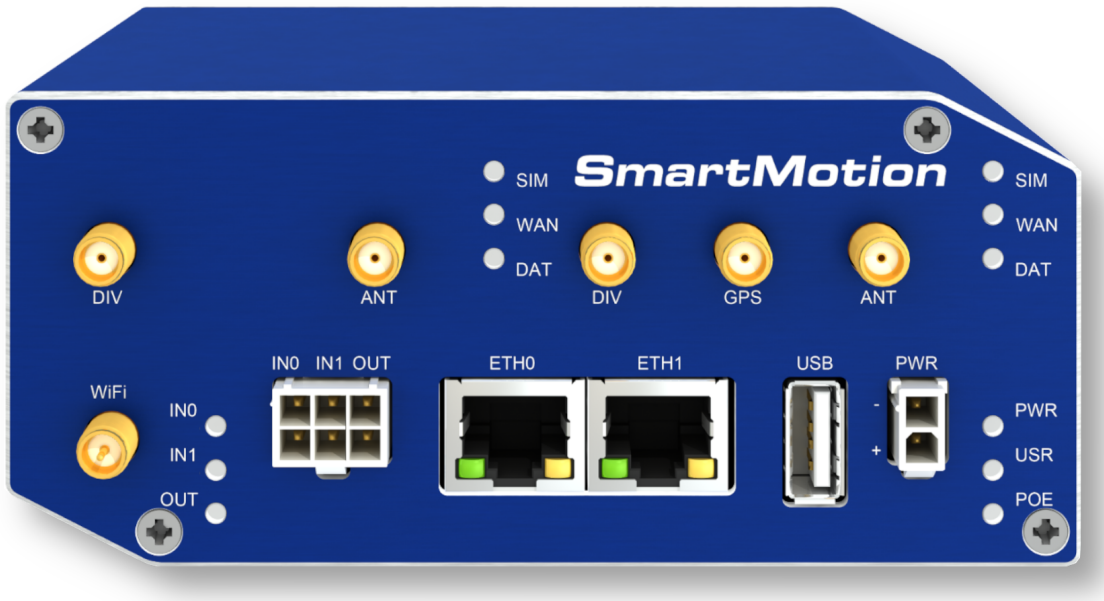
Configuration Manual

SmartMotion Family



Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0024-EN, revision from 25th October, 2024.

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information – Useful tips or information of special interest.

Firmware Version

This manual is compatible with firmware version 6.4.3 (August 16, 2024).

Contents

List of Figures

List of Tables

1. Manual Overview

This *Configuration Manual* details the setup procedures for Advantech SmartMotion family routers, offering comprehensive guidance on the following topics:

- Web configuration interface for the routers – detailed in Chapter 1.1.
- Overview of available remote management system – see Chapter 1.2.
- Detailed configuration instructions, item by item, following the web interface's structure:
  - Status – discussed in Chapter 2.
  - Configuration – outlined in Chapter 3.
  - Customization – covered in Chapter 4.
  - Administration – explained in Chapter 5.
- Configuration examples for typical scenarios – presented in Chapter 6.
- Additional product notes and insights – found in Chapter **??**.

For detailed information on topics such as ordering, hardware features, initial setup, and technical specifications, refer to the ***Hardware Manual*** available on the *Engineering Portal*.

1.1 Web Configuration

> If unsure about the correctness of your configuration or its potential impact on the router's longevity, consult our technical support for guidance.

The router supports configuration via a **web browser** or **Secure Shell** (SSH). This manual primarily covers web browser configuration. For SSH configuration commands, refer to the *Commands and Scripts* Application Note.

Advantech's **remote device management** platform, *WebAccess/DMP*, provides extensive management and monitoring capabilities to ensure devices remain secure and up-to-date. For more information, refer to Chapter 1.2.

Configuring routers is made efficient via a name and password-protected web interface. This interface offers a comprehensive configuration GUI, detailed statistics on router activities, signal strength, system logs, and more (see Figure 1).

To access the web interface on a new router with default settings and establish the router connection, refer to the *Hardware Manual*, specifically the *First Use* chapter.

> For cellular routers, it's essential to correctly configure the carrier settings and activate the account. Ensure you insert the appropriate SIM card. For detailed guidance, refer to the *Hardware Manual*.

To access the web interface, type the router's default IP address *192.168.1.1* into your browser, beginning with *https://* to ensure secure access. The first time you access it, you'll need to install a security certificate to prevent domain disagreement warnings. For detailed instructions, see Chapter 1.1.1.

The default login username is **root**. The default password is indicated on the router's label.[1] Changing the default password as soon as possible is essential for security.

> It is highly recommended to have JavaScript enabled in the browser; otherwise, field validation and some functions will be disabled.

> Three unsuccessful login attempts will block HTTP(S) access from the IP address for one minute.

After a successful login, the web interface presents a menu, providing access to the *Status*, *Configuration*, *Customization*, and *Administration* sections.

Configure the router's *Name* and *Location* in the SNMP settings for display in the web interface's upper right corner (see 3.19.6).

[1] If the router's label does not specify a unique password, use "root" as the default password.

Figure 1: Web Configuration GUI

1.1.1 Managing HTTPS Certificates

The router includes a self-signed HTTPS certificate. Due to the inability to validate this certificate's identity, web browsers may display a warning message. To address this, you can upload your own certificate, signed by a Certification Authority, to the router. If you wish to use your own certificate (for example, in combination with a dynamic DNS service), you should replace the */etc/certs/https_cert* and */etc/certs/https_key* files on the router. This replacement can be easily performed via the GUI on the *HTTP* configuration page, as detailed in Chapter 3.19.3.

To utilize the router's self-signed certificate without encountering the security message (due to domain disagreement) each time you log in, follow these steps:

- Add a DNS record to your DNS system: For Linux/Unix OS, edit /etc/hosts, or for Windows OS, navigate to C:\WINDOWS\system32\drivers\etc\hosts, or configure your own DNS server. Insert a new record pairing the router's IP address with a domain name derived from its MAC address (the MAC address of the first network interface, as seen in the *Network Status* on the router's web interface), using dashes instead of colons for separation. For instance, a router with the MAC address 00:11:22:33:44:55 would use the domain name 00-11-22-33-44-55.
- Access the router via this new domain name address (e.g., https://00-11-22-33-44-55). Should the security warning appear, proceed to add an exception so the message will not recur (e.g., in the Firefox Web browser). If the option to add an exception is unavailable, export the certificate to a file and import it to your browser or operating system.

Note: Utilizing a domain name based on the router's MAC address may not be compatible with all combinations of operating systems and browsers.

1.1.2 Allowed and Restricted Input Characters

When configuring the router via the web interface, it is crucial to avoid using forbidden characters in any input field, not solely the password fields. Below are the specified valid and forbidden characters. Note that for certain fields, the "space" character might also be disallowed.

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

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

Please pay special attention to these guidelines during configuration, as entering invalid characters can lead to errors or unintended behavior.

1.1.3 Supported Certificate Formats

All GUI forms that allow the uploading of certificate files support the following file types:

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

1.2 Remote Management Platform

WebAccess/DMP is an advanced, enterprise-grade platform for provisioning, monitoring, managing, and configuring Advantech's routers and IoT gateways, offering zero-touch enablement for each remote device. For more information, refer to the application note [3] or visit the *WebAccess/DMP* webpage.

New routers come pre-installed with the *WebAccess/DMP* client, which by default activates the connection to the *WebAccess/DMP* server. This connection can be disabled on the *Welcome* page upon initial web interface login or under (*Customization* → *Router Apps* → *WebAccess/DMP Client*).

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

2. Status

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

2.1 General Status

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

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

2.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card
Interface	Defines the interface
Flags	Displays network interface flags: None - no flags Up - the interface is administratively enabled Running - the interface is in operational state (cable detected) Multicast - the interface is capable of multicast transmission
IP Address	IP address of the interface
MTU	Maximum packet size that the equipment is able to transmit
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload
Uptime	Indicates how long the connection to the cellular network has been established

Table 1: Mobile Connection

2.1.2 Ethernet Status

Every Ethernet interface has its separate section on the *General* status page. Items displayed here have the same meaning as items in the previous part. Moreover, the *MAC Address* item shows the MAC address of the corresponding router's interface. Visible information depends on the Ethernet configuration, see Chapter 3.1.

PoE PSE Status

If the router is equipped with the PoE PSE board, there is information about it in the appropriate Ethernet section; see the table below for a description.

Item	Description
LAN1 PoE PSE LAN2 PoE PSE LAN3 PoE PSE LAN4 PoE PSE	• **Disabled** – PoE PSE is disabled in an *Ethernet* configuration page. • **Undervoltage** – Undervoltage, router power supply does not meet the PoE required voltage. • **Overcurrent** / **incompatible device** – Overcurrent, a higher current than the permissible positive difference of the nominal current or a PoE incompatible device connected. • **Idle** – PoE PSE is enabled but currently not used (any device powered). • **Class 0** – Power level (classification unimplemented) • **Class 1** – Power level (very low power) • **Class 2** – Power level (low power) • **Class 3** – Power level (mid power) • **Class 4**[1] – Power level (high power)
PoE PSE Power[2]	Power of PoE PSE [W]
PoE PSE Voltage[2]	Voltage of PoE PSE [V]
PoE PSE Current[2]	Current of PoE PSE [mA]

Table 2: PoE PSE Status

[1] Valid for *IEEE 802.3at/PoE+ Type 2* devices, not allowed for *IEEE 802.3af/PoE Type 1* devices.
[2] Visible only when the PoE is enabled, and an external device is powered.

2.1.3 WiFi Status

Items displayed in this part have the same meaning as items in the previous part. *WiFi AP* part displays information for the WiFi interface (wlan0) working in access point mode, for the configuration see Chapter 3.7. *WiFi STA* part displays information for the WiFi interface (wlan1) working in station mode, for the configuration description see Chapter 3.8.

2.1.4 System Information

System information about the device is displayed in the *System Information* section.

Item	Description
Product Name	Name of the product (may not match with the P/N or order code).
Product Type	Type of the product (may be N/A or the same as the Product Name).
Firmware Version	Information about the firmware version.
Serial Number	Serial number of the router (in case of *N/A* is not available).
Hardware UUID[1]	Unique HW identifier for the device.
Product Revision[1]	Manufactured product revision number.
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation).
CPU Usage	CPU usage value (turn on the refresh in the top right corner).
Memory Usage	Memory usage value (turn on the refresh in the top right corner).
Power Board[2]	Detected type of the PoE extension board.
RTC Battery	RTC battery state.
Supply Voltage	Supply voltage of the router.
Temperature	Temperature in the router.
Time	Current date and time.
Uptime	Indicates how long the router is used.
Licenses	Link to the list of open source software components of the firmware together with their license type. Click on the license type to see the license text.

Table 3: System Information

[1] It may not be available for some models.
[2] Only for models with PoE. The router's power supply voltage must meet the required voltage.

2.2 Mobile WAN Status

The *Mobile WAN* menu item contains current information about connections to the mobile network. On the upper part of the page there are *Mobile Network Information for 1st Module* and *Mobile Network Information for 2nd Module* displayed (information about mobile networks the router operates in). There are also information about the modules mounted in the router.

Item	Description
Registration	State of the network registration
Operator	Specifies the operator's network the router operates in.
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell the router is connected to (in hexadecimal format).
LAC/TAC	Unique number (in hexadecimal format) assigned to each location area. LAC (Location Area Code) for 2G/3G networks and TAC (Tracking Area Code) for 4G networks.
Channel	Channel the router communicates on • ARFCN in case of GPRS/EDGE technology, • UARFCN in case of UMTS/HSPA technology, • EARFCN in case of LTE technology.
Band	Cellular band abbreviation.
Signal Strength	Signal strength (in dBm) of the selected cell, for details see Table 5.
Signal Quality	Signal quality of the selected cell: • EC/IO for UMTS (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
RSSI, RSRP, RSRQ, SINR, RSCP or Ec/Io	Other parameters reporting signal strength or quality. Please note, that some of them may not be available, depending on the cellular module or cellular technology.
CSQ	Cell signal strength with following value ranges: • 2–9 = Marginal, • 10–14 = OK, • 15–19 = Good, • 20–30 = Excelent.
Neighbours	Signal strength of neighboring hearing cells (GPRS only)[1].
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
MEID	MEID number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 4: Mobile Network Information for 1st/2nd Module

The value of signal strength is displayed in different color: in black for good, in orange for fair and in red for poor signal strength.

The middle part of this page, called *Statistics*, displays information about mobile signal quality, transferred data and number of connections for all the SIM cards (for each period). The router has standard intervals,

[1] If a neighboring cell for GPRS is highlighted in red, router may repeatedly switch between the neighboring and the primary cell affecting the router's performance. To prevent this, re-orient the antenna or use a directional antenna.

Signal strength	GPRS/EDGE/CDMA (RSSI)	UMTS/HSPA (RSCP)	LTE (RSRP)
good	> -70 dBm	> -75 dBm	> -90 dBm
fair	-70 dBm to -89 dBm	-75 dBm to -94 dBm	-90 dBm to -109 dBm
poor	< -89 dBm	< -94 dBm	< -109 dBm

Table 5: Value ranges of signal strength for different technologies.

such as the previous 24 hours and last week, and also period starting with *Accounting Start* defined for the MWAN module.

Period	Description
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from Monday 0:00 to Sunday 23:59
Last week	Last week from Monday 0:00 to Sunday 23:59
This period	This accounting period
Last period	Last accounting period

Table 6: Description of Periods

Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establishment
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 7: Mobile Network Statistics

Tips for *Mobile Network Statistics* table:

- *Availability* is expressed as a percentage. It is the ratio of time connection to the mobile network has been established to the time that router has been is turned on.
- Placing your cursor over the maximum or minimum signal strength will display the last time the router reached that signal strength.

The last part (*Connection Log*) displays information about the mobile network connections and any problems that occurred while establishing them.

Mobile WAN Status refresh

Mobile Network Information for 1st Module

Registration	: Home Network
Operator	: Vodafone CZ
Technology	: LTE
PLMN	: 23003
Cell	: 10A802
LAC	: 947C
Channel	: 275
Signal Strength	: -90 dBm
Signal Quality	: -12 dB

» More Information «

Mobile Network Information for 2nd Module

Registration	: Home Network
Operator	: Vodafone CZ
Technology	: LTE
PLMN	: 23003
Cell	: 10A80C
LAC	: 947C
Channel	: 6400
Signal Strength	: -76 dBm
Signal Quality	: -7 dB

» More Information «

Statistics for 1st SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	9 KB	9 KB	0 KB	9 KB	0 KB
Tx Data	: 0 KB	450 KB	450 KB	0 KB	450 KB	0 KB
Connections	: 1	4	5	0	5	0
Signal Min	: -94 dBm	-93 dBm	-94 dBm	?	-94 dBm	?
Signal Avg	: -82 dBm	-81 dBm	-82 dBm	?	-82 dBm	?
Signal Max	: -75 dBm	-77 dBm	-75 dBm	?	-75 dBm	?
Cells	: 6	6	11	0	11	0
Availability	: 99.9%	99.4%	99.8%	0.0%	99.8%	0.0%

Statistics for 2nd SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	: 0	0	0	0	0	0
Signal Min	: ?	?	?	?	?	?
Signal Avg	: ?	?	?	?	?	?
Signal Max	: ?	?	?	?	?	?
Cells	: 0	0	0	0	0	0
Availability	: 0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Statistics for 3rd SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	: 0 KB	484 KB	484 KB	0 KB	484 KB	0 KB
Connections	: 1	4	5	0	5	0
Signal Min	: -77 dBm	-77 dBm	-77 dBm	?	-77 dBm	?
Signal Avg	: -75 dBm	-76 dBm	-75 dBm	?	-75 dBm	?
Signal Max	: -72 dBm	-74 dBm	-72 dBm	?	-72 dBm	?
Cells	: 1	1	1	0	1	0
Availability	: 99.9%	99.3%	99.8%	0.0%	99.8%	0.0%

Statistics for 4th SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	: 0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	: 0	0	0	0	0	0
Signal Min	: ?	?	?	?	?	?
Signal Avg	: ?	?	?	?	?	?
Signal Max	: ?	?	?	?	?	?
Cells	: 0	0	0	0	0	0
Availability	: 0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Connection Log for 1st Module

2019-08-22 00:11:44 (1st SIM card) Connection successfully established.

Connection Log for 2nd Module

2019-08-22 00:11:42 (3rd SIM card) Connection successfully established.

Figure 2: Mobile WAN status

2.3 WiFi Status

This feature is accessible only on routers equipped with a WiFi module.

Selecting the *Status* → *WiFi* → *Status* option in the web interface's main menu displays details about the WiFi access point (AP) and the WiFi station (STA), including a list of all stations connected to the AP.

An example output for WiFi status is illustrated in the figure below. It includes information on the WiFi chip, its firmware version, and the supported modes for the module. For instance, the notation "Supports 1 station and 2 access points" indicates that it is possible to use one station configuration alongside two distinct Access Point configurations simultaneously.

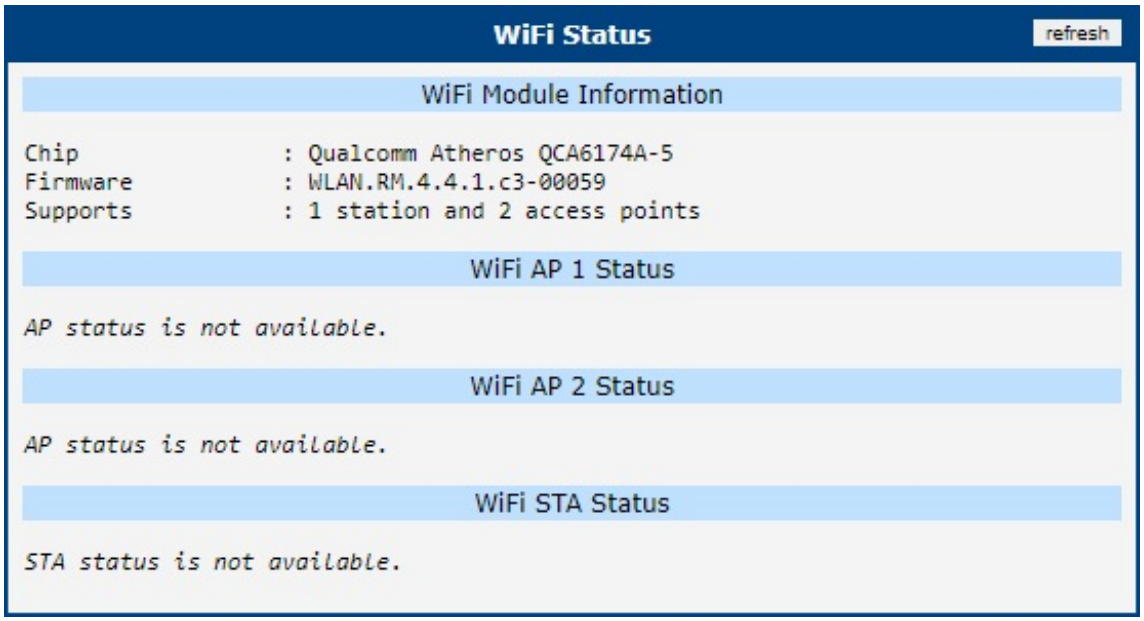


Figure 3: WiFi Status

2.4 WiFi Scan

> This feature is accessible only on routers equipped with a WiFi module.

Selecting *Status* → *WiFi* → *Scan* initiates a scan for nearby WiFi networks, with the results displayed as shown in Figure 4.

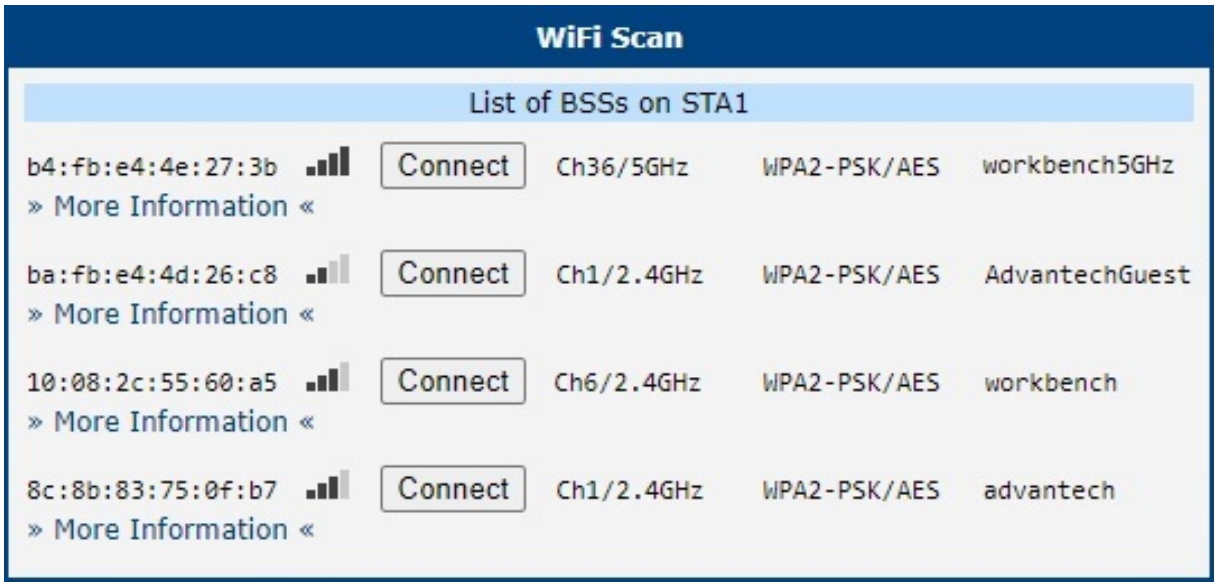


Figure 4: WiFi Scan Output Example

If you click on the *Connect* button next to the respective WiFi network, you will be redirected to the *Configuration* → *WiFi* → *Station* page, where the available fields will be pre-filled and you will be able to connect to the network by entering authentication details.

For each network, you can view details by clicking on the *More Information* button. Below is the description of some items from the WiFi scanning output.

Item	Description
BSS	MAC address of the access point (AP).
TSF	Synchronizes timers across all stations in a Basic Service Set (BSS).
freq	Frequency band of the WiFi network in MHz.
beacon interval	Time between synchronization beacons.
capability	Properties list of the access point (AP).
signal	Signal strength of the access point (AP).
last seen [boottime]	Timestamp of the last time the access point (AP) was detected, relative to the scanning device's boot time.
last seen [ms ago]	Timestamp of the last response from the access point (AP).
SSID	Name identifier of the access point (AP).
Supported rates	Data rates supported by the access point (AP).
DS Parameter set	Broadcasting channel of the access point (AP).

Continued on next page

Continued from previous page

Item	Description
ERP	Provides backward compatibility for PHY rates.
RSN	Protocol ensuring secure wireless communication.
Extended supported rates	Additional supported rates beyond the basic eight.
Country	Regulatory domain for the AP, dictating operational parameters.
BSS Load	Current load information on the Basic Service Set (BSS).
RM enabled capabilities	AP's ability to report radio spectrum measurements.
(V)HT capabilities	Features enhancing data rates for 802.11ac/n networks.
(V)HT operation	Utilization of (V)HT capabilities in the current setup.
Overlapping BSS scan params	Guides scanning for overlapping BSS to minimize interference.
Extended capabilities	Additional AP features improving network functions.
WMM	Prioritizes network traffic to ensure quality for voice and video.

Table 8: Detailed Information about WiFi Networks

2.5 Network Status

To view information about the interfaces and the routing table, open the *Network* item in the *Status* menu. The upper part of the window displays detailed information about the active interfaces only:

Note: Some interfaces may not be available on your router.

Interface	Description
eth*x*	Ethernet interfaces
lan*x*	LAN interfaces
lo	Local loopback interface
nat64	Network interface of internal translator gateway between IPv6 and IPv4 addresses.
switch0	SWITCH interface
usb*x*	Active connection to the mobile network – wireless module is connected via USB interface.
wlan*x*	WiFi interfaces – if configured
ppp*x*	PPP interfaces (e.g. PPPoE tunnel – if configured)
tun*x*	OpenVPN tunnel interfaces – if configured
ipsec*x*	IPSec tunnel interfaces – if configured
gre*x*	GRE tunnel interfaces – if configured
wg*x*	WireGuard tunnel interfaces – if configured

Table 9: Description of Interfaces in Network Status

The following information can be displayed for network interfaces:

Item	Description
HWaddr	Hardware (unique, MAC) address of a network interface.
inet addr	IPv4 address of interface
inet6 addr	IPv6 address of interface. There can be more of them for single network interface.
P-t-P	IP address of the opposite end (in case of point-to-point connection).
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit.
Metric	Number of routers the packet must go through.

Continued on next page

Continued from previous page

Item	Description
RX	• **packets** – received packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – incoming packets lost because of overload. • **frame** – wrong incoming packets because of incorrect packet size.
TX	• **packets** – transmit packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – outgoing packets lost because of overload. • **carrier** – wrong outgoing packets with errors resulting from the physical layer.
collisions	Number of collisions on physical layer.
txqueuelen	Length of buffer (queue) of the network interface.
RX bytes	Total number of received bytes.
TX bytes	Total number of transmitted bytes.

Table 10: Description of Information in Network Status

You may view the status of the mobile network connection on the network status screen. If the connection to the mobile network is active, it will appear in the system information as an usb0 interface.

The *Route Table* is displayed at the bottom of the *Network Status* page. There is IPv4 *Route Table* and *IPv6 Route Table* below.

If the router is connected to the Internet (a default route is defined), the *nat64* network interface is created automatically. This is the NAT64 internal gateway for translating the IPv6 and IPv4 communication. It is used automatically when connected via IPv6 and communicating with IPv4 device or network. It works together with DNS64 running in the router automatically (translation of domain names to IP addresses). The default NAT64 prefix 64:ff9b::/96 is used as you can see in Figure 5 below in the *IPv6 Route Table* section.

Network Status refresh

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 02:AD:FF:00:00:91
          inet addr:10.64.0.91  Bcast:10.64.3.255  Mask:255.255.252.0
          inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
          inet6 addr: fd00:a40::91/56 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:749 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82340 (80.4 KB)  TX bytes:969616 (946.8 KB)

eth1      Link encap:Ethernet  HWaddr 02:AD:FF:01:00:91
          inet addr:10.65.0.91  Bcast:10.65.3.255  Mask:255.255.252.0
          inet6 addr: fd00:a41::91/56 Scope:Global
          inet6 addr: fe80::ad:ffff:fe01:91/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:263 errors:0 dropped:9 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14419 (14.0 KB)  TX bytes:680 (680.0 B)

eth2      Link encap:Ethernet  HWaddr 02:AD:FF:02:00:91
          inet addr:10.66.0.91  Bcast:10.66.3.255  Mask:255.255.252.0
          inet6 addr: fe80::ad:ffff:fe02:91/64 Scope:Link
          inet6 addr: fd00:a42::91/56 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1024
          RX bytes:2234 (2.1 KB)  TX bytes:1008 (1008.0 B)

lan1      Link encap:Ethernet  HWaddr 02:AD:FF:00:00:91
          inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:967 errors:0 dropped:9 overruns:0 frame:0
          TX packets:753 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:84227 (82.2 KB)  TX bytes:970216 (947.4 KB)

switch0   Link encap:Ethernet  HWaddr 02:AD:FF:00:00:91
          inet6 addr: fe80::ad:ffff:fe00:91/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1230 errors:0 dropped:0 overruns:0 frame:0
          TX packets:764 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1024
          RX bytes:125706 (122.7 KB)  TX bytes:977642 (954.7 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
10.66.0.0	0.0.0.0	255.255.252.0	U	0	0	0	eth2
10.70.0.0	0.0.0.0	255.255.252.0	U	0	0	0	wlan0
10.72.0.0	0.0.0.0	255.255.252.0	U	0	0	0	wlan02
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
64:ff9b::/96	::	U	256	1	0	nat64
ff00::/8	::	U	256	1	0	nat64
::/0	::	!n	-1	1	1	lo

Figure 5: Network Status

2.5.1 Connections

On the *Network Status* page, scroll down and click the »Connections« link. A new window listing all active router connections will display, see Figure 6.

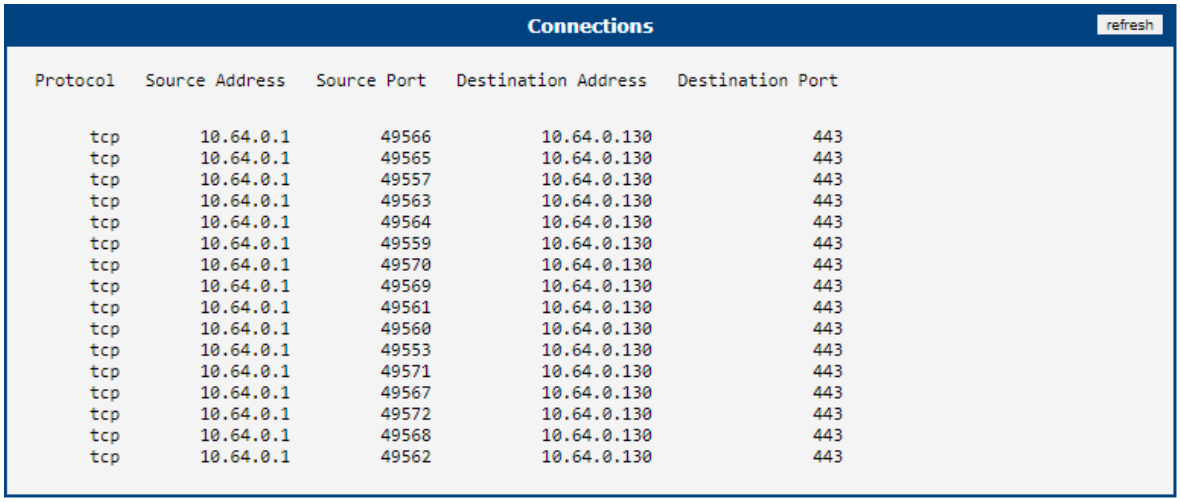


Figure 6: Connection List

2.6 DHCP Status

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

See Figure 7 for the DHCP Status example. Records in the *DHCP Status* window are divided into two parts based on the interface.

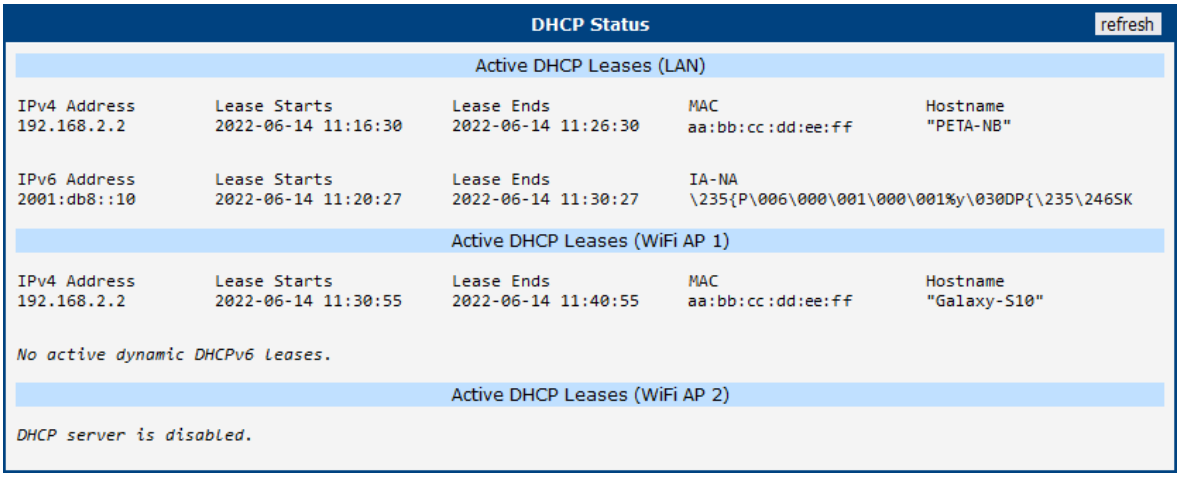


Figure 7: DHCP Status

The DHCP status window displays the following information on a row for each client in the list. All items are described in Table 11.

Item	Description
IPv4 Address	IPv4 address assigned to a client.
IPv6 Address	IPv6 address assigned to a client.
Lease Starts	The time the IP address lease started.
Lease Ends	The time the IP address lease expires.
MAC	MAC address of the client.
Hostname	Client hostname.
IA-NA	IPv6 unique identifier.

Table 11: DHCP Status Description

The DHCP status may occasionally display two records for one IP address. It may be caused by resetting the client network interface.

2.7 IPsec Status

Selecting the *IPsec* option in the *Status* menu of the web page will bring up the information for any IPsec Tunnels that have been established. If the tunnel has been built correctly, the screen will display **ESTABLISHED** and the number of running IPsec connections **1 up** (orange highlighted in the figure below.) If there is no such text in log (e.g. "0 up"), the tunnel was not created!

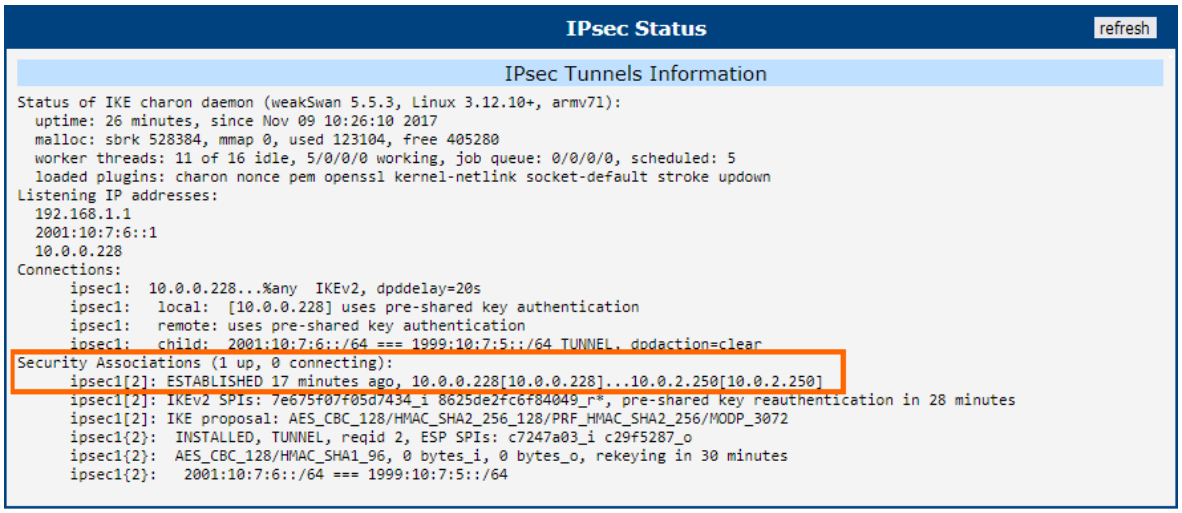


Figure 8: IPsec Status

2.8 WireGuard Status

Selecting the *WireGuard* option in the *Status* menu of the web page will bring up the information for any WireGuard Tunnels established. In the figure below is an example of the first WireGuard tunnel running.

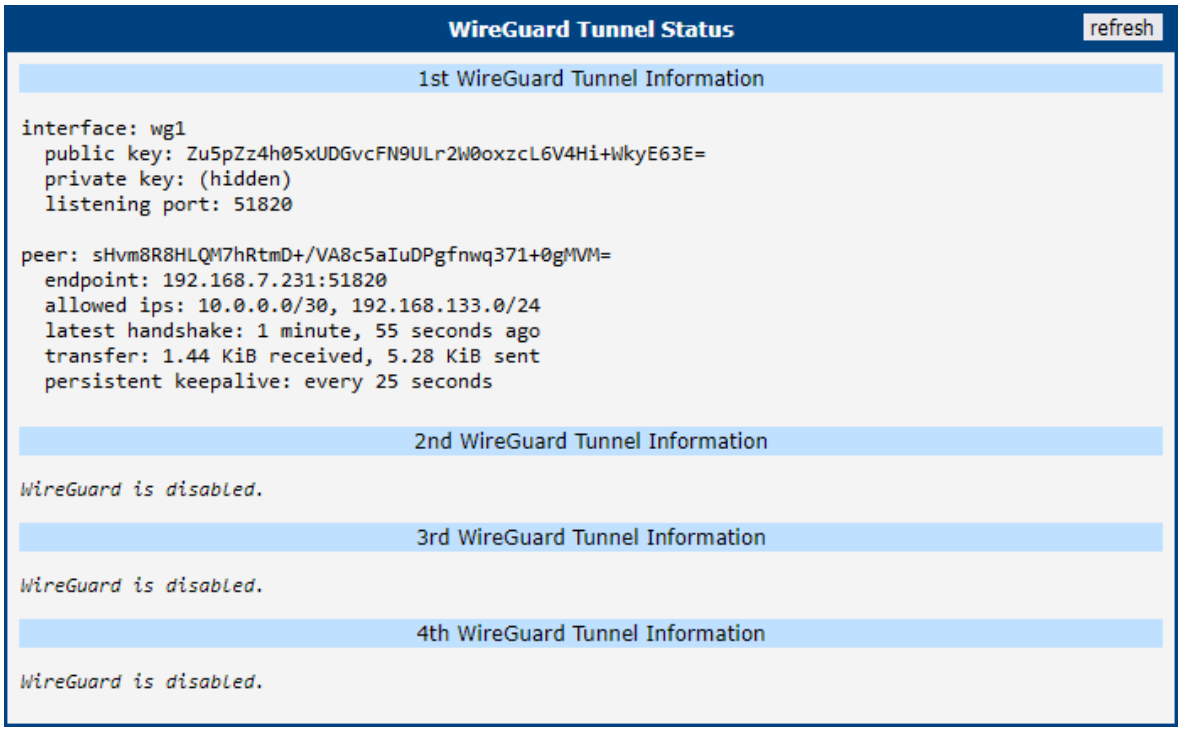


Figure 9: WireGuard Status Page

The *Latest handshake* time is the time left from the latest successful communication with the opposite tunnel side. This item will not be shown here until there is a tunnel communication (data sent by the client-side or the keepalive data sent when *NAT/Firewall Traversal* is set to *yes*).

2.9 DynDNS Status

The router supports DynamicDNS using a DNS server on www.dyndns.org. If Dynamic DNS is configured, the status can be displayed by selecting menu option DynDNS. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.

You can use the following listed servers for the Dynamic DNS service. It is possible to use the DynDNSv6 service with *IP Mode* switched to IPv6 on *DynDNS Configuration* page.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com

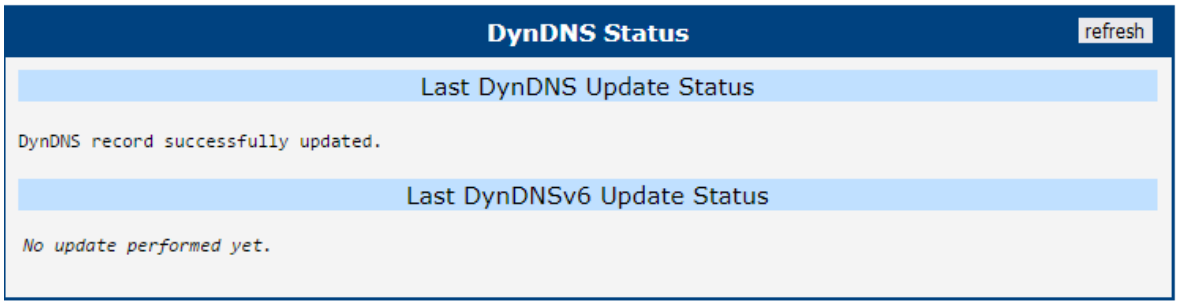


Figure 10: DynDNS Status

When the router detects a DynDNS record update, the dialog displays one or more of the following messages:

- 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 update.
- DNS error encountered.
- DynDNS server failure.

The router's SIM card must have public IP address assigned or DynDNS will not function correctly.

2.10 System Log

If there are any connection problems you may view the system log by selecting the *System Log* menu item. Detailed reports from individual applications running in the router will be displayed. Use the *Save Log* button to save the system log to a connected computer. (It will be saved as a text file with the .log extension.) The *Save Report* button is used for creating detailed reports. (It will be saved as a text file with the .txt extension. The file will include statistical data, routing and process tables, system log, and configuration.)

Sensitive data from the report are filtered out for security reasons.

The default length of the system log is 1000 lines. After reaching 1000 lines a new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with a new file.

The *Syslogd* program will output the system log. It can be started with two options to modify its behavior. Option "*-S*" followed by decimal number sets the maximal number of lines in one log file. Option "*-R*" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog deamon is Linux OS, there has to be remote logging enabled (typically running "*syslogd -R*"). If it's the Windows OS, there has to be syslog server installed, e.g. *Syslog Watcher*). To start *syslogd* with these options, the "*/etc/init.d/syslog*" script can be modified via SSH or lines can be added into *Startup Script* (accessible in *Configuration* section) according to figure 12.

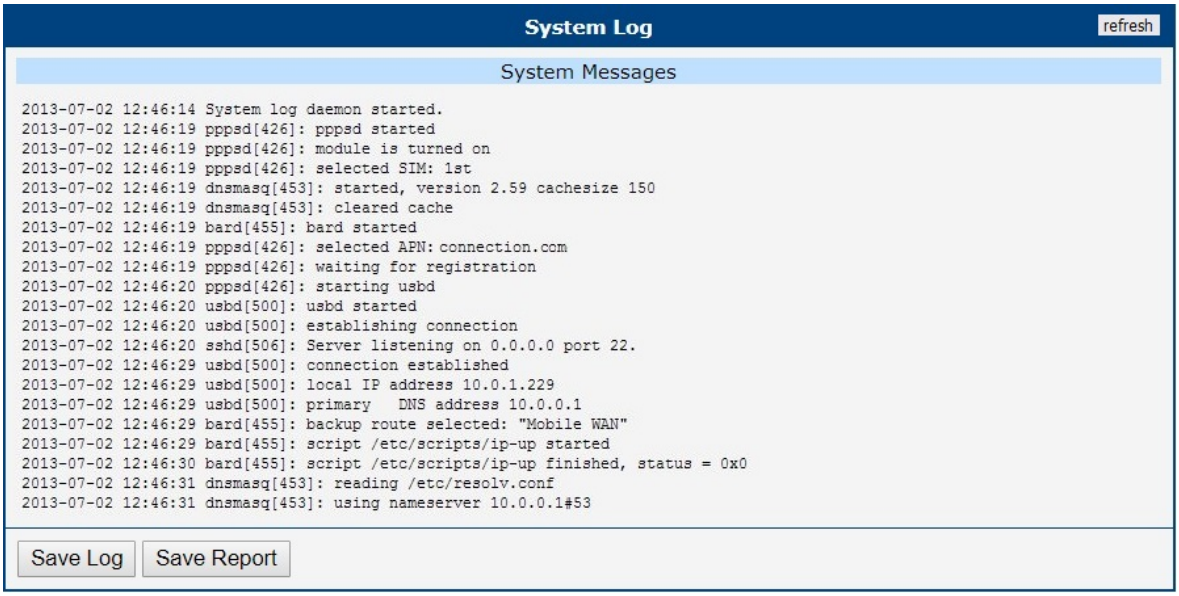


Figure 11: System Log

The following example (figure) shows how to send syslog information to a remote server at 192.168.2.115 on startup.

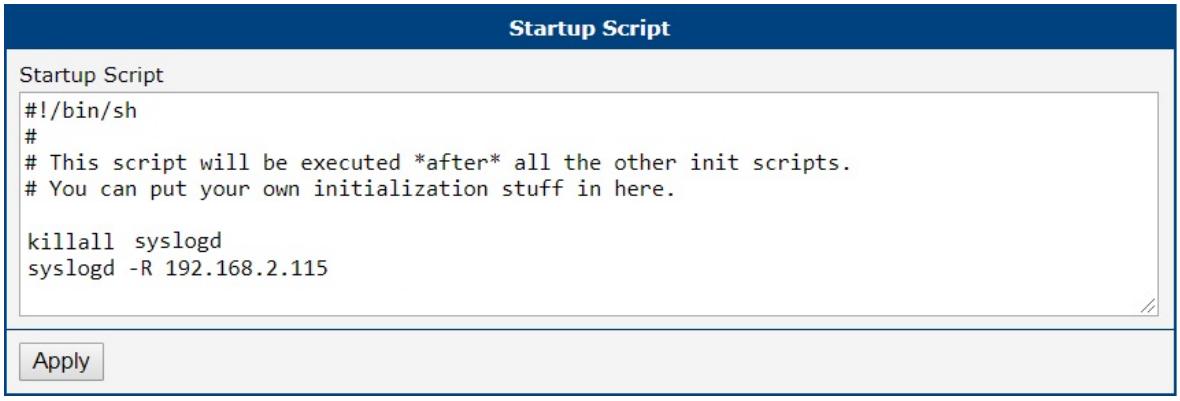


Figure 12: Example program syslogd start with the parameter `-R`

3. Configuration

3.1 Ethernet Configuration

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

LAN Configuration page is divided into IPv4 and IPv6 columns, see Figure 13. There is dual stack support of IPv4 and IPv6 protocols – they can run alongside, you can configure either one of them or both. If you configure both IPv4 and IPv6, other network devices will choose the communication protocol. Configuration items and IPv6 to IPv4 differences are described in the tables below.

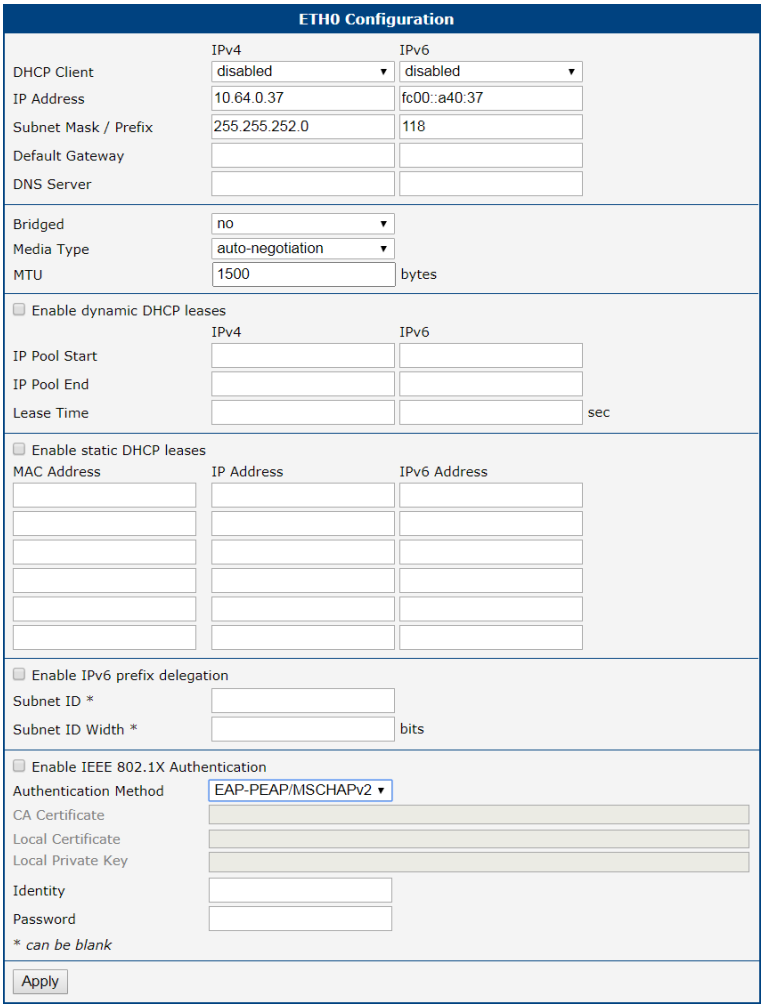


Figure 13: LAN Configuration page

Item	Description
DHCP Client	Enables/disables the DHCP client function. If in IPv6 column, the DHCPv6 client is enabled. DHCPv6 client supports all three methods of getting an IPv6 address – SLAAC, stateless DHCPv6 and statefull DHCPv6. • **disabled** – The router does not allow automatic allocation of an IP address from a DHCP server in LAN network. • **enabled** – The router allows automatic allocation of an IP address from a DHCP server in LAN network.
IP Address	A fixed IP address of the Ethernet interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent to this IP address. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the router forwards the request to DNS server specified here. Use proper IP address notation in IPv4 and IPv6 column.

Table 12: Configuration of the Network Interface – IPv4 and IPv6

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is set to *disabled* and if the ETH0 or ETH1 LAN is selected by the *Backup Routes* system as the default route. (The selection algorithm is described in section 3.9). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces (e.g. eth0 + eth1).

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

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

Item	Description
Bridged	Activates/deactivates the bridging function on the router. • **no** – The bridging function is inactive (default). • **yes** – The bridging function is active.
Media Type	Specifies the type of duplex and speed used in the network. • **Auto-negation** – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • **100 Mbps Full Duplex** – The router communicates at 100 Mbps, in the full duplex mode. • **100 Mbps Half Duplex** – The router communicates at 100 Mbps, in the half duplex mode. • **10 Mbps Full Duplex** – The router communicates at 10 Mbps, in the full duplex mode. • **10 Mbps Half Duplex** – The router communicates at 10 Mbps, in the half duplex mode.
MTU	Maximum Transmission Unit value. Default value is 1500 bytes.
LAN1 PoE PSE[1] LAN2 PoE PSE[1] LAN3 PoE PSE[1] LAN4 PoE PSE[1]	• **enabled** – The PoE PSE feature is enabled for port LANx of an ETH0 interface. • **disabled** – The PoE PSE feature is disabled for port LANx of an ETH0 interface (default).

Table 13: Configuration of the Network Interface – global items

[1] Available only on models equipped with the PoE PSE functionality.

3.1.1 DHCP Server

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

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

If IPv6 column is filled in, the DHCPv6 server is used. DHCPv6 server offers stateful address configuration to connected clients. Only when the *Subnet Prefix* above is set to 64, the DHCPv6 server offers both – the stateful address configuration and SLAAC (Stateless Address Autoconfiguration).

For DHCPv6 static address assignment to work, DHCPv6 client must use DUID-LL or DUID-LLT types that are derived from its MAC address.

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

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

Table 14: Configuration of Dynamic DHCP Server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

Table 15: Configuration of Static DHCP Server

3.1.2 IPv6 Prefix Delegation

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

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

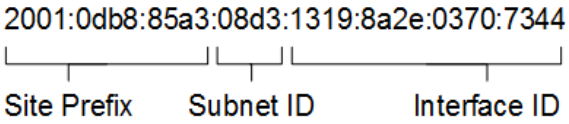


Figure 14: IPv6 Address with Prefix Example

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the *Subnet ID Width*.
Subnet ID Width	The maximum *Subnet ID Width* depends on your Site Prefix – it is the remainder to 64 bits.

Table 16: IPv6 prefix delegation configuration

3.1.3 802.1X Authentication to RADIUS Server

IEEE 802.1X is an **IEEE Standard** for **port-based Network Access Control** (PNAC), part of the IEEE 802.1 group of networking protocols. It provides an **authentication mechanism** for devices wishing to attach to a LAN or WLAN through "EAP over LAN" or **EAPoL**, which encapsulates the **Extensible Authentication Protocol** (EAP) over IEEE 802.

IEEE 802.1X authentication involves three parties: **a supplicant**, **an authenticator**, and **an authentication server**, illustrated in Figure 15.

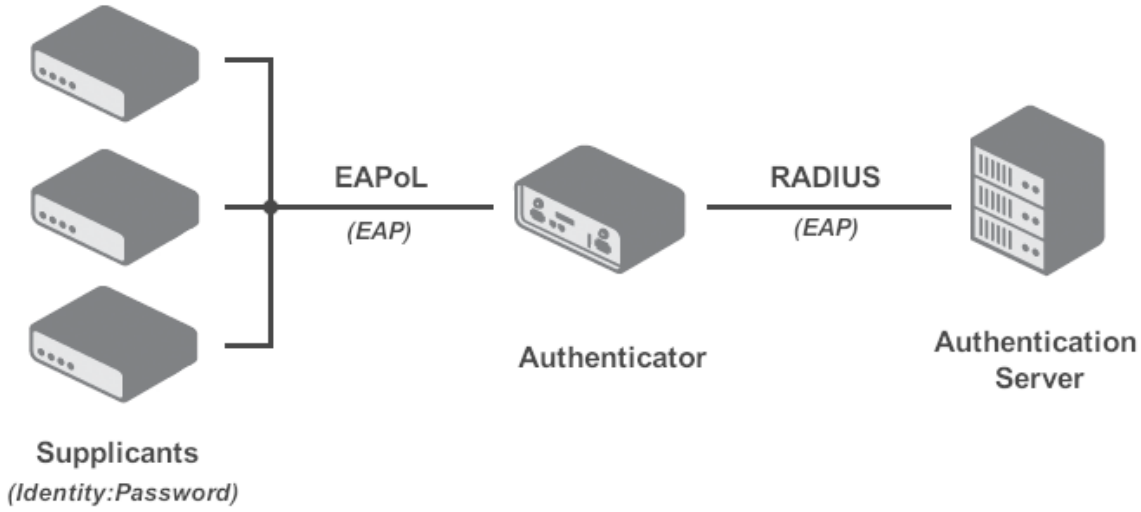


Figure 15: IEEE 802.1X Functional Diagram

- The **supplicant** is a client device (e.g., a laptop) wishing to attach to the LAN/WLAN, also referring to the client software providing credentials to the authenticator.
- The **authenticator** is a network device facilitating the data link between the supplicant and the network, capable of permitting or denying network traffic. This device communicates with the authentication server to decide on network access authorization for a supplicant.
- The **authentication server**, usually a trusted server, handles requests for network access, informing the authenticator about connection permissions and the settings applicable to the client's connection. It commonly runs software supporting the **RADIUS** and **EAP protocols**.

Table 17 summarizes the supported roles and cases for IEEE 802.1X authentication on Advantech routers.

Advantech routers support the roles of supplicant and authenticator only. The authentication server role is not supported.

Interface	Supplicant Role	Authenticator Role
LAN	As a built-in feature, configure LAN with 802.1X authentication, see Chapter 3.1.3.	While not a built-in feature, it can be facilitated by the *802.1X Authenticator* Router App.
WiFi	In Station (STA) mode, see Chapter 3.8.	In Access Point (AP) mode, see Chapter 3.7.

Table 17: Supported Roles for IEEE 802.1X Authentication

Authentication (802.1X) to RADIUS server can be enabled in next configuration section. This functionality requires additional setting of identity and certificates as described in the following table.

Item	Description
Enable IEEE 802.1X Authentication	Select this option to enable 802.1X Authentication.
Authentication Method	Select authentication method (EAP-PEAPMSCHAPv2 or EAP-TLS).
CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
Local Private Key	Definition of local private key for EAP-TLS authentication protocol.
Identity	User name – identity.
Password	Access password. This item is available for EAP-PEAPMSCHAPv2 protocol only. Enter valid characters only, see chap. 1.1.2!
Local Private Key Password	Definition of password for private key of EAP-TLS protocol. This item is available for EAP-TLS protocol only. Enter valid characters only, see chap. 1.1.2!

Table 18: Configuration of 802.1X Authentication

3.1.4 LAN Configuration Examples

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

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

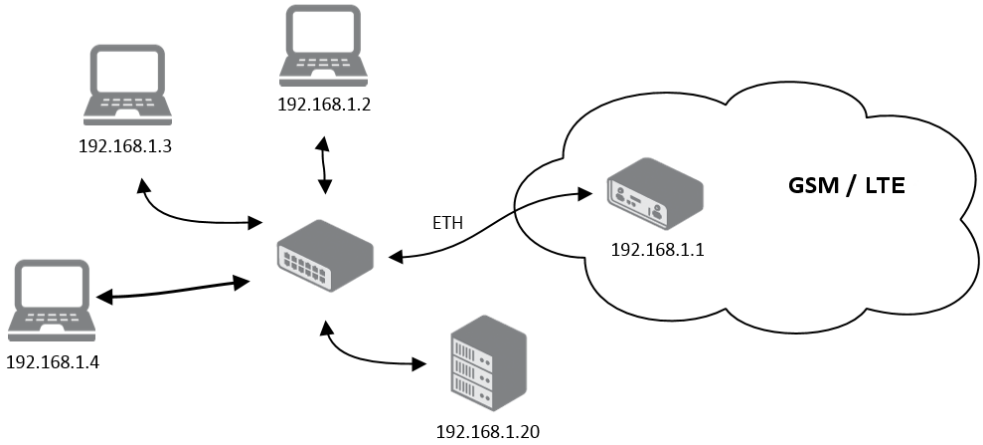


Figure 16: Network Topology for Example 1

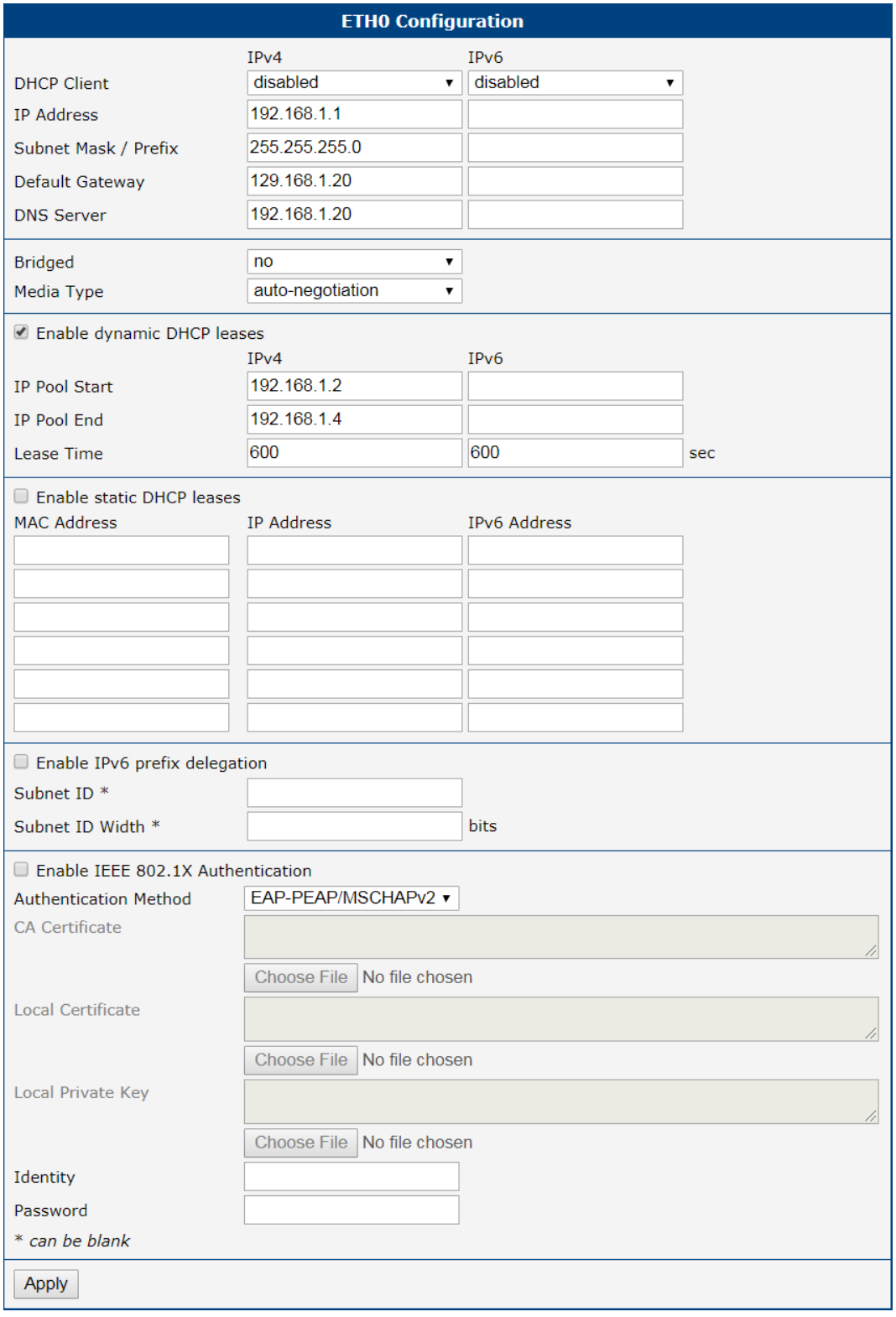


Figure 17: LAN Configuration for Example 1

Example 2: IPv4 Dynamic and Static DHCP server

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

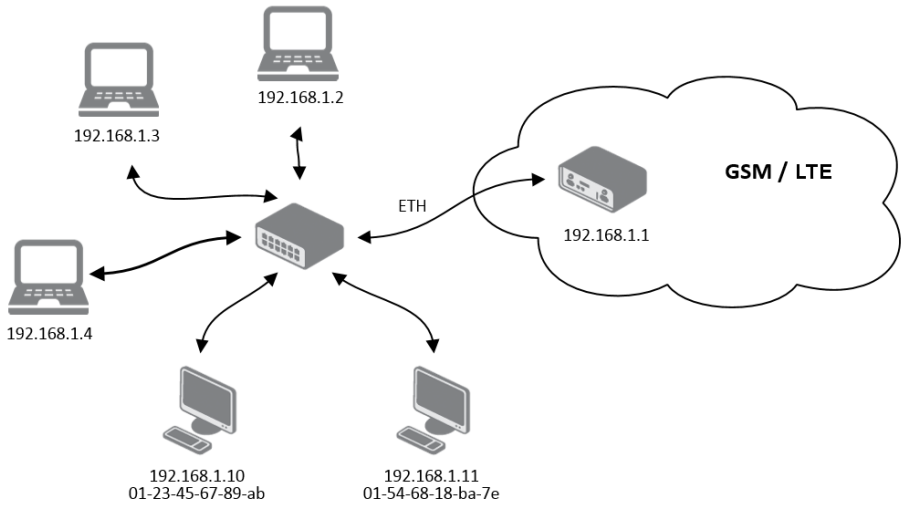


Figure 18: Network Topology for Example 2

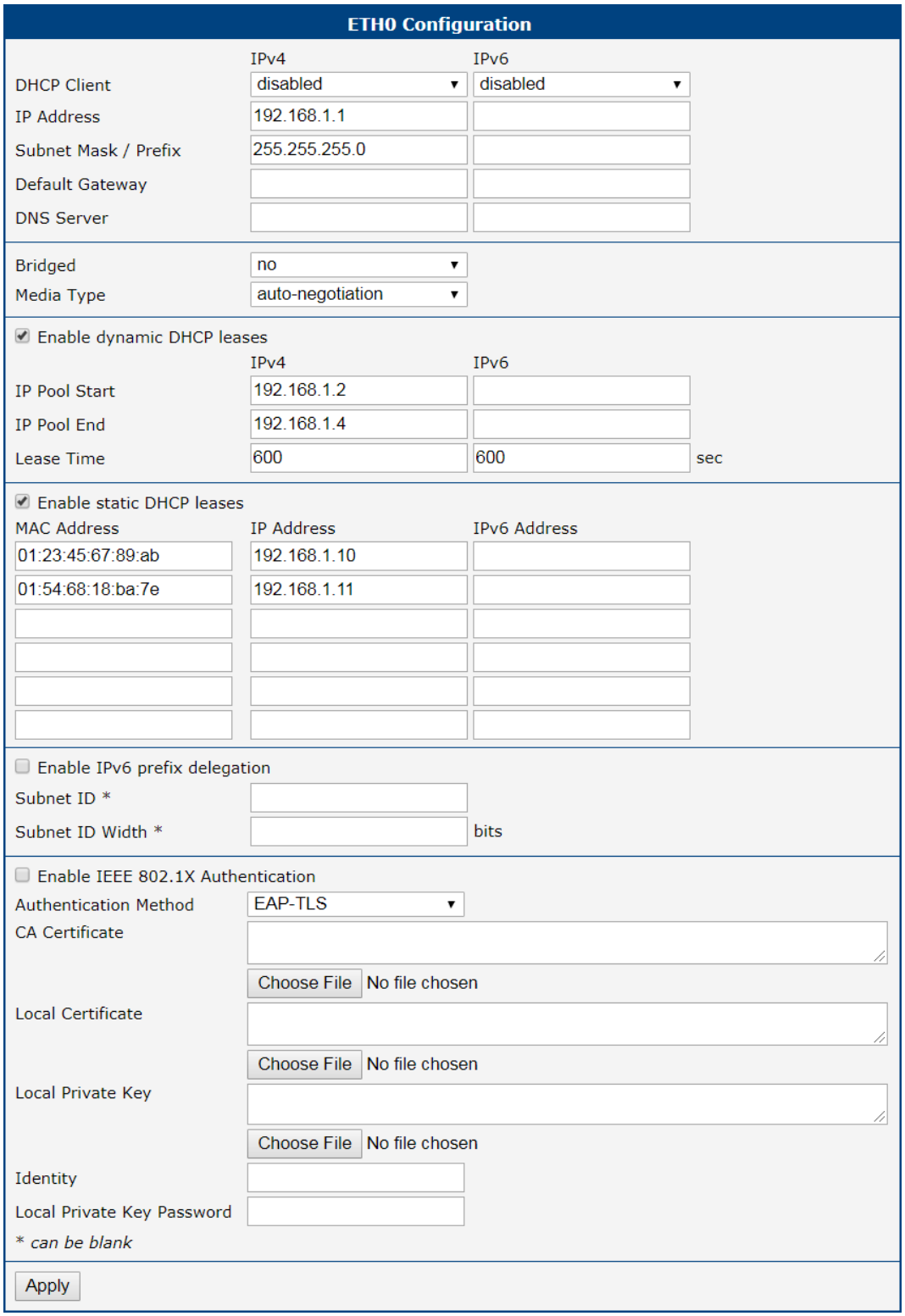


Figure 19: LAN Configuration for Example 2

Example 3: IPv6 Dynamic DHCP Server

- The range of dynamic allocated IPv6 addresses is from 2001:db8::1 to 2001:db8::ffff.
- The address is allocated for 600 second (10 minutes).
- The router is still accessible via IPv4 (192.168.1.1).

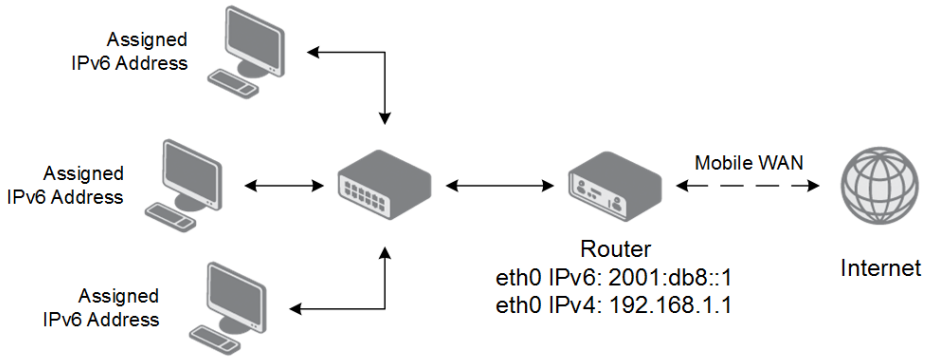


Figure 20: Network Topology for Example 3

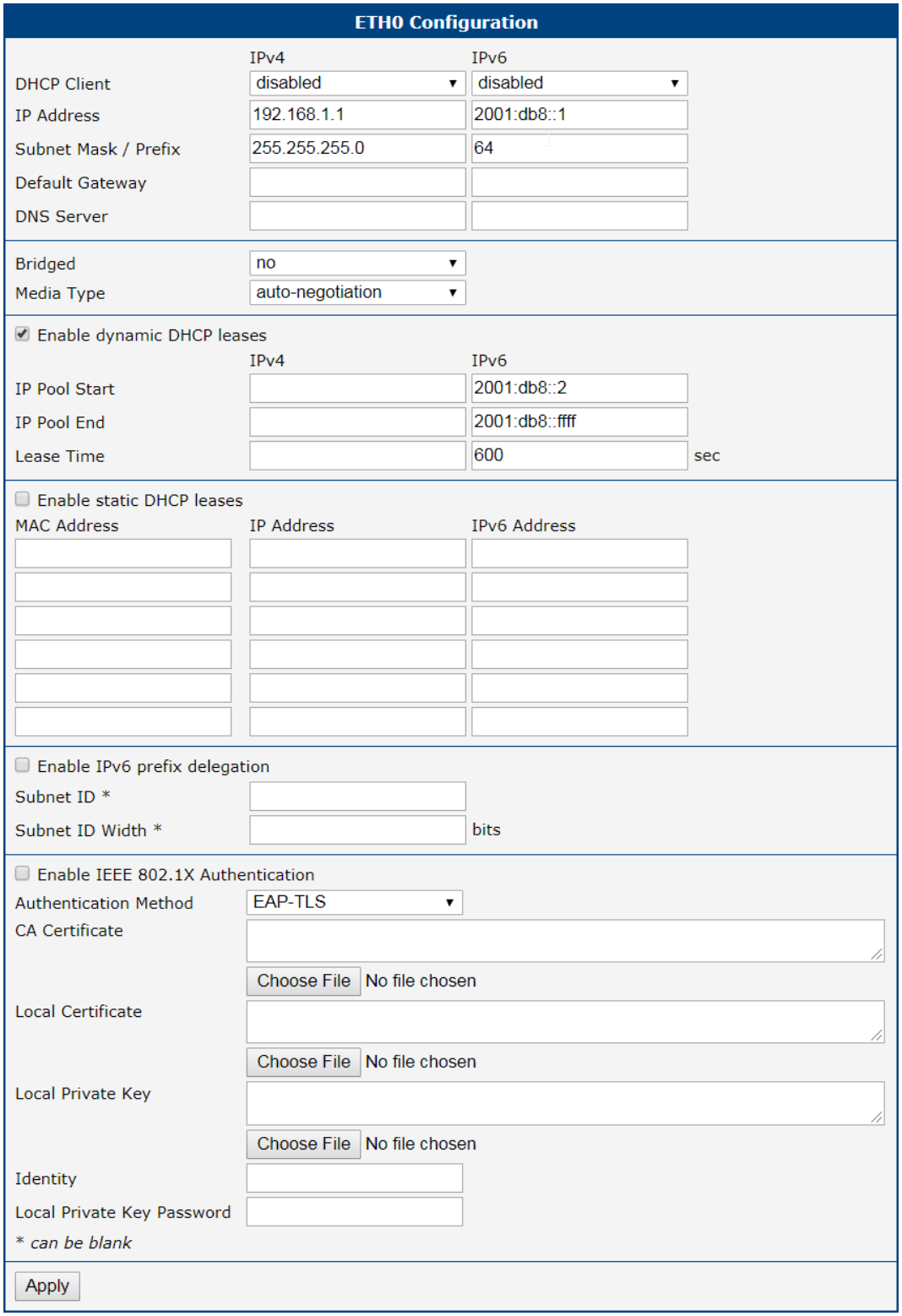


Figure 21: LAN Configuration for Example 3

3.2 VRRP Configuration

Select the *VRRP* menu item to enter the VRRP configuration. There are two submenus which allows to configure up to two instances of 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.) If the *Enable VRRP* is checked, you may set the following parameters.

Item	Description
Protocol Version	Choose version of the VRRP (VRRPv2 or VRRPv3).
Virtual Server IP Address	This parameter sets the virtual server IP address. This address must be the same for both the primary and backup routers. Devices on the LAN will use this address as their default gateway IP address.
Virtual Server ID	This parameter distinguishes one virtual router on the network from another. The main and backup routers must use the same value for this parameter.
Host Priority	The active router with highest priority set by the parameter Host Priority, is the main router. According to RFC 2338, the main router should have the highest possible priority – 255. The backup router(s) have a priority in the range 1 – 254 (default value is 100). A priority value of 0 is not allowed.

Table 19: VRRP configuration

You may set the *Check connection* flag in the second part of the window to enable automatic test messages for the cellular network. In some cases, the mobile WAN connection could still be active but the router will not be able to send data over the cellular network. This feature is used to verify that data can be sent over the PPP connection and supplements the normal VRRP message handling. The currently active router (main/backup) will send test messages to the defined *Ping IP Address* at periodic time intervals (*Ping Interval*) and wait for a reply (*Ping Timeout*). If the router does not receive a response to the Ping command, it will retry up to the number of times specified by the *Ping Probes* parameter. After that time, it will switch itself to a backup router until the PPP connection is restored.

You may use the DNS server of the mobile carrier as the destination IP address for the test messages (Pings).

The *Enable traffic monitoring* option can be used to reduce the number of messages that are sent to test the PPP connection. When this parameter is set, the router will monitor the interface for any packets different from a ping. If a response to the packet is received within the timeout specified by the *Ping Timeout* parameter, then the router knows that the connection is still active. If the router does not receive a response within the timeout period, it will attempt to test the mobile WAN connection using standard Ping commands.

Item	Description
Ping IP Address	Destinations IP address for the Ping commands. IP Address can not be specified as a domain name.
Ping Interval	Interval in seconds between the outgoing Pings.
Ping Timeout	Time in seconds to wait for a response to the Ping.
Ping Probes	Maximum number of failed ping requests.

Table 20: Check connection

Example of the VRRP protocol:

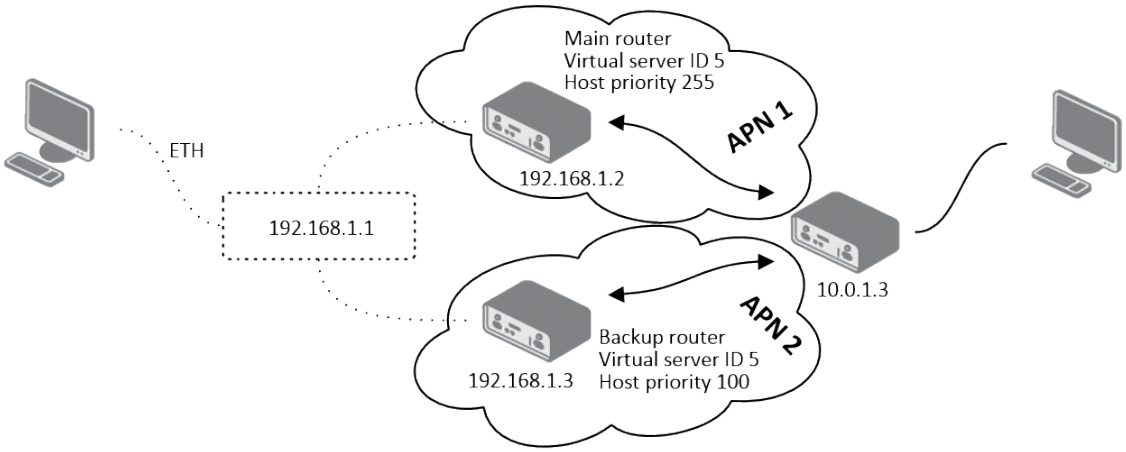


Figure 22: Topology of VRRP configuration example

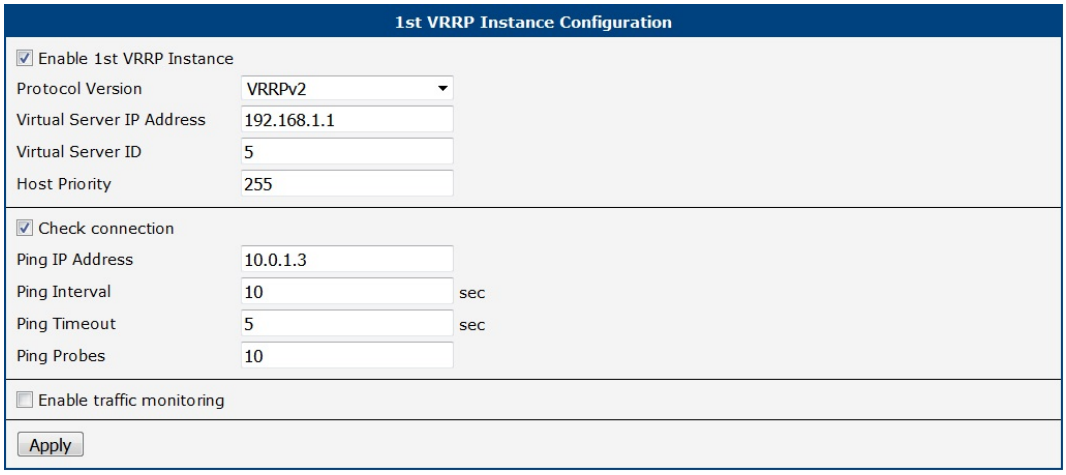


Figure 23: Example of VRRP configuration – main router

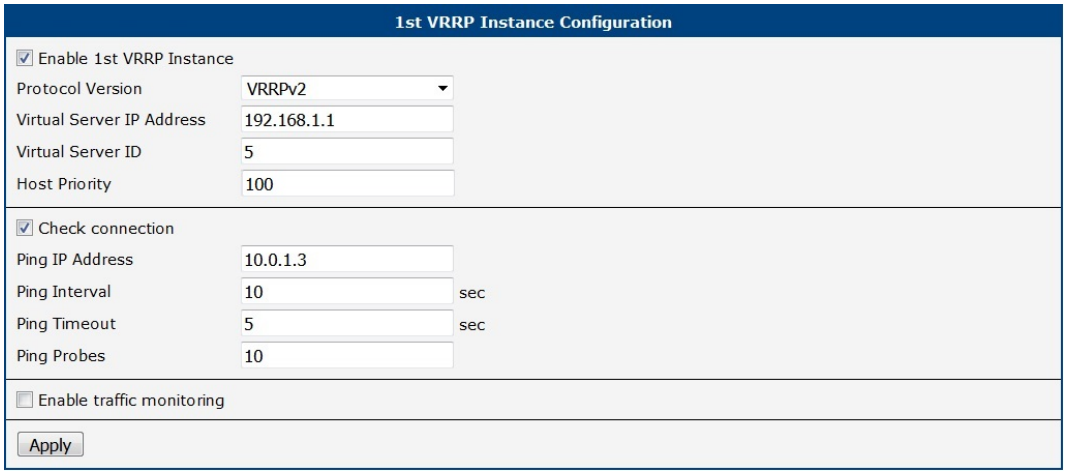


Figure 24: Example of VRRP configuration – backup router

3.3 Mobile WAN Configuration

Select the *Mobile WAN* item in the *Configuration* menu section to enter the cellular network configuration pages. The menu item will expand and you will see three separate configuration pages: *1st module*, *2nd module* and *Module Switching*. The last page – *Module Switching* – is the most important in the hierarchy of decision making when connecting to a mobile network. See the Figure below for help on where to configure decision making for each module and SIM card. The decision concerning which SIM card is used is calculated by the logical outcome of the system and the individual settings of each module and SIM card. The subpages of Mobile WAN are explained below in order of appearance on the menu.

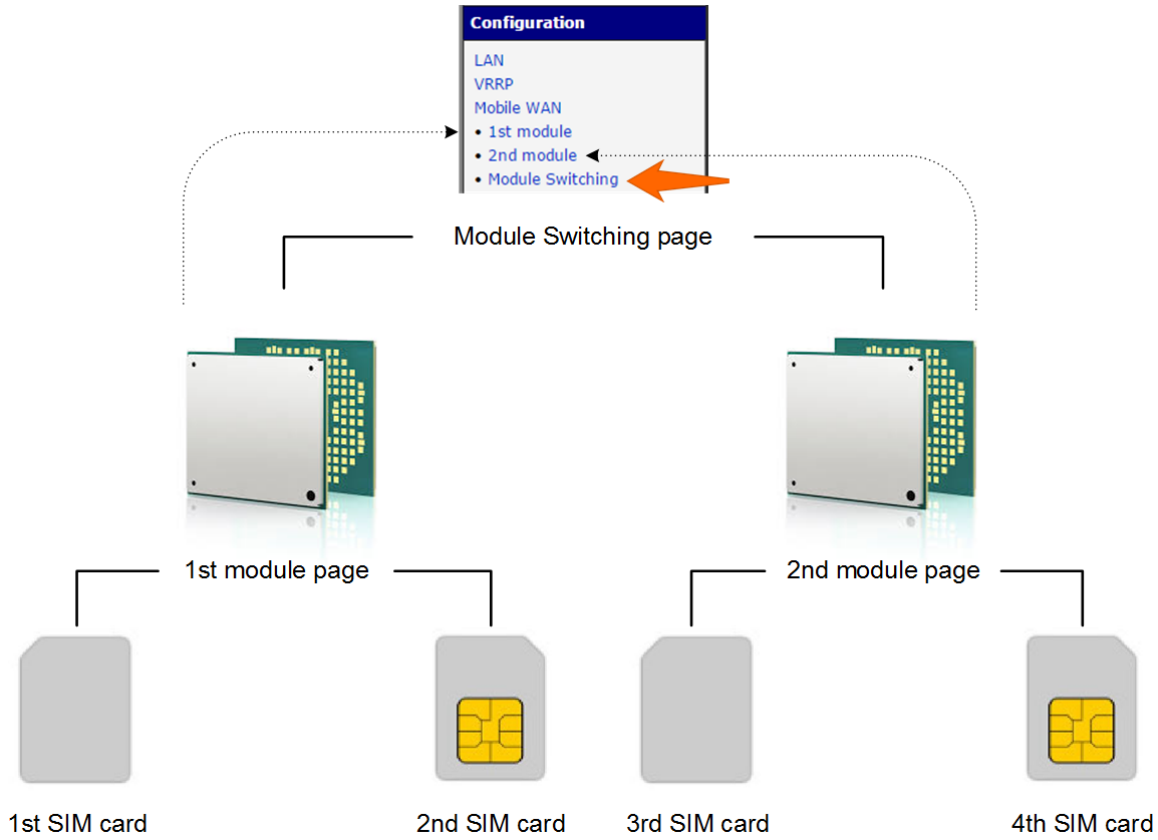


Figure 25: Switching and configuration pages structure

3.4 1st and 2nd Mobile WAN Configuration

To configure the 1st cellular module and 1st and 2nd SIM cards – go to the *1st module* configuration page, as shown in Figure 27 below. The configuration settings of the 2nd cellular module, and 3rd and 4th SIM cards are under the *2nd module* page, which has exactly the same configuration items and options as *1st module* page.

3.4.1 Connection to Mobile Network

If the *Create connection to mobile network* checkbox is checked, then 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
APN	Network identifier (Access Point Name).
Username	The user name used for logging on to the GSM network.
Password	The password used for logging on to the GSM network. Enter valid characters only, see chap. 1.1.2!
Authentication	Authentication protocol used in the GSM network: • **PAP or CHAP** – The router selects the authentication method. • **PAP** – The router uses the PAP authentication method. • **CHAP** – The router uses the CHAP authentication method.
IP Mode	Specifies the version of IP protocol used: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 independent dual stack is enabled.
IP Address	For use in IPv4 and IPv4/IPv6 mode only. Specifies the IPv4 address of the SIM card. You manually enter the IP address only when mobile network carrier has assigned the IP address.
Dial Number	Specifies the telephone number which the router dials for a GPRS or CSD connection. The router uses the default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify this parameter as the PLNM preferred carrier code.
Network type	Specifies the type of protocol used in the mobile network. • **Automatic selection** – The router automatically selects a transmission method according to the availability of transmission technologies. • It is also possible to select one of the following specific methods of data transmission: **LTE**, **UMTS/HSPA**, **GPRS/EDGE**.
PIN	Specifies the PIN used to unlock the SIM card. Use only if this is required by a given SIM card. The SIM card will be blocked after several failed attempts to enter the PIN.
MRU	Maximum Receive Unit – maximum size of packet that the router can receive via Mobile WAN. The default value is 1500 B. Other settings may cause the router to receive data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.
MTU	Maximum Transmission Unit – maximum size of packet that the router can transmit via Mobile WAN. The default value is 1500 B. Other settings may cause the router to transmit data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.

Table 21: Mobile WAN Connection Configuration

The following is a list of tips for working with the *1st/2nd Mobile WAN Configuration* form:

- If the MTU size is set incorrectly, then the router will not exceed the data transfer. If the MTU value is set too low, more frequent fragmentation of data will occur. More frequent fragmentation will mean a higher overhead and also the possibility of packet damage during defragmentation. In contrast, a higher MTU value can cause the network to drop the packet.
- If the *IP address* field is left blank, when the router establishes a connection, the mobile network carrier will automatically assign an IP address. If you assign an IP address manually, then the router will access the network quicker.
- If the ***APN*** field is left blank, the router automatically selects the APN using the IMSI code of the SIM card. The name of the chosen APN can be found in the System Log.
- If you enter the word *blank* in the *APN* field, then the router interprets the APN as blank.

The correct PIN must be filled in. An incorrect PIN may block the SIM card.

Parameters identified with an asterisk require you to enter the appropriate information only if this information is required by the mobile network carrier.

When the router is unsuccessful in establishing a connection to mobile network, you should verify accuracy of the entered data. Alternatively, you could try a different authentication method or network type.

3.4.2 DNS Address Configuration

The *DNS Settings* parameter is designed for easier configuration on the client's side. When this value is set to *get from operator* the router will attempt to automatically obtain an IP address from the primary and secondary DNS server of the mobile network carrier. To specify the IP addresses of the Primary DNS servers manually, on the *DNS Server* pull down list select the value *set manually*. You can also fill-in the IPv4 or IPv6 address of the DNS server (or both) based on the IP Mode option.

3.4.3 Check Connection to Mobile Network

Enabling the *Check Connection* function for mobile networks is necessary for uninterrupted and continuous operation of the router.

If the *Check Connection* item is set to *enabled* or *enabled + bind*, the router will be sending the ping requests to the specified domain or IP address configured in *Ping IP Address* or *Ping IPv6 Address* at regular time intervals set up in the *Ping Interval*.

In case of an unsuccessful ping, a new ping will be sent after the *Ping Timeout*. If the ping is unsuccessful three times in a row, the router will terminate the cellular connection and will attempt to establish a new one.

This monitoring function can be set for both SIM cards separately, but running on the active SIM at given time only. Be sure, you configure a functional address as the destination for the ping, for example an IP address of the operator's DNS server.

If the *Check Connection* item is set to the *enabled*, the ping requests are being sent on the basis of the routing table. Therefore, the requests may be sent through any available interface. If you require each ping request to be sent through the network interface, which was created when establishing a connection to the mobile operator, it is necessary to set the *Check Connection* to *enabled + bind*. The *disabled* option deactivates checking of the connection to the mobile network.

A note for routers connected to the **Verizon** carrier (detected by the router):
The retry interval for connecting to the mobile network prolongs with more retries. First two retries are done after 1 minute. Then the interval prolongs to 2, 8 and 15 minutes. The ninth and every other retry is done in 90 minutes interval.

If *Enable Traffic Monitoring* item is checked, the router will monitor the Mobile WAN traffic without sending the ping requests. If there is no traffic, the router will start sending the ping requests.

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

Table 22: Check Connection to Mobile Network Configuration

3.4.4 Check Connection Example

The figure below displays the following scenario: the connection to the mobile network in IPv4 *IP Mode* is controlled on the address 8.8.8.8 with a time interval of 60 seconds for the first SIM card and on the address www.google.com with the time interval 80 seconds for the second SIM card (for an active SIM only). Because the *Enable traffic monitoring* option is enabled, the control pings are not sent, but the data stream is monitored. The ping will be sent, if the data stream is interrupted.

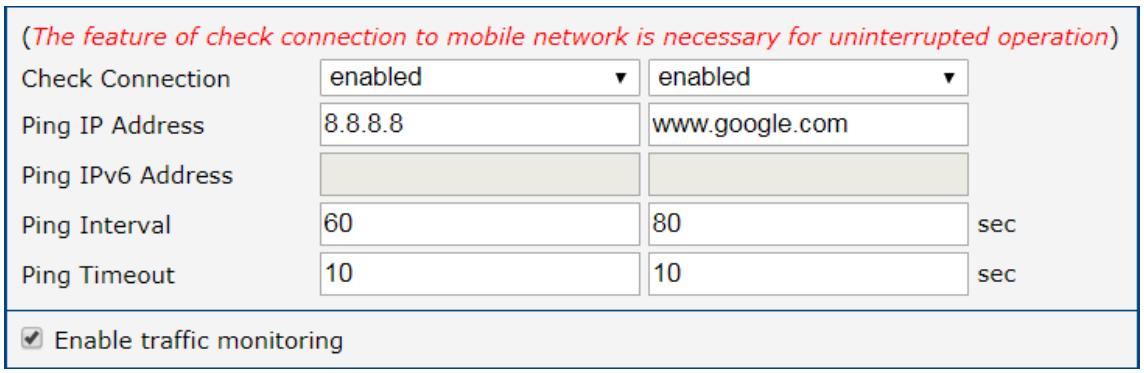


Figure 26: Check Connection Example

3.4.5 Data Limit Configuration

If the parameter *Data Limit State* (see below) is set to *not applicable* or *Send SMS when data limit is exceeded* in *SMS Configuration* is not selected, the *Data Limit* set here will be ignored.

Item	Description
Data Limit	Specifies the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (one month). Maximum value is 2 TB (2097152 MB).
Warning Threshold	Specifies a percentage of the "Data Limit" in the range of 50 % to 99 %. If the given percentage data limit is exceeded, the router will send an SMS in the following form; *Router has exceeded (value of Warning Threshold) of data limit.*
Accounting Start	Specifies the day of the month in which the billing cycle starts for a given SIM card. When the service provider that issued the SIM card specifies the start of the billing period, the router will begin to count the amount of data transferred starting on this day.

Table 23: Data Limit Configuration

3.4.6 Switch between SIM Cards Configuration

In the lower part of the *1st (2nd) Mobile WAN Configuration* page you can specify the rules for toggling between the two SIM cards.

The router will automatically toggle between the SIM cards and their individual setups depending on the configuration settings specified here (manual permission, roaming, data limit, binary inputs state). Note that the SIM card selected for connection establishment is the result of the logical product (AND) of the configuration here (table below).

Item	Description
SIM Card	Enable or disable the use of a SIM card. If you set all the SIM cards to *disabled*, this means that the entire cellular module is disabled. • **enabled** – It is possible to use the SIM card. • **disabled** – Never use the SIM card, the usage of this SIM is forbidden.
Roaming State	Configure the use of SIM cards based on roaming. This roaming feature has to be activated for the SIM card on which it is enabled! • **not applicable** – It is possible to use the SIM card everywhere. • **home network only** – Only use the SIM card if roaming is not detected.
Data Limit State	Configure the use of SIM cards based on the Data Limit set above: • **not applicable** – It is possible to use the SIM regardless of the limit. • **not exceeded** – Use the SIM card only if the Data Limit (set above) has not been exceeded.
BIN0 State	Configure the use of SIM cards based on binary input 0 state: • **not applicable** – It is possible to use the SIM regardless of BIN0 state. • **on** – Only use the SIM card if the BIN0 state is logical 0 – voltage present. • **off** – Only use the SIM card if the BIN0 state is logical 1 – no voltage.

Continued on next page

Continued from previous page

Item	Description
BIN1 State	Configure the use of SIM cards based on binary input 1 state: • **not applicable** – It is possible to use the SIM regardless of BIN1 state. • **on** – Only use the SIM card if the BIN1 state is logical 0 – voltage present. • **off** – Only use the SIM card if the BIN1 state is logical 1 – no voltage.

Table 24: Switch between SIM cards configuration

Use the following parameters to specify the decision making of SIM card switching in a particular cellular module.

Item	Description
Default SIM Card	Specifies the modules' default SIM card. The router will attempt to establish a connection to mobile network using this default. • **1st (3rd)** – The 1st (3rd) SIM card is the default one. • **2nd (4th)** – The 2nd (4th) SIM card is the default one.
Initial State	Specifies the action of the cellular module after the SIM card has been selected. • **online** – establish connection to the mobile network after the SIM card has been selected (default). • **offline** – go to the off-line mode after the SIM card has been selected. Note: If offline, you can change this initial state by SMS message only – see *SMS Configuration*. The cellular module will also go into off-line mode if none of the SIM cards are not selected.
Switch to other SIM card when connection fails	Applicable only when connection is established on the default SIM card and then fails. If the connection failure is detected by *Check Connection* feature above, the router will switch to the backup SIM card.
Switch to default SIM card after timeout	If enabled, after timeout, the router will attempt to switch back to the default SIM card. This applies only when there is default SIM card defined and the backup SIM is selected beacuse of a **failure** of the default one or if **roaming** settings cause the switch. This feature is available only when *Switch to other SIM card when connection fails* is enabled.
Initial Timeout	Specifies the length of time that the router waits before the first attempt to revert to the default SIM card, the range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	Specifies the length of time that the router waits after an unsuccessful attempt to revert to the default SIM card, the range is from 1 to 10000 min.

Continued on next page

Continued from previous page

Item	Description
Additive Constant	Specifies the length of time that the router waits for any further attempts to revert to the default SIM card. This length time is the sum of the time specified in the "Subsequent Timeout" parameter and the time specified in this parameter. The range in this parameter is from 1 to 10000 minutes.

Table 25: Parameters for SIM card switching

The cellular module will go into *offline* mode if no SIM card can be selected. In off-line mode, the *Default SIM card* is selected and the manual change of SIM card is possible via SMS only, see *SMS Configuration* in Chapter 3.19.8.

1st Mobile WAN Configuration

☑ Create connection to mobile network

	1st SIM card	2nd SIM card	
APN *	advantech.agnep.cz		
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	disabled	disabled	
Ping IP Address			
Ping IPv6 Address			
Ping Interval			sec
Ping Timeout	10	10	sec

☐ Enable traffic monitoring

Data Limit			MB
Warning Threshold			%
Accounting Start	1	1	
SIM Card	enabled	enabled	
Roaming State	not applicable	not applicable	
Data Limit State	not applicable	not applicable	
BIN0 State	not applicable	not applicable	
BIN1 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
Subsequent Timeout *		min
Additive Constant *		min

☐ Enable PPPoE bridge mode
* *can be blank*

Apply

Figure 27: 1st Mobile WAN Configuration

3.4.7 Examples of SIM Card Switching Configuration

Example 1: Timeout Configuration

Mark the *Switch to default SIM card after timeout* check box, and fill-in the following values:

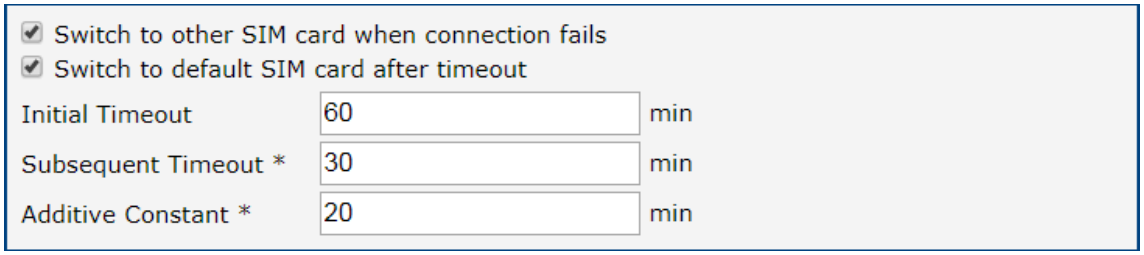


Figure 28: Configuration for SIM card switching Example 1

The first attempt to change to the default SIM card is carried out after 60 minutes. When the first attempt fails, a second attempt is made after 30 minutes. A third attempt is made after 50 minutes (30+20). A fourth attempt is made after 70 minutes (30+20+20).

Example 2: Data Limit Switching

The following configuration illustrates a scenario in which the router changes to the second SIM card after exceeding the data limit of 800 MB on the first (default) SIM card. The router sends SMS upon reaching 400 MB (this settings has to be enabled on the *SMS Configuration* page). The accounting period starts on the 18th day of the month.

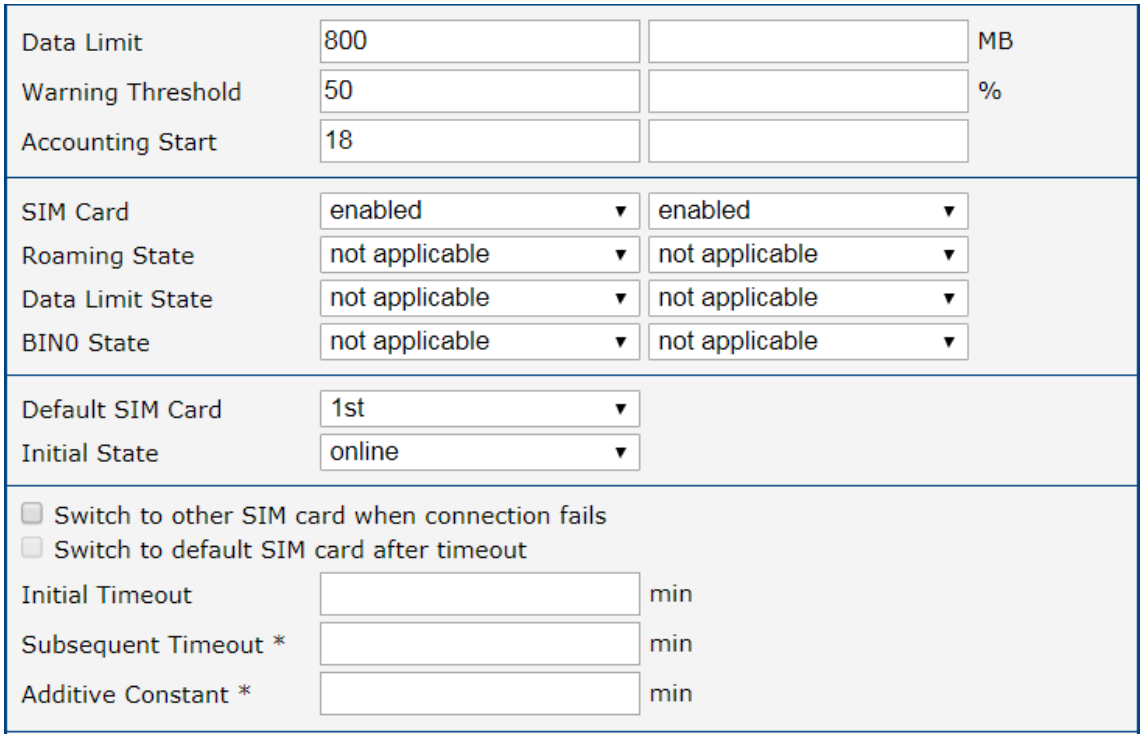


Figure 29: Configuration for SIM card switching Example 2

3.5 Module Switching Configuration

On this page you can configure the main decision process of cellular module switching. The cellular module that is selected is the result of the logical product (AND function) of the decision-making settings of the configuration on this page.

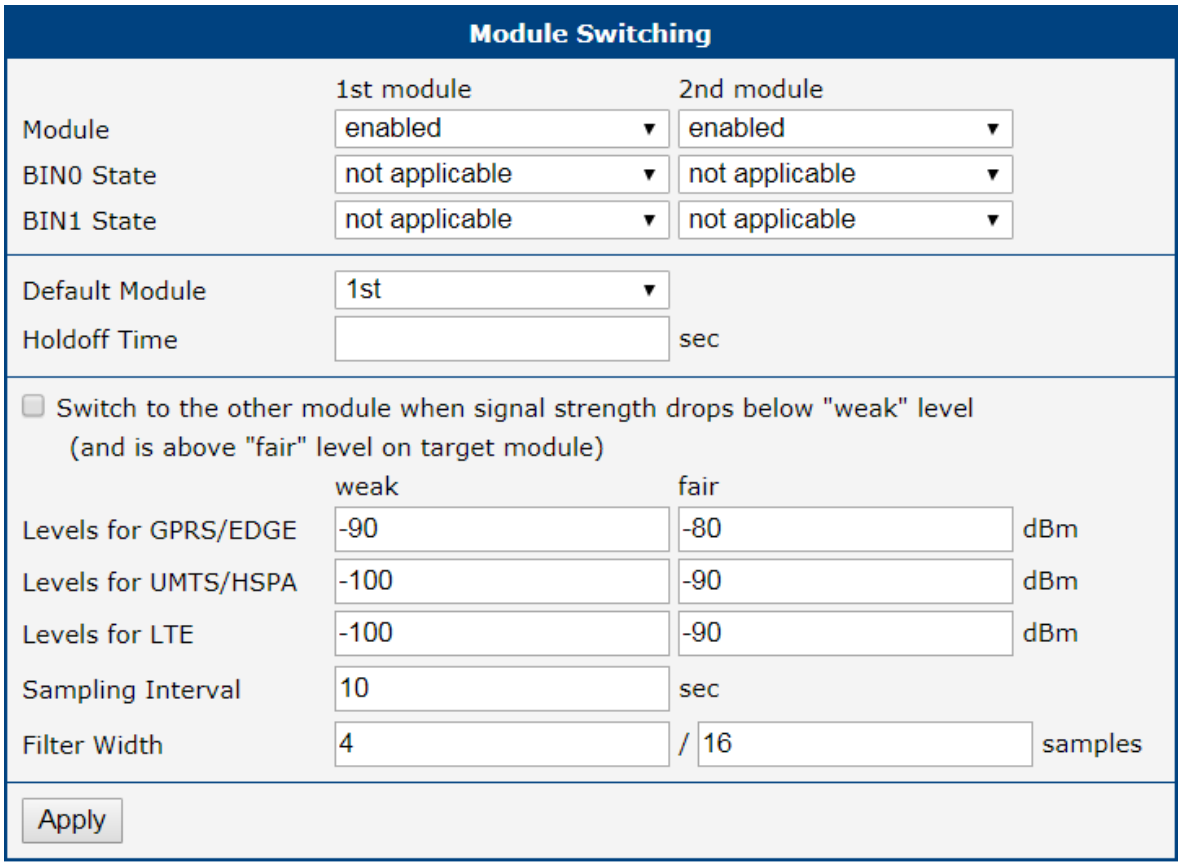


Figure 30: Module Switching Configuration

Item	Description
Module	Enable or disable the cellular module. If all the cellular modules are set to *disabled*, no connection to a cellular network is attempted. • **enabled** – It is possible to use the cellular module if the connection to the cellular network is successfully established. • **disabled** – Usage of the cellular module is forbidden, never use the cellular module.
BIN0 State	Cellular module usage based on binary input 0 state: • **not applicable** – Use the cellular module regardless of the BIN0 state. • **on** – Use the cellular module only if the BIN0 is logical 0 – voltage present. • **off** – Use the cellular module only if the BIN0 is logical 1 – no voltage.

Continued on next page

Continued from previous page

Item	Description
BIN1 State	Cellular module usage based on binary input 1 state: • **not applicable** – Use the cellular module regardless of the BIN1 state. • **on** – Use the cellular module only if the BIN1 is logical 0 – voltage present. • **off** – Use the cellular module only if the BIN1 is logical 1 – no voltage.
Default Module	Specifies the default cellular module. The router uses this default cellular module preferentially for connection to mobile network. • **none** – None cellular module is the default one. • **1st** – The 1st cellular module is the default one. • **2nd** – The 2nd cellular module is the default one.
Holdoff Time	If the default cellular module is de-selected because of a failed signal, the other cellular module is selected after this holdoff time, given in seconds. This is a protection against fast module switching. It applies only when the connection fails on the default module. Switches because of roaming, data limit, BIN or signal levels are performed immediately.
Switch to the other module when signal strength drops below the "weak" level (and is above "fair" level on target module)	This parameter enables automatic switching of cellular modules, when the signal strength of the active one drops below the specified value (and signal strength of the other one is above the specified value). Thy system will switch back to the default cellular module when the signal strength is below the "weak" level again and so on.
Levels for GPRS/EDGE	Signal strength limits for GRPS/EDGE technology.
Levels for UMTS/HSPA+	Signal strength limits for UMTS/HSPA+ technology.
Levels for LTE	Signal strength limits for LTE technology.
Sampling Interval	The period of sample taking when measuring the signal strength, given in seconds.
Filter Width	The width for calculating the moving average of loaded values of signal strength. The first value indicates the lowest number of loaded samples for which the value of a calculated average is valid and can be used to evaluate the relevant condition. The second value is a filter buffer width in the steady state when the moving average algorithm is applied (ie. if another sample is loaded, this replaces the oldest one, which means that the filter width remains constant).

Table 26: Module Switching Configuration

3.5.1 PPPoE Bridge Mode Configuration

If you mark the *Enable PPPoE bridge mode* check box on the configuration page for the first MWAN module, the router will activate the PPPoE bridge protocol. PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. This bridge mode allows you to create a PPPoE connection from a device behind the router. For example, a PC connected to the ETH port of the router. You assign the IP address of the SIM card to the PC.

For **SmartMotion ST355** routers only: If you enable *PPPoE bridge mode*, it is not possible to use *SMS Configuration* features – the router will not send SMSs and you cannot control the router via SMS! The *Send SMS* feature in the *Administration* section will not work. Also in *Mobile WAN Status* there will be no signal strength data displayed. This is caused by the use of the same channel for sending AT commands in the cellular module in this version of the router. If the channel is occupied by AT commands for PPPoE bridge, there is no place for SMS AT commands.

The changes in settings will be applied after clicking the *Apply* button.

3.6 PPPoE Configuration

PPPoE (Point-to-Point over Ethernet) is a network protocol which encapsulates PPP frames into Ethernet frames. The router uses the PPPoE client to connect to devices supporting a PPPoE bridge or server. The bridge or server is typically an ADSL router.

To open the *PPPoE Configuration* page, select the *PPPoE* menu item. If you mark the *Create PPPoE connection* check box, then the router attempts to establish a PPPoE connection after boot up. After connecting, the router obtains the IP address of the device to which it is connected. The communications from a device behind the PPPoE server is forwarded to the router.

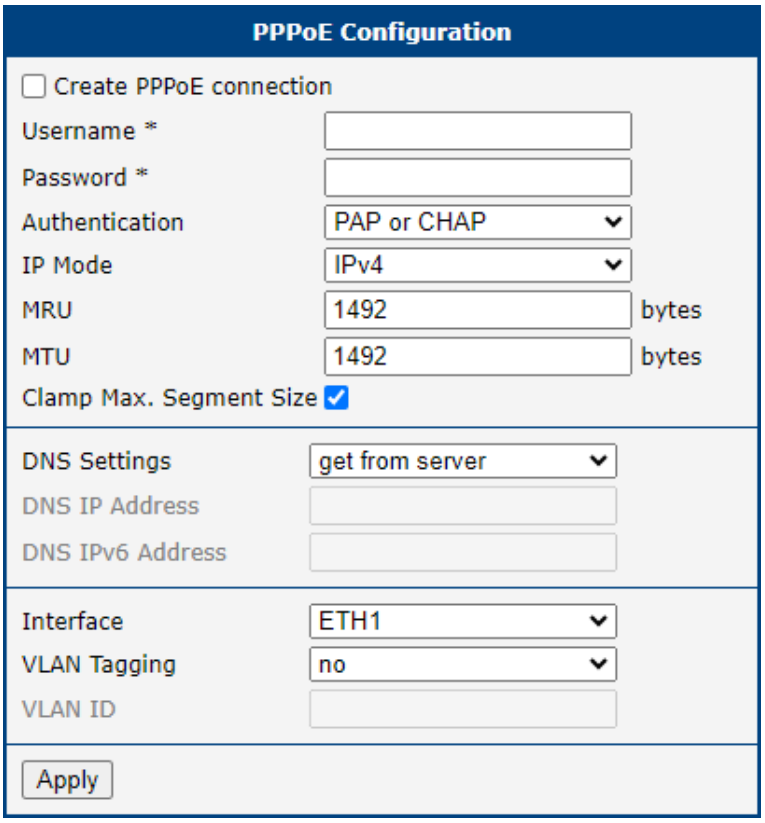


Figure 31: PPPoE Configuration

Item	Description
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only, see chap. 1.1.2!
Authentication	Authentication protocol in GSM network. • **PAP or CHAP** – The router selects the authentication method. • **PAP** – The router uses the PAP authentication method. • **CHAP** – The router uses the CHAP authentication method.

Continued on next page

Continued from previous page

Item	Description
IP Mode	Specifies the version of IP protocol: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 dual stack is enabled.
MRU	Specifies the Maximum Receiving Unit. The MRU identifies the maximum packet size, that the router can receive via PPPoE. The default value is 1492 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.
MTU	Specifies the Maximum Transmission Unit. The MTU identifies the maximum packet size, that the router can transfer in a given environment. The default value is 1492 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.
Clamp Max. Segment Size	Enhances network performance and stability by adjusting the Maximum Segment Size (MSS) of TCP packets to align with the network connection's Path Maximum Transmission Unit (PMTU). It is enabled by default.
DNS Settings	Can be set to obtain the DNS address from the server or to set it manually.
DNS IP Address	Manual setting of DNS address.
DNS IP Address	Manual setting of IPv6 DNS address.
Interface	Select an Ethernet interface.
VLAN Tagging	Select **yes** to turn on the VLAN tagging.
VLAN ID	Set the ID for VLAN tagging. The range is from 1 to 1000.

Table 27: PPPoE configuration

Setting an incorrect packet size value (MRU, MTU) can cause unsuccessful transmission.

3.7 WiFi Access Point Configuration

This feature is accessible only on routers equipped with a WiFi module.

Configuration of two separated WLANs (**Multiple SSIDs**) is supported.

Multi-role mode, which allows to operate as access point (AP) and station (STA) simultaneously, is supported. The multichannel mode is not supported, so the AP and the STA must operate on the same channel only. Please note, that only one AP can be activated together with the STA in operation.

RADIUS (Remote Authentication Dial-In User Service) networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users is supported on WiFi. The router can be RADIUS client only (not the server) – typically as a WiFi AP (Access Point) negotiating with the RADIUS server.

Activate WiFi access point mode by checking *Enable WiFi AP* box at the top of the *Configuration* → *WiFi* → *Access Point 1* or *Access Point 2* configuration pages. In this mode the router becomes an access point to which other devices in *station (STA)* mode can connect. You may set the following properties listed in the table below.

Item	Description
Enable WiFi AP	Enable WiFi access point (AP).
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Bridged	Activates bridge mode: • **no** – Bridged mode is not allowed (default value). WLAN network is not connected with LAN network of the router. • **yes** – Bridged mode is allowed. WLAN network is connected with one or more LAN networks of the router. In this case, the setting of most items in this table are ignored. Instead, the router uses the settings of the selected network interface (LAN).
Enable dynamic DHCP leases	Enable dynamic allocation of IP addresses using the DHCP (DHCPv6) server.
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
Lease Time	Time in seconds for which the client may use the IP address.
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.

Continued on next page

Continued from previous page

Item	Description
Subnet ID	The decimal value of the Subnet ID of the Ethernet inter face. Maximum value depends on the Subnet ID Width.
Subnet ID Width	The maximum Subnet ID Width depends on your Site. Prefix – it is the remainder to 64 bits.
SSID	The unique identifier of WiFi network.
Broadcast SSID	Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame. • **Enabled** – SSID is broadcasted in beacon frame • **Zero length** – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • **Clear** – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.
SSID Isolation	When enabled, by choosing a zone, a WiFi client connected to this Access Point is not able to communicate with another WiFi client connected to another Access Point, having another zone selected. This client still can communicate with a client connected to the same Access Point, unless the Client Isolation is not enabled.
Client Isolation	If checked, the access point will isolate every connected client so they do not see each other (they are in different networks, they cannot PING between each other). If unchecked, the access point behavior is like a switch, but wireless – the clients are in the same LAN and can see each other.
WMM	Basic QoS for WiFi networks is enabled by checking this item. This version doesn't guarantee network throughput. It is suitable for simple applications that require QoS.
Country Code	**This option is not available for NAM routers** – the "US" country code is set by default on these versions of router. Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a *country code* isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default *country code*. If no *country code* is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.
Follow STA radio settings	When enabled and the STA is connected to a foreign AP, the AP's radio settings will be reconfigured based on the settings of the foreign AP that the STA is currently connected to.

Continued on next page

Continued from previous page

Item	Description
HW Mode	HW mode of WiFi standard that will be supported by WiFi access point. • 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)
Channel	The channel, where the WiFi AP is transmitting. **On NAM routers only channels 1 to 11 are supported!**
Bandwidth	Allows you to choose the transfer bandwidth. Note that it may be disabled for some hardware modes, and a lower bandwidth may be used if some is occupied.
Short GI	The option for HW mode 802.11n which allows to enable the short guard interval (GI) of 400 ns instead of 800 ns.
Authentication	Access control and authorization of users in the WiFi network. • **Open** – Authentication is not required (free access point). • **Shared** – Basic authentication using WEP key. • **WPA-PSK** – Authentication using higher authentication methods PSK-PSK. • **WPA2-PSK** – WPA2-PSK using newer AES encryption. • **WPA3-PSK** – WPA3-PSK using newer AES encryption. • **WPA-Enterprise** – RADIUS authentication done by external server via username and password. • **WPA2-Enterprise** – RADIUS authentication with better encryption. • **WPA3-Enterprise** – RADIUS authentication with better encryption. • **802.1X** – RADIUS authentication with port-based Network Access Control (PNAC) using encapsulation of the Extensible Authentication Protocol (EAP) over LAN – EAPOL.

Continued on next page

Continued from previous page

Item	Description
Encryption	Type of data encryption in the WiFi network: • **None** – No data encryption. • **WEP** – Encryption using static WEP keys. This encryption method can be used for *Shared* authentication. However, it is not secure and may be unavailable for some models. • **TKIP** – Dynamic encryption key management that can be used for *WPA-PSK* and *WPA2-PSK* authentication. • **AES** – Improved encryption used for *WPA2-PSK* authentication.
WEP Key Type	Type of WEP key for WEP encryption: • **ASCII** – WEP key in ASCII format. • **HEX** – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.
WEP Key 1–4	Allows entry of four different WEP keys: • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The possible key options for WPA-PSK authentication. • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows: • **256-bit secret** – 64 hexadecimal digits • **ASCII passphrase** – 8 to 63 characters • **PSK File** – absolute path to the file containing the list of pairs (PSK key, MAC address)

Continued on next page

Continued from previous page

Item	Description
RADIUS Auth Server IP	IPv4 or IPv6 address of the RADIUS server. Only with one of RADIUS authentications selected.
RADIUS Auth Password	RADIUS server access password. Only with one of RADIUS authentications selected.
RADIUS Auth Port	RADIUS server port. The default is 1812. Only with one of RADIUS authentications selected.
RADIUS Acct Server IP	IPv4 or IPv6 address of the RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
RADIUS Acct Password	Access password of RADIUS accounting server. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
RADIUS Acct Port	RADIUS accounting server port. The default is 1813. Define only if different from the authentication and authorization server. Only with one of RADIUS authentications selected.
Access List	Mode of Access/Deny list. • **Disabled** – Access/Deny list is not used. • **Accept** – Clients in Accept/Deny list can access the network. • **Deny** – Clients in Access/Deny list cannot access the network.
Accept/Deny List	Accept or Denny list of client MAC addresses that set network access. Each MAC address is separated by new line.
Syslog Level	Logging level, when system writes to the system log. • **Verbose debugging** – The highest level of logging. • **Debugging** • **Informational** – Default level of logging. • **Notification** • **Warning** – The lowest level of system communication.
Extra options	Allows the user to define additional parameters for the hostapd. Options are added as is to the end of a configuration file. For more information, see hostapd.conf Linux man page. Use only if you know what you are doing.

Table 28: WiFi Configuration

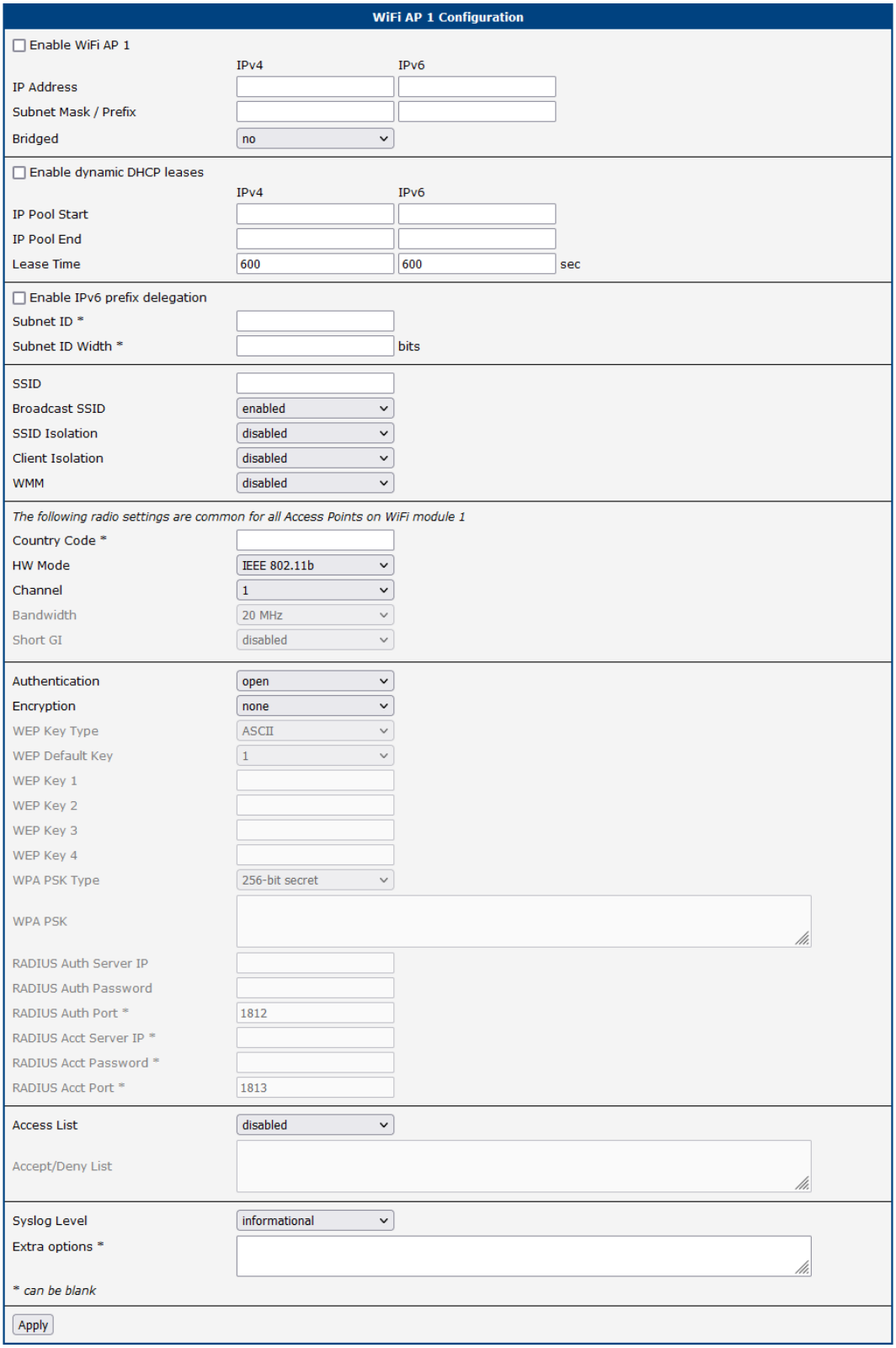


Figure 32: WiFi Access Point Configuration

3.8 WiFi Station Configuration

This feature is accessible only on routers equipped with a WiFi module.

The WiFi module supports multi-role mode which allows to operate as access point (AP) and station (STA) simultaneously. The multichannel mode is not supported, so the AP and the STA must operate on the same channel only.

Activate WiFi station mode by checking *Enable WiFi STA* box at the top of the *Configuration* → *WiFi* → *Station* configuration page. In this mode the router becomes a client station. It will receive data packets from the available access point (AP) and send data from cable connection via the WiFi network. You may set the following properties listed in the table below.

In WiFi STA mode, only the authentication method EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1) and EAP-TLS are supported.

Item	Description
Enable WiFi STA	Enable WiFi station (STA).
DHCP Client	Activates/deactivates DHCP client. If in IPv6 column, the DHCPv6 client is enabled.
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent there. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the this DNS server is requested. Use proper IP address notation in IPv4 and IPv6 column.
SSID	The unique identifier of WiFi network.
Probe Hidden SSID	AP with a hidden SSID (see Broadcast SSID option in the AP configuration) doesn't respond to broadcast probe requests, so the station doesn't have necessary info to connect. Enable this option to force the station probe a specific SSID. It's better to disable it if you don't expect a hidden SSID to avoid messing the radio with useless transmission.
Country Code	**This option is not available for NAM routers** – the "US" country code is set by default on these versions of router. Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a *country code* is not specified and the router has not implemented a system to determine this code, it will use "US" as the default *country code*. If no *country code* is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.

Continued on the next page

Continued from previous page

Item	Description
Authentication	Access control and authorization of users in the WiFi network. • **Open** – Authentication is not required (free access point). • **Shared** – Authentication based on PreShared-Keys using WEP protocol (insecure today). • **WPA-PSK** – Authentication based on PreShared-Keys using original WPA protocol (insecure today). • **WPA2-PSK** – Authentication based on PreShared-Keys using standard WPA2 protocol. • **WPA3-PSK** – Authentication based on PreShared-Keys using newest WPA3 protocol. • **WPA-Enterprise** – Authentication based on RADIUS using original WPA protocol (insecure today). • **WPA2-Enterprise** – Authentication based on RADIUS using standard WPA2 protocol. • **WPA3-Enterprise** – Authentication based on RADIUS using newest WPA3 protocol. • **802.1X** – Authentication using RADUS (802.1X standard) using WEP protocol (insecure today).
Encryption	Type of data encryption in the WiFi network: • **None** – No data encryption. • **WEP** – Encryption using static WEP keys. This encryption can be used together with Shared authentication. However, it is not secure and may be unavailable for some models. • **TKIP** – Older dynamic encryption key management that can be used together with WPA and WPA2 authentication. • **AES** – Newer dynamic encryption can be used together with WPA2 and WPA3 authentication.
WEP Key Type	Type of WEP key for WEP encryption: • **ASCII** – WEP key in ASCII format. • **HEX** – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.

Continued on the next page

Continued from previous page

Item	Description
WEP Key 1–4	Allows entry of four different WEP keys: • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The possible key option for WPA-PSK authentication. • **256-bit secret** • **ASCII passphrase** • **PSK File**
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows. • 256-bit secret – 64 hexadecimal digits • ASCII passphrase – 8 to 63 characters • PSK File – absolute path to the file containing the list of pairs (PSK key, MAC address)
RADIUS EAP Authentication	EAP protocol used to protect authentication. • **EAP-PEAP/MSCHAPv2** – use TLS only to protect legacy EAP authentication. • **EAP-TLS** – use TLS to mutual authentication of client to server and server to client with TLS.
RADIUS CA Certificate	Certification Authority Certificate to verify a server certificate when EAP-TLS is selected.
RADIUS Local Certificate	Clent certificate when EAP-TLS is selected.
RADIUS Local Private Key	Client Private Key when EAP-TLS is selected.
RADIUS Identity	Identity for connecting to RADIUS server.
RADIUS Password	Password to authenticate RADIUS Identity when EAP-PEAP/MSCHAPv2 is selected.

Continued on the next page

Continued from previous page

Item	Description
RADIUS Local Private Key Password	Password to access RADIUS Local Private Key when EAP-TLS is selected.
Syslog Level	Logging level, when system writes to the system log. • **Verbose debugging** – The highest level of logging. • **Debugging** • **Informational** – Default level of logging. • **Notification** • **Warning** – The lowest level of system communication.
Extra options	Allows the user to define additional parameters for the hostapd. Options are added as is to the end of a configuration file. For more information, see hostapd.conf Linux man page. Use only if you know what you are doing.

Table 29: WLAN Configuration

All changes in settings will apply after pressing the *Apply* button.

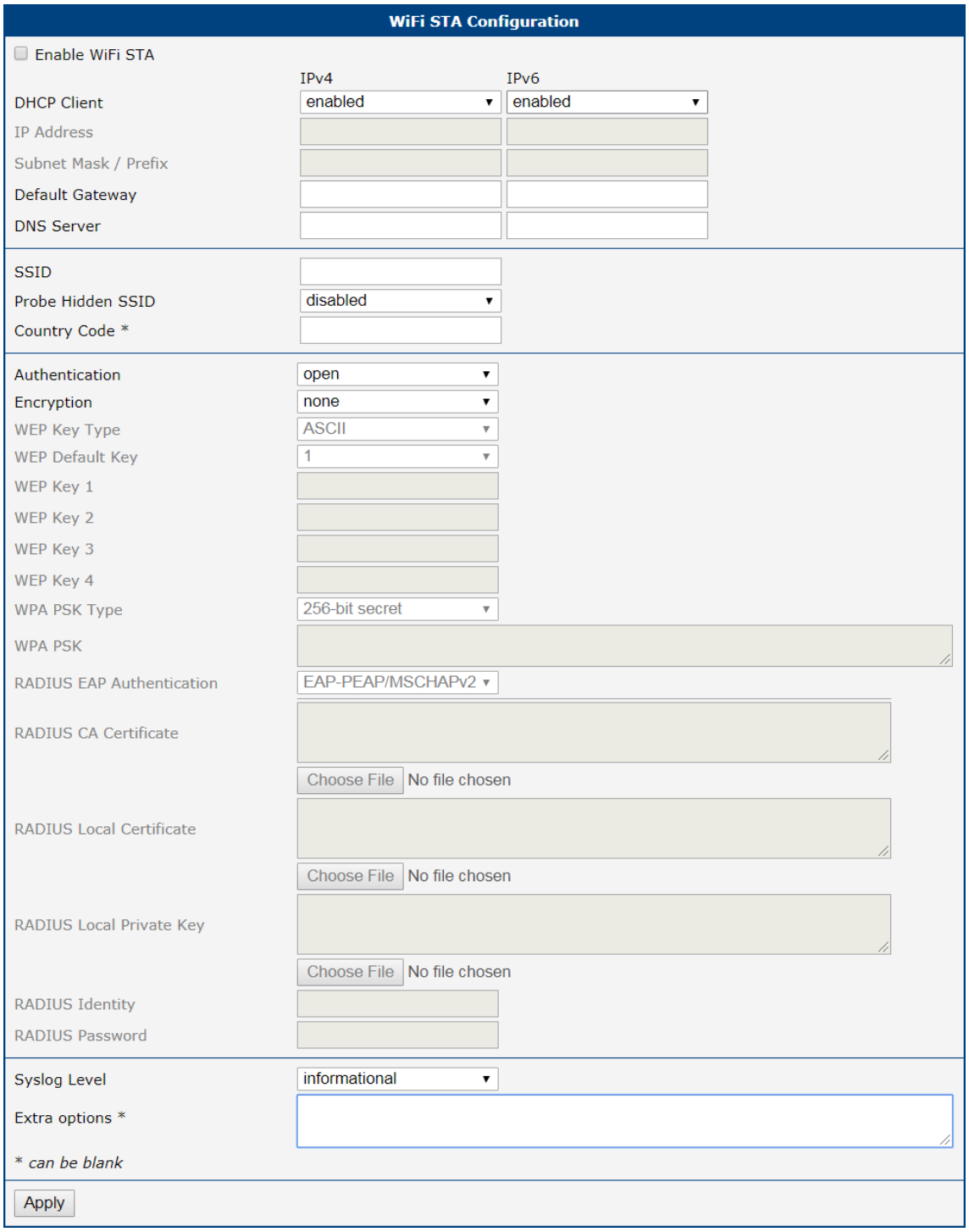


Figure 33: WiFi Station Configuration

3.9 Backup Routes

Note that some interfaces, typically WiFi, ETH2, or ETH1, may not be available for some router product lines or for the model you are currently using.

Typically, you want the router to direct traffic from the whole LAN (Local Area Network) behind the router to an external WAN (Wide Area Network) outside, such as the Internet.

Backup Routes is a mechanism that enables customizing which router's interfaces will be used for communication to the WAN outside the router. The *Backup Routes* configuration page is shown in Figure 34.

You may not care about this configuration and leave this process on the default router mechanism. In this case, leave the *Backup Routes* configuration page as it is, unconfigured, and the router will proceed as described in Chapter 3.9.1.

If you want to set up this feature your way, see Chapter 3.9.2 for more information.

3.9.1 Default Priorities for Backup Routes

By default, when the first checkbox, *Enable backup routes switching*, is unchecked, the backup routes system is not user customized and operates with the default mechanism. Instead, the router selects a route to the WAN based on the default priorities.

The following is the list of the network interfaces in descending order from the highest priority to the lowest priority interface for use as a WAN interface.

1. **Mobile WAN** (pppX, usbX)
2. **PPPoE** (ppp0)
3. **WiFi STA** (wlan0)
4. **ETH1** (eth1)
5. **ETH2** (eth2)
6. **ETH0** (eth0)

For example, based on the list above, we can say that the ETH1 interface will only be used as the WAN interface if Mobile WAN, PPPoE, and WiFI STA interfaces are down or disabled.

It is clear from the above that an interface connected to a LAN network can take over the role of a WAN interface under certain circumstances. Possible communication from the LAN to the WAN can be blocked or forwarded rules configured on the *NAT* and *Firewall* configuration pages.

Note that an ETH interface won't be used as WAN for the default backup route priorities if neither an IP address is configured nor the DHCP client is enabled for this ETH interface.

Just for the default priorities mode: Unplugging the Ethernet cable does not switch the WAN interface to the next one in order.

3.9.2 User Customized Backup Routes

You can choose preferred router interfaces acting as the WAN, including their priorities, on the *Backup Routes* configuration page; see Figure 34. Switching between the WAN is then carried out according to the order of priority and the state of all the affected interfaces.

There are three different modes you can choose for the connection backup as described in Table 30.

Item	Description
Enable backup routes switching	Enables the customized backup routes setting made **on the whole configuration page**. If disabled (unchecked), the backup routes system operates in the default mechanism, as described in Chapter 3.9.1.
Mode	**Single WAN** • Just **one interface** is used for the WAN communication **at a time**. • Other interfaces (if enabled) are used as the backup routes for the WAN communication when the active interface fails (based on the priorities set). • Just one interface, currently active, is allowed to access the router from a network outside the router. **Multiple WANs** • Just **one interface** is used for the WAN communication **at a time**. • Other interfaces (if enabled) are used as the backup routes for the WAN communication when the active interface fails (based on the priorities set). • The router is accessible from networks outside on all enabled interfaces. This is the **only difference** from the *Single WAN* mode. **Load Balancing** • In this mode, it is possible to split the volume of data passing through individual WAN interfaces. • If the mode was chosen, the weight for every interface is enabled in the GUI and can be set. • This setting determines the relative number of data streams passing through the interfaces.

Table 30: Backup Routes Modes

You have now selected a backup route mode. To add a network interface to the backup routes system, mark the enable checkbox of that interface. Enabled interfaces are used for WAN access based on their priorities.

Note for Load Balancing mode: The weight setting for load balancing may not precisely match the amount of balanced data. It depends on the number of data flows and the data structure. The best result of the balancing is achieved for a high amount of data flows.

Note for Mobile WAN: If you want to use a mobile WAN connection as a backup route, choose the *enable + bind* option in the *Check Connection* item on the *Mobile WAN* page and fill in the ping address; see chapter 3.4.1.

Note for an ETH interface: Unlike the default backup route mode, disconnecting the Ethernet cable from an ETH interface switches the route to the next in the sequence.

Settings, which can be made for each interface, are described in the table below. Any changes made to settings will be applied after pressing the *Apply* button.

Item	Description
Priority	Priority for the type of connection (network interface).
Ping IP Address	Destination IPv4 address or domain name of ping queries to check the connection.
Ping IPv6 Address	Destination IPv6 address or domain name of ping queries to check the connection.
Ping Interval	The time interval between consecutive ping queries.
Ping Timeout	Time in seconds to wait for a response to the ping.
Weight	Weight for the Load Balancing mode only. The number from 1 to 256 determines the ratio for load balancing of the interface. For example, if two interfaces set the weight to 1, the ratio is 50% to 50%. If they set the weight up to 1 and 4, the ratio is 20% to 80%.

Table 31: Backup Routes Configuration

Other notes:

- The system checks the status state of an interface. For example, unlike the *Default Priorities* mode, unplugging the Ethernet cable triggers a switchover to the next WAN interface in the sequence.
- To monitor the interface availability, you can use one or both Ping IP Addresses (IPv4 and IPv6) based on the IP protocol used on a particular network interface and WAN connection settings.

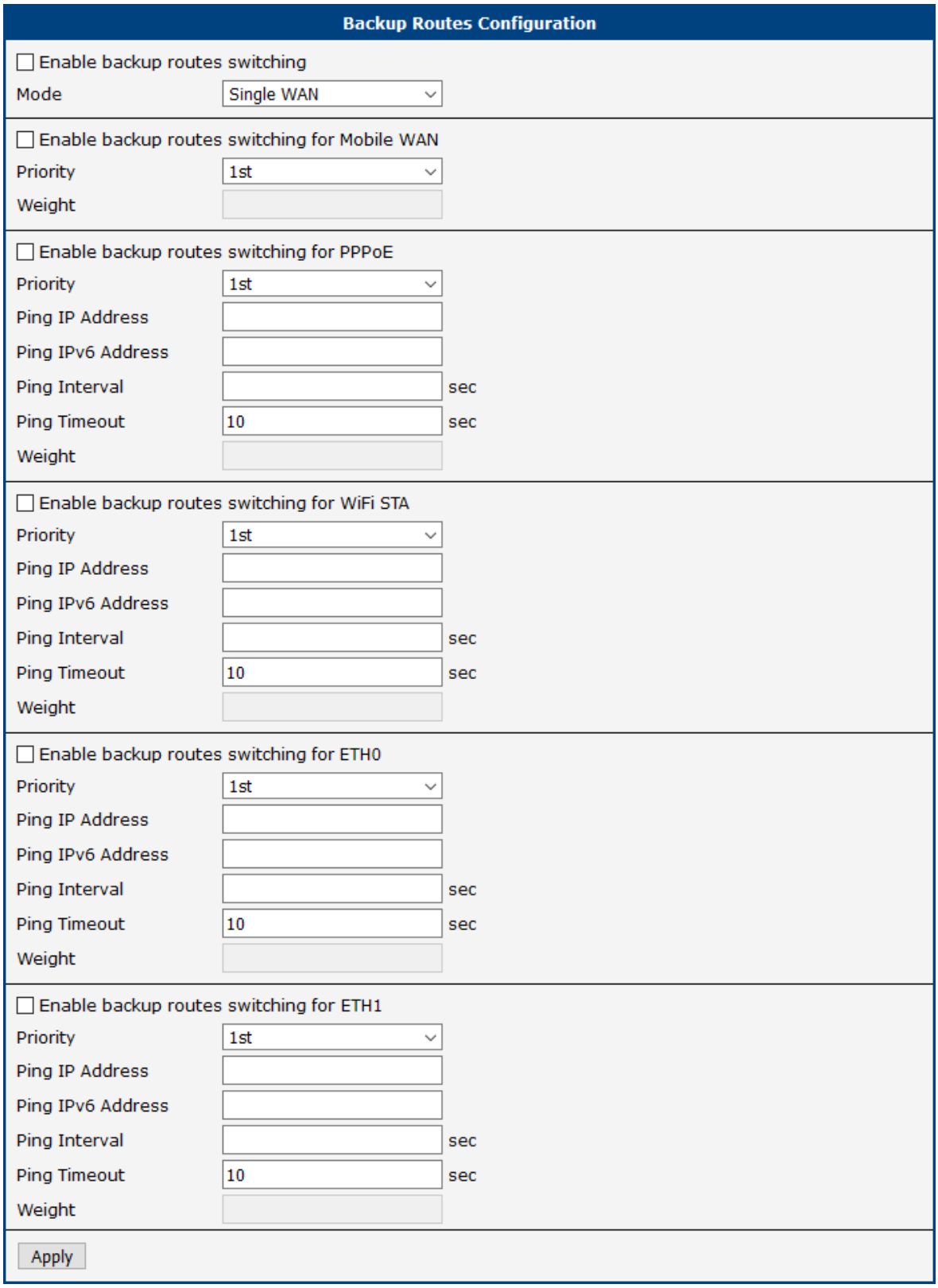


Figure 34: Backup Routes Configuration GUI

3.9.3 Backup Routes Examples

Example #1: Default Settings

As already described above, by default, if the *Backup Routes* are unconfigured, the system operates with the default priorities as described in Chapter 3.9.1. Figure 35 shows the GUI configuration.

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

Figure 35: Example #1: GUI Configuration

Figure 36 illustrates the example topology.

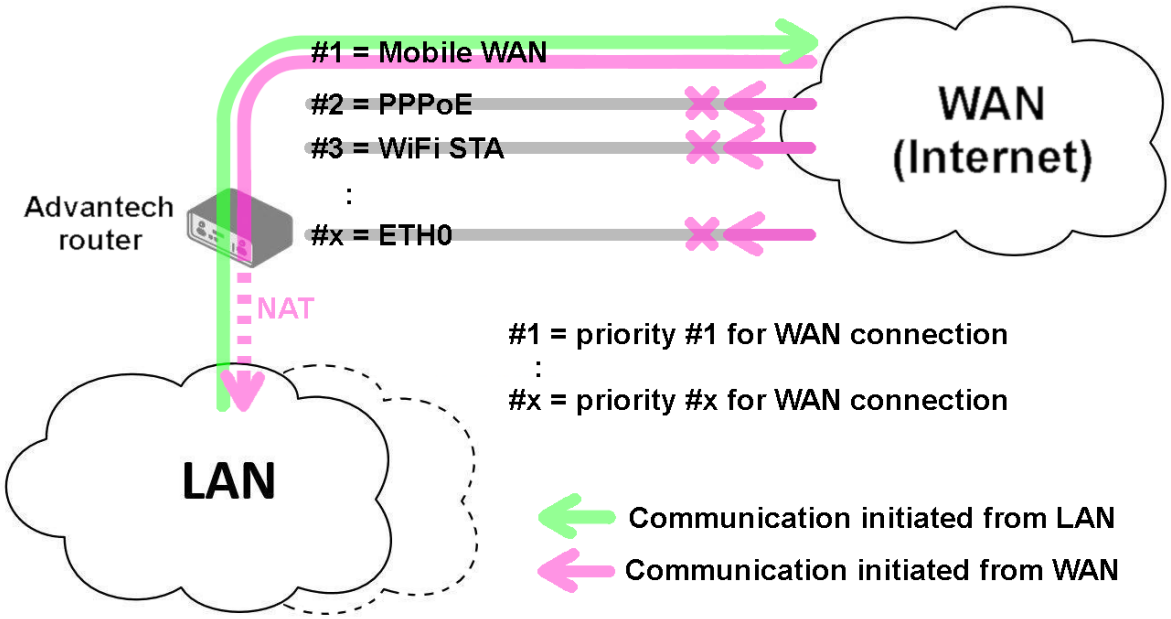


Figure 36: Example #1: Topology

Example #2: Default Routes Switching

This example illustrates when the interface, primarily used for the WAN connection, is down. Its role is taken over by the interface with the second highest priority. Since the *Backup Routes* configuration is still unconfigured, the system operates with the default system priorities described in Chapter 3.9.1. Figure 37 shows the GUI configuration.

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

Figure 37: Example #2: GUI Configuration

Figure 38 illustrates the example topology.

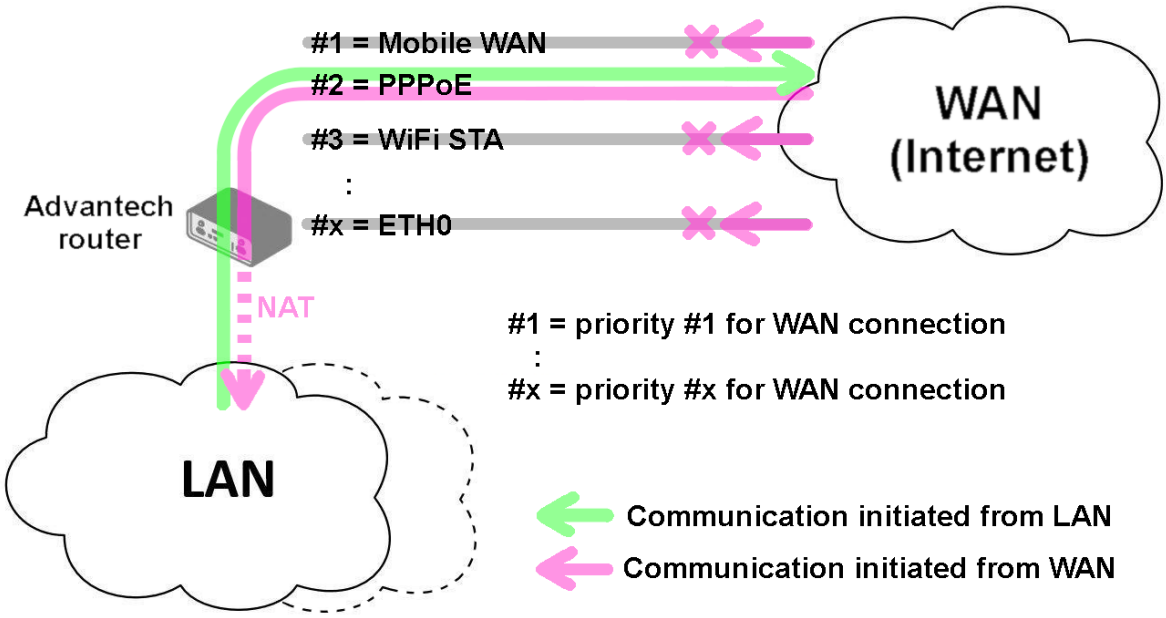


Figure 38: Example #2: Topology

Example #3: Custom Backup Routes

This example illustrates the configuration of custom backup routes for the Mobile WAN, PPPoE, and ETH1 interfaces. The Mobile WAN interface has the highest priority, and the ETH1 interface has the lowest priority. Figure 39 shows the GUI configuration.

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

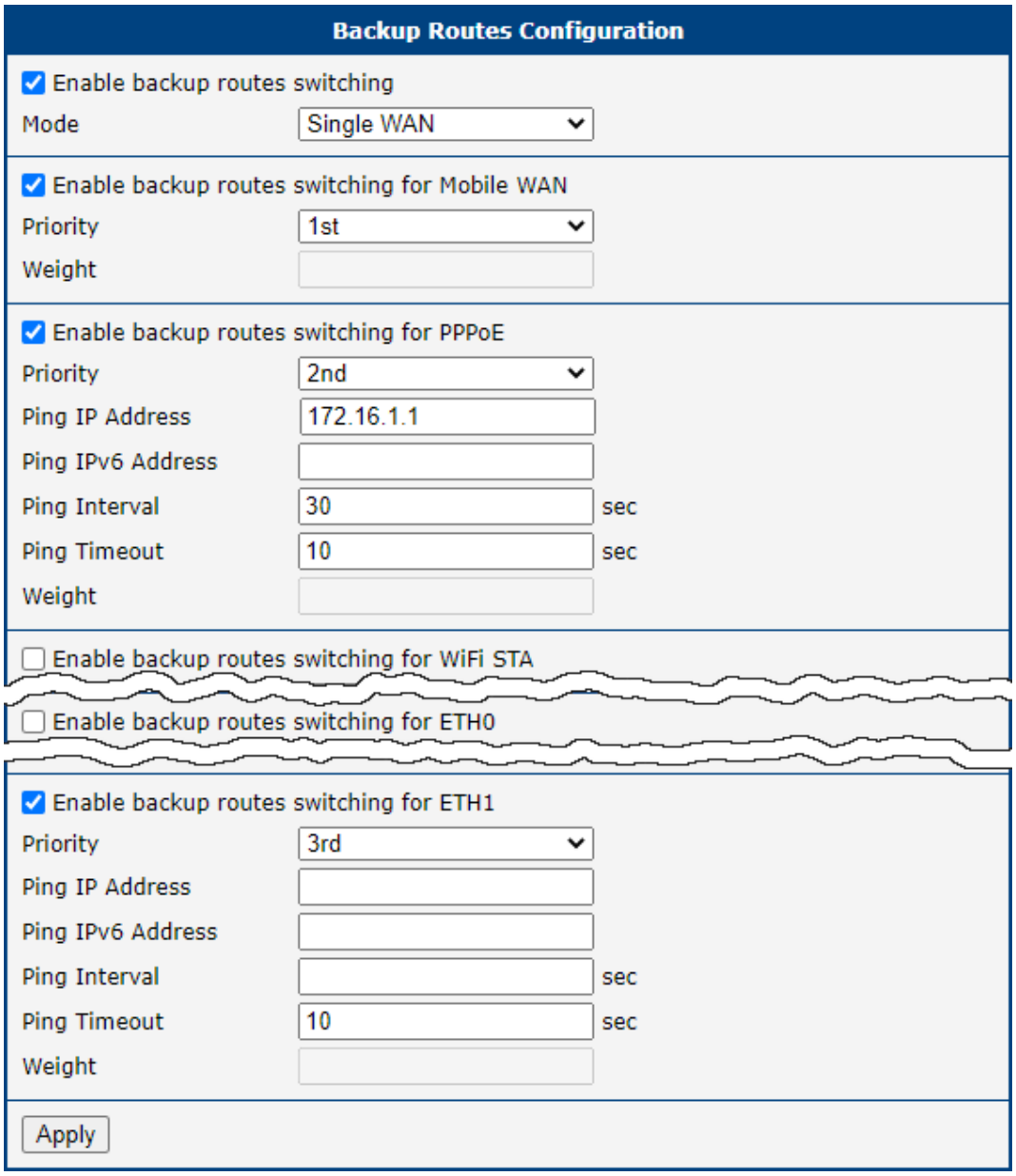


Figure 39: Example #3: GUI Configuration

Figure 40 illustrates the example topology for *Single WAN* mode. If the Mobile WAN connection goes down, the PPPoE tunnel takes its role, and so on. The ping to the 172.16.1.1 address, tested every 30 seconds with a timeout of 10 seconds, checks the status of the PPPoE tunnel.

Figure 41 illustrates the example topology for *Multiple WAN* mode. As you can see, the only difference between these two modes is that in the *Multiple WAN* mode, the router is accessible on all interfaces from the WAN simultaneously.

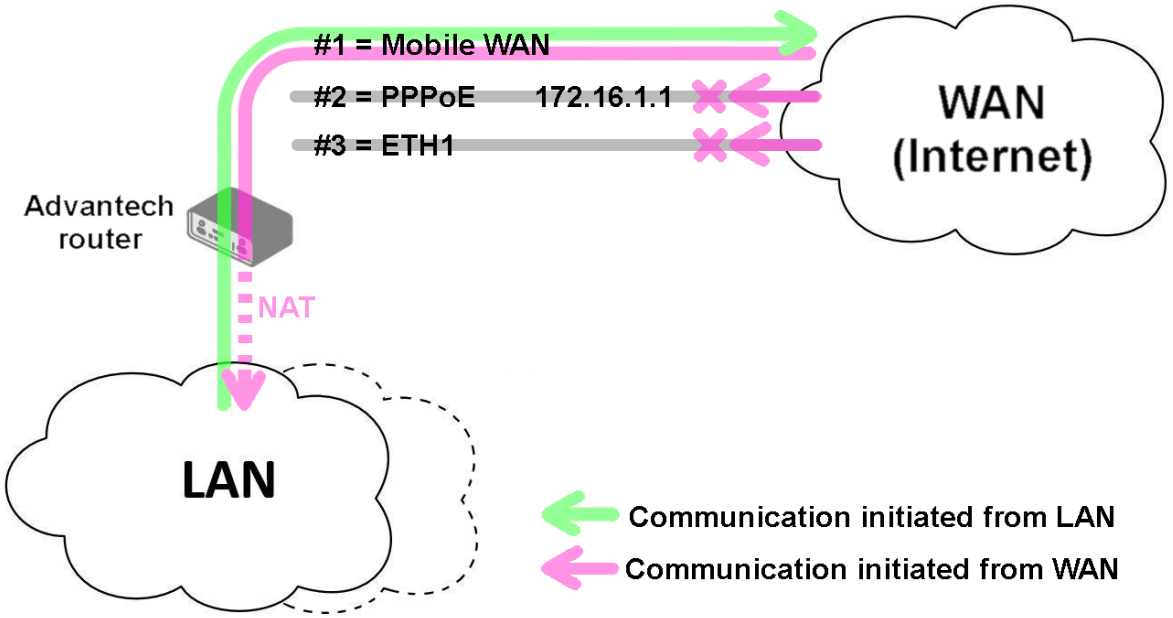


Figure 40: Example #3: Topology for *Single WAN* mode

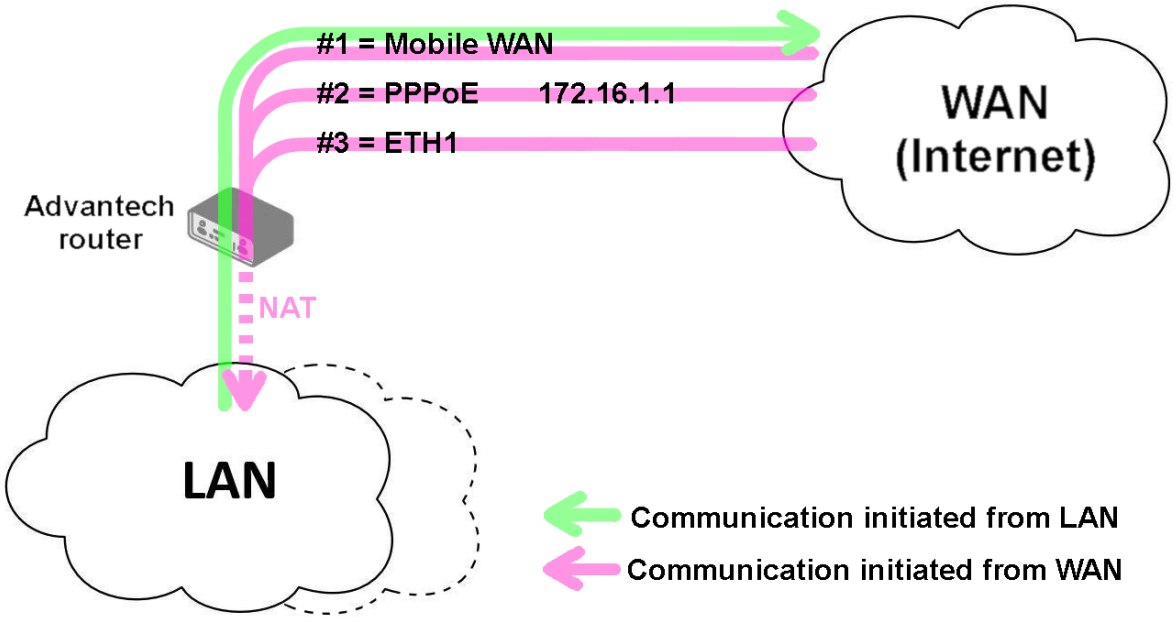


Figure 41: Example #3: Topology for *Multiple WAN* mode

Example #4: Load Ballancing Mode #1

If both cellular modules are enabled, the weight set for the MWAN is applied to both cellular modules. For that reason, the total weight for the MWAN is double.

In this example, the only one enabled is the MWAN interface. Because the entry of the weight field is mandatory, it is set to 1, but it has no significance. Because both cellular modules are enabled and running, 50 % of data streams are directed to the first cellular module and 50 % to the second cellular module. Figure 42 shows the GUI configuration.

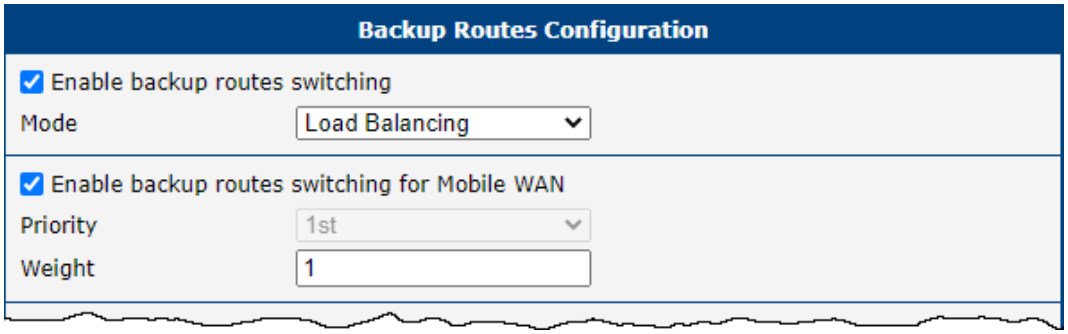


Figure 42: Example #4: GUI Configuration

Figure 43 illustrates the example topology.

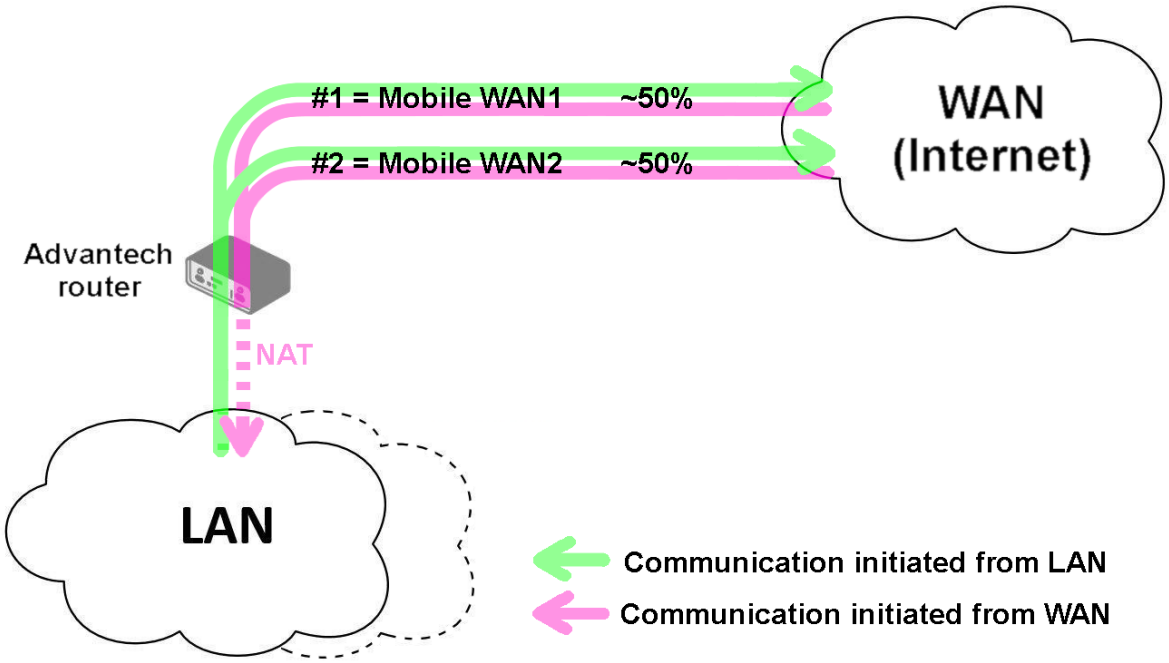


Figure 43: Example #4: Topology

Example #5: Load Ballancing Mode #2

In this are enabled the MWAN and PPPoE interfaces. The weight set to the MWAN is 2 (2 to the first and 2 to the second cellular module – total weight is 4) and 1 to the PPPoE. Because both cellular modules are enabled and running, 40 % of data streams are directed to the first cellular module, 40 % to the second cellular module and 20 % to the PPPoE. Figure 44 shows the GUI configuration.

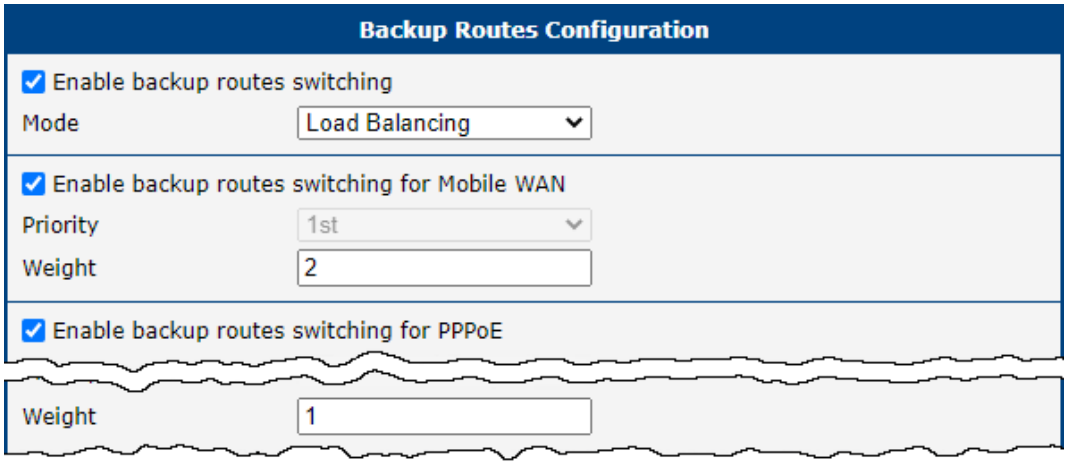


Figure 44: Example #5: GUI Configuration

Figure 45 illustrates the example topology.

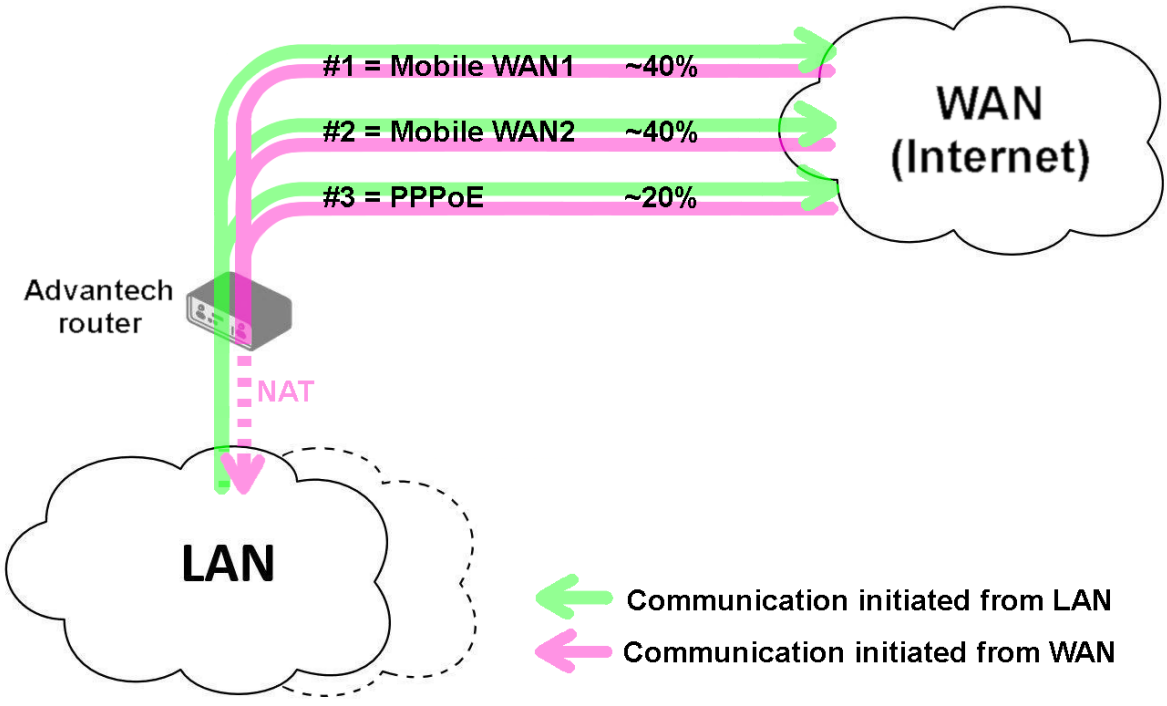


Figure 45: Example #5: Topology

Example #6: Load Ballancing Mode #3

In this example are enabled the MWAN, WiFi STA and 2nd LAN interfaces. The weight set to MWAN is 1 (1 to the first and 1 to the second cellular module – tolal weight is 2), 1 to the WiFi STA and 1 to the 2nd LAN. Because both cellular modules are enabled and running, 25 % of data streams are directed to the first cellular module, 25 % to the second cellular module, 25 % to the WiFi STA and 25 % to the 2nd LAN. Figure 46 shows the GUI configuration. Figure 47 illustrates the example topology.

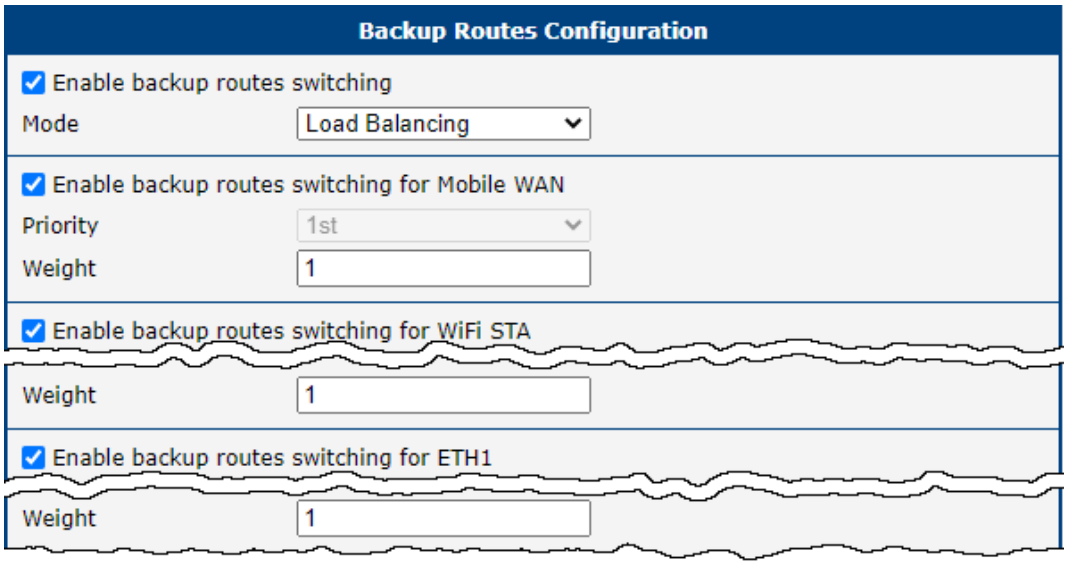


Figure 46: Example #6: GUI Configuration

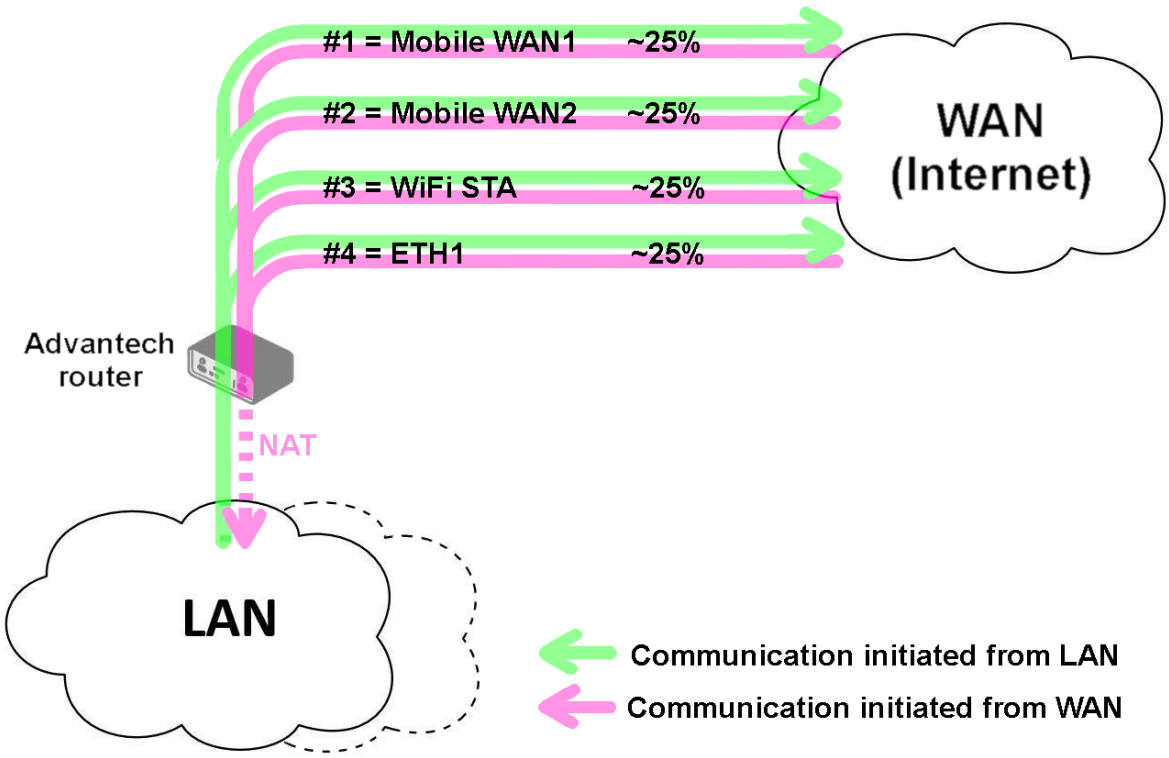


Figure 47: Example #6: Topology

Example #7: No WAN Routes

This example illustrates when *Router Backup* is enabled but no specific interface is selected for the WAN route. In this case, the router has no dedicated WAN interface and routes the traffic within the LANs. Figure 48 shows the GUI configuration.

Note: The Mobile WAN interface is not accessible, even if configured and connected to a cellular network.

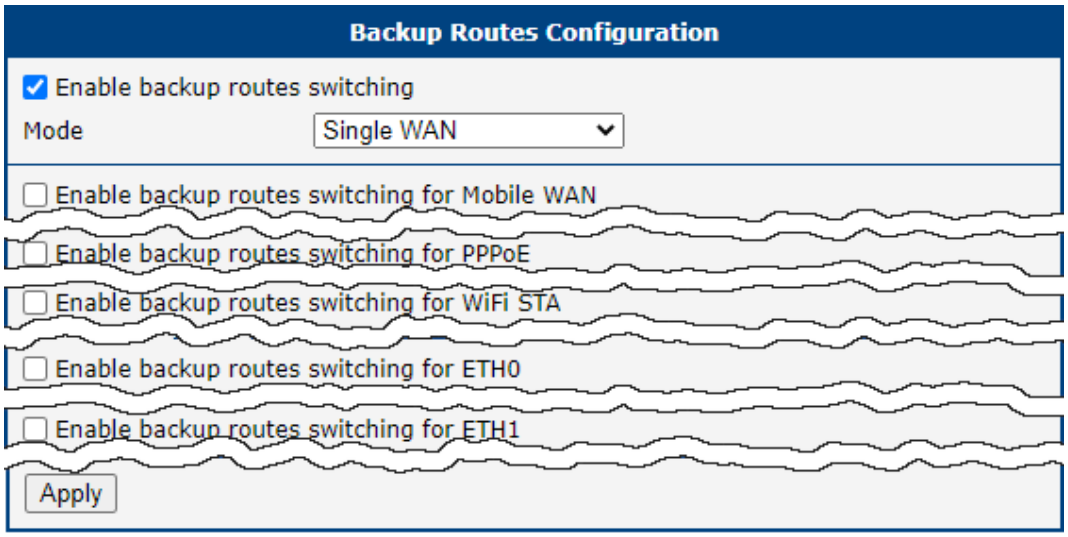


Figure 48: Example #7: GUI Configuration

Figure 49 illustrates the example topology.

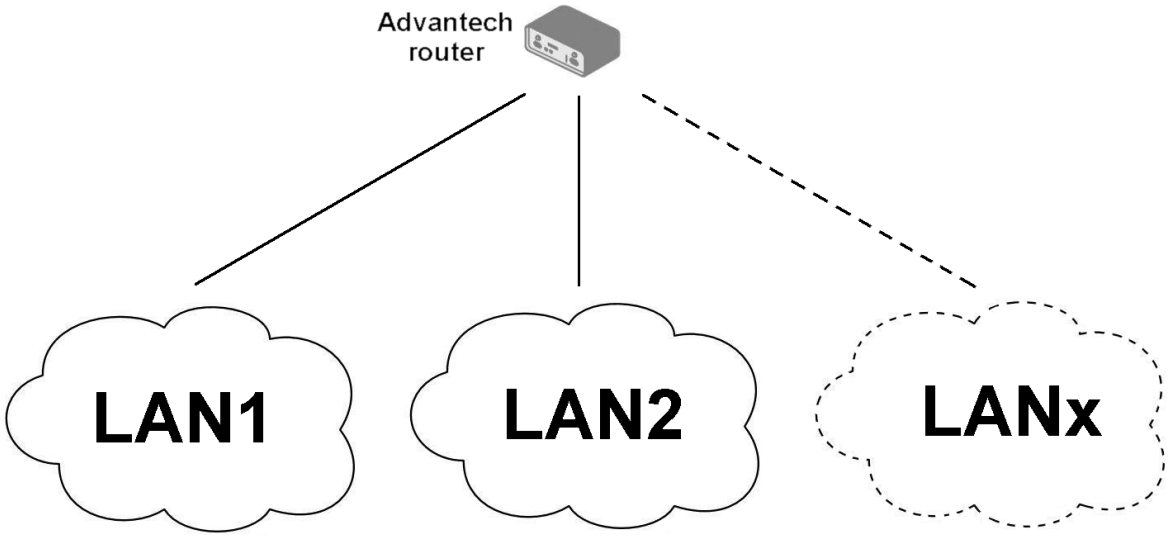


Figure 49: Example #7: Topology

3.10 Static Routes

Static routes can be specified on the *Static Routes* configuration page. A static route provide fixed routing path through the network. It is manually configured on the router and must be updated if the network topology was changed recently. Static routes are private routers unless they are redistributed by a routing protocol. There are two forms, one for IPv4 and the second for IPv6 configuration. Static routes configuration form for IPv4 is shown on Figure 50.

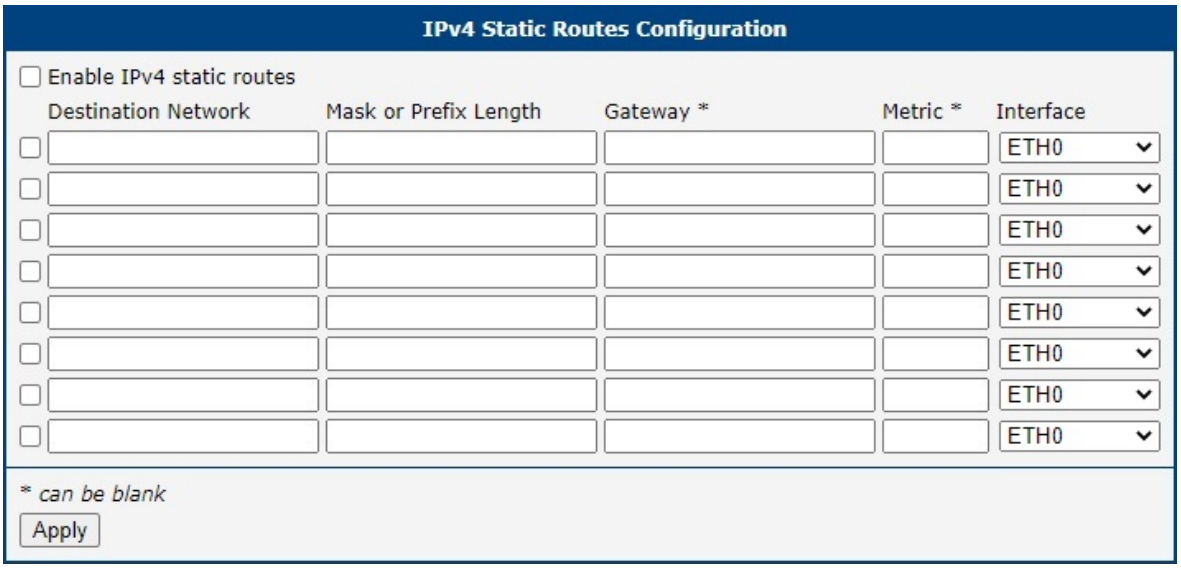


Figure 50: Static Routes Configuration

The description of all items is listed in Table 32.

Item	Description
Enable IPv4 static routes	If checked, static routing functionality is enabled. Active are only routes enabled by the checkbox in the first column of the table.
Destination Network	The destination IP address of the remote network or host to which you want to assign a static route.
Mask or Prefix Length	The subnet mask of the remote network or host IP address.
Gateway	IP address of the gateway device that allows for contact between the router and the remote network or host.
Metric	Metric definition, means number rating of the priority for the route in the routing table. Routes with lower metrics have higher priority.
Interface	Select an interface the remote network or host is on.

Table 32: Static Routes Configuration for IPv4

3.11 Firewall Configuration

The first security element for incoming packets is a check of the enabled source IP addresses and destination ports. There is an independent IPv4 and IPv6 firewall since there is dual stack IPv4 and IPv6 implemented in the router. If you click the *Firewall* item in the *Configuration* menu on the left, it will expand to *IPv4* and *IPv6* optionsm and you can click *IPv6* to enable and configure the IPv6 firewall – see Figure below. The configuration fields have the same meaning in the *IPv4 Firewall Configuration* and *IPv6 Firewall Configuration* forms.

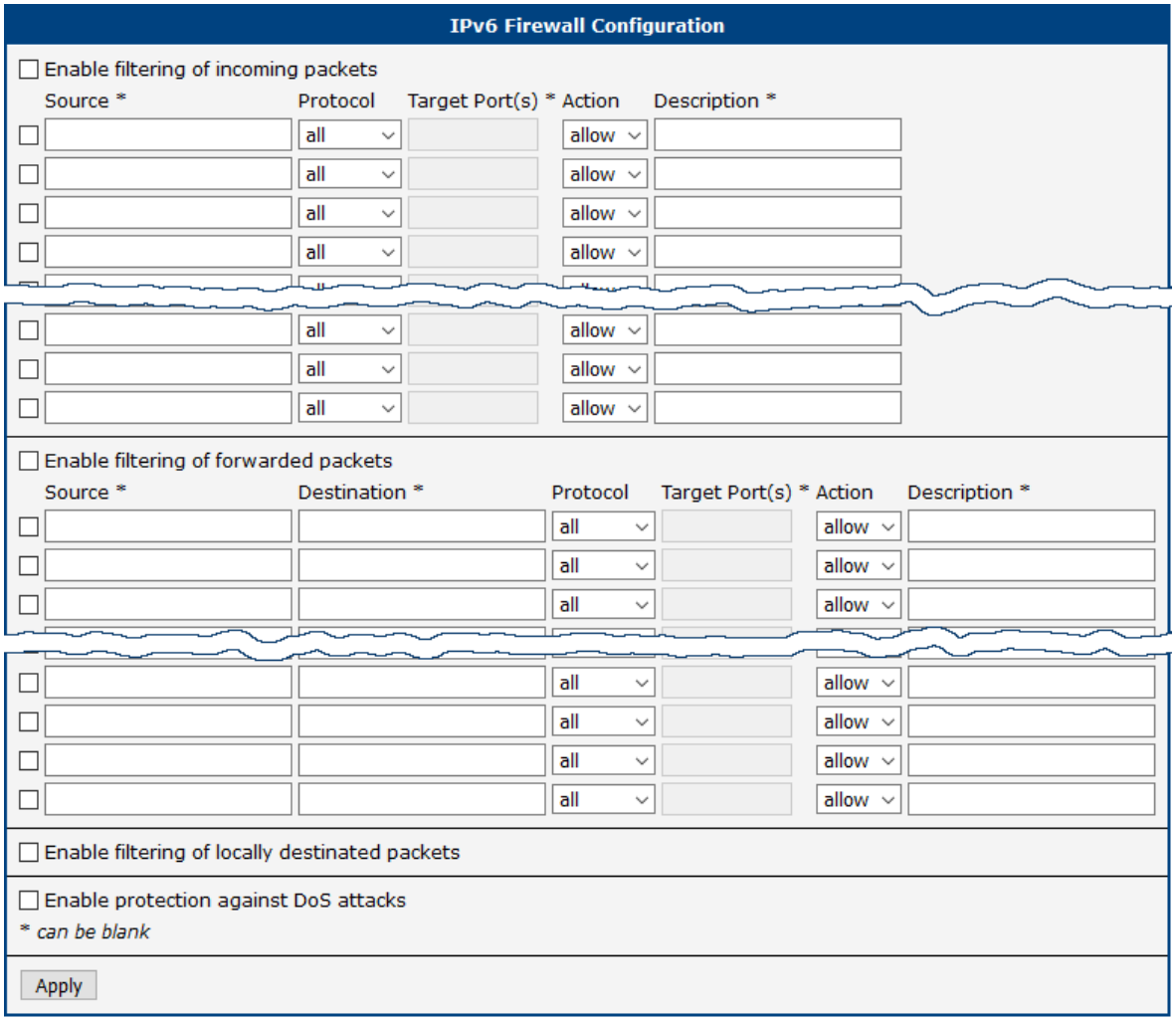


Figure 51: Firewall Configuration – IPv6 Firewall

The first section of the configuration form specifies the incoming firewall policy. If the *Enable filtering of incoming packets* check box is unchecked, all incoming packets are accepted. If checked, and a packet comes from the WAN interface, then the router forwards this packet to the INPUT iptable chain. When the INPUT chain accepts the packet, and there is a rule matching this packet with the *Action* set to *allow*, the router accepts the packet. The packet is dropped if an INPUT rule is unavailable or the *Action* is set to *deny*. You can specify the rules for IP addresses, protocols, and ports to allow or deny access to the router and internal network behind the router. It is possible to specify up to sixteen rules when each rule can be enabled/disabled by ticking the checkbox on the left of the rule row. Please note that the incoming rules are **applied to the WAN interface only**. See Chapter 3.9.1 to see the priority rules for the WAN interfaces. See Table 33 for the incoming definition table description.

Item	Description
Source	IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.
Protocol	Specifies the protocol the rule applies to: • **all** – The rule applies to all protocols. • **TCP** – The rule applies to TCP protocol. • **UDP** – The rule applies to UDP protocol. • **GRE** – The rule applies to GRE protocol. • **ESP** – The rule applies to ESP protocol. • **ICMP**/**ICMPv6** – The rule applies to ICMP protocol. In *IPv6 Firewall Configuration* there is the ICMPv6 option.
Target Port(s)	The port numbers range allowing access to the router. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network.
Description	Description of the rule.

Table 33: Filtering of Incoming Packets

The next section of the configuration form specifies the forwarding firewall policy. If the *Enabled filtering of forwarded packets* check box is unchecked, all incoming packets are accepted. If checked, and a packet is addressed to another network interface, then the router forwards this packet to the FORWARD iptable chain. When the FORWARD chain accepts the packet, and there is a rule for forwarding it, the router forwards the packet. If a forwarding rule is unavailable, then the packet is dropped. It is possible to specify up to sixteen rules when each rule can be enabled/disabled by ticking the checkbox on the left of the rule row. The forwarding setting is applied to all interfaces, regardless of whether it is the WAN interface. The configuration form also contains a table for specifying the filter rules. It is possible to create a rule to allow data with the selected protocol specifying only the protocol or to create stricter rules by specifying values for source IP addresses, destination IP addresses, and ports. See Table 34 for the forwarding definition table description.

Item	Description
Source	IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.
Destination	Destination IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.

Continued on next page

Continued from previous page

Item	Description
Protocol	Specifies the protocol the rule applies to: • **all** – The rule applies to all protocols. • **TCP** – The rule applies to TCP protocol. • **UDP** – The rule applies to UDP protocol. • **GRE** – The rule applies to GRE protocol. • **ESP** – The rule applies to ESP protocol. • **ICMP**/**ICMPv6** – The rule applies to ICMP protocol. In *IPv6 Firewall Configuration* there is the ICMPv6 option.
Target Port(s)	The target port numbers. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network.
Description	Description of the rule.

Table 34: Forwarding filtering

When you enable the *Enable filtering of locally destined packets* function, the router drops the packets requesting an unsupported service. The packet is dropped automatically without any information.

As a protection against DoS attacks, the *Enable protection against DoS attacks* limits the number of allowed connections per second to five. The DoS attack floods the target system with meaningless requirements.

3.11.1 Example of the IPv4 Firewall Configuration

The router allows the following access:

- From IP address 171.92.5.45 using any protocol.
- From IP address 10.0.2.123 using the TCP protocol on port 1000.
- From IP address 142.2.26.54 using the ICMP protocol.
- from IP address 142.2.26.54 using the TCMP protocol on target ports from 1020 to 1040

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

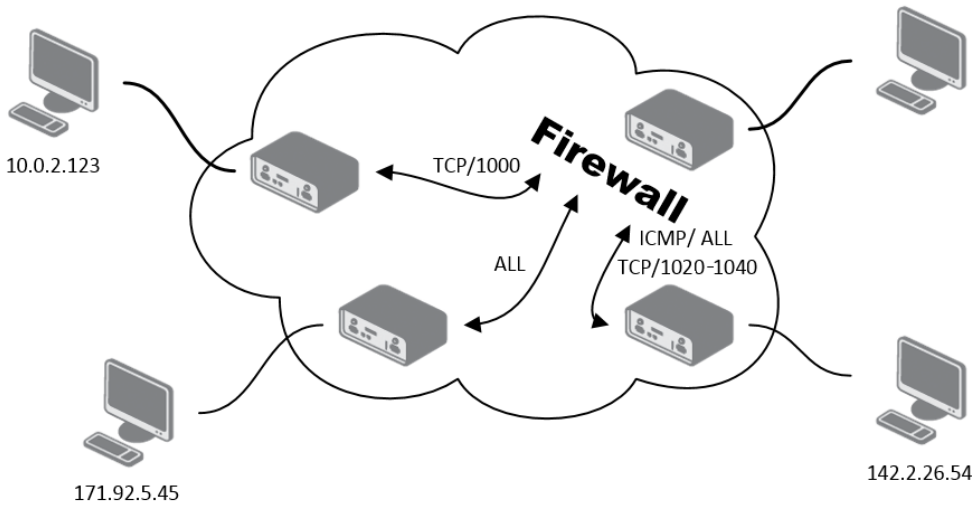


Figure 52: Topology for the IPv4 Firewall Configuration Example

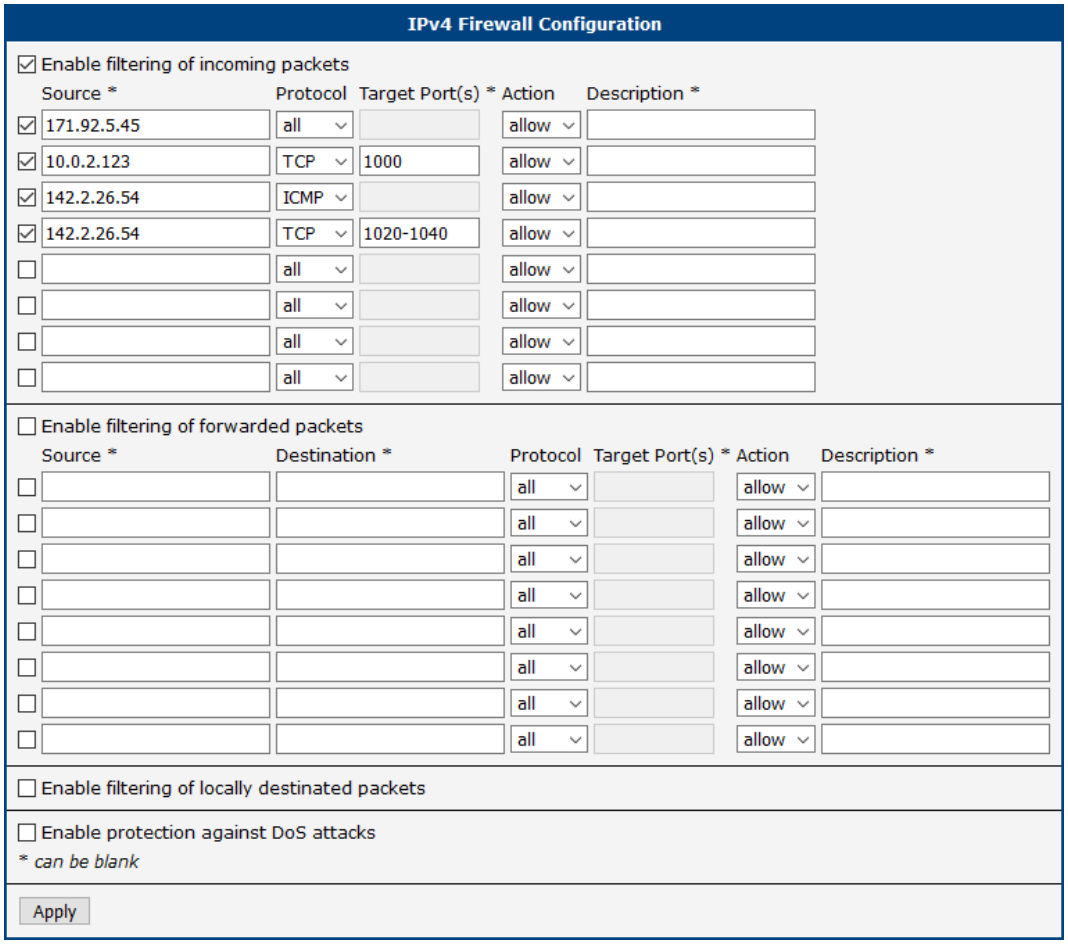


Figure 53: IPv4 Firewall Configuration Example

3.12 NAT Configuration

To configure the address translation function, click on *NAT* in the *Configuration* section of the main menu. There is independent IPv4 and IPv6 NAT configuration since there is dual stack IPv4 and IPv6 implemented in the router. The *NAT* item in the menu on the left will expand to *IPv4* and *IPv6* options and you can click *IPv6* to enable and configure the IPv6 NAT – see Figure below. The configuration fields have the same meaning in the *IPv4 NAT Configuration* and *IPv6 NAT Configuration* forms.

The router actually uses Port Address Translation (PAT), which is a method of mapping a TCP/UDP port to another TCP/UDP port. The router modifies the information in the packet header as the packets traverse a router. This configuration form allows you to specify up to 16 PAT rules.

Item	Description
Public Port(s)	The public port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Private Port(s)	The private port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Type	Protocol type – TCP or UDP.
Server IPv4 address	In *IPv4 NAT Configuration* only. IPv4 address where the router forwards incoming data.
Server IPv6 address	In *IPv6 NAT Configuration* only. IPv6 address where the router forwards incoming data.
Description	Description of the rule.

Table 35: NAT Configuration

If you require more than sixteen NAT rules, insert the remaining rules into the Startup Script. The *Startup Script* dialog is located on *Scripts* page in the *Configuration* section of the menu. When creating your rules in the Startup Script, use this command for IPv4 NAT:

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

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in place of square brackets.
For IPv6 NAT use `ip6tables` command with same options.:

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

If you enable the following options and enter the port number, the router allows you to remotely access to the router from WAN (Mobile WAN) interface.

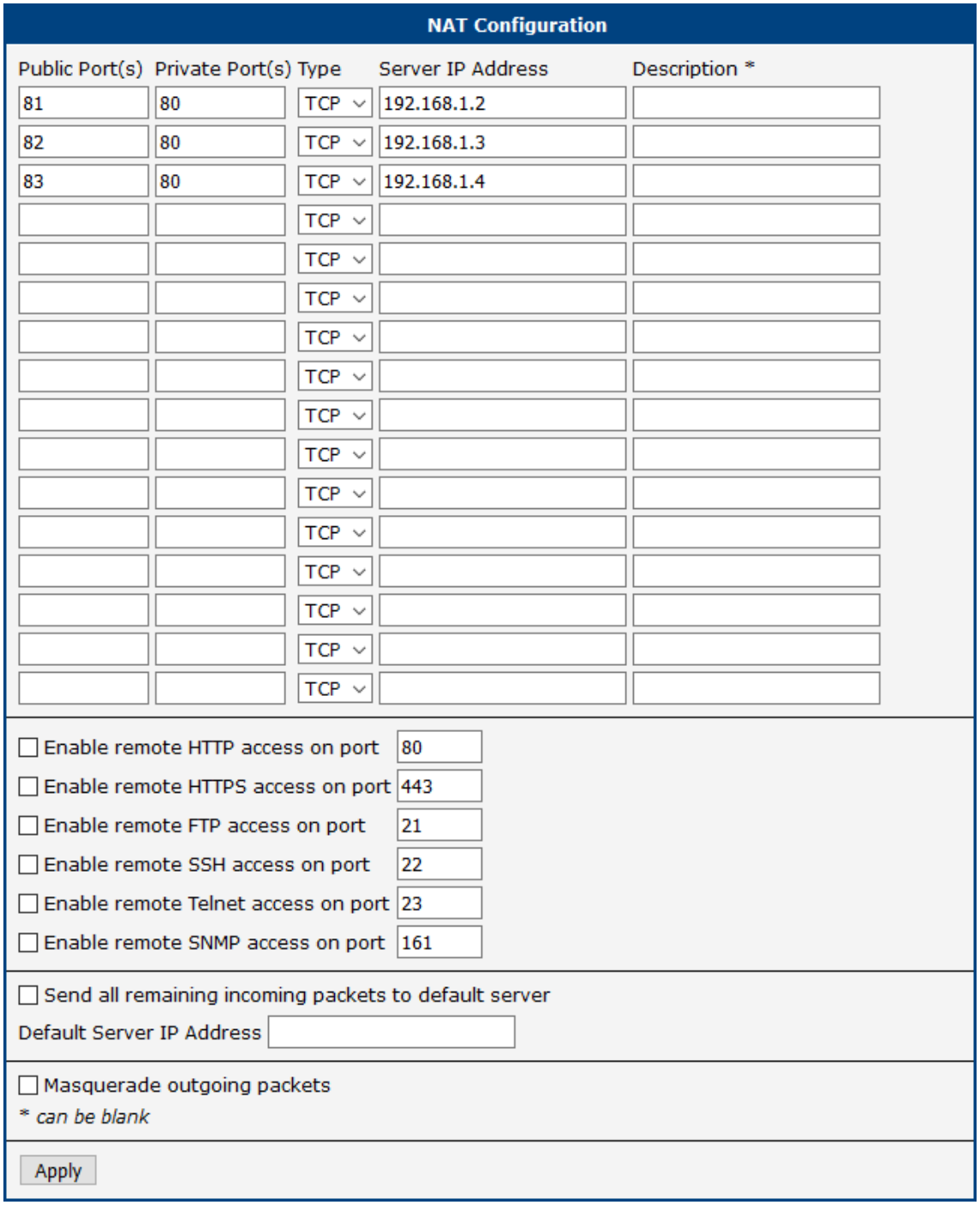


Figure 54: NAT – IPv6 NAT Configuration

Item	Description
Enable remote HTTP access on port	This option **sets the redirect** from HTTP to HTTPS **only** (disabled in default configuration).
Enable remote HTTPS access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote FTP access on port	Select this option to allow access to the router using FTP (disabled in default configuration).
Enable remote SSH access on port	Select this option to allow access to the router using SSH (disabled in default configuration).
Enable remote Telnet access on port	Select this option to allow access to the router using Telnet (disabled in default configuration).
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP (disabled in default configuration).
Masquerade outgoing packets	Activates/deactivates the network address translation function.

Table 36: Remote Access Configuration

Enable remote HTTP access on port activates **the redirect from HTTP to HTTPS protocol only**. The router doesn't allow unsecured HTTP protocol to access the web configuration. To access the web configuration, always check the *Enable remote HTTPS access on port* item. Never enable the HTTP item only to access the web configuration from the Internet (configuration would not be accessible from the Internet). Always check the HTTPS item or HTTPS and HTTP items together (to set the redirect from HTTP).

Use the following parameters to set the routing of incoming data from the WAN (Mobile WAN) to a connected computer.

Item	Description
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for the function is that you specify a default server in the *Default Server IPv4/IPv6 Address* field. The router can forward incoming data from a mobile WAN to a computer with the assigned IP address.
Default Server IP Address	In *IPv4 NAT Configuration* only. The IPv4 address.
Default Server IPv6 Address	In *IPv6 NAT Configuration* only. The IPv6 address.

Table 37: Configuration of Send all incoming packets to server

3.12.1 Examples of NAT Configuration

Example 1: IPv4 NAT Configuration with Single Device Connected

It is important to mark the *Send all remaining incoming packets to default server* check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the *Default Server IPv4 Address* field. The connected device replies if a PING is sent to the IP address of the SIM card.

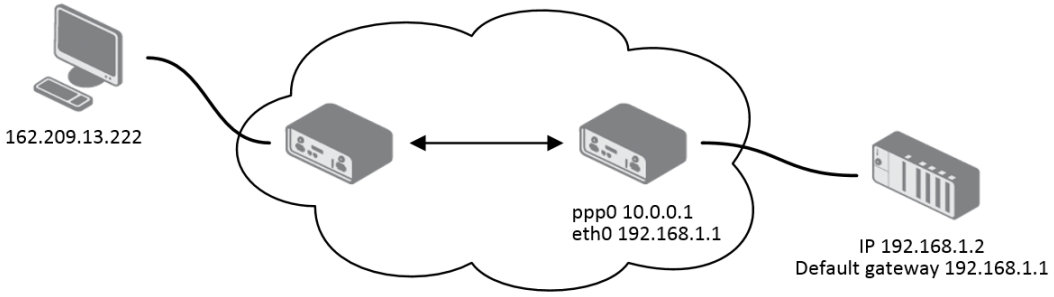


Figure 55: Topology for NAT Configuration Example 1

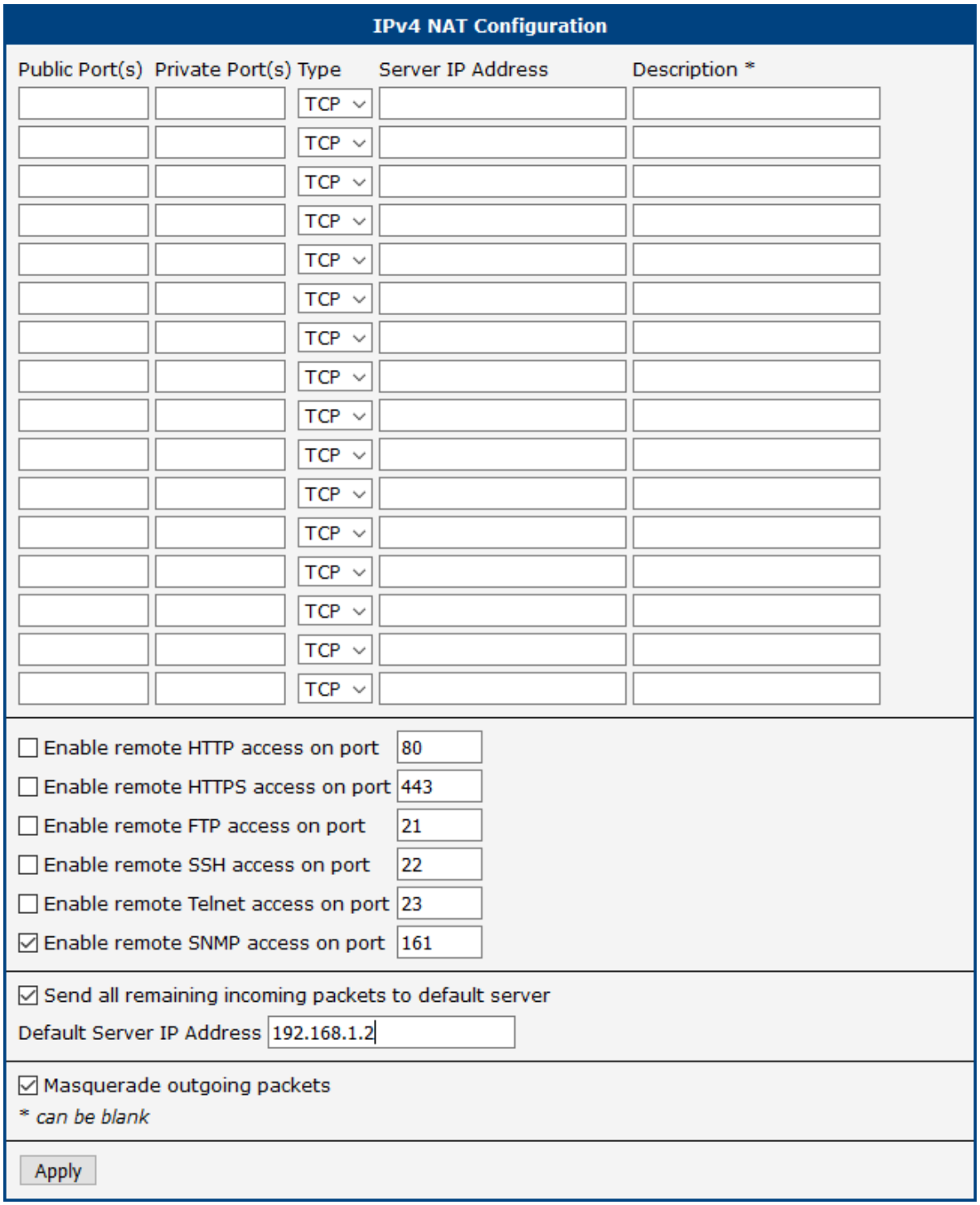


Figure 56: NAT Configuration for Example 1

Example 2: IPv4 NAT Configuration with More Equipment Connected

In this example, using the switch you can connect more devices behind the router. Every device connected behind the router has its own IP address. Enter the address in the *Server IPv Address* field in the *NAT* dialog. The devices are communicating on port 80, but you can set port forwarding using the *Public Port* and *Private Port* fields in the NAT dialog. You have now configured the router to access the 192.168.1.2:80 socket behind the router when accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (not forwarding). And since the *Send all remaining incoming packets to default server* is inactive, the router denies connection attempts.

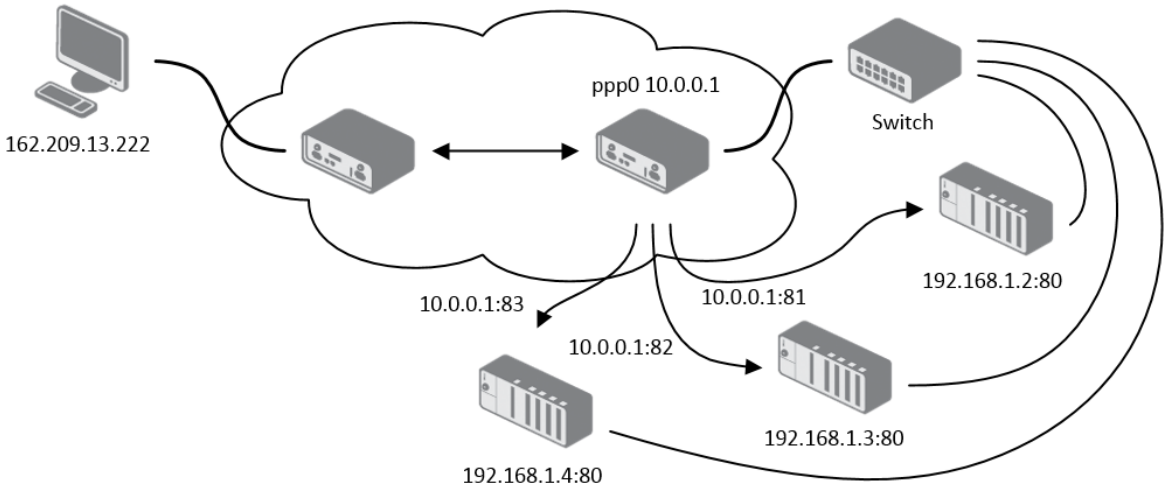


Figure 57: Topology for NAT Configuration Example 2

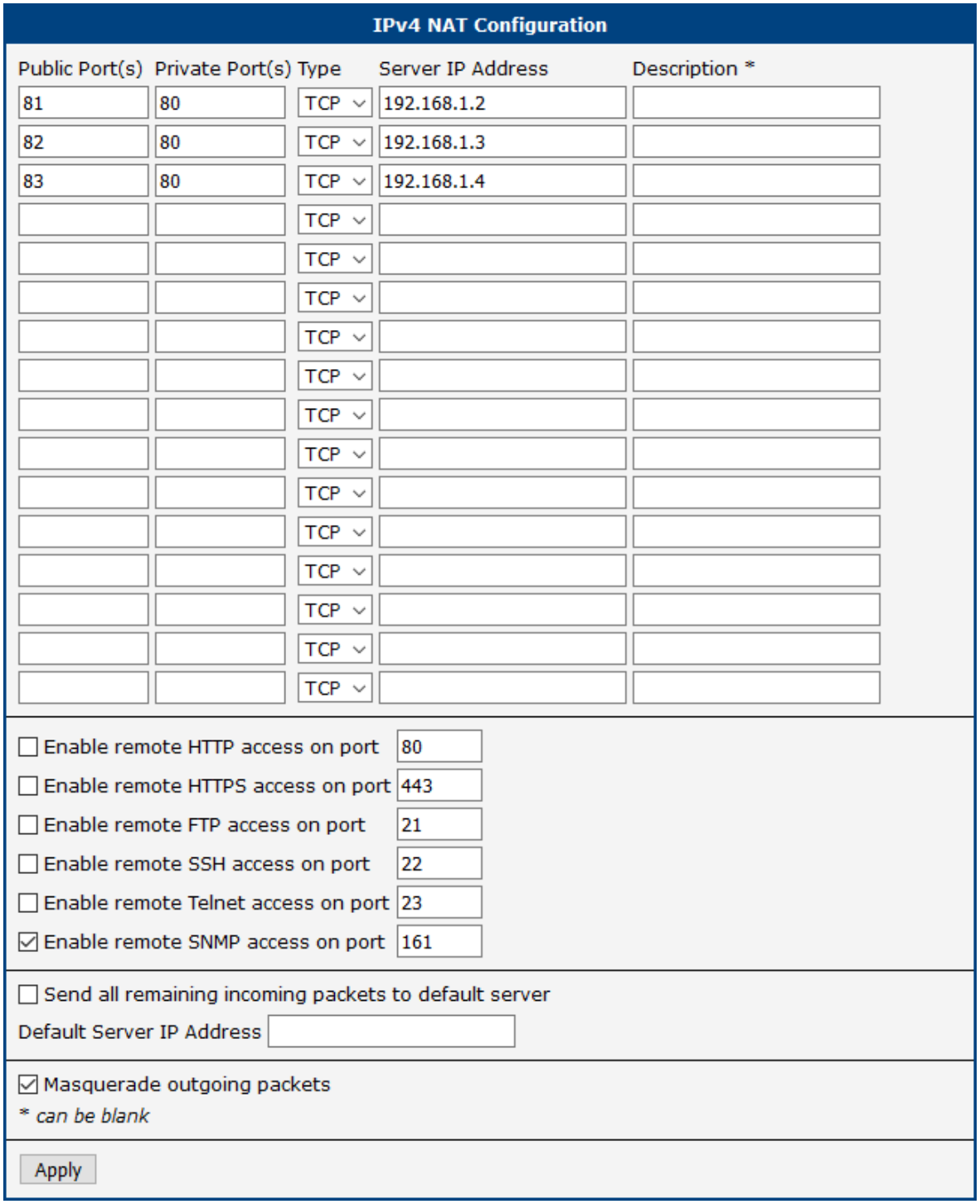


Figure 58: NAT Configuration for Example 2

3.13 OpenVPN Tunnel Configuration

Select the *OpenVPN* item to configure an OpenVPN tunnel. The menu item will expand and you will see separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The router allows you to create up to **four OpenVPN tunnels**. IPv4 and IPv6 dual stack is supported.

Item	Description
Description	Specifies the description or name of tunnel.
Interface Type	TAP is basically at the Ethernet level (layer 2) and acts as a switch, whereas TUN works at the network level (layer 3) and routes packets on the VPN. TAP is bridging, whereas TUN is routing. • **TUN** – Choose the TUN mode. • **TAP** – Choose the TAP mode, but remember first to **configure the bridge** on the ethernet interface.
Protocol	Specifies the communication protocol. • **UDP** – The OpenVPN communicates using UDP. • **TCP server** – The OpenVPN communicates using TCP in server mode. • **TCP client** – The OpenVPN communicates using TCP in client mode. • **UDPv6** – The OpenVPN communicates using UDP over IPv6. • **TCPv6 server** – The OpenVPN communicates using TCP over IPv6 in server mode. • **TCPv6 client** – The OpenVPN communicates using TCP over IPv6 in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
1st Remote IP Address	Specifies the first IPv4, IPv6 address or domain name of the opposite side of the tunnel.
2nd Remote IP Address	Specifies the second IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
Redirect Gateway	Adds (rewrites) the default gateway. All the packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IPv4 address of a local interface. **For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.**
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. **For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.**

Continued on next page

Continued from previous page

Item	Description
Remote IPv6 Subnet	IPv6 address of the remote IPv6 network. Equivalent of the *Remote Subnet* in IPv4 section.
Remote IPv6 Prefix	IPv6 prefix of the remote IPv6 network. Equivalent of the *Remote Subnet Mask* in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	Time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the *Ping Timeout* to greater than the *Ping Interval*.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the *Authenticate Mode* is set to *username/password* or *X.509 certificate*. After this time period, the router changes the tunnel encryption to keep the tunnel secure.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: • **none** – No compression is used. • **LZO** – A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: • **not applied** – NAT rules are not applied to the tunnel. • **applied** – NAT rules are applied to the OpenVPN tunnel.
Authenticate Mode	Specifies the authentication mode: • **none** – No authentication is set. • **Pre-shared secret** – Specifies the shared key function for both sides of the tunnel. • **Username/password** – Specifies authentication using a CA Certificate, Username and Password. • **X.509 Certificate (multiclient)** – Activates the X.509 authentication in multi-client mode. • **X.509 Certificate (client)** – Activates the X.509 authentication in client mode. • **X.509 Certificate (server)** – Activates the X.509 authentication in server mode.

Continued on next page

Continued from previous page

Item	Description
Security Mode	Choose the security mode, *tls-auth* or *tls-crypt*. We recommend to use the *tls-crypt* mode for the security reasons. In this mode, all the data is encrypted with a pre-shared key. Moreover, this mode is more robust against the TLS denial of service attacks.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the username/password and X.509 Certificate authentication modes.
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Local Passphrase	Passphrase used during private key generation.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode. Enter valid characters only, see chap. 1.1.2!
Security Level	Set the Security Level[1]: • **0 - Weak** – [Default] Everything is permitted. This setting is not recommended; it is advisable to set a higher security level! • **1 - Low** – 80 bits of security. • **2 - Medium** – 112 bits of security. • **3 - High** – 128 bits of security. • **4 - Very High** – 192 bits of security.
User's Up Script	Custom script, executed when the OpenVPN tunnel is established.
User's Down Script	Custom script, executed when the OpenVPN tunnel is closed.
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes. For possible parameters see the help text in the router using SSH – run the `openvpnd --help` command.

Table 38: OpenVPN Configuration

There is a condition for tunnel to be established: WAN route has to be active (for example mobile connection established) even if the tunnel does not go through the WAN.

The changes in settings will apply after pressing the *Apply* button.

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

[2] Parameters passed to the script are `cmd tun_dev tun_mtu link_mtu ifconfig_local_ip ifconfig_remote_ip [ init | restart ]`, see Reference manual for OpenVPN, option `-up cmd`.

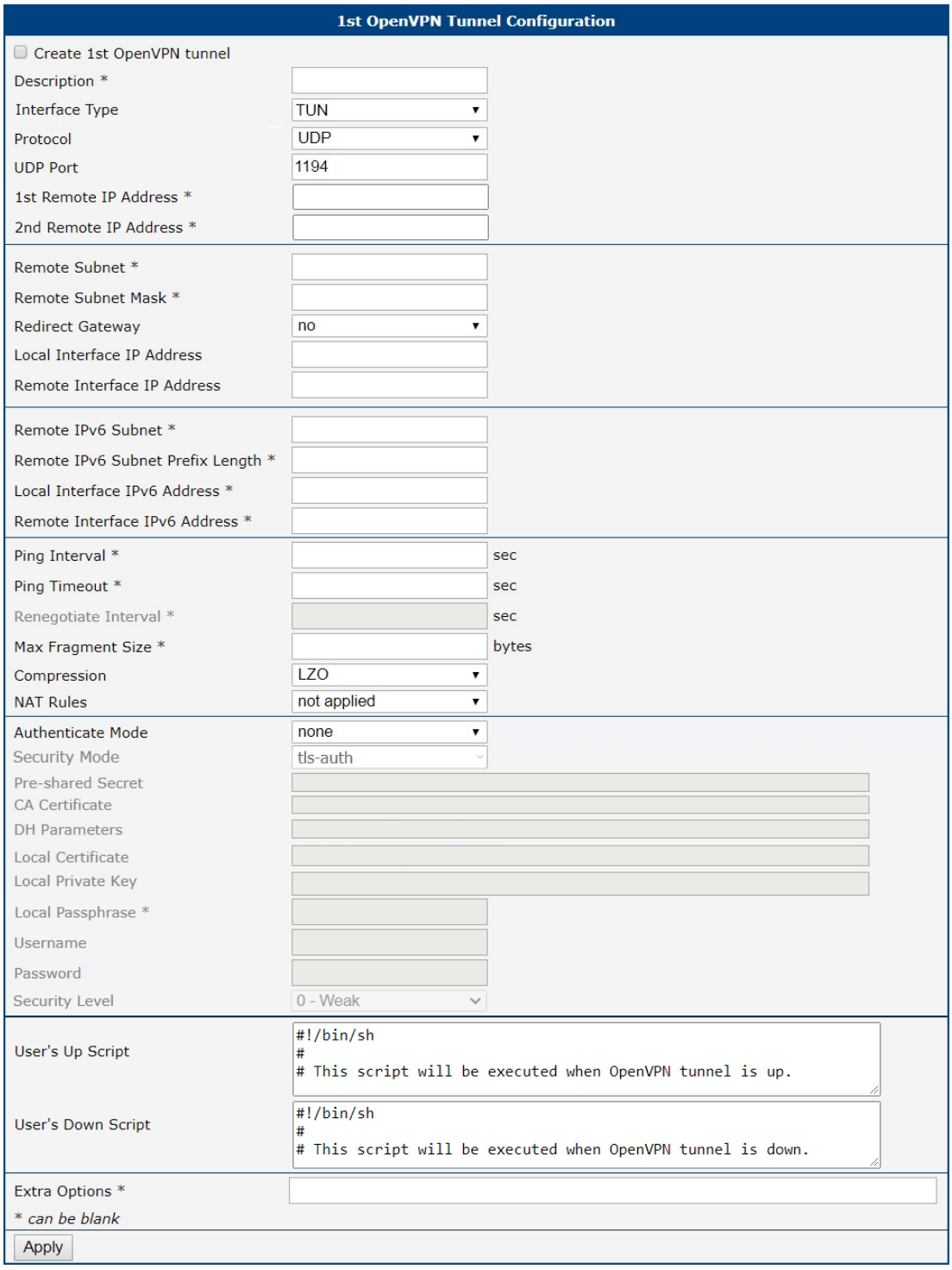


Figure 59: OpenVPN tunnel configuration

3.13.1 Example of the OpenVPN Tunnel Configuration in IPv4 Network

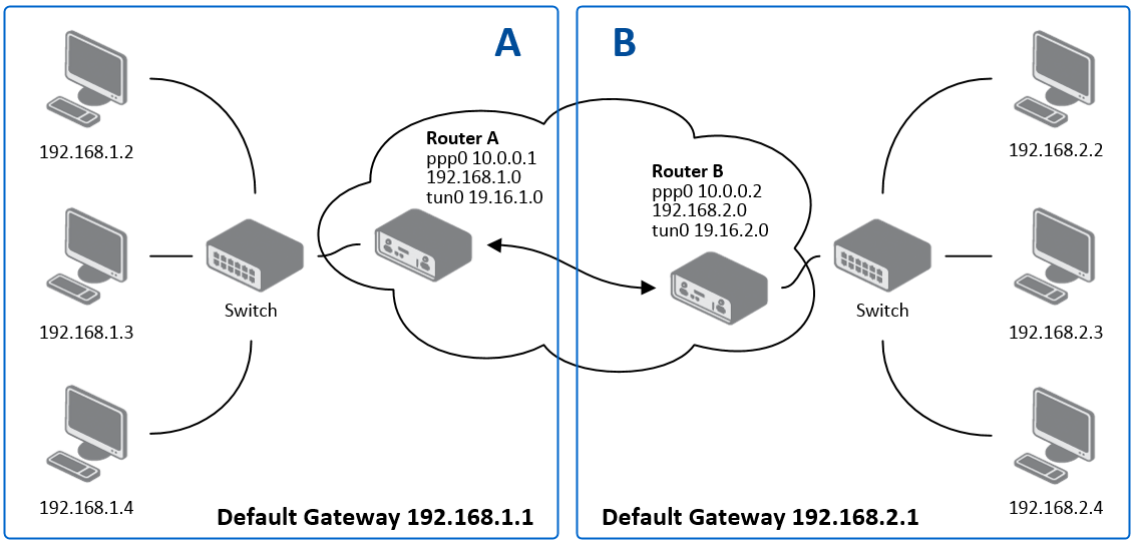


Figure 60: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

Configuration	A	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 Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.16.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 39: OpenVPN Configuration Example

Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the application note *OpenVPN Tunnel* [5].

3.14 IPsec Tunnel Configuration

The IPsec tunnel function allows you to create a secured connection between two separate LAN networks. These 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*.

Supported are both, **policy-based** and **route-based** VPN approaches, see the different configuration scenarios in Chapter 3.14.1.

IPv4 and IPv6 tunnels are supported (**dual stack**), you can transport IPv6 traffic through IPv4 tunnel and vice versa. For different IPsec authentication scenarios, see Chapter 3.14.2.

To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both routers. To encrypt the data stream between the routers only, leave the local and remote subnets fields blank.

If you specify the protocol and port information in the *Local Protocol/Port* field, then the router encapsulates only the packets matching the settings.

For optimal an secure setup, we recommend to follow instructions on the Security Recommendations *strongSwan* web page.

Detailed information and more examples of IPsec tunnel configuration and authentication can be found in the application note *IPsec Tunnel* [6].

FRRouting (FRR) router app is an Internet routing protocol suite for Advantech routers. This UM includes protocol daemons for BGP, IS-IS, LDP, OSPF, PIM, and RIP.

3.14.1 Route-based Configuration Scenarios

There are more different route-based configuration options which can be configured and used in Advantech routers. Below are listed the most common cases which can be used (for more details see Route-based VPNs *strongSwan* web page):

1. **Enabled Installing Routes**
   - Remote (local) subnets are used as traffic selectors (routes).
   - It results to the same outcome as a policy-based VPN.
   - One benefit of this approach is the possibility to verify non-encrypted traffic passed through an IPsec tunnel number X by tcdump tool: `tcpdump -i ipsecX`.
   - Set up the *Install Routes* to *yes* option.

2. **Static Routes**
   • Routes are installed statically by an application as soon as the IPsec tunnel is up.
   • As an application for static routes installation can be used for example FRR/STATICD application.
   • Set up the *Install Routes* to *no* option.

3. **Dynamic Routing**
   • Routes are installed dynamically while running by an application using a dynamic protocol.
   • As an application for dynamic routes installation can be used for example FRR/BGP or FRR/OSPF application. This application gains the routes dynamically from an (BGP, OSPF) server.
   • Set up the *Install Routes* to *no* option.

4. **Multiple Clients**
   • Allows to create VPN network with multiple clients. One Advantech router acts as the server and assigns IP address to all the clients on the network.
   • The server has *Remote Virtual Network* and *Remote Virtual Mask* items configured and the client has *Local Virtual Address* item configured.
   • Set up the *Install Routes* to *yes* option.

3.14.2 IPsec Authentication Scenarios

There are four basic authentication options which can be configured and used in Advantech routers:

1. **Pre-shared Key**
   • Set *Authenticate Mode* to *pre-shared key* option.
   • Enter the shared key to the *Pre-shared key* field.

2. **Public Key**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the public key to the *Local Certificate / PubKey* field.
   • CA certificate is not required.

3. **Peer Certificate**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the remote key to the *Remote Certificate / PubKey* field. Users with this certificate will be allowed.
   • CA certificate is not required.

4. **CA Certificate**
   • Set *Authenticate Mode* to *X.509 certificate* option.
   • Enter the CA certificate or a list of CA certificates to the *CA Certificate* field. Any certificate signed by the CA will be accepted.
   • Remote certificate is not required.

Notes:

- The Peer and CA Certificate (options 3 and 4) can be configured and used simultaneously – authentication can be done by one of this method.
- The Local ID is significant. When using certificate authentication, the IKE identity must be contained in the certificate, either as subject or as `subjectAltName`.

3.14.3 Configuration Items Description

The configuration GUI for IPsec is shown in Figure 61 and the description of all items, which can be configured for an IPsec tunnel, are described in Table 40.

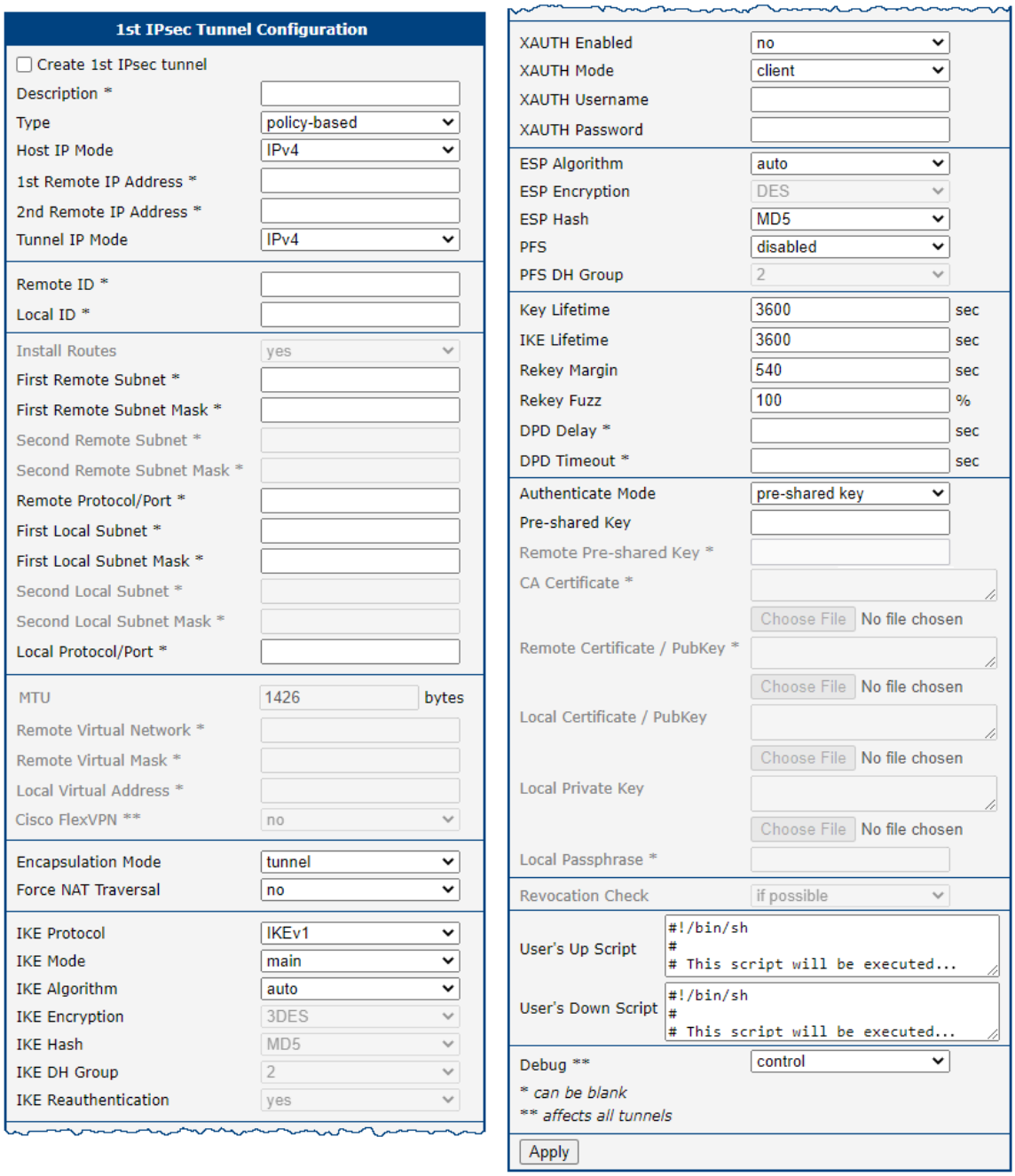


Figure 61: IPsec Tunnels Configuration

Item	Description
Description	Name or description of the tunnel.
Type	• **policy-based** – Choose for the policy-based VPN approach. • **route-based** – Choose for the route-based VPN approach. Note: Data throughput via route-based VPN is slightly lower in comparison with policy-based VPN.
Host IP Mode	• **IPv4** – The router communicates via IPv4 with the opposite side of the tunnel. • **IPv6** – The router communicates via IPv6 with the opposite side of the tunnel.
1st Remote IP Address	First IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected *Host IP Mode* above.
2nd Remote IP Address	Second IPv4, IPv6 address or domain name of the remote side of the tunnel, based on selected *Host IP Mode* above.
Tunnel IP Mode	• **IPv4** – The IPv4 communication runs inside the tunnel. • **IPv6** – The IPv6 communication runs inside the tunnel.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
Install Routers	For route-based type only. Choose **yes** to use traffic selectors as route(s).
First Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on *Tunnel IP Mode* above.
First Remote Subnet Mask/Prefix	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Second Remote Subnet	IPv4 or IPv6 address of the second network behind remote side of the tunnel, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.
Second Remote Subnet Mask/Prefix	IPv4 subnet mask of the second network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is *protocol*/*port*, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
First Local Subnet	IPv4 or IPv6 address of a local network, based on *Tunnel IP Mode* above.
First Local Subnet Mask/Prefix	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Second Local Subnet	IPv4 or IPv6 address of the second local network, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.

Continued on next page

Continued from previous page

Item	Description
Second Local Subnet Mask/Prefix	IPv4 subnet mask of the second local network, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is *protocol*/*port*, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
MTU	Maximum Transmission Unit value (for route-based mode only). Default value is 1426 bytes.
Remote Virtual Network	Specifies virtual remote network for server (responder).
Remote Virtual Mask	Specifies virtual remote network mask for server (responder).
Local Virtual Address	Specifies virtual local network address for client. To get address from server set up the address to 0.0.0.0.
Cisco FlexVPN	Enable to support the Cisco FlexVPN functionality. The *route-based* type must be chossen. For more information, see strongswan.conf page.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. • **tunnel** – entire IP datagram is encapsulated. • **transport** – only IP header is encapsulated. Not supported by route-based VPN. • **beet** – the ESP packet is formatted as a transport mode packet, but the semantics of the connection are the same as for tunnel mode.
Force NAT Traversal	Enable NAT traversal enforcement (UDP encapsulation of ESP packets).
IKE Protocol	Specifies the version of IKE (**IKEv1**/**IKEv2**, **IKEv1** or **IKEv2**).
IKE Mode	Specifies the mode for establishing a connection (*main* or *aggressive*). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. **We recommend that you not use the *aggressive* mode due to lower security!**
IKE Algorithm	Specifies the means by which the router selects the algorithm: • **auto** – The encryption and hash algorithm are selected automatically. • **manual** – The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm – **3DES**, **AES128**, **AES192**, **AES256**, **AES128GCM128**, **AES192GCM128**, **AES256GCM128**.
IKE Hash	Hash algorithm – **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.

Continued on next page

Continued from previous page

Item	Description
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require more time to compute the key.
IKE Reauthentication	Enable or disable IKE reauthentication (for IKEv2 only).
XAUTH Enabled	Enable extended authentication (for IKEv1 only).
XAUTH Mode	Select XAUTH mode (client or server).
XAUTH Username	XAUTH username.
XAUTH Password	XAUTH password.
ESP Algorithm	Specifies the means by which the router selects the algorithm: • **auto** – The encryption and hash algorithm are selected automatically. • **manual** – The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm – **3DES**, **AES128**, **AES192**, **AES256**, **AES128GCM128**, **AES192GCM128**, **AES256GCM128**.
ESP Hash	Hash algorithm – **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.
PFS	Enables/disables the *Perfect Forward Secrecy* function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see *IKE DH Group*).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the router authenticates: • **Pre-shared key** – Sets the shared key for both sides of the tunnel. • **X.509 Certificate** – Allows X.509 authentication in multiclient mode.
(Local) Pre-shared Key	Specifies the shared key (local for IKEv2) for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.
Remote Pre-shared Key	Specifies the remote shared key (for IKEv2) for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.

Continued on next page

Continued from previous page

Item	Description
CA Certificate	Certificate for X.509 authentication.
Remote Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.
Local Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.
Local Private Key	Private key for X.509 authentication.
Local Passphrase	Passphrase used during private key generation.
Revocation Check	Certificate revocation policy: • **if possible** – Fails only if a certificate is revoked, i.e. it is explicitly known that it is bad. • **if URI defined** – Fails only if a CRL/OCSP URI is available, but certificate revocation checking fails, i.e. there should be revocation information available, but it could not be obtained. • **always** – Fails if no revocation information is available, i.e. the certificate is not known to be unrevoked.
User's Up Script[1]	Custom script, executed when the IPSec tunnel is established.
User's Down Script[1]	Custom script, executed when the IPSec tunnel is closed.
Debug	Choose the level of logging verbosity from: **silent**, **audit**, **control** (default), **control-more**, **raw**, **private** (most verbose including the private keys). See Logger Configuration in *strongSwan* web page for more details.

Table 40: IPsec Tunnel Configuration

We recommend that you keep up the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security. The changes in settings will apply after clicking the *Apply* button.

Do not miss:

- If local and remote subnets are not configured then only packets between local and remote IP address are encapsulated, so only communication between two routers is encrypted.
- If protocol/port fields are configured then only packets matching these settings are encapsulated.

[1] Parameters passed to the script:
for policy-based type: one parameter: *connection name*, returns e.g. `ipsec1-1`,
for route-based type: two parameters: *connection name* and *interface name*, returns e.g. `ipsec1-1` and `ipsec0`.

3.14.4 Basic IPv4 IPSec Tunnel Configuration

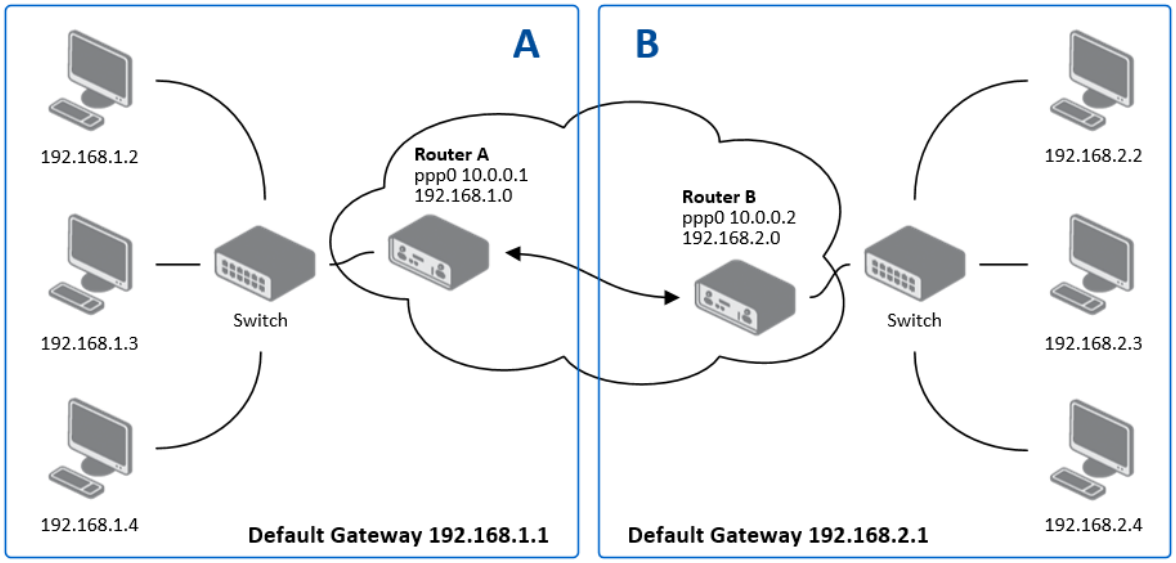


Figure 62: Topology of IPsec Configuration Example

Configuration of *Router A* and *Router B* is as follows:

Configuration	A	B
Host IP Mode	IPv4	IPv4
1st Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
First Remote Subnet	192.168.2.0	192.168.1.0
First Remote Subnet Mask	255.255.255.0	255.255.255.0
First Local Subnet	192.168.1.0	192.168.2.0
First 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 41: Simple IPv4 IPSec Tunnel Configuration

3.15 WireGuard Tunnel Configuration

WireGuard is a communication protocol and free open-source software that implements encrypted virtual private networks (VPNs), and was designed with the goals of ease of use, high speed performance, and low attack surface. It aims for better performance and more power than IPsec and OpenVPN, two common tunneling protocols. The WireGuard protocol passes traffic over UDP. Advantech routers allows you to create **up to four WireGuard tunnels**.

To open the WireGuard tunnel configuration page, click *WireGuard* 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*.

IPv4 and IPv6 tunnels are supported (**dual stack**), you can transport IPv6 traffic through IPv4 tunnel and vice versa.

FRRouting (FRR) router app is an Internet routing protocol suite for Advantech routers. This UM includes protocol daemons for BGP, IS-IS, LDP, OSPF, PIM, and RIP.

Detailed information and more examples of WireGuard tunnel configuration and authentication can be found in the application note *WireGuard Tunnel* [8].

The configuration GUI for WireGuard is shown in Figure 63 and the description of all items, which can be configured for an WireGuard tunnel, are described in Table 42.

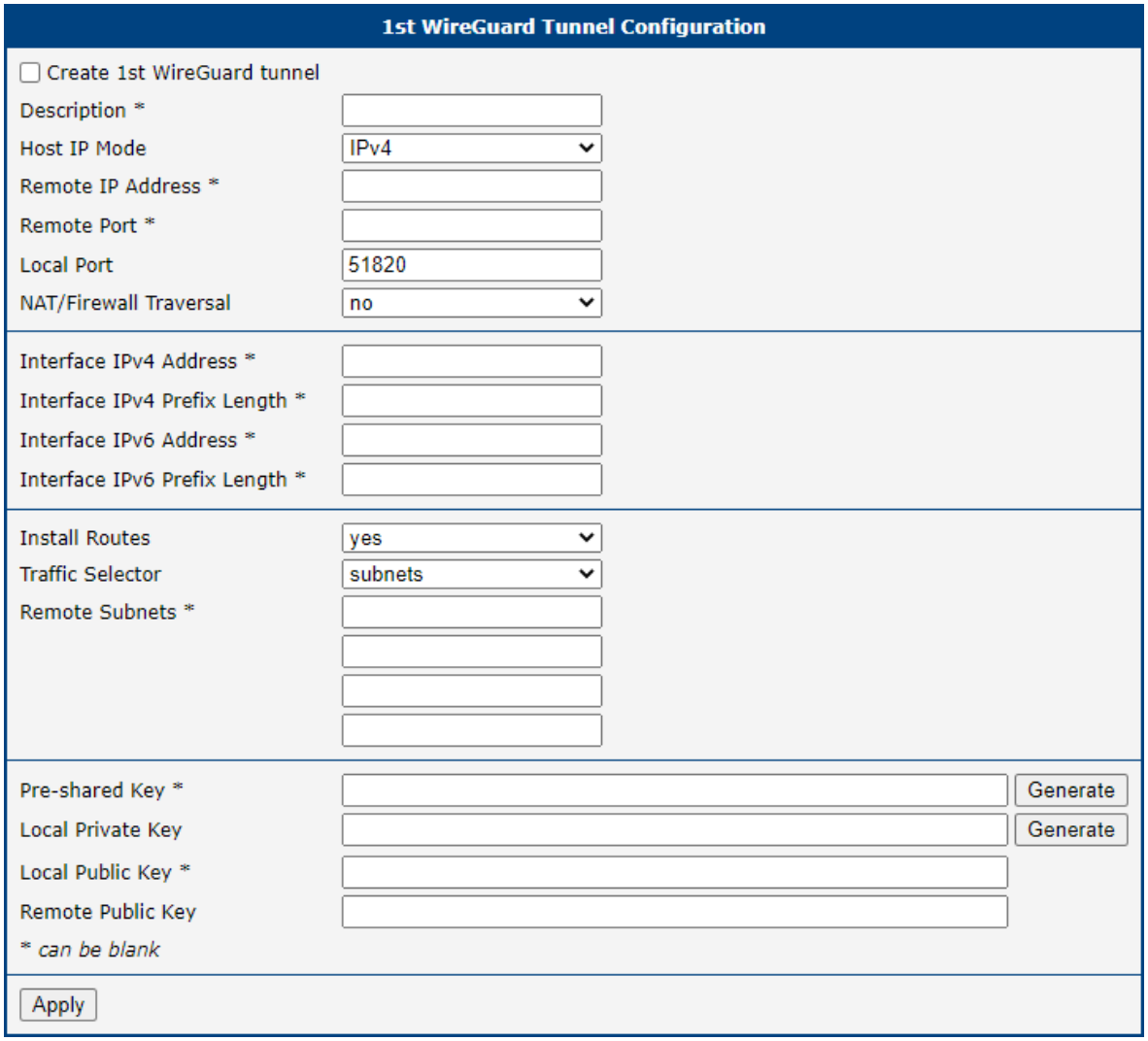


Figure 63: WireGuard Tunnels Configuration

Item	Description
Description	Name or description of the tunnel.
Host IP Mode	• **IPv4** – The router communicates via IPv4 with the opposite side of the tunnel. • **IPv6** – The router communicates via IPv6 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel to connect to. The address must match with the selected *Host IP Mode* above.
Remote Port	Port of the remote side of the tunnel.
Local Port	Port of the local side of the tunnel (default port is 51820).
NAT/Firewall Traversal	If set up to *yes*, keepalive communication (every 25 seconds) is running to preserve the tunnel established. It is useful when a client is running behind the NAT.

Continued on next page

Continued from previous page

Item	Description
Interface IPv4 Address	Local IPv4 tunnel interface address.
Interface IPv4 Prefix Length	Local IPv4 tunnel interface prefix.
Interface IPv6 Address	Local IPv6 tunnel interface address.
Interface IPv6 Prefix Length	Local IPv6 tunnel interface prefix.
Install Routes	• **no** – Do not install routes. Use when a dynamic routing protocol is configured. • **yes** – Install routes.
Traffic Selector	• **all traffic** – Procced all the packets to the WireGuard tunnel. • **subnets** – Route based on the subnets listed below.
Remote Subnets	If the *Traffic Selector* is set to *subnets*, then other subnets (routes) can be routed through the wire tunnel.
Pre-shared Key	The optional key for additional encryption layer and security strengthening. You can use the *Generate* button to generate a random key.
Local Private Key	The private key of the local side. You can use the *Generate* button to generate a random key.
Local Public Key	The public key of the local tunnel side.
Remote Public Key	The public key of the remote tunnel side.

Table 42: WireGuard Tunnel Configuration

The changes in settings will apply after clicking the *Apply* button.

3.15.1 WireGuard IPv4 Tunnel Configuration Example

There is an example of WireGuard IPv4 tunnel configuration between *Router A* and *Router B*.

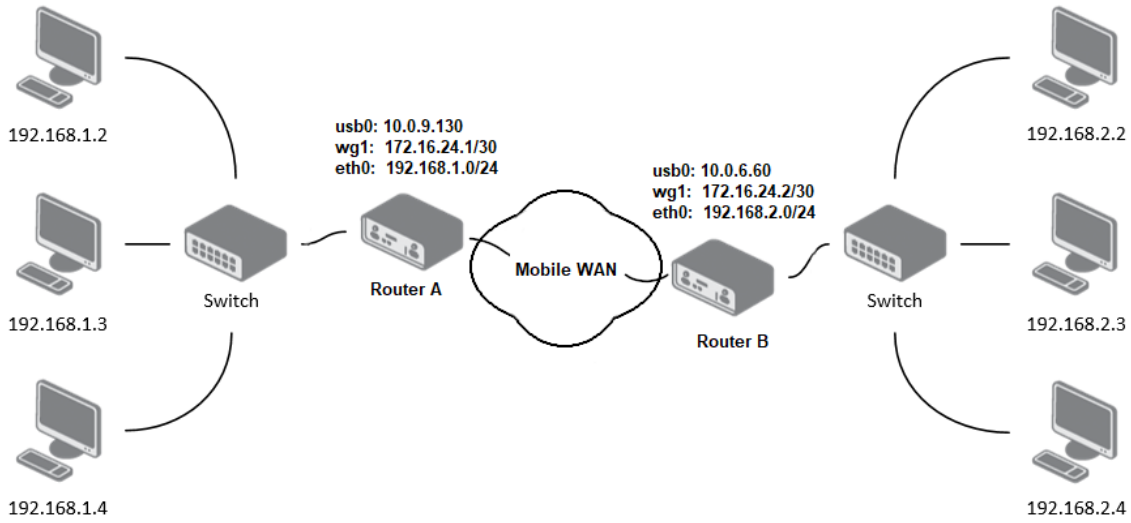


Figure 64: Topology of WireGuard Configuration Example

Router B is configured to listen, and *Router A* is the side initiating the tunnel connection. Configuration of *Router A* and *Router B* from the topology above is as follows:

Configuration	Router A	Router B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.6.60	–
Remote Port	51820	–
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	*a local private key*	*a local private key*
Local Public Key	*a local public key*	*a local public key*
Remote Public Key	*a public key of the opposite side*	*a public key of the opposite side*

Table 43: WireGuard IPv4 Tunnel Configuration Example

In the figure below is the WireGuard status page of *Router A*. If the tunnel connection is established successfully, the *Latest handshake* time is shown here. This value is the time left from the latest successful communication with the opposite tunnel side. This item will not be shown here until there is a tunnel communication (data sent by the *Router A* or the keepalive data sent when *NAT/Firewall Traversal* is set to *yes*).

1st WireGuard Tunnel Information

```
interface: wg1
  public key: jYlVmPwwlmzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  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 65: Router A – WireGuard Status Page and Route Table

1st WireGuard Tunnel Information

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

peer: jYlVmPwwlmzoC3y6xUX7dbXeDfvrRJxL42f4xOA4FkA=
  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 66: Router B – WireGuard Status Page and Route Table

3.16 GRE Tunnels Configuration

GRE is an unencrypted protocol. GRE via IPv6 is not supported.

To open the *GRE Tunnel Configuration* page, click *GRE* 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*.

The GRE tunnel function allows you to create an unencrypted connection between two separate LAN networks. The router allows you to create **four GRE tunnels**.

Item	Description
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Local IP Address	IP address of the local side of the tunnel.
Remote Subnet	IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	IP address of the local side of the tunnel.
Remote Interface IP Address	IP address of the remote side of the tunnel.
Multicasts	Activates/deactivates sending multicast into the GRE tunnel: • **disabled** – Sending multicast into the tunnel is inactive. • **enabled** – Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the router sends the filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops received packets.

Table 44: GRE Tunnel Configuration

The GRE tunnel cannot pass through the NAT.

The changes in settings will apply after pressing the *Apply* button.

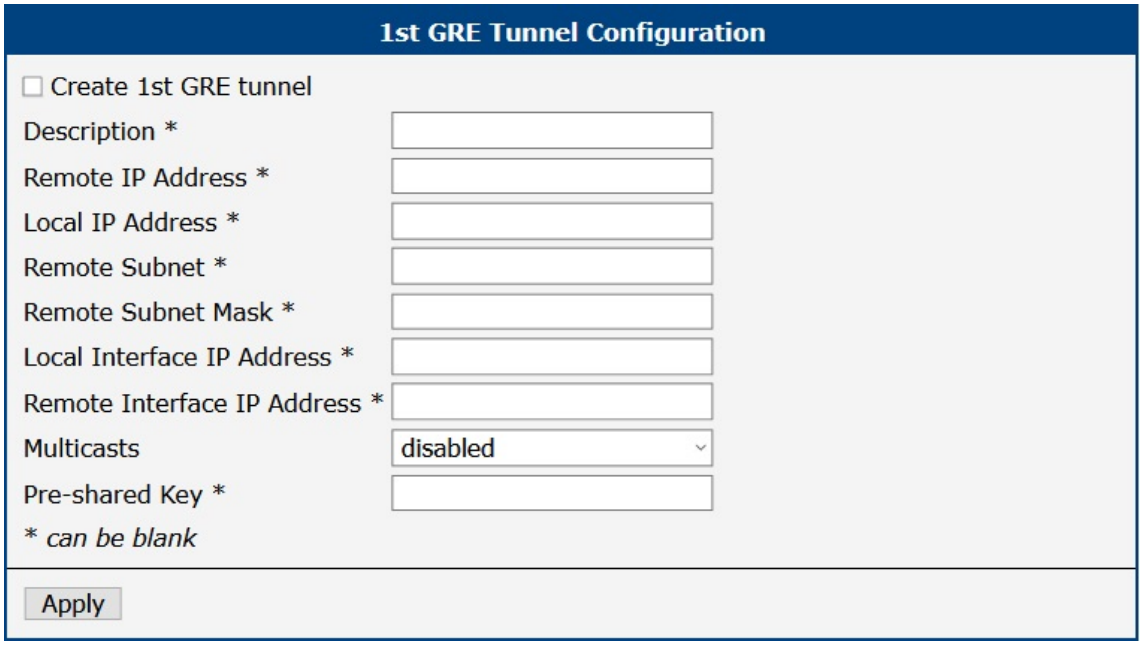


Figure 67: GRE Tunnel Configuration

3.16.1 Example of the GRE Tunnel Configuration

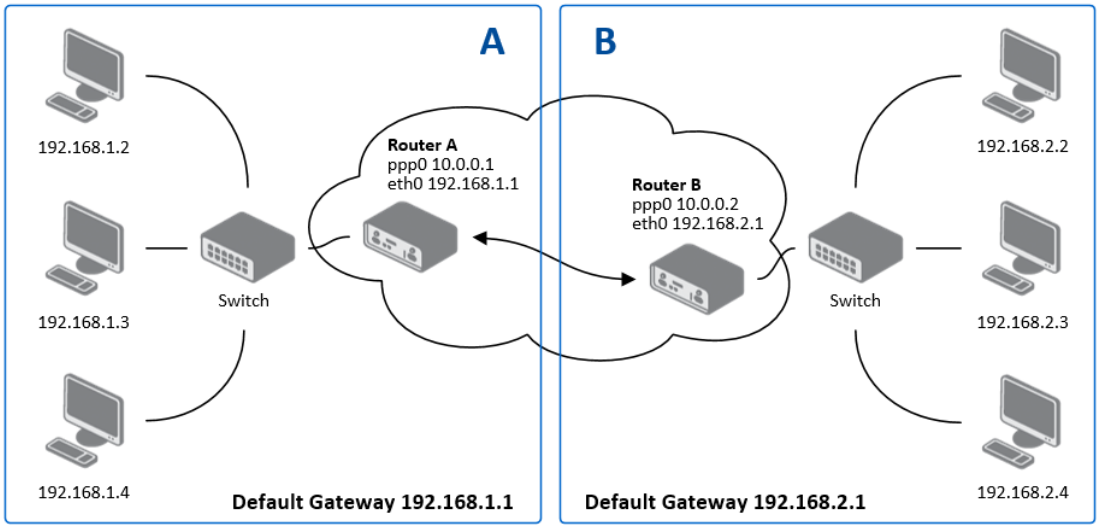


Figure 68: Topology of GRE Tunnel Configuration Example

GRE tunnel configuration:

Configuration	A	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 45: GRE Tunnel Configuration Example

Examples of different options for configuration of GRE tunnel can be found in the application note *GRE Tunnel* [7].

3.17 L2TP Tunnel Configuration

L2TP is an unencrypted protocol. L2TP via IPv6 is not supported.

To open the *L2TP Tunnel Configuration* page, click *L2TP* in the *Configuration* section of the main menu. The L2TP tunnel function allows you to create a password-protected connection between two different LAN networks. Enable the *Create L2TP tunnel* checkbox to activate the tunnel.

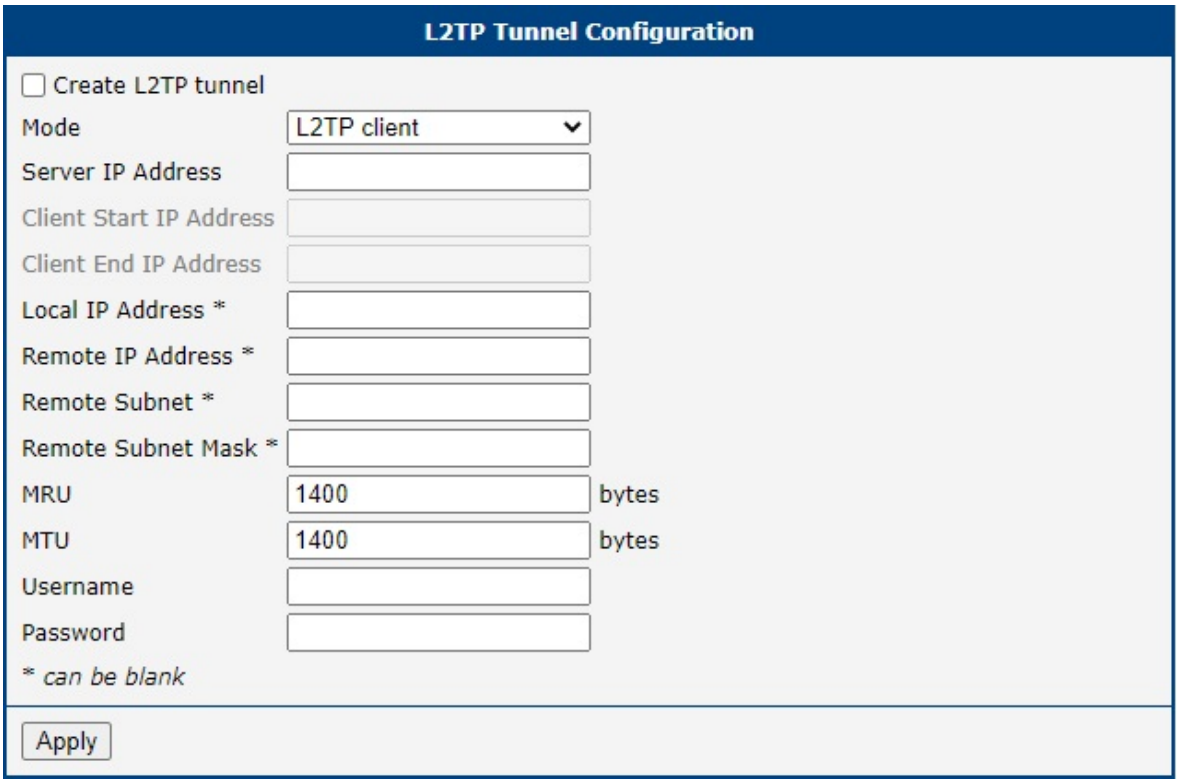


Figure 69: L2TP Tunnel Configuration

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **L2TP server** – Specify an IP address range offered by the server. • **L2TP client** – Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.

Continued on next page

Continued from previous page

Item	Description
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
MRU	Maximum Receive Unit value. Default value is 1400 bytes.
MTU	Maximum Transmission Unit value. Default value is 1400 bytes.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login. Enter valid characters only.

Table 46: L2TP Tunnel Configuration

3.17.1 Example of the L2TP Tunnel Configuration

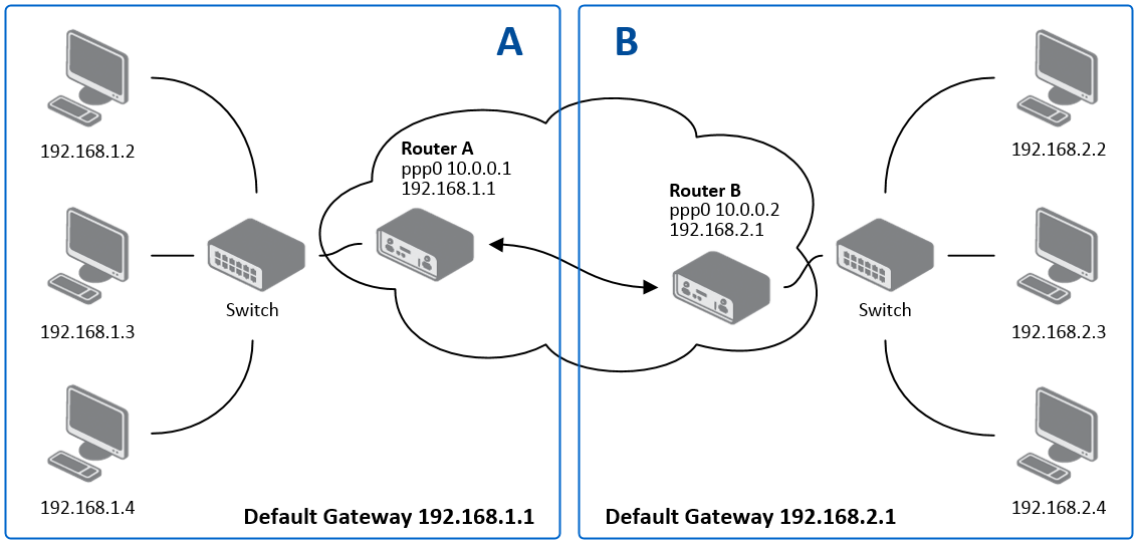


Figure 70: Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

Configuration	A	B
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 IP Address	—	—
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 47: L2TP Tunnel Configuration Example

3.18 PPTP Tunnel Configuration

PPTP is an unencrypted protocol. PPTP via IPv6 is not supported.

Select the *PPTP* item in the menu to configure a PPTP tunnel. PPTP tunnel allows password-protected connections between two LANs. It is similar to L2TP. The tunnels are active after selecting *Create PPTP tunnel*.

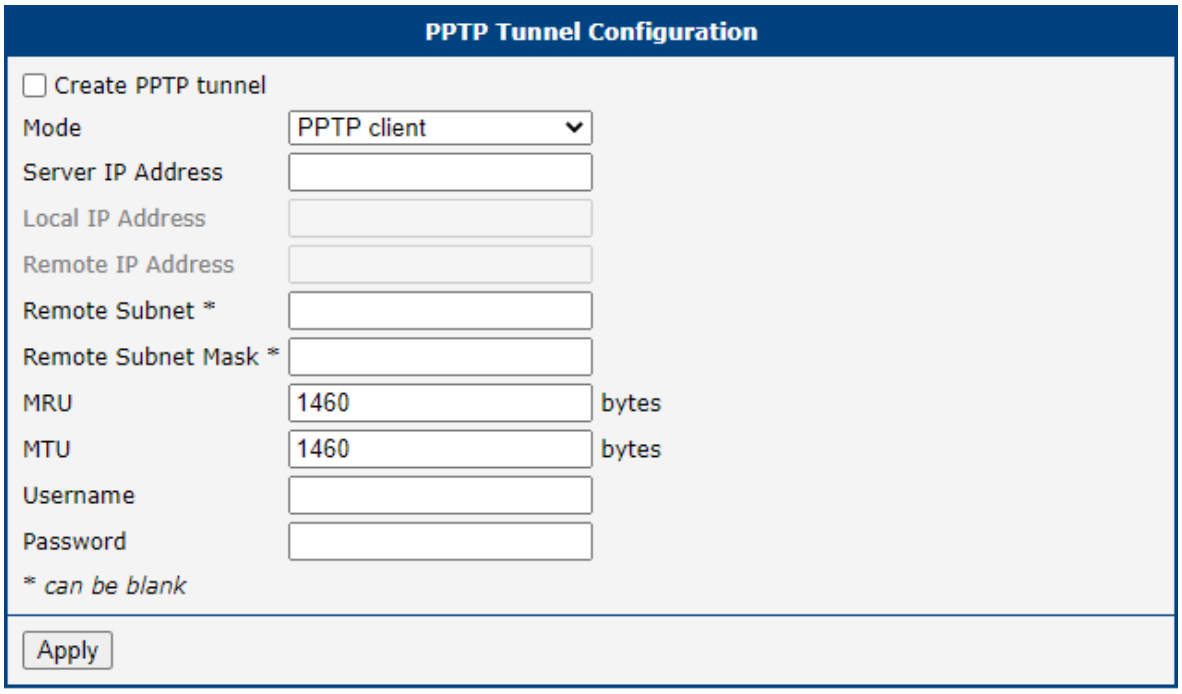


Figure 71: PPTP Tunnel Configuration

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **PPTP server** – Specify an IP address range offered by the server. • **PPTP client** – Specify the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
MRU	Maximum Receive Unit value. Default value is 1460 bytes to avoid fragmented packets.

Continued on next page

Continued from previous page

Item	Description
MTU	Maximum Transmission Unit value. Default value is 1460 bytes to avoid fragmented packets.
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login. Enter valid characters only.

Table 48: PPTP Tunnel Configuration

The changes in settings will apply after pressing the *Apply* button.

The firmware also supports PPTP passthrough, which means that it is possible to create a tunnel through the router.

3.18.1 Example of the PPTP Tunnel Configuration

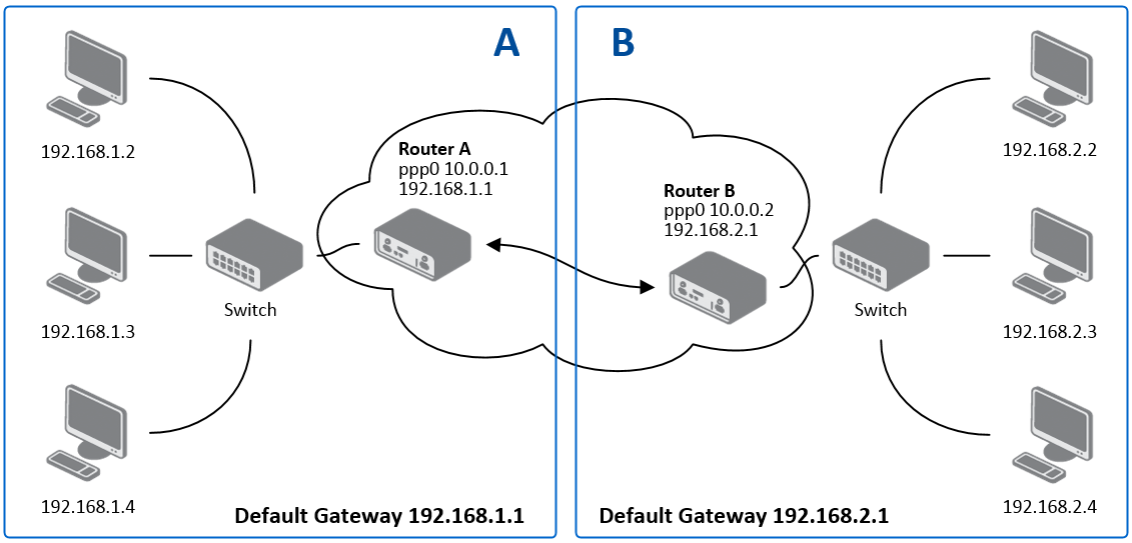


Figure 72: Topology of PPTP Tunnel Configuration Example

Configuration of the PPTP tunnel:

Configuration	A	B
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 49: PPTP Tunnel Configuration Example

3.19 Services

3.19.1 DynDNS

The DynDNS function allows you to access the router remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the router and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Register the custom domain (third-level) and account information specified in the configuration form. You can use other services, too – see the table below, Server item. To open the *DynDNS Configuration* page, click *DynDNS* in the main menu.

Item	Description
Hostname	The third order domain registered on the www.dyndns.org server.
Username	Username for logging into the DynDNS server.
Password	Password for logging into the DynDNS server. Enter valid characters only, see chap. 1.1.2!
IP Mode	Specifies the version of IP protocol: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 dual stack is enabled.
Server	Specifies a DynDNS service other than the www.dyndns.org. Possible other services: www.spdns.de, www.dnsdynamic.org, www.noip.com Enter the update server service information in this field. If you leave this field blank, the default server members.dyndns.org will be used.

Table 50: DynDNS Configuration

Example of the DynDNS client configuration with the domain company.dyndns.org:

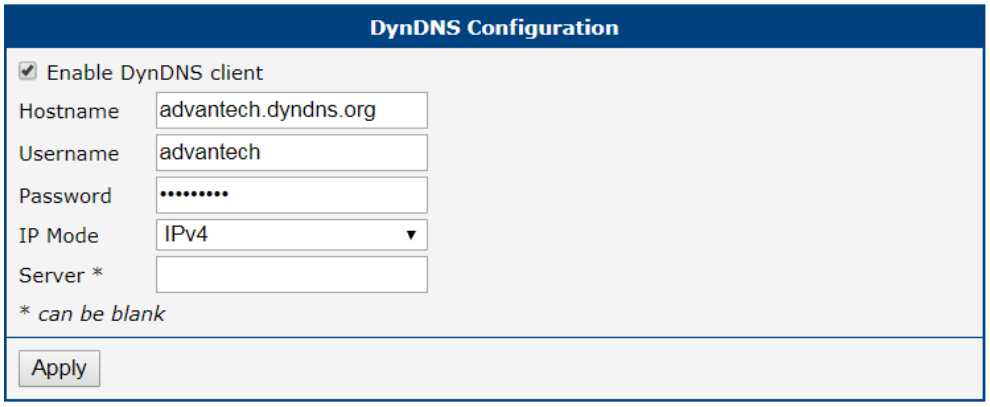


Figure 73: DynDNS Configuration Example

To access the router's configuration remotely, you will need to have enabled this option in the NAT configuration (bottom part of the form), see Chapter 3.12.

3.19.2 FTP

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 51: Parameters for FTP service configuration

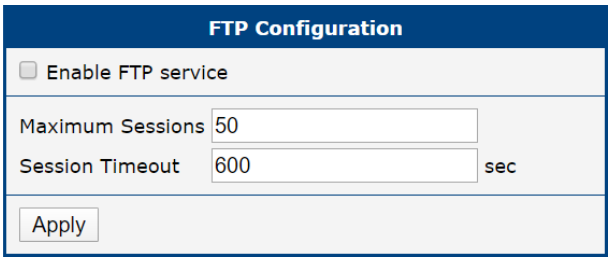


Figure 74: Configuration of FTP server

3.19.3 HTTP

HTTP protocol (Hypertext Transfer Protocol) is internet protocol used for exchange of hypertext documents in HTML format. This protocol is used for accessing the web server used for user's configuration of the router. Recommended usage however is of HTTPS protocol, which used encryption for secure exchange of transferred data. Configuration form of HTTP and HTTPS service can be done in *HTTP* configuration page under *Services* menu item. By default, HTTP service is disabled and preferred is using of HTTPS service. For this default setting, a request for communication with HTTP protocol is redirected to HTTPS protocol automatically.

Item	Description
Enable HTTP service	Enabling of HTTP service.
Enable HTTPS service	Enabling of HTTPS service.
Minimum TLS Version	If specified, the router will disable TLS versions lower than the specified minimum. For better security choose the highest version of TLS protocol, unless you need to use an older web browser.
Session Timeout	Inactivity timeout when the session is closed.
Login Banner	The text specified in this field will be displayed on the login page just above the credentials fields.
Keep the current certificate	Left the current one certificate in the router.
Generate a new certificate	Generate a new self-signed certificate to the router.
Upload a new certificate	Upload custom PEM certificate, which can be signed by Certificate Authority.
Certificate	Choose a file with the PEM certificate.
Private Key	Choose a file with the certificate private key.

Table 52: Parameters for HTTP and HTTPS services configuration

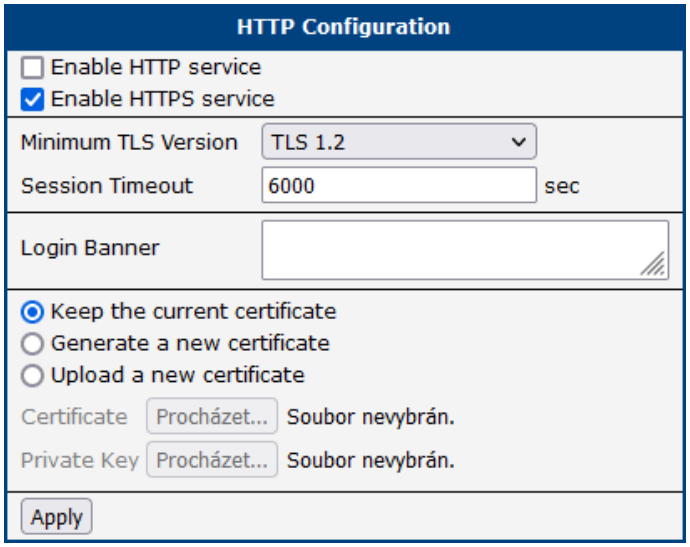


Figure 75: Configuration of HTTP and HTTPS services

3.19.4 NTP

The *NTP* configuration form allows you to configure the NTP client. To open the *NTP* page, click *NTP* in the *Configuration* section of the main menu. NTP (Network Time Protocol) allows you to periodically set the internal clock of the router. The time is set from servers that provide the exact time to network devices. IPv6 Time Servers are supported.

- If you mark the *Enable local NTP service* check box, then the router acts as a NTP server for other devices in the local network (LAN).
- If you mark the *Synchronize clock with NTP server* check box, then the router acts as a NTP client. This means that the router automatically adjusts the internal clock every 24 hours.

Item	Description
Primary NTP Server Address	IPv4 address, IPv6 address or domain name of primary NTP server.
Secondary NTP Server Address	IPv4 address, IPv6 address or domain name of secondary NTP server.
Timezone	Specifies the time zone where you installed the router.
Daylight Saving Time	Activates/deactivates the DST shift. • **No** – The time shift is inactive. • **Yes** – The time shift is active.

Table 53: NTP Configuration

The figure below displays an example of a NTP configuration with the primary server set to *ntp.cesnet.cz* and the secondary server set to *tik.cesnet.cz* and with the automatic change for daylight saving time enabled.

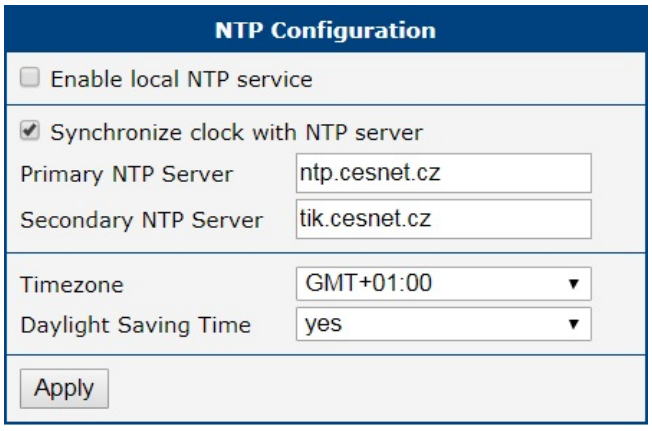


Figure 76: Example of NTP Configuration

3.19.5 PAM

A pluggable authentication module (PAM) is a mechanism that integrates multiple low-level authentication schemes into a high-level application programming interface (API). The configuration made on this page will affect all the router's authentication mechanisms. As the first option, choose the *PAM Mode*.

PAM Modes

In the first configuration option, you can choose the PAM mode. The available modes are described in Table 54.

Item	Description
PAM Mode	• **Local user database** – Authenticate against the local user database only. See Chapter 5.1. • **RADIUS with fallback** – Authenticate against the RADIUS server first, and then against the local database if the RADIUS server is not accessible. • **RADIUS only** – Authenticate only against the RADIUS server. Note that you will not be able to authenticate to the router if the RADIUS server is not accessible! • **TACACS+ with fallback** – Authenticate against the TACACS+ server first, and then against the local database if the TACACS+ server is not accessible. • **TACACS+ only** – Authenticate only against the TACACS+ server. Note that you will not be able to authenticate to the router if the TACACS+ server is not accessible!

Table 54: Available PAM Modes

Common Configuration

In this section, we will describe configuration options common to all the modes, see Figure 77 and Table 55.

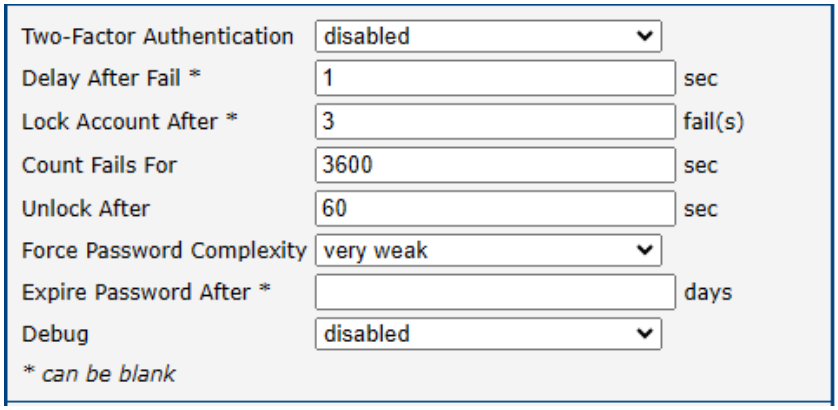


Figure 77: Common Configuration Items

Item	Description
Two-Factor Authentication	Disable or choose the two-factor authentication service; see Chapter 3.19.5.
Delay After Fail	The time after which the login screen will appear again in case of a previous unsuccessful attempt.
Lock Account After	Number of failed login attempts after which the account will be locked.
Count Fails For	The time window for which unsuccessful login attempts will be counted.
Unlock After	The time after which logging will be unlocked if it was previously locked.
Force Password Complexity	Specify the level of password complexity: • **very weak** – Not secure and not recommended. Requires 6 characters. Time to crack: Seconds to minutes. • **weak** – Not secure and not recommended. Requires 8 characters from two sets (numbers, letters) [NIST SP 800-63B compliant]. Time to crack: Hours to days. • **good** – Reasonably secure. Requires 12 characters from three sets (uppercase letters, lowercase letters, and numbers), with a maximum of 3 same characters in sequence [FirstNet compliant]. Time to crack: Months to years. • **strong** – For the best security level. Requires 16 characters from four sets (uppercase and lowercase letters, digits, and special characters). Time to crack: Centuries.
Expire Password After	Number of days after which the password will expire and the user will be prompted to change it; see Chapter 3.19.5.
Debug	Enable or disable debugging in the Syslog.

Table 55: Common Configuration Items Description

RADIUS Mode

When authenticate against the RADIUS server, user with the same name must exist locally. It can be created manually (see Chapter 5.1) or can be created automatically based on data from RADIUS server, if the *Take Over Server Users* option is enabled as described hereunder.

To configure the authentication against a RADIUS server, choose *RADIUS with fallback* or *RADIUS only* as the *PAM mode* and set up all required items, see Figure 78. Table 56 describes all the configuration options for the RADIUS PAM modes.

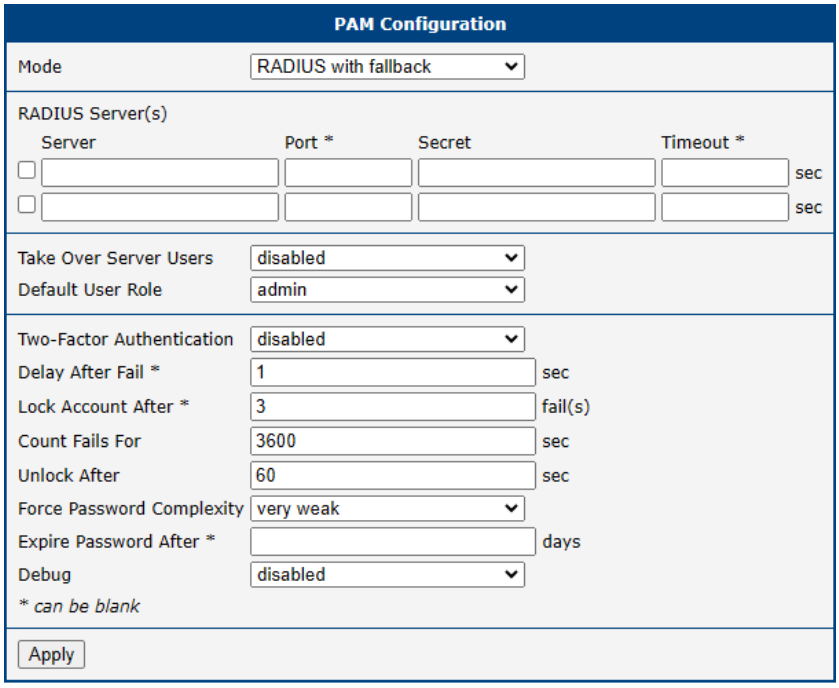


Figure 78: Configuration of RADIUS

Item	Description
Server	Address of the RADIUS server. Up to two servers can be configured.
Port	Port of the RADIUS server.
Secret	The secret For authentication to the RADIUS server.
Timeout	Timeout for authentication to the RADIUS server.
Take Over Server Users	If enabled, a new user account is created during the login, in case the RADIUS authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the user role (*Admin* or *User*). This role corresponds with router's user roles, see Chapter 5.1. Selected role will be used for a user in case the option *Take Over Server Users* is enabled and if the user's *Service-Type* set on the RADIUS server is missing or is not set up to *NAS-Prompt-User* or *Administrative-User*. When *Service-Type* is set to *NAS-Prompt-User*, the *User* role will be used. When *Service-Type* is set to *Administrative-User*, the *Admin* role is used.

Table 56: Configuration of RADIUS

TACACS+ Mode

When authenticate against the TACACS+ server, user with the same name must exist locally. It can be created manually (see Chapter 5.1) or can be created automatically based on data from TACACS+ server, if the *Take Over Server Users* option is enabled as described hereunder.

To configure the authentication against a TACACS+ server, choose *TACACS+ with fallback* or *TACACS+ only* as the *PAM mode* and set up all required items, see Figure 79. Table 57 describes all the configuration options for the TACACS PAM modes.

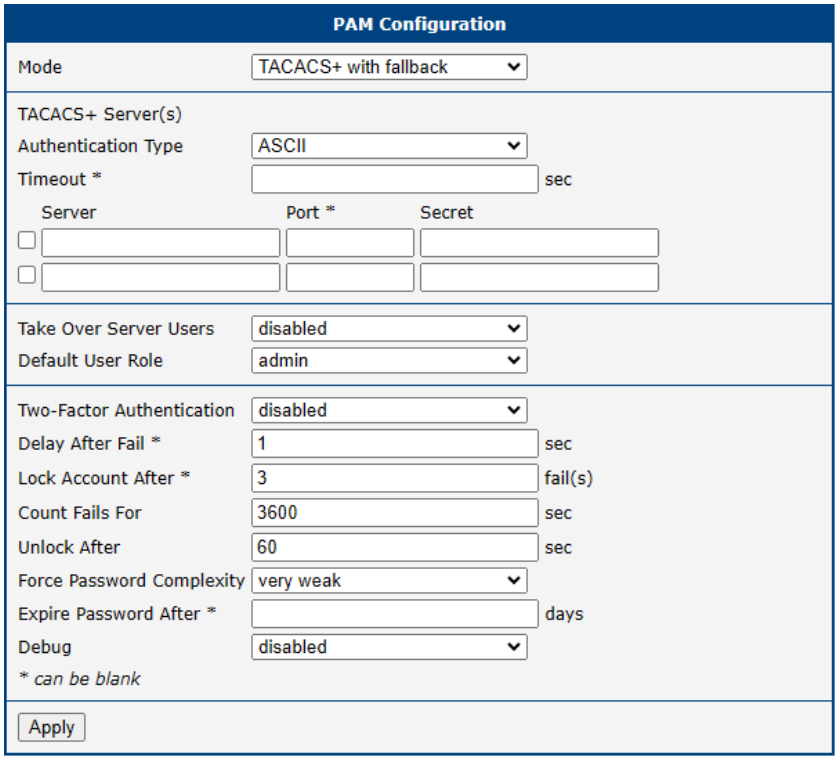


Figure 79: Configuration of TACACS+

Item	Description
Authentication Type	Choose ASCII, PAP or CHAP as authentication type.
Timeout	Timeout for authentication to the TACACS+ server.
Server	Address of the TACACS+ server. Up to two servers can be configured.
Port	Port of the TACACS+ server.
Secret	The secret For authentication to the TACACS+ server.
Take Over Server Users	If enabled, a new user account is created during the login, in case the TACACS+ authentication is successful and appropriate local account does not exist. New accounts are created without the password. An existing user account with a password is never modified by this feature.
Default User Role	Choose the user role (*Admin* or *User*). This role corresponds with router's user roles, see Chapter 5.1. Selected role will be used for a new user when *Take Over Server Users* is used.

Table 57: Configuration of TACACS+

Two-Factor Authentication Service

To enable the two-factor authentication service, choose the service type you want to use from *Google Authenticator* or *OATH Toolkit* in the *Two-Factor Authentication* box, as shown in Figure 80.

To configure the two-factor authentication for a user, see Chapter 5.2.1 Two-Factor Authentication.

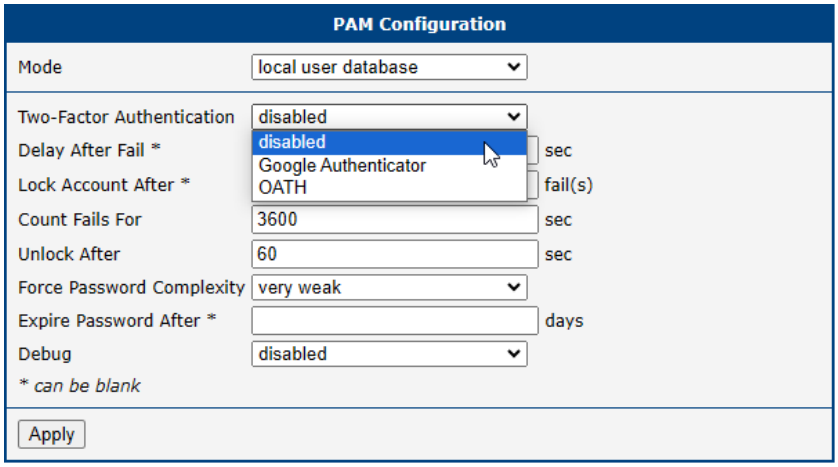


Figure 80: Enabling Two-Factor Authentication Service

Expired Password

If the password expires after the number of days defined in *Expire Password After* has passed, the user will be prompted to enter a new password as shown in Image 112. The new password must match the rules stated in the GUI, which depend on the *Force Password Complexity* level set in *Configuration* → *Services* → *PAM*, as described in Chapter 3.19.5.

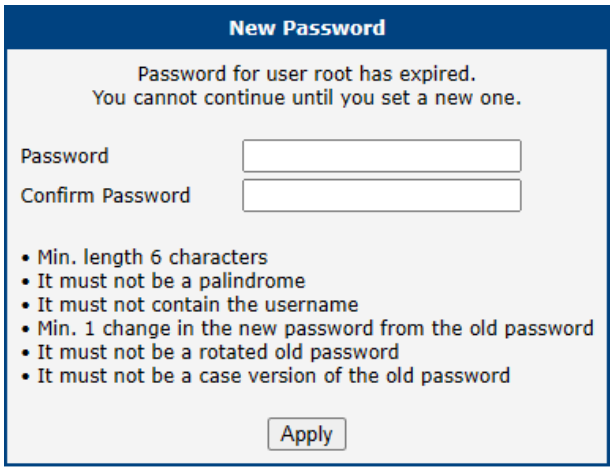


Figure 81: Expired Password Prompt

The user will be prompted to change their password when logging into the new router for the first time or if their password was changed by a user with an admin role.

3.19.6 SNMP

The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent which sends information about the router (and about its expansion ports eventually) to a management station. To open the *SNMP* page, click *SNMP* in the *Configuration* section of the main menu. SNMP (Simple Network Management Protocol) provides status information about the network elements such as routers or endpoint computers. In the version v3, the communication is secured (encrypted). To enable the SNMP service, mark the *Enable the SNMP agent* check box. Sending SNMP traps to IPv6 address is supported.

Item	Description
Name	Designation of the router.
Location	Location of where you installed the router.
Contact	Person who manages the router together with information how to contact this person.
Custom	You can use this input field to enter specific information tailored to your requirements.

Table 58: SNMP Agent Configuration

To enable the SNMPv1/v2 function, mark the *Enable SNMPv1/v2 access* check box. It is also necessary to specify a password for access to the *Community* SNMP agent. The default setting is *public*.

You can define a different password for the *Read* community (read only) and the *Write* community (read and write) for SNMPv1/v2. You can also define 2 SNMP users for SNMPv3. You can define a user as read only (*Read*), and another as read and write (*Write*). The router allows you to configure the parameters in the following table for every user separately. The router uses the parameters for SNMP access only.

To enable the SNMPv3 function, mark the *Enable SNMPv3 access* check box, then specify the following parameters:

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Authentication Password	Password used to generate the key used for authentication. Enter valid characters only, see chap. 1.1.2!
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol. Enter valid characters only, see chap. 1.1.2!

Table 59: SNMPv3 Configuration

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

Selecting *Enable M-BUS extension* and entering the *Baudrate*, *Parity* and *Stop Bits* lets you monitor the meter status connected via MBUS interface. MBUS expansion port is not currently supported, but it is possible to use an external RS232/MBUS converter.

Selecting Enable reporting to supervisory system and entering the *IP Address* and *Period* lets you send statistical information to the monitoring system, R-SeeNet.

Item	Description
IP Address	IPv4 or IPv6 address.
Period	Period of sending statistical information (in minutes).

Table 60: SNMP Configuration (R-SeeNet)

Each monitored value is uniquely identified using a numerical identifier *OID – Object Identifier*. This identifier consists of a progression of numbers separated by a point. The shape of each OID is determined by the identifier value of the parent element and then this value is complemented by a point and current number. So it is obvious that there is a tree structure. The following figure displays the basic tree structure that is used for creating the OIDs.

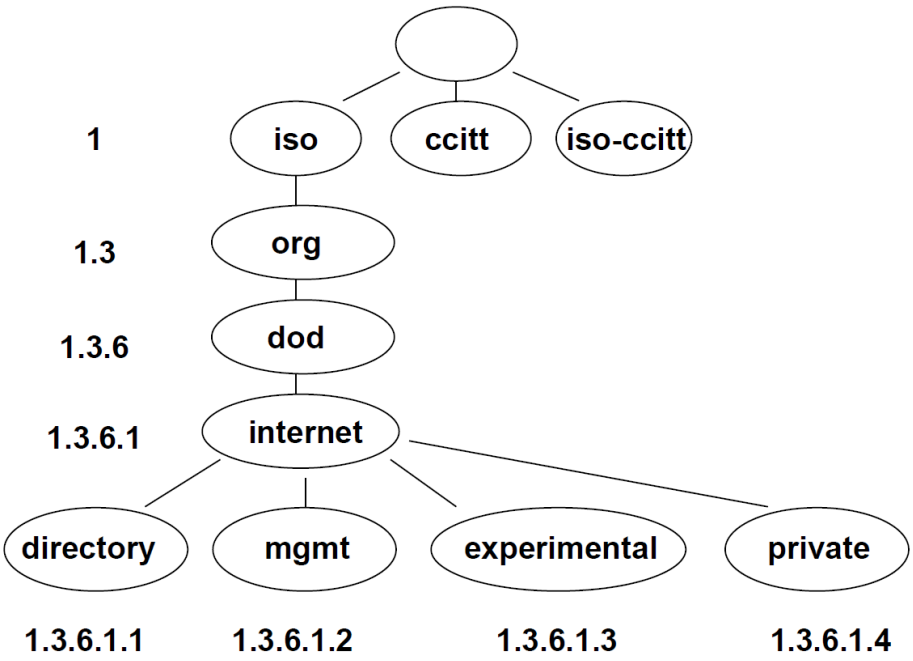


Figure 82: OID Basic Structure

The SNMP values that are specific for Advantech routers create the tree starting at OID = .1.3.6.1.4.1.30140. You interpret the OID in the following manner:

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 about the power voltage (OID 1.3.6.1.4.1.30140.3.4). For binary inputs and output, the following range of OID is used:

The list of available and supported OIDs and other details can be found in the application note *SNMP Object Identifiers* [11].

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

Table 61: Object identifier for binary inputs and output

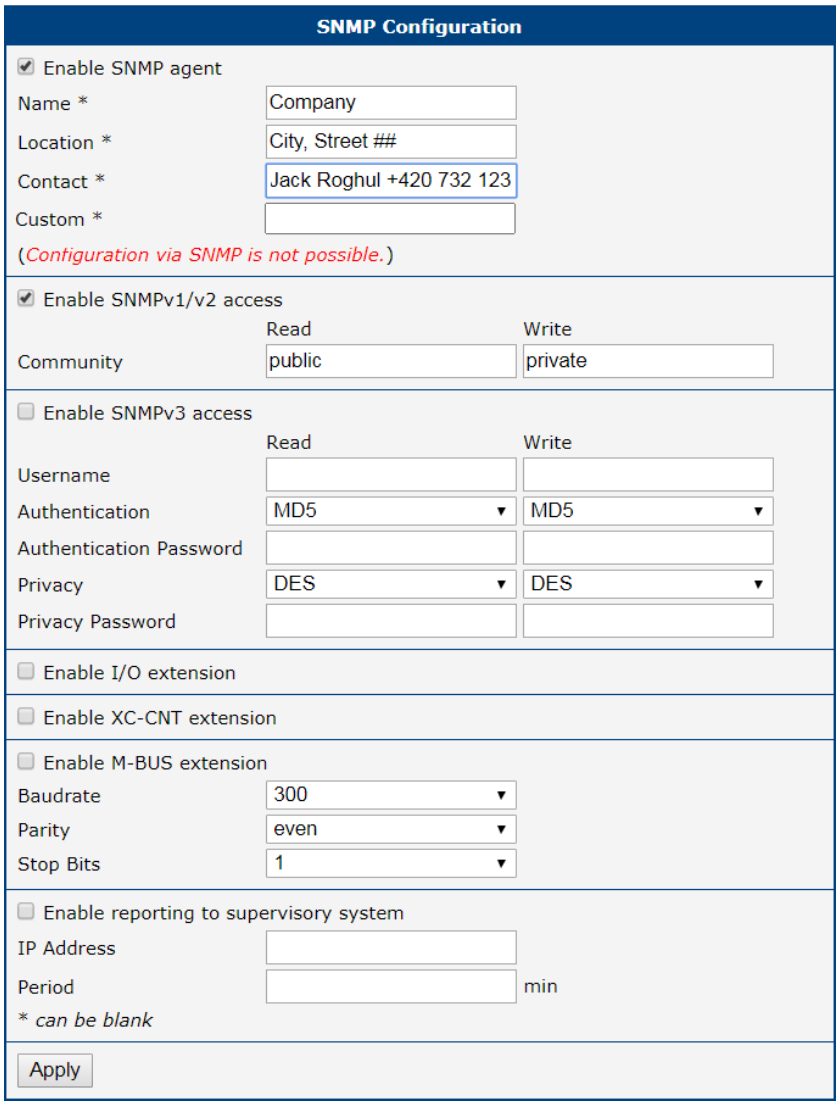


Figure 83: SNMP Configuration Example

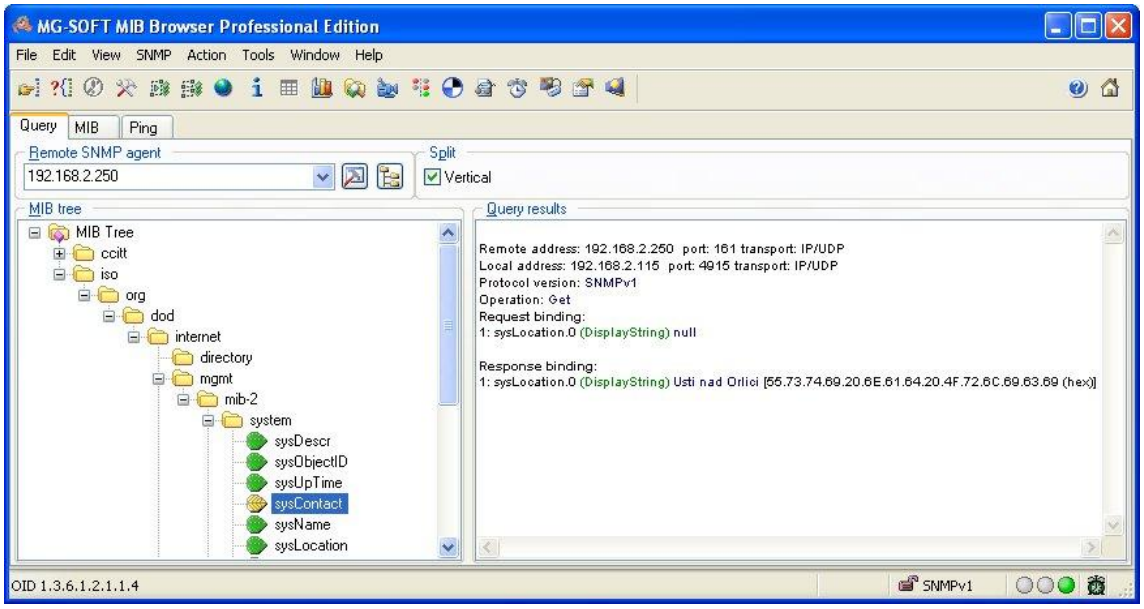


Figure 84: MIB Browser Example

In order to access a particular device enter the IP address of the SNMP agent which is the router, in the *Remote SNMP agent* field. The dialog displayed the internal variables in the MIB tree after entering the IP address. Furthermore, you can find the status of the internal variables by entering their OID.

The path to the objects is:

$$\text{iso} \rightarrow \text{org} \rightarrow \text{dod} \rightarrow \text{internet} \rightarrow \text{private} \rightarrow \text{enterprises} \rightarrow \text{Conel} \rightarrow \text{protocols}$$

The path to information about the router is:

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

3.19.7 SMTP

You use the *SMTP* form to configure the Simple Mail Transfer Protocol client (SMTP) for sending emails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
SMTP Port	Port the SMTP server is listening on.
Secure Method	none, SSL/TLS, or STARTTLS. The secure method must be supported by the SMTP server.
Username	Name for the email account.
Password	Password for the email account. Enter valid characters only.
Own Email Address	Address of the sender.

Table 62: SMTP client configuration

The mobile service provider may block other SMTP servers, so you might only be able to use the SMTP server of the service provider.

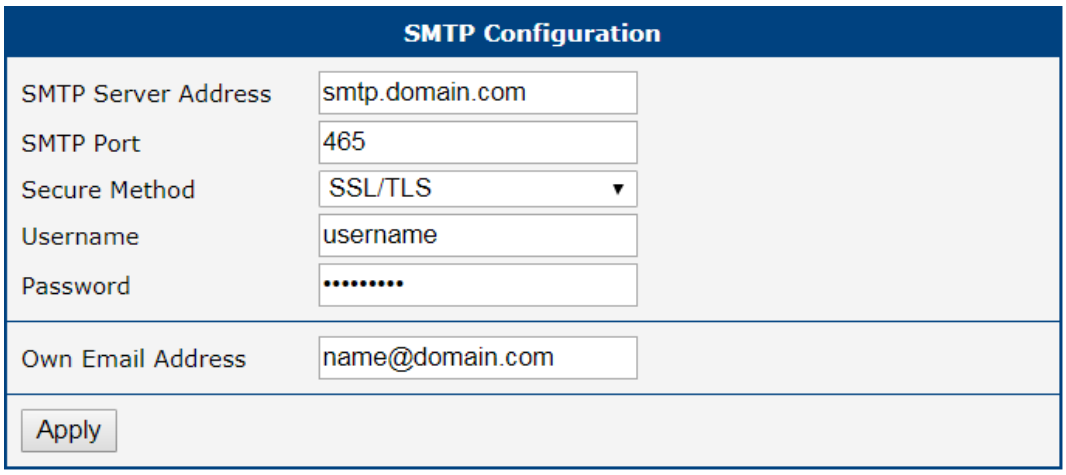


Figure 85: SMTP Client Configuration Example

You can send emails from the startup script. The *Startup Script* dialog is located in *Scripts* in the *Configuration* section of the main menu.

The router also allows you to send emails using an SSH connection. Use the `email` command, see *Commands and Scripts* [1] Application Note for details.

3.19.8 SMS

Open the *SMS Configuration* page, click *SMS* in the *Configuration* section of the main menu. The router can automatically send SMS messages to a cell phone or SMS message server when certain events occur. The form allows you to select which events generate an SMS message.

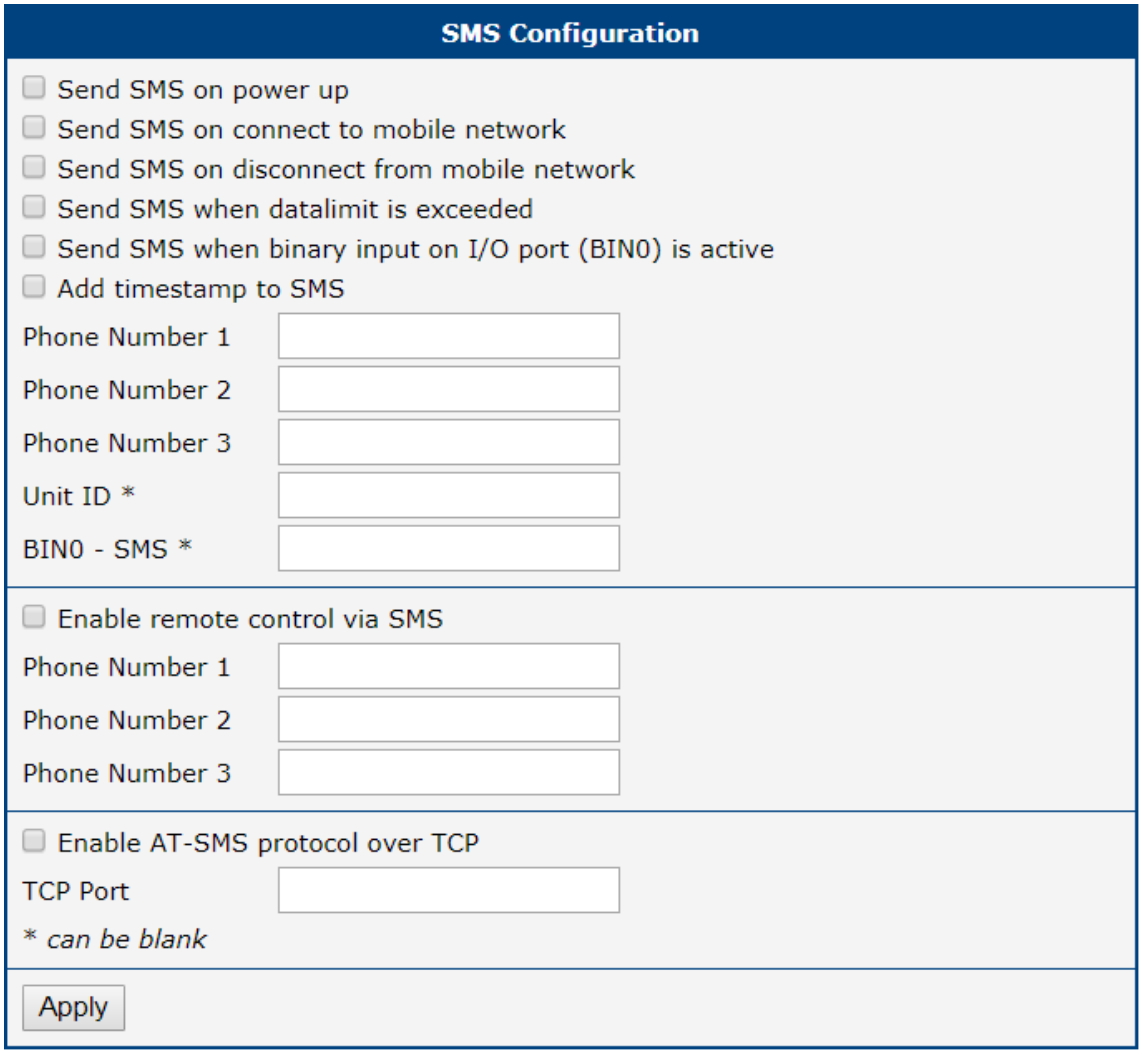


Figure 86: SMS Configuration

Item	Description
Send SMS on power up	Activates/deactivates the sending of an SMS message automatically on power up.
Send SMS on connect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is connected to a mobile network.
Send SMS on disconnect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is disconnection from a mobile network.

Continued on next page

Continued from previous page

Item	Description
Send SMS when datalimit exceeded	Activates/deactivates the sending of an SMS message automatically when the data limit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Add timestamp to SMS	Activates/deactivates the adding a time stamp to the SMS messages. This time stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Specifies the phone number to which the router sends the generated SMS.
Phone Number 2	Specifies the phone number to which the router sends the generated SMS.
Phone Number 3	Specifies the phone number to which the router sends the generated SMS.
Unit ID	The name of the router. The router sends the name in the SMS.
BIN0 – SMS	Text of the SMS message when the first binary input is activated.
BIN1 – SMS	Text of the SMS message when the second binary input is activated.

Table 63: SMS Configuration

Remote Control via SMS

After you enter a phone number in the *Phone Number 1* field, the router allows you to configure the control of the device using an SMS message. You can configure up to three numbers for incoming SMS messages. To enable the function, mark the *Enable remote control via SMS* check box. The default setting of the remote control function is active.

Item	Description
Phone Number 1	Specifies the first phone number allowed to access the router using an SMS.
Phone Number 2	Specifies the second phone number allowed to access the router using an SMS.
Phone Number 3	Specifies the third phone number allowed to access the router using an SMS.
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 64: Control via SMS and AT-SMS over TCP

If you enter one or more phone numbers, then you can control the router using SMS messages sent only from the specified phone numbers.
If you enter the wild card character ∗, then you can control the router using SMS messages sent from any phone number.

Most of the control SMS messages do not change the router configuration. For example, if the router is changed to the off line mode using an SMS message, the router remains in this mode, but it will return back to the on-line mode after reboot. The only exception is *set profile* command that changes the configuration permanently, see the table below.

To control the router using an SMS, send only message text containing the control command. You can send control SMS messages in the following form:

SMS	Description
go online sim 1	The router changes to SIM1
go online sim 2	The router changes to SIM2
go online sim 3	The router changes to SIM3
go online sim 4	The router changes to SIM4
go online	Changes the router to the online mode
go offline	Changes the router to the off line mode
set out0=0	Sets the binary output to 0
set out0=1	Sets the binary output to 1
set profile std	Sets the standard profile. This change is permanent.
set profile alt1	Sets the alternative profile 1. This change is permanent.
set profile alt2	Sets the alternative profile 2. This change is permanent.
set profile alt3	Sets the alternative profile 3. This change is permanent.
reboot	The router reboots
get ip	The router responds with the IP address of the SIM card

Table 65: Control SMS

Note: Every received control SMS is processed and then **deleted** from the router! This may cause a confusion when you want to use AT-SMS protocol for reading received SMS (see section below).

Advanced SMS control: If there is unknown command in received SMS and remote control via SMS is enabled, the script located in "/var/scripts/sms" is run before the SMS is deleted. It is possible to define your own additional SMS commands using this script. Maximum of 7 words can be used in such SMS. Since the script file is located in RAM of the router, it is possible to add creation of such file to Startup Script. See example in *Commands and Scripts* Application Note [1].

AT-SMS Protocol

AT-SMS protocol is a private set of AT commands supported by the routers. It can be used to access the cellular module in the router directly via commonly used AT commands, work with short messages (send SMS) and cellular module state information and settings.

Setting the parameters in the *Enable AT-SMS protocol over TCP* frame, you can enable the router to use AT-SMS protocol on a TCP port. This function requires you to specify a TCP port number.

Item	Description
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 66: Sending/receiving of SMS on TCP port specified

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

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

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the Mobile WAN interface
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+CNUM	Returns the phone number, if available (stored on SIM card)
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to find out the SIM card state and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number
AT+CSCS	Selects the character set
AT+CSQ	Returns the signal strength of the registered network
AT+GMI	Returns the manufacturer specific identity
AT+GMM	Returns the manufacturer specific model identity
AT+GMR	Returns the manufacturer specific model revision identity
AT+GSN	Returns the product serial number
ATE	Determines whether or not the device echoes characters
ATI	Transmits the manufacturer specific information about the device

Table 67: List of AT Commands

A detailed description and examples of these AT commands can be found in the application note *AT commands* [12].

Sending SMS from Router

There are more ways how to send your own SMS from the router:

- Using AT-SMS protocol described above – if you establish a connection to the router through a serial interface or interface using the TCP protocol, then you can use AT commands to manage SMS messages. See application note *AT Commands (AT-SMS)* [12].
- Using HTTP POST method for a remote execution, calling CGI scripts in the router. See *Commands and Scripts* Application Note [1] for more details and example.
- From Web interface of the router, in *Administration* section, *Send SMS* item, see 5.8 Chapter.
- Using `gsmsms` command e.g. in terminal when connected to the router via SSH, see *Commands and Scripts* Application Note [1].

Examples of SMS Configuration

Example 1 Sending SMS Configuration

After powering up the router, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connecting to mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

After disconnecting from the mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

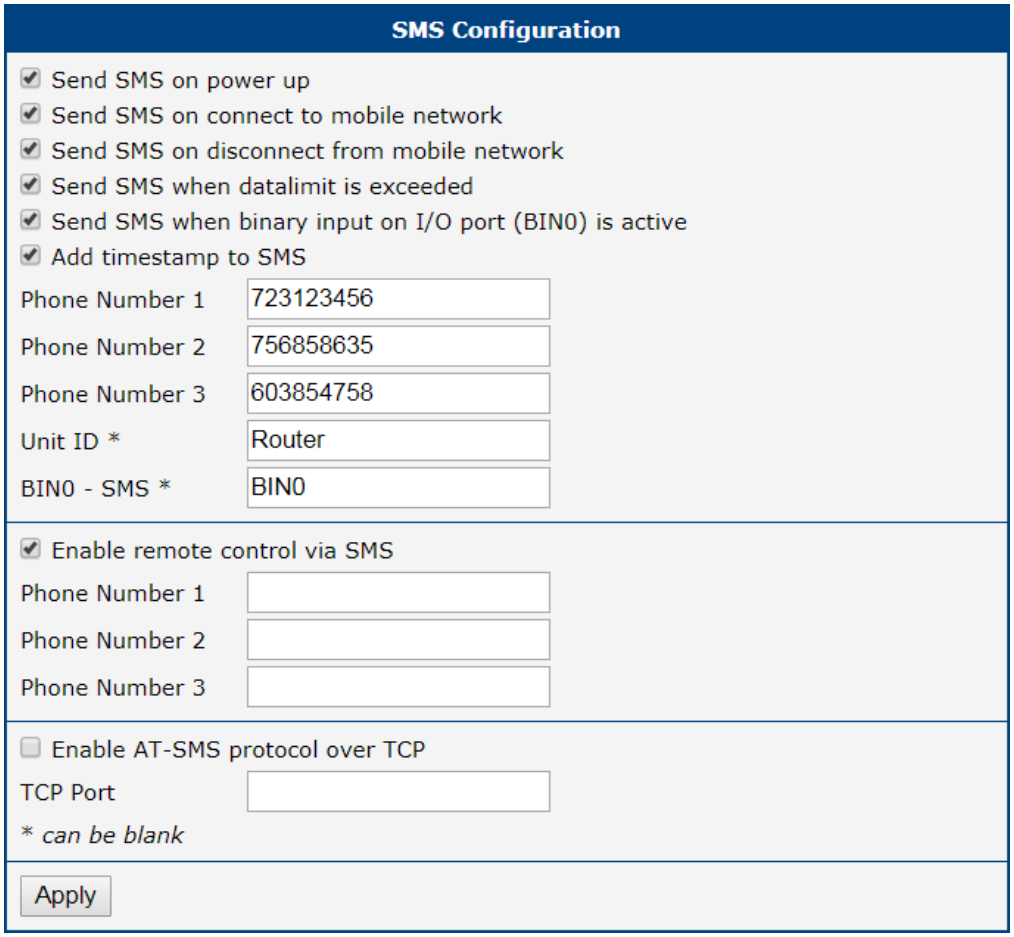


Figure 87: SMS Configuration for Example 1

Example 2 Control the Router Sending SMS from any Phone Number

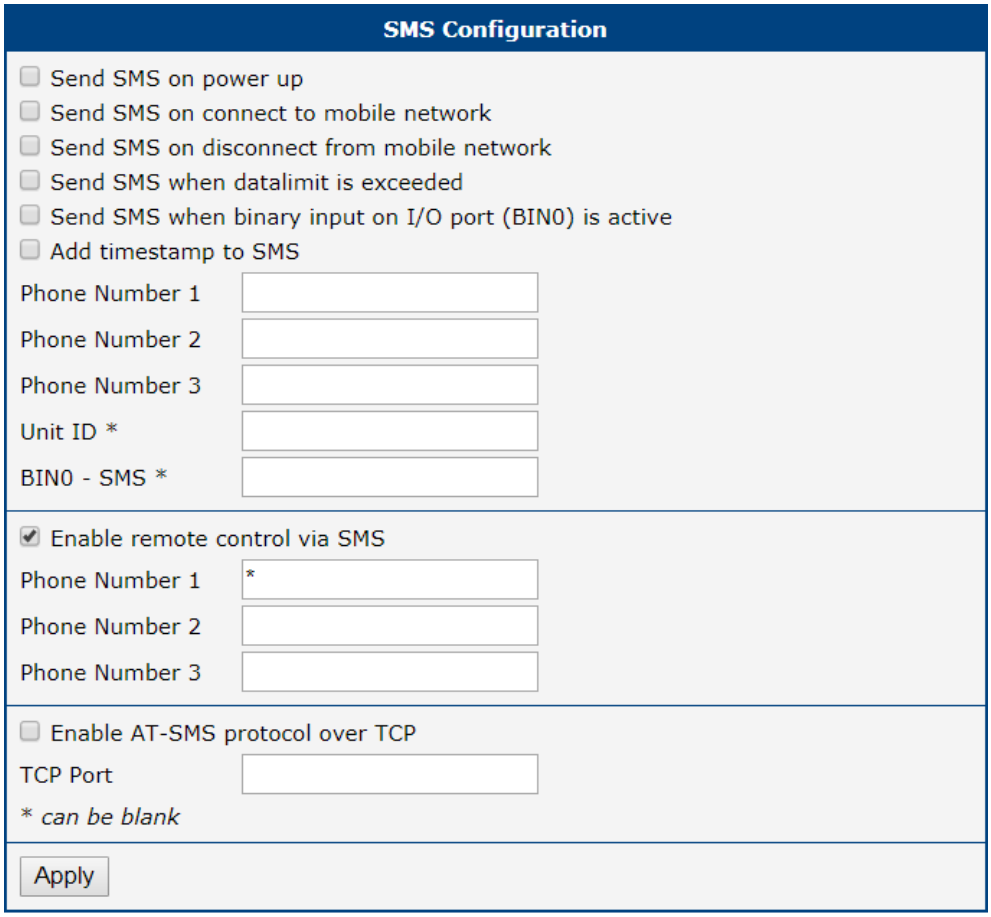


Figure 88: SMS Configuration for Example 2

Example 3 Control the Router Sending SMS from Two Phone Numbers

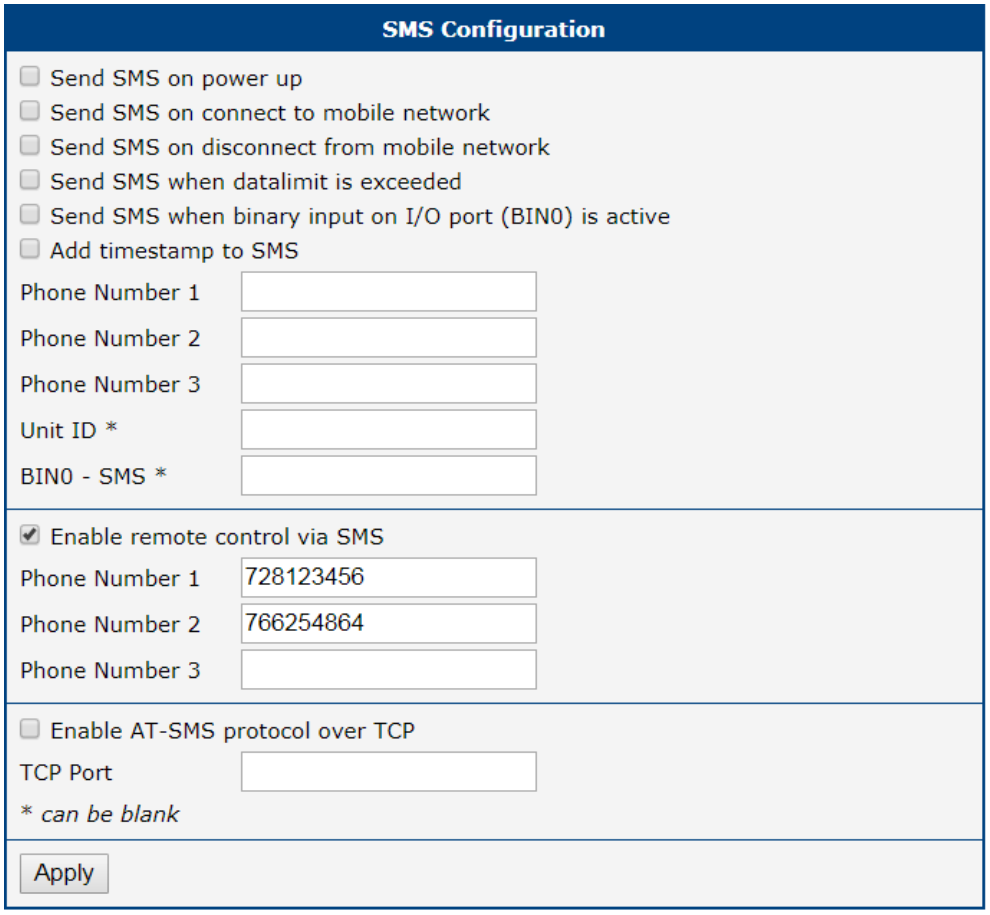


Figure 89: SMS Configuration for Example 3

3.19.9 SSH

SSH protocol (Secure Shell) allows to carry out a secure remote login to the router. Configuration form of SSH service can be done in *SSH* configuration page under *Services* menu item. By ticking *Enable SSH service* item the SSH server on the router is enabled.

Item	Description
Enable SSH service	Enabling of SSH service.
Port	Listening port.
Session Timeout	Inactivity timeout when the session is closed. The maximum allowed value may vary based on security requirements for the specific model.
Login Banner	The text specified in this field will be displayed in the console during the SSH login just after the login name entry.
Keep the current SSH key	Choose to keep current key.
Generate a new SSH key	Choose to generate new key.
Key Type	Choose the key type to be generated. The minimum allowed value may vary based on security requirements for the specific model. There are two types of keys: the RSA (Rivest-Shamir-Adleman) key and the ED25519 key. The ED25519 key is based on elliptic curve cryptography and is considered more secure than RSA.

Table 68: Parameters for SSH service configuration

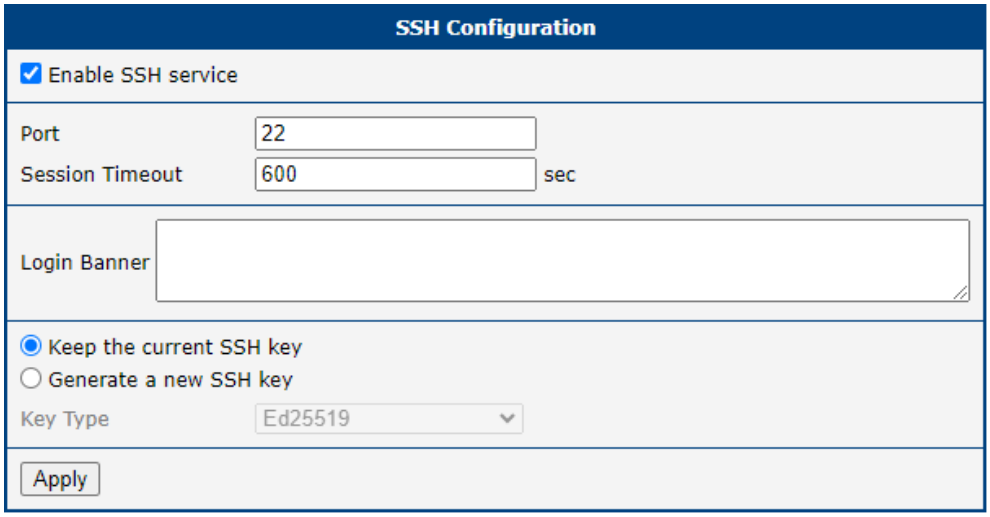


Figure 90: Configuration of HTTP service

3.19.10 Syslog

Configuration of the system log, known as *syslog*, is accessible from this configuration page. It is possible to limit the log size by specifying the maximum number of entries (rows). Additionally, users have the option to set an address and UDP port for distributing the log in real time.

To view this log, navigate to the router's GUI via *Status* → *System Log*, or access it through the console with the `slog` command.

Položka	Popis
Log Size	Restriction of log size by the maximum number of rows.
Log Persistent	Set to *yes* to enable logging to a file saved in non-volatile memory, ensuring that logs are preserved even after the router is powered down. **This feature is exclusive to routers equipped with eMMC memory.**
Remote Host	Remote host address for real-time log distribution. Hostnames are supported[1].
Remote UDP Port	UDP port for real-time log distribution.
Device ID	A unique identification string for remote logging purposes. If left blank, the default string *Router* is utilized.

Table 69: Syslog configuration

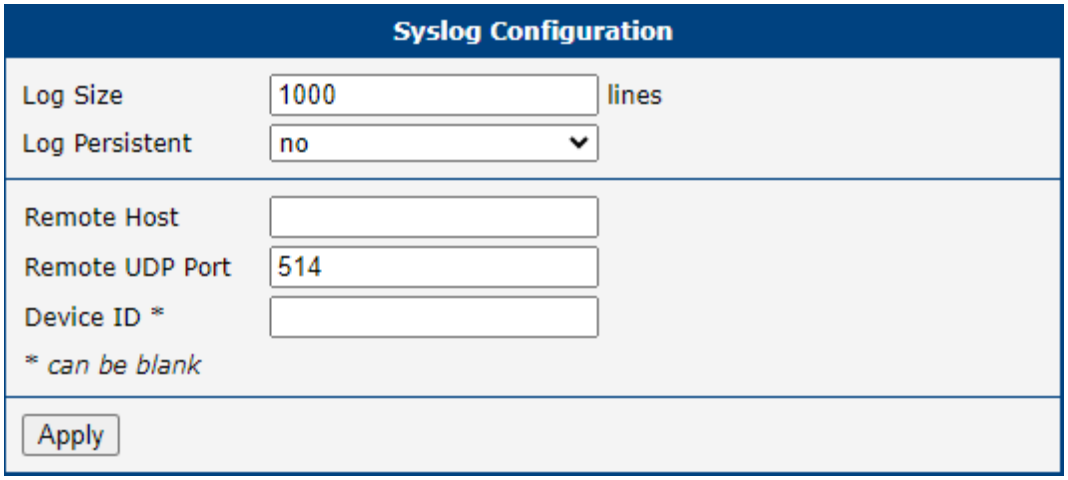


Figure 91: Syslog configuration

[1] DNS translation is refreshed every 60 minutes.

3.19.11 Telnet

Telnet is a protocol used to provide a bidirectional interactive text-oriented communication facility with the router. Configuration form of Telnet service can be done in *Telnet* configuration page under *Services* menu item.

Item	Description
Enable Telnet service	Enabling of Telnet service.
Maximum Sessions	Is used to close inactive sessions. The server will terminate a Telnet session after it has not been used for the given amount of seconds. The range is from 1 to 500.

Table 70: Parameters for Telnet service configuration

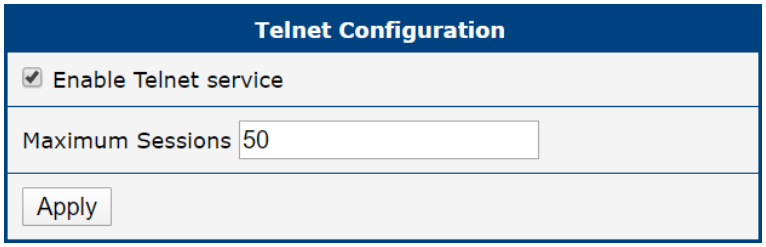


Figure 92: Configuration of Telnet service

3.20 USB Port Configuration

You can use a USB to RS232 converter to send data out of the serial port from the Ethernet network in the same manner as the RS232 expansion port function. To specify the values for the USB port parameters, click *USB Port* in the *Configuration* section of the main menu. The following tables describe the parameters available in the configuration form. IPv6 TCP/UDP client/server are supported.

The USB port can be disabled by clearing the *Enable external USB port* checkbox. Ensure that all filesystems attached to storage are unmounted before disabling the USB port.

The USB port can be disabled by clearing the *Enable external USB port* checkbox. Ensure that all filesystems attached to storage are unmounted before disabling the USB port.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: • **none** – data will be sent without parity. • **even** – data will be sent with even parity. • **odd** – data will be sent with odd parity.
Stop Bits	Number of stop bit.
Flow Control	Set the flow control to **none** or **hardware**.
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.
Protocol	Communication protocol: • **TCP** – communication using a linked protocol TCP. • **UDP** – communication using a unlinked protocol UDP.
Mode	Mode of connection: • **TCP server** – The router will listen for incoming TCP connection requests. • **TCP client** – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to *TCP client* above, it is necessary to enter the *Server address* and *TCP port*. IPv4 and IPv6 addresses are allowed.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 71: USB Port Configuration 1

If you mark the *Reject new connections* check box, then the router rejects any other connection attempt. This means that the router no longer supports multiple connections.

If you mark the *Check TCP connection* check box, the router verifies the TCP connection.

Item	Description
Keepalive Time	Time after which the router verifies the connection.
Keepalive Interval	Length of time that the router waits on an answer.
Keepalive Probes	Number of tests that the router performs.

Table 72: USB Port Configuration 2

When you mark the *Use CD as indicator of the TCP connection* check box, the router uses the carrier detection (CD) signal to verify the status of the TCP connection. The CD signal verifies that another device is connected to the other side of the cable.

CD	Description
Active	TCP connection is enabled
Nonactive	TCP connection is disabled

Table 73: CD Signal description

When you mark the *Use DTR as control of TCP connection* check box, the router uses the data terminal ready (DTR) single to control the TCP connection. The remote device sends a DTR single to the router indicating that the remote device is ready for communications.

DTR	Description server	Description client
Active	The router allows the establishment of TCP connections.	The router initiates a TCP connection.
Nonactive	The router denies the establishment of TCP connections.	The router terminates the TCP connection.

Table 74: DTR Signal Description

The router supports the following USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

The changes in settings will apply after pressing the *Apply* button.

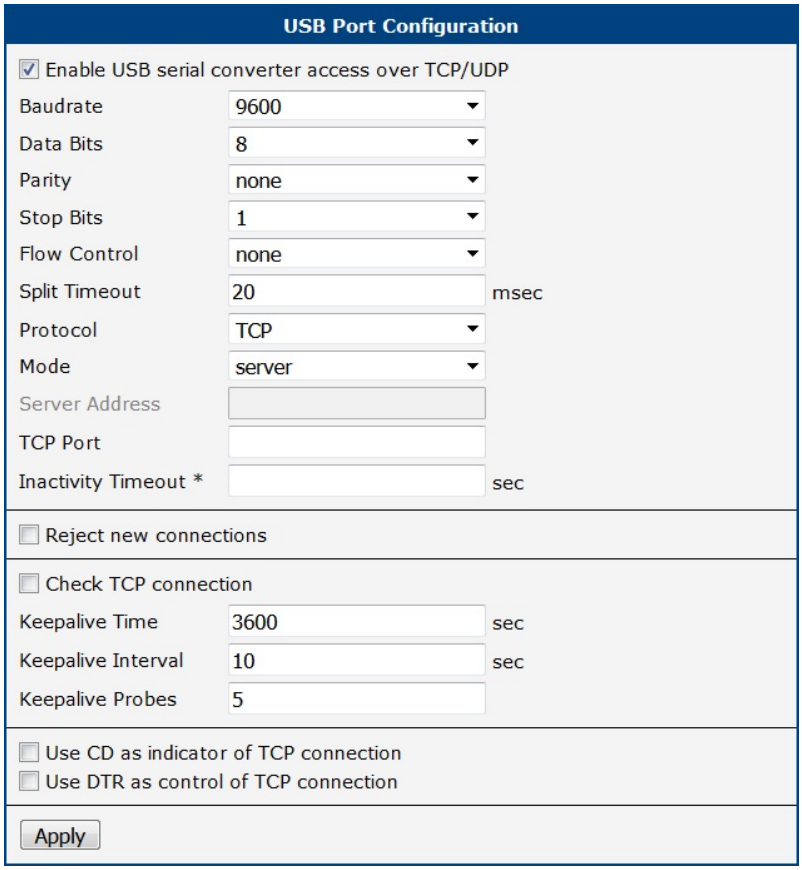


Figure 93: USB configuration

3.20.1 Examples of USB Port Configuration

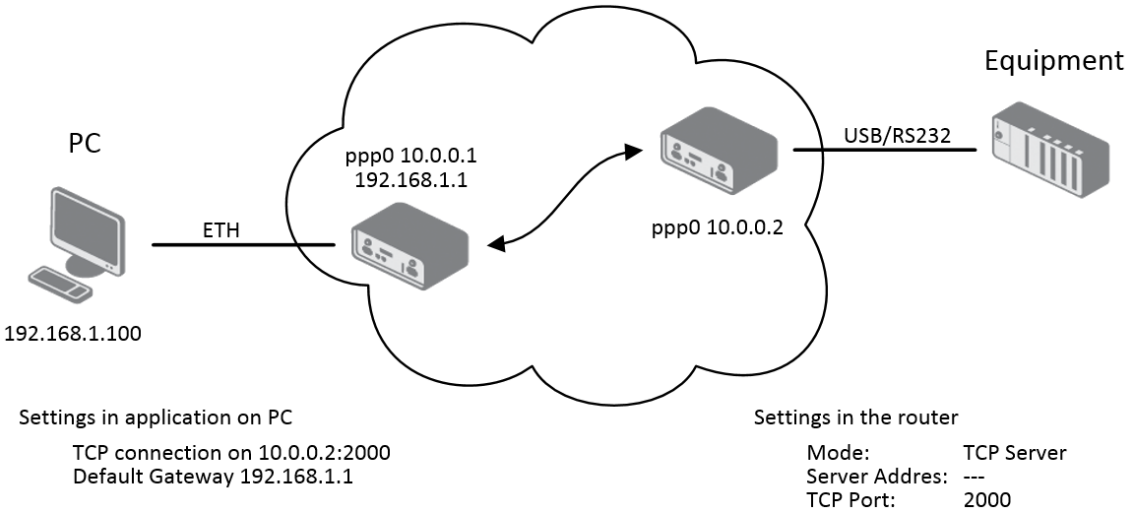


Figure 94: Example 1 – USB port configuration

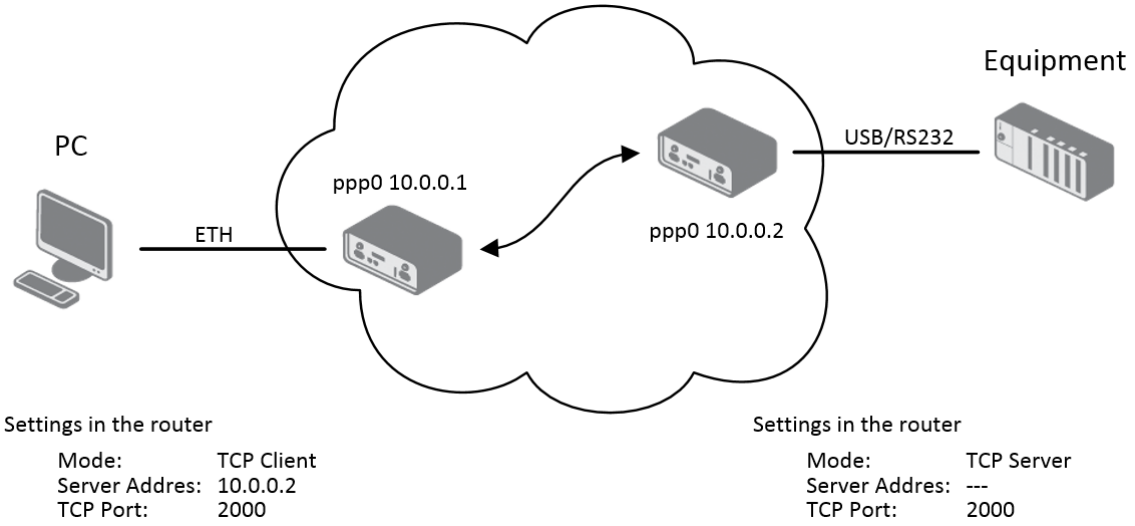


Figure 95: Example 2 – USB port configuration

3.21 Scripts

There is possibility to create your own shell scripts executed in the specific situations. Go to the *Scripts* page in the *Configuration* section in the menu. The menu item will expand and there are *Startup Script*, *Up/Down IPv4* and *Up/Down IPv6* scripts you can use – there is IPv4 and IPv6 independent dual stack. For more examples of Scripts and possible commands see the Application Note *Commands and Scripts* [1].

3.21.1 Startup Script

Use the *Startup Script* window to create your own scripts which will be executed after all of the initialization scripts are run – right after the router is turned on or rebooted. To save the script press the *Apply* button.

Any changes made to a startup script will take effect next time the router is power cycled or rebooted. This can be done with the *Reboot* button in the *Administration* section, or by SMS message.

3.21.2 Example of Startup Script

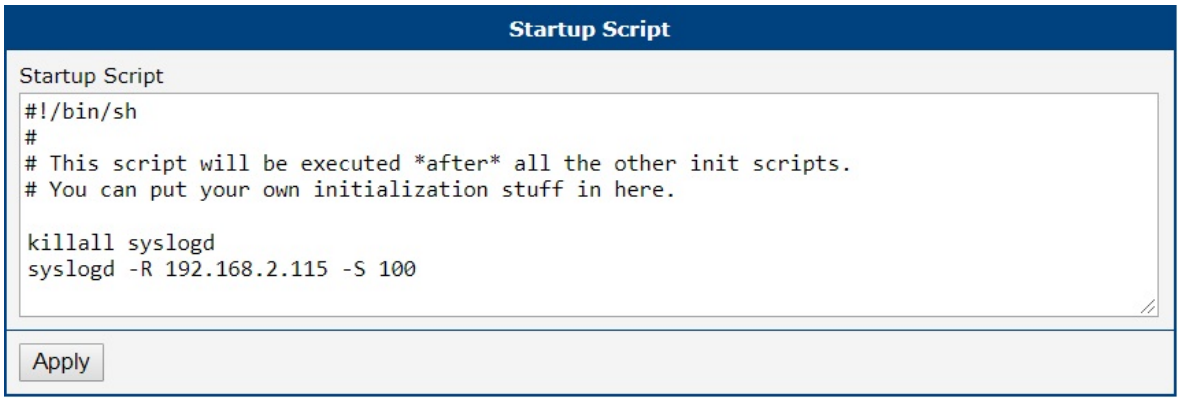


Figure 96: Example of a Startup Script

When the router starts up, stop `syslogd` program and start `syslogd` with remote logging on address 192.168.2.115 and limited to 100 entries. Add these lines to the startup script:

```
killall syslogd
syslogd -R 192.168.2.115 -S 100
```

3.21.3 Up/Down Scripts

Use the *Up/Down IPv4* and *Up/Down IPv6* page to create scripts executed when the WAN connection is established (up) or lost (down). There is an independent IPv4 and IPv6 dual-stack implemented in the router, so there is independent IPv4 and IPv6 Up/Down script. *IPv4 Up/Down Script* runs only on the IPv4 WAN connection established/lost, *IPv6 Up/Down Script* runs only on the IPv6 WAN connection established/lost. Any scripts entered into the *Up Script* window will run after a WAN connection is established. Script commands entered into the *Down Script* window will run when the WAN connection is lost.

The changes in settings will apply after pressing the *Apply* button. Also you need to reboot the router to make Up/Down Script work.

3.21.4 Example of IPv6 Up/Down Script

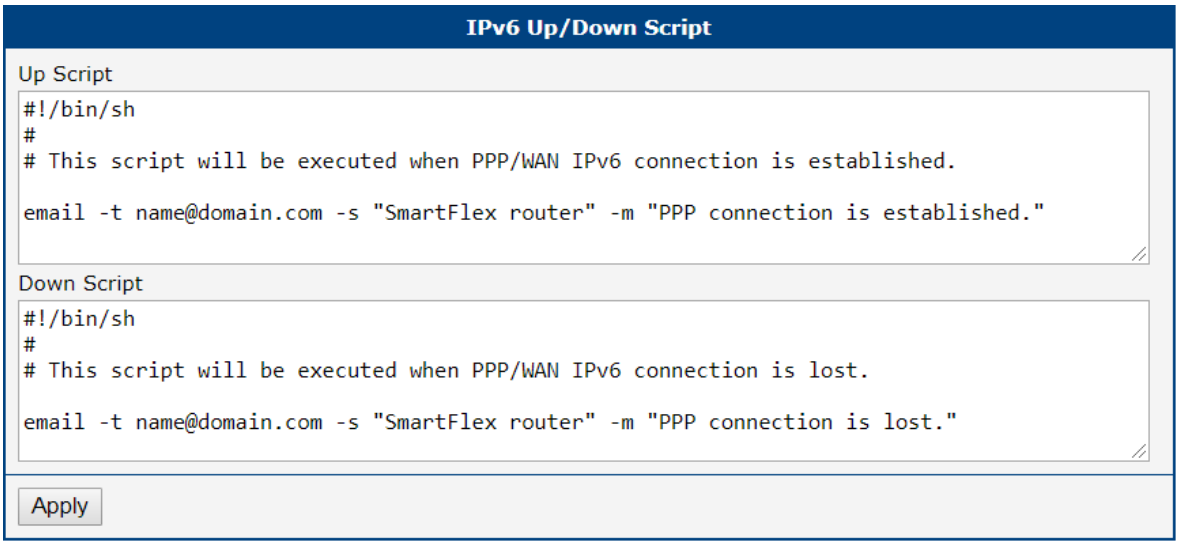


Figure 97: Example of IPv6 Up/Down Script

After establishing or losing an IPv6 WAN connection, the router sends an email with information about the connection state. It is necessary to configure *SMTP* before.

Add this line to the *Up Script* field:

```
email -t name@domain.com -s "Router" -m "Connection up."
```

Add this line to the *Down Script* field:

```
email -t name@domain.com -s "Router" -m "Connection down."
```

3.22 Automatic Update

The router can be configured to automatically check for firmware updates from an FTP site or a web server and update its firmware or configuration information; see Figure 98 and Table 75.

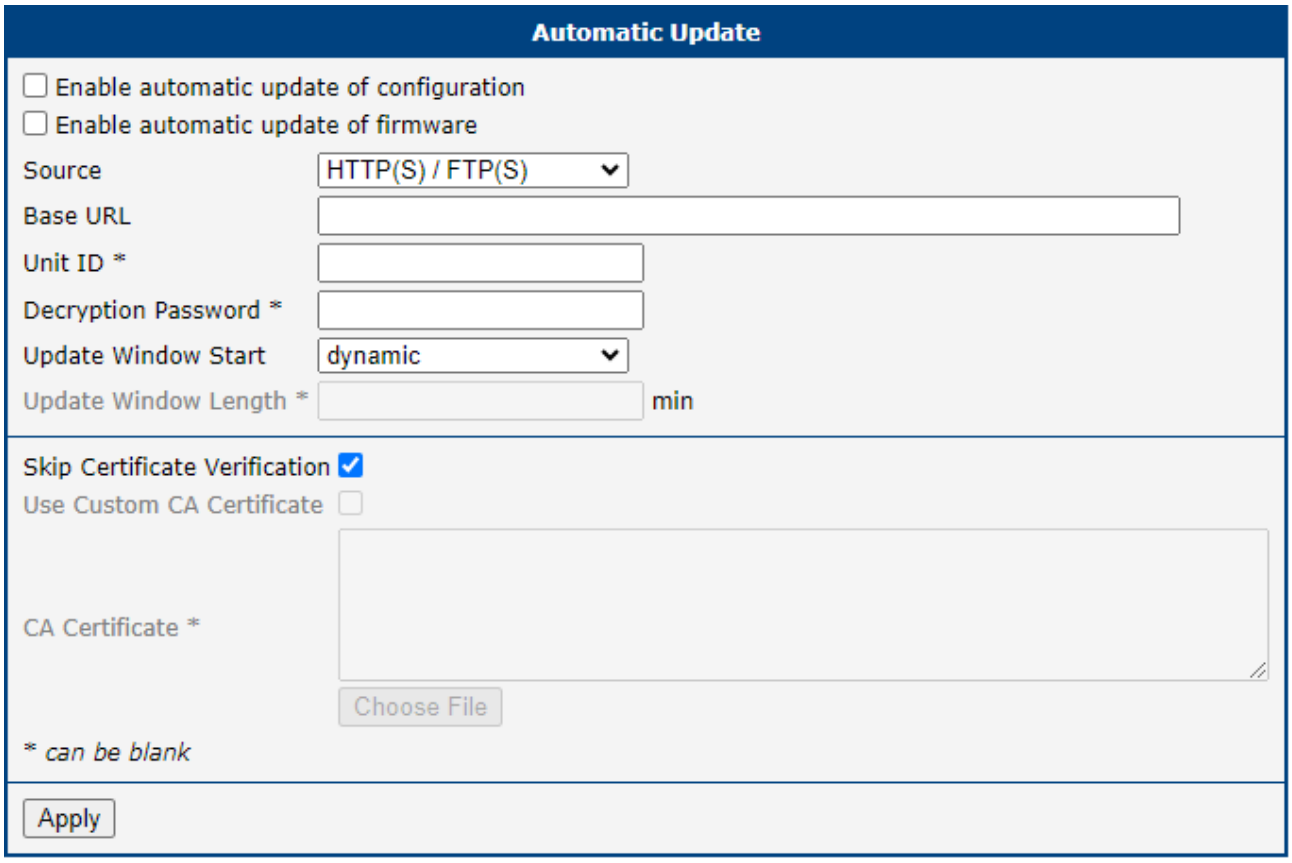


Figure 98: Automatic Update

Item	Description
Enable automatic update of configuration	If enabled and if there is a new configuration file, it will update it and reboot.
Enable automatic update of firmware	If enabled and if there is a new firmware, it will update it and reboot.
Source	Select the location of the update files: • **HTTP(S)/FTP(S) server** – Updates are downloaded from the Base URL address below. The used protocol is specified by that address: HTTP, HTTPS, FTP, or FTPS (only implicit mode is supported). • **USB flash drive** – The router finds the current firmware or configuration in the root directory of the connected USB device. • **Both** – Looking for the current firmware or configuration from both sources.
Base URL	Base URL, IPv4, or IPv6 address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP, or FTPS), see examples below.

Continued on the next page

Continued from previous page

Item	Description
Unit ID	Name of configuration (name of the file without extension). If the *Unit ID* is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot).
Decryption Password	Password for decryption of the encrypted configuration file. This is required only if the configuration is encrypted.
Update Window Start	Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis. If the time is not specified (set to *dynamic*), the automatic update is performed five minutes after the router boots up and then regularly every 24 hours.
Update Window Length	This value defines the period within which the update will be done. This period starts at the time set in the *Update Window Start* field. The exact time, when the update will be done, is generated randomly.
Skip Certificate Verification	If enabled, the server certificate validation is not executed.
Use Custom CA Certificate	If enabled, the server certificate validation is executed to verify server identity.
CA Certificate	CA certificate to validate on the server.

Table 75: Automatic Update Options

To prevent possible unwanted manipulation of the files, the router verifies that the downloaded file is in the `tar.gz` format. First, the format of the downloaded file is checked. Then, the type of architecture and each file in the archive (`tar.gz` file) is checked.

The **configuration file** name consists of the *Base URL*, the hardware MAC address of the ETH0 interface, and the cfg extension. The hardware MAC address and cfg extension are added to the file name automatically, so it is not necessary to enter them. When the parameter *Unit ID* is enabled, it defines the specific configuration name that will be downloaded to the router, and the hardware MAC address in the configuration name will not be used.

The **firmware file** name consists of the *Base URL*, the type of router, and the bin extension. For the proper firmware filename, see the *Update Firmware* page in the *Administration* section; it is written there, see Chapter 5.11.

It is necessary to load two files (**.bin* and **.ver*) to the server. If only the **.bin* file is uploaded and the HTTP(S) server sends an incorrect *200 OK* response (instead of the expected *404 Not Found*) when the device tries to download the nonexistent **.ver* file, the router may download the *.bin* file repeatedly.

Firmware update can cause incompatibility with the router apps. It is recommended that you update router apps to the most recent version. Information about the router apps and firmware compatibility is provided at the beginning of the router app's Application Note.

The automatic update feature is also executed five minutes after the firmware upgrade, regardless of the scheduled time.

3.22.1 Example of Automatic Update

In the following example, the router is configured to check for new firmware or a configuration file daily at 1:00 a.m. This scenario is specifically tailored for the SmartFlex router.

- Firmware file: https://example.com/SPECTRE-v3-LTE.bin
- Configuration file: https://example.com/test.cfg

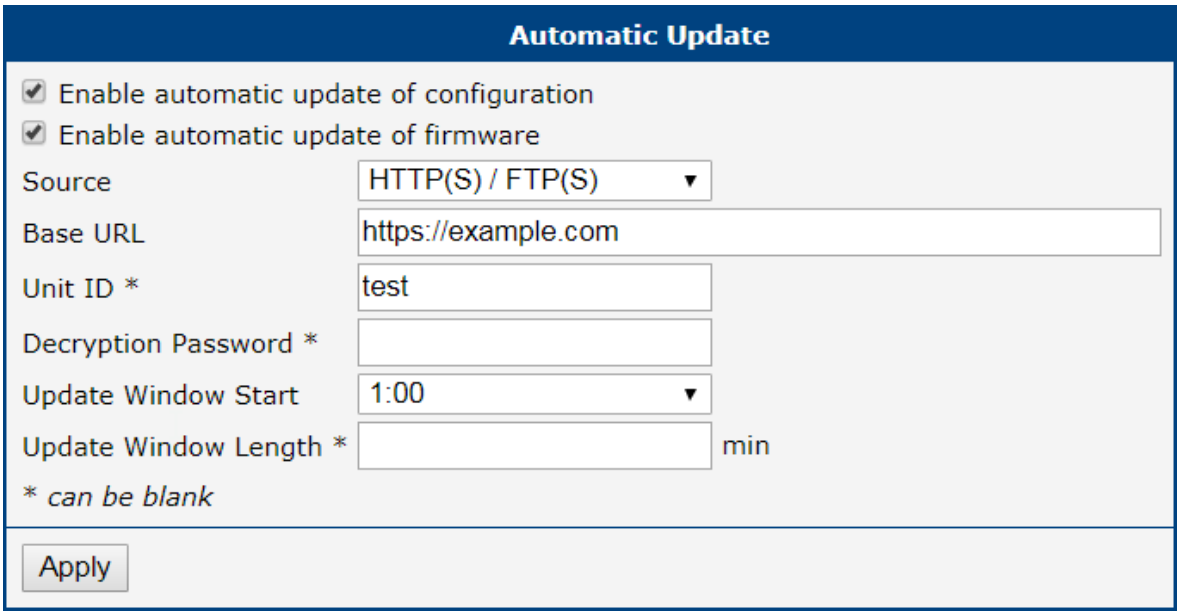


Figure 99: Example of Automatic Update 1

3.22.2 Example of Automatic Update Based on MAC

The example provided demonstrates how to check for new firmware or configurations daily between 1:00 a.m. and 3:00 a.m. The configuration file is encrypted, necessitating the setup of a decryption password. This specific example is applicable to the SmartFlex router with the MAC address 00:11:22:33:44:55.

- Firmware file: https://example.com/SPECTRE-v3-LTE.bin
- Configuration file: https://example.com/00.11.22.33.44.55.cfg

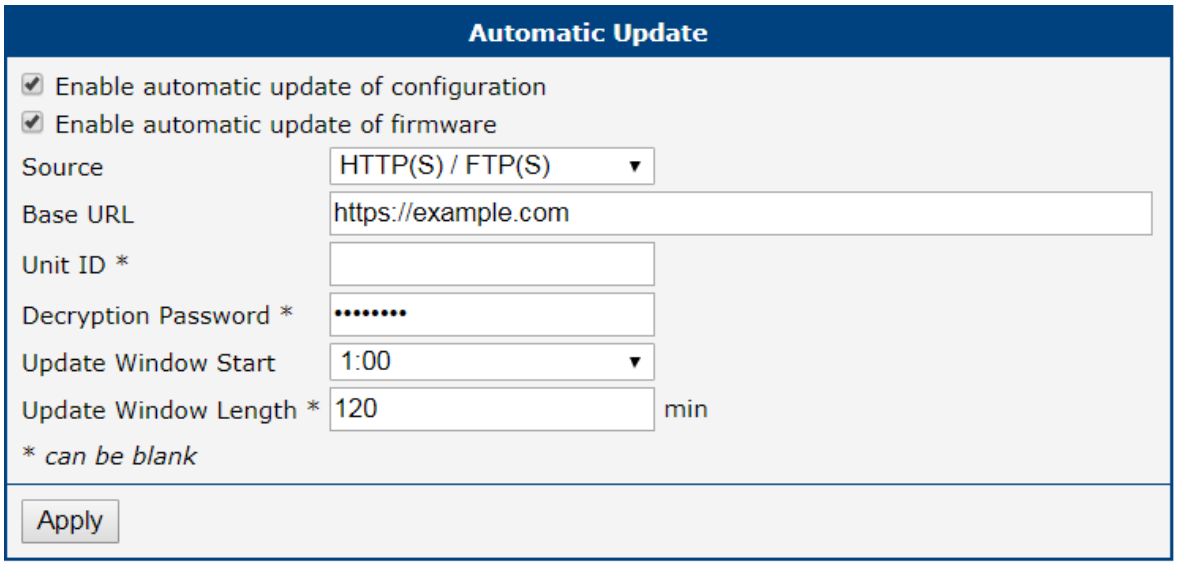


Figure 100: Example of Automatic Update 2

4. Customization

4.1 Router Apps

Router Apps (RA), formerly known as *User Modules*, enhance router functionality through custom software programs. These apps extend the router's capabilities in areas such as security and advanced networking, offering a flexible and customizable experience.

For Advantech routers, a diverse array of Router Apps is offered, encompassing categories such as connectivity, routing, services, among others. These applications are freely accessible on the Advantech *Router Apps* webpage, providing users with a wide range of options to enhance the functionality of their devices.

Figure 101 illustrates the default layout of the *Router Apps* configuration interface. The initial segment, titled *Installed Apps*, presents a comprehensive list of Router Apps currently installed on the device. The subsequent section, *Manual Installation*, provides the functionality for manually adding Router Apps to the system. Lastly, the third section facilitates the online acquisition and installation of RA accessible from a public server.

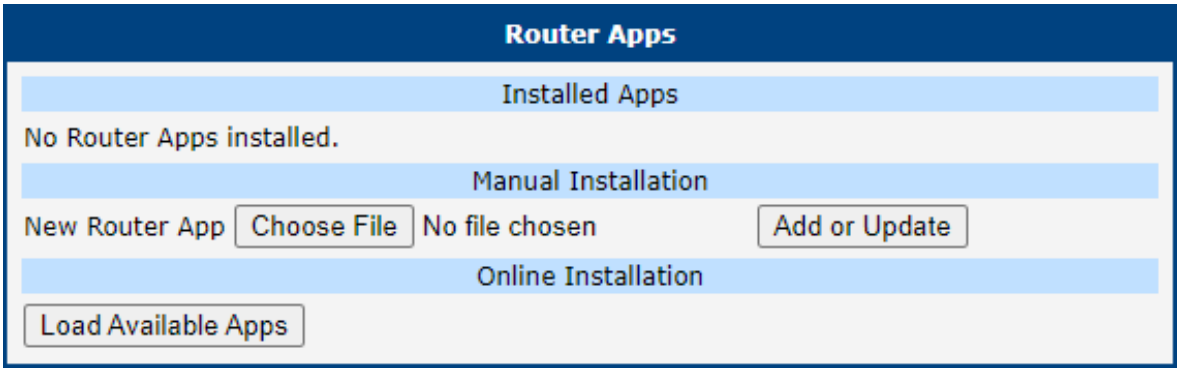


Figure 101: Default Router Apps GUI

Manual RA Installation and Update

For the manual installation of a RA, prepare the application package with a `*.tgz` extension. In the router interface, use the *Choose File* button to select your file and the *Add or Update* button to start the installation.

Online RA Installation and Update

To install Router Apps from the public server, it is imperative to first ensure that the router is correctly configured and connected as outlined in Chapter 4.2. By default, routers are set to automatically connect to the public Advantech server. To proceed with the installation, click on the *Load Available Apps* button, which initiates the loading of a comprehensive list of RA that are available on the server for installation.

Keep these notes in mind:

- The online RA installation functionality starts with firmware version 6.4.0 and is not available for the v2 production platform.
- Note that an Internet connection is required to access the public server. Without it, you will encounter an error: `"Cannot get auth header: Couldn't resolve host name"`.
- The list of online applications is updated only when the *Reload Available Apps* button is pressed. The last loading timestamp is visible next to this button.

- If the router is rebooted, the list of applications is cleared and needs to be reloaded.
- The *Load Available Apps* button is deactivated if the connection to the server is disabled.

Figure 102 displays an instance where the assortment of online applications accessible for installation has been successfully loaded. This figure further demonstrates that only the *Customer Logo* application, version v1.0.0, is installed on the local device, as indicated by its solitary listing in the *Installed Apps* section.

Within the *Online Installation* section, it is highlighted that an updated version of the *Customer Logo* application, version v1.1.0, is available for download from the server, showcasing the potential for upgrading existing applications directly through the router's interface.

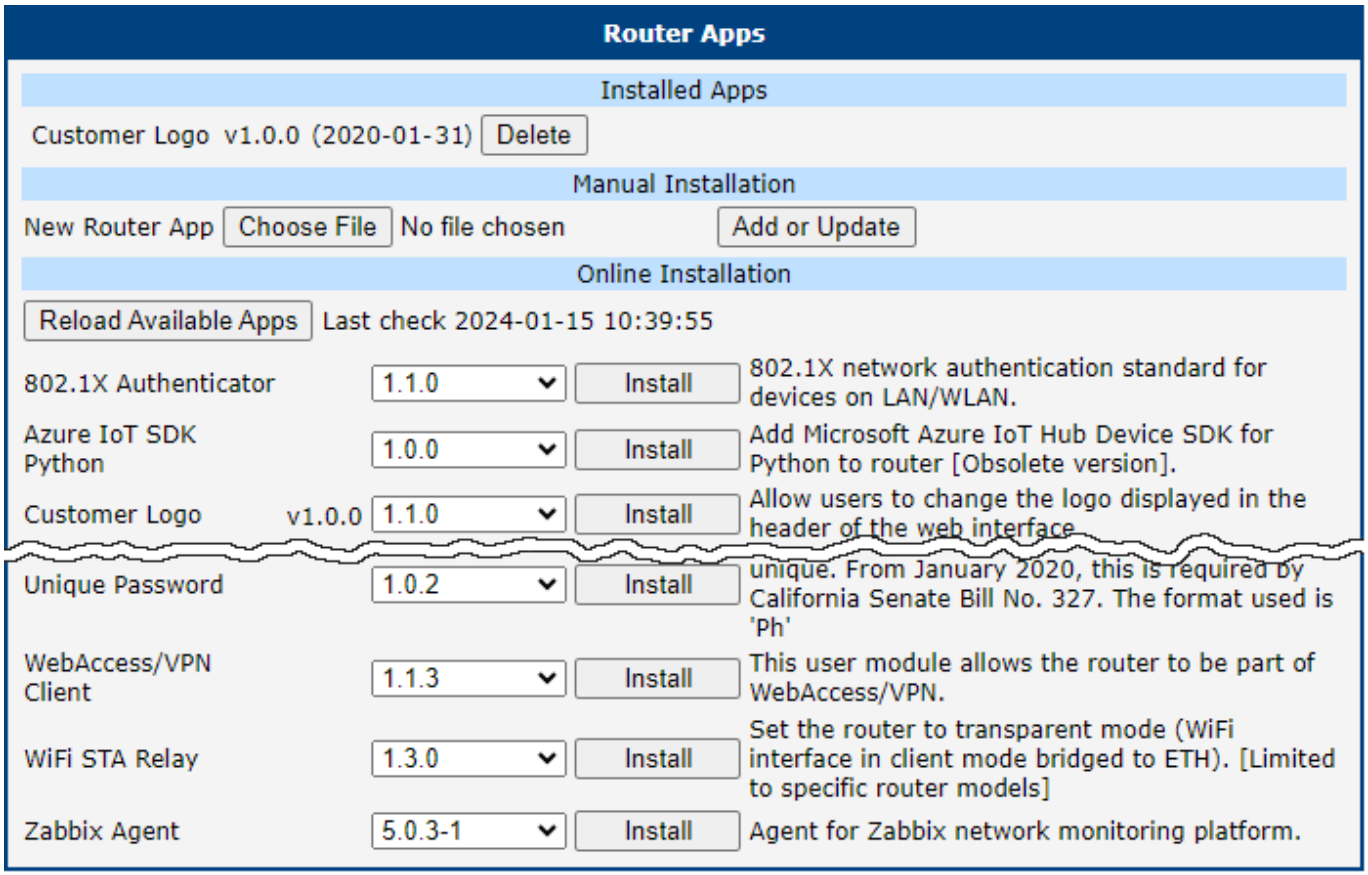


Figure 102: Router Apps GUI with Available Online Apps

RA Management

Installed Router Apps, regardless of whether they were installed manually or from the server, appear in the *Installed Apps* section.

Apps with an `index.html` or `index.cgi` page have a clickable link in their name. Clicking on this link opens the GUI of the respective application.

To remove an app, click the *Delete* button, which is located next to the respective application in the *Installed Apps* section.

The programming and compiling of router applications is described in the Application Note *Programming of Router Apps* [14].

4.2 Settings

To configure the connection settings for the online application hosting server, navigate to the *Customization* → *Settings* menu option. Figure 103 and Table 76 offer comprehensive details regarding the configuration parameters for the server, ensuring users can effectively customize their router to connect to the online application hosting server.

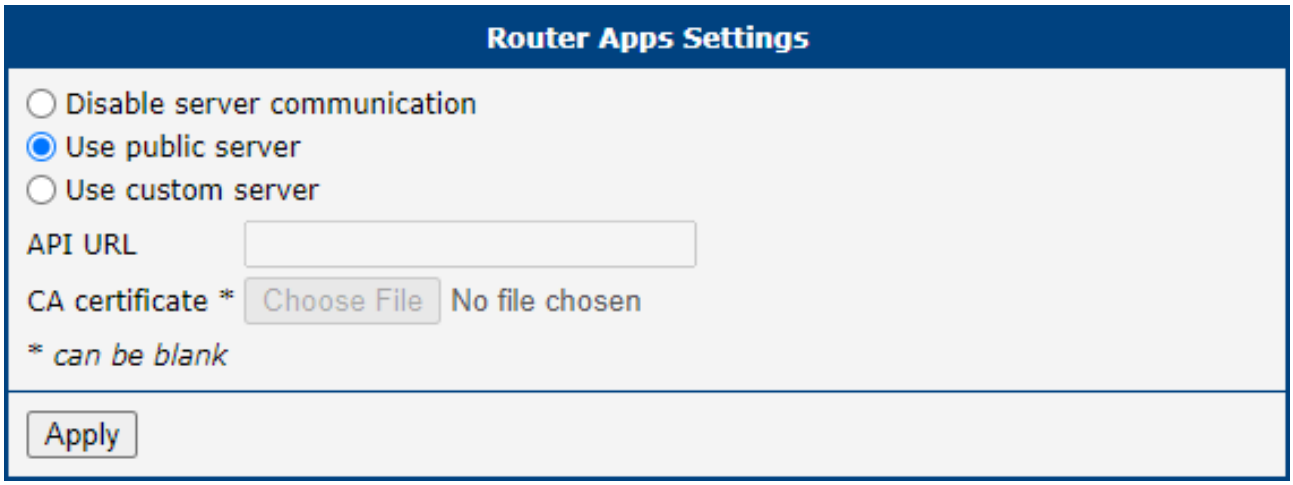


Figure 103: Router Apps Settings

Item	Description
Disable server communication	Connection to the server is disabled, preventing any data exchange with the online application hosting server.
Use public server	Opt to utilize the public server, managed by Advantech, as the primary source for Router Apps. This is the default configuration. An active internet connection is mandatory for accessing the server.
Use custom server[1]	Select this option to establish a connection with a self-hosted server that adheres to the Advantech specifications for Router Apps.
API URL	Enter the URL for the self-hosted server, ensuring the inclusion of the 'https://' prefix to denote a secure connection.
CA certificate	Provide the certificate for the self-hosted server, especially if it utilizes a Certificate Authority (CA) that is not widely recognized or standard.

Table 76: Router Apps Settings

[1] Operating your own self-hosted server is feasible exclusively with an on-premises installation of the *WebAccess/DMP* product by Advantech.

5. Administration

5.1 Manage Users

Be careful not to lock all users of the *Admin* role. In this state, any user has access rights to configure the users!

This configuration menu is only available for users with the *admin* role!

If a user with an admin role creates a new user or changes the password for another user, that user is required to change their password after the first login.

To manage the users, open the *Manage Users* form in the *Administration* section of the main menu, see Figure 104.

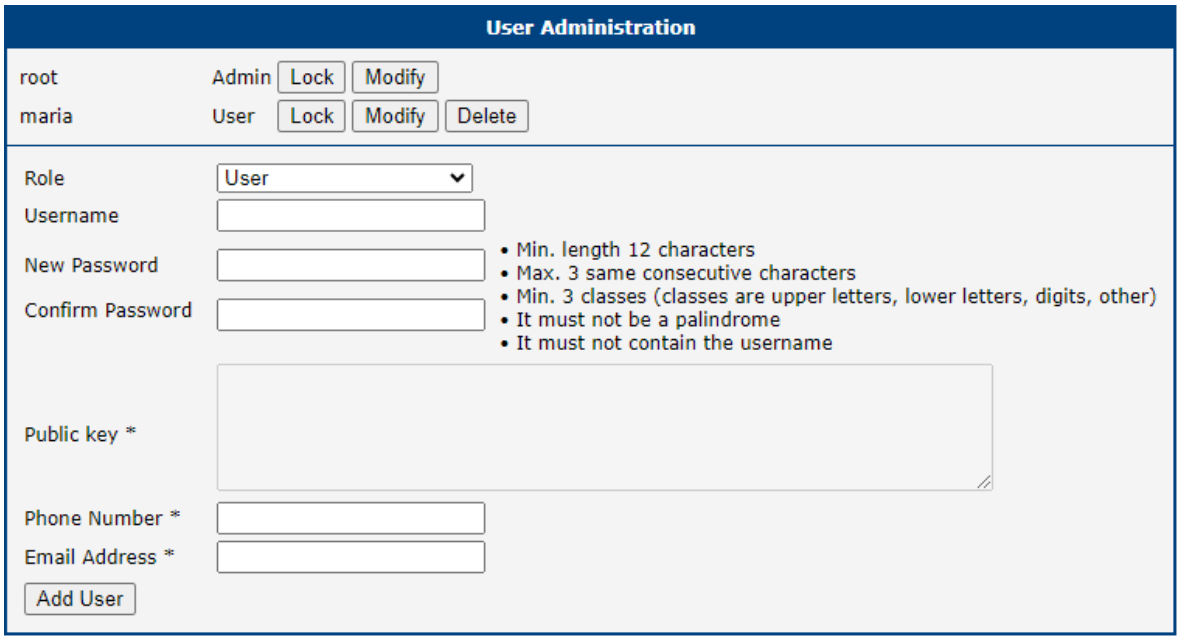


Figure 104: Users Administration Form

The first part of this configuration form contains a list of all existing users. Table 77 describes the meaning of the buttons located on the right of each user.

Button	Description
Lock	Locks the user account. This user is not allowed to log in to the router, either to the web interface or via SSH.
Modify	Allows you to change the password or key for the corresponding user, see Chapter 5.2.
Delete	Deletes the user account.

Table 77: Action Button Description

The second part of the configuration form allows adding a new user. All items are described in Table 78. To create a new user, configure all required items and click the *Add User* button.

Item	Description
Role	• **User** ◦ User with **basic permissions**. ◦ Read-only access to the web GUI. ◦ Some menu items are hidden in the web GUI. ◦ Full access to Router Apps GUI. ◦ No access to the router via Telnet, SSH or SFTP. ◦ Read-only access to the FTP server. • **Admin** ◦ User with **enhanced permissions**. ◦ Full access to all items in the web GUI. ◦ Access to the router via Telnet, SSH or SFTP. ◦ Not the same rights as the superuser on a Linux-based system.
Username	Specifies the name of the user having access to log in to the device.
New Password	Specifies the password for the user. It must match the rules stated in the GUI, which depend on the *Force Password Complexity* level set in *Configuration* → *Services* → *Authentication*, as described in Chapter **??**.
Confirm Password	Confirms the password.
Public key	Enter the SSH Public Key to enable passwordless SSH login. Refer to Chapter 5.2.2 for details.
Phone Number	User's phone number. If configured, an SMS is sent to the user when their password is changed. A functional SIM card is required.
Email Address	User's email address. If configured, an email is sent to the user when their password is changed. SMTP must be configured.
Add User	Click this button to create a new user based on the entries in the fields above.

Table 78: User Parameters

5.2 Modify User

If a user with a *User* role is logged in, they can manage only their user account. This can be done on the *Administration* → *Modify User* page. You will get the same configuration page if you have the *Admin* role when modifying another user account on the *Manage Users* page.

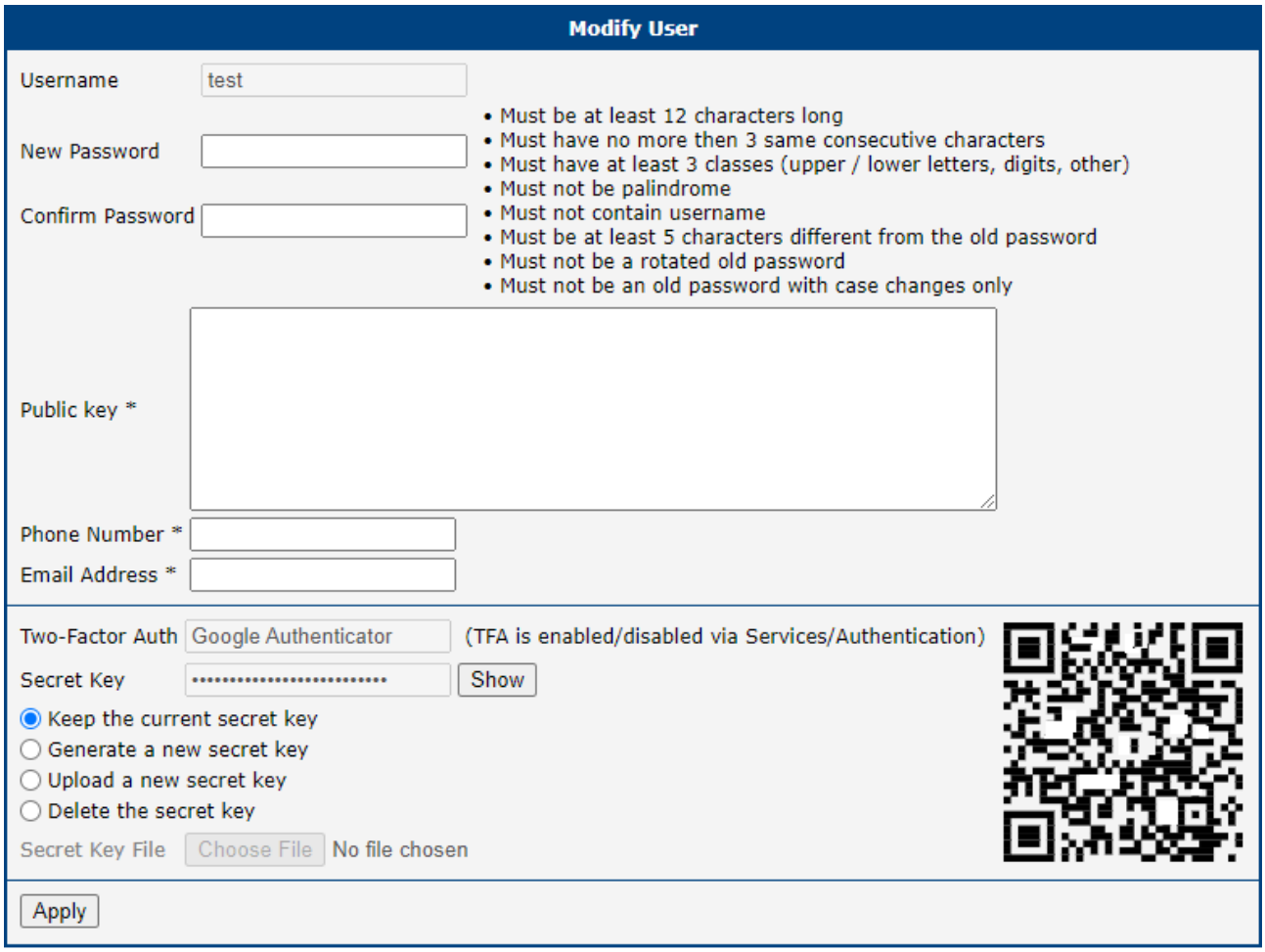


Figure 105: Users Administration Form

The meaning of the items in the first part of this window is clear or described in more detail in Chapter 5.1. If you want to change your own password, you will need to enter the current password as well.

Two-Factor Authentication

In the second part, you can configure two-factor authentication for a user, including its secret key. See Chapter **??** for information on how to enable the two-factor service and Chapter 5.2.1 for more information about two-factor authentication principles.

If the configuration of two-factor authentication fails or does not complete properly, you will be unable to log in to the router using that user account. It is recommended to set up a backup account to log in to the router in case issues arise during the configuration process. You can delete this backup account after successfully configuring two-factor authentication.

To successfully log in using two-factor authentication, the correct system time must be set on the router. Therefore, it is strongly recommended to enable the *Synchronize clock with NTP server* option. For more details, refer to chapter 3.19.4 NTP.

If you have enabled one of the two-factor authentication services, as mentioned above, you should see the chosen service name in the *Two-Factor Auth* field, as shown in Figure 105.

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

Without the secret key, a user will not be able to finish two-factor configuration and log in to the router.

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

5.2.1 Two-Factor Authentication

Implementation Notes

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

Configuration Steps

1. Enable the two-factor authentication service as described in Chapter **??**.
2. Enable the two-factor authentication for a user as described in Chapter 5.2.
3. Use an application or service to perform the two-factor authentication to the router as described in this chapter, section *Authenticator*.

Authenticator

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

You can use the Google Authenticator application; see Figure 106 for the download links.

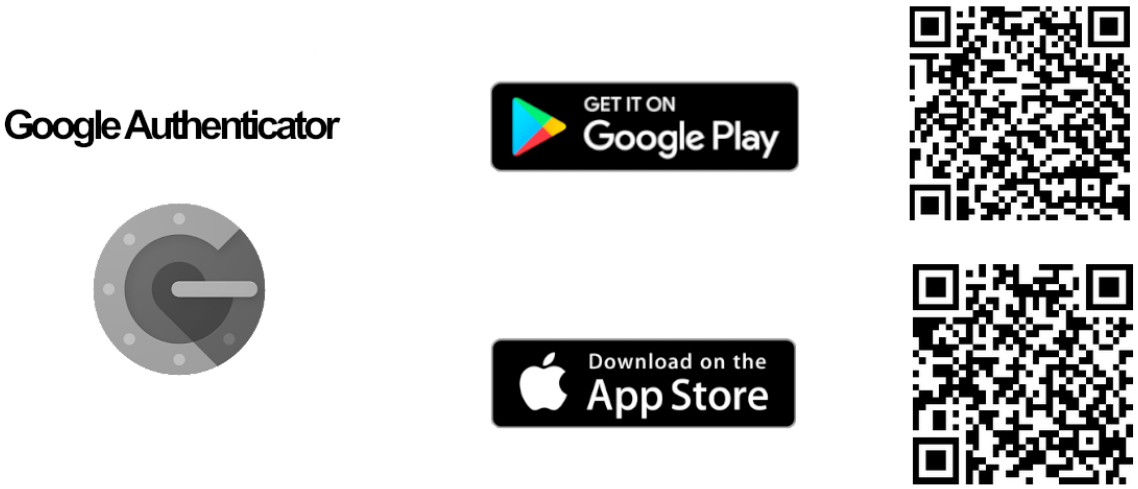


Figure 106: Links for Google Authenticator Application

Authenticator-Extension is available as an extension for all popular browsers; see Figure 107 for the download links.

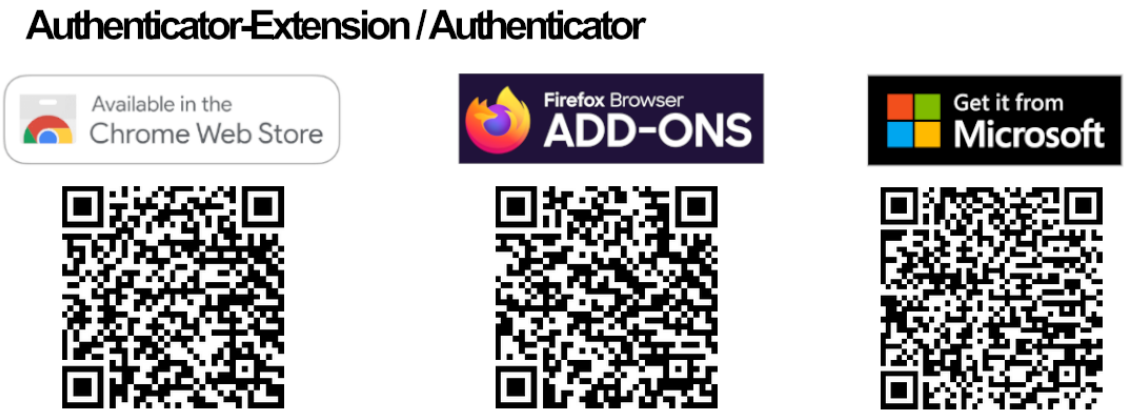


Figure 107: Links for Authenticator-Extension

In an Authenticator application, you enter a new entry and enter the secret key you have written down, or add it by scanning the QR code shown for a user on the *Modify User* configuration page.

Router Web Login

When logging to the router web, enter the *Username* and *Password*, just as you log in standardly; see Figure 108.

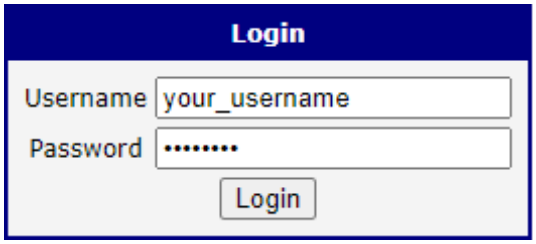


Figure 108: Standard Logging

Now you are prompted to enter the Verification Code; see Figure 109. This code you need to get from your Authenticator. Note that there is **a limited time** for code usage. This time should be within five minutes, assuming the system time is correct.

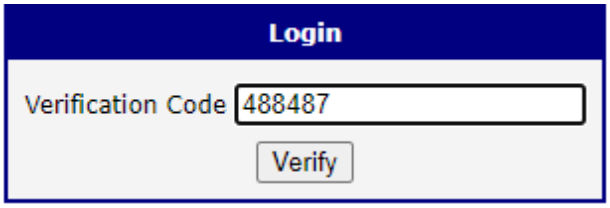


Figure 109: Verification Code

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

SSH and Telnet Logging

Logging by the SSH and Telnet with the two-factor authentication is similar. Enter your username, password, and generated verification code. For an example of SSH login, see Figure 110.

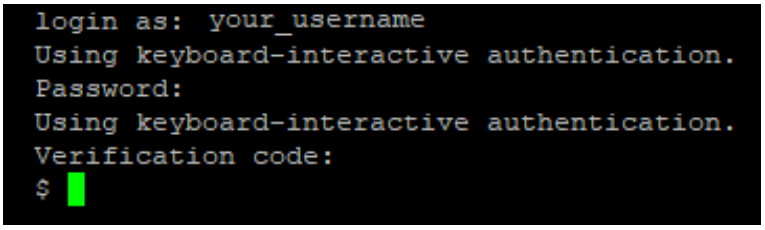


Figure 110: SSH Logging

5.2.2 Passwordless Console Login

You can log in to SSH without a password using the SSH Public Key. The process of key generation and the connection will be demonstrated in this chapter using *PuTTY*, a free terminal emulator for Windows OS. We use PuTTY version 0.80 in the example below:

- For simplicity and clarity, we will perform a manual installation of PuTTY to the directory `C:\bin`, not using an `.msi` installation package.
- From the PuTTY application *download page*, under the section *Alternative binary files*, download the individual files named `putty.exe`, `puttygen.exe`, and `pageant.exe`. You will likely want the 64-bit x86 version. Save these files to the `C:\bin` directory.
- Run the downloaded `puttygen.exe` program to create your SSH Key.
  - Ensure the *RSA* option is selected.
  - Click the *Generate* button. Move your mouse within the window to generate the keys.
  - Once complete, the key details appear, refer to Figure 111.
  - Click both *Save public key* and *Save private key* buttons to save these keys on your computer:
    - ☐ Name the public key something like *hostpublickey* and the private key something like *hostprivatekey*, without manually adding extensions.
    - ☐ If prompted about a passphrase, click *Yes* to save without a passphrase.
  - Leave this application still opened.
- Upload the public key to your router:
  - Ensure the user has the *Admin* role, since the *User* role is not permitted for SSH login.
  - In the router GUI (*Administration* → *Users*), click the *Change Password* button for the user with the *Admin* role.
  - Enter the generated public key to the user:
    - ☐ In the *PuTTY Key Generator*, select the whole public key as demonstrated in the figure above with the blue selection, and copy it to the clipboard.
    - ☐ In the router GUI, paste the key into the *Public key* field.
    - ☐ It is important the key **starts with "ssh-rsa "** followed by the key itself.
  - Re-entering the password is not necessary. Save the user settings by clicking the *Apply* button.
  - Now, you can close the *PuTTY Key Generator* application.
- Confiture the session in PuTTY:
  - Open `c:\bin\putty.exe` application.
  - In the configuration window, navigate to *Connection* → *Data* and enter the username (the router's user to whom the public key was saved) in the *Auto-login username* field.
  - Under *Connection* → *SSH* → *Auth* → *Credentials*, click the *Browse* button near the *Private key file for authentication* field, and select your *hostprivatekey* file.
  - In the *Session* category, configure the following:
    - ☐ *Host Name*: IP address of your router.
    - ☐ *Port*: 22.
    - ☐ *Connection Type*: SSH.

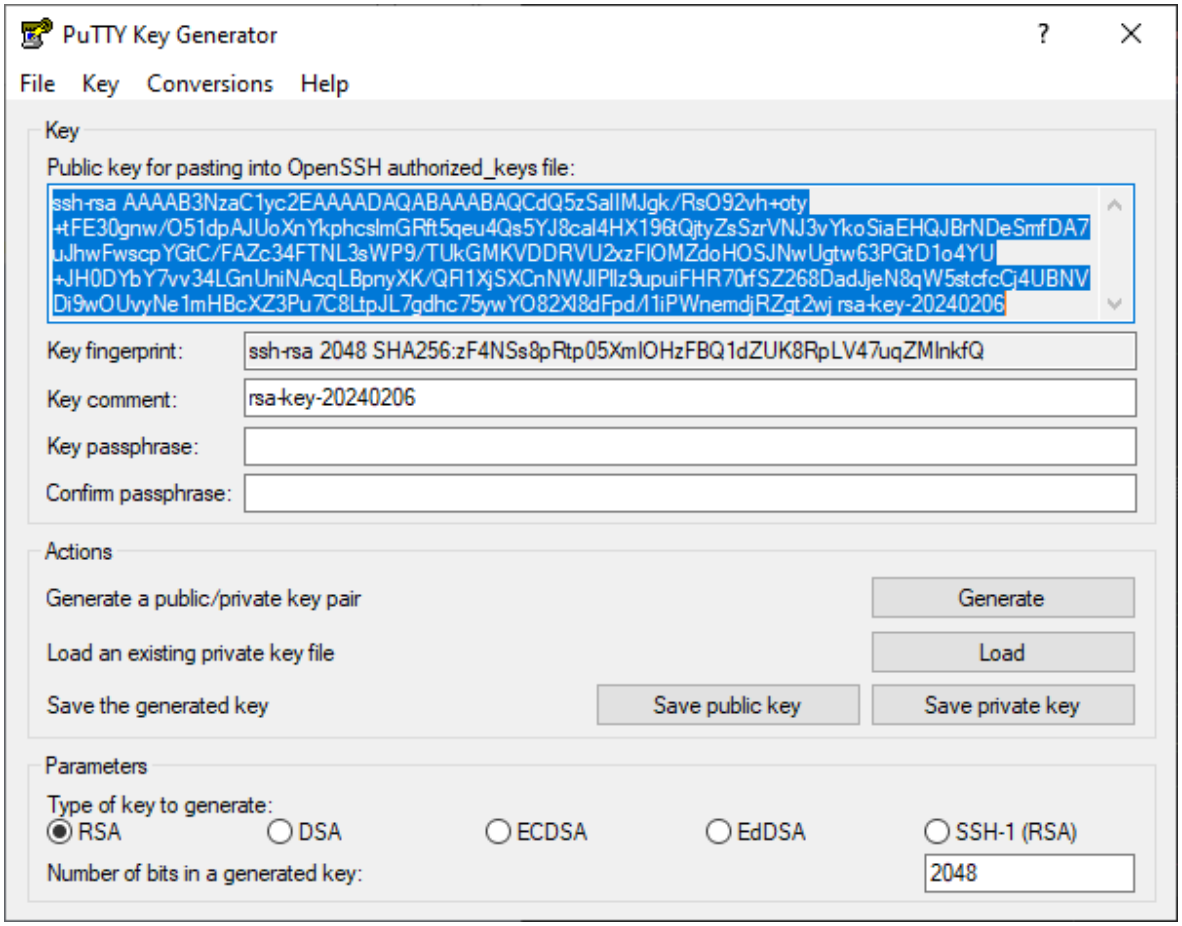


Figure 111: Key Generation

- ☐ *Saved Session*: Enter a name for this session.
- ☐ Click *Save* to store these settings.

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

5.2.3 Expired Password

If the password expires after the number of days defined in *Expire Password After* has passed, the user will be prompted to enter a new password as shown in Image 112. The new password must match the rules stated in the GUI, which depend on the *Force Password Complexity* level set in *Configuration* → *Services* → *Authentication*, as described in Chapter **??**.

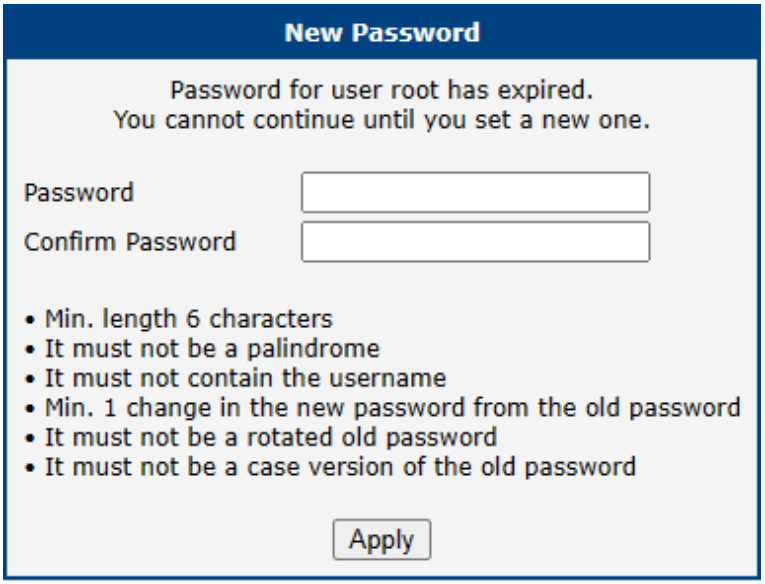


Figure 112: Expired Password Prompt

The user will be prompted to change their password when logging into the new router for the first time or if their password was changed by a user with an admin role.

5.3 Change Profile

In addition to the standard profile, up to three alternate router configurations or profiles can be stored in router's non-volatile memory. You can save the current configuration to a router profile through the *Change Profile* menu item. Select the alternate profile to store the settings to and ensure that the *Copy settings from current profile to selected profile* box is checked. The current settings will be stored in the alternate profile after the *Apply* button is pressed. Any changes will take effect after restarting router through the *Reboot* menu in the web administrator or using an SMS message.

Example of using profiles: Profiles can be used to switch between different modes of operation of the router such as PPP connection, VPN tunnels, etc. It is then possible to switch between these settings using the front panel binary input, an SMS message, or Web interface of the router.

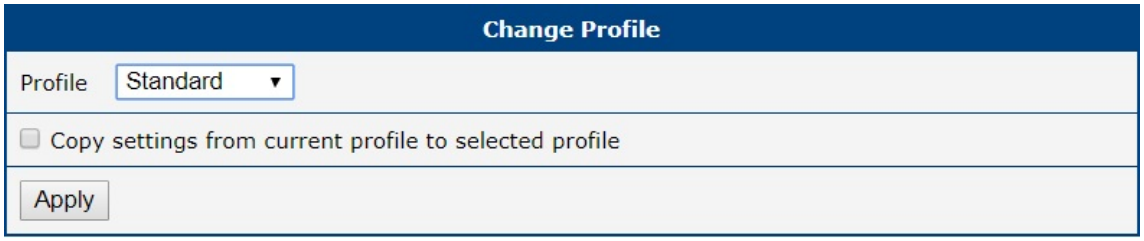


Figure 113: Change Profile

5.4 Set Date and Time

This administration page is not for configuring the NTP client, but only for one-time date and time settings. For permanent NTP client configuration, please go to the *Configuration* → *Services* → *NTP* page.

There are three ways to set the system date and time on a one-time basis, as shown in the figure below:

1. **Set current browser time:** This option sets the device's clock to match the time displayed on your web browser.
2. **Set specific date/time:** You can manually input the date and time. Ensure you adhere to the **yyyy-mm-dd** format for the date. For the time, use the **HH:MM:SS** format. **Note:** The time preloaded is the browser time, not the router time.
3. **Query NTP server:** To query the date and time from an NTP server, input the address of the NTP server. The system supports both IPv4 and IPv6 addresses, as well as domain names.

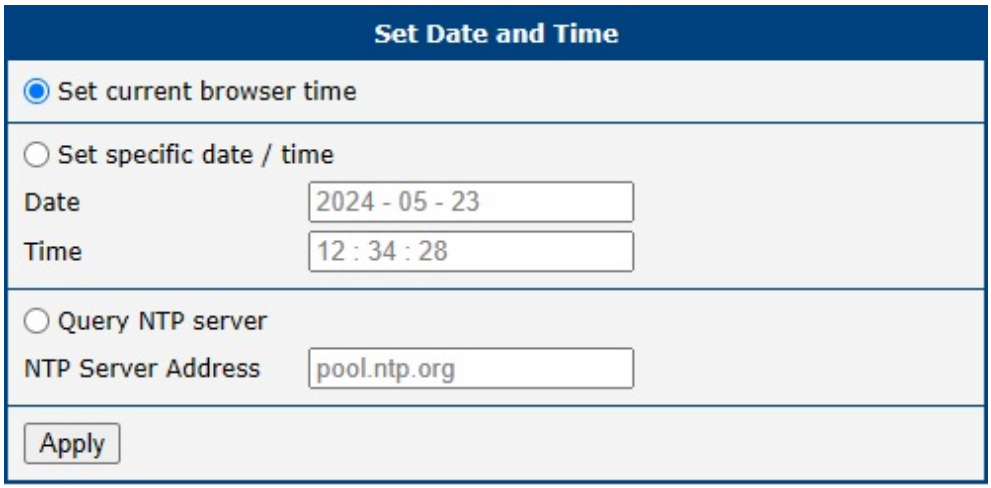


Figure 114: Set Real Time Clock

5.5 Set SMS Service Center Address

This feature works on the 1st cellular module only! (1st or 2nd SIM card.) It is not possible to set the SMS Service Center on the 2nd cellular module this way.

The function requires you to enter the phone number of the SMS service center to send SMS messages. To specify the SMS service center phone number use the *Set SMS Service Center* configuration form in the *Administration* section of the main menu. You can leave the field blank if your SIM card contains the phone number of the SMS service center by default. This phone number can have a value without an international prefix (xxx-xxx-xxx) or with an international prefix (+420-xxx-xxx-xxx). If you are unable to send or receive SMS messages, contact your carrier to find out if this parameter is required.

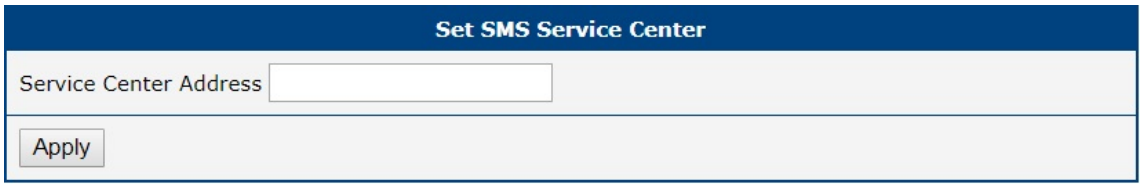


Figure 115: Set SMS Service Center Address

5.6 Unlock SIM Card

This feature works on the 1st cellular module only! (1st or 2nd SIM card.) It is not possible to unlock SIM card in 2nd cellular module this way.

It is possible to use the SIM card protected by PIN number in the router – just fill in the PIN on the *Mobile WAN Configuration* page. Here you can remove the PIN protection (4–8 digit Personal Identification Number) from the SIM card, if your SIM card is protected by one. Open the *Unlock SIM Card* form in the *Administration* section of the main menu and enter the PIN number in the *SIM PIN* field, then click the *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.

The SIM card is blocked after three failed attempts to enter the PIN code. Unblocking of SIM card by PUK number is described in next chapter.

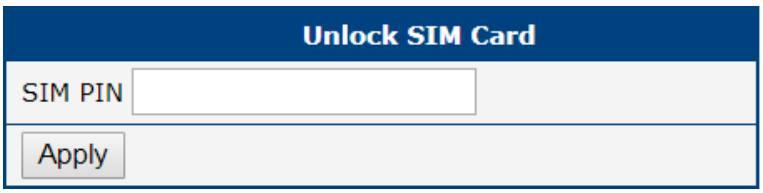


Figure 116: Unlock SIM Card

5.7 Unblock SIM Card

This feature works on the 1st cellular module only! (1st or 2nd SIM card.) It is not possible to unblock SIM card in 2nd cellular module this way.

On this page you can unblock the SIM card after 3 wrong PIN attempts or change the PIN code of the SIM card. To unblock the SIM card, go to *Unblock SIM Card* administration page. In both cases enter the PUK code into *SIM PUK* field and new SIM PIN code into *New SIM PIN* field. To proceed click on *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.

The SIM card will be permanently blocked after the three unsuccessful attempts of the PUK code entering.

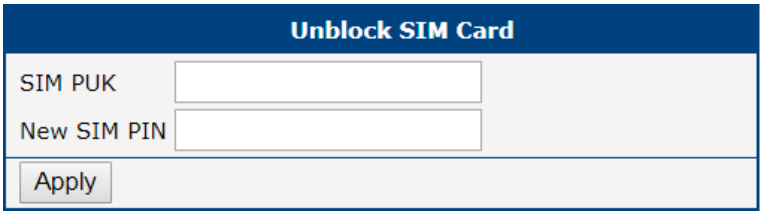


Figure 117: Unblock SIM Card

5.8 Send SMS

This feature works on the 1st cellular module only! (1st or 2nd SIM card.) It is not possible to send SMS from 2nd cellular module this way.

You can send an SMS message from the router to test the cellular network. Use the *Send SMS* dialog in the *Administration* section of the main menu to send SMS messages. Enter the *Phone number* and text of your message in the *Message* field, then click the *Send* button. The router limits the maximum length of an SMS to 160 characters. (To send longer messages, install the *pduSMS* router app).

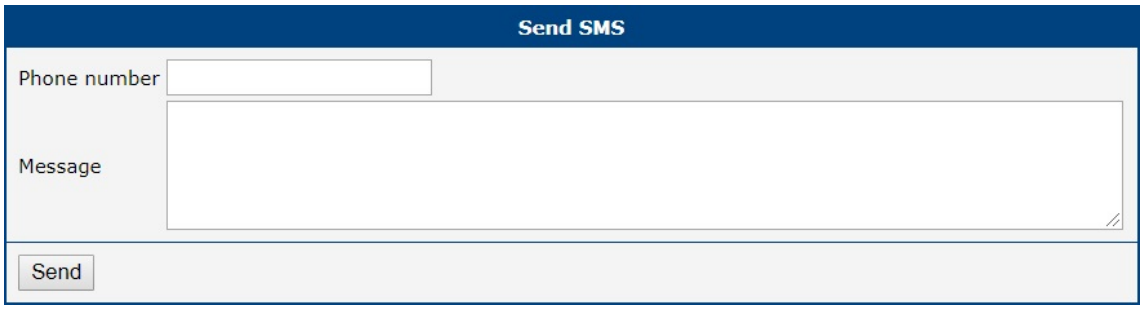


Figure 118: Send SMS

It is also possible to send an SMS message using CGI script. For details of this method. See the application note *Commands and Scripts* [1].

5.9 Backup Configuration

Keep in mind potential security issues when creating a backup, especially for user accounts. Encrypted configuration or a secured connection to the router should be used.

You can save the current configuration of the router using the *Backup Configuration* item in the *Administration* menu section. If you click on this item, a configuration pane will open, see Figure 119. Here you can choose what will be backed up. You can back up the configuration of the router (item *Configuration*) or the configuration of all user accounts (item *Users*). Both types of configurations can be backed up separately or together into one configuration file.

It is recommended to save the configuration into an encrypted file. If the encryption password is not configured, the configuration is stored in an unencrypted file.

Click on the *Apply* button and the configuration will be stored into a configuration file (file with *cfg* extension) in a directory according to the settings of the web browser. The stored configuration can be used later for restoration, see Chapter 5.10 for more information.

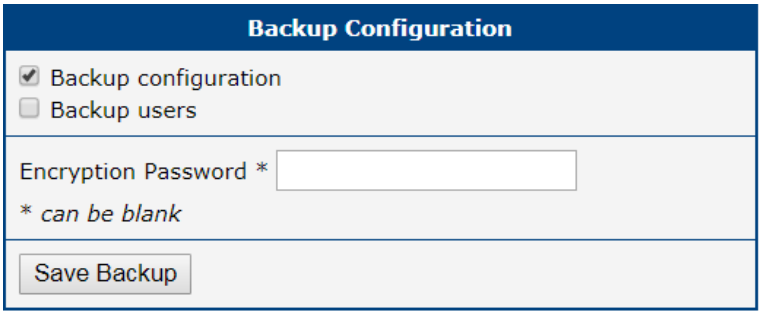


Figure 119: Backup Configuration

5.10 Restore Configuration

You can restore a router configuration stored in a file. You created the file as shown in the previous chapter.

To restore the configuration from this file, use the *Restore Configuration* form. Next, click the *Browse* button to navigate to the directory containing the configuration file you wish to load to the router. If the configuration was stored in an encrypted file, the decryption password must be set to decrypt the file successfully. To start the restoration process, click on the *Apply* button.

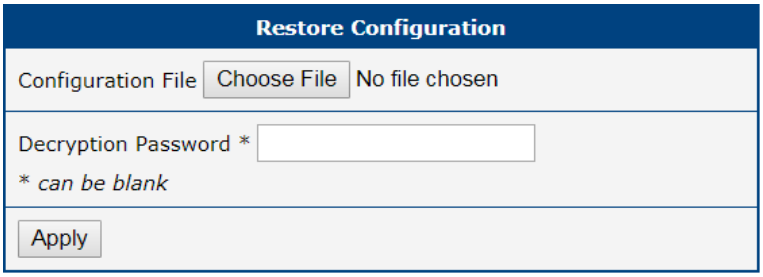


Figure 120: Restore Configuration

5.11 Update Firmware

For enhanced security, it is strongly recommended to regularly update your router's firmware to the latest version. Avoid downgrading the firmware to a version older than the production release, and refrain from uploading firmware meant for different models, as these actions can lead to device malfunction.

Be aware that firmware updates may cause compatibility issues with Router Apps. To minimize such issues, it is advisable to update all Router Apps to their latest versions concurrently with the router's firmware. Detailed compatibility information for each app is provided at the beginning of its Application Note.

The latest firmware for our routers is available on the Engineering Portal's product page. For downloading the appropriate firmware for your router model, please visit https://icr.advantech.com/support/router-models.

The *Update Firmware* administration page showcases the current firmware version and the name of the router's firmware, as illustrated in Figure 121. This page also offers the capability to update the router's firmware, accommodating both manual updates and online updates from the public server.

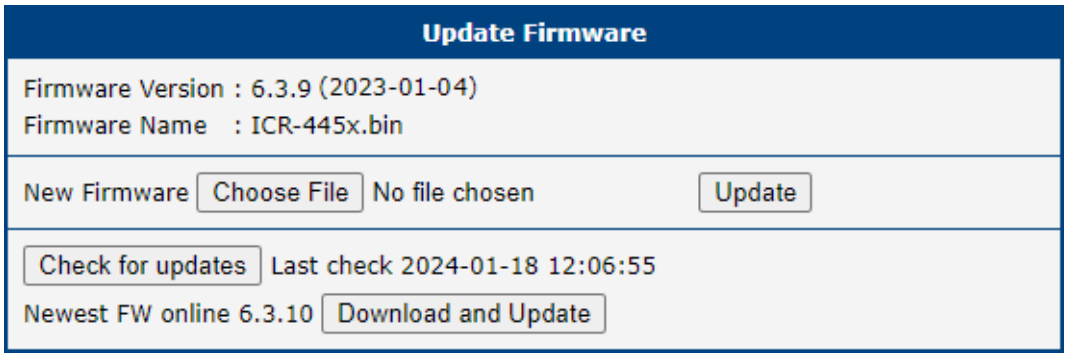


Figure 121: Update Firmware Administration Page

Manual Firmware Update

To manually update the router's firmware, click on the *Choose File* button and select the firmware file. Then, press the *Update* button to initiate the firmware update process.

Online Firmware Update

Starting with firmware version 6.4.0, the firmware can be updated from a public server. Ensure that your router is properly configured as described in Chapter 4.2.

To verify the availability of a newer firmware version on the server, click the *Check for updates* button. If a new version is available, the version information and a *Download and Update* button will appear. Clicking this button initiates the firmware update process.

During the firmware update, the router will display status messages as depicted in Figure 122. Upon completion, the router will automatically reboot. After rebooting, click the *here* link in the web interface to reopen it.

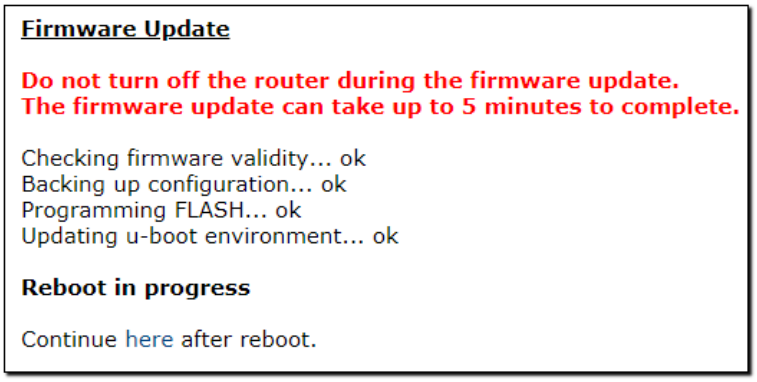


Figure 122: Process of Firmware Update

5.12 Reboot

To reboot the router select the *Reboot* menu item and then press the *Reboot* button.

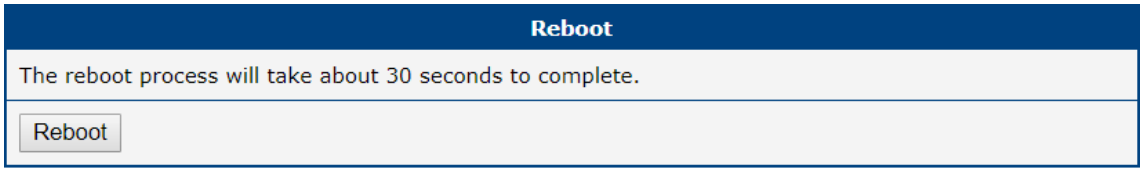


Figure 123: Reboot

5.13 Logout

By clicking the *Logout* menu item, the user is logged out from the web interface.

6. Typical Situations

Although Advantech routers have wide variety of uses, they are commonly used in the following ways. All the examples below are for IPv4 networks.

6.1 Access to the Internet from LAN

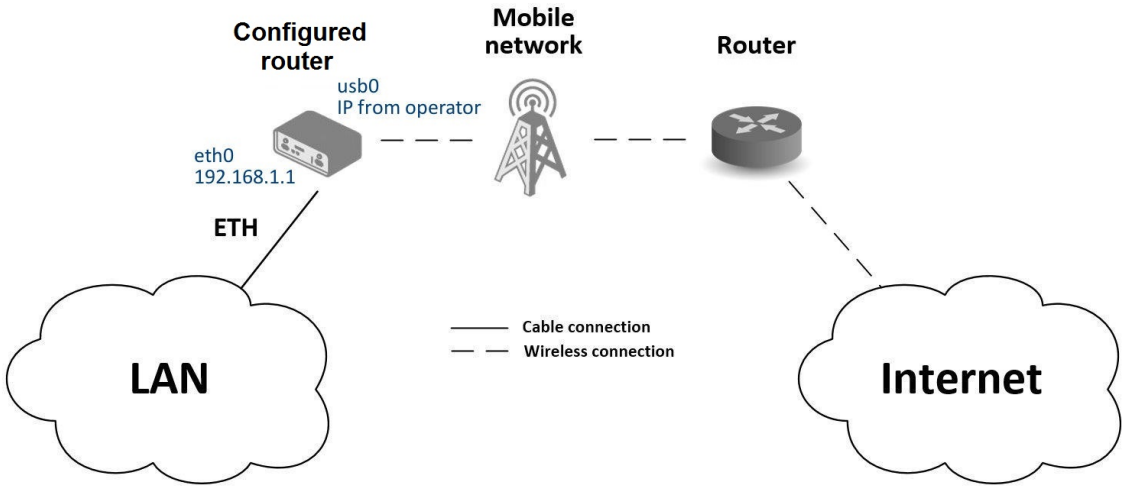


Figure 124: Access to the Internet from LAN – sample topology

In this example, a LAN connecting to the Internet via a mobile network, the SIM card with a data tariff has to be provided by the mobile network operator. This requires no initial configuration. You only need to place the SIM card in the *SIM1* slot (Primary SIM card), attach the antenna to the *ANT* connector and connect the computer (or switch and computers) to the router's eth0 interface (LAN). Wait a moment after turning on the router. The router will connect to the mobile network and the Internet. This will be indicated by the LEDs on the front panel of the router (*WAN* and *DAT*).

Additional configuration can be done in the *LAN* and *Mobile WAN* items in the *Configuration* section of the web interface.

LAN configuration The factory default IP address of the router's eth0 interface is in the form of 192.168.1.1. This can be changed (after login to the router) in the *LAN* item in the *Configuration* section. (See Figure 125.) In this case there is no need of any additional configuration. The DHCP server is also enabled by factory default (so the first connected computer will get the 192.168.1.2 IP address etc.). Other configuration options are described in the Chapter 3.1.

Mobile WAN Configuration Use the *Mobile WAN* item in the *Configuration* section to configure the connection to the mobile network, see Figure 126. In this case (depending on the SIM card) the configuration form can be blank. But make sure that *Create connection to mobile network* is checked (this is the factory default). For more details, see Chapter 3.4.1.

To check whether the connection is working properly, go to the *Mobile WAN* item in the *Status* section. You will see information about operator, signal strength etc. At the bottom, you should see the message: *Connection successfully established*. In problems check also the *Module Switching* page, there has to be *Create connection to mobile network* enabled, too.

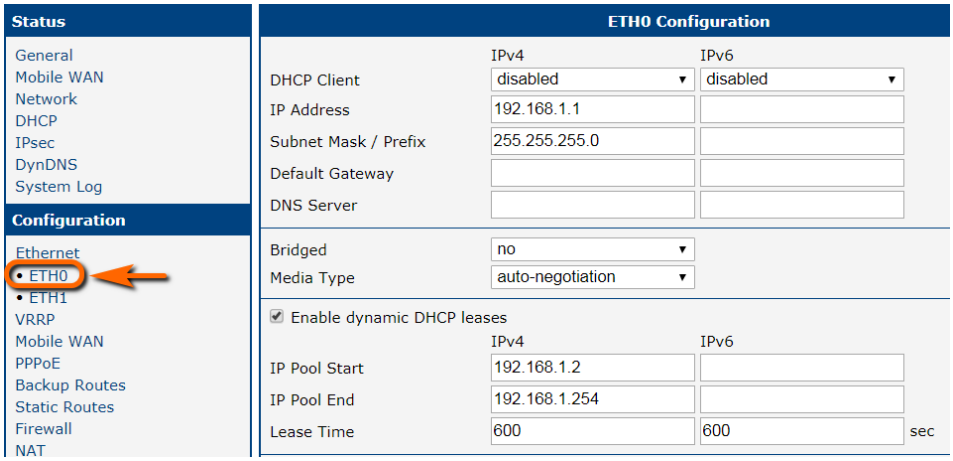


Figure 125: Access to the Internet from LAN – *Ethernet* configuration

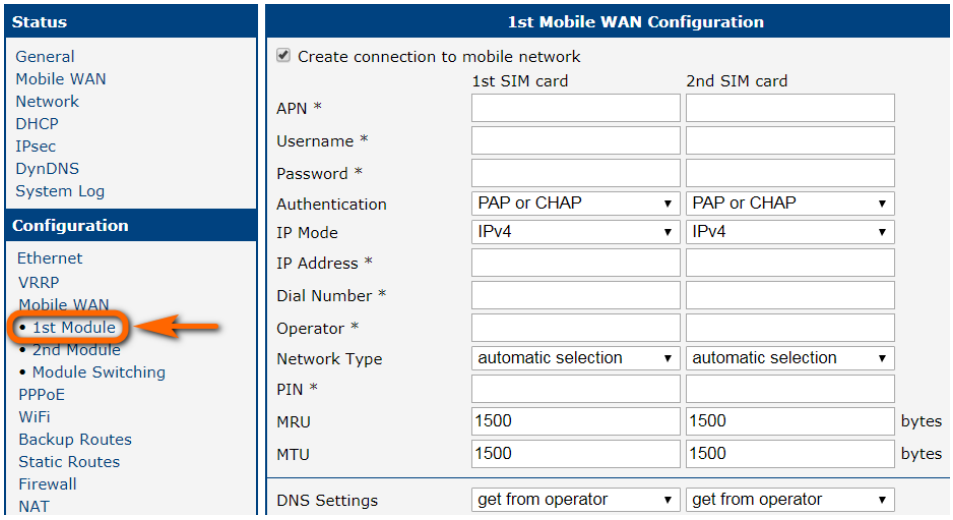


Figure 126: Access to the Internet from LAN – *Mobile WAN* configuration

The *Network* item should display information about the newly created network interface, usb0 (mobile connection). You should also see the IP address provided by the network operator, as well as the route table etc. The LAN now has Internet access.

6.2 Backup Access to the Internet from LAN

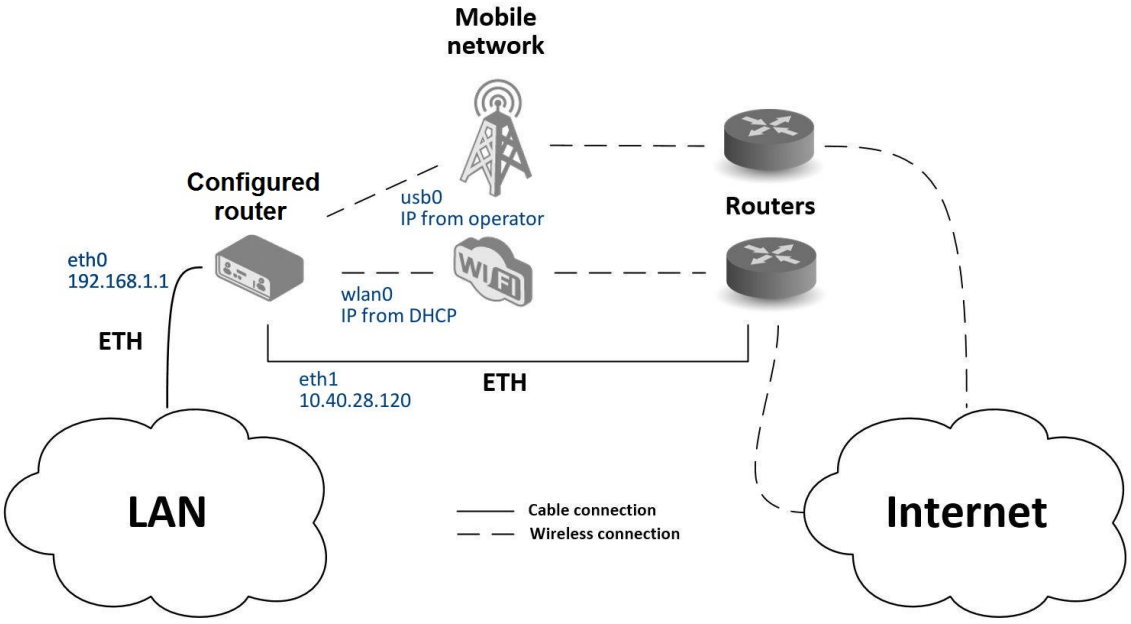


Figure 127: Backup access to the Internet – sample topology

The configuration form on the *Backup Routes* page lets you back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can be assigned a priority.

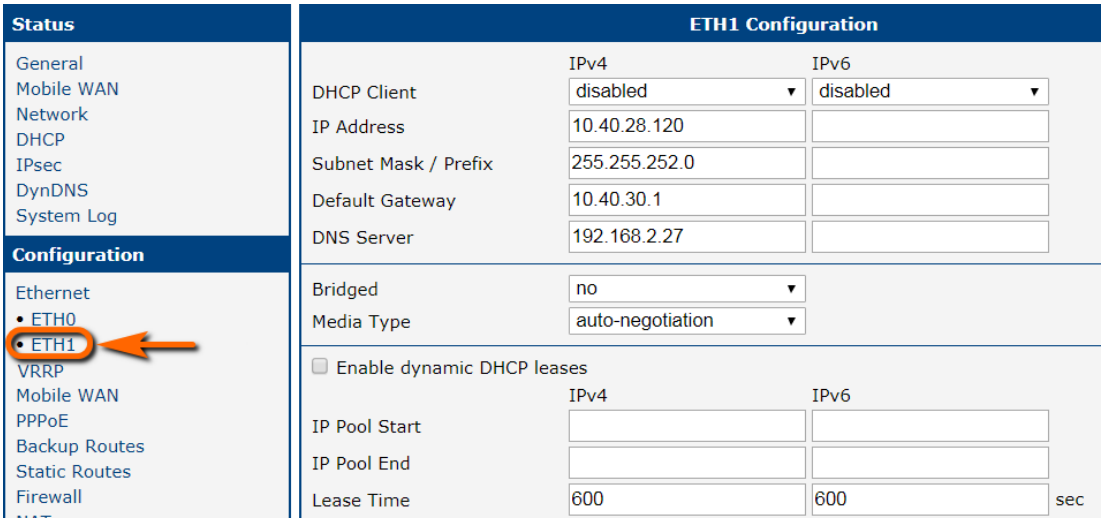


Figure 128: Backup access to the Internet – Ethernet configuration

Ethernet configuration: In the *Ethernet –> ETH0* item, you can use the factory default configuration as in the previous situation. The *ETH1* interface on the front panel of the router is used for connection to the Internet. It can be configured in *ETH1* menu item. Connect the cable to the router and set the appropriate values as in Figure 128. You may configure the static IP address, default gateway and DNS server. Changes will take effect after you click on the *Apply* button. Detailed Ethernet configuration is described in Chapter 3.1.

WLAN configuration: To use the WLAN you will need to configure the WiFi station in the *WiFi - > Station* item, as shown in Figure 129. Check the *Enable WiFi STA*, enable the DHCP client and fill in the adresses of the default gateway and DNS server. Next, fill in the data for the connection (SSID, authentication, encryption, WPA PSK Type and password). For details see Chapter 3.8. Click the *Apply* button to confirm the changes.

To verify that the WiFi connection is successful, check the *WiFi* item in the *Status* section. If the connection is successful you should see the following message: *wpa_state=COMPLETED*.

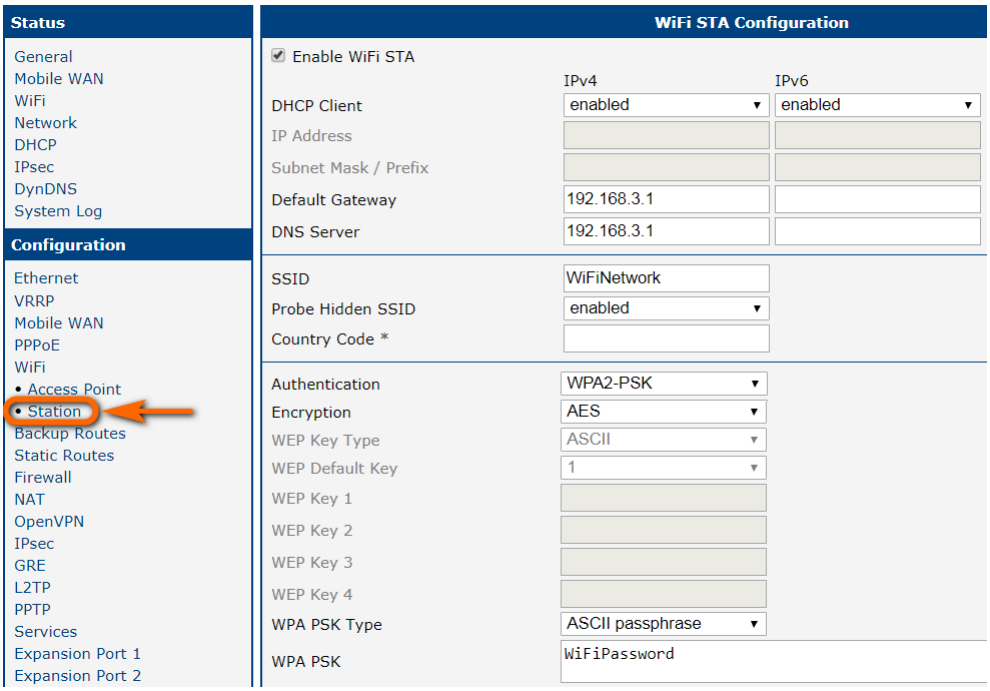


Figure 129: Backup access to the Internet – WiFi configuration

Mobile WAN configuration: To configure the mobile connection it should be sufficient to insert the SIM card into the *SIM1* slot and attach the antenna to the *ANT* connector. (Depending on the SIM card you are using).

To set up backup routes you will need to enable Check Connection in the *Mobile WAN* item. (See Figure 130.) Set the *Check connection* option to *enabled + bind* and fill in an IP address of the mobile operator's DNS server or any other reliably available server and enter the time interval of the check. For detailed configuration, see Chapter 3.4.1.

Backup Routes configuration: After setting up the backup routes you will need to set their priorities. In Figure 131, the ETH1 wired connection has the highest priority. If that connection fails, the second choice will be the WiFi wlan0 network interface. The third choice will be the mobile connection – usb0 network interface.

The backup routes system must be activated by checking the *Enable backup routes switching* item for each of the routes. Click the *Apply* button to confirm the changes. For detailed configuration see Chapter 3.9.

You can verify the configured network interfaces in the *Status* section in the *Network* item. You will see the active network interfaces: eth0 (connection to LAN), eth1 (wired connection to the Internet), wlan0 (WiFi connection to the Internet) and usb0 (mobile connection to the Internet). IP addresses and other data are included.

At the bottom of the page you will see the *Route Table* and corresponding changes if a wired connection fails or a cable is disconnected (the default route changes to wlan0). Similarly, if a WiFi connection is not available, the mobile connection will be used.

Backup routes work even if they are not activated in the *Backup Routes* item, but the router will use the factory defaults.

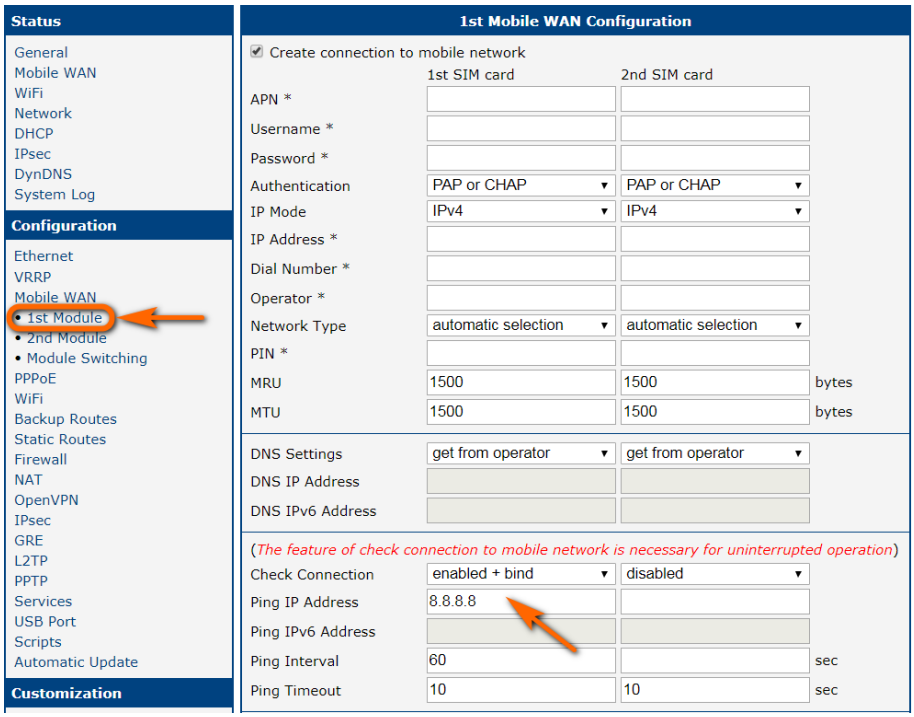


Figure 130: Backup access to the Internet – Mobile WAN configuration

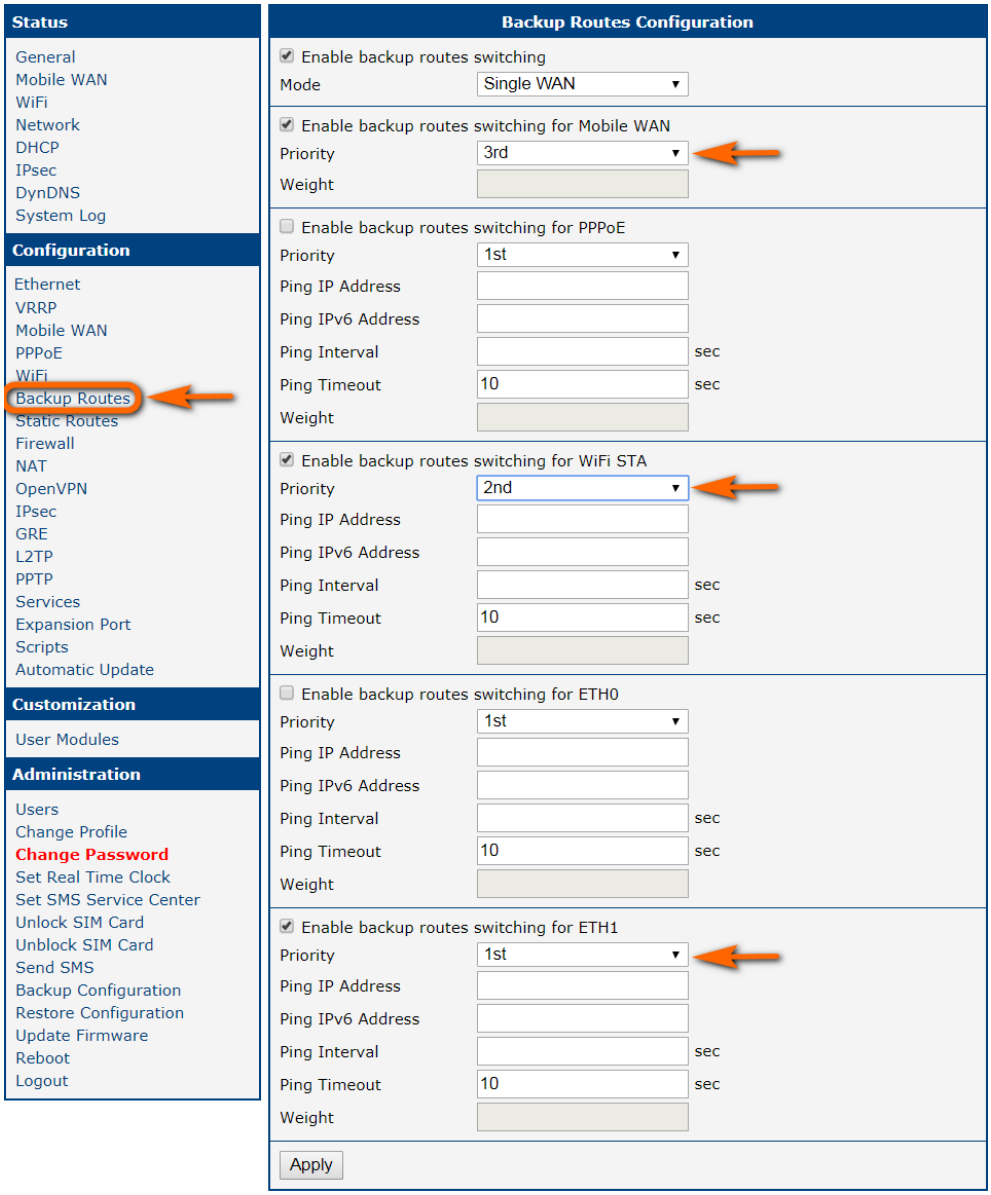


Figure 131: Backup access to the Internet – Backup Routes configuration

6.3 Secure Networks Interconnection or Using VPN

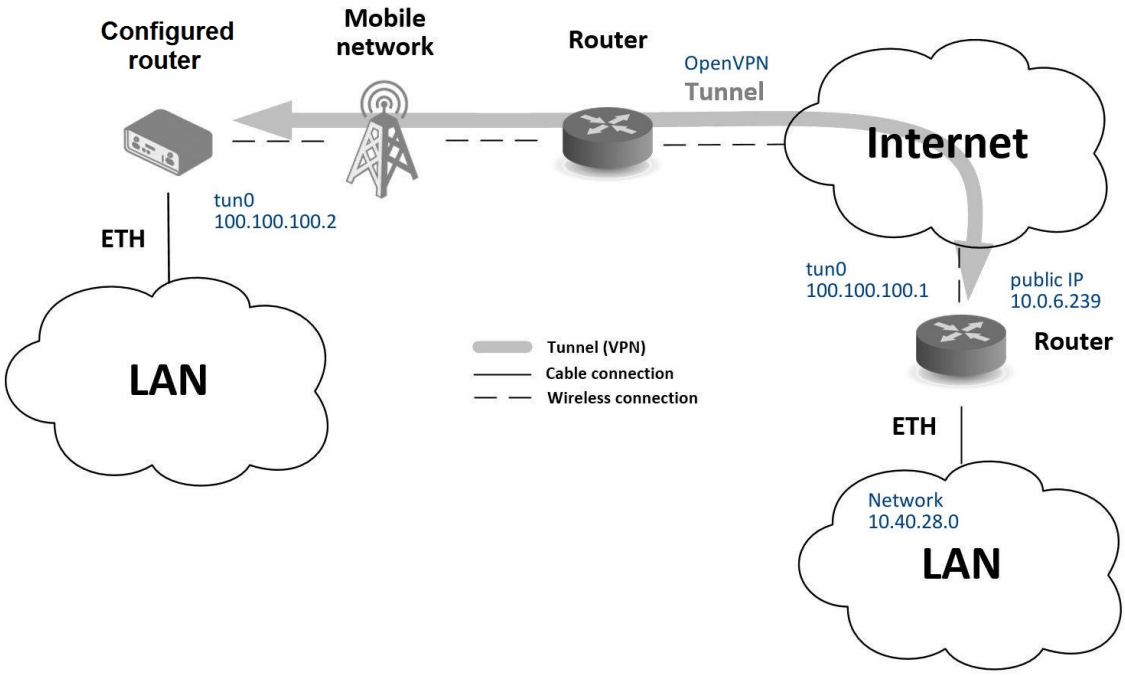


Figure 132: Secure networks interconnection – sample topology

VPN (Virtual Private Network) is a protocol used to create a secure connection between two LANs, allowing them to function as a single network. The connection is secured (encrypted) and authenticated (verified). It is used over public, untrusted networks, see fig. 132. You may use several different secure protocols.

- *OpenVPN* (it is a configuration item in the web interface of the router), see Chapter 3.13 or Application Note [5],
- *IPsec* (it is also configuration item in the web interface of the router), see Chapter 3.14 or Application Note [6].

You can also create non-encrypted tunnels: *GRE*, *PPTP* and *L2TP*. You can use GRE or L2TP tunnel in combination with IPsec to create VPNs.

There is an example of an OpenVPN tunnel in Figure 132. To establish this tunnel you will need the opposite router's IP address, the opposite router's network IP address (not necessary) and the pre-shared secret (key). Create the OpenVPN tunnel by configuring the *Mobile WAN* and *OpenVPN* items in the *Configuration* section.

Mobile WAN configuration: The mobile connection can be configured as described in the previous situations. (The router connects itself after a SIM card is inserted into *SIM1* slot and an antenna is attached to the *ANT* connector.)

Configuration is accessible via the *Mobile WAN* item the *Configuration* section, see Chapter 3.4.1). The mobile connection has to be enabled.

OpenVPN configuration: OpenVPN configuration is done with the *OpenVPN* item in the *Configuration* section. Choose one of the two possible tunnels and enable it by checking the *Create 1st OpenVPN tunnel*. You will need to fill in the protocol and the port (according to the settings on the opposite side of the tunnel or Open VPN server). You may fill in the public IP address of the opposite side of the tunnel including the remote subnet and mask (not necessary). The important items are *Local* and *Remote Interface IP Address* where the information regarding the interfaces of the tunnel's end must be filled in. In the example shown, the *pre-shared secret* is known, so you would choose this option in the *Authentication Mode* item and insert the secret (key) into the field. Confirm the configuration clicking the *Apply* button. For detailed configuration see Chapter 3.13 or Application Note [5].

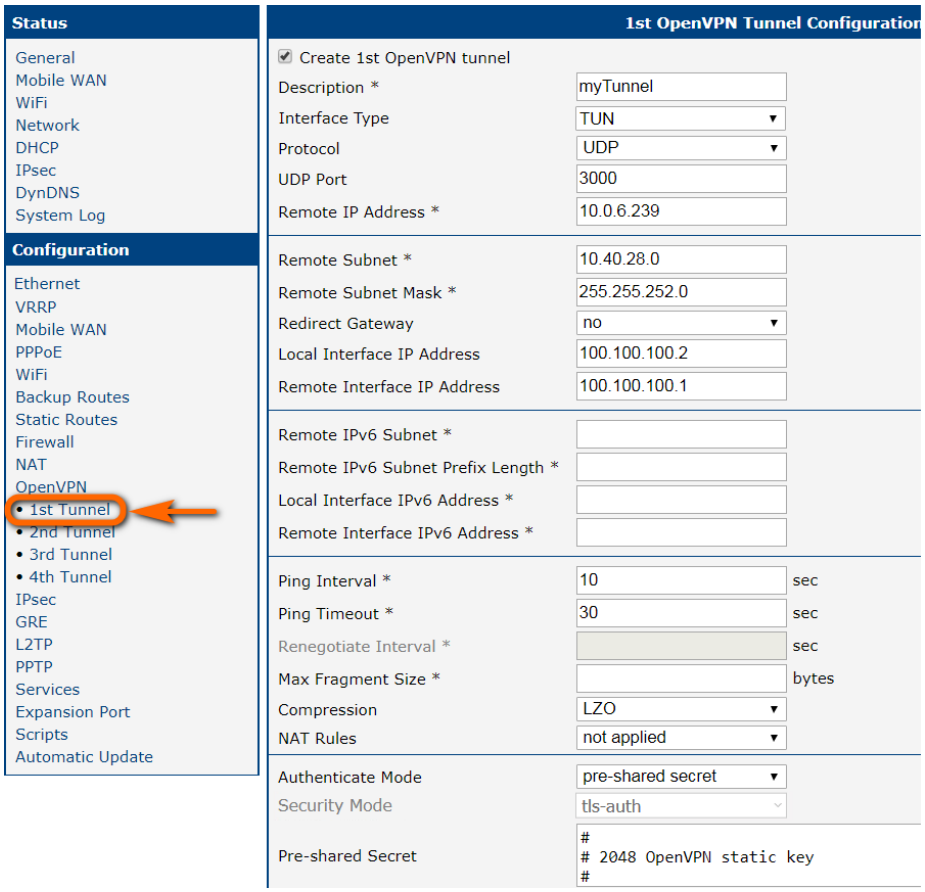


Figure 133: Secure networks interconnection – OpenVPN configuration

The *Network* item in the *Status* section will let you verify the activated network interface tun0 for the tunnel with the IP addresses of the tunnel's ends set. Successful connection can be verified in the *System Log* where you should see the message: `Initialization Sequence Completed`. The networks are now interconnected. This can also be verified by using the `ping` program. (Ping between tunnel's endpoint IP addresses from one of the routers. The console is accessible via SSH).

Appendix A: Open Source Software License

The software in this device uses various pieces of open-source software governed by the following licenses:

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

The list of components and complete license texts can be found on the device itself. See the *Licenses* link at the bottom of the router's main Web page (*General Status*) or point your browser to this address (replace the DEVICE_IP string with the actual router's IP address):

`https://DEVICE_IP/licenses.cgi`

This is a written offer valid for three years since the device purchase, offering any third party for a charge no more than the cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code on a flash drive medium. If you are interested in obtaining the source, please get in touch with us at:

iiotcustomerservice@advantech.eu

Modifications and debugging of LGPL-linked executables:

The device manufacturer, with this, grants the right to use debugging techniques (e.g., decompilation) and make customer modifications of any executable linked with an LGPL library for its purposes. Note these rights are limited to the customer's usage. No further distribution of such modified executables and no transmission of the information obtained during these actions may be done.

Source codes under the GPL license are available at the following address:

`https://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 latest revision 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.

IPv6 is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013. As of late November 2012, IPv6 traffic share was reported to be approaching 1%.

IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons (2001:0db8:85a3:0042:1000:8a2e:0370:7334), but methods of abbreviation of this full notation exist.

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 telecommuni-

cations 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] Commands and Scripts
[2] Remote Monitoring
[3] WebAccess/DMP
[4] R-SeeNet
[5] OpenVPN Tunnel
[6] IPsec Tunnel
[7] GRE Tunnel
[8] WireGuard Tunnel
[9] FlexVPN
[10] VLAN
[11] SNMP Object Identifiers
[12] AT Commands (AT-SMS)
[13] Quality of Service (QoS)
[14] Programming of Router Apps
[15] Security Guidelines

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