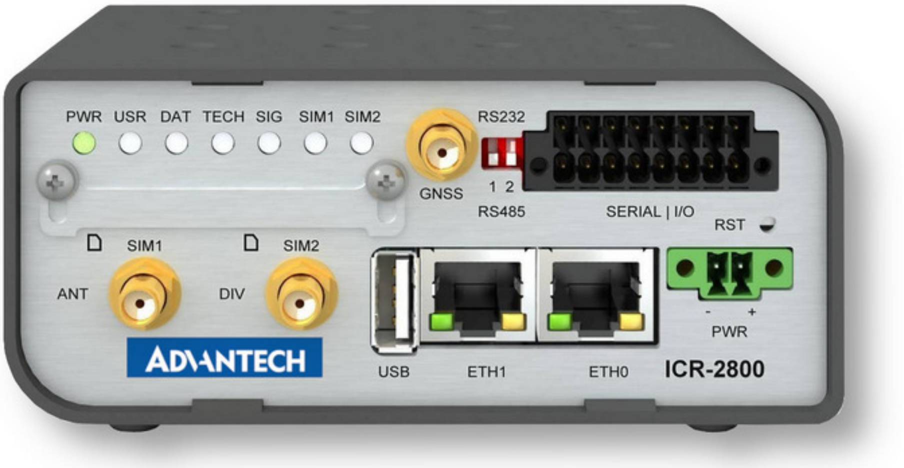
Configuration Manual

ICR-2[78]00 Family



Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0074-EN, revised on December 17, 2025.

Used symbols

Important

Important — Indicates a risk to personal safety or potential damage to the router. Follow these instructions precisely to prevent injury or equipment damage.

Warning

Warning — Highlights conditions that may cause malfunction, loss of data, or unexpected behavior in specific situations. Read carefully before proceeding.

Info

Info — Provides helpful tips, context, or references that improve understanding but are not strictly required to complete the task.

Code Example

```
Code Example - Copy-pasteable configuration snippets or CLI commands.
```

Firmware Version

This manual applies to firmware version **6.6.0 (December 17, 2025)**. Features introduced after this version may not be covered.

Contents

List of Figures

List of Tables

1. Getting Started

Important

To ensure a secure deployment, it is crucial to evaluate potential risks and configure the router to mitigate them. We strongly recommend consulting the *Security Guidelines* application note for fundamental security practices.

1.1 Document Contents

Info

This manual covers the standard (non-S1) router platform, identified by a green line at the top of the web interface, as shown in Figure 1.
For environments with stringent security requirements, a separate `S1 Router` platform is available. S1 models have a limited configuration set, are identified by an orange GUI line and an `-S1` part number suffix, and are covered in their own dedicated configuration manual.

This manual provides detailed setup instructions for Advantech ICR-2[78]00 routers, covering the following key areas:

- An overview of all available configuration environments, including the web interface, command line (SSH), and remote management platforms – detailed in Chapter *1.2 Configuration Environments*.
- Item-by-item descriptions of all settings, structured to match the web interface menu:
  - **Status Pages** – Chapter *2 Status*.
  - **Configuration Settings** – Chapter *3 Configuration*.
  - **Customization Options** – Chapter *4 Customization*.
  - **Administration Tools** – Chapter *5 Administration*.
- Configuration examples for typical use cases – Chapter *6 Typical Use Cases*.

Info

For hardware-related topics, such as product ordering codes, physical features, initial hardware setup, and technical specifications, please refer to the **Hardware Manual** available on the *Engineering Portal*.

1.2 Configuration Environments

Warning

Important Notes Before Configuration

- Before putting the router into operation, ensure all required hardware components (antennas, SIM cards, etc.) are properly connected. For detailed instructions, refer to the *Hardware Manual* for your specific model.
- For security reasons, always keep the router's firmware updated to the latest version. Do not downgrade to a version older than the factory release or upload firmware intended for a different model, as this can cause malfunctions.
- It is highly recommended to have JavaScript enabled in your web browser. Without it, some functions and most field validation checks will be disabled.
- Three consecutive failed login attempts will temporarily block web access from that IP address for one minute.
- All routers have the *WebAccess/DMP* client pre-installed. When activated, the client periodically sends router identifiers and configuration data to the server. For more details, see Chapter *1.2.2 Remote Management Platform*.
- If you are ever unsure about a configuration setting, please contact our technical support for assistance.

Info

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. For other fields, you may find contextual hints or examples.
- When you hover the mouse over an input field, a tooltip will appear showing the item's internal configuration name. This is particularly useful for scripting or remote configuration (e.g., via WebAccess/DMP).

Advantech routers can be configured using one of the following environments:

- **Web Browser:** A graphical user interface (GUI) accessible via HTTP(S). This is the primary method covered in this manual, beginning with Chapter *1.2.1 Web Interface Initial Setup*.
- **Command Line:** A console interface accessible via Secure Shell (SSH). For a detailed guide to all available commands, refer to the *Command Line Interface* Application Note.
- **Remote Management Platform:** Advantech's *WebAccess/DMP* platform allows for extensive remote management, monitoring, and mass configuration of routers. For more information, see Chapter *1.2.2 Remote Management Platform*.

For information on extending the router's functionality with custom scripts and applications, see the *Extending Router Functionality* Application Note.

1.2.1 Web Interface Initial Setup

Warning

Starting with firmware version 6.5.0, both IPv4 and IPv6 firewalls are enabled by default. Proper configuration of these settings is critical to avoid unintentionally blocking router communication during initial setup.

Info

- Users with the *User* role have read-only access to the web interface, except for the ability to change their own password. Certain menu items are not available 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 Chapter *3.22 Quick Setup* for details.

Advantech routers feature a secure, HTTPS-based Web GUI that provides access to all configuration and monitoring functions. The interface offers real-time network statistics, signal strength information, system log access, and comprehensive device management. To ensure secure communication, the Web GUI enforces TLS 1.2 or higher and requires certificate validation to prevent man-in-the-middle attacks.

Figure 1 shows the main elements of the interface, including the router identification header, the navigation menu, and the workspace where detailed configuration options are displayed. These clearly defined sections help users quickly locate system information, adjust operating parameters, and manage administrative settings.

To access the web interface for the first time on a factory-default router:

1. **Hardware Preparation:** For cellular models, insert an active SIM card. For detailed instructions, see the *Hardware Manual* for your specific model. Attach all required antennas before powering on the device and use only an Advantech-approved power supply as specified in the hardware documentation.

2. **Network Connection:** During boot-up, the router's DHCP server activates on the ETH0 interface. Connect your computer to this port and ensure it is configured to obtain an IP address automatically via DHCP. The router will assign your computer an IP address from the `192.168.1.0/24` range.

3. **Web Access:** Open a modern web browser and navigate to `https://192.168.1.1`. Note that unsecured HTTP connections are not permitted.

4. **Login Credentials:** The factory-default administrator account is `root` . The password for this account is printed on the router's product label[1].

5. **Initial Setup:** Upon your first login, you will be required to change the default password. The new password must meet the complexity requirements detailed in Chapter *3.19.1 Authentication*. You will then be automatically directed to the *Quick Setup* page to complete the initial configuration, as described in Chapter *3.22 Quick Setup*.

6. **Certificate Trust:** To avoid browser certificate warnings, it is recommended to install the router's self-signed certificate or upload a certificate from a trusted Certificate Authority (CA), as described in subsection *Managing HTTPS Certificates*.

[1] On older models where the label does not specify a password, the default is `root` .

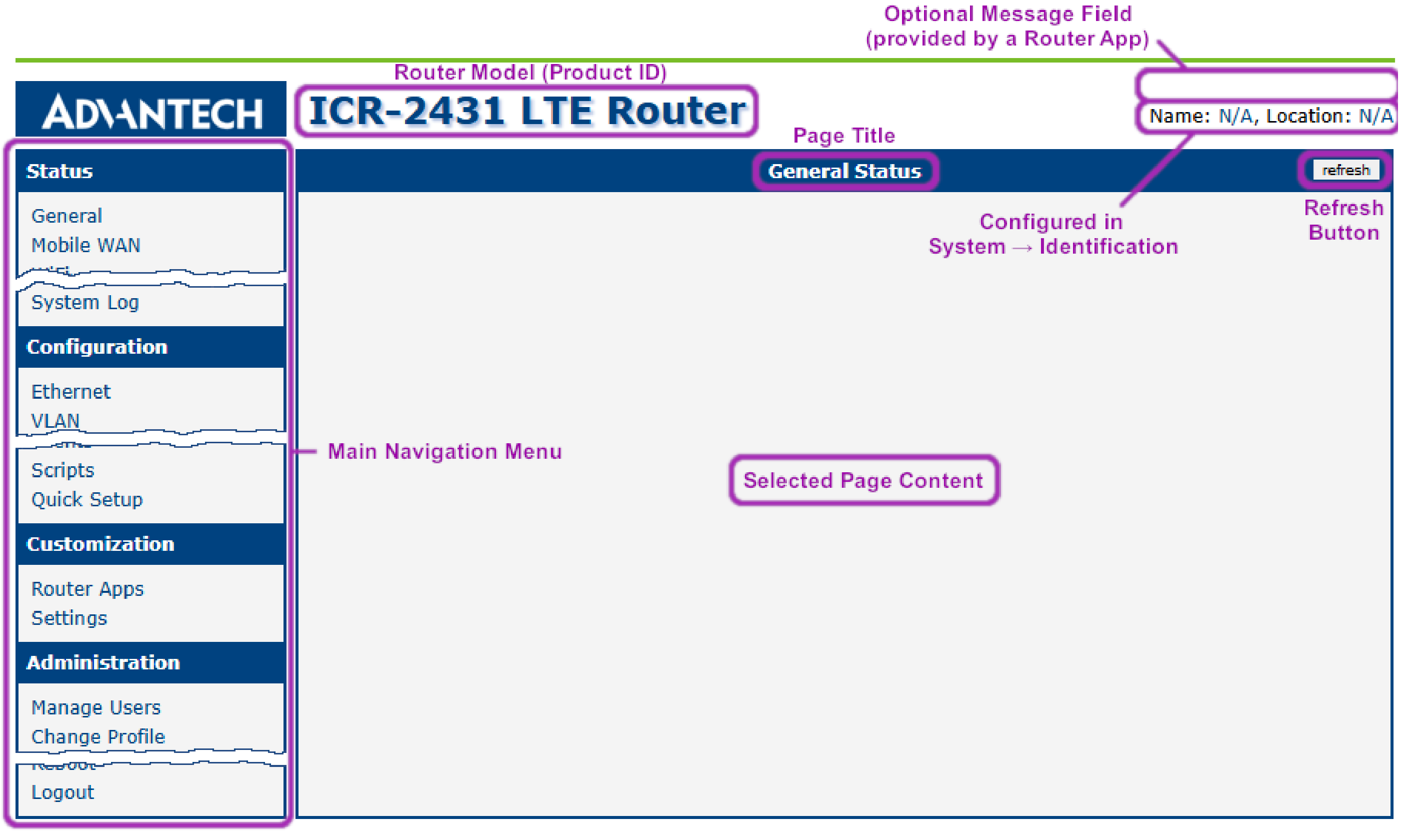


Figure 1: Web GUI layout overview

Managing HTTPS Certificates

By default, the router uses a self-signed HTTPS certificate. Because this certificate is not issued by a trusted Certificate Authority (CA), your web browser will display a security warning each time you access the web interface.

To avoid this warning, we recommend uploading a certificate signed by a trusted CA. This can be done on the *HTTP* configuration page, as described in Chapter *3.17.4 HTTP*. You will need to replace the `/etc/certs/https_cert` and `/etc/certs/https_key` files on the router.

As an alternative, you can add the router's self-signed certificate to your browser's or operating system's trust store. This will suppress the security warnings without needing a CA-signed certificate.

Allowed and Restricted Input Characters

When entering information into any configuration field in the web interface, it is important to use only permitted characters. Using forbidden characters can lead to unpredictable behavior or errors.

- **Allowed characters:** `0-9 a-z A-Z * , + - . / : = ? ! # % @ [ ] _ { } ~`
- **Forbidden characters:** ``" $ & ' ( ) ; < >  ^ ` |``

Warning

Although the system may allow you to save non-ASCII characters after confirming a warning message, using them, especially for passwords, is **not recommended** as it can cause compatibility issues with other systems.

Supported Certificate Formats

The web interface supports the following file formats for certificate and private key uploads:

- **Certificates (CA, Local, Remote):** `.pem` , `.crt` , `.p12`
- **Private Keys:** `.pem` , `.key` , `.p12`

Ensure that your files are in one of these formats to guarantee a successful upload.

1.2.2 Remote Management Platform

WebAccess/DMP is an advanced, cloud-based platform designed for the bulk management of Advantech routers and IoT gateways. It provides a centralized system for monitoring, configuring, and provisioning devices at scale. Key features include:

- Zero-touch provisioning for new device deployments.
- Mass configuration and firmware updates.
- Real-time status monitoring and alerts.
- Secure remote access to device web interfaces and command lines.

For more information, visit the official *WebAccess/DMP* website.

Client Configuration

The *WebAccess/DMP* client (Router App) is pre-installed and enabled by default in the standard (non-customized) router configuration. The connection to the server can be managed from several locations in the web interface:

- *Configuration* → *Quick Setup* (during initial setup or later)
- *Customization* → *Router Apps* → *WebAccess/DMP Client*

Warning

When the *WebAccess/DMP* client is enabled, the router will periodically upload its configuration and identifying information (such as MAC address and IMEI) to the management server.

1.3 Device

1.3.1 Persistent Storage

The device's persistent storage is divided into three main partitions:

- **System Data:** Contains the core operating system and firmware files.
- **User Data:** A separate partition for user-created files and data, accessible at `/var/data` .
- **Router Apps:** A dedicated partition for installed Router Apps, accessible at `/opt` .

1.3.2 Reset Procedures

Warning

Before performing any reset that restores factory defaults, it is highly recommended to back up your current configuration. See Chapter *5.7 Backup Configuration* for instructions.

The router offers three distinct reset procedures to handle different scenarios. The method for initiating these resets varies based on the router model.

- **Reboot (Software Reset):** This action simply restarts the router, keeping the currently saved configuration. It can be triggered from the *Reboot* page in the web interface. On models with an *RST* button, a brief press of **less than 4 seconds** also initiates a reboot.

- **Configuration Reset (Factory Reset):**[1] This procedure restores the router to its original factory settings, including all router and Router App configurations.

  ○ On models with a multi-function *RST* button, press and hold it for **more than 4 seconds**. The *PWR* LED will cycle off and on to indicate success.

- **Emergency Reset:**[1] This is a recovery procedure for situations where the router fails to boot, often due to a configuration error or filesystem issue. It resets all configurations to factory defaults.

  ○ Disconnect the router from its power source.

  ○ Press and hold the *RST* button.

  ○ While still holding the button, reconnect the power and continue holding for **at least 10 seconds**.

The following table summarizes how each reset procedure affects the data stored on the router.

Storage	Reset	Configuration Reset	Emergency Reset
Router and Router App 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

Table 1: Reset storage actions

[1] Upon first login after a reset, the user will be prompted to change their password.

2. Status

Info

All status pages can display live data. To enable this feature, click the *refresh* button in the top-right corner of the page. To stop the automatic updates and reduce data transfer, click the *pause* button.

2.1 General

The *Status* → *General* page provides a summary of the router's basic information and current activities. The content is divided into sections based on the router's hardware configuration and may include status information for the mobile connection, LAN interfaces, system details, Wi-Fi, and peripheral ports.

Info

An IPv6 interface can have multiple addresses simultaneously. If you click *More Information*, you may see an additional IPv6 address in the EUI-64 format. This is a link-local address, automatically generated from the interface's MAC address, and is standard behavior for IPv6.

Mobile Connection

This section displays real-time status and traffic statistics for the active mobile WAN connection.

Item	Description
SIM Card	The currently active SIM card (1st or 2nd).
Interface	The name of the network interface (e.g., `usb0`).
Flags	The current status flags for the interface: • **Up**: The interface is administratively enabled. • **Running**: The interface is operational and connected. • **Multicast**: The interface supports multicast traffic.
IP Address	The IP address assigned to the interface by the mobile operator.
MTU	Maximum Transmission Unit: the largest packet size (in bytes) that can be transmitted over the interface.
Rx Data / *Tx Data*	The total amount of data received (Rx) and transmitted (Tx).
Rx Packets / *Tx Packets*	The total number of packets received (Rx) and transmitted (Tx).
Rx Errors / *Tx Errors*	The number of packets with errors (e.g., failed checksums) during reception (Rx) or transmission (Tx).
Rx Dropped / *Tx Dropped*	The number of packets that were dropped, likely due to a lack of system resources (e.g., full buffers).
Rx Overruns / *Tx Overruns*	The number of packets lost because the hardware buffer was full before the system could process the previous packet.
Uptime	The duration of the current, active mobile network connection.

Table 2: Mobile connection status items

Ethernet

Each physical Ethernet port (e.g., `eth0`, `eth1`) has a dedicated section on the *General* status page.

Item	Description
Interface	The name of the network interface (e.g., `eth0`).
Flags	The current status flags for the interface (see Table 2 for details).
IP Address	The IPv4 address configured for this interface.
IPv6 Address	The IPv6 address configured for this interface.
MAC Address	The unique Media Access Control (MAC) address of the hardware interface.
MTU	The Maximum Transmission Unit for the interface.
Rx Data / Tx Data	The total amount of data received (Rx) and transmitted (Tx).
Rx Packets / Tx Packets	The total number of packets received (Rx) and transmitted (Tx).
Rx Errors / Tx Errors	The number of packets with errors during reception (Rx) or transmission (Tx).
Rx Dropped / Tx Dropped	The number of packets dropped due to resource limitations.
Rx Overruns / Tx Overruns	The number of packets lost due to hardware buffer overruns.

Table 3: Ethernet status items

Peripheral Ports

Info

Available only for ICR-2834 model.

This section displays the status of all installed peripheral ports on the router.

Item	Description
Expansion Port 1	The interface detected on the first expansion port.
Expansion Port 2	The interface detected on the second expansion port.
Digital Input 0	The current state of the first digital input.
Digital Input 1	The current state of the second digital input.
Digital Input 2	The current state of the third digital input.
Digital Input 3	The current state of the fourth digital input.
Digital Output 0	The current state of the first digital output.
Digital Output 1	The current state of the second digital output.

Table 4: Peripheral port status description

To understand the specific voltage levels that trigger the states returned by the `status ports` or `io get` commands, refer to the *Parameters of I/O Ports* chapter in the Hardware Manual. Please note that these specifications may vary for different router platforms.

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.

Table 5: 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 from the list is being used in the position calculation (Y for Yes, N for No).

Table 6: 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.
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	The version of the firmware currently installed on the router.
Serial Number	The unique serial number of the device.
Hardware UUID[1]	A permanent, non-changeable Unique Hardware Identifier for the device.
Product Revision[1]	The manufacturing revision number of the router's hardware.
Profile	The currently active configuration profile (e.g., Standard or an alternative profile).
Free Space	The amount of available storage for Router Apps and user data.
CPU Usage	The current processor load, shown as a percentage. Enable auto-refresh to see live data.
Memory Usage	The current RAM usage, shown as a percentage. Enable auto-refresh to see live data.
Supply Voltage	The current input voltage being supplied to the router.
Temperature	The internal temperature of the router.
Time	The current system date and time.
Uptime	The total time elapsed since the router was last rebooted.
Licenses	A link to a list of open-source software components used in the firmware, along with their respective licenses.

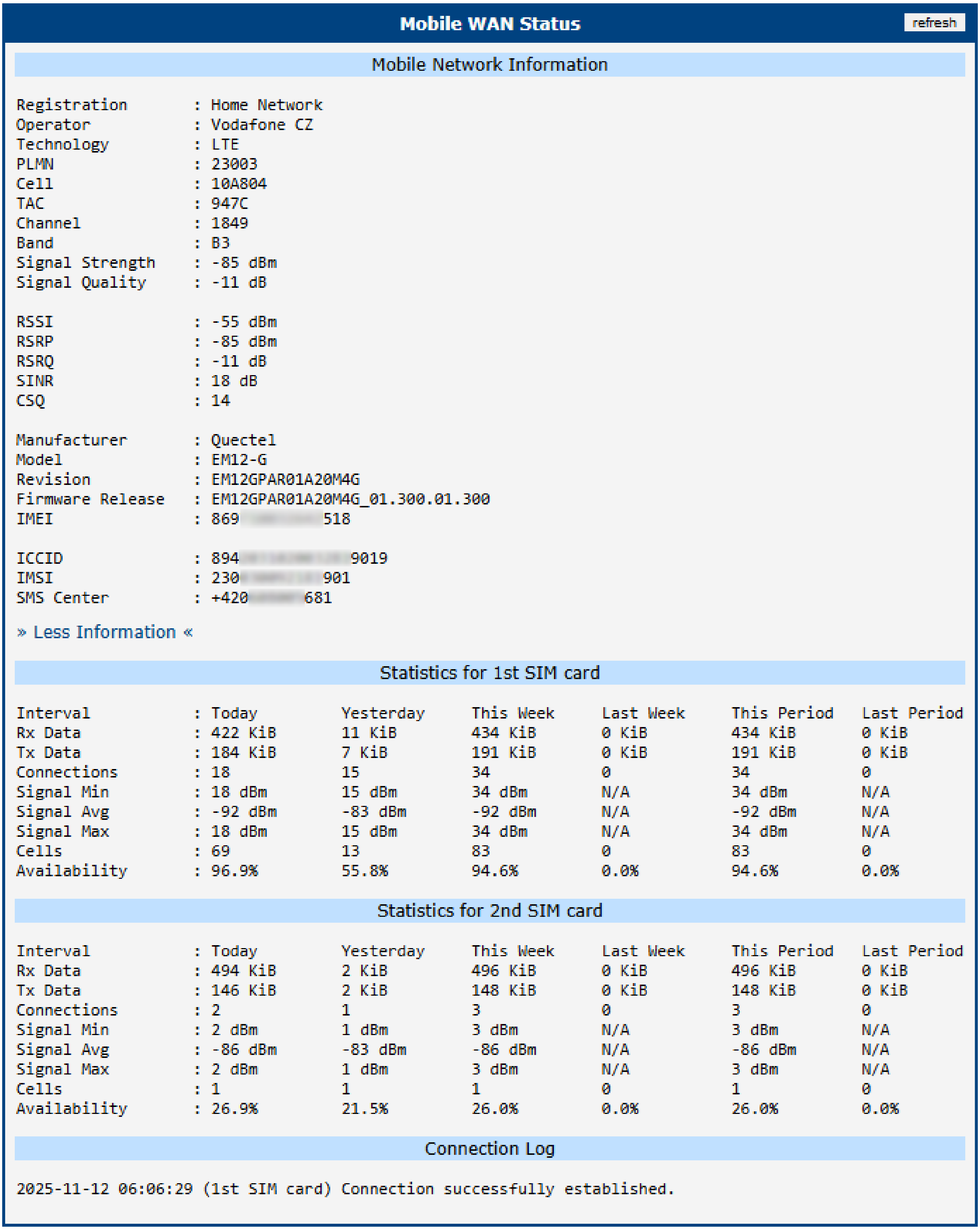
Table 7: System information items

[1] This item may not be available on all router models.

[2] Visible only on models equipped with a PoE expansion board.

2.2 Mobile WAN

The *Status* → *Mobile WAN* page provides a comprehensive, real-time overview of the router's cellular connection. It is divided into three main sections: Mobile Network Information, Connection Statistics, and a detailed Connection Log.



Mobile Network Information

```
Registration        : Home Network
Operator            : Vodafone CZ
Technology          : LTE
PLMN                : 23003
Cell                : 10A804
TAC                 : 947C
Channel             : 1849
Band                : B3
Signal Strength     : -85 dBm
Signal Quality      : -11 dB

RSSI                : -55 dBm
RSRP                : -85 dBm
RSRQ                : -11 dB
SINR                : 18 dB
CSQ                 : 14

Manufacturer        : Quectel
Model               : EM12-G
Revision            : EM12GPAR01A20M4G
Firmware Release    : EM12GPAR01A20M4G_01.300.01.300
IMEI                : 869[redacted]518

ICCID               : 894[redacted]9019
IMSI                : 230[redacted]901
SMS Center          : +420[redacted]681
```

» Less Information «

Statistics for 1st SIM card

```
Interval            : Today      Yesterday   This Week   Last Week   This Period  Last Period
Rx Data             : 422 KiB    11 KiB      434 KiB     0 KiB       434 KiB      0 KiB
Tx Data             : 184 KiB    7 KiB       191 KiB     0 KiB       191 KiB      0 KiB
Connections         : 18         15          34          0           34           0
Signal Min          : 18 dBm     15 dBm      34 dBm      N/A         34 dBm       N/A
Signal Avg          : -92 dBm    -83 dBm     -92 dBm     N/A         -92 dBm      N/A
Signal Max          : 18 dBm     15 dBm      34 dBm      N/A         34 dBm       N/A
Cells               : 69         13          83          0           83           0
Availability        : 96.9%      55.8%       94.6%       0.0%        94.6%        0.0%
```

Statistics for 2nd SIM card

```
Interval            : Today      Yesterday   This Week   Last Week   This Period  Last Period
Rx Data             : 494 KiB    2 KiB       496 KiB     0 KiB       496 KiB      0 KiB
Tx Data             : 146 KiB    2 KiB       148 KiB     0 KiB       148 KiB      0 KiB
Connections         : 2          1           3           0           3            0
Signal Min          : 2 dBm      1 dBm       3 dBm       N/A         3 dBm        N/A
Signal Avg          : -86 dBm    -83 dBm     -86 dBm     N/A         -86 dBm      N/A
Signal Max          : 2 dBm      1 dBm       3 dBm       N/A         3 dBm        N/A
Cells               : 1          1           1           0           1            0
Availability        : 26.9%      21.5%       26.0%       0.0%        26.0%        0.0%
```

Connection Log

```
2025-11-12 06:06:29 (1st SIM card) Connection successfully established.
```

Figure 2: Mobile WAN status page

Mobile Network Information

This section displays detailed information about the current network connection and the cellular module.

Item	Description
Network Parameters	
Registration	The current registration status on the mobile network (e.g., Registered, Home Network; Registered, Roaming).
Operator	The name of the currently connected mobile network operator.
Technology	The cellular technology in use (e.g., 5G, LTE, UMTS, GPRS).
PLMN	The Public Land Mobile Network code, a unique identifier for the mobile operator.
Cell	The hexadecimal ID of the cell tower to which the router is currently connected.
LAC/TAC	The Location Area Code (for 2G/3G) or Tracking Area Code (for 4G/5G), which identifies the current location area of the device within the network.
Channel	The specific radio frequency channel number being used (e.g., ARFCN, UARFCN, EARFCN).
Band	The frequency band being used for the connection (e.g., LTE Band 20).
Signal Quality	
Signal Strength	The primary signal strength metric (RSCP for UMTS, RSRP for LTE/5G, RSSI for GPRS). The value is color-coded for quick assessment: good (black), fair (orange), or poor (red). See Table 9 for detailed ranges.
Signal Quality	The primary signal quality metric (EC/IO for UMTS, RSRQ for LTE/5G). Not available for GPRS/EDGE.
RSSI, RSRP, RSRQ, SINR	Additional signal metrics providing deeper insight into connection quality. Availability depends on the module and technology.
CSQ	A simplified signal quality indicator from 0 to 31, where a higher value indicates better signal.
Neighbours	A list of neighboring cell signals, which can be useful for diagnostics (available only in GPRS mode on certain models).
Module Information	
Manufacturer, Model, Revision	Identifying details for the installed cellular module.
Firmware Release	Displays the full version string of the firmware currently running on the cellular module. This identifier is used for managing Firmware Over-The-Air (FOTA) updates for the module itself.
IMEI / MEID	The unique identifier for the cellular module hardware.
ICCID	The unique serial number of the inserted SIM card.
IMSI	The International Mobile Subscriber Identity, a unique number that identifies the SIM card on the mobile network.
SMS Center	The phone number of the Short Message Service Center (SMSC) provided by the mobile operator.

Table 8: Mobile network information details

The following table provides a general guide for interpreting signal strength values.

Signal Level	2G/3G (RSSI/RSCP)	4G (RSRP)	5G (RSRP)
Good	> -75 dBm	> -90 dBm	> -90 dBm
Fair	-75 dBm to -94 dBm	-90 dBm to -109 dBm	-90 dBm to -119 dBm
Poor	< -94 dBm	< -109 dBm	< -119 dBm

Table 9: Signal strength value ranges

Connection Statistics

This section provides usage and performance data for each SIM card over various time periods. The accounting periods can be customized on the *Configuration* → *Mobile WAN* page.

Item	Description
RX / TX data	The total volume of data received (RX) and transmitted (TX).
Connections	The total number of successful network connections.
Signal Min / Avg / Max	The minimum, average, and maximum signal strength recorded. Hovering over the Min/Max values will display a timestamp of their last occurrence.
Cells	The number of times the router has switched between cell towers.
Availability	The percentage of time the router has been successfully connected to the network since the SIM was activated.

Table 10: Mobile network statistics details

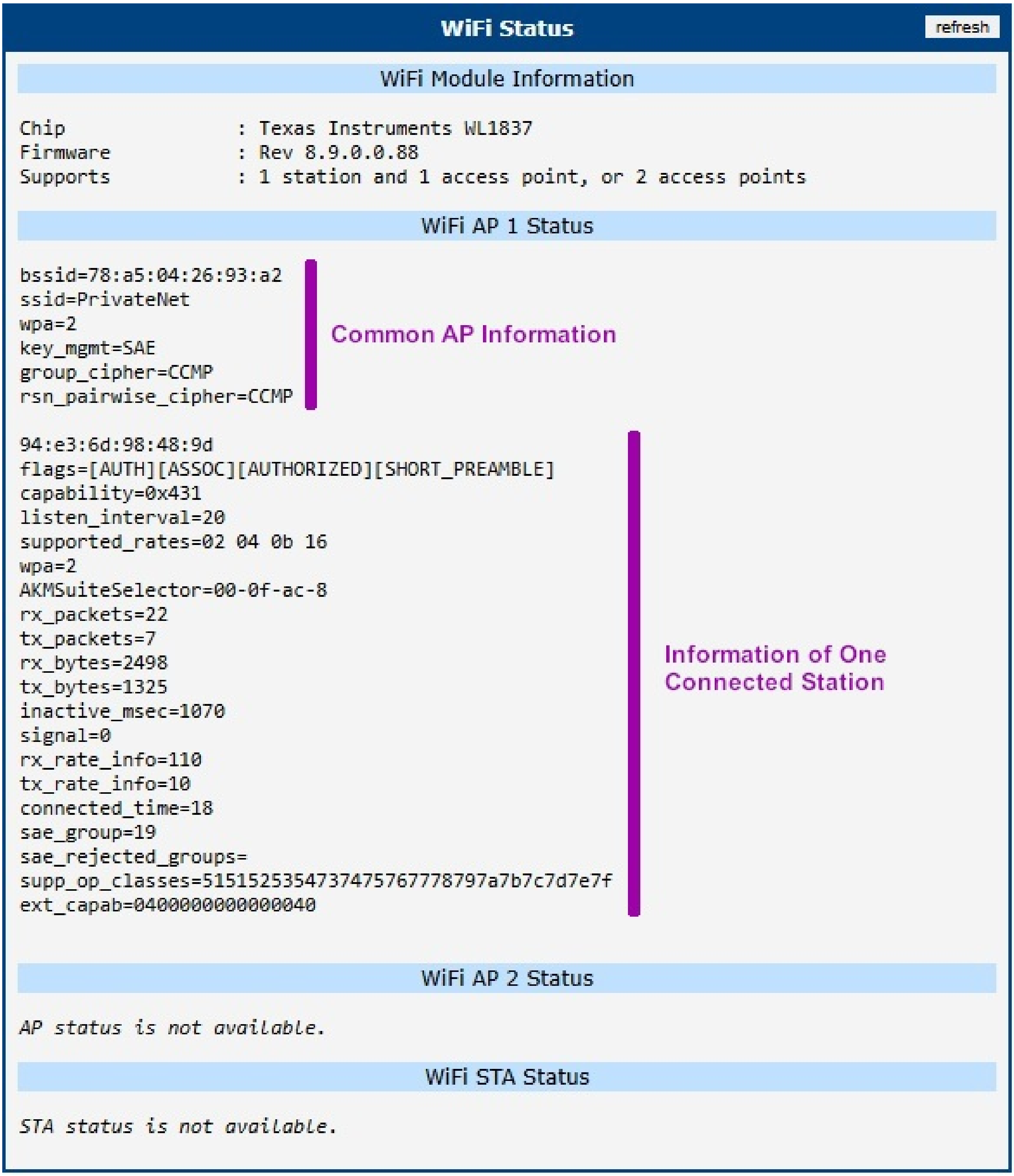
Connection Log

This section displays a detailed, real-time log of events related to the mobile network connection. It is an invaluable tool for troubleshooting, as it records the step-by-step process of network registration and clearly indicates any errors encountered.

2.3 Wi-Fi

2.3.1 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.



WiFi Module Information

```
Chip                 : Texas Instruments WL1837
Firmware             : Rev 8.9.0.0.88
Supports             : 1 station and 1 access point, or 2 access points
```

WiFi AP 1 Status

```
bssid=78:a5:04:26:93:a2
ssid=PrivateNet
wpa=2
key_mgmt=SAE
group_cipher=CCMP
rsn_pairwise_cipher=CCMP

94:e3:6d:98:48:9d
flags=[AUTH][ASSOC][AUTHORIZED][SHORT_PREAMBLE]
capability=0x431
listen_interval=20
supported_rates=02 04 0b 16
wpa=2
AKMSuiteSelector=00-0f-ac-8
rx_packets=22
tx_packets=7
rx_bytes=2498
tx_bytes=1325
inactive_msec=1070
signal=0
rx_rate_info=110
tx_rate_info=10
connected_time=18
sae_group=19
sae_rejected_groups=
supp_op_classes=5151525354737475767778797a7b7c7d7e7f
ext_capab=0400000000000040
```

WiFi AP 2 Status

AP status is not available.

WiFi STA Status

STA status is not available.

Figure 3: Wi-Fi AP status page

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.

Table 11: Wi-Fi module information

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. As shown in Figure 3, 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 table below.

Column/Item	Description
Common AP Information	
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	
[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).

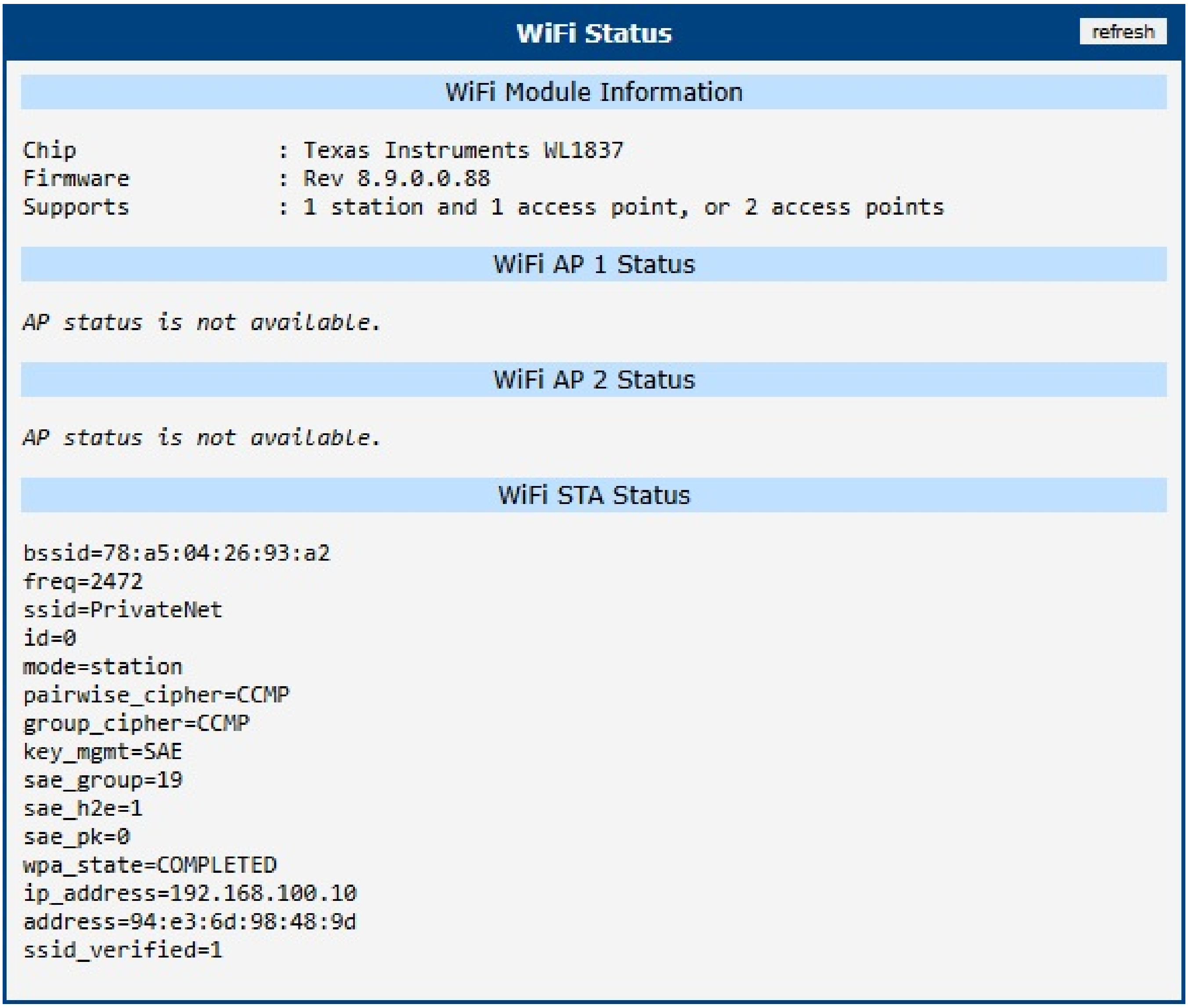
Table 12: Wi-Fi AP status details

Item	Description
rx_packets	Number of packets received from this station.
tx_packets	Number of packets transmitted to this station.
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.

Table 12: (continued)

Wi-Fi STA Status

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



```
Chip                   : Texas Instruments WL1837
Firmware               : Rev 8.9.0.0.88
Supports               : 1 station and 1 access point, or 2 access points
```

```
AP status is not available.
```

```
AP status is not available.
```

```
bssid=78:a5:04:26:93:a2
freq=2472
ssid=PrivateNet
id=0
mode=station
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=SAE
sae_group=19
sae_h2e=1
sae_pk=0
wpa_state=COMPLETED
ip_address=192.168.100.10
address=94:e3:6d:98:48:9d
ssid_verified=1
```

Figure 4: Wi-Fi STA status page

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*).

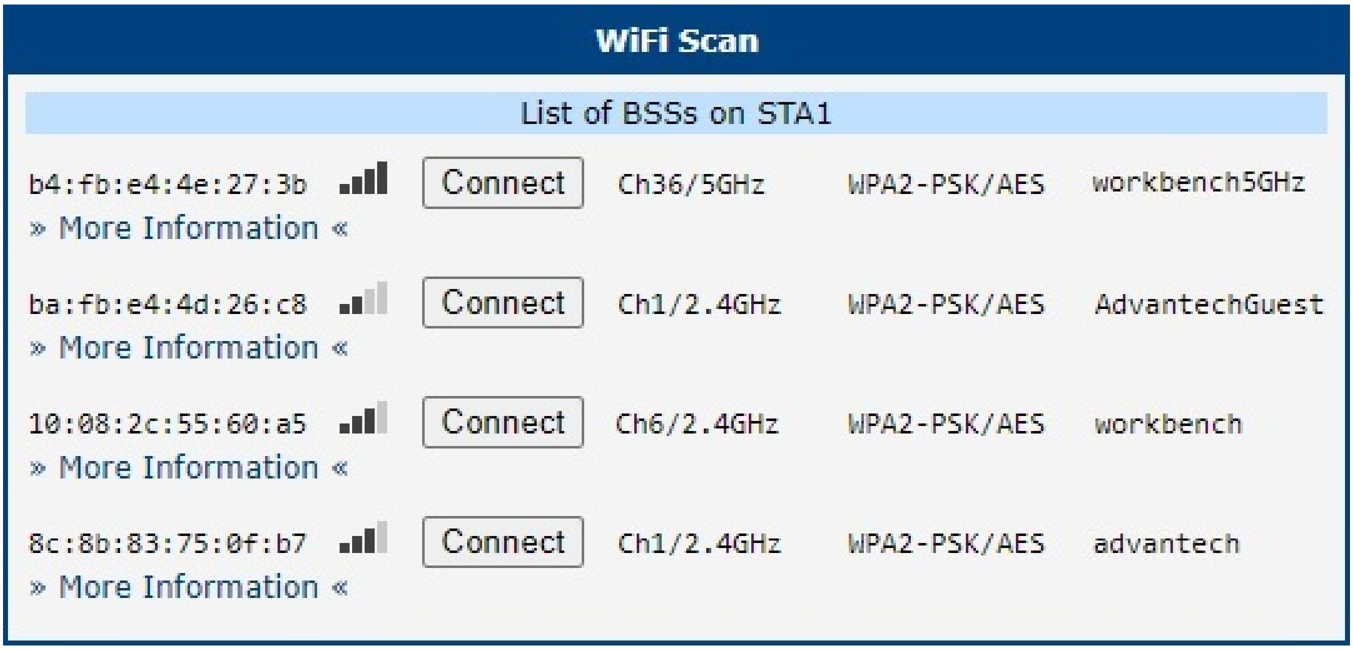
Table 13: Wi-Fi STA status details

Item	Description
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.
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.

Table 13: (continued)

2.3.2 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.



WiFi Scan

List of BSSs on STA1

b4:fb:e4:4e:27:3b » More Information «	▂▄▆█	Connect	Ch36/5GHz	WPA2-PSK/AES	workbench5GHz
ba:fb:e4:4d:26:c8 » More Information «	▂▄	Connect	Ch1/2.4GHz	WPA2-PSK/AES	AdvantechGuest
10:08:2c:55:60:a5 » More Information «	▂▄▆	Connect	Ch6/2.4GHz	WPA2-PSK/AES	workbench
8c:8b:83:75:0f:b7 » More Information «	▂▄▆	Connect	Ch1/2.4GHz	WPA2-PSK/AES	advantech

Figure 5: Wi-Fi scan results

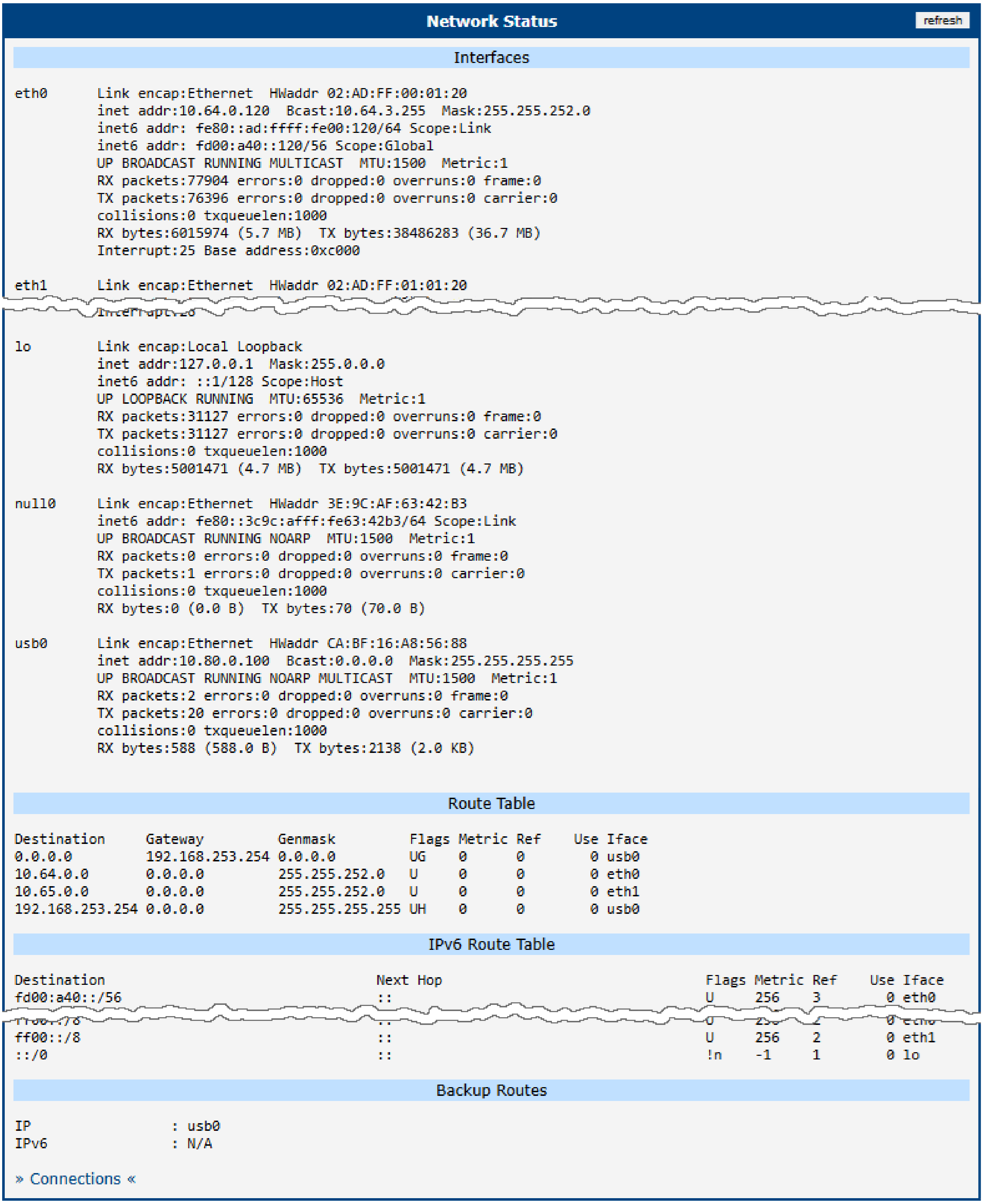
The list is structured into several columns, and each entry provides a *Connect* button and a link to view *More Information*.

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

Table 14: Wi-Fi scan results description

2.4 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.



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:26

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

```
IP                  : usb0
IPv6                : N/A
```

» Connections «

Figure 6: Network status page overview

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 (received and transmitted data). 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
ethX	A physical Ethernet interface directly connected to the CPU. The index *X* identifies the interface instance (e.g., *eth0*, *eth1*).
vlanX	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.
wlanX	A Wi-Fi interface, where *X* identifies the physical radio or a virtual access point instance.
pppoeX	A virtual interface for a PPPoE session, where *X* is the instance number.
tunX	A virtual interface for an OpenVPN tunnel, where *X* is the tunnel instance number (0–3).
ipsecX	A virtual interface for an IPsec tunnel, where *X* is the tunnel instance number (0–3).
wgX	A virtual interface for a WireGuard tunnel, where *X* is the tunnel instance number (0–3).
greX	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.

Table 15: Common interface types

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

Parameter	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.
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).

Table 16: Interface parameter descriptions

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 (in *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*, as shown in Figure 6.

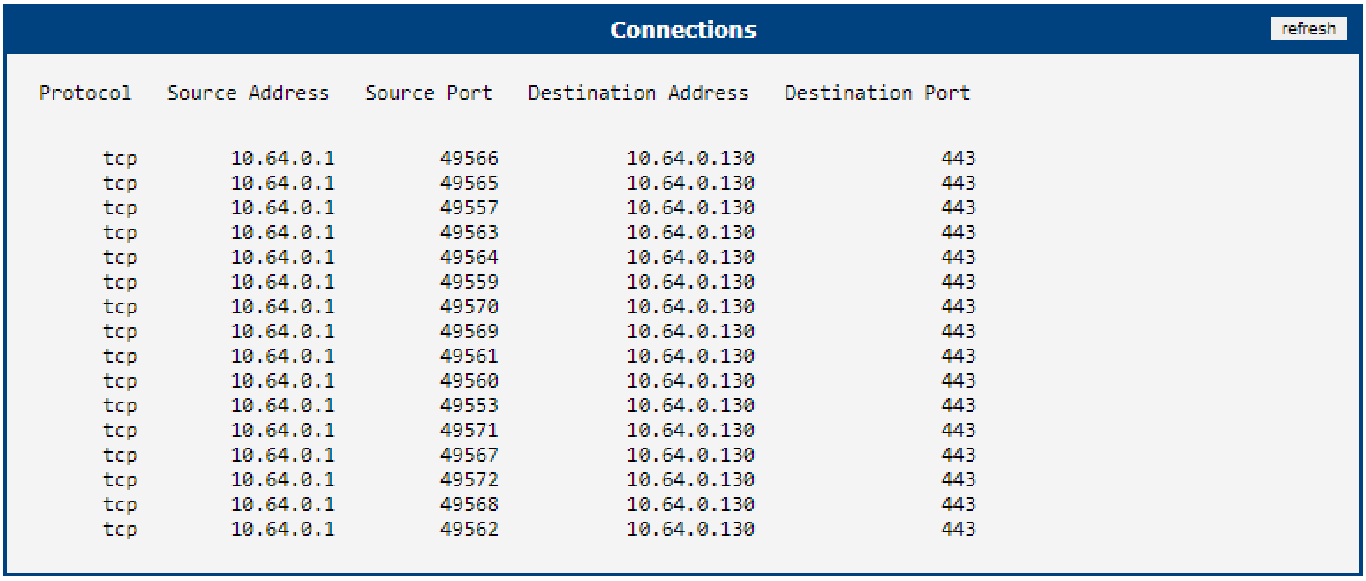
Backup Routes

This section identifies the active primary WAN interface for both IPv4 and IPv6 Internet traffic. The status shown here directly reflects the router's automatic failover system (detailed in Chapter *3.7 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.

- **IP** – Displays the interface currently providing the primary outbound path for all IPv4 traffic. This field shows *N/A* if no IPv4 WAN connection is currently active.
- **IPv6** – Displays the interface currently providing the primary outbound path for all IPv6 traffic. This field shows *N/A* if no IPv6 WAN connection is currently active.

Connections

At the bottom of the *Network Status* page, click the > *Connections* < link to open a new window that lists all active connections passing through the router.



```
Protocol   Source Address   Source Port   Destination Address   Destination Port

     tcp        10.64.0.1         49566         10.64.0.130                443
     tcp        10.64.0.1         49565         10.64.0.130                443
     tcp        10.64.0.1         49557         10.64.0.130                443
     tcp        10.64.0.1         49563         10.64.0.130                443
     tcp        10.64.0.1         49564         10.64.0.130                443
     tcp        10.64.0.1         49559         10.64.0.130                443
     tcp        10.64.0.1         49570         10.64.0.130                443
     tcp        10.64.0.1         49569         10.64.0.130                443
     tcp        10.64.0.1         49561         10.64.0.130                443
     tcp        10.64.0.1         49560         10.64.0.130                443
     tcp        10.64.0.1         49553         10.64.0.130                443
     tcp        10.64.0.1         49571         10.64.0.130                443
     tcp        10.64.0.1         49567         10.64.0.130                443
     tcp        10.64.0.1         49572         10.64.0.130                443
     tcp        10.64.0.1         49568         10.64.0.130                443
     tcp        10.64.0.1         49562         10.64.0.130                443
```

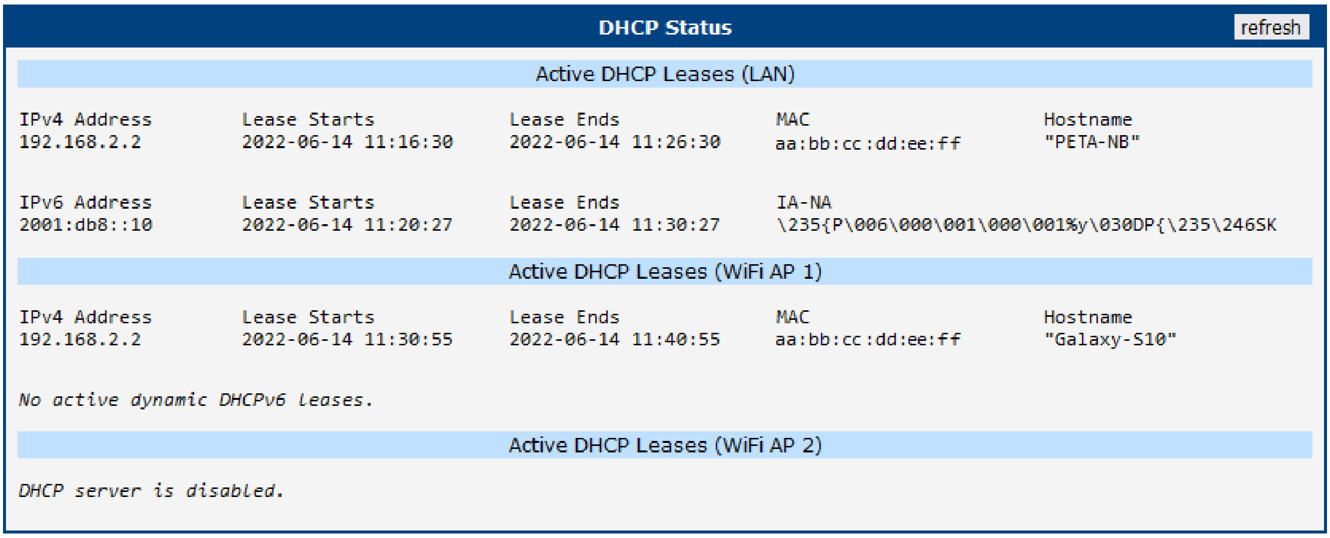
Figure 7: List of active network connections

Column	Description
Protocol	The transport protocol used (e.g., TCP, UDP).
Source Address	The original IP address of the connection.
Source Port	The original source port of the connection.
Destination Address	The final IP address of the connection.
Destination Port	The final destination port of the connection.

Table 17: Description of columns in the connections list

2.5 DHCP

To view information about DHCP server activity, navigate to *Status* → *DHCP*. The router's DHCP server automatically provides network configuration to client devices. For each client, it assigns an IP address, subnet mask, default gateway, and DNS server. The router supports both DHCPv4 and DHCPv6 servers. The *DHCP Status* page lists all active IP address leases, grouped by the interface they are associated with (e.g., *LAN*, *WiFi AP 1*). If no leases are active on an interface or the server is disabled for that interface, a corresponding message is displayed.



Active DHCP Leases (LAN)

```
IPv4 Address        Lease Starts          Lease Ends            MAC                   Hostname
192.168.2.2         2022-06-14 11:16:30   2022-06-14 11:26:30   aa:bb:cc:dd:ee:ff     "PETA-NB"

IPv6 Address        Lease Starts          Lease Ends            IA-NA
2001:db8::10        2022-06-14 11:20:27   2022-06-14 11:30:27   \235{P\006\000\001\000\001%y\030DP{\235\246SK
```

Active DHCP Leases (WiFi AP 1)

```
IPv4 Address        Lease Starts          Lease Ends            MAC                   Hostname
192.168.2.2         2022-06-14 11:30:55   2022-06-14 11:40:55   aa:bb:cc:dd:ee:ff     "Galaxy-S10"

No active dynamic DHCPv6 leases.
```

Active DHCP Leases (WiFi AP 2)

```
DHCP server is disabled.
```

Figure 8: DHCP status page

The table below describes the information provided for each active lease.

Column	Description
IPv4 Address	The IPv4 address assigned to the client.
IPv6 Address	The IPv6 address assigned to the client.
Lease Starts	The date and time when the IP address lease began.
Lease Ends	The date and time when the IP address lease will expire.
MAC	The unique MAC address of the client device (applies to IPv4 leases).
Hostname	The hostname of the client device (applies to IPv4 leases).
IA-NA	Identity Association for Non-temporary Addresses. A unique DHCPv6 identifier for the client's address assignment (applies to IPv6 leases).

Table 18: DHCP status column descriptions

Info

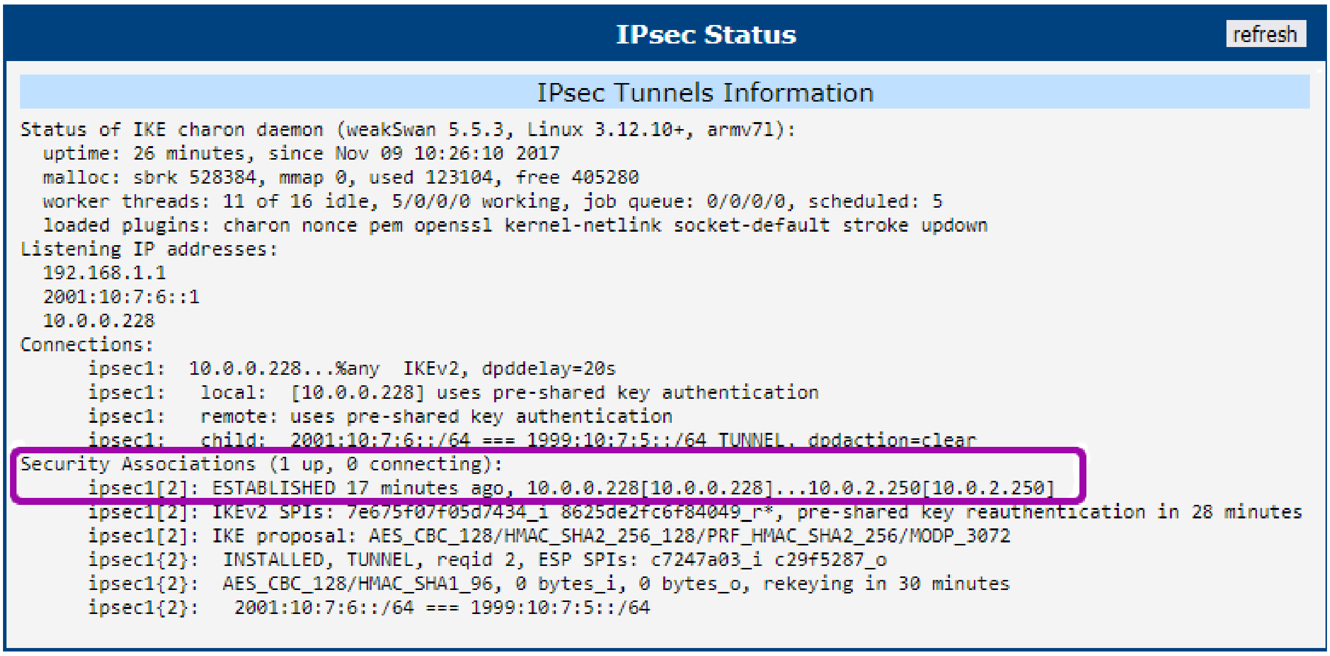
The DHCP status may occasionally display two records for one IP address. This can be caused by a client's network interface being reset.

2.6 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.

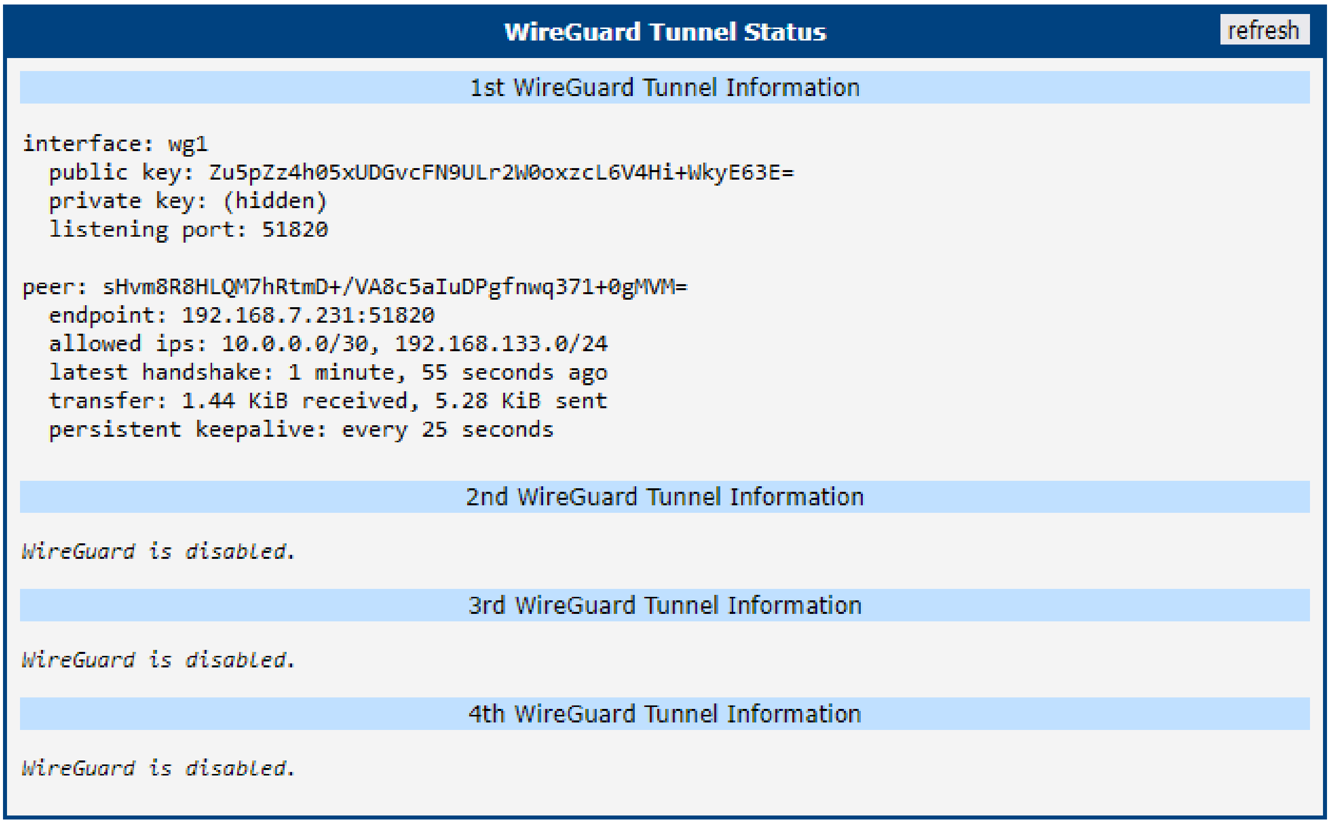


```
Status of IKE charon daemon (weakSwan 5.5.3, Linux 3.12.10+, armv7l):
  uptime: 26 minutes, since Nov 09 10:26:10 2017
  malloc: sbrk 528384, mmap 0, used 123104, free 405280
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
  loaded plugins: charon nonce pem openssl kernel-netlink socket-default stroke updown
Listening IP addresses:
  192.168.1.1
  2001:10:7:6::1
  10.0.0.228
Connections:
      ipsec1:  10.0.0.228...%any  IKEv2, dpddelay=20s
      ipsec1:   local:  [10.0.0.228] uses pre-shared key authentication
      ipsec1:   remote: uses pre-shared key authentication
      ipsec1:   child:  2001:10:7:6::/64 === 1999:10:7:5::/64 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
      ipsec1[2]: ESTABLISHED 17 minutes ago, 10.0.0.228[10.0.0.228]...10.0.2.250[10.0.2.250]
      ipsec1[2]: IKEv2 SPIs: 7e675f07f05d7434_i 8625de2fc6f84049_r*, pre-shared key reauthentication in 28 minutes
      ipsec1[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
      ipsec1{2}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: c7247a03_i c29f5287_o
      ipsec1{2}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 30 minutes
      ipsec1{2}:   2001:10:7:6::/64 === 1999:10:7:5::/64
```

Figure 9: IPsec status

2.7 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.



1st WireGuard Tunnel Information

```
interface: wg1
  public key: Zu5pZz4h05xUDGvcFN9ULr2W0oxzcL6V4Hi+WkyE63E=
  private key: (hidden)
  listening port: 51820

peer: sHvm8R8HLQM7hRtmD+/VA8c5aIuDPgfnwq371+0gMVM=
  endpoint: 192.168.7.231:51820
  allowed ips: 10.0.0.0/30, 192.168.133.0/24
  latest handshake: 1 minute, 55 seconds ago
  transfer: 1.44 KiB received, 5.28 KiB sent
  persistent keepalive: every 25 seconds
```

2nd WireGuard Tunnel Information

WireGuard is disabled.

3rd WireGuard Tunnel Information

WireGuard is disabled.

4th WireGuard Tunnel Information

WireGuard is disabled.

Figure 10: 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.

Table 19: WireGuard status parameter descriptions

2.8 DynDNS

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

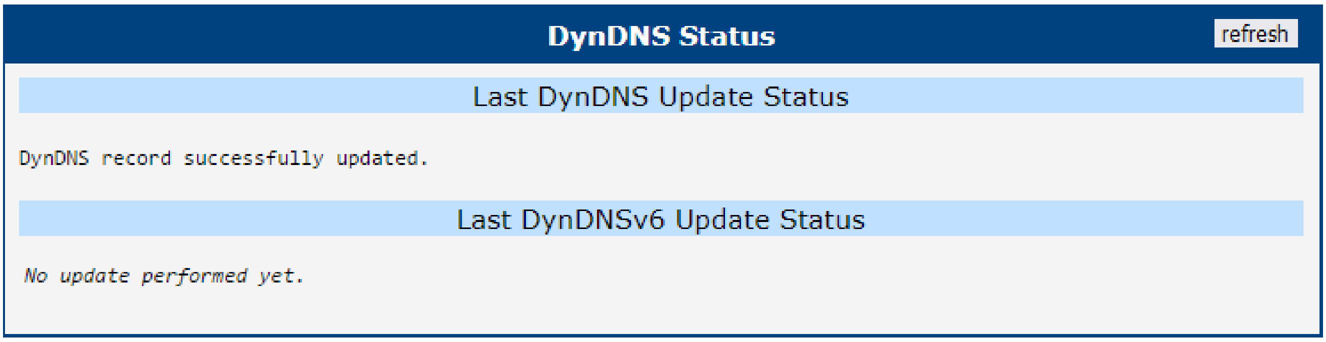
Warning

For the DynDNS 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 DynDNS providers. You can configure the service to use one of the following:

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

DynDNSv6 can be used when *IP Mode* is set to *IPv6* on the *Services* → *DynDNS* configuration page. The status page displays messages that indicate the current state of the DynDNS client and its communication with the provider.



Last DynDNS Update Status

```
DynDNS record successfully updated.
```

Last DynDNSv6 Update Status

```
No update performed yet.
```

Figure 11: DynDNS status page

The table below lists the possible messages you may encounter.

Status Message
DynDNS 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 yet.
DynDNS record is already up to date.
DynDNS record successfully updated.
DNS error encountered.
DynDNS server failure.

Table 20: DynDNS status messages

2.9 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.

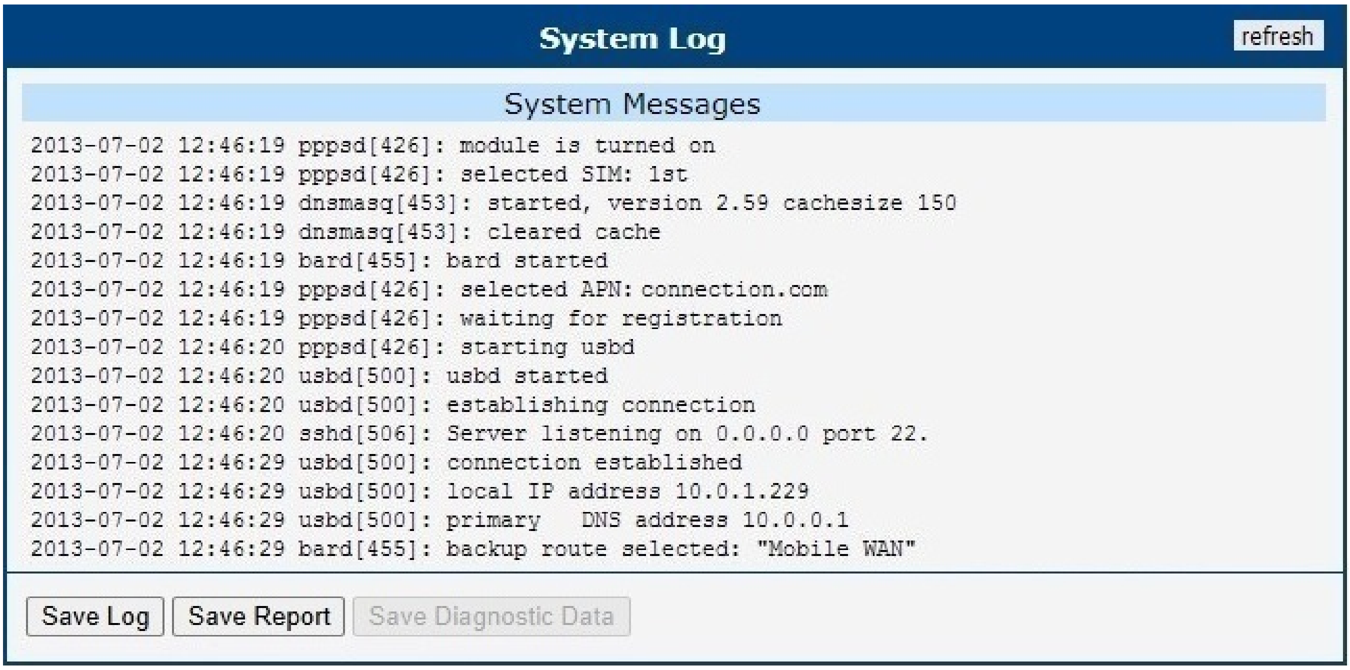
The level of detail in the log is controlled by the *Minimum Severity* setting on the *Configuration* → *Services* → *Syslog* page.

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

  Note: For users logged in with the *Admin* role, the report will additionally include a copy of the current (non-sensitive) 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.



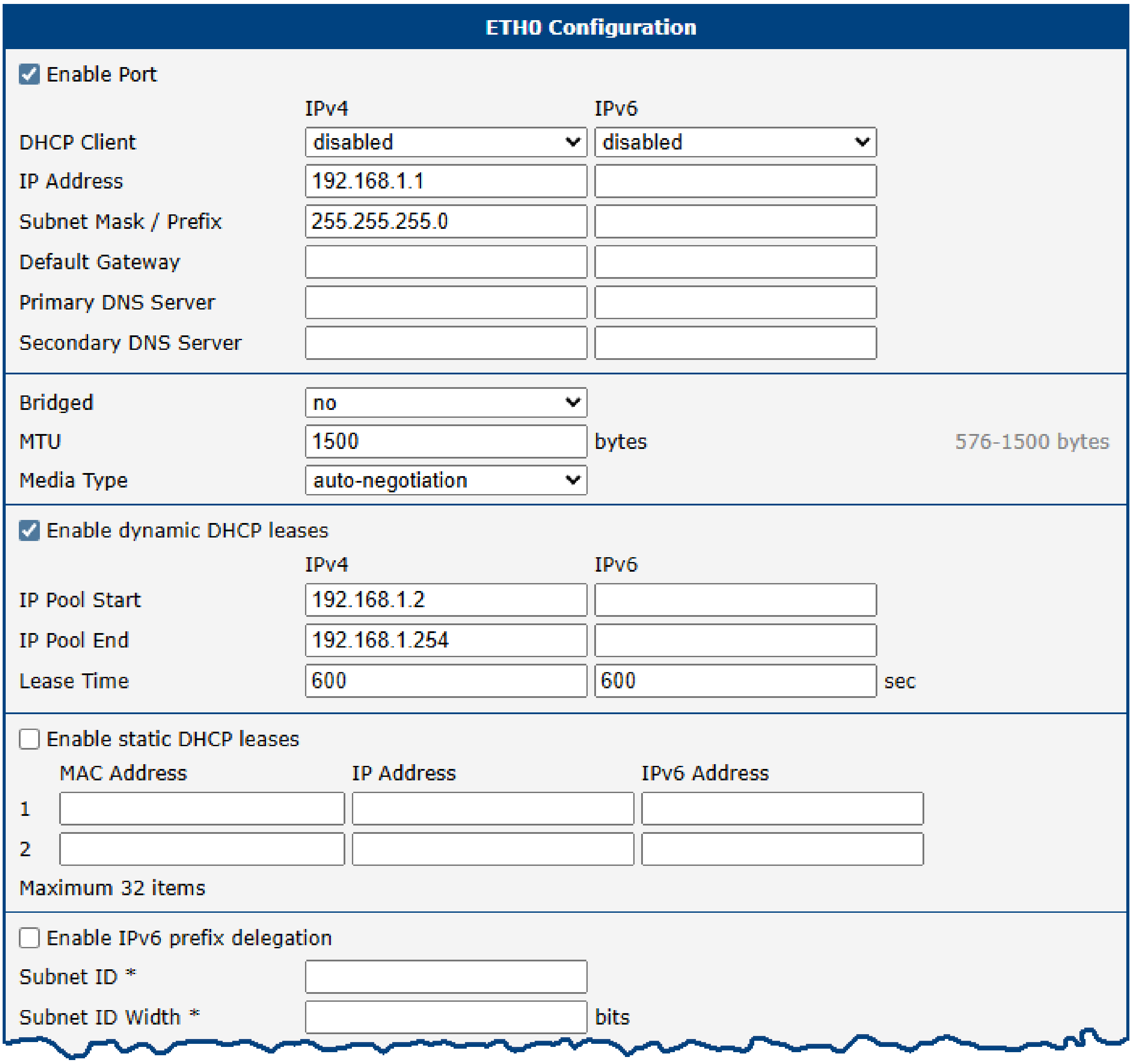
```
2013-07-02 12:46:19 pppsd[426]: module is turned on
2013-07-02 12:46:19 pppsd[426]: selected SIM: 1st
2013-07-02 12:46:19 dnsmasq[453]: started, version 2.59 cachesize 150
2013-07-02 12:46:19 dnsmasq[453]: cleared cache
2013-07-02 12:46:19 bard[455]: bard started
2013-07-02 12:46:19 pppsd[426]: selected APN: connection.com
2013-07-02 12:46:19 pppsd[426]: waiting for registration
2013-07-02 12:46:20 pppsd[426]: starting usbd
2013-07-02 12:46:20 usbd[500]: usbd started
2013-07-02 12:46:20 usbd[500]: establishing connection
2013-07-02 12:46:20 sshd[506]: Server listening on 0.0.0.0 port 22.
2013-07-02 12:46:29 usbd[500]: connection established
2013-07-02 12:46:29 usbd[500]: local IP address 10.0.1.229
2013-07-02 12:46:29 usbd[500]: primary   DNS address 10.0.0.1
2013-07-02 12:46:29 bard[455]: backup route selected: "Mobile WAN"
```

Figure 12: System log page

3. Configuration

3.1 Ethernet

To configure the Local Area Network (LAN), navigate to the *Ethernet* menu item in the *Configuration* section. Expanding the *Ethernet* menu on the left allows you to select the appropriate Ethernet interface for configuration: *ETH0* for the first Ethernet interface and *ETH1* for the second Ethernet interface.
This configuration page is divided into IPv4 and IPv6 sections. The router supports dual-stack operation, meaning IPv4 and IPv6 can run concurrently. You can configure either one or both. When both IPv4 and IPv6 are enabled, network devices automatically select the appropriate protocol. The configuration options for IPv4 and IPv6 are described in the following tables.



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

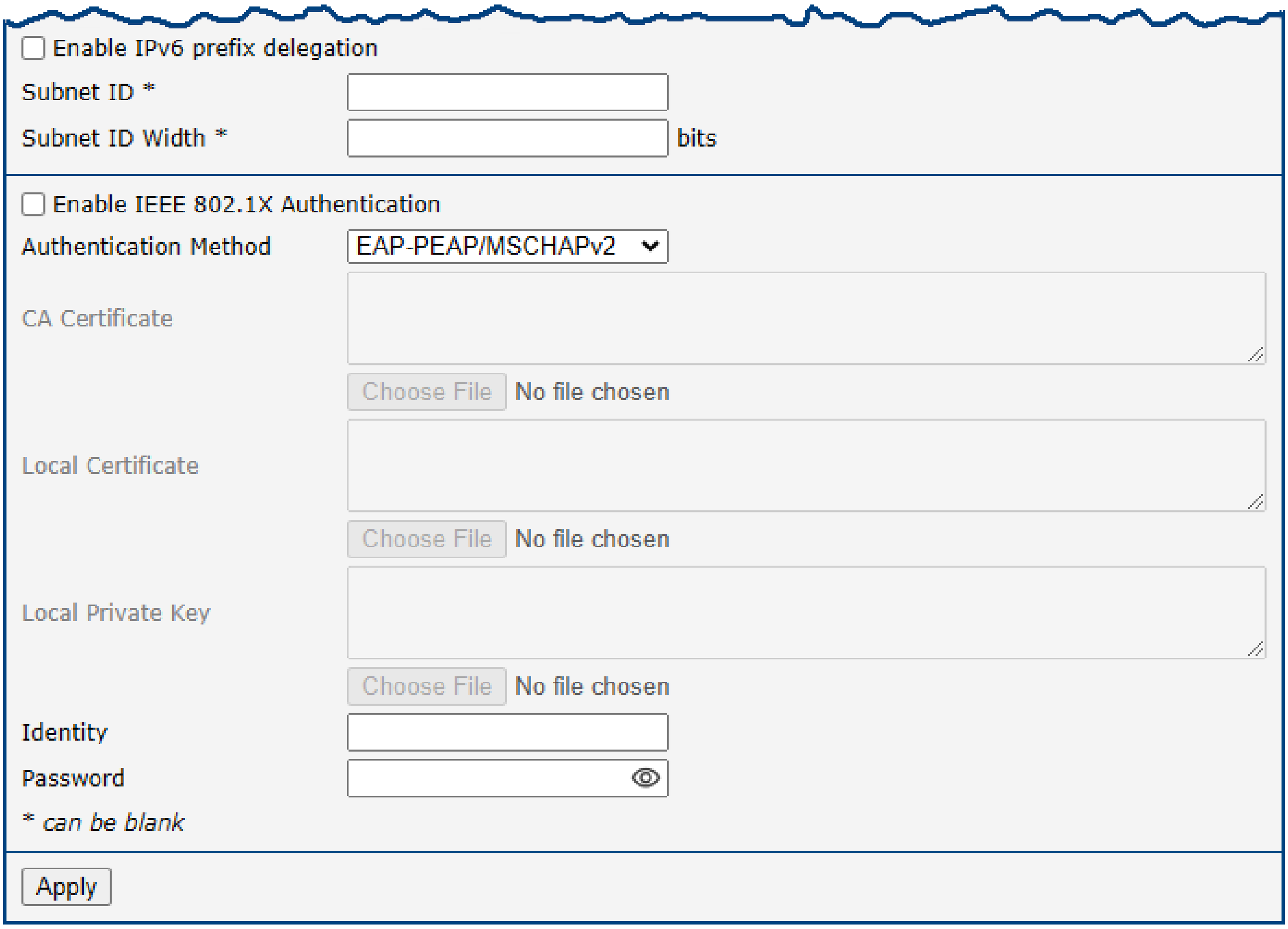
	MAC Address	IP Address	IPv6 Address
1			
2			

Maximum 32 items

☐ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

Figure 13: LAN configuration page



□ Enable IPv6 prefix delegation

Subnet ID *

Subnet ID Width * bits

□ Enable IEEE 802.1X Authentication

Authentication Method: EAP-PEAP/MSCHAPv2

Figure 14: LAN configuration page

Item	Description
Enable Port	Enables or disables the physical Ethernet port.
DHCP Client	Enables or disables the DHCP client function. In the IPv6 column, this enables the DHCPv6 client, which supports all three methods of obtaining an IPv6 address: SLAAC, stateless DHCPv6, and stateful DHCPv6. • **disabled** – The router will not request an IP address from a DHCP server on the LAN. • **enabled** – The router will request an IP address from a DHCP server on the LAN.
IP Address	Sets a static IP address for the Ethernet interface. Use standard IPv4 or IPv6 notation (shortened notation is supported for IPv6).
Subnet Mask / Prefix	Specifies the subnet mask for a static IPv4 address or the prefix length for a static IPv6 address (a number from 0 to 128).
Default Gateway	Specifies the IP address of the default gateway. Packets with a destination not found in the routing table will be sent to this gateway.
Primary DNS Server	Specifies the IP address of the primary DNS server.
Secondary DNS Server	Specifies the IP address of the secondary DNS server.

Table 21: Network interface example – IPv4 and IPv6

The *Default Gateway* and *DNS Server* settings are only used if the *DHCP Client* is set to *disabled* and the corresponding LAN interface (ETH0 or ETH1) is selected as the default route by the *Backup Routes* system (see Chapter *3.7 Backup Routes*).

The following three items are global for the configured Ethernet interface. Only one bridge can be active on the router at a time. When a bridge is created, the *DHCP Client*, *IP Address*, and *Subnet Mask / Prefix* parameters are taken from the member interface with the lowest index (e.g., ETH0 has priority over ETH1). Other interfaces can be added to or removed from an existing bridge at any time.

Warning

Under certain conditions, an Ethernet interface can operate as a WAN interface, in which case firewall rules will apply. For details and examples, see Chapter *3.7 Backup Routes*.

Item	Description
Bridged	Activates or deactivates bridging for this interface. • **no** – Bridging is inactive (default). • **yes** – Bridging is active. See the **Bridge Notes** below for more details.
MTU	Sets the Maximum Transmission Unit (MTU) value. The default is 1500 bytes.
Media Type	Specifies the duplex mode and speed for the Ethernet port. • **Auto-negotiation** – The router automatically determines the optimal speed and duplex mode (default). • **100 Mbps Full Duplex** – Sets a speed of 100 Mbps with full-duplex communication. • **100 Mbps Half Duplex** – Sets a speed of 100 Mbps with half-duplex communication. • **10 Mbps Full Duplex** – Sets a speed of 10 Mbps with full-duplex communication. • **10 Mbps Half Duplex** – Sets a speed of 10 Mbps with half-duplex communication.

Table 22: Network interface global items

Bridge Notes

A bridge functions like a network switch, forwarding packets between the interfaces connected to it. Advantech routers support bridging between Ethernet interfaces or between Ethernet and Wi-Fi Access Point (AP) interfaces. When a bridge is established, a new virtual interface named `br0` is created, which is visible on the *Status* → *Network* → *Interfaces* page.
If two Ethernet interfaces are bridged, the `br0` interface inherits the IP configuration of the interface with the lower index (e.g., ETH0 over ETH1), and the configuration of the higher-indexed interface is disregarded. To include a Wi-Fi AP in a bridge, at least one Ethernet interface must also be a member; the bridge IP will be determined by the Ethernet interface.

3.1.1 DHCP Server

The DHCP server assigns IP addresses, a gateway IP (the router's IP), and a DNS server IP (the router's IP) to connected clients. It supports both static and dynamic IP address assignment. *Dynamic DHCP* assigns IPs from a configured address pool, while *Static DHCP* assigns specific IPs to clients based on their MAC addresses.

Info

- In the IPv6 column, these settings configure the DHCPv6 server. It provides stateful address configuration to clients. If the LAN prefix is set to /64, the server will also offer Stateless Address Autoconfiguration (SLAAC).
- For DHCPv6 static assignments to work, the client must use a DUID-LL or DUID-LLT type, which is derived from its MAC address.

Warning

Do not overlap the IP address ranges for static and dynamic DHCP leases. Doing so can cause IP address conflicts and network instability.

Item	Description
Enable dynamic DHCP leases	Enables the dynamic DHCP server.
IP Pool Start	The starting IP address of the range to be allocated to DHCP clients.
IP Pool End	The ending IP address of the range to be allocated to DHCP clients.
Lease Time	The duration (in seconds) for which an assigned IP address is valid before it can be reassigned.

Table 23: Dynamic DHCP server configuration

Item	Description
Enable static DHCP leases	Enables the static DHCP server. You can define up to 32 rules; a new row appears automatically after you fill in the previous one.
MAC Address	The MAC address of the DHCP client.
IPv4 Address	The IPv4 address to be assigned to the client.
IPv6 Address	The IPv6 address to be assigned to the client.

Table 24: Static DHCP server configuration

3.1.2 IPv6 Prefix Delegation

Warning

This is an advanced feature. IPv6 prefix delegation works automatically with DHCPv6. Only use this section if you require a non-standard configuration and understand the implications.

If you need to override the automatic IPv6 prefix delegation, you can configure it here. You must specify the Subnet ID Width. For example, in a typical /48 site prefix, the 16 bits following the site prefix are the Subnet ID, and the final 64 bits are the Interface ID.

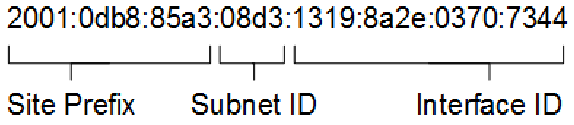


Figure 15: Example of an IPv6 address with prefix

Item	Description
Enable IPv6 prefix delegation	Enables the manual prefix delegation configuration below.
Subnet ID	The decimal value of the Subnet ID for the Ethernet interface. The maximum value depends on the *Subnet ID Width*.
Subnet ID Width	The bit-width of the Subnet ID field. This value is typically the remainder of 64 minus the site prefix length.

Table 25: IPv6 prefix delegation configuration

3.1.3 802.1X 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 involves three parties: a **supplicant**, an **authenticator**, and an **authentication server**, as shown in Figure 16.

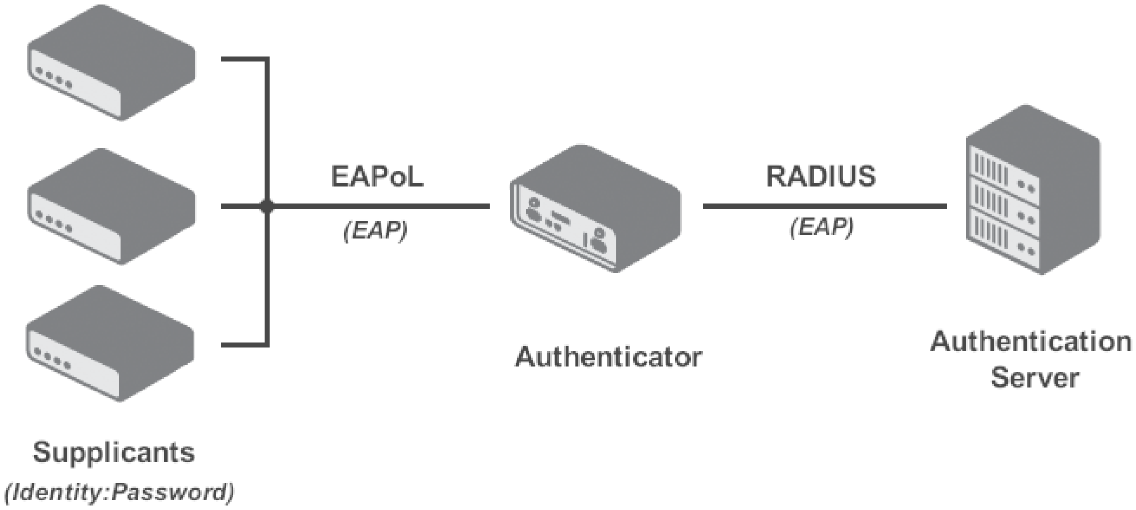


Figure 16: IEEE 802.1X functional diagram

- 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.

Table 26 summarizes the supported 802.1X roles on Advantech routers.

Info

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

Interface	Supplicant Role	Authenticator Role
LAN	Supported as a built-in feature (see Chapter *3.1.3 802.1X Authentication with RADIUS Server*).	Supported via the *802.1X Authenticator* Router App.
Wi-Fi	Supported in Station (STA) mode (see Chapter *3.6.2 Station*).	Supported in Access Point (AP) mode (see Chapter *3.6.1 Access Point*).

Table 26: Supported roles for IEEE 802.1X authentication

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).

Table 27: 802.1X authentication configuration

3.1.4 LAN Configuration Examples

Example 1: Dynamic DHCP with Custom Gateway and DNS

- The dynamic IPv4 address pool is 192.168.1.2 to 192.168.1.4.
- The lease time is 600 seconds (10 minutes).
- The default gateway IP address is 192.168.1.20.
- The DNS server IP address is 192.168.1.20.

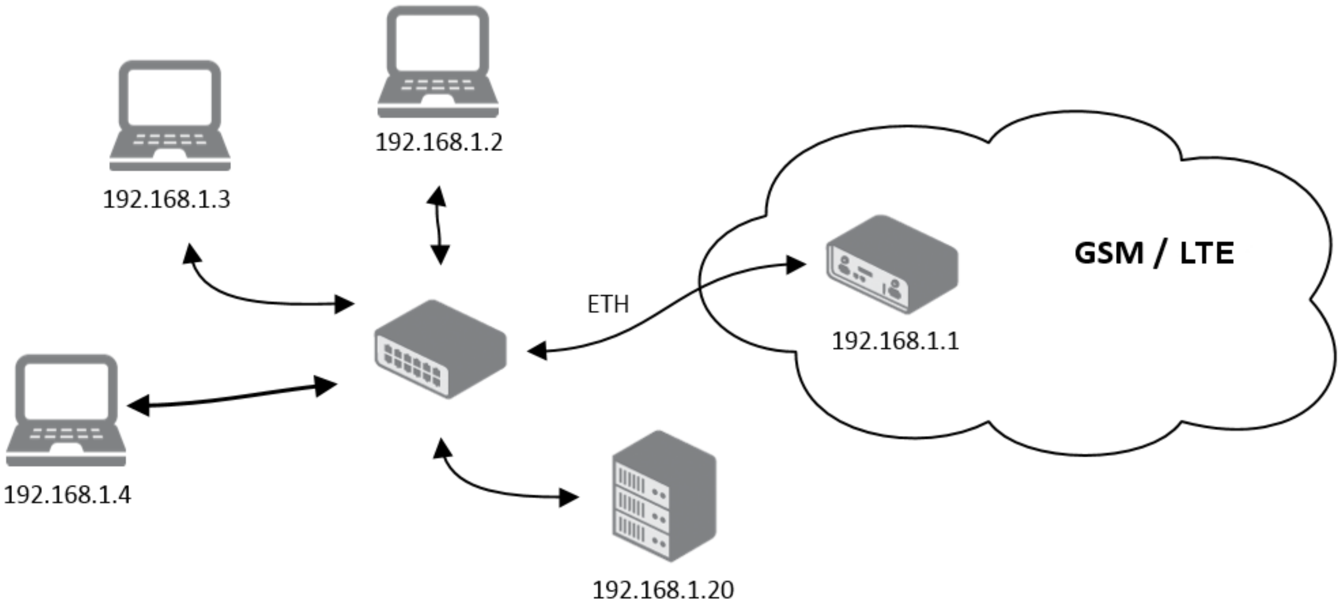
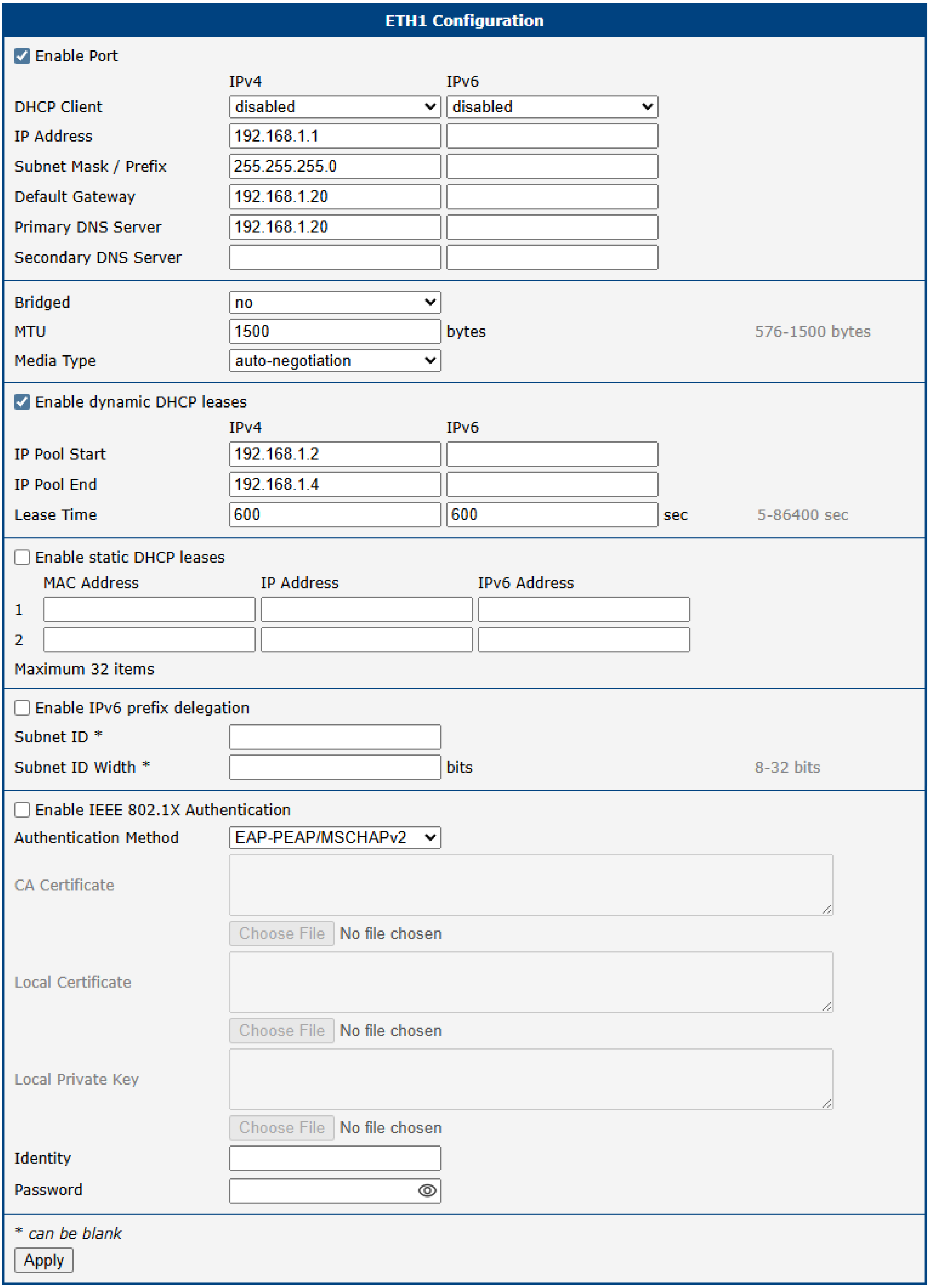


Figure 17: Network topology for example 1



ETH1 Configuration

☑ Enable Port

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway	192.168.1.20	
Primary DNS Server	192.168.1.20	
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	192.168.1.4			
Lease Time	600	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

Local Certificate

Local Private Key

Identity

Password

** can be blank*

Figure 18: LAN configuration for example 1

Example 2: Dynamic and Static DHCP Server

- The dynamic address pool is 192.168.1.2 to 192.168.1.4.
- The lease time is 600 seconds (10 minutes).
- The client with MAC 01:23:45:67:89:ab is assigned the static IP 192.168.1.10.
- The client with MAC 01:54:68:18:ba:7e is assigned the static IP 192.168.1.11.

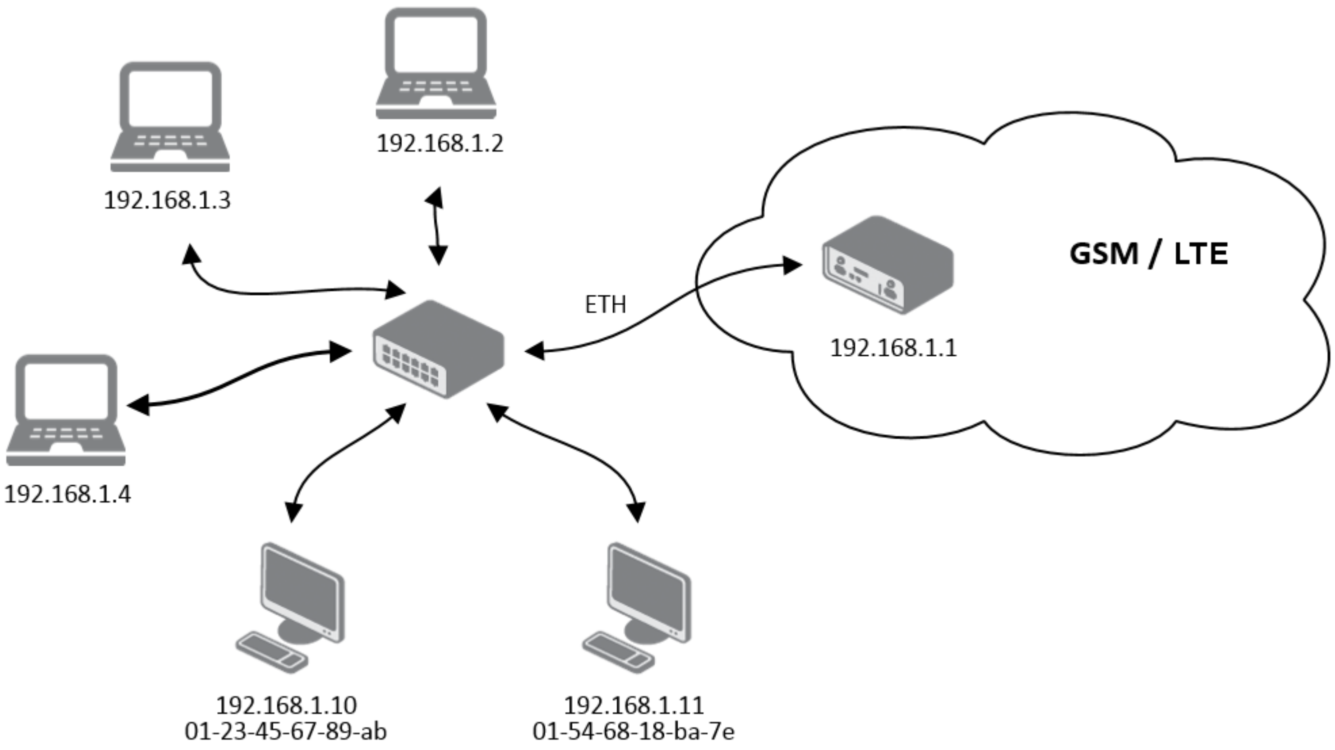
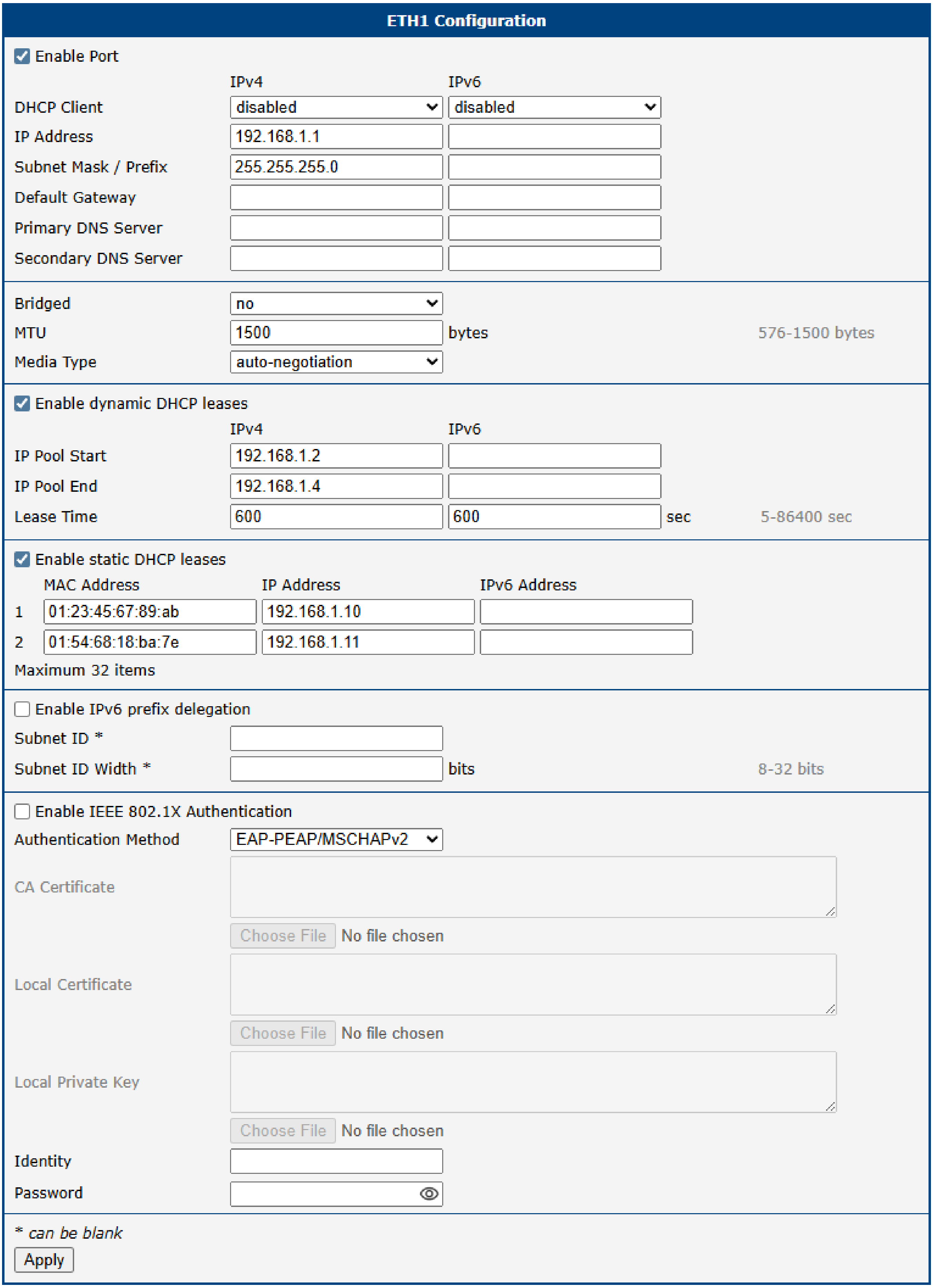


Figure 19: Network topology for example 2



ETH1 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	192.168.1.4			
Lease Time	600	600	sec	5-86400 sec

☑ Enable static DHCP leases

	MAC Address	IP Address	IPv6 Address
1	01:23:45:67:89:ab	192.168.1.10	
2	01:54:68:18:ba:7e	192.168.1.11	

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

Figure 20: LAN configuration for example 2

Example 3: IPv6 Dynamic DHCP Server

- The dynamic IPv6 address pool is 2001:db8::1 to 2001:db8::ffff.
- The lease time is 600 seconds (10 minutes).
- The router remains accessible via its default IPv4 address (192.168.1.1).

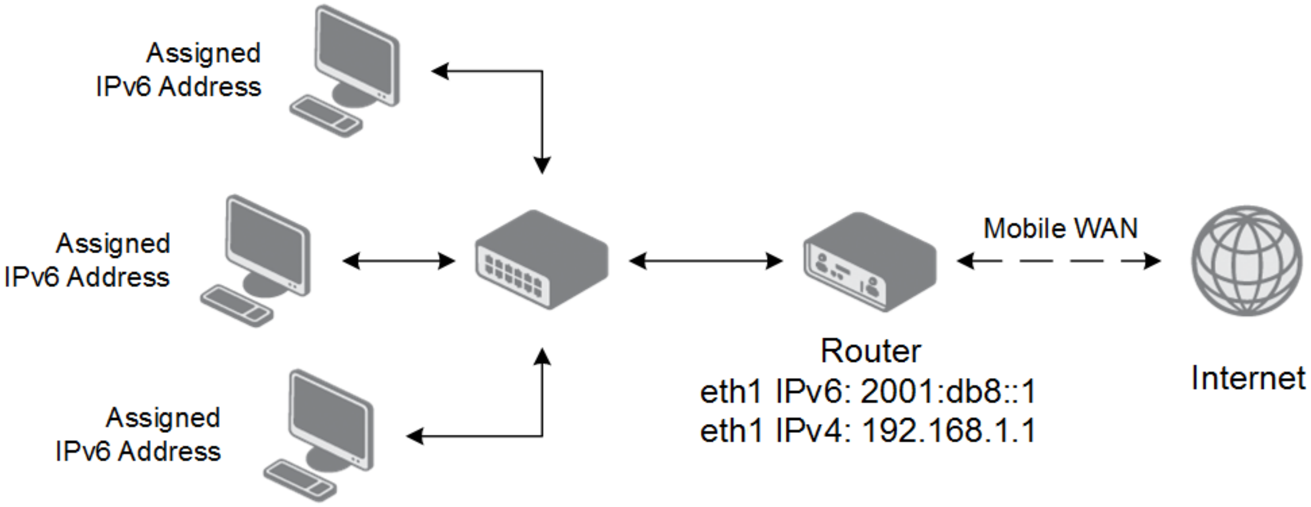
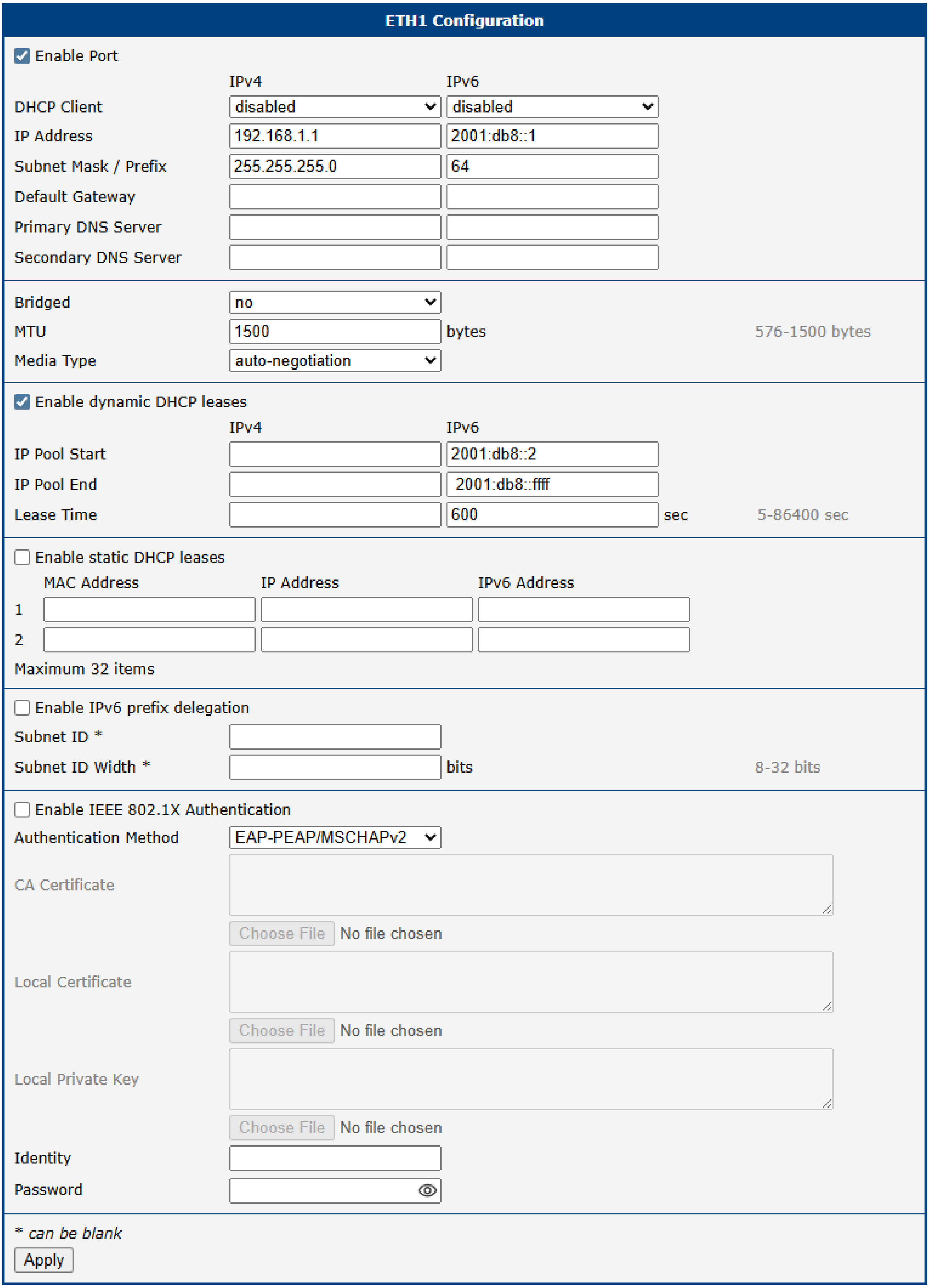


Figure 21: Network topology for example 3



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	

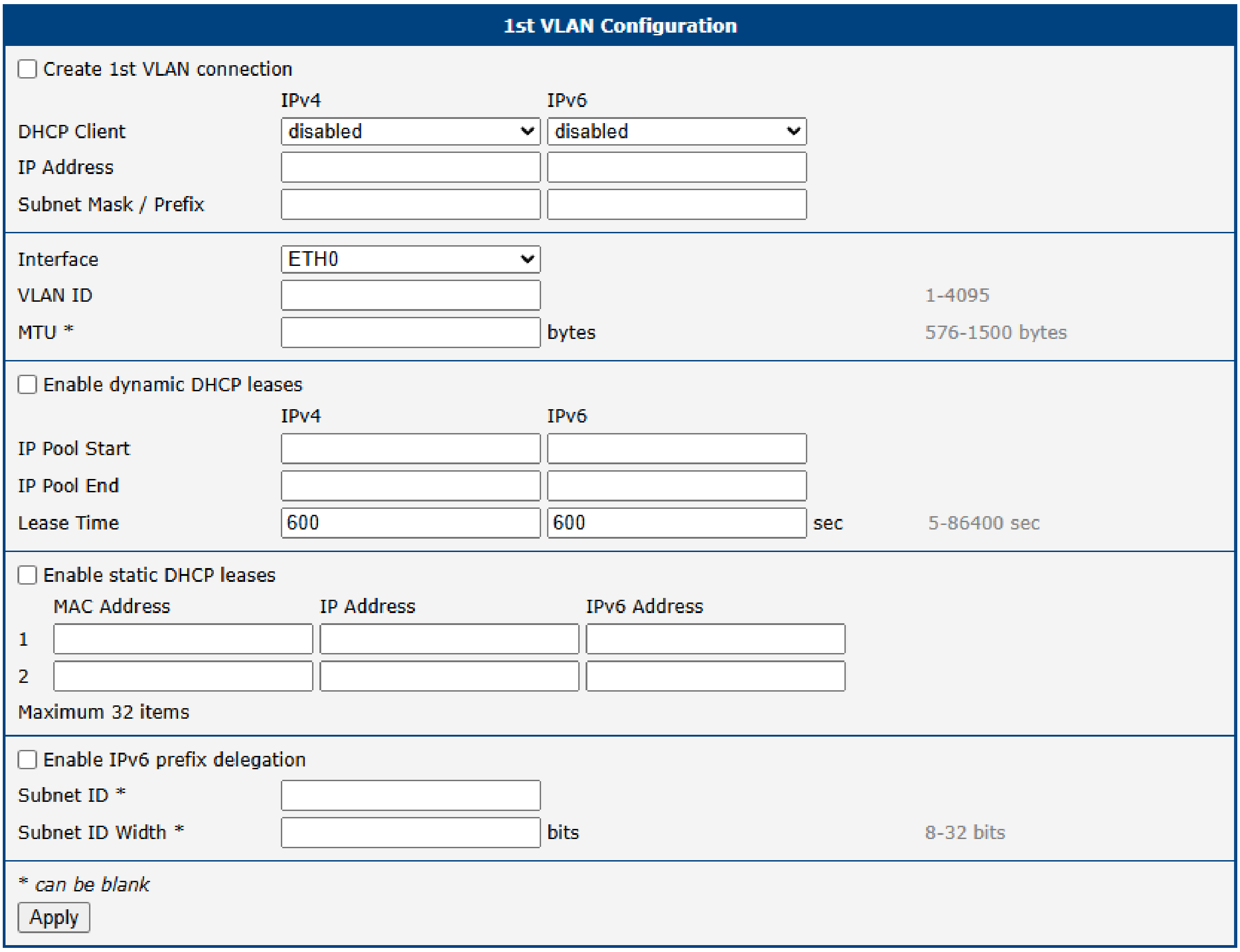
** can be blank*

Apply

Figure 22: LAN configuration for example 3

3.2 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.



1st VLAN Configuration

☐ Create 1st VLAN connection

	IPv4	IPv6	
DHCP Client	disabled	disabled	
IP Address			
Subnet Mask / Prefix			

Interface	ETH0		
VLAN ID			1-4095
MTU *		bytes	576-1500 bytes

☐ Enable dynamic DHCP leases

	IPv4	IPv6		
IP Pool Start				
IP Pool End				
Lease Time	600	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

** can be blank*

Figure 23: 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.
Subnet Mask / Prefix	Defines the subnet mask (for IPv4) or prefix length (for IPv6) for the static IP address.

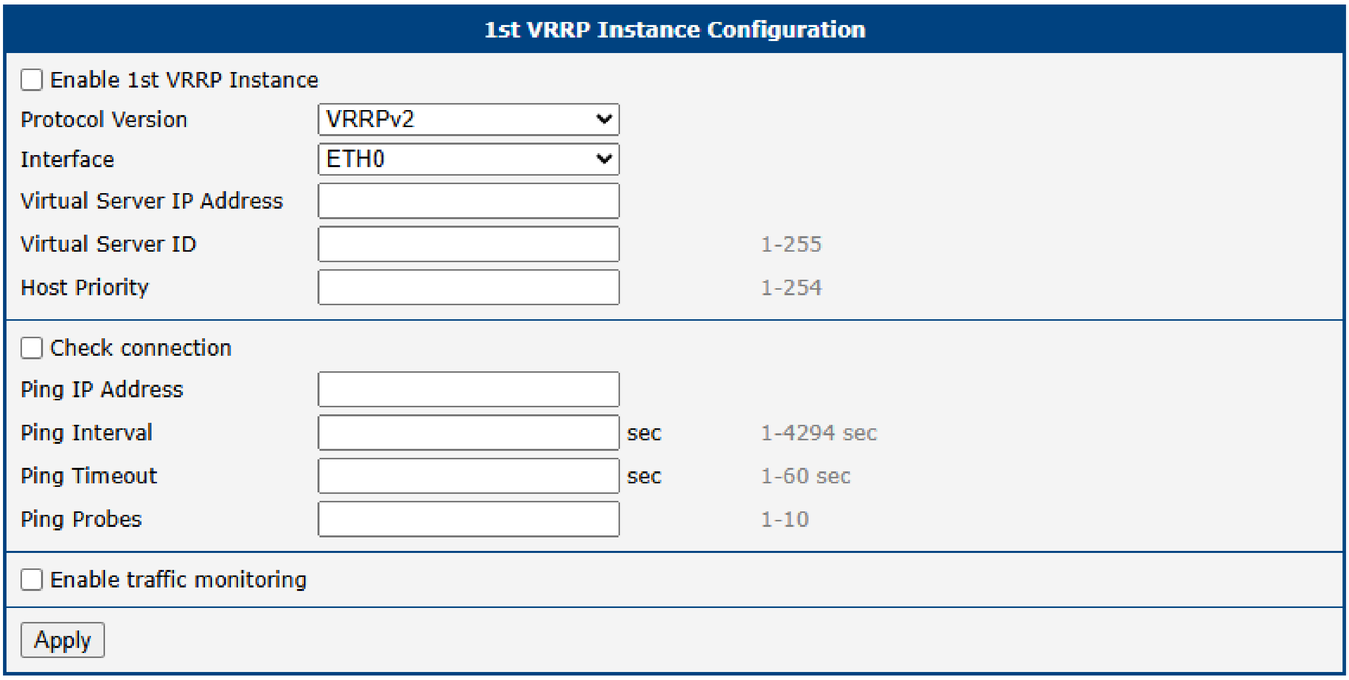
Table 28: VLAN configuration options

Item	Description
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.

Table 28: (continued)

3.3 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.



1st VRRP Instance Configuration

☐ Enable 1st VRRP Instance

Protocol Version	VRRPv2		
Interface	ETH0		
Virtual Server IP Address			
Virtual Server ID			1-255
Host Priority			1-254

☐ Check connection

Ping IP Address			
Ping Interval		sec	1-4294 sec
Ping Timeout		sec	1-60 sec
Ping Probes			1-10

☐ Enable traffic monitoring

Figure 24: 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.

Table 29: VRRP instance configuration options

Item	Description
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.

Table 29: (continued)

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.

Table 30: Connection checking parameters

Configuration 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.

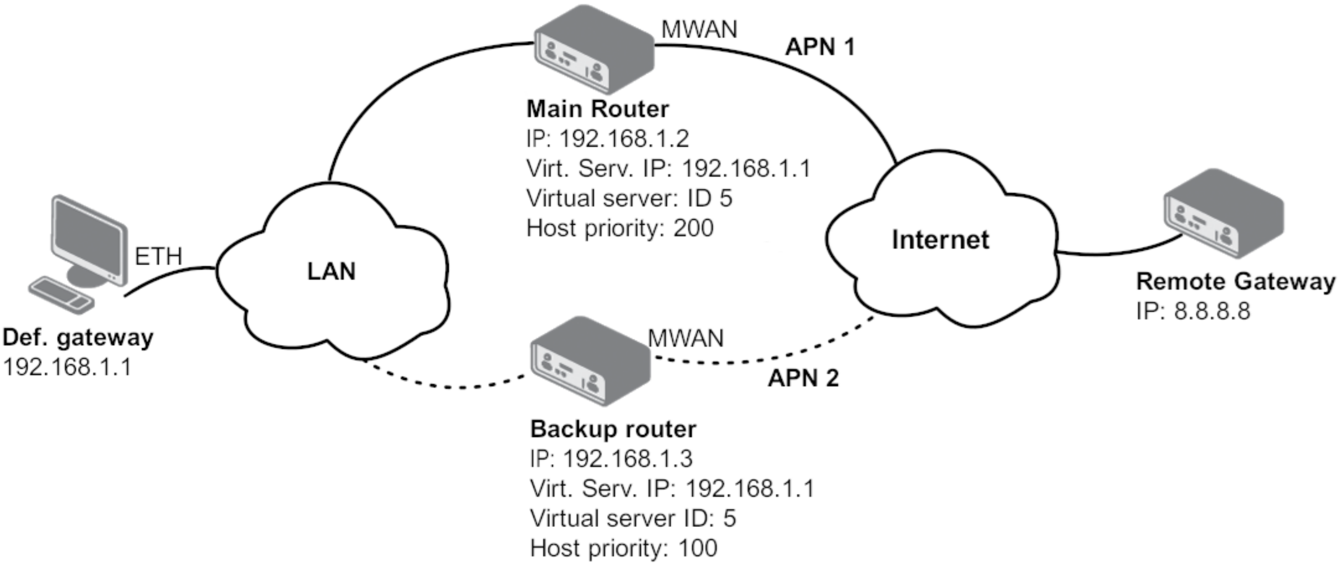
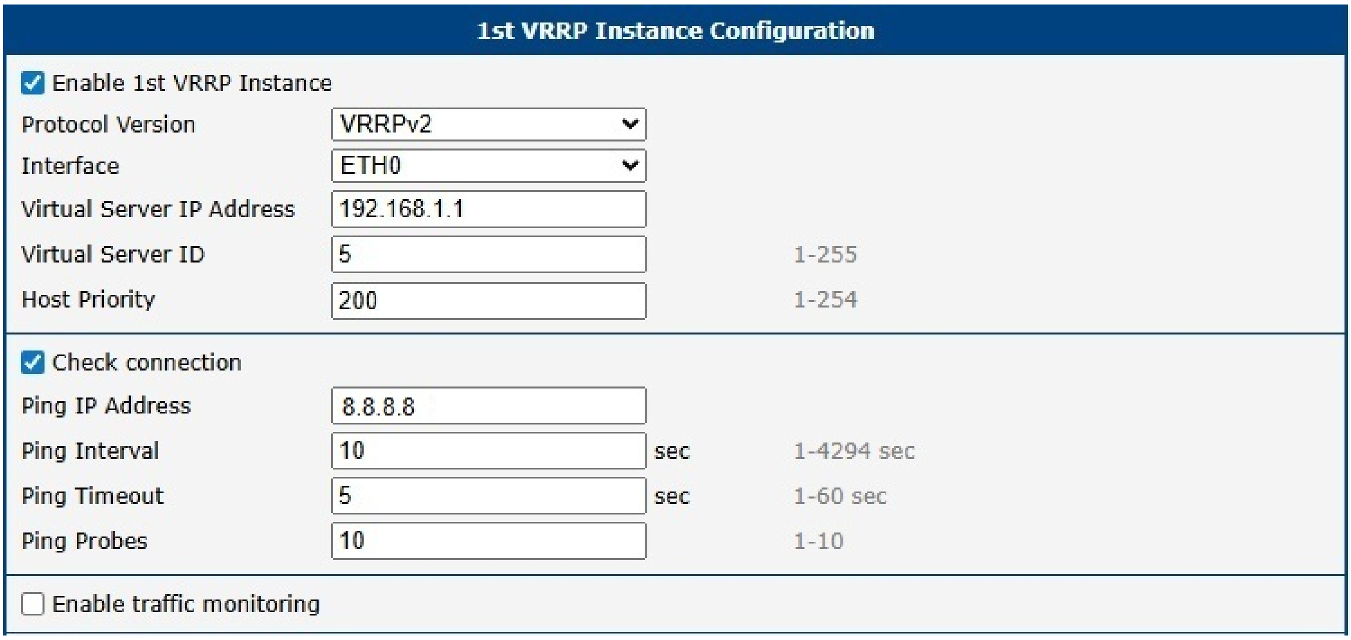


Figure 25: An example of VRRP topology



1st VRRP Instance Configuration

☑ Enable 1st VRRP Instance

Protocol Version	VRRPv2		
Interface	ETH0		
Virtual Server IP Address	192.168.1.1		
Virtual Server ID	5		1-255
Host Priority	200		1-254

☑ Check connection

Ping IP Address	8.8.8.8		
Ping Interval	10	sec	1-4294 sec
Ping Timeout	5	sec	1-60 sec
Ping Probes	10		1-10

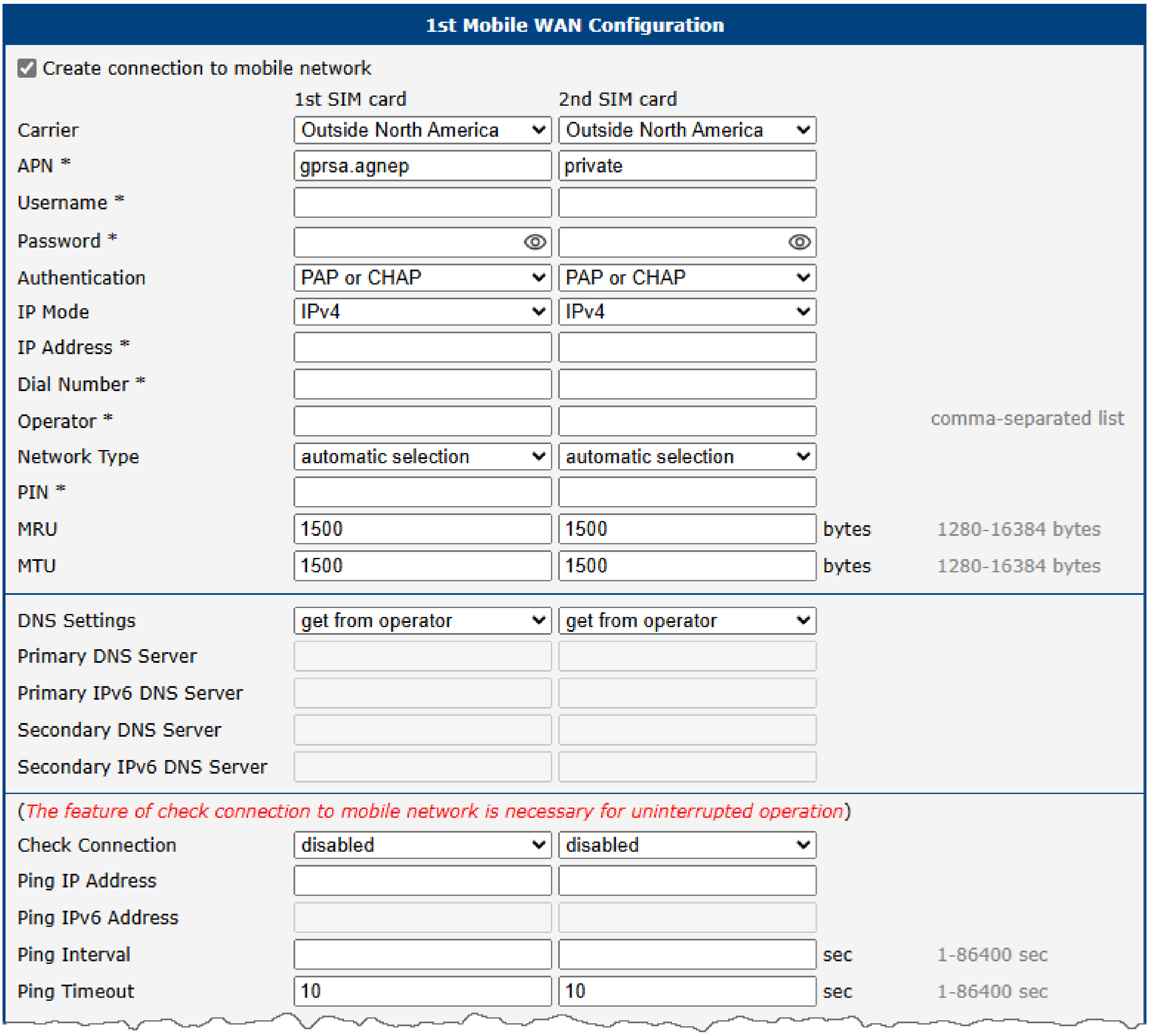
☐ Enable traffic monitoring

Figure 26: Main router configuration

Configure the backup router identically to the main router (see Figure 26), with one exception: set the **Host Priority** to **100**. The *Check connection* settings should remain the same.

3.4 Mobile WAN

Select the *Mobile WAN* item in the *Configuration* menu to open the cellular network configuration page, as shown in Figure 28.



1st Mobile WAN Configuration

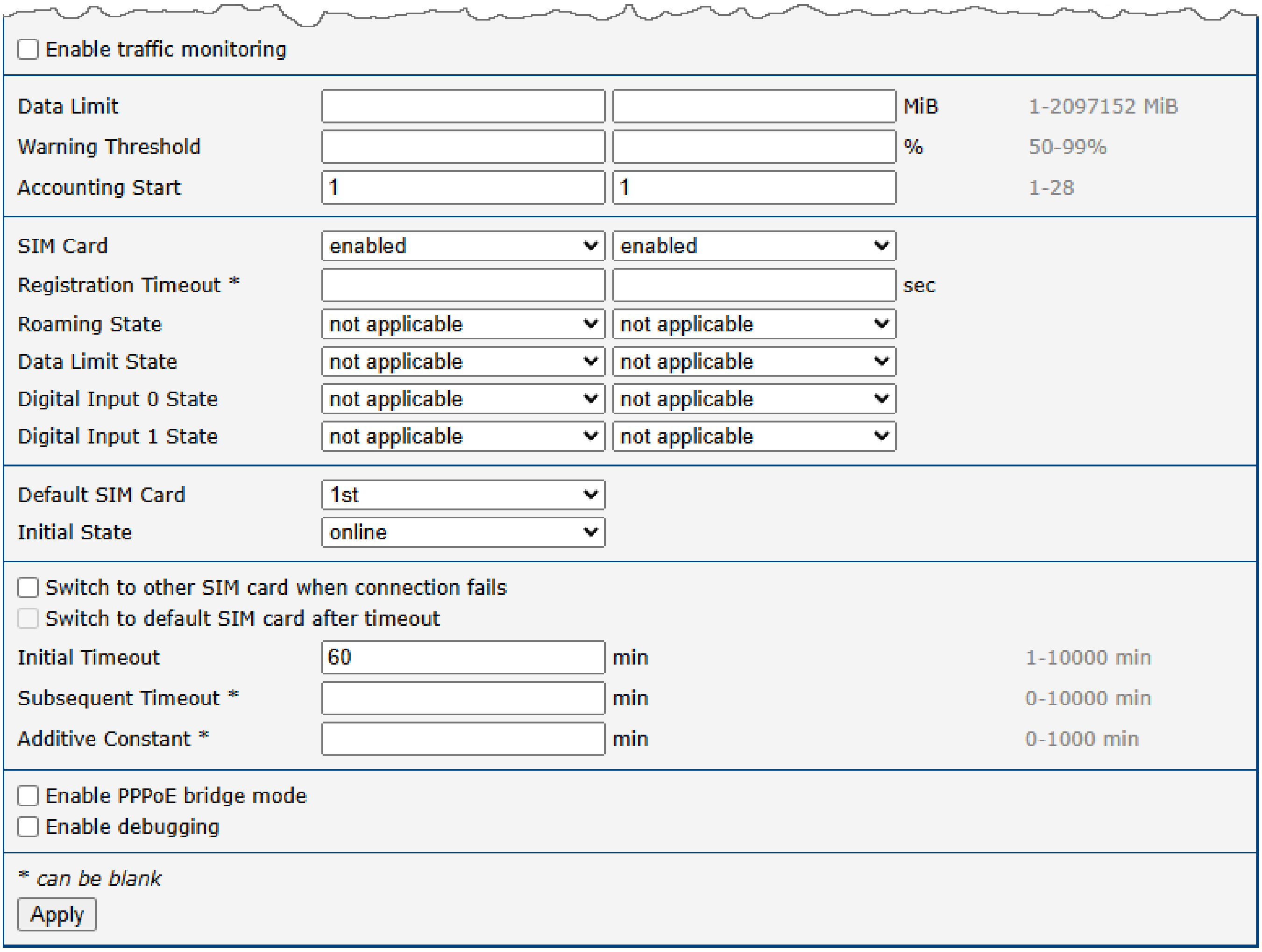
☑ Create connection to mobile network

	1st SIM card	2nd SIM card		
Carrier	Outside North America	Outside North America		
APN *	gprsa.agnep	private		
Username *				
Password *				
Authentication	PAP or CHAP	PAP or CHAP		
IP Mode	IPv4	IPv4		
IP Address *				
Dial Number *				
Operator *				comma-separated list
Network Type	automatic selection	automatic selection		
PIN *				
MRU	1500	1500	bytes	1280-16384 bytes
MTU	1500	1500	bytes	1280-16384 bytes
DNS Settings	get from operator	get from operator		
Primary DNS Server				
Primary IPv6 DNS Server				
Secondary DNS Server				
Secondary IPv6 DNS Server				

(*The feature of check connection to mobile network is necessary for uninterrupted operation*)

Check Connection	disabled	disabled		
Ping IP Address				
Ping IPv6 Address				
Ping Interval			sec	1-86400 sec
Ping Timeout	10	10	sec	1-86400 sec

Figure 27: Mobile WAN configuration page – part 1



☐ Enable traffic monitoring

Data Limit			MiB	1-2097152 MiB
Warning Threshold			%	50-99%
Accounting Start	1	1		1-28

SIM Card	enabled	enabled	
Registration Timeout *			sec
Roaming State	not applicable	not applicable	
Data Limit State	not applicable	not applicable	
Digital Input 0 State	not applicable	not applicable	
Digital Input 1 State	not applicable	not applicable	

Default SIM Card	1st
Initial State	online

☐ Switch to other SIM card when connection fails

☐ Switch to default SIM card after timeout

Initial Timeout	60	min	1-10000 min
Subsequent Timeout *		min	0-10000 min
Additive Constant *		min	0-1000 min

☐ Enable PPPoE bridge mode

☐ Enable debugging

** can be blank*

Figure 28: Mobile WAN configuration page – part 2

3.4.1 Connection to Mobile Network

Info

- Starting with firmware version 6.6.0, PLMN whitelisting is now an integrated firmware feature, available in the *Operator* field. This native functionality replaces the legacy *PLMN Whitelist* Router App.
- To avoid potential conflicts, you must disable or uninstall the legacy Router App before using the integrated PLMN whitelisting feature.

If the *Create connection to mobile network* checkbox is checked, the router will automatically attempt to establish a connection after booting up. You can specify the following parameters for each SIM card separately.

Item	Description
Carrier	Allows for manual or automatic selection of a mobile network carrier. **This is primarily available for global or NAM (North American) certified models.** • For non-NAM or global models, the *Outside North America* option restricts connections to non-NAM operators. • For NAM-certified models, choices typically include: ◦ *North America, Autoselect*: Automatically detects and connects to a suitable NAM operator. ◦ *North America, Generic*: Enables a generic, PTCRB-compliant configuration. ◦ Manual selection of specific operators like *AT&T*, *Rogers*, *T-Mobile*, or *Verizon*.
APN	The Access Point Name (APN) of the mobile network.
Username	The username for logging into the mobile network.
Password	The password for logging into the mobile network.
Authentication	The authentication protocol used by the network. Both *Username* and *Password* must be specified for this setting to apply. • **PAP or CHAP**: The router automatically selects the authentication method. • **PAP**: Forces PAP authentication. • **CHAP**: Forces CHAP authentication.
IP Mode	The version of the IP protocol to be used: • **IPv4**: Use only the IPv4 protocol (default). • **IPv6**: Use only the IPv6 protocol. • **IPv4/IPv6**: Enable an independent dual stack for both IPv4 and IPv6.
IP Address	The IP address of the SIM card (for IPv4 and IPv4/IPv6 modes only). Enter this manually only if the carrier has assigned a static IP address.
Dial Number	The number the router dials for a CSD connection. The default is `*99***1#` .
Operator	Specifies the preferred mobile network operator using the carrier's Public Land Mobile Network (PLMN) code. This field controls how the router selects a network, and its behavior changes based on the input: • **Empty Field:** The router operates in automatic mode, connecting to any available network. • **Single PLMN:** The router locks to the specified operator and will only connect to that network. • **Comma-Separated List (Whitelist):** By providing two or more PLMNs, you create a whitelist of allowed operators. Upon connecting or if the current network is not on the list, the router will perform a network scan (which may take up to two minutes) and connect to the first operator from your list that it finds available. • **Whitelist with Automatic Fallback:** To use automatic network selection but still restrict to a list of preferred operators, start the list with '0,' (e.g., `0,23001,90001`). The router will first connect automatically. If the selected network is not in your whitelist, it will then perform the network scan described above to find and switch to a whitelisted operator.

Table 31: Mobile WAN configuration items description

Item	Description
Network Type	Specifies the preferred mobile network technology. The available options depend on the specific router model and may include: • **automatic selection** – Allows the router to automatically choose the best available technology. However, it will never select NB-IoT. For NB-IoT connectivity, you must select the NB-IoT option explicitly. • **GPRS/EDGE** • **UMTS/HSPA** • **LTE** • **NB-IoT** • **LTE-M** • **NR5G** – Equivalent to *5G SA* (Standalone). Note: *5G NSA* (Non-Standalone) is a combination of LTE and 5G technologies and functions only when the *automatic selection* mode is enabled.
PIN	The Personal Identification Number used to unlock the SIM card. Use this only if required by the SIM card. The card will be blocked after several failed attempts.
MRU	Maximum Receive Unit: the maximum packet size the router can receive. Default is 1500 B. Incorrect values may cause data reception errors. Minimum value is 128 B for IPv4 and 1280 B for IPv6.
MTU	Maximum Transmission Unit: the maximum packet size the router can transmit. Default is 1500 B. Incorrect values may cause data transmission errors. Minimum value is 128 B for IPv4 and 1280 B for IPv6.

Table 31: (continued)

Info

The following tips apply to the *1st/2nd Mobile WAN Configuration* form:

- An incorrect MTU size may cause data transfer failures. A value that is too low increases fragmentation and overhead, while a value that is too high can cause packets to be dropped by the network.
- If the *IP address* field is left blank, the carrier will automatically assign an IP address. Manual assignment can result in a faster connection.
- If the *APN* field is left blank, the router will attempt to auto-select an APN based on the SIM card's IMSI. The selected APN name can be found in the System Log.
- To use a blank APN, enter the word *blank* in the *APN* field.

Warning

An incorrect PIN will block the SIM card after several failed attempts.

Parameters marked with an asterisk (*) are required only if specified by your mobile network operator. If the router fails to connect, verify the accuracy of all entered data and consider trying a different authentication method or network type.

3.4.2 DNS Configuration

The *DNS Settings* parameter simplifies client-side configuration. When set to *get from operator*, the router automatically obtains the primary and secondary DNS server IP addresses from the carrier. To specify them manually, select *set manually* and enter the IPv4 or IPv6 addresses, depending on the selected *IP Mode*.

3.4.3 Mobile Network Connection Check

> **Warning**
>
> Enabling the *Check Connection* function is essential for ensuring uninterrupted operation of the router.

If *Check Connection* is set to *enabled* or *enabled + bind*, the router sends ping requests to the address specified in *Ping IP Address* or *Ping IPv6 Address* at regular intervals defined by *Ping Interval*. If a ping fails, a new one is sent after the *Ping Timeout*. If three consecutive pings fail, the router terminates and re-establishes the cellular connection. This monitoring function can be configured for each SIM card but runs only on the active SIM. Ensure you use a reliable destination address, such as the operator's DNS server.
If *Check Connection* is set to *enabled*, ping requests are sent based on the routing table and may use any available interface. To ensure pings are sent only through the mobile WAN interface, set it to *enabled + bind*. The *disabled* option deactivates connection checking.

> **Warning**
>
> For routers connected to the **Verizon** network, the connection retry interval increases with each attempt. The first two retries occur after 1 minute, followed by intervals of 2, 8, and 15 minutes. The ninth and all subsequent retries occur every 90 minutes.

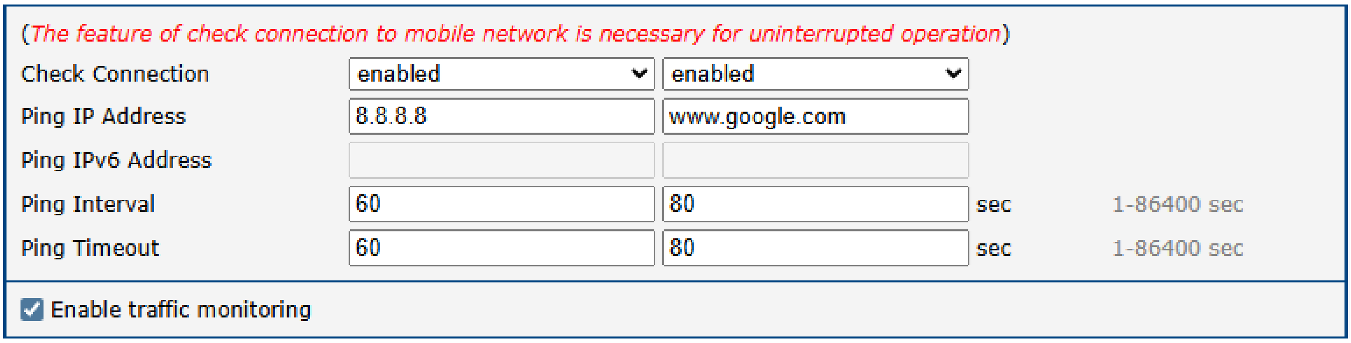
If *Enable Traffic Monitoring* is checked, the router monitors Mobile WAN traffic instead of sending pings. If no data is transmitted, it will begin sending pings.

Item	Description
Ping IP Address	The destination IPv4 address or domain name for ping queries. Available in IPv4 and IPv4/IPv6 *IP Mode*.
Ping IPv6 Address	The destination IPv6 address or domain name for ping queries. Available in IPv6 and IPv4/IPv6 *IP Mode*.
Ping Interval	The time interval between outgoing pings.
Ping Timeout	The time (in seconds) to wait for a ping response.

Table 32: Mobile network connection check configuration

3.4.4 Connection Check Example

The figure below shows a scenario where the IPv4 connection is monitored by pinging 8.8.8.8 every 60 seconds for the first SIM card and 'www.google.com' every 80 seconds for the second SIM card. Since *Enable traffic monitoring* is active, pings are only sent if no other data traffic is detected.



(The feature of check connection to mobile network is necessary for uninterrupted operation)

Check Connection	enabled	enabled		
Ping IP Address	8.8.8.8	www.google.com		
Ping IPv6 Address				
Ping Interval	60	80	sec	1-86400 sec
Ping Timeout	60	80	sec	1-86400 sec

☑ Enable traffic monitoring

Figure 29: Connection check example

3.4.5 Data Limit Settings

Item	Description
Data Limit	The maximum amount of data (sent and received) allowed per billing period (one month). The maximum value is 2 TB (2,097,152 MB).
Warning Threshold	A percentage of the *Data Limit* (50% to 99%). When this threshold is exceeded, the router sends an SMS message.
Accounting Start	The day of the month when the billing cycle begins. The router starts counting data from this day.

Table 33: Data limit configuration

Info

The *Data Limit* setting is ignored if *Data Limit State* (see below) is set to *not applicable* or if *Send SMS when data limit is exceeded* is disabled in *SMS Configuration*.

3.4.6 SIM Card Switching

In the lower part of the form, you can specify rules for switching between SIM cards.

Info

The router automatically switches between SIMs based on the logical AND of all configured rules (manual permission, roaming, data limit, and digital input state).

Item	Description
SIM Card	Enables or disables the use of a SIM card. Setting all SIMs to *disabled* deactivates the cellular module.
Registration Timeout	Sets the registration timeout for the SIM card in seconds (default is 2 minutes).
Roaming State	Configures SIM usage based on roaming status (this feature must be activated by your operator). • **not applicable**: Use the SIM card everywhere. • **home network only**: Use the SIM card only when not roaming.
Data Limit State	Configures SIM usage based on the data limit: • **not applicable**: Use the SIM regardless of the data limit. • **not exceeded**: Use the SIM only if the data limit has not been exceeded.
BINx State	Configures SIM usage based on a digital input's state: • **not applicable**: Use the SIM regardless of the input state. • **on**: Use the SIM only if the input is on (voltage present). • **off**: Use the SIM only if the input is off (no voltage).

Table 34: SIM card switching configuration

Item	Description
Default SIM Card	Specifies the primary SIM card the router should use to connect.
Initial State	The action the module takes after a SIM is selected: • **online**: Establish a connection immediately (default). • **offline**: Remain offline. The state can be changed via SMS. The module will also go offline if no SIM card meets the switching criteria.
Switch to other SIM card when connection fails	If enabled, the router switches to the backup SIM card if the connection on the default SIM fails (as detected by the *Check Connection* feature).
Switch to default SIM card after timeout	If enabled, the router will attempt to switch back to the default SIM after a specified timeout. This applies only if the switch to the backup SIM was triggered by a connection failure or roaming. This feature requires *Switch to other SIM card when connection fails* to be enabled.
Initial Timeout	The time (1 to 10,000 minutes) the router waits before the first attempt to switch back to the default SIM.
Subsequent Timeout	The time (1 to 10,000 minutes) the router waits after a failed attempt to switch back.
Additive Constant	An additional time (1 to 10,000 minutes) added to the *Subsequent Timeout* for each further attempt.

Table 35: Parameters for SIM card switching

3.4.7 Other Settings

This section describes the remaining items in the Mobile WAN configuration.

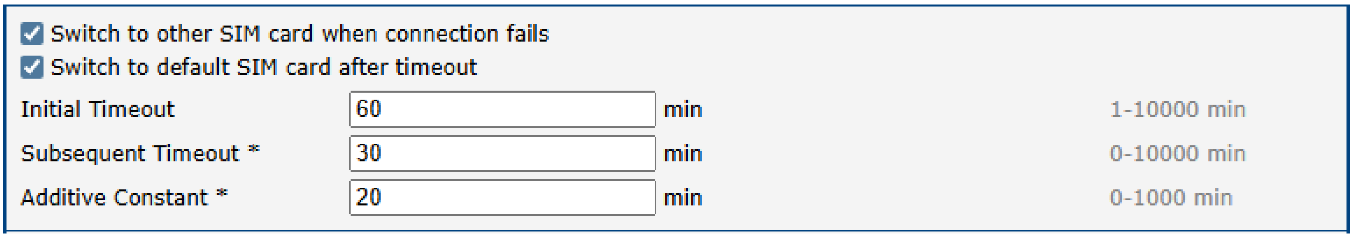
Item	Description
Enable PPPoE bridge mode	Enables PPPoE bridge mode on the *Mobile WAN* interface, allowing a device on the LAN to establish a direct PPPoE connection with the mobile operator and obtain the public IP address.
Enable debugging	Enables detailed diagnostic logging. For messages to appear in the system log, the *Minimum Severity* in *Configuration* → *Services* → *Syslog* must be set to *Debug*. **Note:** This can generate a large volume of data and should be disabled after troubleshooting.

Table 36: Other settings

3.4.8 SIM Card Switching Examples

Example 1: Timeout Configuration

With *Switch to default SIM card after timeout* checked and the following values configured:



☑ Switch to other SIM card when connection fails
☑ Switch to default SIM card after timeout

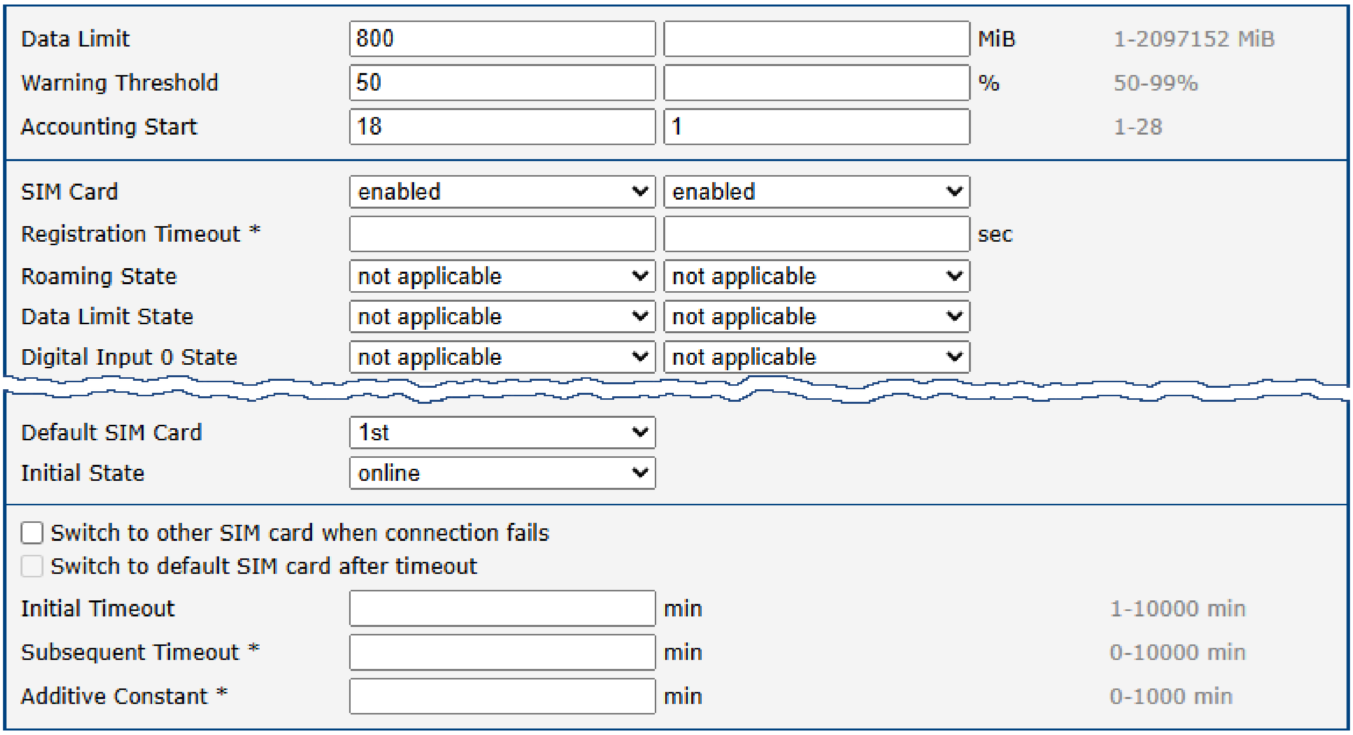
Initial Timeout	60	min	1-10000 min
Subsequent Timeout *	30	min	0-10000 min
Additive Constant *	20	min	0-1000 min

Figure 30: SIM card switching example 1

The first attempt to switch back to the default SIM occurs after 60 minutes. If it fails, the second attempt is made after 30 minutes. The third attempt follows after 50 minutes (30 + 20), and the fourth after 70 minutes (30 + 20 + 20).

Example 2: Data Limit Switching

This configuration shows a switch to the second SIM card after the data limit of 800 MB is exceeded on the first (default) SIM. An SMS is sent upon reaching 400 MB (requires enabling on the *SMS Configuration* page). The billing period starts on the 18th day of the month.



Data Limit	800		MiB	1-2097152 MiB
Warning Threshold	50		%	50-99%
Accounting Start	18	1		1-28
SIM Card	enabled	enabled		
Registration Timeout *			sec	
Roaming State	not applicable	not applicable		
Data Limit State	not applicable	not applicable		
Digital Input 0 State	not applicable	not applicable		
Default SIM Card	1st			
Initial State	online			

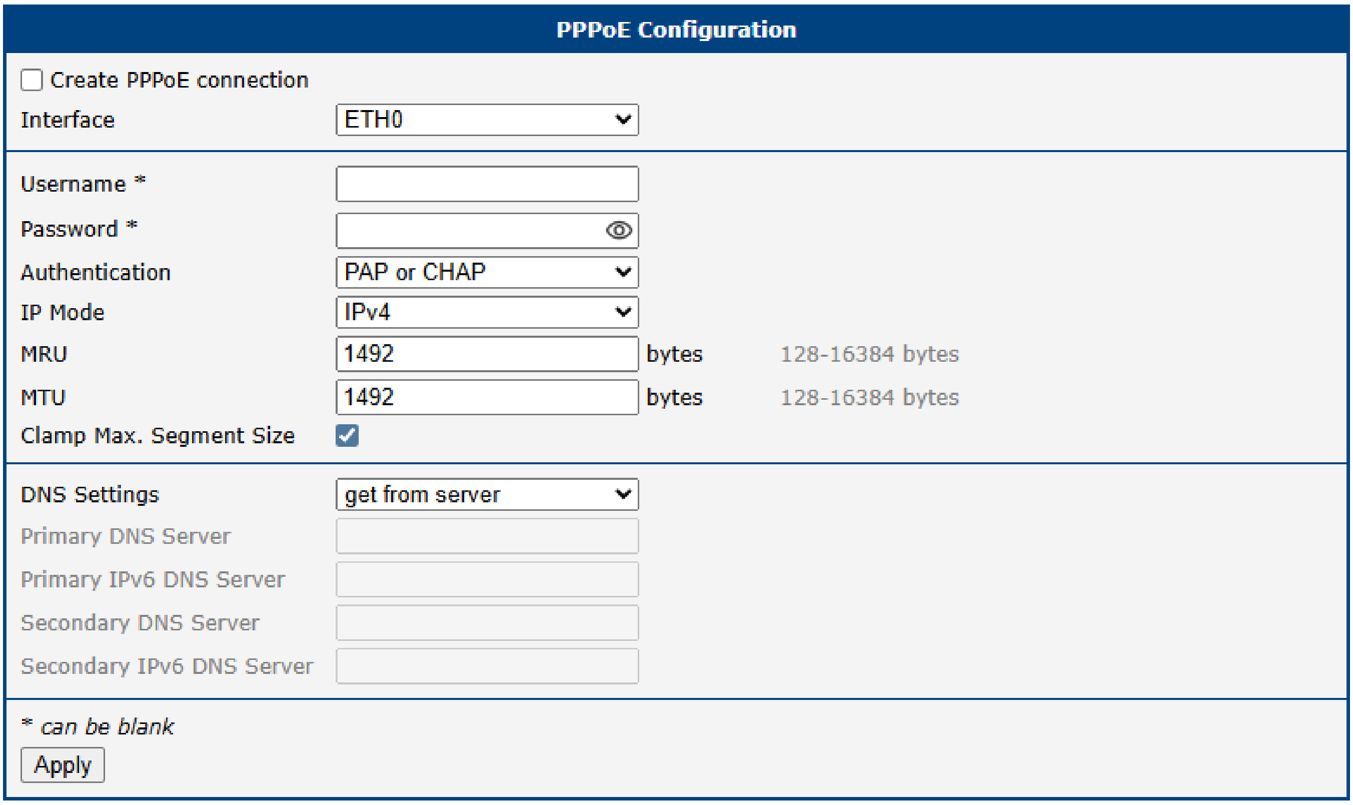
□ Switch to other SIM card when connection fails
□ Switch to default SIM card after timeout

Initial Timeout		min	1-10000 min
Subsequent Timeout *		min	0-10000 min
Additive Constant *		min	0-1000 min

Figure 31: SIM card switching example 2

3.5 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

☐ Create PPPoE connection

Interface	ETH0		
Username *			
Password *			
Authentication	PAP or CHAP		
IP Mode	IPv4		
MRU	1492	bytes	128-16384 bytes
MTU	1492	bytes	128-16384 bytes
Clamp Max. Segment Size	☑		
DNS Settings	get from server		
Primary DNS Server			
Primary IPv6 DNS Server			
Secondary DNS Server			
Secondary IPv6 DNS Server			

** can be blank*

Apply

Figure 32: PPPoE configuration page

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.

Table 37: PPPoE configuration options

Item	Description
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	Defines the Maximum Receive Unit in bytes, which is the largest packet size the router can receive. The default is 1492 bytes.
MTU	Defines the Maximum Transmission Unit in bytes, which is the largest packet size the router can transmit. The default is 1492 bytes.
Clamp Max. Segment Size	When enabled (default), this option automatically adjusts the TCP Maximum Segment Size (MSS) to prevent fragmentation, which can improve performance and reliability.
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.

Table 37: (continued)

Warning

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

3.6 WiFi

3.6.1 Access Point

Warning

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. For more details, please refer to Chapter *3.6.3 Country*.

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.
The tables below list the available configuration options.

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). 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 Chapter *3.1 Ethernet* for further details.

Table 38: Wi-Fi configuration items description

Item	Description
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.
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, but the original length is maintained. 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. This feature is suitable for simple applications that require QoS but does not guarantee network throughput.
Follow STA radio settings	When enabled, if the STA (Station) 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. 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.

Table 38: (continued)

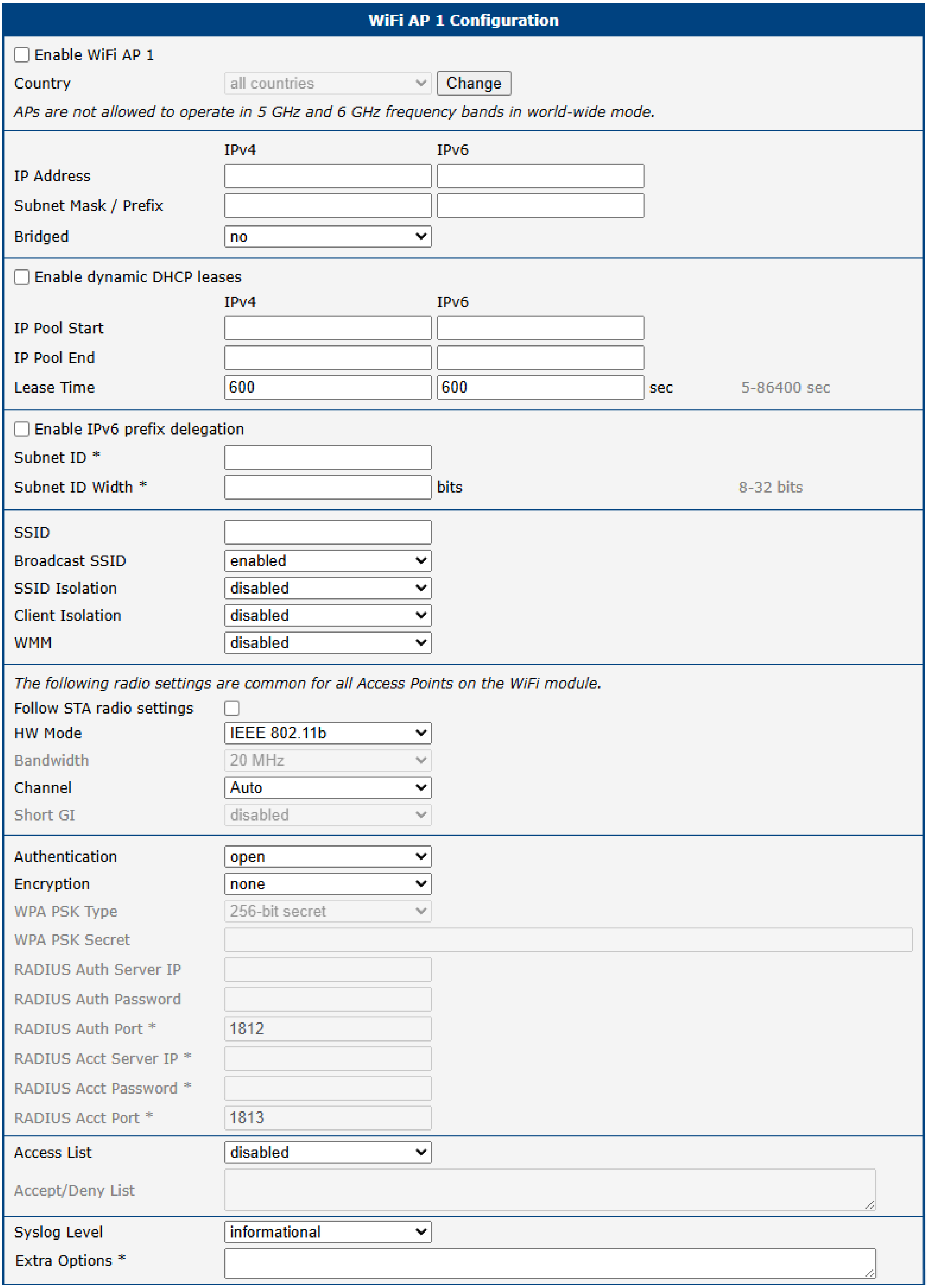
Item	Description
Bandwidth[1]	Allows you to select the transfer bandwidth. This option may be unavailable for some hardware modes. If the selected bandwidth is occupied, the router may automatically switch to a lower bandwidth. This setting is shared by both Access Point 1 and Access Point 2.
Channel[1]	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, the interpretation of the channel number depends on the Wi-Fi band: • In the 2.4 GHz band, the channel number refers to the primary (20 MHz) channel. • In the 5 GHz and 6 GHz bands, the channel number refers to the center frequency of the 40 MHz channel. Note: On NAM routers, only channels 1 to 11 are supported in the 2.4 GHz band.
Short GI	This option, 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 for this option. • **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.
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**: The absolute path to a file containing key-MAC address pairs.
WPA PSK Secret	The secret key or passphrase for WPA-PSK authentication.

Table 38: (continued)

Item	Description
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 logging. • **debugging** • **informational**: The default logging level. • **notification** • **warning**: The lowest level of logging.
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.

Table 38: (continued)

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



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	

Syslog Level	informational
Extra Options *	

Figure 33: Wi-Fi access point configuration page

3.6.2 Station

Warning

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. For more details, please refer to Chapter *3.6.3 Country*.

Info

- You can easily find and connect to an available Wi-Fi network in the GUI. Navigate to *Status* → *Wi-Fi* → *WiFi Scan*, as described in Chapter *2.3.2 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.

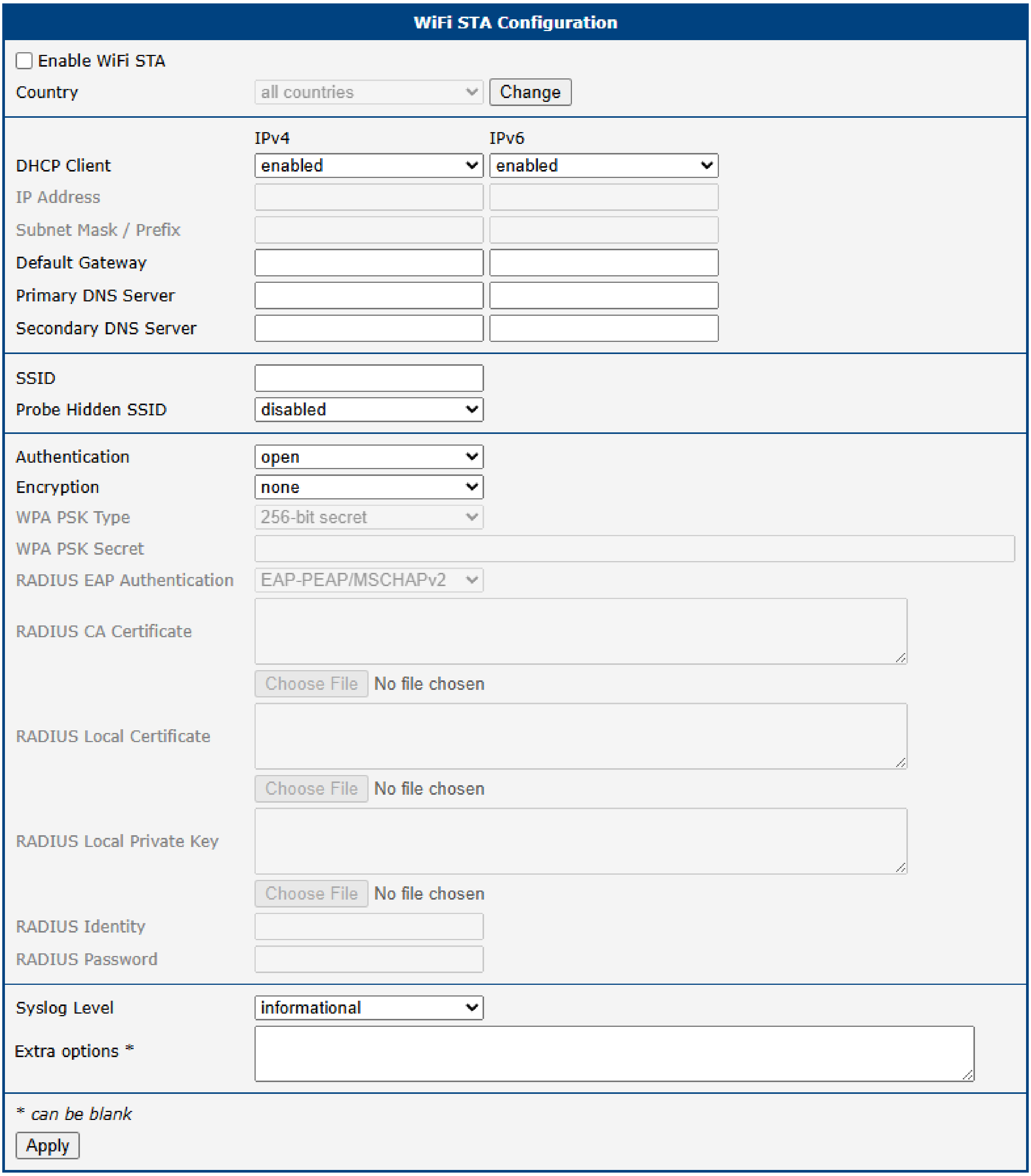
Activate Wi-Fi station mode by checking the *Enable WiFi STA* box at the top of the *Configuration* → *WiFi* → *Station* configuration page. In this mode, the router functions as a client station, connecting to an available access point (AP) and bridging its wired connection to the Wi-Fi network. In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

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). After changing the country, you must review your radio settings.
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.

Table 39: WLAN configuration items description

Item	Description
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 (insecure and may not be supported). • **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.
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). In the case of EAP-TLS, this field is optional and specifies the decryption key for the local private key if it is encrypted.
Syslog Level	The logging level for system log messages: • **verbose debugging**: The highest level of detail. • **debugging** • **informational**: The default level. • **notification** • **warning**: The lowest level of detail.
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. See the *wpa_supplicant.conf* configuration file for details.

Table 39: (continued)



WiFi STA Configuration

☐ Enable WiFi STA

Country	all countries	Change

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

SSID	
Probe Hidden SSID	disabled

Authentication	open
Encryption	none
WPA PSK Type	256-bit secret
WPA PSK Secret	
RADIUS EAP Authentication	EAP-PEAP/MSCHAPv2
RADIUS CA Certificate	Choose File No file chosen
RADIUS Local Certificate	Choose File No file chosen
RADIUS Local Private Key	Choose File No file chosen
RADIUS Identity	
RADIUS Password	

Syslog Level	informational
Extra options *	

** can be blank*

Figure 34: Wi-Fi station configuration page

3.6.3 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.[1]

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.

[1] If the station (STA) connects to an Access Point (AP) 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.

3.7 Backup Routes

The *Backup Routes* feature provides a powerful mechanism for managing WAN (Wide Area Network) connectivity, enabling automatic failover and load balancing across multiple Internet sources. This ensures high availability and optimizes data throughput for critical applications. 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

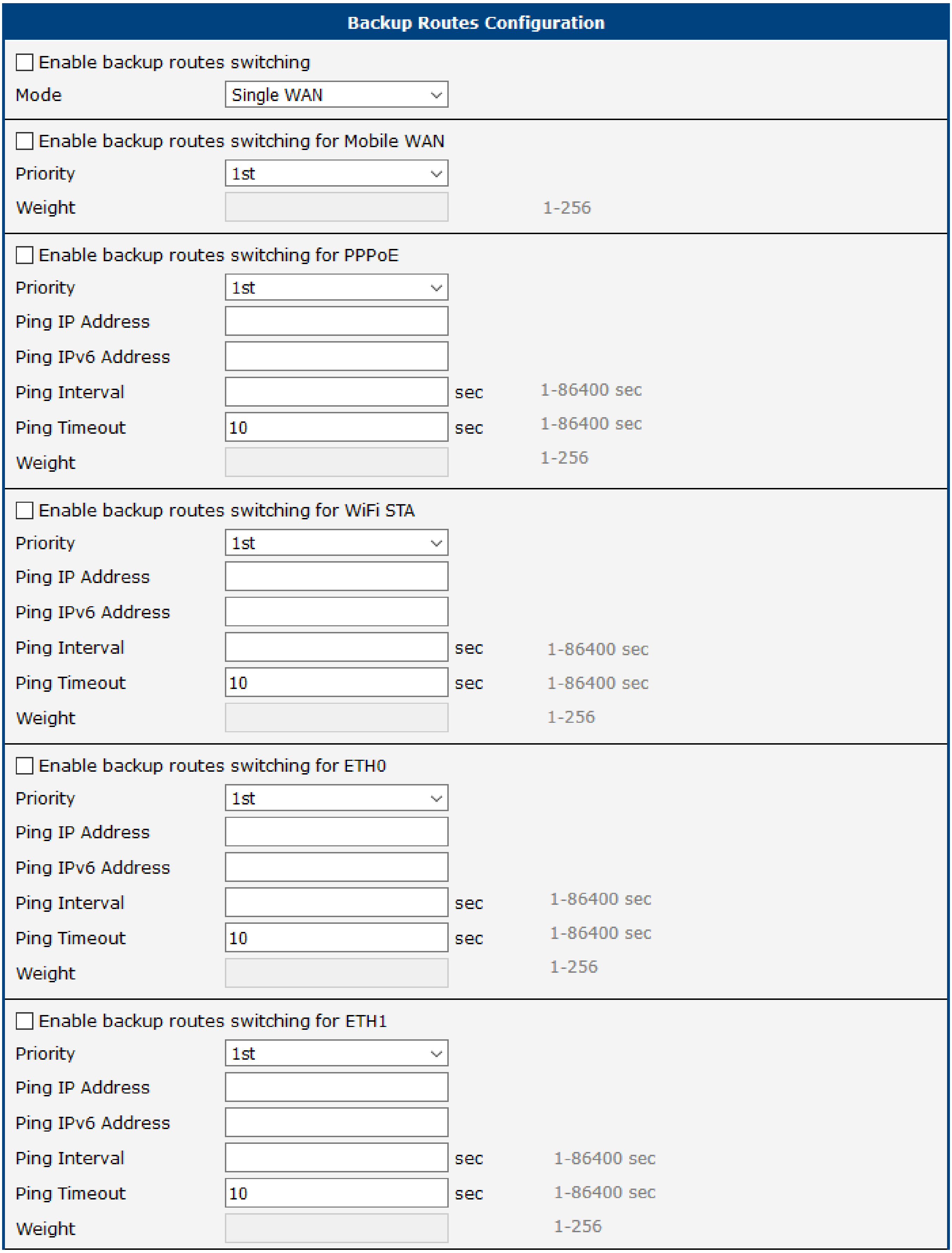
If the *Enable backup routes switching* option is unchecked, the router uses a predefined, internal priority list to select the active WAN interface. This provides a simple, plug-and-play failover mechanism. The default interface priority is as follows:

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. In this mode, it is important to note that a LAN interface (like *ETH0*) can become a WAN interface, 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

☐ Enable backup routes switching

Mode	Single WAN		

☐ Enable backup routes switching for Mobile WAN

Priority	1st		
Weight			1-256

☐ Enable backup routes switching for PPPoE

Priority	1st		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

☐ Enable backup routes switching for WiFi STA

Priority	1st		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

☐ Enable backup routes switching for ETH0

Priority	1st		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

☐ Enable backup routes switching for ETH1

Priority	1st		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

Figure 35: Backup routes configuration page

Operational Modes

The router offers three distinct modes for managing multiple WAN connections:

Item	Description
Mode	Selects the operational mode for managing WAN interfaces: • **Single WAN**: In this mode, only one WAN interface is active at a time. If the primary interface fails, the system automatically switches to the next available interface based on priority. The router is only accessible from the outside on the currently active WAN interface. • **Multiple WANs**: This mode is similar to Single WAN, with one key difference: the router is accessible from the outside on all enabled WAN interfaces simultaneously. Failover still occurs one interface at a time. • **Load Balancing**: This mode allows traffic to be distributed across multiple WAN interfaces simultaneously. You can assign a *Weight* to each interface to control the proportion of data streams it handles.

Table 40: Backup route mode descriptions

Interface Configuration

For each interface you wish to include in the custom 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). In failover modes, the router will always use 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 to have 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 the traffic flows, respectively.

Table 41: Backup routes interface configuration

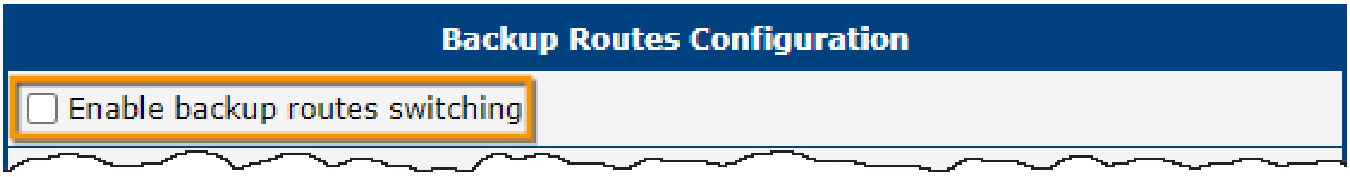
Warning

- **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, you must 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 described in Section 3.7. This provides a simple, automatic failover mechanism. Figure 36 shows the default GUI configuration.



Backup Routes Configuration

□ Enable backup routes switching

Figure 36: GUI configuration for example 1

Figure 37 illustrates the network topology for this example.

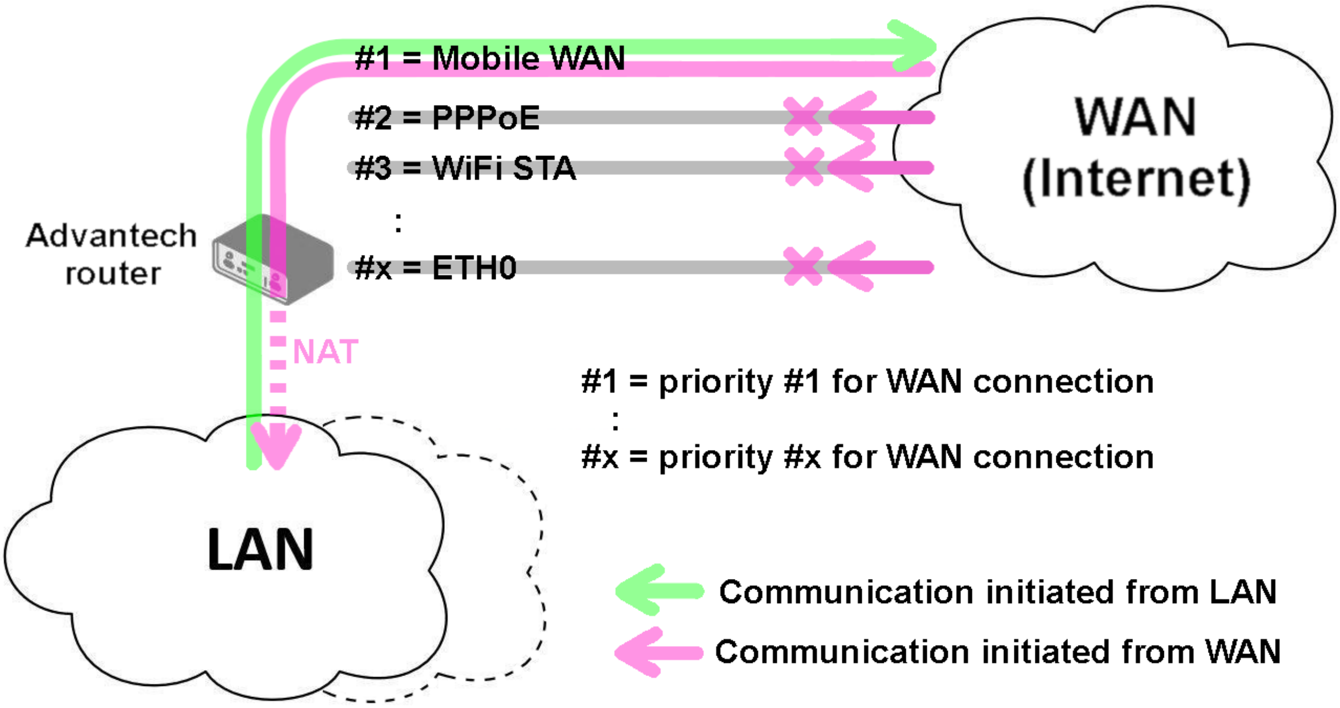
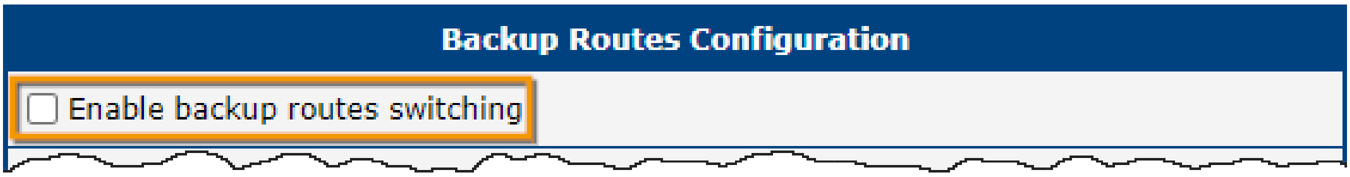

#1 = Mobile WAN
#2 = PPPoE
#3 = WiFi STA
:
#x = ETH0
WAN
(Internet)
Advantech
router
NAT
#1 = priority #1 for WAN connection
:
#x = priority #x for WAN connection
LAN
Communication initiated from LAN
Communication initiated from WAN

Figure 37: Network topology for example 1

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). The configuration remains untouched, as shown in Figure 38.



Backup Routes Configuration

□ Enable backup routes switching

Figure 38: GUI configuration for example 2

Figure 39 illustrates the failover scenario.

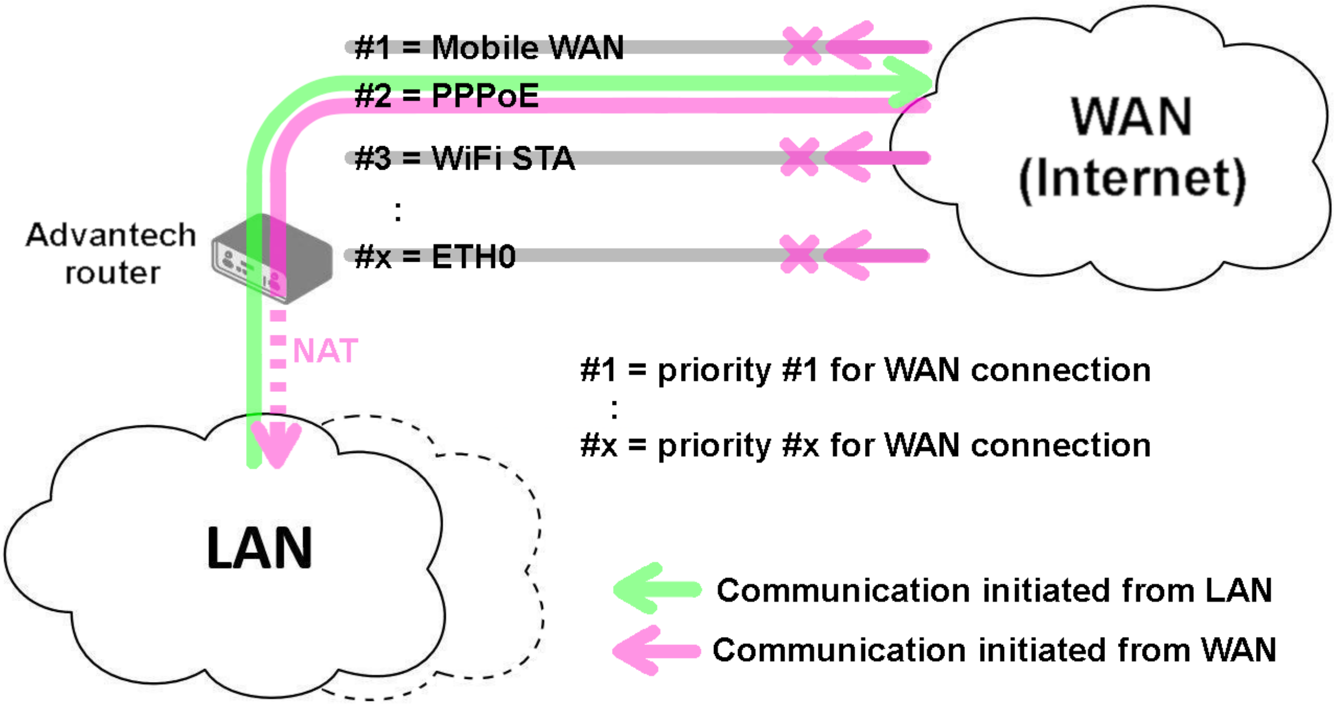
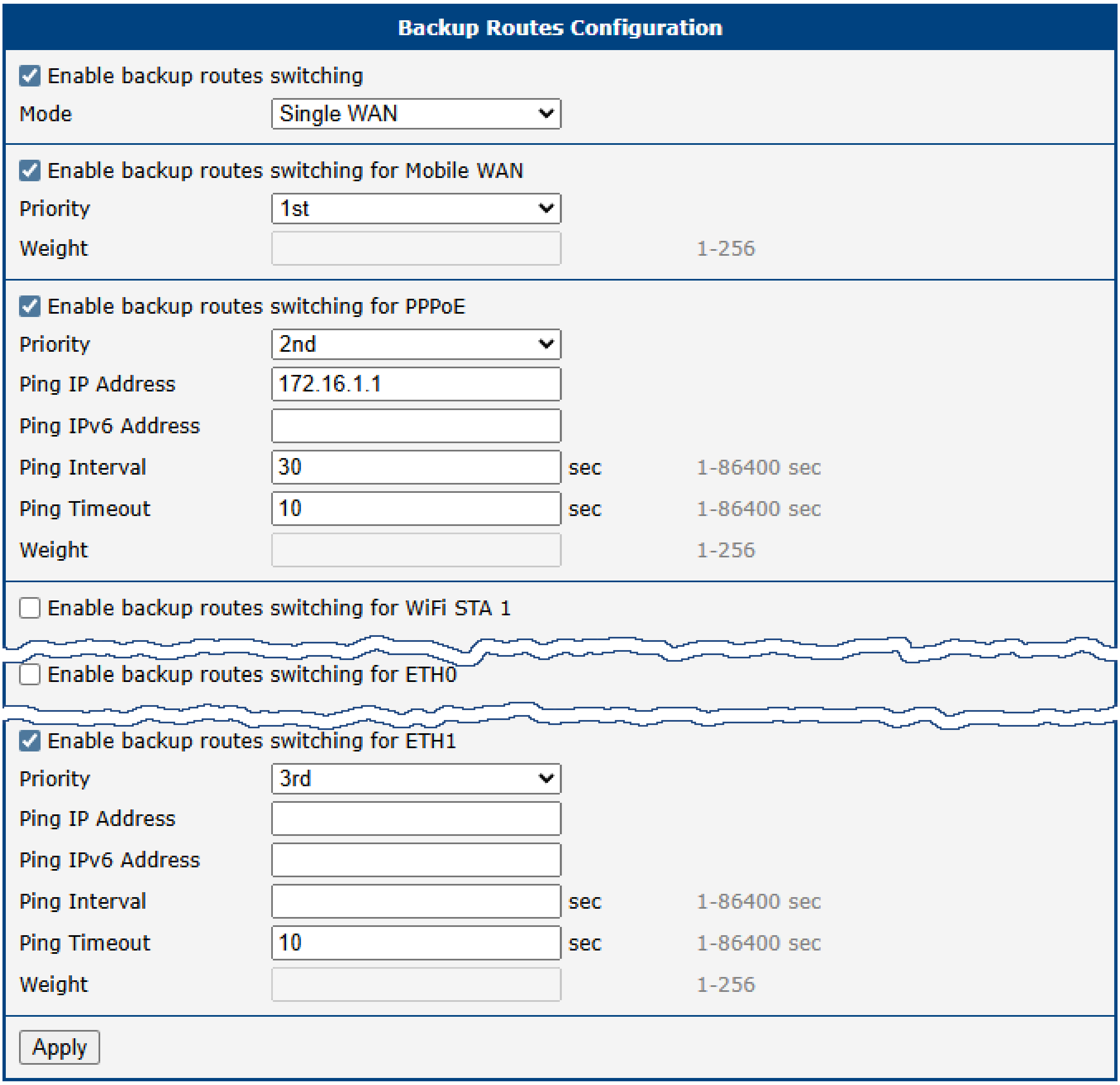

#1 = Mobile WAN
#2 = PPPoE
#3 = WiFi STA
:
#x = ETH0
WAN
(Internet)
Advantech
router
NAT
LAN
#1 = priority #1 for WAN connection
:
#x = priority #x for WAN connection
Communication initiated from LAN
Communication initiated from WAN

Figure 39: Network topology for example 2

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 the IP address 172.16.1.1.
Figure 40 shows the GUI configuration for this scenario.



Backup Routes Configuration

☑ Enable backup routes switching

Mode	Single WAN		

☑ Enable backup routes switching for Mobile WAN

Priority	1st		
Weight			1-256

☑ Enable backup routes switching for PPPoE

Priority	2nd		
Ping IP Address	172.16.1.1		
Ping IPv6 Address			
Ping Interval	30	sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

☐ Enable backup routes switching for WiFi STA 1

☐ Enable backup routes switching for ETH0

☑ Enable backup routes switching for ETH1

Priority	3rd		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight			1-256

Figure 40: GUI configuration for example 3

Figure 41 illustrates the topology for *Single WAN* mode. If the Mobile WAN connection fails, the router will failover to the PPPoE tunnel.

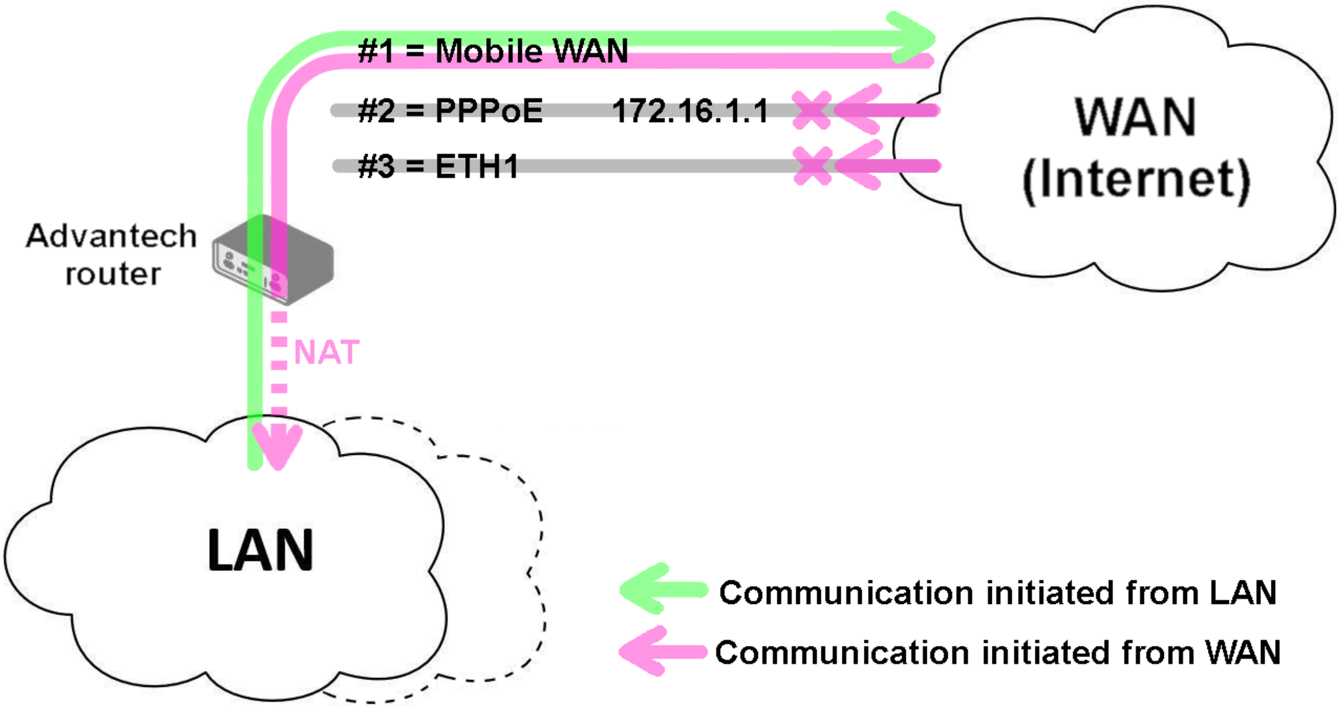


Figure 41: Single WAN mode topology for example 3

Figure 42 shows the same topology in *Multiple WANs* mode. The key difference is that the router can be accessed from the Internet via the public IP addresses of all three interfaces simultaneously, even though only one is used for outbound traffic at a time.

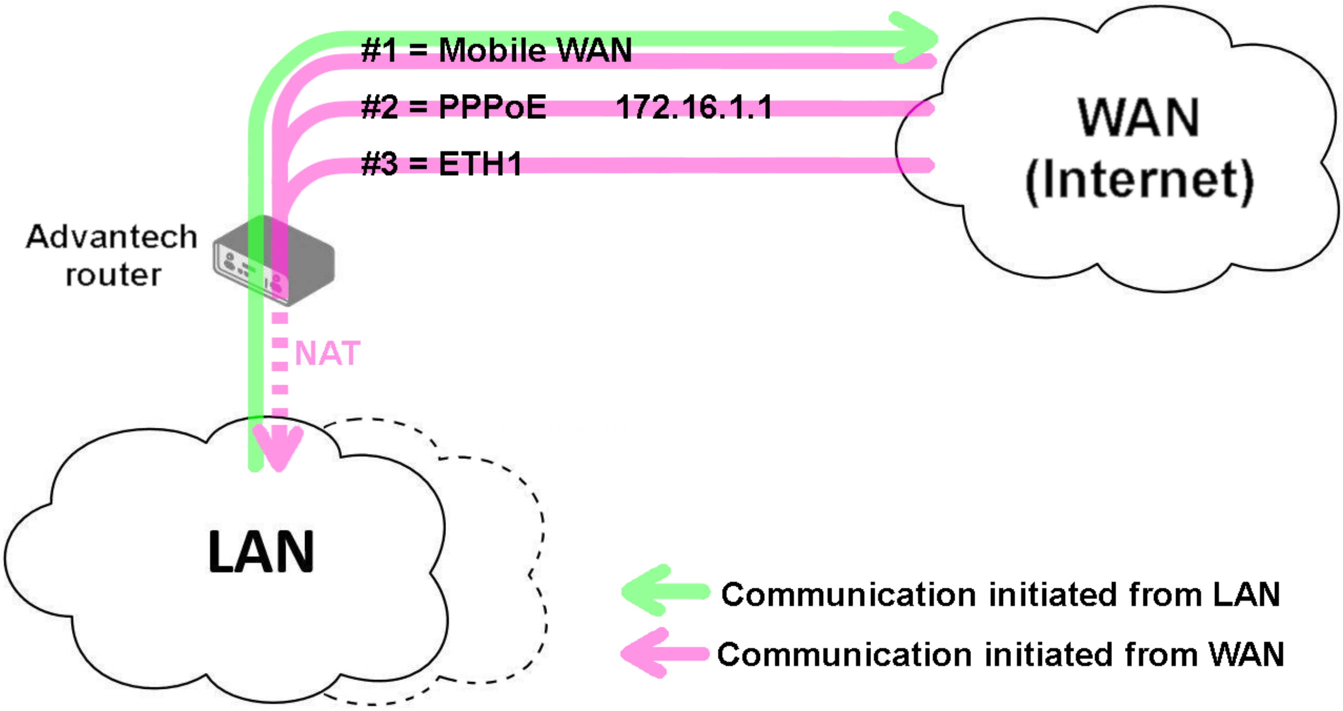
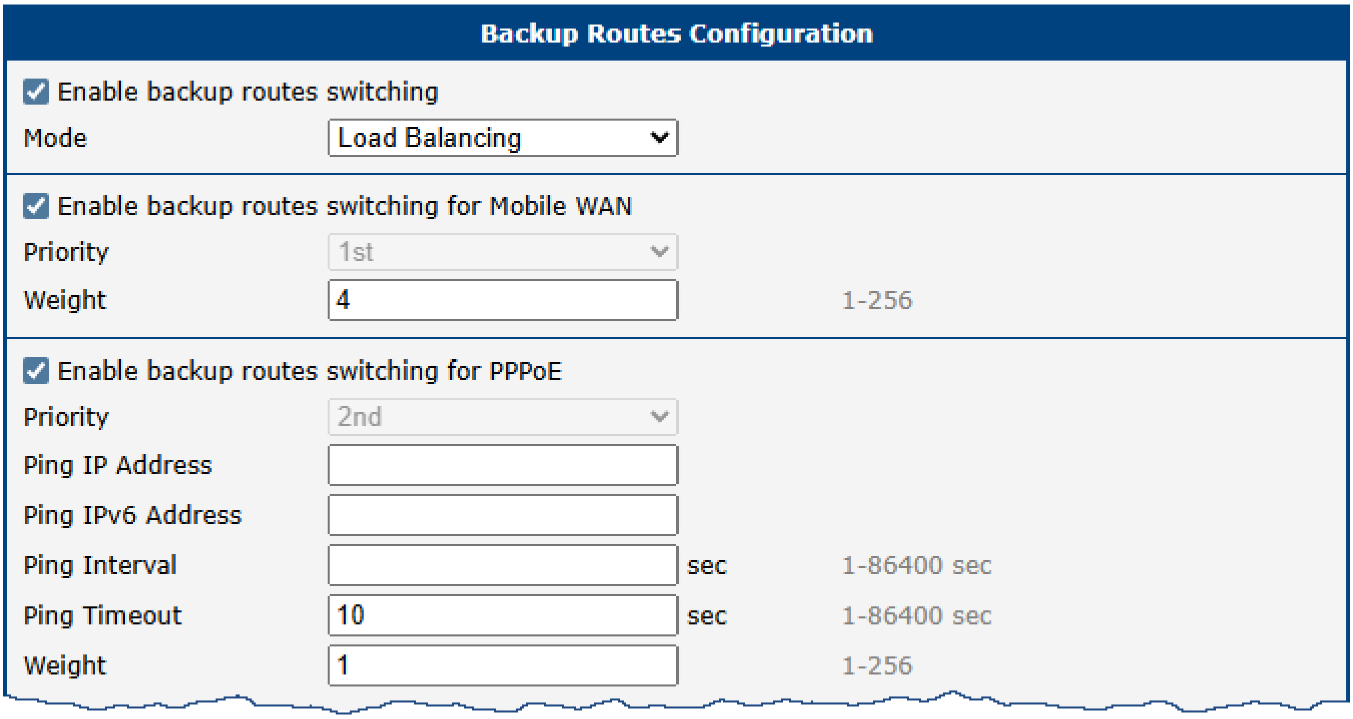


Figure 42: Multiple WANs mode topology for example 3

Example 4: Load Balancing Mode

This example shows a simple 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, while the PPPoE interface will handle the remaining 20%. Figure 43 shows the GUI configuration.



Backup Routes Configuration

☑ Enable backup routes switching

Mode	Load Balancing		

☑ Enable backup routes switching for Mobile WAN

Priority	1st		
Weight	4		1-256

☑ Enable backup routes switching for PPPoE

Priority	2nd		
Ping IP Address			
Ping IPv6 Address			
Ping Interval		sec	1-86400 sec
Ping Timeout	10	sec	1-86400 sec
Weight	1		1-256

Figure 43: GUI configuration for example 4

Figure 44 illustrates the corresponding network topology.

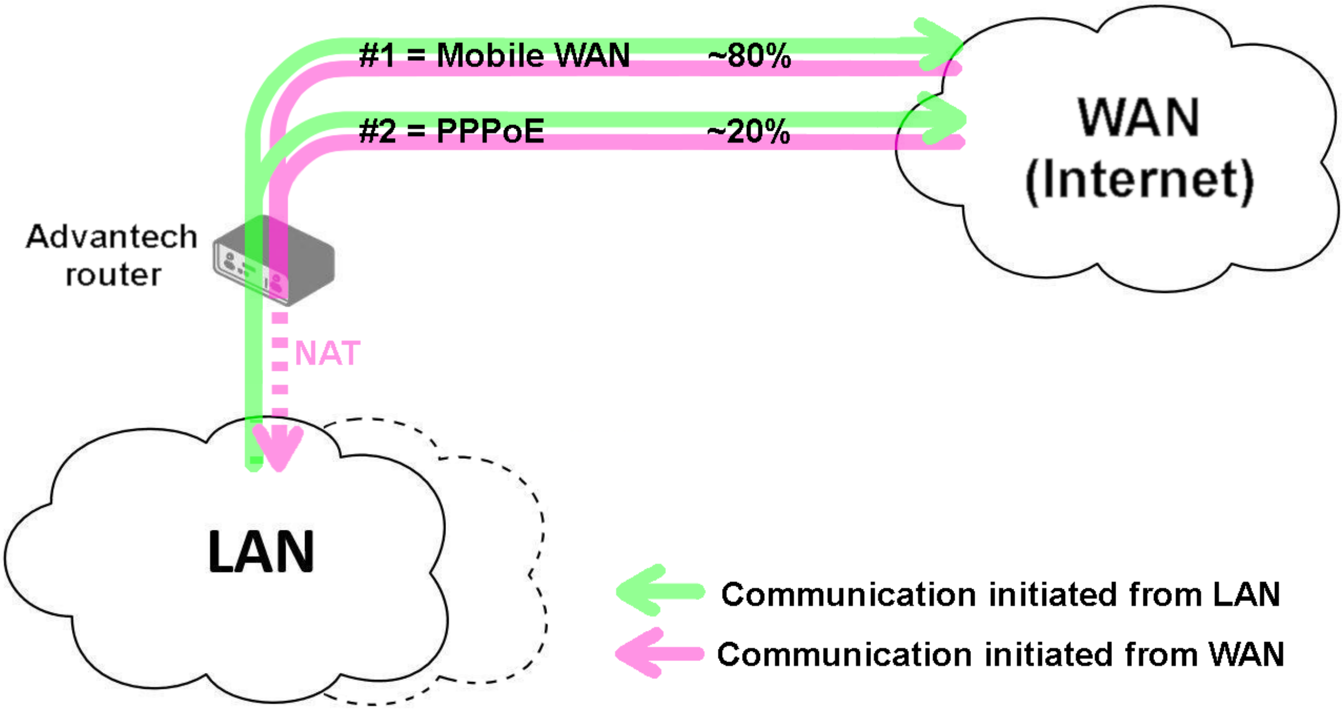
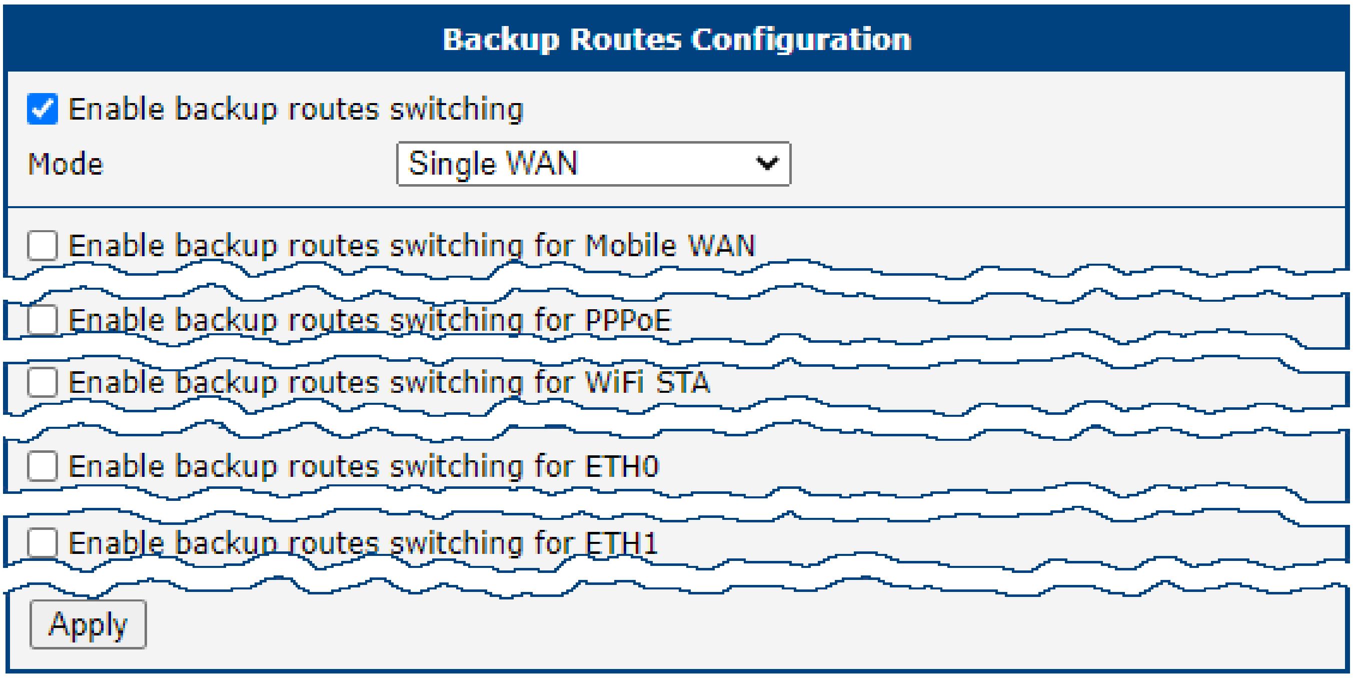


Figure 44: Network topology for example 4

Example 5: No WAN Routes

If *Backup Routes* is enabled but no interfaces are selected for WAN routing, the router will not have a dedicated WAN connection. In this state, it functions purely as a LAN router, forwarding traffic between its local network segments. The Mobile WAN interface will not be used, even if it is connected to a cellular network. Figure 45 shows this configuration.



Backup Routes Configuration

☑ Enable backup routes switching

Mode: Single WAN

☐ Enable backup routes switching for Mobile WAN

☐ Enable backup routes switching for PPPoE

☐ Enable backup routes switching for WiFi STA

☐ Enable backup routes switching for ETH0

☐ Enable backup routes switching for ETH1

Figure 45: GUI configuration for example 5

Figure 46 illustrates the resulting topology.

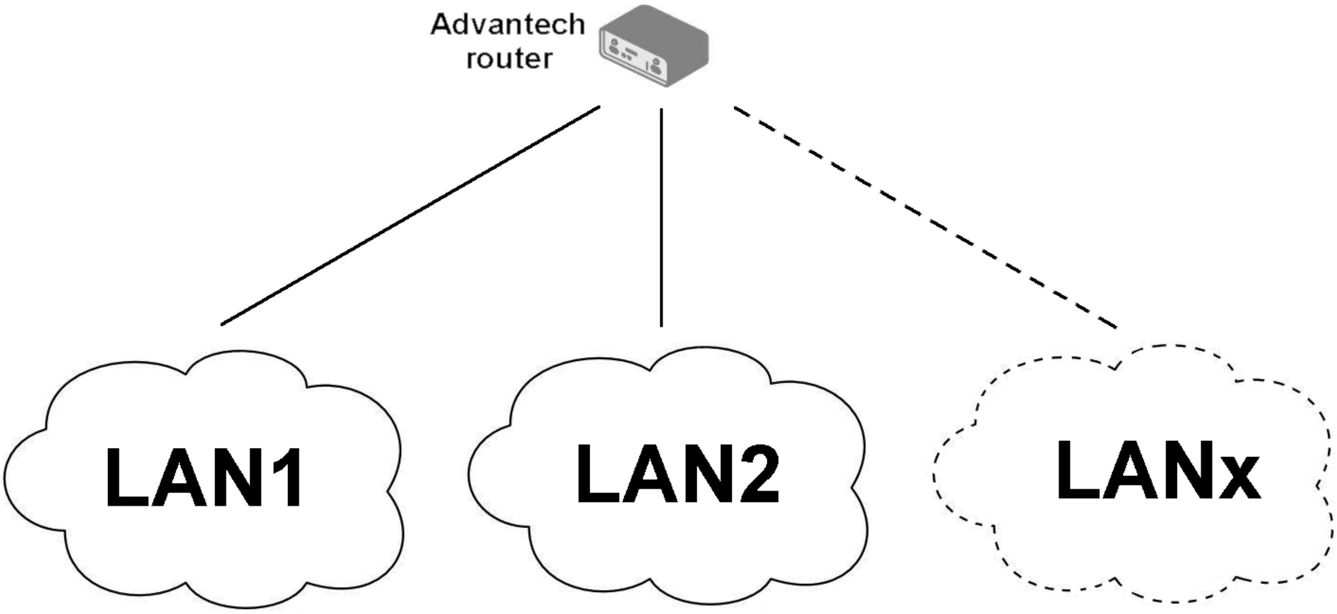
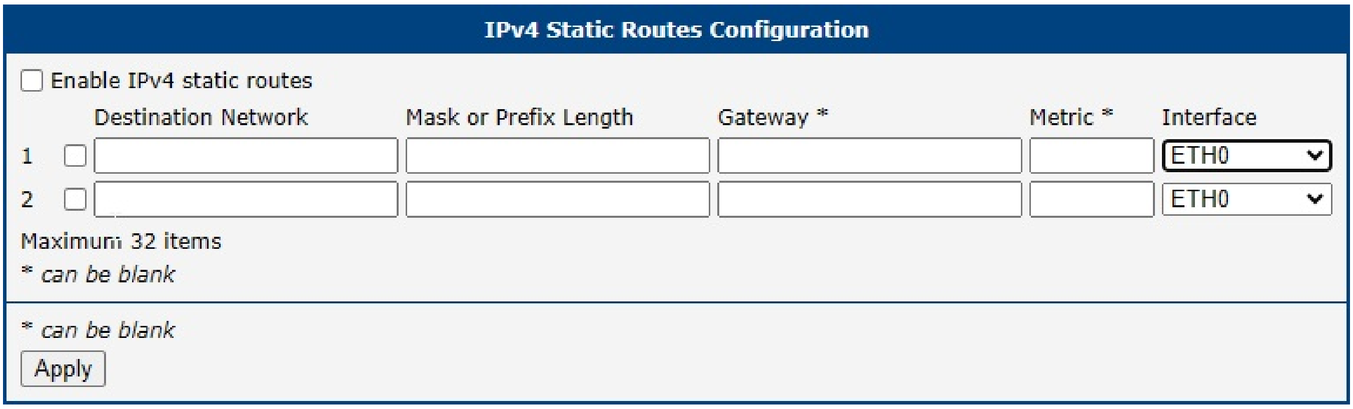


Figure 46: Network topology for example 5

3.8 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.


IPv4 Static Routes Configuration

□ Enable IPv4 static routes

		Destination Network	Mask or Prefix Length	Gateway *	Metric *	Interface
1	□					ETH0
2	□					ETH0

Maximum 32 items

* can be blank

* can be blank

Figure 47: Static routes configuration page

The parameters for defining a static route are described below.

Item	Description
Enable IPv4 static routes	The master switch for the static routing feature. If this is 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.

Table 42: Static routes configuration options

[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.

3.9 Firewall

The router's firewall allows you to control both incoming and outgoing IP traffic. Supported are independent IPv4 and IPv6 firewalls, including a dual-stack configuration for both protocols. This chapter describes how to configure the firewall rules.

Info

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.

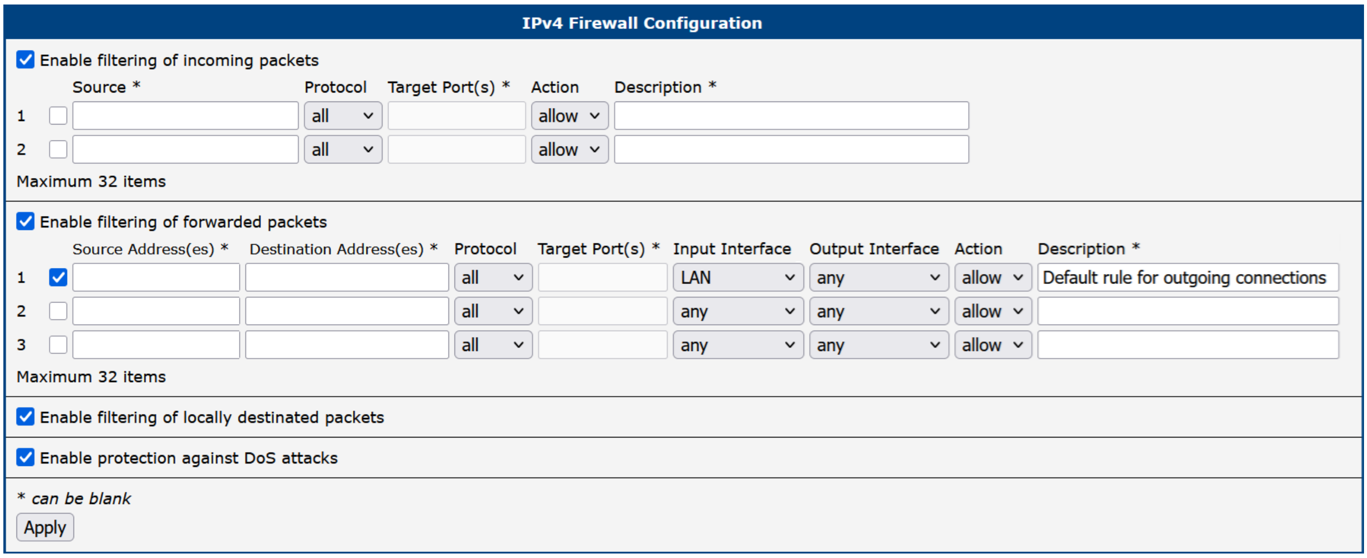
- **LAN Zone (Trusted):** This zone should contain all interfaces configured for your internal, local network. By default, this typically includes the Ethernet LAN ports (e.g., `eth0` , `eth1`) and any configured Wi-Fi Access Points (`wlanX`).
- **WAN Zone (Untrusted):** This zone should contain all 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, see Chapter *3.7 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*.

Figure 48 displays the default configuration page for the IPv4 firewall. The configuration fields are identical for both the *IPv4* and *IPv6* forms.



IPv4 Firewall Configuration

☑ Enable filtering of incoming packets

		Source *	Protocol	Target Port(s) *	Action	Description *
1	☐		all		allow	
2	☐		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		LAN	any	allow	Default rule for outgoing connections
2	☐			all		any	any	allow	
3	☐			all		any	any	allow	

Maximum 32 items

☑ Enable filtering of locally destinated packets

☑ Enable protection against DoS attacks

* *can be blank*

Figure 48: IPv4 default firewall configuration

Info

Starting with firmware version 6.6.0, rule descriptions are stored directly as comments in the system's iptables configuration. This allows users 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. See Table 43 for a description of the incoming rule definitions.

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 Chapter 3.7.

Item	Description
Source[1]	Specifies the IP address to which the rule applies. Use an IPv4 address in the *IPv4 Firewall Configuration* and an IPv6 address in the *IPv6 Firewall Configuration*.
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 the ICMP protocol (ICMPv6 for IPv6 firewall).
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.

Table 43: Incoming packet filtering

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.

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

The configuration form includes a table for specifying filter rules. See Table 44 for a description of the forwarding rule definitions.

Info

As shown in Figure 48, 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 like 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 the *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.

Table 44: Forward packet filtering

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.

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

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.

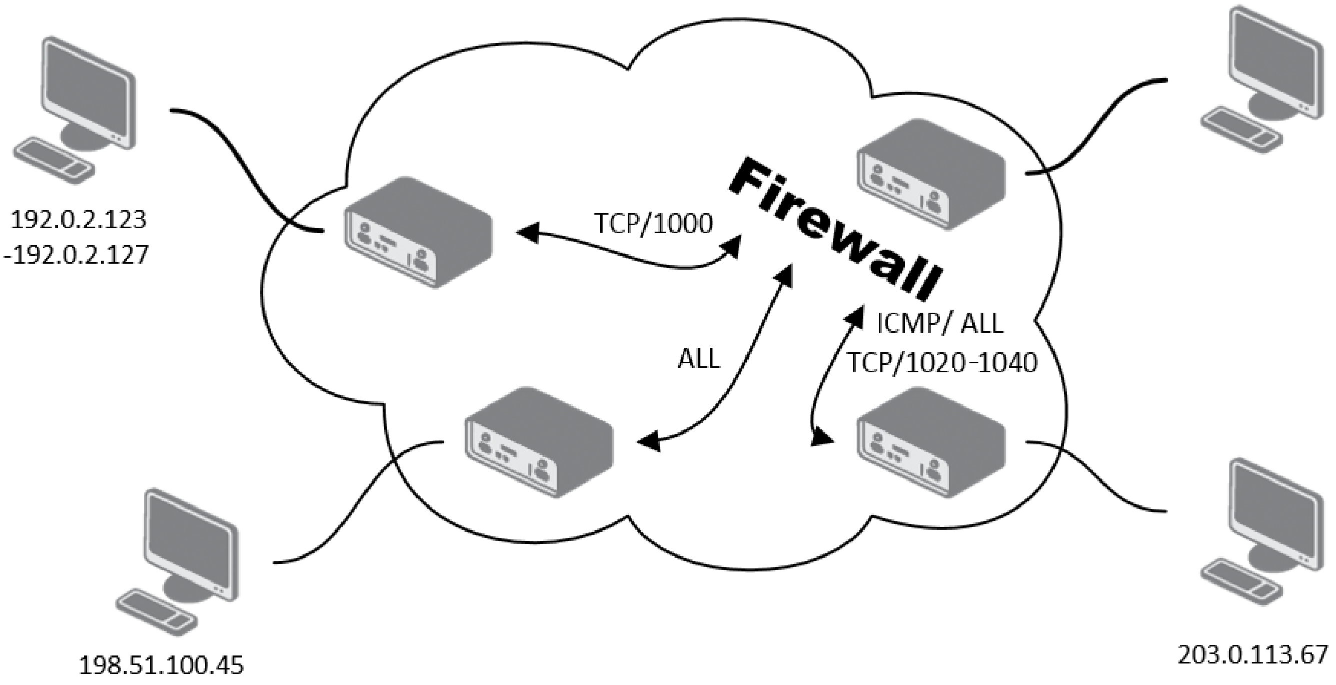
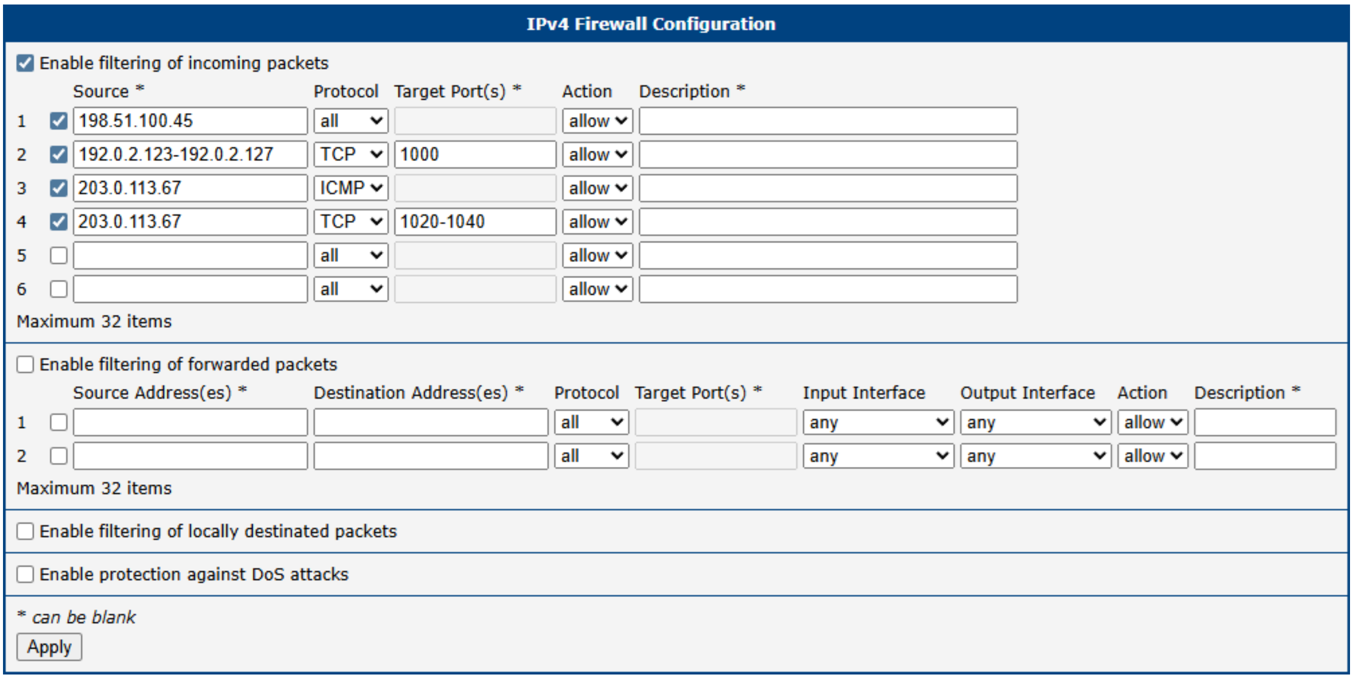


Figure 49: IPv4 firewall configuration topology example



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

Figure 50: IPv4 firewall configuration example

3.9.1 Sites

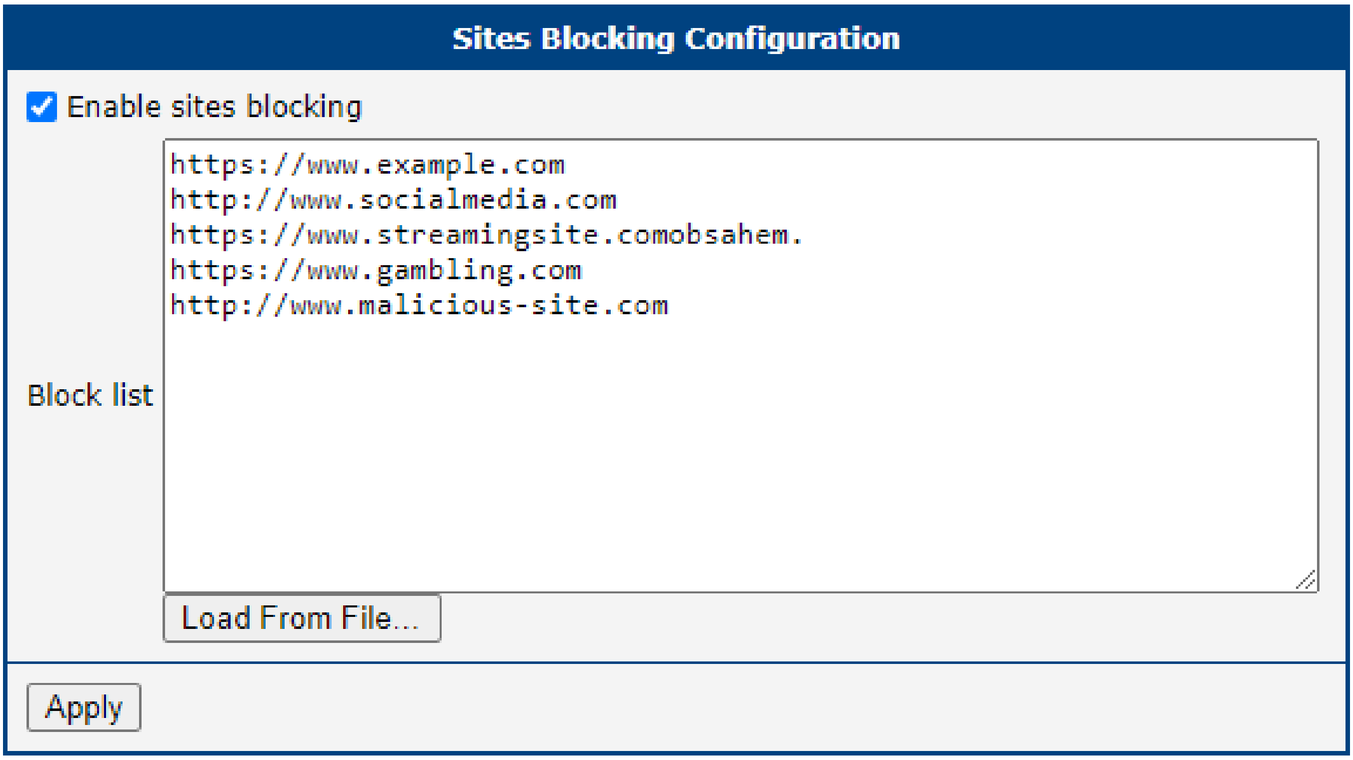
Info

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 (see Figure 51). 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.



Sites Blocking Configuration

☑ Enable sites blocking

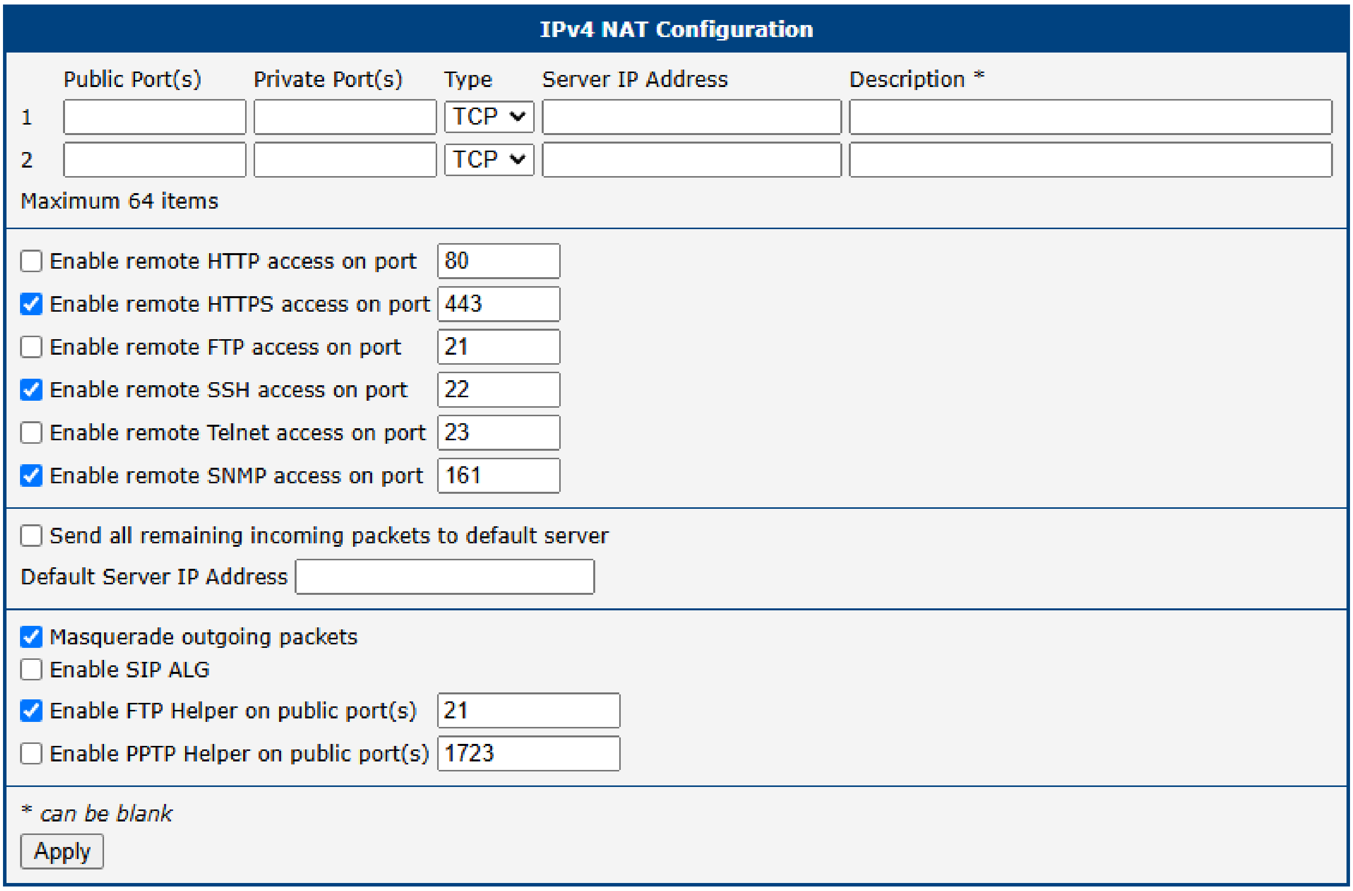
Block list

```
https://www.example.com
http://www.socialmedia.com
https://www.streamingsite.comobsahem.
https://www.gambling.com
http://www.malicious-site.com
```

Figure 51: Firewall sites configuration page

3.10 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*.



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
☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server
Default Server IP Address

☑ Masquerade outgoing packets
☐ Enable SIP ALG
☑ Enable FTP Helper on public port(s) 21
☐ Enable PPTP Helper on public port(s) 1723

* *can be blank*

Figure 52: 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.

Table 45: Port forwarding rule configuration

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:

Code Example

```
iptables -t nat -A pre_nat -p tcp --dport [PORT_PUBLIC] -j DNAT \
--to-destination [IPADDR]:[PORT_PRIVATE]
```

For IPv6, use the `ip6tables` command:

Code Example

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

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	Redirects incoming HTTP requests on the specified port to the router's secure HTTPS web interface. This does not enable unsecured HTTP access.
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.
Enable remote SSH access on port	Allows remote access to the router's command-line interface via SSH.
Enable remote Telnet access on port	Allows insecure remote access to the router's command-line interface via Telnet.
Enable remote SNMP access on port	Allows remote management and monitoring of the router via SNMP.

Table 46: Remote access configuration options

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" or 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.
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	Assists with NAT traversal for the FTP protocol, particularly for active mode FTP, on the specified port (default is 21).
Enable PPTP Helper	(IPv4 only) Assists with NAT traversal for the Point-to-Point Tunneling Protocol (PPTP) for VPN connections on the specified port (default is 1723).

Table 47: Default server and NAT helper configuration

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.

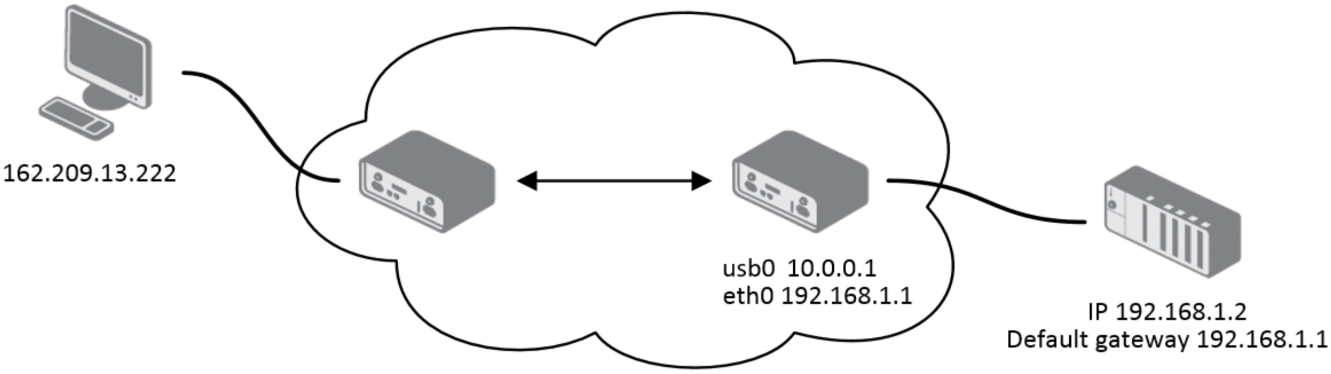
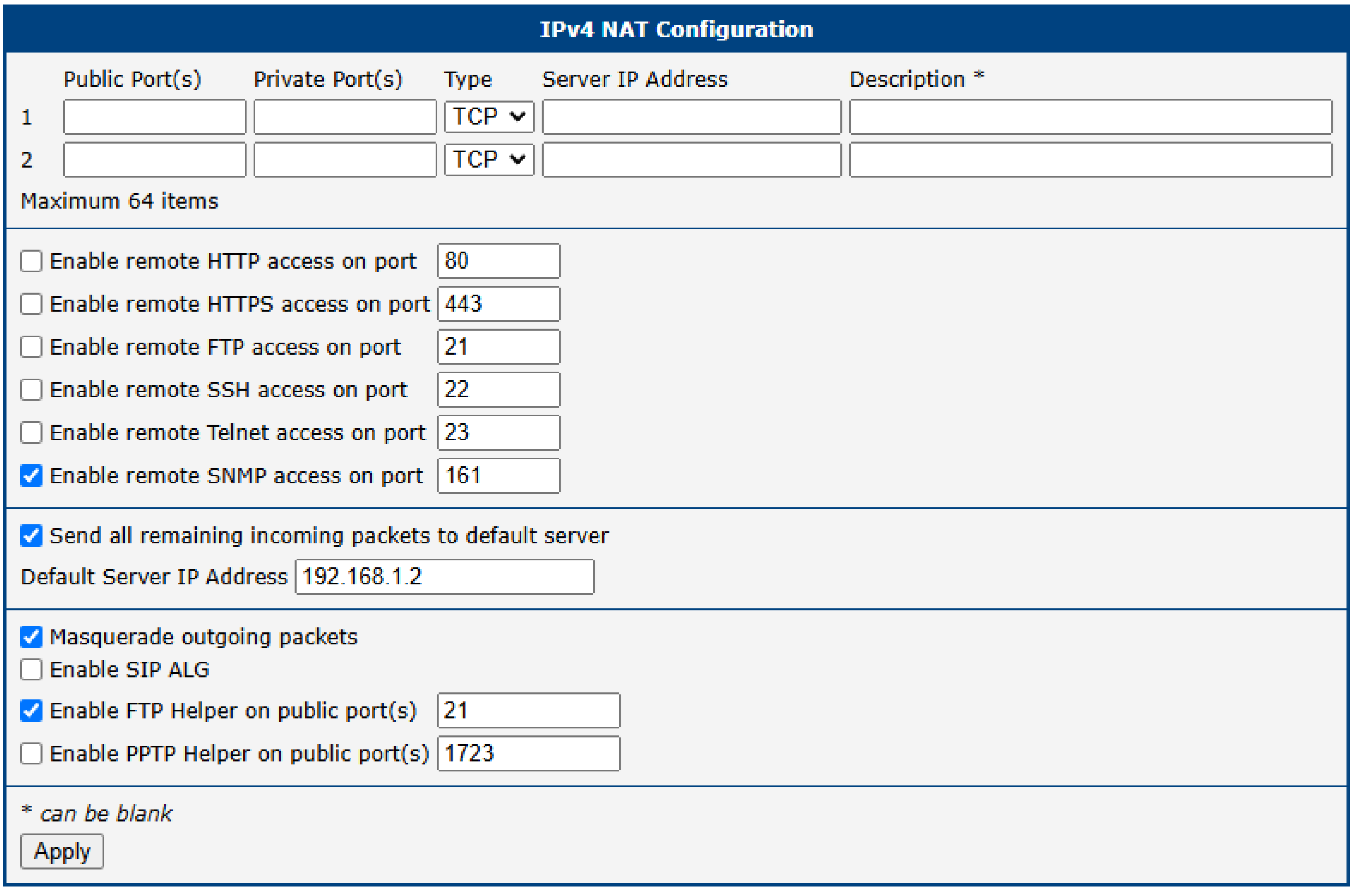


Figure 53: Topology for NAT example 1



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
☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server
Default Server IP Address 192.168.1.2

☑ Masquerade outgoing packets
□ Enable SIP ALG
☑ Enable FTP Helper on public port(s) 21
□ Enable PPTP Helper on public port(s) 1723

* *can be blank*

Figure 54: 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, you would create the following rule:

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

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

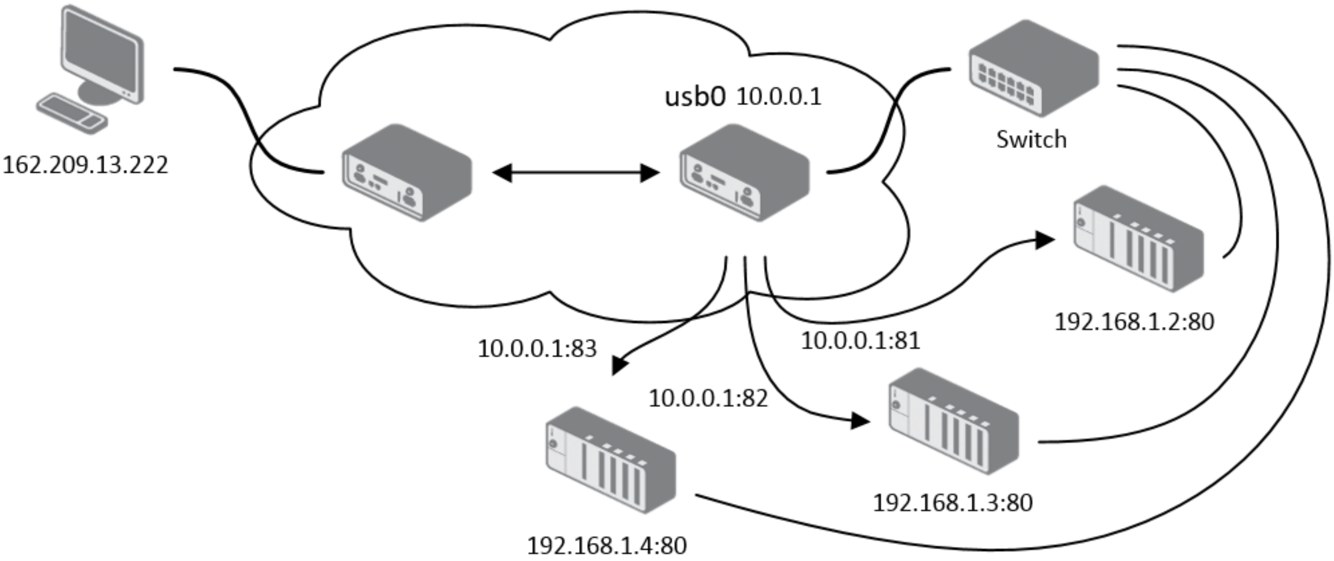
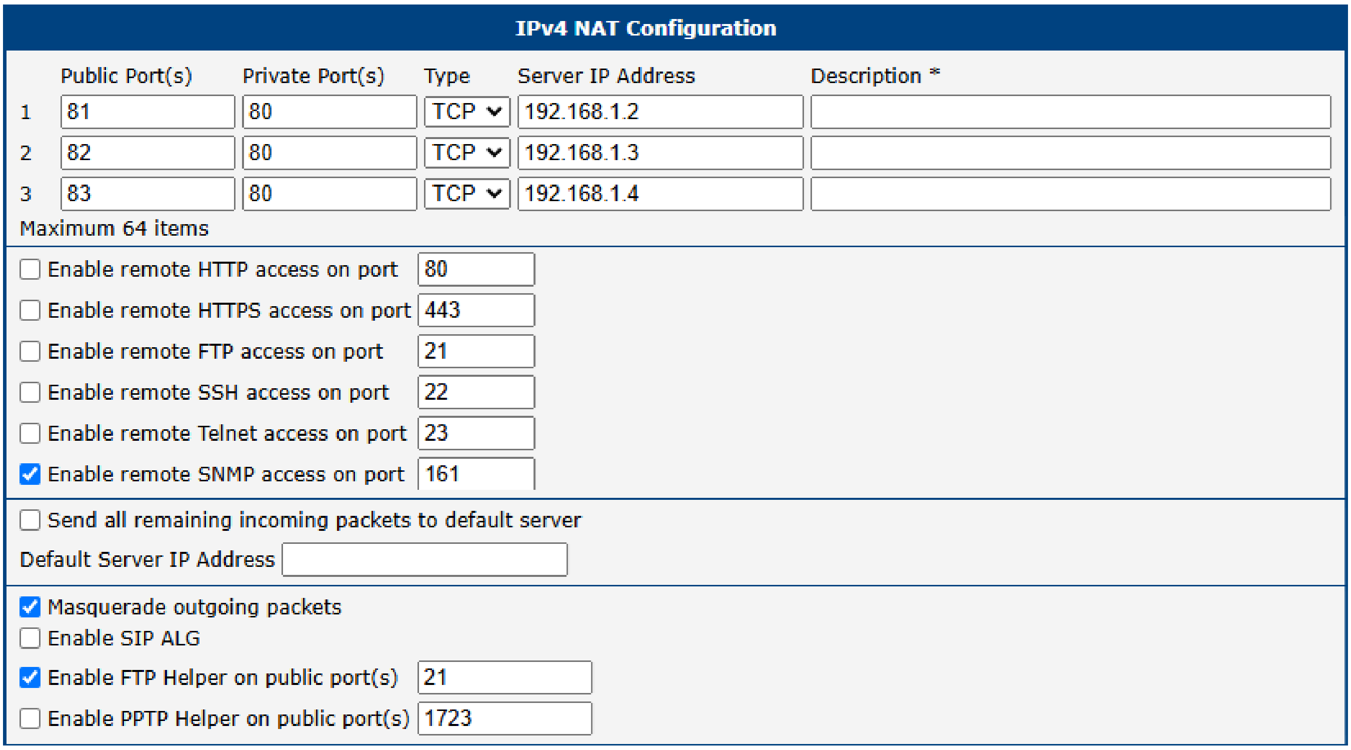


Figure 55: Topology for NAT example 2



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	

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
☑ Enable remote SNMP access on port 161

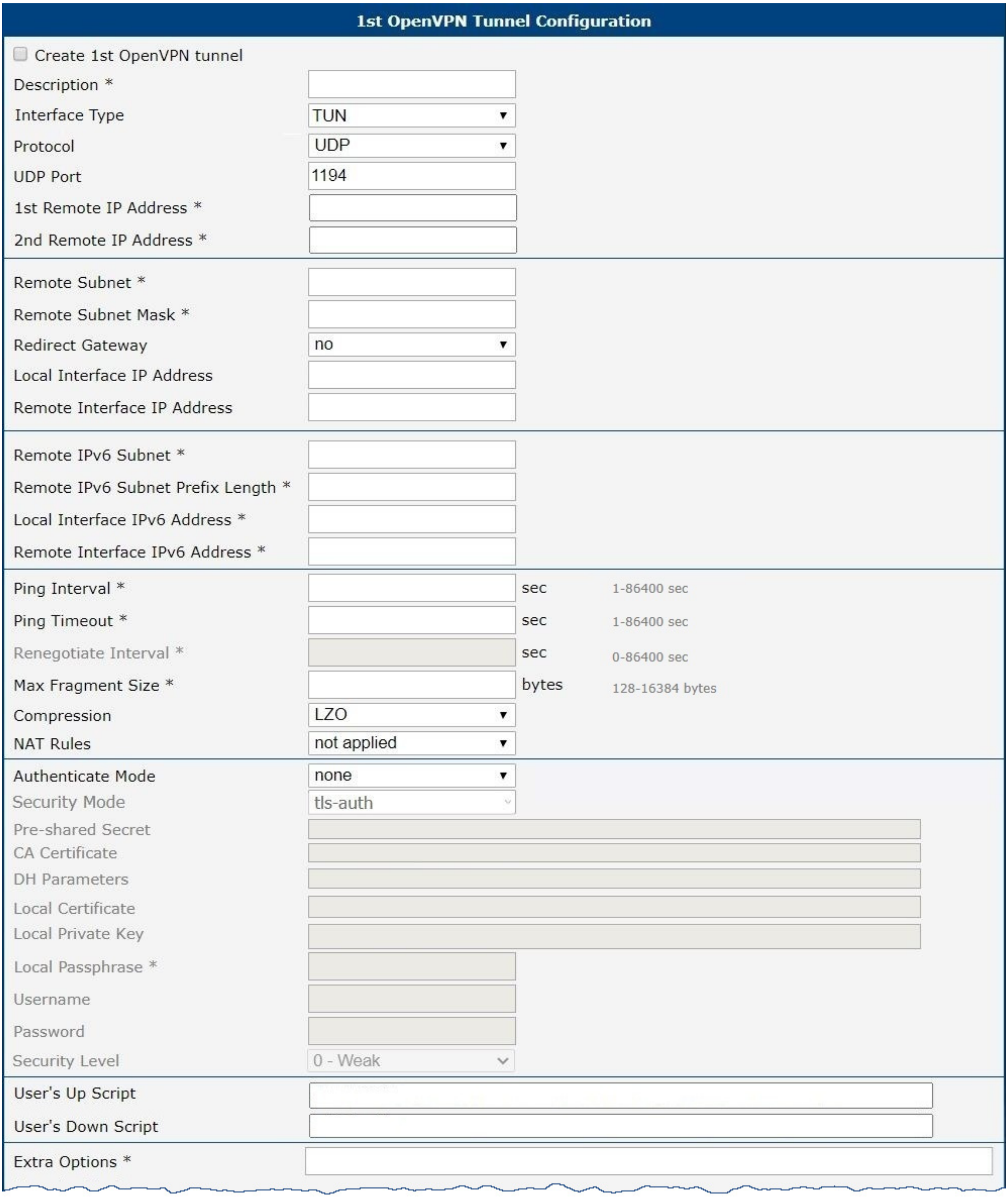
☐ Send all remaining incoming packets to default server
Default Server IP Address

☑ Masquerade outgoing packets
☐ Enable SIP ALG
☑ Enable FTP Helper on public port(s) 21
☐ Enable PPTP Helper on public port(s) 1723

Figure 56: NAT configuration for example 2

3.11 OpenVPN

OpenVPN is a robust and highly flexible Virtual Private Network (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. The settings are managed on the *Configuration* → *OpenVPN* page, which contains separate tabs for each 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	1-86400 sec
Ping Timeout *		sec	1-86400 sec
Renegotiate Interval *		sec	0-86400 sec
Max Fragment Size *		bytes	128-16384 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			
User's Down Script			
Extra Options *			

Figure 57: OpenVPN tunnel configuration page

Tunnel Configuration

The following tables describe 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 itself.
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 the *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.
Compression	Configures data compression for the VPN tunnel. • **None**: [Recommended] No compression is used. This is the most secure setting and avoids any known vulnerabilities. • **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** and it is provided only for backward compatibility with legacy systems.
NAT Rules	Determines if NAT should be applied to traffic passing through the tunnel.

Table 48: OpenVPN configuration items

Authentication and Security

OpenVPN offers multiple methods for authentication, 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 Public Key Infrastructure (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 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.** [Default] • **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).
User's Up/Down Script[2]	Custom shell scripts that are executed when the tunnel is established or torn down.
Extra Options	A field for adding any additional OpenVPN command-line parameters.

Table 49: Authentication and security options

[1] For a detailed explanation of security levels, see the *Security Guidelines* [15], 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.

Configuration Example

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

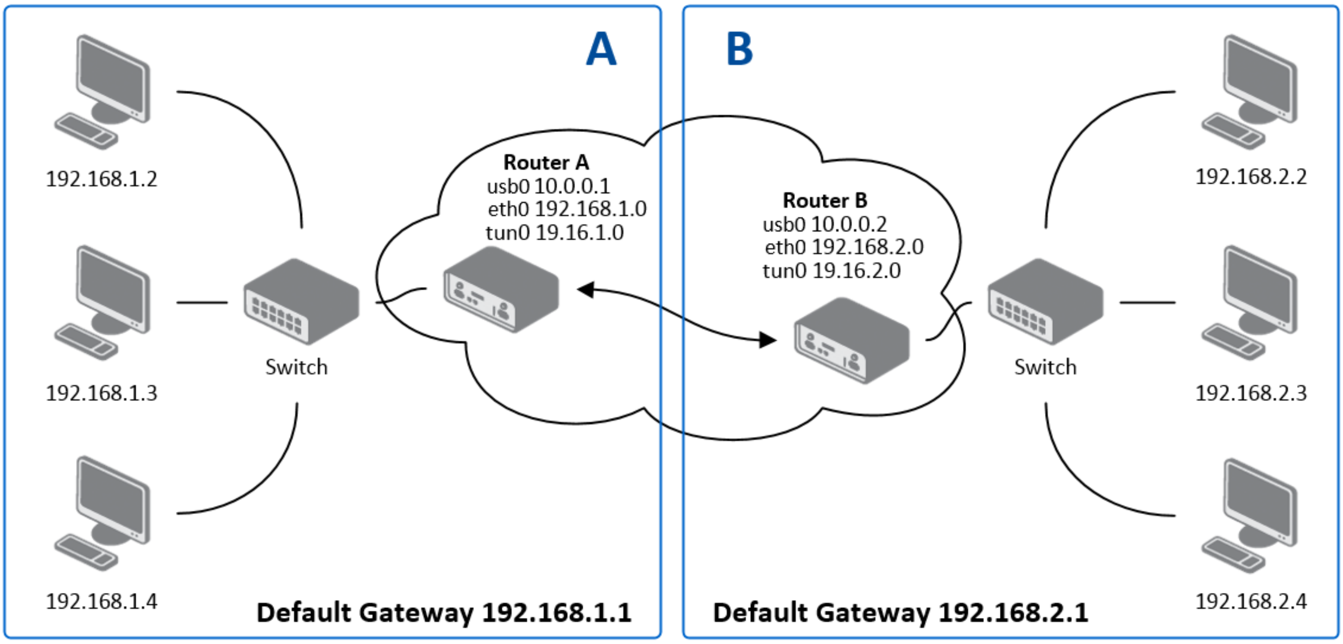


Figure 58: An example of OpenVPN topology

Parameter	Router A	Router B
Protocol	UDP	UDP
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	19.16.1.0	19.16.2.0
Remote Interface IP	19.16.2.0	19.16.1.0
Compression	none	none
Authentication Mode	none	none

Table 50: OpenVPN configuration example

Info

For more detailed examples, including certificate-based authentication, please refer to the *OpenVPN Tunnel* Application Note [6].

3.12 IPsec

The IPsec tunnel function allows you to create a secure connection between two separate LAN networks. This router family allows you to create up to four IPsec tunnels.

To open the IPsec tunnel configuration page, click *IPsec* in the *Configuration* section of the main menu. The menu item will expand, and you will see separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel*, and *4th Tunnel*.

Both **policy-based** and **route-based** VPN approaches are supported—see the different configuration scenarios in Chapter 3.12.

IPv4 and IPv6 tunnels are supported (**dual stack**). You can transport IPv6 traffic through an IPv4 tunnel and vice versa. For different IPsec authentication scenarios, see Chapter 3.12.

Warning

- To encrypt data between the 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 the packets matching those settings.
- For an optimal and secure setup, we recommend following the instructions on the Security Recommendations page of the *strongSwan* website.

Info

- Detailed information and more examples of IPsec tunnel configuration can be found in the application note *IPsec Tunnel* [7].
- 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.

Route-based Configuration Scenarios

The most common route-based scenarios for Advantech routers are:

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**
   - 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**
   - 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

Four basic authentication options are supported:

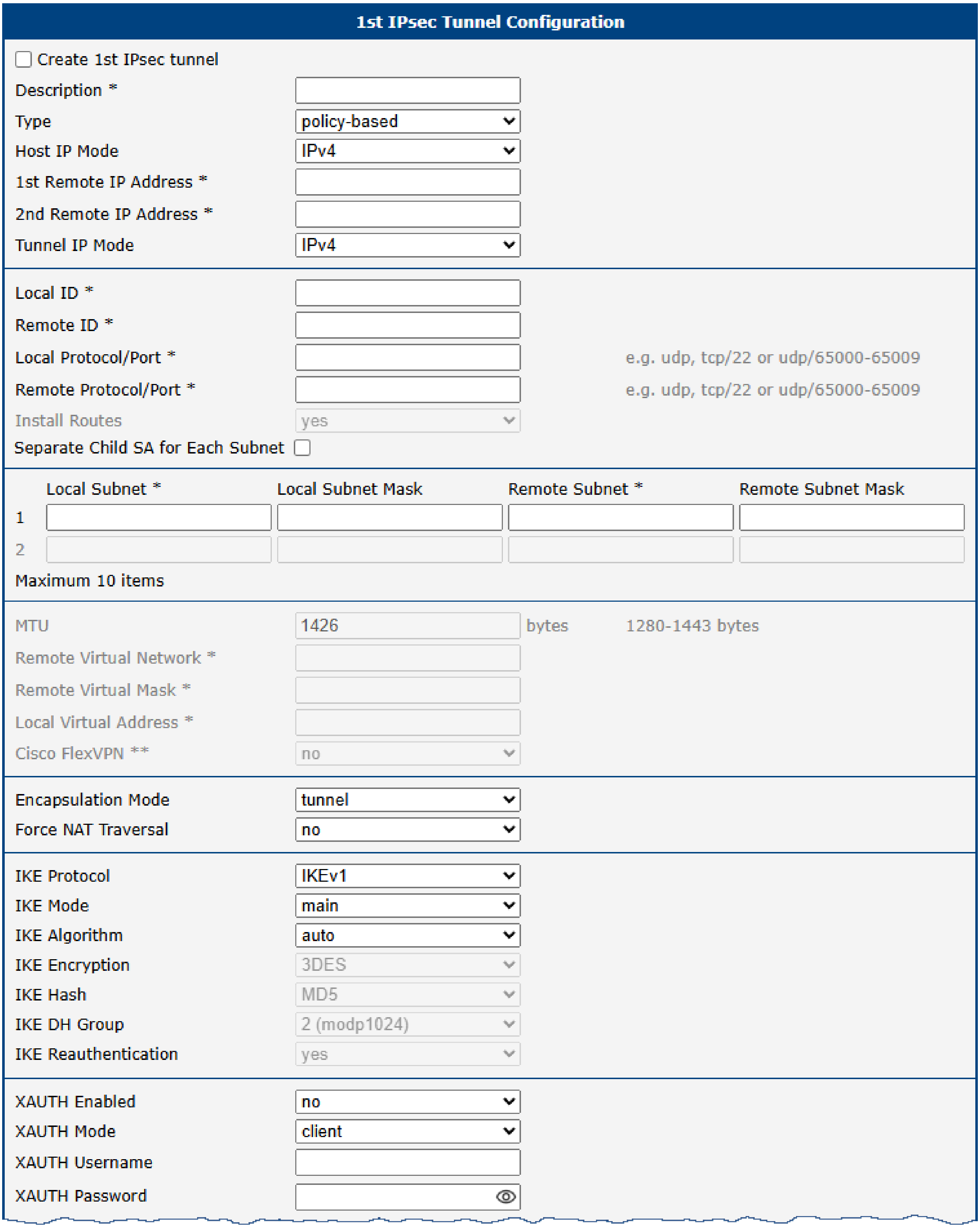
1. **Pre-shared Key**
   - Set *Authenticate Mode* to *pre-shared key*.
   - Enter the shared key into the *Pre-shared Key* field.
2. **Public Key**
   - Set *Authenticate Mode* to *X.509 certificate*.
   - Enter the public key into the *Local Certificate / PubKey* field.
   - A CA certificate is not required.
3. **Peer Certificate**
   - Set *Authenticate Mode* to *X.509 certificate*.
   - Enter the remote key into the *Remote Certificate / PubKey* field. Users with this certificate will be allowed.
   - A CA certificate is not required.
4. **CA Certificate**
   - Set *Authenticate Mode* to *X.509 certificate*.
   - Enter the CA certificate(s) into the *CA Certificate* field. Any certificate signed by the specified CA will be accepted.
   - The remote certificate itself is not required.

Notes:

- The Peer and CA Certificate modes can be used simultaneously; authentication can be performed by either method.
- The *Local ID* is significant. When using certificate authentication, the IKE identity must be contained in the certificate, either as its subject or as a `subjectAltName` .

Configuration Items

The IPsec configuration GUI is shown in Figure 59, and all items are described in the tables below.



1st IPsec Tunnel Configuration

□ Create 1st IPsec tunnel

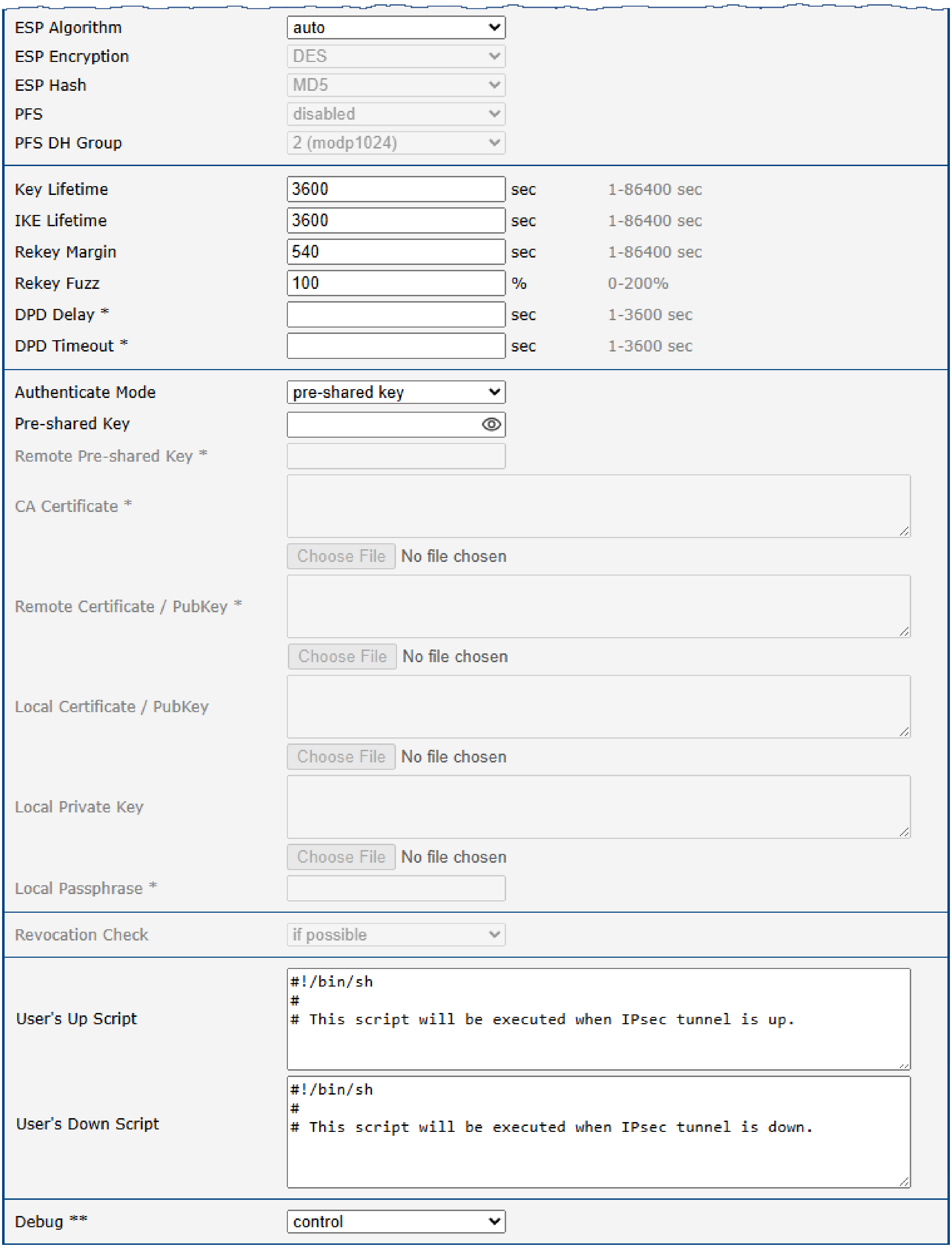
Description *		
Type	policy-based	
Host IP Mode	IPv4	
1st Remote IP Address *		
2nd Remote IP Address *		
Tunnel IP Mode	IPv4	
Local ID *		
Remote ID *		
Local Protocol/Port *		e.g. udp, tcp/22 or udp/65000-65009
Remote Protocol/Port *		e.g. udp, tcp/22 or udp/65000-65009
Install Routes	yes	
Separate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

Figure 59: IPsec tunnels configuration page – part 1



ESP Algorithm	auto		
ESP Encryption	DES		
ESP Hash	MD5		
PFS	disabled		
PFS DH Group	2 (modp1024)		
Key Lifetime	3600	sec	1-86400 sec
IKE Lifetime	3600	sec	1-86400 sec
Rekey Margin	540	sec	1-86400 sec
Rekey Fuzz	100	%	0-200%
DPD Delay *		sec	1-3600 sec
DPD Timeout *		sec	1-3600 sec
Authenticate Mode	pre-shared key		
Pre-shared Key			
Remote Pre-shared Key *			
CA Certificate *	Choose File No file chosen		
Remote Certificate / PubKey *	Choose File No file chosen		
Local Certificate / PubKey	Choose File No file chosen		
Local Private Key	Choose File No file chosen		
Local Passphrase *			
Revocation Check	if possible		
User's Up Script	see below		
User's Down Script	see below		
Debug **	control		

User's Up Script

```
#!/bin/sh
#
# This script will be executed when IPsec tunnel is up.
```

User's Down Script

```
#!/bin/sh
#
# This script will be executed when IPsec tunnel is down.
```

Figure 60: IPsec tunnels configuration page – part 2

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*.
2nd Remote IP Address	The secondary (failover) IPv4, IPv6 address, or domain name of the remote peer.
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).
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).
Force NAT Traversal	Enforces NAT traversal by enabling UDP encapsulation of ESP packets.
IKE Protocol	Specifies the version of the Internet Key Exchange protocol: **IKEv1/IKEv2** (auto-negotiate), **IKEv1**, or **IKEv2**.

Table 51: IPsec tunnel configuration items description

Item	Description
IKE Mode	Specifies the mode for establishing a connection: *main* or *aggressive*. **It is strongly recommended not to use *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, please refer to the official *Algorithm Proposals (Cipher Suites)*.
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	The lifetime for the data part of the tunnel key (60–86400 seconds).
IKE Lifetime	The lifetime for the service part of the tunnel key (60–86400 seconds).
Rekey Margin	How long before a connection expires that the router attempts to negotiate a replacement. This value should be less than half of the *IKE Lifetime* and *Key Lifetime*.
Rekey Fuzz	A percentage of time to extend the *Rekey Margin*.
DPD Delay	The delay after which the Dead Peer Detection functionality tests the tunnel status.
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.
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.

Table 51: (continued)

Item	Description
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 (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, logs normal messages and errors. • **control-more** – More verbose control messages. • **raw** – Logs raw protocol messages. • **private** – Most verbose level, including private keys. See the *Logger Configuration* page on the *strongSwan* website for details.

Table 51: (continued)

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.

Important Considerations

Warning

- If local and remote subnets are not configured, only router-to-router traffic is encrypted.
- If protocol/port fields are configured, only traffic matching those settings is encapsulated.

[1] Parameters passed to the script: for policy-based, the connection name (e.g., `ipsec1-1`); for route-based, the connection name and interface name (e.g., `ipsec1-1` and `ipsec0`).

IPsec Tunnel Configuration Example

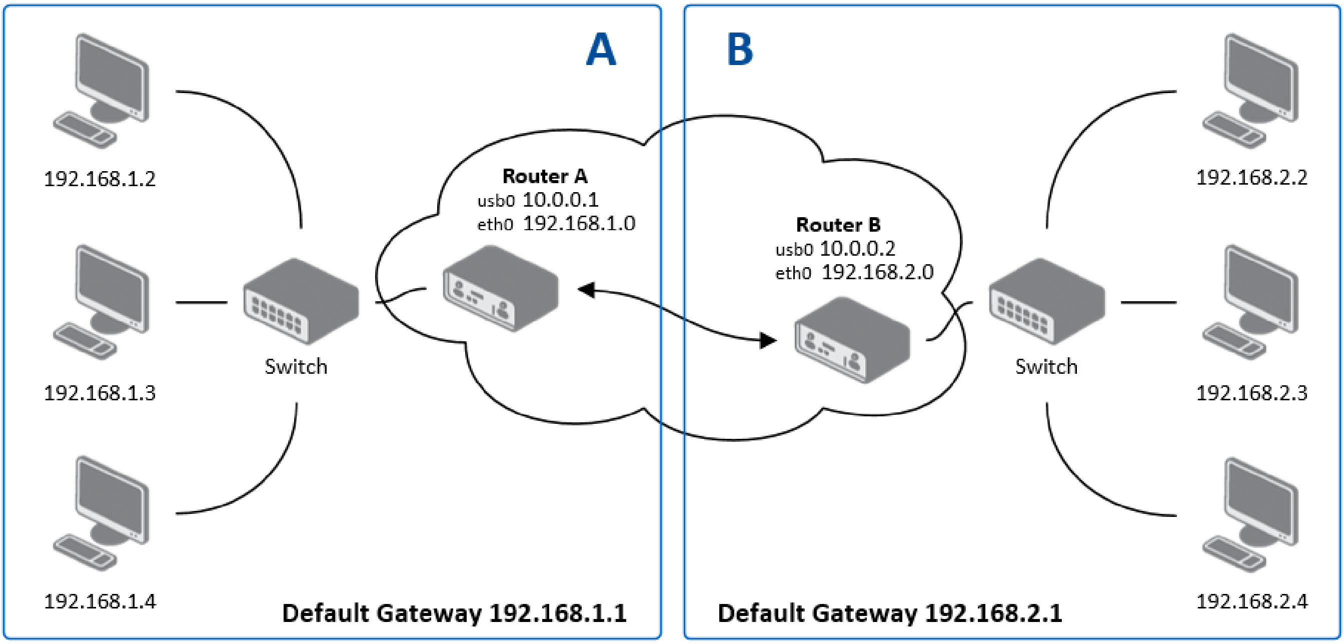


Figure 61: IPsec configuration topology example

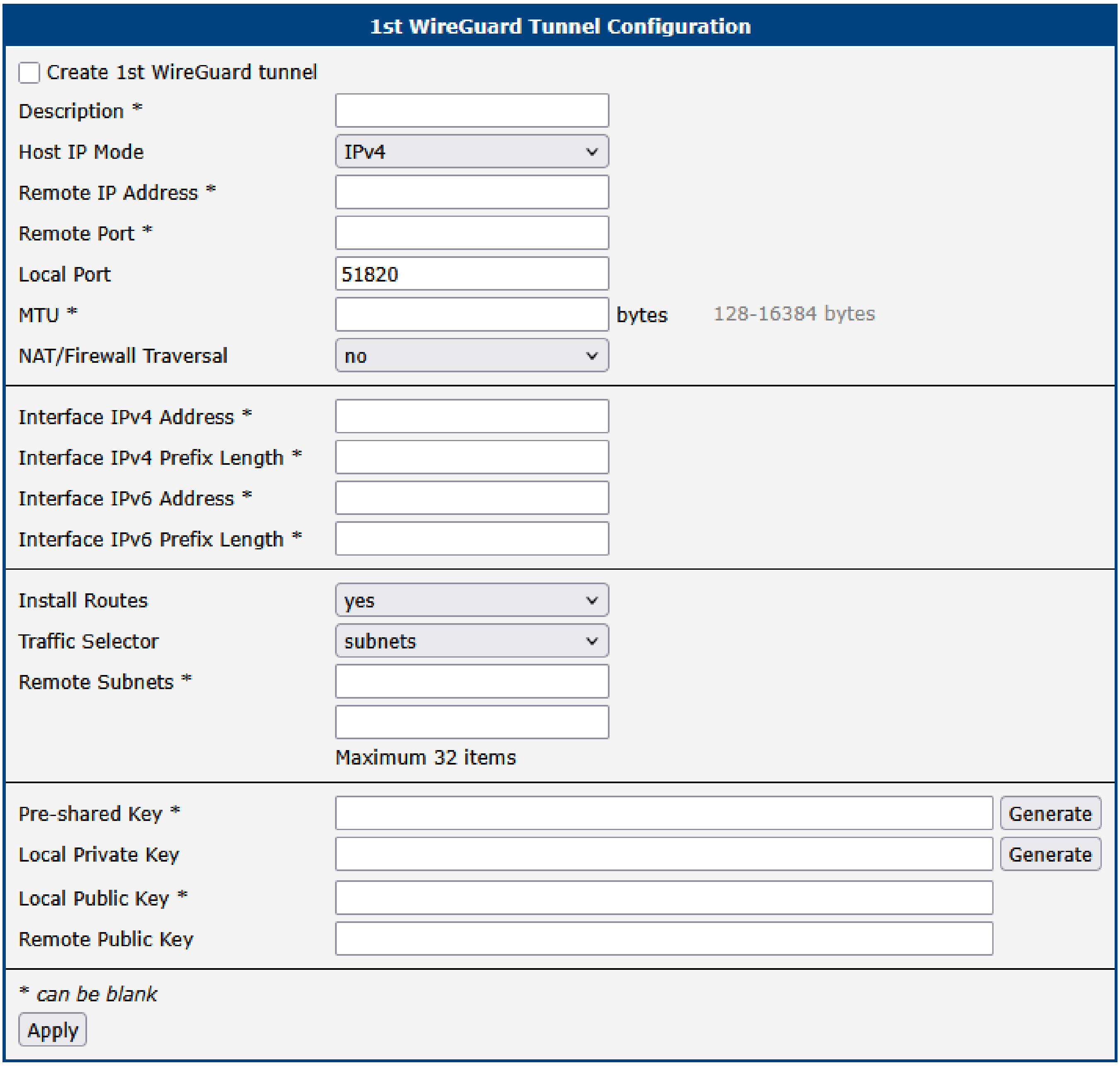
Example configurations for Router A and Router B:

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
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mask	255.255.255.0	255.255.255.0
Authenticate Mode	pre-shared key	pre-shared key
Pre-shared Key	test	test

Table 52: Simple IPv4 IPsec tunnel configuration

3.13 WireGuard

WireGuard is a modern, high-performance VPN protocol known for its simplicity, strong encryption, and small attack surface. It creates secure, encrypted tunnels by encapsulating network traffic within UDP packets. Advantech routers support up to four simultaneous WireGuard tunnels, each with dual-stack (IPv4/IPv6) capabilities.
The configuration pages are located under *Configuration* → *WireGuard*, with separate tabs for each of the four possible tunnels.



1st WireGuard Tunnel Configuration

□ Create 1st WireGuard tunnel	
Description *	
Host IP Mode	IPv4
Remote IP Address *	
Remote Port *	
Local Port	51820
MTU *	bytes 128-16384 bytes
NAT/Firewall Traversal	no
Interface IPv4 Address *	
Interface IPv4 Prefix Length *	
Interface IPv6 Address *	
Interface IPv6 Prefix Length *	
Install Routes	yes
Traffic Selector	subnets
Remote Subnets *	Maximum 32 items
Pre-shared Key *	Generate
Local Private Key	Generate
Local Public Key *	
Remote Public Key	

* *can be blank*

Apply

Figure 62: WireGuard tunnel configuration page

Info

- For dynamic routing over WireGuard, the *FRR* Router App can be installed. This enables the use of standard routing protocols like BGP or OSPF across the tunnel.
- For detailed setup instructions and examples, refer to the *WireGuard Tunnel* Application Note, available on the Advantech documentation portal.

Tunnel Configuration

The following tables describe the parameters for configuring a WireGuard tunnel.

Item	Description
Create WireGuard tunnel	Enables and activates the respective tunnel.
Description	A user-defined name for the tunnel interface.
Host IP Mode	Sets the IP version for communication with the remote peer (*IPv4* or *IPv6*).
Remote IP Address	The public IPv4/IPv6 address or domain name of the remote peer.
Remote/Local Port	The UDP ports used for sending and receiving tunnel traffic. The default is 51820.
MTU	The Maximum Transmission Unit for the tunnel interface. The default of 1400 bytes is recommended.
NAT/Firewall Traversal	When set to *yes*, sends periodic keepalive packets to maintain a connection through a NAT device or firewall.
Interface IPv4/IPv6 Address	The virtual IPv4 or IPv6 address for the router's end of the tunnel.
Interface IPv4/IPv6 Prefix Length	The subnet prefix length for the tunnel interface address.
Install Routes	Available options: • **yes**: Automatically installs routes based on the *Traffic Selector* and *Remote Subnets*. • **no**: Disables automatic route installation, typically used when a dynamic routing protocol like BGP is managing routes.
Traffic Selector	Defines which traffic is sent through the tunnel: • **all traffic**: Routes all outbound traffic through the tunnel (creates a 0.0.0.0/0 or ::/0 route). • **subnets**: Routes only traffic destined for the networks specified in the *Remote Subnets* field.
Remote Subnets	A list of remote IPv4 or IPv6 subnets in CIDR notation (e.g., `192.168.1.0/24`) to be routed through the tunnel. Up to 32 subnets can be defined.

Table 53: WireGuard tunnel configuration options

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. This key is shared with the remote peer so it can authenticate and encrypt traffic sent to this router.
Remote Public Key	The public key of the remote peer. This is used to authenticate the remote peer and encrypt traffic sent to it.
Pre-shared Key	An optional key for 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.

Table 54: Cryptographic key configuration

Configuration Example

This example details a site-to-site WireGuard tunnel between Router A and Router B. Router B acts as the "server" by listening for connections, while Router A initiates the connection.

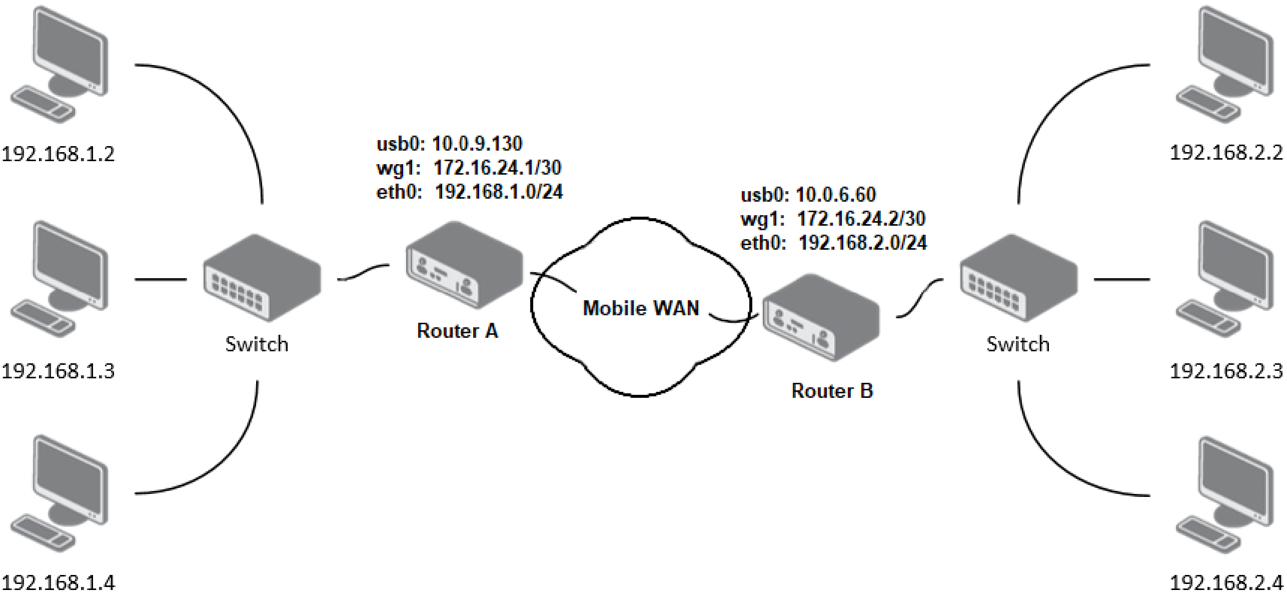


Figure 63: An example of WireGuard topology

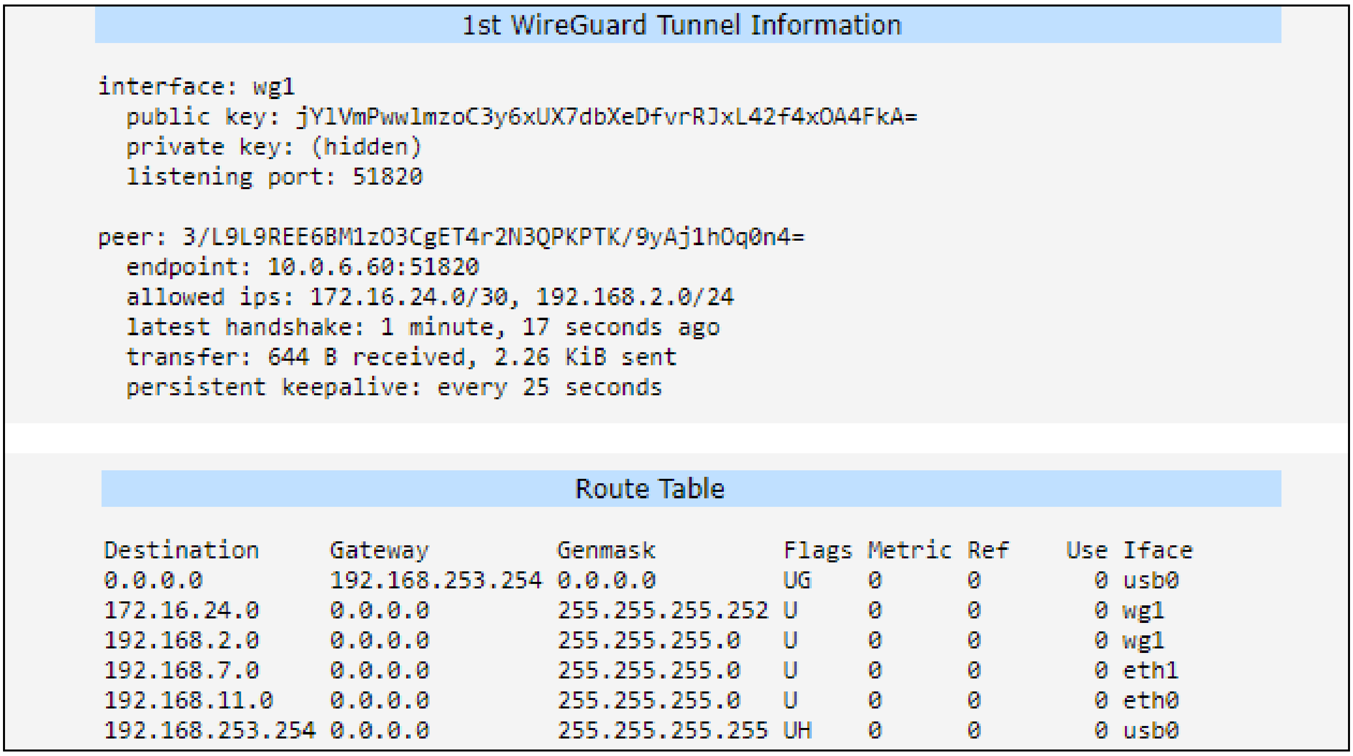
The following table outlines the necessary configuration for each router based on the topology above.

Parameter	Router A Value	Router B Value
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*
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>*

Table 55: WireGuard IPv4 tunnel configuration example

Verifying Connectivity

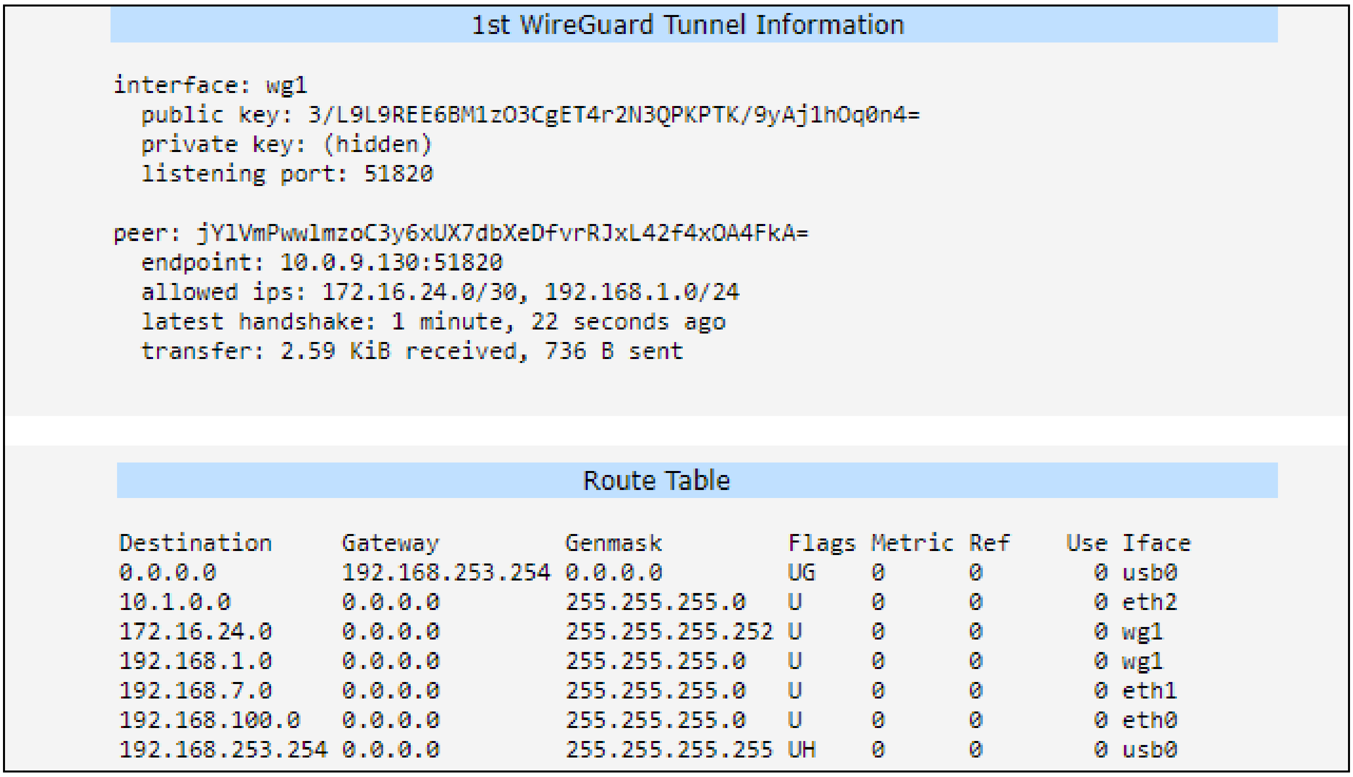
After applying the configuration, the tunnel status can be verified on the *Status* → *WireGuard* page. A successful connection is indicated by the presence of a *Latest handshake* time, which shows how long ago the last cryptographic key exchange occurred. This value will only appear after traffic has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



```
1st WireGuard Tunnel Information

interface: wg1
  public key: jY1VmPww1mzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  private key: (hidden)
  listening port: 51820

peer: 3/L9L9REE6BM1zO3CgET4r2N3QPKPTK/9yAj1hOq0n4=
  endpoint: 10.0.6.60:51820
  allowed ips: 172.16.24.0/30, 192.168.2.0/24
  latest handshake: 1 minute, 17 seconds ago
  transfer: 644 B received, 2.26 KiB sent
  persistent keepalive: every 25 seconds
```

```
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
172.16.24.0     0.0.0.0         255.255.255.252 U     0      0        0 wg1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 wg1
192.168.7.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.253.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

Figure 64: Router A: WireGuard status and route table



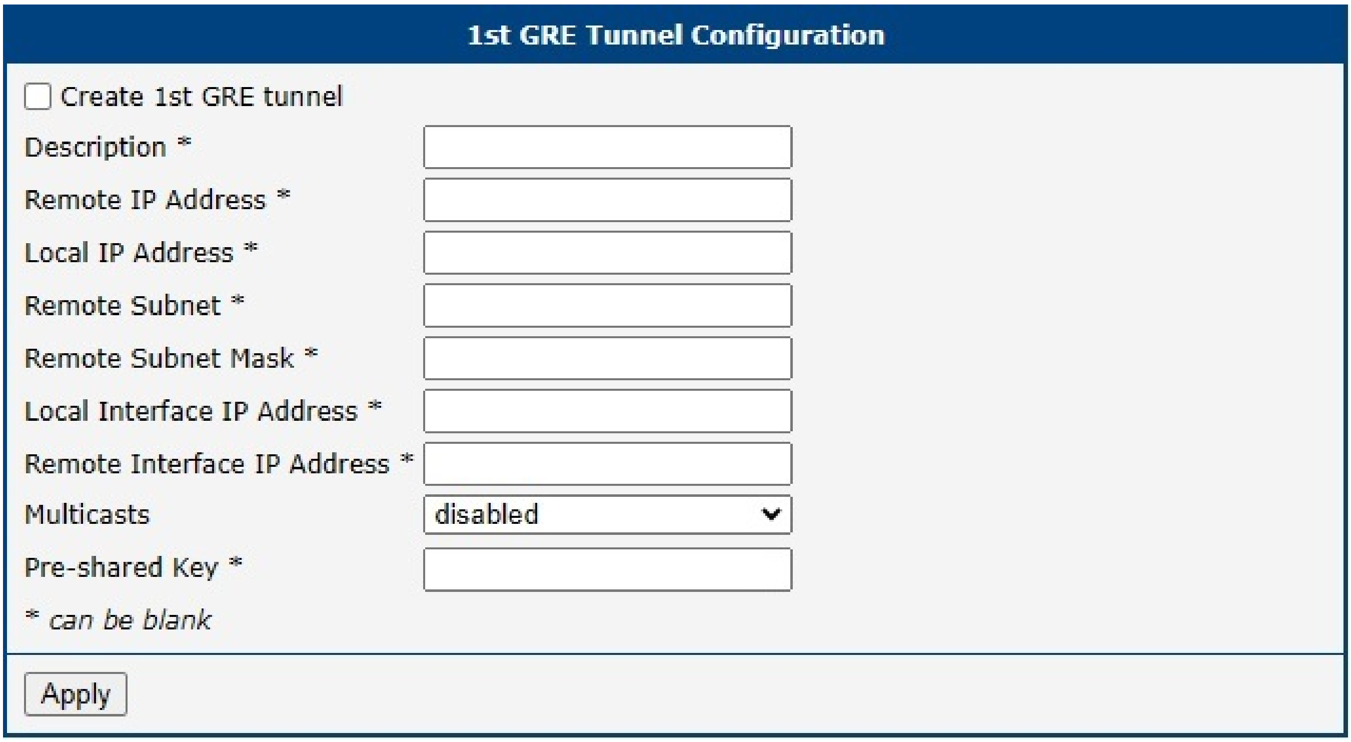
```
1st WireGuard Tunnel Information

interface: wg1
  public key: 3/L9L9REE6BM1zO3CgET4r2N3QPKPTK/9yAj1hOq0n4=
  private key: (hidden)
  listening port: 51820

peer: jY1VmPww1mzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  endpoint: 10.0.9.130:51820
  allowed ips: 172.16.24.0/30, 192.168.1.0/24
  latest handshake: 1 minute, 22 seconds ago
  transfer: 2.59 KiB received, 736 B sent
```

```
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
10.1.0.0        0.0.0.0         255.255.255.0   U     0      0        0 eth2
172.16.24.0     0.0.0.0         255.255.255.252 U     0      0        0 wg1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 wg1
192.168.7.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.253.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

Figure 65: Router B: WireGuard status and route table

3.14 GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an IP network. It is a simple and effective way to create unencrypted tunnels between two separate LANs. The router supports the creation of up to four GRE tunnels.
The configuration pages are located under *Configuration* → *GRE*, with separate tabs for each of the four tunnels.



1st GRE Tunnel Configuration

☐ Create 1st GRE tunnel

Description *	
Remote IP Address *	
Local IP Address *	
Remote Subnet *	
Remote Subnet Mask *	
Local Interface IP Address *	
Remote Interface IP Address *	
Multicasts	disabled
Pre-shared Key *	

** can be blank*

Figure 66: GRE tunnel configuration page

Warning

GRE is an unencrypted protocol and does not support IPv6 transport. For secure communication, it is recommended to use it in combination with IPsec.

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.

Table 56: GRE tunnel configuration options

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

Table 56: (continued)

Warning

GRE tunnels cannot pass through a Network Address Translation (NAT) device without a corresponding NAT traversal solution, such as a port forwarding rule for protocol 47 (GRE).

Configuration Example

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

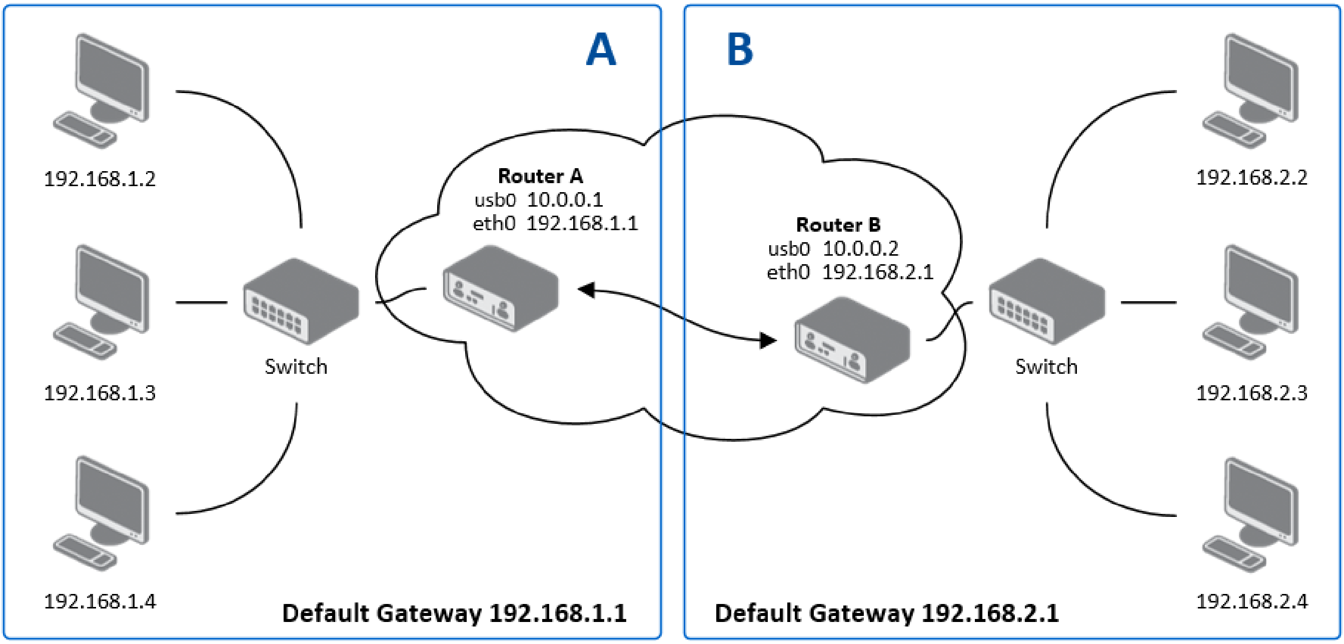


Figure 67: An example of GRE topology

The following table outlines the key parameters for this configuration.

Parameter	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

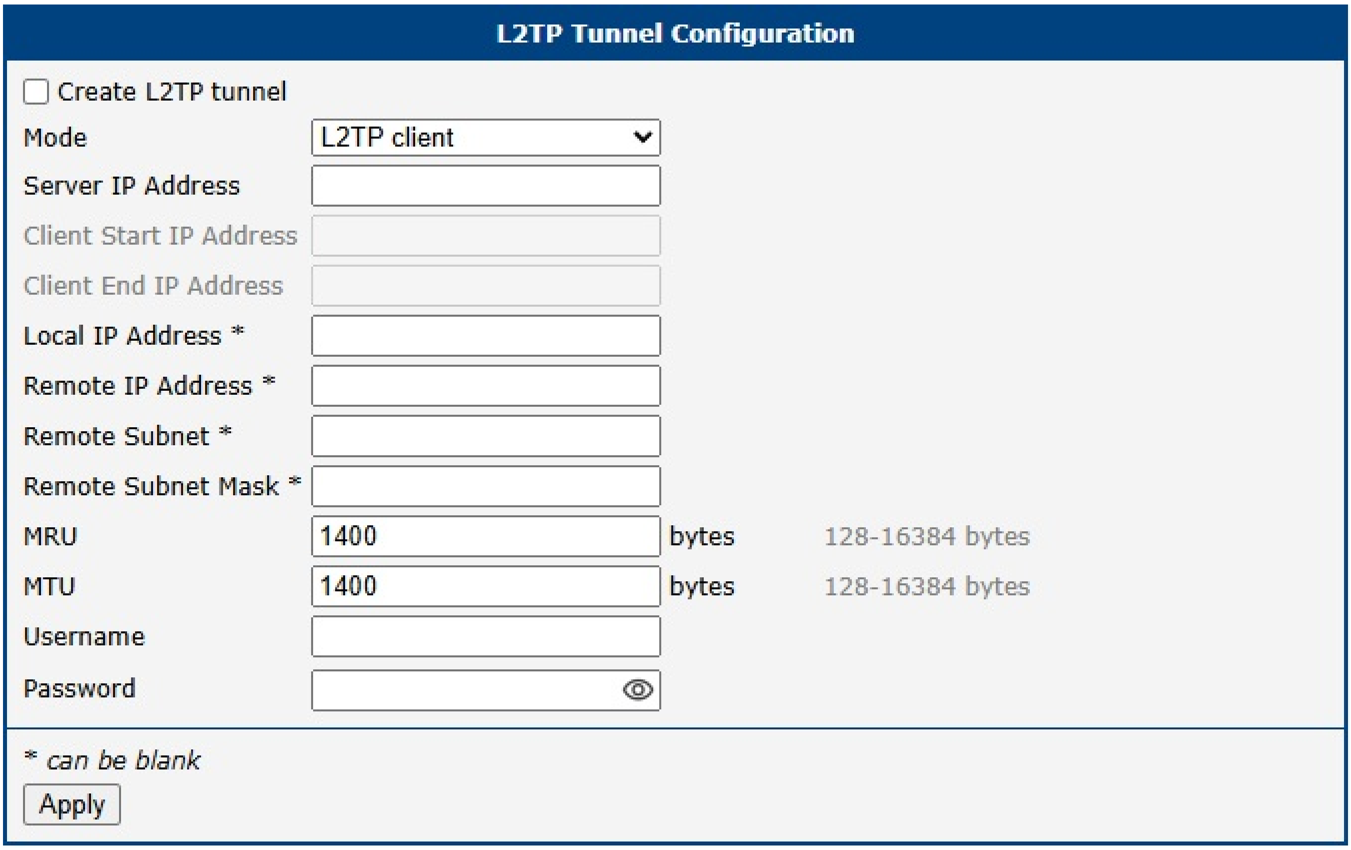
Table 57: GRE tunnel configuration example

Info

For more detailed examples, please refer to the *GRE Tunnel* Application Note [8].

3.15 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

□ Create L2TP tunnel

Mode	L2TP client		
Server IP Address			
Client Start IP Address			
Client End IP Address			
Local IP Address *			
Remote IP Address *			
Remote Subnet *			
Remote Subnet Mask *			
MRU	1400	bytes	128-16384 bytes
MTU	1400	bytes	128-16384 bytes
Username			
Password			

** can be blank*

Figure 68: 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) Defines the starting and ending addresses of the IP pool from which the server will assign addresses to connecting clients.

Table 58: L2TP tunnel configuration options

Item	Description
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.

Table 58: (continued)

Configuration Example

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

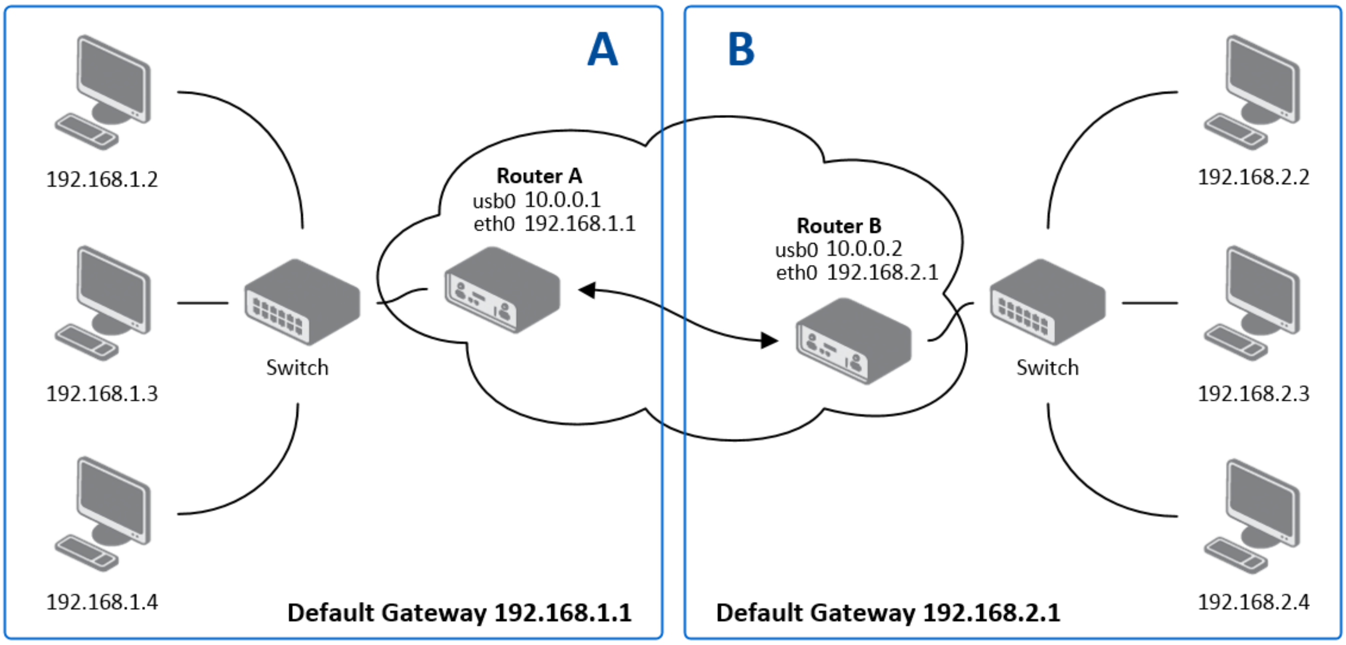


Figure 69: An example of L2TP topology

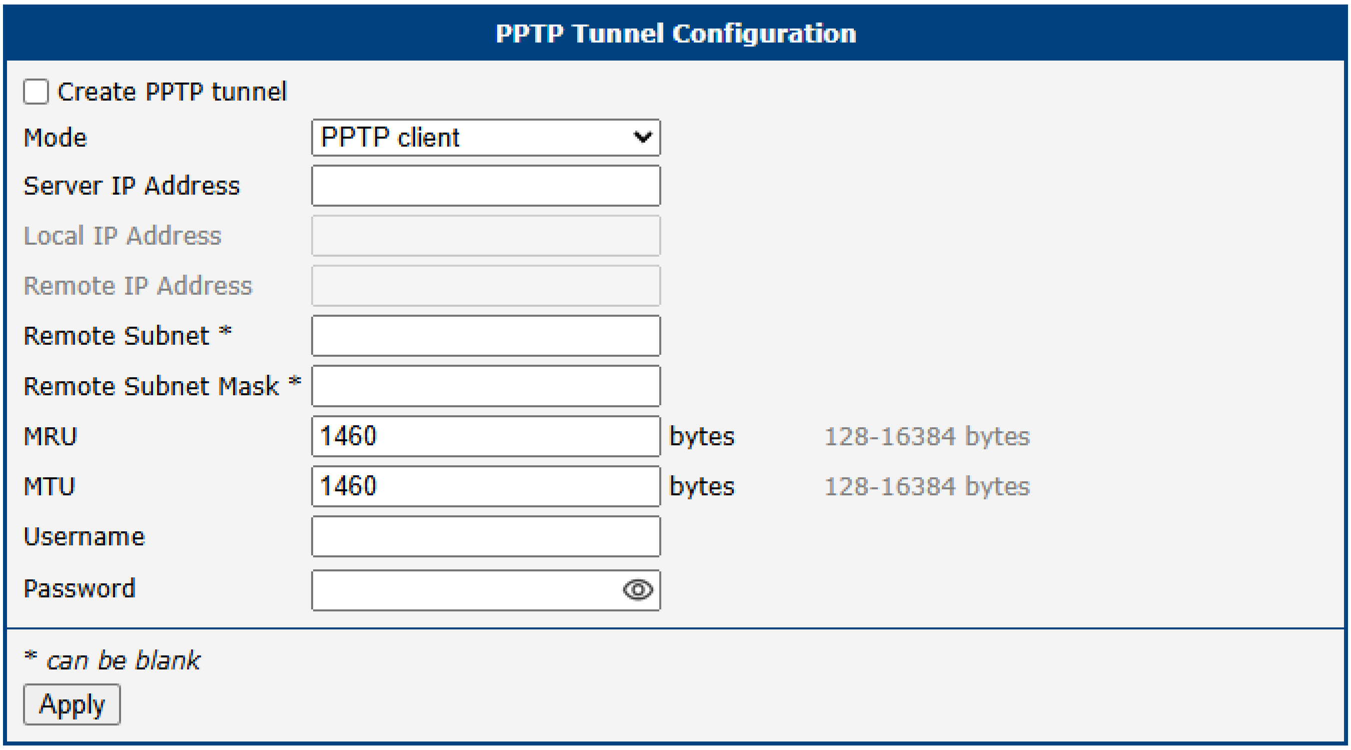
The configuration for each router is detailed below.

Parameter	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

Table 59: L2TP tunnel configuration example

3.16 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 the *Configuration* → *PPTP* page.



PPTP Tunnel Configuration

☐ Create PPTP tunnel

Mode	PPTP client		
Server IP Address			
Local IP Address			
Remote IP Address			
Remote Subnet *			
Remote Subnet Mask *			
MRU	1460	bytes	128-16384 bytes
MTU	1460	bytes	128-16384 bytes
Username			
Password			

** can be blank*

Apply

Figure 70: 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.

Table 60: PPTP tunnel configuration options

Item	Description
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.

Table 60: (continued)

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).

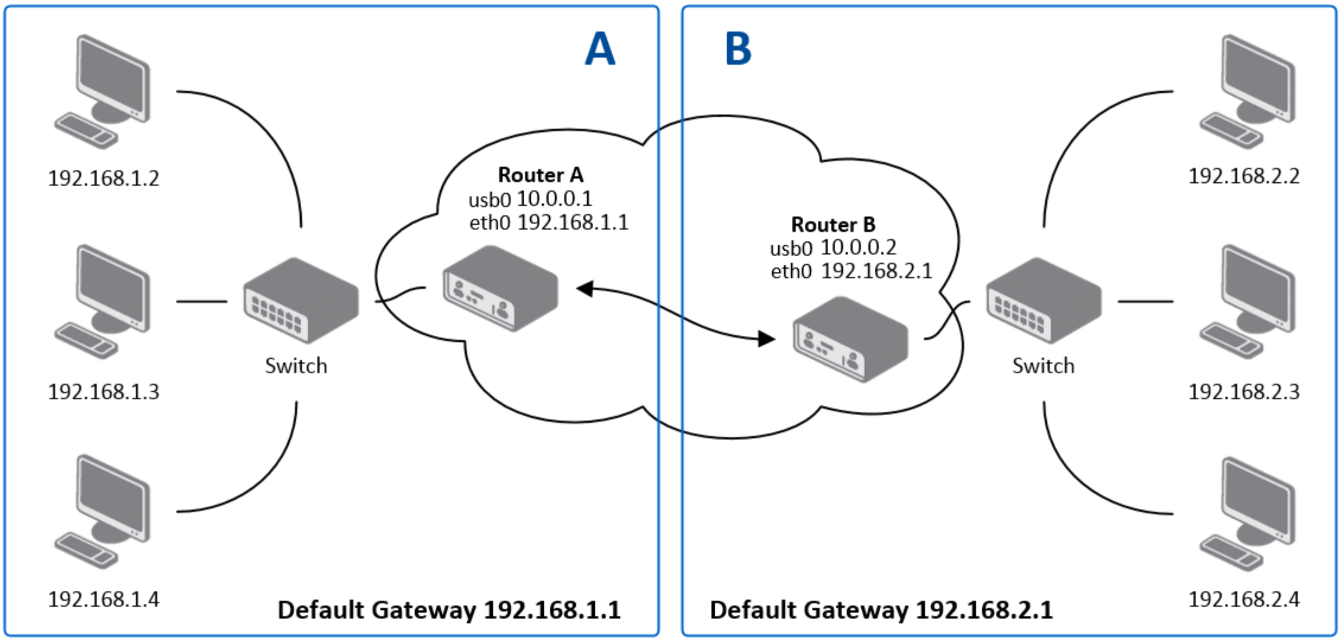


Figure 71: An example of PPTP topology

The configuration for each router is outlined below.

Parameter	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

Table 61: PPTP tunnel configuration example

3.17 Services

3.17.1 DynDNS

The Dynamic DNS (DynDNS) 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 DynDNS server whenever a change is detected.
To configure the service, navigate to *Services* → *DynDNS*.

Warning

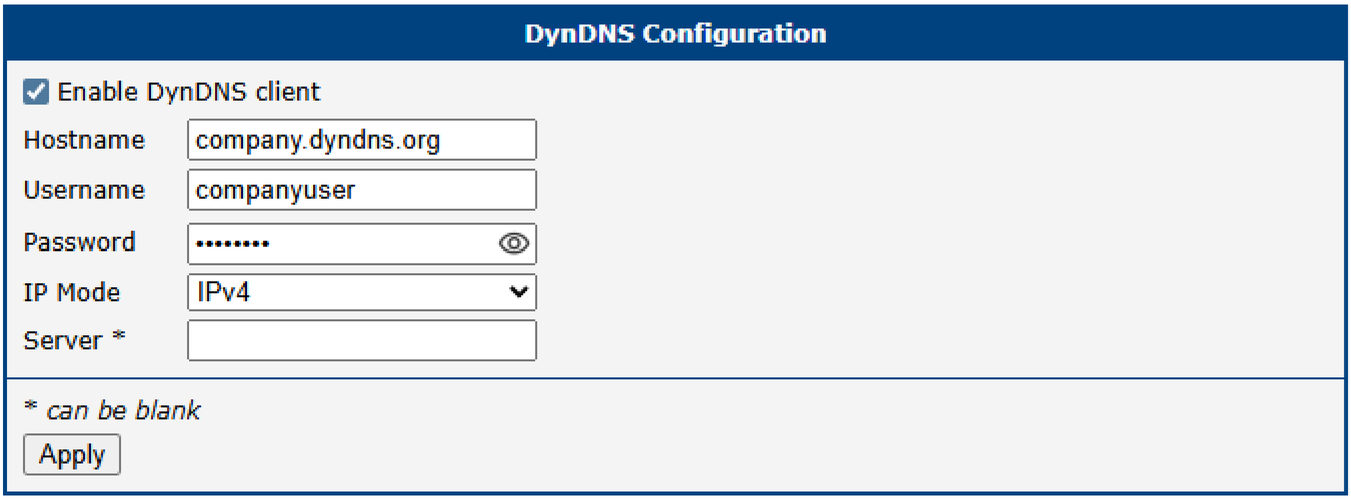
For the DynDNS service to function correctly, the router's SIM card must be assigned a public IP address by the mobile provider.

The table below describes the settings available on the *DynDNS Configuration* page.

Setting	Description
Hostname	Your fully qualified domain name registered with a DynDNS provider (e.g., *my-router.dyndns.org*).
Username	The username for your DynDNS service account.
Password	The password for your DynDNS service account.
IP Mode	Select the IP protocol version for the DynDNS updates: • **IPv4** – Use only the IPv4 address (default). • **IPv6** – Use only the IPv6 address. • **IPv4/IPv6** – Use both IPv4 and IPv6 addresses (dual-stack).
Server	The update server address of your DynDNS provider. If left blank, the default value *members.dyndns.org* is used. Several free services are available, including: *freedns.afraid.org*, *www.duckdns.org*, and *www.noip.com*.

Table 62: DynDNS configuration settings

The figure below shows an example configuration for the hostname *company.dyndns.org*.



DynDNS Configuration

☑ Enable DynDNS client

Hostname	company.dyndns.org
Username	companyuser
Password	••••••••
IP Mode	IPv4
Server *	

* can be blank

Figure 72: DynDNS configuration example

Info

To access the router's web interface from the internet, you must also enable Remote Access. For details, see Chapter *3.10 NAT*.

3.17.2 FTP

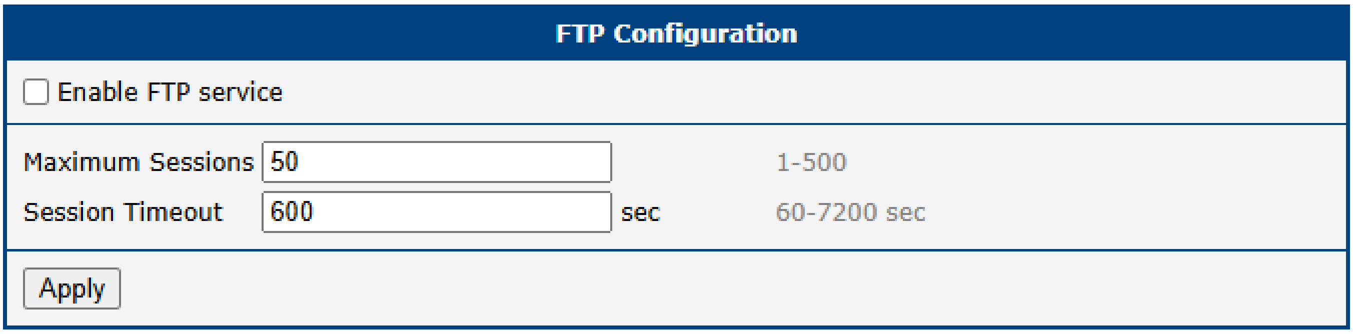
Warning

FTP is an unencrypted protocol.

FTP protocol (File Transfer Protocol) can be used to transfer files between the router and another device on the computer network. Configuration form of TP server can be done in *FTP* configuration page under *Services* menu item.

Item	Description
Enable FTP service	Enabling of FTP server.
Maximum Sessions	Indicates how many concurrent connections shall the FTP server 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.

Table 63: FTP configuration items description



FTP Configuration

□ Enable FTP service

Maximum Sessions	50		1-500
Session Timeout	600	sec	60-7200 sec

Figure 73: Configuration of FTP server

3.17.3 GNSS

> **Info**
>
> - Available only for models equipped with a GNSS module.
> - Starting from firmware version 6.6.0, this functionality replaces the functionality of the *GPS* RouterApp. It is strongly recommended to use the built-in feature instead of the legacy RouterApp. Furthermore, it is not possible to use this functionality together with RouterApp 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 Chapter *4 Geolocation* and Chapter *5 GNSS*).
- The router can use GNSS as a source for time synchronization (see Chapter *3.17.5 NTP*).
- If configured, the router's location can be reported via SNMP for network management and monitoring (see Chapter *3.17.8 SNMP*).

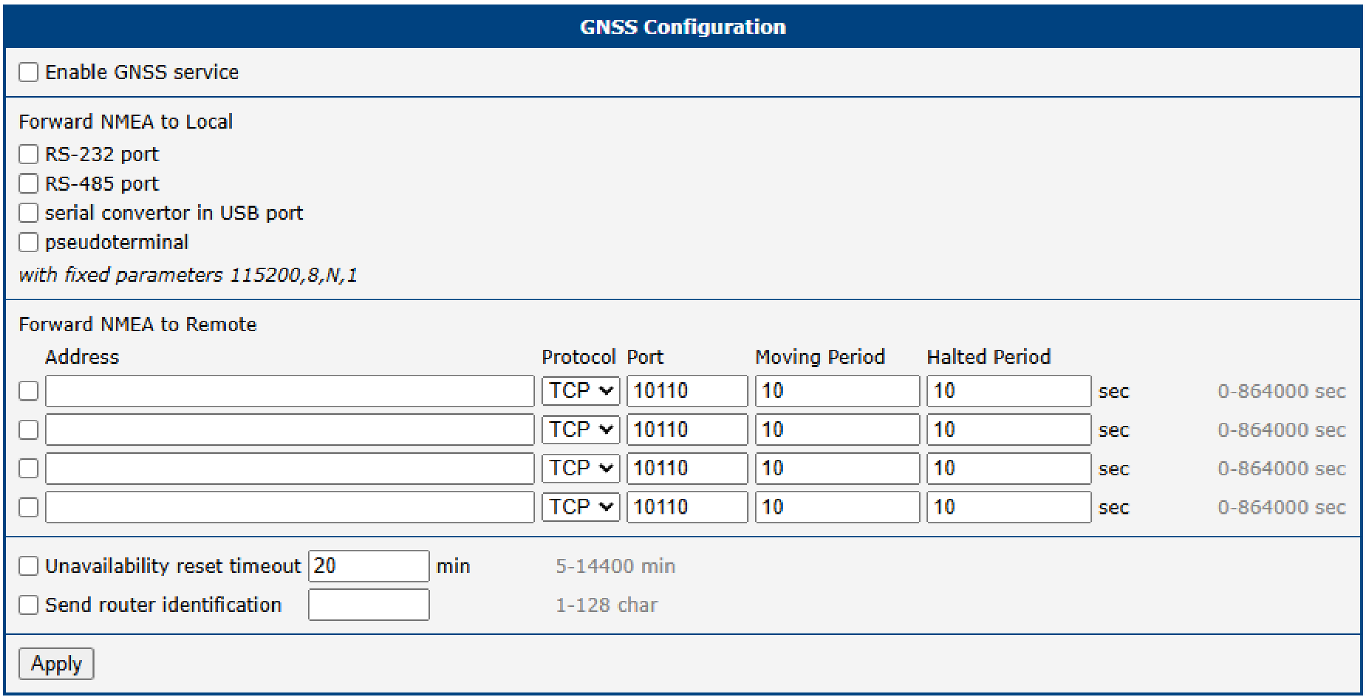
This service is essential for applications requiring precise time and location information, such as vehicle tracking, asset management, or synchronizing distributed network devices. The configuration also allows forwarding of raw NMEA data to both local serial ports and remote servers over the network.

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. Multiple output options are available: • RS-232 port • RS-485 port • serial convertor 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 four remote destinations, each defined by the following parameters: • **Address** – Destination IP address or hostname for NMEA forwarding • **Protocol** – Select TCP or UDP transport • **Port**: Specify 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).
Unavailability reset timeout	If enabled, defines the maximum time in minutes without GNSS data before the service is automatically reset. Set between 5 and 14 400 minutes.
Send router identification	If enabled, a custom identification text (1–128 characters) is sent to the remote destination with NMEA messages.

Table 64: GNSS configuration items description

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 four remote servers.



GNSS Configuration

□ Enable GNSS service

Forward NMEA to Local

□ RS-232 port

□ RS-485 port

□ serial convertor in USB port

□ pseudoterminal

with fixed parameters 115200,8,N,1

Forward NMEA to Remote

	Address	Protocol	Port	Moving Period	Halted Period		
□		TCP	10110	10	10	sec	0-864000 sec
□		TCP	10110	10	10	sec	0-864000 sec
□		TCP	10110	10	10	sec	0-864000 sec
□		TCP	10110	10	10	sec	0-864000 sec

□ Unavailability reset timeout 20 min 5-14400 min

□ Send router identification 1-128 char

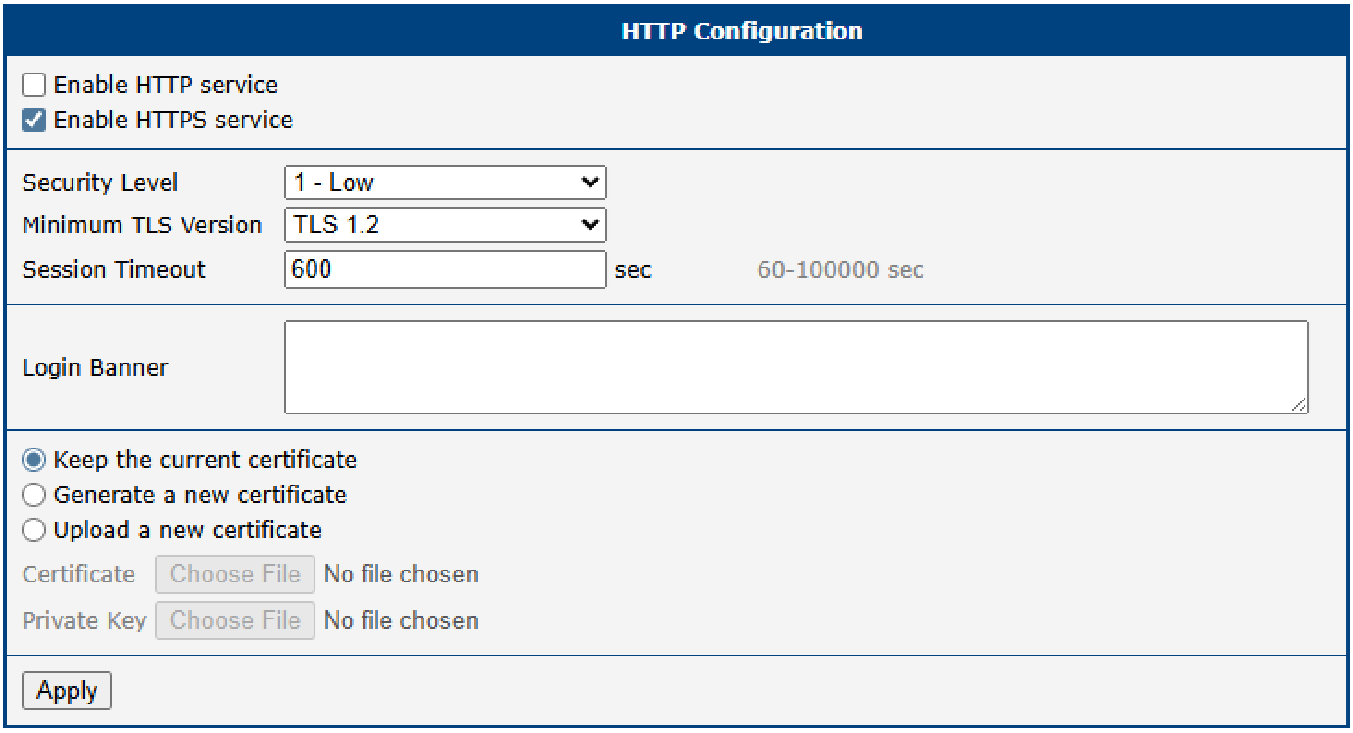
Figure 74: GNSS configuration page

3.17.4 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 allows you to manage both HTTP and the secure HTTPS protocol. For security, it is strongly recommended to use HTTPS, as it encrypts all communication between your browser and the router. By default, the router has HTTPS enabled and HTTP disabled. Any attempt to connect via HTTP will be automatically redirected to the secure HTTPS port.



HTTP Configuration

☐ Enable HTTP service
☑ Enable HTTPS service

Security Level	1 - Low		
Minimum TLS Version	TLS 1.2		
Session Timeout	600	sec	60-100000 sec
Login Banner			

● Keep the current certificate
○ Generate a new certificate
○ Upload a new certificate

Certificate Choose File No file chosen
Private Key Choose File No file chosen

Apply

Figure 75: 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 for the connection 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:** `[Default]` 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 (requires AES-128 or stronger). • **4 - Very High:** Enforces a minimum of 192-bit security (requires AES-192 or stronger).

Table 65: Web server configuration items description

[1] For detailed explanation see the *Security Guidelines* [15], specifically the chapter on *Cryptographic algorithms*.

Item	Description
Minimum TLS Version	Defines the minimum version of the TLS protocol that the router's web server will accept for HTTPS connections. For maximum security, it is recommended to select the highest version compatible with your clients. The available options range from TLS 1.0 to TLS 1.3. Please note that the insecure TLS 1.0 and 1.1 versions are only available for selection if the *Security Level* is set to 0.
Session Timeout	Defines the period of inactivity (in minutes) after which a user is automatically logged out.
Login Banner	Displays custom text on the login page, directly above the username and password fields.
Keep the current certificate	Makes no changes to the certificate currently stored on the router.
Generate a new certificate	Generates a new self-signed certificate for the router, corresponding to the selected *Security Level*. Make sure your certificate matches the *Security Level*.
Upload a new certificate	Allows you to upload a custom certificate, such as one signed by a trusted Certificate Authority (CA).
Certificate	Use the file browser to select the PEM-formatted certificate file to upload. The file can contain a single certificate or a complete certificate chain.
Private Key	Use the file browser to select the private key file corresponding to the certificate being uploaded.

Table 65: (continued)

3.17.5 NTP

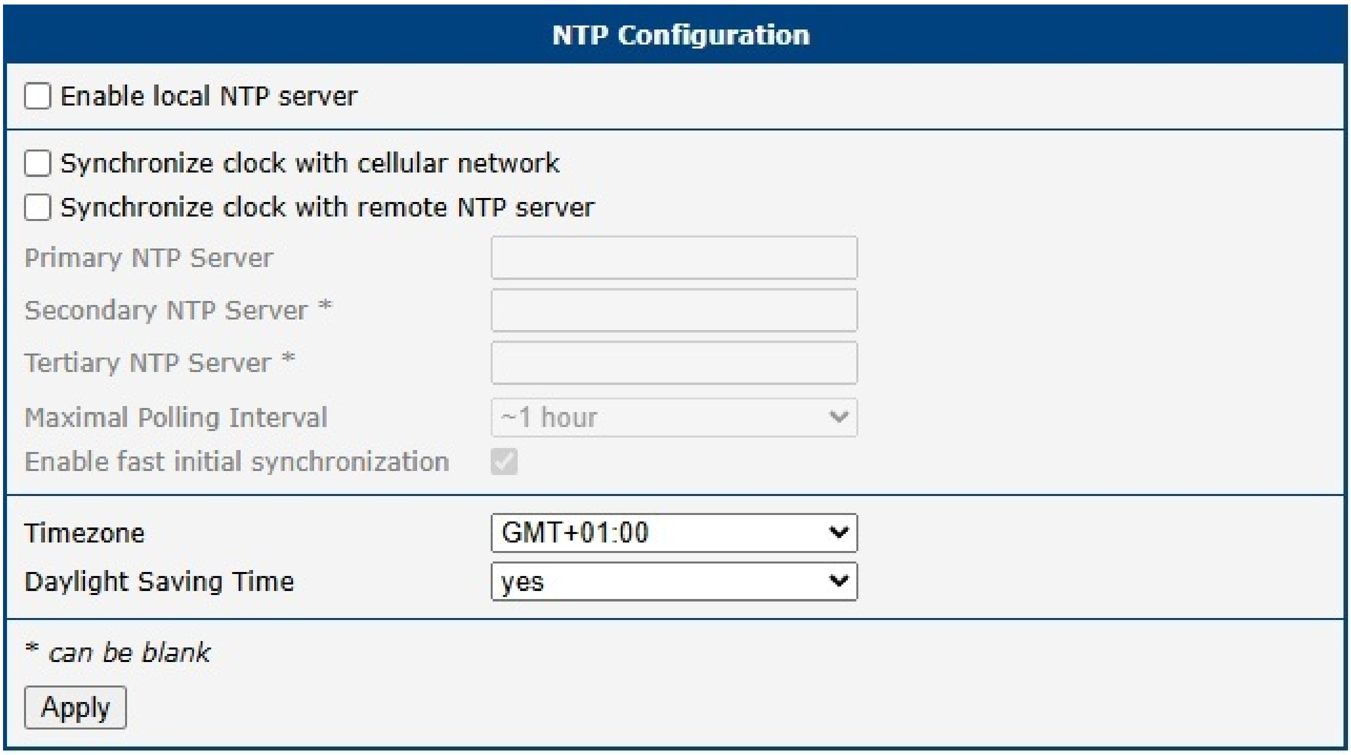
The NTP (Network Time Protocol) configuration page allows you to configure the router's NTP client and/or server functions. To open the *NTP* configuration page, click *NTP* in the *Configuration* section of the main menu.

Info

- Some configuration options described 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

□ Enable local NTP server

□ Synchronize clock with cellular network

□ Synchronize clock with remote NTP server

Primary NTP Server	
Secondary NTP Server *	
Tertiary NTP Server *	
Maximal Polling Interval	~1 hour
Enable fast initial synchronization	☑
Timezone	GMT+01:00
Daylight Saving Time	yes

* can be blank

Figure 76: NTP configuration page

Info

Time-Synchronization Accuracy

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

- **Remote NTP Server:** This is typically the most accurate method. External NTP servers are usually synchronized to atomic clocks and maintained for high-precision timekeeping.
  - Typical accuracy: Within several milliseconds.
- **Cellular Network (NITZ):** Synchronization via the cellular network (a feature known as NITZ) can vary depending on the operator's infrastructure and is generally less precise than dedicated NTP servers.
  - Typical accuracy: Up to several seconds.
- **GNSS:** While satellite-based time is reliable for general clock correction, its precision for NTP is limited by receiver hardware, atmospheric conditions, and internal processing delays. Therefore, it is not recommended for applications requiring high-precision timekeeping.
  - Typical accuracy: Around one second.

For applications requiring precise time synchronization, always prefer remote NTP servers over GNSS.

Item	Description
Enable local NTP server	Enables the built-in NTP server, allowing devices on the local network to synchronize their clocks with the router. The time accuracy depends on how the router itself is synchronized.
Synchronize clock with cellular network	Enables automatic synchronization of the router's system clock with the time provided by the connected cellular network. This functionality depends on support from the mobile operator.
Synchronize clock with GNSS	Enables automatic synchronization of the router's system clock using the precise time signal from a connected GNSS module. This option is only available if a compatible module is installed and receiving a valid satellite signal.
Synchronize clock with remote NTP server	Enables querying of specified remote NTP servers (up to three, in order of preference) for time synchronization.
Primary NTP Server	IP address or domain name of the primary external NTP server. Used if 'Synchronize clock with remote NTP server' is enabled.
Secondary NTP Server	IP address or domain name of the secondary NTP server (optional). Used if the primary server is unavailable.
Tertiary NTP Server	IP address or domain name of the tertiary NTP server (optional). Used if both primary and secondary are unavailable.
Maximal Polling Interval	Sets the maximum interval for synchronization polls (usually in seconds/minutes). Longer intervals reduce network load but may reduce time accuracy.
Enable fast initial synchronization	If enabled, the router performs a rapid clock update when a significant difference is detected between the system time and the received time, reducing convergence time.
Timezone	Defines the router's local timezone for time display and daylight saving adjustment.
Daylight Saving Time	Enables or disables automatic daylight saving adjustment for the set timezone.

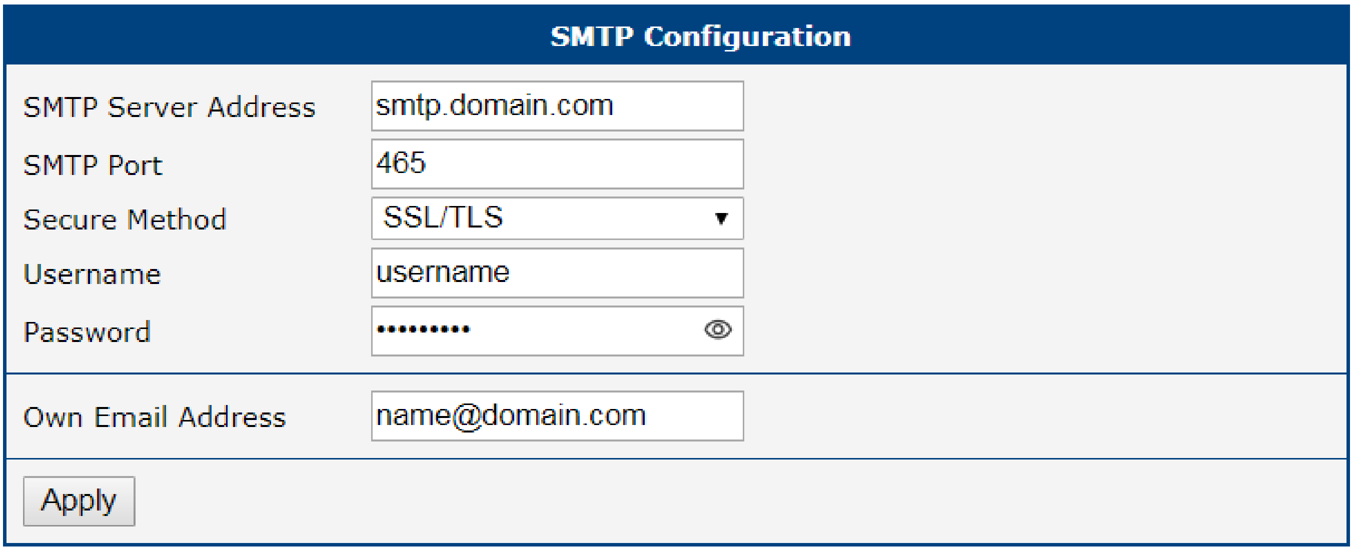
Table 66: NTP configuration items description

3.17.6 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.
- Note that some mobile service providers may block standard SMTP ports, potentially restricting you to using the provider's own SMTP server.



SMTP Configuration

SMTP Server Address: smtp.domain.com
SMTP Port: 465
Secure Method: SSL/TLS
Username: username
Password: •••••••••
Own Email Address: name@domain.com

Figure 77: SMTP client configuration example

Setting	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 include 25, 465 (SSL/TLS), and 587 (STARTTLS).
Secure Method	The encryption method required by the server. The options are *none*, *SSL/TLS*, or *STARTTLS*.
Username	The username for your email account.
Password	The password for your email account.
Own Email Address	The sender's email address that will appear on outgoing emails (e.g., `my-router@mydomain.com`).

Table 67: SMTP client configuration settings

Sending Emails

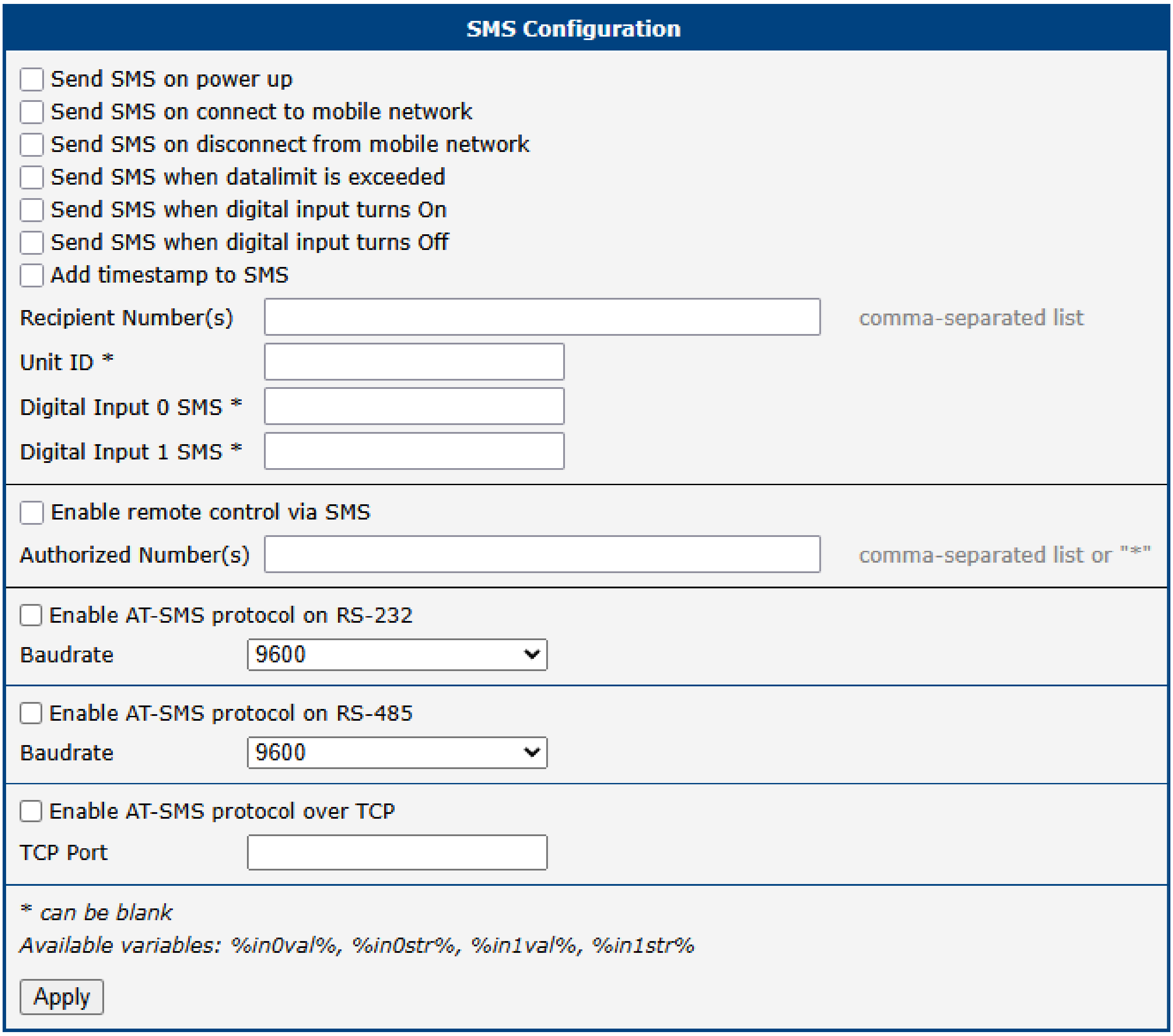
Once the SMTP client is configured, you can trigger emails in two ways:

- **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 Note [1].

3.17.7 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

□ Send SMS on power up
□ Send SMS on connect to mobile network
□ Send SMS on disconnect from mobile network
□ Send SMS when datalimit is exceeded
□ Send SMS when digital input turns On
□ Send SMS when digital input turns Off
□ Add timestamp to SMS

Recipient Number(s)		comma-separated list
Unit ID *		
Digital Input 0 SMS *		
Digital Input 1 SMS *		

□ Enable remote control via SMS

Authorized Number(s)		comma-separated list or "*"

□ Enable AT-SMS protocol on RS-232

Baudrate 9600

□ Enable AT-SMS protocol on RS-485

Baudrate 9600

□ Enable AT-SMS protocol over TCP

TCP Port

** can be blank*
Available variables: %in0val%, %in0str%, %in1val%, %in1str%

Figure 78: 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.

Table 68: SMS notification configuration

Item	Description
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.

Table 68: (continued)

Remote Control via SMS

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

Setting	Description
Enable remote control via SMS	Master switch for SMS processing. If enabled, the router processes incoming SMS messages for remote control commands and custom scripts. **Note:** If 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 execute standard control commands. To accept commands from any number, enter a single asterisk (*).

Table 69: Remote control configuration

[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.

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.

Command	Description
`go online`	Connects the router from the mobile network.
`go online sim [1|2]`	Switches the active mobile connection to the specified SIM card.
`go offline`	Disconnects the router from the mobile network.
set out*x*=[0|1]	Sets the state of a digital output (e.g., `set out0=1`).
`set profile [std|alt1|alt2|alt3]`	Permanently switches to the standard or an alternative configuration profile. For more details, see Chapter *5.3 Change Profile*.
`reboot`	Reboots the router.
`get ip`	Responds with an SMS containing the current IPv4 address of the active mobile connection.
`get ipv6`	Responds with an SMS containing the current IPv6 address of the active mobile connection.

Table 70: SMS control commands

Info

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

Table 71: AT-SMS protocol configuration

Once a connection is established, you can use the AT commands listed in the table below.

Command	Description
`AT+CGMI`	Returns the manufacturer identity.
`AT+CGMM`	Returns the model identity.
`AT+CGMR`	Returns the model revision.
`AT+CGSN`	Returns the product serial number.
`AT+CIMI`	Returns the International Mobile Subscriber Identity (IMSI).
`AT+CMGD`	Deletes an SMS message.
`AT+CMGF`	Sets the SMS message format.
`AT+CMGL`	Lists SMS messages from storage.
`AT+CMGR`	Reads an SMS message.
`AT+CMGS`	Sends an SMS message.
`AT+CMGW`	Writes an SMS message to storage.
`AT+CNUM`	Returns the SIM card's phone number.
`AT+COPS?`	Lists available mobile networks.
`AT+CPIN?`	Retrieves the SIM card status (e.g., PIN required).
`AT+CREG?`	Displays the network registration status.
`AT+CSCA`	Sets the SMS Service Center (SMSC) address.
`AT+CSQ`	Returns the signal strength.
`ATE[0|1]`	Enables or disables command echoing.

Table 72: Supported AT commands

Info

For a complete description of all supported AT commands and their syntax, please refer to the *AT Commands (AT-SMS)* Application Note.

3.17.8 SNMP

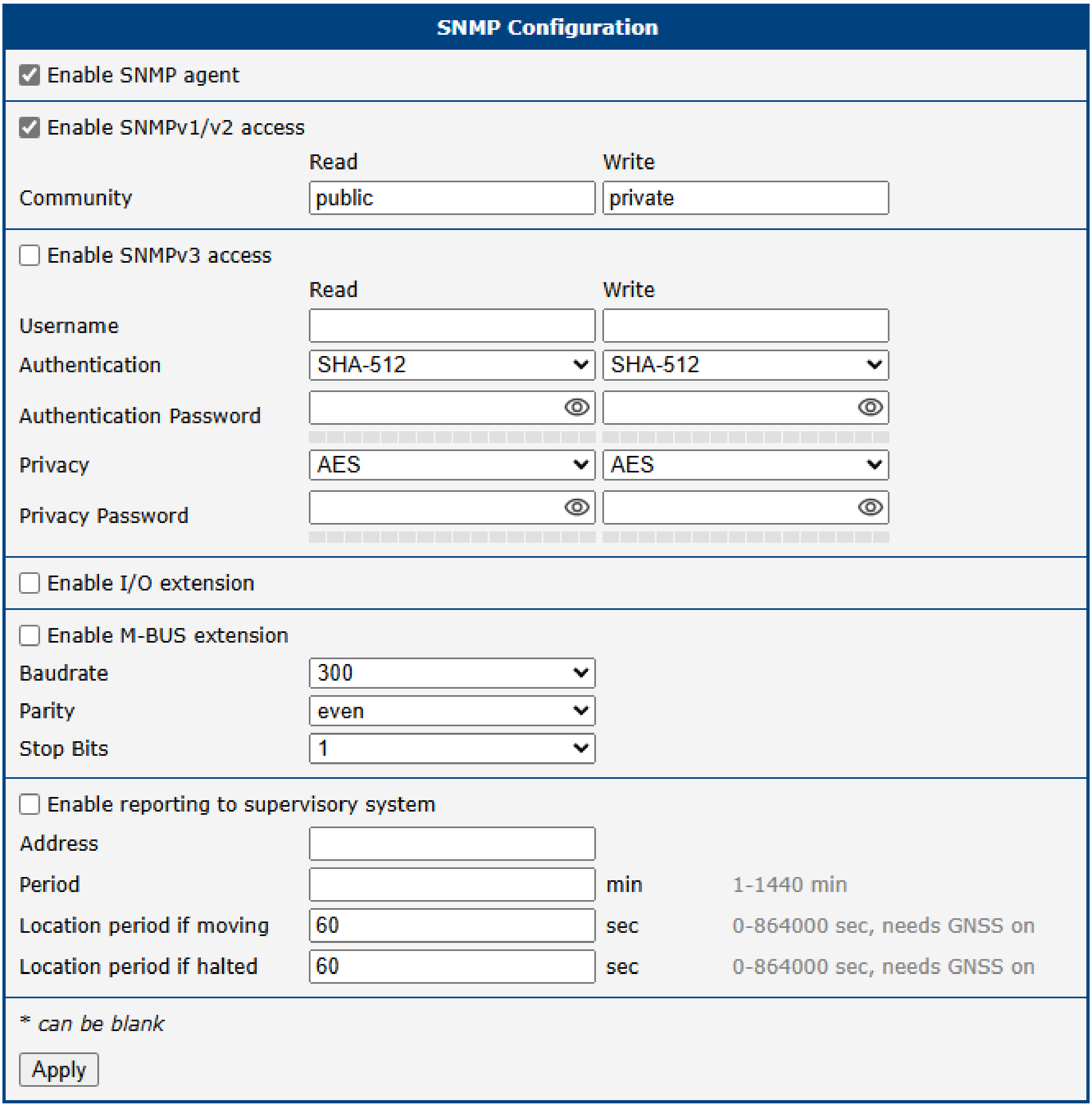
The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent, which transmits information about the router and its expansion ports (if applicable) to a management station. To access the *SNMP* page, click *SNMP* in the *Configuration* → *Services* section of the main menu.
SNMP (Simple Network 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* indetification fields are now configured in the *Configuration* → *System* → *Identification* menu. These fields are no longer present in the SNMP configuration page.

Item	Description
Enable SNMP agent	Turns on the SNMP agent, which allows 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.
Community (Read/Write)	Specify the community strings for SNMPv1/v2 access (for read and write operations, respectively). Default is typically `public` for read and `private` for write.
Enable SNMPv3 access	Activates configuration options for SNMPv3, allowing for stronger authentication and encryption.
Username	Set the username for SNMPv3, independently for read and write access.
Authentication	Select the authentication algorithm (e.g., SHA-512) for SNMPv3 identity verification.
Authentication Password	Password for generating the authentication key.
Privacy	Select the encryption algorithm (e.g., AES) used to secure SNMPv3 communication.
Privacy Password	Password for encrypting SNMPv3 messages.
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 baudrate, parity, and stop bits as required for your metering hardware. External RS232/M-BUS converters may be needed.
Baudrate, Parity, Stop Bits	Configure communication parameters for the M-BUS interface.
Enable reporting to supervisory system	Enables the transmission of statistical and location data to a supervisory or monitoring server.
Address	Destination IP address or hostname for the supervisory system.
Period	Reporting interval in minutes (1–1440).
Location period if moving / halted	Available for GNSS models only. Defines the interval in seconds (0–864000) for location reporting. GNSS service must be enabled. Separate values can be configured for periods when the device is moving and when it is stationary.

Table 73: SNMP configuration items description



SNMP Configuration

☑ Enable SNMP agent

☑ Enable SNMPv1/v2 access

	Read	Write
Community	public	private

☐ Enable SNMPv3 access

	Read	Write
Username		
Authentication	SHA-512	SHA-512
Authentication Password		
Privacy	AES	AES
Privacy Password		

☐ Enable I/O extension

☐ Enable M-BUS extension

Baudrate	300
Parity	even
Stop Bits	1

☐ Enable reporting to supervisory system

Address			
Period		min	1-1440 min
Location period if moving	60	sec	0-864000 sec, needs GNSS on
Location period if halted	60	sec	0-864000 sec, needs GNSS on

* *can be blank*

Apply

Figure 79: SNMP configuration page

Activating the *Enable I/O extension* function allows you to monitor the digital I/O inputs on the router.

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 MBUS interface. While the MBUS expansion port is not currently supported, it is possible to use an external RS232/MBUS converter.

Each monitored value is uniquely identified using a numerical identifier called an *OID* (Object Identifier). This identifier consists of a sequence of numbers separated by dots, forming a hierarchical tree structure. Each OID derives from its parent identifier, appending an additional number to indicate its position in the hierarchy. The figure below illustrates the fundamental tree structure used for creating OIDs.

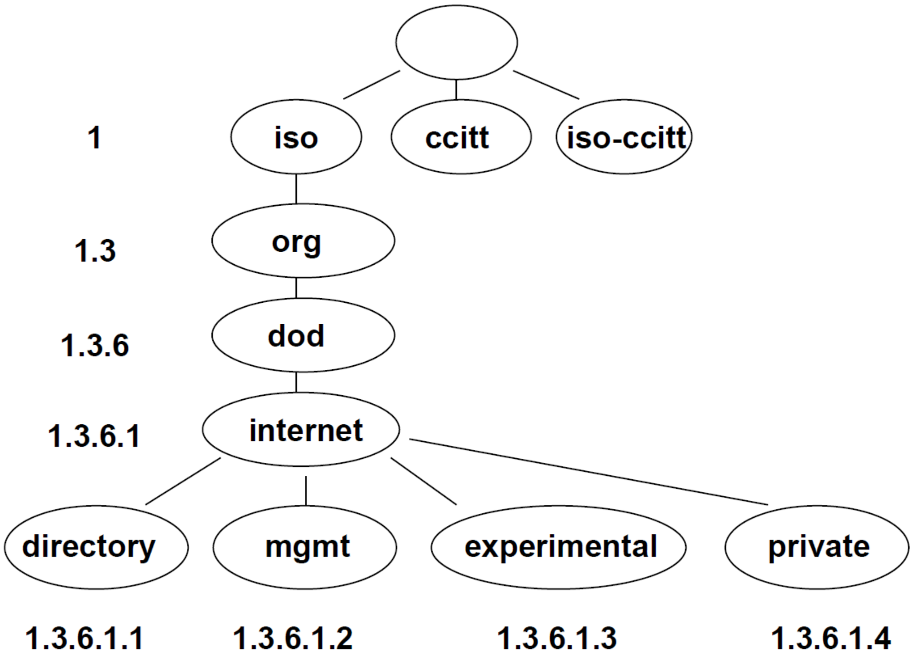


Figure 80: OID basic structure

The SNMP values specific to Advantech routers form a hierarchical tree starting at OID `.1.3.6.1.4.1.30140`. This OID can be interpreted as follows:

iso.org.dod.internet.private.enterprises.conel

This means that the router provides, for example, information about the internal temperature (OID `1.3.6.1.4.1.30140.3.3`) or power voltage (OID `1.3.6.1.4.1.30140.3.4`).

For digital inputs and outputs, the following OID range is used:

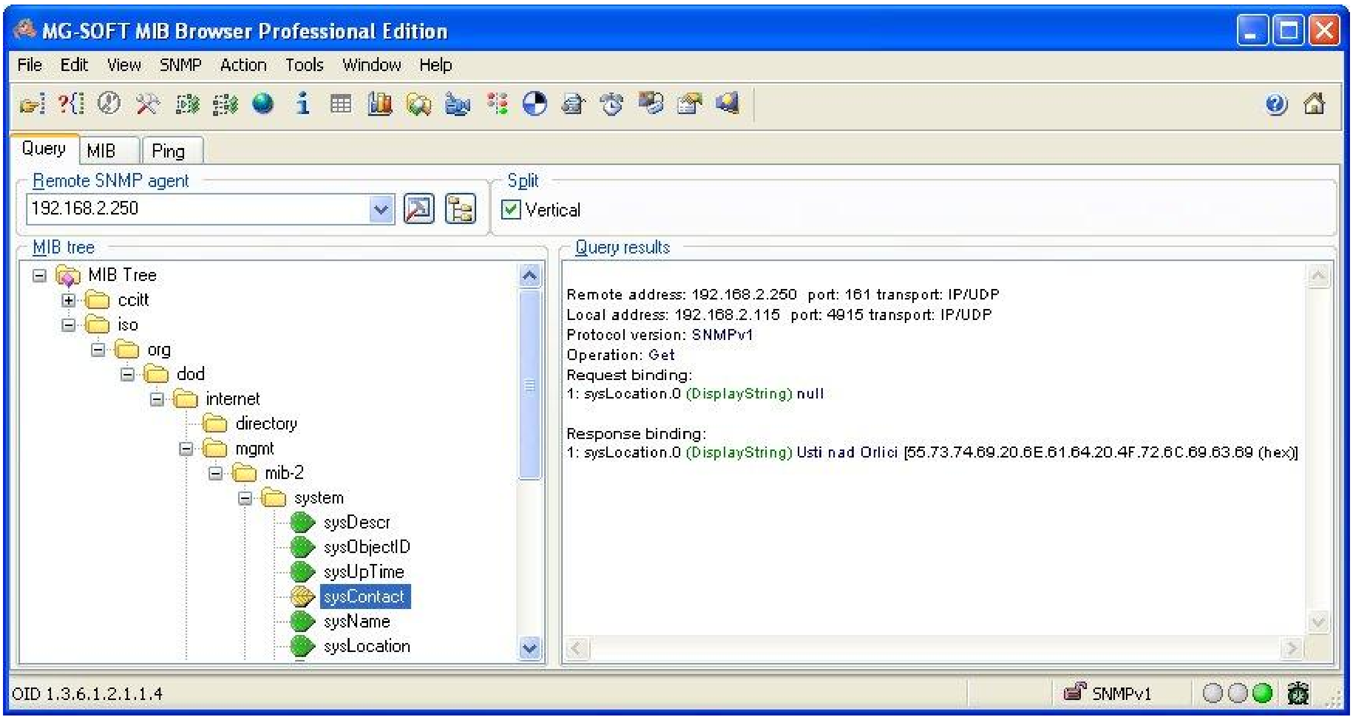
OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Digital input BIN0 (values: 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Digital output OUT0 (values: 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Digital input BIN1 (values: 0,1)

Table 74: Object identifiers for digital inputs and outputs

Info

The list of available and supported OIDs, along with other details, can be found in the application note *SNMP Object Identifiers* [12].

The next figure illustrates SNMP browsing in the *MIB Browser*.



```
Remote address: 192.168.2.250  port: 161 transport: IP/UDP
Local address: 192.168.2.115  port: 4915 transport: IP/UDP
Protocol version: SNMPv1
Operation: Get
Request binding:
1: sysLocation.0 (DisplayString) null

Response binding:
1: sysLocation.0 (DisplayString) Usti nad Orlici [55.73.74.69.20.6E.61.64.20.4F.72.6C.69.63.69 (hex)]
```

Figure 81: MIB browser example

To access a specific device, enter the IP address of the SNMP agent (the router) in the *Remote SNMP Agent* field. The dialog displays the internal variables in the MIB tree after entering the IP address. Additionally, you can check the status of internal variables by entering their corresponding OID.

The path to the SNMP objects is:

$$iso \rightarrow org \rightarrow dod \rightarrow internet \rightarrow private \rightarrow enterprises \rightarrow Conel \rightarrow protocols$$

The path to router-specific information is:

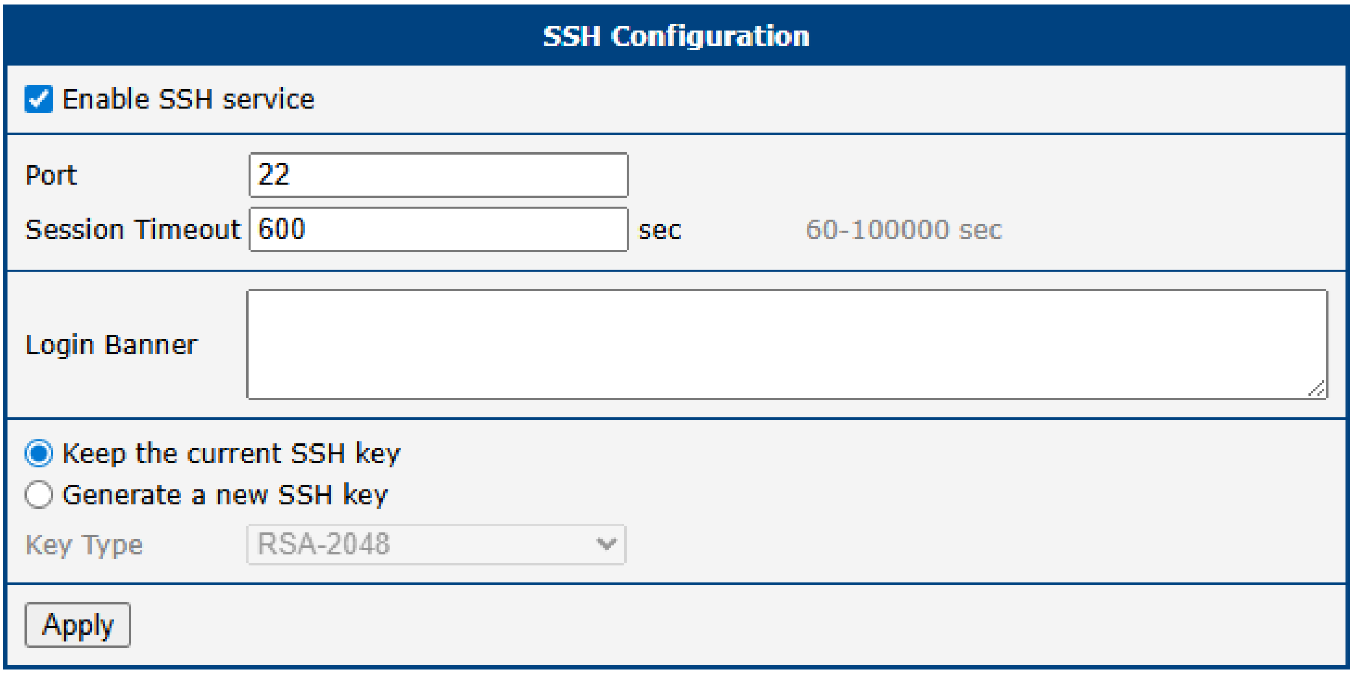
$$iso \rightarrow org \rightarrow dod \rightarrow internet \rightarrow mgmt \rightarrow mib\text{-}2 \rightarrow system$$

3.17.9 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

Access Restriction: Please note that only users assigned the *Admin* role are authorized to log in to the router via SSH. Users with a standard *User* role cannot access the command line.



SSH Configuration

☑ Enable SSH service

Port: 22

Session Timeout: 600 sec 60-100000 sec

Login Banner:

● Keep the current SSH key

○ Generate a new SSH key

Key Type: RSA-2048

Figure 82: SSH server configuration page

General Settings

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

Table 75: General SSH settings

Host Key Management

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

Info

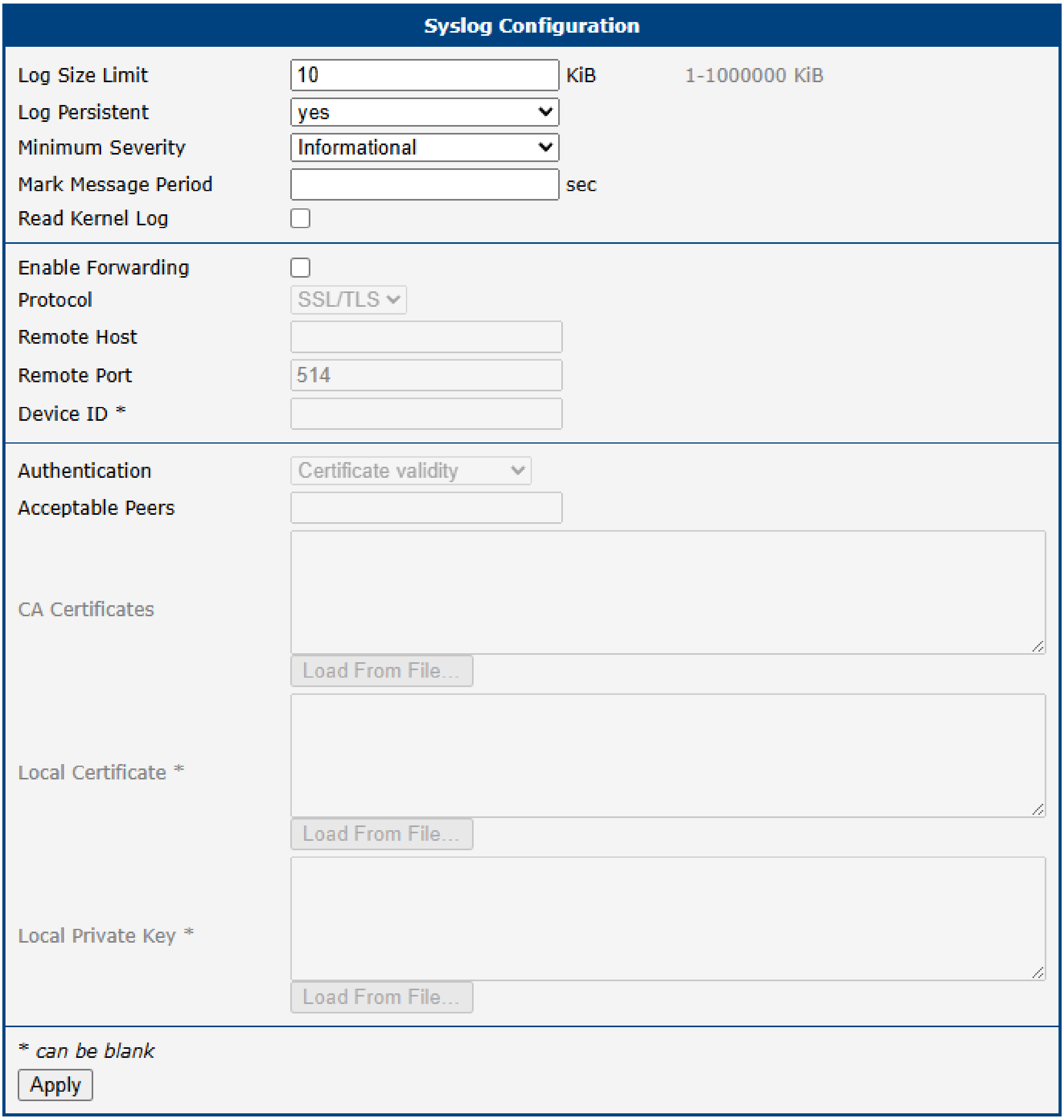
When you connect to the router via SSH for the first time, your client will prompt you to accept the host key's fingerprint. If the host key ever changes (e.g., after a new one is generated), your client will display a security warning. This is expected behavior.

Setting	Description
Keep the current SSH key	Retains the existing host key. This is the default and recommended option for normal operation.
Generate a new SSH key	Discards the current key and generates a new one. This is typically only done for security policy reasons.
Key Type	The cryptographic algorithm used for the host key. **ED25519** is a modern, fast, and secure elliptic curve algorithm. **RSA** is an older, widely supported standard.

Table 76: SSH host key settings

3.17.10 Syslog

The Syslog service collects and manages system messages from the router's operating system and various applications. To configure this service, navigate to *Services* → *Syslog*.
The collected logs can be viewed on the *Status* → *System Log* page (see Chapter *2.9 System Log*) or via the command line with the `slog` command.



Syslog Configuration

Log Size Limit	10	KiB	1-1000000 KiB
Log Persistent	yes		
Minimum Severity	Informational		
Mark Message Period		sec	
Read Kernel Log	□		
Enable Forwarding	□		
Protocol	SSL/TLS		
Remote Host			
Remote Port	514		
Device ID *			
Authentication	Certificate validity		
Acceptable Peers			
CA Certificates	Load From File...		
Local Certificate *	Load From File...		
Local Private Key *	Load From File...		

** can be blank*

Figure 83: Syslog configuration page

Local Logging

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

Setting	Description
Log Size Limit	Sets the maximum size (in KiB) for the local log files. The default is 10 KiB.
Log Persistent	If enabled, the system log will be 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.

Table 77: Local logging settings

Remote Forwarding

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

Setting	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.

Table 78: Remote forwarding settings

Remote Server Authentication

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

Setting	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.
Acceptable Peers	A list of accepted certificate fingerprints (SHA1) or DNS/Common Names. Wildcards (e.g., `*.example.net`) are supported for names.
CA Certificates	A file containing the full CA certificate chain in PEM format, used to validate the remote server's certificate.
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*.

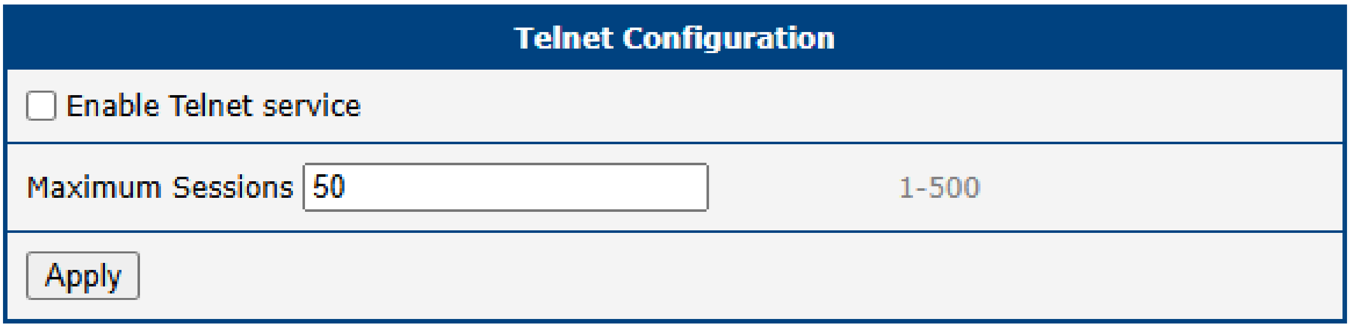
Table 79: Remote server authentication settings

3.17.11 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

□ Enable Telnet service

Maximum Sessions: 50 (1-500)

Figure 84: Telnet server configuration page

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

Table 80: Telnet configuration settings

3.18 Peripheral Ports

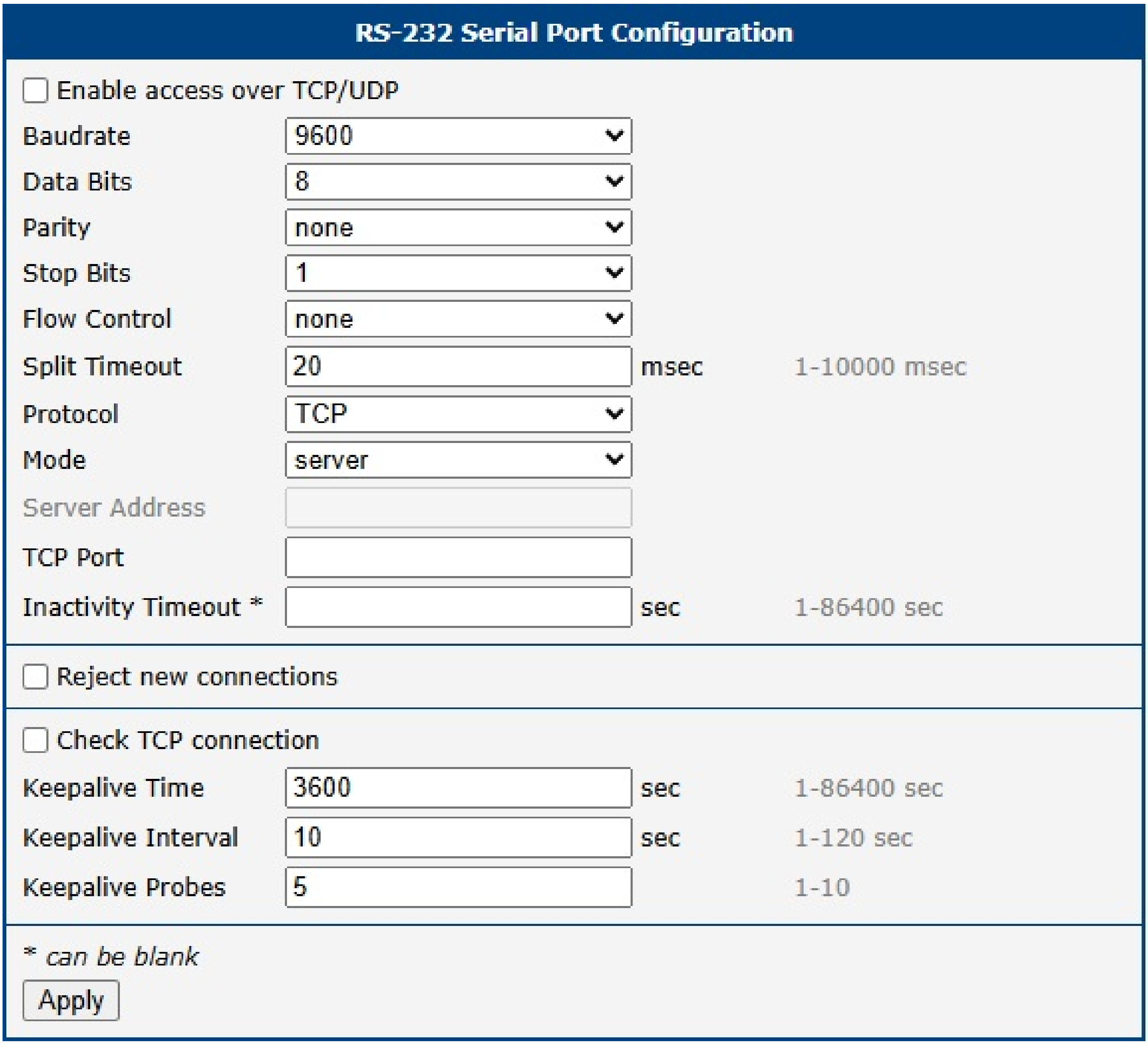
Info

Some interfaces may not be available for all models.

Configuration of physical interfaces such as RS-232, RS-485, USB serial converter, and digial Inputs/Outputs is now accessible from the *Configuration* → *Peripheral Ports* menu. Each interface is configured using its own subpage. Below, each port type is described in its own section.

3.18.1 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

☐ Enable access over TCP/UDP

Baudrate	9600		
Data Bits	8		
Parity	none		
Stop Bits	1		
Flow Control	none		
Split Timeout	20	msec	1-10000 msec
Protocol	TCP		
Mode	server		
Server Address			
TCP Port			
Inactivity Timeout *		sec	1-86400 sec

☐ Reject new connections

☐ Check TCP connection

Keepalive Time	3600	sec	1-86400 sec
Keepalive Interval	10	sec	1-120 sec
Keepalive Probes	5		1-10

** can be blank*

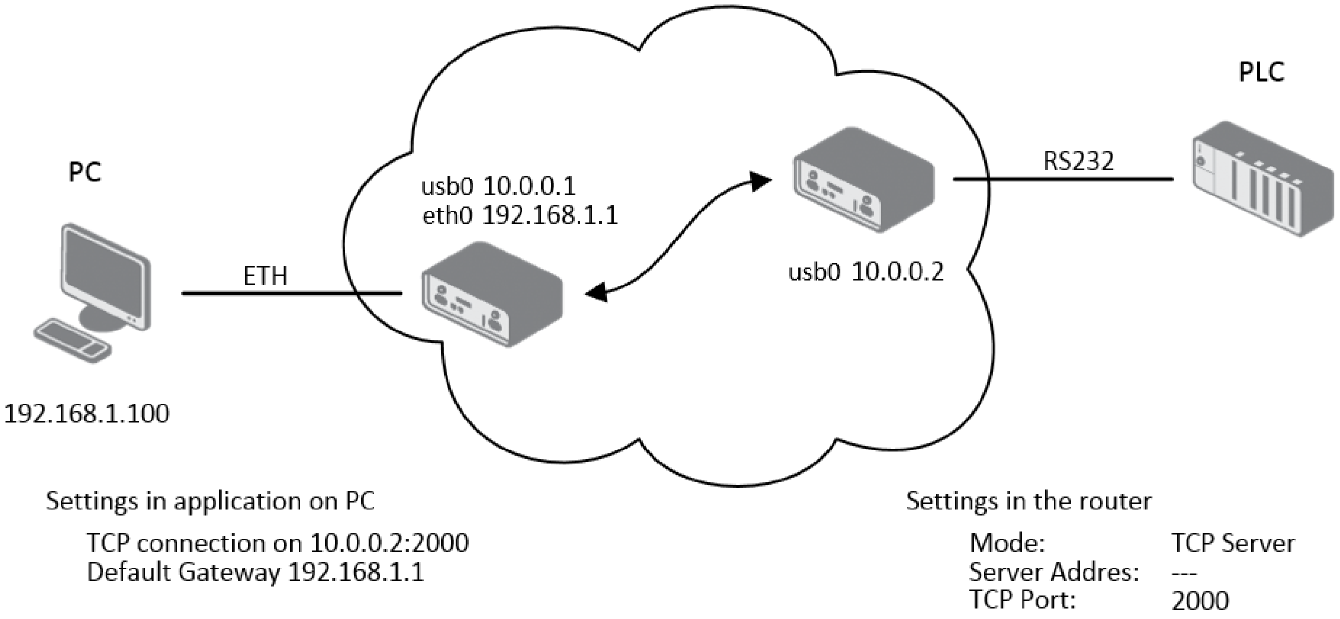
Figure 85: RS-232 serial port configuration

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).
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	Select the 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, specify the IP address or domain name of the remote server. Both IPv4 and IPv6 are supported.
TCP Port	The TCP/UDP port for communication. This setting applies to both server and client modes.
Inactivity Timeout	The time in seconds after which an inactive TCP/UDP connection is automatically terminated.
Reject new connections	If enabled, the router rejects new incoming connections when one is already active, enforcing a single-client connection.
Check TCP connection	If enabled, the router actively monitors the TCP connection status using keepalive packets.
Keepalive Time	The time interval in seconds after which the router sends a keepalive probe to verify the connection.
Keepalive Interval	The duration in seconds the router waits for a response to a probe before resending it.
Keepalive Probes	The number of unanswered probes before the connection is considered inactive.

Table 81: RS-232 serial port configuration items

Ethernet-to-Serial Communication Example

This scenario demonstrates how to use the router as a gateway to connect a PC on an Ethernet network to a remote serial device. As shown in the figure, a PC with the IP address 192.168.1.100 sends data to the remote router (10.0.0.2) on TCP port 2000. This 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.



Settings in application on PC

TCP connection on 10.0.0.2:2000
Default Gateway 192.168.1.1

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Figure 86: Ethernet-to-serial communication configuration example

Serial Interface Communication (Serial Tunnel) Examle

This example illustrates how to create a transparent serial tunnel over an IP network, effectively extending a serial connection over a long distance. The PC is connected via RS-232 to the first router (10.0.0.1), which is configured in *TCP Client* mode. It 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 sent from the PC is automatically tunneled over the TCP connection to the second router and then passed to the PLC.

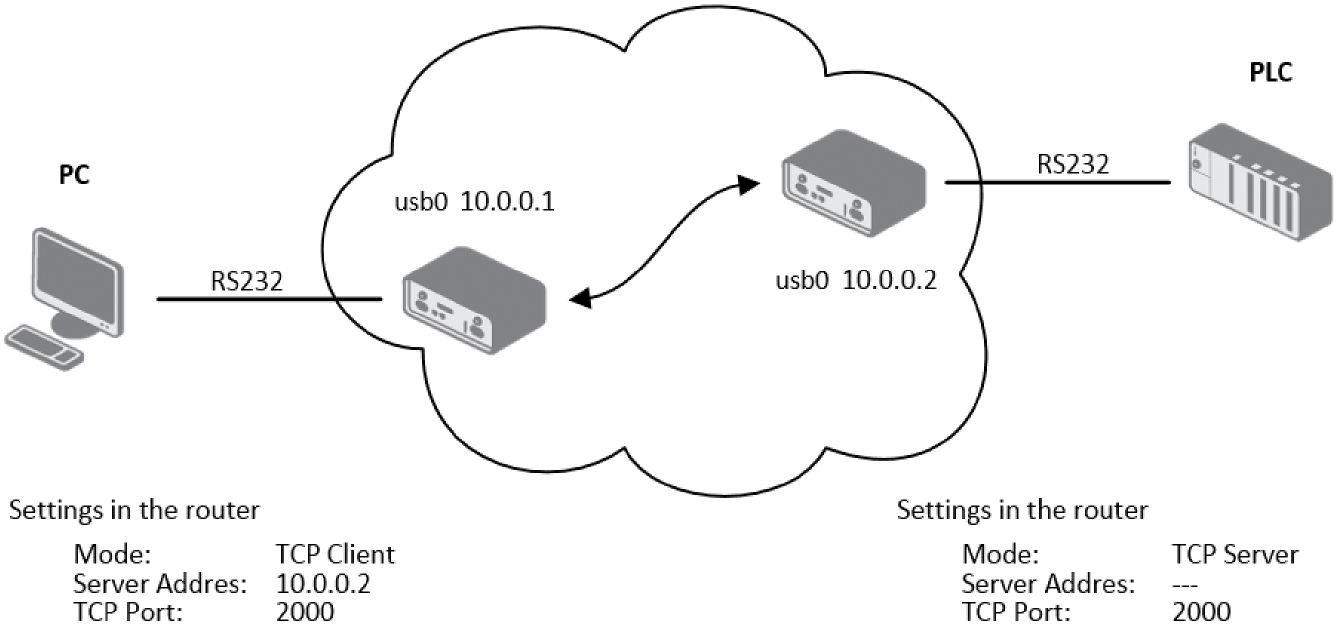


Figure 87: Serial interface configuration example

3.18.2 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 previous section for the RS-232 port.

3.18.3 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 application note for the *Ext4 Filesystem Utilities* Router App.

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 filesystems on attached storage are properly unmounted to prevent data corruption. This can be done in the console using the `umount /mnt/usb_storage` command, for example.
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 a list of supported USB converters, refer to the *Extending Router Functionality* application note. Refer to Chapter 3.18.3 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. **Unmounting 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. USB devices are identified by a **Vendor ID (VID)** and a **Product ID (PID)**.

Finding the VID and PID

You can find the VID and PID of your device:

- **On Linux:** Use the `lsusb` command (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:

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

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

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

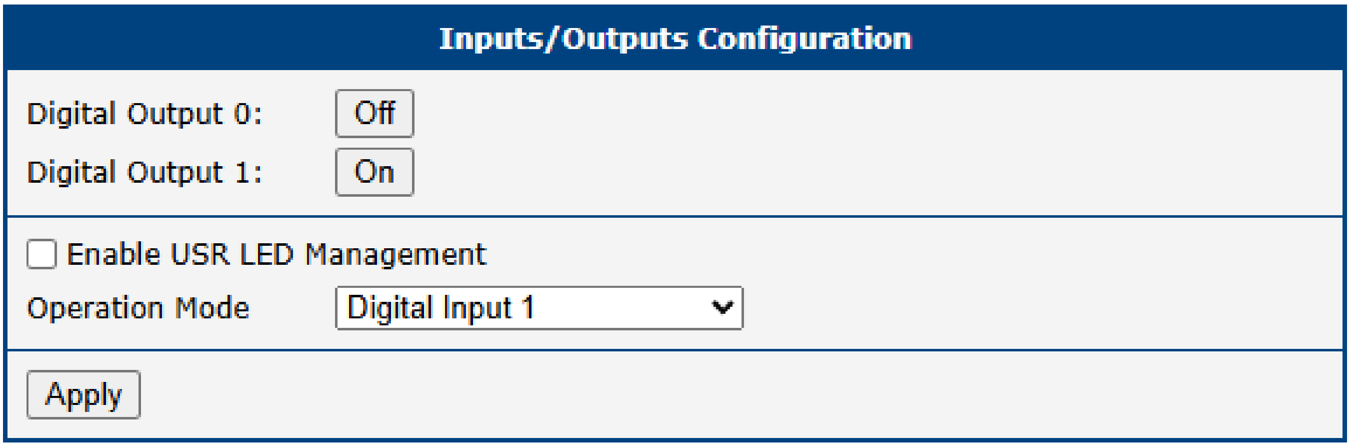
After running this command, the driver should recognize the device. If not, try reloading the driver or reconnecting the device.

3.18.4 Inputs/Outputs

Info

Starting from router firmware version 6.6.0, the USR LED settings on this page replace the original *USR LED Management* RouterApp, 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

Digital Output 0: Off

Digital Output 1: On

□ Enable USR LED Management

Operation Mode: Digital Input 1

Figure 88: Inputs/Outputs configuration example

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 WiFi AP and flashes during communication.
WiFi STA activity	The LED lights when the router is connected to a remote WiFi 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.

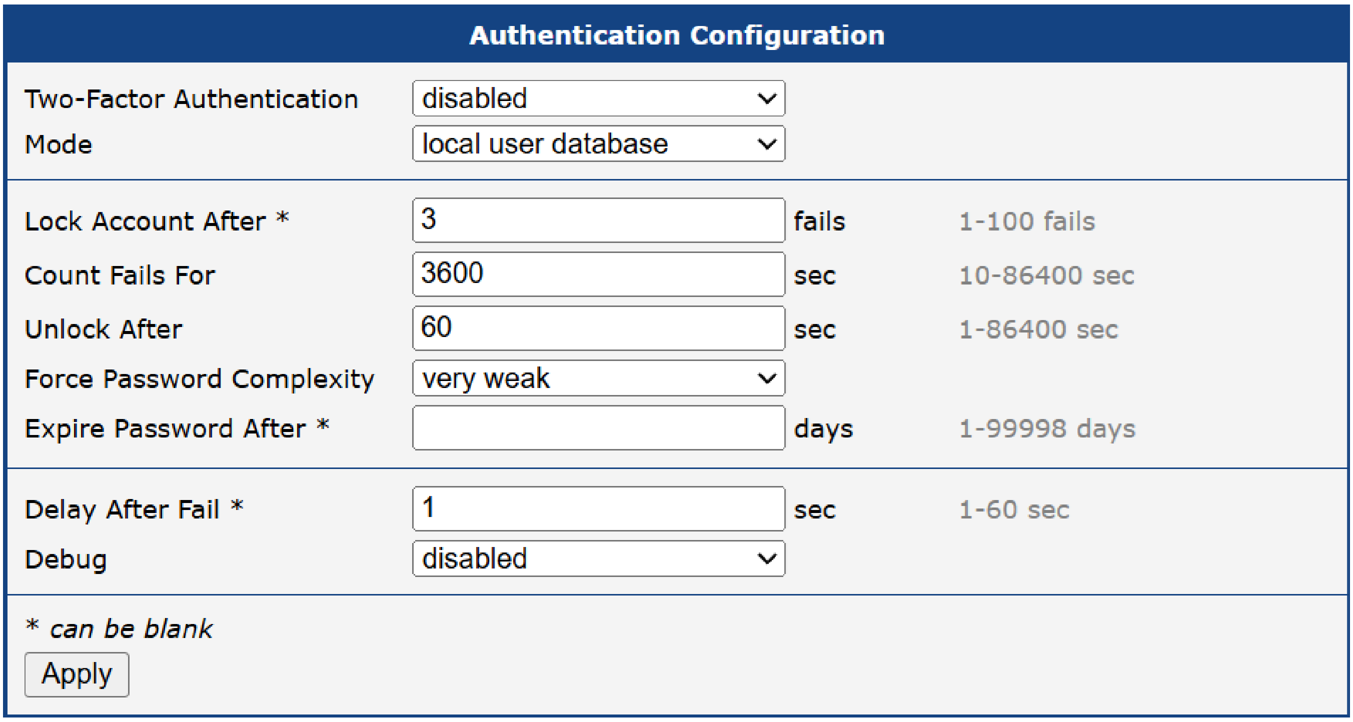
Table 82: USR LED operation modes overview

3.19 System

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

3.19.1 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

Two-Factor Authentication	disabled		
Mode	local user database		
Lock Account After *	3	fails	1-100 fails
Count Fails For	3600	sec	10-86400 sec
Unlock After	60	sec	1-86400 sec
Force Password Complexity	very weak		
Expire Password After *		days	1-99998 days
Delay After Fail *	1	sec	1-60 sec
Debug	disabled		

** can be blank*

Figure 89: 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*. See Chapter *5.1.3 Two-Factor Authentication (2FA)* for details.
Mode	Selects the primary authentication method: • **Local user database**: Authenticates against the router's local user list (see Chapter *5.1 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.

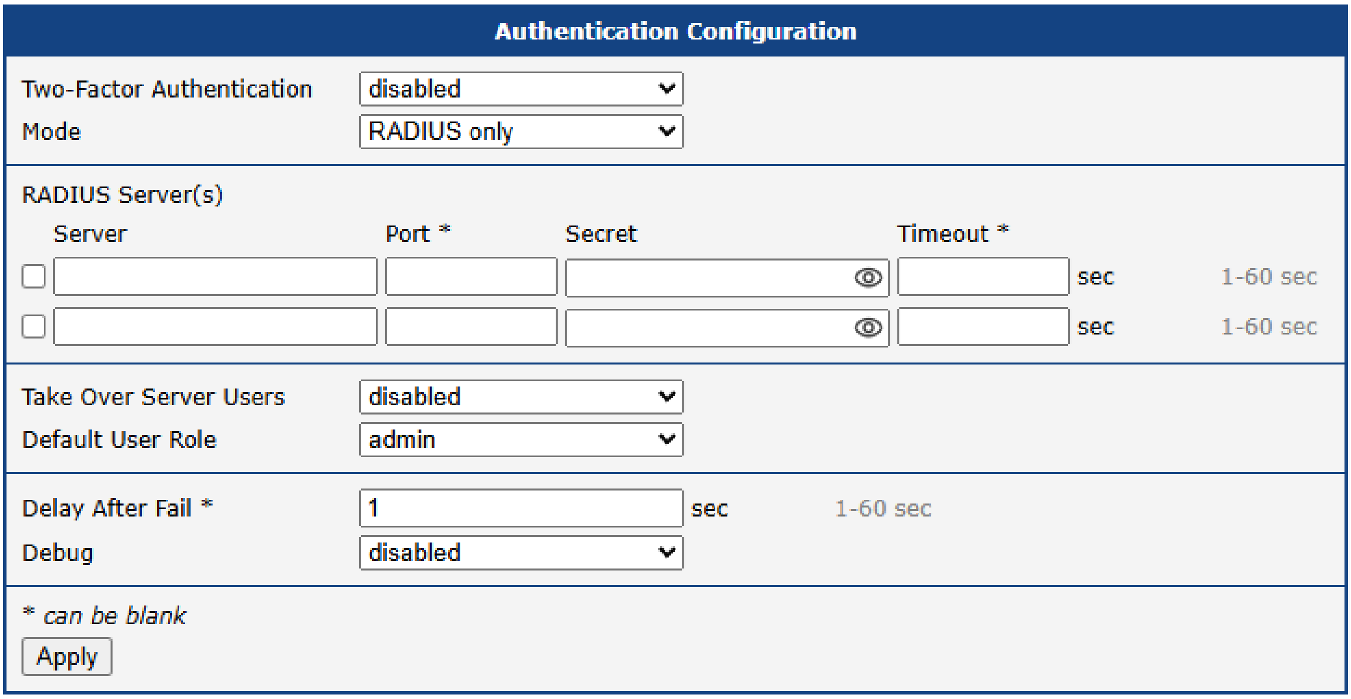
Table 83: General authentication configuration options

Item	Description
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.
Unlock After	The duration in seconds after which a locked account is automatically unlocked.
Force Password Complexity	Enforces minimum password strength requirements. There are four character classes: uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and other characters (e.g., `!@#$+.`). • **Very Weak**: ○ Must be at least 6 characters long. ○ Must not contain the username. ○ Must not be a palindrome. • **Weak**: ○ Must be at least 8 characters long. ○ Must contain characters from at least 2 of the 4 classes. ○ Must not contain the username. ○ Must not be a palindrome. • **Good**: ○ Must be at least 12 characters long. ○ Must contain characters from at least 3 of the 4 classes. ○ Must not contain more than 3 identical consecutive characters. ○ Must not contain the username. ○ Must not be a palindrome. • **Strong**: ○ Must be at least 16 characters long. ○ Must contain characters from all 4 classes. ○ Must not contain 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. See Chapter *5.1.5 Forced Password Change*.
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.

Table 83: (continued)

RADIUS Mode

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



Authentication Configuration

Two-Factor Authentication	disabled
Mode	RADIUS only

RADIUS Server(s)

	Server	Port *	Secret	Timeout *		
□					sec	1-60 sec
□					sec	1-60 sec

Take Over Server Users	disabled		
Default User Role	admin		
Delay After Fail *	1	sec	1-60 sec
Debug	disabled		

** can be blank*

Figure 90: RADIUS configuration

Warning

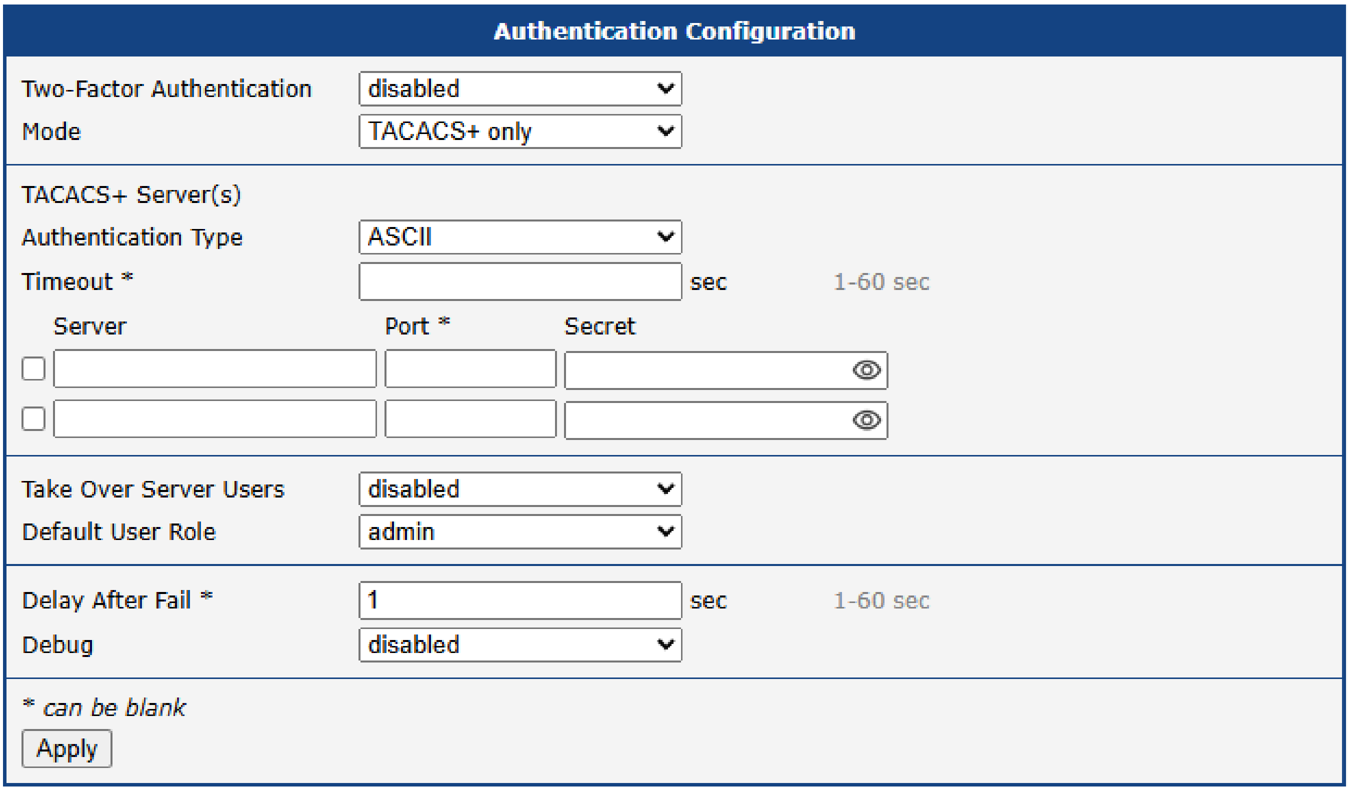
For a RADIUS user to log in, a corresponding user account must exist on the router locally. This account can be created manually (see Chapter *5.1 Manage Users*) or automatically by enabling the *Take Over Server Users* option.

Item	Description
Server	The IP address of the primary and optional secondary RADIUS server.
Port	The UDP port of the RADIUS server (default is 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	If enabled, a local user account will be created automatically upon successful RADIUS authentication if one does not already exist. The local 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.

Table 84: RADIUS configuration options

TACACS+ Mode

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



Authentication Configuration

Two-Factor Authentication	disabled		
Mode	TACACS+ only		
TACACS+ Server(s)			
Authentication Type	ASCII		
Timeout *		sec	1-60 sec

	Server	Port *	Secret
□			
□			

Take Over Server Users	disabled		
Default User Role	admin		
Delay After Fail *	1	sec	1-60 sec
Debug	disabled		

** can be blank*

Figure 91: 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 Chapter *5.1 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 is 49).
Secret	The shared secret used to encrypt communication with the TACACS+ server.
Take Over Server Users	If enabled, a local user account will be created automatically upon successful TACACS+ authentication if one does not already exist. The local account is created without a password.
Default User Role	Assigns a default role (*Admin* or *User*) to users created via the *Take Over* feature.

Table 85: TACACS+ configuration options

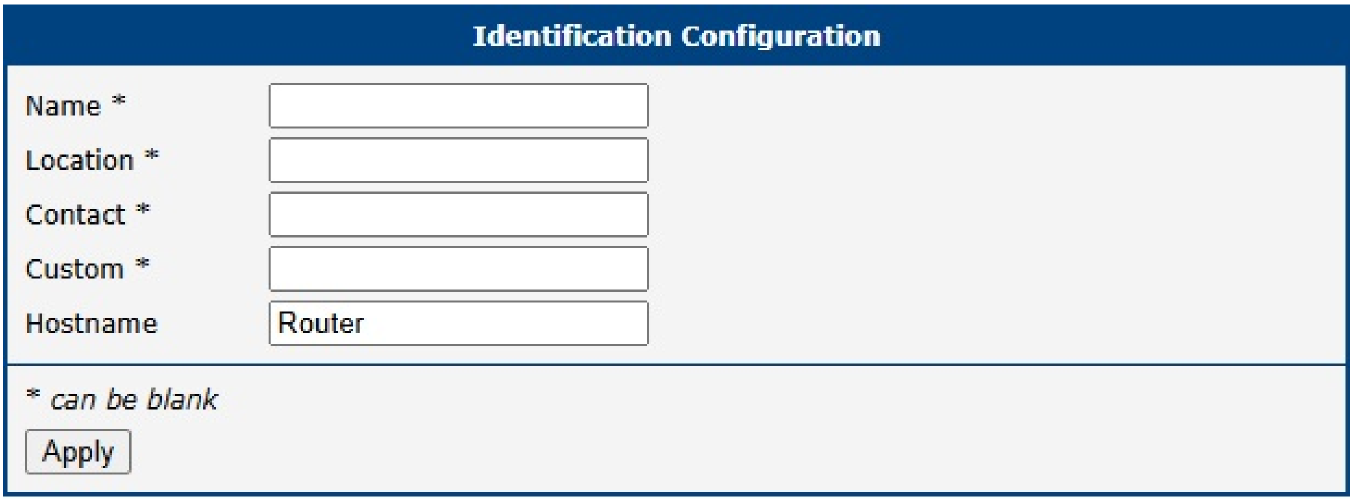
3.19.2 Identification

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 for easy identification.
- The *Name*, *Location*, *Contact*, and *Custom* fields are all exposed via the Simple Network Management Protocol (SNMP) for remote monitoring, as detailed in Chapter *3.17.8 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

Name *	
Location *	
Contact *	
Custom *	
Hostname	Router

** can be blank*

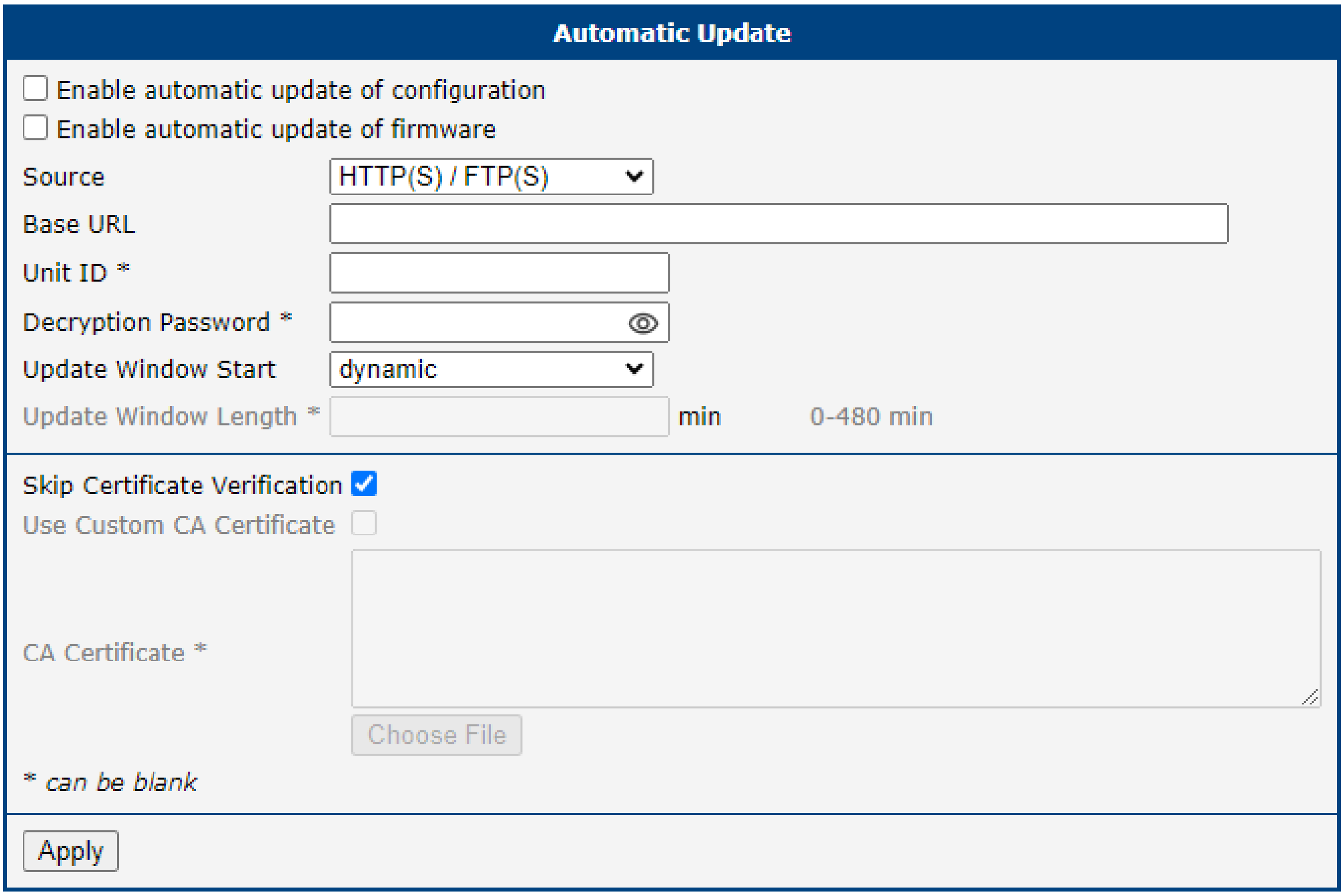
Figure 92: Identification configuration page

Item	Description
Name	A custom name for the router (e.g., "Main Office Gateway"). This is also used as the SNMP System Name (sysName).
Location	The physical location of the router (e.g., "Server Room A"). This is 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). This is used as the SNMP System Contact (sysContact).
Custom	A custom string for any additional information. This is used as the SNMP System Location (infoCustom).
Hostname	The hostname of the router, used to identify the device on the local network (e.g., in DHCP leases).

Table 86: Identification configuration items

3.19.3 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

□ Enable automatic update of configuration

□ Enable automatic update of firmware

Source: HTTP(S) / FTP(S)

Base URL:

Unit ID *:

Decryption Password *:

Update Window Start: dynamic

Update Window Length *: min 0-480 min

Skip Certificate Verification ☑

Use Custom CA Certificate □

CA Certificate *:

* can be blank

Figure 93: Automatic Update configuration page

Update Configuration

The following table describes the parameters for configuring the automatic update process.

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.

Table 87: Automatic Update configuration options

Item	Description
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 this field is 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 that defines a window of time, starting at the *Update Window Start*, during which the update will be performed at a random moment. This helps to distribute the load on the update server in large deployments.
Skip Certificate Verification	If checked, the router will not validate the SSL/TLS certificate of the remote HTTPS/FTPS server.
Use Custom CA Certificate	Enables validation of the server's certificate against a custom Certificate Authority (CA) certificate provided below.
CA Certificate	The custom CA certificate used for server validation.

Table 87: (continued)

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 (see Chapter *5.9 Update Firmware*). A corresponding version file (`*.ver`) must also be present on the server.
- **Configuration**: The configuration filename is determined by the *Unit ID*. If the *Unit ID* is specified, that value is used as the filename (e.g., `test.cfg`). If it is left blank, the router will look for a file named after its ETH0 MAC address, with colons replaced by dots (e.g., `00.11.22.33.44.55.cfg`).

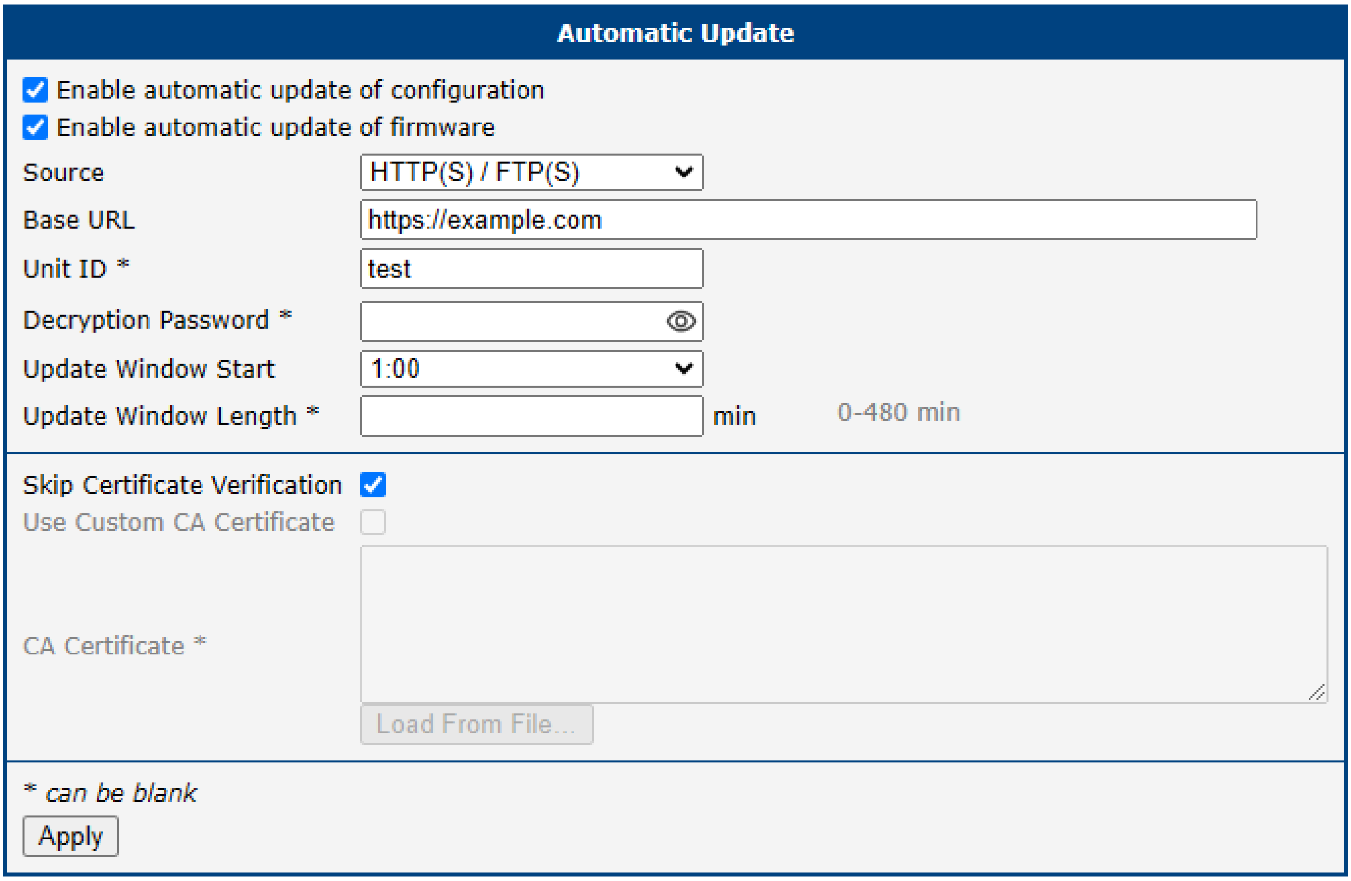
Warning

- 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 application notes 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*



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

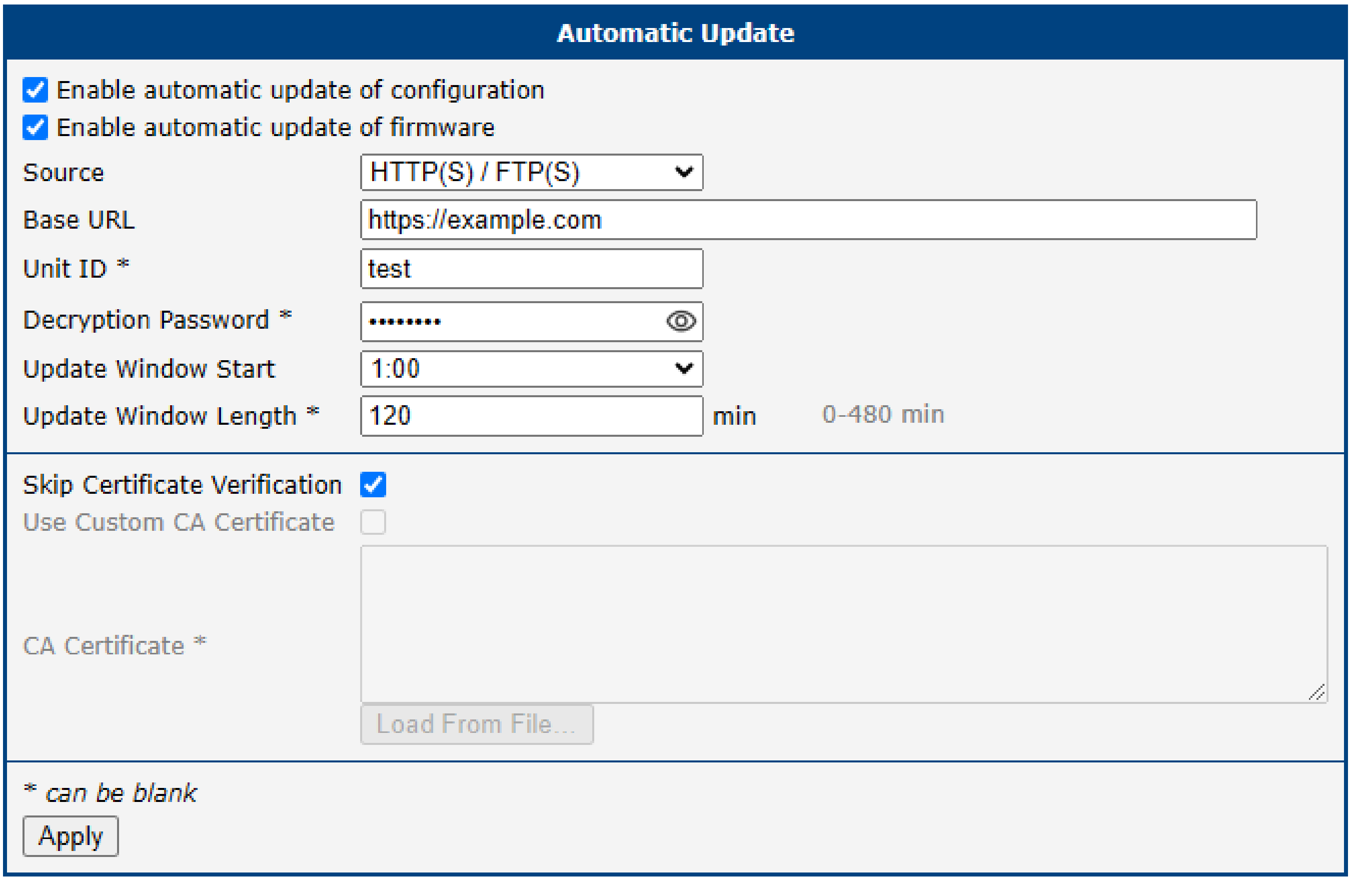
Source	HTTP(S) / FTP(S)		
Base URL	https://example.com		
Unit ID *	test		
Decryption Password *			
Update Window Start	1:00		
Update Window Length *		min	0-480 min
Skip Certificate Verification	☑		
Use Custom CA Certificate	□		
CA Certificate *			

** can be blank*

Figure 94: 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*



Automatic Update

☑ Enable automatic update of configuration
☑ Enable automatic update of firmware

Source	HTTP(S) / FTP(S)	
Base URL	https://example.com	
Unit ID *	test	
Decryption Password *	••••••••	
Update Window Start	1:00	
Update Window Length *	120	min 0-480 min
Skip Certificate Verification	☑	
Use Custom CA Certificate	□	
CA Certificate *		

** can be blank*

Figure 95: Example of an automatic update using the MAC address

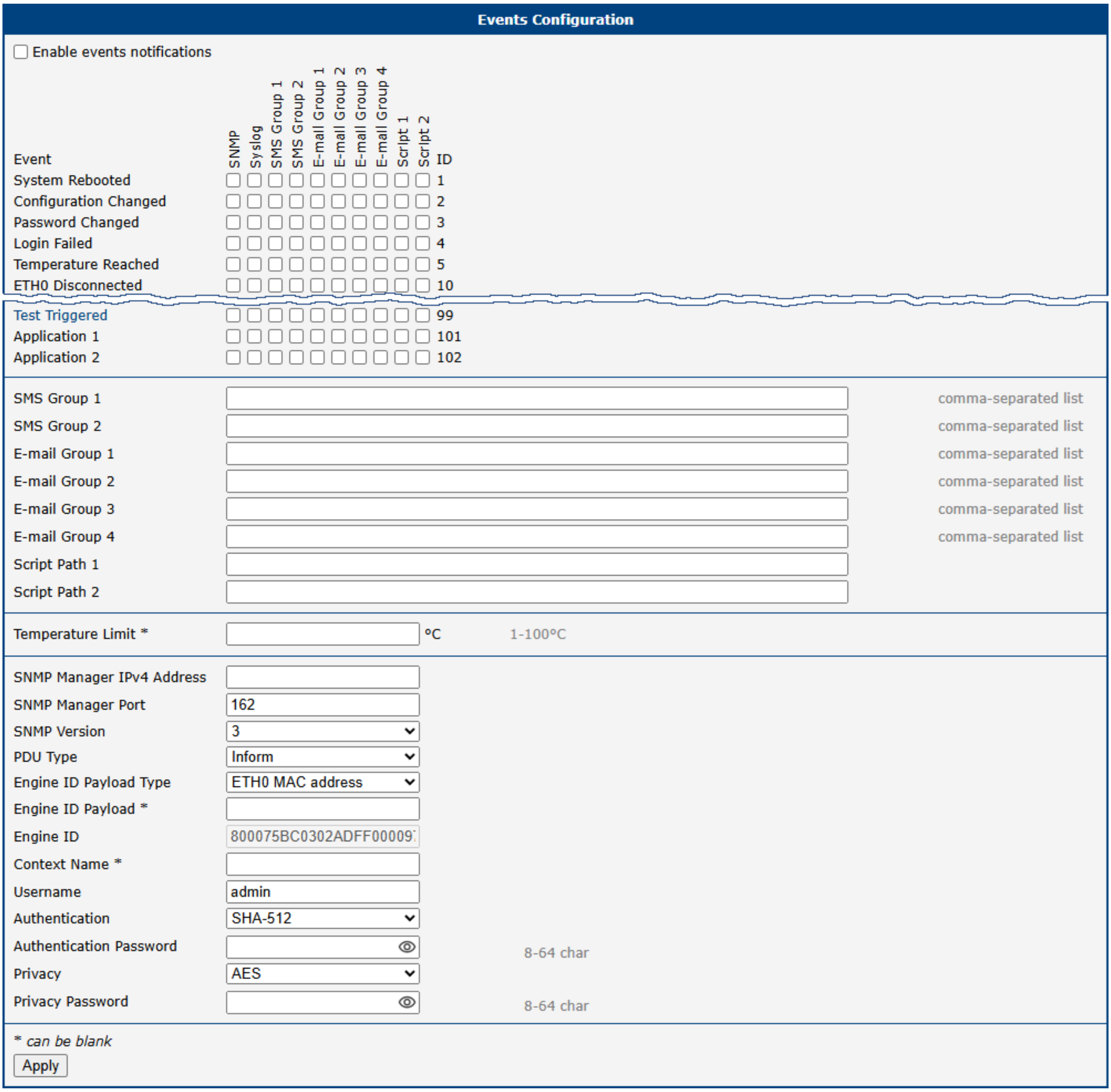
3.20 Events

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.

Info

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

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



Events Configuration

□ Enable events notifications

Event	SNMP	Syslog	SMS Group 1	SMS Group 2	E-mail Group 1	E-mail Group 2	E-mail Group 3	E-mail Group 4	Script 1	Script 2	ID
System Rebooted	□	□	□	□	□	□	□	□	□	□	1
Configuration Changed	□	□	□	□	□	□	□	□	□	□	2
Password Changed	□	□	□	□	□	□	□	□	□	□	3
Login Failed	□	□	□	□	□	□	□	□	□	□	4
Temperature Reached	□	□	□	□	□	□	□	□	□	□	5
ETH0 Disconnected	□	□	□	□	□	□	□	□	□	□	10
Test Triggered	□	□	□	□	□	□	□	□	□	□	99
Application 1	□	□	□	□	□	□	□	□	□	□	101
Application 2	□	□	□	□	□	□	□	□	□	□	102

SMS Group 1		comma-separated list
SMS Group 2		comma-separated list
E-mail Group 1		comma-separated list
E-mail Group 2		comma-separated list
E-mail Group 3		comma-separated list
E-mail Group 4		comma-separated list
Script Path 1		
Script Path 2		
Temperature Limit *	°C	1-100°C
SNMP Manager IPv4 Address		
SNMP Manager Port	162	
SNMP Version	3	
PDU Type	Inform	
Engine ID Payload Type	ETH0 MAC address	
Engine ID Payload *		
Engine ID	800075BC0302ADFF00009	
Context Name *		
Username	admin	
Authentication	SHA-512	
Authentication Password		8-64 char
Privacy	AES	
Privacy Password		8-64 char

* *can be blank*

Figure 96: 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.
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 your configured actions (e.g., to verify that an SMS or email is sent correctly). **Note:** Before testing, you must ensure that the event system is enabled, the desired actions are configured, and all settings are saved. The test can then be triggered manually by clicking on the event name itself, which acts as a hyperlink in the web interface.
Application 1/2	Custom events that can be triggered by user scripts or applications (IDs 101 and 102).

Table 88: Available events

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 E-mail group.
Script 1/2	Executes the user script located at the specified path.

Table 89: Available actions

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 E-mail action group.
Script Path 1/2	The absolute path to the user script to be executed for the respective script action (e.g., `/var/scripts/my_script.sh`).
Temperature Limit	The temperature threshold in degrees Celsius (°C) for the *Temperature Reached* event.

Table 90: Action definitions

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, this field allows you to 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.

Table 91: SNMP settings for events

3.21 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 Note. For broader guidance on customization, see the *Extending Router Functionality* Application Note.

3.21.1 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.

Example

The following script sends an SMS message upon router startup.

Code Example

```
#!/bin/sh

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

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

exit 0
```

3.21.2 Up/Down IPv4

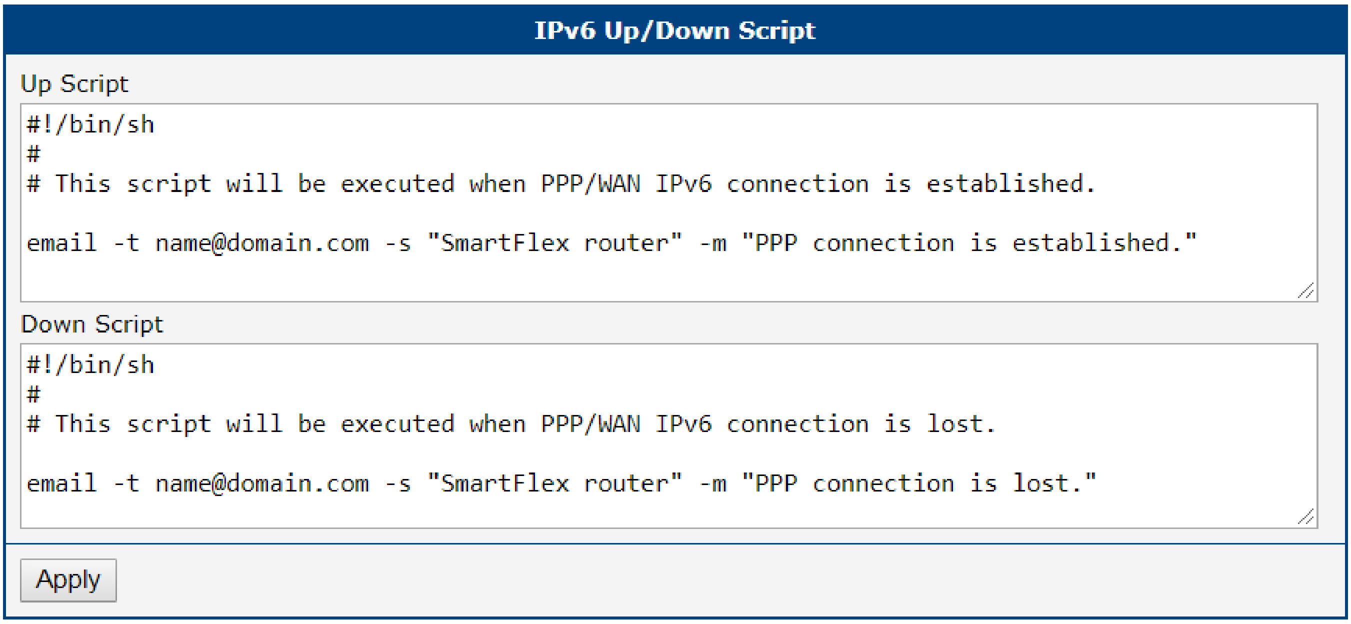
The *Up/Down IPv4* page allows you to define scripts that are triggered by changes in the primary WAN IPv4 connection state. The "Up" script runs when the IPv4 connection is established, and the "Down" script runs when it is lost. Because the router has a dual-stack implementation, scripts for IPv4 and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

3.21.3 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.

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

Up Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is established.

email -t name@domain.com -s "SmartFlex router" -m "PPP connection is established."
```

Down Script

```
#!/bin/sh
#
# This script will be executed when PPP/WAN IPv6 connection is lost.

email -t name@domain.com -s "SmartFlex router" -m "PPP connection is lost."
```

Figure 97: IPv6 up/down script configuration page

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

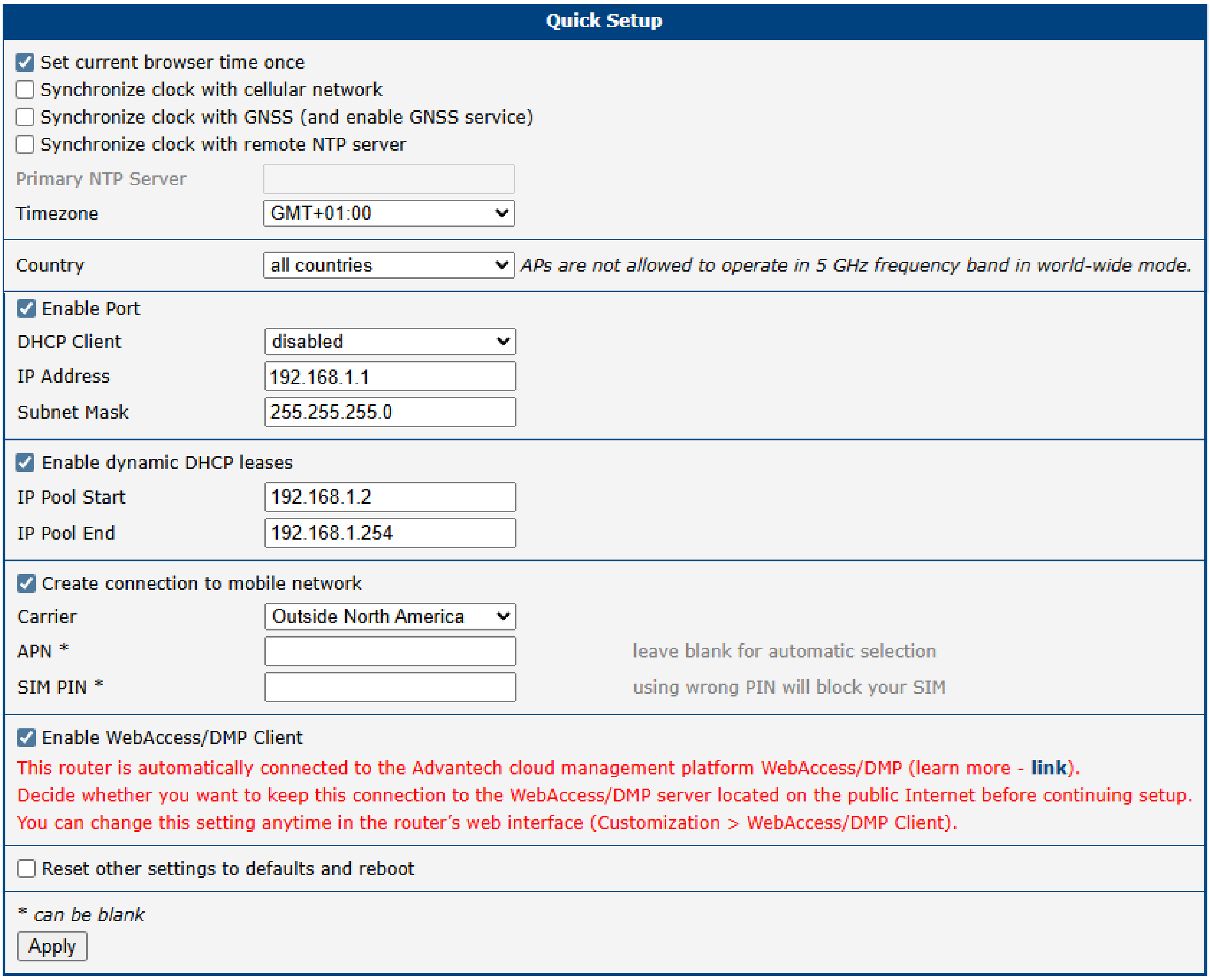
Down Script: `email -t name@domain.com -s "Router Alert" -m "IPv6 WAN connection is DOWN."`

Warning

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

3.22 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 the *Configuration → Quick Setup* menu.
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

☑ Set current browser time once
☐ Synchronize clock with cellular network
☐ Synchronize clock with GNSS (and enable GNSS service)
☐ Synchronize clock with remote NTP server

Primary NTP Server	
Timezone	GMT+01:00

Country: all countries — *APs are not allowed to operate in 5 GHz frequency band in world-wide mode.*

☑ Enable Port

DHCP Client	disabled
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.254

☑ Create connection to mobile network

Carrier	Outside North America	
APN *		leave blank for automatic selection
SIM PIN *		using wrong PIN will block your SIM

☑ Enable WebAccess/DMP Client
This router is automatically connected to the Advantech cloud management platform WebAccess/DMP (learn more - **link**).
Decide whether you want to keep this connection to the WebAccess/DMP server located on the public Internet before continuing setup.
You can change this setting anytime in the router's web interface (Customization > WebAccess/DMP Client).

☐ Reset other settings to defaults and reboot

** can be blank*

Figure 98: Quick Setup page

Time and Region

For a complete overview of these settings, refer to Chapter *5.4 Set Date and Time*, Chapter *3.17.5 NTP*, and Chapter *3.6.3 Country*.

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 be used when *Synchronize clock with remote NTP server* is selected.
Timezone	Sets the local timezone for the router.
Country	For models equipped with Wi-Fi, this setting configures the regulatory domain. It is crucial to select the country of operation to ensure compliance with local radio frequency regulations, as this affects which Wi-Fi channels are available.

Table 92: Quick Setup: Time and Region

LAN Port and DHCP Server

The full configuration options for the LAN interface are described in Chapter *3.1 Ethernet*.

Item	Description
Enable Port	Enables or disables the primary LAN port (`eth0`).
DHCP Client	If enabled, the router's LAN port will request 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 will lease to clients.
IP Pool End	The ending address of the IP range that the DHCP server will lease to clients.

Table 93: Quick Setup: LAN Port and DHCP Server

Mobile Network

Info

This section is only available on cellular router models.

The complete configuration for the mobile network is available in Chapter *3.4 Mobile WAN*.

Item	Description
Create connection to mobile network	When checked, the router will automatically attempt to connect to the mobile network after booting.
Carrier	Allows for 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.

Table 94: Quick Setup: Mobile Network

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 Chapter *1.2.2 Remote Management Platform*.
Reset other settings to defaults and reboot	If checked, any settings not present on this Quick Setup page will be reset to their factory defaults when the new configuration is applied.

Table 95: Quick Setup: System and Service Settings

4. Customization

4.1 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 webpage*.

Info

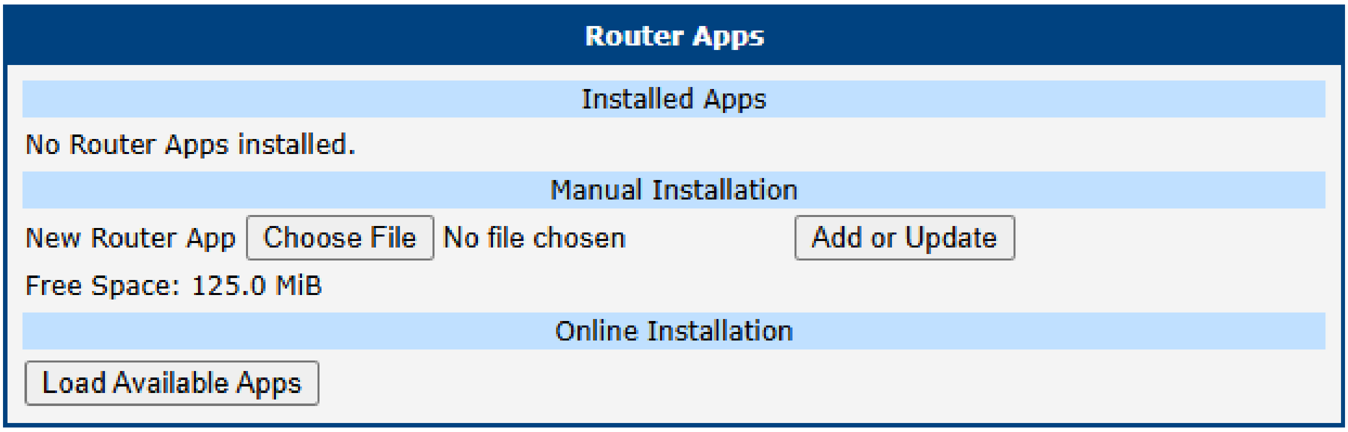
Users with the *Admin* role can install, manage, and view Router Apps. Users with the *User* role can only view the list of installed apps.

Overview of the Router Apps Page

To manage apps, navigate to the *Customization* → *Router Apps* page. 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.



Router Apps

Installed Apps

No Router Apps installed.

Manual Installation

New Router App No file chosen

Free Space: 125.0 MiB

Online Installation

Figure 99: Default Router Apps page

Installation and Management

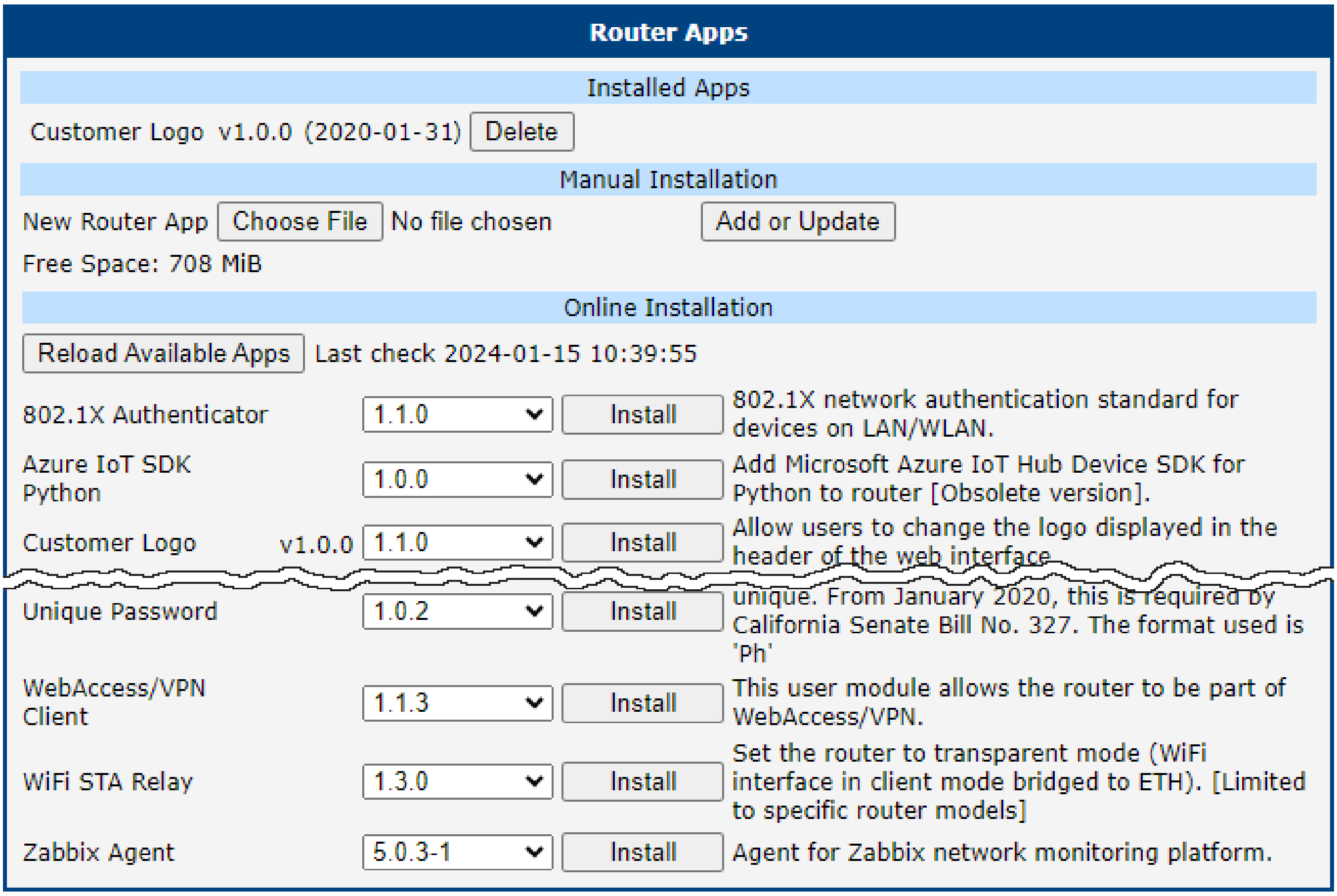
Manual Installation

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 to perform this action. Without DNS, 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 (see Chapter *4.2 Settings*). Note that the *Load Available Apps* button is disabled if communication with the server 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

Installed Apps

Customer Logo v1.0.0 (2020-01-31) Delete

Manual Installation

New Router App Choose File No file chosen Add or Update

Free Space: 708 MiB

Online Installation

Reload Available Apps Last check 2024-01-15 10:39:55

802.1X Authenticator		1.1.0	Install	802.1X network authentication standard for devices on LAN/WLAN.
Azure IoT SDK Python		1.0.0	Install	Add Microsoft Azure IoT Hub Device SDK for Python to router [Obsolete version].
Customer Logo	v1.0.0	1.1.0	Install	Allow users to change the logo displayed in the header of the web interface
Unique Password		1.0.2	Install	unique. From January 2020, this is required by California Senate Bill No. 327. The format used is 'Ph'
WebAccess/VPN Client		1.1.3	Install	This user module allows the router to be part of WebAccess/VPN.
WiFi STA Relay		1.3.0	Install	Set the router to transparent mode (WiFi interface in client mode bridged to ETH). [Limited to specific router models]
Zabbix Agent		5.0.3-1	Install	Agent for Zabbix network monitoring platform.

Figure 100: Router Apps page with online apps loaded

Managing Installed Apps

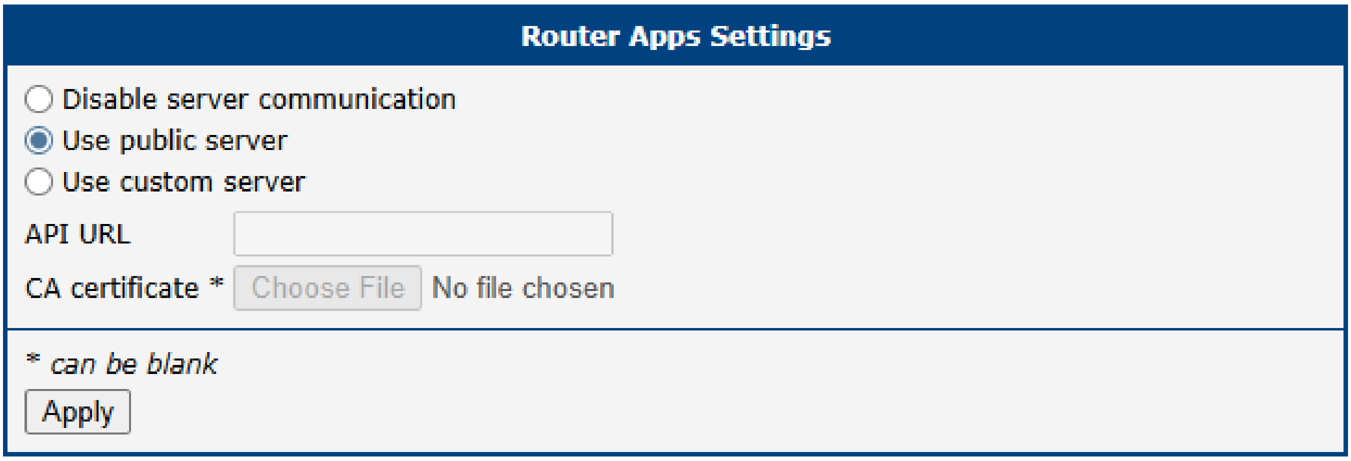
All installed apps are listed in the *Installed Apps* section.

- **Accessing an App GUI:** If an app has a web interface, its name will be 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, please refer to the *Extending Router Functionality* Application Note [2].

4.2 Settings

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



Router Apps Settings

○ Disable server communication
● Use public server
○ Use custom server

API URL

CA certificate * No file chosen

* can be blank

Figure 101: Router Apps server settings

Setting	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.

Table 96: Router Apps server settings descriptions

5. Administration

5.1 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 Chapter *5.2 Modify User*.

5.1.1 Managing User Accounts

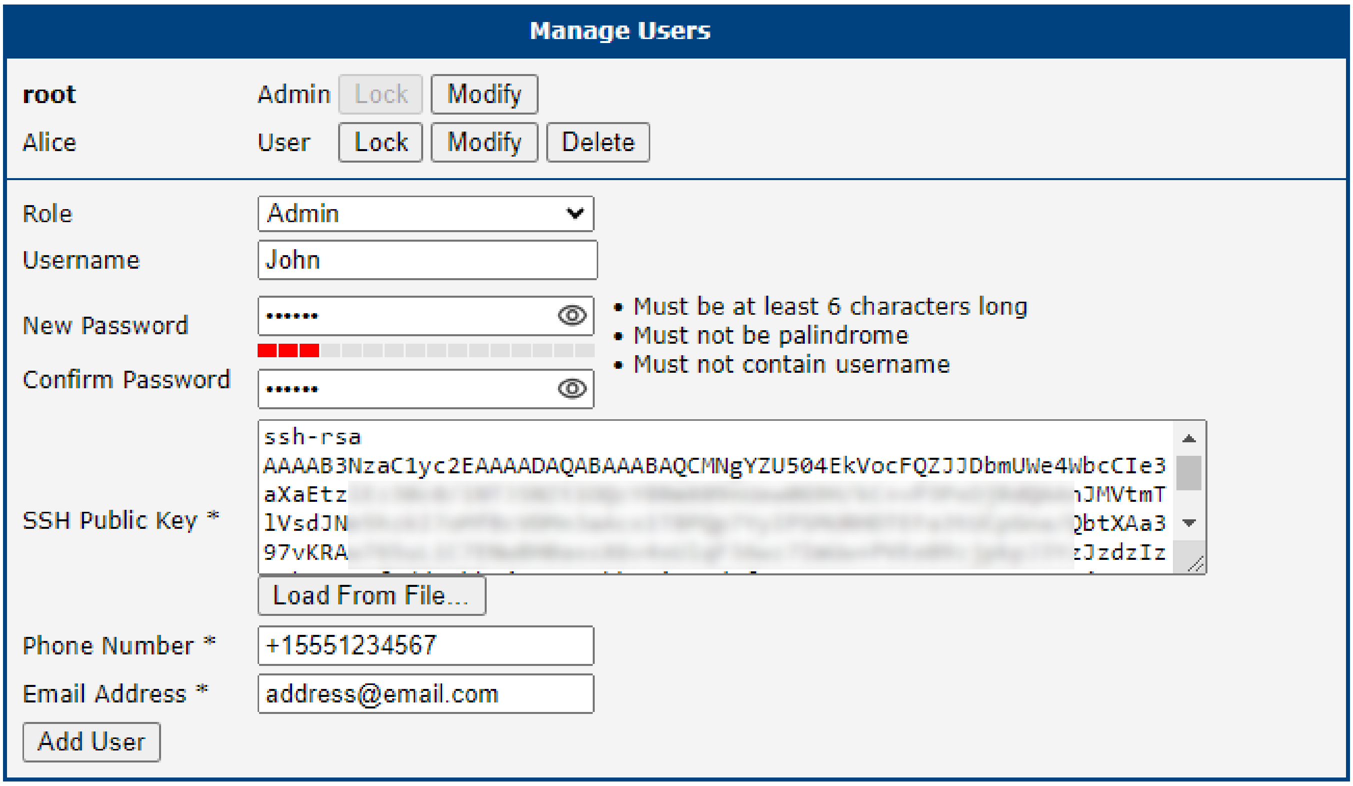
Warning

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, see Chapter *3.19.1 Authentication*.

The *Manage Users* page is the central hub for creating, modifying, and deleting user accounts on the router. In Figure 102, 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

root	Admin	Lock	Modify	
Alice	User	Lock	Modify	Delete

Role	Admin
Username	John
New Password	••••••
Confirm Password	••••••
SSH Public Key *	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCMNgYZU504EkVocFQZJJDbmUWe4WbcCIe3 aXaEtz[redacted]nJMVtmT lVsdJN[redacted]QbtXAa3 97vKRA[redacted]zJzdzIz Load From File...
Phone Number *	+15551234567
Email Address *	address@email.com

- Must be at least 6 characters long
- Must not be palindrome
- Must not contain username

Add User

Figure 102: Manage Users configuration page

User Roles and Permissions

The router supports two distinct 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.

5.1.2 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.
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 Chapter *5.2 Modify User*.
Delete	Permanently removes the user account from the router.

Table 97: User action buttons

To create a new account, fill out the form, as shown in Figure 102 for a new user `John` , and click the *Add User* button.

Item	Description
Role	Assigns the user role, either *Admin* or *User*.
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 Chapter *3.19.1 Authentication*). When changing a password for an existing user, the new password is checked against the most recent old password and must meet the following **additional requirements**: • **Character Difference:** The new password must differ from the old one by a minimum number of characters: ◦ At least **1** new or different character for the *Very Weak* and *Weak* levels. ◦ At least **5** new or different characters for the *Good* and *Strong* levels. • **No Trivial Variations:** The new password cannot be a simple variation of the old one. Specifically, the following are not allowed: ◦ Changing only the case of letters. ◦ Cyclically shifting the characters.
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. See *5.1.4 Passwordless Console Login via SSH Key* 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, as detailed in Chapter *3.17.6 SMTP*.

Table 98: New user parameters

5.1.3 Two-Factor Authentication (2FA)

Two-Factor Authentication adds a critical layer of security by requiring a time-sensitive verification code from an authenticator app in addition to a password.

> **Important**
>
> - **Correct Time is Crucial:** 2FA is time-based. Ensure the router's clock is always accurate by enabling the NTP client. See Chapter *3.17.5 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 login for that user.

Configuration Steps

1. **Enable 2FA Service Globally:** Go to *Configuration* → *System* → *Authentication* and enable either *Google Authenticator* or *OATH* as the 2FA login service; refer to Chapter *3.19.1 Authentication*. This selects the type of 2FA service, which is common for all users on the router. However, for 2FA login to be applied to a specific user, that user must set up their *Secret Key* as described in the next step.

2. **Generate and Save Secret Key:** The *Secret Key* must be configured by each user individually after logging in to the router. A user with the *Admin* role can only delete another user's *Secret Key* but cannot generate or edit it. On the *Modify User* page, in the *Two-Factor Auth* section, select *Generate a new secret key*, click the *Apply* button, and the key will be generated. You can also upload a key from a file containing the pure text of the key. Ensure the key length is sufficient (for example, 26 characters) and do not forget to click the *Apply* button once the key file is chosen.

3. **Link to Authenticator App:** Open your authenticator app (e.g., *Google Authenticator*, *Authy*) and add a new account by scanning the QR code shown in the *Two-Factor Auth* section or by manually inputting the secret code, which can be revealed by clicking the *Show* button.

Login Procedure

With 2FA enabled, the login process has an extra step:

- **Web Interface:** After entering your username and password, you will be prompted for a *Verification Code*. Open your authenticator app to get the current code and enter it to complete the login.

- **Console Access:** The console will prompt you for your username, password, and verification code sequentially.

5.1.4 Passwordless Console Login via SSH Key

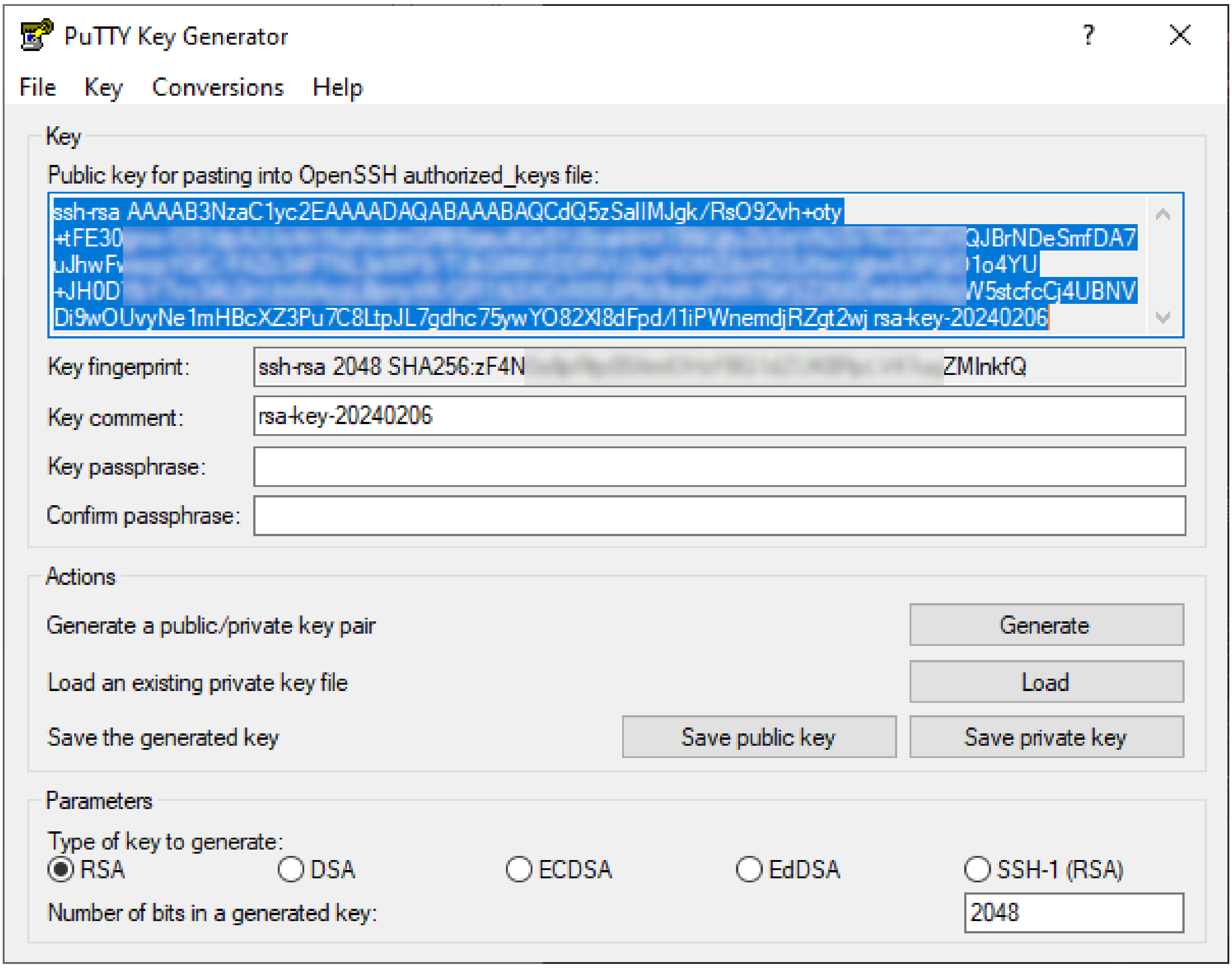
This method allows you to log in to the router’s SSH console using a cryptographic key pair instead of a password. The following guide uses the PuTTY client for Windows.

Prerequisites

From the official *PuTTY download page*, download `putty.exe` (the terminal client), `puttygen.exe` (the key generator), and `pageant.exe` (an authentication agent).

Generating the Key Pair

1. Run `puttygen.exe`.
2. Ensure *RSA* is selected as the key type and click *Generate*.
3. Move your mouse randomly over the blank area to generate randomness for the key.
4. Once complete, click *Save public key* and *Save private key*. Save them to a secure location on your computer. Do not use a passphrase for simplicity in this guide.
5. Keep the PuTTY Key Generator window open.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCdQ5zSalIMJgk/RsO92vh+oty
+tFE30[redacted]QJBrNDeSmfDA7
uJhwF[redacted]1o4YU
+JH0D[redacted]W5stcfcCj4UBNV
Di9wOUvyNe1mHBcXZ3Pu7C8LtpJL7gdhc75ywYO82Xl8dFpd/l1iPWnemdjRZgt2wj rsa-key-20240206
```

Key fingerprint: ssh-rsa 2048 SHA256:zF4N[redacted]ZMInkfQ

Key comment: rsa-key-20240206

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 103: Generating an RSA key pair with PuTTYgen

Uploading the Public Key to the Router

1. In the PuTTY Key Generator window, copy the entire text from the box labeled *Public key for pasting into OpenSSH authorized_keys file*.
2. In the router's web interface, navigate to *Administration* → *Manage Users* and click *Modify* for the desired *Admin*-level user.
3. Paste the copied key into the *Public key* field and click *Apply*.

> **Warning**
>
> The key must be in the correct one-line format, typically starting with `ssh-rsa` . Copying the key directly from the `.pub` file may not work. It is safest to copy it from the PuTTYgen window.

Configuring the PuTTY Session

1. Run `putty.exe`.
2. In the *Session* category, enter the router's IP address.
3. Navigate to *Connection* → *Data* and enter the username in the *Auto-login username* field.
4. Navigate to *Connection* → *SSH* → *Auth* → *Credentials* and browse for your saved private key file.
5. Return to the *Session* category, give the session a name, and click *Save*.

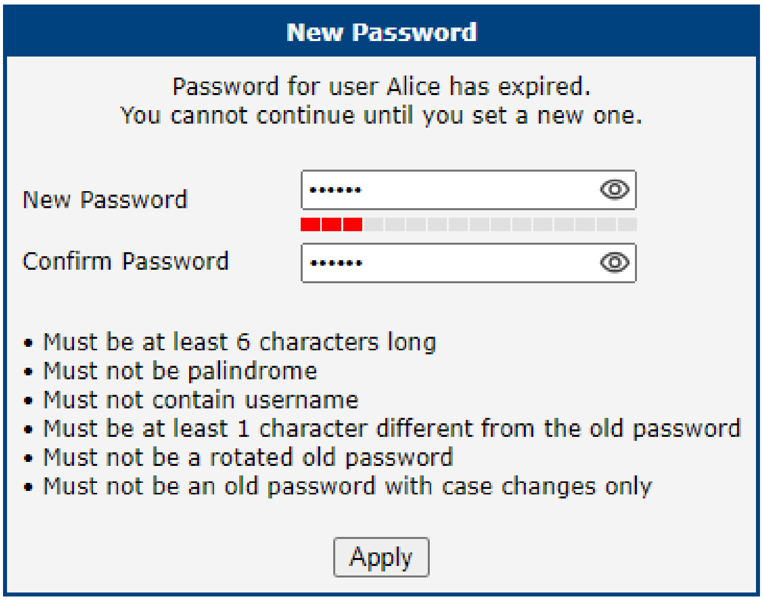
To connect, simply load the saved session and click *Open*. You will be logged in automatically without a password prompt.

5.1.5 Forced Password Change

In certain situations, the router will require a user to change their password immediately upon the next login. This occurs:

- When logging in for the very first time after a factory reset.
- When a user's password has expired (configured in *Authentication* settings).
- When an administrator has manually changed another user's password.

The new password must adhere to the complexity requirements configured on the *Configuration* → *System* → *Authentication* page.



New Password

Password for user Alice has expired.
You cannot continue until you set a new one.

New Password: ••••••

Confirm Password: ••••••

- Must be at least 6 characters long
- Must not be palindrome
- Must not contain username
- Must be at least 1 character different from the old password
- Must not be a rotated old password
- Must not be an old password with case changes only

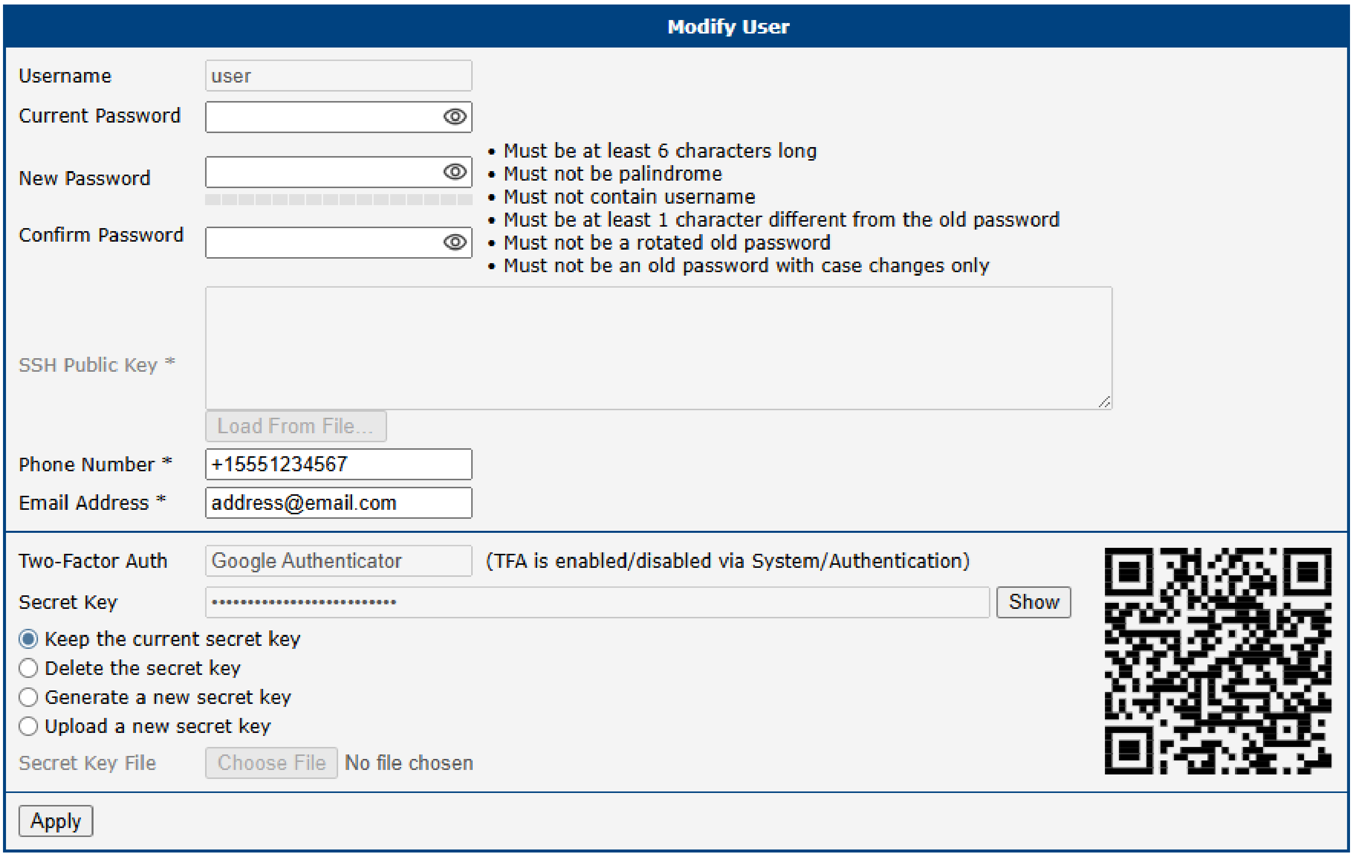
Figure 104: Forced password change prompt

5.2 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 Chapter *5.1 Manage Users*.
Figure 105 shows an example of the *Administration* → *Modify User* configuration page, illustrating a case where a user with the *User* role is logged in to the router and does not have access to the *Administration* → *Manage Users* configuration page.



Modify User

Username	user
Current Password	
New Password	
Confirm Password	
SSH Public Key *	
Phone Number *	+15551234567
Email Address *	address@email.com

- Must be at least 6 characters long
- Must not be palindrome
- Must not contain username
- Must be at least 1 character different from the old password
- Must not be a rotated old password
- Must not be an old password with case changes only

Two-Factor Auth	Google Authenticator (TFA is enabled/disabled via System/Authentication)
Secret Key	••••••••••••••••••••••••••

● Keep the current secret key
○ Delete the secret key
○ Generate a new secret key
○ Upload a new secret key

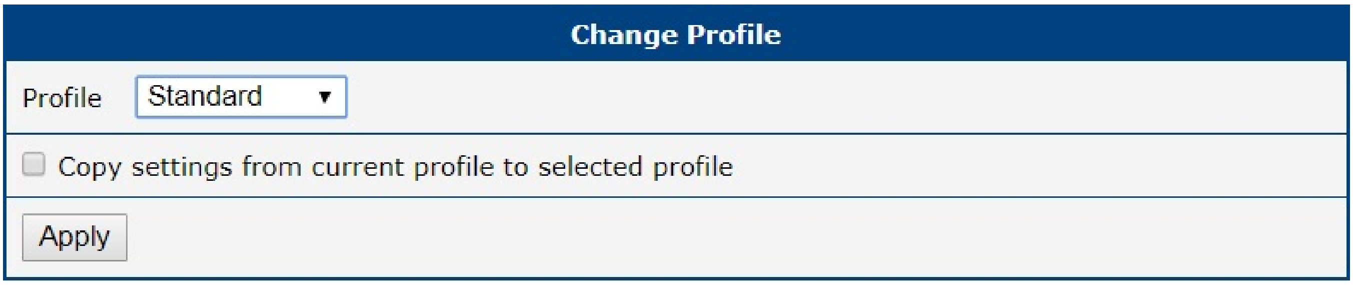
Secret Key File: No file chosen

Figure 105: Modify User configuration page

Most items in Figure 105 are already described in Chapter *5.1 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 Chapter *5.1.3 Two-Factor Authentication (2FA)*.

5.3 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

Profile: Standard

□ Copy settings from current profile to selected profile

Figure 106: Change profile page

Managing Profiles

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 in the dropdown menu above. The router will **not** switch to this profile; it only saves the settings.

Table 99: Profile management options

Warning

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

Methods for Switching Profiles

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* → *Sevices* → *SMS* page.

5.4 Set Date and Time

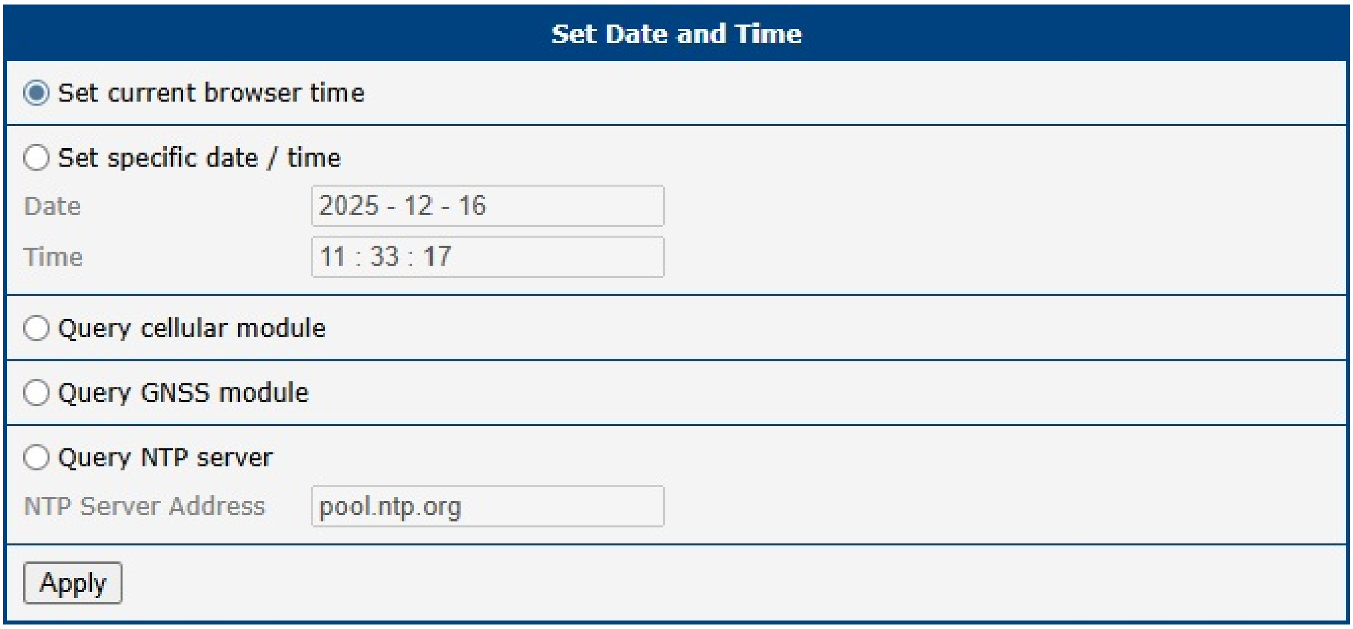
Warning

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 Chapter *3.17.5 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

● Set current browser time

○ Set specific date / time

Date: 2025 - 12 - 16

Time: 11 : 33 : 17

○ Query cellular module

○ Query GNSS module

○ Query NTP server

NTP Server Address: pool.ntp.org

Figure 107: Set date and time page

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.

5.5 Manage SIM

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

5.5.1 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 use the card. This page allows you to permanently remove the PIN protection from the SIM card.

To remove the PIN, navigate to *Administration* → *Manage SIM* → *Unlock SIM*, enter the correct 4–8 digit PIN into the *SIM PIN* field, and click *Apply*. This action targets the currently active SIM card. If no SIM is active, the operation will be applied to the first SIM card.

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 chapter.

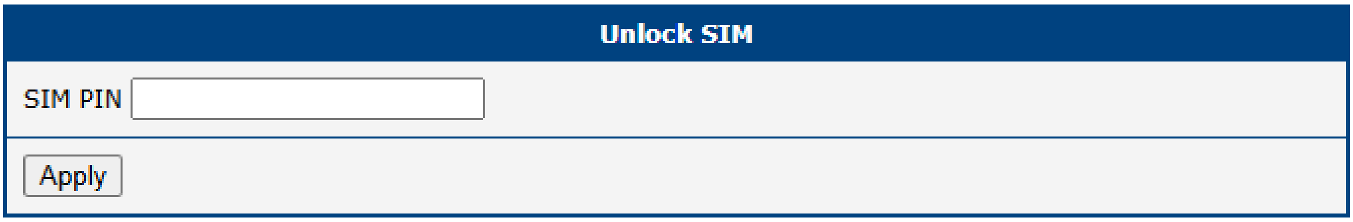


Figure 108: Unlock SIM page

5.5.2 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 change the PIN.

To unblock the card, go to the *Administration* → *Manage SIM* → *Unblock SIM* page. Enter the PUK (Personal Unblocking Key) code provided by your carrier into the *SIM PUK* field and your desired new PIN into the *New SIM PIN* field. Click *Apply* to confirm. The operation is applied to the currently active SIM card or the first SIM if none is active.

Warning

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

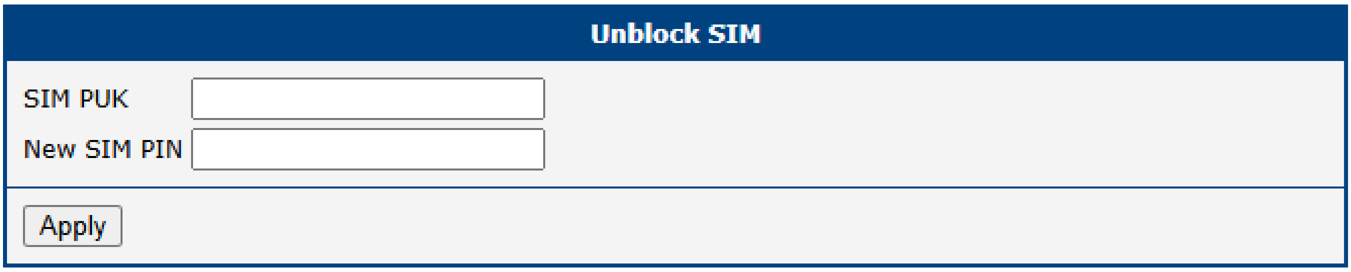


Figure 109: Unblock SIM page

5.5.3 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 (see Chapter *2.2 Mobile WAN*).

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`).

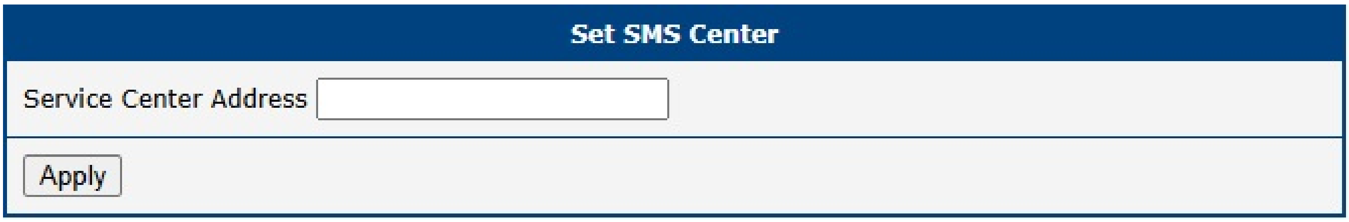


Figure 110: Set SMS service center page

5.6 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.

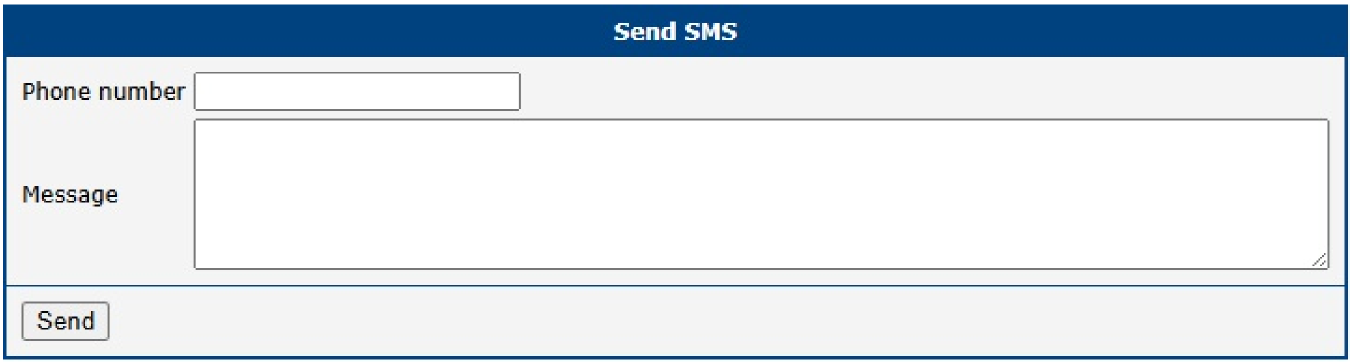
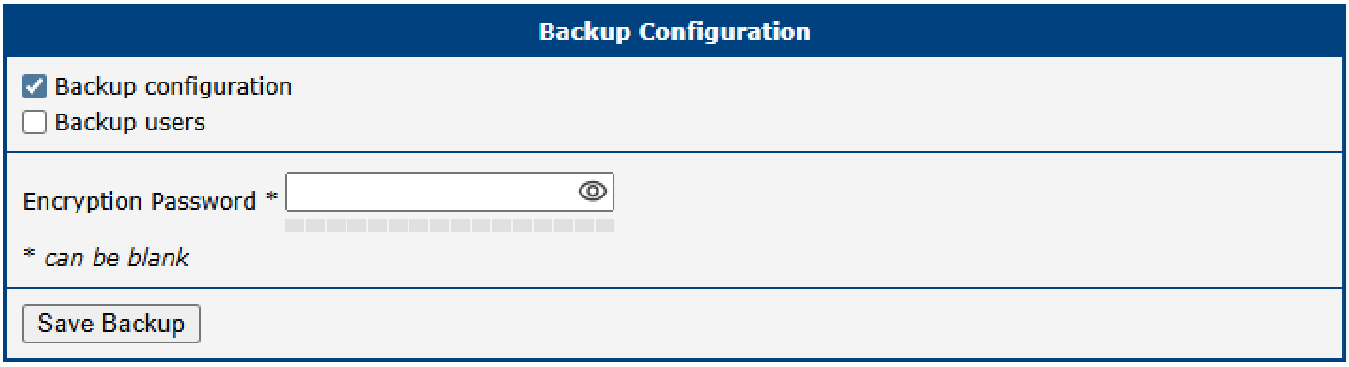


Figure 111: Send SMS dialog

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

5.7 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

☑ Backup configuration
☐ Backup users

Encryption Password *

** can be blank*

Figure 112: Backup configuration page

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.

Table 100: Backup configuration items

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 Chapter *5.8 Restore Configuration*.

5.8 Restore Configuration

This page allows you to restore the router's settings from a previously created backup file. For instructions on creating a backup, please see Chapter 5.7.
To restore a configuration, navigate to the *Administration* → *Restore Configuration* page. 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.

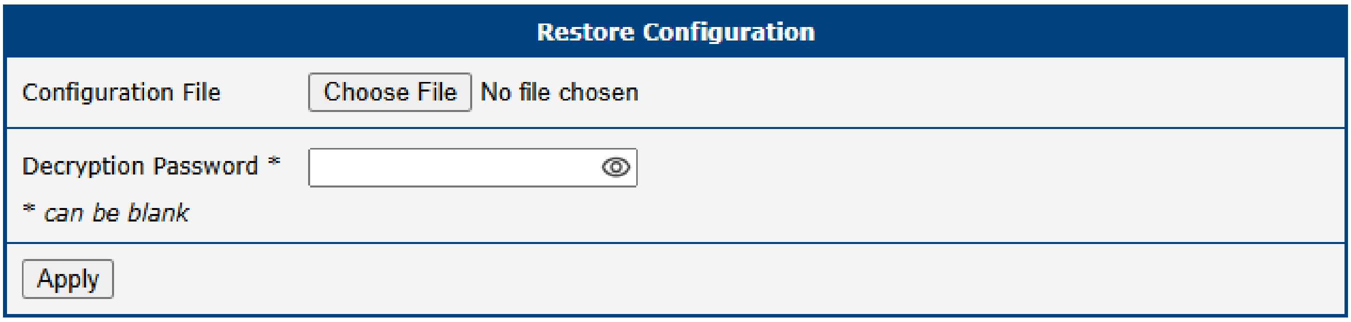


Figure 113: Restore configuration page

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.

Table 101: Restore configuration options

5.9 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.

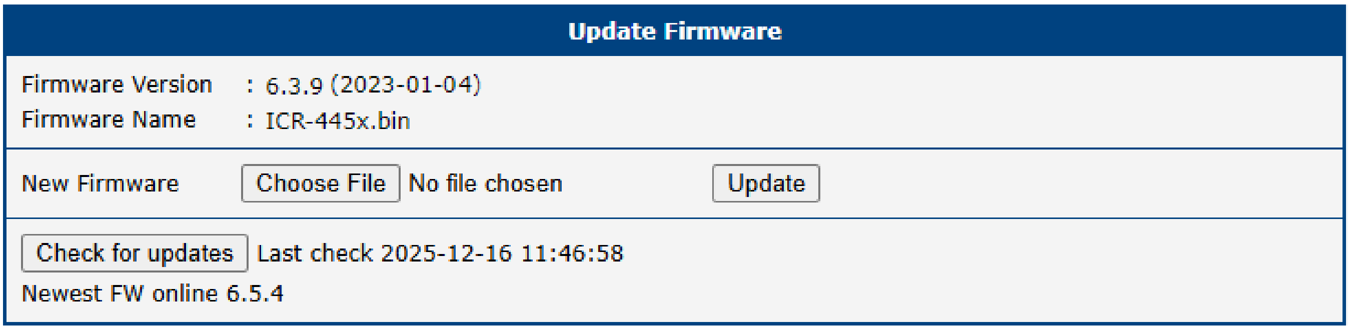
Info

The latest official firmware for your router is always available on the Advantech Engineering Portal at *icr.advantech.com/download/routers-firmware*.

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

Firmware Version : 6.3.9 (2023-01-04)
Firmware Name : ICR-445x.bin

New Firmware No file chosen

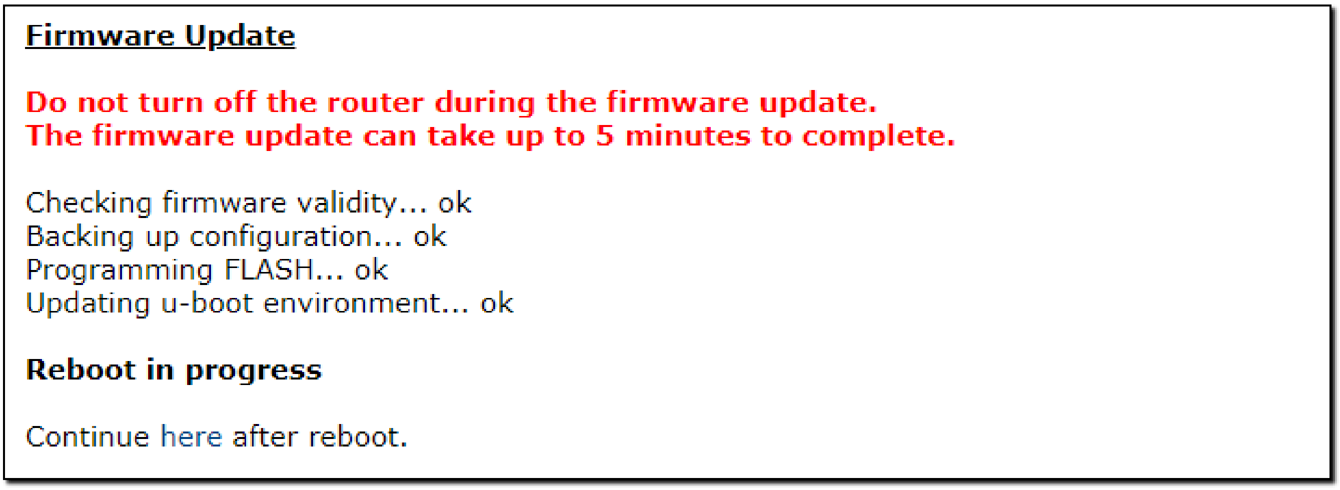
Last check 2025-12-16 11:46:58
Newest FW online 6.5.4

Figure 114: Update firmware administration page

Item	Description
Current Version	
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.
Manual Update	
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.
Online Update	
Check for updates	Connects to the public server to check if a newer firmware version is available. 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.

Table 102: Update firmware page items

During the update, the router will display its progress, as shown in Figure 115. 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.



Firmware Update

Do not turn off the router during the firmware update.
The firmware update can take up to 5 minutes to complete.

Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... ok
Updating u-boot environment... ok

Reboot in progress

Continue here after reboot.

Figure 115: Firmware update in progress

5.10 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, this 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.

5.10.1 Reboot Now

This submenu allows you to immediately reboot the router by clicking the *Reboot* button.

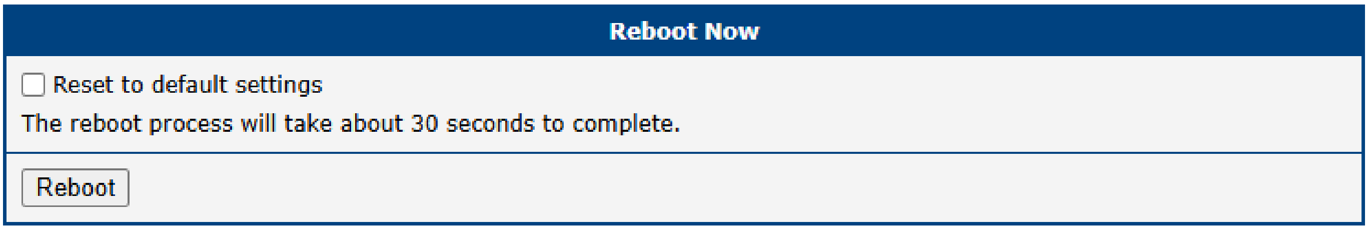
Warning

Caution: Factory Reset Option
Before rebooting, you have the option to select *Reset to default settings*. This 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 Chapter *1.3.2 Reset Procedures*.

A standard reboot takes approximately 30 seconds to complete.



□ Reset to default settings

The reboot process will take about 30 seconds to complete.

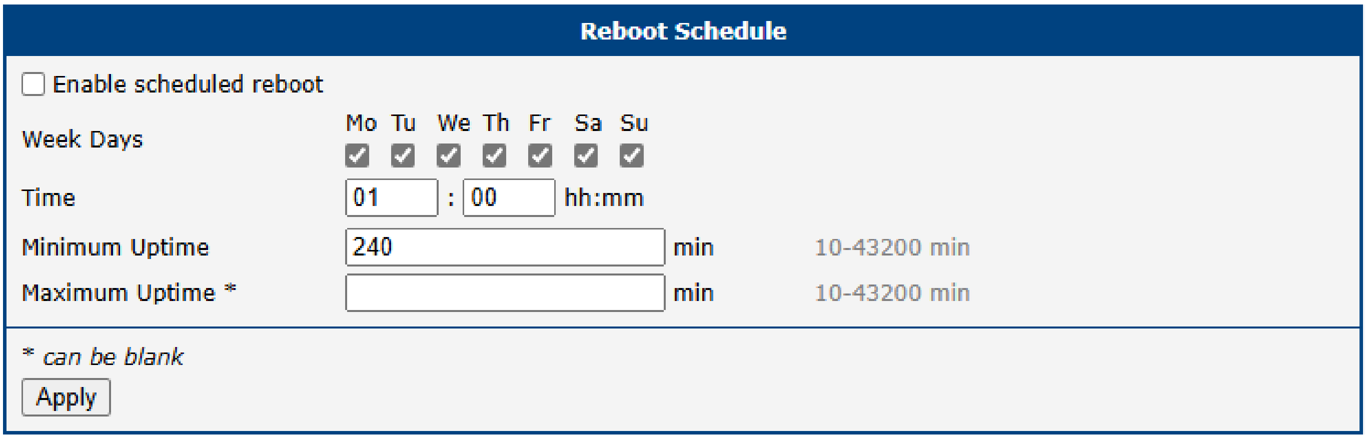
Figure 116: Reboot Now Submenu

5.10.2 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 scheduled reboot. Multiple days can be selected.
Time	Set the exact time for the reboot to occur on chosen days (format: hh:mm).
Minimum Uptime	The minimum amount of time the router must be running before a scheduled reboot is permitted. This setting 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).

Table 103: Reboot schedule configuration items description



Reboot Schedule

☐ Enable scheduled reboot

Week Days	Mo ☑	Tu ☑	We ☑	Th ☑	Fr ☑	Sa ☑	Su ☑		
Time	01 : 00	hh:mm							
Minimum Uptime	240	min	10-43200 min						
Maximum Uptime *		min	10-43200 min						

* *can be blank*

Apply

Figure 117: Reboot schedule submenu

5.11 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.

6. 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.

6.1 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. For this configuration, a SIM card with an active data plan from a mobile network operator is required. The router is designed for a straightforward setup and will often connect to the mobile network automatically without any initial software configuration.

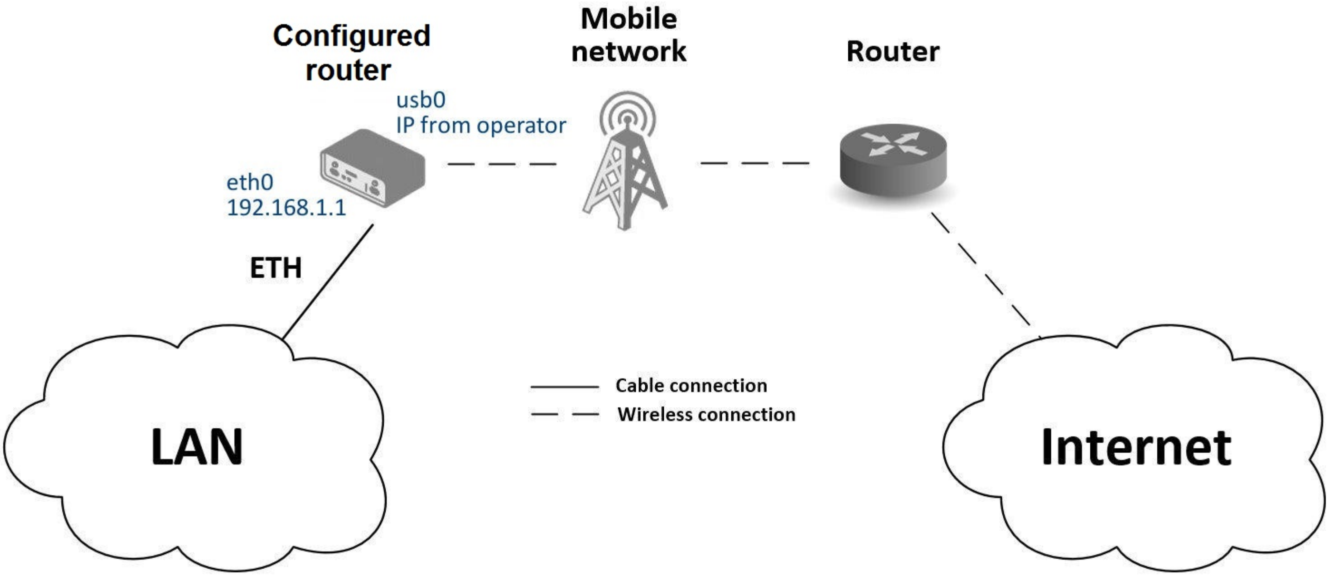


Figure 118: Access to the internet from LAN: a topology example

Initial Setup

1. Insert an active SIM card into the *SIM1* slot.
2. For the router to function correctly, you must securely attach an appropriate antenna to **every** antenna connector on the device. For optimal cellular performance and signal stability, both the main (*ANT*) and diversity (*DIV*) antennas are required. If your router model includes Wi-Fi or GNSS features, 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.

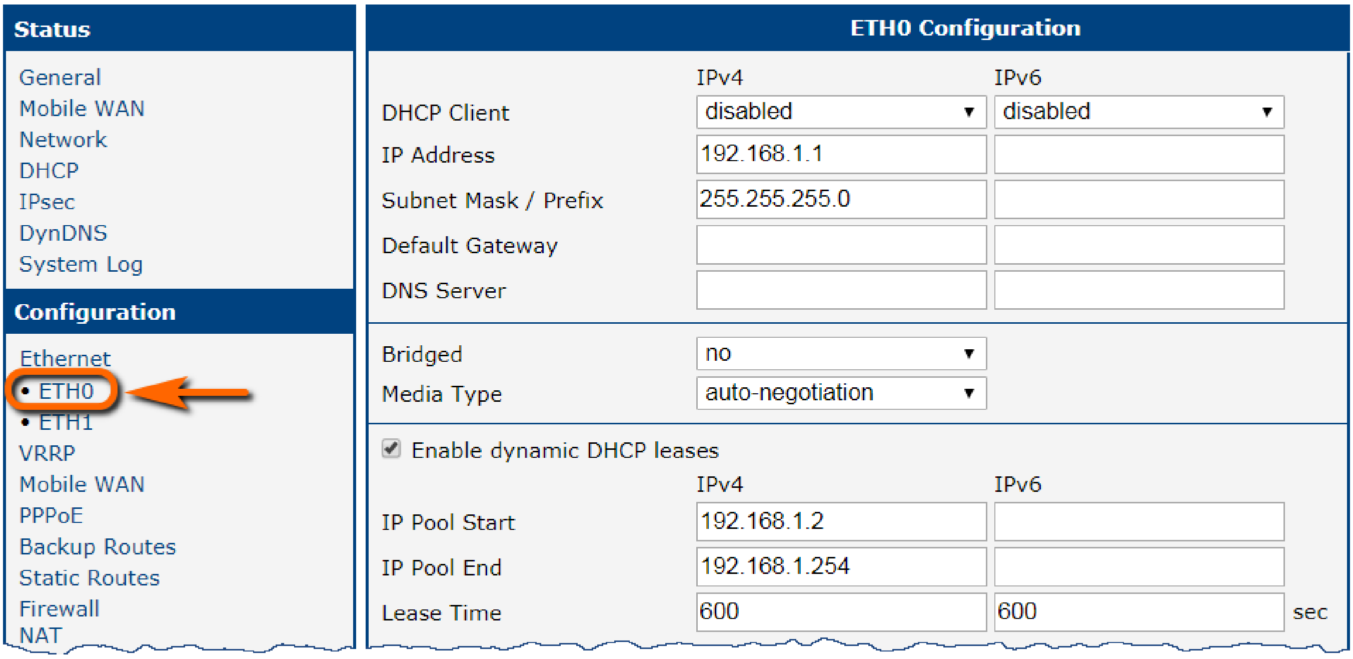
After powering on, wait for the router to register on the mobile network. A successful connection is indicated by the *WAN* and *DAT* LEDs on the front panel.

Configuration

While factory settings are often sufficient, you can review or modify the configuration in the router's web interface, accessible 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, which will automatically assign IP addresses to connected devices (e.g., the first computer will get `192.168.1.2`). No changes are needed for this use case. For more details, see Chapter 3.1.



ETH0 Configuration

	IPv4	IPv6	
DHCP Client	disabled ▼	disabled ▼	
IP Address	192.168.1.1		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway			
DNS Server			
Bridged	no ▼		
Media Type	auto-negotiation ▼		

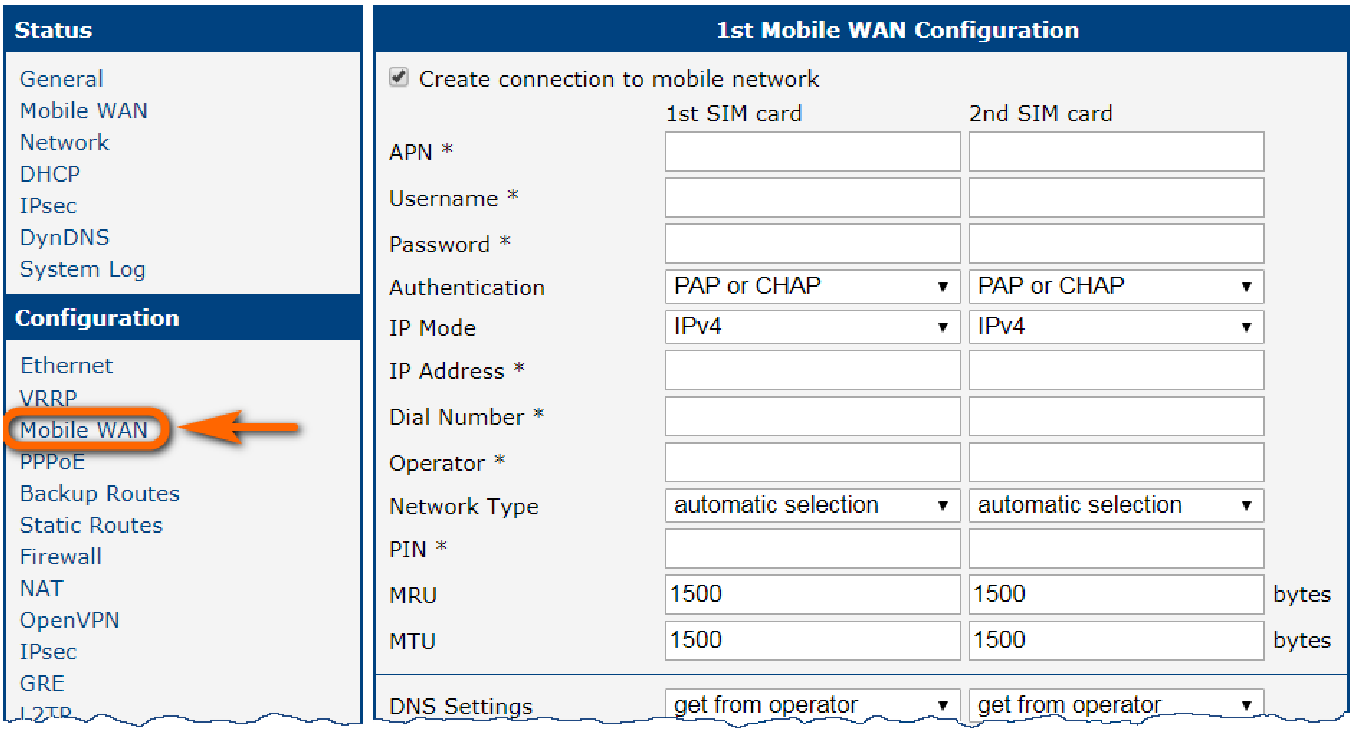
☑ Enable dynamic DHCP leases

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

Figure 119: Access to the internet from LAN: ethernet configuration

Mobile WAN Configuration

Go to the *Configuration* → *Mobile WAN* page. Ensure that the *Create connection to mobile network* option is enabled (this is the default setting). For most public SIM cards, you do not need to fill in the APN, username, or password. For more details, see Chapter 3.4.1 Connection to Mobile Network.



1st Mobile WAN Configuration

☑ Create connection to mobile network

	1st SIM card	2nd SIM card	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP ▾	PAP or CHAP ▾	
IP Mode	IPv4 ▾	IPv4 ▾	
IP Address *			
Dial Number *			
Operator *			
Network Type	automatic selection ▾	automatic selection ▾	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator ▾	get from operator ▾	

Figure 120: Access to the internet from LAN: mobile WAN configuration

Verifying Connectivity

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

6.2 Backup Access to the Internet from LAN

This use case demonstrates how to configure connection redundancy by setting up multiple Internet sources (Ethernet WAN, Wi-Fi, and Cellular) and defining their priority. The router will automatically switch to a lower-priority connection if a higher-priority one fails, ensuring continuous Internet access for the LAN. This is managed through the *Backup Routes* feature.

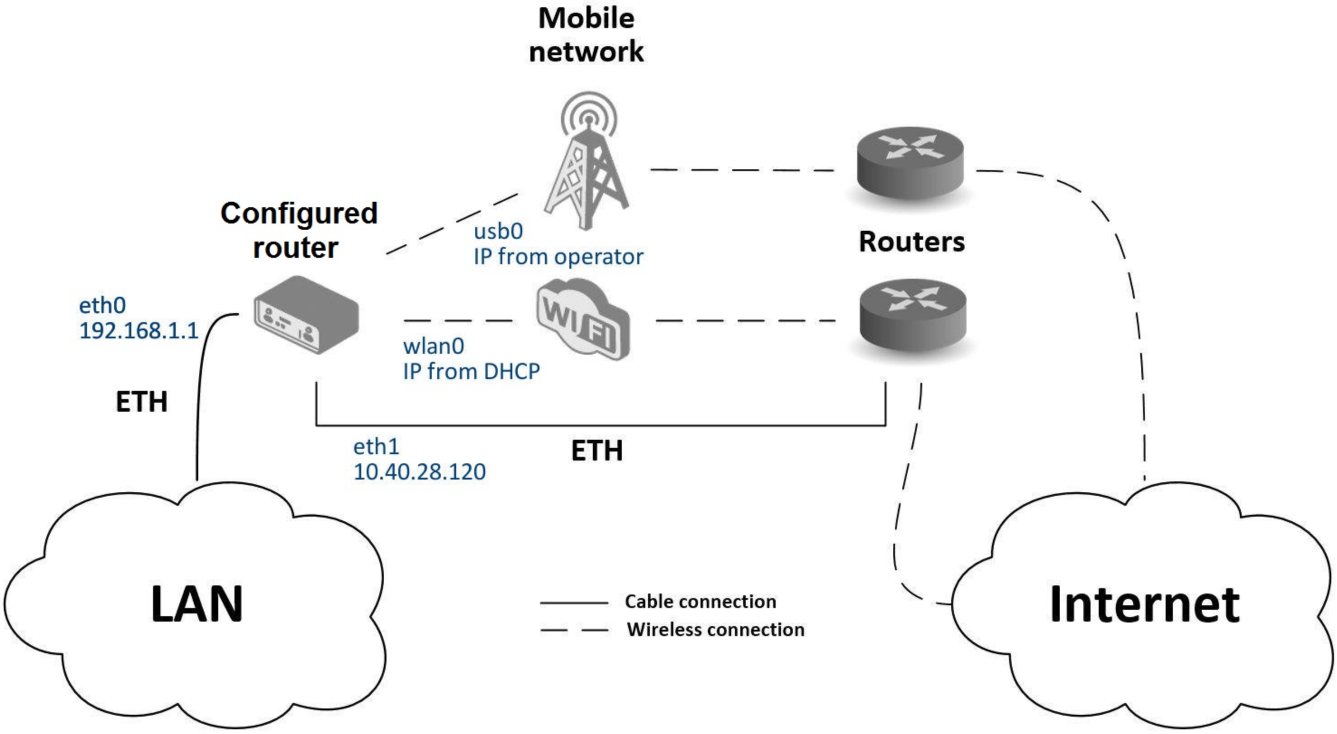


Figure 121: Backup access to the internet: a topology example

Interface Configuration

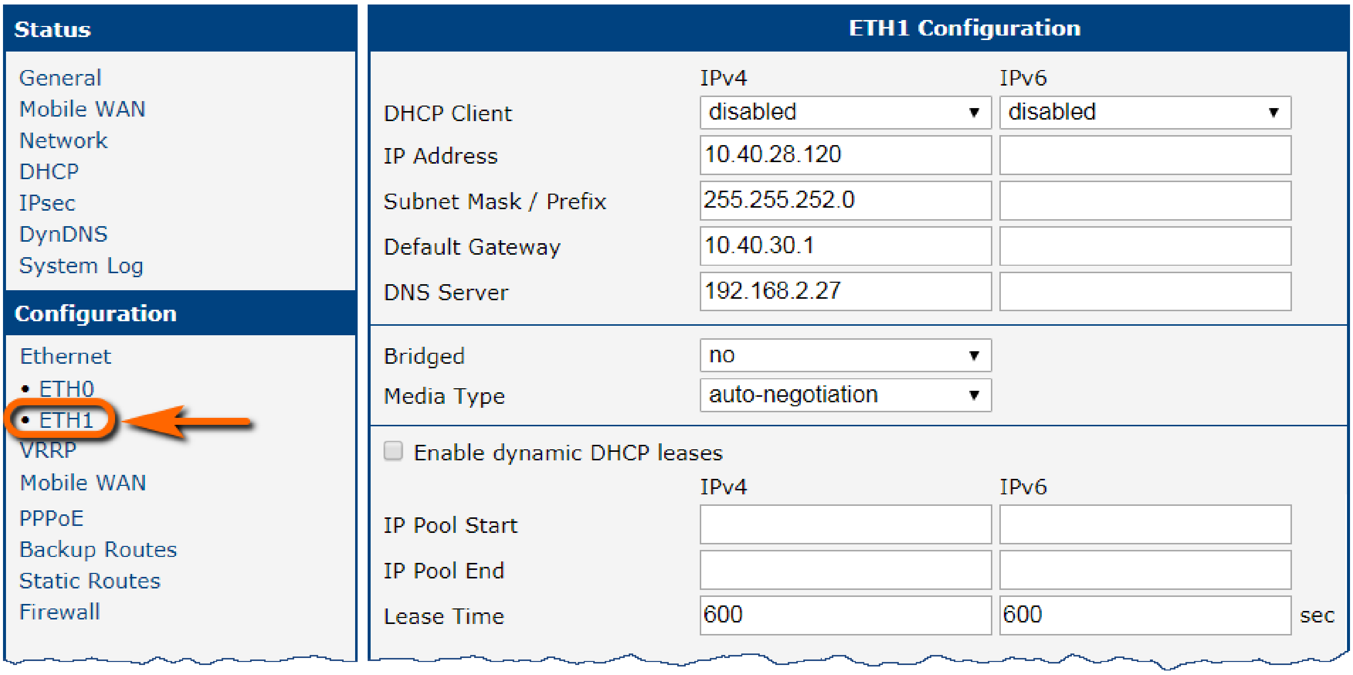
The first step is to configure each interface that will serve as an Internet source. The LAN interface (`ETH0`) can be left with its default settings as in the previous use case.

Ethernet WAN Configuration

The ETH1 port will be 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 the *Apply* button to save the changes.

For more details on Ethernet settings, see Chapter 3.1.



ETH1 Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	10.40.28.120	
Subnet Mask / Prefix	255.255.252.0	
Default Gateway	10.40.30.1	
DNS Server	192.168.2.27	

Bridged	no
Media Type	auto-negotiation

□ Enable dynamic DHCP leases

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

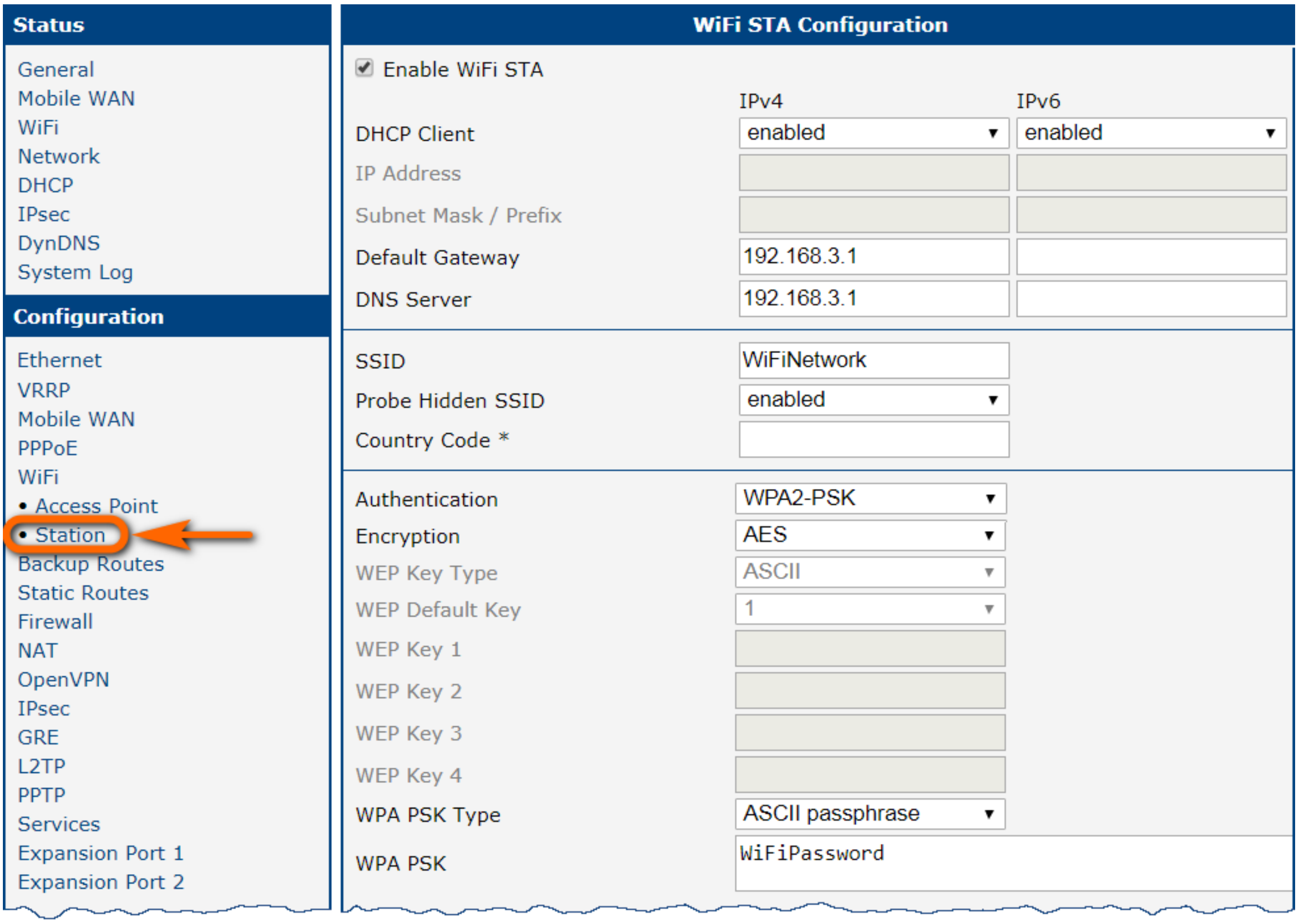
Figure 122: Backup access to the internet: ethernet configuration

Wi-Fi WAN Configuration

To use Wi-Fi as a backup connection, configure the router to act 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 will show the status `wpa_state=COMPLETED`. For more details, see Chapter 3.6.2.



WiFi STA Configuration

☑ Enable WiFi STA

	IPv4	IPv6
DHCP Client	enabled ▾	enabled ▾
IP Address		
Subnet Mask / Prefix		
Default Gateway	192.168.3.1	
DNS Server	192.168.3.1	

SSID	WiFiNetwork
Probe Hidden SSID	enabled ▾
Country Code *	

Authentication	WPA2-PSK ▾
Encryption	AES ▾
WEP Key Type	ASCII ▾
WEP Default Key	1 ▾
WEP Key 1	
WEP Key 2	
WEP Key 3	
WEP Key 4	
WPA PSK Type	ASCII passphrase ▾
WPA PSK	WiFiPassword

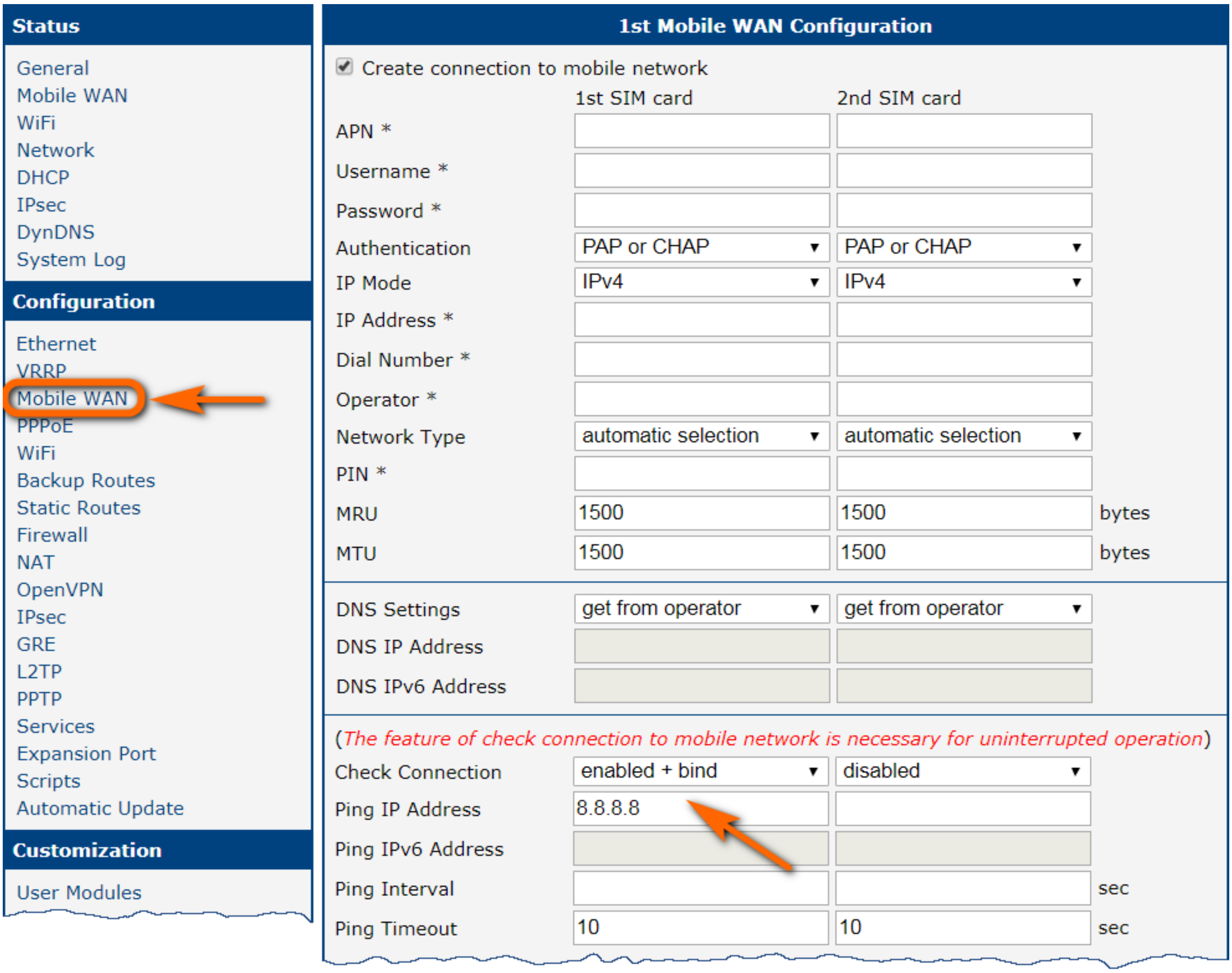
Figure 123: Backup access to the internet: wi-fi configuration

Mobile WAN Configuration

The cellular connection will serve as the final backup. For basic setup, insert an active SIM card into the *SIM1* slot and attach the cellular antenna. To integrate it into the backup system, connection monitoring must be enabled.

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

This allows the router to detect when the cellular connection is active. For detailed settings, see Chapter 3.4.1 Connection to Mobile Network.



1st Mobile WAN Configuration

☑ Create connection to mobile network

	1st SIM card	2nd SIM card	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP	PAP or CHAP	
IP Mode	IPv4	IPv4	
IP Address *			
Dial Number *			
Operator *			
Network Type	automatic selection	automatic selection	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator	get from operator	
DNS IP Address			
DNS IPv6 Address			

(*The feature of check connection to mobile network is necessary for uninterrupted operation*)

Check Connection	enabled + bind	disabled	
Ping IP Address	8.8.8.8		
Ping IPv6 Address			
Ping Interval			sec
Ping Timeout	10	10	sec

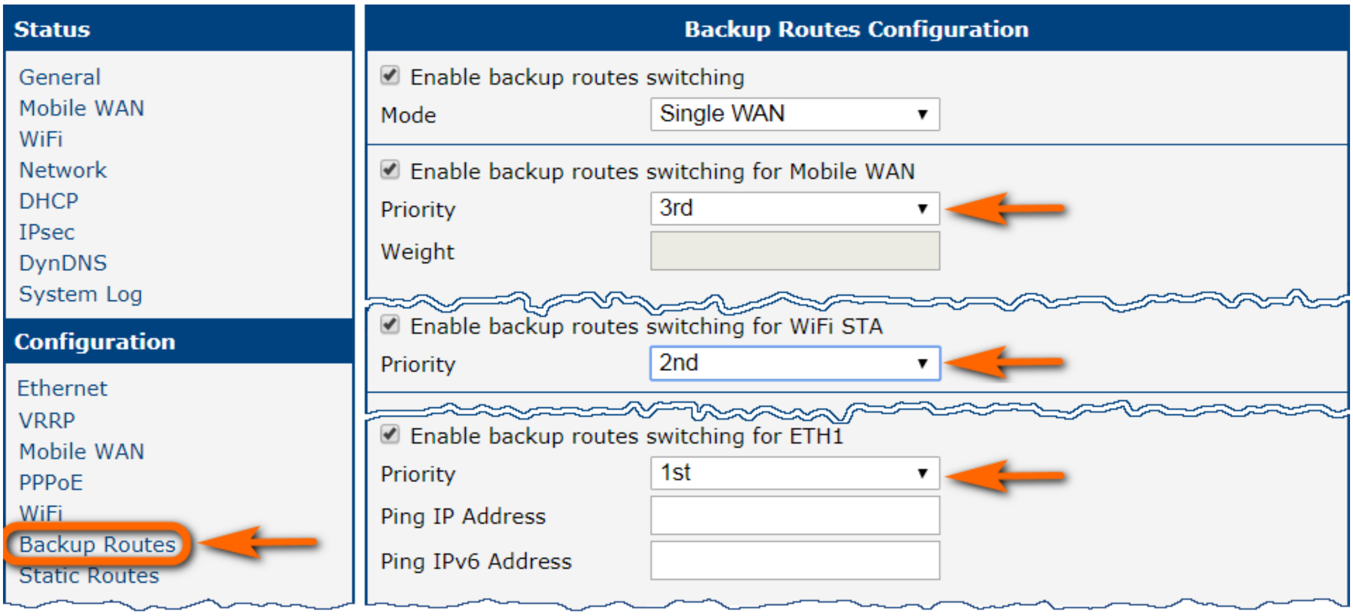
Figure 124: Backup access to the internet: mobile WAN configuration

Backup Routes Configuration

After configuring the interfaces, their priority must be set in the *Backup Routes* menu.

1. Navigate to *Configuration* → *Backup Routes*.
2. Set the priority for each WAN interface. In this example, the priority is:
   - **1 (Highest):** `eth1` (Wired Ethernet)
   - **2 (Medium):** `wlan0` (Wi-Fi)
   - **3 (Lowest):** `usb0` (Cellular)
3. For each route, check the *Enable backup routes switching* box to activate it.
4. Click *Apply* to save the configuration.

For more details, see Chapter 3.7.



Backup Routes Configuration

☑ Enable backup routes switching
Mode: Single WAN

☑ Enable backup routes switching for Mobile WAN
Priority: 3rd
Weight:

☑ Enable backup routes switching for WiFi STA
Priority: 2nd

☑ Enable backup routes switching for ETH1
Priority: 1st
Ping IP Address:
Ping IPv6 Address:

Figure 125: Backup access to the internet: backup routes configuration

Verifying Failover

You can monitor the status of all network interfaces under *Status* → *Network*. The *Route Table* at the bottom of the page will show which interface is currently active as the default route. If the primary `eth1` connection fails, the default route will automatically switch to `wlan0`. If `wlan0` also fails, it will switch to `usb0`.

6.3 Secure Network Interconnection with VPN

A Virtual Private Network (VPN) creates a secure, encrypted tunnel over an untrusted public network (like 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 data exchanged between the networks.

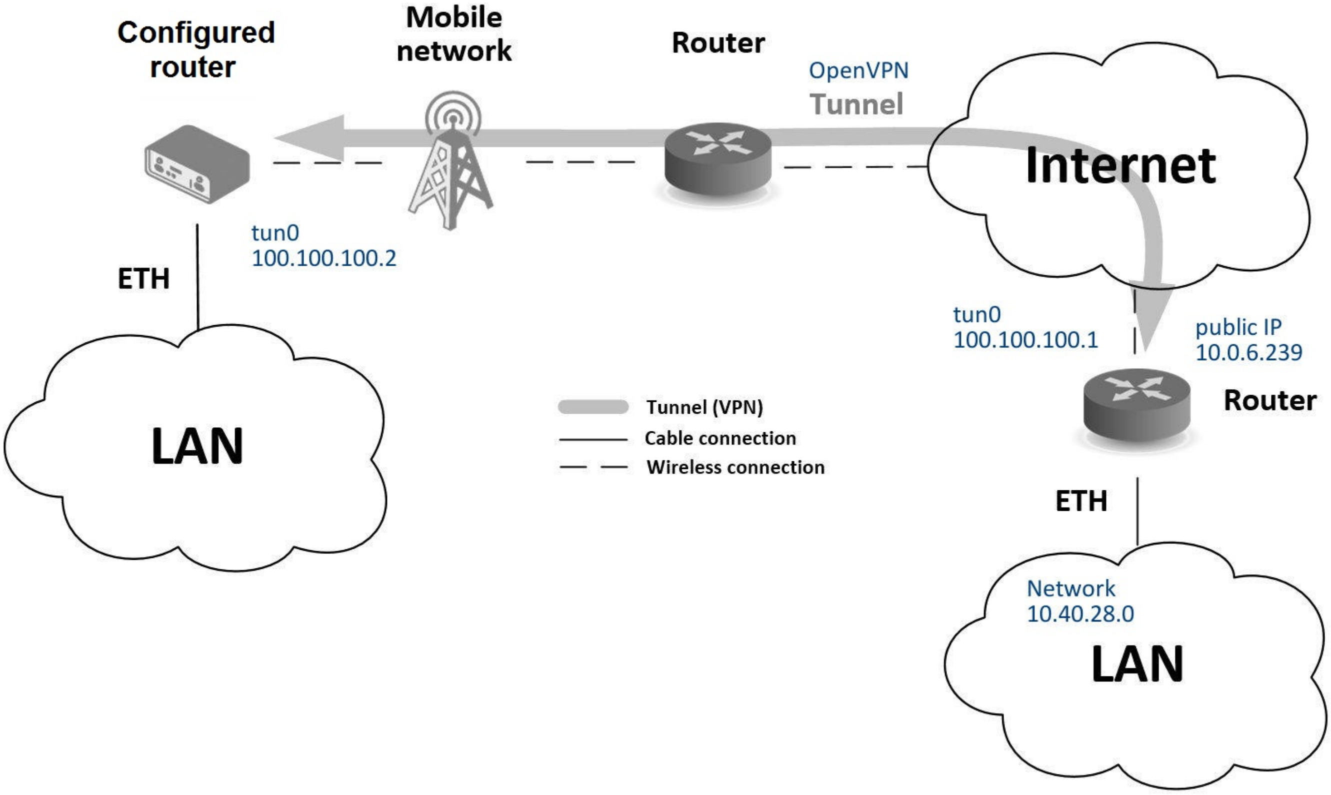


Figure 126: Secure networks interconnection: a topology example

Advantech routers support several VPN protocols, including:

- **OpenVPN:** A highly flexible and secure SSL/TLS-based VPN. See Chapter 3.11 or *OpenVPN Tunnel* [6] Application Note for details.
- **IPsec:** A standards-based framework for securing IP communications. See Chapter 3.12 or *IPsec Tunnel* [7] Application Note for details.

The router also supports non-encrypted tunneling protocols like *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

The setup involves configuring the primary Internet connection and then configuring the OpenVPN tunnel itself.

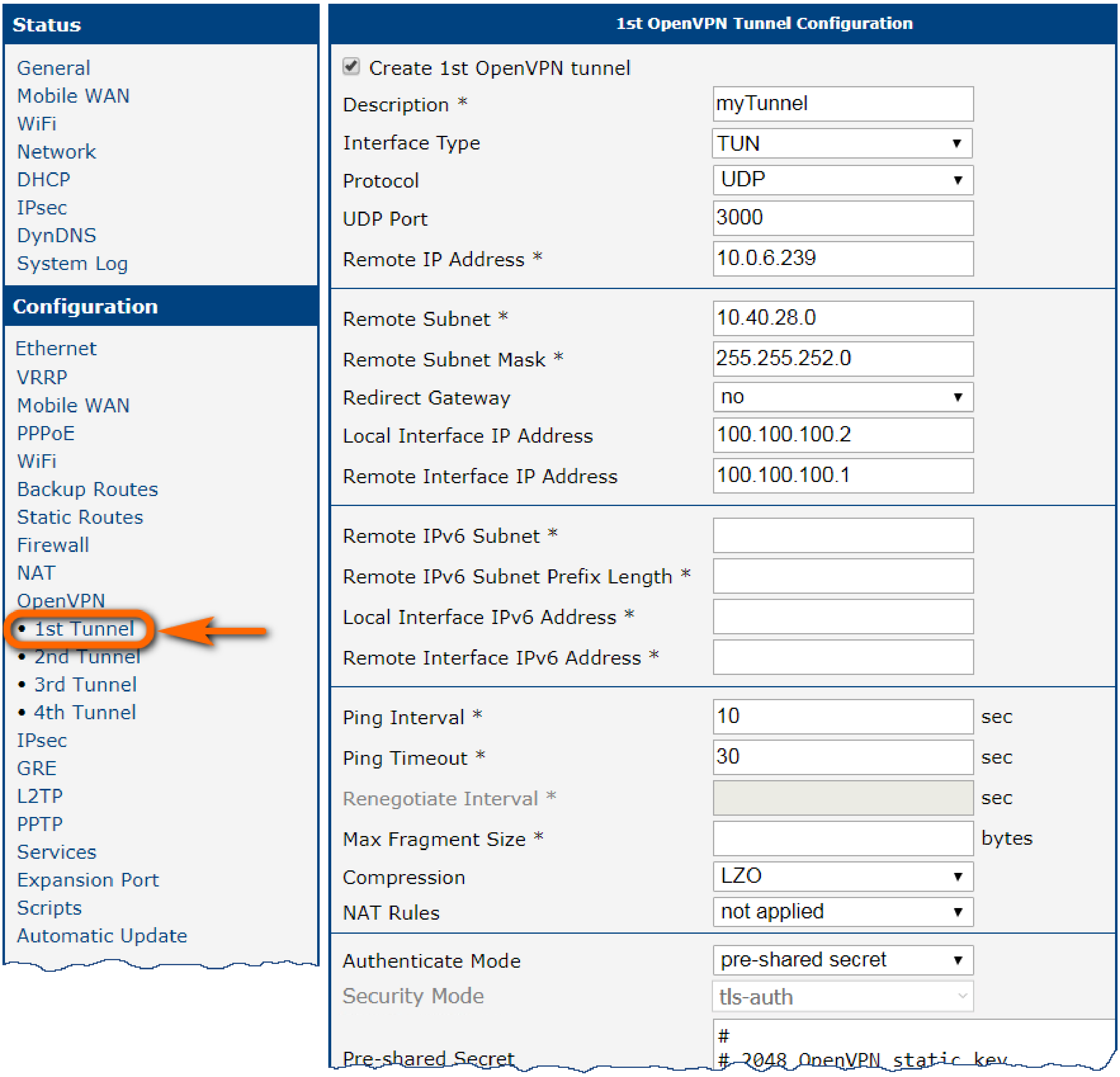
Mobile WAN Configuration

A stable Internet connection is required before establishing a VPN tunnel. As in previous examples, the cellular connection can be used as the primary WAN link. Ensure that a SIM card is inserted and an antenna is attached. The router will typically establish a connection automatically. Verify that the mobile connection is active under *Configuration* → *Mobile WAN*, as detailed in Chapter 3.4.1 Connection to Mobile Network.

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 (the OpenVPN server).
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 the *Local Interface IP Address* and *Remote Interface IP Address* fields. These must be unique and 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.

For more detailed guidance, refer to Chapter 3.11 or *OpenVPN Tunnel* [6] Application Note.



1st OpenVPN Tunnel Configuration

☑ Create 1st OpenVPN tunnel

Description *	myTunnel	
Interface Type	TUN ▾	
Protocol	UDP ▾	
UDP Port	3000	
Remote IP Address *	10.0.6.239	
Remote Subnet *	10.40.28.0	
Remote Subnet Mask *	255.255.252.0	
Redirect Gateway	no ▾	
Local Interface IP Address	100.100.100.2	
Remote Interface IP Address	100.100.100.1	
Remote IPv6 Subnet *		
Remote IPv6 Subnet Prefix Length *		
Local Interface IPv6 Address *		
Remote Interface IPv6 Address *		
Ping Interval *	10	sec
Ping Timeout *	30	sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO ▾	
NAT Rules	not applied ▾	
Authenticate Mode	pre-shared secret ▾	
Security Mode	tls-auth	
Pre-shared Secret	# # 2048 OpenVPN static key	

Figure 127: Secure network interconnection: OpenVPN configuration

Verifying Connectivity

You can confirm that the VPN tunnel is active by checking the following:

- **Network Status Page:** Go 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 a log entry stating `Initialization Sequence Completed`, which confirms that the OpenVPN tunnel has been successfully established.

Once the tunnel is active, the two networks are securely interconnected. You can verify this by pinging the remote tunnel endpoint's IP address from the router's command-line interface (accessible via SSH).

6.4 Serial Gateway

The Serial Gateway feature allows the router to encapsulate serial data into IP packets, enabling communication with serial devices (such as industrial meters, PLCs, or sensors) over an IP network. This powerful function essentially 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.

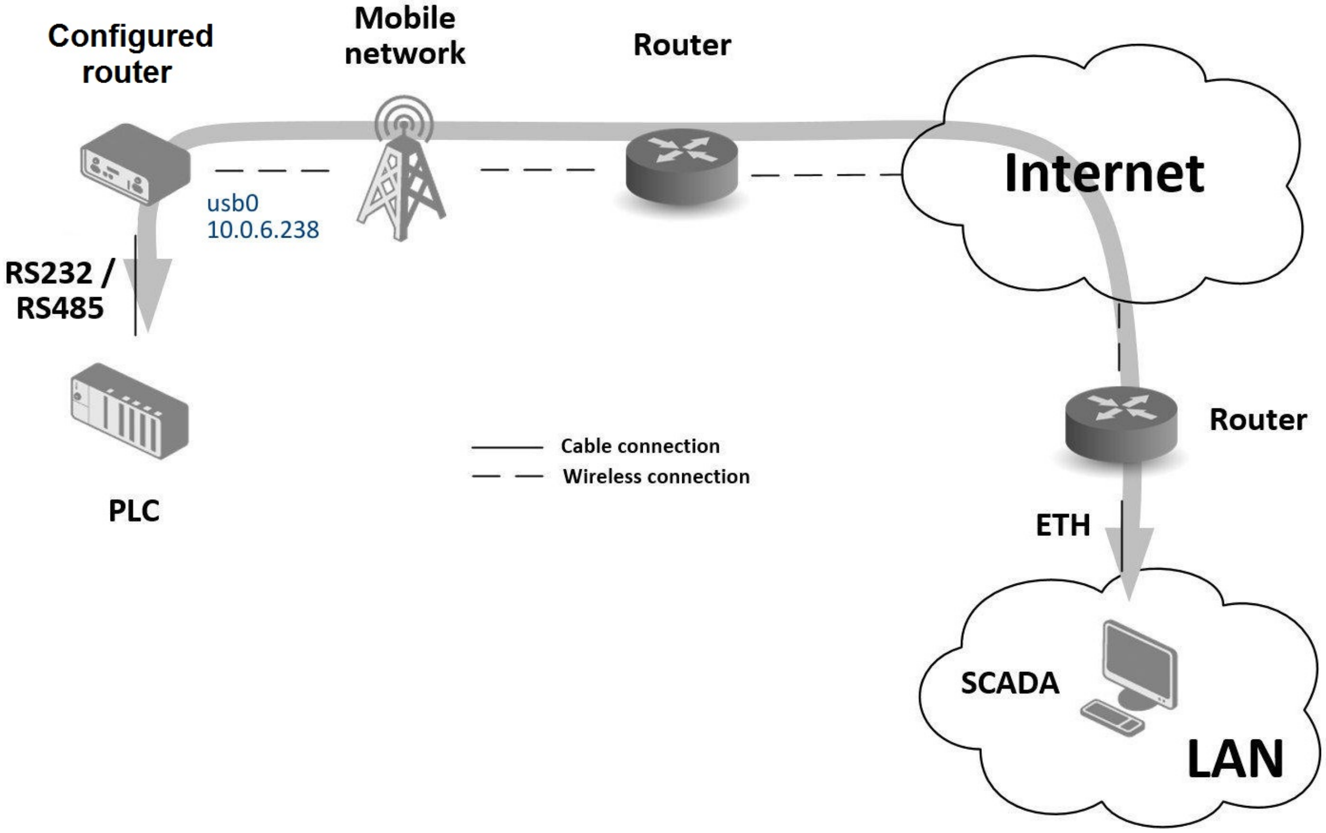


Figure 128: Serial gateway: a topology example

In this example, the router's RS232 (RS485) port is connected to a PLC, and the router is configured as a TCP server. A remote PC (SCADA) will act as a TCP client to establish a connection and communicate with the PLC.

Configuration

The setup requires configuring the router's Internet connection and then setting up the serial port for TCP/IP communication.

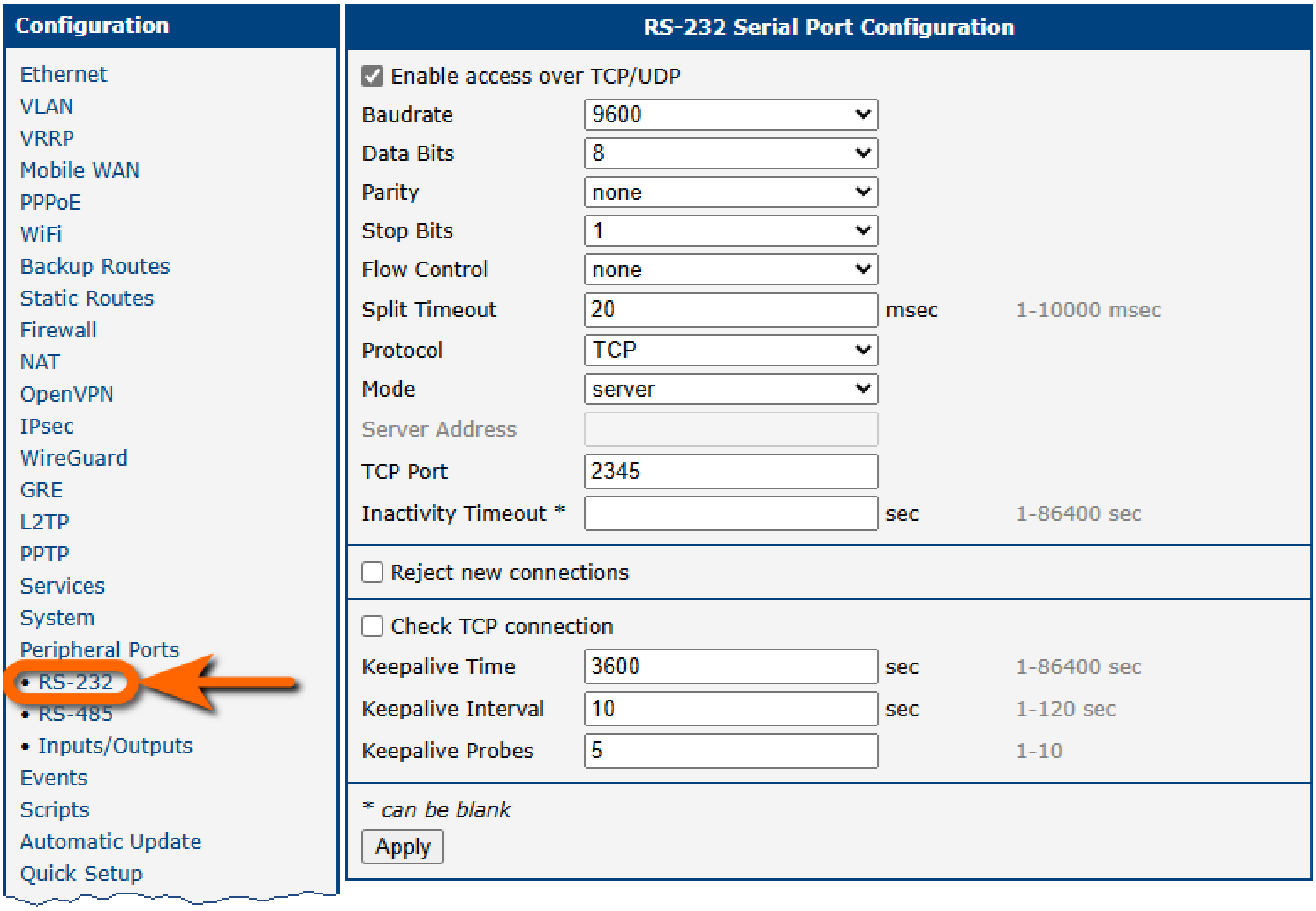
Mobile WAN Configuration

A stable Internet connection is essential. As in previous examples, the cellular connection provides the primary WAN link. Simply insert an active SIM card into the *SIM1* slot and attach the cellular antenna. The router will automatically connect to the mobile network. The public IP address assigned by the mobile operator will be used by the remote client to connect to the serial gateway. For more details, see Chapter 3.4.1 Connection to Mobile Network.

Peripheral Port (RS232) Configuration

The serial-to-IP conversion is configured on the Peripheral Port page. This example uses the RS232 port.

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



RS-232 Serial Port Configuration

☑ Enable access over TCP/UDP

Baudrate	9600		
Data Bits	8		
Parity	none		
Stop Bits	1		
Flow Control	none		
Split Timeout	20	msec	1-10000 msec
Protocol	TCP		
Mode	server		
Server Address			
TCP Port	2345		
Inactivity Timeout *		sec	1-86400 sec

□ Reject new connections

□ Check TCP connection

Keepalive Time	3600	sec	1-86400 sec
Keepalive Interval	10	sec	1-120 sec
Keepalive Probes	5		1-10

* can be blank

Figure 129: Serial gateway: peripheral port 1 configuration

Verifying Connectivity

Once configured, the remote PC (SCADA) can establish a TCP connection to the router's public IP address (e.g., `10.0.6.238` in the example) on the configured port (e.g., `2345`). All data sent from the PC over this TCP session will be forwarded to the PLC via the serial port, and vice versa.
You can monitor the connection status in the *Status* → *System Log* page. When the remote client successfully connects, a message similar to *TCP connection established* will appear in the log.

Appendix A: Open Source Software License

The software in this device includes various open-source components governed by the following licenses:

- GPL versions 2 and 3
- LGPL version 2
- BSD-style licenses
- MIT-style licenses

A complete list of components and their respective license texts can be found directly on the device. To access them, click the *Licenses* link at the bottom of the router's main web page (*General Status*) or navigate to the following URL in your browser (replace `DEVICE_IP` with the actual router's IP address):

https://DEVICE_IP/licenses.cgi

This serves as a written offer, valid for three years from the date of purchase, to provide any third party with a complete machine-readable copy of the corresponding source code on a flash drive medium for a fee no greater than the cost of physically performing the source distribution. If you wish to obtain the source code, please contact us at:

iiotcustomerservice@advantech.eu

Modifications and debugging of LGPL-linked executables:

The device manufacturer grants customers the right to use debugging techniques (e.g., decompilation) and modify any executable linked with an LGPL library for their own use. These rights are strictly limited to personal usage–redistribution of modified executables or sharing information obtained through these actions is not permitted.

Source code under the GPL license is available at:

icr.advantech.com/source-code

Appendix B: Glossary and Acronyms

B | D | G | H | I | L | N | O | P | R | S | T | U | V | W | X

B

Backup Routes Allows user to back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can have assigned a priority. Switching between connections is done based upon set priorities and the state of the connections.

D

DHCP The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

DHCP client Requests network configuration from DHCP server.

DHCP server Answers configuration request by DHCP clients and sends network configuration details.

DNS The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

DynDNS client DynDNS service lets you access the router remotely using an easy to remember custom hostname. This client monitors the router's IP address and updates it whenever it changes.

G

GRE Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. It is possible to create four different tunnels.

H

HTTP The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTPS The Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

I

IP address An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: *A name indicates what we seek. An* *address indicates where it is. A route indicates how to get there*

The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.

IP masquerade Kind of NAT.

IP masquerading see NAT.

IPsec Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The router allows user to select encapsulation mode (tunnel or transport), IKE mode (main or aggressive), IKE Algorithm, IKE Encryption, ESP Algorithm, ESP Encryption and much more. It is possible to create four different tunnels.

IPv4 The Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. It is one of the core protocols of standards-based internetworking methods of the Internet, and routes most traffic in the Internet. However, a successor protocol, IPv6, has been defined and is in various stages of production deployment. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv6 The Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

While IPv4 still handles a significant portion of internet traffic, IPv6 adoption has grown substantially. As of late 2025, measurements from major content providers show that global user traffic over IPv6 is steadily approaching 50IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0042:1000:8a2e:0370:7334), though various abbreviation methods are also used..

L

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

LAN A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media. The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

N

NAT In computer networking, Network Address Translation (NAT) is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.

The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as basic NAT, which is often also called a one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed. The rest of the packet is left untouched (at least for basic TCP/UDP functionality; some higher level protocols may need further translation). Basic NATs can be used to interconnect two IP networks that have incompatible addressing.

NAT-T NAT traversal (NAT-T) is a computer networking methodology with the goal to establish and maintain Internet protocol connections across gateways that implement network address translation (NAT).

NTP Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

O

OpenVPN OpenVPN implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It is possible to create four different tunnels.

P

PAT Port and Address Translation (PAT) or Network Address Port Translation (NAPT) see NAT.

Port In computer networking, a Port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet.

PPTP The Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol that operates at the Data Link Layer (Layer 2) of the OSI Reference Model. PPTP is a proprietary technique that encapsulates Point-to-Point Protocol (PPP) frames in Internet Protocol (IP) packets using the Generic Routing Encapsulation (GRE) protocol. Packet filters provide access control, end-to-end and server-to-server.

R

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

Root certificate In cryptography and computer security, a root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).
Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). See X.509.

Router A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the *traffic directing* functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

S

SFTP Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol.

SMTP The SMTP (Simple Mail Transfer Protocol) is a standard e-mail protocol on the Internet and part of the TCP/IP protocol suite, as defined by IETF RFC 2821. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTPS, default to port 465.

SMTPS SMTPS (Simple Mail Transfer Protocol Secure) refers to a method for securing SMTP with transport layer security. For more information about SMTP, see description of the SMTP.

SNMP The Simple Network Management Protocol (SNMP) is an *Internet-standard protocol for managing devices on IP networks*. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SSH Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities – slogin, ssh, and scp – that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

T

TCP The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.

Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another.

U

UDP The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768.

URL A uniform resource locator, abbreviated URL, also known as web address, is a specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be `http://www.example.com/index.html`, which indicates a protocol (http), a hostname (www.example.com), and a file name (index.html). A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI, and this is not considered a problem.

V

VPN A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPN server see VPN.

VPN tunnel see VPN.

VRRP VRRP protocol (Virtual Router Redundancy Protocol) allows you to transfer packet routing from the main router to a backup router in case the main router fails. (This can be used to provide a wireless cellular backup to a primary wired router in critical applications).

W

WAN A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet can be considered a WAN as well, and is used by businesses, governments, organizations, and individuals for almost any purpose imaginable.

WebAccess/DMP WebAccess/DMP is an advanced Enterprise-Grade platform solution for provisioning, monitoring, managing and configuring Advantech's routers and IoT gateways. It provides a zero-touch enablement platform for each remote device.

WebAccess/VPN WebAccess/VPN is an advanced VPN management solution for safe interconnection of Advantech routers and LAN networks in public Internet. Connection among devices and networks can be regional or global and can combine different technology platforms and various wireless, LTE, fixed and satellite connectivities.

X

X.509 In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

Appendix C: Index

Appendix D: Related Documents

[1] Command Line Interface

[2] Extending Router Functionality

[3] Remote Monitoring

[4] WebAccess/DMP

[5] R-SeeNet

[6] OpenVPN Tunnel

[7] IPsec Tunnel

[8] GRE Tunnel

[9] WireGuard Tunnel

[10] FlexVPN

[11] VLAN

[12] SNMP Object Identifiers

[13] AT Commands (AT-SMS)

[14] Quality of Service (QoS)

[15] Security Guidelines

[EP] Product-related documents and applications can be obtained on **Engineering Portal** at `https://icr.advantech.com/support/router-models` address.

[RA] **Router Apps** (formerly *User modules*) and related documents can be obtained on *Engineering Portal* at `https://icr.advantech.com/products/router-apps` address.