ICR-1600

Router Family User Manual

Applies to firmware 1.4.6

Scan to open online documentation

Introduction

Manual Compatibility

This manual is compatible with firmware: 1.4.6

What You'll Find in This Manual

This manual provides comprehensive information for setting up, operating, and managing your Advantech router. It covers both hardware and software aspects of the device.

- Product Overview
  Product family introduction, model overview, hardware components, package contents, and revision history.
- Hardware and Connectivity
  SIM card slots, antenna connections, Ethernet interfaces, power supply, serial ports, and LED indicators.
- Mounting and Installation
  Product dimensions, mounting options, and installation guidelines.
- Initial Configuration
  First-time setup covering hardware preparation, web interface access, and administration environments.
- Functionalities and Scenarios
  Key functionalities of Advantech routers and examples of typical usage scenarios.
- Status Pages
  Describes the device's web pages that display the router's current status and performance metrics.
- Configuration Pages
  Provides details about all web pages used to configure the device settings and network parameters.
- Customization Pages
  Explains how to extend the device's functionality, primarily through the installation of Router Apps.
- Administration Pages
  Describes the web pages used for managing and administering the device, including system maintenance.
- Technical Parameters
  Detailed technical specifications, certifications, and module parameters.

Product Overview

Introduction

The **ICR-1600 product family** consists of LTE connectivity gateways with Gigabit Ethernet, designed for cost-effective industrial connectivity. The family ranges from the ICR-1602 with two Gigabit Ethernet ports, through the ICR-1642 adding serial interfaces and digital I/O, up to the ICR-1645 with a five-port Gigabit Ethernet configuration. For additional details, see Functionalities and Scenarios.

The secure, password-protected **web interface** enables users to monitor detailed statistics, including activity logs, signal strength, and system logs. For guidance on first-time setup, refer to Initial Configuration.

Model Overview

The ICR-1600 product family includes several models, each tailored to specific regions and applications. The table below summarizes the available models and their features.

> **Tips**
>
> Order code suffixes: **W** = Wi-Fi module, **G** = GNSS module; **-EU** = EMEA models certified with CE/UKCA, **-CN** = models for China. Not all suffix combinations are available for every model — consult your local sales representative.

Order Code	Region	Cellular	ETH	I/O	Serial	SIM	WiFi	GNSS
ICR-1602-EU-A ↗	EMEA	LTE	2	–	–	✓	–	–
ICR-1602-CN-A ↗	CN	LTE	2	–	–	✓	–	–
ICR-1642-EU-A ↗	EMEA	LTE	2	✓	✓	✓	–	–
ICR-1642W-EU-A ↗	EMEA	LTE	2	✓	✓	✓	✓	–
ICR-1642G-EU-A ↗	EMEA	LTE	2	✓	✓	✓	–	✓
ICR-1642-CN-A ↗	CN	LTE	2	✓	✓	✓	–	–
ICR-1642W-CN-A ↗	CN	LTE	2	✓	✓	✓	✓	–
ICR-1642G-CN-A ↗	CN	LTE	2	✓	✓	✓	–	✓
ICR-1645-EU-A ↗	EMEA	LTE	5	✓	✓	✓	–	–
ICR-1645W-EU-A ↗	EMEA	LTE	5	✓	✓	✓	✓	–
ICR-1645G-EU-A ↗	EMEA	LTE	5	✓	✓	✓	–	✓

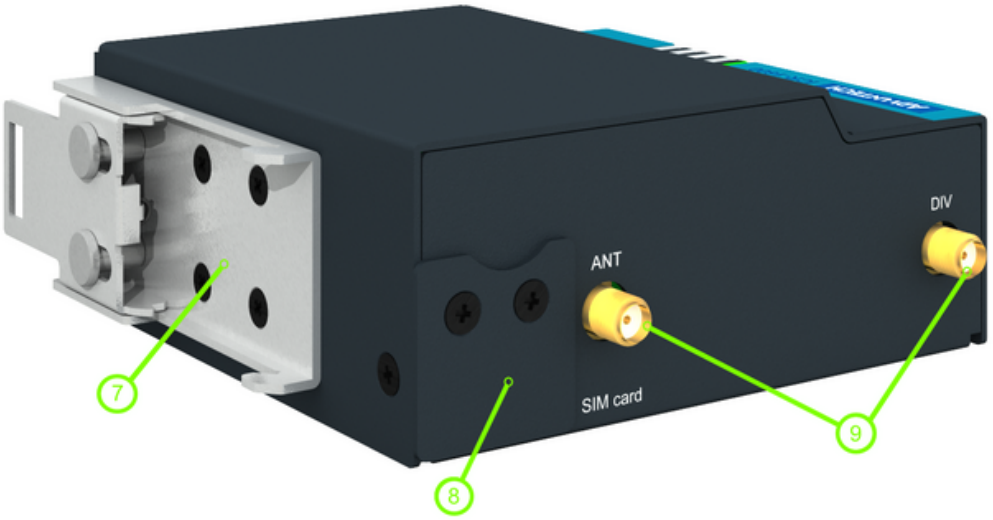
Order Code	Region	Cellular	ETH	I/O	Serial	SIM	WiFi	GNSS
ICR-1645-CN-A ↗	CN	LTE	5	✓	✓	✓	–	–
ICR-1645W-CN-A ↗	CN	LTE	5	✓	✓	✓	✓	–
ICR-1645G-CN-A ↗	CN	LTE	5	✓	✓	✓	–	✓

✓ = included · – = not available · hover a heading or cell for details

Hardware Components

The ICR-1600 series supports the hardware features illustrated in the image below (ICR-1602 shown). Refer to the Model Overview section for model-specific details.

#	Caption	Type	Description
1	RST	—	Button to reboot the router or restore the defaults; see Reset.
2	LEDs	—	Status LED indicators; see LED Indicators.
3	GND Screw	M3	Ensure proper grounding; see Power Supply.
4	PWR	2-pin terminal	Power supply socket; see Power Supply.
5	ETH0, ETH1	RJ45	1 Gb Ethernet LAN interfaces; see Ethernet Interfaces.
6	Wall Clip	—	Wall mounting clip, included as a standard accessory; see Wall Mounting.



#	Caption	Type	Description
7	DIN Clip	—	DIN mounting clip, **not included** as a standard accessory (can be ordered optionally); see DIN Rail Mounting.
8	SIM Slots	Micro SIM	Two Micro SIM card slots; see SIM Card Slots.
9	ANT, DIV	SMA	Connectors for the main and diversity antennas of the cellular module; see Antenna Connections and Cellular Module Parameters.

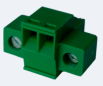
Model differences

- The **ICR-1642** and **ICR-1645** additionally provide a 10-pin **Serial & I/O terminal** (RS232, RS485, one digital input, and one digital output); see I/O Parameters.
- The **ICR-1645** has five Gigabit Ethernet ports (ETH0 four-port switch plus ETH1) and an **AUX** antenna connector; its DIN clip and wall clip placement also differs from the smaller models.

Package Contents

Each router package includes the following:

Item	Description	Image	Quantity
Router	ICR-1600 series router		1
Wall Mount Kit	Packed in the accessory box, including four M3 × 5L screws		1

Item	Description	Image	Quantity
Power Terminal Block	2-pin terminal block for the power supply; pre-installed on the router		1
Serial & I/O Terminal Block	10-pin terminal block; ICR-1642 and ICR-1645 only, pre-installed on the router		1
LTE Antennas	Packed in the accessory box		2 pcs
Wi-Fi Antenna	Packed in the accessory box; Wi-Fi models only		1
Quick Start Guide	Printed quick start guide included in the package		1

Hardware and Connectivity

Refer to the Hardware Components section for a detailed summary of the product's hardware.

SIM Card Slots

The router has two SIM card slots located beneath a metal cover. To communicate over a cellular network, insert an activated, data-provisioned SIM card into a SIM card slot. You can install two SIM cards simultaneously to use the SIM switching feature. You can configure each SIM card with a different APN (Access Point Name).

Tips

SIM card type: **Micro SIM (3FF)** — 15.0 × 12.0 × 0.76 mm.

Changing the SIM Card

1. Always disconnect the router from the power supply before handling the SIM card.
2. Unscrew the two screws on the SIM card cover and remove the cover.
3. To remove an inserted SIM card, use the flat end of a spudger or your fingernail. Press the card slightly into its slot until you hear a click. Release the card; it will pop out of its slot.
4. To insert a SIM card, push the card into the slot until it clicks into place.
5. Replace the cover and tighten the two screws.

If the SIM card requires a PIN, enter it in the router's web interface under **Administration** → **Unlock SIM Card**.

Antenna Connections

Two SMA female connectors — **ANT** (main) and **DIV** (diversity) — are provided for connecting cellular antennas to the router. On models with Wi-Fi or GNSS support, an additional connector labeled **AUX** is located on the router: an RP-SMA female connector for the Wi-Fi antenna, or an SMA female connector for the GNSS antenna.

Warning

Always operate the router with a cellular antenna securely connected to the cellular antenna connector. Transmitting without an antenna attached causes RF energy to be reflected at the open connector, which can permanently damage the radio circuitry. Ensure the antenna is properly installed before powering on or transmitting.

Tips

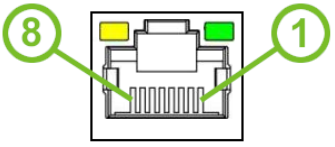
The recommended tightening torque for the antenna SMA connectors is 0.9 Nm.

Ethernet Interfaces

Tips

Model ICR-1645 provides four switched **ETH0** ports and one **ETH1** port. All other models provide one **ETH0** port and one **ETH1** port.

All Ethernet interfaces are accessible via RJ45 panel sockets and support speeds up to 1 Gbps.



Pin	10BASE-T & 100BASE-T	1000BASE-T
1	Tx+ (Transmit Data+)	BI_DA+ (BiDirectional pair A+)
2	Tx− (Transmit Data−)	BI_DA− (BiDirectional pair A−)
3	Rx+ (Receive Data+)	BI_DB+ (BiDirectional pair B+)
4	—	BI_DC+ (BiDirectional pair C+)
5	—	BI_DC− (BiDirectional pair C−)
6	Rx− (Receive Data−)	BI_DB− (BiDirectional pair B−)

Pin	10BASE-T & 100BASE-T	1000BASE-T
7	—	BI_DD+ (BiDirectional pair D+)
8	—	BI_DD− (BiDirectional pair D−)

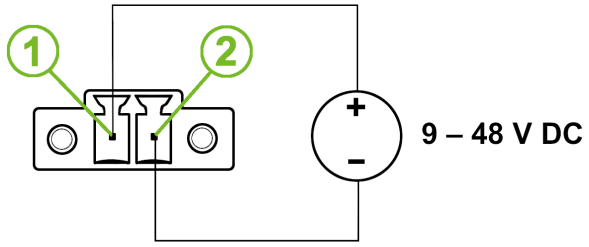
Tips

The isolation barrier of the Ethernet ports from ground is 1500 V.

Power Supply

A two-pin terminal connector (pitch 3.5 mm) is used to power the router. The matching connector is included as a standard accessory.

Pin	Signal	Description
1	VCC(+)	Positive pole of DC supply voltage (+9 to +48 V DC)
2	GND(−)	Negative pole of DC supply voltage



The required supply voltage is +9 to +48 V DC. The router has built-in protection against reversed polarity without signaling.

Warning

- Grounding the router using the grounding screw eliminates the protection against reversed polarity. Ensure the negative pole of the DC supply shares the same voltage reference as the grounding screw. A voltage difference between these points may damage the router; only an authorized service center can perform repairs.
- Use a power supply specified as a Limited Power Source (LPS) or a CEC/NEC Class 2 power supply.

Tips

The power supply common pole is not connected to the router's metal chassis or internal ground.

To protect the router, ground it using the grounding screw as shown below. The maximum tightening torque for the grounding screw is **0.6 Nm**.

LED Indicators

Status LEDs are located on the top side of the router. The ETH0 and ETH1 connectors on the front panel each have two additional LEDs showing the port status.

Symbol	Caption	Color	State	Description
	PWR	Green	On	The router is starting up.
		Green	Blinking	The router is ready (heartbeat).
		Off	Off	The router has no power.
	SIG	Green	On / Blinking	Good cellular signal.
		Orange	On / Blinking	Fair cellular signal.
		Red	On / Blinking	Poor cellular signal.
		Off	Off	No cellular link.
	SIM	Green	Blinking	SIM1 is selected, waiting for a data connection.
		Orange	Blinking	SIM2 is selected, waiting for a data connection.
		Green	On	SIM1 is active for the cellular connection.
		Orange	On	SIM2 is active for the cellular connection.
		Red	Fast blinking	A SIM issue (missing card or PIN not entered).
		Off	Off	No SIM card is selected.
	USR	Green	—	The function of this LED is user-defined.

Symbol	Caption	Color	State	Description
	ETH0, ETH1	Green	On	Selected 1 Gbps bit rate.
		Green	Off	Selected 100/10 Mbps bit rate.
		Yellow	On	Network cable connected.
		Yellow	Brief off blinks	Data transmission.
		Yellow	Off	Network cable not connected.

The following describes the USR LED states when configured for Serial or Wi-Fi:

Symbol	Caption	Color	State	Description
	Serial/USR	Green Off	Blinking Off	Serial Port 1 TX/RX transmitting data. No RS232/RS485 data.
	Wi-Fi/USR	Green Green Off	On Blinking Off	AP or STA mode is selected. Transmitting data. No AP or STA mode is selected.

Reset Options

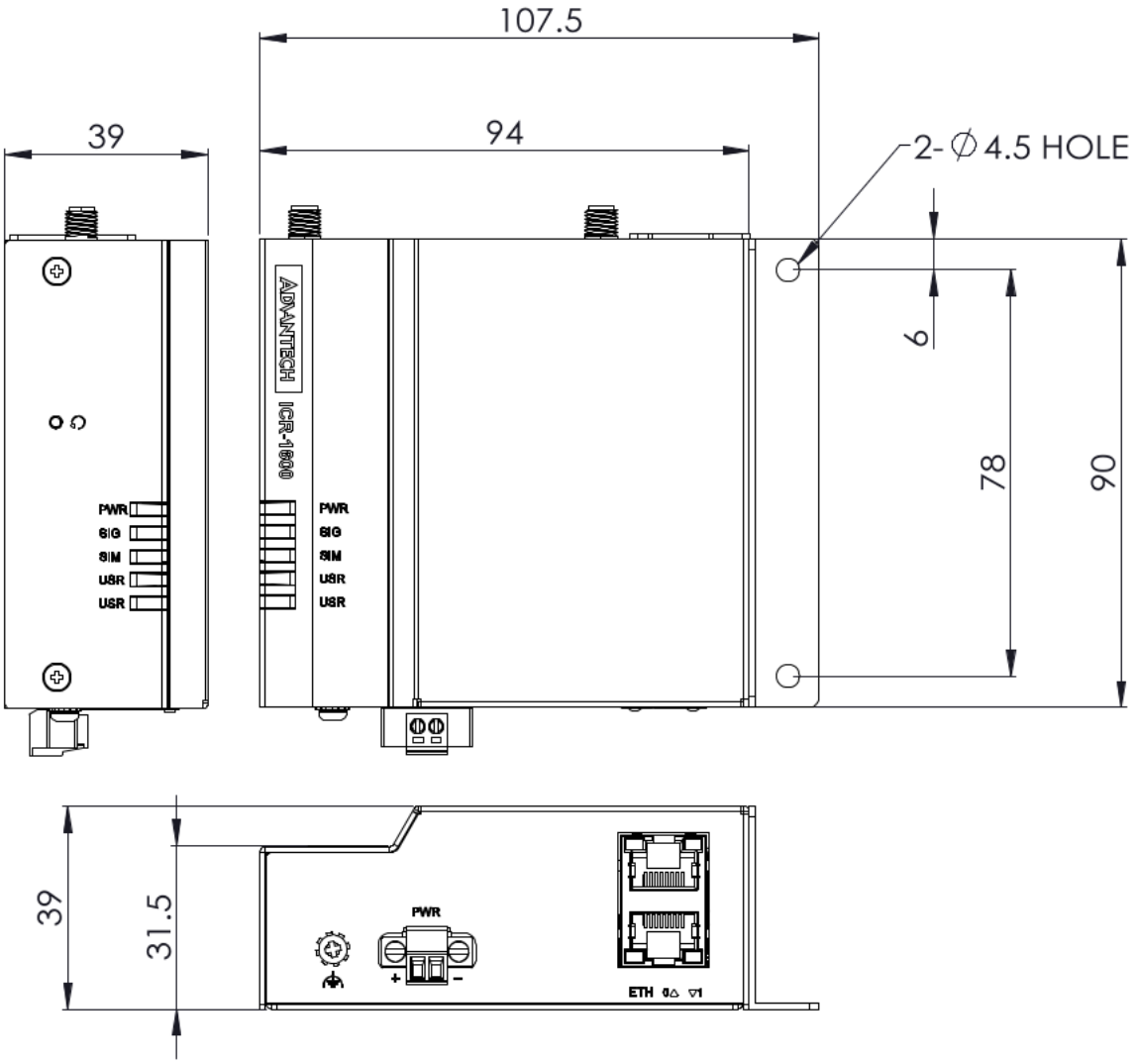
The **RST** button is located in a small opening on the router panel and has multiple functions. For details, refer to Initial Configuration → Reset.

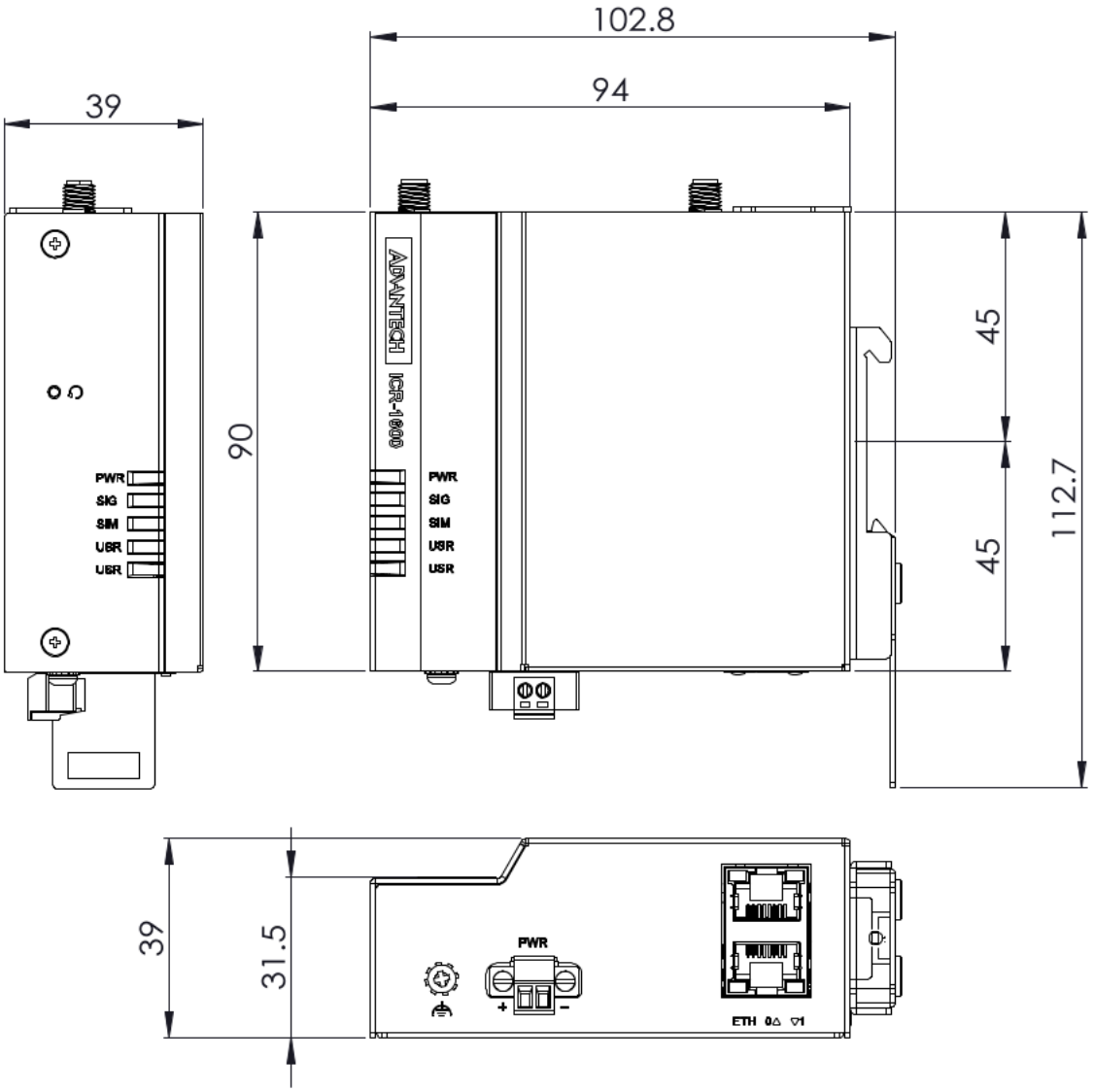
> **Tips**
>
> Use a narrow screwdriver or a small tool to press the RST button.

Mounting and Installation

Product Dimensions

Refer to the diagrams below for detailed measurements (in millimeters).





Mounting Options

The router can be installed in the following ways:

1. **On a Flat Surface**: Place the router on a stable, flat surface.
2. **On a Wall**: Use the wall-mounting clip provided with the router. Refer to the Wall Mounting section for detailed instructions.
3. **On a DIN Rail**: Mount the router using the metal DIN rail clip in compliance with EN 60715 standards. Refer to the DIN Rail Mounting section for additional details.

For most applications involving a built-in router within a switchboard, consider the following environmental types:

- **Non-public industrial environments**: Low voltage with high interference.
- **Public environments**: Low voltage without high interference.

For both cases, mounting the router to a switchboard eliminates the need for additional immunity or EMC-related examinations under EN 61439-1:2011.

Guidelines for Mounting

In compliance with EN 61439-1:2011, observe the following assembly instructions when mounting the router inside a switchboard:

- When using whip antennas, maintain a minimum distance of 6 cm from cables and metal surfaces on all sides to minimize interference.
- Use a lightning conductor for external antennas mounted outside the switchboard.
- When mounting the router on sheet-steel, use a cable antenna.
- Bundle power supply and data cables, ensuring:
  - The combined cable length does not exceed 1.5 m.
  - Surge protectors are installed if data cables exceed 1.5 m or run toward the switchboard.
  - Data cables are not bundled with mains voltage cables (230 V/50 Hz or 120 V/60 Hz).
- Leave sufficient space between connectors for easy cable handling.
- Use an earth-bonding distribution frame to properly ground the router's grounding screw.

Wall Mounting

Tips

The wall-mounting clip is included as a standard accessory, packed in the accessory box together with four M3×5L screws.

The router can be affixed to a wall or similar surface using the wall-mounting clip. The clip has two holes with a diameter of 4.5 mm for screw placement. Refer to the Product Dimensions section for precise spacing.

Warning

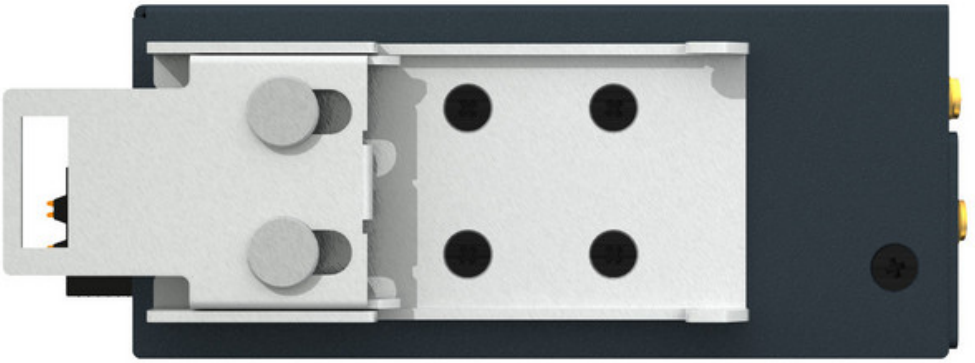
Tighten the wall-mounting clip screws to a maximum torque of 0.6 Nm.

DIN Rail Mounting

Tips

The DIN rail clip is not included as a standard accessory. It can be ordered separately using order code **OPT1-DIN-ICR1X-00**.

The DIN rail clip can be attached to the router for mounting on a DIN rail compliant with EN 60715 standards. The clip can be rotated into all four positions. The default clip position is shown below.



Warning

When attaching the DIN rail clip, use four M3×5L screws and tighten to a maximum torque of 0.6 Nm.

Initial Configuration

Configuration Environments

Caution

To ensure a secure deployment, it is crucial to evaluate the potential risks associated with your specific implementation and to configure the router accordingly to minimize these threats. We strongly recommend consulting the Security Guidelines ↗ application guide, which outlines fundamental security risks and provides recommended settings for their mitigation.

Warning

- If you are unsure about the correctness of your configuration or its potential impact on the router's longevity, consult our technical support for guidance.
- Before putting the router into operation, make sure to connect all the components required for running your applications. Refer to the Hardware and Connectivity and Mounting and Installation chapters for details. **Do not operate** the router **without an antenna** connected to the main antenna connector. Transmitting energy into an open connector may cause damage to the equipment.
- For security reasons, we recommend regularly updating the router's firmware to the latest version. Downgrading the firmware to an older version than the production version or uploading firmware intended for a different device may cause the device to malfunction.
- Enable JavaScript in your browser; otherwise, field validation and some functions are disabled.
- Three unsuccessful login attempts will block HTTP(S) access from the IP address for one minute.
- All routers have the *WebAccess/DMP* client pre-installed by default. The activated client periodically uploads router identifiers and configuration to the *WebAccess/DMP* server. See Remote Management Platform for more information.

You can use one of the following environments to configure an Advantech router:

- Via a **graphical interface** accessible in a **web browser**. This option is primarily covered in this manual, start with Web Interface Initial Setup.
- Via a **console interface** accessing the router by **Secure Shell** (SSH). For console configuration commands, refer to the Command Line Interface application guide.
- Via Advantech's **remote device management** platform, WebAccess/DMP ↗, which provides extensive management and monitoring capabilities to ensure devices remain secure and up-to-date. For more information, refer to Remote Management Platform.

For more information on enhancing the router's basic functionality, refer to the Extending Router Functionality ↗ application guide.

Web Interface Initial Setup

Caution

Starting with firmware version 6.5.0, both IPv4 and IPv6 firewalls are enabled by default. These firewalls permit only traffic originating from the default `192.168.1.0/24` network. Proper configuration of these settings is critical to avoid unintentionally blocking router communication during initial setup.

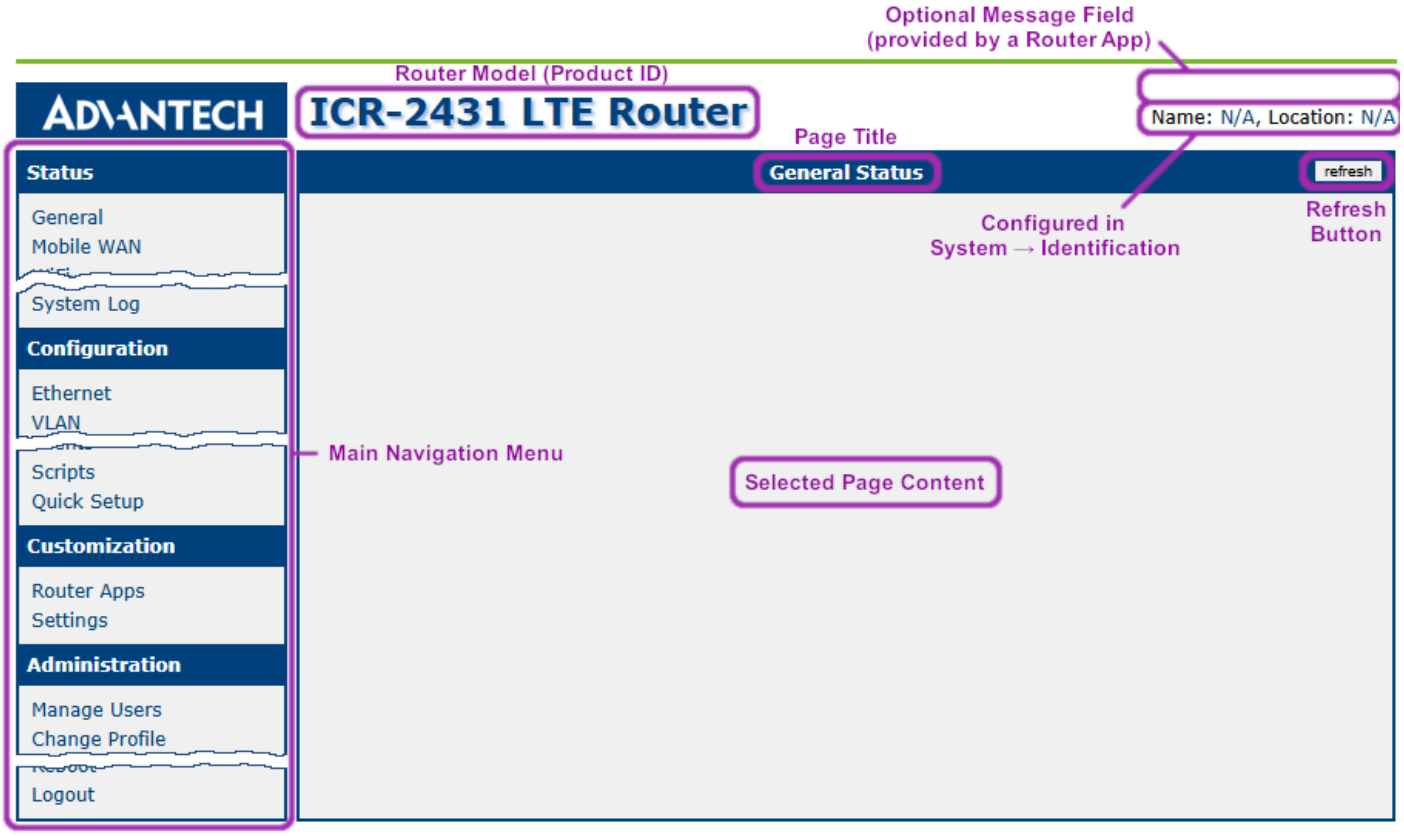
Tips

- Users with the *User* role have read-only access to the web interface, except for the *Modify User* functionality. Certain menu items remain unavailable to non-admin users.
- On a new router, or after a factory reset, the *Quick Setup* page is displayed immediately after login, allowing for a streamlined initial configuration; see Quick Setup for details.
- When configuring text fields in the web interface, consult Allowed and Restricted Input Characters for permitted character sets.
- The router's *Name* and *Location* fields in SNMP settings control the display in the interface's upper-right corner — detailed in SNMP.

GUI Tips

- Throughout the web interface, helpful information is displayed to the right of many input fields. For numeric items, this includes the valid range and unit.
- When you hover over an input field, a tooltip shows the item's internal configuration name — useful for scripting or remote configuration via *WebAccess/DMP*.

Advantech routers feature a secure web-based configuration interface accessible via HTTPS. This interface provides real-time network statistics, signal strength monitoring, system log access, and comprehensive device management capabilities. The web interface enforces TLS 1.2 or higher for all connections, with certificate validation required to prevent man-in-the-middle attacks.



Web GUI layout overview

To establish initial web interface access on a factory-default router:

- First, ensure proper hardware preparation. For cellular models, insert an active SIM card that is compatible with your carrier's frequency bands and verify the required APN configuration. See SIM Card Slots for SIM card insertion instructions.
- Attach all required antennas before powering the device, including Wi-Fi antennas for dual-function models. For connector locations and antenna types, see Antenna Connections. Connect the power supply using only Advantech-approved adapters specified in Power Supply and Grounding.
- During the boot process, the router initializes its DHCP server on the ETH0 interface. Configure connected devices to obtain IP addresses automatically via DHCP.
- The default LAN interface (ETH0) assigns addresses from the `192.168.1.0/24` pool, with the router itself at `192.168.1.1`. Access the web interface by navigating to https://192.168.1.1 ↗ in a modern browser, noting that HTTP connections are strictly prohibited.
- The factory-default administrator account uses the username `root`. The password for this account appears on the router's product label, with `root` serving as the fallback credential if no label information exists.
- Upon first login, you must change the default password. After setting a new password, you are automatically directed to the *Quick Setup* page for the initial configuration.
- To prevent certificate warnings, install the router's self-signed certificate or a third-party CA-signed certificate using the procedures outlined in Managing HTTPS Certificates.

Managing HTTPS Certificates

The router includes a self-signed HTTPS certificate. Since the identity of this certificate cannot be validated, web browsers may display a warning message. To avoid this warning, you can upload your own certificate—signed by a Certification Authority—to the router. If you wish to use your own certificate (for example, in combination with a dynamic DNS service), replace the `/etc/certs/https_cert` and `/etc/certs/https_key` files on the router. You can do this on the *HTTP* configuration page, as detailed in HTTP.

To use the router's self-signed certificate without encountering the security warning (due to a domain name mismatch) each time you log in, follow these steps:

- Add a DNS record to your system. For Linux/Unix systems, edit `/etc/hosts`; for Windows, navigate to `C:\WINDOWS\system32\drivers\etc\hosts`; or configure your own DNS server. Insert a new record pairing the router's IP address with a domain name derived from its MAC address (specifically, the MAC address of the first network interface, as shown in the *Network Status* on the router's web interface), using dashes instead of colons for separation. For example, a router with the MAC address 00:11:22:33:44:55 would use the domain name `00-11-22-33-44-55`.
- Access the router via this new domain name (e.g., `https://00-11-22-33-44-55`). If a security warning appears, add an exception to prevent it from recurring (for example, in the Firefox web browser). If the option to add an exception is unavailable, export the certificate to a file and import it into your browser or operating system.

Note: Using a domain name based on the router's MAC address may not be compatible with all operating system and browser combinations.

Allowed and Restricted Input Characters

When configuring the router via the web interface, it is crucial to avoid using forbidden characters in any input field—not just in password fields. Below are the valid and forbidden characters for input. Note that, in some cases, the space character may also be disallowed.

Valid characters include: `0-9 a-z A-Z * , + - . / : = ? ! # % @ [ ] _ { } ~`

Forbidden characters include: `" $ & ' ( ) ; < > \ ^ ` |`

> **Warning**
>
> Although the system may allow saving non-ASCII characters after confirming a warning message, using them — especially in passwords — is **not recommended**, as it can cause compatibility issues with other systems.

Follow these guidelines; entering invalid characters can lead to errors or unintended behavior.

Supported Certificate Formats

All web interface forms for uploading certificate files support the following file types:

- CA, Local/Remote Certificate: `*.pem`, `*.crt`, `*.p12`
- Private Key: `*.pem`, `*.key`, `*.p12`

Remote Management Platform

WebAccess/DMP is an advanced, enterprise-grade platform for provisioning, monitoring, managing, and configuring Advantech's routers and IoT gateways. It offers zero-touch enablement for each remote device. For more information, refer to the WebAccess/DMP ↗ webpage.

New routers come pre-installed with the *WebAccess/DMP* client, which by default activates the connection to the *WebAccess/DMP* server. Disable this connection on the *Welcome* page upon initial login or under *Customization* → *Router Apps* → *WebAccess/DMP Client*.

> **Warning**
>
> The activated client periodically uploads router identifiers and configurations to the *WebAccess/DMP* server.

Device

Persistent Storage

The device's persistent storage consists of three partitions, combined into a single directory structure:

- **System Data**:
  System data distributed with firmware upgrades.
- **User Data**:
  Separate storage for user data, accessible at `/var/data`.
- **Router Apps Installed**:
  Separate storage for Router Apps data, accessible at `/opt`.

Reset

> **Warning**
>
> Before performing a factory reset on the router, consider creating a backup of its configuration, refer to Backup Configuration.

The reset button on the router, labeled as *RST*, serves three different purposes:

- **Reset**:
  - Hold the *RST* button for **less than 4 seconds**.
  - The router reboots, applying its customized configuration.
  - You can also trigger a reboot by selecting the *Reboot* option in the web interface.
- **Configuration Reset**[1]:
  - Press and hold the *RST* button for **more than 4 seconds**.

    - The *PWR* LED turns off and back on. Hold the *RST* button for an additional second after the *PWR* LED turns back on.
    - The router resets to its default factory configuration, including RA configurations.

- **Emergency Reset**[1]:
    - Use this option if the router fails to boot due to incorrect configuration or a filesystem error.
    - Power off the router by disconnecting its power supply. Then, while holding the *RST* button, **power on the router** and continue holding the *RST* button for **at least 10 seconds**.
    - The router resets its configuration, including RA configurations, similar to the *Configuration Reset*.

[1] Upon first login after a reset, you are prompted to change your password.

The following table summarizes which storage areas are retained and which are deleted during different reset procedures.

Storage	Reset	Configuration Reset	Emergency Reset
Router & Router Apps Configuration	Keep	Reset to default	Reset to default
System Data	Keep	Keep	Keep
User Data	Keep	Keep	Keep
Installed Router Apps	Keep	Keep	Keep
User Account Locks	Keep	Keep	Remove
Factory Reset of Cellular Module	No	No	Yes

Reset Storage Actions

Functionalities and Scenarios

Key Functionalities

Network Features

- **IPv6 Dual Stack**: Supports modern and legacy IP addressing, ensuring comprehensive network compatibility.
- **DHCP and NAT**: Provides seamless network configuration and address translation for efficient network management.
- **Dynamic DNS (DynDNS)**: Facilitates access to the router via dynamic IP addresses, enhancing remote connectivity.
- **VLAN Support**: Enables segmented network configurations for enhanced security and network optimization.
- **QoS (Quality of Service)**: Ensures bandwidth prioritization for critical applications, maintaining optimal network performance.

VPN Tunnels

- **OpenVPN**: Open-source, highly configurable VPN protocol
- **IPsec**: Standards-based network layer encryption
- **WireGuard**: Modern, high-performance VPN protocol
- **GRE**: Generic Routing Encapsulation for network connectivity
- **L2TP**: Layer 2 Tunneling Protocol
- **PPTP**: Point-to-Point Tunneling Protocol

Advanced Features

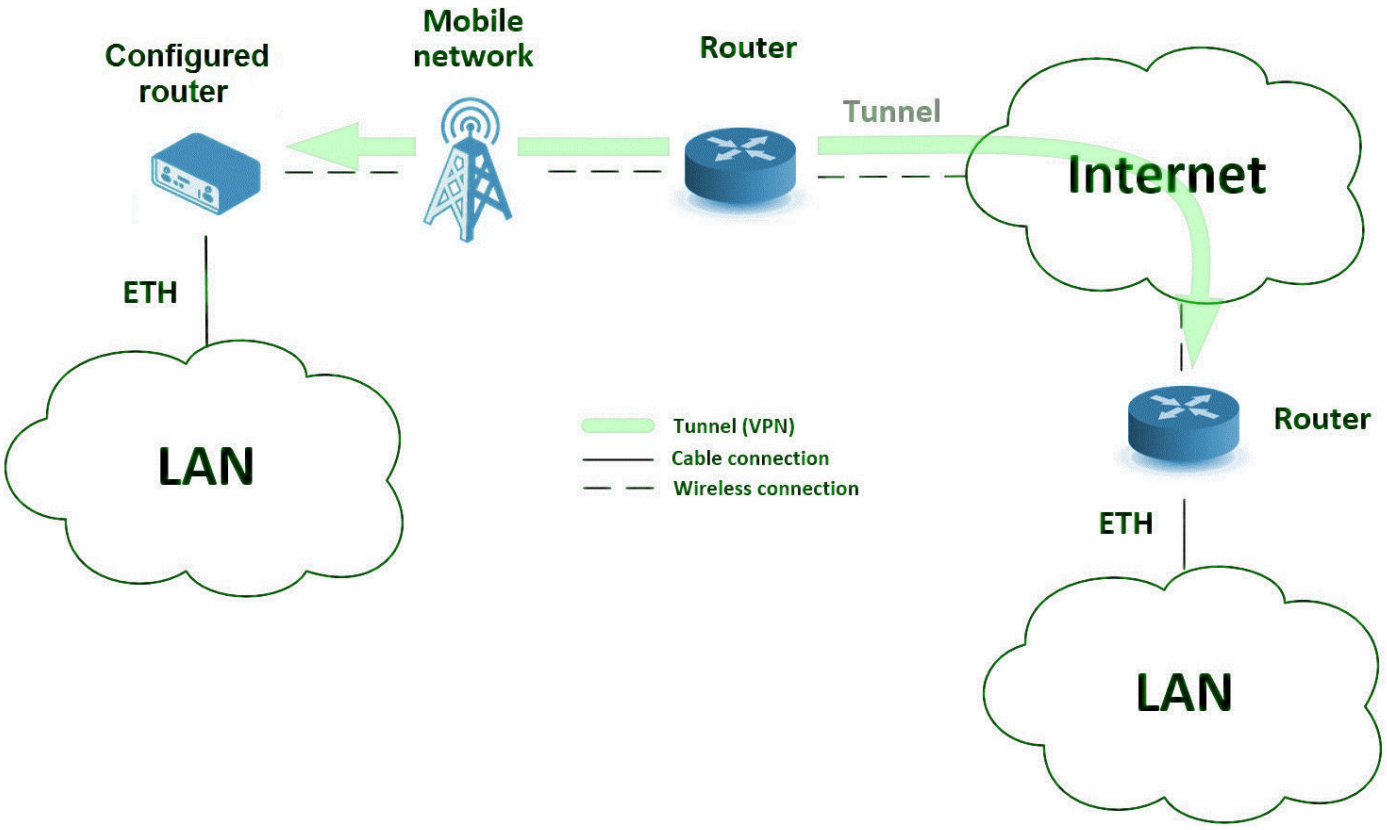
- **Low Power Mode**: Optimizes energy consumption for efficient operation, reducing overall power requirements.
- **Hardware Watchdog**: Ensures system stability by continuously monitoring performance and auto-recovering from potential issues.
- **Linux Script Support**: Enables advanced automation and customization through flexible scripting capabilities.
- **Multi-Configuration Storage**: Allows storing up to four configurations, switchable via web interface, SMS, or digital input.
- **PPP Connection Monitoring**: Automatically restarts the router in case of connection failure, minimizing downtime.
- **Configuration and Firmware Updates**: Accessible remotely via Advantech's public server or a dedicated server, ensuring easy maintenance.

Usage Scenarios Examples

Backup Internet Access

- Acts as a backup connection when the primary connection fails.
- Supports backup options, including:
    - PPPoE connections

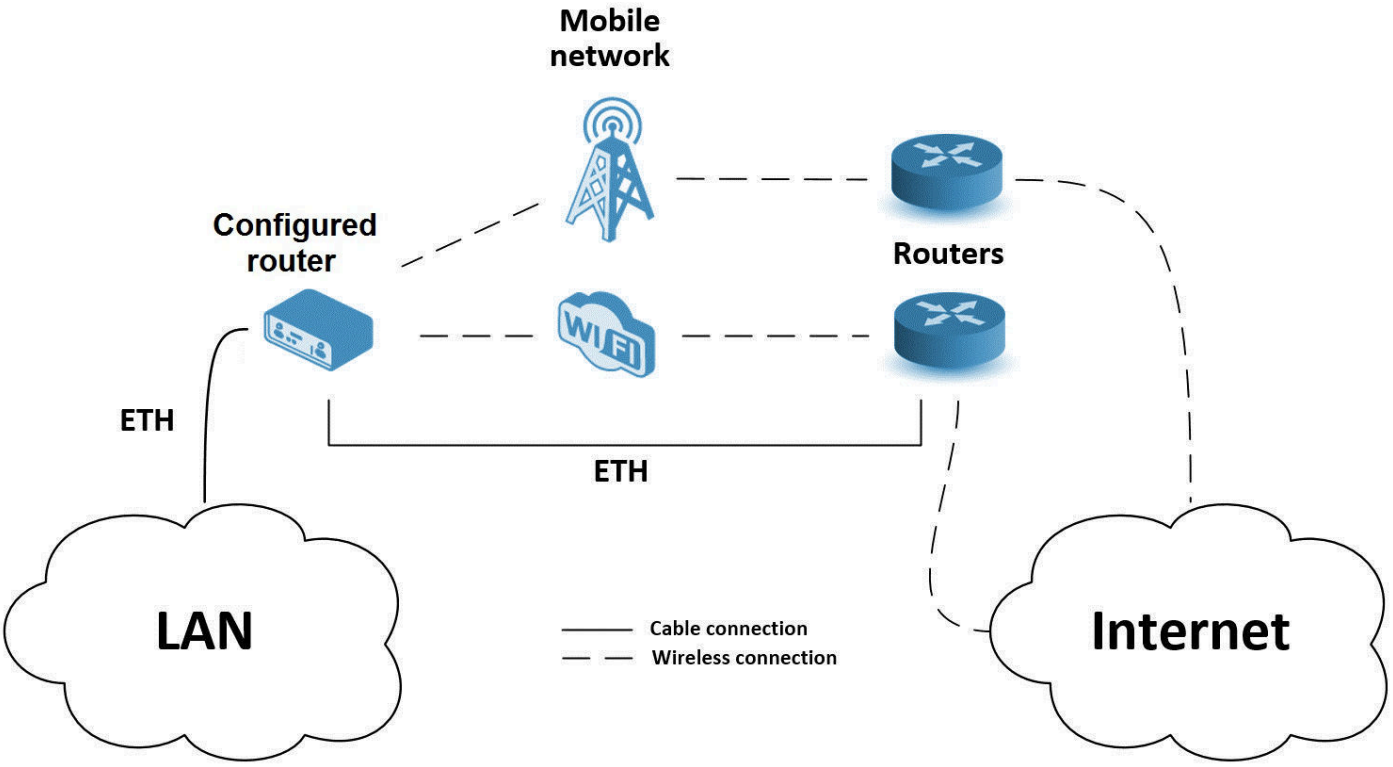
- Wired Ethernet connections
- WiFi (for models with WiFi capabilities)



Backup Internet Access Diagram

VPN Networks Interconnection

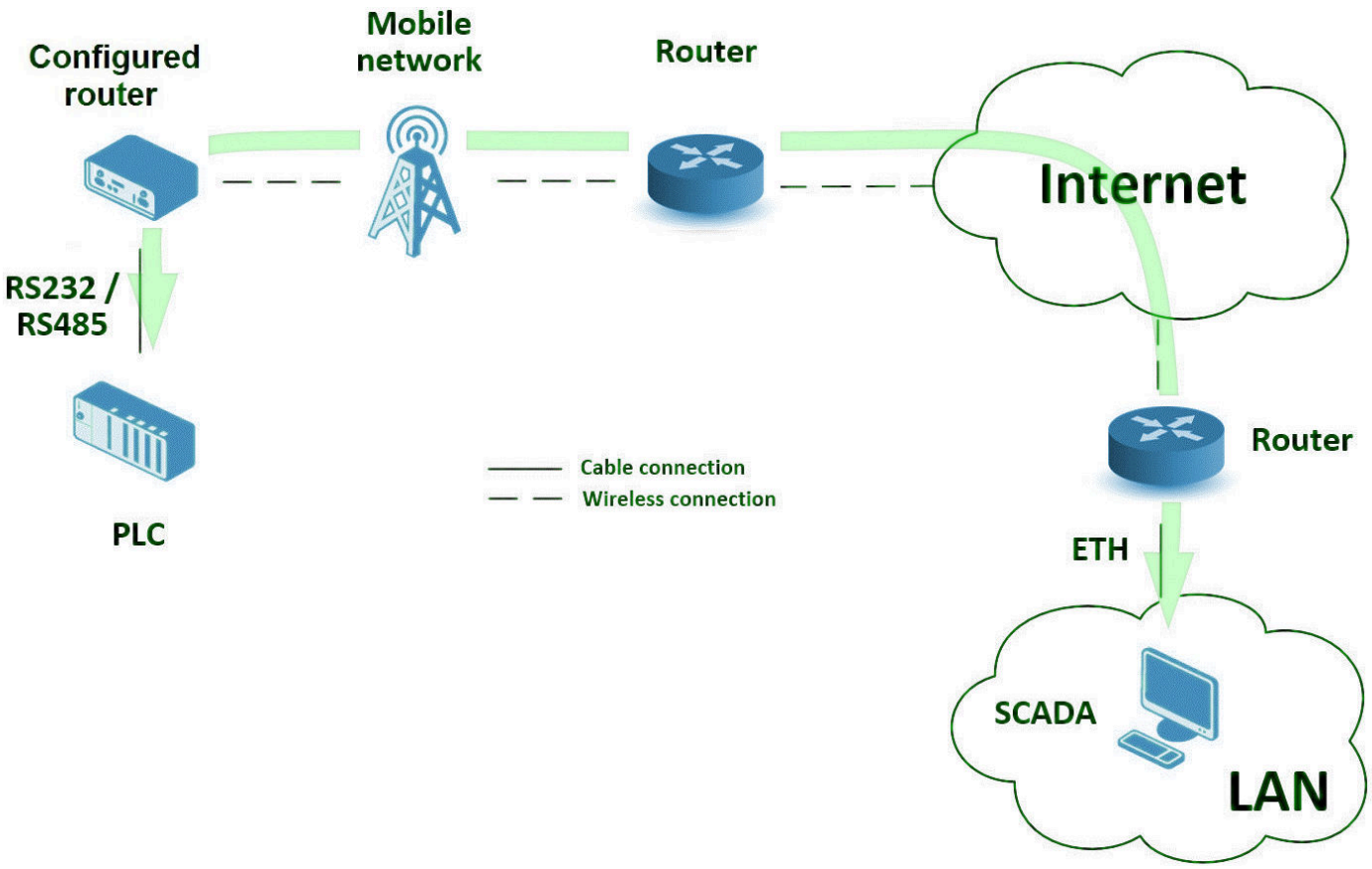
- Configures a secure VPN tunnel to interconnect the router with a remote network using its cellular interface.
- Enables secure and encrypted communication over the Internet.



VPN Networks Interconnection Diagram

Serial Gateway

- Facilitates access to a PLC device connected to the router's serial interface.
- Allows remote control of the PLC via the Internet from a local network (e.g., SCADA system).



Serial Gateway Diagram

Status Pages

Live Data Updates

> **Tips**
>
> All status pages can display live data. To enable this feature, click on the *refresh* button in the top right corner on the status page. To stop the data update and to limit the amount of data transferred, disable automatic data updates by clicking the *pause* button again.

General

You can reach a summary of basic router information and its activities by opening the *General* status page. This page is displayed when you log in to the device by default. The information displayed on this page is divided into several sections, based upon the type of the router and its hardware configuration. Typically, there are sections for the mobile connection, LAN, system information, and eventually for the WiFi and peripheral ports, if the device is equipped with them.

> **Tips**
>
> *IPv6 Address* item can show multiple different addresses for one network interface. This is standard behavior since an IPv6 interface uses more addresses. The second IPv6 Address showed after pressing *More Information* is an automatically generated EUI-64 format link local IPv6 address derived from the MAC address of the interface. It is generated and assigned the first time the interface is used (e.g., cable is connected, Mobile WAN connecting, etc.).

Sections

- **Mobile Connection**: Displays details about the active SIM card and network connection.
- **LAN**: Provides information about the local network configuration.
- **System Information**: Summarizes hardware and software details of the router.
- **WiFi** *(if equipped)*: Shows details about WiFi configuration and status.
- **Peripheral Ports** *(if equipped)*: Lists connected peripheral devices.

Ethernet

Each Ethernet interface has a dedicated section on the *General* status page. The items displayed here have the same meaning as those in the *Mobile Connection* section. Additionally, the *MAC Address* item shows the MAC address of the corresponding router interface. The visible information depends on the Ethernet configuration; see Ethernet for details.

WiFi

If the router is equipped with a WiFi module, the *WiFi AP* section will display information about the WiFi interface operating in access point mode. For configuration details, see WiFi AP.

The *DFS* item indicates whether Dynamic Frequency Selection (DFS) is supported. DFS is a mechanism that allows access points in the 5 GHz spectrum to operate on restricted channels, requiring them to switch to a different channel if interference with priority services (such as radar) is detected.

The *WiFi STA* section displays information about the WiFi interface operating in station mode. For configuration details, see WiFi STA.

The items displayed in this section have the same meaning as those in the *Mobile Connection* section.

Peripheral Ports

These items are reported only for devices equipped with serial or binary interfaces.

> **Info**
>
> For the voltage levels of the binary I/O ports, refer to the Hardware chapter of this manual.

Geolocation

> **Info**
>
> This information is available only on router models equipped with a GNSS module and only when the GNSS service is enabled.

This section displays the router's current position, as determined by the GNSS receiver.

Item	Description
Latitude	The router's current north-south position, expressed in degrees.
Longitude	The router's current east-west position, expressed in degrees.
Altitude	The router's current height above sea level, measured in meters.
Speed over ground	The router's current speed, measured in kilometers per hour.
Course over ground	The direction in which the router is moving, expressed in degrees relative to true north.
Show on map	Clicking this link opens the router's current position in Google Maps in your default web browser.

Geolocation information

GNSS

> **Info**
>
> This information is available only on router models equipped with a GNSS module and only when the GNSS service is enabled.

This section displays detailed information about the satellite signals and the receiver's status.

Item	Description
Current Time (UTC)	The current time obtained from the satellite signals, expressed in Coordinated Universal Time (UTC).
Fix Type	The type of position fix. A **2D** fix requires at least three satellites and provides latitude and longitude. A **3D** fix requires at least four satellites and provides latitude, longitude, and altitude.
HDOP	Horizontal Dilution of Precision. A measure of the geometric quality of the satellite configuration. A lower value indicates higher positional accuracy.
Satellites Used	The number of satellites currently being used for the position fix out of the total number of visible satellites.
Satellites	The list of Pseudo-Random Noise (PRN) numbers for all visible satellites.
SNR	Signal-to-Noise Ratio for each visible satellite. A higher value indicates a stronger and clearer signal. A hyphen (-) indicates that the satellite is visible but its signal is too weak to be measured.
Used	Indicates whether a specific satellite is being used in the position calculation (Y for Yes, N for No).

GNSS information

Security Information

This section provides information about the currently logged-in user, including their last login time, the IP address from which they connected, and the number of failed login attempts since the last successful login.

System Information

The *System Information* section displays key details about the router's hardware, software, and current operational state. Note that some items are only displayed after clicking the *More Information* link.

Item	Description
Part Number	The specific ordering code that identifies the product's exact hardware and software configuration. This is typically printed on the label on the device itself.

Item	Description
Product Type	The hardware model name of the router which identifies the exact hardware configuration. It corresponds to the *Model no.* stated in the datasheet.
Product Name	The commercial name of the product family that shares the same firmware base.
Firmware Version	Information about the firmware version.
Serial Number	Serial number of the router (*N/A* if not available).
Hardware UUID[1]	Unique hardware identifier for the device.
Product Revision[1]	Manufactured product revision number.
Profile	Current profile — standard or alternative profiles (profiles are used, for example, to switch between different modes of operation).
Free Space	Available free space for Router Apps and user data.
CPU Usage	CPU usage value (enable refresh in the top-right corner).
Memory Usage	Memory usage value (enable refresh in the top-right corner).
Time	Current date and time.
Uptime	Duration the router has been running.
Licenses	Link to the list of open-source software components in the firmware along with their license types. Click on a license type to view its text.

[1] Some models may not support this item.

WiFi

Status

The *Status → Wi-Fi* page displays the current operational status of the Wi-Fi module and all configured interfaces, including Access Point (AP) and Station (STA) modes.

Wi-Fi AP Status

Wi-Fi Module Information

This section provides hardware-specific details about the installed Wi-Fi module.

Item	Description
Chip	The model of the Wi-Fi chipset.
Firmware	The version of the firmware running on the Wi-Fi module.
Supports	Lists the number of simultaneous interfaces the module can handle. For example, *1 station and 2 access points* indicates that the router can act as a client to one network while concurrently operating two separate access point interfaces.

Wi-Fi AP Status

The *WiFi AP 1 Status* and *WiFi AP 2 Status* sections display information about the Wi-Fi interfaces operating in Access Point mode. This includes common AP settings followed by a list of connected stations (clients). Each block of connected station data begins with the client's MAC address, followed by the items described in the tables below.

Common AP Information

Column/Item	Description
bssid	The MAC address of the Wi-Fi access point interface.
ssid	The Service Set Identifier (network name) broadcast by the access point.
wpa	Indicates the WPA standard version bitmask currently in use (e.g., *2* indicates support for WPA2/RSN standards). Note that WPA3 also utilizes the RSN framework; to distinguish between WPA2 and WPA3, refer to the *key_mgmt* field.
key_mgmt	The Key Management Method used for authentication. Common values include *WPA2-PSK* (WPA2 Personal) and *SAE* (WPA3 Personal).
group_cipher	The encryption protocol used for broadcast and multicast traffic within the network (e.g., *CCMP*, *TKIP*).
rsn_pairwise_cipher	Encryption protocol used for unicast traffic (e.g., *CCMP*).

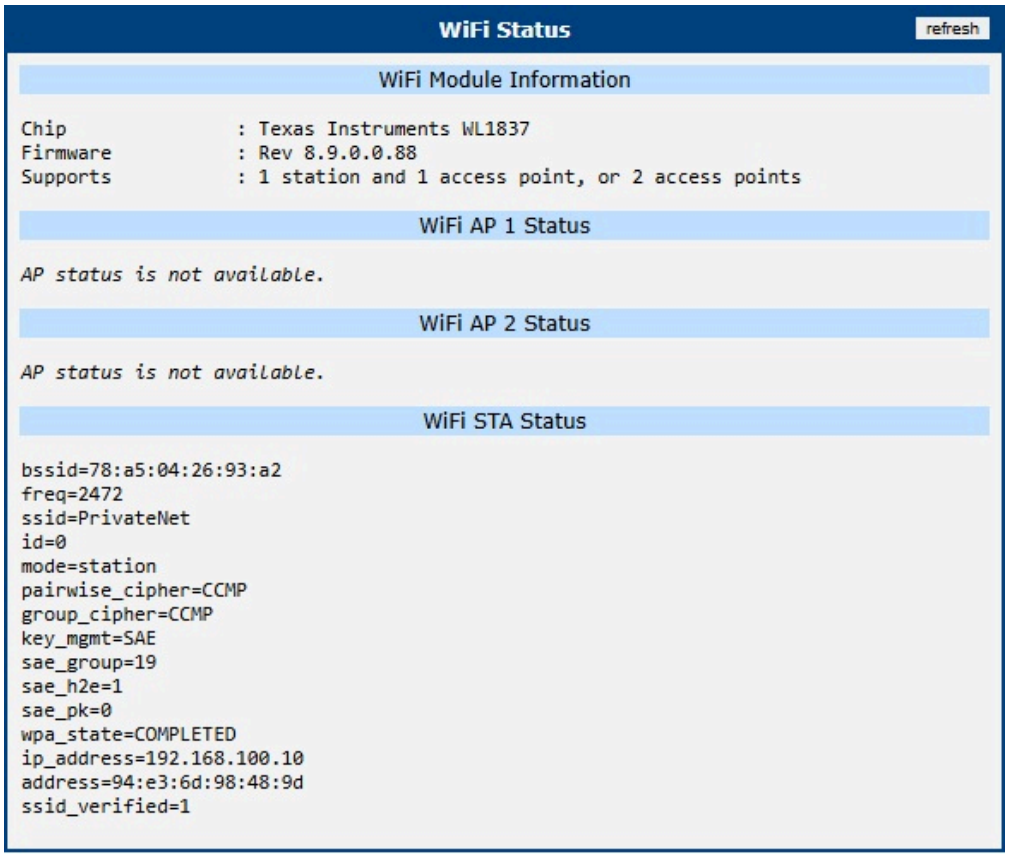
Connected Station Information

Column/Item	Description
[MAC Address]	The MAC address of the connected client device.
flags	Connection flags indicating current state (e.g., *[AUTH]*, *[ASSOC]*, *[AUTHORIZED]*).
capability	A hexadecimal bitmask indicating the station's advertised capabilities (e.g., support for ESS, IBSS, Privacy, Short Preamble) as defined in the IEEE 802.11 standard.
listen_interval	The number of beacon intervals for which the station may enter power-saving mode (sleep) before waking up to receive beacon frames.
supported_rates	A list of data transmission rates (in Mbps or hexadecimal representation) that the station supports.
wpa	Indicates the WPA standard version currently in use for this connection (e.g., *2* indicates support for WPA2/RSN standards). Note that WPA3 also utilizes the RSN framework.
AKMSuiteSelector	The Authentication and Key Management suite selector used. It identifies the authentication method (e.g., *00-0f-ac-8* for SAE/WPA3 or *00-0f-ac-2* for WPA2-PSK).
rx_packets	Number of packets received from this station.
tx_packets	Number of packets transmitted to this station.

Column/Item	Description
rx_bytes	Number of bytes received from this station.
tx_bytes	Number of bytes transmitted to this station.
inactive_msec	The time in milliseconds since the last data packet was received from the station. A lower value indicates an active connection.
signal	Signal strength of the connected station (in dBm).
rx_rate_info	Information about the last received data rate from the station (e.g., bitrate index or MCS index).
tx_rate_info	Information about the last transmitted data rate to the station (e.g., bitrate index or MCS index).
connected_time	Duration of the current connection in seconds.
sae_group	The Diffie-Hellman group (ECC curve) used during the WPA3 SAE handshake (e.g., *19* for NIST P-256). Only applicable when WPA3 (SAE) is used.
sae_rejected_groups	A list of SAE groups that were proposed but rejected during the handshake process.
supp_op_classes	Supported Operating Classes. A hexadecimal string listing the frequency bands and channel behaviors the station supports.
ext_capab	Extended Capabilities. A hexadecimal bitfield indicating support for advanced features (e.g., BSS Transition, WNM) beyond the standard capability field.

Wi-Fi STA Status

The *WiFi STA Status* section displays information about the Wi-Fi interface operating in Station (Client) mode.



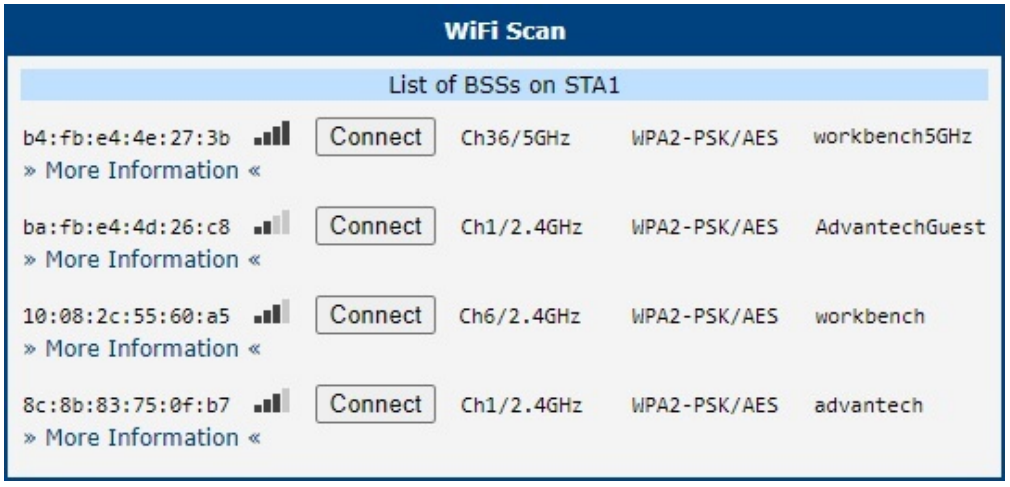
Wi-Fi STA Status

Item	Description
bssid	The MAC address of the Access Point to which the station is connected.
freq	The operating frequency (channel) in MHz (e.g., *2472* corresponds to channel 13).
ssid	The name of the Wi-Fi network the station is connected to.
id	The internal numeric identifier of the configured network profile in the wpa_supplicant.
mode	Operation mode (*station*).
pairwise_cipher	The encryption protocol used for unicast data traffic between the station and the access point (e.g., *CCMP*, *GCMP*, *TKIP*).
group_cipher	The encryption protocol used for broadcast and multicast traffic within the network (e.g., *CCMP*, *TKIP*).
key_mgmt	The Key Management protocol used for authentication. Common values include *WPA-PSK* (WPA2 Personal) and *SAE* (WPA3 Personal).
sae_group	The Diffie-Hellman group (ECC curve) used during the WPA3 SAE handshake (e.g., *19* for NIST P-256). Only applicable when WPA3 (SAE) is used.
sae_h2e	Indicates if the "Hash-to-Element" method was used for SAE password derivation. *1* means H2E was used (mandatory for WPA3 in 6 GHz), *0* means the older "Hunting-and-Pecking" loop method was used.

Item	Description
sae_pk	Indicates if SAE Public Key (SAE-PK) authentication was used. *1* means SAE-PK was used to cryptographically bind the SSID to the password (preventing rogue APs), *0* means standard SAE was used.
wpa_state	The current state of the connection. *COMPLETED* indicates a successful connection. States like *SCANNING* or *DISCONNECTED* imply the router is searching for a network or cannot connect (check credentials or signal).
ip_address	The IP address assigned to the station interface, either obtained dynamically from a DHCP server or configured statically.
address	The MAC address of the router's Wi-Fi station interface.
ssid_verified	Indicates if the SSID has been verified (e.g., *1* for true). Only applicable when WPA3 (SAE) is used.

Scan

The *Status → Wi-Fi → Scan* page allows you to discover all nearby Wi-Fi networks. The results are displayed in a list, showing the key parameters of each detected network.



Wi-Fi Scan Results

The list is structured into several columns, and each entry provides a *Connect* button and a link to view *More Information*.

Column/Item	Description
BSS	The MAC address of the detected access point.
Signal Icon	A visual representation of the signal strength. More bars indicate a stronger signal.
Connect button	Clicking this button redirects you to the *Configuration → Wi-Fi → Station* page with the selected network's details pre-filled, allowing you to easily connect by entering the password.
Channel/Band	The channel number and frequency band the network is operating on.
Security	The security protocol and encryption method used by the network (e.g., WPA2-PSK/AES).
SSID	The public name of the Wi-Fi network.

Column/Item	Description
More Information	Clicking this link expands a section with detailed technical parameters of the access point, intended for advanced diagnostics.

Network

To view detailed information about network interfaces, routing tables, and active connections, navigate to the *Status → Network* page. The upper part of the page displays details for all active network interfaces, followed by the IPv4 and IPv6 routing tables.

Network Status refresh

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 02:AD:FF:00:01:20
          inet addr:10.64.0.120  Bcast:10.64.3.255  Mask:255.255.252.0
          inet6 addr: fe80::ad:ffff:fe00:120/64 Scope:Link
          inet6 addr: fd00:a40::120/56 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77904 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6015974 (5.7 MB)  TX bytes:38486283 (36.7 MB)
          Interrupt:25 Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 02:AD:FF:01:01:20
          Interrupt:28

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:31127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5001471 (4.7 MB)  TX bytes:5001471 (4.7 MB)

null0     Link encap:Ethernet  HWaddr 3E:9C:AF:63:42:B3
          inet6 addr: fe80::3c9c:afff:fe63:42b3/64 Scope:Link
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:70 (70.0 B)

usb0      Link encap:Ethernet  HWaddr CA:BF:16:A8:56:88
          inet addr:10.80.0.100  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:588 (588.0 B)  TX bytes:2138 (2.0 KB)
```

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.253.254	0.0.0.0	UG	0	0	0	usb0
10.64.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth0
10.65.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth1
192.168.253.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

IPv6 Route Table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
fd00:a40::/56	::	U	256	3	0	eth0
ff00::/8	::	U	256	2	0	eth0
ff00::/8	::	U	256	2	0	eth1
::/0	::	!n	-1	1	0	lo

Backup Routes

```
WAN IP Interface   : eth0
WAN IP Address     : 10.40.28.252
WAN IPv6 Interface : N/A
WAN IPv6 Address   : N/A
```

LLDP Neighbors

LLDP service is disabled.

Network Status

Interfaces

This section provides an overview of all active network interfaces on the router. For each interface, it displays essential information such as assigned IP addresses, MAC address, and traffic statistics. In the table below, the `x` in an interface name represents its zero-indexed instance number. The availability of specific interfaces depends on the router model and its configuration.

Interface	Description
eth*x*	A physical Ethernet interface directly connected to the CPU. The index *x* identifies the interface instance (e.g., *eth0*, *eth1*).
vlan*x*	A logical VLAN interface. The index *x* is an internal interface number and does not match the configured VLAN ID. The actual VLAN ID is defined separately and mapped to this logical interface.
lo	The virtual loopback interface used for internal communication within the router.
null0	A virtual interface used by the NAT64 translator. Traffic routed to this interface is discarded.
usb0, usb1	Interfaces representing the cellular WAN connections for the first or second modem module. These interfaces are connected internally via the USB bus.
wlan*x*	A Wi-Fi interface, where *x* identifies the physical radio or a virtual access point instance.
pppoe*x*	A virtual interface for a PPPoE session, where *x* is the instance number.
tun*x*	A virtual interface for an OpenVPN tunnel, where *x* is the tunnel instance number (0–3).
ipsec*x*	A virtual interface for an IPsec tunnel, where *x* is the tunnel instance number (0–3).
wg*x*	A virtual interface for a WireGuard tunnel, where *x* is the tunnel instance number (0–3).
gre*x*	A virtual interface for a GRE tunnel, where *x* is the tunnel instance number (0–3).
l2tp0	A virtual interface for an L2TP tunnel. Only one instance is supported.
pptp0	A virtual interface for a PPTP tunnel. Only one instance is supported.

Each active interface provides a detailed summary of its status and traffic statistics. The parameters are described below.

Item	Description
HWaddr	The hardware Media Access Control (MAC) address of the interface.
inet addr	The primary IPv4 address assigned to the interface.
inet6 addr	The primary IPv6 address assigned to the interface. An interface may have multiple IPv6 addresses.
P-t-P	For a point-to-point link, this is the IP address of the remote peer.
Bcast	The broadcast address for the interface's subnet.
Mask	The subnet mask associated with the IPv4 address.

Item	Description
MTU	The Maximum Transmission Unit, indicating the largest packet size (in bytes) that the interface can transmit without fragmentation.
Metric	A value used by the routing table to determine the cost of a route. Lower values are preferred.
RX/TX packets	The total count of packets received (RX) and transmitted (TX) by the interface.
Errors	A count of errors that occurred during reception or transmission.
Dropped	The number of packets that were dropped during reception or transmission, often due to a lack of buffer space.
Overruns	The number of packets lost due to buffer overloads.
Frame	The number of received packets dropped due to framing errors (e.g., incorrect checksums).
Carrier	The number of transmission errors related to the physical layer carrier signal.
Collisions	The number of packet collisions detected on the physical medium.
txqueuelen	The current length of the transmission queue for the interface.
RX/TX bytes	The total volume of data in bytes received (RX) and transmitted (TX).

Routing Tables

The middle of the page shows the kernel routing tables. Both the *IPv4 Route Table* and the *IPv6 Route Table* are displayed. Below the main routing tables, the *Backup Routes* section lists any currently active backup routes.

If NAT64 is enabled (*Configuration → NAT → IPv6*), it is automatically used for communication between IPv6 and IPv4 networks. This works with the router's DNS64 service, which synthesizes AAAA records from A records. When active, a route for the default NAT64 prefix, `64:ff9b::/96`, will be visible in the *IPv6 Route Table*.

Backup Routes

This section identifies the active primary WAN interface and its corresponding IP address for both IPv4 and IPv6 Internet traffic. The status shown here directly reflects the router's automatic failover system (for details, see Backup Routes), which operates independently of the main routing table. When the primary connection fails, the router automatically switches to a backup interface, and that change is immediately displayed here.

Parameter	Description
WAN IP Interface	Displays the network interface (e.g., `eth0`, `usb0`) currently providing the primary outbound path for all IPv4 traffic. If no connection is active, this shows `N/A`.
WAN IP Address	Displays the current IPv4 address assigned to the active WAN interface.
WAN IPv6 Interface	Displays the network interface currently providing the primary outbound path for all IPv6 traffic. If no connection is active, this shows `N/A`.

Parameter	Description
WAN IPv6 Address	Displays the current IPv6 address assigned to the active WAN IPv6 interface.

LLDP Neighbors

This section displays information about directly connected network devices discovered via the Link Layer Discovery Protocol (LLDP). For this section to be populated, the LLDP service must be enabled in the router's configuration; see LLDP for details.

By default, the page provides a concise summary of all detected neighbors — local interface, the neighbor's MAC address (`ChassisID`), system name (`SysName`), and basic port details. To view extended diagnostic data such as hardware descriptions, management IP addresses, device capabilities, and PoE parameters, click the *» More Information «* link. The following example shows the extended information for an Advantech ICR-3232 router:

```text
Interface:    eth1, via: LLDP, RID: 2, Time: 0 day, 01:03:07
  Chassis:
    ChassisID:    mac 00:11:22:33:44:55
    SysName:      Router
    SysDescr:     ICR-323x 6.6.1 (2026-02-11, commit
2f2ad43db9b08bc71c5d5efe0cf64dfdb0910ff1) #3559
    MgmtIP:       192.168.1.10
    MgmtIface:    9
    MgmtIP:       fe80::85f:aff:febc:7b1e
    MgmtIface:    11
    Capability:   Bridge, off
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       mac 00:11:22:33:44:55
    PortDescr:    eth0
    TTL:          20
    PMD autoneg:  supported: yes, enabled: yes
      Adv:        10Base-T, HD: yes, FD: yes
      Adv:        100Base-TX, HD: yes, FD: yes
      MAU oper type: 100BaseTXFD - 2 pair category 5 UTP, full duplex mode
```

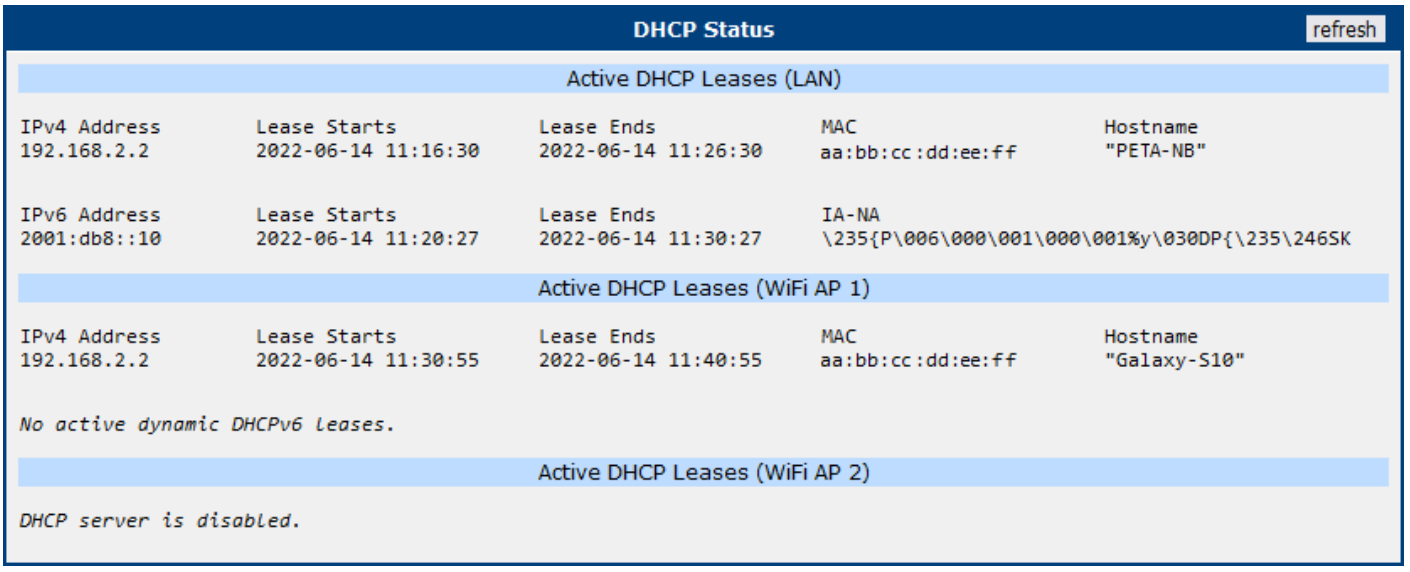
Tips

The structure and meaning of LLDP data units (TLVs) are defined by the **IEEE 802.1AB** standard. For more information about the protocol, visit the official IEEE 802.1 working group page at ieee802.org/1/pages/802.1ab.html ↗. Full versions of IEEE standards are typically accessible through the IEEE GET program ↗.

DHCP

Information about the DHCP server activity is accessible via the *DHCP* item. The DHCP server automatically configures the client devices connected to the router. The DHCP server assigns each device an IP address, subnet mask, and default gateway (IP address of the router) and DNS server (IP address of the router). DHCPv6 server is supported.

See the figure below for the DHCP Status example. Records in the DHCP Status window are divided into two parts based on the interface.



DHCP Status

The *DHCP Status* window displays the following information on a row for each client in the list. All items are described in table below.

Item	Description
IPv4 Address	IPv4 address assigned to a client
IPv6 Address	IPv6 address assigned to a client
Lease Starts	Time IP address lease began
Lease Ends	Time IP address lease expires
MAC	Client's MAC address
Hostname	Client hostname
IA-NA	IPv6 unique identifier

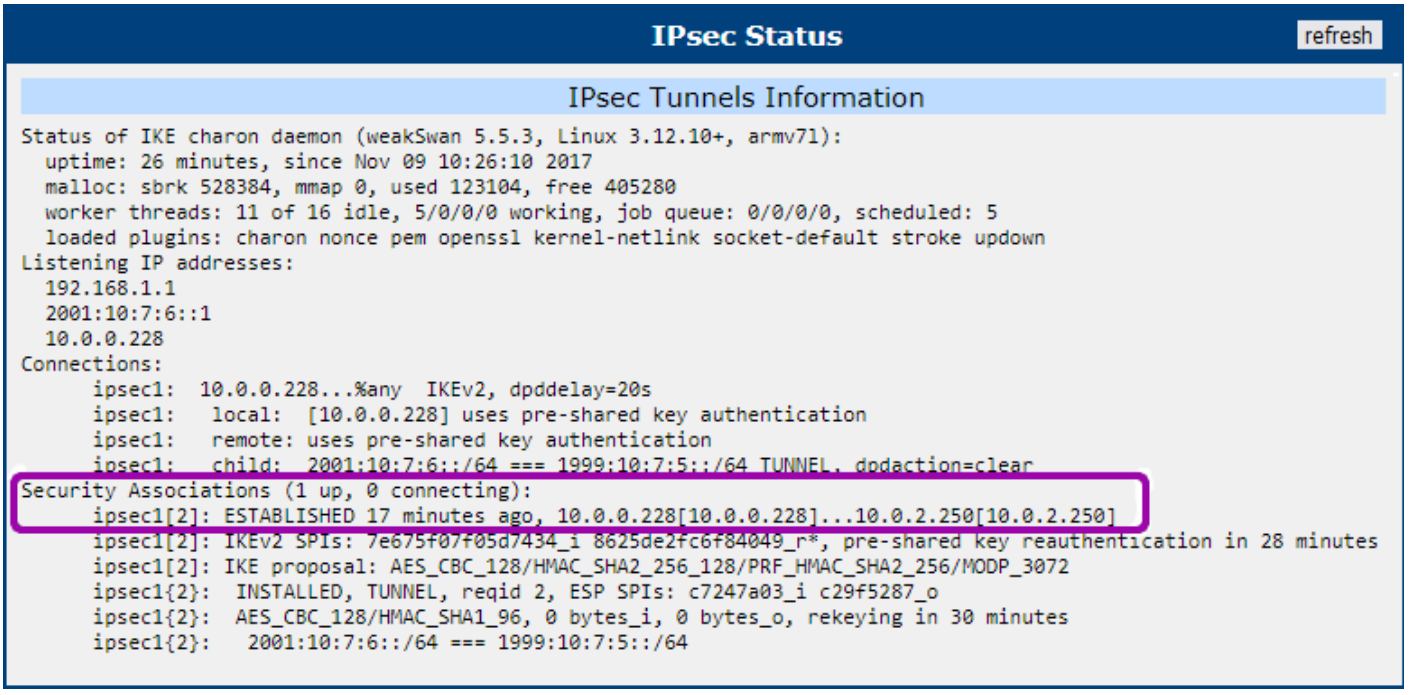
> **Info**
>
> The DHCP status may occasionally display two records for one IP address, potentially caused by resetting the client network interface.

IPsec

To check the status of configured IPsec tunnels, navigate to the *Status → IPsec* page. This page displays a log of the IPsec connection status.

For a successfully established tunnel, the log will contain the keyword **ESTABLISHED**. Additionally, the status summary will show the number of active connections, such as **1 up**, as highlighted in the figure below.

If the log does not show these indicators (e.g., it shows **0 up**), the IPsec tunnel has not been successfully established.

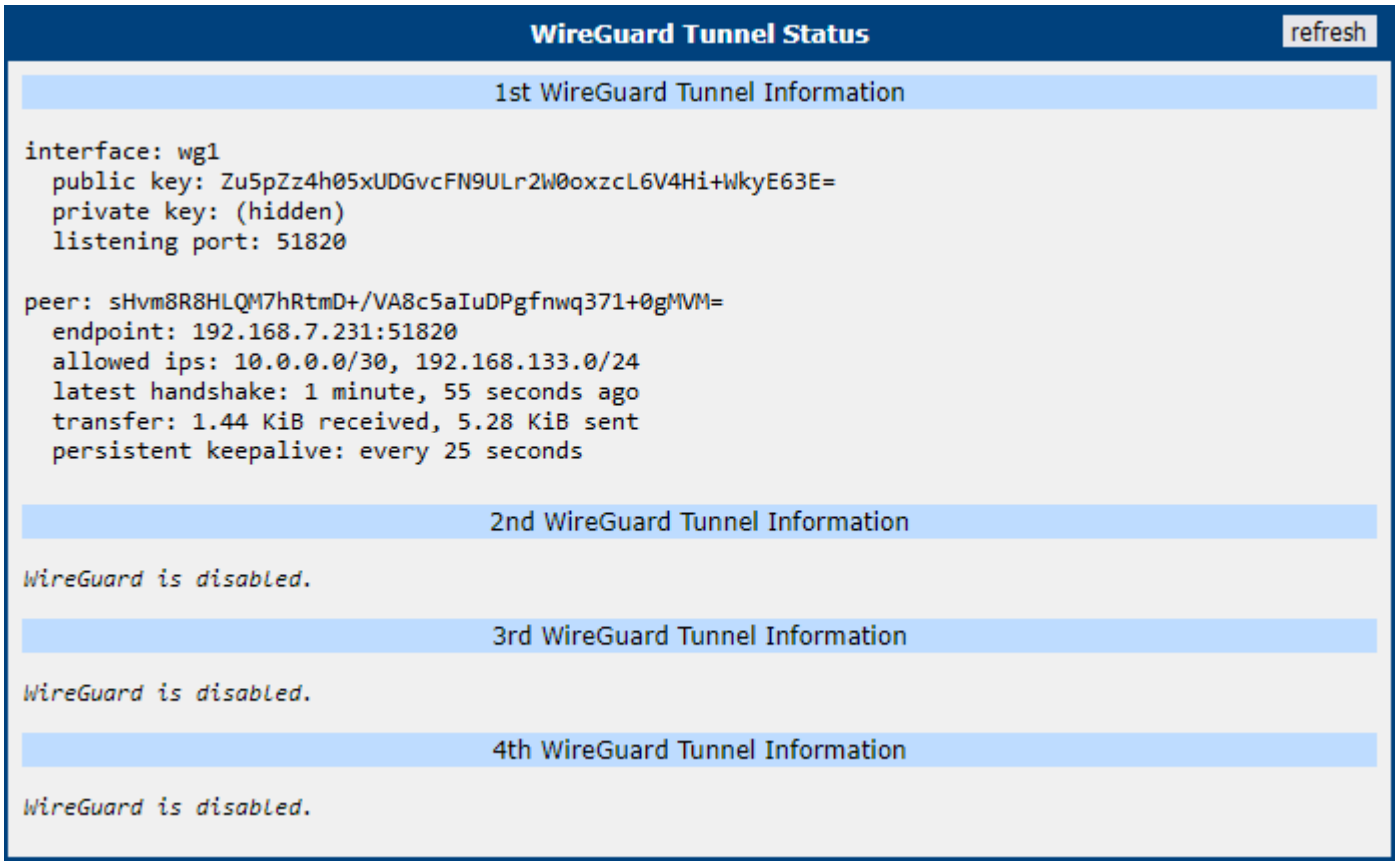


IPsec Status

WireGuard

To check the status of configured WireGuard tunnels, navigate to the *Status → WireGuard* page. This page displays the current operational state and statistics for each active WireGuard interface.

The figure below shows an example of a running WireGuard tunnel.



WireGuard Status Page

The status page displays the following information for each peer connected to a WireGuard interface.

Parameter	Description
Interface	The name of the WireGuard interface on the router (e.g., `wg0`).
Public key	The public key of the connected peer.
Allowed ips	The IP addresses from which this peer is allowed to send traffic through the tunnel.
Latest handshake	The time elapsed since the last successful handshake with the peer. A handshake confirms a secure connection. This time is only displayed after data has been exchanged, either from regular traffic or a keepalive packet (if enabled).
Transfer	The total amount of data received (rx) and transmitted (tx) through the tunnel for this peer.

Warning

Latest handshake time will not appear until tunnel communication occurs (data sent by client-side or keepalive data when *NAT/Firewall Traversal* is set to *yes*).

Dynamic DNS

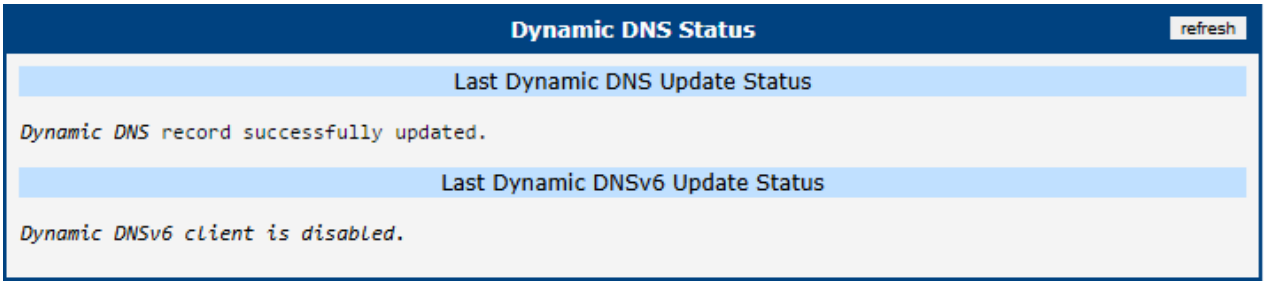
The Dynamic DNS service allows you to access the router using a fixed domain name even when its public IP address changes. To view the service's current status, navigate to the *Status → Dynamic DNS* page.

> **Warning**
>
> For the Dynamic DNS service to function correctly, the router's mobile connection must be assigned a public IP address by your cellular provider.

The router is compatible with several third-party Dynamic DNS providers and supports standard update protocols, including DynDNS (HTTP API) and DDNS (RFC 2136). You can configure the service to use providers such as:

- freedns.afraid.org ↗
- www.duckdns.org ↗
- www.noip.com ↗

IPv6 updates can be used when *IP Mode* is set to *IPv6* on the *Services → Dynamic DNS* configuration page. The status page displays messages that indicate the current state of the Dynamic DNS client and its communication with the provider.



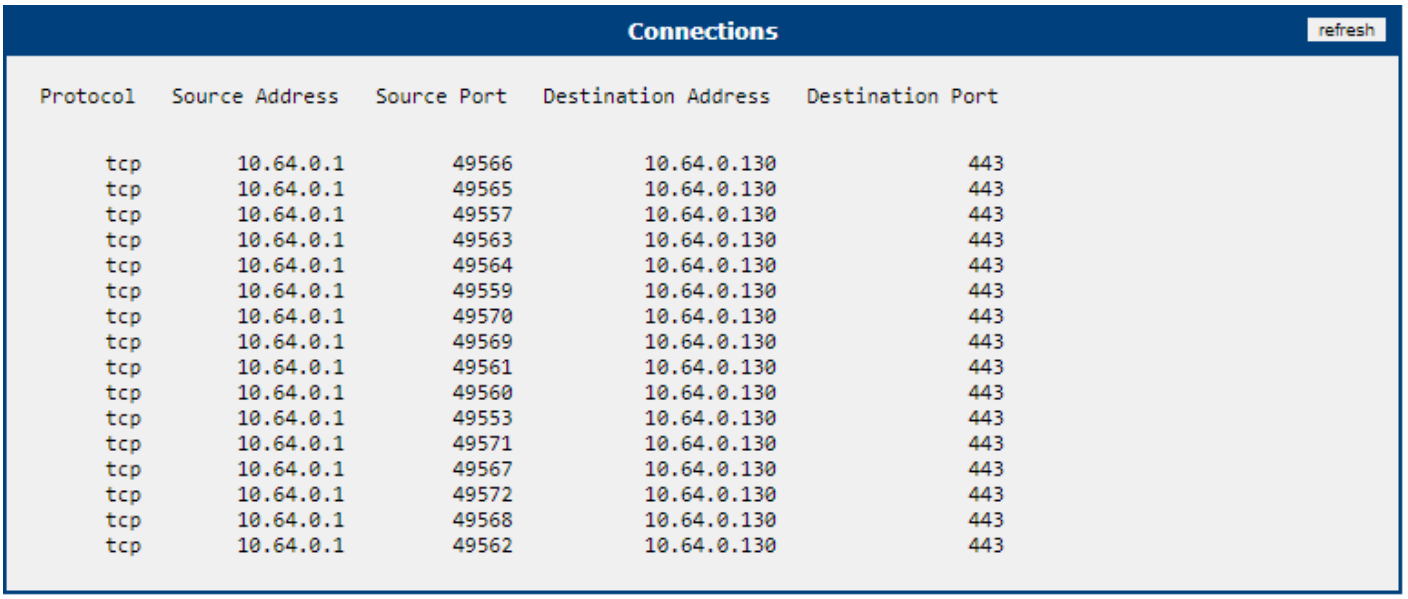
Dynamic DNS Status

The list below shows the possible messages you may encounter:

- Dynamic DNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed since startup.
- DNS error encountered.
- DynDNS record is already up to date.
- DynDNS record successfully updated.
- DynDNS system parametr is not valid.
- DynDNS server failure.
- Last reported IP was [IP address] on [datetime].
- Last report to Dynamic DNS server is unknown.
- Dynamic DNSv6 client is disabled.

Connections

The *Status → Connections* page displays a real-time list of all active network connections passing through the router. This overview is particularly useful for monitoring current network traffic and troubleshooting routing or connectivity issues.



Connections Status

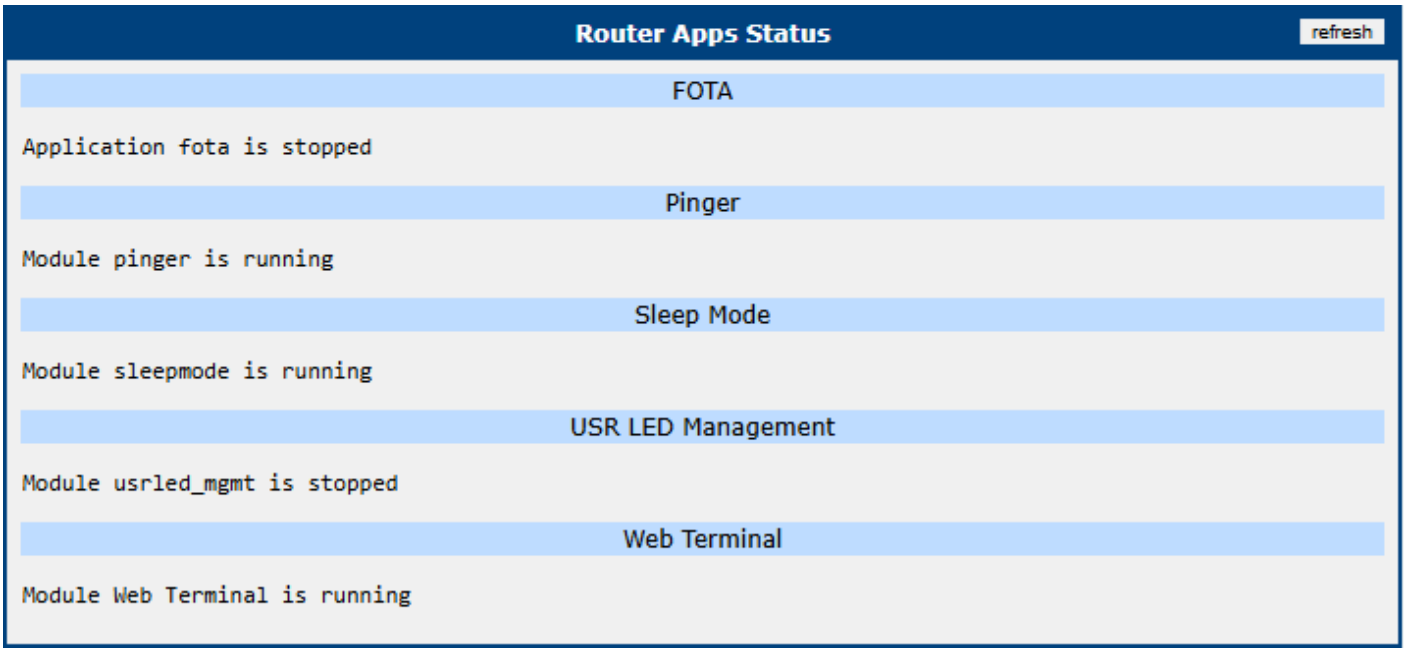
The table below describes the information provided in each column of the connections list.

Column	Description
Protocol	The transport layer protocol used for the connection (e.g., `TCP`, `UDP`, or `ICMP`).
Source Address	The originating IP address of the network connection.
Source Port	The originating port number of the connection.
Destination Address	The target IP address of the network connection.
Destination Port	The target port number of the connection.

Router Apps

The *Status → Router Apps* page provides a quick overview of all Router Apps currently installed on the router. This summary allows administrators to easily verify the operational state of each application without needing to navigate to the primary configuration menu of every single Router App.

As shown in the figure below, the page lists each installed Router App and clearly indicates its current status (e.g., whether the application is actively running or currently stopped).



Router Apps status page

System Log

To view the router's operational logs, navigate to the *Status* → *System Log* page. This page displays messages generated by the router's operating system and various services.

> **Info**
>
> For security, sensitive data such as passwords is automatically filtered out from the system log and diagnostic reports.

The level of detail in the log is controlled by the *Minimum Severity* setting on the *Configuration* → *Services* → *Syslog* page.

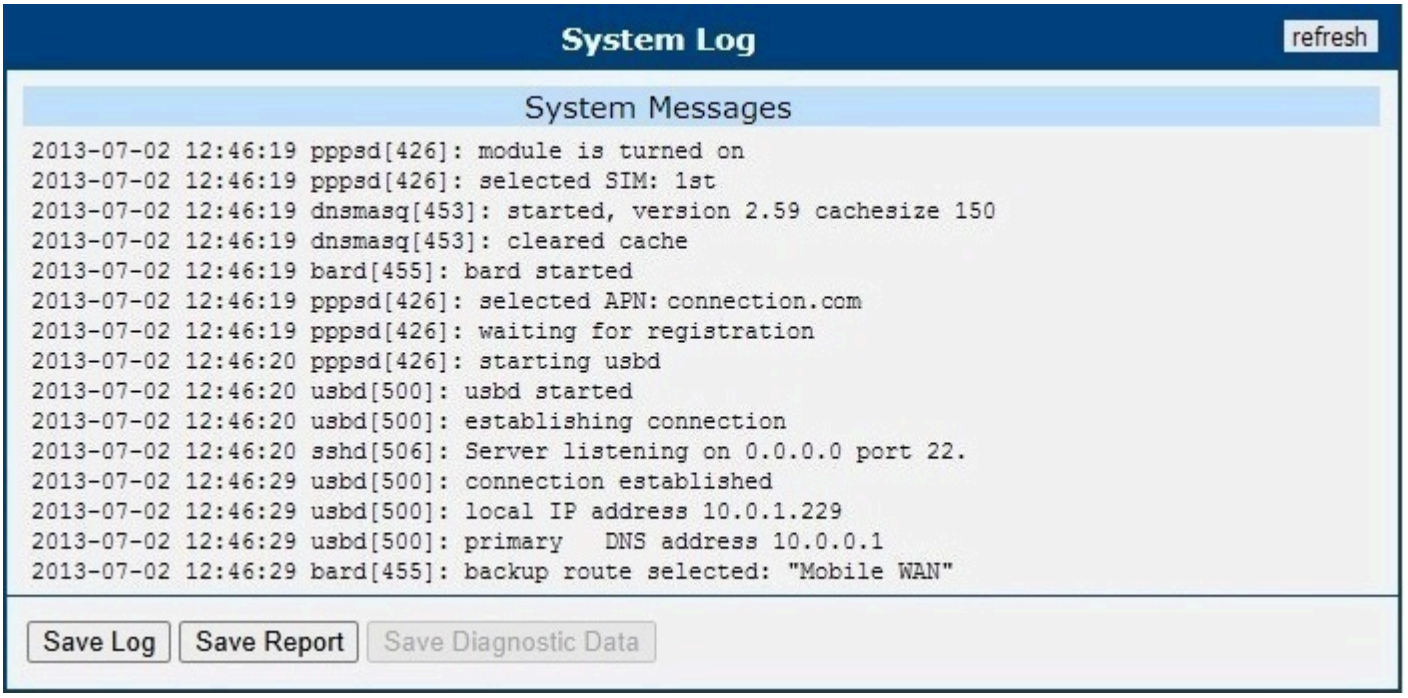
The router manages log storage to prevent files from growing indefinitely. By default, the total log size is limited to 10 KiB, split between two rotating files. When the current file is full, the system switches to the other. Once both are full, new entries overwrite the oldest ones. The *Log Size Limit* can be adjusted on the Syslog configuration page.

The *System Log* page provides several options for downloading diagnostic information:

- **Save Log:** Downloads the current contents of the system log as a plain text file (`*.log`).
- **Save Report:** Generates and downloads a comprehensive diagnostic report file (`*.txt`), which is essential for troubleshooting and providing to technical support. The report always contains the following information:
    - General system information and status
    - Network statistics and current routing tables
    - A list of all running processes
    - Filesystem usage information
    - The complete system log

> **Tips**
>
> For users logged in with the *Admin* role, the report additionally includes a copy of the current router configuration. This section is omitted for standard users.

- **Save Diagnostic Data:** Downloads a compressed archive (`*.gz`) containing detailed data from the last system failure. This button is only visible to users with the *Admin* role and is only enabled when a system crash dump is present. The data is intended for advanced analysis by technical support.



System Log

Configuration Pages

Ethernet

To enter the Local Area Network configuration, select the *Ethernet* menu item in the *Configuration* section. The *Ethernet* item will expand in the menu on the left, allowing you to choose the appropriate Ethernet interface to configure: *ETH0* for the first Ethernet interface and *ETH1* for the second Ethernet interface.

The LAN Configuration page is divided into IPv4 and IPv6 columns, as shown in Figure below. There is dual stack support for IPv4 and IPv6 protocols, meaning they can run concurrently. You can configure either one of them or both. If both IPv4 and IPv6 are configured, network devices will automatically select the communication protocol. The configuration items and differences between IPv6 and IPv4 are described in the tables below.

ETH0 Configuration

☑ Enable Port

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway		
Primary DNS Server		
Secondary DNS Server		

Bridged	no	
MTU	1500 bytes	576-1500 bytes
Media Type	auto-negotiation	

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.254		
Lease Time	600	600	sec

☐ Enable static DHCP leases

	MAC Address	IP Address	IPv6 Address
1			
2			

Maximum 32 items

☐ Enable IPv6 prefix delegation

Subnet ID *	
Subnet ID Width *	bits

☐ Enable IEEE 802.1X Authentication

Authentication Method	EAP-PEAP/MSCHAPv2
CA Certificate	Choose File No file chosen
Local Certificate	Choose File No file chosen
Local Private Key	Choose File No file chosen
Identity	
Password	

** can be blank*

Apply

LAN Configuration Page

Item	Description
Enable Port	Enables or disables the physical Ethernet port.
DHCP Client	Enables or disables the DHCP client function. If in the IPv6 column, the DHCPv6 client is enabled. The DHCPv6 client supports all three methods of obtaining an IPv6 address: SLAAC, stateless DHCPv6, and stateful DHCPv6. Options: • **disabled**: The router does not allow automatic allocation of an IP address from a DHCP server in the LAN network. • **enabled**: The router allows automatic allocation of an IP address from a DHCP server in the LAN network.
IP Address	A fixed IP address for the Ethernet interface. Use IPv4 notation in the IPv4 column and IPv6 notation in the IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies the subnet mask for the IPv4 address. In the IPv6 column, fill in the prefix for the IPv6 address: a number in the range of 0 to 128.
Default Gateway	Specifies the IP address of the default gateway. If provided, every packet with a destination not found in the routing table is sent to this IP address. Use the correct IP address notation in both the IPv4 and IPv6 columns.
Primary DNS Server	Specifies the primary IP address of the DNS server. When the IP address is not found in the routing table, the router forwards the request to the DNS server specified here. Use the correct IP address notation in both the IPv4 and IPv6 columns.
Secondary DNS Server	Specifies the secondary IP address of the DNS server.

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* is set to *disabled* and if the ETH0 or ETH1 LAN is selected by the *Backup Routes* system as the default route.

The following three items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the router at a time. The *DHCP Client*, *IP Address*, and *Subnet Mask / Prefix* parameters of only one of the interfaces are used for the bridge. The ETH0 LAN has higher priority when both interfaces (ETH0 and ETH1) are added to the bridge. Other interfaces can be added to or removed from an existing bridge at any time. The bridge can be created on demand for such interfaces, but not if it is configured by their respective parameters.

Warning

Under certain conditions, the ETH interface may operate as a WAN interface, and the rules defined in the Firewall settings will be applied to it. Details are described in Backup Routes and are demonstrated with examples provided there.

Item	Description
Bridged	Activates or deactivates the bridging function on the router. • **no**: The bridging function is inactive (default). • **yes**: The bridging function is active. See the **Bridge Notes** below the table for further details.

Item	Description
MTU	Maximum Transmission Unit value. Default value is 1500 bytes.
Media Type	Specifies the type of duplex and speed used in the network. • **Auto-negotiation**: The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • **1000 Mbps Full Duplex**: The router communicates at 1000 Mbps, in the full duplex mode. • **100 Mbps Full Duplex**: The router communicates at 100 Mbps, in the full duplex mode. • **100 Mbps Half Duplex**: The router communicates at 100 Mbps, in the half duplex mode. • **10 Mbps Full Duplex**: The router communicates at 10 Mbps, in the full duplex mode. • **10 Mbps Half Duplex**: The router communicates at 10 Mbps, in the half duplex mode.

Bridge Notes

A bridge behaves like a network switch, forwarding packets between interfaces that are connected to it. The Advantech router supports creating a bridge network within Ethernet interfaces or between Ethernet interfaces and Wi-Fi Access Point (AP) interfaces. Once the bridge is configured and established, a new interface named `br0` is created. This interface will appear in the *Status → Network → Interfaces* section.

If a bridge is configured on two Ethernet interfaces, the `br0` interface will inherit the IP address of the Ethernet interface with the lower index. IP address and subnet configuration of the Ethernet interface with the higher index will be removed. This behavior is consistent regardless of the order in which the interfaces are configured.

To include a Wi-Fi AP interface in the bridge, at least one Ethernet interface must also be part of the bridge configuration. In this case, the IP address of the bridge interface `br0` will again be determined by the Ethernet interface (or interfaces) with the lowest index.

DHCP Server

The DHCP server assigns the IP address, gateway IP address (IP address of the router) and IP address of the DNS server (IP address of the router) to the connected clients. If these values are filled in by the user in the configuration form, they will be preferred.

The DHCP server supports static and dynamic assignment of IP addresses. *Dynamic DHCP* assigns clients IP addresses from a defined address space. *Static DHCP* assigns IP addresses that correspond to the MAC addresses of connected clients.

Info

- If IPv6 column is filled in, the DHCPv6 server is used. DHCPv6 server offers stateful address configuration to connected clients. Only when the *Subnet Prefix* above is set to 64, the DHCPv6 server offers both: the stateful address configuration and SLAAC (Stateless Address Autoconfiguration).
- For DHCPv6 static address assignment to work, DHCPv6 client must use DUID-LL or DUID-LLT types that are derived from its MAC address.

Warning

Do not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP server. IP address conflicts and incorrect network function can occur if you overlap the ranges.

Configuration of Dynamic DHCP Server

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP addresses allocated to the DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Configuration of Static DHCP Server

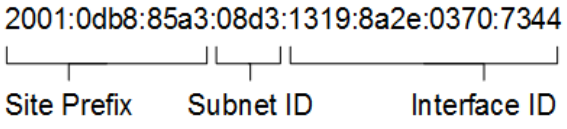
Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server. You can define up to thirty-two rules. A new row for defining the next rule appears automatically after filling in the previous one.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

IPv6 Prefix Delegation

Warning

This is an advanced configuration option. IPv6 prefix delegation works automatically with DHCPv6: use only if different configuration is desired and if you know the consequences.

If you want to override the automatic IPv6 prefix delegation, you can configure it in this form. You have to know your Subnet ID Width (part of IPv6 address), see the figure below for the calculation help: it is an example: 48 bits is Site Prefix, 16 bits is Subnet ID (*Subnet ID Width*) and 64 bits is Interface ID.



IPv6 Address with Prefix Example

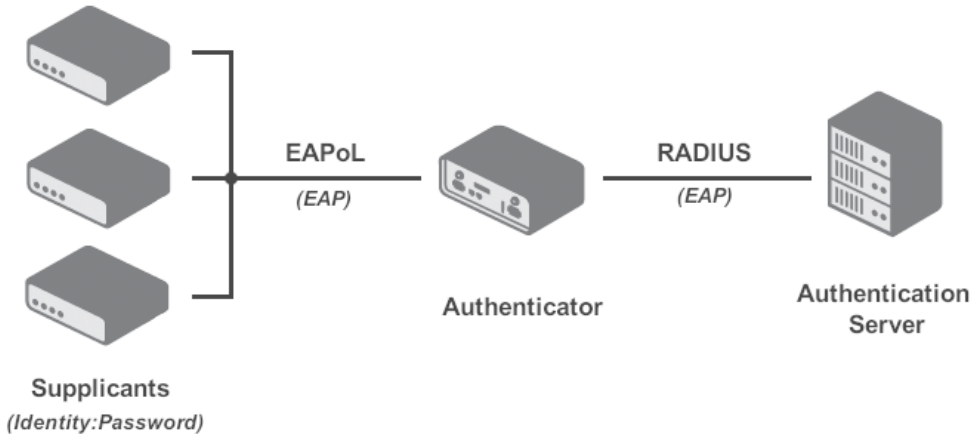
Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the *Subnet ID Width*.

Item	Description
Subnet ID Width	The maximum *Subnet ID Width* depends on your Site Prefix: it is the remainder to 64 bits.

802.1X Authentication with RADIUS Server

IEEE 802.1X is an IEEE standard for **port-based Network Access Control** (PNAC). It provides an authentication mechanism for devices connecting to a LAN or WLAN using "EAP over LAN" (**EAPoL**), which encapsulates the **Extensible Authentication Protocol** (EAP).

IEEE 802.1X authentication involves three parties: a **supplicant**, an **authenticator**, and an **authentication server**, illustrated in the figure below.



IEEE 802.1X Functional Diagram

- The **supplicant** is a client device (e.g., a laptop) requesting network access.
- The **authenticator** is a network device (e.g., a switch or router) that controls network access and mediates communication with the authentication server.
- The **authentication server** (typically a **RADIUS** server) validates the supplicant's credentials and authorizes or denies access.

> **Info**
>
> Advantech routers can function as a supplicant or an authenticator, but not as an authentication server.

Interface	Supplicant Role	Authenticator Role
LAN	As a built-in feature, configure LAN with 802.1X authentication.	While not a built-in feature, it can be facilitated by the *802.1X Authenticator* ↗ Router App.
WiFi	In Station (STA) mode.	In Access Point (AP) mode.

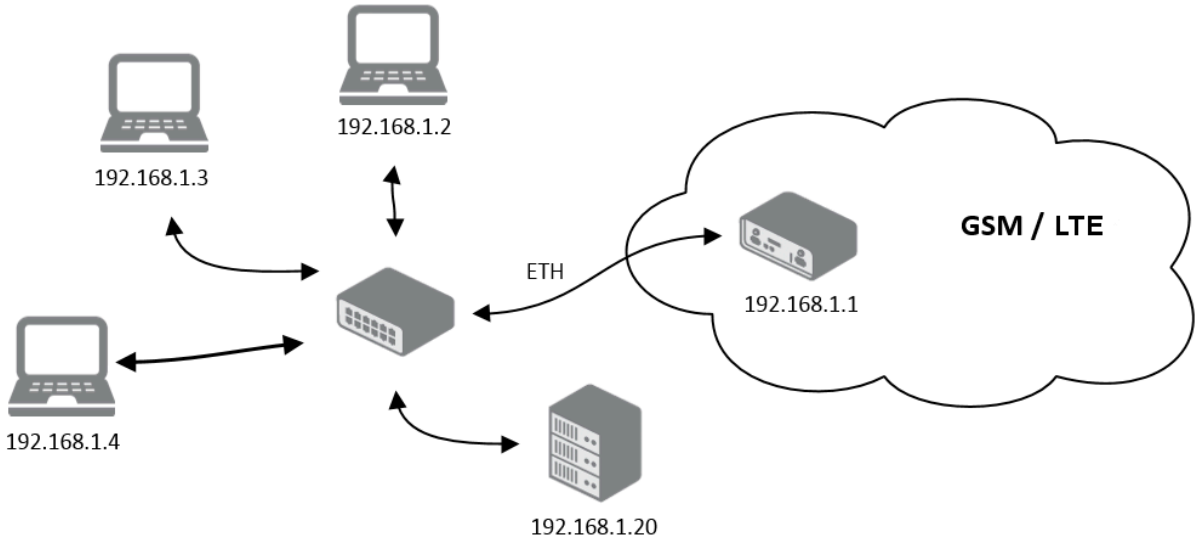
The 802.1X supplicant can be enabled in the section below. This requires configuring an identity and, for EAP-TLS, certificates.

Item	Description
Enable IEEE 802.1X Authentication	Enables the 802.1X supplicant on this interface.
Authentication Method	Selects the authentication method (EAP-PEAP/MSCHAPv2 or EAP-TLS).
CA Certificate	Defines the CA certificate for the EAP-TLS protocol.
Local Certificate	Defines the local certificate for the EAP-TLS protocol.
Local Private Key	Defines the local private key for the EAP-TLS protocol.
Identity	The username (identity) for authentication.
Password	The password for authentication (used only for EAP-PEAP/MSCHAPv2).
Local Private Key Password	The password for the local private key (used only for EAP-TLS).

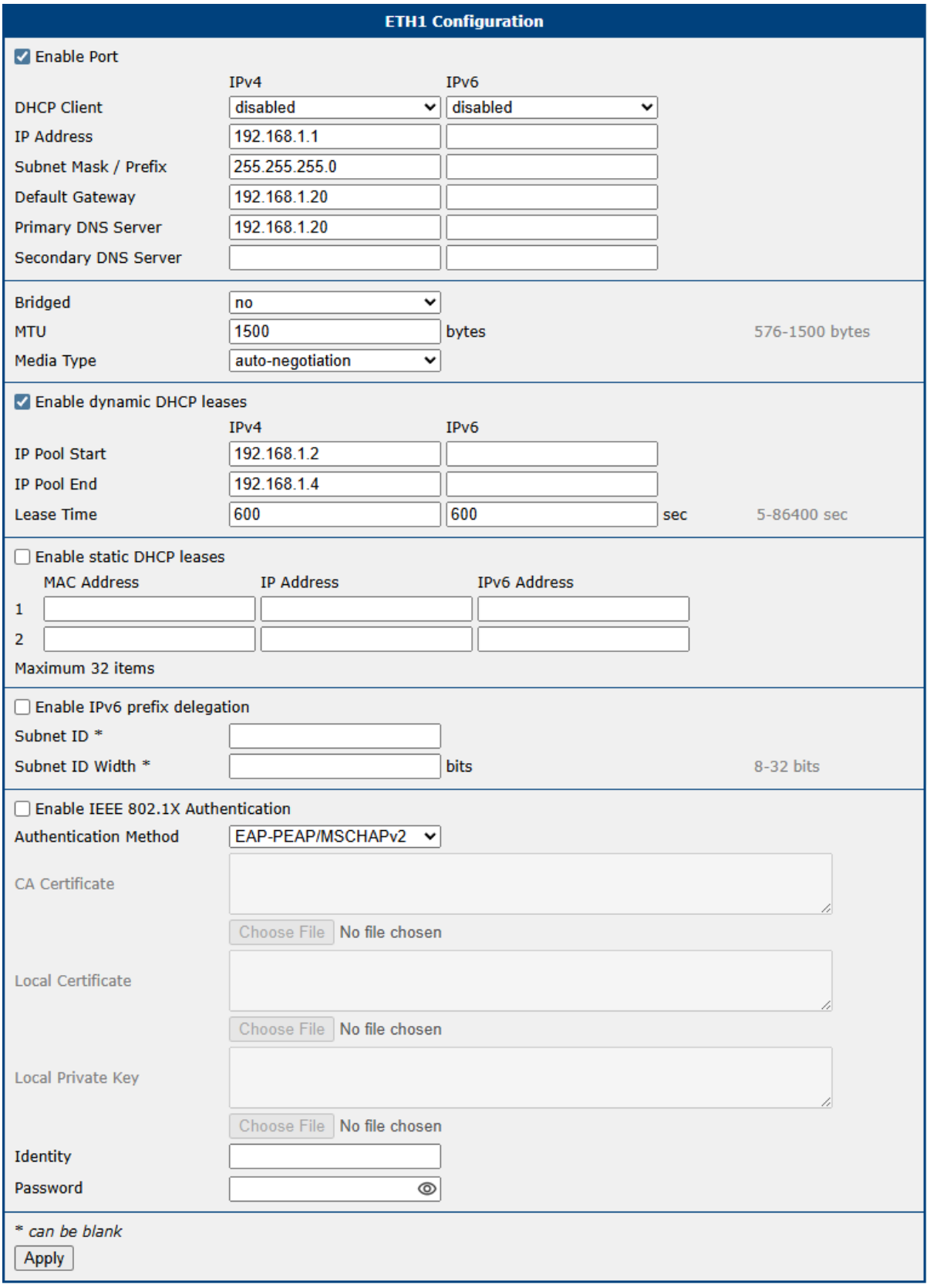
LAN Configuration Examples

Example 1: IPv4 Dynamic DHCP Server, Default Gateway and DNS Server

- The range of dynamic allocated IPv4 addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 second (10 minutes).
- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20



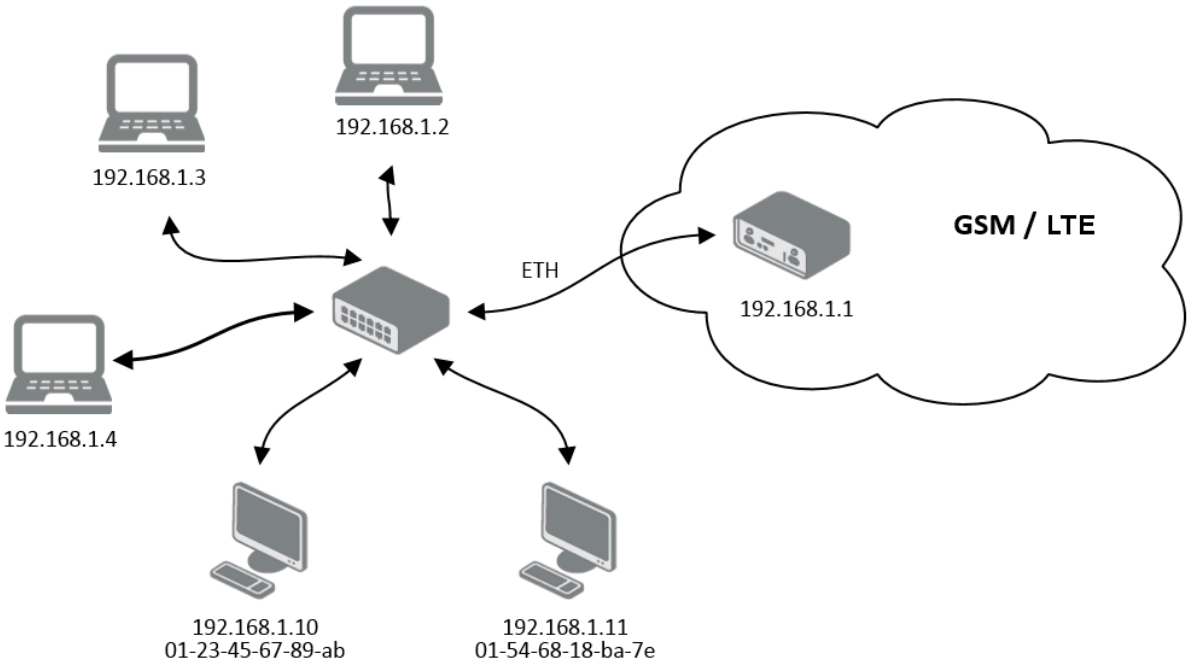
Network Topology for Example 1



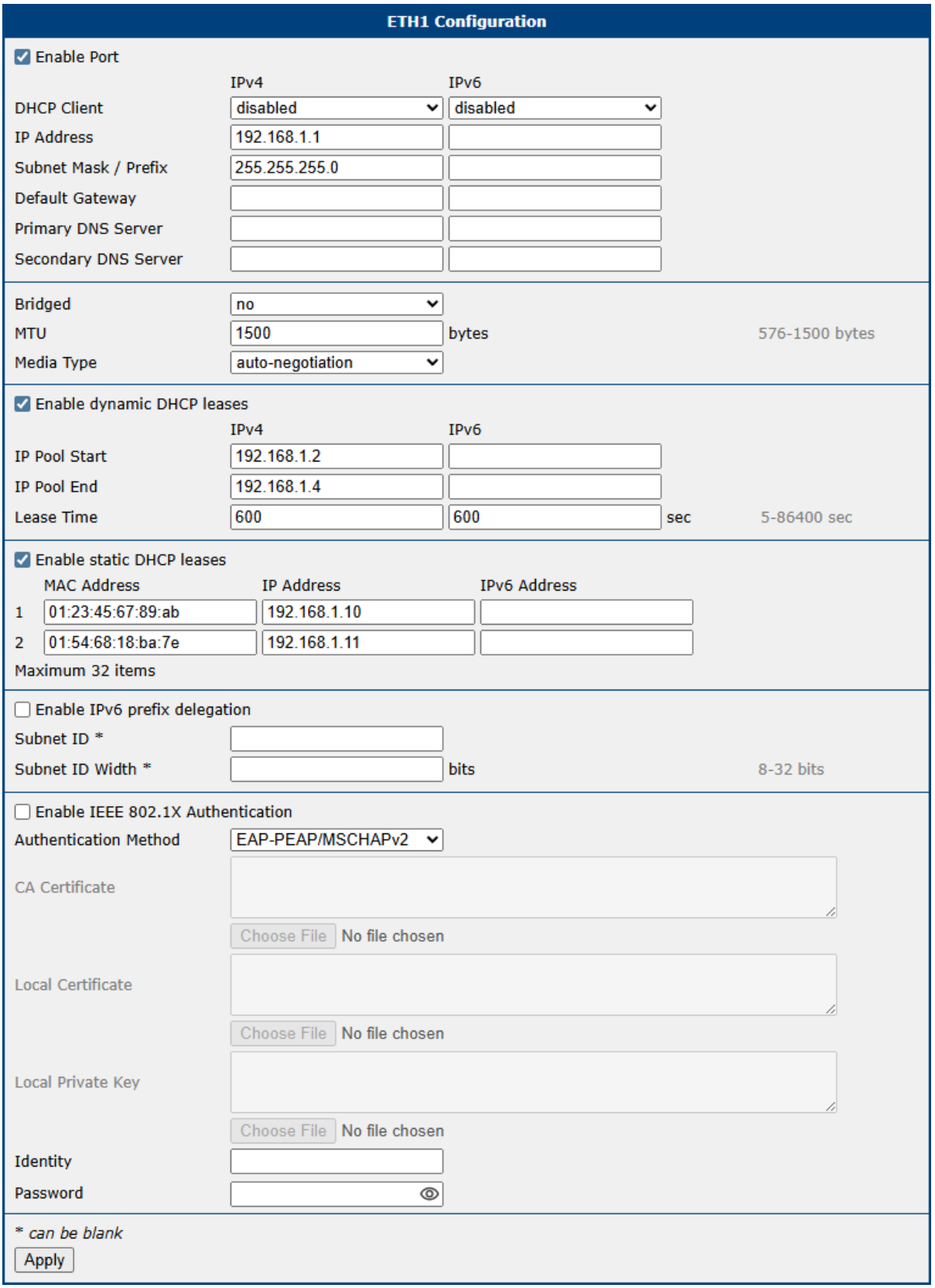
LAN Configuration for Example 1

Example 2: IPv4 Dynamic and Static DHCP server

- The range of allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 seconds (10 minutes).
- The client with the MAC address 01:23:45:67:89:ab has the IP address 192.168.1.10.
- The client with the MAC address 01:54:68:18:ba:7e has the IP address 192.168.1.11.



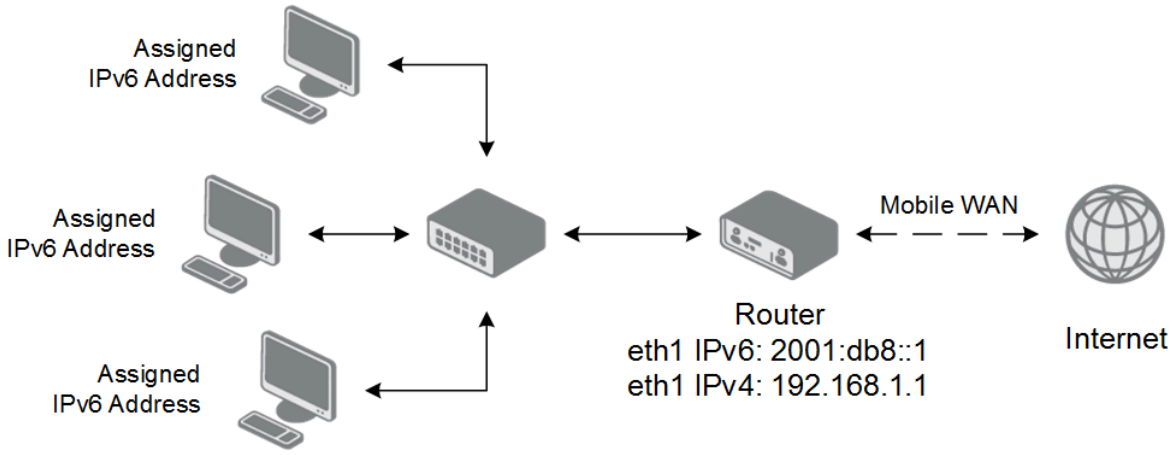
Network Topology for Example 2



LAN Configuration for Example 2

Example 3: IPv6 Dynamic DHCP Server

- The range of dynamic allocated IPv6 addresses is from 2001:db8ffff.
- The address is allocated for 600 second (10 minutes).
- The router is still accessible via IPv4 (192.168.1.1).



Network Topology for Example 3

ETH1 Configuration

Enable Port

	IPv4	IPv6	
DHCP Client	disabled	disabled	
IP Address	192.168.1.1	2001:db8::1	
Subnet Mask / Prefix	255.255.255.0	64	
Default Gateway			
Primary DNS Server			
Secondary DNS Server			
Bridged	no		
MTU	1500	bytes	576-1500 bytes
Media Type	auto-negotiation		

Enable dynamic DHCP leases

	IPv4	IPv6		
IP Pool Start		2001:db8::2		
IP Pool End		2001:db8::ffff		
Lease Time		600	sec	5-86400 sec

Enable static DHCP leases

	MAC Address	IP Address	IPv6 Address
1			
2			

Maximum 32 items

Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *	bits	8-32 bits

Enable IEEE 802.1X Authentication

Authentication Method	EAP-PEAP/MSCHAPv2
CA Certificate	Choose File No file chosen
Local Certificate	Choose File No file chosen
Local Private Key	Choose File No file chosen
Identity	
Password	

** can be blank*

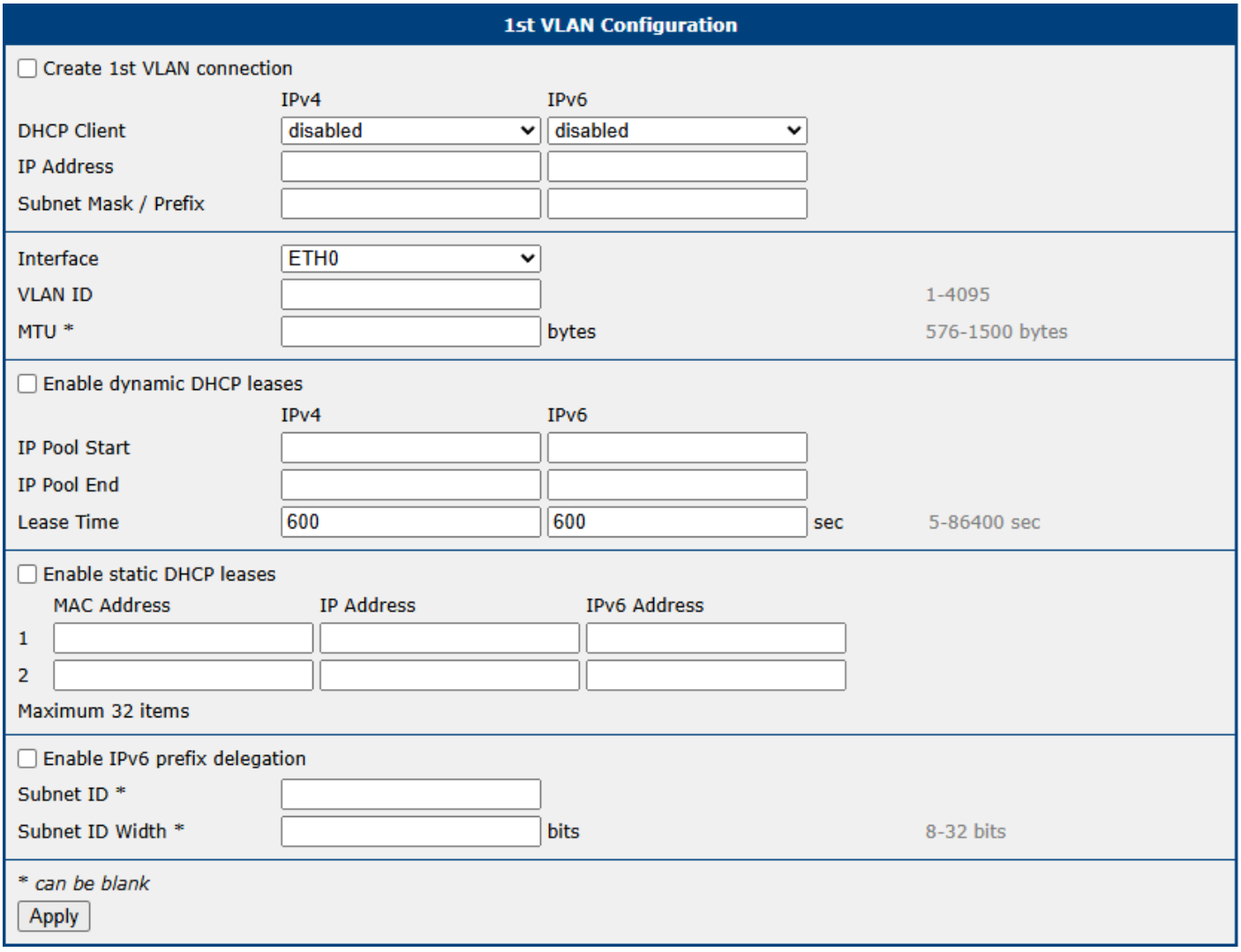
Apply

LAN Configuration for Example 3

VLAN

The router allows for the creation of up to three separate Virtual LAN (VLAN) interfaces, enabling network segmentation for enhanced security and traffic management. Each VLAN can be configured with its own IP address, DHCP server, and other network settings, effectively creating an independent logical network on a shared physical interface.

The VLAN configuration page, accessible via *Configuration → VLAN*, is divided into sections for interface setup, DHCP services, and IPv6 prefix delegation.



VLAN Configuration Page

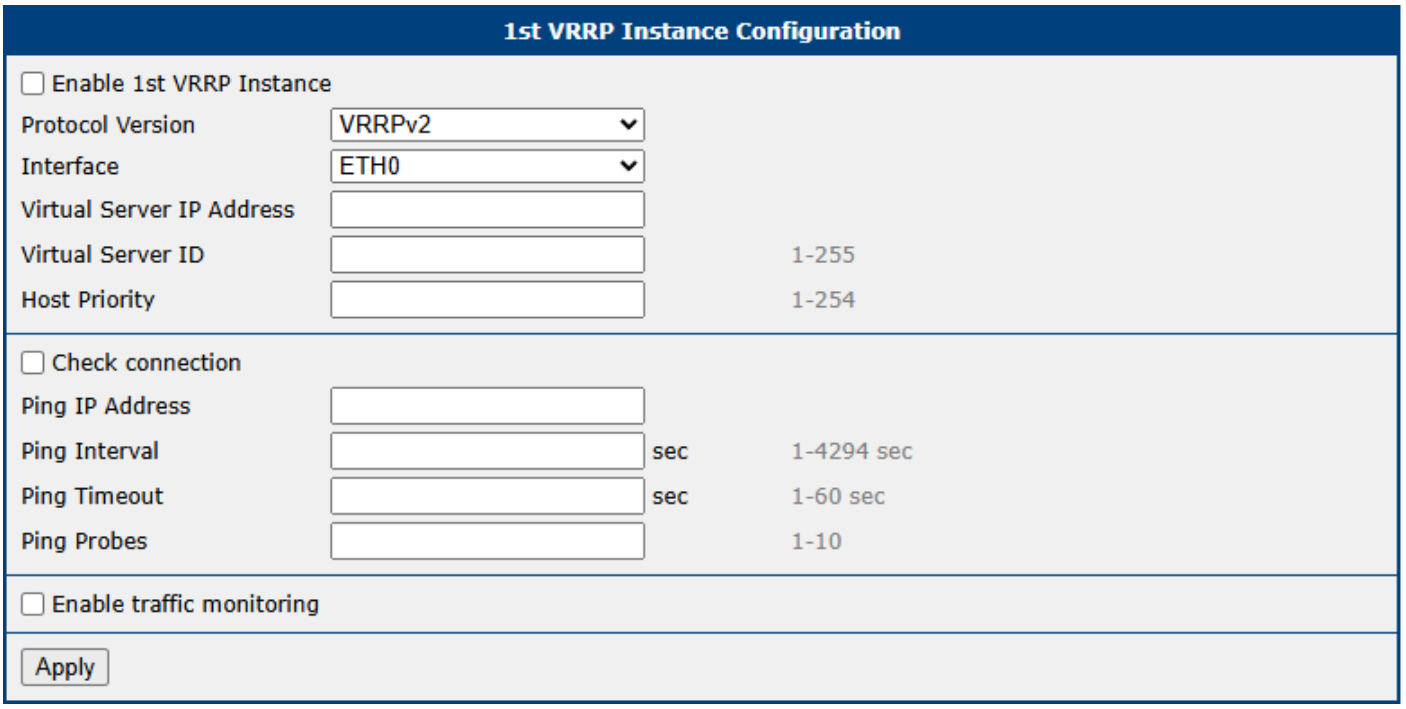
Item	Description
Create VLAN connection	Enables the creation and configuration of this VLAN interface.
DHCP Client (IPv4/IPv6)	Enables or disables the DHCP client for the VLAN interface. When enabled, the interface will request an IP address from a DHCP server on the network.
IP Address	Assigns a static IPv4 or IPv6 address to the VLAN interface.

Item	Description
Subnet Mask / Prefix	Defines the subnet mask (for IPv4) or prefix length (for IPv6) for the static IP address.
Interface	Selects the parent physical Ethernet interface (*ETH0* or *ETH1*) to which this VLAN will be bound.
VLAN ID	Specifies the unique identifier (1–4094) for the VLAN. This ID is used to tag traffic belonging to this virtual network.
MTU	Sets the Maximum Transmission Unit (MTU) in bytes for this VLAN interface. If left blank, the default value of the parent interface is used.
Enable dynamic DHCP leases	Enables the built-in DHCP server for this VLAN, which can dynamically assign IPv4 and IPv6 addresses to clients. • **IP Pool Start**: The first IP address in the DHCP assignment pool. • **IP Pool End**: The last IP address in the DHCP assignment pool. • **Lease Time**: The duration in seconds for which an IP address is leased to a client (default is 600).
Enable static DHCP leases	Enables static IP address assignments based on a client's MAC address. Up to 32 static leases can be defined for each address family (IPv4 and IPv6). • **MAC Address**: The hardware address of the client device. • **IP Address**: The fixed IPv4 address to be assigned to the client. • **IPv6 Address**: The fixed IPv6 address to be assigned to the client.
Enable IPv6 prefix delegation	Configures the router to request a block of IPv6 addresses from an upstream router, which can then be used to assign addresses to clients on this VLAN. • **Subnet ID**: The identifier for the requested subnet. • **Subnet ID Width**: The size of the subnet ID in bits.

VRRP

The Virtual Router Redundancy Protocol (VRRP) is a standard network protocol that provides automatic default gateway redundancy. It creates a virtual router, represented by a shared floating IP address, which is managed by a primary (Master) router and one or more Backup routers. If the Master router fails, a Backup router automatically takes over its role, ensuring that devices on the LAN maintain network connectivity without manual intervention. This is particularly useful for adding cellular redundancy to a primary wired connection or for creating a high-availability setup between two cellular links.

The router supports up to two VRRP instances, which can be configured on the *Configuration → VRRP* page.



VRRP Configuration Page

VRRP Instance Configuration

To enable and configure a VRRP instance, check the *Enable VRRP* box and configure the following parameters:

Item	Description
Protocol Version	Specifies the VRRP version to be used. • **VRRPv2**: The original standard, widely supported, for IPv4 networks. • **VRRPv3**: The newer standard that adds support for IPv6 networks.
Interface	Selects the network interface (e.g., *ETH0*) on which VRRP advertisements will be sent and received.
Virtual Server IP Address	Sets the shared virtual IP address. This address must be identical for all routers in the VRRP group and serves as the default gateway for all LAN devices.
Virtual Server ID	Defines the identifier for the virtual router group. The range is 1–255. This ID must be identical for all routers participating in the same VRRP group.
Host Priority	Sets the priority value used to elect the Master router. The range is 1–254 (default is 100). • The router with the highest priority value becomes the Master. • If the Virtual Server IP matches the interface's real IP, the priority is automatically set to 255 (IP Address Owner), overriding this setting.

Connection Checking

The *Check connection* feature adds a crucial layer of reliability by actively testing the health of the router's WAN connection. While VRRP itself detects router failures, this feature can detect upstream network outages even if the router is still running.

When enabled, the Master router periodically sends ICMP echo requests (pings) to a specified target IP address. If no replies are received after a configurable number of attempts, the router assumes the connection has failed and lowers its VRRP priority, triggering a failover to a Backup router.

> **Info**
>
> For reliable connection monitoring, ping a stable public IP address (e.g., a public DNS server like 8.8.8.8). In a private network, you can ping a remote gateway that is directly accessible or available via a VPN.

The *Enable traffic monitoring* option optimizes this process by suspending ping tests as long as any other traffic is received on the interface. This confirms the connection is active and reduces unnecessary data usage.

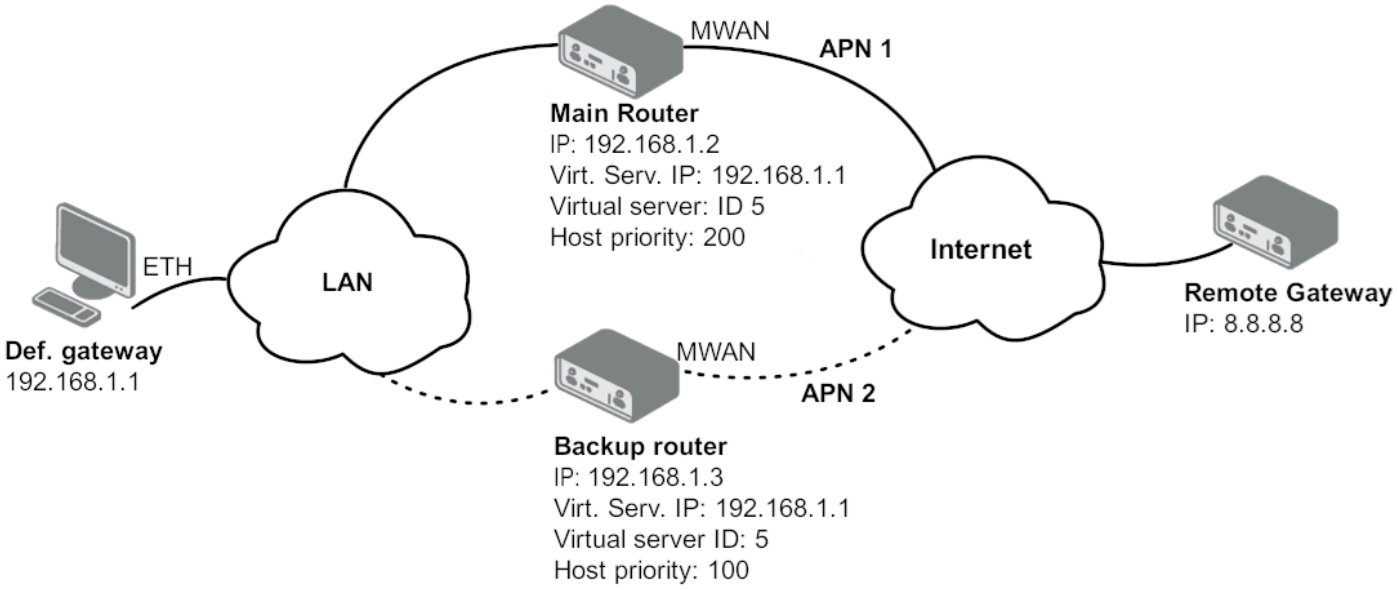
Item	Description
Ping IP Address	The destination IP address for the ICMP echo requests. Domain names are not supported.
Ping Interval	The time in seconds between each ping request.
Ping Timeout	The time in seconds to wait for a response to each ping.
Ping Probes	The number of consecutive failed pings before the connection is declared down.

VRRP Example

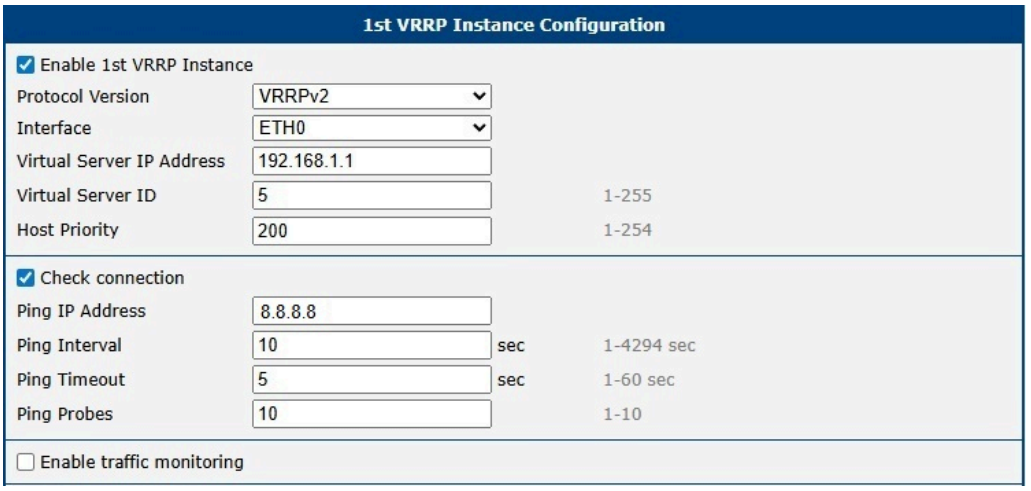
This example illustrates a high-availability topology using two routers, each with an independent cellular connection. For maximum redundancy, APN 1 and APN 2 are provided by different mobile operators.

- **LAN Side:** Both routers share the Virtual IP address **192.168.1.1** (Virtual Server ID 5). LAN clients use this IP as their default gateway, unaware of the physical routers.
- **Priorities:** The Main router (Real IP **192.168.1.2**) is configured with a higher priority of **200**, making it the Master. The Backup router (Real IP **192.168.1.3**) has a lower priority of **100**.
- **WAN Side:** To ensure end-to-end connectivity, both routers monitor a reliable public target (**8.8.8.8**) via their respective cellular WAN interfaces.

If the Main router fails to receive a ping response from 8.8.8.8, it automatically lowers its priority. The Backup router then becomes the new Master and takes over the Virtual IP, ensuring uninterrupted Internet access for all LAN clients.



Topology of VRRP Configuration Example



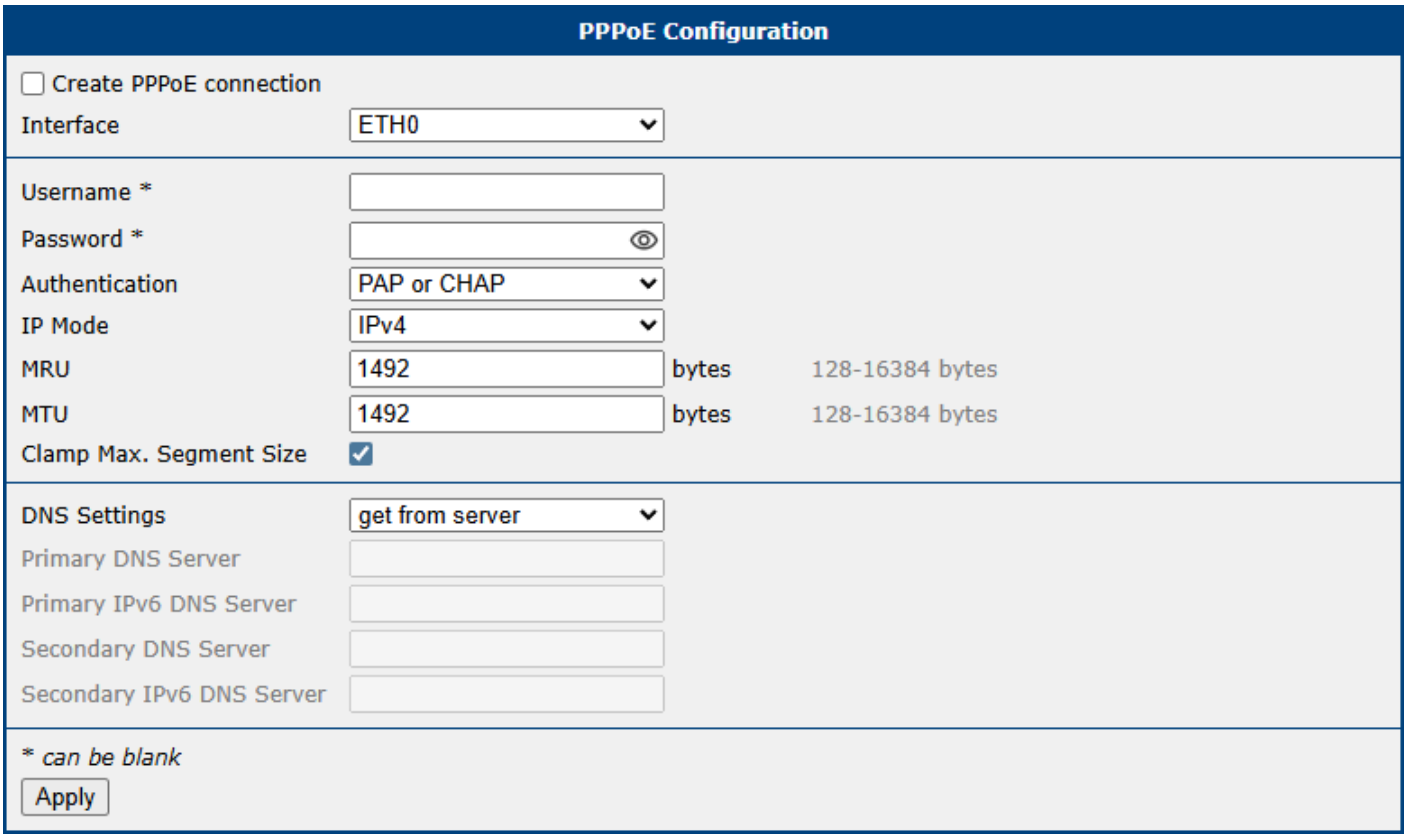
Main Router Configuration

Configure the Backup router identically to the Main router, with one exception: set the *Host Priority* to **100**. The *Check connection* settings should remain the same.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol used to encapsulate PPP frames within Ethernet frames. It is commonly used to establish a connection with a broadband modem (e.g., ADSL) or other network device that acts as a PPPoE server. The router's PPPoE client allows it to authenticate and establish a session, after which it receives a public IP address and can forward traffic to the Internet.

The PPPoE settings are available on the *Configuration → PPPoE* page.



PPPoE Configuration

Item	Description
Create PPPoE connection	Enables the PPPoE client on the selected interface. When checked, the router will automatically attempt to establish a connection on boot.
Interface	Selects the Ethernet interface (*ETH0* or *ETH1*) on which the PPPoE client will operate.
Username	The username required for authentication with the PPPoE server.
Password	The password for the specified username.
Authentication	Specifies the authentication protocol to be used. • **PAP or CHAP**: Allows the router to negotiate and use either protocol (default). • **PAP**: Forces the use of Password Authentication Protocol. • **CHAP**: Forces the use of Challenge-Handshake Authentication Protocol.
IP Mode	Defines the IP protocol version for the connection. • **IPv4**: Establishes an IPv4-only session (default). • **IPv6**: Establishes an IPv6-only session. • **IPv4/IPv6**: Enables a dual-stack session for both IPv4 and IPv6.
MRU	The Maximum Receive Unit in bytes — the largest packet size the router can receive. The default is 1492 B.
MTU	The Maximum Transmission Unit in bytes — the largest packet size the router can transmit. The default is 1492 B.
Clamp Max. Segment Size	When enabled (default), automatically adjusts the TCP Maximum Segment Size (MSS) to prevent fragmentation, improving performance and reliability.

Item	Description
DNS Settings	Configures how DNS servers are obtained. • **Get from server**: Automatically uses the DNS servers provided by the PPPoE server (default). • **Manual**: Allows you to specify primary and secondary DNS servers manually.
Primary DNS Server	Primary IPv4 address of the DNS server.
Primary IPv6 DNS Server	Primary IPv6 address of the DNS server.
Secondary DNS Server	Secondary IPv4 address of the DNS server.
Secondary IPv6 DNS Server	Secondary IPv6 address of the DNS server.

Warning

Setting an incorrect MTU or MRU value can lead to packet fragmentation or loss, resulting in a failed or unreliable connection. Use the default value of 1492 B unless your provider requires a different setting.

WiFi

WiFi Access Point

Important Note on Upgrading to Firmware 6.6.0

When upgrading from a firmware version prior to 6.6.0, any separate *Country* settings for the Wi-Fi Access Point (AP) and Station (STA) modes will be consolidated into a single, unified *Country* setting. This change ensures regulatory compliance and simplifies configuration.

Info

- The router supports configuring two separate WLANs (**multiple SSIDs**) for access point 1 (AP1) and access point 2 (AP2). However, both access points must share the same radio settings (channel, mode, channel width, etc.).
- The router supports operating as both an access point (AP) and a station (STA) **simultaneously**.
- **RADIUS** (Remote Authentication Dial-In User Service) is supported as a networking protocol for centralized authentication, authorization, and accounting (AAA). The router acts only as a RADIUS client, communicating with an external RADIUS server.

To enable Wi-Fi access point mode, check the *Enable Wi-Fi AP* box at the top of the *Configuration → WiFi → Access Point 1* or *Access Point 2* configuration page. In this mode, the router operates as an access point, allowing other devices in *station (STA)* mode to connect.

WiFi AP 1 Configuration

☐ Enable WiFi AP 1

Country: all countries [Change]

APs are not allowed to operate in 5 GHz and 6 GHz frequency bands in world-wide mode.

	IPv4	IPv6	
IP Address			
Subnet Mask / Prefix			
Bridged	no		

☐ Enable dynamic DHCP leases

	IPv4	IPv6		
IP Pool Start				
IP Pool End				
Lease Time	600	600	sec	5-86400 sec

☐ Enable IPv6 prefix delegation

Subnet ID *			
Subnet ID Width *		bits	8-32 bits

SSID	
Broadcast SSID	enabled
SSID Isolation	disabled
Client Isolation	disabled
WMM	disabled

The following radio settings are common for all Access Points on the WiFi module.

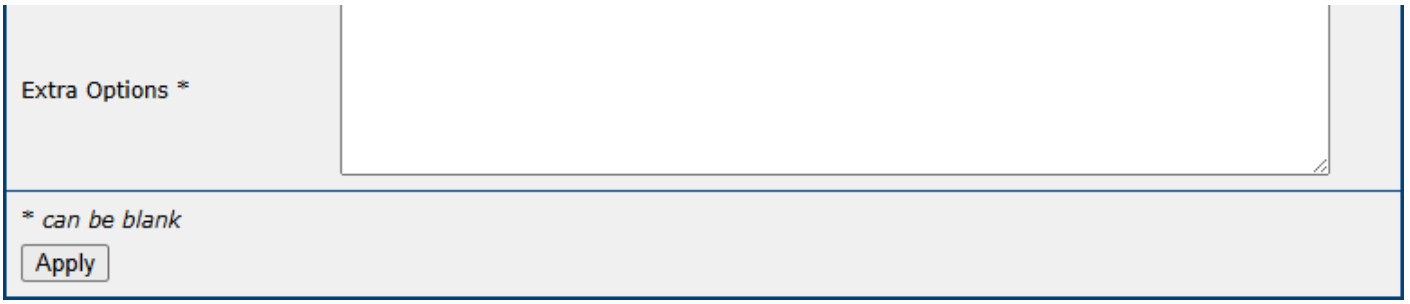
Follow STA radio settings	☐
HW Mode	IEEE 802.11b
Bandwidth	20 MHz
Channel	Auto
Short GI	disabled

Authentication	open
Encryption	none
WPA PSK Type	256-bit secret
WPA PSK Secret	
RADIUS Auth Server IP	
RADIUS Auth Password	
RADIUS Auth Port *	1812
RADIUS Acct Server IP *	
RADIUS Acct Password *	
RADIUS Acct Port *	1813

Access List	disabled
Accept/Deny List *	

[Load from File...]

Syslog Level	informational



WiFi Access Point Configuration Page

Item	Description
Enable WiFi AP	Enables the Wi-Fi access point (AP). Both Access Point 1 (AP1) and Access Point 2 (AP2) can be enabled and operated simultaneously.
Country	A single Wi-Fi country code applies to all AP and STA interfaces and is configured on a separate page (accessible via the *Change* button), refer to WiFi Country. After changing the country, you must review the *HW Mode*, *Bandwidth*, and *Channel* settings.
IP Address	A fixed IP address for the Wi-Fi interface. Use standard IPv4 or IPv6 notation.
Subnet Mask / Prefix	Specifies the subnet mask for an IPv4 address or the prefix length (0 to 128) for an IPv6 address.
Bridged	Activates bridge mode: • **no**: Bridged mode is disabled (default). The WLAN is a separate network from the LAN. • **yes**: Bridged mode is enabled. The WLAN is connected to one or more LAN networks. In this mode, most network settings in this table are ignored, and the router uses the settings of the bridged LAN interface. See the *Bridge Notes* in Ethernet for further details.
Enable dynamic DHCP leases	Enables the dynamic allocation of IP addresses using the DHCP (or DHCPv6) server.
IP Pool Start	The start of the IP address range assigned to DHCP clients.
IP Pool End	The end of the IP address range assigned to DHCP clients.
Lease Time	The duration (in seconds) for which a client can use its assigned IP address.
Enable IPv6 prefix delegation	Enables prefix delegation for IPv6 clients.
Subnet ID	The decimal value of the Subnet ID for the interface. The maximum value is determined by the *Subnet ID Width*.
Subnet ID Width	The maximum Subnet ID width, which depends on your site's configuration. The remaining bits (up to 64) are used for the prefix.
SSID	The unique identifier (name) of the Wi-Fi network. Access Point 1 (AP1) and Access Point 2 (AP2) can have different SSIDs.

Item	Description
Broadcast SSID	Defines how the SSID is broadcast in the beacon frame: • **enabled**: The SSID is included in the beacon frame (standard behavior). • **zero length**: The SSID is omitted from the beacon frame. Requests to send beacon frames are ignored. • **clear**: SSID characters in the beacon are replaced with zeros, maintaining the original length. Requests for beacon frames are ignored.
SSID Isolation	When enabled with a selected zone, clients on this access point cannot communicate with clients on other access points that have a different zone selected.
Client Isolation	If enabled, clients connected to this access point are prevented from communicating with each other. If disabled, the AP functions like a switch, allowing clients on the same LAN to communicate.
WMM	Enables basic QoS (Quality of Service) for the Wi-Fi network. Suitable for simple applications that require QoS but does not guarantee network throughput.
Follow STA radio settings	When enabled, if the STA mode is connected to an external access point, the router's own AP radio settings will automatically adjust to match those of the external AP.
HW Mode[1]	Specifies the Wi-Fi standard supported by the access point. Available options include: IEEE 802.11b (2.4 GHz), IEEE 802.11b+g (2.4 GHz), IEEE 802.11b+g+n (2.4 GHz), IEEE 802.11a (5 GHz), IEEE 802.11a+n (5 GHz), IEEE 802.11ac (5 GHz). This setting is shared by both Access Point 1 and Access Point 2.
Bandwidth[1]	Selects the transfer bandwidth. This option may be unavailable for some hardware modes. If the selected bandwidth is occupied, the router may automatically switch to a lower bandwidth. This setting is shared by both Access Point 1 and Access Point 2.
Channel[1]	The channel on which the Wi-Fi access point operates. Available channels depend on the selected *Country*. Select *Auto* to allow the router to choose the optimal channel automatically. **If you change the country, review this setting**, as the previously selected channel may no longer be valid. This setting is shared by both Access Point 1 and Access Point 2. Note: When *40 MHz* bandwidth is selected, in the 2.4 GHz band the channel number refers to the primary (20 MHz) channel; in the 5 GHz and 6 GHz bands, it refers to the center frequency of the 40 MHz channel. On NAM routers, only channels 1 to 11 are supported in the 2.4 GHz band.
Short GI	Available for 802.11n mode — enables a short guard interval (400 ns instead of 800 ns) to improve data transmission efficiency. This setting is shared by both Access Point 1 and Access Point 2.
Authentication	Defines the access control method for the Wi-Fi network: • **open**: `[insecure]` No authentication required. Encryption is not available. • **shared**: `[insecure]` Basic authentication with a WEP key. • **WPA-PSK**: `[insecure]` Pre-Shared Key authentication with WPA encryption. • **WPA2-PSK**: `[insecure]` Pre-Shared Key authentication with WPA2 encryption (AES). • **WPA3-PSK**: Simultaneous Authentication of Equals (SAE) with WPA3 encryption (AES). • **WPA-Enterprise**: `[insecure]` RADIUS-based authentication via an external server. • **WPA2-Enterprise**: RADIUS-based authentication with stronger encryption. • **WPA3-Enterprise**: RADIUS-based authentication with stronger encryption.

Item	Description
Encryption	Specifies the type of data encryption: • **none**: `[insecure]` No data encryption. • **WEP**: `[insecure]` Wired Equivalent Privacy. • **TKIP**: `[insecure]` Temporal Key Integrity Protocol, used for WPA. • **AES**: Advanced Encryption Standard, used for WPA2/WPA3.
WPA PSK Type	Specifies the format of the WPA Pre-Shared Key: • **256-bit secret**: A 64-character hexadecimal key. • **ASCII passphrase**: A passphrase of 8 to 63 characters. • **PSK File**: Absolute path to a file containing key-MAC address pairs.
WPA PSK Secret	The secret key or passphrase for WPA-PSK authentication.
RADIUS Auth Server IP	The IPv4 or IPv6 address of the RADIUS authentication server.
RADIUS Auth Password	The access password for the RADIUS authentication server.
RADIUS Auth Port	The port number of the RADIUS authentication server (default is 1812).
RADIUS Acct Server IP	The IPv4 or IPv6 address of the RADIUS accounting server (if different from the authentication server).
RADIUS Acct Password	The access password for the RADIUS accounting server.
RADIUS Acct Port	The port number of the RADIUS accounting server (default is 1813).
Access List	Defines the mode of the client access list: • **disabled**: The access list is not used. • **accept**: Only clients in the list can access the network. • **deny**: Clients in the list are blocked from accessing the network.
Accept/Deny List	A list of client MAC addresses for network access control. Each MAC address should be entered on a new line.
Syslog Level	Defines the logging level for messages sent to the system log: • **verbose debugging**: The highest level of detail. • **debugging** • **informational**: The default level. • **notification** • **warning**: The lowest level.
Extra options	Allows the user to define additional parameters for `hostapd`. The options are appended to the configuration file. Use this feature only if you are familiar with its functionality. For more information, refer to the `hostapd.conf` configuration file.

[1] The availability of configuration options may vary depending on the specific WiFi module and can be affected by the selected country code.

WiFi Station

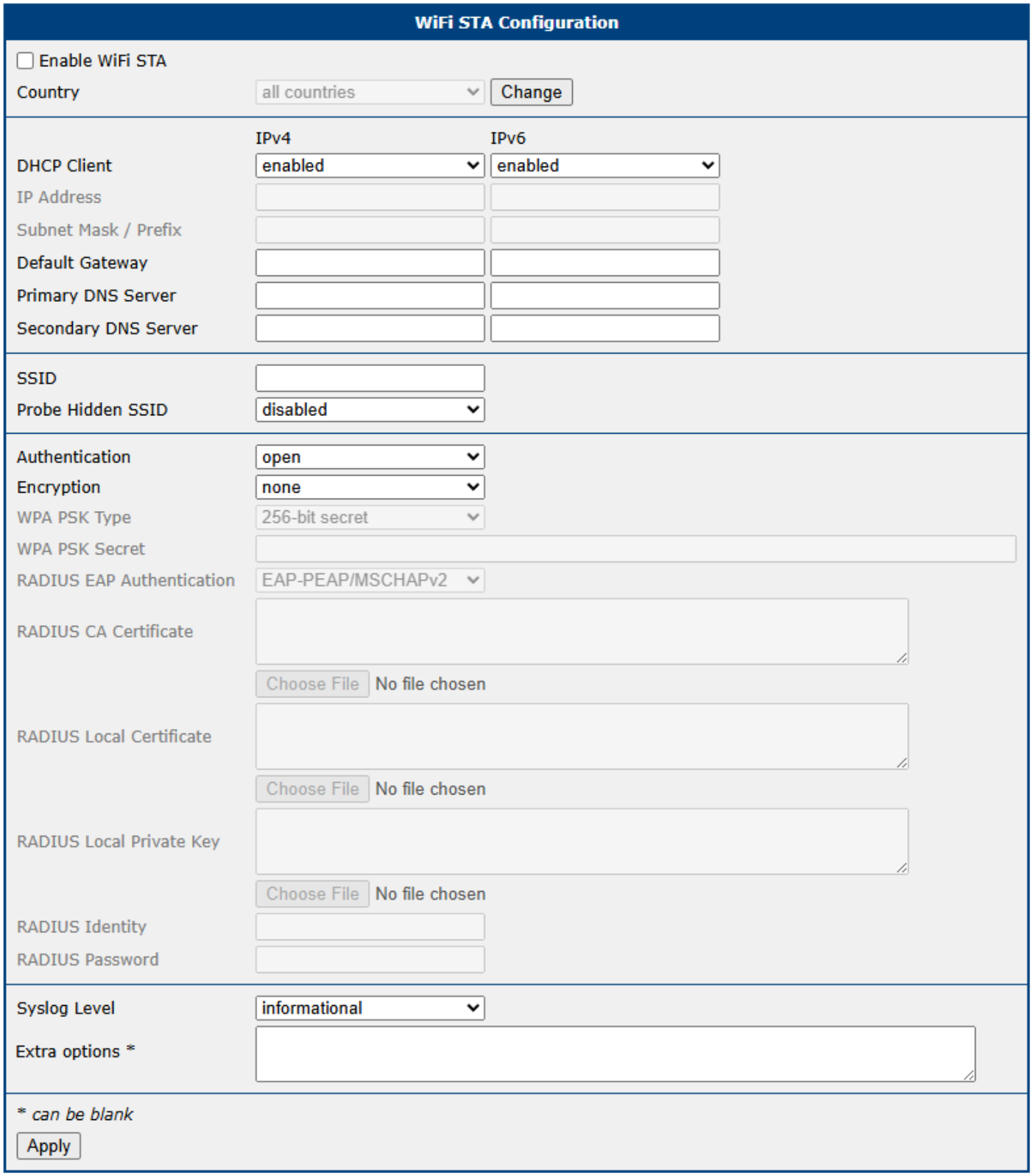
Important Note on Upgrading to Firmware 6.6.0

When upgrading from a firmware version prior to 6.6.0, any separate *Country* settings for the Wi-Fi Access Point (AP) and Station (STA) modes will be consolidated into a single, unified *Country* setting. This change ensures regulatory compliance and simplifies configuration.

Info

- You can find and connect to an available Wi-Fi network using *Status → Wi-Fi → WiFi Scan*.
- The router supports operating as both an access point (AP) and a station (STA) **simultaneously**.
- For networks using **WPA-Enterprise** security (RADIUS authentication), the station mode supports only the **EAP-PEAP/MSCHAPv2** (both PEAPv0 and PEAPv1) and **EAP-TLS** authentication methods.

Activate Wi-Fi station mode by checking the *Enable WiFi STA* box at the top of the *Configuration → WiFi → Station* configuration page. In this mode, the router functions as a client station, connecting to an available access point (AP) and bridging its wired connection to the Wi-Fi network. In station mode, the Wi-Fi channel and bandwidth are determined by the associated access point.



WiFi Station Configuration Page

Item	Description
Enable WiFi STA	Enables the Wi-Fi station (STA) mode.
Country	A single Wi-Fi country code applies to all AP and STA interfaces and is configured on a separate page (accessible via the *Change* button), refer to WiFi Country. After changing the country, you must review your radio settings.

Item	Description
DHCP Client	Activates or deactivates the DHCP client (or DHCPv6 client for IPv6).
IP Address	Specifies a fixed IP address for the Wi-Fi interface. Use standard IPv4 or IPv6 notation.
Subnet Mask / Prefix	Defines the subnet mask for an IPv4 address or the prefix length (0 to 128) for an IPv6 address.
Default Gateway	Specifies the IP address of the default gateway. Packets with destinations not found in the routing table are sent to this gateway.
Primary DNS Server	Specifies the primary IP address of the DNS server.
Secondary DNS Server	Specifies the secondary IP address of the DNS server.
SSID	The unique identifier (name) of the Wi-Fi network to connect to.
Probe Hidden SSID	An access point with a hidden SSID does not broadcast its name, preventing the station from connecting automatically. Enable this option to force the station to probe for a specific hidden SSID. If you are not connecting to a hidden network, keep this disabled to reduce unnecessary radio transmissions.
Authentication	Access control methods for the Wi-Fi network: • **open**: `[insecure]` No authentication required. • **shared**: `[insecure]` Basic authentication with a WEP key. • **WPA-PSK**: `[insecure]` Authentication using a PSK with the WPA standard. • **WPA2-PSK**: `[insecure]` Authentication using a PSK with the WPA2 standard. • **WPA3-PSK**: Authentication using SAE with the WPA3 standard. • **WPA-Enterprise**: `[insecure]` Authentication using a RADIUS server with the WPA standard. • **WPA2-Enterprise**: Authentication using a RADIUS server with the WPA2 standard. • **WPA3-Enterprise**: Authentication using a RADIUS server with the WPA3 standard.
Encryption	The data encryption method: • **none**: `[insecure]` No encryption. • **WEP**: `[insecure]` Static encryption with WEP keys (may not be supported on some models). • **TKIP**: `[insecure]` Legacy dynamic encryption used with WPA/WPA2. • **AES**: Modern dynamic encryption used with WPA2/WPA3.
WPA PSK Type	The format of the key for WPA-PSK authentication: • **256-bit secret**: A 64-character hexadecimal key. • **ASCII passphrase**: A passphrase of 8 to 63 characters.
WPA PSK Secret	The secret key or passphrase for WPA-PSK authentication.
RADIUS EAP Authentication	The EAP protocol used for RADIUS authentication: • **EAP-PEAP/MSCHAPv2**: Uses TLS to protect legacy EAP authentication. • **EAP-TLS**: Uses TLS for mutual authentication between the client and server.
RADIUS CA Certificate	The Certificate Authority (CA) certificate used to verify the server certificate during EAP-TLS authentication.
RADIUS Local Certificate	The client certificate required for EAP-TLS authentication.

Item	Description
RADIUS Local Private Key	The private key associated with the client certificate for EAP-TLS authentication.
RADIUS Identity	The identity (username) used to connect to the RADIUS server.
RADIUS Password	The password used to authenticate the RADIUS identity (for EAP-PEAP/MSCHAPv2). For EAP-TLS, this field is optional and specifies the decryption key for the local private key if it is encrypted.
Syslog Level	Defines the logging level for messages sent to the system log: • **verbose debugging**: The highest level of detail. • **debugging** • **informational**: The default level. • **notification** • **warning**: The lowest level.
Extra options	Allows the user to define additional parameters for `wpa_supplicant`. The options are appended to the configuration file. Use this feature only if you fully understand the implications. For more information, refer to the `wpa_supplicant.conf` configuration file.

WiFi Country

The *Configuration → WiFi → Country* page is used to set a single, global country code that applies to all Wi-Fi interfaces, including both Access Point (AP) and Station (STA) modes. This setting is crucial for ensuring that the router's radio transmissions comply with the regulatory requirements of the region where it is operated.

From the list, select the appropriate country where the router will be used. For proper and optimal Wi-Fi functionality, **always set the correct country code**.

Alternatively, you can select the *all countries* option. Please note that in this mode, the Access Point (AP) is not permitted to operate in the 5 GHz and 6 GHz frequency bands to ensure broad regulatory compliance. However, if the station (STA) connects to an access point broadcasting a country code different from the *all countries* setting, additional channels may become available in AP mode that are otherwise restricted under the *all countries* configuration.

Warning

After selecting a new country, you must click the *Apply* button to save the change. Changing the country code may invalidate previous radio settings (such as *Channel* or *Bandwidth*). As a result, the Wi-Fi AP or STA may fail to operate until it is reconfigured. After changing the country, you must review and re-apply your Wi-Fi AP and STA configurations to ensure they are still valid and that your devices can connect.

Info

- On global models, the Country Code selection is limited to *all countries* and *US* only.
- On North American (NAM) models, this option is not available, as the country code is permanently set to *US* to comply with regional regulations.

Backup Routes

The *Backup Routes* feature provides a mechanism for managing WAN connectivity, enabling automatic failover and load balancing across multiple Internet sources. The configuration is managed on the *Configuration → Backup Routes* page.

You can choose to let the router manage WAN connections automatically using its default priorities, or customize the behavior to meet specific network requirements.

Warning

- Some WAN interfaces (e.g., Wi-Fi, secondary Ethernet ports) may not be available on all router models.
- When using default priorities, an Ethernet interface will not be considered a valid WAN connection unless it has a static IP address configured or its DHCP client is enabled.
- In default priority mode, merely unplugging an Ethernet cable will not trigger a failover. The interface must be administratively down or fail to obtain an IP address.

Default Failover

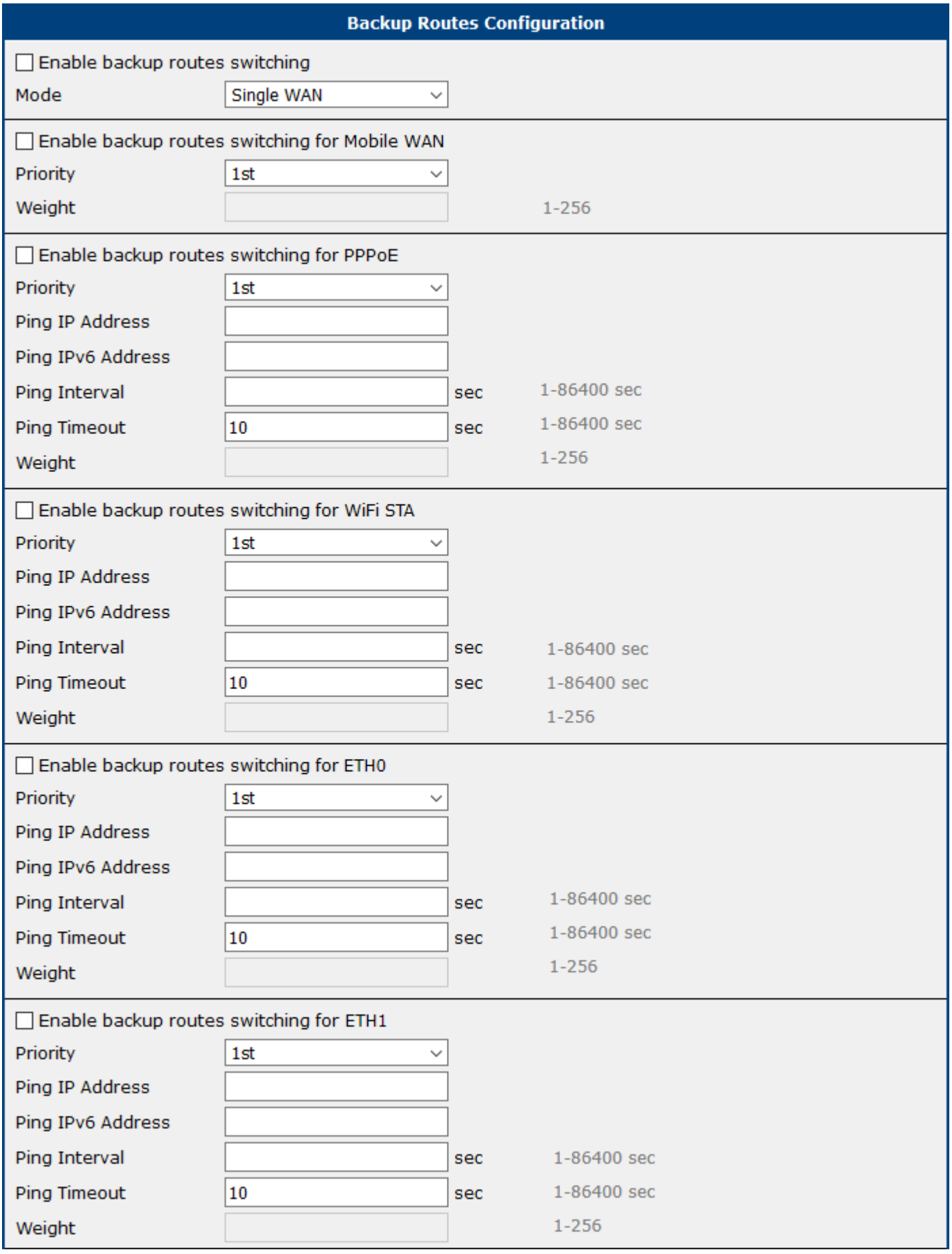
If the *Enable backup routes switching* option is unchecked, the router uses a predefined, internal priority list to select the active WAN interface. The default interface priority is as follows:

1. **Mobile WAN** (`usb0` or `usb1`)
2. **PPPoE** (`pppoe0`)
3. **Wi-Fi STA** (`wlan0`)
4. **ETH1** (`eth1`)
5. **ETH0** (`eth0`)

Based on this order, the router will only use the *ETH1* interface if the Mobile WAN, PPPoE, and Wi-Fi connections are all unavailable. Note that a LAN interface (like *ETH0*) can become a WAN interface under certain conditions, which may have security implications. Ensure your firewall and NAT rules are configured accordingly.

Customized Backup Routes

To gain full control over failover and load balancing, check the *Enable backup routes switching* box. This allows you to define interface priorities, connection checking parameters, and select one of three operational modes.



Backup Routes Configuration Page

Operational Modes

Item	Description
Mode	Selects the operational mode for managing WAN interfaces: • **Single WAN**: Only one WAN interface is active at a time. If the primary interface fails, the router switches to the next available interface by priority. The router is accessible from outside only on the active interface. • **Multiple WANs**: Same as Single WAN, with one difference: the router is accessible from outside on all enabled WAN interfaces simultaneously. • **Load Balancing**: Traffic is distributed across multiple WAN interfaces simultaneously. Assign a *Weight* to each interface to control its share of traffic streams.

Interface Configuration

For each interface to include in the backup system, check its *Enable backup routes switching* box and configure the following parameters.

Item	Description
Priority	Sets the priority of the interface (1st is highest). The router always uses the highest-priority active interface.
Ping IP Address	The destination IPv4 address or domain name for ICMP echo requests used to verify connection health.
Ping IPv6 Address	The destination IPv6 address or domain name for ICMP echo requests.
Ping Interval	The time in seconds between each ping test.
Ping Timeout	The time in seconds to wait for a response before considering a ping test failed.
Weight	(Load Balancing mode only) A value from 1 to 256 that determines the traffic ratio for this interface. For example, if two interfaces have weights of 4 and 1, they will handle approximately 80% and 20% of traffic streams, respectively.

Warning

- **Load Balancing**: The traffic distribution is based on data streams, not total bandwidth. The actual data volume may not perfectly match the weight ratio, especially with a small number of concurrent connections.
- **Mobile WAN**: To use a cellular connection in a custom backup scenario, set *Check Connection* to *enable + bind* on the *Mobile WAN* configuration page.

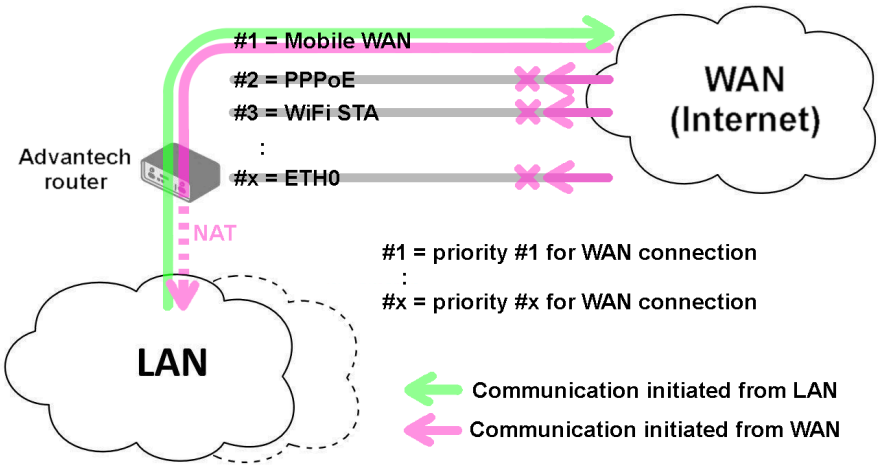
Backup Routes Examples

Example 1: Default Settings

If no settings are configured on the *Backup Routes* page, the system operates with the default priorities. This provides a simple, automatic failover mechanism.

Note: Assume all affected interfaces are correctly configured and activated on their configuration pages.

Example 1: GUI Configuration

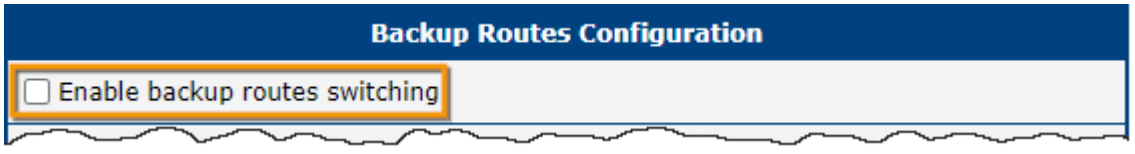


Example 1: Topology

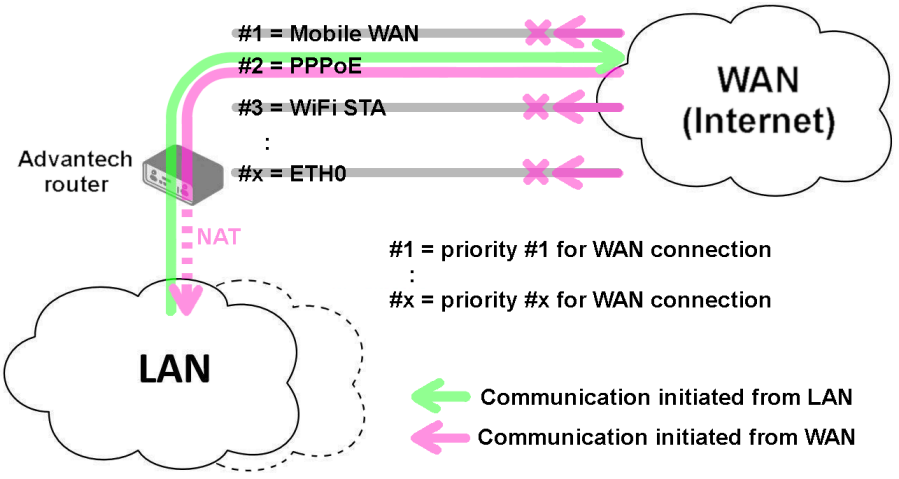
Example 2: Default Route Switching

This example shows how the default system handles a primary interface failure. If the highest-priority interface (Mobile WAN) becomes unavailable, the router automatically switches to the next interface in the default priority list (PPPoE).

Note: Assume all affected interfaces are correctly configured and activated on their configuration pages.



Example 2: GUI Configuration

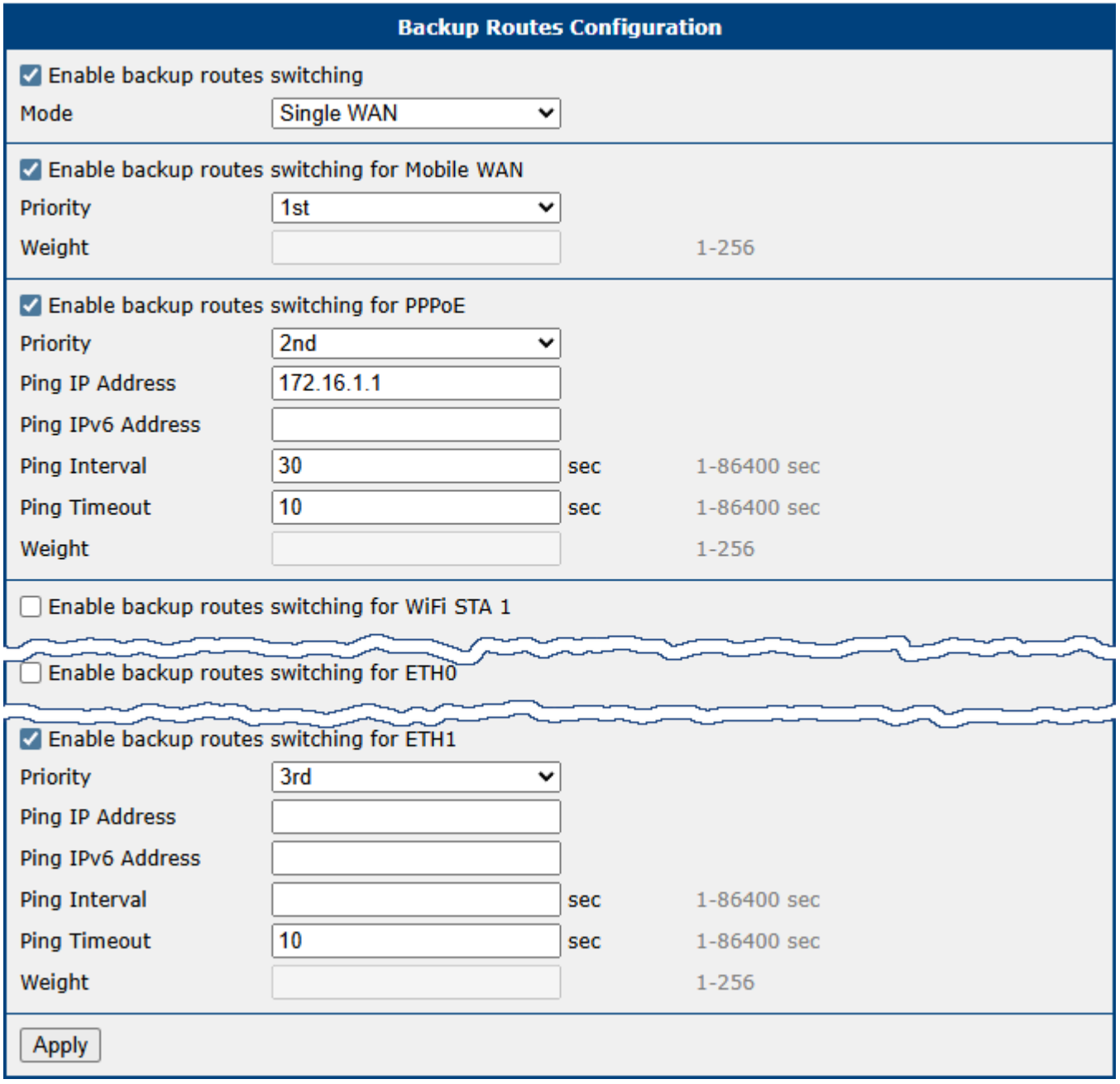


Example 2: Topology

Example 3: Custom Backup Routes

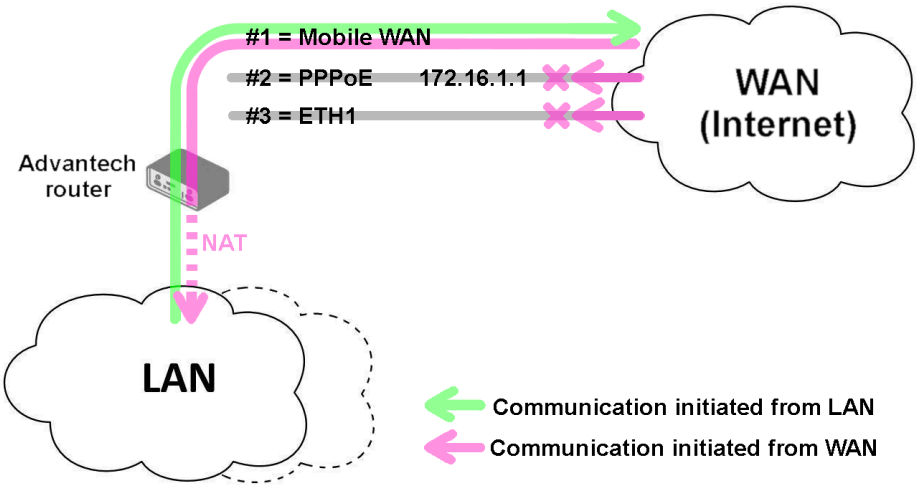
This example demonstrates a custom failover configuration using the Mobile WAN, PPPoE, and ETH1 interfaces. The Mobile WAN is set as the highest priority, followed by PPPoE, and finally ETH1. The connection status of the PPPoE tunnel is monitored by pinging 172.16.1.1.

Note: Assume all affected interfaces are correctly configured and activated on their configuration pages.



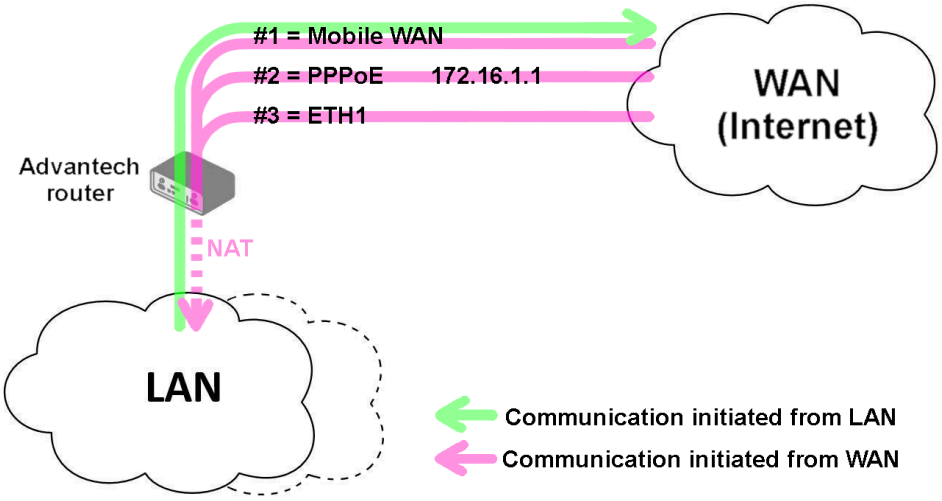
Example 3: GUI Configuration

In *Single WAN* mode, if the Mobile WAN connection fails, the router fails over to the PPPoE tunnel.



Example 3: Topology for Single WAN mode

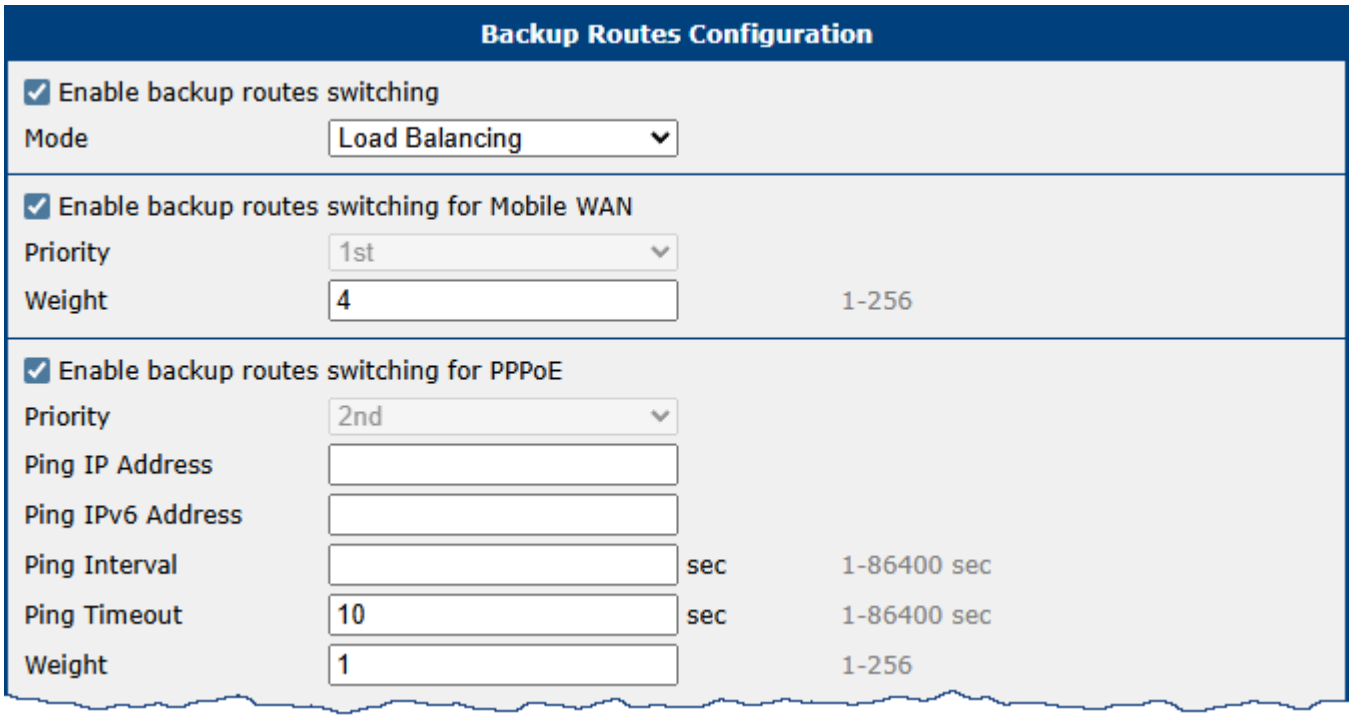
In *Multiple WANs* mode, the router is accessible via all three interfaces simultaneously, even though only one is used for outbound traffic at a time.



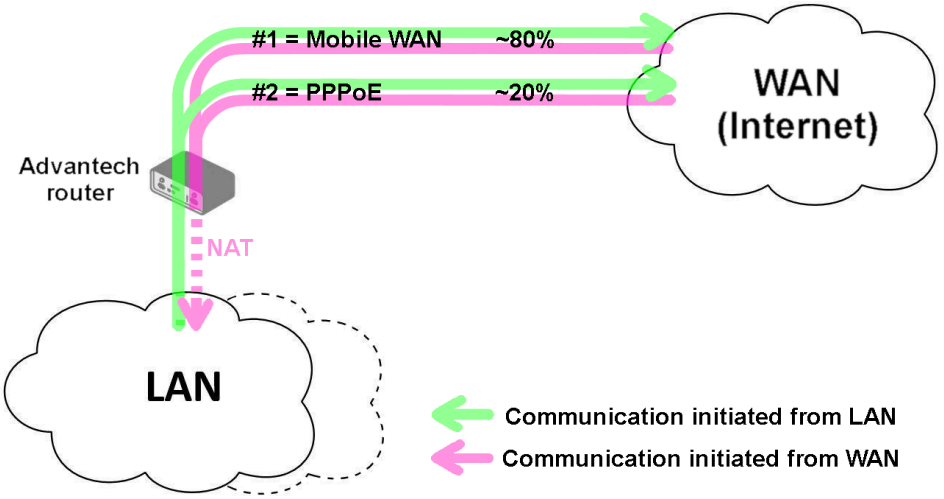
Example 3: Topology for Multiple WANs mode

Example 4: Load Balancing Mode

This example shows a load balancing configuration between the Mobile WAN and a PPPoE interface. The weights are set to 4 and 1, respectively, meaning the Mobile WAN will handle approximately 80% of traffic streams and the PPPoE interface 20%.



Example 4: GUI Configuration

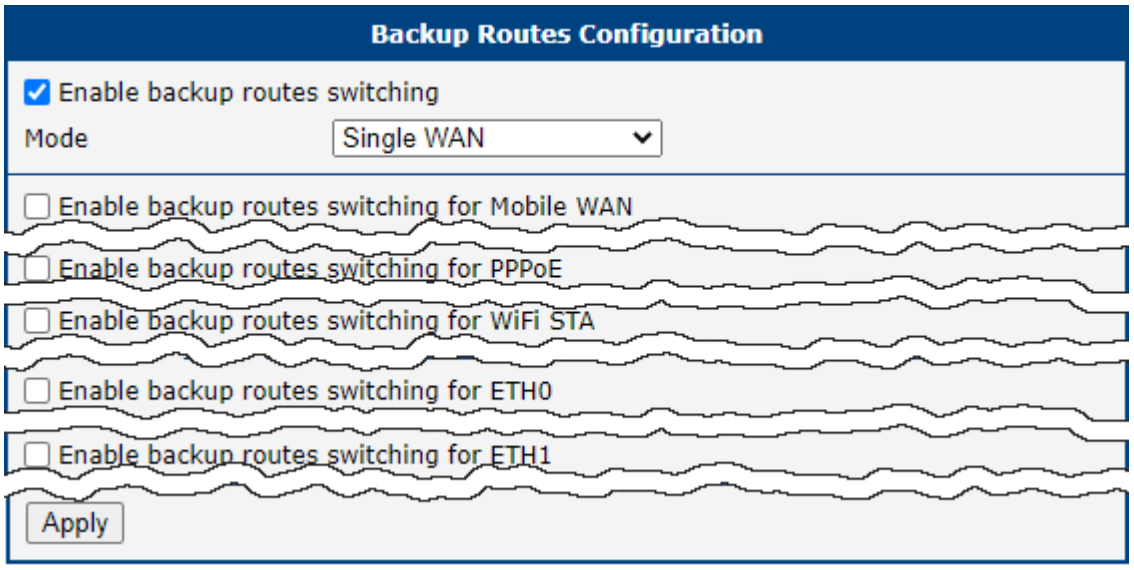


Example 4: Topology

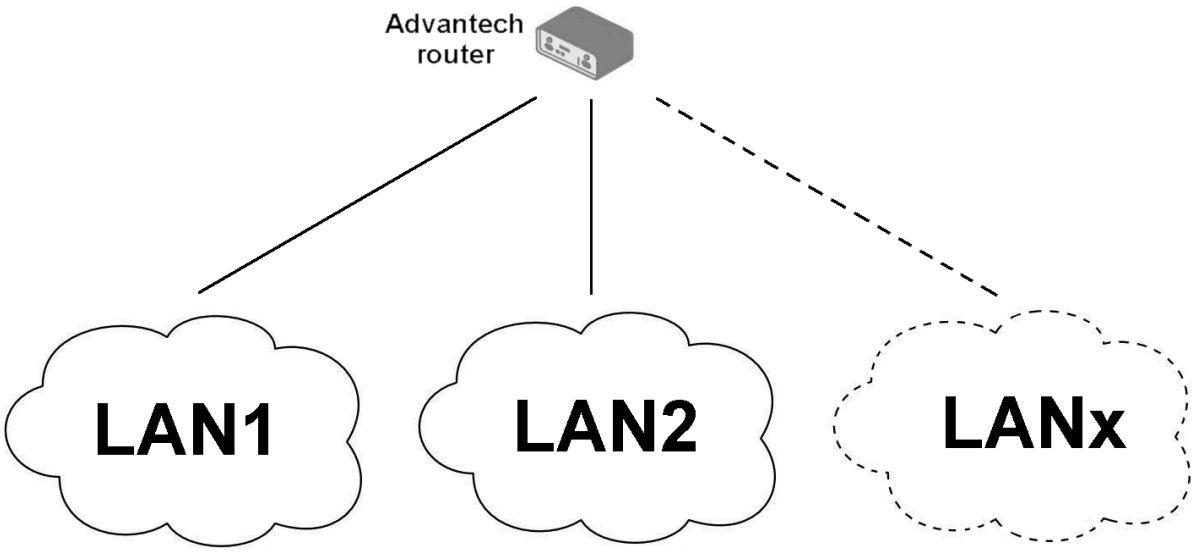
Example 5: No WAN Routes

If *Backup Routes* is enabled but no interfaces are selected for WAN routing, the router has no dedicated WAN connection and functions as a LAN router. The Mobile WAN interface will not be used, even if connected to a cellular network.

Note: Assume all affected interfaces are correctly configured and activated on their configuration pages.



Example 5: GUI Configuration

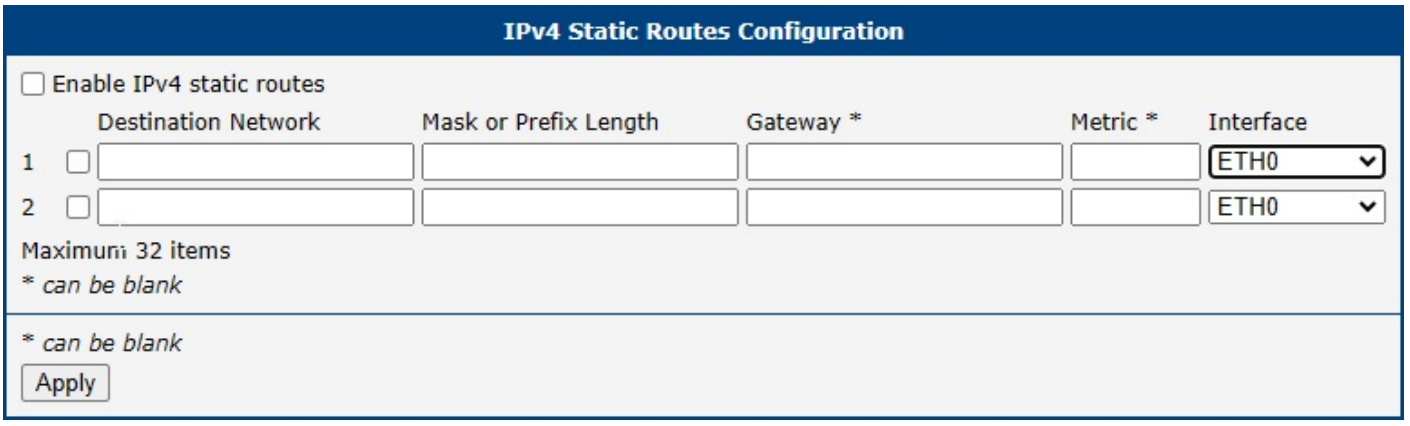


Example 5: Topology

Static Routes

Static routes are manually configured, fixed paths that define how the router should forward traffic to a specific destination network or host. Unlike dynamic routes, which are learned automatically, static routes do not change unless they are manually updated. They are ideal for small, stable networks or for defining a specific path that must always be used.

The configuration is managed on the *Static Routes* page. The router provides separate configuration tables for IPv4 and IPv6, each supporting up to thirty-two individual static routes. A new row is automatically added as you fill in the previous one.



Static Routes Configuration Page

Item	Description
Enable IPv4 static routes	The master switch for the static routing feature. If unchecked, all static routes are disabled. Individual routes must also be enabled using the checkbox in their respective rows.
Destination Network	The IP address of the target network or host for which this route is being created.
Mask or Prefix Length	The subnet mask (for IPv4) or prefix length (for IPv6) of the destination network.
Gateway	The IP address of the next-hop router that will be used to reach the destination network.
Metric	A numerical value (1–255) representing the route's priority. A lower metric indicates a more preferred route.
Interface[1]	The network interface through which the specified gateway is reachable.

[1] The *Any* option allows for the creation of routes where the gateway may not be directly connected, such as a GRE tunnel endpoint. When *Any* is selected, specifying a *Gateway* is mandatory, as it determines which interface will be used.

Firewall

The router's firewall allows you to control both incoming and outgoing IP traffic. The router supports independent IPv4 and IPv6 firewalls, including a dual-stack configuration for both protocols.

Understanding Firewall Zones

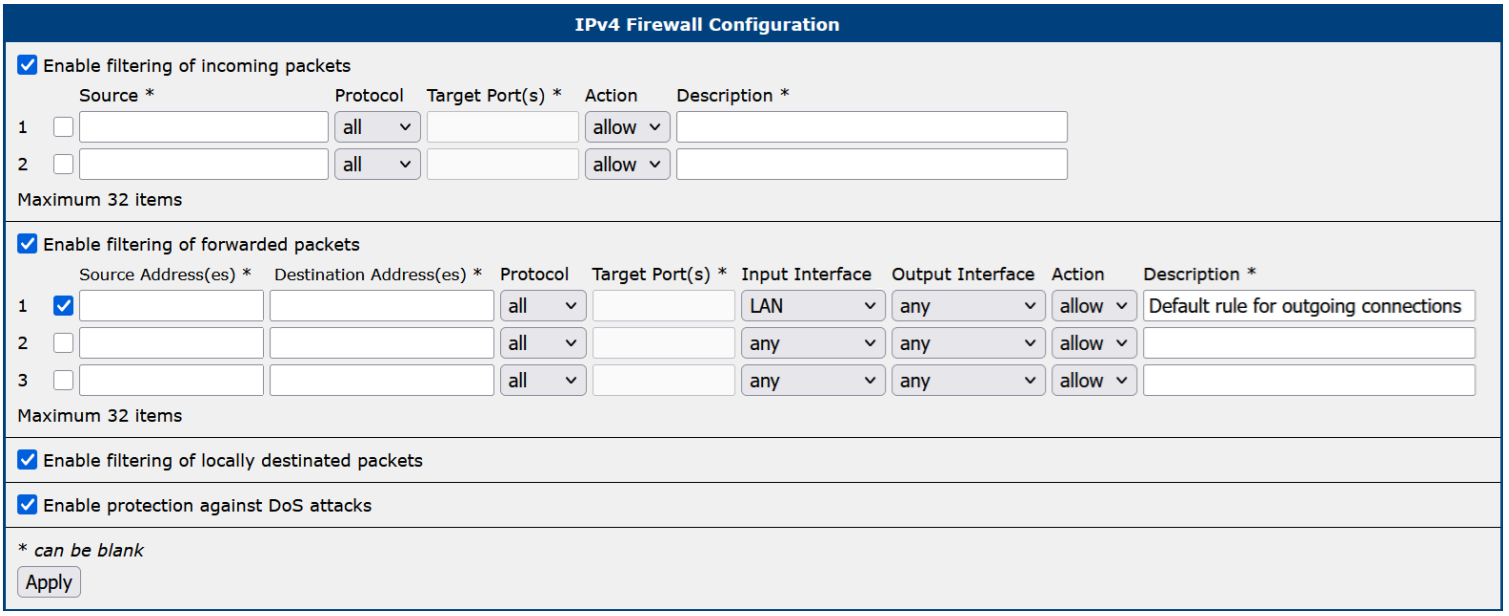
The router's firewall simplifies rule creation by grouping network interfaces into two logical zones based on their configured function: **LAN** (trusted) and **WAN** (untrusted). This assignment, not the interface name (e.g., `eth1`, `wlan0`), determines how the firewall treats its traffic.

- **LAN Zone (Trusted):** Contains all interfaces configured for your internal, local network. By default, this typically includes the Ethernet LAN ports (e.g., `eth0`, `eth1`) and any configured Wi-Fi Access Points (`wlanX`).
- **WAN Zone (Untrusted):** Contains all interfaces configured to connect to external networks like the Internet. Common examples include the cellular module (`usb0`), an Ethernet port re-configured for WAN use, or a Wi-Fi client (STA) connection (`wlanX`). For details on configuring backup WAN interfaces, refer to Backup Routes.

Default Behavior: By default, the firewall blocks all unsolicited incoming traffic from the WAN zone. Outbound traffic originating from the trusted LAN zone to the untrusted WAN zone is permitted. It is strongly recommended to review and customize the firewall rules to match your specific security requirements.

Clicking the *Firewall* item in the *Configuration* menu on the left expands it into three submenus: *IPv4*, *IPv6*, and *Sites*.

The figure below shows the default configuration page for the IPv4 firewall. The configuration fields are identical for both the *IPv4* and *IPv6* forms.



IPv4 Firewall Configuration Page

Info

Starting with firmware version 6.6.0, rule descriptions are stored directly as comments in the system's iptables configuration. This allows you to easily identify rules created via the web interface when managing the firewall from the command line (e.g., using `iptables-save`).

The first section of the configuration form defines the **incoming firewall policy**. If the *Enable filtering of incoming packets* checkbox is unchecked, all incoming connections are accepted. When enabled, and if connections originate from the WAN interface, the router checks them against the PREROUTING chain in the mangle table. The router accepts a connection only if a matching rule exists with the *Action* set to *allow*; otherwise, if no matching rule is found or the *Action* is set to *deny*, the connection is dropped.

You can define up to thirty-two rules based on IP addresses, protocols, and ports. Each rule can be enabled or disabled using the checkbox on the left of its row. A new row for the next rule appears automatically after filling in the previous one.

Please note that incoming rules apply only to connections originating **from the WAN zone**. For details on priority rules related to WAN interfaces, refer to Backup Routes.

Item	Description
Source[1]	Specifies the IP address to which the rule applies. Use an IPv4 address in the *IPv4* form and an IPv6 address in the *IPv6* form.
Protocol	Specifies the protocol to which the rule applies: • **all**: The rule applies to all protocols. • **TCP**: The rule applies to the TCP protocol. • **UDP**: The rule applies to the UDP protocol. • **GRE**: The rule applies to the GRE protocol. • **ESP**: The rule applies to the ESP protocol. • **ICMP/ICMPv6**: The rule applies to ICMP (ICMPv6 for IPv6).
Target Port(s)	Specifies the port number or range. Enter a single port or a range separated by a hyphen (e.g., 1020–1040).
Action	Specifies the action the router performs: • **allow**: Permits the packets to enter the network. • **deny**: Blocks the packets from entering the network.
Description	A user-defined description for the rule, which is stored as a comment in iptables.

[1] This field supports IP address input in the formats: `IP`, `IP/mask`, or `IP_start-IP_end`.

The next section defines the **forwarding firewall policy**. If the *Enable filtering of forwarded packets* checkbox is unchecked, all incoming packets are forwarded. When enabled, and if a packet is addressed to another network interface, the router processes it through the FORWARD chain in iptables. If the FORWARD chain accepts the packet, the router forwards it, provided there is a corresponding entry in the routing table.

You can define up to thirty-two forwarding rules. A new row appears automatically after filling in the previous one. The forwarding settings can be applied to specific interfaces, providing granular control over traffic flow.

Info

As shown in the figure above, the first entry in the IPv6 forwarded packets configuration is the default firewall rule for NAT64, which is disabled by default. To enable the NAT64 function, navigate to *Configuration → NAT → IPv6 → Enable NAT64*.

Item	Description
Source Address(es)[1]	Specifies the source IP address to which the rule applies (IPv4 or IPv6).
Destination Address(es)[1]	Specifies the destination IP address to which the rule applies (IPv4 or IPv6).
Protocol	Specifies the protocol to which the rule applies: • **all**, **TCP**, **UDP**, **GRE**, **ESP**, **ICMP/ICMPv6**.
Target Port(s)	Specifies the target port number or range.
Input Interface	Specifies the interface on which the packet is received. Options include **any**, WAN zone, LAN zone, or specific interfaces such as Ethernet, Bridge, VLAN, Mobile, PPPoE, Wi-Fi, and VPN interfaces.
Output Interface	Specifies the interface through which the packet will be sent. The available options are the same as for *Input Interface*.
Action	Defines the action the router performs: • **allow**: Permits the packets to be forwarded. • **deny**: Blocks the packets from being forwarded.
Description	A user-defined description for the rule, which is stored as a comment in iptables.

[1] This field supports IP address input in the formats: `IP`, `IP/mask`, or `IP_start-IP_end`.

When the *Enable filtering of locally destined packets* function is enabled, the router automatically drops packets requesting an unsupported service without sending any notification.

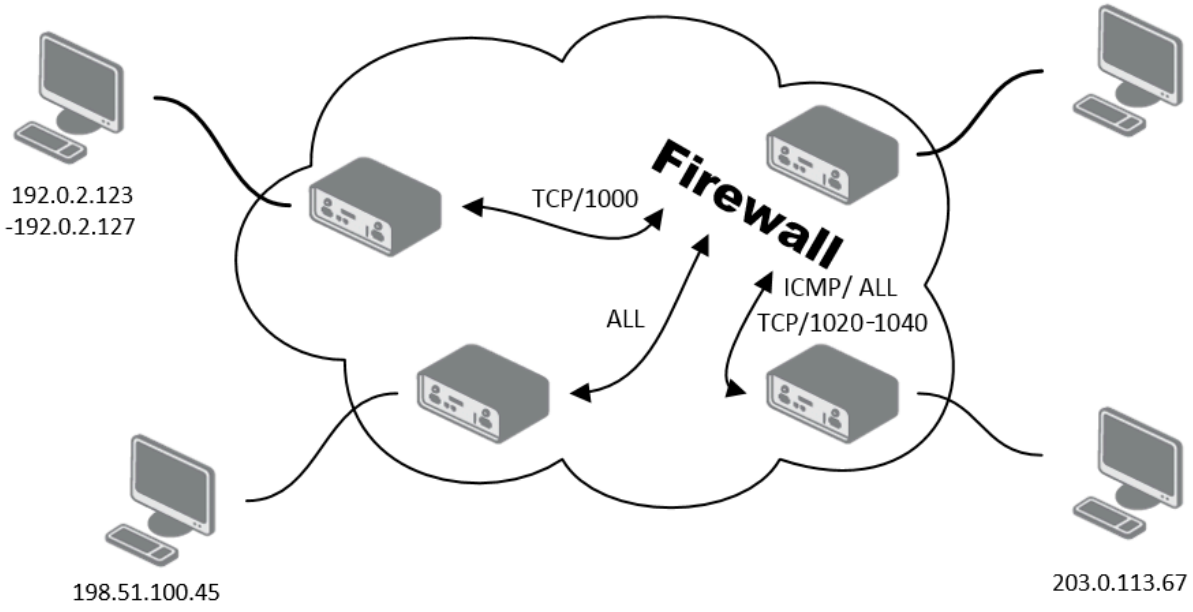
To protect against DoS (Denial of Service) attacks, the *Enable protection against DoS attacks* option limits the number of allowed connections per second to five. A DoS attack floods the target system with excessive requests, overwhelming its resources.

Firewall Configuration Example

In this example, the router is configured to permit the following access:

- Access from IP address 198.51.100.45 using any protocol.
- Access from the IP address range 192.0.2.123 to 192.0.3.127 using the TCP protocol on port 1000.
- Access from IP address 203.0.113.67 using the ICMP protocol.
- Access from IP address 203.0.113.67 using the TCP protocol on target ports ranging from 1020 to 1040.

See the network topology and configuration form in the figures below.



Topology for the IPv4 Firewall Configuration Example

IPv4 Firewall Configuration

Enable filtering of incoming packets

		Source *	Protocol	Target Port(s) *	Action	Description *
1	☑	198.51.100.45	all		allow	
2	☑	192.0.2.123-192.0.2.127	TCP	1000	allow	
3	☑	203.0.113.67	ICMP		allow	
4	☑	203.0.113.67	TCP	1020-1040	allow	
5	☐		all		allow	
6	☐		all		allow	

Maximum 32 items

Enable filtering of forwarded packets

		Source Address(es) *	Destination Address(es) *	Protocol	Target Port(s) *	Input Interface	Output Interface	Action	Description *
1	☐			all		any	any	allow	
2	☐			all		any	any	allow	

Maximum 32 items

Enable filtering of locally destinated packets

Enable protection against DoS attacks

* *can be blank*

Apply

IPv4 Firewall Configuration Example

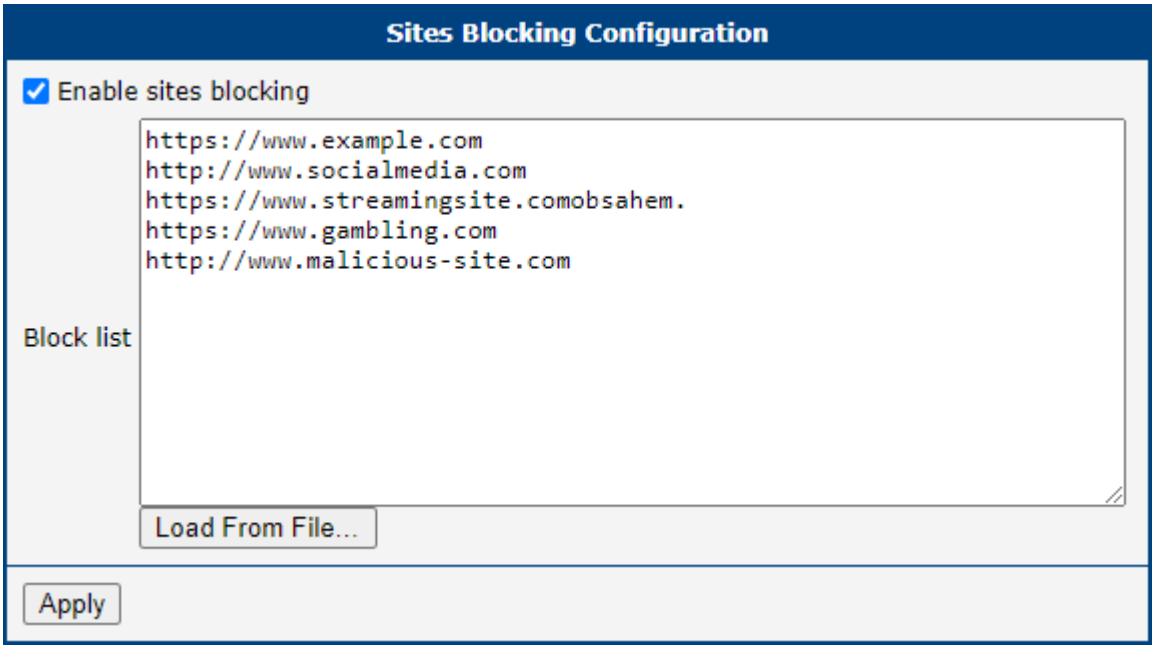
Sites

> **Info**
>
> This feature works only if the device is using the router as its DNS server.

On the *Sites* configuration page, you can define specific URLs that you want the firewall to block. To enable this feature, check the *Enable sites blocking* option.

You can then build your blocklist in two ways:

- Manually enter each URL into the *Block list* box, placing each one on a new line.
- Use the *Load From File...* button to import a predefined list of URLs from a plain text file.

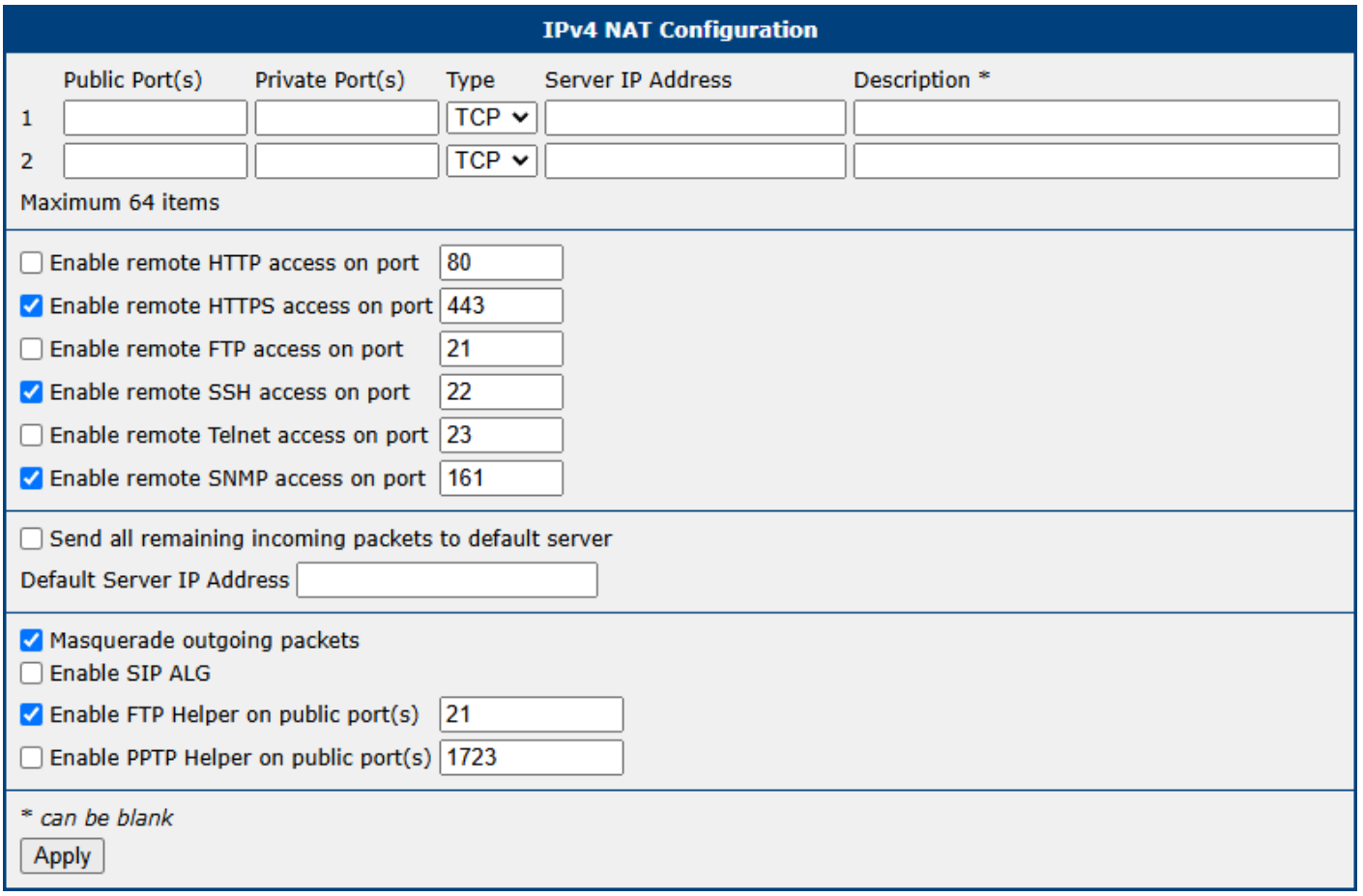


Firewall Sites Configuration Page

NAT

Network Address Translation (NAT) is a fundamental networking function that modifies IP address information in packet headers while they are in transit. The router implements NAPT (Network Address and Port Translation), also known as PAT (Port Address Translation) or IP masquerading, which allows multiple devices in a private network to share a single public IP address.

The NAT configuration is managed on the *Configuration → NAT* page, which has separate subpages for *IPv4* and *IPv6*.



NAT IPv4 Configuration Page

Port Forwarding

Port forwarding, also known as destination NAT (DNAT), allows external devices to connect to a specific service on a device within the private LAN. You can define up to sixty-four port forwarding rules.

Item	Description
Public Port(s)	The external port or port range on the router's WAN interface. A single port or a range (e.g., `8000-8010`) can be specified.
Private Port(s)	The internal port or port range on the destination server.
Type	The protocol for the rule: *TCP* or *UDP*.
Server IP Address	The private IPv4 or IPv6 address of the server on the LAN to which traffic will be forwarded.
Description	An optional description for the rule.

For configurations requiring more than sixty-four rules, additional rules can be added to the startup script (*Configuration → Scripts*). Use the following `iptables` command format for IPv4:

For IPv4 NAT:

```bash
iptables -t nat -A pre_nat -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination
```

```
[IPADDR]:[PORT_PRIVATE]
```

For IPv6, use the `ip6tables` command:

```bash
ip6tables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination [IP6ADDR]:[PORT_PRIVATE]
```

Replace the bracketed values with your specific port numbers and IP addresses.

Remote Access

This section allows you to enable remote access to the router's own management services from the WAN interface.

Item	Description
Enable remote HTTP access on port	Enables remote access to the router's web interface via HTTP on the specified port. If the HTTP service is disabled in *Services → HTTP* while HTTPS is enabled, incoming requests on this port will be redirected to HTTPS.
Enable remote HTTPS access on port	Allows secure remote access to the router's web interface via HTTPS on the specified port.
Enable remote FTP access on port	Allows remote access to the router's FTP server on the specified port.
Enable remote SSH access on port	Allows remote access to the router's command-line interface via SSH on the specified port.
Enable remote Telnet access on port	Allows remote access to the router's command-line interface via Telnet on the specified port.
Enable remote SNMP access on port	Allows remote management and monitoring of the router via SNMP on the specified port.

> **Warning**
>
> For secure management, always use HTTPS access. The HTTP remote access option is for redirection only. Exposing unsecured services to the Internet poses a significant security risk and should be avoided.

Default Server and NAT Helpers

This section contains advanced NAT features, including a default server (DMZ) setting and Application-Layer Gateways (ALGs) for specific protocols.

Item	Description
Send all remaining incoming packets to default server	When enabled, all incoming traffic from the WAN that does not match any other port forwarding rule is forwarded to the specified default server. This is often referred to as a DMZ.

Item	Description
Default Server Address	The private IPv4 or IPv6 address of the default server.
Enable NAT64	(IPv6 only) Activates NAT64 translation, allowing IPv6-only clients to communicate with IPv4-only services. Requires a corresponding firewall rule to be effective.
Masquerade outgoing packets	Enables source NAT (SNAT) for all outgoing traffic, making it appear to originate from the router's public WAN IP address. This should almost always be enabled.
Enable SIP ALG	(IPv4 only) Enables the Session Initiation Protocol Application-Layer Gateway, which helps VoIP traffic traverse NAT by modifying SIP packet headers.
Enable FTP Helper on public port(s)	Assists with NAT traversal for the FTP protocol, particularly for active mode FTP, on the specified port (default is 21).
Enable PPTP Helper on public port(s)	(IPv4 only) Assists with NAT traversal for the Point-to-Point Tunneling Protocol (PPTP) for VPN connections on the specified port (default is 1723).

Warning

The NAT64 functionality is based on the Jool ↗ implementation, which has certain limitations. It is not possible to connect to the router itself using its NAT64-mapped IPv4 address (e.g., `64:ff9b::192.0.2.1`). Furthermore, firewall rules for NAT64 traffic must be created in the input chain, not the forward chain, as Jool processes the packets as if they originate from the router itself.

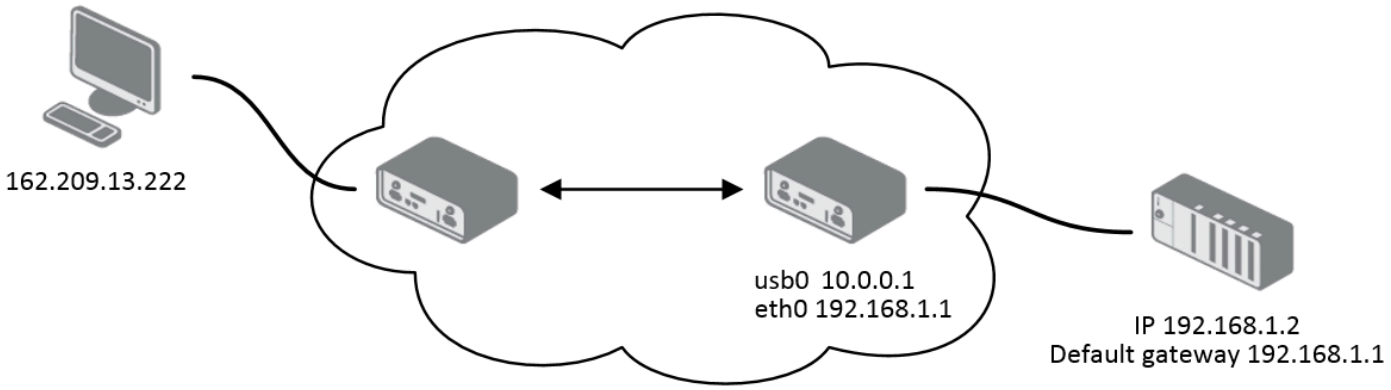
NAT Configuration Examples

Example 1: Forward All Traffic to a Single Device (DMZ)

This configuration forwards all incoming traffic from the Internet to a single device on the LAN, effectively placing it in a Demilitarized Zone (DMZ).

1. Enable the *Send all remaining incoming packets to default server* option.
2. Enter the IP address of the target device in the *Default Server IP Address* field.

The LAN device must be configured to use the router's IP address as its default gateway. With this setup, a ping request to the router's public SIM card IP address will be answered by the device, not the router.



Topology for NAT Configuration Example 1

IPv4 NAT Configuration

	Public Port(s)	Private Port(s)	Type	Server IP Address	Description *
1			TCP		
2			TCP		

Maximum 64 items

- [ ] Enable remote HTTP access on port 80
- [ ] Enable remote HTTPS access on port 443
- [ ] Enable remote FTP access on port 21
- [ ] Enable remote SSH access on port 22
- [ ] Enable remote Telnet access on port 23
- [x] Enable remote SNMP access on port 161

- [x] Send all remaining incoming packets to default server

Default Server IP Address 192.168.1.2

- [x] Masquerade outgoing packets
- [ ] Enable SIP ALG
- [x] Enable FTP Helper on public port(s) 21
- [ ] Enable PPTP Helper on public port(s) 1723

* *can be blank*

Apply

NAT Configuration for Example 1

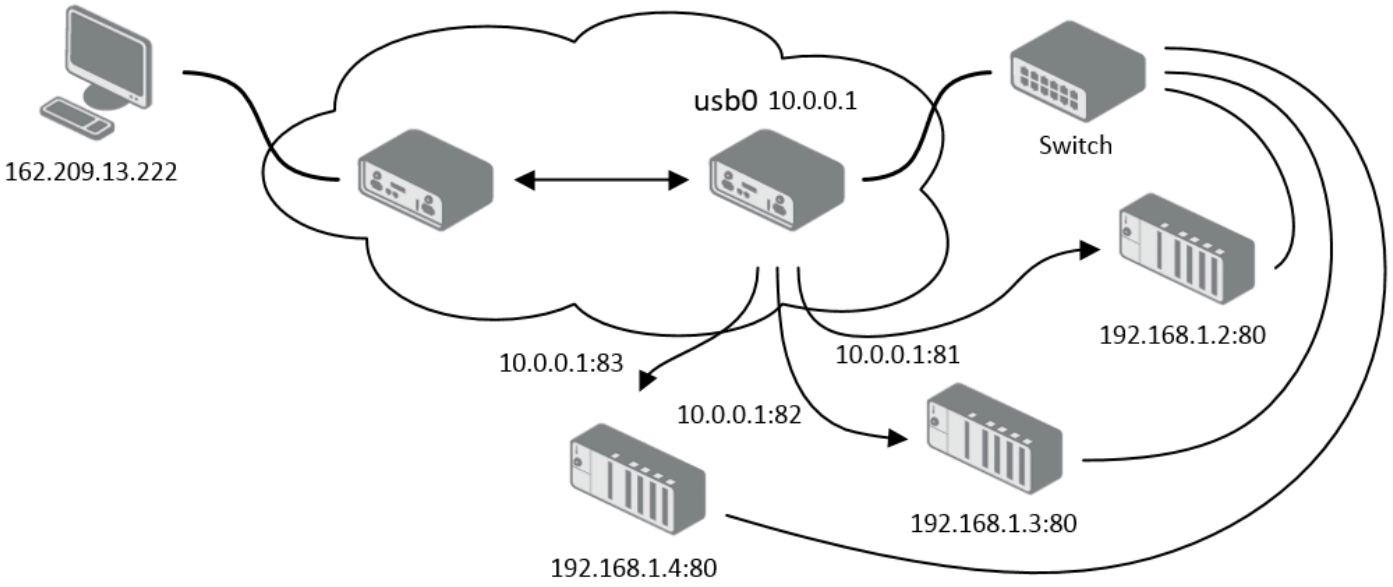
Example 2: Port Forwarding to Multiple Devices

This example shows how to make services on multiple internal devices accessible from the Internet using port forwarding. A different public port is mapped to a service on each internal server.

For instance, to make a web server on device `192.168.1.2` (port 80) accessible via public port 81, create the following rule:

- **Public Port(s)**: `81`
- **Private Port(s)**: `80`
- **Type**: *TCP*
- **Server IP Address**: `192.168.1.2`

External users can then access the web server by navigating to `http://<router_public_ip>:81`. Since the *Send all remaining incoming packets to default server* option is disabled, any traffic not matching a specific rule will be dropped.



Topology for NAT Configuration Example 2

IPv4 NAT Configuration

	Public Port(s)	Private Port(s)	Type	Server IP Address	Description *
1	81	80	TCP	192.168.1.2	
2	82	80	TCP	192.168.1.3	
3	83	80	TCP	192.168.1.4	
4			TCP		
5			TCP		

Maximum 64 items

- [ ] Enable remote HTTP access on port 80
- [ ] Enable remote HTTPS access on port 443
- [ ] Enable remote FTP access on port 21
- [ ] Enable remote SSH access on port 22
- [ ] Enable remote Telnet access on port 23
- [x] Enable remote SNMP access on port 161

- [ ] Send all remaining incoming packets to default server

Default Server IP Address

- [x] Masquerade outgoing packets
- [ ] Enable SIP ALG
- [x] Enable FTP Helper on public port(s) 21
- [ ] Enable PPTP Helper on public port(s) 1723

* *can be blank*

Apply

NAT Configuration for Example 2

OpenVPN

OpenVPN is a robust and highly flexible VPN solution that creates secure point-to-point or site-to-site connections over the Internet. The router supports up to four concurrent OpenVPN tunnels, each with its own configuration. Both IPv4 and IPv6 are supported in a dual-stack configuration.

To configure an OpenVPN tunnel, select *OpenVPN* from the *Configuration* section of the main menu. The menu will expand to show configuration pages for each tunnel (1st Tunnel through 4th Tunnel).

1st OpenVPN Tunnel Configuration

Create 1st OpenVPN tunnel	
Description *	
Interface Type	TUN
Protocol	UDP
UDP Port	1194
1st Remote IP Address *	
2nd Remote IP Address *	
Remote Subnet *	
Remote Subnet Mask *	
Redirect Gateway	no
Local Interface IP Address	
Remote Interface IP Address	
Remote IPv6 Subnet *	
Remote IPv6 Subnet Prefix Length *	
Local Interface IPv6 Address *	
Remote Interface IPv6 Address *	
Ping Interval *	sec
Ping Timeout *	sec
Renegotiate Interval *	sec
Max Fragment Size *	bytes
Compression	LZO
NAT Rules	not applied
Authenticate Mode	none
Security Mode	tls-auth
Pre-shared Secret	
CA Certificate	
DH Parameters	
Local Certificate	
Local Private Key	
Local Passphrase *	
Username	
Password	
Security Level	0 - Weak
User's Up Script	#!/bin/sh # # This script will be executed when OpenVPN tunnel is up.
User's Down Script	#!/bin/sh # # This script will be executed when OpenVPN tunnel is down.
Extra Options *	

* *can be blank*

Apply

OpenVPN Configuration Page

Tunnel Configuration

The following table describes the available parameters for configuring an OpenVPN tunnel.

Item	Description
Description	An optional name or description for the tunnel.
Interface Type	Determines the layer at which the VPN operates: • **TUN** (default): A routed VPN that operates at the network layer (Layer 3). This is the most common mode. • **TAP**: A bridged VPN that operates at the data link layer (Layer 2). This requires a bridge to be configured on the corresponding Ethernet interface.
Protocol	The transport protocol for the VPN tunnel: • **UDP/UDPv6**: Uses UDP for transport. This is generally faster and is the recommended default. • **TCP/TCPv6 Server**: Uses TCP and configures the router to act as a server, listening for incoming client connections. • **TCP/TCPv6 Client**: Uses TCP and configures the router to act as a client, initiating a connection to a remote server.
UDP/TCP Port	The port number for the selected protocol. The default is 1194.
1st/2nd Remote IP Address	The IPv4 address, IPv6 address, or domain name of the remote OpenVPN server. A second address can be provided for redundancy.
Remote Subnet	The IPv4 address of the remote network behind the tunnel.
Remote Subnet Mask	The subnet mask of the remote IPv4 network.
Redirect Gateway	If enabled, all of the router's outbound traffic will be sent through the VPN tunnel.
Local/Remote Interface IP Address	The virtual IPv4 addresses for the local and remote endpoints of the tunnel interface.
Remote IPv6 Subnet	The IPv6 prefix of the remote network behind the tunnel.
Remote IPv6 Prefix	The prefix length of the remote IPv6 network.
Local/Remote Interface IPv6 Address	The virtual IPv6 addresses for the local and remote endpoints of the tunnel interface.
Ping Interval	The interval in seconds at which keep-alive packets are sent to the remote peer.
Ping Timeout	The time in seconds to wait for a response before considering the tunnel to be down. This value should be greater than *Ping Interval*.
Renegotiate Interval	The time in seconds before the session key is renegotiated. This applies to certificate-based authentication modes.
Max Fragment Size	The maximum size in bytes of a packet before it is fragmented.

Item	Description
Compression	Configures data compression for the VPN tunnel: • **none** (recommended): No compression is used. This is the most secure setting. • **LZO** (deprecated): Uses the legacy LZO lossless compression algorithm. **This option is insecure due to the VORACLE vulnerability and is pending removal from future OpenVPN versions. Its use is strongly discouraged** — it is provided only for backward compatibility with legacy systems.
NAT Rules	Determines whether NAT should be applied to traffic passing through the tunnel.

Authentication and Security

OpenVPN offers multiple authentication methods, allowing for flexible and highly secure configurations.

Item	Description
Authenticate Mode	Selects the method used to authenticate the VPN peers: • **none**: No authentication. Not recommended for production use. • **pre-shared secret**: Uses a static, pre-shared key for authentication. • **username/password**: Authenticates using a username, password, and a common CA certificate. • **X.509 cert.**: Uses a full PKI with certificates for authentication. Can be configured in client, server, or multi-client server mode.
Security Mode	Configures an additional HMAC layer for verifying control channel packets: • **tls-auth**: Authenticates control channel packets. • **tls-crypt**: Encrypts and authenticates control channel packets, providing better protection against DoS attacks. This is the recommended mode.
Pre-shared Secret	The static key used for *Pre-shared secret* authentication mode or as the HMAC key for *Security Mode*.
CA Certificate	The certificate of the Certificate Authority that signed the client and server certificates.
DH Parameters	The Diffie-Hellman parameters file, required for server-side X.509 configurations.
Local Certificate	The public certificate for this router.
Local Private Key	The private key corresponding to the local certificate.
Local Passphrase	The passphrase used to protect the local private key file.
Username/Password	The credentials used for the *Username/password* authentication mode.
Security Level[1]	Sets the minimum cryptographic strength for the connection. Higher levels disable older, less secure algorithms. • **0 - Weak** (default): Allows all suites, including insecure legacy algorithms. Not recommended except for compatibility with outdated systems. • **1 - Low**: Provides a baseline of 80-bit security. • **2 - Medium**: Enforces a minimum of 112-bit security. • **3 - High**: Enforces a minimum of 128-bit security (e.g., requires AES-128 or stronger). • **4 - Very High**: Enforces a minimum of 192-bit security (e.g., requires AES-192 or stronger).

Item	Description
User's Up/Down Script[2]	Custom shell scripts executed when the tunnel is established or torn down.
Extra Options	A field for adding any additional OpenVPN command-line parameters.

[1] For a detailed explanation of security levels, see the Security Guidelines ↗ application guide, specifically the chapter on cryptographic algorithms.

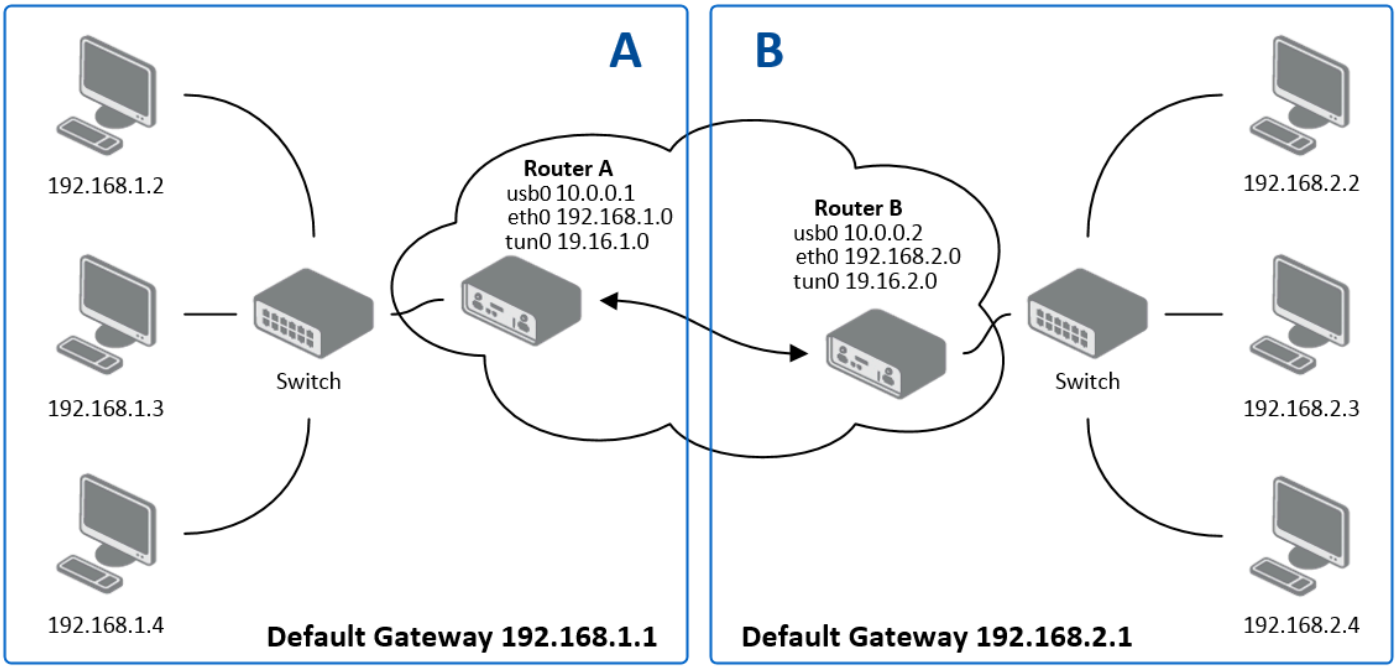
[2] The script is passed the following parameters: `cmd tun_dev tun_mtu link_mtu ifconfig_local_ip ifconfig_remote_ip [ init | restart ]`. See the official OpenVPN Reference Manual ↗ for details on the `--up` option.

Info

- An active WAN connection is required for an OpenVPN tunnel to be established, even if the tunnel's traffic is not intended to traverse that WAN.
- When using high security levels with TLS 1.3, it is recommended to use Elliptic Curve (EC) keys instead of RSA keys. Alternatively, you can limit the TLS version to 1.2 by adding `--tls-version-max 1.2` in the *Extra Options* field.

OpenVPN Configuration Example

This example shows a basic site-to-site OpenVPN tunnel between Router A and Router B.



OpenVPN Configuration Example

Configuration	Router A	Router B
Protocol	UDP	UDP

Configuration	Router A	Router B
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.16.1.0
Compression	none	none
Authentication Mode	none	none

Info

For more detailed examples, including certificate-based authentication, refer to the OpenVPN Tunnel ↗ application guide.

IPsec

The IPsec tunnel feature enables you to create secure connections between two separate LAN networks. You can configure up to four IPsec tunnels, with support for both IPv4 and IPv6 dual stack operation.

To configure an IPsec tunnel, select *IPsec* from the *Configuration* section of the main menu. The menu will expand to show configuration pages for each tunnel (1st Tunnel through 4th Tunnel).

The system supports both **policy-based** and **route-based** VPN approaches. You can transport IPv6 traffic through IPv4 tunnels and vice versa using the dual stack capability.

Warning

When configuring IPsec tunnels, keep these key points in mind:

- To encrypt data between local and remote subnets, specify the appropriate values in the subnet fields on both routers. To encrypt only the data stream between the routers, leave the local and remote subnet fields blank.
- If you specify protocol and port information in the *Local Protocol/Port* field, the router will encapsulate only packets matching those settings.
- For an optimal and secure setup, follow the instructions on the strongSwan Security Recommendations ↗ page.

Info

- Detailed information and more examples of IPsec tunnel configuration can be found in the IPsec Tunnel ↗ application guide.
- The FRR ↗ Router App is an Internet routing protocol suite for Advantech routers. It includes protocol daemons for BGP, IS-IS, LDP, OSPF, PIM, and RIP.

Policy-based vs. Route-based VPN

The router supports two VPN modes, selectable via the *Type* field on the IPsec configuration page. The key differences are summarized in the table below.

Feature	Policy-based	Route-based
Traffic selection	Subnet pairs defined in *Local Subnet* and *Remote Subnet* fields	Routing table entries
Virtual interface	None	`ipsecX` interface is created
Traffic inspection	Not possible on tunnel traffic	Possible using `tcpdump -i ipsecX`
Dynamic routing	Not supported	Supported (e.g., FRR/BGP, FRR/OSPF)
Multiple clients	Limited	Fully supported
Cisco FlexVPN	Not supported	Supported
Configuration complexity	Lower	Higher

In **policy-based** mode, the router encrypts traffic based on configured security policies defined by the subnet pairs in *Local Subnet* and *Remote Subnet*. No virtual interface is created — the kernel's policy engine handles encapsulation transparently. This is the simpler approach and is suitable for most standard site-to-site VPN deployments.

In **route-based** mode, a virtual `ipsecX` interface is created for each tunnel. Traffic is routed into the tunnel using standard routing rules, which enables dynamic routing protocols and more flexible topologies. The available route-based scenarios are described in the Configuration Scenarios section.

Tips

When using policy-based mode, if neither *Local Subnet* nor *Remote Subnet* is configured, only router-to-router traffic is encrypted — no LAN-to-LAN traffic will pass through the tunnel.

Configuration Scenarios

The following scenarios describe the most common VPN topologies supported by Advantech routers. The examples use route-based mode, but — with the exception of scenarios 2 and 3 — they are equally applicable to policy-based mode.

1. **Enabled Installing Routes**
    - Remote and local subnets are used as traffic selectors (routes).
    - This results in the same outcome as a policy-based VPN.
    - A benefit of this approach is the ability to inspect unencrypted traffic on the `ipsecX` interface using a tool like `tcpdump -i ipsecX`.
    - Set *Install Routes* to *yes*.
2. **Static Routes** (route-based only)
    - Routes are installed statically by an application as soon as the IPsec tunnel is established.
    - An application like FRR/STATICD can be used for this purpose.
    - Set *Install Routes* to *no*.
3. **Dynamic Routing** (route-based only)
    - Routes are installed dynamically by a routing protocol application, such as FRR/BGP or FRR/OSPF.
    - Set *Install Routes* to *no*.
4. **Multiple Clients**
    - This allows for a VPN network with multiple clients. One router acts as the server and assigns IP addresses to all clients.
    - The server has *Remote Virtual Network* and *Remote Virtual Mask* configured, while clients use the *Local Virtual Address* setting.
    - Set *Install Routes* to *yes*.

IPsec Authentication Scenarios

The system supports four primary authentication options:

1. **Pre-shared Key**
    - Set Authenticate Mode to *pre-shared key*
    - Enter the shared key in the Pre-shared Key field
2. **Public Key**
    - Set Authenticate Mode to *X.509 certificate*
    - Enter the public key in the Local Certificate/PubKey field
    - CA certificate not required
3. **Peer Certificate**
    - Set Authenticate Mode to *X.509 certificate*
    - Enter the remote key in the Remote Certificate/PubKey field
    - Allows users with this certificate
    - CA certificate not required
4. **CA Certificate**
    - Set Authenticate Mode to *X.509 certificate*
    - Enter the CA certificate or certificate list in the CA Certificate field

- Accepts any certificate signed by the CA
- Remote certificate not required

Note that Peer and CA Certificate authentication methods can be used simultaneously, allowing authentication through either method. The Local ID is significant - when using certificate authentication, the IKE identity must be contained in the certificate as either subject or `subjectAltName`.

Configuration Items Description

The configuration GUI for IPsec is shown in the figure below, and the description of all items is provided in the following table.

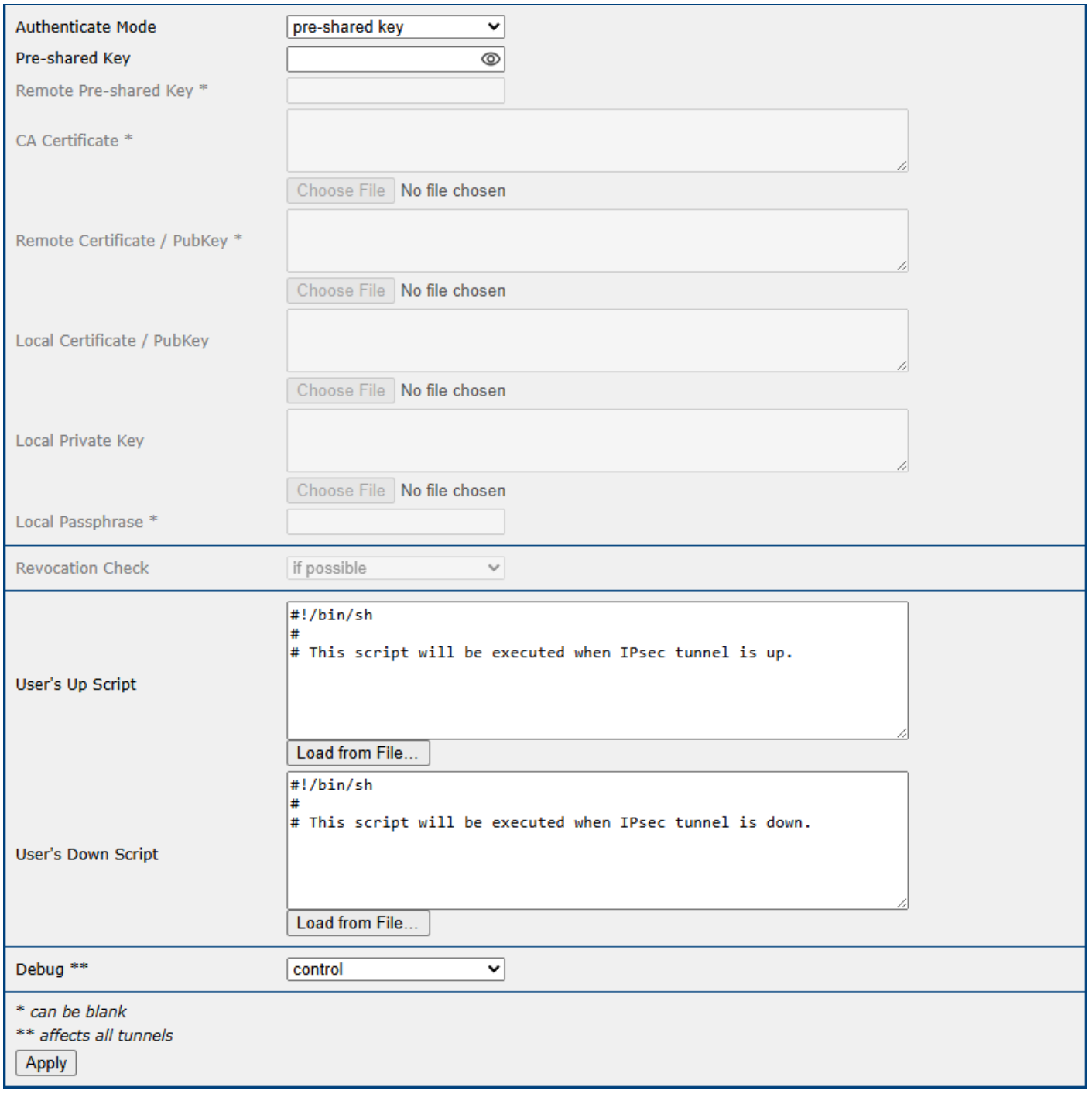
1st IPsec Tunnel Configuration

☐ Create 1st IPsec tunnel		
Description *		
Type	policy-based	
Host IP Mode	IPv4	
1st Remote IP Address *		
2nd Remote IP Address *		
Tunnel IP Mode	IPv4	
Local ID *		
Remote ID *		
Local Protocol/Port *		e.g. udp, tcp/22 or udp/65000-65009
Remote Protocol/Port *		e.g. udp, tcp/22 or udp/65000-65009
Install Routes	yes	
Separate Child SA for Each Subnet	☐	

	Local Subnet *	Local Subnet Mask	Remote Subnet *	Remote Subnet Mask
1				
2				

Maximum 10 items

MTU	1426	bytes	1280-1443 bytes
Remote Virtual Network *			
Remote Virtual Mask *			
Local Virtual Address *			
Cisco FlexVPN **	no		
Encapsulation Mode	tunnel		
Force NAT Traversal	no		
IKE Protocol	IKEv1/IKEv2		
IKE Mode	main		
IKE Algorithm	auto		
IKE Encryption	3DES		
IKE Hash	MD5		
IKE DH Group	2 (modp1024)		
IKE Reauthentication	yes		
XAUTH Enabled	no		
XAUTH Mode	client		
XAUTH Username			
XAUTH Password			
ESP Algorithm	auto		
ESP Encryption	DES		
ESP Hash	MD5		
PFS	disabled		
PFS DH Group	2 (modp1024)		
Key Lifetime	7200	sec	1-86400 sec
IKE Lifetime	28800	sec	1-86400 sec
Lifetime Margin	540	sec	1-86400 sec
Lifetime Fuzz	100	%	0-200%
DPD Delay *		sec	1-3600 sec
DPD Timeout *		sec	1-3600 sec



IPsec Configuration Page

Item	Description
Description	A user-defined name or description for the tunnel.
Type	• **policy-based**: Standard VPN approach based on security policies. • **route-based**: VPN approach based on routing rules. Data throughput may be slightly lower compared to policy-based VPN.
Host IP Mode	• **IPv4**: The router communicates with the remote peer using IPv4. • **IPv6**: The router communicates with the remote peer using IPv6.
1st Remote IP Address	The primary IPv4, IPv6 address, or domain name of the remote peer, corresponding to the selected *Host IP Mode*.

Item	Description
2nd Remote IP Address	The secondary (failover) IPv4 or IPv6 address, or domain name, of the remote peer. If configured, failover works as follows: at startup, the router initiates a connection to the *1st Remote IP Address*. If that connection fails, the router attempts to connect to the *2nd Remote IP Address*. Once the secondary connection is established, the router continues to use it until it fails — it does not automatically switch back to the primary address while the secondary connection is active.
Tunnel IP Mode	• **IPv4**: IPv4 traffic is transported inside the tunnel. • **IPv6**: IPv6 traffic is transported inside the tunnel.
Local ID	The identifier (ID) for the local side of the tunnel, typically composed of a hostname and a domain name (e.g., `router@mycompany.com`).
Remote ID	The identifier (ID) for the remote side of the tunnel.
Local Protocol/Port	Narrows the traffic selector by specifying the protocol and port for the local network. The format is *protocol/port* (e.g., `17/1701` for UDP port 1701).
Remote Protocol/Port	Narrows the traffic selector by specifying the protocol and port for the remote network.
Install Routes	For route-based mode only. If set to **yes**, the router automatically uses the traffic selectors to create and install routes.
Separate Child SA for Each Subnet	If enabled, a unique Child Security Association (SA) is created for each pair of local and remote subnets. This can improve interoperability with certain vendors and allow for more granular traffic policies. If disabled, a single Child SA covers all defined traffic selectors.
Local Subnet	The IPv4 or IPv6 address of the local network, based on the selected *Tunnel IP Mode*.
Local Subnet Mask	The IPv4 subnet mask or IPv6 prefix length (0–128) for the local network.
Remote Subnet	The IPv4 or IPv6 address of the network behind the remote peer.
Remote Subnet Mask	The IPv4 subnet mask or IPv6 prefix length for the remote network.
MTU	The Maximum Transmission Unit for the tunnel in route-based mode. The default value is 1426 bytes.
Remote Virtual Network	Specifies the virtual remote network for a server (responder).
Remote Virtual Mask	Specifies the virtual remote network mask for a server.
Local Virtual Address	Specifies the virtual local network address for a client. Use 0.0.0.0 to have an address assigned by the server.
Cisco FlexVPN	Enable to support Cisco FlexVPN functionality (route-based type only). For more information, see the strongswan.conf ↗ page.
Encapsulation Mode	Specifies the IPsec encapsulation method: • **tunnel**: The entire IP datagram is encapsulated. • **transport**: Only the IP header is encapsulated (not supported for route-based VPN).

Item	Description
Force NAT Traversal	Enforces NAT traversal by enabling UDP encapsulation of ESP packets.
IKE Protocol	Specifies the version of the Internet Key Exchange (IKE) protocol: **IKEv1/IKEv2** (auto-negotiate), or explicitly **IKEv1** or **IKEv2**. When set to IKEv1/IKEv2, the router first attempts to negotiate using IKEv2. If the peer does not support IKEv2, the router automatically falls back to IKEv1. IKEv2 is strongly recommended whenever possible, as it provides improved security and enhanced functionality.
IKE Mode	Specifies the mode for establishing a connection: *main* or *aggressive*. **It is strongly recommended not to use the *aggressive* mode due to lower security.**
IKE Algorithm	Specifies how algorithms are selected: • **auto**: Encryption and hash algorithms are selected automatically. • **manual**: Algorithms are defined by the user.
IKE Encryption	Available encryption algorithms: **3DES**, **AES128**, **AES192**, **AES256**, **AES128GCM128**, **AES192GCM128**, **AES256GCM128**.
IKE Hash	Available hash algorithms: **MD5**, **SHA1**, **SHA256**, **SHA384**, **SHA512**.
IKE DH Group	Selects the Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. The choice of group is a trade-off between security and performance, as stronger groups require more computation. For detailed guidance on selecting an appropriate group, refer to the official Algorithm Proposals (Cipher Suites) ↗ page.
IKE Reauthentication	Enable or disable IKE reauthentication (for IKEv2 only).
XAUTH Enabled	Enable eXtended Authentication (for IKEv1 only).
XAUTH Mode	Select the XAUTH mode: *client* or *server*.
XAUTH Username	The username for XAUTH.
XAUTH Password	The password for XAUTH.
ESP Algorithm	Specifies how algorithms are selected: • **auto**: Encryption and hash algorithms are selected automatically. • **manual**: Algorithms are defined by the user.
ESP Encryption	Available encryption algorithms: **DES**, **3DES**, **AES128**, **AES192**, **AES256**, **AES128GCM128**, **AES192GCM128**, **AES256GCM128**, **CAMELLIA192**, **CAMELLIA256**, **CHACHA20POLY1305**.
ESP Hash	Available hash algorithms: **MD5**, **SHA1**, **SHA256**, **SHA384**, **SHA512**.
PFS	Enables or disables Perfect Forward Secrecy, which ensures that session keys are not compromised if one of the long-term private keys is compromised.
PFS DH Group	Specifies the Diffie-Hellman group for PFS (see *IKE DH Group*).
Key Lifetime	Specifies the maximum interval after which a new set of encryption keys is automatically negotiated. The typical value is a few hours. The connection remains uninterrupted.
IKE Lifetime	Specifies the time period after which the router must re-authenticate the connection. The typical value ranges from a few hours to several days and must be greater than *Key Lifetime*. The entire connection is re-established, and a brief interruption may occur.

Item	Description
Lifetime Margin	Specifies how long before *Key Lifetime* or *IKE Lifetime* expires the router should initiate rekeying or reauthentication, to ensure the process completes within the lifetime interval. This value should be less than half of *Key Lifetime* and *IKE Lifetime*.
Lifetime Fuzz	Specifies a percentage used to calculate a random time offset added to *Lifetime Margin*. This introduces random variation in each rekeying and reauthentication cycle to prevent multiple devices from synchronizing their requests.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period the router waits for a DPD response before considering the peer to be down.
Authenticate Mode	Specifies the authentication method: • **Pre-shared key**: Use a shared secret for both sides. • **X.509 Certificate**: Use X.509 certificates for authentication.
(Local) Pre-shared Key	The shared secret for both sides of the tunnel (for IKEv2, this is the local key). This field appears only when pre-shared key mode is selected.
Remote Pre-shared Key	The shared secret for the remote side (for IKEv2). Appears only when pre-shared key mode is selected.
CA Certificate	The CA certificate or chain used for X.509 authentication to validate the remote peer's certificate.
Remote Certificate \ PubKey	The remote peer's X.509 certificate or public key for signature-based authentication.
Local Certificate \ PubKey	The local router's X.509 certificate or public key.
Local Private Key	The private key corresponding to the local certificate.
Local Passphrase	The passphrase used during private key generation.
Revocation Check	Certificate revocation policy: • **if possible**: Fails only if a certificate is known to be revoked. • **if URI defined**: Fails if a CRL/OCSP URI is available, but revocation checking fails. • **always**: Fails if no revocation information is available (the certificate is not known to be unrevoked).
User's Up Script[1]	A custom script executed when the IPsec tunnel is established.
User's Down Script[1]	A custom script executed when the IPsec tunnel is closed.
Debug	Controls the level of logging verbosity: **silent** (no logging), **audit** (logs only successful connections and disconnections), **control** (default level), **control-more**, **raw**, **private** (most verbose, including private keys). See the Logger Configuration ↗ page on the *strongSwan* website for details.

[1] Parameters passed to the script:

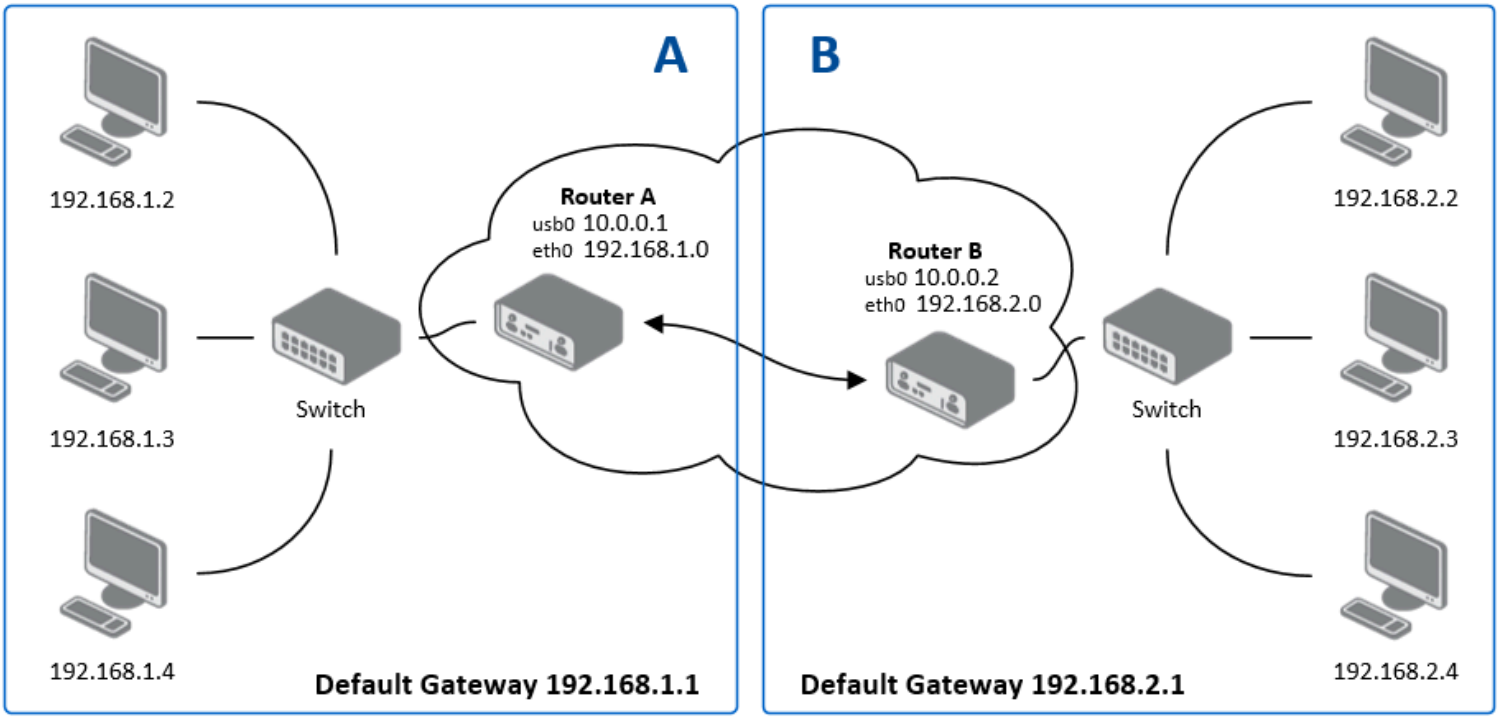
- for policy-based type: one parameter: *connection name*, returns e.g. `ipsec1-1`,
- for route-based type: two parameters: *connection name* and *interface name*, returns e.g. `ipsec1-1` and `ipsec0`.

We recommend retaining the default settings. Increasing key lifetimes reduces operational costs but also decreases security. Conversely, shorter lifetimes increase security but may affect performance. Changes are applied after clicking the *Apply* button.

Warning

- If local and remote subnets are not configured, only packets between local and remote IP addresses are encapsulated, so only router-to-router communication is encrypted.
- If protocol/port fields are configured, only packets matching those settings are encapsulated.

Basic IPv4 IPsec Tunnel Configuration Example



IPsec Configuration Example

Configuration of Router A and Router B is as follows:

Configuration	Router A	Router B
Host IP Mode	IPv4	IPv4
1st Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mask	255.255.255.0	255.255.255.0
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Configuration	Router A	Router B
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

WireGuard

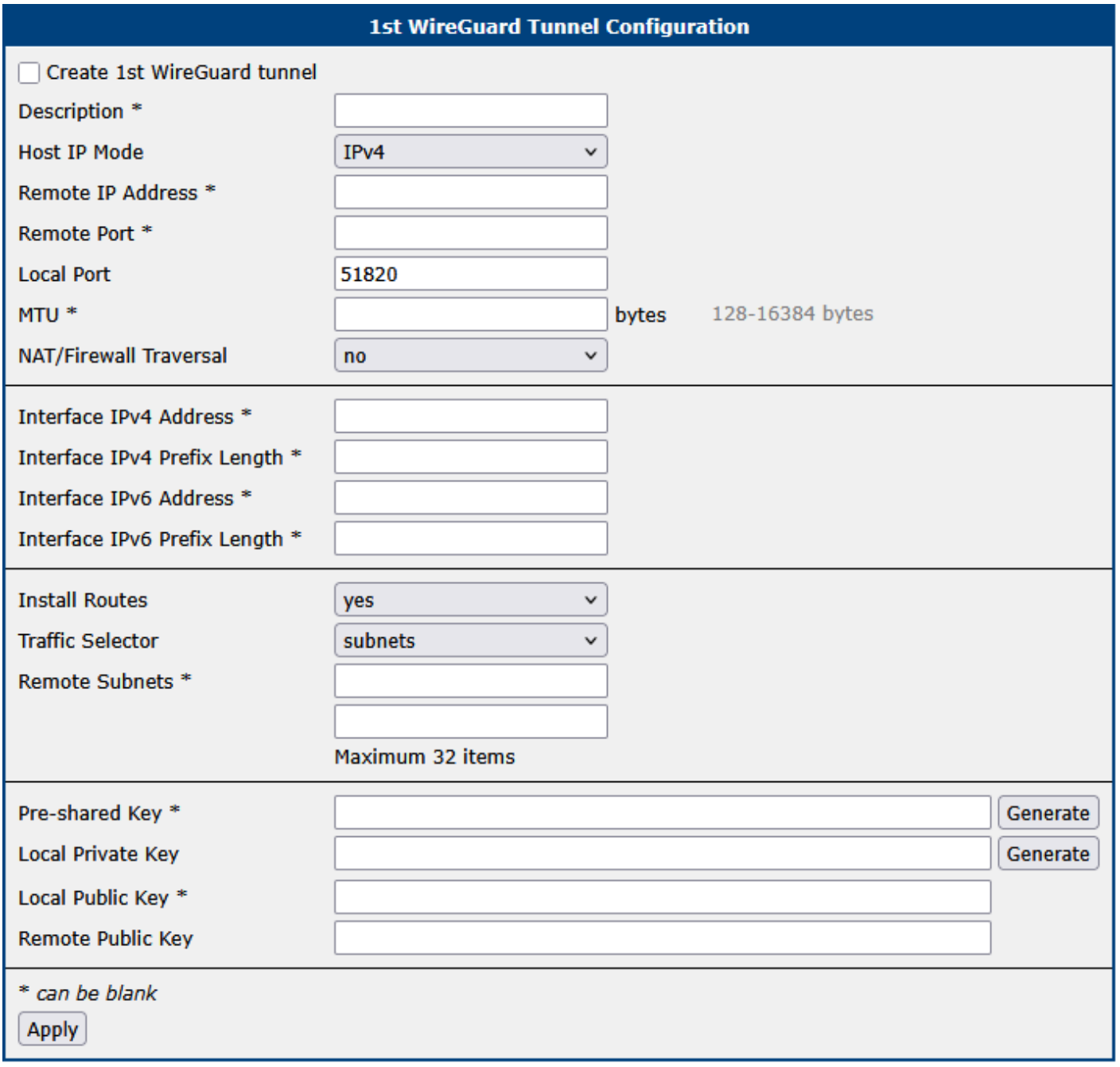
WireGuard is a modern, secure, and high-performance VPN (Virtual Private Network) protocol and opensource software that creates encrypted tunnels. It is designed for ease of use, speed, and a reduced attack surface compared to older protocols like IPsec and OpenVPN. WireGuard operates by encapsulating traffic within UDP (User Datagram Protocol) packets. Advantech routers support the creation of **up to four WireGuard tunnels simultaneously**.

To access the WireGuard tunnel configuration pages, click *WireGuard* in the *Configuration* section of the main menu. The menu item will expand, displaying separate configuration pages for *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel*, and *4th Tunnel*.

WireGuard on Advantech routers supports both IPv4 and IPv6 tunnels (**dual stack**), enabling the transport of IPv6 traffic over IPv4 tunnels and vice versa.

Info

- The FRRouting (FRR) ↗ router app is an Internet routing protocol suite for Advantech routers. This User Module includes protocol daemons for BGP, IS-IS, LDP, OSPF, PIM, and RIP. FRR can be used in conjunction with WireGuard for dynamic routing configurations.
- Detailed information and practical examples of WireGuard tunnel configuration and authentication can be found in the WireGuard Tunnel ↗ application guide.



WireGuard Configuration Interface

The following table describes all available WireGuard tunnel configuration options:

Parameter	Description
Create WireGuard tunnel	Enables and activates the respective tunnel.
Description	A user-defined name or description for the WireGuard tunnel interface.
Host IP Mode	• **IPv4**: The router uses IPv4 for communication with the remote peer. • **IPv6**: The router uses IPv6 for communication with the remote peer.
Remote IP Address	The IPv4 or IPv6 address, or the domain name, of the remote WireGuard peer. This address must correspond to the selected *Host IP Mode*.

Parameter	Description
Remote Port	The UDP port number on the remote WireGuard peer where it is listening for incoming connections.
Local Port	The UDP port number on which the local WireGuard interface listens for incoming connections (default port is 51820).
MTU	The Maximum Transmission Unit (MTU) for the WireGuard tunnel interface, specified in bytes. The default value is 1400 bytes. It's generally recommended to keep the default value unless specific network conditions require adjustment.
NAT/Firewall Traversal	When set to yes, the router sends keepalive packets (every 25 seconds) to maintain the tunnel connection active, especially when the local peer is behind a NAT (Network Address Translation) device or firewall. This ensures the NAT/firewall mapping remains valid, allowing incoming connections to reach the peer behind NAT.
Interface IPv4 Address	The IPv4 address assigned to the local WireGuard tunnel interface. This address is used for routing traffic within the tunnel.
Interface IPv4 Prefix Length	The IPv4 subnet prefix length associated with the local WireGuard tunnel interface address.
Interface IPv6 Address	The IPv6 address assigned to the local WireGuard tunnel interface. This address is used for routing traffic within the tunnel.
Interface IPv6 Prefix Length	The IPv6 subnet prefix length associated with the local WireGuard tunnel interface address.
Install Routes	• **no**: Disables automatic route installation. Use this option when a dynamic routing protocol (e.g., FRR/BGP) is used to manage routes. • **yes**: Enables automatic installation of routes based on the configured subnets.
Traffic Selector	• **all traffic**: All traffic is routed through the WireGuard tunnel (route 0.0.0.0/0 for IPv4 and ::/0 for IPv6). • **subnets**: Traffic is routed through the WireGuard tunnel based on the specific subnets defined below.
Remote Subnets	If *Traffic Selector* is set to *subnets*, specify the destination subnets (networks) to be routed through the WireGuard tunnel in CIDR notation (e.g., `192.168.1.0/24`). A maximum of 32 subnets can be defined.

Cryptographic Keys

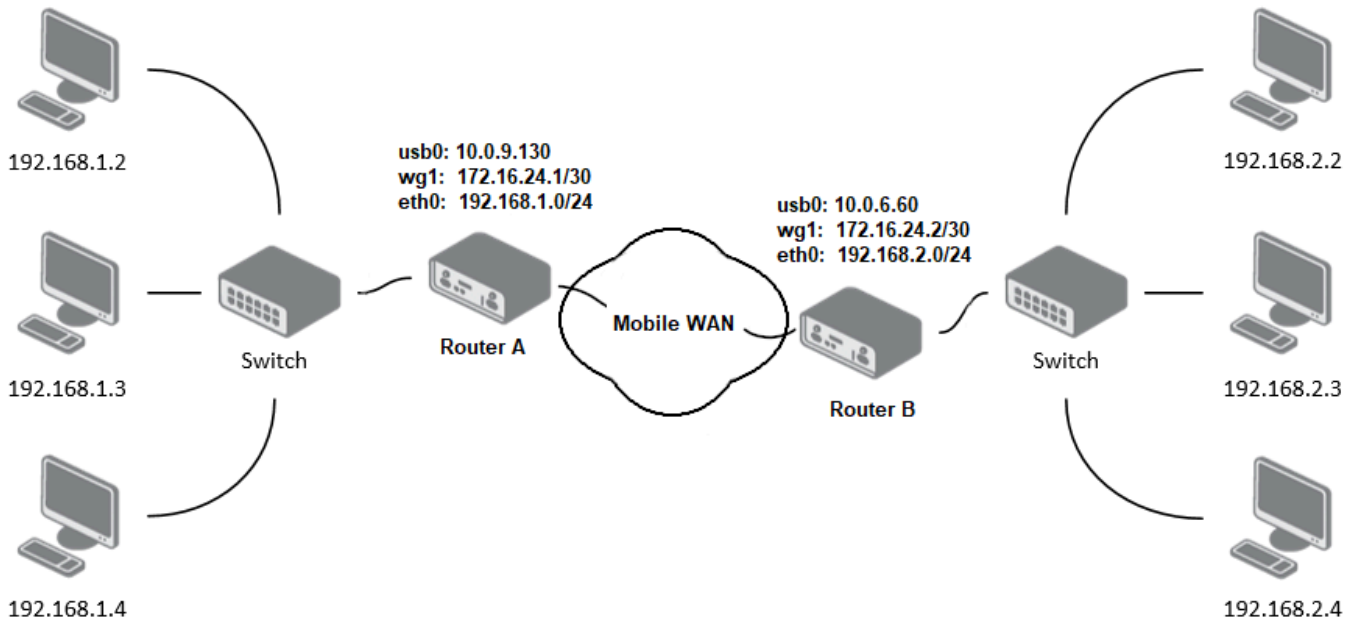
WireGuard's security is based on modern public-key cryptography.

Item	Description
Local Private Key	The secret private key for this router. Click *Generate* to create a new one. This key must never be shared.
Local Public Key	The public key derived from the local private key. Share this key with the remote peer so it can authenticate and encrypt traffic sent to this router.

Item	Description
Remote Public Key	The public key of the remote peer. Used to authenticate the remote peer and encrypt traffic sent to it.
Pre-shared Key	An optional key that adds an additional layer of symmetric-key encryption, providing post-quantum resistance. Click *Generate* to create a new key and share it with the remote peer.

WireGuard Example

The following example demonstrates a WireGuard IPv4 tunnel configuration between *Router A* and *Router B*.



WireGuard Example Topology

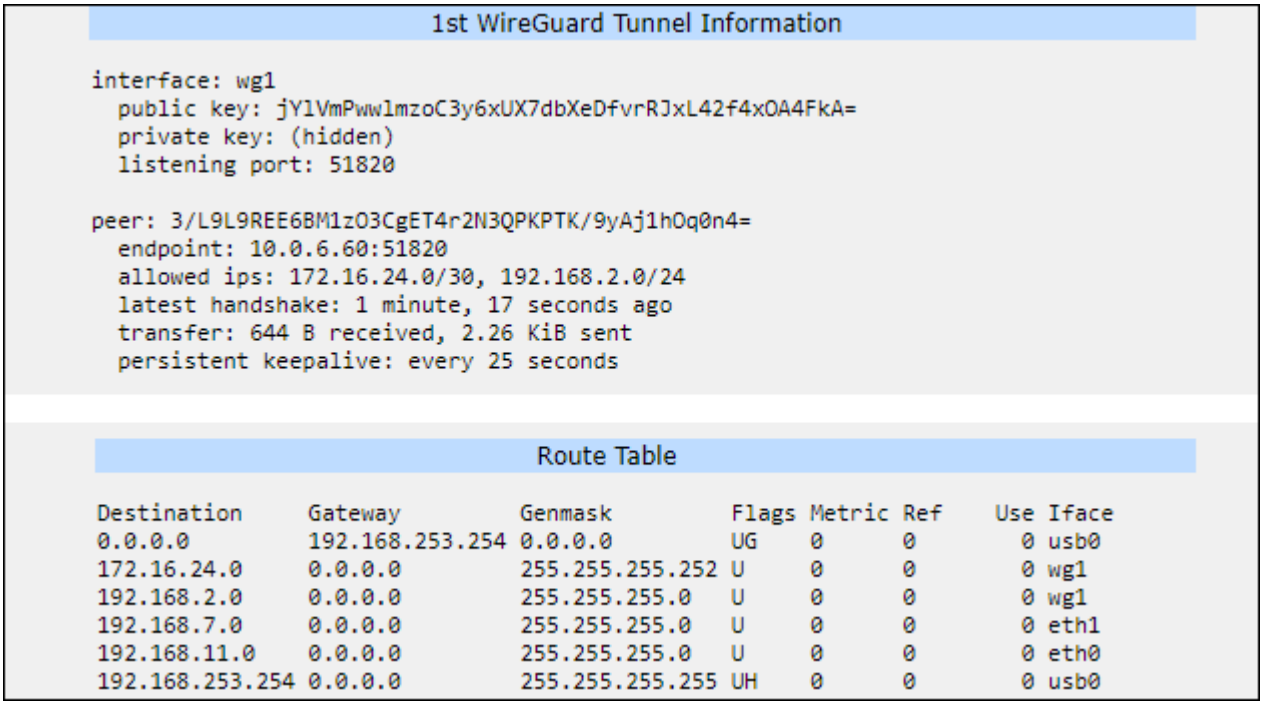
In this setup, *Router B* is configured as the listening side (server), and *Router A* initiates the tunnel connection (client). The configuration details for *Router A* and *Router B*, based on the topology shown above, are as follows:

Configuration	Router A	Router B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.6.60	— (Listens on all interfaces)
Remote Port	51820	— (Listens on local port)
Local Port	51820	51820
NAT/Firewall Traversal	yes	no
Interface IPv4 Address	172.16.24.1	172.16.24.2
Interface IPv4 Prefix Length	30	30
Install Routes	yes	yes

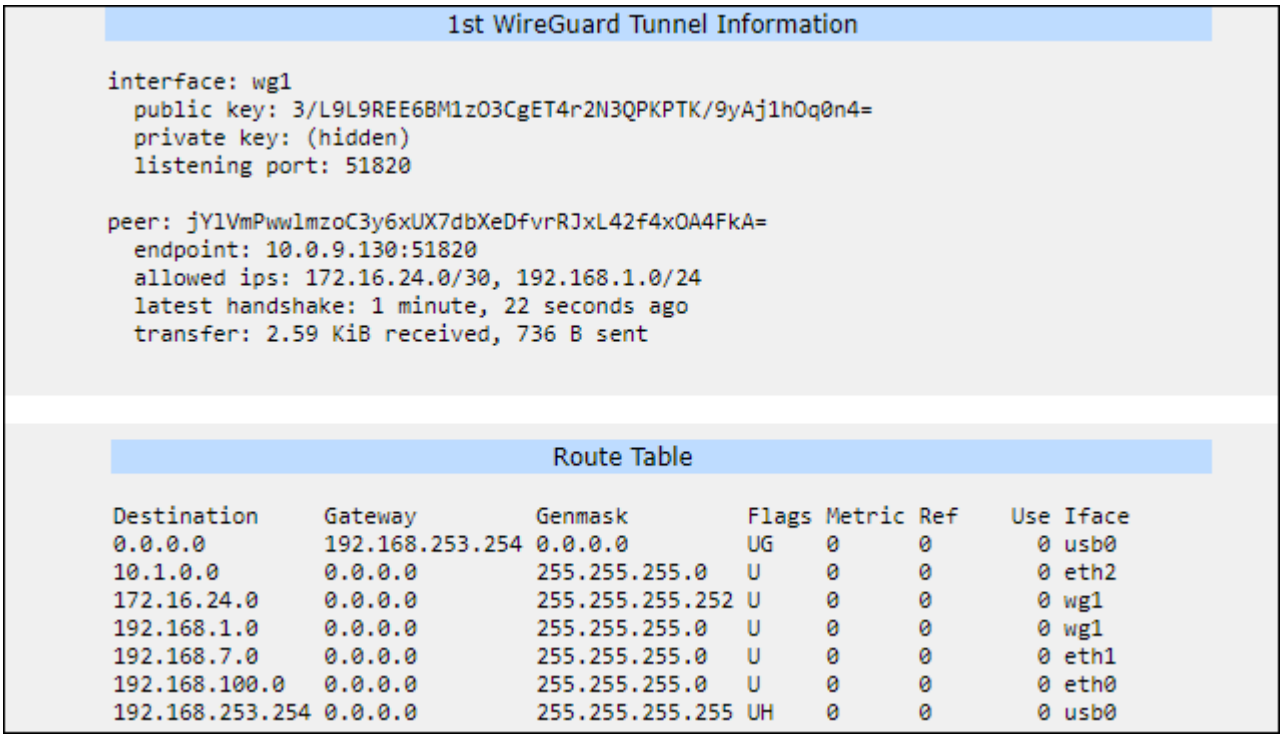
Configuration	Router A	Router B
Traffic Selector	subnets	subnets
Remote Subnets	192.168.2.0/24	192.168.1.0/24
Local Private Key	*generated key A*	*generated key B*
Local Public Key	*public key A*	*public key B*
Remote Public Key	*public Key B*	*public key A*

Verifying Connectivity

After applying the configuration, verify the tunnel status on the *Status → WireGuard* page. A successful connection is indicated by the presence of a *Latest handshake* time, which shows how long ago the last cryptographic key exchange occurred. This value will only appear after traffic has been initiated from the client side (Router A) or after the first keepalive packet has been sent.



Router A: WireGuard Status



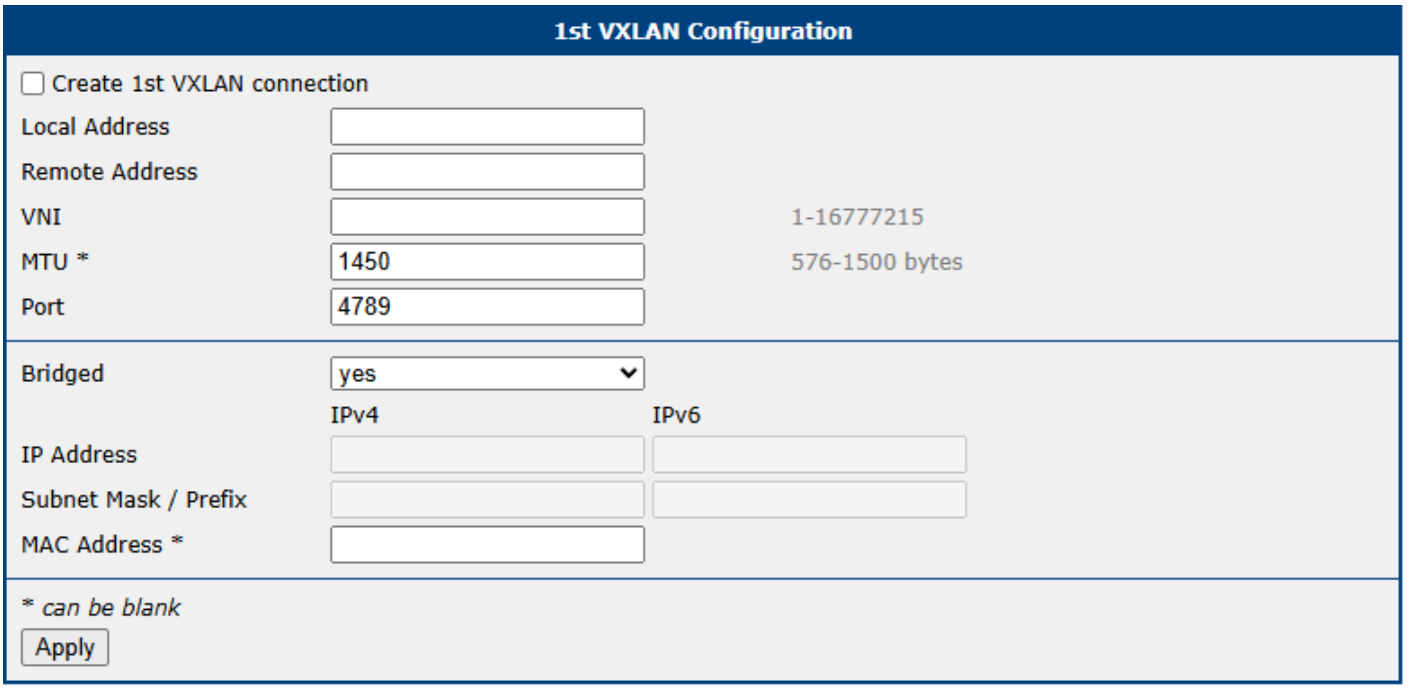
Router B: WireGuard Status

VXLAN

Info

VXLAN does not provide any native encryption or authentication. When deploying VXLAN over public or untrusted networks, it is strongly recommended to route the VXLAN traffic through a secure VPN tunnel, such as *IPsec* or *WireGuard*, to ensure data confidentiality and integrity.

Virtual Extensible LAN (VXLAN) is a Layer 2 overlay scheme on a Layer 3 network. It uses a VLAN-like encapsulation to wrap Layer 2 Ethernet frames within Layer 3 UDP packets. This allows for the creation of virtualized Layer 2 subnets that can span across physical Layer 3 network boundaries. Advantech routers support up to four simultaneous VXLAN tunnels. The configuration pages for VXLAN are located under *Configuration → VXLAN*.



VXLAN configuration page

The table below describes the parameters available for configuring each of the VXLAN interfaces.

Item	Description
Create VXLAN connection	Activates the selected VXLAN tunnel (1st to 4th).
Local Address	The local IP address of the router used as the source for the VXLAN tunnel.
Remote Address	The IP address of the remote tunnel peer (VTEP). For secure deployments, this should be the internal IP of an established VPN tunnel.
VNI	VXLAN Network Identifier (1 to 16777215). This ID must be identical on both VTEP peers.
MTU	Maximum Transmission Unit (576 to 1500 bytes). The recommended value is `1450` to account for the 50-byte VXLAN overhead and prevent fragmentation. This field can be left blank.
Port	The destination UDP port used for the outer header. The standard port is `4789`.
Bridged	Select *yes* to add the VXLAN interface to the router's local bridge, enabling seamless Layer 2 connectivity. If set to *no*, the VXLAN interface is considered "Routed" and has its own IP address.
IP Address	The IPv4 or IPv6 address assigned to the VXLAN interface. Configured when *Bridged* is set to *no* (Routed mode).
Subnet Mask / Prefix	The corresponding IPv4 subnet mask or IPv6 prefix length for the assigned IP address.
MAC Address	A custom MAC address for the VXLAN interface. If specified, the address must be unicast and locally administered. This field is optional and can be left blank.

VXLAN configuration parameters

Deployment Example

In this scenario, two routers bridge their local networks over an existing *WireGuard* tunnel to ensure security. The *Bridged* option is enabled to allow Layer 2 traffic (such as broadcast or non-IP protocols) to pass transparently through the secure tunnel.

Setting	Router A (Site 1)	Router B (Site 2)
Local Address	10.0.0.1 (VPN IP)	10.0.0.2 (VPN IP)
Remote Address	10.0.0.2 (VPN IP)	10.0.0.1 (VPN IP)
VNI	100	100
Port	4789	4789
Bridged	yes	yes

Example of secure VXLAN bridge over VPN

Security Recommendations

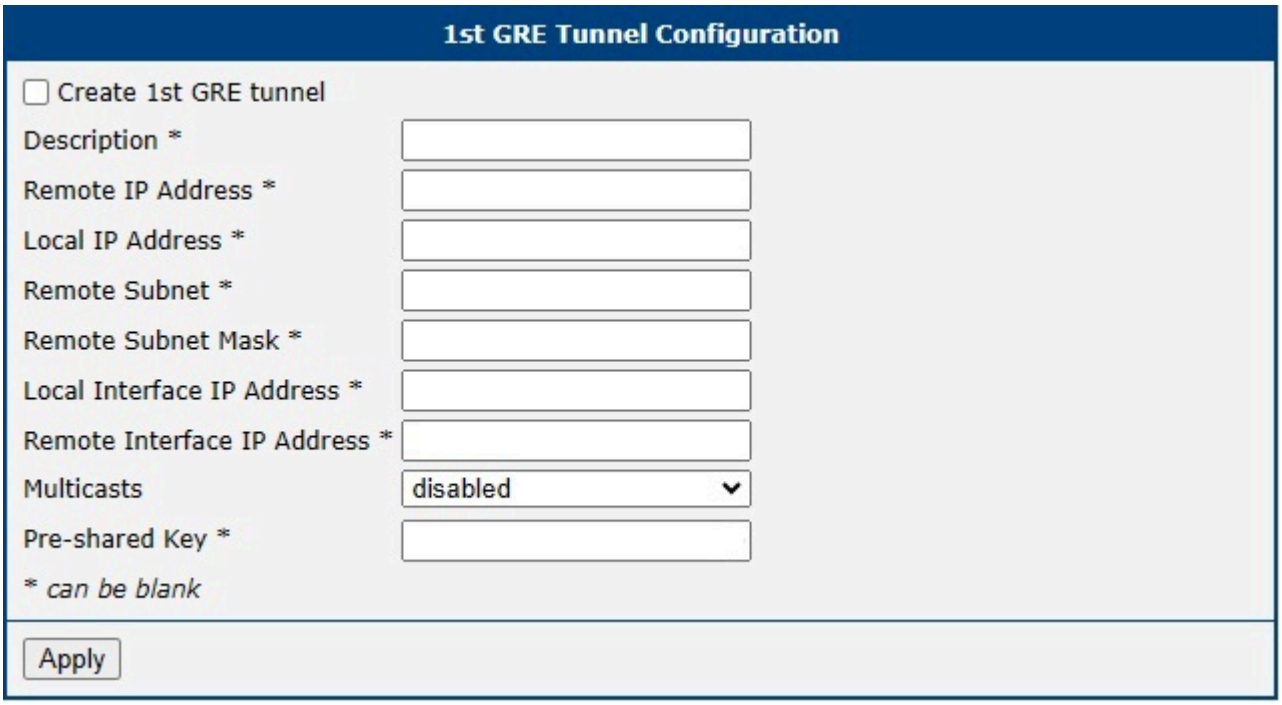
To protect your network when using VXLAN, follow these best practices:

- **Use VPN Transport**: Never expose unencrypted VXLAN traffic directly to the internet. Always encapsulate it within *IPsec* or *WireGuard*.
- **Firewall Whitelisting**: Configure the firewall under *Configuration → Firewall* to allow incoming traffic on UDP port `4789` only from the trusted peer IP address.
- **MTU Adjustment**: Ensure the MTU is correctly set (e.g., `1450`) to avoid packet fragmentation issues caused by the combination of VPN and VXLAN headers.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an IP network. The router supports creating up to four GRE tunnels.

The configuration pages are located under *Configuration → GRE*, with separate tabs for each tunnel.



GRE Tunnel Configuration Page

Warning

- GRE is an unencrypted protocol and does not support IPv6 transport. For secure communication, use it in combination with IPsec.
- GRE tunnels cannot pass through a NAT device without a corresponding NAT traversal solution, such as a port forwarding rule for protocol 47 (GRE).

Tunnel Configuration

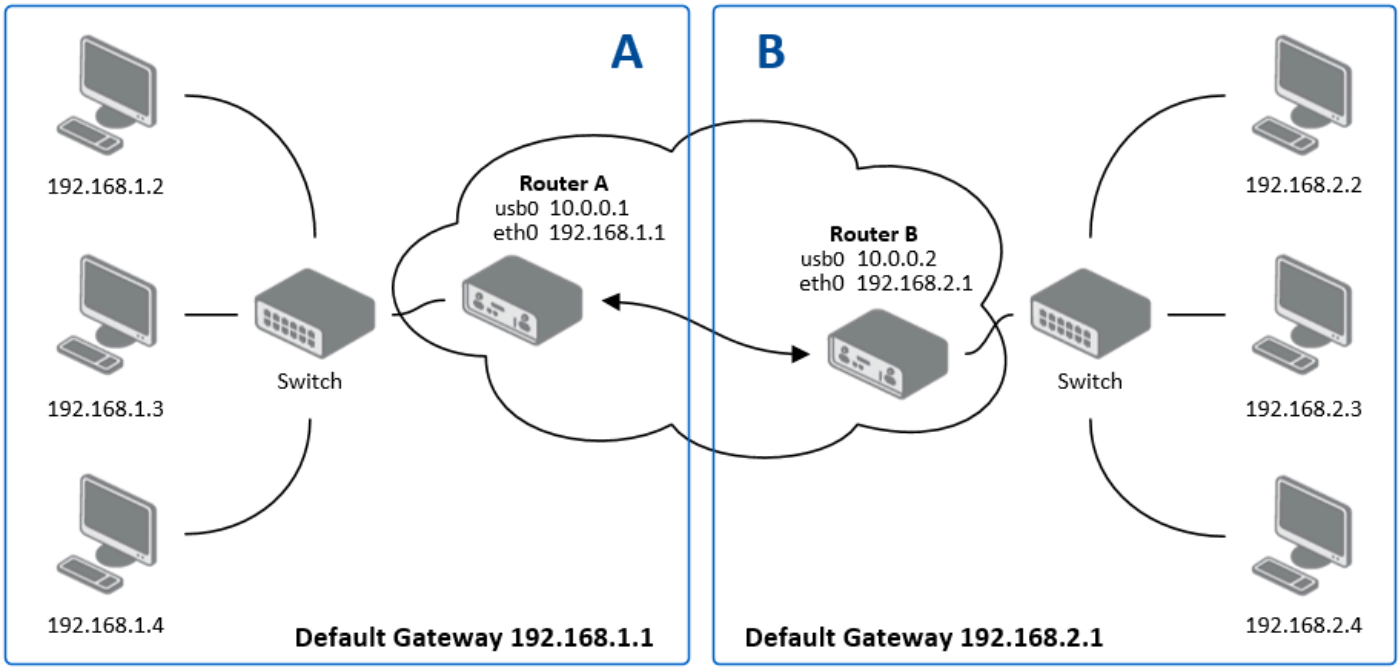
The following table describes the parameters for configuring a GRE tunnel.

Item	Description
Description	An optional name or description for the tunnel.
Remote IP Address	The public IP address of the remote tunnel endpoint.
Local IP Address	The public IP address of the local tunnel endpoint.
Remote Subnet	The IP address of the destination network behind the remote endpoint.
Remote Subnet Mask	The subnet mask of the remote network.
Local Interface IP Address	The virtual IP address of the local end of the GRE tunnel interface.
Remote Interface IP Address	The virtual IP address of the remote end of the GRE tunnel interface.

Item	Description
Multicasts	Controls multicast traffic through the tunnel: • **disabled**: Blocks multicast traffic. • **enabled**: Allows multicast traffic.
Pre-shared Key	An optional 32-bit numerical key for basic packet validation. Both routers must use the same key, or packets will be dropped. This is not a cryptographic key and provides no security.

Configuration Example

This example shows a basic site-to-site GRE tunnel between Router A and Router B, connecting their respective LANs.



GRE Tunnel Example Topology

Configuration	Router A	Router B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

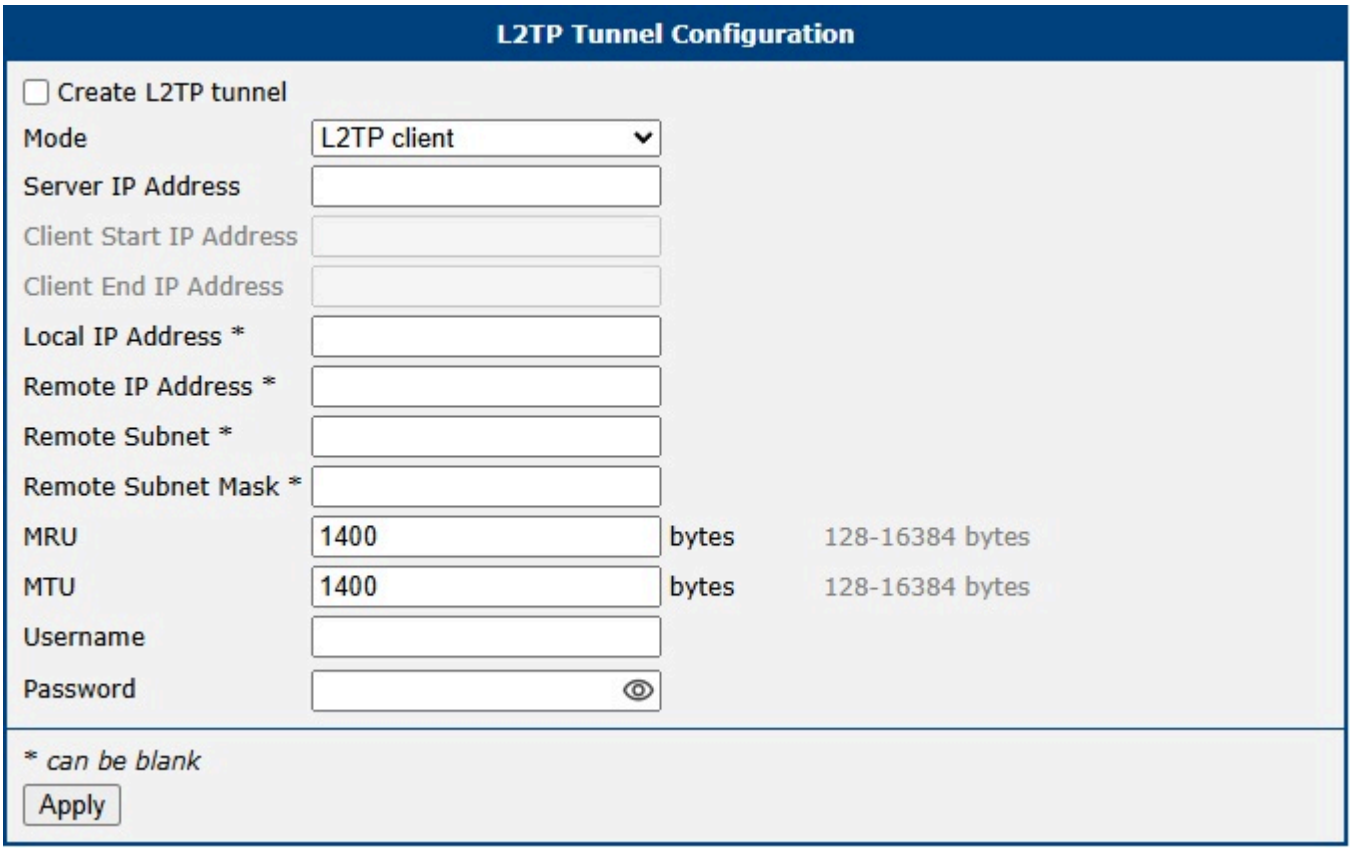
Info

For more detailed examples, refer to the GRE Tunnel ↗ application guide.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The L2TP configuration page is located under *Configuration → L2TP*.



L2TP Tunnel Configuration Page

Warning

L2TP is an unencrypted protocol and does not support IPv6 transport. For secure communication, it must be combined with a security protocol like IPsec.

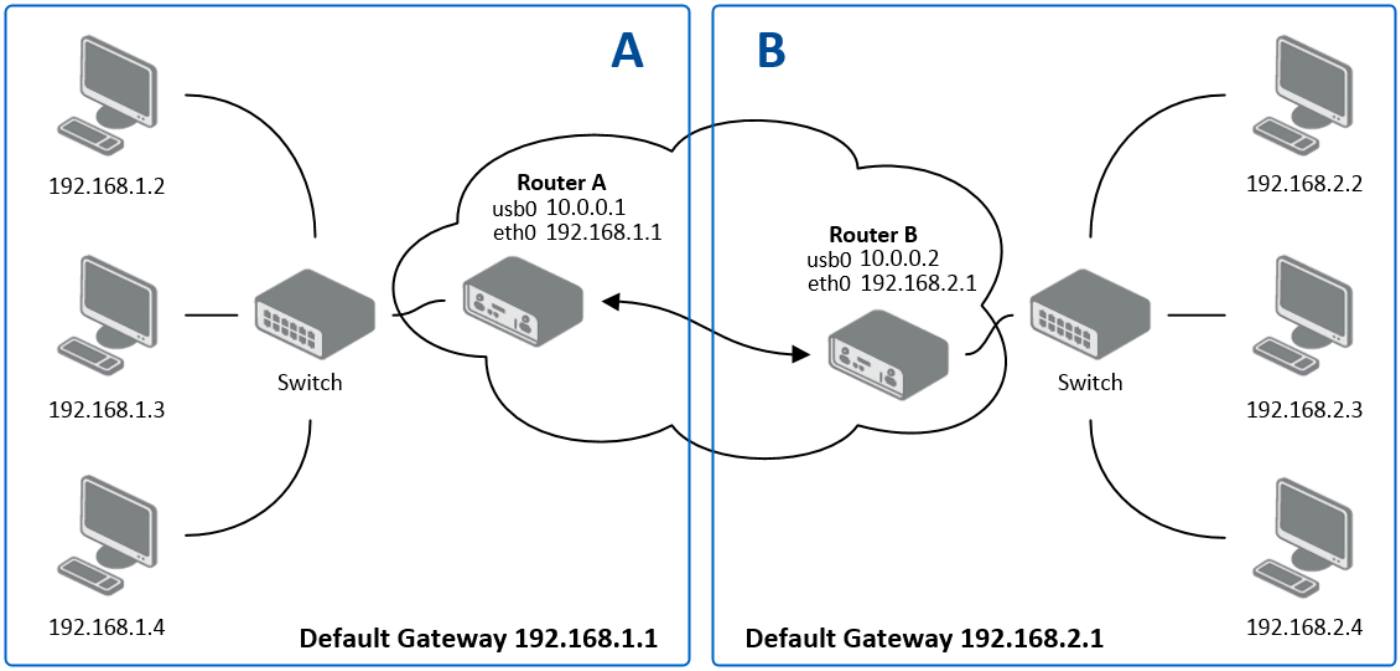
Tunnel Configuration

To set up an L2TP tunnel, check the *Create L2TP tunnel* box and configure the following parameters.

Item	Description
Mode	Determines the router's role in the L2TP connection: • **L2TP server**: The router acts as the L2TP Network Server (LNS), accepting connections from clients. • **L2TP client**: The router acts as the L2TP Access Concentrator (LAC), initiating a connection to a remote server.
Server IP Address	(Client mode only) The IP address of the remote L2TP server.
Client Start/End IP Address	(Server mode only) The starting and ending addresses of the IP pool from which the server assigns addresses to connecting clients.
Local IP Address	The virtual IP address of the local end of the L2TP tunnel.
Remote IP Address	The virtual IP address of the remote end of the L2TP tunnel.
Remote Subnet/Mask	The IP address and subnet mask of the network behind the remote peer, used for creating a static route.
MRU/MTU	The Maximum Receive Unit and Maximum Transmission Unit in bytes. The default value is 1400.
Username/Password	The credentials used for authenticating the L2TP session. Valid characters only — refer to Allowed and Restricted Input Characters.

Configuration Example

This example shows a typical client-server setup, where Router A (Server) provides access to its LAN for Router B (Client).

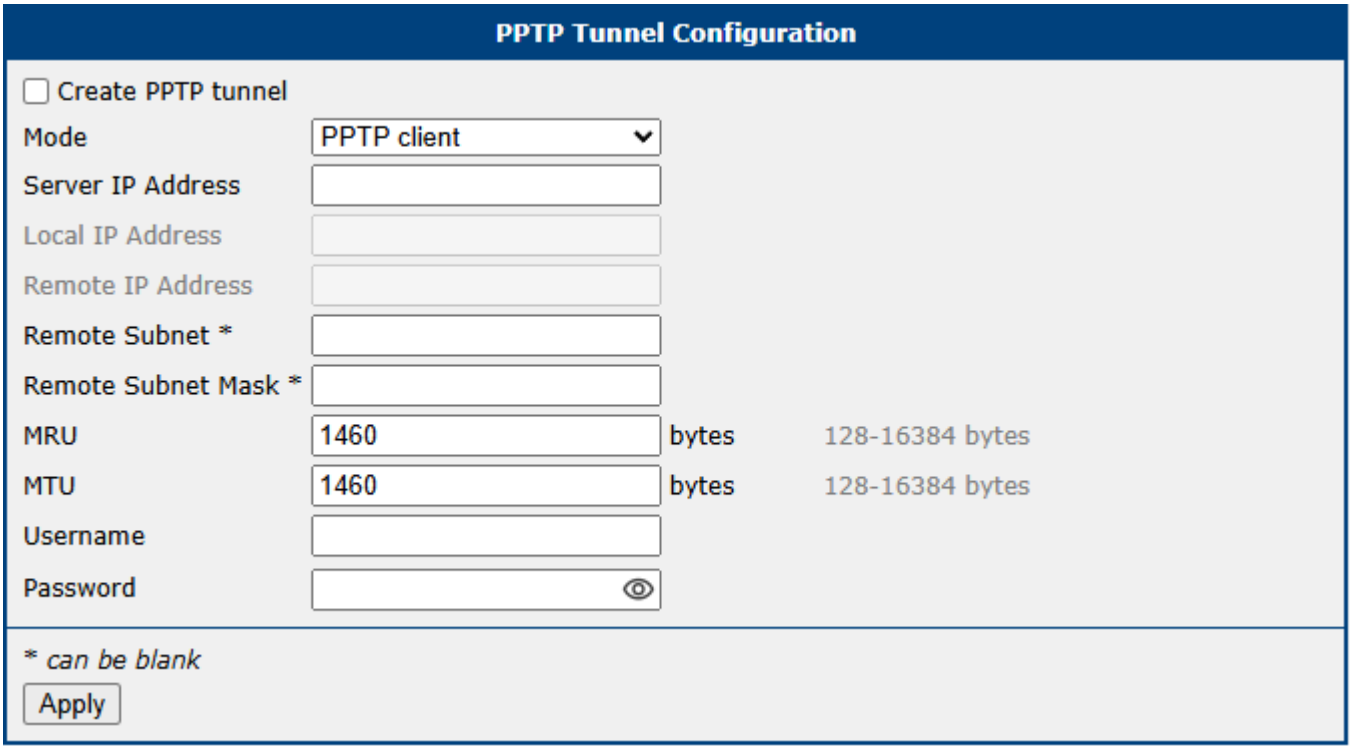


L2TP Tunnel Example Topology

Configuration	Router A (Server)	Router B (Client)
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.2.5	—
Client End IP Address	192.168.2.254	—
Local IP Address	192.168.1.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol used to create simple, password-protected connections between two LANs. To configure a tunnel, navigate to *Configuration → PPTP*.



PPTP Tunnel Configuration Page

Warning

PPTP is an outdated and insecure protocol with known vulnerabilities. It does not support IPv6. It is strongly recommended to use a modern, secure VPN protocol such as WireGuard or OpenVPN instead.

Tunnel Configuration

To set up a PPTP tunnel, check the *Create PPTP tunnel* box and configure the following parameters.

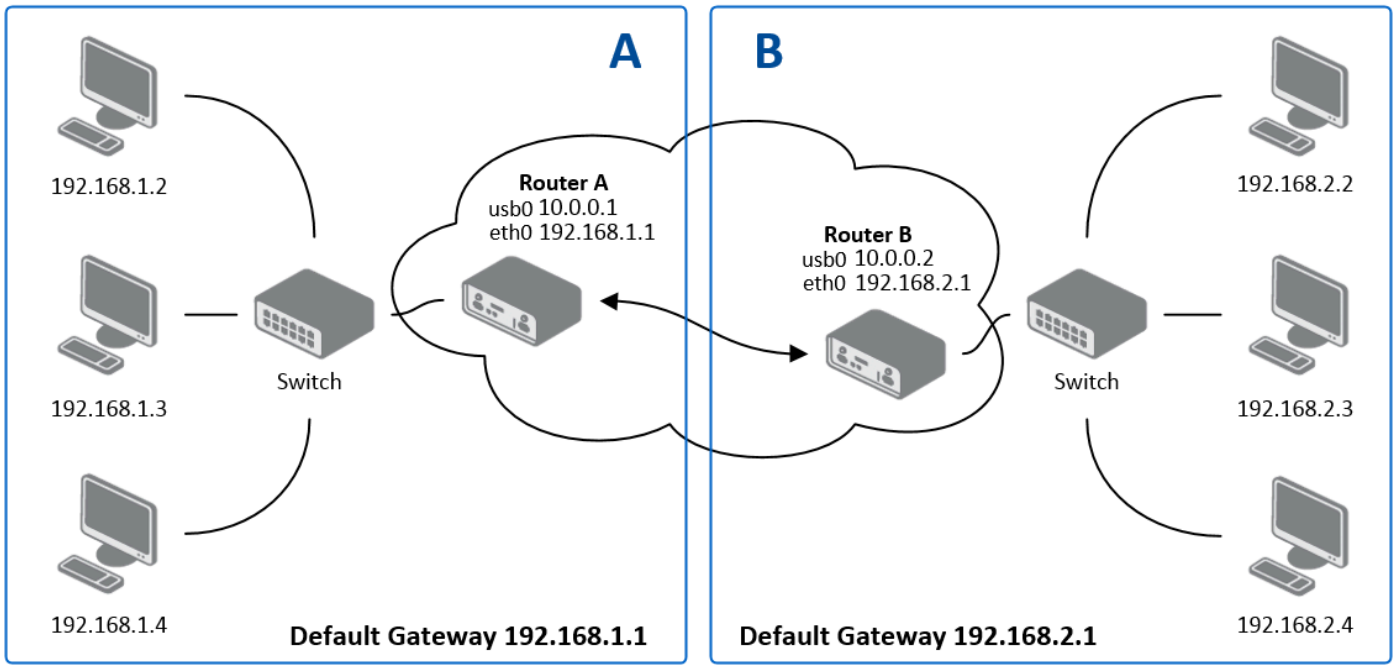
Item	Description
Mode	Determines the router's role in the PPTP connection: • **PPTP server**: The router acts as the server, accepting connections from remote clients. • **PPTP client**: The router acts as the client, initiating a connection to a remote server.
Server IP Address	(Client mode only) The IP address of the remote PPTP server.
Local IP Address	The virtual IP address for the local end of the tunnel.
Remote IP Address	The virtual IP address for the remote end of the tunnel.
Remote Subnet/Mask	The IP address and subnet mask of the network behind the remote peer.
MRU/MTU	The Maximum Receive Unit and Maximum Transmission Unit in bytes. The default value is 1460 to avoid packet fragmentation.
Username/Password	The credentials for authenticating the PPTP session. Valid characters only — refer to Allowed and Restricted Input Characters.

Info

The router firmware also supports PPTP passthrough, which allows PPTP client devices on the LAN to establish tunnels through the router to an external server.

Configuration Example

This example shows a standard client-server setup where Router A (Server) accepts a connection from Router B (Client).



PPTP Tunnel Example Topology

Configuration	Router A (Server)	Router B (Client)
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	192.168.2.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Services

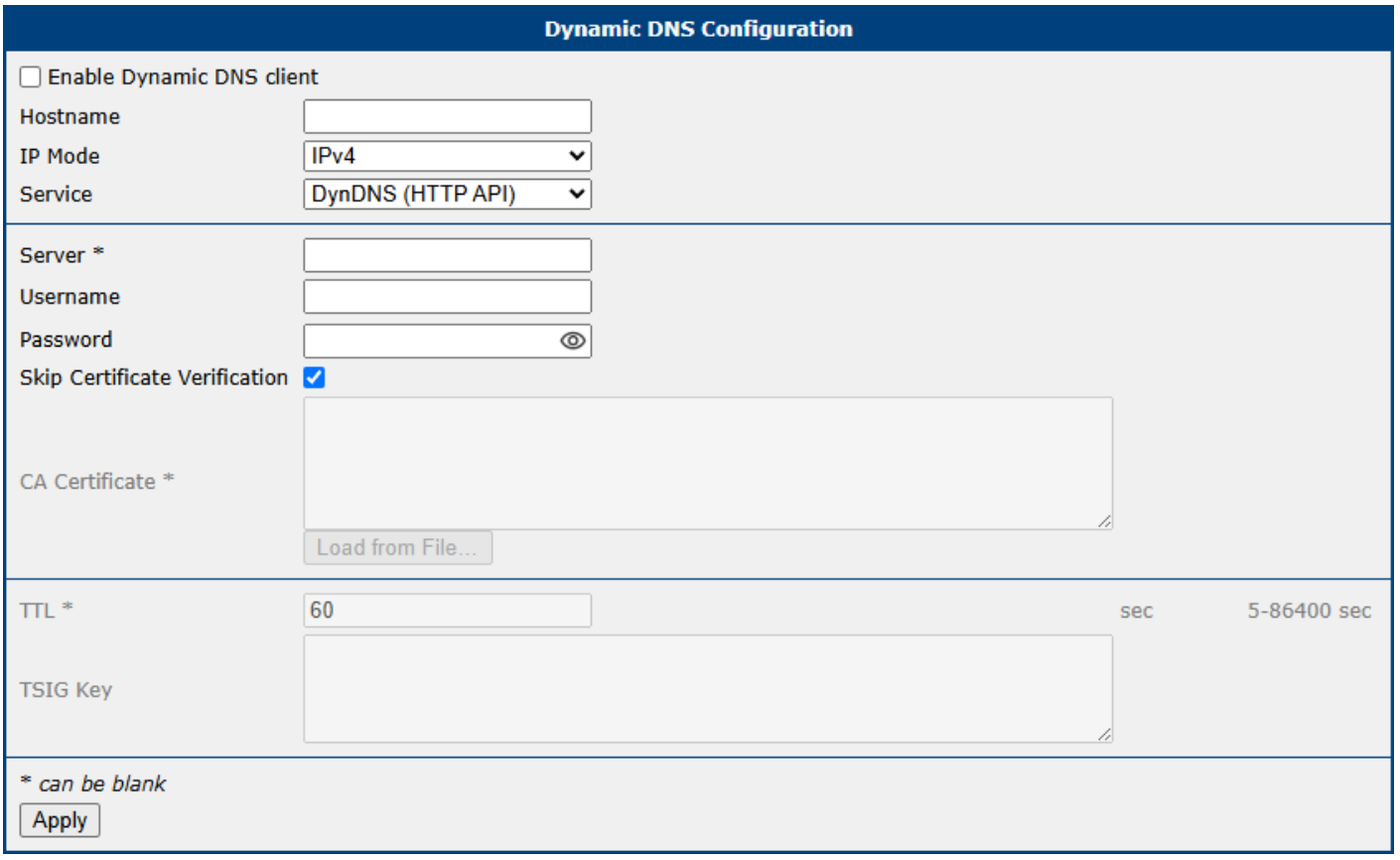
The following sections describe the configuration of services that can be accessed by expanding the menu *Configuration → Services*.

Dynamic DNS

The Dynamic DNS client allows you to access the router using a fixed, memorable hostname, even if the router's IP address changes. The client monitors the router's public IP address and automatically updates the DNS record on a Dynamic DNS server whenever a change is detected. The service supports both standard DDNS (RFC 2136) and secure updates via HTTPS. To configure the service, navigate to *Services → Dynamic DNS*.

Warning

For the Dynamic DNS service to function correctly, the router's SIM card must be assigned a public IP address by the mobile provider.



Dynamic DNS Configuration Page

Item	Description
Hostname	Your fully qualified domain name registered with a Dynamic DNS provider (e.g., `myrouter.example.com`).
IP Mode	The IP protocol version for DNS updates: **IPv4** (default), **IPv6**, or **IPv4/IPv6** (dual-stack).
Service	The protocol for the DNS update: **DynDNS (HTTP API)** for standard web-based providers, or **DDNS (RFC 2136)** for direct updates to standard DNS servers.
Server	The update server address of your Dynamic DNS provider. If left blank, the default value `members.dyndns.org` is used. Several free services are available: freedns.afraid.org ↗, www.duckdns.org ↗, www.noip.com ↗. Secure HTTPS URLs are supported. Active only when *Service* is set to *DynDNS (HTTP API)*.
Username	The username for your Dynamic DNS service account. Active only when *Service* is set to *DynDNS (HTTP API)*.
Password	The password for your Dynamic DNS service account. Active only when *Service* is set to *DynDNS (HTTP API)*.

Item	Description
Skip Certificate Verification	Check to bypass SSL/TLS certificate validation when connecting to an HTTPS server. Active only when *Service* is set to *DynDNS (HTTP API)*.
CA Certificate	The Certificate Authority (CA) certificate used to verify the server's identity during HTTPS updates. Active only when *Service* is set to *DynDNS (HTTP API)*.
TTL	Time to Live for the DNS record, specifying how long the record is cached by DNS resolvers. Default: `60` seconds; range: `5` – `86400` seconds. Active only when *Service* is set to *DDNS (RFC 2136)*.
TSIG Key	The Transaction Signature key used to authenticate DDNS updates. Active only when *Service* is set to *DDNS (RFC 2136)*.

Configuration Example

The example below shows how to configure the router to securely update a dual-stack DNS record using a custom provider's HTTPS API, with certificate verification enforced. The content of the *CA Certificate* is pasted into the corresponding text area (or imported using the *Load From File* button) to authenticate the server.

Setting	Value
Hostname	router.example.com ↗
IP Mode	IPv4/IPv6
Service	DynDNS (HTTP API)
Server	https://ddns.example.com ↗
Username	admin_user
Password	*<your_secure_password>*
Skip Certificate Verification	unchecked
CA Certificate	*<pasted PEM certificate content>*

Info

To access the router's web interface from the internet, you must also enable Remote Access. For details, see NAT.

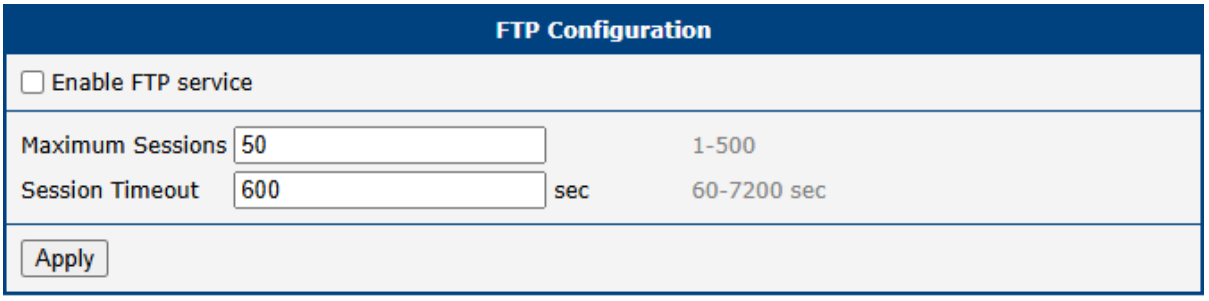
FTP

The FTP protocol (File Transfer Protocol) can be used to transfer files between the router and another device on the network. The FTP server is configured on the FTP page under *Services*.

Warning

FTP is an unencrypted protocol. All data, including credentials, is transmitted in plain text. For secure file transfers, use SFTP over SSH instead.

Item	Description
Enable FTP service	Enabling of FTP server.
Maximum Sessions	Indicates how many concurrent connections the FTP server shall accept. Once the maximum is reached, additional connections will be rejected until some of the existing connections are terminated. The range is from 1 to 500.
Session Timeout	Is used to close inactive sessions. The server will terminate a FTP session after it has not been used for the given amount of seconds. The range is from 60 to 7200.



Configuration of FTP server

GNSS

Info

- Available only for models equipped with a GNSS module.
- **Antenna Placement**: GNSS antennas require a direct line of sight to the satellites. Signal reception is generally not possible inside buildings or tunnels without specialized signal repeaters.
- **Active vs. Passive Antennas**: Active GNSS antennas require power to operate. If an active antenna is connected to a product that supports only passive antennas, no signal will be received.
- Starting from firmware version 6.6.0, this functionality replaces the GPS ↗ Router App. It is strongly recommended to use the built-in feature instead of the legacy Router App. Furthermore, it is not possible to use this functionality together with Router App versions earlier than 2.0.0.

The *GNSS* (Global Navigation Satellite System) page allows you to configure the router's satellite positioning features. When the GNSS service is enabled, the router activates its receiver to acquire satellite signals. This provides several key functionalities:

- Real-time location data becomes available on the router's status pages (see Geolocation and GNSS).
- The router can use GNSS as a source for time synchronization (see NTP).
- If configured, the router's location can be reported via SNMP for network management and monitoring (see SNMP).

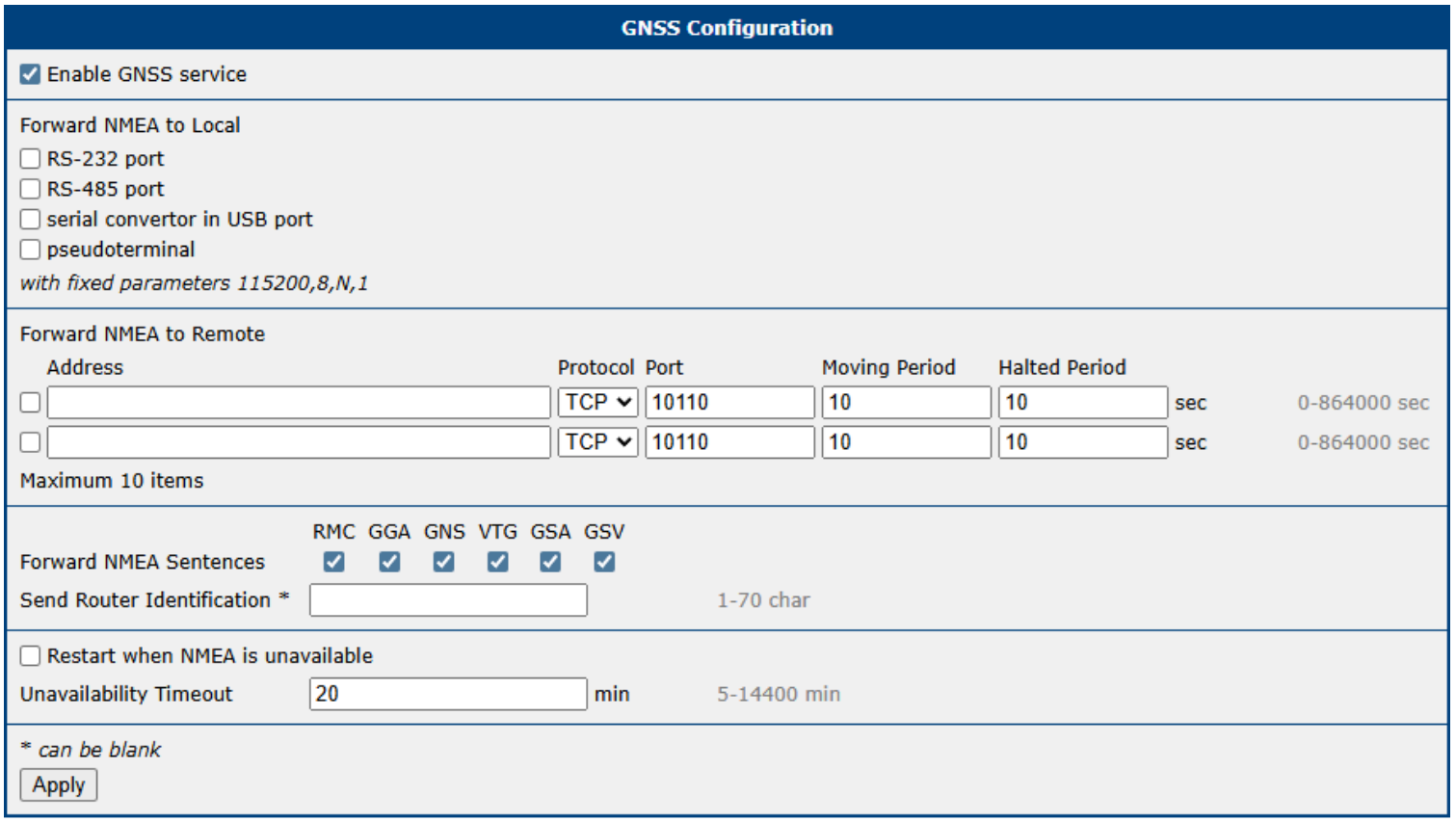
This service is essential for applications requiring precise time and location information, such as vehicle tracking, asset management, or synchronizing distributed network devices. The configuration also allows forwarding of raw NMEA data to both local serial ports and remote servers over the network.

Item	Description
Enable GNSS service	Enables or disables the GNSS functionality in the router. When enabled, the router starts acquiring GNSS data from the integrated receiver.
Forward NMEA to Local	Select the local interface(s) to which the NMEA output from the GNSS receiver will be forwarded. Available options: • RS-232 port • RS-485 port • serial converter in USB port • pseudoterminal The forwarded data uses fixed settings: 115200 baud, 8 data bits, no parity, 1 stop bit.
Forward NMEA to Remote	Configure up to ten remote destinations, each defined by: • **Address**: Destination IP address or hostname • **Protocol**: TCP or UDP transport • **Port**: Destination port • **Moving Period**: Interval (in seconds) to send data when movement is detected • **Halted Period**: Interval (in seconds) to send data when the device is stationary Allowed interval is 0–864000 seconds. Ports default to 10110 (NMEA over TCP/UDP).
Forward NMEA Sentences	Select which specific NMEA sentence types to forward (RMC, GGA, GNS, VTG, GSA, GSV). This allows filtering of the GNSS data sent to local or remote destinations.
Send Router Identification	A custom identification text (1–70 characters) sent to the remote destination as an additional NMEA sentence in the format `$GPFID,X`. Leave the field blank to omit the ID.
Restart when NMEA is unavailable	If enabled, the GNSS service is automatically reset if no data is received for the duration specified in the *Unavailability Timeout* field.
Unavailability Timeout	Defines the maximum time without GNSS data (5–14,400 minutes) before the service is automatically reset.

GNSS configuration items

Info

Local forwarding is possible simultaneously to multiple hardware ports and one pseudoterminal. NMEA forwarding to remote supports both TCP and UDP and can be configured independently for up to ten remote servers.

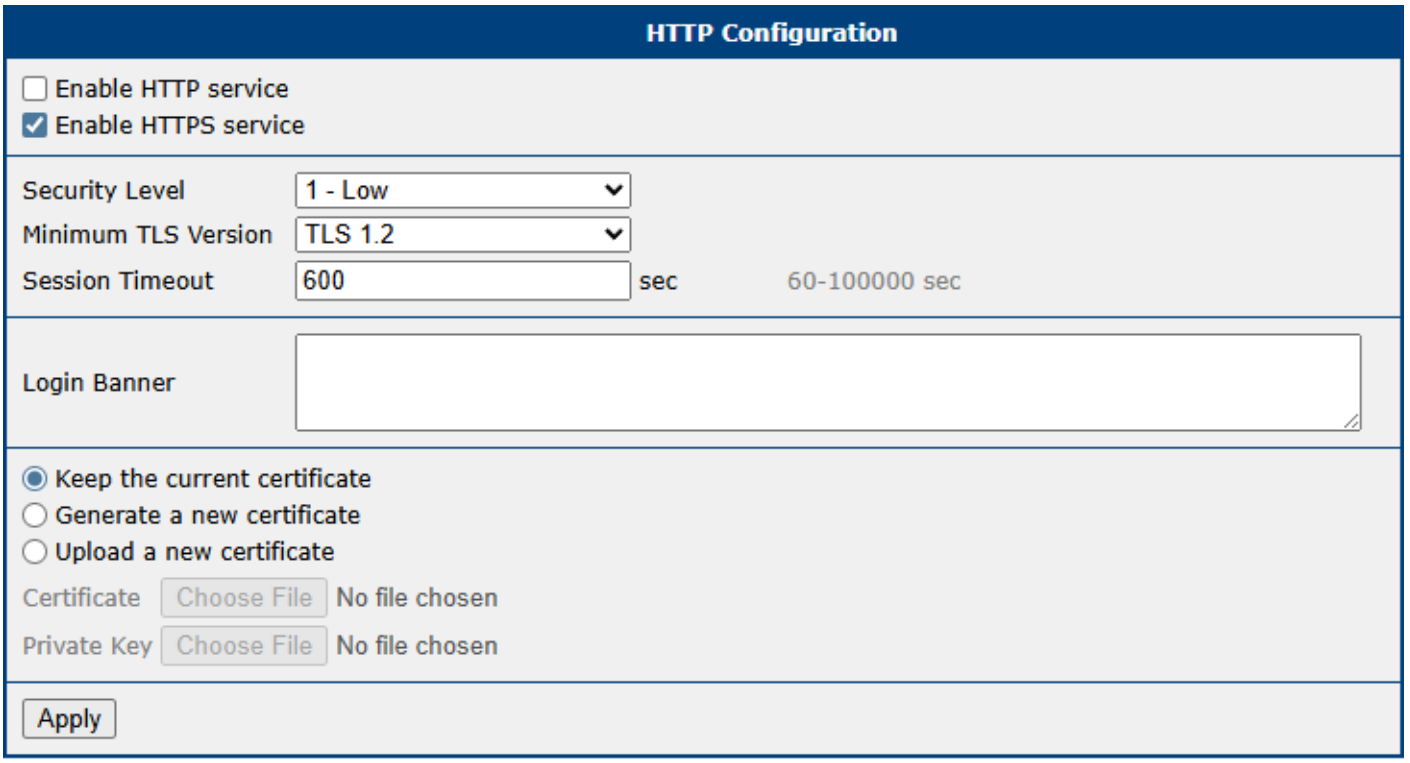


GNSS configuration page

HTTP

> **Warning**
>
> Make sure your certificate matches the *Security Level*. Increasing *Security Level* without generating a new certificate may lead to inability to connect to Web GUI.

This page manages access to the router's web configuration interface via HTTP and HTTPS. For maximum security, use HTTPS — it encrypts all communication between the browser and the router. Even if HTTP is disabled, the router continues to listen on port 80 for the sole purpose of redirecting requests to HTTPS.



Web Server Configuration Page

Item	Description
Enable HTTP service	Enables unencrypted access to the web interface. Not recommended.
Enable HTTPS service	Enables secure, encrypted access to the web interface. This is the default and recommended setting.
Security Level[1]	Sets the minimum cryptographic strength by controlling which TLS versions and cipher suites are permitted. Higher levels disable older, less secure algorithms. • **0 - Weak**: Allows all cryptographic suites, including insecure legacy algorithms. This level is not recommended and should only be used for compatibility with outdated systems. • **1 - Low**: Provides a baseline of 80-bit security (default). • **2 - Medium**: Enforces a minimum of 112-bit security. • **3 - High**: Enforces a minimum of 128-bit security (requires AES-128 or stronger). • **4 - Very High**: Enforces a minimum of 192-bit security (requires AES-192 or stronger).
Minimum TLS Version	The minimum TLS version the router's web server will accept. Options range from TLS 1.0 to TLS 1.3. TLS 1.0 and 1.1 are only available when *Security Level* is set to 0. For maximum security, select the highest version compatible with your clients.
Session Timeout	The inactivity period (in minutes) after which a user is automatically logged out.
Login Banner	Custom text displayed on the login page above the credentials fields.
Keep the current certificate	Retains the certificate currently stored on the router.
Generate a new certificate	Generates a new self-signed certificate corresponding to the selected *Security Level*.

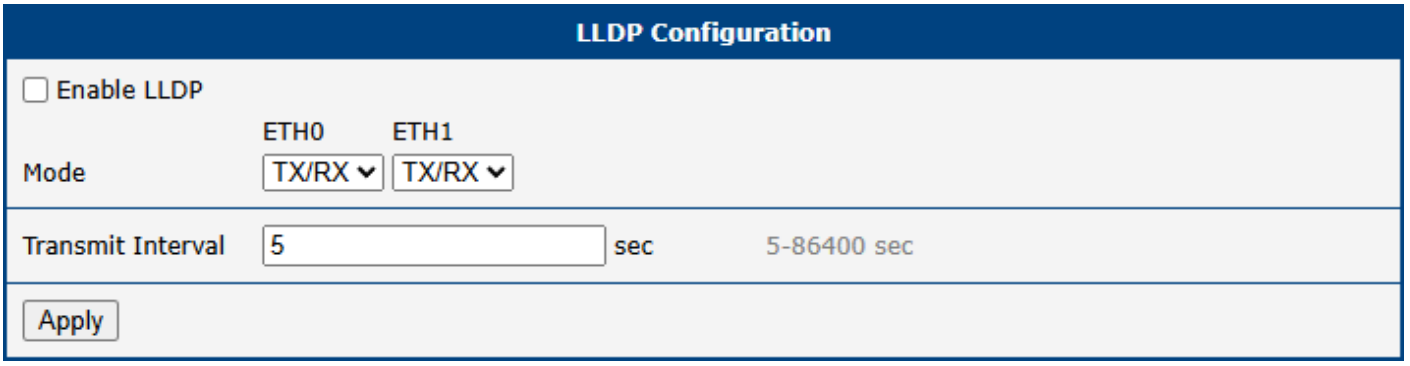
Item	Description
Upload a new certificate	Allows uploading a custom certificate, such as one signed by a trusted Certificate Authority.
Certificate	The PEM-formatted certificate file to upload. The file may contain a single certificate or a full certificate chain.
Private Key	The private key file corresponding to the certificate being uploaded.

[1] For a detailed explanation, see the Security Guidelines ↗ application guide, specifically the chapter on cryptographic algorithms.

LLDP

> **Info**
>
> Information about discovered neighbors can be viewed on the *Status → Network* page, under the *LLDP Neighbors* section.

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral, Layer 2 network protocol used by devices to advertise their identity, capabilities, and neighbors on a local area network. Enabling LLDP on the router facilitates easier network mapping, topology discovery, and troubleshooting in multi-vendor environments. To configure this feature, navigate to *Configuration → Services → LLDP*. After making any changes, click the *Apply* button to save and activate the new configuration.



LLDP configuration page

Item	Description
Enable LLDP	Activates the Link Layer Discovery Protocol globally on the router.
Mode	Defines the communication mode for all available Ethernet interfaces. For devices equipped with a switch, this includes individual switch ports. Available options per interface: • **TX/RX**: The port both transmits LLDP advertisements and receives LLDP packets from neighboring devices. • **RX**: The port only receives LLDP packets. • **off**: LLDP communication is disabled on this port.

Item	Description
Transmit Interval	Specifies the frequency, in seconds, at which LLDP advertisement packets are broadcast to neighbors. The default is `5` seconds; the permitted range is `5` to `86400` seconds.

LLDP configuration parameters

NTP

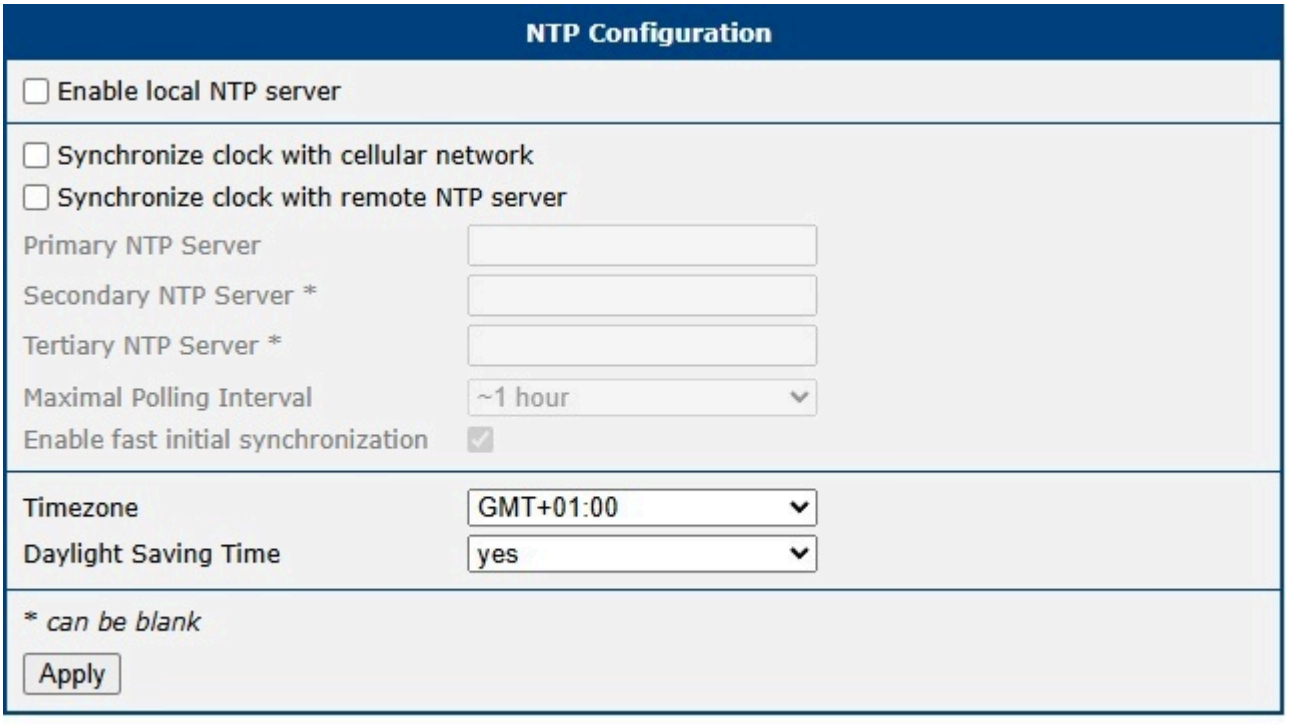
The NTP (Network Time Protocol) configuration page allows you to configure the router's NTP client and/or server functions. To open the NTP configuration page, click *NTP* in the *Configuration* section of the main menu.

Info

- Some configuration options described below may not be available on all router models.
- Upon initial activation, the NTP service may require up to 15 minutes to stabilize due to hardware clock adjustments. During this period, Syslog may report `TIME_ERROR: Clock Unsynchronized` . This is normal and will resolve when synchronization is complete.

Warning

Operating the router as an NTP server while its own clock is not synchronized to a reliable external time source (e.g., remote NTP server, cellular network, or GNSS) is strongly discouraged. This may result in incorrect time propagation to other devices relying on this router.



NTP Configuration Page

Info

Time-Synchronization Accuracy

The accuracy of the router's clock depends on the synchronization source:

- **Remote NTP Server** (recommended): Typically within several milliseconds. External NTP servers are usually synchronized to atomic clocks.
- **Cellular Network (NITZ)**: Typically up to several seconds, depending on the mobile operator's infrastructure.
- **GNSS**: Typically around one second. Not recommended for applications requiring high-precision timekeeping.

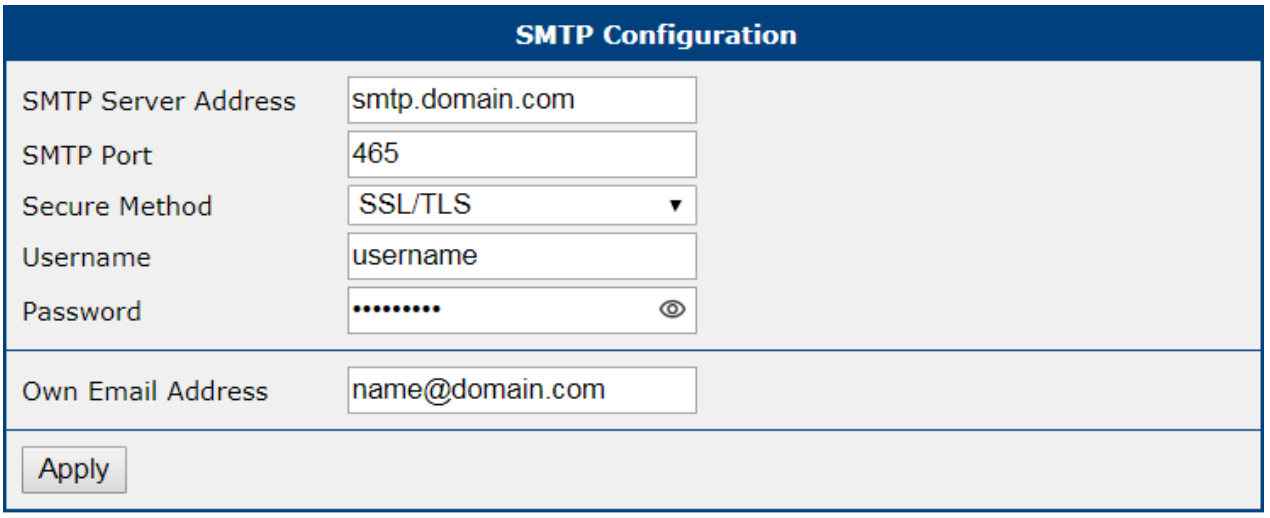
Item	Description
Enable local NTP server	When enabled, the router functions as an NTP server, allowing other devices on the local network to synchronize their time with it. The accuracy of the time served depends on how the router's own clock is synchronized (see options below).
Synchronize clock with cellular network	The router's system clock will be synchronized using time information provided by the connected cellular network (e.g., via NITZ - Network Identity and Time Zone). This option is only effective if the cellular connection is active and the network provider supports this feature.
Synchronize clock with remote NTP server	The router's system clock will be synchronized using the configured NTP server(s). This method provides the highest accuracy and is the recommended option when a reliable internet connection is available.
Synchronize clock with GNSS	The router's system clock will be synchronized using time data from the GNSS receiver. This option is only available on router models equipped with a GNSS module.
Primary NTP Server	IP address or domain name of the primary remote NTP server. This server is queried first for time synchronization.
Secondary NTP Server	IP address or domain name of the secondary remote NTP server. This server is used if the primary server is unavailable.
Tertiary NTP Server	IP address or domain name of the tertiary remote NTP server. This server is used if both primary and secondary servers are unavailable.
Maximal Polling Interval	Defines the maximum time interval (typically in seconds, often expressed as a power of 2) between queries sent to the remote NTP server(s) for time synchronization. Longer intervals reduce network load but may result in less frequent time corrections.
Enable fast initial synchronization	Enables rapid initial time correction if a large discrepancy exists between the router's current system time and the time reported by the NTP server. This allows for a quick jump to the correct time rather than gradual adjustments (slewing).
Timezone	Specifies the geographical timezone where the router is physically located. This setting is crucial for correct local time display and DST adjustments.
Daylight Saving Time	Enables or disables automatic adjustment for Daylight Saving Time (DST). When enabled, the router will adjust its clock according to the DST rules for the selected *Timezone*.

SMTP

The router includes a Simple Mail Transfer Protocol (SMTP) client, which can be configured to send emails for notifications or from scripts. To configure the client, navigate to *Services → SMTP*.

Info

- The settings on this page must match the requirements of your email provider's SMTP server.
- Some mobile service providers may block standard SMTP ports, potentially restricting you to using the provider's own SMTP server.



SMTP Client Configuration

Item	Description
SMTP Server Address	The IP address or domain name of your outgoing mail server.
SMTP Port	The port number the SMTP server uses. Common ports: 25, 465 (SSL/TLS), and 587 (STARTTLS).
Secure Method	The encryption method required by the server: **none**, **SSL/TLS**, or **STARTTLS**.
Username	The username for your email account.
Password	The password for your email account. Enter valid characters only, refer to Allowed and Restricted Input Characters.
Own Email Address	The sender's email address that will appear on outgoing emails (e.g., `my-router@mydomain.com`).

Sending Emails

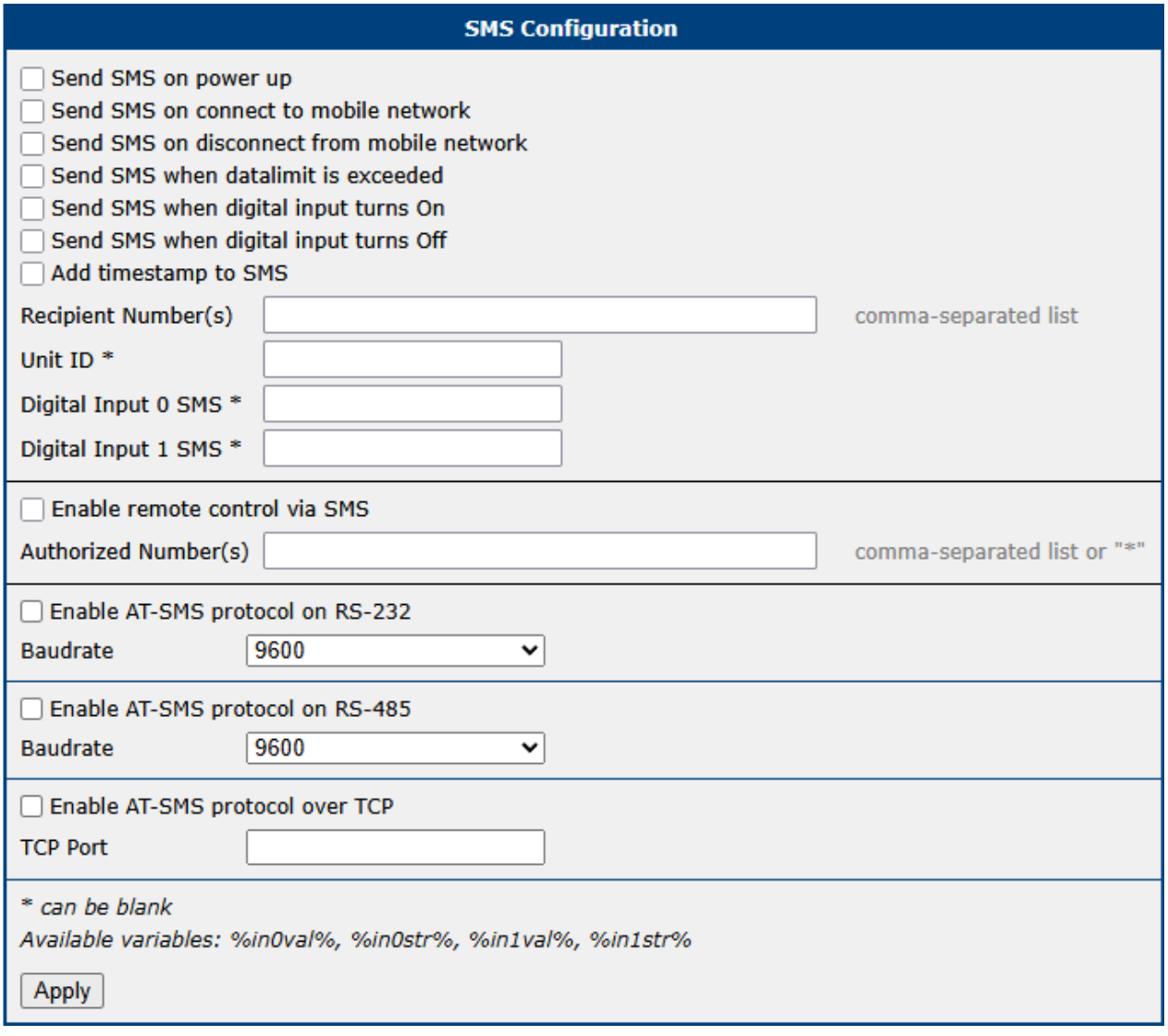
Once the SMTP client is configured, you can send emails in two ways:

- **From a script:** Use the `email` command within a startup or custom script. Scripts are managed on the *Configuration → Scripts* page.
- **From the command line:** Connect to the router via SSH and use the `email` command directly.

For detailed syntax and examples of the `email` command, refer to the Command Line Interface application guide.

SMS

The *Configuration → Services → SMS* page allows you to configure all SMS-related functionality, including automated event notifications, remote control via SMS commands, and direct access to the cellular module using the AT-SMS protocol.



SMS Configuration Page

SMS Notifications

This section allows you to configure the router to automatically send an SMS notification to one or more phone numbers when a specific system event occurs.

Item	Description
Send SMS on power up	If checked, an SMS is sent when the router starts.
Send SMS on connect to mobile network	If checked, an SMS is sent when the router establishes a mobile network connection.
Send SMS on disconnect from mobile network	If checked, an SMS is sent when the router loses its mobile network connection.
Send SMS when datalimit is exceeded	If checked, an SMS is sent when a mobile data limit is exceeded.
Send SMS when digital input turns On/Off	If checked, an SMS is sent when the state of a digital input changes to On or Off, respectively.
Add timestamp to SMS	If checked, a timestamp (YYYY-MM-DD hh:mm:ss) is added to the beginning of each notification SMS.
Recipient Number(s)	A comma-separated list of recipient phone numbers for the notifications.
Unit ID	A custom identifier for the router, which can be included in the SMS text.
Digital Input 0/1 SMS[1]	The custom text to be sent when the corresponding digital input event is triggered.

[1] You can use variables like `%in0val%` (numeric value 0/1) or `%in0str%` (string "Off"/"On") to include the input's state in the message.

Remote Control via SMS

The router can be controlled by sending specific commands via SMS from an authorized phone number. To activate this functionality, enable it and specify at least one authorized number.

Item	Description
Enable remote control via SMS	Master switch for SMS processing. When disabled, all incoming SMS messages are ignored and neither control commands nor the custom script at `/var/scripts/sms` will be executed.
Authorized Number(s)	A comma-separated list of phone numbers authorized to send control commands. Enter `*` to accept commands from any phone number.

The table below lists all supported control commands. Note that most commands trigger temporary actions that are reverted upon reboot; only the `set profile` command makes a permanent change to the router's configuration. To control the router, send an SMS containing only the command text:

SMS	Description
go online sim [1|2]	Switches the active mobile connection to the specified SIM card.
go online	Switch the router to the online mode.
go offline	Switch the router to the offline mode.
set out*x*=0	Set digital output *x* to 0. Example: `set out0=0`.

SMS	Description
set out*x*=1	Set digital output *x* to 1. Example: `set out0=1`.
set profile std	Set the standard profile. This change is permanent.
set profile alt1	Set alternative profile 1. This change is permanent.
set profile alt2	Set alternative profile 2. This change is permanent.
set profile alt3	Set alternative profile 3. This change is permanent.
reboot	Reboot the router.
get ip	Responds with the current IPv4 address of the active mobile connection.
get ipv6	Responds with the current IPv6 address of the active mobile connection.

Info

For advanced users, custom SMS processing can be implemented using a script at `/var/scripts/sms`. This script is invoked only for messages that are NOT processed as standard control commands (e.g., messages with unknown text or from unauthorized numbers). The *Enable remote control via SMS* option must be enabled for the script to run.

The script receives arguments indicating the sender's authorization status. This allows you to implement custom logic for unhandled messages. The script file does not require execute permissions (`chmod +x`). For more details, see the Extending Router Functionality ↗ application guide, chapter Handling Incoming SMS with a Custom Script ↗.

AT-SMS Protocol

The AT-SMS protocol provides direct access to the router's cellular module using standard AT commands. This allows for advanced management of SMS messages and retrieval of detailed module status information.

This feature can be enabled over a serial port or a TCP connection.

Item	Description
Enable AT-SMS protocol on RS-232 / RS-485	Enables the protocol on the selected serial port.
Baudrate	Sets the communication speed for the corresponding serial port.
Enable AT-SMS protocol over TCP	Enables the protocol over a network connection.
TCP Port	The TCP port on which the router will listen for AT-SMS connections.

If you establish a connection to the router through a serial interface or interface using the TCP protocol, then you can use AT commands to manage SMS messages.

Only the commands supported by the routers are listed in the following table. For other AT commands the OK response is always sent. There is no support for treatment of complex AT commands, so in such a case the router sends ERROR response.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CNUM	Returns the phone number, if available (stored on SIM card)
AT+COPS?	Identifies the available mobile networks
AT+CPIN?	Retrieves the SIM card status (e.g., PIN required)
AT+CREG?	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number
AT+CSQ	Returns the signal strength of the registered network
ATE[0|1]	Enables or disables command echoing

Tips

A detailed description and examples of these AT commands can be found in the AT Commands ↗ application guide.

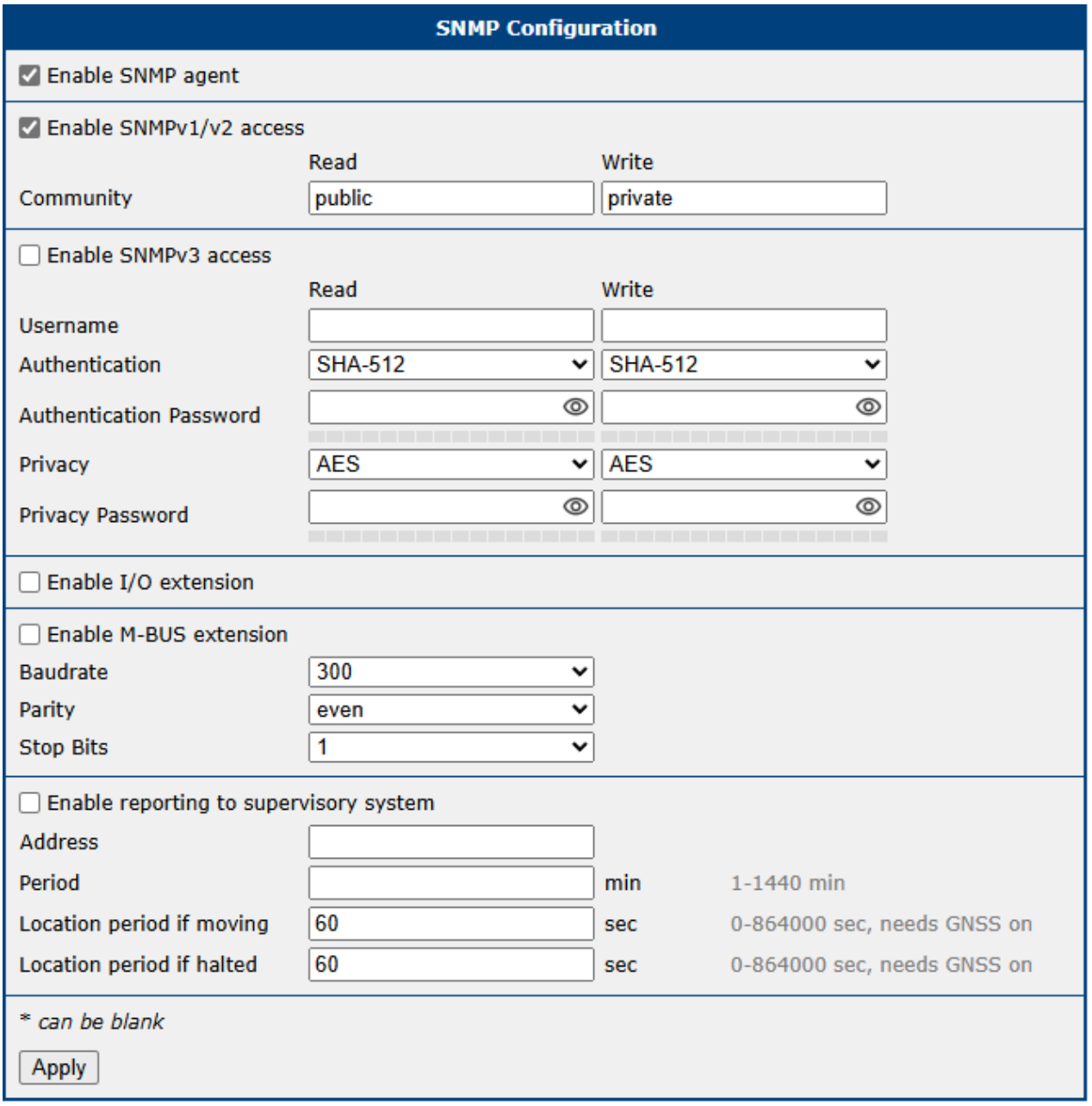
SNMP

The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent, which transmits information about the router and its expansion ports (if applicable) to a management station. To access the page, click *SNMP* in the *Configuration → Services* section.

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or endpoint devices. In SNMP v3, communication is secured through user-specific encryption and authentication. To enable the SNMP service, select the *Enable SNMP agent* checkbox. IPv6 is supported for SNMP traps as well.

Info

Name, *Location*, *Contact*, and *Custom* identification fields are now configured in *Configuration → System → Identification*. These fields are no longer present on the SNMP configuration page.



SNMP Configuration Page

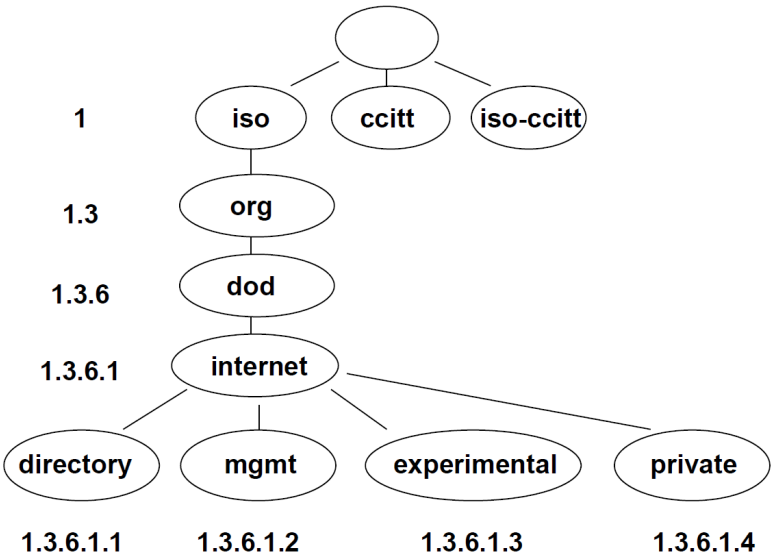
Item	Description
Enable SNMP agent	Turns on the SNMP agent, allowing the router to be managed and monitored using SNMP protocols.
Enable SNMPv1/v2 access	Enables access for SNMPv1 and SNMPv2 protocols. Enter community strings for read and write access.

Item	Description
Community (Read/Write)	Community strings for SNMPv1/v2 access. Default: `public` for read, `private` for write.
Enable SNMPv3 access	Activates configuration options for SNMPv3, providing stronger authentication and encryption.
Username	The username for SNMPv3, configured independently for read and write access.
Authentication	The authentication algorithm (e.g., SHA-512) for SNMPv3 identity verification.
Authentication Password	Password for generating the authentication key. Enter valid characters only, refer to Allowed and Restricted Input Characters.
Privacy	The encryption algorithm (e.g., AES) used to secure SNMPv3 communication.
Privacy Password	Password for encrypting SNMPv3 messages. Enter valid characters only, refer to Allowed and Restricted Input Characters.
Enable I/O extension	Allows monitoring and reporting of digital I/O signals available on the router.
Enable M-BUS extension	Enables support for M-BUS (Meter-Bus) devices. Configure the baudrate, parity, and stop bits as required for your metering hardware. External RS232/M-BUS converters may be needed.
Baudrate, Parity, Stop Bits	Communication parameters for the M-BUS interface.
Enable reporting to supervisory system	Enables transmission of statistical and location data to a supervisory or monitoring server.
Address	Destination IP address or hostname of the supervisory system.
Period	Reporting interval in minutes (1–1440).
Location period if moving / halted	Available on GNSS models only. Defines the reporting interval in seconds (0–864000) for location data. The GNSS service must be enabled. Separate values can be configured for when the router is moving and when it is stationary.

Info

Enabling the *Enable M-BUS extension* option and configuring the *Baudrate*, *Parity*, and *Stop Bits* settings allows you to monitor the status of meters connected via the M-BUS interface. While the M-BUS expansion port is not currently supported, it is possible to use an external RS232/M-BUS converter.

Each monitored value is uniquely identified by a numerical OID (Object Identifier) — a dot-separated sequence of numbers forming a hierarchical tree. The figure below shows the basic tree structure used for creating OIDs.



OID Basic Structure

The SNMP values specific to Advantech routers start at OID `.1.3.6.1.4.1.30140`, interpreted as: **iso.org.dod.internet.private.enterprises.conel**

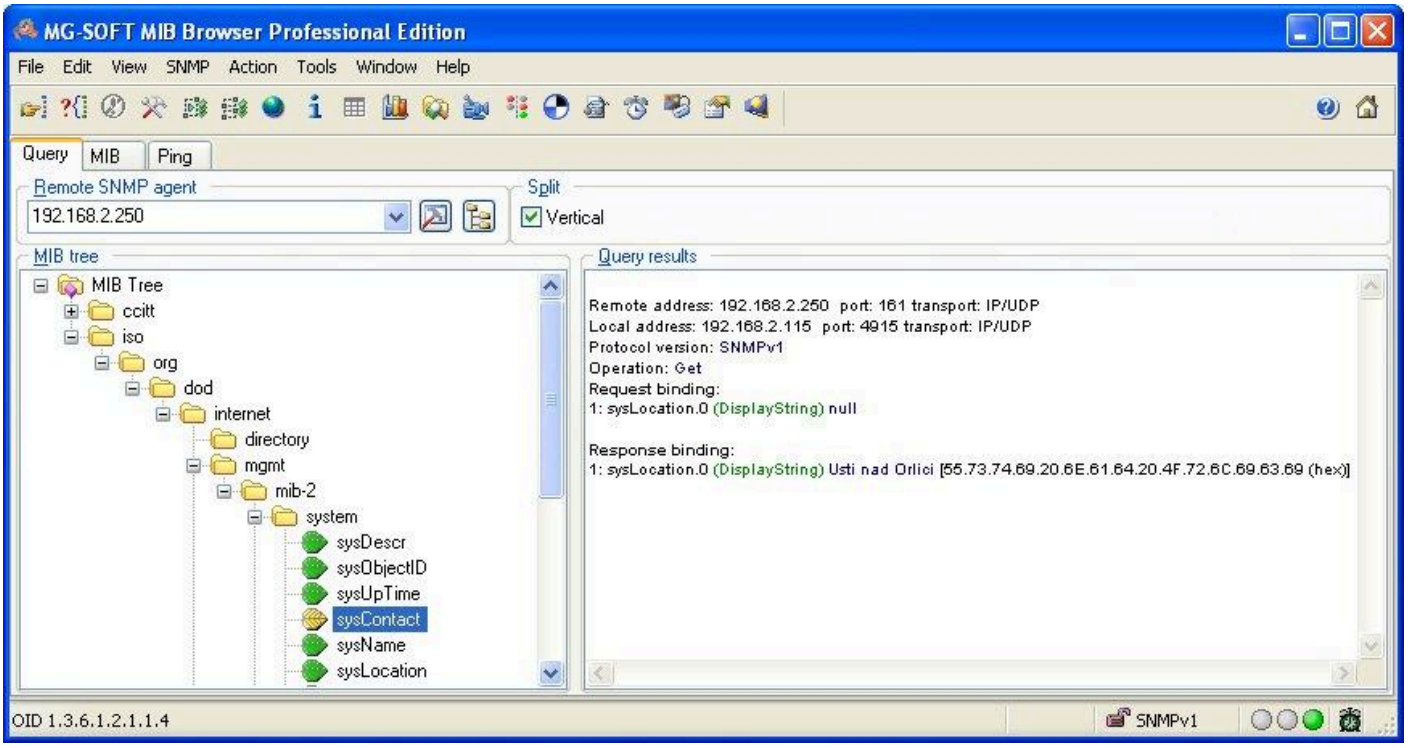
The router provides information such as internal temperature (OID `1.3.6.1.4.1.30140.3.3`) and power voltage (OID `1.3.6.1.4.1.30140.3.4`). For digital inputs and outputs, the following OIDs are used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Digital input BIN0 (values: 0, 1)
.1.3.6.1.4.1.30140.2.3.2.0	Digital output OUT0 (values: 0, 1)
.1.3.6.1.4.1.30140.2.3.3.0	Digital input BIN1 (values: 0, 1)

Info

The list of available and supported OIDs and other details can be found in the SNMP Object Identifiers ↗ application guide.

MIB Browser Example



MIB Browser Example

To access a device, enter the router's IP address in the *Remote SNMP Agent* field. The MIB browser then displays the internal variables in the tree structure. You can also check individual variables by entering their OID.

The path to SNMP objects is: *iso → org → dod → internet → private → enterprises → Conel → protocols*

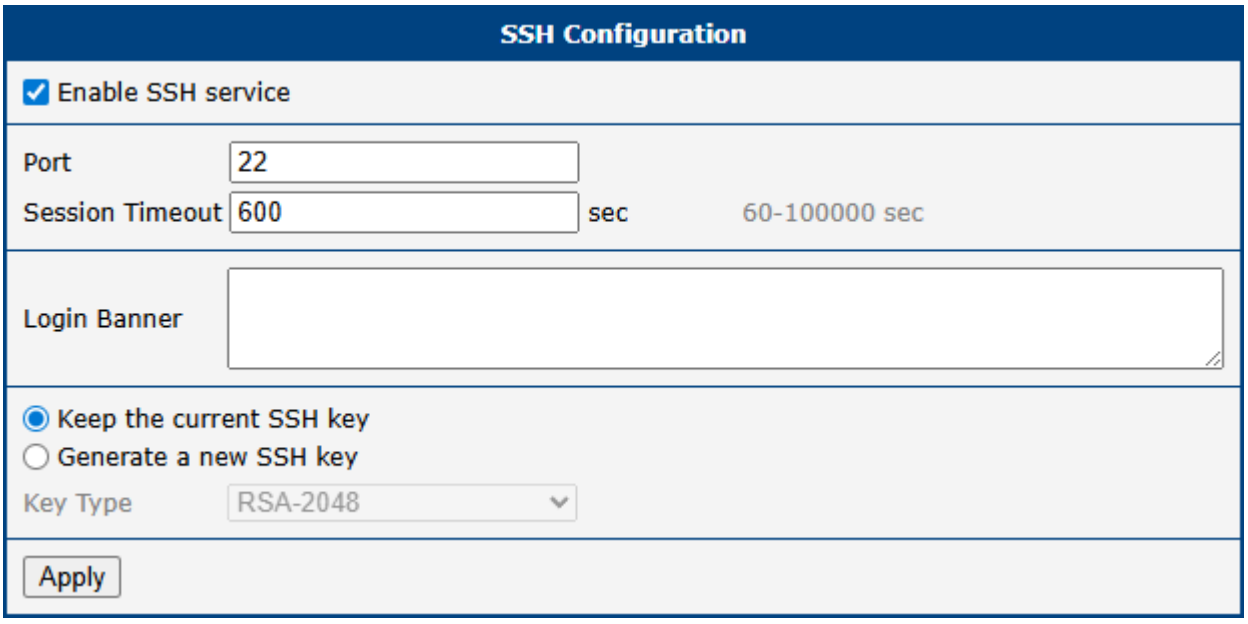
The path to router-specific information is: *iso → org → dod → internet → mgmt → mib-2 → system*

SSH

The Secure Shell (SSH) service allows for secure command-line access to the router's operating system. To configure the SSH server, navigate to *Services → SSH*.

Info

Only users assigned the *Admin* role are authorized to log in via SSH. Users with the standard *User* role cannot access the command line.



SSH Configuration Page

General Settings

Item	Description
Enable SSH service	Enables or disables the SSH server on the router.
Port	The TCP port on which the SSH server listens for incoming connections. Default: port 22.
Session Timeout	The duration of inactivity (in minutes) after which an SSH session is automatically disconnected.
Login Banner	A custom message displayed to users before they are prompted for login credentials.

Host Key Management

The SSH host key is a unique cryptographic key that clients use to verify the router's identity and prevent man-in-the-middle attacks.

> **Info**
>
> When you connect to the router via SSH for the first time, your client will prompt you to accept the host key's fingerprint. If the host key ever changes (e.g., after generating a new one), your client will display a security warning. This is expected behavior.

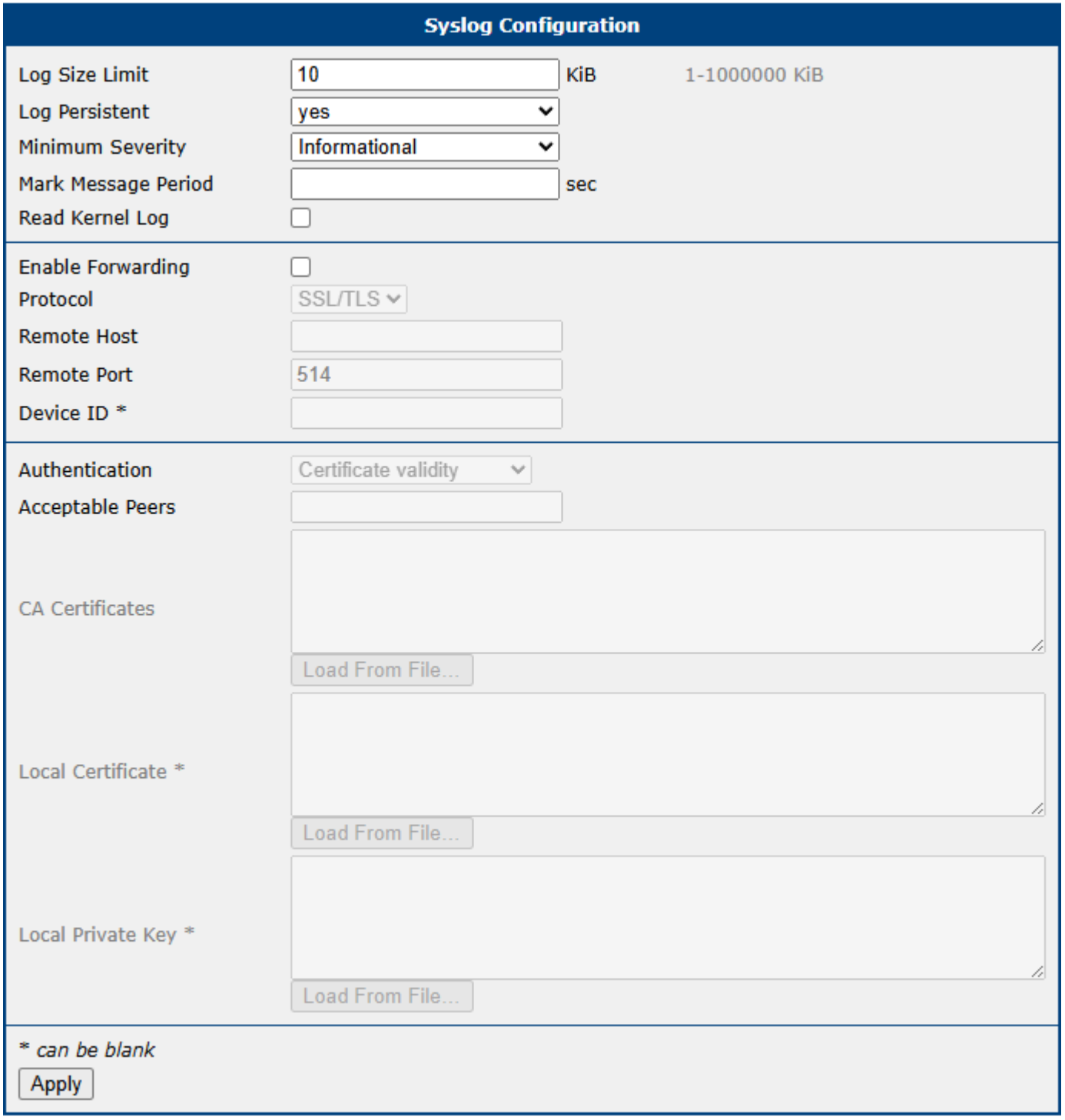
Item	Description
Keep the current SSH key	Retains the existing host key. Recommended for normal operation.
Generate a new SSH key	Discards the current key and generates a new one. Typically used for security policy reasons only.

Item	Description
Key Type	The algorithm for the host key: **ED25519** (modern, fast, and secure elliptic curve algorithm) or **RSA** (older, widely supported standard).

Syslog

The Syslog service collects and manages system messages from the router's operating system and applications. To configure it, navigate to *Services* → *Syslog*.

The collected logs can be viewed at *Status* → *System Log*, or via the command line with the `slog` command.



Syslog Configuration Page

Local Logging

These settings control how logs are stored on the router itself.

Item	Description
Log Size Limit	Sets the maximum size (in KiB) for the local log files. The default is 10 KiB.

Item	Description
Log Persistent	If enabled, the system log is saved in persistent memory and will survive a router reboot.
Minimum Severity	Sets the minimum severity level for messages to be logged by the system. Levels range from *Emergency* (highest severity, least detail) to *Debug* (lowest severity, most detail). **Note:** Some components, such as IPsec or certain Router Apps, have their own independent logging level settings. These act as a secondary filter. A service-specific setting can make that service **less** verbose than the global setting, but it cannot force the system to log messages that fall below the global *Minimum Severity* level.
Mark Message Period	Sets a time interval for the router to write a `-- MARK --` message to the log, which acts as a keepalive indicator.
Read Kernel Log	Check this to include kernel-level messages (e.g., firewall logs, device notifications) in the system log. Upon service (re)start, all existing kernel log entries are sent to the remote server, potentially resulting in duplicate messages; afterward, only new messages are forwarded.

Remote Forwarding

The router can forward log messages in real time to a remote Syslog server for centralized storage and analysis.

Item	Description
Enable Forwarding	Enables the forwarding of all log messages to a remote host.
Protocol	The transport protocol for forwarding: **UDP**, **TCP**, or **SSL/TLS** for a secure connection.
Remote Host	The hostname or IP address of the remote Syslog server.
Remote Port	The port number on which the remote server is listening.
Device ID	A custom identifier for the router, used in the forwarded log messages. If left blank, the default ID *Router* is used.

Remote Server Authentication

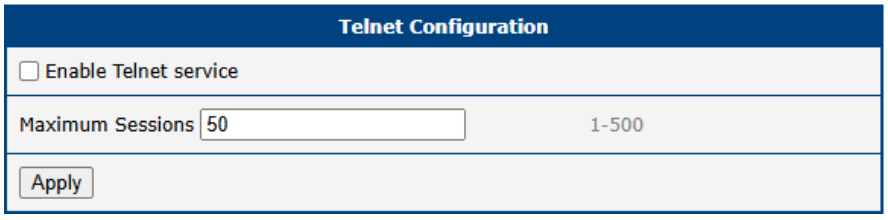
These settings configure authentication when using the **SSL/TLS** protocol for secure forwarding.

Item	Description
Authentication	The method used to authenticate the remote server: • **None (encryption only)**: Encrypts the connection but does not authenticate the server. • **Certificate fingerprint**: Authenticates the server by matching its certificate fingerprint against the one in *Acceptable Peers*. • **Certificate validity**: Authenticates any server that presents a valid certificate signed by the specified CA. • **Certified peer name**: Authenticates the server by checking its certificate's validity and matching its DNS name or Common Name against the *Acceptable Peers* list. **Note:** The server may apply its own sender authentication settings, independent of this configuration.
Acceptable Peers	A list of accepted certificate fingerprints (SHA1) or DNS/Common Names. Wildcards (e.g., `*.example.net`) are supported for names. Required if *Authentication* is set to *Certificate fingerprint* or *Certified peer name*.
CA Certificates	A file containing the full CA certificate chain in PEM format, used to validate the remote server's certificate. Not required if *Authentication* is set to *None*.
Local Certificate	A local client certificate (in PEM format) to present to the remote server if it requires client authentication.
Local Private Key	The private key corresponding to the *Local Certificate*. This is optional if the server does not require client authentication.

Telnet

The Telnet service provides unencrypted, text-based command-line access to the router. To configure it, navigate to *Services → Telnet*.

> **Warning**
>
> Telnet is an insecure protocol. All data, including usernames and passwords, is transmitted in plain text. It is strongly recommended to use the secure SSH service instead.



Telnet Configuration Page

Item	Description
Enable Telnet service	Enables the Telnet server on the router.
Maximum Sessions	The maximum number of concurrent Telnet sessions allowed. The range is from 1 to 500.

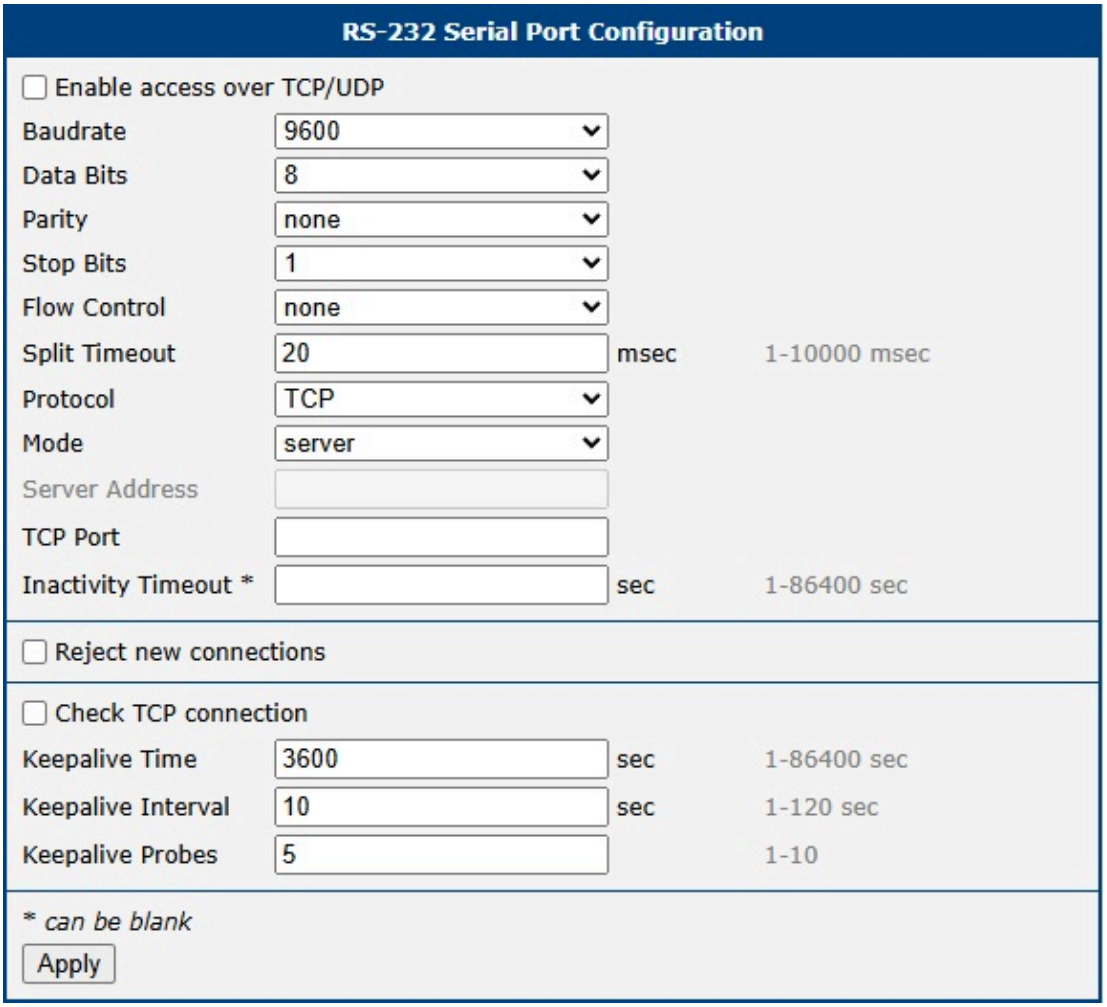
Peripheral Ports

> **Info**
>
> Some interfaces may not be available for all models.

Configuration of physical interfaces such as RS-232, RS-485, USB serial converter, and digital Inputs/Outputs is accessible from *Configuration → Peripheral Ports*. Each interface is configured on its own subpage.

RS-232 Port

On the RS-232 Port configuration page, you can activate the port by ticking the *Enable access over TCP/UDP* checkbox. Additional settings are detailed in the table below. Support is provided for both IPv4 and IPv6 TCP/UDP client/server configurations.

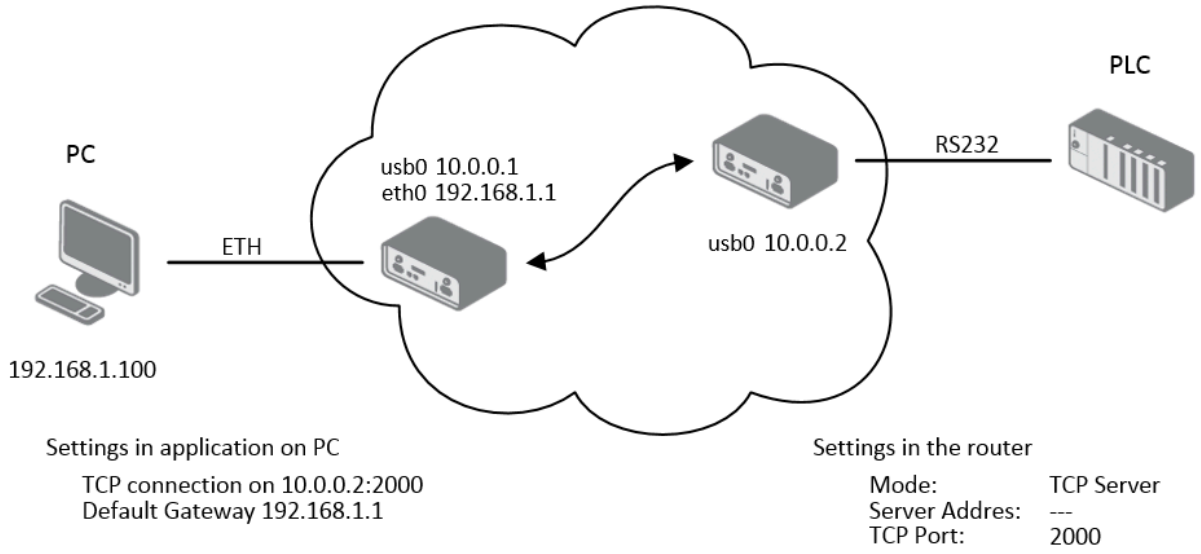


RS-232 Serial Port Configuration

Item	Description
Baudrate	Configurable communication speed: **300**, **600**, **1200**, **2400**, **4800**, **9600** (default), **19200**, **38400**, **57600**, **115200**, **230400**.
Data Bits	Number of data bits: **5**, **6**, **7**, **8** (default **8**).
Parity	Parity control bit: • **None**: Data is sent without a parity bit. • **Even**: Data is sent with even parity. • **Odd**: Data is sent with odd parity.
Stop Bits	Number of stop bits: **1** (default), **2**.
Flow Control	Flow control method: **None** or **Hardware**.
Split Timeout	Time threshold for message segmentation. If the gap between two characters exceeds this value (in milliseconds), any buffered characters are sent over the network.
Protocol	Communication protocol: • **TCP**: Communication using the connection-oriented TCP protocol. • **UDP**: Communication using the connectionless UDP protocol.
Mode	Connection mode for TCP protocol: • **server**: The router listens for incoming TCP connection requests on the specified port. • **client**: The router initiates a connection to a TCP server using the specified IP address and port.
Server Address	When in *client* mode, the IP address or domain name of the remote server. Both IPv4 and IPv6 are supported.
TCP Port	The TCP/UDP port for communication. Applies to both server and client modes.
Inactivity Timeout	Time in seconds after which an inactive TCP/UDP connection is automatically terminated.
Reject new connections	When enabled, the router rejects new incoming connections while one is already active, enforcing a single-client connection.
Check TCP connection	When enabled, the router actively monitors the TCP connection using keepalive packets.
Keepalive Time	Time interval in seconds after which the router sends a keepalive probe to verify the connection.
Keepalive Interval	Time in seconds the router waits for a response to a probe before resending it.
Keepalive Probes	Number of unanswered probes before the connection is considered inactive.

Ethernet-to-Serial Communication Example

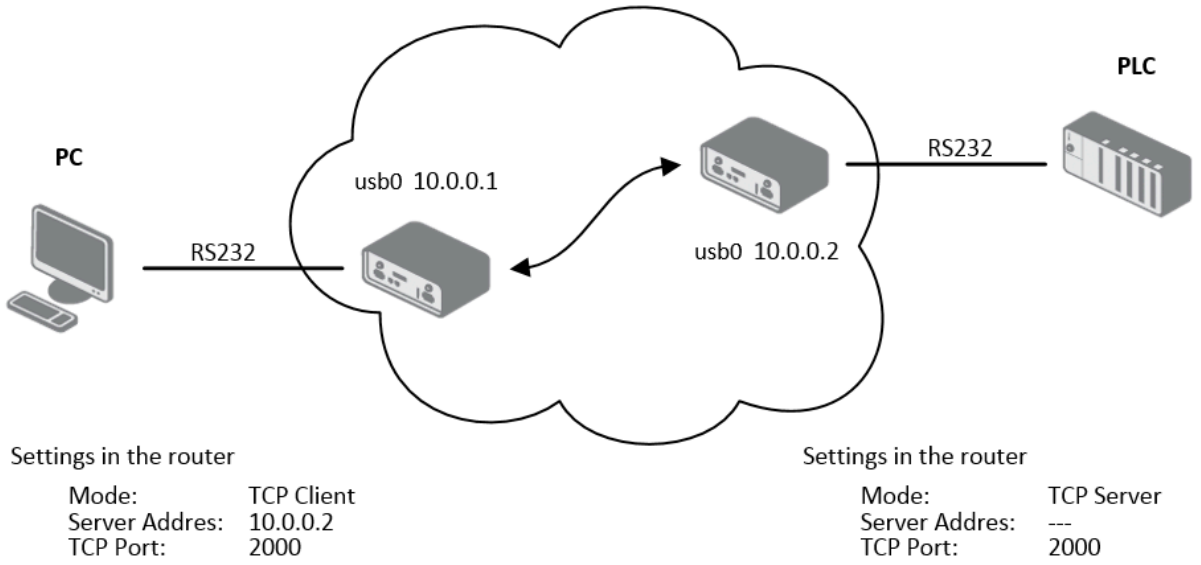
This example demonstrates how to use the router as a gateway to connect a PC on an Ethernet network to a remote serial device. A PC at 192.168.1.100 sends data to the remote router (10.0.0.2) on TCP port 2000. The remote router is configured in *TCP Server* mode and listens for incoming connections. Once a connection is established, it forwards all data from the TCP socket to its RS-232 port, which is connected to the PLC. The first router (192.168.1.1) serves as the default gateway for the PC.



Ethernet-to-Serial Communication Configuration Example

Serial Interface Communication Example

This example illustrates how to create a transparent serial tunnel over an IP network. The PC is connected via RS-232 to the first router (10.0.0.1), which is configured in *TCP Client* mode and initiates a connection to the second router (10.0.0.2) on port 2000. The second router, configured as a *TCP Server*, is connected to the PLC via its RS-232 port. Data from the PC is tunneled over the TCP connection to the second router and passed to the PLC.



Serial Interface Communication Configuration Example

RS-485 Port

The RS-485 port configuration is analogous to the RS-232 port. The configuration items and their meanings are identical to those described in the RS-232 Port section.

USB Port

Info

- The USB port is automatically disabled to prevent damage during an overload condition, which occurs when a connected device draws excessive current. Normal operation is restored after rebooting the router.
- For detailed instructions on creating, mounting, checking, and unmounting a file system on a USB flash drive, refer to the *Ext4 Filesystem Utilities* ↗ router app documentation.

The USB port supports USB **mass storage devices** and **serial converters**. Configuration can be performed via the *USB Port* menu item.

By unchecking the *Enable USB port* option, the USB port can be disabled. Before doing so, ensure that all file systems on attached storage are properly unmounted to prevent data corruption. This can be done in the console using the `umount /mnt/usb_storage` command.

Enabling *Enable USB serial converter access over TCP/UDP* allows the router to create a network-accessible **virtual serial port** for a supported device connected to its USB port. This enables communication with serial-based equipment (e.g., sensors or industrial controllers) over a TCP or UDP connection. Consequently, you can remotely monitor or configure serial devices without needing a dedicated on-site computer. All subsequent configuration items for this feature are identical to those described in the RS-232 Port section. For the list of supported USB converters, refer to the *Extending Router Functionality* ↗ application guide. Refer to Using an Unsupported Serial Converter Chip for instructions on adding support for unsupported serial converters.

Mounting a USB Flash Drive to the System

To access a USB flash drive within the router's system, it must first be mounted. Follow these steps:

1. **Connect the USB Flash Drive**
   Plug the USB flash drive into the router's USB port.
2. **Identify the USB Flash Drive**
   Run the `dmesg` command to display recent system messages and identify the name of the newly connected device. Look for an entry such as `/dev/sda`, with partitions like `/dev/sda1`.
3. **Create a Mount Point (Optional)**
   If you prefer a dedicated directory, create one: `mkdir /mnt/usb`
4. **Mount the USB Flash Drive**
   Use the mount command to attach the drive: `mount /dev/sda1 /mnt/usb`
5. **Verify Successful Mount**
   List mounted file systems with `mount` or check the directory contents with `ls /mnt/usb` to confirm the files are accessible.
6. **Unmount the USB Flash Drive**
   When finished, unmount the drive to prevent data corruption: `umount /mnt/usb`.

Once unmounted, you can safely remove the flash drive. If you encounter issues, ensure the drive is properly connected and its file system (e.g., vfat, ext4, exfat) is supported.

Info

If the mount command fails, you may need to specify the filesystem type with the `-t` option, for example: `mount -t vfat /dev/sda1 /mnt/usb`

Using an Unsupported Serial Converter Chip

In some cases, a serial converter chip may not be natively supported by the router. Every USB device is identified by two numbers:

- **Vendor ID (VID):** Identifies the device manufacturer.
- **Product ID (PID):** Identifies the specific product model.

Finding the VID and PID

You can find the VID and PID of your device:

- **On Linux:** Use the `lsusb` command. Note that it is not available in the router's environment.
- **On Windows:** Open *Device Manager*, locate your device, and find the IDs in its properties.

Enabling the Unsupported Device

Once you have the VID and PID, you can add support for the device by echoing these values to the `ftdi_sio` driver:

```bash
echo <VID> <PID> > /sys/bus/usb-serial/drivers/ftdi_sio/new_id
```

For example, for a device with VID `0403` and PID `d921`, use:

```bash
echo 0403 d921 > /sys/bus/usb-serial/drivers/ftdi_sio/new_id
```

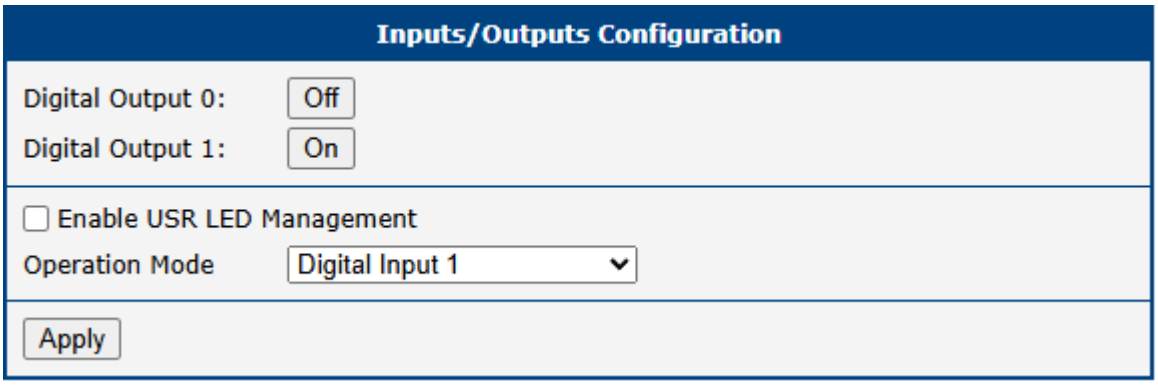
After running this command, the driver should recognize the device. If not, try reloading the driver or reconnecting the device.

Inputs/Outputs

Info

Starting from router firmware version 6.6.0, the USR LED settings on this page replace the original *USR LED Management* ↗ router app, and it is strongly recommended to use this built-in feature instead of the app.

On the *Inputs/Outputs* page, you can manually turn a digital output on or off and define the operation mode for the router's USR LED. In the image below, *Digital Output 0* is *On* and can be turned off by clicking the *Off* button. Conversely, *Digital Output 1* is *Off* and can be turned on by clicking the *On* button.



Inputs/Outputs Configuration

By enabling *Enable USR LED Management*, you can set the desired operation mode for the USR LED. The available modes are described in the table below:

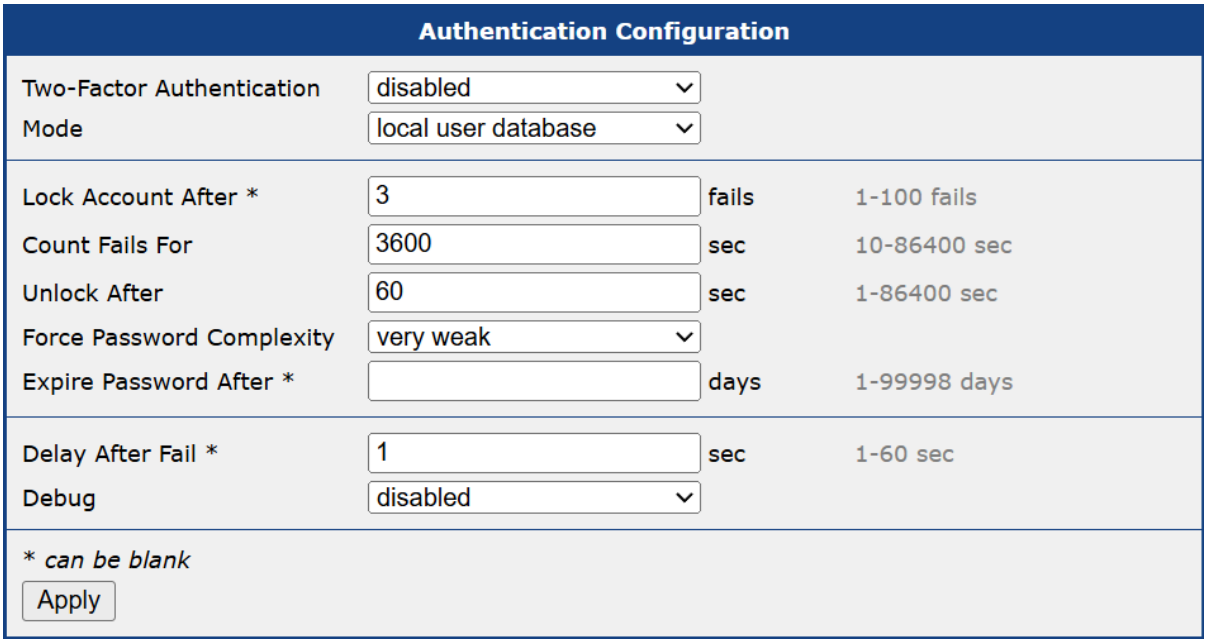
Item	Description
Always OFF	The LED is permanently off.
Always ON	The LED is permanently on. This is useful for physically locating the router among other devices.
Digital Input x	The LED lights when digital input *x* is *On*. The state is updated every 100 ms.
Digital Output x	The LED lights when digital output *x* is *On*. The state is updated every 100 ms.
RS-xxx Rx activity	The LED lights when the serial interface on peripheral port *xxx* is receiving data.
RS-xxx Tx activity	The LED lights when the serial interface on peripheral port *xxx* is transmitting data.
RS-xxx Rx and Tx activity	The LED lights when the serial interface on peripheral port *xxx* is receiving and/or transmitting data.
WiFi AP activity	The LED lights when a client is connected to the router's Wi-Fi AP and flashes during communication.
WiFi STA activity	The LED lights when the router is connected to a remote Wi-Fi AP and flashes during communication.
OpenVPN activity	The LED lights when an OpenVPN tunnel is established and has received data.
IPsec active	The LED lights when an IPsec tunnel is established.
WireGuard activity	The LED lights when a WireGuard tunnel is established and has received data.
WebAccess/DMP active	The LED lights when the router is connected to a WebAccess/DMP server.

System

The *System* configuration menu contains settings that are common to the entire router system, such as authentication, identification, and automatic updates.

Authentication

The *Configuration → System → Authentication* page allows for the configuration of user authentication methods, password policies, and account lockout settings. The router can authenticate users against its local database or against external RADIUS or TACACS+ servers.



Authentication Configuration Page

General Settings

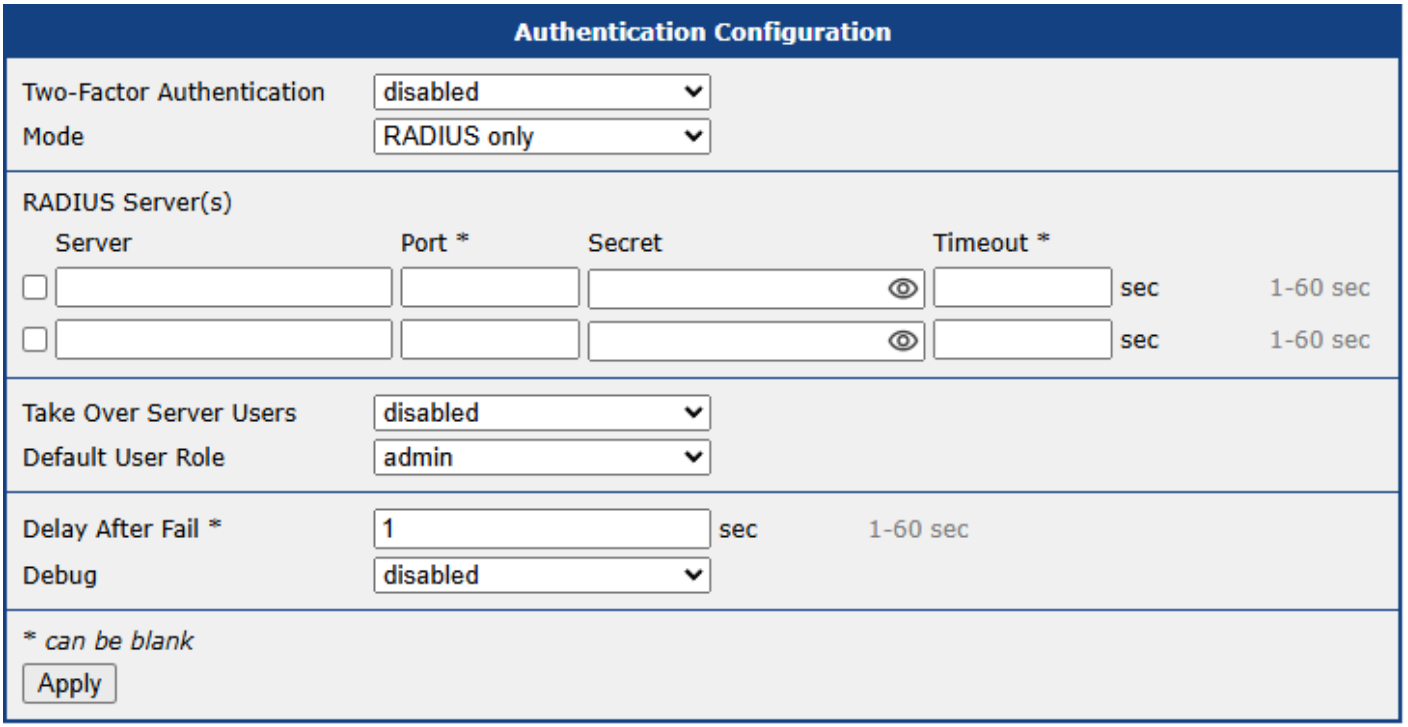
These settings are common across all authentication modes.

Item	Description
Two-Factor Authentication	Enables a second layer of security for user logins. Options include **Google Authenticator** or **OATH**.
Mode	Selects the primary authentication method: • **Local user database**: Authenticates against the router's local user list, refer to Manage Users. • **RADIUS with fallback**: Authenticates against a RADIUS server. If the server is unreachable, it falls back to the local database. • **RADIUS only**: Authenticates only against a RADIUS server. Caution: If the server is unreachable, login will be impossible. • **TACACS+ with fallback**: Authenticates against a TACACS+ server, with fallback to the local database. • **TACACS+ only**: Authenticates only against a TACACS+ server. Caution: If the server is unreachable, login will be impossible.
Lock Account After	The number of failed login attempts before an account is locked.
Count Fails For	The time window in seconds during which failed attempts are counted.

Item	Description
Unlock After	The duration in seconds after which a locked account is automatically unlocked.
Force Password Complexity	Enforces minimum password strength requirements. The four character classes are: uppercase letters (A–Z), lowercase letters (a–z), digits (0–9), and special characters (e.g., `!@#$+.`). • **Very Weak**: At least 6 characters; must not contain the username; must not be a palindrome. • **Weak**: At least 8 characters from at least 2 of the 4 classes; must not contain the username; must not be a palindrome. • **Good**: At least 12 characters from at least 3 of the 4 classes; no more than 3 identical consecutive characters; must not contain the username; must not be a palindrome. • **Strong**: At least 16 characters from all 4 classes; no more than 2 identical consecutive characters; must not contain the username; must not be a palindrome.
Expire Password After	The number of days until a user password expires, forcing a change on next login.
Delay After Fail	The time in seconds the login screen is disabled after a failed attempt.
Debug	Enables detailed authentication-related messages in the system log.

RADIUS Mode

To use RADIUS for authentication, select either *RADIUS with fallback* or *RADIUS only* and configure the server details.



RADIUS Configuration

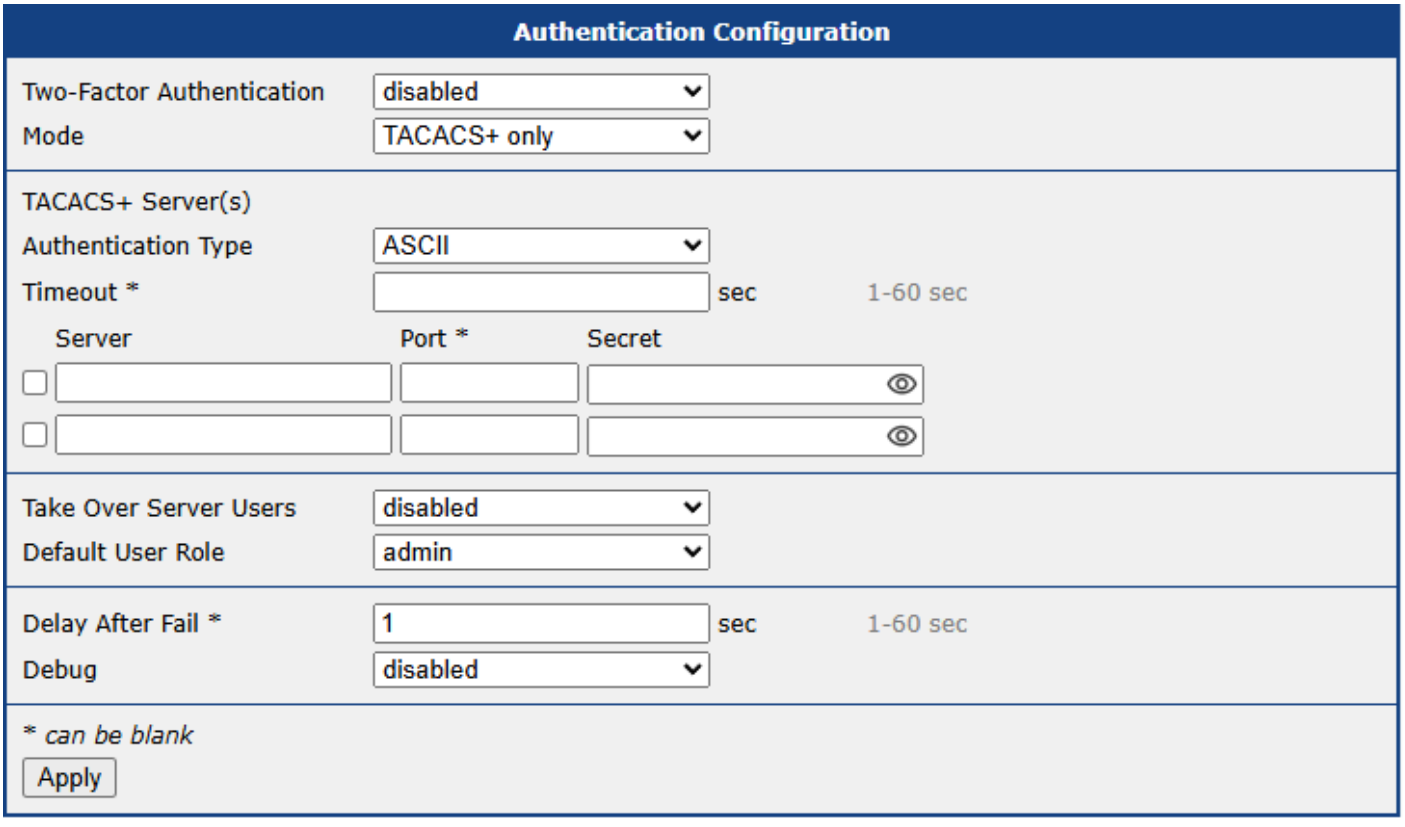
Warning

For a RADIUS user to log in, a corresponding user account must exist on the router locally. This account can be created manually (see Manage Users) or automatically by enabling the *Take Over Server Users* option.

Item	Description
Server	The IP address of the primary and optional secondary RADIUS server.
Port	The UDP port of the RADIUS server (default: 1812).
Secret	The shared secret used to encrypt communication with the RADIUS server.
Timeout	The time in seconds to wait for a response from the RADIUS server.
Take Over Server Users	When enabled, a local user account is created automatically upon successful RADIUS authentication if one does not already exist. The account is created without a password.
Default User Role	Assigns a default role (*Admin* or *User*) to users created via the *Take Over* feature, unless a role is provided by the RADIUS server via the *Service-Type* attribute: • **Administrative-User**: Assigns the *Admin* role. • **NAS-Prompt-User**: Assigns the *User* role.

TACACS+ Mode

To use TACACS+ for authentication, select either *TACACS+ with fallback* or *TACACS+ only* and configure the server details.



TACACS+ Configuration

Warning

As with RADIUS, a corresponding local user account is required for TACACS+ authentication. This account can be created manually or automatically with the *Take Over Server Users* option, as detailed in Manage Users.

Item	Description
Authentication Type	The authentication protocol to use: *ASCII*, *PAP*, or *CHAP*.
Timeout	The time in seconds to wait for a response from the TACACS+ server.
Server	The IP address of the primary and optional secondary TACACS+ server.
Port	The TCP port of the TACACS+ server (default: 49).
Secret	The shared secret used to encrypt communication with the TACACS+ server.
Take Over Server Users	When enabled, a local user account is created automatically upon successful TACACS+ authentication if one does not already exist. The account is created without a password.
Default User Role	Assigns a default role (*Admin* or *User*) to users created via the *Take Over* feature.

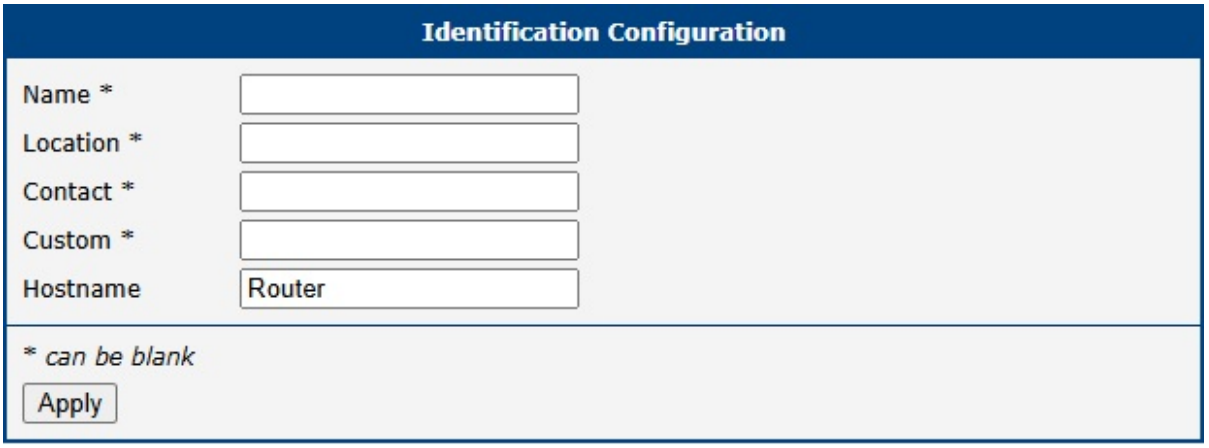
Identification

The *Configuration → System → Identification* page allows you to define several strings used to identify the router. These values serve multiple purposes:

- The *Name* and *Location* strings are displayed in the top-right corner of the web interface.
- The *Name*, *Location*, *Contact*, and *Custom* fields are exposed via SNMP for remote monitoring, as detailed in SNMP.

Info

Previously, these settings were located on the SNMP configuration page. They have been moved here to serve as a central point for router identification.

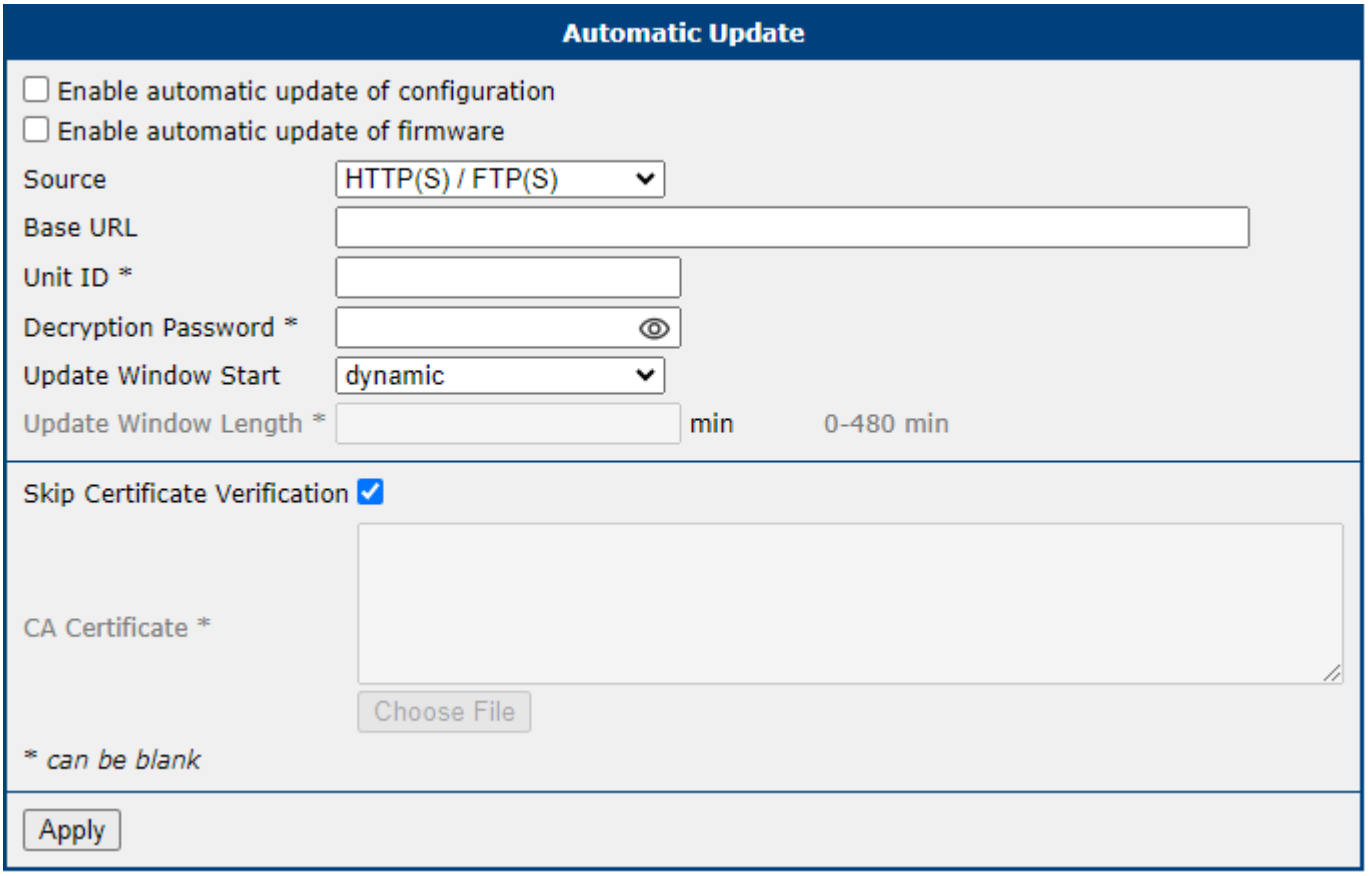


Identification Configuration Page

Item	Description
Name	A custom name for the router (e.g., "Main Office Gateway"). Also used as the SNMP System Name (sysName).
Location	The physical location of the router (e.g., "Server Room A"). Used as the SNMP System Location (sysLocation).
Contact	Contact information for the person responsible for the device (e.g., an email address or phone number). Used as the SNMP System Contact (sysContact).
Custom	A custom string for any additional information. Used as the SNMP infoCustom field.
Hostname	The hostname of the router, used to identify the device on the local network (e.g., in DHCP leases).

Automatic Update

The router can be configured to automatically download and apply firmware and configuration updates from a remote server or a local USB drive. This feature is essential for managing large-scale deployments and ensuring that devices are always up-to-date. The settings are located on the *Configuration → System → Automatic Update* page.



Automatic Update Configuration Page

Update Configuration

Item	Description
Enable automatic update of configuration	Enables the automatic update of the router's configuration file.
Enable automatic update of firmware	Enables the automatic update of the router's firmware.
Source	Specifies the location of the update files: • **HTTP(S)/FTP(S) server**: Updates are downloaded from the *Base URL*. The protocol (HTTP, HTTPS, FTP, or FTPS) is determined by the URL prefix. • **USB flash drive**: The router searches for update files in the root directory of a connected USB drive. • **Both**: The router checks both the remote server and a connected USB drive.
Base URL	The base URL of the remote server where update files are stored. The default protocol is HTTPS. To use a different protocol (HTTP, FTP, or FTPS), the prefix must be specified explicitly (e.g., `http://myupdateserver.com`).
Unit ID	A custom identifier used as the filename for the configuration file. If empty, the router defaults to using its ETH0 MAC address as the filename.
Decryption Password	The password required to decrypt an encrypted configuration file.
Update Window Start	The hour (1–24) when the daily update check should begin. If set to *dynamic*, the check runs five minutes after boot and every 24 hours thereafter.
Update Window Length	A duration in minutes defining a window of time, starting at the *Update Window Start*, during which the update is performed at a random moment. This helps distribute load on the update server in large deployments.
Skip Certificate Verification	When enabled, the router does not validate the SSL/TLS certificate of the remote HTTPS/FTPS server.
CA Certificate	The custom CA certificate used for server validation.

File Naming Conventions

The router looks for files with specific names on the update source. All files must be in a `tar.gz` archive.

- **Firmware**: The firmware filename is composed of the router model and a `.bin` extension (e.g., `icr-440x.bin`). The exact filename can be found on the *Administration → Update Firmware* page. A corresponding version file (`*.ver`) must also be present on the server.
- **Configuration**: The configuration filename is determined by the *Unit ID*. If specified, that value is used as the filename (e.g., `test.cfg`). If left blank, the router looks for a file named after its ETH0 MAC address, with colons replaced by dots (e.g., `00.11.22.33.44.55.cfg`).

Warning

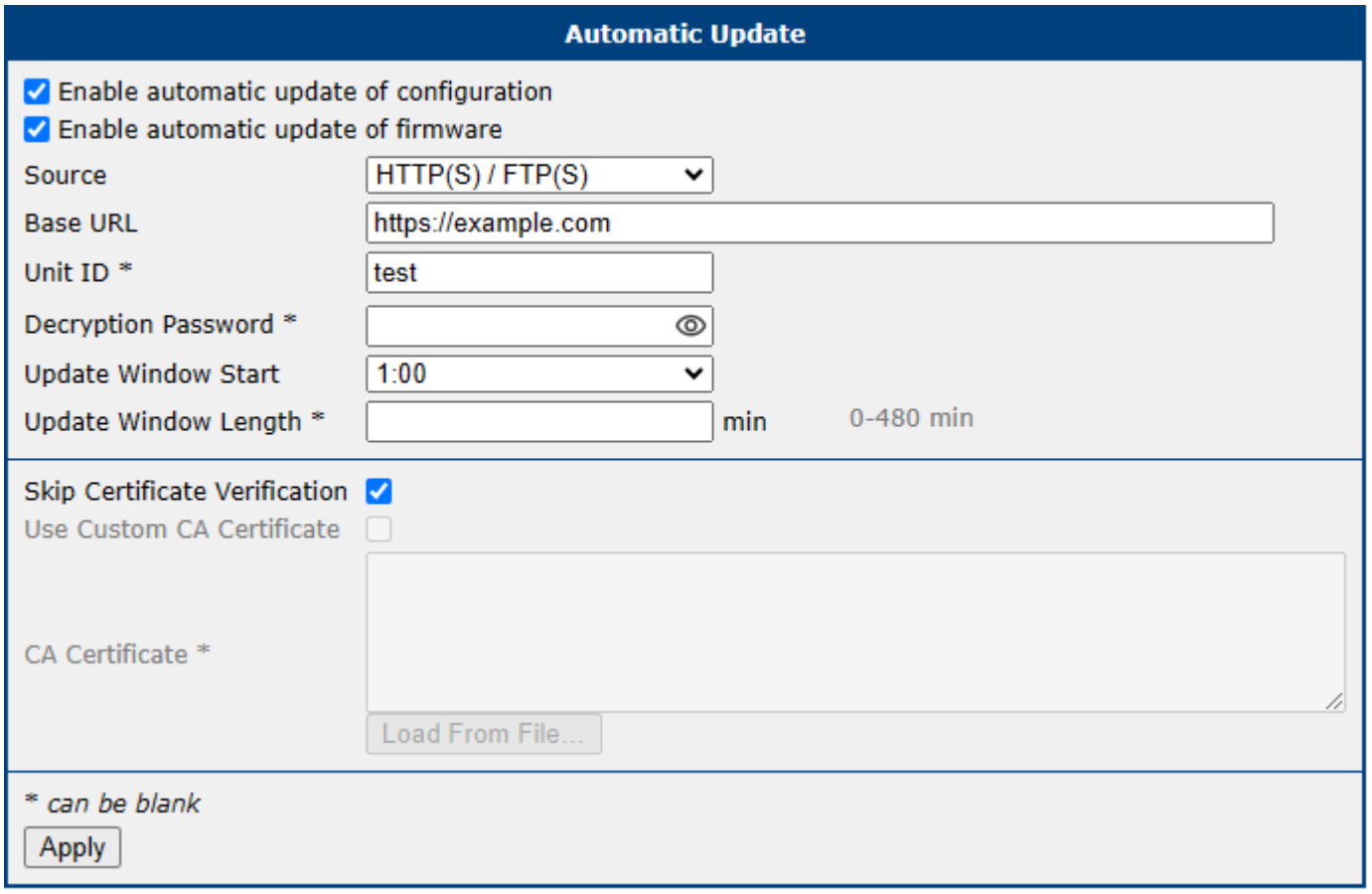
- Always upload both the `*.bin` and `*.ver` files to the server for firmware updates. If the `*.ver` file is missing and the server returns an incorrect success code, the router may enter a continuous download loop.
- Firmware updates may introduce incompatibilities with installed router apps. Always check the router app documentation for compatibility information and update router apps as needed.
- The automatic update process will always run five minutes after a manual firmware upgrade, regardless of the scheduled time.

Configuration Examples

Example 1: Scheduled Update

In this example, an ICR-4401 router is configured to check for a new firmware or configuration file daily at 1:00 AM from a specific URL.

- Firmware URL: `https://example.com/icr-440x.bin`
- Configuration URL: `https://example.com/test.cfg`

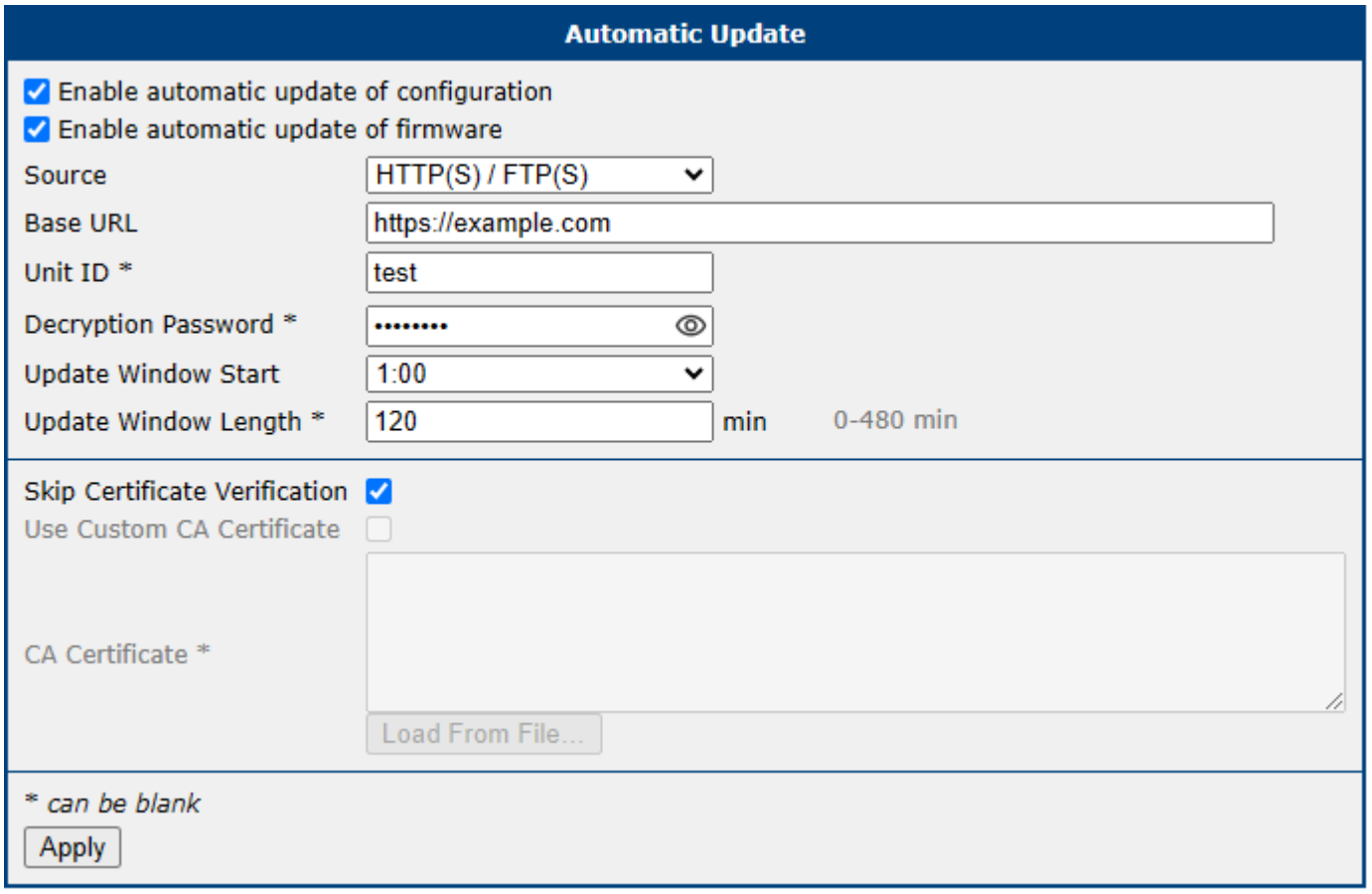


Example of a Scheduled Automatic Update

Example 2: Update Based on MAC Address with Encrypted Configuration

This example shows an ICR-4161 router configured to check for updates within a two-hour window. The configuration file is encrypted and identified by the router's MAC address.

- Firmware URL: `https://example.com/icr-416x.bin`
- Configuration URL: `https://example.com/00.11.22.33.44.55.cfg`



Example of an Automatic Update Using the MAC Address

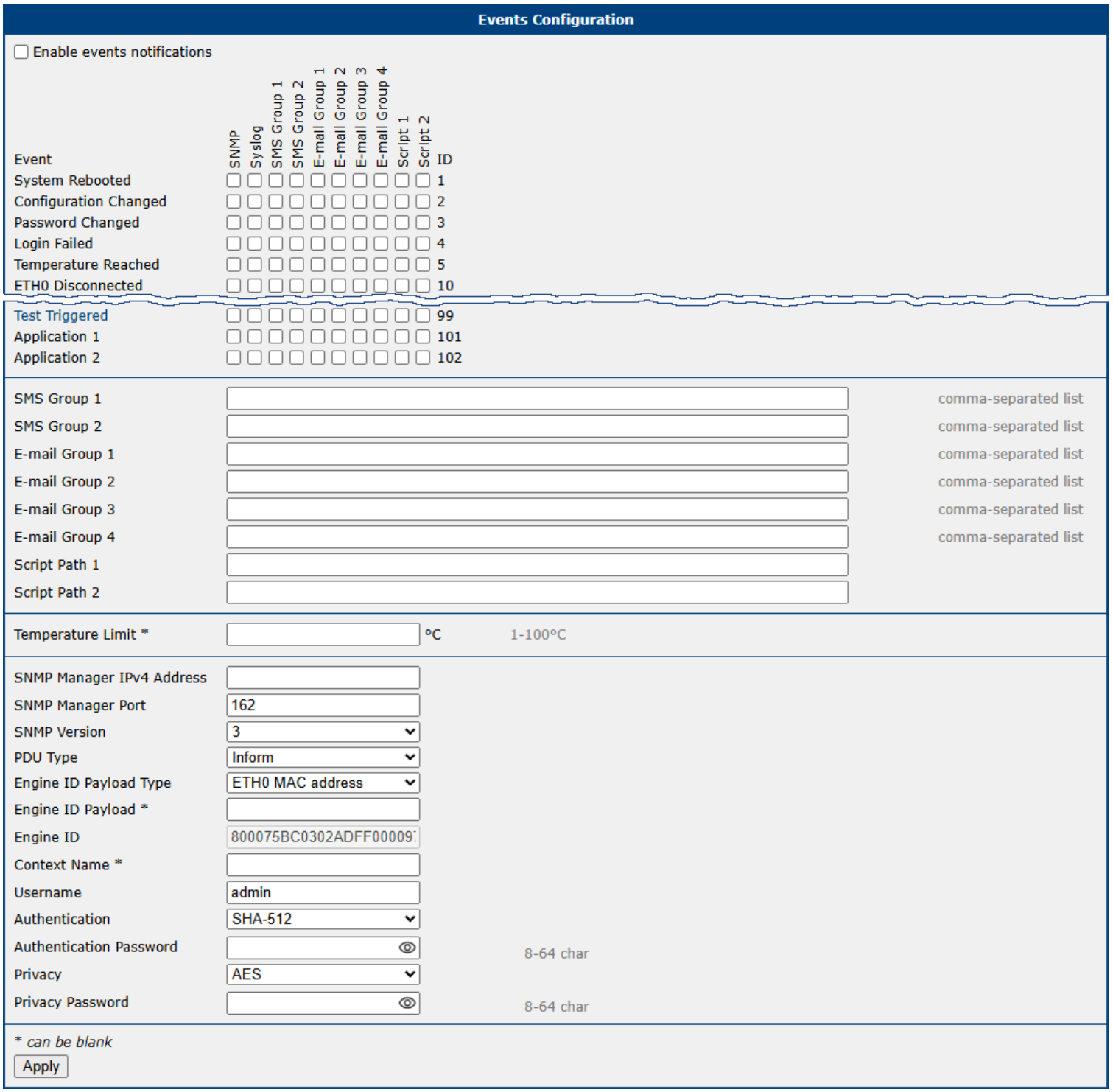
Events

Info

Starting with firmware version 6.6.0, this functionality replaces the legacy Event Notificator ↗ Router App. It is strongly recommended to use this built-in feature instead of the old Router App.

The *Configuration → Events* page provides a powerful system for triggering automated actions in response to specific system events. This feature allows you to create custom notifications and responses for monitoring the router's status and health.

To begin, check the *Enable events notifications* box at the top of the page.



Events configuration page

Event-Action Matrix

The core of this feature is the matrix, which links system events (rows) to specific actions (columns). When a particular event occurs, the router checks this matrix and executes all the actions that are checked in that event's row.

Event	Description
System Rebooted	Triggered when the router finishes its boot sequence.

Event	Description
Configuration Changed	Triggered whenever the router's configuration is modified and saved.
Password Changed	Triggered when a user password is changed.
Login Failed	Triggered after any unsuccessful login attempt to the router, either via the web interface or an SSH connection.
Temperature Reached	Triggered when the internal temperature exceeds the limit defined in the *Temperature Limit* field.
ETHx Disconnected	Triggered when the link on the corresponding Ethernet port is lost.
Test Triggered	A virtual event designed specifically for testing configured actions (e.g., to verify that an SMS or email is sent correctly). **Note:** Before testing, ensure that the event system is enabled, the desired actions are configured, and all settings are saved. The test can be triggered manually by clicking on the event name in the web interface.
Application 1/2	Custom events that can be triggered by user scripts or applications (IDs 101 and 102).

Action	Description
SNMP	Sends an SNMP trap to the defined SNMP manager.
Syslog	Writes a message to the system log.
SMS Group 1/2	Sends an SMS to all numbers in the specified SMS group.
E-mail Group 1–4	Sends an email to all addresses in the specified email group.
Script 1/2	Executes the user script located at the specified path.

Action Definitions

This section is where you define the details for each action.

Item	Description
SMS Group 1/2	A comma-separated list of phone numbers for the respective SMS action group.
E-mail Group 1–4	A comma-separated list of email addresses for the respective email action group.
Script Path 1/2	The absolute path to the user script to be executed (e.g., `/var/scripts/my_script.sh`).
Temperature Limit	The temperature threshold in degrees Celsius (°C) for the *Temperature Reached* event.

SNMP Settings

This section contains the specific settings for the *SNMP* trap action.

Item	Description
SNMP Manager IPv4 Address	The IP address of the server that will receive the SNMP traps.
SNMP Manager Port	The UDP port on which the SNMP manager is listening. The default is 162.
SNMP Version	The version of the SNMP protocol to use. Version 3 is recommended for enhanced security.
PDU Type	The type of Protocol Data Unit to send. *Inform* requires an acknowledgment from the manager, while *Trap* does not.
Community	For SNMPv2c only. A password-like credential used to authenticate communications. This string must exactly match the community string configured on the SNMP manager.
Engine ID Payload Type	Determines the source for generating the Engine ID. Options include the *ETH0 MAC address*, a custom *ASCII Text* string, or a custom *Hexadecimal Value*.
Engine ID Payload	If the Payload Type is set to ASCII or Hexadecimal, enter the custom value to be used for the Engine ID.
Engine ID	The final, unique identifier for the SNMP engine on this device, generated based on the settings above. This field is read-only.
Context Name	An identifier used to group related SNMP data, allowing for different logical subsets of managed objects.
Username	The username for SNMPv3 authentication.
Authentication	The hashing algorithm used for SNMPv3 message authentication (e.g., SHA-512).
Authentication Password	The password for SNMPv3 authentication.
Privacy	The encryption algorithm used for SNMPv3 message privacy (e.g., AES).
Privacy Password	The password for SNMPv3 privacy.

Scripts

The router provides several hooks for executing custom shell scripts in response to system and network events. This powerful feature allows for a high degree of automation and customization. The available script types are:

- **Startup Script**: Executed once every time the router boots up.
- **Up/Down IPv4 Scripts**: Executed when the primary IPv4 WAN connection is established or lost.
- **Up/Down IPv6 Scripts**: Executed when the primary IPv6 WAN connection is established or lost.

For detailed information about available commands, refer to the *Command Line Interface* application guide. For broader guidance on customization, see the *Extending Router Functionality* ↗ application guide.

Startup

The *Startup Script* is ideal for tasks that need to run once at boot, such as initializing custom services, performing configuration checks, or launching background monitoring processes. The script is entered into the text area on the *Configuration → Scripts* page and saved by clicking the *Apply* button.

> **Warning**
>
> Changes to the startup script only take effect after the router is rebooted.

Script Example

The following script sends an SMS message upon router startup.

```bash
#!/bin/sh

# Define variables
PhoneNumber="+420123456789"
Message="Router has successfully started up."

# Send the SMS
sms "$PhoneNumber" "$Message"

exit 0
```

Up/Down IPv4

The *Up/Down IPv4* page allows you to define scripts that are triggered by changes in the primary WAN IPv4 connection state. The "Up" script runs when the IPv4 connection is established, and the "Down" script runs when it is lost. Because the router has a dual-stack implementation, scripts for IPv4 and IPv6 are configured and triggered independently.

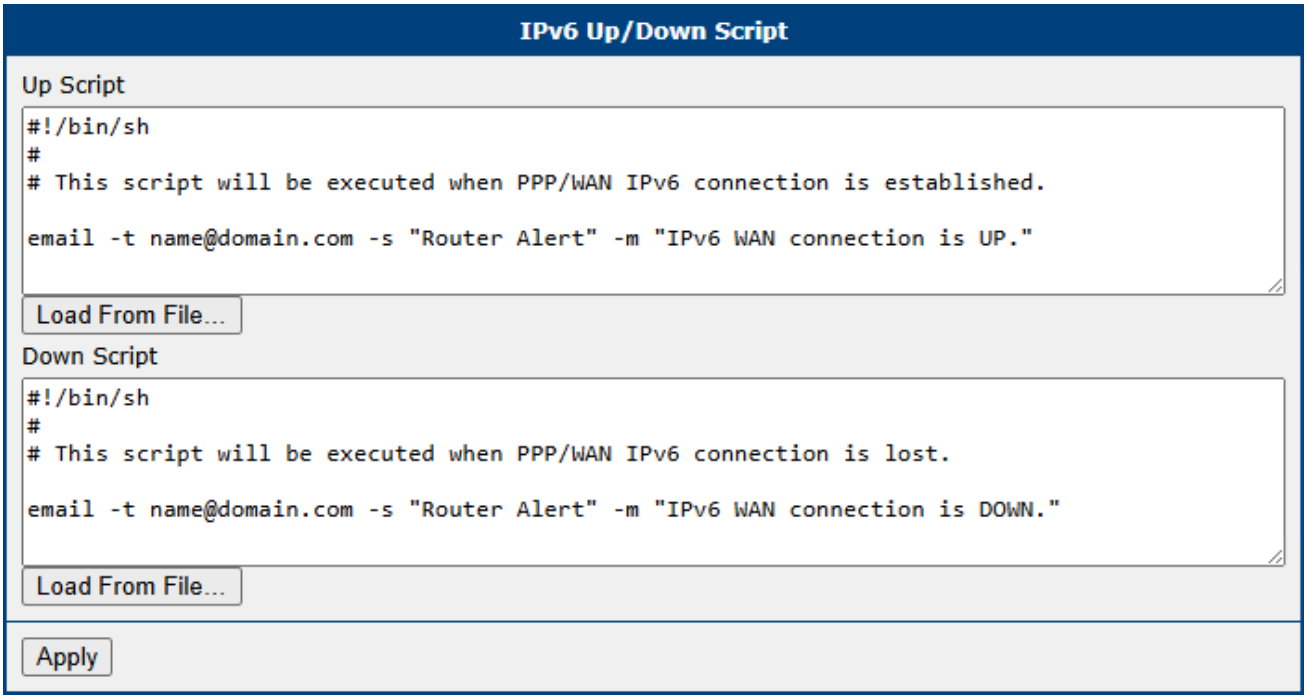
These scripts are passed several arguments that provide context about the connection, such as the interface name and assigned IP address. This allows for dynamic actions based on the current network status.

Up/Down IPv6

The *Up/Down IPv6* page serves a purpose similar to that of the IPv4 page, but it is specifically intended for IPv6 connections.

Script Example

This example uses the IPv6 Up/Down scripts to send an email notification whenever the IPv6 WAN connection status changes. The *SMTP* service must be configured beforehand.



IPv6 Up/Down Script Configuration Page

Up Script:

```
email -t name@domain.com -s "Router Alert" -m "IPv6 WAN connection is UP."
```

Down Script:

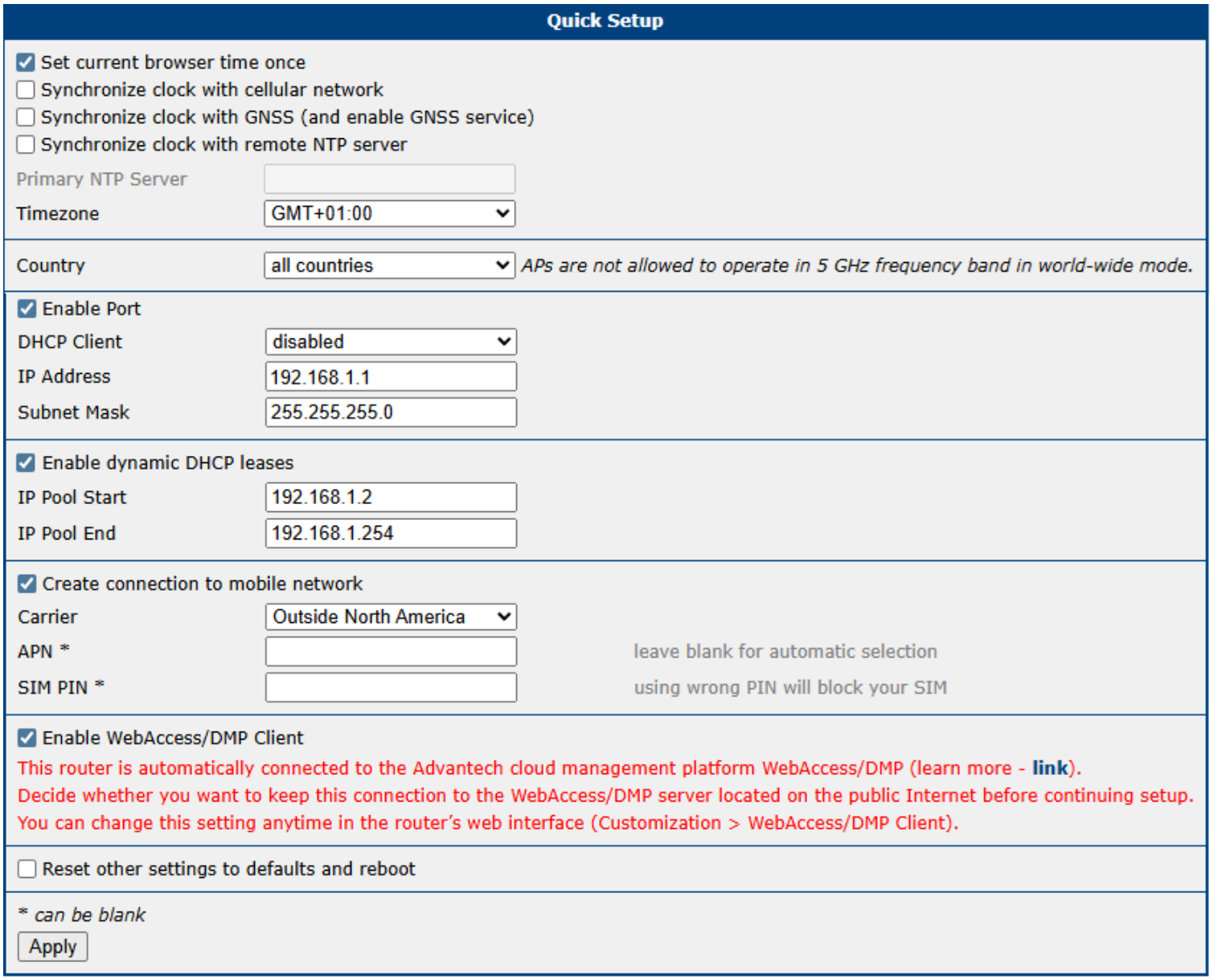
```
email -t name@domain.com -s "Router Alert" -m "IPv6 WAN connection is DOWN."
```

> **Warning**
>
> After saving an Up/Down script, the router must be rebooted for the changes to become active.

Quick Setup

The *Quick Setup* page provides a streamlined, single-page interface that gathers all of the most critical settings for the initial configuration of the router. This page is automatically displayed upon the first login to a new or factory-reset device, but it can also be accessed manually at any time via *Configuration → Quick Setup*.

This wizard conveniently consolidates essential settings from various sections of the web interface, allowing you to configure time, LAN, and mobile network settings from a single page.



Quick Setup page

Time and Region

For a complete overview of these settings, refer to NTP and WiFi Country. To set the date and time manually, see the Set Date and Time administration page.

Item	Description
Set current browser time once	A one-time action that sets the router's system time to match the time of your web browser.
Synchronize clock with...	Selects the method for automatic time synchronization. Note that synchronization via GNSS is only available on router models equipped with a GNSS module.
Primary NTP Server	The address of the NTP server to use when *Synchronize clock with remote NTP server* is selected.
Timezone	Sets the local timezone for the router.

Item	Description
Country	For models equipped with Wi-Fi, this setting configures the regulatory domain. Select the country of operation to ensure compliance with local radio frequency regulations, as this affects which Wi-Fi channels are available.

LAN Port and DHCP Server

The full configuration options for the LAN interface are described in Ethernet.

Item	Description
Enable Port	Enables or disables the primary LAN port (`eth0`).
DHCP Client	If enabled, the router's LAN port requests an IP address from another DHCP server on the network.
IP Address	The static IPv4 address assigned to the router's primary LAN interface.
Subnet Mask	The subnet mask for the primary LAN interface.
Enable dynamic DHCP leases	Enables the router's built-in DHCP server, which automatically assigns IPv4 addresses to client devices on the LAN.
IP Pool Start	The starting address of the IP range that the DHCP server leases to clients.
IP Pool End	The ending address of the IP range that the DHCP server leases to clients.

Mobile Network

> **Info**
>
> This section is only available on cellular router models.

The complete configuration for the mobile network is available in Mobile WAN.

Item	Description
Create connection to mobile network	When checked, the router automatically attempts to connect to the mobile network after booting.
Carrier	Allows the selection of a pre-defined profile for a specific mobile carrier (e.g., for North American operators).
APN	The Access Point Name for your mobile network data plan. In many cases, this can be left blank to allow for automatic selection by the carrier.
SIM PIN	The PIN for your SIM card. Entering an incorrect PIN multiple times may permanently block the SIM card.

System and Service Settings

Item	Description
Enable WebAccess/DMP Client	Enables or disables the client for the WebAccess/DMP remote management platform. For complete details, see Remote Management Platform.
Reset other settings to defaults and reboot	If checked, any settings not present on this Quick Setup page are reset to their factory defaults when the new configuration is applied.

Customization Pages

Router Apps

> **Info**
>
> - Users with the *Admin* role can install, manage, and view Router Apps. Users with the *User* role can only view the list of installed apps.
> - To quickly check the operational state of all installed apps without entering their configuration, navigate to *Status → Router Apps*.

Router Apps (RA), formerly known as *User Modules*, are custom software packages that extend the router's capabilities in areas such as security, advanced networking, and custom services.

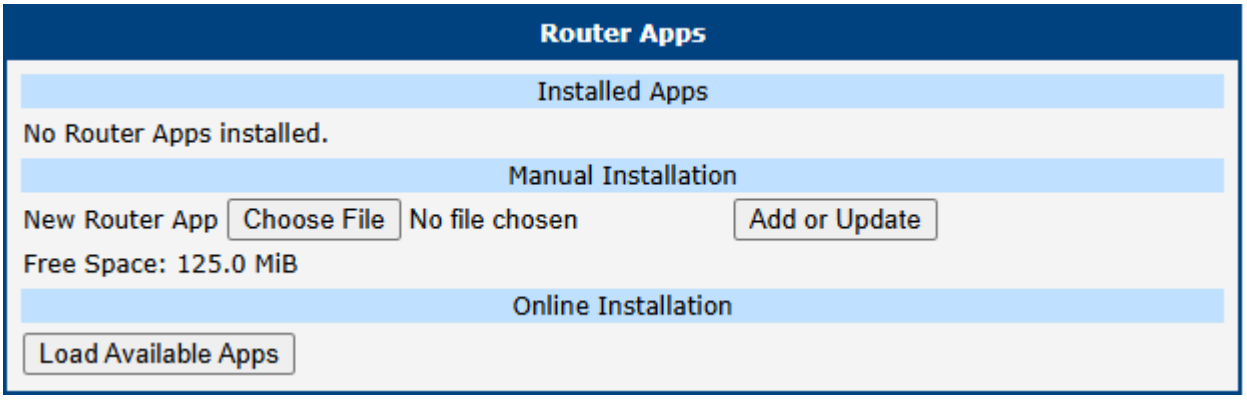
A wide variety of Router Apps are available for free on the Advantech *Router Apps* ↗ page.

Overview of the Router Apps Page

To manage apps, navigate to *Customization → Router Apps*. The page is divided into three main areas:

- **Installed Apps**: Lists all Router Apps currently installed on the device.
- **Manual Installation**: Allows for uploading and installing an app package from your computer.
- **Online Installation**: Allows for downloading and installing apps directly from a server.

The *Free Space* indicator shows how much storage is available for new applications.



Default Router Apps Page

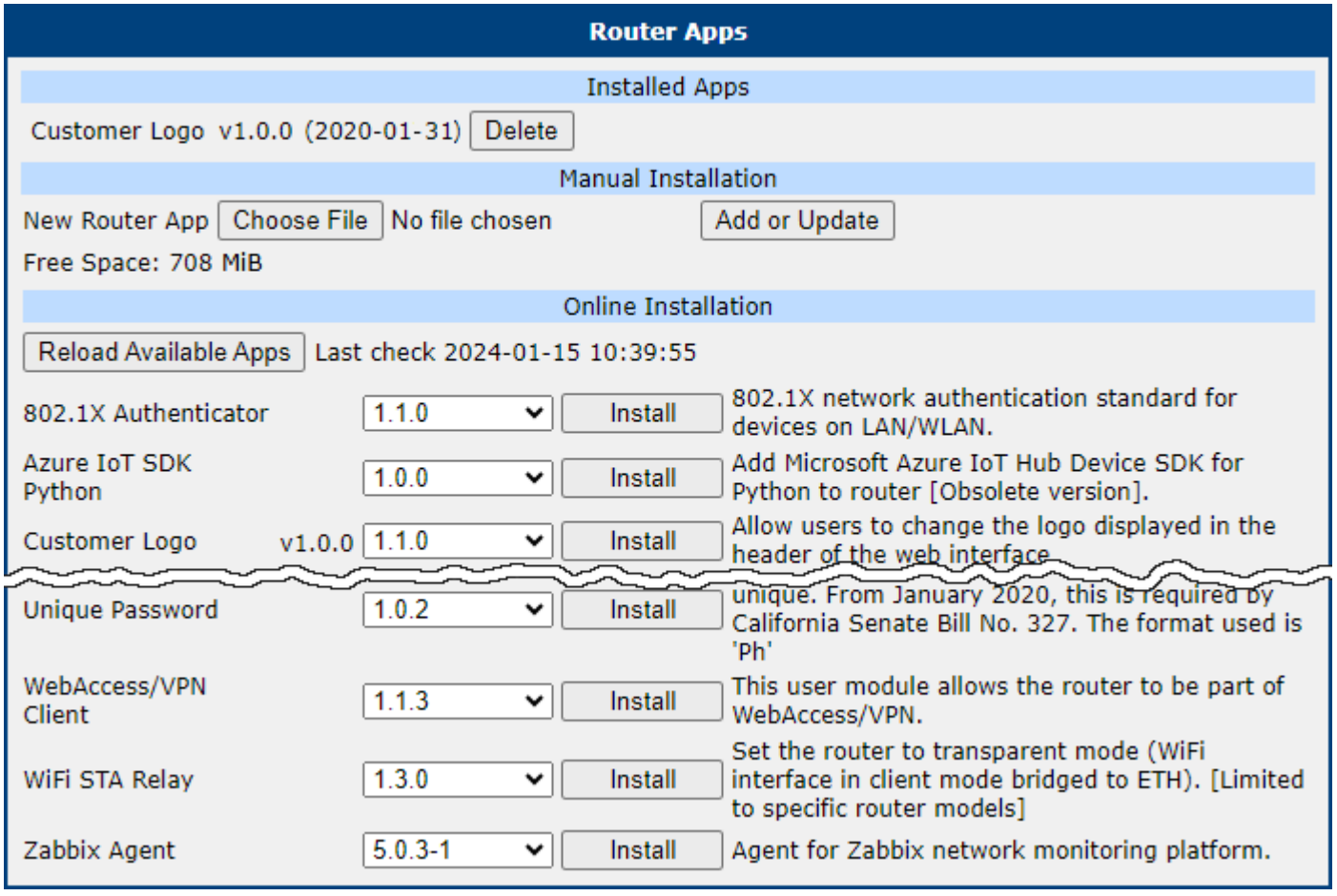
Manual Installation

To install a Router App manually, click the *Choose File* button in the *Manual Installation* section to select the app package from your computer. The package must be a `*.tgz` file. Click the *Add or Update* button to begin the installation.

Online Installation

To install apps from a server, first click the *Load Available Apps* button in the *Online Installation* section. This action fetches and displays a list of all applications available on the configured server.

- An active internet connection with functional DNS name resolution is required. Without it, the router cannot find the server, which will result in a `Couldn't resolve host name` error.
- By default, the router is configured to use the public Advantech server. A custom server can be specified on the Settings page. Note that the *Load Available Apps* button is disabled if server communication is deactivated in the settings.
- The list of available apps is not stored permanently; it is cleared when the router reboots and must be reloaded. The timestamp of the last successful list update is shown next to the button.
- This online installation feature requires firmware version 6.4.0 or newer and is not available on v2 platform routers.



Router Apps Page with Online Apps Loaded

Managing Installed Apps

All installed apps are listed in the *Installed Apps* section.

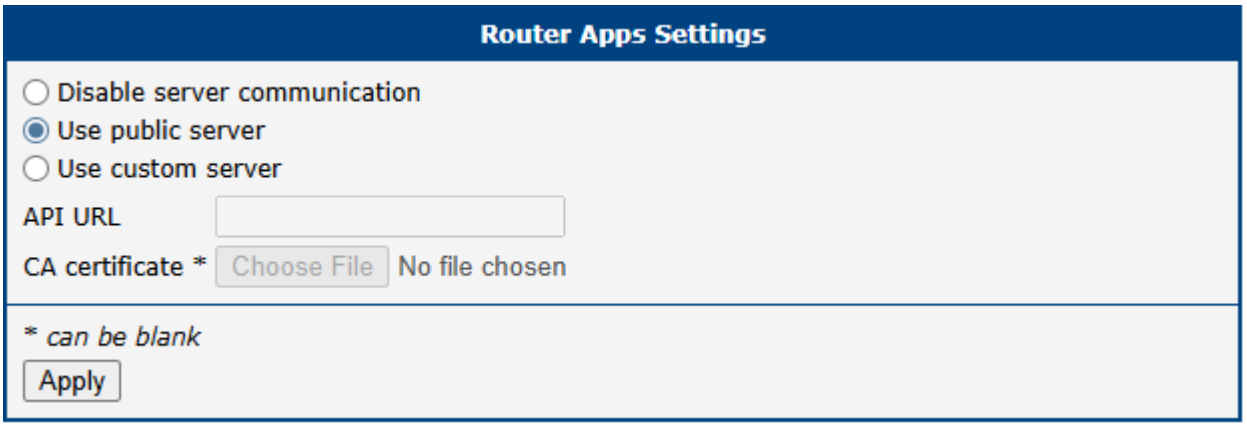
- **Accessing an App GUI**: If an app has a web interface, its name is a clickable link that opens the app's GUI.
- **Removing an App**: To uninstall an app, click the corresponding *Delete* button.

Info

For information on creating your own Router Apps, refer to the Programming of Router Apps ↗ chapter of the *Extending Router Functionality* application guide.

Settings

To configure the server connection for online installation, navigate to *Customization → Router Apps → Settings*.



Router Apps Server Settings

Item	Description
Disable server communication	Check this to disable all communication with the online app server.
Use public server	The default option. Uses the official Advantech server to download Router Apps. Requires an active internet connection.
Use custom server	Connect to a private, self-hosted server. **This requires an on-premises installation of Advantech's *WebAccess/DMP* ↗ software.**
API URL	The URL of your custom server. Must begin with `https://`.
CA certificate	Upload a CA certificate for your custom server if it uses a private or non-standard Certificate Authority.

Administration Pages

Manage Users

This chapter provides a comprehensive guide to user management on the router. It explains the differences between user roles and details how to create, modify, and delete accounts. Additionally, it covers the configuration of advanced security features such as Two-Factor Authentication (2FA) and passwordless SSH login.

The primary administration page is *Administration → Manage Users*, which is fully accessible to users with the *Admin* role. Users with the standard *User* role have restricted access and can only modify their own settings via the separate *Administration → Modify User* page; refer to Modify User.

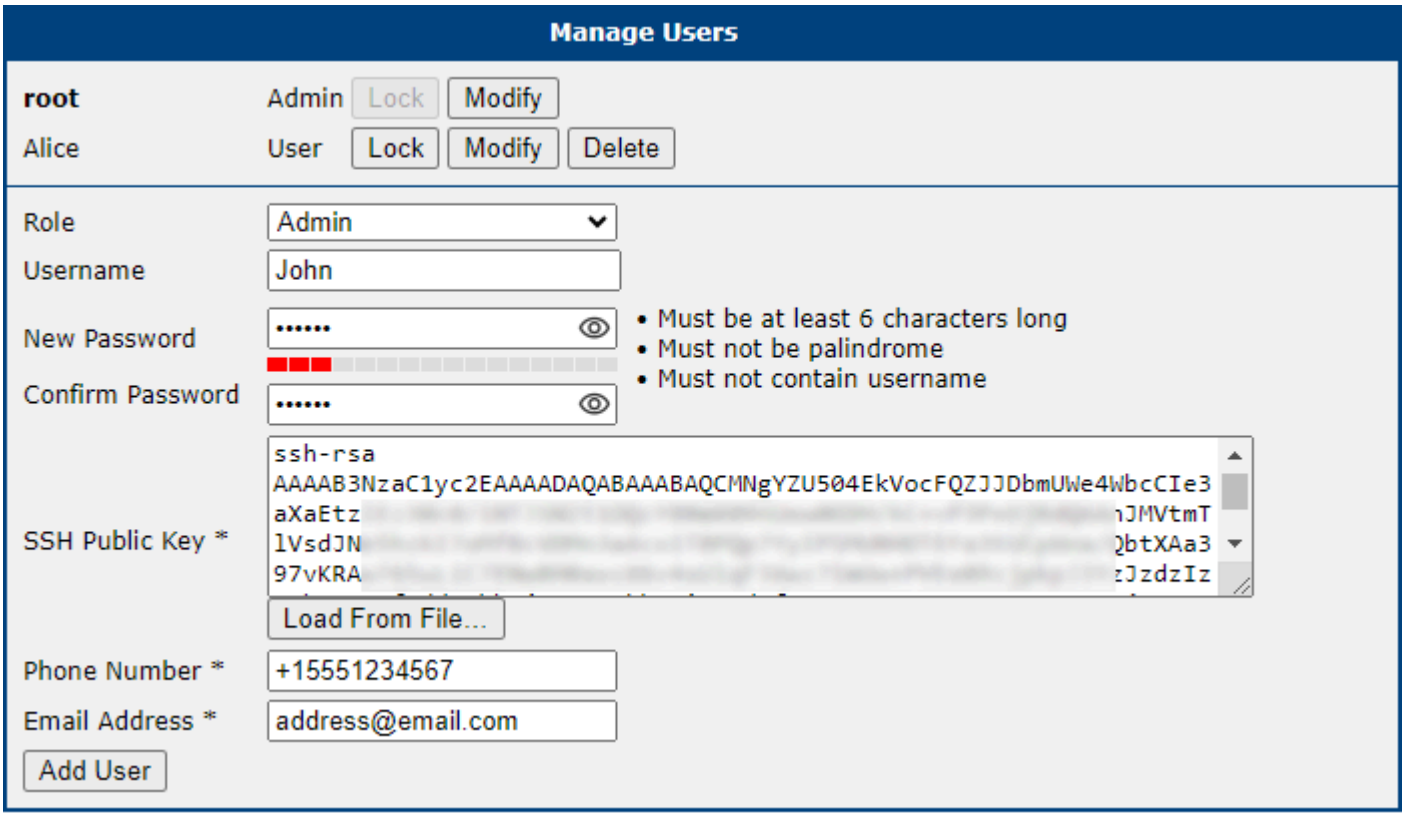
Warning

Be careful not to lock out or delete all users with the *Admin* role. If this happens, no user will have the necessary permissions to manage accounts, and a factory reset may be required.

Info

- The main *Manage Users* page is only accessible to users with the *Admin* role.
- For global authentication settings, such as enabling 2FA services and setting password complexity rules, refer to Authentication.

The *Manage Users* page is the central hub for creating, modifying, and deleting user accounts on the router. In the figure below, you can see that there are two existing users, `root` and `Alice`, and we are about to add a new user named `John` with the *Admin* role.



Manage Users Configuration Page

User Roles and Permissions

The router supports two primary user roles, each with a different level of permissions:

- **User Role**: Intended for basic monitoring. Users with this role have read-only access to most of the web interface and cannot make configuration changes (except for modifying their own account). Console access is disabled.
- **Admin Role**: Intended for full device management. Administrators have full read-write access to the entire web interface and can log in via the console. However, this is not equivalent to the `root` superuser on a standard Linux system.

> **Info**
>
> In addition to the primary roles, the system includes a highly restricted **Operator Role**. Users with this role can only log in and change their own password, with no other capabilities or access to the web interface. This role is intended solely for special-purpose Router Apps and future high-granularity access rights configurations.

Adding, Modifying, and Deleting Users

The main part of the page lists all existing users. For each user, you have three available actions:

Button	Description
Lock	Temporarily disables the user account, preventing login via both the web interface and the console.

Button	Description
Modify	Opens the *Modify User* page, allowing you to change the password, update contact information, or manage security settings like the SSH public key and 2FA; refer to Modify User.
Delete	Permanently removes the user account from the router.

To create a new account, fill out the form shown in the figure above and click the *Add User* button.

Item	Description
Role	Assigns the user role. Available options are *Admin*, *User*, and the highly restricted *Operator* role.
Username	The name for the new user account.
New Password	Sets the password for the user. It must always comply with the rules defined by the *Force Password Complexity* setting (see Authentication). When changing a password for an existing user, the new password is also checked against the previous password and must meet these additional requirements: • **Character Difference**: Must differ from the old password by at least 1 character (*Very Weak* / *Weak* levels) or at least 5 characters (*Good* / *Strong* levels). • **No Trivial Variations**: Changing only the case of letters or cyclically shifting characters is not allowed.
Confirm Password	Re-enter the new password to confirm it. This helps prevent typos.
Public key	Paste a public SSH key here to enable passwordless console login for this user. The maximum supported size is 16 KiB. Refer to Passwordless Console Login for a detailed guide.
Phone Number	The user's mobile phone number. If provided, an SMS notification will be sent to this number whenever the user's password is changed. **Note:** This feature is only available on cellular router models.
Email Address	The user's email address. If provided, an email notification will be sent to this address whenever the user's password is changed. **Note:** This feature requires a functional SMTP server configuration.

Two-Factor Authentication

Caution

- **Correct time is crucial:** Two-factor authentication is time-based. Ensure the router's clock is always accurate by enabling the NTP client; see NTP.
- **Risk of lockout:** An incorrect 2FA setup can lock you out of your account. It is highly recommended to have a separate admin account without 2FA as a backup during the setup process.
- **Secret key is vital:** Without the secret key, you cannot complete the setup or log in. A user with the *Admin* role cannot retrieve a secret key for another user; they can only delete it.
- **Secret key deletion:** If a user is unable to log in using 2FA for any reason, a user with the *Admin* role can delete their secret key, thereby disabling 2FA for that user.

> **Tips**
>
> A user with the *Admin* role cannot generate or upload the secret key for another user; they can only delete the key.

If you have enabled one of the two-factor authentication services, as mentioned above, you should see the chosen service name in the *Two-Factor Auth* field, as shown in the figure above.

A secret key is required to activate the two-factor authentication. You can generate this key by choosing the *Generate a new secret key* option. You can upload the user's secret key from a file using *Upload a new secret key*. Clicking the *Apply* button the secret key will be saved. Next, click the *Show* button, located to the right of the secret key, the secret key will be shown. If the secret key is defined, a QR code will appear on the right, allowing you to easily add this key to the chosen authentication application by scanning it.

Implementation Notes

- Two different two-factor implementations are supported:
  - Google Authenticator ↗
  - OATH Toolkit ↗
- Implemented for the following services only:
  - The router's web server login
  - SSH login
  - TELNET login
- Two-factor authentication is disabled by default
- Two-factor authentication data are backed up/restored during user backup/restore
- All private two-factor authentication data are removed when the corresponding user is deleted
- No internet or mobile connection is required to use two-factor authentication, but keep in mind the need to synchronize the system time

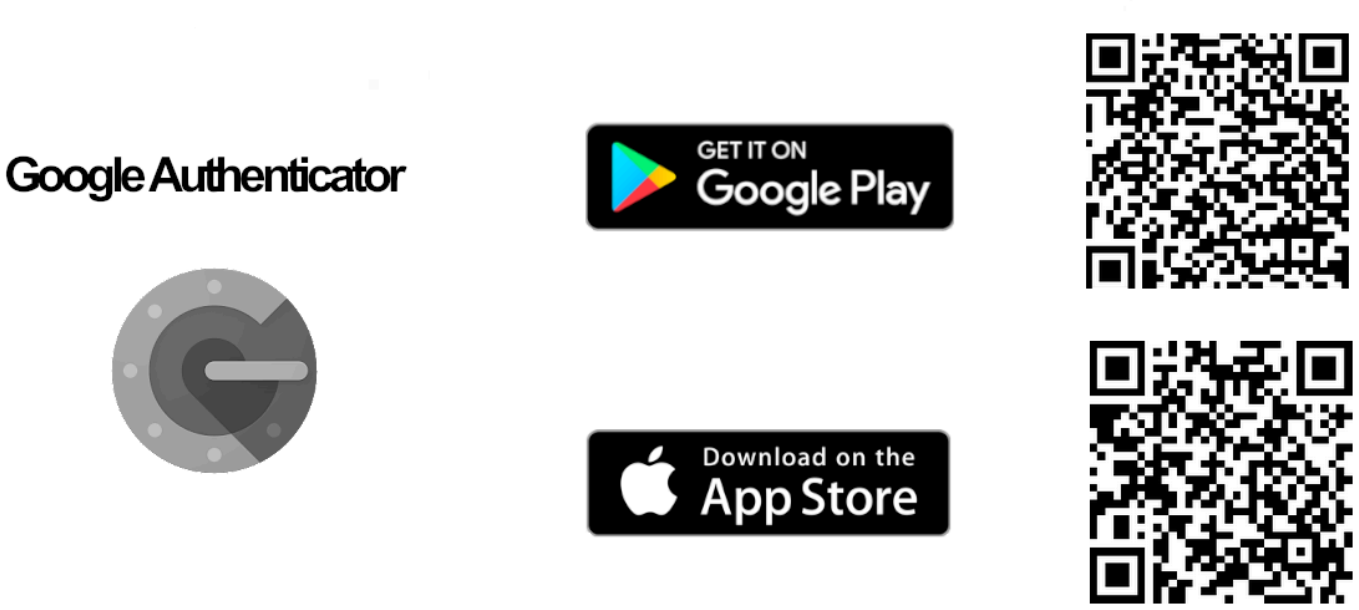
Configuration Steps

1. Enable the two-factor authentication service as described in the Authentication.
2. Enable the two-factor authentication for a user as described in the Modify User section.
3. Use an application or service to perform the two-factor authentication to the router as described in the following section.

Authenticator

To log in with two-factor authentication, you need an Authenticator application. Both *Google Authenticator* and *OATH* use TOTP (Time-based One-Time Password, RFC 6238 ↗) mode by default. You can use any compatible authenticator. For information about authenticator usage, see the corresponding manual.

You can use the Google Authenticator ↗ application; see the figure below for the download links.



Links for Google Authenticator Application

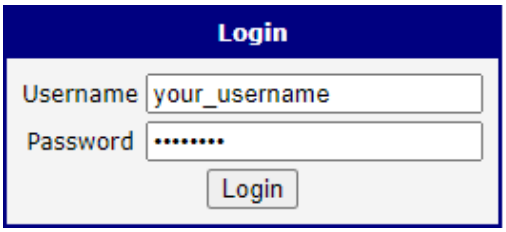
Authenticator-Extension ↗ is available as an extension for all popular browsers; see the figure below for the download links.

Links for Authenticator-Extension

In an Authenticator application, you can create a new entry by entering the secret key you have noted down or by scanning the QR code shown for the user on the *Modify User* configuration page.

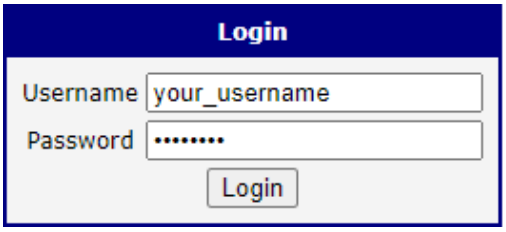
Router Web Login

When logging into the router's web interface, enter the *Username* and *Password* as you would for a standard login; see the figure below.



Standard Login

Next, you will be prompted to enter the Verification Code; see the figure below. This code is obtained from your Authenticator. Note that there is a **limited time** for code usage, typically within five minutes, assuming the system time is correct.

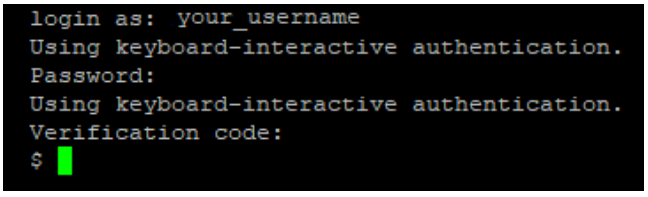


Verification Code

After entering the correct code, you will be successfully logged in to the router's web interface.

SSH and Telnet Login

Logging into SSH and Telnet with two-factor authentication is similar. Enter your username, password, and the generated verification code. For an example of SSH login, see the figure below.



SSH Login

Passwordless Console Login

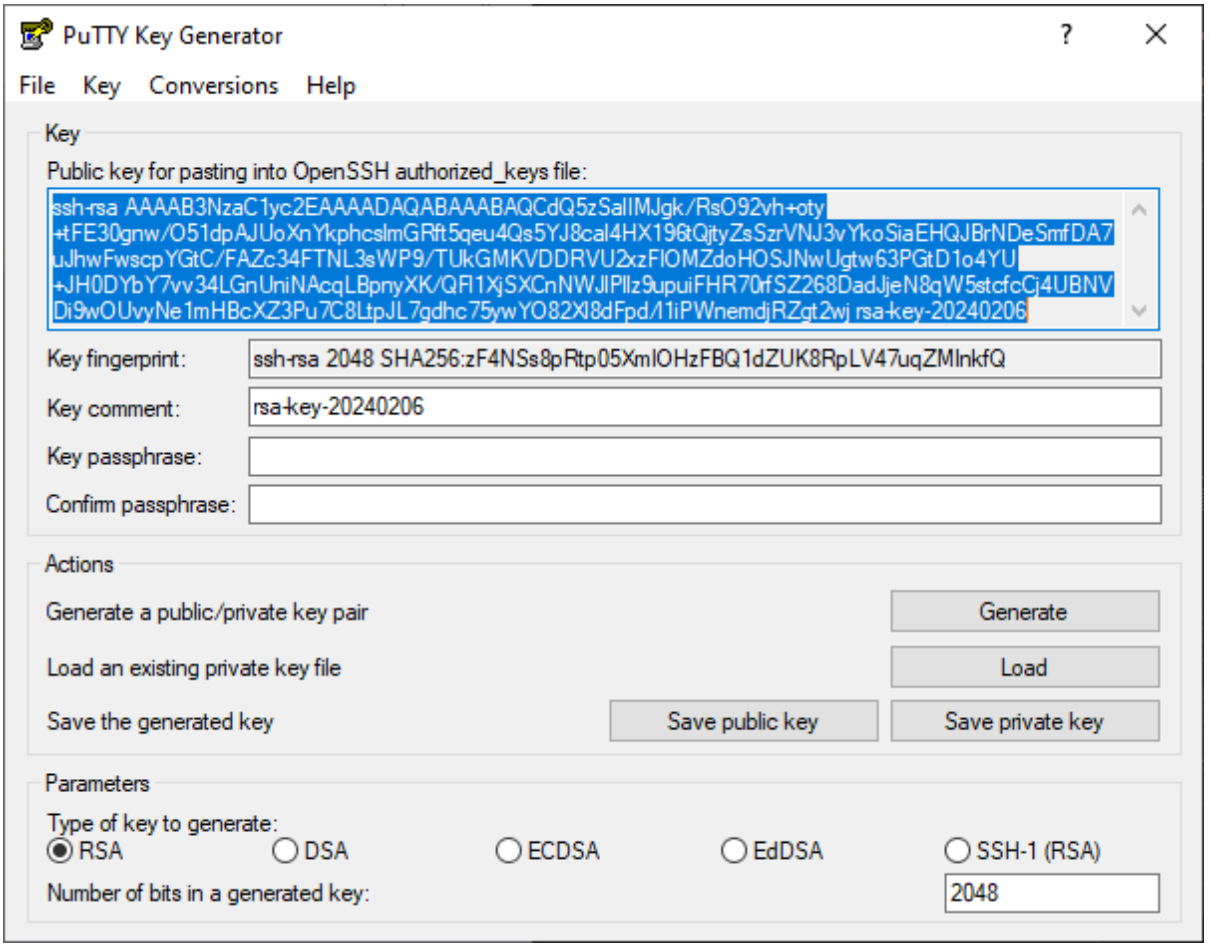
You can log in to SSH without a password using an SSH Public Key. This chapter demonstrates the key generation and connection process using *PuTTY*, a free terminal emulator for Windows OS available at *PuTTY* ↗.

Installation Notes

- For simplicity, this guide details a manual installation of PuTTY to the directory `C:\bin`, instead of using an `.msi` installation package.
- From the PuTTY application *download page* ↗, locate the *Alternative binary files* section and download `putty.exe`, `puttygen.exe`, and `pageant.exe`. The 64-bit x86 version is generally recommended. This guide uses *PuTTY* version 0.80. Save these files to the `C:\bin` directory.

Generate Keys

- Run the downloaded `puttygen.exe` application to create your SSH key, as shown in the figure below.
- Ensure the *RSA* option is selected.
- Click the *Generate* button. Move your mouse randomly within the window to generate the keys.
- Once complete, the key data will appear in the window.



Key Generation

- Click both *Save public key* and *Save private key* buttons to save these keys on your computer:
  - Name the public key *hostpublickey* and the private key *hostprivatekey*. **Do not** manually add any file extensions.
  - If prompted about a passphrase, click *Yes* to save without a passphrase. Using a passphrase adds security, but this guide proceeds without one for simplicity.
- Leave the *PuTTY Key Generator* application open.

Uploading Public Key to the Router

- In the router GUI (*Administration -> Manage Users*), click the *Modify* button for the user to whom you want to add the public key. Ensure the user has the *Admin* role; SSH login is not permitted for users with the *User* role.
- Enter the generated public key for the user:

    - In the *PuTTY Key Generator*, select the entire public key (the data within the text box) and copy it to the clipboard.
    - In the router GUI, paste the key into the *SSH Public Key* field.
    - It is important that the key **starts with "ssh-rsa "** followed by the key itself. If the key is not properly recognized, the SSH login will fail.
- Save the user settings by clicking the *Apply* button.
- You can now close the *PuTTY Key Generator* application.

> **Caution**
>
> If you have a public key generated previously and want to copy it to the router, the easiest way is to open the key file in the *PuTTY Key Generator* application and copy it from there. If you attempt to copy it directly from a file or from the GUI of another router, the key may not be in the correct format, and authentication will fail.

PuTTY Session Configuration

- Open the `c:\bin\putty.exe` application.
- In the configuration window, navigate to *Connection -> Data* and enter the username (the router's user to whom the public key was saved) in the *Auto-login username* field.
- Under *Connection -> SSH -> Auth -> Credentials*, click the *Browse* button near the *Private key file for authentication* field, and select your *hostprivatekey* file generated earlier.
- In the configuration window, navigate to the *Session* menu item and configure the following:
    - *Host Name*: IP address of your router.
    - *Port*: 22.
    - *Connection Type*: SSH.
    - *Saved Session*: Enter a name for this session.
    - Click *Save* to store these session settings.

Connecting to the Router

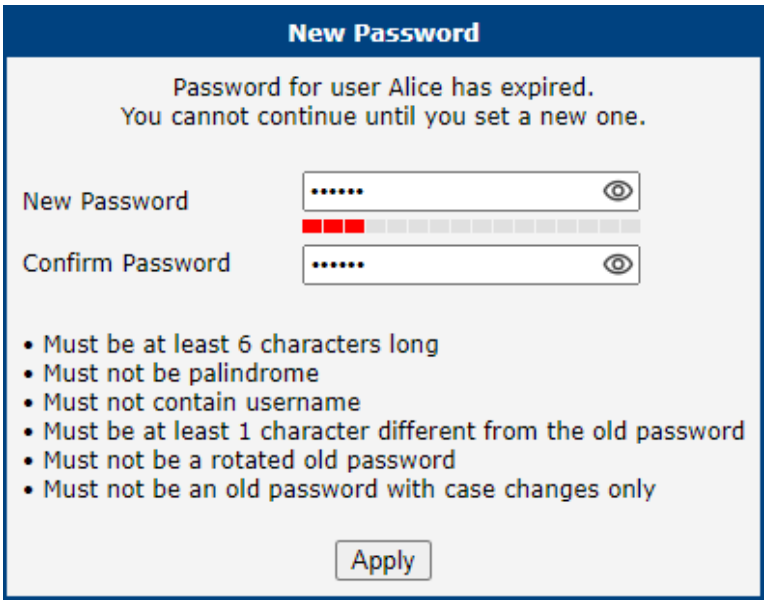
- Open the `c:\bin\putty.exe` application.
- Select your session and click the *Load* button.
- Click *Open* to establish the connection.
- If everything is configured correctly, an SSH console prompt will open with the user automatically logged in.

Forced Password Change

If a user is required to change their password, the prompt appears upon login, whether accessing the system via the web interface or the console environment. The password change is required in the following situations:

- When logging into a new router for the first time.
- When the user's password has expired after the *Expire Password After* period; see Authentication.
- When an *Admin*-role user has forcefully changed the password.
- When a *Configuration Reset* or *Factory Reset* is performed on the router; see Reset.

The dialog for entering a new password is shown in figure below. The new password must comply with the rules stated in the GUI, which depend on the *Force Password Complexity* level set in *Configuration → System → Authentication*, as described in Authentication.



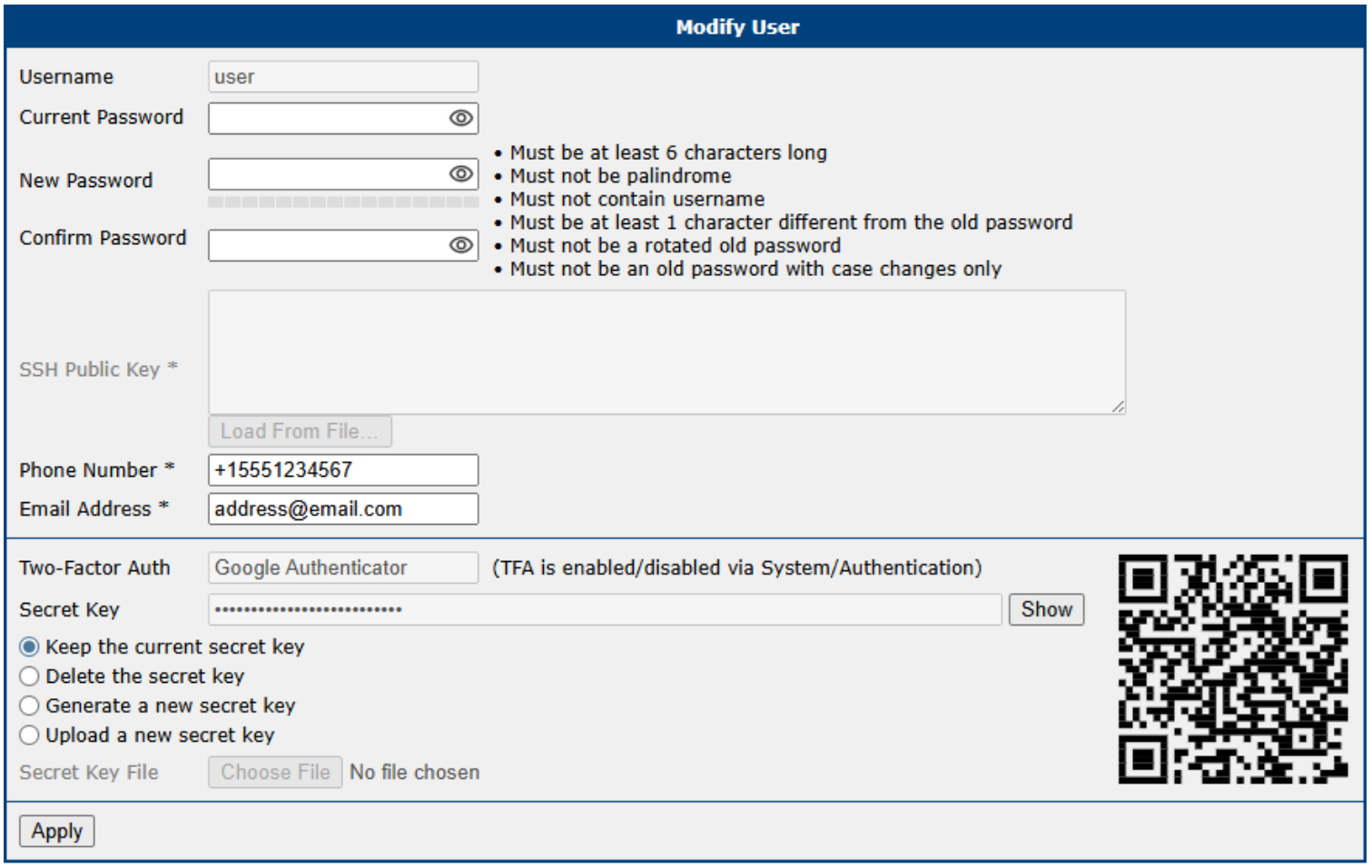
Forced to Change the Password in GUI

Modify User

> **Info**
>
> The *Administration → Modify User* page is only accessible to users with the *User* role.

The *Administration → Modify User* page allows users to edit their own configuration settings. While a standard user is restricted to this page, a user with the *Admin* role can modify all user accounts via the *Administration → Manage Users* page, as described in Manage Users.

The figure below shows an example of the *Administration → Modify User* configuration page, illustrating a case where a user with the *User* role is logged in and does not have access to the *Administration → Manage Users* page.

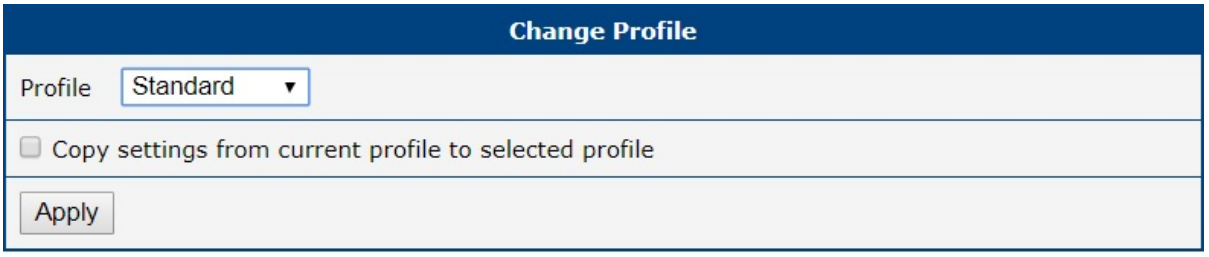


Modify User Configuration Page

Most items are already described in Manage Users. If the user wants to change their password, they must enter their original password into the *Current Password* field. The *SSH Public Key* field is disabled here because users with the *User* role are not permitted to log in via the console. In addition to the password, the user can also change their phone number and email address. In the last section of the screen, the user can modify their Two-Factor Authentication settings; for details, see Two-Factor Authentication.

Change Profile

Advantech routers allow you to store up to four complete sets of configurations, known as profiles: one *Standard Profile* and three *Alternative Profiles* (alt1, alt2, alt3). This feature is particularly useful for switching between different operational modes, such as changing mobile provider settings, activating different VPN tunnels, or modifying firewall rules based on location or time.



Change Profile

The *Administration → Change Profile* page serves two main purposes: saving the router's current running configuration into a specific profile, and switching the router to use a different profile.

Item	Description
Profile	Chooses the configuration profile that the router will load and use after the next reboot.
Copy settings from current profile to selected profile	When this box is checked, clicking *Apply* will save the router's **current running configuration** into the profile selected above. The router will **not** switch to this profile; it only saves the settings.

Warning

Any change made on this page, whether switching a profile or saving one, takes effect only after the router is rebooted.

You can switch the active profile using several methods:

- **Web Interface:** Select the desired profile from the *Select profile to switch to* dropdown and click *Apply*. Then, reboot the router.
- **SMS Command:** Send an SMS with the text `set profile [std|alt1|alt2|alt3]` to the router. This change is permanent and will be used after the next reboot. This is configured on the *Configuration → Services → SMS* page.

Set Date and Time

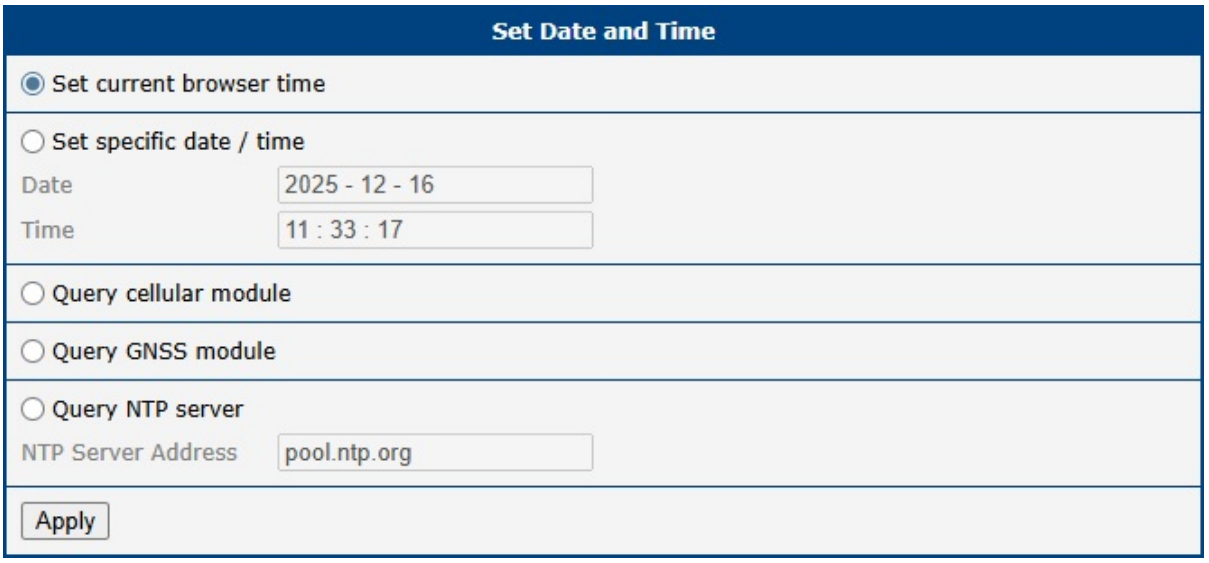
Warning

This page is for a **one-time manual setting** of the router's clock. For continuous time synchronization, you must configure the NTP client. See NTP for details.

Info

Please note that some of the options described below may not be available on all router models.

This page offers several methods for setting the system date and time.



Set Date and Time

1. **Set current browser time**: Synchronizes the router's clock with the time on your computer.
2. **Set specific date/time**: Allows you to manually enter a specific date and time. Use the format `yyyy-mm-dd` for the date and `HH:MM:SS` for the time.
3. **Query cellular module**: Retrieves the time from the mobile network using the NITZ standard. This requires an active cellular connection and support from both the mobile operator and the router's cellular module.
4. **Query GNSS module**: On routers equipped with a GNSS module, this option sets the time based on satellite data. The GNSS receiver must be enabled and have a valid position fix.
5. **Query NTP server**: Performs a one-time synchronization with a specified NTP server. You can enter the server's IP address (IPv4 or IPv6) or its domain name.

Manage SIM

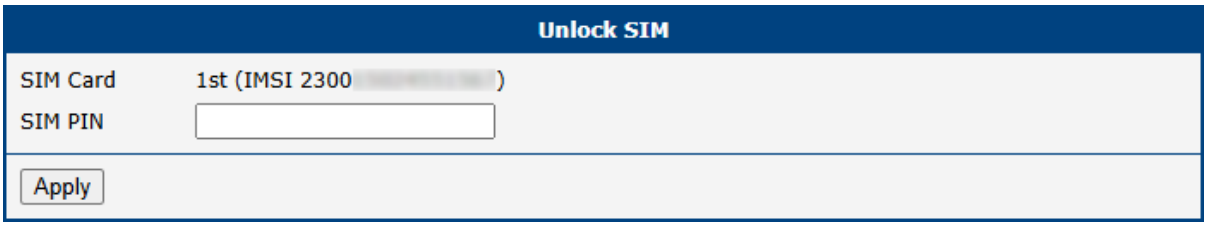
The *Administration → Manage SIM* menu provides tools for managing the security and settings of your SIM cards.

Unlock SIM

If your SIM card is protected by a Personal Identification Number (PIN), you must first enter it on the *Mobile WAN* configuration page to establish a connection. This page, however, allows you to permanently remove the PIN protection from the SIM card so it will no longer be required upon startup.

To remove the PIN, navigate to *Administration → Manage SIM → Unlock SIM*. The page displays the *SIM Card* (1st or 2nd) that is currently active within the system, along with its unique IMSI number. This ensures you are unlocking the correct card. Note that this operation can only be performed on a SIM card that is currently detected by the system. To proceed, enter the correct 4–8 digit PIN into the *SIM PIN* field and click *Apply*.

> **Warning**
>
> The SIM card will be blocked after three incorrect PIN entry attempts. To unblock it, you will need the PUK code, as described in the next section.



Unlock SIM Card

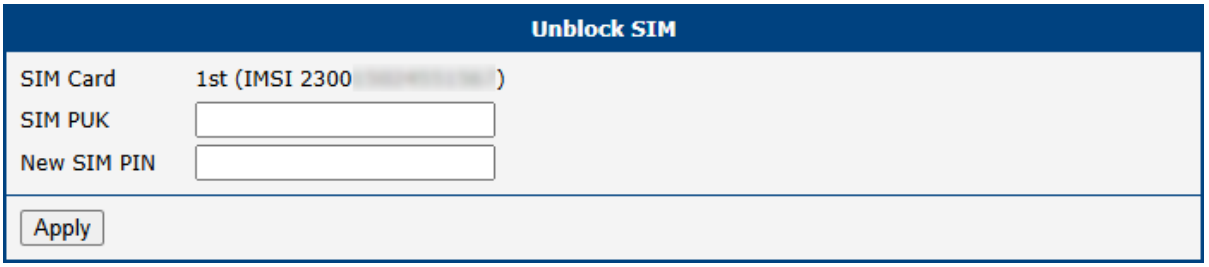
Unblock SIM

This page allows you to unblock a SIM card that has been locked due to three incorrect PIN attempts. You can also use this page to set a new PIN by utilizing the PUK code.

To unblock the card, navigate to *Administration → Manage SIM → Unblock SIM*. The page displays the *SIM Card* (1st or 2nd) that is currently active within the system, along with its unique IMSI number. This ensures you are unblocking the correct card. Note that this operation can only be performed on a SIM card that is currently detected by the system.

To proceed, enter the PUK (Personal Unblocking Key) code provided by your carrier into the *SIM PUK* field, and specify your desired new PIN in the *New SIM PIN* field. Click *Apply* to confirm the changes.

> **Warning**
>
> The SIM card will be permanently blocked if the PUK code is entered incorrectly too many times (typically ten attempts).



Unblock SIM Card

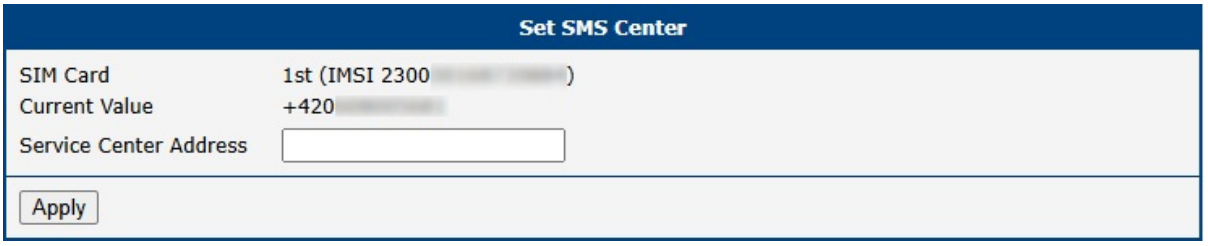
Set SMS Center

This page allows you to manually set the phone number for the SMS Service Center (SMSC), which is essential for sending SMS messages from the router. To access this page, navigate to *Administration → Manage SIM → Set SMS Center*.

The currently configured SMSC number can be viewed at any time on the *Status → Mobile WAN* page.

Info

In most cases, the SMSC number is automatically provisioned by the SIM card, and you do not need to change this setting. You should only set this value manually if you are experiencing issues sending SMS messages and your mobile network operator has provided a specific number to use. The number can be entered in a local format or with a full international prefix (e.g., `+420123456789`).



Set SMS Service Center Address

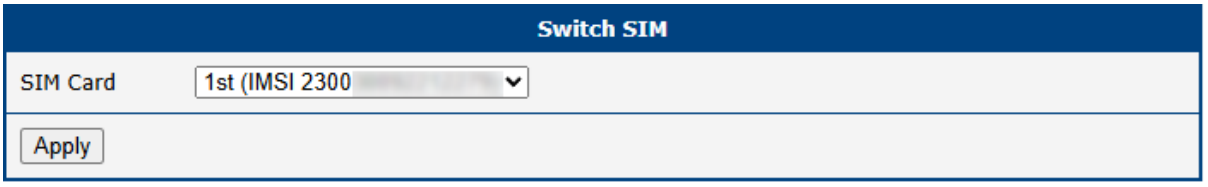
Switch SIM

The *Switch SIM* page allows for manual switching between SIM cards. This is primarily used for maintenance or testing purposes to force the router to a specific SIM slot, bypassing the automatic selection logic temporarily.

Info

To enable manual SIM switching, you must first deactivate the mobile connection. Navigate to *Configuration → Mobile WAN* and uncheck the *Create connection to mobile network* checkbox. If this is not done, the *SIM Card* selection will be disabled with a message "*Disable connection to mobile network first*" displayed.

To switch the active SIM card, navigate to *Administration → Manage SIM → Switch SIM*.



Switch SIM

Select the desired SIM card from the *SIM Card* drop-down list and click *Apply*. Each option includes the slot number and the IMSI number for precise identification.

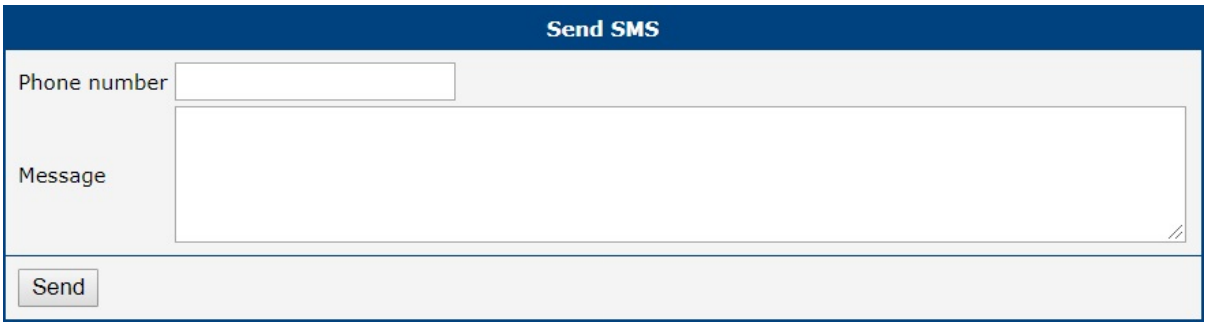
Warning

The manual selection made on this page is temporary. Once you re-enable the mobile connection in *Configuration → Mobile WAN*, the router will automatically select the active SIM card based on the rules and priorities defined in the *Mobile WAN* configuration, potentially overriding your manual selection.

Send SMS

You can send an SMS message directly from the router to test cellular functionality or send a quick notification. To do so, use the *Send SMS* dialog in the *Administration* menu.

Enter the recipient's *Phone number*, type your message in the *Message* field, and click *Send*. By default, the router limits SMS messages to 160 characters. To send longer messages, you must install the *PDU SMS* ↗ Router App.

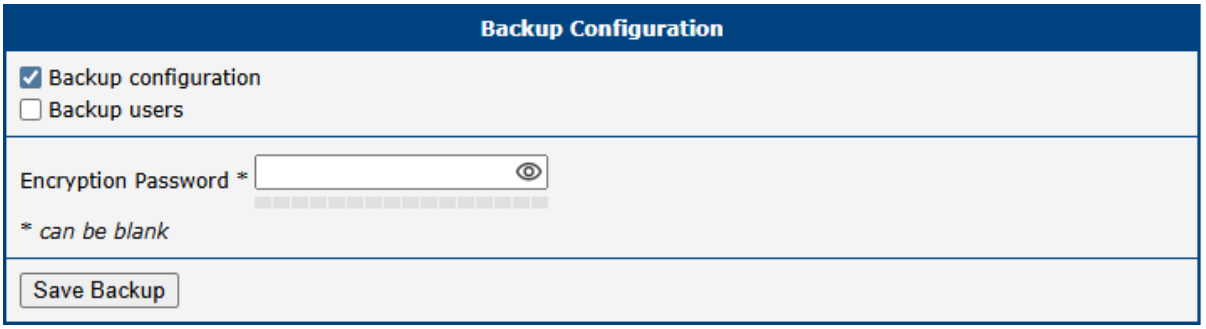


Send SMS

It is also possible to send SMS messages programmatically via a CGI script. For detailed instructions, please refer to the *Command Line Interface* application guide.

Backup Configuration

The *Administration → Backup Configuration* page allows you to save the router's current configuration settings to a file. This backup file can be used later to restore the router to a previous state or to clone the configuration to other devices.



Backup Configuration

Item	Description
Backup Configuration	When checked, the backup will include all router configuration settings.
Backup Users	When checked, the backup will include all user accounts and their passwords.
Encryption Password	If you set a password here, the backup file will be encrypted. If left blank, the file will be saved unencrypted.

> **Warning**
>
> Configuration backups can contain sensitive information, including user credentials. It is **strongly recommended** to always set an encryption password to protect the backup file. Also, ensure you are downloading the backup file over a secure (HTTPS) connection.

After selecting the desired options, click the *Apply* button. Your web browser will then prompt you to save the configuration file (with a `.cfg` extension). For instructions on how to use this file, see Restore Configuration.

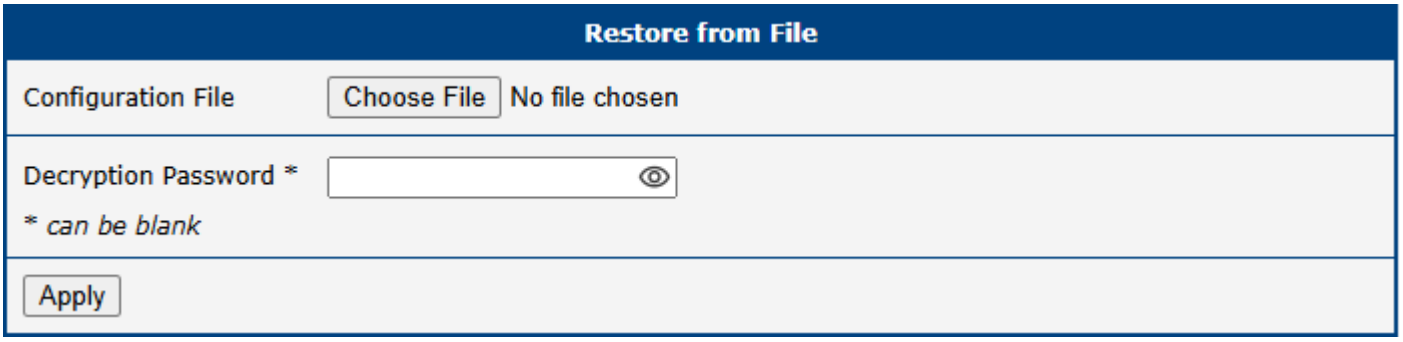
Restore Configuration

The *Restore Configuration* menu contains options for reverting the router's settings to a previous state or resetting them entirely. It is divided into two sub-menus: *Restore from File* and *Factory Reset*.

Restore from File

This page allows you to restore the router's settings from a previously created backup file. For instructions on creating a backup, please see Backup Configuration.

To restore a configuration, navigate to *Administration → Restore Configuration → Restore from File*. Click the *Choose File* button to select the `.cfg` backup file from your computer. If the file is encrypted, you must provide the correct password in the *Decryption Password* field. Clicking the *Apply* button will upload the file, apply the settings, and reboot the router.



Restore Configuration

> **Warning**
>
> Restoring a configuration from firmware older than version 6.2.0 is not supported. While upgrading the firmware from an older version is possible, attempting to restore a configuration file from such versions will result in some settings being reset to their factory defaults.

Item	Description
Configuration File	Select the `.cfg` backup file from your local computer.
Decryption Password	The password required to decrypt an encrypted backup file. Leave blank if the file is not encrypted.

Factory Reset

Warning

Factory reset is a destructive action that completely erases all configuration and restores the router to its original factory state. **This action is irreversible and should be used with extreme caution.**

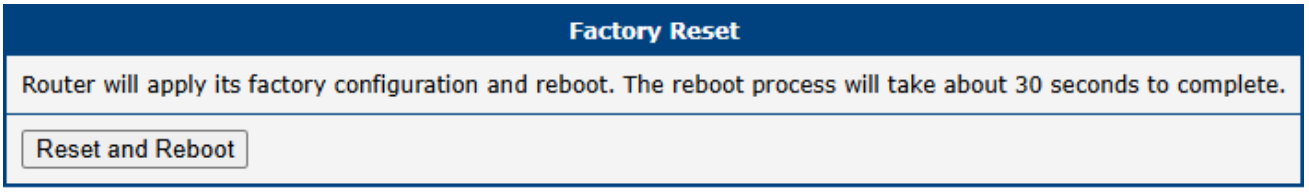
Key consequences of performing a factory reset include:

- All custom configurations (including network, VPN, and firewall rules) will be permanently deleted.
- All user accounts will be erased, leaving only the default administrator account.
- The router's LAN IP address will revert to its factory default (typically `192.168.1.1`), which will likely disconnect you from the web interface.

This software reset is equivalent to a hardware factory reset using the *RST* button, as detailed in Reset.

To reset the router to its default factory settings, navigate to *Administration → Restore Configuration → Factory Reset*.

Clicking the *Reset and Reboot* button will erase all custom configurations, apply the factory default settings, and automatically restart the device. The reboot process typically takes about 30 seconds to complete.



Factory Reset

Update Firmware

Keeping your router's firmware up to date is crucial for security and access to the latest features. This page allows you to view the current firmware version and perform updates.

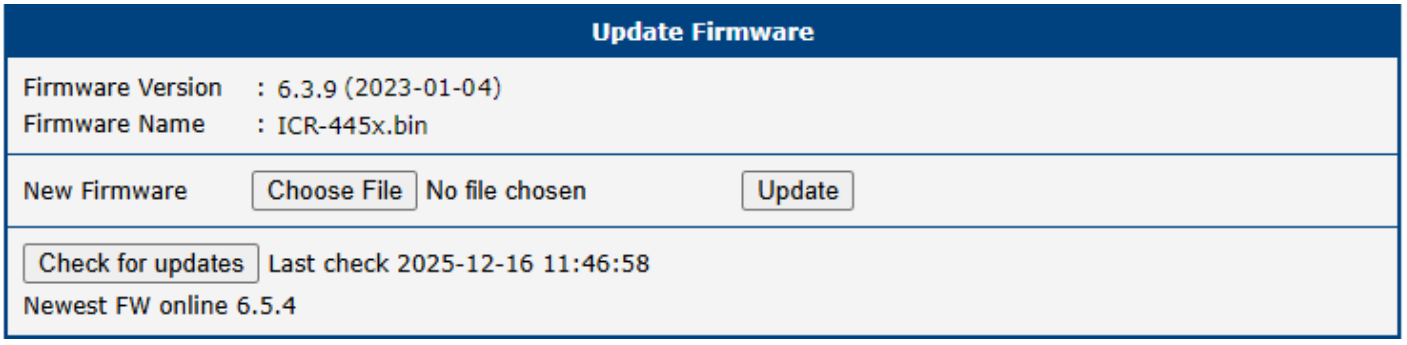
Info

The latest official firmware for your router is available on the Download Current Versions ↗ page.

Warning

- For security reasons, always use the latest firmware version. Do not downgrade to a version older than the one the router was manufactured with, and never upload firmware designed for a different router model, as this can cause irreversible damage.
- Firmware updates can occasionally affect Router App compatibility. It is recommended to update all Router Apps at the same time as the firmware.
- If you are using an unsecured HTTP connection, some firewalls may block the firmware upload. In such cases, switch to HTTPS or contact your network administrator.

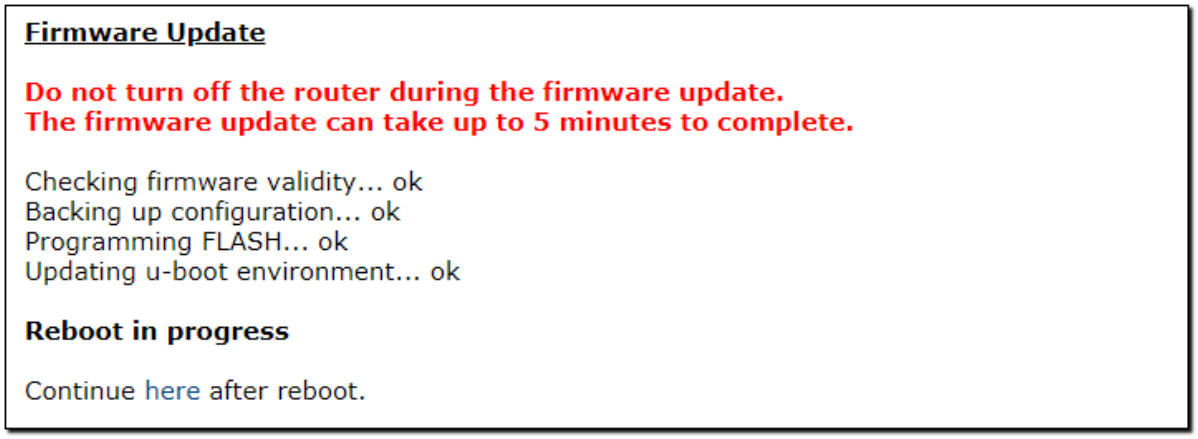
The *Administration → Update Firmware* page is divided into sections for viewing the current version and performing manual or online updates.



Update Firmware Administration Page

Item	Description
Firmware Version	The version number and release date of the currently installed firmware.
Firmware Name	The name of the firmware file currently running on the router.
New Firmware	Allows you to manually upload a firmware file from your computer using the *Choose File* button.
Update	Starts the update process using the selected file.
Check for updates	Connects to the public server to check if a newer firmware version is available (supported since firmware version 6.4.0). The timestamp of the last check is displayed.
Download and Update	This button appears if a newer version is found. Clicking it will automatically download the new firmware and initiate the update process.

During the update, the router will display its progress, as shown in the figure below. Once the update is finished, the router will automatically reboot. After it comes back online, click the provided *here* link to return to the web interface.



Process of Firmware Update

Reboot

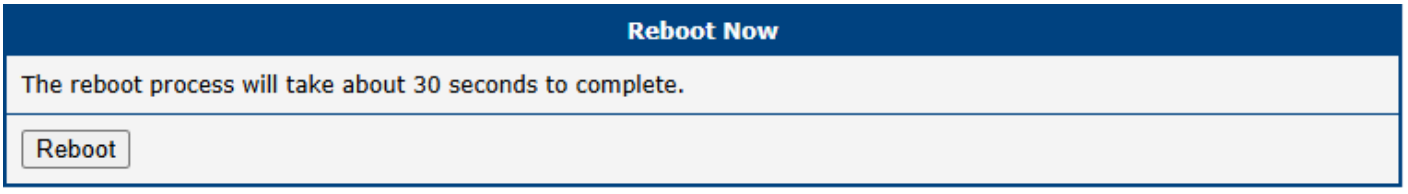
The *Reboot* menu provides two different options to restart or schedule automatic restarts of the router. To access these options, select the *Reboot* item in the *Administration* menu.

Info

- Starting with firmware version 6.6.0, the reboot functionality is integrated directly into the router's base firmware and replaces the legacy Daily Reboot ↗ Router App.
- To prevent conflicts, you must disable or uninstall the legacy Router App before using the integrated firmware feature.

Reboot Now

This submenu allows you to immediately reboot the router by clicking the *Reboot* button. A standard reboot takes approximately 30 seconds to complete.

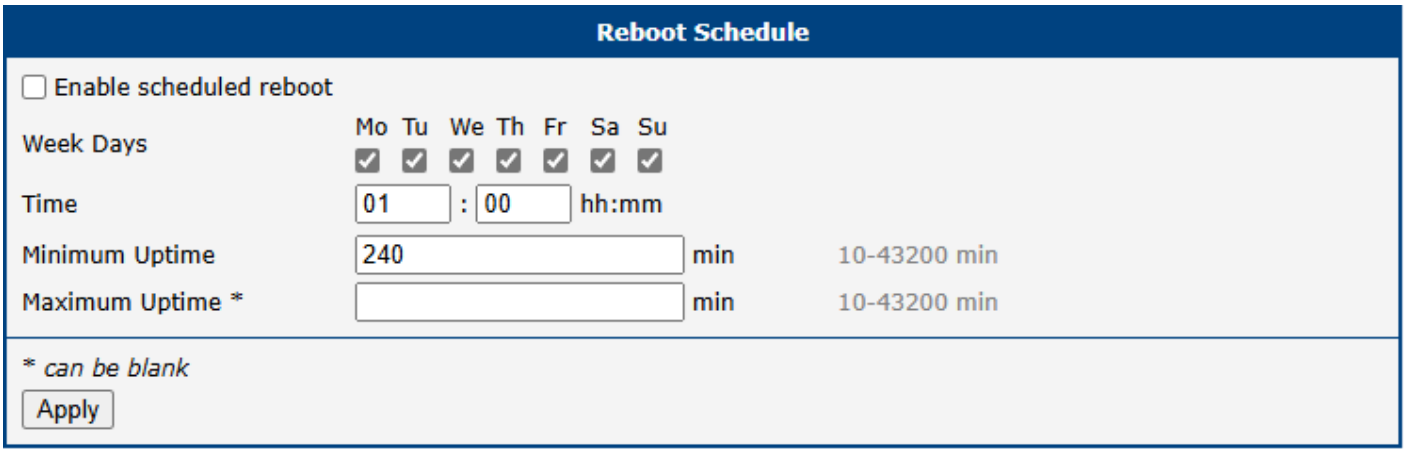


Reboot

Reboot Schedule

The *Reboot Schedule* submenu allows scheduled, automatic restarting of the router. The following parameters can be configured:

Item	Description
Enable scheduled reboot	Activates or deactivates periodic router restarts according to the selected schedule.
Week Days	Select specific days of the week (Monday–Sunday) for the scheduled reboot. Multiple days can be selected.
Time	Set the exact time for the reboot to occur on the chosen days (format: hh:mm).
Minimum Uptime	The minimum amount of time the router must be running before a scheduled reboot is permitted. This prevents reboot loops (e.g., during unstable power conditions). Range: 10–43,200 minutes.
Maximum Uptime	(Optional) Triggers an automatic reboot once the router's continuous uptime reaches this specified value. This is often used to ensure long-term system stability. If left blank, no reboot is triggered based on maximum uptime (range: 10–43,200 minutes).



Reboot Schedule

Logout

Clicking the *Logout* item in the main menu immediately terminates your session and logs you out of the router's web interface. You will be redirected to the login page.

> **Info**
>
> For security reasons, it is always recommended to log out when you have finished configuring the router, especially when accessing it from a shared or public computer.

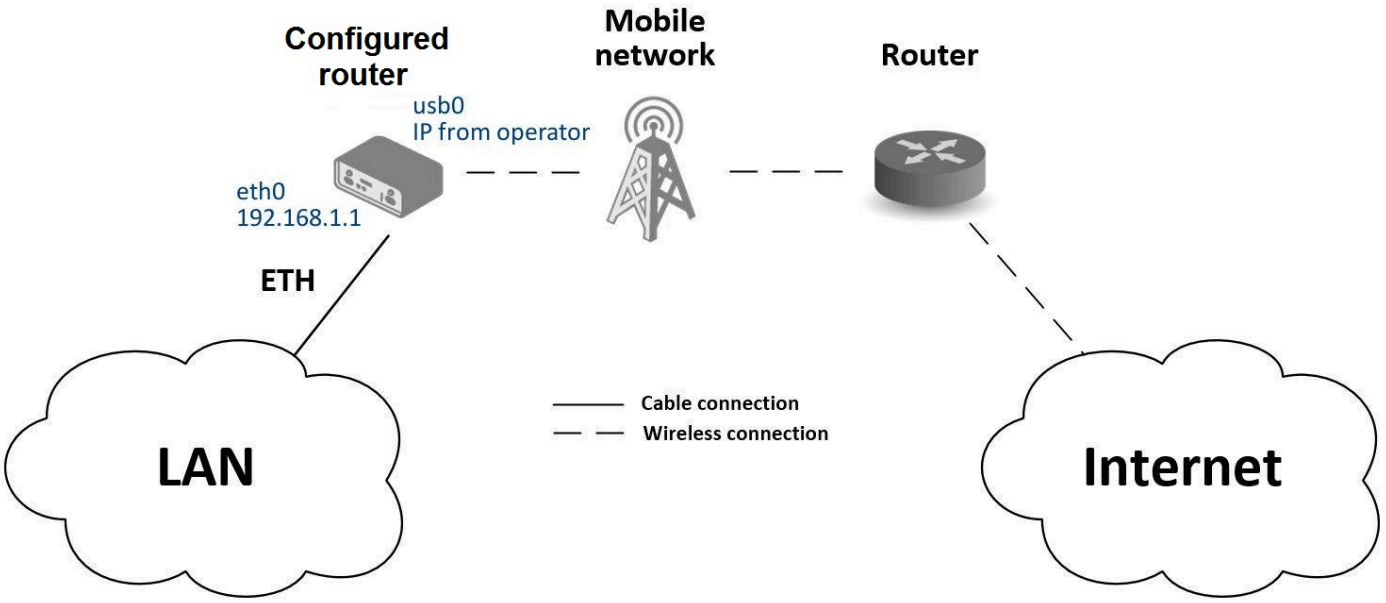
Typical Use Cases

Advantech routers are highly versatile and support a wide range of applications. This chapter outlines several common deployment scenarios to illustrate the router's key features and capabilities in practical, real-world examples.

The configuration examples provided in this chapter are based on IPv4 networks.

Access to the Internet from LAN

This use case describes how to provide Internet access to a Local Area Network (LAN) using the router's cellular connection. A SIM card with an active data plan from a mobile network operator is required.



Access to the Internet from LAN: topology example

Initial Setup

1. Insert an active SIM card into the *SIM1* slot.
2. Attach an appropriate antenna to every antenna connector on the router. For optimal cellular performance, both the main (*ANT*) and diversity (*DIV*) antennas are required. If your router includes Wi-Fi or GNSS capabilities, their respective antennas must also be connected.
3. Connect your computer or a local network switch to the router's *ETH0* port.
4. Connect the power supply to power on the router.

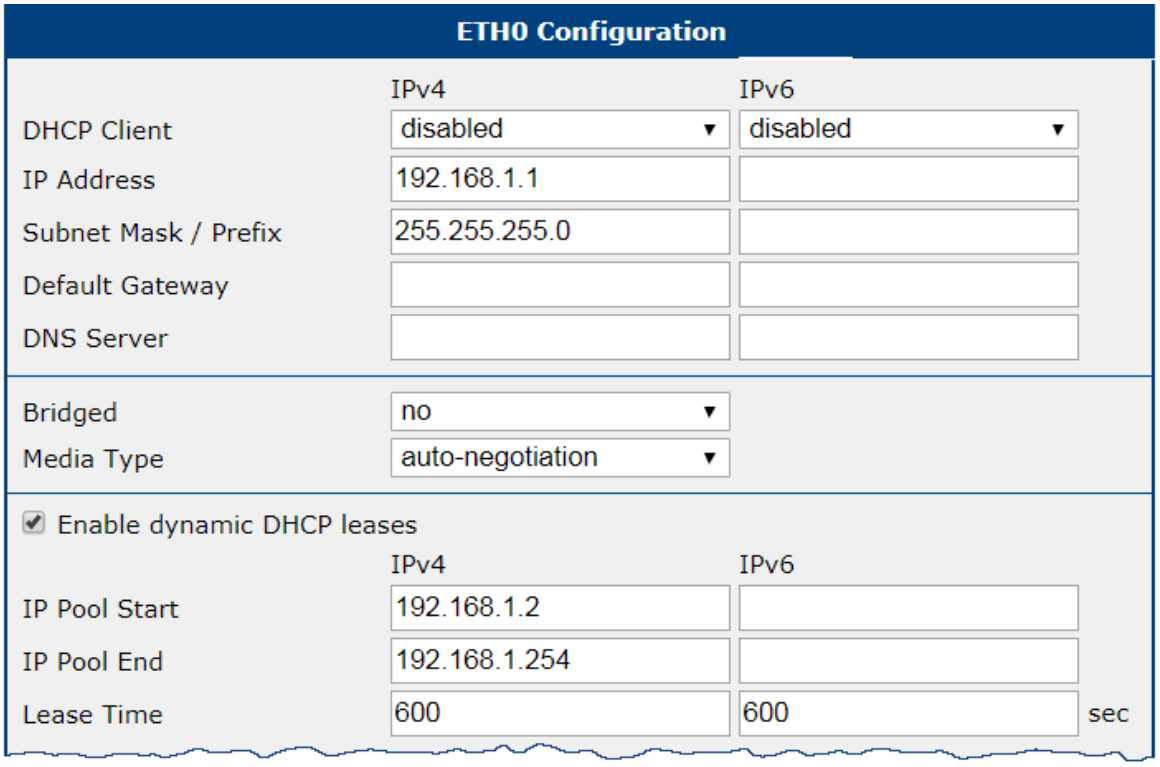
After powering on, wait for the router to register on the mobile network. A successful connection is indicated by the *WAN* and *DAT* LEDs on the front panel.

Configuration

While factory settings are often sufficient, you can review or modify the configuration in the router's web interface via the *Configuration* section.

Ethernet Configuration

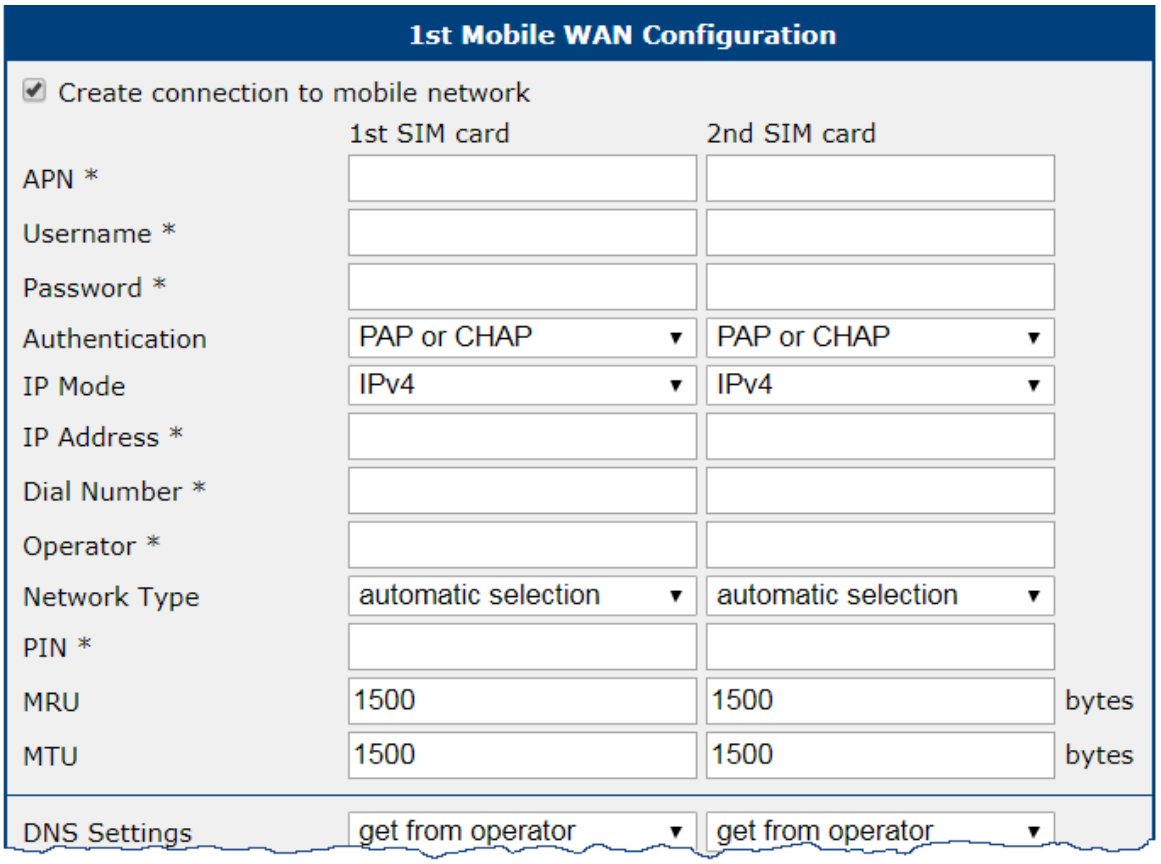
Navigate to *Configuration → Ethernet*. The LAN interface (`ETH0`) is pre-configured with a static IP address of `192.168.1.1` . The DHCP server is also enabled by default, automatically assigning IP addresses to connected devices (the first device receives `192.168.1.2` , and so on). No changes are needed for this use case.



Access to the Internet from LAN: Ethernet configuration

Mobile WAN Configuration

Navigate to *Configuration → Mobile WAN*. Ensure that the *Create connection to mobile network* option is enabled (the default setting). For most public SIM cards, you do not need to fill in the APN, username, or password.



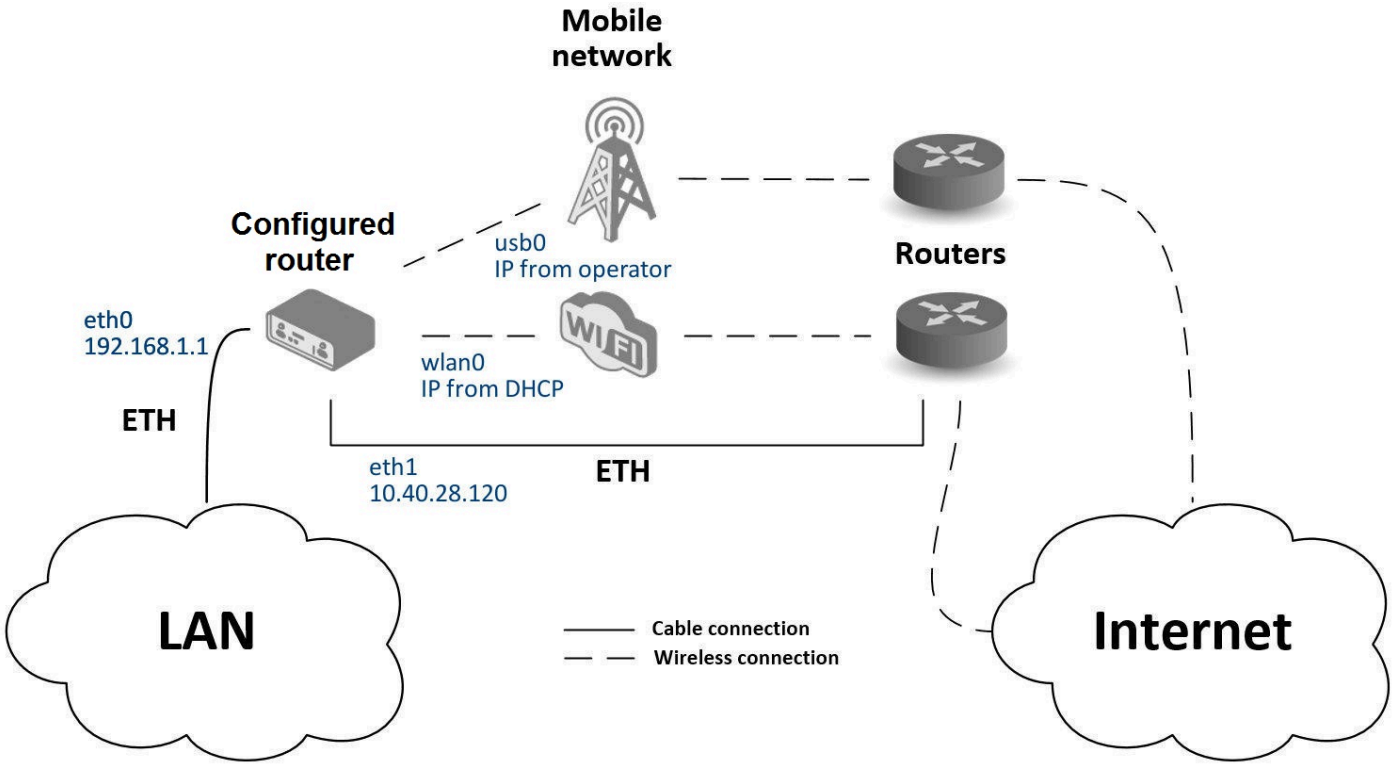
Access to the Internet from LAN: mobile WAN configuration

Verifying Connectivity

Navigate to *Status → Mobile WAN*. This page displays key details about the connection, including the operator, signal strength, and a *Connection successfully established* message. You can also inspect *Status → Network* to see the new mobile interface (`usb0`) and the IP address assigned by the operator. Once confirmed, all devices on the LAN have Internet access.

Backup Access to the Internet from LAN

This use case demonstrates how to configure connection redundancy by setting up multiple Internet sources and defining their priority. The router automatically switches to a lower-priority connection if a higher-priority one fails, ensuring continuous Internet access for the LAN via the *Backup Routes* feature. A typical scenario is **LTE failover**, where the cellular (Mobile WAN) connection automatically backs up the primary wired or Wi-Fi WAN connection.



Backup access to the Internet: topology example

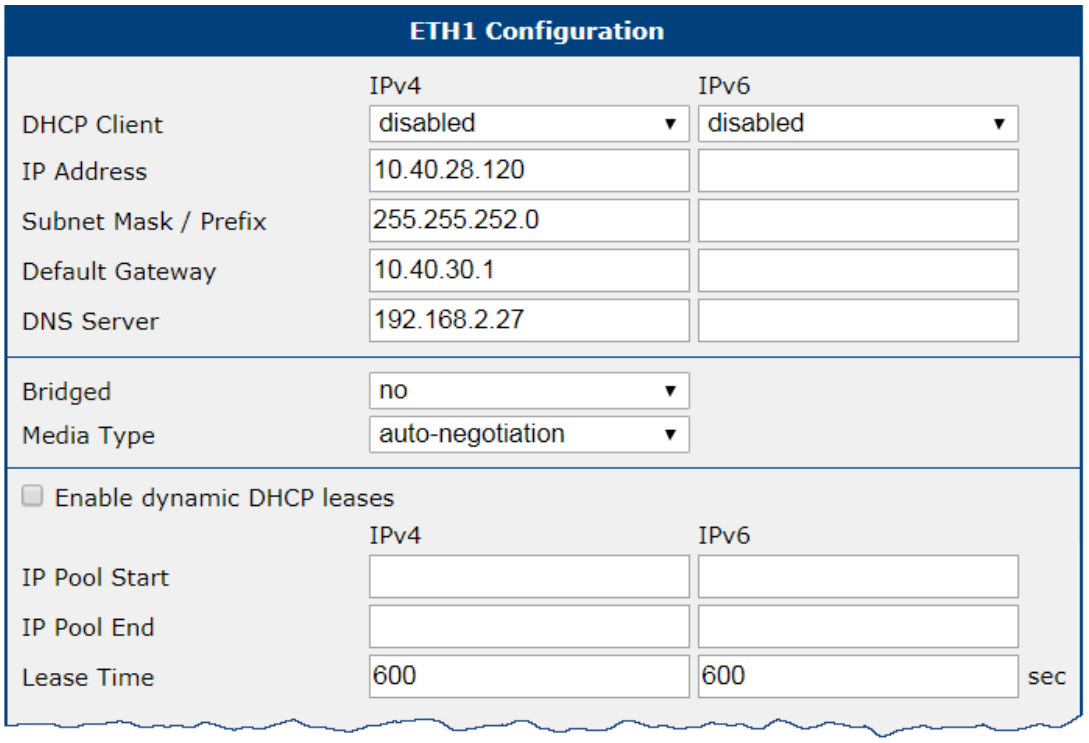
Interface Configuration

Configure each interface that will serve as an Internet source. Leave the LAN interface (`ETH0`) at its default settings.

Ethernet WAN Configuration

The `ETH1` port is used as the primary wired WAN connection.

1. Navigate to *Configuration → Ethernet → ETH1*.
2. Configure the interface with a static IP address, subnet mask, default gateway, and DNS server provided by your Internet Service Provider.
3. Click *Apply* to save the changes.



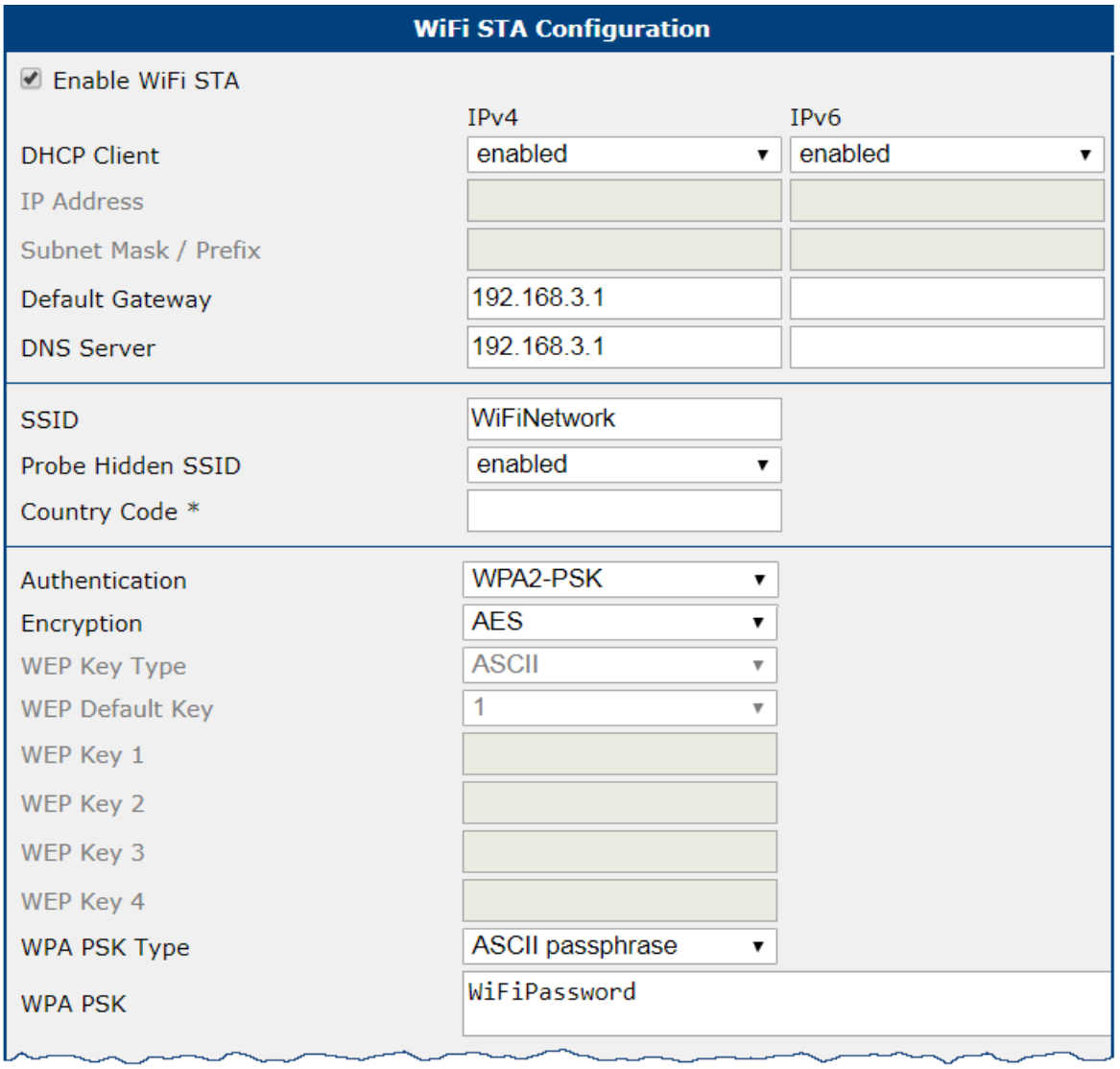
Backup access to the Internet: Ethernet configuration

Wi-Fi WAN Configuration

To use Wi-Fi as a backup connection, configure the router as a client (Station) to another Wi-Fi network.

1. Navigate to *Configuration → WiFi → Station*.
2. Check *Enable WiFi STA*.
3. If the Wi-Fi network provides settings automatically, enable the DHCP client. Otherwise, manually enter the default gateway and DNS server addresses.
4. Enter the network's *SSID* and select the appropriate *Authentication*, *Encryption*, and *WPA PSK Type*.
5. Enter the Wi-Fi password and click *Apply*.

You can verify the connection in *Status → WiFi*, where a successful connection shows `wpa_state=COMPLETED`.

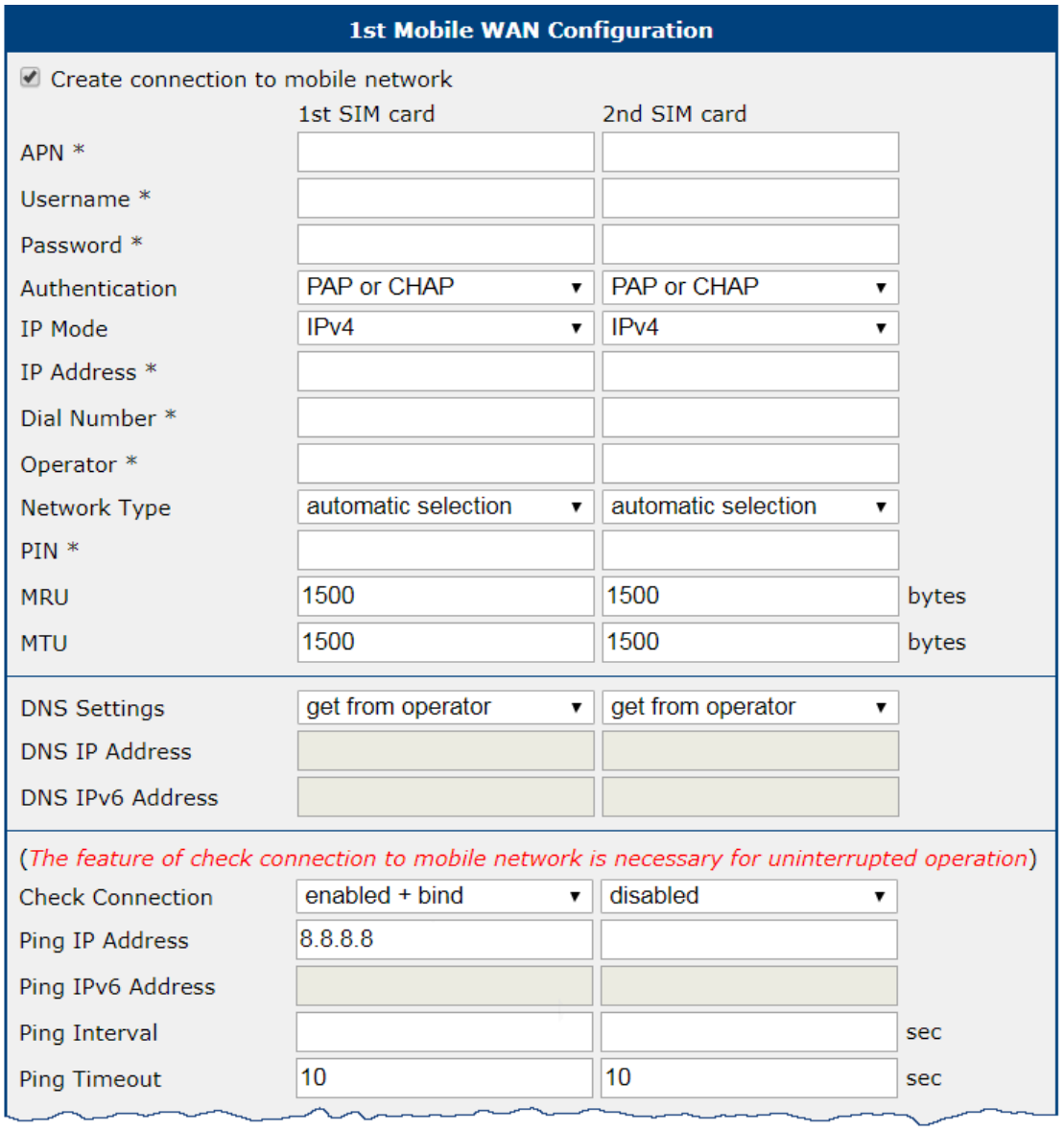


Backup access to the Internet: Wi-Fi configuration

Mobile WAN Configuration

The cellular connection serves as the final backup. Insert an active SIM card into the *SIM1* slot and attach the cellular antenna. To integrate it into the backup system:

1. Navigate to *Configuration → Mobile WAN*.
2. Set the *Check connection* option to *enabled + bind*.
3. Enter a reliable IP address to ping (e.g., your operator's DNS server) and set the check interval.

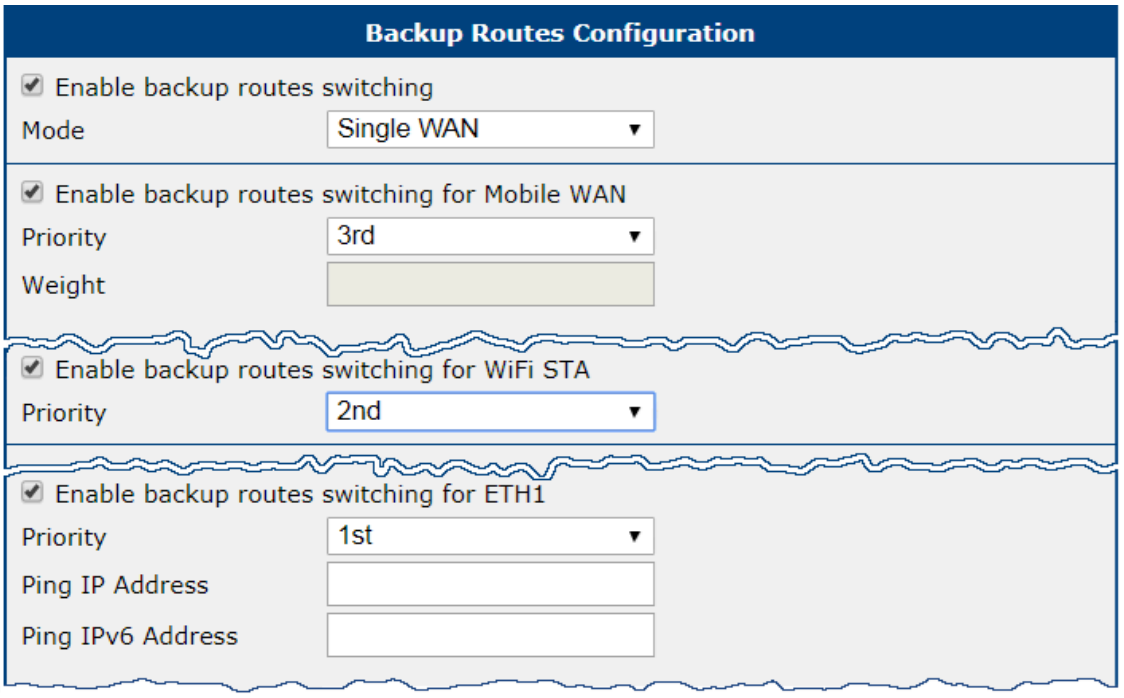


Backup access to the Internet: mobile WAN configuration

Backup Routes Configuration

After configuring the interfaces, set their priority in *Configuration → Backup Routes*.

1. Set the priority for each WAN interface:
    - **1 (Highest):** `eth1` (Wired Ethernet)
    - **2 (Medium):** `wlan0` (Wi-Fi)
    - **3 (Lowest):** `usb0` (Cellular)
2. Check *Enable backup routes switching* for each route.
3. Click *Apply* to save the configuration.



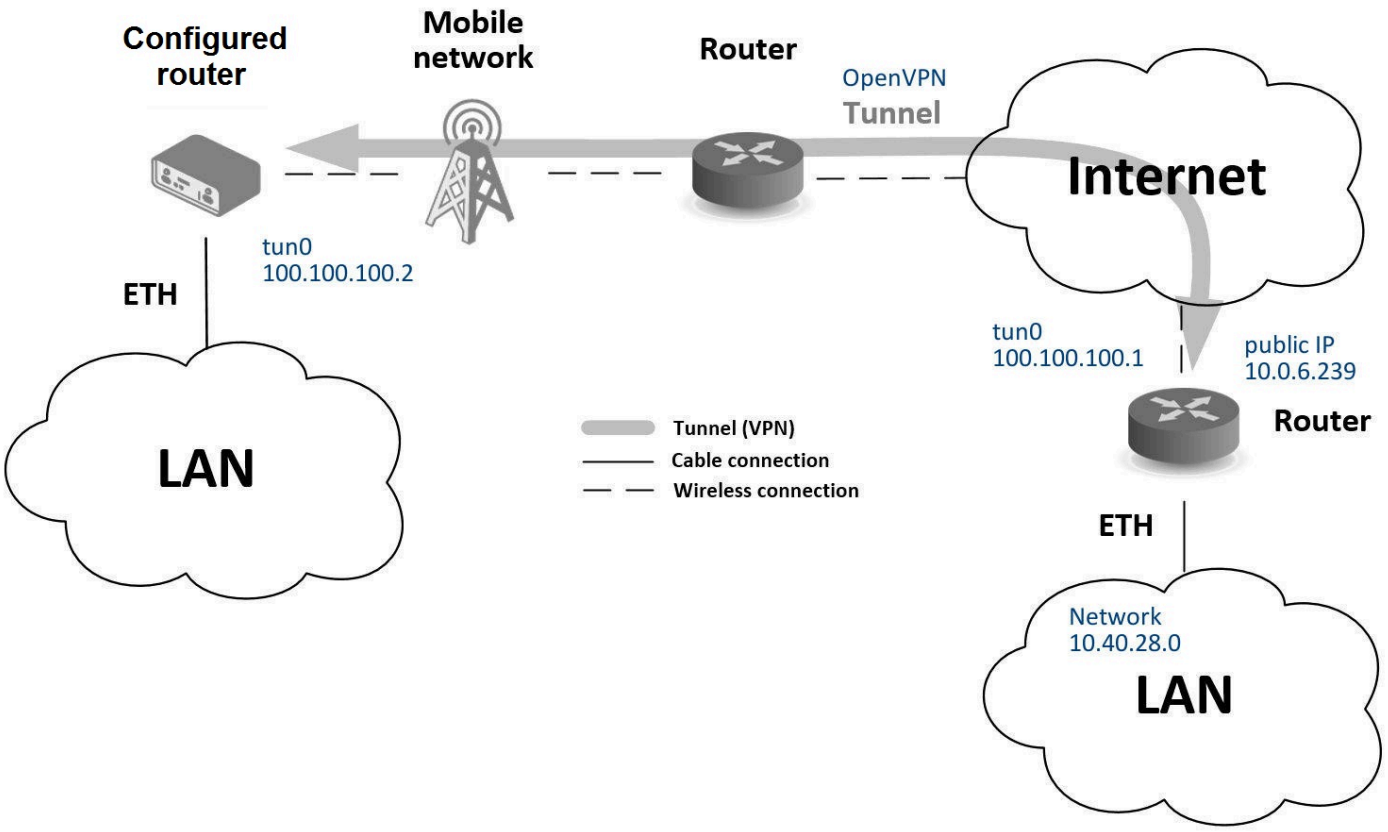
Backup access to the Internet: backup routes configuration

Verifying Failover

Monitor all network interfaces under *Status → Network*. The route table at the bottom of the page shows which interface is currently active as the default route. If `eth1` fails, the default route switches to `wlan0`. If `wlan0` also fails, it switches to `usb0`.

Secure Network Interconnection with VPN

A Virtual Private Network (VPN) creates a secure, encrypted tunnel over an untrusted public network (such as the Internet), allowing two or more separate LANs to communicate as if they were a single private network. This ensures both the confidentiality and integrity of the exchanged data.



Secure network interconnection: topology example

Advantech routers support several VPN protocols, including:

- **OpenVPN:** A highly flexible and secure SSL/TLS-based VPN.
- **IPsec:** A standards-based framework for securing IP communications.

The router also supports non-encrypted tunneling protocols such as *GRE*, *PPTP*, and *L2TP*, which can be combined with IPsec to create secure VPNs.

This example demonstrates how to establish an OpenVPN tunnel between two routers using a pre-shared secret key for authentication.

Configuration

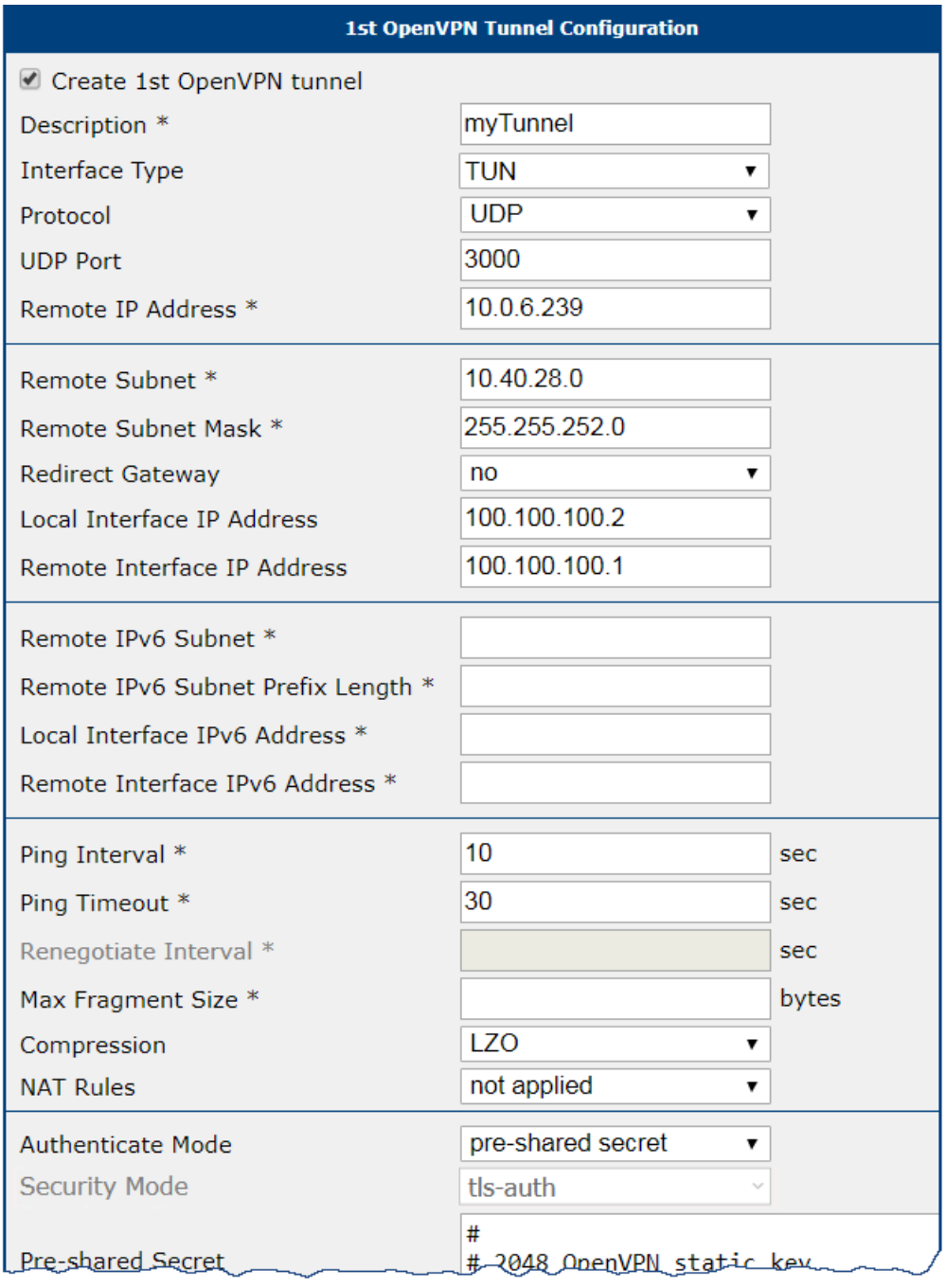
Mobile WAN Configuration

A stable Internet connection is required before establishing a VPN tunnel. Insert a SIM card and attach the antenna. The router typically establishes a cellular connection automatically. Verify that the mobile connection is active under *Configuration → Mobile WAN*.

OpenVPN Configuration

1. Navigate to *Configuration → OpenVPN*.
2. Enable one of the available tunnels by checking *Create 1st OpenVPN tunnel*.
3. Set the *Protocol* and *Port* to match the settings of the remote router.
4. In the *Remote Host and Port* field, enter the public IP address of the remote router.

5. In the *Authentication Mode* dropdown, select *Static key (pre-shared)*.
6. Paste the pre-shared secret key into the *Static key* field.
7. Define the virtual IP addresses for the tunnel endpoints in *Local Interface IP Address* and *Remote Interface IP Address*. These must form a mini-subnet for the tunnel (e.g., `10.8.0.1` and `10.8.0.2`).
8. Click *Apply* to save the configuration.



Secure network interconnection: OpenVPN configuration

Verifying Connectivity

Confirm that the VPN tunnel is active:

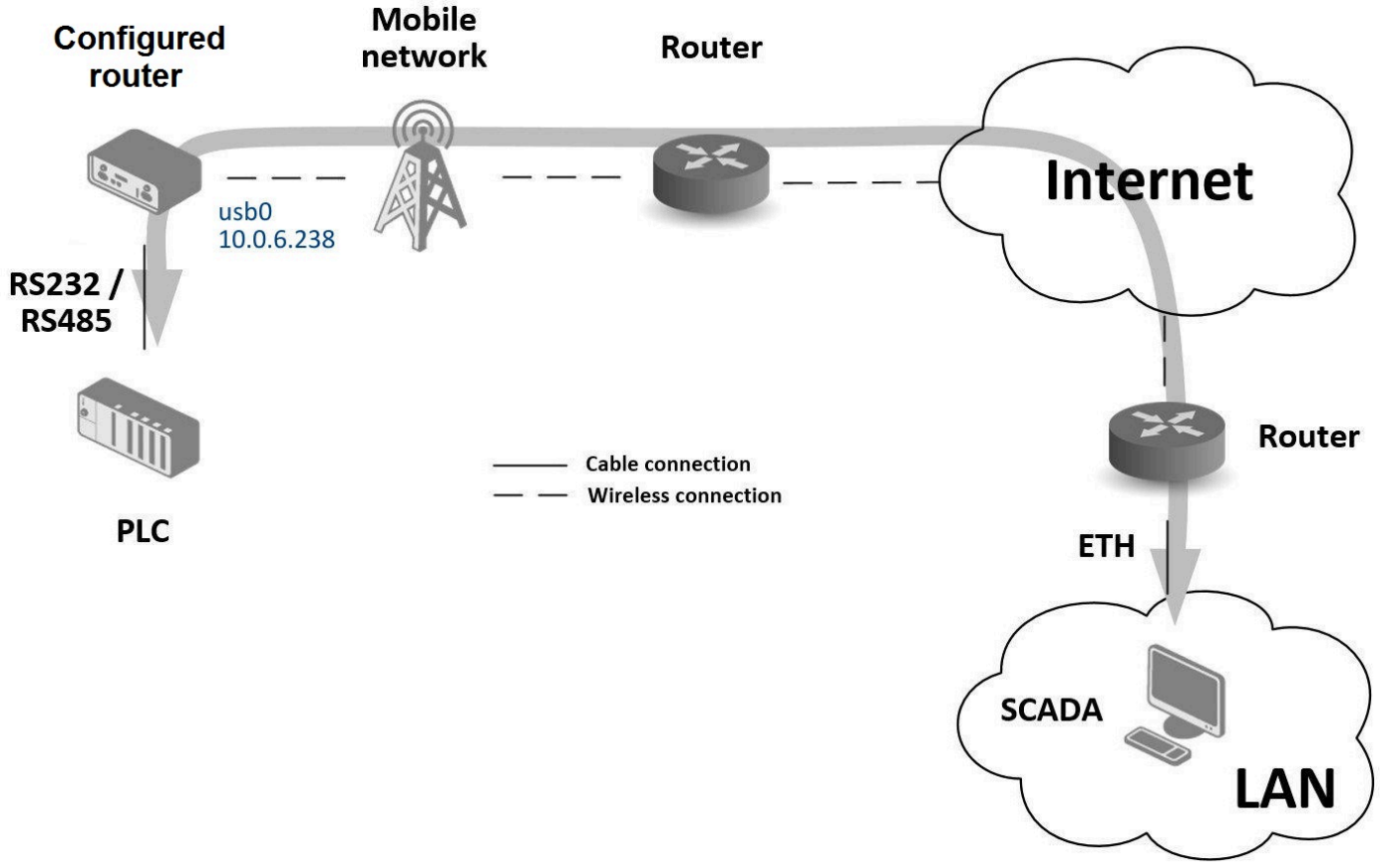
- **Network Status:** Navigate to *Status* → *Network*. A new virtual interface `tun0` should be listed with the IP address you configured.

- **System Log:** Navigate to *Status* → *System Log*. Look for an `Initialization Sequence Completed` entry, confirming the OpenVPN tunnel is established.

Once the tunnel is active, you can verify it by pinging the remote tunnel endpoint's IP address from the router's command-line interface via SSH.

Serial Gateway

The Serial Gateway feature encapsulates serial data into IP packets, enabling communication with serial devices (such as PLCs, meters, or sensors) over an IP network. This creates a virtual serial port across the Internet, allowing a central SCADA system or remote PC to collect data from or control legacy serial equipment.



Serial gateway: topology example

In this example, the router's RS232 port is connected to a PLC, and the router is configured as a TCP server. A remote PC (SCADA) connects as a TCP client to communicate with the PLC.

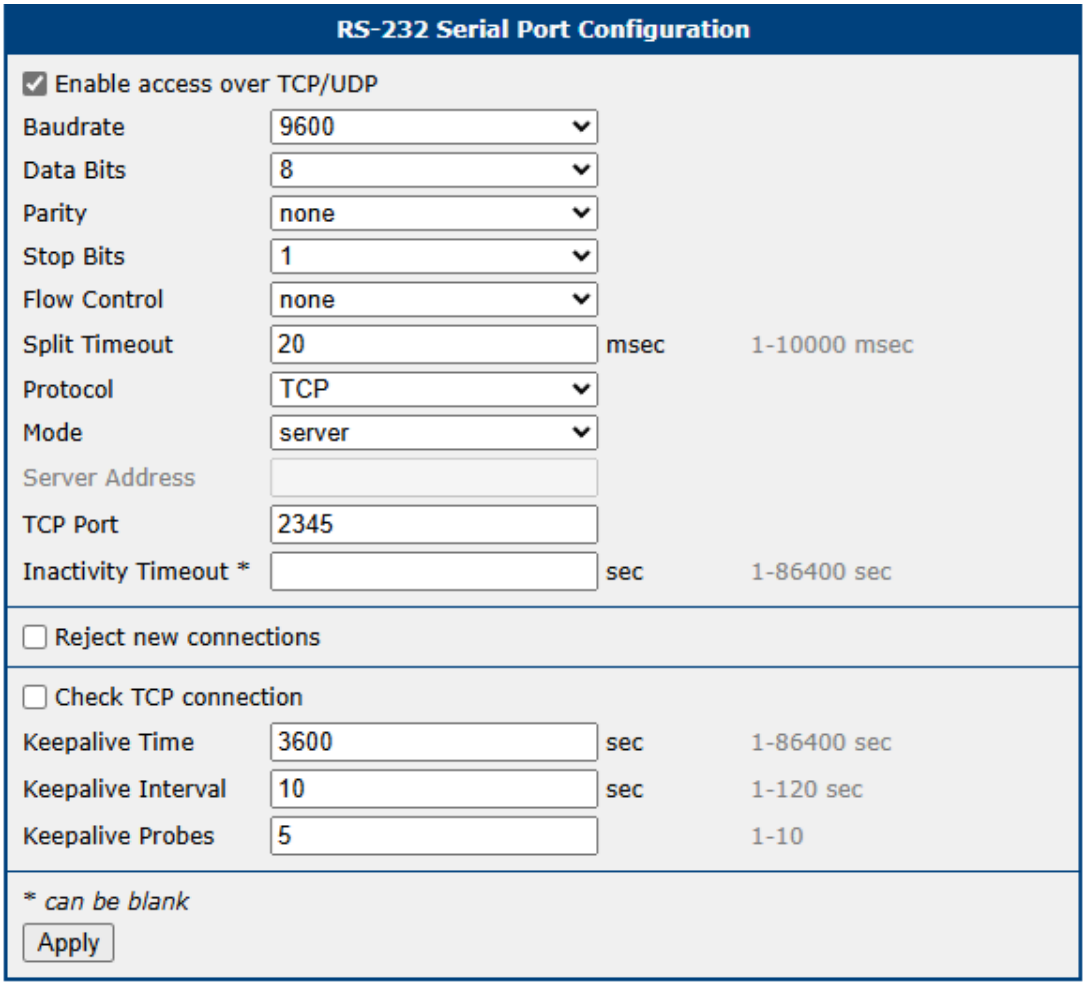
Configuration

Mobile WAN Configuration

A stable Internet connection is essential. Insert an active SIM card into the *SIM1* slot and attach the cellular antenna. The router automatically connects to the mobile network. The public IP address assigned by the mobile operator is used by the remote client to connect to the serial gateway. For more details, see the *Mobile WAN* section in the *Configuration* chapter.

Peripheral Port (RS232) Configuration

1. Navigate to *Configuration → Peripheral Ports → RS-232*.
2. Check *Enable access over TCP/UDP*.
3. Set *Protocol* to `TCP`.
4. Set *Mode* to `server`. The router will listen for incoming connections.
5. In the *TCP Port* field, enter the port number on which the router will listen (e.g., `2345`).
6. Configure the serial communication parameters (*Baud Rate*, *Data Bits*, *Parity*, etc.) to match the connected serial device.
7. Click *Apply* to save the configuration.



Serial gateway: Peripheral Port configuration

Verifying Connectivity

The remote PC (SCADA) can establish a TCP connection to the router's public IP address (e.g., `10.0.6.238`) on the configured port (e.g., `2345`). All data sent over this TCP session is forwarded to the PLC via the serial port, and vice versa.

Monitor the connection status in *Status → System Log*. When the remote client connects successfully, a *TCP connection established* message appears in the log.

Technical Parameters

Basic Parameters

ICR-1602 and ICR-1642

Parameter	Condition	Value
Temperature Range	Operating Storage	-40 °C to +75 °C (-40 °F to +167 °F) -40 °C to +85 °C (-40 °F to +185 °F)
Humidity	Operating Storage	5 to 95 % relative humidity, non-condensing 5 to 95 % relative humidity, non-condensing
Altitude	Operating	2000 m / 70 kPa
Degree of Protection		IP30
Supply Voltage		9 to 48 V DC
Consumption (non-Wi-Fi / Wi-Fi)	Idle Average Maximum	2.8 W / 3.8 W 3.5 W / 4.5 W 3.8 W / 5.5 W
Dimensions (without clips)		94 × 39 × 90 mm (3.7" × 1.53" × 3.54")
DIN Rail Clip (optional)		DIN 30 mm
Weight		ICR-16XX: 331 g (0.73 lbs) (excluding accessories) LTE antenna: 25.2 g (0.06 lbs) Wall-mount bracket: 45 g (0.10 lbs)

ICR-1645

Parameter	Condition	Value
Temperature Range	Operating Storage	-30 °C to +75 °C (-22 °F to +167 °F) -40 °C to +85 °C (-40 °F to +185 °F)
Humidity	Operating Storage	5 to 95 % relative humidity, non-condensing 5 to 95 % relative humidity, non-condensing
Altitude	Operating	2000 m / 70 kPa
Degree of Protection		IP30
Supply Voltage		9 to 48 V DC
Consumption (non-Wi-Fi / Wi-Fi)	Idle Average Maximum	2.7 W / 3.6 W 3.7 W / 4.8 W 5.5 W / 6.8 W

Parameter	Condition	Value
Dimensions (without clips)		116 × 39 × 113.5 mm (4.56" × 1.53" × 4.47")
DIN Rail Clip (optional)		DIN 30 mm
Weight		ICR-16XX: 470 g (1.04 lbs) (excluding accessories) LTE antenna: 25.2 g (0.06 lbs) Wall-mount bracket: 50 g (0.11 lbs) Wi-Fi antenna: 7.8 g (0.02 lbs)

Standards and Regulations

The routers comply with the following standards and regulations:

Parameter	Description
Radio	EN 301 908-1, EN 301 908-2, EN 301 908-13, EN 301 908-25, EN 303 413, EN 300 328, EN 301 893
EMC	EN 301 489-1, EN 301 489-17, EN 301 489-19, EN 301 489-52, EN 61000-6-2, EN 61000-6-3, EN 55032, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6
Safety	EN 62368-1
Mechanical	EN 60529, EN 60068-2-27, EN 60068-2-64
Climatic	EN 60068-2-1, EN 60068-2-2, EN 60068-2-14, EN 60068-2-78
National	ICR-16xx-EU: CE, UKCA compliant
Environmental	REACH, RoHS3 and WEEE compliant

Type Tests and Environmental Specifications

Routers undergo the following tests to ensure durability and reliability:

ICR-1602 and ICR-1642

Phenomena	Test	Description	Test levels
ESD	EN 61000-4-2	Enclosure contact	± 8 kV (crit. B)
RF field AM modulated	EN 61000-4-3	Enclosure	3 V/m (crit. A) (80 – 1000 MHz)
Fast transient	EN 61000-4-4	Signal ports Power ports Ethernet ports	± 0.5 kV (crit. A)

Phenomena	Test	Description	Test levels
Surge	EN 61000-4-5	Ethernet ports Power ports	± 0.5 kV (crit. B) ± 1 kV (crit. B) open circuit
RF conducted	EN 61000-4-6	All ports	3 V/m (crit. A) (0.15 – 80 MHz)
Radiated emission	EN 55032	Enclosure	Class B
Conducted emission	EN 55032	Signal ports Power ports Ethernet ports	Class B Class B Class B
Dry heat	EN 60068-2-2	Storage +85 °C (+185 °F) Operation +75 °C (+167 °F)	
Cold	EN 60068-2-1	Storage -40 °C (-40 °F) Operation -40 °C (-40 °F)	
Damp heat	EN 60068-2-78	95 % rel. humidity (+40 °C / +104 °F)	
Dry heat, cyclic	EN 60068-2-30	+55 °C (+131 °F) / +25 °C (+77 °F), 95 % rel. humidity, 12 h – 12 h	
Thermal shock / temp. variation	EN 60068-2-14	-40 °C (-40 °F) / +75 °C (+167 °F), 3 h/3 h, 2 cycles, 3 K/min	
Degrees of protection	EN 60529	IP30	
Vibration	EN 60068-2-64	Spectrum A.3 cat 1, breakpoints A.6 cat 1	
Shock	EN 60068-2-27	50 m/s^2, 11 ms, half sine, 10 in each direction	

ICR-1645

Phenomena	Test	Description	Test levels
ESD	EN 61000-4-2	Enclosure contact	± 8 kV (crit. B)
RF field AM modulated	EN 61000-4-3	Enclosure	3 V/m (crit. A) (80 – 1000 MHz)
Fast transient	EN 61000-4-4	Signal ports Power ports Ethernet ports	± 0.5 kV (crit. A)
Surge	EN 61000-4-5	Ethernet ports Power ports	± 0.5 kV (crit. B) ± 1 kV (crit. B) open circuit

Phenomena	Test	Description	Test levels	
RF conducted	EN 61000-4-6	All ports	3 V/m (crit. A) (0.15 – 80 MHz)	
Radiated emission	EN 55032	Enclosure	Class B	
Conducted emission	EN 55032	Signal ports Power ports Ethernet ports	Class B Class B Class B	
Dry heat	EN 60068-2-2	Storage +85 °C (+185 °F) Operation +75 °C (+167 °F)		~
Cold	EN 60068-2-1	Storage -40 °C (-40 °F) Operation -40 °C (-40 °F)		~
Damp heat	EN 60068-2-78	95 % rel. humidity (+40 °C / +104 °F)		~
Dry heat, cyclic	EN 60068-2-30	+55 °C (+131 °F) / +25 °C (+77 °F), 95 % rel. humidity, 12 h – 12 h		~
Thermal shock / temp. variation	EN 60068-2-14	-30 °C (-22 °F) / +75 °C (+167 °F), 3 h/3 h, 2 cycles, 3 K/min		~
Degrees of protection	EN 60529	IP30		~
Vibration	EN 60068-2-64	Spectrum A.3 cat 1, breakpoints A.6 cat 1		~
Shock	EN 60068-2-27	50 m/s^2, 11 ms, half sine, 10 in each direction		~

Cellular Module Parameters

ICR-16xx-EU Variant

Parameter	Description
Antenna	Connector type: SMA Input impedance: 50 Ω
LTE parameters	**LTE:** Cat.4, 3GPP Rel. 11 **FDD bands:** B1 (2100 MHz), B3 (1800 MHz), B7 (2600 MHz), B8 (900 MHz), B20 (800 MHz), B28A (700 MHz) **TDD bands:** B38 (2600 MHz), B40 (2300 MHz), B41 (2500 MHz) **Bit rates:** 150 Mbps (DL) / 50 Mbps (UL)
HSPA+/UMTS parameters	**Supported frequencies:** B8 (900 MHz), B1 (2100 MHz) **Bit rates:** 42 Mbps (DL) / 5.76 Mbps (UL)

Parameter	Description
EDGE/GPRS parameters	**Supported frequencies:** B8 (900 MHz), B3 (1800 MHz) **Bit rates:** 296 kbps (DL) / 236.8 kbps (UL)

ICR-16xx-CN Variant

Parameter	Description
Antenna	Connector type: SMA Input impedance: 50 Ω
LTE parameters	**LTE:** Cat.4, 3GPP Rel. 11 **FDD bands:** B1 (2100 MHz), B3 (1800 MHz), B5 (850 MHz), B8 (900 MHz) **TDD bands:** B34 (2000 MHz), B38 (2600 MHz), B39 (1900 MHz), B40 (2300 MHz), B41 (2500 MHz) **LTE FDD bit rates:** 150 Mbps (DL) / 50 Mbps (UL) **LTE TDD bit rates:** 130 Mbps (DL) / 30 Mbps (UL)
HSPA+/UMTS parameters	**WCDMA bands:** B1, B8 **WCDMA bit rates:** 384 kbps (DL/UL) **TD-SCDMA bands:** B34, B39 **TD-SCDMA bit rates:** 2.4 Mbps (DL) / 2.2 Mbps (UL)
EVDO/CDMA parameters	**CDMA:** 800 MHz **EVDO bit rates:** 3.1 Mbps (DL) / 1.8 Mbps (UL)
EDGE/GPRS parameters	**Supported frequencies:** EGSM 900 MHz, DCS 1800 MHz **GPRS bit rates:** 107 kbps (DL) / 85.6 kbps (UL) **EDGE bit rates:** 296 kbps (DL) / 236.8 kbps (UL)

GNSS Parameters

Tips

This section applies to ICR-16xxG models only.

Parameter	Description
GNSS Systems	GPS, Galileo, QZSS, GLONASS, BeiDou
Antenna	Connector type: SMA Input impedance: 50 Ω Supports active or passive antenna
Protocol	NMEA 0183

Parameter	Description
Frequency	GPS: 1575.42 ± 1.023 MHz Galileo: 1575.42 ± 2.046 MHz QZSS: 1575.42 MHz GLONASS: 1597.5 – 1605.8 MHz BeiDou: 1561.098 ± 2.046 MHz
Sensitivity (autonomous)	Acquisition: −146 dBm Reacquisition: −157 dBm Tracking: −157 dBm
Acquisition Time (autonomous)	Cold start: 35.0 s Warm start: 26.0 s Hot start: 2.5 s
Accuracy	2.5 m

Wi-Fi Parameters

Caution

The 5 GHz Wi-Fi interface operates in frequency bands (specifically 5150–5350 MHz) that are restricted to **indoor use only** in certain EU member states. Refer to the regulatory documentation for your router model for details.

Tips

This section applies to ICR-16xxW models only.

Parameter	Description
Antenna Connector	R-SMA — 50 Ω
Supported Wi-Fi Bands	2.400 – 2.4835 GHz 5.150 – 5.850 GHz
Standards	IEEE: 802.11b, 802.11b/g, 802.11b/g/n, 802.11a, 802.11a+n, 802.11ac
2.4 GHz Supported Channels	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
5 GHz Supported Channels	36, 40, 44, 48, 149, 153, 157, 161, 165
Type of Device	Access point (AP), Station (STA)
Security — Standards	WPA, WPA2, WPA3, 802.1X
Security — Encryption	WEP, TKIP, AES
AP Maximum Users	Up to 16 clients

I/O Parameters

> **Tips**
>
> *This section applies to ICR-1642 and ICR-1645. ICR-1602 does not include I/O or serial interfaces.*

The digital input status is available in the router's web interface (*General Status* page) and via the `status ports` and `io get` commands — refer to the Command Line Interface ↗ application note.

Characteristics of digital input:

`io get` **output**[1]	**Status**[2]
1	Open
0	Short to ISO_GND

[1] The digital status returned by the `io get` shell command.
[2] The digital status returned by the `status ports` shell command and displayed on the *General Status* page.

The maximum digital output load is **500 mA** at **48 V**.

Serial Interfaces

> **Tips**
>
> The RS232 and RS485 interfaces can be configured in *Expansion Port 1* and *Expansion Port 2*.

Parameter	Description
Baudrate	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps
Data Bits	5, 6, 7, 8
Parity	None, even, odd
Stop Bits	1, 2
Flow Control	None, CTS/RTS

System Configuration

Parameter	Description
CPU Architecture	ARM Cortex-A7
CPU Frequency	1.2 GHz
CPU Power	1.9 DMIPS/MHz
Flash Memory	512 MB NAND: • ~65 MB for Router Apps • ~26 MB for customer data
RAM	Total: 256 MB; available: ~160 MB
Watchdog	HW watchdog

404

Page not found

Looks like we've got some broken links.

Go back Take me home