RACOM

User manual

WaSP
Embedded Radio Modem

Quick start

Hardware

Configuration

Parameters

fw 2.3.6.0
2026-08-21
version 1.1

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Important Notice

Copyright

Products offered may contain software proprietary to RACOM. The offer of supply of these products and services does not include or infer any transfer of ownership.

Disclaimer

Although every precaution has been taken in preparing this information, RACOM assumes no liability for errors and omissions, or any damages resulting from the use of this information. This document or the equipment may be modified without notice, in the interests of improving the product.

RACOM reserves the right to make changes in the technical specification or in this product function or to terminate production of this product or to terminate its service support without previous written notification of customers.

Trademark

All trademarks and product names are the property of their respective owners.

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e. have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the WaSP are used in an appropriate manner within a well-constructed network. WaSP should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. RACOM accepts no liability for damages of any kind resulting from delays or errors in data transmitted or received using WaSP, or for the failure of WaSP to transmit or receive such data.
- Under no circumstances is RACOM or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. RACOM does not provide the user with any form of guarantee containing assurance of the suitability and applicability for its application.
- RACOM products are not developed, designed or tested for use in applications which may directly affect health and/or life functions of humans or animals, nor to be a component of similarly important systems, and RACOM does not provide any guarantee when company products are used in such applications.

1. Product

WaSP is a compact, high-performance radio modem, tailored for wireless surveillance applications. Designed for fast, secure and reliable data transfer in mission-critical operations, its lightweight, embedded form makes it ideal for UGVs (Unmanned Ground Vehicles) and UAVs (Unmanned Aerial Vehicles), where every gram and watt matters.

1.1. Dimensions

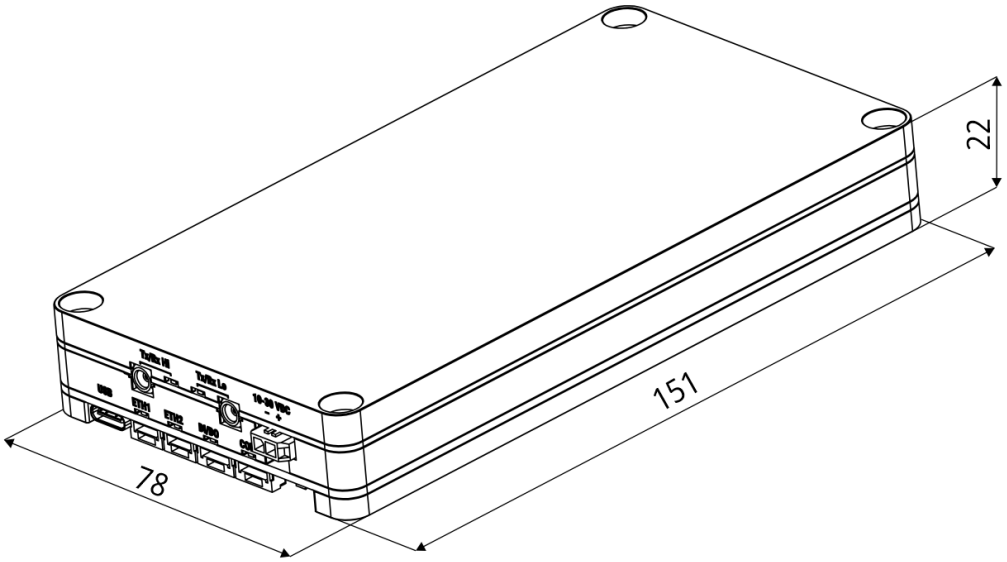


Fig. 1.1: WaSP dimensions - without cooler

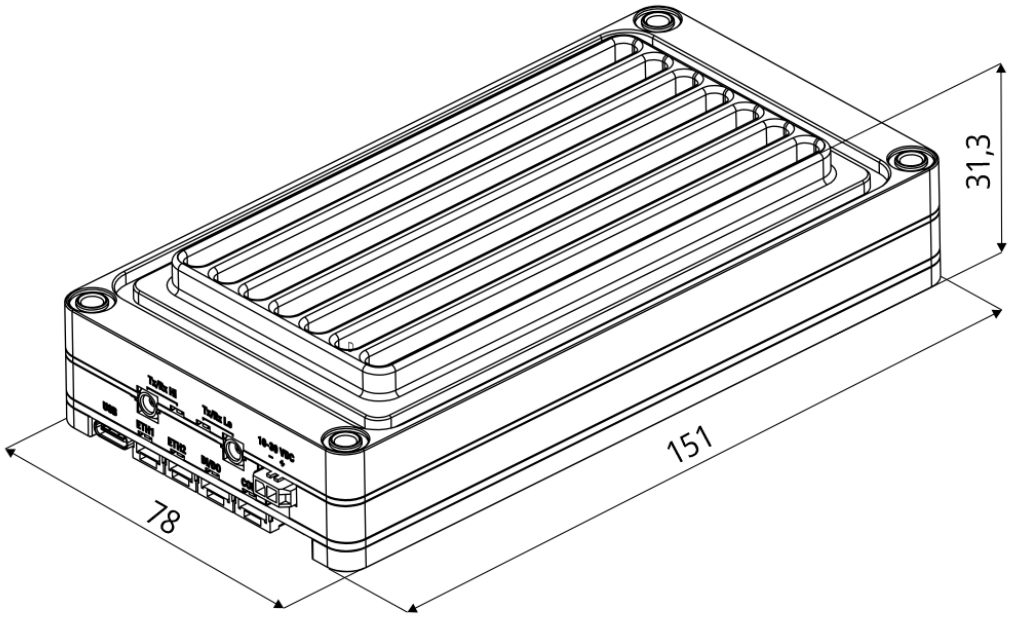


Fig. 1.2: WaSP dimensions - with cooler

Note

The 31.3 mm dimension can be changed according to the height of the passive cooler used.

1.2. Connectors

All connectors and LEDs are located on the front panel.

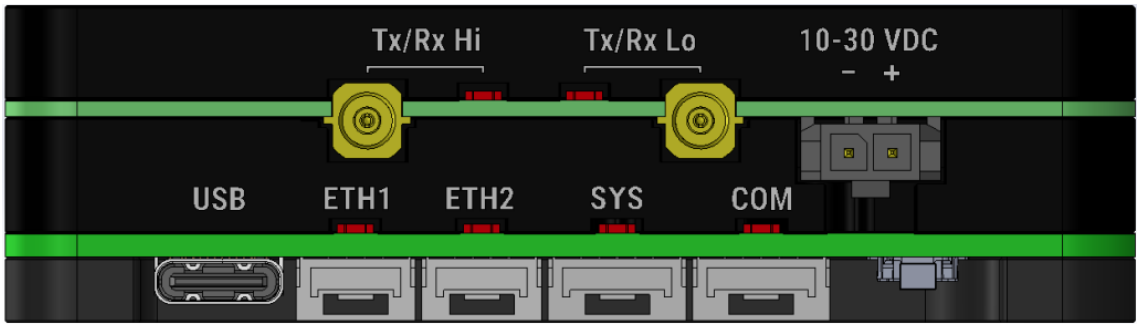


Fig. 1.3: All connectors

1.2.1. Antenna

An antenna can be connected to WaSP via MCX female 50Ω connector.

WaSP is equipped with two connectors. Both connectors are used for Tx/Rx according to SW setting of the radio. The left connector is used for higher frequencies band antenna connection, the right for lower frequencies band antenna.

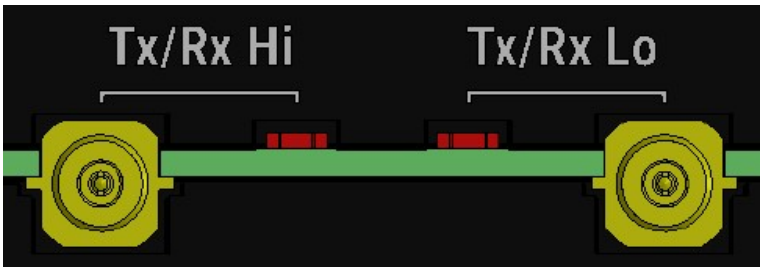


Fig. 1.4: Antenna connectors

Warning

WaSP radio modem may be damaged when operated without an antenna or a dummy load.

1.2.2. Power

This rugged connector connects to a power supply.

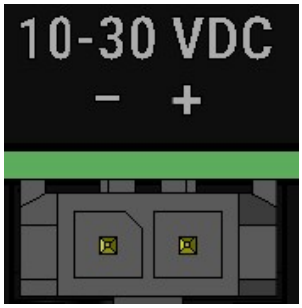


Fig. 1.5: Power supply connector

POWER

The POWER pins labelled + and - serve to connect a power supply 10–30 VDC. The requirements for a power supply are defined in *Section 2.3, "Power supply"* and *Chapter 6, Technical parameters*.

Fig. 1.6: MOLEX Micro-Fit 3.0 socket

Tab. 1.1: Pin assignment

Pin labeled	Signal
+	+ POWER (10 to 30 V)
−	− POWER (GND)

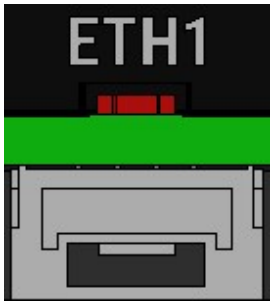
1.2.3. ETH1 - ETH2

JST-GH connectors for Ethernet connection. WaSP has 10/100Base-T Auto MDI/MDIX interfaces so it can connect to 10 Mb/s or 100 Mb/s Ethernet network. The speed can be selected manually or recognized automatically by WaSP. WaSP is provided with Auto MDI/MDIX function which allows it to connect over both standard and cross cables, adapting itself automatically.

Pin assignment

Tab. 1.2: Ethernet to cable connector connections

Pin	Signal	Direct cable	Crossed cable
1	Rx−	green	orange
2	RX+	green – white	orange – white
3	TX−	orange	green
4	TX+	orange – white	green – white



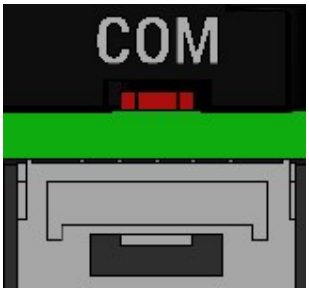
1.2.4. COM

WaSP provides serial interface terminated by JST-GH connector.

RS232 of WaSP is a hard-wired DCE (Data Communication Equipment) device. Equipment connected to the serial port of WaSP unit should be DTE (Data Terminal Equipment) and a straight-through cable should be used. If a DCE device is connected to the serial port of WaSP, a null modem adapter or cross cable has to be used.

Tab. 1.3: COM pin description

DSUB9F	COM – RS232	
Pin	Signal	In/ Out
1	CTS	Out
2	RTS	In
3	RxD	Out
4	TxD	In
5	GND	



1.2.5. USB

WaSP uses USB 2.0. USB interface is wired as standard USB-C:

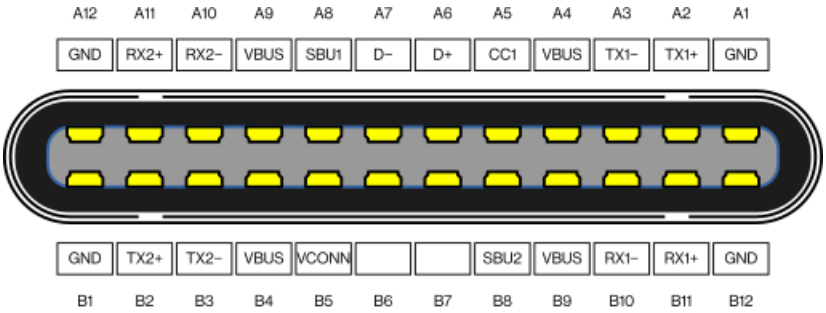


Fig. 1.7: USB-C Pins

The USB interface is designed for the connection to an external ETH/USB adapter or a Wi-Fi adapter. They are optional accessories to WaSP. The adapters are used for service access to web configuration interface of WaSP unit.

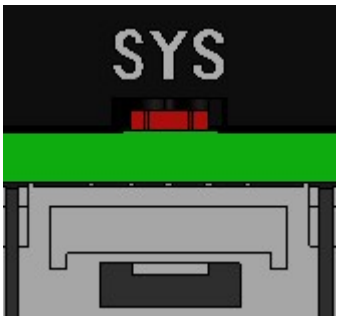
The USB connector also provides power supply (5 V / 0.5 A). It can be used to temporarily power a connected device, for instance a telephone. The USB connector should not be used as permanent source of power supply.

1.2.6. Digital Inputs and Outputs

The digital input and output interface connector is located below the SYS status LED.

Tab. 1.4: Digital Inputs and Outputs

Pin	Description	Signal
1	SI	Sleep Input
2	AI	Alarm Input
3	GND	Ground
4	AO	Alarm Output
5	GND	Ground



Digital Outputs:

- Open drain output max. 30 VDC, 0.2 A

Digital inputs:

- Schmitt-triggered inverted input
- Pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)
- Max. 30 VDC

1.2.7. HW button

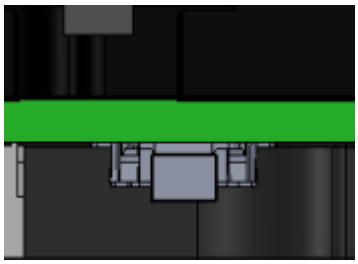


Fig. 1.8: HW button

HW button is placed on the right side of COM interface.

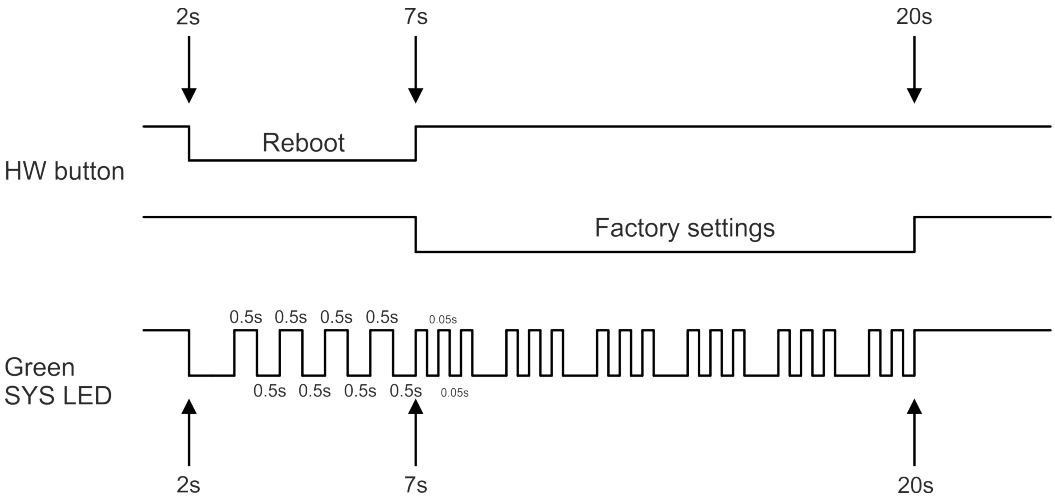


Fig. 1.9: HW button scheme

HW button operation

- Press less than 2 seconds - Nothing happens
- Press from 2 up to 7 seconds - Reboot is performed on button release
- Press from 7 up to 20 seconds - Factory settings are performed on button release
- Press more than 20 seconds - Nothing happens

1.3. Indication LEDs

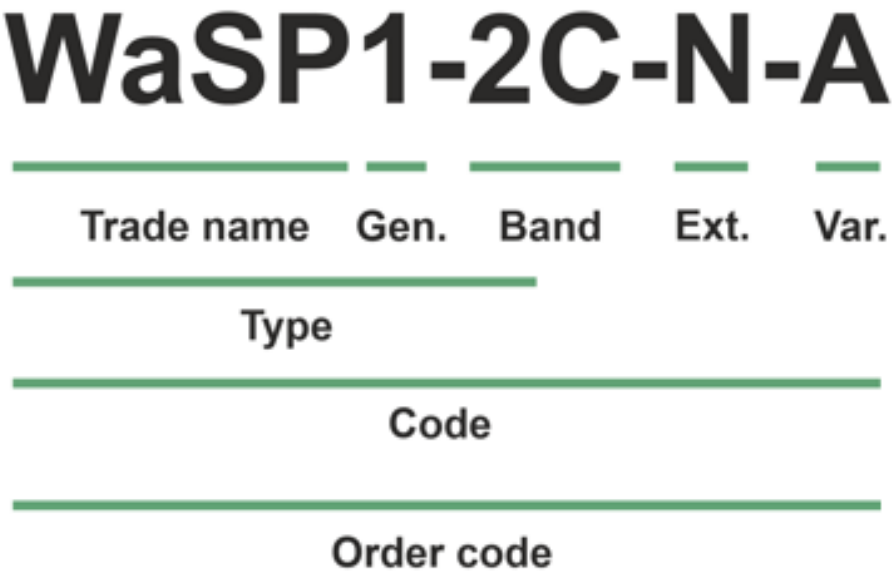
Tab. 1.5: Key to LEDs

LED	Colour	Status	Function
SYS	Green	Permanently lit	System OK
		Flashing - period 500 ms	HW button pushed
		Three fast (50 ms) flashes - pause (500 ms)	HW button factory reset
		Flashing regularly - period 2000 ms	Sleep mode activated
	Red	Permanently lit	Alarm
		Flashing regularly - period 500 ms	Serious system error
	Orange	Permanently lit	Unit booting
		Three fast (75 ms) flashes	USB flash disc inserted
		Flashing fast (75 ms) - period 1000 ms	Interaction with USB flash disc
	Green / Orange	Flashing regularly - period 300 ms	FW activation - do not shut down the device
Tx/Rx Hi Tx/Rx Lo	Green	Permanently lit	Receiver is synchronized to a packet
	Red	Permanently lit	Transmitting to radio channel
COM	Green	Permanently lit	Data receiving
	Yellow	Permanently lit	Data transmitting

Alarm

An Alarm is triggered by any event with severity Error or higher (see *Section 5.4, "Events"*).

1.4. Ordering codes



Trade name – trade and marketing name of the product. This name is used for all products within the same product family.
Possible values: **WaSP**

Gen. – generation of the product of specific Trade name.
Possible values: **1**

Band – frequency band and sub-band
Possible values:
2C: 200 - 470 and 700 - 960 MHz

Ext. – Extension module embedded in mPCIe slot.
Possible values:
N – not used

Var. – designation of product variant. This variant is fixed in unit HW and cannot be changed later on.
Possible values:
A – casing without cooling radiator
B – casing with cooling radiator

Type – specific product type
Possible values:
WASP1-2

Code – part of order code which is printed on Product label on the housing (SW keys are not HW dependent and can be ordered later on, so they are not printed on Product label).

Order code – the complete product code, which is used on Quotations, Invoices, Delivery notes etc.

The WaSP unit uses frequency hopping listed as 5A001.b.3.b in the Regulation (EU) 2021/821, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. Units are subject to export control when exporting outside the European union, according to national, EU and US law (ECCN 5A001.b.3.b), see
https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.
In the case of export from the country where the units were delivered by RACOM, the exporter must inform RACOM of the new country of delivery.

2. Installation

2.1. Mounting

2.1.1. Mounting variant A (without a heat sink)

Mounting is possible in two ways:

- using M4 screws - the screw passes through the device (available only for variant A - without heat sink)
- using M5 screws - the screw uses the thread in the device

For cooling reasons, it is recommended that the marked surface A (upper) be in contact (pressed) with the device structure after mounting for heat dissipation.

Fig. 2.1: Mounting

2.1.2. Mounting variant B (with a heat sink)

Mounting is possible in two ways:

- via side A (heat sink) - the device has a preparation for mounting so that it is possible to push the heat sink through the housing slot and seal the slot with an additional sealing between WaSP and the housing wall.
- via side B (heat sink opposite) - on any structure with the appropriate preparation for screws, the screw holes are not through, the M5 thread in the device is always used during installation, recommended for indoor installations.

2.2. Antenna feed line

The antenna feed line should be chosen so that its attenuation does not exceed 3 to 6 dB as a rule of thumb. Use 50 Ω impedance cables only. The shorter the feed line, the better.

Always follow the installation recommendations provided by the cable manufacturer (bend radius, etc.). Use suitable connectors and install them diligently. Poorly attached connectors increase interference and can cause link instability.

2.3. Power supply

We do not recommend switching on power supply of the WaSP unit before connecting the antenna and other devices. Connecting the RTU and other devices to WaSP while powered increases the likelihood of damage due to the discharge of difference in electric potentials.

WaSP may be powered from any well-filtered 10 to 30 VDC power source. The supply must be capable of providing the required input for the projected RF output. The power supply must be sufficiently stable so that voltage doesn't drop when switching from receiving to transmission, which takes less than 1.5 ms. To avoid radio channel interference, the power supply must meet all relevant EMC standards. Never install a power supply close to the antenna. Connector is internally connected to the casing of the WaSP unit.

3. Web interface

WaSP can be easily managed from your computer using a web browser. If there is an IP connection between the computer and the respective WaSP, you can simply enter the IP address of any WaSP in the network directly in the browser address line and log in. However, it is not recommended to manage an over-the-air connected WaSP in this way, because high amounts of data would have to be transferred over the channel

System fonts are utilized to accelerate the loading of web pages. This functionality was introduced in FW 2.2.5.0. As system fonts are dependent on the operating system, the screenshots featured in this manual were captured on a Microsoft Windows OS.

When you need to manage an over-the-air connected WaSP, log-in to a WaSP, which your computer is connected to using either a cable (via LAN) or a high-speed WAN. The WaSP which you are logged-in to in this way is called Local. Then you can manage any remote WaSP in the network over-the-air in a throughput-saving way: all the static data (e.g. Web page graphic objects) is downloaded from the Local WaSP and only information specific to the remote unit is transferred over the channel. WaSP accessed in such a way is called Remote.

You can also connect to WaSP unit to the hybrid networks in a same way.

For the sake of security only HTTPS protocol is used for the connection between the web browser and WaSP unit. If the http://... is used into the web browser address line, the communication is immediately automatically redirected to HTTPS protocol.

For better protection against unauthorized access to the network there is a timer build within the WaSP unit and the web interface (set to 24 hours by default), which is monitoring user activity. In case of user inactivity, the connection between the web interface and the unit will be interrupted (i.e. automatic logout). Timer is automatically launched in parallel both In the unit and in the web browser. In case of changing the timer setting, we recommend to logout and login, so the correct initialization of timeout inactivity can occur.

First time login page

Login page

The login page informs you about the Unit name and IP address of the WaSP unit you are trying to log in.
The login page allows to view and copy the password.
Web interface is designed for usage on all kinds of equipment - with different screen sizes and screen resolutions. Most of the pictures depicted in this User manual are taken on the desktop type of screen resolution.

Note
A mechanism against brute-force attack is implemented. When wrong combination of the Account / Password is entered you have to wait a while for the following attempt. The time is growing with every wrong attempt.

Web page header

The header of each web page contains:

- Unit name
- IP address of the WaSP unit you are connected to

- Remote access button
- Identification of the current web page (2nd or 3rd level of the menu)
- Changes to commit button
- Notifications button
- Refresh settings button
- User menu button

3.1. Supported web browsers

Supported web browsers for desktop are current versions of:

- Edge
- Chrome
- Firefox
- Safari

Supported Web browsers for mobile equipment are current versions of:

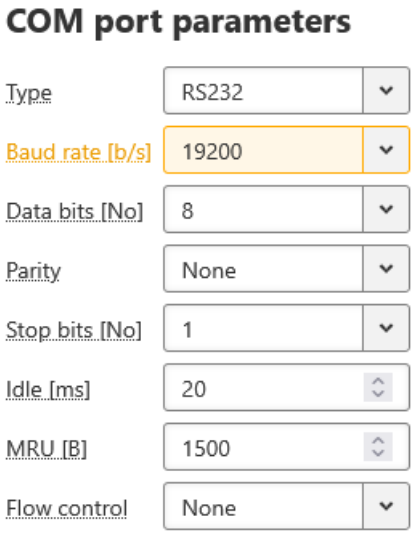
- Safari for iOS
- Chrome for Android

Note

For safety reasons, it is recommended to use a web browser without any extensions (especially extensions, which could get access to data).

3.2. Changes to commit

WaSP is capable of remembering changes, which were done in its configuration and collecting them in a Changes to commit "basket". All changes of configuration parameters are highlighted by different color.



To access the Changes to commit "basket", click on the Changes button (top right corner in the Web page header) or use "Ctrl+Alt+C" shortcut.

Changes to commit "basket" collects all changed settings, which:

- Are separated in the menu alphabetically. Alphabetical separation is sorted hierarchically according to the name of items in the menu.
- Are displayed in the menu (including the path of their placement) and provided with a link for a quick transfer to its original placement.
- Carry an information about their changed values ("Old value" → "New value").

From this page, it is possible to:

- Return to configuration - return to the last changed value's configuration menu.
- Reset changes - all changes will be reset back to their previously set value (not default).
- Send configuration - Apply (Save to the unit) all the changes.

3.3. Notifications

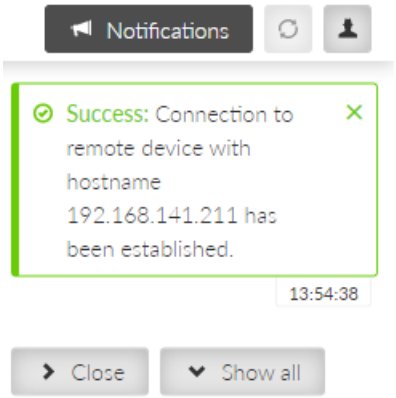
With WaSP new way of showing important system events to the user is introduced. It is called Notification Center and is used consistently throughout the interface. Notification Center is located on the top right corner of the interface. It exists in two forms: active notification display and full Notification Center. Both the active notification display and the full Notification Center are displayed either below the top header of the interface or in the right hand sidebar depending on the size of user's display. The behavior is responsive so in case the user needs to make the browser window narrower, the notification center automatically changes place to use the most efficient location.

Note

To access Notifications it is possible to use shortcut "Ctrl+Alt+N".

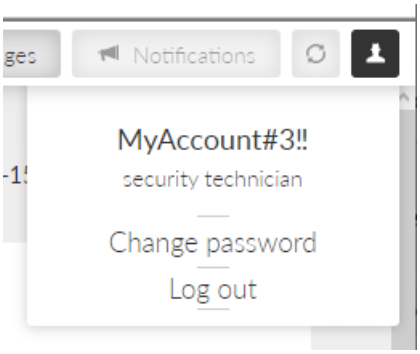
Notifications are mostly triggered by user actions in the interface, for example success or failure of Fast Remote Access connection. They are not to be confused with Events, which are triggered mostly by the system and are not shown in the Notification Center, but on Diagnostics > Events page. In other words Notifications are caused by the user, Events are caused by changing status of the unit.

Every new notification is displayed in the Notification Center drawer. User can either dismiss the notification by clicking the cross in the notification body, close all displayed notifications in the drawer or expand full Notification Center using buttons (“Close all” and “Show all”) on the right side of the Notification Center drawer.



Notification Center collects all notifications that have not been dismissed and allows users to browse them.

3.4. User menu



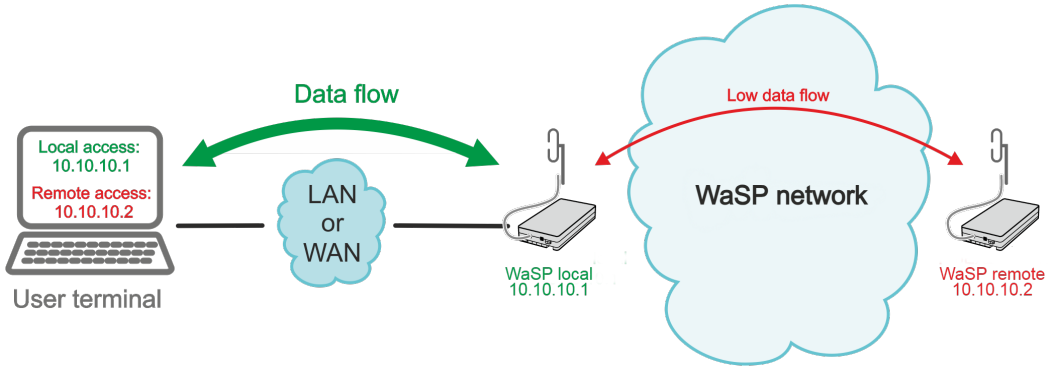
3.5. Remote access

WaSP unit management is designed to work smoothly even when the unit under configuration is connected via relatively slow channel. In case of locally connected unit - direct configuration of the unit (accessing the unit IP address directly from the web browser) works fine. If the unit should be connected remotely via the network, the so-called "Remote access" needs to be used to configure and manage remote unit using bandwidth friendly volumes of transmitted data. Open the web browser, enter the IP

address of a locally connected unit and connect to a remote unit (which needs to be accessible from the locally connected unit via the network).

Note

To access Remote access it is possible to use shortcut "Ctrl+Alt+R".



WaSP local unit must have the newest firmware version in the whole network to ensure proper Remote access functionality. Nevertheless it is recommended to keep the same version of firmware in the whole network. See details in chapter Firmware.

Remote access can be activated by clicking on the Connect access button.

Once the Remote access is successful, the IP address line changes its color to black together with the web page identification.

The IP address of the currently connected WaSP unit is displayed as a part of the Remote access button. All the configuration settings are remotely available using standard web interface. Some of the Diagnostic features are available via local connection only.

Remote access connection can be established directly by entering the IP address of the Remote unit as an additional parameter into the URL. The required format is:
https://LOCAL_UNIT_IP_ADDRESS?remoteAccessTarget=REMOTE_UNIT_IP_ADDRESS

for example: https://192.168.141.210?remoteAccessTarget=10.10.10.212

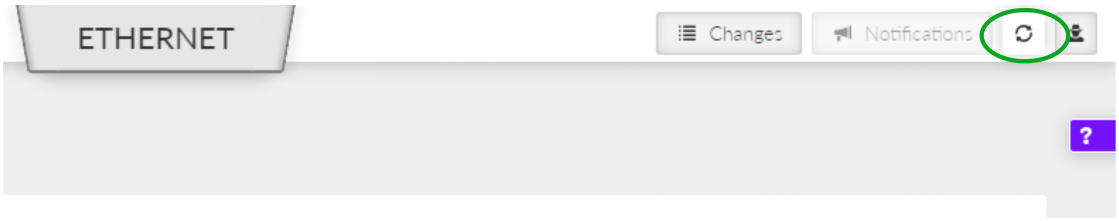
Note

It is possible to use this URL format to make a web browser's bookmark. Such bookmarks can be used for faster access to remote units.

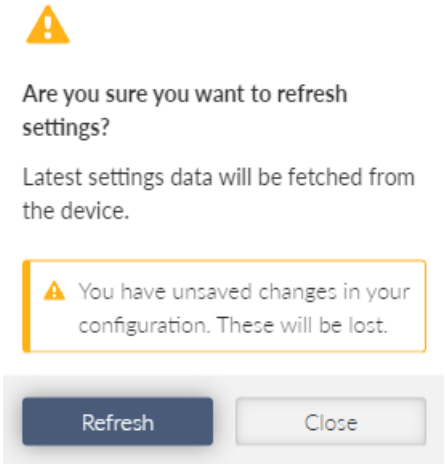
By default, remote access utilizes the **_RO_Rmt_Access_Host_Key** for establishing connections to remote units. However, for enhanced security purposes, we strongly recommend utilizing a custom **RMTACCESS Key** (menu SETTINGS > Security > Credentials).

3.6. Refresh settings

Refresh settings button (placed in the right corner of the web page header) triggers a feature which assures the user that he is working with current data.



Triggering the Refresh will upload current data from the unit to the web client.



Note

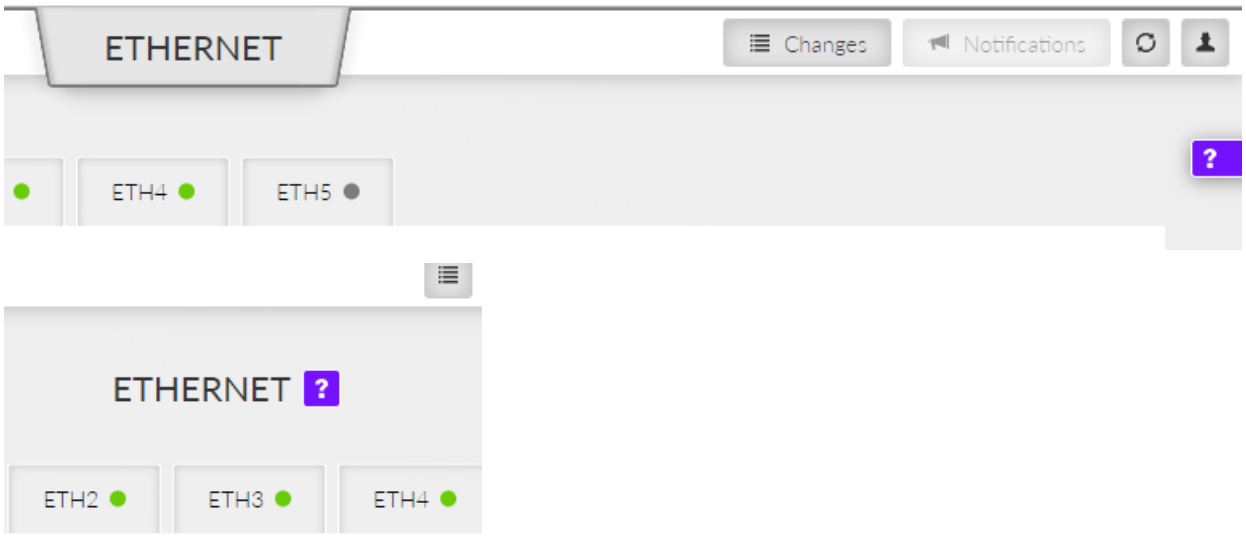
Refresh deletes all non-saved changes which were done in the client.

3.7. Status info area

Status info area provides a general overview about WaSP's individual SETTINGS (or DIAGNOSTICS) section by displaying diagnostic data relevant to the section. To update the data it is necessary to click the Refresh button. It is also possible to use auto refresh feature (Start auto refresh button), which automatically triggers Refresh after defined time period (3, 4, 5... 300 seconds).

3.8. Help

This feature is available on individual web pages of the graphical user interface by clicking on the purple box with the question mark on the right upper corner (or in the middle) of the screen (according to the width of the screen).



The content of the help is identical with the respective sub-chapter of the User manual.

3.9. Shortcuts

Tab. 3.1: Table of shortcuts

Shortcut	Shortcut on STATUS	Access to
Ctrl+Alt+R	R	Remote Access
Ctrl+Alt+O	O	DIAGNOSTICS > Overview
Ctrl+Alt+C	C	Changes
Ctrl+Alt+N	N	Notifications

4. Settings

The Settings chapter contains a description of all configuration parameters of the unit. The division into chapters corresponds to the menu structure in the graphical web interface. The Help pages, which are built into the unit firmware, are identical to this chapter of the manual.

4.1. Interfaces

4.1.1. Ethernet

WaSP provides two physical metallic Ethernet ports ETH1 and ETH2. There is a possibility to define an Ethernet bridge - a logical Network interface - by bridging (joining) together multiple physical Ethernet interfaces. All interfaces bridged together share the same traffic.

4.1.1.1. Network interfaces

The Network interface (technically - an Ethernet bridge) is identified by a name. The name always begins with a "LAN-" prefix. Multiple Network interfaces can be defined. Multiple physical Ethernet interfaces can be bridged together by using single Network interface.

When unit is operating in Bridge mode - the default Network interface bridges together not only physical Ethernet ports, but also the Radio interface. All the Ethernet traffic received by those Ethernet ports is transferred to the Radio interface and transmit by the Radio channel and vice versa.

When unit is operating in Router mode - the Radio channel transmits only the traffic, which is destined to the Radio interface by Routing rules.

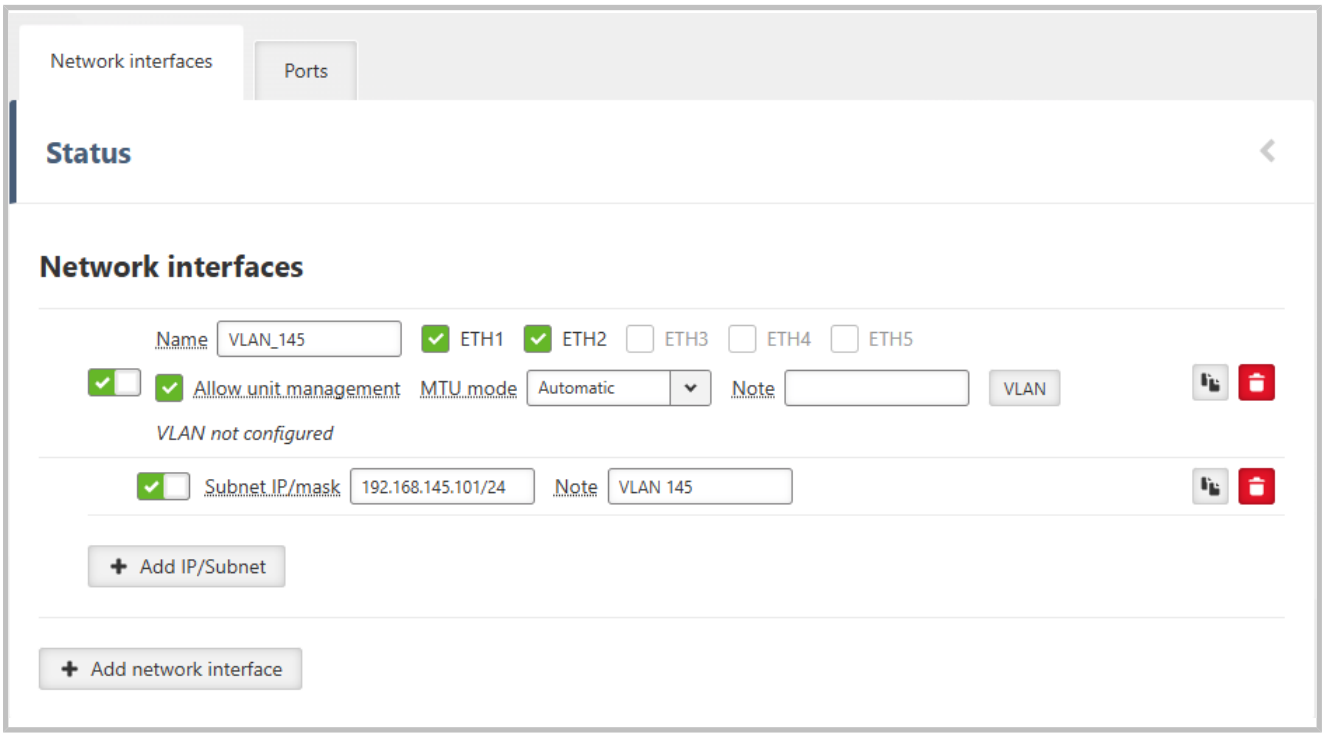


Fig. 4.1: SETTINGS > Interfaces > Ethernet > Network interfaces

The radio unit default setting bridges all Ethernet ports together. New Network interfaces can be defined to split the Ethernet traffic of the individual ports. Any single Ethernet port can be detached from an existing Network interface and added to another Network interface.

Single or multiple Ethernet subnets can be defined within one Network interface. Each subnet is identified by its IP / mask. Use the optional parameter Note to keep your network configuration in human readable manner.

Enable / Disable
Enables / disables the Network interface.

Name
Mandatory name of the Network interface.

ETH1 - ETH2
Range on Ethernet ports selected within the specific Network interface.

Note
If the Network interface has set up either a Radio interface or GRE L2 tunnel, it does not require any ETH ports.

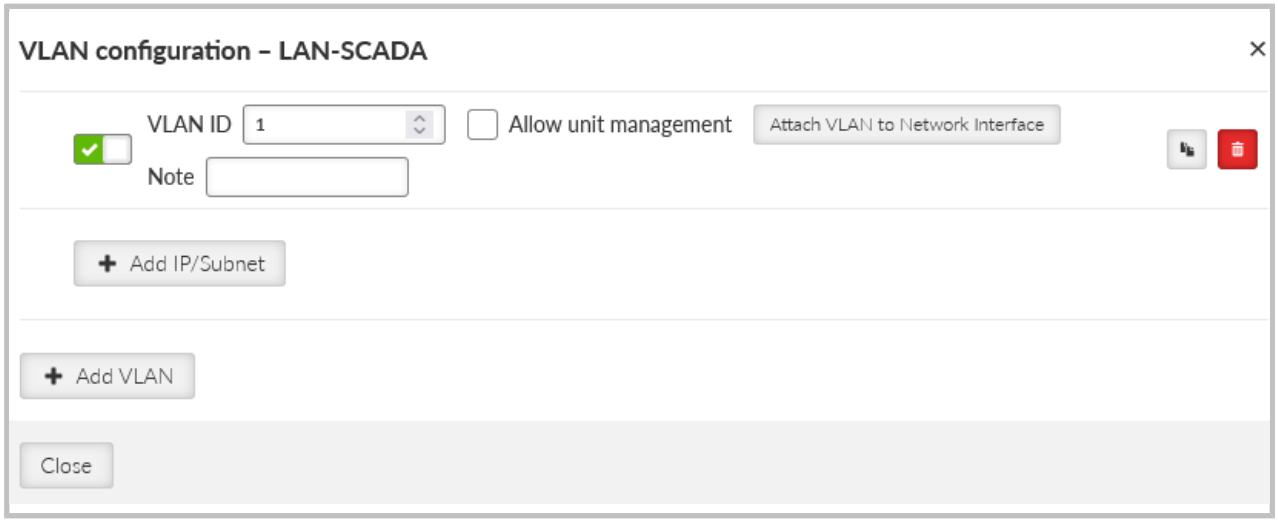
Allow unit management
Enables / disables unit management for the specific Network interface.

Add IP/Subnet
Adds defined subnet to the Network interface.

IP / Mask
IP / mask of the specific Ethernet subnet (in CIDR notation). IP address represents the Network interface in the Layer 3 Ethernet network.

Note
Optional comment.

VLAN
Each Network interface can have one or more attached VLANs with one or more Subnets.



Enable / Disable
Enables / disables VLAN.

VLAN ID
Number {0 – 4094}, default = 1
Specifies the VLAN ID according to IEEE 802.1Q

Allow unit management
Allows / denies unit management for the specific VLAN. This switch is not connected with the Network interface switch with the same name, so only this VLAN can be used for diagnostics.

VLAN priority mapping
Relates to QoS

Attach VLAN to Network interface
Attaches VLAN to the defined network interface

Note
Optional comment.

Add IP/Subnet
Adds defined subnet to the VLAN.

4.1.1.2. Ports

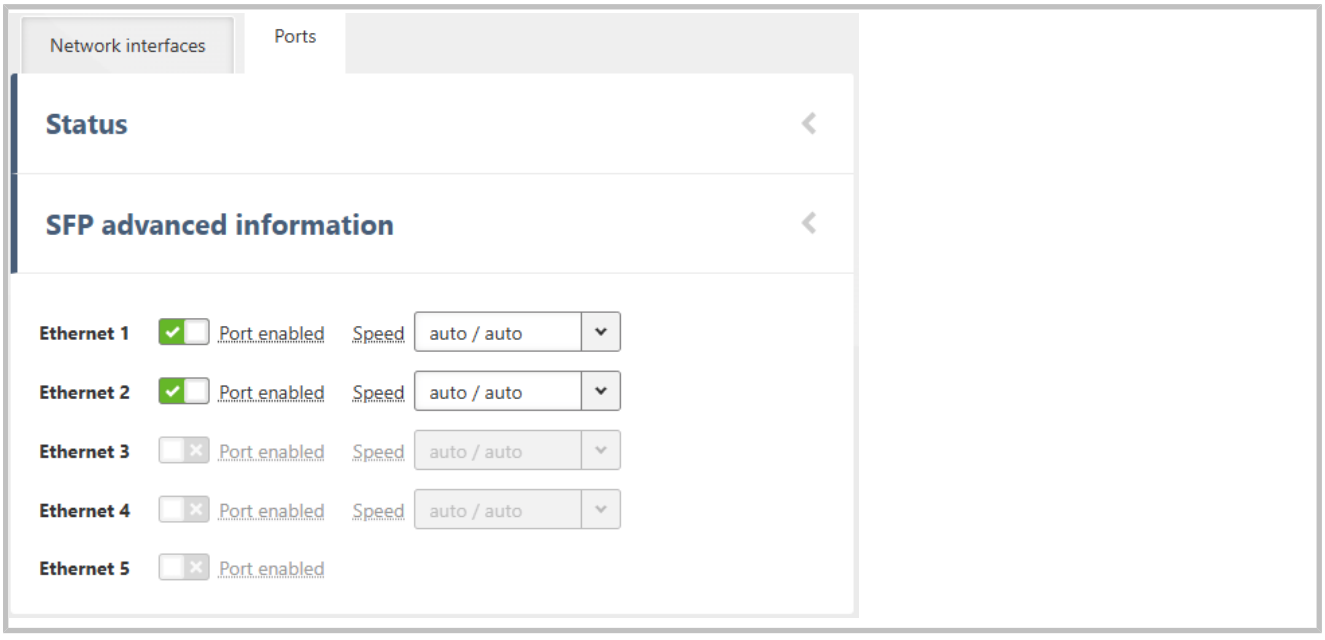


Fig. 4.2: SETTINGS > Interfaces > Ethernet > Ports

Enable / Disable
Enables / Disables ETH ports (1 - 2) SW control.

ETH1 - ETH2 speed
List box {auto / auto; auto / full; auto / half; 100 Mbps / auto; 100 Mbps / full; 100 Mbps / half; 10 Mbps / auto; 10 Mbps / full; 100 Mbps / half}, default = "auto / auto"
Defines the speed and half / full duplex traffic.

Note

When several bridges are interconnected in the network, it is appropriate to switch on Spanning Tree Protocol (ADVANCED > Interfaces > Ethernet > STP) to prevent bridge loops and build a loop-free logical topology.

4.1.2. Radio

Settings of Radio is divided to 5 sections:

- Radio interface
- Radio protocol
- Radio parameters
- Encryption
- Individual link option (router mode only)

Radio interface behavior is heavily affected by a Radio interface mode. For Bridge mode, there is one protocol available:

- *Transparent* – This protocol is very simple; no channel access mechanism takes place. Suitable for star topology with maximum one repeater along the packet path. Available in Bridge mode.

For router mode:

- *Flexible* - Suitable for master or even multi master-slave polling and report by exception from remotes concurrently. No limits in network design – each radio can work as base station, a repeater, a remote, or all of these simultaneously.

Radio channel parameters (such as frequency, output power etc.) are common for all protocols. They are described later in this chapter.

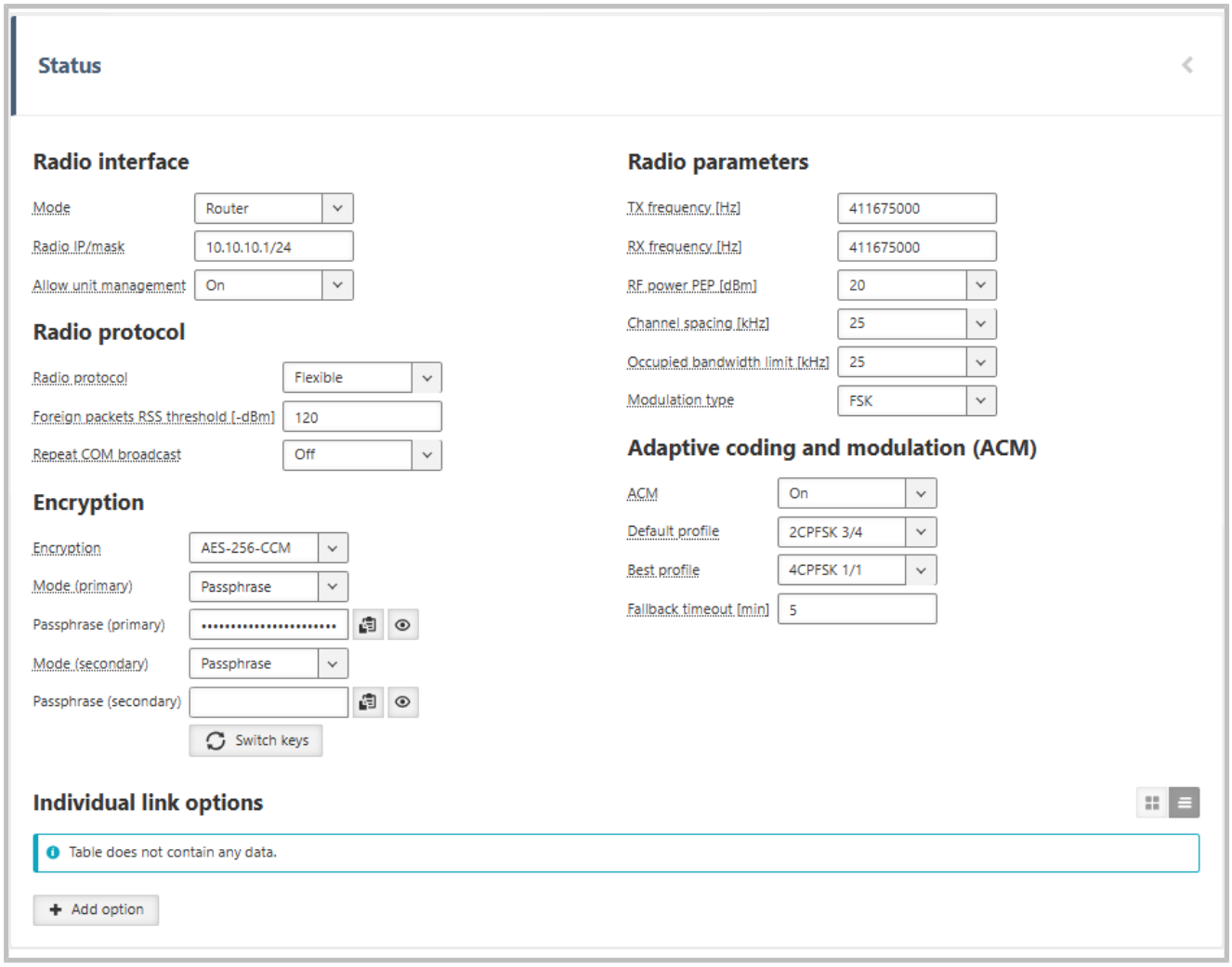


Fig. 4.3: SETTINGS > Interfaces > Radio

4.1.2.1. Radio interface

Mode

List box {Bridge; Router}, default = "Bridge"
Selecting Bridge or Router mode affects many other parameters across the unit. See *???* and *???* for detailed description.

IP / Mask

IP address of the radio interface and the mask of the radio network. This parameter occurs only, if parameter "**Mode**" is set to "Router".

Allow unit management
List box {On; Off}, default = "On"
Allows / disables unit management for the Radio interface.

4.1.2.2. Radio channel parameters

TX frequency
Transmitting frequency in Hz.
The value entered must be within the frequency tuning range of the product as follows:
WaSP1-2C: 200 - 470 MHz, 700 - 960 MHz

RX frequency
Receiving frequency, the same format and rules apply as for TX frequency.

RF power PEP
See *PEP versus RMS RF power*[1].

Channel spacing [kHz]
List box {5, 6.25, 12.5, 25, 50, 100, 150, 200, 250, 300, 400, 625, 1250, 2500, 5000, 10000}, default = "25 kHz"
Sets the width of the radio channel.

Channel spacing (RX) [kHz]
List box {5, 6.25, 12.5, 25, 50, 100, 150, 200, 250, 300, 400, 625, 1250, 2500, 5000, 10000}, default = "25 kHz"
Sets the width of the RX radio channel in Full Duplex mode.

Occupied bandwidth limit [kHz]
List box {5, 6.25, 11, 12.5, 14, 16, 20, 25, 40, 50, 80, 100, 125, 150, 175, 200, 225, 250, 300, 400, 625, 1250, 2500, 5000, 10000}, default = "25 kHz"
Occupied bandwidth is limited by granted radio channel.

Occupied bandwidth limit (RX) [kHz]
List box {5, 6.25, 11, 12.5, 14, 16, 20, 25, 40, 50, 80, 100, 125, 150, 175, 200, 225, 250, 300, 400, 625, 1250, 2500, 5000, 10000}, default = "25 kHz"
Sets the occupied bandwidth of the RX radio channel in Full Duplex mode.

[1] https://www.racom.eu/eng/products/m/ripex/app/pep/pep.html

Modulation type
List box {FSK}, default = "FSK"

FSK
Suitable for difficult conditions – longer radio hops, non-line of sight, noise / interferences on Radio channel…

Modulation

FSK modulations:
List box {2CPFSK; 4CPFSK}, default = "2CPFSK"

Note
For more detailed information see *???*.

FEC
List box {3/4; Off}, default = "Off"
FEC (Forward Error Correction) is a very effective method to minimize radio channel impairments. Basically, the sender inserts some redundant data into its messages. This redundancy allows the receiver to detect and correct errors; used is Trellis code with Viterbi soft-decoder. The improvement comes at the expense of the bitrate. The lower the FEC ratio, the better the capability of error correction and the lower the bitrate. Bitrate = Modulation rate × FEC ratio.

Radio can receive not only radio frames with the very same setting, but also frames with different type of modulation - the Auto-speed functionality.

4.1.2.3. Adaptive coding and modulation (ACM)

The ACM mechanism adapts the current modulation and coding to the signal quality of each individual radio link between stations. Specific modulation and coding pairs (profiles) are arranged so that the transmission channel capacity increases with increasing signal quality due to the gradual switching of ACM profiles. ACM works independently for each direction of the link. The signal quality measurement required for the ACM algorithm is performed on the receiver side. The signal quality information is delivered to the transmitter as an extension of the data packets. ACM therefore brings a certain overhead in addition to the transmitted data.

Implementation differences according to the type of radio protocol:

Transparent: ACM can be used with only 2 stations in the network, i.e. only for point-to-point communication.

Flexible: ACM is not limited by the network topology. It therefore also works in point-to-multipoint communication including multiple retranslation in a daisy-chain scenarios.

Base driven: ACM is not limited by the network topology. It therefore also works in point-to-multipoint communication including retranslations.

The ACM parameter setting is global for the entire network. All stations in the entire radio network should either have ACM enabled or disabled.

ACM
List box {On; Off}, default = "Off"

Enables / Disables Adaptive coding and modulation (ACM) for the radio interface. When enabled, the **Modulation** and **FEC** parameters selection is disabled. Modulation a FEC is controlled automatically by ACM. To enable ACM, you must have the corresponding SW key installed.

Default profile

List box {2CPFSK 3/4 (FSK); 4CPFSK 3/4 (FSK); 4CPFSK 1/1 (FSK)}, default = "2CPFSK 3/4"
Initial and also minimum ACM profile.

Best profile

List box {2CPFSK 3/4 (FSK); 4CPFSK 3/4 (FSK); 4CPFSK 1/1 (FSK)}, default = "2CPFSK 3/4"
Maximum ACM profile. The Best profile can be the same or higher than the Default profile.

Fallback timeout [min]

Number {1 – 60}, default = 10
If no communication occurs on the monitored radio channel during this time interval, the information about the status of this channel is declared obsolete and the ACM is switched to the initial profile - the **Default profile** value.
Switching to the Default profile is performed at the next communication on the radio channel.

4.1.2.4. Encryption

Encryption

List box {Off; AES-256-CCM; AES-256-CCM+KEX}, default = "Off"
AES 256-CCM (Advanced Encryption Standard with Cipher Block Chaining-Message Authentication Code) according to RFC 6655 can be used for encryption and authentication of packets on Radio channel to protect your data from an intrusion and replay attack. When AES 256-CCM is On, a control block of 25 Bytes length (13 B nonce + 12 B TAG) is attached to each frame on Radio channel. AES requires an encryption key. The length of key is 256 bits. The same key must be stored in all units within the network. The AES-CCM provides assurance of the confidentiality and the authenticity of data according to NIST SP 800-38C.
AES-256-CCM+KEX uses a static shared key to negotiate dynamic keys that encrypt user data. Dynamic keys are unique to each station and are changed periodically. It encrypts the data content of packets and monitors the integrity of part of the headers.

Mode

List box {Passphrase; Key ID}, default = "Passphrase"
This parameters occur, if parameter "**Encryption**" is set to "AES-256-CCM; AES-256-CCM+KEX".

Passphrase

The key can be automatically generated based on a Passphrase. Fill in your Passphrase (any printable ASCII character, min. 1 char, max. 128 char). The same Passphrase must be set in all units within the network. This parameter occurs only, if parameter "**Mode**" is set to "Passphrase".

Key

The Key stored in SETTINGS > Security > Credentials is used. It is possible to use the default key with IDRadio_Encryption_Key or (highly recommended) to generate own key (Generate credential : your ID, Type PSK Key (PRI) AES, PSK length 32 B). The same key must be used in all units within the network (it is possible to download it from the first unit and upload it to allother units: SETTINGS > Security > Credentials > Add credential: fill your ID, change Type to PSK Key (PRI) AES and select the proper file with the key).

Note
The required key type is “PSK key” and it must be exactly 32 bytes long (256 bits).

This parameter occurs only, if parameter "**Encryption**" is set to "AES-256-CCM+KEX".

Key replacement period

Number {5 – 10080}, default = 1440 [min]
The average data channel key replacement period (randomized within a range of +- 10%).

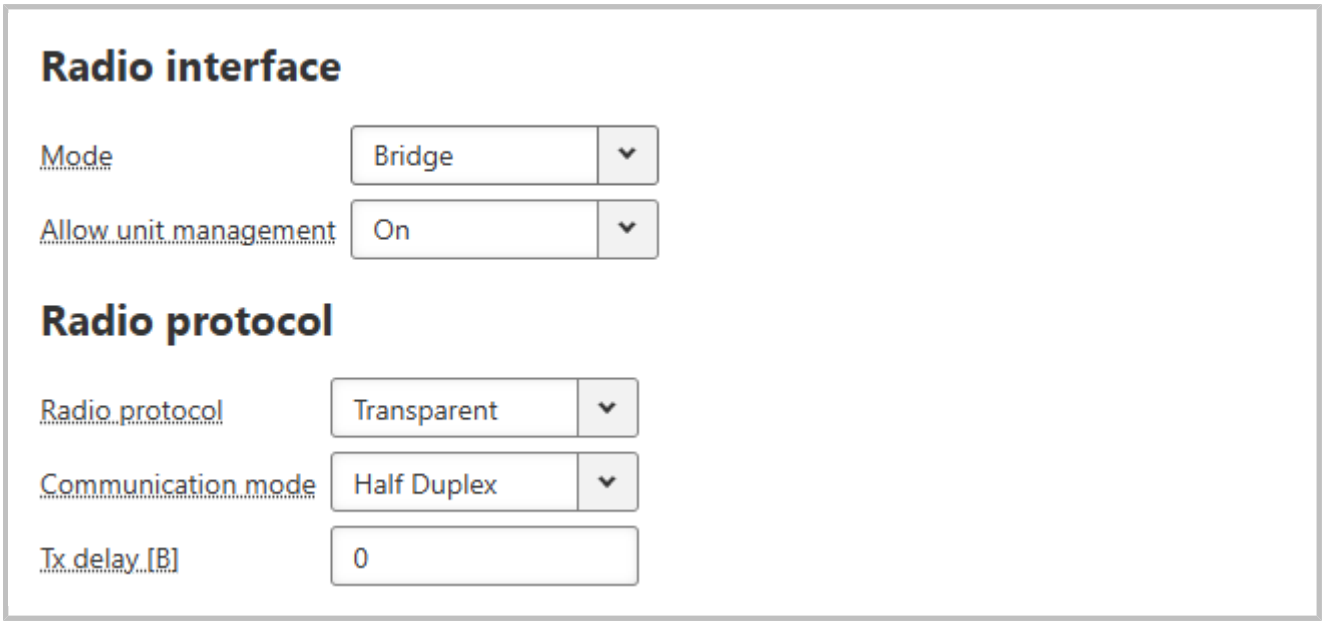
4.1.2.5. Transparent protocol (Bridge mode)

Bridge mode with fully transparent Radio protocol is suitable for all polling (request-response) applications with star network topologies, however repeater(s) are possible.

A packet received through any interface (bridged with the radio interface) is broadcasted to the appropriate interfaces of all units within the network.

Any unit can be configured as a repeater. A repeater relays all packets it receives through the radio channel. The network implements safety mechanisms which prevent cyclic loops in the radio channel (e.g. when a repeater receives a packet from another repeater) or duplicate packets delivered to the user interface (e.g. when WaSP receives a packet directly and then from a repeater).

Transparent protocol does not solve collisions on the radio channel protocol. There is a CRC check of data integrity, however, i.e. once a message is delivered, it is 100% error free.



Radio protocol

List box {Transparent; None}, default = "None"

Communication mode

List box {Half Duplex; Full Duplex}, default = "Half Duplex"

Full duplex mode is intended to be used mainly for Point-to-Point communication. Full duplex operation is not possible in networks with repeaters.

Note

HW option RipEX2e (product variant ‘H' and 'J’) enables Half duplex operation only.

Unit is repeater

List box {On; Off}, default = "Off"

Each WaSP may work simultaneously as a Repeater (Relay) in addition to the standard Bridge operation mode.

If "On", every frame received from Radio channel is transmitted to the respective user interface (ETH, COM) and to the Radio channel again.

The Bridge functionality is not affected, i.e. only frames whose recipients belong to the local LAN are transmitted from the ETH interface.

It is possible to use more than one Repeater within a network. To eliminate the risk of creating a loop, the “Number of repeaters” has to be set in all units in the network, including the Repeater units themselves.

Warning: Should Repeater mode be enabled “Modulation rate” and “FEC” must be set to the same value throughout the whole network to prevent frame collisions occurring.

No of repeaters

Number {0 – 7}, default = 0

If there is a repeater (or more of them) in the network, the total number of repeaters within the network MUST be set in all units in the network, including the Repeater units themselves. After transmitting to or receiving from the Radio channel, further transmission (from this WaSP) is blocked for a period calculated to prevent collision with a frame transmitted by a Repeater. Furthermore, a copy of every frame transmitted to or received from the Radio channel is stored (for a period). Whenever a duplicate of a stored frame is received, it is discarded to avoid possible looping. These measures are not taken when the parameter “Number of repeaters” is zero, i.e. in a network without repeaters.

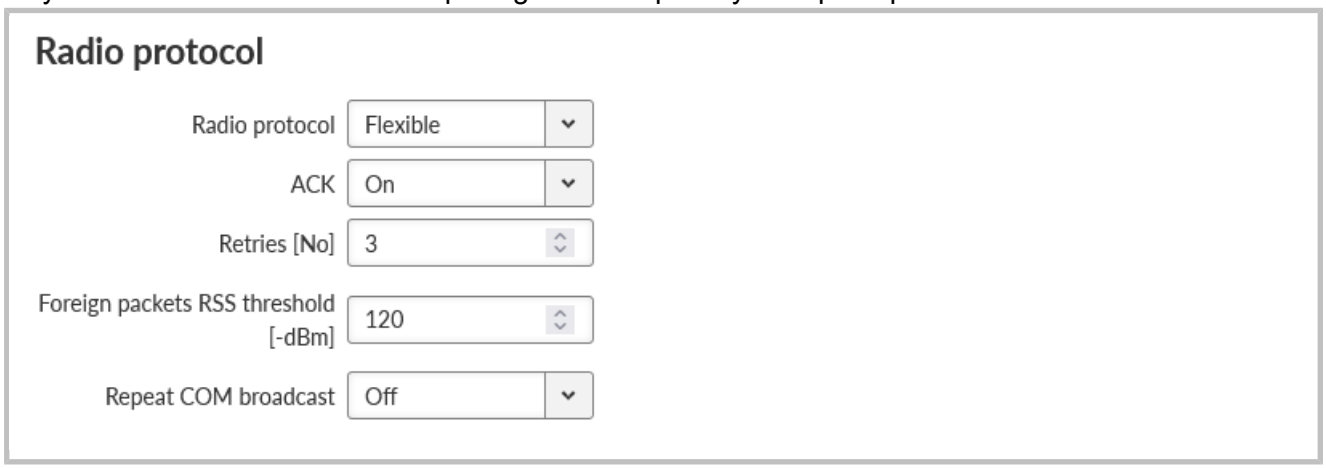
Tx delay [B]

Number {0 – 1600}, default = 0

This parameter should be used when all substations (RTU) reply to a broadcast query from the master station. In such case massive collisions would ensue because all substations (RTU) would reply at nearly the same time. To prevent such collision, TX delay should be set individually in each slave WaSP. The length of responding frame, the length of **Radio protocol overhead**, modulation rate have to be taken into account.

4.1.2.6. Flexible Protocol (router mode)

Router mode with Flexible protocol is suitable for Multipoint networks of all topologies with unlimited number of repeaters on the way, and all types of network traffic where Multi-master applications and any combination of simultaneous polling and/or report-by-exception protocols can be used.



ACK

List box {On; Off}, default = "On"

General setting of acknowledging of received packets. It can be set differently in individual link options.

Retries

Number {0 – 15}, default = 3

Foreign packets RSS threshold [-dBm]

Number {50–150}, default = 120

When the received foreign packet (the packet which is not addressed to the actual unit) has weaker signal (the listed number bigger, e.g. the limit 120 - in minus dBm - compared with actual RSS -126 dBm), the channel is evaluated as free. If the foreign packet RSS is over this limit, the channel is occupied and the unit will wait till the end of it with the procedure of transmission.

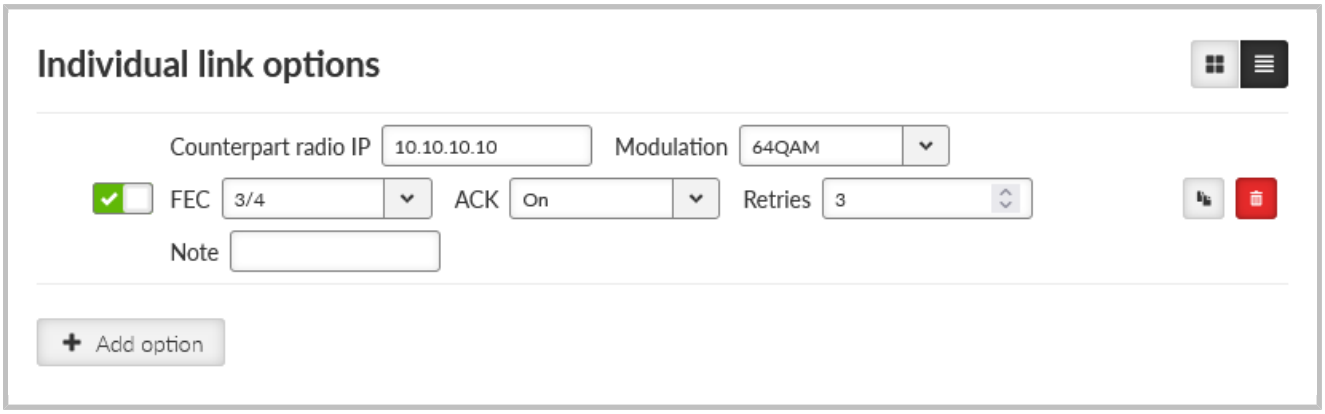
Repeat COM broadcast

List box {On; Off}, default = "Off"

When On the broadcasted COM packets will be retranslated into the radio channel. When Off these packets will not be repeated.

4.1.2.6.1. Individual link option

It is possible to add some exceptions for radio links with particular conditions (e.g. longer or shorter ones than common).



The individual link is defined by **Counterpart radio IP**. For this link it is possible to set individually **Modulation, FEC, ACK, Retries.**

Retries are used to set a number of repeats, when the packet is not acknowledged (in case of ACK ON). The standard number of retries is 3.

Note

It is highly recommended to set common modulation to the lowest required modulation within the network. Modulation for Individual link is recommended to set higher, because broadcast frames are always transmitted over the common modulation.

4.1.2.7. Advanced radio parameters

The Advanced setting option allows to customize radio and radio protocol parameters. Typically these parameters should remain on default values.

These settings you can find in ADVANCED > Interfaces > Radio > menu

4.1.2.7.1. Radio interface - advanced

MTU [B]

Number {70 – 1500}, default = 1500 B
If a packet entering to an interface exceeds the maximum value, it is either discarded or fragmented.
Minimum MTU value to establish TCP between WaSP units = 576 B.
Minimum MTU value for IPv6 (Babel) = 1280 B.

Only for Flexible

Gratuitous ARP broadcast

List box {On; Off}, default = "Off"
Enables regular sending of gratuitous ARP Reply broadcasts (notification of the radio's IP address to neighbors)

Gratuitous ARP interval

Number {1 – 24}, default = 2
Length of period [hours] of sending gratuitous ARP Reply

4.1.2.7.2. Radio channel - advanced

Maximal distance

Number {0 – 200}, default = 100

This parameter allows to set a maximal distance of a radio hop (in km). The same number shall be used for the whole network. We recommend to change the value only in case that the network uses radio hops longer than 100 km.

Resilience

List box {High sensitivity; Auto; High resilience; User}, default = "Auto"

WaSP is equipped with cognitive function of receiving mode selection. When exposed in a radio environment where strong interfering signals (stronger than -45 dBm) are present, WaSP senses them and adaptively increases its resistance to interference (by lowering its sensitivity by up to 2-3 dB).

Resilience parameter controls this functionality. By default the **Auto** is set - when intereference holds, WaSP stays in High resilience mode of receiver operation and signals this state by turning the yellow RX LED on. Once the interfering signals fade away, WaSP automatically returns to its High sensitivity mode of receiver operation. It is possible to switch this functionality permanently off (**High sensitivity**) or permanently on (**High resilience**).

The last option is to set this Resilience value to a fixed value from 0 to 31 dB (if the "User" option is specified).

High resilience LED indication

List box {On; Off}, default = "Off"

Enables indication of High resilience mode by yellow RX status LED.

4.1.2.7.3. Queues

TX Buffers

The Radio protocol transmission buffer handles data waiting to be transmitted. Its size is defined by both the number of records (Queue length) and total storage space (Queue size) requirement. Records are held in a queue which is considered full, if either the Queue length or Queue size is reached. New incoming frames are not accepted when the queue is full.

The TX buffer is active for all radio protocols.

This functionality is available in ADVANCED > Interfaces > Radio > Queues menu

Queue length [packets]

Number {1 – 31}, default = 5

Queue length dictates the maximum number of records held in the queue.

Queue size [kB]

Number {1 – 48}, default = 5

Queue size dictates the total size of all records that can be held in the queue.

TX Buffer timeout enabled

List box {Off; On}, default = "Off "

The frames waiting for transmission in the Radio protocol output frame queue will be discarded after the TX Buffer timeout expires. This parameter should be enabled for types of applications where sending old frames brings no benefit.

When the frame is discarded the event is recorded, both in the statistics (as “Rejected”) and in the monitoring (the respective frame is displayed with the “Tx buffer timeout” tag).

TX Buffer store timeout [s]

Number {0.01 – 150}, granularity 0.01, default = 5

Radio protocol transmit buffer timeout. The “TX Buffer timeout” must be enabled for this parameter to be initiated.

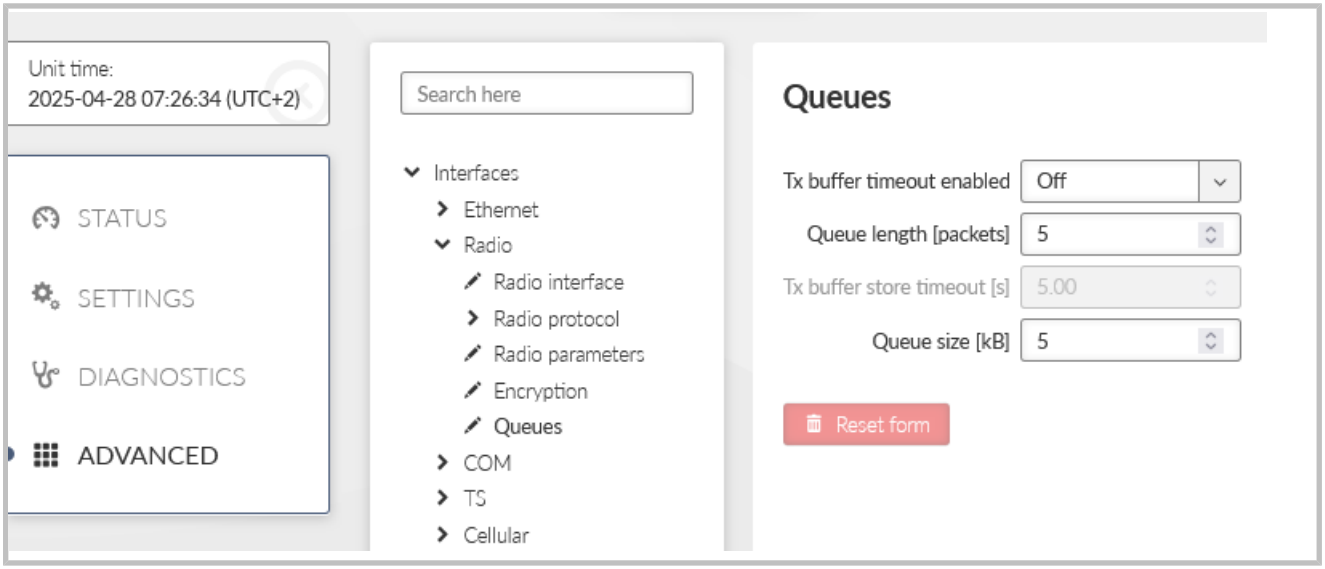


Fig. 4.4: ADVANCED > Interfaces > Radio > Queues

4.1.2.7.4. Flexible protocol - advanced

This settings allows to customize individual length and numbers of slots used for accessing of the radio channel or waiting with retransmissions of an undelivered packet.

The length of the slots has to be same in all radio units within on radio network. It is highly recommended to consult changes of these parameters with our technical support.

4.1.3. COM

Data incoming to the WaSP unit from the COM port are received by the Protocol module. The Protocol module behavior depends on the Protocol selected. In case of Transparent protocol (available in Bridge mode only), it is transparently transmitted to the WaSP network and sent out through all COM ports with Transparent protocol selected. If any other protocol is selected, the incoming frame from the COM port is processed by the Protocol module, translated into UDP frame, forwarded to the WaSP router module and further processed according to router rules. Such UDP frames received by the WaSP unit from the WaSP network (based on the unit IP address and UDP port of the Protocol module) are translated into original frame format (by the Protocol module) and send out through the COM port.

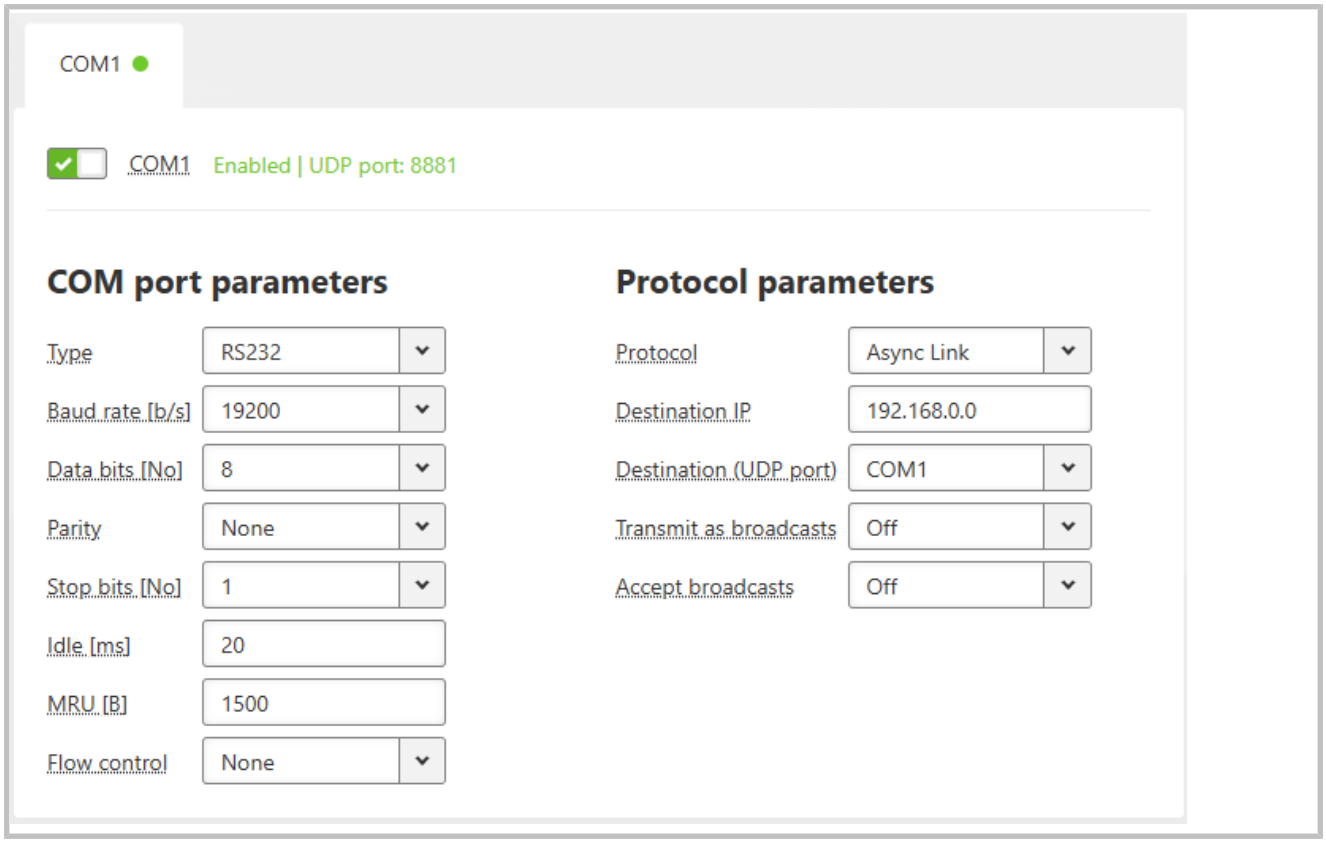


Fig. 4.5: SETTINGS > Interfaces > COM

The menu is divided to two parts:

4.1.3.1. COM port parameters

This settings of Baud rate, Data bits, Parity and Stop bits of COM port and setting of connected device must match.

Type

List box {possible values}, default = "RS232"

COM port can be configured to RS232.

Baud rate [b/s]

List box {standard series of rates from 600 to 1152000 b/s}, default = "19200"
Select Baud rate from the list box: 600 to 1152000 b/s rates are available.
Serial ports use two-level (binary) signaling, so the data rate in bits per second is equal to the symbol rate in bauds.

Data bits

List box {5; 6; 7; 8}, default = 8
The number of data bits in each character.

Parity

List box: {None; Odd; Even}, default = "None"
Wikipedia: Parity is a method of detecting errors in transmission. When parity is used with a serial port, an extra data bit is sent with each data character, arranged so that the number of 1-bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1-bits, then it must have been corrupted. However, an even number of errors can pass the parity check.

Stop bits

List box {1; 2 (1.5)}, default = 1, for 5 data bits the 1.5 length of stop bits is used instead of 2
Wikipedia: Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronize with the character stream.

Idle [ms]

Number {10 – 16383}, default = 20
This parameter defines the maximum gap (in milliseconds) in the received data stream. If the gap exceeds the value set, the link is considered idle, the received frame is closed and forwarded to the network.

MRU [B]

Number {1 – 2047}, default = 1500
MRU (Maximum Reception Unit) — an incoming frame is closed at this size even if the stream of bytes continues. Consequently, a permanent data stream coming to a COM results in a sequence of MRU-sized frames sent over the network.

Note
1. Very long frames (>800 B) require good signal conditions on the Radio channel and the probability of a collision increases rapidly with the length of the frames. Hence if your application can work with smaller MTU, it is recommended to use values in 200 – 400 bytes range.

Note
2. This MRU and the MTU in Radio settings are independent, however MTU should be greater or equal to MRU.

Flow control

List box {None; RTS/CTS}, default = "None"
RTS/CTS (Request To Send / Clear To Send) hardware flow control (handshake) between the DTE (Data Terminal Equipment) and WaSP (DCE - Data Communications Equipment) can be enabled in order to pause and resume the transmission of data. If RX buffer of WaSP is full, the CTS goes down.

Note
RTS/CTS Flow control requires a 5-wire connection to the COM port.

Buffer flush time [ms]
Number {0 – 65535}, default = 0
This parameter can be used to prevent unwanted deadlock of the serial communication. The timer is reset by every received or transmitted packet over the COM port. When the timer expires, the protocol status is reset and the packet buffer is cleared. Setting parameter to 0 disables the feature. This parameter is available only via ADVANCED menu.

4.1.3.2. Common Protocol parameters

Each SCADA protocol used on serial interface is more or less unique. The COM port protocol module performs conversion to standard UDP datagrams to travel across WaSP Radio network. The same settings are valid for Terminal servers as well (for more details about TS see *Section 4.1.4, "Terminal servers"*).

Protocol
List box {None; Transparent; Async Link; COMLI; DNP3; DF1; IEC101; Mars-A; Modbus RTU; PR2000; RDS; S3964R; SAIA S-BUS; UNI}, default = "None"
Transparent protocol can be used when unit operates in Bridge mode only. All the traffic is bridged transparently to WaSP network.

Broadcast
List box {On; Off}, default = "On"
Some Master SCADA units sends broadcast messages to all Slave units. SCADA application typically uses a specific address for such messages. WaSP (Protocol module) converts such message to a customized IP broadcast and broadcasts it to all WaSP units resp. to all SCADA units within the network.

Broadcast address
Number {0 – 65535}, default = 255
The protocol address which is treated as broadcast address.

Address translation
List box {Mask; Table}, default = "Mask"
SCADA protocol address is translated to the IP address using either Mask (common rule for all addresses) or Table (specific rule per address) type of conversion

Base IP / Mask

A part of Base IP address defined by this Mask is replaced by 'Protocol address'. The SCADA protocol address is typically 1 byte long, so Mask 24 (255.255.255.0) is most frequently used. This IP address is used as a destination IP address of the UDP datagram into which the serial SCADA packet received from COM is encapsulated.

Destination UDP port

List box {Manual; COM1 – COM3; TS1 – TS5}, default = "COM1"
The same UDP port will be used for all destination. This UDP port is used as the destination UDP port in UDP datagram in which serial SCADA packet received from COM is encapsulated. Default UDP ports for COM or Terminal servers can be used or UDP port can be set manually. If the destination IP address belongs to a WaSP and the UDP port is not assigned to COM or to a Terminal server or to any other special SW module running in the destination WaSP, the packet is discarded.

Protocol address (from)

This is the address which is used by SCADA protocol.
The typical Protocol address length is 1 Byte. Some protocols, e.g. DNP3 are using 2 Bytes long addresses.

Protocol address (to)

Several consecutive SCADA addresses shall be translated using one rule.

IP address (base)

IP address to which Protocol address will be translated. This IP address is used as a destination IP address of the UDP datagram into which the serial SCADA packet received from COM is encapsulated. When several addresses are used, this will be the first IP address, the following one will have +1 etc.

Destination (UDP port)

List box {MANUAL; COM1 – COM3; TS1 – TS5}, default = "COM1"
This is UDP port number which is used as destination UDP port into UDP datagram in which the serial SCADA message, received from COM, is encapsulated. Different Destination UDP ports can be used in different rules.

Address translation: Mask

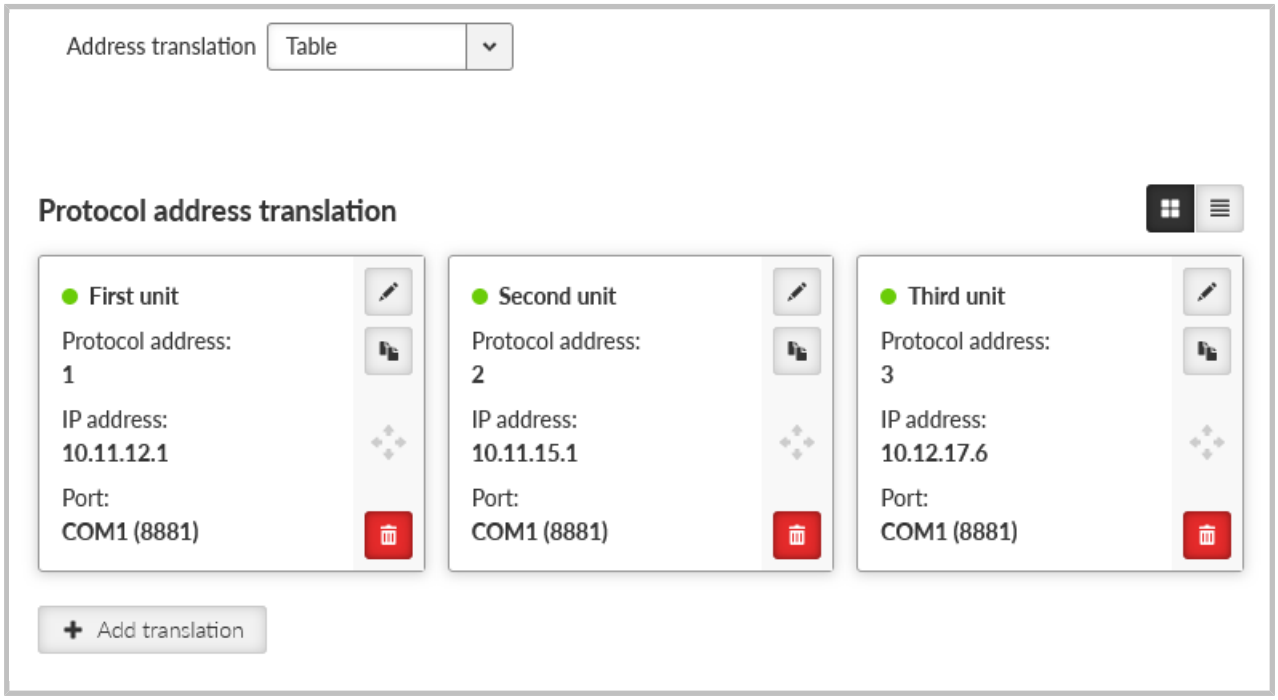
Note
All IP addresses used have to be within the same subnet, which is defined by this Mask
The same UDP port is used for all the SCADA units, which results in the following limitations:

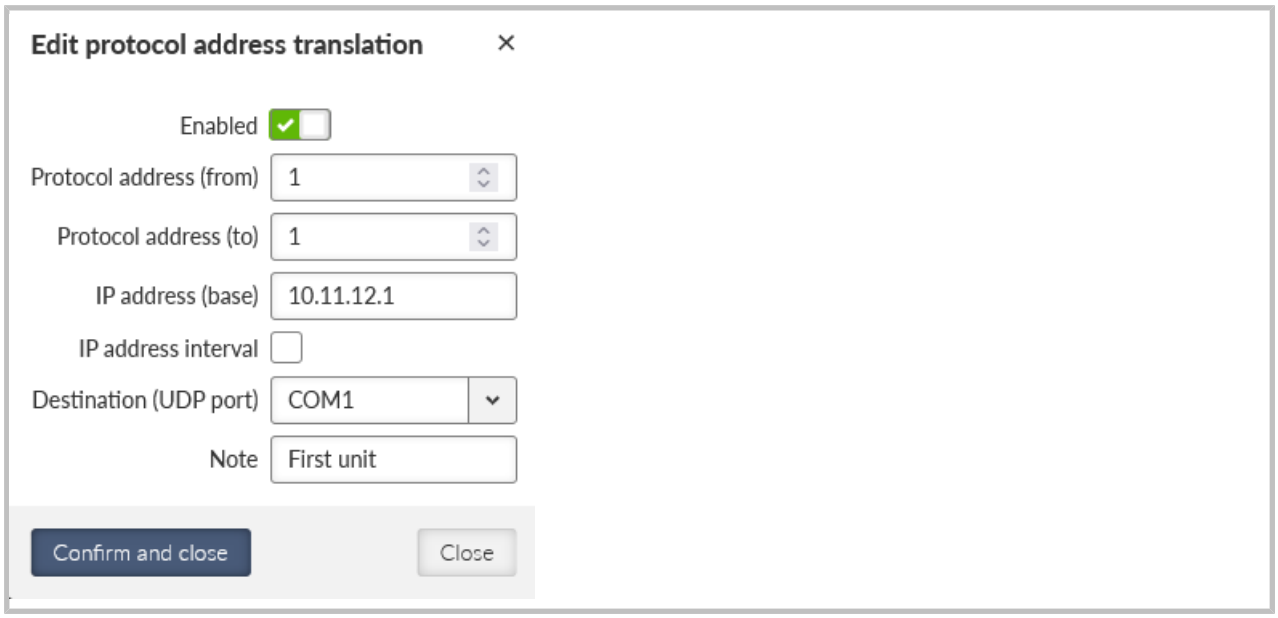
SCADA devices on all sites have to be connected to the same interface

Only one SCADA device to one COM port can be connected, even if the RS485 interface is used.

Address translation: Table

The Address translation is defined in a table. There are no limitations such as when the "Mask" translation is used. If there are more SCADA units connected via the RS485 interface, their multiple "Protocol addresses" are translated to the same IP address and UDP port pair.





Note
You may add a note to each address with your comments (UTF8 is supported) for your convenience.

4.1.3.3. Individual protocol parameters

Some of the SCADA protocols are able to setup additional Slave device response behavior.

Response target mode

List box {LASTRCV; TARGET}, default = "LASTRCV"

Response for the incoming frame shall be directed to the IP address of the Master which sent the frame (LASTRCV) or to a specified IP address (TARGET).

Response target IP
IP address to which the response is sent when TARGET is chosen in the Response target mode.

4.1.3.3.1. None

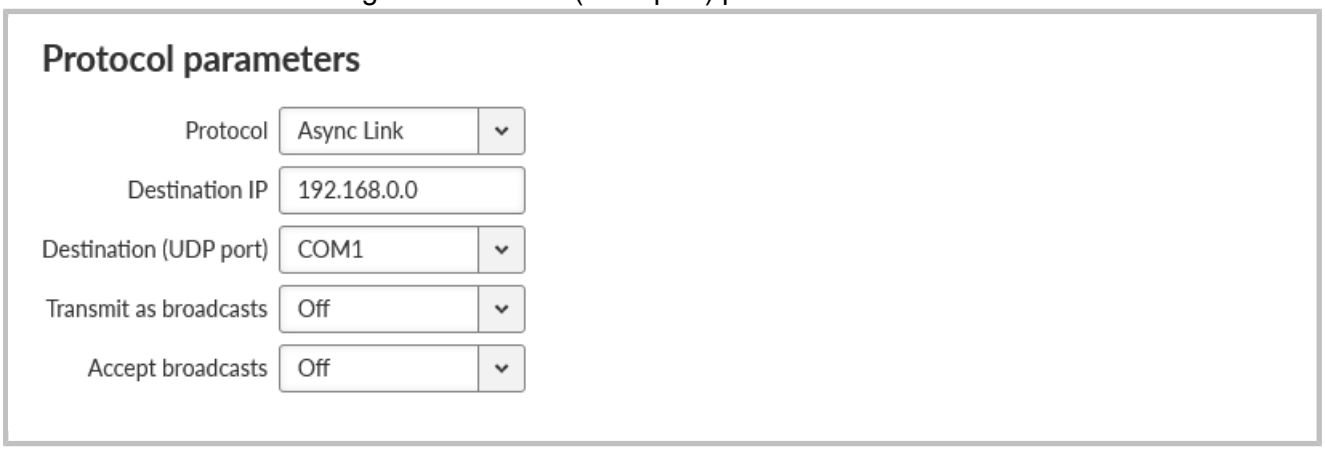
The None protocol switches the COM port off. All incoming data will be thrown away, no data will be sent into the COM interface.

4.1.3.3.2. Transparent protocol

Operates in Bridge mode only. All the traffic is bridged transparently to WaSP network (see *???* for details).

4.1.3.3.3. Async link

Async link creates an asynchronous link between two COM ports on different WaSP or WaSP units. Received frames from COM port or from a Terminal server are sent without any processing transparently via router to the set IP destination and UDP port. Received frames from the network are sent to COM or Terminal server according to Destination (UDP port) parameter.



Destination IP
Defines destination IP address of WaSP or WaSP).

Transmit as broadcasts
List box {On; Off}, default = "Off"
Allows sending of the packets incoming from COM port as broadcast.

Accept broadcasts
List box {On; Off}, default = "Off"
On: Broadcast packets from the radio channel will be send to the COM port.
Off: Only unicast packets will be sent to the COM port.

4.1.3.3.4. COMLI

COMLI is a serial polling-type communication protocol used by Master-Slave application. When WaSP radio network in Router mode is used, more COMLI Masters can be employed within one Radio network and one Slave can be polled by more Masters. Broadcast packets are not used.

The frame of COMLI protocol is sent transparently, but without STX, ETX and BCC. STX (start of data), ETX (end of data) and BCC (8-bit XOR) are added on the receiving participant. While transfer, data integrity is properly secured by individual protocol checksums.

Note

The COMLI protocol in the WaSP or WaSP is not fully compatible on COM port with WaSP and MR modems. WaSP implementation is not supporting “Intercharacter tx delay”.

Mode of Connected device: MASTER

Congestion timeout [ms]

Number {0 – 65535}, default = 3000, 0 switches this functionality off

Timeout for checking of the duplicity of two following frames. Used when the very same frame is incoming via COM port within the timeout measured from the moment of dispatch of the previous frame.

Mode of Connected device: SLAVE

Response timeout [ms]

Number {0 – 16383}, default = 1000

COMLI protocol response timeout is used for waiting on COM port for the response of connected device.

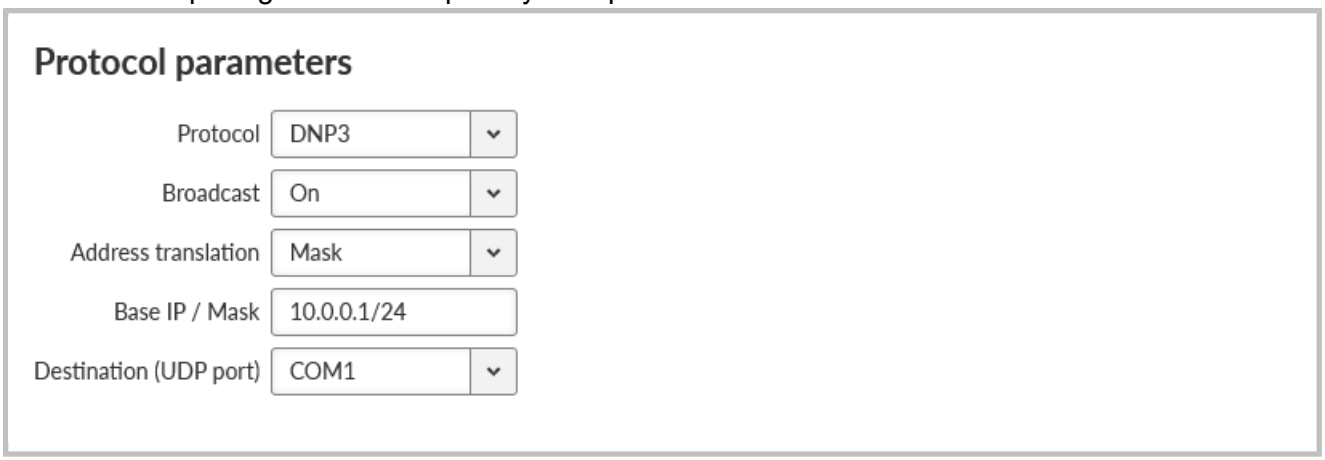
Response target mode

List box {LASTRCV; TARGET}, default = ”LASTRCV”

Slave response will be sent to the address of the last received request (LASTRCV) or to the specified **Response target IP** address (TARGET).

4.1.3.3.5. DNP3

Each frame in the DNP3 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in terms of the WaSP configuration. The DNP3 allows both Master-Slave polling as well as report-by-exception communication from the remote units.



The common parameters (e.g. address translation) shall be set.

Broadcast

List box {On; OFF}, default = "On"

Note

There is not an option to set the Broadcast address, since DNP3 broadcast messages always have addresses in the range 0xFFFD - 0xFFFF. Hence when Broadcast is On, packets with these destinations are handled as broadcasts.

4.1.3.3.6. DF1

Each frame in the Allen-Bradley DF1 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in the Full duplex mode in terms of WaSP configuration.

Duplex mode

List box {Full duplex; Half duplex}, default = “Full duplex“

Mode of DF1 protocol operation: Only Full duplex mode is implemented now.

DF1 advanced parameters

Protocol DF1 supports protocol local acknowledgment. Typically the default setting shall be used. In case a need it is possible to change ACK parameters in ADVANCED > Generic > com_x_prot/Protocol_DF1 menu.

ACK locally

List box {On; Off}, default = ”On”

Allows to switch On / Of the local ACK

Repeats

Number {0 – 31}, default = 2

Sets number of repeats when local ACK is nor received.

ACK timeout [ms]

Number {0 – 1683}, default = 1000

Timeout of waiting for ACK.

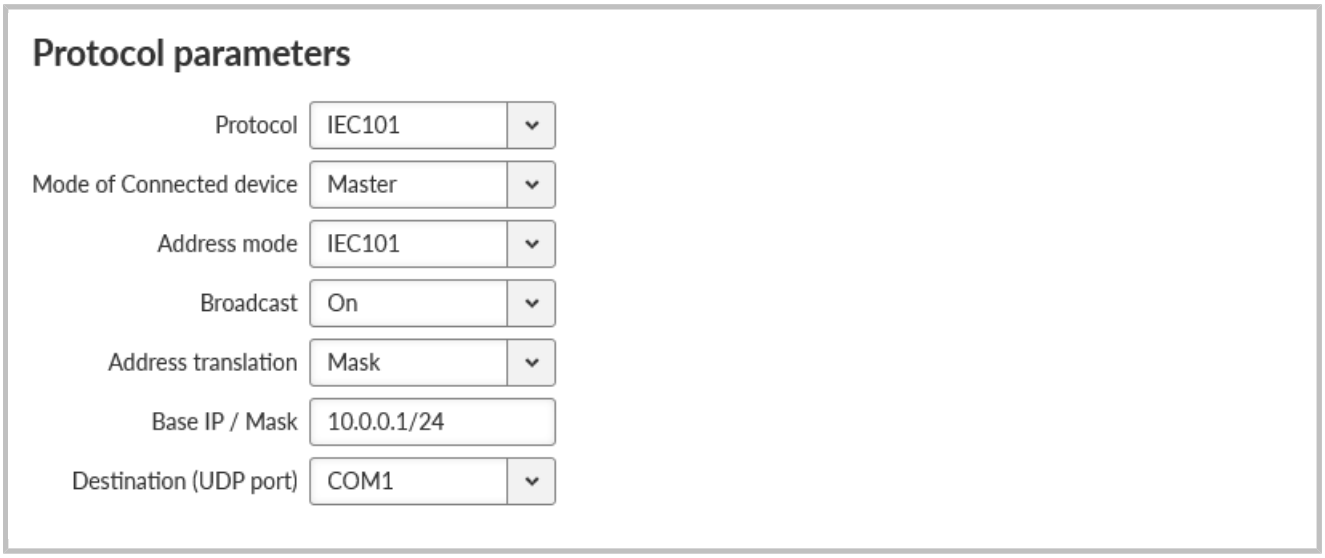
Block control mode

List box {BCC; CRC}, default = "BCC"

According to the DF1 specification, either BCC or CRC for Block control mode (data integrity) can be used.

Note
According to the DF1 specification, packets for the destination address 0xFF are considered broadcasts. Hence when Broadcast is On, packets with this destination are handled as broadcasts.

4.1.3.3.7. IEC101



Mode of Connected device
List box {Master; Slave; Combined}, default = “Master”

Note
For connected SCADA Master set Master, for connected SCADA Slave set Slave.

Address mode
List box {IEC101; 2B ADDR; TELEGYR; SINAUT; No addr}, default = “IEC101”

Broadcast
List box {On; Off}, default = "On"

4.1.3.3.8. Mars-A

MARS-A is a full duplex protocol featuring:

- 32bit long addresses
- error detection (based on 16 bit checksum (XOR) or 16 bit CRC)
- error correction

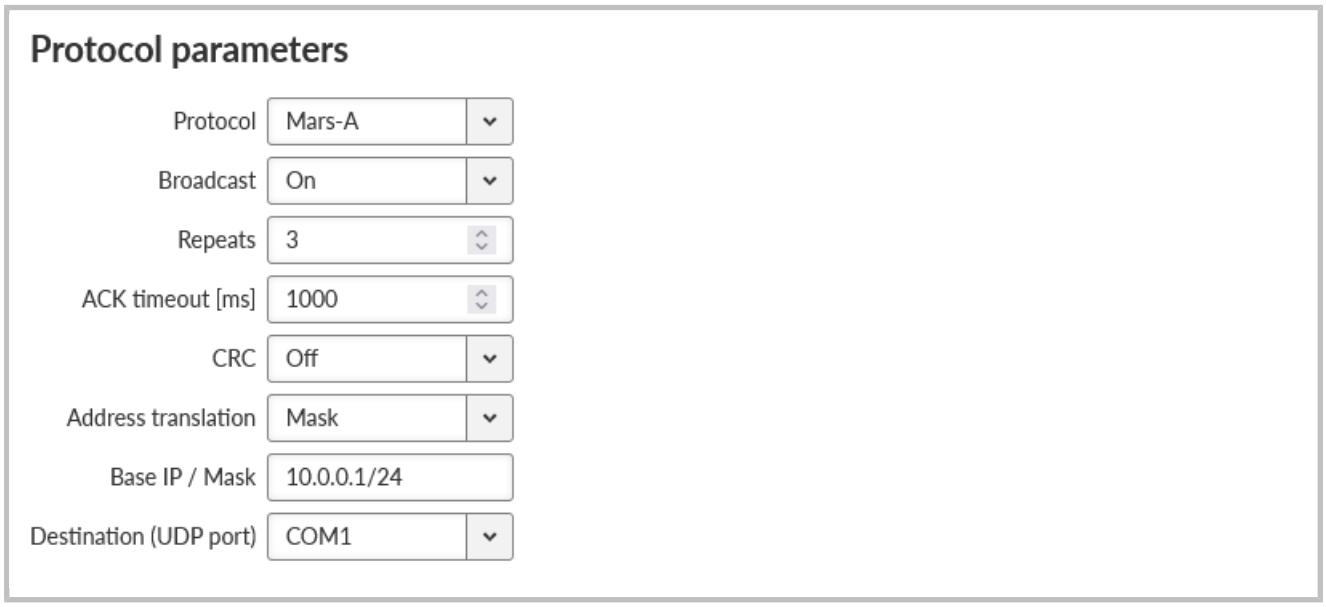
MARS-A was widely used by legacy RACOM radio modems in the MORSE system from the year 1999.

The new implementation of this protocol in WaSP or WaSP is limited to the parts of the complex protocol which can be used together with modern packet type of these routers:

USER DATA (0x09) from router to the serial interface (e.g. to RTU),

USER DATA (0x09) and PROT DATA (0x0A) from serial interface (e.g. from RTU) to the router.

Mars-A headers are removed from the packet prior to transmitting to the network - only data are transmitted.



ACK timeout [ms]
Number {0 – 16383}, default = 1000
Serial interface acknowledge timeout.

Repeats
Number {0 – 31}, default = 3
Number of repeats. Repetition is triggered when NAK frame is received or if ACK frame was not received within ACK timeout.

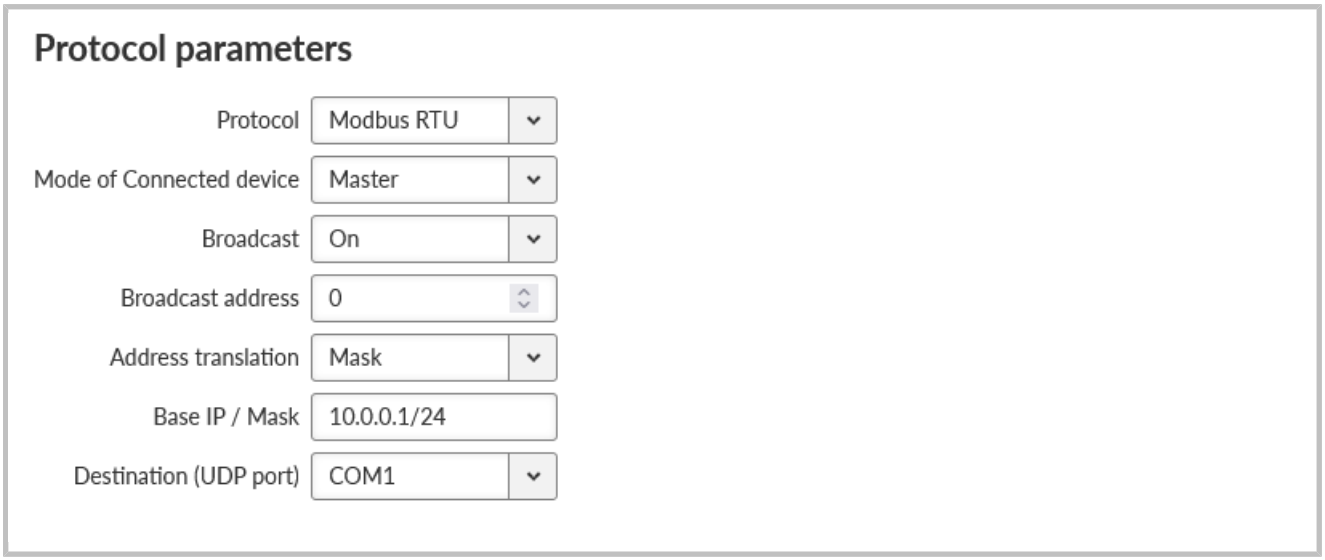
Security bit
List box {On; Off}, default = "Off"
Needed for compatibility with legacy MORSE network implementations. This parameter does not change protocol behavior.

CRC
List box {On; Off}, default = "Off"
Error detection algorithm:
- On - CRC algorithm is used
- Off - XOR algorithm is used

4.1.3.3.9. Modbus RTU

Modbus RTU is a serial polling-type communication protocol used by Master-Slave application.

When WaSP radio network run in Router mode, more Modbus Masters can be used within one Radio network and one Slave can be polled by more Masters.



Mode of Connected device

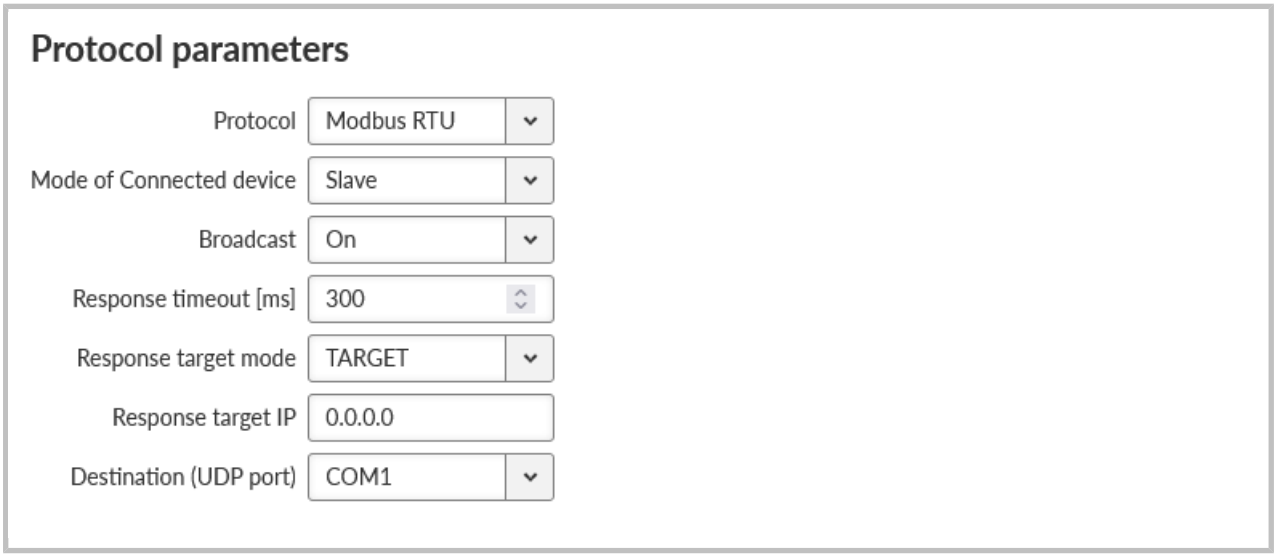
List box {Master; Slave}, default = "Master"

Mode of connected device: MASTER

Broadcast address

It is possible to set address, which will be handled as a broadcast address while Broadcast = "On". Default broadcast address of the Modbus RTU protocol is 0.

Mode of connected device: SLAVE



Response timeout

Number { 0 – 8190}, default = 300

The Response timeout parameter controls how long the unit waits for an acknowledgement frame. The timeout is started when the original frame received from the Radio channel is transmitted to the connected device (over the serial channel). Transmission of any other frame to the connected device is temporarily blocked, whilst Response timeout is active. Response timeout = 0 disables this feature.

4.1.3.3.10. PPP protocol

The PPP protocol (Point-to-Point Protocol, specified in RFC 1661) is intended for a direct duplex connection between two network points. It works at the link layer as an extension of the HDLC protocol. Both network points receive a configuration on the basis of which they negotiate connection properties with each other over the serial line. The consequence of a successful negotiation is the creation of network interfaces on both sides. Depending on the selected network protocol, these can be interfaces of different types. In our case, the IPCP protocol (IPV6CP) is used and the resulting interface is of the TUN type (e.g. ppp1). The interface is assigned an IP address according to the configuration and user data are transferred through it. PPP encapsulation is used to encapsulate IP packets into frames transmitted over a serial line (see Frame format, RFC 1662).

4.1.3.3.10.1. Typical course of establishing a connection

Line Parameter Negotiation (LCP)

Basic connection parameters at the serial line level
LCP (Link Control Protocol, RFC 1661)
Negotiated parameters:

- Maximum receive unit (MRU)
- Asynchronous Control Character Map (ACCM)
- Authentication protocol
- Compression of the protocol field in the PPP frame header
- Compression of the address and control fields in the PPP frame header

Authentication

Optional, if negotiated, the appropriate protocol will be used
It can be two-sided, where each side may require a different protocol
Protocols:

- PAP (Password authentication protocol)
- CHAP (Challenge Handshake Authentication Protocol)

Negotiation of data compression parameters (CCP)

Data compression type and parameters
Compression Control Protocol (CCP, RFC 1962)

Network Protocol (NCP) Negotiation

Connection parameters at the network layer level
Network Control Protocol (NCP):

- IPCP (Internet Protocol Control Protocol, RFC 1332)
- IPv6CP (IPv6 Control Protocol, RFC 5072)

4.1.3.3.10.2. Format of frames

The format of PPP frames (RFC 1661, RFC 1662) is based on the HDLC protocol standard.

4.1.3.3.10.3. Common frame format

Flag	Address	Control	Protocol	Information	Padding	FCS	Flag
0x7E	0xFF	0x03	8/16 bits	*	*	16/32 bits	0x7E

4.1.3.3.10.4. Meaning of individual fields

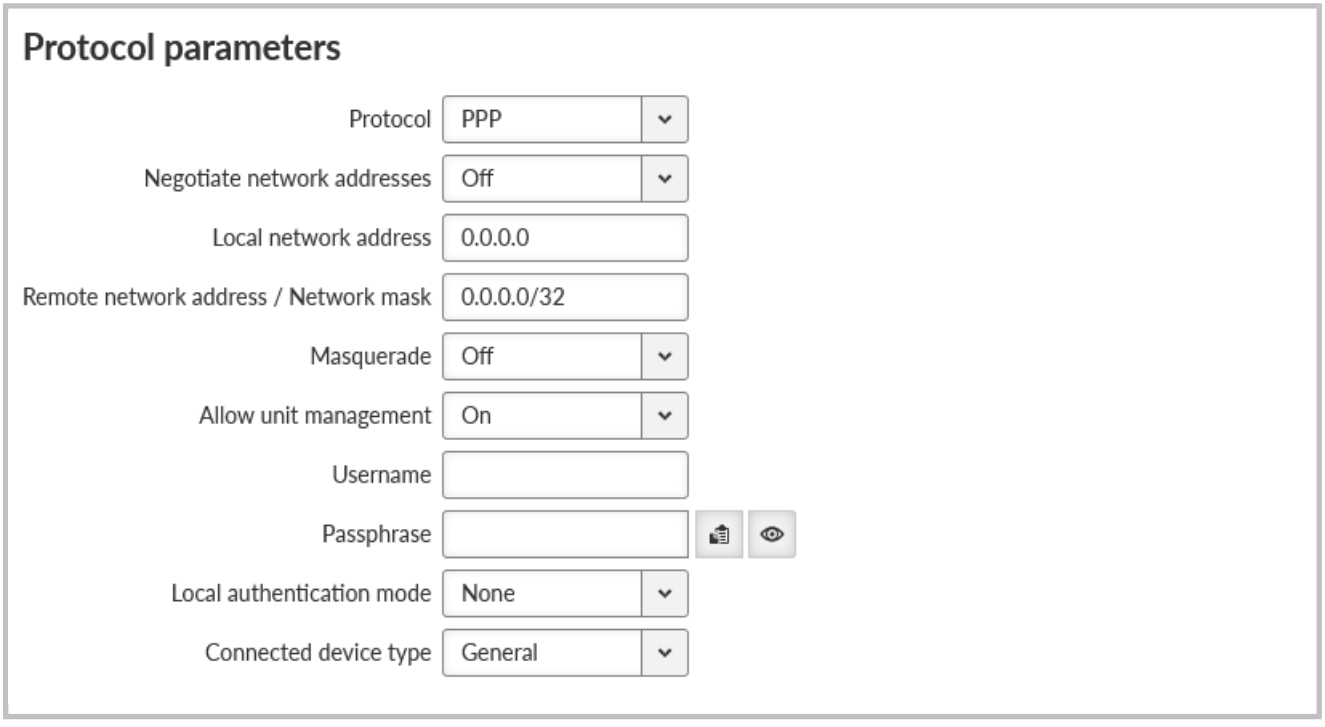
- **Flag**: value 0x7E defined in the protocol specification
- **Address field**: address field, value 0xFF defined in the protocol specification
- **Control field**: control field, value 0x03 defined in the protocol specification
- **Protocol field**: protocol field, indicates the type of data in the Information field
  - Example: 0xC021 for LCP, 0xC023 for PAP
- **Information**: encapsulated data
  - Example: IP packet
- **Padding**
- **Frame Check Sequence (FCS) field**: control sequence for detecting transmission errors

4.1.3.3.10.5. Configuration

Some configuration items are closely related to the native parameters of the pppd daemon. Individual parameters are listed in the text below in bullet points marked "pppd:" and detailed information about them can be found in the daemon's manual pages.

"<NR>" is used to indicate the PPP index (1/2/3).

4.1.3.3.10.6. Protocol parameters



Negotiate network addresses
List box {On; Off}, default = ”Off”
Enables local/remote PPP interface address negotiation.
If disabled Local network address and Remote network address must be set manually.

Local network address
IP address; default = 0.0.0.0
Local IP address of the PPP interface

Remote network address / Network mask

IP address; default = 0.0.0.0/32

Remote IP address and mask of the PPP interface. Address and Mask are used to determine the target range of a rule routing to the PPP interface

Masquerade

List box {On; Off}, default = ”Off”

Enables/disables Source NAT (masquerade) on packets sent over the PPP interface.

With masquerade enabled, packets leaving the station over the PPP interface are rewritten with the source address to the address assigned to that interface

Allow unit management

List box {On; Off}, default = ”On”

Enables unit management access via PPP interface

Username

String {up to 50 char}, default = <empty>

The username to use when authenticating to the counterparty, regardless of the protocol that is required.

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Passphrase

String {up to 50 char}, default = <empty>

The passphrase to use when authenticating to the counterparty, regardless of the protocol that is required.

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Local authentication mode

Selection of the protocol with which the counterparty is to be authenticated when establishing a connection.

For PAP (legacy) and CHAP options, the credentials set by **Local authentication username** and **Local authentication password** are used

Local authentication username

String {up to 50 char}, default = <empty>

The username that the counterparty should use during authentication (see **Local authentication mode**).

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Local authentication password

String {up to 50 char}, default = <empty>

The password that the counterparty should use during authentication (see **Local authentication mode**).

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Connected device type

List box {General; TETRA terminal (Motorola MTM5x00)}, default = ”General”

Connected device type. Sets the corresponding command sequence to switch the connected device to PPP mode.

Negotiate network addresses must be enabled for TETRA.

Advanced menu parameters:

Asynchronous control character map
Number {0 – 65535}, default = 0
Async-Control-Character-Map (ACCM) settings.
A non-zero value can be used to select control characters that the counterparty should not include in sent PPP packets.

LCP keepalive failure count
Number {0 – 255}, default = 0
A non-zero value means the maximum number of sent LCP echo-request messages before the peer is marked as disconnected and the connection is closed (see **LCP keepalive interval** [s]).
A zero value disables the function.

LCP keepalive interval [s]
Number {0 – 255}, default = 10
Interval of sending LCP echo-request messages, to which the counterparty responds with an LCP echo-reply message in normal state.
Along with that entry **LCP keepalive failure count** can be used to detect if a party is connected
Active if **LCP keepalive failure count** is greater than 0

Idle timeout to reconnect [s]
Number {0 – 65535}, default = 0
Disconnects an inactive connection after a defined period of time

Enable using modem control lines
List box {On; Off}, default = ”Off”
Option to use "modem control lines" (DTR/DSR serial port signals).

Enable control messages logging
List box {On; Off}, default = ”Off”
Option to verbose pppd daemon control messages.
Messages are written to the standard log /var/log/pppd_<NR>/log, which is available in a Diagnostic package.

Compression negotiation mode
List box {Automatic; Manual}, default = ”Automatic”
Mode for selecting configuration parameters related to compression (all remaining items below). When Automatic is selected, the configuration items below are ignored and the pppd daemon uses its default values. When Manual is selected, the configuration items below are active and their values are used by the pppd daemon when negotiating with the counterparty.

Enable address and control field compression
List box {On; Off}, default = ”On”
Choice of whether to negotiate address and control field compression in the PPP frame header (Address/Control field compression, see Frame format), in both directions of data transfer.
Active if **Compression negotiation mode** is Manual.

Enable protocol field compression
List box {On; Off}, default = ”On”
Choice of whether to negotiate protocol field compression in the PPP frame header (Protocol field compression, see Frame format), in both directions of data transfer.
Active if **Compression negotiation mode** is Manual.

Van Jacobson IP header compression max slots
Number {0; 2 – 16}, default = 16

Option of Van Jacobson compression of IP headers.
A non-zero value is a parameter of the compression algorithm (number of connection slots).
A zero value disables the function.
Active if **Compression negotiation mode** is Manual.

Enable compression control protocol
List box {On; Off}, default = ”On”
Option to use CCP (Compression Control Protocol) to negotiate data compression parameters.
The option to disable CCP is provided for compatibility with legacy PPP clients that do not support data compression.
Active if **Compression negotiation mode** is Manual.

BSD data compression receive code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "BSD-Compress" algorithm for data compression in the incoming direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

BSD data compression transmit code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "BSD-Compress" algorithm for data compression in the outgoing direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

Deflate data compression receive code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "Deflate" algorithm for data compression in the incoming direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

Deflate data compression transmit code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "Deflate" algorithm for data compression in the outgoing direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

4.1.3.3.10.7. Routing

Routing Mode
The listbox is extended with PPP <NR> options
If the routing rule has one of the PPP <NR> options selected, routing is done to the appropriate PPP interface.

Routing Persistent
List box {On; Off}, default = ”Off”

The routing rule is persistent (see Cellular configuration for detailed explanation).

4.1.3.3.10.8. Protocol status

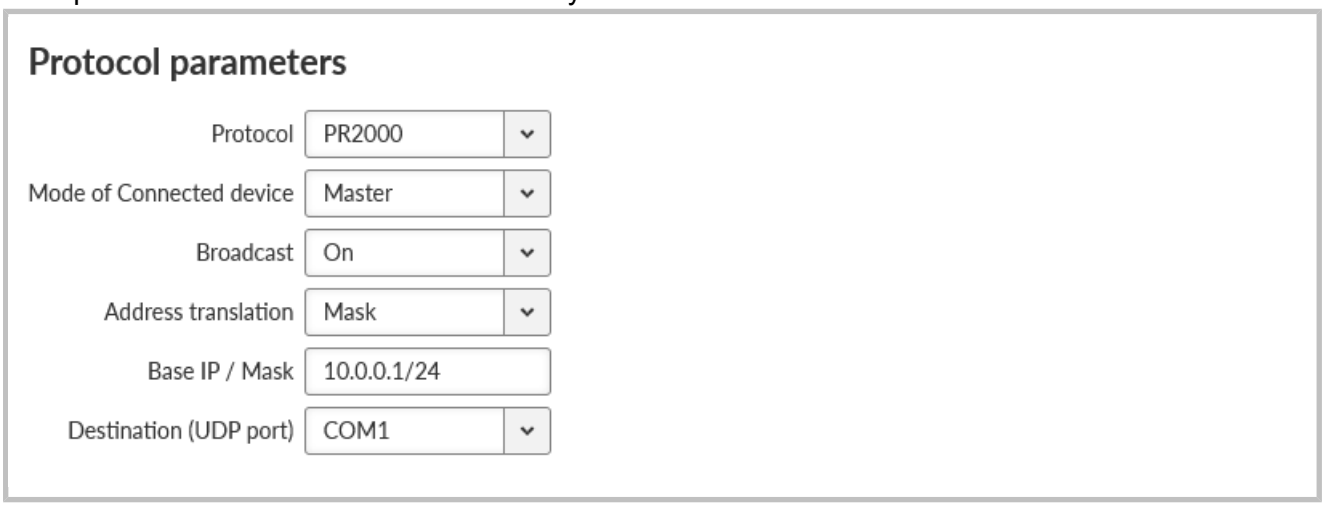
PPP status information is available in the Diagnostics > Information > Interfaces > PPP menu. Status provides following information

- Interface
  - PPP Interface name.
- State
  - Current state of the PPP interface daemon.
- Peer MRU
  - Maximum receive unit (MRU) in bytes requested during negotiation by the counterparty.
- Peer Auth. mode
  - Authentication protocol requested by counterparty.
- Peer ACCM
  - ACCM setting requested by counterparty.
- Negotiated compression options
  - Negotiated options of PPP compression.

4.1.3.3.11. PR2000

PR2000 is an abbreviation for the PROTEUS 2000 SCADA protocol. This protocol is used in Master-Slave applications.

The PR2000 protocol is implemented in a fully transparent manner. The original protocol frames are transported over the network in their entirety.



4.1.3.3.12. Siemens 3964(R)

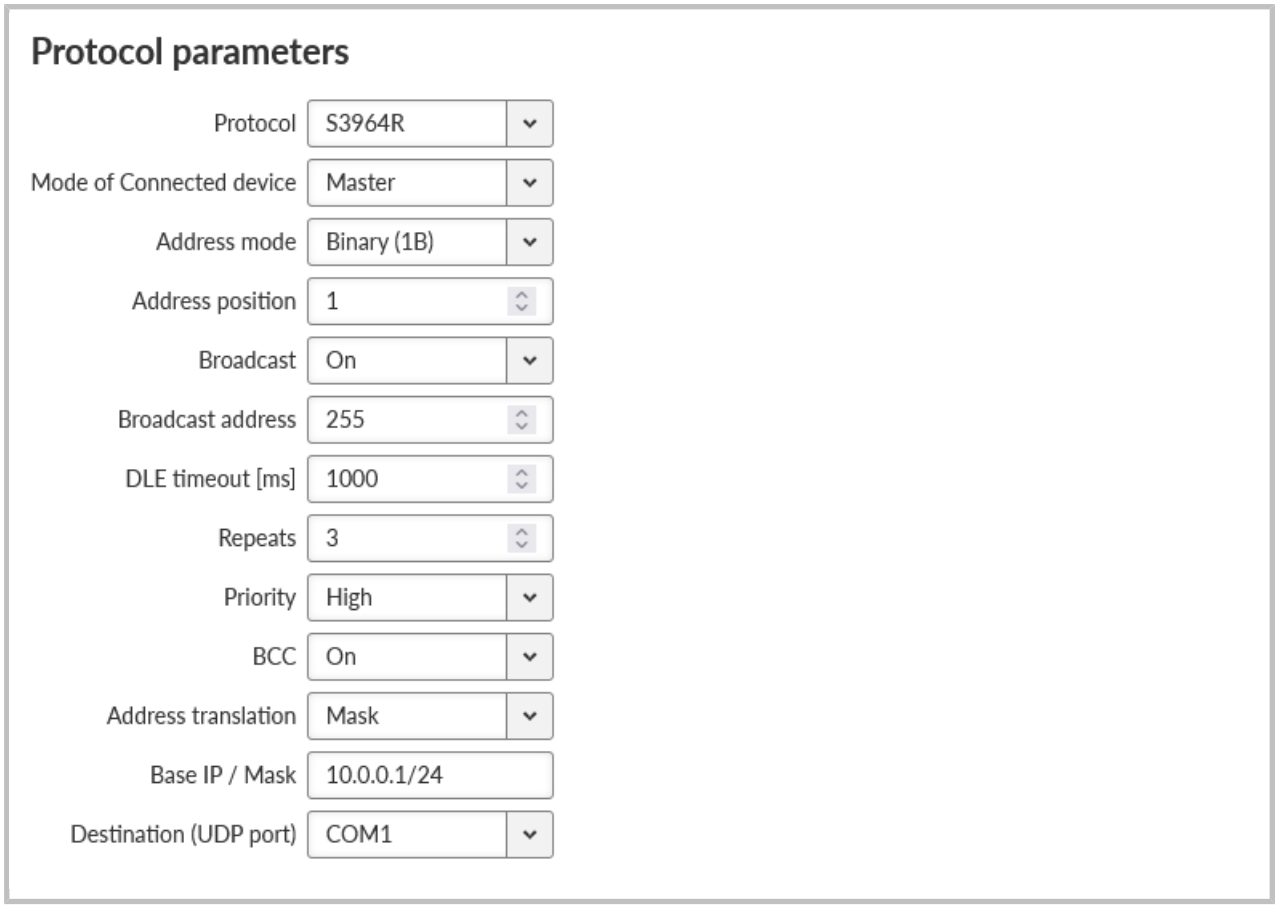
The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has developed into an industry standard that can be found on many devices as a universal communications interface. 3964R is the same as 3964, in addition it only uses BCC (Block Check Character). 3964(R) handles only the link layer (L2 in OSI model), hence WaSP uses a similar way to read “SCADA address” as in UNI protocol.

There is a handshake STX(0x02) – DLE(Ox10) on the start of communication and DLE+ETX – DLE on the end. This handshake is performed by WaSP locally, it is not transferred over the WaSP network.

Communication goes as follows:
LocalRTU −> STX −> Local WaSP
LocalWaSP −> DLE −> LocalRTU
LocalRTU −> DATA+DLE+ETX+BCC −> Local WaSP
LocalWaSP −> DATA −> Remote WaSP*
Local WaSP −> DLE −> LocalRTU
Remote WaSP −> STX −> RemoteRTU
RemoteRTU −> DLE −> Remote WaSP
Remote WaSP −> DATA+DLE+ETX+BCC −> RemoteRTU
RemoteRTU −> DLE −> RemoteWaSP

* only this packet is transferred over the WaSP network, all the other ones are handled locally.

Master



Address mode

List box {Binary (1 B); Binary (2B LSB first); Binary (2B MSB first)}, default = "Binary (1 B)"

WaSP reads the Protocol address in the format and length set (in Bytes).

Address position

Specify the sequence number of the byte, where the Protocol address starts.

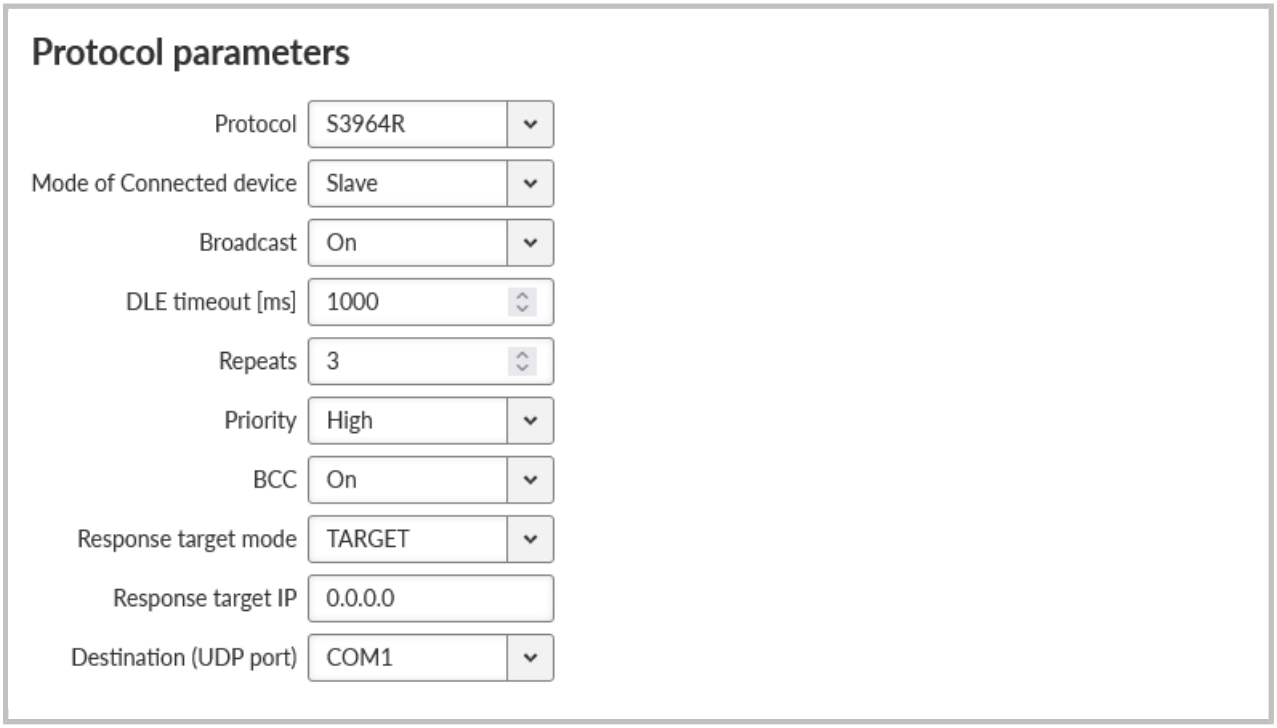
Note

3964(R) protocol is using escape sequence (control sequence) for DLE(0x10). I.e. when 0x10 is in user data, 0x1010 is sent instead. When address position is calculated, the bytes added by escape sequence algorithm are not taken into account.

Note

The first byte in the packet has the sequence number 1, not 0.

Slave



DLE timeout [ms]

Number {300 – 8190}, default = 1000

WaSP expects a response (DLE) from the connected device (RTU) within the set timeout. If it is not received, WaSP repeats the frame according to the “Retries” setting.

Retries [No]

Number {0 – 7}, default = 3

When DLE packet is not received from the connected device (RTU) within the set DLE timeout, WaSP retransmits the frame. The number of possible retries is specified.

Priority

List box {Low; High}, default = "Low"

When the equipment sends STX and receives STX instead of DLE, there is a collision, both equipments want to start communication. In such a case, one unit has to have a priority. If the Priority is High, WaSP waits for DLE. When it is Low, WaSP sends DLE.

Note
Obviously, two pieces of equipment which are communicating together must be set so that one has High priority and the other has Low.

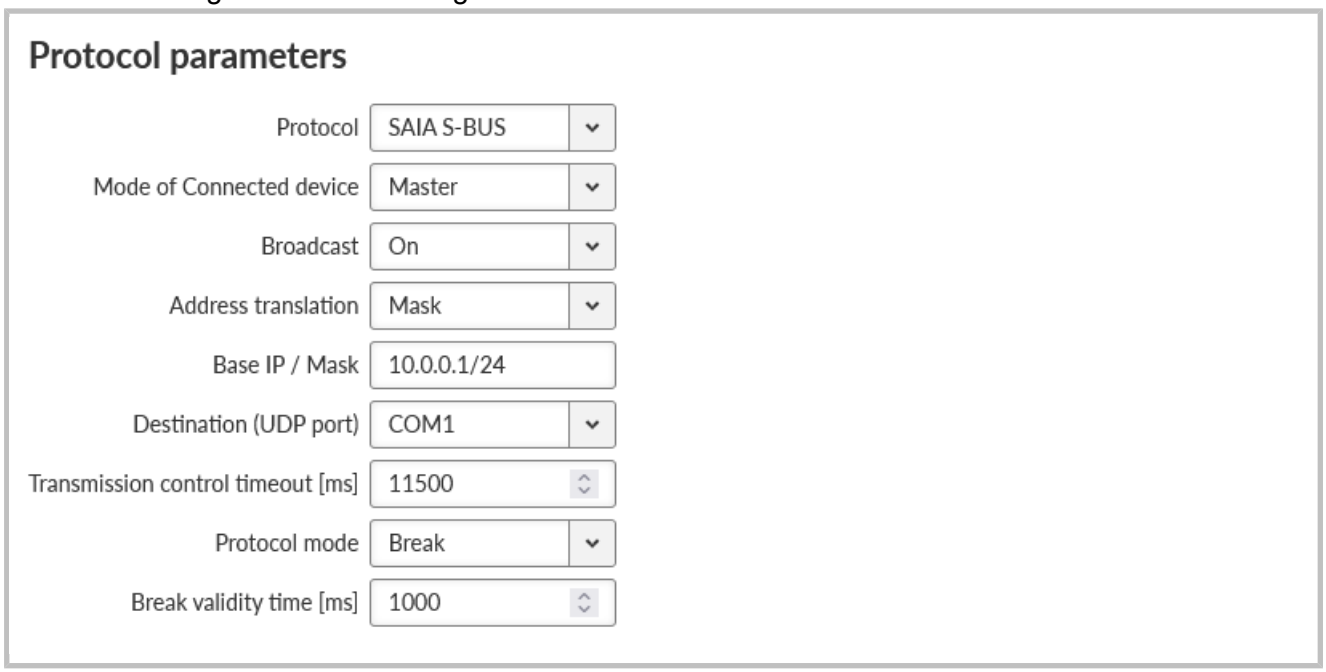
BCC

List box {On; Off}, default = "On"
BCC (Block Check Character) is a control byte used for data integrity control, it makes the reliability higher. BCC is used by 3964R, 3964 does not use it.
WaSP checks (calculates itself) this byte while receiving a packet on COM. WaSP transmits DLE (accepts the frame) only when the check result is OK. BCC byte is not transferred over the WaSP network, it is calculated locally in the end WaSP and appended to the received data.

4.1.3.3.13. SAIA S-Bus

SAIA S-Bus protocol was widely used by legacy RACOM radio modems in the MORSE system. The S-Bus protocol is implemented as an access module for communication with the SAIA PCD device. The protocol is a MASTER/SLAVE type; the MASTER does not have its own address. There can be at most 254 SLAVEs, the address 255 is reserved for broadcast transmitting which is not acknowledged. The physical layer of the S-Bus protocol uses the RS232 or RS485 interface. The data addressed to 255 is processed as broadcast.

Protocol frame has to be as whole received in the one buffer, so the IDLE parameter should be set properly. The S-bus protocol header does not always contain the length of the data, so it is not possible to work with fragmented and defragmented frames.



Mode of connected device

List box {Master; Slave; Slave Plus}, default= “Master”
Master and **Slave** behaves like standard Master or Slave Saia PCD. The **Slave Plus** mode allows to behave in limited way as a Master and sends to other Slave/Slave Plus write command (read command is not allowed).

Broadcast

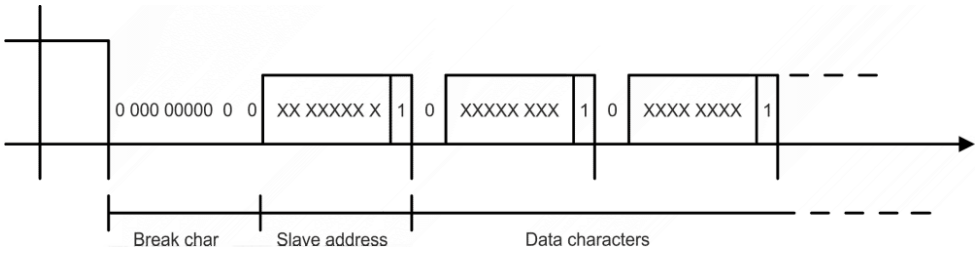
List box {On; Off}, default =”On”
When **On**, the 255 address is treated as a broadcast, When **Off**, the 255 address is ignored.

Protocol mode

List box {Break; Data}, default =”Break”
Break or Data protocol modes can be used.

Break mode (SM0)

The frames are synchronised by the break characters of a configured length which are sent before the addressed command.

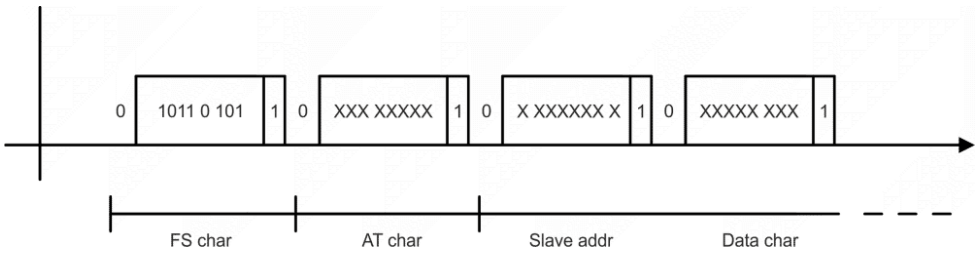


Break mode is available only with COM port, it is not implemented on TS (the break signal is not available there). The Break signal check is very rough (with step of 100 ms) due to Linux kernel limitations.

Data mode (SM2)

Frame synchronization is accomplished by inserting the character 0xB5 in the beginning of frame. If another character 0xB5 should appear in the frame, then it is replaced by the following DLE sequence:

Character	DLE sequence
0x85	0xC500
0xC5	0xC501



Note
See details of the RACOM’s implementation on *https://www.racom.eu/eng/support/prot/sbus/index.html* [2]

Mode of Connected device: MASTER

Transmission control timeout [ms]
Number {0 – 65535}, default = 11500
Master timeout. This timeout is reset after receiving of an answer from Slave or a frame incoming from the connected master.

Mode of Connected device: SLAVE

Response timeout [ms] Number {0 – 16383}, default = 300
Slave’s response timeout - waiting for response, otherwise the reply to master is resent.

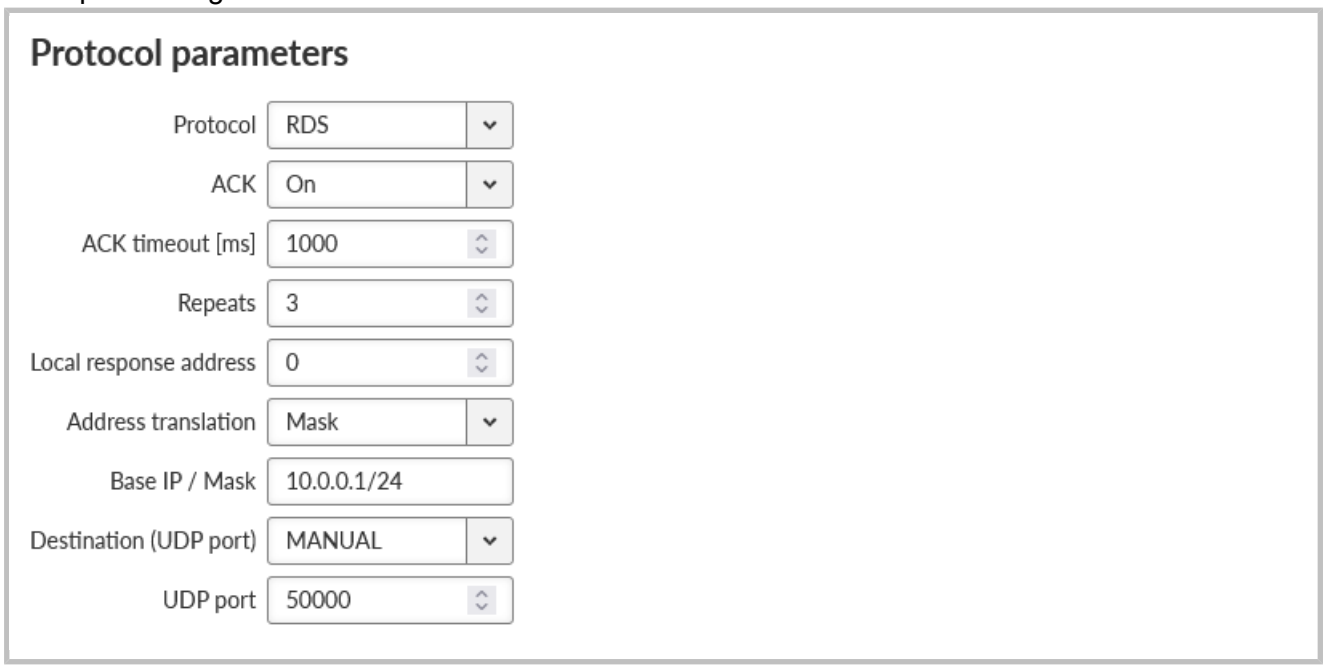
[2] https://www.racom.eu/eng/support/prot/sbus/index.html

Repeats
Number {0 – 7}, default = 3
Number of repeats when the response from master is not received.

Break mode
(additional parameter)
Master, Slave Plus
Break validity time [ms]
Number {0 – 5000}, default = 1000
Slave, Slave Plus
Break length [ms]
Number {0 – 128}, default = 2
Length of break in ms.

4.1.3.3.14. RDS

RDS protocol is a protocol used in MRxx networks. It supports network communication; any node in the network can talk to any other (unlike Master-Slave type of protocols). The RDS protocol is typically used when combining WaSP and MRxx networks or SCADA networks adapted to MRxx networks. Frames are received from the Radio channel and sent to COM1-3 or Terminal server 1-5 according to UDP port settings and vice versa - from wire to Radio channel.



ACK
List box {On; Off}, default = "On"
Frame acknowledgement when transmitted over wire (COM or Ethernet) interface. ACK (0x06) frames are transmitted on successful reception and NAK (0x15) on unsuccessful frame reception.

ACK timeout [ms]
Number {0 – 16383}, default = 1000

Note
ACK timeout is measured from the beginning of the packet transmission.

When "ACK" is enabled, WaSP is waiting "ACK timeout [ms]" after transmitting frame to receive acknowledgement. If the ACK frame isn't received, the frame is re-transmitted. Frame re-transmission happens up to "Repeats" number of times.

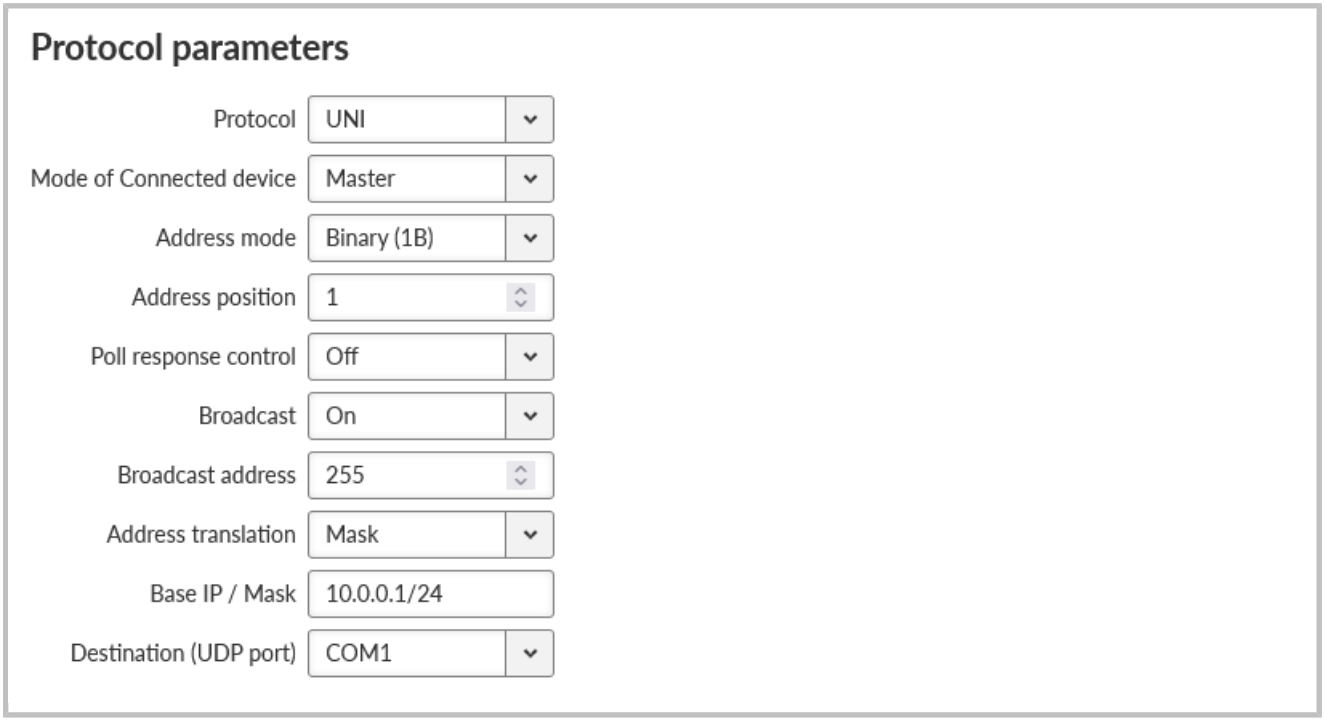
Repeats
Number {0 – 31}, default = 3
Number of frame re-transmissions.

Local response address
Number {0 – 255}, default = 0
This address is used only with status query (0x51). Response of WaSP is "0x54 <Local response address> 0x00".

4.1.3.3.15. UNI

UNI is the 'Universal' protocol utility designed for WaSP. It is supposed to be used when the required application protocol is not available in WaSP and the network communication is using addressed mode (which is a typical scenario). The key prerequisite is: messages generated by the Master application device must always contain the respective Slave address and the address position, relative to the beginning of the message (packet, frame), is always the same (**Address position**). Generally, two communication modes are typical for UNI protocol: In the first one, communication is always initiated by the Master and only one response to a request is supported; in the second mode, Master-Master communication or combination of UNI protocol with ASYNC LINK protocol and spontaneous packets generation on remote sites are possible.

The UNI protocol is fully transparent, i.e. all messages are transported and delivered without any modifications.



Mode of Connected device
List box: {Master, Slave}, default = Master

Adress mode

List box {Binary (1B); ASCII (2B); Binary (2B LSB first); Binary (2B MSB first)}, default = "Binary (1B)"

Protocol address format and length (in Bytes). ASCII 2-Byte format is read as 2-character hexa-decimal representation of one-byte value. E.g. ASCII characters AB are read as 0xAB hex (10101011 binary, 171 decimal) value (the ASCII-2-Byte format function will be available in a future FW release).

Address position

Number {1 – 255}, default = 1

Specify the sequence number of the byte, where the Protocol address starts. Note that the first byte in the packet has the sequence number 1, not 0.

Poll response control

List box {On; Off}, default = "On"

"On" – The Master accepts only one response per a request and it must come from the specific remote to which the request has been sent. All other packets are discarded. This applies to the Master - Slave communication scheme.

Note

It may happen, that a response from a slave (No.1) is delivered after the respective timeout expired and the Master generates the request for the next slave (No.2) in the meantime. In such case the delayed response from No.1 would have been considered as the response from No.2. When Poll response control is On, the delayed response from the slave No.1 is discarded and the Master stays ready for the response from No.2.

"Off" – The Master does not check packets incoming from the RF channel - all packets are passed to the application, including broadcasts. That allows e.g. spontaneous packets to be generated at remote sites. This mode is suitable for Master-Master communication scheme or a combination of the UNI and ASYNC LINK protocols.

Mode of Connected device: SLAVE

Accept broadcasts

List box {On; Off}, default = "On"

"On" – Broadcast packets received at the radio channel are forwarded to the COM port.

"Off" – Broadcast packets (received at the radio channel) are discarded. Unicast packets are forwarded to the COM port.

4.1.4. Terminal servers

Generally, a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to a WaSP over the local area network (LAN). It is a virtual substitute for devices used as serial-to-TCP (UDP) converters.

In some special cases, the Terminal server can be also used for reducing the network load from applications using TCP. A TCP session can be terminated locally at the Terminal server in WaSP, user data extracted from TCP messages and processed like it comes from a COM port. When data reaches the destination WaSP, it can be transferred to the RTU either via a serial interface or via TCP (UDP), using the Terminal server again.

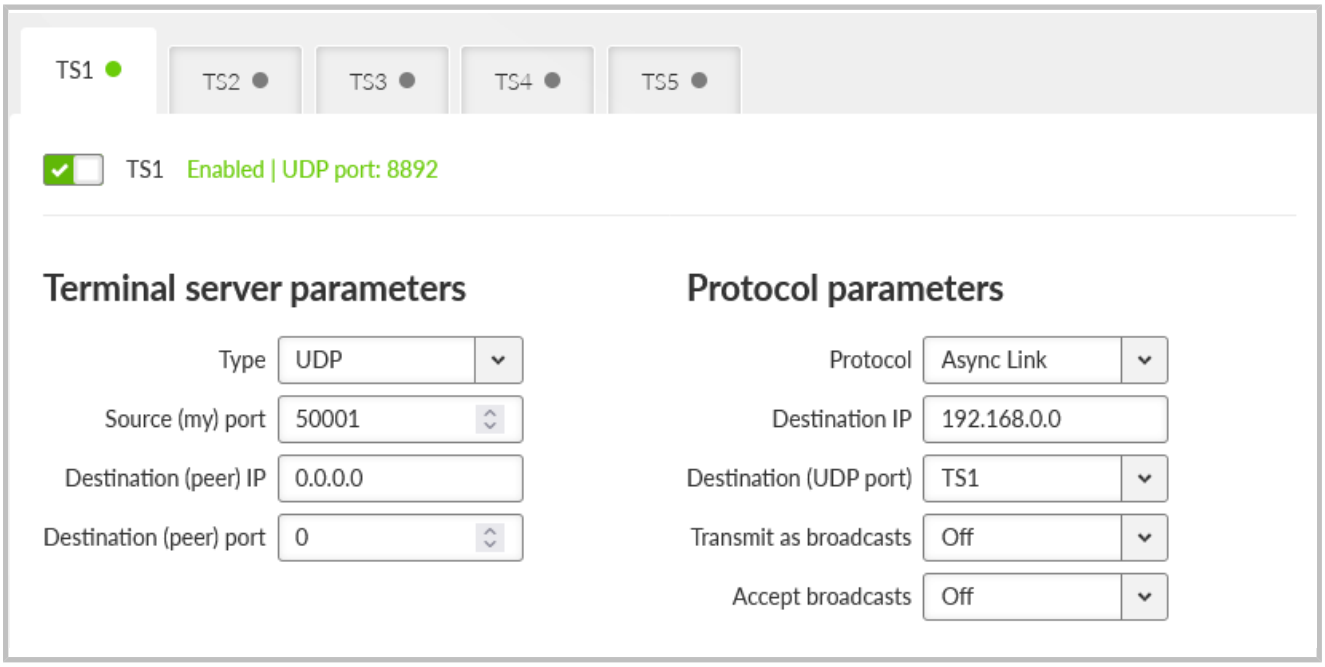


Fig. 4.6: SETTINGS > Interfaces > Terminal servers

Up to 5 independent Terminal servers can be set up. Each one can be either TCP or UDP Type, **TCP Inactivity** is the timeout in seconds for which the TCP socket in WaSP is kept active after the last data reception or transmission. As source IP address of a Terminal server will be used the IP address of the WaSP ETH interface (**Local preferred source address** if exists see *Section 4.2.1, " Static"*), **Source (my) port** can be set as required. **Destination (peer) IP** and **Destination (peer) port** values belong to the locally connected application (e.g. a virtual serial interface). In some cases, applications dynamically change the IP port with each datagram. In such a case set Destination port=0. WaSP will then send replies to the port from which the last response was received. This feature allows to extend the number of simultaneously opened TCP connections between a WaSP and locally connected application to any value up to 10 on each Terminal server. **Protocol** follows the same principles as a protocol on COM interface.

For details of settings see *Section 4.1.3.2, "Common Protocol parameters"*.

Note

Max. user data length in a single datagram processed by the Terminal server is 8192 bytes.

Note

The port range 0-1023 is reserved and prohibited for Terminal Server. Port 502 is an exception for ModbusTCP.

4.1.5. PPPoE client

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol that encapsulates PPP frames within Ethernet frames. The PPP protocol itself is already described among *serial protocols*. With PPPoE, we distinguish between two basic phases: "Discovery" and "PPP Session".

Discovery phase

The primary goal of the PPPoE Discovery Phase is to acquire essential information for establishing the PPP Session Phase. This information includes the MAC address of the peer device and the PPPoE session ID.

PPP Session phase

The primary goal of the PPP Session Phase is to establish and maintain a connection between the client and the server. This phase utilizes standard PPP frames for data exchange. All frames within this phase carry an ETHER_TYPE value of 0x8864 and are considered Ethernet unicasts.

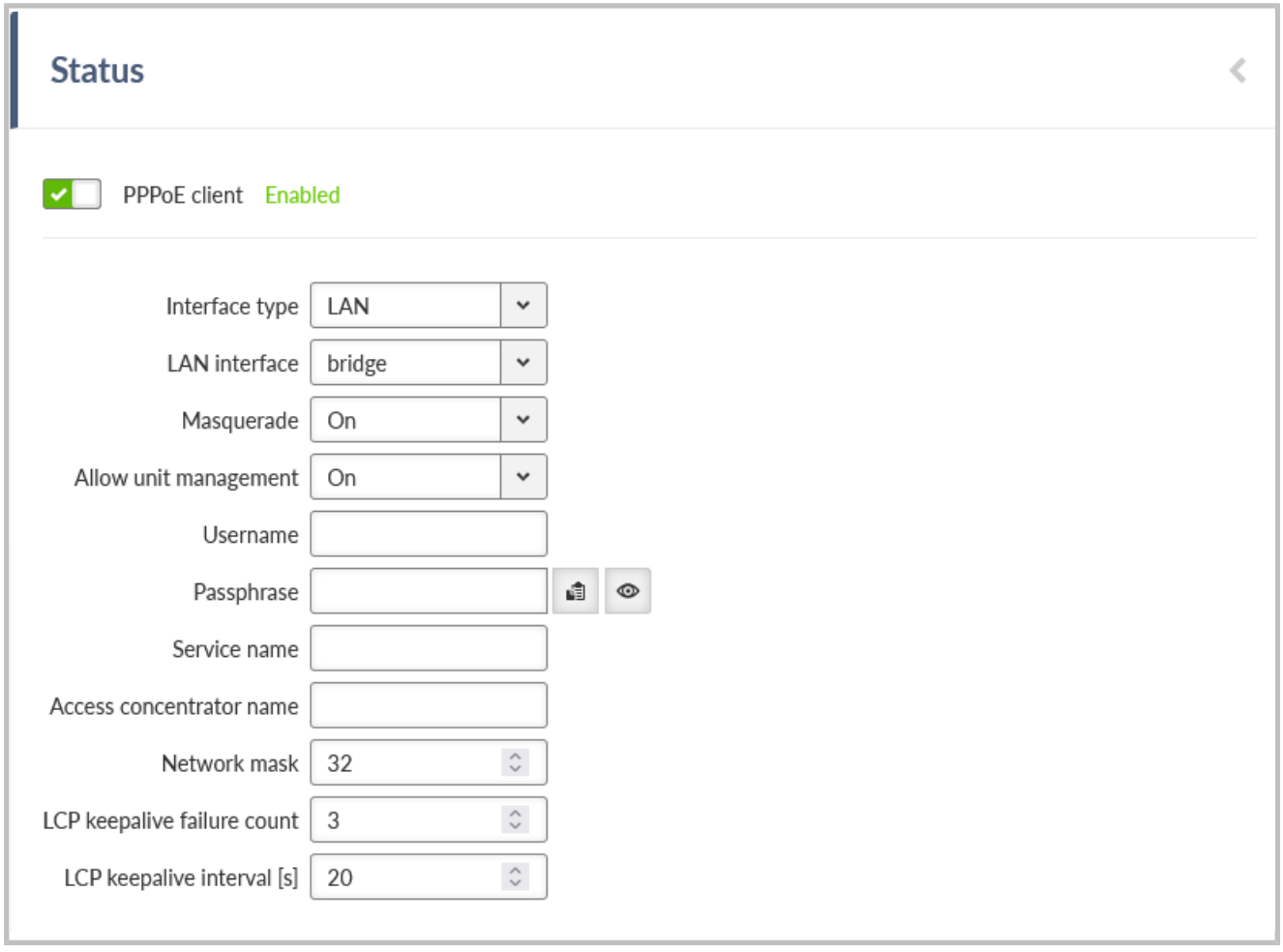


Fig. 4.7: SETTINGS > Interfaces > PPPoE client

Interface type

List box {LAN; VLAN}, default = "LAN"

This parameter specifies from which table the interface will be selected using a name.

- LAN - The name of the LAN interface to be used for PPPoE connection establishment.
- VLAN - The name of the VLAN interface to be used for PPPoE connection establishment.

Masquarade
List box {On; Off}, default = "On"
Enables/disables SNAT (masquerade) on packets sent over the PPP interface.
With masquerade, outgoing packets from the station over the PPP interface have their source address rewritten to the address assigned to this interface. Returning packets are then correctly routed back through the station.

Allow unit management
List box {On; Off}, default = "On"
Allows to manage the unit over PPP interface.

Username
String {up to 64 characters}, default = <empty>
The username to be used for authentication with the peer, regardless of the protocol required.

Passphrase
String {up to 64 characters}, default = <empty>
The passphrase to be used for authentication with the peer, regardless of the protocol required.

Service name
String {up to 64 characters}, default = <empty>
The service name to be used when searching for the server to connect to.

Access concentrator name
String {up to 64 characters}, default = <empty>
The name of the server to connect to.

Network mask
Number {0 – 32}, default = 0
Used together with the peer's IP address to determine the destination range of the routing rule pointing to the PPP interface.

LCP keepalive failure count
Number {0 – 255}, default = 3 (disabled if 0)
A non-zero value specifies the maximum number of LCP request messages sent before the peer is considered disconnected and the connection is terminated.

LCP keepalive interval
Number {0 – 255}, default = 10
The interval for sending LCP request messages, to which the peer normally responds with an LCP reply message.
This parameter can be used in conjunction with LCP keepalive failure count to detect whether the peer is connected.
This parameter is active only when LCP keepalive failure count is greater than 0.

4.2. Routing

WaSP router supports both static and dynamic IP routing.

Static routing is based on fixed – static – definition of routing tables. Dynamic routing is based on automatic creating and updating of routing tables. Various methods and protocols are used for this purpose. Babel, OSPF and BGP standard routing protocols are available in WaSP networks.

Link management option was added allowing to set the switchover of the main link (in the event of its failure) to an existing backup link by automatic changes of routing rules.

Note

Due to static internal routing to clients, OpenVPN L3 is incompatible with dynamic routing protocols. Dynamic routing over the OpenVPN L3 interface will not function.

4.2.1. Static

WaSP works as a standard IP router with multiple independent interfaces: Radio interface, Network interfaces (bridging physical Ethernet interfaces), COM ports, Terminal servers, optional Cellular interface etc. Each of the interfaces has its own IP addresses and Masks. All IP packets are processed according to the Routing table.

Unlimited number of subnets can be defined on the Network interface. They are routed independently.

The COM ports are treated in the standard way as router devices, messages can be delivered to them as UDP datagrams to selected UDP port numbers. Destination IP address of COM port is either IP of a Network interface (bridging Ethernet interfaces) or IP of Radio interface. The IP address source of outgoing packets from COM ports is equal to IP address of interface (either Radio or Network interface) through which packet has been sent. The source address can also be assigned to **Local preferred source address** value - see description below. Outgoing interface is determined in Routing table according to the destination IP.

The IP addressing scheme can be chosen arbitrarily, only 127.0.0.0/8 and 192.0.2.233/30 and 192.0.2.228/30 restriction applies. It may happen that also the subsequent addresses from the 192.0.2.0/24 subnet according to RFC5737 may be reserved for internal usage in the future.

Fig. 4.8: SETTINGS > Routing > Static

Active
{On / Off}
Switches the rule on / off.

Destination IP / mask
IP address, default = 0.0.0.0/0
Each IP packet, received by WaSP through any interface (Radio, ETH, COM, ...), has got a destination IP address. WaSP (router) forwards the received packet either directly to the destination IP

address or to the respective Gateway, according to the Routing table. Any Gateway has to be within the network defined by IP and Mask of one of the interfaces, otherwise the packet is discarded. Each item in the routing table defines a Gateway (the route, the next hop) for the network (group of addresses) defined by Destination IP and Mask. When the Gateway for the respective destination IP address is not found in the Routing table, the packet is forwarded to the Default gateway, when Default gateway (0.0.0.0/0) is not defined, the packet is discarded.
The network (Destination IP and Mask) is written in CIDR format, e.g. 10.11.12.0/24.

Note
Network defined by the same combination of Destination IP and Mask cannot be used for two different rules.

Mode
List box {Static; PPP1; PPP2; PPP3; Link manager; PPPoE Client}, default = Static

- Static - Used for static IP routing rules. If the next hop on the specific route is over the radio channel, the Radio IP is used as a **Gateway**. If Base driven protocol is used and the destination Remote is behind a Repeater, the destination Remote Radio IP is used as a Gateway (not the Repeater address).

- PPP1; PPP2; PPP3 - Routing rule to the PPP interface associated with the COM protocol. The interface may have a dynamically assigned address. Can only be set if the corresponding COM port is enabled and with the PPP protocol.

- Link manager - Routing rule via active link selected by the Link manager. The rule will be dynamically switched in case of a link change or loss. It can be set if the Link manager is enabled.

- PPPoE Client - Routing rule to the PPP interface created by the PPPoE client. The interface has a dynamically assigned address. It can only be set if the PPPoE client is active.

Local preferred source address
IP address, default = 0.0.0.0
Local IP address used as a source address for packets originating in the local WaSP unit being routed by this routing rule. It might be for example packets originating from the COM port or from the Terminal Server. If the address is set to 0.0.0.0 it is not considered active. The IP address has to belong to some of the following interfaces: Radio interface, Network interfaces.

Metric
Number {0 – 4294967294}, default = 0
Routing rule metric value.

Note
You may add a name to each route with your comments up to 16 characters (UTF8 is supported) for your convenience.

Persistent route
List box {On; Off}, default = Off
Sets the persistence (time of presence) of dynamic routing rule.
This parameter is available only if parameter **Mode** is set to "WWAN (EXT)".

- On - Routing rule is always present. When the WWAN interface is closed, it reports "unreachable" messages (via ICMP) and the traffic cannot be caught by a different rule.

- Off - Routing rule exists only if the WWAN interface is open. If it is closed, the traffic can be caught by a different rule.

4.2.1.1. Loopback addresses

Table of loopback addresses contains IP addresses of WaSP, which are set on the loopback interface as "support" addresses independent on specific interface. Maximum number of addresses is 256. Loopback addresses can be useful e.g. for specific routing purposes or specific user data traffic. For example using different routing rules for different traffic.

Fig. 4.9: ADVANCED > Interfaces > Loopback

Enable address
List box {On; Off}, default = "On"

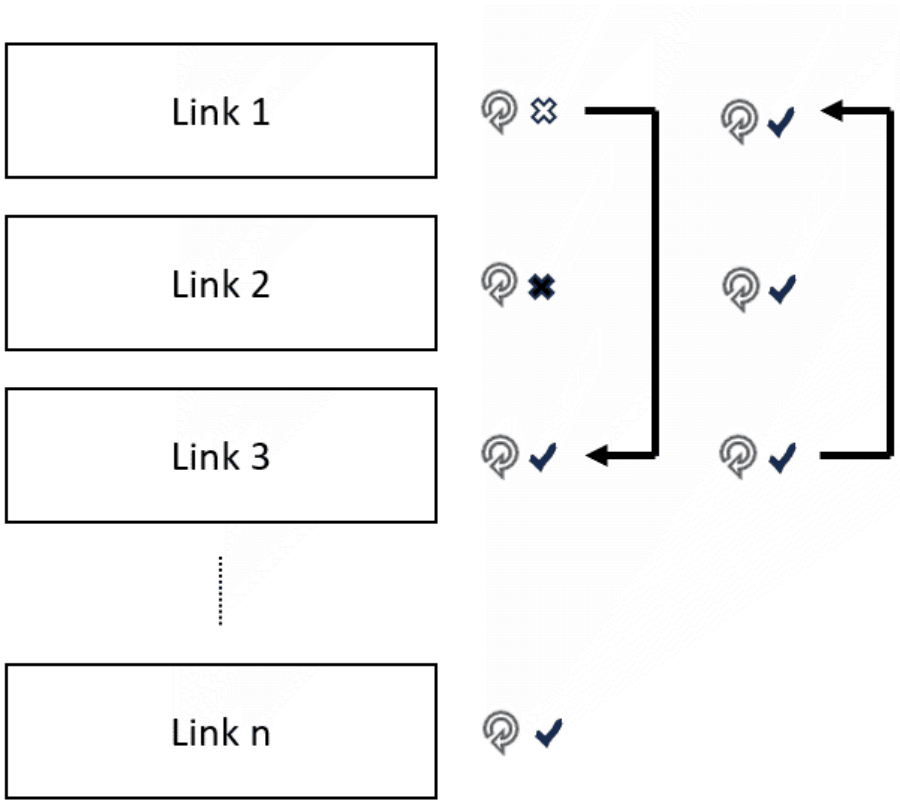
Note
Optional comment.

IP
IP address, default = 0.0.0.0
Defines the IP address which will be set on the loop-back interface. The mask is automatically /32.

4.2.2. Link management

Link manager is a mechanism providing switching of several pre-configured alternative links (alternative routes). Link switch is triggered in case of the active link failure. Link failure can be detected passively – by checking link interface status (see **Watched interface** parameter) and actively by ICMP ping (see **Link testing** parameter).

Link testing is active on currently active link and all higher priority links (to detect when they are available again). Lower priority links can also be tested (see **Test backup link** parameter). When the current link fails, link manager switches to the next functional lower priority link. If the link is not being checked (Test backup link parameter is disabled), it is assumed to be functional. Routing rules are updated automatically on link switchover.



4.2.2.1. Parameters

Fig. 4.10: SETTINGS > Routing > Link management

Enable Link manager
Enables/disables the Link manager

IPsec control
List box {Off; On}, default = “Off”

Enables / disables binding between a link and particular IPsec tunnel. This option is available only when IPsec is enabled and configured. Configuration parameter: SETTINGS > VPN > IPsec > IPsec associations > **Management mode** provides two options:

Link manager (Master)
One of the IPsec associations is declared as **Master**. Traffic selectors (CHILD SA) define the traffic to be encrypted.

Link manager (Slave)
All other associations are declared as **Slave**. No Traffic selectors are defined for such a tunnel. The Master's traffic selectors are used.

4.2.2.2. Links

Every alternative link is configured separately. The priority of individual links is determined by their order. Maximal number of links is 16.

Possible link states:
- **down**: link is not present
- **untested**: link is present, no Link test result is available yet
- **up**: link is present and functional. Should the Link test be activated, the test result is successful
- **test failed**: link is present, the Link test failed

Possible link roles:
- **active**: link is selected as the active one. Only one of the links can be active
- **backup**: link has a lower priority compared to the active link
- **rejected**: link has a higher priority compared to the active link, but can not be used

Enable link
Enables / disables individual link

Label
String {a..z A..Z 0..9 @ _ -}, max 42 char, default = "LINK"
Name of the link that's used in the Status info and System logs

Link type
List box {Static}, default = "Static"

- Static – LAN, GRE or radio interfaces
  Gateway needs to be configured. Watched interfaces can be selected.

Gateway
IP address, default = 0.0.0.0
Next-hop (gateway) address for the Static type of the link

Watched interface (ETH1 .. ETH2, Radio)
Enables / Disables checking of individual interface.
When all checked interfaces are down, the link state is **down**
ETHx Link status is checked for ETH1-ETH2 options. Successful establishment of Radio interface is checked for the Radio option

IPsec association
List box {list of available Peer IDs}, default = first Peer ID

When **IPsec control** is On, the individual link is paired with an individual IPsec tunnel defined by its **Peer ID**. In such a case the individual IPsec tunnel is activated/deactivated together with the respective link. It is automatically switched back to the higher priority link once it is restored..

Link testing
List box {Off; On}, default = “Off”
Enables active link testing. Links are tested using ICMP echo packets

Test period [s]
Number {3 – 3600}, default = 60
Testing period of a link that is in the **up** state

Repeat period [s]
Number {3 – 3600}, default = 10
Testing period of a link that has to be tested (above the active link) and it is normally not tested or the test failed

Reply timeout [s]
Number {1 – 60}, default = 5
ICMP ping reply timeout

Passes [No]
Number {1 – 20}, default = 1
Uninterrupted number of successful tests (pings) after which the link status is up

Retries [No]
Number {1 – 20}, default = 3
Uninterrupted number of failed tests (pings) after which the link status is **test failed**

Target address
IP address, default = 0.0.0.0
Primary tested IP address

Enable second target address
List box {Off; On}, default = "Off"
Enables / Disables testing of the second IP address

Second target address
IP address, default = 0.0.0.0
Secondary tested IP address.

Test mode
List box {One address succeeds; Both addresses succeed}, default = "One address succeeds"

- One address succeeds - only one address is enough to pass the test
- Both addresses succeed - both addresses must pass the test

Test backup link
List box {Off; On}, default = "Off"
Enables active link testing of a link having lower priority compared to **active** link

Note
String {0–42 char}, default = <empty>

NOTE: Link manager is not a full featured dynamic routing protocol (as Babel, OSPF or BGP). Dynamic routing protocols provide synchronization of alternative packet routes across the whole network. Link manager works locally – there is no synchronization of the selected link (route) with other units across the network. Keep in mind this fact when planning Link manager configuration across your network and preserve symmetrical behaviour. One effect of the fact that each Link manager instance in the network operates independently is the occasional asymmetric traffic when switching alternate routes.

NOTE: Link test packets (ICMP echo to test addresses) must actually test the individual link (be routed through it). In combination with IPsec control, it must not happen that the IPsec tunnel captures and encrypts these packets. Otherwise, non-standard behaviour may occur (oscillation, test never succeeds, stuck on broken link).

4.2.2.3. Status

Status info area provides list of all enabled link. Link state and Link role (see description above) provide information about individual status of each link and which of the links is the active one.

4.2.3. Babel

Babel is a loop-avoiding distance-vector routing protocol that is designed to be robust and efficient both in networks using prefix-based routing and in networks using flat routing ("mesh networks"), and both in relatively stable wired networks and in highly dynamic wireless networks (for more information see *RFC 6126*[3]).

Babel is also a dynamic routing protocol for Internet Protocol (IP) networks. It is an Interior Gateway Protocol (IGP) working within one Autonomous system. It is based on OSPF protocol (see the next chapter for OSPF protocol description) with the following differences:

- Works within one autonomous system
- Babel provides both wired and wireless type of network interface

Babel protocol is typically used within the network hops or other networks with limited data throughput.

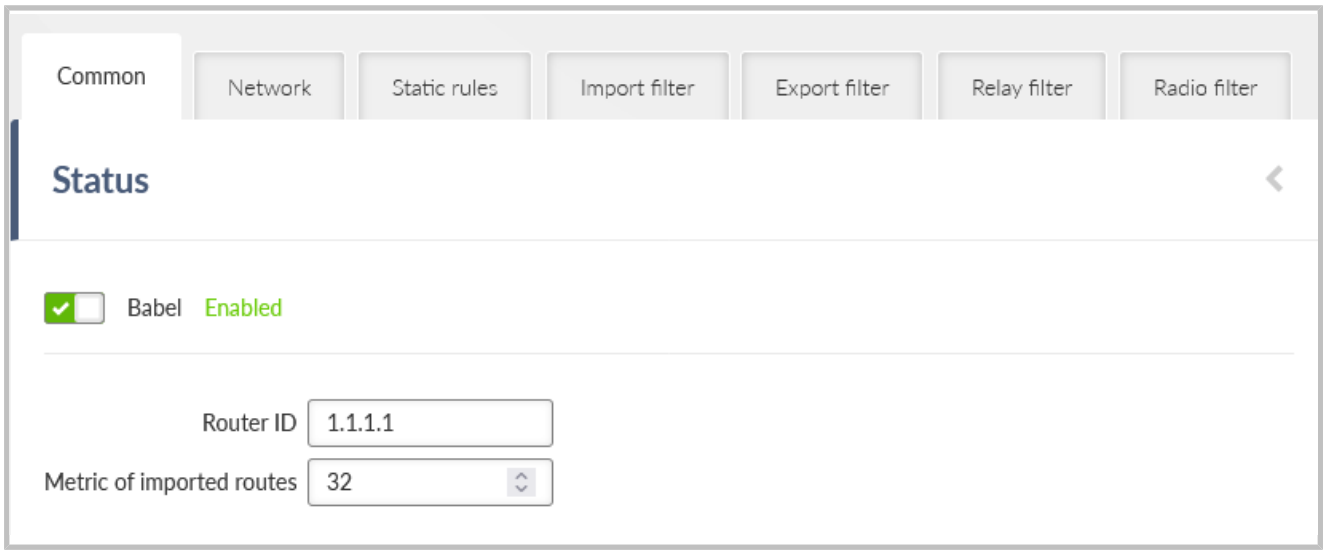


Fig. 4.11: SETTINGS > Routing > Babel

[3] https://datatracker.ietf.org/doc/html/rfc6126.html#section-1.1

Configuration parameters are described in the following chapters. Several use case scenarios and configuration examples are described in the *Babel Application note*[4].

4.2.3.1. Description

Every router defines which interfaces are used for Babel protocol to search for available network neighbors.

Each router is periodically transmitting and receiving Hello packets to determine existence and quality of a connection to neighboring network nodes. The result information about available routes (paths) and their quality is shared across the network. Routing tables are exchanged periodically and also after their update.

Routing path decision is based on a “metric”:

- Metric is set on each interface. It reflects a “price” for the packet reception. The higher the metric value, the more disadvantageous is usage of such a path.
- Maximum value is 65535.

There are two types of interfaces:

- Wired: assumes a reliable link. The quality is evaluated according to the number of received Hello packets. If configured limit of lost packets is exceeded, the line is considered down.
- Wireless: assumes a variable connection quality. The price of the interface increases gradually witch each lost Hello packet until the line is declared down.

Routing decision:

- SETTINGS > Routing > Static routes are valid even if the Dynamic routing is enabled. Dynamic routing protocols “export” resulting routing rules into Linux and they are added to the existing (static) routing rules.
- Particular routing decision takes IP mask as a primary decision rule (narrower mask has a higher priority) and metric as a secondary decision rule. Rules received from dynamic protocols have higher metric compared to Static routes (they always have the highest possible metric).
- Internal metrics of dynamic protocols are processed only inside them. Only the final set of routing rules is exported to the Linux router.

Example 1:

- SETTINGS > Routing > Static routes rule: 0.0.0.0/0 → 10.10.1.11
- Dynamic rule: 192.168.1.0/24 → 192.168.11.1 metric 32
- Packet with DST 192.168.1.42 will be routed to 192.168.11.1 because the dynamic rule has a narrower mask.

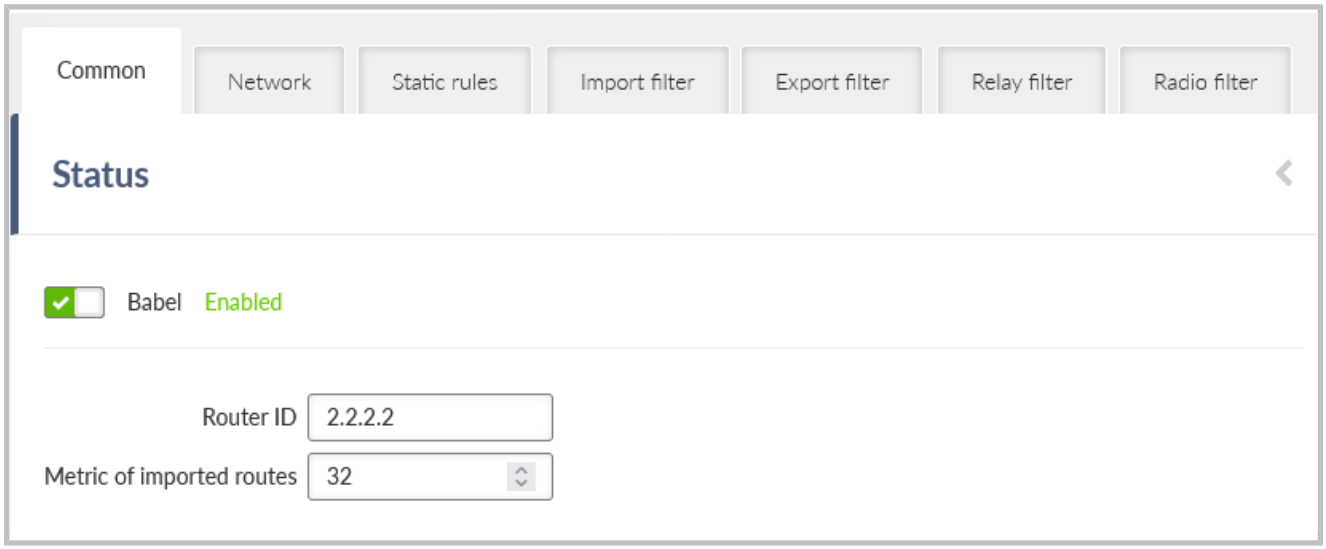
Example 2 – similar situation with additional static rule:

- SETTINGS > Routing > Static routes rule: 0.0.0.0/0 → 10.10.1.11

[4] https://www.racom.eu/download/hw/ripex/free/eng/1_application/ripex2-app-bab-en.pdf

- SETTINGS > Routing > Static routes rule: 192.168.1.0/24 → 192.168.22.1
- Dynamic rule: 192.168.1.0/24 → 192.168.11.1 metric 32
- Packet with DST 192.168.1.42 will be routed to 192.168.22.1 because the static rule has the same mask, but better metric.

4.2.3.2. Common - Common settings



Router ID

IP address, default = 0.0.0.0
WaSP unit acts in the Babel network as a dynamic router. Every router is identified by an ID having the format of IP address. This IP address does not have to be 'real'.
Router ID is shared across all dynamic protocols.

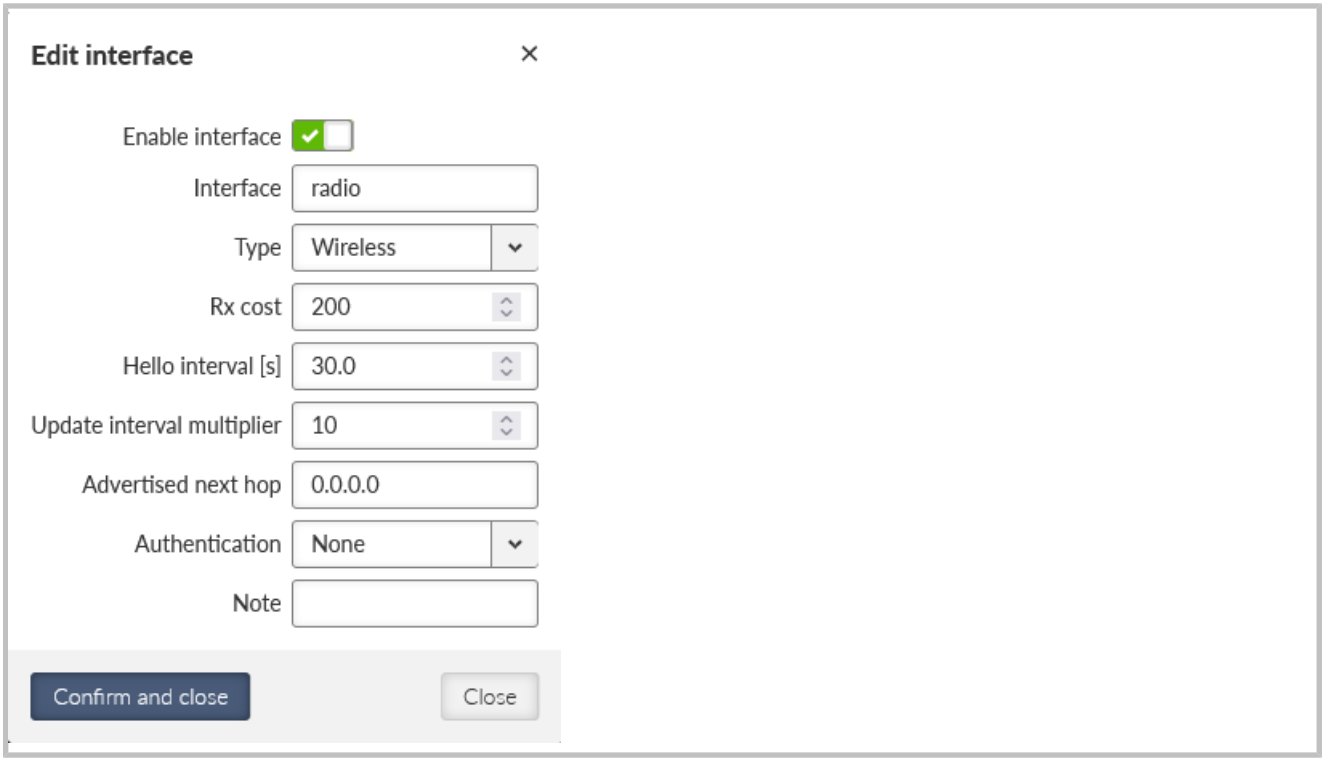
Randomize ID

List box {On; Off}, default = "Off"
Advanced feature: Enables randomization of the upper 4 Bytes of the router identification. The lower 4 Bytes are set by a **Router ID** parameter. This feature might be used in a case the Babel node is often restarted resulting in refusing its messages by its neighbors.

Routing offering

List box {On; Off}, default = "On"
Enables propagation of routing rules acquired from the neighbors. When disabled, the incoming rules are not propagated to other routers and this router behaves as an end point terminal – network paths are started or terminated in such a point, but do not travel through.

4.2.3.3. Network - Interfaces



Active

List box {On; Off}, default = "Off"
Enables / disables the interface.

Interface

String {a..z A..Z 0..9}, max 16 char, default = <empty>Interfaces which will be used by Babel for searching the available connections. Name of an existing unit interface has to be used. Following interfaces can be used:

LAN – “if_” prefix must be used followed by Network interface name, e.g. “if_LAN-141”

VLAN – “if_” prefix must be used followed by Network interface name, ‘.’ dot and VLAN number, e.g. “if_LAN-141.29”

Radio – “radio”

Hot standby – “hstdby”

GRE L3 – “gre_tunX” where ‘X’ is the tunnel number, starting from zero

Type

List box {Wired; Wireless}, default = "Wireless"
Type of network interface and also the type of link status evaluation. “Wired” link status is evaluated by checking the limit of received Hello packets – if not met, the link is considered down. “Wireless” link is status is evaluated using ETX criteria – each lost Hello packet gradually decreases the link metric.

Rx cost

Number {1 – 65534}, default = 128
The cost of using this interface to receive packet from a neighbor. It is added to Babel path metric.

Hello limit

Number {1 – 16}, default = 12

For “Wired” interface only: limit of received Hello packets from the 16 expected; if not met, the link is considered down.

Hello interval

Number {0.1 – 327.0}, default = 4.0

Interval (in seconds) of sending Hello packets.

Update interval multiplier

Number {2 – 30}, default = 4

Interval of sending the routing table update packets – to share the network topology information across the Babel network. The update interval is calculated as a multiplication of this parameter and **Hello interval**. The maximum length of the update interval (after the multiplication) is 655 seconds.

Advertised next hop

IP address, default = 0.0.0.0

This is the Next hop address which is announced to neighbors to be routed over this interface. Should this interface serve more IP addresses, this parameter enables selection of which of the addresses should be used for this station in the network neighbors routing tables.

Authentication

List box {None; Full; Only sign}, default = "None"

Enables packets authentication of Babel protocol.

- Full - packets are signed during transfer and the signature is validated when receiving incoming packets. Packets with invalid signature are reported to the log and thrown away.
- Only sign - Packets are signed during transfer and the signature is validated when receiving incoming packets. Packets with invalid signature are reported to the log and accepted. This settings is intended for gradual network switch to safe mode.

Authentication algorithm

List box {HMAC SHA256; HMAC SHA384; HMAC SHA512; BLAKE2s-128; BLAKE2s-256; BLAKE2b-256; BLAKE2b-512}, default = "HMAC SHA256"

Selects the authentication algorithm. This parameter occurs only, if parameter **Authentication** is set either to "Full" or "Only sign".

Each algorithm has its own passphrase length limit.

HMAC SHA256 - string length up to 128 char
HMAC SHA384 - string length up to 128 char
HMAC SHA512 - string length up to 128 char
BLAKE2s-128 - string length up to 32 char
BLAKE2s-256 - string length up to 32 char
BLAKE2b-256 - string length up to 64 char
BLAKE2b-512 - string length up to 64 char

Passphrase

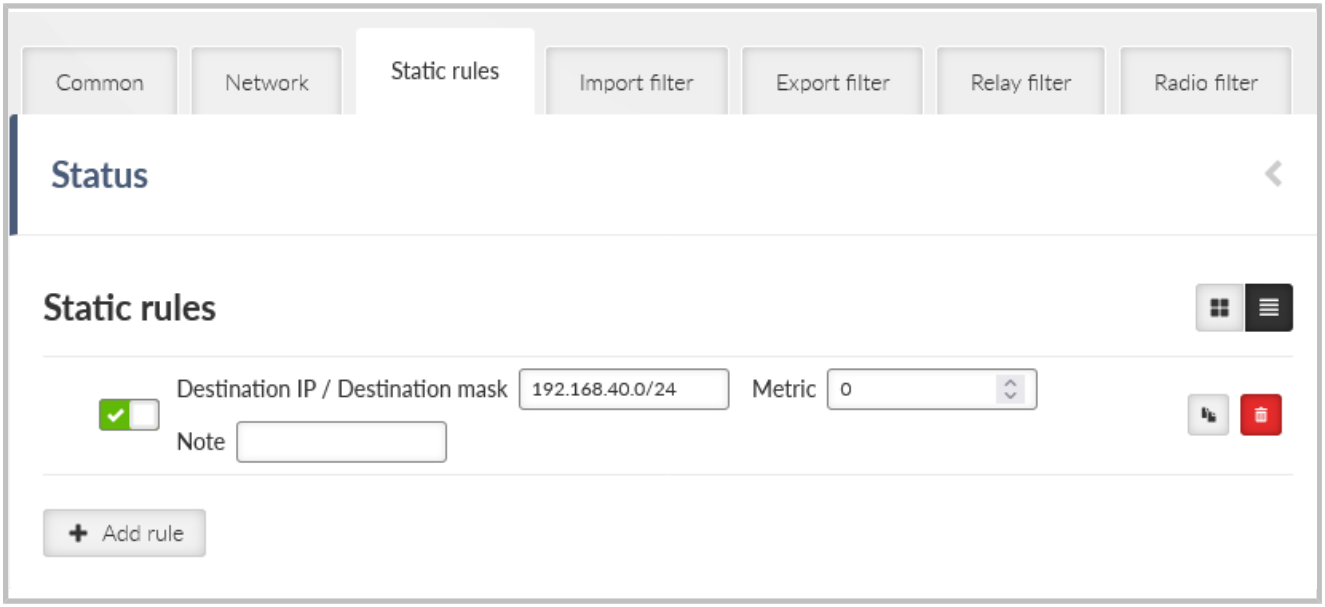
String {up to 128 char}

Defines the passphrase for packets authentication.

Note

Optional comment.

4.2.3.4. Static rules



Pre-defined static routing rules to be exported over the Babel protocol. Maximum number of rules is 256.

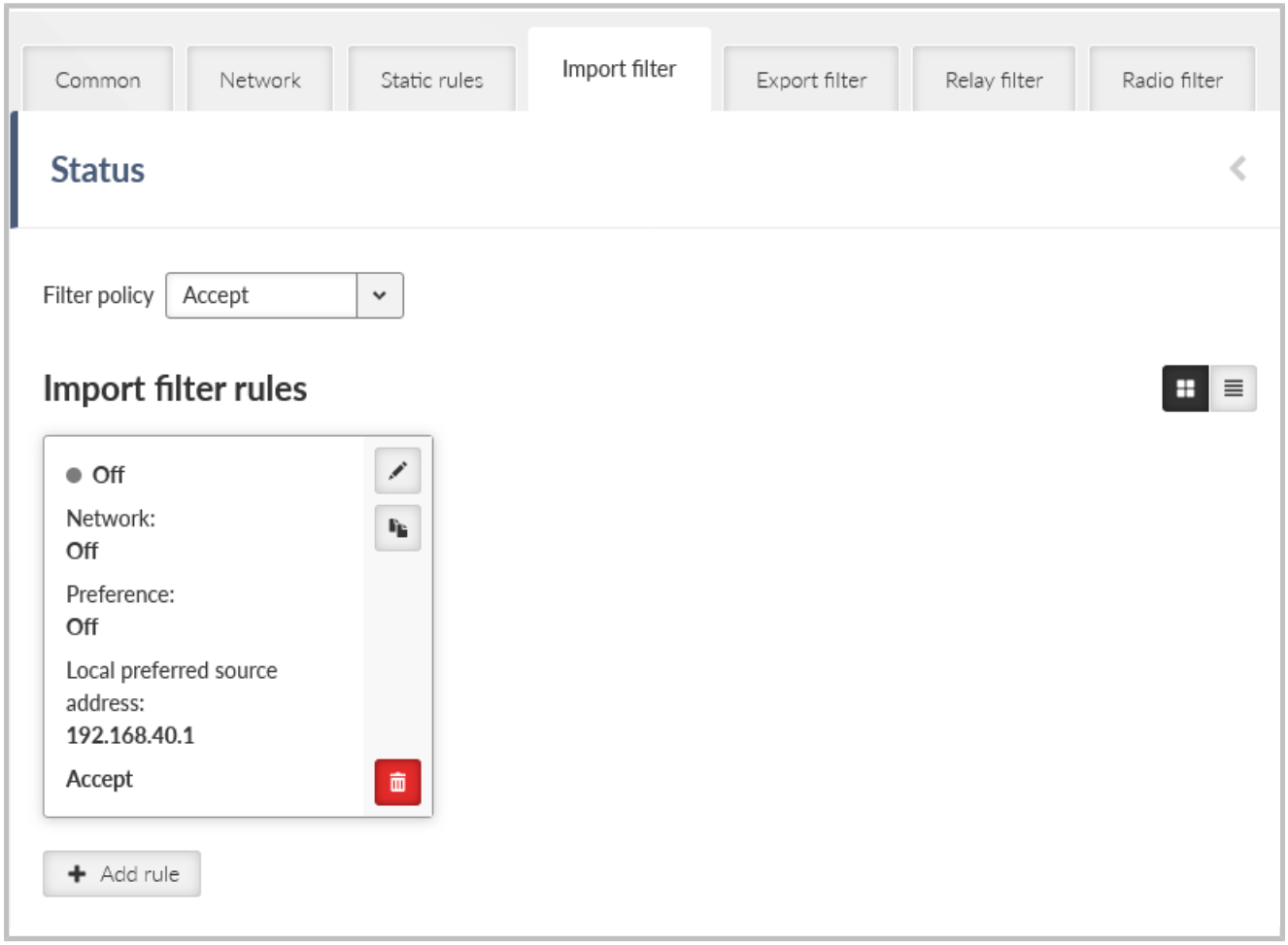
Active
List box {On; Off}, default = "On"
Enables / disables the static routing rule.

Destination IP / Destination mask
IP address, default = 0.0.0.0/0
IP address and mask defining the exported routing rule address range.

Metric
Number {0 – 65534}, default = 0
Routing rule metric value. The higher the value, the more “expensive” the path is.

Note
Optional comment.

4.2.3.5. Import filter



Babel import filter rules. The order of rules matters. Each incoming routing rule is processed by those Import filters. Maximum number of filter rules is 256.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Filter network
List box {Off; Match; Not match}, default = "Off"
Method of the routing rule target range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defining the network range to be compared.

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.
Examples:

Rule 0.0.0.0/0 {0,32} captures all IP ranges

Rule 192.168.1.0/24 {24,32} captures 192.168.1.0/24 and all subnets (for example 192.168.1.1/32)

Rule 10.9.8.7/32 {8,32} captures all ranges having the mask longer than 8 covering the address 10.9.8.7 (e.g. 10.9.0.0/16)

Action

List box {Accept; Reject; Pass}, default = "Accept"
Type of action to be performed when the filter rules above matches the incoming routing rule. When “Pass” is selected, the packet processing continues.

Set preference

List box {On; Off}, default = "Off"
When enabled, the Preference (see next parameter) will be set to this rule.

Preference

Number {0 – 65535}, default = 210
Routing rule preference in the routing table (to be used when Set preference is enabled). The higher the number the better the preference.

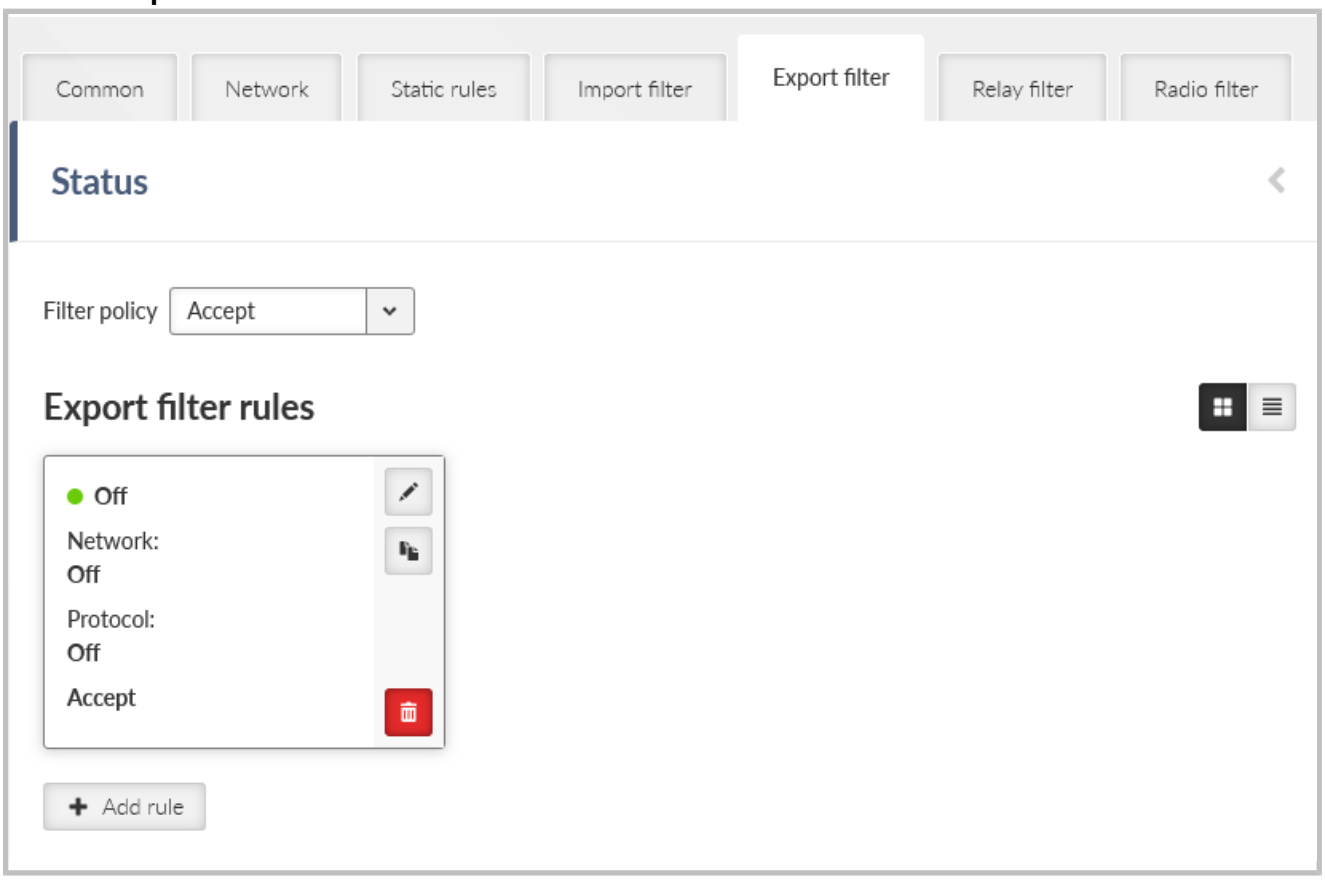
Local preferred source address

IP address, default = 0.0.0.0
Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

Note

Optional comment.

4.2.3.6. Export filter



Babel export filter rules define set of routing rules to be exported from the unit to other Babel routers. The order of rules matters. Maximum number of filter rules is 256.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Filter network
List box {Off; Match; Not match}, default = "Off"
Method of the routing rule target range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defining the network range to be compared.

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.

Filter protocol
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule source protocol is compared.

Protocol
List box {System; BGP; BGP external; BGP internal; OSPF}, default = "System"
Selection of the protocol origin. “System” – stands for rules from the ordinary routing table.

Filter BGP path
List box {Off; Is empty; Not empty}, default = "Off"
Compares BGP routing rule path if it is empty (i.e. the rule originates in this AS).

Filter OSPF source
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule from the OSPF protocol is compared.

OSPF source
List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 2"
OSPF sources. "Internal" – stands for internally generated rule (e.g. interface range). "Inter-area" – stands for rule generated on the area borders.

Filter OSPF tag
List box {Off; Match; Not match}, default = "Off"
OSPF tag based filtering method.

OSPF tag
Number {0 – (2^{32}-1)}, default = 0
OSPF tag to be compared.

Action
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken on the routing rule. When “Pass” is selected, the packet processing continues.

Metric from other protocol
List box {Off; BGP MED; OSPF Metric 1; OSPF Metric 2; OSPF Metric Sum}, default = "Off"
Defines source of metric.

Off: The static **Metric** value (see the following parameter) is used.

BGP MED: MED (Multi-Exit Discriminator) rules from the BGP protocol. If the rule does not have a MED value filled in, the static Metric value is used.

OSPF metric 1: Metric of OSPF type 1. If the rule does not have a metric value filled in, the static Metric value is used.

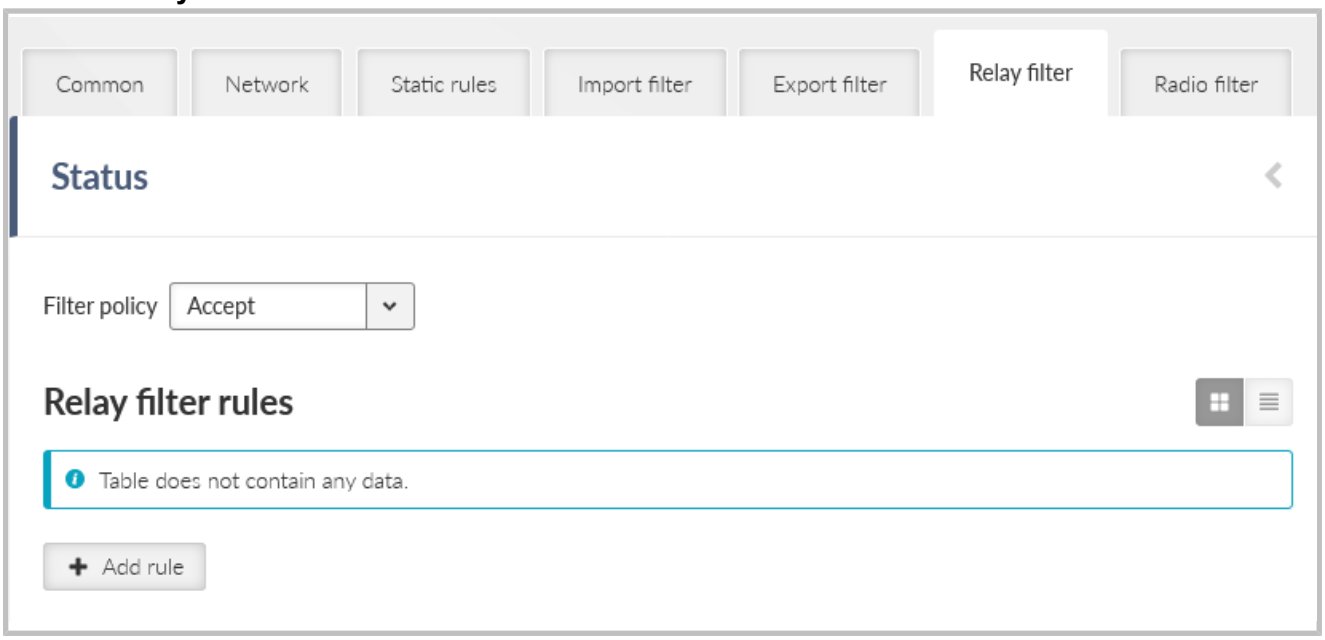
OSPF metric 2: Metric of OSPF type 2. If the rule does not have a metric value filled in, the static Metric value is used.

OSPF metric sum: Sum of OSPF type 1 a type 2 metrics. If the rule does not have both metric values filled in, the static Metric value is used.

Metric
Number {0 – 65534}, default = 0
Routing rule metric value. The higher the value, the more “expensive” the path is.

Note
Optional comment.

4.2.3.7. Relay filter



Relay filter selects what happens to a rule received from another Babel instance that were not captured in the filter. When disabled, the rules will not be forwarded to other routers and this station will act as a terminal where paths begin and end in the Babel network, but do not pass through it.

Filter policy
List box {Accept; Reject}, default = "Accept"

Enable rule
Check box {On; Off}, default = "On"

Activates/disables the rule

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a way to compare the target range of the rule

Network IP/Network mask	IP address / mask, default = 0.0.0.0/0
	Compares network prefix
Mask from	Number {0 – 32}, default = 0
	Defines the allowed mask length range of the compared rule
Mask to	Number {0 – 32}, default = 32
	Defines the allowed mask length range of the compared rule

Action
List box {Accept; Reject; Pass}, default = "Accept"
Chooses what to do with the rule

Filter metric
List box {Off; <; <=; >=; >}, default = "Off"
Selects a way to compare Babel metrics rules

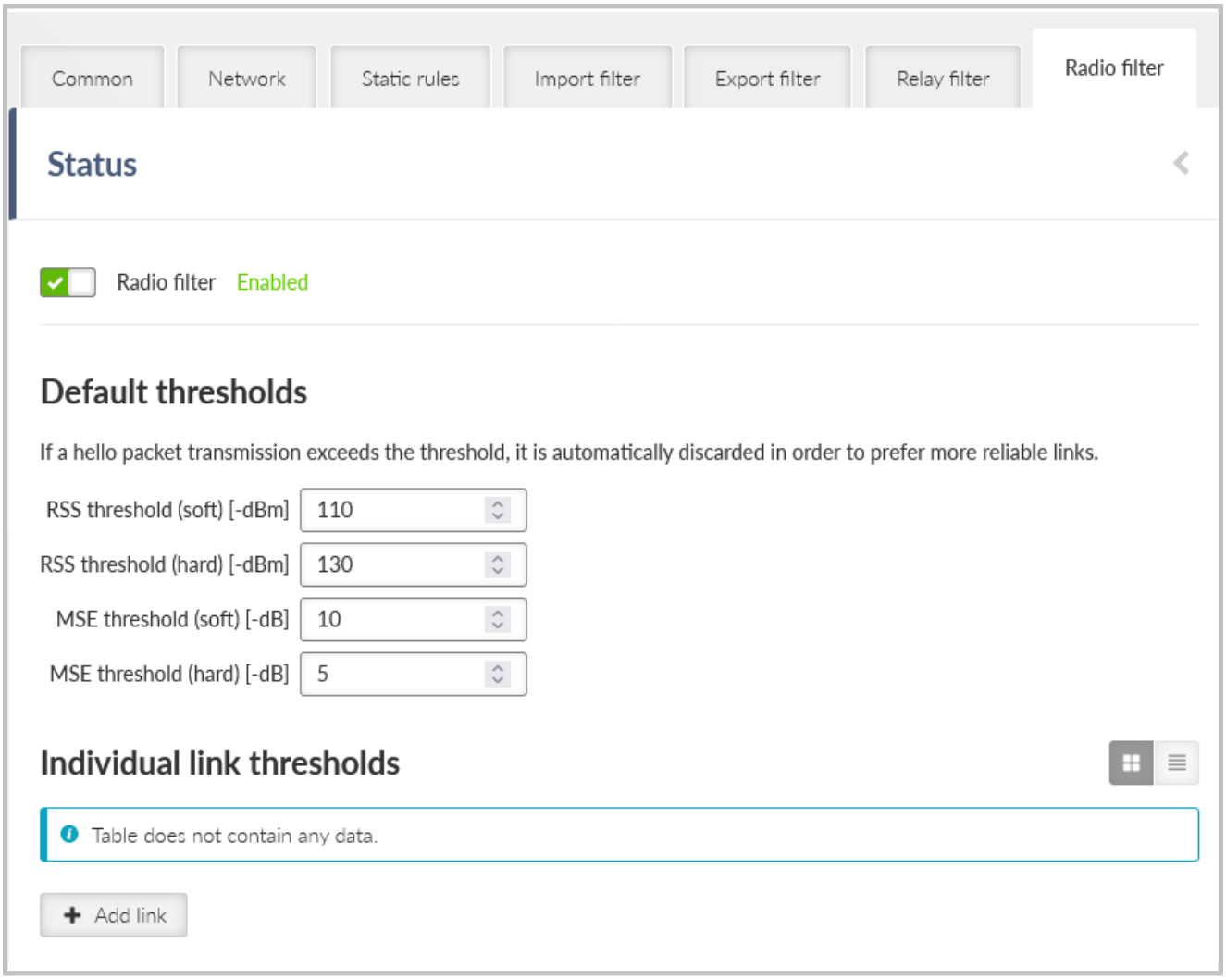
Metric value	Number {0 – 65534}, default = 0
	The compared value of the rule metric

Increase metric
List box {Off; On}, default = "Off"
Enables incrementing Babel rule metrics on forwarding. It is used to penalize paths through this router. Only when Action is Accept or Pass.

Added metric	Number {1 – 65534}, default = 1
	Value added to the rule metric

4.2.3.8. Radio filter

The Radio Filter is a function designed to improve the reliability of Babel, by ensuring user traffic is only routed over high-quality radio links. The filter operates by applying configurable **Soft** and **Hard** thresholds to Received Signal Strength (RSS) and Mean Square Error (MSE) in received Babel Hello packets. Packets exceeding the **Hard** limit are always discarded; packets falling between the thresholds are discarded with a probability that increases linearly as quality degrades; and only packets meeting the **Soft** threshold are always accepted.



Contains global Babel Hello packet filter settings in the radio protocol. This function is used to exclude radio links that do not have sufficient radio signal strength or signal quality to transmit standard packets, although short hello packets come through well.

The Default thresholds contain settings for filtering Babel Hello packets based on the quality metrics of the received signal, these settings are applied to all links until specific individual thresholds are configured.

RSS threshold (soft)
Number {50 – 150}, default = 110
RSS level limits [-dBm] of the received Hello packet
Soft limit is the worst value below which the packet is not discarded

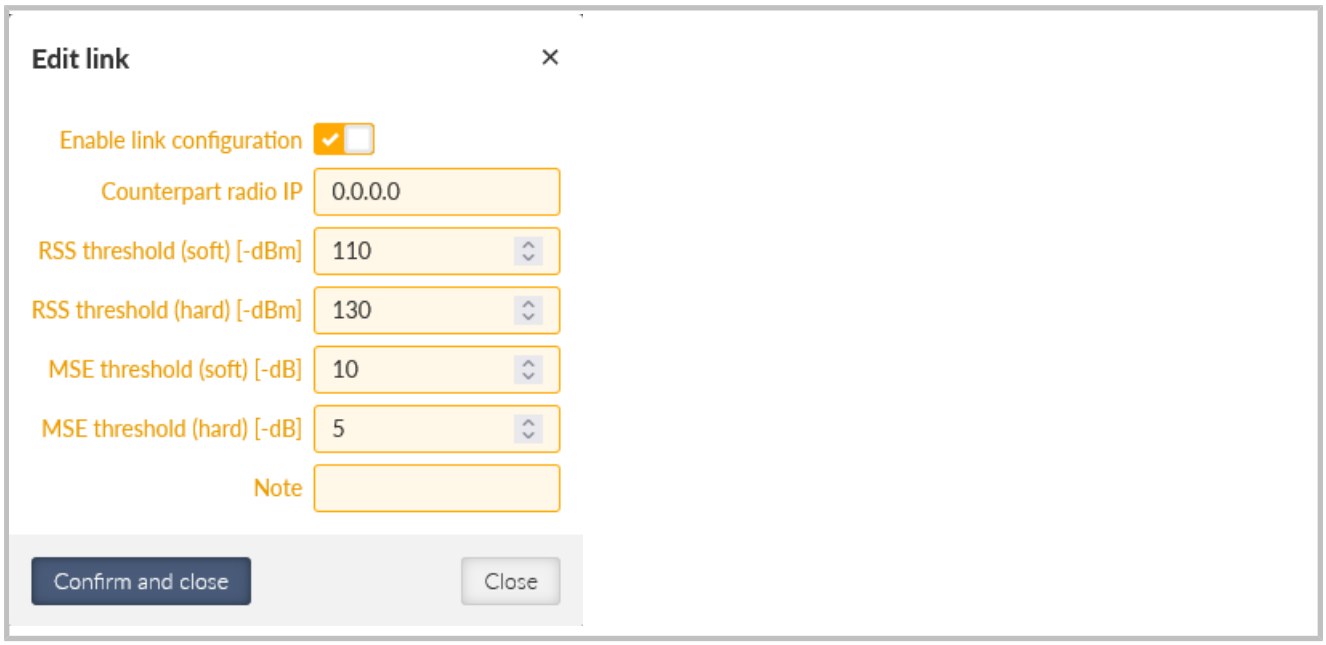
RSS threshold (hard)
Number {50 – 150}, default = 130
RSS level limits [-dBm] of the received Hello packet
Hard limit is the best value to always discard the packet

Note
Must be Soft threshold <= Hard threshold

MSE threshold (soft)
Number {0 – 60}, default = 10
MSE data level limits [-dB] of the received Hello packet
Soft limit is the worst value below which the packet is not discarded

MSE threshold (hard)
Number {0 – 60}, default = 5
MSE data level limits [-dB] of the received Hello packet
Hard limit is the best value to always discard the packet

Note
Must be Soft threshold >= Hard threshold



Individual link thresholds contain settings for filtering Babel Hello packets with specific remote based on the source link address.

Enable link configuration
List box {Off; On}, default = "On"
Activates individual settings

Counterpart radio IP
IP address, default = 0.0.0.0
Radio IP address of the Hello packet source for which the individual filter setting applies

Note
Optional note

Advanced settings

Filter poisoned routes
List box {Off; On}, default = "Off"
Enables filtering of poisoned route rules (which arise, for example, when a routing rule is revoked) when importing from the Babel protocol to the babel_ipv4 table (and thus to other tables). It does not affect their retranslation (special behavior of the Babel protocol).

Filter routes with high metric

List box {Off; On}, default = "Off"

Enables filtering of rules with metrics higher than the set metric when importing from the Babel protocol to the babel_ipv4 table. These rules cannot be used for routing in the station or propagated to other stations. They serve to limit the size of routing tables, but if set incorrectly, they can result in remote network stations having no valid path between them.

Maximal accepted route metric

Number {1 - 65534}, default = 1000

The highest value of the imported routing rule metric that will still be accepted.

4.2.4. OSPF

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). OSPF Version 2 defined in RFC 2328 (1998) for IPv4 is implemented in the WaSP router. OSPF provides Layer 2 dynamic routing. In the context of WaSP networks it is typically used for the backhaul network routing.

OSPF splits the network into “areas” to simplify the network topology. There is a primary “backbone” (0.0.0.0) area and the other areas are connected to this backbone area via border routers.

The route decision process is affected by the path “metric”. There are two types of metrics:

- Metric Type 1 – path length; individual interfaces pass-over costs are added.
- Metric Type 2 – is setup on the rules which are exported to the OSPF from outside. Rules having metric ‘Type 2’ are always treated as worse (i.e. longer path) comparing to metric ‘Type 1’.

Routers in a specific area are always connected via interfaces.

- An address range can be defined for an interface where is the OSPF working. Multiple address ranges can be defined (behaving as another interface).
- Router to router interconnection can be protected by encryption with the passphrase.
- Specific “Cost” is defined for each interface which is added to metric ‘Type 1.’
- There are multiple types of interfaces:
  - Stub – interface only announces to OSPF: its presence and its address ranges to be propagated further to the network.
  - Broadcast – to be used in the network where all the participants always hear each other (Ethernet). Designated Router (DR) and Backup DR (BDR) are setup between the neighbors. They are responsible for the update propagation (broadcast).
  - NBMA (Non-Broadcast Multiple Access) – to be used in the network where only specific participants can communicate between each other; all the participants hear each other but multicast is not available. DR and BDR is setup.
  - Point2Point – network having only two participants. They discover each other using multicast.
  - Point2Multipoint – network where only predefined pairs of participants can hear each other (e.g. star topology); multicast is not available.

- Static rules can be defined. Such a routing rules are propagated to the network from this router.
- It is possible to define exported routing rules aggregation or specific routing rule hiding.
- It is possible to control the routing rules which are imported into the WaSP unit from the OSPF protocol and those that are exported into the OSPF protocol from the unit by using ‘filters’.
  - Export filters – to control rules exported from the unit to the OSPF protocol which is propagating them further.
  - Import filters – to control rules imported from the OSPF into the unit.

4.2.4.1. OSPF Common - Common settings

Active
List box {On; Off}, default = "Off"
Enables the dynamic routing and the OSPF protocol.

Router ID
IP address, default = 0.0.0.0
WaSP unit acts in the OSPF network as a dynamic router. Every router is identified by an ID having the format of IP address. This IP address does not have to be ‘real’. Router ID is shared across all dynamic protocols.

Instance ID
Number {0 – 255}, default = 0
OSPF protocol instance number. This number is needed in case of running multiple OSPF protocols (for example on the border of 2 independent OSPF networks).

4.2.4.2. OSPF Network - Areas and interfaces

4.2.4.2.1. Areas and interfaces

OSPF areas WaSP unit belongs to are described here. Maximum number of areas is 32.

Enable / Disable
Enables / disables the specific area.

Area ID
IP address, default = 0.0.0.0
OSPF area identifier. The ID has a format of an IP address. This IP address does not have to be ‘real’. The ‘Router ID’ value is used typically. The default value of 0.0.0.0 is called ‘backbone’ and it has to be present somewhere in the OSPF network.

Stub area
Click box {On; Off}, default = "Off"
Defines if the area is of a ‘stub’ type – which means, the traffic is not routed through such an area. Every traffic is originated or terminated in the ‘stub’ area.

Stub default GW (ADVANCED parameter)
List box {On; Off}, default = "On"
If ‘On’ – only default GW is routed to the ‘stub’ area. Of ‘Off’ – individual routes are routing the traffic into the area. It may be effective to disable this parameter when multiple border routers are present.

Note
Optional comment. It is a good practice to enter some descriptive area name since this value is displayed (when filled) instead of the **Area ID** as an **Area** name in other configuration dialogs (e.g. Networks configuration).

OSPF interfaces of the respective OSPF area are defined here. Maximum number of interfaces is 128.

Active
List box {On; Off}, default = "Off"
Enables / disables the interface.

Interface
String {a..z A..Z 0..9}, max 16 char, default = <empty>
OSPF interface name. Name of an existing unit interface has to be used. Following interfaces can be used:

- LAN – “if_” prefix must be used followed by Network interface name, e.g. “if_LAN-141”
- VLAN – “if_” prefix must be used followed by Network interface name, ‘.’ dot and VLAN number, e.g. “if_LAN-141.29”
- Radio – “radio”
- Hot standby – “hstdby”
- GRE L3 – “gre_tunX” where ‘X’ is the tunnel number, starting from zero
- Cellular – “ext”

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask of the address range above which the OSPF protocol will be working on this interface. The default value is 0.0.0.0/0, which means the whole address range on this interface is available for the OSPF protocol.

Network type
List box {Broadcast; Point2Point; Point2Multipoint; NBMA; Stub}, default = "Broadcast"
Defines the type of the network behind the interface.

Cost
Number {1 – 65535}, default = 10
The cost of traffic over this interface. The higher the Cost, the worse the path. It is added to OSPF metric ‘Type 1’.

Hello interval
Number {1 – 3600}, default = 10
Interval (in seconds) of sending Hello packets. The interval must be the same for the all participants of the given interface.

Poll interval
Number {1 – 3600}, default = 20
Interval (in seconds) of sending Hello packets to inactive neighbors in the NMBA type of interface.

Retransmit interval
Number {1 – 3600}, default = 5

Interval (in seconds) of repeating unacknowledged packets.

Dead count
Number {2 – 64}, default = 4
Number of lost Hello packets from the neighbor to treat the connection as interrupted.

TTL security
List box {On; Off}, default = "On"
Protection against OSPF packets spoofing.

Authentication, Passphrase
List box {None; Keyed MD5 (OSPFv2); HMAC SHA256; HMAC SHA384; HMAC SHA512}, default = "None"
Selection of a method to authenticate the OSPF messages. Passphrase is used as a secret key for the selected hash function. Maximum length of the passphrase is 128 characters.

Priority
Number {0 – 255}, default = 1
Priority is used to select primary or backup router responsible for the routing updates propagation. The higher the number, the higher the priority. '0' states the router cannot be used as a primary or backup router.

Use broadcast
List box {On; Off}, default = "Off"
Defines if OSPF packets distribution is provided using multicasts (default behavior) or broadcasts (nonstandard behavior).

Note
Optional comment. It is possible to enter some descriptive OSPF interface name. This value is used (when filled) instead of the original **Interface** identification as an **Interface** name in other configuration dialogs (e.g. Neighbors configuration).

4.2.4.2.2. Neighbors

Network neighbors of Point2Multipoint and NBMA types of OSPF interfaces are defined here. Maximum number of neighbors is 512.

Active
List box {On; Off}, default = "Off"
Enables / disables the interface.

Interface
List box {list of existing OSPF interfaces}
OSPF interface the neighbor belongs to. The interface – **Note** value is used when defined. The interface – **Interface** value is used otherwise.

IP
IP address, default = 0.0.0.0
IP address of the neighbor.

Note
Optional comment.

4.2.4.2.3. Networks

The Networks table modifies networks announced out of the area. It enables partial networks aggregation into the common prefixes or specific network hiding. Maximum number of rules is 256.

Active
List box {On; Off}, default = "Off"
Enables / disables the interface.

Area
List box {list of existing OSPF areas}
OSPF area the record belongs to.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask of the range (i.e. network) which will be aggregated or hidden.

Action
List box {Aggregate; Hide}, default = "Aggregate"

- Aggregate – small network prefixes will be exported from this area aggregated into this range (defined by **IP / mask**)

- Hide – this network prefix will be hidden and will not be exported

Example:
Area 0.0.0.1 exports two subnets: 192.168.1.0/24 and 192.168.2.0/24. Area border router between Area 0.0.0.1 and 0.0.0.0 defines a rule for network aggregation: 192.168.0.0/16. As a result of this, the area border router announces to the area 0.0.0.0 only one route 192.168.0.0/16 instead of the two individual routes.

Note
Optional comment.

4.2.4.3. OSPF Static rules

Pre-defined static routing rules to be exported over the OSPF protocol. Maximum number of rules is 256.

Active
List box {On; Off}, default = "Off"
Enables / disables the static routing rule.

Destination IP / Destination mask
IP address, default = 0.0.0.0/0
IP address and mask defining the exported routing rule address range.

Metric type
List box {Type 1; Type 2}, default = "Type 1"
Metric type of the routing rule. Metric 1 is added to the path cost. Metric 2 stays apart and compared to metric 1 is always bigger.

Metric
Number {1 – 65535}, default = 1000
Routing rule metric value.

OSPF tag
Number {0 – (2^{32}-1)}, default = 0
OSPF tag is added to a rule at the moment of its insertion to the network. The tag travels through the OSPF without any modification so it can be used to distinguish the rule in the filters.

Note
Optional comment.

4.2.4.4. OSPF Import filter

OSPF import filter rules. The order of rules matters. Each incoming routing rule is processed by those Import filters. Maximum number of filter rules is 256.

Active
List box {On; Off}, default = "Off"
Enables / disables the filter rule.

Filter network
List box {Off; Match; Not match}, default = "Off"
Method of the routing rule target range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defining the network range to be compared.

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.
Examples:

- Rule 0.0.0.0/0{0,32} captures all IP ranges
- Rule 192.168.1.0/24{24,32} captures 192.168.1.0/24 and all subnets (for example 192.168.1.1/32)
- Rule 10.9.8.7/32{8,32} captures all ranges having the mask longer than 8 covering the address 10.9.8.7 (e.g. 10.9.0.0/16)

Filter source
List box {Off; Match; Not match}, default = "Off"
Method of the OSPF routing rule source comparison.

Source
List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 1"
Source types comments:

- Internal – internally generated rule, for example interface range
- Inter-area – rule generated on the area border

Filter OSPF tag
List box {Off; Match; Not match}, default = "Off"
Method of the OSPF routing rule OSPF tag comparison

OSPF tag
Number {0 – (2^{32}-1)}, default = 0
OSPF tag to be compared.

Action
List box {Accept; Reject; Pass}, default = "Accept"
Type of action to be performed when the filter rules above matches the incoming routing rule.

Set preference
List box {On; Off}, default = "Off"
When enabled, the **Preference** (see next parameter) will be set to this rule.

Preference
Number {0 – 65535}, default = 200
Routing rule preference in the routing table (to be used when **Set preference** is enabled). The higher the number the better the preference.

Local preferred source address
IP address, default = 0.0.0.0
Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

Note
Optional comment.

4.2.4.5. OSPF Export filter

OSPF export filter rules define set of routing rules to be exported from the unit into the OSPF area. The order of rules matters. Maximum number of filter rules is 256.

Active
List box {On; Off}, default = "Off"
Enables / disables the filter rule.

Note
Optional comment.

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defines the network prefix to be compared.

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.

Filter protocol
List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule source protocol is compared.

Protocol
List box {System; BGP; BGP external; BGP internal}, default = "System"
Selection of the protocol origin. “System” – stands for rules from the ordinary routing table.

Filter BGP path
List box {Off; Is empty; Not empty}, default = "Off"
Compares BGP routing rule path if it is empty (i.e. the rule originates in this AS).

Action
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken on the routing rule. "Pass" continues in processing.

4.2.5. BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems. BGP is classified as a path-vector routing protocol, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

BGP splits the network into Autonomous Systems (AS) which are identified by a specific number. Individual BGP routers are interconnected with their neighbors using TCP connections. Any connection can travel over multiple hops. Any connection can be secured using MD5 signatures.

Connections inside the AS are called ‘internal’ (iBGP):

- All BGP routers within given AS must be fully interconnected – every router must have connection to all other routers.
- It is possible to define ‘Route reflectors’ – they must be fully interconnected. The other routers behave as Route reflector clients and they need a connection to their reflector only. Route reflector and its clients form a ‘cluster’. It is possible to create a cluster with multiple Route reflectors for the purpose of backup.
- The iBGP router having a higher local preference will be preferred during the internal AS path selection.

Connections to another AS are called ‘external’ (eBGP):

- It is possible to communicate from the router to the neighbor AS the MED (Multi-Exit Discriminator) metric designating which of the AS border routers will be used as an input point.

When the routing rules are spread across the multiple AS, those AS are added into the accumulated path (BGP path). Path length is the primary criteria during the decision which of the routing rules will be used.

It is possible to prescribe routing rules toward this router which will be spread across the network (Static rules).

It is possible to control the routing rules which are imported into the WaSP unit from the BGP protocol and those that are exported into the BGP protocol from the unit by using ‘filters’.

Import IGP filter – controls which of the routing rules from the BGP are accepted to the dynamic routing table and how

Export IGP filter – controls which of the routing rules from the dynamic routing table are exported to the BGP and how

Import OUT filter – controls which of the routing rules from the other AS are accepted to the BGP and how

Export OUT filter – controls which of the routing rules are exported from the BGP to other AS and how

Routing rules passed on between iBGP and BGP tables are not filtered

4.2.5.1. BGP Common - Common settings

Active
List box {On; Off}, default = "Off"
Enables the dynamic routing and the BGP protocol.

Router ID
IP address, default = 0.0.0.0
WaSP unit acts in the BGP network as a dynamic router. Every router is identified by an ID having the format of an IP address. This IP address does not have to be 'real'. Router ID is shared with the OSPF protocol.

Local AS
Number {0 – (2^{32}-1)}, default = 65000
Local Autonomous System identification number. AS numbers are assigned by IANA. Part of the range is reserved for private network usage: 64512 – 65534 and 4200000000 – 4294967294. AS numbers from this range can be safely used by anyone.

Preference
Number {0 – (2^{32}-1)}, default = 100
Router preference within the local AS. The higher the number, the higher the preference.

MED (Multi-Exit Discriminator)
List box {Off; Static; OSPF metric 1}, default = "Off"
Setting of MED (Multi-Exit Discriminator) on the routing rules being exported to other AS. MED makes it possible to advertise which of the routers in the local AS is the preferred input point to the AS. "Static" option sets the fixed value for all rules (**Static MED**). "OSPF metric 1" copies the OSPF metric to MED; for the rules which are not from the OSPF it enters the fixed value **Static MED**.

Static MED
Number {0 – (2^{32}-1)}, default = 0
Metric to be used for the preferred input point to the AS selection (see MED (Multi-Exit Discriminator) description). The higher the number the lower the preference.

Route reflector
List box {Off; On}, default = "Off"
Enables the Route reflector function on this router. iBGP requires connection in between all routers under normal circumstances. Route reflector makes it possible to avoid this requirement by distributing routing updates to all its clients. Such clients do not need any other connection except connection to this Route reflector. Route reflector and its clients form a 'cluster'. See more details at the beginning of the BGP chapter.

Cluster ID type
List box {Router ID; Manual}, default = "Router ID"
Controls the iBGP cluster identification. Cluster identification must be the same inside the cluster and it has to be different in another cluster. If the "Router ID" is selected, the **Router ID** value is used as a cluster id.

Cluster ID
IP address, default = 0.0.0.0
Cluster identification in the format of an IP address. This IP address does not have to be 'real' (valid).

4.2.5.2. BGP Neighbors

Neighboring BGP routers. Maximum number of neighbors is 256.

Active
List box {On; Off}, default = "On"
Enables the specific neighbor.

Note
Optional comment.

Neighbor type
List box {Internal; External}, default = "External"
Neighbor router type selection. "Internal" neighbor belongs to the same AS (iBGP). "External" belongs to other AS (eBGP).

Neighbor AS
Number {0 – (2^{32}-1)}, default = 65000
Neighbor AS number.

Neighbor IP
IP address, default = 0.0.0.0
Neighbor router IP address.

Local IP of the connection
IP address, default = 0.0.0.0
Local IP address of the connection. Default value 0.0.0.0 provides automatic set up of this address – from the routing.

Neighbor connection
List box {Direct; Multihop}, default = "Direct"
Network connection type between the neighbors. "Direct" means direct – one hop – connection. This is typical for eBGP routers. "Multihop" means connection over the multiple routers. This is typical for iBGP routers.

MD5 authentication
List box {On; Off}, default = "Off"
Enables BGP packets authentication using TCP MD5 Signature extension.

Passphrase
String {up to 128 char}
Passphrase for the **MD5 authentication**.

Passive
List box {On; Off}, default = "Off"
Passive BGP router does not initiate connection to a neighbor, it is waiting for the neighbor activity.

Hold interval [s]
Number {3 – 10800}, default = 240
Time (in seconds) to wait for the keepalive message from the neighbor. It is negotiated with the neighbor. When it expires, the connection is treated as interrupted.

Keepalive interval [s]
Number {1 – 3600}, default = 80
Period (in seconds) of sending keepalive messages. It should not be longer than 1/3 of the **Hold interval**.

Connection retry interval [s]
Number {1 – 3600}, default = 120
Time (in seconds) to wait before trying to re-connect the interrupted connection.

TTL security
List box {On; Off}, default = "On"
Protection against BGP packets spoofing. [PP1] The Generalized TTL Security Mechanism (GTSM – RFC 5082) is used. BGP transmits packets with known TTL value. Incoming packets having lower than expected value (expected number of hops) are discarded.

Expected hops
Number {2 – 32}, default = 2
Number of expected hops between the neighbors.

Route reflector client
List box {On; Off}, default = "Off"
Defines if this neighbor is a client of this Route reflector.

Set cost
List box {On; Off}, default = "Off"
Enables to set a specific **Cost** of the BGP connection.

Cost
Number {0 – (2^{32}-1)}, default = 10
The cost of connection to this neighbor. The higher the number the higher the cost. It enables to make decisions inside the router between multiple paths from the same neighbor.

Next hop self
List box {Off; Always; Internal; External}, default = "Off"
Defines it the exported routing rules should have ‘next hop’ addresses overwritten to the address of this router. "Internal" overwrites only the rules from the local AS. "External" overwrites only the rules from the other AS.

4.2.5.3. BGP Static rules

Pre-defined static routing rules to be exported over the BGP protocol. Maximum number of rules is 256.

Active
List box {On; Off}, default = "Off"

Enables / disables the static routing rule.

Destination IP / Destination mask
IP address, default = 0.0.0.0/32
IP address and mask defining the exported routing rule destination address range.

Note
Optional comment.

4.2.5.4. BGP Import IGP filter

Import IGP filter [PP1] rules. The order of rules matters. Maximum number of filter rules is 256.

Filter policy
List box {Accept; Reject}, default = "Reject"
Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Import IGP filter**.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Note
Optional comment.

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defines the network prefix to be compared

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.

Filter source
List box {Off; Internal; External}, default = "Off"
Selection based on the routing rule source. "Internal" selects rules received from the internal (iBGP) connection. "External" selects rules received from the other AS (eBGP).

Filter BGP path
List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"
Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

Path position
List box {Any; Neighbor; Source}, default = "Any"

Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule was originated from this AS (first on the path).

Path AS
Number {0 – (2^{32}-1)}, default = 65000
The number of the AS searched for.

Action
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken on the captured [PP1] routing rule. "Pass" continues in processing.

Set preference
List box {Off; On}, default = "Off"
Defines if the specific **Preference** will be set up for this rule.

Preference
Number {0 – 65535}, default = 100
Routing rule preference in the routing table. The higher the number the higher the preference.

Local preferred source address
IP address, default = 0.0.0.0
Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

4.2.5.5. BGP Export IGP filter

Export IGP filter rules. The order of rules matters. Maximum number of filter rules is 256.

Filter policy
List box {Accept; Reject}, default = "Reject"
Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Export IGP filter**.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Note
Optional comment.

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defines the network prefix to be compared

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

Filter protocol
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule source protocol is compared.

Protocol
List box {System; OSPF}, default = "System"
Selection of the protocol origin. "System" – stands for rules from the ordinary routing table. "OSPF" stands for rules from the OSPF protocol.

Filter OSPF source
List box {Off; Match; Not match}, default = "Off"
Selects the OSPF routing rule source comparison mode.

OSPF source
List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 2"
OSPF sources. "Internal" – stands for internally generated rule (e.g. interface range). "Inter-area" – stands for rule generated on the area borders.

Filter OSPF tag
List box {Off; Match; Not match}, default = "Off"
Selects the way of filtering based on OSPF tag.

OSPF tag
Number {0 – (2^{32}-1)}, default = 0
OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.

Action
List box {Accept; Reject; Pass}, default = "Accept"Defines what action is taken on the routing rule. "Pass" continues in processing.

4.2.5.6. BGP Import OUT rules

Import OUT filter [PP1] rules. The order of rules matters. Maximum number of filter rules is 256.

Filter policy
List box {Accept; Reject}, default = "Accept"
Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Import OUT filter**.

Filter limit
Number {1 – 65535}, default = 1024
Limit of the accepted routing rules from the neighbor. The limit applies before this Import OUT filter. Excess rules are dropped.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Note
Optional comment.

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.

IP address / mask
IP address / mask, default = 0.0.0.0/0
IP address and mask defines the network prefix to be compared

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.

Filter BGP path
List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"
Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

Path position
List box {Any; Neighbor; Source}, default = "Any"
Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule originates from this AS (first on the path).

Path AS
Number {0 – (2^{32}-1)}, default = 65000
The number of the AS searched for.

Action
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken with the matching routing rule. "Pass" continues in processing.

Prepend local AS
Number {0 – 8}, default = 0
Enables to append (even multiple times) local AS number to the BGP path end – making the path virtually longer. The longer path is handicapped during the comparisons and selections.

4.2.5.7. BGP Export OUT filter

Export OUT filter rules. The order of rules matters. Maximum number of filter rules is 256.

Filter policy
List box {Accept; Reject}, default = "Accept"
Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Export OUT filter**.

Active
List box {On; Off}, default = "On"
Enables / disables the filter rule.

Note
Optional comment.

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.

IP address / mask
List box {Off; Match; Not match}, default = "Off"
IP address and mask defines the network prefix to be compared

Mask from
Number {0 – 32}, default = 0

Mask to
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.

Filter protocol
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule source protocol is compared.

Protocol
List box {System; OSPF; BGP; BGP external; BGP internal}, default = "System"
Selection of the protocol origin. "System" – stands for rules from the ordinary routing table.

Filter OSPF tag
List box {Off; Match; Not match}, default = "Off"
Selects the way of filtering based on OSPF tag.

OSPF tag
Number {0 – (2^{32}-1)}, default = 0
OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.

Filter BGP path
List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"
Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

Path position
List box {Any; Neighbor; Source}, default = "Any"
Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule was originated from this AS (first on the path).

Path AS
Number {0 – (2^{32}-1)}, default = 65000
The number of the AS searched for.

Action
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken on the routing rule. "Pass" continues in processing.

4.3. Firewall

A firewall is a critical security tool that monitors and controls network traffic based on predefined rules. It acts as a protective barrier, filtering data packets to prevent unauthorized access, malicious attacks, and other threats.

Firewalls operate at Layer 2 (L2) and Layer 3 (L3) of the OSI model, offering features like packet filtering, traffic inspection, and stateful connection tracking for robust network protection.

4.3.1. Firewall L2

An L2 firewall operates at the data link layer, managing traffic based on MAC addresses and Ethernet frames within the same local network or broadcast domain. It can block or allow traffic based on source and destination MAC addresses, VLAN tags, or specific Ethernet frame types. L2 firewalls are essential for enforcing network segmentation, controlling device access, and optimizing bandwidth in narrowband networks.

4.3.1.1. Blocklist/Allowlist

L2 firewalls enable MAC address filtering to control network access. Administrators can define rules to allow or block traffic from specific devices, enhancing security and isolating compromised endpoints.

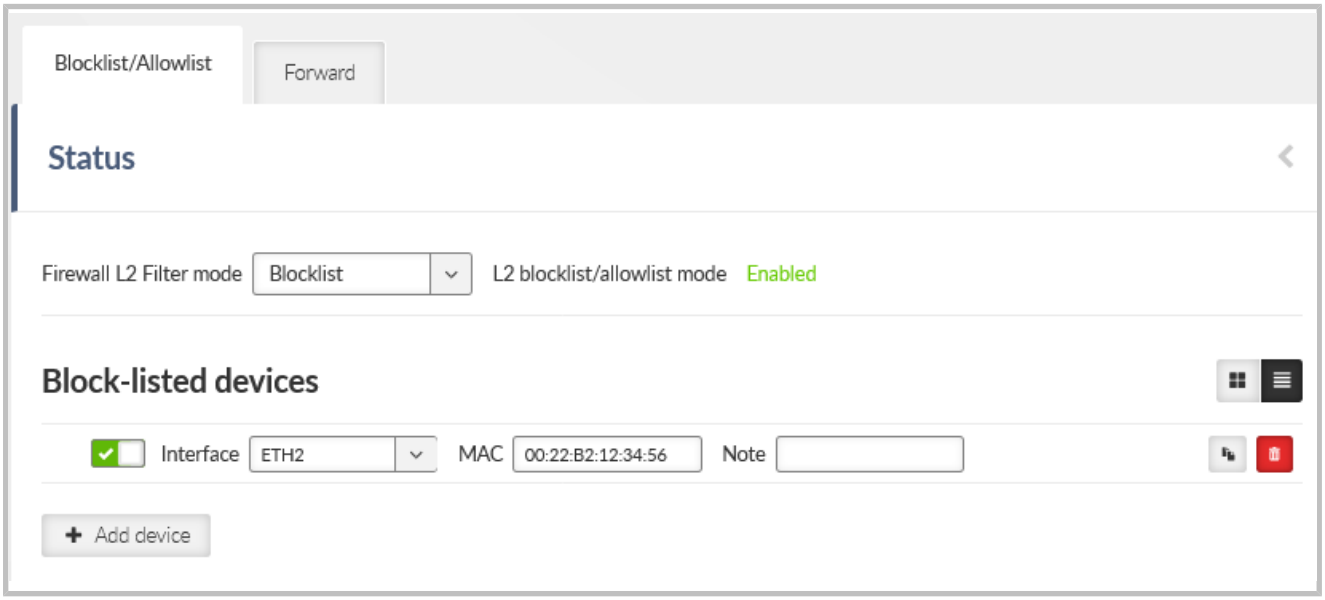


Fig. 4.12: SETTINGS > Firewall > L2

Filter mode
List box {Off; Blocklist; Allowlist}, default = "Off"

Blocklist
The MAC addresses listed in the table are blocked, i.e. all packets to/from them are discarded. The traffic to/from other MAC addresses is allowed.

Allowlist
Only the MAC addresses listed in the table are allowed, i.e. only packets to/from them are allowed. The traffic to/from other MAC addresses is blocked.

Active
List box {Off; On}, default = "On"
If "On", Layer 2 Linux firewall rule is activated.

Interface
List box {All; ETH1..ETH2}, default = "All"

MAC
IPv4 MAC address

Note

L2 firewall settings do not impact the local ETH access, i.e. settings never deny access to a locally connected WaSP (web interface, ping, ...).

4.3.1.2. Forward

Forward rules manage how Ethernet frames are handled within the broadcast domain. These rules control communication paths, enforce segmentation, and filter unwanted traffic. Forward filtering applies to packets traversing a bridge but not to traffic originating from or destined for the station.

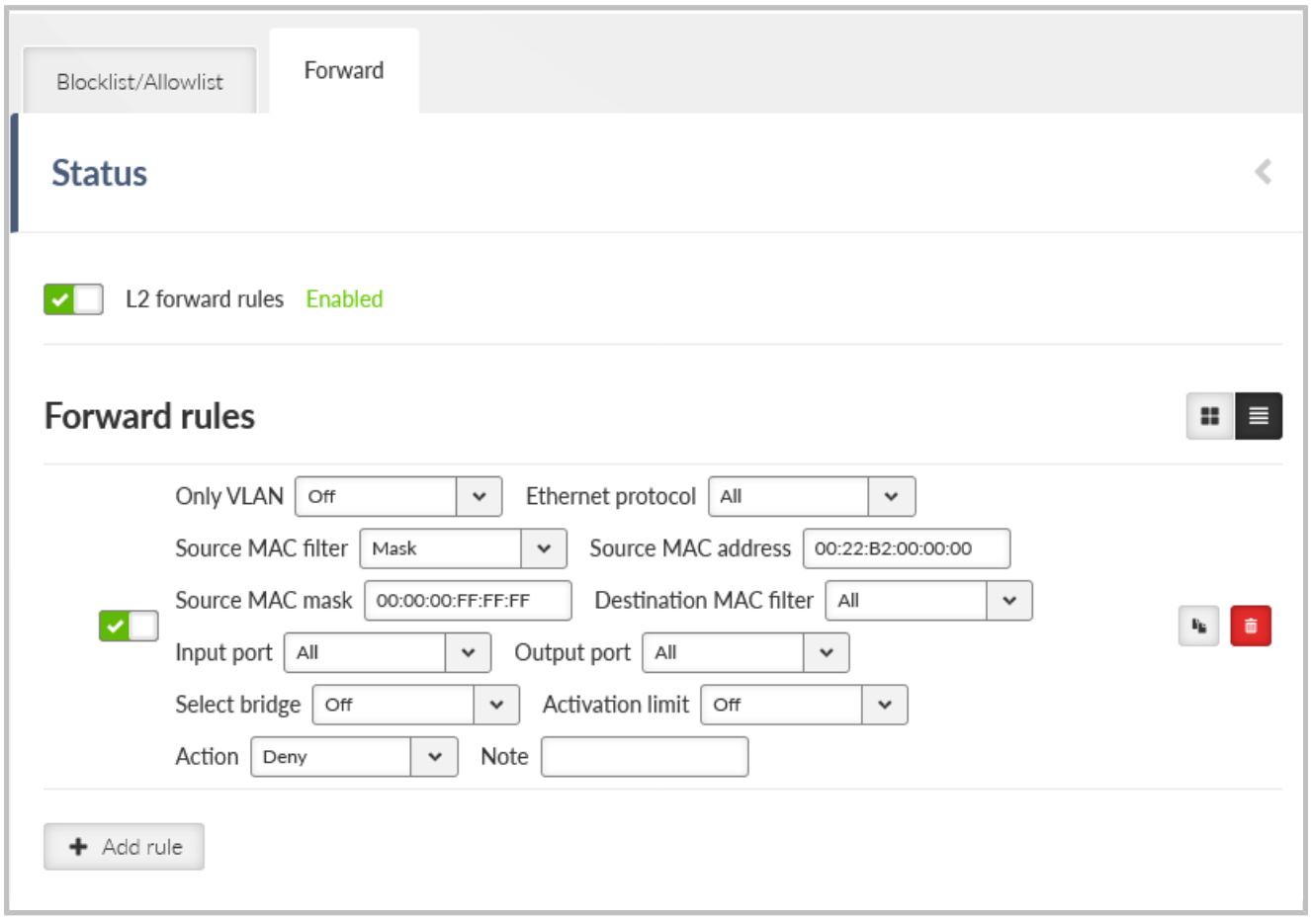


Fig. 4.13: SETTINGS > Firewall > L2 > Forward

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Only VLAN
List box {Off; On}, default = "Off"
Enables packet filtering for a specific VLAN and deep packet inspection.
If enabled:

VLAN
Number (0-4094), default = 1
ID of the filtered VLAN

Ethernet protocol
List box {All; Not VLAN; All VLAN; IPv4; IPv6; ARP; Other}, default = "All"
Filter based on EtherType (protocol carried in the Ethernet frame).

Source MAC filter
List box {All; Mask; Unicasts; Multicasts; Broadcasts}, default = "All"
Enables filtering based on the source MAC address of the packet.
For Mask option:

Source MAC address
Address used to compare against the source MAC address of packets.

Source MAC mask
Mask used to compare against the source MAC address of packets.

Destination MAC filter
List box {All; Mask; Unicasts; Multicasts; Broadcasts}, default = "All"
Enables filtering based on the destination MAC address of the packet.
For Mask option:

Destination MAC address
Address used to compare against the destination MAC address of packets.

Destination MAC mask
Mask used to compare against the destination MAC address of packets.

Input port
List box {All; Radio; All ETH; ETH1; ETH2; GRE L2; OpenVPN L2; Other"}, default = "All"
Filters based on the port that the packet entered the bridge through.
For Other option:

Input port name
String {0–16 char}, default = <empty>
Name of the input port. Must be the name of an existing interface used as a bridge port.

Output port
List box {All; Radio; All ETH; ETH1; ETH2; GRE L2; OpenVPN L2; Other"}, default = "All"
Filters based on the port that the packet exits the bridge through.
For Other option:

Output port name
String {0–16 char}, default = <empty>

Name of the output port. Must be the name of an existing interface used as a bridge port.

Select bridge
List box {Off; On}, default = "Off"
Enables limiting of the rule to a specific bridge. The rule will only be applied to packets that pass through the selected bridge.

Activation limit
List box {Off; On}, default = "Off"
Enables limiting the number of times the rule can be triggered per time unit.
If enabled:

Frame count
Number (1-10000), default = 3
Average packet/activation rate limit per time unit.

Measurement period
List box {Second, Minute, Hour, Day}, default = "Minute"
Time unit for limiting the packet/activation rate.

Burst size
Number (1-10000), default = 3
Initial and maximum number of TBF tokens. After a period of inactivity, TBF allows a burst of traffic to pass through at once. Must be greater than or equal to Frame count.

Action
List box {Deny; Allow}, default = "Deny"
Selects the action to be taken on a packet that matches the configured filter.

4.3.2. Firewall L3

An L3 firewall operates at the network layer, filtering traffic based on IP addresses and protocols. It enables control over data packets as they traverse different networks, allowing administrators to block or permit traffic based on source and destination IPs, port numbers, and protocol types. L3 firewalls are crucial for enforcing inter-network security, managing traffic flow, and protecting against external threats.

4.3.2.1. Forward

Forward rules in an L3 firewall control how IP packets are routed between networks. These rules specify whether traffic should be allowed or blocked as it passes through the router. Packets coming from addresses on the Blocklist are automatically dropped. By applying forward rules, administrators can manage traffic flow, enforce security policies, and prevent unauthorized access between different network segments.

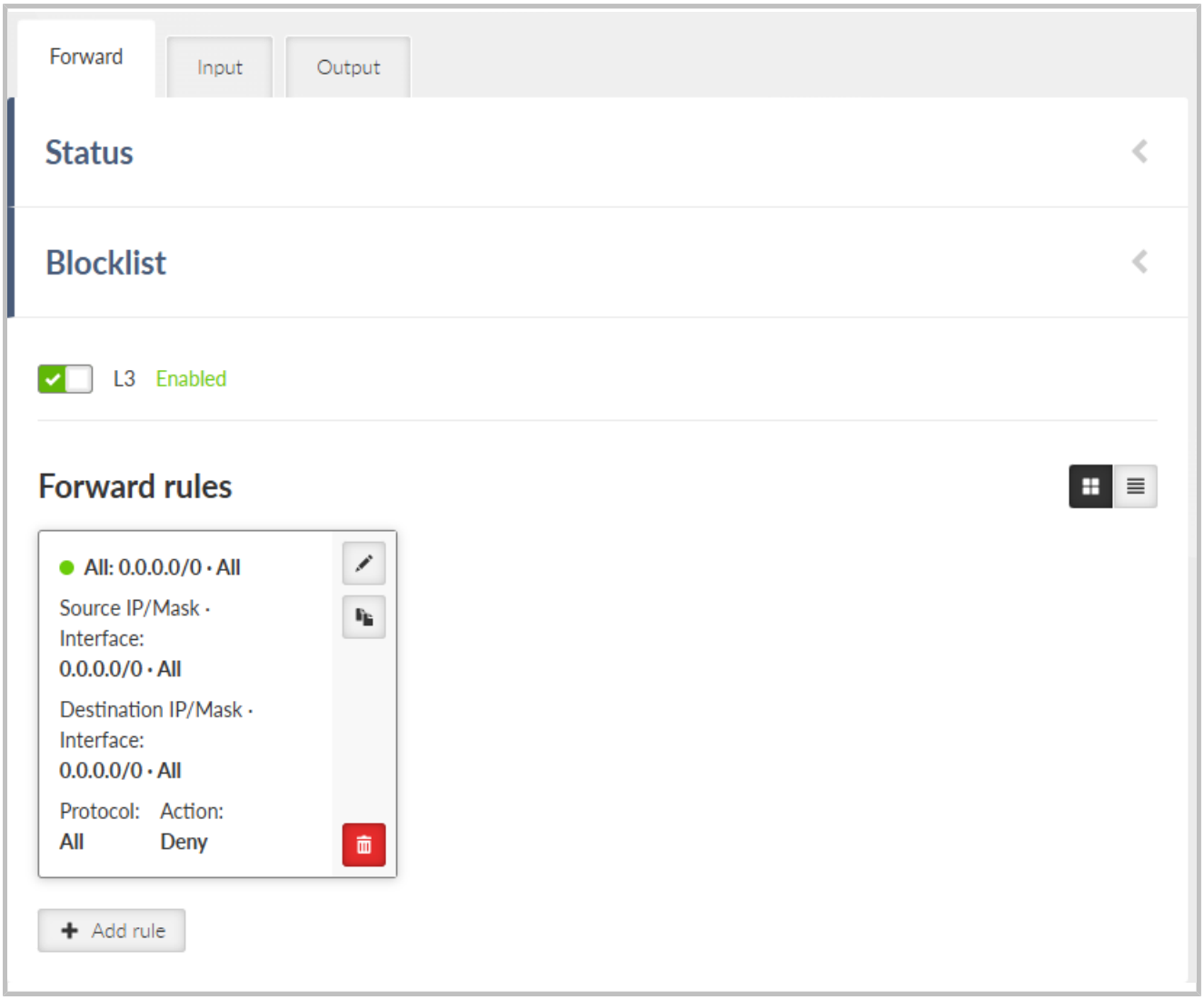


Fig. 4.14: SETTINGS > Firewall > L3

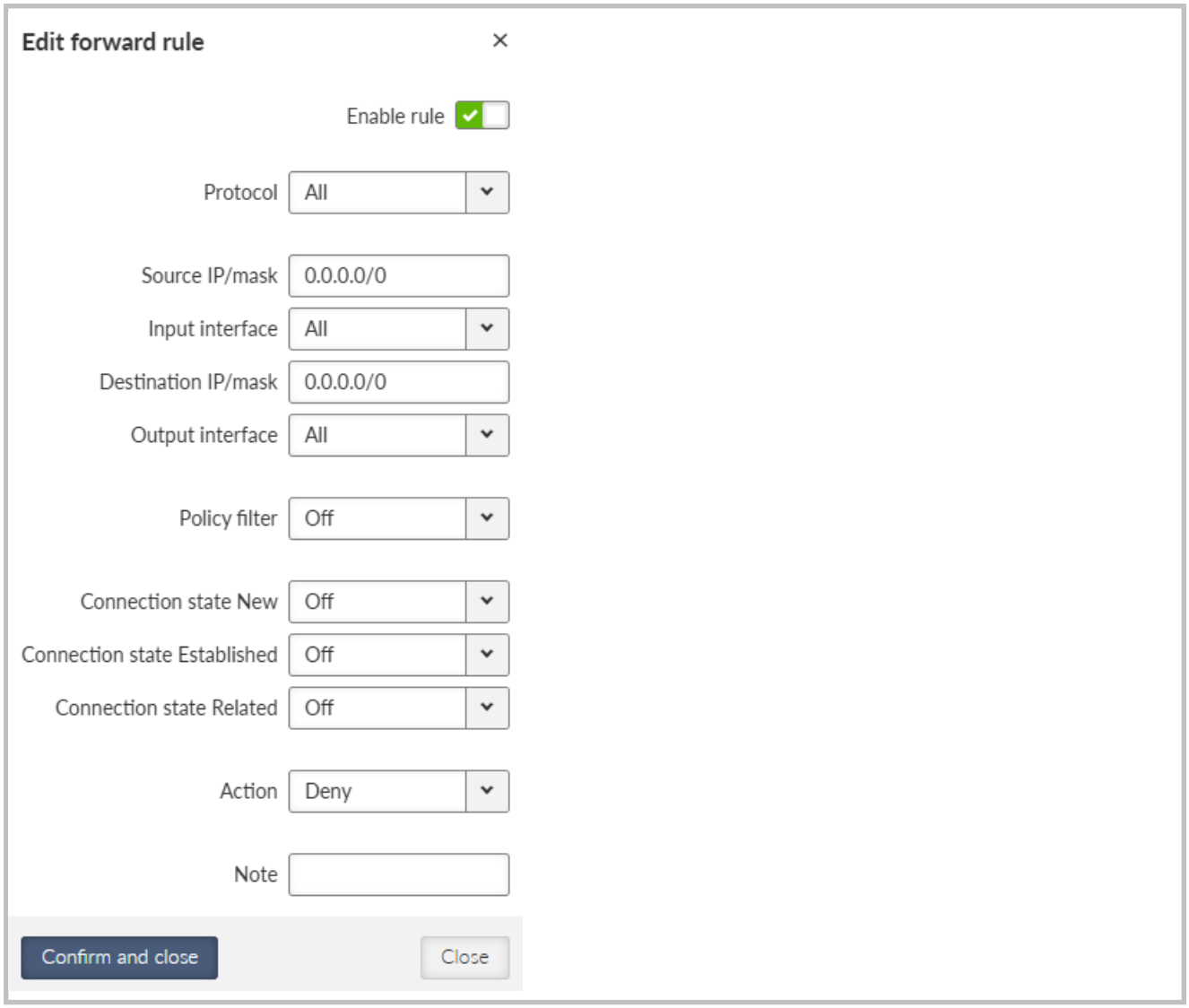


Fig. 4.15: SETTINGS > Firewall > L3 forward

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address. The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Input interface
List box {All; Radio; All ETH; ETH1..ETH2; All serial PPP; PPPoE client; GRE L2; GRE L3; OpenVPN L2; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the input device (interface, port) from which the packet came.

Input interface name
String (0-16 symbols), default = <empty>
The name of the input interface (or bridge port) of the packet.
This parameter occurs only when parameter Input interface is set to "Other".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destionation IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Output interface
List box {All; Radio; All ETH; All serial PPP; PPPoE client; GRE L3; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the output interface from which the packet leaves. Cannot select the bridge port.

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Direction
Listbox: {In (Decapsulation), Out (Encapsulation)}, default = "Out (Encapsulation)"
Filters by packet processing direction.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (decapsulation and encapsulation)
IPsec - The packet will be processed by IPsec

Connection state New
List box {Off; On}, default = "Off"
Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from WaSP network to outside.

Connection state Established
List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from WaSP network to outside.

Connection state Related

List box {Off; On} default = "Off"
A connection related to the "Established" one, e.g. FTP typically uses 2 TCP connections control and data, where data connection is created automatically by using dynamic ports.

Note
Management connection to a remote WaSP may be lost, when another WaSP acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing WaSP (FORWARD chain).

Action

List box {Deny; Allow}, default = "Deny"
Selects the action to perform on a packet that matches the configured filter.

4.3.2.2. Input

Input rules in an L3 firewall regulate how IP packets destined for the router itself are handled. These rules determine whether traffic should be accepted or dropped based on factors like source IP address, protocol, and port number.

Packets coming from addresses on the Blocklist are automatically dropped. Addresses are added to the Blocklist as a result of an Input firewall rule with the Action set to "Deny, Add to Blocklist."

Additionally, the system creates automatic Input rules based on interface settings:

- Management access is limited on individual interfaces according to the "Allow unit management" setting for that interface.
- Remote access is restricted on individual interfaces based on the "Allow Remote access" setting for that interface.

By configuring input rules and interface settings, administrators can ensure robust protection against unauthorized access and direct attacks targeting the device.

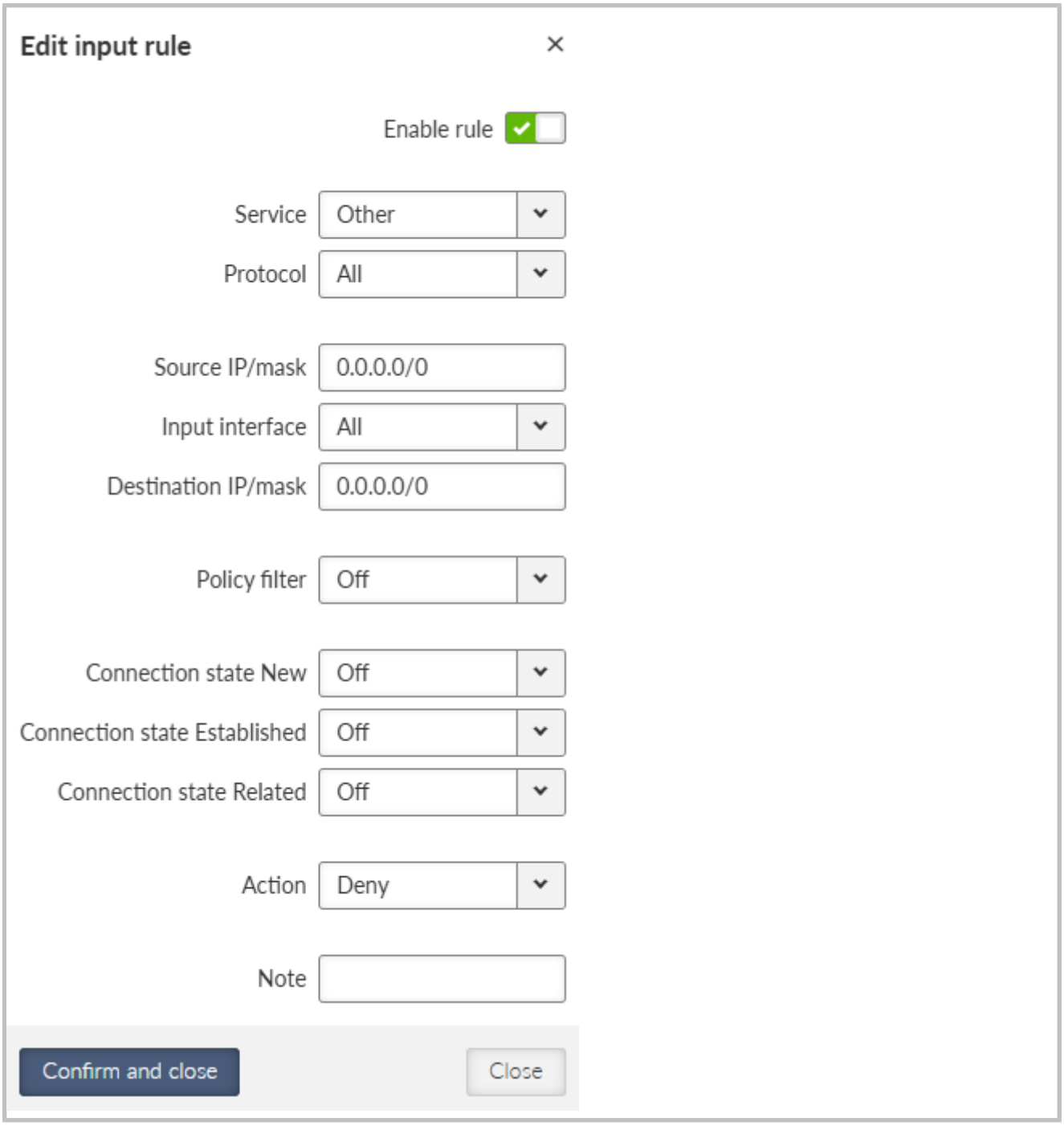


Fig. 4.16: SETTINGS > Firewall > L3 input

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Service
List box {Other; COM1; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Remote access; SNMP; NTP}, default = "Other"

Allows you to select a known service on the station whose protocol and destination port the rule filter will capture.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Input interface
List box {All; All ETH; ETH1..ETH2; All serial PPP; PPPoE client; GRE L2; GRE L3; OpenVPN L2; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the input device (interface, port) from which the packet came.

Input interface name
String (0-16 symbols), default = <empty>
The name of the input interface (or bridge port) of the packet.
This parameter occurs only when parameter Input interface is set to "Other".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destionation IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (decapsulation)
IPsec - The packet will be processed by IPsec

Connection state New

List box {Off; On}, default = "Off"

Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from WaSP network to outside.

Connection state Established

List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from WaSP network to outside.

Connection state Related

List box {Off; On} default = "Off"

A connection related to the "Established" one. e.g. FTP typically uses 2 TCP connections control and data, where data connection is created automatically by using dynamic ports.

Note

Management connection to a remote WaSP may be lost, when another WaSP acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing WaSP (FORWARD chain).

Action

List box {Deny; Allow; Deny, Add to Blocklist}, default = "Deny"

Selects the action to perform on a packet that matches the configured filter.

Deny, Add to Blocklist - all traffic from the particular address will be automatically dropped. Blocklist has limited capacity of 512 addresses. Once its capacity is exceeded, the oldest address is overwritten. Addresses added to the blocklist remain in for one week (604,800s) and are deleted from it afterwards. Change of configuration including firewall, or unit reboot will delete those addresses as well.

4.3.2.3. Output

Output rules in an L3 firewall govern how IP packets originating from the router itself are handled. These rules allow administrators to control traffic sent by the router, specifying whether it should be allowed or blocked based on factors such as destination IP address, protocol, and port number. By configuring output rules, administrators can restrict unnecessary or potentially harmful outbound traffic, enforce security policies, and manage communication initiated by the router.

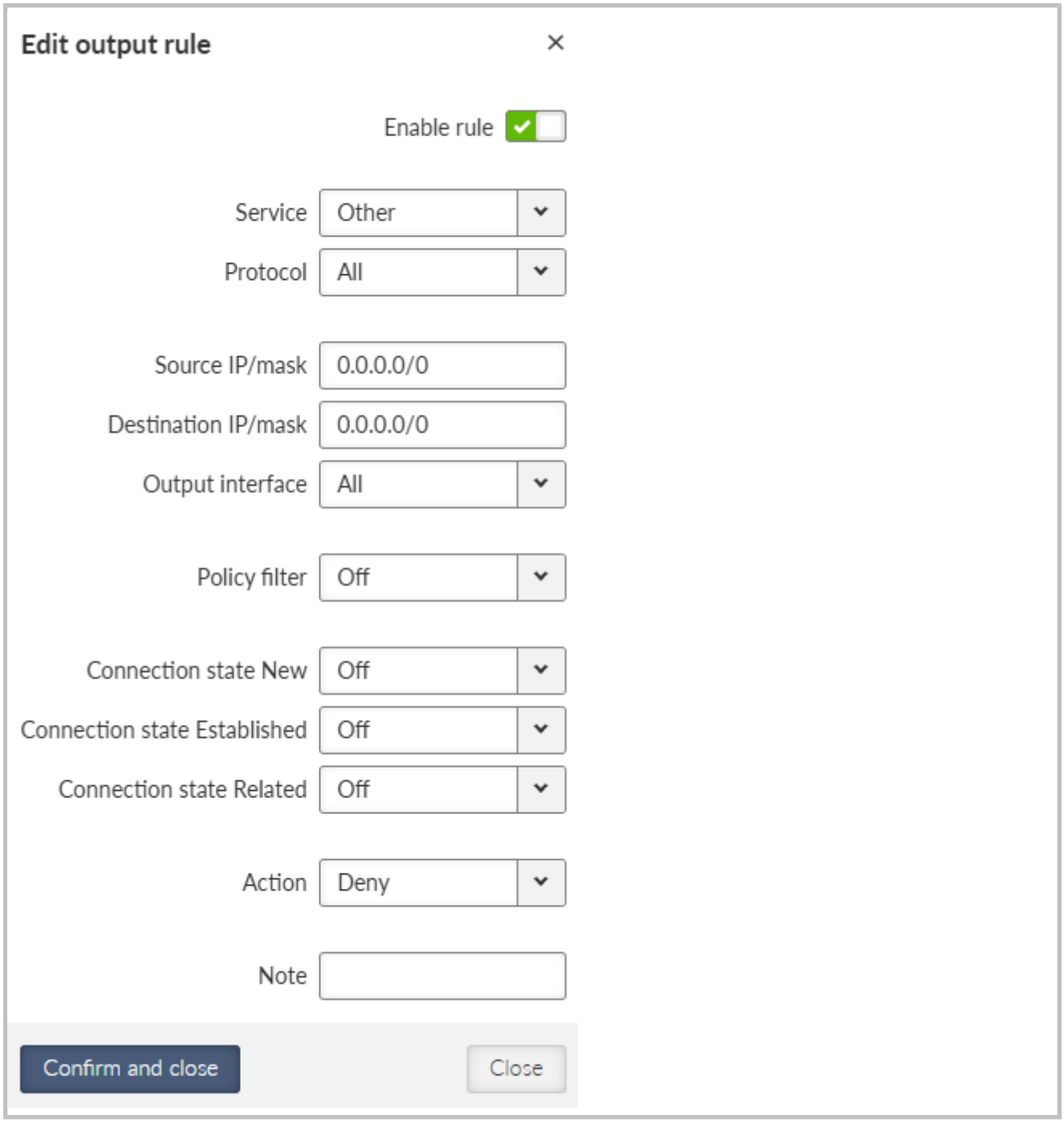


Fig. 4.17: SETTINGS > Firewall > L3 output

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Service
List box {Other; COM1; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Remote access; SNMP; NTP}, default = "Other"
Allows you to select a known service on the station whose protocol and destination port the rule filter will capture.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address. The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destionation IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Output interface
List box {All; All ETH; PPPoE client; GRE L3; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the output interface from which the packet leaves. Cannot select the bridge port.

Output interface name
String (0-16 symbols), default = <empty>
The name of the output interface of the packet.
This parameter occurs only when parameter Input interface is set either to "Other".

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (encapsulation)
IPsec - The packet will be processed by IPsec

Connection state New
List box {Off; On}, default = "Off"
Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from WaSP network to outside.

Connection state Established

List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from WaSP network to outside.

Connection state Related

List box {Off; On} default = "Off"

A connection related to the "Established" one. e.g. FTP typically uses two TCP connections control and data, where data connection is created automatically by using dynamic ports.

Note

Management connection to a remote WaSP may be lost, when another WaSP acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing WaSP (FORWARD chain).

Action

List box {Deny; Allow}, default = "Deny"

Selects the action to perform on a packet that matches the configured filter.

4.3.3. NAT - Network address translation

Network address and port translation (**NAPT**) is a method of mapping an IP address (or port) space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

4.3.3.1. Source NAT

Source Network Address Translation (SNAT) - rewrites the source address and/or port within the leaving connection and performs opposite changes for returning packets.

SNAT:

- Allows to pretend, that the packets come from a device, that performs SNAT.
- Performs during packet output from a device (after routing and filtering in firewall).

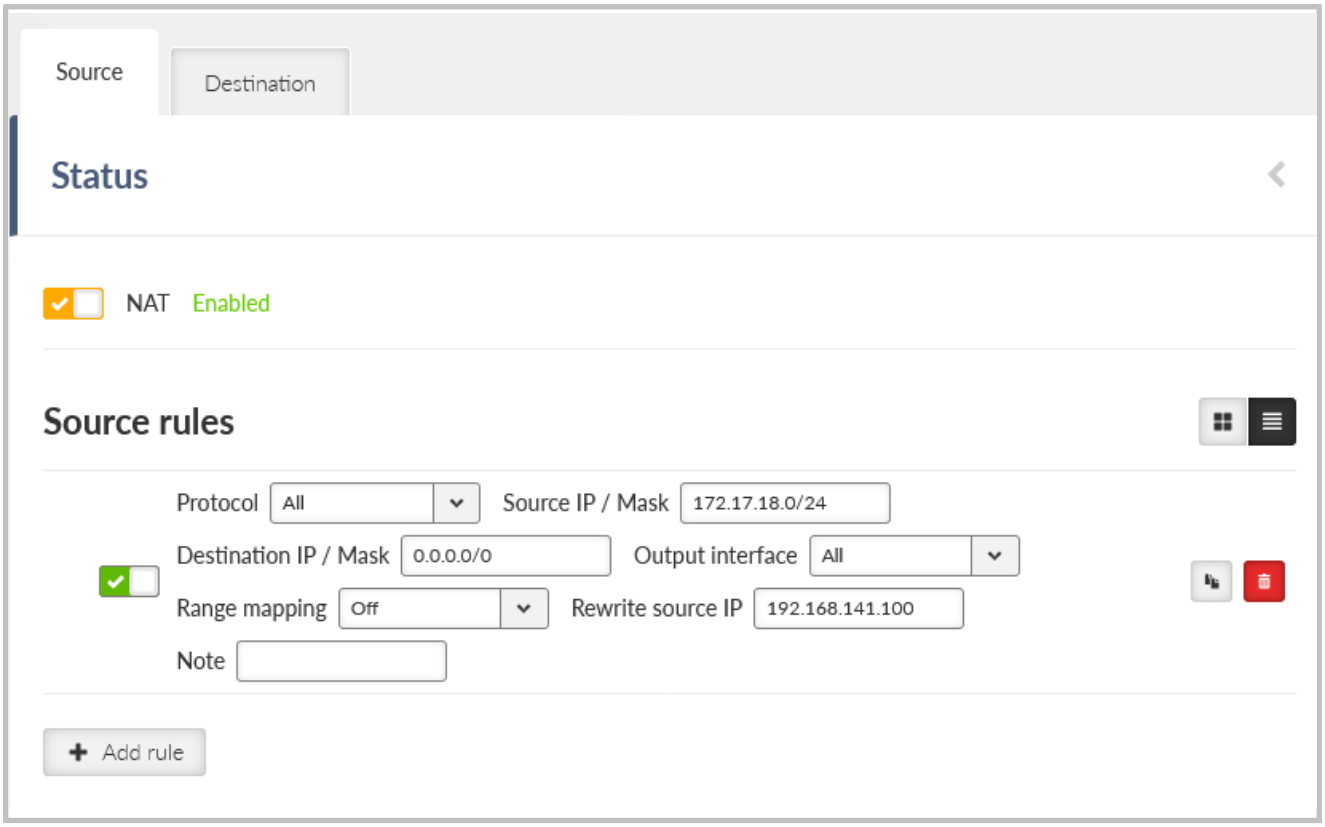


Fig. 4.18: SETTINGS > Firewall > NAT

- Parameters “**Protocol**”, “**Source IP / Mask**”, “**Destination IP / Mask**”, “**Output Interface**”,“**Source port from**”, “**Source port to**”, “**Destination port from**”, “**Destination port to**” and “**Protocol number**” define a filter, which is capturing specified packets. SNAT rule applies for those packets.
- Parameters “**Source port from**”, “**Source port to**”, “**Destination port from**” and “**Destination port to**” occur only if parameter “**Protocol**” is set to “UDP” or “TCP”.
- Parameter “**Protocol number**” occurs only if parameter “**Protocol**” is set to “Other”.

Each individual NAT rule is described by following parameters:

Enable rule
List box {Enable; Disable}, default = "Disable"
Enables / disables all Source NAT rules.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Filters selected protocol. If none of the mentioned values suits, select “Other”.

Protocol number
Number {0 – 255}, default = 1
This parameter occurs only, if parameter “**Protocol**” is set to “Other”.

Source IP / Mask
IP address, default = 0.0.0.0/0
Defines the source IP subnet.

Source port (from) / Source port (to)
Number {0 – 65535}, default = 0
Defines the range of values of source port. Value 0 means, that it is not filtered according to the source port. If only one port is required, set both parameters to the same number. These parameters occur only, if parameter "**Procotol**" is set to "UDP" or "TCP".

Destination IP / Mask
IP address, default = 0.0.0.0/0
Defines the destination IP subnet.

Destination port (from) / Destination port (to)
Number {0 – 65535}, default = 0
Defines the range of values of destination port. Value 0 means, that it is not filtered according to the destination port. These parameters occur only, if parameter "**Procotol**" is set to "UDP" or "TCP".

Output Interface
List box {All; Radio; All ETH; EXT; GRE L3; Hot standby; Other}, default = "All"
Filters selected interfaces.

Output interface name
Has to be set as one of existing interfaces ("radio", the name of LAN (or VLAN) interface, the name of GRE tunnel, etc.). This parameter occurs only, if parameter "**Output Interface**" is set to "Other".

Range mapping
List box {Off; IP address to IP address}, default = "Off"
Off – Source address and (or) port will be replaced by values from parameters "**Rewrite source IP**" and "**Rewrite source port**". This applies only if those parameters are set (they are not set as 0.0.0.0).
IP address to IP address (NETMAP) – Rewriting the Range mapping of source IP address. New source address will contain prefix from parameters "**Rewrite Source IP**" and "**Rewrite Source IP / Mask**". Rest of the source address will be filled by the original source address.

Rewrite source IP
IP address, default = 0.0.0.0/0
Defines a new source address. Value 0.0.0.0/0 means, that the source address is not changed.

Rewrite source port
Number {0 – 65535}, default = 0
Defines a new source port (rewriting multiple defined ports into one). Value 0 means, that the source port is not changed.

Note
Optional comment.

4.3.3.2. Destination NAT

Destination Network Address Translation (DNAT) - rewrites the destination address and/or port within incoming connection and performs opposite changes for returning packets.

DNAT:

- Allows to redirect connection destination to a device, that performs DNAT.
- Performs during packet input to a device (before redirecting and filtering in firewall).

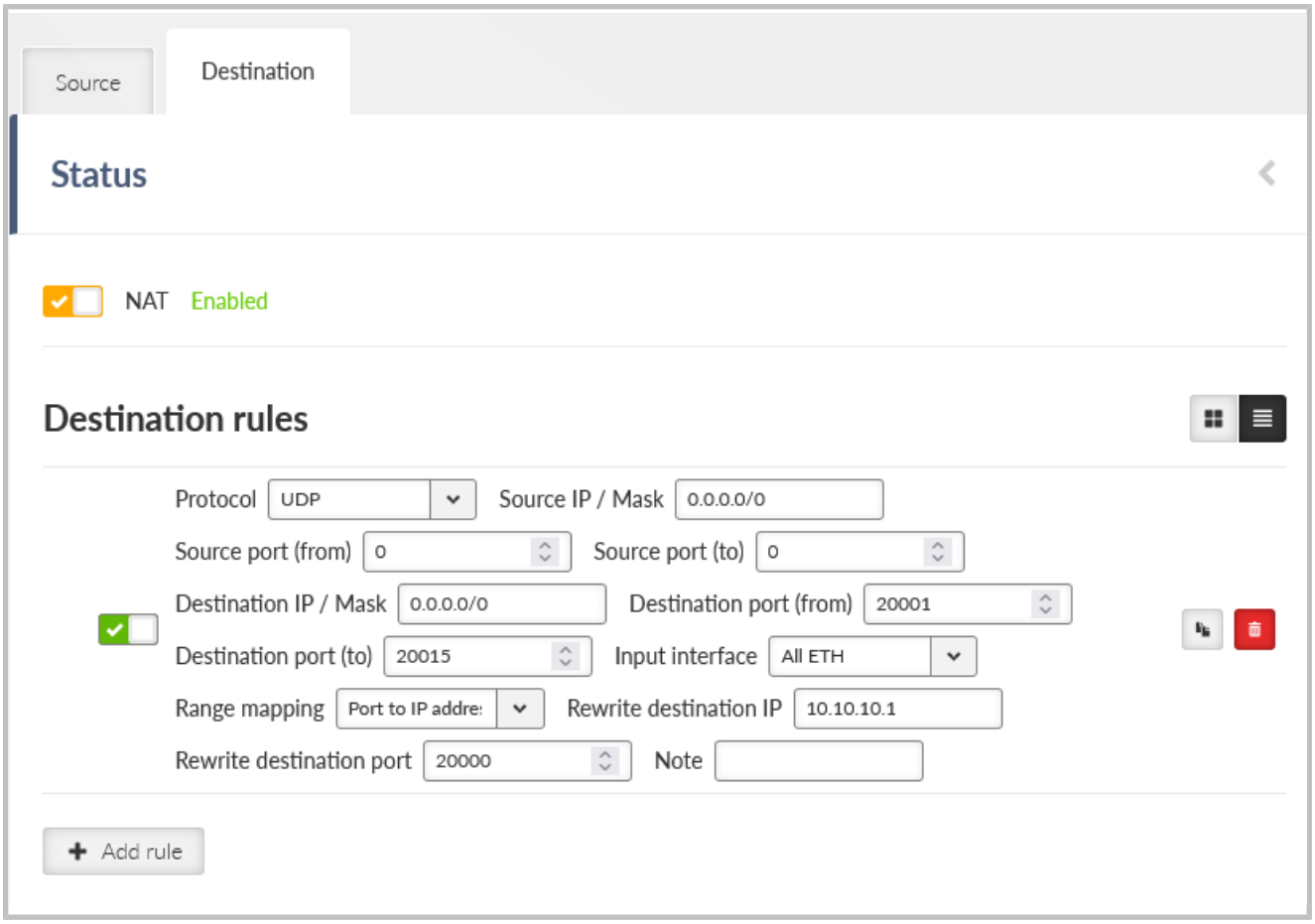


Fig. 4.19: SETTINGS > Firewall > NAT > Destination

- Parameters “**Protocol**”, “**Source IP / Mask**”, “**Destination IP / Mask**”, “**Output Interface”**,“**Source port from**”, “**Source port to**”, “**Destination port from**”, “**Destination port to**” and “**Protocol number**” define a filter, which is catching specified packets. SNAT rule applies for those packets.
- Parameters “**Source port from**”, “**Source port to**”, “**Destination port from**” and “**Destination port to**” occur only if parameter “Protocol” is set to “UDP” or “TCP”.
- Parameter “**Protocol number**” occurs only if parameter “**Protocol**” is set to “Other”.

Each individual NAT rule is described by following parameters:

Enable rule
List box {Enable; Disable}, default = "Disable"
Enables / disables all Destination NAT rules.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Filters selected protocol. If none of the mentioned values suits, select “Other”.

Protocol number
Number {0 – 255}, default = 1
This parameter occurs only, if parameter “**Protocol**” is set to “Other”.

Source IP / Mask
IP address, default = 0.0.0.0/0

Defines the source IP subnet.

Source port (from) / Source port (to)
Number {0 – 65535}, default = 0
Defines the range of values of source port. Value 0 means, that it is not filtered according to the source port. If only one port is required, set both parameters on the same number. These parameters occur only, if parameter “**Procotol**” is set to “UDP” or “TCP”.

Destination IP / Mask
IP address, default = 0.0.0.0/0
Defines the destination IP subnet.

Destination port (from) / Destination port (to)
Defines the range of values of destination port. Value 0 means, that it is not filtered according to the destination port. These parameters occur only, if parameter “**Procotol**” is set to “UDP” or “TCP”.

Input interface
List box {All; Radio; All ETH; EXT; GRE3; Hot standby; Other}, default = "All"
Filters selected interfaces.

Input interface name
Has to be set as one of existing interfaces (“radio”, the name of LAN (or VLAN) interface, the name of GRE tunnel, etc.). This parameter occurs only, if parameter “**Input Interface**” is set to “Other”.

Range mapping
List box {Off; IP address to IP address}, default = "Off"

- Off – Destination address and (or) port will be replaced by values from parameters “**Rewrite destination IP**” and “**Rewrite destination port**”. This will apply only if those parameters are set (they are not set as 0.0.0.0).

- IP address to IP address (NETMAP) – Rewriting the Range mapping of source IP address. New source address will contain prefix from parameters “**Rewrite Source IP**” and “**Rewrite Source IP / Mask**”. Rest of the source address will be filled by the original source address.

- Port to IP address (PORTMAP): Range mapping of destination ports (parameters “**Destination port from**”, “**Destination port to**”). New range mapping of destination ports origins in parameter “**Rewrite destination IP**”. It can be additionally overwritten to parameter “**Rewrite destination port**”.
  Explanation of non-typical and interesting parameters:

  Destination port (from) and Destination port (to)
  DNAT rule applies to UDP data with destination ports within the 20001-20015 range only

  Input interface
  Data must be received on any ETH port

  Range mapping
  Set to “Port to IP address” - i.e., destination ports change the destination IP address(es) accordingly.

  Rewrite destination IP and Rewrite destination port
  Set to IP 10.10.10.1 and port 502 - resulting in a range of IPs 10.10.10.1 - 10.10.10.15 due to Destination ports of received UDP data in a range of 20001-20015 (15 ports = 15 IP addresses). A new port is always 20000 (i.e., DNP3 default port).

Rewrite destination IP

IP address, default = 0.0.0.0/0

Defines a new destination address. Value 0.0.0.0/0 means, that the destination address is not changed.

Rewrite destination port

Number {0 – 65535}, default = 0

Defines a new destination port (rewriting multiple defined ports into one). Value 0 means, that the destination port is not changed.

Note

Optional comment.

Note

FTP connection is a special type of TCP with multiple sessions being opened and internal functionality. If you configure DNAT for the connected FTP server, enable the “FTP connection tracker” parameter and specify a correct port (default is 21). These parameters can only be set in the Advanced menu.

4.3.3.3. Cooperation with other services

- MASQUERADE rule for Cellular connection has lower priority that user NAT (it is tested after the NAT), thus it is possible to create exceptions in NAT settings.
- By using DNAT it is possible to intercept a passing connection and redirect it into the WaSP (similar to a proxy behavior).
- For redirection
  - Local IP address will be filled into “**Rewrite destination IP**” parameter.
  - Service port, to which is the local address being redirected will be filled into “**Rewrite destination port**” parameter.

NAT and IPsec

- DNAT can be used before packing a packet into the IPsec. For more information see *Section 4.4.1.3.3, “Interaction with DNAT”*.
- SNAT works on packets unpacked from IPsec.
- SNAT can be used before packing a packet into the IPsec (parameter “**Output interface**” must be set to “All”)
- Rules of SNAT and MASQUERADE (from Cellular) changes packets addresses before capturing by IPsec traffic selector.

4.4. VPN

VPN (Virtual Private Network) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

Note

OpenVPN and IPsec are not suitable for the narrowband radio networks with the capacity of several kb/s or Mb/s. Both VPN protocols are designed for fast speed Ethernet connections of 100-1000 Mb/s. If you need to encrypt the Radio channel, use its AES256 Encryption option. Utilize OpenVPN or IPsec on Ethernet or cellular interfaces. On the other hand, both VPN options will work on the Radio channel as well, but could slow down the overall network operation.

4.4.1. IPsec

Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec is an end-to-end security scheme operating within the Internet Layer of the Internet Protocol Suite. IPsec is recognized as a secure, standardized and well-proven solution by the professional public.

There are 2 modes of operation, WaSP offers both the Tunnel mode and the Transport mode. In Tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet (ESP – Encapsulating Security Payloads) with a new IP header. In Transport mode, only the payload of the original IP packet is encrypted and authenticated. The original IP header remains intact, allowing for direct routing, while the data itself is secured using AH or ESP protocols.

Symmetrical cryptography is used to encrypt the packets. The symmetric keys must be safely delivered to the peer. In order to maintain a secure connection, symmetric keys must be regularly exchanged. The protocol used for secure key exchange is IKE (Internet Key Exchange). Both IKE version 1 and the newer version 2 are available in WaSP.

IKE protocol communication with the peer is established using UDP frames on port 500. However, if NAT-T (NAT Traversal) or MOBIKE (MOBile IKE) are active, the UDP port 4500 is used instead.

Note

NAT-T is automatically recognized by IPsec implementation in WaSP.

The IPsec tunnel is provided by Security Association (SA). There are 2 types of SA:

- IKE SA: IKE Security Association providing SA keys exchange with the peer.
- CHILD SA: IPsec Security Association providing packet encryption.

Every IPsec tunnel contains 1 IKE SA and at least 1 CHILD SA. In WaSP can be set maximum of 24 IKE_SA and 48 CHILD_SA (TS).

Link partner (peer) secure authentication is assured using Pre-Shared Key (PSK) authentication method: Both link partners share the same key (passphrase).

As and when the CHILD SA expires, new keys are generated and exchanged using IKE SA.

As and when the IKE SA version IKEv1 expires - new authentication and key exchange occurs and a new IKE SA is created. Any CHILD SA belonging to this IKE SA is re-created as well.

As and when the IKE SA version IKEv2 expires one of two different scenarios might occur:

- If the re-authentication is required - the behavior is similar to IKEv1 (see above).
- It the re-authentication is not required - only new IKE SA keys are generated and exchanged.

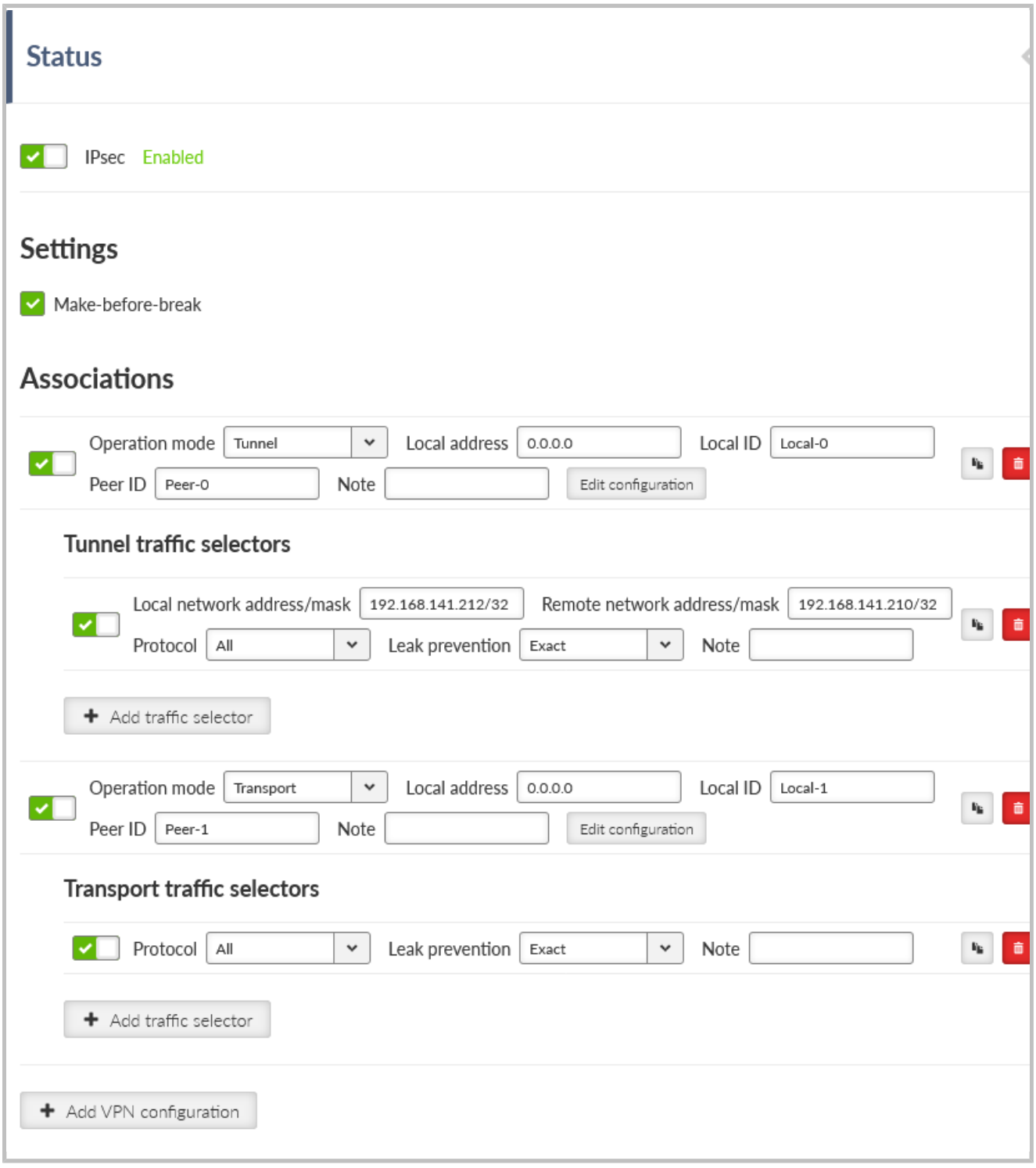


Fig. 4.20: SETTINGS > VPN > IPsec

IPsec
{Enable; Disable}, default = "Disable"

IPsec system turning On/Off
There can be a maximum of 16 active CHILD SA (in total over all Active IKE SA).
Every "Active" line must have an equivalent on the peer side with reversed "Local network..." and "Remote network..." fields.
"Local network..." and "Remote network..." fields must contain different address ranges and must not interfere with the USB service connection (10.9.8.7/28) or internal connection to FPGA (192.0.2.233/30).
Each "Active" Traffic selector in the configuration table must be unique.

4.4.1.1. IPsec settings

Make-before-break
{On; Off}, default = "Off"
This parameter is valid for all IKE SA using IKEv2 with re-authentication. A temporary connection breaks during IKE_SA re-authentication is suppressed by this parameter. This function may not operate correctly with some IPsec implementations (on peer side).

4.4.1.2. IPsec associations

To further configure IPsec VPN tunnel, click the **Add VPN configuration** button.

Operation mode
List box {Tunnel; Transport}, default = "Tunnel"
Selects IPsec mode

Note
The Tunnel mode is usually used for site-to-site and host-to-site connections. The Transport mode is used for host-to-host connection and very often combined with GRE and dynamic routing.

Add / Edit IPsec VPN tunnel associations
Every item in the table represents one IKE SA. There can be a maximum of 24 active IKE SA (limited by system resources).

Local address

IP address, default = "0.0.0.0"

IP address used as the source address for IKE negotiation. If specified, must be a valid local address.

When left at 0.0.0.0 the Local address becomes dynamic.

Peer address

IP address, default = "0.0.0.0"

IP address of the peer running the IKE daemon that will be negotiated with. It must not be the same as Local address.

Local ID

IP address or FQDN (Fully Qualified Domain Name), default = "Local-0"

IP address or FQDN used as the Local side identification. It must be the same as "Peer ID" of the IKE peer.

Peer ID

IP address or FQDN (Fully Qualified Domain Name), default = "Peer-0"

IP address or FQDN used as the IKE peer identification. It must be the same as "Local ID" of the IKE peer. The "Peer ID" must be unique in the whole table.

Start state

List box {Passive; On demand; Start}, default = "Passive"

Passive - the connection is not established, it is waiting for the other side.

On Demand - The connection will start to establish when a packet tries to pass through it.

Start - the connection is established immediately.

MOBIKE

List box {On; Off}, default = "On"

Enables MOBIKE for IKEv2 supporting mobility or migration of the tunnels. Please note IKE is moved from port 500 to port 4500 when MOBIKE is enabled. The peer configuration must match. It is strongly recommended to use MOBIKE mode in case of routing the traffic over the Cellular interface.

Dead Peer Detection

List box {On; Off}, default = "Off"
Detection of lost connection with the peer. IKE test packets are sent periodically. When packets are not acknowledged after several attempts, the connection is closed (corresponding actions are initialized). In the case when Detection is not enabled, a connection loss is discovered when regular key exchange process is initiated.

DPD period [s]

Number {5 - 28800}, default = 30
Dead Peer Detection check period.
This parameter is available only if parameter **Dead Peer Detection** is set to "On".

DPD action

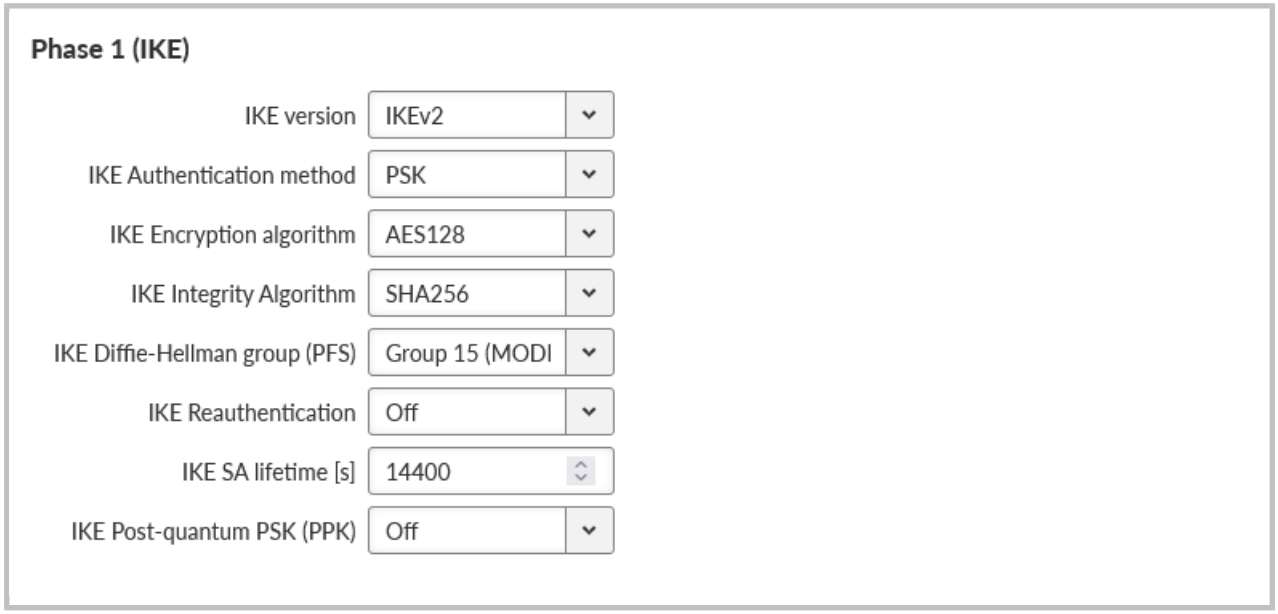
List box {Clear; Hold; Restart}, default = "Hold"
One of three connection states automatically activated when connection loss is detected:
Clear – connection is closed and waiting
Hold – connection is closed. Connection is established when first packet transmission through tunnel is attempted.
Restart – connection is established immediately
This parameter is available only if parameter **Dead Peer Detection** is set to "On".

Management mode

List box {Off; Master; Slave}, default = "Off"
Selects how to manage the IPsec association.
Master - Managed by the Link Manager. Defines the Traffic selector of the tunnel.
Slave - Managed by the Link Manager. Takes over Traffic selectors from the Master Association.
This parameter is available only if parameter **Link management** is set to "On".

Phase 1 IKE

Parameters related to IKE SA (IKE Security Association) provide SA keys exchange with the peer.



IKE version

List box {IKEv2, IKEv1}, default = "IKEv2"
IKE version selection.
Must match the settings on the peer.

IKE Authentication method

List box {PSK}, default = "PSK"
Peer authentication method. Peer configuration must match.
The "main mode" negotiation is the only option supported. The "aggressive mode" is not supported; it is recognized as unsafe when combined with PSK type of authentication.

IKE Encryption algorithm

List box {3DES (legacy); AES128; AES192; AES256; AES128CCM (AEAD); AES192CCM (AEAD); AES256CCM (AEAD); AES128GCM (AEAD); AES192GCM (AEAD); AES256GCM (AEAD); ChaCha20Poly1305 (AEAD)}, default = "AES128"
IKE SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

IKE Integrity Algorithm

List box {MD5 (legacy); SHA1 (legacy); SHA256; SHA384; SHA512}, default = "SHA256"
IKE SA integrity algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

IKE Diffie-Hellman group (PFS)

List box {None (legacy); Group 2 (MODP1024, legacy); Group 5 (MODP1536, legacy); Group 14 (MODP2048); Group 15 (MODP3072); Group 25 (ECP192); Group 26 (ECP224); Group 19 (ECP256); Group 20 (ECP384); Group 21 (ECP521); Group 27 (ECP224BP); Group 28 (ECP256BP); Group 29 (ECP384BP); Group 30 (ECP512BP); Group 31 (X25519); Group 32 (X448)}, default = "Group 15 (MODP3072)"
The PFS (Perfect Forward Secrecy) feature is performed using the Diffie-Hellman group method.
PFS increases IKE SA key exchange security. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.
The higher the Diffie-Hellman group, the higher the security but also the higher the network and CPU load.

IKE Reauthentication

List box {On; Off}, default = "Off"
This parameter is valid if IKEv2 is used. It determines the next action after IKE SA has expired.
When enabled: the new IKE SA is negotiated including new peer authentication. When disabled: only the new keys are exchanged.

IKE SA lifetime [s]

Number {180 – 86400}, default = 14400 s (4 hours)
Time of SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%.
Unfortunately, the more frequent the key exchange, the higher the network and CPU load.

Note
If low capacity channel is used, the WaSP's channel load can affected during the key exchange process.

IKE Post-quantum PSK (PPK)

List box {On; Off}, default = "Off"

Enables additional protection using PPK when using IKEv2.

IKE PPK ID

String {0–64 char}, default = <empty>

PPK key identifier, which can be an FQDN. It must not be empty or the same as the identifier in another IKE SA. It is used to identify and select the PPK key between peers, and they must have the same identifier.

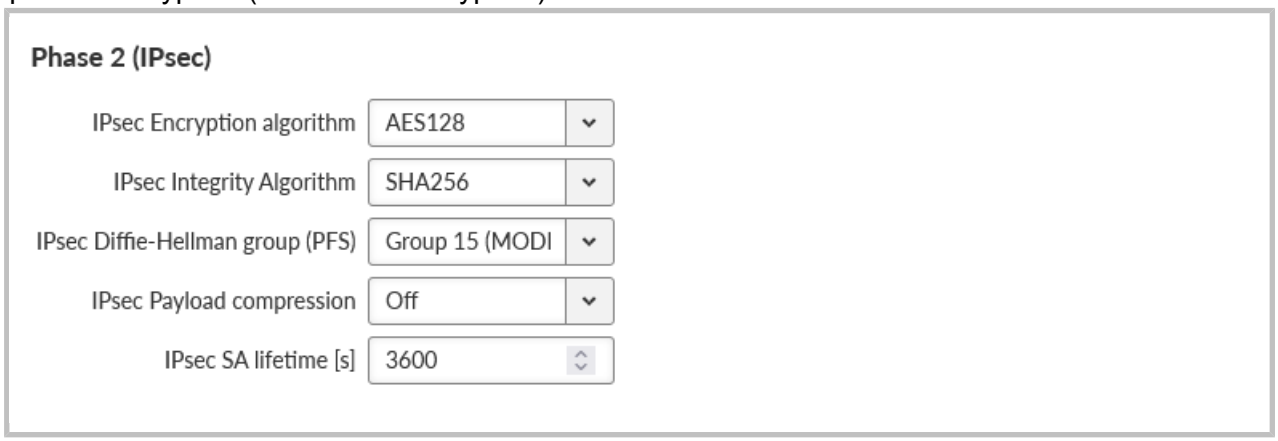
IKE PPK KEY ID

List box {None; Radio Encryption Key}, default = "None"

Key identifier in the keyring. The key must exist and be populated with the type 'psk' and a length of at least 32B (256 bits).

Phase 2 – IPsec

Certain parameters are shared by all subordinate CHILD SA. IPsec Security Association provides packet encryption (user traffic encryption).



Encryption algorithm

List box {3DES (legacy); AES128; AES192; AES256}, default = "AES128"

IKE CHILD SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

IPsec Integrity algorithm

List box {MD5 (legacy); SHA1 (legacy); SHA256; SHA384; SHA512}, default = "SHA256"

IKE CHILD SA integrity algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

IPsec Diffie-Hellman group (PFS)

List box {None (legacy); Group 2 (MODP1024, legacy); Group 5 (MODP1536, legacy); Group 14 (MODP2048); Group 15 (MODP3072); Group 25 (ECP192); Group 26 (ECP224), Group 19 (ECP256); Group 20 (ECP384); Group 21 (ECP521); Group 27 (ECP224BP); Group 28 (ECP256BP); Group 29 (ECP384BP); Group 30 (ECP512BP); Group 31 (X25519); Group 32 (X448)}, default = "Group 15 (MODP3072)"

The PFS (Perfect Forward Secrecy) feature is performed using the Diffie-Hellman group method.

PFS increases IKE CHILD SA key exchange security. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

The higher the Diffie-Hellman group, the higher the security but also the higher the network and CPU load.

Payload compression

List box {On; Off}, default = "Off"

This parameter enables payload compression. This takes place before encryption. Peer configuration must match.

IPsec SA lifetime [s]

Number {180 – 86400}, default = 3600

Time of CHILD SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%. The SA lifetime for CHILD SA is normally much shorter than SA lifetime for IKE SA because the CHILD SA normally transfers much more data than IKE SA (key exchange only). Changing the keys serves as protection against breaking the cypher by analyzing big amounts of data encrypted by the same cypher.

Note

If low capacity channel is used, the WaSP's channel load can affected during the key exchange process.

PSK

PSK (Pre-shared key) authentication is used for IKE SA authentication. The relevant peer is identified using it's "Peer ID". The key must be the same for both local and peer side of the IPsec.

Mode

List box {Passphrase; Key ID}, default = "Passphrase"

Passphrase

The PSK key is entered as a passphrase. An empty passphrase is not allowed (max. length is 128 characters). Passphrase for the FW version 2.1.1.0 must not contain any unsupported characters. Unsupported characters are: ", `, \, $, ;. The full UTF-8 character set is available since FW 2.1.2.0.

Note

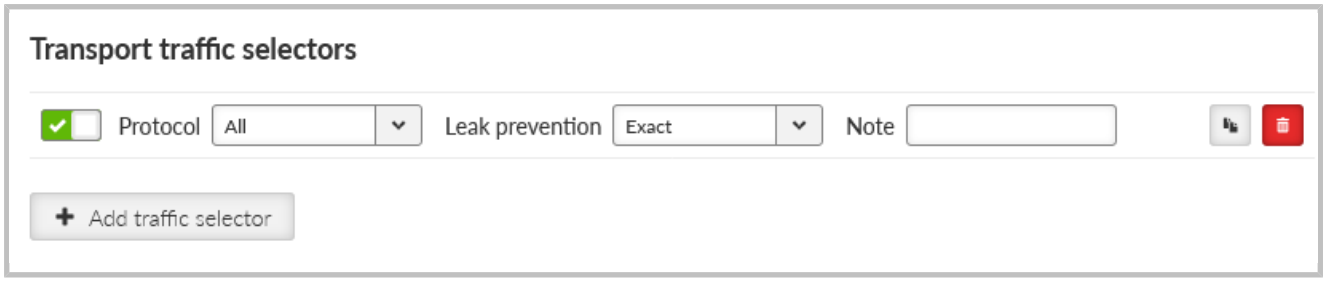
If the passphrase starts with the characters 0x or 0s, then the connection between WaSP with FW 2.1.2.0 (and newer) and WaSP with FW 2.1.1.0 (and older) will not be established. Likewise, any other device that writes the passphrase into its configuration as a plain string (not 'hexa' or 'base64' encoded).

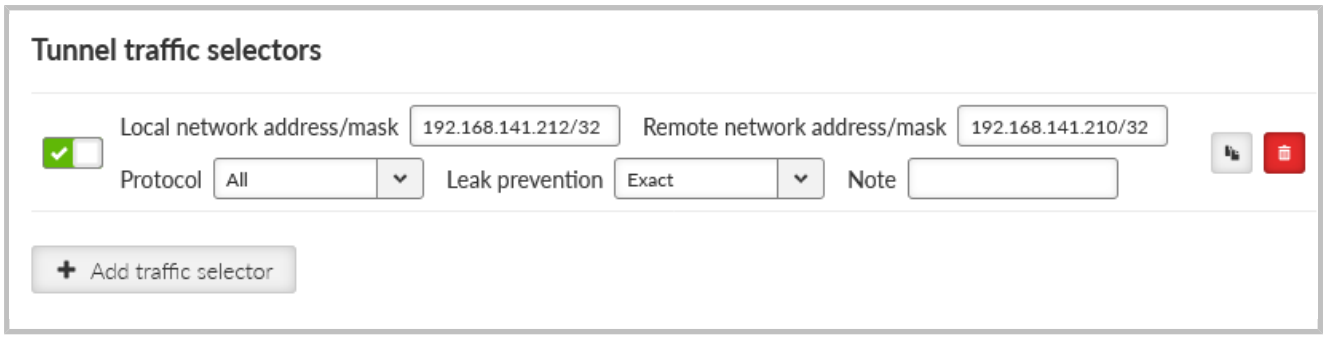
Key

It is possible to set 256 bits long Key instead of Passphrase. This parameter occurs only, if parameter **Mode** is set to "Key".

4.4.1.2.1. Transport/Tunnel Traffic selectors

Defines which traffic is forwarded to the IPsec tunnel. The rule that defines this selection matches an incoming packet to "Local network ..." and "Remote network ..." address ranges.





Local network address / Mask
IP address/Mask, default = "0.0.0.0/32"
Source IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

Remote network address / Mask
IP address/Mask, default = "0.0.0.0/32"
Destination IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Defines the transport protocol of packets which will be caught and encrypted.

Protocol number
Number {1 – 255}, default = 1
Defines the number of the transport protocol of packets which will be caught and encrypted. This parameter is available only if parameter **Protocol** is set to "Other".

Leak prevention
List box {Off; Exact; Paranoid}, default = "Exact"
The level of automatic protection against leaking or receiving unencrypted traffic.
Off - No automatic protection rules. The user must write his own in the L3 firewall.
Exact - Automatic rules exactly copy the CHILD SA settings.
Paranoid - For input/forward rules it's the same as Exact. For output, the automatic rules are stricter because they do not filter by the source address of the packet.

4.4.1.3. Cooperation with other services

4.4.1.3.1. Automatically generated routing rules

For Tunnel mode, a special IPsec routing table is created to correctly fill in the source IP address of packets sent from the unit over IPsec.

For each traffic selector (CHILD SA), the service tries to find a local IP address that matches the address and mask of the local part of the selector. If such an address exists, an auxiliary routing rule is created in the IPsec table that has the address and mask of the remote part of the selector as the destination and the found local address as the local preferred source address. With this rule, the locally generated packets will have addresses that match the CHILD SA selector and will be encrypted.

At the same time, the existence of a routing rule for the packet is ensured. If the routing rule did not exist, the packet would be dropped before being captured and encrypted by IPSec.

Note

If the selector is limited to a specific protocol, however, a routing rule will not be created because it would cover all protocols, including traffic that the selector does not capture.

User routing is required for Transport mode; without it, the IKE SA association could not be established. This mode does not use the special IPsec routing table.

4.4.1.3.2. Manually created firewall rules

A user-defined firewall filters packets before or after encryption in IPsec. If automatic protection against leakage of unencrypted traffic is disabled, custom protection rules (**Policy filter**) can be applied.

Handwritten protection rules must prevent

Sending traffic to be encrypted as unencrypted (data leakage).
Receiving unencrypted traffic that should have been encrypted (data insertion).

Tunnel mode

INPUT - For each traffic selector (CHILD SA) a rule discarding traffic with **Policy** “None” and with swapped address ranges.
OUTPUT - For each traffic selector (CHILD SA) a rule discarding traffic with **Policy** “None” and with the same address ranges.
FORWARD - For each traffic selector (CHILD SA) 2 rules:
Discarding traffic with **Policy** “None” and **Direction** “Out (Encapsulation)” and with the same address ranges.
Discarding traffic with **Policy** “None” and **Direction** “In (Decapsulation)” and with swapped address ranges.

Transport mode

INPUT - For each traffic selector (CHILD SA), a rule to discard traffic with a **Policy** set to “None” and with a source address of the IPsec peer address and a destination address of the IPsec local address.
OUTPUT - For each traffic selector (CHILD SA), a rule to discard traffic with a **Policy** set to “None” and with a source address of the IPsec local address and a destination address of the IPsec peer address.

4.4.1.3.3. Interaction with DNAT

If IPsec captures packets which were modified by DNAT, routing rules automatically created by IPsec rules will not apply to them, because DNAT rewrites their destination address. Therefore a new static routing rule must be created (SETTINGS > Routing > Static) for those packets.

4.4.2. GRE

4.4.2.1. GRE L2

GRE L2 tunnel is interconnected to the bridge (LAN interface) as one of the bridge's port, it captures Ethernet frames of the bridge and sends them to the other end of the tunnel. It enables to build bridge via the complex network and combine the local partial networks to one network.

GRE L2 tunnel can be used to tunnel the Q-in-Q and IPv6 traffic over the WaSP IPv4 network.

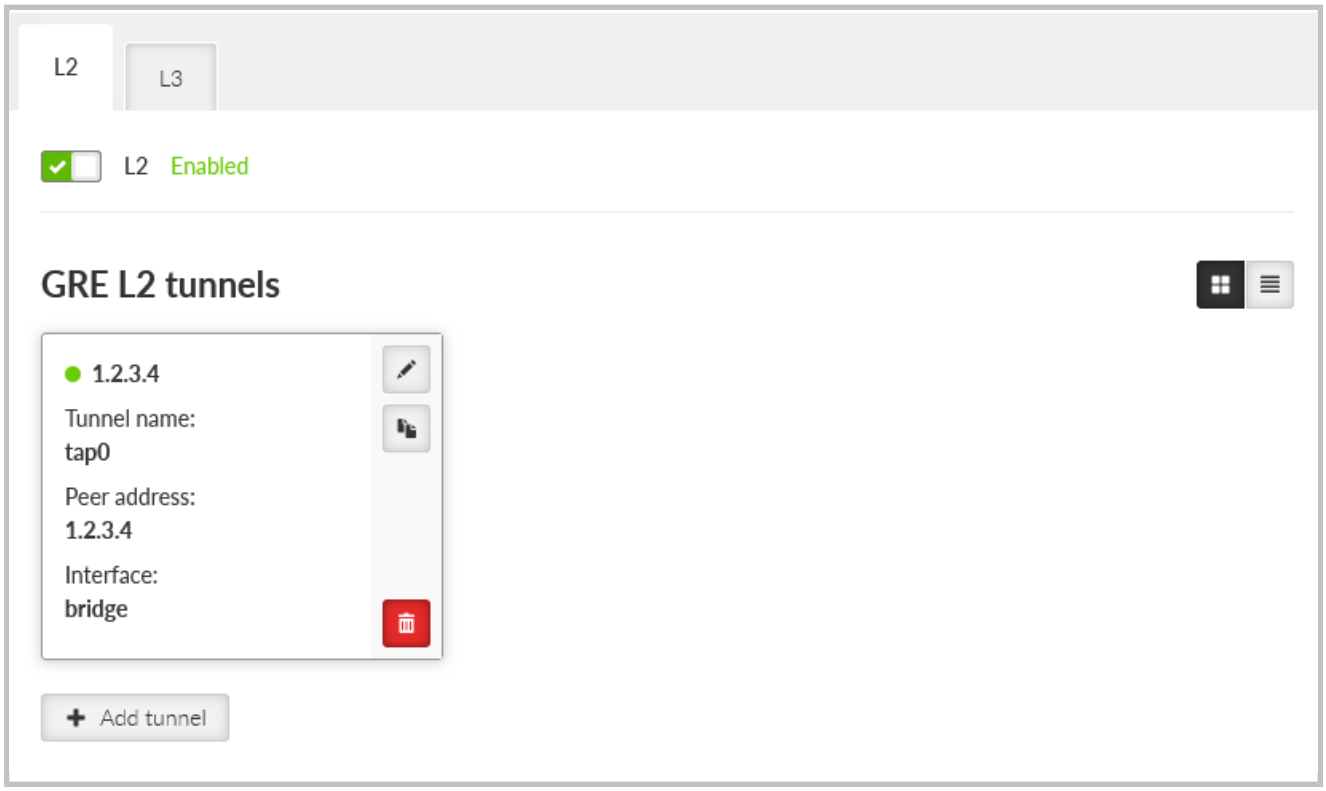
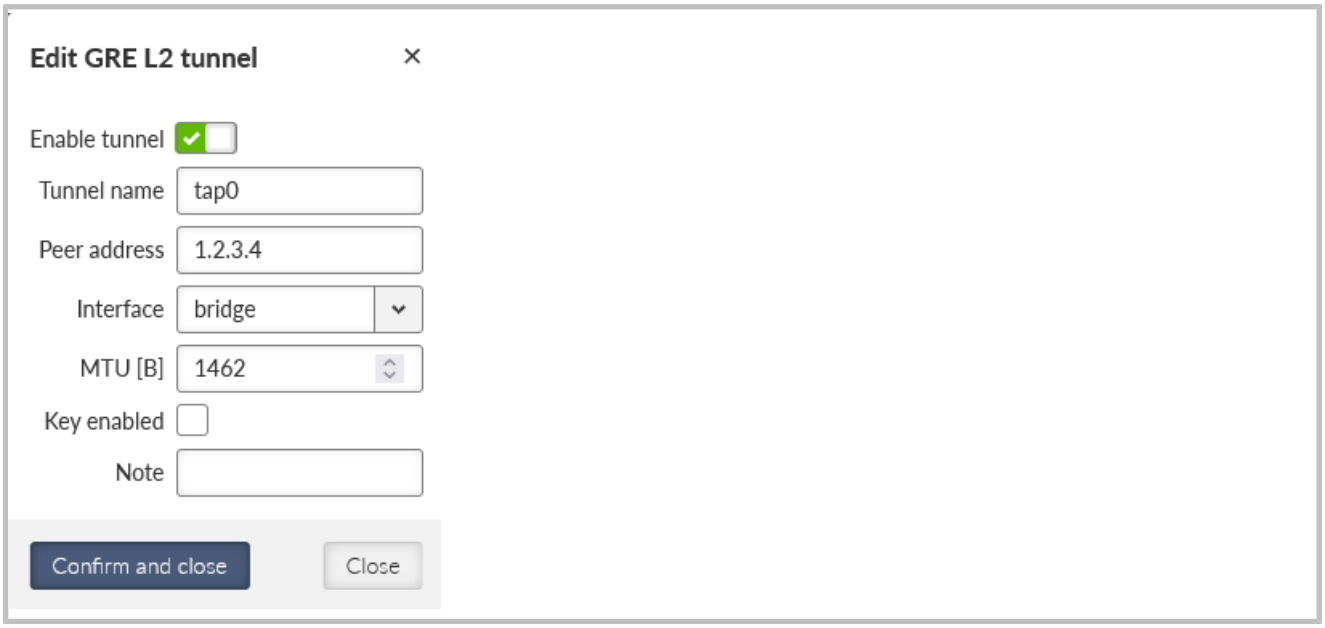


Fig. 4.21: SETTINGS > VPN > GRE

GRE L2 Enable
Switches all L2 tunnels On or Off.



Individual L2 tunnels:

Enable
Enables particular L2 tunnel. Maximum number of configurable tunnels is 256.

Tunnel name
The base of the tunnel interface name, prefixed with "gre_".

Peer address
IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.

Interface
Has to be set as one of existing bridge's name in SETTING/Interfaces/Ethernet/ Network interface Name.

MTU [B]
MTU of the L2 tunnel. Number {74 – 1500}, default = 1430 B
Overhead of the L2 tunnel is 38 B, so it should be GRE MTU = Path MTU - 38.
Minimum MTU value to establish TCP between WaSP units = 576 B.

Note
For traffic in bridged network (e.g. when using Transparent protocol), it is necessary to set the MTU to a proper value, otherwise there is a risk of packet fragmentation and thus compromising efficiency and reliability of the transfer.

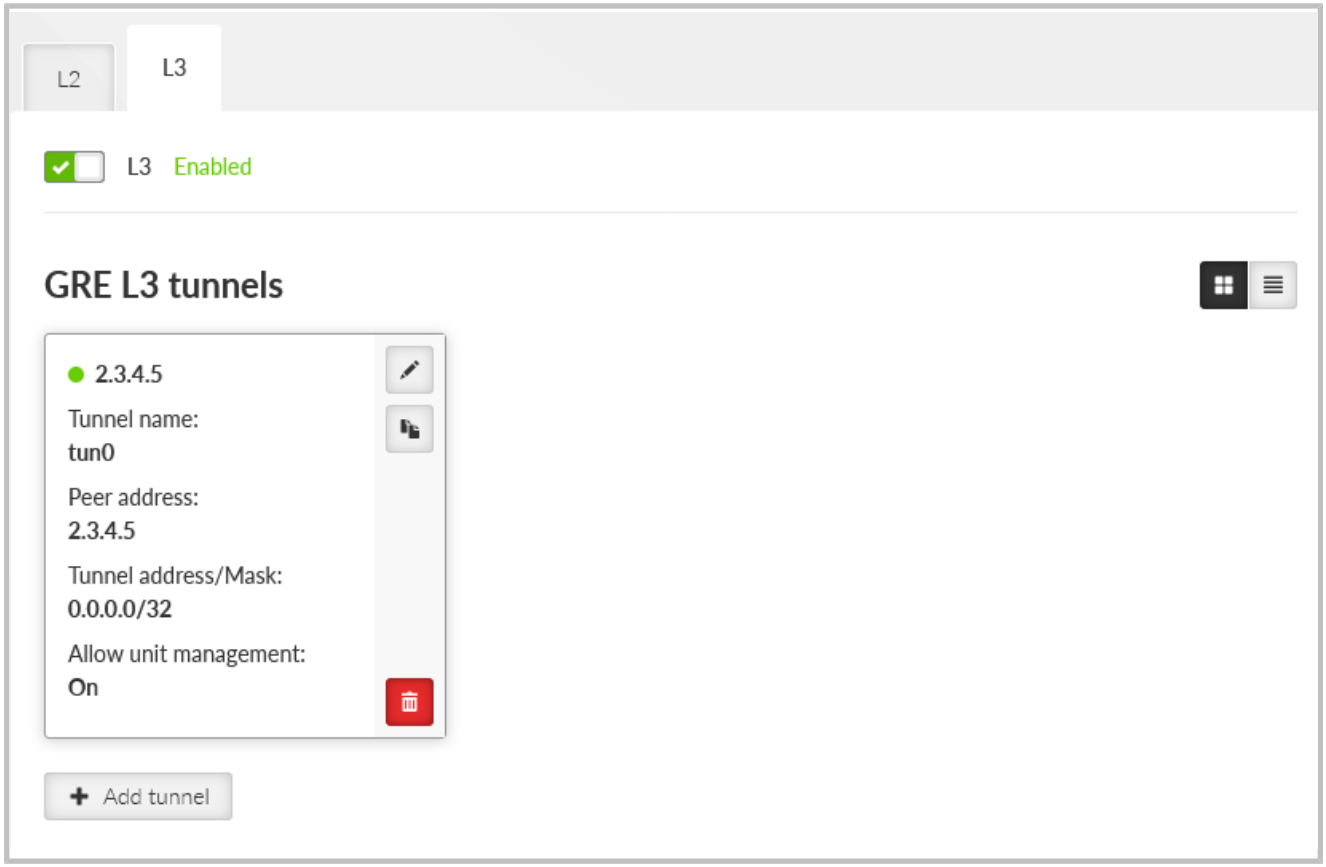
Key enabled
Enables using key identification of the tunnel from/to the same peer.

Key
Identification number of the tunnel Number {0 – 4,294,967,295}, default = 0

Note
Optional comment.

4.4.2.2. GRE L3

GRE L3 tunnel works as an additional unit's interface with its own IP address (and mask). The routing rules are used for sending packets to this interface. It bridges part of the network, so it seems to be one hop for the user traffic.



GRE L3 Enable

Switches all L3 tunnels On or Off.

Individual L3 tunnels:

Enable
Enables particular L3 tunnel. Maximum number of configurable tunnels is 256.

Tunnel name
The base of the tunnel interface name, prefixed with "gre_".

Peer address
IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.

Tunnel address / Mask
IP address and mask of the GRE tunnel interface

MTU
MTU of the L2 tunnel. Number {70 – 1476}, default = 1476
Overhead of the L3 tunnel is 24 B, so it should be GRE MTU = Path MTU - 24. If the MTU is bigger than is allowed along the route, the GRE packets will be discarded and ICMP report will be send back to the source of the original packet (Path MTU discovery).
Minimum MTU value to establish TCP between WaSP units = 576 B.

Key enabled
Enables using key identification of the tunnel from/to the same peer.

Key
Identification number of the tunnel Number {0 – 4,294,967,295}, default = 0

Allow unit management
Allows / disables unit management via GRE tunnel.

Note
Optional comment.

4.4.3. OpenVPN

OpenVPN is a virtual private network (VPN) system that allows to create secure encrypted point-to-multipoint connections in routed (TUN) or bridged (TAP) modes. Up to four instances (clients and/or servers) can be used simultaneously in one unit. Each server is capable of establishing connections with several tens of clients.

OpenVPN allows peers to authenticate to each other using pre-shared secret keys and certificates. An OpenVPN server is capable to release an authentication certificate for every client, using signatures and certificate authority (certificates can be generated / uploaded in the SETTINGS>Security>Credentials menu).

A time synchronisation of individual units is required for proper OpenVPN function.

Link for *OpenVPN application note*[5].

Note

OpenVPN has a very aggressive initialization process. It is not possible to operate OpenVPN within the Transparent protocol in Half duplex mode.

[5] https://www.racom.eu/eng/products/m/ripex/app/openvpn/index.html

Dynamic routing protocols cannot be used over OpenVPN L3 due to static internal routing in the server. Additionally, for Babel, the server does not route IPv6 link addresses (dynamically assigned by the kernel) that it uses for its control packets.

Warning

Attention is required to prevent routing loops, where traffic from the link between OpenVPN endpoints is directed back into the OpenVPN tunnel. Unlike IPsec, there is no protective mechanism against packet wrapping.

4.5. Security

User authentication is required to access WaSP unit management. There are two types of user authentication which differ in the user account location:

Local authentication – user accounts are stored directly in the WaSP unit

Remote authentication – user accounts are stored on a remote authentication server (RADIUS is implemented)

There are four different levels of user access privileges – they are bound with four different user access roles:

Guest (role_guest)
Read only access for configuration parameters (except secured part of configuration). Diagnostics tools are available.

Technician (role_tech)
All privileges of Guest role plus: write access for non-secured part of configuration; unit firmware up/down-grade.

Security technician (role_sectech)
All privileges of Technician role plus: write access for secured part of configuration (except unit authentication related parts).

Administrator (role_admin)
No access level restrictions. All privileges of Security technician role plus: user accounts management; remote authentication configuration.

Limitations:

Tab. 4.1: Overview of roles and rights in each section

Section	Features		Roles / Rights			
			Guest	Tech	Sec tech	Admin
SETTINGS	Interfaces	Ethernet, Radio, COM, Terminal servers, Cellular	Read-only	Write	Write	Write
		Radio - Encryption	Read-only	Read-only	Write	Write
	Routing	Static	Read-only	Write	Write	Write
		Babel, OSPF, BGP, Link management	Non-visible	Non-visible	Write	Write
	Firewall	L2, L3, NAT	Read-only	Write	Write	Write
	VPN	IPsec	Non-visible	Non-visible	Write	Write
		OpenVPN	Non-visible	Non-visible	Write	Write
		GRE	Read-only	Write	Write	Write
	Quality of service		Read-only	Write	Write	Write
	Security	Policy	Non-visible	Non-visible	Non-visible	Write
		Local authentication	Non-visible	Non-visible	Non-visible	Write
		Credentials	Non-visible	Non-visible	Non-visible	Write
		Management access	Non-visible	Non-visible	Non-visible	Write
		RADIUS	Non-visible	Non-visible	Non-visible	Write
		Tamper reset	Non-visible	Non-visible	Non-visible	Write
	Device	Unit	Read-only	Write	Write	Write
		Configuration	Read-only	Write	Write	Write
		Events	Read-only	Write	Write	Write
		Software keys	Read-only	Write	Write	Write
		Firmware	Non-visible	Write	Write	Write
	Services	Firmware distribution	Non-visible	Write	Write	Write
		SNMP	Non-visible	Non-visible	Write	Write
		SMS	Non-visible	Non-visible	Write	Write
		Hot standby	Read-only	Write	Write	Write
DIAGNOSTICS	Monitoring		Non-visible	Write	Write	Write
	Tools		Read-only	Write	Write	Write

At least one Administrator type of account must be defined in the unit.

Maximal number of concurrently active sessions is 64. One user can have multiple sessions opened in the same time. If this limit is reached and a new session is to be opened, the oldest active session is deactivated and a new one is opened.

Maximal number of Local user accounts (all roles together) is 100.

Note

The **Remote access** uses local identity and role of the user – there is no additional login to the remote unit (the login into local unit serves as login to the whole network).

4.5.1. Policy

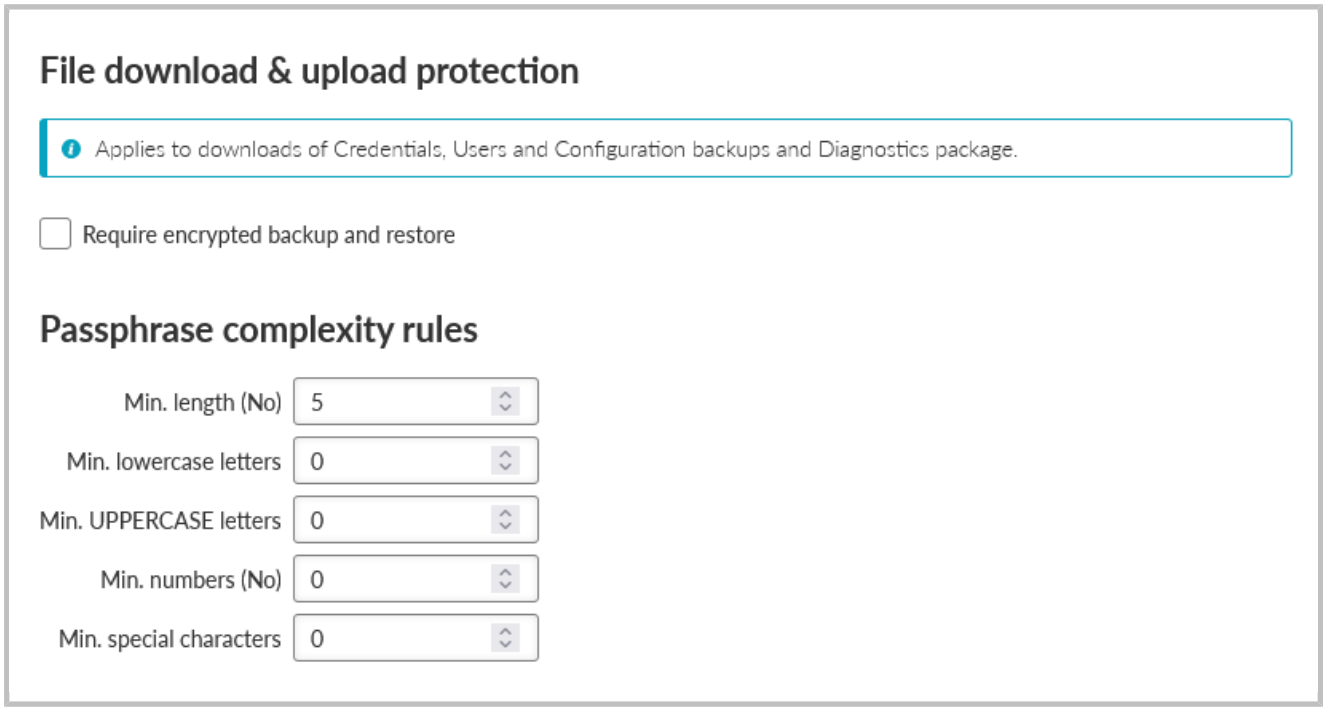


Fig. 4.22: SETTINGS > Security > Policy

Passphrase - Minimal length
Number {5 – 64}, default = 5
The minimum length of the passphrase.

Passphrase - Minimal number of lower case characters
Number {0 – 5}, default = 0
The minimum number of lowercase letters (English letters) which are required in the passphrase.

Passphrase - Minimal number of uppercase characters
Number {0 – 5}, default = 0
The minimum number of uppercase letters (English letters) which are required in the passphrase.

Passphrase - Minimal number of digits
Number {0 – 5}, default = 0
The minimum number of number characters (0 to 9) which are required in the passphrase.

Passphrase - Minimal number of special characters
Number {0 – 5}, default = 0
The minimum number of special characters (not English upper or lower cases or numbers) which are required in the passphrase. Non-English letters (like Greek, Russian, Arabic) are counted as special characters.

This setting applies to the download of Credentials, Users, Configuration backups, and Diagnostics packages. The **Require encrypted backup and restore** parameter enforces the use of encrypted files for all users. The following parameters allow you to define passphrase complexity rules for encryption.

4.5.2. Local authentication

4.5.2.1. User Accounts

The following settings are available only for user with the Administrator role.

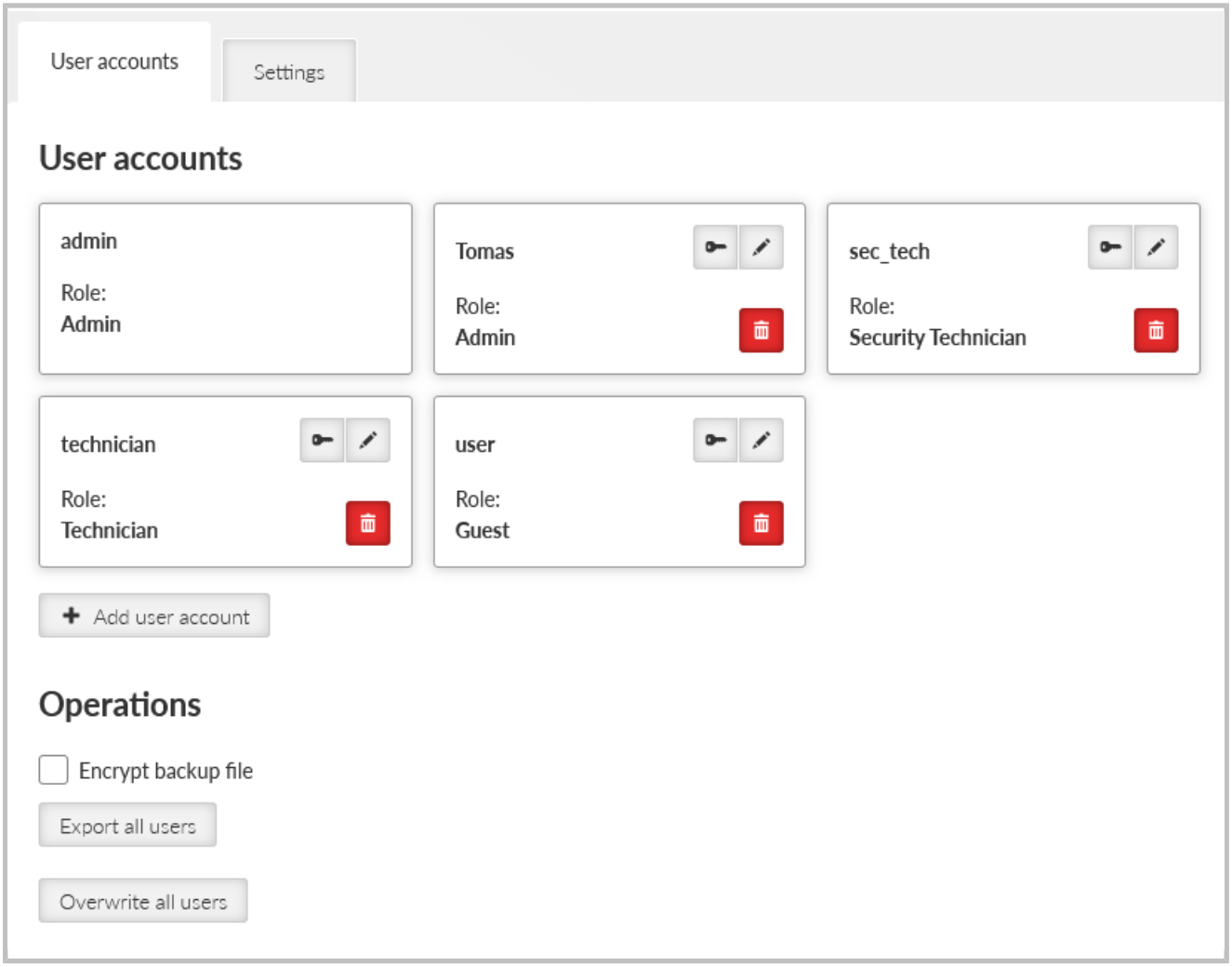


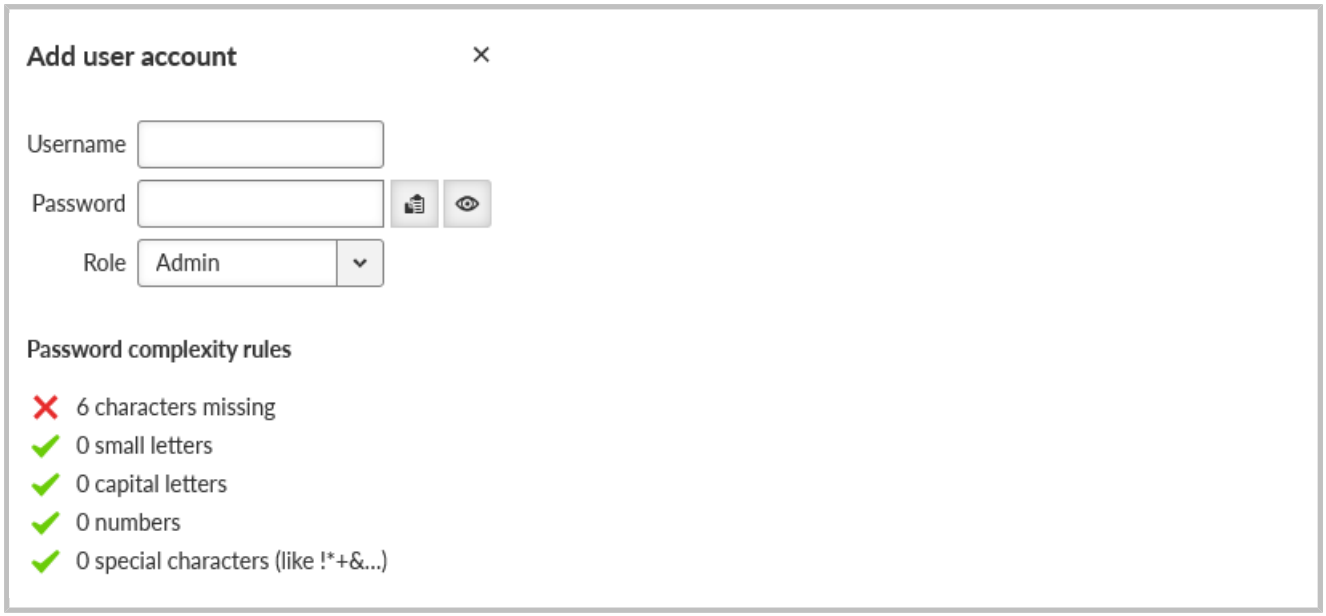
Fig. 4.23: SETTINGS > Security > Local authentication

Following user account parameters can be changed: password, user role. Any account (expect the last one of Administrator role) can be deleted.

Export all users button provides backup of all Local user accounts into a file.

Import all user button provides restoration of all Local user accounts from a backup file. Active session is logged out automatically after this command.

+ Add user account button invokes new user account creation dialog:



Username

String {1–128 char}, default = <empty>
New Username. Every username in the unit must be unique.

Password

String {5–128 char}, default = <empty>
Password is stored in a secure way.

Role

List box {Admin; Security Technician; Technician; Guest}, default = "Admin"

Note
It is highly recommended to create a new administrator type of account and delete the default “Admin” account.

“Export all users

The exported user accounts are stored in a text file (.json file type) or in an encrypted .zip file. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section 7.5.1 Policy.

Overwrite all users

All existing current users will be deleted and replaced by users stored in imported file. You will be logged off after the import and you have to log in using the imported user account.”

Advanced feature

When the user account is not active for some time, the user will be automatically logged-out. The in-activity timeout of the account is set for 1 day by default. It is possible to change in the range of 5 minutes up-to 2 days (menu ADVANCED > Generic > UserAccess > **Web inactivity timeout**).

Note

It is necessary to install firmware version 1.4.5.0 or higher to assure proper functionality of Local and Remote authentication.

4.5.2.2. Settings

Allows to set password complexity rules.

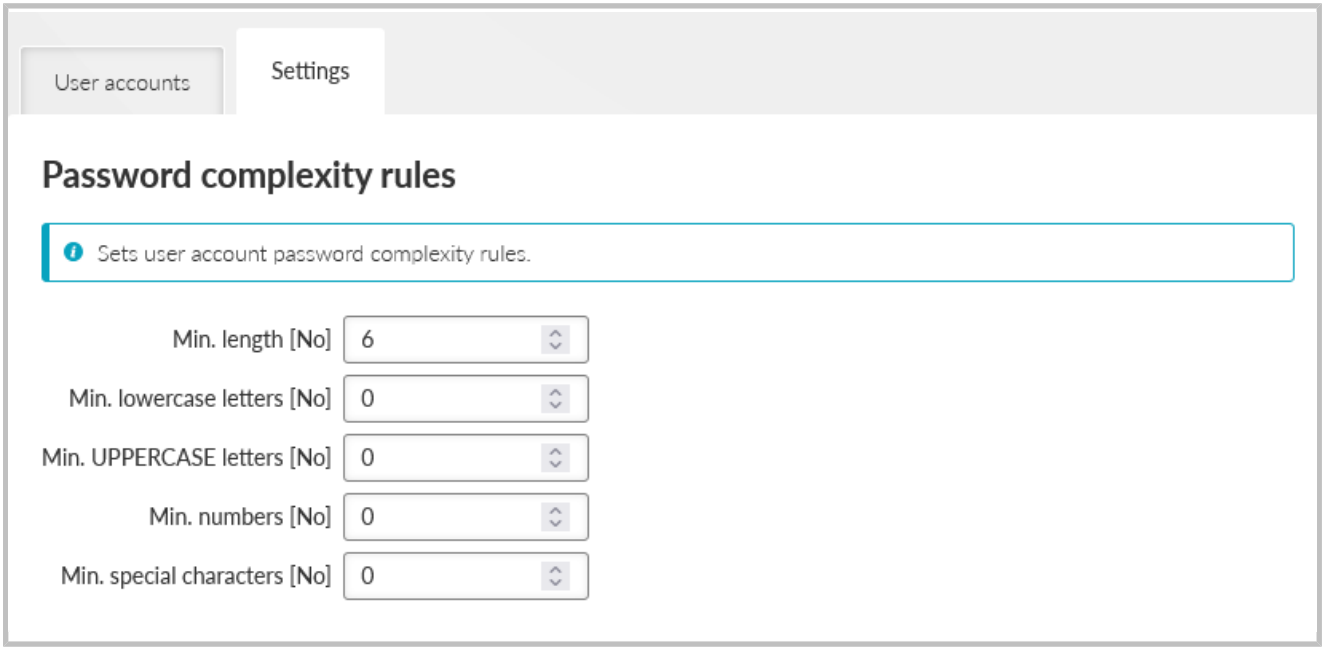


Fig. 4.24: SETTINGS > Security > Local authentication > Settings

Min. length [No]
Number {8 – 64}, default = 8
The minimum length of the password for all users.

Min. lowercase letters [No]
Number {0 – 5}, default = 1
The minimum number of lowercase letters (English letters) which are required in the user password.

Min. UPPERCASE letters [No]
Number {0 – 5}, default = 1
The minimum number of uppercase letters (English letters) which are required in the user password.

Min. numbers [No]
Number {0 – 5}, default = 1
The minimum number of number characters (0 to 9) which are required in the user password.

Min. special characters [No]
Number {0 – 5}, default = 1
The minimum number of special characters (not English upper or lower cases or numbers) which are required in the user password. Non-English letters (like Greek, Russian, Arabic) are counted as special characters.

Note
The settings are applicable for new passwords only, already existing passwords will not be affected.

4.5.3. Credentials

WaSP units feature a unified storage solution for keys, certificates and other credentials. This storage is secured and only accessible to users with Sectech permission and higher.

Credentials are separate from configuration to improve security and it also is protected using checksum to prevent unauthorised modification. Because of this all Repository/Key changes are executed immediately and do not go through the “Changes” workflow like the regular configuration.

Note: In this manual and in the user interface we are calling all Credential storage entries “Keys”. While this is a simplification, we believe it is understandable. Further on “Keys” are all keys, public and private certificates, DH parameters, CA chains etc.

Warning: Downgrading the Unit will always reset all Credentials to defaults.

4.5.3.1. General

Credentials are stored in Repositories. Repository is a reserved space, which contains 0-1 Key and is addressable via its ID in the rest of the unit configuration. This construct, while it may seem complicated at first, brings major benefits. Mainly the user can simply update expired certificates in a repository without any need to change configuration using that Repository.

There are two types of Keys: Read-only, easily identifiable by a lock icon and “_RO_” prefix. These Keys are built into firmware, or generated automatically on device. The rest are user-defined keys.

Admin website allows users to perform various operations with the keys and repositories.

Using buttons on the bottom of the page we also allow users to download complete credential backup.

There are two ways to restore credentials: Replace, which replaces all Keys with ones from the file, and Update, which merges current and new Keys.

4.5.3.2. Credentials

Credentials show all Repositories and Keys currently on the device. Users can filter them by type and show only valid or all Keys. The card border and bottom label indicate whether the Repository is empty, or whether the Key is valid or invalid.

Each card represents a Repository. Card title is Repository ID. All user-defined repositories can be edited using the “Edit” button and deleted using the red “Delete” button.

ID
Unique identifier used to reference Repository in configuration.
Validated according to regular expression: [a-zA-Z0-9_]\\{1,128\\}. IDs starting with underscore “_” are reserved for Read Only keys.

Type
Defines the type of Key the Repository can contain.

Note
Optional comment.
There are several operations, that can be performed on a repository:

Info
Displays Key info including checksums.

Generate
Generates a new Key using local Certification authority (see below).

Update
Updates the Key with a new one. Both file and text, encrypted and unencrypted Keys are supported.

Download
Allows download of the Key. Both encrypted and unencrypted downloads are supported. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section *7.5.1 Policy*.

Generate CSR (Certificate Signing Request)
Generates and downloads CSR from eligible Keys.

Sign CSR (Certificate Signing Request)
Signs CSR. Both file and text certificates are supported. Signed certificate is automatically downloaded. It is possible to add “extended key usage” Certificate modifier for OpenVPN client/server.

Operation “Add repository” creates an empty Repository.

Shortcut operations “Generate credential” and “Add credential” allow users to create a Repository and generate/upload a key into it. These buttons cannot be used to modify existing repositories.

4.5.3.3. Read-only keys

_RO_Ssh_Host_Key
Type: SSH Key (PRI)
The SSH host key used to authenticate the server on the client. If missing, it is generated when the station boots.

_RO_Rmt_Access_Host_Key
Type: RMTACCESS Key (PRI)
Host key for the Remote access server (QSSH). It is used to authenticate the server.
If missing, it is generated when the station starts.

_RO_Rmt_Access_Client_Key
Type: RMTACCESS Key (PRI)
Key for Remote access (QSSH) client login to the server. Must be present on both sides.
Obtained from FW. If it differs from the version in FW, it is updated.

_RO_Web_Private_Key
Type: Certificate (PRI)
Web server private key (default).
Obtained from FW. If it is different from the version in FW, it is updated.

_RO_Web_Cert
Type: Certificate Key (PUB)
Web server certificate (default).
Obtained from FW. If it is different from the version in FW, it is updated.

_RO_Web_CA_Chain
Type: CA Chain (PUB)
The certificate string of the authority that signed the Web server certificate. If self-signed, it will be empty.
Retrieved from FW. If it differs from the version in FW, it is updated.

_RO_Web_DH_Param
Type: DH Parameters (PUB)
Parameters for the Diffie-Hellman key exchange in the Web server.
Retrieved from FW. If it differs from the version in FW, it is updated.

_RO_File_Distribution_Key
Type: UFTP Key (PRI)
Key for authenticating stations in the "File distribution" (UFTP) service.
Obtained from FW. If it differs from the version in FW, it is updated.

4.5.3.4. Settings

This tab displays additional settings needed for Local CA authority and Passphrase complexity rules for Key downloads.

Local authority

Private key ID
Private key used for local certification authority.

Certificate ID
Public certificate used for local certification authority.

Signature algorithm
Algorithm used for certificate signing. It depends on the Certification Authority key algorithm and may not be used in case CA uses a specific algorithm.

Expiration period (days)
Expiration period in days. Default 7300.

4.5.3.5. Organisation

Contains organisation identification used for certificate generation.

- Country
- Country code (pre filled automatically, possible to manually set by using “Other” in “Country”)
- Organisation
- Department
- Location
- State
- Common name
- E-mail

4.5.3.6. Creating Local Certification Authority

To create local CA you need to follow these steps:

1. Generate a new private certificate “Certificate key (PRI)”
2. Generate a new “CA Chain (PUB)” using certificate created in previous step as “Certificate key”
3. Activate Local CA by going to Settings tab and activating Local CA, selecting newly created “Private key ID” (= new private certificate “Certificate key (PRI)”) and “Certificate ID” (= new “CA Chain (PUB)”)

Note

Web server private key must use “RSA” or “EC (ECDSA)” algorithms. Other algorithms are not supported by web browsers.

4.5.4. Management access

4.5.4.1. Administration website

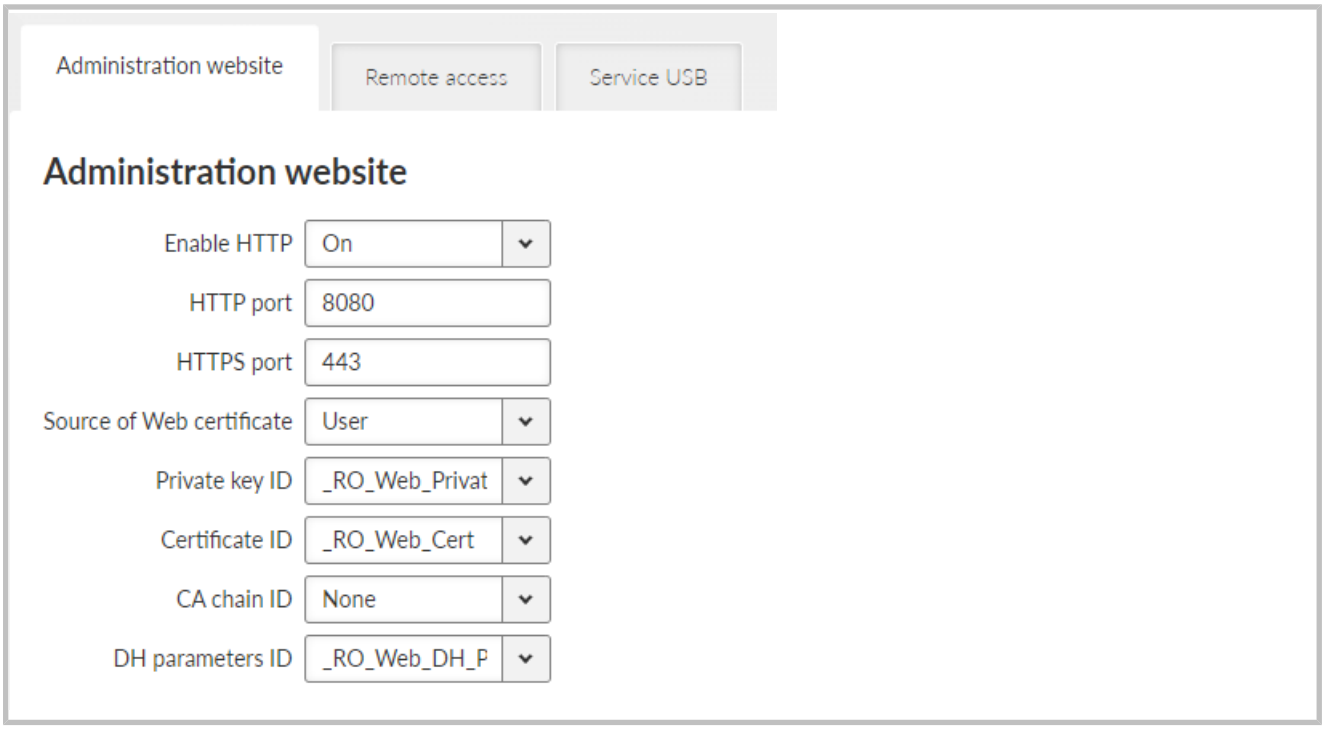


Fig. 4.25: SETTINGS > Security > Management access > Administration website

Enable HTTP — List box {On; Off}, default = "On"

Enables HTTP access to the station. When enabled, HTTP immediately redirects to HTTPS.

HTTP port — Number {1 – 65535}, default = 80

The TCP port number on which HTTP access is available.

HTTPS port Number {1 – 65535}, default = 443

The TCP port number on which HTTPS access is available.

Source of Web certificate

List box {Default; User}, default = "Default"

Choses source of Web server certificate. "Default" uses key, certificate and DH parameter distributed in FW (see SETTINGS > Security > Credentials), default values are as follows:

- Private key: _RO_Web_Private_Key
- Certificate : _RO_Web_Cert
- CA chain: _RO_Web_CA_Chain": CA chain, of the CA which signed the certificate. For self-signed certificate shall remain empty - None).
- DH parameters: _RO_Web_DH_Param

Web inactivity timeout [min] Number {5 – 2880}, default = 1440

When the inactivity timeout is reached, the HTTPS session terminates.

Available in ADVANCED > Security > Management access menu.

“User” allows to use user key and certificate included in the Credentials storage. Add your certificate and other files using menu SETTINGS > Security > Credentials. In the individual list boxes will be shown available certificate of keys for each category and you can choose those previously added.

4.5.4.2. Remote access

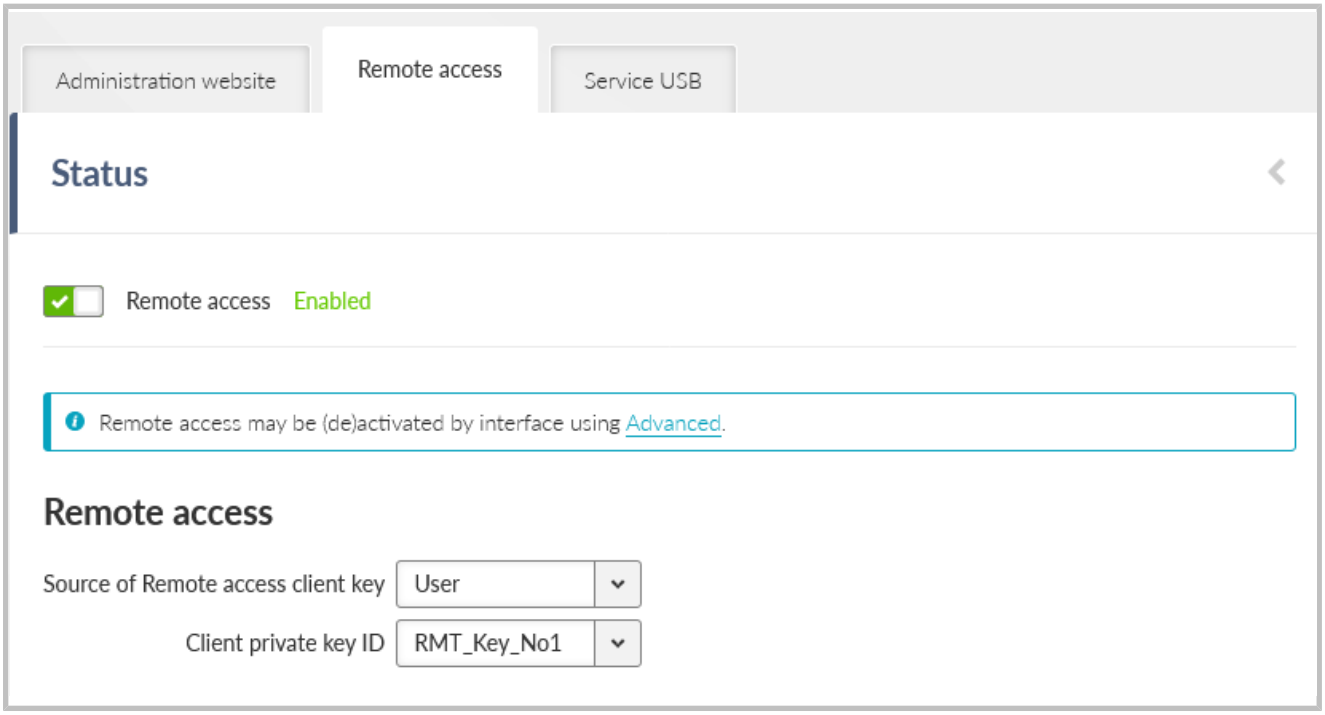


Fig. 4.26: SETTINGS > Security > Management access > Remote access

Enable/Disable
If enabled, allows the unit to be accessed via the Remote access feature.

Note
Remote access is enabled or disabled globally in this menu. Individual settings for each interface are available in the ADVANCED menu. By default, Radio and Ethernet interfaces are enabled, while all other interfaces are disabled. The current settings are displayed in the Status area.

Source of Remote access client key
List box {Default; User}, default = "Default"

Client private key ID
When the User in list box above is chosen, then you cab select a key previously downloaded to the Credentials storage (SETTINGS > Security > Credentials) or or generated in the same menu. The Remote access key has to be the same for the whole network (or the part of it for which you will use the Remote access). The remote access to the unit with different Remote access key is not possible.

Note

The use of a dedicated **Client private key** is highly recommended.

4.5.4.3. Service USB

The USB service interface primary purpose is to provide unit service and management access. Ethernet or Wi-Fi connection can be established using an external ETH/USB or Wi-Fi adapter.

Only adapters supplied with the product can be used for this purpose.

See *list of available adapters*[6].

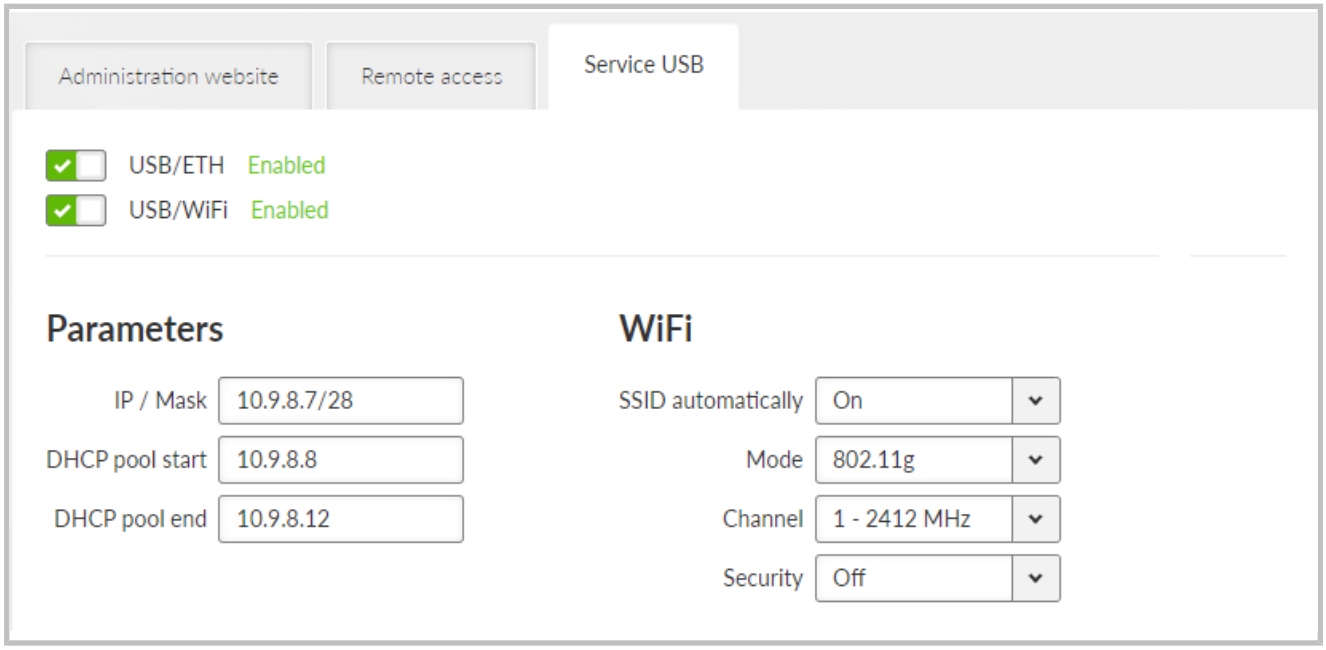


Fig. 4.27: SETTINGS > Security > Management access > Service USB

The DHCP server is running on this service interface to enable easier connection of the management device (PC, tablet or smart phone).

Enable / Disable
Each of the ETH or Wi-Fi service can be enabled or disabled separately. When the Wi-Fi is enabled, the unit acts as a Wi-Fi Access Point (AP).

IP address / Mask
IP address, default = 0.0.0.0/0
IP address of the DHCP server. This is the IP address to be used when accessing the unit management via this serial interface.

DHCP pool start
Default = IP address of the DHCP server + 1
DHCP Server assigns addresses to connected clients starting from this address.

DHCP pool end
DHCP server assigns IP addresses to connected clients in the range defined by **DHCP pool start** and **DHCP pool end** (inclusive).

Wi-Fi
Wi-Fi AP parameters can be customized.

SSID automatically
List box {On; Off}, default = "On"
When automatic definition of SSID is enabled, the SSID contains unit Serial number.

SSID
Wi-Fi AP SSID. When entered manually, it must follow SSID naming conventions.

[6] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

Mode
List box {802.11g; 802.11g }, default = "802.11g "
Wi-Fi AP mode.

Channel
Selected Wi-Fi channel.

Security
List box {Off; WPA2-PSK}, default = “Off”
It is a good practice to use WPA2-PSK secured connection together with a strong password. It is highly recommended in case of permanent Wi-Fi adapter installation.

4.5.5. RADIUS

User accounts can be managed centrally with an authentication server. RADIUS client-server protocol is used for remote authentication. RADIUS accounts can be mapped to one of the four user roles. This is either managed by the server itself or by local WaSP settings.

Local accounts are checked first and if the account does not exist, RADIUS accounts will be used. If the RADIUS server is not accessible, users may use the local username/password to “fall back” to local authentication.

Fig. 4.28: SETTINGS > Security > RADIUS

Menu SETTINGS > Security > RADIUS allows to set all the main parameters.

RADIUS server address
IP Address of RADIUS server used for authentication.

RADIUS server authentication key
Text {0 – 32 characters}
Password to authenticate against the RADIUS server.

User realm
Text {must contain at least one dot “.”}
Realm allows to shorten the login name - e.g. when the full login name is "tech@noname.eu" and the realm is "noname.eu" the Username filled in the login page is only "tech".

Server response timeout [s]
Number {1 – 30}, default = 10
Time measured while waiting to the server's response before sending a request retry.

Server request retries
Number {1 – 7}, default = 3
Number of request retries in case of WaSP did not receive a valid reply.

Additional expert parameters shall be set in the ADVANCED menu.

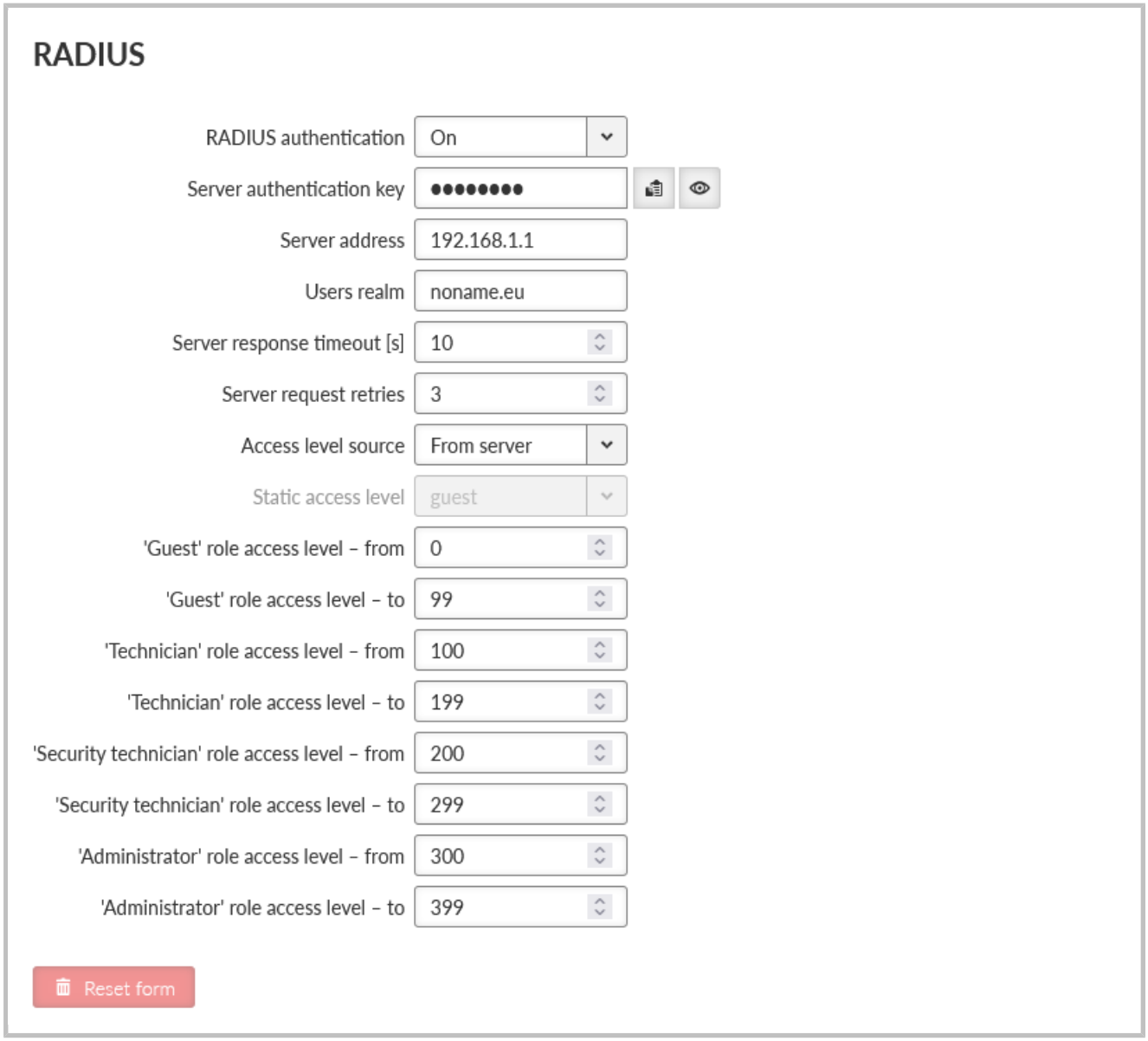


Fig. 4.29: ADVANCED > Security > RADIUS

The level of access is realised by Management-Privilege-Level (RFC 5607, index 136, type integer). The level for each account shall be set during the server configuration. The user access level will be granted according to the integer ranges for individual role levels. When the server does not allow setting of Management-Privilege-Level the static account level option (for all users) has to be used.

4.6. Device

4.6.1. Unit

4.6.1.1. General

The general settings affecting the whole unit.

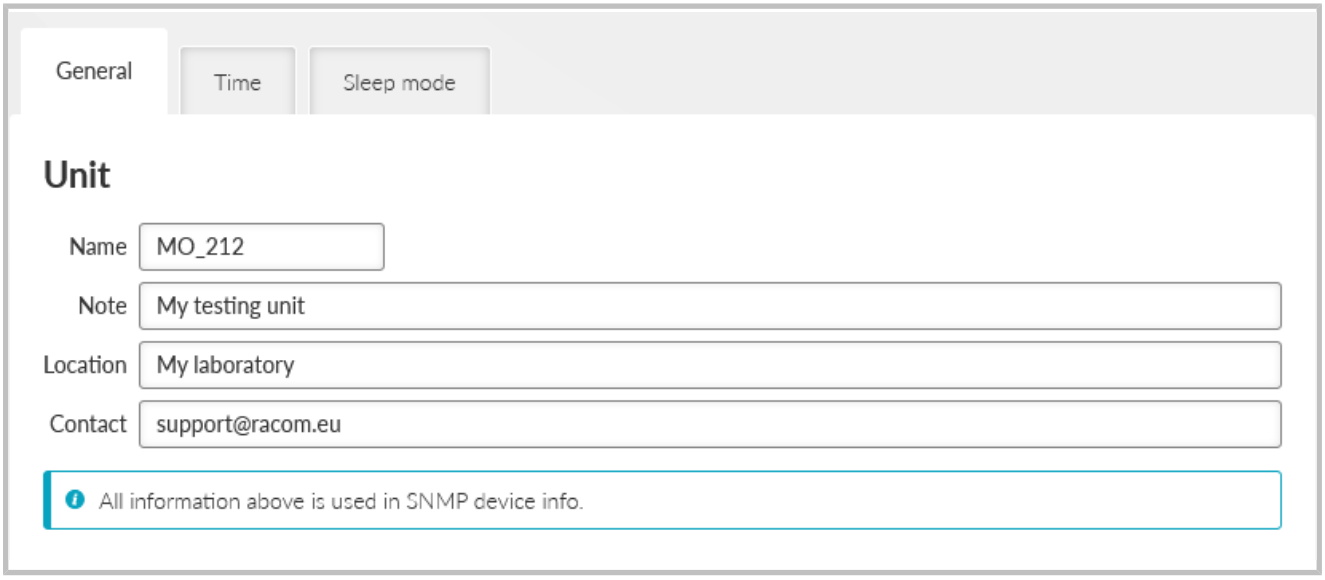


Fig. 4.30: SETTINGS > Device > Unit

Unit name
This name is used as a real name of the Linux router, so the allowed characters are strictly limited to:
Text; default = _a..zA..Z0..9

Unit note
Text; default = _a..zA..Z0..9
Longer unit name without special characters restrictions.

Unit location, Unit contact
Text; default = _a..zA..Z0..9
Additional SNMP information. All the fields above are typically used in the NMS systems to identify the specific unit.

4.6.1.2. Time

Unit Event time stamps, unit Statistics records and unit internal logs are using Unit time. It is good practice to keep the Unit time synchronized to ease unit and network diagnostics.

Unit time can be setup manually or it can be synchronized with an NTP server. NTP server synchronization is recommended.

The unit itself serves as an NTP server providing the time synchronization to another IP clients. If no NTP server is defined or no one is available, the unit runs in an “orphan” mode. The unit internal NTP server Stratum is set to 8 in this case. If the unit is synchronized with an NTP server, the unit NTP

server Stratum is set a 1 higher comparing to Stratum of the NTP server providing the time synchronization to the unit.

If the unit is synchronized to a time source and the unit (synchronized) time differs from the unit RTC time (by more than 8 seconds), the RTC time is updated.

Note

Each unit can serve as NTP server for further IP equipment, this functionality is always on.

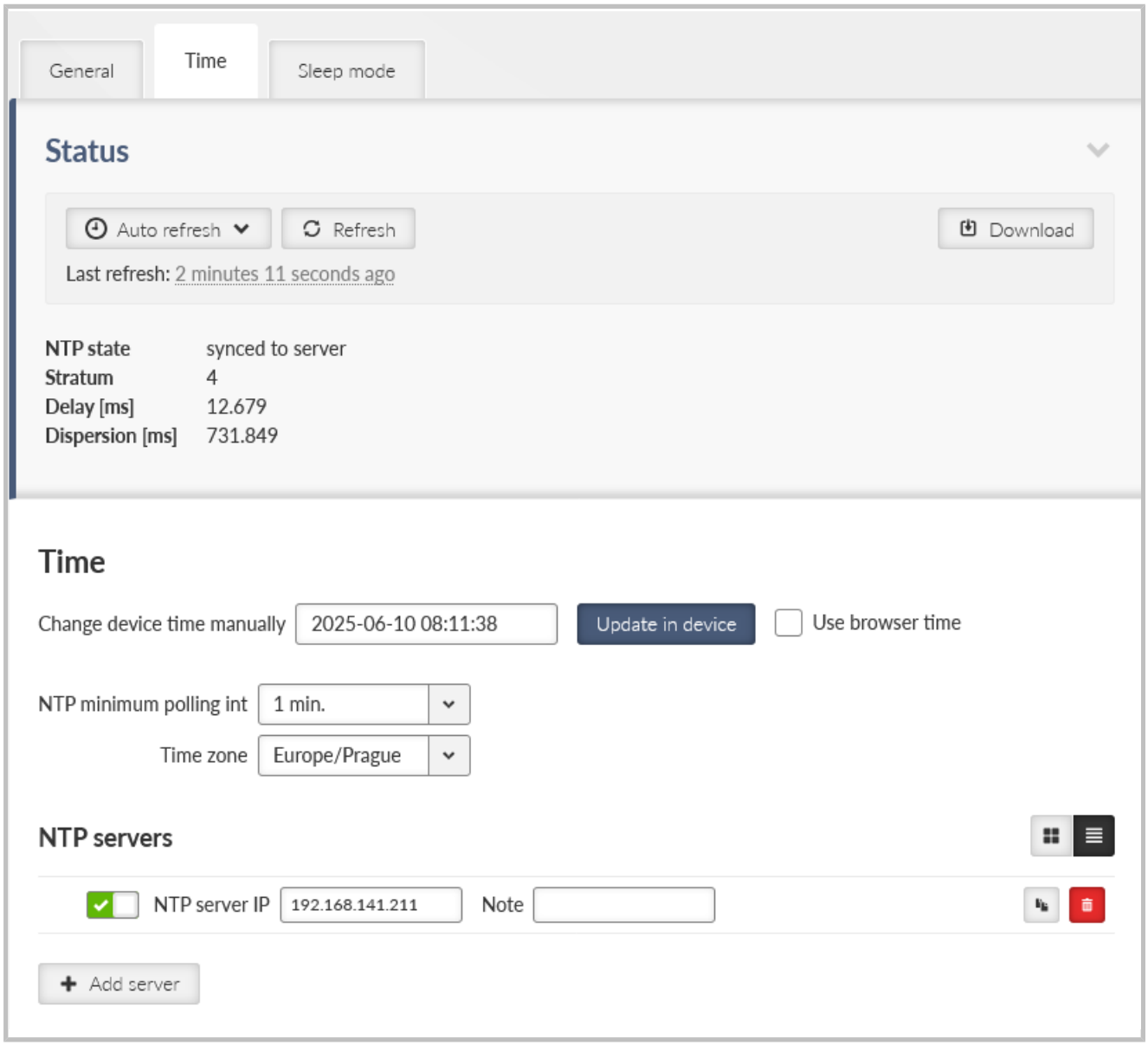


Fig. 4.31: SETTINGS > Device > Unit > Time

Status

The Status field provides information about NTP synchronization status.
Refresh button is used to update the Status information.

4.6.1.2.1. Time

Change device time manually
This field is used to setup unit time manually.

Update in device
Sets the given time to the unit.

Use browser time checkbox
Continuously updates the Change device time manually field to minimize the delay between the time input and the moment of time setup.

NTP client synchronization source
Synchronization source of the NTP client. The only option “NTP server” is implemented at this firmware version.

NTP server minimum polling time
Minimal period of the NTP server queries. NTP client is allowed to prolong this time in case of poor quality of the server or connection to the server.

Time zone
Time zone to represent unit internal time. All the unit timestamps are displayed using this time zone. Changing the time zone does not affect unit internal records – they are always recorded using UTC time zone.
NTP status information is based on standard ntpq daemon status output (ntpq -c lpeers, ntpq -c rv) - see *https://docs.ntpsec.org/latest/ntpq.html* (system, peer and clock variables) for details.

4.6.1.2.2. NTP servers

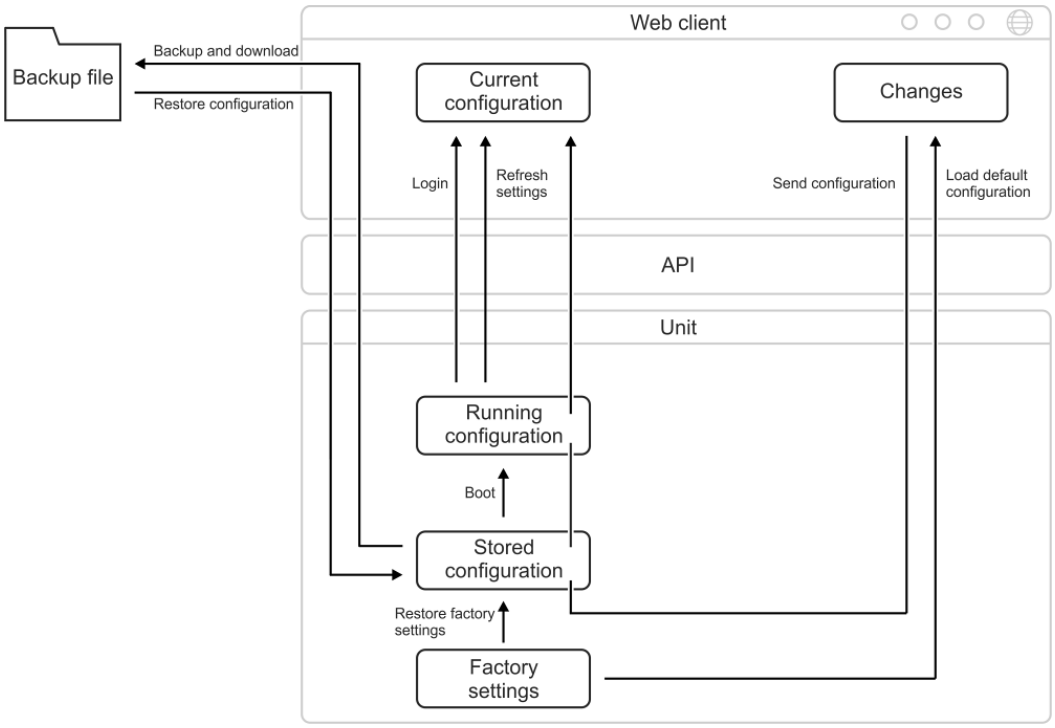
Multiple NTP servers can be configured to get more precise time synchronization or to have a backup solution in case of an individual NTP server unavailability. Maximum number of records in the list is 32. The unit runs in an “orphan” mode if the **NTP client synchronization source** is set to “NTP server” and there is no NTP server defined in this list.

Enable / Disable	Enables / Disables a NTP server.
NTP server IP	Defines the IP address of the NTP server.
Note	Informational comment.

4.6.2. Configuration

Configuration in WaSP operates on following system:

- Current configuration - displayed configuration, which is seen in the web client.
- Running configuration - actual configuration, running in the WaSP unit.
- Stored configuration - configuration stored in the WaSP unit. This configuration is stored in the unit, even when its turned off.
- Factory settings - default configuration.
- Changes - all changes done to the Current configuration (in the web client). For more information see *Section 3.2, "Changes to commit"*.



There are several tools to operate full unit configuration:

Backup

It is a good practice to make a configuration backup into an external file every time the configuration is changed, to be able to restore the configuration into another unit in case of unit maintenance.
Backup and download button triggers the web browser Download action. The specific behavior depends on your web browser personal settings - whether the configuration backup file is downloaded to a predefined download folder or the file Download dialog to select destination folder is shown. The configuration is stored in a text file (.json file type) or in an encrypted .zip file. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section *7.5.1 Policy*.
The backup configuration has following limitations:

- The set of configuration data is limited by a user access privileges of the user who performed the backup. The full configuration backup can only be issued by a user with the Administrator (role_admin) access privileges. The same user access limit applies when the configuration is

restored (i.e. the full configuration Restore can only be issued by a user with the Administrator (role_admin) access privileges).

- The configuration data are valid only for the given configuration version (CNF version - see below). If the new firmware version brings the new configuration version, **the new configuration backup file needs to be downloaded after the firmware upgrade.**

Note
The current unit configuration (inside the running unit) is converted to a new version automatically during the firmware upgrade. No need to take care about that process.

Configuration version is stored in the parameter called “CNF version” which can be checked in the menu: DIAGNOSTICS > Information > Device > Advanced information.

Restore

The configuration can be restored from a backup file (containing the same configuration version as the configuration version currently running in the unit - see above).

Choose File Button

Triggers the file selection dialog. Once the configuration backup file is selected, it is uploaded to the unit. The upload action can take some time - depends on the speed of your service connection to the unit.

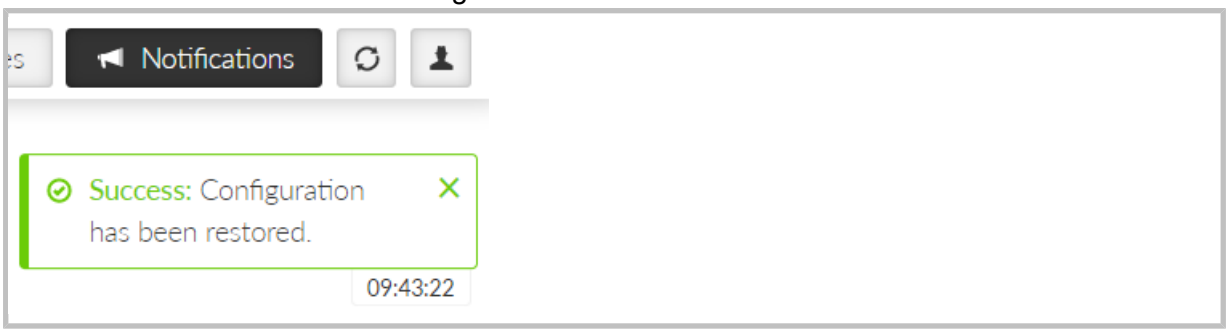
Factory settings

Load default configuration button loads default values of all configuration parameters into the web interface. All parameters whose current value differs from the default are marked as changed. They are listed in the Changes to commit dialog. They do not affect the running unit until eventually sent to the unit by the Send configuration button.

Note
This action can be used (for example) to check which set of parameters differs from the default value.

Restore configuration button

Enabled after the backup configuration is uploaded. Press the button to restore the unit configuration. The configuration restore result is reported as an error message (in case of failure) or Notification center success message:



Restore factory settings

Restores all configuration parameters to default setup (including monitoring settings). Logout from station will apply.
Deletes user database.

Total purge

Restores all configuration parameters to default setup (including monitoring settings). Logout from station will apply.
Deletes user database.
Deletes all diagnostic logs and statistics.
Clears Radio Tx and antenna degradation detector calibration.

Note

Basic data such as Code, Region, SW keys will always remain in the unit.

Warning

This action can take up to two minutes - do not power off the unit until finished.

Configuration validation

FW from version 2.2.0.0 introduces an improved configuration validation process. In older FW versions, some configuration item validations (e.g., allowed value range, string length) were validated only in the web application (front-end). When modifying the configuration in other ways (API calls, direct editing of the backup configuration file), it was possible to enter a value into a configuration item that caused the resulting unit configuration to be invalid. Recently, full configuration validation is performed directly in the unit (back-end). No method of configuration change (web interface, API, text backup modifications) can cause the unit to use an invalid configuration.

Consequences of running the unit with an invalid configuration:
The system event "EVENT_CNF_BOOT_ERROR" is active. The event has a default severity of Alarm, which causes the SYS status LED to light up red.

Until all items that failed the validation process are corrected, no configuration changes can be saved. The updated configuration can only be activated once the entire configuration successfully passes validation.

Tab. 4.2: Configuration versions

CNF version	FW version
28	2.2.6.0
27	2.2.4.0
26	2.2.2.0
25	2.2.1.0
24	2.2.0.0
23	2.1.7.0
22	2.1.6.0
21	2.1.2.0
20	2.1.1.0
19	2.1.0.0
18	2.0.18.0
17	2.0.16.0
16	2.0.14.0

CNF version	FW version
15	2.0.13.0
14	2.0.10.0
13	2.0.8.0
12	2.0.7.0
11	2.0.5.0
10	2.0.3.0
9	2.0.1.0
8	1.4.8.0
7	1.4.6.0
6	1.4.5.0
5	1.4.3.0
4	1.4.1.0
3	1.3.6.0
2	1.3.4.0
1	1.3.2.0
0	1.3.1.0

The Status section displays the **Configuration checksum**. This checksum is unique to each unit and its current settings. Any modification to the configuration will result in a different checksum value. The checksum can also be retrieved via an API call.

4.6.3. Events

Settings of the severities of the individual events. Some events can generate SNMP notification and can change level of the HW alarm outputs (AO, DO1, DO2) see *Section 1.2.2, “Power”*.

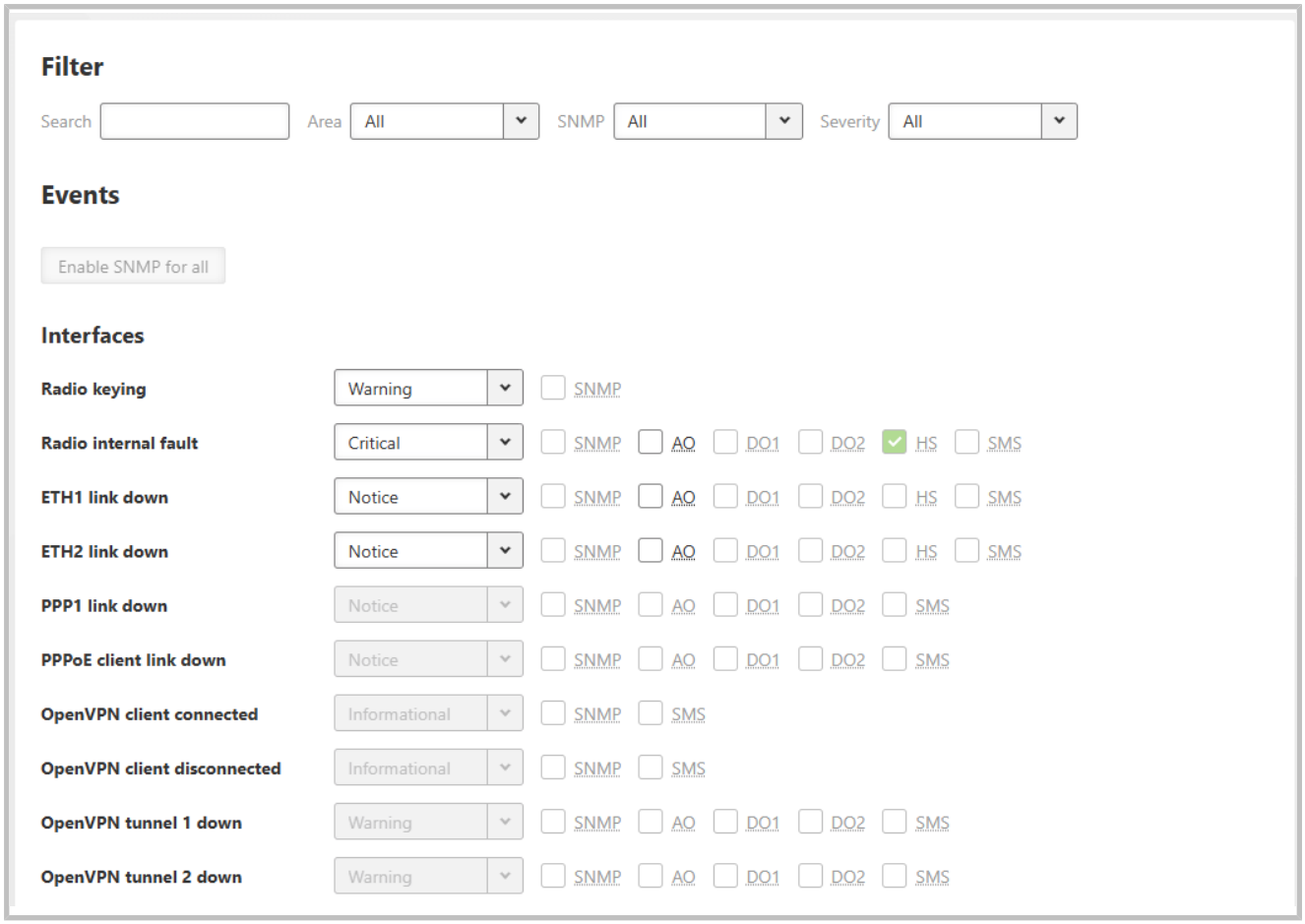


Fig. 4.32: SETTINGS > Device > Events

4.6.3.1. Test event

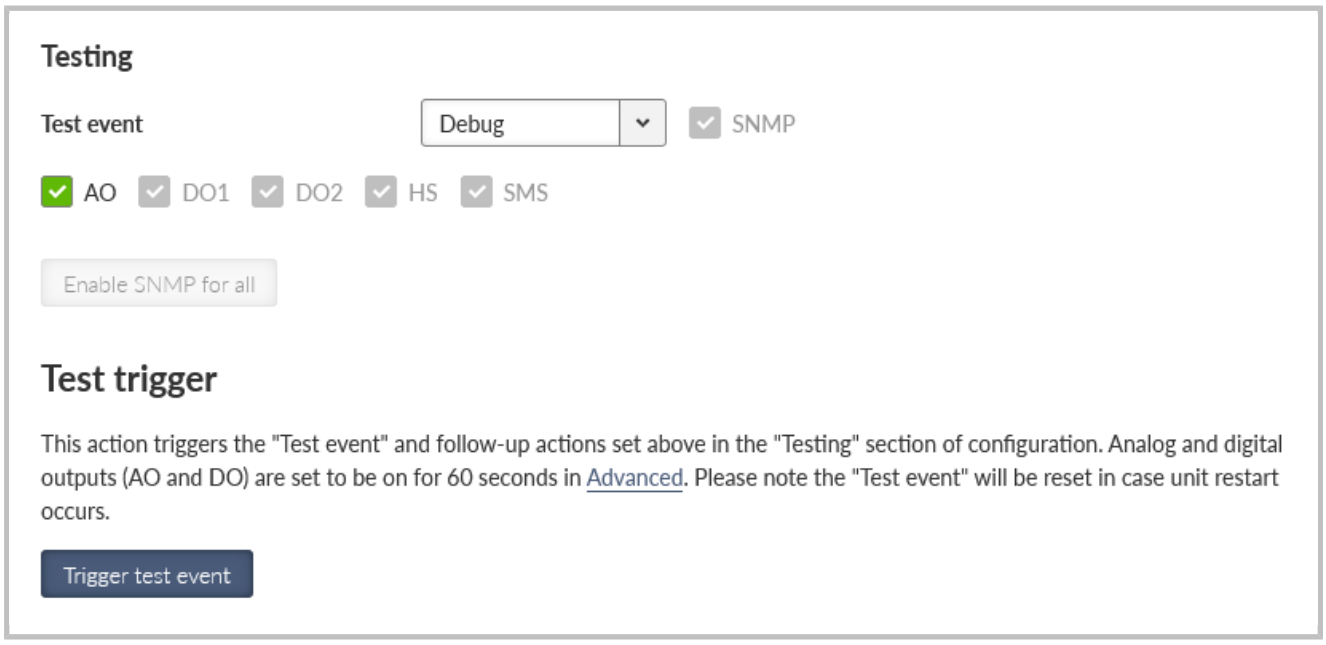


Fig. 4.33: SETTINGS > Device > Events

Pressing the "Trigger test event" button will activate the 'Test event' along with any subsequent actions defined in the 'Testing' configuration section . Specifically, the analog and digital outputs (AO and DO) will be active for 60 seconds (can be changed in Advanced menu).

Note

Unit restart will reset the Test event.

4.6.4. Firmware

4.6.4.1. Local

Unit firmware defines the unit functionality. There are several principles for managing the firmware in the running network:

- Maintain the same version of firmware in the network (recommended). WaSP units are able to co-operate with different versions of firmware running, but using the same firmware version in all units is the best way to keep the network maintenance simple.
- Upgrading firmware to a newer version is not obligatory, unless there are bug/security fixes etc.
- The cyber security issues may force the firmware to be upgraded e.g. when some serious security vulnerability was fixed.

There are 3 stages of the firmware upgrade procedure:

- Choosing new firmware and loading it into the web browser.
- Uploading new firmware into the unit’s internal archive.
- Activating the unit firmware.

Every operation can take up to several tens of seconds.

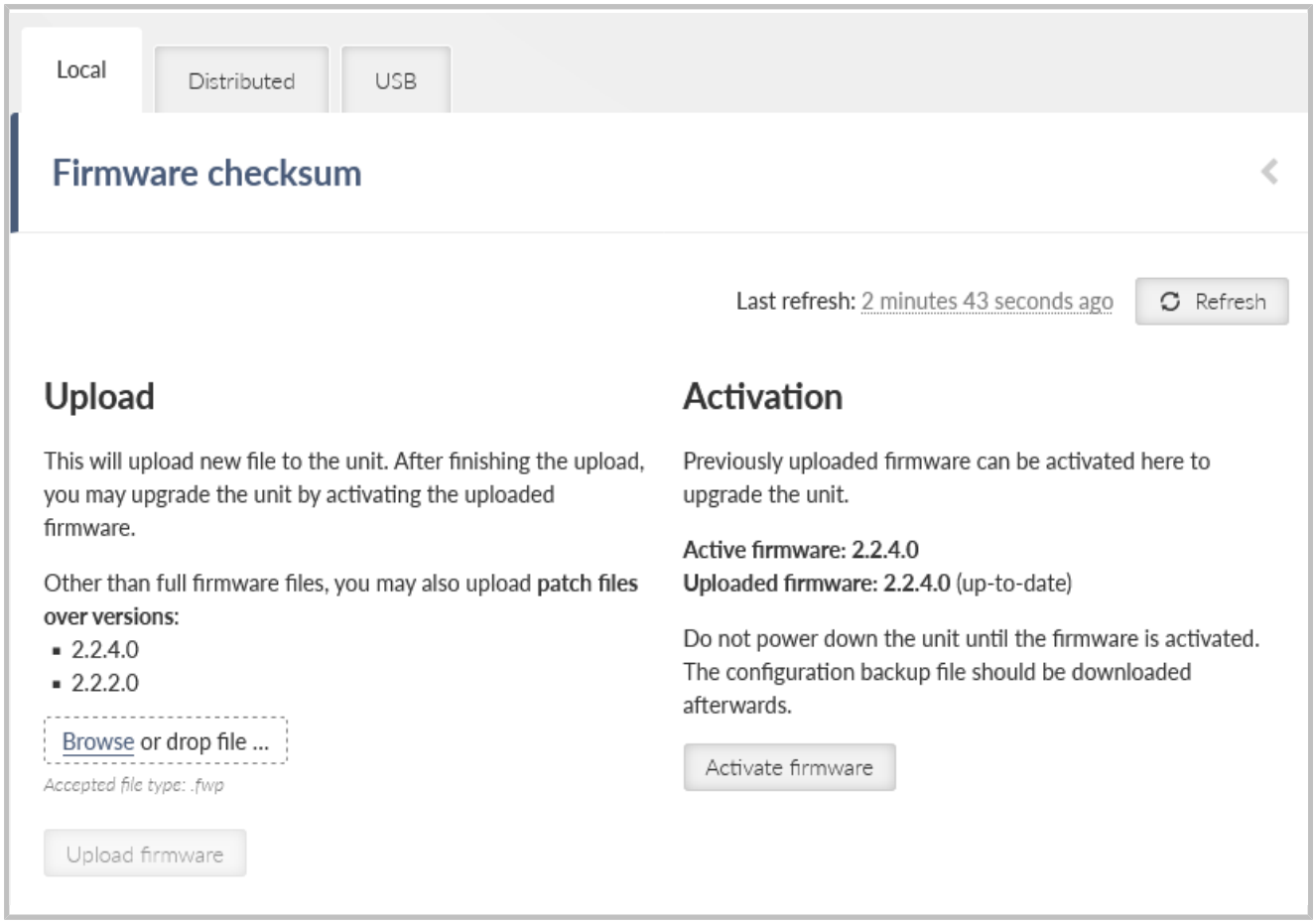


Fig. 4.34: SETTINGS > Device > Firmware

The Status section displays the Firmware checksum. This checksum is unique to each individual unit, differing even between units with the same firmware version. The checksum can also be retrieved via an API call.

Note

Unit configuration backup is recommended after the firmware upgrade. See *Section 4.6.2, "Configuration"* for details.

To upgrade the firmware:

1. Optional (recommended): Backup the current unit configuration (menu SETTINGS > Device > Configuration – Backup and download).
2. Download the required firmware from the *Racom web*[7]: Products – WaSP – Download – Firmware RipEX2 – ripex2-fw-x.x.x.0.fwp
3. Click the **Choose File** button (the button label may differ based on your web browser localization) to select the firmware file.
4. Click the **Upload firmware** button to transfer the firmware file into the unit. The upload can take a long time – depending on the connection speed between the management PC and the WaSP unit. In case of slow connection and file transfer longer than 120 s, the web browser will shut down the

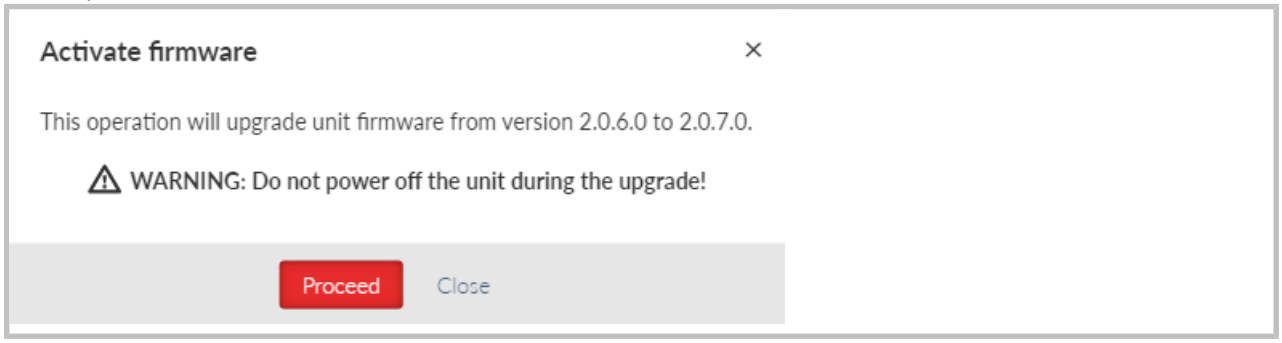
[7] https://www.racom.eu/eng/products/radio-modem-ripex.html#download

connection and the action will not finish successfully. This action does not update the running unit firmware yet. There is no affection on the other communication running through this unit. Successful uploading of the new firmware into the archive is announced in the Notifications and the available firmware version is highlighted under the "Activation" heading as "**Uploaded firmware:**".

Note

Admin level account has a possibility to dissable FW downgrade (menu ADVANCED > Firmware > Firmware - local by seting of the **Enable firmware downgrade** to Off), by default is this functionality allowed.

5. Click the **Activate firmware** button to upgrade (i.e. reinstall) the unit firmware. The upgrade process takes approx. one minute. The user data communication running through this unit is interrupted for a while. All the processes are restarted in a certain moment (e.g. VPN tunnels need to be re-established).



Warning

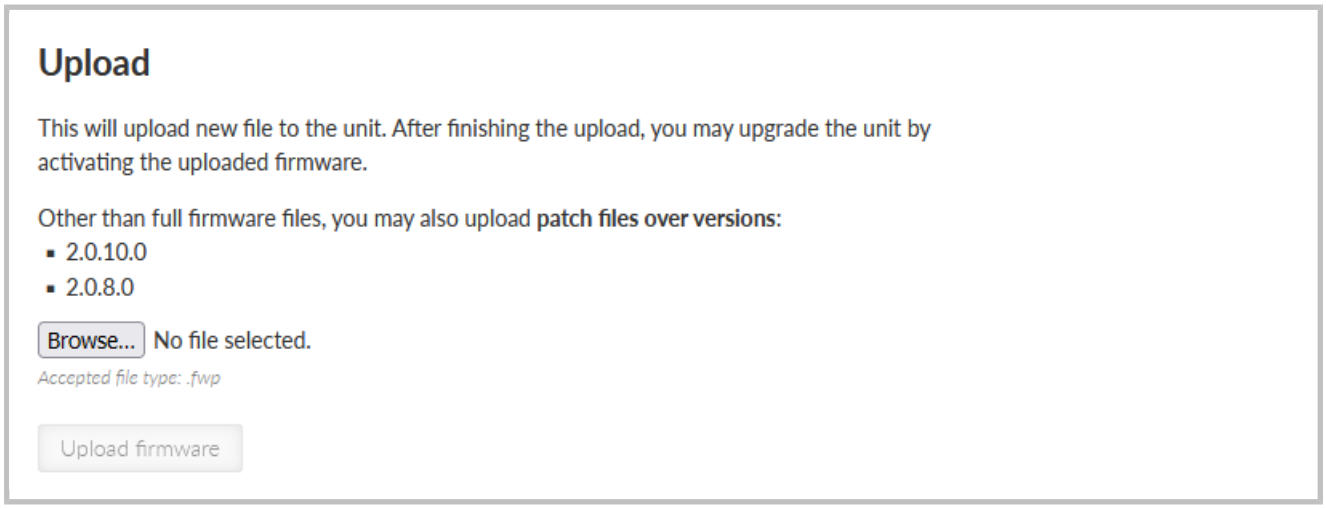
Do not shut down the unit during the firmware update process. It may permanently damage the unit.

6. It is possible not only to upgrade the firmware version, but to even downgrade it, although this operation is not recommended. Be aware of eventual security issues of firmware downgrade as eventually outdated security code can be part of an old firmware. After FW downgrade, all unit parameters will be set to factory defaults.

4.6.4.1.1. Patch files

In some cases, instead of uploading and activating full FW version, patch files can be used. Advantage of the patch files is that they are smaller comparing to the full version files. For successful activation a compatibility between the patch file and active firmware (or uploaded firmware) must be ensured. Patch

files for WaSP can be downloaded from *RACOM's web site*[8]. FW versions stored in WaSP are displayed in SETTINGS > Device > Firmware.



Example: There are 2 older FW versions (2.0.8.0 and 2.0.10.0) stored in WaSP (picture above).

For successful activation of newer FW version (e.g. 2.0.13.0) using patch file either:

- Download patch files version upgrading from 2.0.8.0 to 2.0.13.0 or
- Download patch files version upgrading from 2.0.10.0 to 2.0.13.0 (recommended, because this patch file will be smaller).

The result will be the very same in both cases.

Note

FW versions (both patch files and full versions) are stored in *WaSP archive*[9] .

4.6.4.2. Distributed

When enabled, firmware file (or patch file) can be delivered to this unit using Firmware distribution service. This section configures the receiver part of the service. Receiver units accept distributed firmware files only from authorized senders. When the whole firmware file is accepted, it is saved into units firmware archive. Received firmware must be manually activated (SETTINGS > Device > Firmware > Local > Activate firmware button). Receiver unit will delete all transfers which are older than 14 days.

For more information, see *Section 4.7.1, "Firmware distribution"*.

[8] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr2
[9] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_archive

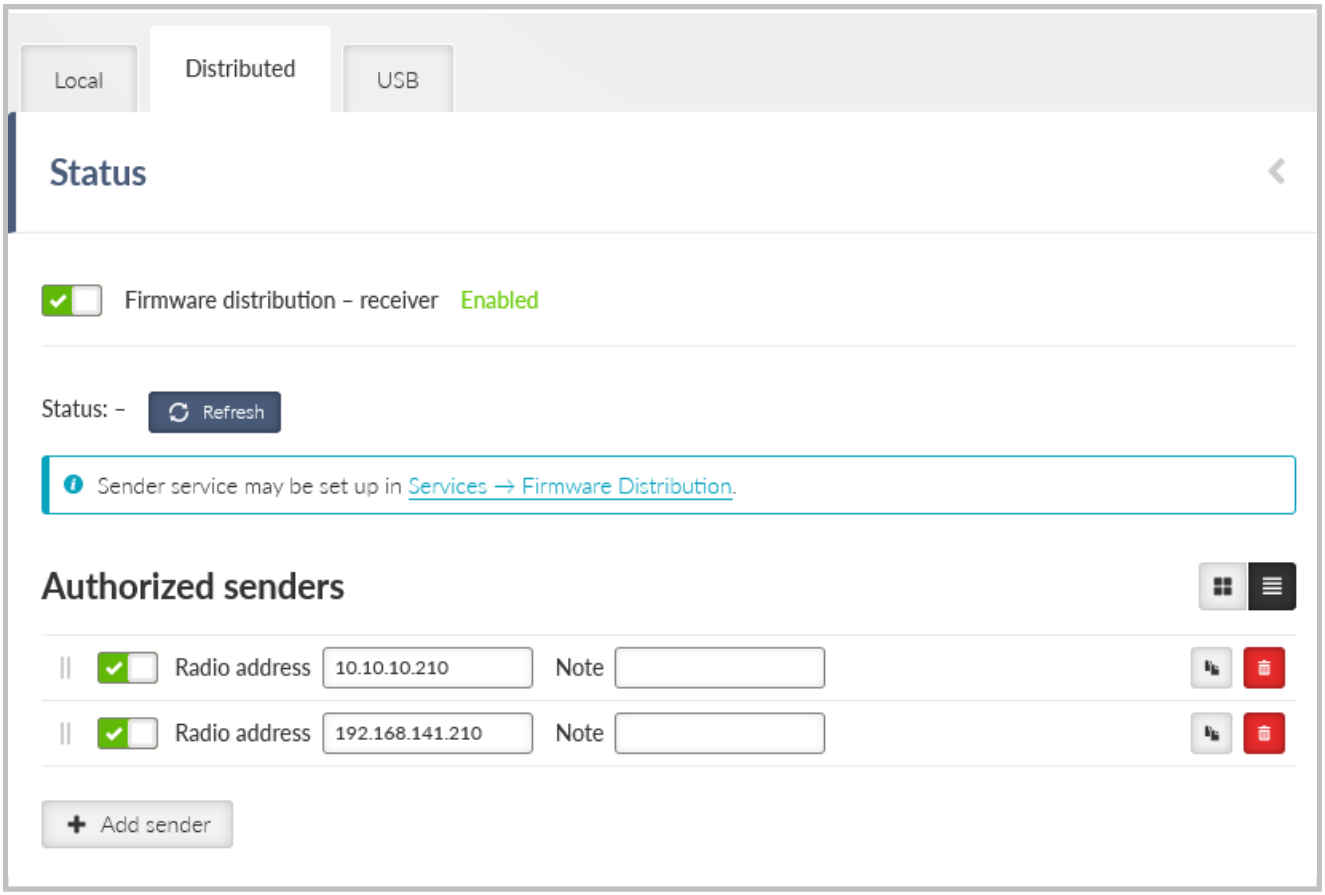


Fig. 4.35: SETTINGS > Device > Firmware > Distributed

Firmware distribution - receiver
Enable; Disable, default = "Disable"
Enables / disables the unit as a receiver.

4.6.4.2.1. Status

Information about running firmware distribution process (status, firmware file name, file size, progress) is described in this section.

4.6.4.2.2. Authorized senders

Defines the sender, from which the receiver unit accepts the distributed FW file.

Enable / Disable
Enables / disables the specific remote radio - sender.

Radio address
Defines the IP address of the radio interface.

Note
Informational note.

4.6.4.3. USB

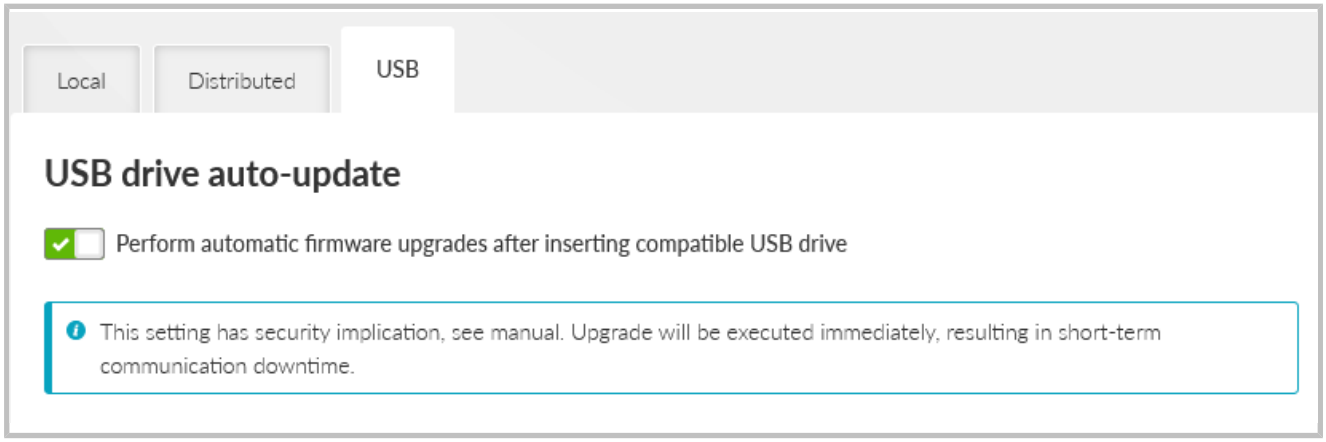


Fig. 4.36: SETTINGS > Device > Firmware > USB

Switch **Perform automatic firmware upgrades after inserting compatible USB drive** allowing FW upgrade from a USB flash disk. Downgrading using a USB disk is not possible. The change of this setting is activated after a new boot process.

The FW of the unit itself will be upgraded (not the FW of an eventual embedded module).

When allowed, the FW upgrade (from the USB flash disk) starts automatically after inserting the USB flash disk into the USB connector. The user is informed about the process via the SYS LED signalization (see Chapter 2.4. *Indication LEDs*).

The following conditions apply to processing:

- The USB drive must contain at least one partition. If there are more partitions, only the first one will be connected to the device.
- The first partition must be primary (physical) and must be formatted with the FAT12, FAT16, or FAT32 file system.
- The FW files must be located in the root directory. Subdirectories are not searched. FW files can be either standard files or soft links.
- The FW file name must have a .fwp or .cpio.enc extension. It does not matter whether the characters are lowercase or uppercase (case insensitive).
- There are no restrictions on the name of the FW file, only the extension rules must be followed. The character set allowed by the file system of the given USB drive (but we still recommend using the standard ASCII set).
- Any number of FW files (FW packages) can be stored on the USB drive (not all of them even have to be for a given device). From these, the device then "chooses" the FW that suits the given HW and has the highest version.
- If two or more suitable FWs are found on the disk, which have the same version, the first one is selected in order according to the lexicographic arrangement (this can happen, for example, if one file is full FW, while the other is FW-patch).

4.7. Services

4.7.1. Firmware distribution

WaSP can distribute its uploaded firmware to other WaSP units. This feature can be used during unit's regular traffic and offers to distribute firmware from one unit (sender) to another unit(s) (receiver) within one network. Firmware distribution is suitable especially in potentially problematic cases, e.g. for units with low signal quality, busy traffic or placed in a hard-accessible environment.

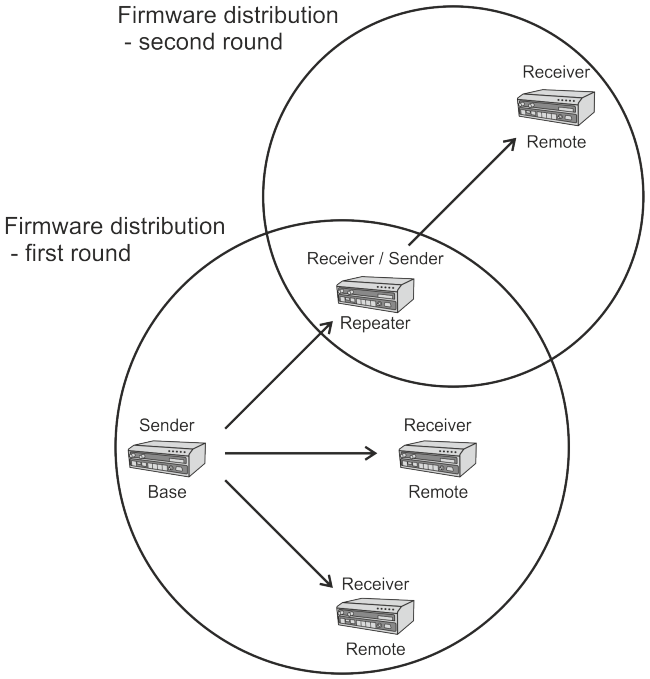
Distribution works over the radio network (FOTA - Firmware over the air) in form of multicast. Units must be available to each other within one IP hop. To set up FW distribution, WaSP unit must be set either as a sender or a receiver.

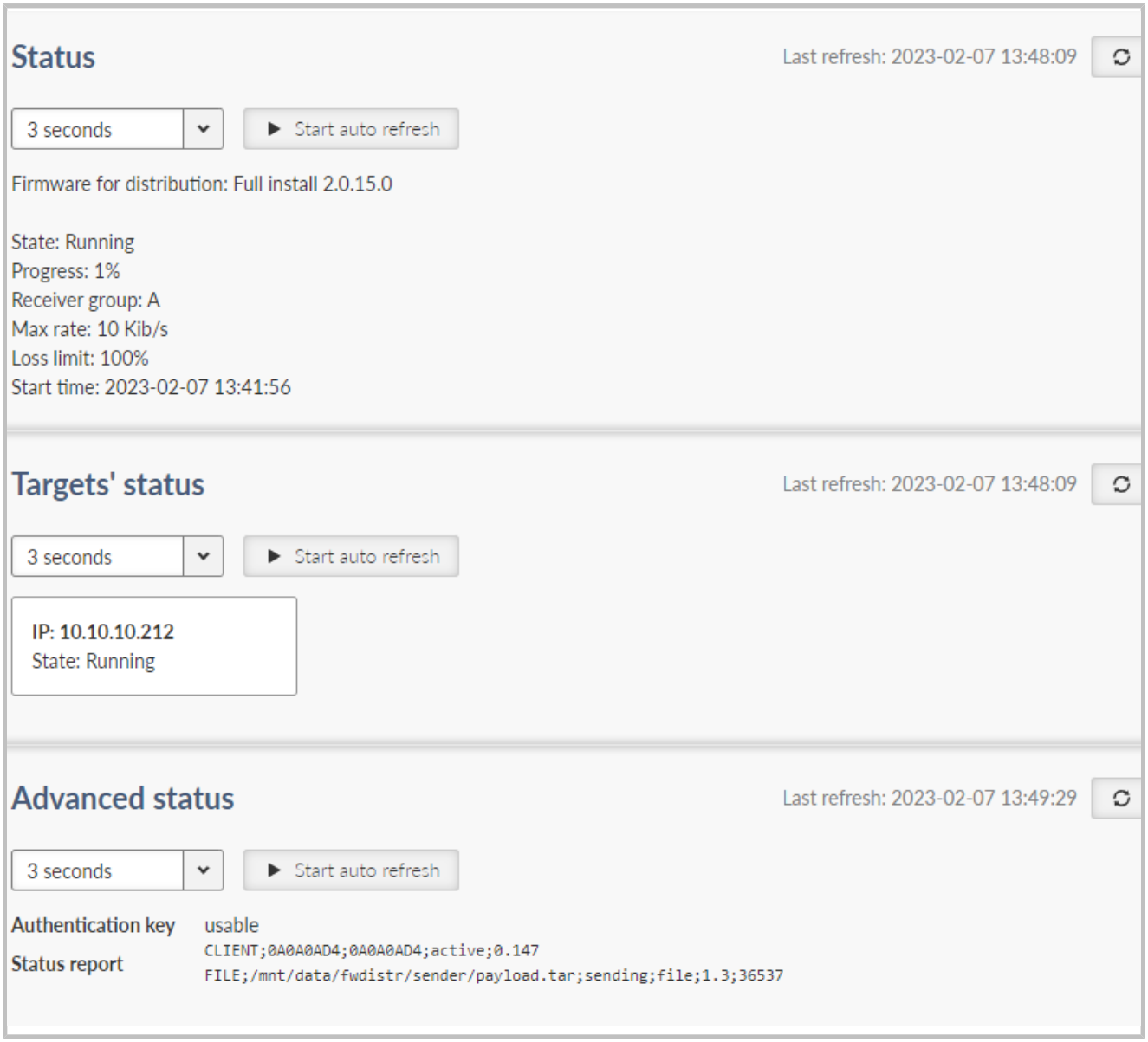
The process of Firmware distribution is composed of individual attempts of delivering the firmware file. The firmware file is uploaded into WaSP's firmware archive. During distribution, the file is divided into multiple pieces (data blocks) which are gradually transferred to defined receiver units (the size of a data block is set to 512 B). If a data block is not transferred successfully (it gets lost), the receiver unit will again request the sender for it, until the data block is received (more information in ***Loss limit*** parameter). Only one file at a time can be distributed.

The transfer can be interrupted by events such as changing the configuration, unit reboot, Hot standby unit switch, etc. When the transfer is interrupted, its status is saved into unit's FLASH memory. The transfer will continue once the unit returns to its normal state. Interruptions which do not save the status (e.g. power outage) can lead into the loss of the distribution progress. If such a case occurs, the transfer will start from the beginning.

Patch files can be also distributed via Firmware distribution. A compatibility between the patch file and firmware of the receiver unit must be ensured (for more information, see *Section 4.6.4.1.1, "Patch files"*.

- When in Flexible protocol, the Firmware distribution works only in a star topology. In case of more complex topology, the firmware distribution must be launched gradually (from star to star). After the first round of firmware distribution finishes, another one can be launched from the repeater. The repeater will be re-configured to a sender and will distribute its uploaded firmware to receiver units within its star topology.


Firmware distribution
- second round
Receiver
Remote
Firmware distribution
- first round
Receiver / Sender
Repeater
Sender
Base
Receiver
Remote
Receiver
Remote


Status
Last refresh: 2023-02-07 13:48:09
3 seconds
Start auto refresh
Firmware for distribution: Full install 2.0.15.0
State: Running
Progress: 1%
Receiver group: A
Max rate: 10 Kib/s
Loss limit: 100%
Start time: 2023-02-07 13:41:56
Targets' status
Last refresh: 2023-02-07 13:48:09
3 seconds
Start auto refresh
IP: 10.10.10.212
State: Running
Advanced status
Last refresh: 2023-02-07 13:49:29
3 seconds
Start auto refresh
Authentication key
usable
Status report
CLIENT;0A0A0AD4;0A0A0AD4;active;0.147
FILE;/mnt/data/fwdistr/sender/payload.tar;sending;file;1.3;36537

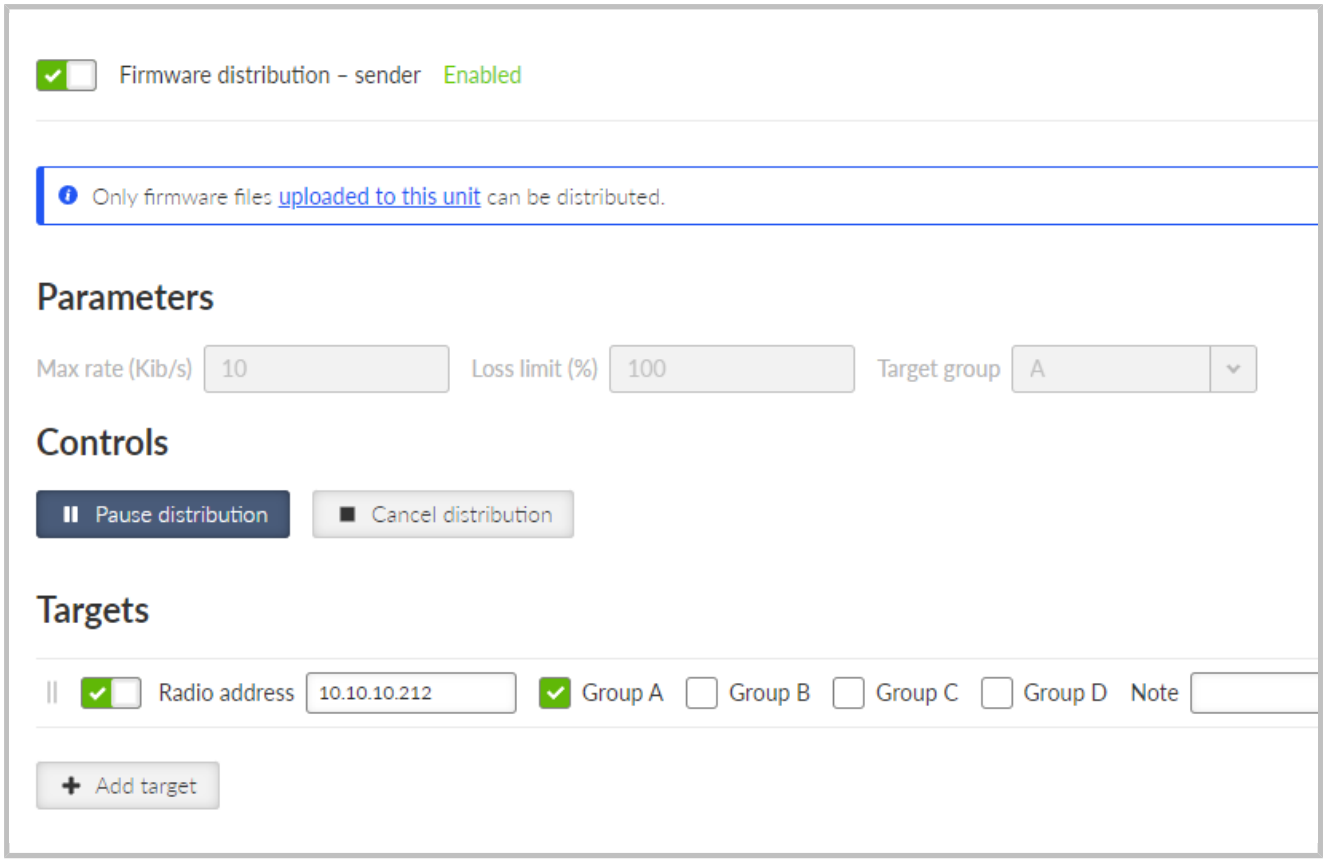


Fig. 4.37: SETTINGS > Services > Firmware distribution

Firmware distribution - sender

Enable; Disable, default = "Disable"

Enables / disables the unit as a sender. When enabled, the unit can transfer its uploaded firmware to defined receiver units.

To set the unit as a receiver, see *Section 4.6.4.2, "Distributed"*.

4.7.1.1. Status

Information about running firmware distribution process (status, progress, receiver group, max. rate, loss limit, start time) is described in this section.

4.7.1.2. Parameters

Max. rate (Kib/s)

Number {1 – 1000}, default = 10

Defines the maximum broadcast speed. The broadcast starts at a lowest speed and accelerates until it reaches the defined limit.

Loss limit [%]

Number {0 – 100}, default = 100

Defines the acceptable % of data loss (lost data blocks) for the first attempt to deliver the file. During the first attempt, receivers which exceeds the set Loss limit can be temporarily disabled from the transfer, so they would not restrain other receivers. After delivering the firmware file to receivers which were not disabled by the Lost limit, the transfer is restarted and attempts to deliver lost data

blocks to remaining units without Loss limit control. The number of attempts is limited to 256. If the data block is not successfully transferred after the last attempt, the transfer is declared to be invalid.

Target group (A, B, C, D)
List box {Group A; Group B; Group C; Group D}, default = "Group A"
Selects the group of receivers to which the firmware will be distributed.

4.7.1.3. Controls

Start / Pause distribution
Starts / Pauses the Firmware distribution. Once the firmware distribution is launched, **Loss limit** and **Target group** cannot be changed.

Cancel distribution
Cancels the Firmware distribution. If the firmware distribution is cancelled, the transfer progress will be lost.

4.7.1.4. Targets

Enable / Disable
Enables / disables the specific remote radio - receiver.

Radio address
IP address, default = 0.0.0.0
Defines the IP address of the radio interface.

Target Group
Click box {Group A; Group B; Group C; Group D}, default = "Group A"
Selects the receiver unit into a individual group to which the firmware will be distributed. One unit can be in multiple groups.

Note
Informational note.

4.7.2. DHCP servers

The DHCP server listens on selected interfaces. When a client from another station requests it, it assigns an IP address (DHCP lease) from the specified range.

Corresponding network interface must have a defined network range that includes the allocated range.

The DHCP server is then used specifically for this interface (ETH1 - ETH2).

Fig. 4.38: SETTINGS > Services > DHCP servers

4.7.2.1. DHCP servers configuration

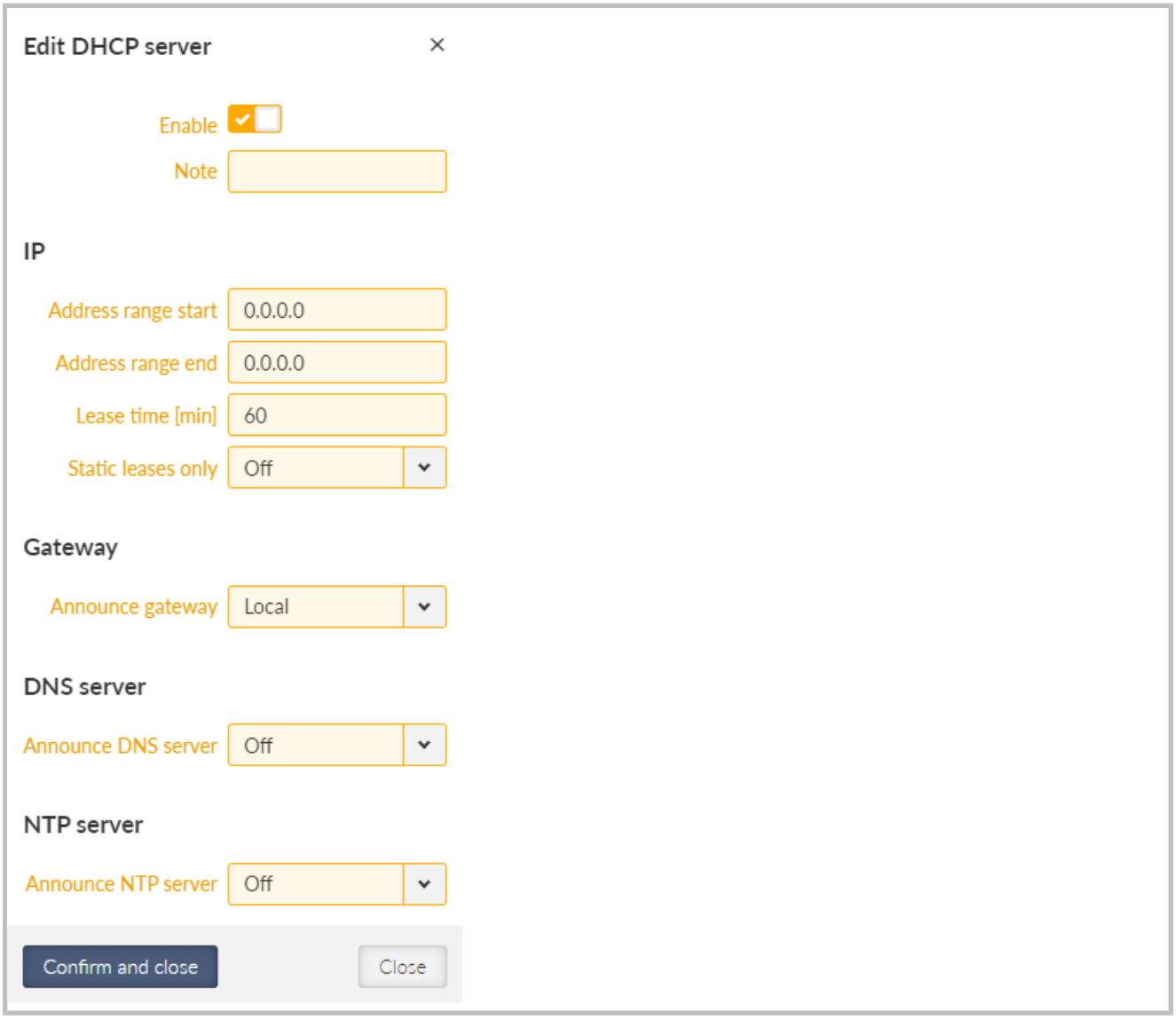


Fig. 4.39: SETTINGS > Services > DHCP servers > Configure

Enable
{Enable; Disable}, default = "Enable"
Enables the currently selected DHCP server.

Note
Informational note.

Address range start
IP address, default = 0.0.0.0
The start of the range of IP addresses allocated. It must be the case that **Address range start** <= **Address range end**.
Address must be in the address range of the ETH, LAN or VLAN.

Address range end
IP address, default = 0.0.0.0

The end of the range of IP addresses allocated. It must be the case that **Address range start** <= **Address range end**.
Address must be in the address range of the ETH, LAN or VLAN.

Note
The ranges of active DHCP servers must not overlap.

Lease time [min]
Number {2 – 10080}, default = 60
Address lease period. It is applied to both dynamic and static addresses.

Static leases only
List box {Off; On}, default = "Off"
Specifies whether the range is used only for allocating fixed (static) addresses. If enabled, it must be in the Static Leases table.

Announce gateway
List box {Off; Local; Manual}, default = "Local"
Configures the announcing of the router to clients.
Off: Gateway is not announced.
Local: The router's IP is announced as a gateway.
Manual: Manually set IP address is announced as a gateway.

Gateway address
IP address, default = 0.0.0.0
The IP address of the gateway being announced.

Announce DNS
List box {Off; Local; Manual}, default = "Local"
Configures the announcing of the DNS server to clients.
Off: DNS server is not announced.
Local: The router's IP is announced as a DNS server. Only if **DNS forwarding** is enabled.
Manual: Manually set IP address is announced as a DNS server.

Primary DNS server
IP address, default = 0.0.0.0
The IP address of the primary DNS server being announced.

Set secondary DNS server
List box {Off; On}, default = "Off"
Determines if the secondary DNS server is announced.

Secondary DNS server
IP address, default = 0.0.0.0
The IP address of the secondary DNS server being announced.

Announce NTP server
List box {Off; Local; Manual}, default = "Off"
Configures the announcing of the NTP server to clients.
Off: NTP server is not announced.
Local: The router's IP is announced as an NTP server. In WaSP, the NTP daemon is always active, even if it only uses local time.
Manual: Manually set IP address is announced as an NTP server.

NTP server
IP address, default = 0.0.0.0
The IP address of the NTP server being announced.

4.7.2.2. Static leases

Fig. 4.40: SETTINGS > Services > DHCP servers > Static leases

Each line defines a static assignment of a fixed IP address to the client based on the MAC address.

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

IP address
IP address, default = 0.0.0.0
The fixed IP address assigned to the client.
Must be unique in the Static Leases table.
Must belong to the parent range in the DHCP Servers table.
It must not conflict with the local station address.

MAC address
MAC address, default = 00:00:00:00:00:00
The MAC address of the client for which the fixed IP address is assigned.
Must be unique in the Static Leases table.

Note
Informational note.

4.7.3. DNS

DNS forwarding functions as a DNS proxy server. Receives DNS queries from clients on selected interfaces. Filters queries. Translation of selected names can be blocked. Sends custom queries to a specified list of servers. Maintains a cache from which the client can respond immediately without querying parent servers.

4.7.3.1. Configuration

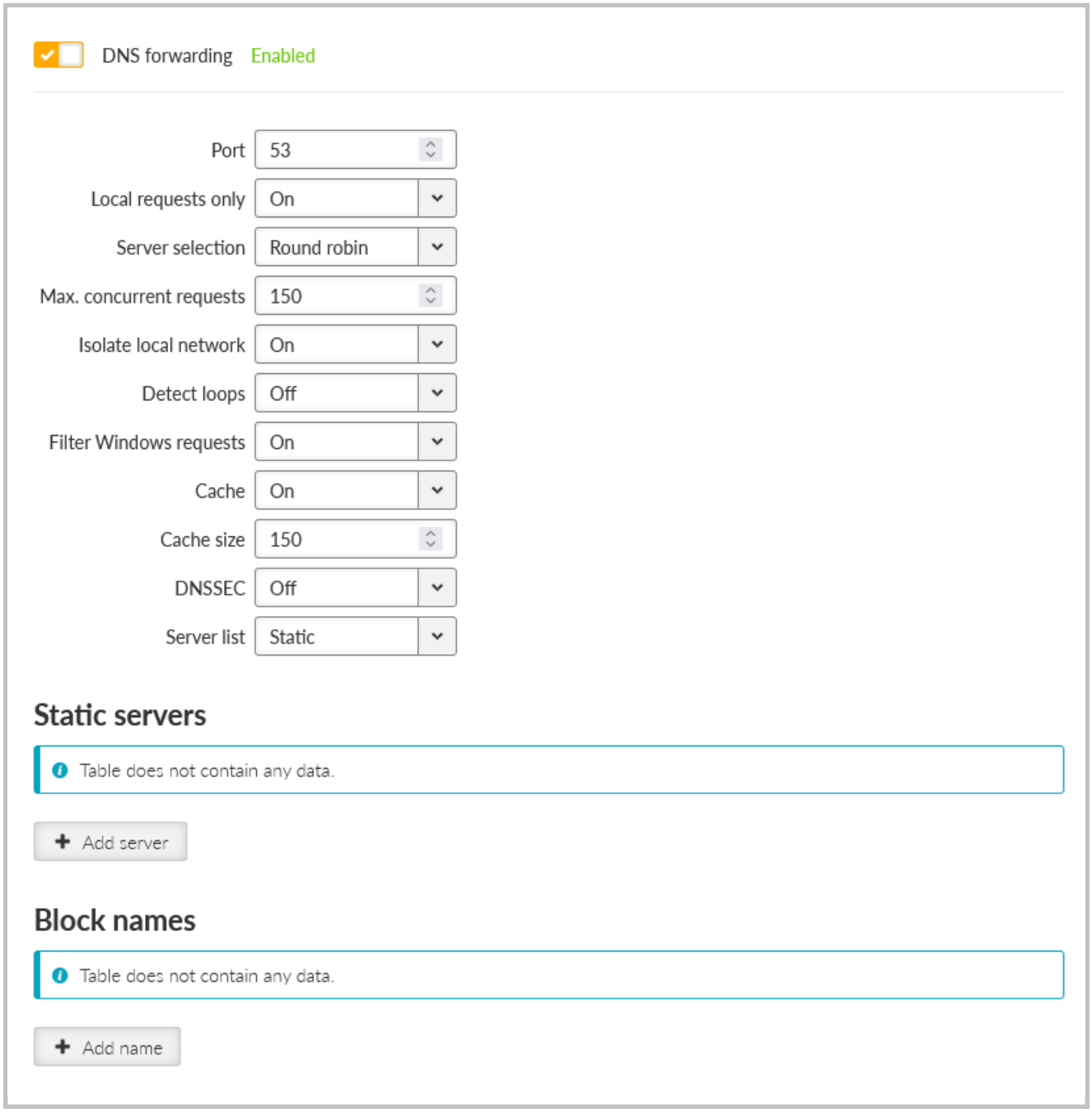


Fig. 4.41: SETTINGS > Services > DNS

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables DNS forwarding.

Port
Number {1 – 65535}, default = 53
The port number (both UDP and TCP) on which the server listens for client requests.

Local requests only
Listbox {Off; On}, default = "On"

Determines if the server only serves requests from addresses on the local network (from addresses in ranges set on the interfaces). Requests from other addresses will be rejected.

Server selection
List box {Round robin; Strict order; All simultaneously}, default = "Round robin"
Sets how servers are selected for the query.

Round robin
Selects servers one by one, preferring those that answered.

Strict order
Always starts with the first server in the list, and tries the next in the sequence if it fails.

All simultaneously
The request is sent to all servers at the same time and the first response is awaited.

Max. concurrent requests
Number {5 – 250}, default = 150
The maximum number of DNS requests running simultaneously.

Isolate local network
Listbox {Off; On}, default = "On"
Determines whether the server isolates the local network. If enabled, it blocks forcing translation of local addresses from parent servers, it does not send reverse queries to private addresses to parent servers.

Detect loops
Listbox {Off; On}, default = "Off"
Enables loop detection between DNS servers.

Filter Windows requests
Listbox {Off; On}, default = "On"
Filters periodic DNS requests generated by Windows.

Cache
Listbox {Off; On}, default = "On"
Enables cache responses to DNS requests. If the response to the client request is cached, it is returned immediately and there is no need to make further requests to the parent servers.

Cache size
Number {50 – 10000}, default = 150
Maximum number of entries in the cache.

DNSSEC
Listbox {Off; On}, default = "Off"
Enables authentication of responses from parent servers using DNSSEC and chain of trust (**DNS trust anchors** table).

Server list
Listbox {Static; Dynamic}, default = "Static"

Static
Static list of servers in the **Static servers** table.

Dynamic
Listbox {WWAN (MAIN); WWAN (EXT); PPP 1; PPP 2; PPP 3; PPPoE client}, default = "PPPoE client"
The list of servers is obtained from the dynamic WAN interface parameters. The corresponding interface must be active.

4.7.3.1.1. Static servers

The rows define the addresses of the parent DNS servers in the static list.

The maximum number of DNS servers is 32.

Active only if Server list is set to Static.

Fig. 4.42: SETTINGS > Services > DNS > Static servers

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Domain
String {0–128 char}, default = <empty>
Domain name.

IP address
IP address, default = 0.0.0.0
IP address of the static server.

Port
Number {1 – 65535}, default = 53
The destination port on which the server listens for DNS requests.

Note
Informational note.

4.7.3.1.2. Block names

Each line defines DNS names whose translation is blocked.

The maximum number of blocked names is 128. The order does not matter.

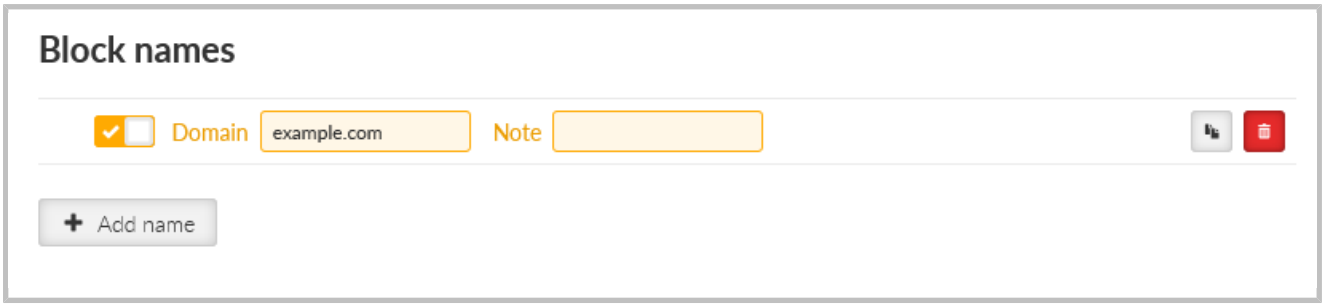


Fig. 4.43: SETTINGS > Services > DNS > Block names

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Domain
String {0–128 char}, default = "example.com"
Domain name, which translation to the address will be blocked.

Note
Informational note.

4.7.3.1.3. DNS trust anchors

Each line defines a DNSSEC Trust Anchor.

The maximum number of DNSSEC Trust Anchors is 8. The order does not matter.

Active only if Cache and DNSSEC are turned On.

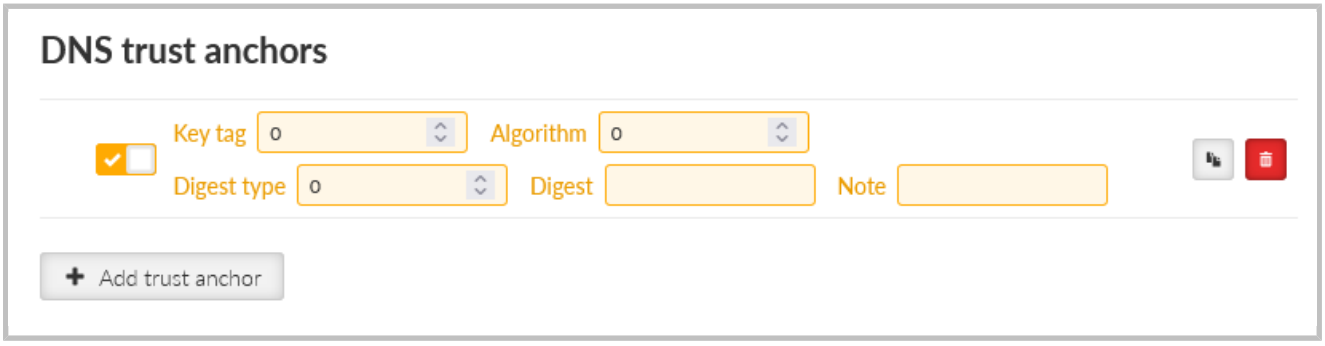


Fig. 4.44: SETTINGS > Services > DNS > DNS trust anchors

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Key tag
Number {0 – 65535}, default = 0
Key identifier. Must be unique among the active lines in the table.

Algorithm
Number {0 – 255}, default = 0
Key algorithm identifier.

Digest type
Number {0 – 255}, default = 0
Key digest algorithm identifier.

Digest
Hexadecimal string, default = <empty>
Digest (hash) key.

Note
Informational note.

4.7.4. SNMP

SNMP (Simple Network Management Protocol) implementation in WaSP provides three SNMP versions: v1, v2c and v3.

Note

Following characters are prohibited in SNMP communication:
" (Double quote) ` (Grave accent) \ (Backslash) $ (Dollar symbol) ; (Semicolon)

SNMP mode
List box {Off; v1_v2c_v3; v3}, default = "Off"
Enables the SNMP and defines which protocol versions are available.

Community name
String {1–32 char}, default = "public"
Community name used by v1 and v2c. When mode v1_v2c_v3 is used, this parameter is mandatory.

Version 3 settings

Security username
String {1–32 char}, default = <empty>
Username for SNMPv3. When v3 protocol is selected, this parameter is mandatory.

Security level
List box {NoAuthNoPriv; AuthNoPriv; AuthPriv}, default = "NoAuthNoPriv"
The v3 protocol security level. Switches on/off Authentication (Auth) and the SNMP data encryption (Priv).

Authentication
List box {MD5_legacy; SHA1_legacy; SHA224; SHA256; SHA384; SHA512}, default = "SHA256"
Authentication algorithm. Legacy algorithms are not recommended to use, they are available for compatibility reasons only.

Authentication passphrase
String {8–128 char}, default = <empty>
Passphrase used for authentication with SNMP server.

Encryption
List box {DES_legacy; AES128; AES192; AES256}, default = "AES128"
Encryption algorithm.

Encryption passphrase
String {8–128 char}
Passphrase used for data encryption when communicating with SNMP server.

Engine ID mode
List box {Default; User defined}, default = "Default"
Engine ID serves for unique identification of the SNMP instance (i.e. the WaSP unit) according to RFC3411. When the "Default" Engine ID mode is selected the MAC address of the ETH1 interface is used for the unique part of the Engine ID (the whole Engine ID example: 800083130302a92006ef).

Engine ID
String {1–27 char}
When "User defined" Engine ID mode is selected the differentiated part of the Engine ID can be entered as ASCII characters or generated (e.g. U3qPrisWoDYbBVNsAWluZYGL3M5). This string is converted into HEX number (i.e. 55 33 71 50 72 69 73 57 6f 44 59 62 42 56 4e 73 41 57 6c 75 5a 59 47 4c 33 4d 35). The whole Engine ID for mentioned example: 800083130455337150726973576f44596242564e7341576c755a59474c334d35.

Notification

Notification is used for asynchronous notification from a WaSP unit into the SNMP server.

Notification mode
List box {Off; Trap; Inform}, default = "Off"
Mode of notification; Inform is not supported by SNMPv1.

Notification version
List box {v1; v2c; v3}, default = "v2c"
Notification packets version.

Inform repeats
Number {0 – 10}, default = 3
Number of repeats used when Inform acknowledge was not received.

Inform timeout [s]
Number {1 – 20}, default = 10
Inform acknowledge timeout.

Notification destinations

Destination IP
IP address, default = 0.0.0.0
IP address of SNMP server receiving notification packets.

Destination port
Number {1 – 65535}, default = 162
Notification packets destination port.

For more detailed information, please see *SNMP application note*[10].

[10] https://www.racom.eu/eng/products/m/ripex/app/snmp-ripex2/index.html

4.7.5. Syslog

Syslog enables logging of events on a remote server. Syslog messages are created in the unit in accordance with RFC5424 and sent to a remote server. Messages can be sent using UDP or TCP.

New system logs and events start to be sent to the remote server after the station boots. Incase of unavailability of the remote server, the logs are stored in the disk buffer and sent to the remote server after re-establishing a connection with it.

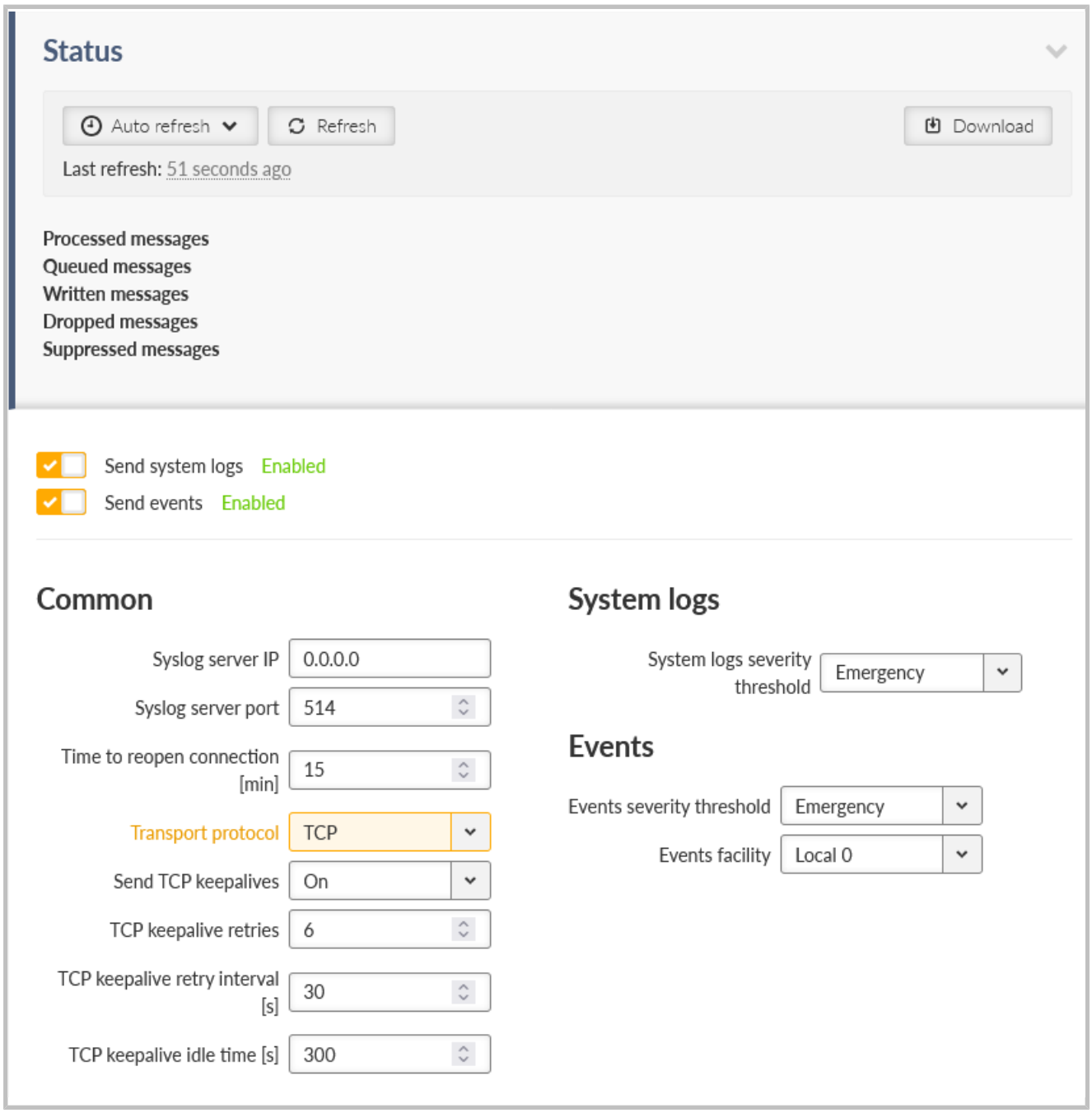


Fig. 4.45: SETTINGS > Services > Syslog

Send system logs
{Enable; Disable}, default = "Disable"
Activates/Deactivates sending of system logs to the remote server

Send events
{Enable; Disable}, default = "Disable"
Activates/Deactivates sending of system events to the remote server

Common

Syslog server IP
IP address, default = 0.0.0.0
IP address of the remote syslog server

Syslog server port
Number {1 – 65535}, default = 514
Syslog remote server port number

Time to reopen connection [min]
Number {1 – 240}, default = 15
Time (in minutes) to wait to retry of the connection to the remote server when the connection was closed

Transport protocol
List box {UDP; TCP}, default = "UDP"
Type of the protocol for the data transport

When TCP:

Send TCP keepalives
List box {Off; On}, default = "On"
Switches On/Off sending of the TCP keepalives messages

TCP keepalive retries
Number {1 – 15}, default = 6
Number of keepalive retries when the reply was not received.

TCP keepalive retry interval [s]
Number {10 – 240}, default = 30
The interval (in seconds) at which a TCP keepalive message is re-sent if no response is received.

TCP keepalive idle time [s]
Number {60 – 64800}, default = 300
Connection inactivity time (in seconds) waiting for the TCP keepalive message to be sent.

System logs

System logs severity threshold
List box {Emergency; Alert; Critical; Error}, default = "Emergency"
System messages with this and higher severities will be sent to the remote server. Messages with lower severities will not be sent.

Events

Events severity threshold
List box {Emergency; Alert; Critical; Error; Warning; Notice; Informational}, default = "Emergency"
System events with this and higher severities will be sent to the remote server. Events with lower severities will not be sent.

Events facility

List box {Local 0; Local 1; Local 2; Local 3; Local 4; Local 5; Local 6; Local 7}, default = "Local 7"
Classification of system events into facilities as per RFC 5424 for local use: Local 0 to Local 7 (numerical codes 16 to 23) can be set. Consult with your Syslog server administrator about which facility will be used for individual groups of units.

4.8. Advanced

WaSP introduces new concept for expert settings and rapid deployment of new features called “Advanced” section. Advanced section displays all configuration set points currently present in the device automatically, without need to design a special configuration page (like the ones in “Settings”). This allows us to deploy new features rapidly with each new firmware and also allows experienced users to fine-tune their WaSP.

Please note, that WaSP is a very powerful device and it really shows all parameters in the Advanced section.

When you visit the page for the first time, you will see a search field and below a tree of configuration pages.

Search field looks through all labels and the tree itself and is capable of showing all relevant configuration pages. It features so called “fuzzy” search capable of returning right answers even when there is a typo in search query. Try searching for “Ethernet” or “BGP” to see the feature in action. To use the whole tree again, simply delete search query.

Configuration tree has two parts. For your convenience first few items (Interfaces, Routing, …) use similar hierarchy to “Settings”, but include all advanced settings. The newest features then can be found in the last item called “Generic”, which contains all configuration tables there are in the unit.

By selecting a configuration page (marked with pencil icon) a window is shown on the right side of the screen containing selected configuration page set points. You can change settings and then send them to the device the same way you know from “Settings”.

Be careful when adjusting settings in Advanced section and review the “Changes” page in detail before sending changes to the device.

5. Diagnostics

5.1. STATUS overview

Provides overview information about individual sections of the unit. Each section is linked with an area of Events (see Section 8.4, *“Events”*).

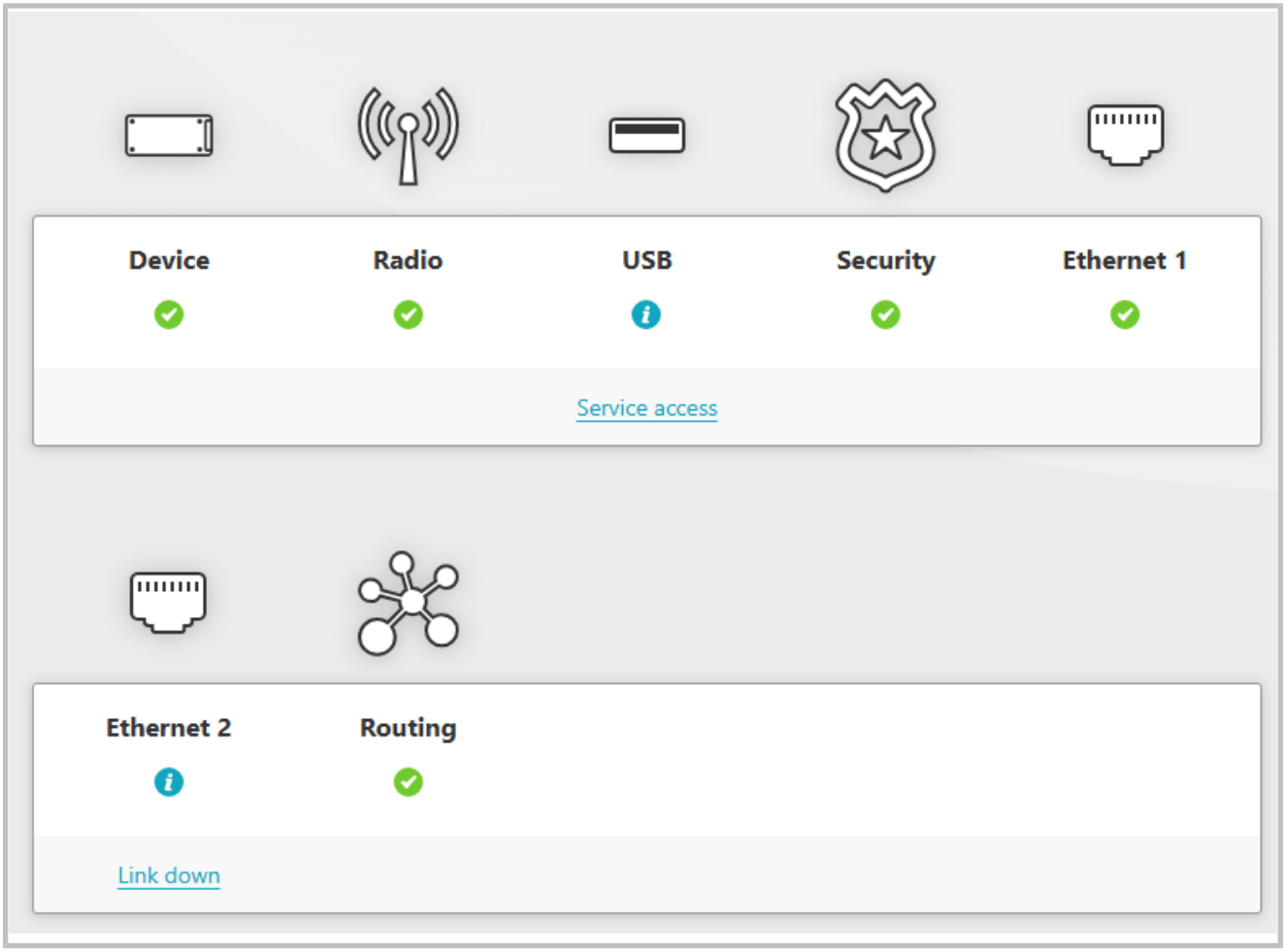


Fig. 5.1: STATUS

When any event with severity higher than Notice occurs in the unit, corresponding icon will change the color according to the severity of the event, the link leads to further information about the event in the DIAGNOSTICS menu. STATUS also shows and describes alarms in last week which are highlighted under icons. Latest 25 Emergency, Alert, Critical and Error Events are displayed at the bottom of the page.

Tab. 5.1: Unit section icons

	USB
	Security

	Ethernet 1-2

Note

The number of visible Ethernet icons is depended on the units settings. (SETTINGS > Interfaces > Ethernet > Ports)

To each event an individual severity can be assigned. When multiple Events with different severities are triggered in the same section, the priority goes: Error > Warning > Notice.

Tab. 5.2: Severity icons

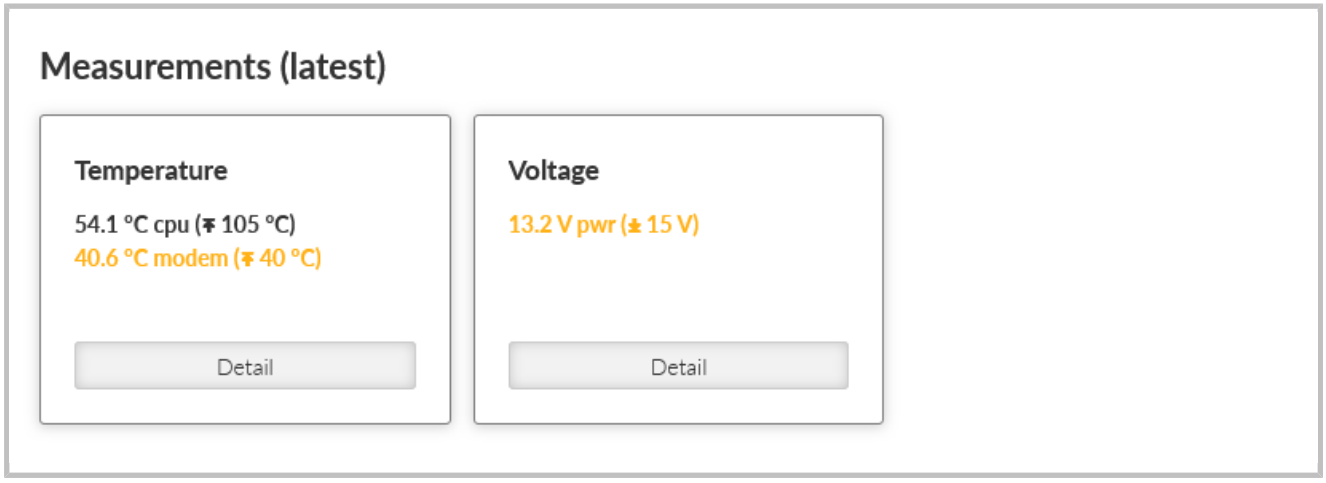
	Unit works flawlessly
	Informational, Notice
	Warning
	Error, Critical, Alert, Emergency

5.2. Overview

The Overview section serves to give general information about the WaSP.

5.2.1. Measurements

Section Overview - Measurements contains current data measurement (obtained from sensors).



- Card Temperature - provides data about temperature (on CPU, modem and radio).

Note

If the temperature exceeds its specified range (-45 – +95 °C), the radio receiving/transmitting will be blocked. If the temperature will return to a specified range (-40 – +85 °C), the radio starts receiving/transmitting again.

This feature can be disabled in parameters ADVANCED > Interfaces > Radio > Radio parameters > Block radio in extreme temperatures.

- Card Voltage - provides data about voltage measured on input connector.

Arrow-headed symbols (↑, ↓, →) have following meaning:

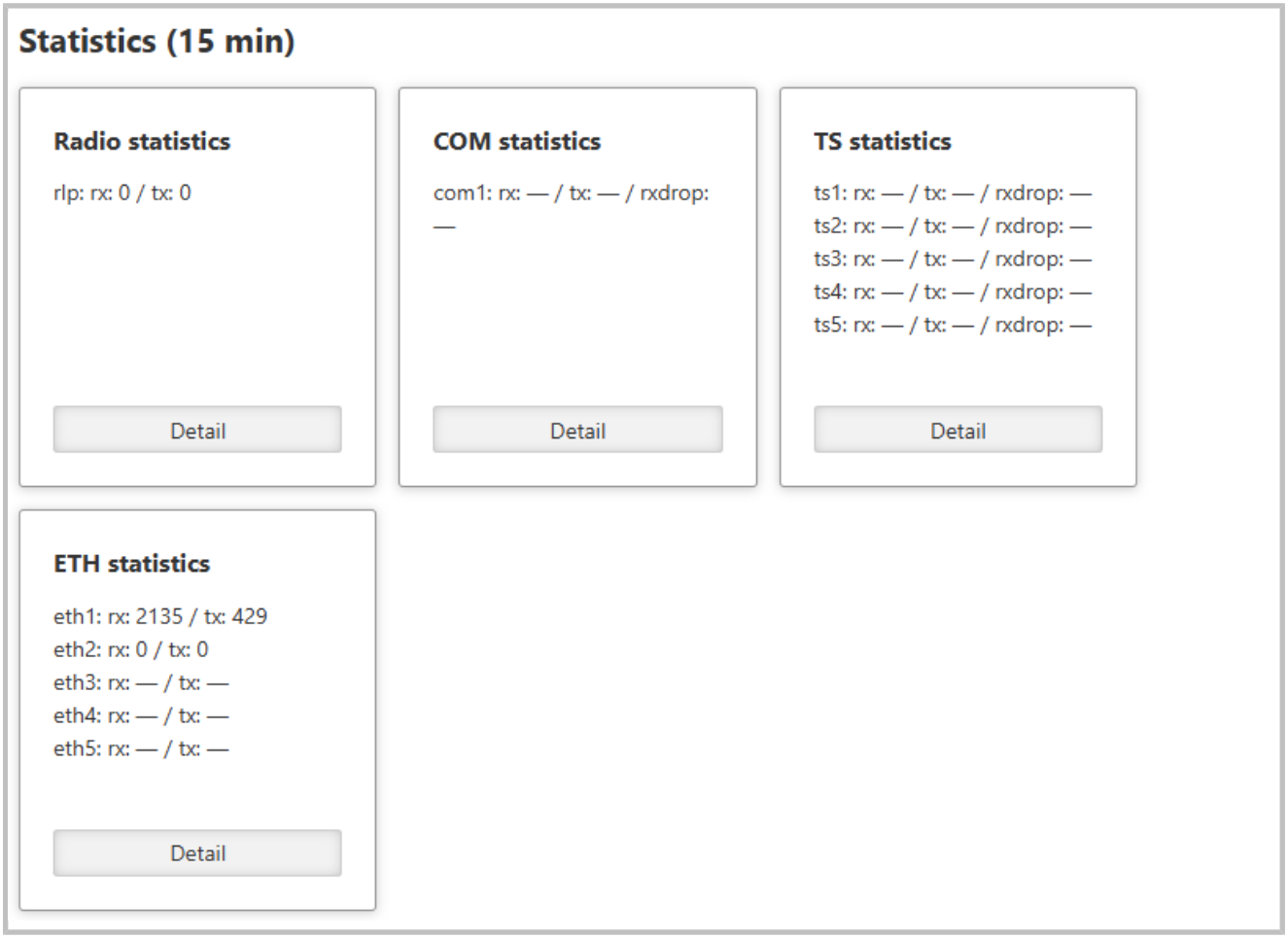
- ↑ - Maximum-limit value. An alarm is triggered, when the value (displayed in brackets) is exceeded.
- ↓ - Minimum-limit value. An alarm is triggered, when the value falls under the value, which is displayed in the brackets.
- →- Value is supposed to head to another one.

Note

Value measurements are collected once per 10 s (excluding radio interface, where values can be collected once per 10 s or more often – depends on the radio communication character).

5.2.2. Statistics

Section Overview - Statistics shows a short view of the statistics over last 15 minutes (from the time of opening the window or pressing Refresh button).



- Cards Statistics are always displayed for all interfaces.
- If the interface is off, its statistics (record) is displayed as “-“.
- Statistics collection is updated every 1 s (each second is possible to see new values).

- 15-min interval is collected by taking 14 mins from history + seconds passed from current minute.

5.3. Information

This section provides more detailed information (data extract) about settings of WaSP unit. It provides also a deeper explanation about some of set values and interfaces. Diagnostic data are provided as well.

5.3.1. Interfaces

Provides a complete information extract about all active interfaces (addresses, details and statistics included). All interfaces used by the linux router (including all internal interfaces like npi, loop, ag, ip6tnl, etc.) are displayed in this section.

5.3.1.1. Ethernet Interfaces

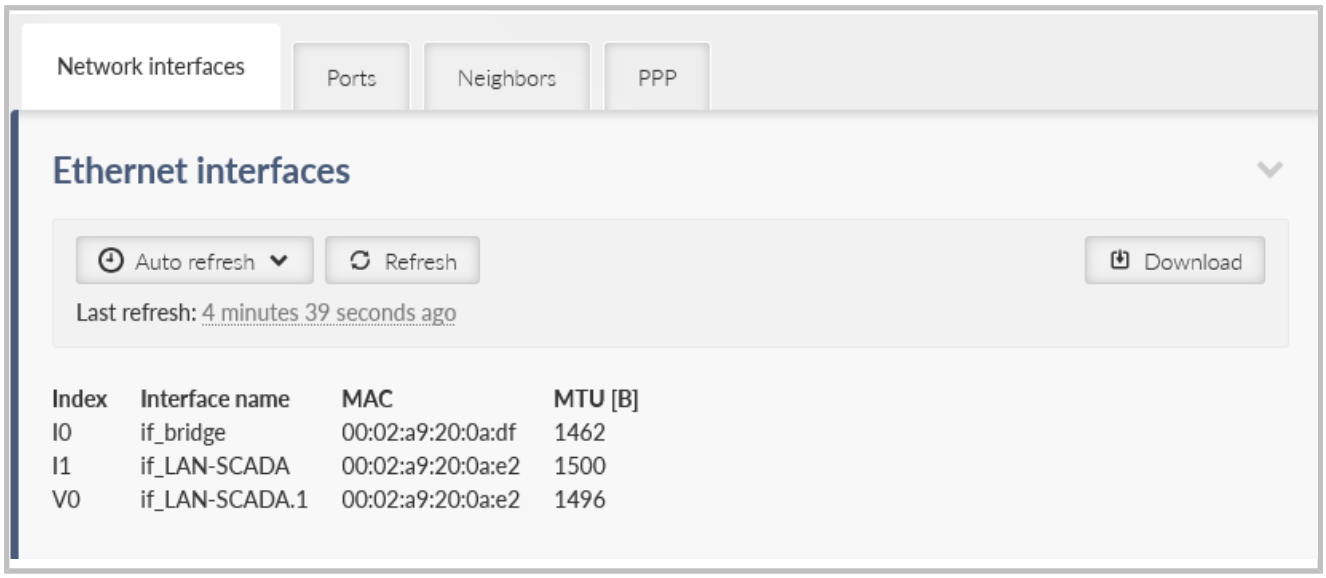


Fig. 5.2: DIAGNOSTICS > Information > Interfaces > Ethernet

Interfaces used in WaSP units are in general either Bridged ports (BP-L2) or Routed interfaces (RI-L3).

All interfaces used by the linux router (internal interfaces excluded) are displayed in the following list.

if_<*LanIface_Name*>
LAN bridge interface RI-L3 type
(SETTINGS > Interfaces > Ethernet > Network interfaces)

if_<*LanVlan_IfName*>.<*LanVlan_VlanId*>

- VLAN BP-L2 interface type (if used as a port in LAN bridge) (SETTINGS > Interfaces > Ethernet > Network interfaces>VLAN)
- VLAN RI-L3 interface type (if not used as a port in LAN bridge) (SETTINGS > Interfaces > Ethernet > Network interfaces > IP/Subnet > VLAN)

5.3.1.2. Network Interfaces

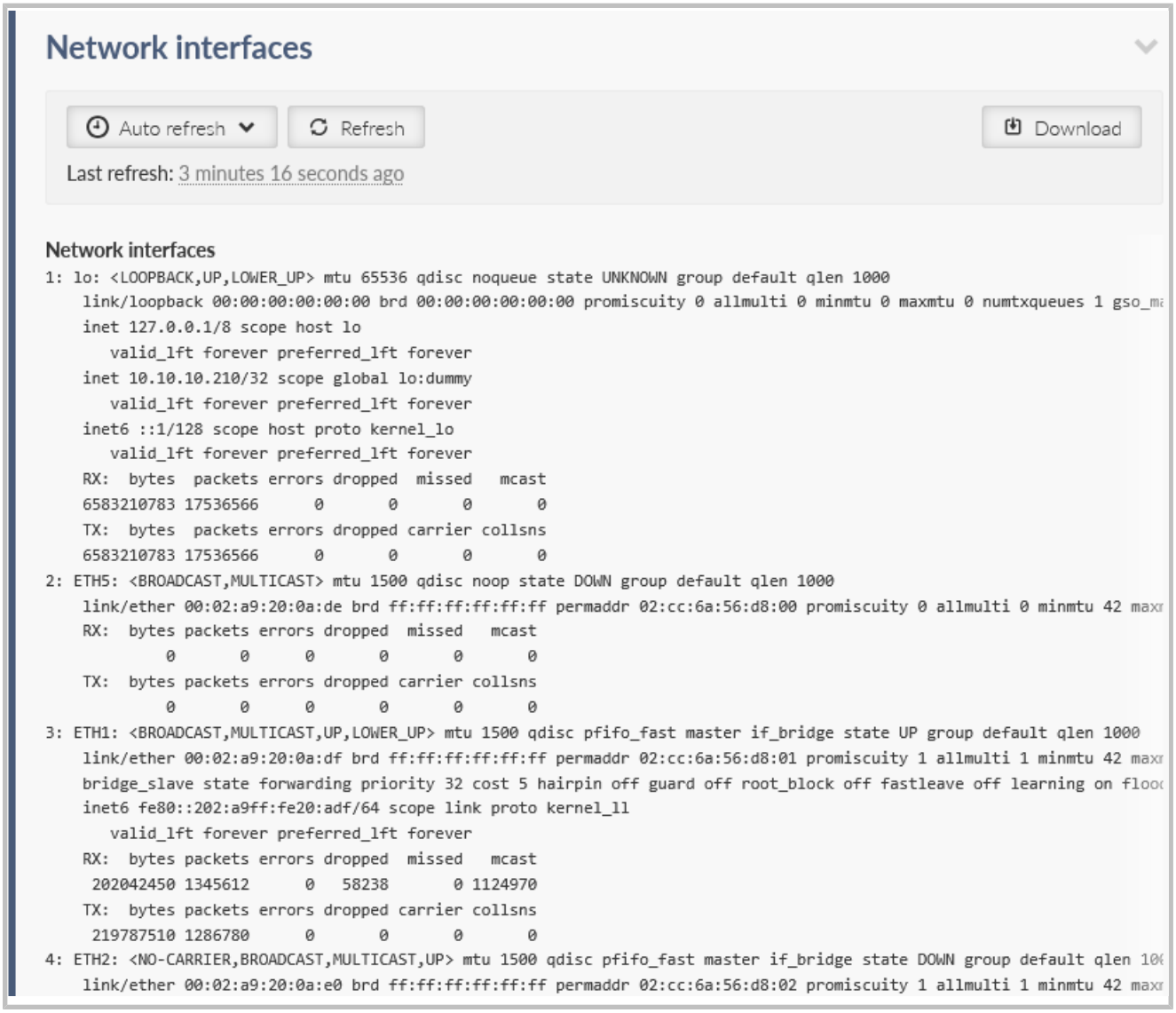


Fig. 5.3: DIAGNOSTICS > Information > Interfaces > Ethernet

eth1, eth2
Interface of physical Ethernet ports ETH1 – ETH2, BP-L2 interface type

eth0
Interface of physical port SFP (ETH5), BP-L2 interface type

radio
RF radio interface

- BP-L2 interface type when Bridge mode of Radio interface is used (SETTINGS > Interface > Radio)
- BP-L2 interface type when Bridge mode of Radio interface is used (SETTINGS > Interface > Radio)

ext
Bridge interface of the EXT cellular module, RI-L3 interface type (SETTINGS > Interface > Cellular > EXT)

gre_tap*<INDEX>*
GRE L2 tunnel interface, BP-L2 interface type (SETTINGS > VPN > GRE > L2)

gre_tun*<INDEX >*
GRE L3 tunnel interface, RI-L3 interface type (SETTINGS > VPN > GRE > L3)

lo
Loopback interface RI-L3 type of interface – The IP addresses of the loopback (ADVANCED > Interfaces > Loopback).

5.3.1.3. Radio interface

Fig. 5.4: DIAGNOSTICS > Information > Interfaces > Radio

5.3.1.4. PPPoE client

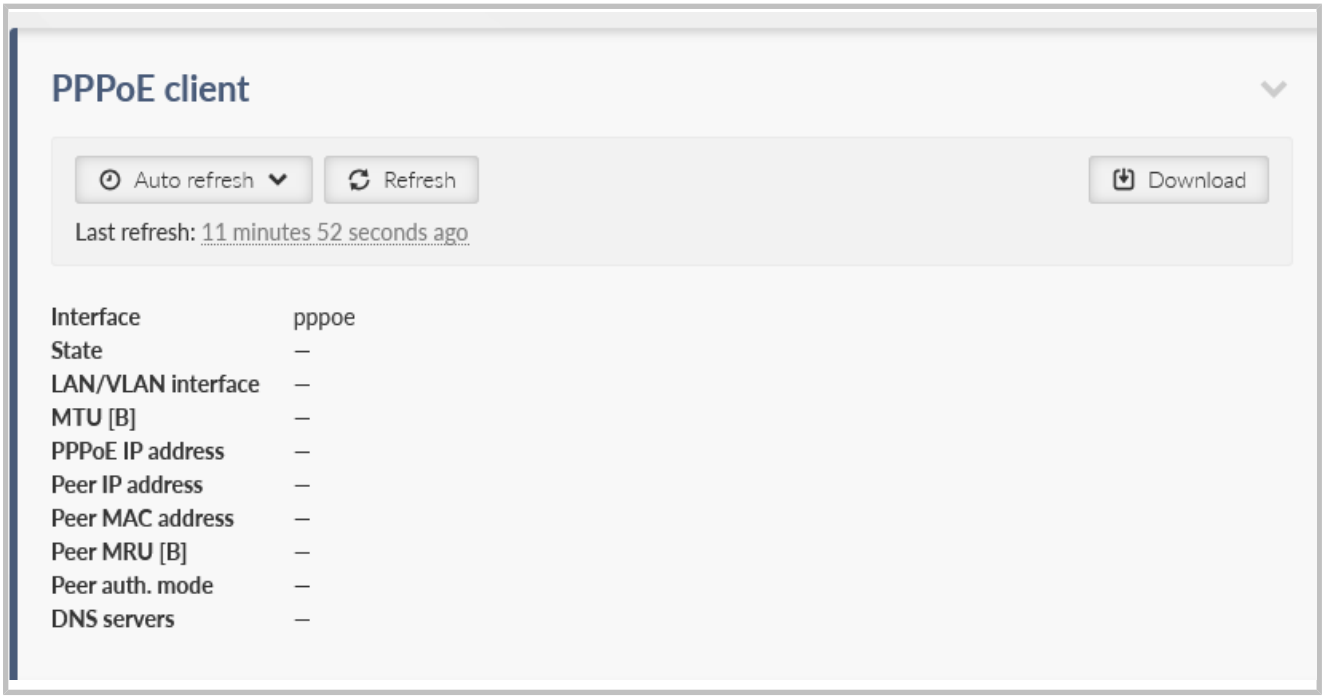


Fig. 5.5: DIAGNOSTICS > Information > Interfaces > PPPoE client

Interface	PPPoE interface name
State	Current state of the interface
LAN/VLAN interface	Name of the LAN/VLAN interface on which the PPPoE client is running
MTU [B]	MTU of the LAN/VLAN interface on which the PPPoE client is running
IP address	Assigned IP address
Peer IP address	IP address of the peer (server)
Peer MAC address	MAC address of the peer (server)
Peer MRU [B]	Maximum Receive Unit (MRU) in bytes requested by the negotiating peer
Peer auth. mode	Authentication protocol requested by the peer
DNS servers	IP addresses of DNS servers, separated by a space

5.3.1.5. Wi-Fi

Provides a detailed info about Wi-Fi Access point and connected Wi-Fi clients.

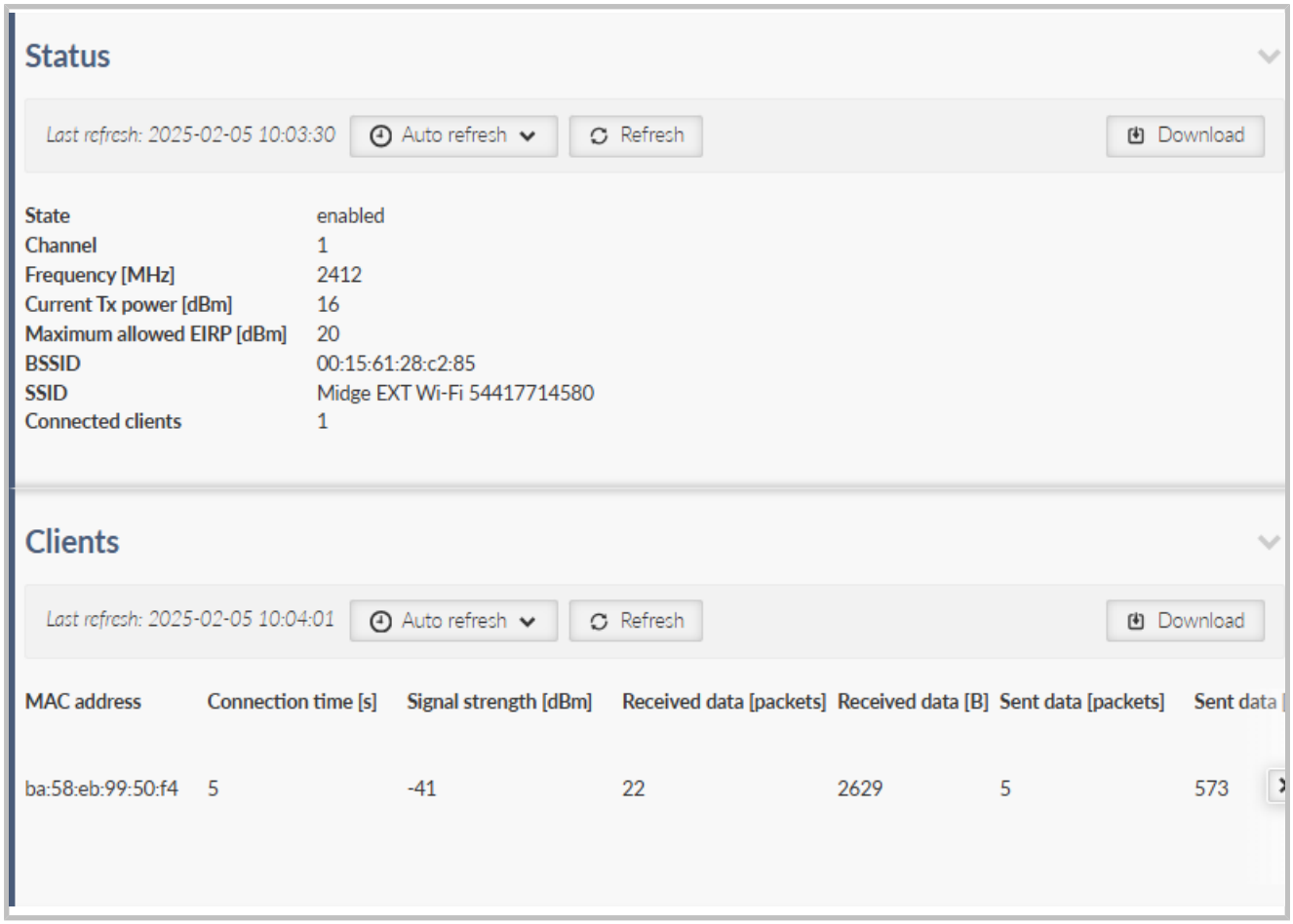


Fig. 5.6: DIAGNOSTICS > Information > Interfaces > Wi-Fi

5.3.2. Routing

Provides information about data extract from section Routing.

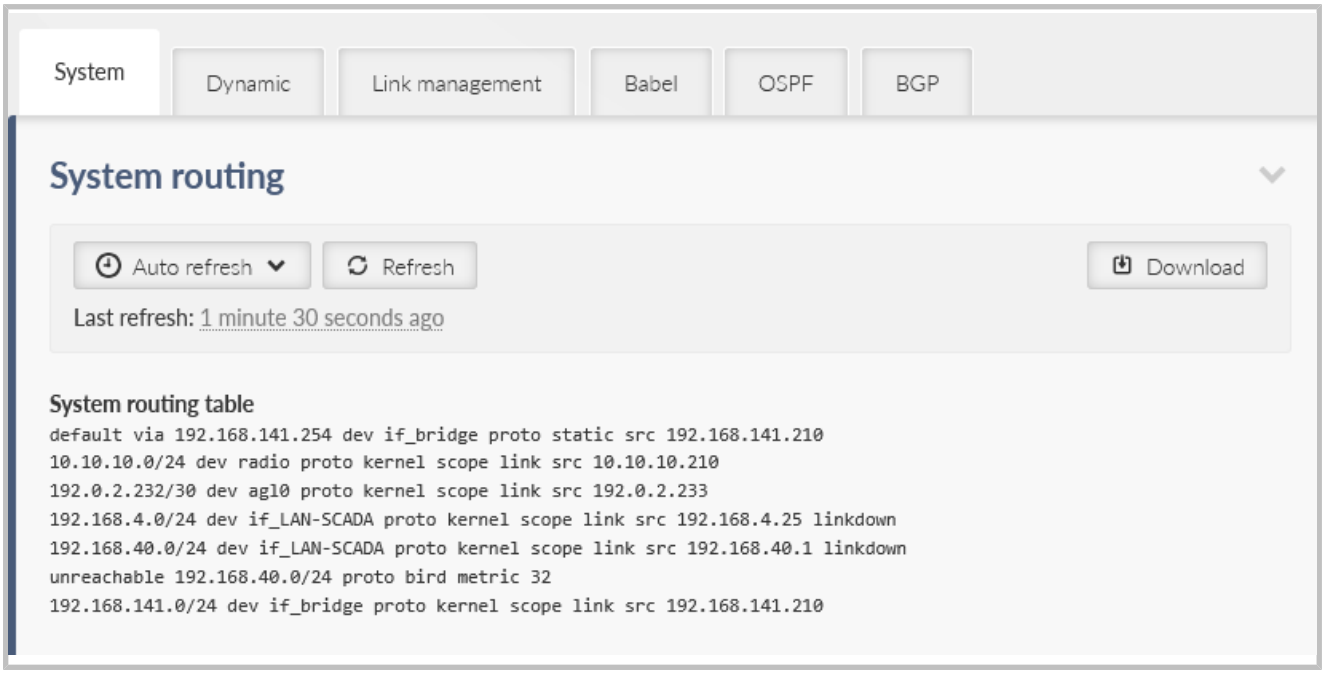


Fig. 5.7: DIAGNOSTICS > Information > Routing

This section is divided into following parts:

- System - complete data extract of system routing table. Displays data called by linux command “ip route show”.
- Dynamic - complete data extract of internal routing table of dynamic routing service bird master4. Displays data called by linux command “birdcl show route all table master4”.
- Babel - data extract of status of Babel protocol. Displays data called by following linux commands: “birdcl show babel interfaces”, "birdcl show babel neighbors", "birdcl show babel routes", "birdcl show babel entries", "birdcl show route all table babel_ipv4".
- OSPF- data extract of status of OSPF protocol. Displays data called by following linux commands: "birdcl show ospf neighbors", "birdcl show ospf state", "birdcl show ospf interface", "birdcl show route all table ospf_ipv4".
- BGP - data extract of status of all BGP protocol instances. Displays data called by following linux commands: "birdcl show protocol '"bgp*"'", "birdcl show protocol all '"bgp*"'", "birdcl show route all table bgp_ipv4".

5.3.3. Firewall

Provides general overview about data extract from sections L2, L3 and NAT.

5.3.3.1. Firewall L2

Displays data called by linux command “iptables -L”.

Fig. 5.8: DIAGNOSTICS > Information > Firewall > L2

5.3.3.2. Firewall L3

Displays data called by following linux commands “iptables -nvL --line-numbers”.

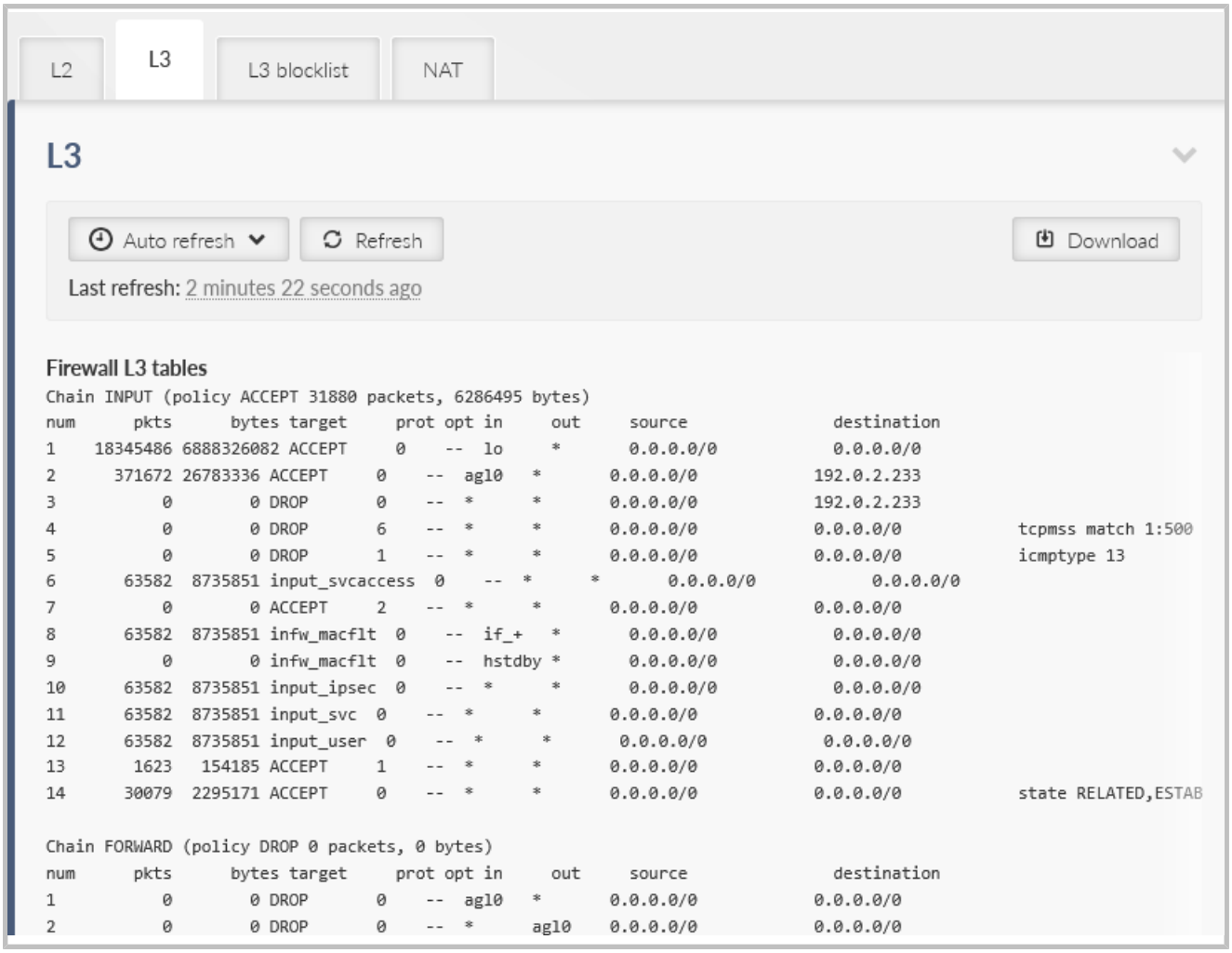


Fig. 5.9: DIAGNOSTICS > Information > Firewall > L3

5.3.3.3. Firewall L3 blocklist

Listing of the list of banned addresses. Addresses are added to the list if the Action: “Deny, Add to Blocklist” (adding the source address of the incoming packet to the banned list) is configured in the Firewall L3 - Input rules

5.3.3.4. NAT

Displays data called by following linux commands:

- "iptables -t nat -nvL postrouting_user" – data about SNAT
- "iptables -t nat -nvL prerouting_user" – data about DNAT

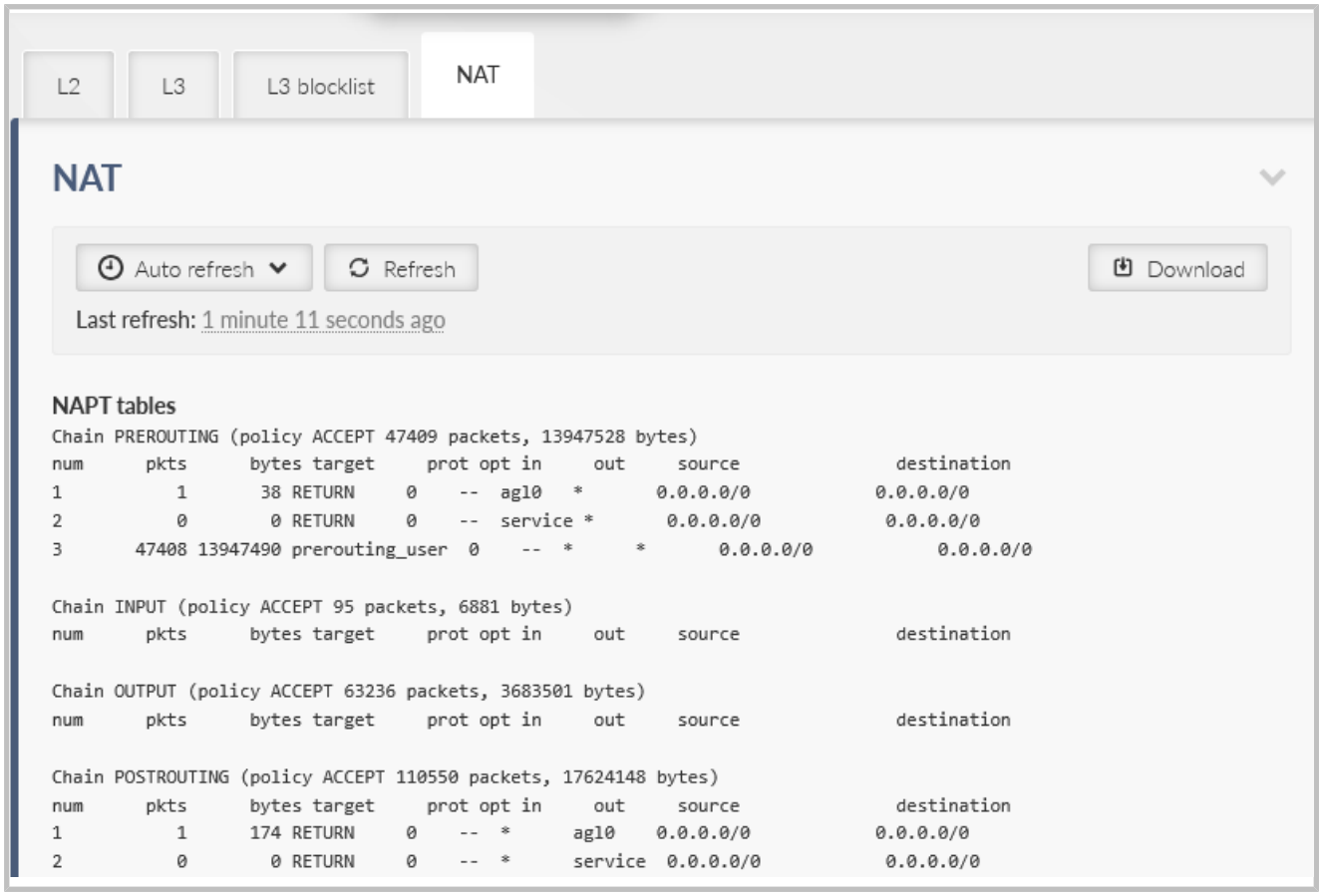


Fig. 5.10: DIAGNOSTICS > Information > Firewall > NAT

5.3.4. Quality of service

Creates a table about object and statistics extract for each given interface. This table contains:

- Name of an interface.
- Status and statistics of front disciplines - displays data called by linux command “tc qdisc show”.
- Status and statistics of classes - displays data called by linux command “tc class show”.
- Status and statistics of filter - displays data called by linux command “tc filter show”.

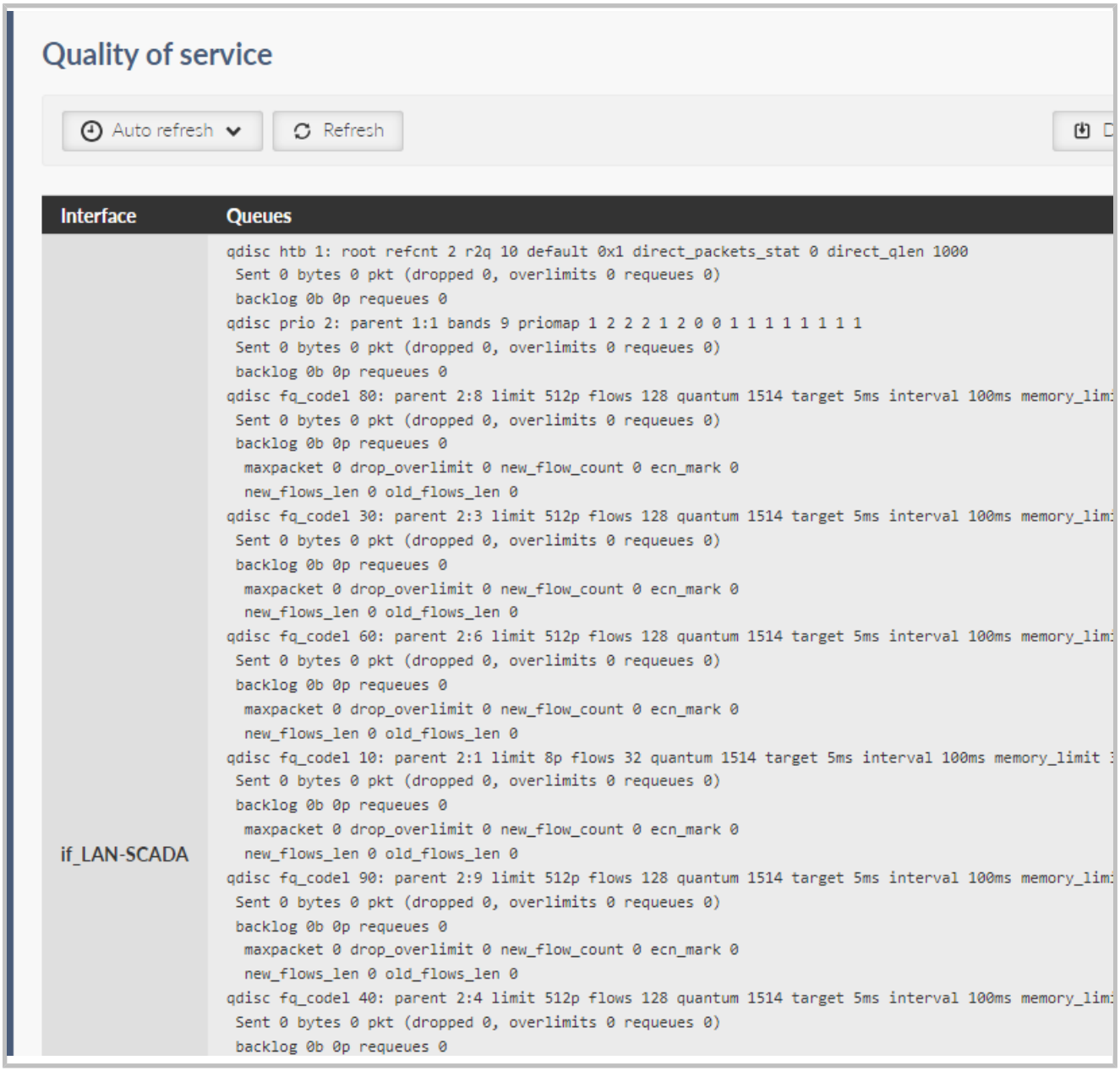


Fig. 5.11: DIAGNOSTICS > Information > Quality of service

5.3.5. DHCP servers

List of addresses assigned by the DHCP server.

IP address The assigned IP address of the client

MAC address MAC address of the client

Lease until The time when the lease expires

5.3.6. SNMP

Listing the Engine ID value. The Engine ID is used to uniquely identify the station when communicating with the SNMP manager.

Fig. 5.12: DIAGNOSTICS > Information > Services > SNMP

5.3.7. Syslog

Listing the message counters to a remote Syslog server.

Fig. 5.13: DIAGNOSTICS > Information > Services > Syslog

5.3.8. Device

Provides general information about the unit (device).

5.3.8.1. System information

Basic unit information is provided.

- Product code - Identifies the unit hardware.
- Serial number - Unique unit identification number.
- FW version - Currently installed unit firmware.

5.3.8.2. Advanced information

Additional unit information is provided which might be requested for advanced diagnostics. Partial description:

- Modem board SN - Modem boards system number.
- Radio board SN - Radio boards system number.
- Radio SW version - Current radio software.
- CNF version - Version of the unit configuration. Configuration version is updated if the new firmware version brings major configuration changes leading to incompatibility with the previous configuration. See *Section 4.6.2, "Configuration"* for more details.
- Web client version - Version of the current web client.
- Region ID - If the unit is delivered with certain limits applied according to a specific Region (specified when ordering a new unit), the specific Region identification is visible here. No limits are applied if the Region ID is empty ("---").
- Region description - Detailed description of the Region (if active).

5.3.9. Diagnostic package

This menu serves for collecting data, either from local or remote station and storing them into a package (file). Diagnostic package serves primarily as a help tool, for RACOM's technical support in case of any potential unit issues. Minimum size of a package is 5kB. Maximum size depends on the amount of radio links contained in the statistics. Diagnostic package is downloaded already compressed, which saves approx. 1/3 of its original size.

Only one package collecting (applies for both local and remote) at a time is supported.

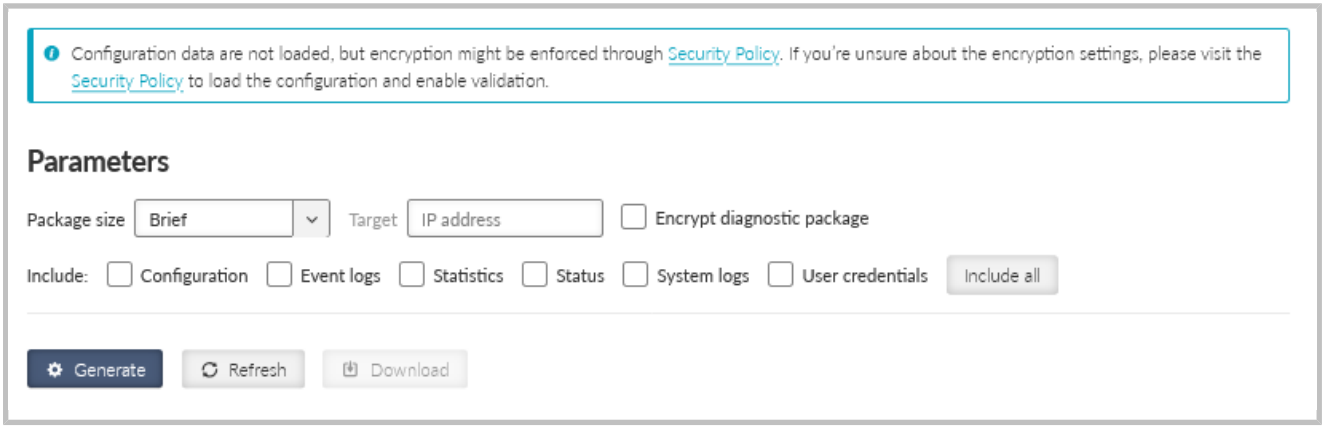


Fig. 5.14: DIAGNOSTICS > Information > Diagnostic package

Package size
List box {Brief; Detailed}, default = "Brief"
Defines the size of the generated package.

Target
Defines the station, from which is the Diagnostic package being collected.

- Diagnostic package from a local station - this parameter stays empty.
- Diagnostic package from a remote station - destination IPv4 address of the requested station must be used.

Encrypt diagnostic package

Allows generating of the diagnostic package as an encrypted .zip file. The rules for the password complexity are set in the SETTINGS > Security > Policy menu. In the same menu, it is possible to set encryption to always be required.

Note
You cannot use Windows Explorer for extracting the package. You need to use a software that can work with files encrypted with AES-256 algorithm (e.g. WinZip, WinRAR, 7-zip, Total commander).

Include

- Configuration - configuration of the unit is added to the package (json format)
- Event logs - adds a list of events exported to csv
  - Brief: Last 50 events
  - Detailed: Last 500 events
- Statistics - adds list of statistics exported to csv
  - Interval of frames statistics: 30 min
  - Brief: 10 frames
  - Detailed: 24 frames
- Status - lists detailed status of networks devices and services
- System logs - adds last system logs
  - Brief: 100 of current lines from all logs
  - Detailed: whole logs content
- User credentials - adds a list of user accounts

After setting all parameters, click on "Generate" button. By clicking the "Refresh" button update the processing status of the package. Once the package is ready, it can be downloaded by clicking the "Download" button. After its download, the package is deleted from the unit. The package will be deleted even if its download is unsuccessful and if the download is not initiated, the package will be deleted automatically after 24h.

5.4. Events

This menu shows all events which occur within the unit history.

For filtering of events you can use the filtering tool. When no filter rules are used, the last 30 events will be displayed after Display button click.

Older events should be displayed using Load more button click, the events which occur during the viewing of this window can be loaded by using Load newer button.

Alarms are displayed in red color, warnings in orange, notices in black and debugs in gray.

Part of the event record is also the information about action really triggered by the event. Changing the settings of a requested action or severity of the event (SETTINGS > Device > Events) does not change information about the events that have already occurred.

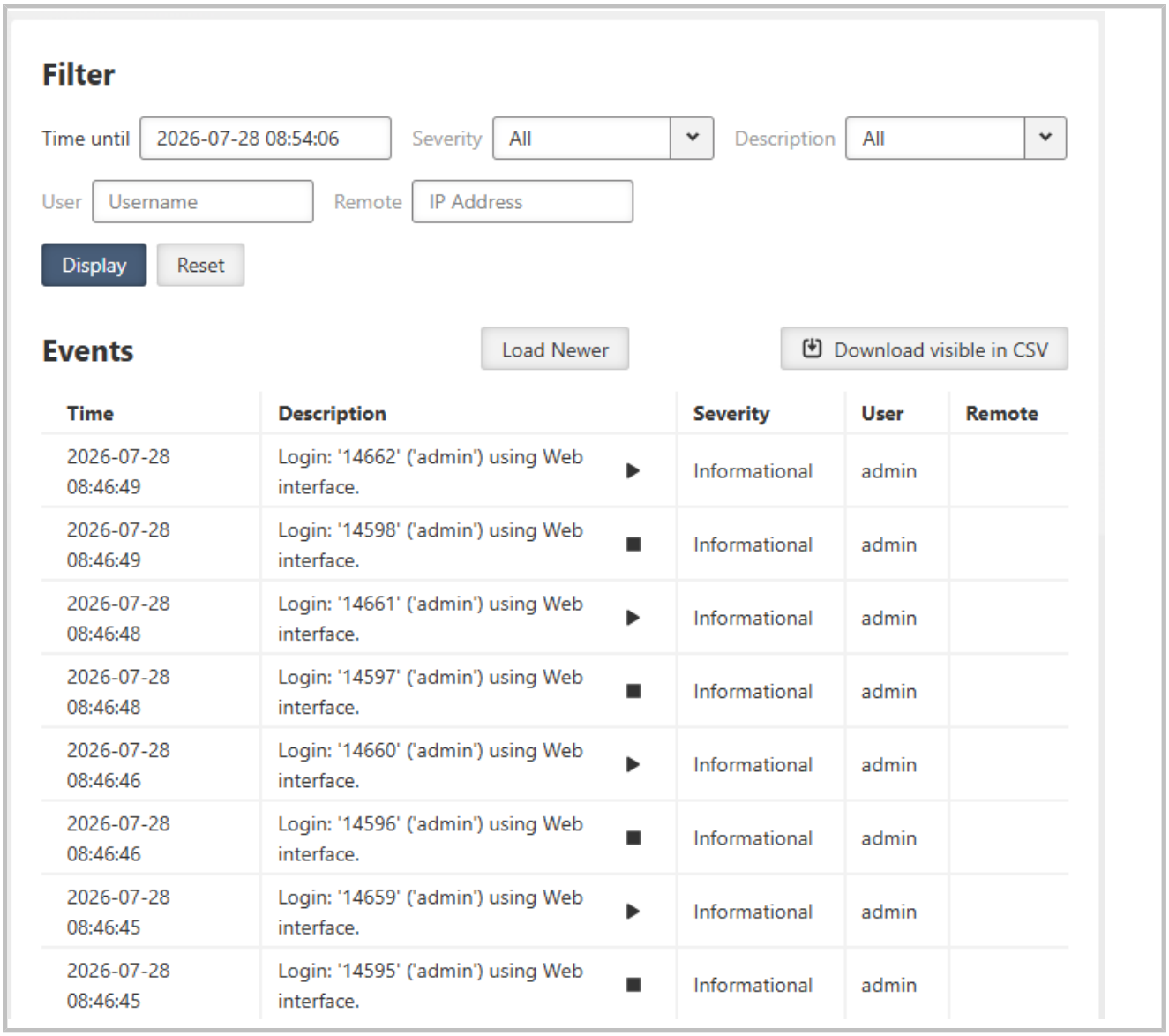


Fig. 5.15: DIAGNOSTICS > Events

It is possible to change severities of individual events in the menu SETTINGS > Device > Events.

Tab. 5.3: Default Events level description

Severity group	Level	Severity	Color code	Description	Action
ALARM	0	Emergency	Red	Faulty unit. HW repair is probably needed.	Replace the unit. Contact Technical support.
	1	Alert	Red	Unit does not work. HW or SW problem.	Check the unit. Consult Technical support.
	2	Critical	Red	Serious error. Communication does not work.	Check the unit immediately.

Severity group	Level	Severity	Color code	Description	Action
	3	Error	Red	Error. Communication can work.	Check the unit.
WARNING	4	Warning	Orange	Communication is OK. Self-healing action proceeded.	When often, consult with Technical support.
	5	Notice	Blue	Security important action proceeded or I/O action.	Security check, the I/O status check.
INFO	6	Informational	-	Informational item	Standard behavior
	7	Debug	-	Debug info, if set so.	Debug

5.5. Statistics

WaSP unit permanently monitors various system 'channels'. There are several types of those channels: Physical interfaces (Ethernet ports, serial ports, radio interface, additional module interface (e.g. LTE module) when installed), virtual interfaces (e.g. VLAN interfaces) and HW sensors (CPU temperature, supply voltage, ...). Monitored values are stored in the internal database.

Statistics page provides aggregated statistical data from this internal database. Data can be both displayed and downloaded in CSV format. This file format is suitable to be imported to any 3rd party spreadsheet program for further analysis.

There are two different options how to display statistics data:

Historical
Statistics counters are aggregated over the defined time interval. The interval is defined by two time stamps "From" and "To".

Differential
Statistics counters are aggregated between the counter reset and the current time (the moment when the Display button was pressed). Reset is triggered by a unit reboot or by the Reset statistics button.
Reset statistics button - initiates the Differential statistic counters reset. Such a reset does not affect normal statistic counters - i.e. the Historical statistics are not affected by such a Reset at all.

Length of statistics data

Statistics data are stored in the internal database. There is a fixed memory size allocated for the statistics data - the database is limited by number of records. As a result of this, the length of statistics history - how old records are available - depends on the actual network configuration: The more monitored values, the higher the rate of new recorded values, the shorter the available history.

Some sets of monitored values are constant (Ethernet ports and their counters) or do not rise to a high values (COM ports, Terminal servers and their counters). What affects the length of available history the most is the number of radio links - how many radio “neighbors” the unit communicates with or how many of the neighboring signals are received. This is different for each unit in the network.

5.5.1. Parameters

Statistics data are always retrieved as aggregated for a certain time Interval. This Interval can be set by putting specific date and time into "From" and "To" fields, or using buttons “Last day”, “Last hour”

or “More options” fast presets (from several minutes to several days). Button “Set Current Time” sets current time to both From and To fields to ease current unit status diagnostics.

There are following sets of statistical data available in the unit:

- Radio interface statistics
- Radio protocol statistics
- Radio protocol non-addressable statistics
- Radio signal statistics
- Radio signal non-addressable statistics
- Serial protocols statistics
- Ethernet statistics
- Cellular statistic
- Measurements

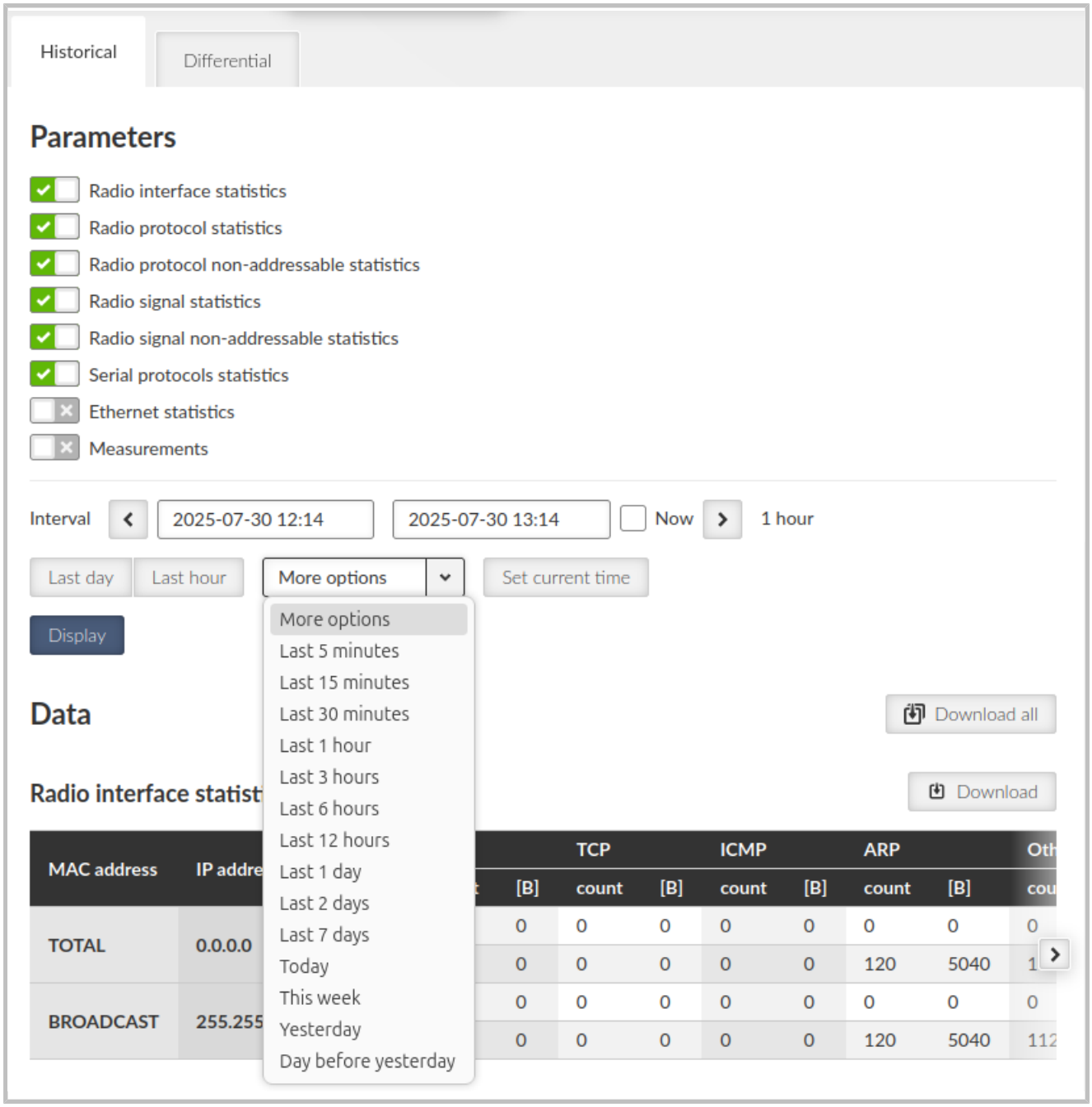


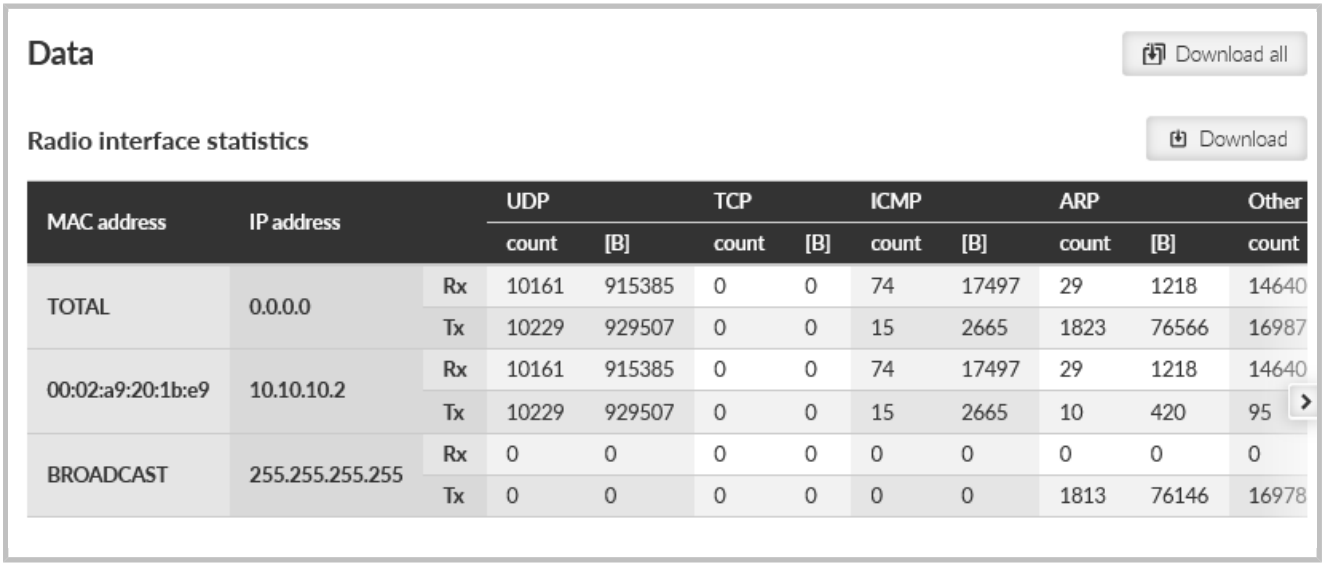
Fig. 5.16: DIAGNOSTICS > Statistics

“Display” button then shows chosen data below. “Download Selected Data” button generates CSV (UTF-8 encoded) file of all chosen systems’ data and downloads them as files without displaying them. Both "Display" and "Download ..." buttons send a request for the required set of statistics data to the unit. Retrieving and transferring of the data (over the radio channel) takes some time. Downloading the data is practical when the user needs to process them in a spreadsheet and wants to save some bandwidth. It is also recommended to use spreadsheet editor like Microsoft Excel or Apple Numbers to process statistics on mobile devices due to better user experience provided by the specialized apps.

5.5.2. Radio interface statistics

Radio interface statistics provides set of data monitoring the interface between the Router module (IP routing engine in the unit) and the Radio protocol module. It corresponds to monitoring Radio - Router.

Tx direction: from the Router module to the Radio protocol module. Rx direction: from the Radio protocol module to the Router module.



MAC address	IP address		UDP		TCP		ICMP		ARP		Other
			count	[B]	count	[B]	count	[B]	count	[B]	count
TOTAL	0.0.0.0	Rx	10161	915385	0	0	74	17497	29	1218	14640
		Tx	10229	929507	0	0	15	2665	1823	76566	16987
00:02:a9:20:1b:e9	10.10.10.2	Rx	10161	915385	0	0	74	17497	29	1218	14640
		Tx	10229	929507	0	0	15	2665	10	420	95
BROADCAST	255.255.255.255	Rx	0	0	0	0	0	0	0	0	0
		Tx	0	0	0	0	0	0	1813	76146	16978

MAC address - MAC address of the IP packet. Source for Rx or destination for Tx packets.

IP address – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.

UDP, TCP, ICMP, ARP - Packet count and amount of data in Bytes [B] for different protocol types. Amount of data is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

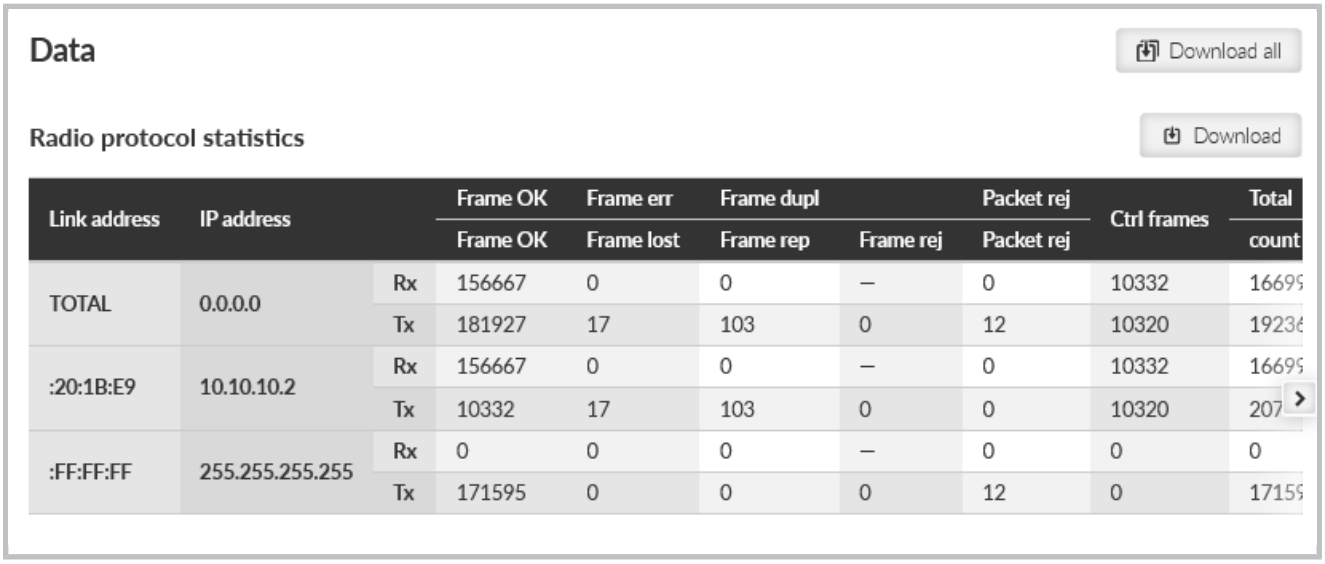
Other – Packets not handled by the previous counters (e.g. VLAN, services, GRE, IPsec (ESP), ...)

5.5.3. Radio protocol statistics

Radio protocol statistics provides set of data monitoring the radio channel access protocol frames and events. It corresponds to monitoring Radio - Interface.

Frames which are not addressed to/from this unit are not handled (they do not affect any counter).

Rx direction: from the 'air' radio interface to the Radio protocol module. Tx direction: from the Radio protocol module to the radio interface.



Link address	IP address		Frame OK	Frame err	Frame dupl		Packet rej	Ctrl frames	Total
			Frame OK	Frame lost	Frame rep	Frame rej	Packet rej		count
TOTAL	0.0.0.0	Rx	156667	0	0	–	0	10332	16699
		Tx	181927	17	103	0	12	10320	19236
:20:1B:E9	10.10.10.2	Rx	156667	0	0	–	0	10332	16699
		Tx	10332	17	103	0	0	10320	207
:FF:FF:FF	255.255.255.255	Rx	0	0	0	–	0	0	0
		Tx	171595	0	0	0	12	0	17159

Link address – Link address of the frame. Source for Rx or destination for Tx frames. This is a Link address assigned at the origin (input) - when entering, or at the target (output) - when leaving the radio network.

This address pair is not modified when re-translated. As a result of this fact, the whole traffic to a remote station behind the re-translation is counted together in a line assigned to the remote station.

For the Link address:

IP address – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.

Frame OK (Rx) – Correctly received data frames count.

Frame OK (Tx) – Correctly send data frames count. Control frames are not included. When ACK is on, only acknowledged frames are included. Re-translated data frames are not included.

Frame err (Rx) – Received corrupted data frames count (CRC error)

Frame lost (Tx) – Transmitted unacknowledged frames count. It happens when ACK is on and acknowledging frame was not received even when full number of re-transmission attempts was reached.

Frame dupl (Rx) – Received, but dropped, duplicated data frames count. 'Duplicated' frames are repeatedly received acknowledged frames.

Frame rep (Tx) – Repeated frames count (they can appear when ACK is on). Re-translated frames are not included.

Frame rej (Tx) – Rejected frames count (rejected just before transmission) – reason: buffer timeout. In case of Transparent protocol (Bridge mode) it happens when there is a collision during re-translation.

Packet rej (Rx) – Correctly received but rejected packets count - reason: impossible to decrypt or decompress.

Packet rej (Tx) – Rejected packets count (rejected before handed over to the transmitter) – reason: buffer overflow, buffer timeout.

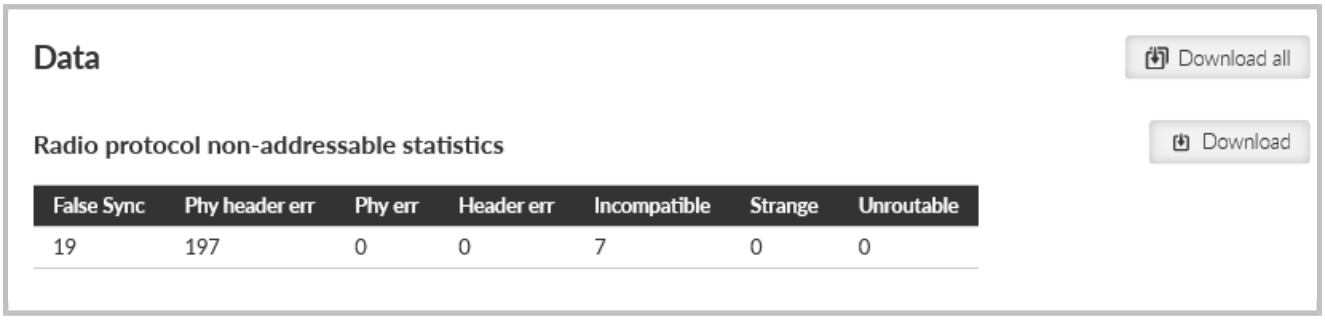
Ctrl frames (Rx, Tx) – Received / transmitted control frames count.

Total (Rx) – Received frames count and amount of data in Bytes. Amount of data - for both Rx and Tx - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

Total (Tx) – Transmitted frames count and amount of data in Bytes. Re-translated frames are included.

5.5.4. Radio protocol non-addressable statistics

Radio protocol 'non-addressable' statistics provides set of data monitoring the radio channel access protocol frames and events which cannot be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.



False Sync – False synchronization incidents count

Phy header err – Packet reception failure count - reason: sub header error

Phy err – Packet reception failure count - reason: physical layer analysis error

Header err - Packet reception failure count - reason: header content error or CRC error.

Incompatible – Received incompatible frames count - reason: different radio protocol

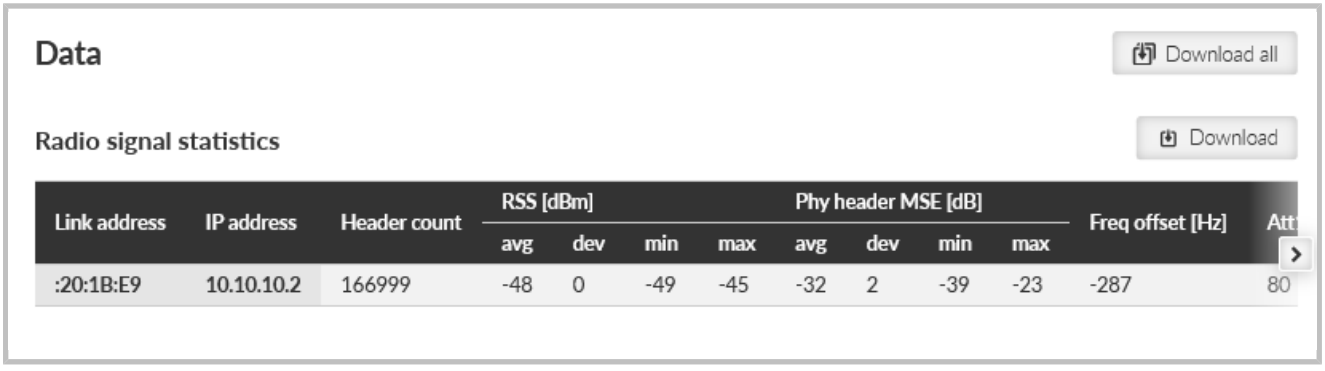
Strange – Received unexpected frames count - reason: wrong addresses, wrong sequence etc. Valid for Base Driven Protocol only.

Unroutable – Packets counter which were scheduled for transmission but impossible to be forwarded to the Radio protocol - multiple reasons: e.g. the destination IP address is not known

5.5.5. Radio signal statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. It corresponds to monitoring Radio - Interface.

Statistic data are collected by the frame source address - Link address, which is an address of the originating radio transmitter (unlike "Radio protocol statistics" where the Link address is an address of the unit where the packet entered the WaSP network).



Header count – Received headers count

RSS [dBm] – Radio Signal Strength - measured within the header reception

avg / dev / min / max – average / standard deviation / minimum / maximum

Phy header MSE [dB] – modulation Mean Squared Error - measured within the header reception

Freq offset [Hz] – Averaged frequency offset between the transmitter and the receiver station, measured by the receiver station.

Att1 [%] - First internal attenuator (15 dB) activated. Shown in percents of affected frames.

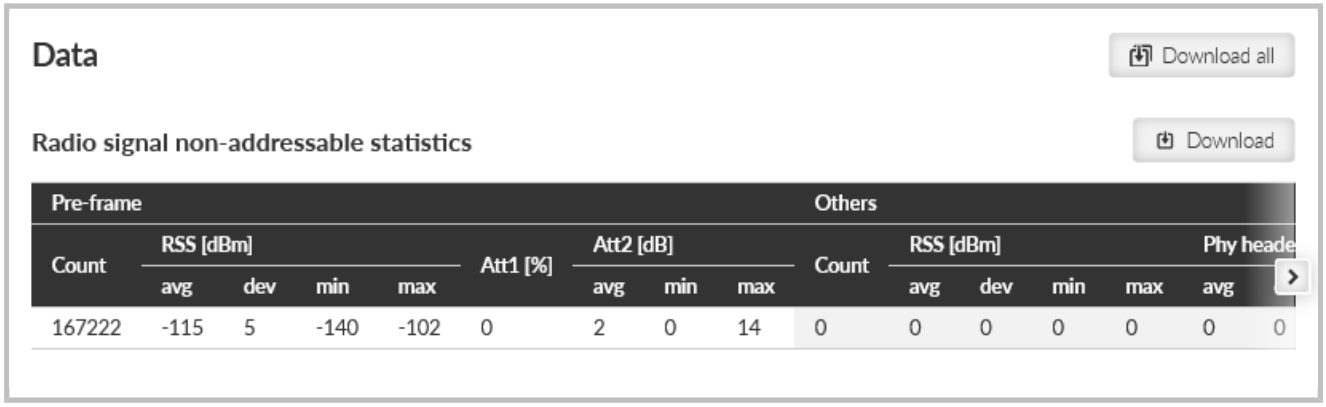
Att2 [dB] – Value of the 2nd internal attenuation applied (0 - 31 dB).

Data count – Received complete frames (including data part) count. Frames with valid header CRC, but wrong data CRC are not counted

Data MSE [dB] - modulation Mean Squared Error - measured within the frame data part reception

5.5.6. Radio signal non-addressable statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. This table contains measurements handled before the frame reception and measurements which cannot be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.



Pre-frame									Others						
Count	RSS [dBm]				Att1 [%]	Att2 [dB]			Count	RSS [dBm]				Phy heade	
	avg	dev	min	max		avg	min	max		avg	dev	min	max	avg	
167222	-115	5	-140	-102	0	2	0	14	0	0	0	0	0	0	0

Pre-frame – Values based on measurements handled before the frame reception

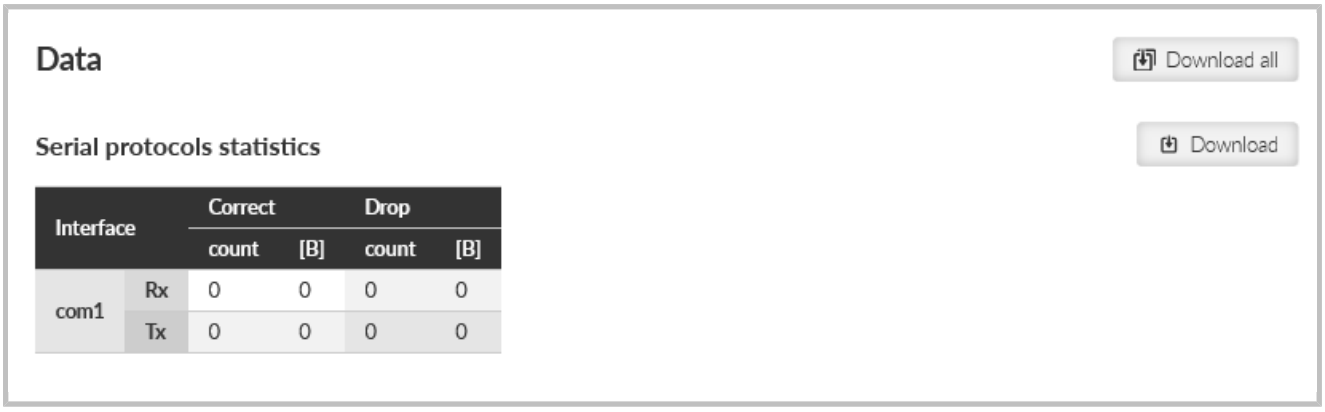
RSS [dBm] – Radio Signal Strength - measured short time just before the frame reception

Others – Values for frames which cannot be linked with any address

5.5.7. Serial protocol statistics

Serial protocols statistics provides set of data monitoring the COM port(s) and Terminal server (s). Only enabled interfaces are displayed. The statistics counters are based on packets entering or leaving the COM port or Terminal server module. As a result of this the 'count' values correspond to the Protocol messages (the "Protocol" selected on the specific COM port or Terminal server). If the packet is 'glued' from the several frames, it is evaluated as a single packet. In case of COM port statistics, the summary of 'Correct' and 'Drop' Bytes provides the total amount of Bytes on the physical interface.

Rx direction: from the connected (at the COM or ETH port) external device to the WaSP unit (i.e. from the COM port module or Terminal server module to the Router module). Tx direction: from the WaSP unit to the external device.



Interface		Correct		Drop	
		count	[B]	count	[B]
com1	Rx	0	0	0	0
	Tx	0	0	0	0

Interface – Interface name

Correct (Rx, Tx) – Correctly received / transmitted packets count and amount of data in Bytes. Accepted by the COM port or Terminal server module - based on the selected Protocol processing. Amount of data - for both Correct and Drop counters - is affected by COM port data only (i.e. IP headers of the UDP frames created in the COM port module are NOT counted).

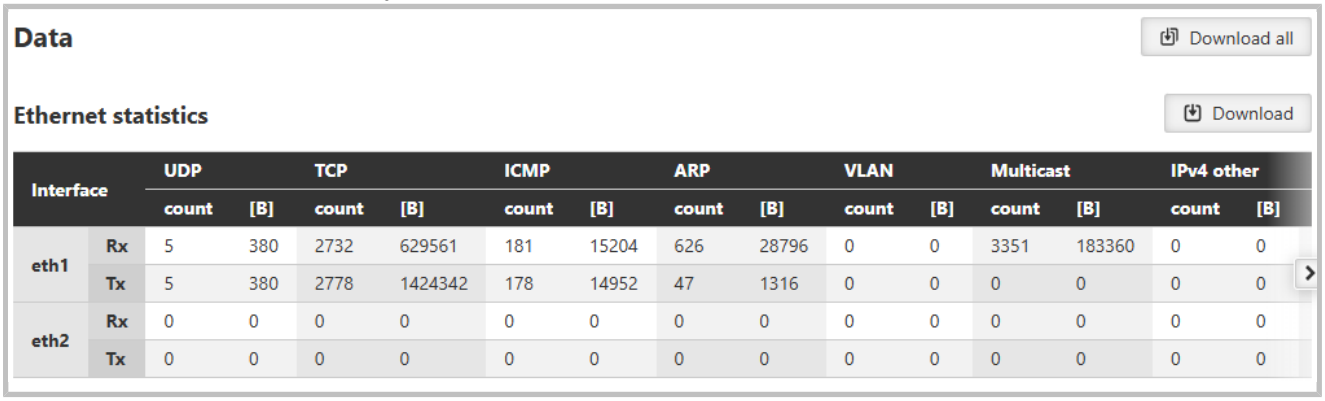
Drop (Rx, Tx) - Dropped received / transmitted packets - reason: corrupted frame, CRC error, wrong protocol message, unsupported protocol message.

5.5.8. Ethernet statistics

Ethernet statistics provides set of data monitoring the physical Ethernet ports. Only enabled interfaces are displayed.

Only correctly received frames are handled. The counters correspond to the specific IP protocol types.

Rx direction: from the physical Ethernet port to the WaSP unit (i.e. to the Router module). Tx direction: from the WaSP unit to the physical Ethernet port.



Interface		UDP		TCP		ICMP		ARP		VLAN		Multicast		IPv4 other	
		count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]
eth1	Rx	5	380	2732	629561	181	15204	626	28796	0	0	3351	183360	0	0
	Tx	5	380	2778	1424342	178	14952	47	1316	0	0	0	0	0	0
eth2	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Interface – Interface name.

UDP, TCP, ICMP, ARP, VLAN, Multicast - Packet count and amount of data in Bytes [B] for different protocol types - IPv4 traffic. Amount of data - for all counters - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

IPv4 other - IPv4 traffic not handled by the previous counters

IPv6 - IPv6 traffic counter

Other - Counter summing up the frames which were not handled by the previous counters - for example MPLS and GOOSE protocols.

5.5.9. Measurements

Sensor	count	avg	min	max
CPU [°C]	59708	51.9	51.2	53.5
Modem board [°C]	59708	42.3	41.9	42.8
Radio board [°C]	252778	41.1	40.7	41.7
Input [V]	59708	13.3	12.6	13.5

Sensor
Measured values on WaSP.

count
Number of times that the sensor measured given value (counter).

avg / min / max
Average / minimum / maximum value.

5.6. Monitoring

Monitoring is an advanced on-line diagnostic tool, which enables a detailed analysis of communication over any of the WaSP router interfaces. In addition to all the physical interfaces (RADIO, EXT, ETHs, COMs, TSs), some internal interfaces between software modules can be monitored when such advanced diagnostics is needed.

Monitoring consists of two independent processes: settings of the monitored items and outputs. Please note that even if both of the outputs are switched off and some interfaces are set to On, the monitoring is still running in the background.

The monitoring screen has two main parts - Settings and Output

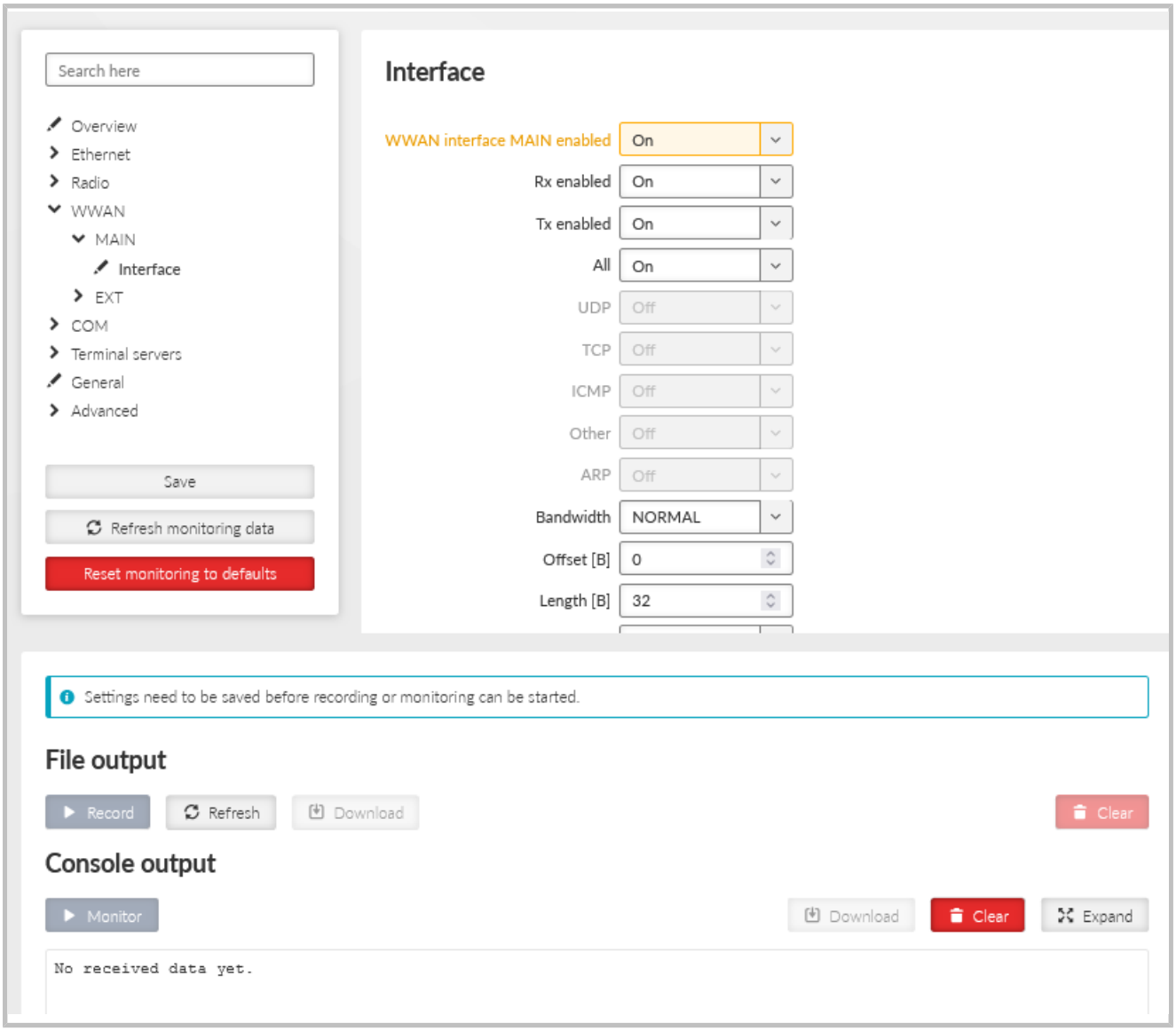


Fig. 5.17: DIAGNOSTICS > Monitoring

5.6.1. Settings

Save button - saves the new settings of the monitoring parameters.

Refresh monitoring data button - refreshes the settings menu according to the statistics status saved in the unit. The difference between the displayed and saved status can occur for example when the status is changed in different browser tab.

5.6.1.1. Overview

All status (On/Off) of individual interfaces are displayed on this place for quick overview on monitoring settings.

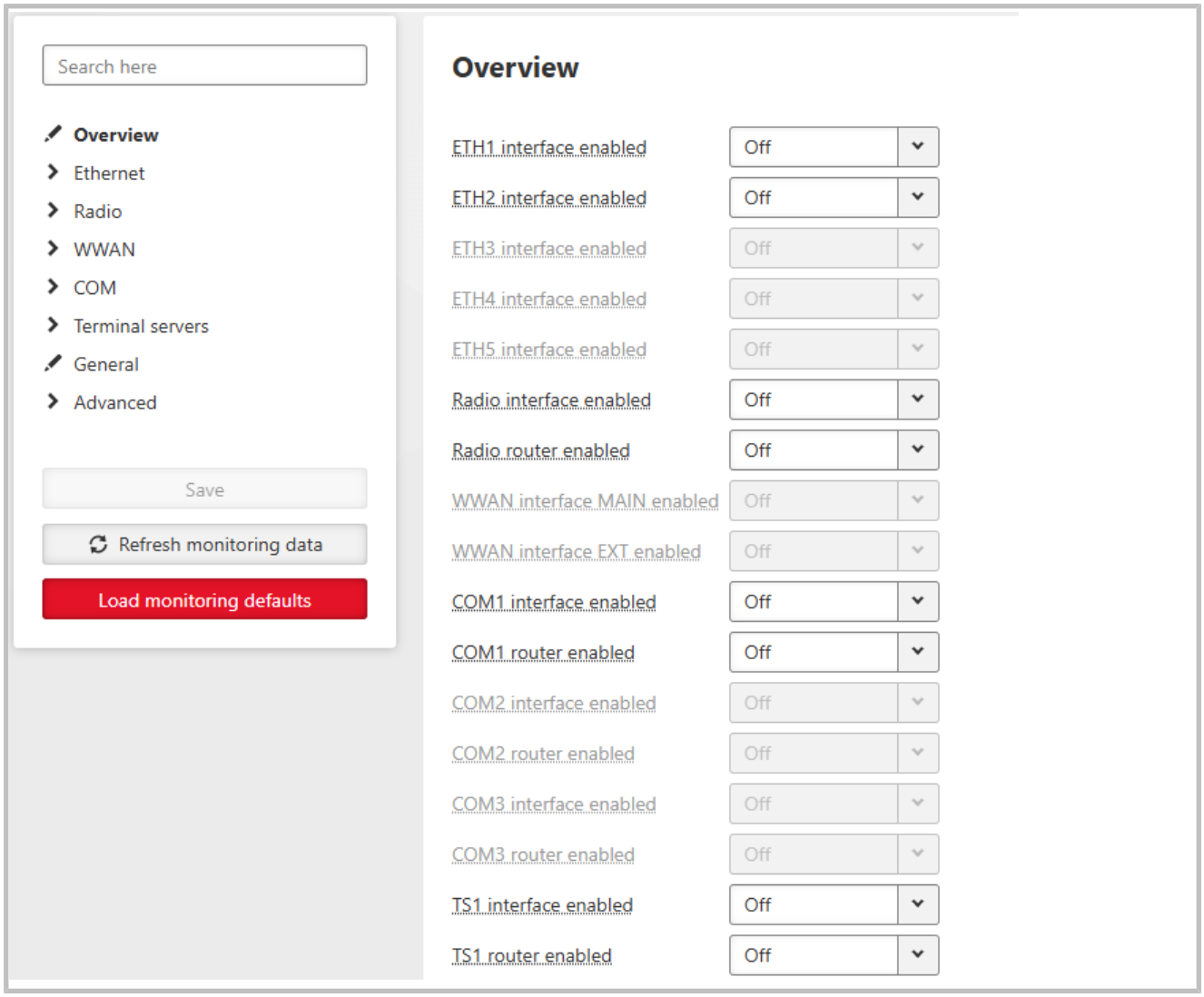


Fig. 5.18: DIAGNOSTICS > Monitoring > Overview

5.6.1.2. Interfaces

This section allows detailed settings of particular monitoring parameters for all interfaces.

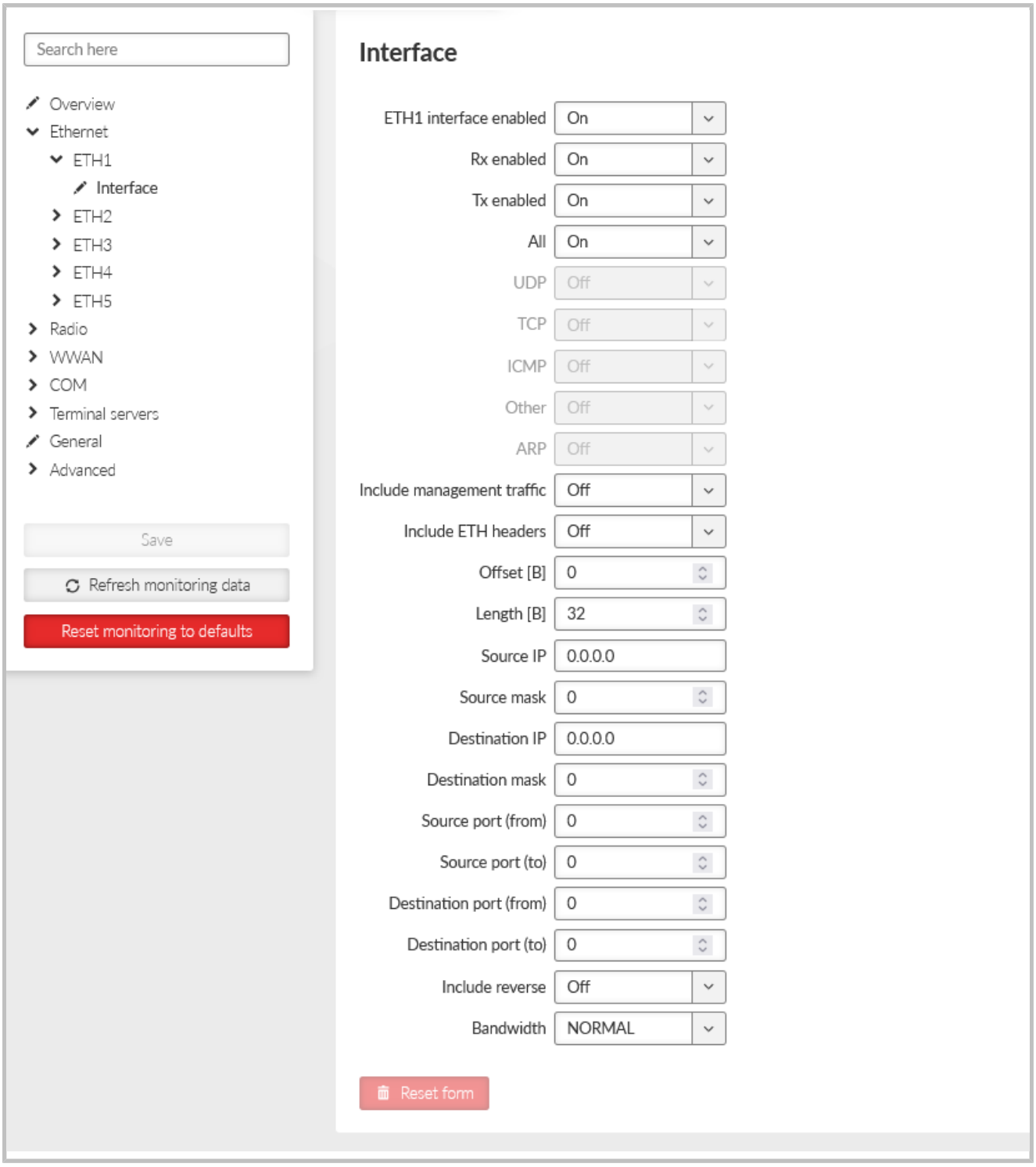


Fig. 5.19: DIAGNOSTICS > Monitoring > Ethernet > ETH1 > Interface

Common parameters for several interfaces:

Rx enabled, Tx enabled

List box {On; Off}, default = "On"

A packet is considered a Tx one when it comes out from the respective software module (e.g. RADIO or Terminal Server) and vice versa. When an external interface (e.g. Interface COM) is monitored, the Tx also means packets being transmitted from the WaSP over the respective interface (Rx

means "received"). Understanding the directions over the internal interfaces may not be that straightforward, please see *???* above for clarification.

All

List box {On; Off}, default = "On"

Monitoring output can also be limited by IP protocol type. Select Off to be able to enable/disable specific protocol output individually - see next parameter(s).

UDP / TCP / ICMP / Other / ARP

List box {On; Off}, default = "Off"

Monitoring output of specific IP protocol limitation.

Offset [B]

Default = 0

Number of bytes from the beginning of packet/frame, which will not be displayed - the monitoring output is truncated by 'Offset' bytes at the beginning of the message.

Length [B]

Default = 32

Number of bytes to be displayed from each packet/frame.

Example: Offset=2, Length=4 means, that bytes from the 3rd byte to the 6th (inclusive) will be displayed:

Data (HEX): 01AB **3798 A285** 93CD 6B96

Monitoring output: 3798 A285

Bandwidth

List box {LOW; NORMAL; HIGH; UNLIMITED}, default = "NORMAL"

Monitoring bandwidth limit to prevent overload of management link between client PC and the WaSP unit. LOW (up to ~300 kb/s), NORMAL (up to ~800 kb/s), HIGH (up to ~2 Mb/s), UNLIMITED (up to ~8 Mb/s)

Source port (from) / Source port (to)

TCP/UDP source port to be enabled/disabled in the monitoring output. Use these parameters to specify the source range of ports <from - to>.

Destination port (from) / Destination port (to)

TCP/UDP destination port to be enabled/disabled in the monitoring output. Use these parameters to specify the destination range of ports <from - to>.

Dropped frames

List box {On; Off}, default = "Off"

When On, monitoring shows frames which are dropped (e.g. CRC is not valid, buffer overflow, ...).

5.6.1.2.1. ETH interfaces

Include management traffic

List box {On; Off}, default = "Off"

Enable/disable management packets monitoring output.

Include ETH headers

List box {On; Off}, default = "Off"

Displays (enable) / omits (disable) L2 headers in the monitoring output.

Include reverse
List box {On; Off}, default = "Off"
Enable/disable reverse traffic (e.g. TCP reply to a request) monitoring.

Source IP / mask, Destination IP / mask
Monitoring output can also be limited to a specific address range - Source and Destination IP address and mask can be used to define the required range.

5.6.1.2.2. Radio interface

Corrupted frames
List box {On; Off}, default = "On"
Corrupted ("header CRC error", "data CRC error", etc.) received frames monitoring output can be suppressed. This can be useful when the communication in the channel is heavily disturbed by interference or noise, resulting in „garbage" messages which can make the monitoring output difficult to read.

Other modes
List box {On; Off}, default = "Off"
When Promiscuous mode is enabled, the unit is capable to monitor (receive) frames from the other WaSP units even if the other unit(s) is(are) working in the other Unit mode (Bridge versus Router). Frames transmitted under another Unit mode may not be properly 'analyzed'. In such a case frames are displayed in raw data format.

Include headers (Router)
List box {None; Packet (IP); Frame (ETH)}, default = "None"

- None – Only the payload (L4) is displayed, e.g. the data part of a UDP datagram.
- Packet (IP) – Headers up to a Network layer (L3) are included, i.e. the full IP packet is displayed.
- Frame (ETH) – The full Ethernet frame (L2) is displayed, i.e. including the ETH header.

Include headers (Interface)
List box {None; Radio link; Data coding; Both}, default = "None"

- None - no headers will be displayed
- Radio link – radio link headers will be included into the monitoring output
- Data coding – data coding header will be included, where C: type of compression, E: type of encryption
- Both – both Radio link and data coding headers will be included

Promiscuous mode
List box {On; Off}, default = "Off"

- Off – only frames which are normally received by this unit, i.e. frames whose Radio IP destination equals to Radio IP address of this WaSP unit and broadcast frames are available for the monitoring. Monitoring filters are applied afterwards.
- On – all frames detected on the Radio channel are available for the monitoring. Monitoring filters are applied afterwards.

Link Control Frames

List box {On; Off}, default = "Off"

- Off – Radio Link Control Frames (e.g. ACK frames) are never displayed.
- On – Radio Link Control Frames are processed by monitoring. Monitoring filters are applied.

Source IP / mask, Destination IP / mask (router)

Monitoring output can also be limited to a specific address range - Internal (router) Source and Destination IP address and mask can be used to define the required range.

Source IP / mask, Destination IP / mask (radio)

Monitoring output can also be limited to a specific address range - Radio interface Source and Destination IP address and mask can be used to define the required range.

Include reverse / Include Radio reverse

Includes reverse traffic for source / destination settings.

Menu DIAGNOSTICS > Monitoring > Advanced groups together all setting across all monitoring web pages, mentioned above, in one web page.

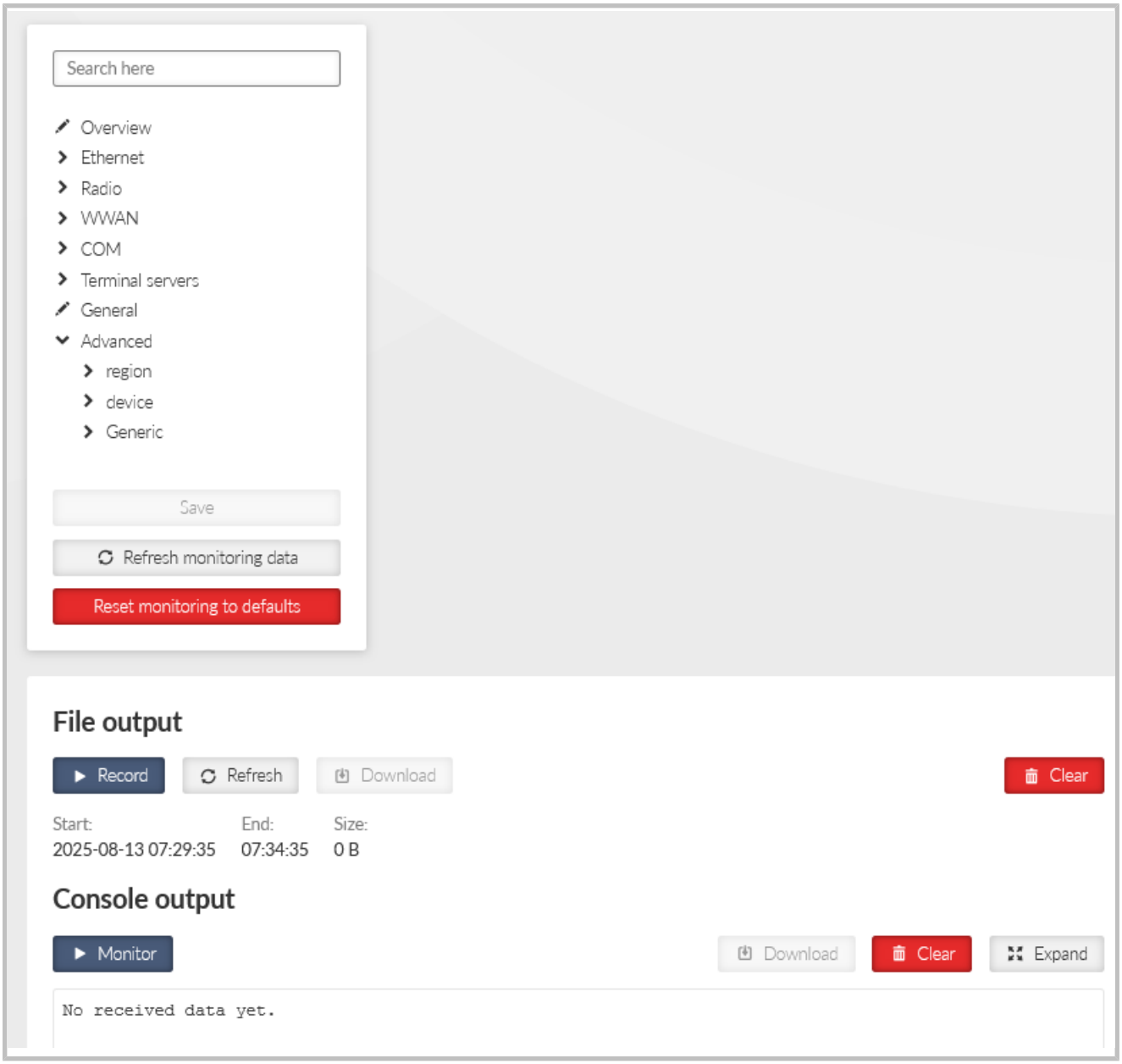


Fig. 5.20: DIAGNOSTICS > Monitoring > Advanced

Extended measurement

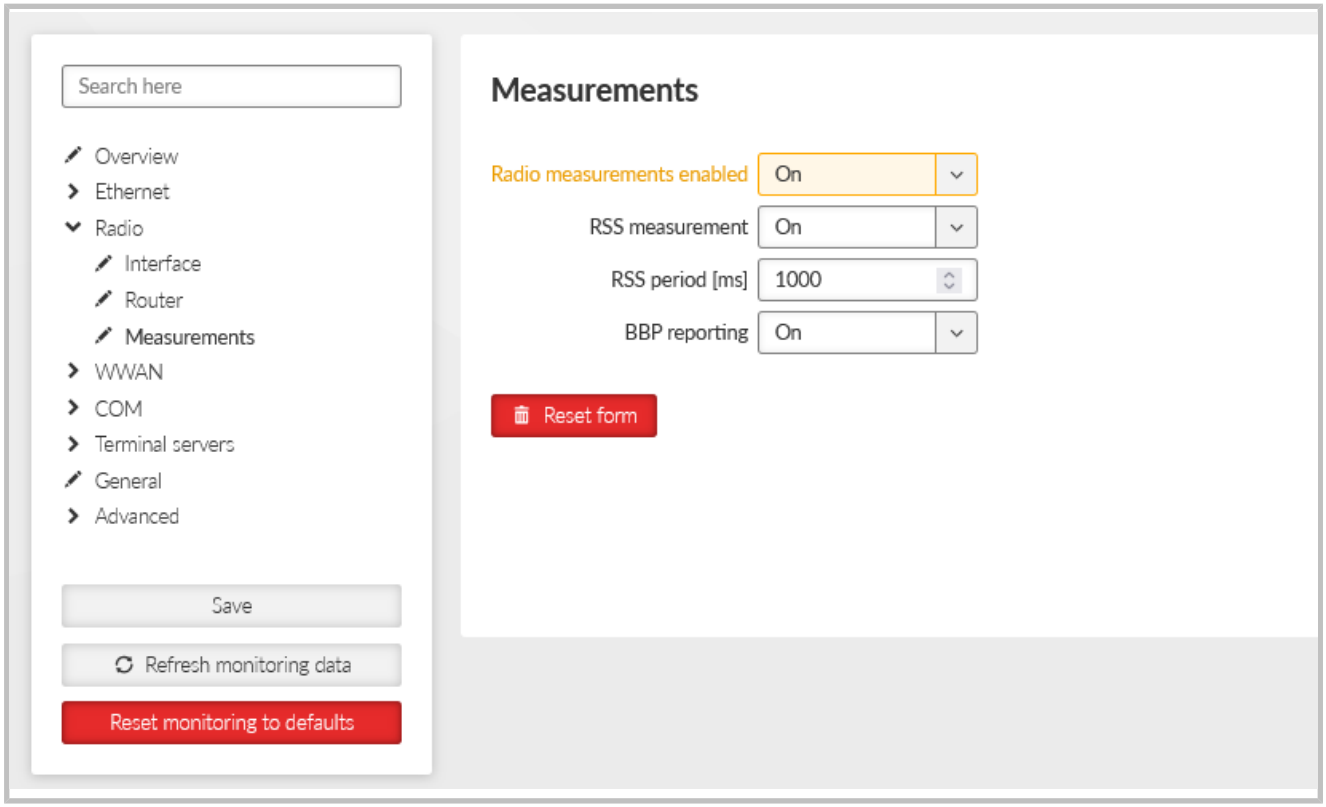


Fig. 5.21: Diagnostics > Monitoring > Radio > Measurements

Monitoring now includes additional parameters such as modulation type, FEC code, RF power, and temperature for TX, as well as modulation type, FEC code, frequency offset, and pre-packet RSS for RX.

Monitors regular measurements of radio channel and HW variables.

Individual measurements can be switched on and off, or the measurement period can be modified.

The signal strength is measured at the receiver at the set interval, regardless of any ongoing activity—even during transmission.

The BBP reporting function is included, providing the measured integrated power level across the entire bandwidth.

5.6.1.3. General

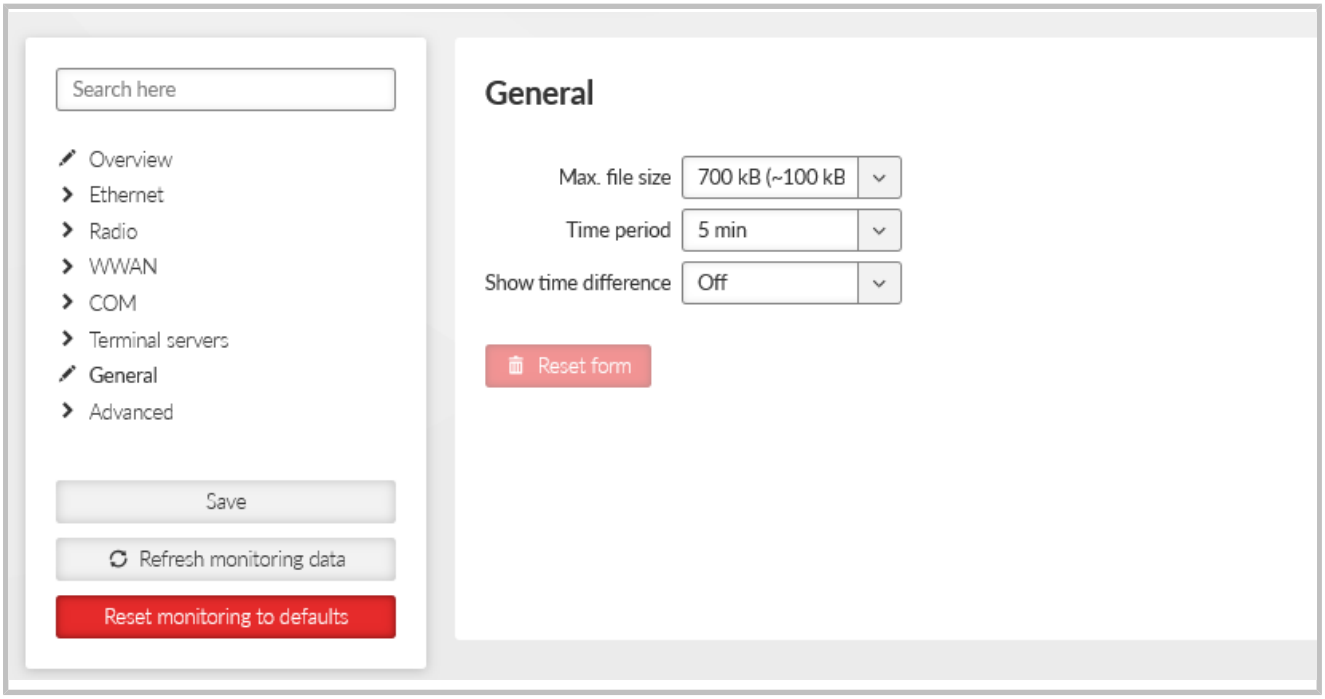


Fig. 5.22: DIAGNOSTICS > Monitoring

The settings of output parameters for file output – **Max. file size** and **Time period**, the first parameter matched closes the monitoring file. File is saved in compressed way, so the uncompressed and approximate compressed size is displayed in the list box.

Max. file size
List box {7 kB (~1 kB); 70 kB (~10 kB); 358 kB (~50 kB); 700 kB (~100 kB); 3 MB (~500 kB); 7 MB (~1 MB); max (~2 MB)}, default = "700 kB (~100 kB)"

Time period
List box {1 min; 2 min; 5 min; 10 min; 20 min; 30 min; 1 hour; 3 hours; 24 hours; Off}, default = "5 min"

Show time difference
List box {On; Off}, default = "Off"
When On, the time difference between subsequent packets is displayed in the monitoring output.

5.6.2. File output

Record button – starts recording to the file. Triggers a process, which is set by parameters in the chapter above (*Section 5.6.1.3, "General"*).

Stop recording button – stops recording to the file. The recording will be stopped immediately regardless of the size and time of recording. When the Record button is pressed for the second time the previously recorded data will be cleared.

Refresh button – refreshes the information about time remaining and size of the recorded data (in uncompressed way).

Download button – downloads file to a connected computer. The default name contains of the Unit name, date and time of the begin and day and time of the end of the monitoring. Before downloading you have to stop recording.

Clear button – allows to clear the monitoring data stored in the unit – both downloaded or not downloaded.

5.6.3. Console output

Monitor / Stop monitoring button

Download button – downloads the content of the console output as a file

Clear button - clears Console output screen

Note

If the amount of monitored data exceeds the limit (2.7 kB for remote monitoring and 32 kB for local monitoring) for one time period (approx. 1 s), some data will not be displayed in the console output. A note about the omited data will be inserted to the console output to the position of the non-displayed data.

5.7. Tools

Set of diagnostic tools

5.7.1. ICMP ping

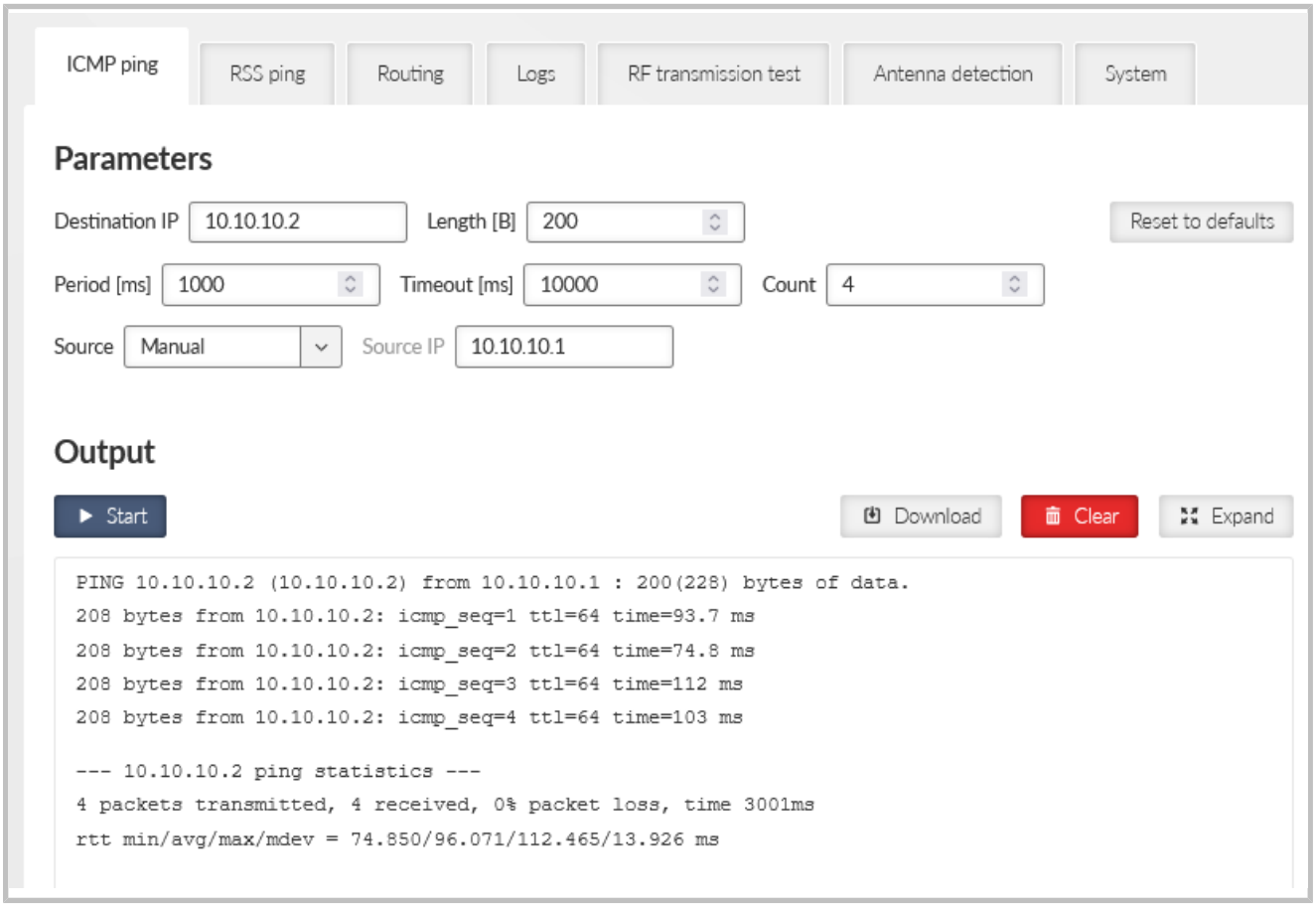


Fig. 5.23: DIAGNOSTICS > Tools > ICMP ping

All parameters used by standard ICMP ping are available. Start / Stop button starts / stops pinging.

5.7.2. RSS ping

(WaSP / WaSP combination)

RSS ping is a diagnostic tool for the radio performance measurement (Radio Signal Strength and modulation Mean Squared Error) of the individual radio hops within a WaSP network. Hybrid networks are supported. Output format of different type (other than radio) of hops is similar to ICMP ping.

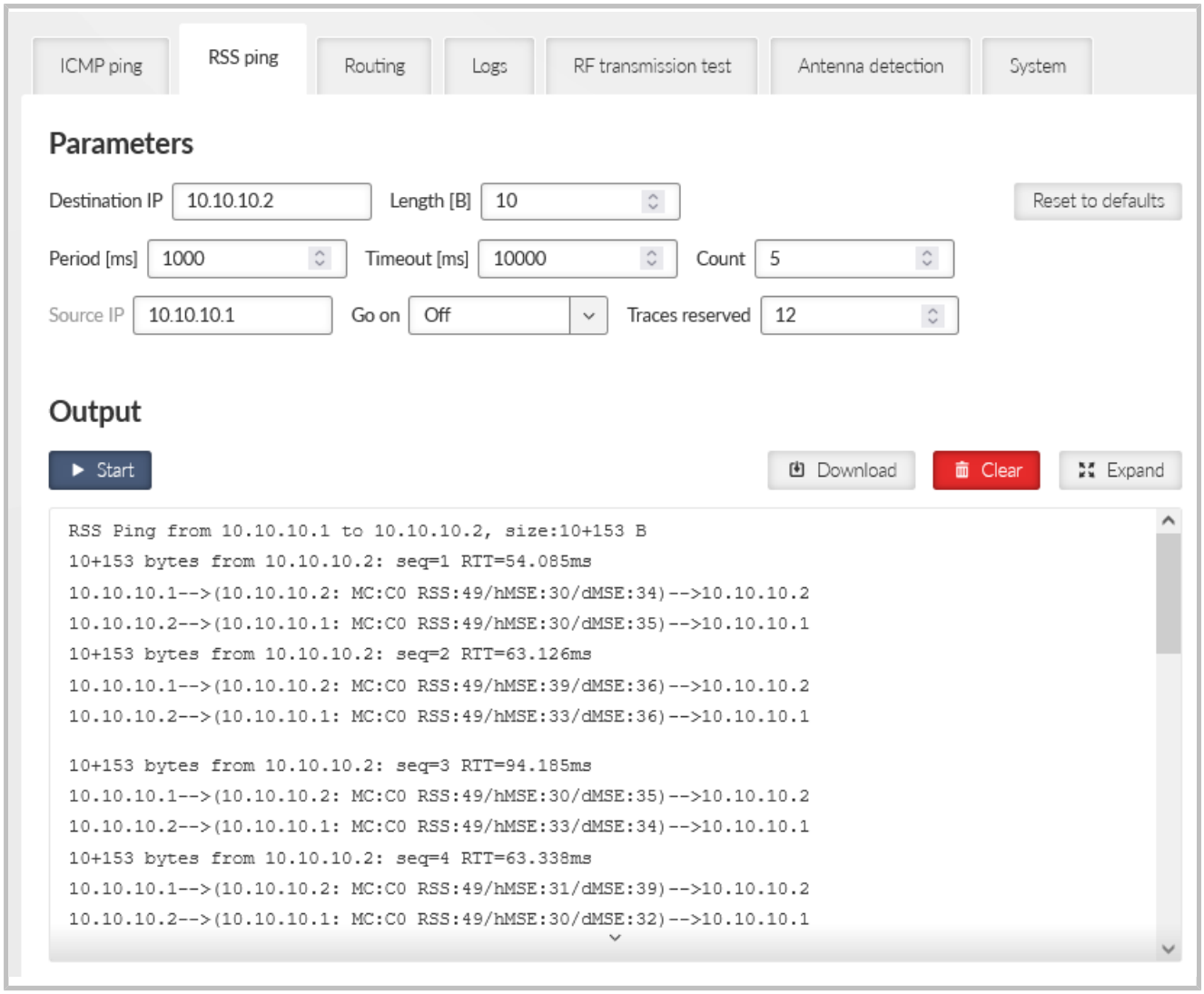


Fig. 5.24: DIAGNOSTICS > Tools > RSS ping

Destination IP

Destination IP address. This address must belong to a WaSP unit as the RSS ping can be initiated only between two WaSP units.

Length [B]

Number {8 – 1500}, default = 10

The length of data used by RSS ping. In case the length of RSS ping packet is longer than the length of **Radio interface MTU**, the first RSS ping packet will be lost and will cause decreasing of the packet length to the value matching to the current radio MTU. Random data are used as a payload.

Period [ms]

Number {100 – 3 600 000}, default = 1000

Period of sending RSS ping packets

When the period is set to a shorter number than the actual RTT, collisions might appear (depends on the selected Radio protocol). In order to reach the shortest possible period enable the **Go on** mode.

Timeout [ms]
Number {100 – 3 600 000}, default = 10000
Response timeout

Count
Number {1 – 10000}, default = 5
Number of RSS pings to be send

Source IP
The local IP address of WaSP unit originating RSS ping. Blank field (equal to 0.0.0.0 address) is used to assign the source address automatically - address is assigned automatically according to the routing rules.

Go on
List box {On; Off}, default = “Off”
Go on mode. When Enabled, RSS pings are sent immediately after receiving the RSS ping reply (Period parameter is ignored).

Traces reserved
The RSS ping also contains data about the route (RSS, MSE), this parameter allows to set number of radio hops within the network to be measured. Radio hop is measured in both directions, so the number has to be higher than number of hops in route multiplied by 2 (for example: link consisting of 2 radio hops needs 5 traces to be reserved).

Output:

- **MC** – Encodes Modulation and Coding – see transcription table:

Tab. 5.4: Translation table for Modulation rates and FEC

	Modulation	**FEC**
00	2CPFSK	FEC off
01		FEC 3/4
10	4CPFSK	FEC off
11		FEC 3/4

- **RSS** – Radio Signal Strength [dBm] - measured within the header reception
- **hMSE** – Phy header modulation Mean Squared Error [dB] - measured within the header reception
- **dMSE** – Data modulation Mean Squared Error [dB] - measured within the frame data part reception

5.7.3. Routing

Routing tool provides the next hop routing information of the given IP address.

Fig. 5.25: DIAGNOSTICS > Tools > Routing

Destination IP
The examined IP address.

Output
Output section provides the following details:

- Examined address (example: 8.8.8.8)
- Next hop (gateway) address (example: via 192.168.141.254)
- Next hop interface (example: dev if_bridge)
- Outgoing packet Source address (example: src 192.18.141.210)

5.7.4. Logs

This tool provides a real-time display of process logs for active device operations. These logs are designed for live station diagnostics and do not offer historical data retrieval. For retrospective analysis, please utilize an alternative method, such as the *Diagnostic package*.

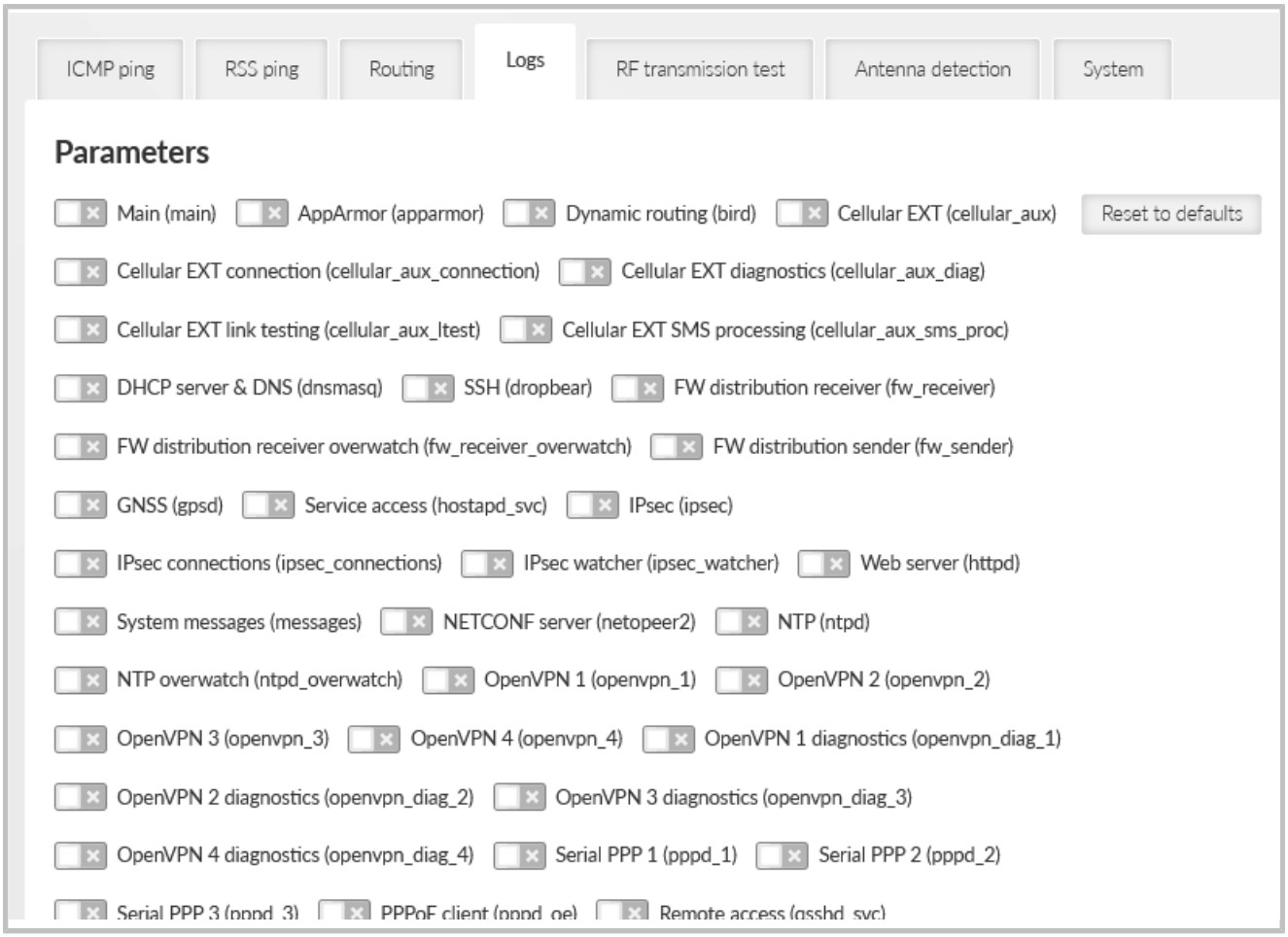


Fig. 5.26: DIAGNOSTICS > Tools > Logs

The core functionalities of this tool include:

- Real-time record display.
- Support for multiple independent instances (up to 10).
- Consolidated display of records from any number of processes within a single instance.
- Record filtering based on specified severity levels.
- Record length limitation to 1024 characters, with truncation of longer entries.

5.7.5. RF Transmission test

RF transmission test
Pre-defined type of RF signal can be transmitted for a specific purpose.

- **Type**
  List box {Random data; Carrier wave; Single tone}, default = "Random data"
  Type of transmitted signal during the test. In case of Single tone a frequency with an offset from the central frequency is transmitted.

- **Period [s]**
  Number {1 – 120 s}

Transmission test pre-set duration.

- **Start** button
  Starts the transmission test. If "Start" is requested during running test, it will not be launched again, but an error value will return. Currently running test will finish its time period.

- **Stop** button
  Allows to stop the test before the pre-set time. If "Stop" is requested and there is no running test, and error value will return.

Note

Testing is only allowed without standard radio protocol. Please set "Radio protocol" to "None" in Radio Settings before using this feature.

5.7.6. System

Reboot button
Performs unit cold restart (power cycle equivalent).

5.8. Syslog

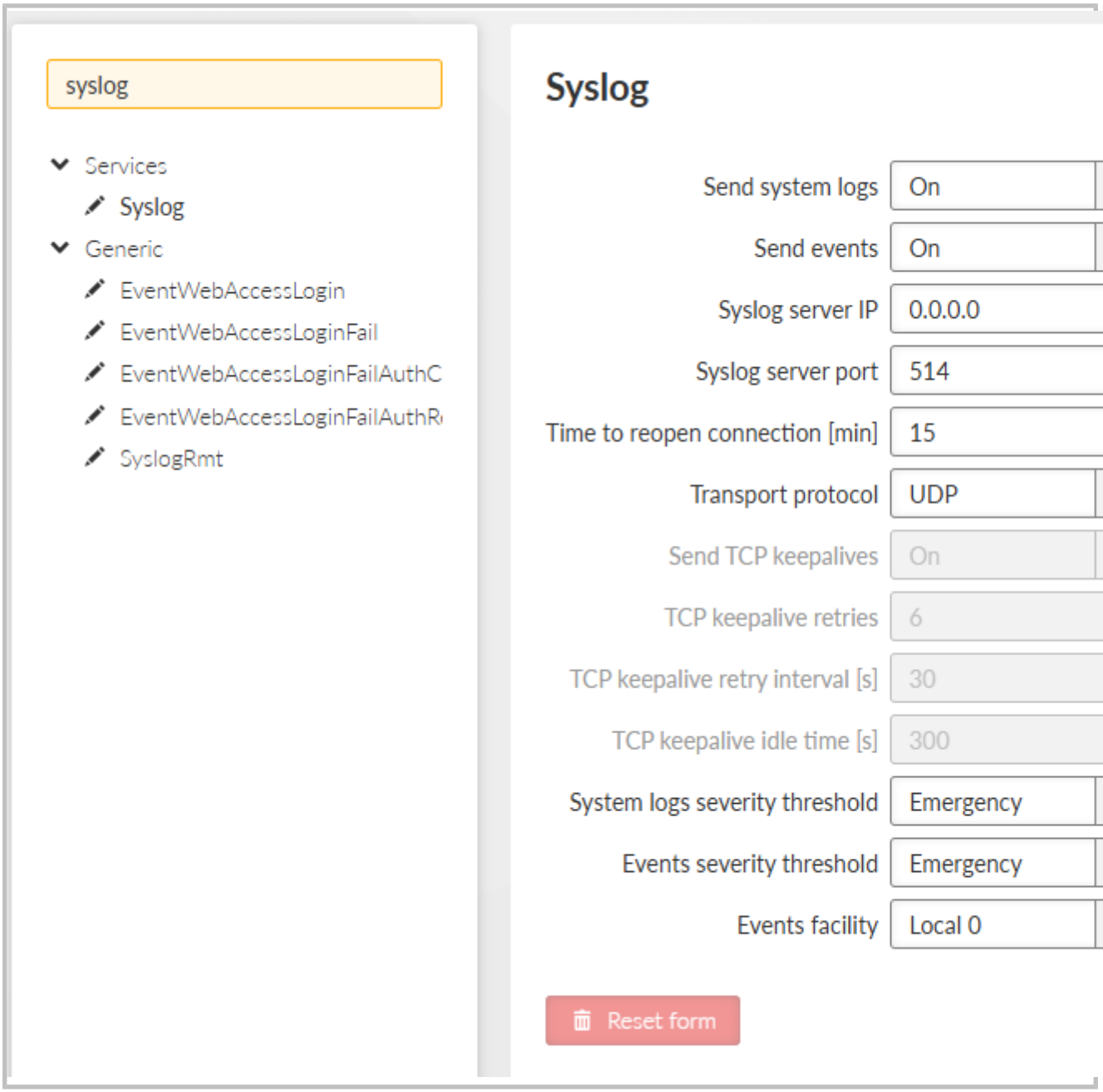


Fig. 5.27: ADVANCED > Services > Syslog

SYSLOG server IP
IP address of the remote Syslog server to which logs will be sent with severity higher than severity set in the Max. severity

SYSLOG server Port
Port used by the Syslog server

Max. severity
List box {Off; 0 Emergency; 1 Alert; 2 Critical; 3 Error}, default= ”Off”
Off - switches off the SYSLOG functionality

Only the events with set severity (and higher) will be sent to the Syslog server. Severities for individual Events can be set in *Section 4.6.3, “Events”*.

Login attempt

List box {Off; Web}, default = "Off"

Switches whether login attempts (both successful and unsuccessful) will be sent to the SYSLOG server.

6. Technical parameters

Tab. 6.1: Technical parameters

Radio parameters	**WaSP**
Frequency bands	200 - 470 and 700 - 960 MHz
Channel spacing	25; 50; 100; 200; 400; 625; 1 250; 2 500; 5 000; 10 000 kHz
Frequency stability	±0.5 ppm
Modulation	4CPFSK; 2CPFSK
FEC (Forward Error Correction)	3/4; Off Trellis code with Viterbi soft-decoder
Gross data rate (data speed)	up to 8.3 Mb/s
RF Output power	20-35 dBm PEP (0.1-3 W RMS) 1 dB step programmable
Duty cycle	Continuous
Rx to Tx Time	< 0.7 ms @ 25 kHz channel
Sensitivity	-110 dBm (2CPFSK; 200 kHz BER 10^{-2}; 3/4 FEC) -95 dBm (2CPFSK; 10 MHz BER 10^{-2}; 3/4 FEC)
Technical parameters are subject to change without prior notification.	

Electrical	**WaSP**	
Primary power	10 to 30 VDC, negative GND	
Rx	9 W @ 24 V, *see details*	
Tx	10 - 27 W @ 24 V for 200 - 470 MHz; 13 - 35 W @ 24 V for 700-960 MHz	
Sleep mode	0.01 W	
Interfaces		
Ethernet	2× 10/100Base-T Auto MDI/MDIX	2× JST-GH (4 pins)
COM	RS232	1× JST-GH (5 pins)
	600 b/s - 1 Mb/s	
USB	USB 2.0	C - connector
Antenna	50 Ω SW configurable 1× Tx / Rx Hi + 1× Rx / Tx Lo	2× MCX @50 Ω
Inputs/Outputs	1× HW alarm input 1× HW alarm output 1× Sleep input	1× JST-GH (5 pins)

Indication LEDs	
LED panel	4× tri-color status LEDs (SYS, RX, TX, COM)
ETH	2× ETH (Link and Activity LEDs)
Environmental	
IP Code (Ingress Protection)	IP 30
MTBF (Mean Time Between Failure)	> 900 000 hours (> 100 years)
Operating temperature	−40 to +60 °C (−40 to +140 °F)
Operating humidity	5 to 95 % non-condensing
Storage	−40 to +85 °C (−40 to +185 °F) / 5 to 95 % non-condensing
Mechanical	
Casing	Rugged aluminium
Dimensions H×W×D	var. A: 22×78×154 mm (0.8×3.0×6.0 in) var. B: 31.3×78×154 mm (1.1×3.0×6.0 in)
Weight	var. A: 295 g (0.65 lbs) var. B: 458 g (1.01 lbs)
Mounting	Through hole M4 (only var. A) or to the thread (M5)
SW	
User protocols on COM	DNP3, DF1, IEC101, Modbus RTU, PR2000, RDS, Siemens 3964(R), COMLI, SAIA S-bus, Mars-A, PPP, UNI, Async Link
User protocols on Ethernet	Modbus TCP, IEC104, DNP3 TCP, Comli TCP, Terminal server…
Serial to IP convertors	DNP3 / DNP3 TCP, Modbus RTU / Modbus TCP
Routing (both, Radio and Ethernet)	Static, Dynamic - Babel, OSPF, BGP, Link management
QoS	8 levels on all interfaces
Protocol on Radio channel	
Radio channel protocols	Transparent, Flexible
Repeaters	Store-and-forward Every unit Unlimited number
Frequency hopping	Interference awareness* - pending
Data integrity control	CRC 32
Security	
Management	HTTPS (Web Interface or Application Programming Interface)
Role-based access control (RBAC)	4 levels (Guest, Tech, SecTech, Admin)
Encryption	AES256-CCM
VPN	IPsec, OpenVPN, GRE
VLAN	IEEE 802.1Q (tagging), Q-in-Q for Transparent mode
Firewall	Layer 2 - MAC, Layer 3 - IP, Layer 4 - TCP/UDP
FW	Digitally signed

Diagnostic and Management	
Link testing	ICMP ping, RSS ping
Status information	User interfaces
Statistics	Historical and differencial statistics for all interfaces
Event log	Events filtered by time, severity, user, remote IP address and type of event
SNMP	SNMPv1, SNMPv2c, SNMPv3 Trap / Inform alarms generation as per settings
NTP	Client / Server
Monitoring	Real time analysis of all interfaces (RADIO, ETH , COM, TS and internal interfaces between software modules).

Tab. 6.2: List of connected cables

Input / Output	Specified length	Shielded / Nonshielded	Recommended cable type
DC power supply 10 – 30 V	As needed	N	V03VH-H 2×0,5
GPIO (Sleep Input, HW Alarm Input, HW Alarm Output)	As needed	S	LiYCY 6×0,14
Antenna connection	As needed	S	Coaxial
COM (RS232)	As needed, typically up to 15 m (RS232)	S	LiYCY 4×0,14
ETH	As needed, typically up to 100 m	S	STP CAT 5e
USB	Max. 3 m	S	USB3

Standards	
CE	RED (pending), RoHS,WEEE, ЕАЭС
Spectrum	ETSI EN 300 220-2 V3.3.1
EMC (electromagnetic compatibility)	ETSI EN 301 489-1 V2.2.3 ETSI EN 301 489-5 V3.2.1
Product safety	EN 62368-1:2014 + A11:2017
Cybersecurity	EN 18031-1:2024
RF health safety	EN 62311:2008

Rx Power consumption @24Vdc	**WaSP**
WaSP	8.3 W
+Ethernet	+0.1 W @ 10BaseT +0.12 W @ 100BaseT per Eth interface with connected equipment
COM	+0.2 W

6.1. Detailed radio channel parameters

Tab. 6.3: Channel spacing 25 kHz

Channel spacing [kHz]	**25**
Occupied BW limit [kHz]	25
Modulation type	FSK
Baudrate [kBaud]	10.42
WaSP Compliance	NA

25 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
10.42	2CPFSK	12K8F1BDN	12.8	25
20.83	4CPFSK	13K7F1DDN	13.7	25

25 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
10.42	7.81	3/4	2CPFSK	-112
10.42	10.42	1/1	2CPFSK	-111
20.83	15.63	3/4	4CPFSK	-110
20.83	20.83	1/1	4CPFSK	-107

Tab. 6.4: Channel spacing 50 kHz

Channel spacing [kHz]	**50**
Occupied BW limit [kHz]	50
Modulation type	FSK
Baudrate [kBaud]	20.83
WaSP Compliance	RED

50 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
20.83	2CPFSK	25K6F1BDN	25.6	50
41.67	4CPFSK	29K1F1DDN	29.1	50

50 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
20.83	15.62	3/4	2CPFSK	-110.1
20.83	20.83	1/1	2CPFSK	-109.2
41.67	31.25	3/4	4CPFSK	-108.1
41.67	41.67	1/1	4CPFSK	-104.9

Tab. 6.5: Channel spacing 100 kHz

Channel spacing [kHz]	**100**
Occupied BW limit [kHz]	100
Modulation type	FSK
Baudrate [kBaud]	41.67
WaSP Compliance	RED

100 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
41.67	2CPFSK	51K2F1BDN	51.2	100
83.33	4CPFSK	58K2F1DDN	58.2	100

100 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
41.67	31.25	3/4	2CPFSK	-108.1
41.67	41.67	1/1	2CPFSK	-107.6
83.33	62.5	3/4	4CPFSK	-106.6
83.33	83.33	1/1	4CPFSK	-101.4

Tab. 6.6: Channel spacing 200 kHz

Channel spacing [kHz]	**200**
Occupied BW limit [kHz]	200
Modulation type	FSK
Baudrate [kBaud]	83.33
WaSP Compliance	RED

200 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
83.33	2CPFSK	103KF1BDN	103	200
166.67	4CPFSK	118KF1DDN	118	200

200 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
83.33	62.5	3/4	2CPFSK	-106.5
83.33	83.33	1/1	2CPFSK	-105.9
166.67	125	3/4	4CPFSK	-104.9
166.67	166.67	1/1	4CPFSK	-101.4

Tab. 6.7: Channel spacing 400 kHz

Channel spacing [kHz]	**400**
Occupied BW limit [kHz]	400
Modulation type	FSK
Baudrate [kBaud]	166.67
WaSP Compliance	NA

400 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
166.67	2CPFSK	207KF1BDN	207	400
333.33	4CPFSK	233KF1DDN	233	400

400 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
166.67	125	3/4	2CPFSK	-103.8
166.67	166.67	1/1	2CPFSK	-103.3
333.33	250	3/4	4CPFSK	-102.8
333.33	333.33	1/1	4CPFSK	-98.8

Tab. 6.8: Channel spacing 625 kHz

Channel spacing [kHz]	**625**
Occupied BW limit [kHz]	625
Modulation type	FSK
Baudrate [kBaud]	260.417
WaSP Compliance	NA

625 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
260.417	2CPFSK	316KF1BDN	316	625
520.833	4CPFSK	356KF1DDN	356	625

625 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
260.417	195.31	3/4	2CPFSK	-101
260.417	260.42	1/1	2CPFSK	-100.5
520.833	390.62	3/4	4CPFSK	-100
520.833	520.83	1/1	4CPFSK	-95.1

Tab. 6.9: Channel spacing 1250 kHz

Channel spacing [kHz]	**1250**
Occupied BW limit [kHz]	1250
Modulation type	FSK
Baudrate [kBaud]	520.833
WaSP Compliance	NA

1250 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
520.833	2CPFSK	637KF1BDN	637	1250
1041.666	4CPFSK	717KF1DDN	717	1250

1250 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
520.833	390.62	3/4	2CPFSK	-98.5
520.833	520.83	1/1	2CPFSK	-97.5
1041.666	781.25	3/4	4CPFSK	-97
1041.666	1041.67	1/1	4CPFSK	-93.6

Tab. 6.10: Channel spacing 2500 kHz

Channel spacing [kHz]	**2500**
Occupied BW limit [kHz]	2500
Modulation type	FSK
Baudrate [kBaud]	1041.666
WaSP Compliance	NA

2500 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
1041.666	2CPFSK	1M28F1BDN	1280	2500
2083.333	4CPFSK	1M45F1DDN	1450	2500

2500 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
1041.666	781.25	3/4	2CPFSK	-95.7
1041.666	1041.67	1/1	2CPFSK	-95.2
2083.333	1562.5	3/4	4CPFSK	-94.1
2083.333	2083.33	1/1	4CPFSK	-90.6

Tab. 6.11: Channel spacing 5000 kHz

Channel spacing [kHz]	**5000**
Occupied BW limit [kHz]	5000
Modulation type	FSK
Baudrate [kBaud]	2083.333
WaSP Compliance	NA

5000 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
2083.333	2CPFSK	2M51F1BDN	2510	5000
4166.666	4CPFSK	2M87F1DDN	2870	5000

5000 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
2083.333	1562.5	3/4	2CPFSK	-92.5
2083.333	2083.33	1/1	2CPFSK	-92.2
4166.666	3125	3/4	4CPFSK	-90.6
4166.666	4166.67	1/1	4CPFSK	-87.1

Tab. 6.12: Channel spacing 10000 kHz

Channel spacing [kHz]	**10000**
Occupied BW limit [kHz]	10000
Modulation type	FSK
Baudrate [kBaud]	4166.666
WaSP Compliance	NA

10000 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
4166.666	2CPFSK	4M81F1BDN	4810	10000
8333.332	4CPFSK	5M44F1DDN	5440	10000

10000 kHz				
Classification				**Sensitivity**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-6}**
4166.666	3125	3/4	2CPFSK	-89.4
4166.666	4166.67	1/1	2CPFSK	-89
8333.332	6250	3/4	4CPFSK	-85.5
8333.332	8333.33	1/1	4CPFSK	-80.4

7. Safety, regulations, warranty

7.1. Frequency

The radio modem must be operated only in accordance with the valid frequency license issued by national frequency authority and all radio parameters have to be set exactly as listed.

Important

Use of frequencies between 406.0 and 406.1 MHz is worldwide-allocated only for International Satellite Search and Rescue System. These frequencies are used for distress beacons and are incessantly monitored by the ground and satellite Cospas-Sarsat system. Other use of these frequencies is forbidden.

Important

The radio operator is responsible for setting the radio parameters of the radio modem exactly in accordance with the valid frequency license issued by national frequency authority, and all radio parameters to be set exactly as listed.

7.2. High temperature

If the WaSP is operated in an environment where the ambient temperature exceeds 55 °C, the WaSP must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

7.3. SW license

Conditions of use of this product software abide by the license mentioned below. The program spread by this license has been freed with the purpose to be useful, but without any specific guarantee. The author or another company or person is not responsible for secondary, accidental or related damages resulting from application of this product under any circumstances.

RACOM Open Software License

Version 1.0, November 2009

Copyright (c) 2001, RACOM s.r.o., Mírová 1283, Nové Město na Moravě, 592 31

Everyone can copy and spread word-for-word copies of this license, but any change is not permitted.

The program (binary version) is available for free on the contacts listed on https://www.racom.eu. This product contains open source or another software originating from third parties subject to GNU General Public License (GPL), GNU Library / Lesser General Public License (LGPL) and / or further author licenses, declarations of responsibility exclusion and notifications. Exact terms of GPL, LGPL and some further licenses is mentioned in source code packets (typically the files COPYING or LICENSE). You can obtain applicable machine-readable copies of source code of this software under GPL or LGPL licenses on contacts listed on https://www.racom.eu. This product also includes software developed by the University of California, Berkeley and its contributors.

7.4. Warranty

RACOM-supplied parts or equipment ("equipment") is covered by warranty for inherently faulty parts and workmanship for a warranty period as stated in the delivery documentation from the date of dispatch to the customer. The warranty does not cover custom modifications to software. During the warranty period RACOM shall, on its option, fit, repair or replace ("service") faulty equipment, always provided that malfunction has occurred during normal use, not due to improper use, whether deliberate or accidental, such as attempted repair or modification by any unauthorised person; nor due to the action of abnormal or extreme environmental conditions such as overvoltage, liquid immersion or lightning strike.

Any equipment subject to repair under warranty must be returned by prepaid freight to RACOM direct. The serviced equipment shall be returned by RACOM to the customer by prepaid freight. If circumstances do not permit the equipment to be returned to RACOM, then the customer is liable and agrees to reimburse RACOM for expenses incurred by RACOM during servicing the equipment on site. When equipment does not qualify for servicing under warranty, RACOM shall charge the customer and be reimbursed for costs incurred for parts and labour at prevailing rates.

This warranty agreement represents the full extent of the warranty cover provided by RACOM to the customer, as an agreement freely entered into by both parties.

RACOM warrants the equipment to function as described, without guaranteeing it as befitting customer intent or purpose. Under no circumstances shall RACOM's liability extend beyond the above, nor shall RACOM, its principals, servants or agents be liable for any consequential loss or damage caused directly or indirectly through the use, misuse, function or malfunction of the equipment, always subject to such statutory protection as may explicitly and unavoidably apply hereto.

Appendix A. Proprietary UDP/TCP ports

The following UDP and TCP ports are reserved for use in the unit's management system: 8800 - 9823. This entire range can be shifted to a different base value using the Advanced parameter DevicePortBase.

The following table lists some basic ports that may be important when configuring the unit.

Tab. A.1: WaSP proprietary UDP/TCP ports

UDP/TCP port number	Name
8881	COM1
8882	COM2
8883	COM3
8889	Remote access
8892	TS1
8893	TS2
8894	TS3
8895	TS4
8896	TS5
8906	RSS ping

Revision History

Revision
This manual was prepared to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you.

Revision 1.0 2026-01-15
First issue

Revision 1.1 2026-08-04
Connectors updated reflecting final version of the connectors and LED labels
Diagnostics corrected
Technical parameters updated to actual version of technical parameters