Configuration Guide for

RAK LoRaWAN Industrial Gateway

WisDevice Series

RAK7249/58

Version 1.7 | October, 2019

www.RAKwireless.com

Visit our website for the latest copy of this manual.

35 PAGES

Table of Contents

1 Overview

This document describes in detail the functionality of the Web Management UI. The interface builds on top of OpenWRT and all gateway products of the RAK72xx line share it.

The document gives instructions on configuring WAN, the LoRa Packet Forwarder and Gateway MQTT Bridge. It explains how to do system-monitoring, update of the firmware and reset the device. Last, but not least in provides information on using the built-in LoRa Server.

This guide functions as reference for several products with similar functionality. Thus, some sections will apply to certain products and not others.

2 Gateway Start-up

Make sure all the antennas are connected before powering the Gateway.

For RAK7258 use the included adapter. RAK7249 comes with a PoE injector, which you need to connect to the grid on one side and to the Gateway on the other (Ethernet cable not included).

The Gateway comes configured in such a way that you can use either the Ethernet port or the Wi-Fi in AP mode to connect to the Management platform.

In both modes you can access the Management UI via a web browser pointing to the IP address of the Gateway (check your router DHCP list). Alternately, the IP Address (192.168.230.1) is preconfigured as the one to use for access to the device provided you are directly connected to it.

WiFi AP mode

By default the Gateway is configure to work in Access Point (AP) mode. It has the following parameters:

Wi-Fi

SSID: RAK72XX_xxxx (no password is required to connect via Wi-Fi)

Web UI

Connect via a browser to the IP address assigned to the gateway, which is 192.168.230.1 by default. You should see the login window in Figure 1. Use the credentials below:

UI user: root

UI password: root

***Figure 1** | Login window*

WAN port (DHCP IP) mode

Connect the Ethernet cable to the port marked “ETH” and the other end to your Router. Use the same credentials for the Web UI as for AP mode.

3 Web Management Platform

After you have entered the correct credentials, you can start exploring the configuration and monitoring interface of the RAK LoRa Gateway.

3.1 Status

This is where statistics about the Gateway behavior can be monitored in real time.

3.1.1 Overview

Upon logging in the browser displays the page in Figure 2.

The following are the parts of the Overview window:

Received:

Shows the total number of uplink LoRa messages received by the gateway.

Transmitted:

Shows the total number of downlink LoRa message sent by the gateway.

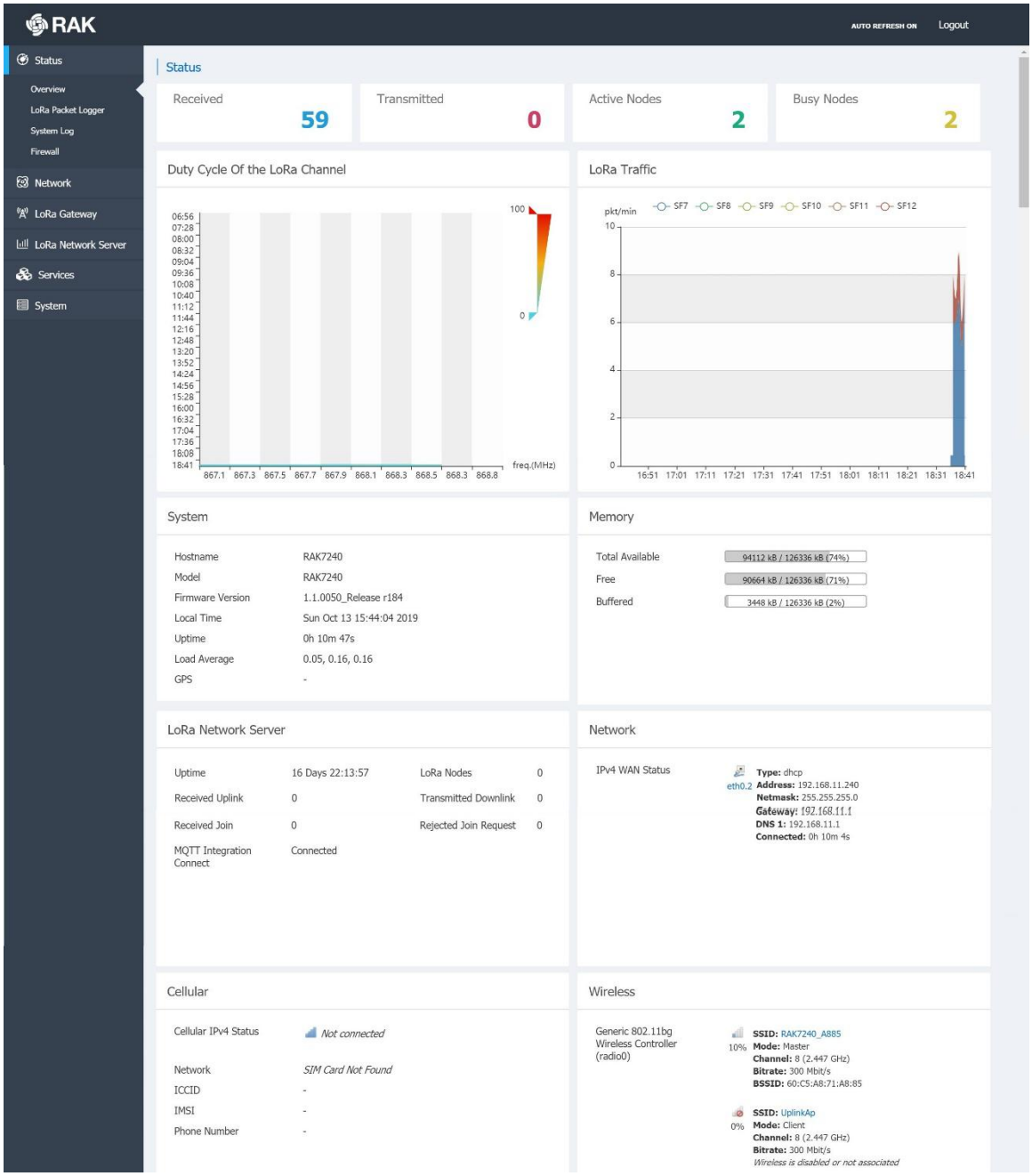

***Figure 2** | Status Overview page*

Active Nodes:

Shows the number of active LoRa nodes within the LoRa gateway coverage (those that have sent no data for more than 10 min are discarded from the count).

Busy Nodes:

Shows the number of busy nodes within the LoRa gateway coverage (nodes with an average message spacing of less than 60s).

Duty Cycle of the LoRa Channel

The graph represents the Duty Cycle load by frequency channel (Data is kept for the last 12 hours). The minimum resolution along the time axis is 60s. Each value is an average over 60s. The values are color code – green to red, low to high.

LoRa Traffic:

The graph shows the packet per minute rate as a function of time. Above the image, one can see the color-coding of the different Spreading Factors, where the actual height of the values is a sum of all the packets over all spreading factors for the time sample.

Additionally you have sub-windows displaying the System, Memory, LoRa Netowrk Server, Network (WAN). Cellular, and Wi-Fi information. Those have their separate sections and will be discussed in detail further down.

System:

Information for the Hostname and model of the Gateway can be found here. There is also the Local Time and Uptime of the Gateway. Most importantly you can see the Firmware version here.

Memory:

There are bars in this section that show how much the Total Available, Free and Buffered Memory is.

LoRa Network Server:

You can see statistics for you network server. Number of associated LoRa Nodes, Uplink, Downlink, Received Join, Rejected Join, those types of packets all have a numerical value associated with them. Additionally, you can check the Uptime and whether you have the MQTT Integration running.

Network:

The WAN status with its Type and Addressing parameters, together with the time since it has been connected are displayed here.

Cellular:

The connection status of your cellular together with the corresponding Network ID and the parameters of your Sim (ICCID, IMSI, Phone number).

Wireless:

The status of the Wi-Fi is displayed here. There is the connectivity status, signal strength and Ip addressing parameters for both the AP and Client interfaces.

3.1.2 LoRaWAN Packet Logger

This is where a log of the LoRa messages is shown in real time. There are several options for filtering as well as the possibility to download the statistics in a file. Additionally there is a summary (Total, Uplink, and Downlink), below the filter fields.

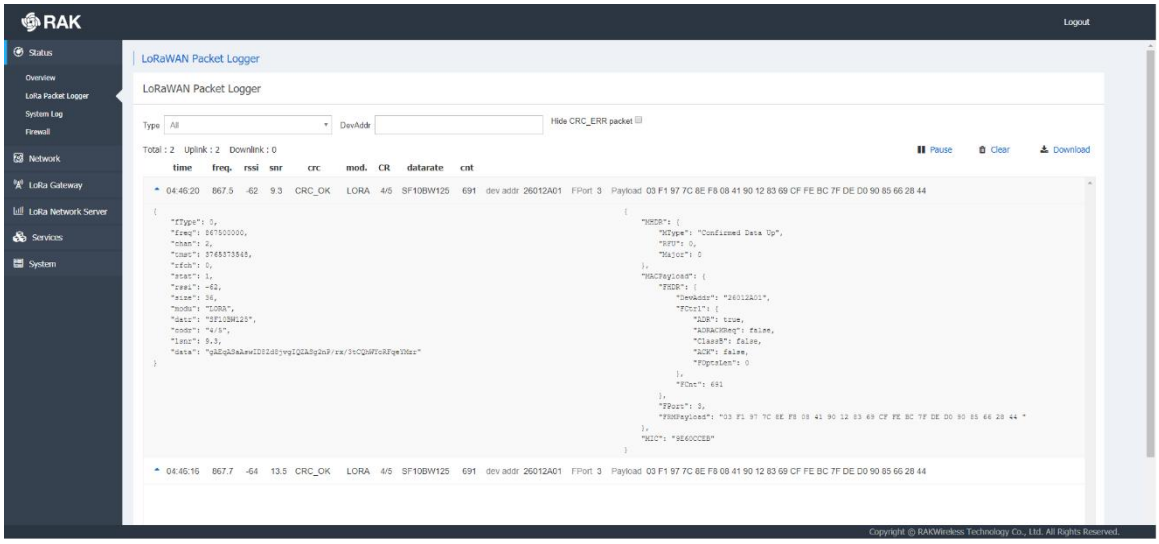

***Figure 3** | LoRa Packet Logger page*

The user can choose to filter the packets by one of the following:

Type:

Filter by message type. By default, all messages are displayed, where possible options are: Join Request/Accept, Unconfirmed Data Up/Down, and Confirmed Data Up/Down

DevAddr:

Filter messages based on the Device Address in order to single out a node.

Hide CRC_ERR packet:

This check box hides messages that are corrupted in some way and will not be forwarded.

The buttons for Pause/Play, Clear and Download of the data are in the top right over the list.

If the user clicks on a given packet the window is expanded detailed information about the contents of the message is displayed

3.1.3 System Log

The complete system log. It is useful mainly for debugging purposes.

3.1.4 Firewall

Statistics for the Gateway Firewall

3.2 Network

3.2.1 WAN Interface

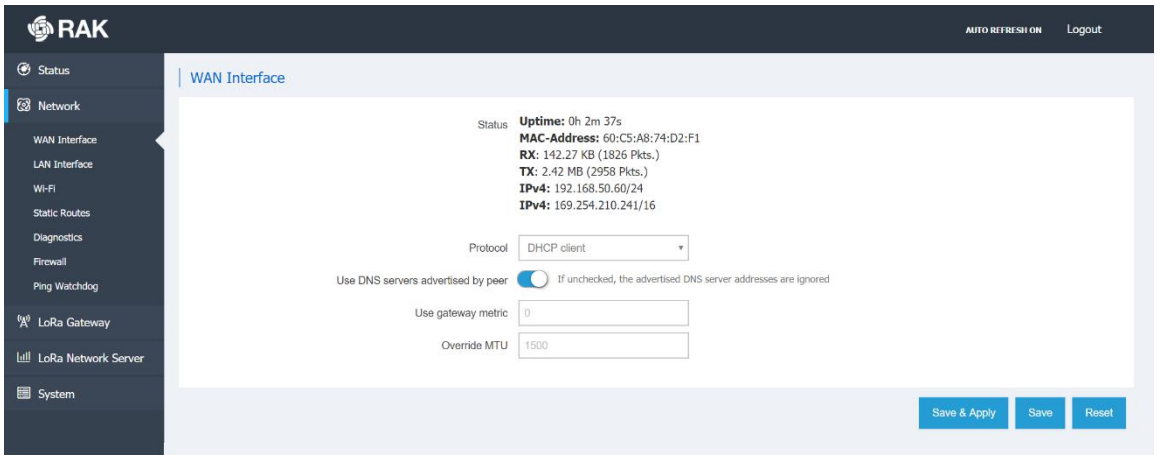

***Figure 4** | WAN Interface*

The user can check the Status (Uptime, IPv4 Address, etc.), or configure the protocol to be used for connecting to your provider's network.

The following options are available: DHCP/PPPoE/Static address.

3.2.2 Cellular Interface

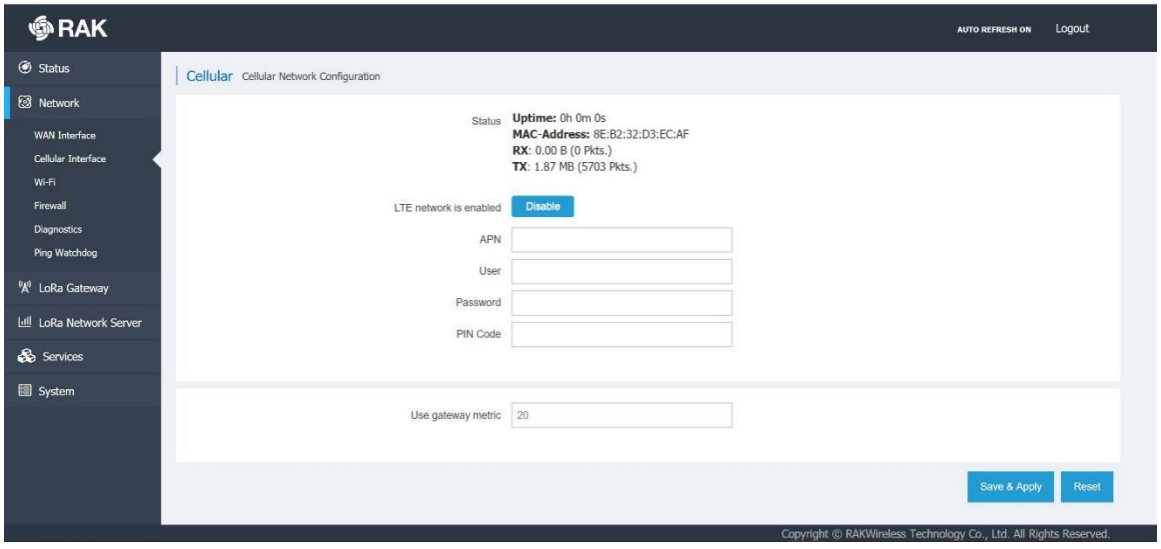

***Figure 5** | Cellular Interface*

The same statistics as with the WAN Interface are available. It is here that you set the **APN**, **User**, and **Password**. The gateway metric determines the priority of this interface, compared with the other connectivity options. The lower the value the higher the priority.

There is also a field for the PIN Code in case your SIM card is locked.

3.2.3 Wi-Fi

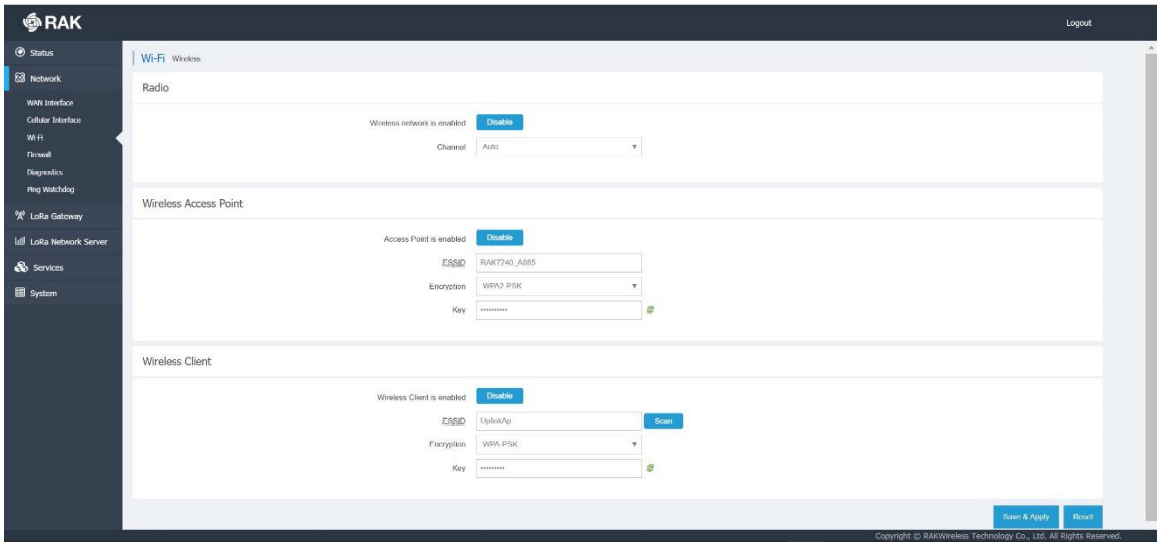

***Figure 6** | Wi-Fi Interface*

Enabling/Disabling the Wi-Fi is done from this page via the blue button at the top. Additionally you can pick a radio channel or leave it on Auto configuration. The Wi-Fi can work in one of two modes:

Access Point:

By default, there is no password. One can access the Web UI via the IP address: 192.168.230.1 once connected to the AP. The SSID is RAK72xx_xxxx by default.

Client:

Choose this option to use Wi-Fi as a backhaul for the Gateway. You need to manually enter the SSID, Encryption method and the Key itself.

By default, the client mode is disabled. If you want to use it you have to click the “Enable” button. Click the “Scan” button to choose your preferred wireless network. Choose the encryption method, fill in the password and press Save & Apply.

3.2.4 Firewall

You can configure a number of settings including, but not limited to: Zones, Port Forwarding, NAT, etc.

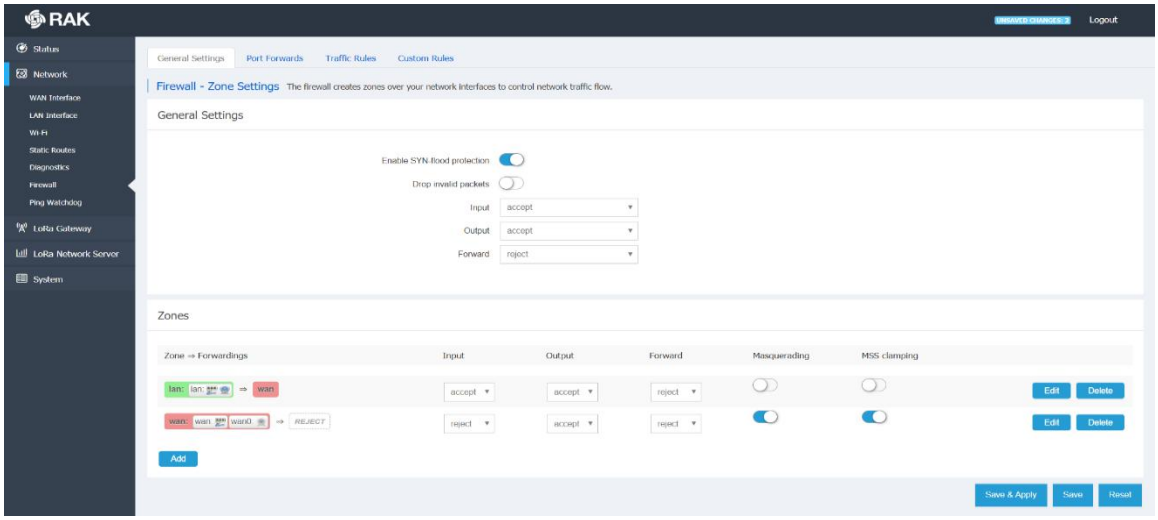

***Figure 7** | Firewall Settings*

3.2.5 Diagnostics

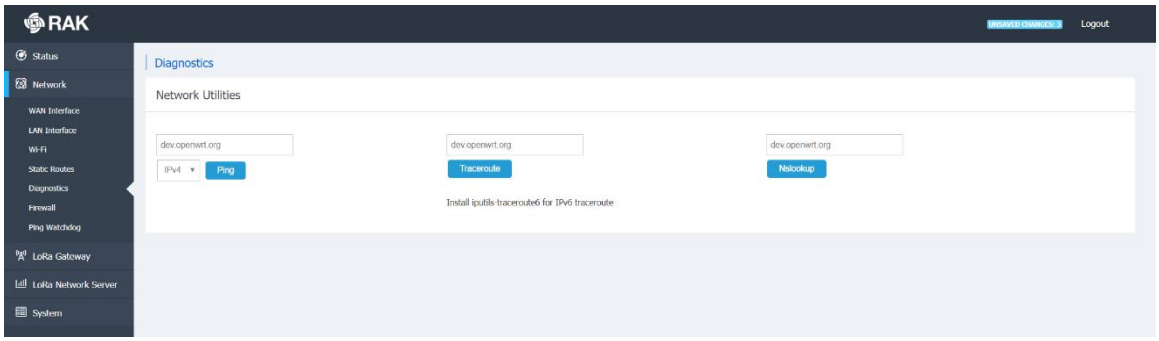

***Figure 8** | Diagnostics*

This is where you can perform checks via the built-in tools: *Ping*, *Traceroute*, *Nslookup.*

You can enter either an URL or an IP Address in the text box and execute the command with the button. Both IPv4 and IPv6 are supported. The results are conveniently displayed in a CLI box.

3.2.6 Ping Watchdog

Ping Watchdog monitors the quality of network links by constantly pinging the specified IP Address or Domain name on the specified uplink network interface. When network link failures are detected, scheduled measures are taken automatically. Those include: Interface restart, Interface priority reduction, Device restart, etc.

Note: Reducing the priority of an uplink interface only works when the LoRa Gateway uses both Ethernet and Cellular as uplink methods at the same time.

WAN interface represents the Ethernet uplink interface and WWAN represents the LTE cellular network uplink interface.

For example if Ping Watchdog is enabled for both uplink interfaces at the same time and the response to degradation of the link quality is set as Increase Gateway Metric the two uplink interfaces work as backups for each other. In the event of significant degradation on one, the Gateway switches to the other.

The Gateway Metric determines the priority of interfaces. The default value can be adjusted in the Network menu for the corresponding interface. The lower the Gateway metric, the higher the priority of the link.

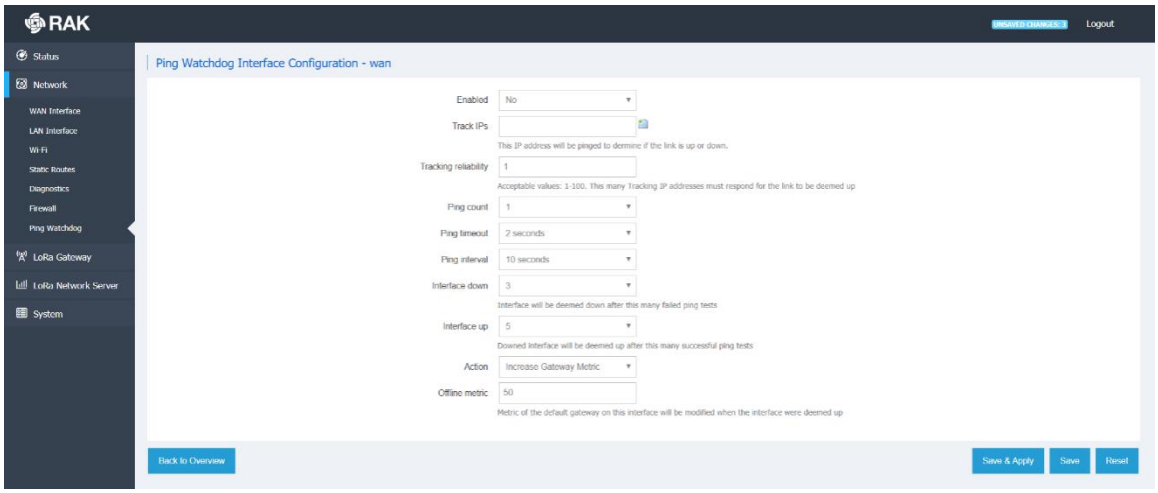

***Figure 9** | Ping Watchdog Interface Configuration*

3.3 LoRa Gateway

All the LoRa Settings reside in this section.

3.3.1 LoRa Packet Forwarder

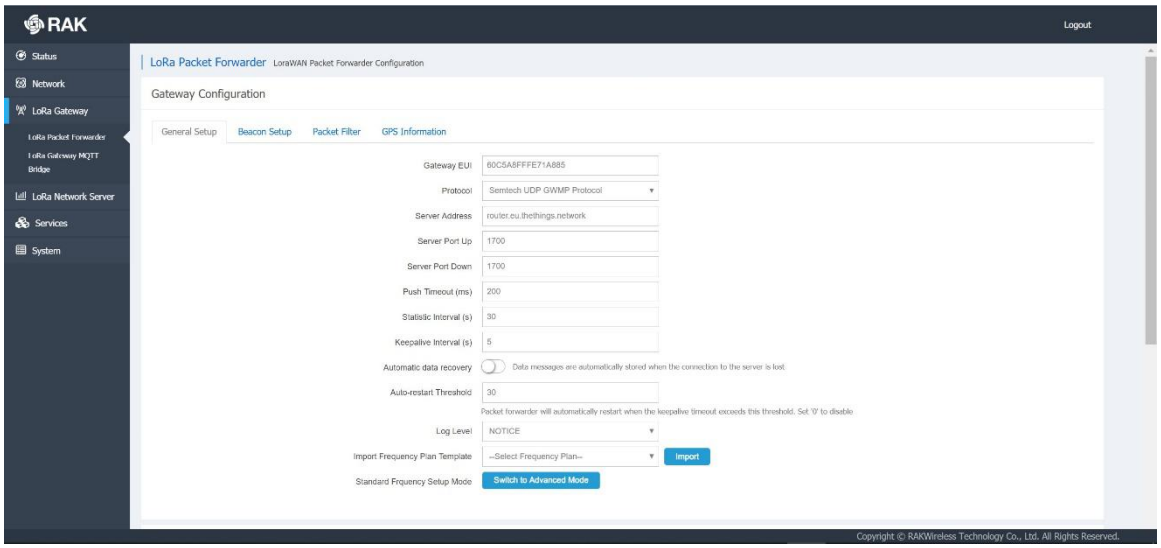

***Figure 10** | Packet Forwarder General Setup*

As this is the most important part of the LoRaWAN Gateway, the number of settings and options is greatest here. Thus, this section will be larger and provide information in more detail than previous ones. For the aforementioned reasons this section has several configuration tabs, which are listed in the following paragraphs. Additionally some of the configuration options have their own documents, with detailed explanation of the configuration process.

General Setup

This is where the core settings are: Gateway EUI, Frequency channels, etc.

Gateway EUI:

The value in this field is necessary for registering your gateway with any LoRaWAN Network Server.

Protocol:

You have three options, which define how the Gateway will function:

Semtech UDP GWMP Protocol:

By default, this is the Semtech Packet Forwarder, which sends packets to the Server Address of your choice (IP or URL). By default, it points to the local TTN router.

The default port value is 1700 used by TTN.

One can also set parameters as the *Push Timeout (ms), Statistic Interval (s)*, *Keep Alive Interval (s)* and the *Auto-restart Threshold*.

Automatic Data Recovery

This is an important feature that allows LoRa Frames to be stored on the SD card (provided there is one in the slot), if there is no connection to the LoRa Network Server. Upon restoring connectivity, these buffed messages will be forwarded, so no data will be lost. This is done in blocks of 8 (FIFO), until all are cleared from the buffer.

LoRa Gateway MQTT Bridge:

By choosing this option, you make the Gateway act as a bridge to the MQTT Broker, which is hosted somewhere separate. You need to configure the Gateway to point to the correct address of the MQTT broker

Built-in LoRa Server:

In case you require an integrated solution where the LoRa Network Server is hosted on the gateway itself you choose this option. The configuration of the LoRa MQTT Bridge itself is done in a separate section of the configuration UI, which is discussed in Paragraph 3.3.2

Log Level

You can choose from 5 different log levels (*Error/Warning/Notice/Info/Debug*). This will affect System Log. From Errors only to full system log for debugging.

Beacon Setup

In the case of Class B LoRa devices, you need to have a beacon in order to synchronize downlink message windows. Thus, you have to configure its parameters: Frequency Channel, SF, Bandwidth, Tx Power, etc. Make sure you adhere to the LoRa Alliance recommendations.

Packet Filter

By enabling this functionality, you can filter incoming traffic and only forward packets from the desired nodes in order to optimize bandwidth usage over backhaul. You can filter by OUI or Network ID by whitelisting.

The *Enable Auto Filter* slider allows nodes to be automatically dropped in accordance with a set of parameters. One can set threshold values for *Discard Period*, *Join Period*, *Join Interval*, and *Join Count* (1 and 2 for Join Interval and Join Period respectively).

GPS Information

In case, you want to enter the GPS parameters for the Gateway manually.

Frequency Plan

This is a part of the page, common for all gateway from the RAK72xx series, however depending on the number of Concentrator modules installed there are variations. The difference when there is a second Concentrator is that first it has to also be configured, and second only the fields for the central frequencies for Radio 0 and Radio 1 need be set.

There are two mode for setting the frequencies:

Standard Mode:

You can start by importing a region via the drop down menu (EU868 is the default one). You will get the defaults channels for the chosen frequency band and the option to add additional ones. Simply enter the frequency in the text box (in MHz) and click the “Add” button. You can add as many channels as you need as long as they fall in the Regional band.

Additionally, there is a field for adding the Standard LoRa Channel and FSK channel (you need also choose the SF, Bandwidth and data rate of each of the aforementioned).

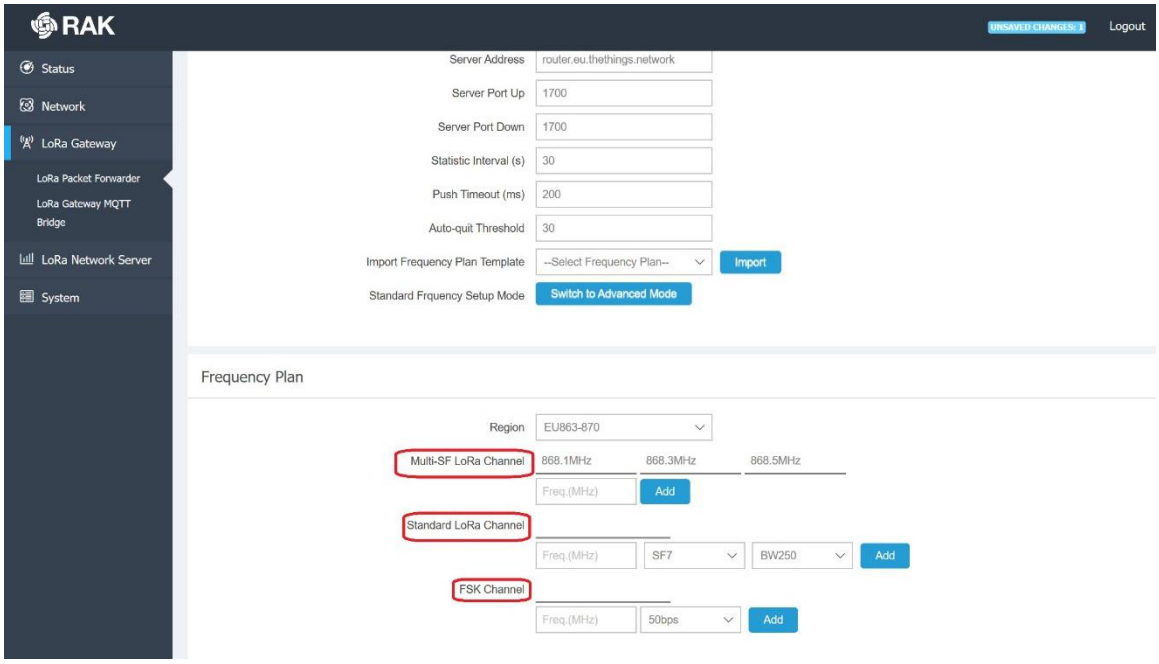

***Figure 11** | Packet Forwarder General Setup*

Advanced Mode:

Because of the presence of double SX1257s, you need to configure the two radios separately. You have eight Multi Spreading Factor Channels, The LoRa Standard Channel and the FSK Channel. The sliders can enable or disable those, so you can choose to have any number of them active. Additionally you can choose which radio to use for a given, channel as long as you do not assign more than five channels per radio. In order to set the desired channel to a given frequency you need to input an offset value in the *If* field. Thus, the channel frequency will be the central frequency (*Radio 0 Freq* or *Radio 1 Freq* parameter) summed with the offset value (in Hz).

Additionally for the LoRa Standard and FSK channels, you are also required to select the Bandwidth and Data Rate.

As mentioned before you can choose to import those settings for the Indian, Russian and EU Regions (in accordance with the LoRa Alliance specifications).

For details on the procedure refer to the Packet Forwarder Customs Spectrum Settings Guide.

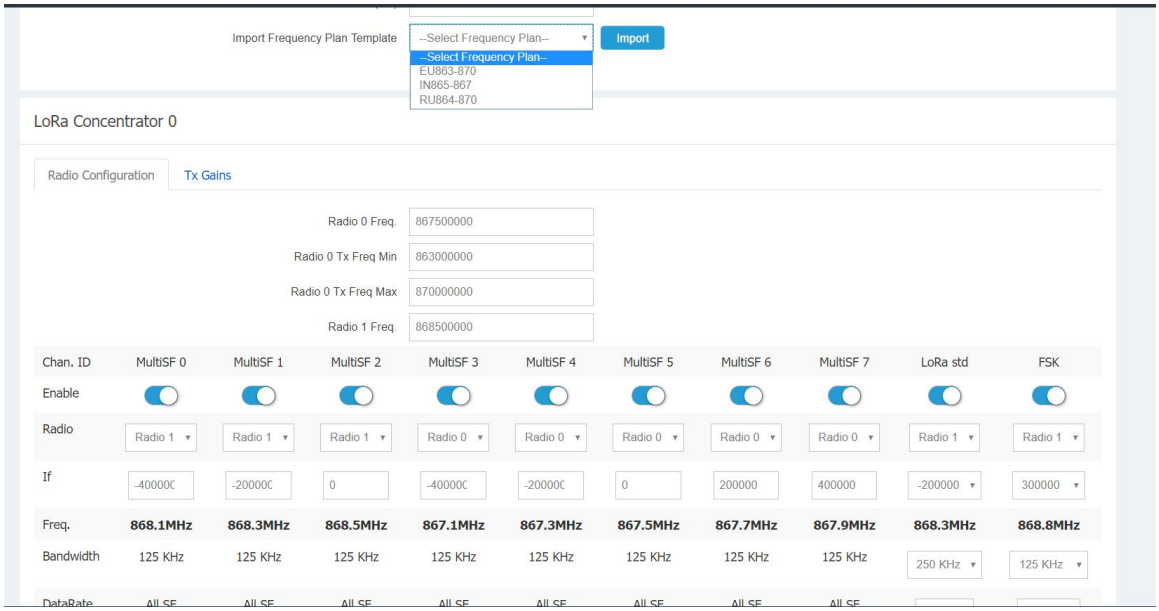

***Figure 12** | Frequency Plan configuration*

3.3.2 LoRa Gateway Bridge

The Gateway is capable of working with an external LoRa Server, where the MQTT Broker is functioning separately. For this purpose, there are several tabs with their corresponding parameters to be filled.

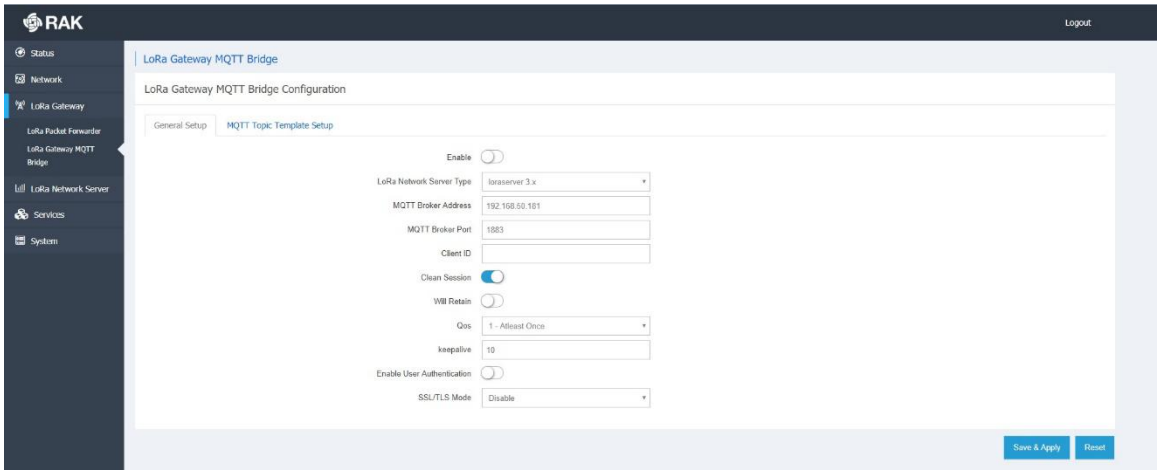

***Figure 13** | MQTT Bridge*

General Setup

The tab starts with the button to enable/disable this functionality, followed by:

MQTT Broker Address:

You have 3 options here.

- Built-in LoRa Network Server

  Choose this if you are going to be using the Built-in LoRa Network Server

- ChirpStack 2x

  Choose this if you are pointing to an MQTT 2x Broker (JSON)

- ChirpStack 3x

  Choose this if you are pointing to an MQTT 3x Broker (Protobuf)

MQTT Broker Address:

The IP Address where the MQTT Broker is hosted.

MQTT Broker Port:

The corresponding port.

Enable Authentication:

The switch turns on Encryption of the transmitted data. You need to configure the Certificates used to encrypt the data in order for secure authentication to be performed.

TLS Version:

The version of the TLS protocol to be used. Options are TLSv1, TLSv1.1, TLSv1.2

Username/Password:

Credentials the MQTT Bridge is to use for connecting to the LoRa Server instance

CA Certificate, TLS Certificate, TLS Key:

Those are to be generated via the appropriate algorithm and distributed between the MQTT Broker and the LoRa Server.

Please refer to the MQTT Bridge with TLS Encryption Configuration Manual for details on how to edit the settings in order for the Gateway to work as an MQTT Bridge with TLS Encryption.

MQTT Topic Template Setup

Refer to the image below for the MQTT 2x Topic Template

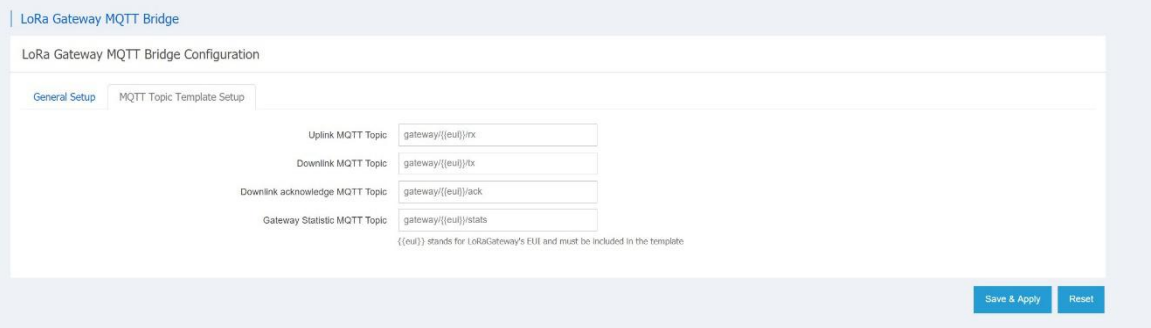

***Figure 14** | MQTT 2x*

Refer to the image below for the MQTT 3x Topic Template

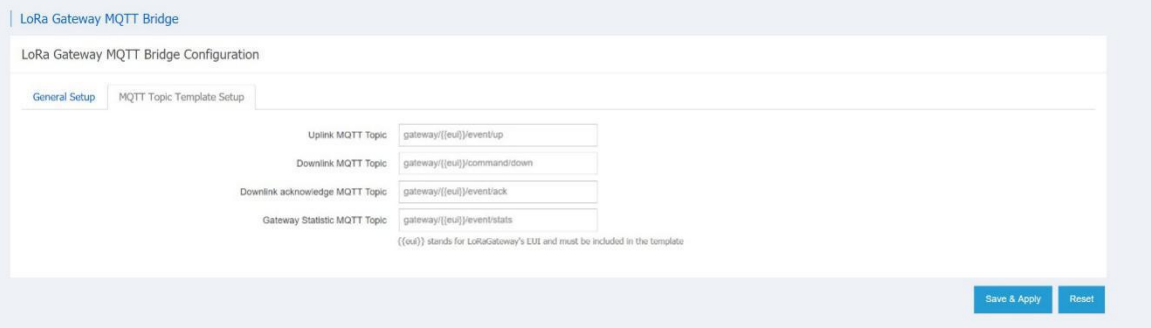

***Figure 15** | MQTT 3x*

3.4 LoRa Network Server

The Gateway comes with an integrated LoRa Networks server. This makes the Gateway a standalone solution for the whole LoRaWAN chain in one device, which is immensely helpful for testing purposes, and provided for flexibility in deployment options.

Naturally, one can opt to disable this feature and use a LoRa Network Server hosted separately.

3.4.1 Status

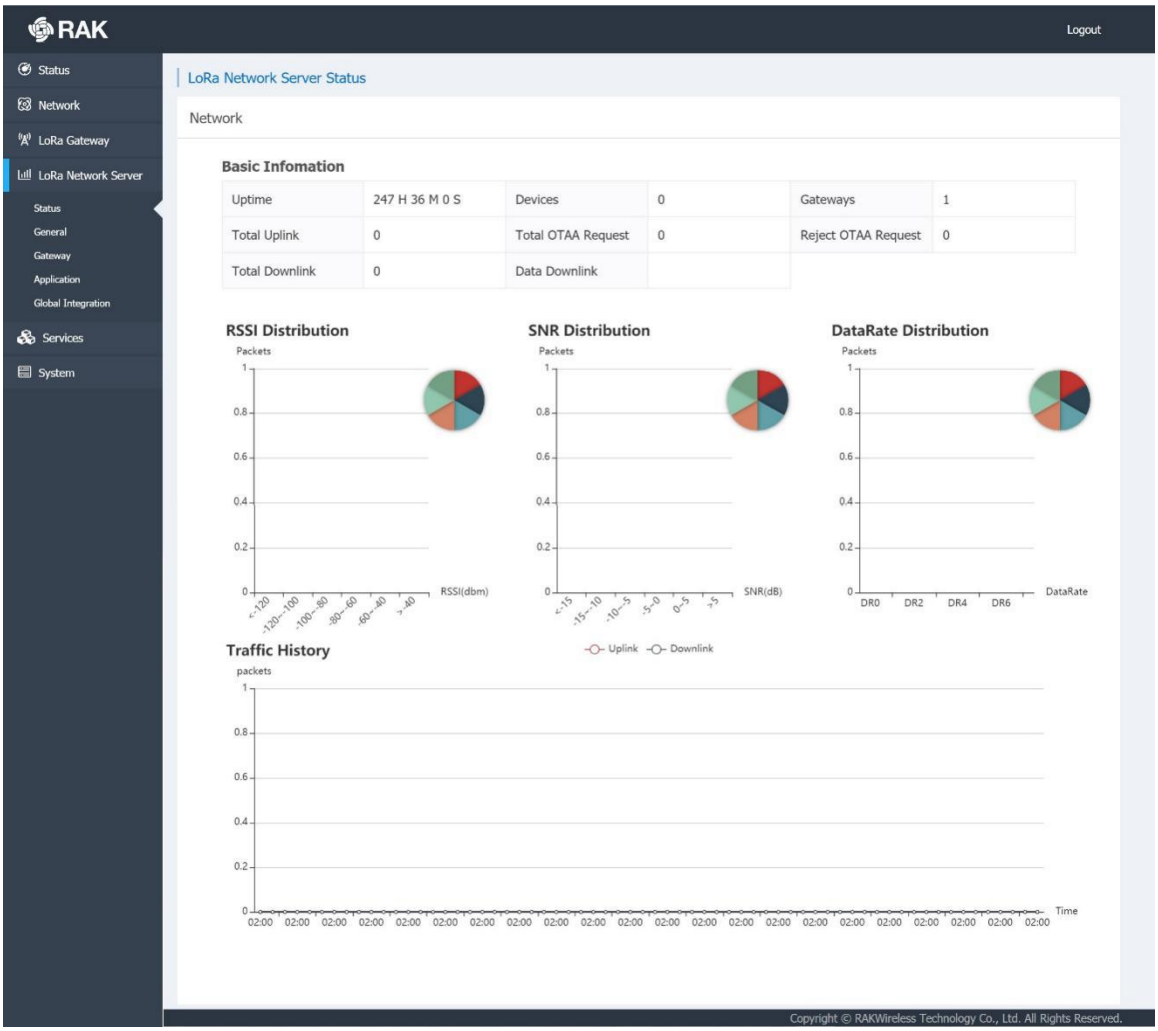

***Figure 16** | LoRa Network Server Status page*

3.4.2 General

In order to use the LoRa Server you need to enable its protocol from the following menu:
LoRa Gateway Menu -> LoRa Packet Forwarder -> Protocol -> Built-in LoRa Server
Now you can choose to enable/disable it via the slider in the General Configuration tab.

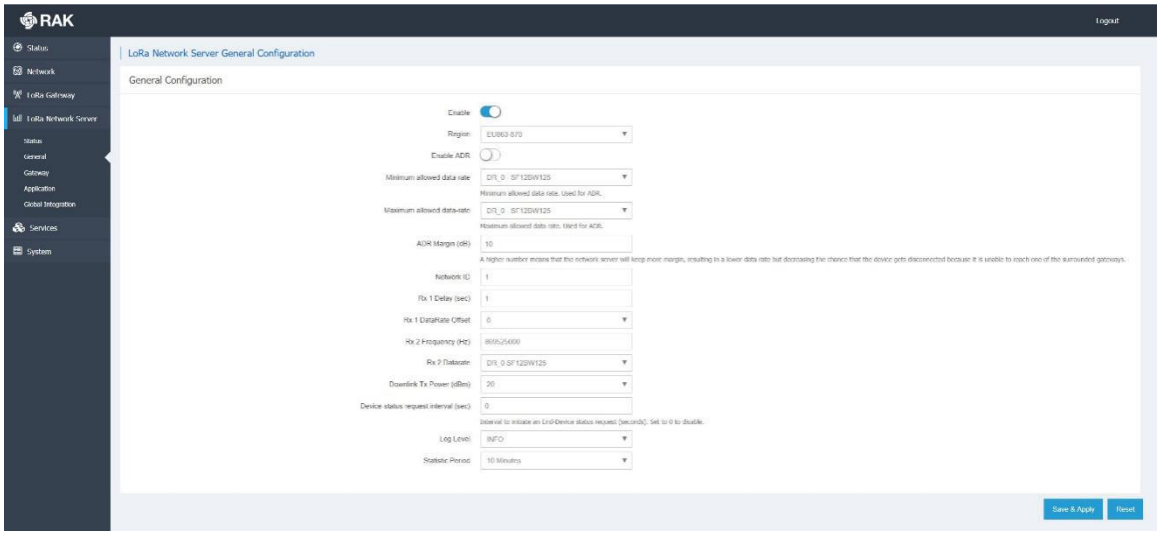

***Figure 17** | NS General Configuration*

Below is a short explanation of the main parameters:

Frequency Plan (Region)

A drop-down menu list including the following:
EU-863-870, IN868-867, US902-928, AS923, CN470-510, AU915, KR920

Enable ADR

If you choose to use Adaptive Data Rate, you need to enable it via the slider and further configure the Minimum and Maximum allowed value.

Minimum and maximum allowed data-rate

Note the DR_0, to DR_15 values represent a bits/s value and max payload size. Those are dependent on your region of operation and the bandwidth and SF used. However as they are predefined by the LoRa Alliance the menu does not list the full parameter values. Please refer to the official documentation for details.

ADR Margin

This value is in dB and it directly affects the probability of a node being disconnected if channel quality is poor. Higher value will result in a lower data rate, but better range.

Network ID

The ID of the network to be advertised to end devices in case you want to have roaming to other networks

Rx 1 Delay (sec)

The First Receive window delay can be west here (check with local recommendations)

Rx 1 DataRate Offset

In case you want to have a different data rate for the Downlink (synch with node)

Rx 2 Frequency (Hz)

The frequency of the Second Receive window.

Rx 2 Datarate

A value can be picked that corresponds to a combination of Spreading Factor and Bandwidth.

Downlink Tx Power

This is the maximum power in *dBm* the Gateway is allowed to use when transmitting frames to the nodes. It is region specific (for example EU – 14dBm)

Device-status request interval

The time in *seconds* between node status request messages sent by the Gateway. Default value of 0 (disabled status requests).

Log Level

You can choose from 5 different log levels (*Error/Warning/Notice/Info/Debug*). This will affect System Log. From Errors only to full system log for debugging.

Statistics Period

This is the aggregation interval for the Gateway Statistics

3.4.3 Gateway

In this section you can add and External Gateways to work with your LoRa Network Server. This way packet forwarded by the listed Gateways will be forwarded as though they were within the range of this device. Refer to Figure 11 for an overview of the section window:

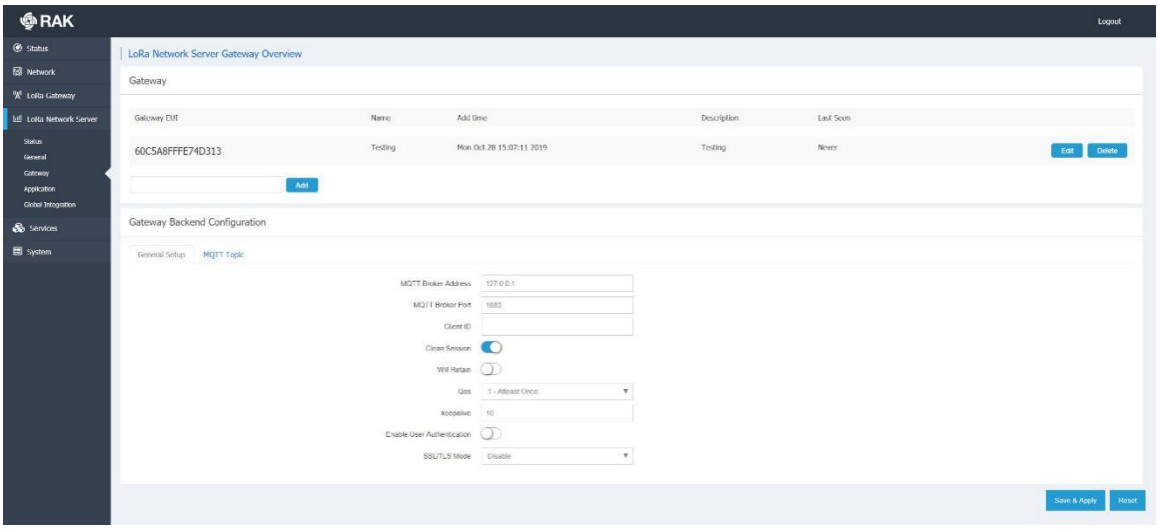

***Figure 18** | NS Gateway tab*

Below is a short explanation of the main parameters:

Gateway

Here you can add a Gateway. You simply need to input the EUI into the text box and press the *Add* button. Additionally you can add a Name, Description and the coordinates of the Gateway.

Gateway Backend Configuration

By filling this section, you are pointing the LoRa Network Server to the MQTT Broker

MQTT Broker Address:

The IP Address where the MQTT Broker is hosted.

MQTT Broker Port:

The corresponding port.

Enable User Authentication:

If this is switched on, an Username, Password, and a Certificate (Disabled by default) will be required for user authentication.

SSL/TLS Mode:

Choose the certificate type here:

CA Signed server certificate, Self-signed server certificate, Self-signed server & client certificate. All certificated have support for TLSv1, TLSv1.1, and TLSv1.2.

MQTT Topic

Here you can get information on the topic templates: *Uplink MQTT topic, Downlink MQTT Topic, Downlink Acknowledge MQTT Topic, Gateway Statistic MQTT Topic.*

3.4.4 Applications

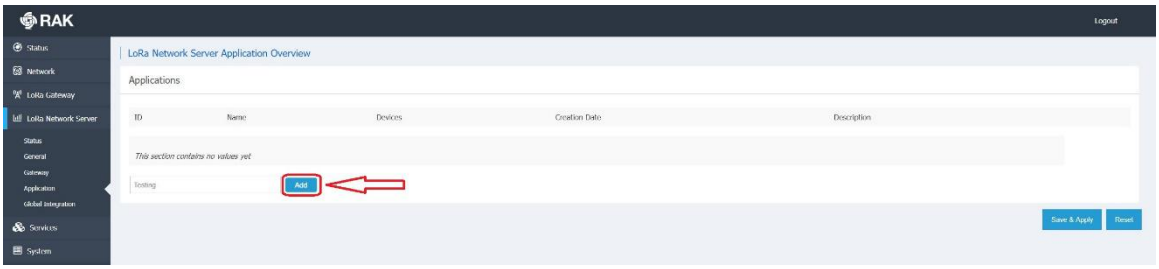

***Figure 19** | NS Application*

The first time you access the menu it will have no applications listed. Create one by Entering a name in the field and pressing the “Add” button

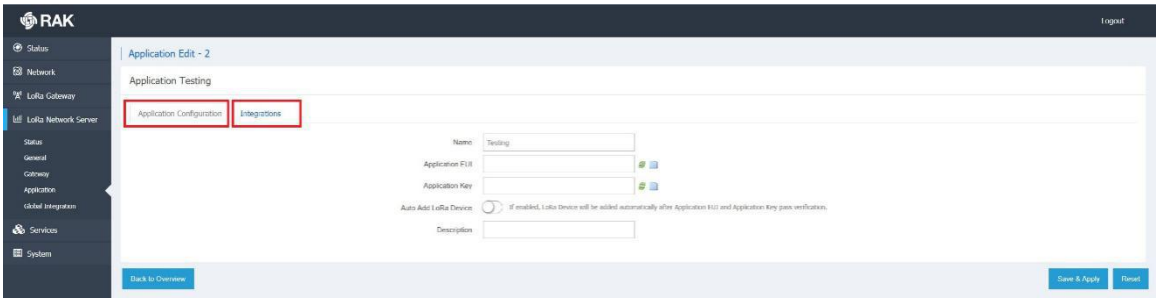

***Figure 18** | NS Application Configuration*

You will be automatically forward to the Application Edit screen. You have two tabs here, which are explained below:

Application Configuration

This is where you configure the parameters required to successfully create your application.

Name

A way of identifying it in the Built-in NS.

Application EUI

The *Application EUI* is a global application ID in IEEE EUI64 address space that uniquely identifies the entity able to process the JoinReq frame. Thus, you need one which you can either enter yourself (for example if you have copied it from TTN) or press the green button after the text field to generate a random one.

Application Key

The Key is used to generate the Application Session Key and Network Session Key in cause of using OTAA. As with the EUI you can either enter it itself or generate a random one.

Auto Add LoRa Device

This slider determines if the device will be automatically added if the application EUI and Key are valid.

Description

An optional field for entering information describing the Application.

Integrations

There is an option to have a HTTPS integration for your application. See Figure 19 for details:

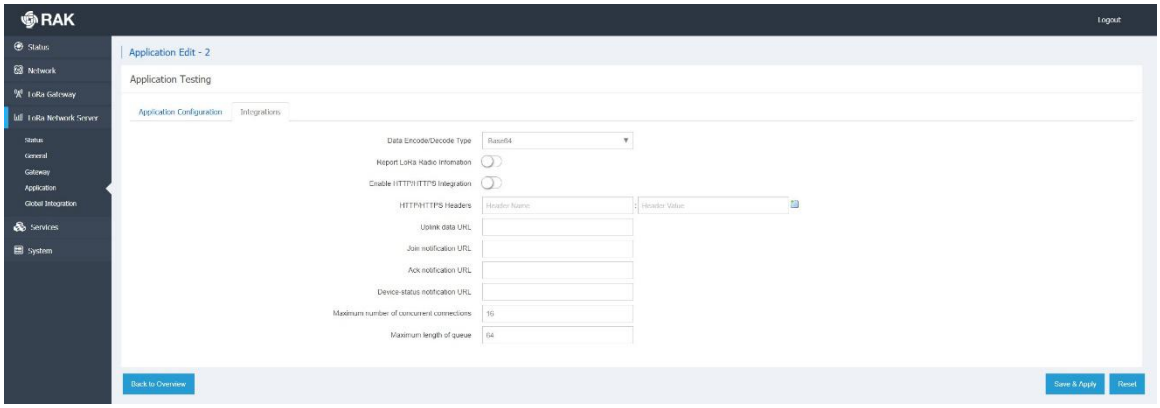

***Figure 20** | Application Integration Tab*

There are several fields that need to be filled in, starting with the Data Encoder/Decoder type (Base 64 or HEX String). Once selected you can Enable the functionality with the slider.

Afterwards make sure to fill the rest of the fields: HTTP/HTTPS Headers, Uplink data URL, Join notification URL, Ack notification URL, Device-status notification URL.

You can test the HTTP endpoint integration with a free service like https://webhook.site

Last but not least select a value for the Maximum number of concurrent connections and the Maximum length of the queue (default values are 16 and 64 respectively).

One done with filling in the parameters “Save & Apply”.

Adding and configuring a device

Below is in depth explanation of the data available per device. You can enter this section by either inputting a valid EUI and pressing the *Add* button, or pressing the *Edit* button for an existing device:

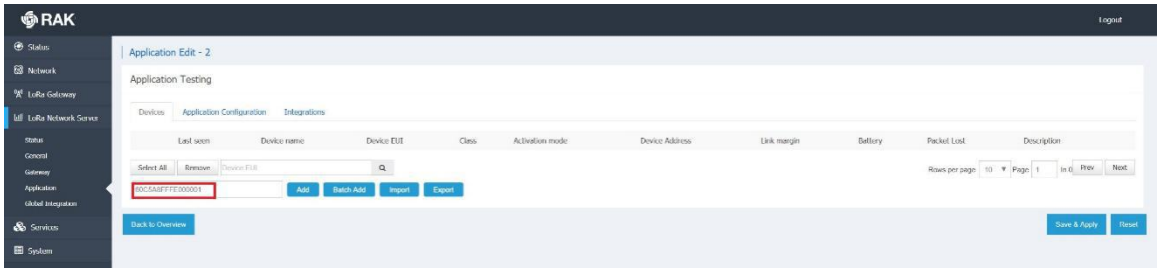

***Figure 21** | NS Adding a Device*

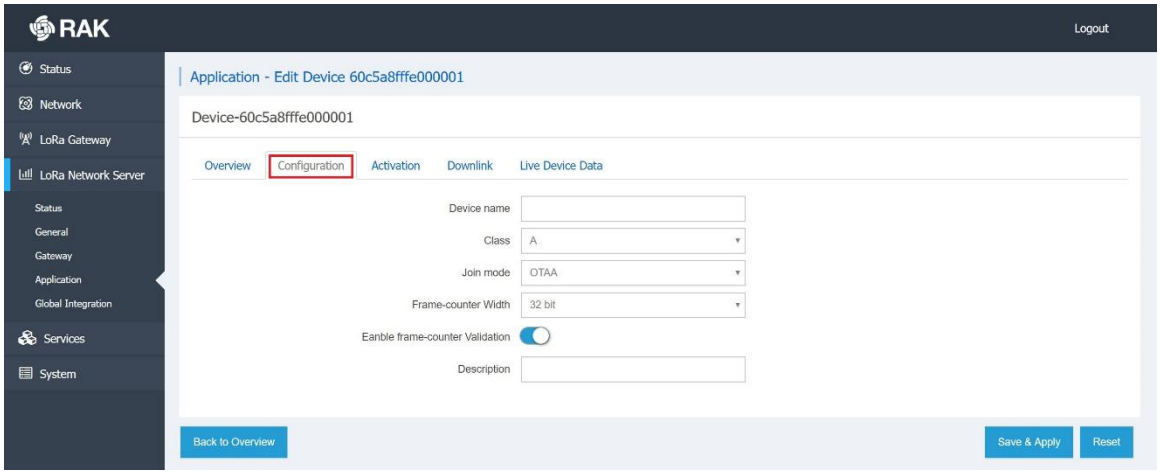

***Figure 22** | NS Device Configuration (OTAA)*

Overview

This page displays per device metrics. Things as RSSI, SNR and Traffic are displayed in a graph for the user's convenience

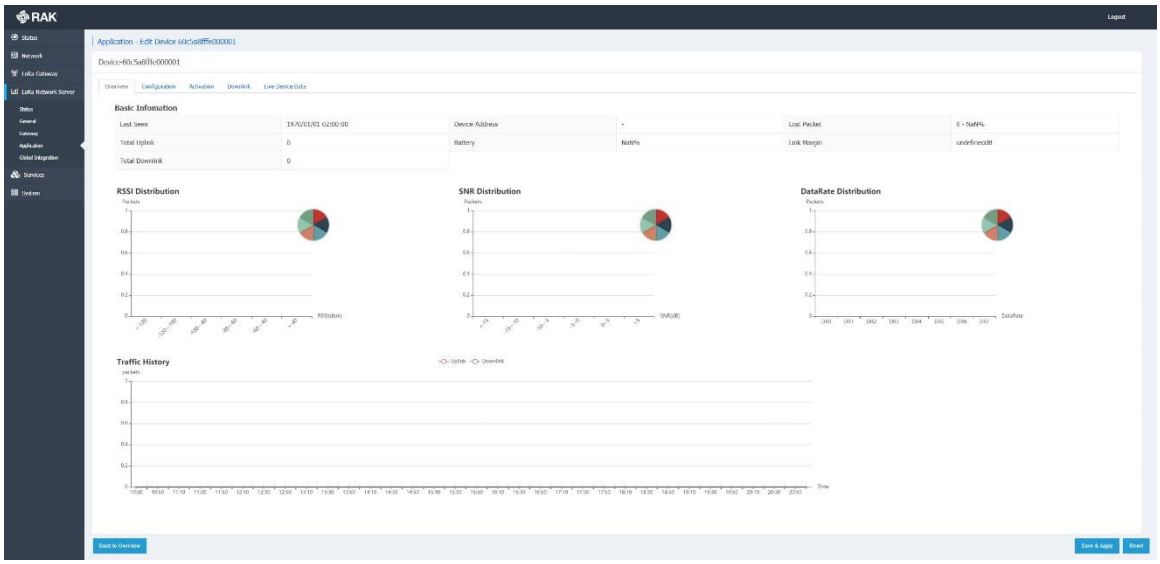

***Figure 23** | Device Overview page*

Configuration

Here you can edit device parameters as follows:

Name – does not need to match the EUI, batch loading results in a match by default

Class – both Class A and Class C devices are supported

Join Mode – both OTAA and ABP are supported

Frame counter width – 32 or 64 bits

Enable frame-counter Validation – turn the counter on or off with the slider

Description – optional explanation

If you choose Join mode to be ABP you have to additionally enter the Device Address, Application Session Key, Network Session Key (optionally you can generate random ones). Refer to Figure 21 if you want to see how the window changes with ABP mode.

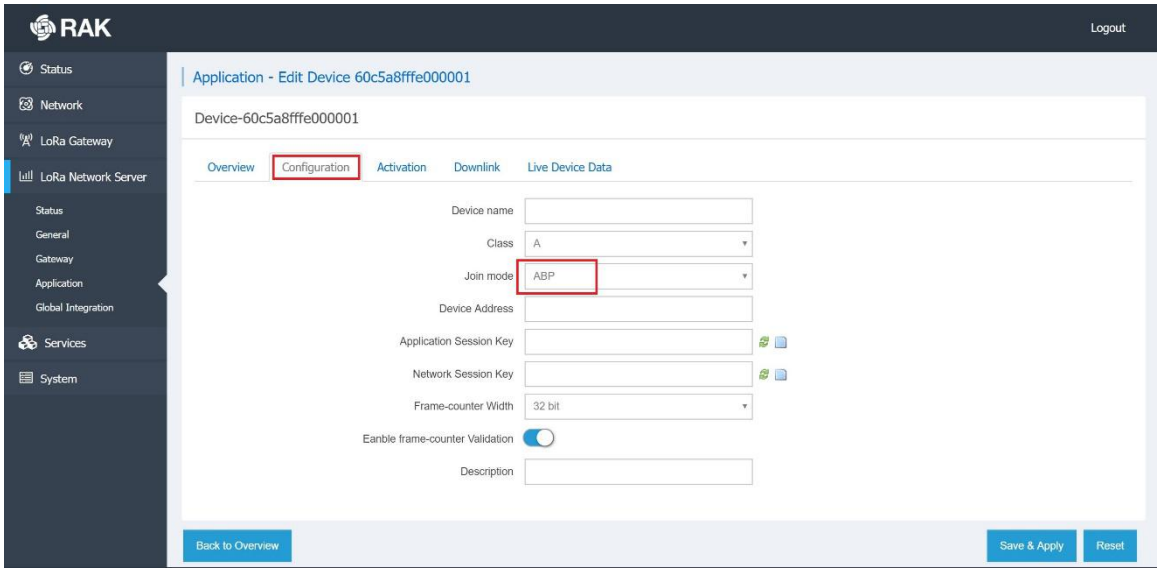

***Figure 24** | NS Device Configuration (ABP)*

Activation

Once you have properly configured the parameters of the device mentioned above you should see the data in the following picture (Activation tab):

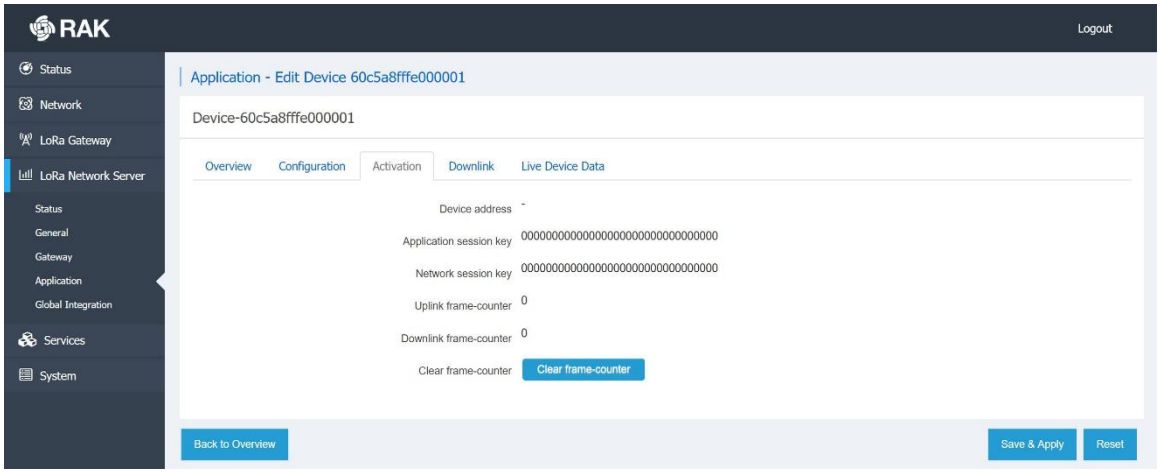

***Figure 25** | NS Device Activation*

Device Address – The field is generated automatically and displays the address assigned to the node. This is how you distinguish devices in the LoRa Packet Logger.

Application session key – The key assigned to the device upon OTAA Activation, or the one input manually if ABP is used.

Network session key – Same as for the Application Session Key

Uplink frame-counter – The number of messages that have been received by the Gateway since the device activation

Downlink frame-counter – The number of messages the Gateway has sent to the node

Downlink

You can send a downlink frame with this tool. The slider determines if the frame is Confirmed or Unconfirmed. You need to enter the number of the Frame Port (Fport) and a payload in HEX format. The downlink will be transmitted in the next Rx window in case of Class A for example.

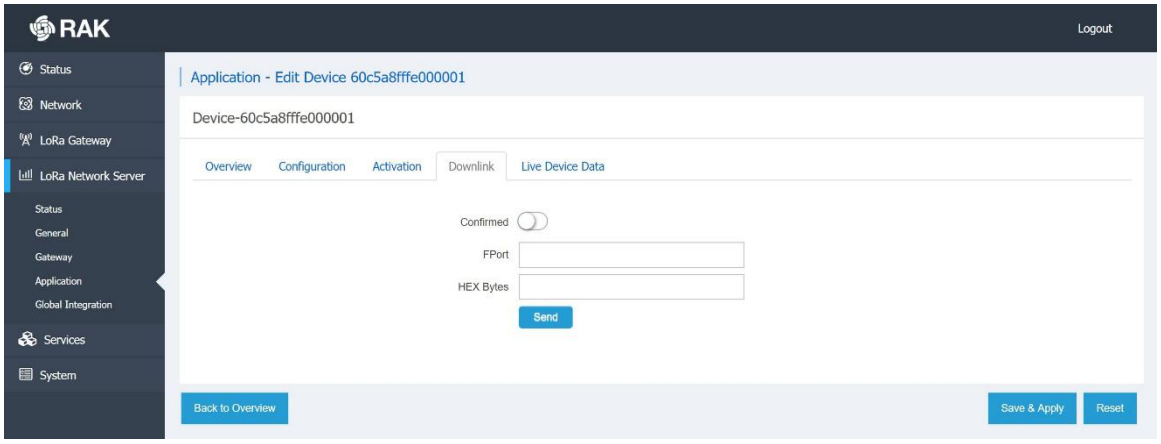

***Figure 26** | NS Device Downlink*

Live Device Data

You can see the packets for the selected devices in real time in this section.

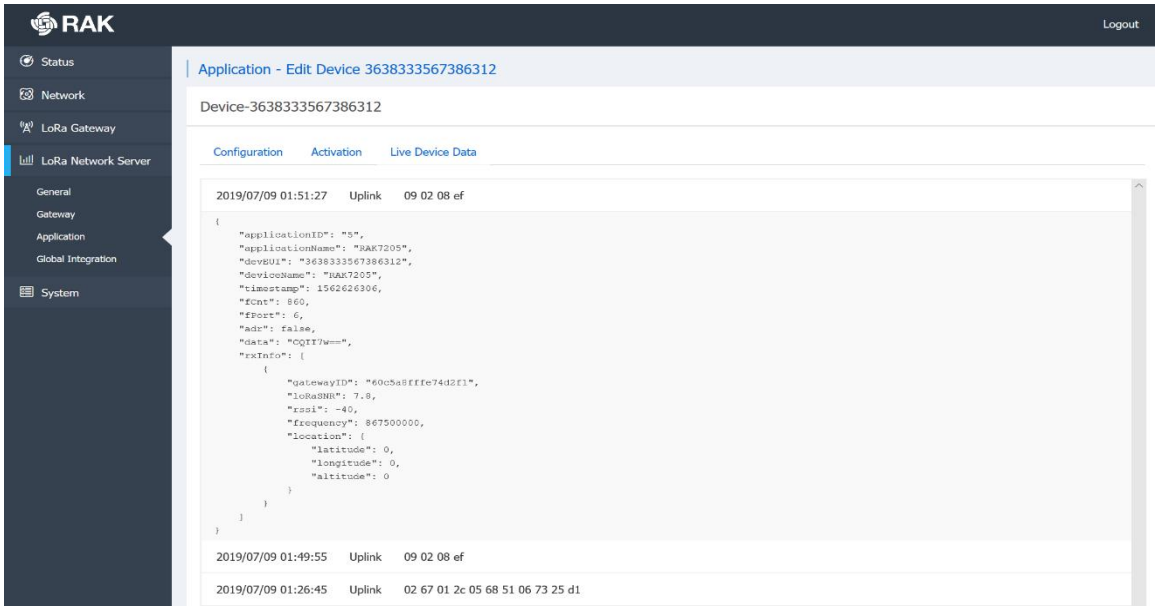

***Figure 27** | NS Device Live Data*

3.4.5 Global Integration

This feature allows for integration of the Built-in LoRa Application Server with an External MQTT broker.

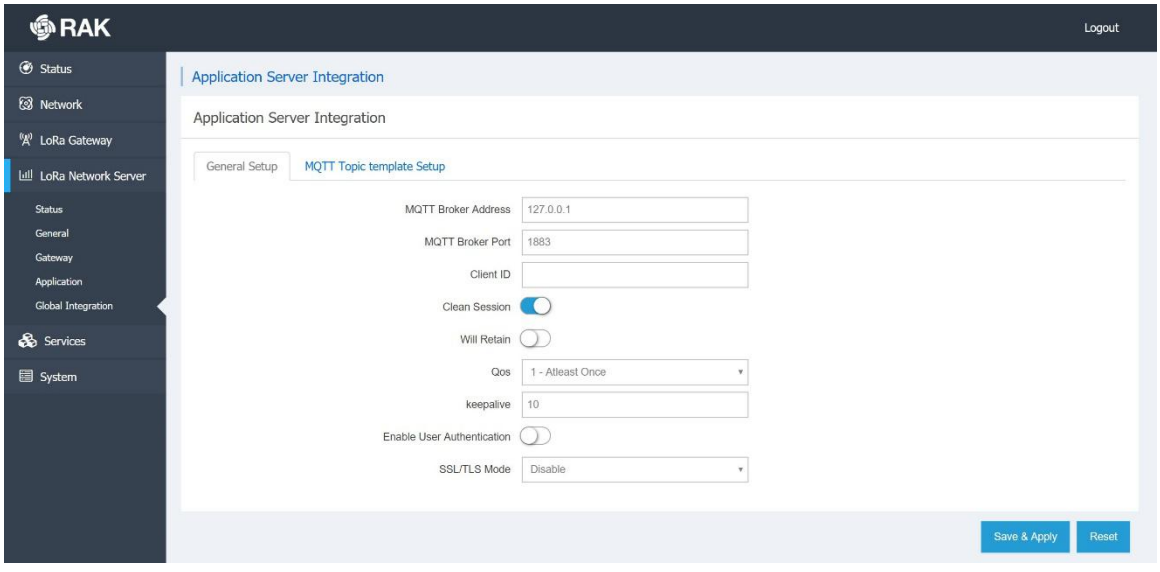

***Figure 28** | NS Global Integration*

General Setup

MQTT Broker Address – the IP Address of the external MQTT broker

MQTT Broker Port – the Port of the external MQTT broker

Client ID – the Client ID

Clean Session – a slider that determines if you will start fresh when the integration runs

Will Retain – a slider for data retention

QoS – the service level (Almost/At least/Exactly once)

Keep Alive – the Keep Alive interval is seconds

Enable User Authentication – a slider to enable/Disable Authentication

In addition to setting an Username and Password, there is a drop-down menu for the SSL/TLS Mode (Disabled by default). The following certificates are supported: *CA Signed server certificate, Self-signed server certificate, Self-signed server & client certificate*

MQTT Topic Template Setup

Here you can get information on the topic templates: *Join Topic, Uplink Topic, Downlink Topic, Ack Topic.*

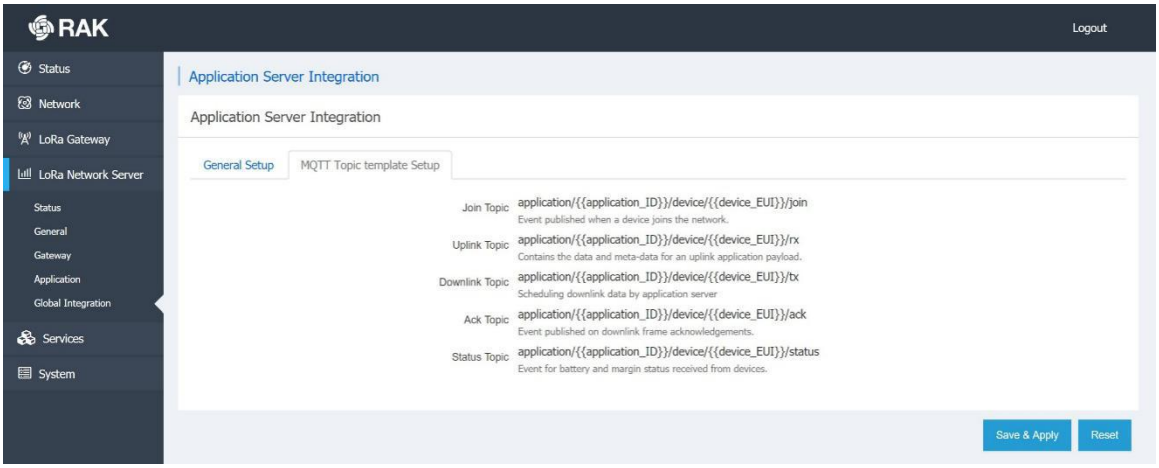

***Figure 29** | NS Global Integration MQTT Topic Template*

3.5 System

This is the place where you configure general device parameters.

3.5.1 System

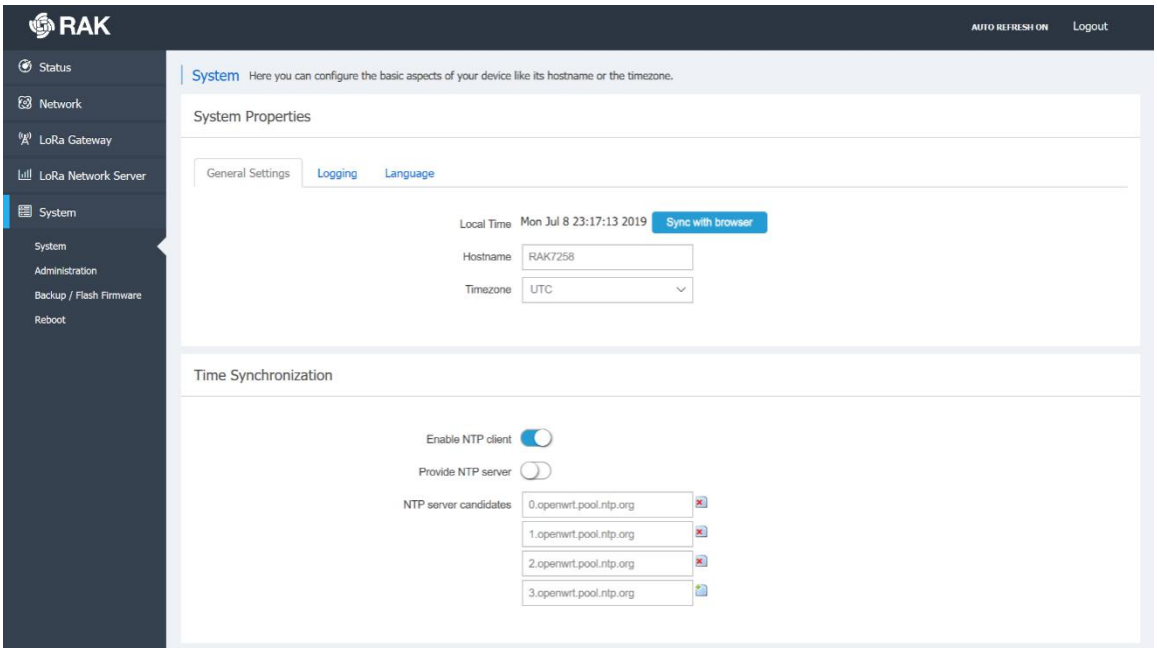

***Figure 30** | System Tab*

General Settings

The system time is displayed here. Additionally you can edit the Host Name and select the Time zone.

Another way to get the correct time is to use Timing Synchronization. You can Enable NTP client mode, enable NTP server and provide server candidate URLs.

Note that the Time Synchronization tab is displayed in all System submenus.

Logging

In case you want to keep a log of system events you can configure how this is done here:

You can set the Buffer size, provide the IP Address and port of an External log server, and set the Log Level.

Language

By default, this is in Auto (English), however you can choose from several options including German, Spanish, Russian, etc.

3.5.2 Administration

This is where you change the administration password of the device.

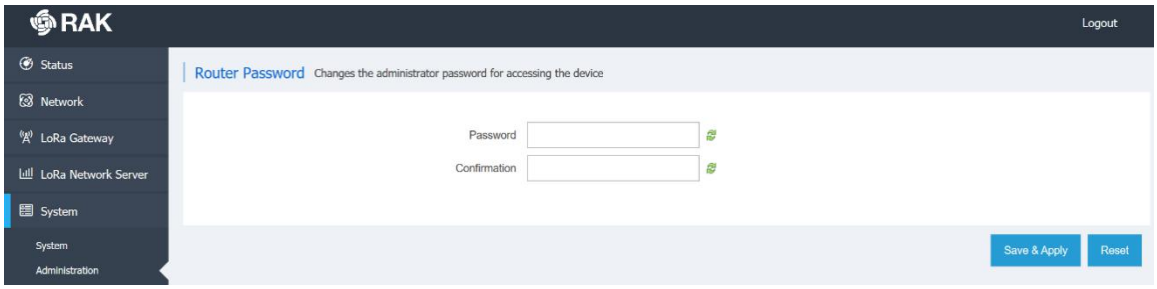

***Figure 31** | Administration Tab*

3.5.3 License

This is the status of your license. You can see the Type, Number of Supported Nodes, Expiration date, and the Number of External Gateways Supported. There is a field to ender the License data in case you are upgrading.

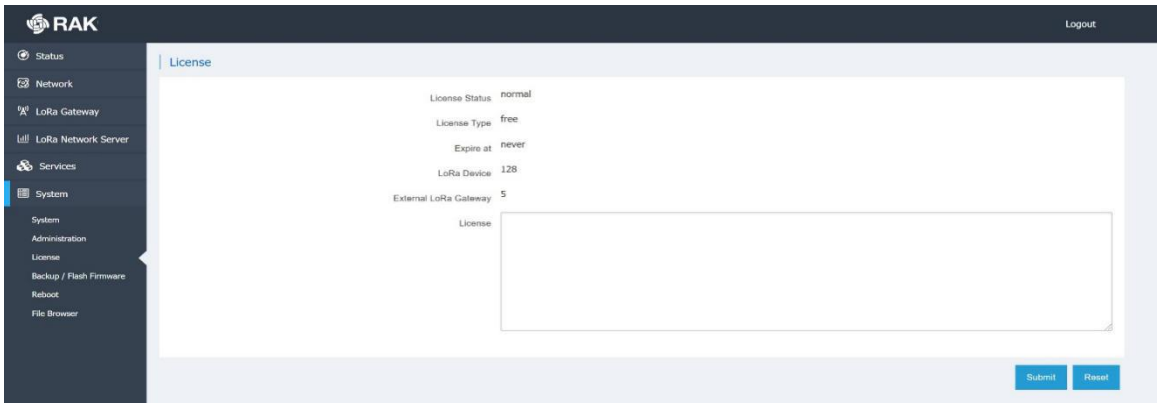

***Figure 32** | License Tab*

3.5.4 Backup / Flash Firmware

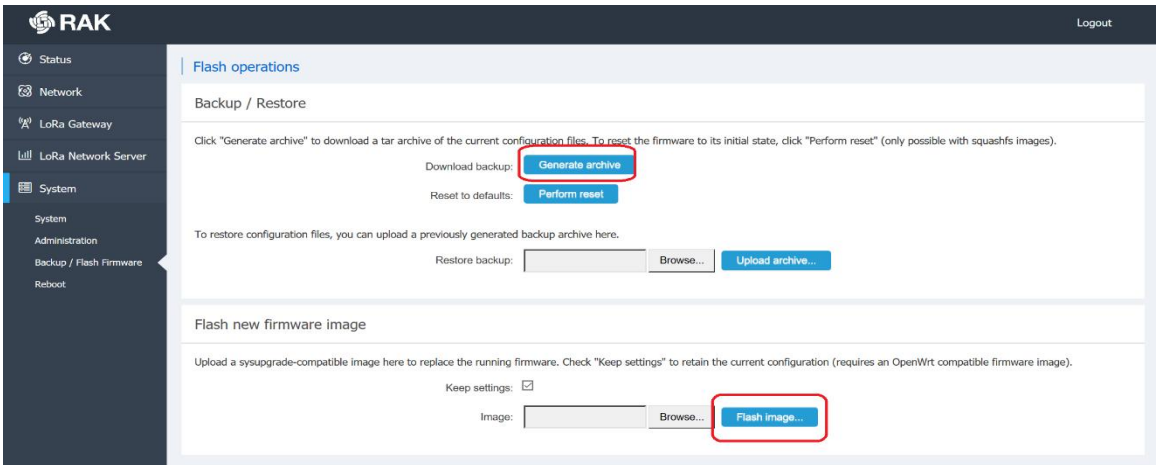

***Figure 33** | Backup Tab*

Generate archive – downloads an archive of the current configuration

Perform reset – resets the Gateway to the default settings

Restore – you can upload a previously generated archive to restore the configuration settings at the time of its making

Flash new firmware – update the firmware by flashing a *bin* file. Use the button to select the location of the new firmware file and the blue button to initiate the flashing process. There is a tick box to toggle the option of keeping the current settings of the gateway.

Note it is selected by default as unchecking it will results in having a gateway with stock settings after the firmware update.

3.5.5 Reboot

Reboots the gateway. All unsaved changes will be discarded. This is not a reset in any way and only power cycles the device. All configuration settings will be left intact.

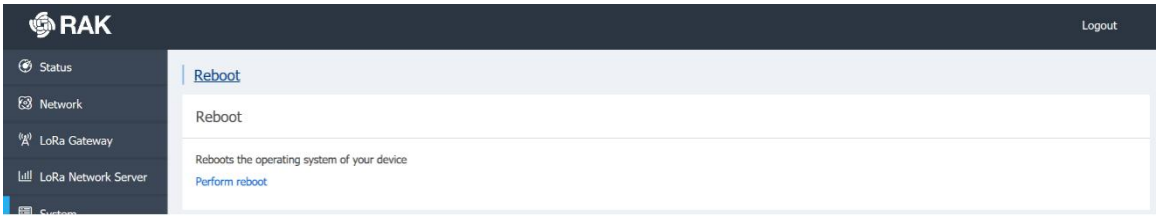

***Figure 33** | Reboot Tab*

Please contact us if you need technical support or want to know more information.

Support center: https://forum.rakwireless.com/

Email us: info@rakwireless.com

4 Appendix – LoRa Network Server Global Integration Interface API(Topic definition and Data Format)

Built-in LoRa Network Server supports integration to the user's application server through MQTT protocol.

MQTT messages are published automatically when the following events occur:

join – When OTAA request occurs to LoRa node

uplink – When LoRa node sends uplink message

ack – When the downlink message pushed by the application server receives the confirmation message

status – When LoRa node status is updated (information such as battery capacity / Link margin)

Built-in LoRa Network Server will subscribe to the downlink topic, so the third-party application server should publish messages to the topic. After receiving the message, LoRa network server will push the downlink message to the LoRa node.

The topic and message payload format are defined as follows:

Event type	join
	Event published when a device joins the network.
Topic	application/[applicationID]/device/[devEUI]/join

Example	{
	"applicationID": "123",
	"applicationName": "temperature-sensor",
	"deviceName": "garden-sensor",
	"devAddr": "06682ea2", // assigned device address
	"devEUI": "0202020202020202" // device EUI
	}

Event type	uplink
	Contains the data and meta-data for an uplink application payload.
Topic	application/[applicationID]/device/[devEUI]/rx

Example	{
	"applicationID": "123",
	"applicationName": "temperature-sensor",
	"deviceName": "garden-sensor",
	"devEUI": "0202020202020202",
	"rxInfo": [
	{
	"gatewayID": "0303030303030303", //ID of the receiving gateway
	"name": "rooftop-gateway", // name of the receiving gateway
	"time": "2016-11-25T16:24:37.295915988Z", // time when the package was received (GPS time of gateway, only set when available)
	"rssi": -57, // signal strength (dBm)
	"loRaSNR": 10, // signal to noise ratio
	"location": {
	"latitude": 52.3740364, // latitude of the receiving gateway
	"longitude": 4.9144401, // longitude of the receiving gateway
	"altitude": 10.5, // altitude of the receiving gateway
	}
	}
	],
	"txInfo": {
	"frequency": 868100000, // frequency used for transmission
	"dr": 5 // data-rate used for transmission
	},

	"adr": false, // device ADR status "fCnt": 10, // frame-counter "fPort": 5, // FPort "data": "..." // base64 encoded payload (decrypted) }

Event type	ack
	Event published on downlink frame acknowledgements.
Topic	application/[applicationID]/device/[devEUI]/ack

Example	{
	"applicationID": "123",
	"applicationName": "temperature-sensor",
	"deviceName": "garden-sensor",
	"devEUI": "0202020202020202", // device EUI
	"acknowledged": true, // whether the frame was acknowledged or not (e.g. timeout)
	"fCnt": 12 // downlink frame-counter
	}

Event type	status
	Event for battery and margin status received from devices.
Topic	application/[applicationID]/device/[devEUI]/status
Example	{ "applicationID": "123", "applicationName": "temperature-sensor", "deviceName": "garden-sensor", "devEUI": "0202020202020202",

	"battery": 200, "margin": 6, "externalPowerSource": false, "batteryLevelUnavailable": false, "batteryLevel": 75.5 }

When a third-party server needs to send a downlink message to a LoRa node, you should publish the message to the downlink topic in the following format:

Event type	downlink
	Scheduling downlink data by application server
Topic	application/[applicationID]/device/[devEUI]/tx

Example	{
	"confirmed": true, // whether the payload must be sent as confirmed data down or not
	"fPort": 5, // FPort to use (must be > 0)
	"data": "...." // base64 encoded data (plaintext, will be encrypted by LoRa Server)
	}

Note:
All messages are in JSON format. The data field contents in the uplink and downlink messages are in base64 encoding format.

5 Revision History

Revision	Description	Date
1.0	Initial Release	2019-04-02
1.1	Add the LoRa Gateway MQTT Bridge Configuration	2019-04-03
1.2	Add Customize the Channel and MQTT Bridge Chapter	2019-04-23
1.3	Add LoRa Network Server Chapter. Remove Frequency channel settings and MQTT Bridge Chapter (will be in separate documents)	2019-05-31
1.4	Addition of new features set	2019-06-16
1.5	Features update for new Firmware	2019-07-22
1.6	Features update for new Firmware	2019-10-15
1.7	Features update for new Firmware	2019-10-28

6 Document Summary

Prepared by	Checked by	Approved by
Penn, Vladislav	Vladislav	

About RAKwireless:

RAKwireless is the pioneer in providing innovative and diverse cellular and LoRa connectivity solutions for IoT edge devices. It's easy and modular design can be used in different IoT applications and accelerate time-to-market.

For more information, please visit RAKwireless website at www.rakwireless.com.