IP/mask and management URL. |

## CHECK IN THIS ORDER AFTER POWER-UP

1. Inspect power/system indication first; check input method, rated range and polarity if unlit.
2. Connect the PC to the actual LAN. If link indication exists but Web fails, check PC IP/mask, management URL, HTTP/HTTPS and port.
3. Inspect the active cellular NET/CEL and SIG, then SIM recognition, registration, session IP and selected SIM/modem in Web.
4. After steady NET, test actual server IP, hostname and application; require application success.

### DIAGNOSE COMMON COMBINATIONS

| OBSERVATION | CHECK IN ORDER |
|---|---|
| SIG indicates signal; NET/CEL keeps blinking or stays off | Signal is not a session. Inspect SIM/subscription/registration/APN/auth/session IP, then egress. |
| NET steady, platform or VPN unreachable | Separate session state from selected egress; inspect DNS/routes/service port/auth/application logs. |
| Ethernet indicates link/activity but PC cannot open Web | Inspect port role, PC subnet/gateway, management protocol/port and proxy before factory reset. |

**Record**: label, observed state, associated SIM/port, Web state and application result. For a discrepancy retain model, photo/short video and status page, then verify hardware and delivery LED definitions.

## 2.2 Main specifications

| ITEM | SPECIFICATION |
|---|---|
| CPU | MT7621AT |
| RAM / Flash | 512 MB DDR3 / 16 MB SPI NOR |
| Ethernet | 2 × Gigabit RJ45; default 1 WAN/LAN + 1 LAN |
| Serial | Standard 2 × RS485; one port can be ordered as RS232 |
| SIM | 1 × pull-out SIM tray, 1.8 / 3 V |
| DC | 9–36 V DC barrel input, nominal 12 V DC |
| Consumption | < 3 W |
| Dimensions | 84.81 × 65.09 × 32.70 mm |
| Weight | 130 g |
| Operating temperature | −30–75 °C |
| Mounting | Metal enclosure; side-mounted DIN rail |
| Operating humidity | < 95 % non-condensing |

The current datasheet gives no IP rating; follow the delivered installation/environment requirements. MAIN and DIV cellular connectors are standard; the DIV antenna follows the order.

> This model does not support PoE. Connect power according to the DC rating above.

## 2.3 Package and antenna connections

Check the YZW280, a power supply matching its input, the ordered cellular/Wi-Fi antennas, Ethernet cable, terminals and mounting accessories. Follow the order packing list and confirm ordered options separately.

This model has no GPS, PLC Collect or Node-RED. Only a 2.4 GHz Wi-Fi menu is present. Shell scripting does not imply Python or Node.js. The primary WAN IPv4 selector includes LAN. Retain another local management connection and recheck uplink selection before changing its role.

## 2.4 Dimensions and mounting position

Enclosure dimensions: 84.81 × 65.09 × 32.70 mm. Reserve space for the illustrated antennas, mounting hardware and cables.

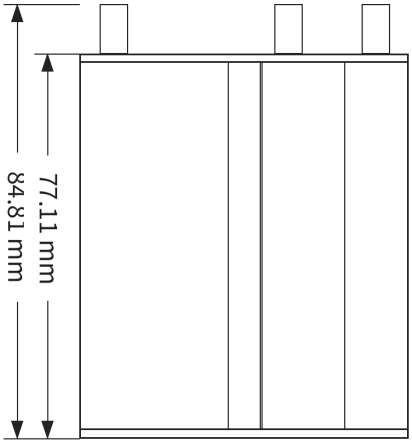



Figure 2-3 Dimension view 1

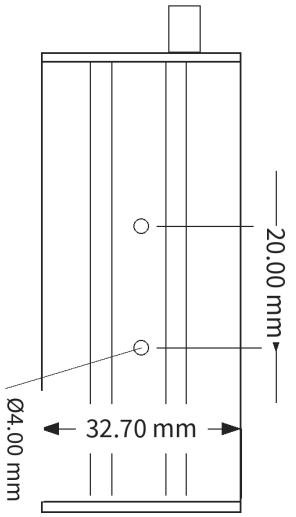



Figure 2-4 Dimension view 2

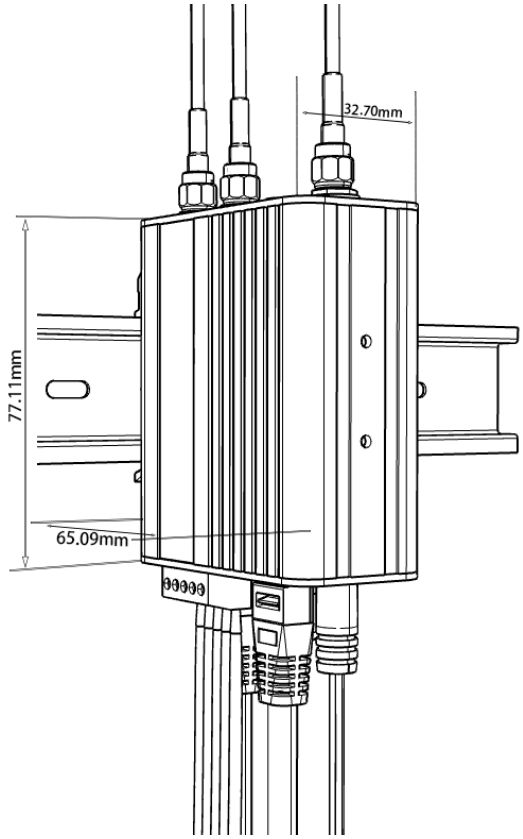



Figure 2-5 Mounting reference

## 2.5 SIM installation and power connection

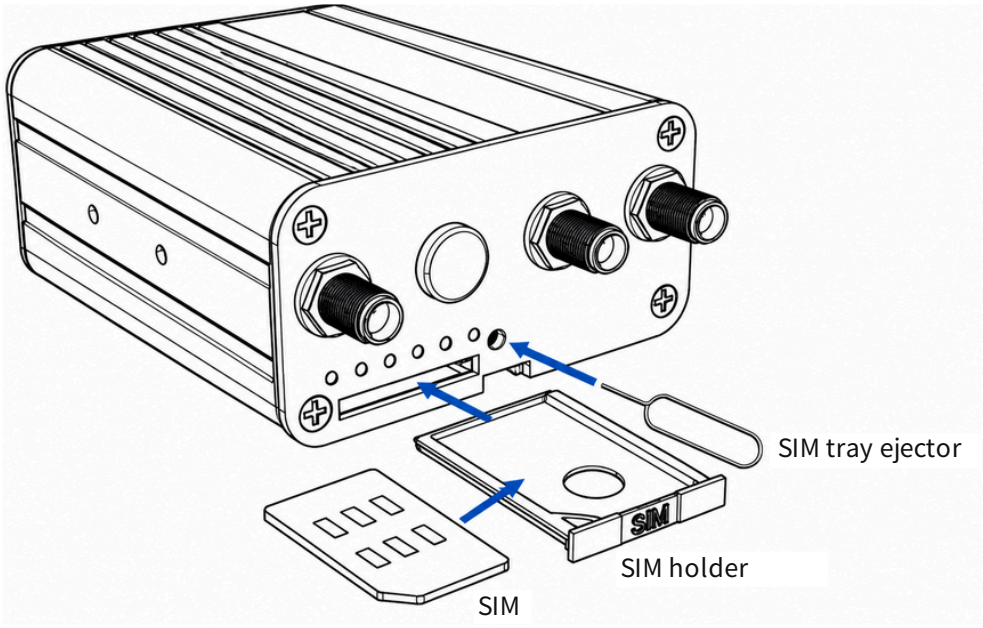



Figure 2-6 SIM installation

1 × pull-out SIM tray, 1.8 / 3 V. Metal enclosure; side-mounted DIN rail

### HOW TO CONFIGURE

1. Disconnect power. Insert the SIM according to enclosure labels and tray orientation; do not hot-swap the tray.

2. Connect cellular antennas to their labeled connectors and Wi-Fi antennas to Wi-Fi connectors; do not interchange them by appearance.
3. Secure the enclosure with its mounting kit and reserve cooling/cable space. Restore covers and connector sealing on outdoor units.
4. Check polarity and input range: 9–36 V DC barrel input, nominal 12 V DC. Connect the LAN PC, then apply power.
5. After boot, inspect SIM recognition, registration and addressing in Web. SIM detection does not establish a data connection.

**Check the result** Starts on the correct supply/wiring and is reachable over LAN

## 2.6 Serial wiring and service ownership

Pins from left to right: TX/A, RX/B, GND, A, B. In the standard dual-RS485 build, the left pair is the first A/B and the right pair the second. An ordered RS232 build uses TX/RX/GND on the left. Confirm the delivered electrical variant before wiring.

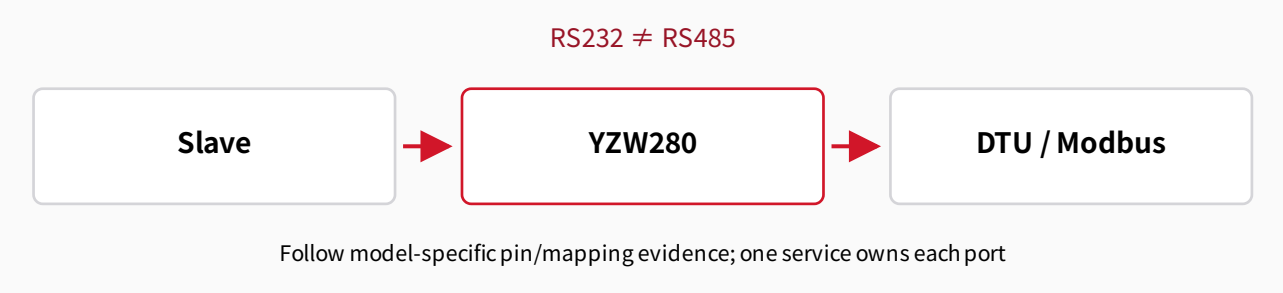



Figure 2-7 Serial wiring and service ownership

### HOW TO CONFIGURE

1. Wire with power disconnected and confirm RS232/RS485 electrical type and pin labels.
2. Match baud, parity, data and stop bits to the slave; Modbus RTU uses 8 data bits.
3. Use one service to read one known read-only point repeatedly before adding reporting.
4. If silent, check wiring and logical mapping, then slave/address/ownership; do not start with control writes.

**Check the result** Physical wiring, logical mapping and electrical type agree; one known point reads repeatedly

CHAPTER

# 03

# Getting started

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 3. Basic operation and status

## 3.1 PC connection and Web login

Path Web Login

Use a wired LAN connection for initial setup. Configure the PC address before signing in. For a deployed router, use the current management address supplied by its administrator.

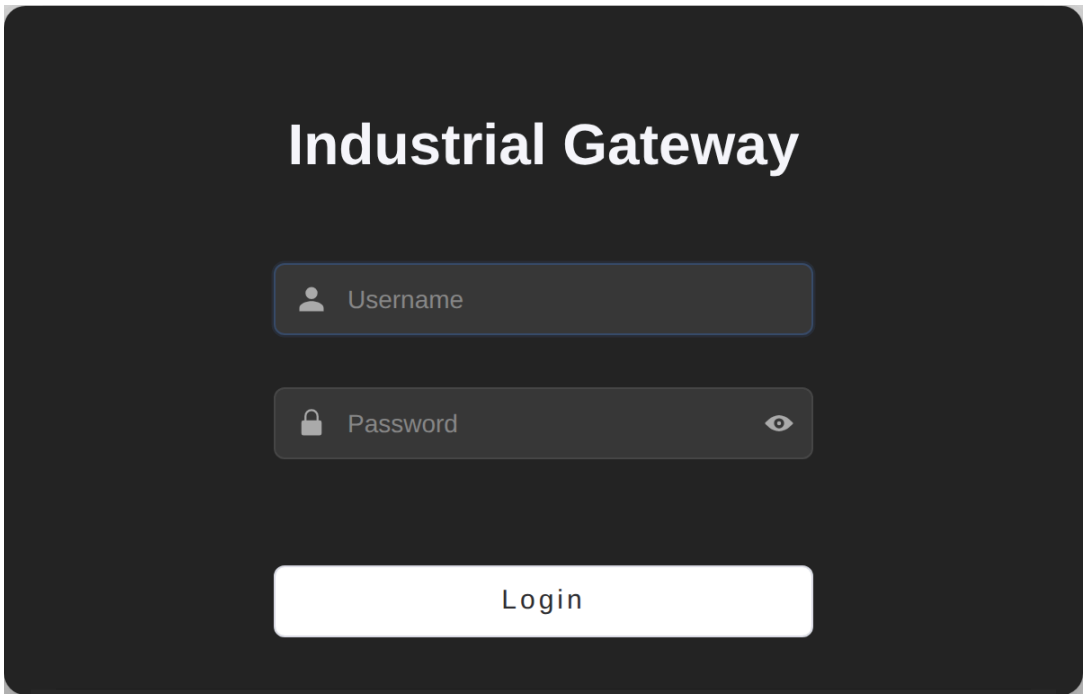



Figure 3-1 Web login

### FIELD TASK: FIRST CONNECTION: MATCH THE PC TO THE DEVICE DEFAULT SUBNET

Distinguish defaults from configured units.192.168.8.1 below is for defaults; bench188 addresses are not factory defaults. For configured units use the handover record.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Cable | PC to actual LAN | Temporarily remove conflicting PC adapters/proxies |
| PC IPv4 / Mask | 192.168.8.10 / 255.255.255.0 | Static access example; verify unused |
| URL / Account | http://192.168.8.1/ / admin | Initial password admin only at defaults |

### SAVE, TEST AND OBSERVE

1. Run ipconfig to verify Ethernet IP, ping192.168.8.1 and enter the full URL in the browser address bar.
2. Change the password and verify a new login. To reproduce the lab, then change LAN to 192.168.10.1/24 using the LAN section.

### PASS CRITERIA AND DIAGNOSIS

No link: inspect cable/power/port role. Ping fails: inspect subnet/conflicts. Ping works but Web fails: inspect protocol/port/proxy. Wrong password: check prior changes.

**Finish and restore:** Restore PC IP/DNS/adapters and securely retain new management settings.

### DEFAULT ACCESS SETTINGS

| ITEM | DEFAULT |
| --- | --- |
| LAN address / mask | 192.168.8.1 / 255.255.255.0 (/24) |
| Address assignment | LAN DHCP is enabled; the PC can obtain its address automatically |
| Web address | http://192.168.8.1/ (HTTP, port 80) |
| Username / initial password | admin / admin |

Use the delivered access settings if different defaults were specified, or the current settings if the router has already been configured.

### METHOD 1: OBTAIN A PC ADDRESS AUTOMATICALLY

1. Connect the PC to an RJ45 port currently assigned to LAN and check the link indicator.
2. Press Win+R, enter `ncpa.cpl` and open Properties for the connected Ethernet adapter.
3. Open Internet Protocol Version 4 (TCP/IPv4) Properties and select automatic IP and DNS assignment.
4. Check that the acquired address is in the router LAN subnet; the default subnet is 192.168.8.x/24.

### METHOD 2: ASSIGN A PC ADDRESS MANUALLY

1. In the same IPv4 window, select Use the following IP address.
2. With the default LAN settings, an example PC address is `192.168.8.10`, mask `255.255.255.0`. The address must be free; do not assign the router's `.1` address to the PC.
3. If Windows asks for a prefix length, enter `24`. When Internet access through the router is required, use the site gateway and DNS settings; with the default plan these can be `192.168.8.1`.
4. If the LAN address was changed, use its current subnet rather than copying this example.

### OPEN THE BROWSER AND SIGN IN

1. Enter the complete `http://192.168.8.1/` in the address bar, rather than a search box. For a configured router, enter its current address.
2. Enter `admin` in Username and the initial or changed password in Password, then select Login.

3. After Overview opens, check the link and change the admin password under System Management > Account. See “admin password management”.

> Check the result: Overview opens and the PC address matches the LAN subnet. If access fails, check cabling, port role and addressing before checking the management protocol and port.

### MANAGEMENT SECURITY AT FIRST DEPLOYMENT

> **Check the result** Overview opens and the new password works after a password change

## 3.2 Web interface layout

Path Overview

Inspect port state at the top, select a function on the left and configure it on the right. This is the current menu on this model. Configuration submission, runtime state and service validation are separate steps.

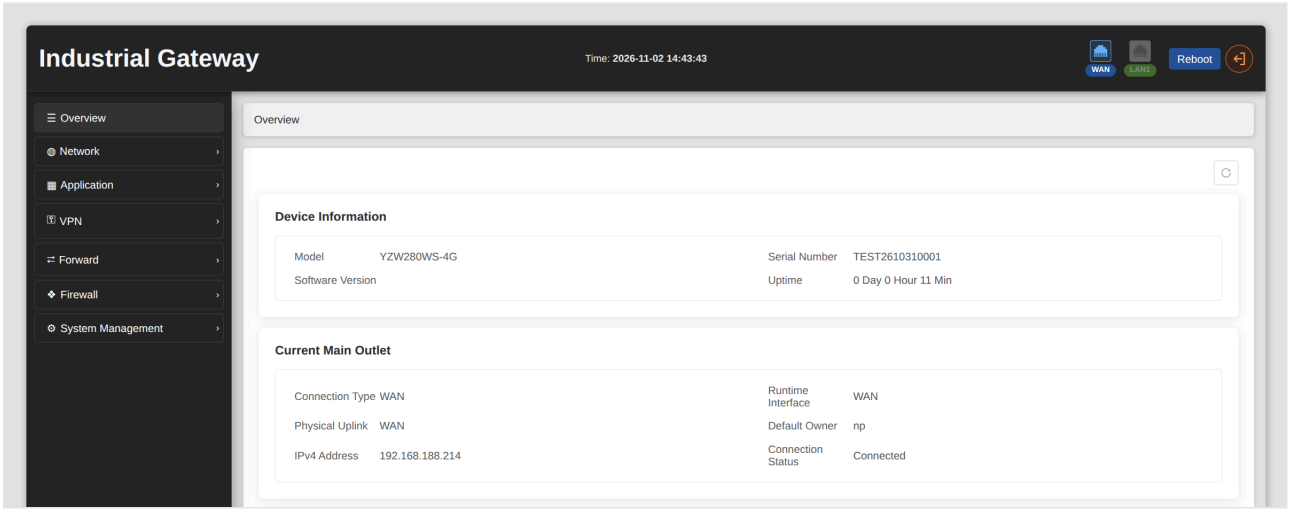



Figure 3-2 Web menu and complete upper overview cards

Firmware identifier omitted

> **Check the result** The actual menu and intended configuration object are identified before saving

# 3.3 Device, uplink and client status

Path Overview

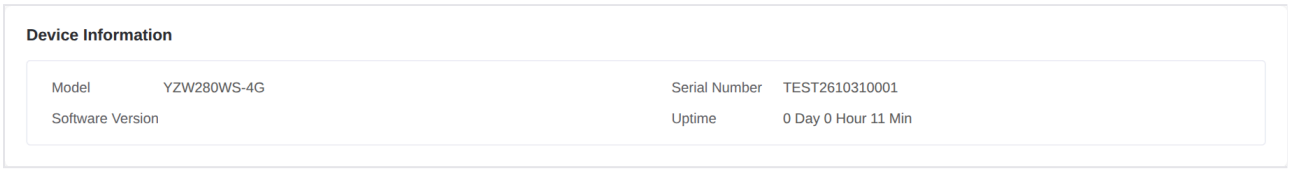



Figure 3-3 Device, uplink and client status

Firmware identifier omitted

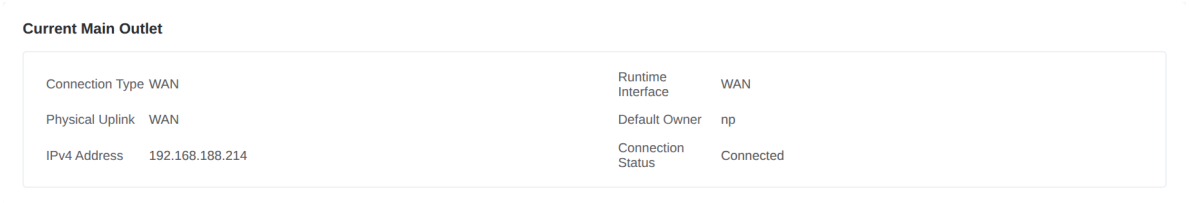



Figure 3-4 Device, uplink and client status

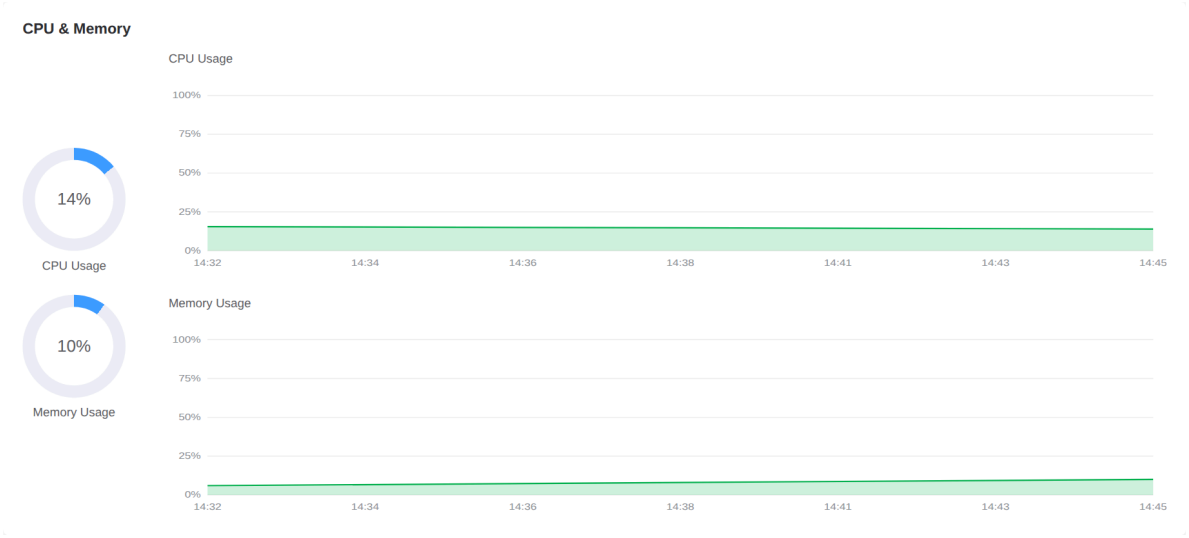



Figure 3-5 CPU and memory runtime status

## FIELD TASK: SEPARATE LINK, ADDRESS AND APPLICATION STATUS

Configure uplink and prepare an actual platform/site-service test. Reference screenshot values are not factory parameters.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Device / Uptime / Performance | record actual values | Observe CPU/memory over time; unavailable “-” is not zero |
| Link / Current / Clients | actual IPs, egress and clients | Correlate clients by real MAC/IP |

## SAVE, TEST AND OBSERVE

1. Record system uptime, WAN/cellular IP, current egress and PC lease; then open the actual application from the PC.
2. Distinguish system/session/virtual-interface uptime where provided and observe refresh changes rather than diagnosing from one screenshot.

## PASS CRITERIA AND DIAGNOSIS

IP without application: use Network Tools. High CPU: correlate with points/flows/connections. Missing client: inspect access port and lease.

**Finish and restore:** Restore temporarily stopped services and record the normal baseline.

| AREA | WHAT TO INSPECT |
|---|---|
| Device information | Model, software version and uptime; firmware must match model/storage |
| Current uplink | Check IPv4/IPv6 interface, address, gateway and DNS separately; an addressed backup need not be active |
| Cellular | Check SIM, modem, registration and data state; IMEI/ICCID are outside the illustrated overview cards |
| Routes and clients | Web access alone does not establish Internet, VPN or MQTT reachability; verify each required service |

## REFRESHED STATUS AND CONNECTION DURATION

The homepage periodically refreshes CPU/memory samples. A failed read can show a dash or Status unavailable; a previous sample is not a current health result. System uptime, PPPoE session duration and VPN online duration describe different lifetimes. Reconnection or recreation of the relevant interface restarts its connection age; one failed status read alone does not prove application failure.

> **Check the result** Current firmware, addressing and links match the delivery and site plan

CHAPTER

# 04

# Network settings

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 4. Network settings

## 4.1 WAN settings

Path Network > WAN

2 × Gigabit RJ45; default 1 WAN/LAN + 1 LAN

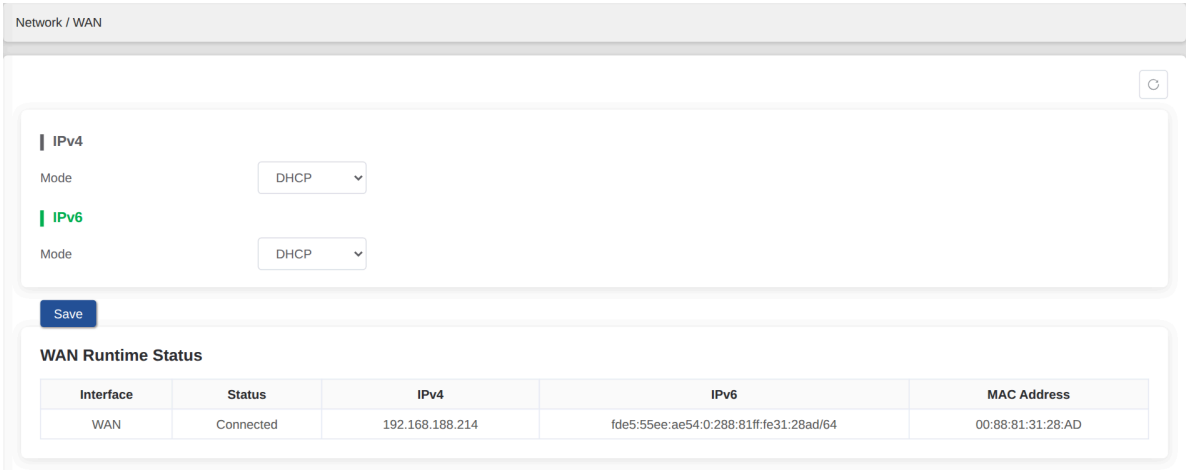



Figure 4-1 WAN settings

### FIELD TASK: ESTABLISH A STATIC WIRED UPLINK FIRST

The upstream router is 192.168.20.1/24 with Internet and DNS; gateway LAN is 192.168.10.1/24, WAN connects to upstream LAN. An upstream test PC is 192.168.20.10/24. These are isolated lab values, not ISP-assigned addresses.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode | Static | Select the actual WAN |
| IP Address | 192.168.20.2 | Check for conflicts |
| Subnet Mask | 255.255.255.0 | /24 |
| Gateway / DNS1 | 192.168.20.1 / 192.168.20.1 | Upstream must provide routing and DNS |

### SAVE, TEST AND OBSERVE

1. Save the table. Inspect WAN address/gateway on Home. In Network Tools ping 192.168.20.1, test the project server IP, then resolve its hostname.
2. If upstream uses DHCP, select DHCP and save; do not retain the table’ s static address. For PPPoE obtain ISP credentials, enter PPPoE Username/Password, keep negotiated options, save and inspect the session IP and duration.

## PASS CRITERIA AND DIAGNOSIS

Pass upstream gateway, server IP, hostname and application tests in that order. Link LEDs or an assigned IP alone do not prove Internet access.

Overlapping WAN/LAN subnets: change LAN first. PPPoE auth failure: check ISP credentials and stale sessions; the Web admin password is unrelated.

**Finish and restore:** Restore the recorded mode/settings. Before assigning the port to LAN, retain local management through another LAN connection.

| PURPOSE | IPV4 MODE | WHAT TO CONFIGURE |
|---|---|---|
| Upstream assigns addressing | DHCP | After saving, check the leased address, gateway and DNS |
| Assigned static addressing | Static | Set address, mask, gateway and DNS without overlapping the LAN |
| Broadband dial-up | PPPoE | Use ISP credentials and the required advanced PPP settings |
| Join this port to LAN | LAN | Retain management access first; this port ceases to be a separate WAN uplink |

Selecting LAN for IPv4 also assigns the port's IPv6 side to LAN. After changing IPv4 back to DHCP, Static or PPPoE, recheck IPv6 addressing. IPv4 uplink and IPv6 LAN are not independent physical-port roles.

When IPv4 and IPv6 both use PPPoE, they share one PPPoE session and the IPv4 dial-up credentials. They are not two independent broadband sessions. Connection duration follows the current PPPoE session and restarts after reconnection.

This two-port model defaults to 1 WAN/LAN plus 1 LAN. Connect the PC to the other LAN before changing the primary WAN to LAN. Do not apply a five-port 4-WAN layout.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | WAN interface / tab | Select an actual interface tab and match physical wiring; do not infer port count from another model |
| 2 | Mode | Choose DHCP, Static or PPPoE for uplink, or LAN to join the LAN; recheck the port role and IPv6 together. |
| 3 | IP Address / Subnet Mask | For Static mode, use the assigned address and mask without conflicting with LAN or other site subnets |
| 4 | Gateway | Use the upstream next hop for this WAN, not the router LAN address |
| 5 | DNS1 / DNS2 | DNS resolvers. Check them when IP access works but names fail |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 6 | PPPoE Username / Password | Use ISP-provided broadband credentials, not the router Web account |
| 7 | Authentication / Compression | Match advanced PPP authentication and compression to the provider |
| 8 | MTU / MRU / MSS | Control transmit, receive and TCP segment sizes; use provider or network requirements |
| 9 | IPv6 | Configure addressing, prefix, gateway and DNS separately; the upstream must support the selected IPv6 access |
| 10 | Runtime | After saving, check runtime addressing/link state; submission alone does not establish service reachability |
| 11 | LAN port role | Selecting IPv4 LAN joins the port to LAN and also sets its IPv6 role to LAN. Recheck IPv6 acquisition when restoring uplink use. |
| 12 | PPPoE dual stack and duration | Dual-stack PPPoE shares the session and IPv4 credentials; duration is the current session age, not system uptime. |

**Check the result** Assigned addressing, gateway, external IP, DNS and a LAN client service are checked separately

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Address acquired but no Internet access | Check the upstream gateway and default route. Test an external IP and then a domain; check DNS if only the domain fails. |

# 4.2 LAN settings

Path Network > LAN

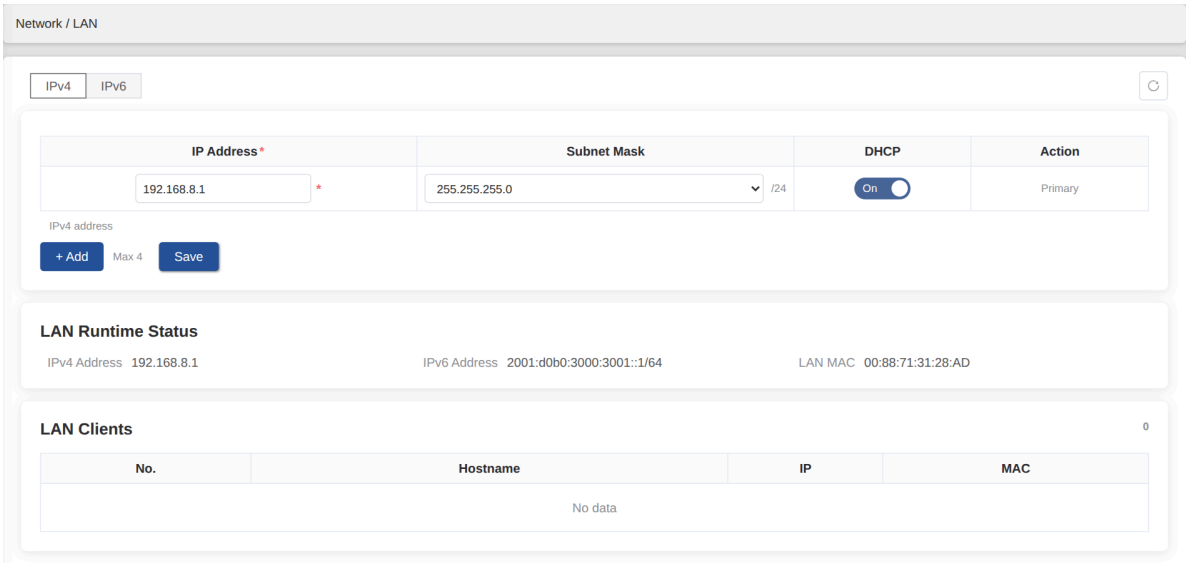



Figure 4-2 LAN settings

## FIELD TASK: MOVE THE SITE LAN TO 192.168.10.0/24

Connect a PC directly to LAN and export a configuration backup. The 10 subnet is a lab plan. Check that it differs from the uplink subnet; if already occupied, replace it consistently throughout the cases.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| IP Address | 192.168.10.1 | Primary LAN IPv4 address |
| Subnet Mask | 255.255.255.0 | Prefix 24; this is not the uplink gateway |

## SAVE, TEST AND OBSERVE

1. Keep the local cable attached. Change the primary LAN address/mask and save. A disconnected browser is expected; do not factory-reset for this reason.
2. Set the PC manually to 192.168.10.10/24, gateway 192.168.10.1. Sign in at http://192.168.10.1/ and configure the dynamic pool in DHCP.
3. Run ipconfig and ping 192.168.10.1 on Windows, then open the new management page. Update static PLC/camera addresses, NAT targets, VPN local subnets and saved management URLs.

## PASS CRITERIA AND DIAGNOSIS

Pass only when the page opens and the PC is 192.168.10.10/24. Ping works but Web fails: check HTTP/HTTPS and the management port.

PC remains on the old subnet: use static 192.168.10.10/24 to separate lease issues, then repair DHCP; verify that the cable is in a LAN port.

**Finish and restore:** To revert, restore the old LAN address/mask through the new page, move the PC back, and restore related rules from the recorded plan.

After changing the LAN address or mask, reconnect at the new management address and renew the test client lease. Check DHCP gateway, DNS and pool as well; a successful save does not mean clients have moved to the new subnet.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | IPv4 / IPv6 | Maintain LAN addresses for each protocol; do not mix IPv4 masks with IPv6 prefix lengths |
| 2 | IP Address | LAN management address. Reconnect at the new address after changing the primary address |
| 3 | Subnet Mask | Defines the IPv4 LAN subnet; coordinate it with WAN and other interfaces |
| 4 | Primary | Main LAN management address; secondary addresses do not replace its correct planning |
| 5 | Add / Delete | Maintain addresses within firmware limits; removal affects clients using that subnet |
| 6 | Prefix | Defines the IPv6 subnet; also check prefix requirements for DHCP operation |
| 7 | DHCP | Enables assignment for the subnet; maintain pools and related settings on the DHCP page |
| 8 | Runtime / Clients | Shows active addresses and clients; the client list is not a permanent equipment inventory |

**Check the result** The PC obtains the intended addressing and can sign in at the new management IP

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Management access lost after saving | Reconnect to the new LAN address, update the PC address or DHCP lease, and check that the port is still assigned to LAN. |

# 4.3 VLAN settings

Path Network > VLAN

VLANs segment Layer-2 networks by tags. Configure advanced interface settings when a VLAN needs an IP and DHCP. Plan membership and switch tagging first.

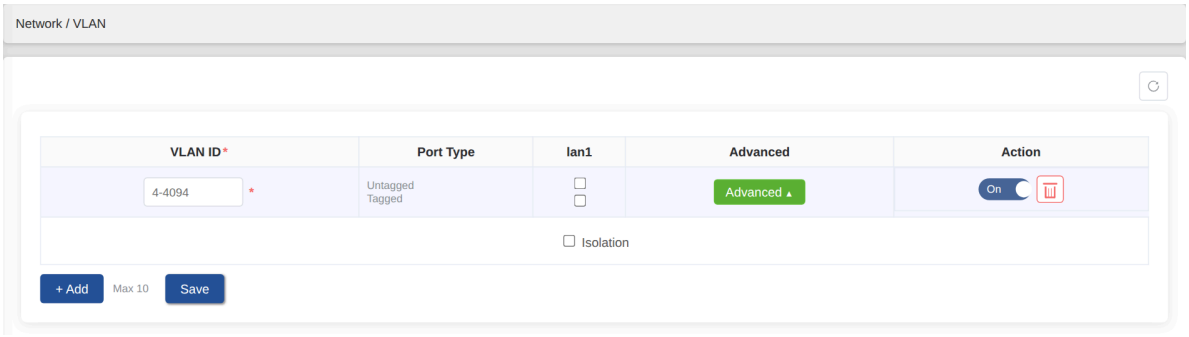



Figure 4-3 VLAN settings

Native unsaved form / browser draft; not applied to device

### FIELD TASK: PLACE ONE GROUP OF CLIENTS IN VLAN 10

Use a managed switch. Its gateway uplink retains untagged management traffic and allows tagged VLAN10; client ports are access/PVID10. Retain a separate local management connection.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| VLAN ID | 10 | Must match the switch |
| Port Type / Members | tagged uplink | Do not remove every management port |
| Advanced IP / Prefix | 192.168.40.1 / 24 | Separate L3 VLAN interface in this case |
| DHCP / Pool / Gateway | On / 192.168.40.100–199 / 192.168.40.1 | Use a genuinely reachable DNS service |

### SAVE, TEST AND OBSERVE

1. Configure the switch while retaining management, add VLAN10 and its L3/DHCP settings, then save. Connect a client to its access port and renew the lease.
2. Expect a 40-subnet address and access to 192.168.40.1 and the application. The management PC should still reach .10.1.

### PASS CRITERIA AND DIAGNOSIS

No lease: inspect tags, access/PVID and membership. VLAN grouping alone does not guarantee L3 isolation; configure firewall policy and test both allowed and denied traffic.

**Finish and restore:** Move the client back before deleting the VLAN/DHCP and switch VLAN10 settings.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | VLAN ID | Up to 10 configurations, VID 4–4094; match the tagging plan at both ends |
| 2 | Port Type | Tagged carries VLAN tags, typically on uplinks; Untagged serves untagged endpoints |
| 3 | Port Members | Select actual member ports after checking their current WAN/LAN roles |
| 4 | Advanced / Interface | Enable and address a Layer-3 interface when routing is needed; a Layer-2 VLAN only segments Ethernet |
| 5 | IP / Prefix | Address and prefix of the routed VLAN interface; avoid conflicts with existing interfaces |
| 6 | DHCP / Pool / Gateway / DNS | Address assignment for VLAN clients; all values must match the VLAN subnet |
| 7 | Lease Time | Lease lifetime in seconds; choose for the client population and address turnover |

**Check the result** Required same-VLAN services work, inter-VLAN access matches the plan and management remains reachable

# 4.4 Wi-Fi settings

Path Network > WIFI2.4G

Currently exposes 2.4 GHz IEEE 802.11b/g/n. Do not borrow another model’ s 5 GHz provision or 5G/Wi-Fi exclusion rule

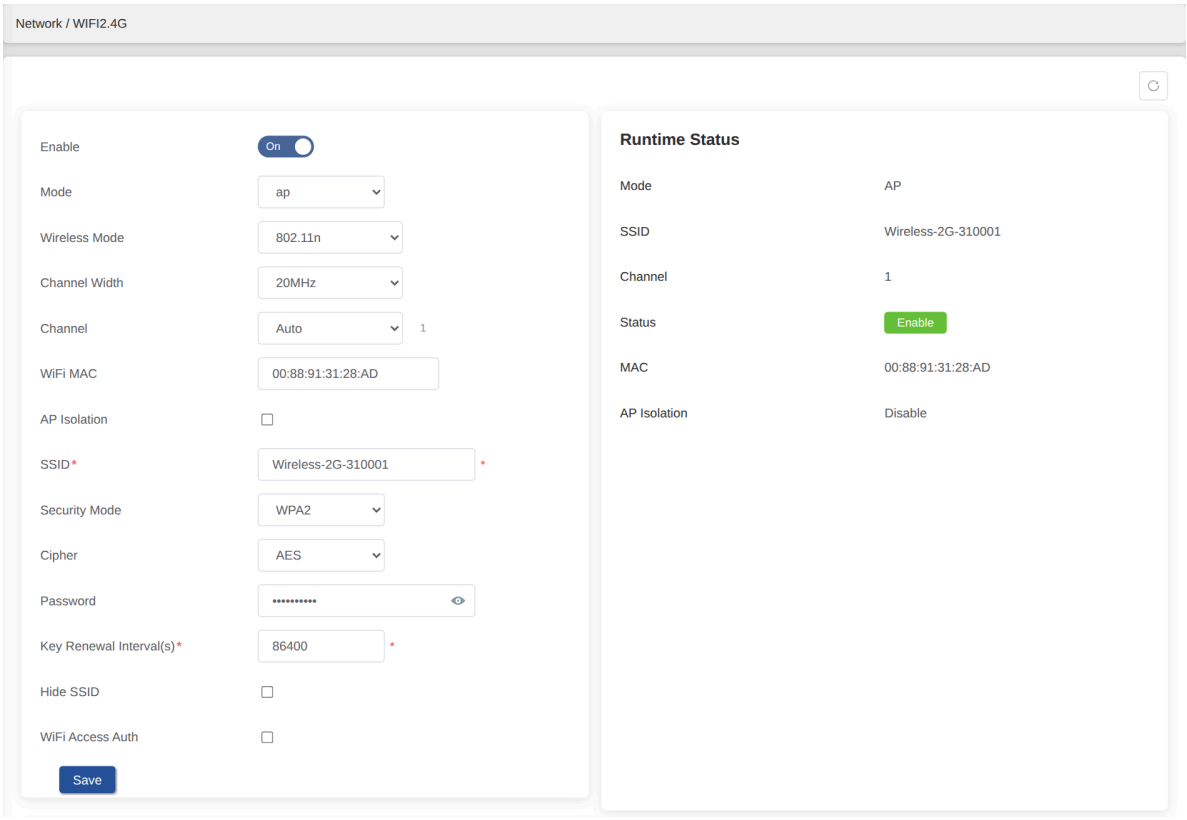



Figure 4-4 Wi-Fi settings (1/2)

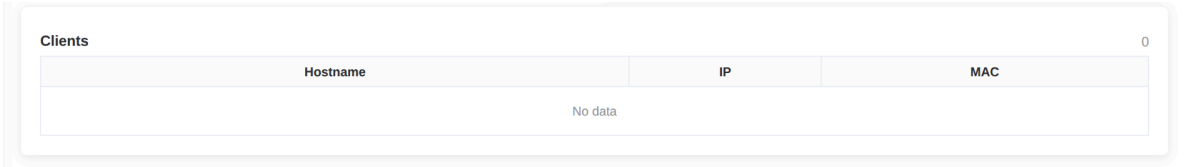



Figure 4-5 Wi-Fi settings (2/2)

## FIELD TASK: CONNECT A PHONE TO AP OR USE WI-FI AS AN UPLINK

Test AP and Station as separate uses. Retain wired LAN management. Simultaneous roles depend on the delivered radio and page.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| AP Mode / SSID | AP / FieldLab | Phone joins site LAN |
| Security / Password | WPA2-PSK / LabWifi2026 | Lab-only password; replace on site |

| UI FIELD | ENTRY | BASIS |
| --- | --- | --- |
| Station Mode / SSID | Station / actual upstream SSID | Obtain the exact upstream SSID/password from its administrator |
| Channel / Bandwidth | Auto / keep current | Avoid locking an unverified channel initially |

### SAVE, TEST AND OBSERVE

1. AP test: enable the fitted band, set FieldLab/password and save. Disable phone mobile data, join the SSID, verify a 10-subnet IP and open http://192.168.10.1/.
2. Station test: enter the actual upstream SSID, security mode and password, save and inspect association/uplink IP. Select an available wireless combination in Link Configuration and test the service. MT7621 SSIDs are limited to 32 UTF-8 bytes.

### PASS CRITERIA AND DIAGNOSIS

SSID absent: inspect band, enable and hidden settings. Joined without IP: inspect DHCP. Station associated without service: inspect uplink IP, priority and subnet overlap.

**Finish and restore:** Use wired LAN to restore the radio role, SSID and security settings; disconnect test clients and replace the lab password.

### STATION UPLINK AND SSID LENGTH

AP provides local wireless access; Station connects to an upstream AP. A Station SSID is at most 32 UTF-8 bytes. Non-ASCII characters can occupy several bytes, so this is not a 32-character guarantee. BSSID describes the AP actually associated and does not replace the target SSID.

After saving Station settings, verify association, addressing and DNS before selecting its available Link Configuration combination.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
| --- | --- | --- |
| 1 | Band / Enable | Currently exposes 2.4 GHz IEEE 802.11b/g/n. Do not borrow another model’ s 5 GHz provision or 5G/Wi-Fi exclusion rule |
| 2 | Mode | AP serves wireless clients; Station connects upstream. Use modes available on the selected radio |
| 3 | SSID | Local network name in AP mode; upstream network name in Station mode |
| 4 | Channel / Bandwidth | Coordinate with radio conditions and regional settings; bandwidth selection is not a throughput guarantee |
| 5 | Security / Password | Match the authentication settings of clients or the upstream AP |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 6 | AP Isolation / Hide SSID | Control client-to-client access and SSID broadcast; hiding the name does not replace authentication |
| 7 | Station List / Scan | When configuring Station access, select the intended upstream network and its credentials |
| 8 | Station SSID length | At most 32 UTF-8 bytes; match the complete upstream SSID, including spaces and case. |

**Check the result** The client joins the intended SSID, obtains expected addressing and reaches its service

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| SSID connected but no Internet | Check the client address, gateway and LAN before the uplink; changing the Wi-Fi password alone will not resolve an upstream problem. |

## 4.5 Cellular settings

Path Network > Mobile

This section applies to equipped cellular variants. Install SIM and matching antennas before dial configuration. The modem determines available network types/bands; do not borrow options from another model.

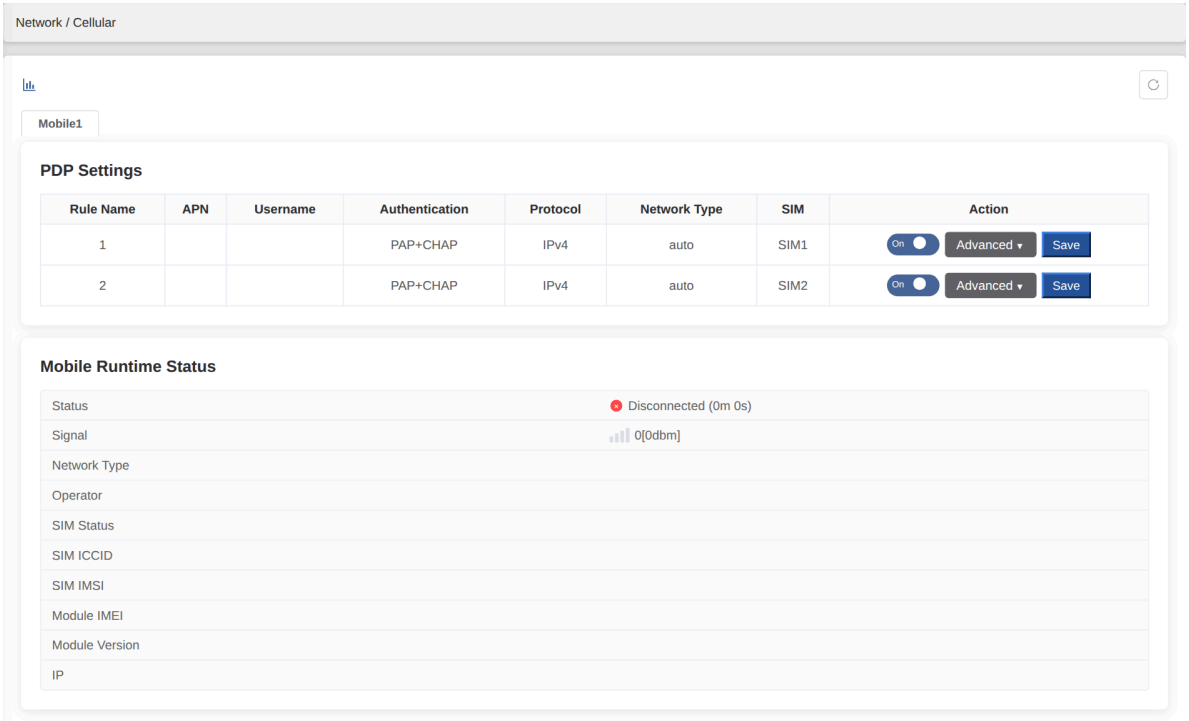



Figure 4-6 Cellular settings

### FIELD TASK: RESOLVE A RECOGNIZED SIM THAT CANNOT REACH THE NETWORK

Use an activated data SIM with matching bands and no billing restriction. Install with power disconnected and attach the model’ s cellular antennas. Obtain APN, credentials if any, auth mode, PIN and private-network reachability from the carrier.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable | enabled | Use an actually fitted modem |
| APN | carrier APN | Copy the exact spelling |
| Username / Password / Authentication | carrier handover | Leave blank only when the carrier specifies no authentication; not Web admin |
| PIN | follow SIM state | Blank if PIN is disabled; verify before retrying |
| Protocol / Network Type | per subscription and coverage | Start with automatic network selection; follow carrier IP-family requirements |

### SAVE, TEST AND OBSERVE

1. Record ICCID/SIM state. If absent, power down, reseat and check SIM format. If recognized, inspect registration, signal and carrier; after registration inspect session IP, DNS and current egress.
2. Save carrier settings and wait for registration/session updates. In Applications > Network Tools, enter the gateway cellular interface current local IP in Source IP; if left blank, test using and verify the default-route egress, test the project server IP and DNS, then open the platform from a LAN client.

### PASS CRITERIA AND DIAGNOSIS

Require SIM recognition, registration, a session IP and the actual platform connection; signal strength does not prove a usable data session.

Registered without IP: check APN, billing and private-APN authorization. IP works but names fail: check DNS. Gateway Internet works but clients fail: inspect LAN gateway/routes.

**Finish and restore:** Restore the APN/network mode and remove experimental band/cell locks. Retain the original configuration and timestamped logs for the carrier.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | APN | Use the public/private APN provided for the SIM, not a universal value copied from another carrier |
| 2 | Username / Password / PIN | Fill only as required by the SIM provider; PIN is the SIM lock code, not the Web password |
| 3 | Authentication | Match NONE, PAP, CHAP or PAP+CHAP to the APN authentication requirements |
| 4 | Protocol | Choose IPv4, IPv6 or IPv4v6 as supported by the modem and carrier |
| 5 | Network Type | AUTO chooses an available network; fixed types must be supported by the installed modem |
| 6 | SIM / Enable | Select the tray for the profile and check SIM availability and profile enable state separately |
| 7 | Band / Cell Lock | Use only with a defined radio plan; an incorrect restriction can prevent registration |
| 8 | Runtime Status | Inspect registration, signal, SIM, IP, gateway and DNS. SIM detection does not prove a data connection |

**Check the result** Registration and a data connection succeed; an address is assigned and external IP/DNS tests pass

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| SIM detected but connection fails | Check SIM service, APN, authentication and antennas, then inspect connection status and logs. |

# 4.6 DHCP service

Path Network > DHCP

DHCP assigns addresses to wired and wireless clients. Pools must belong to their LAN subnet and coordinate with static assignments; adding a conflicting DHCP server does not solve address planning.

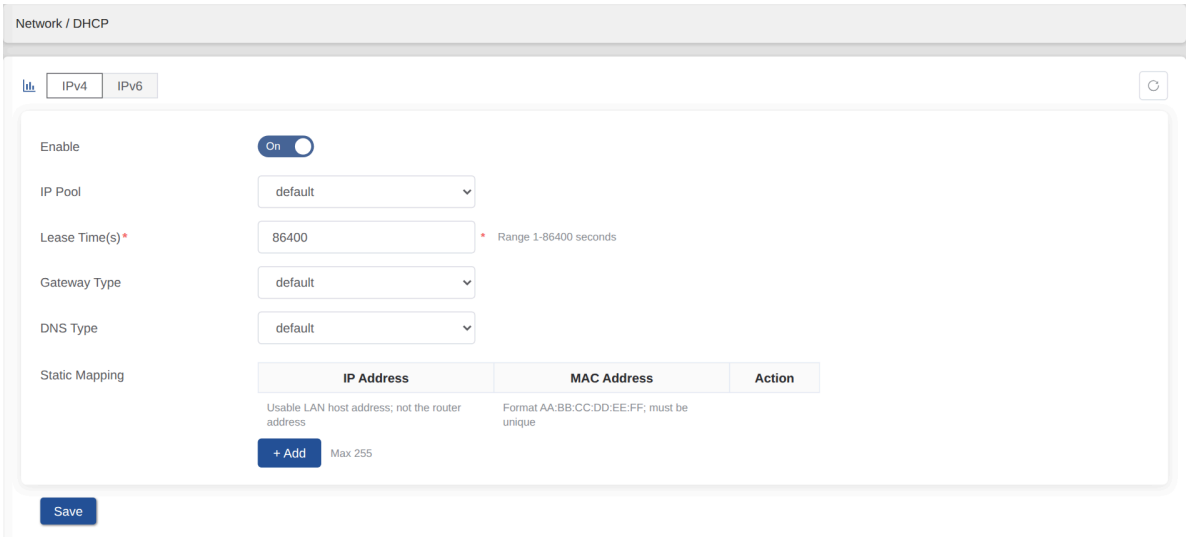



Figure 4-7 DHCP service

## FIELD TASK: LEASE ADDRESSES AUTOMATICALLY AND RESERVE A PLC ADDRESS

First set LAN to 192.168.10.1/24. Keep the test PC static at .10 and test leases with another client. Static PLC .20 and camera .30 stay outside the pool.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Pool Start / End | 192.168.10.100 / 192.168.10.199 | Dynamic pool |
| Gateway | 192.168.10.1 | LAN gateway |
| DNS1 | 192.168.10.1 | Requires working gateway DNS forwarding; repair uplink DNS first |
| Lease Time | keep current value | Record the displayed unit; do not mix seconds and minutes |

## SAVE, TEST AND OBSERVE

1. Enable DHCP, enter the table and save. Set the client to automatic IPv4/DNS. On Windows run ipconfig /release, ipconfig /renew and ipconfig /all.
2. For a reservation, copy the actual PLC MAC from Clients, add binding 192.168.10.20, switch the PLC to DHCP and renew. A PLC using a static address does not need a duplicate reservation.

## PASS CRITERIA AND DIAGNOSIS

Expect .100–.199/24, gateway .1 and DNS .1; test Web and the actual uplink service. 169.254.x.x indicates no lease.

Unexpected gateway/subnet: inspect a second DHCP server on LAN. Renew after a LAN change; saving alone does not clear old leases.

**Finish and restore:** Remove the new reservation or restore the pool after checking static-address conflicts.

## ADDRESS ASSIGNMENT AFTER A LAN SUBNET CHANGE

The DHCP service regenerates its configuration for the actual LAN IPv4 address and mask. Automatic pools follow that subnet; check custom pools, reservations and manually assigned client addresses yourself. Renew the client lease after the LAN change and verify address, mask, gateway and DNS rather than validating against an old lease.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Pool Start / End | Keep the pool within its LAN subnet and exclude gateway and occupied static addresses |
| 2 | Gateway | Default gateway delivered to clients; it need not be the DHCP server address |
| 3 | DNS1 / DNS2 | DNS resolver addresses sent to clients; check the resulting client configuration |
| 4 | Lease Time | Client address lease lifetime in seconds |
| 5 | Static Binding | Reserve an address by MAC; the client may need to renew or wait for its current lease |
| 6 | Clients | Check assigned addresses; a successful lease does not verify upstream reachability |

**Check the result** A new client receives an in-pool address, intended gateway and DNS without an address conflict

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| The PC receives another gateway | Check for another DHCP server, then the LAN/VLAN membership and address pool. |

# 4.7 Link Configuration and failover

Path Network > Link Configuration

Configure failover and keepalive for the selected uplinks, actual interface count and address families. Configure interface addressing before selecting the combination here.

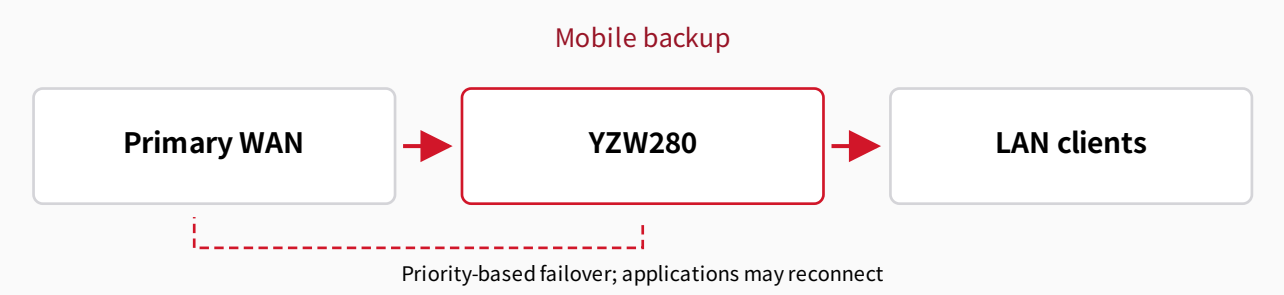



Figure 4-8 Link Configuration and failover

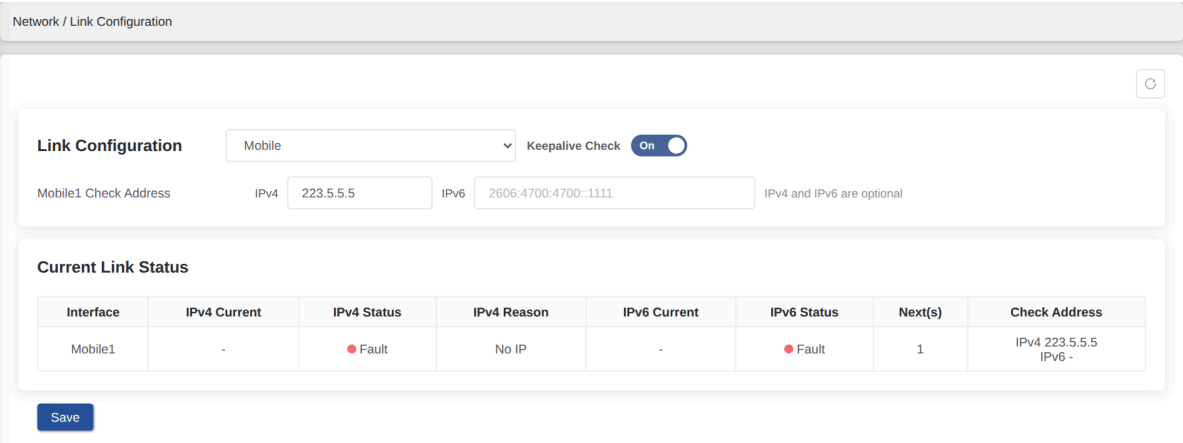



Figure 4-9 Link Configuration and failover

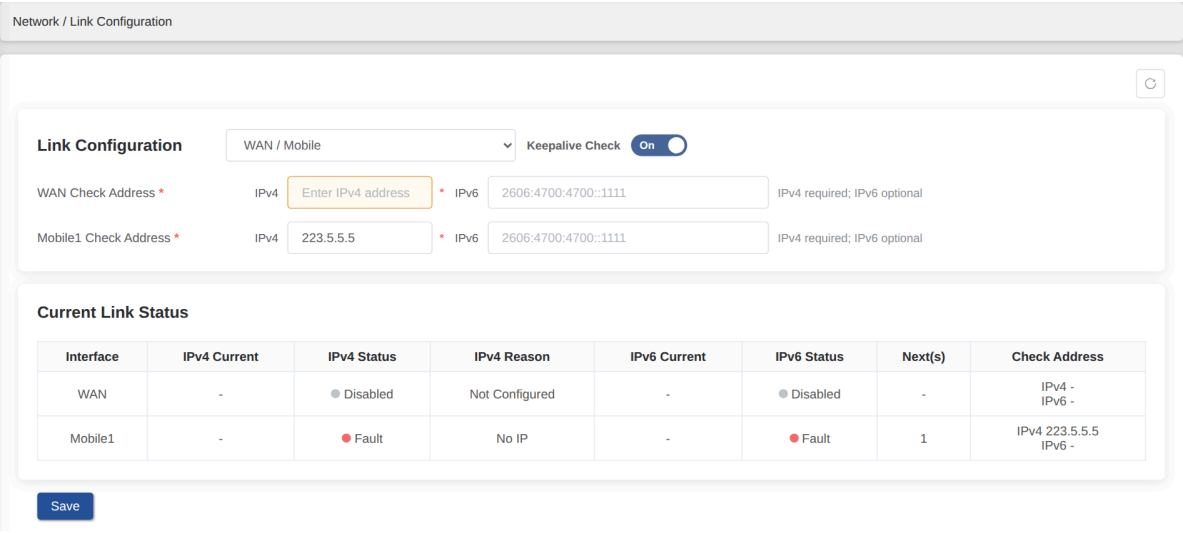



Figure 4-10 Link Configuration and failover

Native unsaved form / browser draft; not applied to device

## FIELD TASK: PROVE WIRED PRIORITY, CELLULAR BACKUP AND RECOVERY

Prove WAN and cellular applications individually before this test. Disable a conflicting load-balancing plan. WAN test gateway is 192.168.20.1; cellular probes need a real carrier-reachable ICMP target, not the WAN private address.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Link Configuration | WAN / Mobile | Use this combination if present; wired first |
| Keepalive Check | enabled | Configure for multiple actual interfaces as required |
| WAN IPv4 Check Address | 192.168.20.1 | Proves reachability only to upstream gateway; use a reachable end-to-end target to detect upstream outages |
| Cellular IPv4 Check Address | carrier-reachable IP | One literal IPv4 address per interface |

### SAVE, TEST AND OBSERVE

1. Save and record Current, Status and Reason for IPv4/IPv6 plus the LAN application result. A healthy non-current backup is normally expected.
2. At the unit, disconnect only the WAN uplink cable, retaining LAN management. Record fault time, egress change and application reconnection time. Restore WAN, observe recovery and retest.
3. Also test upstream Internet failure with Ethernet still connected. If 192.168.20.1 still answers, that probe cannot detect the upstream outage; choose an end-to-end reachable target and repeat.

### PASS CRITERIA AND DIAGNOSIS

Pass when the application recovers; no fixed switching time is promised. No switch: check backup IP/service. Switched without data: check application reconnect and platform IP allowlists.

**Finish and restore:** Restore the cable and original priority plan; finish only after checking egress and application. For this platform, see Link Configuration for single-interface/cellular keepalive and Mobile bootstrap rules; verify the interfaces actually participating.

### EXPAND THE MODE INTO ACTUAL INTERFACES

| MODE OR CONDITION | MEANING |
|---|---|
| Mobile | Select cellular uplink; its probes are heartbeats |
| WAN | Wired uplink group ordered by WAN number; a five-port model may expand this into several interfaces |
| WAN / Mobile | Try the wired group before cellular; this is not equal traffic distribution |
| Wi-Fi uplink | Configure Station with a valid uplink before using its available link combinations; AP service does not establish wireless backhaul |

Single/multiple link rules apply to the expanded interface count. Selecting WAN alone can still mean multiple links on a five-port model.

## KEEPALIVE AND FAILURE DECISIONS

Keepalive is optional with one actual interface. Keepalive Only means heartbeats are sent; missing ICMP replies do not by themselves fail that sole uplink or switch its exit. Check addressing, interface, routes, DNS and the real application separately. Cellular probes remain heartbeats in multi-link operation as well; replies are not application acceptance.

With two or more actual interfaces, enable keepalive and enter one literal IPv4 target per interface. Do not enter hostnames or multiple IPv4 addresses in that field. IPv6 targets are optional and several can be comma-separated. In multi-link mode, wired and Station links participate in failover through their probe and recovery states.

## STATUS AND MODE CHANGES

| DISPLAY | WHAT TO CHECK |
|---|---|
| Current is Yes while a backup is also healthy | Normal: health and current-exit selection are different facts |
| Keepalive Only | ICMP replies do not establish Internet or application reachability |
| No IP / STA Disconnected | Check interface addressing, wireless association or cellular registration/dial-up |
| LAN Subnet Conflict | Correct overlapping LAN/uplink subnets rather than saving the same addresses again |
| DNS Unavailable | Check DNS supplied by the selected exits; an address or probe reply alone is insufficient |
| Recovering | Continue observing status and service; one displayed value is not a guaranteed switchover time |

After changing modes, an old NP exit excluded by the new mode is retired. Mobile mode has an exception: while cellular is unavailable, a configured WAN with suitable addressing, gateway and DNS can provide the firmware's bootstrap path. Check any independent VPN default exit separately. Verify actual IPv4/IPv6 exits and routes; selecting a mode is not traffic-isolation enforcement. If selected uplinks are unavailable, check their interfaces, addresses and DNS. Resolve load-balancing conflict prompts before combining configurations.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Link Configuration | Priority follows the combination from left to right; WAN is a wired group. Count expanded interfaces when deciding single/multi-link behavior. |
| 2 | Keepalive Check | Optional for a sole interface, required for multiple interfaces. Sole-link and cellular ICMP heartbeats do not directly arbitrate failure. |
| 3 | IPv4 Check Address | Enter one literal IPv4 address per interface, without a hostname or comma list. It must be reachable through that exit. |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 4 | IPv6 Check Address | Optional; comma-separate literal IPv6 addresses and assess its current state separately from IPv4. |
| 5 | Current / Status / Reason | Separate exit selection, health and reason, including Keepalive Only, DNS Unavailable, No IP and Recovering. |
| 6 | Next(s) | Probe scheduling information, not a guaranteed switchover countdown. |

**Check the result** Each uplink works independently before service behaviour is checked through failure, switchover and recovery

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| WAN selected but two probe targets are required | Inspect the table: the WAN group may include WAN and WAN2. Count participating interfaces, not mode labels. |
| Keepalive cannot be turned off | It is mandatory in multi-interface mode. If one interface is intended, review the actual participating interfaces and site plan. |
| Settings or Save are unavailable | Check for enabled Load Balance or a read-only legacy configuration. Back up and choose the intended policy before following the page prompt. |
| Healthy but the service is unavailable | Health is not server availability. Check routes, DNS, policy and the service port; verify the private-side path for a private APN. |

# 4.8 Load balancing

Path Network > Load Balance

Load balancing distributes sources or sessions among usable uplinks. It differs from failover and does not automatically give one TCP connection the sum of all uplink bandwidth.

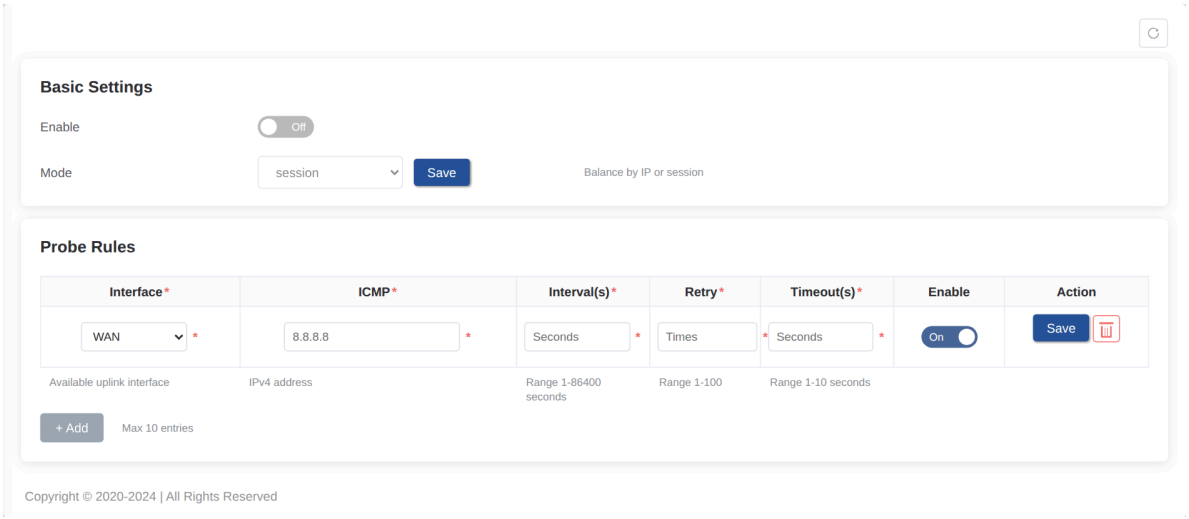



Figure 4-11 Load balancing

Native unsaved form / browser draft; not applied to device

## FIELD TASK: VERIFY DISTRIBUTION ACROSS CONNECTIONS

Prove both uplinks separately and record their egress. Resolve priority/full-tunnel conflicts shown on the page before enabling. Use at least two LAN clients and multiple new connections.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode | IP then Session | IP preserves source affinity; Session distributes connections |
| Interface / ICMP | actual egresses and reachable targets | Prove each target via its own link |
| Interval / Retry / Timeout | 5 s / 3 / 2 s | For the current form with seconds as units |

## SAVE, TEST AND OBSERVE

1. Save each link rule and the mode, then enable the master switch. Open multiple fresh HTTP connections from both clients and inspect server source logs or egress counters.
2. Disconnect one uplink, repeat new connections and restore it. Record failures/reconnections rather than relying on one speed test.

## PASS CRITERIA AND DIAGNOSIS

One TCP download does not combine both link rates. Uneven distribution: inspect connection reuse, IP mode and health checks.

**Finish and restore:** Disable the master switch, restore priority/probes and verify the platform application.

### CHOOSE FAILOVER OR DISTRIBUTION FIRST

| REQUIREMENT | USE | WHAT TO OBSERVE |
|---|---|---|
| Prefer one exit and use a backup on failure | Link Configuration | Current exit, backup health and failback after recovery |
| Use several links for separate clients/connections | Load Balance | Distribution across several sources or connections |
| Route required traffic through a WireGuard full tunnel | The VPN arrangement | Resolve the outbound-policy conflict with Load Balance first |

Multi-link failover triggers a prompt to select a single-link mode before Load Balance can be enabled. WireGuard IPv4 Full Tunnel also prevents enabling it. Resolve the displayed prerequisite according to the site design; repeated switch clicks or temporarily unplugging a cable do not resolve a configuration conflict.

WAN may expand to several ports in a Multi-WAN layout and is not automatically a single-link mode. If the offered combinations do not meet the intended distribution design, confirm this unit's uplink settings and delivered firmware combinations before implementation rather than copying another unit.

### SAVE EACH RULE SEPARATELY

The master switch, mode and individual rules apply separately. IP mode keeps a source on a consistent exit; Session distributes separate connections. Neither bonds one ordinary TCP connection across all links.

### HOW TO CONFIGURE

1. Select the actual interface for the new row and a target reachable through that exit, not solely through another link
2. Enter interval, retry and timeout in the displayed units, then save that row. Review other rows individually rather than accumulating unsaved drafts
3. Check the row and master switches and test multiple sessions. A successful save establishes submission, not service reachability

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable | The master switch is separate from mode/per-rule saves. Resolve multi-link failover or WireGuard IPv4 Full Tunnel prompts first |
| 2 | IP / Session | IP mode keeps one source on a consistent uplink; session mode distributes separate connections |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 3 | Interface | Select an actual uplink to participate |
| 4 | ICMP | Reachable probe target for the uplink; avoid one that consistently blocks probes |
| 5 | Interval / Retry / Timeout | Interval 1–86400 seconds, retry 1–100, timeout 1–10 seconds. Do not enter milliseconds for this timeout |
| 6 | Per-connection behavior | Multiple uplinks do not turn one ordinary connection into their summed bandwidth |

**Check the result** Multiple sources or sessions follow the selected policy and a failed link no longer receives new test traffic

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| One download is not faster | Use multiple sessions or sources to verify distribution; do not treat load balancing as single-connection bandwidth bonding. |
| Enable is forbidden | Resolve the displayed multi-link failover or WireGuard IPv4 Full Tunnel conflict, then check for unsaved rule drafts. |
| Changing the mode has no effect | Mode Save, per-row Save and the master switch are separate. Also check that the test creates new connections. |

## 4.9 DDNS

Path Network > DDNS

DDNS publishes a changing egress address to a hostname. Successful resolution and inbound service access are separate: check carrier addressing, upstream NAT, forwarding and policies.

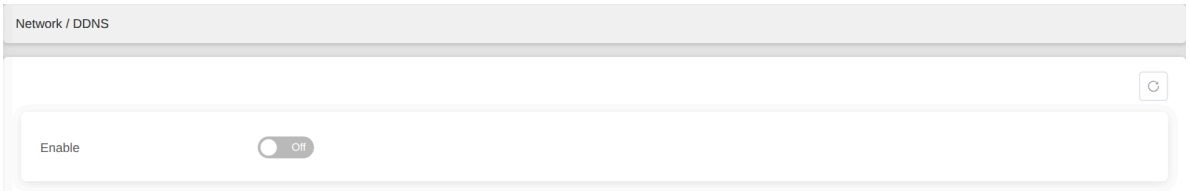



Figure 4-12 DDNS

### FIELD TASK: KEEP A HOSTNAME ALIGNED WITH THE REACHABLE PUBLIC ADDRESS

First prove a reachable public address and any upstream mapping. Obtain hostname, account/token and update permission from the selected DDNS provider.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Service / Domain | Registered provider / registered FQDN | Provider and registered FQDN must match |
| Username / Password / Token | provider credentials | Follow provider requirements; not Web admin |
| Interface / Address Family | Actual public egress / required IPv4 or IPv6 | Specify which egress/family to update |

## SAVE, TEST AND OBSERVE

1. Save/enable, inspect update status and run nslookup with the registered hostname from an external network; compare with actual public egress.
2. From outside, access an approved real service port; DNS success alone is insufficient.

## PASS CRITERIA AND DIAGNOSIS

Update fails: inspect credentials/provider. Old resolution: inspect cache/TTL. Correct address but blocked port: inspect CGNAT, upstream forwarding, firewall and application.

**Finish and restore:** Disable test updates, restore DNS/egress choices and revoke test tokens.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Service | Select the registered provider; update and authentication requirements are provider-specific |
| 2 | Domain | Full hostname authorized for update by the account |
| 3 | Username / Password / Token | Use provider credentials or token, not the router Web password |
| 4 | Interface / Address | Check the address being published; a successful update does not prove inbound reachability |
| 5 | Update Interval | Periodic update interval, using the page units |
| 6 | IPv6 | Choose IPv6 publication according to the DNS record and provider support |
| 7 | Status | Check authentication and update results against the provider response |

**Check the result** DNS resolves to the intended reachable public address and the target service is accessible

## TROUBLESHOOTING

| SYMPTOM | **WHAT TO CHECK** |
| --- | --- |
| The name resolves but remote access fails | Check inbound reachability, port mapping and policy. DDNS does not create a remote tunnel. |

CHAPTER

05

# Applications

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 5. Applications

## 5.1 Choose acquisition and data processing

| SITE REQUIREMENT | START HERE | CONDITION |
|---|---|---|
| Read instrument values to MQTT | M1: Modbus→device→command | Prove mock255, then replace with the real register map |
| Forward serial bytes to an existing server | DTU: echo FIELD-001 first | Transparent forwarding does not parse registers |

| METHOD | DATA PATH | USE |
|---|---|---|
| DTU | Raw serial frames ↔ TCP/UDP/MQTT | Server already parses the device protocol |
| Modbus | RTU/TCP → command values → reporting | Instruments with a defined register map |

Validate one known read-only point before reporting. Raw DTU frames and acquisition JSON writes use different formats.

## 5.2 ICMP monitoring

Path Application > ICMP

ICMP rules periodically test a path and execute the selected action after failure conditions are met. Choose targets that distinguish a silent host from an actual link failure.

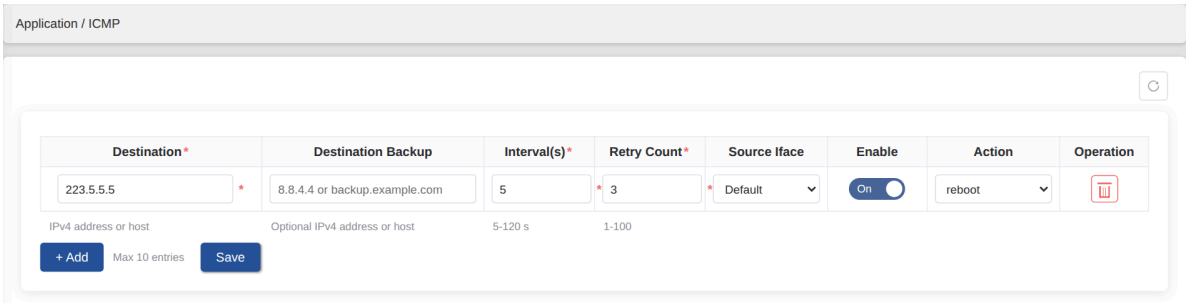



Figure 5-1 ICMP monitoring

Native unsaved form / browser draft; not applied to device

### FIELD TASK: TEST PROBE ACTIONS WITH A RECOVERABLE FAULT

ICMP actions differ from link-priority probes. Work beside the unit with LAN management. Reboot/modem-reset tests require an agreed maintenance window.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Target | 192.168.20.1 | Wired lab upstream; production needs an ICMP target reachable through the chosen egress |
| Source Interface | WAN | Actual egress |
| Interval / Retry | 10 s / 3 | Use page units |
| Action | reboot | Enable beside the unit only in the maintenance window; restore the target path immediately after triggering |

## SAVE, TEST AND OBSERVE

1. Prove the same-source probe in Network Tools first. If no alarm-only action exists, keep the rule disabled until a reboot maintenance window.
2. During the window interrupt the target path, record failures/action/recovery, restore the target and verify triggers stop and the platform recovers.

## PASS CRITERIA AND DIAGNOSIS

Repeated reboots: disable the rule and inspect blocked ICMP, source and timing. A Cellular2 option does not prove a second modem is fitted.

**Finish and restore:** Disable the test rule, restore original action/timing and verify stability.

ICMP action rules are separate from Link Configuration heartbeat/failover. Actions include reboot, Cellular-reset and Cellular2-reset and can interrupt service by restarting the router or modem. Select only an actual installed modem and enable the action under a maintenance plan. A generic second-modem option does not establish that hardware is fitted.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Target / Backup Address | Probe the required path; a backup distinguishes a failed target from a failed uplink |
| 2 | Source Interface | Choose the egress so a healthy alternate link does not mask a failed target link |
| 3 | Interval / Retry | Set probing cadence and failure conditions before triggering an action |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 4 | Action | Choose the exposed recovery action, such as reboot or modem restart; it interrupts the affected service |
| 5 | Enable | Enable after validating that the chosen targets are normally reachable |

**Check the result** Probe targets match their uplinks and results reflect actual link health

## 5.3 Scheduled tasks

Path Application > Timer

Scheduled tasks execute maintenance events in device local time. Verify synchronization and time zone before configuring them.

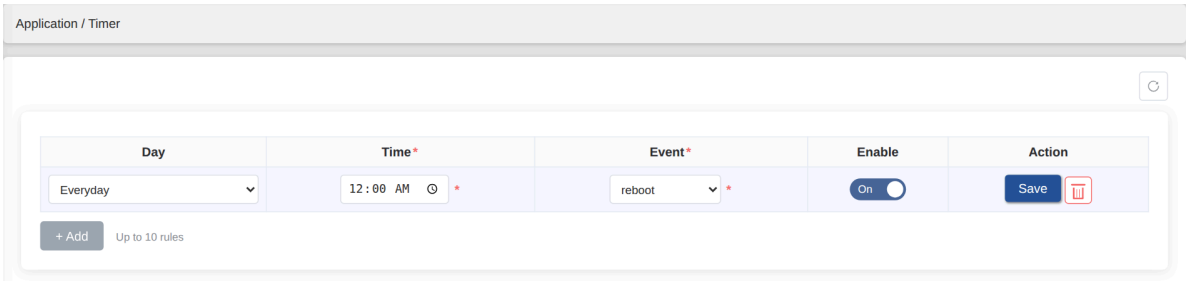



Figure 5-2 Scheduled tasks

Native unsaved form / browser draft; not applied to device

### FIELD TASK: SCHEDULE A TASK AGAINST VERIFIED SITE TIME

Confirm local timezone, date/time and synchronization first. Identify actually fitted modems and the maintenance window; a scheduled reboot interrupts service.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Day / Time | Test day / 10 minutes after current device time | Use device-local time and record the date |
| Event | reboot | Device reboot in a maintenance window; interrupts service |
| Enable | initially off | Enable only after checking the effect |

### SAVE, TEST AND OBSERVE

1. Save the new task, recheck weekday/time/timezone/event and enable only in the maintenance window. Retain LAN access and record logs plus application recovery.

### PASS CRITERIA AND DIAGNOSIS

No trigger: inspect device time, weekday and relevant switches. Service does not recover: inspect uplink, application reconnect and modem state.

**Finish and restore:** Delete the temporary schedule immediately after testing to prevent recurrence and confirm original schedules remain.

Scheduled events follow system time, so check timezone and synchronization first. Everyday runs daily; other choices select a weekday. Reboot and cellular-reset events interrupt the affected services. Choose events for installed modems; Cellular2-reset in a generic menu does not prove a second modem exists.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Day | Select a weekday or Everyday, interpreted in the device time zone |
| 2 | Time | Use the displayed time format after checking system clock and time zone |
| 3 | Event | Choose the maintenance action; saving a schedule does not execute it immediately |
| 4 | Enable / Save / Delete | Control rule activation, committing edits and removing rules |

**Check the result** Task time, timezone, target and enabled state match the plan and the resulting service state is correct

## 5.4 Network diagnostics

Path Application > Diagnostics

Diagnostics test reachability and routes from a chosen source; they do not replace application-protocol testing.

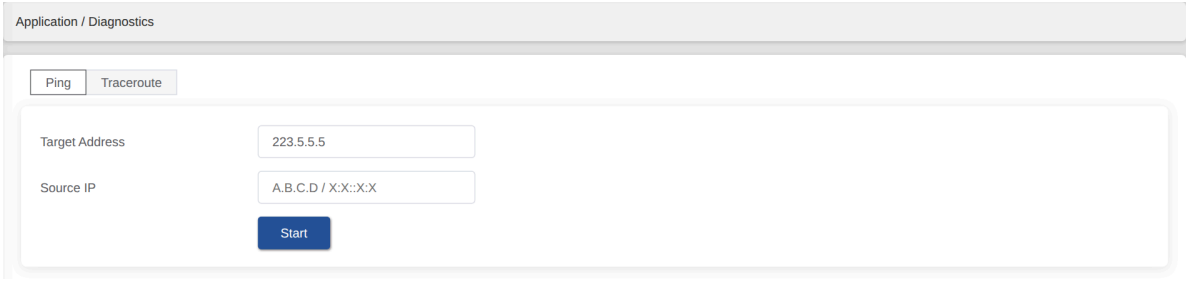



Figure 5-3 Network diagnostics

### FIELD TASK: SEPARATE AN INTERNET FAILURE INTO FOUR CHECKS

For the static-WAN case LAN is 192.168.10.1, WAN 192.168.20.2, upstream .20.1. Obtain a real project server IP/hostname from its handover; do not test the Internet using a fictional hostname.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode / Destination | Ping / 192.168.20.1 | First hop |
| Source | actual uplink under test | Avoid hiding failure through another working link |
| Mode / Destination | Ping / actual server IP | Separate routing from DNS |
| Mode / Destination | DNS / same server hostname | Resolution must match the platform plan |

## SAVE, TEST AND OBSERVE

1. Check PC IP/gateway, first hop, server IP and DNS, then open the application. Record source interface, destination, time and result for each test.
2. If the target blocks ICMP, use Windows Test-NetConnection with the real IP/port or the application itself.

## PASS CRITERIA AND DIAGNOSIS

First hop fails: inspect wiring/IP. First hop works but server fails: inspect upstream routing/carrier. IP works but name fails: inspect DNS. Application alone fails: inspect port/auth/certificate time/platform permission.

**Finish and restore:** Stop diagnostics, restore temporary source/route choices and retain the results.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Mode | Ping tests reachability; Traceroute inspects the route |
| 2 | Destination | Test actual IP and hostname targets separately to distinguish DNS and connectivity problems |
| 3 | Source | Specify the source exposed by the interface to test a particular path |
| 4 | Start / Result | Inspect loss, delay or route; an intermediate non-response does not necessarily make the destination unreachable |

**Check the result** Local, gateway, external IP and DNS tests identify and record the failing layer

# 5.5 SMS settings and manual sending

Path Application > SMS

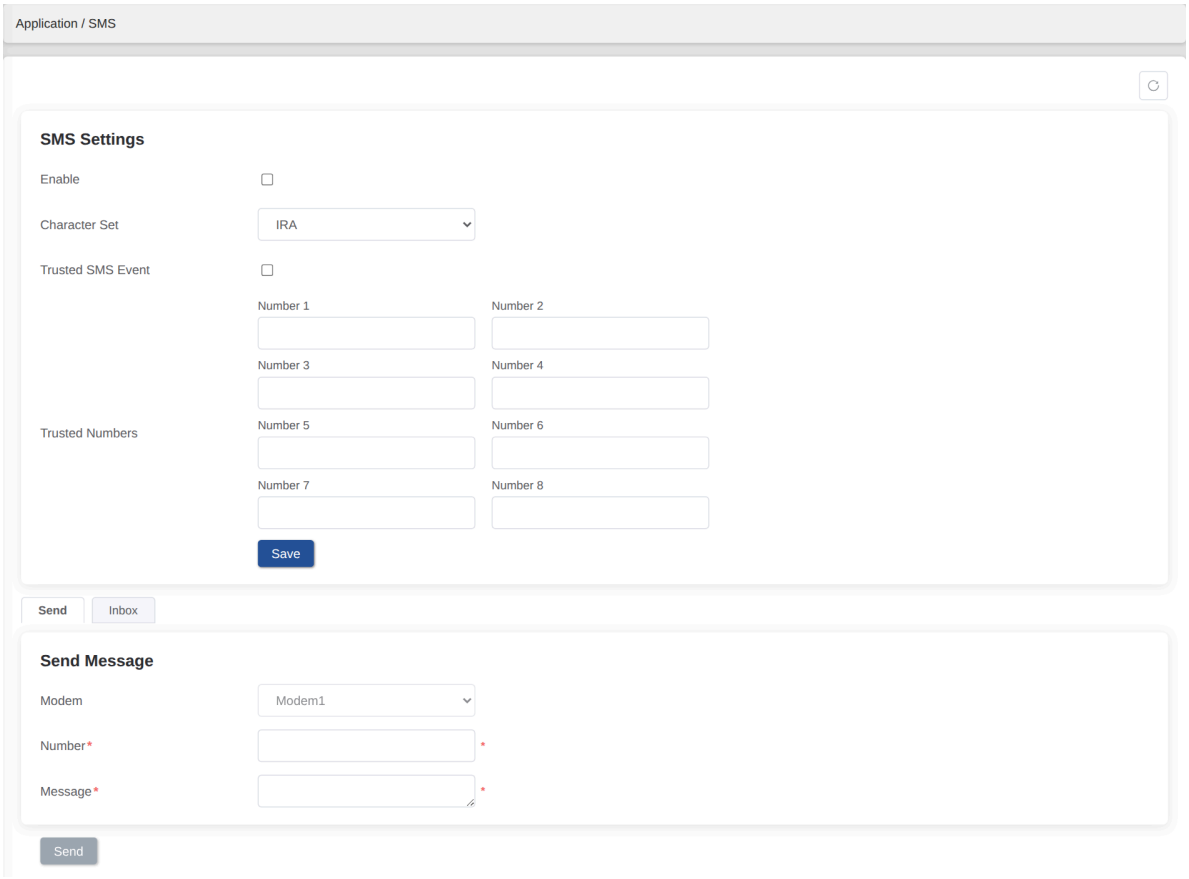



Figure 5-4 SMS settings and manual sending

## FIELD TASK: VERIFY MANUAL SMS BEFORE AUTOMATIC NOTIFICATION

The SIM subscription, modem and carrier must support SMS on the current network. Obtain recipient consent and the real number; keep LAN management.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Modem / SIM | fitted registered modem | Not every menu option is fitted hardware |
| Recipient / Content | Authorized real number / FIELD-001 | Start with short ASCII; use carrier number format |

## SAVE, TEST AND OBSERVE

1. Check SIM/registration, enter the number and FIELD-001 on the manual-send page, send and record result/time; verify actual receipt.
2. Enable automatic notification or authorized SMS control only after manual testing. Verify available source/auth restrictions and avoid production shutdown commands.

### PASS CRITERIA AND DIAGNOSIS

Failure: inspect credit, SMS service and network support. Accepted but absent: inspect number, filtering and carrier delay. Data connectivity does not prove SMS capability.

**Finish and restore:** Remove test numbers/messages/control rules and restore notification settings.

SMS requires modem and SIM service support. Select IRA, GSM or UCS2 to match encoding. The page provides eight trusted-number slots. Trusted events and manual sending are separate operations and do not imply unrestricted remote control.

1. Confirm registration and SMS service.
2. Configure enablement, character set and trusted numbers/events, then save.
3. In Send Message select Modem1 and send one test message to an approved number.
4. Verify page feedback and actual receipt; submission alone is insufficient.

## 5.6 DTU transparent transport

Path Application > DTU

DTU transports messages between serial and network connections. Match protocol, client/server role and serial settings to the peer; raw transport does not automatically interpret the equipment protocol.

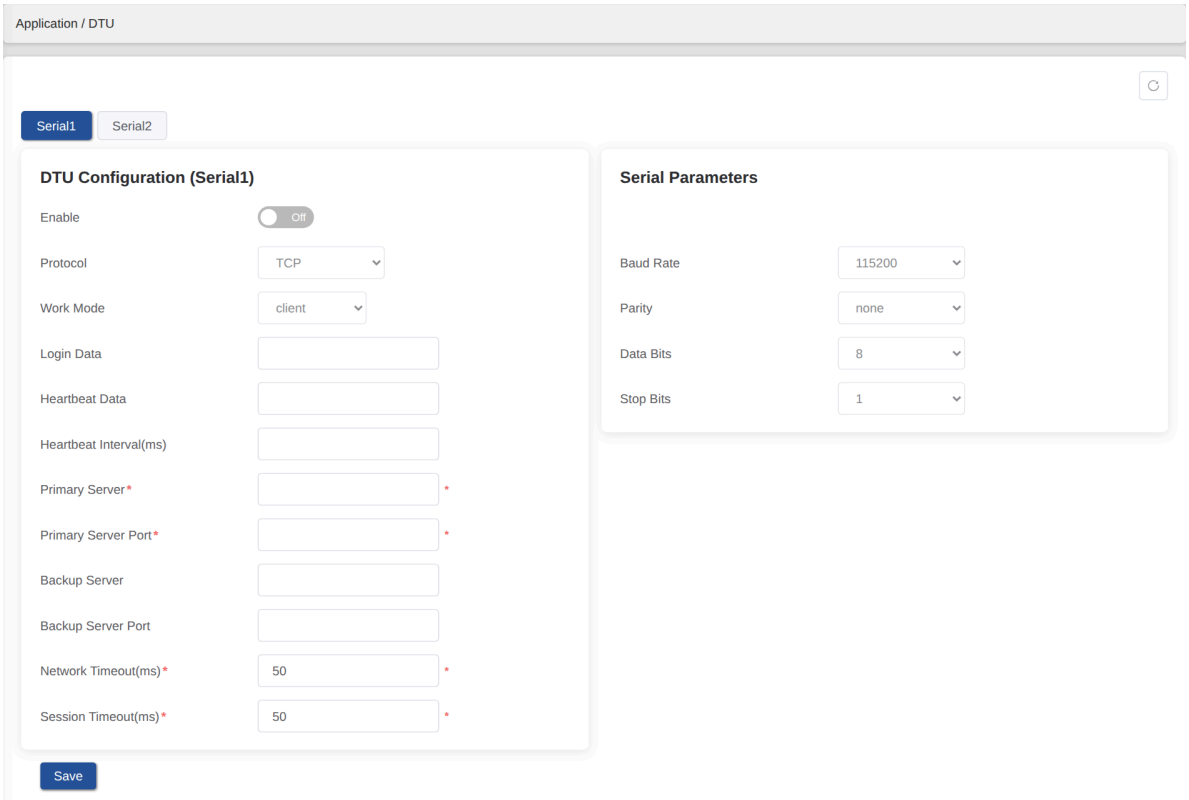



Figure 5-5 DTU transparent transport

### FIELD TASK: USE TCP ECHO TO PROVE TRANSPARENT BYTE ROUND TRIPS

Confirm a free port from this model’ s pin table. With power off, connect a matching USB RS232/RS485 adapter; never connect RS232 levels to RS485. PC 192.168.10.10 runs bench. Use a serial terminal that displays TX/RX bytes and can send ASCII.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Serial | verified free port | Use the model mapping below; do not guess Serial1 |
| Baud / Data / Parity / Stop | 9600 / 8 / none / 1 | Match gateway and terminal |
| Protocol / Work Mode | TCP / Client | Gateway initiates connection |
| Primary Server / Port | 192.168.10.10 / 5001 | PC echo service |
| Registration / Heartbeat Packet | off or blank | Exclude extra bytes on first test |
| Network Timeout(ms) / Session Timeout(ms) | 50 / 50 | TCP/UDP lab values, both milliseconds; these are not uplink selectors |
| MQTT Client ID | field-dtu-001 | MQTT subcase only; unique on this broker |
| MQTT QoS / Keepalive(s) | 0 / 60 | MQTT subcase only; keepalive in seconds |
| MQTT Transport / CA / SN Suffix | plain / none / Off | Isolated MQTT subcase only; disable SN topic suffixes |

## SAVE, TEST AND OBSERVE

1. Stop other acquisition/DTU/flow use of this port. Save DTU network settings and the Serial tab, then enable the instance.
2. Disable terminal local echo and send FIELD-001. Expect the exact bytes back through gateway→TCP service→gateway, once in TX and once in RX.
3. For UDP, select UDP Client and server port5002. For MQTT use broker 192.168.10.10:1884, field/DemoOnly2026, Publish=plant/site1/dtu/up and Subscribe=plant/site1/dtu/down. Watch upstream, then publish --topic plant/site1/dtu/down --payload FIELD-002 and inspect serial RX.
4. TCP server subcase: select server, Local Port5001 and save. Run python site_lab.py echo --host 192.168.10.1 --port 5001 --seconds 30. The serial terminal should receive FIELD-001; return the exact bytes within30 seconds without CR/LF. Expect PASS echo.

## PASS CRITERIA AND DIAGNOSIS

No connection: inspect PC firewall/listener5001. Network connected without bytes: inspect electrical type, pins, settings and ownership. Garbled data: inspect baud/parity. Local echo does not prove a network round trip.

**Finish and restore:** Disable test DTU, release the port and restore the original service; power down before rewiring.

## CHOOSE HOW THE NETWORK APPLICATION CONNECTS

| SITE NEED | DTU MODE | CONNECTION DIRECTION |
|---|---|---|
| The gateway forwards serial data to a remote server as a client | TCP / UDP Client | The gateway initiates TCP or sends UDP; enter the server address and listening port |
| A host application initiates access to a field serial device | TCP / UDP Server | YZW280 listens; the host must reach the listener address and port |
| Exchange serial data over MQTT topics | MQTT | Configure the broker, credentials and publish/subscribe topics; verify both directions |

## OTHER PROTOCOL MODES ON THIS PAGE

| OPTION | CONFIGURATION AND SCOPE |
|---|---|
| MODBUS | Modes include modbus_rtu_master/slave and modbus_ascii_master/slave. Match serial/network roles, local port, primary/backup destinations and timeouts. This DTU protocol gateway is distinct from the device/command/MQTT point workflow in Modbus Collect. |
| DNP3 | Choose master or outstation to match the peer. Set server/port and network/serial data timeouts in ms. Match none/hardware flow control to real wiring; TX/RX/GND alone does not establish hardware handshake lines. |
| AT | Select Mobile1 for modem-specific engineering diagnostics. Commands and effects follow modem/service instructions; do not send ordinary application frames as AT commands. |

## CLIENT: CONNECT SERIAL EQUIPMENT TO A SERVER

Use this mode when the remote server listens and the gateway initiates communication. Start the receiving server before configuring the gateway.

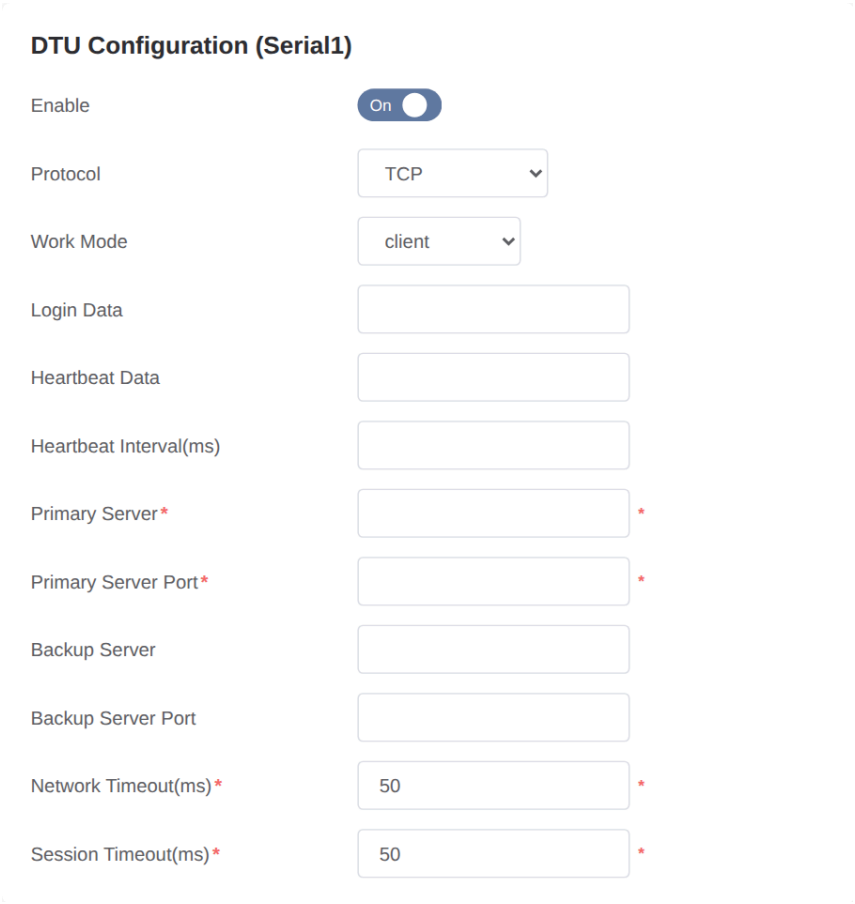



Figure 5-6 Client: connect serial equipment to a server

Native unsaved form / browser draft; not applied to device

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Protocol / Work Mode | Select TCP or UDP and client mode; the gateway initiates the connection or sends to the peer |
| 2 | Primary Server / Port | Enter the reachable address and service port of the serial-data receiver, rather than the gateway listener |
| 3 | Backup Server / Port | Complete both fields when a backup destination is required; otherwise leave both blank |
| 4 | Registration Packet | Identify the connection to the peer; agree the contents with the receiving application. This is not the slave address |
| 5 | Heartbeat Packet / Interval | Agree the heartbeat content and cadence with the receiver, separately from acquisition and MQTT reporting |
| 6 | Network / Session Timeout (ms) | Configure the data-wait parameters in milliseconds, as labelled in the interface, to match the connected application |

## SERVER: LET A NETWORK APPLICATION REACH SERIAL EQUIPMENT

Use this mode when the application initiates communication with the gateway. Match its destination to the local listener and provide the required routing and access policy.

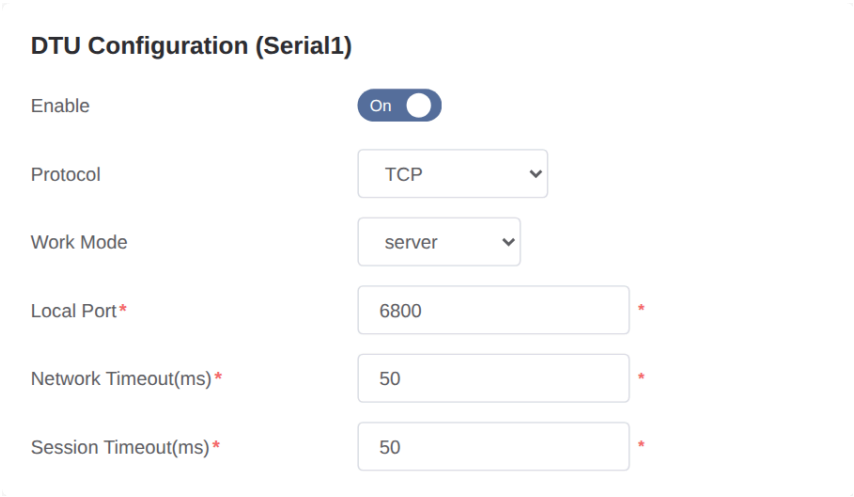



Figure 5-7 Server: let a network application reach serial equipment

Native unsaved form / browser draft; not applied to device

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Protocol / Work Mode | Select TCP or UDP and server mode; the remote application contacts the gateway |
| 2 | Local Port | Set the local listener without conflicting with Web, VPN or other services |
| 3 | Network / Session Timeout (ms) | Set the data-wait parameters in milliseconds; they are not a periodic acquisition schedule |

## MQTT: TRANSFER DATA IN BOTH DIRECTIONS USING TOPICS

Distinguish the directions: serial-to-cloud uses the publish topic, and cloud-to-serial uses the subscribe topic. DTU raw messages are distinct from Modbus/PLC point-write JSON.

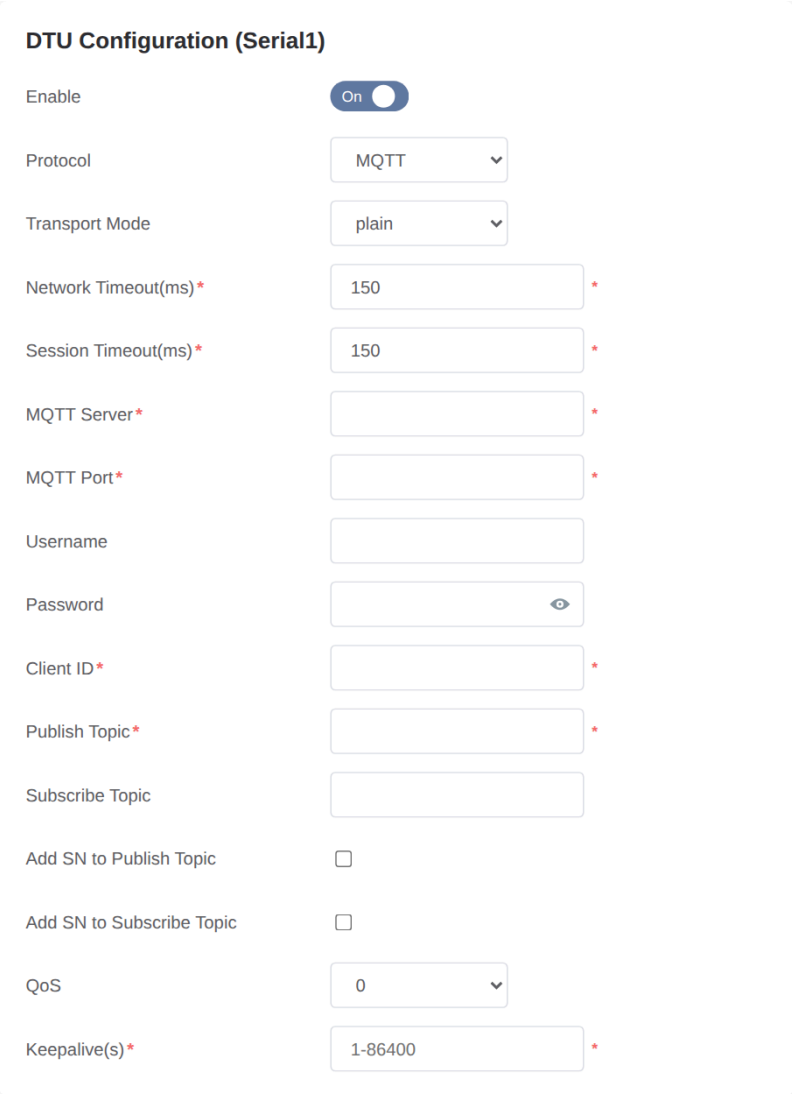



Figure 5-8 MQTT: transfer data in both directions using topics

Native unsaved form / browser draft; not applied to device

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Server / Port | Enter the MQTT broker address and matching listener port |
| 2 | Username / Password / Client ID | Use the broker credentials and a client ID distinct from other online clients |
| 3 | Publish Topic | Serial-originated data is published here; check the effective topic when the SN suffix is enabled |
| 4 | Subscribe Topic | Messages received on this topic are forwarded to serial; keep it distinct from the reporting topic |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 5 | Network / Session Timeout (ms) | Set the data-wait parameters in milliseconds, distinct from MQTT keepalive in seconds and business reporting intervals |
| 6 | TLS / CA | For TLS, select the matching CA and check device time and certificate validity |
| 7 | QoS / Keepalive | Set message quality of service and MQTT keepalive for the receiving service |

## SERIAL PARAMETERS AND COMMUNICATION CHECKS

After the network settings, check the serial parameters on the same port. Test a known message in one direction and then the reverse, without starting another service on that port.

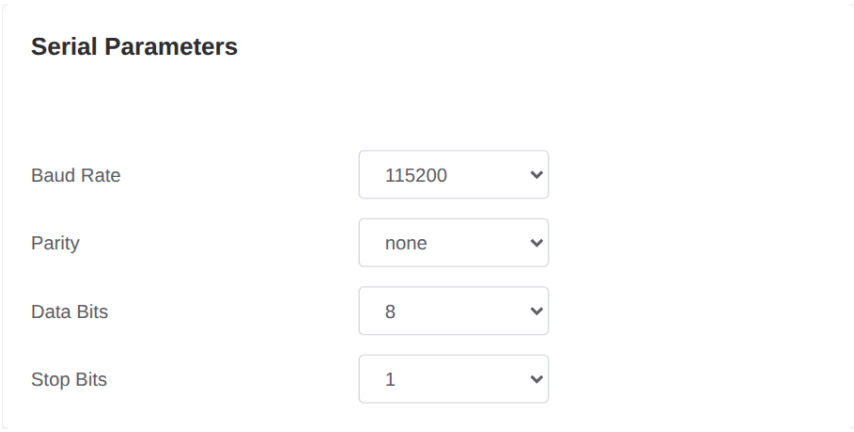



Figure 5-9 Serial parameters and communication checks

Native unsaved form / browser draft; not applied to device

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Serial Tab | Choose the required logical serial tab; use delivered documentation for its physical mapping |
| 2 | Baud / Parity | Match the attached equipment, including parity as well as baud rate |
| 3 | Data Bits / Stop Bits | Match both values to avoid received data that the peer cannot interpret |
| 4 | Port Ownership | Assign each physical serial port to one acquisition, transport or remote service |

**Check the result** Known messages pass in both directions without port conflicts and reconnect behaviour meets the application need

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
| --- | --- |
| Network session works but serial data is absent | Check physical port mapping, A/B, baud, parity and ownership, then protocol/mode and the destination port. |

## 5.7 Modbus acquisition and reporting

Path Application > Modbus Collect




Figure 5-10 Modbus acquisition and reporting

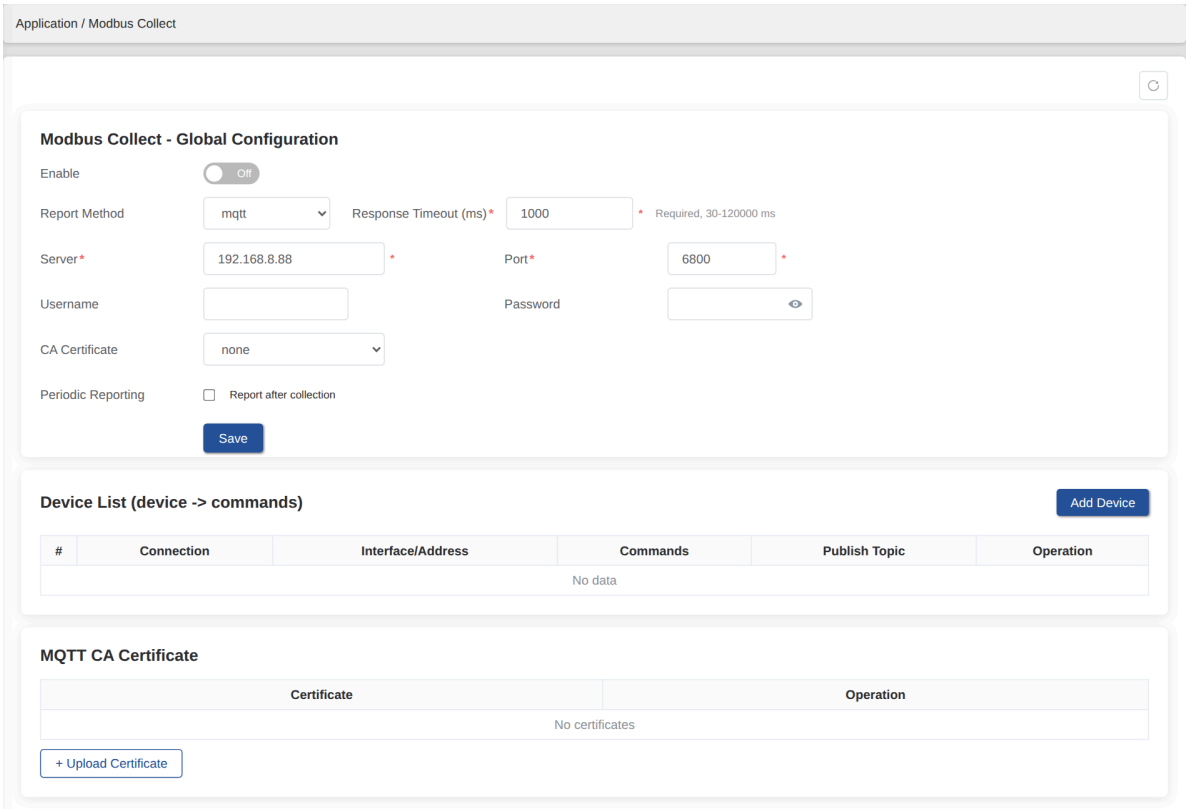



Figure 5-11 Modbus acquisition and reporting

### FIELD TASK: M1: READ 255 FROM A SIMULATED INSTRUMENT AND REPORT BY MQTT

On an isolated LAN set the gateway to 192.168.10.1/24 and PC to 192.168.10.10/24, gateway .10.1. Get the Field Test Tools package from Product Documents / Shared Resources. Install Python 3.8+, open its extracted folder and run python site_lab.py bench --bind 192.168.10.10. Keep it open. Allow only the lab LAN to TCP1502/1884/5001/8080 and UDP5002 on the PC firewall.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable / Report Method | On / MQTT | Enable collection and MQTT reporting |
| MQTT Server / Port | 192.168.10.10 / 1884 | PC test broker, separate from the gateway broker |
| Username / Password | field / DemoOnly2026 | Lab credentials for the supplied tool only |
| CA / TLS | TLS off | Plain transport on isolated LAN only; use platform certificates for production |
| Response Timeout | 1000 ms | Enter 1 if the page uses seconds |
| Periodic / Report Interval | On / 5 s | Use the periodic-report option exposed on the page |

## SAVE, TEST AND OBSERVE

1. In a second PC window run python site_lab.py modbus-get --host 192.168.10.10. Expect values [255], proving the mock slave runs.
2. Add a TCP device as in the next section, then the temperature command. Save command, device connection and global settings in order; confirm acquisition is enabled.
3. Run python site_lab.py watch --host 192.168.10.10 --topic plant/site1/plc1/data --seconds 30 --expect temperature=255. The tool prints raw messages and PASS when it observes numeric 255.

## PASS CRITERIA AND DIAGNOSIS

Require successful acquisition and an observed temperature=255. MQTT online alone is insufficient. No message: inspect broker/auth/topic then collection logs. Wrong value: inspect FC, start and type.

For a real instrument replace IP/port/unit/register map individually. 255 is a lab raw value; a 0.1 scale gives 25.5. Do not label raw 255 as 255°C.

**Finish and restore:** Disable the test connection, stop the tool with Ctrl+C and remove temporary firewall rules. Configure production credentials/TLS from the handover sheet.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable / Report Method | Enable acquisition and choose MQTT, TCP, UDP or IEC104, each with its own connection parameters |
| 2 | Response Timeout | 30–120000 ms, distinct from polling/reporting intervals in seconds |
| 3 | Server / Port / CA | Reporting destination and MQTT CA, not the slave connection address |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 4 | Immediate / Periodic | Periodic reporting: 1–86400 s. The first sample is immediate, later intervals send fresh values; IEC104 updates immediately |
| 5 | Device Connection | Up to 16 device connections and 32 commands per connection; TCP uses slave IP/port, RTU uses the actual serial port |
| 6 | Publish / Subscribe | Set separate data publication and cloud-write subscription topics per connection |
| 7 | Command | Configure name, slave, function, type, start/count, Writable and polling interval |
| 8 | IEC104 Mapping | Common address and IOA belong to IEC104 mapping, not Modbus register addressing |

**Check the result** Correct local readback is established before matching command updates arrive at the cloud

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| MQTT connected but no data | Validate slave reads first, then check the publication topic and report mode. Broker connectivity does not validate acquisition. |

# 5.8 Modbus device connection

Path Application > Modbus Collect > Add Device

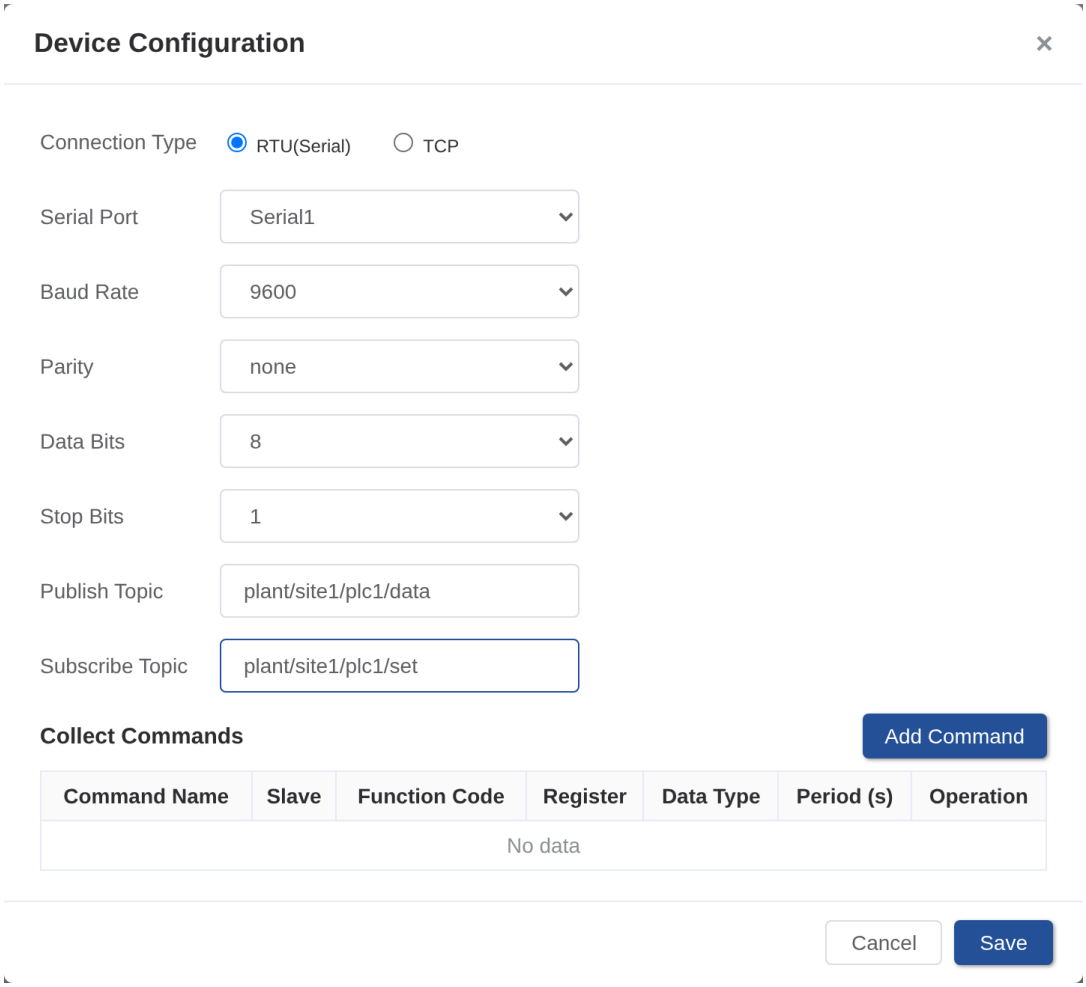



Figure 5-12 Modbus slave connection

Native unsaved form / browser draft; not applied to device

## FIELD TASK: M1 DEVICE CONNECTION: TCP SLAVE AND TWO TOPICS

Start the M1 PC tool first. This TCP case consumes no serial port. Keep port 1502; that is where the mock listens.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Connection / TCP IP / Port | TCP / 192.168.10.10 / 1502 | TCP slave endpoint |
| Publish Topic | plant/site1/plc1/data | Gateway publishes readings to broker |
| Subscribe Topic | plant/site1/plc1/set | Gateway receives write requests |
| Command List | temperature | Add the read-only command in the next section |

### SAVE, TEST AND OBSERVE

1. Add a TCP connection, fill the table, create temperature in Command List, then save device and global configuration.
2. From another LAN PC run Test-NetConnection 192.168.10.10 -Port 1502. Expect TcpTestSucceeded=True, then inspect gateway acquisition logs and the M1 subscriber.

### PASS CRITERIA AND DIAGNOSIS

TCP open but collection times out: inspect unit address, function code and slave access. Topics are case-sensitive and slash-sensitive.

**Finish and restore:** Delete/disable and save the lab connection. Replace endpoints using the real instrument documentation.

### PROCEDURE

1. Open Modbus Collect and select **Add Device**.
2. For RTU, select the physical serial port and match its settings. For TCP, enter the slave IP and its actual listening port.
3. If using MQTT, configure separate publish and subscribe topics. This example uses `plant/site1/plc1/data` and `plant/site1/plc1/set` respectively.
4. Add acquisition commands, review the parameters, then save the device configuration.

> Verify: the connection appears in the list with the intended interface and topics. The figure shows unsaved example topics, not factory settings.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | RTU / TCP | Choose the master-to-slave transport; the router is not the acquisition slave |
| 2 | Serial / Baud / Parity / Data / Stop | For RTU, match the bus; one connection configuration exclusively owns its port |
| 3 | TCP IP / Port | Use the slave service address and port, not the MQTT broker |
| 4 | Publish Topic | Acquired values are published here; the cloud subscribes for data |
| 5 | Subscribe Topic | The cloud publishes controls here; do not confuse it with the data topic |
| 6 | Command List | Configure slave/register commands within the connection, up to 32 per connection |

> **Check the result** The device connection, serial port or TCP endpoint and effective topics match the plan

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
| --- | --- |
| A new device repeatedly times out | First check Serial1/2 against wiring, or the TCP IP/port; then slave address and serial settings. |

## 5.9 Modbus commands and addressing

Path Application > Modbus Collect > Add Device > Add Command

32-bit integers and floating-point values occupy two consecutive registers. Match the slave's ABCD / CDAB float byte order. Do not enter display-style register numbers such as 40001 without converting them.

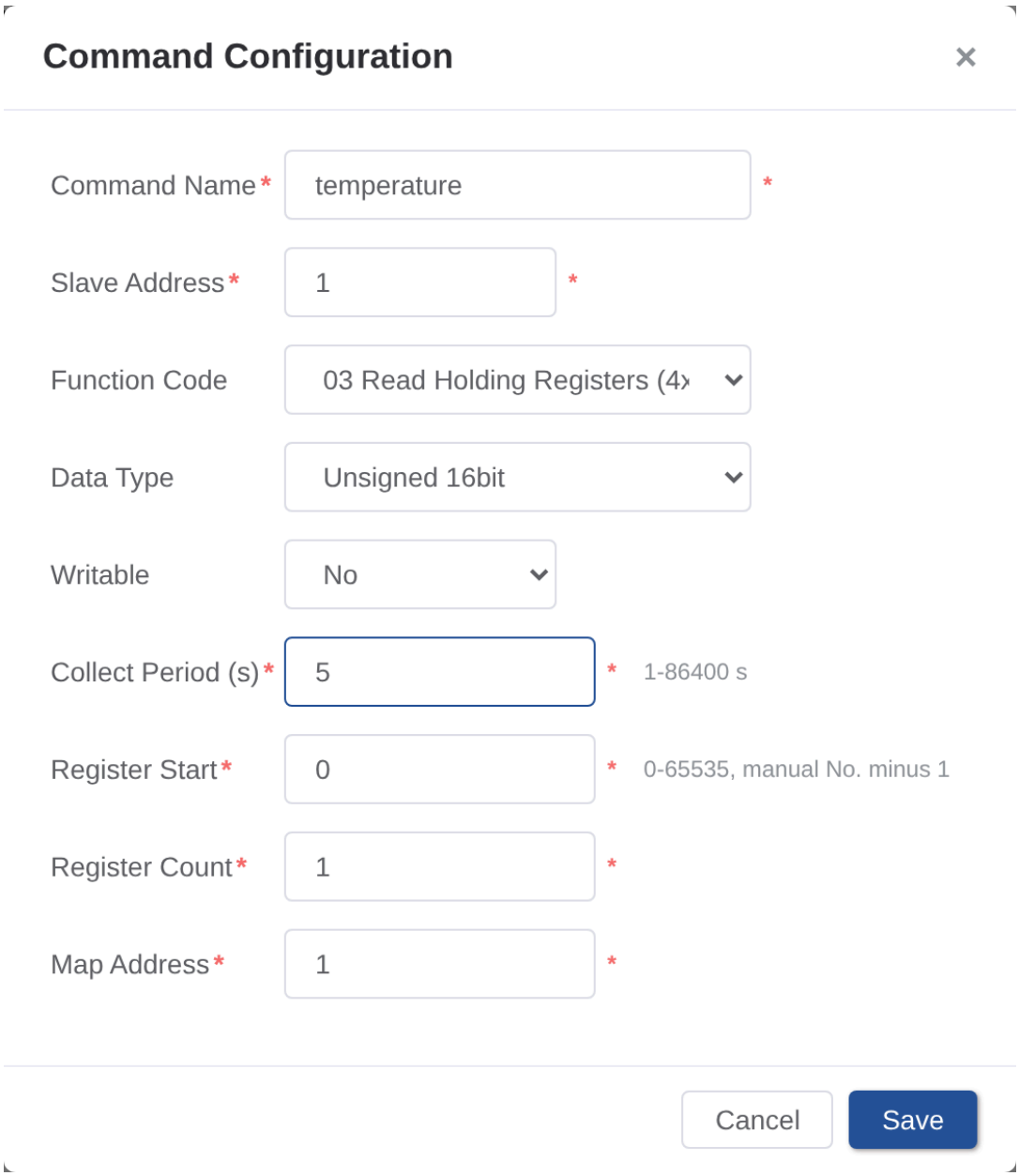



Figure 5-13 Read-only acquisition command example

Native unsaved form / browser draft; not applied to device

### FIELD TASK: M1 COMMAND: 40001 CORRESPONDS TO PDU START 0

The tool exposes unit 1 holding register PDU address 0 with value 255. Confirm any traditional 40001 notation in the instrument map; do not enter 40001 as a PDU start.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Command Name | temperature | Unique name and JSON key |
| Slave Address / Function Code | 1 / FC03 | Read holding registers |
| Register Start / Count | 0 / 1 | Zero-based PDU address, one 16-bit register |
| Data Type | UInt16 | Unsigned 16-bit choice on the page |
| Collect Period / Writable | 5 s / Off | Read-only initially; independent of reporting period |
| Map Address | 0 | Enter0 for this case; not40001 or a TCP port |

### SAVE, TEST AND OBSERVE

1. Save the command, parent device and global configuration. Use the M1 watch command to observe temperature=255.
2. For a real slave confirm unit, FC, start, register count, type, word order and scale point by point. A 32-bit value occupies two 16-bit registers; select ABCD/CDAB from the instrument map, not by hiding byte-order errors with a scale.

### PASS CRITERIA AND DIAGNOSIS

Exception 02 often means illegal address; 01 unsupported function. Unstable values: inspect type/order. All points time out: inspect the connection before changing addresses.

**Finish and restore:** Disable/delete the command and restore the original point list from its export.

**Example reference:** this section continues M1, the read-only temperature point. The 40001 entry explains address notation, not another acquisition address; use your instrument register map.

## RELATE REGISTER NUMBERING TO THE START ADDRESS

This explains input conventions, not a real instrument map. The temperature example uses function 03, start 0, Unsigned 16bit, quantity 1, a 5 s period and Writable No initially.

| ADDRESS CONVENTION EXPLICITLY STATED BY THE VENDOR | **WHAT TO ENTER** |
|---|---|
| PDU address or zero-based offset 0 | Start 0; do not subtract 1 again |
| One-based numbering, with 1 as the first register | The first register has start 0 |
| 4xxxx denotes holding registers and 40001 is explicitly the first | Select function 03 and start 0 for that first register; do not enter 40001 unchanged |

The function selects the object area, the slave address selects the device on the bus, and the start address selects a position inside it. Do not interchange them. A 32-bit value uses two consecutive registers and requires the correct vendor byte order. Check sign, decimal placement, range and update time after reading.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Command Name | Identifies reporting and MQTT writes; keep command names unambiguous within the connection |
| 2 | Slave Address | Slave identifier; devices on one RTU bus need distinct addresses |
| 3 | Function Code | 01 coils, 02 discrete inputs, 03 holding registers, 04 input registers |
| 4 | Data Type | Six current Web types: int16, uint16, int32 ABCD, uint32 ABCD, float ABCD and float CDAB. Other backend byte orders or 64-bit types are not implied UI options |
| 5 | Writable | Enable only for intended control commands; areas 02/04 remain non-writable |
| 6 | Collect Period | Per-command polling: 1–86400 s, distinct from response timeout and MQTT reporting cadence |
| 7 | Register Start / Count | PDU addresses start at 0; 32-bit values occupy at least two consecutive registers |
| 8 | Map Address | Used for IEC104 IOA mapping, not MQTT command-name selection |

**Check the result** Readback sign, decimal placement, range and updates match the slave documentation

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
| --- | --- |
| Scale, sign or decimal value is wrong | Check address offset, consecutive-register count, data type and byte order against the slave map. |
| Replies arrive but values are wrong | Identify zero-based, one-based or 4xxxx conventions first, then function, type, byte order and scaling rather than checking only A/B. |

## 5.10 Modbus cloud writes over MQTT

Path Application > Modbus Collect

### FIELD TASK: M2: WRITE 300 TO THE MOCK REGISTER AND READ IT BACK

Complete M1 first. This test changes PC memory only and connects no actuator. Real writes require control authorization, valid ranges and agreed safe operating conditions.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
| --- | --- | --- |
| Command Name / Slave Address | setpoint / 1 | Add a separate command |
| Function Code / Register Start / Count | FC03 / 1 / 1 | Periodic readback after a write |
| Data Type / Writable / Collect Period | UInt16 / On / 5 s | Only this simulated point is writable |
| Map Address | 1 | Separate test mapping; not a replacement for register start |
| Subscribe / Publish Topic | plant/site1/plc1/set / plant/site1/plc1/data | Same M1 connection, different topics |

### SAVE, TEST AND OBSERVE

1. Save command, device and global configuration. Start readback first: python site_lab.py watch --topic plant/site1/plc1/data --seconds 60 --expect setpoint=300.
2. In another window run python site_lab.py publish --topic plant/site1/plc1/set --set setpoint=300. It sends a flat numeric JSON object; avoid strings, nested objects and arrays.
3. Then run python site_lab.py modbus-get --start 1 --count 1. Expect values [300] and setpoint=300 in upstream data.

### PASS CRITERIA AND DIAGNOSIS

A broker PUBACK only accepts the message; it does not acknowledge a gateway/slave write. There is no independent MQTT write acknowledgement here; inspect readback and logs.

No change: inspect subscription topic, exact command name, Writable and permissions. Out of range: use a valid value; do not enable writes on all points.

**Finish and restore:** Disable Writable on setpoint and save. Restart bench to reset its simulated value to 100.

**Independent example M2 (authorized write):** use test slave 1, setpoint, read FC03, PDU start 1, Unsigned 16bit, count 1, no scaling and Writable enabled. A single-register write uses FC06. The expected change is 100 to 300, checked by a later FC03 read. It shares the M1 TCP connection but uses a different register; run and 32-bit entries describe other independent types.

### BEFORE WRITING

Enable the collector and MQTT reporting. The target command must exist and be Writable. The cloud client and collector use the same broker; publish to the device's **subscribe topic**.

Example topic: `plant/site1/plc1/set`. Send control messages with `retain=false`.

```
{"setpoint":300}
```

Use a flat JSON object with numeric values, not strings, Boolean values or a nested data envelope. A 32-bit value uses function 16 (0x10) and two consecutive registers. Areas 02 / 04 cannot be written. UTF-8 payload size is 1–511 bytes.

> Verify: this module has no dedicated MQTT write reply. Confirm with subsequent collected readback and device logs. Message delivery or an absent reply cannot replace field readback. Multiple commands execute independently, not atomically.

### VERIFY ONE CONTROL COMMAND IN ORDER

1. Confirm normal read acquisition, then permit writing only as allowed by the slave map. JSON keys must match configured command names; setpoint is not a built-in command.
2. Inspect subsequent collected values and logs. Resume normal control after expected readback.
3. If nothing changes, check the topic, command name, Writable flag and numeric type, then the slave response. Do not repeatedly resend because there is no dedicated reply.

| ACTIVE MODULE | TARGET LOOKUP | VALUE FORM | CONFIRMATION |
|---|---|---|---|
| Modbus Collect | JSON key matches command name, such as setpoint | JSON number, such as 300 | Later collected readback and logs; no dedicated reply |

### END-TO-END EXAMPLE: WRITE A SETPOINT AND READ IT BACK

**Assumptions:** an authorized test slave; a working `setpoint` command in holding-register area 03, PDU start 1, quantity 1, UInt16, no scaling. This address/value convention is illustrative, not a real meter/PLC control address.

| STEP | ACTION / EXPECTED OBSERVATION |
|---|---|
| 1. Read first | Confirm setpoint=100 locally and at the gateway; record name, address and type |
| 2. Publish | Send `{"setpoint":300}` to the actual device subscription topic `plant/site1/plc1/set`, retain=false |
| 3. Execute | Backend matches the writable command, encodes UInt16 and writes one register with FC06; inspect logs for slave rejection/timeout |
| 4. Read back | In a later report on the device uplink topic, verify setpoint=300; keep other fields as actually reported |
| 5. Confirm locally | Check the field setpoint/state; read before any retry or authorized restoration, then verify again |

Client example; supply broker/authentication/TLS settings for the delivery:

```
mosquitto_sub -h broker.example.com -t 'plant/site1/plc1/data' -v
mosquitto_pub -h broker.example.com -t 'plant/site1/plc1/set' -m '{"setpoint":300}'
```

Do not add `-r` or retain control commands. This module has no independent MQTT write acknowledgement. PUBACK, receipt or silence is not field readback. Read before retrying after a timeout. **Status:** source/format-reviewed walkthrough; no field slave was written.

### START WITH ONE VERIFIED WRITABLE POINT

setpoint is a command created for this example, not a built-in control. The illustration uses a 16-bit holding register at offset 1. Enable writing on a field point only where its slave documentation permits it.

### HOW TO CONFIGURE

1. First confirm normal readback and the slave address, function, offset, type and allowed value range, then enable Writable
2. Use the same broker and publish one {"setpoint":1200} request to the effective device subscribe topic with retain=false. The key must exactly match the command name
3. Check subsequent point readback and device logs. There is no dedicated MQTT write reply; after a timeout, read back before repeating a control

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Subscribe Topic | Publish to the target connection subscribe topic, not its data publication topic |
| 2 | Command Name / Numeric Value | Flat JSON keys are configured command names and values must be JSON numbers |
| 3 | run | Writable coil command, read function 01; numeric 0/1 is written using function 05 |
| 4 | setpoint | Writable uint16 holding-register command, read function 03, written using function 06 |
| 5 | 32-bit values | Occupies two consecutive registers and uses function 16 (0x10), with the configured byte order |
| 6 | Readback | No dedicated MQTT write reply; check subsequent reads and logs. No reply does not prove no write occurred |

**Check the result** Subsequent readback or field feedback confirms the write; MQTT publish success alone is insufficient

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Publish succeeds but the field value does not change | Check the topic, Writable, command name and JSON numeric type. Confirm subsequent readback; there is no dedicated MQTT write acknowledgement. |

# 5.11 SNMP

Path Application > SNMP

SNMP integrates the device into a management system. Obtain the matching MIB and manager requirements before setting version, credentials, listener and Trap destination.

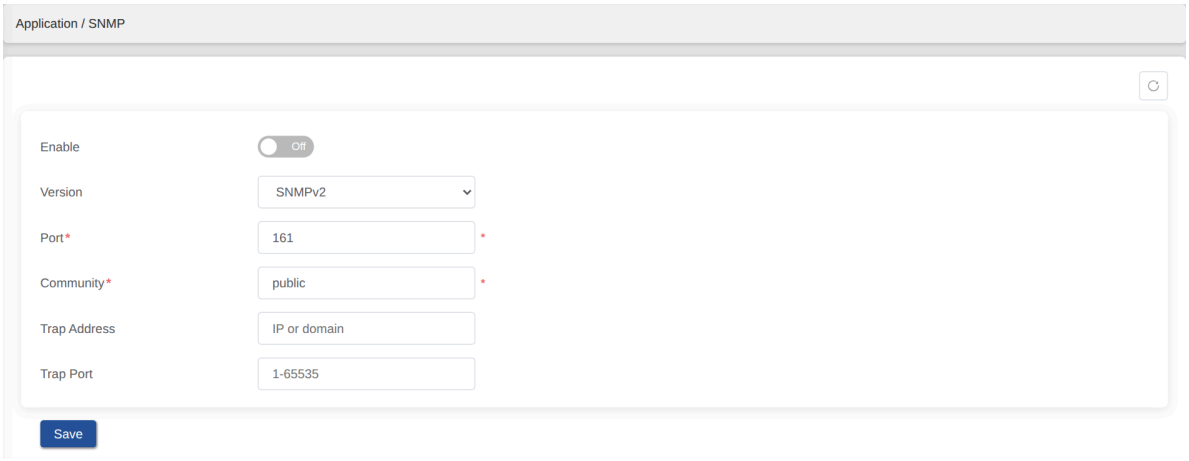



Figure 5-14 SNMP

## FIELD TASK: READ ONE READ-ONLY OID FROM LAN

Install a Net-SNMP client on the PC and allow UDP161 only on the isolated LAN. For production v3 obtain user/security level/auth/privacy algorithms from the administrator.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Version / Port | v2c / 161 | Isolated read-only test |
| Read Community | field_ro | Custom lab community |
| Write Community | disable or unset | No SET in this case |

## SAVE, TEST AND OBSERVE

1. Save/enable and run snmpget -v2c -c field_ro 192.168.10.1 1.3.6.1.2.1.1.1.0 on the PC; expect a sysDescr string.
2. Obtain the matching MIB and read actual status OIDs. Verify traps in receiver logs; GET success does not prove trap delivery.

## PASS CRITERIA AND DIAGNOSIS

Timeout: inspect UDP161, version, community and access scope. No Such Object: inspect MIB/OID and the .0 instance suffix.

**Finish and restore:** Disable lab v2c or apply production v3; revoke field_ro and temporary UDP access.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Version / Port | The page’ s community-based SNMPv2 is SNMPv2c; SNMPv3 is also available. Match version and port to the manager |
| 2 | Read / Write Community | SNMPv2 access identifiers for read and write, not Web accounts |
| 3 | Trap Address / Port | Destination for unsolicited notifications; configure its receiver in the management system |
| 4 | Mode / Username | SNMPv3 security mode and user must match the manager |
| 5 | Authentication / Privacy | Set authentication protocol/password and privacy protocol/key for the selected mode |
| 6 | MIB | Available monitoring objects depend on the delivered MIB, not arbitrary third-party OIDs |

**Check the result** The management station reads the required information using the configured version and authentication

## 5.12 Local MQTT Broker

Path Application > MQTTBroker

The local broker accepts MQTT client publish/subscribe connections and can aggregate site messages. Collectors may use a local or external broker, with connection and topic settings configured separately.

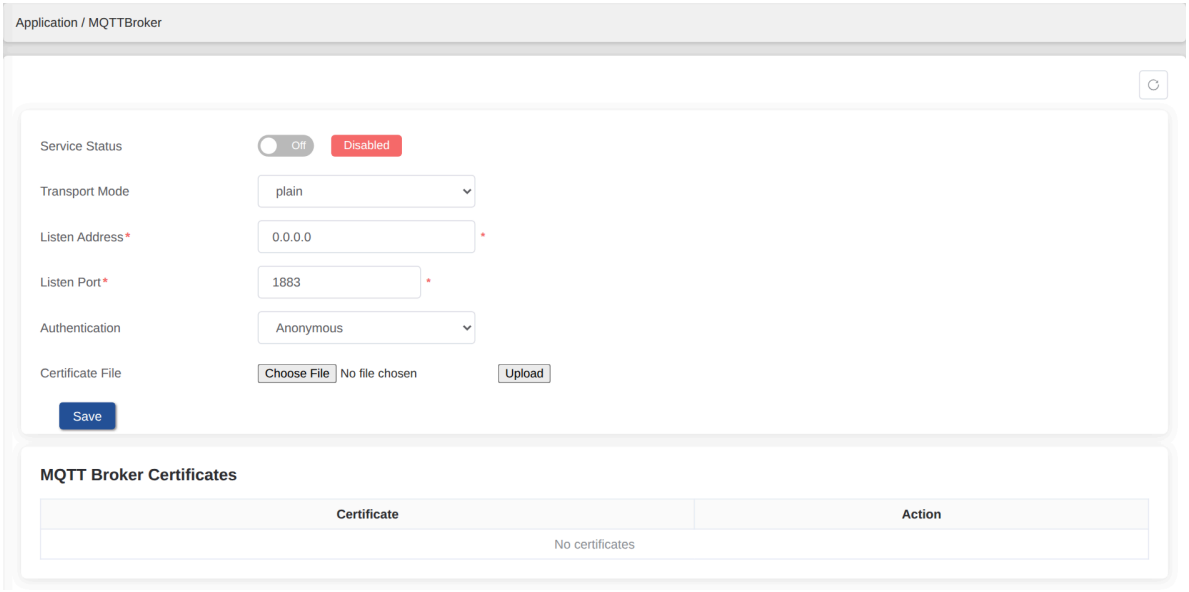



Figure 5-15 Local MQTT Broker

### FIELD TASK: PUBLISH AND SUBSCRIBE THROUGH THE GATEWAY BROKER

Complete M1 with the external PC first. This separate case tests the gateway broker. Choose unused port1884; the PC lab broker uses another host, so its port1884 does not conflict.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Service / Transport | On / plain TCP | Isolated LAN test; configure production TLS as required |
| Listen Address / Port | 192.168.10.1 / 1884 | If only all-address binding is supported, restrict access sources |
| Authentication / Username / Password | Enabled / field / DemoOnly2026 | Lab-only credentials; save authentication before testing |

### SAVE, TEST AND OBSERVE

1. Save/enable broker. In one PC window run python site_lab.py watch --host 192.168.10.1 --topic plant/site1/test --seconds 30.
2. In another window run python site_lab.py publish --host 192.168.10.1 --topic plant/site1/test --payload FIELD-001. Expect identical topic/content in the subscriber.

### PASS CRITERIA AND DIAGNOSIS

Connection refused: inspect listener/port/service. Auth failure: inspect broker credentials. The tool supports MQTT3.1.1 plain lab transport and fixed lab credentials, not production TLS credentials.

**Finish and restore:** Stop the test broker or apply production auth/TLS; revoke the lab account and temporary access.

> **Interface example and production security**: the service is off in the illustration. The plain transport, anonymous authentication and `0.0.0.0` values are examples, not recommended production settings. `0.0.0.0` listens on all local IPv4 interfaces; WAN reachability also depends on firewall/access rules. Before enabling, restrict access to the required LAN/VPN or specified sources, configure authentication, and use suitable TLS where supported by the delivered firmware and clients. Do not expose an unauthenticated MQTT service to an untrusted network.

Use an authorized client to publish and subscribe to a test topic and check access restrictions after configuration. The screenshot does not replace site verification.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Service / Transport | Control the local broker and plain/TLS transport |
| 2 | Listen Address / Port | Defines where MQTT clients connect; avoid conflicts with other services |
| 3 | Authentication | Select anonymous or username/password authentication and match client settings |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 4 | Server Certificate / Key | TLS server identity; the certificate name should match the client target |
| 5 | Function Boundary | This configures the local message server, not acquisition tasks or an m2mCloud tunnel |

**Check the result** Clients reach the intended listener and another authorized client receives a test-topic publication

## 5.13 Alarm notifications

Path Application > Alarm Control

Alarms send selected events through configured notification channels. Verify event generation, channel delivery and receipt separately.

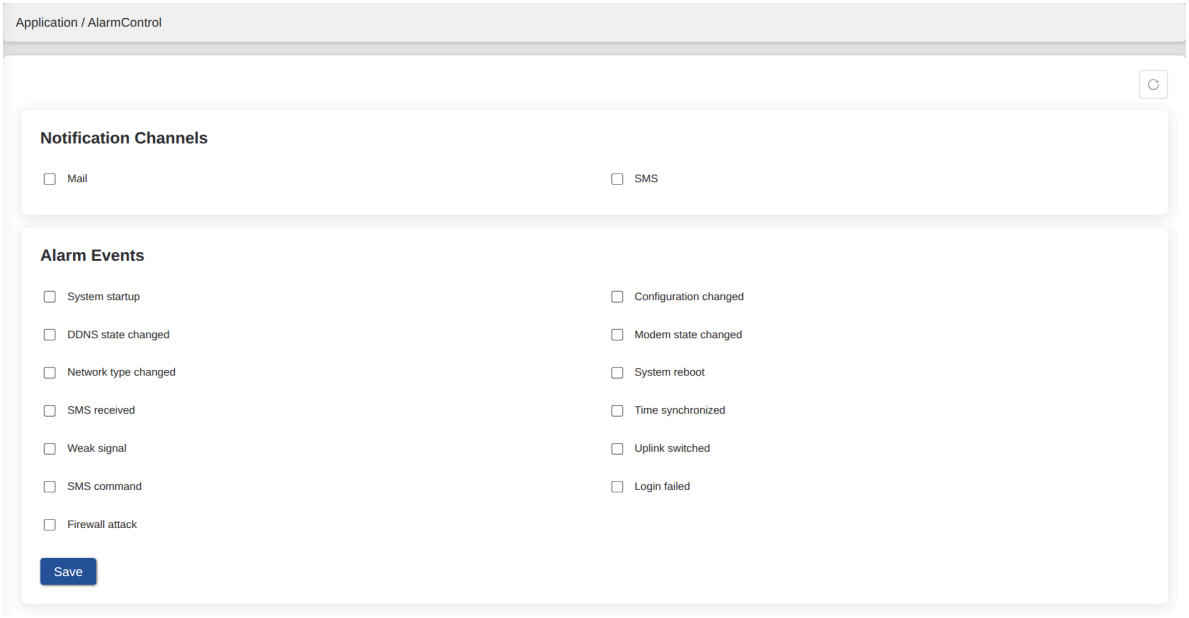



Figure 5-16 Alarm notifications

### FIELD TASK: TRACE ONE EVENT FROM LOG TO NOTIFICATION RECIPIENT

Verify each selected channel first: SMTP test receipt, manual SMS receipt or an active platform session. Choose only a supported event safe to trigger on site.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Notification Channels | Email | Complete SMTP test receipt first |
| Alarm Events | Login failed | Retain a valid session and try one wrong password in another window |

### SAVE, TEST AND OBSERVE

1. Save Email and Login failed. Keep the valid session; in a private window submit one wrong admin password and stop. Compare timestamped login-failure log, alarm send result and received mail.
2. Confirm a new login with the correct password, then select production events; add/test further channels individually.

### PASS CRITERIA AND DIAGNOSIS

Event without send: inspect event/channel selection. Send failure: diagnose that channel. Wrong received content: inspect event type/recipient account.

**Finish and restore:** Restore conditions/configuration, remove test recipients and retain a real notification sample.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Notification Channels | Select Mail or available SMS channels and configure the channel service itself |
| 2 | Alarm Events | Select exposed events such as startup, configuration change, uplink change or failed login |
| 3 | Dependencies | Mail depends on SMTP; SMS depends on an SMS-capable cellular configuration |
| 4 | Verification | Validate the channel, then check event notifications during controlled maintenance |

> **Check the result** The test condition matches its destination and trigger/recovery information follows the configured rule

# 5.14 SMTP mail service

Path Application > SMTPService

SMTP provides the mail-alarm transport. Credentials and security mode follow the mail service, not the router Web account.

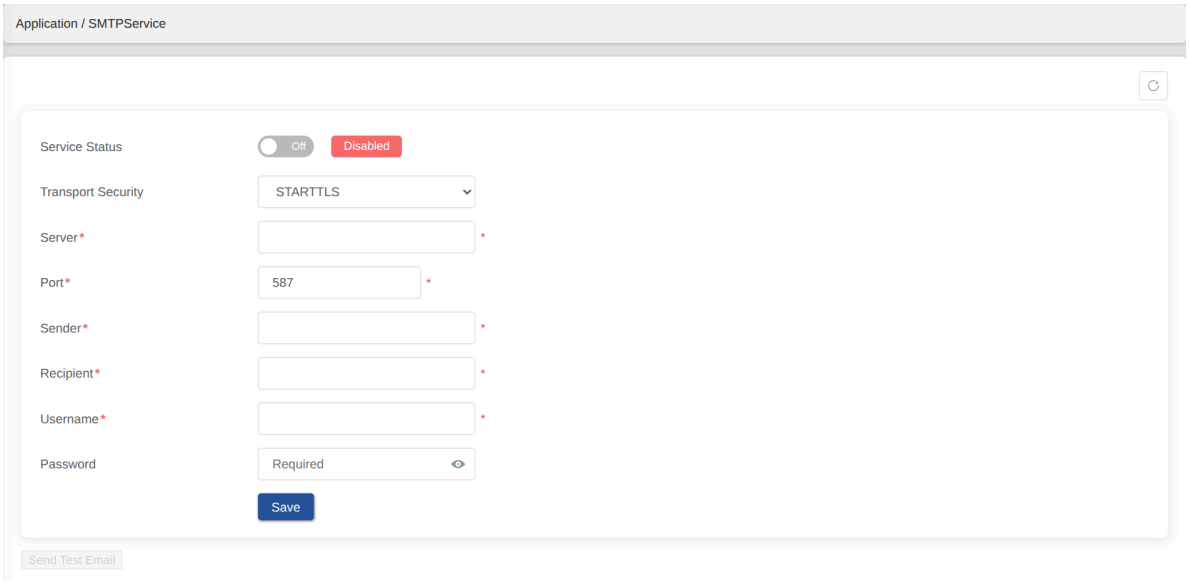



Figure 5-17 SMTP mail service

## FIELD TASK: SEND A TEST EMAIL BEFORE ENABLING EMAIL ALARMS

Obtain SMTP host, submission port, NONE/STARTTLS/TLS mode, account, app password, allowed sender and recipient from the mail administrator. Verify device time and DNS first.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Server / Port | Administrator SMTP host / matching submission port | Use the matching port/security pair, not an assumed465 |
| Transport Security | Administrator-specified NONE/STARTTLS/TLS | Match server; do not bypass certificate errors by disabling TLS |
| Sender / Recipient | Authorized sender / test recipient | Full addresses |
| Username / Password | Sender account / SMTP app password | Follow provider; may differ from the mailbox login password |

## SAVE, TEST AND OBSERVE

1. Save fields, then click Send Test Email. Record device result/time and have the recipient inspect inbox and spam.
2. Only after receipt, enable email in Alarm, select a safely testable event and compare event/email timestamps.

## PASS CRITERIA AND DIAGNOSIS

Timeout: inspect DNS/port. Auth fails: inspect app password/sender permission. TLS fails: inspect time/certificates/mode. Accepted but missing mail: inspect bounces, spam and recipient.

**Finish and restore:** Remove test recipients/alarms while retaining production settings; deliver app passwords securely.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Server / Port | SMTP server and its submission port |
| 2 | Transport Security | Match NONE, STARTTLS or TLS to the mail provider |
| 3 | Sender / Recipient | Use complete mail addresses; sender must satisfy the server policy |
| 4 | Username / Password | Use the mail account credential or app password, not the router Web password |
| 5 | Send Test Email | Verify receipt after configuring the service, before relying on mail alarms |

**Check the result** The destination mailbox receives the test or actual notification with the intended time and recipient

CHAPTER

# 06

# VPN

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 6. VPN

## 6.1 Choose remote access and tunnels

| SITE REQUIREMENT | START HERE | CONDITION |
|---|---|---|
| No site public IP; remote maintenance | m2mCloud or ZeroTier | Authorization→tunnel IP→site service |
| Existing corporate VPN server | OpenVPN or IPsec | Obtain complete endpoint, certificates/PSK and routes |
| Controlled peers; encrypted site access | WireGuard | Start split routes before changing default egress |
| Specific GRE/VXLAN/DMVPN deployment | Corresponding tunnel case | Physical peer→tunnel IP→LAN/return routes |

### CHOOSE BY YOUR PROBLEM

| PROBLEM | SELECTION PATH | PREREQUISITES |
|---|---|---|
| 4G only, no public IP, remote PLC work | Use matching authorized m2mCloud, or a suitable client to an existing reachable enterprise VPN | Platform/client, outbound path, vendor tool and PLC return route; DDNS alone is insufficient |
| Existing OpenVPN / IPsec / WireGuard | Reuse a supported reachable peer with its actual keys/certificates and networks | Matching peer settings, authorization, Allowed IP/policies and return path |
| Vendor tool needs broadcast discovery | Verify available L2 bridging and bind the virtual NIC | Unique addresses and actual broadcast tests; L3 connectivity is not discovery |
| Different site subnets, explicit IP access | Plan L3 routed access | Non-overlapping sites, forward/return routes and access controls |
| Office and site use the same subnet | Prefer renumbering; otherwise test the client's explicit overlap policy | No unplanned bridging; record local reachability and rollback |
| Multiple devices/sites | Define site IDs, subnets, authorization and access scope before VPN/platform setup | Online devices do not establish LAN-to-LAN reachability; test each site and cross-site service |

Confirm each server/platform address, authorization and maintenance owner; for formal handover, record them in Service acceptance and handover. VPN support does not replace connectivity, peer, identity and engineering-tool compatibility checks.

### THEN CHECK PROTOCOL AND PEER REQUIREMENTS

Start with your server, platform and protocol, then distinguish explicit-IP access from LAN broadcast discovery. No public IP does not make a local server externally reachable.

| EXISTING PEER OR NEED | ENTRY | NETWORK PREREQUISITE | ACCESS AND SECURITY BOUNDARY |
|---|---|---|---|
| Matching maintenance platform | m2mCloud | Matching PC client, device authorization and Internet access | Platform provisions L2/L3; confirm P2P/relay and security with the delivered service |
| Service and certificates supplied | OpenVPN client | Reachable server and transport port | Match certificates/keys; still configure site routes |
| Key-based tunnel at both ends | WireGuard | A genuinely reachable peer/mapped path | Encrypted L3; plan allowed IPs, return paths and full-tunnel exits separately |
| Enterprise firewall peer | IPsec | Matching policies, authentication and negotiation reachability | Protects agreed IP traffic; does not resolve address overlap or broadcast discovery |
| Existing ZeroTier network | ZeroTier | Controller approval and suitable network paths | Joining the virtual network does not configure all LAN routes and permissions |
| Existing L2TP/PPTP installation | Matching client/server | Compatible peer and reachability | L2TP itself does not encrypt data; PPTP is not recommended for new security-sensitive projects |
| Existing encapsulation requirement | GRE / VXLAN | Reachable outer addresses and encapsulation traffic | GRE/VXLAN do not provide encryption by themselves |

### TWO COMMON DECISIONS

- PLC broadcast discovery requires an applicable L2 service at the platform/peer. An online L3 tunnel does not forward LAN broadcasts automatically.
- A server on this gateway needs an actual path to its listening address and port. Enabling a server, DDNS or cellular access alone does not create inbound reachability.

For new projects, use an encrypted tunnel or authorized platform supported by the delivery and suitable for your security policy. Configure identity, access rules and vendor-tool permissions separately.

**Configuration entries**: 6.2 OpenVPN clients • 6.4 WireGuard • 6.6 IPsec • 10.1 Client configuration and networking

## 6.2 OpenVPN clients

Path VPN > OpenVPN Client

Two OpenVPN clients and a server can operate independently. Each instance has separate connection/authentication settings and needs appropriate business routes.

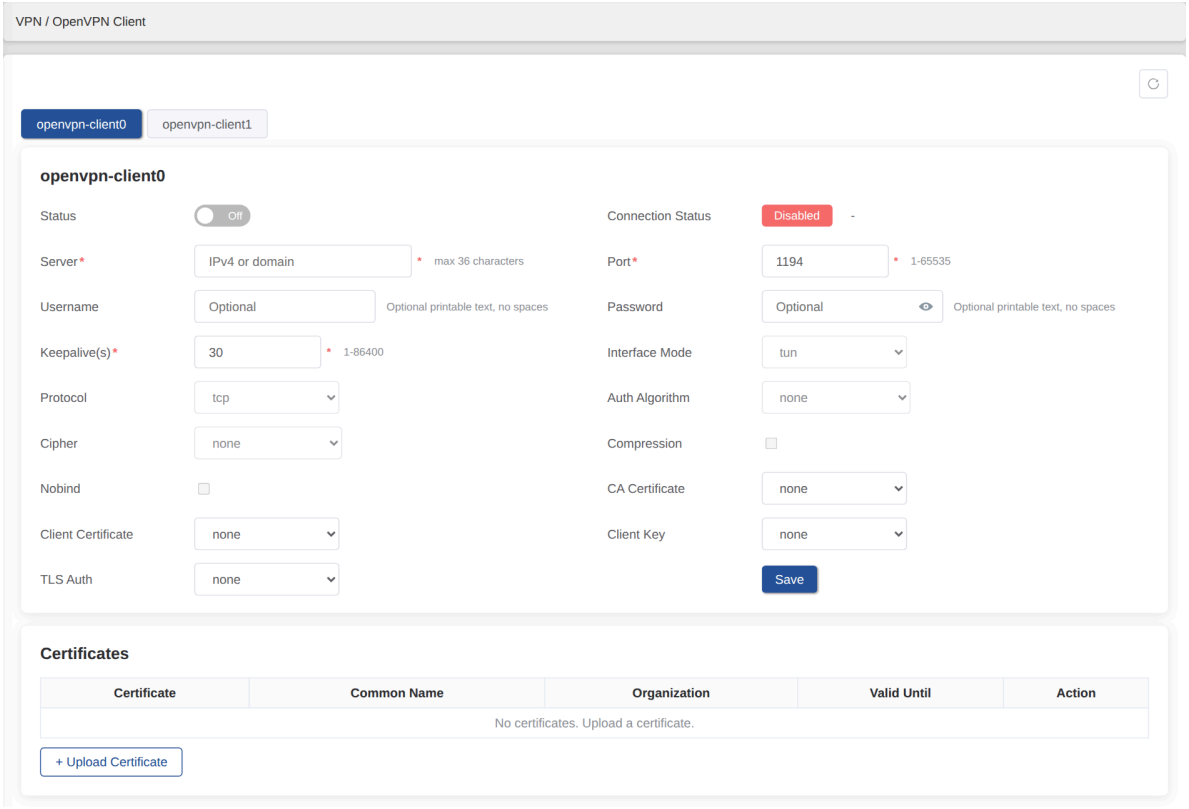



Figure 6-1 OpenVPN clients

### FIELD TASK: IMPORT A COMPLETE OPENVPN CLIENT HANDOVER

Build the server case first or obtain the complete client bundle and allowed LAN routes from the VPN administrator. Do not mix CA/key files from different projects.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Server / Port / Protocol | 192.168.20.3 / 1194 / UDP | Lab server; production follows remote/proto in the profile |
| Interface Mode | TUN | Match server |

| UI FIELD | ENTRY | BASIS |
| --- | --- | --- |
| CA / Certificate / Private Key | bundle files | Upload separately; protect private key |
| Username / Password | only if required | Not Web admin credentials |

### SAVE, TEST AND OBSERVE

1. Select the client instance, copy algorithms/certificates/optional TLS auth from the bundle, upload each file, save and enable. Record Connected, virtual IP and routes.
2. Test server virtual IP, then an authorized remote service from a LAN PC; confirm the original uplink still behaves as planned.

### PASS CRITERIA AND DIAGNOSIS

TLS failure: inspect CA/time/transport. AUTH_FAILED: inspect VPN account. Connected without service: inspect pushed routes, target firewall and return path.

**Finish and restore:** Disable the instance and restore routes; do not bypass all certificate checks to resolve a mismatch.

Use the remote-access decision section to confirm the peer, certificates and reachability, then follow the client settings below. Both clients and the server use separate configurations; verify service routes after connection.

### CHOOSE A CLIENT INSTANCE AND CONFIGURE THE CONNECTION

openvpn-client0 and openvpn-client1 maintain their own servers, authentication and routes. Configure one or both as required; the server is configured separately.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
| --- | --- | --- |
| 1 | Client Instance | Configure openvpn-client0 and openvpn-client1 separately; two clients and a server operate independently |
| 2 | Server / Port / Protocol | Match the server address, port and TCP/UDP transport |
| 3 | Interface Mode | tun is routed Layer 3 and tap is Layer 2; match the intended design at both ends |
| 4 | Username / Password | Use when account authentication is required; it does not replace required certificates |
| 5 | Auth Algorithm / Cipher | Match peer settings and use values compatible with the selected certificates and authentication |
| 6 | Keepalive / Compression / Nobind | Configure for server and NAT conditions, keeping peer parameters consistent |

## UPLOAD AND SELECT CERTIFICATES, THEN CHECK THE CONNECTION

Obtain the CA, client certificate and matching private key from the server administrator. Upload the required files with Upload Certificate, then select them in the client. Check identities and validity; use TLS Auth and other options as required by the server.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | CA | Validates the peer certificate trust chain; commonly ca.crt, provided by the VPN administrator |
| 2 | Certificate | Identifies this client and must match its private key; assign identities according to server policy |
| 3 | Private Key | Select the matching client key; do not distribute a server private key to clients |
| 4 | TLS Auth | Use when the server requires the corresponding control-channel authentication; match its file and direction requirements |
| 5 | Upload Certificate | Upload the required files, select them in connection settings, then save the connection; uploading does not establish a tunnel |
| 6 | Connected / Virtual IP | After connection, inspect state and the tunnel address, then check remote-subnet routes and service access |

**Check the result** The intended client connects and the remote target IP and service are reachable

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Connected but remote equipment is unreachable | Check service subnets, routes/pushed routes, return routing and firewall rules on both sides. Test the target IP before its service port. |

# 6.3 OpenVPN server

Path VPN > OpenVPN Server

As a server, the router accepts client connections. Reachability, certificate identity, tunnel pools and routes must be configured together.

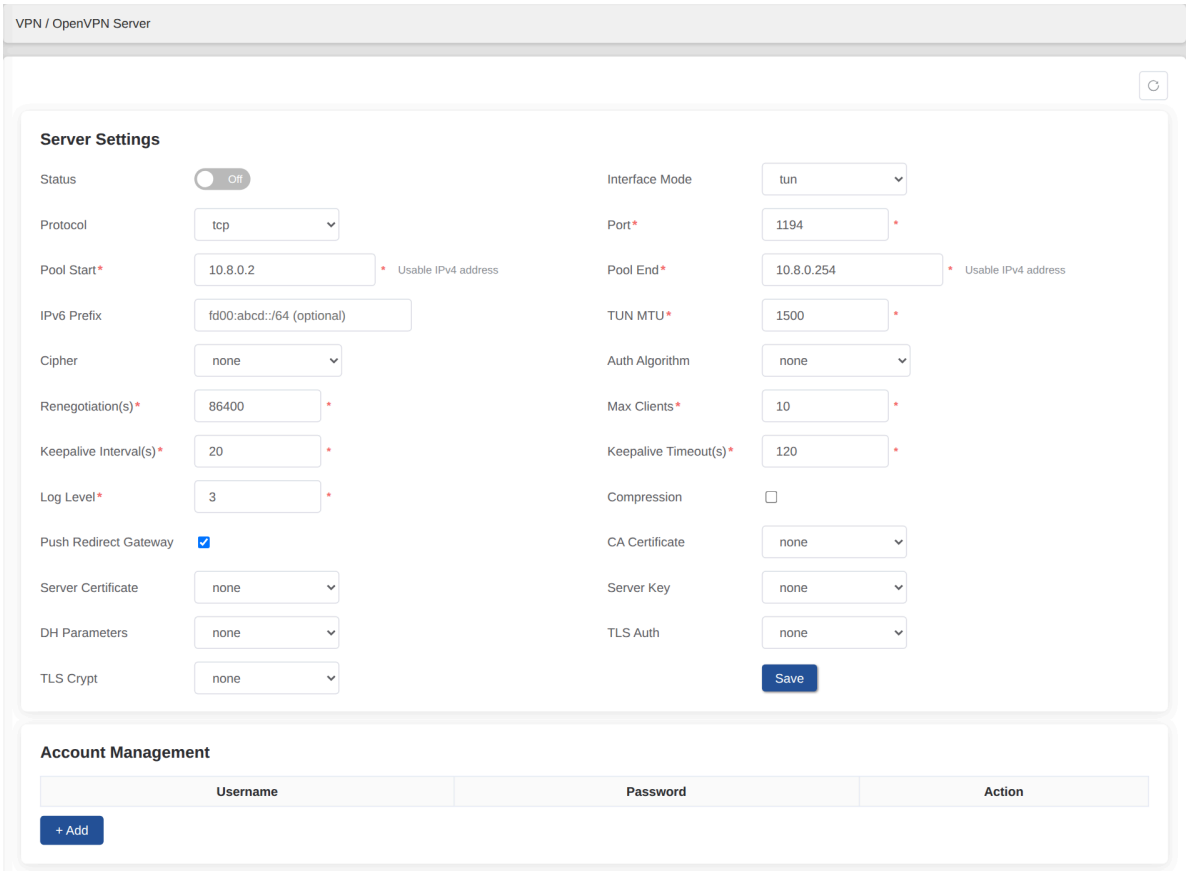



Figure 6-2 OpenVPN server (1/2)

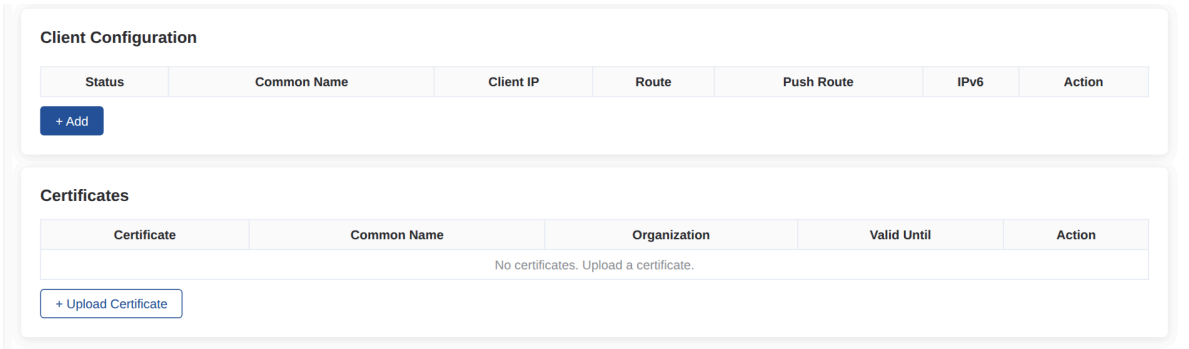



Figure 6-3 OpenVPN server (2/2)

## FIELD TASK: BUILD AN OPENVPN SERVER AND EXPORT A CLIENT PROFILE

Build the server on reachable gateway B, WAN 192.168.20.3 and LAN 192.168.30.1/24. Synchronize time. Obtain a matching CA, server certificate/key and client certificate/key with correct usages from the project VPN administrator.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode / Protocol / Port | TUN / UDP / 1194 | Match both endpoints |
| Pool Start / End | 10.45.0.2 / 10.45.0.20 | No overlap with either LAN |
| Server Certificates / Key / CA | administrator-issued files | Do not substitute a client certificate |
| Push Route | 192.168.30.0/24 | Use the page’ s network/mask syntax |

## SAVE, TEST AND OBSERVE

1. Upload certificates/keys. Configure DH/TLS-auth files, cipher and authentication from the same server plan. Save, enable and export the client profile.
2. Import on the client, checking remote 192.168.20.3, port1194 and all required files. Connect and test assigned tunnel IP and a real subnet-30 service.

## PASS CRITERIA AND DIAGNOSIS

Certificate failure: check time, CA, usage and key matching. Connected without LAN access: check push route and return path to 10.45.0.0/24. Client-LAN routing additionally needs server routes/client-subnet association.

**Finish and restore:** Disable the server, revoke test client certificates, remove routes and protect exported keys.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable / Mode / Protocol / Port | Define the server listener consistently with client configuration |
| 2 | Pool Start / End | Tunnel addresses assigned to clients; avoid overlap with LAN and other tunnels |
| 3 | Cipher / Auth / MTU | Coordinate these parameters with client compatibility |
| 4 | Server Certificates / DH / TLS | Provide the server certificates, private key and negotiation material required by the selected mode |
| 5 | Account / Client Configuration | Maintain VPN client authentication and assignment rules, not router Web multi-user accounts |
| 6 | Route / Push Route | Configure reachable subnets and return routes, not only the address pool |
| 7 | Keepalive / Maximum Clients | Set for the service and delivered runtime environment |

**Check the result** An authorized client obtains the expected tunnel address and reaches services allowed by routes and policy

# 6.4 WireGuard

Path VPN > WireGuard

WireGuard uses peer keys and UDP endpoints. Plan tunnel and business addressing before exchanging public keys.

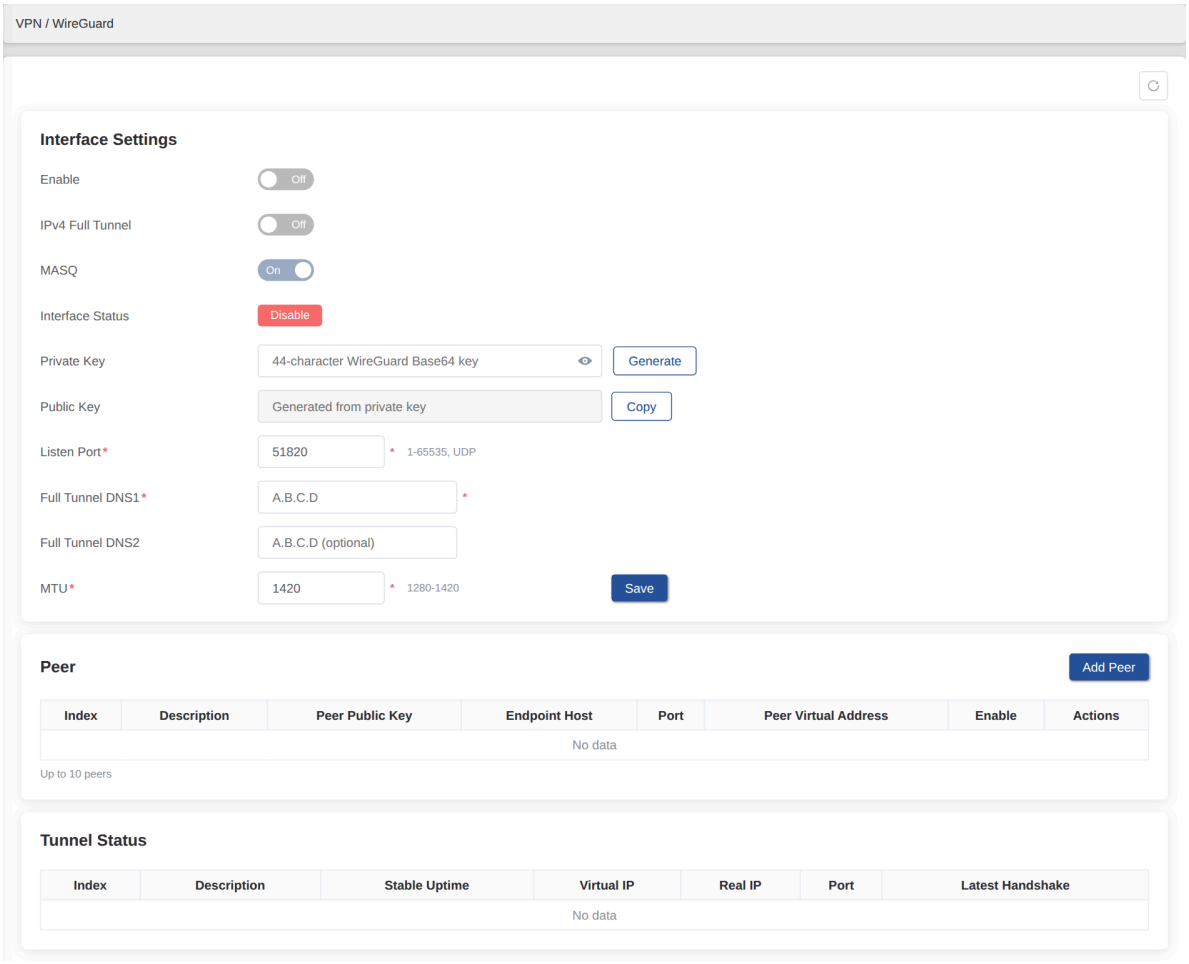



Figure 6-4 WireGuard

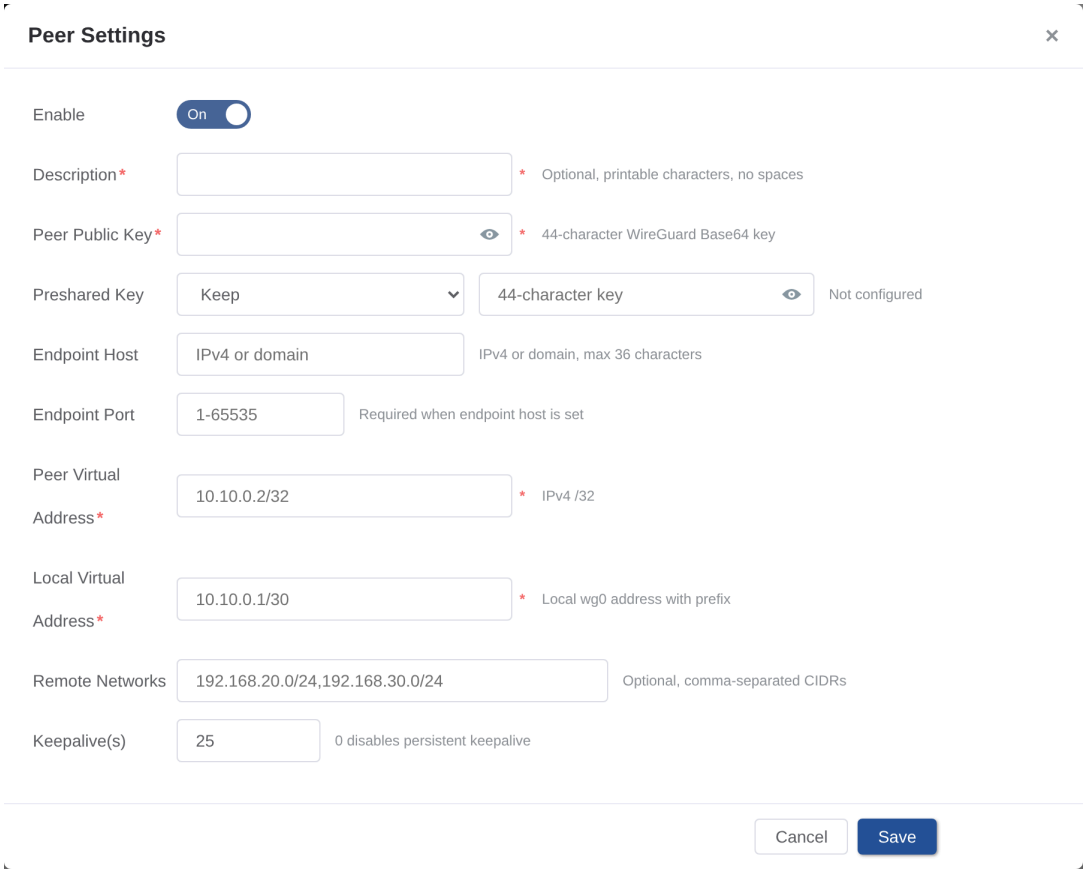



Figure 6-5 WireGuard

Native unsaved form / browser draft; not applied to device

## FIELD TASK: MINIMUM WIREGUARD PLAN FOR TWO LANS

A is this gateway: WAN 192.168.20.2, LAN 192.168.10.1/24. B is another gateway: WAN 192.168.20.3, LAN 192.168.30.1/24. Prove WAN reachability and allow UDP51820. For production replace endpoints with reachable public addresses/ports.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable / Listen Port / Full Tunnel | On / 51820 / Off | Start split routing without taking over the default route |
| Private Key / Public Key | Generate / Copy | Click Generate on each end; Copy its public key to the peer, never its private key |
| Peer Enable / Description | On / siteB on A; siteA on B | Add a unique peer description |
| Peer Public Key | copied peer public key | Not the peer private key |
| Local Virtual Address A / B | 10.44.0.1/30 / 10.44.0.2/30 | Local wg0 address with prefix; unique on each end |
| Peer Virtual Address A / B | 10.44.0.2/32 / 10.44.0.1/32 | Peer virtual address uses /32 |
| Endpoint Host A / B | 192.168.20.3 / 192.168.20.2 | Host IP only, without colon/port |

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Endpoint Port / Keepalive(s) | 51820 / 25 | Separate port field; keepalive in seconds |
| Remote Networks A / B | 192.168.30.0/24 / 192.168.10.0/24 | Remote application subnet |

### SAVE, TEST AND OBSERVE

1. Configure B then A, each with the other public key, addresses and subnets. Save and enable. If the delivered form lacks listed local-address/subnet fields, use that release' s interface/routing settings; do not enter values into unrelated fields.
2. From 192.168.10.10 access an active service at 192.168.30.10; from 192.168.30.10 access 192.168.10.10:8080. Inspect recent handshake and traffic counters in both directions.

### PASS CRITERIA AND DIAGNOSIS

No handshake: inspect endpoint, UDP and keys. Handshake but no LAN traffic: inspect remote subnets, client gateways, firewall and return routes. Keep full tunnel off initially.

**Finish and restore:** Disable test peers and restore routes; protect private keys outside public acceptance records.

**Relation to Load Balance:** choose the outbound design before enabling WireGuard IPv4 Full Tunnel. The current firmware does not allow it and Load Balance to be enabled together. Updated handshakes still require target-service and return-path checks.

### WHAT TO ENTER IN THE PEER ADDRESS FIELDS

The current configuration interface uses IPv4. **Independent example W1:** the local LAN is 192.168.50.0/24 and the remote LAN is 192.168.20.0/24. These are entry examples, not a completed two-peer tunnel test.

| UI FIELD | EXAMPLE AND PURPOSE ON THIS ROUTER |
|---|---|
| Local Virtual Address | 10.0.0.2/32, the local wg0 address |
| Peer Virtual Address | 10.0.0.1/32, the peer tunnel address; use /32, not the remote LAN subnet |
| Remote Networks | 192.168.20.0/24, the business subnet reached through this peer; comma-separate multiple subnets |
| Endpoint Host / Endpoint Port | For an initiating connection, enter the reachable peer and UDP port together, not a tunnel-internal address |

The peer needs the matching public key, reversed tunnel addresses and routes/access rules to the local LAN. Configure a preshared key only when agreed at both ends; Keep retains its existing value. Leave IPv4 Full Tunnel off when only remote business subnets are required. Before using full tunnel, check default-route ownership, keepalive requirements and the load-balancing exclusion.

Save the peer and base settings separately and check both enable states. Generate traffic to the peer tunnel address, inspect the handshake, then test the remote business IP. If the handshake succeeds but the service fails, check remote networks, local addressing, return paths and access rules. Resolve address/route conflicts by checking overlapping peer addresses and subnets.

This version provides IPv4 tunnels and up to 10 peers; a preshared key is optional. This is a model-specific configuration limit, not a throughput guarantee.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable / Private Key / Public Key | Keep the local private key private and share its public key with the peer; use distinct identities |
| 2 | Listen Port / MTU | Set the local UDP listener and MTU for the network path |
| 3 | IPv4 Full Tunnel / DNS | Full tunnel affects egress and DNS; enable only when that routing behavior is intended |
| 4 | Peer Public Key / Endpoint | The key identifies the peer; endpoint is its reachable address and UDP port |
| 5 | Peer Virtual Address | Peer Virtual Address is the peer tunnel IPv4 address with /32. Enter the local wg0 address in Local Virtual Address and business subnets separately in Remote Networks. |
| 6 | MASQ / Runtime | Choose masquerading according to return routing and check actual handshake and traffic |

**Check the result** Handshakes update, traffic counters change and the target service works with a valid return path

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| No handshake, or no traffic after handshake | Check public keys, endpoint and UDP reachability first, then AllowedIPs, tunnel addressing and return routes. |

# 6.5 ZeroTier

Path VPN > ZeroTier

The router joins a ZeroTier network as an authorized node. Address and route acceptance depends on local settings and controller rules.

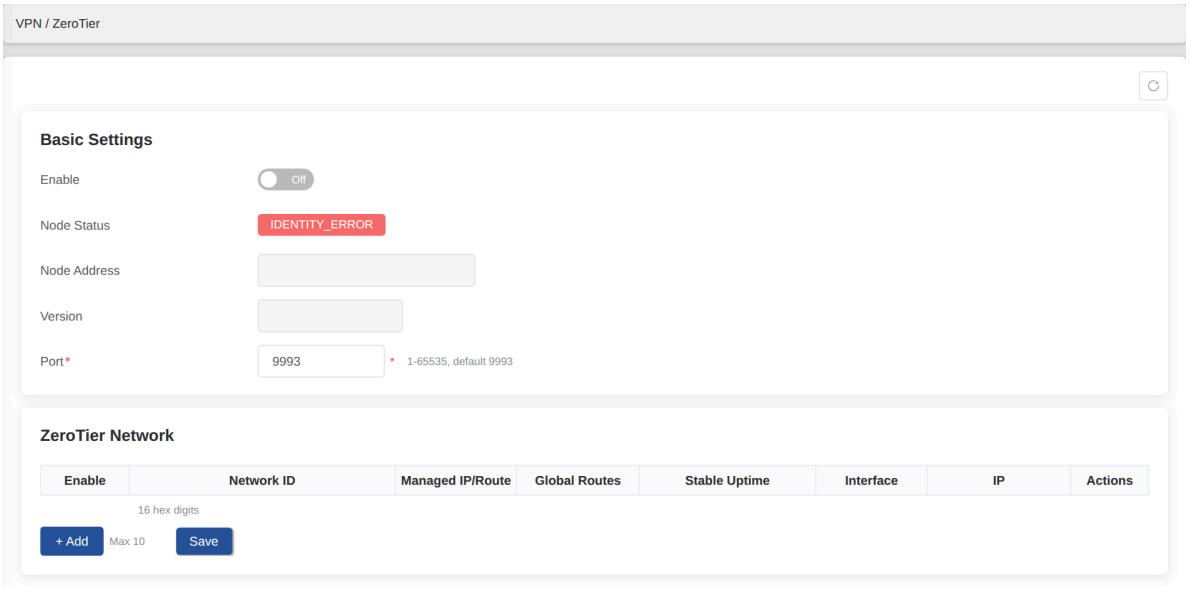



Figure 6-6 ZeroTier

## FIELD TASK: AUTHORIZE BOTH ENDS, THEN TEST MANAGED IP AND SITE LAN

Create a controller network and obtain its 16-hex-digit Network ID. Install the remote client. Authorize both nodes and use their actually assigned managed IPs.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable / Network ID | On / controller Network ID | Network ID, not node ID |
| Managed Route | 192.168.10.0/24 via gateway managed IP | Configure on controller; avoid remote-LAN overlap |

## SAVE, TEST AND OBSERVE

1. Join both ends, authorize in controller and record managed IPs. Test them first, then inspect the remote PC site route.
2. Access site 192.168.10.10:8080 and inspect bidirectional traffic. Keep Global Routes off initially unless the project explicitly requires a default-route change.

## PASS CRITERIA AND DIAGNOSIS

No IP: inspect network ID/authorization. Managed IP works but LAN fails: inspect managed route, forwarding/return and client gateway. Recreated-interface uptime differs from system uptime.

**Finish and restore:** Leave the test network, revoke routes/node authorization and inspect original routes.

After controller authorization, still verify the virtual address, required routes and target service. Recreating the ZeroTier interface restarts its online duration; that value is neither system uptime nor proof the whole project has never been interrupted.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable / Node Status | Start the client and confirm that the node identity is valid |
| 2 | Network ID | Use the platform network identifier, not the device serial number |
| 3 | Authorization | Authorize the node at the network controller, then inspect assigned addresses |
| 4 | Managed IP / Route | Choose whether to accept controller-provided addresses and routes |
| 5 | Global Routes | Coordinate broader route acceptance with the existing egress plan |
| 6 | Port / Interface / IP | Check service port, virtual interface and actual assignment |

**Check the result** The node is authorized, has a virtual address and reaches required peers and services

## 6.6 IPsec

Path VPN > IPsec

IPsec protects selected IP traffic with matching peer policies. Define peer, authentication and protected networks, not just encryption algorithms.

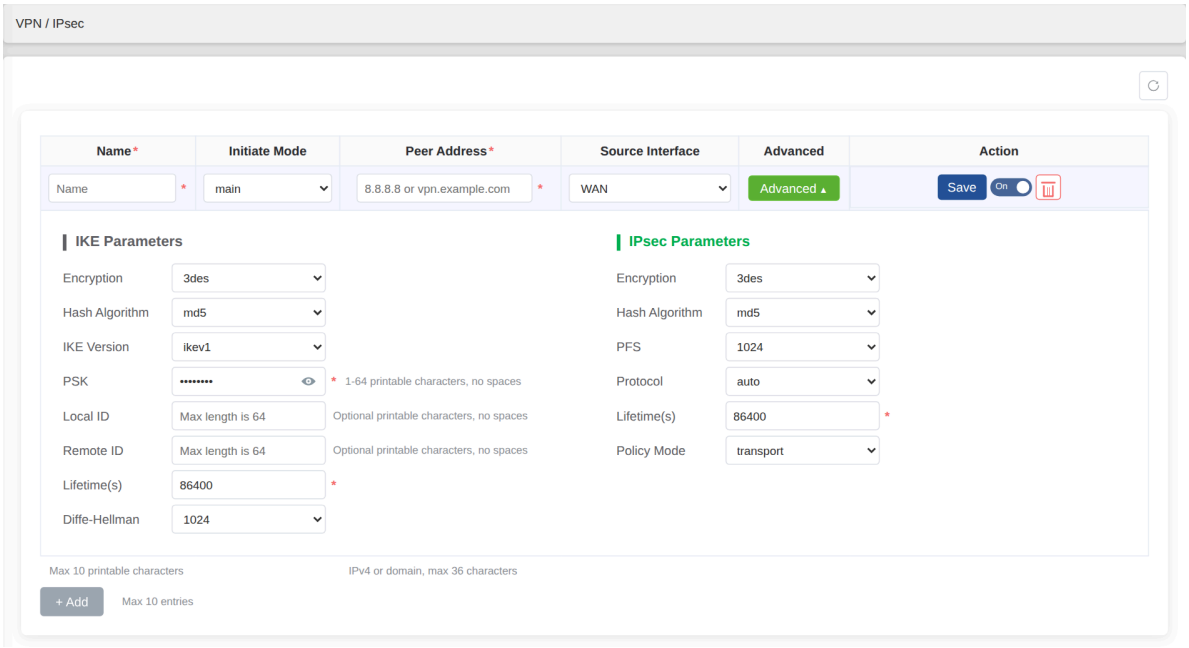



Figure 6-7 IPsec

Native unsaved form / browser draft; not applied to device

### FIELD TASK: CONNECT TWO SITES WITH SYMMETRIC IPSEC SELECTORS

A: WAN 192.168.20.2, LAN 192.168.10.0/24; B: WAN 192.168.20.3, LAN 192.168.30.0/24. Prove peer reachability first. Public/NAT deployment requires actual peer addresses and NAT-T policy.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Name / Transport | siteA / Tunnel | Names may differ; policies must match |
| Peer Address A / B | 192.168.20.3 / 192.168.20.2 | Physical peers |
| Local / Remote Network A | 192.168.10.0/24 / 192.168.30.0/24 | Reverse on B |
| Authentication / PSK | PSK / LabIpsec2026 | Lab-only; match both ends |
| IKE / Child SA | IKEv2 / AES128-SHA256 / DH14-PFS14 | Choose only if supported at both ends; lifetime3600s |

### SAVE, TEST AND OBSERVE

1. Match local/remote identities and algorithms, save B then A and initiate. Inspect both IKE and Child SAs.
2. Access the 192.168.30.10 application from 192.168.10.10 and inspect encryption/decryption counters increasing both ways; test the reverse direction.

### PASS CRITERIA AND DIAGNOSIS

IKE failure: inspect PSK, identities, UDP500/4500 and proposals. Child failure: inspect selectors/PFS. SAs up without service: inspect client gateways, return path and firewall.

**Finish and restore:** Disable test tunnels/policies on both ends and confirm original services.

### ADVANCED SETTINGS AND PROTECTED SUBNETS

Save and enable each rule separately. Expand Advanced to match IKE and Child SA algorithms, lifetimes, DH/PFS, PSK and identities. Phase lifetimes are 120–86400 seconds. Tunnel mode requires complete local/remote policy subnets. Configure Transport mode for the actual protected traffic instead of inserting unrelated LAN subnets. After saving, inspect application results, negotiation, policy routes and traffic in both directions.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Name / Initiate Mode | Name the rule and match exposed negotiation modes such as main/aggr to the peer |
| 2 | Peer Address / Source Interface | Set the reachable peer and local egress for negotiation |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 3 | Transport / Tunnel | Select for the protected traffic and peer policy; the modes represent different designs |
| 4 | Authentication / Encryption | Coordinate credentials/identity, algorithms and negotiation parameters at both ends |
| 5 | Local / Remote Network | Define protected traffic and valid return routing |
| 6 | Status / Logs | Check both negotiation success and protected traffic forwarding |
| 7 | Tunnel / Transport mode | Tunnel protects corresponding local/remote subnets; Transport follows the intended endpoint design. |
| 8 | Phase lifetimes | Configure IKE and Child SA lifetimes separately within 120–86400 seconds and match the peer agreement. |

**Check the result** Negotiation succeeds and actual services across protected subnets work in both directions

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Negotiation fails or protected subnets are unreachable | Compare negotiation logs and settings on both peers, then subnets, routes and firewall rules; algorithm names alone are insufficient. |

## 6.7 L2TP client

Path VPN > L2TP Client

The client establishes L2TP with server-assigned credentials. L2TP itself does not encrypt; configure the required separate protection when needed.

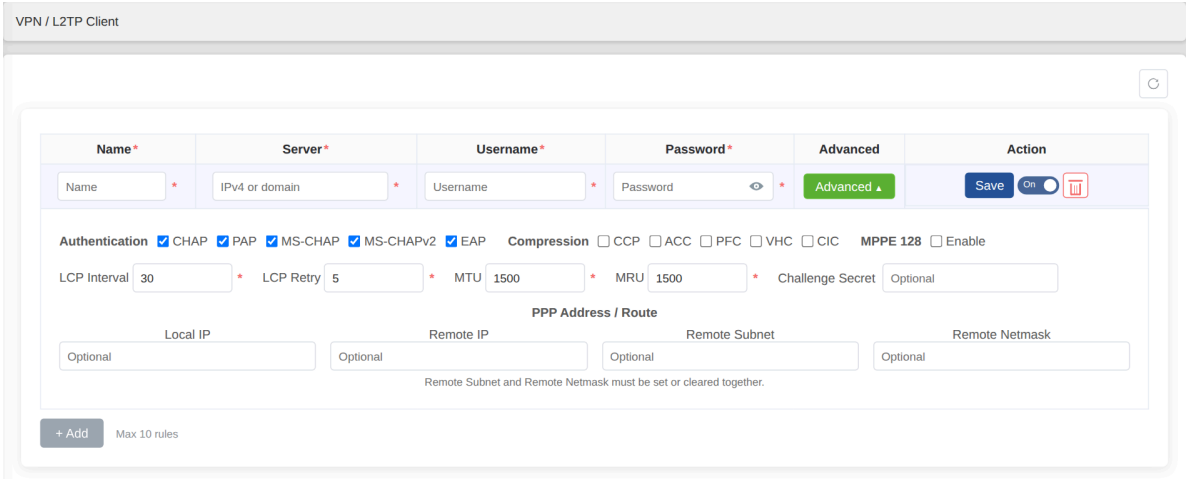



Figure 6-8 L2TP client

Native unsaved form / browser draft; not applied to device

## FIELD TASK: L2TP CLIENT TO AN ISOLATED TEST SERVER

Configure the corresponding server at 192.168.20.3 first; this gateway WAN is .20.2. Encryption limits are detailed below; these protocols alone do not replace a required encrypted VPN.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Server | 192.168.20.3 | Reachable lab server |
| Username / Password | field / LabTunnel2026 | Matching lab credentials |
| Authentication / Compression / MPPE | match server | Match server settings as a set |
| MTU / MRU | 1400 / 1400 | Use if supported; retain planned LCP settings |

## SAVE, TEST AND OBSERVE

1. Save/enable, inspect session/assigned IP and test server tunnel IP. LAN access additionally needs bilateral routes and return paths.
2. Access an active remote test service and record the result; configure PPTP server pool/accounts/DNS using its server field reference below.

## PASS CRITERIA AND DIAGNOSIS

Auth fails: inspect credentials/negotiation. L2TP: inspect UDP1701 and any separate IPsec protection. PPTP: inspect TCP1723 and GRE protocol47. LAN failure after tunnel connects: inspect routes/gateways.

**Finish and restore:** Disable the client and remove temporary routes/server lab accounts.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Name / Server | Name the connection and set a reachable server |
| 2 | Username / Password | Match the PPP credentials assigned by the server |
| 3 | Authentication / Compression | Use options supported by the server, not arbitrary combinations |
| 4 | LCP / MTU / MRU | Set link maintenance and transmit/receive sizes according to the peer |
| 5 | Routes | Provide destination and return routes, rather than only testing login |
| 6 | Encryption boundary | L2TP itself does not encrypt traffic; configure matching IPsec or other protection when required |

**Check the result** The client connects and routes provide access to the target subnet and service

> L2TP itself does not encrypt data. Login authentication is not encryption; separately confirm the required protection arrangement.

## 6.8 L2TP server

Path VPN > L2TP Server

The server authenticates clients and assigns tunnel addresses. Avoid pool overlap with LAN, other VPNs or remote site networks.

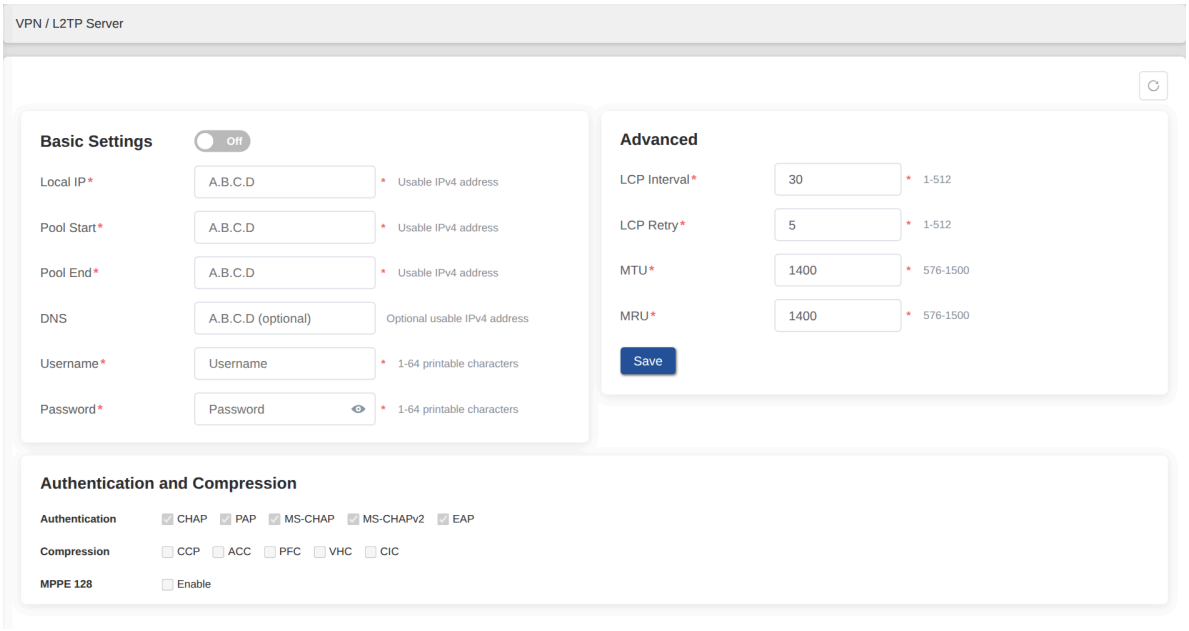



Figure 6-9 L2TP server

### FIELD TASK: CREATE A MINIMAL L2TP DIAL-IN ACCOUNT

Operate on server WAN 192.168.20.3; client WAN .20.2. Pool must not overlap LAN/WAN. L2TP alone is unencrypted; apply the required project protection separately.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Local IP | 10.49.0.1 | Server tunnel address |
| Pool Start / End | 10.49.0.2 / 10.49.0.10 | Client pool |
| Username / Password | field / LabTunnel2026 | Isolated lab account |
| DNS | reachable DNS | Follow form requirements if optional |
| MTU / MRU / LCP | 1400 / 1400 / keep current | Match the client plan |

### SAVE, TEST AND OBSERVE

1. Save server/account and enable. Connect with the L2TP client case, verify pool assignment and test tunnel IP and real service.

### PASS CRITERIA AND DIAGNOSIS

No session: inspect UDP1701/auth. Session without LAN: inspect routes, client gateways and return paths.

**Finish and restore:** Disable the test server and remove its account/routes.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Local IP / Pool Start / End | Server tunnel address and client pool must be consistent and non-conflicting |
| 2 | DNS | DNS resolver delivered to clients |
| 3 | Username / Password | Credentials for tunnel access, not a router administration-account creation page |
| 4 | Authentication / Compression / MPPE | Match exposed options to client capabilities; they do not establish IPsec by themselves |
| 5 | LCP / MTU / MRU | Configure tunnel link checks and transmit/receive sizes |

**Check the result** An authorized client connects, receives addressing and reaches the required service

## 6.9 GRE

Path VPN > GRE

GRE encapsulates traffic between reachable peers without encrypting it. Configure outer addresses, inner addresses and routes separately.

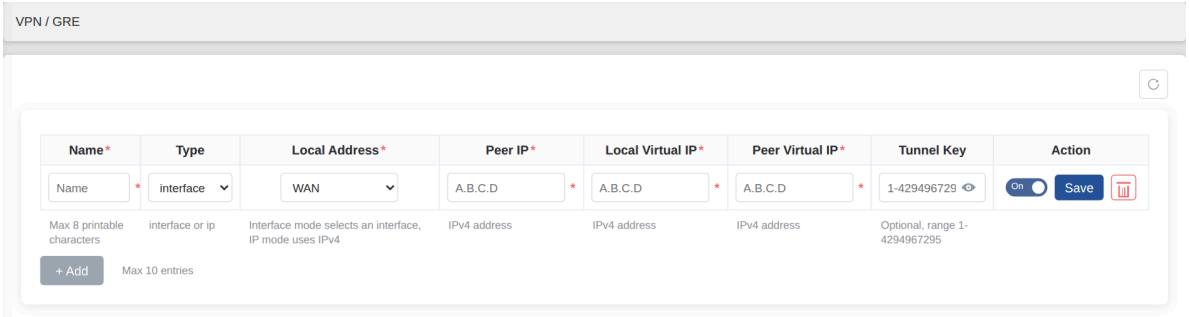



Figure 6-10 GRE

Native unsaved form / browser draft; not applied to device

### FIELD TASK: BUILD GRE AND ROUTE THE REMOTE LAN

A WAN 192.168.20.2/LAN 192.168.10.1; B WAN 192.168.20.3/LAN .30.1. Permit IP protocol47, not TCP port47. GRE itself is unencrypted.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Name / Type | gretest / ip | For interface binding select the real uplink |
| Local / Peer Address A | 192.168.20.2 / 192.168.20.3 | Reverse on B |
| Local / Peer Virtual IP A | 10.46.0.1 / 10.46.0.2 | Use the same tunnel subnet with the page prefix fields |
| Tunnel Key | 100 | Same on both; not an encryption key |

### SAVE, TEST AND OBSERVE

1. Save/enable both ends, test peer tunnel IP, then route subnet30 via10.46.0.2 on A and subnet10 via10.46.0.1 on B.
2. Test actual LAN services both ways and inspect tunnel counters. If only large packets fail inspect MTU before changing unrelated settings.

### PASS CRITERIA AND DIAGNOSIS

Physical peer works but tunnel fails: inspect protocol47, binding and key. Tunnel works but LAN fails: inspect routes, client gateways and firewall.

**Finish and restore:** Delete added LAN routes, then disable the GRE test tunnels.

The new rule Type is ip or interface, selecting local binding rather than encryption. ip uses a local physical address; interface binds an actual source interface. Then configure physical peer, local/peer virtual addressing and a matching tunnel key. The 1–4294967295 key identifies the tunnel; it is not an encryption password.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Name / Type | Name the tunnel and choose interface- or local-IP-based egress |
| 2 | Local Address / Peer IP | Reachable outer addresses, not tunnel-internal addresses |
| 3 | Local / Peer Virtual IP | Plan inner addresses and routes to destination networks |
| 4 | Tunnel Key | Match as required to distinguish tunnels; it is not an encryption key |
| 5 | Protocol boundary | GRE encapsulation does not encrypt traffic; verify service routing after establishment |

**Check the result** Tunnel endpoints are reachable, tunnel/service routes are correct and the target service works

# 6.10 VXLAN

Path VPN > VXLAN

VXLAN carries a Layer-2 network over IP. Match identifiers, outer connectivity and bridging scope and plan the resulting broadcast domain. VXLAN itself does not encrypt data; use a confirmed protection arrangement where confidentiality is required.

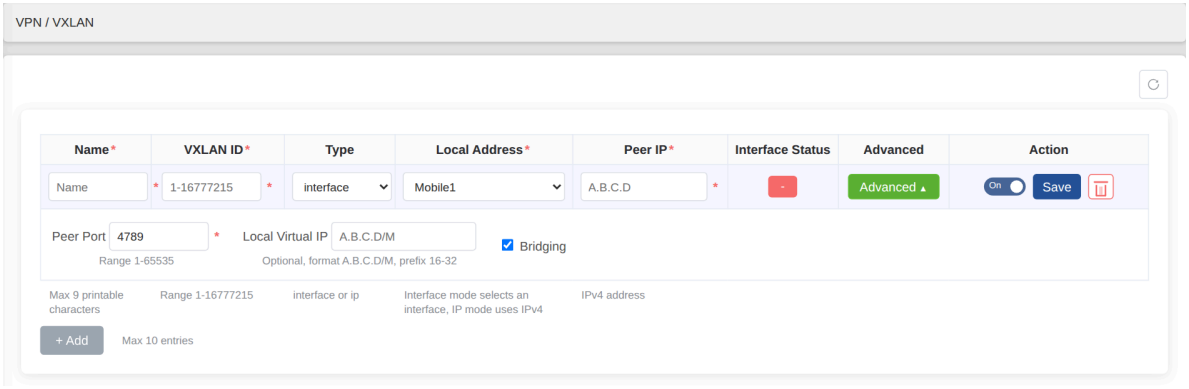



Figure 6-11 VXLAN

Native unsaved form / browser draft; not applied to device

## FIELD TASK: VERIFY VXLAN ENCAPSULATION ON AN ISOLATED NETWORK

Prove WAN 192.168.20.2/192.168.20.3 reachability. Use separate test interfaces; do not bridge active site LANs together and create loops or duplicate DHCP servers.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Name / VXLAN ID | vxlab / 100 | Match VNI |
| Type / Local Address A | ip / 192.168.20.2 | B uses 192.168.20.3 |
| Peer IP / Peer Port A | 192.168.20.3 / 4789 | B peer 192.168.20.2, matching UDP port |
| Local Virtual IP A / B | 10.47.0.1/30 / 10.47.0.2/30 | Use same-subnet values in the form syntax |

## SAVE, TEST AND OBSERVE

1. Save/enable both ends, inspect interfaces/encapsulation counters and test virtual IPs. Bridge only if the delivered page supports it and an explicit L2 plan requires it, keeping one DHCP server.

## PASS CRITERIA AND DIAGNOSIS

Inspect UDP4789, VNI and physical peers on failure. VXLAN is not intrinsically encrypted; virtual IP connectivity does not prove broadcast discovery or application access.

**Finish and restore:** Remove test bridging/addresses, disable VXLAN and verify no L2 loop remains.

VXLAN ID is 1–16777215. Type interface or ip selects local binding. Match peer IP, UDP port and the required virtual addressing/bridging. Peer port is 1–65535. VXLAN itself does not encrypt traffic. After saving, verify underlay IP reachability, the VXLAN interface and the intended Layer-2 service separately.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Name / VXLAN ID | Name the virtual interface and use the same VXLAN identifier as the peer |
| 2 | Type / Local Address / Peer IP | Configure local egress and reachable peer for outer transport |
| 3 | Peer Port | Match the peer UDP listener |
| 4 | Local Virtual IP / Bridge | Configure for routed or bridged operation and check the broadcast domain and addressing |
| 5 | Interface Status | An up interface does not prove remote equipment access; test the intended Layer-2/Layer-3 service |

**Check the result** Peer settings match and the intended Layer 2 service communicates as planned

## 6.11 DMVPN

Path VPN > DMVPN

DMVPN configures roles and virtual addresses for a hub-and-spoke design. Use a complete topology rather than treating a Hub address as proof of all-site connectivity.

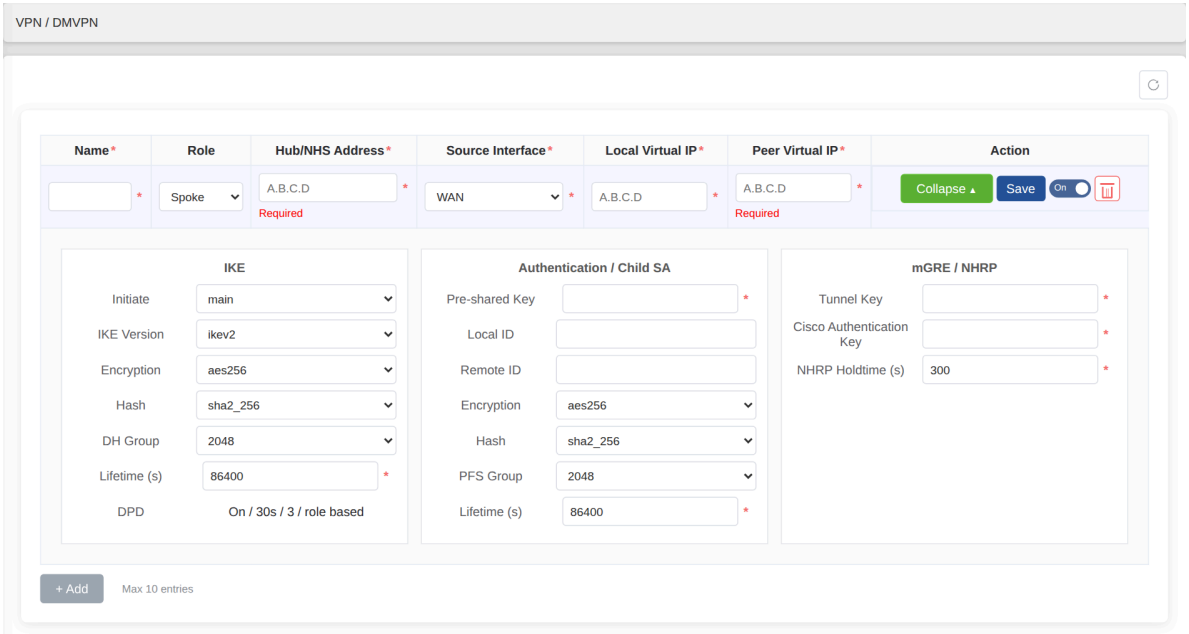



Figure 6-12 DMVPN

Native unsaved form / browser draft; not applied to device

### FIELD TASK: START DMVPN WITH ONE HUB AND ONE SPOKE

Hub H: WAN 192.168.20.2, LAN .10.1. Spoke S: WAN 192.168.20.3, LAN .30.1. Both ends must support the same DMVPN/IPsec plan; avoid multiple rules with overlapping selectors.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Name H / S | hub1 / spoke1 | Test rule names |
| Role H / S | Hub / Spoke | Correct roles |
| Source Interface | actual WAN | Choose reachable physical egress |
| Local Virtual IP H / S | 10.48.0.1 / 10.48.0.2 | Same planned tunnel subnet |
| Peer Virtual IP on S | 10.48.0.1 | Spoke uses hub virtual IP; do not copy spoke fields onto Hub |
| Hub / NHS Address on S | 192.168.20.2 | Spoke uses hub physical IP; leave spoke fields unset on Hub |
| Tunnel Key / NHRP Authentication | 100 / LabNhrp2026 | Match both ends |
| PSK / IKE / SA Lifetime | LabDmvpn2026 / match both ends / 3600s | Match cipher/hash/DH/PFS and identities from the bilateral plan |

### SAVE, TEST AND OBSERVE

1. Save/enable Hub then Spoke. Inspect IKE/Child SAs, NHRP registration and tunnel IP reachability. Add remote LAN and return routes from the site routing plan.
2. Test services both ways between 192.168.10.10 and 192.168.30.10 and record counters. A second spoke needs a unique tunnel IP and real peer, without duplicate enabled selectors.

### PASS CRITERIA AND DIAGNOSIS

Selector conflict: MT7621 checks Hub source interface and Spoke source+physical peer. Renaming does not bypass it. SAs but no registration: inspect NHRP. Registered without LAN service: inspect routes/return path.

**Finish and restore:** Remove test-site routes, then disable Spoke and Hub test rules while retaining production rules.

### CONFIGURE HUB AND SPOKE RULES

Up to 10 rules are available, with one unsaved new rule at a time. Hub does not use the spoke-specific physical peer and peer virtual IP. Spoke requires a reachable hub/NHS address and matching virtual peer.

Expand Advanced and match IKE version, negotiation mode, encryption, hash, DH, PSK, peer identities, Child SA, PFS, tunnel key and NHRP authentication. Both phase lifetimes are 120–86400 seconds; NHRP holdtime is 1–65535 seconds. These time fields are not interchangeable.

Enabled rules must not duplicate a hub on one source interface, or a spoke with the same source interface and physical peer. Resolve the conflicting rule when prompted; renaming or repeatedly toggling it does not fix the conflict. After saving, check application results, the tunnel and destination return routes. The displayed new rule is an unsaved field example.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Name / Role | Choose the role in the hub-and-spoke network plan |
| 2 | Hub / NHS Address | Use the reachable hub/NHS address and coordinate spoke settings with the hub |
| 3 | Source Interface | Select local egress for the tunnel |
| 4 | Local / Peer Virtual IP | Plan tunnel addresses and destination routes without LAN conflicts |
| 5 | Deployment | Obtain complete peer settings; a hub address alone does not provide all site routes |
| 6 | IKE / Child SA advanced settings | Match IKE version, mode, encryption, hash and DH/PFS at both ends; phase lifetimes are 120–86400 seconds. |
| 7 | PSK / peer identities | Match the PSK and local/remote identities to peer authentication requirements; a tunnel name is not an authentication identity. |
| 8 | Tunnel key / NHRP | Tunnel key: 1–4294967295. Match NHRP authentication; holdtime: 1–65535 seconds. |
| 9 | Duplicate selector check | Enabled hubs must have distinct source interfaces; enabled spokes must have distinct source-interface/physical-peer combinations, both on save and enable. |

**Check the result** Node registration and negotiation succeed and required site services are reachable

# 6.12 PPTP client and server

Path VPN > PPTP Client / PPTP Server

This section describes the delivered PPTP pages. Match client/server addressing, authentication and PPP parameters, then configure service routes.

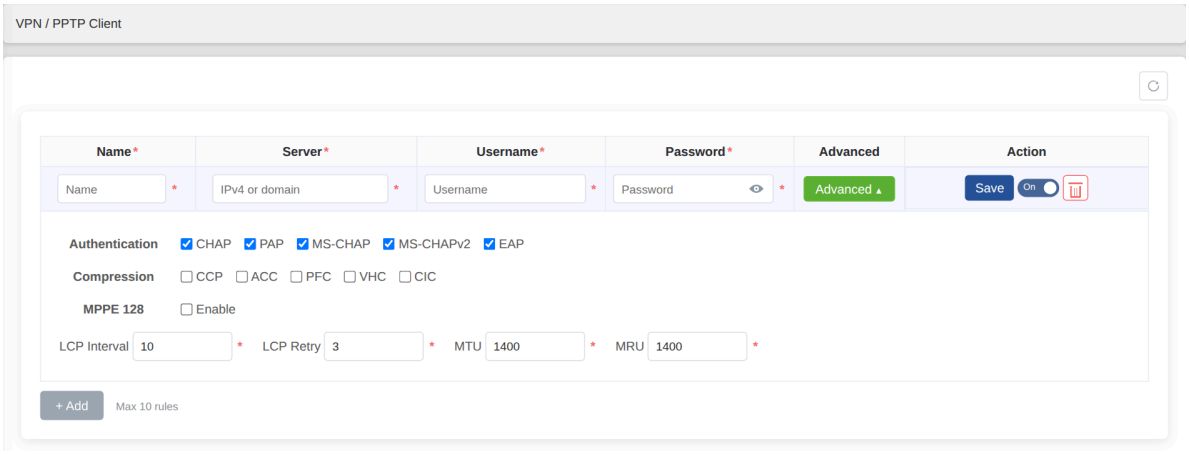



Figure 6-13 PPTP client and server

Native unsaved form / browser draft; not applied to device

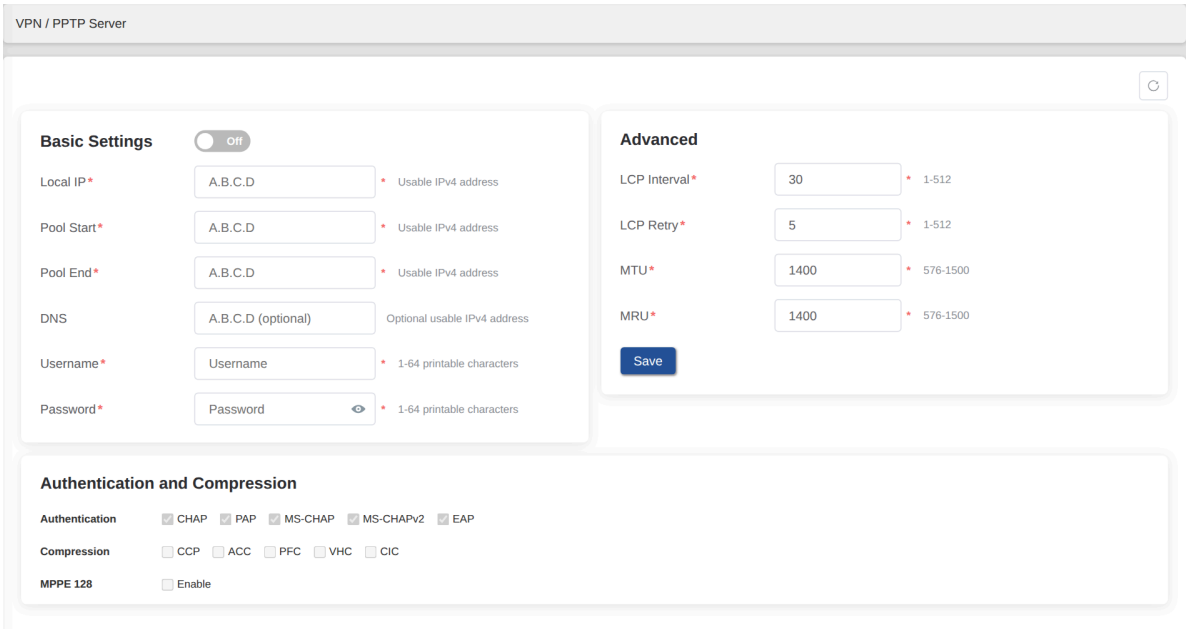



Figure 6-14 PPTP client and server

## FIELD TASK: PPTP CLIENT TO AN ISOLATED TEST SERVER

Configure the corresponding server at 192.168.20.3 first; this gateway WAN is .20.2. Encryption limits are detailed below; these protocols alone do not replace a required encrypted VPN.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Server | 192.168.20.3 | Reachable lab server |
| Username / Password | field / LabTunnel2026 | Matching lab credentials |

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Authentication / Compression / MPPE | match server | Match server settings as a set |
| MTU / MRU | 1400 / 1400 | Use if supported; retain planned LCP settings |
| Server Local IP / Pool Start / End | 10.50.0.1 / 10.50.0.2 / 10.50.0.10 | Set on B PPTP server; account field/LabTunnel2026, negotiation matching client |

## SAVE, TEST AND OBSERVE

1. First configure B PPTP server Local IP/pool and lab account, save/enable, then configure this client. Permit both PPTP transport and GRE in both directions.
2. Save/enable, inspect session/assigned IP and test server tunnel IP. LAN access additionally needs bilateral routes and return paths.
3. Access an active remote test service and record the result; configure PPTP server pool/accounts/DNS using its server field reference below.

## PASS CRITERIA AND DIAGNOSIS

Auth fails: inspect credentials/negotiation. L2TP: inspect UDP1701 and any separate IPsec protection. PPTP: inspect TCP1723 and GRE protocol47. LAN failure after tunnel connects: inspect routes/gateways.

**Finish and restore:** Disable the client and remove temporary routes/server lab accounts.

PPTP is retained for compatibility with existing installations, not as the default for new security-sensitive projects. Start with the remote-access selection section and match the available peer and your security policy.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Client / Server | The client connects to a server; the server maintains tunnel addressing and authentication |
| 2 | Server / Username / Password | Use the parameters assigned for the PPTP service |
| 3 | Address Pool / DNS | Tunnel addressing and DNS assigned in server mode |
| 4 | Authentication / PPP Parameters | Match exposed authentication, compression and link settings to both peers |
| 5 | Routing | After establishment, verify destination and return routes |

**Check the result** The relevant connection establishes and addressing, routes and required services are verified

CHAPTER

# 07

# Forwarding

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 7. Forwarding

## 7.1 NAT and port forwarding

Path Forward > NAT

NAT modifies source/destination addressing for matching traffic. Remote site-service access also needs a reachable ingress, allowed policy and correct return routing.

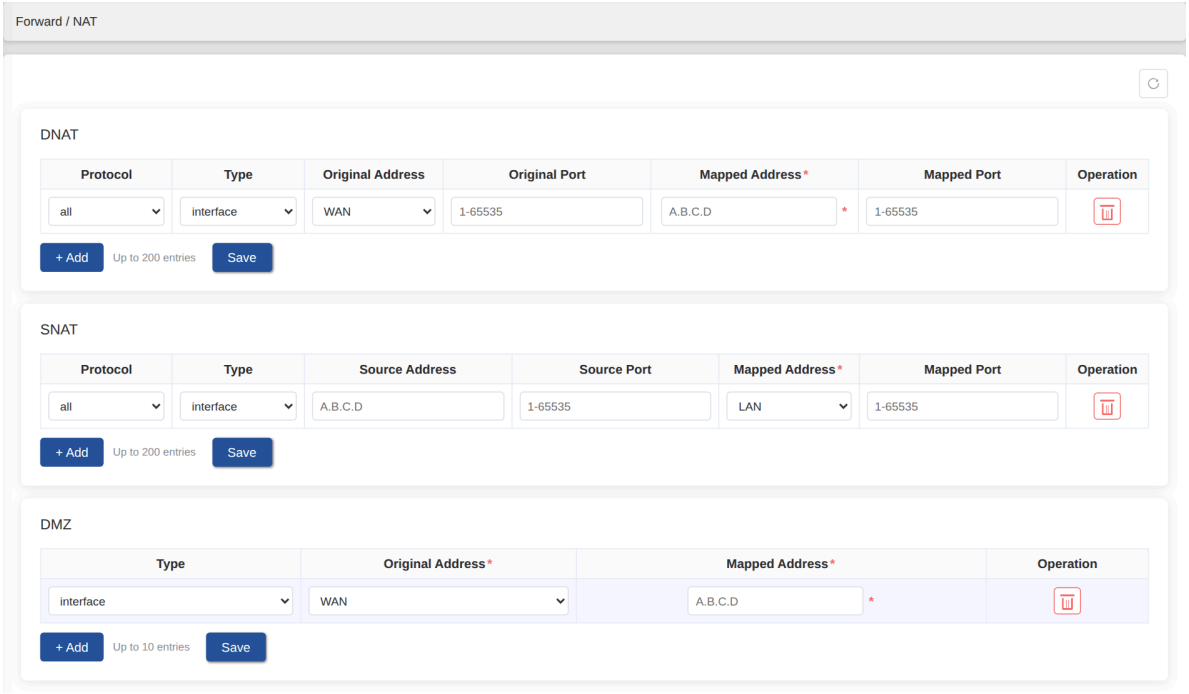



Figure 7-1 NAT and port forwarding

Native unsaved form / browser draft; not applied to device

### FIELD TASK: ACCESS A LAN HTTP SERVICE FROM UPSTREAM

Run bench on LAN PC .10.10. WAN is 192.168.20.2/24 and upstream PC 192.168.20.10/24. First open http://192.168.10.10:8080/ from LAN and expect YZW-FIELD-LAB HTTP OK.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Rule / Protocol | DNAT / TCP | Add one port mapping |
| Type / Interface | interface / WAN | Select the proven physical WAN |
| Original Port | 18080 | Upstream PC accesses this port |
| Mapped Address / Port | 192.168.10.10 / 8080 | LAN service; its default gateway is 192.168.10.1 |

### SAVE, TEST AND OBSERVE

1. Add, enable and save the rule. From the upstream PC open http://192.168.20.2:18080/. A LAN-to-WAN hairpin test is not a substitute.
2. Disable the mapping and repeat: upstream access should fail while direct LAN access to 8080 still works.

### PASS CRITERIA AND DIAGNOSIS

Failure: check local 8080 service, PC firewall, target gateway, WAN IP and rule direction. Internet access additionally requires a reachable public address, upstream forwarding and carrier permission. DDNS does not bypass CGNAT.

**Finish and restore:** Delete the mapping and close the test service/firewall allowance. Publish only the required production ports.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | DNAT | Translates matching destinations to a site service, commonly for port mapping |
| 2 | SNAT | Changes source addressing for a defined egress or return-path plan |
| 3 | DMZ | Forwards a broader inbound range according to the rule, not merely one service port |
| 4 | Protocol / Type | Choose the protocol and interface- or IP-based matching |
| 5 | Original Address / Port | Address/service-port match before translation; use the supported range syntax |
| 6 | Mapped Address / Port | Address and port after translation; the target host must also allow the service |
| 7 | Return Path | The target must return through the correct gateway; translation does not replace routing |

**Check the result** A test from the actual outside network reaches the mapped target service within the intended rule scope

# 7.2 Static routes

Path Forward > Static Route

A static route defines the next hop for a destination subnet. Plan the peer return path as well; one local rule alone does not establish two-way communication.

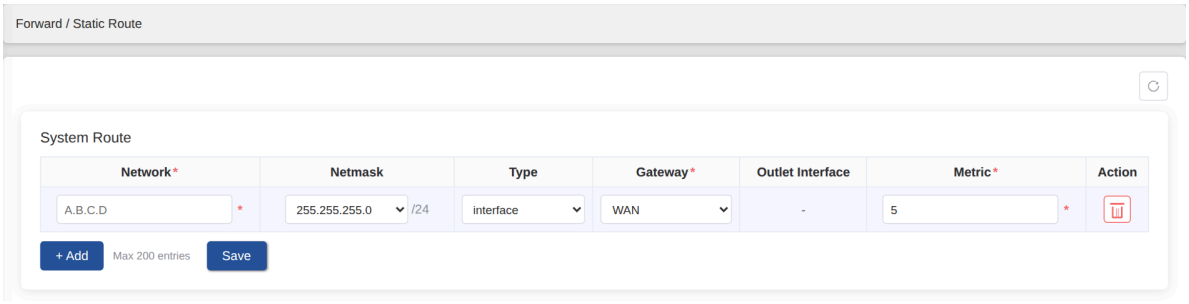



Figure 7-2 Static routes

Native unsaved form / browser draft; not applied to device

## FIELD TASK: REACH ANOTHER SUBNET THROUGH A SECOND LAN ROUTER

Gateway LAN 192.168.10.1; second router 192.168.10.254 on this LAN and 192.168.30.1 on its other LAN; target PC 192.168.30.10/24, gateway .30.1. Enable forwarding and permit the service on the second router.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Network / Mask | 192.168.30.0 / 255.255.255.0 | Destination subnet, not the local LAN |
| Type / Gateway | gateway / 192.168.10.254 | Next hop must be directly reachable |
| Metric | 10 | Record precedence against other routes to the same target |

## SAVE, TEST AND OBSERVE

1. Save the route. From 192.168.10.10 run ping 192.168.10.254 and ping 192.168.30.10, then access an actually running target HTTP/PLC service.
2. Check the return path. The second router is directly connected to subnet 10 and 192.168.30.10 must use 192.168.30.1 as gateway. For further hops add return routes to 192.168.10.0/24 at each hop.

## PASS CRITERIA AND DIAGNOSIS

Next hop works but target fails: inspect second-router forwarding and remote firewall. A route-table entry does not prove an application listener or return path.

**Finish and restore:** Delete the added route and restore the second router without deleting the existing default route.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Network / Mask | Specify the destination subnet, not an unrelated local interface address |
| 2 | Type | Choose interface or explicit-IP next-hop mode |
| 3 | Gateway / Interface | Ensure the next hop is reachable through the selected interface |
| 4 | Metric | Expresses preference among eligible routes; it does not replace longest-prefix matching |
| 5 | Return Route | The peer needs a route back to the local subnet |

**Check the result** The route uses the intended exit and both forward and return paths work

## 7.3 MASQ masquerading

Path Forward > MASQ

MASQ translates source traffic to the egress address, commonly for client access through the router. Its use depends on return routing to the site subnet.

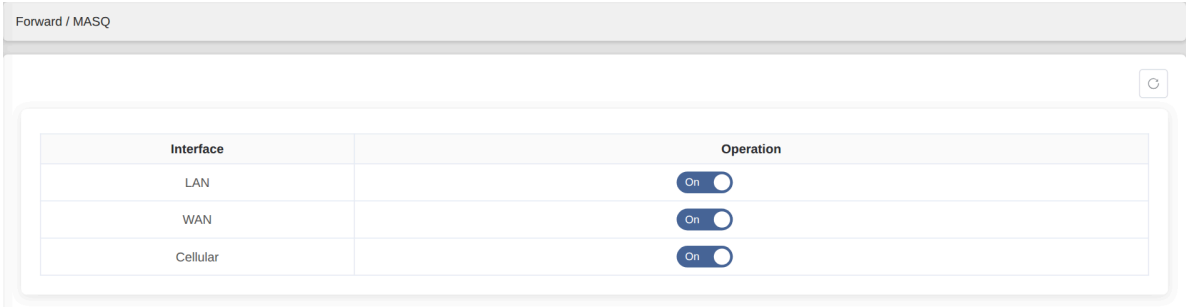



Figure 7-3 MASQ masquerading

### FIELD TASK: VERIFY LAN-CLIENT ACCESS THROUGH EGRESS MASQUERADING

Gateway LAN 192.168.10.1/WAN 192.168.20.2; upstream 192.168.20.10 serves HTTP8080 without a subnet10 return route. First prove gateway access to that service.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Interface / Enable | Actual WAN / On | Only this test egress; retain VPN policy |

### SAVE, TEST AND OBSERVE

1. Save, access http://192.168.20.10:8080/ from 192.168.10.10 and verify upstream sees source WAN .20.2.

2. In an isolated window briefly disable that egress MASQ for comparison; without a return route, LAN access fails. Restore immediately.

### PASS CRITERIA AND DIAGNOSIS

Gateway works but client fails: inspect MASQ, client gateway and forwarding. For VPNs requiring source identity prefer return routes over blanket masquerading.

**Finish and restore:** Restore original MASQ state and verify other services and site return routing.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Interface | Select the interface whose egress address is used for source masquerading |
| 2 | Enable | Enable for the network design; routed and masqueraded return paths differ |
| 3 | Access Behavior | Test newly established connections after changes; existing session state can affect observations |

> **Check the result** The selected source reaches its target through the intended exit and replies return to the original client

## 7.4 QoS rate control

Path Forward > QoS

QoS controls bandwidth within the configured scope. Match direction, interface, network and rate units to the intended service.

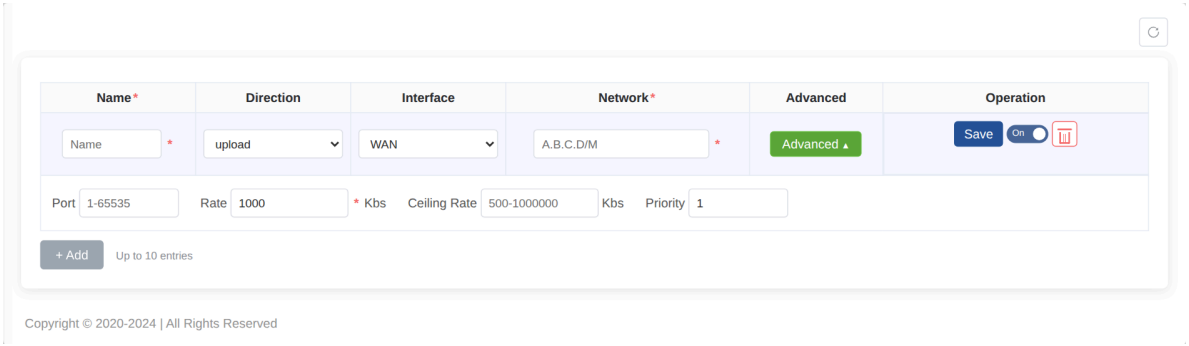



Figure 7-4 QoS rate control

Native unsaved form / browser draft; not applied to device

### FIELD TASK: LIMIT ONE TEST CLIENT TO ABOUT 2 MBIT/S

Use test client 192.168.10.11 and control PC .10.10. Install iperf3 upstream at 192.168.20.10 and run iperf3 -s. Prove baseline speed exceeds 2 Mbit/s and remove overlapping test-client limits. Allow iperf3 TCP5201 on the server firewall only from test sources.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Name / Direction | labup / Upload | For download create a separate labdown / Download rule |
| Interface / Network | Actual egress / 192.168.10.11/32 | MT7621 matches the LAN client before NAT |
| Port | blank | Limit the whole client; do not enter a remote HTTP port |
| Rate / Ceiling Rate | 2000 / 2000 kbit/s | Both values use kbit/s |
| Priority | 10 | If the priority field is present |

### SAVE, TEST AND OBSERVE

1. Save upload rule. On 192.168.10.11 run iperf3 -c 192.168.20.10 -t 20 and record before/after throughput.
2. Add the download rule and run iperf3 -c 192.168.20.10 -R -t 20. Control PC 192.168.10.10 should not be limited by this /32 rule.

### PASS CRITERIA AND DIAGNOSIS

Expect throughput near, and not persistently far above, 2 Mbit/s with protocol overhead. Check direction, egress, CIDR and save if ineffective. A baseline below 2 Mbit/s cannot prove shaping. MT7621 has no separate master switch here.

**Finish and restore:** Delete labup/labdown, rerun iperf3 to confirm baseline recovery and stop the server.

### USE ORIGINAL LAN ADDRESSING

For upload, select the real uplink and match the pre-NAT LAN source subnet or client /32. For download, select LAN (br-lan) and match the LAN destination subnet or client /32. Do not substitute the WAN public address for the internal client, including when NAT and QoS are used together.

The advanced Port field matches source port on upload and destination port on download, for the corresponding TCP/UDP traffic. Upload port 80 does not mean all clients accessing remote web port 80. Start with Port empty for a whole-client limit, then refine only for a specific requirement.

| FIELD | RANGE AND MEANING |
|---|---|
| Rules | Up to 10, each saved and switched separately; no separate master switch |
| Name | 1–10 printable non-whitespace characters; names must be unique |
| Network | IPv4 CIDR, such as the actual client address/32 or LAN subnet/24 |
| Port | Optional, 1–65535; empty does not restrict matching by port |
| Rate / Ceiling Rate | 500–1000000 kbit/s; a specified ceiling must be at least Rate |
| Priority | Optional, 1–30; does not replace network/port matching |

The displayed Kbs means kbit/s, not KB/s; 1000 kbit/s is about 1 Mbit/s. After saving, inspect application results and test new traffic matching direction, interface, address and port. Aggregate WAN traffic does not validate one client, and a local rate limit does not guarantee external bandwidth.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Direction / Interface / Network | Upload matches the original LAN source; download matches the LAN destination on br-lan. Enter an IPv4 CIDR. |
| 2 | Port | Optional 1–65535; source port for upload, destination port for download. Leave empty initially when limiting an entire client. |
| 3 | Rate / Ceiling Rate | 500–1000000 kbit/s; a specified ceiling must be at least Rate. |
| 4 | Priority / Save / Switch | Optional priority 1–30. Save and enable each rule separately; avoid duplicate names and overlapping matches. |

**Check the result** Matched traffic follows the intended limits while other required services continue to work

CHAPTER

# 08

# Firewall

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 8. Firewall

## 8.1 Management ports and remote access

Path Firewall > Port Setting

This page manages listener settings and source-network access to the router services. Management access control is not a universal policy for forwarded business traffic.

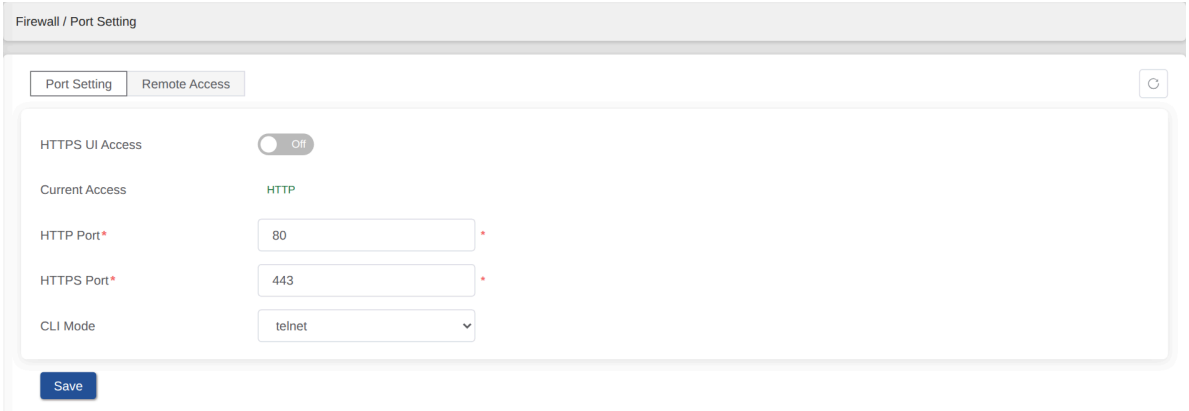



Figure 8-1 Management ports and remote access

### FIELD TASK: CHANGE MANAGEMENT PORTS WHILE RETAINING LOCAL ACCESS

Back up and record current URL/LAN-WAN-VPN permissions. Keep local wired access; test the new entry before closing the old one.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| HTTPS Port | 8443 | If HTTPS is supported, ensure port is unused |
| HTTP / HTTPS / LAN Access | retain working LAN entry | Do not disable every management method |
| WAN / CLI Access | approved scope only | Prefer authorized VPN for remote management |

### SAVE, TEST AND OBSERVE

1. Save HTTPS port and open https://192.168.10.1:8443/ in another window. Verify certificate identity, log in, then retire unneeded old entries.
2. Test success from allowed LAN/VPN and rejection from unauthorized WAN sources.

## PASS CRITERIA AND DIAGNOSIS

Connection refused: inspect port/protocol/enable. Login failure: inspect credentials/session. CLI and Web ports are different.

**Finish and restore:** Restore ports/permissions through retained LAN access and retest both URLs.

> **Management protocol security**: the screenshot shows HTTP and Telnet settings on the illustrated firmware, not recommended security settings. Telnet and HTTP do not provide transport encryption; avoid management across public or untrusted networks. Prefer SSH and HTTPS when supported by the delivered firmware, restrict WAN management sources, and retain a recoverable local access path before changing settings.

## MANAGEMENT AFTER INITIAL SETUP

1. Keep a working LAN maintenance connection and record the current address, protocol and port. Do not change every management rule over the only remote path.
2. Where the delivered firmware provides HTTPS, switch using the page, sign in at the new HTTPS address/port and check certificate identity and browser notices. A switch on the page does not establish that HTTPS is already enabled.
3. Plan access separately for LAN/WAN/VPN sources. Restrict WAN management when unnecessary; prefer an authorized VPN/platform maintenance path.
4. Verify access from allowed sources and denial from excluded sources; retain the rules and recovery access method.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | HTTPS UI Access / Current Access | Distinguish enabling HTTPS from the protocol currently used by the browser |
| 2 | HTTP / HTTPS Port | Web listeners; reconnect with the matching protocol and port after changes |
| 3 | CLI Mode | Interpret CLI access mode separately from the Web account page |
| 4 | Protocol | Configure ICMP, Web, SSH and CLI access separately |
| 5 | LAN / WAN / VPN | Rules are grouped by source network; follow this firmware interface for allow/deny semantics |
| 6 | Management Path | Retain a working maintenance path before changing the protocol or source policy used for access |

> **Check the result** Only intended services are accessible from the specified direction and management remains available

# 8.2 SPI filtering

Path Firewall > SPI Filter

SPI enables the connection-state and abnormal-traffic checks exposed by the firmware. Select needed protections and verify legitimate services.

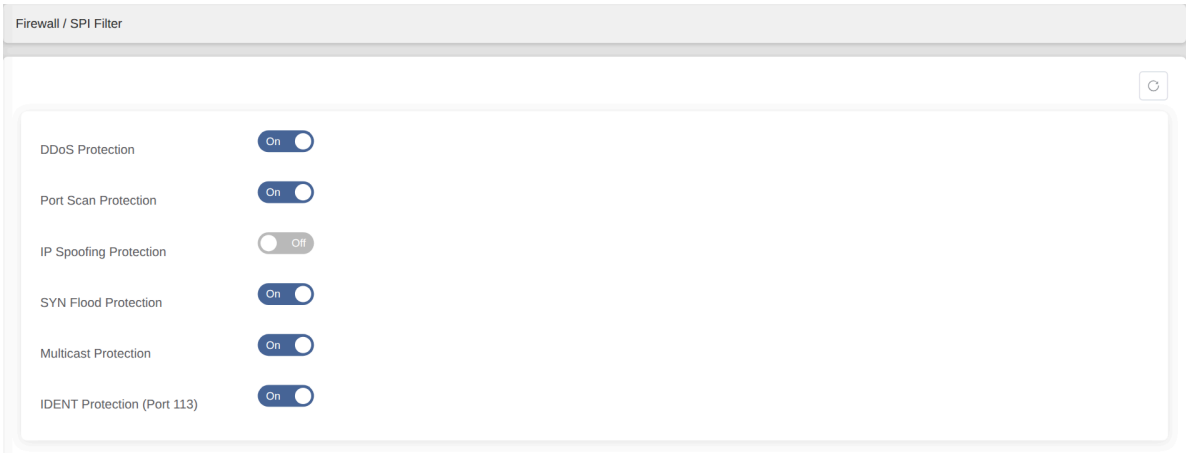



Figure 8-2 SPI filtering

### FIELD TASK: VERIFY SERVICES AND UNAUTHORIZED ACCESS AFTER ENABLING PROTECTION

Back up and record VPN/reporting/management baseline. Change one protection item at a time and keep LAN access.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Protection Item | actual required item | Do not assume every protocol is covered |
| Enable | On | Save/test one item at a time |

### SAVE, TEST AND OBSERVE

1. Enable/save one item, repeat permitted applications and an unauthorized external access test, record results/logs, then move to the next item.

### PASS CRITERIA AND DIAGNOSIS

If valid VPN/acquisition breaks, restore the last item and inspect protocol/direction. SPI does not replace explicit source/port rules.

**Finish and restore:** Restore the prior switches and retest, retaining per-item results.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Protection Items | Select exposed protections such as DDoS, port-scan, IP-spoofing and SYN-flood checks |
| 2 | Enable / Save | Save enabled options, then verify services that must remain reachable |
| 3 | Effect | Stateful checks do not replace endpoint controls or guarantee blocking every attack |

**Check the result** The intended filter direction and rules take effect while required connections and replies work

## 8.3 Address filtering

Path Firewall > IP Filter

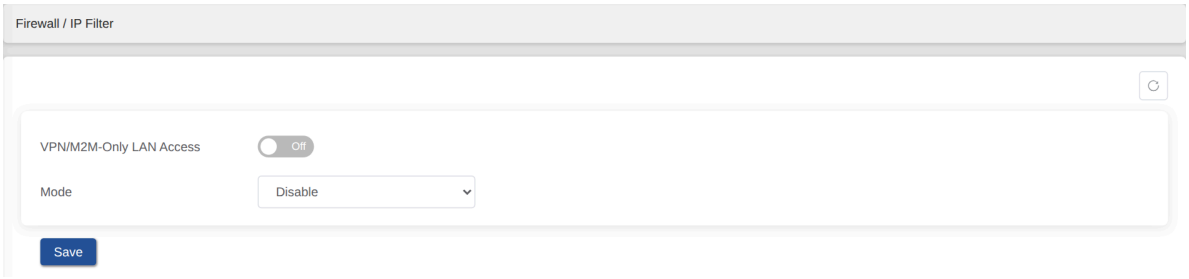



Figure 8-3 Address filtering

### FIELD TASK: BLOCK ONE SERVICE FOR ONE TEST CLIENT

Keep management on 192.168.10.10; use 192.168.10.11 as test client. Upstream 192.168.20.10 runs bench --bind 192.168.20.10. First prove both can open http://192.168.20.10:8080/.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode / Scope | Blacklist / forward | Test forwarding, not input management access |
| Filter Option / Protocol | ip / TCP | Match IP |
| Source / Destination | 192.168.10.11/32 / 192.168.20.10/32 | Source is test client; destination is service |
| Destination Port / Source Port | 8080 / blank | Do not enter management 80/443 |

## SAVE, TEST AND OBSERVE

1. Save the rule and close existing test-client connections before retrying. 192.168.10.11 should fail at 8080; 192.168.10.10 should succeed; management at 192.168.10.1 should remain available.

## PASS CRITERIA AND DIAGNOSIS

Both fail: check service. Both succeed: check forward scope, mode, source IP and existing sessions. VPN/M2M-Only LAN Access is independent; disabling the blacklist does not disable it.

**Finish and restore:** Disable/delete the rule and verify both recover. For a whitelist, permit the management source before enabling it.

## CONFIGURATION STEPS

1. Decide whether VPN/M2M-Only LAN Access is required. Its switch submits and applies independently; selecting Disable below does not remove this restriction.
2. When enabled, direct Internet forwarding from LAN clients is restricted. VPN/m2mCloud paths still need their own routes, authorization and access rules; the switch does not create a tunnel or disable gateway connectivity.
3. Select Disable, Blacklist or Whitelist and edit the selected list. After switching modes, check which list is displayed.
4. Select Rule first: input applies to services on the gateway; forward applies to client traffic routed through it. Keep management access and client forwarding scopes distinct.
5. Choose ip, mac or ip&mac. Combined rules require both entered IP and MAC conditions. Do not fill disabled IP/port fields in MAC-only mode; ICMP does not match ports.
6. Enter source, destination and protocol as required. Type ip uses a destination address; Type interface selects the actual incoming interface, not the outgoing interface.
7. Preserve an allowed management path before saving the list. Test new connections from both allowed and denied clients rather than relying on an existing session.

> Verify whitelist behavior in the input/forward scopes containing rules; do not use an empty whitelist as a deny-all policy. Saving the list and operating the independent switch are separate actions; disabling one does not disable the other.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | VPN/M2M-Only LAN Access | Independent switch restricting direct LAN Internet forwarding. Disabling the lists does not remove it; check gateway connectivity and tunnel authorization separately. |
| 2 | Mode | Disable stops rule filtering; Blacklist denies matches; Whitelist permits the allowed scope |
| 3 | Filter Option | ip matches IP conditions, mac matches source MAC and ip&mac requires both. Select input/forward scope first. |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 4 | Protocol / Source Port / Destination Port | Match the actual transport protocol and service ports |
| 5 | Source / Destination Address | Source initiates access and destination is its target; do not swap directions |
| 6 | Source MAC | Matches LAN device identity, not arbitrary remote-device MACs across routers |
| 7 | Verification | Test allowed and denied access separately and retain management access before enabling a whitelist |

**Check the result** List mode and matching follow the plan, verified with one allowed and one restricted client

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Rules saved but behavior differs | Test an allowed and a denied client. Check blacklist/whitelist mode and the IP, MAC or combined matching fields. |

## 8.4 Domain filtering

Path Firewall > Domain Filter

Domain filtering applies a blacklist/whitelist policy. Their default behaviors differ, so test allowed and denied targets separately.

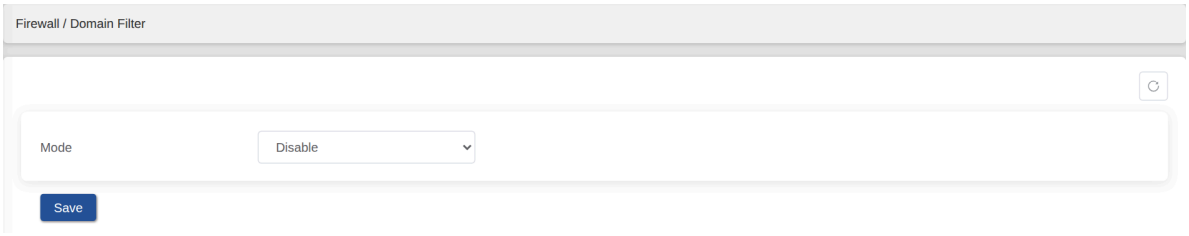



Figure 8-4 Domain filtering

### FIELD TASK: BLOCK ONE VERIFIED REACHABLE DOMAIN

Use an approved real test domain/server. Prove nslookup and application access first; a nonexistent domain cannot demonstrate filtering. Retain management on the control PC.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Mode | Blacklist | Do not start with an empty whitelist |
| Domain | actual test FQDN | Hostname only, no URL scheme/path |

### SAVE, TEST AND OBSERVE

1. Save the domain, close old connections/clear application cache and retry, then test an allowed service.
2. Inspect client DNS path, encrypted DNS and direct-IP behavior; accept only the filter scope actually proven, not universal content blocking.

### PASS CRITERIA AND DIAGNOSIS

Fails before and after: inspect the original site. Ineffective: inspect hostname/mode/cache and bypass paths.

**Finish and restore:** Delete the test domain, restore mode and confirm access recovery.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Mode | Choose disabled, blacklist or whitelist operation |
| 2 | Domain | Use the domain to match, not a complete page path |
| 3 | Add / Delete / Save | Save rule edits and test both target and required normal access |
| 4 | Scope | Domain filtering is not full content inspection of encrypted applications; test direct-IP and other paths separately |

**Check the result** The test client follows the domain policy and required services remain functional

CHAPTER

# 09

# System management

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 9. System management

## 9.1 Local logs

Path System Management > Log

Local logs record system and service events for connection failures, configuration changes, acquisition errors and reboots. Check the clock before correlating event times.

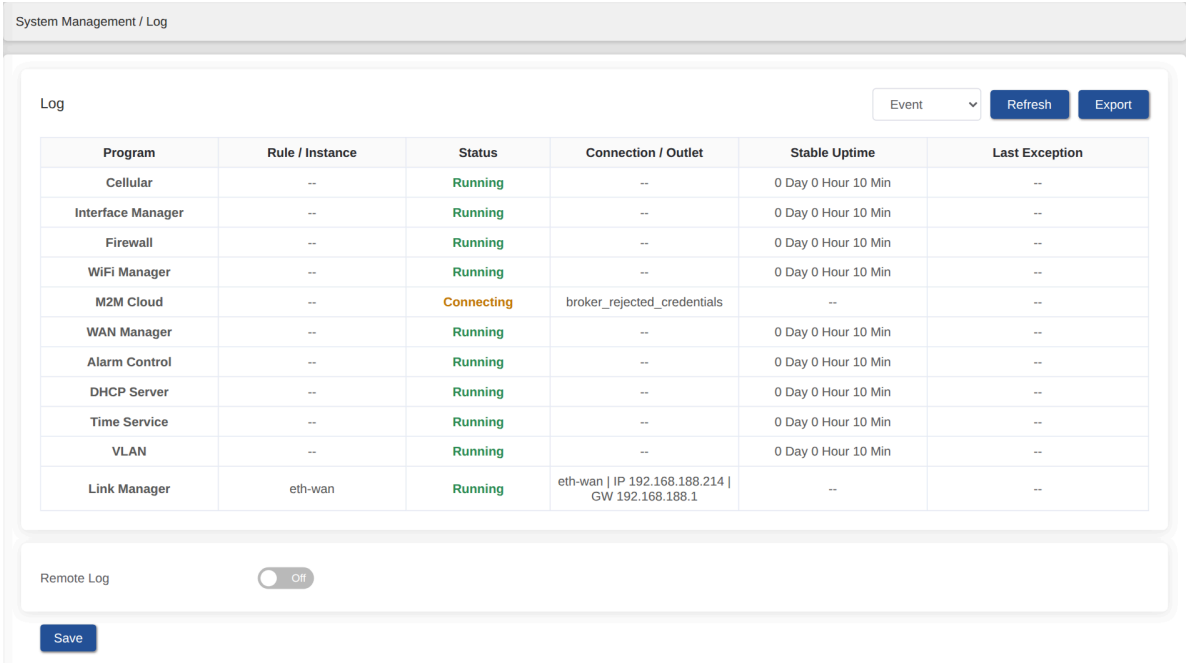



Figure 9-1 Local logs

### FIELD TASK: CAPTURE EVIDENCE THAT SUPPORT CAN REPRODUCE

Synchronize time and identify the failed link, device, topic or port; avoid submitting only a generic connection-failed screenshot.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Time / Operation | timestamped operation | Include timezone |
| Evidence | Status page + related logs + actual test results | Redact passwords/keys/full SIM identifiers before sharing |

### SAVE, TEST AND OBSERVE

1. Record egress/service state before reproduction. Perform one defined test, then export/copy logs covering its time window.

2. Provide problem/expected/actual/time/topology/failure stage/logs/recovery actions and retain a controlled original.

### PASS CRITERIA AND DIAGNOSIS

No logs: inspect time and whether the service triggered. Repeated errors: identify the first failure and surrounding context, not only the last line.

**Finish and restore:** End temporary debugging and restore log levels/polling to avoid excessive ongoing logging.

Record the start time, relevant interface and operation and keep the surrounding event sequence. A single error line may hide an upstream cause. Exclude passwords, private keys and complete SIM identities from shared logs.

> **Check the result** The fault time and relevant module are identified and align with the observed symptom

## 9.2 System time

Path System Management > System Time

System time supports logs, schedules and certificate validation. Configure a reachable time source and verify actual synchronization.

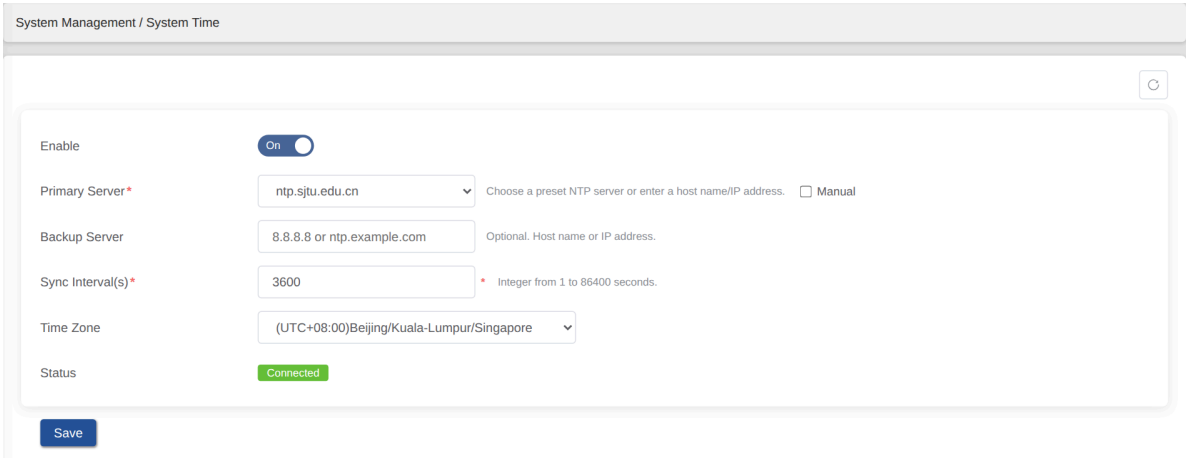



Figure 9-2 System time

### FIELD TASK: SET TIME BEFORE DIAGNOSING CERTIFICATES OR SCHEDULES

Obtain site timezone and allowed NTP servers. China sites use UTC+08:00; use local requirements elsewhere rather than the documentation PC timezone.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Enable / Primary / Backup | On / administrator primary NTP / backup NTP | Use reachable NTP servers; permit UDP123 |
| Time Zone | site timezone | China example UTC+08:00 |
| Sync Interval | retain and record unit | First prove synchronization |

## SAVE, TEST AND OBSERVE

1. Save, inspect current time/sync/source and compare with a synchronized PC against the project tolerance.
2. Retest TLS, schedules and log timestamps; cellular time fallback does not prove NTP success.

## PASS CRITERIA AND DIAGNOSIS

Whole-hour offset: inspect timezone. Wrong date/no sync: inspect DNS, UDP123 and server. Jumps: inspect source changes/startup sync.

**Finish and restore:** Restore production NTP/interval and record timezone/source.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Enable / Primary / Backup | Configure reachable NTP services and backup operation |
| 2 | Sync Interval | Set the synchronization period in the displayed units, separately from acquisition timing |
| 3 | Time Zone | Controls local display and schedule interpretation, not the time reference itself |
| 4 | Status / Time Source | Check synchronization and the actual source; certificates and log analysis also rely on correct time |

**Check the result** Timezone and current time are correct and logs align with site records

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Log times do not match the site | Check timezone first, then reachability of the time synchronization server. |

# 9.3 Admin password management

Path System Management > Account

The current Web account page only changes the existing admin password. It has no guest enable/disable, user creation or permission assignment.

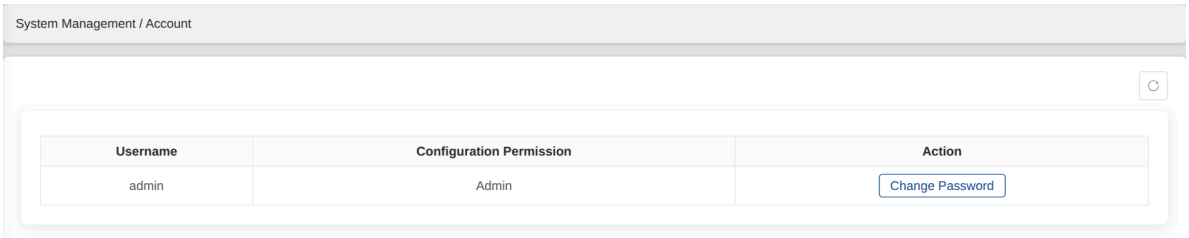



Figure 9-3 Admin password management

## FIELD TASK: CHANGE ADMIN PASSWORD AND IMMEDIATELY VERIFY LOGIN

Retain local LAN and the current session. Prepare a password meeting the unit rules and store securely. The current page’s 5–16 ASCII-character limit still applies.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Current Password | current valid password | Not admin after a prior change |
| New / Confirm Password | same new password | Do not record in public forms |

## SAVE, TEST AND OBSERVE

1. Save, then log in with admin/new password in a private window. Confirm Home before closing the old session.
2. Confirm the old password cannot create a new session. Manage VPN/platform/Node-RED/mail credentials separately.

## PASS CRITERIA AND DIAGNOSIS

Save rejected: inspect length/ASCII/confirmation. New login fails: inspect keyboard/account before retries. For lost credentials prepare backup/recovery as described in Reset.

**Finish and restore:** If reverting, log in with the new password and set the approved replacement; do not keep the public initial password for production.

### FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | admin | The router Web interface only maintains the existing admin password |
| 2 | Change Password | Password is the only input: 5–16 printable ASCII characters, without spaces or non-ASCII characters. Save applies the change; Cancel discards it. |
| 3 | Permission Boundary | No user creation, guest toggling or permission assignment; VPN/platform accounts are separate |

**Check the result** The new password signs in as admin and the password record is updated

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Login fails with the new password | Check case, spaces and length. Confirm the change was saved and enter the actual new password again. |

## 9.4 Configuration backup and restore

Path System Management > Config Management

Export a backup before changing networks or services. Import, factory reset and reboot have different effects; confirm the intended action.

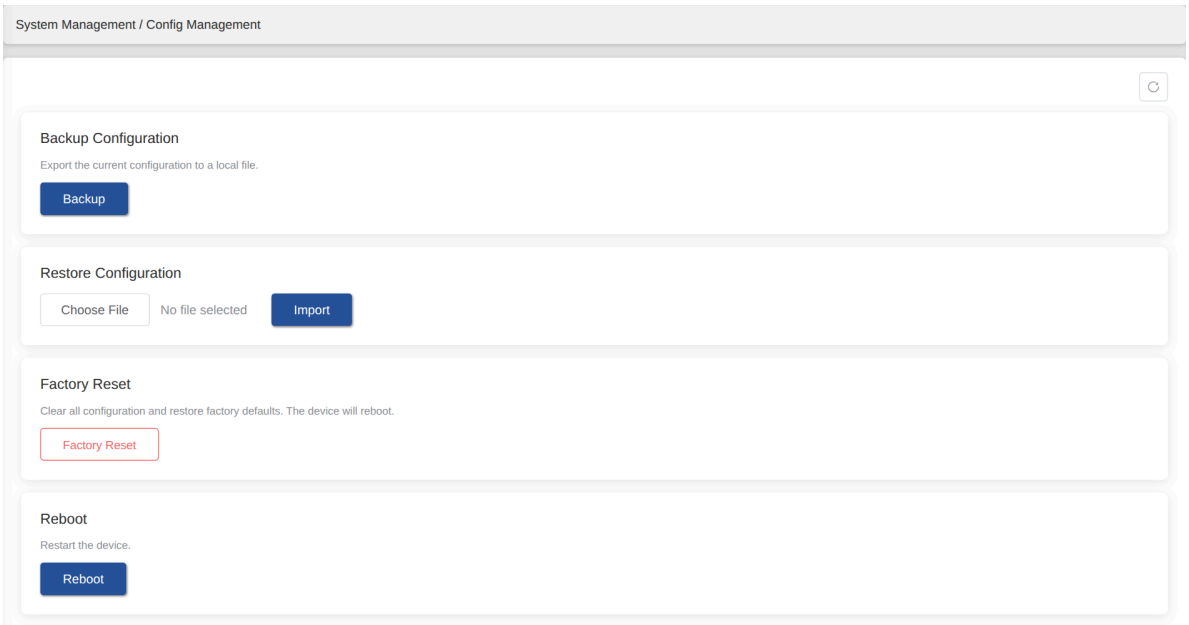



Figure 9-4 Configuration backup and restore

## FIELD TASK: CREATE A CONFIGURATION BACKUP THAT CAN BE RESTORED

Record model, ordered hardware, management address, service list and backup date. Configuration may contain secrets; store it in the controlled project folder.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Backup | Model_site_date.cfg (keep actual export extension) | Keep the actual exported extension and format |
| Choose File / Import | compatible same-model backup | Do not import across models |

## SAVE, TEST AND OBSERVE

1. Export, verify non-empty file and record size/SHA256 using Windows Get-FileHash with -Algorithm SHA256.
2. Test restoration in a maintenance window or on a spare same-model unit. Import, wait as instructed, reconnect using the backed-up address and retest uplink/acquisition/reporting/remote access.

## PASS CRITERIA AND DIAGNOSIS

A file alone proves export, not restorability. Require all core services after import. Lost access: inspect restored management subnet/port/password.

**Finish and restore:** Keep a pre-restore backup; use the delivered recovery procedure if incompatible rather than trying other-model files.

## KEEP A USABLE CONFIGURATION RECORD

Export a backup after completing a service group. A useful filename is model_site_firmware_date. Record the LAN address, uplink method, serial assignments, effective MQTT topics and remote network name alongside it. Keep passwords and keys through your established secure process.

A restore file must be compatible with the model and firmware. Restoring may change the management address and password; reconnect using the saved configuration and revalidate acquisition, reporting and remote services.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Backup | Export the current configuration and identify it by model, firmware and date |
| 2 | Choose File / Import | Import a compatible model/firmware configuration and recheck management access and services |

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 3 | Factory Reset | Clears business configuration and reboots; prepare a backup and reconnection details |
| 4 | Reboot | Restarts the system and temporarily interrupts services |

**Check the result** The backup is available; after restore, its management address works and essential services are revalidated

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| The old address fails after restore | Reconnect with PC addressing appropriate for the LAN stored in the backup; check whether its password was restored. |

## 9.5 Firmware upgrade

Select Factory reset after upgrade when the new firmware changes the configuration. Leave it unchecked for a program-only update with no configuration changes. A checked box resets settings; it does not retain them. Reconfigure after the reset and separately confirm whether an old backup is compatible.

Path System Management > Firmware Upgrade

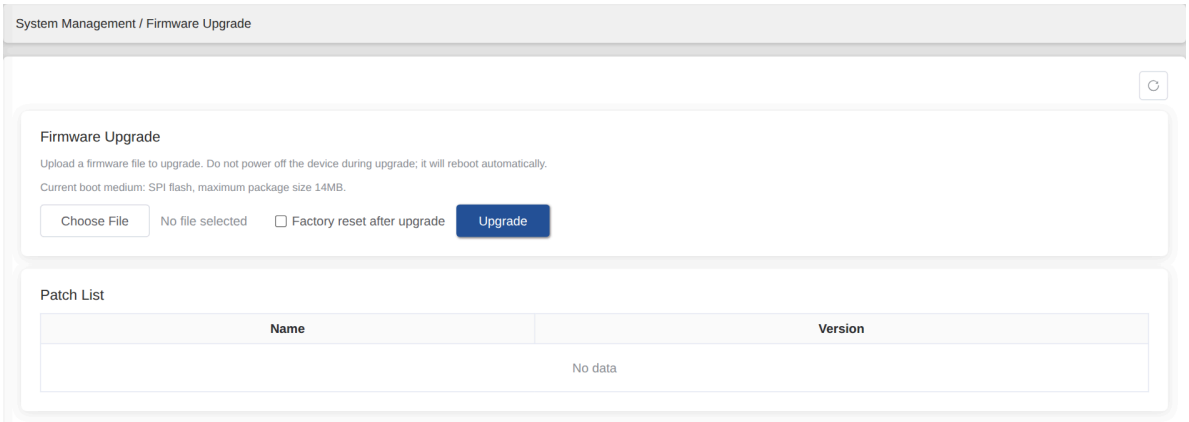



Figure 9-5 Firmware upgrade

### FIELD TASK: UPGRADE IN A MAINTENANCE WINDOW AND VERIFY SERVICES

Obtain firmware for the exact model/hardware, checksum, configuration-retention compatibility and rollback plan from the supplier. Export configuration, point lists and flows first.

## FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Firmware File | supplier-approved file | Match SHA256 against the release handover |
| Factory reset after upgrade | Select Factory reset after upgrade when the new firmware changes the configuration. Leave it unchecked for a program-only update with no configuration changes. A checked box resets settings; it does not retain them. Reconfigure after the reset and separately confirm whether an old backup is compatible. | Reconfigure after the factory reset |

## SAVE, TEST AND OBSERVE

1. Upgrade through local wired management with stable power and wait for completion/reboot without interrupting the write.
2. Log in again and verify LAN/WAN, cellular, failover, acquisition values, MQTT, VPN and schedules, recording actual results.

## PASS CRITERIA AND DIAGNOSIS

Upload rejected: inspect integrity/model. Lost access after reboot: inspect default address, PC lease and HTTP/HTTPS. Upgrade completion does not prove service recovery.

**Finish and restore:** For incompatibility follow supplier rollback plus backup. If startup state is unknown, obtain supplier recovery guidance before repeated flashing.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Firmware File | Use a released image matching YZW280 and its 16 MB SPI NOR storage layout |
| 2 | Factory reset after upgrade | Select Factory reset after upgrade when the new firmware changes the configuration. Leave it unchecked for a program-only update with no configuration changes. A checked box resets settings; it does not retain them. Reconfigure after the reset and separately confirm whether an old backup is compatible. |
| 3 | Upgrade | Back up first, maintain stable power and wait for the upgrade and boot to finish |
| 4 | Version Check | Check the version after reconnecting, then verify network, acquisition and remote access |

**Check the result** After login, firmware matches the intended package and networking, acquisition, reporting and remote services work

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Login works after upgrade but services do not | Check firmware, retained configuration and port roles, then validate networking, VPN, acquisition, MQTT and remote maintenance. |

## 9.6 Reset button and recovery

### FIELD TASK: RECOVER MANAGEMENT ACCESS BEFORE DECIDING ON RESET

Prepare model, old/new addresses, backup and local assistance. Factory reset clears configuration; use this model’ s reset illustration and delivered hold time rather than assuming a universal duration.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| PC Network | Current subnet first;192.168.8.10/24 only at defaults | Use .8.1 only when the unit is actually at defaults |
| Access Check | Correct LAN port, IP, HTTP/HTTPS and management port | Rule out PC VPN/proxy and stale leases |

### SAVE, TEST AND OBSERVE

1. Check power/link/PC IP and current address. After a LAN change move the PC to the new subnet; after port change use the full protocol/port URL.
2. If reset is necessary, follow model-specific steps and wait for boot. At defaults use DHCP or .8.10/24 to reach .8.1, reset the password, restore compatible backup and retest all services.

### PASS CRITERIA AND DIAGNOSIS

Still inaccessible: inspect actual reset trigger, port role, PC IP and supply. Configuration reset does not repair PLC programs or hardware faults.

**Finish and restore:** Rebuild using the backup/site record; without backup restore LAN/uplink first, then acquisition and remote access one service at a time.

Recovery clears network/application configuration. Back up and ensure local reconnection first. Hold duration before release selects the operation. The table follows the audited firmware script; recovery was not executed on the unit.

| HOLD DURATION | **AUDITED FIRMWARE ACTION** |
|---|---|
| < 5 s | Reboot |
| ⩾ 5 s | Factory configuration reset and reboot |

Web Reboot and Factory Reset are separate operations. If boot fails, use recovery instructions matching this model, storage and boot-loader.

CHAPTER

10

# m2mCloud

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 10. m2mCloud remote management

## 10.1 Client configuration and networking

Path Application > M2M Cloud

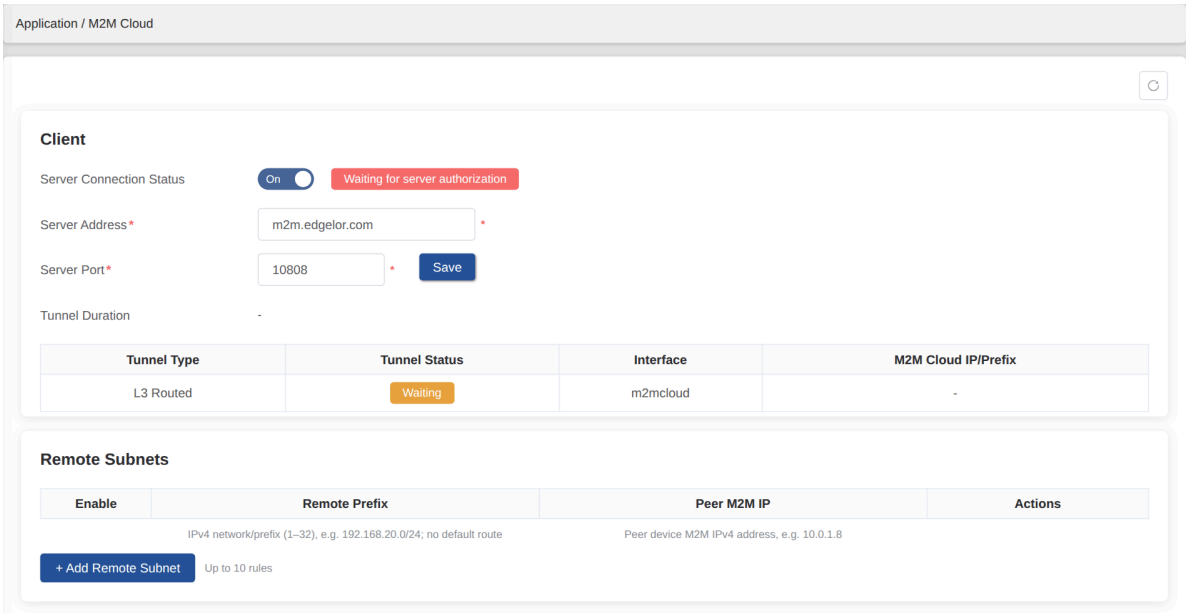



Figure 10-1 Client configuration and networking

### FIELD TASK: ESTABLISH REMOTE MAINTENANCE WITHOUT A PUBLIC SITE IP

Site LAN192.168.10.0/24 must not overlap the remote PC LAN. Obtain server/port, account authorization, network type, tunnel IPs and allowed subnets from the platform administrator. Validate session, virtual network and site service separately.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Client / Server / Port | On / actual platform server / port | Copy the actual platform endpoint |
| Connection / Tunnel Type | Authorized connection / L3 example | Authorized connection; this L3 case does not imply L2 broadcast |
| M2M IP | Gateway10.44.0.2; remote PC10.44.0.3 | Must actually be assigned/approved by platform |
| Remote Prefix / Peer M2M IP | remote network plan | Do not route the gateway’ s own LAN as remote; PC route to subnet10 goes via gateway tunnel IP |

### SAVE, TEST AND OBSERVE

1. Prove server reachability, save endpoint/authorization/network settings and enable. Inspect session/interface address and authorize both gateway and PC on the platform.
2. Join the same authorized network from the remote PC. Ping the actual gateway tunnel IP and inspect route192.168.10.0/24 via that IP. Do not add conflicting routes if platform manages them.
3. Run bench on LAN PC .10.10. From remote open http://192.168.10.10:8080/ before testing the actual PLC/HMI service.

### PASS CRITERIA AND DIAGNOSIS

Online but no tunnel-IP access: inspect authorization/type/address. Tunnel works but 192.168.10.10 fails: inspect PC route, LAN client gateway 192.168.10.1, firewall and return path.

**Finish and restore:** Leave the test network and revoke temporary routes/authorization; retain approved maintenance scope and local recovery.

### OBTAIN PROJECT DELIVERY INFORMATION

Ask the equipment supplier or platform administrator for server/port, CA, account, device authorization and compatible PC client. Confirm Windows and Linux packages/capabilities separately. An online device does not establish an authorized business tunnel.

1. Enter the delivered server address and port, enable the client and check Internet access.
2. Authorize or group the device in the cloud and check tunnel status. L2 bridging or L3 routing is assigned by the platform.
3. In L3 mode, configure remote subnets and peer M2M IPs according to the network plan. Up to 10 rules are supported, without a default route. Rules remain saved but inactive in L2 mode.
4. Join the authorized network from the remote PC. Confirm reachability before using compatible PLC/HMI vendor tools for program upload/download, debugging or maintenance.

The site needs no public IP. Connectivity may use a peer-to-peer path or server relay, depending on the network and authorization. Remote serial access requires the platform proxy client and an unoccupied serial port.

> Verify: the tunnel is online and the PC reaches the required site IP and service. An online tunnel alone does not satisfy PLC programming access policies or protocol requirements.

### VERIFY PLATFORM CONTROL AND THE SERVICE TUNNEL SEPARATELY

Platform control handles identity, authorization and network settings. A separate service path carries PLC/HMI traffic. An online control connection does not prove business reachability.

| LAYER | WHAT TO CHECK | DISTINCTION |
|---|---|---|
| Platform control | Device and PC belong to an authorized network | Platform online does not establish tunnel and target health |
| Service path | Actual direct/P2P or relay conditions and usable tunnel | Direct operation depends on networks; relay availability/limits follow the delivered platform |
| L2 / L3 | Planned bridging for L2; destination routes and return paths for L3 | L3 does not provide LAN broadcast discovery; L2 still needs broadcast and loop control |
| Engineering service | Vendor tool connects to the target and reads information | Ping does not validate drivers, project permissions or programming services |

### START WITH THE PROBLEM: NO PUBLIC IP, SUBNETS AND DISCOVERY

| OBSERVATION | DECISION PATH | COMPLETION CHECK |
|---|---|---|
| 4G only, no public IP | Verify SIM-to-platform access; authorize gateway/PC on the same platform; inspect control and tunnel separately | Gateway virtual IP → explicit PLC IP → vendor tool; an online list is not acceptance |
| PLC IP works; discovery fails | Check L3 versus L2, tool virtual NIC, local firewall and actual platform L2 availability | Use explicit IP where supported; test L2 only when broadcast is required |
| Office/site overlap or duplicate site networks | Prefer renumbering; otherwise follow the client's explicit authorized overlap workflow | Test office LAN, remote PLC, gateway and rollback without silently hijacking office routes |
| Gateway reachable; PLC unreachable | Check site LAN, target gateway/return path, platform rules and access policy | Compare local access to the same PLC, then test layer by layer |

See 10.4 Windows client: remote access and 10.5 Linux client: login and bridge for the respective steps.
Platform control, tunnel operation, IP reachability and engineering-tool success are four separate results to record.

## INFORMATION TO INCLUDE WHEN REQUESTING A CLIENT

Provide the model and gateway firmware, PC operating system/architecture, intended platform endpoint/version, purchase-order or service contact, PLC model and remote-serial requirement. Ask the supplier to confirm the installer version/checksum, account and device permissions. See 10.4/10.5 for Windows 2.2.25 versus Linux 0.1.2. Published website contacts are enquiry routes; the delivery owner must still confirm the formal support channel and compatible version. This manual does not record a completed client business test.

## CHECK CLOUD CONNECTION SEPARATELY FROM SITE ACCESS

Verify cloud session, virtual-network readiness, route reachability and the PLC/HMI application separately. After cloud-session recovery, recheck the remote network and actual site service. After adding, editing or deleting a route, inspect its saved prefix, next hop and switch instead of relying on previous route results.

## FIELD REFERENCE

| NO. | FIELD | WHAT TO ENTER / HOW TO USE IT |
|---|---|---|
| 1 | Client / Server / Port | Enable the client with the platform server and port assigned to this device. |
| 2 | Connection / Tunnel Type | Check management and tunnel states separately; the platform authorizes L2/L3 mode |
| 3 | M2M IP / Interface | Inspect the assigned address; it does not make all remote subnets reachable |
| 4 | Remote Prefix / Peer M2M IP | In L3 mode, assign a next hop for the remote business subnet; default routes are not accepted |
| 5 | Rules in L2 Mode | Remote-subnet rules remain saved but inactive and are not bridge configuration |
| 6 | Remote Serial | Use the supplied proxy client and authorized session with an available physical port |

**Check the result** Router and PC join the authorized network and reach both the field target IP and its service

## TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| Tunnel online but PLC/HMI access fails | Check authorization, L2/L3 mode, remote subnets/return paths and equipment access permissions before using the compatible vendor tool. |

## 10.2 Remote PLC/HMI program transfer

### FIELD TASK: PROVE REMOTE READ ACCESS BEFORE A PLC DOWNLOAD

Complete m2mCloud/VPN and the 192.168.10.10:8080 test first. Example PLC is 192.168.10.20/24, gateway .10.1. Obtain actual model, service port, protection settings and authorization from the PLC project.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| PLC IP / Mask / Gateway | 192.168.10.20 / 255.255.255.0 / 192.168.10.1 | Confirm on the PLC itself |
| Vendor Tool Target | 192.168.10.20 | Use direct IP and the actual model protocol |
| Engineering File | backed-up site project | Verify CPU/release compatibility and protection password |

### SAVE, TEST AND OBSERVE

1. Locally perform read-only online monitoring and back up the project. Remotely select the correct virtual adapter/direct IP and repeat monitoring.
2. Compare a known point, CPU state and project checksum. Download only with an agreed window, backup and rollback owner, following the vendor procedure.

### PASS CRITERIA AND DIAGNOSIS

Discovery fails but direct IP works: inspect broadcast scope. Port works but engineering tool fails: inspect PLC protection, model, session limits and tool version. Web access does not prove a PLC download.

**Finish and restore:** Close the session and restore operating mode/access scope. Recover failed downloads with the prepared PLC backup, not by resetting the gateway.

> **Check the result** The vendor tool identifies the correct target and post-maintenance project version and field operation are correct

> Authorized access does not require a site public IP, but vendor protocol, endpoint policy and project version must still be compatible.

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| The router is reachable but the PLC is not found | Test the PLC IP and service, then remote subnet routes, return path and the vendor tool connection method. |

## 10.3 Remote serial access

### FIELD TASK: ECHO-TEST REMOTE SERIAL BEFORE CONNECTING EQUIPMENT

Verify physical/logical mapping and release the port. Use a matching electrical echo tester or a USB-serial peer. First prove the m2mCloud/VPN network.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Remote Serial / Serial | Enable delivered feature / verified free port | Use delivered virtual-COM component/support |
| Baud / Data / Parity / Stop | 9600 / 8 / N / 1 | Match both ends |

### SAVE, TEST AND OBSERVE

1. Install/start the delivered remote serial mapper, select the authorized gateway/port and record its assigned COM number.
2. Open that COM in a terminal, disable local echo and send FIELD-001. Have the local peer return identical content, compare bytes both ways, then test the real device protocol.

### PASS CRITERIA AND DIAGNOSIS

COM fails to open: inspect mapper, authorization and ownership. No bytes: inspect serial settings/wiring/latency. Transparent forwarding does not automatically convert the device protocol.

**Finish and restore:** Close COM/mapping, release the port and restore acquisition/access scope.

> **Check the result** The proxy exchanges known messages through the intended port and required local services are restored afterward

### TROUBLESHOOTING

| SYMPTOM | WHAT TO CHECK |
|---|---|
| The proxy connects but there is no reply | Check Serial1/2 mapping, serial settings and port ownership. Proxy connection does not establish a slave response. |

## 10.4 Windows client: remote access

### FIELD TASK: VERIFY REMOTE ACCESS ON WINDOWS USING ROUTES

Install the delivered Windows client and obtain platform/account/network authorization. Its local subnet must differ from site subnet10; record route print and ipconfig first.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Server / Account / Network | platform handover | Not the gateway Web admin account |
| Site Route | 192.168.10.0/24 via actual gateway tunnel IP | Prefer managed routes; add only after confirming absence |

### SAVE, TEST AND OBSERVE

1. Sign in and join the authorized network, then inspect virtual IP with ipconfig and site route with route print.
2. Ping the gateway tunnel IP, run Test-NetConnection 192.168.10.10 -Port 8080 and open http://192.168.10.10:8080/.

### PASS CRITERIA AND DIAGNOSIS

Tunnel IP works but service fails: inspect route priority, subnet overlap and site client gateway/firewall; disabling all firewall protection is not a final fix.

**Finish and restore:** Leave the test network, delete only manually added test routes and verify original networking.

## 10.5 Linux client: login and bridge

### FIELD TASK: VERIFY LINUX TUNNEL INTERFACE AND SITE ROUTE

Use the delivered Linux client and its actual configuration path. Do not embed credentials in command lines. Record ip addr and ip route first.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Platform / Network | platform handover | Authenticate/authorize using the delivered client instructions |
| Route | 192.168.10.0/24 via gateway tunnel IP | Use the gateway tunnel IP, not the local physical router |

### SAVE, TEST AND OBSERVE

1. Start/join the authorized network. Use ip addr to inspect its interface and ip route get 192.168.10.10 to verify egress/next hop.
2. Run curl --connect-timeout 5 http://192.168.10.10:8080/ and expect YZW-FIELD-LAB HTTP OK. Do not bridge physical LAN for an L3 test.

### PASS CRITERIA AND DIAGNOSIS

Physical default route selected: site route is missing/conflicting. Tunnel route selected but service fails: inspect authorization, return path and site firewall. Bridging needs a separate L2 plan to avoid loops.

**Finish and restore:** Leave the test network and restore manual route/bridge changes while retaining original interfaces.

CHAPTER

# 11

# Troubleshooting

Configure, inspect and accept the interfaces and functions available on this model



YZW280

# 11. Troubleshooting

## 11.1 Locate faults along the service path

### FIELD TASK: DIAGNOSE THE FIRST FAILING STAGE

Record failure time and the last normal operation. Test stages in order, change one item and repeat.

### FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

| UI FIELD | ENTRY | BASIS |
|---|---|---|
| Management page unavailable | ipconfig → ping management IP → full URL | Check PC subnet/port role/scheme/management port |
| Uplink failure | First hop → server IP → hostname → application | Select actual source in Network Tools |
| MQTT online without data | Mock read → collection log → raw-topic subscription | Prove255 in M1 before real registers |
| Tunnel IP works but PLC fails | Remote route → 192.168.10.10:8080 → actual PLC port | Inspect client gateway/protection/return path |
| Unclear write result | Pause retry → inspect logs/reply → independent readback | M2 has no separate write ack; P1 also needs readback |

### SAVE, TEST AND OBSERVE

1. Export the current configuration before reset. Reproduce once with the relevant chapter command and record input/output/time.
2. For support provide model/topology/actual settings/redacted logs/failure stage/recovery actions and retain controlled originals.

### PASS CRITERIA AND DIAGNOSIS

After a fix retest the failed service and one previously working service to detect regressions.

**Finish and restore:** Undo ineffective changes and return to the last proven backup before continuing.

### WHAT TO INCLUDE IN ONE SUPPORT REPORT

1. Model, firmware, fault time, interfaces in use and a simple wiring sketch.
2. Record the first failing test and its result: for example, gateway reachable but DNS failing, no serial reply, a decoding error, or an online tunnel with an unreachable PLC service.
3. Include relevant configuration, runtime status and logs for that time. Hide passwords, private keys and complete SIM identifiers.

For failover issues, record the combination, actual participating interfaces, per-interface probe targets, and IPv4/IPv6 Current and Status. “Ping works” without the tested exit does not identify the path.

Export a current backup before changing, restoring or upgrading. After correction, repeat the same tests and, when useful, complete Site commissioning record. For formal handover also use Service acceptance and handover; retain actual results and the backup location.

### WHERE TO REQUEST SUPPORT

Official support: `https://www.edgelor.com/support/`; technical documents: `https://www.edgelor.com/support/documents/`. Published contact email: `zhanghailong@x8link.com`; WhatsApp: `+86 185 7641 5335` (`https://wa.me/8618576415335`). Describe the need through `https://www.edgelor.com/project/` or confirm the service owner through the original purchase-order channel.

Supply the model, firmware, time, failure layer, logs and screenshots listed above, with passwords, private keys, tokens and full SIM identifiers hidden. Website information was checked on 2026-10-31; use the official site for later changes.

## 11.2 Bilingual terms and section mapping

Chinese and English use matching section numbers and function IDs; consult the contents in the required language.

| ENGLISH TERM | 中文术语 | MEANING IN THIS MANUAL |
|---|---|---|
| Requirements confirmation | 需求确认 | Goal, existing system, constraints and acceptance |
| Failover | 主备切换 | Backup exit after primary-path failure |
| Link Configuration | 链路配置 | Participating interfaces, keepalive and priority |
| Load Balance | 负载均衡 | Distribute traffic by rules |
| Return route | 回程路由 | Target path back to the remote source |
| L2 bridging | 二层桥接 | Layer-2 transport; check addresses and broadcast |
| L3 routing | 三层路由 | IP-subnet forwarding, not automatic broadcast transport |
| Public IP | 公网 IP | Actual port/path reachability is still required |
| Subnet overlap | 地址重叠 | Office/sites use overlapping address ranges |
| Raw-frame forwarding | 原始报文透传 | Forward raw data without point decoding |
| Polling/reporting interval | 采集周期/上报周期 | Reading and publishing are configured separately |
| Writable command | 可写命令 | Modbus control addressed by configured command name |
| Readback verification | 读回验证 | Later reading compared with field state |

| ENGLISH TERM | 中文术语 | MEANING IN THIS MANUAL |
|---|---|---|
| Retained message | 保留消息 | The broker can keep the latest retained message for a topic and deliver it to a new subscription. Control examples use retain=false; this neither clears an existing retained message nor prevents duplicates caused by QoS, session delivery or application retries |
| Clear threshold | 恢复阈值 | Alarm-clear condition distinct from trigger |
| Example/verified test | 实施示例/实测 | Separate illustration/assumption from actual test |

YZW280

# Site commissioning record

Complete with actual results. Deliver credentials through the project’ s secure channel rather than public records.

| ITEM | RECORD / RESULT / OWNER |
| --- | --- |
| **Model / serial / firmware** | |
| **Management address / access port** | |
| **Supply / SIM / antennas** | |
| **Interfaces / serial type / settings** | |
| **WAN / cellular / failover order** | |
| **Point map / topics / platform** | |
| **VPN / routes / remote access** | |
| **Backup / flows / date** | |

Implemented by: _____ Reviewed by: _____ Date: _____

YZW280

# Service acceptance and handover

Complete with actual results. Deliver credentials through the project’ s secure channel rather than public records.

| ITEM | RECORD / RESULT / OWNER |
| --- | --- |
| **Local access and credentials** | |
| **Networking and failover recovery** | |
| **Acquired values and units** | |
| **Reporting topics and updates** | |
| **Authorized writes/readback if required** | |
| **Remote maintenance/access scope** | |
| **Recovery and operational stability** | |
| **Backup and handover training** | |

Implemented by: _____ Reviewed by: _____ Date: _____