

VT-LTE500

INDUSTRIAL ROUTER



USER MANUAL

4G Industrial Router

4G

4G LTE Cat-4
150 Mbps downlink

SIM

1 x SIM
External SIM holder

LAN

2 x Gigabit Ethernet
WAN configurable to LAN

IO

2 x RS485
Industrial serial interface

WiFi

2.4 GHz WiFi
AP / STA, up to 50 users

Document version V1.0 · For firmware v3.x and above

www.valtoris.com

CONTENTS

1. Introduction	03	5. VPN	33
1.1 Legal Notice	04	5.1 OpenVPN	34
1.2 Safety and Compliance	04	5.2 L2TP	37
1.3 About This Manual	04	5.3 GRE	38
1.4 Conventions	05	5.4 IPsec	41
1.5 Hardware Overview	05	5.5 PPTP	44
1.6 Hardware Specifications	05	5.6 WireGuard	46
1.7 Symbols Used in This Manual	07	5.7 VXLAN	49
2. Status	09	6. Forward	50
2.1 Overview Dashboard	9	6.1 NAT (DNAT / SNAT / DMZ)	51
2.2 WAN Status	10	6.2 Static Route	53
2.3 LAN Status	11	6.3 MASQ	54
2.4 WiFi Status	12	6.4 QoS	55
2.5 Modem Status	13	7. Firewall	56
2.6 VPN Status	13	7.1 Port & Remote Access	57
2.7 Route Status	14	7.2 SPI Filter	59
2.8 Traffic Statistics	15	7.3 IP Filter	60
3. Network Settings	16	7.4 Domain Filter	61
3.1 WAN	17	8. System Management	62
3.2 LAN	19	8.1 Local Log	63
3.3 WiFi	20	8.2 System Time	64
3.4 Modem (Cellular)	21	8.3 User Account	65
3.5 DHCP Server	23	8.4 Configuration Management	66
4. Application	24	8.5 Firmware Upgrade	67
4.1 ICMP Watchdog	25	9. CFE Recovery Upgrade	68
4.2 DTU (Transparent Transmission)	26	9.1 When to Use CFE Recovery	69
4.3 Modbus Collect	27	9.2 What You Need	69
4.4 Scheduled Tasks (Timer)	28	9.3 Enter CFE Upgrade Mode	69
4.5 Network Diagnostics (Tools)	29	9.4 Web Recovery Upload	70
4.6 SNMP	30	9.5 Verification	70
4.7 m2mCloud (Zero-config Remote Access)	31	9.6 Troubleshooting	70

CHAPTER

01

Introduction

Legal terms, safety requirements, and document conventions.



1. Introduction

“

This first chapter covers the legal terms under which this manual is supplied, the safety statements that must be observed when installing and operating the router, an overview of the device family, and the typographic conventions used throughout the rest of the document.

1.1 Legal Notice

This document and the information it contains are the property of the manufacturer and are supplied to customers and channel partners on the understanding that no part of the document may be copied, redistributed, translated into another language, stored in a retrieval system, or transmitted by any means — electronic, mechanical, or otherwise — without prior written permission of the publisher.

In the interest of continuous product improvement, the manufacturer reserves the right to alter the specifications described in this document, or the device itself, at any time and without prior notice.

All third-party product names, service names, and trademarks referenced in this document are recognised as the property of their respective owners and appear here for identification only.

1.2 Safety and Compliance

No.	Topic	Statement
1.	Read first	Read this manual end-to-end before installing, configuring, or operating the router. Failure to follow the instructions may damage the equipment, degrade service, or void the warranty.
2.	Do not open the enclosure	Operating the device with a cracked or removed cover exposes live circuitry, creates a shock hazard, and voids the warranty. There are no user-serviceable parts inside.
3.	Radio interference	Cellular and Wi-Fi performance depends on the surrounding RF environment. Walls, metal structures, weather, and other transmitters can attenuate or interfere with the signal. Site the antenna and the device accordingly.
4.	Environment	The enclosure is rated for indoor use only and is not sealed against rain, splashing water, or condensing humidity. Mount it in a dry, ventilated location and away from heat sources.
5.	Power supply	Power the device only from the supplied 12 V DC adapter or from a regulated source with the same rated output. Applying a higher voltage or a poorly regulated source will permanently damage the unit and is not covered by the warranty.
6.	Antennas	Use only the antennas supplied with the device or antennas of an equivalent gain and impedance. Always tighten the SMA connectors hand-tight before powering on; loose connectors degrade the link and may damage the RF front-end.

1.3 About This Manual

This manual describes how to install, configure and maintain the **VT-LTE500 4G industrial router**. The router provides a **4G (LTE)-Cat 4** modem, built-in **2.4 GHz Wi-Fi (AP / STA)**, two RJ-45 Gigabit Ethernet ports (1 WAN configurable to LAN + 1 LAN), two RS485 serial ports, one external SIM holder, and DIN-rail mounting. The Web UI can be accessed from any modern web browser by entering the device's LAN IP address.

Two capabilities set the VT-LTE500 apart from a plain cellular router:

- **Edge industrial acquisition** — a built-in Modbus master (TCP + RTU) polls field devices and reports the collected data to an MQTT / TCP / UDP server, and a DTU function transparently bridges serial equipment to the network. No separate gateway or PC is required at the site.

- **Zero-configuration remote access** — **SD-LAN** + **m2mCloud** form a ready-to-use remote environment. Once the SIM is connected and the account is bound, the router and every device behind it become reachable for remote monitoring, remote control and remote program upload / download — with no public IP, port mapping or per-device VPN setup.

This manual focuses on **how to operate the product**: every page in the Web UI is described with its purpose, fields, and a short troubleshooting note. Worked examples follow each major feature so the most common deployments can be reproduced step-by-step without contacting technical support.

i

Who should read this Field engineers installing the router, IT administrators configuring the network, and integrators developing on top of the Web API. Some familiarity with cellular networks (APN, RAT, PCI) and basic Linux network concepts (DHCP, NAT, routing) is assumed.

1.4 Conventions

The text uses the following typographic conventions:

- **Bold** text is a user-interface label, a button, or a key concept.
- `Monospace` text is a literal value, file name, or command.
- *Italic* text is a placeholder you replace with your own value.

1.5 Hardware Overview

The VT-LTE500 is supplied in a compact metal enclosure, designed for cabinet, wall-mount or DIN-rail installation. Connectors and indicators are grouped for simple cable management once the device is fitted into a cabinet or junction box.



Compact metal enclosure, DIN-rail mounted · three SMA antenna connectors (1 × 4G + 1 × WiFi).



Both panels · RS485 terminal (TX/RX/GND/A/B) · LAN/WAN + LAN RJ45 · RST · DC power · antenna ports · status LEDs · SIM.

1.6 Hardware Specifications

The VT-LTE500 is built around a MediaTek industrial-grade SoC and is designed for unattended 24×7 operation. The table below follows the VT-LTE500 datasheet; cellular bands are region specific.

SYSTEM

No.	Item	Specification
1.	Processor	MediaTek MT7621AT
2.	RAM	512 MB DDR3
3.	Flash	16 MB SPI-NOR

No.	Item	Specification
4.	Operating system	OpenWrt-based Linux, kernel 5.4.215; web management out of the box

CELLULAR

No.	Item	Specification
1.	Modem module	4G (LTE)-Cat 4, LTE-FDD maximum downlink 150 Mbps / uplink 50 Mbps, LTE-TDD maximum downlink 130 Mbps / uplink 30 Mbps
2.	SIM slot	1 × SIM slot, 1.8 V / 3 V, external SIM holder
3.	Antenna connectors	1 × SMA for 4G (Main), 1 × SMA for WIFI
4.	Status	Signal strength (RSSI), SINR, RSRP, RSRQ, BAND, IMSI, ICCID
5.	APN / PDP	Auto APN; Custom APN; multiple PDNs for network access and services

WIRELESS

No.	Item	Specification
1.	Wireless mode	2.4 GHz frequency band, IEEE 802.11b/g/n, Access Point (AP), Station (STA)
2.	WiFi security	WPA2-PSK, WPA-PSK; AES, TKIP
3.	SSID	SSID stealth mode
4.	WiFi users	Up to 50 simultaneous connections

WIRED AND SERIAL

No.	Item	Specification
1.	WAN	1 × WAN port (can be configured to LAN), 10/100/1000 Mbps, supports auto MDI/MDIX
2.	LAN	1 × LAN port, 10/100/1000 Mbps, supports auto MDI/MDIX
3.	Serial	2 × RS485

POWER, ENVIRONMENT, MECHANICAL

No.	Item	Specification
1.	Input voltage	9 – 36 V DC, with reverse-polarity protection
2.	Power consumption	< 3 W
3.	DC input connector	12 V industrial DC socket
4.	Operating temperature	–30 °C to +75 °C
5.	Operating humidity	< 95 %, non-condensing
6.	Dimensions (W × H × D)	84.81 × 65.09 × 32.70 mm (housing only, without antennas)
7.	Weight	130 g
8.	Enclosure	Metal casing, DIN-rail mountable (sideways)
9.	Ingress protection	IP30 (indoor use only)

No.	Item	Specification
10.	EMC / safety	EN 301 489 · EN 61000-4-2...-11 · FCC 47 CFR Part 15B

INDICATORS AND BUTTONS

No.	Item	Specification
1.	LED indicators	SYS (power) · Modem NET · Modem SIG · WIFI · WAN/LAN · LAN
2.	Reset button	Recessed; short press = reboot; press-and-hold during power-on = enter CFE recovery (see Chapter 9)

1.7 Symbols Used in This Manual

The following callout symbols mark short pieces of advice that interrupt the main flow of the text:

No.	Symbol	Meaning
1.	 Info	Background or context that helps you understand a feature.
2.	 Tip	An optimisation or shortcut that is not strictly required.
3.	 Note	An important point easy to overlook. Read it.
4.	 Caution	An action that may interrupt service or void support.



CHAPTER

02

Status

Read-only views of link state, addresses, signal strength, and traffic counters.

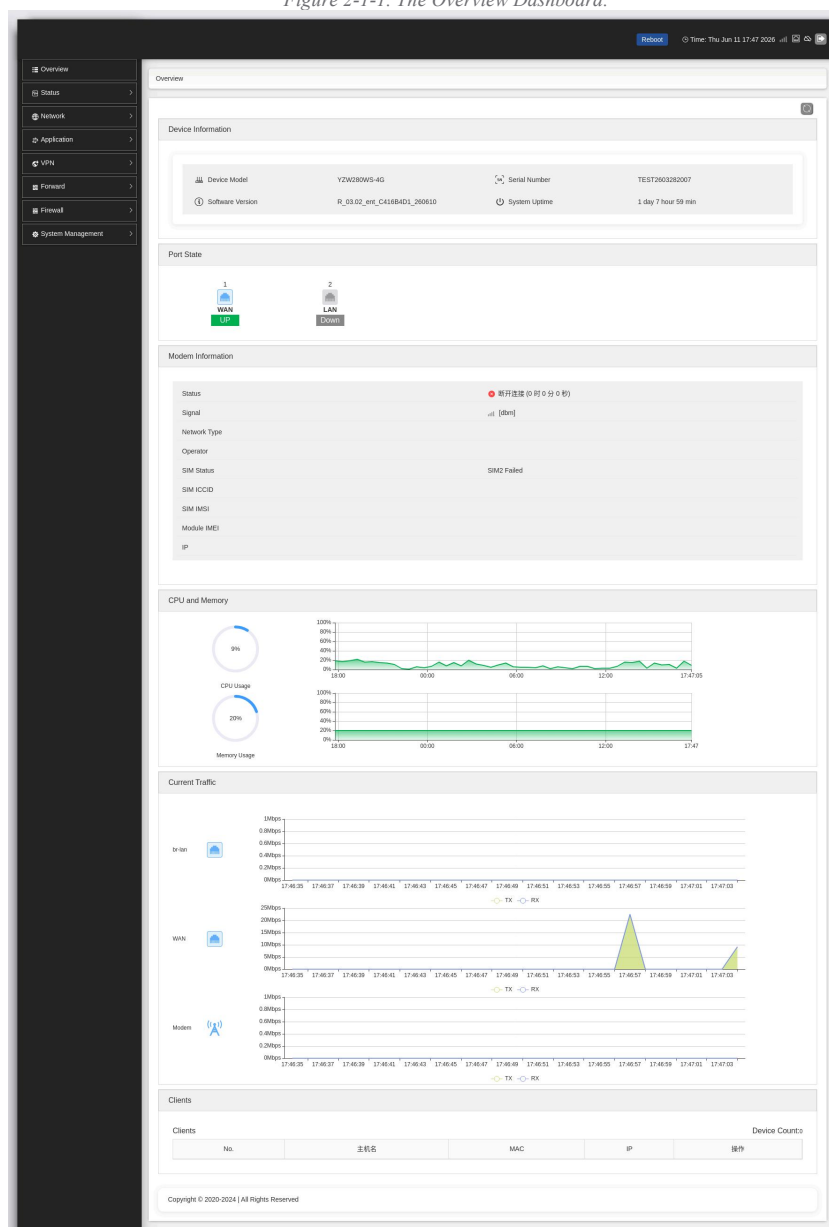


2. Status

2.1 Overview Dashboard

The Overview Dashboard is the landing page after login. It bundles the at-a-glance health of every subsystem on one screen: device identification, port link state, cellular module attach state, CPU / memory utilisation, and a small live traffic chart per interface. Use it as the first stop when triaging an issue — most problems become obvious here before drilling into the detailed Status pages.

Figure 2-1-1. The Overview Dashboard.



WHAT THE WIDGETS SHOW

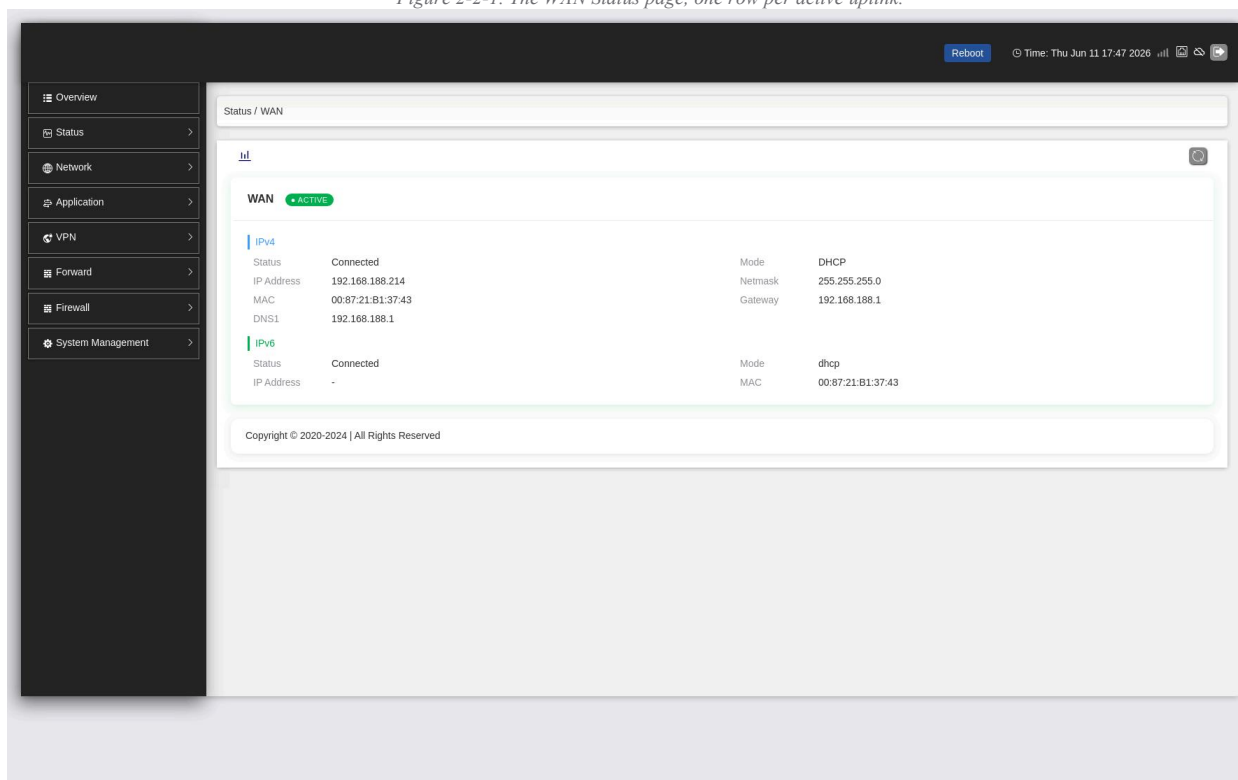
No.	Widget	Meaning
1.	Device Information	Model, serial number, firmware version, and current up-time. Confirms the unit is running the firmware you expect.
2.	Port State	One coloured pill per Ethernet port. Green = link up at the expected speed; grey = no link; amber = link up but mis-negotiated speed (cable / port issue).
3.	Modem Block	SIM signal bars, RAT (LTE), operator name, and PDP state. A red "X" here is the single most common explanation for "no Internet from the LAN side".

No.	Widget	Meaning
4.	Cell Camping Status	Compact view of the serving cell (band, PCI, RSRP / RSRQ / SINR). Equivalent to Status → Modem → Cell Camping (Section 2.5).
5.	CPU and Memory	Sliding window with the last few minutes of utilisation. A sustained spike usually points at a runaway feature (rogue VPN, busy SNMP poller, or a stuck Modbus rule).
6.	Network Traffic	Sparkline per active interface. The fastest visual check that traffic is flowing through the device.

2.2 WAN Status

The WAN Status page lists every interface that has been promoted to a WAN role (one or more wired uplinks, the cellular module, or both). For each WAN it shows the negotiated IPv4 / IPv6 address, the router and DNS the carrier handed out, and whether the link currently passes the keep-alive probe.

Figure 2-2-1. The WAN Status page, one row per active uplink.



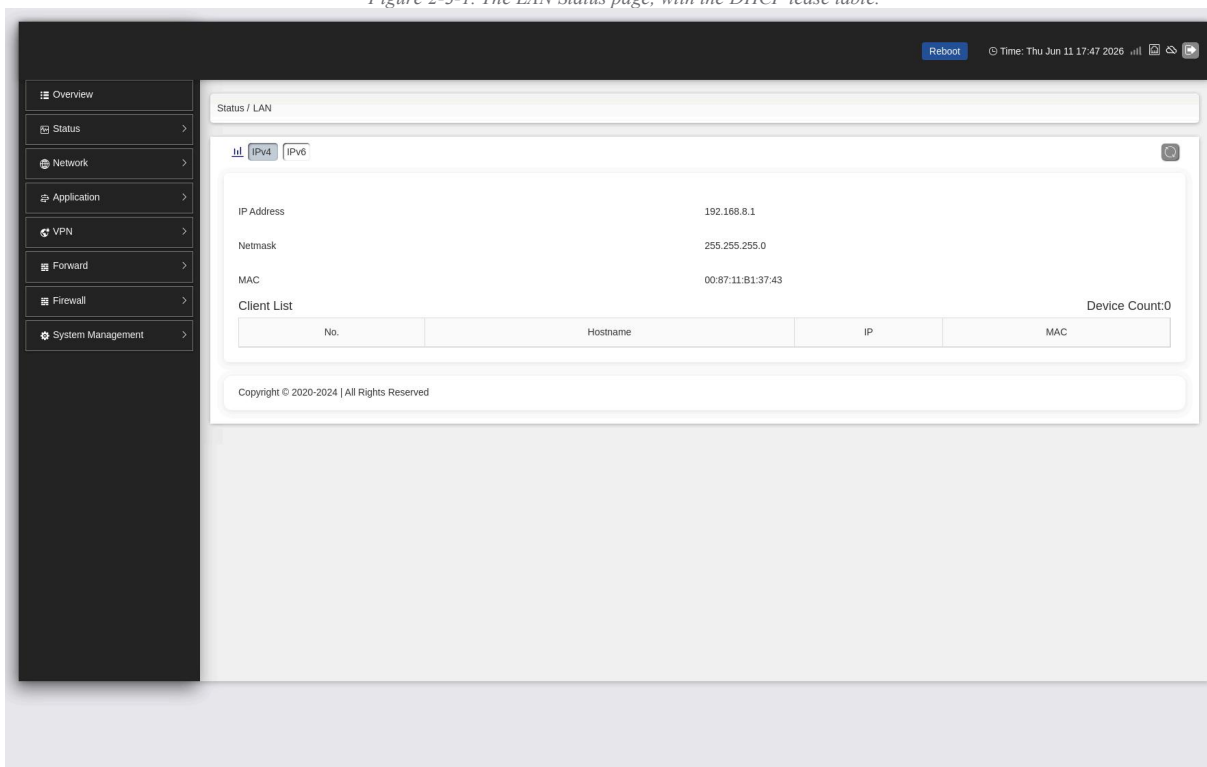
QUICK CHECKS

No.	Symptom	What to look for
1.	LAN clients cannot reach the Internet	Is the WAN's Status column Connected ? If yes but no traffic, check DNS and Gateway values — both must be carrier-provided, not blank.
2.	The expected WAN is missing from the list	The role assignment in Network → WAN (Section 3.1) does not match what you remember; the page only lists interfaces that are currently in the WAN role.
3.	The IPv6 column is blank	IPv6 is not being delegated by the carrier, or IPv6 is disabled in the WAN profile. Most Chinese carriers require an explicit request.

2.3 LAN Status

The LAN Status page shows the current address and netmask of the LAN bridge (`br-lan`) and a live list of DHCP leases the router has handed out. Use it to confirm a client device received the address you expect, to find the MAC address of an unknown LAN device, or to spot a duplicate-IP situation.

Figure 2-3-1. The LAN Status page, with the DHCP lease table.



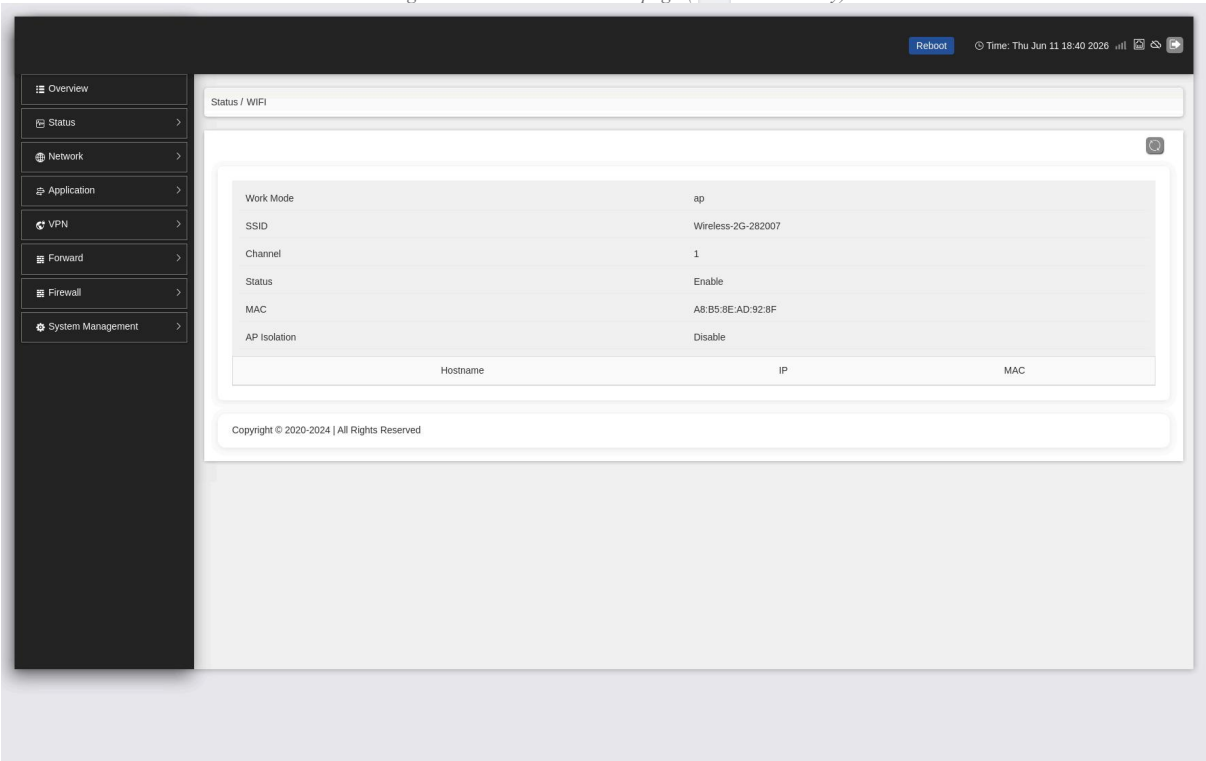
FIELDS IN THE LEASE TABLE

No.	Field	Meaning
1.	Hostname	The client's reported hostname (when DHCP option 12 was offered).
2.	MAC address	The client's Ethernet / WiFi MAC. Useful for matching against a serial-number label.
3.	IP address	The IPv4 address currently leased to the client.
4.	Remaining lease	Time until the lease expires. A constantly-near-expiry value usually means the client is renewing aggressively, which is normal.

2.4 WiFi Status

The WiFi Status page shows the running state of the 2.4 GHz radio. For each radio you see the operating channel, country code, transmit power, and the list of currently associated stations along with their signal strength and link rate.

Figure 2-4-1. The WiFi Status page (w variants only).



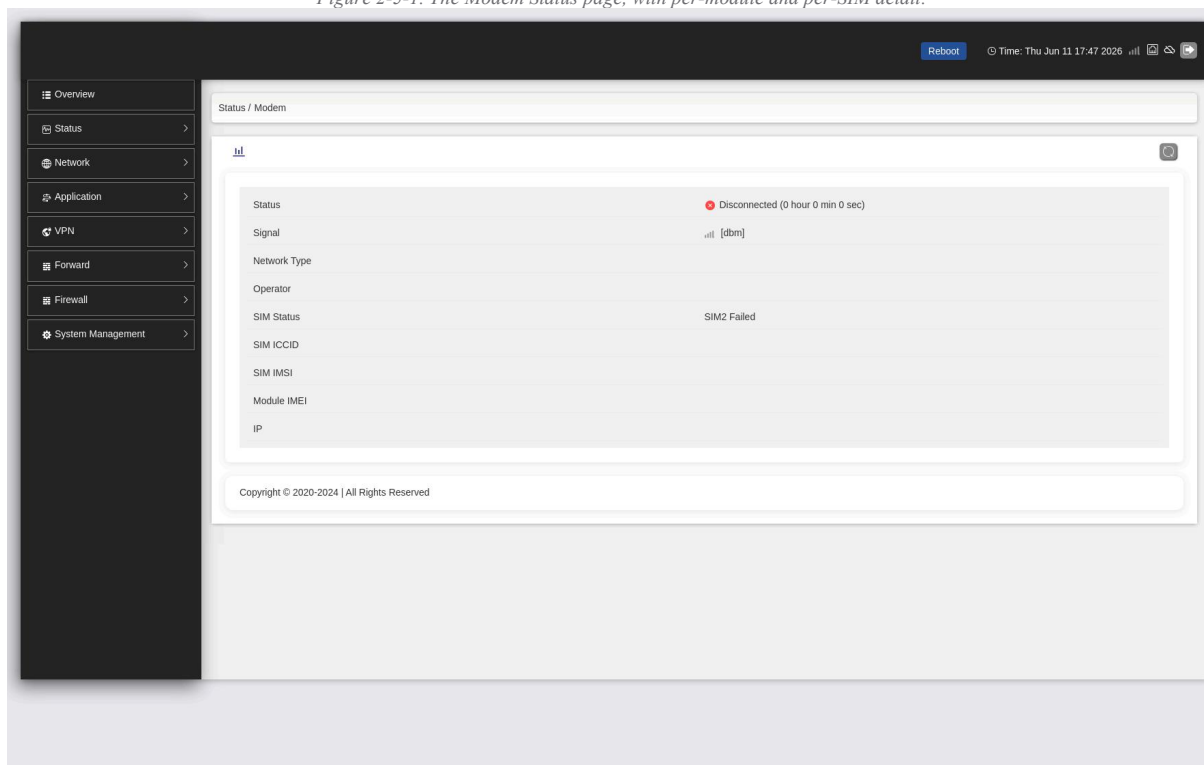
QUICK CHECKS

No.	Situation	Where to look
1	A client keeps disconnecting	Check RSSI in the station list. Below -75 dBm is borderline; below -80 dBm clients will reconnect frequently.

2.5 Modem Status

The Modem Status page is the source of truth for everything related to the cellular module: SIM detection, registration, attach state, the serving cell, and the running PDP context. It is the page you open when the LAN side reports "no Internet via cellular" — most cellular issues become visible here before any other page.

Figure 2-5-1. The Modem Status page, with per-module and per-SIM detail.



2.6 VPN Status

This page summarises every VPN tunnel that has been configured under **VPN** (Chapter 5) and is currently allowed to run. Use it as the single source of truth when verifying that a freshly-configured tunnel actually came up, when triaging an outage from the LAN side, or when confirming which peer the router is connected to.

i

Empty page = no active tunnels. If no VPN profile has been added or every profile is disabled, this page is deliberately blank. The presence of a row therefore means at least one VPN service is enabled and the daemon has started — it does **not** by itself prove the remote peer is reachable; check the **Status** column.

FIELDS TYPICALLY SHOWN PER TUNNEL

No.	Field	Meaning
1.	Type	The tunnel protocol: OpenVPN , L2TP , IPsec , WireGuard , GRE , PPTP .
2.	Name / Profile	The profile name you assigned when creating the tunnel. Helps when the same protocol is used for several peers.
3.	Status	Connected / Connecting / Disconnected / Error . Most issues fall into one of these four; see Section 5.x of the matching protocol chapter for the cause table.
4.	Local IP	The address the router took on the tunnel interface (often a private overlay address).
5.	Remote IP	The peer's tunnel address, or the server address for client-mode profiles.
6.	Up-time	How long the tunnel has been continuously connected. A constantly-low value usually means the link is flapping — re-check authentication and routing.

QUICK CHECKS

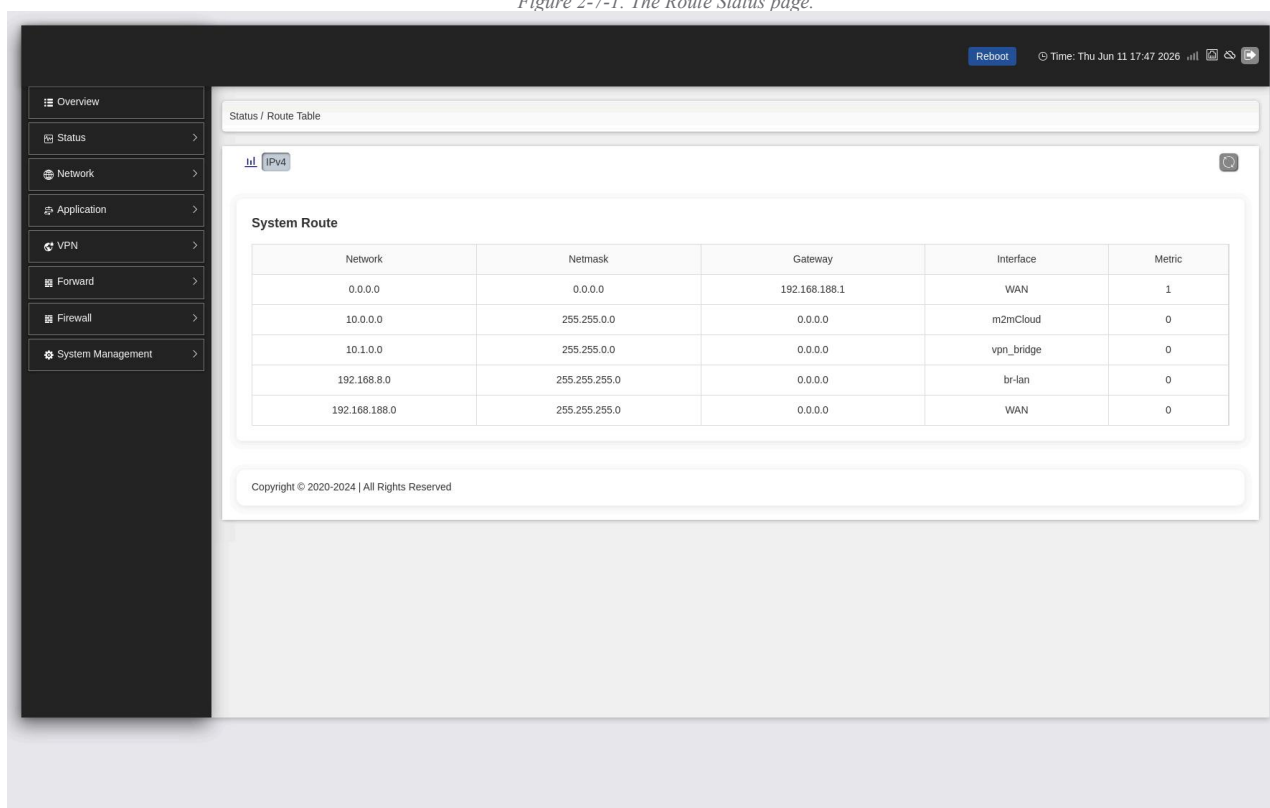
1. If a tunnel shows **Disconnected** while you expected it to be up, open the matching profile in Chapter 5 and re-save — the daemon picks up the change in a few seconds.

- If a tunnel shows **Connected** but LAN clients still cannot reach the remote subnet, verify that **Forward** → **Static Route** (Section 6.2) has a route pointing at the tunnel interface for that subnet.
- For IPsec, the status here only reflects the IKE / child-SA state seen by the router; the remote peer's view may differ. If both ends show "Connected" and traffic still does not flow, suspect a mismatched proposal or a missing firewall allow rule on the far side.

2.7 Route Status

The Route Status page is the kernel's IPv4 / IPv6 routing table, rendered as a sortable list. Use it to confirm that a route you configured (in **Forward** → **Static Route**, Section 6.2) actually landed in the kernel, to find which interface a particular destination would exit through, and to spot a default route that points at the wrong WAN after a fail-over.

Figure 2-7-1. The Route Status page.



FIELDS PER ROUTE

No.	Field	Meaning
1.	Destination	The subnet a packet must match to take this route. <code>0.0.0.0/0</code> is the default route.
2.	Gateway	The next hop. * (or blank) means the route is on-link — no next hop, the destination is directly reachable on the listed interface.
3.	Interface	Which interface the packet leaves through. <code>br-lan</code> for LAN, <code>eth0</code> for WAN, <code>ppp0</code> / <code>usb0</code> for cellular, a tunnel name for VPN.
4.	Metric	When multiple routes match, the lower-metric one wins. Useful to confirm WAN-failover ordering.

2.8 Traffic Statistics

This page shows cumulative byte and packet counters for every active network interface on the router. Use it to confirm that the link you expect to be carrying traffic actually is, to spot an interface that is silently dropping, and to compare carrier-billed usage against what the router has seen on its WAN.

i

Counters are reset on reboot. A freshly-restarted router will show zeros for every interface until traffic begins to flow. The counters are not persisted across reboots; if you need long-term accounting, export the values via the management API or use an external collector (SNMP — Section 4.6).

FIELDS TYPICALLY SHOWN PER INTERFACE

No.	Field	Meaning
1.	Interface	Internal name such as <code>eth0</code> (WAN), <code>br-lan</code> (LAN bridge), <code>usb0</code> / <code>ppp0</code> (cellular), or a VPN tunnel name.
2.	RX bytes / packets	Cumulative traffic the interface has received since boot.
3.	TX bytes / packets	Cumulative traffic the interface has transmitted since boot.
4.	Errors	Bad frames the driver could not process. A non-zero value rising slowly is usually noise; a fast climb points to a cable, antenna, or carrier issue.
5.	Dropped	Packets the kernel had to discard, typically because a queue was full. Sustained drops on the WAN side usually indicate that QoS (Section 6.4) is mis-sized for the link.

QUICK CHECKS

1. If the **RX** / **TX** counters on the WAN interface are not climbing while you know traffic is flowing through the router, the path is not using that interface — check the routing table (Section 2.7).
2. A large gap between LAN-side **TX** and WAN-side **RX** is normal because of internal processing, NAT, and packet aggregation. A *persistent* discrepancy of one order of magnitude usually indicates an asymmetric routing problem.
3. The cellular interface's counters can be reconciled with the carrier's billing data; minor variance (5-10 %) is normal because the carrier counts at a different layer.



CHAPTER

03

Network Settings

Bring up wired, wireless and cellular uplinks; manage IP addressing and DHCP.

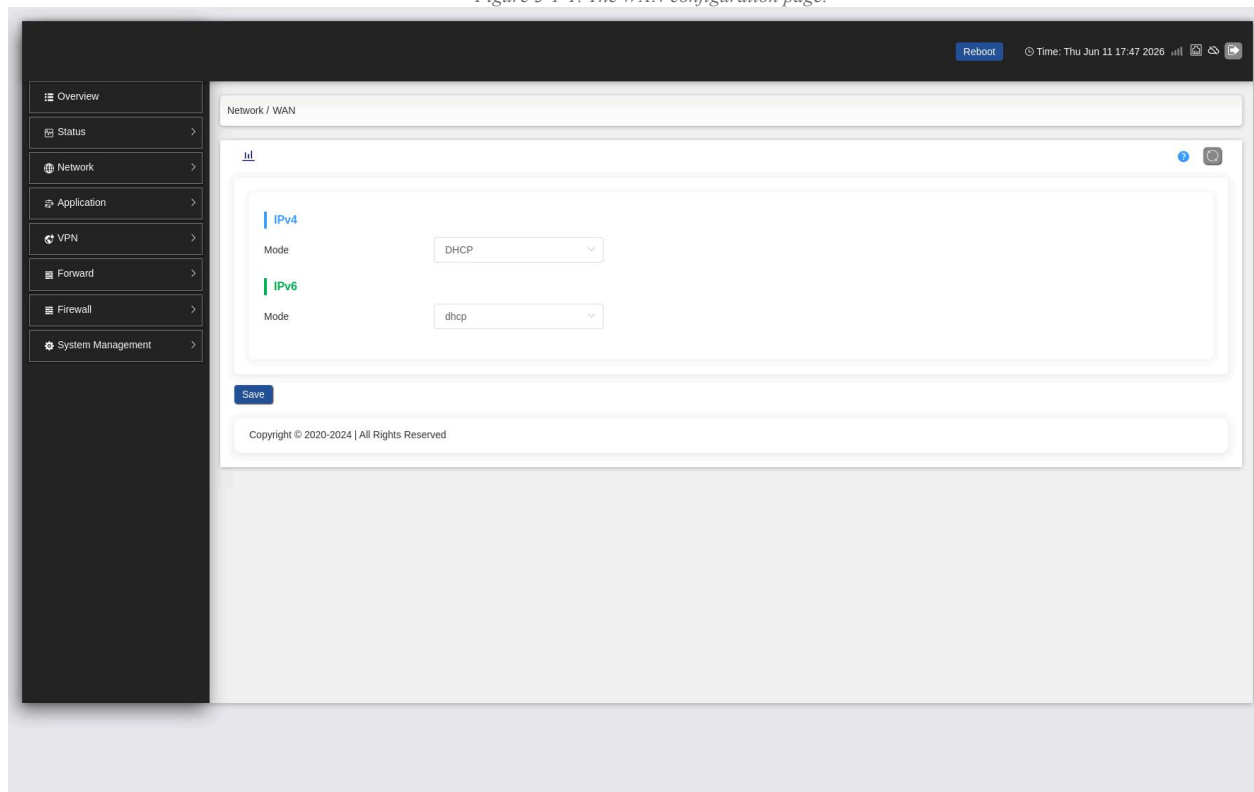


3. Network Settings

▶ 3.1 WAN

This is where you tell the router how the **wired** uplink connects to the Internet. You only need this page when you have an Ethernet cable going into the WAN port (from a broadband modem, a fibre router, or your office switch). If your only uplink is the cellular SIM, skip ahead to Section 3.4 Modem.

Figure 3-1-1. The WAN configuration page.



HOW TO: CONNECT THE ROUTER BEHIND AN EXISTING ROUTER OR BROADBAND MODEM

This is the most common case — you already have a router or a fibre / cable modem that hands out addresses on its LAN side, and you want the VT-LTE500 to sit behind it.

1. Plug the cable from the upstream router into the router's **WAN** port.
2. **Network** → **WAN** → set **Mode** to `DHCP`. (This is the factory default, so usually no change needed.)
3. **Save**. Within a few seconds the device asks the upstream router for an address.
4. Verify on **Status** → **WAN** (Section 2.2): the row for the wired WAN should show a non-empty IP address and the **Status** column should read `Connected`.

HOW TO: USE A STATIC IP GIVEN TO YOU BY YOUR ISP OR IT ADMIN

1. **Network** → **WAN** → set **Mode** to `Static IP`.
2. Fill in the four fields exactly as the supplier wrote them: **IP**, **Subnet mask**, **Gateway**, **DNS1** (and optionally **DNS2**).
3. **Save**. Verify on **Status** → **WAN**.

Important: the WAN IP must not be in the same subnet as any LAN port. If the LAN side is `192.168.1.0/24`, the WAN must be on a different subnet, otherwise the router will not know which interface to send each packet through.

HOW TO: CONNECT A PPPOE BROADBAND LINE (CHINESE / EUROPEAN TELECOMS)

1. **Network** → **WAN** → set **Mode** to `PPPoE`.
2. Fill in **Username** and **Password** — these come from your broadband ISP. They are usually printed on the welcome letter or available in the customer portal.

3. Leave the **Auth** field at the default (`CHAP/PAP auto`). Change it only when the ISP explicitly tells you a specific mode.
4. **Save**. The device dials within ~10 seconds. Verify on **Status** → **WAN**.

HOW TO: TURN A WIRED PORT INTO A LAN PORT (MULTI- PORT MODELS)

1. **Network** → **WAN** → at the top, change the **WAN Layout** selector from e.g. `1 WAN + 1 LAN` to `2 LAN` .
2. **Save**. The previously-WAN port immediately starts acting as a LAN port and clients plugged into it pick up addresses from the LAN DHCP server (Section 3.5).

FIELD REFERENCE

No.	Field	What to put there
1.	Mode	The most common choice is <code>DHCP</code> (router gets IP from the upstream automatically). Other choices: <code>Static IP</code> (manually filled), <code>PPPoE</code> (broadband dial-up), <code>LAN</code> (turn this port into LAN).
2.	IP / Subnet / Gateway / DNS1 / DNS2	Only visible in <code>Static IP</code> mode. Use exactly the values the ISP / IT admin supplied.
3.	Username / Password	Only visible in <code>PPPoE</code> mode. Come from the broadband ISP.
4.	MTU / MRU / MSS	Advanced. Leave at defaults unless a specific carrier instruction tells you to change them.
5.	IPv6	A separate section on the same page. Configure exactly the same way as IPv4 (<code>DHCP</code> / <code>Static</code> / <code>PPPoE</code>). Most ISPs leave this off — only enable when the carrier specifically supports IPv6.
6.	WAN Layout (multi-port models)	Decides the role split of the physical ports, e.g. <code>1 WAN + 1 LAN</code> or <code>2 LAN</code> .

i

NAT is always on for WAN. The router automatically translates LAN-side private addresses into the WAN-side address — there is no switch to disable it. If you need pure routing without NAT (rare, advanced deployments), contact your distributor.

IPv6: configured the same way as IPv4 (DHCP/Static/PPPoE), available only when the port acts as WAN.

3.2 LAN

LAN is the internal-network interface of the device. This page sets the LAN IP address, which is both the router of the internal subnet and the address used to reach this management page.

Figure 3-2-1. The LAN configuration page.

Reboot Time: Thu Jun 11 17:47 2026

Network / LAN

IPv4

IP Address	Netmask
IP1 192.168.8.1	255.255.255.0 / 24
IP2	Select /
IP3	Select /

Save

Copyright © 2020-2024 | All Rights Reserved

OVERVIEW

A primary LAN IP plus up to 2 secondary IPs can be configured, so the device can sit on several internal subnets at once.

IPv4 / IPv6 are switched by the tabs at the top (the IPv6 tab depends on the model and configuration).

The LAN DHCP service is on by default and assigns addresses to internal devices automatically.

PARAMETERS

IP address: the IP of the LAN interface. IP1 is the primary address (required) and is also the address of this management page; IP2 and IP3 are optional secondary addresses that place the device on additional internal subnets.

Subnet mask: the mask for each LAN IP, determining the size of that subnet (/16 to /30 available).

Note: a LAN IP must not share a subnet with the WAN, and the LAN IPs must not share subnets with each other; after changing the primary IP (IP1) and saving, the management address changes accordingly and the browser is redirected to the new address.

3.3 WiFi

On **W** variants the router carries a 2.4 GHz radio and this page configures it. The radio can operate as an access point for LAN clients, or be switched off entirely; SSID, channel, and security are configurable.

Figure 3-3-1. The WiFi configuration page (**W** variants).

Network / WiFi

Reboot Time: Thu Jun 11 18:40 2026

On

Basic Setting

Mode AP

Frequency 2.4

Wireless Mode 802.11n

Channel Width 20MHz

Channel auto

Isolate ☐

* SSID Wireless-2G-282007 18/32

Security Mode WPA2

* Cipher AES

* Password *****

* Re-key Interval(s) 86400

Hide ☐

Save

Copyright © 2020-2024 | All Rights Reserved

OVERVIEW

The WiFi service is bridged to the LAN by default, so any client that associates and authenticates obtains a LAN IP through the DHCP server (Section 3.5).

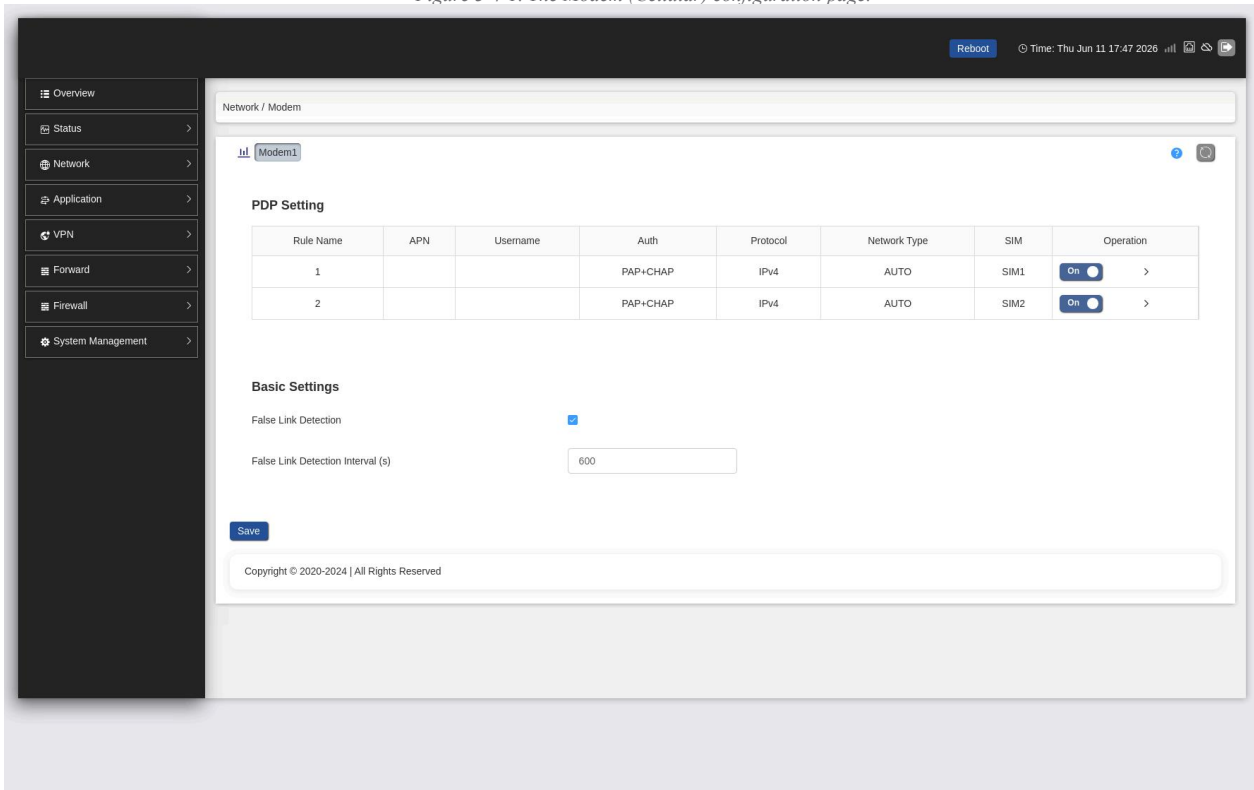
PARAMETERS

No.	Field	Meaning
1.	Status	Master switch for the radio. Off shuts down the transmit chain and saves a small amount of power.
2.	SSID	The network name broadcast by the radio. Up to 32 ASCII characters; avoid non-ASCII names for legacy-client compatibility.
3.	Hidden SSID	When on, the beacon does not include the name and clients must know it in advance. Hiding the SSID is not a security measure.
4.	Channel	Auto lets the driver pick a clear channel at boot; pin a value when the RF environment is known or when clients refuse to roam between channels.
5.	Country code	Determines the legal channel set and maximum transmit power. Must match the region of deployment.
6.	Security mode	Open / WPA2-PSK / WPA3-PSK / WPA2/WPA3 mixed . WPA3 is recommended for new deployments; WPA2 stays for legacy clients.
7.	Pre-shared key	The password clients use to associate. 8 - 63 ASCII characters.
8.	Maximum clients	Caps the number of associated stations. Useful in public-area deployments to keep one runaway crowd from degrading service for everyone.

3.4 Modem (Cellular)

This page is where you tell the router *how* to use the SIM card you inserted, so that the LAN side gets Internet through the cellular network. **In most cases the defaults are good enough — insert a SIM, save the page once, and the device dials up by itself within a minute.** You only need to change something on this page when the carrier gave you a custom APN, when you want to lock to a 4G band, or when you need to lock to a specific base station.

Figure 3-4-1. The Modem (Cellular) configuration page.



HOW TO: BRING THE CELLULAR LINK ONLINE FOR THE FIRST TIME

This walk-through assumes you have a single SIM card and the carrier does **not** require a custom APN (true for over 90 % of consumer / IoT SIMs worldwide).

1. **Power the device off**, slide the SIM card into **SIM 1** with the gold contacts facing down, push until it clicks.
2. **Power the device back on**. Wait about 60 seconds for the cellular module to register on the network.
3. Open the Web UI, go to **Network** → **Modem**. Confirm that the first row in the table is **On** (the master switch on the right of the row). If it is off, switch it on and click **Save**.
4. Open **Status** → **Modem** (Section 2.5). Within a few seconds you should see:
5. **Status:** `Connected`, with an up-time counting up.
6. **Signal:** a non-zero CSQ value (anything above 10 is workable; above 20 is good).
7. **IP:** a non-empty IPv4 address — that's the address the carrier gave you.
8. From a LAN client, open any website. Internet should work. **You are done.**

If the **Status** column stays `Disconnected` for more than two minutes, jump to **Troubleshooting** at the end of this section.

HOW TO: USE A NON- DEFAULT APN (PRIVATE / INDUSTRIAL SIM)

Some industrial SIMs, MVNO SIMs, and corporate SIMs require an APN that is not in the device's auto-detect list. Symptoms: the module registers on the network (Signal is non-zero) but never reaches `Connected`.

1. Get the APN, optional username, and optional password from your SIM supplier — usually printed on the welcome letter or available on the supplier's portal.
2. **Network** → **Modem** → expand the first row.
3. Fill in **APN**, **Username**, **Password** with the values the supplier gave you. Leave **Auth** at its default unless the supplier specified otherwise.

4. **Save.** The module reconnects within 30 seconds; verify on **Status → Modem**.

HOW TO: LOCK TO A 4 G BAND

The module selects the available 4G band automatically. Lock to one band only when the automatic selection keeps choosing a weak or congested band.

1. **Network → Modem** → expand the first row.
2. Set **Network Type** to **4G** and choose the required band under **Lock Band**.
3. **Save.** The module re-registers within ~15 seconds.

FIELD REFERENCE — PROFILE IDENTITY AND AUTHENTICATION

No.	Field	What to put there
1.	Rule Name	A short label that shows up in logs. The default default works for most people.
2.	APN	Leave blank unless the carrier told you otherwise. The device tries the carrier's known APN automatically when this is blank.
3.	Username / Password	Blank for the vast majority of SIMs. Fill in only when the SIM supplier explicitly says so.
4.	PIN	Blank unless the SIM has a PIN lock active. Locked SIMs without a PIN here will never connect.
5.	Auth	PAP+CHAP works for all carriers and is the default. Change only when explicitly told to.

FIELD REFERENCE — RADIO AND SIM BEHAVIOUR

No.	Field	What to put there
6.	Protocol	IPv4 is the right choice for 99 % of deployments. IPv4v6 if you really need IPv6 from the cellular side and the carrier supports it.
7.	Network Type	AUTO lets the module pick the available 4G network automatically. Lock to 4G only when you have a specific reason.
8.	SIM	The physical SIM slot used by this profile.
9.	Lock Band	Restrict the module to one or more cellular bands. Useful when you want to avoid a band that has bad coverage at your site. Leave empty to let the carrier pick.
10.	Operation	The master switch for the row. The first row with this set to On is the active profile.

TROUBLESHOOTING

No.	Symptom	Most likely cause	What to do
1.	Status stays Disconnected indefinitely.	SIM is not seated correctly, or the carrier requires a custom APN.	Power off, re-seat the SIM, power on, wait 60 s. If still no good, see "use a non-default APN" above.
2.	Status flips Connected / Disconnected every few seconds.	Wrong APN, or fail-over policy is alternating between two SIMs.	Set the APN explicitly. Disable the secondary SIM row to isolate.
3.	Signal is 0 or blank.	No usable cellular signal at the antenna.	Check the antenna is screwed in, move to a window, or fit an external high-gain antenna.
4.	Status is Connected but LAN clients have no Internet.	The carrier APN may be whitelist-only; or the router's WAN-side firewall blocks LAN→WAN.	Verify with ping 1.1.1.1 from a LAN client. Check Forward → NAT is enabled for the cellular interface.
5.	The signal value shown on Status is good but speed is poor.	The module is camping on a weak / congested cell even though the band itself is fine.	Use Lock Band or the advanced Lock Cell feature to pin the module to a known good cell.

3.5 DHCP Server

The router runs a DHCP server on the LAN bridge so that wired and wireless clients obtain an IPv4 address automatically. This page tunes that server: the lease range, the per-host static-binding table, the default gateway and DNS handed out, and the lease duration.

Figure 3-5-1. The DHCP Server configuration page.

The screenshot displays the DHCP Server configuration page. On the left is a sidebar menu with options: Overview, Status, Network, Application, VPN, Forward, Firewall, and System Management. The main content area is titled 'Network / DHCP' and has tabs for IPv4 and IPv6. The IPv4 tab is active. Settings include: IP Pool (default), Lease Time (86400), Gateway Type (default), DNS Type (default), and Network Port Compatibility (Off). Below these is a 'MAC Address Binding' section with a table with columns: No., IP, MAC, and Operation. A 'Save' button is located below the table. The footer of the page reads 'Copyright © 2020-2024 | All Rights Reserved'.

OVERVIEW

The DHCP service is enabled by default. The lease range must be a subset of the LAN subnet defined in Section 3.2; any address outside the lease range is treated as reserved for static assignment. Static bindings (MAC → IP) survive a reboot and are honoured even when the requesting client identifies under a different hostname.

PARAMETERS

No.	Field	Meaning
1.	Status	Master switch for the DHCP server. Off forces every LAN client to be statically configured — useful only in tightly-controlled industrial deployments.
2.	Lease range start / end	The first and last address the server will hand out. Must be inside the LAN subnet and must not overlap any static binding.
3.	Default gateway	The address sent in DHCP option 3. Defaults to the LAN IP of the router itself — change only when the LAN has a different upstream router.
4.	DNS servers	Up to two DNS addresses sent in DHCP option 6. Empty values fall back to the WAN-supplied DNS.
5.	Lease time	Validity of each lease in seconds (120 - 86400). Short leases reclaim addresses faster; long leases reduce DHCP traffic on busy LANs.
6.	Static binding table	One row per reserved client: MAC address, IP, optional hostname. Bindings outside the lease range are stable; bindings inside the range pre-empt regular allocation.



Why a host sometimes gets the "wrong" address. A client that previously held a lease will try to renew it before requesting a new one. If the lease is still valid on the server side, it is renewed even when a static binding has been added in the meantime. Either wait for the lease to expire, or restart the client's network stack to force a fresh `DHCPDISCOVER`.

CHAPTER

04

Application

Edge Modbus acquisition,
DTU transparent
transmission, zero-config
remote access, automation,
and diagnostic utilities.

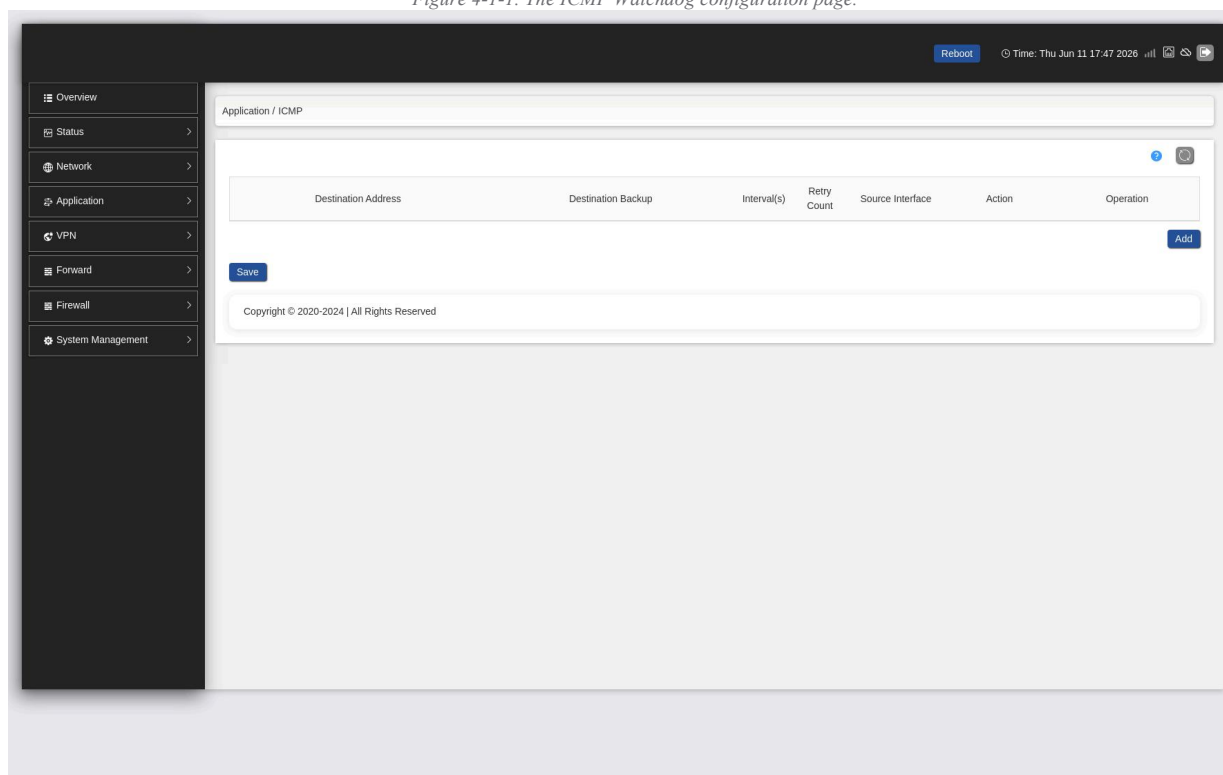


4. Application

▶ 4.1 ICMP Watchdog

ICMP link detection monitors whether a link is healthy by periodically pinging a target address. When the number of consecutive failures reaches the configured value, it automatically runs a preset action (reboot the device or reset the mobile network) for self-recovery — suitable for unattended hang recovery on remote sites.

Figure 4-1-1. The ICMP Watchdog configuration page.



PARAMETERS

Detection starts only 180 seconds after the device boots, to avoid false triggers during startup. The action runs only after consecutive ping failures reach the retry count. If the source interface does not exist or has no IP, repeated abnormalities also trigger the action. The target address accepts IPv4 only; rules with the same target address, source interface and action cannot be duplicated. Up to 10 rules are supported.

▶ 4.2 DTU (Transparent Transmission)

DTU (Data Transfer Unit) bridges the router serial port and the network. Data from field serial devices can be passed through or converted to a server over **TCP, UDP or MQTT**, and the server can also send data down to the serial device. It is commonly used to connect serial meters and PLCs to a network without a separate protocol converter.

Figure 4-2-1. The DTU (Transparent Transmission) configuration page.

Application / DTU

Reboot Time: Thu Jun 11 17:47 2026

Protocol TCP

Mode Client

* Network Timeout(ms) 150

* Serial Timeout(ms) 150

Registration Packet Max length is 64

Heartbeat Data Max length is 64

Heartbeat Interval 1-65535

* Server&Port Main A.B.C.D : 1-65535

Server&Port Backup A.B.C.D : 1-65535

Serial Type RS232

Baud Rate 115200

Parity none

数据位 8

停止位 1

Save

Copyright © 2020-2024 | All Rights Reserved

OVERVIEW

Enable DTU with the switch in the top-right corner. On multi-serial devices, first select the target serial port using the tabs at the top, then choose the working protocol (TCP / UDP / MQTT) and fill in the server address.

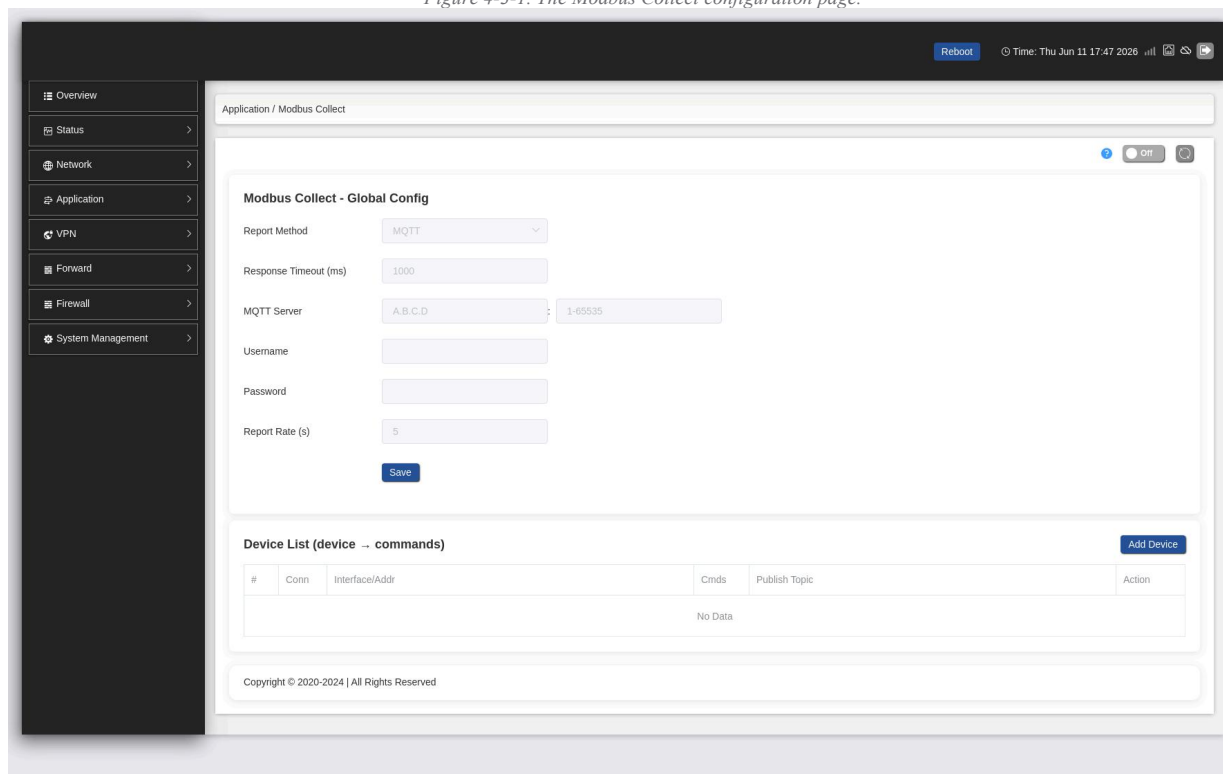
PARAMETERS

The serial parameters (baud rate, parity, data bits, and stop bits) must exactly match those of the connected serial device ; otherwise, data may be garbled. Each RS485 port supports one independent DTU channel. The VT-LTE500 provides two RS485 ports.

4.3 Modbus Collect

Modbus Collect is a self-contained Modbus master that polls slave devices on the field bus, caches the most recent value of each register in the router, and pushes the cache northbound to a server. It is the core industrial-acquisition feature of this product line.

Figure 4-3-1. The Modbus Collect configuration page.



OVERVIEW

A rule consists of a set of slave devices (each with an address and a transport — Modbus RTU over serial, Modbus TCP over Ethernet, or one of the Modbus-over-TCP variants) and, per device, a list of register groups to poll. The engine merges adjacent registers into a single request to minimise bus traffic. Polling failures are isolated per device — a stuck slave does not block the others.

The northbound side is built into the same engine, with three deliverable channels: **MQTT** (default), plain **TCP**, and plain **UDP**. The channel is part of the rule, not a global setting, so different rules can target different platforms.

PARAMETERS

No.	Field	Meaning
1.	Device name	Free-form label used in logs and in the payload. Must be unique within the rule.
2.	Transport	Modbus RTU / Modbus TCP / Modbus RTU over TCP / Modbus ASCII / Modbus ASCII over TCP : your slave actually speaks.
3.	Serial port (RTU only)	The physical RS485 port used to reach the slave. Must match how the device is wired.
4.	Baud / data / stop / parity (RTU only)	Serial-line parameters. Mismatches show up as CRC errors in the per-device error counter.
5.	IP : Port (TCP only)	Address of the slave or of the RTU-over-TCP converter.
6.	Slave address	The Modbus unit identifier (1 – 247).
7.	Polling interval	How often the engine re-reads the slave's registers (in milliseconds). Lower values increase fidelity but raise bus load.
8.	Register groups	One or more (function code, start address, length) tuples. Function codes 01–06 are supported; data is decoded as 16 / 32 / 64-bit integer, float or double.
9.	Report method	MQTT / TCP / UDP . Selects how the cached values are sent north.
10.	Broker / server / topic	Address and topic (MQTT) or endpoint (TCP/UDP) the engine pushes payloads to.

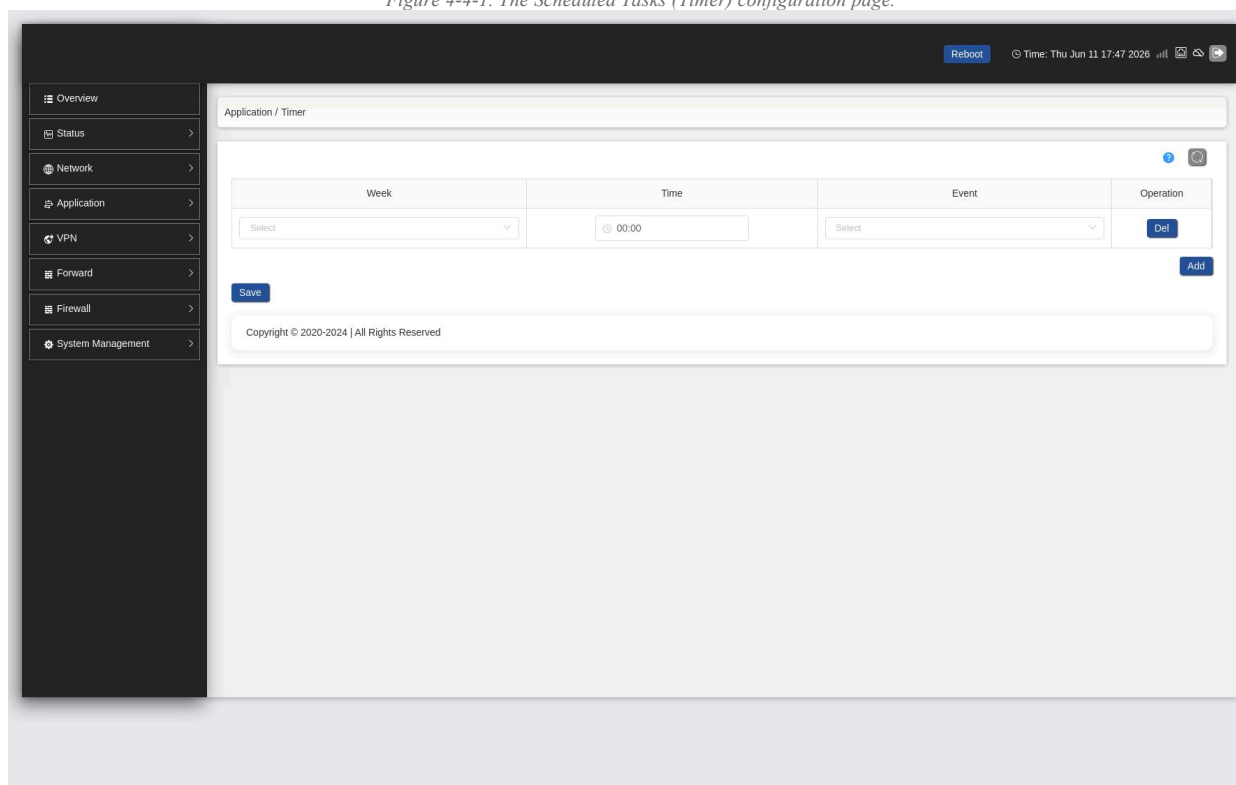
i **RTU is shared, TCP is not.** All RTU devices on one serial port share the bus and are polled in turn; a slow device delays every other device on the same port. TCP devices are polled in parallel because each has its own connection. When mixing fast and slow Modbus devices, split them across serial ports — or move the slow ones to TCP through an RS-485-to-TCP router.

▶ 4.4 Scheduled Tasks (Timer)

The Timer is a small cron-like scheduler built into the router. It runs commands on the device at the time of day you specify, on the weekdays you specify. Typical uses:

- **Reboot the router every night** to clear long-running memory pressure.
- **Switch the WAN port** between primary and backup on a fixed schedule (e.g. cheaper traffic plan at night).
- **Run a maintenance script** that lives in `/flash` — e.g. log rotation, snapshot upload.

Figure 4-4-1. The Scheduled Tasks (Timer) configuration page.



HOW TO: SCHEDULE A NIGHTLY REBOOT AT 03 : 00

This is the single most common Timer use case in production deployments. Many cellular carriers re-assign IP addresses or expire PDN contexts after long up-times; a nightly reboot avoids the slow degradation that follows.

1. Click **Add** at the top of the page to create a new task.
2. Fill in: **Name** `nightly-reboot` · **Time** `03:00` · **Repeat** tick every day (or just Sunday) · **Action / Command** `reboot` · **Status** `On`.
3. **Save.** Verify by waiting for the next 03:00, or set the time a couple of minutes ahead for a quick check.

FIELD REFERENCE

No.	Field	What to put there
1.	Name	Short label for this task; must be unique.
2.	Time	Hour and minute (24-hour clock) when the task fires.
3.	Repeat	Days of the week the task fires on. Tick at least one.
4.	Action / Command	The shell command to run. Single-line; for complex flows, put the steps in a script and call the script here.

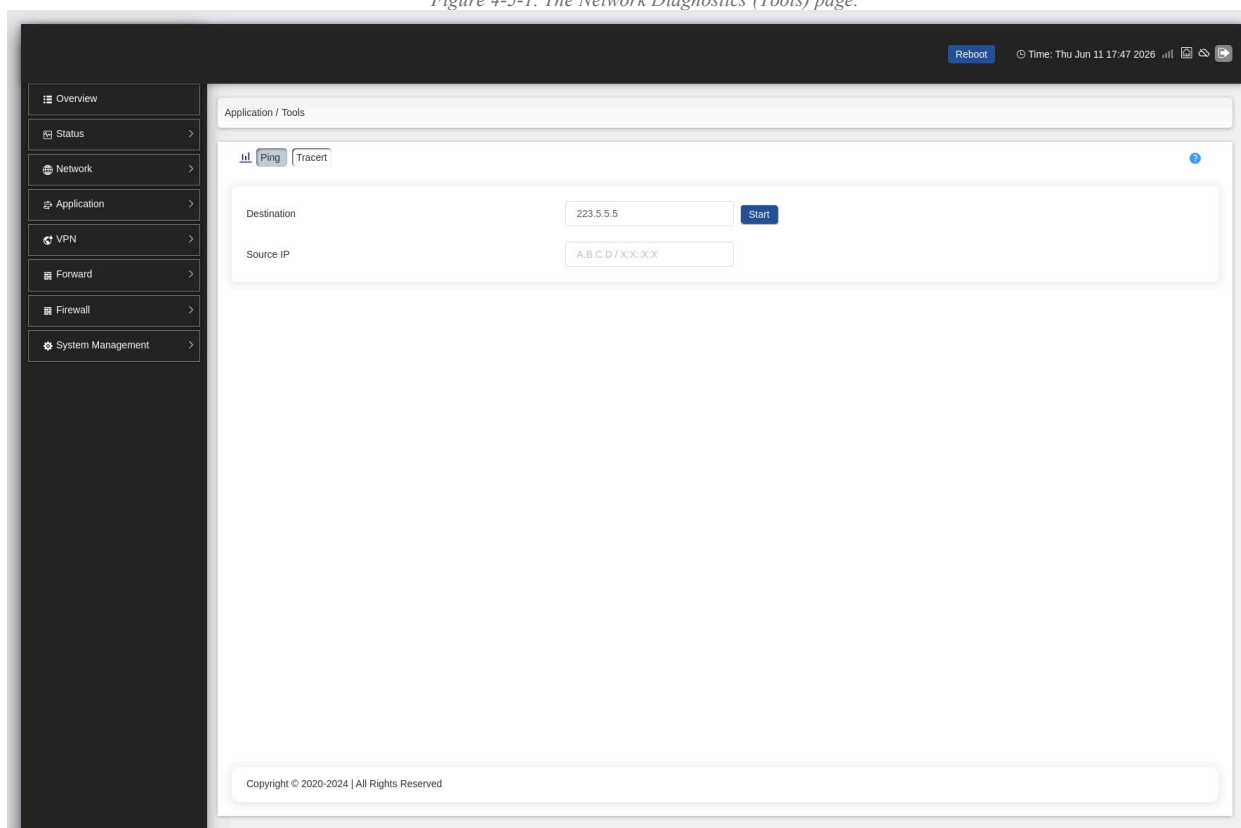
No.	Field	What to put there
5.	Status	Master switch for the task. Off keeps the row in the table but skips it.

The Timer fires in the router's system time — if tasks never fire, check the clock via **System Management** → **System Time**.

4.5 Network Diagnostics (Tools)

Built-in Ping and route-trace (Tracert) tools run diagnostics directly on the router and show the results live in an in-page terminal window, for troubleshooting network connectivity.

Figure 4-5-1. The Network Diagnostics (Tools) page.



OVERVIEW

Choose **Ping** or **Tracert** at the top, enter the destination address (a domain name, IPv4 or IPv6 is accepted), and click **Start**. Leave the source address empty in most cases (automatic routing); to force an exit interface, enter an IP that exists on the device.

PARAMETERS

An address containing a colon is automatically treated as IPv6, with no manual switching needed. The source address accepts only an IP that exists on the device, not a domain name. An invalid destination address is reset to the default 223.5.5.5. Ping keeps running and must be stopped manually; leaving the page ends the diagnostic automatically.

4.6 SNMP

SNMP lets the router expose device information (system name, serial number, interface status, etc.) so an enterprise network-management platform can query device status remotely and receive Trap alarms when something goes wrong.

Figure 4-6-1. The SNMP configuration page.

The screenshot shows the 'Application / SNMP' configuration page. On the left is a dark sidebar with navigation links: Overview, Status, Network, Application, VPN, Forward, Firewall, and System Management. The main content area has a title bar with a 'Reboot' button and a timestamp 'Time: Thu Jun 11 17:47 2026'. Below the title bar is a form with the following fields: 'Version' (a dropdown menu set to 'SNMPv2'), '* Port' (a text box with '161'), '* Community' (a text box with '*****' and a toggle icon), and 'Trap' (two text boxes, the first with 'A.B.C.D' and the second with '1-65535'). A 'Save' button is at the bottom left of the form. At the bottom of the page, there is a copyright notice: 'Copyright © 2020-2024 | All Rights Reserved'.

OVERVIEW

Enable the SNMP service with the switch in the top-right corner and choose the version (**SNMPv2c** or **SNMPv3**). For SNMPv2c, set the listening port and the community string (which acts as an access password). For SNMPv3, choose the security level, then fill in the username, authentication password and algorithm, and the encryption key and algorithm. For alarms, fill in the IP and port of the Trap receiver, then save.

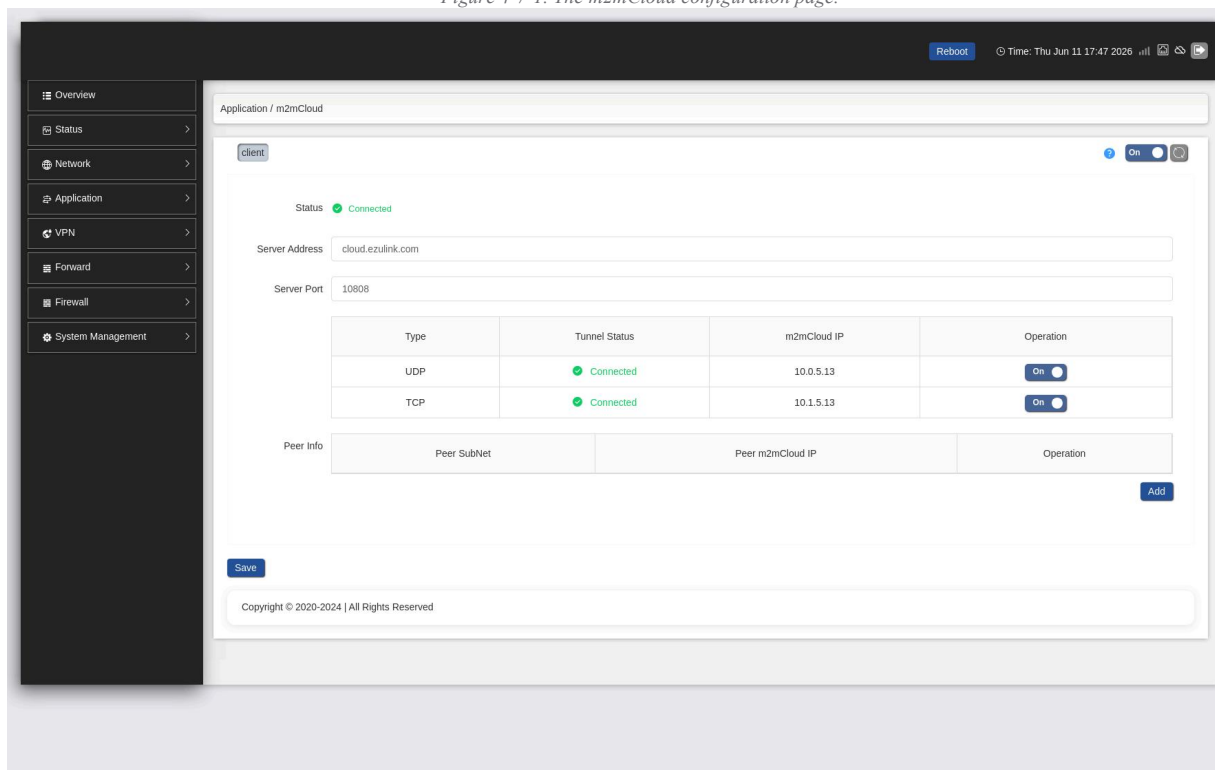
PARAMETERS

The username, password and encryption key allow letters and digits only. The password and encryption key must be 8 to 32 characters long. The Trap IP and port must either both be filled in or both be left empty. The visible SNMPv3 fields change with the chosen security level.

4.7 m2mCloud (Zero-config Remote Access)

m2mCloud is a software-defined remote-access service — built on an SD-LAN peer-to-peer tunnel — that lets you reach this router, and every device behind it, from anywhere **without a public IP, port mapping or manual VPN setup**. The router dials an outbound tunnel to the m2mCloud platform; once connected, the remote engineer's PC and the field equipment behave as if they were on the same local network. This is the **remote-control** capability of the product: remote monitoring, remote program upload / download, and remote control of the device and the equipment behind it.

Figure 4-7-1. The m2mCloud configuration page.



OVERVIEW

Turn m2mCloud on with the switch in the top-right corner. The router connects outbound to the **Server Address / Server Port** of the m2mCloud platform (for example `cloud.haolink.com : 10808`); once **Status** shows **Connected**, it builds UDP and TCP tunnels, each with its own **m2mCloud IP**. Because the tunnel is outbound, it works behind carrier-grade NAT and private cellular APNs where inbound VPN cannot.

FIELDS

No.	Field	Meaning
1.	Status	Connection state to the m2mCloud platform (Connected / Disconnected).
2.	Server Address / Port	The m2mCloud platform endpoint the router dials out to.
3.	Tunnel table	One row per transport (UDP / TCP) showing the tunnel status and the m2mCloud IP assigned to this router.
4.	Peer Info	Other members of the same virtual network — their subnet and m2mCloud IP — reachable from this router. Use Add to register a peer subnet.

TYPICAL USES

- **Remote PLC / HMI maintenance** — open the PLC programming software on your office PC and reach the field PLC's IP directly over the tunnel.
- **Remote monitoring** — reach field cameras, meters and panels without a static SIM or public IP.
- **Remote program upload / download** — push new PLC or device firmware to the field over the tunnel.

Connect the SIM, bind the account, and the whole site is reachable — no public IP, no firewall changes, no per-device VPN configuration.



CHAPTER

05

VPN

Site-to-site and remote-access tunnels using industry-standard protocols.



5. VPN

5.1 OpenVPN

OpenVPN builds a single encrypted tunnel between this router and another OpenVPN endpoint. The most common deployment is **client mode**: this router dials out to a company's OpenVPN server so that everything on the LAN side appears to be inside the company network. The router can also act as an **OpenVPN server** so that remote laptops or other routers dial in.

Figure 5-1-1. The OpenVPN configuration page.

VPN / OPENVPN Client

Reboot Time: Thu Jun 11 17:47 2026

openvpn-client0 openvpn-client1

Basic

Status Disconnected

Virtual IP

Server&Port A.B.C.D 1-65535

Username Max length 32

Password Max length 32

Device Mode tun

Protocol tcp

Encrypt none

Cipher none

Compress ☐

No Bind ☐

Root CA none

Key none

Cert none

Tls none

Keepalive 30

Certificate

Cert Name	Common Name	Organization	Expiration Time	Operation
-----------	-------------	--------------	-----------------	-----------

Add

Save

Copyright © 2020-2024 | All Rights Reserved

BEFORE YOU BEGIN

You need three things from whoever runs the OpenVPN server (your IT team, an MSP, or a cloud provider). Without them, the connection cannot be set up:

No.	Item	Typical form
1.	The server address and port	A public hostname or IPv4, plus a UDP or TCP port number (UDP 1194 is the default).
2.	A set of certificate /key files	Usually three files: <code>ca.crt</code> , <code>client.crt</code> , <code>client.key</code> . Some servers add a fourth— <code>ta.key</code> for the TLS-Auth hardening.
3.	The protocol settings the server uses	The most important are: transport (<code>udp</code> or <code>tcp</code>), tunnel type (<code>tun</code> is far more common than <code>tap</code>), and the cipher (e.g. <code>AES-256-CBC</code> or <code>AES-256-GCM</code>).

These come together as a single `.ovpn` profile in many real-world deployments. If you only have the `.ovpn` file, open it in a text editor — every field above is inside, plus the cert / key files are embedded as `<ca>...</ca>` `<cert>...` `</cert>` `<key>...</key>` blocks.

HOW TO: CONNECT THIS ROUTER TO A COMPANY OPENVPN SERVER (CLIENT MODE)

- 1. Upload the certificate files.** Stay on this page, look for the certificate card (towards the bottom). Click **Add** and upload `ca.crt`, `client.crt`, `client.key` (and `ta.key` if the server uses TLS-Auth). The files appear in the table once uploaded.
- 2. Switch the master toggle** at the top-right corner of the page to **On**. On multi-instance devices the tabs at the top let you pick which client slot to configure (`openvpn client1`, `openvpn client2`, etc.); this router can hold several independent clients side-by-side.
- 3. Fill in the basic block:**
- 4. Status:** must be `On` for this row to actually try to connect.
- 5. Server / Port:** the values from item 1 of the preparation list.
- 6. Device Mode:** `tun` for the vast majority of servers; `tap` only when the IT team explicitly says "layer-2 / bridged".
- 7. Protocol:** match the server (`udp` is the default and is faster; `tcp` is a fall-back for networks that block UDP).
- 8. Cipher:** match the server. `AES-256-CBC` is a safe default; `AES-256-GCM` is faster on modern servers.
- 9. Pick the certificate files** in the **Root CA**, **Cert**, **Key**, and **TLS** dropdowns. The dropdowns only list files you uploaded in step 1.
- 10. Account authentication (optional).** If the server requires a username / password in addition to certificates, fill them in. Many servers accept certificate-only and leave these empty.
- 11. Save.** The client tries to connect within ~5 seconds.
- 12. Verify on Status → VPN** (Section 2.6). The row should reach `Connected` within 10–30 seconds. The **Local IP** column shows the VPN-side address the server assigned to this router.

HOW TO: TURN THE ROUTER INTO AN OPENVPN SERVER (SERVER MODE)

This use case lets remote laptops or other routers dial in to your site.

- Switch to the **OpenVPN Server** tab at the top of the VPN page.
- Generate or upload server-side certificates** (CA + server certificate + server key). The Web UI provides a generator; export the matching client bundle for each remote user.
- Listen address / port:** the public IPv4 (or hostname) and UDP / TCP port the router should listen on. The port must be reachable from outside — see **Forward → NAT** (Section 6.1) if the router is behind a NAT.
- VPN subnet:** the IP range used inside the tunnel. Must not overlap your LAN. A common choice is `10.8.0.0/24`.
- Push routes:** the LAN subnets that connected clients should learn about. Add the router's LAN subnet here so clients can reach LAN devices.
- Save**, then distribute the generated client bundle to each remote user.

FIELD REFERENCE — CONNECTION

No.	Field	What to put there
1.	Status	Master switch for this client row. Off makes the form read-only and disables the connection.
2.	Server / Port	The public hostname / IP and port of the OpenVPN server. Both must be reachable from this router's WAN.
3.	Device Mode	<code>tun</code> (routed) for over 95 % of deployments. <code>tap</code> only when explicitly told.
4.	Protocol	<code>udp</code> is the default and recommended. <code>tcp</code> only when the path drops UDP.

No.	Field	What to put there
5.	Cipher	Must match the server. Common defaults: <code>AES-256-CBC</code> , <code>AES-256-GCM</code> , <code>AES-128-CBC</code> .

FIELD REFERENCE — AUTHENTICATION AND TUNING

No.	Field	What to put there
6.	Root CA / Cert / Key	Drop-downs picking the matching uploaded files. The CA validates the server; Cert and Key prove this router's identity.
7.	TLS	The optional TLS-Auth / TLS-Crypt key (often <code>ta.key</code>). Only populate when the server uses this extra hardening layer.
8.	Username / Password	Fill both, or leave both blank. Half-filled = invalid.
9.	Compression / LZO	Match the server. Mismatched compression causes silent connection failures (handshake fine, no traffic flows).
10.	Keepalive	Time between probes that keep NAT mappings open. <code>10 60</code> (probe every 10 s, declare dead after 60 s) is a good default.

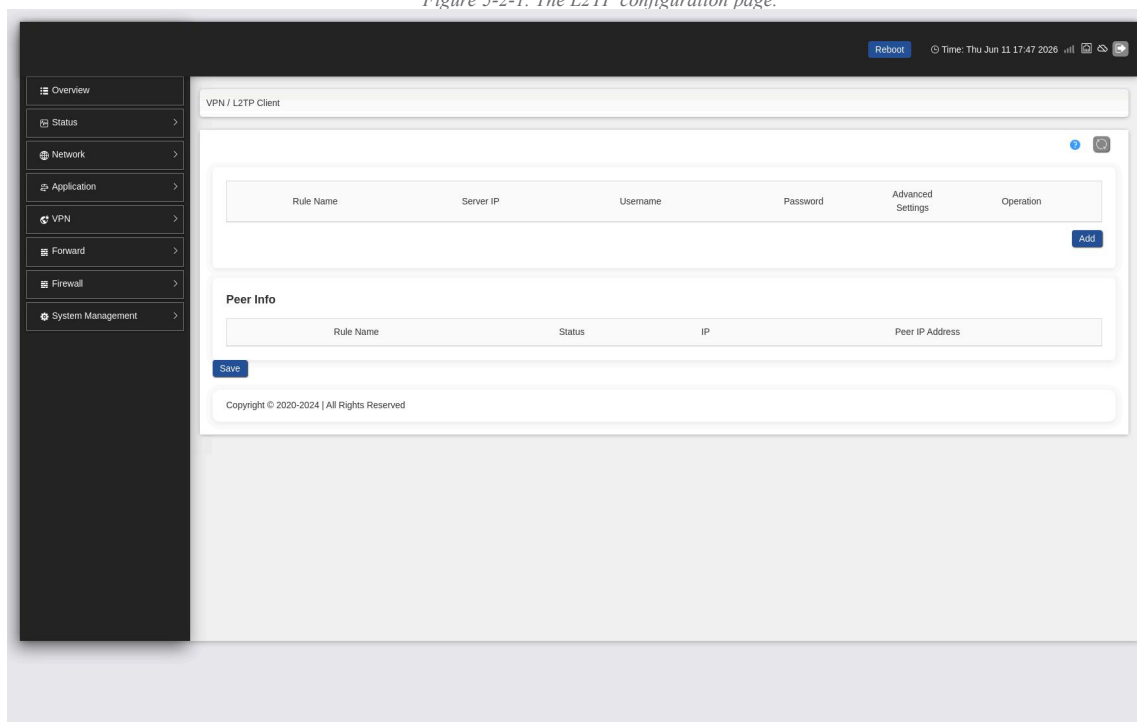
TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	Status never leaves <code>Connecting</code> .	Server unreachable from this router's WAN, or wrong port / protocol.	From the router: <code>nc -zv <server> <port></code> . If this fails, the issue is reachability, not OpenVPN.
2.	Status reaches <code>Connected</code> for a few seconds, then drops, repeatedly.	Server is configured with <code>client-disconnect</code> based on auth failure, or two clients share the same certificate.	Confirm with the server administrator that the certificate is unique to this router.
3.	<code>Connected</code> but LAN clients cannot reach the remote network.	Routes are not being pushed by the server, or the server pushes them but Push routes does not include the LAN-side subnet.	On the server side, add a <code>push "route <lan-subnet> <mask>"</code> line. Verify on Status → Route (Section 2.7) that a route through the tunnel interface appeared.
4.	"TLS Error: TLS handshake failed" in the log.	Time skew, missing TLS-Auth key, or wrong CA file.	Verify the router's clock (Section 8.2). Confirm the CA file is the same one the server uses.
5.	Speed is much slower than the underlying link.	TCP-over-TCP if both transport and tunnel are TCP, or the cipher is software-only.	Switch transport to UDP. Use a hardware-accelerated cipher (<code>AES-128-GCM</code> , <code>AES-256-GCM</code>).

5.2 L2TP

L2TP (Layer 2 Tunneling Protocol) builds a virtual point-to-point link from this router to an L2TP server somewhere else, usually at company headquarters. The most common deployment uses **L2TP/IPsec** — L2TP carries the user authentication and routing while IPsec provides the encryption. L2TP on its own carries traffic in the clear and should be used only over a network you already trust (e.g. a dedicated private circuit).

Figure 5-2-1. The L2TP configuration page.



BEFORE YOU BEGIN

From the L2TP server administrator, get:

No.	Item	Example
1.	Server address	Public IP or hostname.
2.	Username and password	The PPP-style credentials the server accepts for this client.
3.	Pre-shared key (L2TP/IPsec only)	The IPsec PSK that wraps the L2TP layer.
4.	Tunnel name (optional)	Some servers want a hostname; usually safe to leave blank.

HOW
TO:

CONNECT TO A COMPANY L 2 TP SERVER

1. Click **Add** at the top of the page to create a tunnel.
2. Fill in:
3. **Name:** a short label (e.g. `to-HQ`).
4. **Status:** `On`.
5. **Server address:** the public IP or hostname of the L2TP server.
6. **Username / Password:** the credentials the server expects.
7. **Authentication:** `Auto` works with most modern servers. `PAP` / `CHAP` / `MS-CHAPv2` if explicitly required.
8. **MTU:** leave at the default (1400) unless the server administrator specifies otherwise.
9. If the server uses **L2TP/IPsec**, enable **IPsec on the rule** and fill in:
10. **Pre-shared key:** the IPsec PSK from item 3 above.
11. **IPsec encryption / hash / DH group:** match the server.
12. **Save.** The client dials within a few seconds.

13. **Verify on Status** → **VPN** (Section 2.6). The row reaches **Connected** and the **Local IP** column shows the address assigned by the server.

FIELD REFERENCE

No.	Field	What to put there
1.	Name	Unique label for the tunnel.
2.	Status	Master switch — On for the tunnel to attempt the connection.
3.	Server address	Public IP or hostname of the L2TP server.
4.	Username / Password	PPP credentials.
5.	Authentication	Auto for new deployments; PAP / CHAP / MS-CHAPv2 when the server specifies.

FIELD REFERENCE — TRANSPORT AND IPSEC WRAPPING

No.	Field	What to put there
6.	MTU / MRU	Defaults work for over 95 % of links. Lower only when there is a clear packet-fragmentation problem on the path.
7.	Use IPsec	Turn on for L2TP/IPsec deployments (recommended). Off only for L2TP over a trusted private circuit.
8.	IPsec PSK	The shared key wrapping the L2TP layer. Long random string.
9.	Tunnel name	Optional. Set when the server requires a hostname-style identity.

TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	Status stays Connecting .	Wrong server address or the router cannot reach the server.	From the router: <code>nc -zv <server> 1701</code> and <code>nc -zv <server> 500</code> (IPsec). Fix the reachability first.
2.	"Authentication failed" in the log.	Wrong username / password, or the server expects MS-CHAPv2 while the client tries PAP .	Confirm credentials. Set the Authentication field explicitly.
3.	L2TP/IPsec: Phase 1 fails.	PSK or IPsec ciphers do not match.	Verify with the server admin and update the rule.
4.	Connected but LAN clients cannot reach the remote network.	Server is not pushing routes to the LAN-side subnet.	Add a static route via Forward → Static Route (Section 6.2) pointing the remote LAN through the L2TP interface.

The username, password and authentication method must match the server.

When LCP, MTU or MRU values are out of range, they roll back to the previous value with a message.

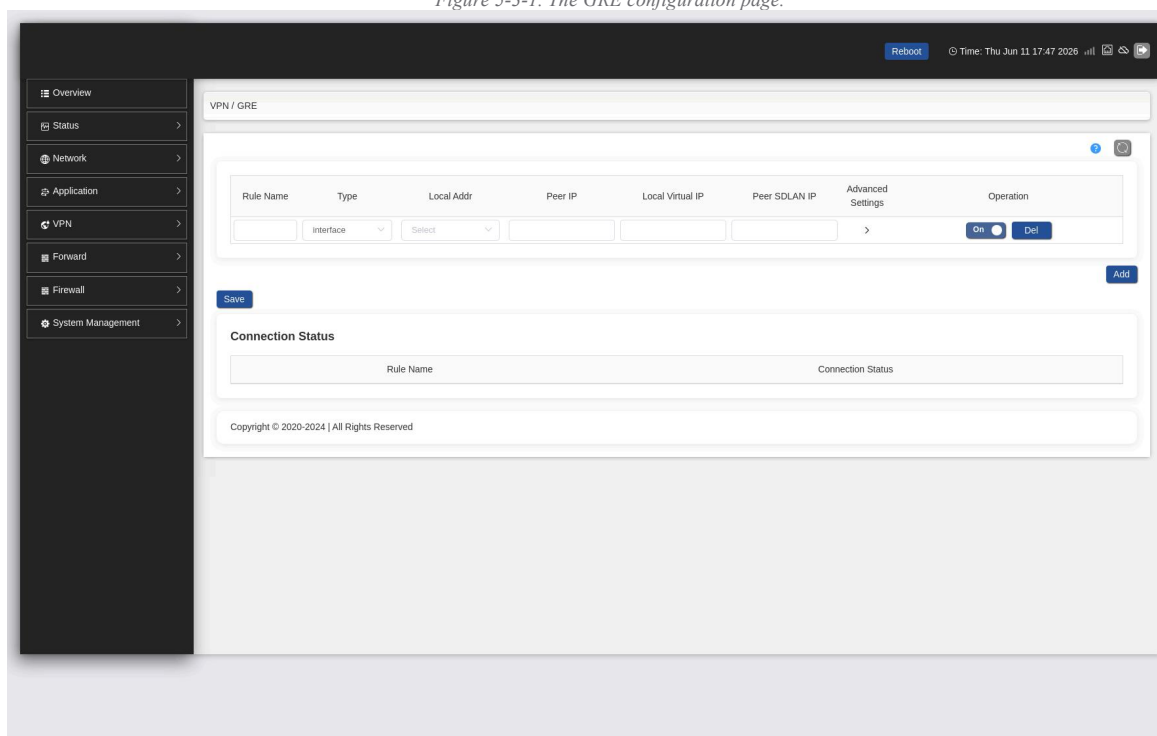
L2TP and PPTP share an underlying process, so saving this page may briefly restart the PPTP side.

► 5.3 GRE

GRE (Generic Routing Encapsulation) is the simplest possible site-to-site tunnel: it wraps each LAN packet inside an IP-over-IP envelope and sends the envelope to the other end. The other end unwraps and delivers the packet to its LAN. Unlike OpenVPN and IPsec, GRE does **no encryption** — it is a pure transport. For confidential traffic, combine GRE with IPsec (configure IPsec separately in Section 5.4 to protect the GRE traffic).

GRE shines when both ends are under your control and you want a stable, predictable tunnel with low overhead. It does not do user authentication and there is no concept of a "client" vs "server" — both ends are peers.

Figure 5-3-1. The GRE configuration page.



HOW GRE ADDRESSES WORK

Each end of a GRE tunnel has **two IPs you need to keep separate**:

- **The physical WAN IP** — what the other end uses to send the envelope to. This is the address of your router on the public Internet.
- **The tunnel-side virtual IP** — what shows up *inside* the tunnel as the source address of decapsulated packets. Common practice is to pick a small private subnet (e.g. `10.0.0.0/30`) and give one end `10.0.0.1` and the other end `10.0.0.2`.

A typical mistake: thinking the virtual IPs need to be in a subnet related to the LAN. They do not — they are an internal addressing layer between the two routers only.

HOW TO: BUILD A GRE TUNNEL BETWEEN TWO HAO- LINK ROUTERS

Two sites, two HAO-LINK routers, one wired upstream at each side. Site A's LAN is `192.168.1.0/24`, site B's LAN is `192.168.50.0/24`.

1. **Pick virtual IPs.** For example: A = `10.0.0.1`, B = `10.0.0.2`. Use the `/30` netmask (`255.255.255.252`).
2. **On Router A**, add a rule:
3. **Name:** `to-B`.
4. **Local address:** the WAN IP of A.
5. **Remote address:** the WAN IP of B.
6. **Local virtual IP:** `10.0.0.1`.
7. **Remote virtual IP:** `10.0.0.2`.
8. **Local subnet:** `192.168.1.0/24` (A's LAN).
9. **Remote subnet:** `192.168.50.0/24` (B's LAN).
10. **On Router B**, the mirror:
11. **Local address:** WAN IP of B, **Remote address:** WAN IP of A.
12. **Local virtual IP:** `10.0.0.2`, **Remote virtual IP:** `10.0.0.1`.
13. **Local subnet:** `192.168.50.0/24`, **Remote subnet:** `192.168.1.0/24`.
14. **Save both.** Within a few seconds each end shows `Up` on the GRE row.

15. **Verify:** from a LAN client on A, `ping 192.168.50.1` (B's router). It should reply.

i

GRE is plaintext on the public Internet. If anyone on the path can capture packets, they can read the GRE-encapsulated payload. If you carry sensitive traffic, configure IPsec (Section 5.4) between the same two WAN IPs — the IPsec layer encrypts the GRE envelopes transparently.

FIELD REFERENCE

No.	Field	What to put there
1.	Name	Unique label for this tunnel.
2.	Local address	WAN IP of this router. <code>0.0.0.0</code> for "any local interface".
3.	Remote address	WAN IP of the peer router. Must be reachable from here.
4.	Local virtual IP	The address this end takes inside the tunnel, e.g. <code>10.0.0.1/30</code> .
5.	Remote virtual IP	The address the peer takes inside the tunnel. The two virtual IPs form a tiny point-to-point subnet.

FIELD REFERENCE — CARRIED SUBNETS AND TUNING

No.	Field	What to put there
6.	Local subnet	The LAN behind this router, e.g. <code>192.168.1.0/24</code> .
7.	Remote subnet	The LAN behind the peer, e.g. <code>192.168.50.0/24</code> . Used to install a static route automatically.
8.	Key (optional)	A 32-bit value that both ends must share. Useful when several GRE tunnels exist between the same two WAN IPs and you need to demultiplex them.
9.	TTL	Time-to-live of the outer GRE packet. Default works for most networks.

TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	The row shows <code>Down</code> .	Either side's WAN IP is wrong, or a firewall on the path drops GRE (IP protocol 47).	Verify the WAN IPs. Run <code>tcpdump -i <wan> proto 47</code> on both ends to confirm GRE packets are flowing.
2.	The row shows <code>Up</code> but <code>ping</code> across does not work.	Static route to the remote LAN is missing on one side.	Check Status → Route (Section 2.7) for a route to the remote subnet via the GRE tunnel. Re-save the rule to re-install.
3.	Sometimes works, sometimes not.	Both ends are behind dynamic public IPs and one of them changed.	Use a static public IP, or a third-party DDNS hostname, on at least one end instead of a raw IP.
4.	Throughput is low compared to the underlying link.	GRE adds 24 bytes of overhead per packet, and the path MTU is forcing fragmentation.	Lower the LAN MTU to 1476 (or enable MSS clamping).

The tunnel key accepts digits only and must be identical on both ends; leave it empty to disable the key.

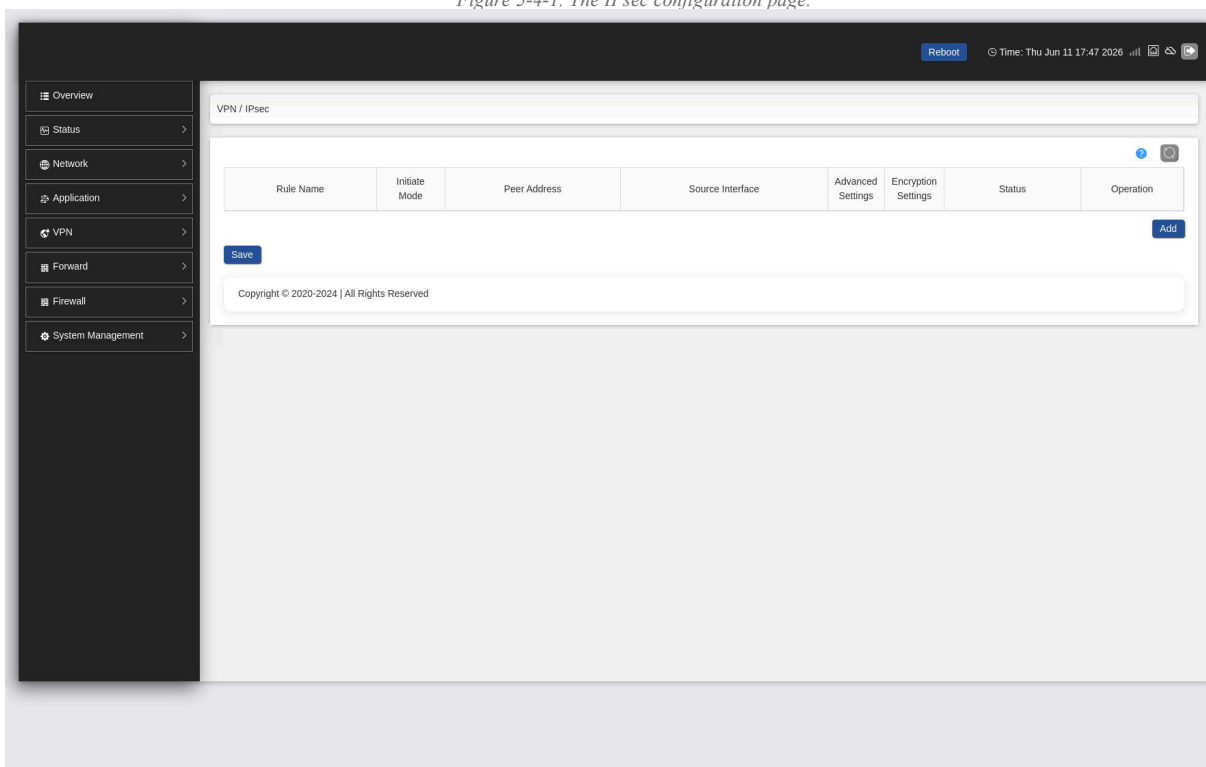
The physical IP does not accept invalid addresses such as a first or last octet of 0.

Up to 10 rules.

5.4 IPsec

IPsec is the industry-standard site-to-site VPN. It builds an encrypted tunnel between two routers and routes traffic between their LAN subnets transparently. Every commercial firewall (Cisco, Fortinet, Huawei, pfSense, FortiGate, MikroTik, etc.), every public cloud (AWS, Azure, Aliyun) and every other HAO-LINK router speaks IPsec, which makes it the safest choice when "the other end" is not under your control.

Figure 5-4-1. The IPsec configuration page.



HOW IPSEC SETS UP A TUNNEL (THE 30 - SECOND VERSION)

A working IPsec tunnel requires the two ends to agree on **two** sets of parameters:

- 1. Phase 1 (IKE):** the handshake that proves "you are who you say you are" and establishes a temporary secure channel. Pre-shared key (PSK), encryption (e.g. `AES-256`), integrity hash (e.g. `SHA-256`), Diffie-Hellman group (e.g. `Group 14`) and lifetime — **all five must match exactly on both ends**.
- 2. Phase 2 (ESP):** the real tunnel. Encryption, integrity, optional PFS group, lifetime, and the two subnets being connected — **must match (or be a subset of) the other end**.

If any single value is different, negotiation fails with `No proposal chosen` or `INVALID_KEY_PAYLOAD` in the log. Trying random combinations is the slow way; the fast way is to copy the exact settings to both ends.

BEFORE YOU BEGIN

For each tunnel you need to know, from the other end's administrator:

No.	Item	Example
1.	The peer's public address	The WAN IP or hostname of the remote router.
2.	The pre-shared key (PSK)	A long random string both ends must hold. Treat this like a password.
3.	IKE settings	Version (v1 or v2), encryption, hash, DH group, lifetime.
4.	ESP settings	Encryption, hash, optional PFS group, lifetime.
5.	Local subnet (your LAN)	e.g. <code>192.168.1.0/24</code> .

No.	Item	Example
6.	Remote subnet (their LAN)	e.g. 192.168.50.0/24. The two subnets must not overlap.

HOW TO: CONNECT TWO HAO-LINK ROUTERS TOGETHER (THE TEXTBOOK CASE)

You have two sites, each with a HAO-LINK router and one LAN. You want any device on site A to reach any device on site B as if they were on the same network.

- Pick the parameters.** A modern, safe, and widely interoperable set is:
- IKE:** version IKEv2, encryption AES-256, hash SHA-256, DH group Group 14 (2048-bit), lifetime 28800 s.
- ESP:** encryption AES-256, hash SHA-256, PFS Group 14, lifetime 3600 s.
- PSK:** any long random string. Use the same string on both ends.
- Decide who initiates.** When at least one end has a fixed public IP, that end can be either responder or initiator; when both ends are behind dynamic public IPs, you need a third-party DDNS hostname or a cloud relay (out of scope here).
- On Router A,** go to **VPN → IPsec**, add a new rule:
- Name:** to-site-B (any unique label).
- Mode:** Tunnel.
- Local address:** the WAN IP of Router A (or 0.0.0.0 to let any local IP match).
- Remote address:** the public IP / hostname of Router B.
- Local subnet:** 192.168.1.0/24 (A's LAN).
- Remote subnet:** 192.168.50.0/24 (B's LAN).
- PSK:** the random string from step 1.
- IKE / ESP:** the values from step 1.
- Save.**
- On Router B,** add a mirror rule:
- Local address** = WAN IP of B, **Remote address** = WAN IP of A.
- Local subnet** = 192.168.50.0/24, **Remote subnet** = 192.168.1.0/24.
- Same PSK, same IKE / ESP settings.
- Save.** Within 10–20 seconds the two routers negotiate the tunnel.
- Verify on Status → VPN** (Section 2.6) on either side: the row should show **Connected**. Then ping across the tunnel: from a LAN client on site A, ping 192.168.50.1 (B's router). It should reply.

i **Mirror the subnets, do not swap them.** A common mistake is leaving both ends with the same Local / Remote columns. Each end's "Local" is its own LAN; each end's "Remote" is the other end's LAN. The rules are mirrors of each other, not copies.

HOW TO: CONNECT TO A THIRD- PARTY FIREWALL (CISCO / FORTINET / HUAWEI / AWS)

The mechanics are the same — Phase 1 and Phase 2 still have to match — only the GUI on the other end looks different. The general procedure is:

- Ask the remote admin for their Phase 1 and Phase 2 parameters.** Most firewalls have a "show" or "export" function. Copy the values verbatim.
- Configure this router as in the previous walk-through,** using those values.
- One field that often differs: Local ID / Remote ID.** Some firewalls require an explicit identity string (often the public IP as text, sometimes an email-format string, sometimes an FQDN). When the remote admin specifies a Local / Remote ID, set it here even though the field is optional.

4. When the remote side is behind NAT (e.g. AWS VPN Gateway sometimes), enable NAT Traversal on both ends.

This wraps ESP packets in UDP4500 so they survive NAT.

FIELD REFERENCE — TUNNEL IDENTITY

No.	Field	What to put there
1.	Name	A short label for this tunnel; must be unique on the router.
2.	Mode	<code>Tunnel</code> for site-to-site (the common case). <code>only</code> for host-to-host.
3.	Local / Remote address	The WAN IPs / hostnames of this end and the peer. Leave Local as <code>0.0.0.0</code> to mean "any local interface".
4.	Local / Remote subnet	The LAN subnets being connected. Must mirror the peer.
5.	Pre-shared key (PSK)	A long random string identical on both ends. If you leave it blank the router uses <code>12345678</code> — change this in production.

FIELD REFERENCE — IKE / ESP CIPHER SUITE

No.	Field	What to put there
6.	IKE version	<code>IKEv2</code> for new deployments. <code>IKEv1</code> only when the peer is too old.
7.	IKE encryption / hash / DH group / lifetime	All four must match the peer exactly.
8.	ESP encryption / hash / PFS group / lifetime	All four must match (or be a subset of) the peer's proposals.
9.	Local ID / Remote ID	Optional. Set when the peer requires explicit identities (common with Cisco and AWS).
10.	DPD (Dead Peer Detection)	Default <code>restart</code> lets strongSwan decide when to renegotiate after a peer becomes unreachable. Leave at default unless instructed.

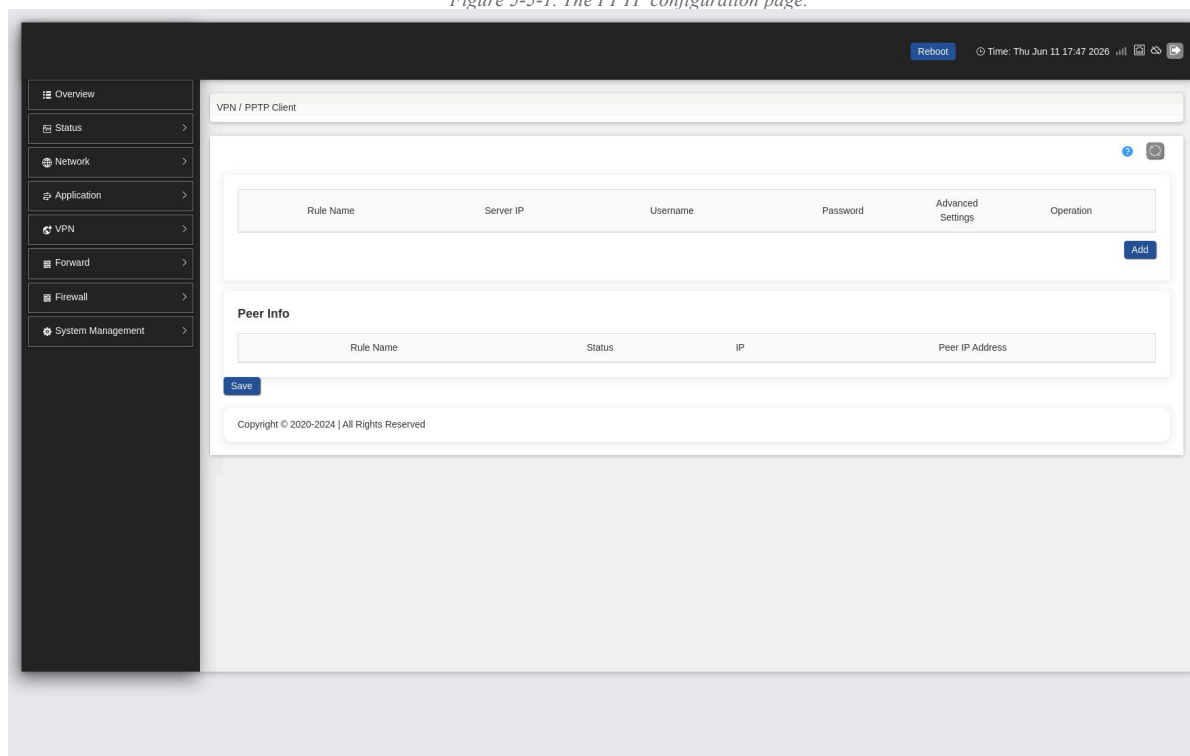
TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	Negotiation fails with <code>No proposal chosen</code> .	One or more Phase 1 / Phase 2 parameters do not match.	Get the exact list from the peer. Cross-check encryption, hash, DH group, lifetime — all four.
2.	<code>INVALID_KEY_PAYLOAD</code> on every retry.	The two ends advertise different DH groups.	Force the same DH group on both ends.
3.	Phase 1 succeeds, Phase 2 fails.	Local / Remote subnet mismatch — the two ends propose different "interesting traffic".	Each end's Local subnet must equal the other end's Remote subnet.
4.	Tunnel up, but <code>ping</code> across does not work.	Routing is OK, but the router's LAN-side firewall or the peer's firewall blocks the source subnet.	Allow inbound from the remote subnet to the LAN. Verify with <code>tcpdump -i br-lan icmp</code> .
5.	Tunnel up but flaps every 1 hour.	Phase 2 lifetime expires and the renegotiation fails.	Set lifetimes (Phase 1 + Phase 2) to the same value on both ends.
6.	Works from one side, fails from the other.	One end is behind NAT but NAT-T is not enabled.	Enable NAT Traversal on both ends. The tunnel will move from UDP 500 → UDP 4500 automatically.

5.5 PPTP

PPTP is included for **legacy interoperability only**. It is the oldest of the VPN protocols on this router and the one with the weakest cryptography (MS-CHAPv2 + MPPE). Modern Microsoft and Apple operating systems have removed PPTP client support. Use PPTP only when the other end is an old Windows Server, an old Mikrotik, or a legacy device you cannot upgrade. **For any new deployment, choose WireGuard (Section 5.6) or OpenVPN (Section 5.1) instead.**

Figure 5-5-1. The PPTP configuration page.



PPTP is not secure on the public Internet. A passive attacker who captures the handshake can recover the password through well-known MS-CHAPv2 weaknesses. Carry PPTP traffic only over a network you already trust (private circuit, MPLS, LAN), or wrap it in an outer IPsec / WireGuard tunnel.

BEFORE YOU BEGIN

From the PPTP server administrator:

No.	Item	Example
1.	Server address	Public IP or hostname (TCP port 1723 must be reachable).
2.	Username	The dial-in account.
3.	Password	The corresponding password.
4.	Encryption setting	Whether MPPE is required (almost always yes; usually 128-bit).

HOW TO: CONNECT TO A LEGACY PPTP SERVER

1. Click **Add** at the top of the page.
2. Fill in:
3. **Name:** a short label.
4. **Status:** ☐ On ☒ .
5. **Server address:** the IP or hostname of the legacy server.
6. **Username / Password:** the dial-in credentials.
7. **MPPE encryption:** ☒ Required (the common case). ☐ Optional only when the server explicitly says it is not used.
8. **MTU:** leave at default (1400) unless the server documentation says otherwise.

9. **Save.** The dial completes within a few seconds when the server is reachable and the credentials are correct.

10. **Verify on Status** → **VPN** (Section 2.6).

FIELD REFERENCE

No.	Field	What to put there
1.	Name	Unique label for the tunnel.
2.	Status	Master switch. Off keeps the row but does not dial.
3.	Server address	IP or hostname of the PPTP server. TCP 1723 + GRE protocol 47 must be open to it from this router.
4.	Username / Password	Dial-in credentials.
5.	MPPE encryption	Required for any internet-side server; Optional only inside a trusted network.
6.	Authentication	MS-CHAPv2 is the only mode in real use today.
7.	MTU / MRU	Defaults work for most links.

TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	Status stuck at Connecting .	TCP 1723 or GRE 47 is filtered on the path.	Confirm the network between the router and the server allows both. Many home / 4G NATs filter GRE.
2.	"Authentication failed".	Wrong password, or the server requires PAP / CHAP instead of MS-CHAPv2.	Confirm with the server admin.
3.	"MPPE required by peer but client refuses".	Encryption mismatch.	Set MPPE to Required .
4.	The remote side reports "Tunnel ID conflict".	Two PPTP tunnels to the same server are using the same Call ID.	Disable one of the duplicate rules; PPTP cannot multiplex multiple tunnels to the same server from a single source IP.

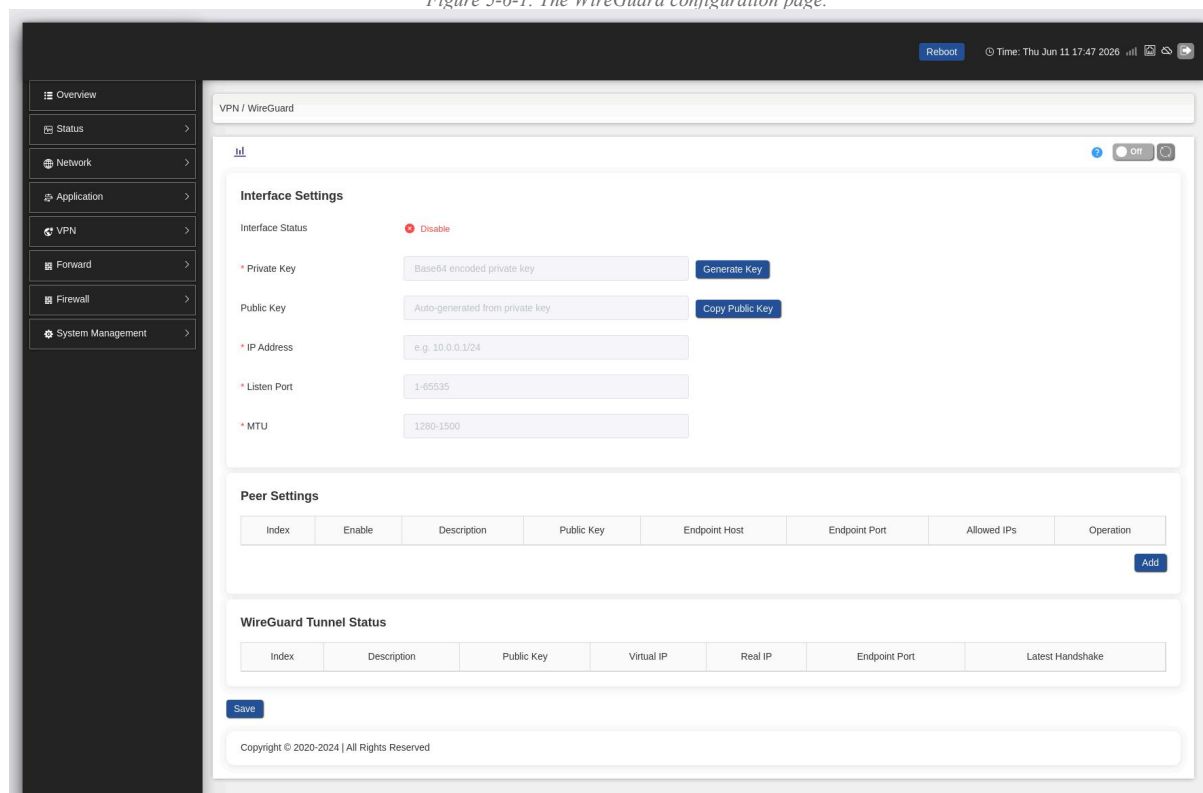
PPTP encryption is weak and some newer systems (such as macOS 10.15 and later) disable it by default; for stronger security use L2TP, IPsec or WireGuard.

L2TP and PPTP share an underlying process, so saving this page may briefly restart the L2TP side.

5.6 WireGuard

WireGuard is the modern, fast, low-overhead VPN protocol. Compared to OpenVPN and IPsec it has a fraction of the configuration surface (a handful of fields, no certificate hierarchy), it connects in milliseconds instead of seconds, and the cryptography is fixed (no negotiation, no mismatched-cipher headaches). For new deployments it is the recommended default when both ends support it.

Figure 5-6-1. The WireGuard configuration page.



HOW WIREGUARD WORKS (60 SECONDS)

A WireGuard tunnel has **no client / server distinction** — both ends are simply "peers". Each peer has a **private key** (which it keeps to itself) and the matching **public key** (which it gives to every peer that should be allowed to connect). To bring up a tunnel between two devices:

1. Each device generates its own keypair.
2. They **exchange public keys** out of band (email, secure chat, USB).
3. Each device adds the other as a peer, pasting in the **other's public key** and the IP they should take inside the tunnel.
4. One end (the one with a public IP / hostname) declares its **endpoint**; the other end connects to it.

That's the whole protocol. There is no handshake retry storm, no negotiation log to debug.

BEFORE YOU BEGIN

For each peer you plan to add, get from the other side:

No.	Item	Example
1.	The peer's public key	A 44-character base64 string ending in '='.
2.	The peer's tunnel IP	The address it should take inside the tunnel, e.g. 10.0.0.2.
3.	The peer's endpoint (if you initiate the connection)	Public IP / hostname and UDP port, e.g. vpn.company.com:51820.

No.	Item	Example
4.	The peer's allowed-ips	The subnets you want to route through this peer's side, e.g. <code>10.0.0.2/32</code> (just the peer) or <code>10.0.0.0/24, 192.168.50.0/24</code> (the peer + its LAN behind it).

HOW TO: CONNECT THIS ROUTER TO A CLOUD / COMPANY WIREGUARD SERVER

The cloud side has a static public IP; this router is the connector behind some random NAT (typical for an industrial site).

1. **Generate this router's keypair.** On this page click **Generate keys**. The **private key** auto-fills; copy the **public key** and email it to the server administrator.
2. **Fill in the local interface block:**
3. **Local IP:** the tunnel-side address the cloud assigned to this router, e.g. `10.0.0.42`.
4. **Listen port:** can be left blank (the kernel picks one automatically when you initiate).
5. **MTU:** leave at default (1420) unless the path drops large packets.
6. **Add a peer** (the cloud server) with:
7. **Public key:** the cloud server's public key (from the admin).
8. **Endpoint:** the cloud server's public hostname and port, e.g. `vpn.company.com:51820`.
9. **Allowed-IPs:** `10.0.0.0/24, <company-lan>/24` — every subnet you want to route through the tunnel. If you want **all** traffic (full-tunnel VPN), use `0.0.0.0/0`.
10. **Persistent keepalive:** `25` (seconds). **This is essential when this router is behind NAT** — without it, the NAT mapping expires after a minute of silence and the cloud cannot reach back.
11. **Save.** The tunnel becomes `Up` within a second.
12. **Verify on Status** → **VPN** (Section 2.6) and `ping 10.0.0.1` (the cloud side's tunnel IP).

HOW TO: CONNECT TWO HAO- LINK ROUTERS TOGETHER (PEER- TO-PEER)

Two industrial sites, both behind NAT. Pick one to be the "endpoint" — it needs to have its WAN port-forwarded to UDP 51820, or have a public IP, or use a DDNS name. Site A has the public IP; Site B initiates.

1. **On both routers**, generate a keypair on this page. Send each other the public key.
2. **On Site A** (the endpoint side):
3. **Local IP:** `10.0.0.1/24`.
4. **Listen port:** `51820`.
5. **Add a peer:** Site B's public key, **Allowed-IPs** = `10.0.0.2/32, 192.168.50.0/24` (B's tunnel IP + B's LAN), **Endpoint** left blank (Site A is the receiver), **Persistent keepalive** blank.
6. **On Site B** (initiates):
7. **Local IP:** `10.0.0.2/24`.
8. **Listen port:** blank.
9. **Add a peer:** Site A's public key, **Allowed-IPs** = `10.0.0.1/32, 192.168.1.0/24` (A's tunnel IP + A's LAN), **Endpoint** = A's WAN IP : 51820, **Persistent keepalive** = `25`.
10. **Save both.** Within a second the tunnel comes up.

FIELD REFERENCE

No.	Field	What to put there
1.	Status	Master switch. Off keeps the configuration but stops the tunnel.
2.	Private key	Auto-generated. Never copy or share. The matching public key is what you share with peers.
3.	Local IP	This router's tunnel-side address with mask, e.g. <code>10.0.0.2/24</code> .
4.	Listen port	The UDP port to listen on. Required only when other peers will connect to this router. Blank otherwise.

No.	Field	What to put there
5.	MTU	Path MTU for the tunnel. Default 1420 is correct for almost every link.

FIELD REFERENCE — PEER CONFIGURATION

No.	Field	What to put there
6.	Peer public key	The other end's public key. Paste exactly — the smallest typo and the tunnel silently never comes up.
7.	Peer endpoint	Public IP / hostname and UDP port of the peer. Fill in when this router is the initiator; leave blank when this router is the receiver.
8.	Allowed-IPs	Acts as both a routing table and an inbound filter. Pre-populate every subnet that should be reachable through this peer. <code>0.0.0.0/0</code> = send everything via this peer.
9.	Persistent keepalive	Seconds between empty datagrams that keep a NAT mapping open. <code>25</code> is the well-tested value. Set on the side behind NAT; leave blank on the side with a public IP.

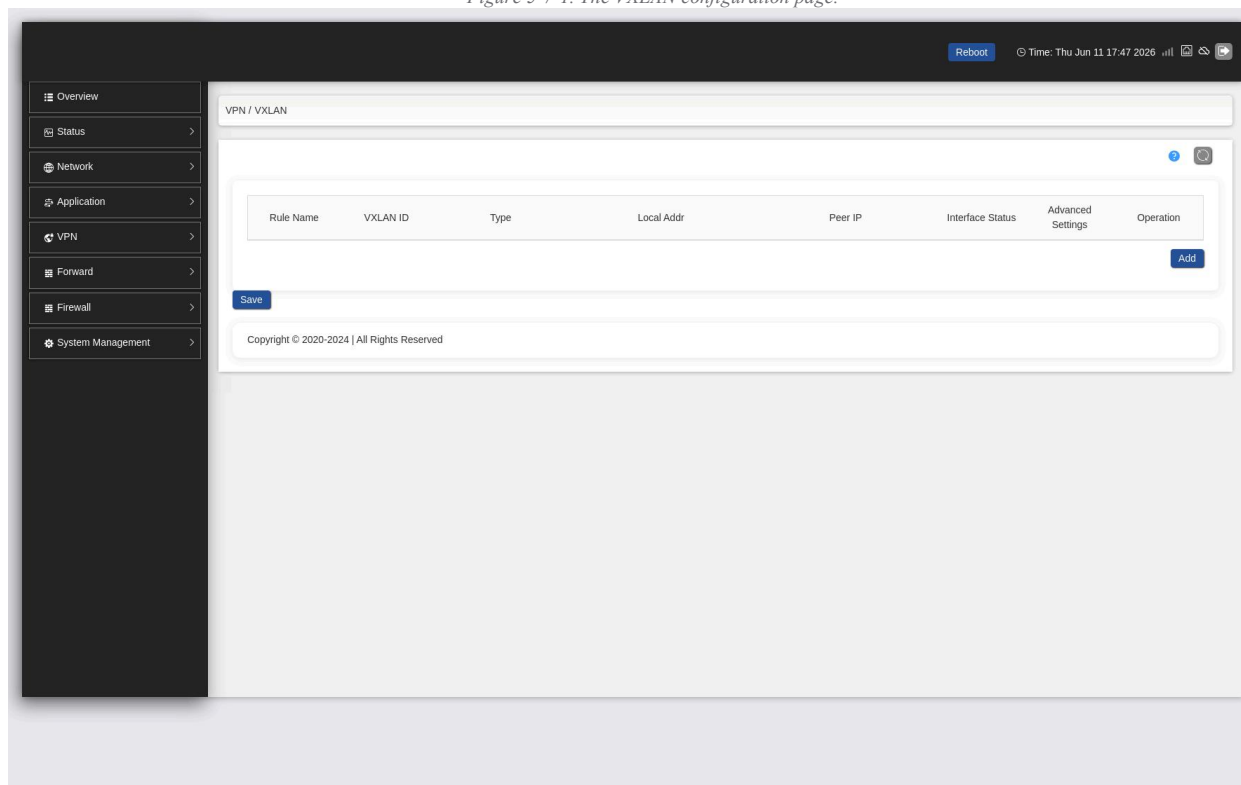
TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	The tunnel never comes up — no handshake in the log.	One end's public key is wrong (typo), or <code>Allowed-IPs</code> does not include the other end's tunnel IP.	Re-copy the public keys character by character. Double-check Allowed-IPs on both ends.
2.	Handshake completes, then nothing flows in one direction.	Asymmetric routing — Allowed-IPs covers the destination on one end but not the other.	Mirror Allowed-IPs so each end can route to the other's LAN.
3.	Tunnel works for a minute then dies.	This router is behind NAT and the NAT mapping expired.	Set Persistent keepalive = 25 on this end.
4.	<code>Status</code> shows <code>Up</code> but <code>ping</code> reports 100 % loss.	LAN-side firewall on the peer drops traffic from the tunnel.	Allow inbound from the tunnel subnet on the peer's firewall.
5.	Throughput is low compared to the underlying link.	MTU does not match path MTU; fragments are being dropped.	Lower MTU to 1380 or enable MSS clamping on the router.

5.7 VXLAN

VXLAN (Virtual Extensible LAN) builds a **Layer-2 overlay** across a Layer-3 (routed) network: it encapsulates Ethernet frames in UDP and carries them between sites so that hosts on the two LANs appear to share the **same broadcast domain**, even though they are separated by the Internet or a cellular link. Where GRE and the other tunnels in this chapter carry **routed** (Layer-3) traffic, VXLAN carries **bridged** (Layer-2) traffic — use it when an application needs the two segments to look like one flat LAN (for example legacy equipment that relies on broadcast discovery).

Figure 5-7-1. The VXLAN configuration page.



FIELDS

No.	Field	Meaning
1.	VNI (VXLAN Network Identifier)	The 24-bit segment ID. Both ends must use the same VNI to join the same overlay.
2.	Local IP	The WAN / source address this router sends VXLAN packets from.
3.	Remote IP	The peer router's address the overlay connects to.
4.	Port	The UDP port used for VXLAN encapsulation (default 4789). Must match on both ends.
5.	Bridge / interface	The local interface the overlay is bridged into, so LAN traffic crosses the tunnel.

i

Layer-2 reach has a cost. Because VXLAN floods broadcast and unknown-unicast traffic across the tunnel, a busy LAN can generate significant overlay traffic. On metered cellular links, prefer a Layer-3 tunnel (GRE / WireGuard / IPsec) unless the application genuinely needs a flat Layer-2 segment.

CHAPTER

06

Forward

Translate, route, mask, and shape traffic that traverses the router.



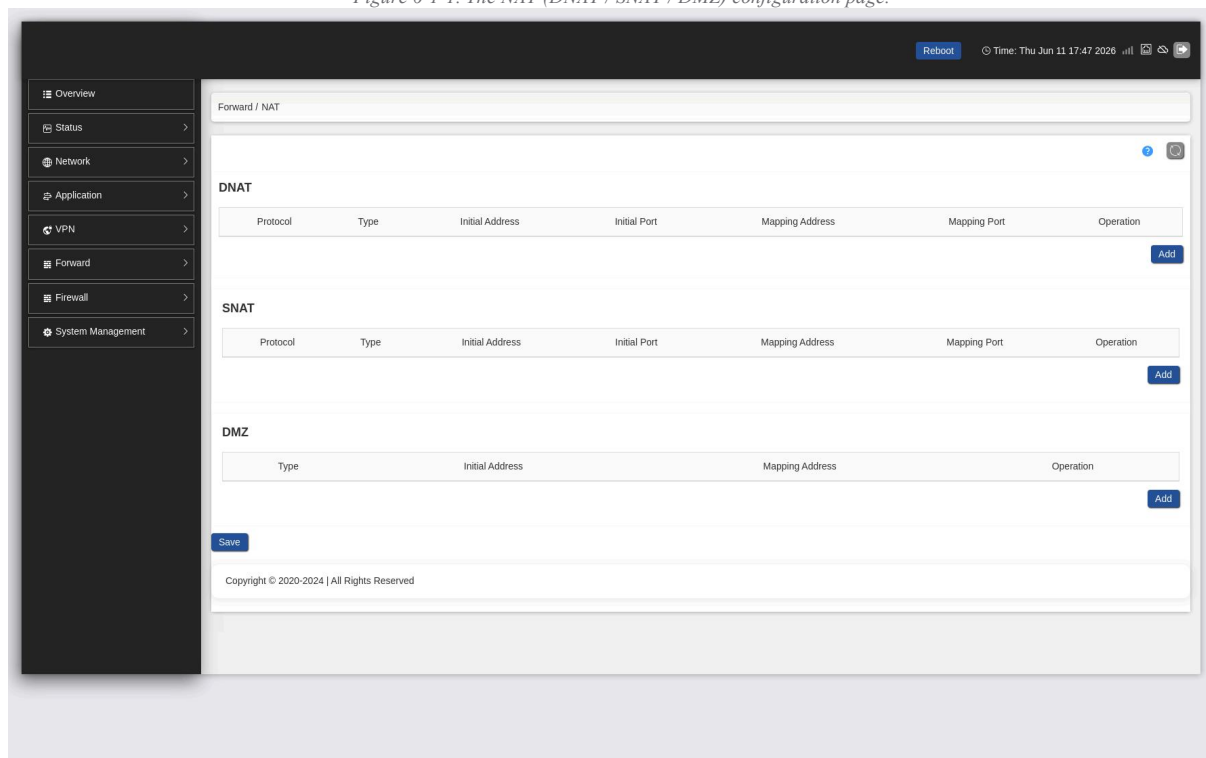
6. Forward

▶ 6.1 NAT (DNAT / SNAT / DMZ)

NAT (Network Address Translation) is what lets devices with private addresses on the LAN reach the public Internet, and lets specific public traffic reach designated devices on the LAN. This page is organised into three blocks, each for a different direction of the translation:

Block	Direction	When you use it
DNAT (Destination NAT)	Inbound	"From the Internet, make port X reach my internal camera / NVR / server / database." Same idea as "port forwarding" or "port mapping".
SNAT (Source NAT)	Outbound	"When this internal subnet sends to the Internet, rewrite the source IP." Used when several public IPs are bound to the router and you want a specific group of LAN devices to appear from one of them.
DMZ (Demilitarised Zone)	Inbound, all ports	"Forward <i>every</i> port at this entry to this one LAN device." Equivalent to one giant DNAT rule for ports 1-65535. Use sparingly — it fully exposes the chosen host.

Figure 6-1-1. The NAT (DNAT / SNAT / DMZ) configuration page.



HOW TO: FORWARD UDP / TCP FROM THE INTERNET TO AN INTERNAL DEVICE

The classic case: a security camera, an NVR, a Modbus TCP slave, or a small web service is on the LAN, and you want a specific external port to land at it.

- 1. Make sure the router has a reachable WAN IP.** If the WAN is behind another NAT (e.g. a 4G carrier NAT), DNAT alone is not enough — you also need the upstream device or carrier to forward the port to your router.
- 2. DNAT block** → click **Add**. Fill in:
- 3. Protocol:** **TCP** for HTTP/HTTPS/SSH/Modbus TCP/NVR web; **UDP** for SIP / WireGuard / DNS forwarder; **All** if both apply.
- 4. Type:** **Interface** (forward from "anything that arrives at the WAN interface") in 95 % of cases. Use **IP** only when you have several public IPs and want to forward only one of them.

5. **Initial address / port:** the **outside** entry — when **Type = Interface**, leave the address as the WAN interface name and put the **external portnumber** (e.g. `8080`). When **Type = IP**, put the public IP and external port.
6. **Mapping address / port:** the **inside** destination — the LAN IP of the target device (e.g. `192.168.1.50`) and its port (e.g. `80`).
7. **Save.** The rule takes effect immediately.
8. **Verify:** from outside the LAN (e.g. mobile data), `nc -zv <router-WAN-IP> 8080`. If the camera answers, the rule is working.

A typical pair: external port `8080` → `192.168.1.50:80` (the camera's web UI). The two ports do not need to match; in fact, **using a non-standard external port is recommended security practice** — scanners hammer 80 and 443 constantly.

HOW TO: REWRITE THE SOURCE IP OF A SUBNET (SOURCE NAT)

Use this when you have multiple WAN IPs and want each LAN segment to leave under a different one.

1. **SNAT block** → click **Add**. Fill in:
2. **Protocol:** `All` for everything, or narrow with TCP / UDP.
3. **Initial address:** the **inside** source subnet, e.g. `192.168.1.0/24`.
4. **Mapping address:** the **outside** address the router should rewrite the source to. `Interface` = take whatever IP that WAN interface currently has; `IP` = a specific public IP.
5. **Save.**

HOW TO: SET UP A DMZ HOST (EXPOSED INTERNAL DEVICE)

Used when an industrial device or a legacy server cannot be reached on a specific port and the simplest fix is "let it have the whole public-facing endpoint".

1. **DMZ block** → click **Add**. Fill in:
2. **Initial address:** `Interface` (usually the WAN interface).
3. **Mapping address:** the LAN IP of the host.
4. **Save.**

! A DMZ host is fully exposed to the Internet. Every open service on it can be probed and attacked. Use DMZ only for hardened, regularly-updated devices, and **never for a Windows desktop or an unpatched IoT camera**.

FIELD REFERENCE (DNAT)

No.	Field	What to put there
1.	Protocol	<code>TCP / UDP / All / ICMP</code> . Pick what the destination service uses.
2.	Type	<code>Interface</code> (forward anything that hits a named WAN interface) or <code>IP</code> (forward only what comes to a specific public IP).
3.	Initial address	The outside-facing entry — WAN interface name (Type = Interface) or public IP (Type = IP).
4.	Initial port	The outside port someone connects to from the Internet. Choosing a non-standard value reduces scan noise.
5.	Mapping address	The inside target — the LAN IP of the device.

No.	Field	What to put there
6.	Mapping port	The inside port. May differ from the initial port.

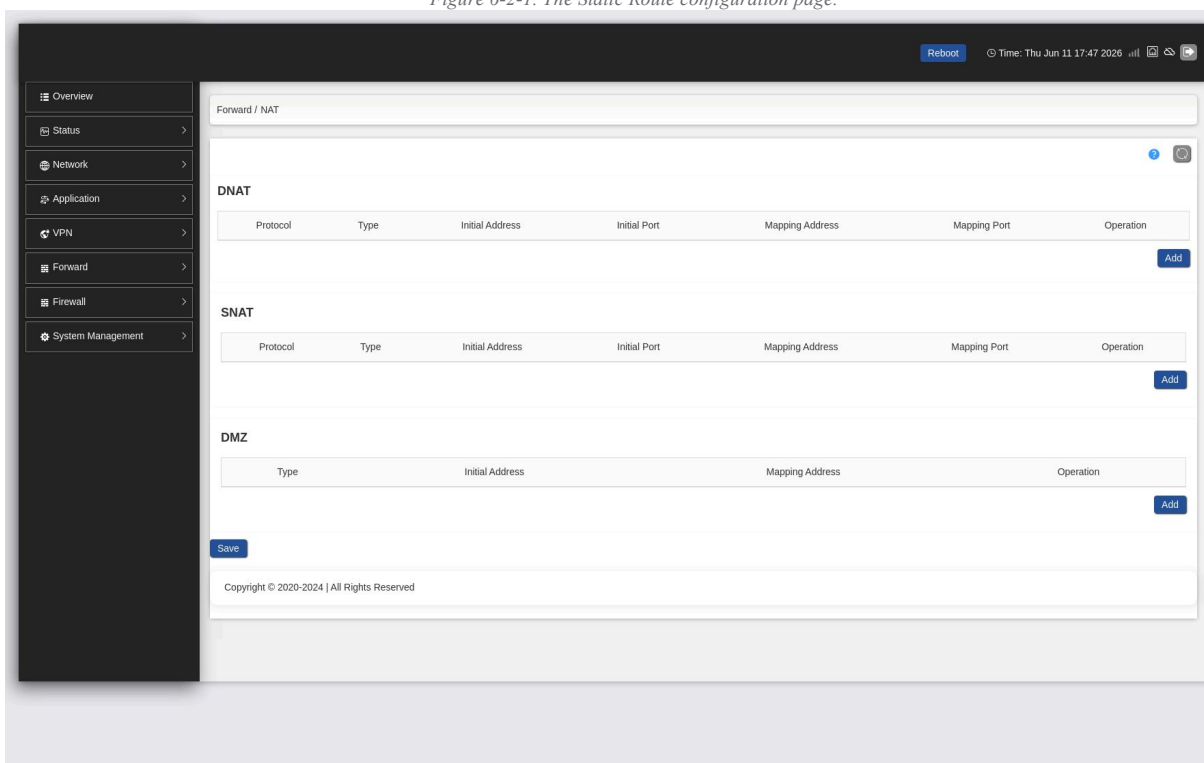
TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	"I added a DNAT rule but the port still does not reach inside."	The WAN itself is behind upstream NAT (4G carrier NAT, hotel router) and the upstream is not forwarding the port.	Test from a known-public host: <code>nc -zv <WAN-IP> <port></code> . If TCP refuses, upstream NAT is the wall.
2.	"Internal device shows traffic but the source IP is wrong."	A SNAT rule above the DNAT changed the source.	Re-order rules: DNAT for inbound first, SNAT only for outbound that does not overlap.
3.	"Saved, but the WAN interface IP changes (DHCP) and DNAT stops."	The rule was bound to a specific IP that no longer applies.	Set Type = Interface instead of IP — the rule then follows whatever the WAN interface gets.
4.	"DMZ host can reach the Internet but no one can reach it."	The DMZ host's local firewall blocks inbound.	Open the relevant port on the DMZ host itself.
5.	"Port forwards work over IPv4 but not IPv6."	NAT applies to IPv4 only. IPv6 traffic does not need DNAT — it needs the Firewall chapter's IP Filter to <i>allow</i> the inbound flow.	Open the matching rule under Firewall → IP Filter (Section 7.3).

6.2 Static Route

Static routes manually specify which path traffic to a given destination network should take, useful for steering specific subnets apart from the default route (e.g. sending a subnet through a VPN, a specific WAN or a next hop).

Figure 6-2-1. The Static Route configuration page.



OVERVIEW

Each row is one route entry; IPv4 and IPv6 are configured under separate tabs at the top.

When forwarding a packet the device selects a route by longest-prefix match; static routes take precedence over dynamically learned routes.

Entries are managed by adding/deleting rows, with no per-row enable switch; click Save after editing.

PARAMETERS

Target network: the destination network address. Setting 0.0.0.0 (mask becomes 0.0.0.0) means the default route - it matches all traffic not caught by another route.

Subnet mask: the mask of the destination network (/0, /16 to /32 available), which together with the target network defines the address range this route covers. IPv6 takes no mask and is treated as /64.

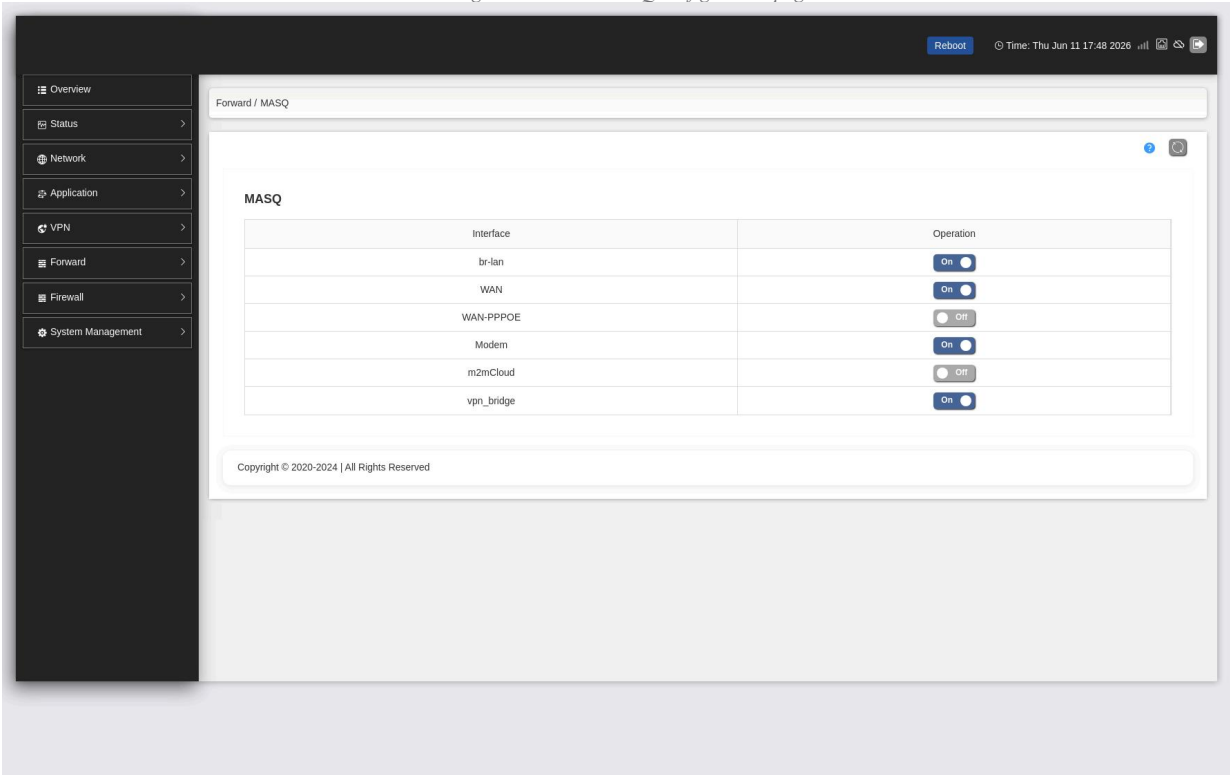
Type / Gateway: with Type set to Interface the traffic leaves through the chosen egress interface; set to IP it is handed to the specified next-hop IP.

Priority (metric): when several routes can reach the same destination, a smaller priority value is preferred, range 5-255.

6.3 MASQ

MASQ (address masquerade) controls, per egress interface, whether traffic passing through it has its source address masqueraded (MASQUERADE). When on, an internal device going online through that interface has its source IP automatically replaced with the egress address of the interface - the basis of internal shared Internet access.

Figure 6-3-1. The MASQ configuration page.



OVERVIEW

The page is an interface-to-switch table; the interface column is auto-enumerated from the currently available egresses (LAN, the WANs, cellular, WiFi, VPN, GRE, etc.) and cannot be added or removed manually.

Each switch takes effect immediately on toggle, with no separate Save.

MASQUERADE versus SNAT: it automatically uses the current egress IP of the interface as the translated address, so it needs no reconfiguration when the interface IP changes (e.g. a dial-up reconnect), making it suited to dynamic-address egresses.

PARAMETERS

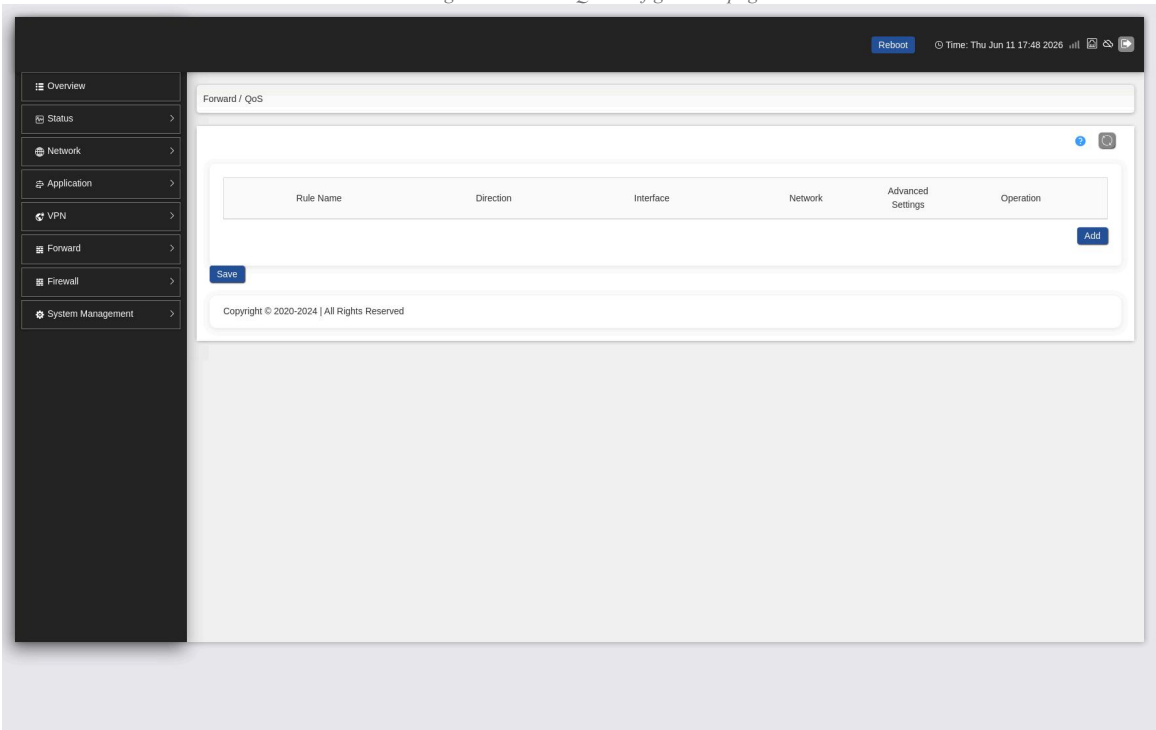
Interface: one egress interface of the system.

Switch: on = traffic leaving through this interface is source-masqueraded, so internal devices behind it can go online through it; off = no masquerade, the interface does plain routing only. LAN is on by default; VPN, GRE, cellular and other interfaces are enabled one by one as the network design requires.

6.4 QoS

QoS (Quality of Service) does traffic shaping - it allocates bandwidth per rule to traffic of a given subnet/port, so that no single device or application saturates the link and key services stay protected.

Figure 6-4-1. The QoS configuration page.



OVERVIEW

Each row is one rate-limit rule, up to 10; it is implemented on the Linux tc HTB queue.

A rule matches traffic by subnet (and optionally port): Rate is the guaranteed bandwidth (always available) and Peak rate is the upper bandwidth it may borrow up to.

It is per-rule rate limiting, not automatic per-IP sharing; click Save after editing.

PARAMETERS

- Rule name: the rule identifier, up to 10 characters.
- Direction: upload (internal to external) or download (external to internal); the interface is set accordingly on selection (download on the LAN side, upload on the WAN side).
- Interface: the network interface the limiting applies to.
- Network: the IP subnet the rule matches, in CIDR form A.B.C.D/mask.
- Port (advanced): narrows the match further by port; leave blank to match the whole subnet regardless of port.
- Rate (advanced): the guaranteed bandwidth (Kbps) the rule traffic can always use, required.
- Peak rate (advanced): the upper bandwidth (Kbps) it may borrow up to when the link is idle; leave blank for no cap.
- Priority (advanced): the scheduling priority when rules contend for bandwidth, 1-30, a smaller value is higher priority.



CHAPTER

07

Firewall

Filter traffic by port, address, and domain; harden management exposure.



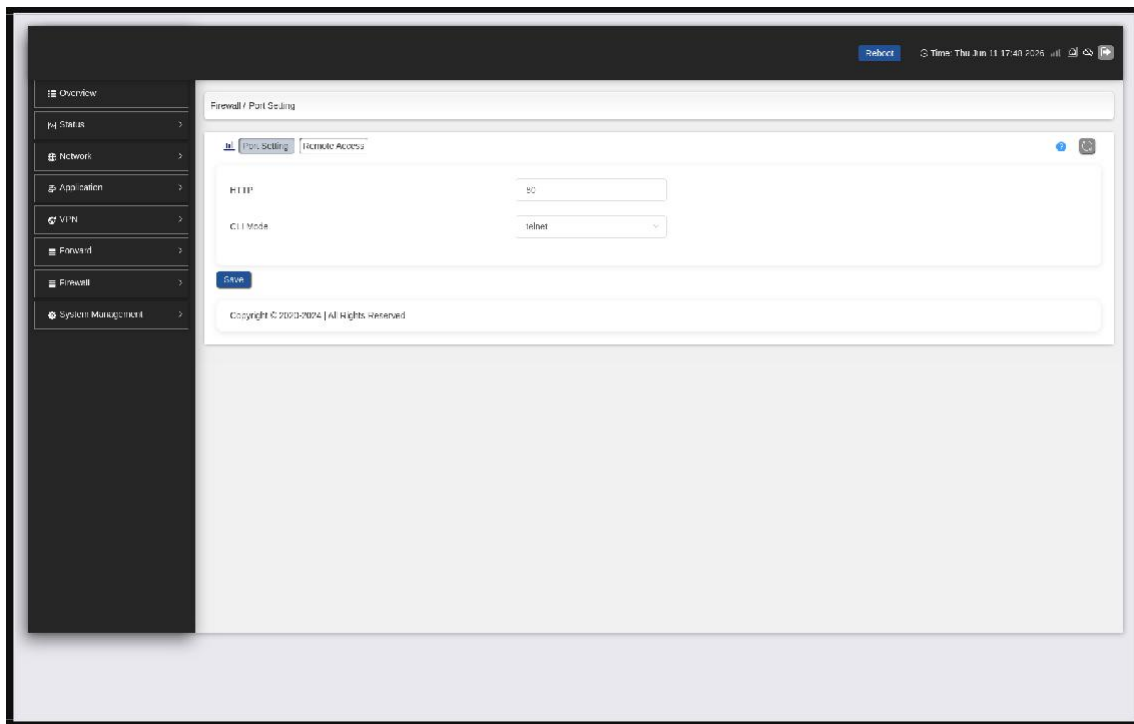
7. Firewall

7.1 Port & Remote Access

This page decides **who is allowed to manage the router, and on which port**. It controls two things:

1. **The TCP port each management service listens on** — HTTP (Web UI), HTTPS (Web UI over TLS), SSH, and the local CLI. Moving these to non-standard ports drastically cuts the volume of opportunistic Internet-wide scans hitting the router.
2. **Which direction each service may be accessed from** — `LAN only`, `WAN only`, or `LAN and WAN`. The factory default is **LAN only for everything**, which is the safe choice. Opening any service to the WAN side immediately exposes it to the entire Internet — proceed with care.

Figure 7-1-1. The Port & Remote Access configuration page.



Opening the Web UI to the WAN side exposes your management password to every IP on the Internet. Within minutes the router will receive hundreds of brute-force login attempts. Only open it to the WAN when you have **all three** of: a non-trivial admin password (Section 8.3), a non-standard port, and a source-IP allow list. Otherwise leave Web management as `LAN only` and reach the WAN-side management through a VPN.

HOW TO: MOVE SSH OFF PORT 22 TO DISCOURAGE SCANNERS

1. On this page, find the **SSH port** field.
2. Change `22` to a high-numbered port the scanners do not pick first — e.g. `34022`, `52022`. Any value from 1024 to 65535 works; avoid 22, 2222, 8022 which are common scan targets.
3. **Save.** The SSH daemon restarts within a second.
4. **Reconnect on the new port:** `ssh -p 34022 root@<router-ip>`.
5. Update any bookmarks, scripts, and configuration management tools that referenced the old port.

HOW TO: ALLOW ONLY THE OFFICE IP TO REACH THE WEB UI

This narrows the WAN-side attack surface to a single source.

1. On this page, set **HTTPS access direction** to `LAN and WAN`.
2. **Source allow list**: add the office's public IP. The router rejects any TLS handshake from a source outside the list.
3. **Save**.
4. **Test from the office IP** that the Web UI is reachable, and from a different IP (e.g. mobile tethering) that it is **not** reachable.

HOW TO: HARDEN THE ROUTER IN THREE MINUTES (RECOMMENDED BASELINE)

1. Change the admin password from the factory default to a strong unique password — **System Management** → **Account** (Section 8.3).
2. On this page, **disable WAN access for HTTP, HTTPS, SSH, and CLI**. Keep them on LAN only.
3. If you need remote management, set up a VPN (Chapter 5) and manage the router through the VPN's tunnel-side address.
4. Disable **PING from WAN** if you have no operational need for ICMP from the Internet.

FIELD REFERENCE

No.	Field	What to put there
1.	HTTP port	The TCP port the plain Web UI listens on. Default <code>80</code> . <code>0</code> to disable HTTP entirely (recommended — use HTTPS only).
2.	HTTPS port	The TCP port the TLS-encrypted Web UI listens on. Default <code>443</code> . Move to a high port when exposing to the WAN.
3.	SSH port	The TCP port the SSH service listens on. Default <code>22</code> . Strongly recommended to move when SSH is reachable from the WAN.
4.	CLI port	The TCP port the local CLI listens on (typically used by the router's own tooling). Change only when there is a port-conflict reason.
5.	Access direction	One of <code>LAN only</code> (factory default — safest), <code>WAN only</code> (rare — managed from public Internet only), <code>LAN and WAN</code> .
6.	Source allow list	When direction includes <code>WAN</code> , lists the public IPs / subnets allowed to reach the service. Empty = anyone.
7.	PING from WAN	Whether the router replies to ICMP echo from the WAN side. Disabling makes the router "invisible" to a casual scan, at the cost of losing a useful liveness check.

TROUBLESHOOTING

No.	Symptom	Likely cause	What to do
1.	"Cannot reach the Web UI after I changed the port."	The browser bookmark still points at the old port.	Use the new port in the URL: <code>http://<router>:<new-port></code> .
2.	Web UI works from inside the office but not when working from home.	Direction is <code>LAN only</code> , or the home IP is not in the allow list.	Either set direction to <code>LAN and WAN</code> (with allow list), or reach the router through a VPN.
3.	"Forgot the new SSH port."	The change took effect but then new value was not noted.	Connect over the Web UI (LAN side) and re-check this page. If even Web UI is unreachable, factory reset via CFE Recovery (Chapter 9).
4.	"I locked myself out of the router."	Both Web UI and SSH are set to <code>WAN only</code> and the WAN happens to have no public IP at the moment.	The same — factory reset via CFE Recovery. Avoid this by keeping at least one management path on <code>LAN only</code> .

CLI mode: the access mode of the command line (CLI).

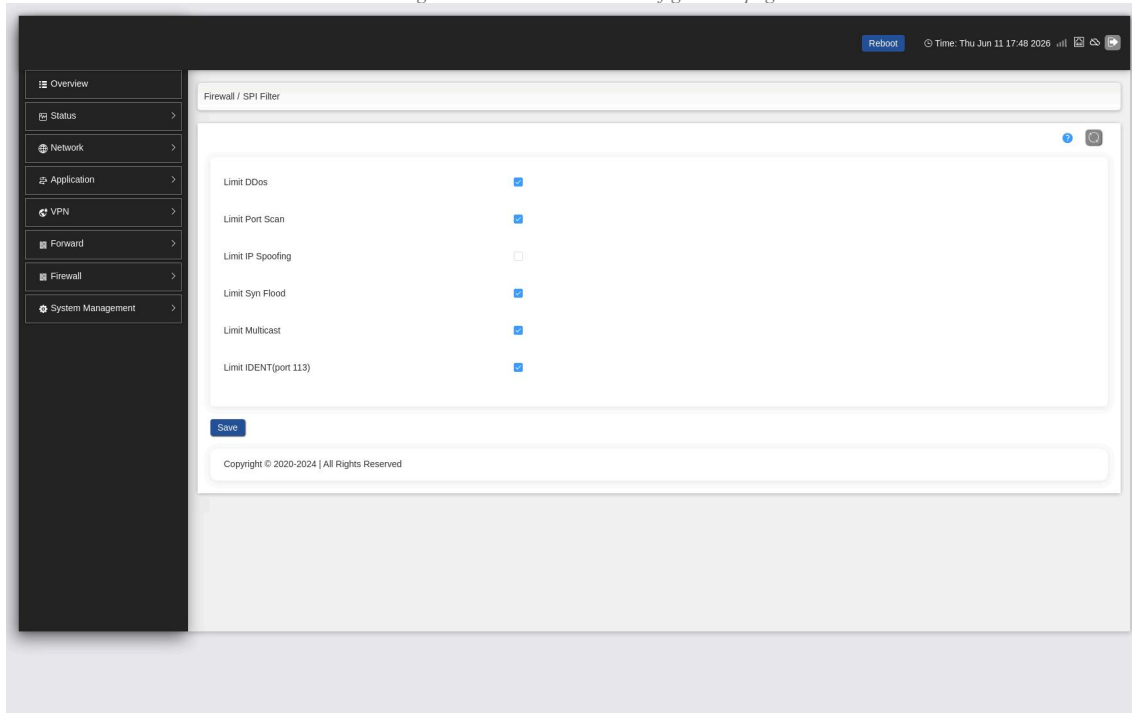
Remote-access matrix: each row is a management protocol (PING/WEB/SSH/CLI), each column a source direction (LAN/WAN/VPN); checked = access from that direction is allowed, unchecked = denied.

Security advice: unless remote management is genuinely needed, leave the WAN (public) column unchecked - especially for SSH/CLI/WEB - so the management entry is not exposed on the public network.

7.2 SPI Filter

SPI (Stateful Packet Inspection) is a set of protection switches against common network attacks. The device tracks connection state and identifies abnormal traffic; turning on a switch blocks the corresponding attack.

Figure 7-2-1. The SPI Filter configuration page.



OVERVIEW

Each switch is one class of attack protection, independent and individually toggled, acting mainly on abnormal traffic from the WAN side.

Leaving them all on is recommended - these protections do not affect normal Internet use and only block attack traffic.

PARAMETERS

Anti DoS/DDoS: blocks denial-of-service attacks - abnormally high-rate traffic floods.

Anti port scan: detects and blocks probing scans of the open ports of the device.

Anti IP spoofing: drops packets with a forged source address that does not match the ingress interface.

Anti SYN Flood: defends against TCP half-open connection floods (forged SYNs exhausting connection resources).

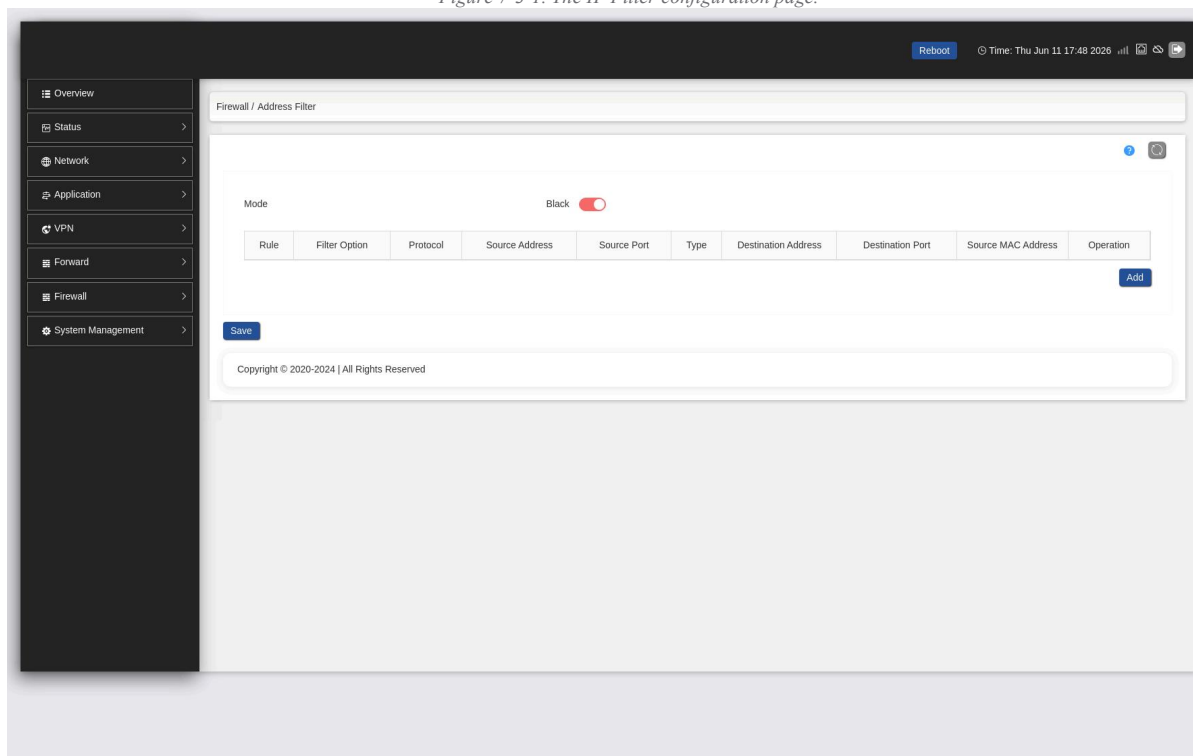
Limit multicast: filters multicast traffic.

Limit IDENT: limits the IDENT protocol (TCP 113) identity query, reducing the information-exposure surface.

7.3 IP Filter

Address Filter does access control by IP address and MAC address - it can restrict which internal devices reach the Internet, or restrict access to the device itself.

Figure 7-3-1. The IP Filter configuration page.



OVERVIEW

The switch at the top is both the master switch and the mode selector: off means no filtering; blacklist mode - traffic matching the rules in the table is denied and the rest allowed; whitelist mode - only traffic matching the rules is allowed and the rest denied.

The blacklist and whitelist each keep their own rule table, up to 5 rules per mode.

MAC address filtering is also on this page - via the Match type, choose to match by IP, by MAC, or by both. Rules on this page apply to IPv4 only.

PARAMETERS

Chain (direction): input - applies to traffic destined for the router itself (controls who can access the device); forward - applies to traffic routed through the device (controls whether internal devices can go online or reach each other).

Match type: match by IP, by MAC, or by IP and MAC together.

Protocol: TCP/UDP/ICMP, etc.; ports cannot be filled when ICMP is selected.

Source address / port: the IP of the initiator (a single IP or a CIDR subnet) and the port.

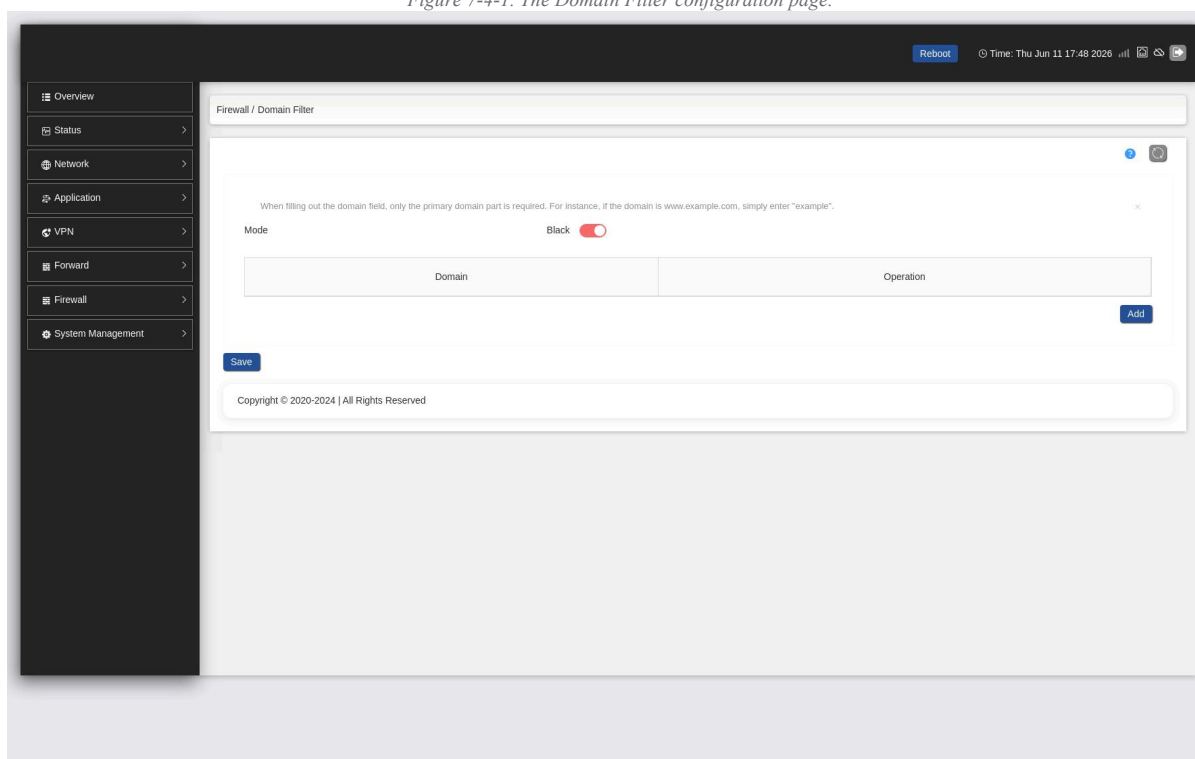
Type / Destination address / port: the destination can be a specific IP or subnet, or a chosen interface, narrowed further by destination port.

MAC address: matches by the hardware address of the network card, in the form XX:XX:XX:XX:XX:XX.

7.4 Domain Filter

Domain Filter controls the Internet access of internal devices by domain name / website, commonly used to block specific sites or to allow only specified sites.

Figure 7-4-1. The Domain Filter configuration page.



OVERVIEW

The switch at the top is both the master switch and the mode selector: off means no filtering; blacklist - the domains in the list are blocked and the rest allowed; whitelist - only the domains in the list are allowed and the rest blocked.

How it works: it matches keywords inside DNS query (port 53) packets - so a domain only needs its main part (for www.example.com just fill example) to catch related domains.

Limitations: it may not work for apps using encrypted DNS (DoH/DoT) or connecting by raw IP; the rules apply to the whole internal network and cannot be set per device.

PARAMETERS

Mode switch: three states - Disable / Blacklist / Whitelist; the blacklist and whitelist each keep their own list, up to 5 entries per mode.

Domain: the domain keyword to match. Fill only the main part of the domain (drop prefixes such as www. and the suffix); it is matched as a substring, and a hit is blocked or allowed per the current mode.

CHAPTER

08

System Management

Inspect logs, set time, manage user accounts, back up configuration, and upgrade firmware.

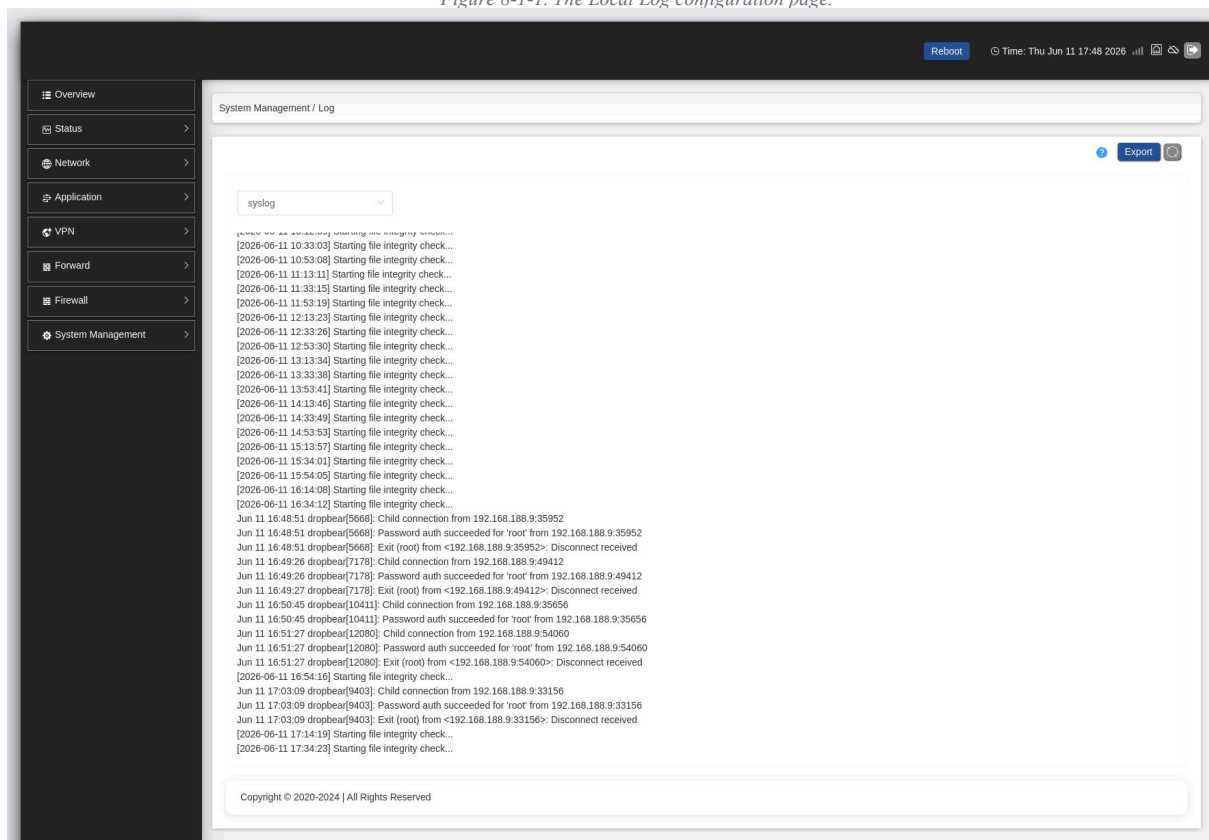


8. System Management

8.1 Local Log

This page shows the running logs of the device, the first source of evidence when troubleshooting - logs of different types can be browsed online and exported to a file.

Figure 8-1-1. The Local Log configuration page.



OVERVIEW

The log is shown online and refreshes automatically every few seconds; it can also be refreshed manually, and the view scrolls to the latest entries after a refresh.

Use the type drop-down to switch between logs of different sources.

PARAMETERS

Log type: syslog - the system log (services and network events, the most used); dmesg - the kernel log (drivers and hardware); modem - the cellular module / mobile-network log. The latter two depend on the model.

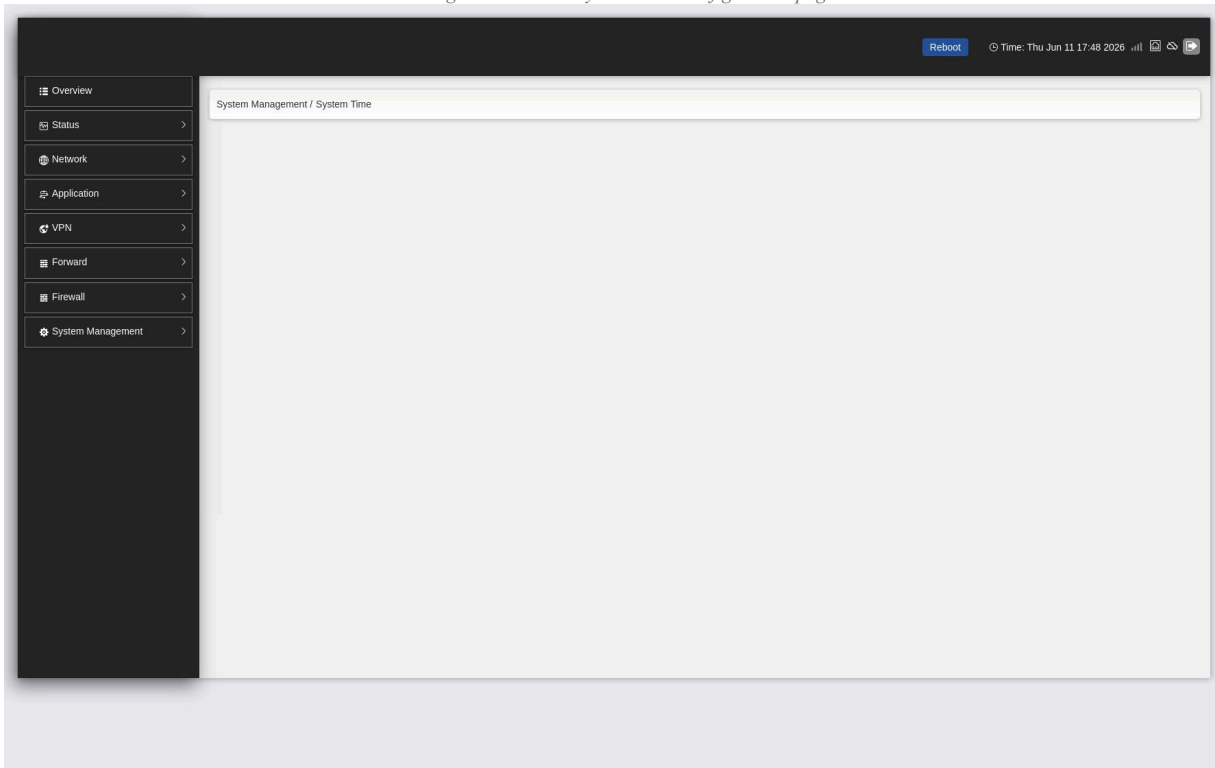
Export: downloads the current log type as a local file, for keeping or for sending to technical support.

Refresh: re-fetches the latest log immediately.

8.2 System Time

This page keeps the device clock accurate automatically via NTP (Network Time Protocol). An accurate system time is the prerequisite for correct log timestamps, scheduled tasks and certificate validation.

Figure 8-2-1. The System Time configuration page.



OVERVIEW

The switch at the top right enables or disables NTP auto time sync and takes effect immediately.

Once enabled, the device syncs time with the NTP server on the set interval; the State field shows whether the sync currently succeeds.

PARAMETERS

Primary NTP server: the preferred time server, selected from the list by default; tick Manual to enter a server domain or IP yourself.

Backup NTP server: the fallback used when the primary is unavailable, optional.

Sync interval: the number of seconds between two syncs (1-86400).

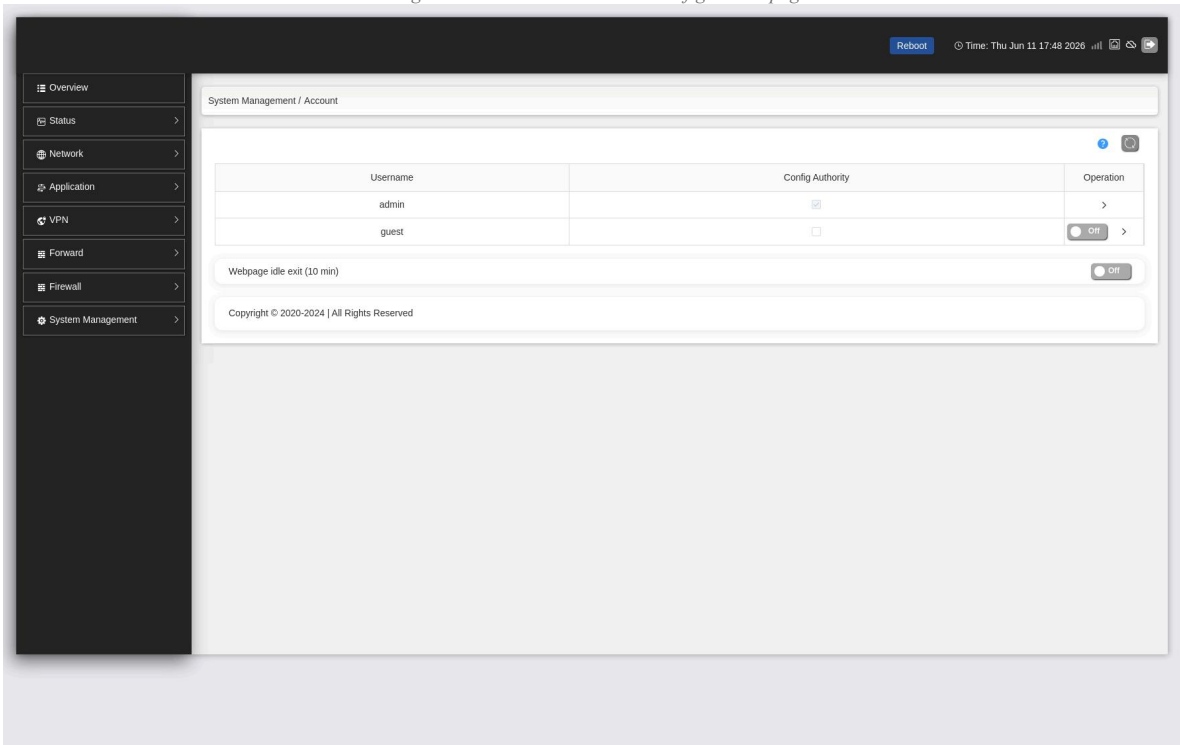
Time zone: the time zone of the device - set it correctly, otherwise the displayed time is off by a fixed offset.

State: read-only, shows whether NTP is currently connected and synced.

8.3 User Account

This page manages the accounts that log in to the device management interface - their permission level, enabled state, and login password.

Figure 8-3-1. The User Account configuration page.



OVERVIEW

Each row in the list is one account; the administrator account (admin) has a fixed permission that cannot be changed. Expand a row to change the login password of that account; after changing the password of the currently logged-in account, you are logged out and asked to log in again.

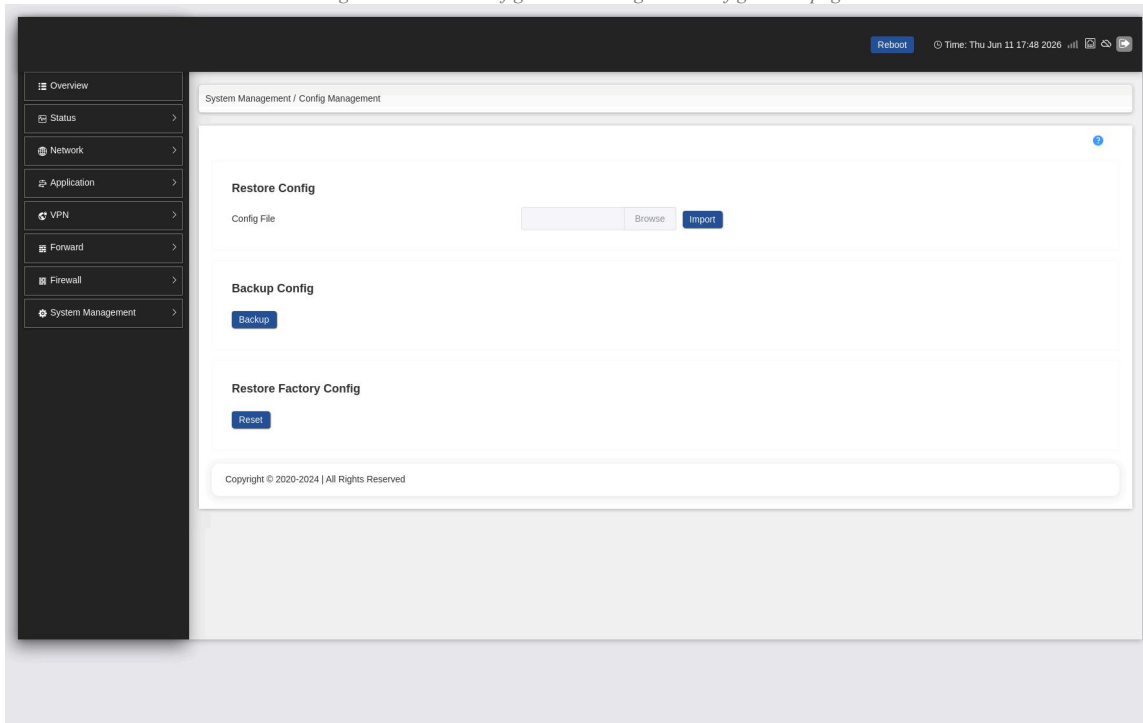
PARAMETERS

- Username: the login name of the account.
- Config permission: checked = the account may change settings; unchecked = a read-only account that can only view. The administrator account always has full permission.
- Enable switch: a non-administrator account can be enabled or disabled individually; once disabled the account cannot log in.
- Change password: expand the row and enter the new password and confirmation (an administrator changing the own password must also verify the old one); a password may only contain letters, digits and characters such as @ . - _ : .

▶ 8.4 Configuration Management

This page backs up, restores and resets the device configuration - backing up before a major change is recommended so you can roll back quickly if something goes wrong.

Figure 8-4-1. The Configuration Management configuration page.



OVERVIEW

Backup: exports all current settings of the device to a file saved locally.

Restore: reverts the device configuration from a previously backed-up file.

Reset to factory: clears all settings and returns the device to its factory initial state.

PARAMETERS

Backup: downloads the current configuration as a file at once; keep it safe for a later restore or for batch-deploying devices of the same model.

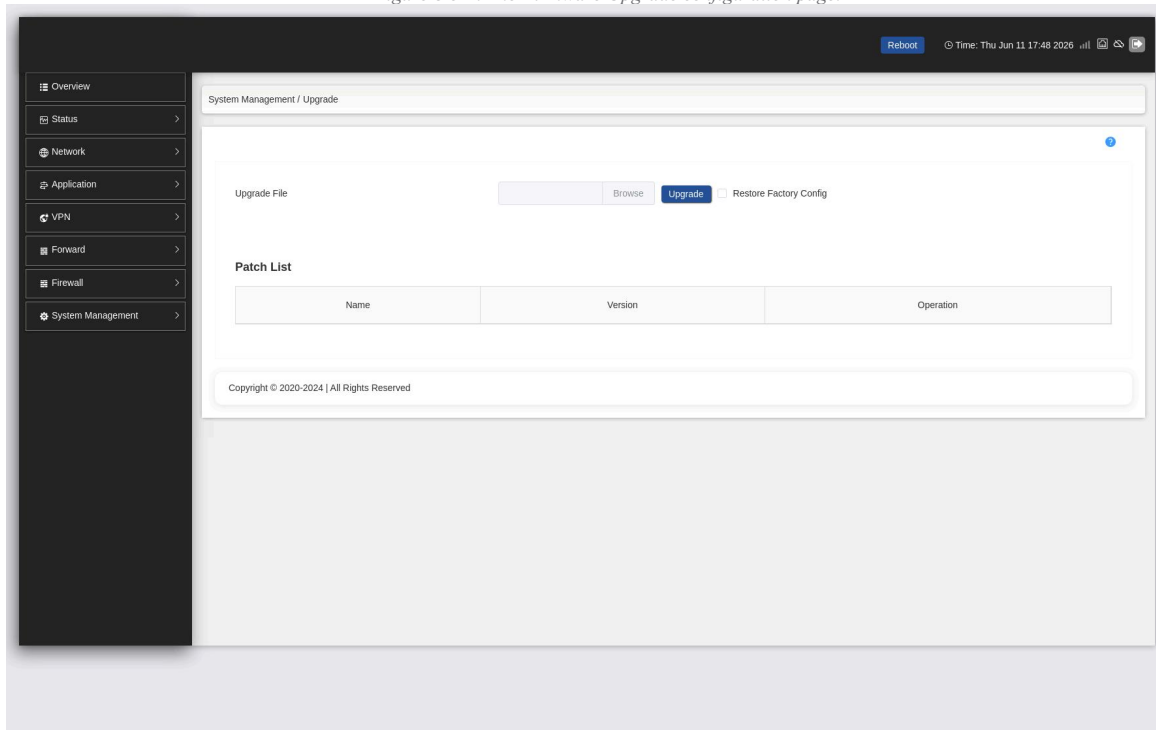
Restore: first Browse to select the configuration file, then click Import; importing reboots the device, do not cut power during it.

Reset to factory: after clicking Restore and confirming, the device clears its configuration and reboots, and all settings (including the management IP, account and password) return to factory defaults. The action cannot be undone - always back up first.

8.5 Firmware Upgrade

This page upgrades the device firmware and manages installed patches. Use a firmware file that matches this device model.

Figure 8-5-1. The Firmware Upgrade configuration page.



OVERVIEW

The upgrade is by local upload: select a firmware file and click Upgrade; once uploaded the device flashes it and reboots automatically.

The Patch List below shows the installed patches, which can be deleted individually.

During the upgrade do not cut power and do not close or refresh the page; the whole process takes a few minutes and returns to the login page when done.

PARAMETERS

Firmware file: click Browse to select the local firmware package (make sure it matches the device model - flashing the wrong firmware may make the device unbootable).

Reset to factory: checked = clear the configuration and reset to factory while upgrading; unchecked (default) = keep the current configuration. Ticking it is recommended for a major-version upgrade to avoid incompatible old settings.

Patch list: lists the name and version of installed patches, which can be deleted one by one.



CHAPTER

09

CFE Recovery Upgrade

Low-level boot-loader
recovery for units that no
longer boot the normal Web UI.



9. CFE Recovery Upgrade

“

CFE recovery is a low-level upgrade procedure that runs from the device's boot loader rather than from the running operating system. Use it when the router no longer boots, when a standard Web UI upgrade has failed, or when the unit needs to be force-restored to a known-good firmware image before deployment.

9.1 When to Use CFE Recovery

The Web UI upgrade procedure described in **Section 8.5** is suitable for everyday firmware updates and is the recommended path in normal operation. CFE recovery should be reserved for the following situations:

No.	Situation	Why CFE recovery
1.	The device hangs at boot, never reaches the Web UI, and only the SYS LED blinks abnormally.	The operating system image may be corrupted; CFE lives in a separate flash partition and can re-flash the OS partition.
2.	A previous Web UI upgrade was interrupted (power loss, network drop, browser closed) and the unit no longer responds.	CFE can write a clean firmware image without relying on the operating system.
3.	You need to downgrade to a much older firmware that the running OS refuses to install.	CFE does not enforce version-compatibility checks, so it accepts any firmware that matches the hardware.
4.	A new unit from stock needs a customer-specific image flashed before shipment.	Production lines commonly use CFE recovery for batch provisioning.

!

CFE recovery overwrites the system partition unconditionally. Any configuration that has not been exported via **System Management** → **Configuration Management** will be lost. Always export the running configuration first when the unit is still bootable.

9.2 What You Need

Prepare the following before you start. Mismatched cables or an unmatched firmware package are the two most common causes of a stalled recovery.

No.	Item	Notes
1.	A workstation with a wired Ethernet port and a modern browser.	Windows / macOS / Linux all work. Wireless-only laptops will not work for CFE recovery; the procedure requires a direct cable to the router.
2.	A short, straight-through Ethernet cable.	Plug it directly between the workstation and the router's LAN port; do not pass through a switch or router.
3.	The recovery firmware package.	A <code>SYS*.ent</code> file released by the manufacturer for the exact model (for example <code>SYS_VT-LTE500V1.x.x.ent</code>). Flashing firmware for a different model or hardware version may prevent the unit from booting.

I

CFE recovery overwrites the system partition unconditionally. Any configuration that has not been exported via **System Management** → **Configuration Management** will be lost. Always export the running configuration first when the unit is still bootable.

9.3 Enter CFE Upgrade Mode

The router enters CFE recovery mode when the **Reset** button is held across the power-on sequence. Follow these steps in order:

1. Power the router off (disconnect the DC adapter or PoE injector).

2. Connect the Ethernet cable from your workstation to the router's **LAN** port.
3. Set the workstation's wired adapter to a static address in the `192.168.1.0/24` subnet, for example `192.168.1.100 / 255.255.255.0`. The recovery loader uses `192.168.1.1` as its own address.
4. Press and **hold** the **Reset** button on the rear of the unit.
5. While still holding **Reset**, reconnect power. Keep the button held for approximately 8-10 seconds, until the LEDs first blink and then change to **all on (steady)** — that is the recovery-mode indicator.
6. Release the **Reset** button. The unit is now ready to accept a firmware upload over HTTP on `192.168.1.1`.

i LED pattern as a state indicator. The CFE recovery sequence is: power-on → brief LED flicker → **all LEDs solid on**. If instead the unit comes up with its normal boot animation (SYS solid green, network LEDs blinking with traffic), recovery mode was not entered — power-cycle the unit and repeat the button-hold, slightly longer.

9.4 Web Recovery Upload

With the unit in CFE recovery mode and the workstation on the `192.168.1.0/24` subnet, the firmware is uploaded through a browser:

1. Open a browser on the workstation and navigate to `http://192.168.1.1`. The CFE recovery page loads within a few seconds.
2. Click the **Browse** (or **Choose File**) button on the recovery page and select the `SYS*.ent` file you prepared in Section 9.2.
3. Click **Upgrade** to start the write. The page may show a progress bar; some versions just show a "writing" message.
4. **Wait approximately 5 to 10 minutes.** The unit looks idle for most of this period but is busy decompressing the package and writing flash. Do not touch the cables, do not refresh the browser, and do not power the unit off.
5. When the write is finished, the unit restarts automatically. The recovery page becomes unresponsive (this is normal — the unit has left CFE mode) and the LEDs return to their normal post-boot pattern.

! Block out 10 minutes before touching anything. The flash write is the longest single step. Interrupting it part-way through may corrupt the boot loader itself, at which point only a factory re-flash can save the unit. If the LEDs go dark or the workstation loses link mid-write, leave everything connected and wait until the 10-minute window expires before reacting.

9.5 Verification

After the unit restarts:

1. Power-cycle the unit **once more** to confirm the new firmware survives a cold start (a recovery image that boots once but not twice is a sign of a partially-written flash).
2. Restore the workstation's wired adapter to its normal address (DHCP, or whatever was in use before recovery).
3. Move the cable to one of the LAN ports and open the device's normal management address `http://192.168.1.1` (by default) in the browser.
4. Log in with the default credentials and navigate to **System Management** → **Upgrade**. The displayed firmware version should match the `SYS*.ent` package you just flashed.
5. If you had exported a configuration earlier, restore it via **System Management** → **Configuration Management** → **Import**.

9.6 Trouble shooting

No.	Symptom	Likely cause	Action
1.	The LEDs never go to "all on" after the button hold.	The Reset button was not held long enough, or was pressed <i>after</i> power-up rather than across the boot.	Power off completely, hold Reset before applying power, keep holding for at least 10 seconds.

No.	Symptom	Likely cause	Action
2.	The browser cannot reach <code>http://192.168.1.1</code> .	The cable is plugged into the wrong port (CFE recovery uses a LAN port), the workstation has the wrong static IP, or the firewall on the workstation is blocking HTTP.	Move the cable to a LAN port, set the workstation to <code>192.168.1.100/24</code> , disable the workstation firewall on the wired interface for the duration of the recovery.
3.	The upload completes but the device never restarts.	The selected file was not a valid <code>SYS*.ent</code> package, or the package is for a different hardware revision.	Cancel, return to step 1, select a <code>SYS*.ent</code> file that matches the model label on the bottom of the unit.
4.	The unit restarts but the Web UI is unreachable on the new firmware.	The firmware package and the hardware do not match (e.g. wrong regional package or a wrong-platform image).	Re-enter CFE mode and recover with the correct package. Double-check the model label against the file name before clicking Upgrade .
5.	After flashing, the unit reverts to the previous firmware on the second reboot.	The flash write completed but did not commit. This is rare and indicates a CFE issue specific to certain hardware revisions.	Repeat the recovery; if it persists, contact your distributor with a screenshot of the recovery page attached.