February 2020

SAFEGUARDING AGAINST IMPROPER CONFIGURATIONS FOR LORAWAN GATEWAYS

Su Xia

Christine Hwang

Bob Lo

Xiaochen Cao

Simarpreet Kaur

SAFEGUARDING AGAINST IMPROPER CONFIGURATIONS FOR LORAWAN GATEWAYS

AUTHORS:

Su Xia
Christine Hwang
Bob Lo
Xiaochen Cao
Simarpreet Kaur

ABSTRACT

Presented herein are safeguard features for Long Range wide-area network (LoRaWAN) deployments on a LoRa gateway. The techniques presented herein provide a solution to prevent end users from wrongly or accidentally deploying LoRa gateways in unlawful Industrial, Scientific and Medical (ISM) radio bands. The techniques presented herein require little computational and storage resources to be integrated into any LoRa gateway embedded system, operate automatically based on the standard LNS protocol, and are sufficiently flexible to suit different use cases.

DETAILED DESCRIPTION

LoRa gateways for LoRaWAN supports the LoRa™ physical layer technology and complies with the LoRaWAN specification to provide Low Power Wide Area wireless connectivity for low data rate, battery-powered devices and sensors through the unlicensed sub-GHZ ISM radio bands. Figure 1, below, illustrates a typical setup of a LoRaWAN network.

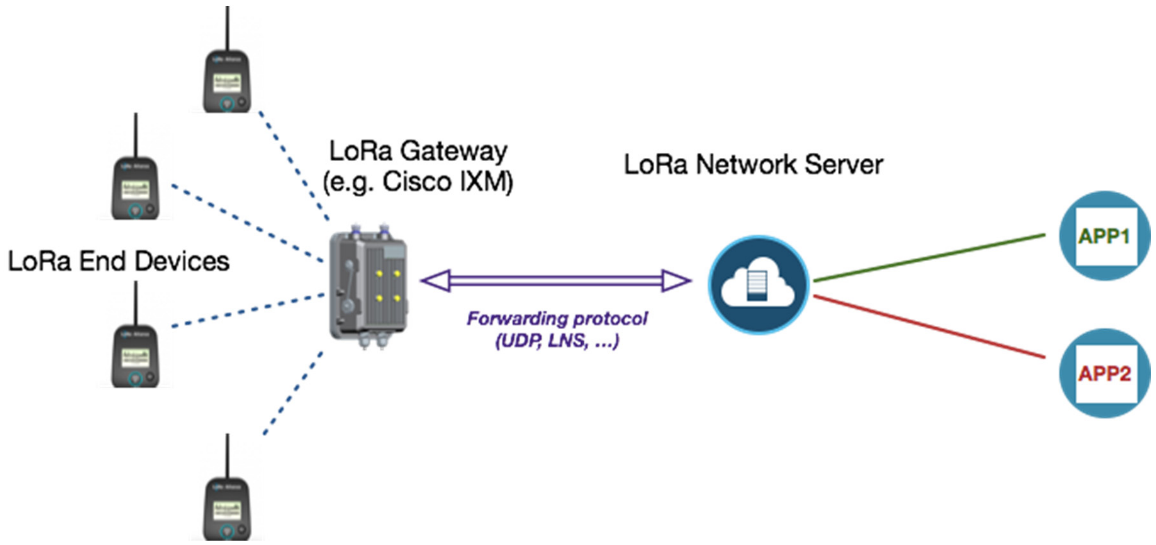


Figure 1. LoRaWAN with LoRa Gateway

A LoRa gateway requires proper configurations in order to both control local LoRa radio hardware and interact with the LoRa NS at the backend. These configurations can be classified into two categories:

- Static, platform dependent configurations (such as radio TX Look Up Table - TX LUT).
- Dynamic, platform independent and user-controlled configurations (such as the channel plans, i.e. frequency allocation).

Generally, platform dependent configurations could be well controlled by gateway vendors and are rarely exposed to the end user. On the other hand, the platform independent configurations are vulnerable to error and abuse. The fact that LoRa gateways operate in ISM radio bands worldwide complicates the scenario, since each country/region has different rules and regulations for devices using ISM bands.

The techniques presented herein address these issues by providing a “safeguard” layer to end users that prevents improper configurations, which in turn could lead to violations of local regulations and legal disputes.

Terminology:

- LoRa - Stands for Long Range, which is based on spread spectrum modulation techniques derived from chirp spread spectrum (CSS) technology.
- LoRaWAN - A low power, wide area networking (LPWAN) protocol based on LoRa technology.
- LNS - Stands for LoRa Network Server, which takes the LoRa packets from end devices and distributes them to applications. Also, it controls end LoRa devices and LoRa gateways through LoRa MAC commands and protocols.
- LoRa Packet Forwarder - An agent running on a LoRa gateway, forwarding RF packets received by LoRa radio hardware to a LoRaWAN Network Server and transmitting RF packets sent by the LNS to end LoRa devices.
- LoRa UDP Packet Forwarder (UPF in short) - The legacy LoRa Packet Forwarder using UDP/IP as network layer and operating based on a basic communication protocol between LoRa gateway and LNS (udp packet forwarder protocol, UPF protocol in short).
- CPF- Stands for Common Packet Forwarder, which is a new generation of LoRa Packet Forwarder supported on certain LoRa gateways. CPF is based on the implementation of "basic station," which enables certain LoRaWAN gateways to operate as open platforms.
- LNS Protocol - The protocol running between a LoRa gateway and the LoRa Network Server in CPF, which includes the LNS discovery, authentications, gateway configurations, uplink and downlink data interactions, synchronization.
- Channel Plan - A set of frequency and bandwidth combinations along with some other LoRa specific parameters, such as Spreading Factor (SF), where the gateway's radio operates on. The LoRa end devices communicates with the gateway on these channels.

After the LoRa gateway starts the packet forwarder, it takes the configurations, programs the LoRa radio, then starts relaying the LoRa packets. The configurations may come from:

- One configuration file (local or downloaded from remote server), which contains both platform dependent and independent parameters.
- One local configuration file, containing only platform dependent parameters, while the platform independent parameters are from LNS. CPF, as the state-of-art LoRa Packet Forwarder, uses this method.

On the LoRa gateway, only limited sanity checks are performed when configurations are received. For example, while applying the radio configurations to the RF hardware, the gateway only checks whether those parameters are beyond the hardware limits, such as bandwidth, frequency, etc.

Some variants of packet forwarders, which are mostly proprietary to their own LNS vendors, often use a different approach. For example, for the packet forwarder, long range relay (LRR), the backend server takes control of everything and some validations and checks could be done when setting up the gateway. The LRR then needs to obtain the configurations from the server through side channels.

However, little has been done on the gateway side to validate the configurations before setup of the radio hardware. Verification at this stage is even more critical due to the fact that:

- The gateway is the last chance to check against improper configurations before turning on the radio.
- The gateway has the most accurate local information, such as locations, channel qualities, which are important for some of the configurations.
- The gateway is neutral to the backend LNS. Any implementation of LNS complying with the LoRa specifications could interact with the gateway. It is not safe to assume that backend server would always provide the correct parameters for the gateway. Doing everything on the LNS side still leaves the gateways vulnerable to misconfigurations or malicious attacks, especially when gateways need to interact with LNS from different vendors.
- Since LoRa gateways operate in a broad range of ISM radio bands, there are an enormous number of feasible channel plans. Furthermore, a LoRa radio covers a much wider area (in terms of miles) compared to other low power wireless

techniques (e.g., WIFI, 802.15.4) running on the ISM bands. As such, it is very critical for the LoRa gateway to strictly comply with the local ISM radio regulations. It is also necessary for end users to have a simple automated mechanism to safeguard against invalid channel plans.

The so-called “safeguard” techniques presented herein include two key parts, referred to as “Localization” and “Validation.” Localization utilizes the GPS modules on the LoRa gateways to identify the resident country/region, which is suitable for the outdoor deployment. GPS localization (reverse geocoding) usually is done through online map services, which require Internet access and have limits on the number of queries per day. However, this method cannot be used in gateways located in air gapped LoRa networks or austere locations with limited Internet access. Accordingly, an offline localization method is adopted here.

Given the limited storage and computation resources on gateways, a lightweight localization algorithm and condensed GPS database footprint (~3 to 4 MB compressed) [CH(1]is used instead to achieve comparable accuracy to the Internet-based map services. The GPS database stores boundary landmarks (longitude and latitude coordinates) of each country/region. Given a point with GPS coordinates, the system finds the boundary landmark with the closest distance, of which resident region/country is in. Note that the landmarks in GPS database are partitioned into smaller areas according to their coordinates, so that it only needs search a handful of point sets for the closest landmark. The overall procedure is shown in Figure 2, below.

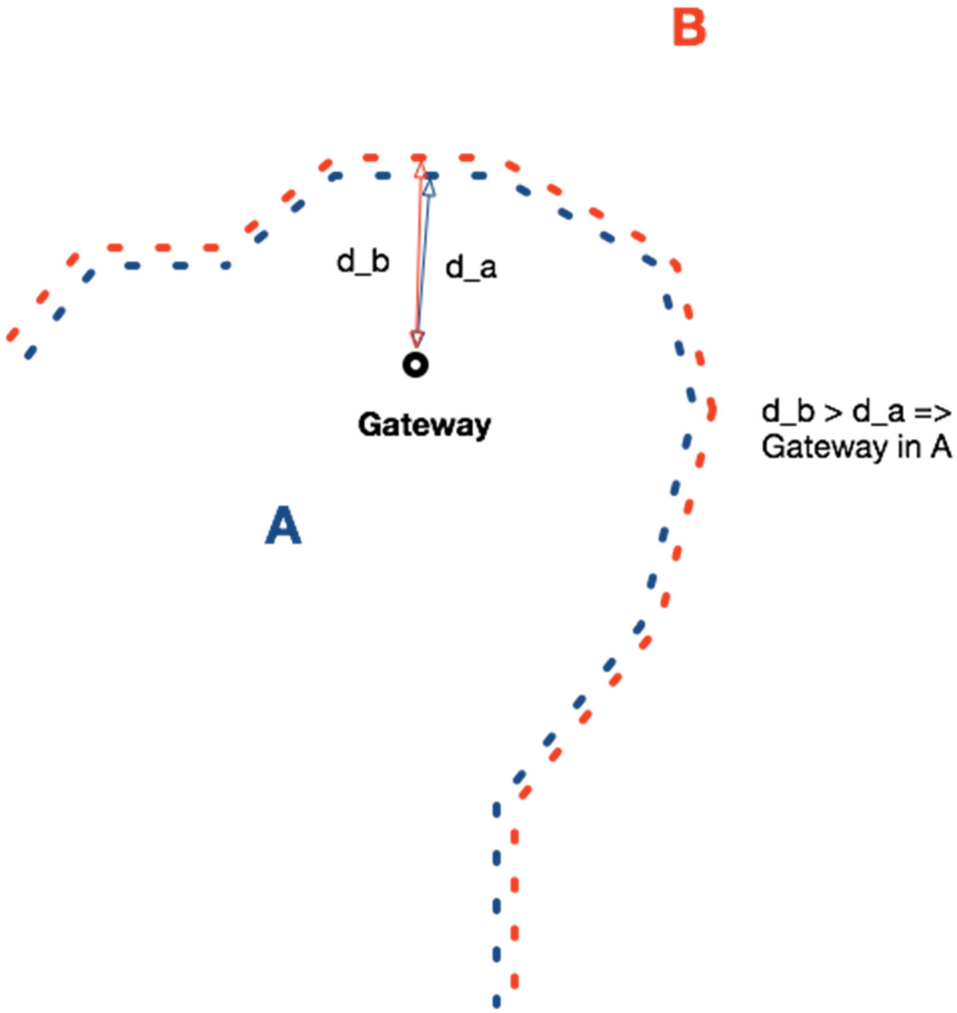


Figure 2. Offline Reverse Geocoding (Localization)

Validation of configuration uses the result of the gateway localization process, as explained above. First, a Region/Country Rule Database has been created to collect all the constraints for a LoRa gateway to use the ISM radio bands in each region/country. The Region/Country Rule Database consists of:

- All available LoRa Multi-SF band, in format of <*center freq, bandwidth, min_SF, max_SF*>.
- All available LoRa standard band, in format of <*center freq, bandwidth, SF*>.
- All available LoRa FSK band, in format of <*center freq, bandwidth, bit_rate*>.

- Max EIRP.

The checking criteria can be expanded as needed. When a packet forwarder on a gateway takes configurations, the packet forwarder validates each applicable configuration with the *Region/Country Rule Database* before applying all the configurations to the radio hardware. The validation passes only if all of the configurations do not violate the checking criteria. If one or more configurations do violate the checking criteria, then the packet forwarder rejects the configurations and prompts a user with an error message, thereby preventing the gateway from operating with improperly assigned configurations (e.g., improper radio frequencies, bandwidth, etc.).

The following illustrates how the safeguard techniques presented herein can be integrated into the CPF on a LoRa gateway. Similar procedures can be used to integrate this feature into other packet forwarders on LoRa gateways.

Figure 3, below, illustrates a series of stages used to start up CPF on an example LoRa gateway.

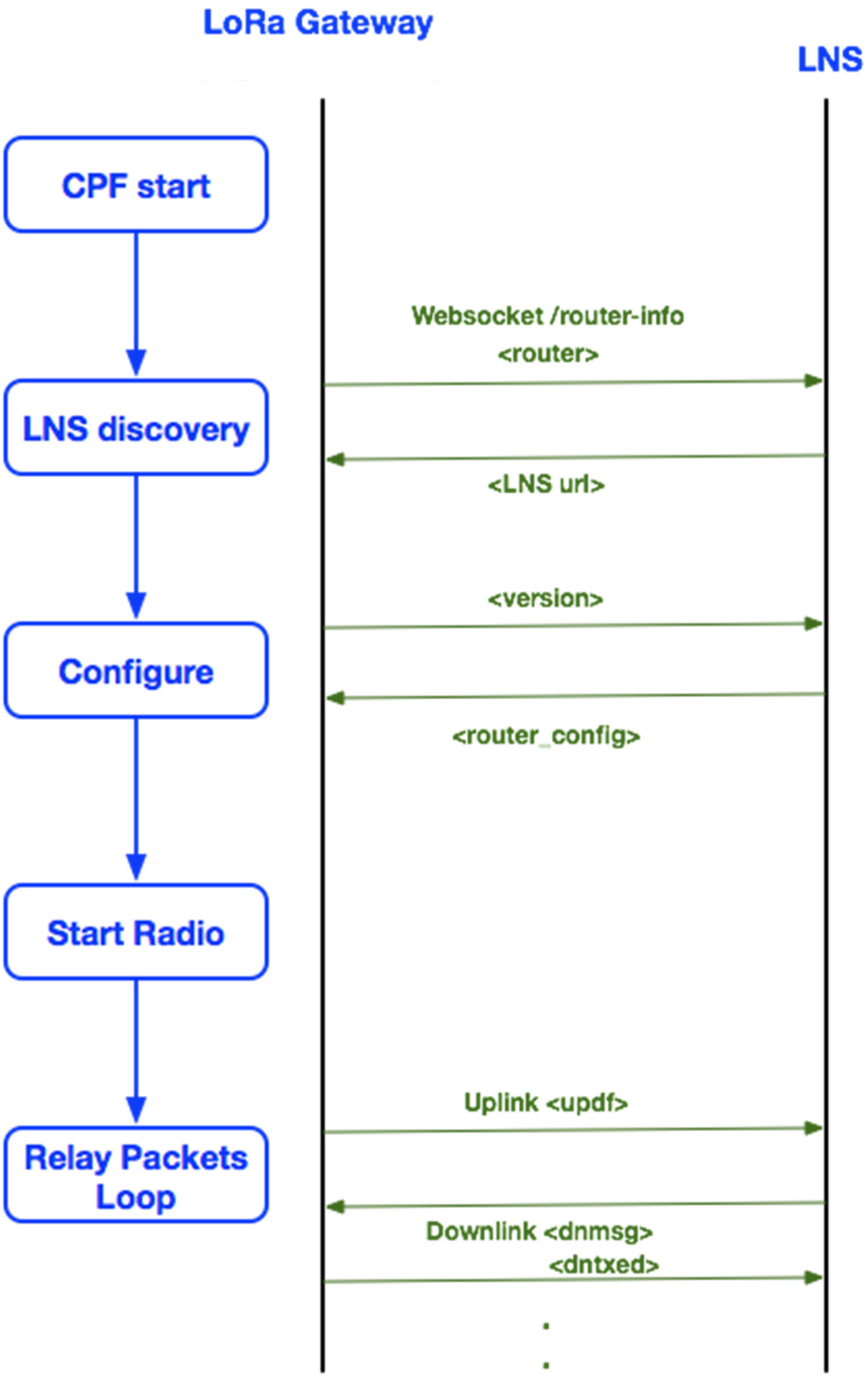


Figure 3. Integration Example with CPF

Some additional procedures are introduced into the startup process shown above to implement the safeguards against improper configuration. As shown in Figure 4 below, the

Localization module periodically updates the location information based on the offline reverse geocoding method as explained previously.

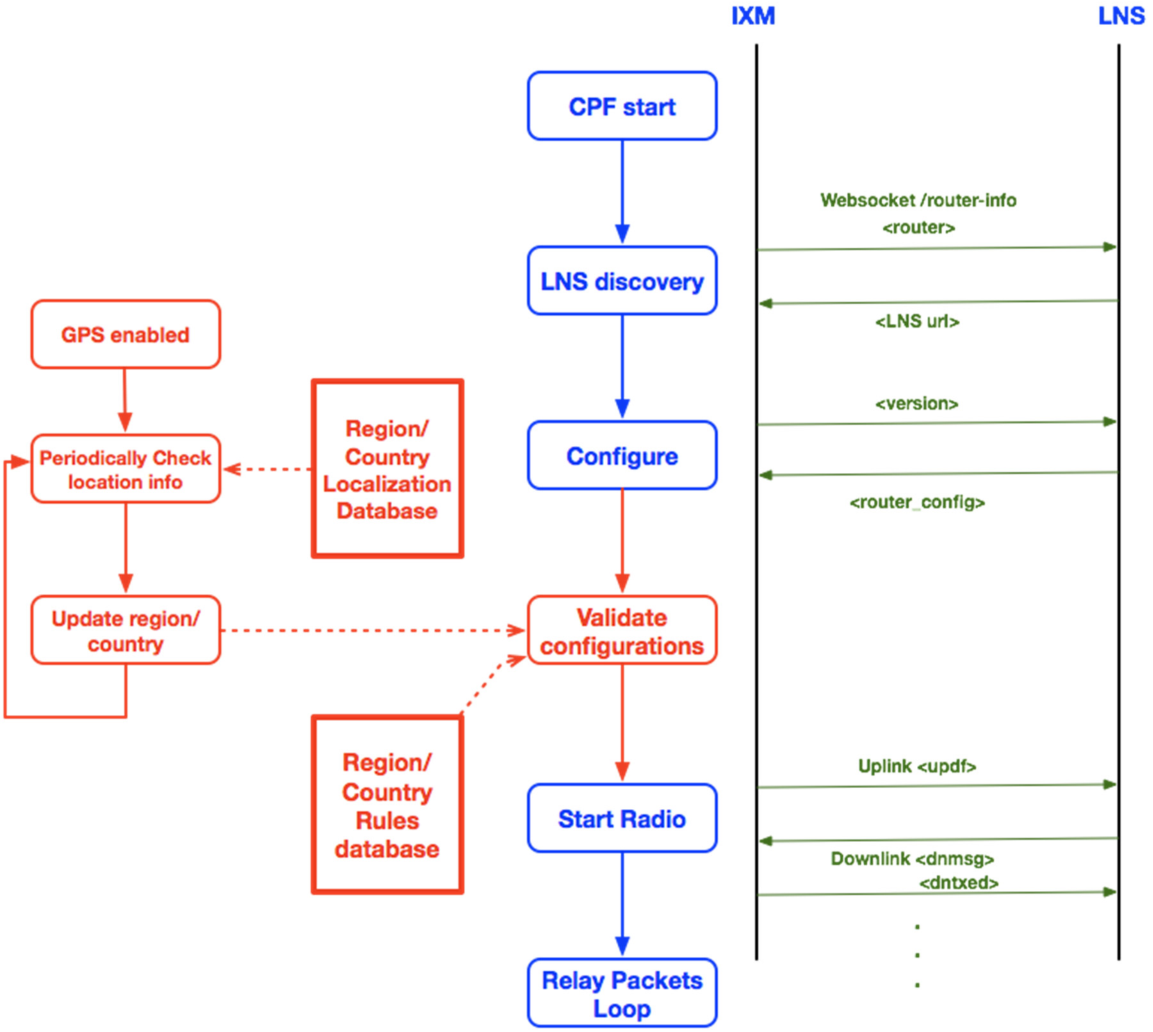
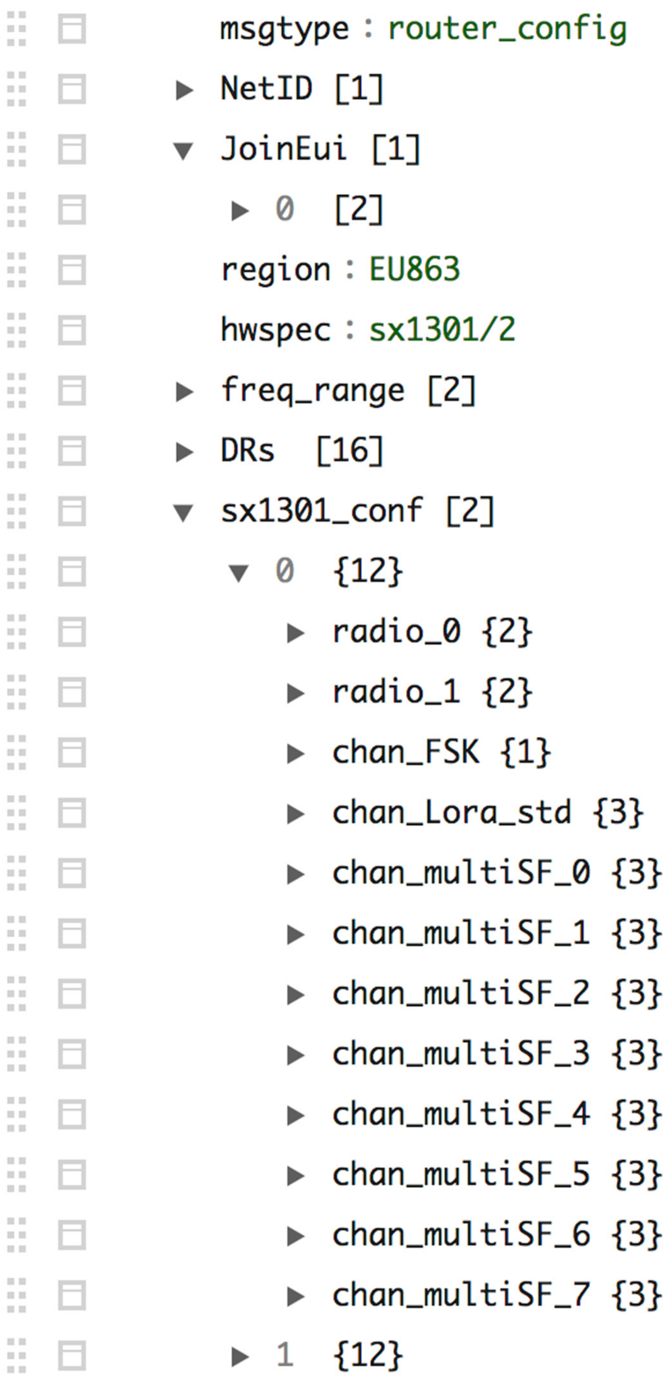


Figure 4. Integration Example with CPF

When the CPF interacts with the LNS and receives the <*router_config*> message (which is in JSON format as shown in Figure 5), it then parses the message and validates each radio band configuration with *Region/Country Rule Database* before programming to the radio hardware.



```
    msgtype : router_config
  ▶ NetID [1]
  ▼ JoinEui [1]
      ▶ 0  [2]
    region : EU863
    hwspec : sx1301/2
  ▶ freq_range [2]
  ▶ DRs  [16]
  ▼ sx1301_conf [2]
      ▼ 0  {12}
          ▶ radio_0 {2}
          ▶ radio_1 {2}
          ▶ chan_FSK {1}
          ▶ chan_Lora_std {3}
          ▶ chan_multiSF_0 {3}
          ▶ chan_multiSF_1 {3}
          ▶ chan_multiSF_2 {3}
          ▶ chan_multiSF_3 {3}
          ▶ chan_multiSF_4 {3}
          ▶ chan_multiSF_5 {3}
          ▶ chan_multiSF_6 {3}
          ▶ chan_multiSF_7 {3}
      ▶ 1  {12}
```

Figure 5. An Example of router_config Message in LNS

As noted above, the proposed safeguard features are flexible and can be switched on or off depending on different scenarios and practices. For example, the proposed safeguard features could be enabled for the formal deployment of LoRa Gateways or disabled for small area lab testing.