VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV MIKROELEKTRONIKY

DEPARTMENT OF MICROELECTRONICS

LORA GATEWAY

LORA GATEWAY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Matěj Očenášek

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Pavel Šteffan, Ph.D.

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Mikroelektronika**

Ústav mikroelektroniky

Student: Bc. Matěj Očenášek ***ID:*** 203309

Ročník: 2 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

LoRa Gateway

POKYNY PRO VYPRACOVÁNÍ:

V rámci diplomové práce navrhněte systém za využití technologie LoRa, který se bude skládat z koncového zařízení, gateway, serveru a uživatelského rozhraní. Koncové zařízení navrhněte tak, aby se skládalo z řídícího mikrokontroleru, LoRa modulu a senzoru, který bude sloužit jako zdroj přenášených dat. Součástí práce bude také popis, jak gateway správně připojit k serveru tak, aby skrze něj bylo následně možné na server přenášet data z koncového zařízení. Ověřte funkčnost navrženého systému.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 24.5.2022

Vedoucí práce: doc. Ing. Pavel Šteffan, Ph.D.

doc. Ing. Lukáš Fujcik, Ph.D.
předseda rady studijního programu

Abstrakt

Tato diplomová práce se zabývá realizací dvou systémů LoRaWAN a tvorbou návodu, jak tyto systémy uvést do provozu. Oba systému se skládají z koncového zařízení, přístupové brány, síťového a aplikačního serveru a webové stránky pro zobrazení získaných dat z koncového zařízení. Pro realizaci těchto dvou systémů je použita veřejná síť „The Things Network“ a lokální síť ChirpStack.

Klíčová slova

LoRa, LoRaWAN, LoRa gateway, LoRa Alliance, STM32, ISM pásmo, IoT, ChirpStack, TTN, koncové zařízení, přístupová brána

Abstract

This diploma thesis deals with the implementation of two LoRaWAN systems and the creation of instructions on how to put these systems into operation. Both systems consist of a end device, an access gateway, a network and application server, and a website to display the data obtained from the end device. The public network "The Things Network" and the local network ChirpStack are used to implement these two systems.

Keywords

LoRa, LoRaWAN, LoRa gateway, LoRa Alliance, STM32, ISM pásmo, IoT, ChirpStack, TTN, end device, access gateway

Bibliografická citace

OČENÁŠEK, Matěj. LoRa Gateway. Brno, 2022. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/142451. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav mikroelektroniky. Vedoucí práce doc. Ing. Pavel Šteffan, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	*Matěj Očenášek*
VUT ID studenta:	*203309*
Typ práce:	*Diplomová práce*
Akademický rok:	*2021/22*
Téma závěrečné práce:	*LoRa Gateway*

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně dne: 24. května 2022 ----------

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce doc. Ing. Pavlu Šteffanovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce.

V Brně dne: 24. května 2022 ----------

podpis autora

Obsah

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Úvod

Cílem této práce je návrh systému s využitím technologie LoRa/LoRaWAN. LoRa je technologie, která vznikla na začátku 21. století ve Francii, kde ji vyvinula společnost Cycleo. Jedná se o technologie dlouhého dosahu, a to v řádech jednotek kilometrů. Její vysílání je určeno pro ISM pásmo, což je pásmo rádiového vysílání pro vědecké, průmyslové a zdravotnické účely. Radiové vysílání na tomto pásmu je umožněno bez licenčních poplatků všem zařízením, které jsou pro toto pásmo homologované. Technologie LoRa v EU využívá pro vysílání a příjem frekvenční pásmo 868 MHz, tato frekvence spadá do frekvenčního rozsahu ISM pásma. Je tedy možné vysílat bez licenčních poplatků. U společnosti Cycleo, která je autorem technologie LoRa, došlo následně k akvizici společností Semtech.

Tato práce se zabývá koncepcí, návrhem a realizaci dvou systémů využívající technologii LoRaWAN. Jeden ze systémů je založen na síti TTN, což je mezinárodní virtuální síť. Druhý je založen na lokální síti ChripStack. Oba systémy se skládají ze čtyř hlavních bloků, a to koncového zařízení, přístupové brány, síťového a aplikačního serveru a externí uživatelské webové stránky pro zobrazení dat z koncového zařízení. Koncové zařízení bude osazeno celkem třemi různými LoRa moduly, řízení pak bude realizováno mikrokontrolérem STM32. Toto zařízení je možné napájet z přenosných zdrojů elektrické energie. Využití tří různých modulů je z důvodu, aby bylo možné v budoucnu návrh DPS využít i v případě, bude-li ukončena sériová výroba některého z nich. Na DPS koncového zařízení se bude nacházet také senzor teploty, sloužící jako zdroj přenášených dat skrze LoRa moduly. Pro realizaci samostatné přístupové brány pro oba typy sítí je využit komerčně dostupný router od společnosti Mikrotik.

Cílem této práce není pouze realizace dvou fungujících systému, ale také podrobný návod pro případné zájemce o využívání LoRaWAN sítě pro své vlastní domovní aplikace. Práce může taktéž sloužit jako pomocný materiál k realizaci vlastního podnikatelského záměru. Motivací této práce je nedostatek veřejně dostupných dostatečně kvalifikovaných informací o tom, jak si vytvořit svůj vlastní LoRaWAN ekosystém, ke kterému by bylo možné připojit senzory využívající technologii LoRa.

1. TEORETICKÁ ČÁST

Teoretická část se zabývá popisem dostupných technologií pro Internet věcí a zároveň obecně popisuje, co to Internet věcí je. Popisuje a porovnává Technologie SigFox, NB-IoT a LoRaWAN, přičemž největší důraz klade na popis technologie LoRaWAN. U technologie LoRaWAN popisuje jak fyzickou, tak síťovou vrstvu, třídy, způsoby aktivace a obecnou architekturu sítě.

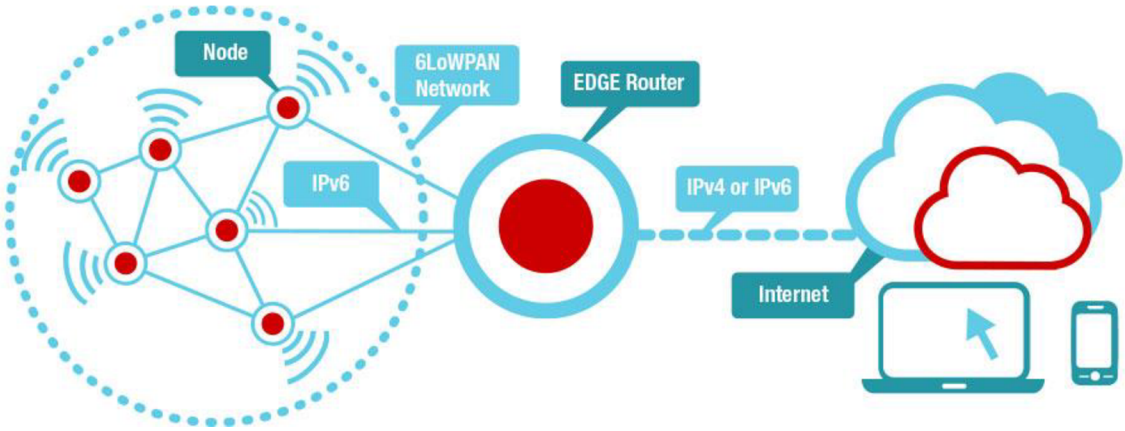
1.1 Co je to Internet věcí (IoT)

Jedná se o síť fyzických zařízení napříč různými segmenty, které jsou připojeny do jedné globální informační architektury na bázi internetu. Zařízení připojené do této sítě nachází využití v zemědělství, průmyslu, domácí automatizaci, ale také ve zdravotnictví, nebo v automobilovém průmyslu. Velikost trhu Internetu věcí je v roce 2022 odhadována na cca 29 miliard připojených zařízení. Hlavní iniciativou zmíněné sítě je bezpečné propojování různých zařízení, jež jsou využívaný během každodenních činností mezi sebou. Tato zařízení lze pak vzdáleně sledovat, či kontrolovat pomocí již existující infrastruktury, jako je počítačová síť. Díky možnosti ovládat zařízení v této síti roste efektivita (například výroby) a zároveň se snižují nároky na uživatele. [1]

Využití Internetu věcí přesahuje využití pouze v segmentu spotřebitelském a průmyslovém. Jedna ze zajímavých oblastí využití jsou městské infrastruktury, kdy je možné sledovat, vzdáleně řídit a regulovat systémy pro městskou dopravu, mosty, železniční přejezdy, elektrárny, hydranty, první pomoc a mnohé další. Velké množství větších měst proto často provozují vlastní lokální sítě, ke kterým jsou taková zařízení připojena. Tímto způsobem lze v rámci měst napomáhat k lepší efektivitě při plánování oprav, narušujících plynulost dopravy a zlepšení přenosu informací mezi dodavateli, nebo poskytovateli služeb. Systémy v této infrastruktuře mohou zlepšit řešení nehod a jiných mimořádných situací. Mimo tyto kritické situace svojí efektivitou napomáhají snížit náklady na obhospodařování těchto infrastruktur. Dostatečný velký objem těchto senzorů v rámci měst razantně zvýší jejich automatizaci a tím sníží nutnost zásahu člověka, snižuje se taktéž riziko chyby. [1]

Využití v segmentu jako zemědělství je pak primárně zaměřeno na sběr dat okolních podmínek, což jsou například: údaje o teplotě, vlhkosti, nebo rychlosti větru. Tyto a jiné informace pak napomáhají k automatizaci zemědělství, dále napomáhají snižovat ekonomická rizika. V oblasti správy energií mohou zařízení napomáhat optimalizovat spotřebu energie. Cílem zařízení v této oblasti je přímá komunikace s dodavatelem energií, kteří by tak mohli mít vzdálený dohled a byli by schopni diagnostikovat poruchy bez osobní přítomnosti servisního technika na místě. [1]

Vzhledem k vysokým nárokům na škálovatelnost v síťovém prostoru je nutné, aby síťová architektura zvládala velký objem nově připojených zařízení. Pro možnost připojení zařízení k těmto sítím se využívá technologie IETF 6LoWPAN. CoAP od IETF, ZeroMQ a MQTT poskytly odlehčený přenos dat. Jako životaschopná varianta, která má potenciál zabránit velkému toku dat přes internet jsou tzv. výpočty v mlze, kde se v podstatě jedná o rozšíření cloudu. Ke zpracování dat by pak následně mohl být využit výpočetní výkon okrajových zařízení, což by umožňovalo škálovatelnost v reálném čase. Na obr. 1 lze vidět schéma 6LoWPAN sítě. [1]



Obr. 1. Grafické schéma 6LoWPAN sítě [2]

1.2 IEEE 802.15.4

IEEE 802.15.4 je technický standard, definující provoz nízko-rychlostních bezdrátových osobních sítí (LR-WPAN). Specifikuje fyzickou vrstvu a řízení přístupu k zařízením využívajících LR-WPAN. Pracovní skupina IEEE 802.15, kterou je tento standard spravován, jej definovala v roce 2003 [12]. Tento standard zahrnuje protokoly pro: [13]

- ZigBee,
- 6LoWPAN,
- ZigBee IP,
- ISA100.11a,
- Wireless HART,
- Thread.

1.2.1 Fyzická vrstva

Výše uvedený standard nabízí širokou škálu možností fyzické (PHY) vrstvy v ISM pásmech od 2,4 GHz do sub-GHz frekvencí. IEEE 802.15.4 umožňuje přenos dat

rychlostí 20 kilobitů za sekundu, 40 kilobitů za sekundu, 100 kilobitů za sekundu a 250 kilobitů za sekundu. Základní struktura předpokládá dosah 10 metrů a rychlost přenosu dat 250 kilobitů za sekundu. Pro snížení spotřeby elektrické energie je možné snížit přenosové rychlosti. IEEE 802.15.4 reguluje radiové vysílače/přijímače, výběr kanálů, a dokonce i některé funkce regulující sílu signálu na fyzické vrstvě. Na základě frekvenčního rozsahu a potřebného datového toku je specifikováno šest fyzických vrstev. Čtyři z těchto vrstev využívají techniky frekvenčního přeskakování známé jako „Direct Sequence Spread Spectrum“ (DSSS), ve volném překladu do češtiny se tato technika nazývá rozprostřené spektrum přímé sekvence. [13]

1.2.2 MAC vrstva

Tato vrstva zajišťuje spojení s fyzickou vrstvou takovým způsobem, který určuje, jaká zařízení v dané oblasti budou sdílet přiřazené frekvence. Na této vrstvě je také spravováno plánování a směrování datových paketů. Vrstva MAC 802.15.4 je však zodpovědná za řadu dalších funkcí: [13]

- Vysílání pro zařízení, která v síti fungují jako řadiče,
- sdružování a oddělování PAN pomocí zařízení,
- bezpečnost zařízení,
- zajištění konzistentní komunikace mezi dvěma zařízeními, která jsou ve vztahu peer-to-peer.

K vykonání výše zmíněných funkcí používá MAC vrstva několik zavedených typů rámců. V 802.15.4 existují čtyři různé typy rámců MAC vrstvy: [13]

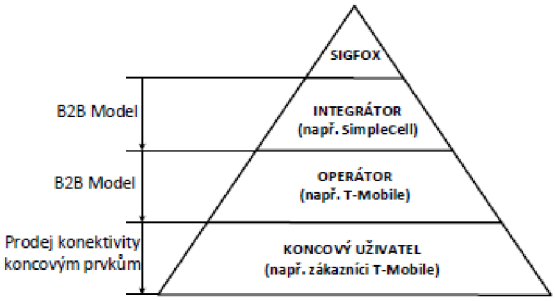
- Datový rámec,
- rámec pro zprávu,
- rámec pro potvrzení,
- rámec pro MAC příkazy.

1.2.3 Topologie

Sítě založené na standardu IEEE 802.15.4 mohou být navrženy v topologii hvězdy, peer-to-peer nebo soustavy sítě. V soustavě sítí dochází k propojování velké množství koncových zařízení. To umožňuje těmto zařízením, které by jinak byly mimo dosah, vzájemně komunikovat a používat přilehlá zařízení k přenosu vlastních dat k cílovým zařízením. [13]

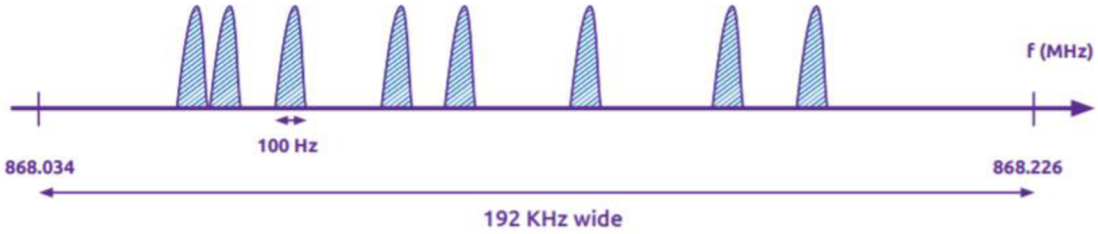
1.3 SigFox

Technologie Sigfox vznikla v roce 2009 ve Francii s cílem vytvořit vzájemnou konektivitu mezi fyzickými zařízeními a internetem. Jedná se o dalšího výrobce radiové komunikace, který využívá LPWAN technologii operující v ISM pásmu. Obchodní model této společnosti není postaven na bázi B2C (přímý prodej zákazníkům), ale využívá tzv. model B2B (prodej dalším firmám), podle kterého prodává svoje služby přes integrátory, což jsou telekomunikační firmy typu T-Mobile, Vodafone, O_2 a další. Tyto společnosti pak prosazují využití této technologie v zemích, ve kterých mají pokrytí signálem. V ČR je model nastaven takovým způsobem, že společnost SigFox prodává své služby společnosti SimpleCell, ta je následně přeprodává společnosti T-Mobile. Společnost T-Mobile následně zajišťuje pokrytí a koncovou konektivitu pro zákazníky. Tento model lze vidět na obr. 2. [4]



Obr. 2. Obchodní model společnosti SigFox na území ČR [4]

Sigfox využívá k výměně zpráv modulaci s ultra úzkou šířkou pásma UNB (Ultra-Narrow Band) o šířce pásma 192 kHz zobrazenou na obr. 3. Každá zpráva je 100 Hz široká a její data jsou přenášena rychlostí 100 nebo 600 bitů za vteřinu v závislosti na geografické poloze. Právě tato vlastnost umožňuje přenášet data na vysokou vzdálenost s malou pravděpodobností rušení datového přenosu. V Evropě se pro komunikační frekvenci používá v rámci ISM pásma frekvenční rozsah 868 MHz – 868,2 MHz. Zpráva o velikosti 12 bajtů se přenáší ze zařízení na server cca 2,08 sekund rychlostí cca 100 bps (bitů za sekundu). Po přijetí zprávy dochází v SigFox stanici k demodulaci UNB signálu v celém jeho rozsahu. [3]



Obr. 3. Schéma ultra širokého pásma [3]

Společnost SigFox vymyslela tento model komunikace pro situace, ve kterých je potřeba mít nízké náklady a zároveň sledovat autonomně připojená zařízení v síti. Tento model nazvala „malé zprávy“, přičemž velikost zprávy se pohybuje od 0–12 bajtů. Zpráva o velikosti 12 bajtů je již dostatečně velká pro odeslání základních dat ze senzorů, jako například upozornění na danou akci/iteraci, data souřadnic GPS, stav událostí, nebo jiná základní data ze senzorů. V tab. 1. jsou znázorněny příklady takovýchto datových balíků podle typu přenášených dat. [3]

Tab. 1. Různé typy přenášených dat a jejich velikost [3]

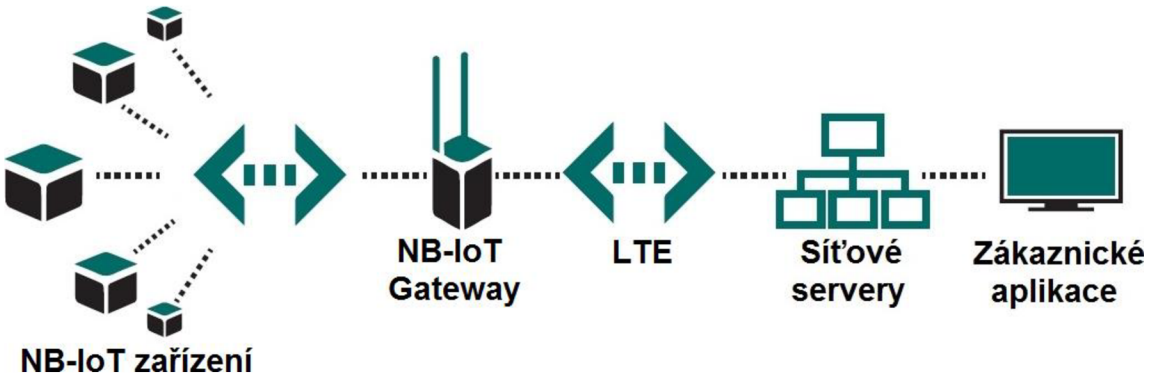
Typ dat	Jejich velikost
GPS souřadnice	6 bajtů
Teplota	2 bajtů
Rychlost	1 bajtů
Stav zařízení	1 bajtů
Výstražné upozornění	0 bajtů

Vzhledem k Evropským regulacím pro vysílání v ISM pásmu je maximální počet zpráv odeslaných na server (uplink) za 1 den pouze 140, přičemž 1 zpráva má velikost 12 bajtů. V rámci jednoho dne se pak jedná o maximální 1 % celkového vysílacího času. [3]

1.4 Narrowband IoT

Technologie NB-IoT podobně jako technologie SigFox spadá do kategorie LPWAN sití. Ve 13. vydání standardu LTE byla standardizována skupinou 3GPP, což je skupina, která se zabývá tvorbou standardů pro mobilní telekomunikace. Ačkoli technologie NB-IoT vychází právě ze standartu LTE, přináší oproti ní velké množství optimalizací a usnadnění protokolu, obecné schéma fungování NB-IoT sítě zobrazuje obr. 4. Díky těmto úpravám vůči původnímu LTE standardu se snížila složitost zařízení a zároveň i výrobní cena. Podobně jako u síťové infrastruktury, kde NB-IoT využívá

většinu prvků ze standardních LTE sítí, tak i fyzická vrstva této sítě má svůj původ u LTE sítí. Díky sdílení pásem může NB-IoT fungovat paralelně s LTE. [4]



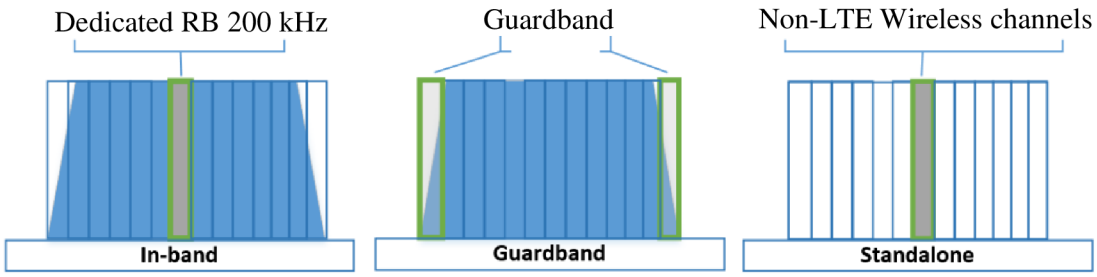
Obr. 4. Schéma architektury NB-IoT sítě [5]

Číslování frekvenčních pásem u NB-IoT je v závislosti na využívaném standardu stejné jako u LTE. Na rozdíl od LTE se však jedná o využití pouze 14 frekvenčních pásem, tato pásma jsou shrnuta v tab. 2. Vzhledem k tomu, že NB-IoT je narozdíl od LTE využíváno hlavně v aplikacích tzv. stroj-stroj (M2M), předpokládá se využití primárně v oblastech s vysokým rušením a špatnými podmínkami pro přenos dat. Vzhledem k této skutečnosti jsou pro účely komunikace přes NB-IoT uvolněna pásma s frekvencí pod 1 GHz. To vyplívá z fyzikální podstaty šíření signálu, kdy je možné dosáhnout lepších vzdálenosti na frekvenci pod 1 GHz. [4]

Tab. 2. Frekvenční pásma pro NB-IoT [4]

Označení pásma	Uplink – frekvence [MHz]	Downlink – frekvence [MHz]
1	1920-1980	2110-2170
2	1850-1910	1930-1990
3	1710-1785	1805-1880
5	824-849	869-894
8	880-915	925-960
12	699-716	729-746
13	777-787	746-756
17	704-716	734-746
18	815-830	860-875
19	830-845	875-890
20	832-862	791-821
26	814-849	859-894
28	703-748	758-803
66	1710-1780	2110-2200

Šířka frekvenčního pásma u této technologie je 180 kHz. Tento rozsah pak odpovídá přesně jednomu zdrojovému bloku u technologie LTE, v závislosti na tom je pak možné NB-IoT provozovat celkem ve třech režimech, tyto režimy lze vidět na obr. 5. Prvním režimem je nasazení v pásmu LTE (In-bank operations), kdy jeden zdrojový blok v síti operátora LTE je vyhrazen pro NB-IoT signál. Druhým režimem je nasazení v ochranném pásmu (Guard band operation), to funguje v ochranném pásmu bezprostředně sousedícím s LTE nosičem, aniž by byla ovlivněna kapacita LTE nosiče. Díky této možnosti si operátor může vybrat nejvhodnější provozní režim, aby naplnil požadavky na výkon sítě a zároveň nabídl služby aplikacím IoT. Třetím režimem je pak samostatné nasazení (Stand-alone operation), u kterého se využívá nově vytvořené nízké pásmo GSM, které již v mnoha zemích existuje (700 MHz, 800 MHz a 900 MHz). [6]



Obr. 5. Operační módy NB-IoT [6]

1.5 LoRaWAN

Tato technologie patří mezi tři nejvýznamnější technologie v oblasti Internetu věcí. Jedná se o technologii s typem sítě LPWAN a podobně jako SigFox pracuje v bezlicenčním ISM pásmu, v Evropě pak frekvenci 868 MHz (USA – 915 MHz, Asie – 434 MHz). Z pohledu vrstev je LoRa typ modulace, která tvoří fyzickou vrstvu. LoRaWAN je pak vrstva, která zajišťuje funkcionalitu MAC vrstvy. Síťová architektura LoRaWAN je typická hvězdicová topologie, ve které jsou brány transparentním mostem, přenášející zprávy mezi koncovými zařízeními a centrálním síťovým serverem. Brány jsou připojeny k síťovému serveru prostřednictvím standardních IP připojení, zatímco koncová zařízení používají bezdrátovou komunikaci s jedním nebo více branami. Veškerá komunikace mezi koncovými body je obousměrná s podporou více směrového vysílání, což umožňuje aktualizaci softwaru bezdrátově a další hromadnou distribuci zpráv takovým způsobem, aby se zkrátila doba radiového vysílání. [4,7]

Využití LoRaWAN v průmyslových prostorách a chytrých městech je silně na vzestupu, a to z důvodu, protože se jedná o cenově dostupný obousměrný komunikační protokol s dlouhým dosahem a s velmi nízkou spotřebou energie — zařízení mohou fungovat na malou baterii až deset let. Koncová zařízení se mohou k LoRaWAN síti připojit dvěma způsoby. Prvním způsobem je metoda aktivace přes vzduch (OTAA). Zařízení musí

vytvořit dva klíče, a to síťový klíč a klíč relace aplikace pro připojení k síti. Druhým způsobem je metoda aktivace pomocí personalizace (ABP). Zařízení je od výroby naprogramováno s klíči potřebnými pro komunikaci se sítí, takže připojení je méně bezpečné, ale jednodušší. [8]

Následující kapitoly se budou zabývat popisem LoRa/LoRaWAN technologie z pohledu modulace, komunikačního protokolu, zabezpečení a praktického využití.

1.5.1 LoRa fyzická vrstva

LoRa je proprietární schéma modulace s rozprostřeným spektrem, které je odvozeno od modulace rozprostřeného spektra (CSS) měnící rychlost přenosu dat za citlivost v rámci pevné šířky pásma kanálu. CSS, jenž byl vyvinut ve 40. letech 20. století, byl tradičně používán ve vojenských aplikacích kvůli svým dominantním vlastnostem, a to schopnostem komunikovat na dlouhé vzdálenosti a zároveň mít velkou odolnosti vůči rušení. LoRa je jeho první ekonomicky akceptovatelná implementace pro komerční využití. Název LoRa pochází z anglických slov „long range“, což v překladu znamená dlouhá vzdálenost, čímž název poukazuje na dominantní parametr této technologie. Parametry fyzické vrstvy LoRa lze sledovat v tab. 3. [9]

K dosažení komunikace na velké vzdálenosti používá síť LoRaWAN adaptivní modulační techniku s vícekanálovým více-modemovým vysílačem/přijímačem v základních stanicích pro příjem vícenásobného počtu zpráv z několika kanálů. Rozprostřené spektrum poskytuje ortogonální oddělení mezi signály za využití unikátního faktoru rozprostření k jednotlivému signálu. Tato metoda je výhodná pro regulaci rychlosti přenosu dat. Výhodou LoRa modulace je také její flexibilita, tato modulace zároveň pracuje v širokém frekvenčním rozsahu, a to od 173 MHz do 1020 MHz. Tři klíčové parametry modulace, které mají vliv na rychlost komunikace a robustnost signálu jsou: činitel rozprostření (SF), šířka pásma modulace (BW) a kódovací poměr (CR). Díky těmto parametrům je pak možné udržovat rádiový přenos i za neideálních podmínek. Vztah mezi požadovanou přenosovou rychlostí, „chirp“ rychlostí a „symbolovou“ rychlostí v modulační technice LoRa lze vyjádřit jako bitovou rychlost modulace Rb podle vzorce (1.1) [4,9]

$$R_b = SF * \frac{1}{\left[\frac{2^{SF}}{BW}\right]} bit/s \tag{1.1}$$

SF = činitel rozprostření a BW = šířka pásma modulace v Hz. Podle vzorce (1.1) je rychlost přenosu dat Rb přímo úměrná faktoru šíření SF. [9]

Tab. 3. Parametry fyzické vrstvy LoRa [9]

Parametry	Technologie LoRa
Spektrum	Nelicencované
Typ modulace	CSS
Šířka pásma	500-125 kHz
Špičková rychlost přenosu dat	290 bps – 50 kbps
Link budget	154 dB
Maximální počet zpráv/den	Neomezený
Energetická efektivita	Velice vysoká
Energetická účinnost	Zařízení může z baterií pracovat až 10 let
Spektrální účinnost	CSS CDMA je lepší než FSK
Odolnost vůči rušení	Velice vysoká
Špičkový proud	32 mA
Odběr proudu v režimu spánku	1 uA

1.5.2 Činitel rozprostření (SF)

Činitel rozprostření (SF) má vliv komunikační výkon LoRa. Může nabývat celočíselných hodnot od 7 do 12. Čím větší je činitel rozprostření, tím delší je doba, kterou signál stráví „ve vzduchu“ mezi vysílačem a přijímačem. To má za následek vyšší spotřebu energie a nižší přenosovou rychlost, zároveň je však možné dosáhnout komunikace na větší vzdálenosti. Pro úspěšnou komunikaci mezi vysílačem a přijímačem je však nutné, aby měly obě strany stejný činitel rozprostření, ten pak udává vzorec (1.2): [11]

$$SF = \log 2 \left(\frac{R_C}{R_S} \right) \tag{1.2}$$

kde Rc je čipová rychlost a Rs je symbolová rychlost. SF je pak logaritmický poměr mezi počtem čipů a symbolů, přičemž se pohybuje v rozmezí od 7 do 12. [11]

1.5.3 Kódový poměr (CR)

Tato hodnota udává poměr mezi počtem bitů užitečných dat a počtem bitů vyslaných dat. Nejčastěji používaná hodnota je 4/5, u speciálních aplikací s vyššími požadavky na spolehlivost se používá hodnota 4/7. Hodnota kódovacího poměru je dána vzorcem (1.3). [4]

$$CR = \frac{4}{4+R} \tag{1.3}$$

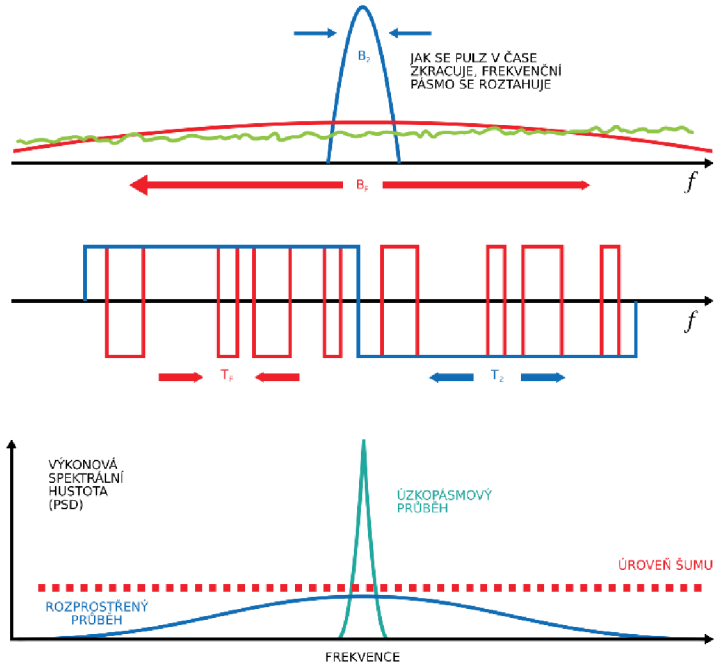
Parametr R udává samotnou identifikaci poměru dle tab. 4. [4]

Tab. 4. Použitelné hodnoty kódového poměru [4]

Kódový poměr	Max počet opravených chyb	Max počet detekovaných chyb	R
4/5	0	0	1
4/6	0	1	2
4/7	1	2	3
4/8	1	3	4

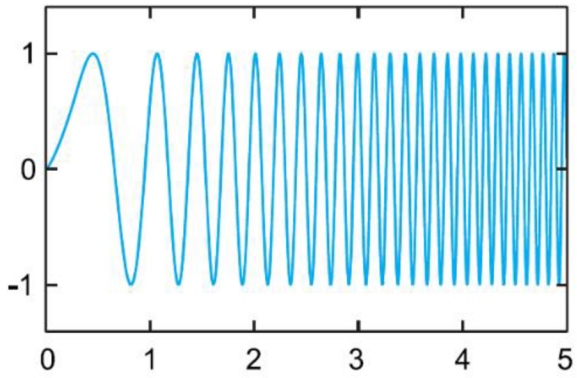
1.5.4 Rozprostření spektra CSS – modulace LoRa

LoRa má patentovanou modulační techniku s rozprostřeným spektrem odvozenou od technologie Chirp Spread Spectrum (CSS). Technologie LoRa je ideální kompromis mezi citlivostí a přenosovou rychlostí při provozu v kanálu s pevnou šířkou pásma buď 125 kHz nebo 500 kHz (pro nahrávací kanály) a 500 kHz (pro stahovací kanály). U systémů DSSS (Direct Sequence Spread Spectrum), ve volném překladu: Rozprostřené spektrum přímé sekvence, se nosná fáze signálu vysílače mění podle kódové sekvence, jak je znázorněno na obr. 6. Při násobení datového signálu předem definovaným bitovým vzorem s mnohem vyšší rychlostí, také známém jako rozprostírací kód (nebo čipová sekvence), je následně vytvořen tzv. „rychlejší“ signál, který má vyšší frekvenční složky než původní datový signál. To znamená, že šířka pásma signálu je rozšířena na šířku pásma původního signálu. V radioelektronické terminologii se bity kódové sekvence nazývají čipy (aby bylo možné rozlišit mezi delšími, nekódovanými bity původního datového signálu). Když vysílaný signál dorazí do radiového přijímače, je vynásoben identickou kopií rozšiřovacího kódu použitého v radiovém vysílači, což má za následek repliku původního datového signálu. [10]



Obr. 6. Změny fáze nosného signálu vysílače s modulací DSSS [10]

Poměr kódové sekvence rychlosti čipu a bitové rychlosti datového signálu se nazývá „zisk zpracování“ (Gp). Tento zisk umožňuje přijímači obnovit původní datový signál, i když má kanál zrovna negativní poměr signál/šum (SNR). Technologie LoRa má ve srovnání s modulací FSK (klíčování frekvenčním posuvem), lepší zisk zpracování, což umožňuje snížit úroveň výstupního výkonu vysílače při zachování stejné přenosové rychlosti signálu. Nevýhodou systému DSSS je potřeba vysoce přesného (a zároveň drahého) zdroje referenčních hodin. Na rozdíl od DSSS, technologie LoRa, která využívá modulační techniky CSS, umožňuje vytvářet zařízení s nízkou spotřebou elektrické energie a za ekonomicky výhodných podmínek, zároveň je také velice robustní alternativou modulace DSSS, kdy na rozdíl od ní nevyžaduje vysoce přesné referenční hodiny. V modulaci LoRa je šíření spektra signálu dosaženo generováním signálu, který se ve frekvenci plynule mění. Průběh tohoto signálu je pak možné sledovat na obr. 7. [10]

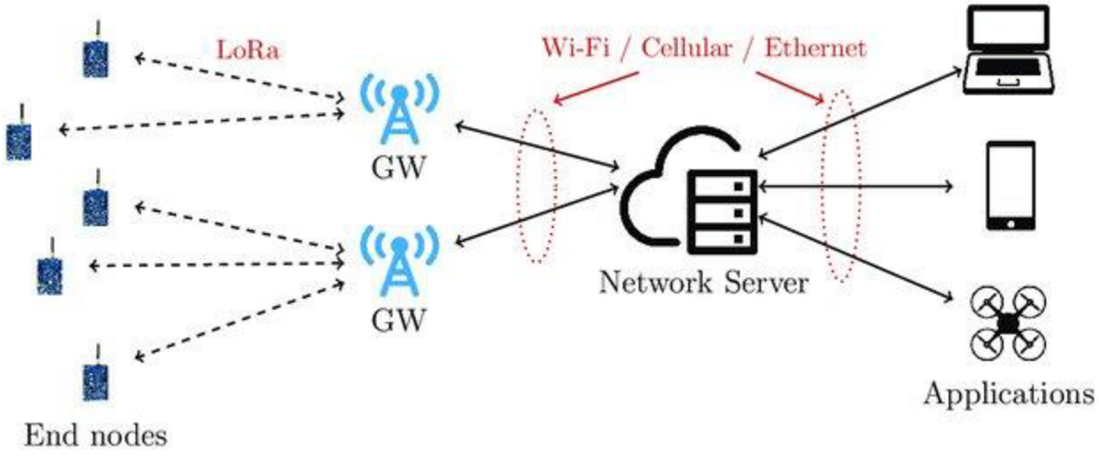


Obr. 7. Signál modulace CSS LoRa [10]

V technologii LoRa se kód, který se rozprostírá na původním datovém signálu nazývá činitel rozprostření (SF). Modulace LoRa má celkem šest faktorů šíření (SF7 až SF12). Čím vyšší je použitý faktor šíření, tím větší je vzdálenost, kterou bude signál schopen cestovat, přičemž jej stále možné přijímat bez chyb na straně radiových přijímačů. [10]

1.5.5 Architektura sítě LoRaWAN

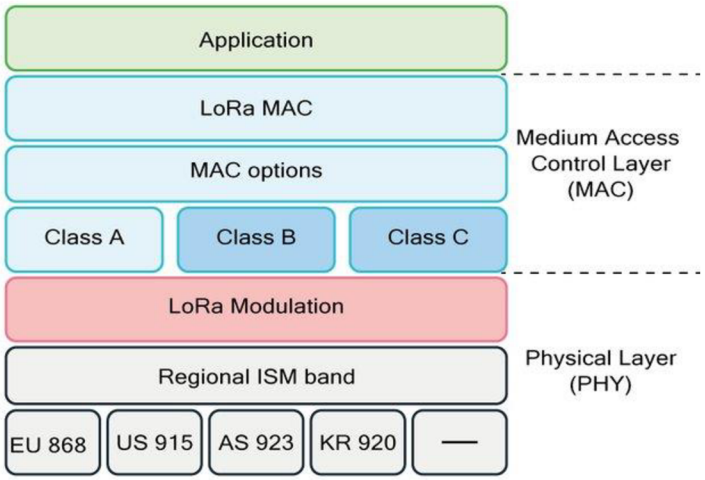
Jak již bylo zmíněno v předchozích kapitolách LoRaWAN (síťová vrstva) definuje komunikační protokol a architekturu systému, zatímco LoRa definuje fyzickou vrstvu. LoRaWAN využívá hvězdicovou architekturu s dlouhým dosahem (lze vidět na obr. 8), ve které vstupní brány slouží jako mosty mezi koncovými zařízeními a centrální jádrovou sítí na internetu (vzdálené datové úložiště). V síti LoRaWAN nejsou koncová zařízení přidružena ke konkrétní vstupní bráně. Místo toho jsou data odeslaná z koncových zařízení obvykle přijímána více různými branami. Každá vstupní brána přepošle přijatý datový balíček z koncového zařízení na vzdálený datový síťový server prostřednictvím páteřního připojení (buď mobilního, ethernetového, satelitního nebo Wi-Fi připojení). Koncová zařízení (tj. senzory) komunikují s jednou nebo více vstupními branami prostřednictvím jedno-skokové komunikace LoRa, zatímco všechny brány jsou připojeny k serveru hlavní sítě prostřednictvím standardních IP připojení. Síťový server má potřebnou inteligenci pro filtrování zdvojených datových balíčků z různých vstupních bran, kontrolu zabezpečení, odesílání potvrzení ACK vstupním branám a odesílání datových balíčků na konkrétní aplikační server. Protože si síť může vybrat informace s nejvyšší kvalitou z informací přenášených různými vstupními bránami, odpadá potřeba předávání. Pokud je koncové zařízení mobilní, nebo se pohybuje, není potřeba žádné předávání z brány na bránu, což je velice důležitá funkce pro možnost vytváření aplikací pro sledování různých aktivit, což je hlavní cílová aplikace pro vertikální IoT. Pomocí soustavy sítí může systém zvýšit komunikační dosah a velikost buněk sítě na úkor životnosti baterie v koncovém zařízení. [9]



Obr. 8. Architektura sítě LoRaWAN [14]

1.5.6 LoRaWAN MAC vrstva

Protokol MAC LoRaWAN je protokol s otevřeným zdrojovým kódem, podléhající standardu „LoRa Alliance“, jenž běží nad fyzickou vrstvou LoRa. Vrstva LoRaWAN MAC poskytuje střední mechanismus řízení přístupu, který umožňuje komunikaci mezi více koncovými zařízeními a síťovými bránami. Schéma protokol LoRaWAN lze vidět na obr. 9 [15]



Obr. 9. Blokové schéma protokolu LoRaWAN [16]

Norma LoraWAN definuje tři třídy koncových zařízení, a to třídy A, B a C. Třída A je základní implementace, musí být pro všechna koncová zařízení podporována vždy. Třídy B, C jsou k základní třídě A pouze rozšiřující, není proto nezbytné, aby byly implementovány ve všech případech. [4,15]

1.5.7 Třída A

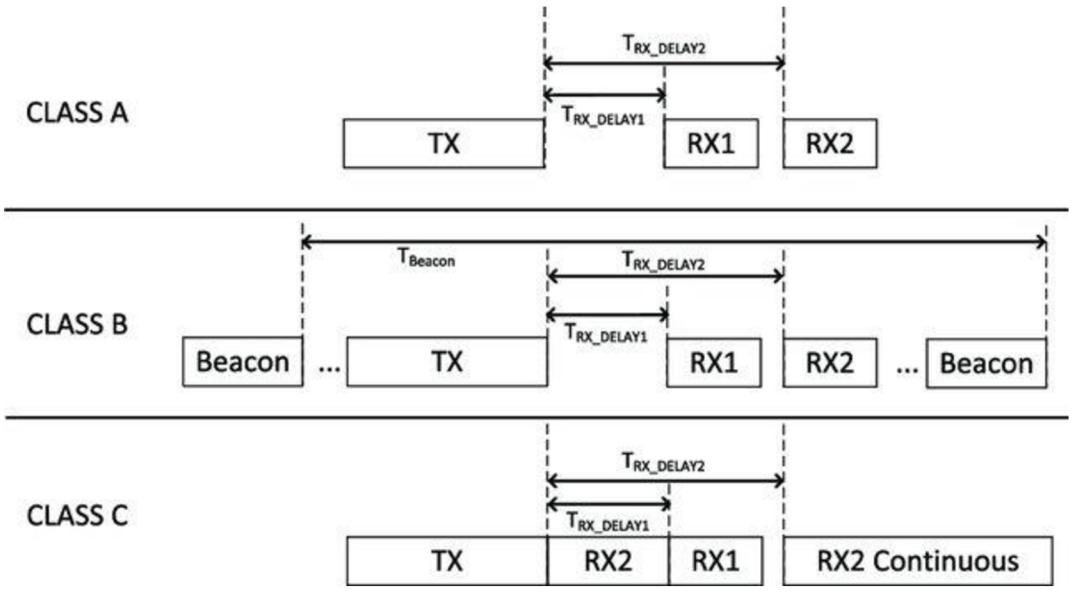
Parametry třídy A jsou sadou základních možností, které musí být implementovány pro každé koncové zařízení, aby se zařízení mohla připojit k síti LoRaWAN. Aby koncovému zařízení byla umožněna obousměrná komunikace, tak po každém nahrávacím vysílacím přenosu u zařízení třídy A následují dvě krátká po sobě jdoucí přijímací okna (RX1 a RX2), během kterých je koncovému zařízení umožněno přijímat, nebo stahovat zprávy. Stahovací komunikace je spouštěna koncovým zařízením, což znamená, že každý sestupný rámec musí čekat na vzestupnou komunikaci TX1. První a druhé sestupné přijímací okno (RX1 a RX2) vždy začíná první sekundu a druhou sekundu po skončení nahrávacím vysílání. Pokud k sestupnému přenosu dojde během prvního časového okna, pak se stejný kanál, který se používá pro nahrávání, použije i pro stahování. V případě, že je pro sestupný přenos použito druhé přijímací okno, pak se použije pevný faktor šíření a pevný kanál. Typicky se jedná o 125 kHz kanál se středím kmitočtem na 869,525 MHz pomocí SF12, který má 10% pracovní cyklus a vysoký vysílací výkon 24 dBm. Odpovědností síťového serveru je naplánovat časový rámec pro stahování, v přesných časech a zároveň provádět kontrolu tohoto časování. Koncová zařízení třídy A spotřebují nejmenší množství elektrické energie, protože většinu času se nachází v režimu spánku. Průběh komunikace v třídě A lze vidět na obr. 10. [15]

1.5.8 Třída B

Na rozdíl od třídy A má třída B zvýšenou možnost stahování. Pro dosažení zvýšení stahování, jsou u koncových zařízení třídy B otevřena další přijímací okna v předem naplánovaných intervalech. Přijímací brány tak ve stahovacím režimu do datových balíčků pro koncová zařízení třídy B přidávají vysílače – nejen z důvodu možné synchronizace, ale také síťový server věděl, kdy bude dané koncové zařízení naslouchat stahovacímu provozu. Zařízení třídy B spotřebovávají vyšší množství elektrické energii ve srovnání se zařízeními v třídě A, kvůli potřebě otevřít více přijímacích oken, ačkoli tato okna nemusí být pro sestupný provoz vůbec použita. Průběh komunikace v třídě B lze vidět na obr. 10. [15]

1.5.9 Třída C

Zařízení pracující ve třídě C mají otevřená přijímací okna téměř kontinuálně, tato okna jsou uzavřena pouze v době, kdy dochází k vysílání z koncových zařízení. Průběh komunikace v třídě C lze vidět na obr. 10. Výhodou této třídy je přenos dat s velice malým zpožděním, nevýhodou je naopak velká spotřeba elektrické energie. Zařízení v této třídě jsou obvykle nasazována v místech s trvalým přísunem elektrické energie. [4,15]



Obr. 10. Průběh komunikace LoRaWAN v třídách A, B a C [17]

1.5.10 Adaptivní a datový mechanismus

Mechanismus Adaptive Data Rate (ADR), ve volném překladu do češtiny adaptivní datová rychlost, je implementován v MAC vrstvě LoRaWAN pro dynamickou správu parametrů linky koncových zařízení. Cílem tohoto mechanismu je navýšení poměru doručených datových balíčků vzhledem ke ztraceným. Mechanismus ADR udává rychlost přenosu dat a zároveň určuje vysílací výkon koncových zařízení. Aby mohl síťový server řídit přenosové parametry koncového zařízení, musí mít s koncovými zařízeními konektivitu. Ta bude zajištěna pomocí nastavení nahrávacího bitu ADR v daných komunikačních balíčcích. V opačném případě má koncové zařízení možnost řídit své přenosové parametry samo pomocí ADR mechanismu, který je v tomto nastavení umístěn na straně koncového zařízení. Obě části mechanismu ADR tedy běží asynchronně na síťovém serveru a na koncovém zařízení. V nejnovější verze standardu LoRaWAN (v1.1) je algoritmus ADR na koncovém zařízení velice jednoduchý. Zahrnuje pouze dva parametry, a to „ADR_ACK_LIMIT“ a „ADR_ACK_DELAY“. Koncové zařízení zvýší „ADR_ACK_CNT“ pro každý odeslaný nahrávací datový balíček. Jakmile bude hodnota ADR_ACK_CNT vyšší než hodnota ADR_ACK_LIMIT, koncové zařízení nastaví bit ADRACKReq a bude čekat na zpětné potvrzení ze sítě pro další nahrávací datové balíčky ADR_ACK_DELAY. Pokud nedojde k potvrzení nahrávacích datových balíčků před ADR_ACK_DELAY, koncové zařízení sníží, při pokusu o opětovné připojení k síti, rychlost přenosu dat. Koncové zařízení se nejprve snaží získat připojení zvýšením vysílacího výkonu. Pokud nestačí zvýšit vysílací výkon, pokračuje ve snižování

rychlosti přenosu dat. Mechanismus ADR v síťovém serveru udává přenosové parametry (SF a vysílací výkon) koncových zařízení, na základě odhadu velikosti linky u nahrávací a prahové hodnoty SNR, pro správné dekódování datových balíčků při definované rychlosti přenosu dat. [15]

1.5.11 Mechanismus připojení zařízení LoRaWAN do sítě

Před připojením koncového zařízení do LoRaWAN sítě musí být každé zařízení aktivováno. Zařízení se dá do sítě připojit celkem dvěma způsoby, a to pomocí aktivace personalizací (ABP), nebo aktivací vzduchem (OTAA). Před tím, než je zahájen proces připojení do sítě, je nutné do koncových zařízení nahrát aktivační klíče. Tyto klíče lze vidět v tab. 5. Klíče jsou určeny pouze pro jednu komunikaci mezi koncovým zařízením a aplikačním serverem. Z důvodu bezpečnosti přenášených dat je nezbytné, aby byly klíče aktualizovány. [15]

1.5.12 Metoda OTAA (v1.1)

U metody OTAA je koncové zařízení aktivováno pomocí klíčů a identifikátorů, které jsou uloženy před zahájením aktivačního procesu podle tab. 5. Koncové zařízení odesílá požadavky na připojení nebo na znovu připojení k síťovému serveru. Na tyto pokusy server odpovídá se zprávou o povolení k připojení. Zpráva s požadavkem o připojení obsahuje DevEUI, JoinEUI a 2 bajty DevNonce. Samotný požadavek o připojení není nijak šifrován, ale je k ní připojena MIC (kontrola integrity zprávy), která se vypočítává za pomoci NwkKey. Pokud je připojení koncového zařízení k síti schváleno, pak síťový server odešle koncovému zařízení zprávu o povolení k připojení. Tento datový balíček s sebou mimo jiné komunikační parametry ponese také DevAddr a 3 bajty JoinNonce (jedná se o přírůstkové číslo, které se nebude opakovat). Samotná zpráva o povolení k připojení je šifrována pomocí NwkKey, nebo JSEncKEy. Nwkey je použit v případě, kdy se jedná o odpověď na zprávu s žádostí o připojení, naopak JSEncKey se používá tehdy, kdy se jedná o odpověď na zprávu s žádostí o opětovné připojení. MCI je pak ověřen pomocí JSIntKey. Zpráva o povolení k připojení je přijata tehdy, pokud dojde k ověření MIC a JoinNonce hodnota je vyšší než poslední hodnota uložená v paměti. Klíče FNwkSIntKey, SNwkSIntKey a NwkSEncKey jsou následně vypočteny z NwkKey, naproti tomu AppSkey je odovozen z AppKey. Na konci komunikace odesílá koncové zařízení MAC příkaz do síťového serveru pro potvrzení přepnutí zabezpečení. Nové zabezpečení je použito tehdy, jakmile dojde k potvrzení daného MAC příkazu ze strany síťového serveru. Kvůli potřebě udržení se v síti, odesílá koncové zařízení během komunikace se serverem datové pakety s žádostí o opětovné připojení. [15]

1.5.13 Metoda ABP (v1.1)

Na rozdíl od metody OTAA jsou u metody ABP všechny klíče potřebné k aktivaci v koncovém zařízená uloženy předem. Není proto potřeba aktivačního procesu mezi koncovým zařízením a LoRaWAN branou kvůli odvození šifrovacích klíčů. Riziko u použití této metody vzniká tehdy, podaří-li se zařízení odcizit. Klíče z odcizeného zařízení je následně totiž možné vytáhnout. Zařízení útočníka se pak v síti může jevit jako zařízení odcizené. [15]

Tab. 5. LoRaWAN klíče [15]

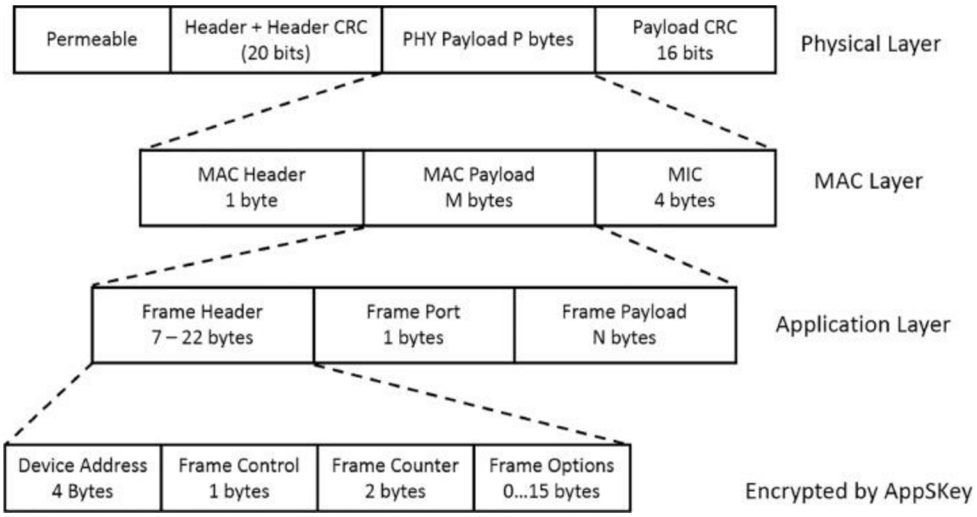
Klíč	Popis	OTAA	ABP	Získáno způsobem
NwkKey	Slouží pro kalkulaci MIC paketů požadavků o připojení	ANO	NE	Předem uloženo
AppKey	Používá se k odvození AppSKey	ANO	NE	
JSIntKey	Používá se pro MIC žádosti o opětovné připojení	ANO	NE	Generováno z NwkKey a DevEUI
JSEncKey	Používá se k šifrování požadavku o připojení spuštěného požadavkem na opětovné připojení	ANO	NE	
FNwkSIntKey	Používá se pro výpočet MIC části všech uplinkových datových paketů	ANO	ANO	Generováno z NwkKey a zprávy o přijetí
SNwkSInKey	Používá se k ověření MIC všech downlinkových datových paketů a výpočtu části MIC uplinkových paketů	ANO	ANO	
NwkSEncKey	Používá se k šifrování všech downlinkových a uplinkových MAC paketů	ANO	ANO	
AppSKey	Používá se k šifrování/dešifrování užitečného obsahu datových paketů	ANO	ANO	Generováno z AppKey a zprávy o přijetí
JoinEUI	64bitové globálně jedinečné ID aplikace, které identifikuje server pro připojení	ANO	NE	Předem uloženo
DevEUI	64bitové globálně jedinečné ID zařízení od síťového serveru	ANO	NE	
DevAddr	32bitová jedinečná adresa zařízení v aktuální síti	ANO	ANO	Přijato zprávou požadavku o připojení

1.5.14 Struktura datového rámce LoRaWAN

Datový rámec fyzické vrstvy LoRaWAN začíná preambulí o velikosti 8 bajtů. Preambule slouží především k synchronizaci a určení zvoleného modulačního schématu. Po preambuli následuje hlavička fyzické vrstvy s kontrolním součtem CRC s velikostí 20 bitů. Hlavička fyzické vrstvy není povinnou součástí rámce na této vrstvy. Následují uživatelská data s jejich kontrolním součtem o velikosti 16 bitů. Zobrazení vrstvy lze vidět na obr. 11. V síťové vrstvě se pak nachází jako první hlavička o velikosti 1 bajtu. Hlavička této vrstvy nese informaci o použité verzi komunikačního protokolu a informaci o typu rámce. Za ní následují uživatelská data a za uživatelskými daty se nachází MIC o velikosti 4 bajtů. Data MIC na síťové vrstvě zajišťují autentičnost dat, která jsou vypočítávána za pomoci šifry symetrické AES a NwkSkey klíče. Nejdůležitější druhy rámců jsou: [18]

- žádost o připojení,
- přijmout připojení,
- nepotvrzené údaje,
- potvrzená data.

Na úrovni aplikační vrstvy jsou šifrovaná uživatelská data rozšířena o číslo portu s velikostí 1 bajt. Za uživatelskými daty následuje variabilní hlavička rámce s velikostí 7 až 22 bajtů, tato hlavička nese informace jako: adresa zařízení, hodnotu čítače rámce, řídící informace rámce a pole pro přenos příkazu síťové vrstvy. Hlavička obsahuje čtyři pole. Prvním polem je adresa zařízení, ta se skládá z 32 bitů, které identifikují koncové zařízení. Druhé pole je pro ovládání datového rámce. Obsahuje 1 bajt používaný pro řízení informací o síti, jako jsou datové rychlosti používané pro přenos nahrávacích zpráv a potvrzení zprávy. Třetím polem je počítadlo rámců, sledující počet datových zpráv v odesílací cestě a stahovací cestě odeslaných/přijatých sítí. Ve čtvrtém jsou možnosti datového rámce. Zde se přenáší MAC příkazy „zabalené do datových rámců“. [18]



Obr. 11. Datový rámec LoRaWAN [18]

1.5.15 LoRaWAN Multihop sítě

Současnou hvězdicovou topologii LoRaWAN nelze využít ve všech typech aplikací. Pro koncová zařízení, která jsou umístěna daleko od bran, nebo mají špatnou kvalitu signálové komunikace s bránou může být řešení multi-hop komunikace. Multi-hop komunikace je u síťové topologie LoRa považovány za metodu, která by mohla zvýšit spolehlivost těchto komunikačních síti ve směru spolehlivosti přenášeného signálu a tím menší chybovost. [15]

1.5.16 LoRaWAN zabezpečení

Jedním z hlavních cílů při vývoji technologie LoRaWAN byla úroveň zabezpečení přenášených dat. Z pohledu implementace se systém zabezpečení technologie LoRa dělí do dvou samostatných oddílů. Protokol LoRaWAN zajišťuje tzv. End-to-End komunikaci mezi koncovými zařízeními a servery. End-to-End je takové šifrování, u kterého je přenos dat zabezpečen jak koncovým zařízením, tak serverem samotným. Zabezpečení mezi aplikačním serverem a uživatelskou aplikací je vytvořeno nezávisle na předchozím zabezpečení. Zabezpečení dat aplikačního serveru je realizováno běžnými mechanismy jako HTTPS, nebo VPN připojením. Komunikace End-to-End mezi koncovým zařízením a aplikačním serverem zajišťuje protokol LoRaWAN. Ten pak zajišťuje jak důvěrnost zprávy, tak autenticitu. Standartně se používá 128bitová velikost klíče využitého pro šifrování AES. Uživatelská data jsou také zabezpečena pomocí klíče AppSKey, využívajícího stejné šifrování zmíněné výše. AES zde pracuje v režimu CTR (čítač). Autentičnost je zde zajištěna na základě pole MIC – jedná se o unikátní podpis zprávy. Pole MIC je generováno s použitím 128bitové šifry AES, kde však ale tato šifra pracuje v módu CMAC (kód pro ověřování zpráv založený

na šifrách), je zde také využíván klíč NwkSKey, který má 128bitové šifrování. Obdobně se pak přistupuje také k ověření autentičnosti na LoRaWAN bráně. Brána podle adresy koncového zařízení DevAddr vyhledává odpovídající NwkSkey a z uživatelských dat přijaté zprávy znovu počítá podle MIC. To je pak porovnáváno s tím z přijaté zprávy. [4]

1.6 Srovnání LoRaWAN s NB-IoT

1.6.1 Kvalita služby

LoRa využívá nelicencované spektrum a zároveň má asynchronní komunikační protokol. Modulace LoRa je založená na modulaci CSS, která má velmi dobré výsledky odolnosti k okolnímu rušení. Srovnáme-li však technologie NB-IoT a zmíněnou Loru, NB-IoT dosahuje stále kvalitnějších výsledků, z důvodu využití licencovaného pásma společně se synchronním protokolem využívajícím časová okna. Tato výhoda však vzniká na úkor nákladů. Licence spektra v pásmu sub-GHz se obvykle pohybují v cenové hladině větší než 500 milionů dolarů za MHz. Od tohoto parametru se následně odvíjejí také zvolené technologie do určitých aplikací. Pokud je rozhodující kvalita přenášeného signálu, nikoliv však cena, je častěji zvolena technologie NB-IoT. V opačném případě je volena technologie LoRa. [9]

1.6.2 Výdrž baterie a latence

Zařízení využívající technologii LoRaWAN mohou být v režimu spánku tak dlouho, jak daná aplikace vyžaduje. Je to možné díky tomu, že komunikační protokol LoRaWAN je asynchronní, a je založený na principu ALOHA. Naproti tomu zařízení využívající technologii NB-IoT mají větší spotřebu elektrické energie, a to v důsledku toho, že kvůli pravidelné synchronizaci s nadřazenou sítí se tato zařízení uvádějí do chodu v pravidelných intervalech. Navíc tato zařízení vyžadují vyšší špičkový proud, v důsledku použití lineárního vysílače. Porovnání proudů je uvedeno v tab. 6. Z předcházejícího popisu je jasné, že zařízení využívající technologii NB-IoT mají vyšší spotřebu elektrické energie než technologie využívající technologii LoRa. Naproti tomu má NB-IoT nízkou latenci a vysoký datový tok. Vzhledem k těmto parametrům je pak vhodné volit technologii dle potřeb dané aplikace. [9]

Tab. 6. Proudy a latence [9]

Technologie	Špičkový A	A v režimu spánku	Latence
LoRa	32 mA	1 uA	Necitlivý k latenci
NB-IoT	120/130 mA	5 uA	<10 s

1.6.3 Pokrytí a dosah sítě

Hlavní výhodou využití technologie LoRa je, že celé město, či daná oblast může být pokryto jednou bránou nebo základnovou stanicí. Například v Belgii, zemi s celkovou rozlohou přibližně 30500 km^2, pokrývá nasazení sítě LoRa celou zemi s typicky sedmi základnovými stanicemi. Technologie NB-IoT se zaměřuje hlavně na zařízení třídy MTC, která jsou typicky instalována na místech daleko od obvyklého dosahu, pokrytí by proto nemělo být nižší než 23 dB. Nasazení technologie NB-IoT je omezeno pouze na základové stanice 4G/LTE. NB-IoT proto není příliš vhodný pro příměstské, venkovské oblasti, které mají špatné, nebo žádné pokrytí 4G signálem. Výhodou ekosystému LoRaWAN je tak jeho flexibilita, protože může mít širší pokrytí sítě než NB-IoT. Maximální ztráta spojení (MCL) je dána mezní hodnotou ztráty spojení, při které může být služba dodána. Rozsah služby pro technologii LoRaWAN a NB-IoT je uveden v tab. 7. [9]

Tab. 7. MCL a dosah LoRaWAN a NB-IoT [9]

Technologie	Uplink MCL	Downlink MCL	Dosah
LoRaWAN	165 dB	165 dB	<15 km
NB-IoT	145-169 dB	151 dB	<35 km

2. PRAKTICKÁ ČÁST

Praktická část se zabývá návrhem a realizací postupu pro vytvoření dvou LoRaWAN systémů, přičemž jeden je postaven na globální síti TTN a druhý je postaven na lokální síti ChirpStack. U obou typů je popsán postup pro vytvoření síťového a aplikačního serveru, připojení přístupové brány, testování funkčnosti sítě za pomoci komerčně dostupné LoRa testeru, připojení vlastního koncového zařízení do sítě a zobrazení získaných dat z koncového zařízení na webové stránce.

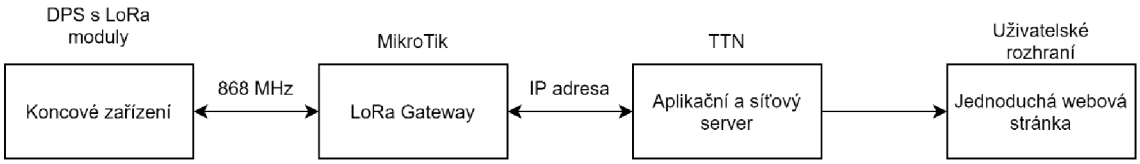
2.1 Koncepty systémů

Tato kapitola popisuje systém na bázi sítě TTN a na bázi sítě ChirpStack. Oba tyto koncepty jsou graficky znázorněny pomocí blokových schémat.

2.1.1 Koncept systému LoRaWAN síť TTN

První z konceptů je postaven na využití LoRaWAN sítě „The Things Network“ (TTN). Jedná se o komunitní síť, ve které se nachází velké množství veřejně dostupných LoRa přístupových bran pro připojení vlastích koncových zařízení. V rámci sítě je zároveň možné přes vytvořený profil připojovat vlastní LoRa přístupové brány. Tyto přístupové brány je možné nastavit jako veřejné, nebo také jako soukromé. V případě, že jsou nastaveny jako veřejné, tak poté mohou být přes přístupové brány distribuována data z koncových zařízení různých uživatelů v dané lokalitě. V případě nastavení přístupové brány jako soukromé (privátní), mohou být skrze tyto přístupové brány distribuována data pouze vybrané skupiny koncových zařízení. Hustota sítě je tvořena především komunitními přístupovými branami, pokrytí je pak závislé na velikosti komunity v daném regionu. Nejhustější pokrytí je z globálního pohledu v Evropě, po ní následuje Jižní a Severní Amerika, menší hustota pokrytí je v Africe, Asii a Austrálii. Z pohledu pokrytí v Evropě má největší počet veřejných přístupových bran Německo, Velká Británie, následně Francie a Španělsko. Počet veřejných přístupových bran v České republice je okolo 140 zařízení, přičemž nejvíce jich má Praha a Středočeský kraj, po něm pak Jihomoravský kraj. V posledních letech však můžou tuto síť využívat také soukromé společnosti, a to od malých firem po korporátní společnosti. V důsledku toho je pak možné při registraci vybrat profil, který indikuje, za jakým účelem bude síť využívána a podle výběru je následně vybrán síťový server. Účty v síti se dělí na dvě kategorie, komunitní a obchodní. Za účelem této práce byla zvolena kategorie komunitní s profilem student. Jako přístupová brána je využit nastavitelný router MikroTik RBwAPR-2nD&R11e-LoRa8, ke kterému se bezdrátově připojují koncová zařízení za účelem přenosu dat na server. Systém je koncepčně navržen takovým způsobem, že koncové zařízení odesílá svá naměřená data z teplotního senzoru na server. Tato data odesílá z jednoho ze tří LoRa modulů, které jsou na DPS navrženy. Vzhledem k tomu,

že pro použité koncové zařízení je využita šifrovací metoda ABP, není nutné, aby docházelo k opětovnému aktivačnímu procesu, mezi koncovým zařízením a LoRaWAN přístupovými branami za účelem předání šifrovacích klíčů. U použití metody ABP totiž dochází k uložení klíčů do paměti koncového zařízení ještě před zahájením komunikace se serverem. Síťový server má v rámci LoRaWAN sítě na starost autentifikaci zařízení vstupujících do sítě. Mimo autentifikaci s koncovým zařízením pak také zajišťuje de-duplikaci přijatých komunikačních rámců, má na starost plánování stahování a komunikaci s aplikačním serverem. Po úspěšném spárování koncového zařízení se síťovým serverem jsou data přenášena na aplikační server. Aplikační server následně zajišťuje bezpečnost (šifrování) komunikace s koncovou aplikací, a má na starost správu připojených zařízení (uživatelů). Data jsou z aplikačního serveru TTN poté přenášena na jednoduchou webovou stránku, která slouží jako uživatelské rozhraní ke sledování naměřených dat ze senzorů na koncovém zařízení. Tři různé moduly jsou zvoleny z toho důvodu, aby bylo možné zajistit vyrobitelnost zařízení. Riziko spojené s výrobou vzniká v důsledku nedostatku komponent, který je způsoben současnou součástkovou krizí. Celý koncept systému lze vidět v blokovém schématu na obr. 12.

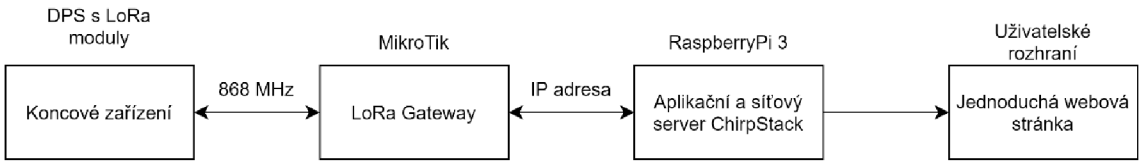


Obr. 12. Blokové schéma realizovaného LoRaWAN systému na síti TTN

2.1.2 Koncept systému LoRaWAN lokální síť ChirpStack

Druhý koncept je lokální síť LoRa s využitím systému ChirpStack. ChirpStack je LoRaWAN síťová aplikace s otevřeným zdrojovým kódem, který poskytuje jednotlivé komponenty pro vytvoření lokální sítě. Jedná se o řešení, které je možné jako modul implementovat do již vytvořené infrastruktury a nabízí přívětivé uživatelské rozhraní pro správu zařízení. Všechny komponenty této aplikace jsou pod licencí MIT a tudíž může být tato aplikace použita také pro komerční účely. Lokální sítě jsou využívány například v průmyslových halách, kde je potřeba přenášet data z koncových zařízení do jedné společné databáze za účelem následného zpracování. Data jsou z koncových zařízení skrze přístupové brány přenášena do lokálních síťových a aplikačních serverů, kde jsou data zpracovávána a nebo odkud se odesílají dále do nadřazených systému. V rámci této práce je jako přístupová brána, podobně jako u předchozího konceptu, použit router MikroTik RBwAPR-2nD&R11e-LoRa8. Jako průmyslový počítač, na kterém je síťový a aplikační server spuštěn je použito Raspeberry Pi 3, k tomuto zařízení je pak přístupová brána připojena. Uživatelské rozhraní v podobě webové stránky je také pro demonstraci spuštěno lokálně na Raspberry Pi 3. Koncové

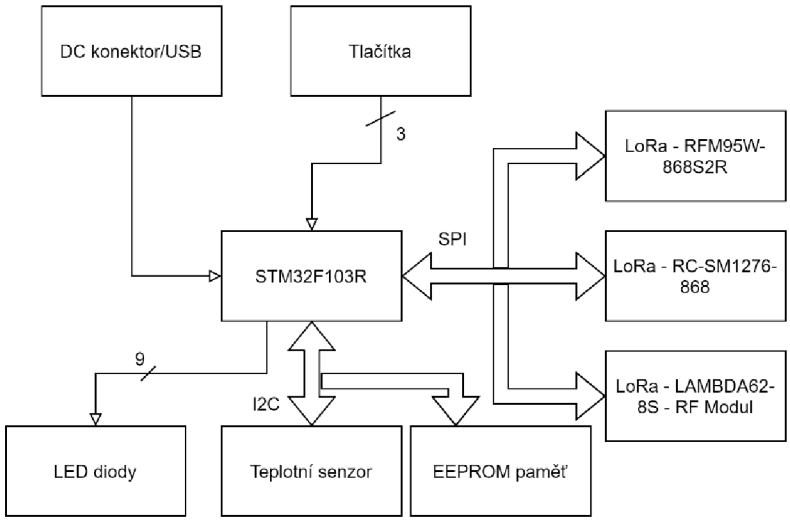
zařízení se podobně jako v předchozím konceptu připojuje přes gateway do lokální sítě kam odesílá svá naměřená data. Celý koncept systému lze vidět v blokovém schématu na obr. 13



Obr. 13. Blokové schéma realizovaného LoRaWAN systému na lokální síti ChirpStack

2.2 Blokové schéma koncového zařízení

Koncové zařízení je jedním z hlavních částí celého systému. Řízení celé DPS zajišťuje mikrokontrolér STM32 řady F, konkrétně pak STM32F103C. Tento mikrokontrolér pracuje na frekvenci až 72 MHz, disponuje třemi 16bitovými časovači, dvěma I2C sběrnicemi, třemi USART sběrnicemi a dvěma SPI s rychlostí až 18 Mbit/s. Důležitou částí tohoto zařízení je možnost výběru mezi třemi LoRa moduly, pomocí kterých dochází ke komunikaci s LoRaWAN gateway. Tři různé LoRa moduly jsou na tomto zařízení navrženy, také z toho důvodu, aby bylo možné testovat jejich parametry a vyhodnotit tak, který z nich přináší největší užitek v poměru cena/dosažený výkon. Zároveň se také použitím více různých LoRa modulů snižuje riziko na případnou opakovanou výrobu zařízení. Volit modul, který právě vysílá je možné za pomoci tlačítka, které je pro tento účel v zařízení navrženo a výběr daného vysílače indikuje jedna ze tří LED. Všechny tyto vysílače disponují vlastní externí anténou k dosažení lepších vysílacích parametrů, zejména pak většího dosahu radiového signálu, a jsou určeny k provozu na frekvenci 868 MHz, což je frekvenční pásmo vymezené v EU na provoz systémů s využitím technologie LoRa. Vysílače jsou vybrány od tří různých výrobců: RF SOLUTIONS, RADIOCONTROLLI a HOPE MICROELECTRONICS. Všechny tyto společnosti disponují licencí od společnosti Semtech na využívání této technologie. Moduly jsou k mikrokontroléru připojeny přes jednu společnou SPI sběrnici a jejich výběr je prováděn přes výběr čipu. V závislosti na tom, že je požadováno, aby bylo zařízení přenosné, je pak celá DPS napájena přes bateriový zdroj 9 V. Toto vstupní napájení je pak na DPS stabilizovány na napětí 3,3 V. Posledním modulem na tomto zařízení je modul teplotního senzoru. Tento senzor je k mikrokontroléru připojen také přes sběrnici SPI a je zdrojem dat, které jsou přes LoRu přenášeny do sítě a zobrazovány ve na jednoduché webové stránce. Blokové schéma koncového zařízení lze vidět na obr. 14.



Obr. 14. Blokové schéma koncového zařízení

2.3 Návrh vlastního koncového zařízení

Nezbytnou součástí této diplomové práce je návrh vlastního hardwaru v podobě koncového zařízení, které umožní použití v předchozí kapitole zmíněných LoRa modulů. Z širokého portfolia komerčně dostupných modulů byly nakonec vybrány tři LoRa moduly, které zajišťují možnost připojení pomocí sběrnice SPI. SPI sběrnice byla vybrána na základě potřeby komunikace s modulem ve vyšších rychlostech, než dovoluje například UART rozhraní, nebo I2C sběrnice. SPI sběrnice navíc oproti UART rozhraní zajišťuje možnost připojení více zařízení na stejnou sběrnici za pomoci pouze jednoho vodiče, a to navíc pro každý modul. Z pohledu zapojení byly z jednotlivých modulů vedeny ideálně všechny volné signálové cesty označené obvykle jako DIO. Tento krok byl učiněn s vidinou možnosti použití různých zdrojů přerušení, nebo podřadného řízení ze strany mikrokontroléru, případně i LoRa modulu.

Z hlediska elektrického zapojení bylo potřeba zohlednit strmé napěťové přechody na vedení, které mohou na digitálním vedení nastat a mohli by způsobit nechtěné komplikace. Z pohledu zapojení modulů a úvaze o možnosti bateriovém napájení je možno každý modul samostatně připojit k napájení nebo jej od napájení odpojit pomocí samostatného tranzistoru. Stejně tak je možné každý modul uvést do reset stavu za pomoci samostatného vývodu určeného k této funkci. Reset vývod LoRa modulů je multifunkčním vývodem, kde některé moduly nesmí mít přivedené externí kladné napětí. Za účelem splnění této podmínky je u každého modulu navržen obvod s tranzistorem, který dokáže reset vývod připojit na aktivní zem a tím LoRa modul uvést do reset stavu. Pro zachování funkcionality, je zároveň na reset vývod přiveden druhý vývod mikrokontroléru, sloužící ke čtení stavu tohoto vývodu.

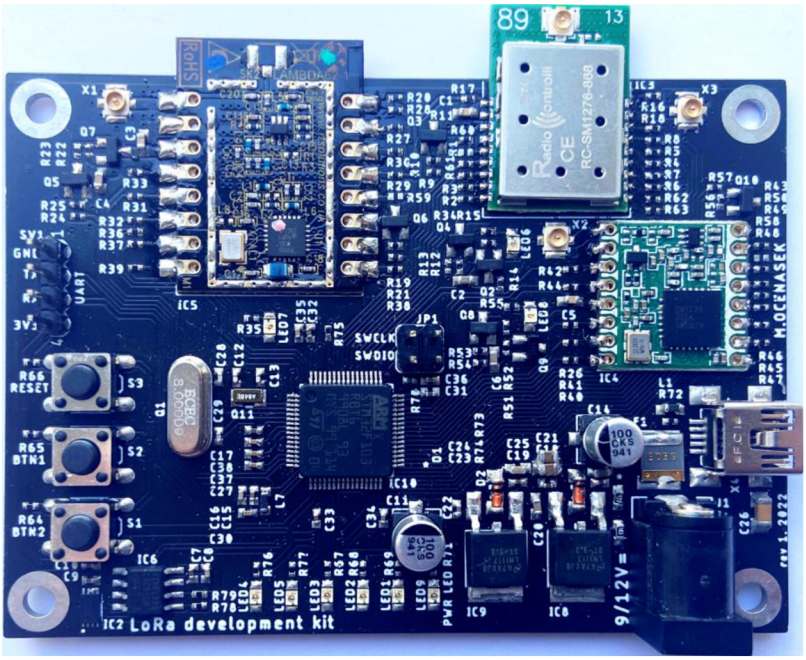
Jelikož jsou na navržené DPS použity celkem tři LoRa moduly, byla ke každému modulu připojena samostatná LED dioda signalizující stav jeho napájení. Mimo tyto signalizační LED diody jsou na DPS osazeny také další tři LED diody s univerzálním použitím, tyto LED jsou pak vedeny přímo na volné vývody mikrokontroléru. K těmto třem LED diodám jsou přivedeny ještě dvě další, celkem tedy pět uživatelských LED diod k signalizaci jakéhokoli požadovaného stavu. Tyto dvě další LED diody jsou multiplexované s vývody sériové linky, která je na DPS umístěna zejména pro účely snazšího ladění programu a případného rozšíření do budoucna. Na DPS je poté situována ještě jedna poslední LED dioda, která je určena k indikaci napájení celé DPS.

DPS byla navržena s důrazem na vyšší flexibilitu napájení, které je možno zavést pomocí dvou různých vstupů. První možností napájecího vstupu je USB port určený k připojení k záložnímu zdroji nebo k napájecí záložní bance. Tento USB vstup nemá zapojené datové linky a je použit pouze pro napájení DPS. Tomu je tak zejména z důvodu možnosti ušetření volných vývodů mikrokontroléru, které je možné díky možnému použití zařízení v osamostatněném zařízení bez osobního počítače nebo jiného zařízení, kde by USB připojení dávalo smysl. Druhým napájecím vstupem je tzv. barel konektor sloužící pro připojení stejnosměrného vstupního napětí s rozsahem mezi 9 V a 12 V nominálních, nebo 5-15 V celkově. Tento konektor je předpokládaným hlavním napájecím konektorem, kdy zařízení by mělo být napájené z externí 9 V baterie připojené právě k tomuto konektoru.

Z pohledu finálního použití DPS se jedná zejména o demonstrační konstrukci zapojení, které bude sloužit primárně k výuce a případně také k ladění komunikace na frekvenčním pásmu 868 MHz, čemuž napomáhá i možnost použití jednoho ze tří různých LoRa modulů. K demonstraci nebo testování těchto LoRa modulů je možné použít hned několik zdrojů informací, které lze následně v rámci komunikace zasílat. Těmito zdroji jsou například digitální teplotní čidlo LM75, které bylo přidáno na I2C sběrnici mikrokontroléru a které slouží jako zdroj dat o teplotě DPS v místě, kde není DPS ničím teplotně zatěžovaná. Změřená teplota tak může být považována za teplotu okolí, pokud zařízení nebude v krabičce. Druhým zdrojem informací jsou celkem dvě uživatelská tlačítka, která jsou připojena přímo na vývody mikrokontroléru a nemají žádnou konkrétní funkci. Díky tomu je možné je použít pro libovolný účel, pro který je bude ve finální aplikaci potřeba. Posledním možným zdrojem informací je možnost měření vstupního napětí na napájecím konektoru, které je přivedeno na AD převodník použitého mikrokontroléru. Měřené napětí má v obvodu zařazen pouze jednoduchý RC filtr tvořený částí děliče samotného a malým kondenzátorem k odstranění rušení. Díky tomu je možné měřit přesné vstupní napětí nezatížené téměř žádnou chybou a měření lze považovat za plně dostačující k reálnému stanovení například životnosti akumulátoru.

Použité periferie, sloužící jako zdroj informací jsou velice vhodné pro otestování a demonstraci funkce vysílání na frekvenci 868 MHz, na které LoRa moduly vysílají. Pro demonstraci a testování možnosti příjímání dat ze sítě, ať už lokální, nebo internetové, je na DPS implementována pouze pětice LED diod popsaných výše a také malá EEPROM paměť. Tato paměť je připojena na I2C sběrnici spolu s teplotním senzorem a její účel je zejména možnost logování přijatých dat. Použitá paměť má kapacitu 64 kb neboli 8 kB. Tato kapacita je pro logování dat přijatých LoRa moduly určena jako plně dostačující, jelikož i datová propustnost této sítě je velmi malá a díky účelu zařízení jakožto demonstrační a výukové zařízení není důvod testovat například roční zápis velkého množství dat s využitím celého povolené střídy na ISM pásmu.

Jako hlavní řídící člen celé DPS bylo potřeba vybrat vhodný mikrokontrolér. Vybraný mikrokontrolér nemusí pracovat se složitým datovým zpracováním, ani se zpracováním velkého množství různých datových komunikací. Z tohoto důvodu nebylo tedy potřeba volit drahé, ani vysoce výkonné mikrokontroléry. Z výše uvedených požadavků a z hlediska možností daného zařízení vyplívá, že vybíraný mikrokontrolér musí splňovat podmínku dostatku vývodů pro obsluhu všech potřebných periferií, musí mít minimálně jedno I^2C rozhraní a jedno SPI rozhraní. Z pohledu parametrů vybraných LoRa modulů je potřeba vybírat mikrokontrolér s napájením o velikosti 3.3 V, aby nebylo potřeba používat posuvníky úrovní nebo buffery na vedení. Vybraný mikrokontrolér by měl také podporovat různé nízko-příkonové režimy. Z dostupných mikrokontrolérů byl proto vybrán mikrokontrolér typu STM32F103RBT6, splňující všechny vyjmenované podmínky a omezení. Vybraný mikrokontrolér je navíc dostatečně rychlý, kdy při maximálním příkonu může pracovat s frekvencí jádra až 72 MHz. K umožnění operace v této frekvenční třídě je potřeba použít externí krystal, zajišťující vstup externího taktovacího kmitočtu do PLL periferie, jelikož interní oscilátor neumožní tak vysoké vynásobení a frekvence jádra by byla maximálně 64 MHz. Z pohledu počtu vývodů je tento mikrokontrolér plně dostačující, a navíc, i po zapojení všech potřebných periferií, zbyde dostatek volných vývodů k osazení externího krystalu zajišťujícího i taktovací signál pro obvod reálného času, který může zajistit například další datový vstup pro komunikaci přes LoRa moduly, nebo k zajištění časové značky u přijatých dat. Z pohledu energetické spotřeby mikrokontroléru nelze obvod zařadit mezi zvláště úsporné, nicméně při pod-taktování jádra, vypnutí některých periferií anebo přechodu do jednoho z několika možných nízko-příkonových režimů je možno dosáhnout velmi nízkého příkonu, kdy díky RTC je možné mikrokontrolér v pravidelné okamžiky probouzet za účelem například zaslání pravidelného balíčku dat přes dostupné LoRa moduly. Na obr. 15 je pak možné sledovat již osazenou DPS vlastního koncového zařízení.



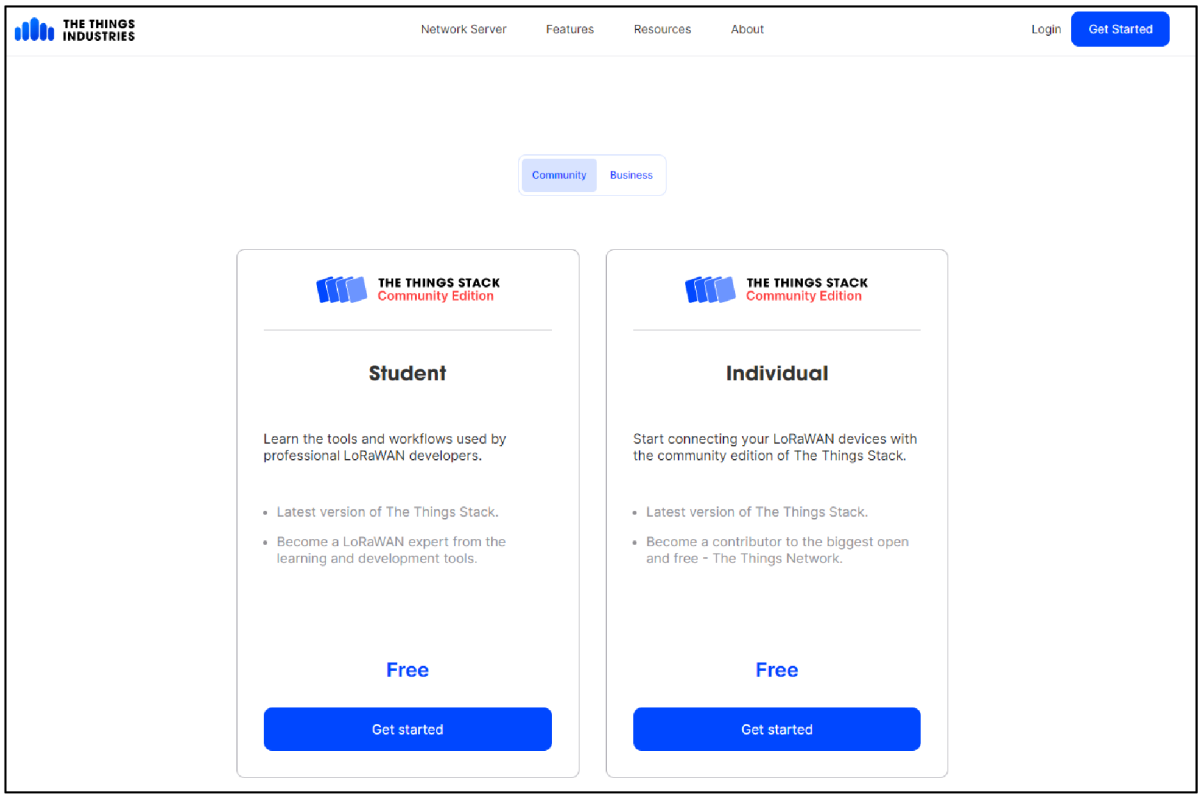
Obr. 15. Osazená DPS vlastního koncového zařízení

2.4 Postup realizace systému s využitím LoRaWAN sítě TTN

Tato kapitola se věnuje uvedení systému s využitím sítě TTN do provozu. Popisuje konfiguraci přístupové brány, nastavení profilů přístupové brány a koncového zařízení v rozhraní TTN, testování připojení k síti přes LoRa tester, připojení a popis vlastního koncového zařízení a postup pro zobrazení získaných dat z koncového zařízení na uživatelském webovém rozhraní.

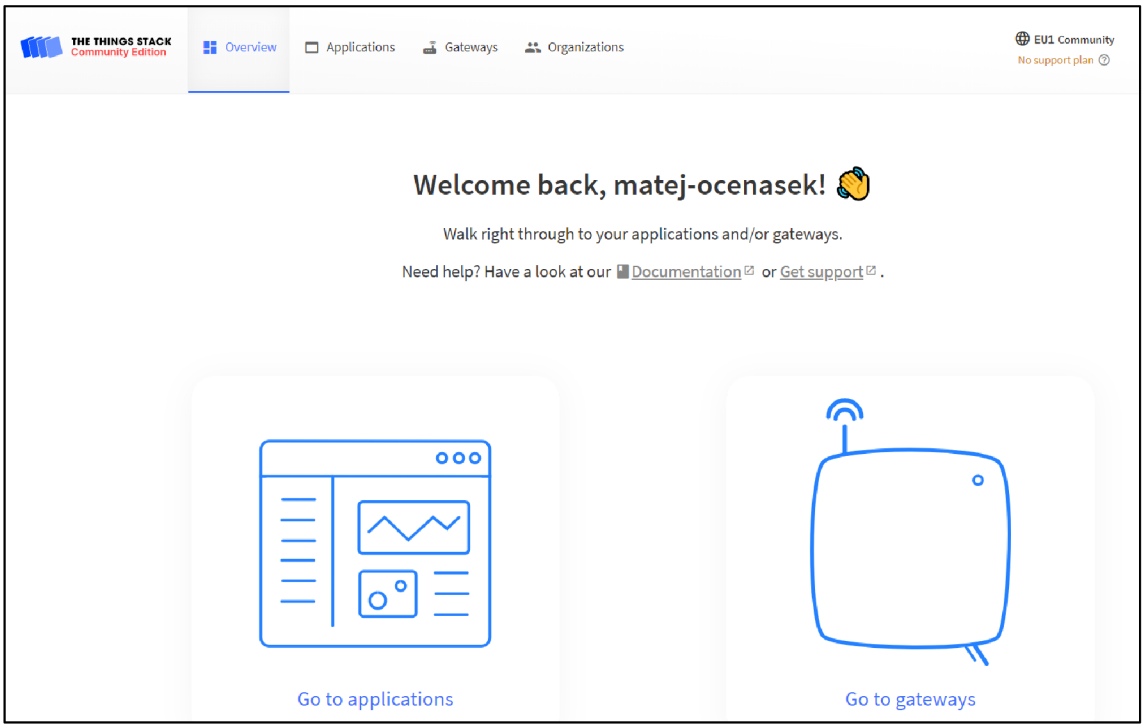
2.4.1 Připojení a konfigurace přístupové brány

K tomu, aby bylo možné používat síť TTN pro provoz ať už vlastních koncových zařízení, které se mohou do sítě připojit přes přístupové brány jiných uživatelů v síti, nebo vlastních přístupových bran, které mohou být užitečné i pro ostatní uživatele, je nezbytné si vytvořit uživatelský profil v jedné z možných kategorií. Na výběr je ze dvou kategorii, a to komunitní profil, nebo profil podnikový. Za účelem zpracování této diplomové práce byla zvolena kategorie komunitní, s typem profilu student. Uživatelský profil se pak registruje na webové stránce organizace TTN, a to na www.thethingsindustries.com, náhled kategorií je možné vidět na obr. 16.



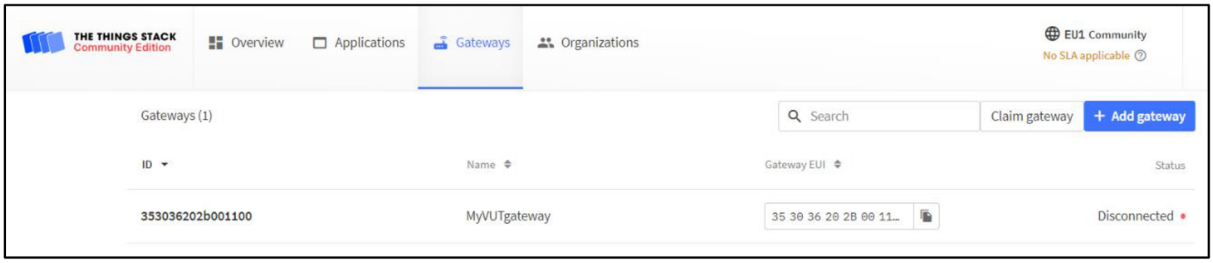
Obr. 16. Volba kategorie uživatelského profilu na webu TTN

Pro započetí registrace je potřeba kliknout na modře označené tlačítko „Get started“. V následujícím kroku je nutné vybrat kontinent, pod kterým bude profil uložen v databázi. V případě potřeby upřesnění doplňujících informací je možné kliknout na modře označené tlačítko „More information“. Po výběru kontinentu se otevře okno, ve kterém je nezbytné vyplnit registrační formulář, a to uživatelské jméno, emailovou adresu a heslo. Následně je na zadaný email odeslaný verifikační email, který je nutné do definované doby potvrdit. V případě, že registrace proběhla správně, ukáže se v internetovém prohlížeči okno, které je možné vidět na obr. 17.



Obr. 17. Okno výběru nastavení

Pro to, aby bylo připojení vlastní přístupové brány do sítě možné, je nejprve nutné přístupovou bránu zaregistrovat. V prvním kroku je potřeba kliknout na ikonu přístupové brány s označením „Go to gateway“, které je možní vidět na obr. 17.



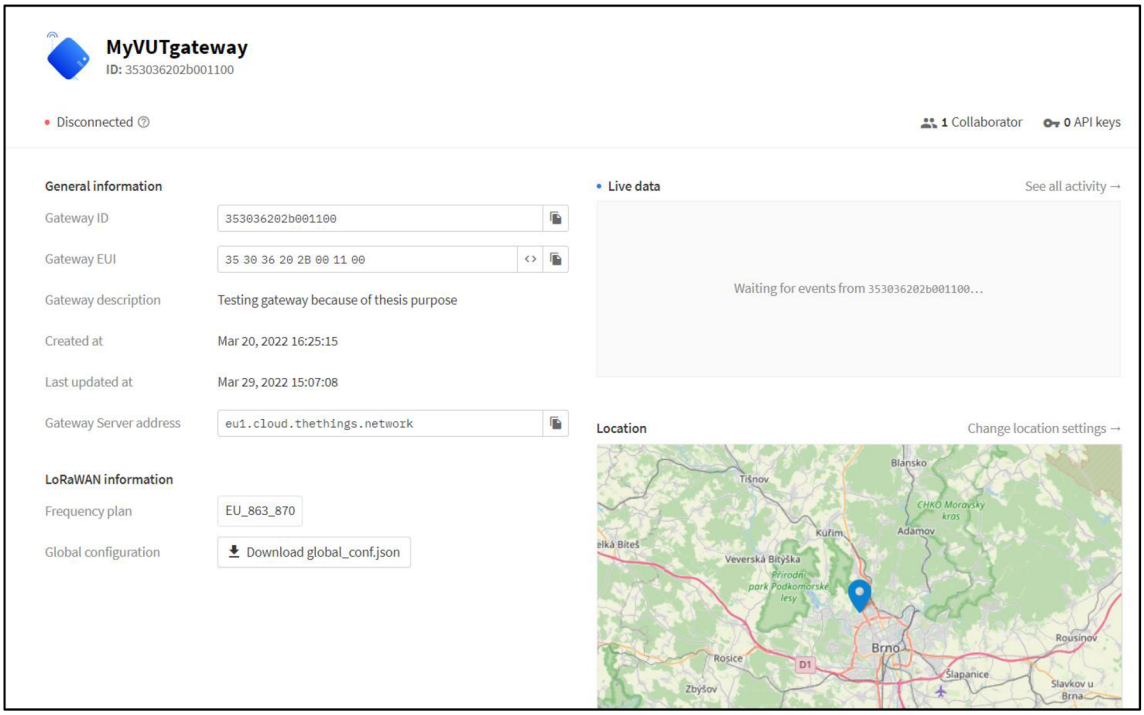
Obr. 18. Webové okno pro výběr nebo registraci nových přístupových bran

V druhém kroku je potřeba kliknout na modře označené tlačítko „+ Add gateway“, které je možné vidět na obr. 18. Následně je potřeba vyplnit jednotlivé údaje náležící nově registrované přístupové bráně. Potřebné údaje jsou „Gateway ID“ – jedná se o unikátní identifikační název přístupové brány. V případě, že je přístupová brána zrušena/smazána, nelze tento název už nikdy použít, a to kvůli duplicitě, tento parametr musí být nezbytně doplněn. „Gateway EUI“ – jedná se o 64bitový prodloužený identifikační kód, tento kód je zpravidla dodáván výrobcem dané přístupové brány a je uveden buď na zařízení samotném, nebo v návodu na příbalovém letáku. Aby bylo

možné přístupovou bránu spárovat se serverem, musí být tento parametr zadán. „Gateway name“ – libovolný název přístupové brány, který je i pro ostatní uživatele sítě viditelný, pokud je přístupová brána nastavena jako veřejná. „Gateway description“ – krátký popis přístupové brány, na co je určena. „Gateway Server address“ – adresa serveru, ke kterému je daná přístupová brána připojena, tento parametr se nastavuje v nastavení routeru, který pak slouží jako přístupová brána. „Require authenticated connection“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, pak může být přístupová brána připojena pouze v případě, pokud používá TLS s povolenou základní stanicí, nebo spojení přes MQTT. „Gateway status“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, nastaví se status přístupové brány na veřejný, a to umožní využití této přístupové brány i pro ostatní koncová, zároveň to také umožní sdílení informací o této přístupové bráně ostatním uživatelům sítě. „Gateway location“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, stane se poloha přístupové brány veřejná i pro ostatní uživatele sítě. „Attributes“ – tento parametr lze použít k nastavení libovolných informací o entitě, nejedná se o povinný parametr. „Frequency plan“ – v tomto okně dochází k výběru frekvenčního pásma, na kterém bude následně přístupová brána schopná přijímat datové balíčky z koncových zařízení. Vzhledem k tomu, že je přístupová brána provozována v Evropě, je nutné nastavit komunikační pásmo na frekvenci 863–870 MHz, toto pásmo je totiž na provoz LoRa zařízení v Evropě určeno. K provozu LoRa zařízení dochází na ISM pásmu, tento parametr musí být nastaven. „Schedule downlink late“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, povolí se vyrovnávací paměť pro stahování zpráv na straně serveru. „Enforce duty cycle“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, bude síťový server plánovat zprávy pouze s ohledem na omezení pracovního cyklu zvoleného frekvenčního plánu. „Schedule any time delay“ – tento parametr nastavuje zpoždění přístupové brány, přičemž minimální možné zpoždění je 130 ms, nastavení tohoto parametru je povinné. „Automatic updates“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, pak se přístupová brána může aktualizovat automaticky.

K nastavení polohy přístupové brány na mapě dochází v samostatném nastavení. Podobně jako u nastavení přístupové brány samotné je i u nastavení polohy nezbytné nastavit několik parametrů. „Location privacy“ – pokud dojde k zaškrtnutí tohoto zaškrtávacího políčka, nastaví se poloha přístupové brány jako veřejná, to znamená, že bude viditelná i pro ostatní uživatele v síti. „Location source“ – možnost výběru zdroje pro získání polohy přístupové brány. Tento zdroj lze nastavit dvěma způsoby, a to manuálně anebo aktualizací ze status zprávy, za účelem tvorby této práce byl zvolen způsob manuálního nastavení. „Placement“ – jedná se nastavení toho, kde se přístupová brána nalézá, zda je jeho poloha vnitřní, vnější, nebo neznámá, v rámci testování sítě v této diplomové práci byla přístupová brána umístěna uvnitř budovy. Ručně museli být nastaveny parametry zeměpisná šířka, zeměpisná délka a nadmořská výška, tyto

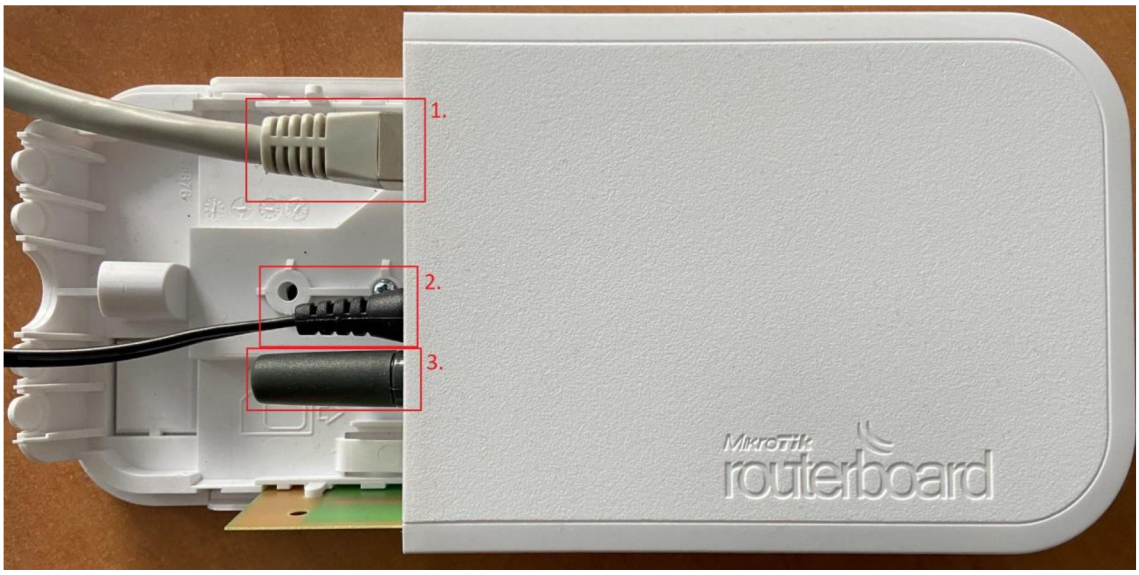
parametry lze získat za pomoci nástroje „měření vzdálenosti a plochy“ na webových stránkách mapy.cz.



Obr. 19. Výchozí nastavení přístupové brány na webu TTN

Na obr. 19 je zobrazeno uživatelské rozhraní již nastavené předpřipravené přístupové brány před prvním připojením routeru do sítě. Na pravé straně obrázku je možné sledovat přenos dat skrz přístupovou bránu do sítě a jeho polohu. Po levé straně je možné vidět již nastavené parametry přístupové brány.

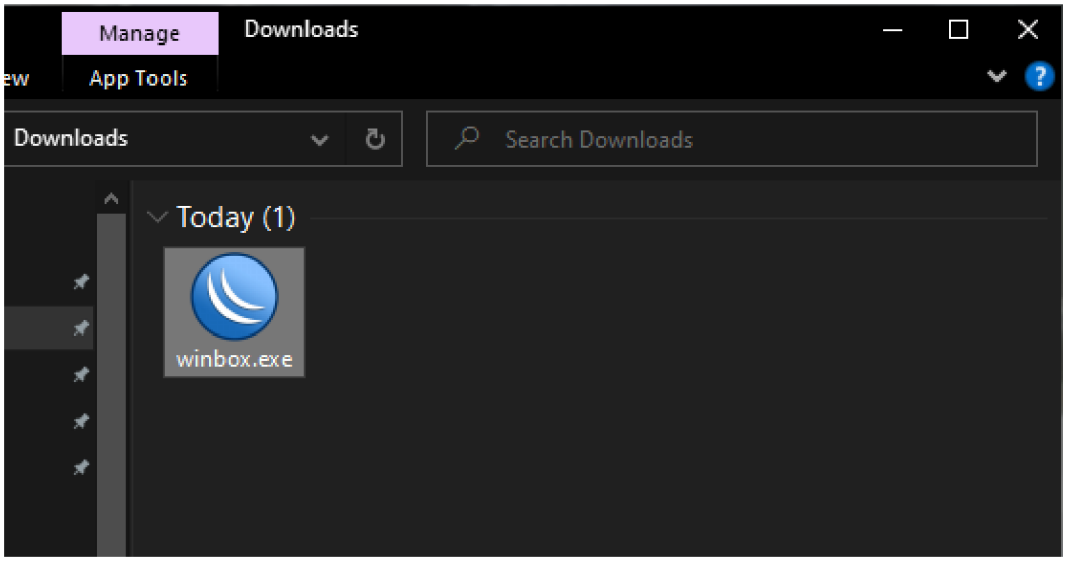
Ve třetím kroku je potřeba zprovoznit samotný router Mikrotik wAP LR8 kit tak, aby se následně dal nastavit jako přístupová brána LoRa.



Obr. 20. Router Mikrotik s popisem zapojeného příslušenství

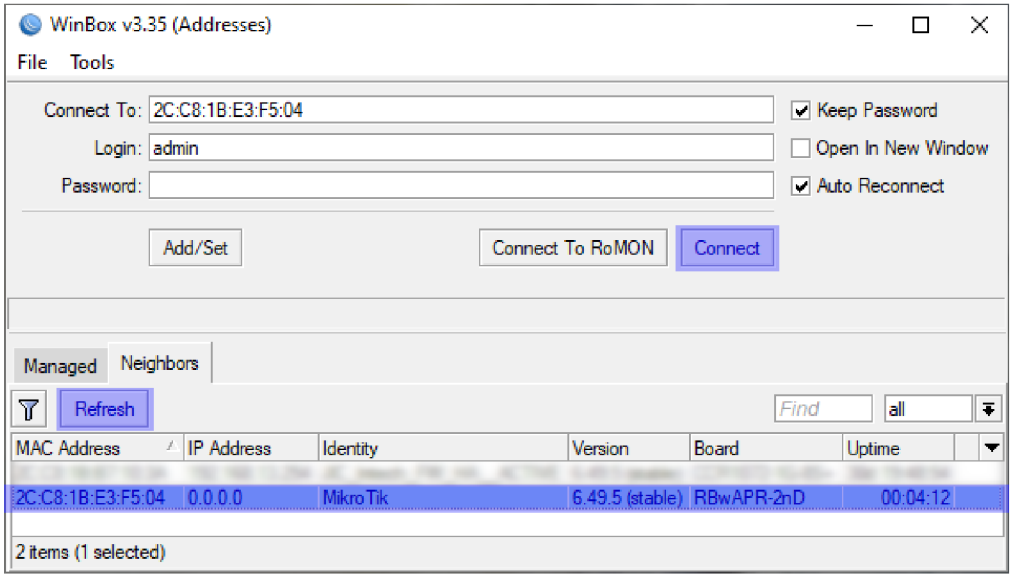
Na obr. 20 je vidět samotný router s číselně označenými konektory a anténou, které je potřeba připojit Po sundání horního krytování routeru je potřeba připojit přes RJ45 konektor router ke zdroji internetového připojení, tento konektor s kabelem je označen číslem 1., následně je nutné připojit router do napájecí sítě, router je napájen 24 V adaptérem, připojení je na obrázku označeno číslem 2. Poslední částí, kterou je potřeba připojit je anténa pro příjem signálu, pro tuto aplikaci byla použita anténa AN-07 IQRF TECH, která má zisk 2,15 dBi má impedanci 50 ohmů a může být použita na kmitočtu 868 MHz, nebo 916 MHz, připojená anténa je na obrázku označena číslem 3. Předtím, než se provede první konfigurace routeru, je potřeba udělat tvrdý restart zařízení, který restartuje celý systém. Tvrdý reset zařízení se vyvolá tak, že po zapojení zařízení do sítě dojde ke stisku a držení označeného tlačítka reset. Toto tlačítko je pak drženo do doby, než k němu přiřazená LED nezačne blikat. Po zhruba 5 sekundách, co LED bliká se musí tlačítko uvolnit a dojde k samovolnému restartu routeru. Poté je možné provést na routeru novou požadovanou konfiguraci.

Ve čtvrtém kroku je potřeba na routeru Mikrotik provést novou konfiguraci a nastavit router jako přístupovou bránu LoRa. Aby bylo možné Mikrotik nakonfigurovat, je potřeba stáhnout a nainstalovat aplikaci, která k této konfiguraci slouží. Aplikace se jmenuje Winbox a je možné ji stáhnout z internetu přes libovolný internetový prohlížeč. Ikonu aplikace je možné vidět na obr. 21.



Obr. 21. Ikona aplikace Winbox v průzkumníku souborů

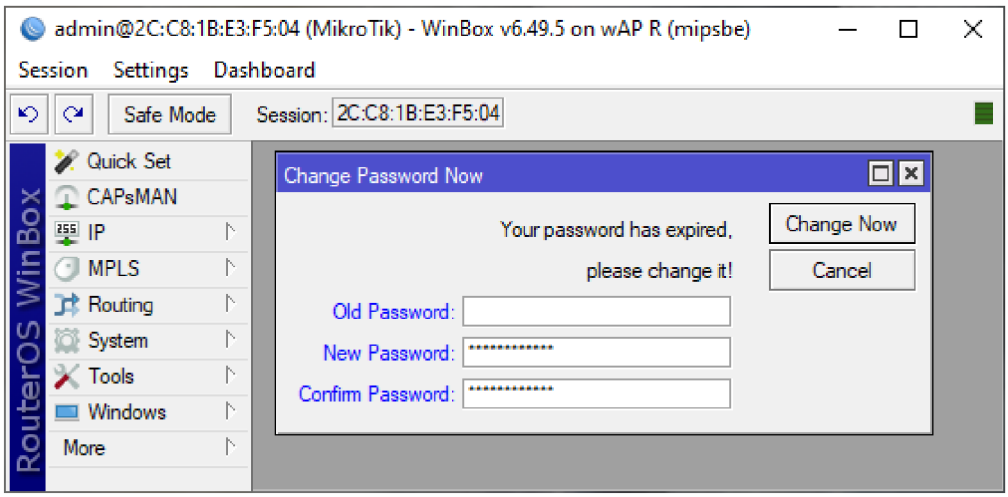
Po otevření aplikace se zobrazí okno, které je možné vidět na obr. 22.



Obr. 22. Výchozí přihlašovací okno přes aplikaci Winbox do routeru Mikrotik

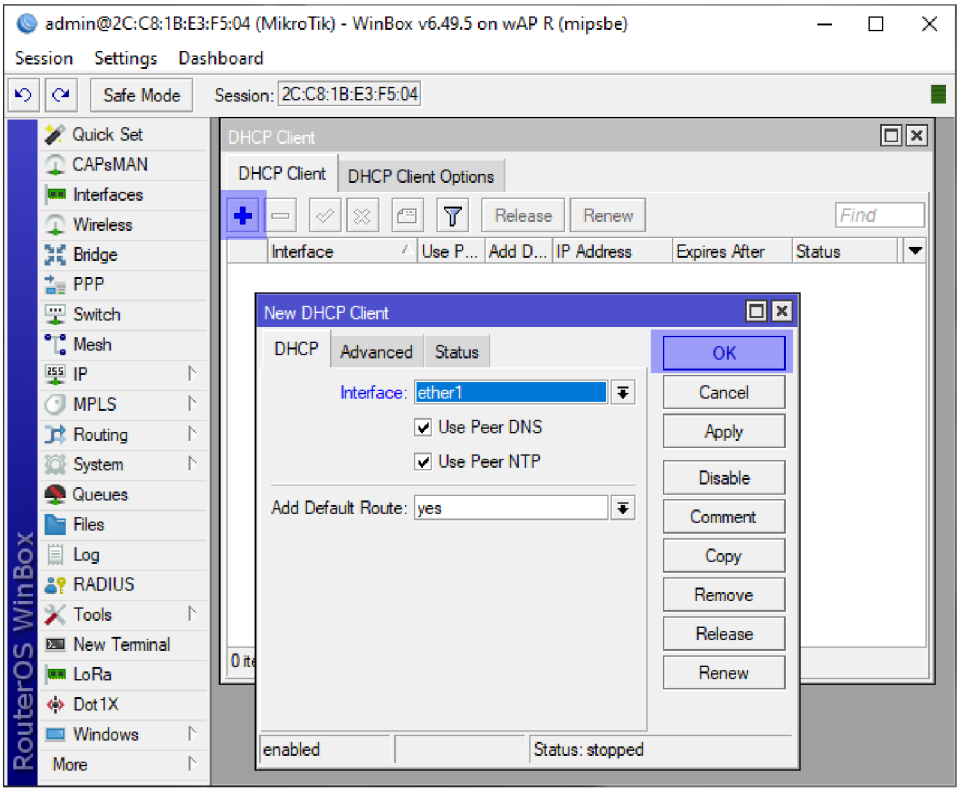
K tomu, aby bylo možné získat informace o aktuálně připojeném zařízení, je potřeba kliknout na modře označenou ikonu v levé části okna „refresh“, tak pak načte všechny informace o připojeném routeru. Modře označený řádek je IP adresa připojeného Mikrotik routeru. Pro prvotní přihlášení do konfiguračního menu aplikace je potřeba vyplnit přihlašovací údaje, a to jméno a heslo. Pro prvotní přihlášení se jako uživatelské jméno použije „Admin“ a heslo se nevyplňuje. Po vyplnění se k dalšímu kroku přejde

přes kliknutí na tlačítko „Connect“. V následujícím kroku je potřeba změnit heslo, jak je vidět na obr. 23, staré heslo zůstane nevyplněné.



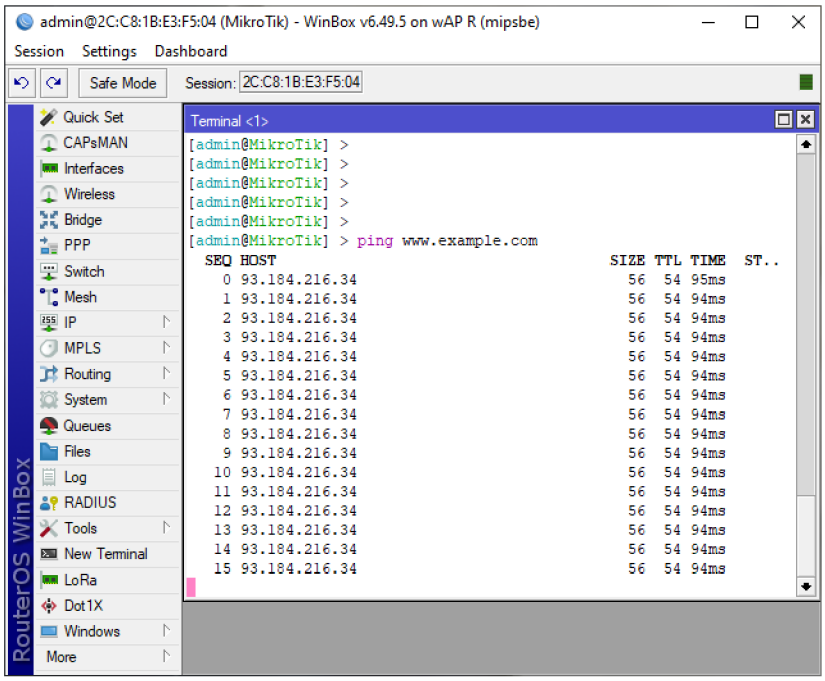
Obr. 23. Okno aplikace Winbox pro nastavení přístupového hesla

Jako první část nastavení routeru je potřeba nastavit internetové připojení, z toho důvodu bude potřeba nastavit DHCP klient. Do tohoto nastavení je možné se dostat tak, že se v levém postranním panelu zvolí záložka IP, ve které je zvolena možnost nastavení DHCP klienta. Po výběru tohoto nastavení se otevře okno DHCP Client, které je možné vidět na obr. 24. Pro přidání nového DHCP klienta je potřeba myší kliknout na modře označené tlačítko „+“. Poté se rozbalí nové okno s názvem „New DHCP Client“, všechny potřebné údaje jsou již automaticky předvyplněné, po kontrole správnosti údajů se nastavení odsouhlasí kliknutím na modře označené tlačítko „OK“



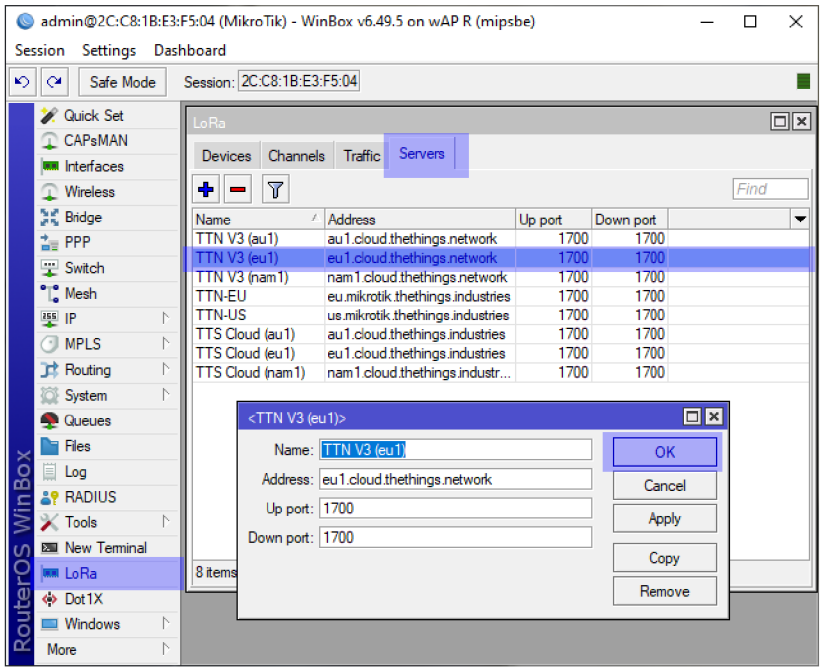
Obr. 24. Okno určené pro nastavení DHCP klienta

Pro kontrolu toho, zda nastavení proběhla správně je potřeba připojení k internetu ověřit. Ověření se provede tak, že v aplikaci Winbox spustíme funkci „New terminal“. Do konzole, která se následně otevře, zapíšeme „ping www.example.com“ a ověříme, zda komunikace s internetem funguje. Kladný výsledek, tedy že se router podařilo připojit k internetové síti, je možné vidět na obr. 25.



Obr. 25. Okno terminálu pro testování připojení routeru k internetu

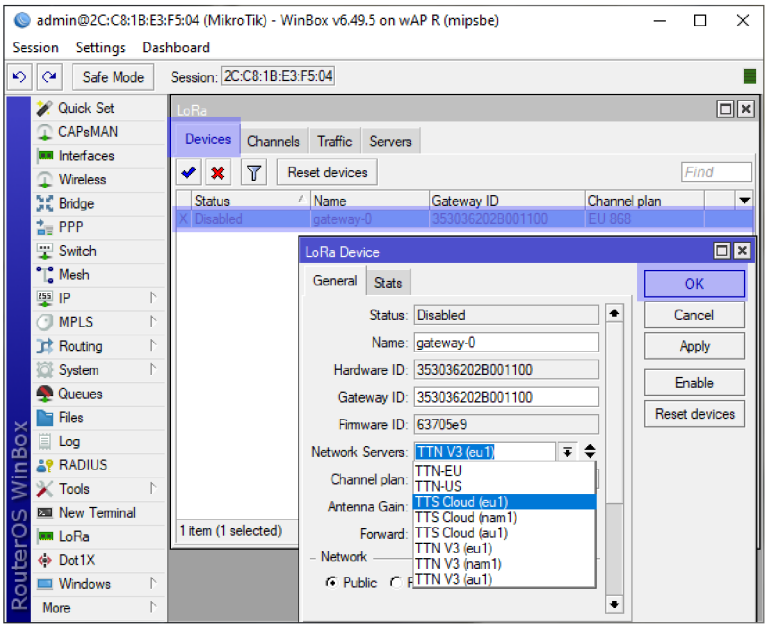
Poté, co je router připojen k síti, je v něm potřeba nakonfigurovat LoRa parametry, aby jej bylo možné připojit k síti TTN. Do nastavovacího okna je možné se dostat přes levý postranní panel. Poté, co se otevře výchozí okno, je potřeba přepnout na záložku „Servers“, tato záložka je zobrazena na obr. 26.



Obr. 26. Okno pro nastavování TTN LoRaWAN serverů

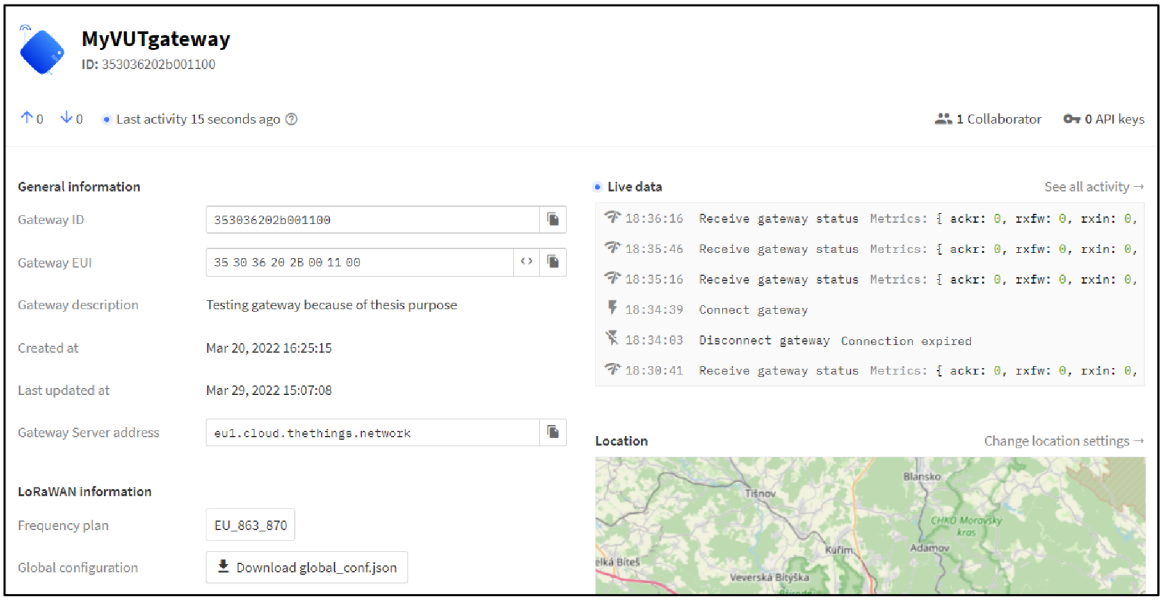
V záložce „Servers“ je nutné zkontrolovat nastavení sítě TTN V3 (eu1). Toto nastavení se kontroluje kvůli tomu, protože danému vytvořenému profilu na TTN byla přiřazena tato serverová adresa. V okně „<TTN V3 (eu1)>“ je potřeba zkontrolovat, zda souhlasí parametr „Address“, který by měl odpovídat adrese v profilu přístupové brány na stránkách TTN a zda sedí parametry „Up port“ a „Down port“, tyto parametry totiž definuje samotná TTN a neměli by být vyšší hodnotu než 1700. Pokud jsou všechny parametry korektní, je možné je odsouhlasit kliknutím na modře označené tlačítko „OK“.

V záložce „Devices“ je pak nutné zkontrolovat základní nastavení routeru. Na obr. 27 je možné toto nastavení vidět. Předtím, než se změní jakékoli nastavení je potřeba nastavit status routeru na „disable“, poté je možné dělat změny. Pokud by bylo nastavení routeru „enable“, nebylo by možné cokoli změnit a konfigurační program by vypsal chybovou hlášku. Poté, co je status routeru nastaven na „disable“ je možné změnit název, ten pak může být libovolný. Hardware ID / Gateway ID slouží jako jeden z parametrů, který je definován výrobcem. Tento parametr musí být shodný s parametrem Gateway EUI, který se nastavuje v uživatelském rozhraní na webu TTN. V parametru „Network servers“ je pak nutné vybrat správný server, v tomto případě pak TTT V3 (eu1). V nastavení „Channel plan“ je pak potřeba vybrat kanál tak, aby se adresa shodovala s adresou na rozhraní webu TTN, tedy eu1.cloud.thethings.network. Pokud jsou všechny parametry zapsány, je potřeba kliknout na tlačítko „Apply“, následně na tlačítko „Enable“, aby došlo ke spuštění LoRa zařízení na routeru, a nakonec okno potvrdit modře vyznačeným tlačítkem „OK“. V tento moment je veškeré nastavení přístupové brány LoRa hotové a může dojít k propojení s TTN sítí.



Obr. 27. Okno pro nastavení LoRaWAN parametru přístupové brány

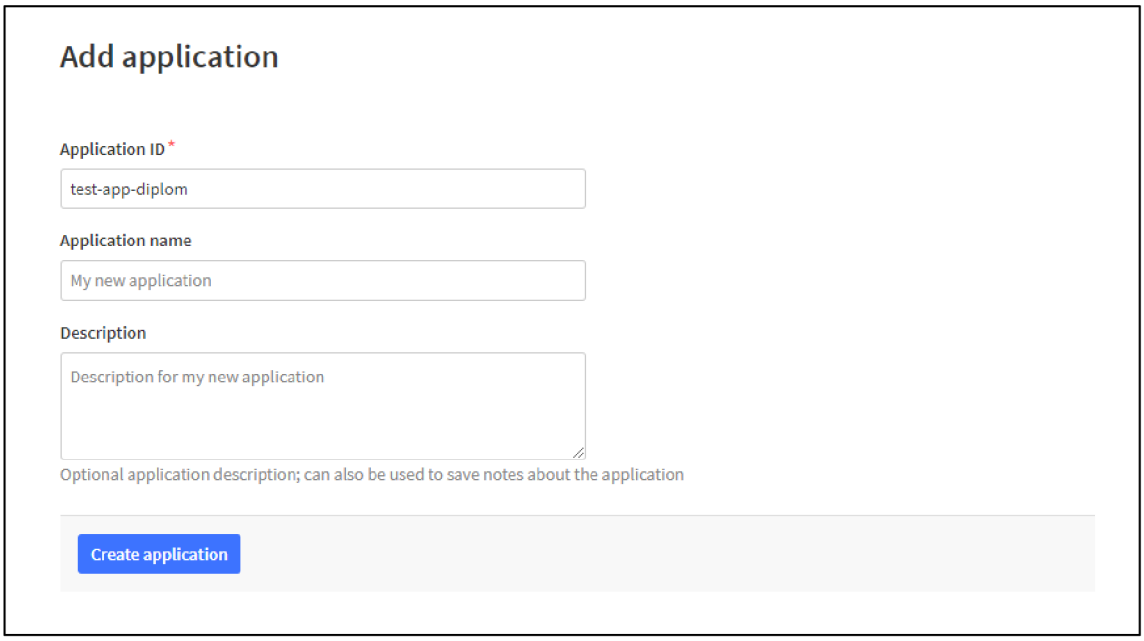
Jak je možné vidět na obr. 28 došlo k úspěšnému propojení routeru Mikrotik nastaveného jako přístupová brána LoRa se serverem TTN. Skrze tuto přístupovou bránu je možné přijímat data jak z vlastních koncových zařízeních, tak z koncových zařízení jiných uživatelů, protože je přístupová brána nastavená jako veřejná. Na pravé straně obrázku je možné sledovat data s časovou značkou, která skrze přístupovou bránu prošla na TTN server.



Obr. 28. Výchozí obrazovka nastavené přístupové brány připojené k síti TTN

2.4.2 Konfigurace aplikace – koncového zařízení

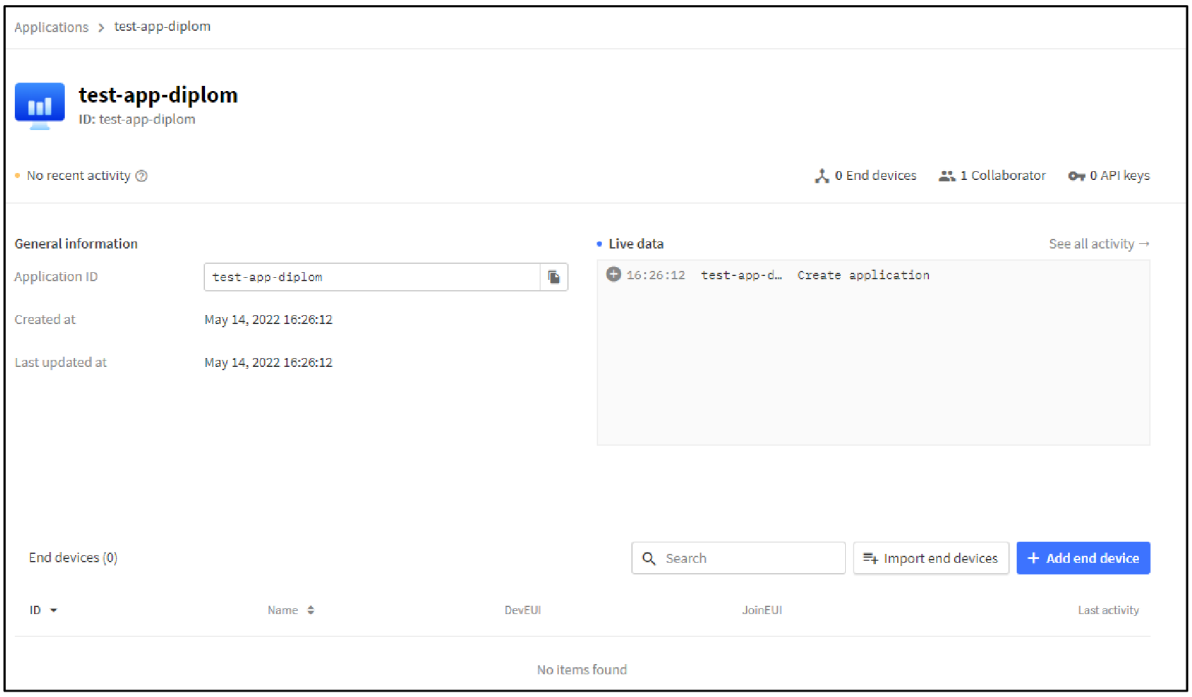
K tomu, aby bylo možné do sítě TTN přes přístupovou bránu připojit vlastní koncové zařízení, je potřeba takové zařízení v rámci sítě vytvořit. Na obr. 17, který je uveden v předchozí kapitole, je možné vidět graficky znázorněné tlačítko „Go to applications“. Přes kliknutí na toto tlačítko je možné se dostat do přehledového panelu všech již vytvořených aplikací. Pro vytvoření nové aplikace je potřeba kliknout na modře označené tlačítko v pravé části stránky „Add application“. Na následující stránce, která je zobrazena na obr. 29 je možné vidět parametry, které je potřeba k vytvoření aplikace nastavit.



Obr. 29. Nastavovací okno pro přidání aplikace pro koncové zařízení

Jediným povinným parametrem, který je potřeba vyplnit je Applicatin ID, tento parametr slouží pro rozpoznání vlastní aplikace v databázi ostatních aplikaci. U toho parametru je nezbytné dodržet předepsaný formát. Dále je možné, ale ne nezbytné, vyplnit parametr Application name, resp. název samotné zařízení a jeho popis. Pokud jsou všechny potřebné parametry vyplněné, je potřeba kliknout na modře označené tlačítko „Create application“ aby se aplikace vytvořila.

Po vytvoření aplikace se ve webovém prohlížeči objeví okno, které je možné vidět na obr. 30. V tomto okně je možné vidět základní parametry, jako ID aplikace, kdy byla aplikace vytvořena, kdy byla naposledy aktualizována a případné další informace, jako změny s časovou značkou v sekci „Live data“. Pro vytvoření nové koncové aplikace je potřeba kliknout na modře označené tlačítko „Add end device“

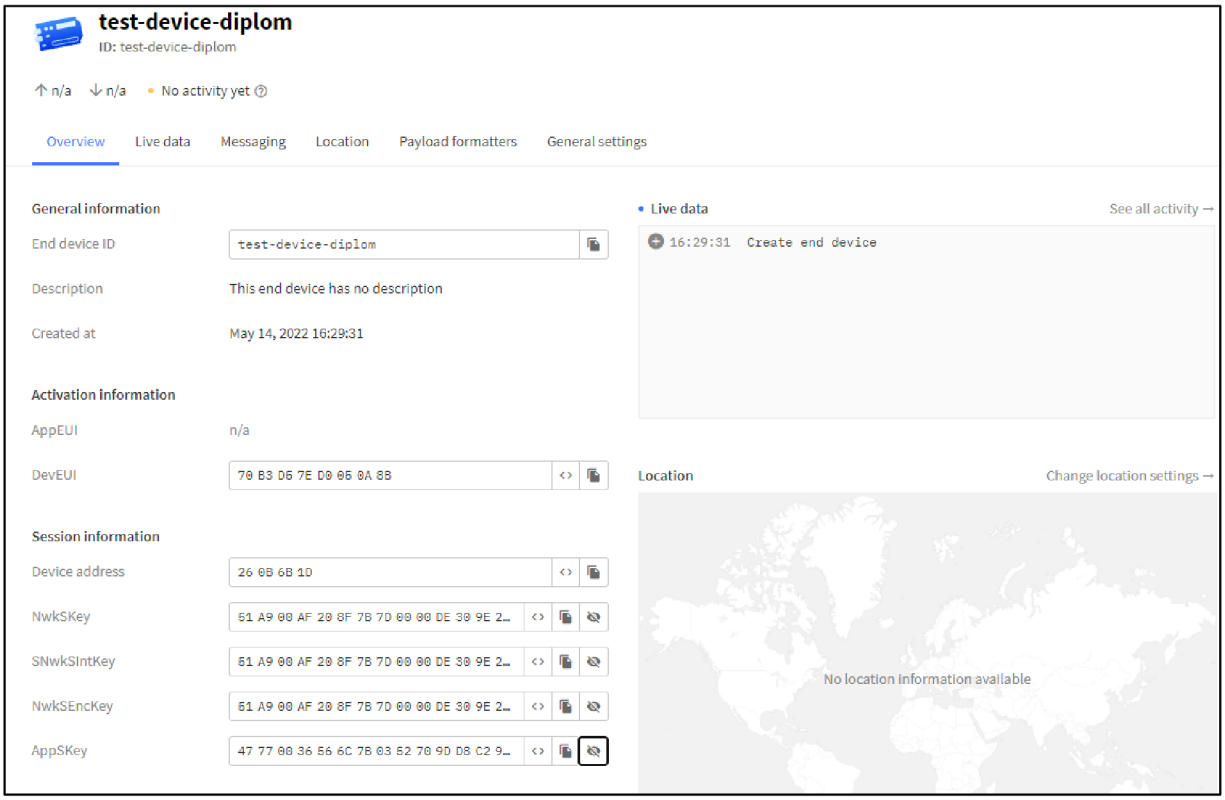


Obr. 30. Výchozí nastavení aplikace koncového zařízení

V okně pro přidání nového koncového zařízení je možný výběr ze dvou možností, a to LoRaWAN Device Repository, nebo manuální nastavení. V rámci této diplomové práce byla zvolena cesta manuálního nastavení požadovaných parametrů. Bylo potřeba nastavit povinný parametr frekvenční plán, tento parametr udává kontinent, na kterém k použití koncového zařízení dochází, frekvenční rozsah, na kterém zařízení komunikují a faktor rozprostření. Dalším povinným parametrem je LoRaWAN verze, tento parametr je již předvolený a doporučuje se použít verze „LoRaWAN Specification 1.0.0“. Parametr regionální verze se v rámci Evropy nevolí. V rámci rozšířených nastavení je pak potřeba zvolit aktivační mód. Koncové zařízení v této diplomové práci aktivaci typu ABP, z uvedených možností je tedy potřeba vybrat tento typ aktivace. Dále je potřeba zvolit LoRaWAN třídu, LoRaWAN totiž definuje tři třídy koncových zařízení, a to A, B a C. Třídu A pak musí mít implementovanou každé koncové zařízení v síti, tuto informaci o třídě zařízení je pak možné najít v katalogovém listu od výrobce daného modulu. Třída B a C jsou pak rozšířením třídy A, které specifikují jiné chování při přijmu zpráv ze serveru. Následně je potřeba zaškrtnout zaškrtávací políčko použití výchozího MAC nastavení. Toto nastavení definuje přijímací zpoždění, datové rychlosti, a komunikační frekvenci pro koncové zařízení. Tato výchozí nastavení jsou tvořena na základě doporučených nastavení pro vybranou lokaci, ve které bude zařízení používáno a ve většině případů jsou aplikace korektní. Dále je možné nastavit si vlastní klastr, pokud je to potřeba. Toto nastavení je vhodné spíše pro rozsáhle aplikace, které vyžadují vlastní back-end server. Poslední částí je generace klíčů DevEUI, Device address AppEUI, AppKey a nastavení End device ID. Vysvětlení jednotlivých typů klíčů je popsáno

v teoretické části této práce. Tyto klíče je potřeba vygenerovat, jsou pak v pozdější fázi nahrávány do paměti koncového zařízení jako jeden z parametrů pro připojení do sítě TTN. Parametr End device ID se generuje automaticky po vygenerování klíče DevEUI, jedná se o unikátní identifikátor pro koncové zařízení. V posledním kroku je potřeba kliknout na modře označené tlačítko „Register end device“, které koncové zařízení s uvedenými parametry zaregistruje do TTN databáze.

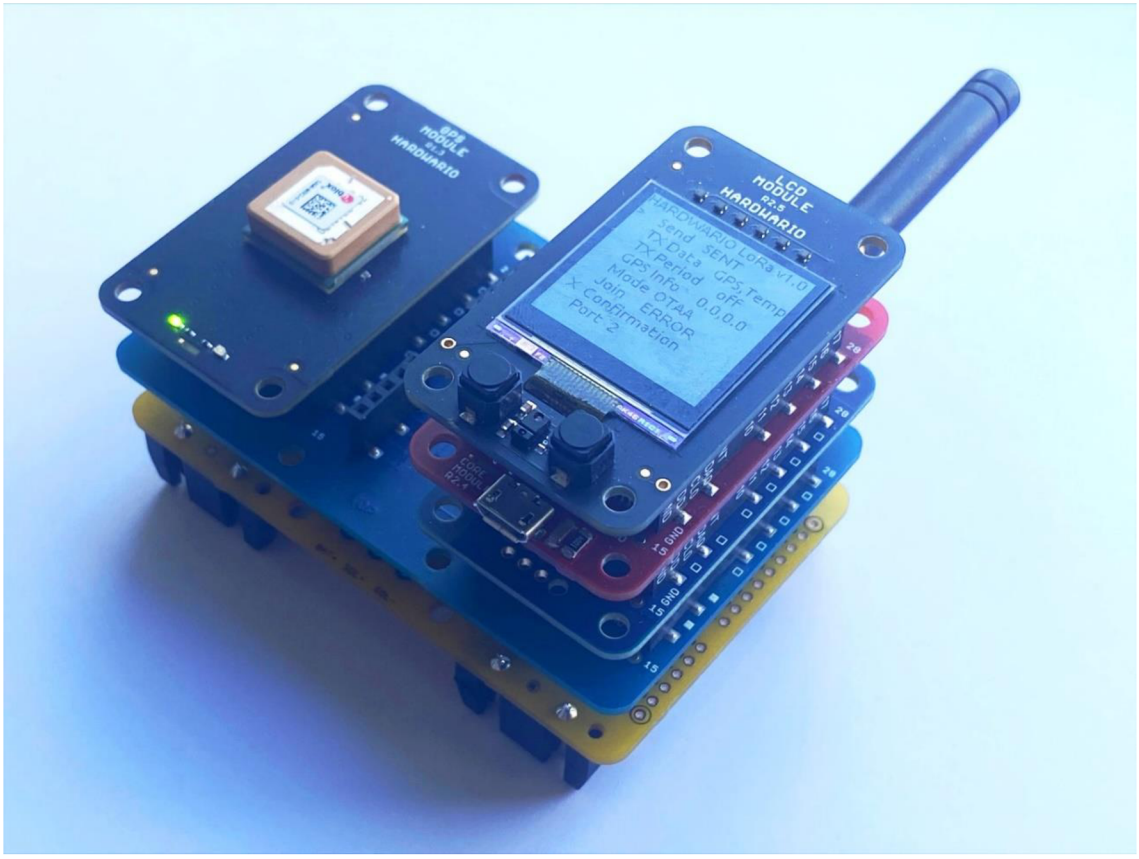
Na obr. 31 lze vidět konečné nastavení aplikace test-device-diplom společně s klíči pro konfiguraci koncového zařízení, ty lze kliknutím na ikonu oka dočasně zobrazit, případně je možní je kliknutím na ikonu listu papíru zkopírovat pro pozdější použití.



Obr. 31. Výchozí nastavení aplikace koncového zařízení s vygenerovanými klíči

2.4.3 Testování TTN sítě za pomoci komerčního LoRaWAN testeru

K tomu, aby mohlo být určeno, že je přístupová brána připojená do TTN sítě nakonfigurovaná korektně, a že i nastavení přístupové brány na straně TTN bylo nakonfigurováno správně, je potřeba připojit koncové zařízení do sítě tak, aby se přes přístupovou bránu byly datové balíčky schopné dostat na síťový server a uložili se do databáze. Aby bylo takové připojení možné, je potřeba mít vyrobený hardware koncového zařízení se spolehlivě funkčním softwarovým vybavením. Vzhledem k tomu, že konstrukce takového zařízení je součástí této diplomové práce, není tedy možné tvrdit, že bude toto koncové zařízení plně funkční a do TTN sítě se bez komplikací připojí. Pokud by se toto koncové zařízení nebylo do TTN sítě schopné připojit, není pak možné tvrdit, že je chyba na straně hardwaru koncového zařízení, nebo v softwaru tohoto zařízení, nebo na straně nastavení přístupové brány případně na straně samotné konfigurace sítě TTN. Vzhledem k těmto skutečnostem je výhodnější pro prvotní ověření funkčnosti přístupové brány a sítě TTN použít komerčně dostupné zařízení, u kterého existuje jistota, že má již vyladěné jak hardwarové, tak softwarové vybavení a je jak výrobcem, tak jinými uživateli v praxi vyzkoušeno, že funguje. Takovýmto zařízením je pak možné ověřit funkčnost jak přístupové brány, tak nastavení TTN sítě samotné. Pokud by se totiž ukázalo, že se takovéto testovací zařízení není schopno do sítě připojit, bylo by nejlepší cestou jít postupně hledat příčinu této chyby, která by se s největší pravděpodobností ukázala na straně nastavení TTN sítě, nebo přístupové brány. Takovéto zařízení lze na trhu koupit od různých výrobců z celého světa. Do této diplomové práce však bylo zvoleno zařízení LoRa tester od společnosti HARDWARIO, která se vývojem, výrobou a implementací LoRaWAN sítí v rámci České republiky zabývá. Zařízení od této společnosti bylo zvoleno také v důsledku české lokalizace a lokální podpory v případě problému s jejich zařízením. Tento LoRa tester je možné vidět na obr. 32.



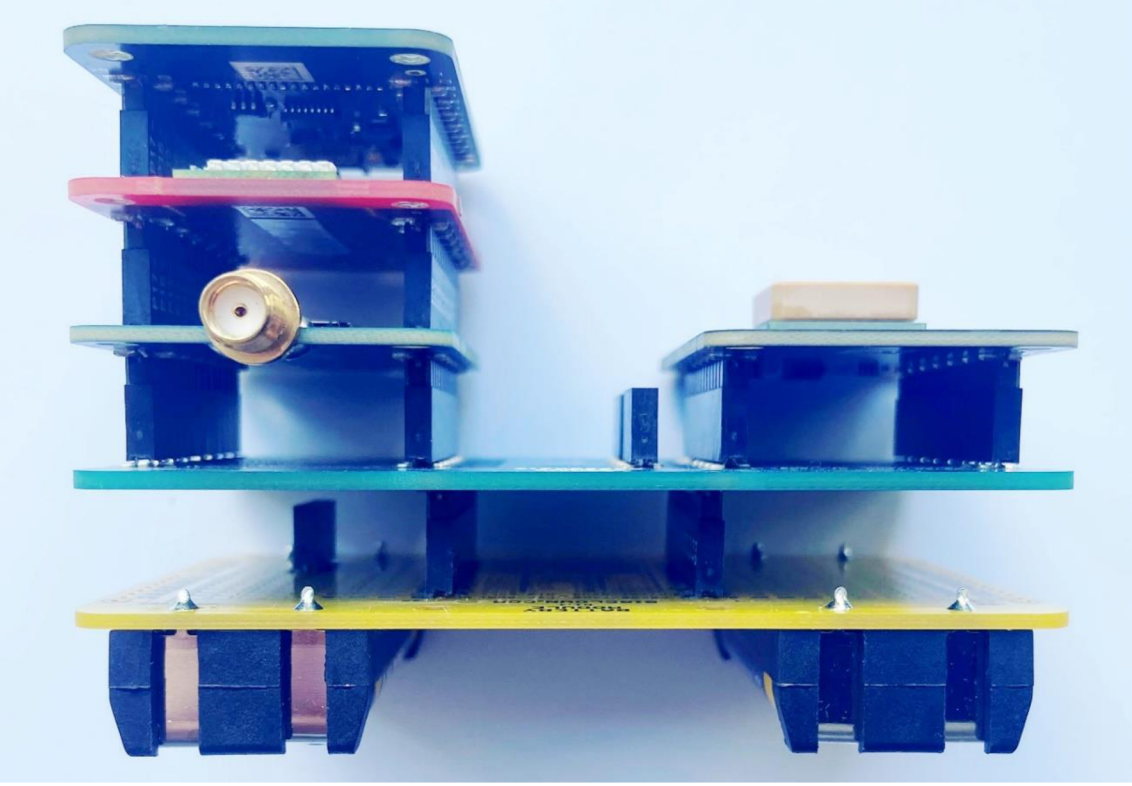
Obr. 32. Sestavený HARDWARIO LoRa tester

Jak již bylo zmíněno v předchozím odstavci, zařízení, které bylo pro testování TTN sítě a funkčnosti přístupové brány použito se nazývá HARDWARIO LoRa tester. Jedná se o konfigurovatelnou sestavu několika modulů, které se vzájemně propojují pomocí pinové lišty. Tyto moduly mohou být napájeny například z PC přes USB port, nebo je možné je za účelem mobility možné napájet bateriově skrze bateriový modul. Jednotlivá nastavení na LCD displeji je možné konfigurovat na jednom z modulů přes uživatelská tlačítka. Sestava se skládá z celkem šesti samostatných modulů, které lze vidět na obr. 33.

Obr. 33. Rozložená sestava všech HARDWARIO LoRa tester modulů

Sestava se skládá z celkem šesti výše vyobrazených modulů. Šedý modul s displejem a tlačítky slouží pro konfiguraci nastavení jednotlivých funkcí. Tento modul využívá tzv. „memory display“, který má rozlišení 128x128 pixelů při velmi malé velikosti displeje 1,28 palce. Zároveň má tento displej velice malý odběr elektrické energie, a proto je možné ho používat až několik hodin pouze z bateriových zdrojů. Červený modul slouží jako řídící pro celou sestavu, jedná se o modul, který je osazen mikrokontrolérem, ve kterém se nachází obslužný firmware. Na tomto řídím modulu se mimo mikrokontroléru nachází také periferie jako tříosý akcelerometr, nebo digitální teploměr. Tyto periferie pak mohou sloužit jako zdroj dat, které se mohou odesílat přes LoRa modul na server. Malý modrý modul je pak LoRa modul osazený modulem CMWX1ZZABZ-078 od společnosti Murata. Jedná se o radiový modul, ke kterému je přes SMA konektor možné připojit anténu a skrze něj následně odesílat data na server, tento modul stejně jako modul na vlastním koncovém zařízení komunikuje na frekvenci 868 MHz. Na plný provoz tomuto modulu stačí jen velice malé množství elektrické energie, a to 35 uA pro

vysílací režim. Černý modul je GPS modul, který je osazen GPS modulem SAM-M8Q od společnosti Ublox. Díky tomuto modulu je možné získat přesnou polohu celého složeného testeru. GPS modul je navíc kompatibilní se třemi globálními GPS standardy, a to s GPS, Galileo a GLONASS, modul je schopný měřit polohu s přesností na 2,5 metru. Velký modrý modul nese název „Split Modul“, jedná se o modul, který zajišťuje přenos dat mezi GPS modulem a hlavním řídícím modulem. Zároveň zajišťuje propojení s posledním žlutým modulem, což je bateriový modul, který po připojení čtyř AAA baterií zajišťuje pro všechny modul zdroj elektrické energie.



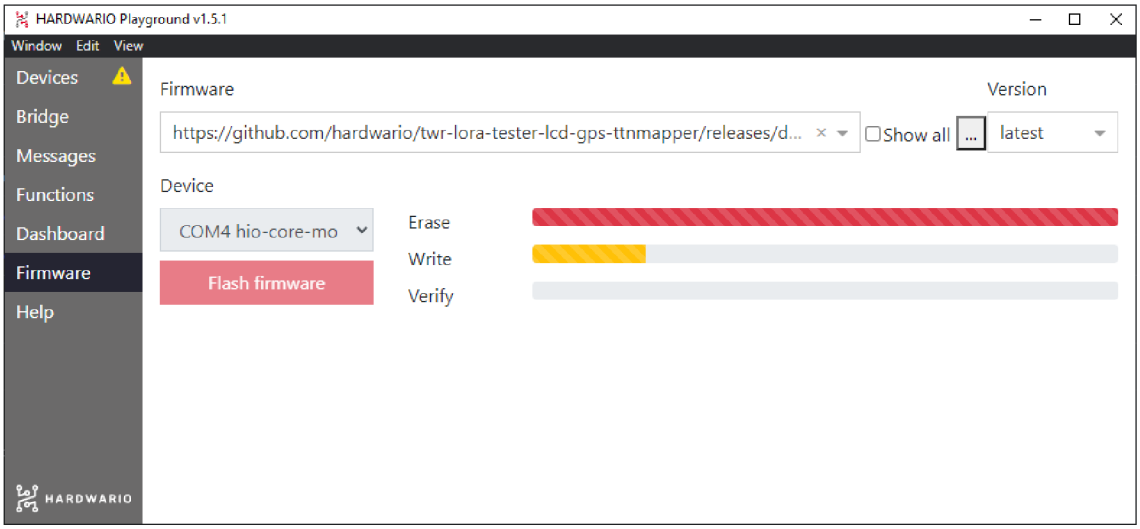
Obr. 34. Složený LoRa tester – pohled shora

Na obr. 34 je možné vidět již zapojenou sestavu LoRa tester modulů. Aby byla funkce korektní, je potřeba moduly zapojit právě v tomto určitém pořadí. Všechny moduly jsou orientovány potiskem na nepájivé masce tak, aby jejich název směřoval k pozorovateli a název byl z pohledu pozorovatele nahoře. Jako první je potřeba umístit Split modul do bateriového modulu. Následně je vhodné zapojit tři menší moduly zvlášť, aby se usnadnilo zapojení do modulu Split. Je tedy potřeba zapojit červeny hlavní řídící modul do modrého LoRa modulu, následně pak do červeného řídícího modulu zapojit šedý modul s displejem. Jakmile jsou tyto tři moduly složeny, je potřeba je z pohledu pozorovatele zapojit do levé části Split modulu. Černý GPS modul se pak z pohledu pozorovatele zapojuje do pravé části split modulu. To, že hardware funguje je možní zjistit připojením ke zdroji elektrické energie, a to buď přidáním baterií do bateriového

modulu, nebo připojením do PC nebo notebooku pomocí mini USB portu. Aby bylo možné se sestaveným LoRa testerem dále pracovat, je potřeba do něj nahrát konfiguraci, je tedy potřeba tento tester přes hlavní řídící modul připojit do počítače.

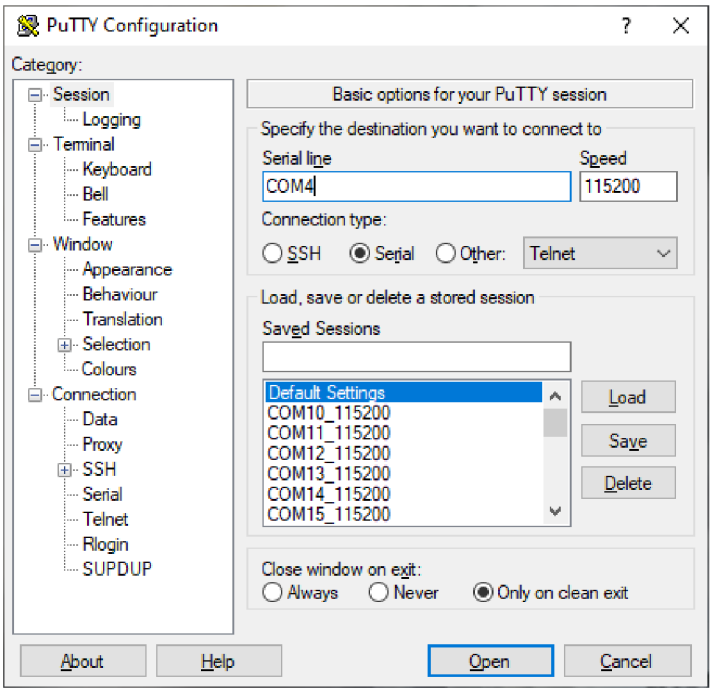
K tomu, aby bylo možné připojený HARDWARIO LoRa tester nakonfigurovat, je potřeba stáhnout z internetových stránek společnosti HARDWARIO počítačovou aplikaci s názvem „HARDWARIO Playground“. Tato aplikace slouží pro konfiguraci všech zařízení, které společnost Hardwario v rámci vyráběných stavebnic dodává Pomocí této aplikace je možné nahrát firmware do flash paměti mikrokontroléru, který se nachází na hlavní řídící DPS testeru. Modul jako takový je primárně dodáván bez výchozího firmwaru pro konkrétní aplikaci, případně v něm může být nahrán jednoduchý DEMO firmware pro demonstraci například blikající LED, nebo jiných základních funkcí hardwaru. Tester samotný je programovatelný modul, do kterého je možné nahrát různé aplikace k různému využití v potřebné koncové aplikaci. Za účelem testování LoRaWAN sítě TTN byl do modulu nahrán firmware, který zajišťuje obsluhu LoRa modulu, hlavní řídící jednotky a s ní souvisejících periferií. Firmware je dodávaný a spravovaný výrobcem, který ho průběžně aktualizuje. Tento firmware pak slouží k obsluze modulu s displejem, LoRou, GPS modulem a obsluze sériové linky skrz USB port. Tento zdrojový kód je tzv. „open-source“, tzn. volně dostupný a je možné ho použít bez licenčních poplatků.

Po spuštění aplikace HARDWARIO Playground je nutné přejít do záložky firmware. Tato záložka slouží k nahrávání vybraného firmwaru. Prvním možným zdrojem obrazu firmwaru může být soubor, který lze vybrat skrze dialogové okno, které je možné vyvolat kliknutím na tlačítko se třemi tečkami. Druhou možností je on-line metoda, kde se obraz nachází na GIT repozitáři. V případě použití metody s GIT repozitářem je zapotřebí do kolonky „firmware“ vložit úplnou URL adresu obrazu firmwaru. V této záložce se zároveň nastavuje „Device“, což je políčko, ve kterém se vybírá zařízení, do kterého se bude firmware implementovat. Toto políčko by se za normálních okolností mělo zvolit samo, pokud tomu tak není, je potřeba zkontrolovat připojení USB kabelu do zařízení. Uživatel by si měl zároveň tento port poznamenat pro pozdější použití. V rámci této diplomové práce byl použit způsob implementace firmwaru přes GIT repozitář. Tento repozitář spravuje společnost HARDWARIO, která je jeho autorem. Je tedy potřeba se na hlavní webové stránce github.com prokliknout do repozitáře „hardwario“. V tomto repozitáři je následně potřeba vyhledat “twr-lora-tester-lcd-gps-ttnmapper”. Poté, co se tato složka na gitu objeví, je potřeba vybrat podsložku, ve které je uložena vydaná verze firmwaru 1.1. po nakliknutí do této složky je potřeba zkopírovat URL adresu „twr-lora-tester-lcd-gps-ttnmapper-v1.1.0.bin“ která se následně vkládá do aplikace HARDWARIO playground. Výsledné okno pro implementaci firmwaru je možné vidět na obr. 35.



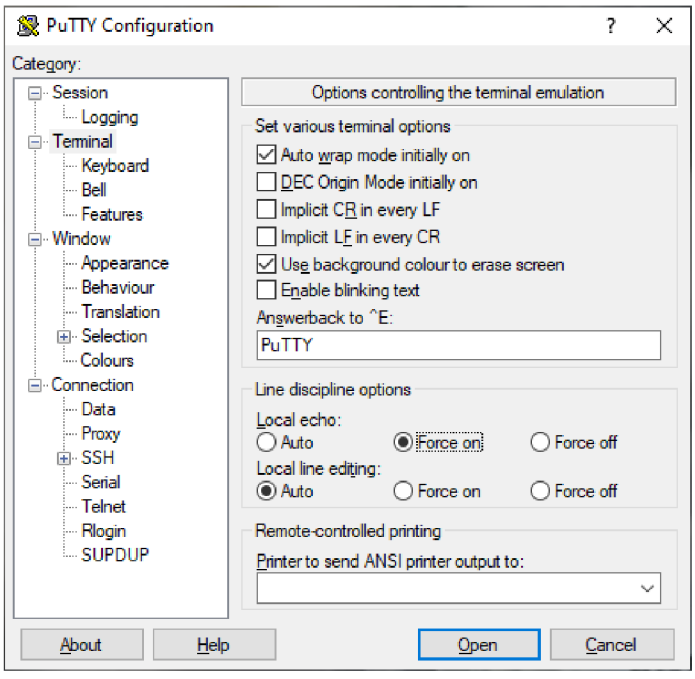
Obr. 35. Okno aplikace HARDWARIO playground – záložka firmware

V tento moment zavřeme okno aplikace HARDWARIO Playground. Pro další konfiguraci LoRa testeru je potřeba použít aplikaci PuTTY. Tuto aplikaci je možné stáhnout z internetu za pomoci libovolného webového prohlížeče. Jedná se o terminál pro komunikaci po sériové lince. Po tom, co je tato aplikace stažena, nainstalována a spuštěna, je potřeba v ní provést prvotní konfiguraci. V prvním kroku je potřeba v záložce „Session“ nastavit „Connection type“ na „Serial“, následně je potřeba vyplnit políčko „Serial line“, do tohoto políčka zapíšeme COM port, na kterém je zařízení LoRa testeru připojeno, poté je potřeba vyplnit políčko „Speed“, toto políčko udává rychlost komunikační sběrnice, v tomto případě je rychlost 115200 bit/s. Nastavení je možné vidět na obr. 36.



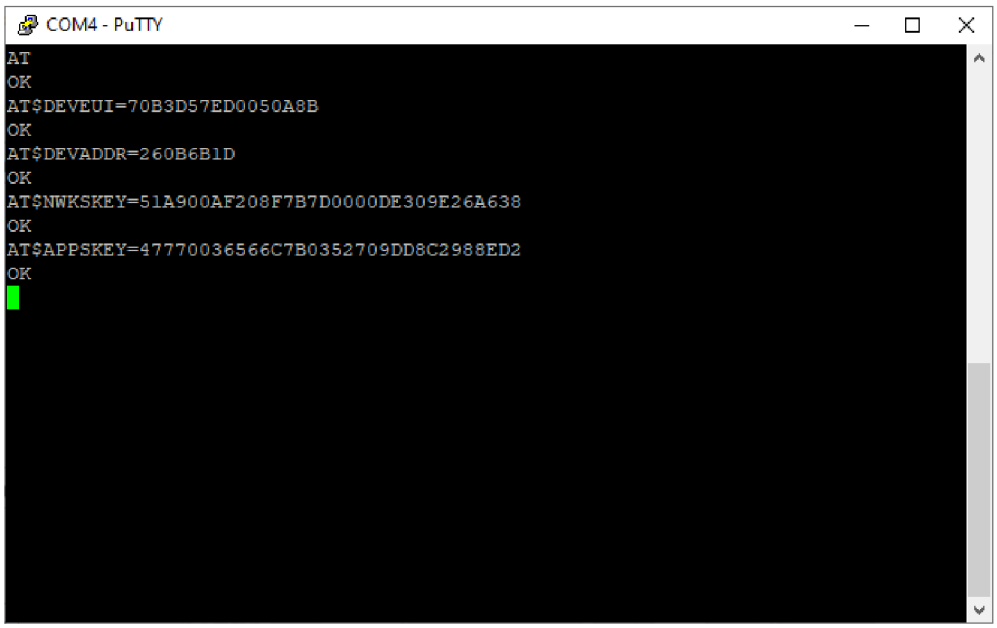
Obr. 36. Výchozí okno aplikace PuTTY – záložka Session

Pro lepší přehlednost je vhodné povolit echo stisknutých znaků. Toto nastavení lze nalézt v levém postranním panelu v kategorii „Terminal“. Funkci echo lze povolit zvolením varianty „Force on“ v nastavení „Local echo“. Toto nastavení je možné vidět na obr. 37.



Obr. 37. Okno aplikace PuTTY – záložka Terminal

Po dokončení výše uvedených nastavení je potřeba kliknout na tlačítko „Open“, následně se otevře terminál. V terminálu je potřeba zadat příkaz AT postupným stisknutím kláves: A T ENTER CTRL+J. Po tomto příkazu by měla v konzoli přijít odpověď OK. V tuto chvíli je potřeba do konzole zadat klíče. Tyto klíče se získávají z nastavení aplikace na webu TTN. Jedná se o klíče DevEUI, Device address, NwkSKey a AppSKey. Klíče je nutné do konzole vkládat postupně a každý klíč je nutné potvrdit stiskem klávesy ENTER a CTRL+J. Vložené klíče je možné vidět na obr. 38.



Obr. 38. Výpis z konzole aplikace PuTTY – nastavení klíčů přes AT příkazy

V tento moment je nezbytné zkontrolovat, zda byla konfigurace parametrů v LoRa testeru úspěšná. K této kontrole dochází přímo na samotném LoRa testeru, který je vybaven displejem. Krátkým stisknutím lze tlačítky, které se nachází na modulu s displejem, listovat v hlavním menu. Hlavní menu se skládá z následujících parametrů. Send SENT – aktivace přenosu dat na server. TX Data – výběr objemu testovacích dat. TX Period – nastavení prodlevy automatického odesílání dat. GPS Info – zobrazení aktuální polohy a času v případě připojeného GPS modulu. Mode – výběr komunikačního protokolu (ABP/OTAA). Join – požadavek na registraci do sítě TTN (režim OTAA). Confirmation – povolení potvrzení přijetí dat serverem. Port – cílový port. Band – výběr frekvenčního pásma. Datarate – nastavení faktoru rozprostření a šířky pásma. Network public – nastavení statusu sítě. Class A – nastavení řízení třídy spotřeby. Received – počet přijatých datových balíčků. Battery – stav napětí na baterii. Sleep – uvedení zařízení do režimu spánku.

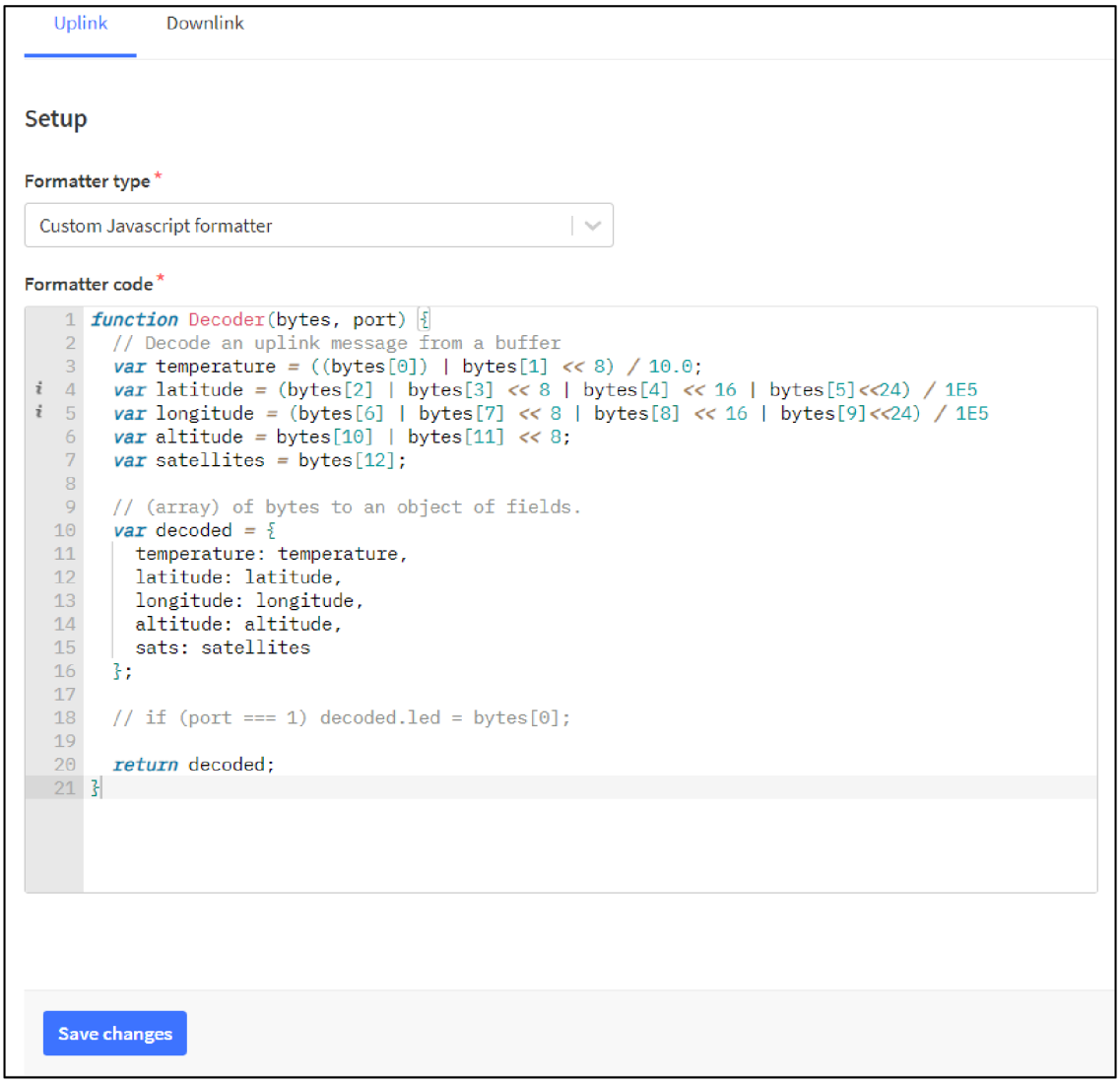
Přidržením pravého tlačítka lze změnit stav vybrané položky, případně vstoupit do podmenu. V hlavním menu je potřeba zkontrolovat mód v režimu ABP, zvolené frekvenční pásmo (Band), které by mělo být „EU868“, odesílání TX Data GPS o poloze zařízení, datovou rychlost „datarate“ na „SF7/125kHz“, nastavení statusu network public, Class A. Pokud jsou všechna tato nastavení správná, je možné pokusit se odeslat zprávu obsahující zaenkódované GPS souřadnice na server TTN. Nastavení parametrů na displeji je možné sledovat na obr. 39.

Obr. 39. Displejový modul testeru se zobrazenými nastavenými parametry

Zahájení odeslání zprávy na server lze provést stiskem a přidržením pravého tlačítka nad vybranou položkou „Send“, která se nachází na prvním místě seznamu v hlavním menu. V případě, že přístupová brána zachytí zprávu, předá ji síťovému serveru, který tuto zprávu zpracuje a předá ji aplikační vrstvě serveru. Zpráva se následně ve formátu JSON logu zobrazí v záložce přijatých dat. Pokud se TTN serveru podaří data přijmout a zobrazit, pak lze tvrdit, že je nastavení přístupové brány i koncového zařízení vytvořeno správně a lze tedy zařízení považovat za korektně nakonfigurovaná. Příchozí datové balíčky z LoRa testeru je možné vidět na obr. 40.

Obr. 40. Přehled datového toku koncového zařízení na webu TTN

Data na TTN server vždycky přijdou zaenkódovaná. Tato data je možné přečíst, pouze pokud se dekódují. Data se dají dekódovat tak, že se v záložce „Payload formatters“ na webovém rozhraní TTN do okna „Formatter code“ vloží potřebný formátovací kód. Tento kód lze získat na GIT repozitáři společnosti HARDWARIO. Zdrojem dat formátovacího dekodéru je pole surových bytů, které odpovídá odeslané datové části balíčku dat zařízení. Cílem tohoto dekodéru je převést pole na pole v jazyce JavaScript, který dokáže aplikační vrstva dále zpracovávat a předávat. Pro uložení tohoto dekodéru je potřeba kliknout na modře označené tlačítko „Save changes“. Nastavení datového formátu je možné sledovat na obr. 41.



Obr. 41. Kód pro dekódování zprávy z LoRa testeru

2.4.4 Připojení vlastního koncového zařízení do sítě TTN

Poté, co je za pomoci LoRa testeru ověřeno, že je komunikace se sítí TTN přes přístupovou bránu LoRa gateway funkční, je možné připojit vlastní koncové zařízení. Aby však bylo možné takové zařízení do sítě připojit, je nutné do něj doprogramovat firmware. Z pohledu dílčích části je nutné vytvořit ovladače pro obsluhu jednotlivých periferií, naimportovat knihovnu pro obsluhu komunikace s TTN sítí a vytvořit logiku, která bude zajišťovat propojení vrstev mezi sebou. Ze všech tří dostupných LoRa modulů na koncovém zařízení byl ke zprovoznění komunikace s TTN sítí použit modul RFM95W. K obsluze tohoto modulu mikrokontrolérem jsou potřeba ovladače pro obsluhu sběrnice SPI, po které mikrokontrolér s LoRa modulem komunikuje. Poté, co jsou zprovozněny ovladače, je možné s modulem komunikovat, posílat mu instrukce o tom, co má dělat a zpracovávat data, která mu ze sítě přijdou po zprovoznění knihovny

pro komunikaci s TTN sítí. Jedním ze zdrojů dat pro přenos jsou data z teplotního senzoru. Tento teplotní senzor je s mikrokontrolérem propojen pomocí I2C sběrnice, aby tedy bylo možné číst data z teplotního senzoru, je potřeba zprovoznit komunikaci přes I2C sběrnici. Po zprovoznění komunikace přes I2C sběrnici je možné ze senzoru číst data, přenášet je do mikrokontroléru a tam s nimi dále pracovat. Na DPS jsou zapojena celkem dvě uživatelská tlačítka, aby bylo možné tato tlačítka využívat, je potřeba i pro ně napsat ovladače, v tomto případě se jedná o ovladače GPIO. Ovladače GPIO je nutné zprovoznit také pro uživatelské LED, které slouží k signalizaci přijatých a odeslaných datových zpráv. Jako poslední je potřeba zprovoznit ovladač pro systémové hodiny, ty mají na starost kontrolu doby běhu jednotlivých úloh, nebo pozastavení úlohy v rámci programu.

Pro co nejefektivnější implementaci komunikace koncového zařízení s TTN serverem je vhodné použít již existující knihovnu, která již obsahuje MAC vrstvu kompatibilní s TTN serverem. Psát vlastní knihovnu je z pohledu rychlé implementace a testování v reálném provozu časově neefektivní, ať už z pohledu komplexnosti takovéto knihovny, nebo z pohledu chyb, které je potřeba při tvorbě takovéto knihovny vyřešit. V rámci této práce proto byla použita LoRaWAN LMIC knihovna, která tuto vrstvu obsahuje. Jedná se o knihovnu, která byla dříve vyvinuta společností IBM pod MIT licencí. Tato knihovna byla následně upravena, tak aby byla spustitelná i na jiných zařízeních jako Arduino, nebo STM32 Nucleo. Tato knihovna umožňuje použití na zařízeních využívající vysílače SX1272 a SX1276, nebo také jiné kompatibilní moduly s jinými kompatibilními čipy od společnosti HopeRF nebo Murata. Knihovna nabízí kompletní implementaci LoRaWAN třídy A a B a podporuje komunikaci na Evropském komunikačním frekvenčním pásmu 868 MHz. Knihova mimo jiné obsahuje kompletní síťovou vrstvu, dokáže odesílat datové balíčky na server s ohledem na pracovní cyklus a také dokáže kontrolovat integritu zpráv. Vzhledem ke všem výše uvedeným informacím je zřejmé, že nasazení takovéto knihovny na zařízení, jehož funkci je potřeba vyzkoušet v krátkém čase, je více než vyhovující. V důsledku použití aktivační metody ABP u vlastního koncového zařízení je, podobně jako u nastavení HARDWARIO LoRa testeru, potřeba konfigurační klíče do paměti zařízení nahrát manuálně. V tomto případě však není k dispozici počítačová aplikace, která by umožňovala nahrání klíčů do paměti zařízení přes AT příkazy, klíče je proto nutné zapsat přímo do kódu formou textové řetězce, který se následně parsuje.

Aplikační část firmwaru spravuje veškerou obsluhu jednotlivých dílčích částí kódu. Její obecná funkce je taková, že zpracovává požadavek na získání teploty z teplotního senzoru. Data, která z něj získá, následně zabalí do požadované datové struktury. Tato struktura se následně předává knihovně LMIC, která zajišťuje odeslání této datové struktury skrze LoRa modul na server TTN. Vyvolání funkce pro odeslání dat na server

je zajištěno dvěma způsoby, a to stiskem uživatelského tlačítka, nebo v pravidelných intervalech.

2.4.5 Zobrazení přijatých dat z TTN serveru na uživatelské webové stránce

Poté, co se úspěšně podaří dostat data z koncového zařízení na server, je potřeba obsah přijatých zpráv zobrazit pro koncové uživatele na externí webové stránce. Takovouto webovou stránku je potřeba na externím serveru zprovoznit z toho důvodu, že zprávy z koncových zařízení chodí na TTN server v takovém formátu, ve kterém jejich obsah není možné jednoduše zobrazit. Aby však bylo možné tyto zprávy na externí webové stránce číst, je potřeba jejich odesílání na server, na kterém webové stránky běží, nastavit na webovém rozhraní serveru TTN.

Nastavení se realizuje ve webovém rozhraní sítě TTN v sekci aplikace. V této sekci jsou zároveň zobrazeny všechny koncové zařízení, které byly pod daným účtem do sítě zaregistrovány. Vzhledem k tomu, že odesílání dat na externí server se pro každé zařízení nastavuje samostatně, je potřeba vybrat, z kterého z již vytvořených zařízení je potřeba data odesílat dál. Za účelem popisu toho, jak toto nastavení probíhá bylo zvoleno již registrované koncové zařízení s názvem test-app-diplom. Po otevření nastavení tohoto zařízení je potřeba v levém postranním panelu kliknout na panel záložku „Webhooks“, tato záložka slouží k nastavení přenášení dat z vybraného koncového zařízení na nastavený externí server. Vzhledem k tomu, že tento způsob zobrazení dat koncovému uživateli není nejtypičtější aplikací zpracování dat, nabízí platforma TTN možnost integrace nasbíraných dat do cloudových platforem jako AWS IoT, Azure IoT, nebo LoRa Cloud. V záložce „Webhooks“ je možné zvolit jeden z již předpřipravených serveru, na které je možné data odesílat, nebo je možné zvolit variantu „Custom webhook“, ve které se nastavení volí dle potřeby. Ve vlastím nastavení je pak potřeba vyplnit několik parametrů. Prvním parametrem, který je potřeba nastavit je jedinečné ID, toto ID musí být v definovaném formátu např moje-nové-zařízení. Následně je potřeba zvolit způsob, v jakém formátu budou data dále odesílána. Na výběr je formát JSON, nebo protokol vyrovnávací paměti. Dále je potřeba nastavit URL adresu serveru, na který se mají data následně odesílat, k tomu slouží kolonka „Base URL“. Následně je pak potřeba zaškrtnou zaškrtávací políčko s typem požadované zprávy. V rámci této diplomové práce byla zvolena varianta „Uplink messanges“. Zvolené a vyplněné parametry je potřeba ulož.

V následujícím kroku je potřeba nachystat vlastní server ke zpracování příchozích dat ze sítě TTN. V případě, že má vlastní server uzavřené porty, je potřeba tyto porty pro vstup dat z TTN sítě otevřít. Poté, co jsou porty otevřeny, je potřeba připravit na vlastním serveru aplikaci. Aplikace by měla být napsána ve vhodném programovacím jazyce,

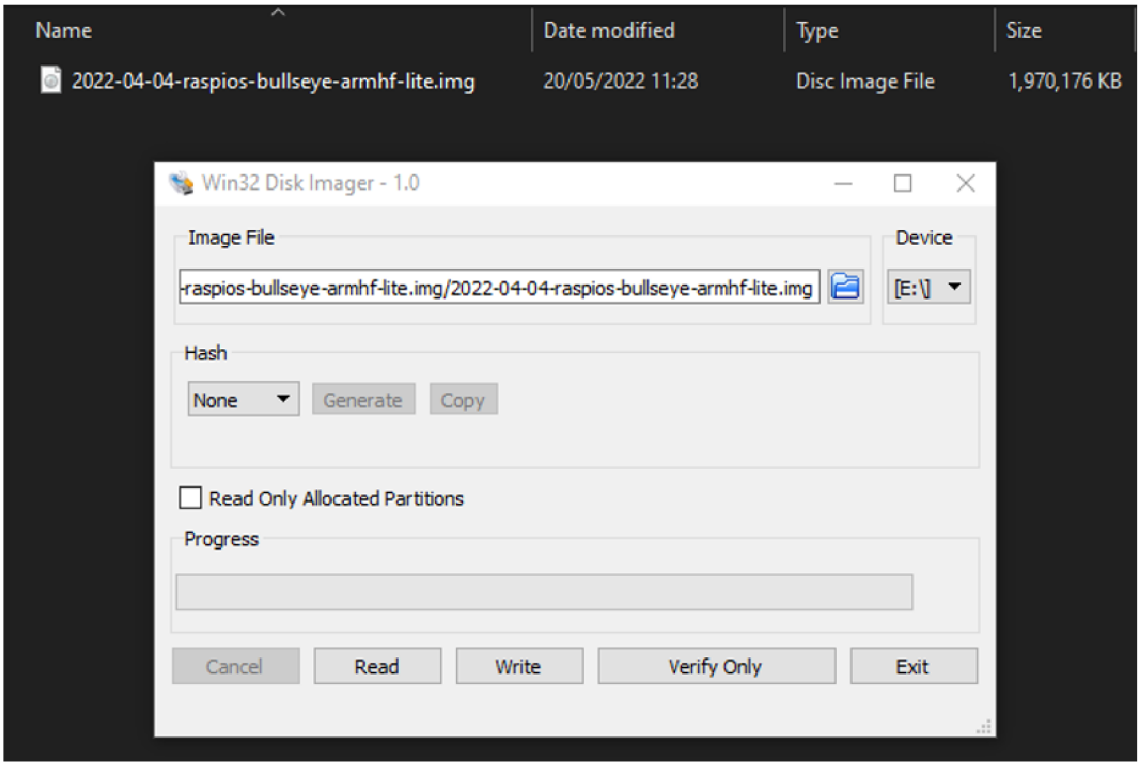
ke kterému jsou vytvořeny knihovny pro distribuci webových stránek. V rámci této diplomové práce byl však použit z důvodu jednoduché implementace jazyk Python, který disponuje knihovnami pro práci s HTTP dotazy a zpracování JSON formátu. Aplikace na serveru zajišťuje to, že pokud na server přijde datový balíček ve formátu JSON ze sítě TTN, tak tento balíček parsuje za účelem získání užitečné části dat, které jsou následně uživateli předkládány ve formě HTML stránky.

2.5 Postup realizace systému s lokální LoRaWAN sítí ChirpStack

Celý systém lokální sítě ChirpStack je provozován na platformě Raspeberry Pi 3. Systém je spustitelný i na jiných průmyslových počítačích, jako například OnLogic CL210G-10, který je lepší volbou pro průmyslové aplikace a obecně pro komplexnější systémy na bázi LoRaWAN, tomu odpovídá i jeho cena, která se pohybuje v řádech nižších desítek tisíců korun. Pro tuto diplomovou práci byla však zvolena platforma Raspberry Pi, nejen z toho důvodu, že je řádově levnější, ale i kvůli tomu, že je pro sestavení základní sítě naprosto dostačující a je obecně dostupnější pro běžné uživatele. Tato platforma je pro běžné uživatelé vhodná také z toho důvodu, že je Raspberry Pi komerčně známé a tím pádem nabízí širokou škálu různých diskusních fór, na kterých lze nalézt pomoc v situaci, kdy se zařízení nebo jeho software nechová dle očekávání. Zároveň se lze v případě problémů obrátit přímo na technickou podporu samotného výrobce, která je také pro běžného uživatele dostupnější než u profesionálních průmyslových řešení. Platforma Raspberry Pi 3 nabízí čtyř jádrový procesor Broadcom BCM2837B0, který využívá jádro ARM Cortex-A53 a frekvenci procesoru až 1.4 GHz, velikost operační paměti RAM je pak 1 GB. Platforma dále nabízí velké množství uživatelských konektorů jako 4 USB porty, HDMI připojení nebo připojení pro Ethernet, které je nezbytné pro možnost připojení routeru Mikrotik. [19]

Aby však bylo možné tuto platformu pro požadovanou aplikaci použít, je potřeba na ni nahrát požadovaný operační systém. Procesor na Raspberry Pi zavádí svůj operační systém z SD karty. Nejprve je tedy potřeba operační systém na SD kartu nahrát. K tomu je potřeba SD karta o velikosti alespoň 4 GB, což je nejmenší možná velikost pro základní verzi potřebného operačního systému. Potřebný operační systém se jmenuje Raspbian, jedná se o Linuxovou distribuci, která vznikla na základě Linuxového operačního systém Debian. Obraz disku operačního systému Raspbian je možné stáhnout z webových stránek výrobce platformy Raspberry Pi. Obraz disku je možné stáhnout také z alternativních webových stránek, ale v důsledku bezpečnosti je silně doporučeno použít originální stránky výrobce. Originální stránky výrobce Britské společnosti The Raspberry

Pi Foundation jsou www.raspberrypi.org. Poté, co je obraz disku stažen, je potřeba ho nahrát na SD kartu. Aby bylo možné obraz disku na SD kartu nahrát, je potřeba použít aplikaci, která takovouto operaci umožňuje. Je možné použít originální aplikace od výrobce Raspberry Pi, s názvem „Raspberry Pi Imager“, v rámci této práce byla však použita aplikace Win32 Disk Imager. Okno této aplikace s obrazem disku je možné vidět na obr. 42. Poté, co je na kartu nahrán obraz disku, je možné tuto SD kartu vložit do určeného slotu na zařízení a zařízení následně spustit.

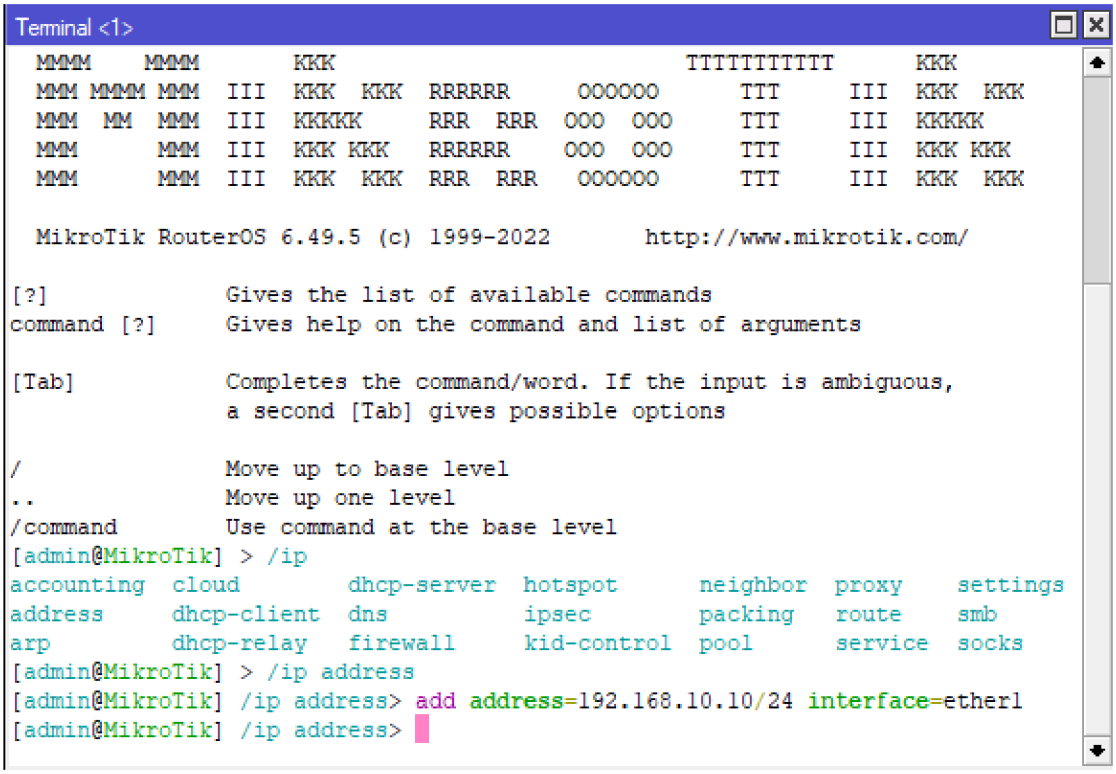


Obr. 42. Aplikace pro nahrátí obrazu disku na SD kartu Win32 Disk Imager

2.5.1 Rekonfigurace routeru Mikrotik

Z toho důvodu, že pro koncept LoRaWAN sítě s Chirpstackem je odlišný od sítě TTN a síť s Chirpstackem je lokální síť postavená na platformě Raspberry Pi 3, je potřeba i upravit konfiguraci routeru Mikrotik tak, aby byl s nastavením sítě kompatibilní. Výhodou je to, že router je možné nastavit na lokální síti. Jediné, co je pro to potřeba je mít připojený počítač do stejné lokální sítě, aby bylo možné router přes aplikaci Winbox nastavit. Přes lokální síť dojde k přednastavení konfigurace routeru tak, aby bylo následně možné router samotný pouze připojit do Raspberry Pi a po připojení nebylo už potřeba nic upravovat.

Router Mikrotik je ale potřeba, stejně jako u konfigurace pro síť TTN, uvést do továrního nastavení. Tento postup je uveden v kapitole 2.4.1. Poté, co se router nachází v továrním nastavení, je možné provést novou konfiguraci. Nová konfigurace začíná stejně, jako u nastavování routeru pro síť TTN, proto bude část o změně hesla a přihlášení přeskočena. Jakmile se v aplikaci zobrazí výchozí obrazovka, je možné přejít k zadání adresy platformy Raspberry Pi a rozhraní, přes které se následně komunikuje. Tyto parametry se nastavují přes terminál. Aby bylo tedy možné parametry zadat, je potřeba otevřít terminál. Ten se v aplikaci nachází v levém postranním panelu. Jakmile se po kliknutí na ikonu nového terminálu okno terminálu otevře, je možné v něm adresu a rozhraní nastavit. V konzoli je nejprve potřeba příkazem /ip otevřít virtuální adresář, ten pak nabízí více možností pro nastavení, jako například cloud, DHCP, nebo firewall. V rámci této aplikace se zapsáním příkazu /ip adress do příkazové řádky vyvolá možnost nastavení adresy a komunikačního rozhraní. Nastavení je možné vidět na obr. 43.



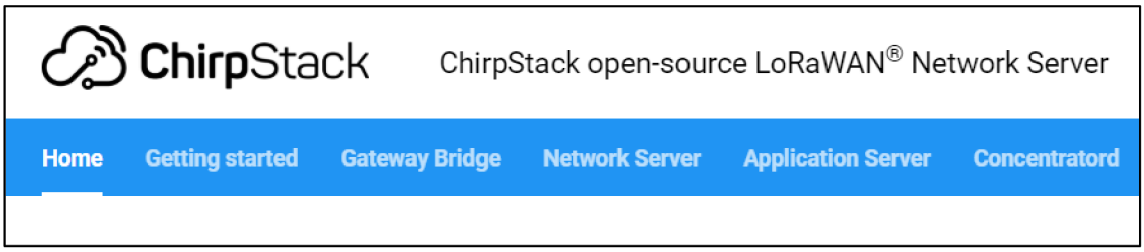
Obr. 43. Konzole aplikace Mikrotik při nastavování adresy a rozhraní

Jakmile je nastavena adresa a komunikační rozhraní, je potřeba nastavit poslední část routeru, a to konfiguraci LoRy samotné. V levém postranním panelu aplikace je proto nutné kliknout na záložku LoRa, které vyvolá otevření okna pro konfiguraci. V tomto okně je potřeba zvolit záložku serverů, ve které je, na rozdíl od sítě TTN, potřeba vytvořit nový server. Kliknutím na ikonu pro přidání serveru se otevře nastavovací okno, ve kterém je potřeba vyplnit název serveru, adresu a nastavení portů. Název serveru

je libovolný a není nijak omezen formátem, do adresy serveru je potřeba zapsat lokální adresu platformy Raspberry Pi, porty serveru jsou závislé na výchozích portech platformy, tyto porty je potřeba v konfiguraci platformy najít a doplnit. Jakmile dojde k vyplnění všech potřebných parametrů, klinutím na tlačítko „použít“ a následně na tlačítko OK, dojde k uložení nastavených parametrů a vytvoření nového serveru. Po vytvoření serveru je potřeba zkontrolovat nastavení zařízení, je proto potřeba překliknout do okna „Devices“. V této záložce je potřeba otevřít nastavení vytvořeného serveru a zkontrolovat, zda souhlasí nastavené parametry, především adresa síťového serveru. Pokud adresa souhlasí, je potřeba povolit status routeru na „enable“ v případě, že tomu tak není, je potřeba nastavit status serveru na „disable“. V posledním kroku je potřeba kliknout na tlačítko použít a OK, čímž se nastavení server uloží a nastavovací okno se zavře. V momentě, kdy jsou hotovy všechny výše popsané kroky nastavení, je možné router Mikrotik připojit k platformě Raspberry Pi, kde by se měl chovat jako vstupní brána. Než však dojde k fyzickému připojení samotného routeru, je potřeba na platformě Raspberry Pi spustit systém ChirpStack.

2.5.2 Implementace LoRaWAN ChirpStack na RasppberryPi 3

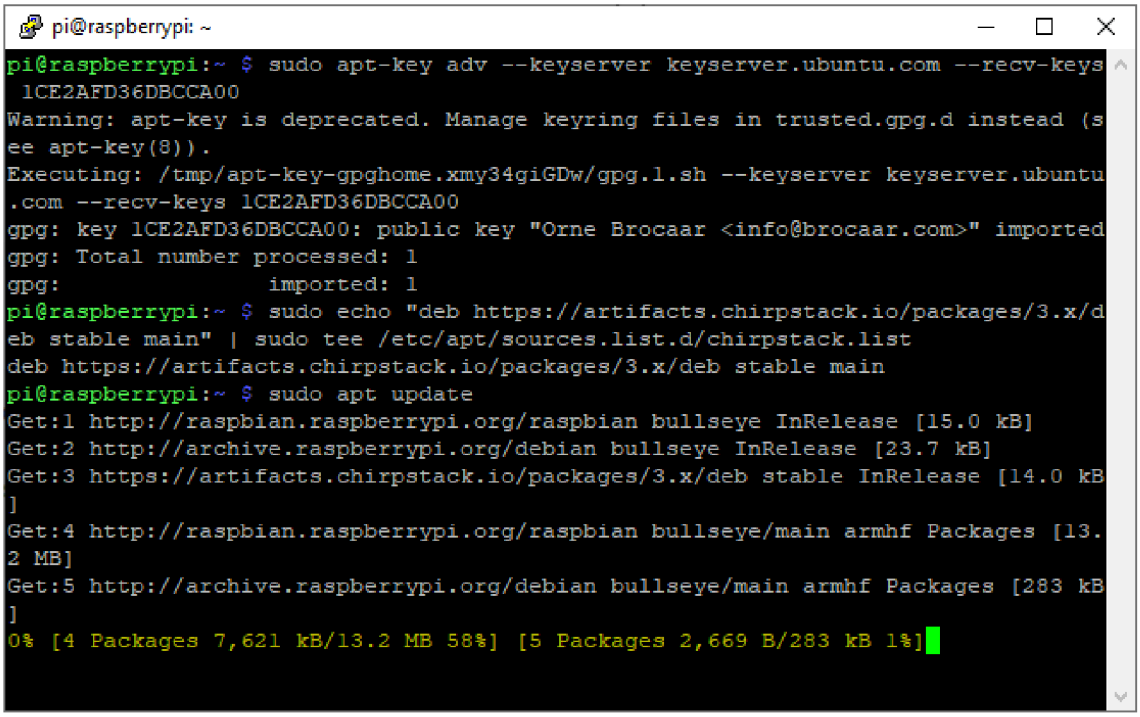
Poté, co je možné spustit Raspberry Pi s operačním systém Raspbian, je potřeba jako následující krok stáhnout, nainstalovat a spustit sytém ChirpStack. Aby však byl tento krok možný, je potřeba stáhnout všechny potřebné komponenty tohoto systému ze serveru výrobce. Aby bylo stažení potřebných souborů možné, je potřeba připojit platformu Raspberry Pi k internetu. V rámci této diplomové práce byla platforma připojena k síti fyzicky, a to z toho důvodu, že fyzické spojení umožňuje přenášet větší objem dat za kratší čas. Stažení potřebných instalačních souborů je možné z Debianového repozitáře ChirpStack přes konzoli otevřenou na Raspberry Pi. Hlavní části, které je potřeba pro dosažení požadované funkce stáhnout, nainstalovat a spustit jsou Gateway Bridge, Síťový server a Aplikační server. Instalační popis jednotlivých dílčích částí je uveden na webové stránce výrobce ChirpStack, a to www.chirpstack.io. Popis instalačního postupu v této diplomové práci slouží k tomu, aby poukázal na části postupu, které nejsou v originálním popisu dostatečně popsány, nebo na ně není dostatečně upozorněno a mohou vést k neúspěšné implementaci systému. Postupovat podle originálního postupu, s přihlédnutím na upozornění v této práci, je vhodné z toho důvodu, že jednotlivé kroky nemusí být jednoznačné a může tak být předejito nefunkčnosti systému v důsledku špatné instalace.



Obr. 44. Výchozí panel aplikací na webové stránce ChirpStack

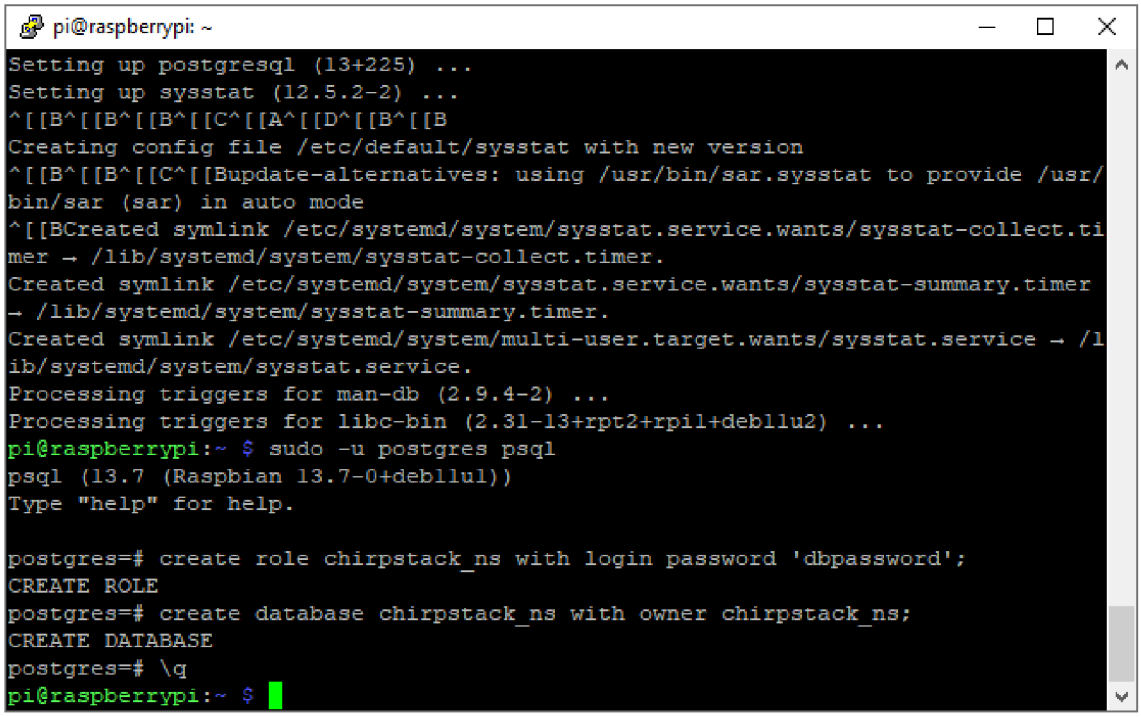
Na obr. 44 je možné vidět úvodní panel na webové stránce, na které je dostupný návod pro implementaci systému ChirpStack. Stažení a instalaci je možné provést v libovolném pořadí. V této práci byl nejprve implementován Gateway Bridge, následně Síťový server a poté Aplikační server.

Nejprve je tedy potřeba kliknout na záložku Gateway Bridge, po kterém se otevře stránka s popisem různých části této vrstvy. V levém postranním panelu je potřeba otevřít menu s názvem Instalace. Po rozbalení tohoto menu je v podmenu potřeba kliknout na záložku Požadavky. V této záložce jsou uvedeny prerekvizity, které budou k dané části systému potřebné pro jeho korektní funkci. V této části instalace není žádný krok, na který je potřeba dát si pozor. Po instalaci této prerekvizity je možné se v levém postranním menu překliknout do záložky Debian/Ubuntu. Tuto část lze provést přesně podle návodu, jen je potřeba nezapomenout na konfiguraci, kterou je potřeba provést po instalaci. Postup pro provedení správné konfigurace je popsán v záložce konfigurace v levém postranním panelu v menu Instalace. Na obr. 45 je možné vidět část instalace Gateway bridge.



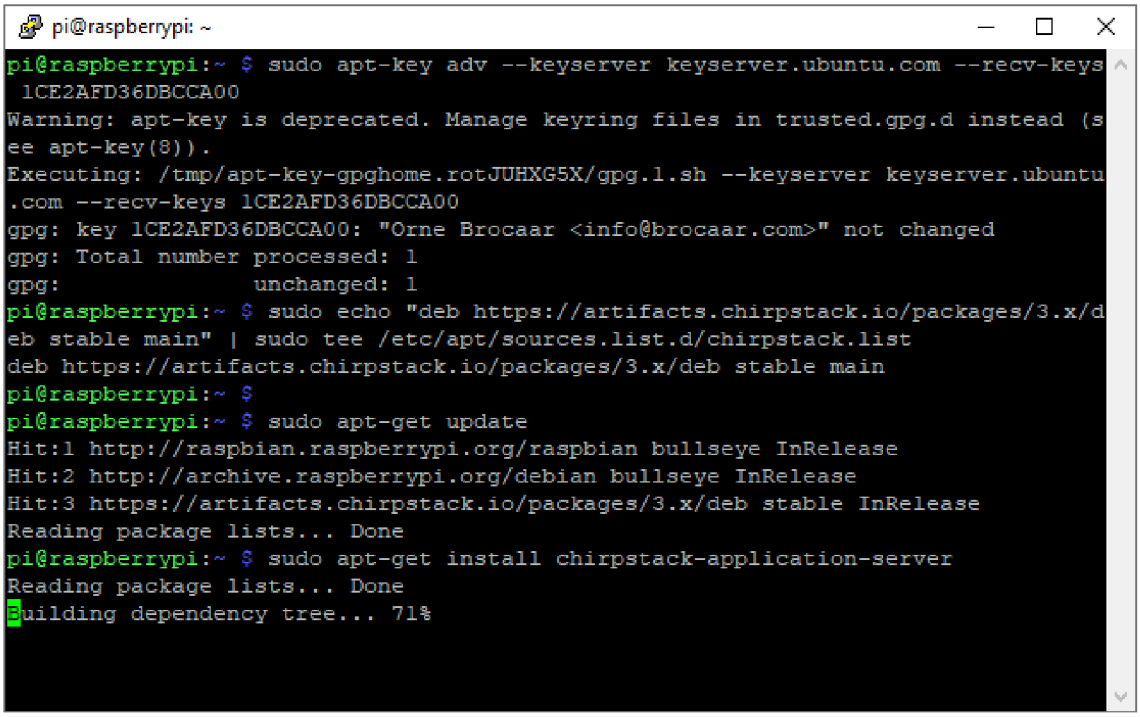
Obr. 45. Výpis z konzole při instalaci Gateway Bridge

Jakmile je Gateway bridge nainstalovaný je možné přejít k dalšímu kroku. V tomto kroku je potřeba stáhnout a nainstalovat Síťový server. Je tedy potřeba kliknout na správnou záložku v horním modrém panelu a po otevření výchozí stránky Síťového serveru přes levý postranní panel otevřít menu Instalace. Stejně jako v předchozím kroku je nejdříve potřeba otevřít záložku Požadavky. V této záložce se nachází prerekvizity, které budou k dané části systému potřebné pro jeho korektní funkci. Po instalaci potřebných prerekvizit je potřeba se v levém postranním menu překliknout do záložky Debian/Ubuntu instalace. V této části je potřeba také nezapomenout na konfiguraci. Na obr. 46 je možné vidět výpis z konzole, ve které dochází k instalaci jedné z částí Síťového serveru.



Obr. 46. Výpis z konzole při instalaci Síťového serveru

Jakmile je Síťový server nainstalovaný je možné přejít k poslednímu kroku instalace systému ChirpStack. V posledním kroku je potřeba stáhnout a nainstalovat Aplikační server. Podobně jako ve výše uvedených krocích je i zde potřeba kliknout na záložku v horním modrém panelu. Po otevření stránky Aplikačního serveru je potřeba přes levý postranní panel otevřít záložku Instalace a v podmenu kliknout na záložku Požadavky. Jak je zřejmé z prerekvizit, všechny požadavky na provoz Aplikační vrstvy byly již splněny v předchozích krocích. Je tedy možné přejít do záložky Debian/Ubuntu. V této části je potřeba, stejně tak jako v předešlé instalaci, nezapomenout na konfiguraci Na obr. 47 je možné vidět výpis z konzole, ve které dochází k instalaci jedné z částí Aplikačního serveru.

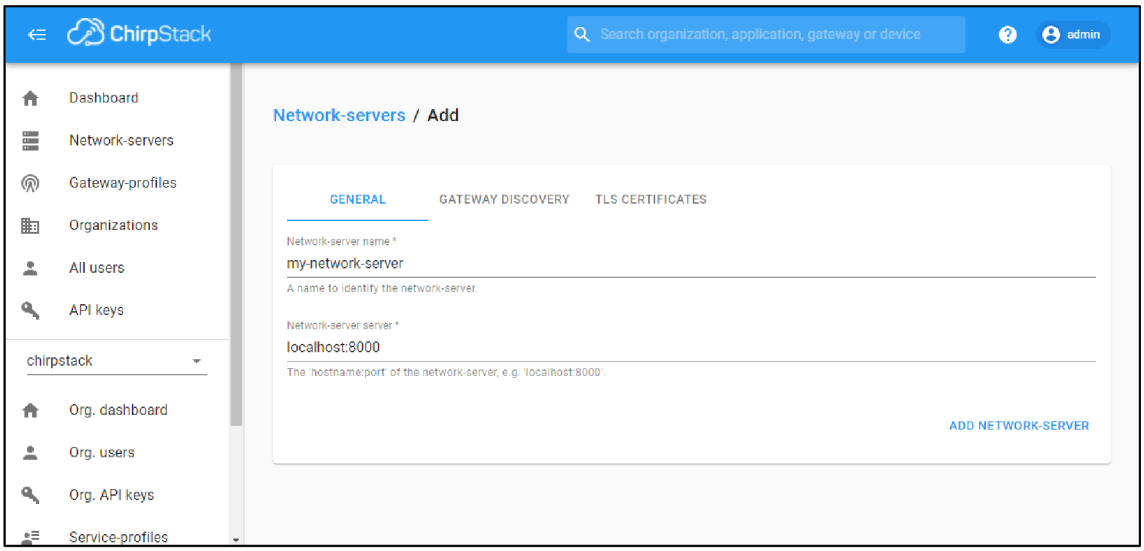


Obr. 47. Výpis z konzole při instalaci Aplikačního serveru

Poté, co jsou všechny tři části systému ChirpStack nainstalovány na Raspberry Pi, je možné k němu připojit router s předpřipravenou konfigurací. Router je do Raspberry Pi připojen přes ethernetový konektor.

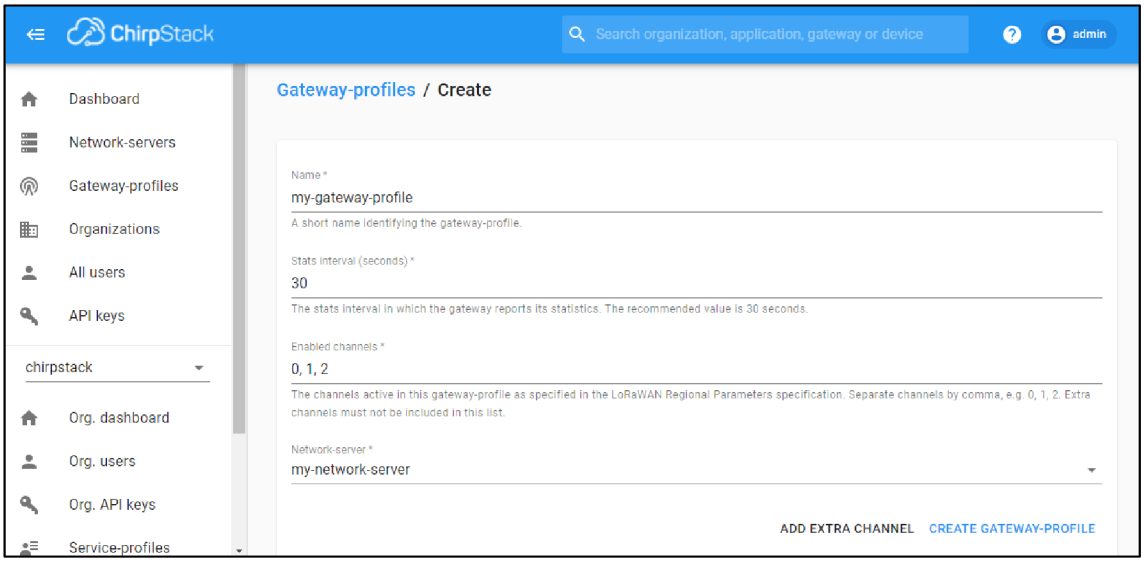
Následně je potřeba přes webové rozhraní stránky ChirpStack spuštěné na Raspberry Pi přejít do konfiguračního prostředí. V případě, že je Raspberry Pi připojeno přes rozbočovač do lokální sítě, je možné konfiguraci spustit také přes osobní počítač. Do konfiguračního prostředí se lze dostat přes webové okno, ve kterém je zobrazen návod pro instalaci Aplikační vrstvy. Na konci tohoto okna se nachází kapitola, která popisuje přístup do Aplikačního serveru buď přes HTTP, nebo HTTPS. Do Aplikačního serveru lze přistoupit buď přes API, nebo přes webové rozhraní. V rámci této diplomové práce byl zvolen přístup přes webové rozhraní. V tomto rozhraní je potřeba nastavit parametry Síťového serveru, profil přístupové brány, servisní profil, profil zařízení, přístupovou bránu a aplikace.

V síťovém serveru je potřeba nastavit název serveru ve formátu síťový-server, název serveru pak může být libovolný, jenom je potřeba, aby byl dodržen správný formát. Dále je potřeba nastavit server síťovému serveru, ten musí být ve formátu hostitel:port, v rámci této diplomové práce byl z důvodu omezení chybovosti nastaven výchozí server ve formátu localhost:8000. Nastaveni lze vidět na obr. 48.



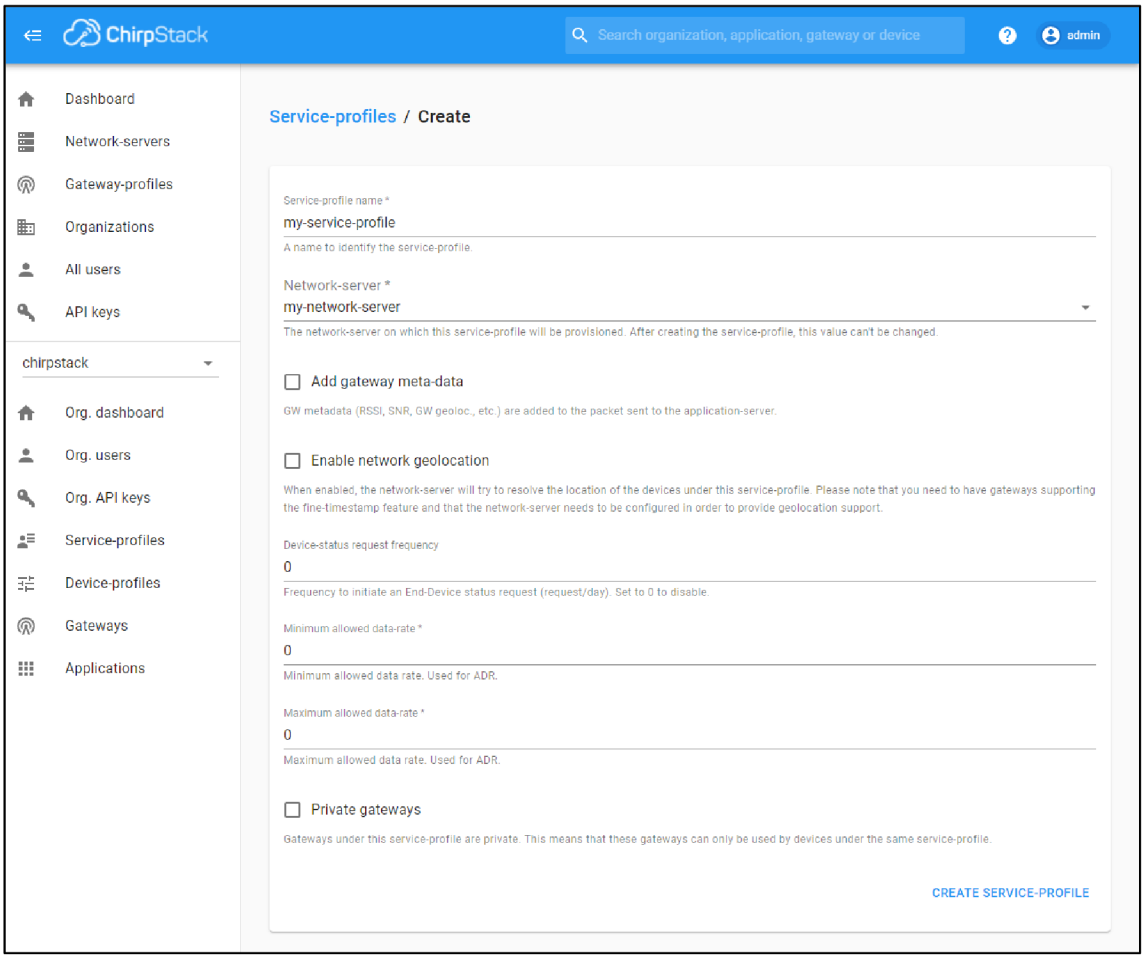
Obr. 48. Přidání nového síťového serveru v konfiguračním rozhraní ChirpStack

V profilu přístupové brány je potřeba nastavit čtyři parametry. Prvním parametrem je název, ten musí být podobně jako v předchozím nastavení uveden v definovaném formátu. Pro tuto diplomovou práci byl zvolen název „my-gateway-profile“. Druhým parametrem, který je potřebné nastavit je délka intervalu statistiky vstupní brány. Doporučená hodnota tohoto intervalu je 30 sekund, doporučená délka intervalu byla v rámci této práce zachována. Třetím parametrem je povolení kanálů, v rámci této práce byly nastaveny kanály 0, 1 a 2. Čtvrtým a posledním parametrem je volba síťového serveru, ke kterému se bude přístupová brána připojovat. Nastavení lze vidět na obr. 49.



Obr. 49. Přidání nového profilu přístupové brány v konfiguračním rozhraní ChirpStack

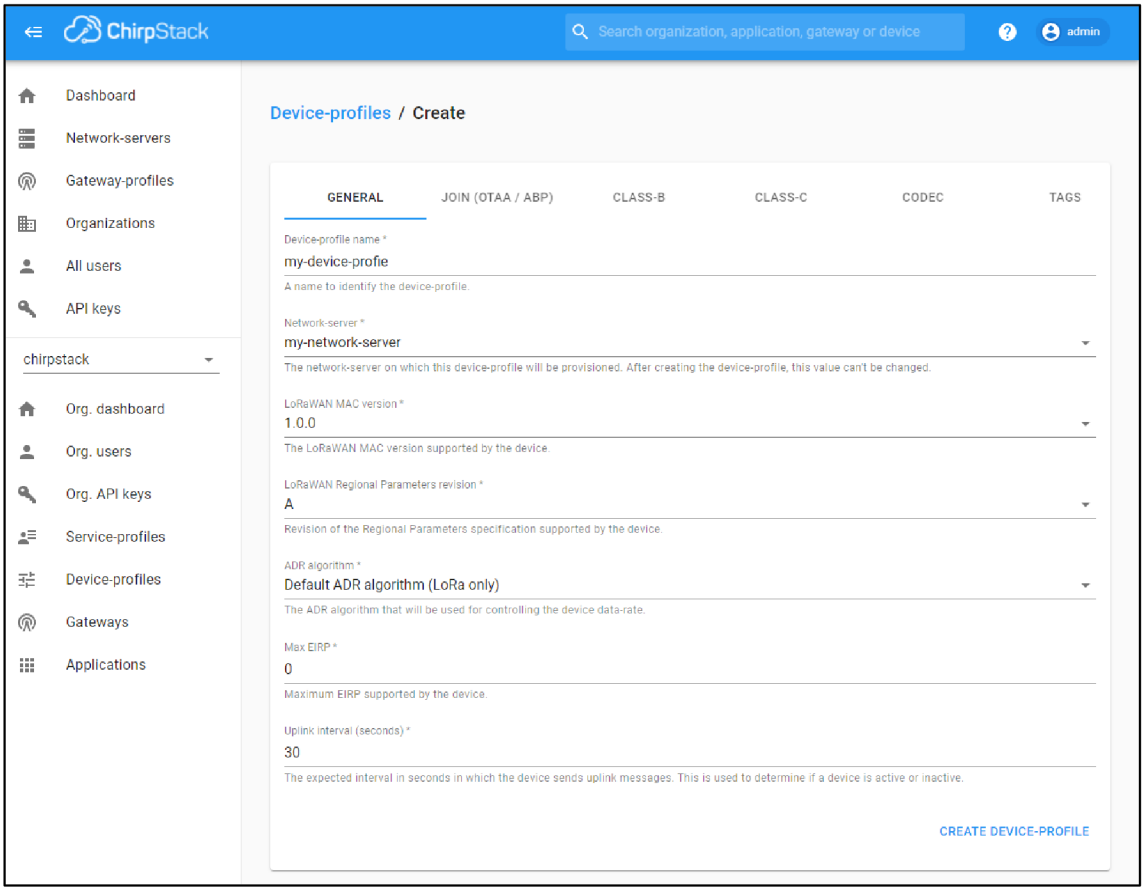
V servisním profilu je potřeba nastavit několik parametrů. Prvním parametrem je název servisního profilu, ten musí být v požadovaném formátu, podobně jako názvy u předchozích částí. Dále je potřeba zapsat název síťového serveru, ke kterému bude tento servisní profil přiřazen. V případě, že je to potřebné, je také možné nastavit frekvenci, po jaké si server vyžádá od koncového zařízení jeho status. V rámci této práce tato funkce nebyla potřebná, proto se zapsáním 0 do tohoto parametru funkce vypnula. V posledních dvou parametrech je potřeba nastavit minimální a maximální možnou rychlost přenosu dat. Vzhledem k tomu, že tento parametr není pro aplikaci v této práci nezbytný, byla jak pro maximální, tak pro minimální přenosovou rychlost nastavena hodnota 0. Nastavené parametry lze vidět na obr. 50.



Obr. 50. Přidání nového servisního profilu v konfiguračním rozhraní ChirpStack

V nastavení profilu zařízení je potřeba nastavit hned několik parametrů. Prvním z nich je název zařízení. Název zařízení může mít opět libovolný název, pouze musí být zachován formát podobně jako u předchozích nastavení. Dále je potřeba vybrat jeden z již vytvořených síťových serverů, ke kterému se bude vytvořené zařízení připojovat.

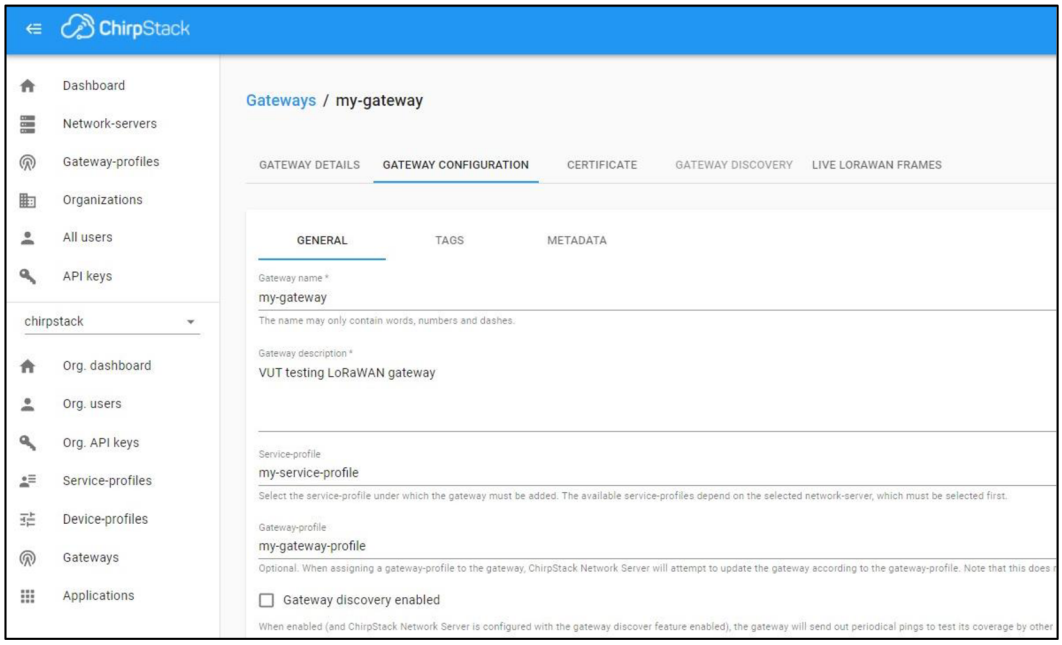
Po vytvoření zařízení tento parametr již nemůže být změněn. Následně je potřeba zvolit verzi síťové vrstvy koncového zařízení, které se bude pod profilem vytvářeného zařízení do sítě připojovat. Dále je potřeba vybrat kategorii zařízení, která je koncovým zařízením podporována, tento údaj bývá uveden v katalogovém listu LoRa modulu, který je na koncovém zařízení osazen. Následně je potřeba z uvedených možností vybrat algoritmus, který bude nastavovat přenosovou rychlost vytvářeného zařízení. Dále je potřeba nastavit maximální hodnotu EIRP, což je efektivní vyzařovaná síla, tato hodnota v katalogovém listu použitého LoRa modulu nebyla nalezena, byla proto nastavena na hodnotu 0. Jako poslední parametr je potřeba nastavit časový interval, po jakém koncové zařízení odešle zprávu na server. Tento časový interval slouží také k určení toho, zda je zařízení aktivní, nebo ne. Nastavené parametry zařízení lze vidět na obr. 51.



Obr. 51. Přidání nového profilu zařízení v konfiguračním rozhraní ChirpStack

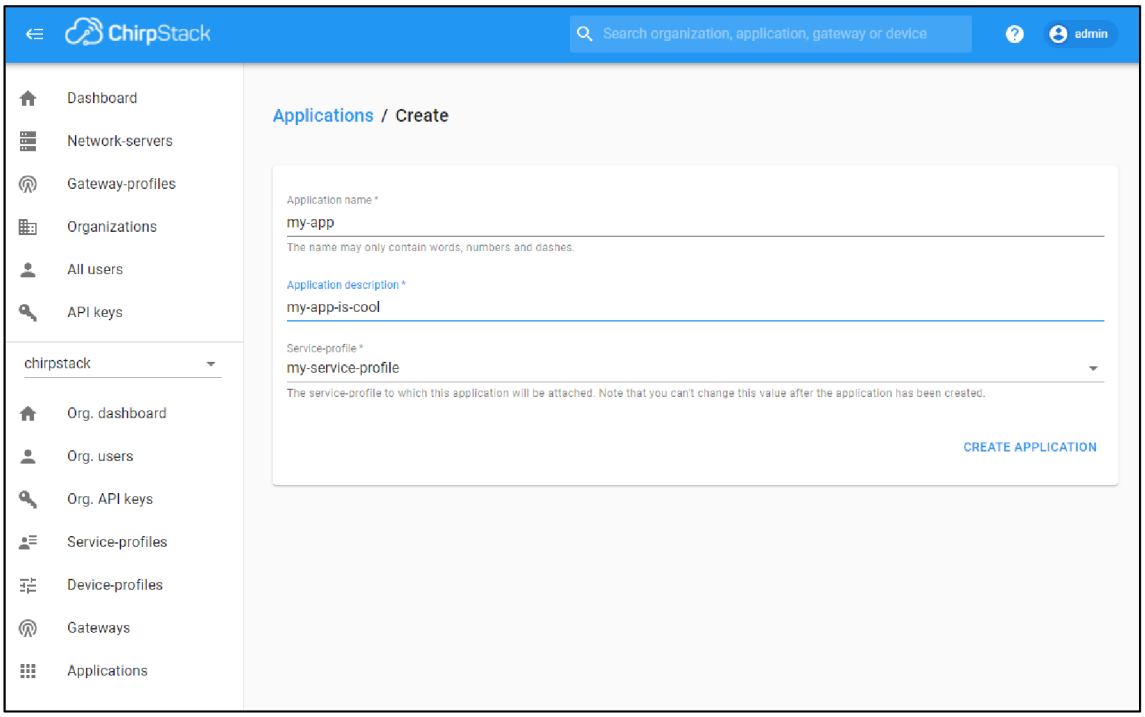
Dále je potřeba vytvořit a nastavit profil pro přístupovou bránu. Na obr. 52 je možné vidět konfiguraci již vytvořené přístupové brány. Parametry, které musí být v konfiguraci nastaveny jsou název přístupové brány v podobném formátu, jako názvy v předešlých částech a popis toho, k čemu je přístupová brána určená. Dále je v konfiguraci přístupové

bráně nastavit dva profily, které byly vytvořeny na začátku, a to servisní profil a profil přístupové brány.



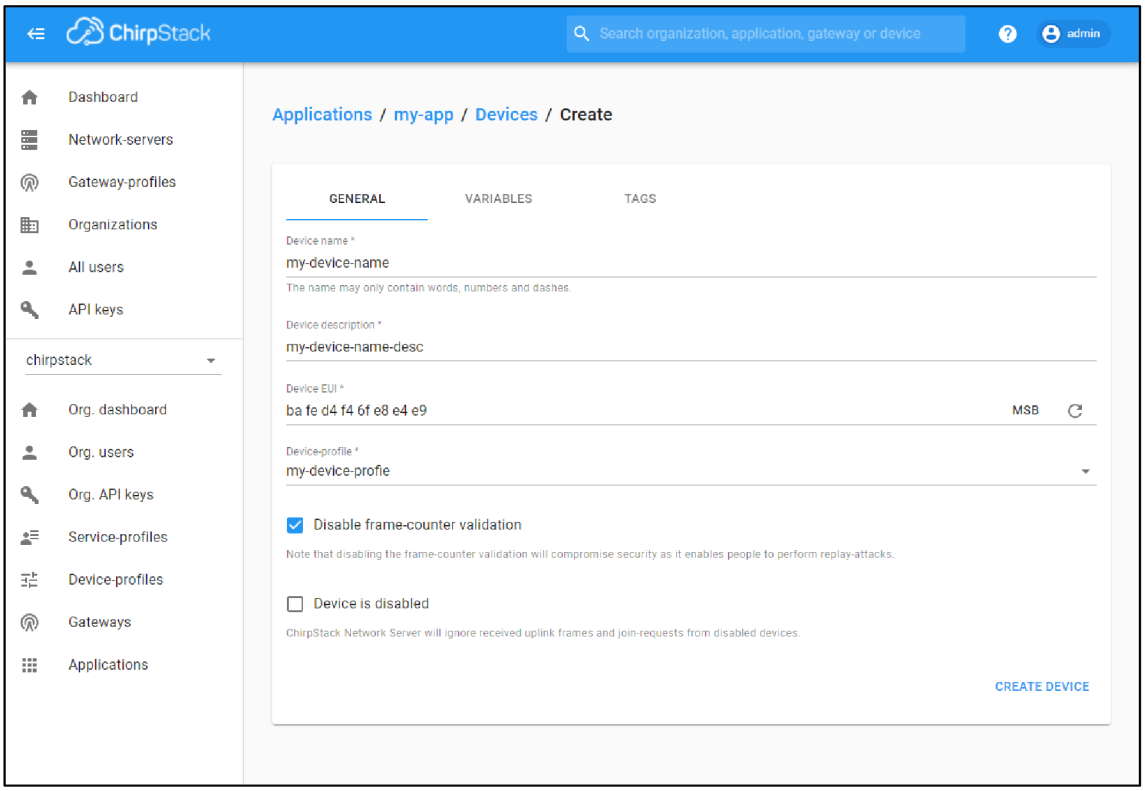
Obr. 52. Konfigurace přístupové brány v konfiguračním rozhraní ChirpStack

Poslední částí, kterou je potřeba vytvořit je aplikace. Při tvorbě aplikace je potřeba vyplnit tři požadované parametry, a to název aplikace, popis aplikace, se přiřadit k ní již vytvořený servisní profil. Stránku s těmito třemi vyplněnými parametry lze vidět na obr. 53.



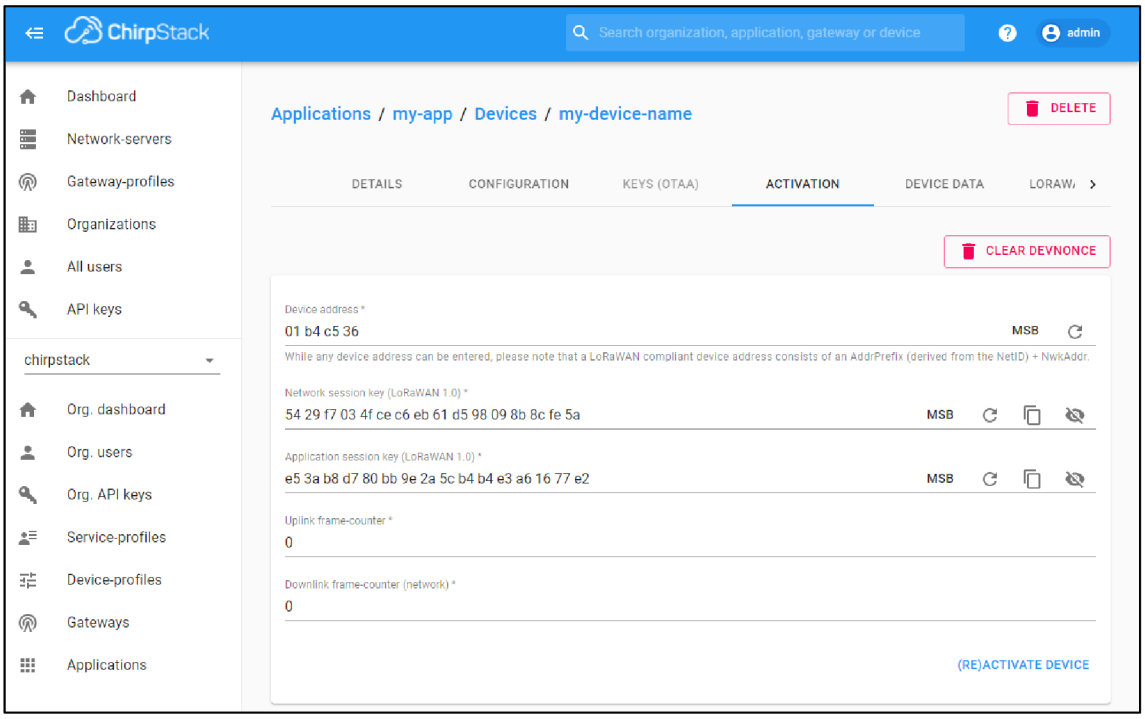
Obr. 53. Okno pro vytvoření nové aplikace v konfiguračním rozhraní ChirpStack

Poté, co je aplikace vytvořena, je možné do ní přidat nové zařízení. K tomu je potřeba kliknutím na vytvořenou aplikaci dojít na stránku, kde je seznam všech již dříve vytvořených zařízení. K vytvoření nového zařízení je potřeba na této stránce kliknout na tlačítko „+ CREATE“, kterým dojde k otevření stránky, která slouží pro zadání parametrů nového zařízení. Stránku s těmito parametry je vidět na obr. 54. Na této stránce je potřeba vyplnit základní parametry. Prvními dvěma parametry jsou název a popis zařízení. U obou těchto popisů musí být dodržen požadovaný formát. Dále na této stránce dochází ke generování EUI klíče, tento klíč musí být následně jako jeden z nezbytných parametrů zapsán do paměti koncového zařízení, jedná se totiž o jeden z aktivačních klíčů pro připojení na server. Posledním parametrem, který je potřeba zvolit je profil zařízení, pod který bude nově vytvořené zařízení spadat. Následně je možné pomocí zaškrtávacího políčka zvolit zbývající parametry. V rámci této diplomové práce bylo zaškrtnuto zaškrtávací políčko, které vypíná validaci podle počítání rámců. Tato bezpečnostní funkce není v rámci této práce nezbytná pro provoz zařízení.



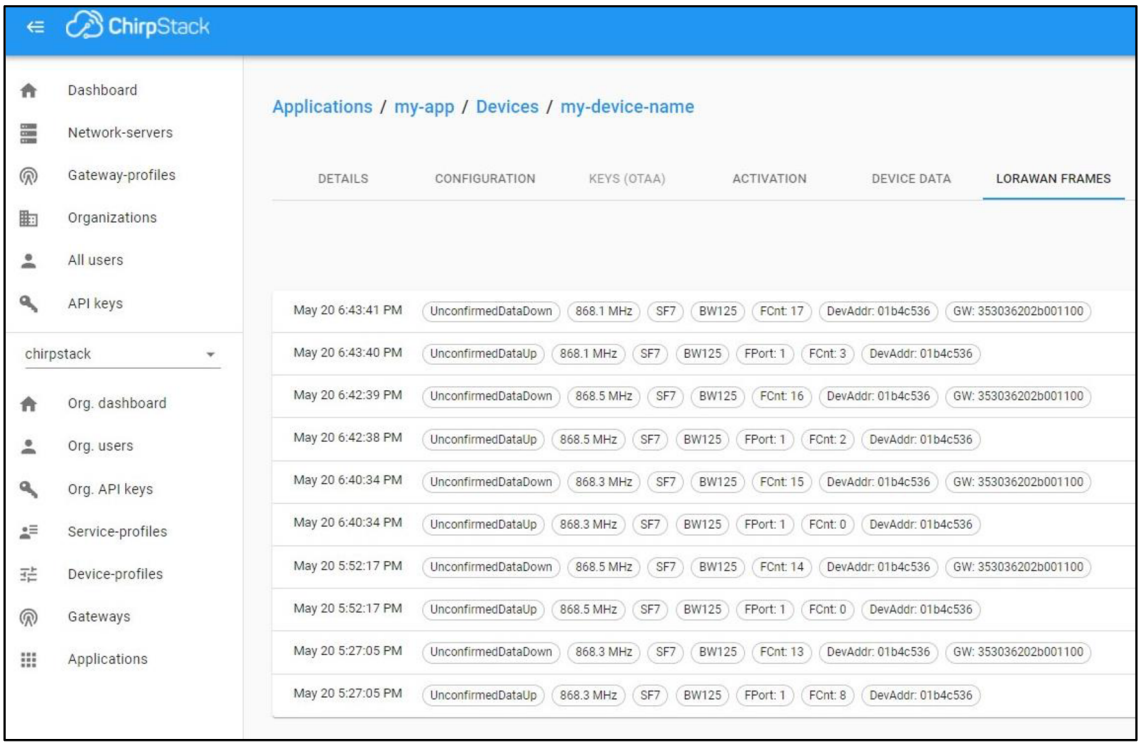
Obr. 54. Okno pro vytvoření nového zařízení v konfiguračním rozhraní ChirpStack

Po vytvoření zařízení je potřeba pro koncové zařízení vygenerovat aktivační klíče. Generování klíčů lze realizovat v záložce aktivace v nově vytvořeném zařízení. Tyto klíče lze buď vygenerovat nové, nebo lze použít ty, které již v paměti zařízení uloženy jsou. V případě vygenerování nových klíčů je potřeba tyto klíče před první aktivací nahrát do paměti zařízení, jinak nebude možné spojení se serverem realizovat. Nově vygenerované klíče pro koncové zařízení lze vidět na obr. 55.



Obr. 55. Okno nastavení aktivace nového zařízení v konfiguračním rozhraní ChirpStack

Poté, co jsou aktivační klíče nahrány do paměti zařízení, je možné se koncovým zařízením připojit do sítě ChirpStack. Způsob, jakým se tyto klíče nahrávají do LoRa testeru byl popsán v kapitole 2.4.3 a není tudíž potřeba tento postup popisovat od začátku. Jak je možné vidět na obr. 56, do sítě ChirpStack přichází data z koncové zařízení. LoRa testeru se úspěšně podařilo připojit do sítě ChirpStack. Je tedy možné tvrdit, že konfigurace sítě ChirpStack proběhla úspěšně a síť je plně funkční. Po uložení aktivačních klíčů do paměti vlastního koncové zařízení může být do ChirpStack sítě toto zařízení připojeno také.

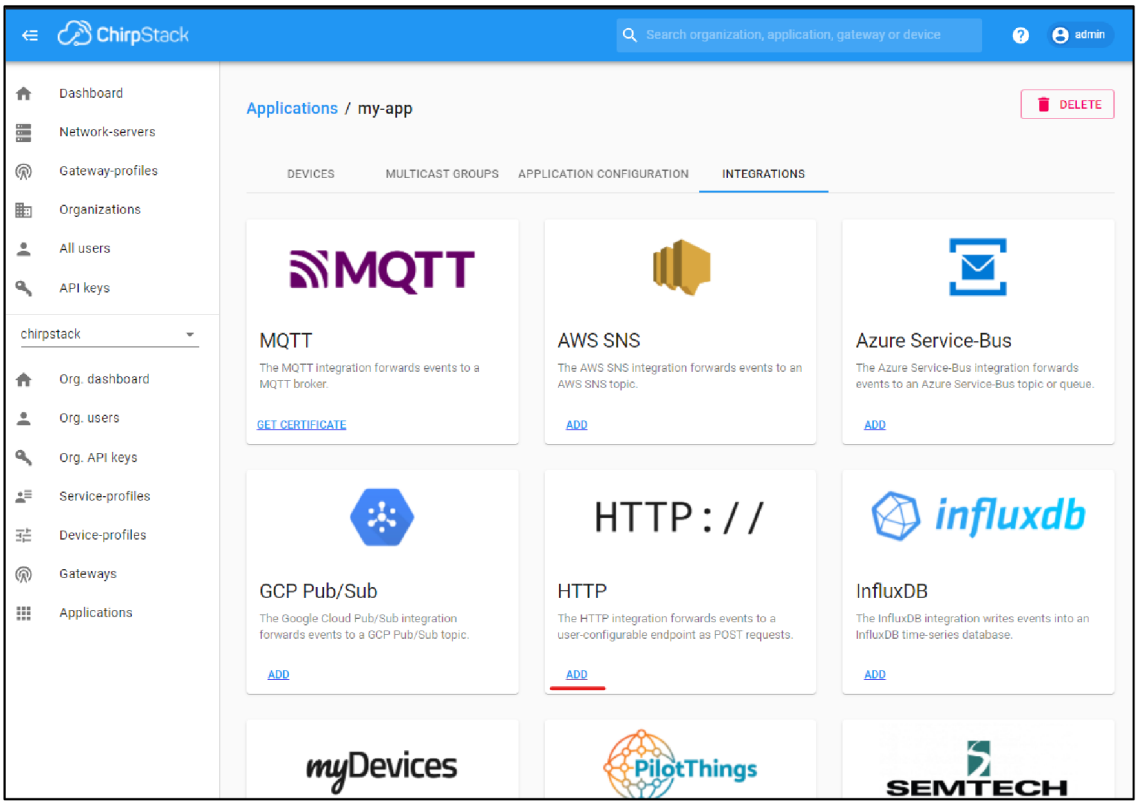


Obr. 56. Příchozí a odchozí datové rámce v síti ChirpStack

2.5.3 Zobrazení přijatých dat ze sítě ChirpStack na lokální webové stránce

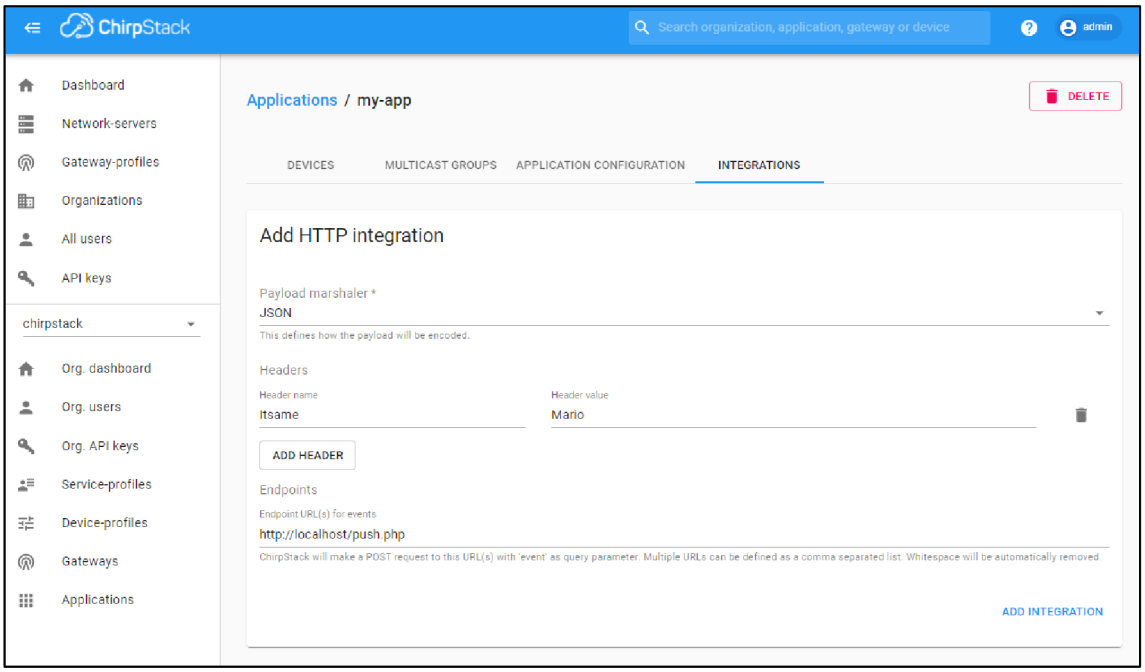
Aby bylo pro koncového uživatele možné sledovat přijatá data z koncového zařízení, je potřeba tato data někde zobrazovat. Za tímto účelem je proto potřeba vytvořit lokální server, na který se budou tato data posílat a koncový uživatel si je tak může prohlédnout a dále s nimi pracovat. Systém ChirpStack umí odesílat přijaté datové rámce z koncových zařízení na jiný server jako http push požadavek. Na to, aby mohli být tyto http push požadavky zpracovány, je potřeba mít server, který dokáže tyto požadavky uložit a následně je zobrazovat. Pro takovouto aplikaci je vhodný jazyk PHP, aby ale bylo možné hostovat PHP na platformě Raspberry Pi, je potřeba mít vytvořený server. Vhodný typ serveru by mohl být server Apache, ten ale na Raspberry Pi není předinstalovaný, a proto je potřeba ho nainstalovat, společně s potřebnými soubory pro PHP. Je tedy potřeba otevřít konzoli na Raspberry Pi a do ní zapsat příkaz: sudo apt install apache2 php libapache2-mod-php. Tento příkaz nainstaluje Apache2 lib mod PHP, což je modul, který umožňuje hostovat PHP. Následně je potřeba odstranit výchozí index.html., do konzole je tedy potřeba zadat příkaz: sudo mv /var/www/html/index.html /var/www/html/_index.html. Tento příkaz přejmenuje index.html na _index.html, díky tomuto přejmenování může být nahrán vlastní index.php. V posledním kroku je potřeba nakopírovat soubory push.php a index.php do složky /var/www/html.

Jakmile je server hotový, je možné propojit systém ChirpStack se serverem Apache. Systém ChirpStack k tomuto účelu nabízí několik možností integrace s různými aplikacemi, v této diplomové práci bude ale použit http požadavek, pro který byl vytvářen Apache server. Tyto integrace jsou vždy vázány na konkrétní aplikaci. Je tedy potřeba vybrat požadovanou aplikaci, u jejíhož koncového zařízení je požadováno odesílat data dál a přidat novou integraci http. Na obr. 57 je možné vidět různé integrační aplikace, spolu s označeným tlačítkem pro přidání http požadavku.



Obr. 57. Integrační aplikace dostupné v síti ChripStack

Pro přidání http integrace je potřeba vyplnit několik parametrů. Je potřeba vybrat formát zpráv, ve kterém budou rámce ze serveru odcházet, v rámci této diplomové práce byl zvolen formát JSON. Nastavení hlavičky není nutné, může být ale použita například pro autorizaci. Nakonec je potřeba nastavit adresu, na kterou budou datové rámce odesílány. Nastavovací stránku lze vidět na obr. 58.



Obr. 58. Nastavení HTTP integrace v síti ChirpStack

Příchozí data je následně možné sledovat na webové stránce, která je hostovaná na Apache serveru na Raspberry Pi (index.php).

3. ZÁVĚR

Cílem, této práce bylo realizovat dva LoRaWAN systémy, přičemž jeden z nich využíval síť TTN a druhý využíval síť ChirpStack. Tyto dva systémy se liší v tom, že TTN je primárně globální komunitní síť, jejíž systém běží na vzdálených serverech a není tudíž potřebné síť nikam instalovat. Naproti tomu síť ChirpStack je lokální síť, kterou je potřeba realizovat na průmyslovém počítači, nebo jiné dostatečně výkonné platformě. Zároveň bylo také potřeba vytvořit přesný popis toho, jak zmíněné LoRaWAN sítě uvést do provozu, protože korektních popisů, jak takovou síť uvést do provozu moc neexistuje a postup podle těch dostupných často končí neúspěchem.

Součástí práce byl také návrh a zprovoznění vlastního koncového zařízení, s následným připojením do sítě TTN a sítě ChirpStack. Součástí návrhu zařízení bylo blokové schéma, elektrické schéma a návrh desky plošného spoje. Deska byla navržena s ohledem na současnou situaci s nedostatkem komponent. Z toho důvodu jsou v zapojení navrženy tři různé LoRa moduly, které mají riziku s nedostupností předejít. Zároveň je výhoda tří různých modulů v tom, že pokud dojde k poškození jednoho z nich, je možné použít dva zbylé. Na DPS byl jako hlavní řídící člen zvolen mikrokontrolér STM32, který nabízí obsáhlou dokumentaci, různé podpůrné nástroje pro vývoj a výhodnou cenu vzhledem k dostupnému výkonu. Jako zdroj přenášených dat byl použit teplotní senzor komunikující po sběrnici I^2C. Z pohledu softwarového vybavení byly zprovozněny potřebné periferie mikrokontroléru, jako sběrnice SPI, I^2C, nebo GPIO vstupy/výstupy. Pro komunikaci se sítěmi TTN a ChirpStack byla použita LMIC knihovna, která zajišťuje síťovou vrstvu komunikace kompatibilní se zmíněnými sítěmi. Vlastní koncové zařízení se úspěšně podařilo připojit jak do sítě TTN, tak do sítě ChirpStack.

V rámci tvorby návodu, jak síť TTN a ChirpStack zprovoznit byl kladen důraz na to, aby byly popsány i kroky, které se mohou tvářit zdánlivě jednoznačné. U sítě TTN byl důkladně popsán postup tvorby vhodného uživatelského profilu, ve kterém se následně tvořili a konfigurovali parametry přístupové brány a koncového zařízení. Byl také popsán návod, jak správně nakonfigurovat a připojit routeru Mikrotik jako LoRaWAN vstupní bránu do sítě, a to i po fyzické stránce. Pro otestování toho, zda došlo ke korektní konfiguraci sítě TTN a vstupní brány byl použit komerčně dostupný LoRa tester od společnosti HARDWARIO, jehož konfigurace je také součástí návodu. Z pohledu prvního připojené koncového zařízení do sítě, je totiž lepší použít zařízení, o kterém je možné tvrdit, že neobsahuje takové chyby, které by mohli mít negativní vliv na připojení k síti. V postupu bylo popsáno také připojení vlastního koncového zařízení do sítě a tvorba integrační části pro přenesení dat z koncového zařízení na uživatelskou webovou stránku.

Vzhledem k tomu, že systém ChirpStack tvoří lokální LoRaWAN síť, bylo potřeba celý systém zprovoznit na dostatečně výkonné platformě, jako platforma bylo pak zvoleno Raspberry Pi 3, na kterém byl systém sítě zprovozněn. Tato platforma byla zvolena z důvodu dostupnosti i pro běžné uživatele a také zpětné kompatibilitě z dalšími verzemi platformy. Podobně jako u sítě TTN byl i u sítě ChirpStack popsán podrobný návod, jak tuto síť uvést do provozu. Byly popsány kroky konfigurace routeru Mikrotik, který bylo nutné překonfigurovat v důsledku jiných požadavků systému ChirpStack. Konfigurace platformy Raspberry Pi tak, aby na ni bylo možné systém ChirpStack nainstalovat. Postup instalace potřebných aplikací systému ChirpStack na platformu Raspberry Pi. Nastavení přístupové brány v konfiguračním rozhraní sítě. Nastavení koncového zařízení v síti tak, aby bylo možné data přijímat. Testovací připojení k síti s využitím LoRa testeru a zobrazení dat z koncového zařízení na lokálním webové stránce.

Výstupem této práce je zprovoznění dvou různých systémů, které tvoří síť LoRaWAN spolu s popisem toho, jak tyto systémy bod po bodu uvést do provozu. Součástí výstupů je také vlastní koncové zařízení, které se úspěšně podařilo do obou sítí připojit.

3.1 Budoucí využití

Díky vlastnímu koncovému zařízení se třemi různými LoRa moduly a zkušenostmi se zprovozněním lokální sítě bude možné vybudovat si vlastní rozsáhlejší lokální síť s vícero přístupovými branami, která bude sloužit jako část chytré domácnosti v rámci chystané domovní automatizace. Navíc bude možné testovat vhodnost jednotlivých LoRa modulů jak z pohledu spotřeby elektrické energie, tak z pohledu jejich spolehlivosti a schopnosti komunikovat na větší vzdálenosti.

POUŽITÉ ZDROJE:

[1] *Internet věcí.* [online]. Wikipedie. [Cit. 30.12.2021]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_věcí

[2] *WHAT IS 6LOWPAN AND WHY SHOULD I TRY IT IN MY IOT PROJECT?* [online]. Zolertia. [Cit. 30.12.2021]. Dostupné z: https://zolertia.io/6lowpan-iot-protocol/

[3] *Sigfox Technical Overview* [online]. Avnet. [Cit. 30.12.2021]. Dostupné z: https://www.avnet.com/wps/wcm/connect/onesite/03aebfe2-98f7-4c28-be5f-90638c898009/sigfox-technical-overview.pdf?MOD=AJPERES&CVID=magVa.N&CVID=magVa.N&CVID=magVa.N

[4] MAŠEK Pavel, ŠTŮSEK Martin, FUJDIAK Radek, MLÝNEK Petr, HOŠEK Jiří, *KOMUNIKACNÍ SYSTÉMY PRO IOT*. ÚSTAV RADIOELEKTRONIKY, FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ, VUT V BRNĚ, Technická 3058/10, 616 00 Brno, Česká republika, 2020. [Cit. 30.12.2021]

[5] LOM Michal, PŘIBYL Ondřej, *Sítě pro internet věcí v České republice* [online]. TZB-info. [Cit. 30.12.2021]. Dostupné z: https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice

[6] BOISGUENE Rubbens, SHENG-CHIA Tseng, CHIH-WEI Huang, PHONE Lin, *A Survey on NB-IoT Downlink Scheduling: Issues and Potential Solutions,* Department of Communication Engineering, National Central University, Taoyuan, Taiwan. [Cit. 30.12.2021]

[7] *LoRaWAN R1.0 Open Standard Released for the IoT.* [online]. Businesswire. [Cit. 30.12.2021]. Dostupné z: https://www.businesswire.com/news/home/20150616006550/en/LoRaWAN-R1.0-Open-Standard-Released-IoT

[8] *LoRaWAN.* [online]. TREND MICRO. [Cit. 30.12.2021]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/lorawan

[9] RASMI SHARAN Sinha, YIQIAO Wei, SEUNG-HOON Hwang. *A survey on LPWA technology: LoRa and NB-IoT*. [online]. Division of Electronics and Electrical Engineering, Dongguk University-Seoul, Republic of Korea. [Cit. 30.12.2021]. Dostupné z: www.sciencedirect.com

[10] *What are LoRa® and LoRaWAN®?*. [online]. LORA DEVELOPER PORTAL. [Cit. 30.12.2021]. Dostupné z: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/

[11] SEUNGKU Kim, HEONKOOK Lee, SUNGHO Jeon, *An Adaptive Spreading Factor Selection Scheme for a Single Channel LoRa Modem.* [online]. National Center for Biotechnology Information. [Cit. 30.12.2021]. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7070984/

[12] *IEEE 802.15.4.* [online]. Wikipedie. [Cit. 30.12.2021]. Dostupné z: https://en.wikipedia.org/wiki/IEEE_802.15.4

[13] *Introduction of IEEE 802.15.4 Technology.* [online]. Geeks for Geeks. [Cit. 30.12.2021]. Dostupné z: https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/

[14] CODELUPPI Gaia, CILFONE Antonio, DAVOLI Luca, FERRARI Gianluigi. LoRaFarM: A LoRaWAN-Based Smart Farming Modular IoT Architecture. [online]. Research Gate. [Cit. 30.12.2021]. Dostupné z: https://www.researchgate.net/publication/340484378_LoRaFarM_A_LoRaWAN-Based_Smart_Farming_Modular_IoT_Architecture

[15] HAXHIBEQIRI Jetmir, POORTER Eli De, MOERMAN Ingrid, HOEBEKE Jeroen, *A Survey of LoRaWAN for IoT: From Technology to Application.* IDLab, Department of Information Technology at Ghent University—IMEC, 9052 Ghent, Belgium [Cit. 30.12.2021].

[16] KIM Dong-Hoon, LEE Eun-Kyu, KIM, Jibum. *Experiencing LoRa Network Establishment on a Smart Energy Campus Testbed.* [online]. Research Gate. [Cit. 30.12.2021]. Dostupné z: https://www.researchgate.net/publication/332151302_Experiencing_LoRa_Network_Establishment_on_a_Smart_Energy_Campus_Testbed

[17] LIANDO Jansen Christiano, GAMAGE Amalinda, TENGOURTIUS Augustinus, LI Mo, *Known and Unknown Facts of LoRa: Experiences from a Large-scale Measurement Study.* [online]. Research Gate. [Cit. 30.12.2021]. Dostupné z: https://www.researchgate.net/publication/331294324_Known_and_Unknown_Facts_of_LoRa_Experiences_from_a_Large-scale_Measurement_Study

[18] NOURA Hassan, HATOUM Tarif, SALMAN Ola, YAACOUB Jean-Paul, CHEHAB Ali, *LoRaWAN security survey: Issues, threats and possible mitigation techniques.* [online] Science Direct. [Cit. 30.12.2021]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S2542660520301359

[19] *The Raspberry Pi Foundation* [online] Raspberry Pi [4.5.2022]. Dostupné z: https://www.raspberrypi.com/products/raspberry-pi-3-model-a-plus/

SEZNAM SYMBOLŮ A ZKRATEK

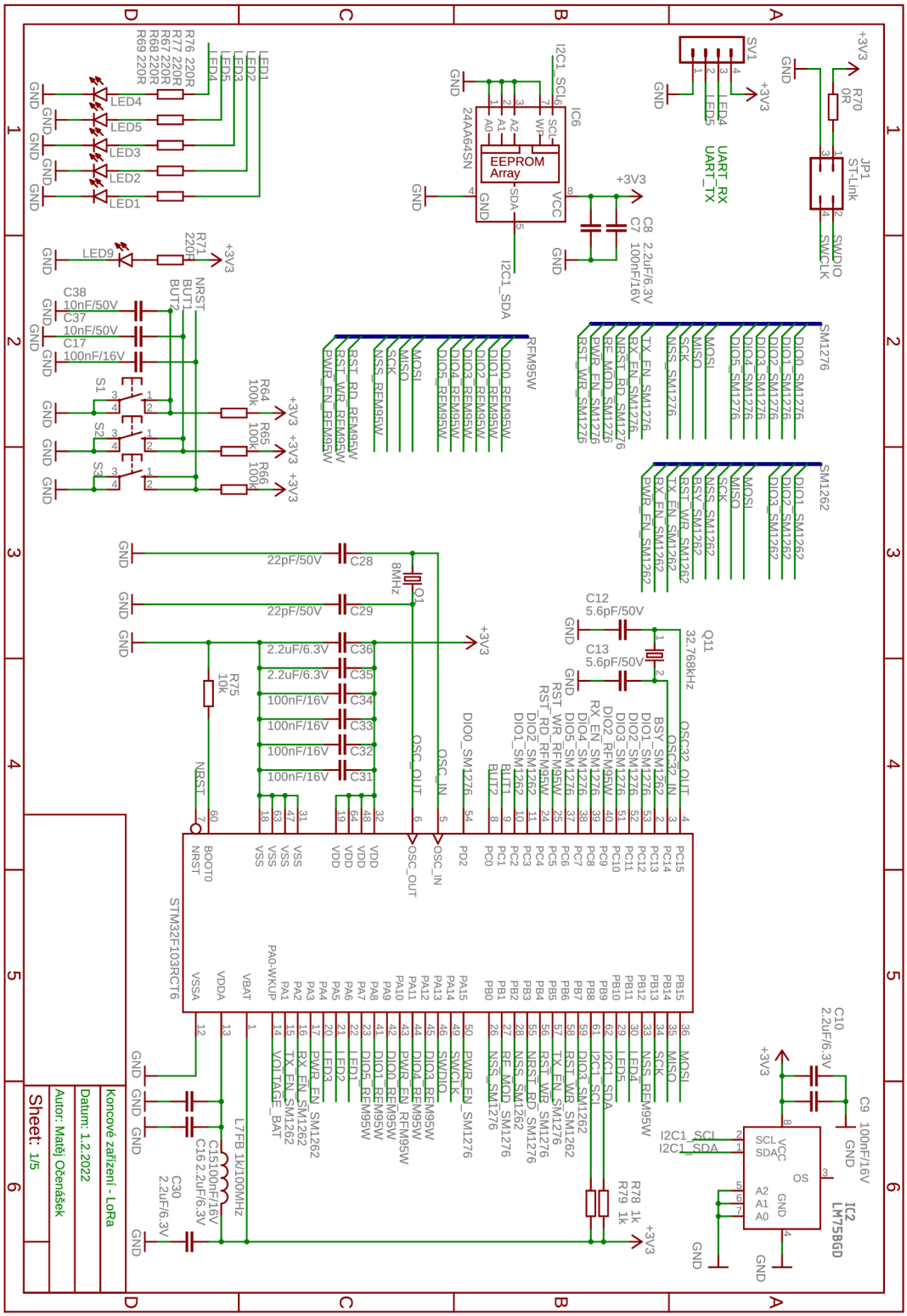
Zkratky:

WAN	Wide Area Network
ISM	Insdustrial, Sience, Medical
LoRa	Long Range
TTN	The Things Network
WPAN	Wireless Personal Area Network
IETF	Internet Engineering Task Force
CoAp	Constrained Application Protocol
MQTT	MQ Telemetry Transport
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
PHY	Physical Layer
DSSS	Direct Sequence Spread Spectrum
B2B	Business to Business
B2C	Business to Customer
UNB	Ultra-Narrow Band
bps	bits per second
GPS	Global Positioning System
NB-IoT	Narrow Band - Internet of Things
LTE	Long Term Evolution
OTAA	Over The Air Authentication
ABP	Authentication By Personalisation
CSS	Chirp Spread Spectrum
SF	Spreading Factor
BW	Bandwidth
CR	Code Rate
TX	Transmitt
RX	Receive
ADR	Adaptive Data Rate
MIC	Message Integrity Check
CRC	Cyclic Redundancy Check
AES	Advanced Encryption Standard
VPN	Virtual Private Network
HTTPS	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
CMAC	Cipher-based Message Authentication Code

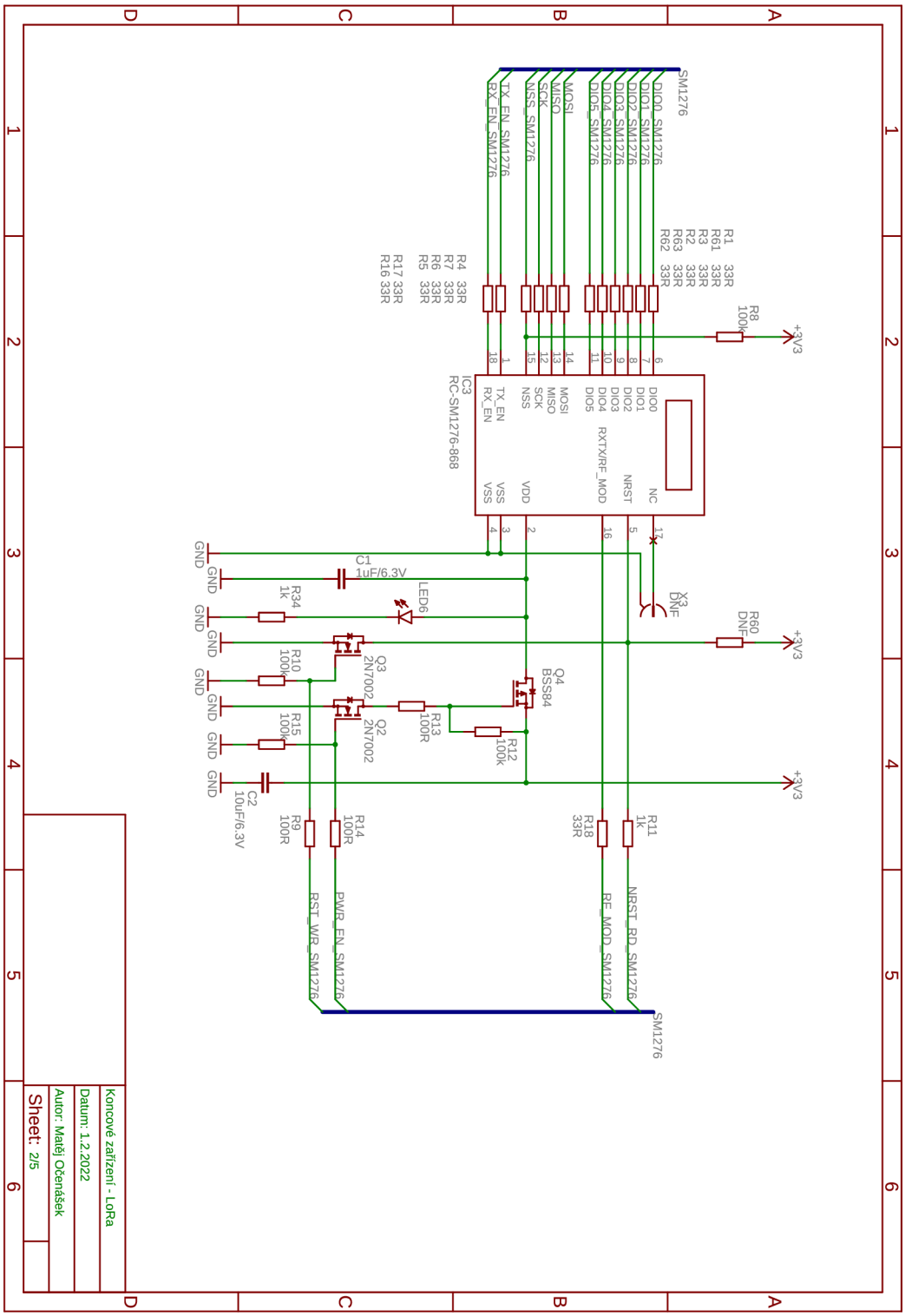
Symboly:

Rb	bitová rychlost modulace	(bit/s)
BW	šířka pásma modulace	(Hz)
SF	činitel rozprostření	(-)

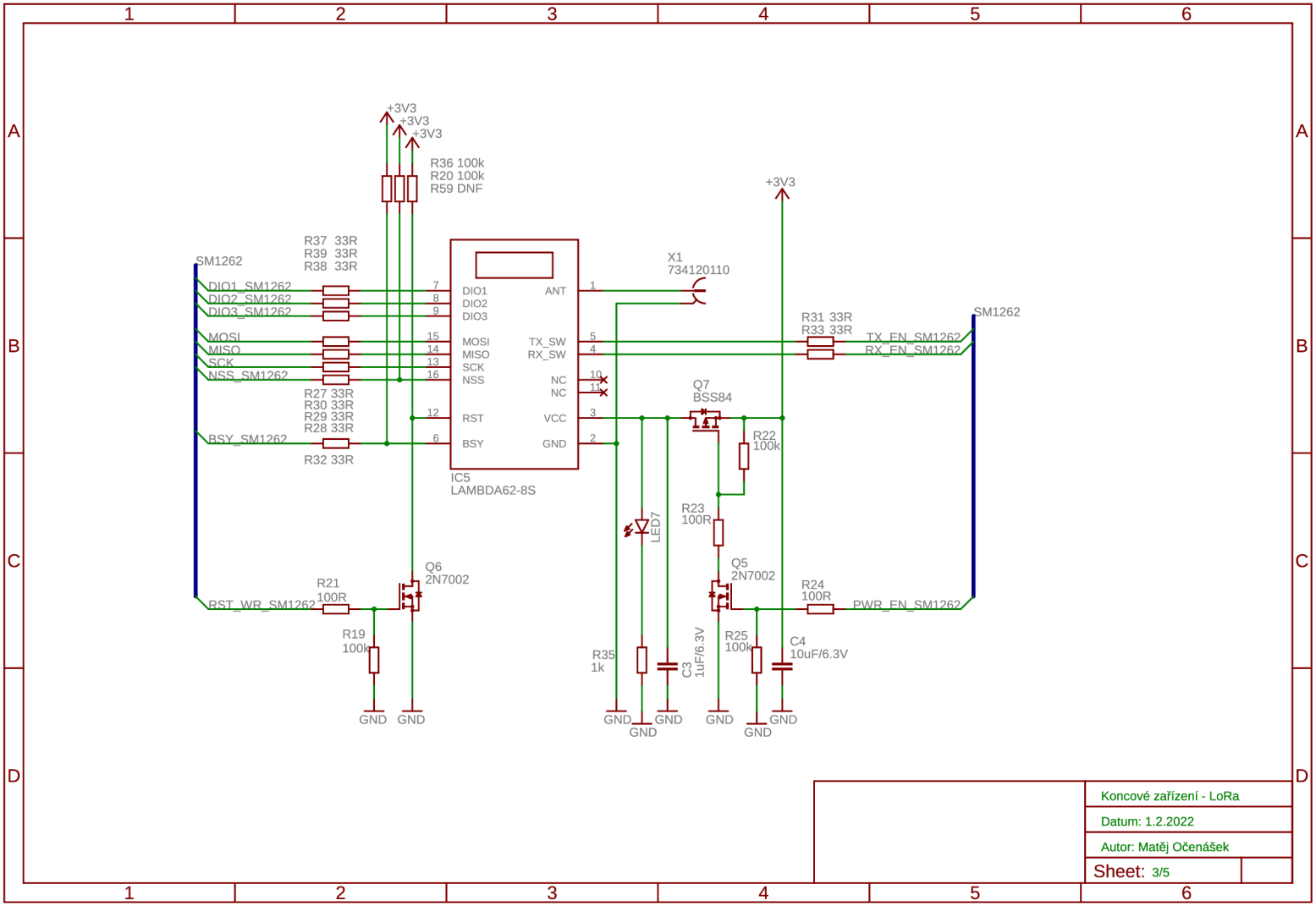
Příloha A – Elektrické schéma obvodu



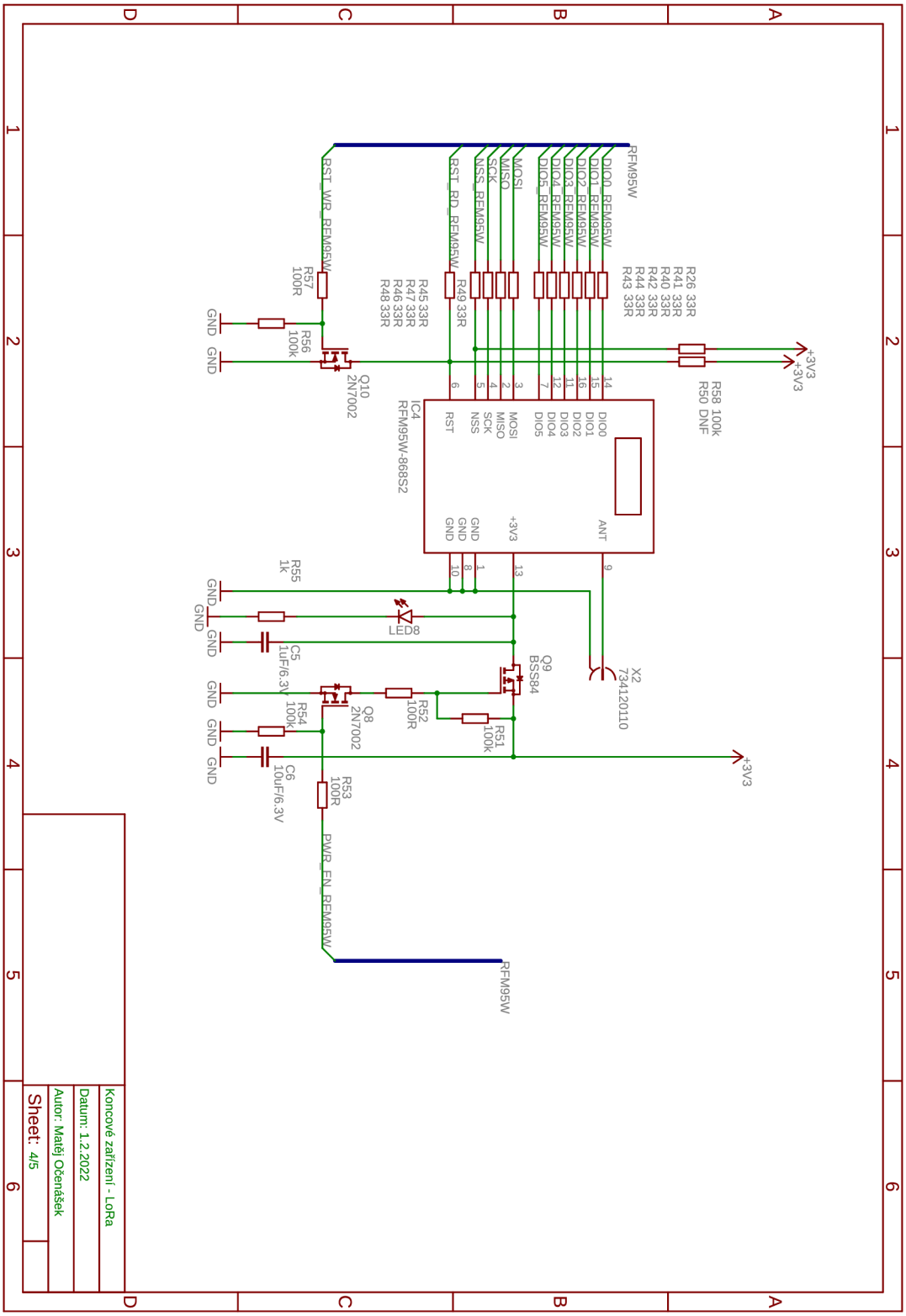
Obr. A1. Elektrické schéma obvodu část 1



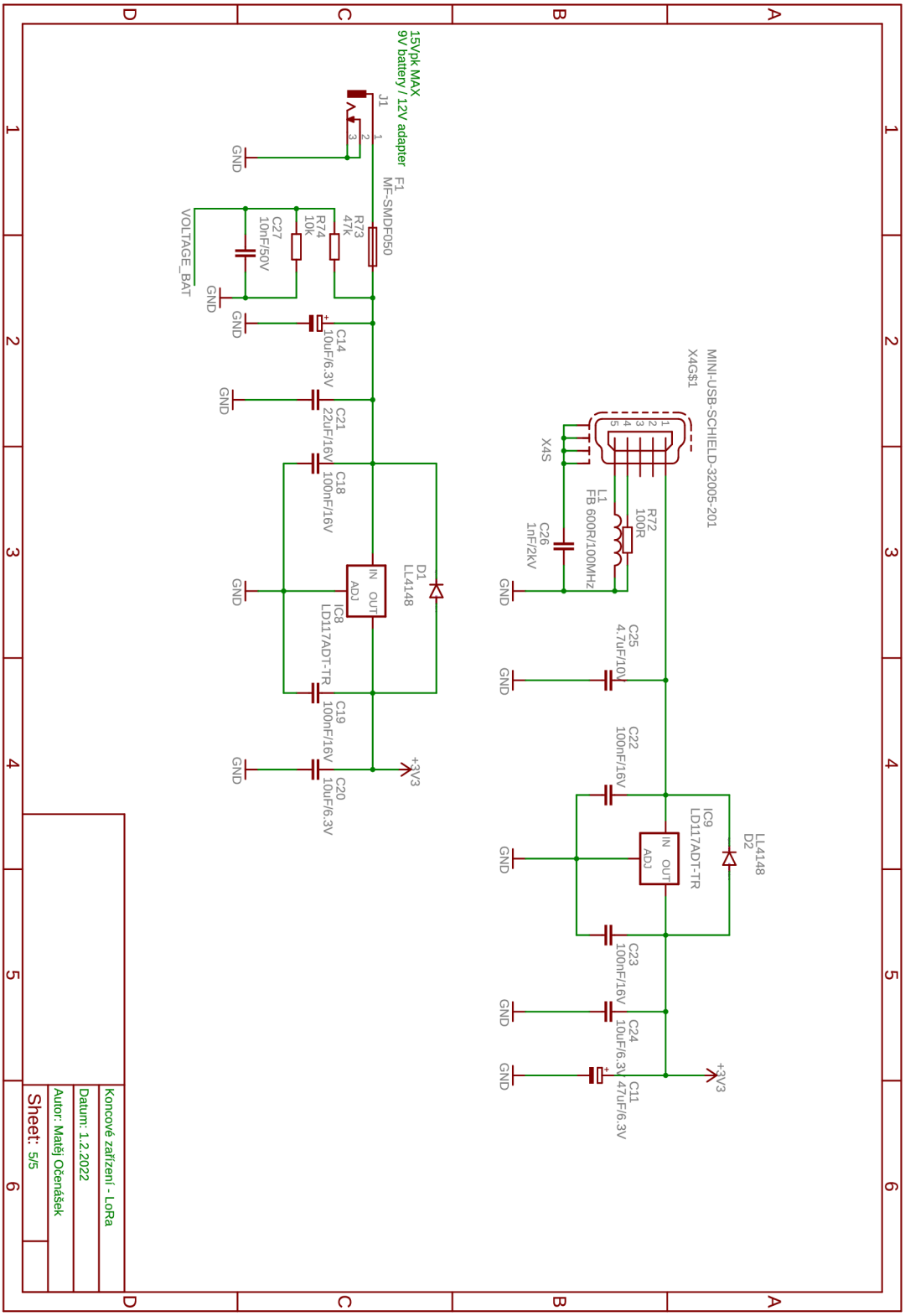
Obr. A2. Elektrické schéma obvodu část 2



Obr. A3. Elektrické schéma obvodu část 3

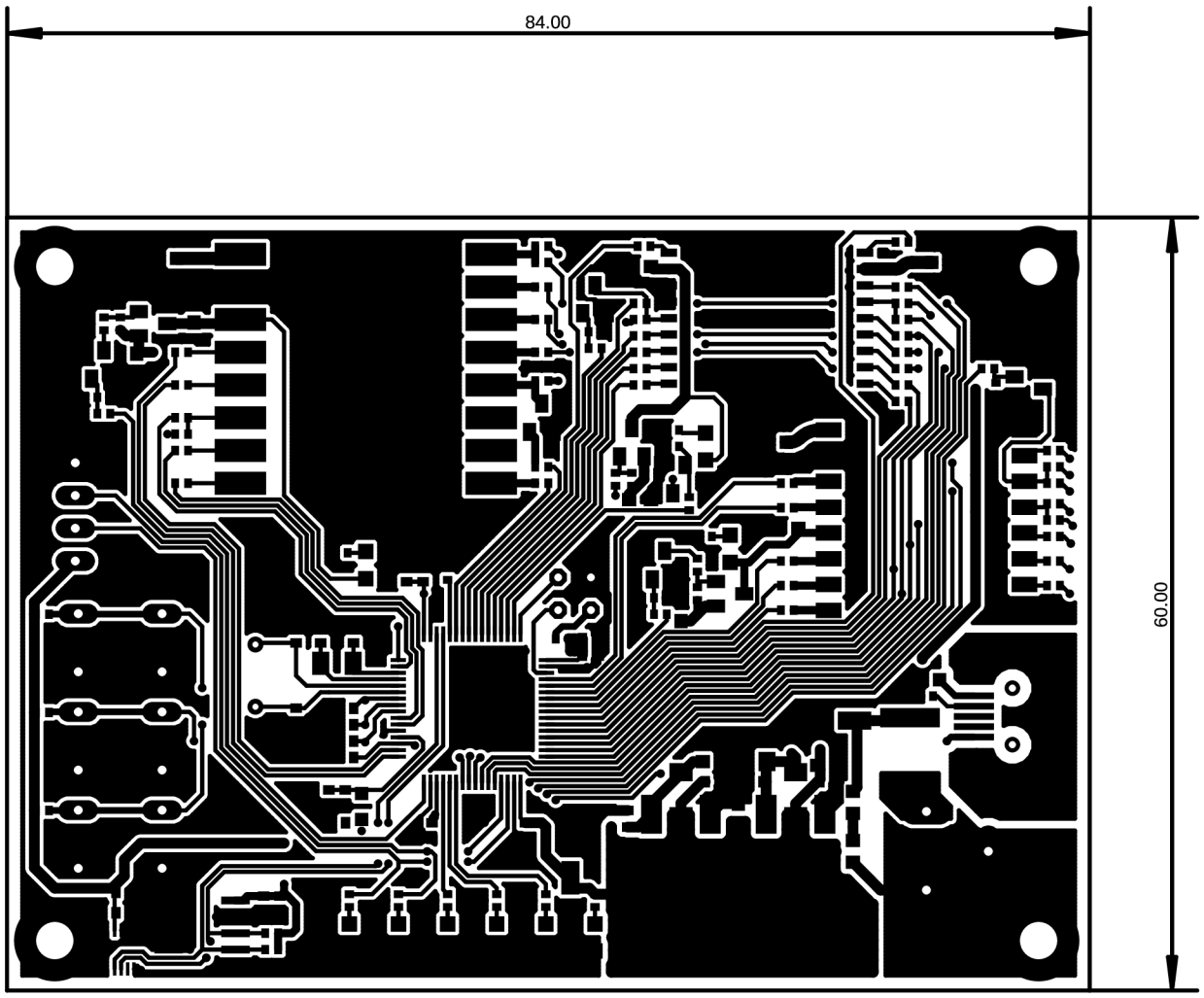


Obr. A4. Elektrické schéma obvodu část 4

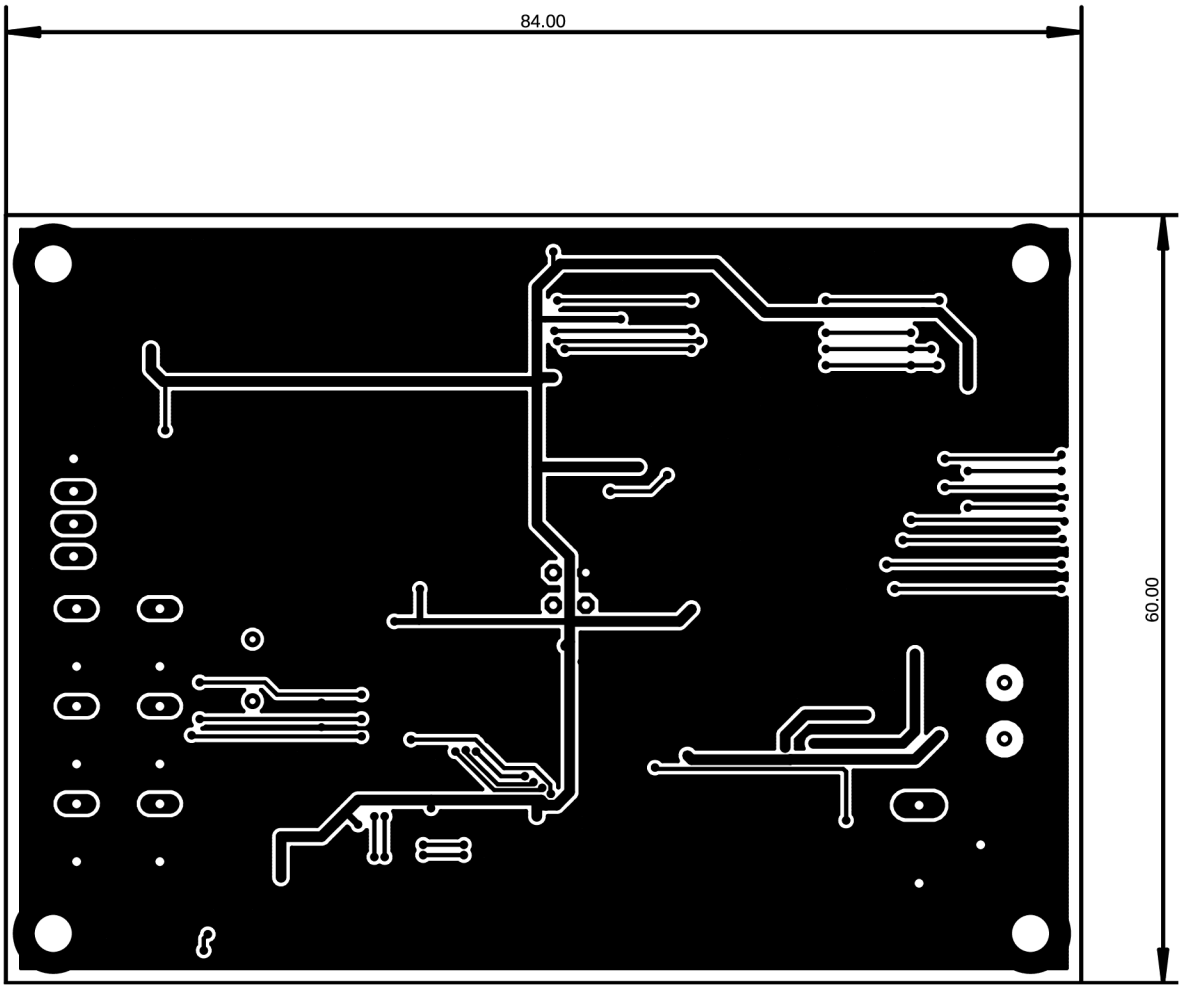


Obr. A5. Elektrické schéma obvodu část 5

Příloha B – Motiv DPS

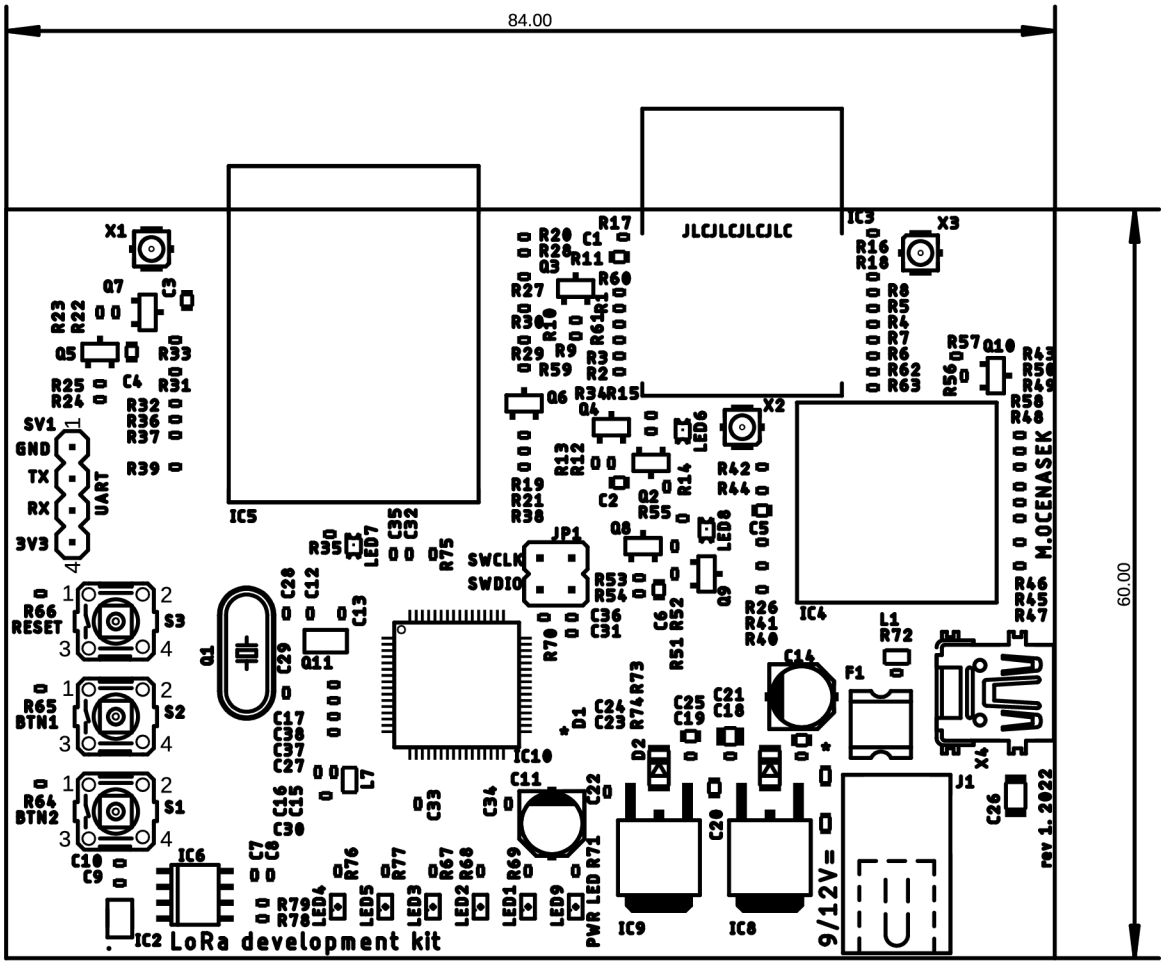


Obr. B1. Okótovaný DPS motiv z horní strany



Obr. B2. Okótovaný DPS motiv ze spodní strany

Příloha C – Osazovací plán



Obr. C 1. Osazovací plán DPS