YZW1000

Industrial communication and edge computing gateway



USER MANUAL

2 × Gigabit SFP

8 × Gigabit RJ45

3 × RS485
2 ext. + 1 internal

Dual DC inputs

PoE • af/at/bt

Node-RED included

m2mCloud

−30 to 75 °C

Document version V1.5 • Installation, configuration and maintenance

CONTENTS

1. Gateway introduction 5
1.1 Product overview 6
1.2 Variants and options 7
1.3 Solution 1: remote PLC/HMI maintenance 8
1.4 Solution 2: instrument and PLC data to cloud 9
1.5 Solution 3: fibre primary and cellular backup 10
1.6 Solution 4: PoE camera power and networking 12
1.7 Solution 5: edge data processing and integration 13
1.8 Prerequisites and capability boundaries 14

2. Interfaces, installation and connections 15
2.1 Interfaces and indicators 16
2.2 Main specifications 18
2.3 Package and antenna connections 19
2.4 Dimensions and mounting position 19
2.5 SIM installation and power connection 21
2.6 RS485 wiring and port ownership 22

3. Basic operation and status 24
3.1 PC connection and Web login 25
3.2 Web interface layout 27
3.3 Device, uplink and client status 28

4. Network settings 31
4.1 WAN settings 32
4.2 LAN settings 36
4.3 VLAN settings 37
4.4 Wi-Fi settings 39
4.5 Cellular settings 43
4.6 DHCP service 45
4.7 Link Configuration and failover 47
4.8 Load balancing 51
4.9 DDNS 54
4.10 PoE output and management 56

5. Applications 60
5.1 Choose acquisition and data processing 61
5.2 ICMP monitoring 62
5.3 Scheduled tasks 64
5.4 Network diagnostics 65
5.5 DTU transparent transport 66
5.6 PLC and instrument acquisition 72
5.7 PLC data reporting 75
5.8 Modbus acquisition and reporting 77
5.9 Modbus device connection 81
5.10 Modbus commands and addressing 83
5.11 Modbus cloud writes over MQTT 86
5.12 PLC cloud writes over MQTT 91
5.13 Node-RED runtime management 94
5.14 SNMP 95
5.15 Local MQTT Broker 97
5.16 Optional GPS 100
5.17 Alarm notifications 101
5.18 SMTP mail service 103

6. VPN 105
6.1 Choose remote access and tunnels 106
6.2 OpenVPN clients 108
6.3 OpenVPN server 110
6.4 WireGuard 114
6.5 ZeroTier 117
6.6 IPsec 119
6.7 L2TP client 121
6.8 L2TP server 122
6.9 GRE 124
6.10 VXLAN 125
6.11 DMVPN 127
6.12 PPTP client and server 128

7. Forwarding 131
7.1 NAT and port forwarding 132
7.2 Static routes 133
7.3 MASQ masquerading 135
7.4 QoS rate control 136

8. Firewall 138
8.1 Management ports and remote access 139
8.2 SPI filtering 141
8.3 Address filtering 142
8.4 Domain filtering 144

9. System management 146
9.1 Local logs 147
9.2 System time 148
9.3 Admin password management 150
9.4 Configuration backup and restore 151
9.5 Firmware upgrade 154
9.6 Reset button and recovery 156

10. Node-RED visual programming 158
10.1 Open the editor and understand nodes 159
10.2 Import and deploy flows 161
10.3 Export flows and maintain backups 167
10.4 Case: temperature conversion, filtering and MQTT reporting 168
10.5 Case: multi-point state and alarms 170

11. m2mCloud remote management 173
11.1 Client configuration and networking 174
11.2 Remote PLC/HMI program transfer 178
11.3 Remote serial access 179
11.4 Windows client: remote access 180
11.5 Linux client: login and bridge 181

12. Troubleshooting 183
12.1 Locate faults along the service path 184
12.2 Bilingual terms and section mapping 186

YZW1000

Start with your requirements

Choose the task and follow entries, save, tests, readback and diagnosis. M1 uses 现场测试工具.zip beside this PDF. For initial access use the next page; lab addresses are in the introduction.

YOUR REQUIREMENT	FUNCTIONS	PREREQUISITES	SOLUTION
Remote PLC/HMI maintenance	m2mCloud or suitable VPN + LAN	Platform/peer, vendor tool, addressing, L2/L3	1.3 Remote maintenance
Instrument data to cloud	RS485/Ethernet + acquisition + MQTT	Point map, communications, broker and schema	1.4 Data to cloud
Connectivity after fibre failure	WAN + cellular + Link Configuration	Cellular delivery, probes, application recovery	1.5 Uplink failover
Camera power and networking	PoE + LAN + WAN/NVR	Port/total budget, supply, video bandwidth	1.6 PoE video
Custom data processing	Acquisition + Node-RED + MQTT	Input schema, rules, nodes and output topic	1.7 Edge processing
Existing platform/system	Reuse protocol and schema	Protocol/map, authentication, integration owner	5.1 Acquisition choice
4G without public IP	m2mCloud or reachable VPN peer	Authorization, client, vendor tool	6.1 Remote-access choice
Multiple devices/sites	Plan subnets + platform/VPN	Unique subnets, scope, return path	1.8 Prerequisites and capability boundaries

FREQUENT OPERATIONS • DIRECT LINKS

First access and maintenance 2.5 SIM and power • 3.1 Web login • 9.3 Change password • 9.4 Back up and restore

Data and field connections 2.6 RS485 wiring • 5.1 Acquisition choice • 5.8 Poll and report • 5.6 PLC acquisition

Uplinks and diagnostics 4.1 WAN access • 4.7 Link Configuration • 4.8 Load Balance • 12.1 Troubleshooting

USE YOUR ORDERED CONFIGURATION

Standard: 4G plus dual-band Wi-Fi 6. The 5G variant has no Wi-Fi. GPS is optional and Node-RED is included. Replace example addresses, topics and points.

Keep settings, backups and actual verification results for maintenance. For formal project handover, use the site record and service acceptance and handover.

YZW1000

First use: from wiring to network access

Goal: sign in from one PC through YZW1000, establish the required network access, then add site services. Use your address plan when one exists.

Connect → **Sign in** → **Go online** → **Verify service**

STEP AND SECTION	WHAT TO DO
1 • Connect and power 2.5 SIM and power	Fit the SIM and antennas for the ordered variant; connect the PC to LAN. Router input is 12–55 V DC. PSE output requires 52–55 V DC; the supplied 12 V adapter cannot power PoE loads
2 • Sign in 3.1 Web login	Set the PC to obtain an address automatically. Standard factory LAN is 192.168.8.1/24; open http://192.168.8.1 and sign in with admin / admin. Follow delivery records for custom configurations
3 • Secure management 9.3 Change password	Change the admin password and verify login. Restrict WAN management; enable HTTPS when supported. Keep VPN, Node-RED and platform credentials separately
4 • Establish one uplink 4.1 WAN access	For fibre, select DHCP, static IP or PPPoE as provided upstream; for cellular, use the SIM and operator settings. Verify one uplink before adding failover or load balancing
5 • Test a LAN client 5.4 Network diagnostics	Test the gateway, an external IP, then DNS, followed by the actual service from the LAN PC. Verify router connectivity and client connectivity separately
6 • Add the required service 5.8 Poll and report	Configure acquisition for instruments and VPN or m2mCloud for remote access only as needed. Assign one service per serial port. Establish correct readback before enabling writes
7 • Keep a working backup 9.4 Back up and restore	Export configuration and record firmware, LAN, uplinks, serial assignments and topics. Retain actual verification results for maintenance and recovery

! If a step fails, diagnose that layer first. For example, check DNS when IP access works but names fail. If local acquisition has no value, check the serial link or slave before changing MQTT formatting.

CHAPTER

01

Introduction

Choose connectivity, acquisition, remote maintenance, PoE and edge processing for the project



YZW1000

1. Gateway introduction

1.1 Product overview

YZW1000 combines industrial connectivity, acquisition, remote maintenance and edge data processing, with fibre, Ethernet and ordered cellular access. Select VPN/m2mCloud, Modbus/PLC, MQTT, PoE and Node-RED to suit the project. Start with this chapter's five solutions, then follow the configuration chapters. Capabilities follow ordered hardware and delivered firmware; assign each physical serial port to one service.

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.

CORE FUNCTIONS

- 2 Gigabit SFP slots and 8 Gigabit RJ45 ports with configurable WAN/LAN roles
- 3 RS485 ports: 2 external and 1 on the internal PCB
- Modbus TCP/RTU master and PLC/instrument acquisition with MQTT cloud writes
- m2mCloud networking, site access and PLC/HMI program transfer and maintenance
- OpenVPN, WireGuard, ZeroTier, IPsec and L2TP tunnel configuration
- Per-port PoE output management and Node-RED on the standard NAND variant

1.2 Variants and options



Figure 1-1 Variants and options

CONFIGURATION	DESCRIPTION
Standard 4G variant	4G cellular Internet access plus dual-band Wi-Fi 6 (2.4 GHz and 5 GHz)
Optional 5G variant	Select at ordering for 5G cellular Internet access; Wi-Fi is unavailable and cannot be ordered with this variant
Optional GPS positioning	Available at ordering for either variant, using a separate GPS antenna connector
Standard memory/storage	512 MB DDR3 and 512 MB SPI NAND Flash; no eMMC
Node-RED	Standard; runtime version follows the delivered firmware

“5G” means the cellular network; “5 GHz” is a Wi-Fi frequency band. Specify the variant and any GPS option when ordering. Follow the delivered configuration; a menu entry alone does not mean the corresponding hardware is fitted.

1.3 Solution 1: remote PLC/HMI maintenance



1 Cabinet: gateway, PLC and DC
2 Pump station: field equipment
3 Office: engineering PC

Figure 1-2 Placement illustration; AI-generated generic scene, not a actual installation

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 Solution 2: instrument and PLC data to cloud



1 Electrical room: meters and PLC
2 Cabinet: gateway and separate power
3 Platform: MQTT data

Figure 1-3 Placement illustration; AI-generated generic scene, not a actual installation

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 Solution 3: fibre primary and cellular backup



1 Network cabinet: gateway and fibre
2 Primary fibre, cellular backup
3 Service: application recovery

Figure 1-4 Placement illustration; AI-generated generic scene, not a actual installation

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. Check modes, probe conditions and switching behavior in this manual Link Configuration section and the delivered UI. Verify each uplink first, then application recovery in a maintenance window.

1.6 Solution 4: PoE camera power and networking



1 Indoor cabinet: gateway and DC
2 Outdoor pole: PoE cameras
3 Control room: NVR / video platform

Figure 1-5 Placement illustration; AI-generated generic scene, not a actual installation

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 Solution 5: edge data processing and integration



1 Production line: temperature / pressure
2 Cabinet: Node-RED processing
3 Platform: state and alarm reception

Figure 1-6 Placement illustration; AI-generated generic scene, not a actual installation

FIELD TASK: VERIFY PROCESSING/REPUBLISHING WITH E1

The supplied field_temperature.json uses standard MQTT/JSON/Function nodes and separate input/output topics. Keep PC bench running and connect no control output.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
MQTT Broker	192.168.10.10:1884 / field / DemoOnly2026	Enter credentials in config node
Input / Output	plant/site1/raw / plant/site1/processed	Avoid feeding output back to input
Function	temperature × 0.1	Accept finite numbers only; separate raw value/unit

SAVE, TEST AND OBSERVE

1. Import/deploy field_temperature.json. Run python site_lab.py watch --topic plant/site1/processed --seconds 60 --expect temperature=25.5.
2. In another window run python site_lab.py publish --topic plant/site1/raw --set temperature=255. Expect temperature=25.5 and unit=C. Publish --payload INVALID next; inspect rejection in Debug with no valid output.
3. To consume M1, change input to plant/site1/plc1/data and extract from its actual payload structure. Inspect Debug first; payload structures vary.

PASS CRITERIA AND DIAGNOSIS

No output: inspect broker/auth/topics/JSON. Tenfold error: inspect duplicate scaling. Debug output alone does not prove republishing; verify the processed subscriber.

Finish and restore: Disable E1 and restore topics/credentials; do not connect its test output to production control.

1.8 Prerequisites and capability boundaries

Before use, identify the function you need and check the ordered gateway configuration, field equipment, network and external platform prerequisites.

CATEGORY	FUNCTIONS / PREPARATION	CONFIRMATION
Standard functions	Routing, licensed VPN/m2mCloud, acquisition, PoE management and Node-RED, as ordered/enabled	Check ordered hardware, firmware and current menus; test the relevant workflow
External services	SIM/APN, MQTT broker, platform account/authorization or reachable VPN peer/server	Prepare endpoints, credentials, subnets and access rights
PLC/instrument compatibility	A driver/protocol entry is not coverage of every model, version or data block	Obtain exact model/firmware and protocol/point map; verify one read-only point
Remote engineering	Vendor software/license, NIC binding, discovery method and PLC return route	Prove local reads/backup, then test the same remote service
Node-RED integration	Core-node examples here; third-party nodes, databases and notifications need assessment	Check dependencies, licenses, resources, faults and restart policy
PoE supply	90 W design maximum per port, 720 W total; PSE input 52–55 V DC	Size for worst-case loads plus router/path losses; test dual-DC changeover
Example versus test	Site scenes/addresses are illustrative; isolated Node-RED tests are not field tests	Record Pass / Fail / Untested / Not applicable and supporting evidence

Before implementation: configure when prerequisites are met; obtain missing platform/protocol data; assess custom integrations first; leave untested compatibility, PoE loading and program transfers for field acceptance.

> PoE 90 W/port and 720 W total are design limits; sustained full load and dual-DC changeover remain unverified. See 4.10 PoE output for supply conditions and budgeting.

CHAPTER

02

Installation

Identify interfaces and connect the SIM, antennas, power and serial equipment



YZW1000

2. Interfaces, installation and connections

2.1 Interfaces and indicators

Identify physical connectors and the ordered variant before connecting any cables. Follow the markings on the enclosure.

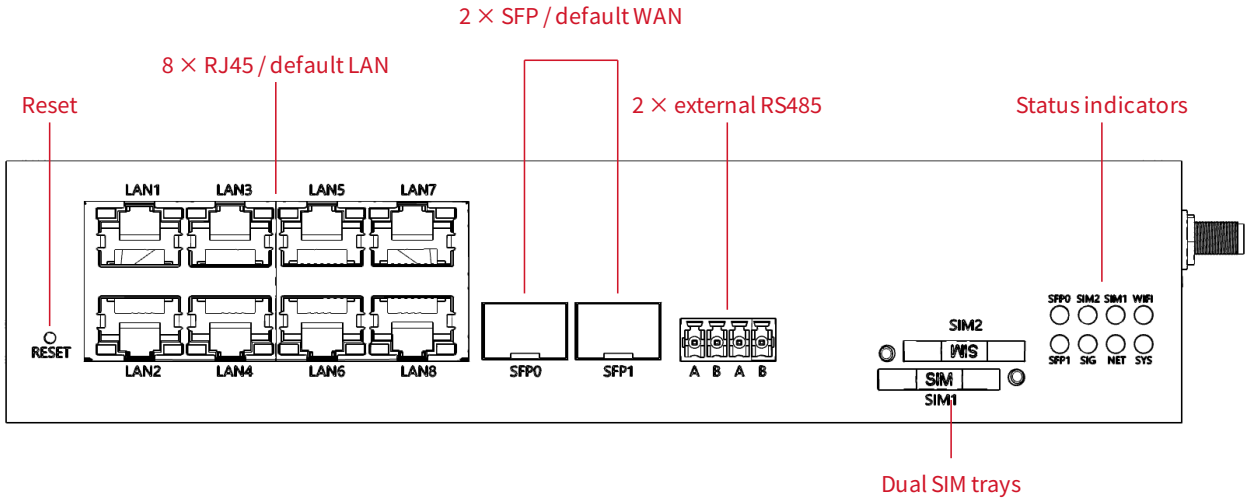


Figure 2-1 Interfaces and indicators

The standard 4G variant provides dual-band Wi-Fi 6. On the 5G variant, the Wi-Fi antenna connectors are reassigned to 5G, and the 5G variant has no Wi-Fi. GPS is an independent hardware option for either variant.

> Check: connector counts, input voltage and wireless variant match the order. SFP transceivers are not included.

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 wireless is enabled on a Wi-Fi-equipped build.	Check wireless on the4G/Wi-Fi build. The mutually exclusive5G build has no Wi-Fi; do not diagnose it using this LED.
SIM1 / SIM2	Current software lights the selected card’ s established data session; this is not merely card-insertion detection.	If off, inspect recognition, selection and dialing separately. Card presence/recognition is not a data session; dual-modem builds need their own owner mapping.
SFP0 / SFP1 (optical)	Used to observe the corresponding optical link; do not infer speed from unconfirmed colors/cadence.	Module insertion is not link-up. Inspect module, fiber TX/RX, peer and Web link state without assuming copper-LED behavior.
8 integrated RJ45 indicators	Inspect link/activity per port; distinguish Link/Act from separate speed LEDs.	Data-link indication does not prove PSE output; inspect PoE power state and the camera stream separately.

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
Platform	MediaTek MT7981
RAM / Flash	512 MB DDR3 / 512 MB SPI NAND Flash
Optical / copper ports	2 × Gigabit SFP (default WAN) / 8 × Gigabit RJ45 (default LAN)
Serial	3 × RS485: 2 external, 1 internal
SIM	2 × pull-out Nano-SIM trays; one cellular modem with SIM switching
Power	Dual primary/backup DC inputs, 12–55 V DC
Dimensions / weight	202 × 121 × 45 mm / 450 g
Enclosure / protection	Metal / IP30
Operating temperature	−30 to 75 °C
Mounting	Ears supplied; DIN-rail mounting supported
PoE	RJ45 IEEE 802.3af/at/bt PSE with automatic PD negotiation; PSE input requires 52–55 V DC

SYS, NET, SIG, WIFI, SIM1, SIM2 and SFP LEDs indicate the corresponding states; RJ45 ports have network indicators. LEDs assist diagnosis but do not replace runtime and actual service checks.

2.3 Package and antenna connections

4G + Wi-Fi variant



1–2: Wi-Fi 3–4: 4G

5: GPS (optional)

Match the numbered positions 1–5

5G variant (no Wi-Fi)



1–4: 5G cellular antennas

5: GPS (optional)

Match the numbered positions 1–5

Figure 2-2 4G/Wi-Fi and 5G antenna connections; GPS optional

ACCESSORY	**QUANTITY OR VARIANT**
Power adapter	1, 12 V DC output
Mounting ears	Included
RS485 terminal	1 × 4-pin, A / B / A / B
Power terminal	1 × 4-pin, V1+ / V1− / V2+ / V2−
4G variant antennas	2 Wi-Fi + 2 4G antennas
5G variant antennas	4 5G antennas, without Wi-Fi antennas
GPS antenna	1 when GPS is ordered
SFP transceivers	Not included

On the 4G variant, ANT-RES1/ANT-RES2 connect Wi-Fi and Cellular1/Cellular2 connect 4G. All four connect 5G antennas on the 5G variant. Use GPS only for the optional GPS antenna.

2.4 Dimensions and mounting position

Dimensions describe the enclosure and exclude projecting antenna connectors. Use mounting ears or the matching DIN-rail arrangement and leave clearance for terminals, trays and cable bends.

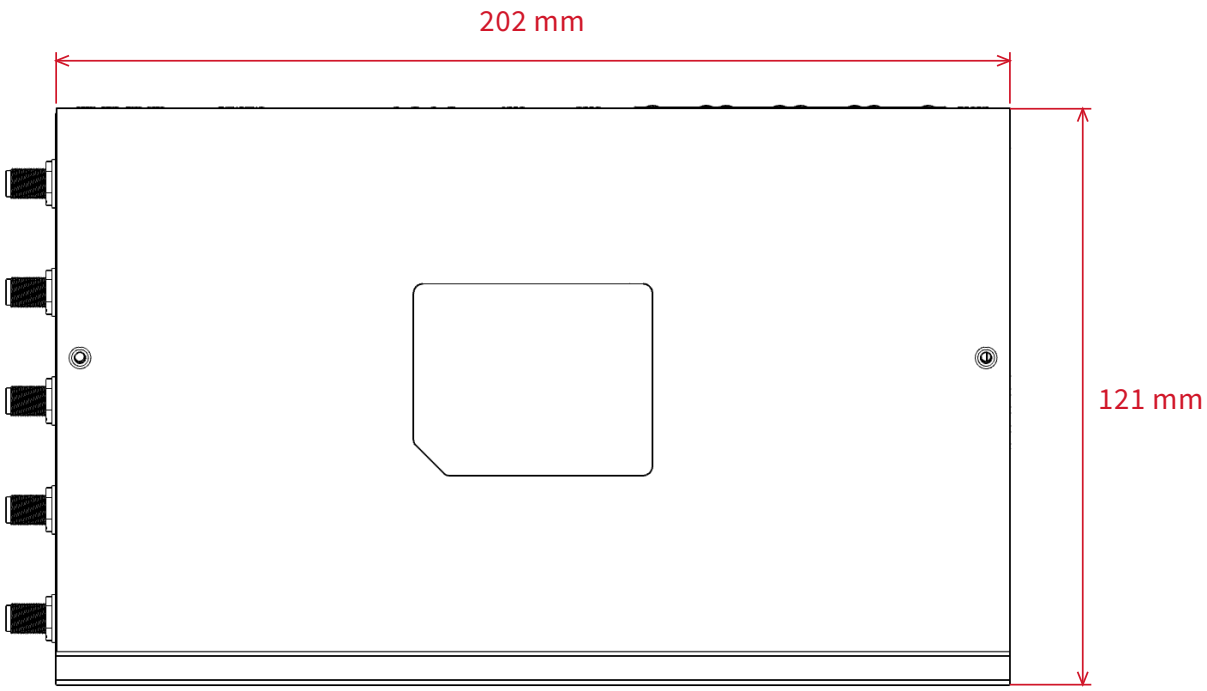


Figure 2-3 Top-view enclosure dimensions

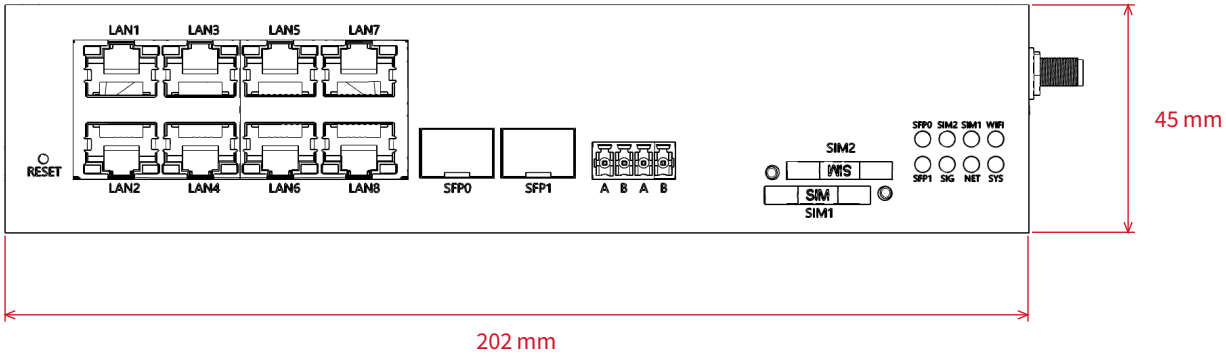


Figure 2-4 Front-view enclosure dimensions

2.5 SIM installation and power connection

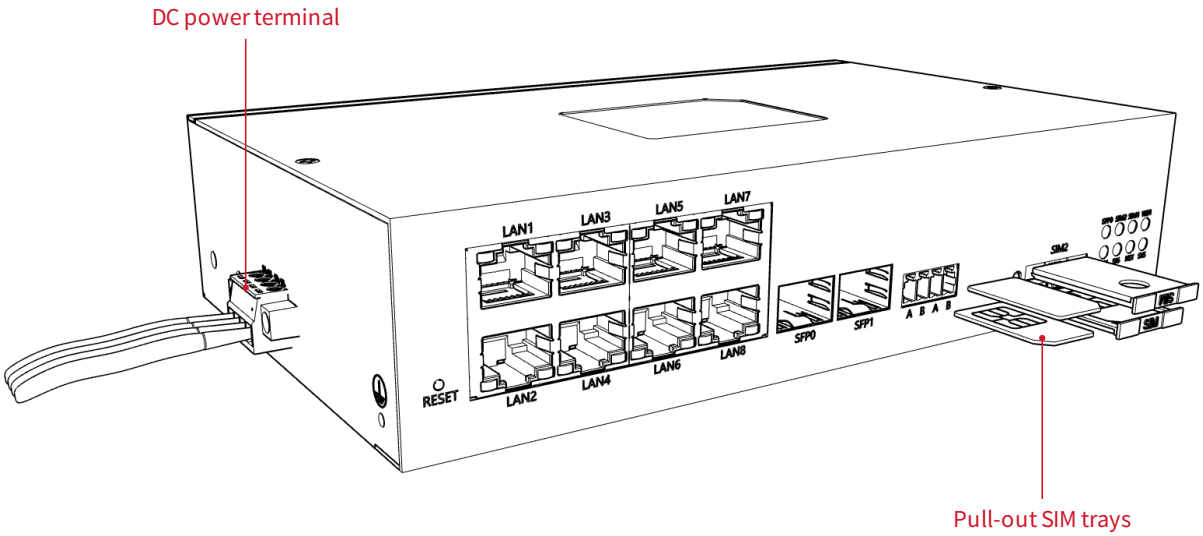


Figure 2-5 SIM tray and DC power connection locations

1. Disconnect power. Remove the required SIM tray and fit a Nano-SIM card in the orientation shown.
2. Slide the tray back into its original slot until fully seated. This model uses pull-out trays, not push-push SIM slots.
3. Connect DC power using the table and terminal markings. Check polarity and voltage; use the two input pairs for primary/backup supply.
4. Attach the cellular, Wi-Fi and optional GPS antennas for the ordered variant, then connect network cables. Check the trays and wiring before powering up.

TERMINAL MARKING	**WIRING DEFINITION**
V1+ / V1−	First DC input: positive / negative
V2+ / V2−	Second DC input: positive / negative, for primary/backup supply

Router power: 12–55 V DC input. The package includes 1 × 12 V DC adapter. Both terminal pairs are power inputs, not accessory power outputs.

PoE output requires 52–55 V DC input; the supplied 12 V adapter powers the router itself. See “PoE power and management” for per-port checks.

> **Check the result** The router can be reached over LAN after startup; PSE use has 52–55 V DC input.

2.6 RS485 wiring and port ownership

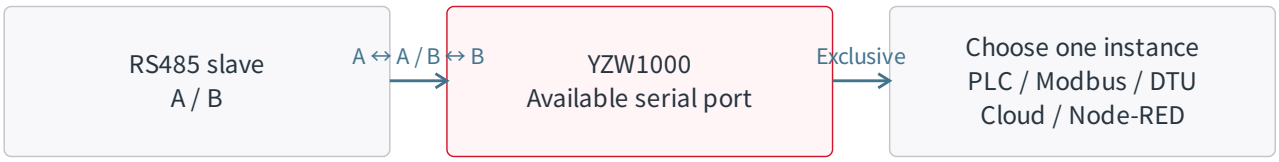


Figure 2-6 RS485 wiring and port ownership

WIRING POSITION, VIEWED FROM THE FRONT	SOFTWARE PORT	CONNECTION AND PURPOSE
Left A / B pair on the external 4-pin terminal	Serial1	First external RS485; connect A to slave A and B to slave B
Right A / B pair on the external 4-pin terminal	Serial2	Second external RS485; connect A to slave A and B to slave B
RS485 on the internal PCB	Serial3	Internal connection, not brought through the enclosure; do not select it for external wiring

CONNECT AND VERIFY ONE SLAVE

1. Disconnect power before wiring. Identify A / B from the terminal labels; follow the slave and site requirements for bus wiring and termination.
2. Select Serial1 in Modbus Collect, PLC Collect or DTU for the left pair; select Serial2 for the right pair.
3. Match baud rate, data bits, stop bits, parity and slave address. Assign one service to each physical serial port at a time; different ports can operate independently.
4. Read one known point and compare it with the instrument display or vendor tool. Expand the point list after readback is stable.

> For persistent timeouts, check the selected port against the wiring position first, then A/B, communication settings and slave address. Do not enable multiple services on the same serial port.

INSTALLATION INFORMATION TO CHECK BEFORE WIRING

Use the front-view A/B/A/B terminals for Serial1 and Serial2; do not connect A/B to a power terminal. V1+/V1−/V2+/V2− belong to the two power inputs. Disconnect power before inserting or removing the keyed terminal blocks and SIM trays. Serial3 is on the internal PCB, not a third externally accessible terminal; use the supplier-confirmed integration method.

Follow the actual bus design and verified installation drawing for shielding, equipotential bonding and termination. Unconfirmed terminal pitch/current, strip length, torque, conductor size and mounting-hole spacing are not inferred here; obtain the drawings and ratings for the delivered hardware before installation. Do not treat the chassis or supply negative as an additional RS485 signal pin.

Check the result Wiring matches Serial1 / Serial2 and one known point reads correctly over repeated polls.

CHAPTER

03

Getting started

Set up PC access, sign in and inspect device and link status



YZW1000

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 PC connection and 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.

> 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

Change the admin password on first use and verify a new login. Restrict WAN management and allowed source addresses while keeping a recoverable local access path. When HTTPS is available in the delivered firmware, enable it through management access settings and check certificate indications. Keep VPN, Node-RED and platform credentials separately; do not reuse the public initial password. The actual 5–16-character ASCII rule is retained; mandatory first-login changes, multiple accounts and a stronger password policy are not claimed.

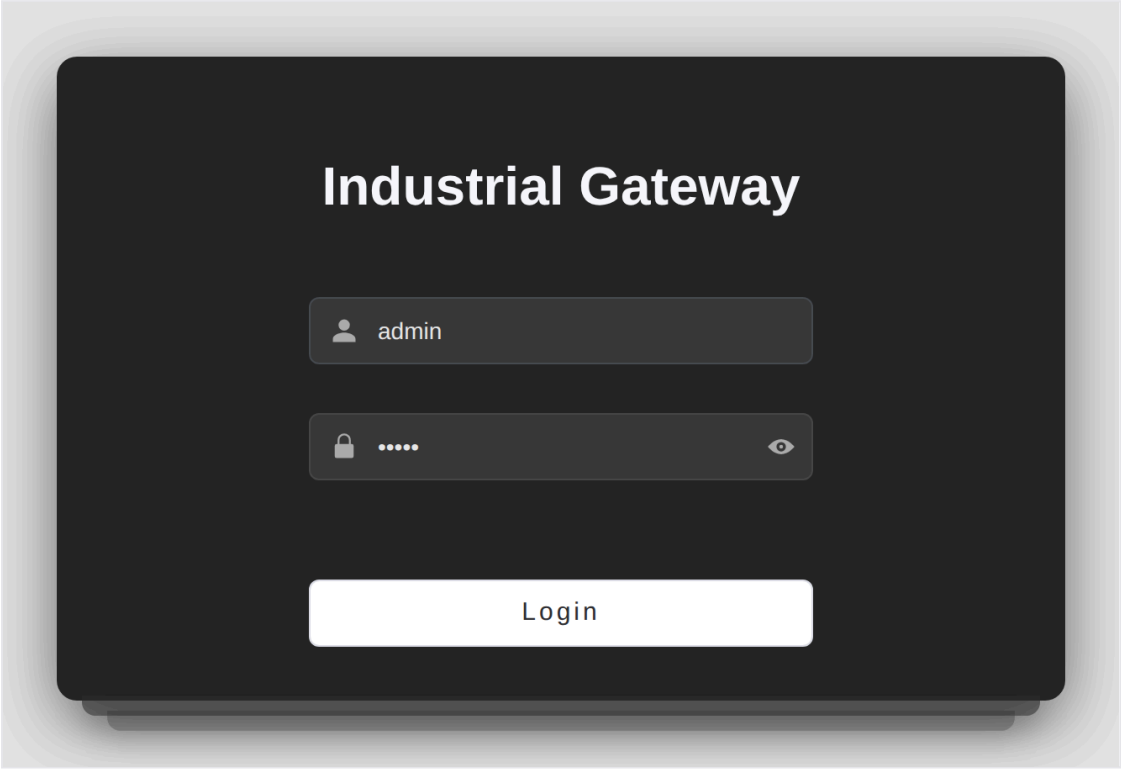


Figure 3-2 Web login

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

3.2 Web interface layout

Path Overview

The left menu groups pages by function. Expand a group to select a page. Port indicators appear at the top, with configuration and runtime information on the right; check configured and actual states separately.

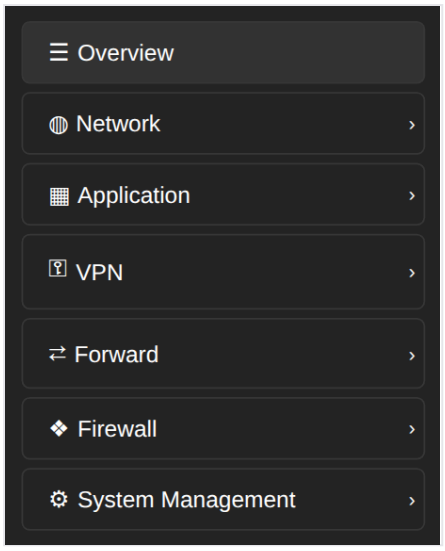


Figure 3-3 Main menu groups

AREA	USE
Port status	Check link and roles. Enclosure SFP0/SFP1 and some firmware UI labels differ; confirm the delivered mapping
Menu	Network, Application, VPN, Forward, Firewall and System Management group the corresponding functions
Configuration list	Identify the connection/rule being edited; new-form example values are not saved configuration
Runtime	Check actual results separately from settings; addresses, online state and service success are distinct

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

3.3 Device, uplink and client status

Path Overview

Overview identifies model, firmware, uptime, active egress, resource use and clients. Inspect detailed WAN/LAN, wireless, VPN and SFP state on the relevant configuration pages; not every firmware has a separate Status menu.

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.

DEVICE INFORMATION: CHECK THE MODEL AND FIRMWARE

Read the model, software version and uptime in the Overview device information area. Include the software version in maintenance records so that it can be matched to firmware files and delivered functions.

CURRENT UPLINK: IDENTIFY THE ACTIVE EGRESS

Use connection type, interface, IP, gateway and DNS to identify the active egress. An addressed standby link is not necessarily carrying current traffic.

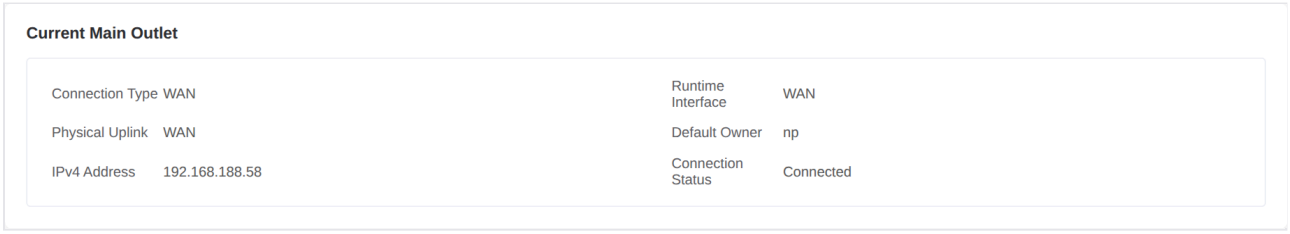
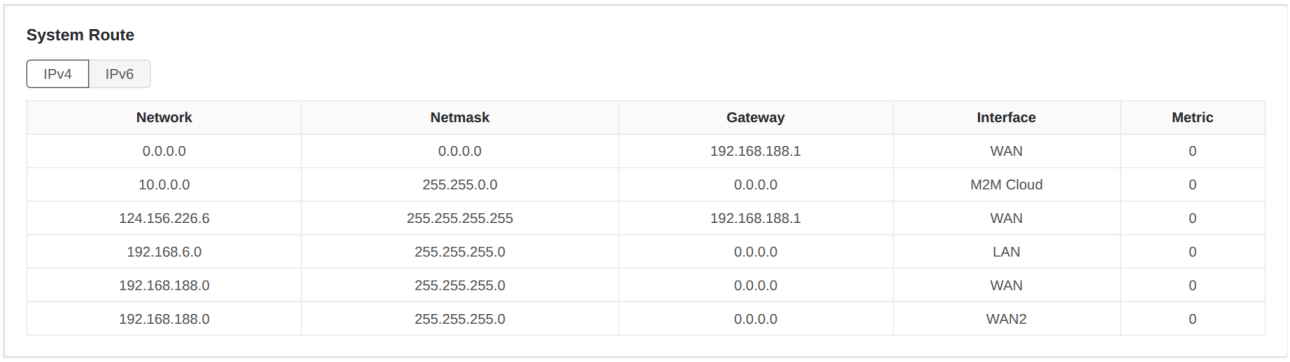


Figure 3-4 Current uplink

ROUTES AND CLIENTS: CHECK PATHS AND ATTACHMENT

A default route supplies the next hop for otherwise unmatched networks; specific routes match their destination subnets. Use the client list for attachment checks; static or undiscovered clients may not appear.



Network	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.188.1	WAN	0
10.0.0.0	255.255.0.0	0.0.0.0	M2M Cloud	0
124.156.226.6	255.255.255.255	192.168.188.1	WAN	0
192.168.6.0	255.255.255.0	0.0.0.0	LAN	0
192.168.188.0	255.255.255.0	0.0.0.0	WAN	0
192.168.188.0	255.255.255.0	0.0.0.0	WAN2	0

Figure 3-5 Current routing table

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

CHAPTER

04

Network settings

Configure optical, Ethernet, wireless and cellular links, and PoE output



YZW1000

4. Network settings

4.1 WAN settings

Path Network > WAN

Select the WAN connected to the upstream network and use the addressing method required by that network. YZW1000 defaults to two WANs, with both SFP slots assigned to WAN.

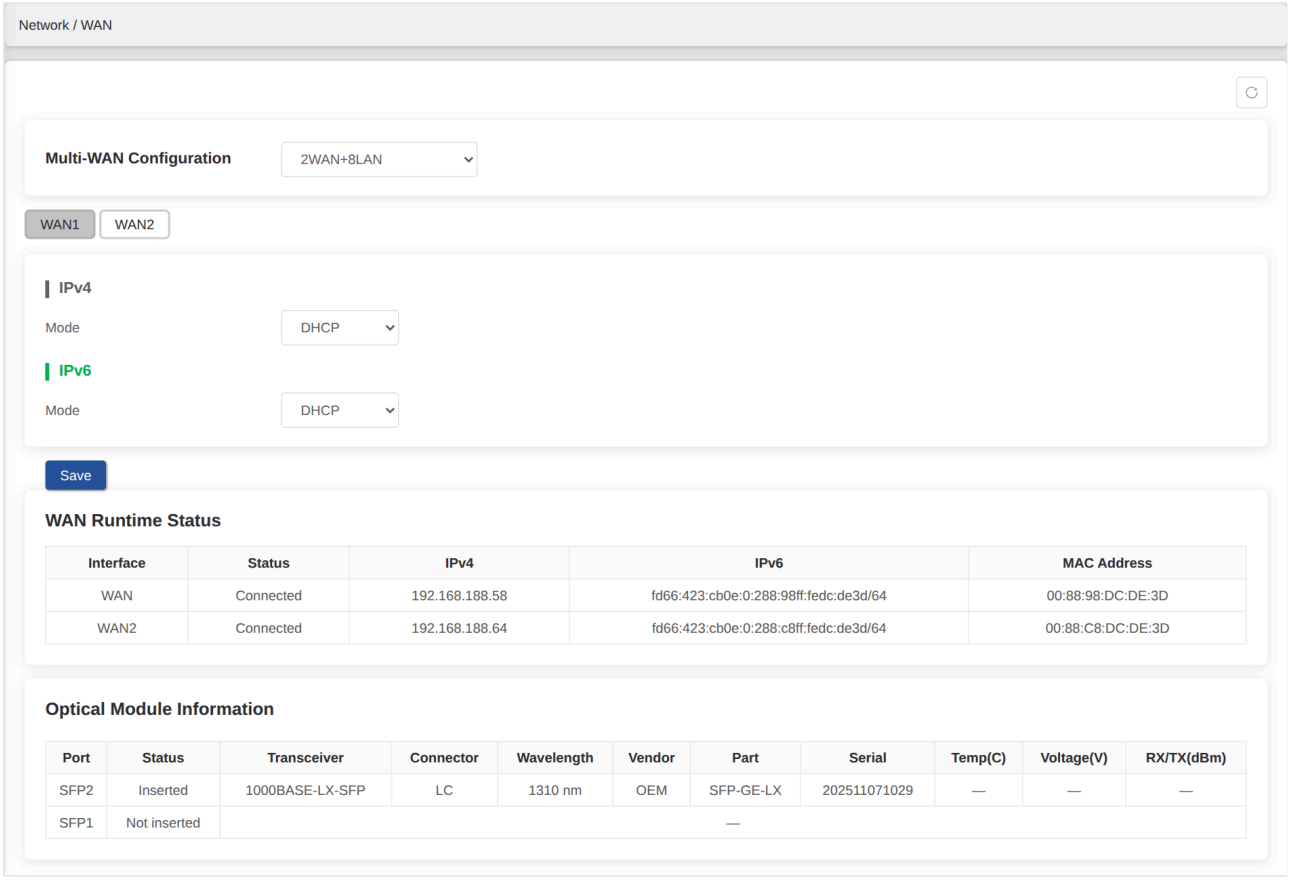


Figure 4-1 WAN settings

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

UI FIELD	ENTRY	BASIS
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.

MATCH THE UPSTREAM ACCESS METHOD

INFORMATION SUPPLIED UPSTREAM	METHOD	WHAT TO ENTER
Address assigned automatically after connection	DHCP	Select DHCP; no static address or broadband credentials
Assigned address, mask, gateway and DNS	Static IP	Enter the assigned values; do not choose an apparently unused address yourself
Broadband username and password	PPPoE	Enter operator credentials, not the Web admin account

BRING ONE WAN ONLINE FIRST

1. Match the connected optical port to the WAN shown on the page. SFP transceivers are not included and must match the peer speed and fibre link.
2. Select the WAN and access method, then enter its required settings. Leave other link policies unchanged while establishing this uplink.
3. Save and inspect the runtime address, mask, gateway and connection state. LAN and WAN subnets must not overlap.

4. In Diagnostics, test the upstream gateway, a permitted external IP, then a domain name. Next test the actual service from a LAN PC.

> A WAN address confirms address configuration only. If external IP access works but names fail, check DNS first. If the router can connect but a LAN PC cannot, check the PC gateway, DNS, routes and forwarding rules.

CONFIGURE A STATIC ADDRESS IN THE CORRECT ORDER

Select Static, enter the assigned address and mask, then enter the gateway and DNS for that uplink. Use values from the same network plan.

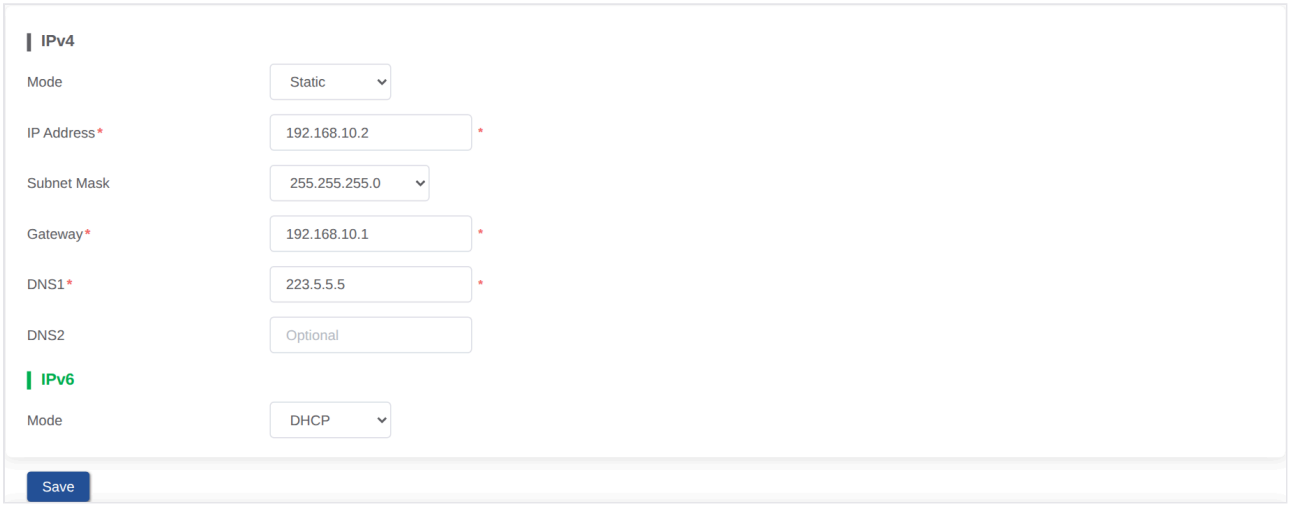


Figure 4-2 Static IPv4 configuration

BEFORE AND AFTER CHANGING THE MULTI-WAN LAYOUT

Multi-WAN Configuration assigns physical WAN/LAN roles. Individual WAN tabs configure addressing. Link Configuration then determines failover use of those interfaces.

1. Export a backup and identify upstream cables versus field clients. Connect the PC to a port planned to remain LAN.
2. Confirm the layout. This model defaults to 2WAN+8LAN and offers 1WAN+9LAN through 4WAN+6LAN. A role change affects that port; old LAN wiring assumptions may no longer apply.
3. Open each WAN tab in the new layout and set DHCP, static IP or PPPoE. Check for LAN/upstream subnet overlap.
4. After saving, check the top bar, WAN runtime state and actual port use. If management disconnects, reconnect using the new plan rather than repeatedly saving.
5. Revisit Link Configuration or Load Balance, check participating interfaces/probes and test the service from a LAN client.

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

LINK AND ADDRESS MODE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Multi-WAN Configuration	Assign WAN/LAN roles. This model defaults to 2WAN+8LAN and provides layouts from 1WAN+9LAN to 4WAN+6LAN
2	WAN1 / WAN2	Select the WAN to configure before editing its settings. Confirm enclosure-to-UI optical-port mapping
3	Mode	DHCP obtains an address; Static uses assigned settings; PPPoE uses ISP credentials; LAN joins the LAN network

ADDRESSING AND DIAL PARAMETERS

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
4	IP Address / Subnet Mask	For Static mode, use the assigned address and mask without conflicting with LAN or other site subnets
5	Gateway	Use the upstream next hop for this WAN, not the router LAN address
6	DNS1 / DNS2	DNS resolvers. Check them when IP access works but names fail
7	PPPoE Username / Password	Use ISP-provided broadband credentials, not the router Web account
8	Authentication / Compression	Match advanced PPP authentication and compression to the provider

PACKET AND RUNTIME PARAMETERS

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
9	MTU / MRU / MSS	Control transmit, receive and TCP segment sizes; use provider or network requirements
10	IPv6	Configure addressing, prefix, gateway and DNS separately; the upstream must support the selected IPv6 access
11	Runtime / Optical Module Information	Check addresses and link state. Module insertion, link and service reachability differ; basic information does not imply full DDM

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.
SFP information is present but the link is down	Check module speed, fiber type, peer port and transmit/receive pairing, then inspect the interface state.

4.2 LAN settings

Path Network > LAN

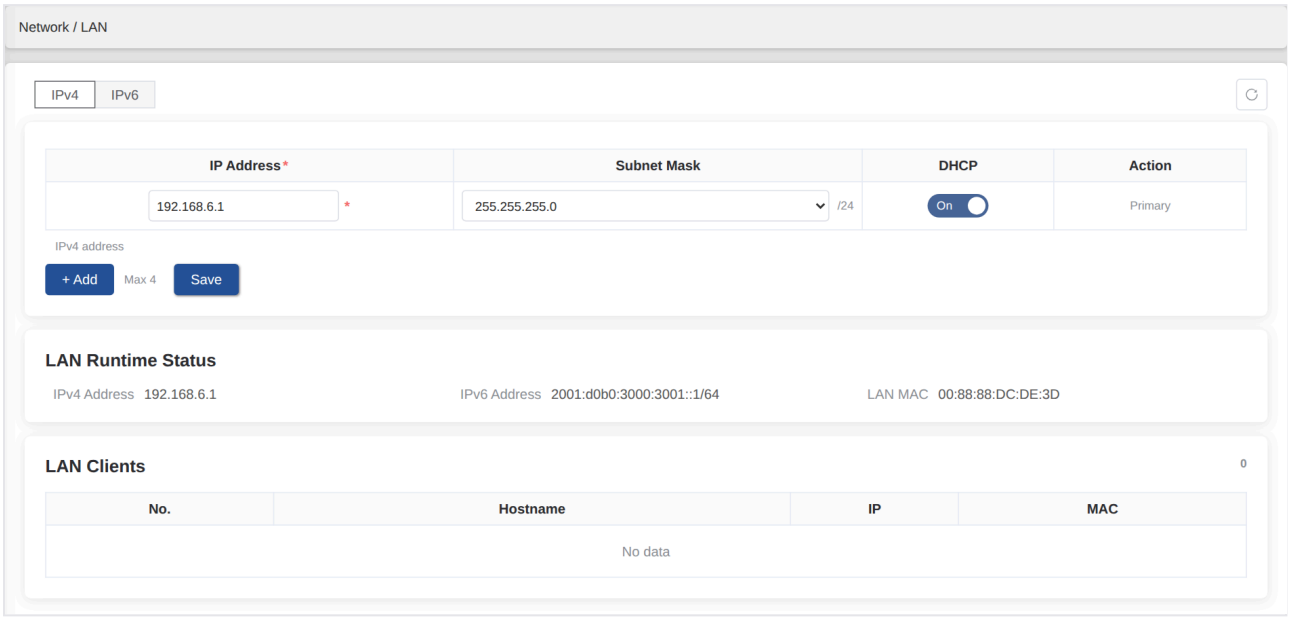


Figure 4-3 LAN settings

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.

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

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

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.

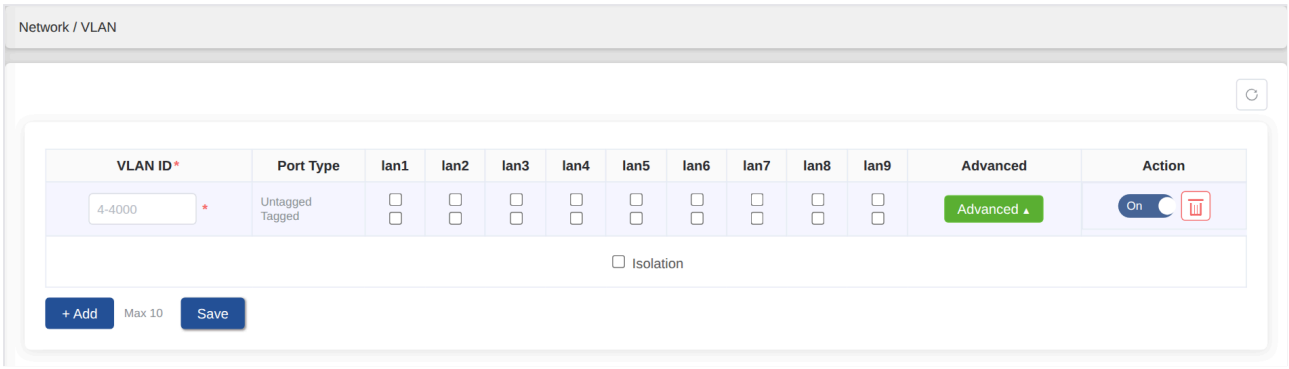


Figure 4-4 VLAN settings

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.

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	VLAN ID	Tag identifying a Layer-2 network; coordinate both ends of the link
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

4.4 Wi-Fi settings

Path Network > WIFI2.4G / WIFI5.8G

On the 4G variant, ANT-RES1 / ANT-RES2 are Wi-Fi connectors and Cellular1 / Cellular2 are 4G connectors. All four serve 5G on the 5G variant, which has no Wi-Fi. Optional GPS uses its separate connector.

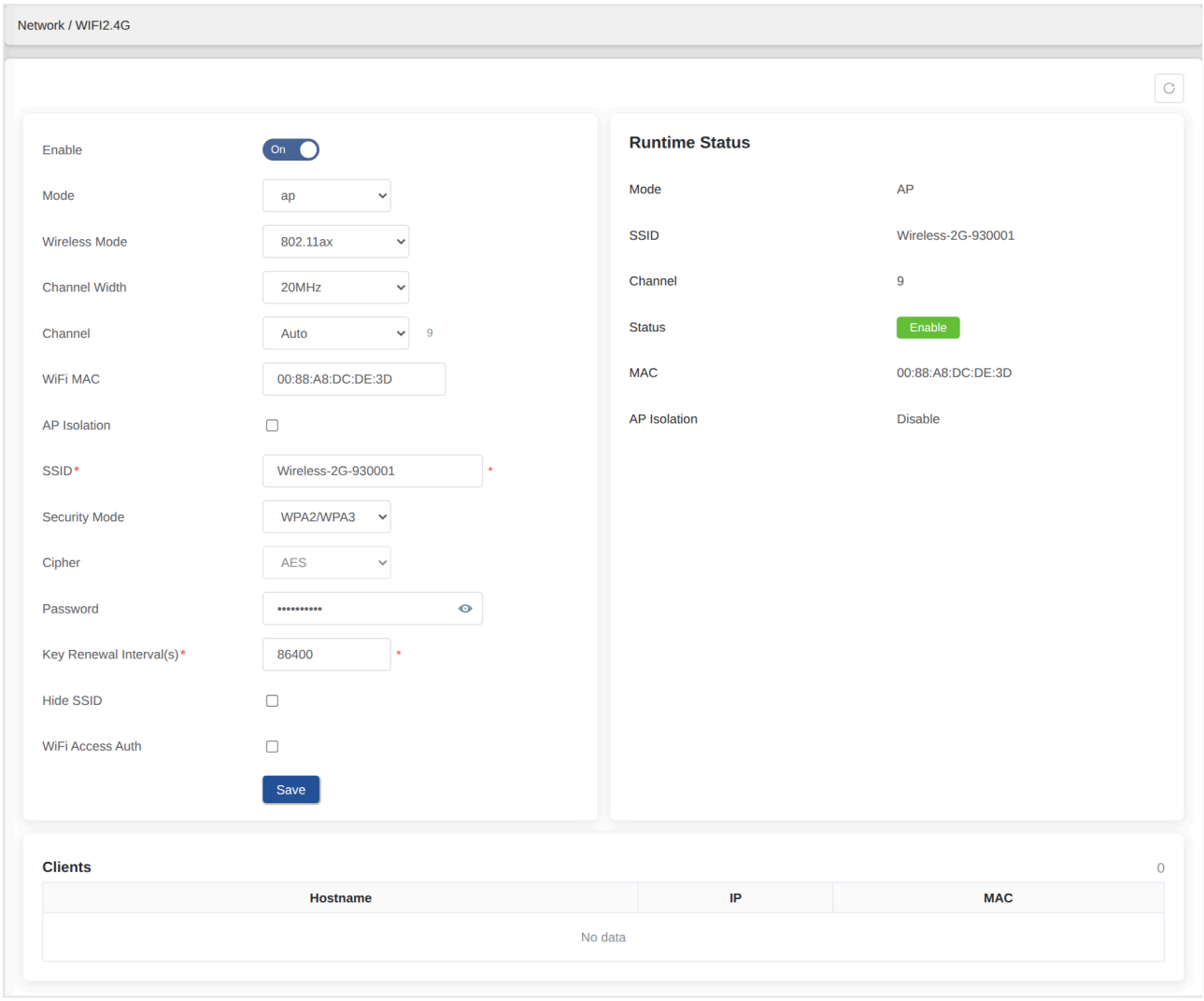


Figure 4-5 2.4 GHz Wi-Fi settings

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
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.

1. Confirm that the unit is the Wi-Fi-equipped 4G variant and attach both Wi-Fi antennas.
2. Open the required band page and configure the wireless mode, SSID and access password. Configure each band separately.
3. Save, connect a client to the SSID and check address assignment and actual network access.

> Verify: the client connects to the intended band and SSID and reaches the required network. Wi-Fi association alone does not prove Internet access. These steps do not apply to the 5G variant.

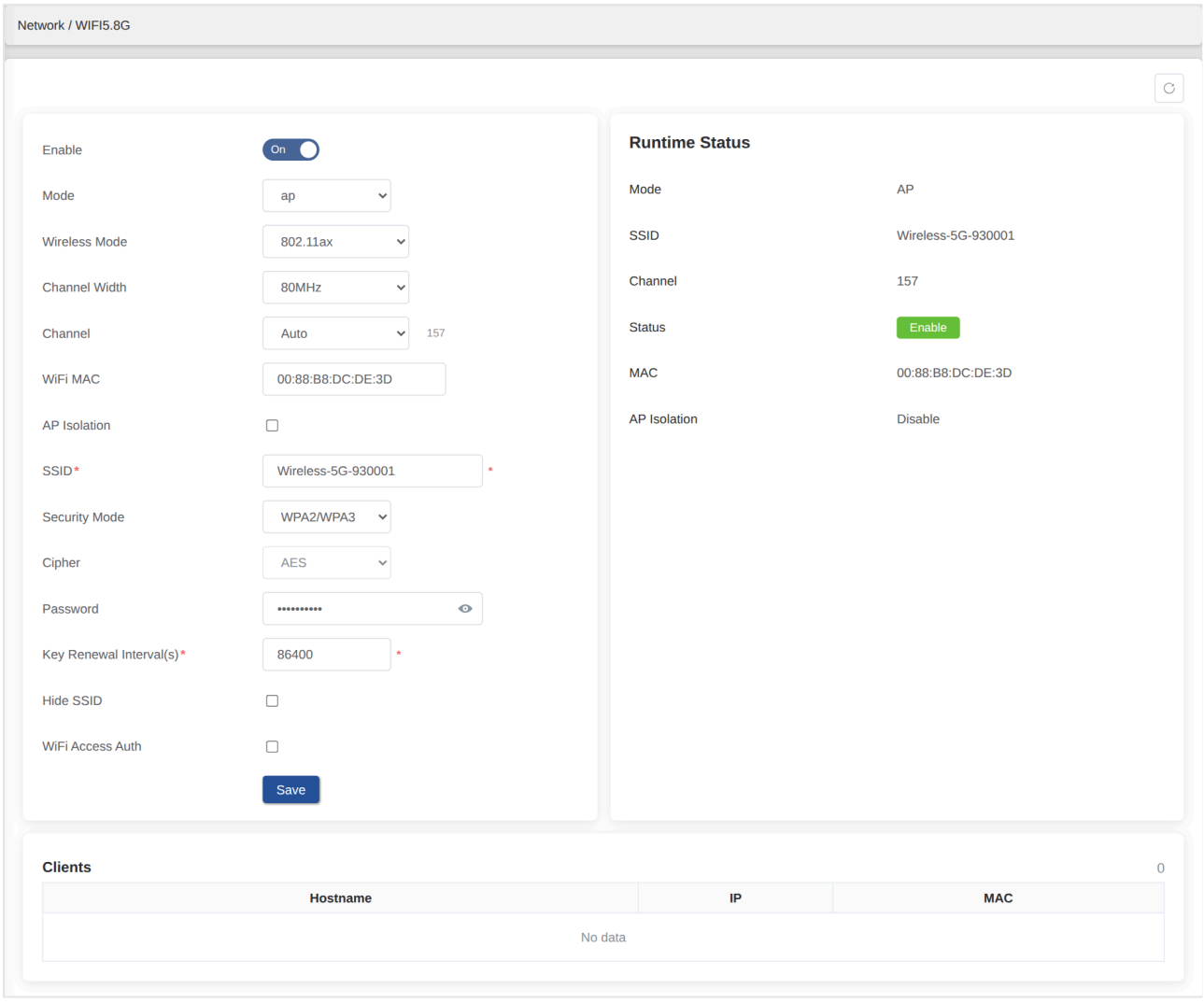


Figure 4-6 5 GHz Wi-Fi settings

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Band / Enable	Configure 2.4 GHz and 5 GHz separately on the 4G variant; cellular 5G variants have no Wi-Fi
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

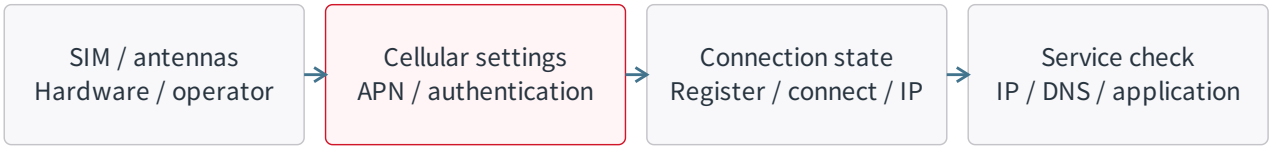
TROUBLESHOOTING

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.



Use fitted-module and operator settings; validate the link before services

Figure 4-7 Cellular connection and validation

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

UI FIELD	ENTRY	BASIS
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.

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

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

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

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.

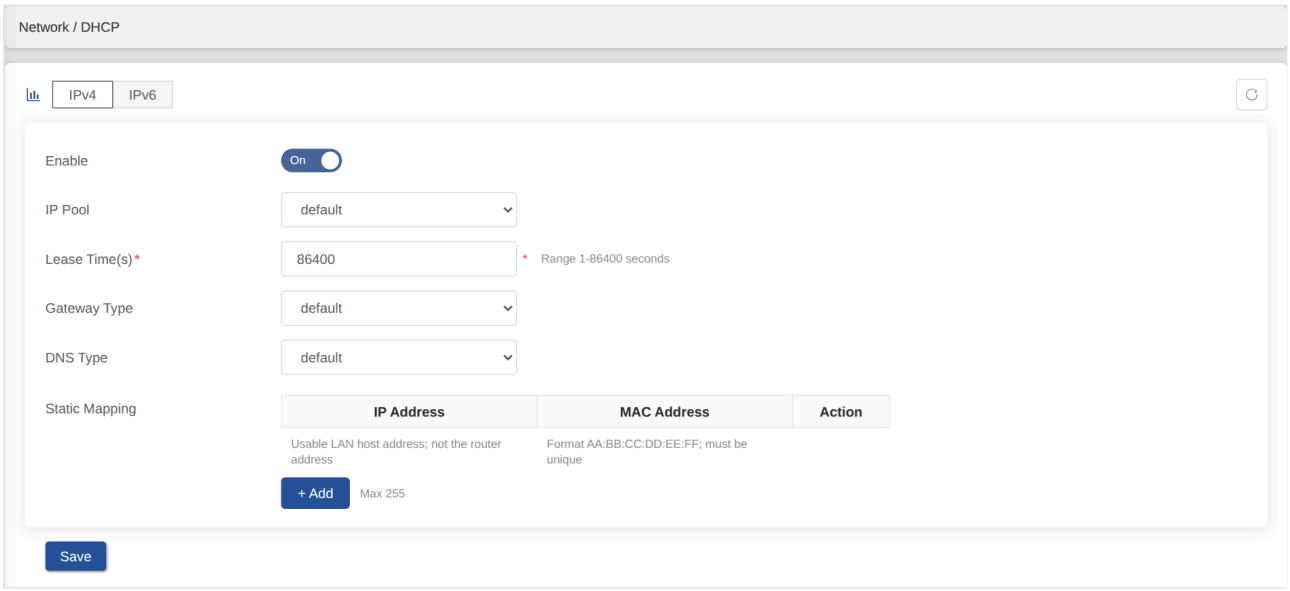


Figure 4-8 DHCP service

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

UI FIELD	ENTRY	BASIS
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.

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

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

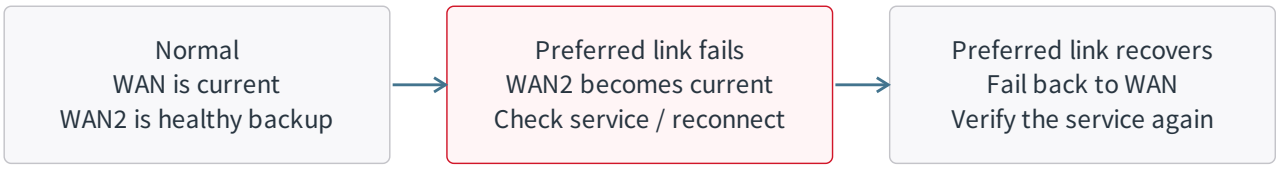
TROUBLESHOOTING

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

Link Configuration selects uplink priority and keepalive checks. Configure the individual uplinks first, then select their use policy. For distributing separate connections across exits, see Load Balance.



IPv4 dual-WAN example; check IPv6 separately. No fixed switchover time is implied

Figure 4-9 IPv4 dual-WAN failover and recovery example

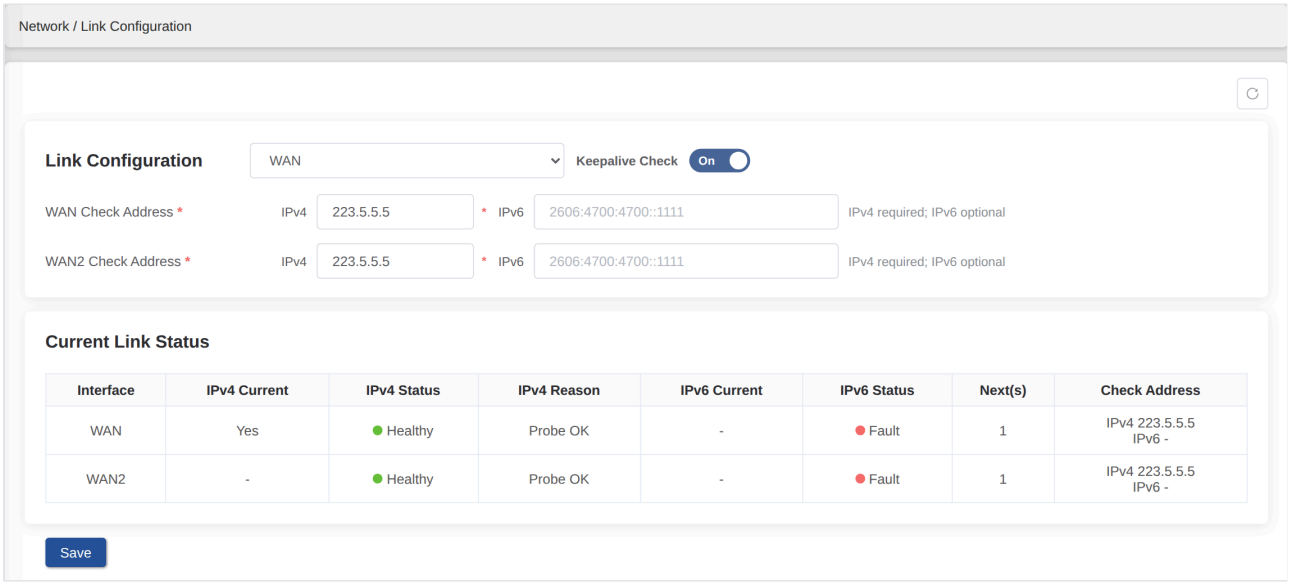


Figure 4-10 Link Configuration and current state

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. Check modes, probe conditions and switching behavior in this manual Link Configuration section and the delivered UI. Verify each uplink first, then application recovery in a maintenance window.

DISTINGUISH THE THREE CONFIGURATION JOBS

JOB	WHERE TO CONFIGURE IT	RELATION TO THIS PAGE
Set uplink addressing or broadband credentials	WAN, cellular or Wi-Fi Station page	This page does not replace DHCP, static IP, PPPoE, APN or wireless association settings
Use primary and backup links in priority order	Link Configuration	Select combinations, probes and inspect the current exit here
Distribute sources or connections across links	Load Balance	It conflicts with multi-link failover here; do not configure two competing outbound policies

WHY “WAN” MAY CONTAIN MORE THAN ONE LINK

WAN represents the group of wired interfaces currently assigned as WAN. YZW1000 defaults to two SFP WAN ports, so selecting WAN may show both WAN and WAN2 in the status table. That is multi-link operation and requires a keepalive address for each port.

Within the WAN group, participating interfaces are used in WAN, WAN2, WAN3, WAN4 order. Do not infer priority from enclosure SFP numbering or table-row position. Confirm the current physical-to-WAN mapping on this unit.

EXAMPLE MODE LABEL	PRIORITY FROM LEFT TO RIGHT	PREREQUISITE
WAN	WAN group in WAN-number order	Configure the participating wired ports on the WAN page first
WAN / WIFI5.8G	WAN group, then 5 GHz Station	Wi-Fi hardware fitted and that radio configured as an eligible Station uplink
WAN / Mobile	WAN group, then cellular	Cellular hardware/function enabled, registered and connected
WIFI5.8G / WIFI2.4G	5 GHz Station, then 2.4 GHz Station	Both radios must qualify as uplinks; an AP hotspot alone is not a Station uplink

Only combinations eligible on the current unit are offered. If an option is missing, check ordered hardware, enabled functions and interface operating mode before comparing with another device. Observe the ordered variant's 5G/Wi-Fi mutual exclusion.

ENTER KEEPALIVE ADDRESSES

The illustration shows a dual-WAN form. Each target must be reachable and answer ICMP through its assigned exit. For a private network, use a permitted target inside that network rather than copying screenshot addresses.

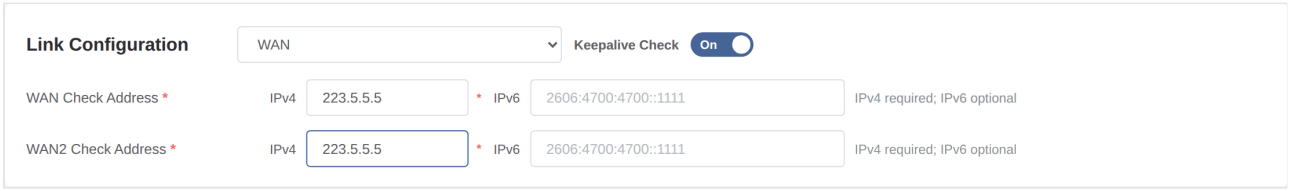


Figure 4-11 Dual-WAN keepalive address fields

1. With one actual participating interface, keepalive can be on or off. Off means this active connectivity check is not performed.
2. With two or more participating interfaces, keepalive is mandatory and every interface needs an IPv4 target; configuring only the primary is incomplete.
3. Enter a literal dotted-decimal IPv4 address, not a hostname. IPv6 targets are optional; use valid literal IPv6 addresses, separated by commas if several are entered.
4. After saving, inspect each address family separately. Cellular keepalive has the special behavior explained below.

READ CURRENT LINK STATUS

Healthy means the check or interface usability conditions are met. Current identifies the exit actually selected for that address family. A healthy backup that is not Current is normal in failover operation.



Figure 4-12 Current IPv4 and IPv6 link status

1. Read IPv4 Current, then the row state and reason. A healthy backup does not mean traffic is being distributed across links.
2. Check IPv6 Current and IPv6 Status separately. Working IPv4 does not establish working IPv6, and the two families need not select the same exit.
3. Use reasons such as No IP, STA Disconnected, LAN Subnet Conflict, No Target or Probe Failed to correct the corresponding prerequisite first.
4. Cellular IPv4 usability follows modem-assigned addressing and readiness. Keepalive packets keep the bearer active; their replies do not drive cellular failover. A private APN is not failed merely because a public probe target is silent.
5. After the preferred link meets recovery health conditions, priority-based failback applies. Existing sessions may require application reconnection; failover does not guarantee seamless retention of every session.

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Link Configuration	Use the selected mode from left to right; WAN is a wired group ordered by WAN number and may contain several ports
2	Keepalive Check	Optional for one interface; mandatory for several. Cellular probes keep the bearer active rather than determining failure from replies
3	IPv4 / IPv6 Check Address	Each multi-link interface requires a literal IPv4 target. IPv6 is optional; comma-separate several IPv6 targets. Do not enter hostnames
4	Current / Status / Reason	Distinguish selected exit, health and reason; inspect IPv4 and IPv6 independently. A backup can be healthy without being selected
5	Next(s)	Probe scheduling information; it does not establish a fixed switchover time for every scenario

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.

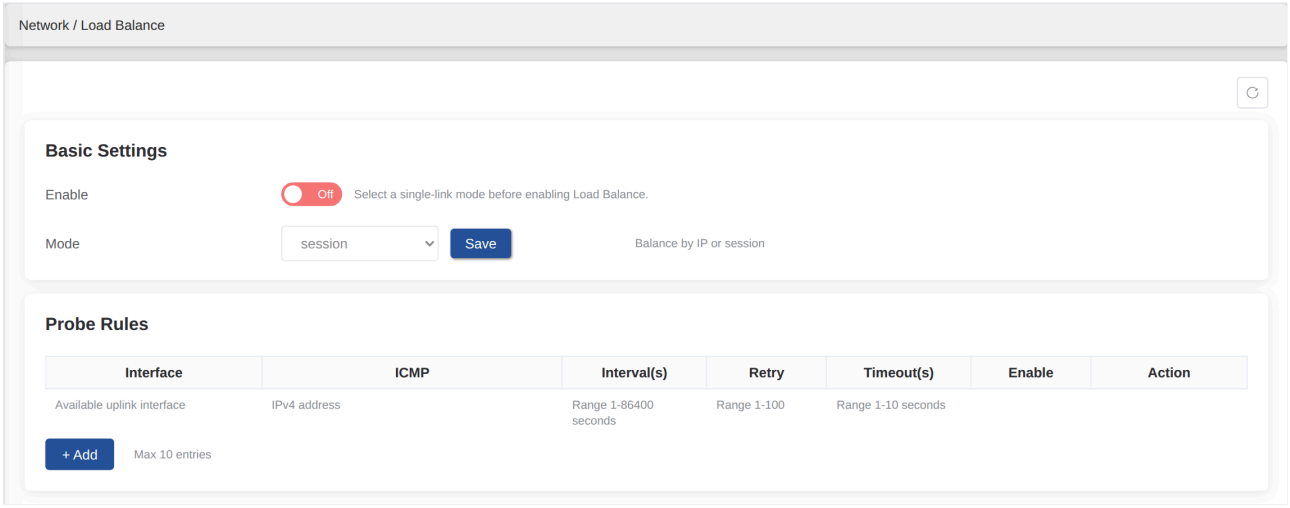


Figure 4-13 Load balancing

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.

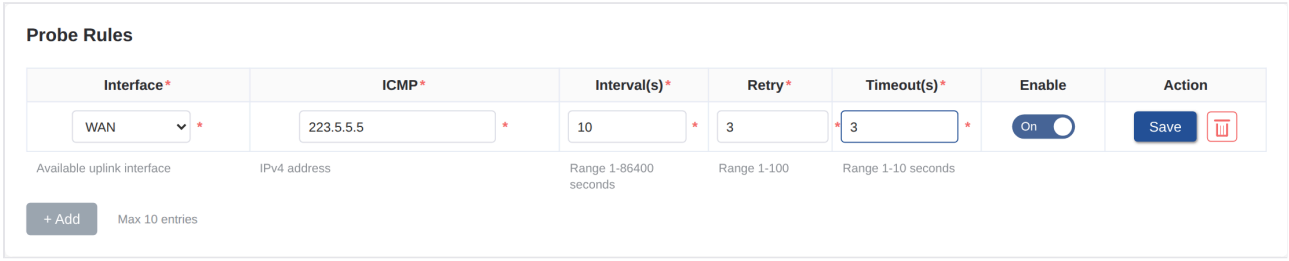


Figure 4-14 Load Balance rule example

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.

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

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
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

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.

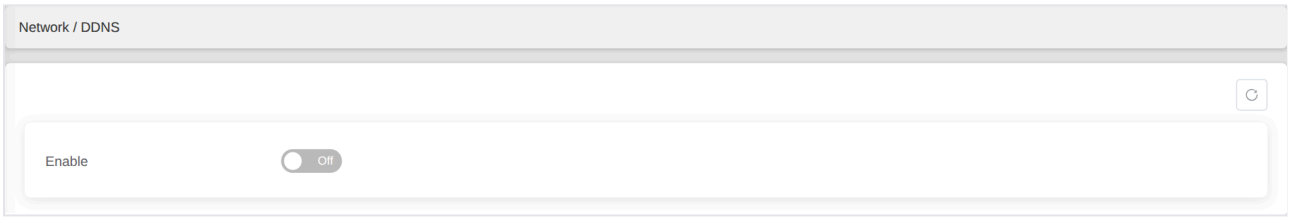


Figure 4-15 DDNS

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.

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

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

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.

4.10 PoE output and management

Path Network > PoE

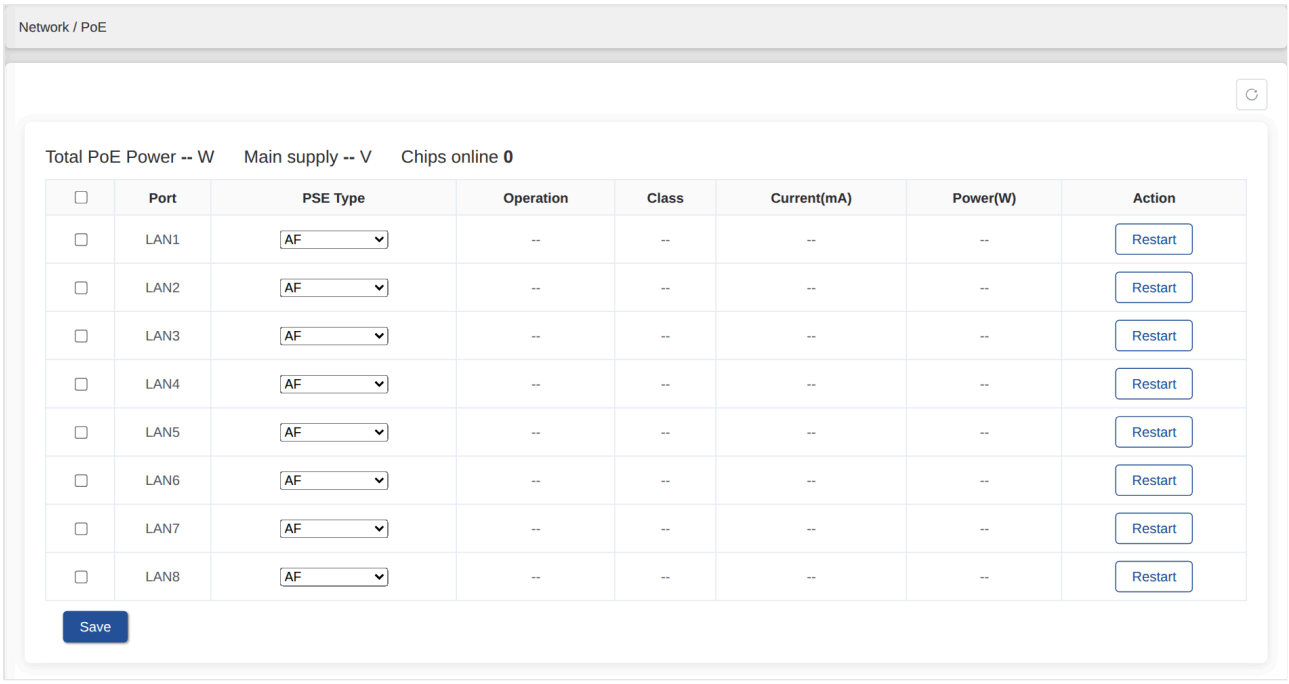


Figure 4-16 PoE output and management

FIELD TASK: CHECK SUPPLY BUDGET BEFORE CONNECTING CAMERAS PER PORT

For this model with specified PSE. Router power and PoE output differ: PSE requires52–55V DC; the supplied12V adapter cannot verify PSE. Follow the model input/polarity diagram.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Supply / Budget	52–55 V DC / actual rated supply capacity	90W/port and720W are design limits subject to supply/cabling/thermal limits
Port / Enable	One test PSE port / On	Verify camera PD standard/power class
Camera IP / Gateway	192.168.10.30 / 192.168.10.1	Camera settings matching LAN

SAVE, TEST AND OBSERVE

1. Check input voltage/budget before connecting. Attach one matching PD camera, enable/save its port and inspect Operation/Class/Current/Power/Total Power.
2. Verify a stable local camera stream before adding cameras one by one. Record steady/peak port loads, total supply budget and temperature; do not assume full rated simultaneous load.

PASS CRITERIA AND DIAGNOSIS

No power: inspect52–55V input, port, PD compatibility and cable. Power works but no stream: inspect IP/stream. Design limits are not a claim of completed load testing.

Finish and restore: Disable test ports before disconnecting, restore port policy and retain actual supply/load results.

> Specification and verification: 90 W design maximum per port and 720 W design total PoE output limit are confirmed product specifications. No loaded-test report is available. They do not establish tested eight-port full-load operation, sustained output or dual-DC changeover; verify the actual supply and loads under this section’ s conditions.

CONFIRM THE POWER ARRANGEMENT

The router accepts **12–55 V DC** for its own operation. **52–55 V DC** input is required for RJ45 PoE power output (PSE). The supplied 12 V adapter powers the router itself and cannot supply PoE output.

The PSE supports **IEEE 802.3af / 802.3at / 802.3bt**, with automatic power negotiation with compatible powered devices. **Design maximum PoE output is 90 W per port and 720 W in total**. Select the supply current rating and load count for actual loads, router consumption and line losses, within both output limits.

CONNECT ONE POE POWERED DEVICE

1. Before attaching the powered device, check supply output and polarity, then connect a 52–55 V DC supply as shown in the power-terminal instructions.
2. Connect the powered device to the intended RJ45 port. In Network → PoE, identify its current port name. If port roles have changed, use the displayed name rather than an old LAN number.
3. Check the port power setting and PSE Type. AF, AT and BT identify the supported standard types; configure them according to the delivered power arrangement. Save, allow PSE/PD negotiation, then inspect Operation, Class, Current and Power.
4. Confirm that the powered device boots, then test its IP and actual service. Use Restart only after identifying the intended port.

> An enabled setting does not prove actual power output. For a power fault, check for 52–55 V DC input, the actual port state and load requirements first. Restart interrupts the powered device's service on that port.

OUTPUT LIMITS AND SUPPLY SIZING

REQUIRED PARAMETER	APPLICATION TO THIS PROJECT
Per-port design output limit	90 W; actual power is negotiated between PSE and PD and must meet startup and running requirements
Total PoE design output limit	720 W across all 8 ports; the sum of port outputs must stay within this limit. Displayed current power is a live reading

REQUIRED PARAMETER	APPLICATION TO THIS PROJECT
Supply voltage/current rating	PSE requires 52–55 V DC; size current from delivered budgets and device/line losses, not bt support
Dual-input and changeover conditions	Verify PoE behavior with the delivered dual-input test; primary/backup DC does not establish uninterrupted PoE
Test conditions and evidence	Retain supply, port/load list, cabling, environment, negotiation and startup/continuous-operation results

90 W and 720 W are PoE design output limits, not router consumption or a guarantee of full output from any supply. Size the supply for all loads and losses, then verify wiring, negotiation and the actual service.

WORKED EXAMPLE: SIX CAMERAS

All figures below are **calculation assumptions**, not supplied cameras or a field-tested PSU recommendation: four fixed-camera ports budgeted at 20 W each and two PTZ ports at 45 W each. These are PSE-side budgets and must already include startup needs and Ethernet-cable losses.

- PoE sum: $4 \times 20 + 2 \times 45 =$ **170 W**. The largest port is 45 W, below 90 W; the sum is below 720 W.
- Assume a further 30 W for router consumption and the DC power path. This is an illustration allowance, to be replaced by measurements.
- At a selected 80% maximum PSU loading, rating $\geqslant (170 + 30) / 0.8 =$ **250 W**. Under these assumptions, 54 V / 5 A (270 W) is a candidate to verify.

See 1.6 for connection, supply limits and acceptance.

CONFIRM DESIGN LIMITS SEPARATELY FROM SUSTAINED POWER

90 W/port and 720 W total are previously confirmed design maxima. **No sustained full-load report is available; they are not verified continuous ratings or a guarantee of eight ports simultaneously at maximum load.** 52–55 V DC is a PSE input prerequisite, not proof that the supply, terminals, wiring and cooling can deliver 720 W.

Before choosing a supply, confirm the complete power path against actual port loads, cable/conversion losses, temperature and derating. The supply current, 4-pin terminal current, conductor selection and sustained dual-DC changeover conditions lack a complete model-specific confirmation; a theoretical division does not establish a hardware rating. The supplied 12 V adapter must not power external PoE loads. Verify each confirmed supply/load combination, then the simultaneous operating combination, recording negotiation, temperature, restart and video continuity.

> **Check the result** The intended port is powering the PD, its service works and actual load meets the delivery power budgets.

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Port / PSE Type	Manage eight RJ45 ports individually; IEEE 802.3af/at/bt with automatic PD negotiation. Set PSE Type for the delivered power arrangement
2	Enable / Operation	Inspect configuration and actual power state separately; an enabled switch does not prove output
3	Class / Current / Power	View detected PD class, current and output power per port
4	Main Supply / Total Power	PoE output requires 52–55 V DC input; assess actual total power against the confirmed per-port and system budgets
5	Restart	Power-cycles the selected port, not the router
6	Standard types	AF, AT and BT are supported standard types. Assess load capability from actual negotiation and the delivery power budgets

TROUBLESHOOTING

SYMPTOM	WHAT TO CHECK
Enabled but the PD does not start	Check 52–55 V DC input, port identity, actual power state and compatibility. The supplied 12 V adapter cannot power PSE output.
One PD works but several do not	Check loads against the 90 W per-port and 720 W total limits, then verify the 52–55 V DC supply capacity, cabling and negotiation.

CHAPTER

05

Applications

Configure serial transport, industrial acquisition, MQTT reporting and services



YZW1000

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
Vendor PLC or multi-protocol instrument	P1: PLC→Monitor→report	Only on a unit with PLC acquisition
Scale/filter existing JSON	E1: Node-RED	Only when delivered

Decide whether the target needs raw frames or decoded point values. Node-RED can process existing data without polling the serial port again.

METHOD	INPUT AND OUTPUT	INTENDED NEED	RESOURCES AND LIMITS
DTU	Raw serial frames ↔ TCP/UDP/MQTT	Your server already parses the device protocol	Owns the selected serial port; does not generate register values automatically
Modbus Collect	RTU/TCP registers → command values → MQTT	Instruments with a defined register map	Serial operation owns that port; writes use command names
PLC Collect	PLC/instrument protocol and point list → sources → reporting	Dedicated protocols or a unified point list	Match device series, addresses and access attributes; its write schema differs from Modbus Collect
Node-RED	Existing messages/node input → processing → output	Unit conversion, field mapping, filtering and integration	This example receives MQTT; serial nodes also require exclusive port ownership

CHECK BEFORE COMBINING FUNCTIONS

1. Validate acquisition with one service before adding MQTT or Node-RED. Do not open Serial1 in two services.
2. Modbus Collect can publish to a broker for Node-RED to subscribe. This shares data over MQTT without Node-RED opening the serial port again.

3. Match downlink to the service: DTU frames, Modbus command writes and PLC source/identifier writes use different formats.

Configuration entries: 5.5 DTU transparent transport • 5.6 PLC and instrument acquisition • 5.8 Modbus acquisition and reporting • 10.4 Case: temperature conversion, filtering and MQTT reporting

THREE EQUIPMENT-BASED EXAMPLES

EXISTING EQUIPMENT	CONFIGURATION PATH	SUCCESS CRITERION
Modbus RTU RS485 meter	Serial1 left A/B → 9600/8/N/1 (example only) → slave 1 → known read-only register → MQTT	Meter, gateway and platform values agree; scale, unit and addressing verified
Ethernet PLC	LAN → verify supported series/protocol → PLC IP/port → known read-only point → reporting rule	Vendor-tool and acquired values agree; source/identifier match platform fields
Server already parses proprietary binary frames	Serial2 right A/B → DTU → TCP/UDP/MQTT server channel	Server receives and parses raw frames; DTU is not expected to decode points

A read-only register example does not authorize control writes. One service owns each serial port; processing existing MQTT in Node-RED does not open that port again.

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.

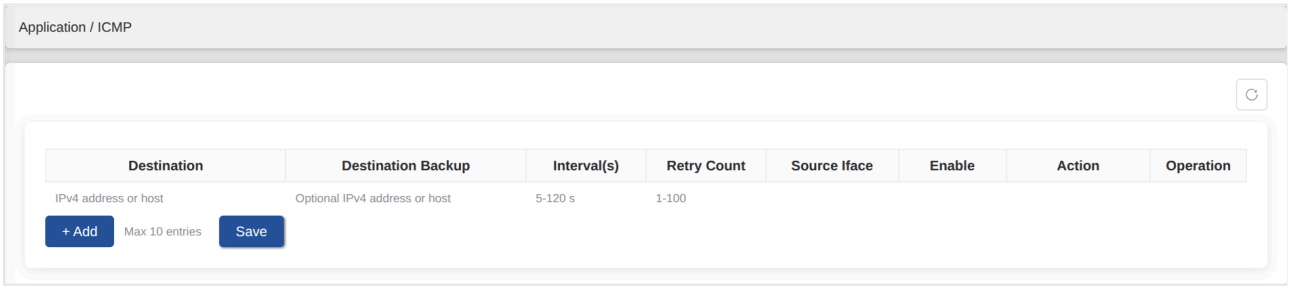


Figure 5-1 ICMP monitoring

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.

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

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
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

5.3 Scheduled tasks

Path Application > Timer

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

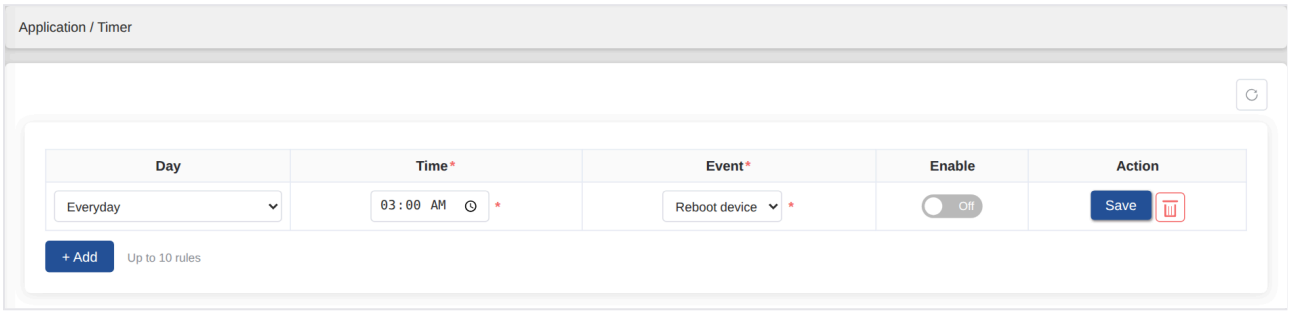


Figure 5-2 Scheduled tasks

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.

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

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

5.4 Network diagnostics

Path Application > Diagnostics

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

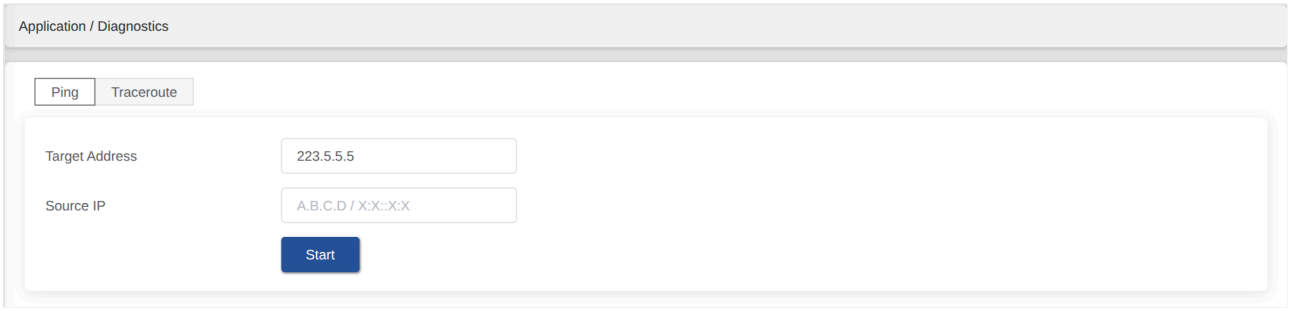


Figure 5-3 Network diagnostics

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.

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

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

5.5 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.

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	YZW1000 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

DTU transfers serial data. For register polling and structured acquisition points, use Modbus Collect or PLC Collect. Server mode does not create inbound reachability by itself; where direct access is unavailable, use the planned m2mCloud or VPN remote-access path.

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.

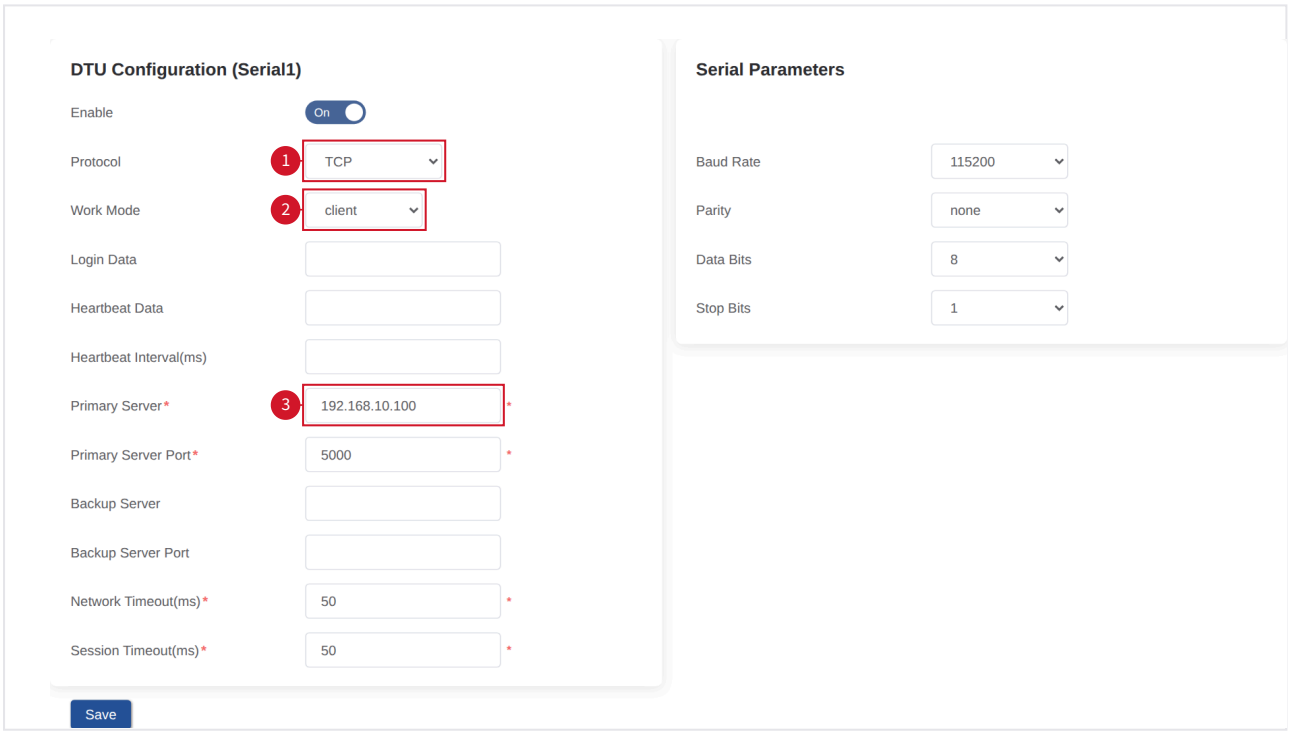


Figure 5-4 DTU client network parameters

1. Choose the transport
2. Select client mode
3. Enter the primary server

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.

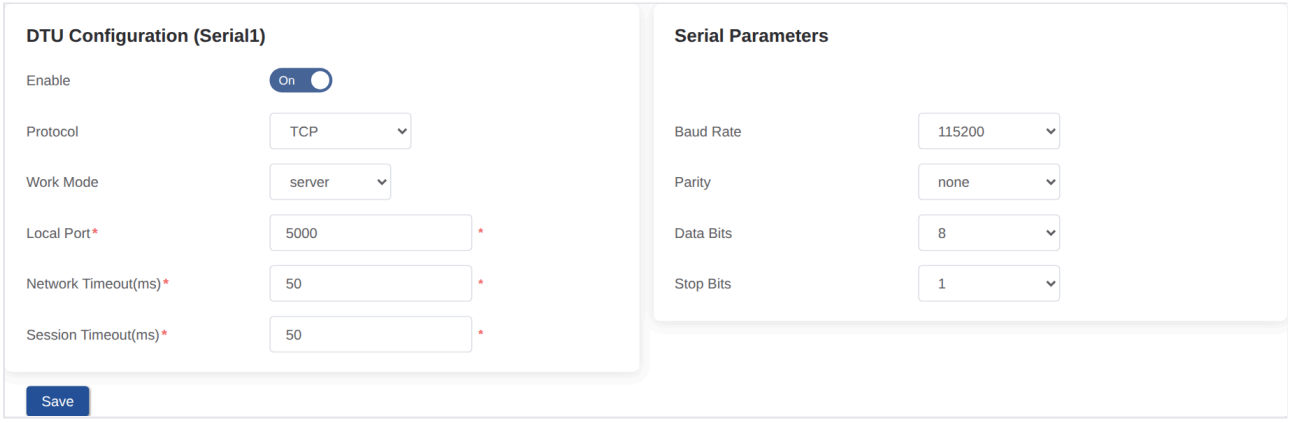


Figure 5-5 DTU server listener parameters

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.

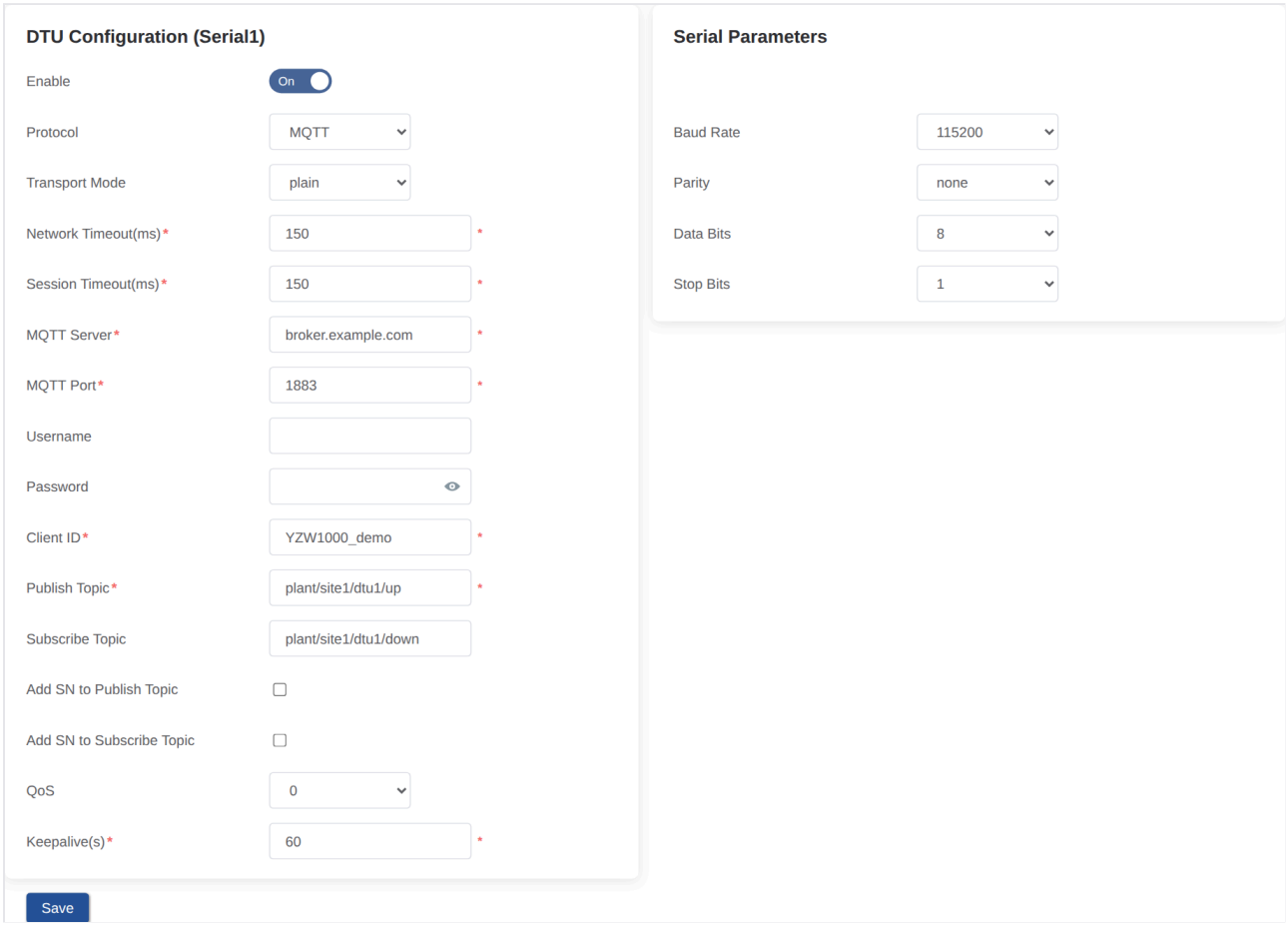


Figure 5-6 DTU MQTT connection and topics

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
5	Network / Session Timeout (ms)	Set the data-wait parameters in milliseconds, distinct from MQTT keepalive in seconds and business reporting intervals

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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.

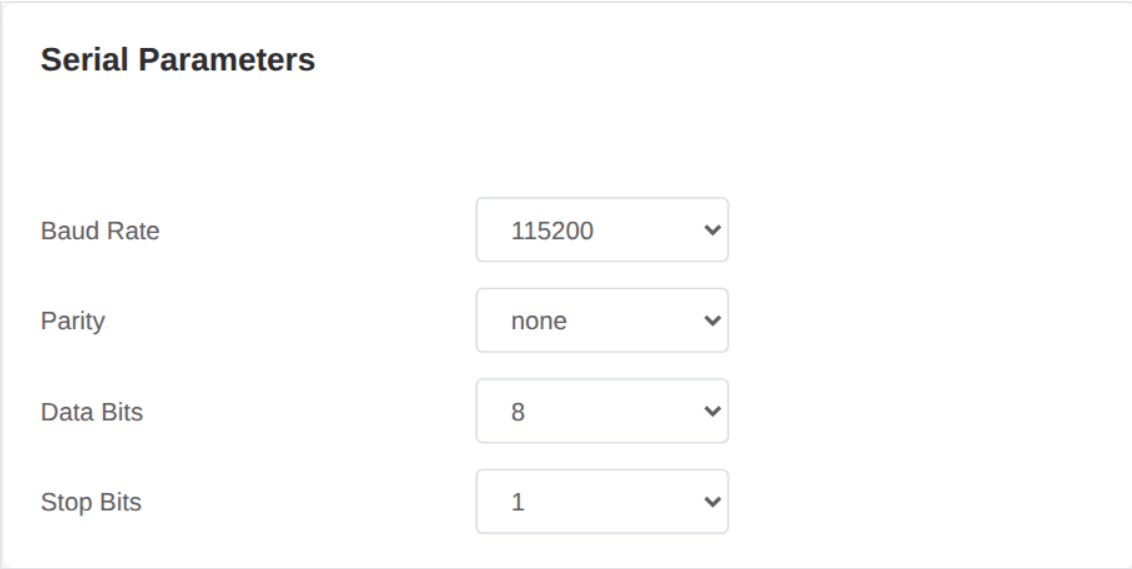


Figure 5-7 DTU serial settings

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 port to one of DTU, acquisition, PLC, Node-RED or remote serial access

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.

5.6 PLC and instrument acquisition

Path Application > PLC Collect

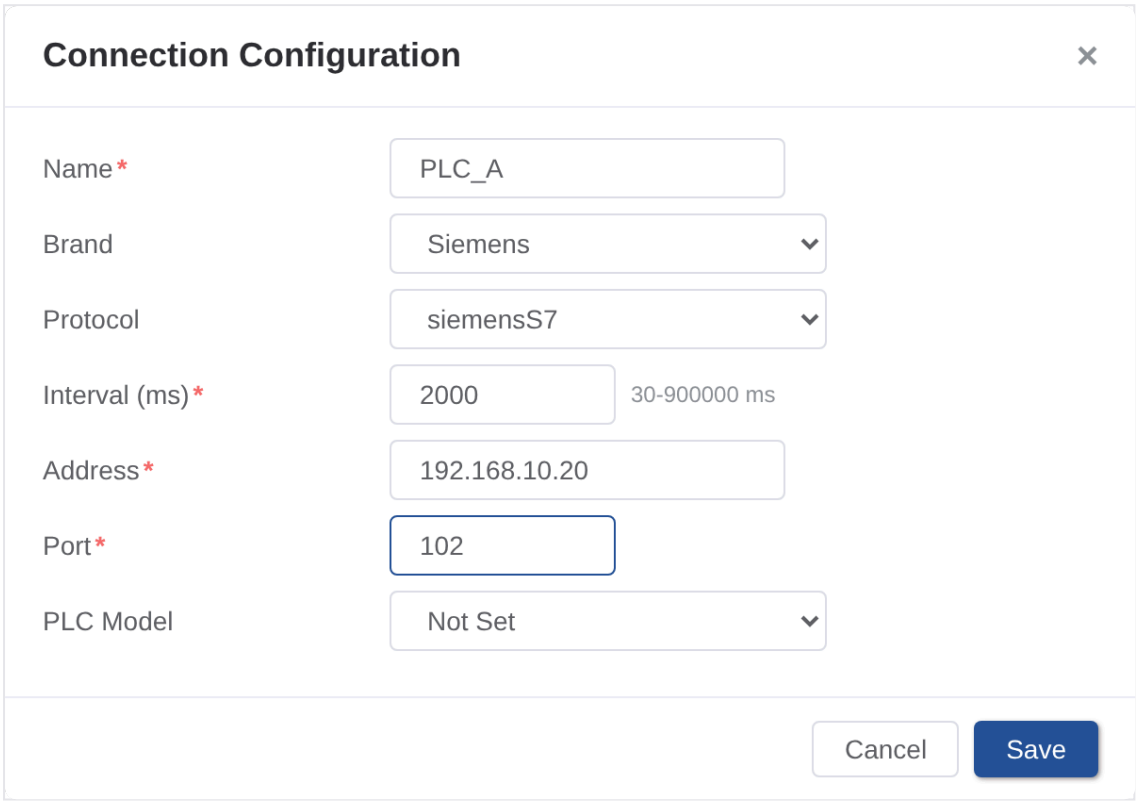


Figure 5-8 Add an acquisition connection

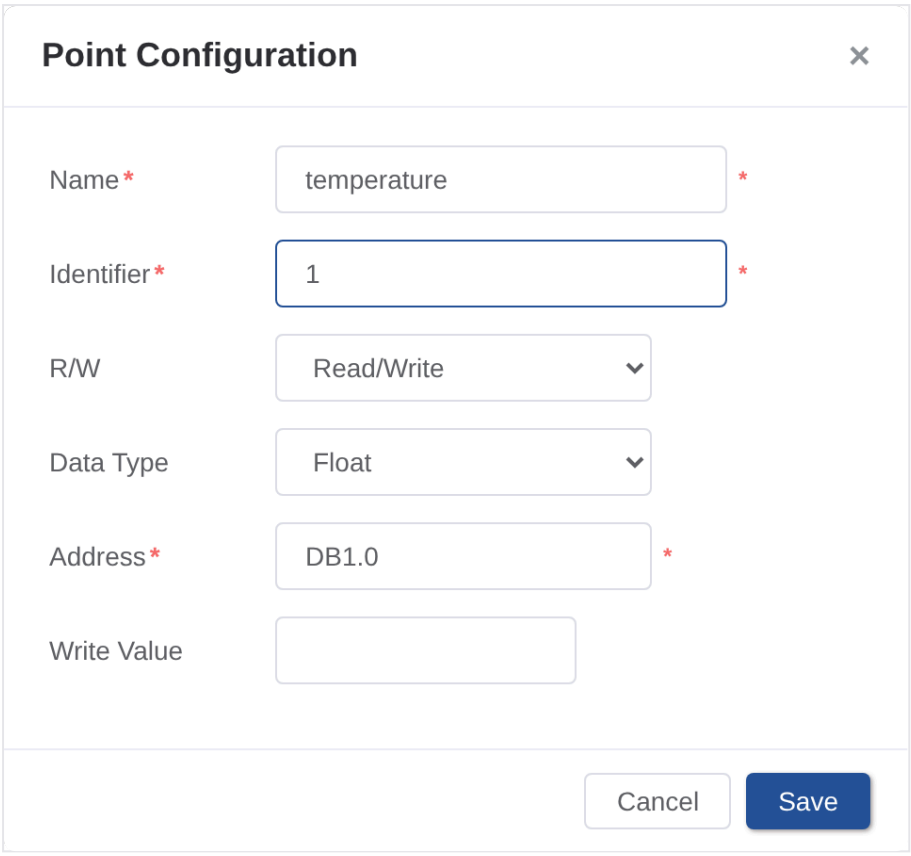


Figure 5-9 Configure acquisition points

FIELD TASK: P1: START WITH ONE READ-ONLY POINT ON A REAL PLC

Obtain a connection/point map already verified in the vendor tool. The example PLC network plan is 192.168.10.20/24, gateway .10.1. Different protocol address syntaxes must not be guessed. Record one known point/current value and map it below.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Name	PLC_A	Source name reused in reporting
Protocol / Connection	Engineer-confirmed exact protocol / Network	Match PLC series/CPU; copy port/rack/slot and other connection settings from its project
IP / Polling Interval	192.168.10.20 / 1000 ms	Use page units; enter1 for seconds
Point Name / Identifier	test_value / 1	Single test point
Address / Data Type	exact project map	Preserve protocol address/type/length, not a Modbus start
Read-write Mode / Periodic Write	Read Only / Off	Read-only first; no control output

SAVE, TEST AND OBSERVE

1. Read the point locally in the vendor tool and record it. Create PLC_A, enter its exact connection and one point, save point/connection and enable.
2. Compare monitored test_value and updates with the vendor tool at the same time. Add MQTT in PLC Data Reporting; add points in batches and return to the last proven batch if errors occur.

PASS CRITERIA AND DIAGNOSIS

Connection fails: inspect exact protocol, PLC access, IP/port and rack/slot. Point fails: inspect syntax/type/length/CPU protection. A list of64 protocols does not make all PLCs interchangeable.

Finish and restore: Disable PLC_A and restore the point map. Label exports with model/protocol/project revision.

CONFIGURATION FLOW

1. Add a connection in PLC Collect and choose the actual PLC/instrument protocol. Do not interchange protocols between different families from one vendor.
2. Enter network or serial settings and check PLC-side access permissions and communications.
3. Add or import the point table: configure name, identifier, address, type and read/write mode for each point.
4. Validate a small set of read-only points first, then add required writable points and periodic writes.
5. Select the data sources, topics and interval in PLC reporting.

> **Check the result** One known point has the expected type, value and updates compared with the vendor tool or field display.

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Name / Protocol	Name identifies the source; choose the actual PLC family or instrument protocol, not merely its vendor
2	Connection / Polling Interval	Choose network or serial transport, then its connection and polling settings
3	Point Name / Identifier	Names aid reading; identifiers support message addressing and must be unambiguous within a source
4	Address	Use the selected protocol address syntax, not register names copied from another PLC
5	Data Type / Read-write Mode	Match type and size to the field project; enable writes only for intended control points

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
6	Periodic Write	Configure periodic writes per point; this differs from one cloud downlink command
7	Import / Export / Monitor	Use CSV for point-table maintenance and monitoring to inspect active connections and values

TROUBLESHOOTING

SYMPTOM	WHAT TO CHECK
Connection established but point values are wrong	Compare protocol, address, type and byte order with the vendor tool. Validate one known read-only point before extending the point list.

5.7 PLC data reporting

Path Application > PLC Collect > Data Report

PLC reporting publishes points from configured acquisition sources to MQTT. Validate acquisition before selecting sources, topics and reporting intervals.

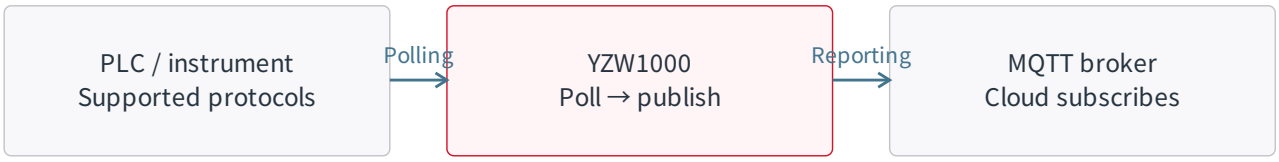


Figure 5-10 PLC/instrument reporting path using supported protocols

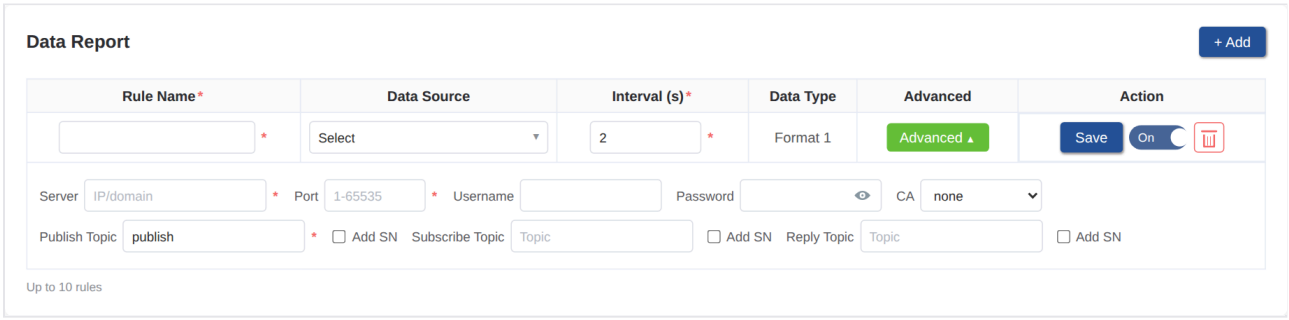


Figure 5-11 Configure sources and reporting

FIELD TASK: P1: REPORT ONE PROVEN PLC_A POINT THROUGH MQTT

First prove PLC_A test_value updates in Monitor. Run bench at .10.10. P1 uses separate topics from M1/M2.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Rule Name / Data Source	P1 / PLC_A	Select only that source
Server / Port / Credentials	192.168.10.10 / 1884 / field + DemoOnly2026	Isolated lab broker
Publish / Subscribe / Reply Topic	plant/site1/plcA/data / plant/site1/plcA/set / plant/site1/plcA/reply	Configure all three exactly
Report Interval / SN Suffix	5 s / Off	Disable suffix initially to avoid topic mismatch
Format	Format 1 if available	Inspect the raw payload in the selected format

SAVE, TEST AND OBSERVE

1. Save/enable rule and run python site_lab.py watch --topic plant/site1/plcA/data --seconds 30.
2. Find PLC_A, identifier1 or its mapped point name in the payload and compare with Monitor. For unchanged values inspect sampling time and whether the source is actually static.

PASS CRITERIA AND DIAGNOSIS

Connected without data: inspect rule/source/point state. Unexpected topic: inspect SN suffix. P1 write format differs from Modbus flat numeric JSON; see the next section.

Finish and restore: Disable P1, stop the lab service and restore production platform settings.

> **Check the result** The effective publish topic receives updates with identifiers and values matching local acquisition.

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Rule Name / Data Source	Name the rule and select one or more configured acquisition sources
2	Server / Port / Credentials	Configure the broker and credentials and select a CA certificate where required
3	Report Interval	Controls publication cadence, separately from connection polling
4	Publish / Subscribe / Reply Topic	Separate data publication, receiving cloud writes and reporting write results

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
5	SN Suffix	Configured per topic; when enabled, use the effective topic with the actual SN appended
6	Format 1	Data contains deviceId, deviceName, params and status; point values are strings and reporting status is not a write reply

TROUBLESHOOTING

SYMPTOM	WHAT TO CHECK
Broker online but expected points are missing	Check local acquisition, selected sources, the effective publication topic and SN suffix. Check acquisition and report intervals separately.

5.8 Modbus acquisition and reporting

Path Application > Modbus Collect

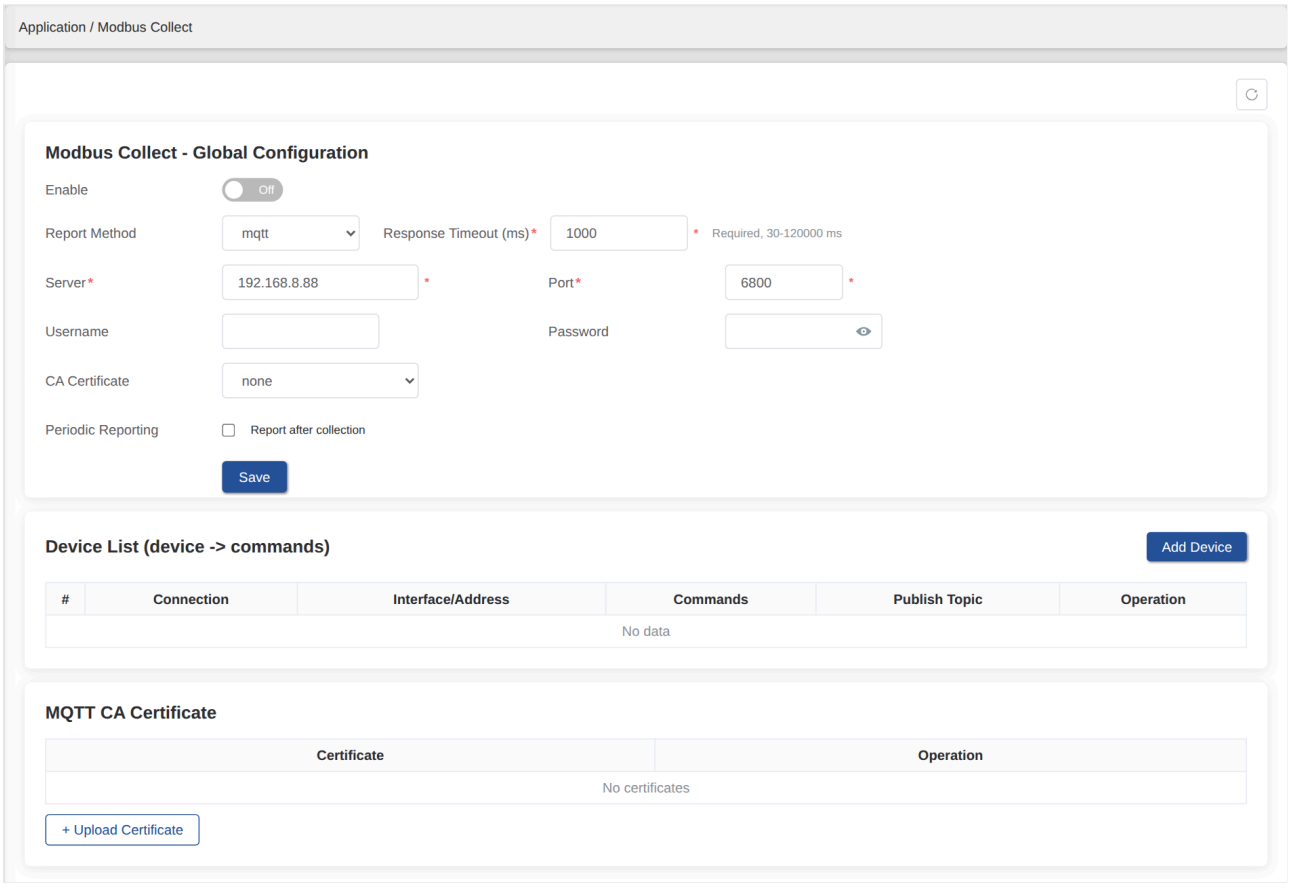


Figure 5-12 Modbus acquisition and reporting

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.

Independent example R1 (read only): R1 is a separate RS485 reference in this section, not the M1 TCP connection. Use slave 1, Serial1, temperature, FC03, PDU start 0, Unsigned 16bit, count 1, a 5 s period and Writable disabled. Screenshot form values are separate illustrations; follow the example table. R1 does not share its control point with the write example in 5.11.

CHOOSE ACQUISITION BEFORE CONNECTING THE CLOUD

Modbus Collect polls Modbus RTU / TCP instruments by device and command. Use PLC Collect for PLC-specific protocols or a unified multi-source point list. The devices, commands and MQTT write format in this section belong to **Modbus Collect**.

EXAMPLE: REPORT ONE RS485 INSTRUMENT TO MQTT

This is a teaching configuration. Replace the slave address, serial settings and register definitions with the instrument documentation. Other addresses and topics in screenshots are separate input examples.

ITEM	EXAMPLE PLAN
Wiring and port	Instrument on the external left A / B pair; select Serial1
Serial / slave	Example only: 9600 bit/s, 8 data bits, no parity, 1 stop bit; slave address 1
First point	Command name temperature; example: FC03, PDU start 0, Unsigned 16bit, quantity 1, period 5 s, Writable No. Replace these with the instrument register map
MQTT server	Configured broker, port and credentials; configure the required CA when using TLS
Publish / subscribe topics	plant/site1/rtu1/data / plant/site1/rtu1/set

1. Follow “Device connections” and “Acquisition commands” to create one device and one read-only point. Confirm local readback before investigating cloud formatting.
2. Enable acquisition globally, select mqtt as Report Method, and enter the broker and authentication settings.
3. Choose report-after-acquisition or periodic reporting. The command polling period controls reads; the reporting period controls sends. Configure them separately.
4. Subscribe at the cloud to the device's actual publish topic. Observe several reports and check command names, values and updates.
5. If remote control is required, configure a confirmed writable command, then follow “Modbus MQTT cloud writes” and verify readback after writing.

In periodic reporting, a point's first collected value is sent immediately; subsequent reports send newly collected values on the reporting period. Old history is not replayed. An MQTT connection does not prove successful instrument acquisition.

CHECK R1 TOPICS AND PAYLOAD

R1 and the pictured device form use `plant/site1/rtu1/data` for publishing and `plant/site1/rtu1/set` for subscription. These are user-defined example channel names, not protocol selectors. PLC Data Report example P1 retains its separate `plcA` topics.

Subscribe to the actual R1 publishing topic, save one raw message, then check the location, type, count and unit of `temperature`. An MQTT connection does not establish a successful instrument read. Single-value and multi-value commands can yield a number and an array respectively.

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

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	Slave response wait in ms, distinct from polling and reporting intervals
3	Server / Port / CA	Reporting destination and MQTT CA, not the slave connection address
4	Immediate / Periodic	Immediate reports follow collection; periodic mode sends the first value immediately, then fresh samples periodically
5	Device Connection	Up to 16 connections; TCP specifies slave IP/port and RTU specifies the serial port and settings
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

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.

5.9 Modbus device connection

Path Application > Modbus Collect > Add Device

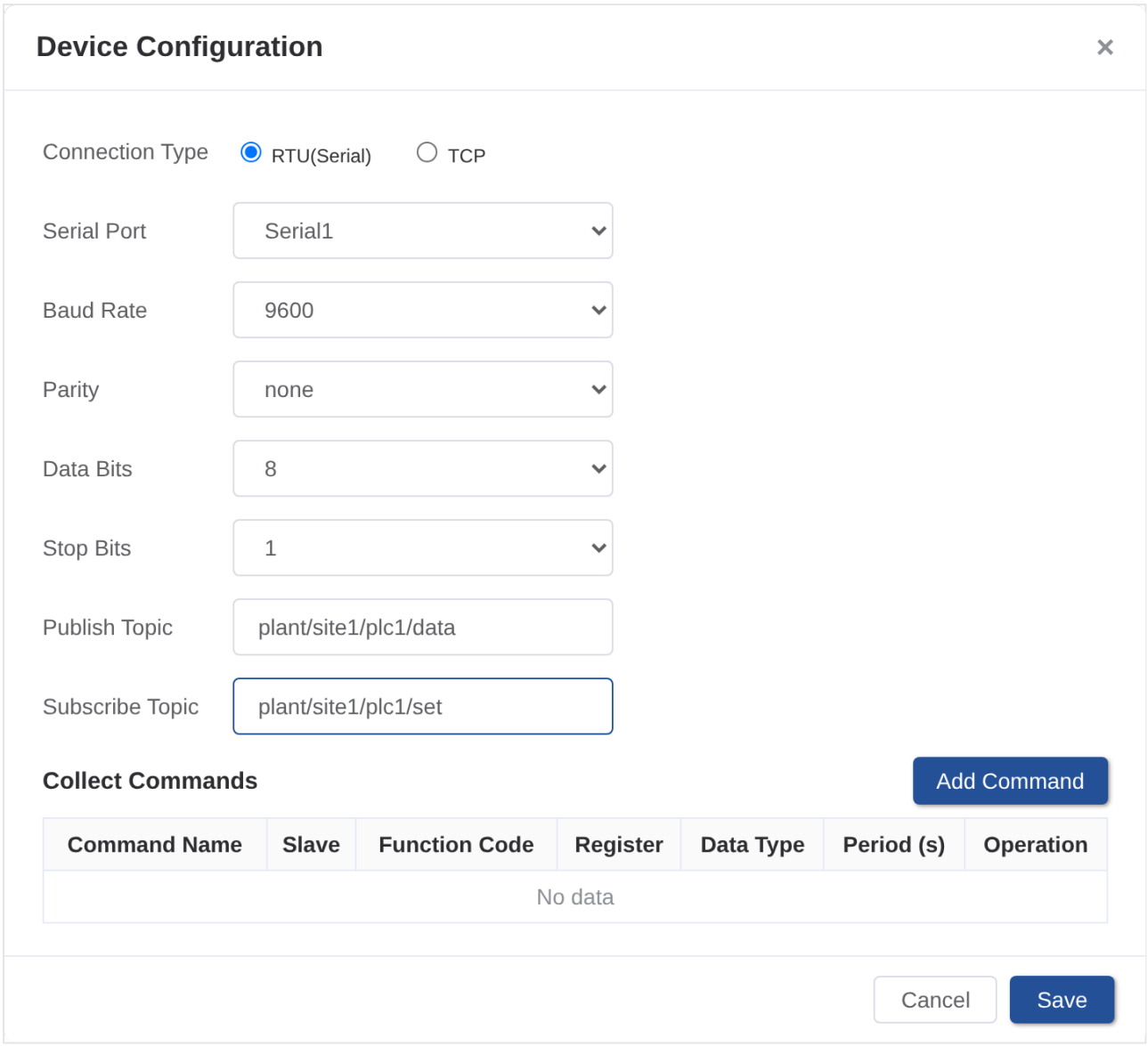


Figure 5-13 Modbus slave connection

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

UI FIELD	ENTRY	BASIS
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.

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

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

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

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.

5.10 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.

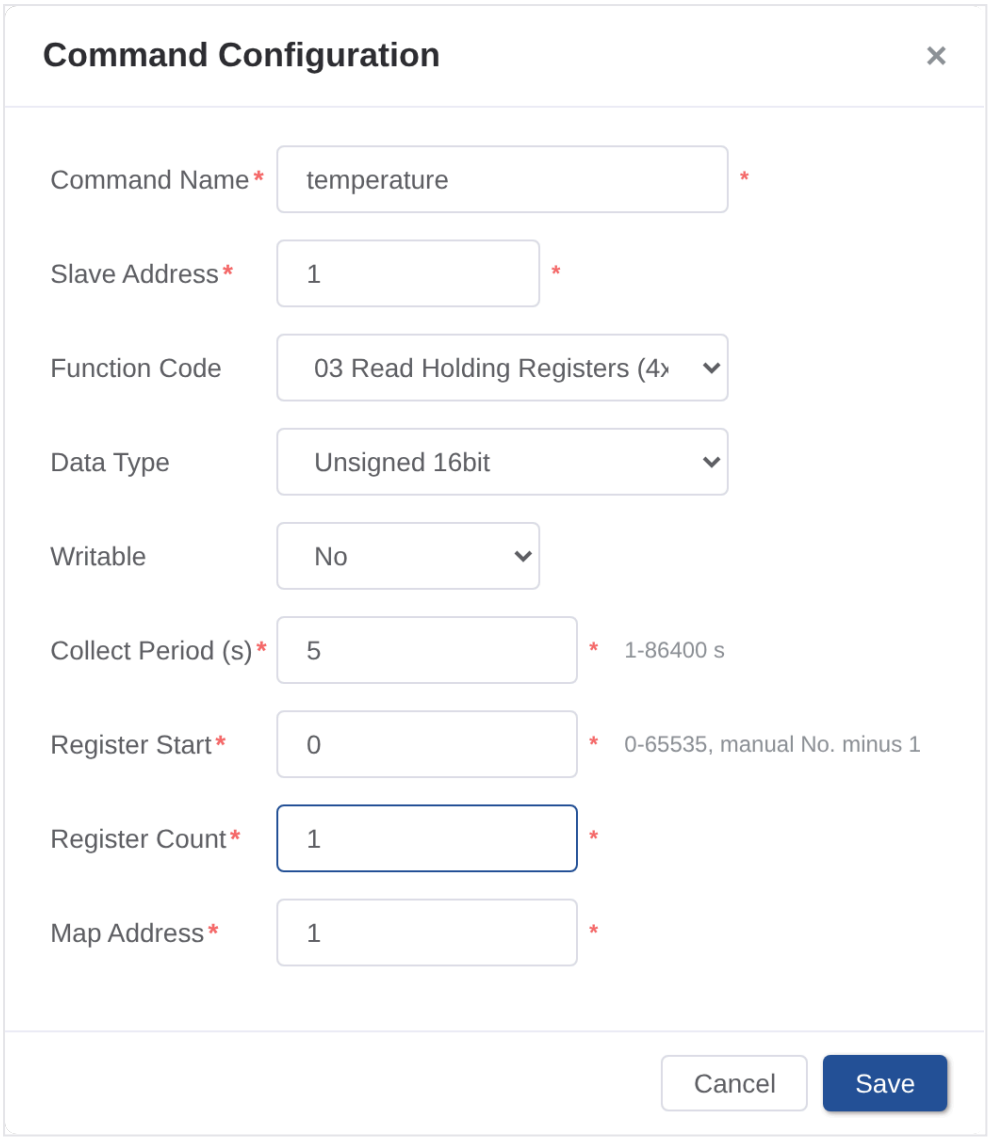


Figure 5-14 Read-only acquisition command example

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

UI FIELD	ENTRY	BASIS
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.

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

IDENTITY AND ADDRESSING

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

DATA INTERPRETATION AND ACQUISITION

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
4	Data Type	Select an exposed integer/float type and match slave byte order
5	Writable	Enable only for intended control commands; areas 02/04 remain non-writable
6	Collect Period	Per-command polling period in seconds, not MQTT publication 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

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.

5.11 Modbus cloud writes over MQTT

Path Application > Modbus Collect

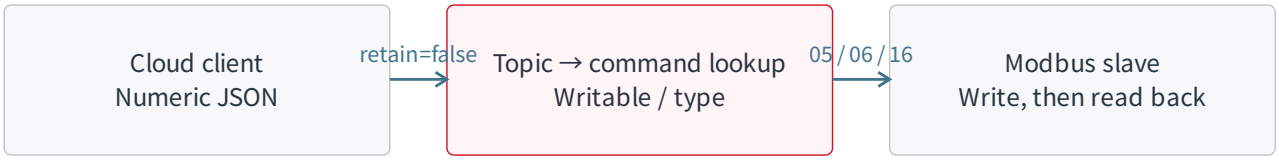


Figure 5-15 Modbus cloud writes over MQTT

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. Publish one test value to this device's effective subscribe topic. Do not send this format to a PLC reporting rule.
3. Inspect subsequent collected values and logs. Resume normal control after expected readback.
4. 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.

DO NOT MIX THIS WITH PLC REPORTING WRITES

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
PLC Collect reporting rule	source + identifier selects a source/point included by the rule	String, such as "25.5"	Optional reply topic; write_applied still requires field readback

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

STEP	ACTION / EXPECTED OBSERVATION
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.

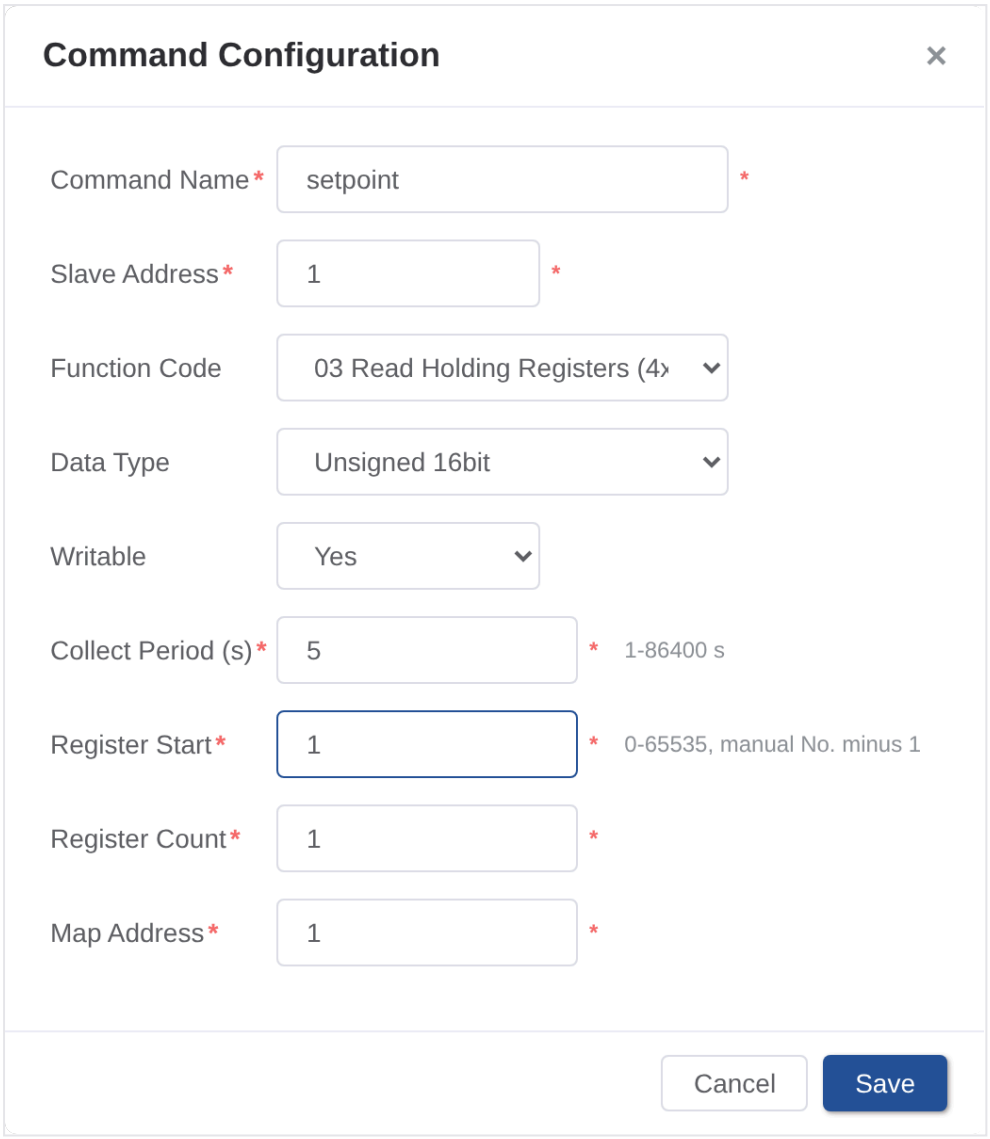


Figure 5-16 Independent M2: setpoint, start 1, Unsigned 16bit, writable

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.

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

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

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.

5.12 PLC cloud writes over MQTT

Path Application > PLC Collect > Data Report

FIELD TASK: P1 WRITE: INSPECT THE REPLY, THEN INDEPENDENTLY READ BACK

P1 reporting must work. Use an authorized test point with known range/type/original value. PLC_A identifier1 must refer to that writable test point; do not rename a production control point merely to match the example.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Data Source / Identifier	PLC_A / 1	Must be selected in ruleP1
Read-write Mode	target writable	Disable unneeded periodic writes
Write Payload	{"source":"PLC_A","identifier":"1","value":"25.5"}	value is a string; use25.5 only for a compatible type/range

SAVE, TEST AND OBSERVE

1. Subscribe to plant/site1/plcA/reply and plant/site1/plcA/data and record the old value. Send the table JSON to plant/site1/plcA/set using a MQTT client with retain=false.
2. Check reply source/identifier/status/reason. write_applied indicates protocol success only. Independently compare Monitor, subsequent acquisition and vendor-tool/physical state.

PASS CRITERIA AND DIAGNOSIS

On timeout/missing reply read back before retrying; do not duplicate control blindly. Use reason to inspect source/identifier/permission/type. P1 must not use the M2 flat numeric format.

Finish and restore: Restore/read back the authorized original value, then disable test write permission/rules.

Independent example P1 (PLC Data Report): PLC_A / identifier 1 is unrelated to M1/M2. Example uplink, downlink and reply topics are plant/site1/plcA/data, plant/site1/plcA/set and plant/site1/plcA/reply. Replace them with your rule topics before sending a string value.

A PLC reporting rule receives writes on its effective subscribe topic and returns results on its reply topic. Its format differs from independent Modbus Collect numeric objects.

```
{"source":"PLC_A","identifier":"1","value":"25.5"}
```

FIELD	MEANING
source / data_source	A source selected by this reporting rule, for unambiguous addressing
identifier / name / addr	Match a configured point identifier, name or address; prefer source + identifier
value	String-form write value matching the point type and write permission

Send one UTF-8 JSON object of 1–4096 bytes. Without source, the first match in rule source order is used; this is not a broadcast to all sources.

With a reply topic configured, a success example is:

```
{"status":"success","reason":"write_applied","data":{"source":"PLC_A","identifier":"1","value":"25.5"}}
```

write_applied means protocol-write success, not field-state readback. Use retain=false. A timeout or absent reply does not prove no write occurred; read back before deciding to retry.

CHECK THE WRITE AND ITS FEEDBACK

1. Confirm the reporting rule includes the target source and that the point is writable and already reads correctly.
2. Subscribe to the configured reply topic first, then send one request to the rule's effective subscribe topic, using existing source and identifier values.
3. Check source, identifier, status and reason in the reply against the intended point.

4. Check subsequent acquisition or field state separately; protocol success and the intended physical state require separate confirmation.

END-TO-END EXAMPLE: ADDRESS SOURCE AND IDENTIFIER

Assume the rule includes source PLC_A, writable numeric point identifier 1, currently reading 20.0. Downlink is plant/site1/plcA/set and reply is plant/site1/plcA/reply. Replace these example names, values and topics with configured ones.

1. Subscribe to the reply and current rule's uplink topics; record the original value and permissions.
2. Publish `{"source":"PLC_A","identifier":"1","value":"25.5"}` on the downlink, retain=false. Here value is a string.
3. Match source/identifier in the reply. status=success and reason=write_applied mean the protocol write returned successfully.
4. Verify a later acquisition of the same point reads 25.5 and compare with the field tool/state. Protocol success and physical result are separate checks.
5. On failure, timeout or silence, keep request/topic/time and read back before retrying. Silence does not prove the write did not occur.

Chain: request → selected source/point → protocol write → reply topic → later acquisition/field check. Do not invent request_id or physical-state feedback in the reply. Queue/match concurrent requests at the platform if needed. **Status:** implementation example from the code contract; no field PLC write was performed.

> **Check the result** The reply identifies the intended point and subsequent acquisition or field feedback confirms the expected state.

TROUBLESHOOTING

SYMPTOM	WHAT TO CHECK
write_applied received but the state is unexpected	This indicates protocol write success only. Read the target point and check PLC logic, interlocks and field state.

5.13 Node-RED runtime management

Path Application > NODE-RED

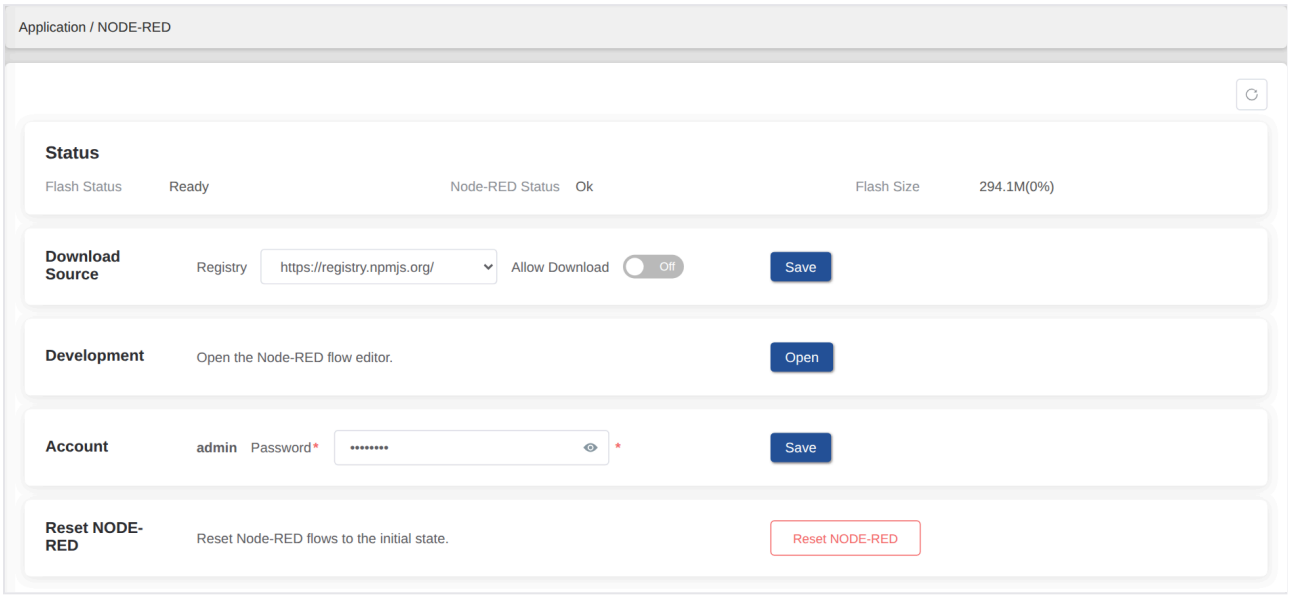


Figure 5-17 Node-RED runtime management

FIELD TASK: OPEN THE EDITOR BEFORE IMPORTING A REPRODUCIBLE FLOW

Use only when Node-RED is delivered. Complete external-PC M1 and export existing configuration/flows. Optional models need confirmed entitlement/storage/install state.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Status / Development	Start runtime / enable development entry if needed	Inspect running state before opening editor
Account / Password	change delivered credentials	Separate from Web admin
Broker in supplied flow	192.168.10.10:1884	Enter lab credentials in the flow broker configuration

SAVE, TEST AND OBSERVE

1. Start the runtime and open the provided editor URL. Sign in with delivered credentials and export current flows before importing field_temperature.json.
2. Enter field/DemoOnly2026 in the MQTT config node, check topics, deploy and inspect connection status plus Debug, not only runtime state.

PASS CRITERIA AND DIAGNOSIS

Editor unavailable: inspect runtime, port, permissions and development entry. Missing nodes: inspect delivered components before resetting flows.

Finish and restore: Remove/stop lab flows and restore the export; close development access according to project policy.

PROCEDURE

1. Check Node-RED runtime status and open the flow editor using the link provided on the management page.
2. Start with a simple read-only acquisition or MQTT reporting flow and inspect node settings and debug output.
3. Before using a Modbus serial port, release any other PLC, DTU, collector or remote-serial instance using it.
4. Check the wiring, triggers and destinations, then deploy. Validate persistence and restart behavior during a maintenance window.

Verify: the flow is healthy and produces expected data. For control nodes, check the actual target and resulting field state.

Check the result The editor opens and the required nodes and runtime environment are available.

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Status	Inspect storage and runtime state; an accessible editor does not mean a business flow is deployed
2	Download Source / Registry	Select the delivered download source; availability depends on network access and installed runtime
3	Development / Open	Opens the flow editor; its account settings are separate from router admin password changes
4	Account / Password	Maintains editor access credentials; it does not imply router multi-user management
5	Reset NODE-RED	Export flows before resetting and check the scope described on the page
6	Serial Ownership	Serial nodes exclusively own their physical port; coordinate with collection and transparent transport

5.14 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.

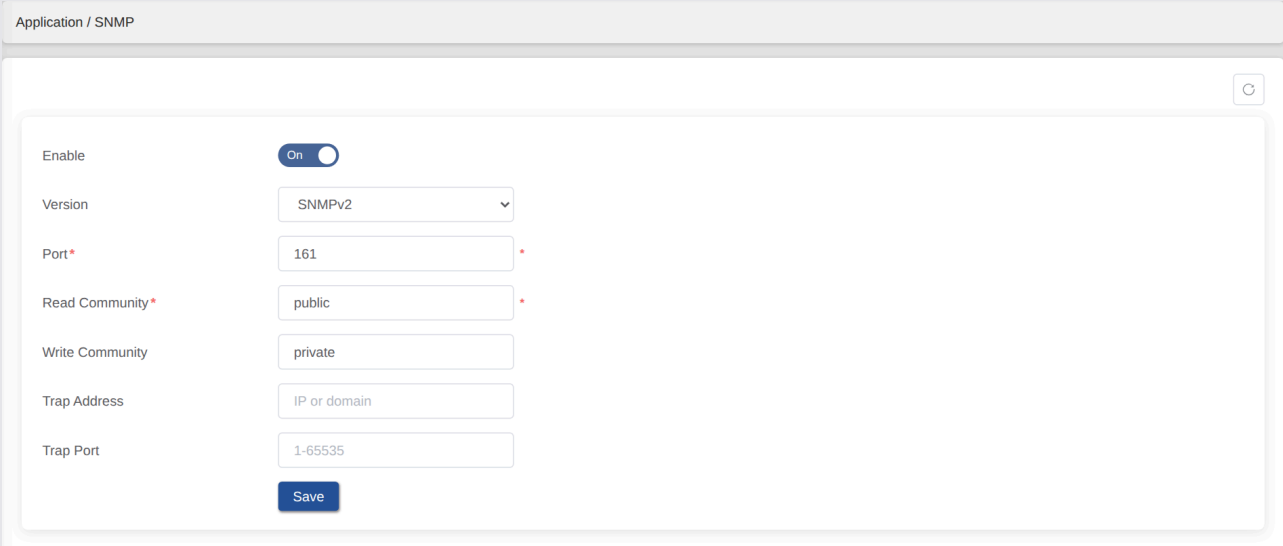


Figure 5-18 SNMP

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.

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Version / Port	Select SNMPv2 or SNMPv3 and match the manager version and port
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

5.15 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.

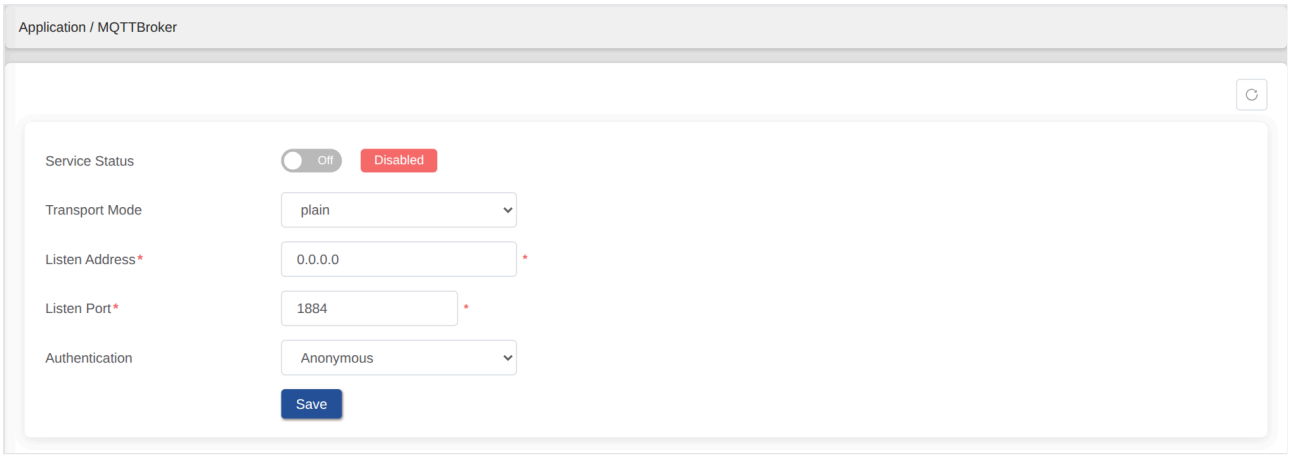
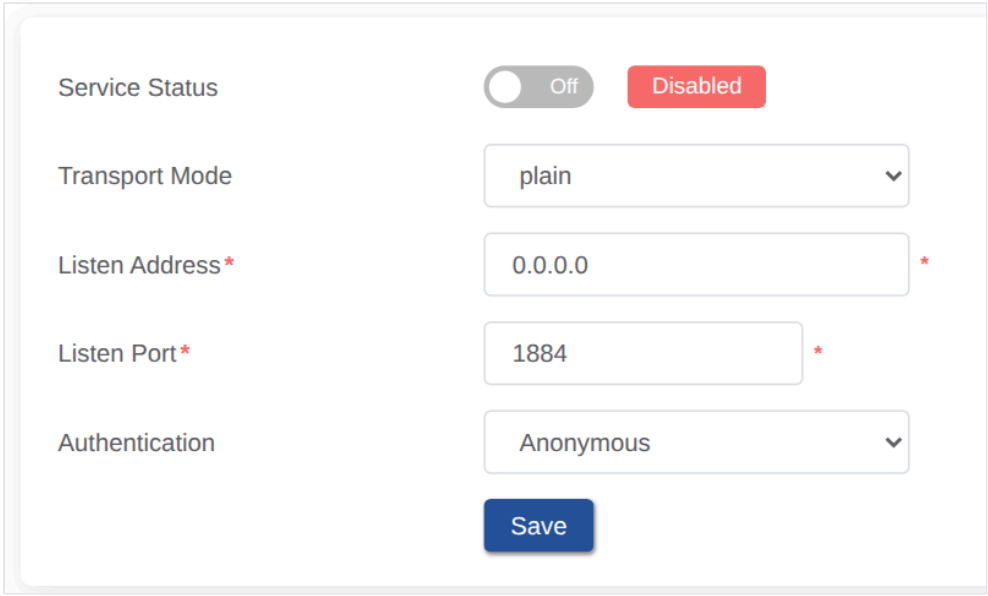


Figure 5-19 Local MQTT Broker

Native interface detail (complete panel above)



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.

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

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
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

5.16 Optional GPS

Path Application > GPS

With GPS fitted, attach its antenna, obtain a valid fix and then configure TCP/UDP reporting. A page or reserved connector alone does not establish positioning capability.

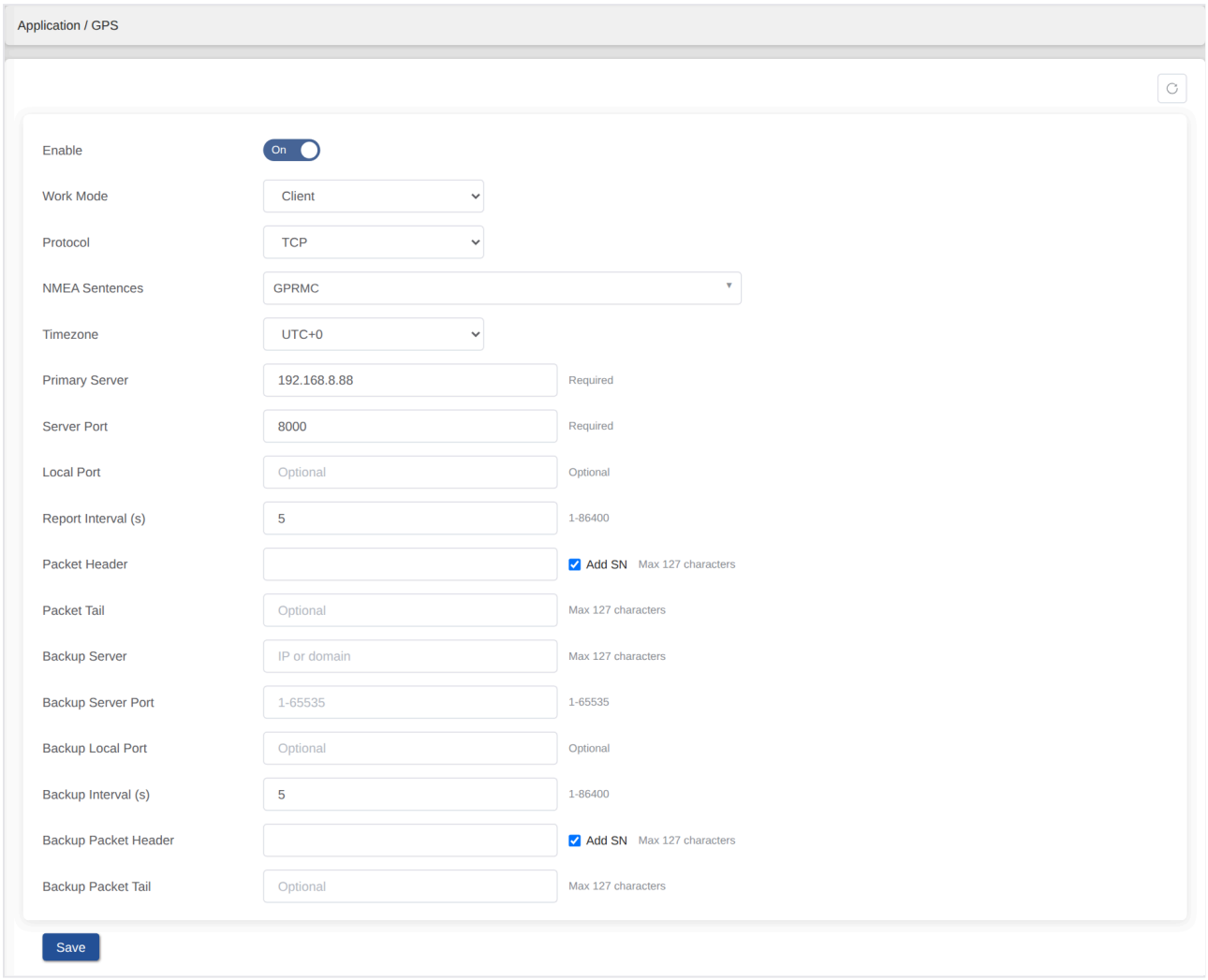


Figure 5-20 Optional GPS

FIELD TASK: CONFIRM FITTED POSITIONING HARDWARE BEFORE TESTING OUTDOORS

GPS is an ordered option. Check order, antenna and interface. Test with suitable outdoor protection and clear sky; a menu alone does not prove fitted hardware.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Work Mode / Protocol	delivered mode	Verify local fix before network forwarding
Destination / Port	project receiver	Only for required forwarding

SAVE, TEST AND OBSERVE

1. Attach the specified antenna, enable and inspect Fix/Satellites/position/time. Allow initial acquisition; indoor no-fix does not prove failed hardware.
2. After a valid fix configure forwarding and compare the receiver’ s timestamp/position in NMEA or the delivered protocol.

PASS CRITERIA AND DIAGNOSIS

No satellites: inspect antenna/sky/fitted option. Fix without reports: inspect receiver listener/port/network separately.

Finish and restore: Restore positioning/forwarding settings and close the test receiver.

> **Check the result** The optional hardware obtains a valid fix and, when reporting is required, the receiver obtains its data.

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Hardware Option	Valid positioning requires the optional GPS hardware and antenna; a menu or reserved connector does not prove fitment
2	Work Mode / Protocol	Select an exposed Client, Server or Traccar mode for the target platform and match TCP/UDP transport
3	NMEA Sentences / Time Zone	Select required positioning sentences and display time zone; the receiver must parse those sentences
4	Position / Fix / Satellites	Use coordinates together with fix status, not values shown before a valid fix
5	TCP / UDP Destination	Set destination address and port to match the positioning-data receiver
6	Interval / Header / Tail / Identifier	Set reporting cadence and framing for the receiver; framing text is not positioning data
7	Backup Target	Review backup destination, port, interval and its framing fields
8	Reporting	Verify local positioning and remote data receipt separately

5.17 Alarm notifications

Path Application > Alarm Control

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

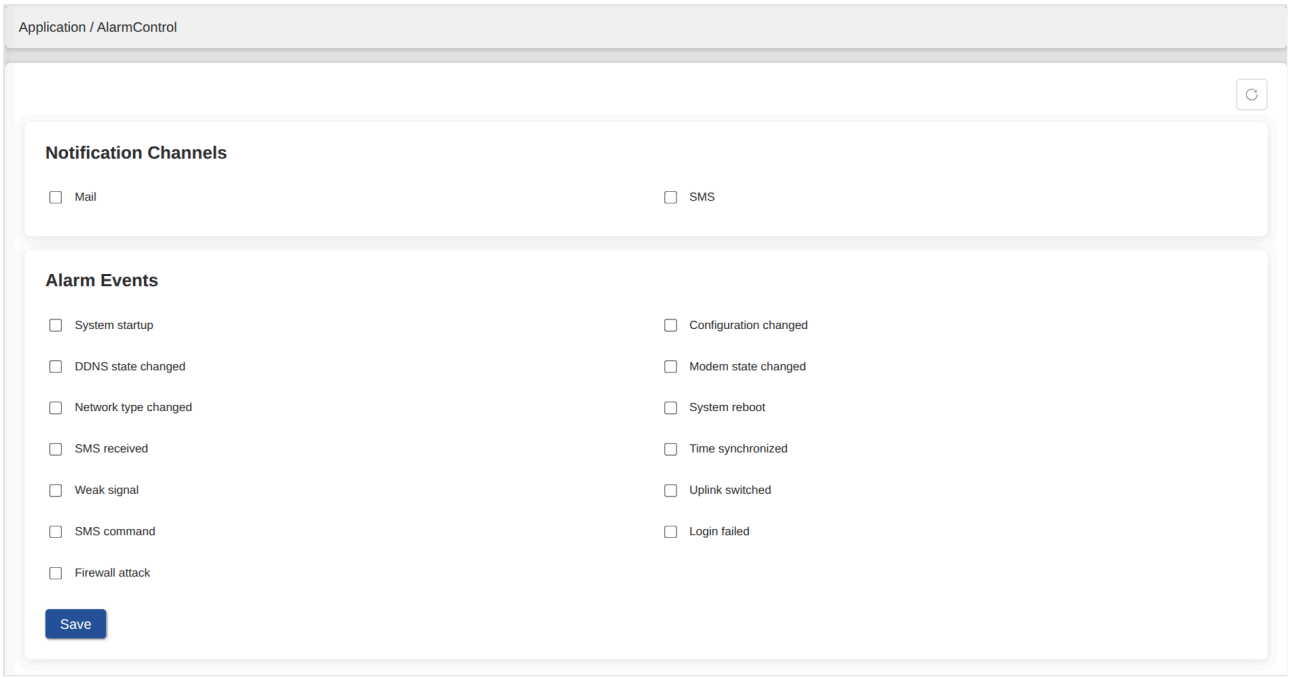


Figure 5-21 Alarm notifications

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.

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

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

5.18 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.

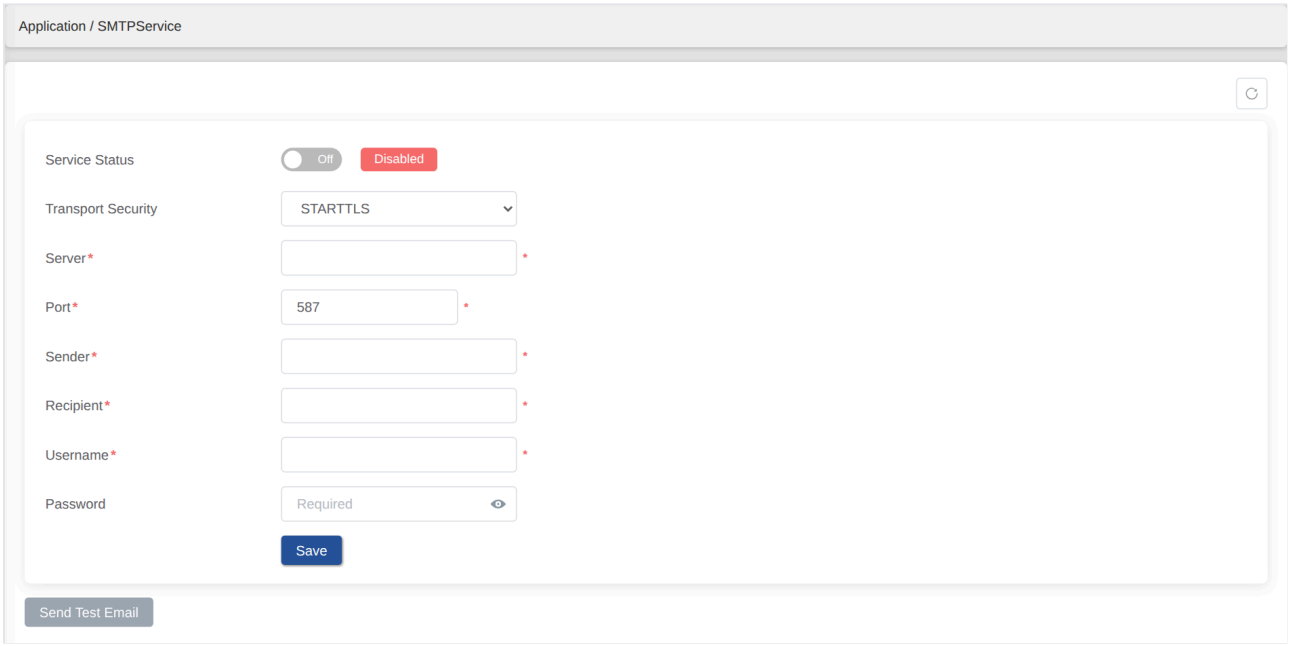


Figure 5-22 SMTP mail service

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.

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

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

CHAPTER

06

VPN

Establish tunnels and verify authentication, routing and service reachability



YZW1000

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 • 11.1 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.

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
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.

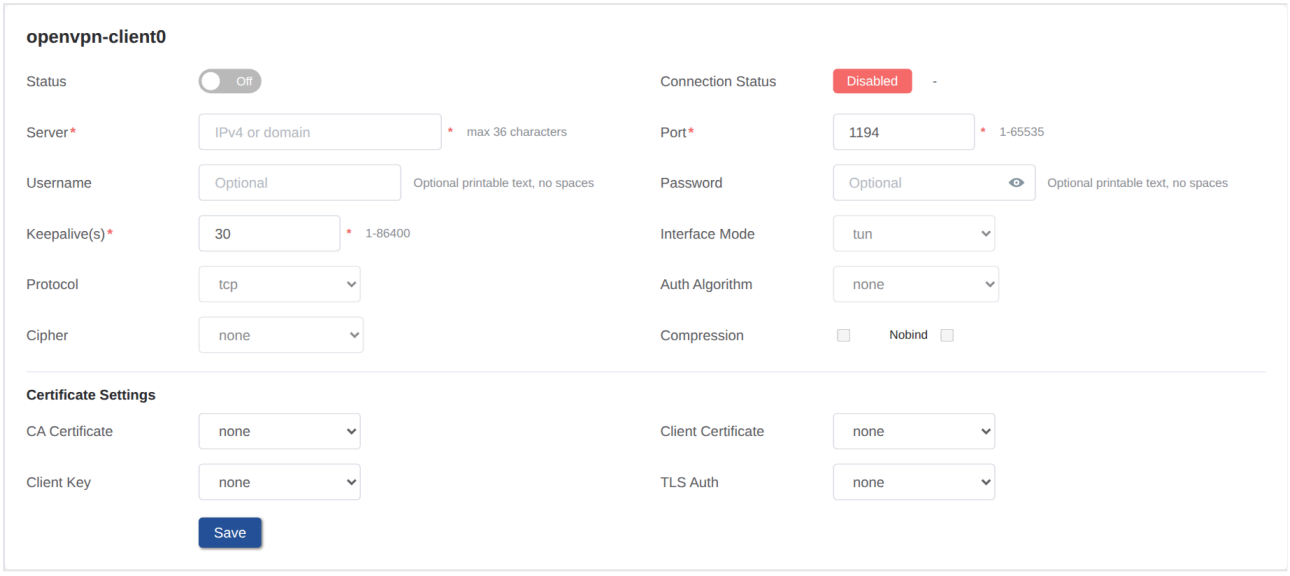


Figure 6-1 OpenVPN client connection settings

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.

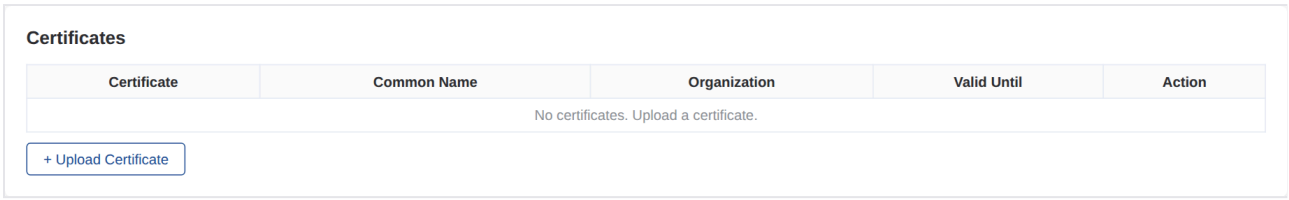


Figure 6-2 OpenVPN certificate files

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.

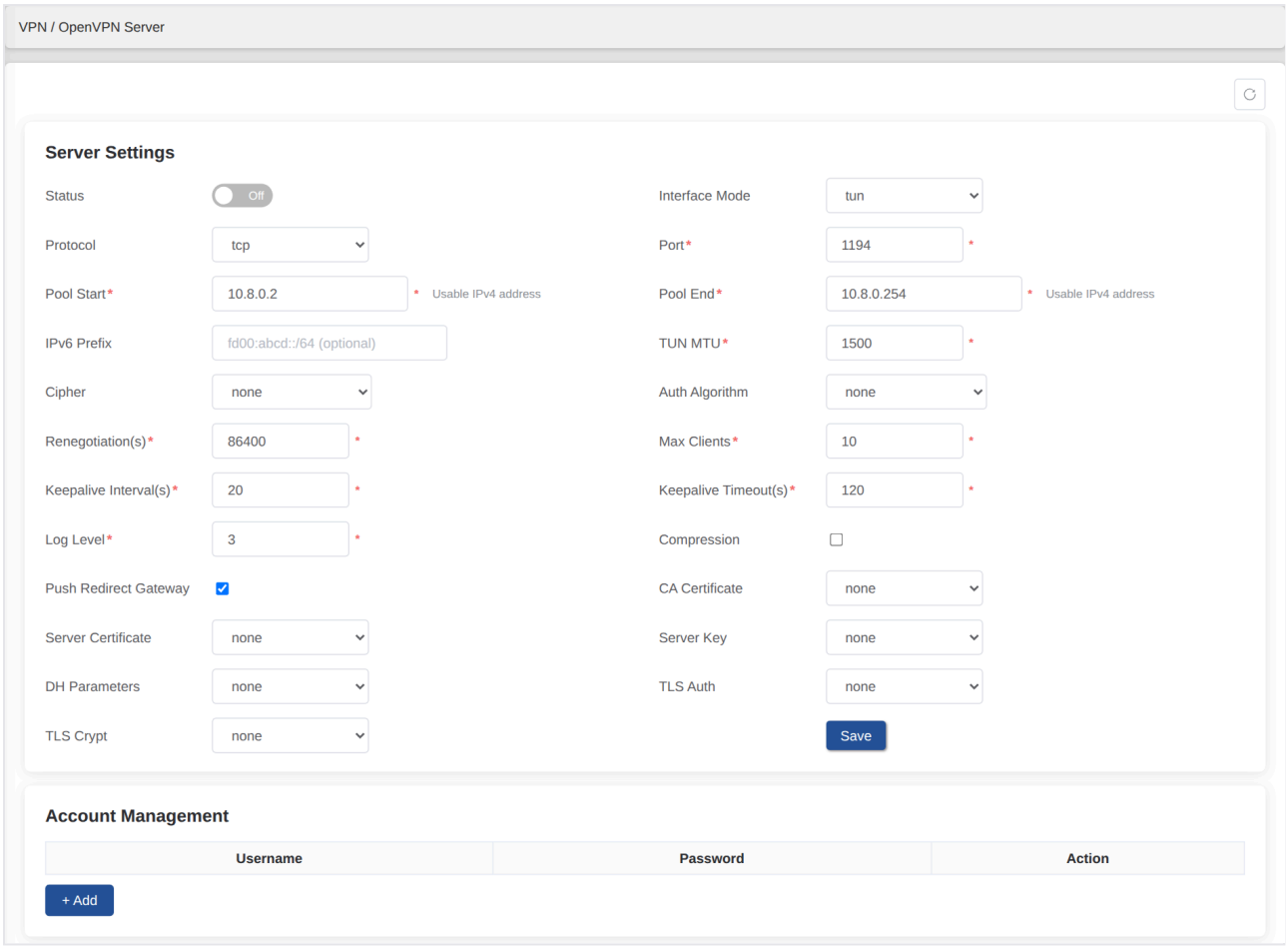


Figure 6-3 OpenVPN server (1/2)

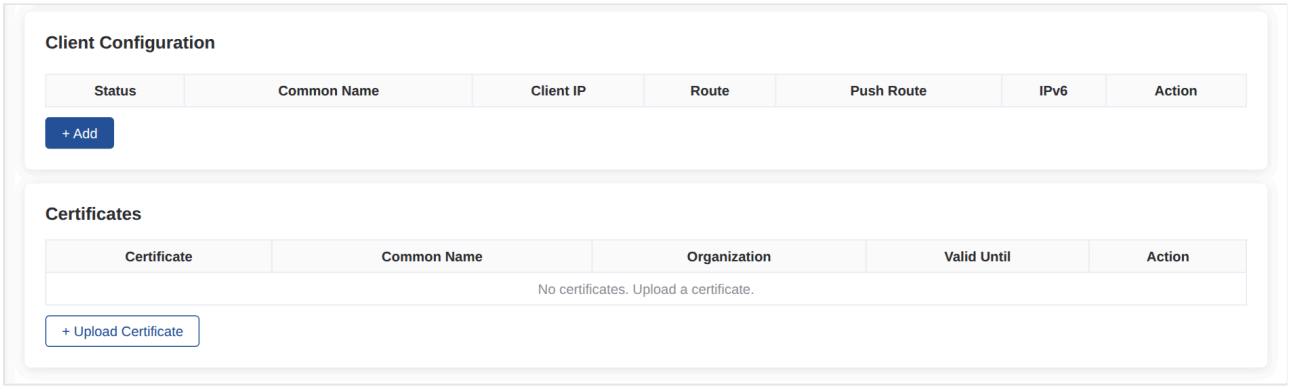


Figure 6-4 OpenVPN server (2/2)

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

UI FIELD	ENTRY	BASIS
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.

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

LISTENER AND ADDRESSING

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

AUTHENTICATION AND CERTIFICATES

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

ROUTES AND RUNTIME

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

6.4 WireGuard

Path VPN > WireGuard

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

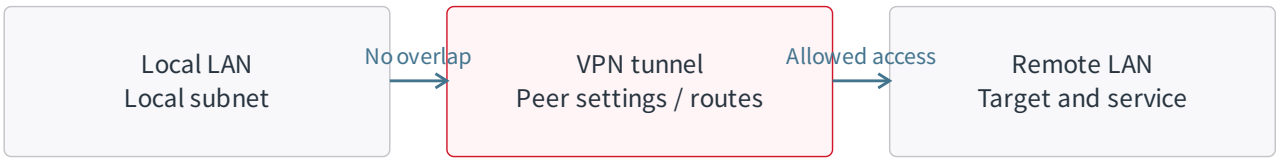


Figure 6-5 WireGuard

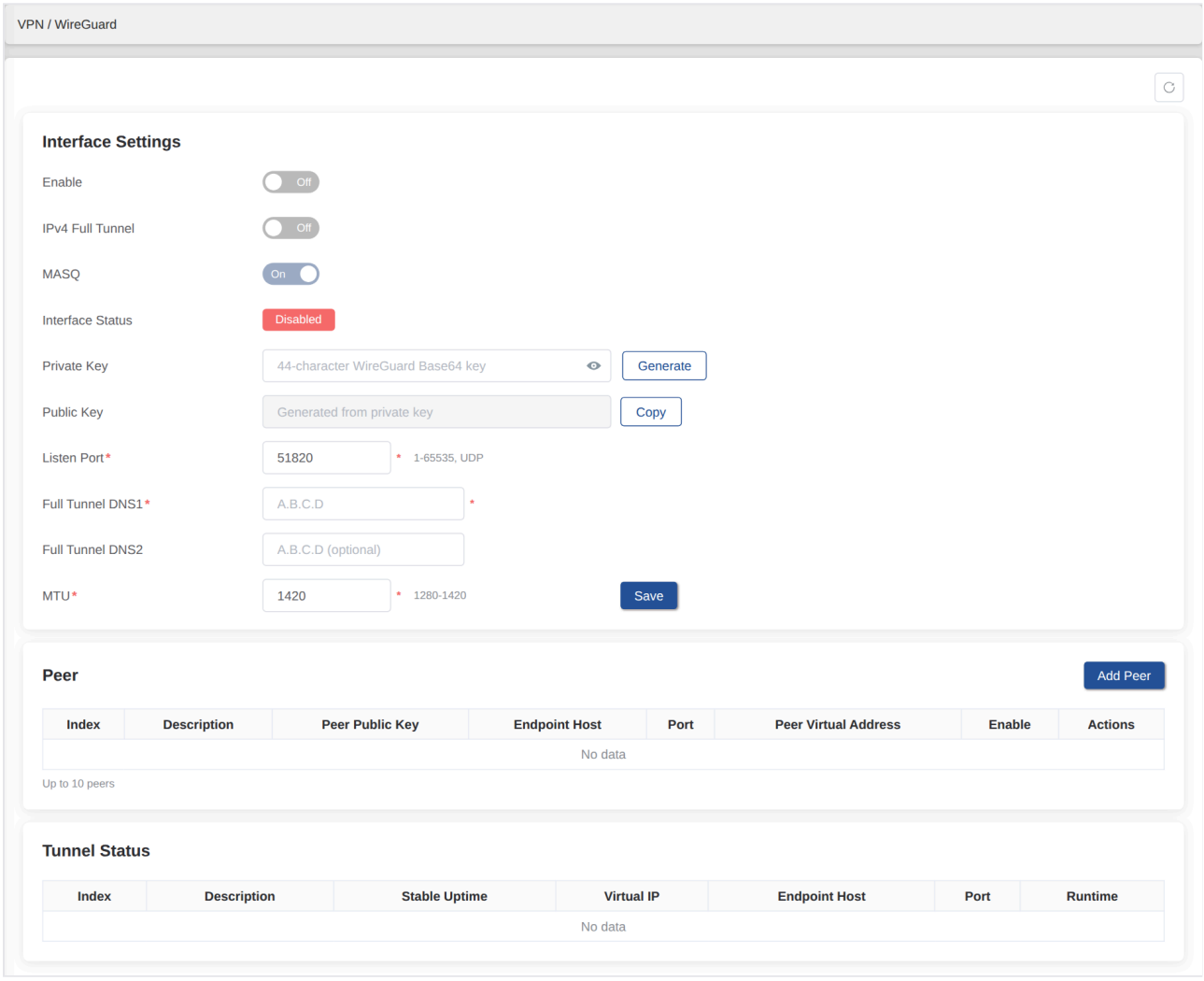


Figure 6-6 WireGuard

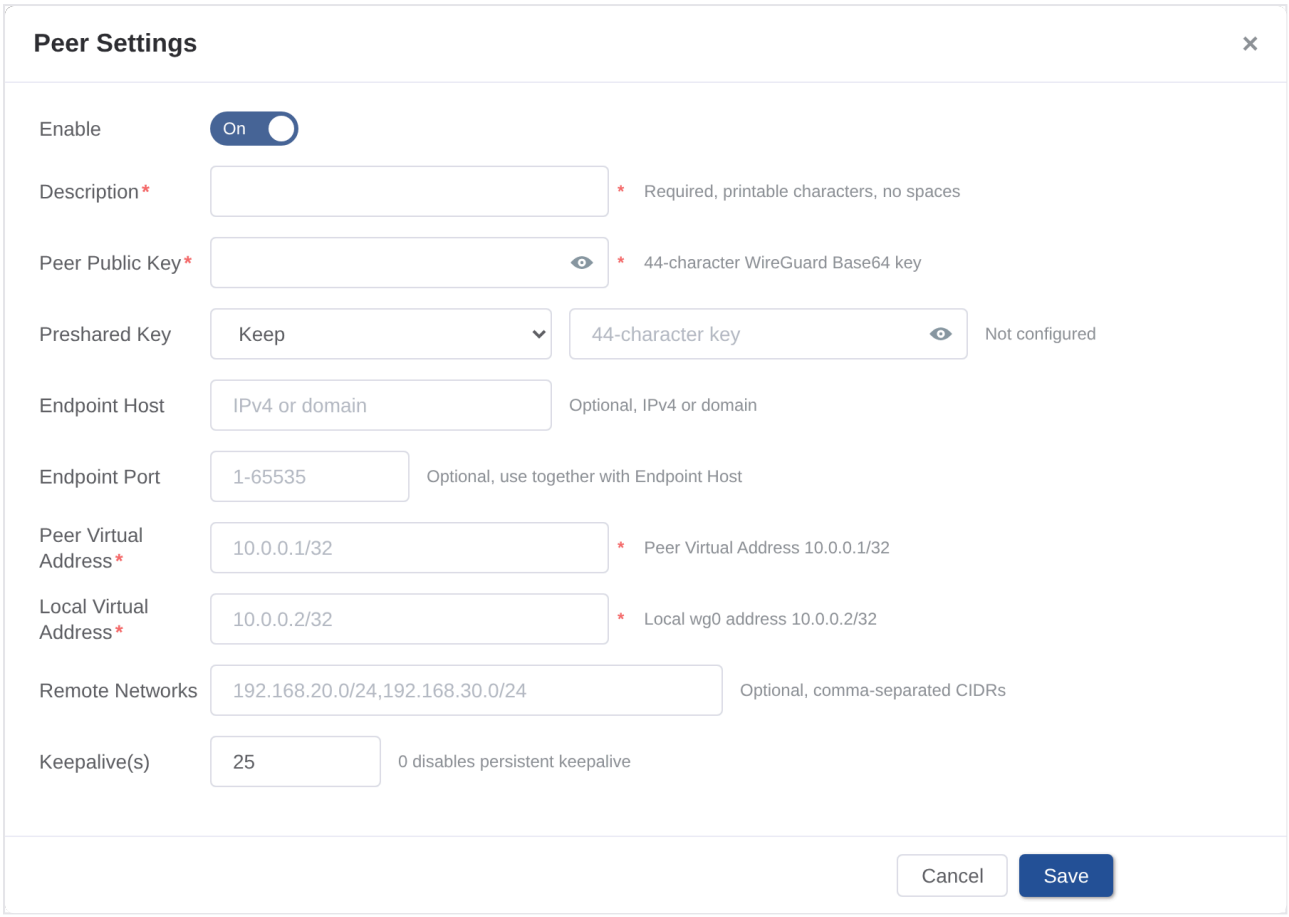


Figure 6-7 WireGuard

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.

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

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

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.

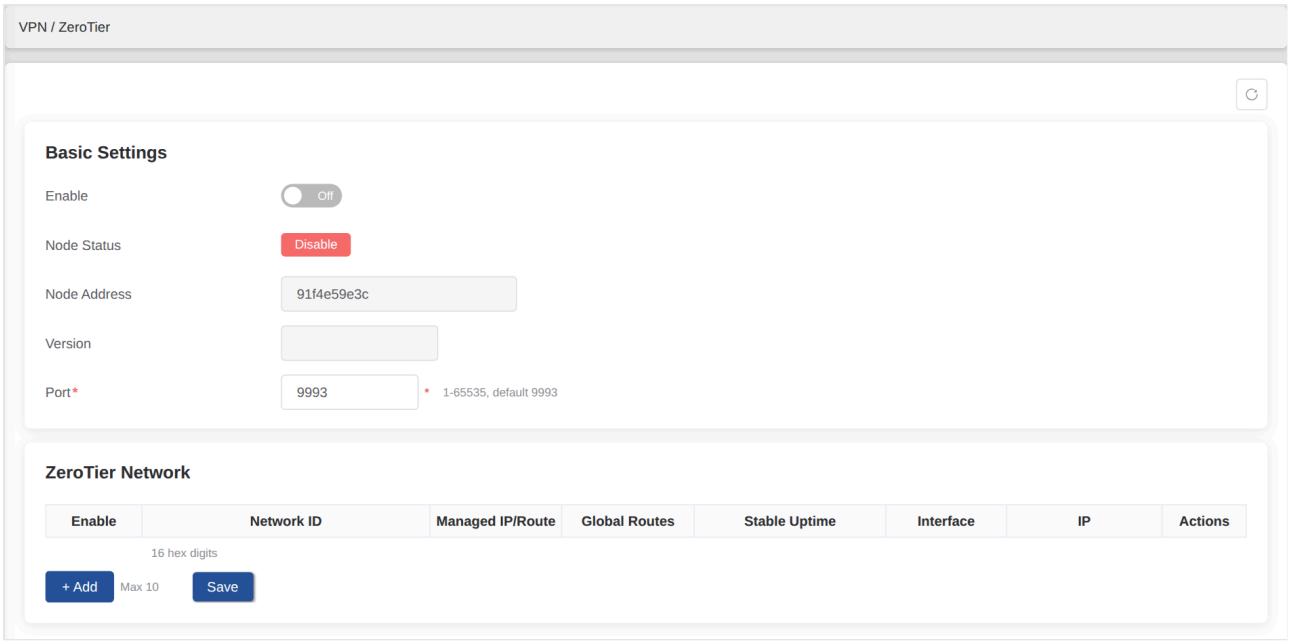


Figure 6-8 ZeroTier

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.

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

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

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.

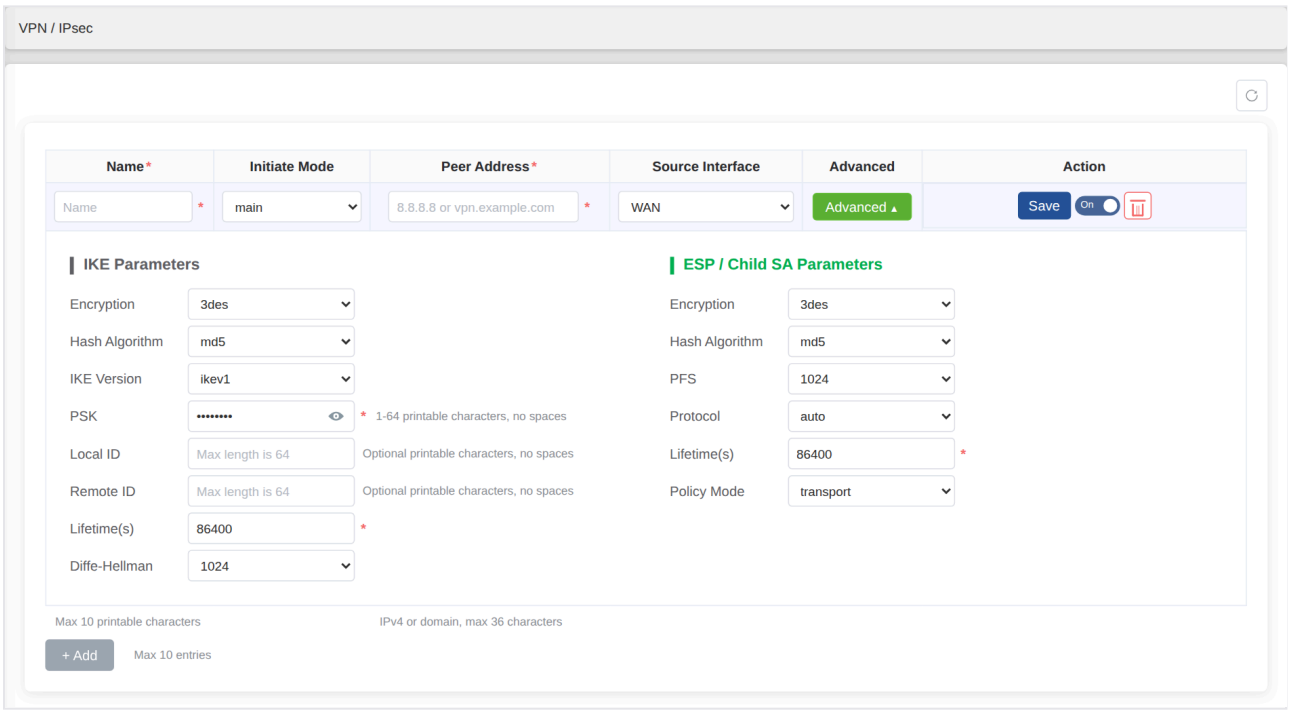


Figure 6-9 IPsec

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.

> **Check the result** Negotiation succeeds and actual services across protected subnets work 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
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

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.

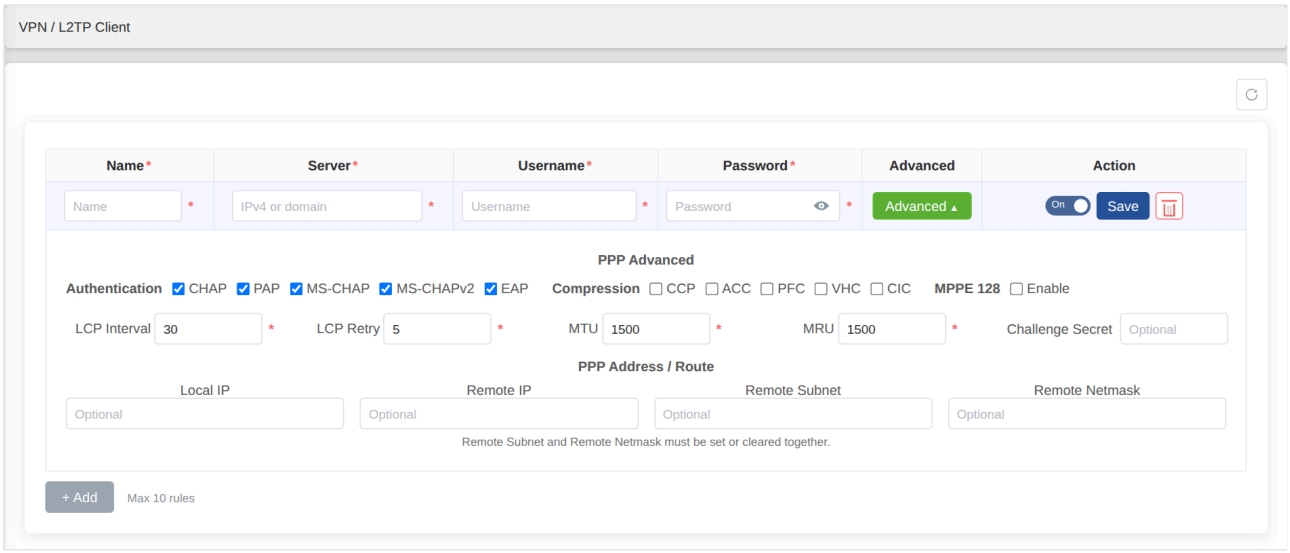


Figure 6-10 L2TP client

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.

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

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

> ! 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.

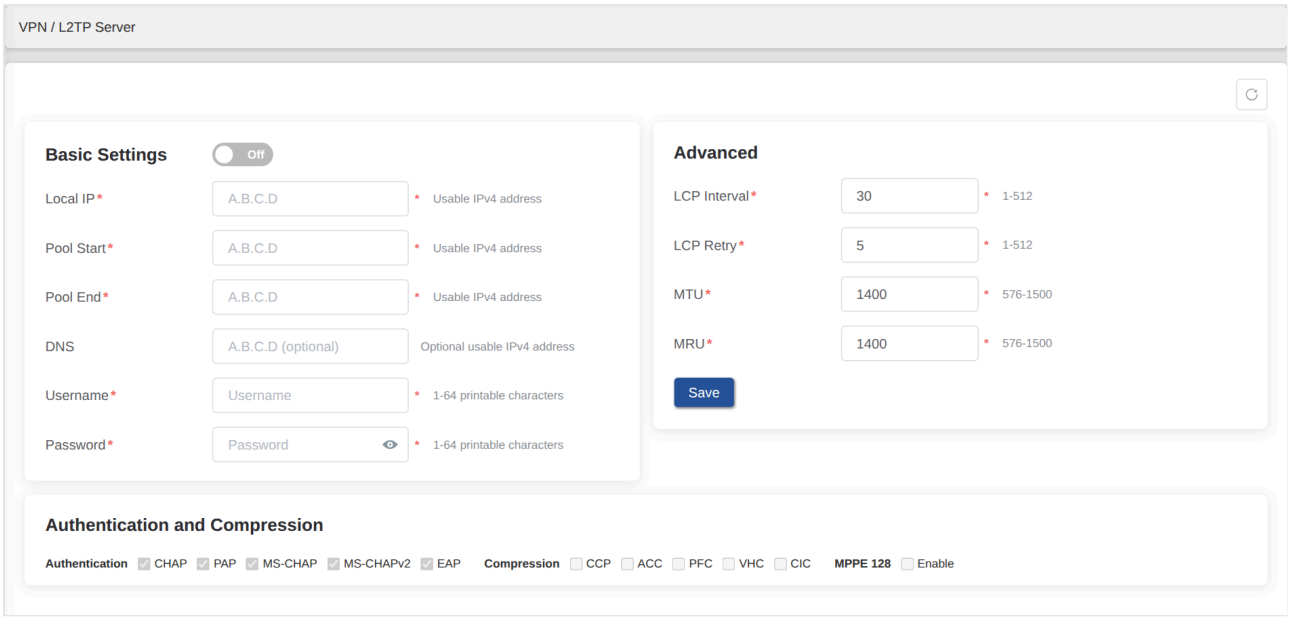


Figure 6-11 L2TP server

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.

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

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

6.9 GRE

Path VPN > GRE

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

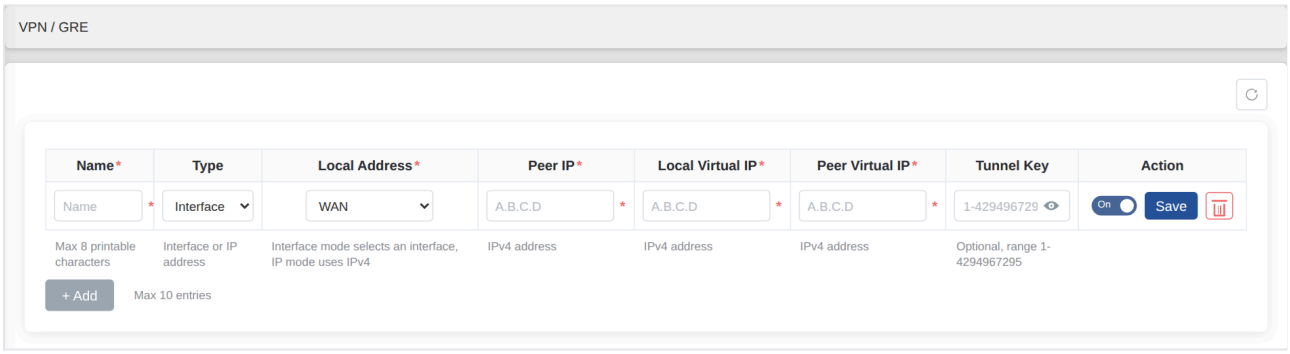


Figure 6-12 GRE

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.

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

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

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.

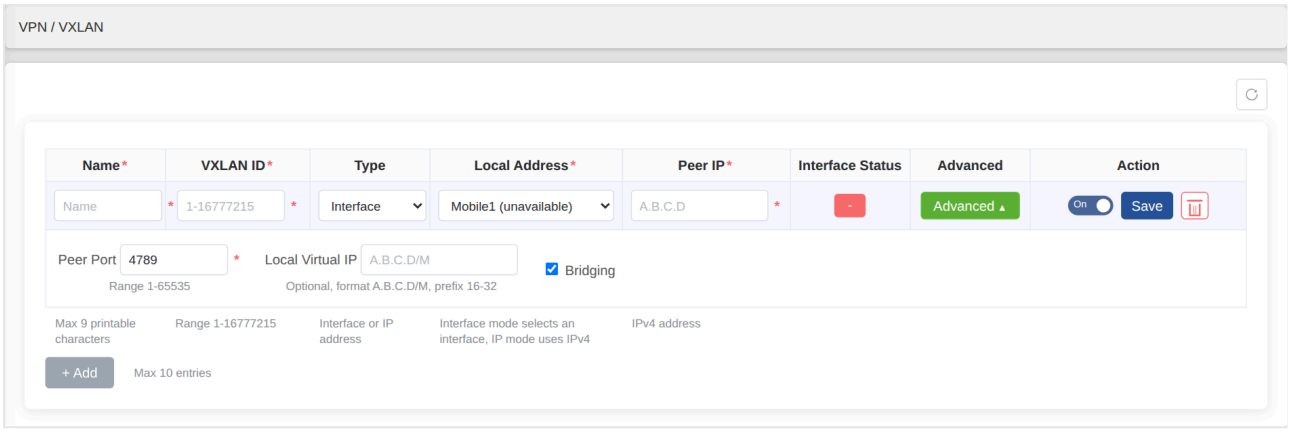


Figure 6-13 VXLAN

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.

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

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

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.

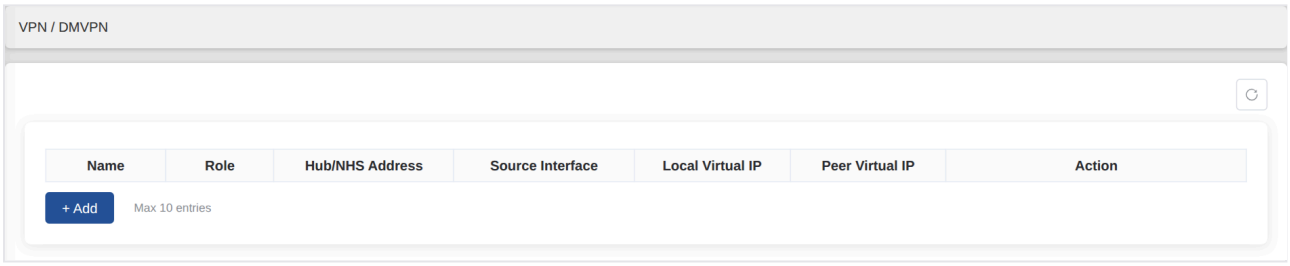


Figure 6-14 DMVPN

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

UI FIELD	ENTRY	BASIS
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.

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

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

6.12 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.

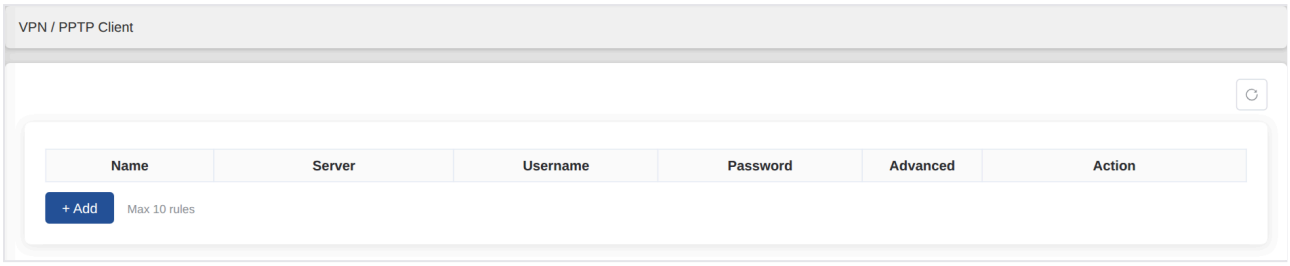


Figure 6-15 PPTP client and server

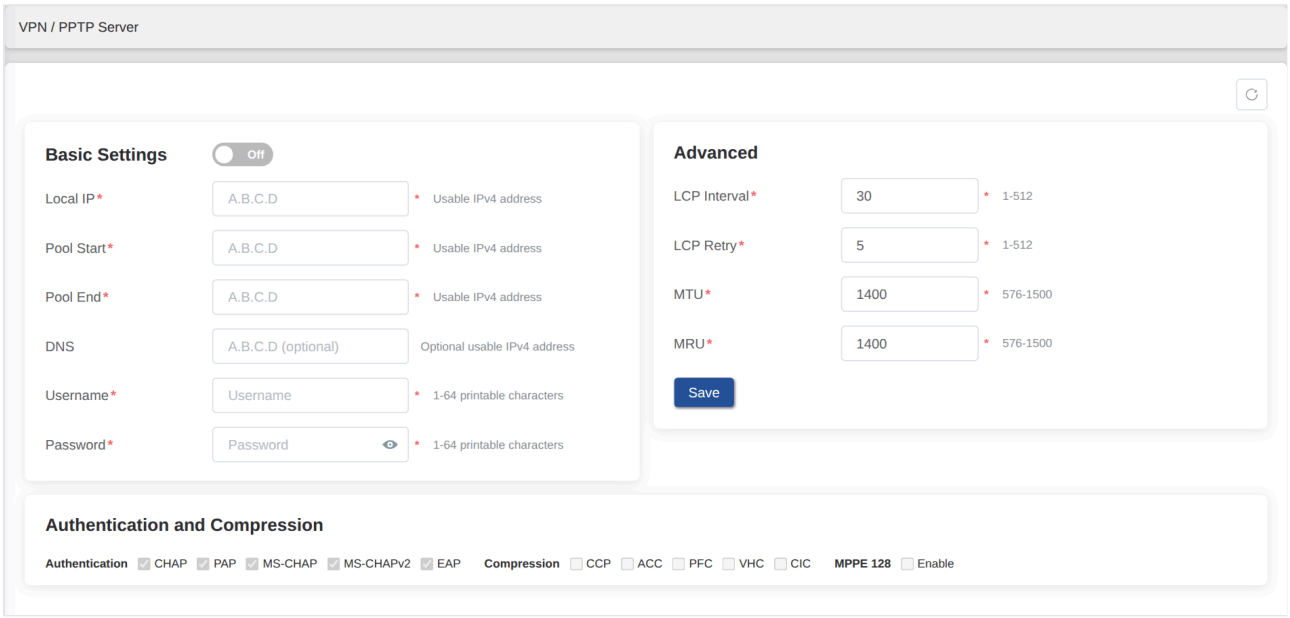


Figure 6-16 PPTP client and server

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
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.

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

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

CHAPTER

07

Forwarding

Configure mappings, routes and bandwidth limits for the site network



YZW1000

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.

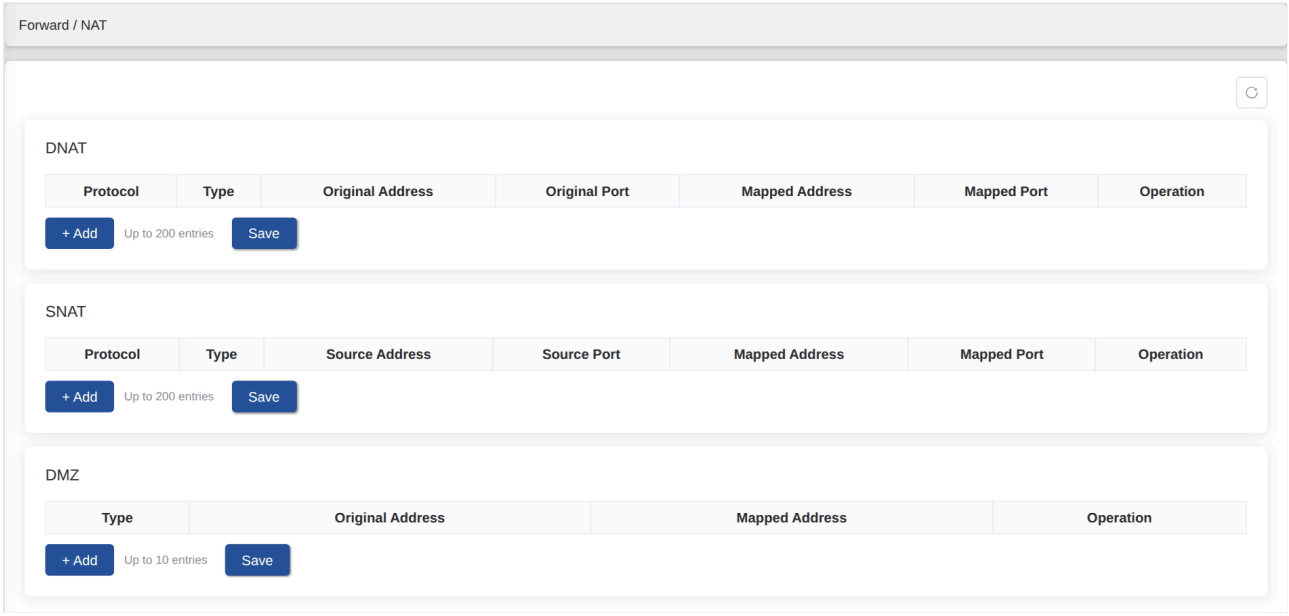


Figure 7-1 NAT and port forwarding

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.

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

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

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.

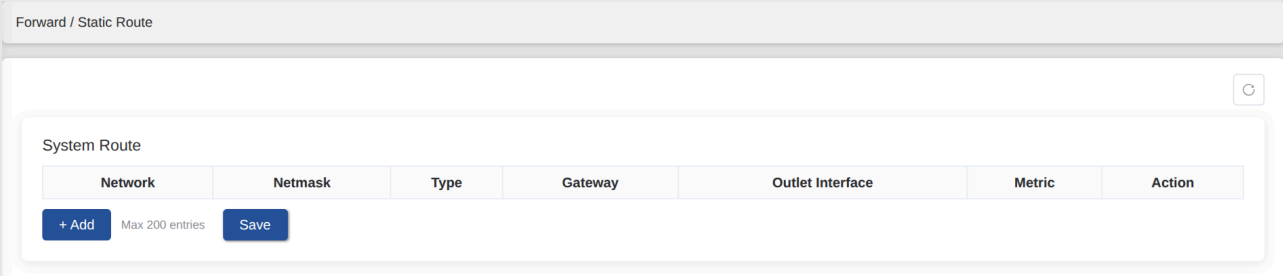


Figure 7-2 Static routes

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.

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

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

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

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.

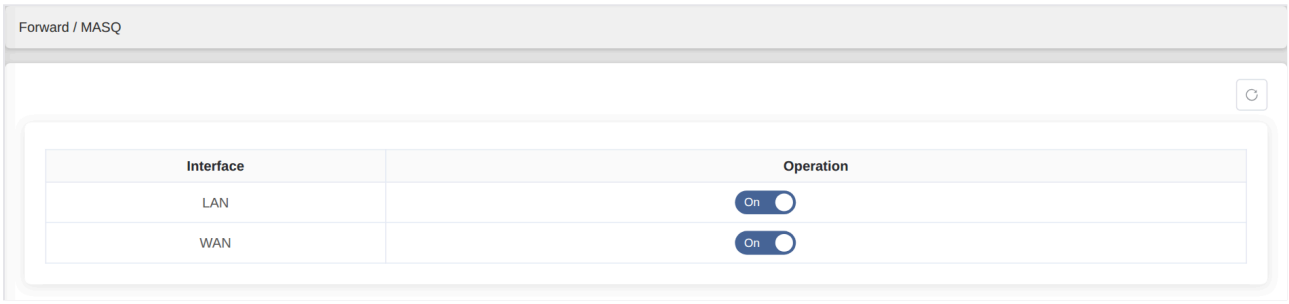


Figure 7-3 MASQ masquerading

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.

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

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

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.

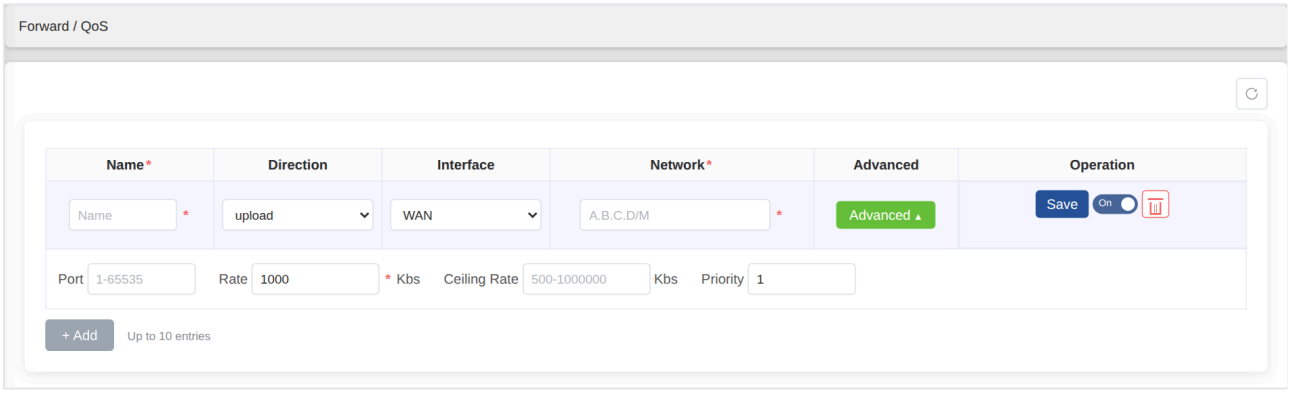


Figure 7-4 QoS rate control

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

UI FIELD	ENTRY	BASIS
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.

The displayed Kbs unit means kbit/s (kilobits per second), not KB/s; 1000 kbit/s is approximately 1 Mbit/s.

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Name / Direction	Name the rule and select upload/download according to the page definition
2	Interface / Network	Define the affected interface and network scope
3	Port	Specify service ports when limiting applications; follow the page semantics for an empty field
4	Rate / Ceiling Rate	Use kbit/s, not KB/s. Ceiling Rate is the rule maximum and must be at least Rate; actual scheduling also depends on link capacity and other traffic.
5	Priority	Sets scheduling preference within the rule, not end-to-end bandwidth on external networks

CHAPTER

08

Firewall

Manage service ports, address rules and domain access policies



YZW1000

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.

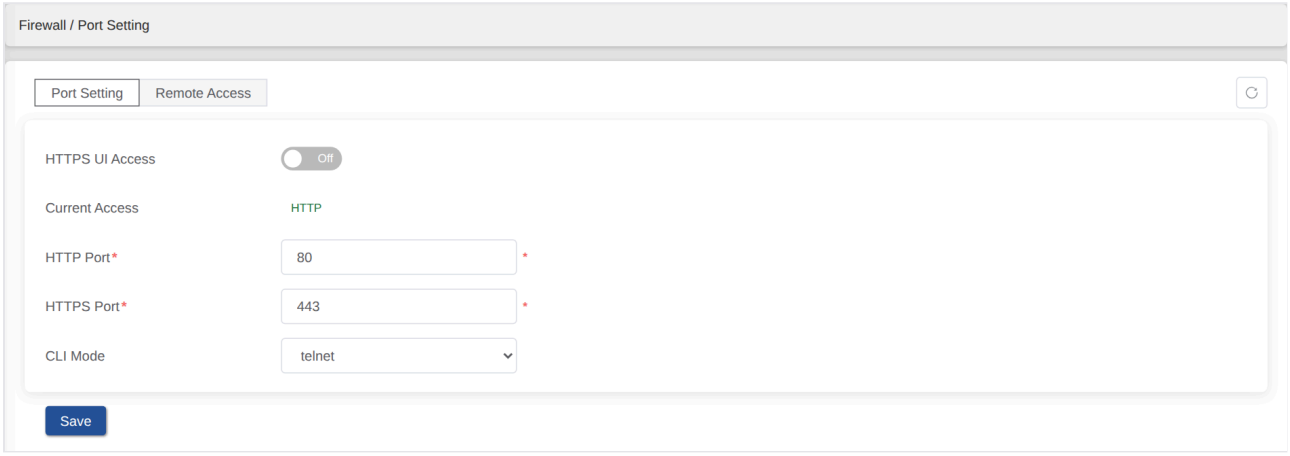
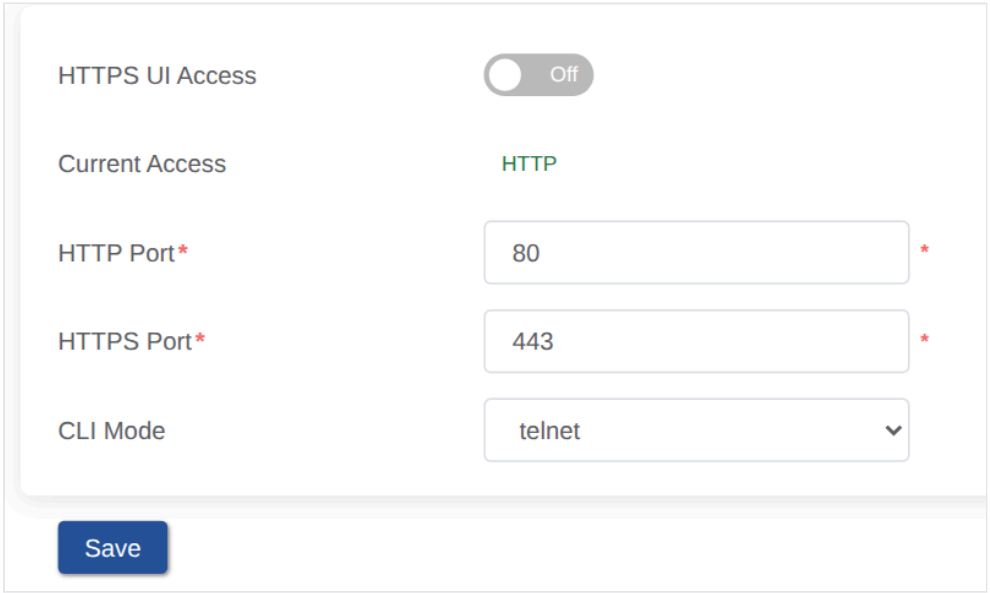


Figure 8-1 Management ports and remote access

Native interface detail (complete panel above)



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.

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

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

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.

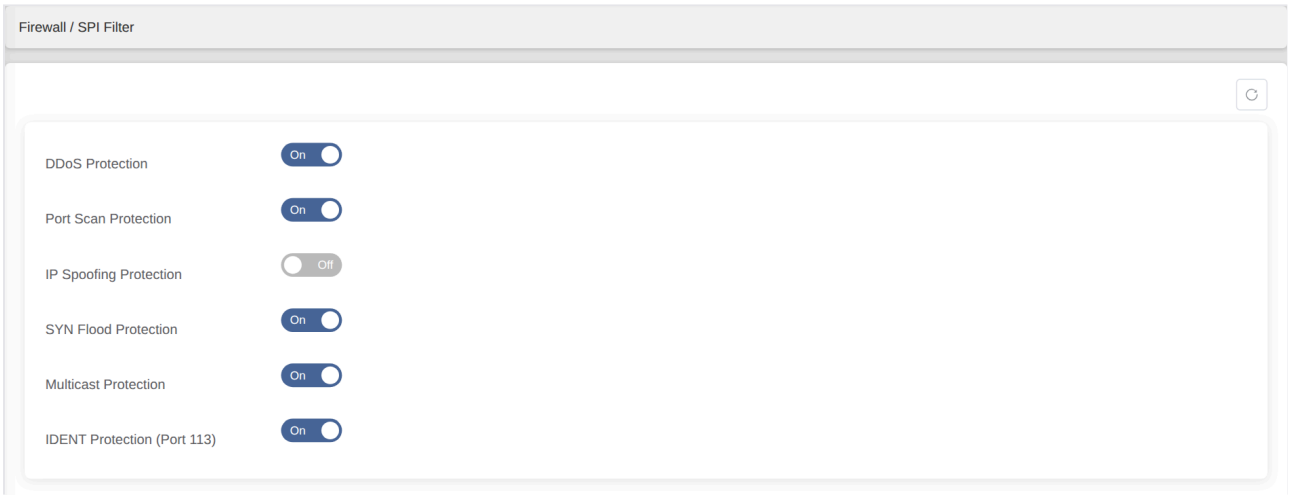


Figure 8-2 SPI filtering

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.

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

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

8.3 Address filtering

Path Firewall > IP Filter

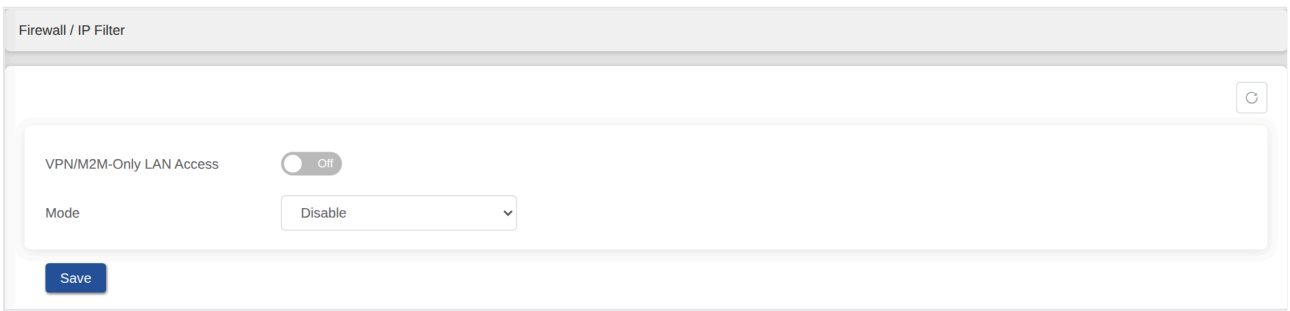


Figure 8-3 Address filtering

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.

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

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.
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

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.

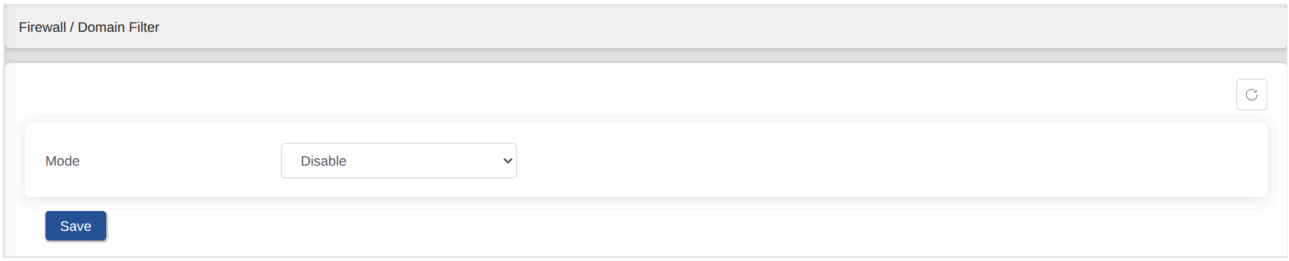


Figure 8-4 Domain filtering

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.

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

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

CHAPTER

09

System management

Maintain time, logs, passwords, configuration backups and firmware



YZW1000

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.

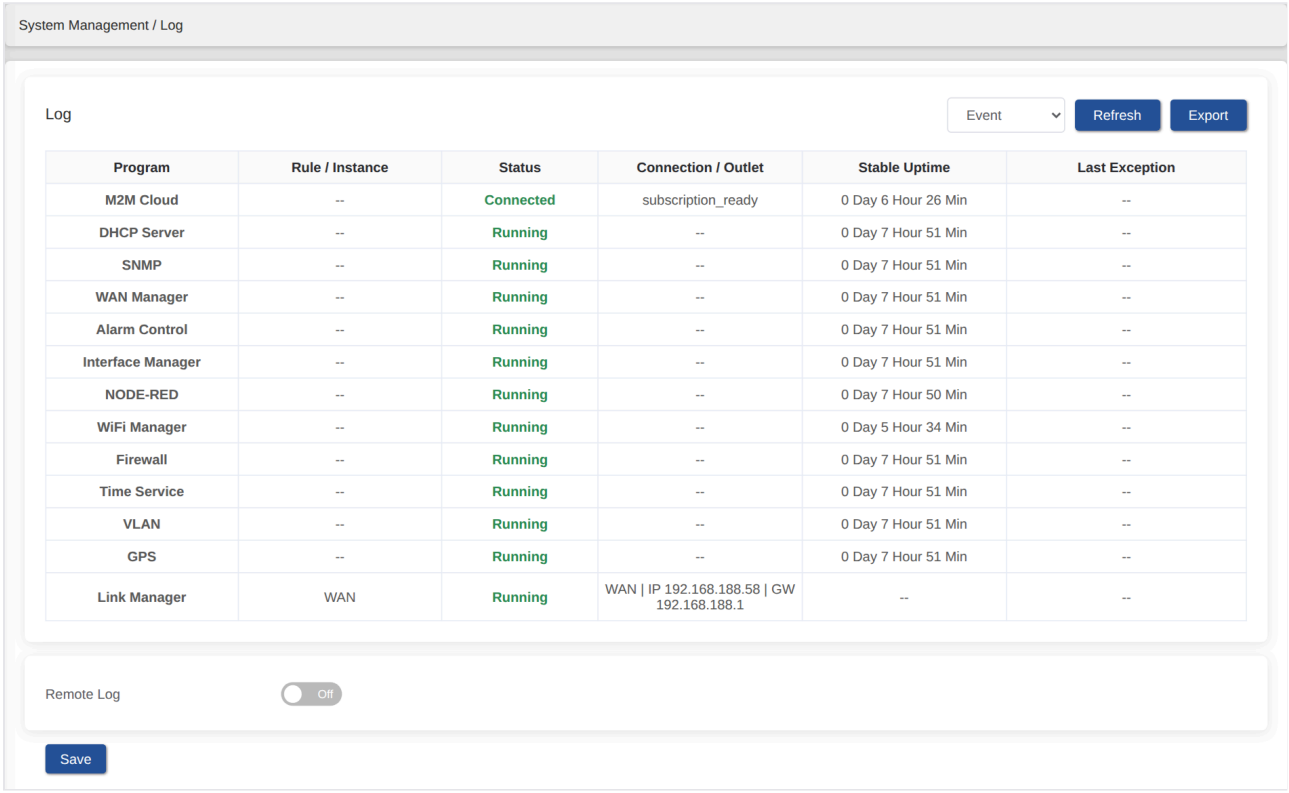


Figure 9-1 Local logs

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.

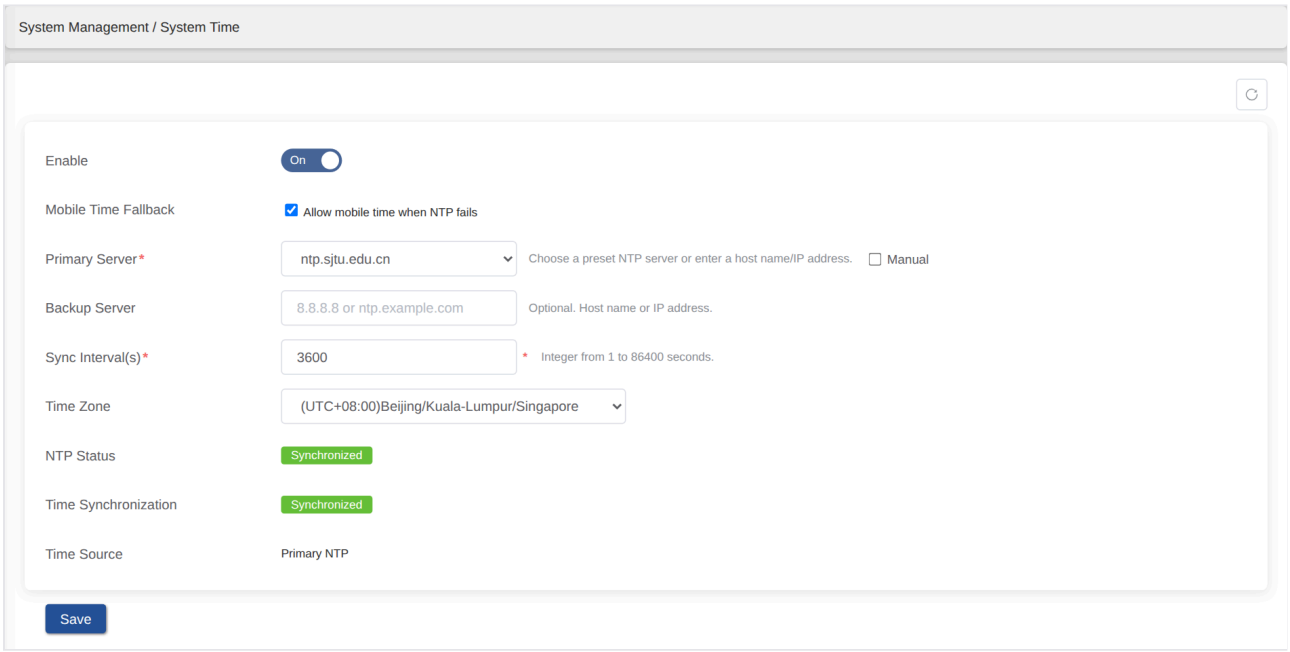


Figure 9-2 System time

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.

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

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	Mobile Time Fallback	Use only with an available modem time source and exposed support; still check NTP reachability
5	Status / Time Source	Check synchronization and the actual source; certificates and log analysis also rely on correct time

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.

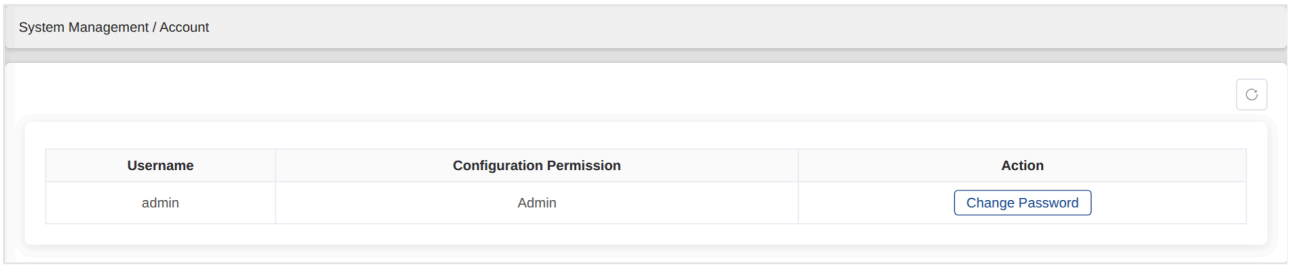


Figure 9-3 Admin password management

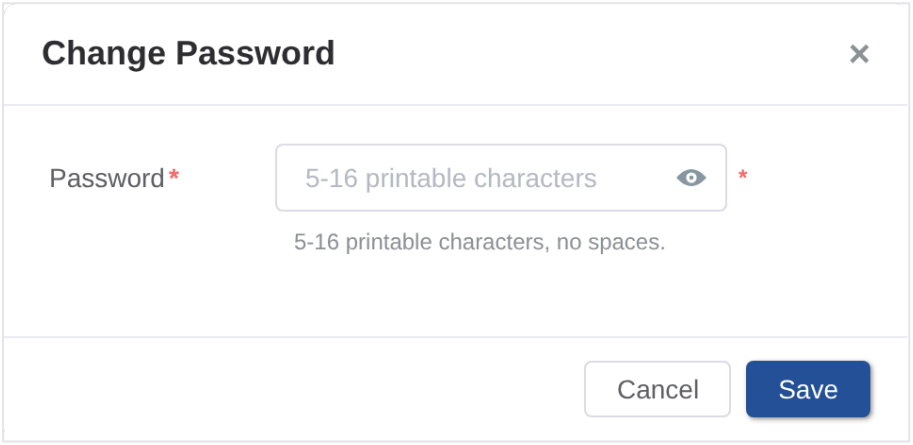


Figure 9-4 admin password dialog

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.

Change the initial admin password before enabling public or remote management. Use 5–16 printable ASCII characters: letters, digits or ASCII punctuation, without spaces or non-ASCII characters. Save and sign in again with the new password. Maintain Node-RED and VPN credentials separately.

Verify a new login after saving. For WAN-source restrictions, HTTPS and separate VPN/Node-RED credentials, see the deployment actions in 3.1 First login. The actual 5–16-character ASCII rule does not establish mandatory first-login changes or multiple accounts.

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

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/Node-RED accounts are separate

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.

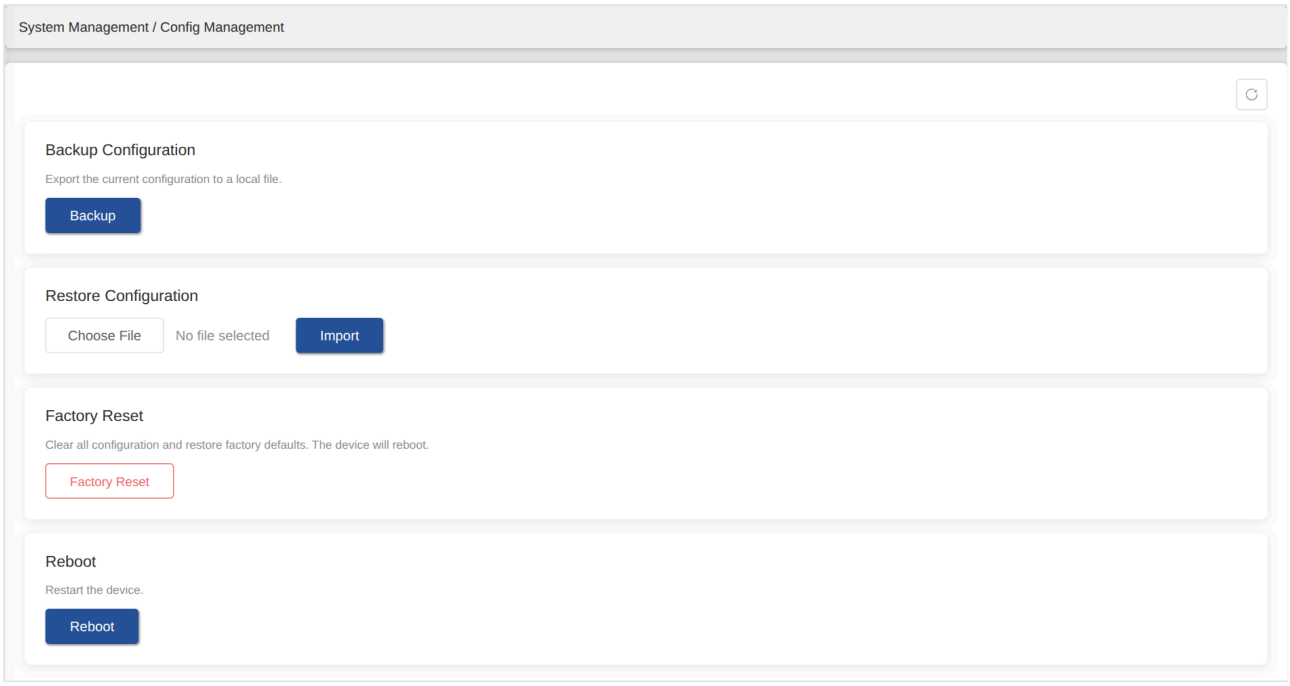


Figure 9-5 Configuration backup and restore

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.

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

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
3	Factory Reset	Clears business configuration and reboots; prepare a backup and reconnection details
4	Reboot	Restarts the system and temporarily interrupts services

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

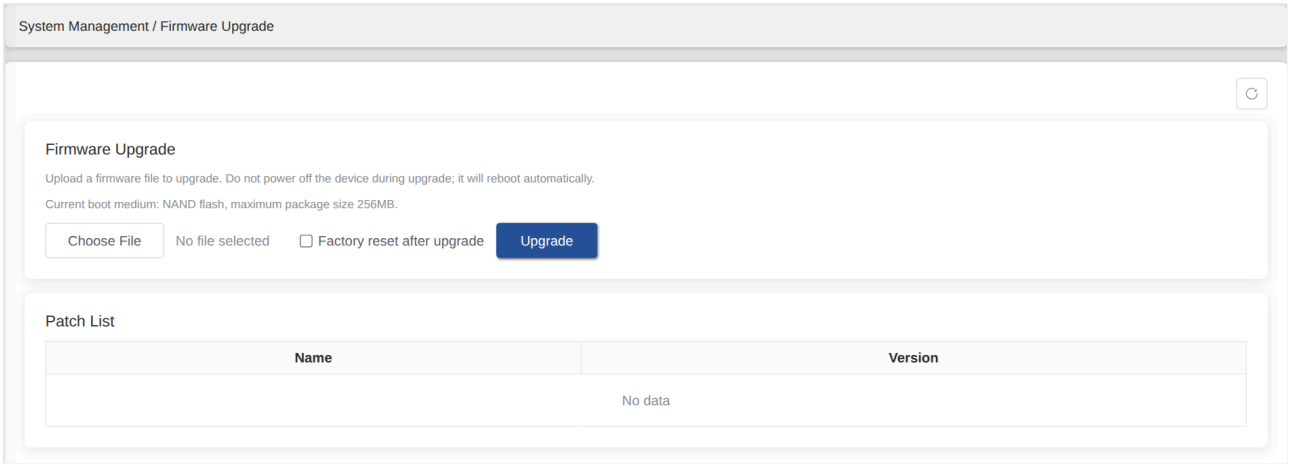


Figure 9-6 Firmware upgrade

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.

FIRMWARE UPGRADE

1. Back up configuration and obtain the released firmware matching YZW1000 and its storage variant. Read the release notes.
2. Select the file on the upgrade page and choose whether to retain configuration as required for this upgrade.
3. Maintain power while upgrading and booting. Sign in again and verify version, networking, acquisition and remote services.

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

FIELD REFERENCE

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
1	Firmware File	Select a released package matching YZW1000 and its NAND storage variant
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

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.

> **Factory reset clears saved network and application configuration.** Export a backup, record the firmware, management address and access method, and ensure local reconnection is possible before proceeding. Holding Reset to the factory-reset threshold is not an ordinary reboot.

ACTION	EFFECT ON THIS MODEL
Release reset button before 5 seconds	Reboot
Hold at least 5 seconds, then release	Factory reset
Web Reboot	Normal restart, temporarily interrupting services
Web Factory Reset	Clear configuration, restore defaults and reboot

Reconnect using the delivered default access information after reset. If the system cannot start, use the recovery package and instructions matching this unit's NAND storage and boot-loader. Follow that version's service instructions for addresses, connectors and button timing.

CHAPTER

10

Node-RED

Use the editor to import, inspect, deploy and back up flows



YZW1000

10. Node-RED visual programming

10.1 Open the editor and understand nodes

Path Application > NODE-RED > Editor

This chapter uses an “Example data → Inspect payload” flow to introduce the editor. The supplied Node-RED_Basic_Example.json contains only Inject and Debug nodes and does not connect to field equipment.

IDENTIFY THE FOUR EDITOR AREAS

Find nodes on the left, arrange them in the workspace, inspect help/debug on the right, and deploy at the upper right. Read a selected node’s help before setting its input, connections and output target.

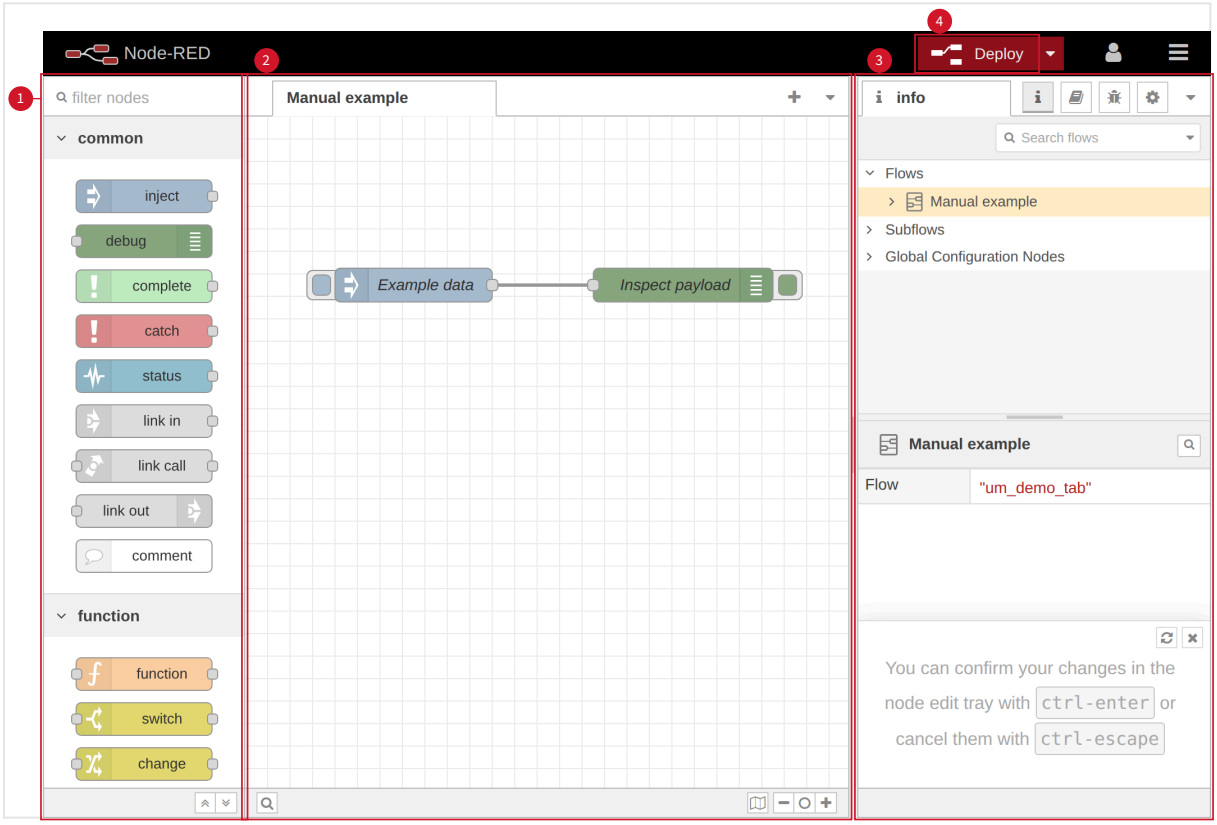


Figure 10-1 Node-RED editor areas

1 Palette: find input, processing and output nodes

2 Workspace: arrange and wire nodes

3 Sidebar: inspect information, help and Debug

4 Deploy: apply reviewed flows to the runtime

1. Use the left palette to find and drag nodes; wire their inputs and outputs on the center workspace.
2. Select a node and read Info / Help in the right sidebar. Use Debug to inspect messages.
3. Import and inspect the supplied example before deploying and triggering it as described next.

SELECT A NODE AND READ ITS HELP

Select Inspect payload on the canvas, then open the Help sidebar to read its inputs, outputs and configuration. Use the same method for other nodes and follow the help for the installed version.

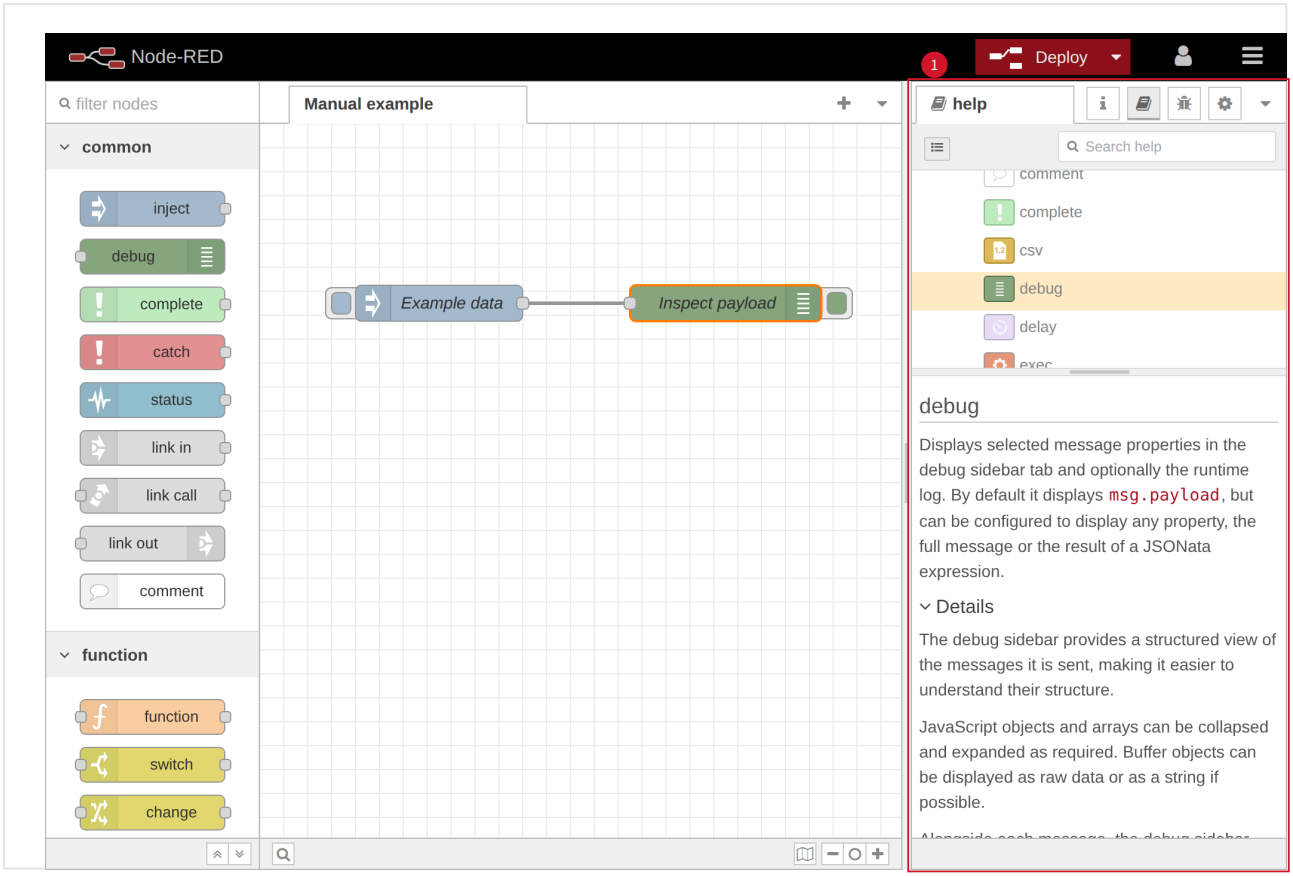


Figure 10-2 Read node help

1 Help: read the selected node documentation

1. Select Inspect payload and confirm the selected node.
2. Open Help in the sidebar and read its purpose, inputs, outputs and settings.
3. Follow the same process for other nodes. For network or serial nodes, also check their targets and resource ownership.

FIELD TASK: OPEN THE EDITOR AND INSPECT FLOW STATE

Use only when Node-RED is delivered. Complete external-PC M1 and export existing configuration/flows. Optional models need confirmed entitlement/storage/install state.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Status / Development	Start runtime / enable development entry if needed	Inspect running state before opening editor
Account / Password	change delivered credentials	Separate from Web admin
Broker in supplied flow	192.168.10.10:1884	Enter lab credentials in the flow broker configuration

SAVE, TEST AND OBSERVE

1. Start the runtime and open the provided editor URL. Sign in with delivered credentials and export current flows before importing field_temperature.json.
2. Enter field/DemoOnly2026 in the MQTT config node, check topics, deploy and inspect connection status plus Debug, not only runtime state.

PASS CRITERIA AND DIAGNOSIS

Editor unavailable: inspect runtime, port, permissions and development entry. Missing nodes: inspect delivered components before resetting flows.

Finish and restore: Remove/stop lab flows and restore the export; close development access according to project policy.

Read node help and distinguish msg.payload, topic, connection parameters and node configuration. For serial or field-control nodes, check port ownership and target equipment first. A healthy runtime does not mean the workspace business logic is deployed.

Gateway inspection: runtime, installed nodes and UI were checked read-only. The supplied flows were not deployed to the gateway; gateway service operation remains unverified.

> **Check the result** After manual triggering, Debug shows temperature as 25.5; this is demonstration data.

10.2 Import and deploy flows

Path Node-RED > Menu > Import

FIELD TASK: BACK UP BEFORE IMPORT AND VERIFY OUTPUT AFTER DEPLOY

Get field_temperature.json or field_alarm.json from the tool package. Export current complete flows; importing creates a draft and Deploy applies it.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Import	select JSON file	Use the actual supplied filename
MQTT Configuration	192.168.10.10:1884 / field / DemoOnly2026	Enter credentials after import

SAVE, TEST AND OBSERVE

1. Import the file, inspect types/topics/config nodes, fill credentials and deploy only after resolving unknown nodes/validation errors.
2. Send E1/E2 test data and inspect results from a separate subscriber.

PASS CRITERIA AND DIAGNOSIS

Missing nodes: inspect delivered components. Imported without data: inspect Deploy/broker/topics; a draft is not running.

Finish and restore: Remove the lab tab, restore the export and deploy the original flows.

OBTAIN THE COMPANION FILES

The companion archive is delivered with the PDFs under this exact name:

`YZW1000_使用说明书_V1.5_配套交付包_20261031.zip`

THREE FLOW JSON FILES: USE THESE PRIMARY FILENAMES

`Node-RED_Basic_Example.json`

Section 10.2 basic import; no external broker. Check the destination flow before import.

`Node-RED_Temperature_Processing_Example.json`

Section 10.4 N1 temperature processing; configure the broker, authentication/TLS, actual topics, fields and scale.

Chinese filename alias (byte-identical to the primary file):

`Node-RED_温度处理案例.json`

`Node-RED_Multi_Point_and_Alarm_Example.json`

Section 10.5 N2 state/alarm pair; configure pump1 topics, points, thresholds and the alarm receiver.

Chinese filename alias (byte-identical to the primary file):

`Node-RED_多点组合与异常告警.json`

The three flows use Node-RED 3.0.2 core nodes. Gateway compatibility reference: 交付固件 This identifies the reviewed version; it does not establish field acceptance on that firmware.

BILINGUAL README AND VERSION INVENTORY

`Node-RED案例使用说明.txt`

`Node-RED_Example_Readme_EN.txt`

`配套文件清单_V1.5.txt`

`SHA256SUMS_V1.5.txt`

The readme explains settings and verification limits. The inventory lists versions, purposes, exact names and SHA-256 values. Find the complete filename after extraction rather than transcribing screenshot JSON.

THREE AUXILIARY PUBLICATIONS: ONE CHINESE AND ONE ENGLISH EDITION EACH, SIX PDFS

Requirements and Function Selection Guide

`YZW1000_使用需求与功能选型指南_V1.5_中文.pdf`

`YZW1000_Requirements_and_Function_Selection_V1.5_EN.pdf`

Industrial Application Casebook

YZW1000_典型工业应用解决方案手册_V1.5_中文.pdf

YZW1000_Industrial_Application_Casebook_V1.5_EN.pdf

Compatibility and Acceptance Checklist

YZW1000_功能兼容性与实施验收清单_V1.5_中文.pdf

YZW1000_Compatibility_and_Acceptance_Checklist_V1.5_EN.pdf

All six are V1.5 language editions of the same three publications; use each edition's final page references. If only the main PDF was received, request the archive named above through the original purchase-order support/supplier contact and check the inventory and hashes. A statement that files are included does not replace delivery of those files.

STEP 1: OPEN THE IMPORT DIALOG

Open the upper-right menu and select Import. Both file import and built-in examples start here.

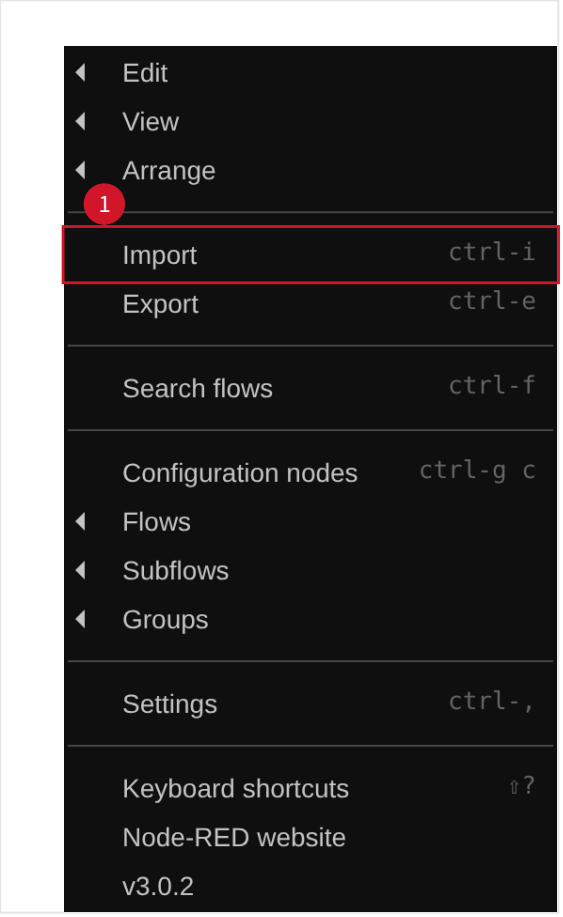


Figure 10-3 Open the Node-RED Import menu

1 Select Import

1. Open the editor menu at the upper right.
2. Select Import to open the flow import dialog.
3. Choose a flow file, paste JSON or open Examples as described next.

STEP 2: SELECT A FILE OR PASTE JSON

Choose the supplied basic example or paste flow JSON. Choose the current or a new flow, then select Import. Restore missing configuration nodes or credentials before proceeding.

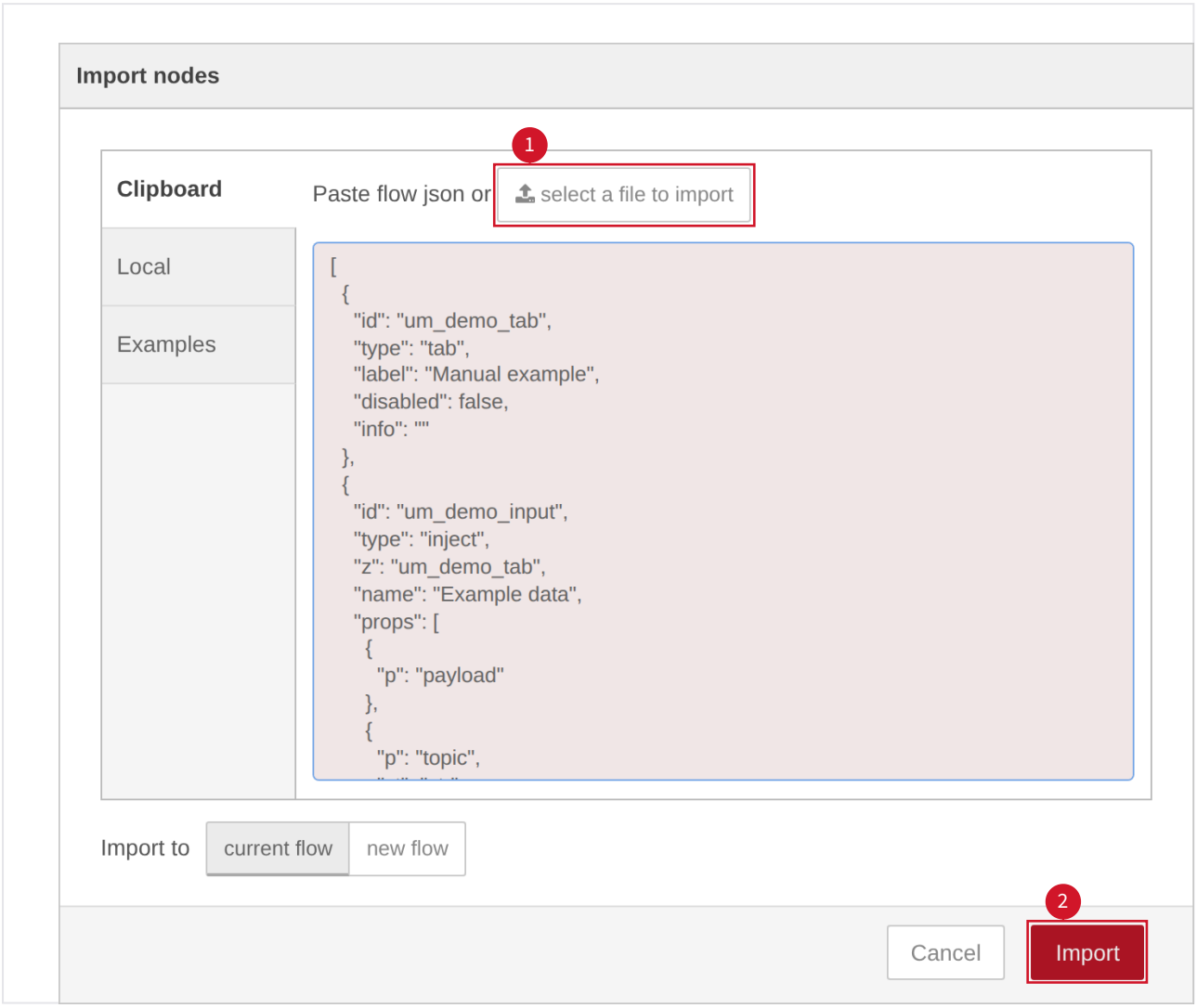


Figure 10-4 Choose a flow file or paste JSON

1 Choose a flow JSON file

2 Review the scope and select Import

1. Use the file selector to choose Node-RED_Basic_Example.json, or paste reviewed flow JSON.
2. Select the current or a new flow. Check the destination before adding to an existing service flow.
3. Select Import and verify that Example data is wired to Inspect payload on the canvas.

STEP 3: REVIEW THE FLOW AND DEPLOY

Check that Example data is wired to Inspect payload. Before deploying, check node validity and any unintended timers or field outputs. Select Deploy, trigger Inject manually, and check that temperature is 25.5 in Debug.

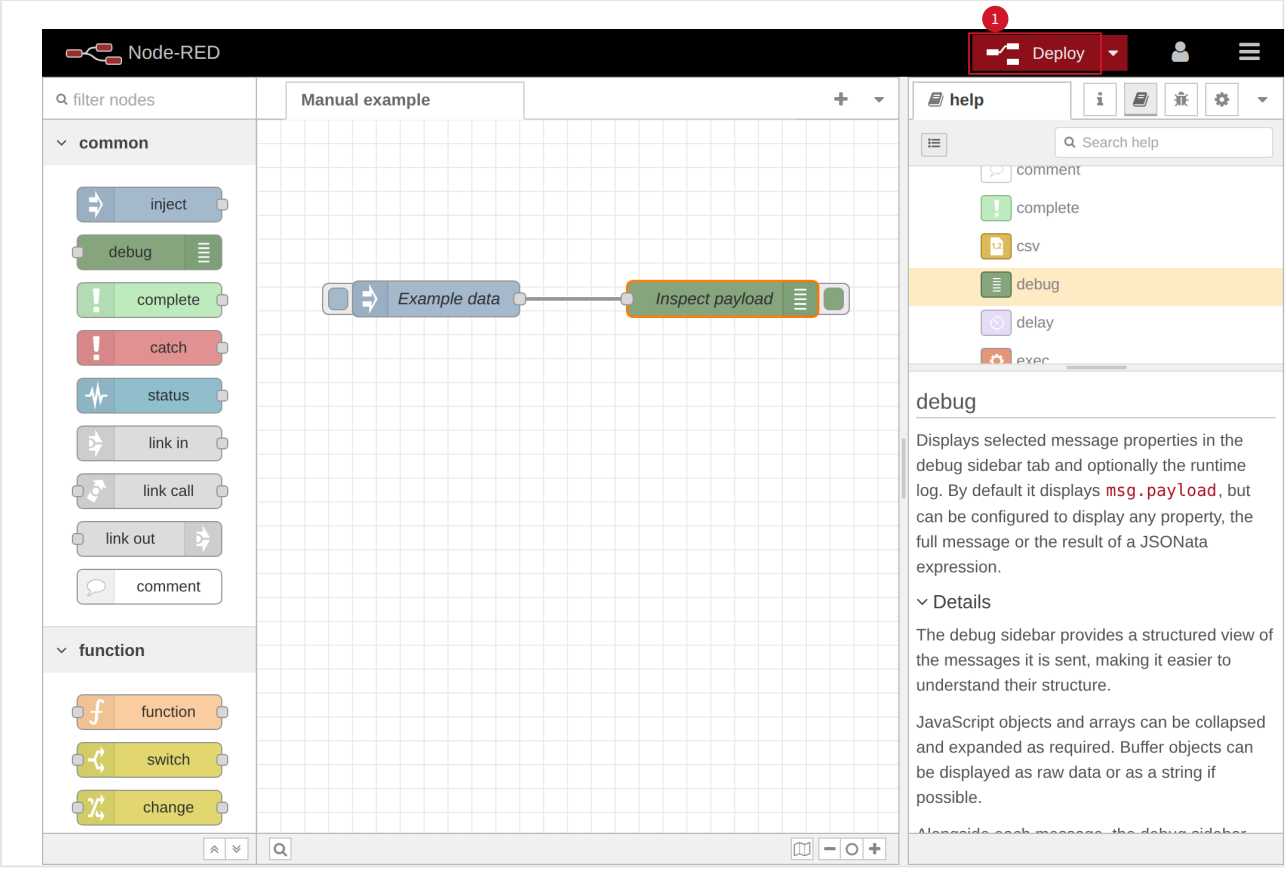


Figure 10-5 Review the workspace and locate Deploy

1 Use Deploy after reviewing the flow

1. Check for missing settings or node errors and for unintended field outputs.
2. Select Deploy, wait for its result and open the Debug sidebar.
3. Use the Inject button beside Example data to trigger the example.
4. Inspect the output and confirm temperature is 25.5. This is demonstration data generated inside the flow.

PRACTICE WITH BUILT-IN EXAMPLES

Choose Examples in the Import dialog, expand a package and its examples, then select and import a flow. Read its help and replace example addresses. Do not deploy a flow that requires unavailable hardware or packages.

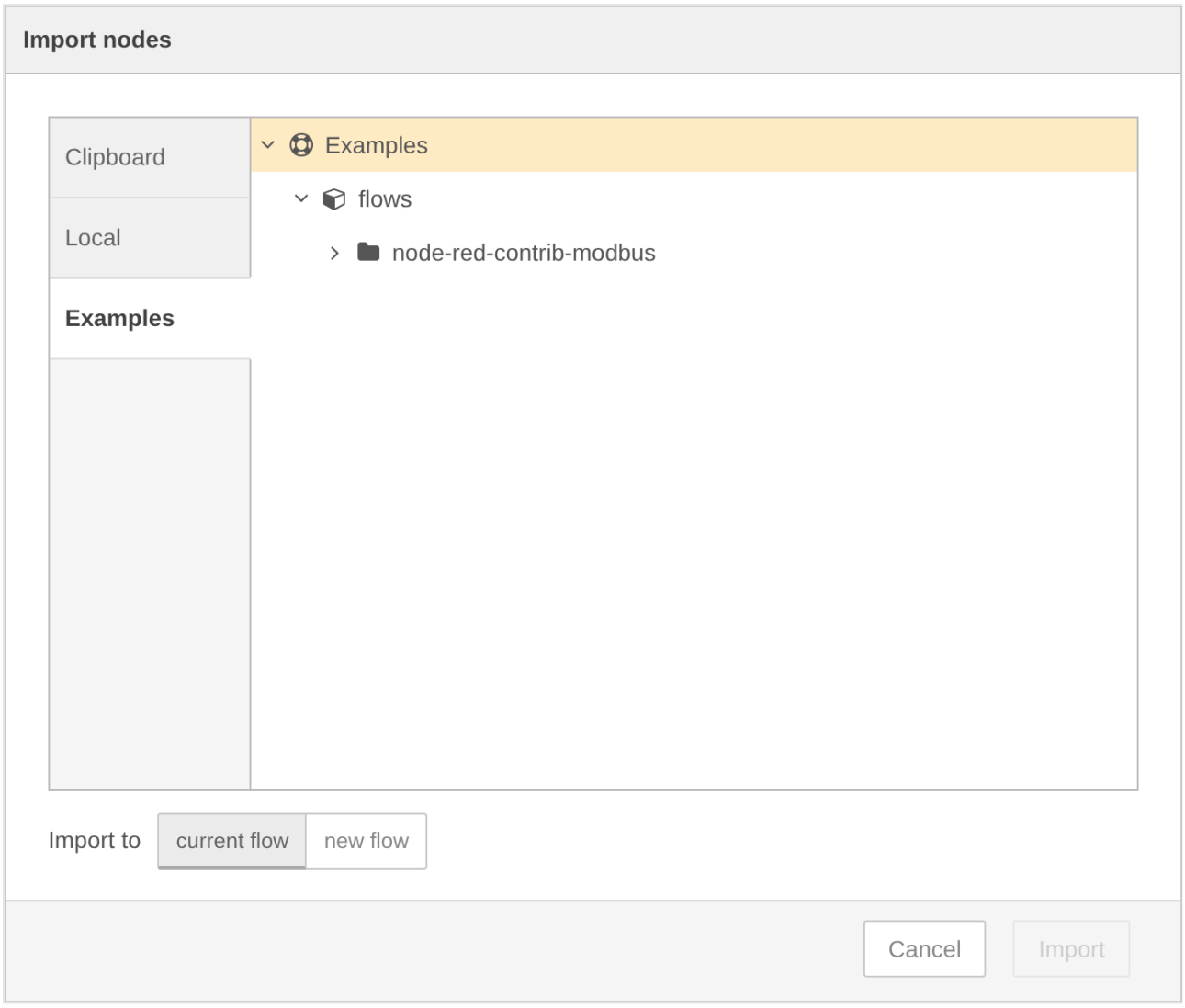


Figure 10-6 Browse Node-RED examples

1. Open Examples in the Import dialog and expand the required package and example folder.
2. Import an example, read node help and review addresses, credentials and external dependencies.
3. Deploy only when the necessary interfaces, packages and settings are available. Use Inject / Debug for basic practice.

Check the result Only intended nodes and wires are imported; after review and deployment, Debug receives the example output.

! Import places a flow in the workspace; Deploy applies it to the runtime. Review field targets and triggers before deploying control outputs.

10.3 Export flows and maintain backups

Path Node-RED > Menu > Export

FIELD TASK: EXPORT FLOWS WITH EVERYTHING NEEDED TO REBUILD

Record flow names, deployment time, node versions and config nodes. Flow JSON generally does not provide directly restorable plaintext credentials; hand them over securely.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Export Scope	all flows or named tabs	Record scope
Filename	Model_site_date_flows.json	Separate from gateway configuration backup

SAVE, TEST AND OBSERVE

1. Export formatted JSON, verify it is non-empty/parseable and save custom-node and credential handover lists.
2. Import in a spare matching environment without production outputs, restore credentials and verify E1/E2 simulated data.

PASS CRITERIA AND DIAGNOSIS

Imports but cannot run: inspect nodes/credentials/paths. Gateway configuration backup alone does not prove third-party flows/dependencies are preserved.

Finish and restore: Restore production flows, remove spare test credentials and securely retain backup/recovery results.

SELECT AN EXPORT SCOPE AND SAVE THE FILE

Choose Export from the editor menu. Check whether selected nodes, the current flow or all flows are included, then select Download. The illustration uses this chapter’ s basic example.

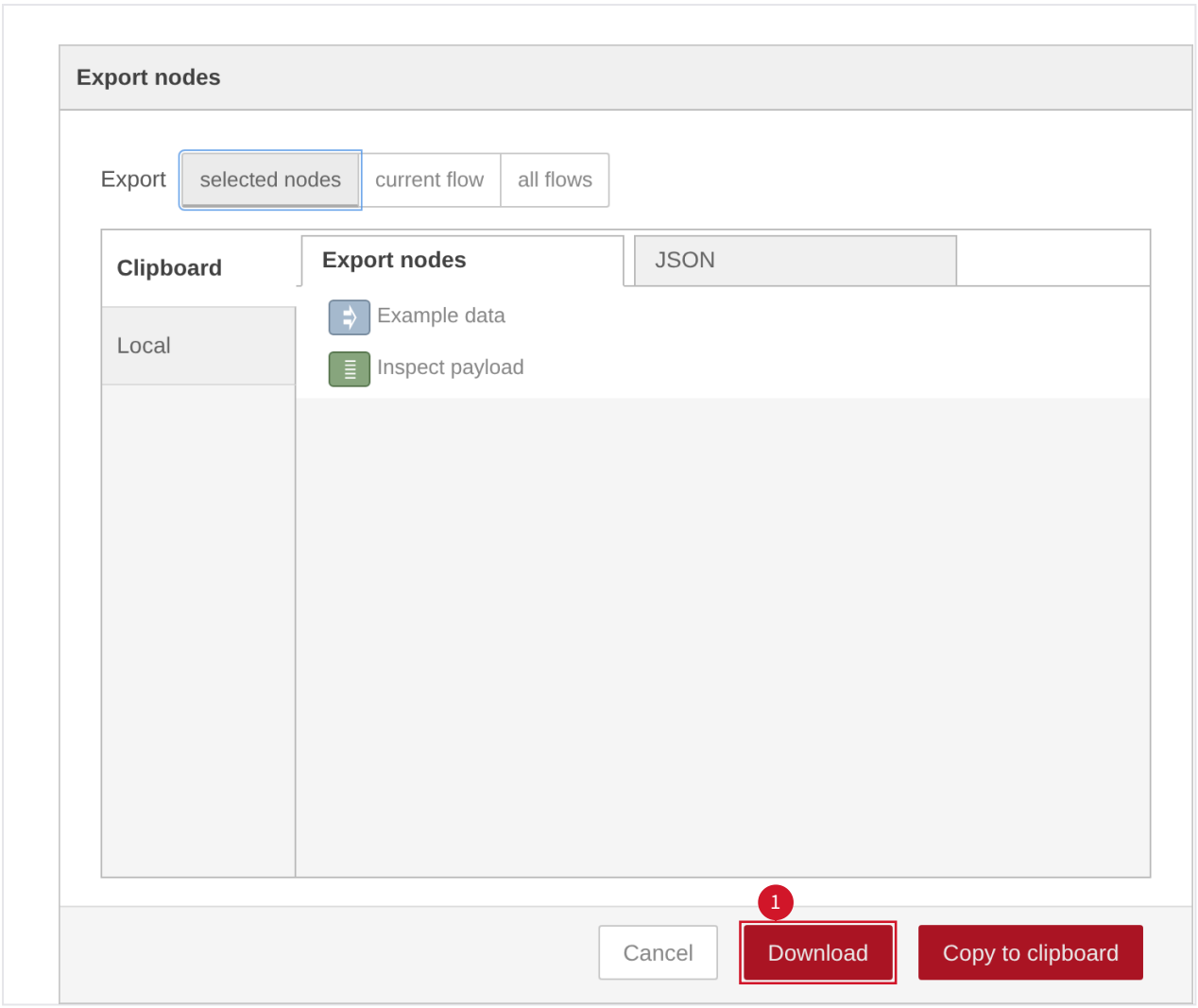


Figure 10-7 Select an export scope and download

1 Check the export scope and download JSON

1. Open the editor menu and select Export.
2. Choose the selected nodes, current flow or all flows. Check names and preview contents.
3. Select Download and save the JSON with its model, date and purpose.
4. To restore, use Import, check missing packages and any credentials that must be re-entered, then deploy after review.

Check the result Exported JSON contains the intended scope and the saved file has a recorded purpose.

10.4 Case: temperature conversion, filtering and MQTT reporting

The included `Node-RED_Temperature_Processing_Example.json` receives Modbus Collect MQTT data for one instrument. It uses core MQTT, JSON and Function nodes; no extra Modbus package, direct serial access or field-write node is required.

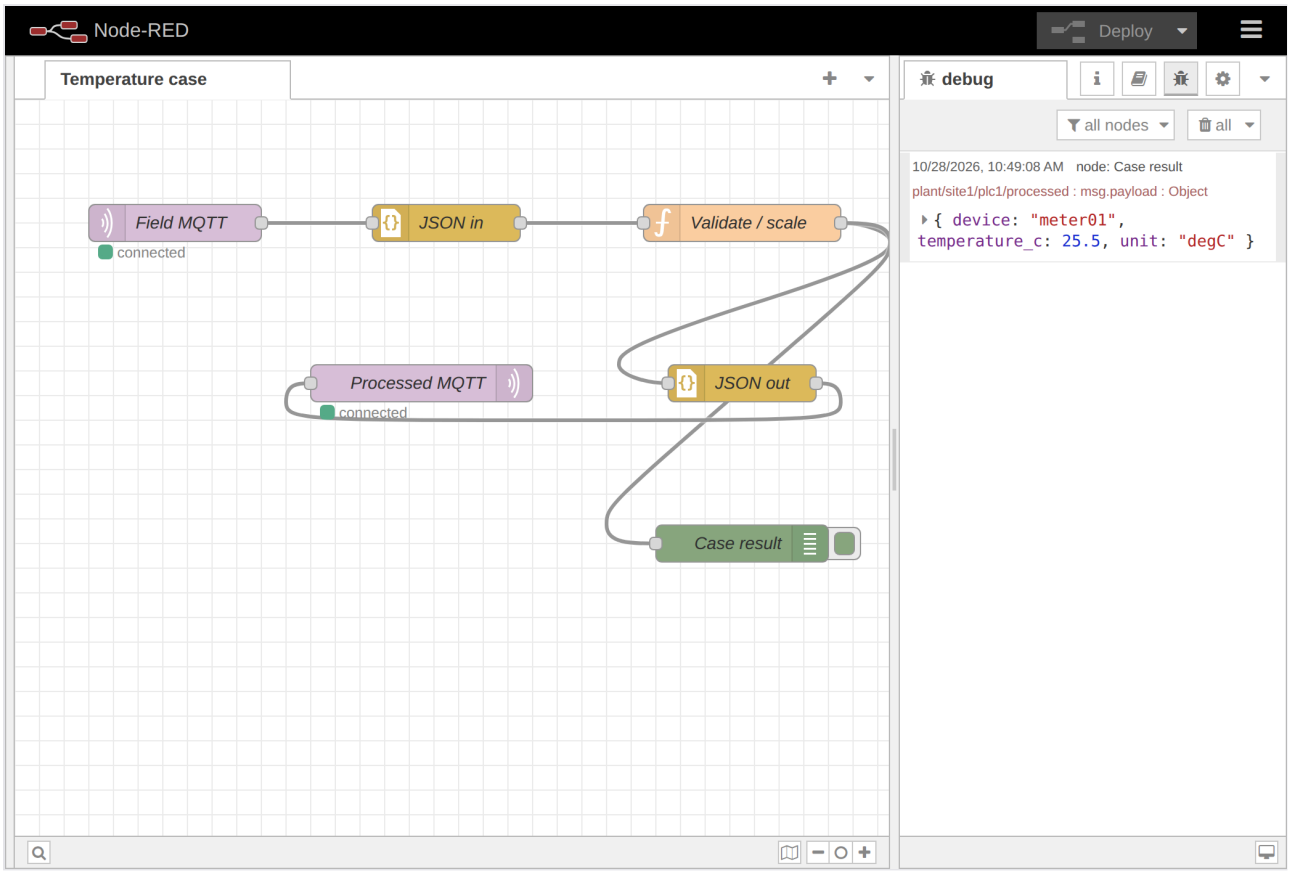


Figure 10-8 Actual temperature-processing flow in the isolated lab

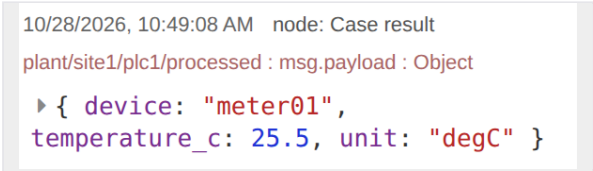


Figure 10-9 Debug output from the same test

FIELD TASK: E1: SCALE RAW255 TO25.5 AND REJECT INVALID VALUES

The supplied field_temperature.json uses standard MQTT/JSON/Function nodes and separate input/output topics. Keep PC bench running and connect no control output.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
MQTT Broker	192.168.10.10:1884 / field / DemoOnly2026	Enter credentials in config node
Input / Output	plant/site1/raw / plant/site1/processed	Avoid feeding output back to input
Function	temperature × 0.1	Accept finite numbers only; separate raw value/unit

SAVE, TEST AND OBSERVE

1. Import/deploy field_temperature.json. Run python site_lab.py watch --topic plant/site1/processed --seconds 60 --expect temperature=25.5.
2. In another window run python site_lab.py publish --topic plant/site1/raw --set temperature=255. Expect temperature=25.5 and unit=C. Publish --payload INVALID next; inspect rejection in Debug with no valid output.
3. To consume M1, change input to plant/site1/plc1/data and extract from its actual payload structure. Inspect Debug first; payload structures vary.

PASS CRITERIA AND DIAGNOSIS

No output: inspect broker/auth/topics/JSON. Tenfold error: inspect duplicate scaling. Debug output alone does not prove republishing; verify the processed subscriber.

Finish and restore: Disable E1 and restore topics/credentials; do not connect its test output to production control.

10.5 Case: multi-point state and alarms

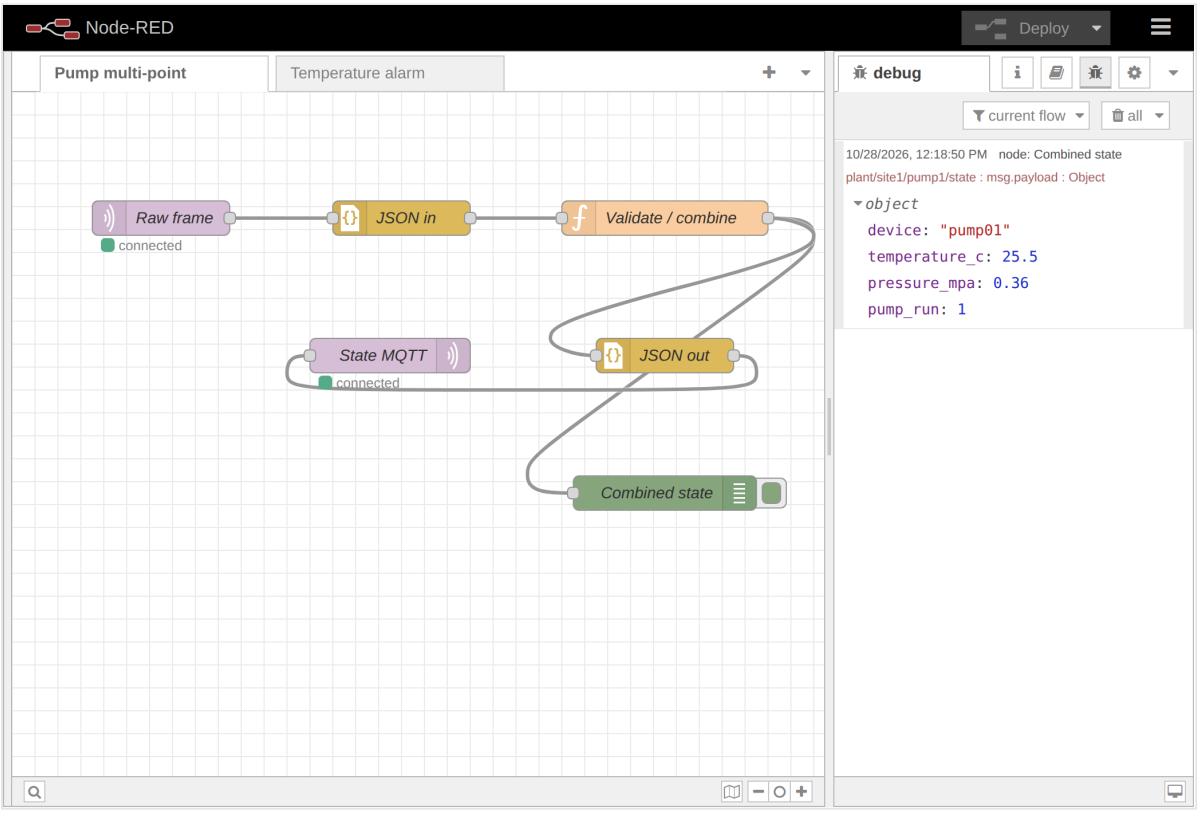


Figure 10-10 Multi-point flow and actual MQTT result (isolated test)

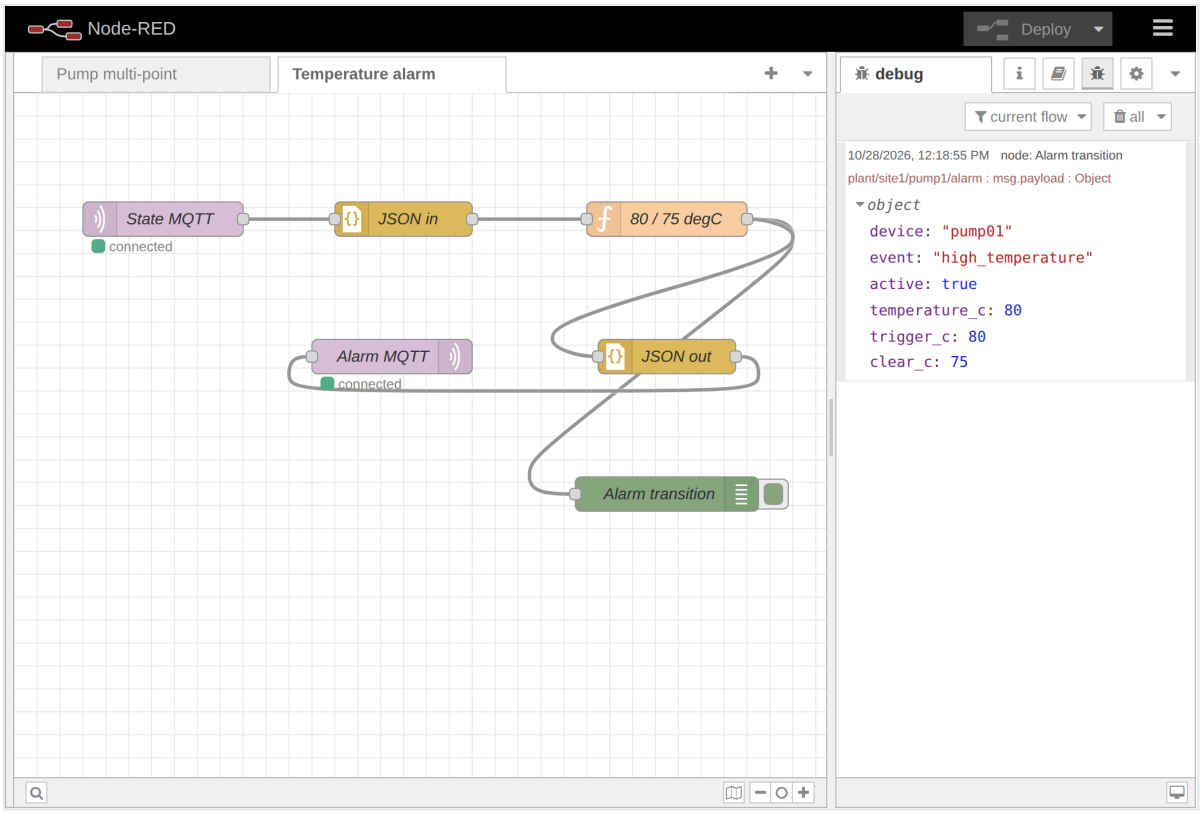


Figure 10-11 Alarm and clear-threshold flow (isolated test)

FIELD TASK: E2: COMBINE POINT STATES AND PUBLISH A SEPARATE ALARM

Import field_alarm.json. This example processes simulated temperature/run state and sends no start/stop commands. Input temperature is already an engineering value; do not scale again.

FIELD ENTRIES (LAB PLAN, NOT FACTORY DEFAULTS)

UI FIELD	ENTRY	BASIS
Input / Output	plant/site1/state / plant/site1/alarm	Separate topics from E1
Condition	temperature > 30 and run = 1	Finite numeric temperature and run0/1
Broker	192.168.10.10:1884 / field / DemoOnly2026	Enter credentials in config node

SAVE, TEST AND OBSERVE

1. Deploy and subscribe to plant/site1/alarm. Run python site_lab.py publish --topic plant/site1/state --json-file alarm_hot.json, or use a MQTT client to send {"temperature":35,"run":1} to plant/site1/state and expect alarm=true.
2. Send {"temperature":25,"run":1} and {"temperature":35,"run":0}; both should produce alarm=false. Missing/string fields should be rejected with a Debug reason.

PASS CRITERIA AND DIAGNOSIS

Repeated alarms: inspect repeated triggering input. This flow outputs state for each valid input; it does not send SMS/email or promise deduplication. Connect a proven notification channel separately.

Finish and restore: Disable E2, restore original output routing and retain valid/invalid test results.

CHAPTER

11

m2mCloud

Connect to the cloud, reach site networks and maintain PLC/HMI programs



YZW1000

11. m2mCloud remote management

11.1 Client configuration and networking

Path Application > M2M Cloud



Verify IP reachability before programming or maintenance

Figure 11-1 Client configuration and networking

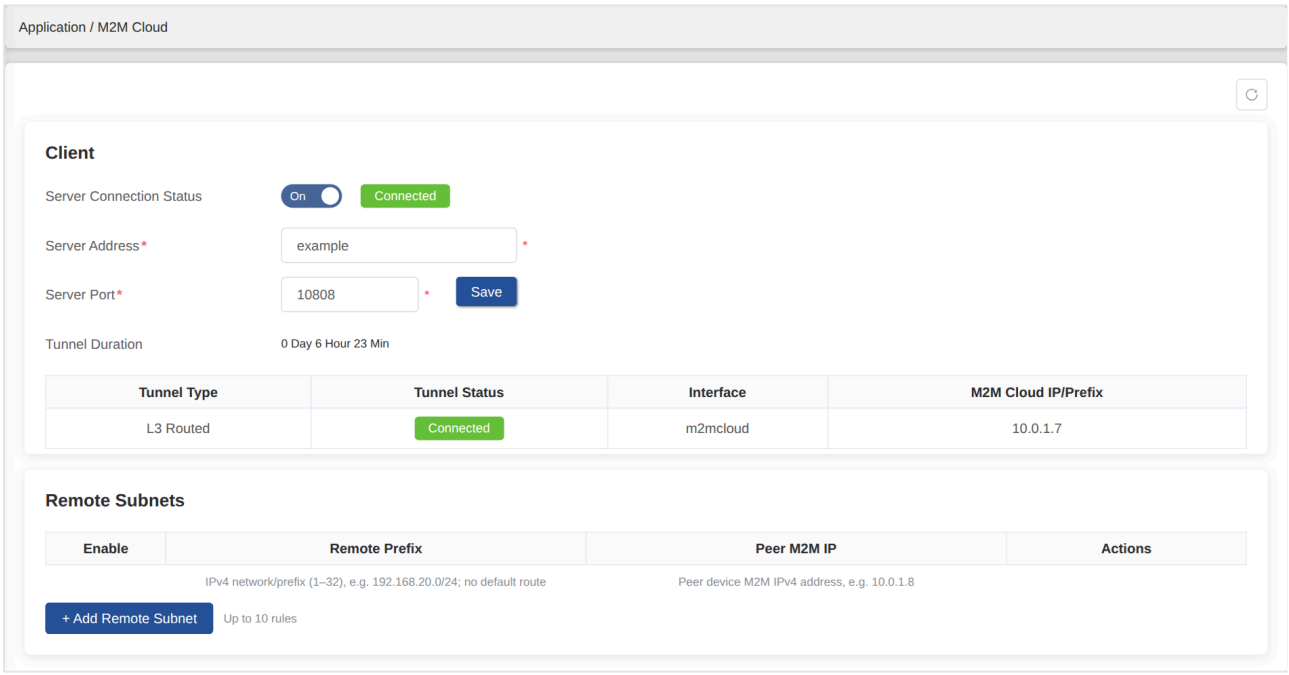


Figure 11-2 Client configuration and networking

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 THESE ITEMS BEFORE FIRST USE

Official site: https://www.edgelor.com/ ; M2M overview: https://www.edgelor.com/m2m/ ; platform sign-in: https://m2m.edgelor.com/ . The sample device list on the overview page does not connect to real devices.

ITEM	SOURCE AND CHECKS
Platform server and CA	Your platform administrator supplies the address, ports and certificates; an example endpoint is not a public service
Account and device authorization	Use the official project route https://www.edgelor.com/project/ or published email zhanghailong@x8link.com to confirm accounts, ownership, permitted network and access scope; self-service registration is not assumed

ITEM	SOURCE AND CHECKS
Matching PC client	Request the compatible installer and release information through https://www.edgelor.com/support/ or the published contact; no verified public client-download link was found in this review. The firmware directory is not a PC-client download page
Business prerequisites	Prepare the PLC model, vendor tool, target IP/port and broadcast requirement; check Windows/Linux feature differences separately

An installer, account, device authorization and service tunnel are separate requirements. Establish local networking while obtaining them; an online device does not establish remote-maintenance permission.

PROCEDURE

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 11.4 Windows client: remote access and 11.5 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 11.4/11.5 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 the result** Router and PC join the authorized network and reach both the field target IP and its service.

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

NO.	FIELD	WHAT TO ENTER / HOW TO USE IT
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

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.

11.2 Remote PLC/HMI program transfer



Verify IP reachability before programming or maintenance

Figure 11-3 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.

11.3 Remote serial access

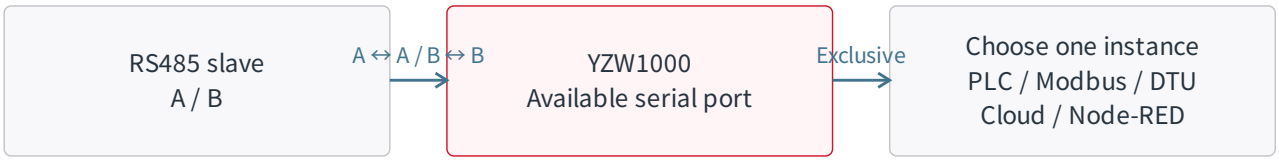


Figure 11-4 Remote serial access

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.

11.4 Windows client: remote access

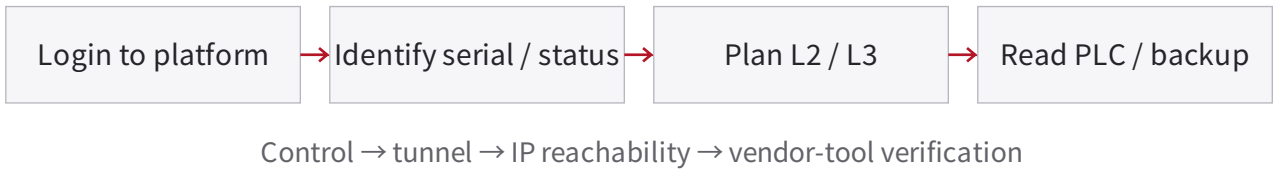


Figure 11-5 Windows: identification to PLC service verification

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.

11.5 Linux client: login and bridge



Control → tunnel → IP reachability → vendor-tool verification

Figure 11-6 Linux: login, inspect, bridge and exit

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

12

Troubleshooting

Check the physical link, network, protocol and service result in order



YZW1000

12. Troubleshooting

12.1 Locate faults along the service path

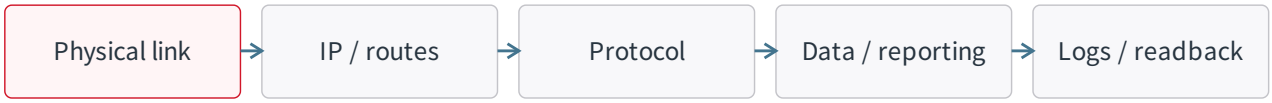


Figure 12-1 Locate faults along the service path

FIND THE NEXT STEP FROM THE SYMPTOM

Find the first failing layer in order and change settings relevant to it. After each change, repeat the same test point.

SYMPTOM	CHECK IN THIS ORDER	PROCEDURE
Management page unavailable	Check that the PC uses a current LAN port and matching subnet. After a layout change or restore, use the management address stored in that configuration	3.1 PC connection and Web login 4.1 WAN settings 9.4 Configuration backup and restore
Address assigned but no Internet	Test the upstream gateway, a permitted external IP, then a name. Prioritize DNS when only names fail	4.1 WAN settings 5.4 Network diagnostics
Failover does not follow the plan	Check actual interface count, Current exit and reason in Link Configuration, then probe targets. WAN need not mean one port, and cellular probe replies do not determine cellular failure	4.7 Link Configuration and failover 4.8 Load balancing
Slave repeatedly times out	Match Serial1/2 to wiring, then check A/B, serial settings, slave address and ownership. For TCP, check IP and service port first	2.6 RS485 wiring and port ownership 5.9 Modbus device connection
Replies arrive but values are wrong	Check address conventions, function, type, byte order and scaling rather than repeatedly changing gateways for a point-decoding problem	5.10 Modbus commands and addressing 5.6 PLC and instrument acquisition
Local acquisition works but cloud data is absent	Check broker connectivity and the effective publish topic, then reporting rule, source and interval. Do not reverse publish and subscribe topics	5.8 Modbus acquisition and reporting 5.7 PLC data reporting

SYMPTOM	CHECK IN THIS ORDER	PROCEDURE
Cloud write has no effect	Identify Modbus Collect versus a PLC reporting rule, verify that module's JSON and target lookup, then inspect post-write readback	5.11 Modbus cloud writes over MQTT 5.12 PLC cloud writes over MQTT
Tunnel online but PLC maintenance fails	From the remote PC, check the field target IP and service, subnet conflicts, return path and authorization, then the vendor tool connection method	11.1 Client configuration and networking 11.2 Remote PLC/HMI program transfer

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.

12.2 Bilingual terms and section mapping

Both editions share section numbers and feature IDs; page numbers may differ. The selection guide lists bilingual page references for key workflows.

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
Powered device (PD)	受电设备	Device receiving PoE power
Power sourcing equipment (PSE)	供电设备	Equipment supplying PoE power

ENGLISH TERM	中文术语	MEANING IN THIS MANUAL
Per-port/total output limit	单口/总输出上限	90 W/port and 720 W total are design limits, not verified continuous ratings; see 4.10
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
Source/identifier	数据源/标识	Point addressing within a PLC reporting rule
Readback verification	读回验证	Later reading compared with field state
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

YZW1000

Site commissioning record

Record actual site values for handover and maintenance. Complete the functions used on this project. Keep passwords and private keys separately.

ITEM	ACTUAL SITE VALUE
Project / location / date	_____ / _____ / _____
Unit ID / firmware	ID: _____ Firmware: _____
Management addressing	LAN: _____ Mask: _____
WAN access	WAN: _____ WAN2: _____
Upstream gateway / DNS	Gateway: _____ DNS: _____
Outbound policy	Combination / priority: _____
Probe targets	Interface and IPv4 / IPv6: _____
Serial1 • external left A/B	Service / slave / serial settings: _____
Serial2 • external right A/B	Service / slave / serial settings: _____
Serial3 • internal PCB	Service / slave / serial settings: _____
Acquisition and cloud	Broker / topics / point-list version: _____
Remote maintenance	Platform network / target / verified service: _____
PoE, when used	52–55 V DC input; supply / confirmed budget / loads: _____
Configuration backup	Filename and location: _____
Actual service check	Test point / readback or service result / date: _____
Maintenance contact	Name / contact details: _____

YZW1000

Service acceptance and handover

Confirm actual services with the site and platform. Retain with the preceding record; identify any untested items and reasons.

CONFIRMATION	PROJECT RECORD
Requirements / success criteria	Service goal, allowed interruption and expected outcome
Existing equipment / systems	PLC/instruments, software/versions, platform and protocol evidence
Selected solution / rationale	Solution, ordered options, topology revision and selection reason
Unmet needs / follow-up	Write None if none; impact, alternative, owner and due date
Platform confirmation	Platform, confirming person, receipt and service time
Verification evidence	Test/result, screenshot or log identifiers and storage
Rollback plan	Trigger, backup file, recovery method and responsible person
Handover / sign-off / date	Installer, site, platform and maintenance confirmation