Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Integrace IoT do infrastruktury podniku

Bakalářská práce

Autor: Jakub Střihavka
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Pavel Blažek

Hradec Králové duben 2019

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

……

V Hradci Králové dne 28.4.2019 Jakub Střihavka

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Pavlu Blažkovi za metodické vedení práce, cenné rady, pevné nervy a ochotu. Rád bych také poděkoval Rostislavu Špinarovi za jeho pomoc při zprovoznění IQRF brány.

Anotace

Tato bakalářská práce se zaměřuje na problematiku integrace Internet of Things (IoT), neboli Internetu věcí, do stávající infrastruktury datové sítě podniku a jejího zabezpečení. V podmínkách dynamicky se rozrůstajících firem je implementace nových progresivních technologií nezbytným krokem v konkurenčním boji. Pro bezpečné zapojení specifických komponent, jakými IoT jednoznačně je, do podnikového systému je potřeba znát detailně stávající topologii sítě, požadavky nové technologie a případná bezpečnostní rizika, která s sebou mohou přinést. V rámci této práce je zpracován jak teoretický základ, tak i popsán praktický postup modelové implementace IoT zařízení do datové sítě, který byl simulován v domácí síti autora.

Klíčová slova

IoT, IQRF, Infrastruktura, Zabezpečení, Topologie, Cloud

Annotation

Title: IoT integration into enterprise infrastructure

This bachelor thesis focuses on the issue of integration of Internet of Things (IoT) into the existing data network infrastructure of the company and its security. Under the conditions of dynamically growing companies, the implementation of new progressive technologies is a necessary step in the competitive fight. To securely connect specific components such as the IoT to the enterprise system, it is necessary to know in detail the current network topology, the requirements of the new technology and the potential security risks they may bring. In this work is elaborated both theoretical basis and described practical procedure of model implementation of IoT devices into data network, which was simulated in author's home network.

Keywords

IoT, IQRF, Infrastructure, Security, Topology, Cloud

Obsah

Seznam obrázků

1 Úvod

V dnešní době moderních technologií a stálého technologického růstu není v silách firem neustále reagovat na nové trendy. Novější technologie ale mohou výrazně pomoci v organizaci, ulehčit práci zaměstnancům, zautomatizovat výrobu a zvýšit zisk podniku. Například se může jednat o automatické nastavování klimatizace v místnosti podle toho, jaký zaměstnanec se zrovna v místnosti nachází a jakou teplotu on sám preferuje, nebo třeba automatické skladníky, které vyzvednou zboží z regálu a dovezou ho na požadované místo. Většina delší dobu zavedených podniků však používá již funkční infrastrukturu a předělat ji celou na novější technologie je velice nákladné a náročné. Cílem této práce je seznámit s technologiemi Internet of Things (IoT), nastínit problematiku jejich fungování, navrhnout integraci IoT technologií do existující firmy a poukázat na specifičnost problematiky zabezpečení dat. Nejdůležitější je totiž vyřešit, jaké technologie zvolit a jak je zabezpečit, spolu s jejich důležitými a soukromými daty, proti přístupu neoprávněných uživatelů a jejich následným zneužitím.

Pro dosažení cíle je nutné mít dostatečný přehled o technologiích a principech jejich fungování. Proto se úvodní část zaměřuje na popis základů počítačových sítí, jejich prvky, zařízení, firemní topologie a zabezpečení sítí. Dále je zde popsáno, jaké zabezpečení je nejlepší ve firmě zvolit pro ochranu všech důležitých dat a co je to IoT. Právě u IoT bylo dále rozvedeno, jak je možné jej s co nejmenšími náklady a vysokým stupněm zabezpečení zaintegrovat do infrastruktury podniku.

V další části je pak popsáno praktické provedení zprovoznění zvolené IoT technologie, IQRF. Zapůjčená zařízení byla zapojena do infrastruktury autorovy domácí sítě s demonstrací možného základního zabezpečení.

Jedním z důvodů vybrání tohoto tématu je autorova práce v oboru analýzy uživatelských dat. Dalším důvodem je zájem o nové technologie a svět IoT, jelikož dokážou velice ulehčit a zpříjemnit život.

2 Prvky datové sítě

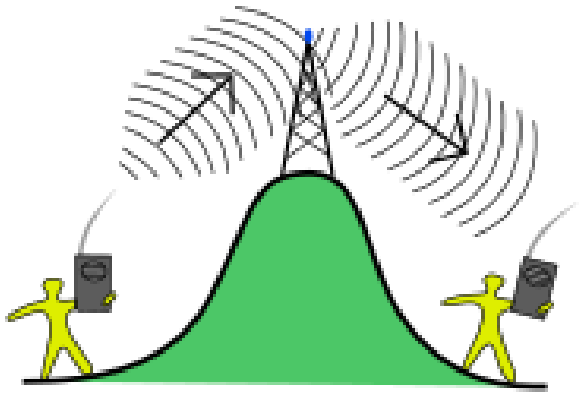
Síťové prvky se dělí na aktivní a pasivní. Jejich vhodnou kombinací dostáváme datovou síť, která zabezpečuje přenos informací mezi koncovými zařízeními, která jsou do ní připojená.

2.1 Aktivní síťové prvky

Tyto prvky jsou jakákoliv zařízení, sloužící k vzájemnému propojení v síti. Za aktivní prvky se považuje vše, co jakýmkoli způsobem aktivně působí na přenášené signály (zesiluje, regeneruje, nebo jinak upravuje). Mezi aktivní prvky patří především repeater (opakovač), hub (rozbočovač), switch (přepínač), bridge (most) a router (směrovač). Do skupiny aktivních síťových prvků patří i síťová karta, nebo tiskový server.

2.1.1 **Repeater**

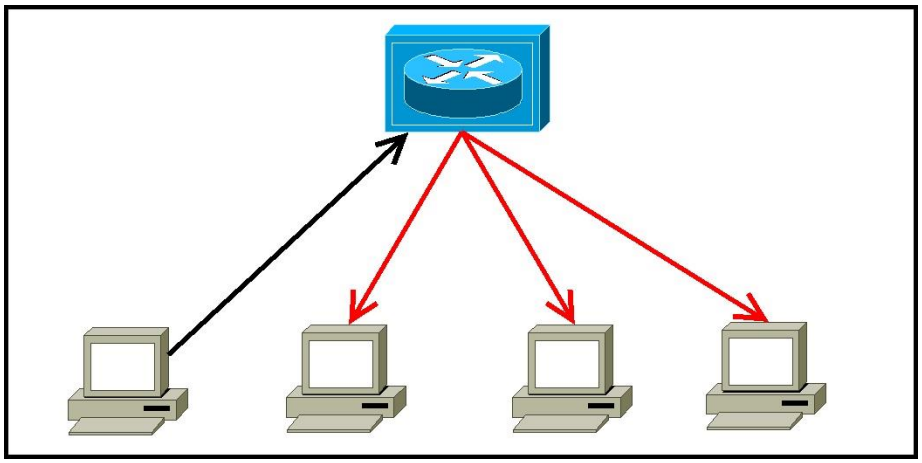
Elektronické zařízení, které přijímá zašuměný, zkreslený, nebo jinak poškozený signál a vysílá ho dále již opravený a zesílený. Tím lze dosáhnout vyššího dosahu média bez ztráty kvality. [1] Funkcionalita repeateru je zobrazena na Obr. 1.



Obr. 1 - Funkcionalita repeateru (zdroj: [2])

2.1.2 Hub

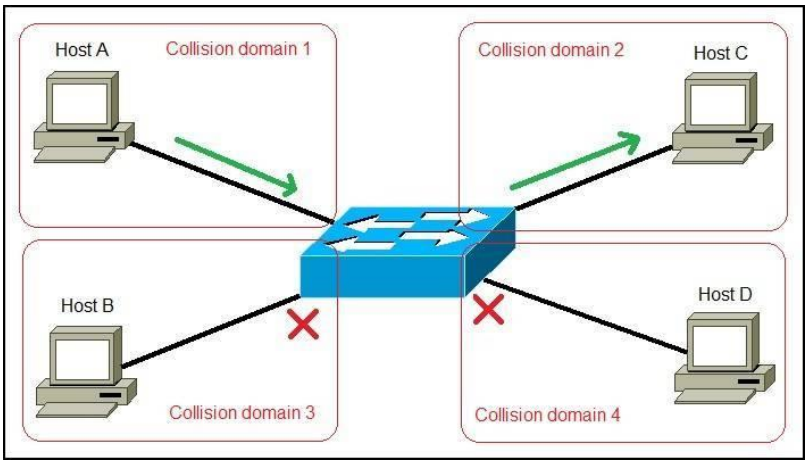
Umožňuje větvení sítě tím, že veškerá data, která přijdou na jeden z portů, zkopíruje na všechny ostatní porty. Nebere v potaz, komu data náleží. To způsobuje, že každý v síti může vidět všechna síťová dat a ve větších sítích to znamená zbytečné přetěžování uzlů, kterým data nejsou určena.[1] Funkcionalita Ethernet hubu zobrazena na Obr. 2.



Obr. 2 – Funkcionalita ethernet hubu (zdroj: [3])

2.1.3 Switch

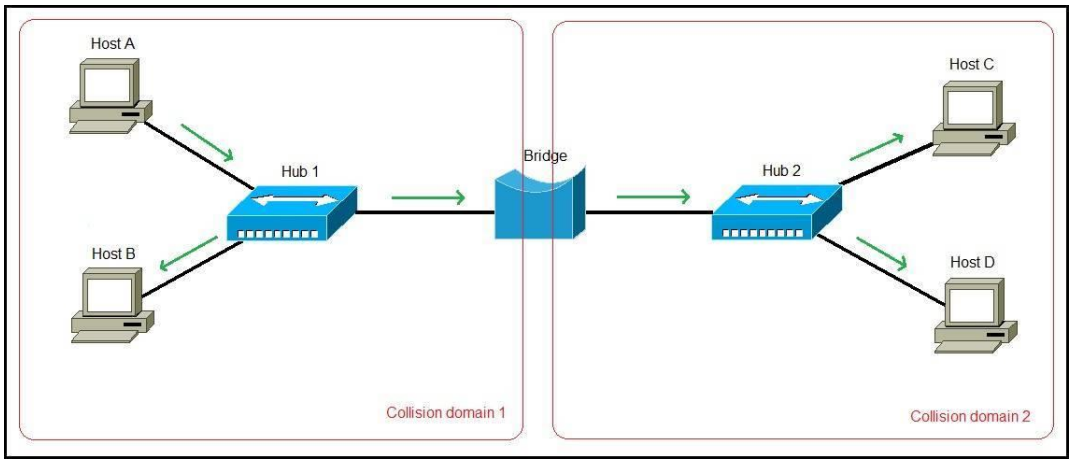
Propojuje jednotlivé segmenty sítě. Připojují se k němu síťová zařízení, nebo části sítě. Rámce se rozesílají jen do rozhraní, pro které jsou určena pomocí MAC adresy, které se postupně učí. Pokud danou MAC adresu nezná, vyšle rámec na všechny své porty kromě portu, ze kterého rámec přišel. [1] Znázornění funkce switche je zobrazeno na Obr. 3.



Obr. 3 – Switch (zdroj: [4])

2.1.4 Bridge (most)

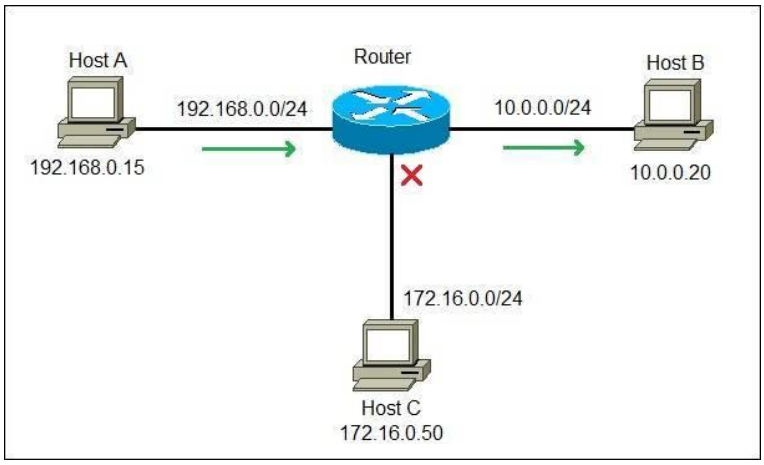
Určen ke spojení dvou LAN (Local Area Network) sítí. Odděluje také provoz mezi různými segmenty sítě. Ve své paměti RAM si sestavuje tabulku MAC adres (fyzické adresy) a jejich portů. Podle této tabulky zjišťuje, zda příjemce leží ve stejném segmentu jako odesílatel. Pokud v tomto segmentu leží, tak do jiného segmentu rámce nerozešle. [5] Spojení dvou LAN sítí pomocí mostu je znázorněno na Obr. 4.



Obr. 4 – Bridge (zdroj: [4])

2.1.5 Router

Procesem zvaným routování přeposílá datagramy do jejich cíle dle jejich IP adresy. Vybírá nejvhodnější cestu do cíle podle kritérií zvoleného routovacího protokolu. Router si uchovává záznamy o nejlepší cestě k danému cíli ve své směrovací tabulce. [1] Funkce routeru viz Obr. 5.



Obr. 5 – Router (zdroj: [6])

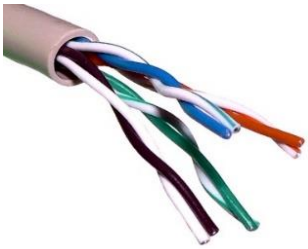
2.2 Pasivní síťové prvky

Mezi pasivní síťové prvky řadíme především kabeláž, konektory, rozvaděče a zásuvky, které fyzicky přenáší data mezi koncovými body. Pro svůj provoz nespotřebovávají elektrickou energii.

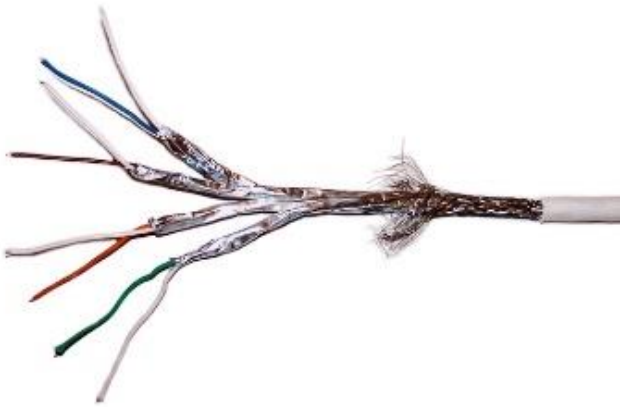
2.2.1 Kroucená dvojlinka

Druh kabelu používaný v počítačových sítích. Je tvořen páry vodičů, které přenášejí data. Páry vznikají zakroucením 2 vodičů do sebe. Následně jednotlivé páry jsou do sebe také pravidelným způsobem zakrouceny. Souběžně jdoucí vodiče, kterými prochází nějaký střídavý signál, vyzařují do svého okolí elektromagnetické vlny. Důvodem kroucení párů je právě odstínění a minimalizace tohoto vyzařovaného elektromagnetického záření do okolí i jeho příjem z okolí.
Existuje buď nestíněná kroucená dvojlinka (UTP – Unshielded Twisted Pair, viz Obr. 6), nebo stíněná (STP – Shielded Twisted Pair, viz Obr. 7).
Stíněná kroucená dvojlinka obsahuje navíc stínění, které mnohem více eliminuje vyzařované a přijímané elektromagnetické záření. [7]
Druhy stínění:

- Individuální stínění – Každý pár, nebo čtveřice vodičů, je obalen pokovenou fólií. Toto stínění zmírňuje elektromagnetickému záření vstoupit do kabelu, nebo ho opustit a také zamezuje přeslechy sousedních párů. [8]
- Celkové stínění – Všechny vodiče jsou spolu obaleny pokovenou fólií, nebo pletenými kovovými drátky. Toto stínění zmírňuje elektromagnetickému záření vstoupit do kabelu, nebo ho opustit. [8]
- Individuální stínění + celkové stínění – Kombinace individuálního a celkového stínění. [8]



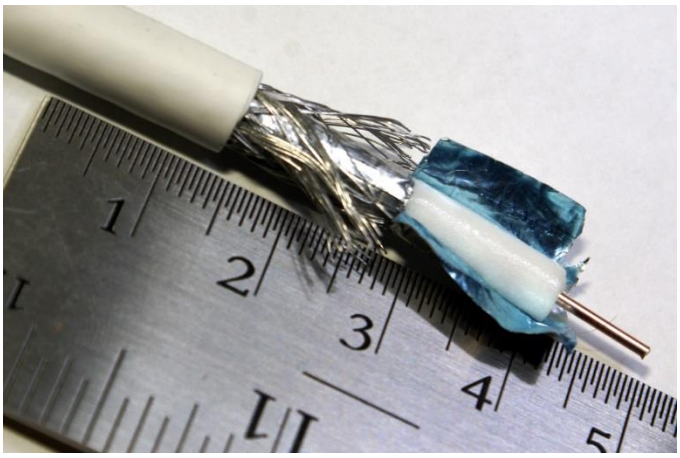
Obr. 6 – Nestíněná kroucená dvojlinka (zdroj:[9])



Obr. 7 – Stíněná kroucená dvojlinka (zdroj: [10])

2.2.2 Koaxiální kabel

Elektrický kabel, který obsahuje jeden vnější vodič a jeden vodič vnitřní. Vnější vodič je válcový a je často nazýván jako stínění. Vnitřní vodič je buď drátový, nebo trubkový a je označován jako jádro. Mezi vnějším a vnitřním vodičem se nachází nevodivá vrstva (dielektrikum), která napomáhá oddělení vodičů. [11] Koaxiální kabel RG-6 viz Obr. 8.



Obr. 8 - Koaxiální kabel RG-6 (zdroj:[12])

2.2.3 Optický kabel

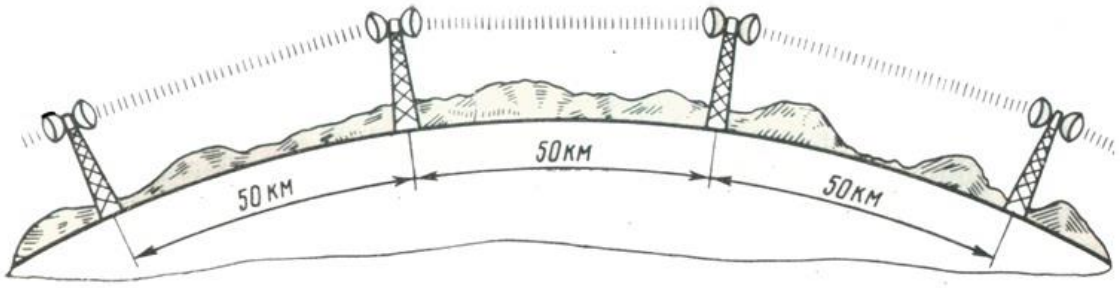
Obsahuje skleněná nebo plastová vlákna, přes které se prostřednictvím světla přenáší signály. Umožňují přenos na delší vzdálenosti a mnohem vyšší rychlost než jiné formy komunikace. [13] Optický kabel je vyobrazen na Obr. 9.

Obr. 9 – Optický kabel (zdroj:[14])

2.2.4 Mikrovlnné spoje

Bezdrátové připojení za pomocí radiových vln. Přenáší obvykle digitální signál. Často se používá pro přenos signálu na dlouhou vzdálenost. Může se používat pro pozemský přenos, pro komunikaci mezi Zemí a satelity na oběžné dráze Země, nebo i komunikaci ve vesmíru. [15]

Mikrovlny se používají i pro radary, radionavigační systémy a senzorové systémy. Přenos informací může probíhat jednosměrně (televizní vysílání) a obousměrně (komunikační satelity). [15] Radioreléová trasa je zobrazena na Obr. 10.



Obr. 10 - Radioreléová trasa (zdroj:[16])

2.2.5 **Wi-Fi**

Jedná se o bezdrátový přenos dat v počítačových sítích. Wi-Fi zařízení jsou dnes prakticky ve všech přenosných počítačích a chytrých telefonech.

Spojení je tvořeno pomocí bezdrátového média (nejčastěji elektromagnetických vln), a ne drátovým spojem. Často jsou bezdrátové sítě prodloužením sítí drátových nebo existují společně. Jejich signál lze zachytit i přes zeď. Dosah Wi-Fi závisí na anténě a jejím vysílacím výkonu. Většinou se ale jedná o vzdálenosti v řádech desítek až stovek metrů. Běžné Wi-Fi sítě dosáhnou přibližně do 100 metrů. [17]

Wi-Fi pracuje v bezlicenčním pásmu 2,4 GHz a 5 GHz a používá standardy IEEE 802.11. [17] Přehled IEEE 802.11 standardů viz Obr. 11.

Standard	Pásmo (GHz)	Maximální rychlost (Mbit/s)
IEEE 802.11	2,4	2
IEEE 802.11a	5	54
IEEE 802.11b	2,4	11
IEEE 802.11g	2,4	54
IEEE 802.11n	2,4 nebo 5	600
IEEE 802.11ac	2,4 nebo 5	1800

Obr. 11 – Přehled standardů IEEE 802.11 (zdroj: vlastní zpracování)

Mimo toho existují i další standardy, které pracují na frekvencích licencovaných, tedy placených, pásem. Často jsou používané pro přenosy dat na větší vzdálenosti, kde není možné nebo výhodné použít kabeláž.

2.2.6 **Strukturovaná kabeláž**

Jedná se o instalaci kabelových systémů, které budou podporovat vícero hardwarových použití a jsou vhodné pro dnešní potřeby i potřeby v budoucnu. Správně nainstalovaný systém strukturované kabeláže bude schopen podporovat jakýkoliv později přidaný hardware. [18]

Ve strukturované kabeláži se vyskytují pojmy telekomunikační zásuvky, patch panel, horizontální kabeláž a vertikální kabeláž.

Hlavní část strukturované kabeláže je serverovna. V ní je umístěn hlavní switch (nebo více switchů) a propojuje jednotlivé switche budov, pater, nebo místností.

Uvedené switche jsou vzájemně propojeny vertikální kabeláží. Vertikální kabeláž se také nazývá páteřní kabeláž. [19]
Jednotlivé switche se umisťují do uzamykatelných racků, nebo uzavřených místností pro zamezení přístupu nepovolaným osobám a zvýšení zabezpečení sítě. Do switchů jsou horizontální kabeláží připojeny telekomunikační zásuvky, nejčastěji přes patch panel. Telekomunikační zásuvky jsou umístěny na pracovišti a lze do nich připojit koncová zařízení, jako je třeba počítač, tiskárna a jiná zařízení pomocí kabelu. Typ potřebného kabelu závisí na použité telekomunikační zásuvce a jejích portech. Zásuvky obvykle obsahují porty RJ-45 pro připojení ethernetového kabelu (často se jedná o UTP kroucenou dvojlinku). [19]
Patch panel obsahuje totiž velké množství portů a je tak ideální pro připojení většího množství zásuvek. Patch panel propojuje jednotlivé zásuvky a je potom připojen do switche pomocí patch kabelu. [19]

2.2.7 **Aktuální – praktické využití pasivních prvků**

Nejpoužívanější typ strukturované kabeláže je UTP kabel kategorie 5e (Cat 5e). Pro svůj přenos využívá kroucenou dvojlinku. Při využití všech čtyř párů nabízí maximální rychlost 1000BASE-T, neboli 1 Gb/s při použití na vzdálenost do 100 metrů. [20][21]
Tato kabeláž se nejčastěji používá v síti Ethernet pro pevné připojení počítačů k síti. Rovněž se používá pro přenos video a telefonního signálu.
Další kategorií je kategorie 6 (Cat 6), která umožňuje přenosovou rychlost až 10 Gb/s, ale pouze do teoretické vzdálenosti 50 metrů. [21]
Ještě větší rychlost nabízí kabely optické. Ty jsou zejména používány pro stavbu telekomunikačních sítí. Mohou nahrazovat i klasické UTP kabely, ale je potřeba speciální port. Výhodou nahrazení klasického UTP kabelu optickým je mnohonásobná rychlost, skladnost a menší rušení.

Jedním z nejčastějších použití koaxiálních kabelů je přenos videa a zvuku. Od přenosu kabelové televize až po použití v postprodukčních studiích. Koaxiální kabel je také používán pro přenos radiových frekvencí a mikrovln. Velkou oblibu získal při použití pro napájení antén, jelikož umožňuje přenášet stejnosměrný proud a má

malé ztráty, malou velikost a cenu. Může být i použit ve vysokofrekvenčních přenosech. [11]

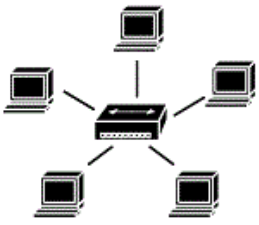
Bezdrátové připojení se ve firmách nejvíce používá pro připojení malých zařízení, jako jsou senzory, kamery a také jako Wi-Fi síť pro hosty a zaměstnance.

2.3 Topologie počítačových sítí

Topologie popisuje, jak jsou jednotlivé prvky uspořádány a propojeny v počítačové sítí. Může se dělit na logickou a fyzickou.
Logická topologie pouze znázorňuje virtuální prvky v síti a jakým způsobem mezi nimi probíhá komunikace. [22]
Fyzická topologie představuje reálné (fyzické) rozložení síťových prvků v síti.
Existují čtyři základní topologie: hvězdicová, kruhová, stromová a sběrnicová. Rozdíl mezi nimi je způsob zapojení a styl komunikace jednotlivých prvků. [22]

2.3.1 Hvězdicová topologie

Ve hvězdicové topologii jsou počítače zapojeny do útvaru připomínající hvězdu. Je to nejpoužívanější typ fyzické topologie. Každý počítač je připojený k centrálnímu prvku (hub nebo switch). Mezi dvěma počítači existuje vždy jen jedna cesta (viz Obr. 12). Tím vzniká nevýhoda, že neexistuje náhradní cesta, pokud vypadne spojení mezi počítačem a centrálním prvkem. Pokud přestane fungovat centrální prvek, nebude možná komunikace mezi jednotlivými počítači. [22]

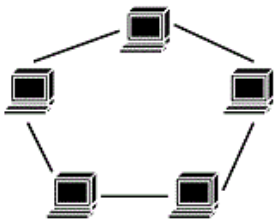


Obr. 12 - Hvězdicové zapojení (zdroj: [22])

2.3.2 Kruhová topologie

Kruhová topologie se od hvězdicové liší tím, že každé zařízení je připojeno právě ke dvěma dalším zařízením (počítačům) a tím vzniká kruh (viz Obr. 13). Není zde centrální prvek, který by jednotlivé zprávy rozesílal daným příjemcům, ale zpráva

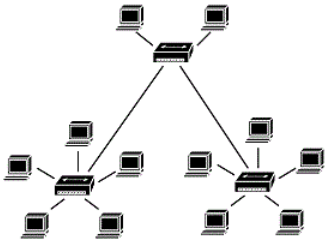
prochází přes všechna zařízení, nacházející se mezi odesílatelem a příjemcem. Při přerušení kruhu dojde k přerušení veškeré komunikace. [22]



Obr. 13 - Kruhové zapojení (zdroj: [22])

2.3.3 Stromová topologie

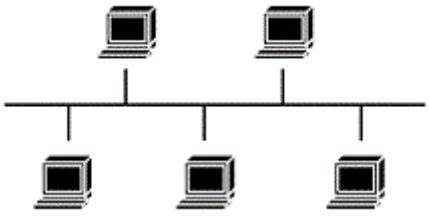
Stromová topologie vychází z hvězdicové topologie. Jednotlivé hvězdy jsou propojeny do útvaru, který připomíná strom (viz Obr. 14). Nejvíce používané v rozsáhlých počítačových sítích, převážně ve firmách. Jednotlivé hvězdice mohou představovat jednotlivá oddělení, patra nebo budovy. [22]



Obr. 14 - Stromové zapojení (zdroj: [22])

2.3.4 Sběrnicová topologie

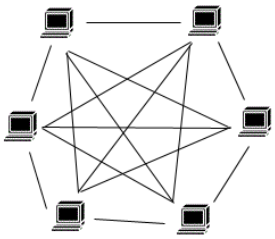
Sběrnicová topologie používá jediné přenosové médium, na které jsou připojeny všechny počítače (viz Obr. 15). Výhodou tohoto jednoduchého zapojení jsou nízké pořizovací náklady, ale mohou zde vznikat kolize, pokud dva klienti na síti začnou vysílat ve stejný okamžik. Toto se děje poměrně často, proto je třeba se kolizím vyvarovat. K tomu se používá tzv. systém náhodného přístupu (CSMA/CD), který se snaží kolizím vyvarovat a pokud nastanou, tak je vyřešit. [22]



Obr. 15 – Sběrnicová topologie (zdroj: [22])

2.3.5 Smíšená topologie (mesh topologie)

Smíšená (neboli mesh) topologie je označení pro topologii sítě, ve které je každé zařízení propojeno s každým (neboli full mesh – viz Obr. 16), nebo některé spoje jsou vynechány (partial mesh). To napomáhá zvýšené spolehlivosti pomocí redundantních cest – pokud nějaký spoj vypadne, je možno se k cíli dostat jinou cestou. Tato topologie je spíše realizována v bezdrátových sítích. [23]



Obr. 16 – Smíšená topologie (zdroj: [22])

2.4 Topologie firemní sítě

2.4.1 Propojení zařízení

Pevné počítače, tiskárny a jiná zařízení jsou ve firmě často připojeny do telekomunikačních zásuvek, které jsou navrhnuté pomocí zásad pro strukturovanou (vertikální a horizontální) kabeláž. Jednotlivá oddělení, patra, či místnosti jsou připojena do různých switchů, které jsou poté připojeny k centrálnímu switchi, nebo routeru.

2.4.2 Redundance

Pro firemní sítě je nejdůležitější záložní trasy, bezpečnost, spolehlivost a rychlost internetového připojení. To poskytuje stromová topologie sítě, protože jednotlivé switche jsou mezi sebou propojeny a existuje mezi nimi více cest. V dnešní době je i možnost záložního internetové připojení v případě výpadku poskytovatele, nebo linky mezi firmou a poskytovatelem. Tím se zajistí stoprocentní konektivita. [24]

2.4.3 Připojení firemní sítě do internetu

Ideální variantou pro hlavní připojení firmy je optická, či metalická síť s velkou maximální rychlostí a levné ADSL s menší rychlostí, případně mobilní 3G/4G síť jako záložní. [24]

2.4.4 Zabezpečení sítě – vnitřní/vnější hrozby

Hraničním síťovým prvkem topologie je router či firewall s WAN porty pro připojení k externí síti a LAN porty pro připojení interních sítí. WAN spoje jsou napojeny poskytovatele služeb (ISP), do LAN portů zapojeny infrastrukturní prvky firemní sítě, switche a Wi-Fi routery. [24]

Interní síť tvoří switche, do kterých se zapojí všechna firemní zařízení (počítače, kamery, tiskárny a podobně). Do této sítě se budou zařízení připojovat pouze kabelem a je výhodné zapnout filtrování zařízení podle MAC adresy. [24]

Druhou interní síť mohou tvořit Wi-Fi router s WPA2 zabezpečením, do které se budou připojovat pouze zaměstnanci z mobilních zařízení. Tato síť bude odizolována od sítě s pevně připojenými počítači, ale bude přes ní možno přistoupit k intranetu firmy.

Třetí interní síť je dedikována pro připojení návštěv, obchodním partnerům, zákazníkům atd. Tato síť může, ale nemusí být zabezpečená [24]. Je ale kompletně odizolována od ostatních firemních sítí a slouží pouze pro přístup k Internetu.

Pro sdílení dat na síti mezi počítači je vhodné používat cloud. Ten nabízí možnost přístupu k datům odkudkoliv. Tato data jsou zálohovaná a cloud má velice dobré zabezpečení. Firmy mohou využívat služby speciálních firem, které cloudové služby nabízejí, nebo mít vlastní server, na který data budou ukládat a přes cloud k němu přistupovat. Cloudové společnosti zaručují vysokou bezpečnost, zálohu dat, dostupnost kdykoliv a pro firmy je mnohem jednodušší tyto služby využívat. Služby těchto firem jsou ale často zpoplatněny.

Pro velmi rozsáhlou firmu je topologie složitější, obsahuje více switchů a může dělit i provozy na síti dle oddělení a práv (například lidé ve výrobě nemají přístup k datům, které si sdílí management). Toho lze docílit použitím VLAN (Virtuální LAN), nebo fyzickým rozdělením sítě. Ve firmách se převážně používá stromová topologie, která člení síť na menší segmenty a umožňuje redundantní (záložní) trasy v případě výpadku hlavní trasy.

3 Technologický základ pro IoT

3.1 Internet of Things

Internet věcí je pojem s globálně užívanou zkratkou IoT, která vychází z anglického termínu Internet of Things. Jde o označení pro mnohdy jednoúčelová zařízení, která jsou připojena k Internetu. Každé takové zařízení je schopno pracovat samostatně v existující infrastruktuře sítě, či Internetu a také spolupracovat s dalšími zařízeními a vyměňovat si svá data.[25]

Může se jednat o senzory sbírající data, domácí spotřebiče, části automatizované výroby, automobily atp.

IoT umožnuje vzdálenou kontrolu, ovládání, či sledování daného zařízení přes Internet, počítačovou síť, mobilní síť a podobné. [26]

Pojem IoT je velice široký, jelikož „věcí“ může být senzor sledující fyzikální veličinu, bezpečnostní kamera vysílající živé závěry ze sledovaného objektu, autonomní skladová vozidla, či přístroj výrobní linky.

IoT zařízení mohou sbírat informace pomocí připojených senzorů a poté je ve formě dat rozesílat prostřednictvím datové sítě mezi ostatní zařízení.

Stejně jak narůstá počet provozovaných IoT zařízení, roste i objem dat z nich získaný.

Některá se vyhodnocují okamžitě bez dalšího ukládání, jiná tvoří základ pro budoucí analýzy. Z toho důvodu se s implementací IoT musí zároveň uvažovat o možnostech ukládání předpokládaného objemu dat, jeho třídění, dostupnosti, zpracování a indexování, případně i archivaci.[27]

Největší výhodou IoT je miniaturizace, jednoúčelovost, nízká spotřeba elektrické energie a nízké pořizovací náklady. Pomocí těchto zařízení lze efektivně provést automatizaci.

IoT nabízí mnoho výhod pro organizace, kterým umožňuje například:

- Monitorování podnikových procesů a výroby [28]
- Může přinést zkvalitnění služeb zákazníkům [28] (například automaticky naváděná vozidla přivezou správné zboží za pomocí čárového kódu)
- Vzdálená správa zařízení [28]

- Ušetřit čas i peníze zefektivněním procesů a šetřením elektrické energie
- Zlepšit produktivitu zaměstnanců – příjemná teplota v místnosti, automatické otevírání dveří, RFID čtečky a čárové kódy [28]
- Produkovat větší obraty [28]

3.2 Cloud Computing

Cloud umožňuje přístup ke sdíleným službám a datům skrz jakékoliv kompatibilní zařízení kdekoliv na světě pomocí Internetu. Může sloužit k ukládání a správě dat, provozování webových aplikací, či k pronájmu hardwaru pro výpočetní výkon.
Umožňuje výrazně zmenšit vysoké investice za hardware a strávený čas budováním a nastavováním vlastního hardwaru. Firmy poskytující cloudové služby nabízí svůj hardware a služby. [29]
Zákazníci těchto firem nemusí mít vlastní servery, či datová uložiště, ale mohou využívat právě hardware daných firem a přes Internet ho obsluhovat.
IoT zařízení se připojují ke cloudovým službám převážně proto, jelikož je v současné době nedostatek IPv4 adres (toto by měla vyřešit IPv6). Cloudové služby právě tento problém řeší, jelikož se přes IoT bránu připojí ke cloudu a následně je přes daný cloud možné k zařízením přistoupit.

3.3 Průmysl 4.0

Jedná se o označení současného trendu digitalizace a automatizace výroby. Hlavní myšlenkou jsou takzvané „chytré továrny“, které využívají autonomní systémy a tím převezmou triviální a opakující se činnosti, které do té doby museli dělat lidé. V této myšlence dostanou stroje i produkty své čipy, pomocí kterých spolu budou navzájem komunikovat, vyměňovat si potřebná data a bude je možné vzdáleně řídit a obsluhovat. [30]
Základ průmyslu 4.0 tvoří IoT zařízení, která ve spojení s cloudovými uložišti, umělou inteligencí, či strojovým učením, dokáží automaticky hlásit problémy ve výrobě. Také například umožňuje řídit chytré sklady, které umí kontrolovat stav svých zásob a automaticky je doplňovat. [30]

Průmysl 4.0 často zmiňuje pojem kyberfyzikální systémy. Jedná se o označení systému skládajícího se z fyzických entit, které řídí počítačové algoritmy. Tyto entity jsou schopny se samostatně rozhodovat a spolupracovat s ostatními. [31]

Ke komunikaci IoT zařízení se používají technologie jako je například LoRaWAN, Narrowband IoT, či IQRF.

3.3.1 **LoRaWAN**

LoRaWAN (Long Range Wide Area Network) je jedna z nízko příkonových bezdrátových technologií, která umožňuje levnou a zabezpečenou obousměrnou komunikaci. Využívá pásmo 1 GHz a rychlost jejího přenosu je od 0.3 kb/s do 50 kb/s. Je navržena k bezdrátovému připojení bateriemi napájených „věcí" do Internetu (buď lokálního, národního, nebo globálního). [32] Má deklarovaný dosah až 40 km v terénu, 15 km v příměstském prostředí a 2-5 km ve městě. Napájecí baterie by měla mít životnost 5-15 let v závislosti na četnosti komunikace a typu použití. Technologie používá šifrování AES128. [33]

3.3.2 **Narrowband IoT**

Další bezdrátovou technologií se nazývá Narrowband IoT (NB-IoT). Jedná se o úzkopásmovou LSWA technologii, která byla vyvinuta pro Internet věcí a její největší výhodou je možnost nasazení v pásmech GSM a LTE. Poskytuje lepší pokrytí uvnitř budov, zvládá masivní počet zařízení a koncová zařízení budou mít velmi nízkou cenu i spotřebu energie. Jeho dosah je až 15 km a přenosová rychlost je 50 kb/s. [34]

3.3.3 **IQRF**

IQRF je kompletní technologie určena pro bezdrátovou komunikaci při nízkých energetických nákladech, malou rychlostí a s nízkým objemem dat s dosahem desítek až stovek metrů. Tato technologie může být použita pro průmyslové řízení a automatizaci budov a měst. IQRF může být použito s jakýmkoliv elektronickým zařízením, pokud je potřeba bezdrátového přenosu, jako je dálkové ovládání, monitorování dálkově získaných dat, či připojení více zařízení k bezdrátové síti.

IQRF využívá paketově orientovanou komunikaci. Lze využít k peer-to-peer komunikaci, ale jeho největší síla je v komplexních mesh sítích. Využití IQRF závisí na nahraném aplikačním softwaru. Tento software je snadno programovatelný. IQRF zařízení nemají poplatky za licenci či nosič. [35]

IQRF je kompletní řešení od jednoho výrobce, který zahrnuje hardware (transceivery, brány, routery, příslušenství, vývojové nástroje), software, protokoly, podporu a služby. [35]
Základním komunikačním IQRF zařízením je transceiver. Jedná se o malé zařízení, které má v sobě zabudovaný operační systém s podporou mesh sítí. Díky těmto zařízením je možno komunikovat oběma směry, tedy přijímat i odesílat. Transceivery jsou použity jak v senzorech, tak i v IQRF bránách, routerech a dalších prvcích. [36]

Do existující sítě lze IQRF zařízení připojit přes IQRF bránu. Tato brána umožňuje propojit IQRF zařízení s jinými zařízeními pomocí běžně používaných standardů (USB, Ethernet, Wi-Fi, GSM) a také připojit ke cloudu a data přes něho odeslat do Internetu. [37] [38]

4 Zabezpečení sítě

Pokud se útočník (neboli hacker) dostane do sítě, může zachytávat komunikaci mezi počítači, nebo přistupovat do databází, kde jsou velice citlivá firemní data. Cílem útočníků může být sabotáž dat či celé firmy s úmyslem vyřadit firmu na nějakou dobu z provozu, nebo získání dat.

Získaná citlivá a tajná data by mohl útočník dále prodávat například konkurenční firmě (patenty, plány výroby, či aktuální finanční stavy firmy pro akcionářské účely) a tím se obohatit.

Pokud útočník získá přístup k těmto zařízením, tak toto obrovské množství zařízení připojených k Internetu by navíc mohlo být zneužito k hromadnému a obrovskému *DDoS*[1] útoku na určitou firmu, server či počítač.

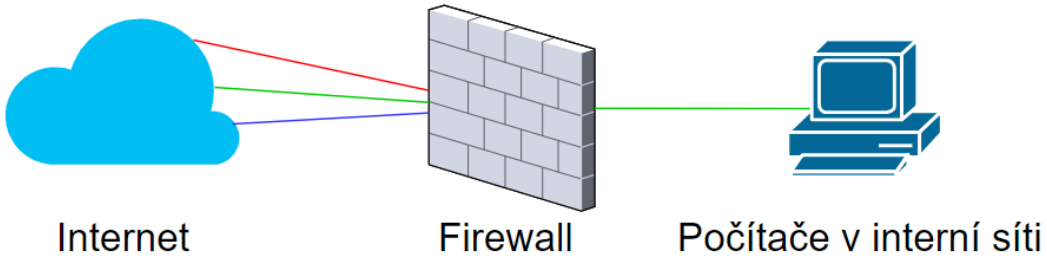
Není potřeba zajistit pouze bezpečnost přenášených dat a sítě, ale také samotných IoT zařízení. Napadnutí těchto zařízení, která automatizují provoz výroby, by mohlo vyřadit výrobu na dlouhé hodiny až dny, což by mohlo přinést obrovské peněžní ztráty.

4.1 Firewall

Je zařízení, nebo software (program), který umožňuje vytváření pravidel (tzv. firewallová pravidla) pro síťovou komunikaci. Pravidla mohou být pro příchozí i odchozí komunikaci do vnitřní sítě, či zařízení. Přes firewall je možné blokovat komunikaci z určitých IP adres, MAC adres, či síťových portů a tím snížení rizika vniku viru, či hackera do sítě, nebo počítače. Díky firewallu je tedy možné zablokovat škodlivou příchozí a také nechtěnou odchozí komunikaci. [39]

Znázornění filtrování komunikace viz Obr. 17. Čáry na tomto obrázku znázorňují příchozí komunikaci z Internetu a pouze zelená čára má povoleno dostat se do interní sítě.

[1] DDoS – Typ útoku, který je založen na zahlcení webové stránky, internetové služby, či serveru a tím zamezení přístupu ostatním uživatelům velkým množstvím rozptýlených počítačů.



Obr. 17 – Znázornění funkce firewallu (zdroj: vlastní zpracování)

4.2 Drátové sítě

Při zabezpečování sítě se lidé často zaměřují pouze na zabezpečení bezdrátové části sítě, jelikož Wi-Fi lze zachytit a napadnout i pokud útočník sedí s počítačem na lavičce vedle budovy, nebo pohodlně v autě na parkovišti.

Hrozby mohou ale přijít i zevnitř. Návštěvníci, či dokonce zaměstnanci by mohli firemní síť i nevědomě ohrozit. Stačí pouze připojit zařízení, na kterém se skrývá virus, který se po připojení do sítě rozšíří. Proto je potřeba zabezpečit i drátovou síť. Drátové sítě mají oproti bezdrátovým sítím výhodu v tom, že nemohou být zachyceny útočníkem mimo budovu. K napadení této sítě se musí útočník fyzicky dostat k síťovému portu, serveru, počítači, či kabelu připojeného k dané síti.

Existují doporučení zabezpečení drátové sítě, mezi něž například patří filtrování pomocí IP a MAC adres a povolit tak pouze známá a důvěryhodná zařízení. To zamezí neopatrným zaměstnancům způsobit nechtěnou bezpečnostní hrozbu. Tabulku MAC adres je ale potřeba aktualizovat při jakékoliv plánované změně.

Zkušený hacker může však filtrování pomocí MAC adres snadno obejít. [40]

Dále je vhodné nastavit na routeru statické routování, jelikož dynamické routování se při vyhledávání tras šíří dále do sítě. Je také méně náročnější a tolik nezatěžuje router, což by ve velké firemní síti mohlo mít za následek zpomalení sítě.

Na všech koncových zařízeních je také vhodné mít aktuální verzi dobrého antivirového programu.

4.3 Bezdrátové sítě (Wi-Fi)

Problémem Wi-Fi je, že síť může být viditelná i mimo objekt, který daná Wi-Fi pokrývá. Tedy síť s potenciálními důvěryhodnými informacemi může být napadena i zvenčí. Potenciální útočník může zachytávat komunikaci mezi jednotlivými zařízeními, či prolomit heslo a do dané sítě se dostat.
K zabezpečení Wi-Fi sítí se používají následující metody:

- Zablokování vysílání SSID
    - Neboli zdánlivé skrytí Wi-Fi sítě. Pokud má Wi-Fi síť skryté SSID[2], tak se klientům v seznamu dostupných Wi-Fi sítí tato síť nezobrazí. Pro připojení je tedy nutné ručně zadat SSID sítě. [41]
- Ověření MAC adres
    - Přípojný bod Wi-Fi sítě má v sobě uložen tabulku s MAC adresami klientů, kterým je umožněno se k dané síti připojit (tzv. whitelist). Podobně tak je možné zakázat MAC adresu určitého zařízení a tím mu omezit přístup k síti (tzv. blacklist). [41]
- WPA2
    - Využívá šifrování na obou stranách bezdrátového spojení. Šifrovací klíče jsou dynamicky a bezpečně měněny. [41]
- RF stínění
    - Jelikož Wi-Fi může proniknout zdmi a tím být zachycena i mimo pokrývaný objekt, může se využívat speciální nátěr na zdi a fólie na okna. Tyto opatření výrazně oslabí signál, který opouští budovu. Tím je pro útočníka zvenčí mnohem obtížnější zachytit toto vysílání a napadnout danou síť. [41]

4.4 Techniky vlámání se do sítě a ochrana před nimi

Jednou z prvních technik, kterou může útočník zkusit je zkoušení přihlašovacích údajů (například k zaměstnanecké WiFi). Stačí pouze dokola zkoušet kombinace

[2] SSID – jedinečný identifikátor sítě

přihlašovacích jmen a hesel. Tato technika většinou není moc efektivní při složitějších heslech. Útočník může využít programů, které budou automaticky hesla zkoušet a tím proces urychlit. Při použití WPA2 zabezpečení na WiFi síti a použití silného hesla, které kombinuje čísla, velká a malá písmena i speciální znaky je tato technika velice neúčinná a při použití většího množství znaků (8 a více) i v reálném čase téměř nemožná (zabere například roky až tisíce let).

Další technikou může být virus, který se do sítě dostal z Internetu, nebo připojením zařízení, které v sobě daný virus obsahuje (je tzv. infikováno). Je mnoho druhů virů. Nějaké mohou zachytávat komunikaci na síti včetně přihlašovacích hesel a důležitých dat, které může odesílat útočníkovi. Další mohou sloužit pro sabotáž tím, že se dostanou do databáze, kde by mohly data smazat nebo zničit. A jiné mohou sloužit jako tzv. zadní vrátka do sítě, přes které se může útočník do sítě dostat a dělat prakticky cokoliv. Pro toto je vhodné mít nainstalovaný a aktualizovaný dobrý antivirus na všech zařízeních.

Útočník může i síť napadnout fyzicky, pokud by se dostal k routeru nebo switchi. V tom případě by žádné zabezpečení zařízení nepomohlo, jelikož by jednoduše mohl zařízení resetovat do továrního nastavení, nebo se připojit přes správcovskou konzoli (ta ale může být zabezpečena heslem). Pro tyto případy je dobré mít zařízení v zabezpečené místnosti či skříni, kam má přístup pouze správce sítě. [42]

4.5 Problémy se zabezpečením a soukromím

Jelikož IoT zařízení jsou propojena, tak vše, co potřebuje útočník udělat, je najít zranitelnost a bude moci manipulovat se všemi daty, zneužít je, nebo je třeba smazat. Správci sítě navíc pravidelně neaktualizují svá zařízení, a tím je nechávají zranitelná pro potenciální útočníky.

Problémem nejsou pouze hackeři, ale také soukromí uživatelů. IoT zařízení mohou být ve vlastnictví firem, které je provozují, ale také je mohou mít pronajaté. Firmy, které pronajímají zákazníkům IoT zařízení, se snadno dostanou k datům jednotlivých uživatelů a mohly by je bez vědomí uživatelů prodávat dále, jelikož

osobní data uživatelů mají pro firmy obrovskou hodnotu (například pro reklamní společnosti).

Do Internetu se připojují miliony zařízení, a to zahrnuje velké množství datových bodů, které je potřeba zabezpečit. Kvůli rostoucím útokům na data uživatelů je bezpečnost a soukromí nejdůležitější problém, který je potřeba vyřešit.

4.6 Obecné nařízení o ochraně osobních údajů (GDPR)

Jedná se o nařízení Evropské unie, jehož cílem je stanovit pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů, a tím výrazně zvýšit ochranu osobních dat a zamezit neoprávněnému zacházení s jejich daty. [43]
Každá fyzická osoba má práva: [44]

- Na opravu svých údajů
- Na trvalé vymazání svých údajů (tzv. právo být zapomenut)
- Na omezení dalšího zpracování (například zákaz předávání osobních informací třetím stranám)

Firmy mohou za pomocí IoT zařízení zjišťovat osobní informace o svých zaměstnancích (například čas příjezdu a odjezdu vozidel pracovníků na firemní pracoviště). Tato data ukládají a toto může být v rozporu s GDPR. Je proto nutné přijmout adekvátní opatření (databázi šifrovat a omezit přístup neoprávněným osobám).

5 Nasazení IoT do sítě

5.1 Úvod

V předešlé kapitole byly představeny topologie sítě. Bylo popsáno, že nejpoužívanější topologií je hvězdicové zapojení, které umožňuje připojit větší počet zařízení do jediného switche a je tedy velice levné, ale jeho nevýhoda je v tom, že nebude možná komunikace při vypadnutí centrálního prvku. Toto zapojení je velice oblíbené pro malé sítě.

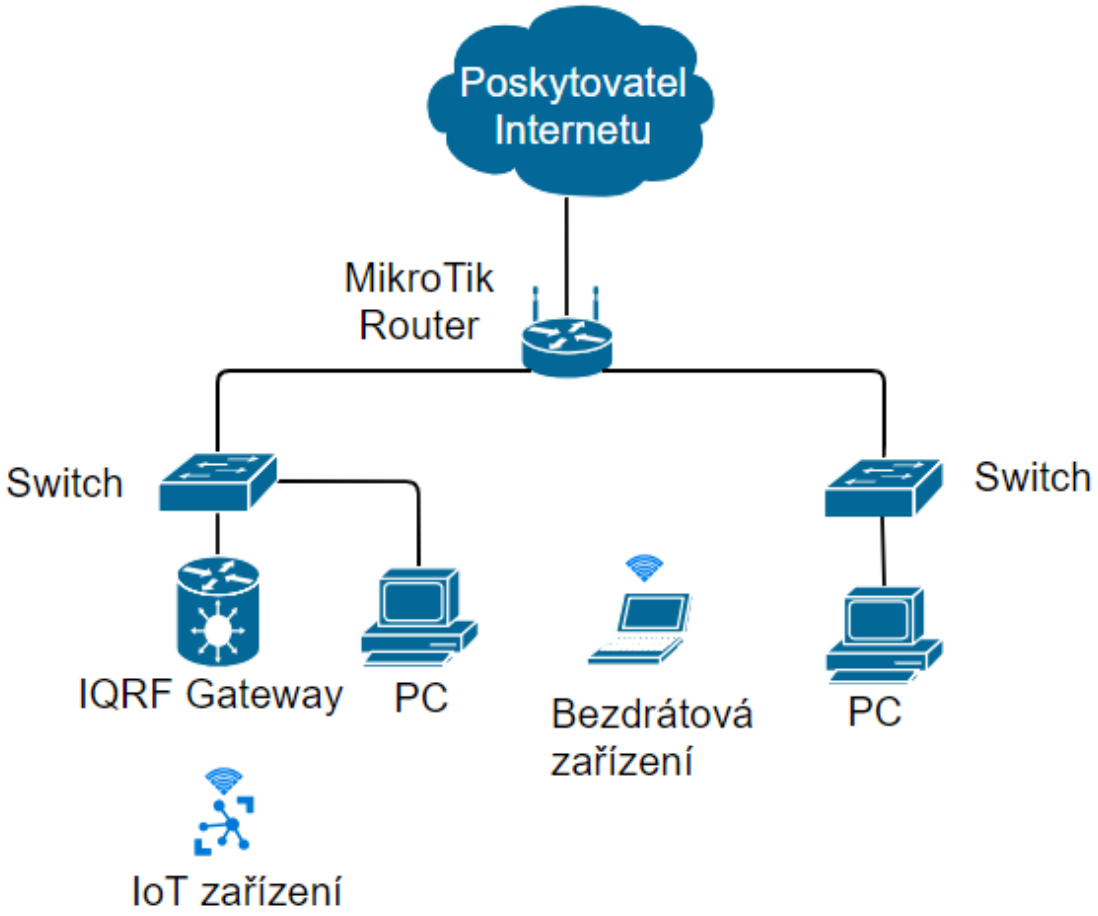
Doporučenou topologií pro firemní použití je stromová topologie, která umožňuje redundantní spoje a obsahuje hvězdicovou topologii, kde jednotlivé hvězdice představují jednotlivá oddělení, či patra firmy.

Dále byla popsána IoT zařízení a převážně jejich použití a nasazení ve firmách. Bylo uvedeno, že IoT síť musí být dobře zabezpečena, aby nedošlo k napadení zařízení v ní zapojených a kompromitaci dat, jelikož ta mohou být velice citlivá a nesmí se dostat k nesprávným osobám.

5.2 Technologie a protokoly

Pro nastínění problému zapojení IoT zařízení do již funkční infrastruktury sítě a jejich zabezpečení bude popsáno zapojení IQRF zařízení do autorovy domácí sítě. Ta obsahuje celkově 1 router, 2 switche, 2 počítače a mobilní zařízení připojená přes Wi-Fi. Od poskytovatele internetového připojení vede kabel do MikroTik routeru. Ten má v sobě integrované 2 switche, na jeden je přímo kabelem připojen jeden počítač a sem se také připojí IoT brána. Na druhý switch je připojen druhý počítač. Router vysílá Wi-Fi signál a mobilní zařízení se mohou připojit i bezdrátově. Logické zapojení viz Obr. 18.

Této infrastruktury bude využito a budou do ní zapojena IQRF zařízení. Pro demonstraci zabezpečení se router nastaví tak, aby byla data z IQRF zařízení přístupná pouze z počítače připojeného na první switch. Tím se nasimuluje odstínění části sítě, kde budou data z IQRF zařízení, od druhé sítě s počítači.



Obr. 18 – Logická infrastruktura zapojení (zdroj: vlastní zpracování)

Na Obr. 18 je znázorněno logické zapojení prvků v autorově domácí síti. Přes IQRF bránu jsou získána data z IoT (IQRF) zařízení. Ty jsou přístupná z počítače připojeného ke stejnému switchi, který slouží také jako počítač pro správu brány. Tento počítač má neomezený přístup k Internetu, ale pro přístup k bráně je povoleno pouze několik vybraných portů, kvůli většímu zabezpečení před potenciálními hrozbami z Internetu. Přenosná zařízení a zařízení připojena k druhému switchi mají přístup do Internetu a nemají přístup k IQRF bráně.

5.2.1 Mosquitto (MQTT protokol)

Jednotlivá IoT zařízení (například snímače) by neměla určovat, kdo co má udělat, ale pouze snímat a posílat zprávy do centrálního místa a o více se nestarat. Ta zařízení, která mají zájem o jejich zprávy, se pouze přihlásí k odběru. To zařizuje zprostředkovatel zpráv Mosquitto.

Mosquitto implementuje MQTT (Message Queuing Telemetry Transport) komunikační protokol. Jedná se o nenáročný a velice jednoduchý protokol, který byl navrhnut pro jednoduchá zařízení. Základem je minimalizace zatížení sítě a omezení požadavků na zdroje zařízení. Také se snaží zajistit spolehlivé doručení zprávy. Je založený na principu zveřejňování a odebírání (publish/subscribe). Zařízení, jako například senzory, nebo snímače zveřejňují (publikují) zprávy do jednoho místa (MQTT Broker). Zprávy jsou publikovány s názvem tématu (topic) a broker je rozešle všem klientům, kteří dané téma odebírají (subscribe). Jako klient může být aplikace, webová stránka, nebo nějaké zařízení, které zprávu dále zpracovává. Předávání zpráv probíhá standardně na portu 1883, pro zabezpečený přenos pak přes SSL jde o port 8883. [45]

MQTT protokol definuje tři úrovně Quality of Service (QoS). QoS definuje, jak moc se bude broker nebo klient snažit, aby zpráva byla doručena. Úroveň QoS je nastavena jak na klientovi, který odebírá zprávy, tak na zařízení, které zprávy publikuje. Každé zařízení může mít vlastní úroveň QoS a závisí na klientovi, jakou úroveň si zvolí. Pokud klient zvolí úroveň 0 a zařízení publikuje na QoS úrovně 2, klient obdrží zprávu na úrovni 0. Pokud klient zvolí maximální hodnotu (tedy hodnotu 2) a zařízení publikuje zprávy na hodnotě QoS 0, tak klient obdrží zprávu s QoS hodnotou 0. [46]

Vyšší úrovně QoS jsou spolehlivější, ale mají větší odezvu a jsou náročnější na šířku pásma dané sítě (bandwidth). [46]

Úrovně QoS:

0: Odesílatel doručí zprávu nejvýše jednou a bez potvrzení. Zpráva (PUBLISH paket) je pouze odeslána a poté na ni odesílatel zapomene. [46]
1: Odesílatel doručí zprávu alespoň jednou a požaduje potvrzení, že zpráva byla přijata. Příchozí zpráva je zařazena do fronty a smazána až poté, co je úspěšně doručena a potvrzena. Po obdržení zprávy odešle příjemce zpátky potvrzení (PUBREC paket), že zprávu přijal. [46]
2: Odesílatel doručí zprávu právě jednou za použití tzv. four-way handshake. Funguje podobně, jako QoS úrovně 1, že příjemce vždy musí odpovědět PUBREC paketem odesílateli, ale ten si ho v QoS2 uloží a odešle příjemci

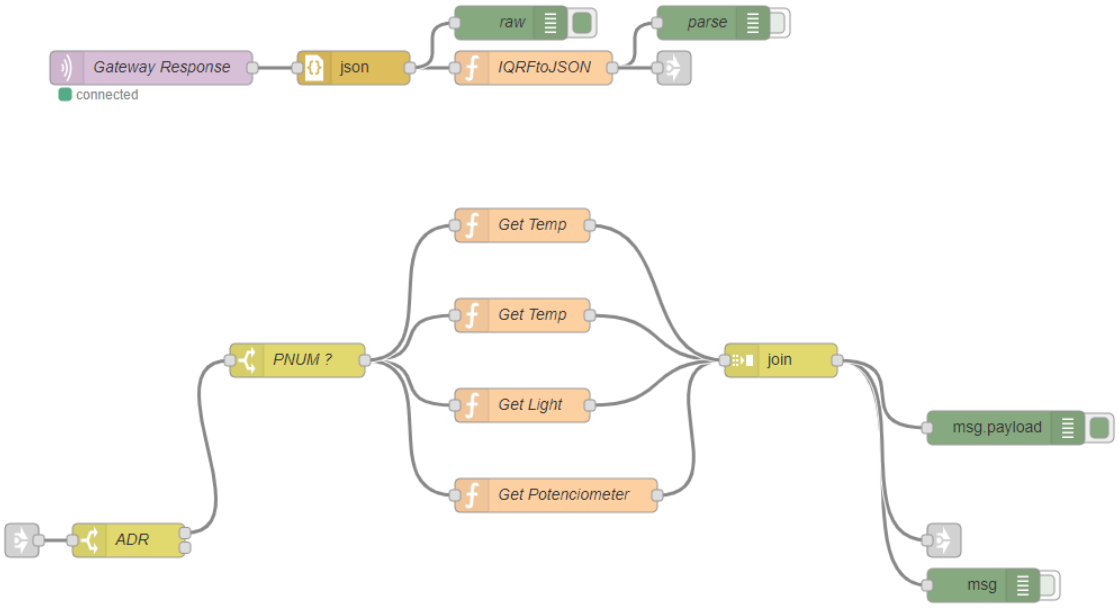
PUBREL paket a na PUBREL paket musí příjemce odpovědět PUBCOMP paketem. Pakety obsahují identifikátor paketu a zamezují duplicitám. To zajistí, že zpráva je doručena pouze jednou. [46]

5.2.2 Node-RED

Programování funkce jednotlivých IoT zařízení lze provést jednoduše pomocí programovacího nástroje Node-RED.

Jedná se o uživatelsky přívětivý programovací nástroj. Programování zde probíhá za pomocí tzv. flow-based přístupu a je přístupné z webového rozhraní, tudíž je možné programovat skrze jakýkoliv internetový prohlížeč. [47]

Základním prvkem je node (neboli uzel). Jedná se o objekt ve smyslu objektově orientovaného programování, který má nějaký svůj předdefinovaný účel, nebo funkci a jeho funkce jde i přeprogramovat. Tyto objekty je možno navazovat na sebe a tím vzniká tzv. flow (datový tok). [47] Je možné mít více flows (toků) a jednotlivé flows jsou pak vykonávány paralelně, viz Obr. 19



Obr. 19 – Příklad flow v Node-RED (zdroj: vlastní zpracování na základě IoT-Starter-Kit flow dostupného z https://gitlab.iqrf.org/alliance/iot-starter-kit)

5.3 Zařízení

V praktické části byla použita zařízení:

- Vývojový set IQRF s názvem DS-START-04
- Raspberry Pi 2 Model B
- MikroTik RB493G

5.3.1 Vývojový set DS-START-04

Jedná se o set obsahující 3 IQRF transceivery TR-72DA, 1 CK-USB programátor a debugger, 2 DK-EVAL-04A univerzální přenosné vývojové sady pro transceiver moduly, 1 micro USB kabel a 1 flash disk se softwarem a dokumentací, viz Obr. 20

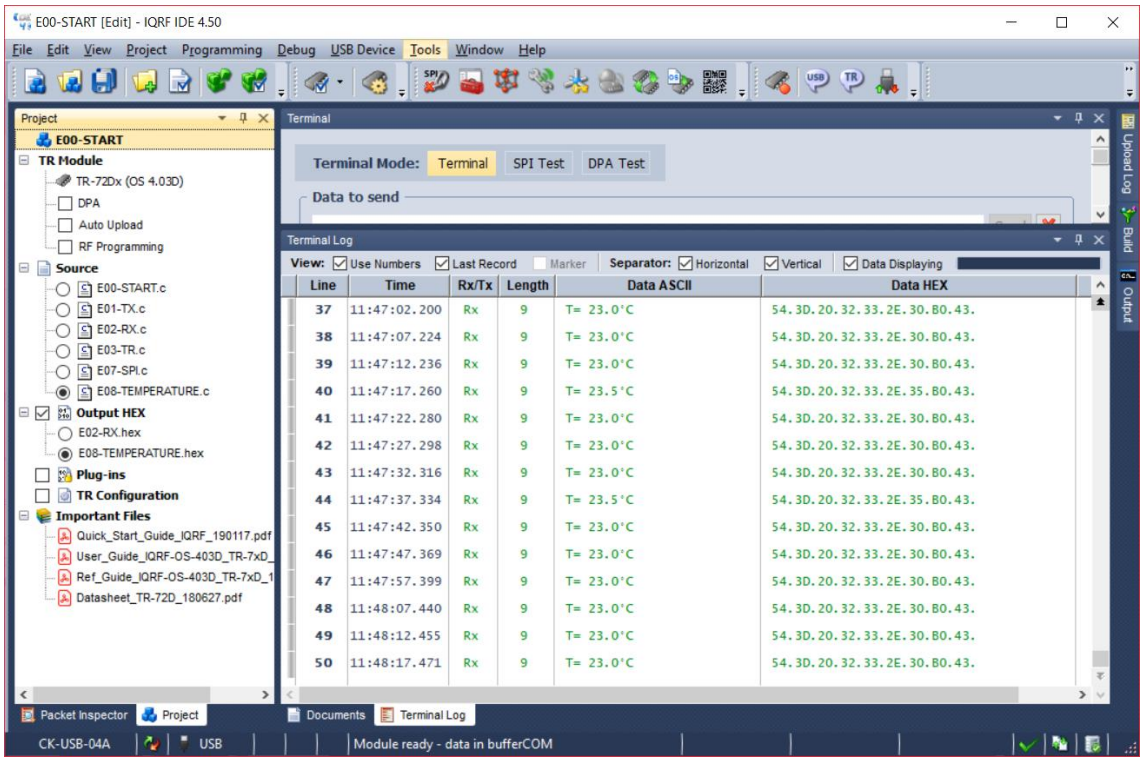
Obr. 20 – IQRF DS-START-04 vývojový set (zdroj: vlastní zpracování)

Po připojení flash disku do počítače lze na disku najít základní informace o setu, výuková videa, podrobnou dokumentaci, návody, software pro programování transceiverů a předem vytvořené ukázkové kódy pro objasnění základů jeho programování.

5.3.2 IQRF IDE4

Software pro programování transceiverů dostupný na flash disku se jmenuje IQRF IDE4.

Tento software je prostředí pro vytváření IQRF aplikací, umožňuje programovat a debugovat transceivery, spravovat IQMESH síť, párovat nody s koordinátorem, prozkoumávat síť a mnoho dalšího.



Obr. 21 – Vývojové prostředí programu IQRF IDE4 (zdroj: vlastní zpracování)

Na Obr. 21 lze vidět připojený USB modul CK-USB-04A s transceiverem TR-72DA naprogramovaný k získání teploty z přenosného transceiveru.

5.3.3 Transceiver TR-72DA

Jedná se o zařízení velikosti SIM karty, na kterém se nachází EEPROM paměť, teplotní senzor, anténa a kontrolní LED. [48]

Má velmi malou spotřebu elektrické energie a je tedy vhodný do bateriově napájených aplikací. Použití těchto transceiverů je k vytvoření bezdrátové komunikace, automatizace budov, ovládání pouličních světel, ale především v Internetu věcí. [49]

Transceiver je zobrazen na Obr. 22.

Obr. 22 – Transceiver TR-72DA (zdroj: vlastní zpracování)

5.3.4 Raspberry Pi 2 Model B

Jedná se o miniaturní počítač, který disponuje HDMI výstupem pro připojení monitoru, ethernetovým portem pro připojení k připojení do Internetu. Dále obsahuje 4 USB porty a GPIO rozhraním pro připojení dalších periferií. Lze využívat jako domácí server, multimediální centrum, či jako plnohodnotný počítač.

Hlavním operačním systémem je Raspbian, který je založený na linuxové distribuci odvozené ze systému Debian. [50]

Raspberry využívá micro SD kartu jako svoji paměť.

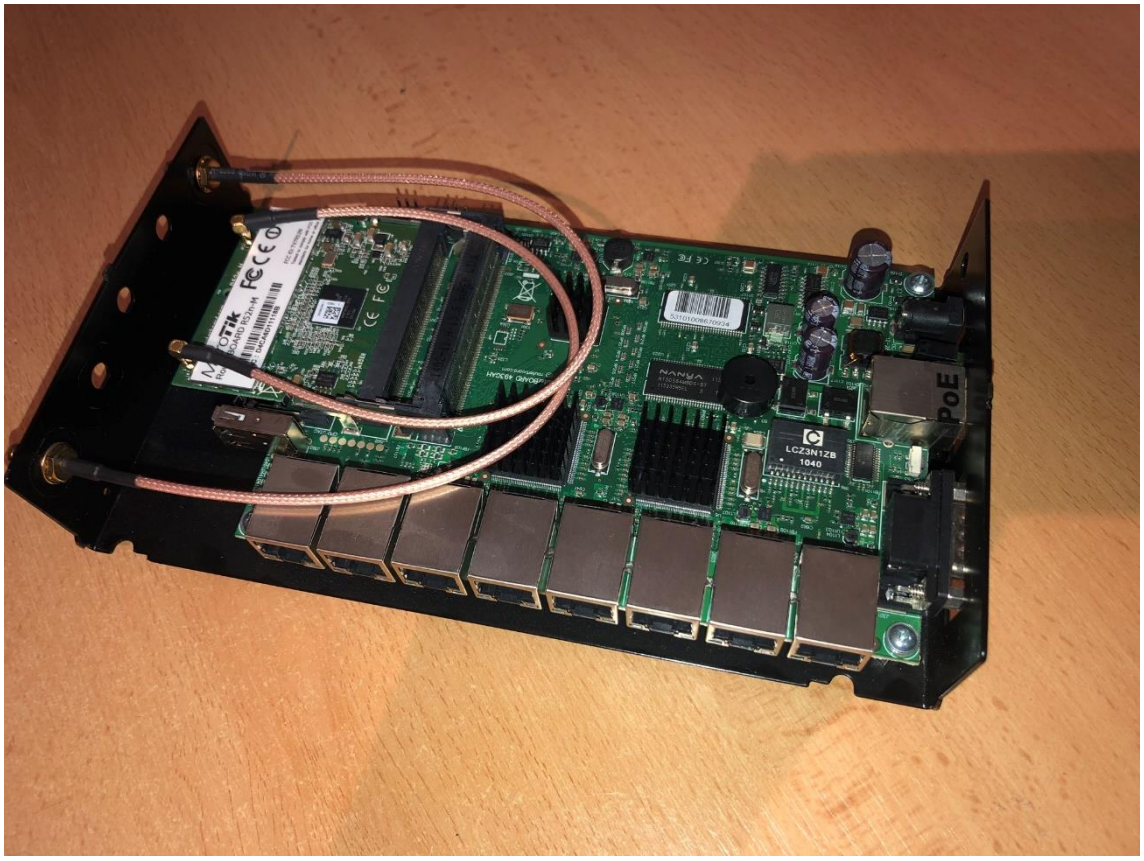
Toto zařízení bylo v této práci použito jako brána pro IQRF zařízení, viz Obr. 23

Obr. 23 – Raspberry Pi 2 Model B (zdroj: vlastní zpracování)

5.3.5 MikroTik RB493G

MikroTik RB493G neboli routerBOARD, je základní deska routeru doplněná několika sloty. Základní funkce lze za pomocí doplňkových modulů (Wi-Fi karty, antény a podobně) rozšířit. Hardwarové modifikace lze variabilně využít jako aktivní síťový prvek (přístupový bod, router, bridge, …). [51] Na Obr. 24 je vyobrazený použitý set usazený do kovové krabice.

MikroTik RouterBOARDy jsou dodávány s operačním systémem RouterOS. Router lze jednoduše spravovat prostřednictvím grafického rozhraní Winbox, pomocí něhož lze nastavovat většinu funkcí, které MikroTik umí. [52]



Obr. 24 – MikroTik RB493G se zapojeným modulem R52n-M (zdroj: vlastní zpracování)

5.4 Příprava IQRF zařízení pro připojení do sítě

5.4.1 Základy IQRF technologie

Pro přenos je využíváno bezlicenční pásmo 868 MHz a 916 MHz (což je frekvence v souladu s legislativou využívaná v jiných zemích). [48]

Každá IQRF síť je tvořena transceivery, které se označují jako koordinátory a nody. Koordinátor řídí síť a komunikuje s nody. Nody jsou zařízení, která reagují na řídící signály koordinátoru.

Při využití protokolu DPA je možno mít v jedné síti až 239 nodů. V případě potřeby většího množství nodů je vhodné použít větší množství menších sítí, které lze spolu propojit. [48]

Pro připojení IQRF zařízení do počítačové sítě se používá brána. Brána slouží k vytvoření mostu mezi různými typy komunikací. V tomto případě se jedná

o propojení IQRF technologie s počítačem, či Internetem. Může se jednat o USB, ethernetovou či GSM bránu, nebo i Raspberry Pi, Arduino, či jiné podobné zařízení [48].

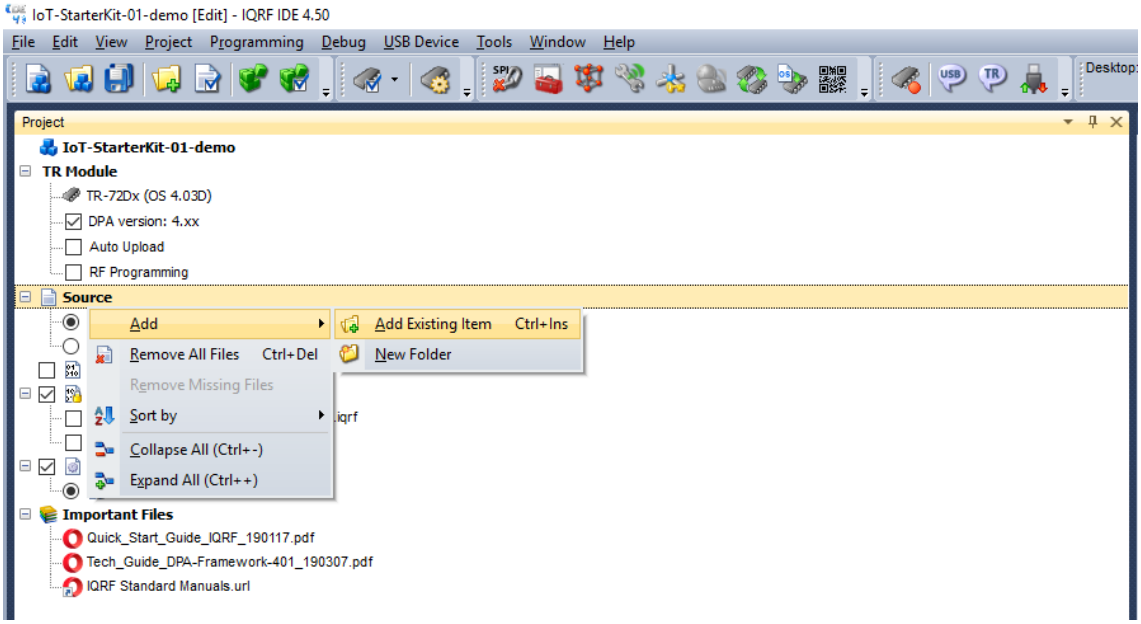
Pro dosažení vytyčeného bylo potřeba provést konfiguraci koordinátora a nodů a jejich vzájemné spárování. Poté bylo potřeba zapojit a nastavit IQRF bránu a v poslední řadě nakonfigurovat MikroTik RouterBOARD pro demonstraci zabezpečené integrace do datové sítě.

5.4.2 Nastavení IQRF transceiverů před připojením k IQRF bráně

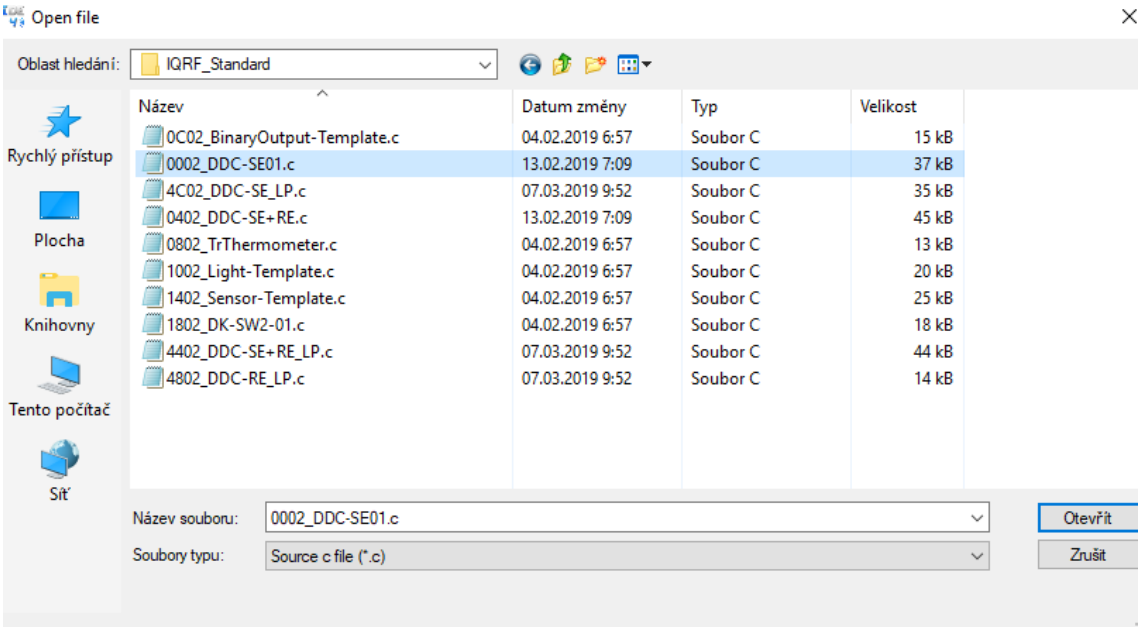
Před připojením IQRF transceiveru k IQRF bráně je potřeba nejdříve nastavit transceivery jako koordinátor a nody. V IQRF-IDE je tedy nutné nahrát do jednoho transceiveru program pro koordinátor a do ostatních transceiverů nahrát program pro node. Pro snadné nahrání těchto programů je možné otevřít soubor *IoT-StarterKit-01-demo.iqrfprj*, který se nachází ve složce *IoT-StarterKit-01* s cestou *Examples**DPA**IoT-StarterKit-01* na flash disku, který je v balení IoT Starter Kit DS-START-04.

Je nutné připojit CK-USB programátor s připojeným TR-72DA transceiverem, na který se bude program nahrávat.

V levé části obrazovky v sekci Source lze přidat požadovaný program, který bude transceiver vykonávat. Po kliknutí pravým tlačítkem na Source a vybráním Add Existing Item lze najít v počítači požadovaný program, viz Obr. 25. Pro program, který umí získat teplotu z interního teplotního senzoru TR-72DA transceiveru je vhodné nahrát soubor 0002_DDC-SE01.c, který se nachází ve složce IQRF_Standard s cestou *Examples**DPA**CustomDpaHandlerExamples**IQRF_Standard*, viz Obr. 26

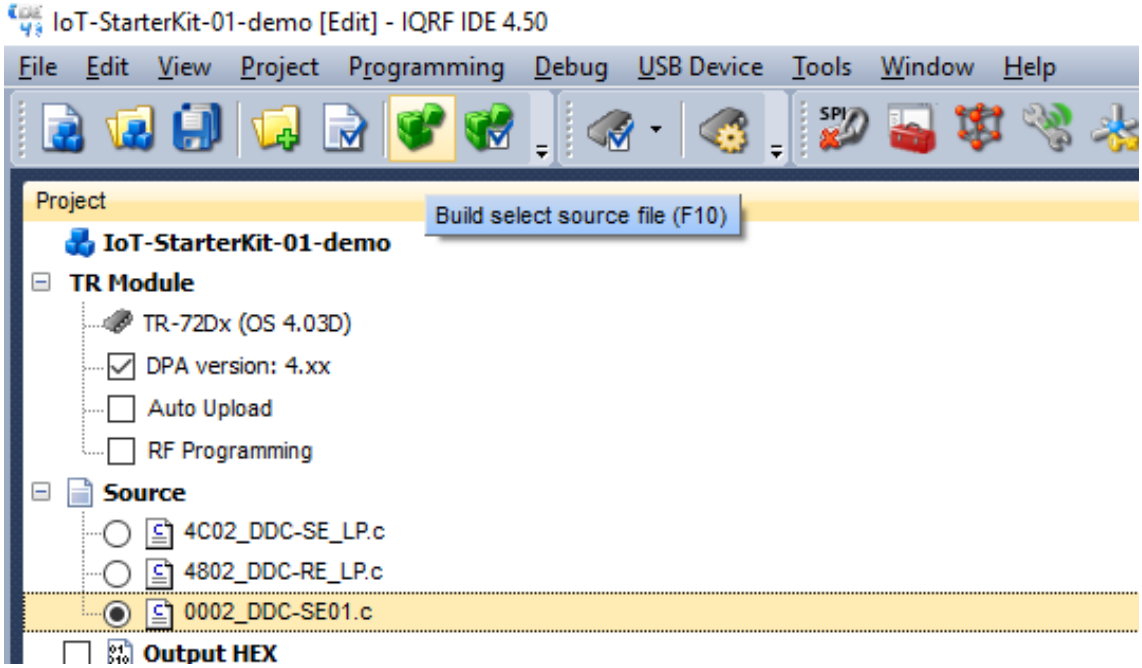


Obr. 25 – Přidání nového programu do IQRF_IDE (zdroj: vlastní zpracování)



Obr. 26 – Výběr programu pro transceiver umožňující měření teploty (zdroj: vlastní zpracování)

Z přidaného souboru je nutné vytvořit HEX soubor, který lze následně nahrát do transceiveru. HEX soubor lze vytvořit vybráním přidaného souboru a kliknutím na zelené tlačítko „Build select source file“ nebo tlačítkem F10, viz Obr. 27



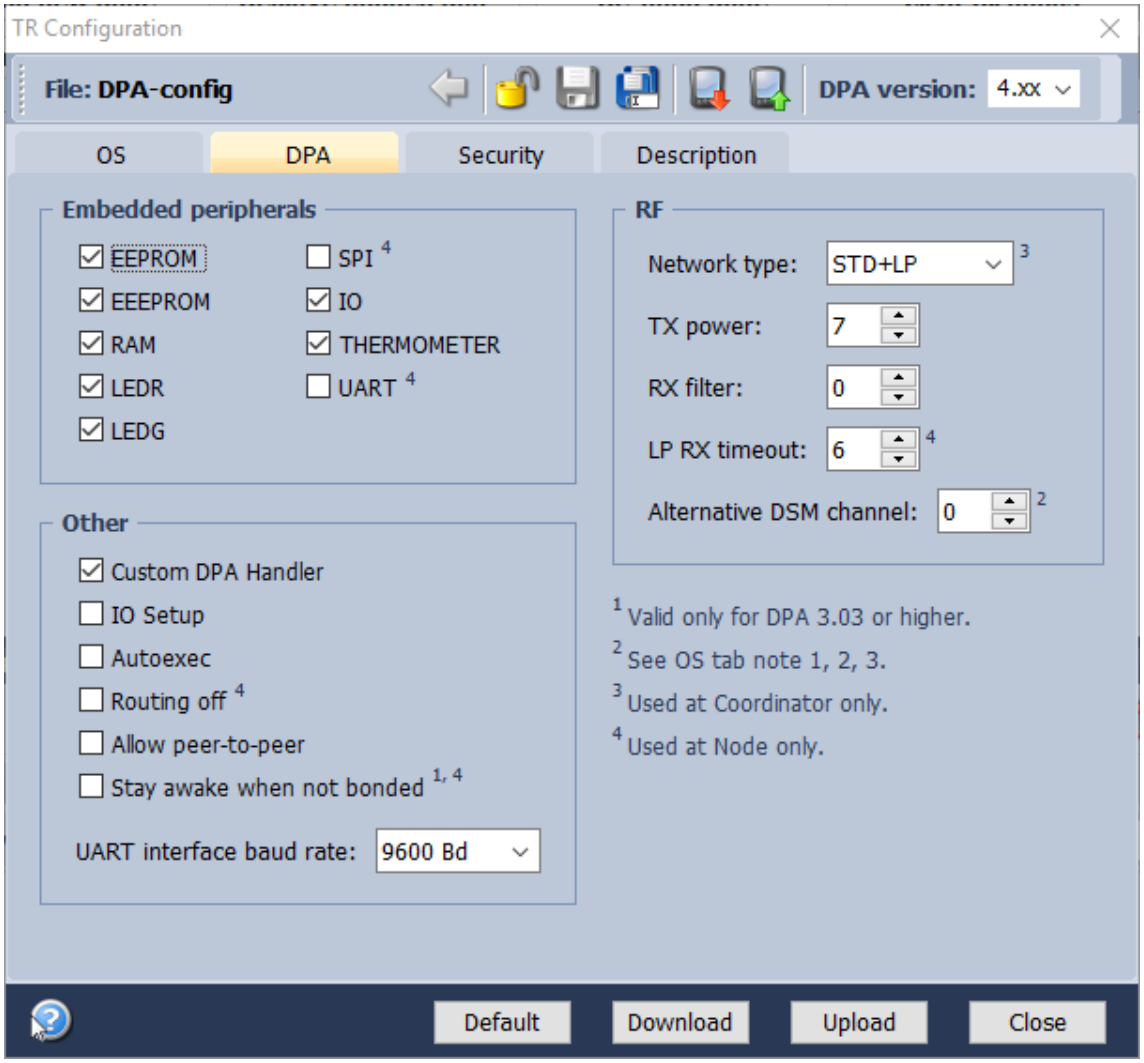
Obr. 27 – Vytvoření HEX souboru z přidaného souboru (zdroj: vlastní zpracování)

Nyní při otevření souboru DPA-config.xml v levé části obrazovky se zobrazí nastavení transceiveru. Je zde možné nastavit RF kanál, vysílací výkon a jiné vlastnosti transceiveru - viz Obr. 28. Přenos dat mezi IQRF zařízeními zde lze také zabezpečit heslem. Tyto nastavení by měla být až na pár výjimek shodná pro všechny transceivery (koordinátor i nody), které budeme chtít spojit.

5.4.3 Vytvoření nodu

K vytvoření nodu je potřeba nahrát do transceiveru program pro nod.

Před tím je ale důležité zaškrtnout možnost Custom DPA Handler na kartě DPA. Custom DPA Handler umožní práci s externími připojenými zařízeními, jako jsou externí senzory (senzor teploty, světla), či relé. Toto nastavení není potřeba zaškrtnout při konfiguraci koordinátoru, viz Obr. 28



Obr. 28 – Okno nastavení transceiveru DPA-config.xml (zdroj: vlastní zpracování)

Konfigurace se uloží kliknutím na ikonu diskety nahoře uprostřed. Pro nahrání programu do transceiveru, který bude sloužit jako nod, je nyní nutné zaškrtnout sekci Plug-ins a v ní soubor DPA-Node-LP-7xD-V401-190307.iqrf. Dále je nutné zaškrtnout sekci Output HEX a vybrat soubor HEX, který byl vytvořen po kliknutí na tlačítko „Build select source file“, nebo zmáčknutí klávesy F10.

Nyní je možné konfiguraci nahrát do připojeného transceiveru tlačítkem „Upload selected files by menu selection“, nebo klávesou F5.

5.4.4 Vytvoření koordinátoru

Nahrání koordinátoru, který bude řídit IQRF síť bude podobné jako nahrání nodu. Do CK-USB programátoru připojíme transceiver, který bude používán jako koordinátor.

V DPA-config.xml není ale potřeba mít zaškrtnutou možnost „Custom DPA Handler“, jelikož je na koordinátoru zbytečná. Po odškrtnutí Custom DPA Handleru je nutné konfiguraci uložit kliknutím na disketu a konfiguraci je nyní možné zavřít.

Do koordinátoru se nebude nahrávat žádný HEX soubor. Odškrtneme tedy sekci Output HEX a v Plug-ins místo DPA-Node-LP-7xD-V401-190307.iqrf nyní zvolíme DPA-Coordinator-SPI-7xD-V401-190307.iqrf.

Nyní, jako v případě nodu, je možné konfiguraci nahrát do připojeného transceiveru tlačítkem „Upload selected files by menu selection“, nebo klávesou F5.

5.4.5 Párování nodů ke koordinátoru

Pro spárování nodů ke koordinátoru je nutné transceivery, naprogramované jako nody, zapojit například do DK-EVAL-04A přenosné sady s baterií a transceiver, naprogramovaný jako koordinátor připojit k počítači přes CK-USB programátor. Na nodech by měla blikat červená LED dioda. To značí, že je nod připraven k párování. Pokud nebliká, je nutno nod odpárovat podržením obou tlačítek na DK-EVAL-04A, puštěním tlačítka reset a až blikne zelená led, tak poté puštěním tlačítka User (SW1). Nyní by již červená dioda měla blikat a je možné nod spárovat.

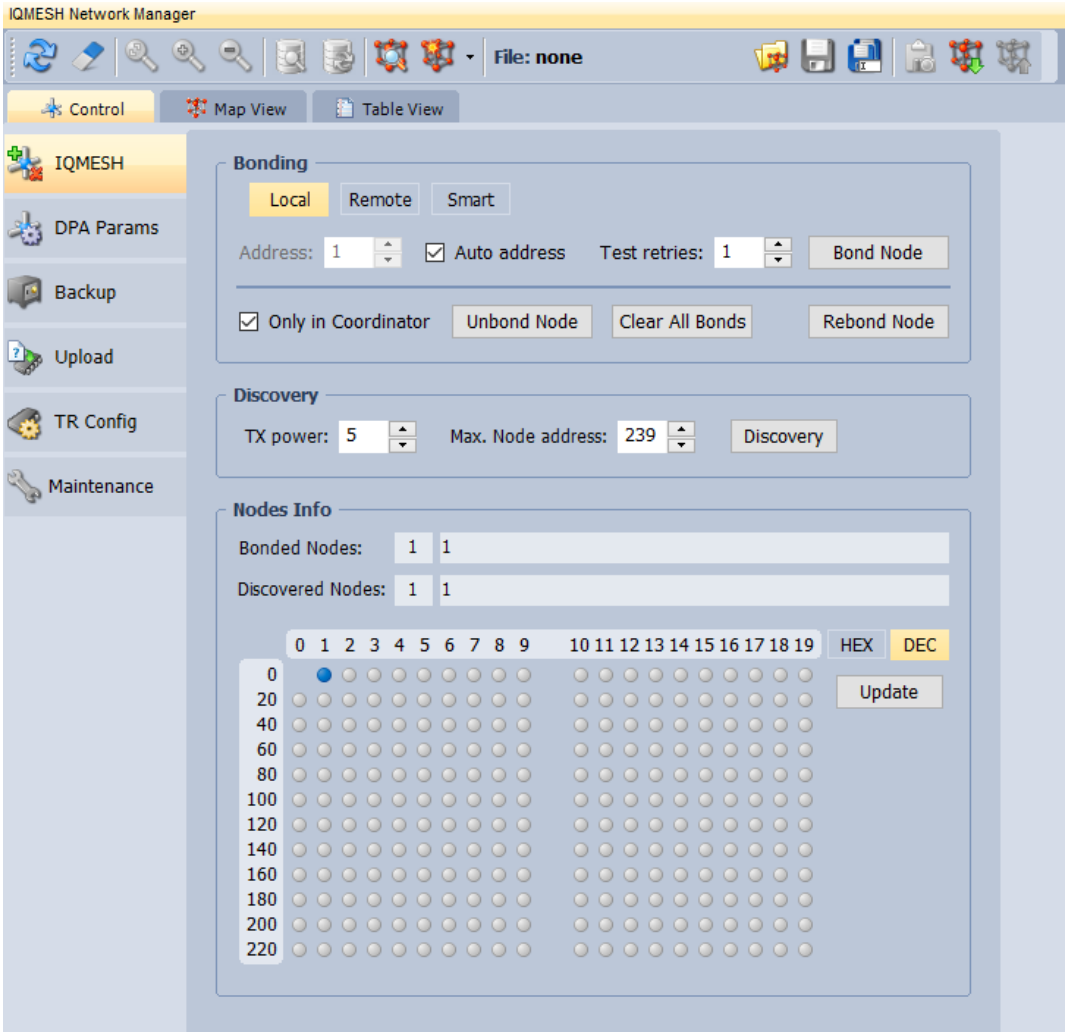
Pro spárování je možné použít prostředí IQRF_IDE a jeho sekci IQMESH Network Manager.

Doporučené je odškrtnout možnost „Only in Coordinator“ a kliknout na tlačítko „Clear All Bonds“ pro odpojení všech připojených nodů.

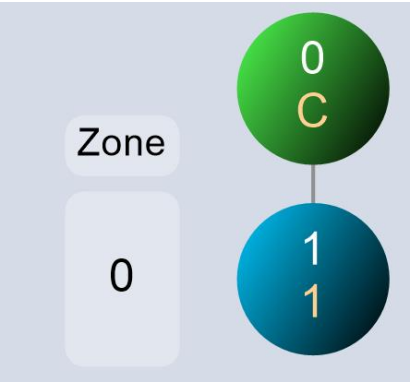
Po kliknutí na tlačítko „Bond Node“ je několik vteřin na to, zmáčknout na nodu tlačítko SW1. Takto lze spárovat vícero nodů.

Kliknutím na tlačítko „Discovery“ se automaticky nastaví routovací topologie sítě. Rozhraní je zobrazeno na Obr. 29.

Na záložce Map View lze vidět aktuální mapu IQMESH sítě, viz Obr. 30



Obr. 29 – IQMESH Network Manager s připojeným nodem (zdroj: vlastní zpracování)

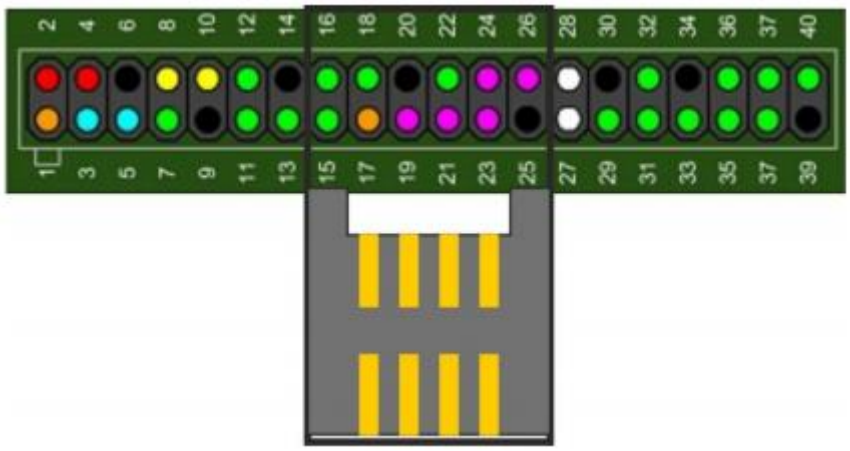


Obr. 30 – Mapa IQMESH sítě s koordinátorem a spárovaným nodem (zdroj: vlastní zpracování)

5.5 Příprava, instalace a nastavení Raspberry Pi

5.5.1 Instalace operačního systému a prvotní spuštění Raspberry Pi

Aby bylo možné k Raspberry Pi připojit transceiver TR-72DA, je využíváno přídavného modulu KON-RASP-01. Ten je kompatibilní se všemi verzemi Raspberry Pi a připojuje se pomocí GPIO konektoru přesně doprostřed (na Raspberry Pi 2 Model B), viz Obr. 31



Obr. 31 – Schéma připojení modulu KON-RASP-01 přes GPIO konektor (zdroj: [53])

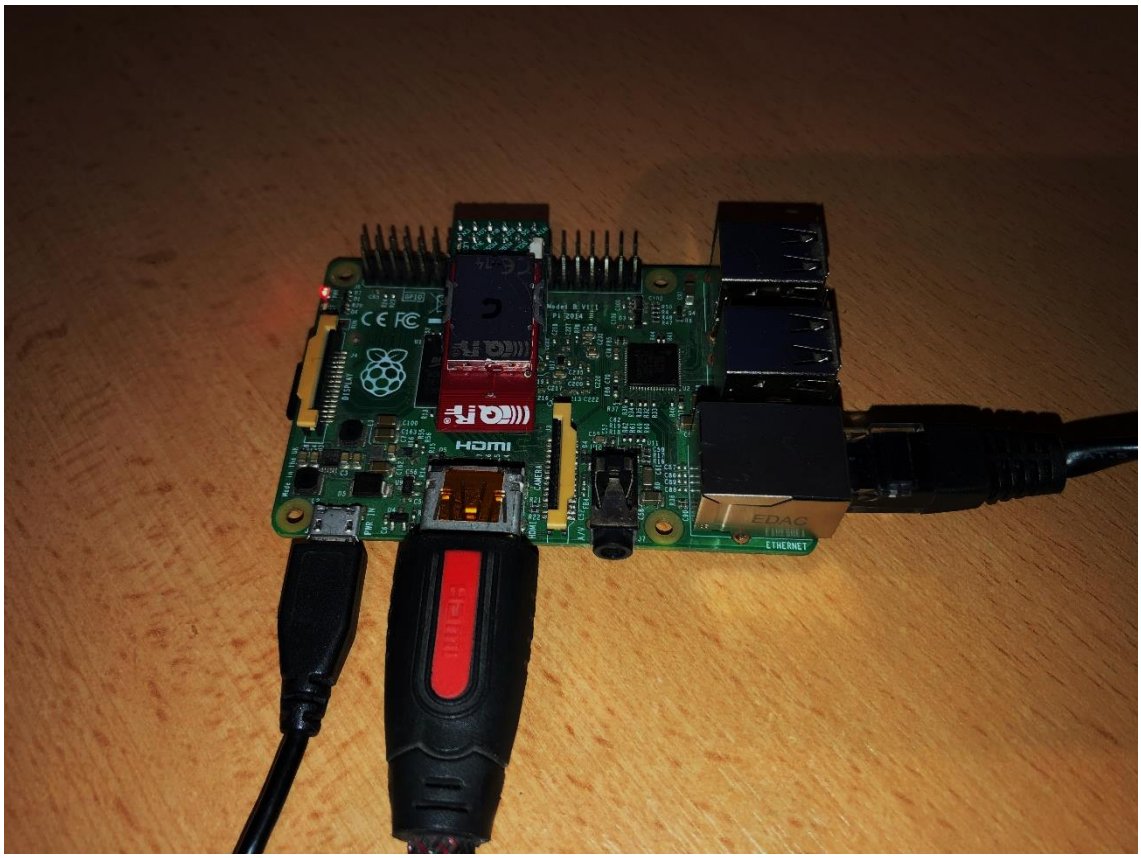
Následně je nutné nainstalovat a nastavit Raspberry Pi jako IQRF bránu. Test byl proveden na operačním systému Linux, přesněji se jedná o linuxovou distribuci s názvem Raspbian, která je určena přímo pro Raspberry Pi.

Instalace je velice snadná. Nejjednodušší způsob instalace Raspbianu do Raspberry Pi je přes instalátor zvaný NOOBS (New Out Of the Box Software). Stačí pouze stáhnout NOOBS, nakopírovat ho na naformátovanou micro SD kartu, která má kapacitu větší než 8 GB (4 GB pro lite verzi) a vložit ji do Raspberry Pi počítače.

Počítač je nutno připojit k monitoru, či jinému zobrazovacímu zařízení. K tomu slouží HDMI port. Dále je nutno připojit alespoň myš, nebo klávesnici přes USB porty. Je doporučené připojit myš i klávesnici a Raspberry Pi připojit i k Internetu přes ethernetový port. Napájení Raspberry Pi je možné přes microUSB port. V základním zapojení bez periferií lze, díky relativně nízké spotřebě, napájet Raspberry z USB portu počítače či notebooku.

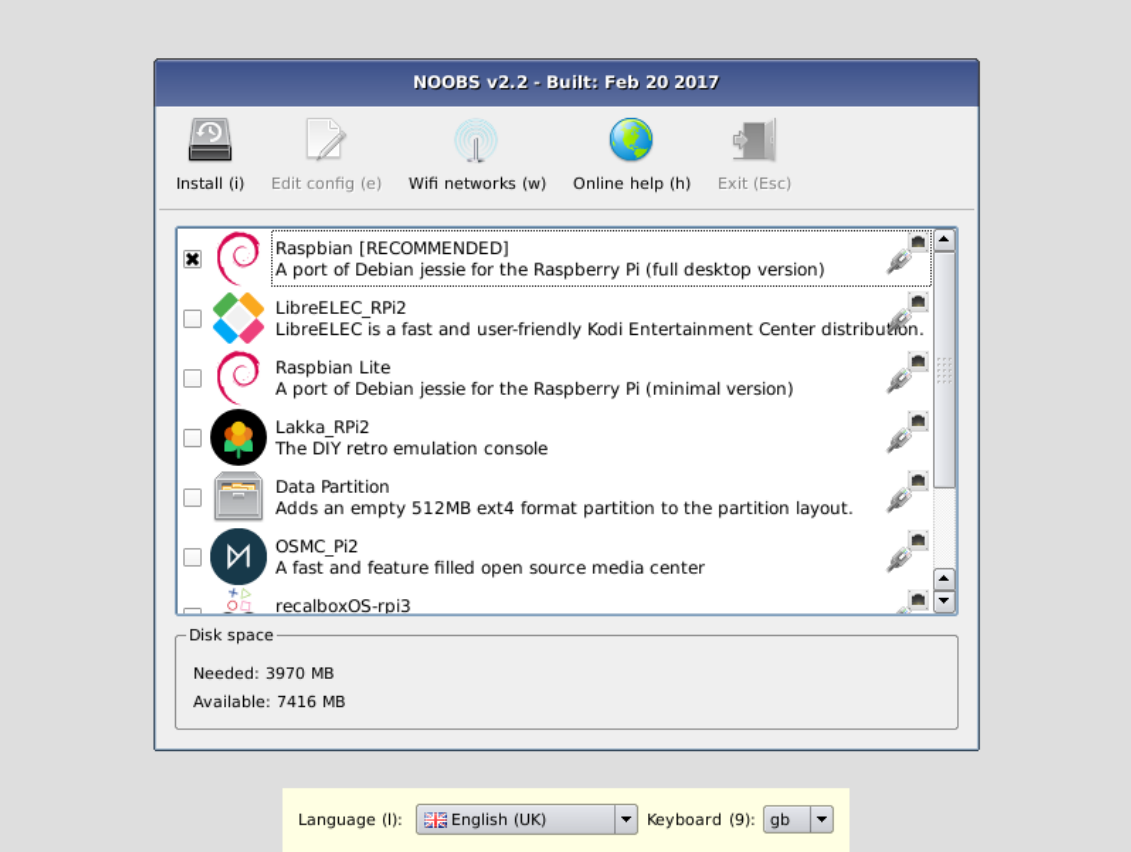
Po připojení napájení se rozsvítí kontrolky. Svítící červená kontrolka znamená, že zařízení je napájeno a blikající zelená kontrolka značí aktivitu mikro SD karty. Zařízení nemá žádné tlačítko na vypnutí či zapnutí, tudíž se zapne ihned po připojení napájení.

Zapojené Raspberry Pi použité v této práci je na Obr. 32.



Obr. 32 – Raspberry Pi s připojeným napájením, modulem pro IQRF transceiver, HDMI kabelem pro výstup a ethernetovým kabelem pro připojení k internetové síti (zdroj: vlastní zpracování)

Po zapnutí zařízení se na připojené obrazovce zobrazí tabulka s výběrem požadovaného operačního systému. Zde lze vybrat operační systém, který bude nainstalován. Doporučené je zvolit Raspbian, viz Obr. 33



Obr. 33 – Instalační prostředí NOOBS k instalaci operační systému (zdroj:[54])

Po zvolení požadovaného operačního systému se systém automaticky nainstaluje (v případě lite verze se stáhne a nainstaluje – je ale nutné, aby bylo Raspberry připojeno k Internetu).

Délka instalace systému závisí na zvoleném systému, jeho velikosti a rychlosti micro SD karty, na kterou se systém instaluje.

5.5.2 Aktualizace systému Raspbian Linux

Potom, co se systém nainstaluje a spustí je vhodné systém aktualizovat na nejnovější verzi. To se provede otevřením terminálu v horním levém rohu a napsáním příkazu

```
sudo apt-get update && sudo apt-get -y full-upgrade
```

Příkaz sudo znamená „substitute user do“, který slouží k vykonání nějaké operace s oprávněním jiného uživatele. V tomto případě se jedná o uživatele root, který je obdobný administrátorovi (nebo také správci) ve Windows. Stejně jako on, root má

nejvyšší práva v systému. [55] `Apt-get` je nástroj k práci s APT softwarovými balíčky. `Apt-get update` načte seznam balíčků, které potřebují aktualizovat. Znaky && znamenají logický and, tudíž až po úspěšném provedení první části před && se provede část druhá. Druhá část `apt-get -y full-upgrade` nainstaluje nejnovější verze softwarových balíčků a část `-y` znamená, že se příkaz potvrdí a není nutné ručně potvrzovat, že opravdu chceme balíčky nainstalovat.

5.5.3 Instalace SSH serveru na Raspbian Linux

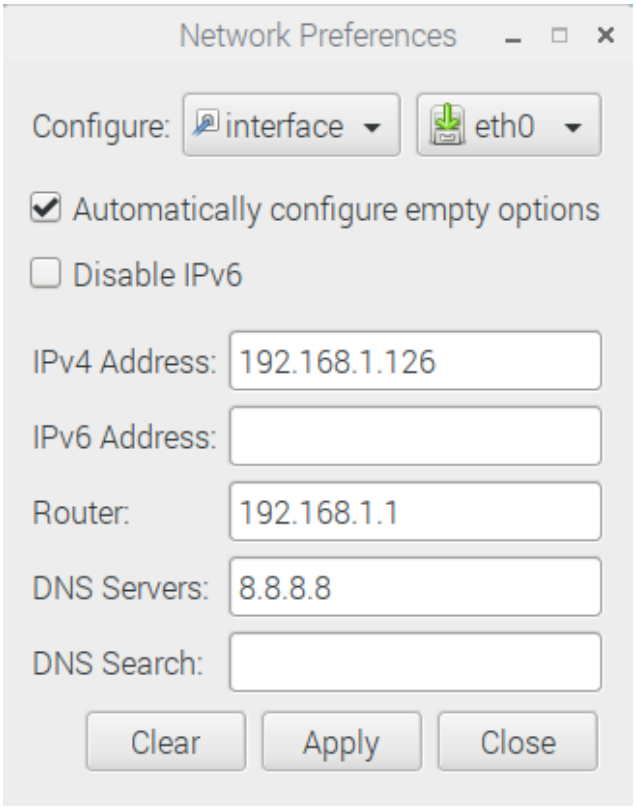
Dále pro pohodlnější ovládání Raspberry lze nainstalovat SSH server. Ten umožní ovládání Raspberry Pi přes jiný počítač. To lze provést příkazem

```
sudo apt-get install -y ssh
```

Je nutné restartovat a spustit SSH službu. K tomu slouží příkaz

```
sudo systemctl enable ssh.service && sudo systemctl start ssh.service
```

Je potřebné nastavit statickou (fixní) IP adresu Raspberry Pi, aby nedošlo k její automatické změně. Nejjednodušeji toto lze provést v grafickém rozhraní pravým kliknutím na ikonky šipek v horním menu a kliknutím na „Wireless & Wired Network Settings", kde je potřeba zvolit rozhraní (v našem případě eth0) a vyplnit požadovanou IP adresu a výchozí bránu routeru z aktuálního adresního rozsahu připojené sítě (v tomto případě IPv4 adresa 192.168.1.126 a výchozí brána (Router) 192.168.1.1), viz Obr. 34



Obr. 34 – Nastavení statické IP adresy v Raspberry Pi (zdroj: vlastní zpracování)

Nyní je možné se připojit k Raspberry Pi přes jiný počítač. K tomu byl použit program Putty. Pro kontrolu nastavení je tedy v terminálu možné použít příkaz *sudo ifconfig*.

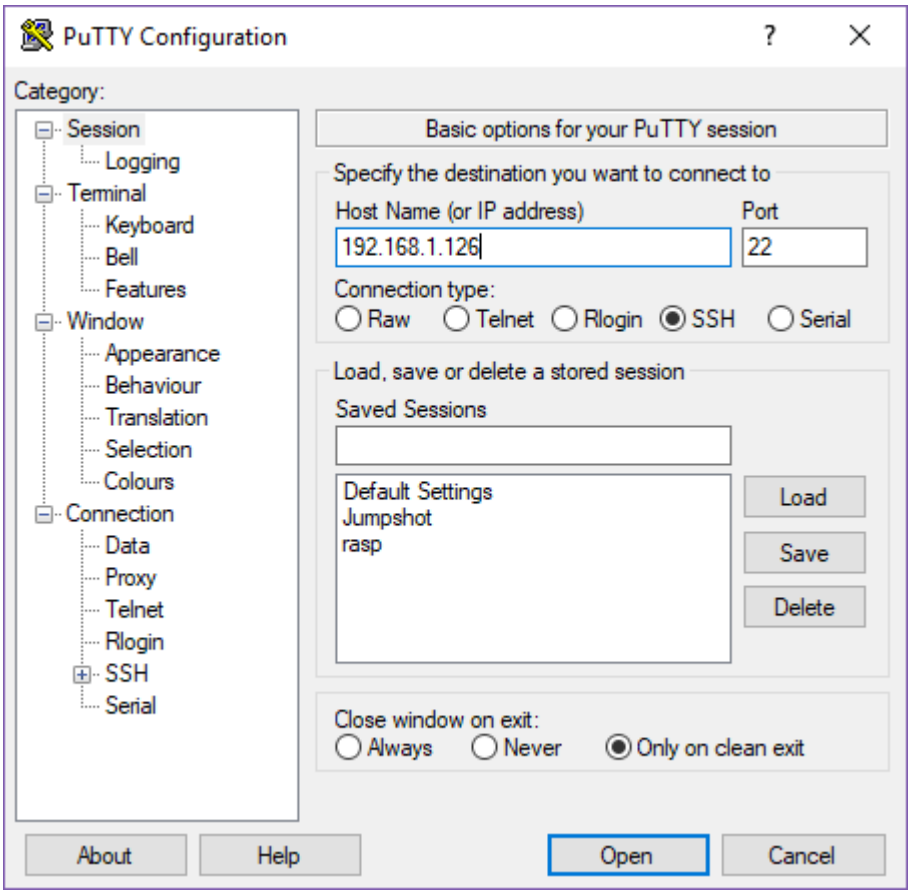
```
pi@raspberrypi:~ $ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.126  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::58e9:4e9f:ecd6:3fe8  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:10:97:b7  txqueuelen 1000  (Ethernet)
        RX packets 16006  bytes 16302011 (15.5 MiB)
        RX errors 0  dropped 29  overruns 0  frame 0
        TX packets 8905  bytes 833254 (813.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8972  bytes 862523 (842.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8972  bytes 862523 (842.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pi@raspberrypi:~ $
```

Obr. 35 – Výpis příkazu *sudo ifconfig* (zdroj: vlastní zpracování)

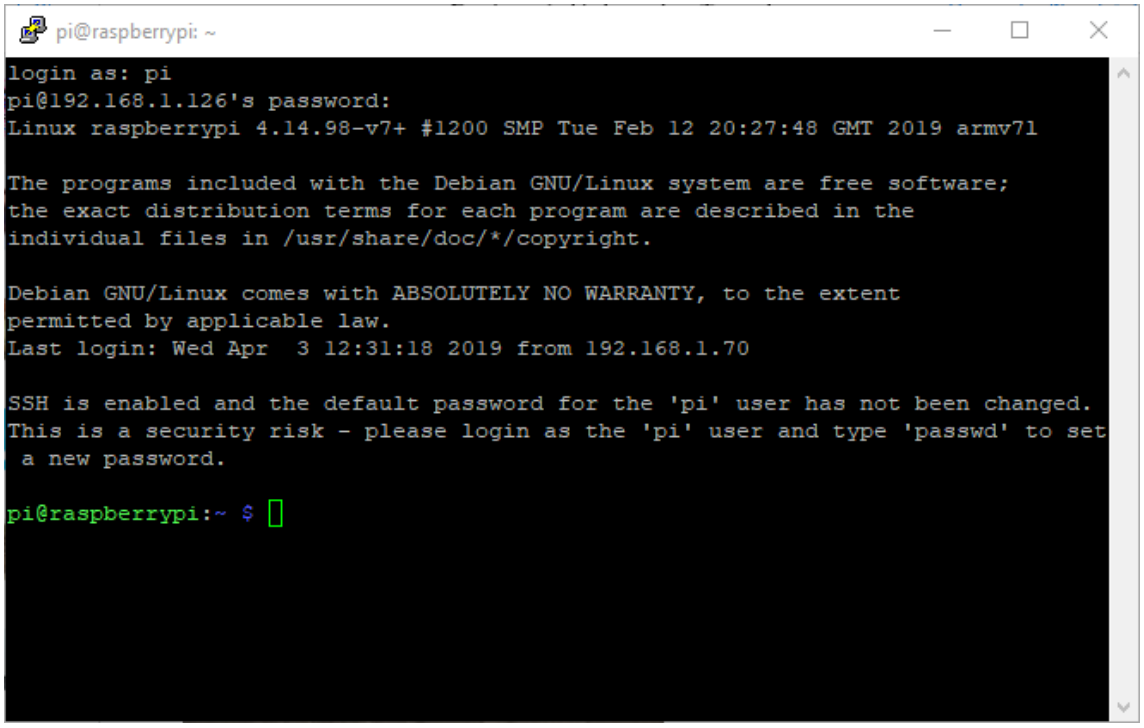
Na Obr. 35, na rozhraní eth0, v řádku inet lze vidět IP adresa 192.168.1.126. Tu je možné zadat do programu Putty v jiném počítači, který je připojen ve stejné síti jako Raspberry Pi a spravovat tak Raspberry Pi z daného počítače, viz Obr. 36



Obr. 36 – Putty pro připojení přes SSH s vyplněnou IP adresou Raspberry Pi (zdroj: vlastní zpracování)

Po kliknutí na Open se zobrazí okno, ve kterém je potřeba se přihlásit. Výchozí jméno je „pi“ a heslo je „raspberry“

Po úspěšném přihlášení se zobrazí základní informace, z níž lze vyčíst například verzi Linuxu, aktuální čas a kdy byl uskutečněn poslední login, viz Obr. 37.

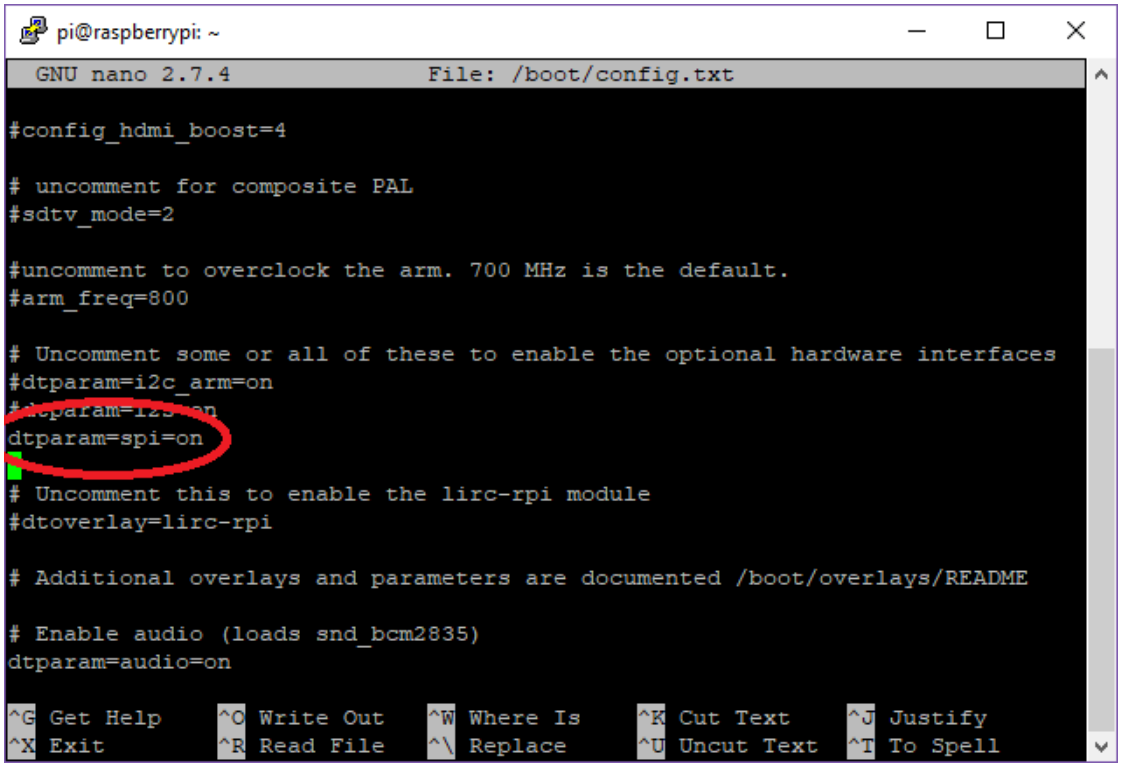


Obr. 37 – Úvodní stránka po úspěšném přihlášení (zdroj: vlastní zpracování)

5.5.4 Povolení SPI

Pro povolení připojeného modulu KON-RASP-01 je nutné povolit SPI (Serial Peripheral Interface). K tomu je potřeba otevřít konfigurační soubor config.txt, který je umístěný ve složce boot. Pro otevření a editaci souboru lze použít textový editor GNU nano. Ten lze zavolat příkazem nano <cesta k soboru>. Pro editaci konfiguračního souboru config.txt je nutné zavolat tento příkaz jako root. To se provede příkazem: `sudo nano /boot/config.txt`

V tomto souboru je potřeba odkomentovat (odstranit #) řádek dtparam=spi=on. Tím se SPI povolí, viz Obr. 38



Obr. 38 – Soubor /boot/config.txt s povoleným SPI (zdroj: vlastní zpracování)

Následně je třeba restartovat systém příkazem *sudo reboot.* Po tomto příkazu se Raspberry Pi restartuje a je nutné se znovu přes Putty připojit.

5.5.5 Implementace Mosquitto (MQTT protokolu)

V následujícím kroku je třeba nainstalovat a nastavit Mosquitto.

Instalace MQTT brokera se provede příkazem:

```
sudo apt-get install -y mosquitto mosquitto-clients
```

Pro ověření, že je MQTT správně nainstalován a spuštěn je možné použít příkaz `systemctl status mosquitto.service`.

Na Obr. 39 lze vidět správně nainstalovanou a spuštěnou službu Mosquitto.

```
pi@raspberrypi:~ $ systemctl status mosquitto.service
● mosquitto.service - LSB: mosquitto MQTT v3.1 message broker
   Loaded: loaded (/etc/init.d/mosquitto; generated; vendor preset: enabled)
   Active: active (running) since Thu 2019-04-04 15:30:01 CEST; 1h 14min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 274 ExecStart=/etc/init.d/mosquitto start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/mosquitto.service
           └─377 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

Apr 04 15:29:58 raspberrypi systemd[1]: Starting LSB: mosquitto MQTT v3.1 message broker...
Apr 04 15:30:00 raspberrypi mosquitto[274]: Starting network daemon:: mosquitto.
Apr 04 15:30:01 raspberrypi systemd[1]: Started LSB: mosquitto MQTT v3.1 message broker.
pi@raspberrypi:~ $
```

Obr. 39 – Výpis stavu MQTT brokeru (zdroj: vlastní zpracování)

5.5.6 Zabezpečení Mosquitto pomocí statického hesla a ACL souboru

Je vhodné Mosquitto zabezpečit tím, že se přidá autentifikace. Vytvoří se tedy heslo pro uživatele příkazem:

```
sudo mosquitto_passwd -c /etc/mosquitto/passwd pi
```

Poslední část příkazu (pi) je uživatelské jméno uživatele, pro kterého chceme vytvořit heslo.

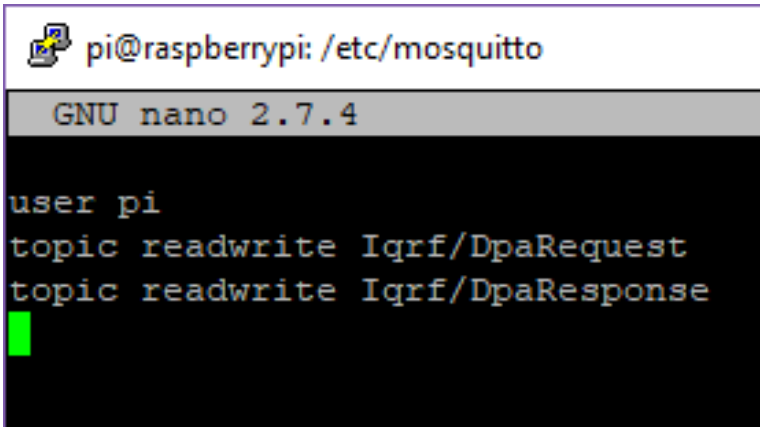
Dále je nutné vytvořit ACL soubor pod názvem „acls“ ve složce /etc/mosquitto

Ten se vytvoří pomocí příkazu *sudo touch /etc/mosquitto/acls*

Nyní je ještě potřeba ho editovat pomocí *sudo nano /etc/mosquitto/acls*

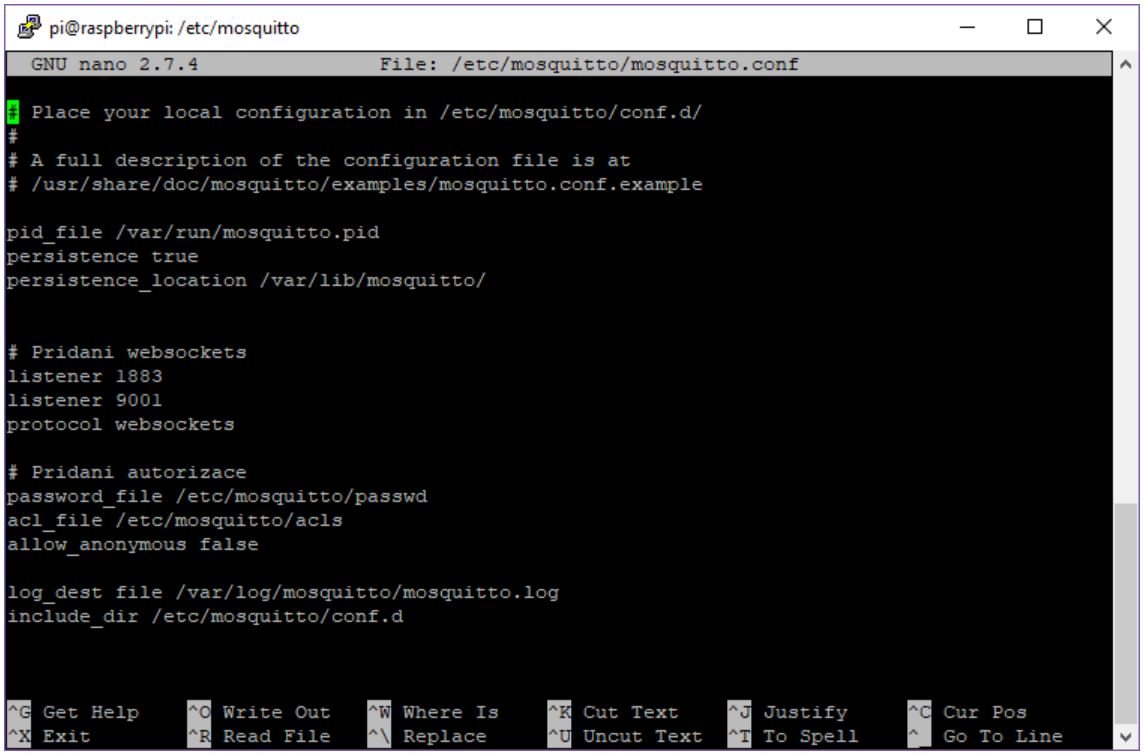
A vepsat do něho uživatele, který bude moci používat MQTT broker a témata (topic).

Soubor tedy bude vypadat jako na Obr. 40.



Obr. 40 – Mosquitto ACL soubor (zdroj: vlastní zpracování)

Nutné je také povolit autorizaci v konfiguračním souboru a také povolit websockets pro možnost zobrazování dat v reálném čase ve webovém rozhraní.
sudo nano /etc/mosquitto/mosquitto.conf, upravený soubor viz Obr. 41.



Obr. 41 – Konfigurace souboru mosquitto.conf pro přidání websockets a autorizace (zdroj: vlastní zpracování)

5.5.7 Instalace IQRF daemona

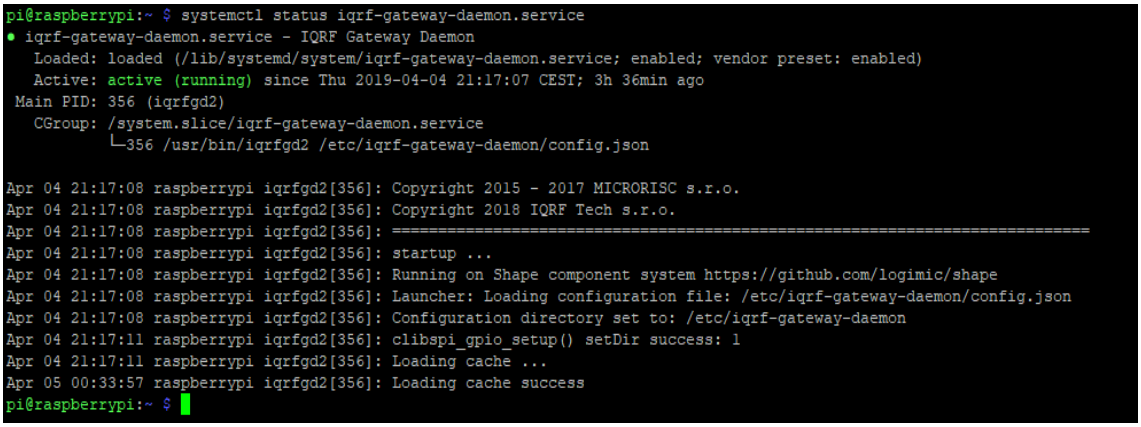
IQRF Gateway Daemon je open source softwarový balíček, který umožňuje snadno vytvořit IQRF bránu s připojením k Internetu a cloudu z Linuxového zařízení a umožňuje spravovat komunikační kanály UDP, MQ, WebSocket a MQTT z webového rozhraní přes IQRF Gateway WebApp. [56]
K nainstalování IQRF daemona je potřeba zadat 4 příkazy:

1. `sudo apt-get install -y dirmngr apt-transport-https`
2. `sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 9C076FCC7AB8F2E43C2AB0E73241B9B7B4BD8F8E`
3. `echo "deb http://repos.iqrf.org/testing/debian stretch testing" | sudo tee -a /etc/apt/sources.list.d/iqrf-gateway.list`
4. `sudo apt-get update && sudo apt-get install -y iqrf-gateway-daemon`

Pro zjištění, že konfigurace proběhla správně, slouží příkaz:

```
systemctl status iqrf-gateway-daemon.service
```

Na Obr. 42 lze vidět, že je služba ve stavu active (running) a vše je tedy v pořádku.



Obr. 42 – Výpis stavu IQRF Daemona (zdroj: vlastní zpracování)

5.5.8 IQRF Gateway Daemon WebApp

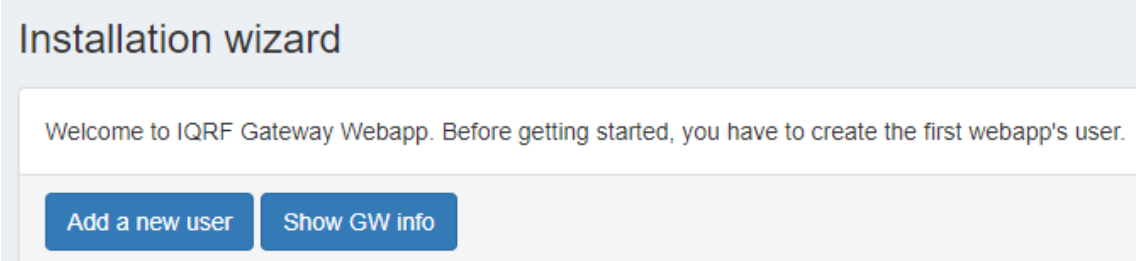
IQRF Gateway Daemon WebApp je webová aplikace, která umožní správu IQRF zařízení.

K nainstalování této webové aplikace je nutné zadat tyto 4 příkazy:

1. `sudo apt-get -y install apt-transport-https lsb-release ca-certificates dirmngr`
2. `sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys D93B0C12C8D04D7AAFBCFA27CCD91D6111A06851`
3. `sudo sh -c 'echo "deb https://repozytorium.mati75.eu/raspbian stretch-backports main contrib non-free" > /etc/apt/sources.list.d/php.list'`
4. `sudo apt-get update && sudo apt-get install -y iqrf-gateway-webapp`

K ověření funkčnosti je z Raspberry Pi možné v internetovém prohlížeči jít na adresu http://localhost/. Pro přistoupení k webovému rozhraní z jiného počítače ve stejné síti, jako je Raspberry Pi, je možné zadat do prohlížeče IP adresu Raspberry Pi (v tomto případě 192.168.1.126).

Po zadání dané adresy do internetového prohlížeče je zobrazena úvodní stránka IQRF brány, kde je možné přidat uživatele a zobrazit informace o bráně, viz Obr. 43.



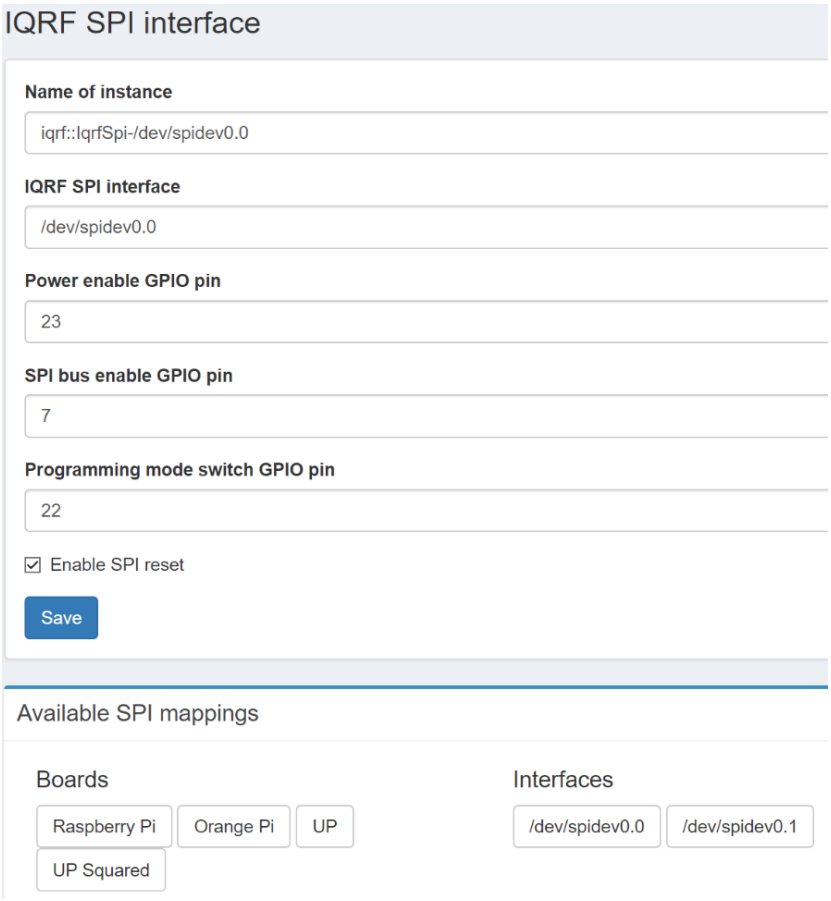
Obr. 43 – Úvodní stránka IQRF brány ve webovém rozhraní (zdroj: vlastní zpracování)

Pro pokračování je nutné přidat uživatele kliknutím na tlačítko „Add a new user“, zadat uživatelské jméno a heslo, vytvořit nového uživatele a poté se pomocí stejného uživatelského jména a hesla přihlásit.

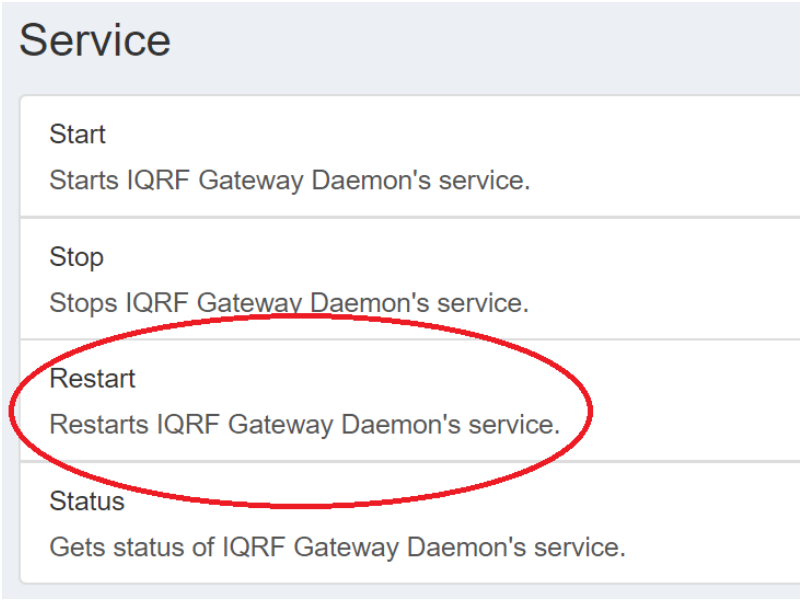
5.5.9 Konfigurace IQRF SPI rozhraní

V sekci Configuration – IQRF SPI interface je důležité zvolit ve spodní části právě používané zařízení, jeho rozhraní a kliknout na tlačítko Save pro uložení. V tomto případě bylo vybráno Raspberry Pi a /dev/spidev0.0, viz Obr. 44.

Po tomto kroku je důležité restartovat IQRF Gateway Daemon. To lze provézt přes webové rozhraní v sekci Service a kliknutím na položku Restart, viz Obr. 45



Obr. 44 – Nastavení IQRF SPI rozhraní ve webovém rozhraní (zdroj: vlastní zpracování)



Obr. 45 – Restart IQRF Gateway Daemona přes webové rozhraní (zdroj: vlastní zpracování)

Po restartu je možné zasílat DPA pakety přes webové rozhraní Gateway Daemona v sekci IQRF Net – Send DPA packet.

Ačkoliv by vše mělo fungovat, byl při zkoušení objeven problém, že ačkoliv byly všechny služby ve stavu „Active (running)“, nebylo možné odeslat ani přijmout žádný DPA paket přes webové rozhraní.

Tento problém byl vyřešen změnou souboru /etc/iqrf-gateway-daemon/config.json, ve kterém bylo nutné změnit „enabled“ z true na false u iqrf::IqrfCdc a iqrf::IqrfUart a nechat povolené pouze iqrf::IqrfSpi, viz Obr. 46.

Obr. 46 – Opravený problém v souboru /etc/iqrf-gateway-daemon/config.json (zdroj: vlastní zpracování)

5.5.10 Node.js

Node.js je serverové prostředí, které umožňuje chod JavaScriptu na serveru. JavaScript je programovací jazyk pro HTML a webové stránky.

K instalaci Node.js jsou potřeba následující příkazy:

1. `sudo apt-get install -y curl`
2. `curl -sL https://deb.nodesource.com/setup_6.x | sudo -E bash -`
3. `sudo apt-get install nodejs`

5.5.11 **Node-RED**

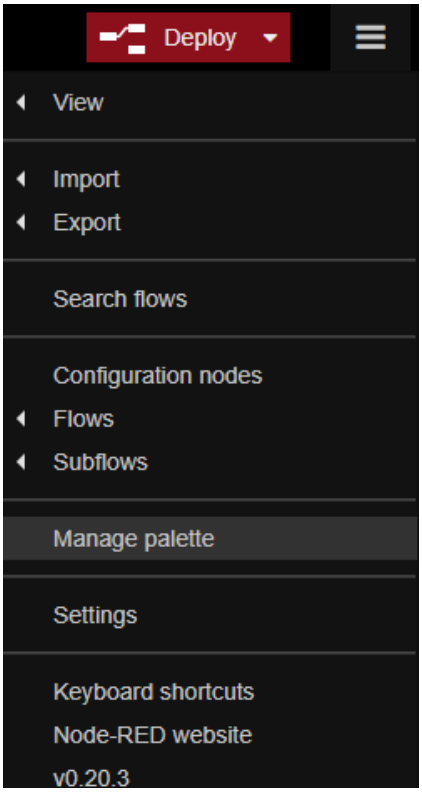
Pro nainstalování Node-RED a tedy možnosti programování funkce IoT zařízení jsou potřeba následující příkazy:

1. `sudo npm install -g --unsafe-perm node-red`
2. `sudo npm install -g pm2`

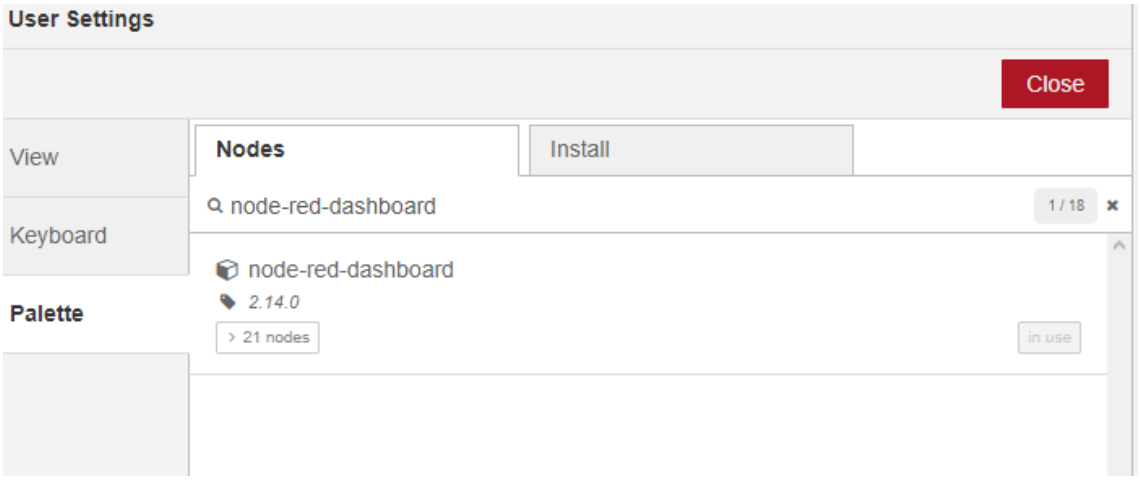
Následně je nutné Node-RED spustit příkazy:

1. `cd /home/pi`
2. `pm2 start /usr/bin/node-red --node-args="--max-old-space-size=128"`

Pro přistoupení k Node-RED webovému rozhraní slouží IP adresa IQRF brány s portem 1880 (v tomto případě tedy 192.168.1.126:1880). Aby bylo možné zobrazit aktuálních data z IQRF zařízení je vhodné použít například Node-RED dashboard, který lze snadno přes Node-RED nastavovat a upravovat. Ten lze přidat ve vysouvacím menu – Manage palette, vyhledáním node-red-dashboard a kliknutím na tlačítko install, viz Obr. 47 a Obr. 48



Obr. 47 – Menu nabídka v Node-RED webovém rozhraní (zdroj: vlastní zpracování)



Obr. 48 – Vyhledání a instalace Node-RED Dashboardu (zdroj: vlastní zpracování)

5.5.12 IoT-Starter-Kit flow

Flow udělaný přímo pro IQRF-Starter-Kit a umožní rychlé nasazení a vyzkoušení funkčnosti IQRF brány. Je již naprogramován pro odesílání požadavku pro získání

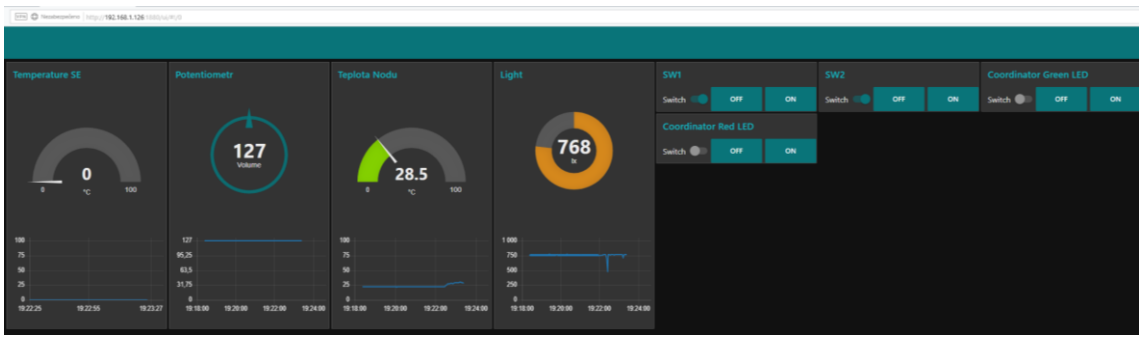
dat z IQRF nodů každé 3 vteřiny. Získává teplotu nodu, teplotu externího senzoru teploty připojeného k nodu, získání hodnoty osvětlení z externího světelného senzoru a hodnoty potenciometru. Dále jsou zde 4 přepínače, z toho 2 slouží k ovládání LED na koordinátoru a 2 přepínače jsou pro nastavování relé připojeného k nodu.

IoT-Starter-Kit flow je nainstalován stažením a nakopírováním Starter-Kit souborů do složky /home/pi/.node-red a následným restartem Node-RED.

To se provede následujícími příkazy:

1. `cd /home/pi`
2. `git clone https://gitlab.iqrf.org/alliance/iot-starter-kit.git`
3. `cd iot-starter-kit/install`
4. `cp rpi-board/node-red/* /home/pi/.node-red`
5. `pm2 restart node-red`

V nainstalovaném IoT-Starter-Kit flow byl objeven problém, že neprobíhala žádná komunikace mezi nodem a koordinátorem. To bylo způsobeno tím, že v MQTT nodech nebyl přidán vytvořený účet, který byl přidán pro zabezpečení. Po přidání uživatelského jména a hesla již vše funguje tak, jak má[3], viz Obr. 49



Obr. 49 – Node-RED dashboard (zdroj: vlastní zpracování)

Nyní je možné přepínači vypínat a zapínat LED diodu na koordinátoru a sledovat aktivní teplotu nodu pomocí všech počítačů, které jsou ve stejné síti s IQRF bránou.

[3] Zdrojem veškerých příkazů a postupu nastavení Raspberry Pi je [53]

Pro zabezpečený přístup k datům z nodů přes internet je vhodné použít vlastní server, nebo například cloud.

5.6 Zabezpečení a nastavení routeru s IoT zařízeními

Pro zabezpečení a zamezení přístupu neoprávněným osobám je vhodné síť, ve které jsou IoT zařízení a IoT brána oddělit od jiných zařízení (například tiskárny, zaměstnanecké počítače, bezdrátově připojené zařízení a podobně). V praxi to může znamenat separování různých oddělení a služeb firmy. Není totiž bezpečné, aby pracovníci výroby, byli ve stejné síti s jiným oddělením firmy, které s nimi nemá nic společného. Zamezí se tak neoprávněným přístupům k datům.

Toho lze docílit tím, že jednotlivá oddělení budou mít vlastní síť, tudíž budou připojena na jiný switch s jiným rozsahem IP adres.

Pokud přeci jen bude potřeba nějaká komunikace mezi těmito sítěmi, je možné toho docílit implementací routeru, tedy směrováním datového provozu společně s použitím firewallových pravidel, která povolí pouze požadovanou síťovou komunikaci mezi definovanými zařízeními.

5.6.1 Zapojení MikroTik routeru

MikroTik RB493g obsahuje dva hardwarové, oddělené switche. Jeden switch je na portech ether1, ether6-ether9. Druhý switch je na portech ether2-ether5.

Toto oddělení portů může nahradit použití dvou fyzických zařízení (switchů). Uvedené zjednodušení je zde využito a do jednoho switche je přes ethernetový kabel zapojena IoT brána (port ether2) a počítač (port ether 3). Do druhého switche je připojen další počítač (port ether9). Poskytovatel Internetu je připojen do portu ether1, viz Obr. 50

Obr. 50 – Zapojený MikroTik RB493g (zdroj: vlastní zpracování)

5.6.2 Připojení a zabezpečení MikroTik routeru

Připojený router je nyní možné nastavovat přes připojené počítače. Nejjednodušším způsobem je použít již dříve zmíněný program Winbox. Ten umí zjistit připojená MikroTik zařízení a připojit se na ně přes IP nebo MAC adresu.

V případě použitého MikroTiku je výchozí uživatelské jméno účtu správce *admin* a heslo žádné není.

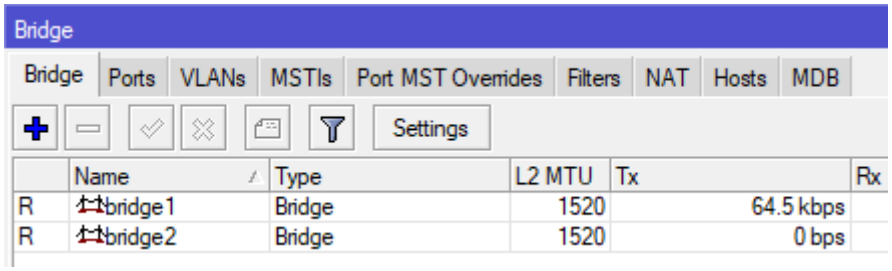
Po připojení je vhodné router zabezpečit a změnit přihlašovací jméno a heslo, případně s tím vytvořit uživatele s jiným jménem a heslem a nižšími oprávněními.

Změna hesla se provádí v sekci System – Password. Nový uživatel lze přidat v sekci System – Users. Pro větší zabezpečení lze novému uživateli přiřadit i IP adresa nebo rozsah adres, ze které bude moci k zařízení přistupovat.

5.6.3 Přiřazení portů do bridge

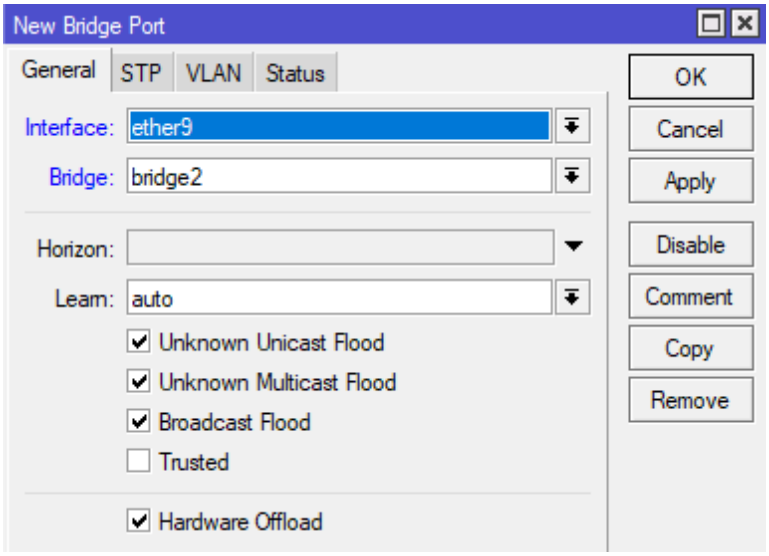
Pro možnost komunikace jednotlivých portů routeru je nutné vytvořit bridge a přiřadit do něho požadované porty.

V sekci Bridge byly tedy vytvořeny dva bridge tlačítkem +, viz Obr. 51



Obr. 51 – Vytvořené bridge rozhraní (zdroj: vlastní zpracování)

Porty se do jednotlivých bridge rozhraní přidají na kartě Ports a tlačítkem +, jak je zřejmé z Obr. 52.



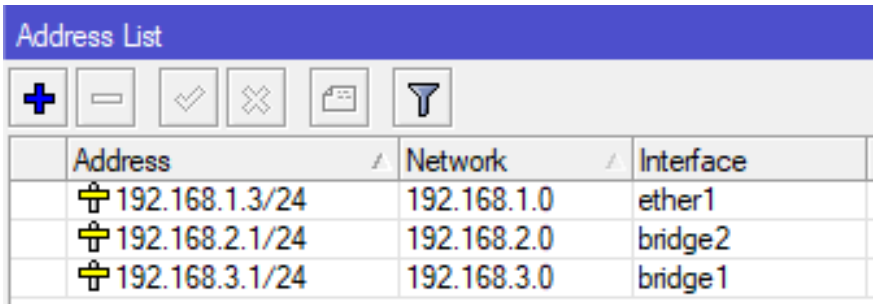
Obr. 52 – Přidání portu do bridge rozhraní (zdroj: vlastní zpracování)

Postupně byly rozděleny všechny porty. Pro bridge1 byly přidány porty ether2 až ether5. Pro bridge2 pak byly přidány porty ether6 až ether9.

5.6.4 Přiřazení IP adres na jednotlivá rozhraní

Pro ukázku byla IP adresa IoT brány (Raspberry Pi) změněna z 192.168.1.126 na 192.168.3.126, aby se nacházela v jiné síti. Počítač připojený do druhého switche má nastavenou IP adresu 192.168.2.70 a router poskytující Internet je zapojen do portu ethernet1 a má lokální adresu 192.168.1.1. Je nutné přiřadit IP adresy jednotlivým rozhraním v sekci IP – Addresses.

Portu ether1 byla nastavena IP adresa 192.168.1.3. Bridge rozhraní bridge1 byla nastavena IP adresa 192.168.3.1 a rozhraní bridge2 adresa 192.168.2.1, viz Obr. 53



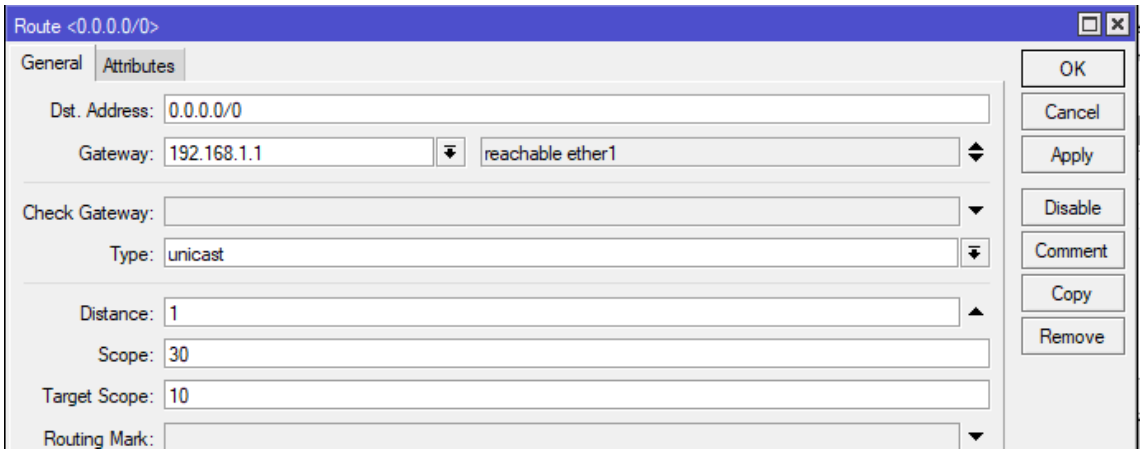
Obr. 53 – Přiřazené IP adresy jednotlivým rozhraním (zdroj: vlastní zpracování)

5.6.5 Přidání default route pro povolení cesty k Internetu

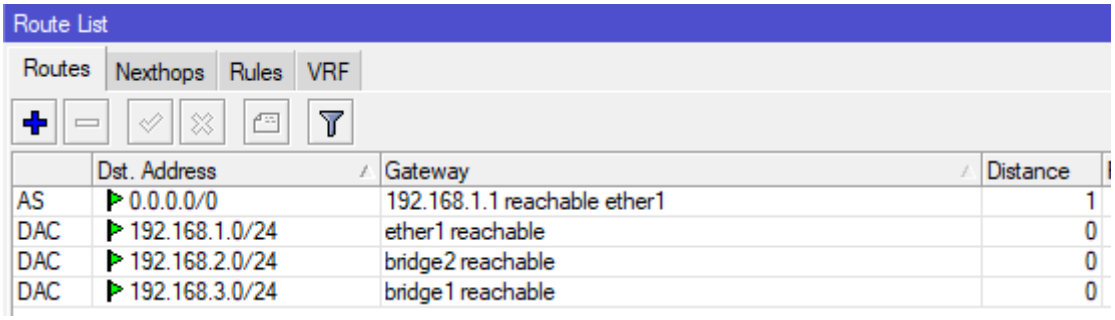
Aby připojená zařízení mohla přistoupit k Internetu, je nutno přidat tzv. default route, neboli výchozí cestu, přes kterou odejde paket, který nenajde požadovanou cílovou adresu. Vyznačuje se adresou 0.0.0.0/0 a pro přístup k Internetu je nutné ji přidat do routovací tabulky routeru v sekci IP – Routes.

Zde již také dynamický routovací protokol nalezl cesty do připojených sítí, viz Obr. 55.

Přidání default route se provede tlačítkem +, do kolonky Dst. Address se vyplní 0.0.0.0/0 a následně gateway (v tomto případě 192.168.1.1), viz Obr. 54.



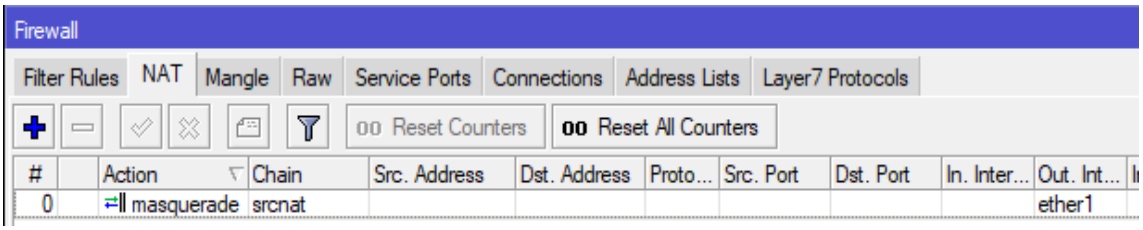
Obr. 54 – Přidání default route do routovací tabulky (zdroj: vlastní zpracování)



Obr. 55 – Routovací tabulka po přidání default route (zdroj: vlastní zpracování)

5.6.6 Povolení překladu IP adres

Překlad IP adres (neboli NAT) je nutný pro přístup k Internetu a funguje tak, že se více počítačů s různými IP adresami maskují za jednou IP adresou. Z Internetu tedy přijde paket na jednu IP adresu a NAT ji přeloží a předá zařízení, kterému je určené. Překládání adres se povolí v sekci IP – Firewall na záložce NAT. Tlačítkem + se přidá nové pravidlo, zvolí se Out. Interface, na kterém se budou adresy překládat (v tomto případě ether1) a na záložce Action je potřeba změnit Action na „masquarade“. Přidané NAT pravidlo znázorněno na Obr. 56.



Obr. 56 – Přidané NAT pravidlo (zdroj: vlastní zpracování)

5.6.7 Nastavení Firewall pravidel

Zabezpečení IoT brány může být provedeno několika způsoby. Jedním z nich je nastavení firewall pravidel.

Vhodné je, aby brána mohla komunikovat s počítačem, který ji může spravovat a zakázat ostatní komunikaci mezi bránou a ostatními zařízeními. Je také možno povolit určité porty, přes které se k části brány budou moci komunikovat (například přístup k webové stránce, kterou poskytuje webový server).

Zakázání je možné přes IP adresu, MAC adresu, síťový port či hardwarový port.

Pro lepší zabezpečení je doporučeno zakázat pravidly veškerou komunikaci a povolit pouze tu, kterou chceme.

U firewallových pravidel je důležité pořadí příkazů. Při uplatnění politik je procházeno pravidly ze shora dolů. První pravidlo, které se shoduje s procházejícím síťovým provozem, přepíše všechny následující pravidla. Proto se pravidla pro zakazování síťového provozu dávají až jako poslední pravidla a povolovací pravidla naopak před ně.

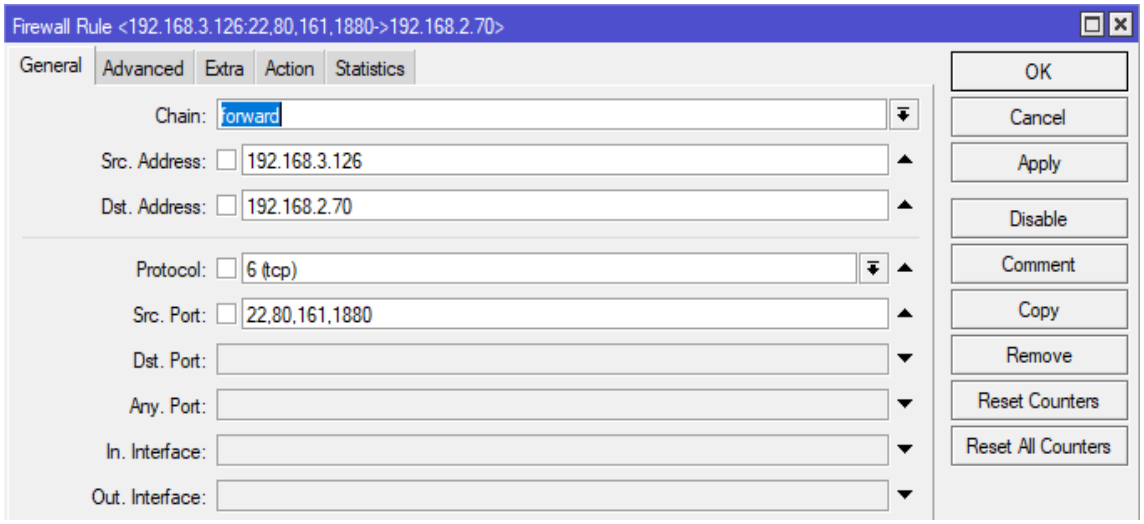
Pro možnost správy IoT brány necháme povolené porty 22 a 161 (SSH a SNMP[4] protokol), dále jelikož na IoT bráně je nainstalovaný webové rozhraní IQRF Gateway Daemon WebApp a webové rozhraní Node-RED, povolíme i porty 80 a 1880. Je nutné povolit tyto porty jdoucí k IP adrese brány (Dst Address - 192.168.3.126) z IP adresy počítače určeného pro správu (Src. Address - 192.168.2.70) a i v opačném směru, viz Obr. 57. Pro jistotu, že potenciální útočník nebude moci změnit IP adresu svého počítače na IP adresu povoleného počítače, je dobré přidat i MAC adresu daného počítače (Src. MAC Address). Na kartě Action bude akce „accept".

Nyní jsou porty povolené a je potřeba přidat pravidlo zakazující komunikaci mezi všemi ostatními počítači a IoT bránou. Vytvoříme tedy dvě firewallová pravidla. Jedno bude s cílovou adresou brány (tedy 192.168.3.126) a druhé se zdrojovou adresou brány (192.168.3.126). Na kartě action se nastaví akce „drop", neboli zahození daného paketu.

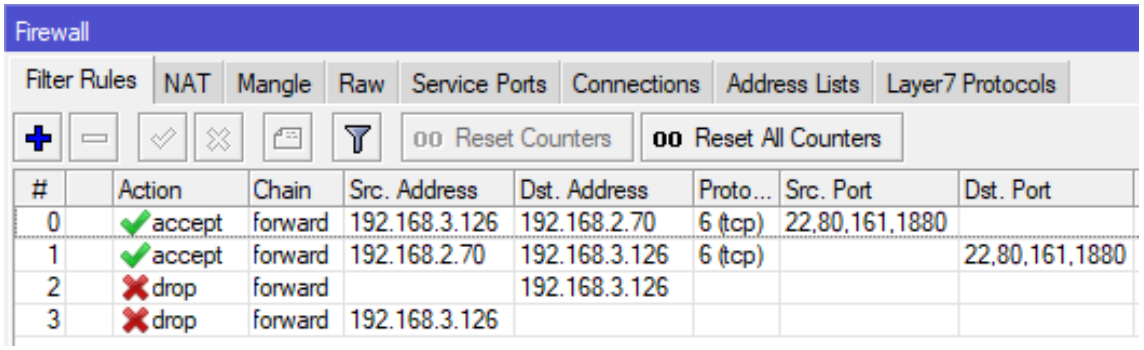
Filtrování je možné provádět i podle síťových rozhraní (např. pouze porty ether2). Je také možné přidat další filtrování i pro jiné počítače. To záleží na individuálním a preferovaném nastavení dané firmy. Pro budoucí využití je i vhodné povolit port pro odesílání dat do datového uložiště umístěného v síti, nebo cloudu.

Pro názornou ukázku nastínění funkčnosti byly ale použity pouze tato pravidla, viz Obr. 58.

[4] SNMP protokol umožňuje sběr dat pro správu sítě a jejich vyhodnocování



Obr. 57 – Přidání firewallového pravidla (zdroj: vlastní zpracování)



Obr. 58 – Přehled firewallových pravidel (zdroj: vlastní zpracování)

Pro ověření je nyní možné zkusit přistoupit k SSH, nebo webovému rozhraní IoT brány z povoleného počítače – to se úspěšně podařilo. To samé není možné z jiného počítače – nastavení tedy funguje.

6 Shrnutí výsledků

V průběhu práce bylo získáno velké množství informací o manipulaci s technologiemi IoT. Na tomto základě bylo navrženo a následně fyzicky provedeno úspěšné zapojení do funkční infrastruktury počítačové sítě a to za pomoci jedné z doporučených IoT bran, které pro tyto účely slouží. Přesněji šlo o mikropočítač Raspberry Pi s modulem KON-RASP-01. Ta umožňuje propojit IQRF technologii s lokální sítí a Internetem. K jejímu použití byla potřeba nastavit IQRF zařízení, jako koordinátor a nody. K použití Raspberry Pi jako IQRF brána bylo nutné nainstalovat systém Raspbian, povolit SPI rozhraní, implementovat MQTT protokol, nainstalovat IQRF daemona, IQRF Gateway Daemon webovou aplikaci a následně Node-RED rozhraní pro možnost programování nodů a koordinátoru. Hardwarový modul postavený na Raspberry Pi se dal velice snadno nastavit. Přes Node-RED webové rozhraní se také dala velice snadno programovat funkce IQRF nodů.

IQRF brána byla připojena společně s dalšími prvky do MikroTik routeru, přes který bylo nutné daná zařízení zabezpečit. K tomu byly použity firewall pravidla s filtrováním pomocí IP a MAC adres. To povolilo přístup k IoT bráně pouze povolenému počítači s povolenou IP a MAC adresou. Tento počítač mohl z IQRF senzorů získat data a zařízení spravovat. Po změně IP adresy povoleného počítače již přístup k bráně možný nebyl. Stejně tak jiná zařízení přístup k bráně nemají, jelikož nemají povolenou IP a MAC adresu. Ve filtrovacím pravidle se navíc ukázal záznam o využití filtrovacího pravidla. Po vypnutí filtrovacích pravidel bylo možné přistoupit k datům (například k webovému rozhraní) přes všechna zařízení připojena ke stejné síti, a dokonce i přes mobilní zařízení připojené k Wi-Fi.

7 Závěry a doporučení

Při práci bylo zjištěno, že připojit IoT zařízení do již funkční a zavedené infrastruktury podniku s jednoduchou topologií není, při dodržení bezpečnostních zásad, složité. Postačuje využít dostupných technologií a jednu z doporučených bran pro dané IoT. V této práci k tomu byl využitý Mikrotik RouteBoard a brána Raspberry Pi s adaptérem KON-RASP-01, která tvořila rozhraní mezi sítí a IQRF zařízením. Jednotlivé IoT prvky si ale předávají mnohdy citlivá data, která by neměla padnout do nesprávných rukou. Nejdůležitější částí integrace IoT do infrastruktury podniku je proto fyzické zabezpečení těchto zařízení a přenosu jejich dat. Podnikové sítě mají běžně ustanovenu bezpečnostní politiku, tedy, integrace IoT by měla proběhnout i na této úrovni.

Bylo očekáváno, že bude velice snadné zapojit a provozovat IoT zařízení. Autor si zpočátku nebyl vědom nutnosti důrazu na zabezpečení, a tedy i možných způsobů. Bylo očekáváno, že stačí pouze zařízení opatřit heslem a více není potřeba řešit. Nicméně při hlubším zkoumání bylo zjištěno, že data šířící se po síti jdou poměrně snadno zachytit a hesla jsou prolomitelná. Následně proto byla přijata opatření pro maximální omezení nepovolaného přístupu k službám poskytovaným v rámci IoT síťového segmentu. K tomu bylo použito pouze výchozí bezpečnostní nastavení, které nemusí mít dostatečnou sílu. Útočník by se mohl například pokusit nastavit na svém počítači povolenou IP a MAC adresu. Musel by ale vyvinout dostatečné úsilí na jejich získání, což nemusí být v slabě zabezpečené síti složitý úkol, a proto je kladen důraz na zabezpečení infrastrukturních prvků.

Pro dokonalejší zabezpečení je možné použít Next-generation firewall (NGFW), který výrazně rozšiřuje funkci tradičního firewallu. Dále je možné síťovou komunikaci šifrovat a požadovat autentifikaci například použitím protokolu IPSec, SSL nebo s využitím IEEE 802.1X. To zamezí možnosti odposlouchávání a zachytávání komunikace mezi počítači nějakým jiným zařízením umístěným v dané síti. Již samotný IQRF bezdrátový přenos může být šifrován a zabezpečen heslem, což je součástí použité technologie a trendem vývoje IoT v poslední době. Přesto stále existují zařízení, která integrované prvky ochrany nemají a je třeba je řešit na vyšší vrstvě.

8 Seznam použité literatury

[1] HORÁK, Michal. *Aktivní prvky sítí – princip switche, hubu | Bubeníkova Komnata* [online]. jaro 2009 [vid. 2019-04-17]. Dostupné z: http://www.buben.piranhacz.cz/aktivni-prvky-siti-princip-switche-hubu/

[2] MOUAQIP. *Repeater-schema.svg* [online]. 23. únor 2011 [vid. 2019-04-18]. Dostupné z: https://commons.wikimedia.org/wiki/File:Repeater-schema.svg

[3] UNIVERSITY, Geek. *How hub works* [online]. 2019. Dostupné z: https://geek-university.com/ccna/what-is-a-network-hub/

[4] UNIVERSITY, Geek. *Differences between a switch and a bridge | CCNA* [online]. [vid. 2019-04-18]. Dostupné z: https://geek-university.com/ccna/differences-between-a-switch-and-a-bridge/

[5] UNIVERZITY, Geek. What is a network bridge? | CCNA. *Geek University* [online]. [vid. 2019-04-17]. Dostupné z: https://geek-university.com/ccna/what-is-a-network-bridge/

[6] UNIVERSITY, Geek. *What is a router? | CCNA* [online]. [vid. 2019-04-18]. Dostupné z: https://geek-university.com/ccna/what-is-a-router/

[7] *CCNA: Network Media Types > Twisted-Pair Cable* [online]. 14. březen 2003 [vid. 2019-04-17]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=31276

[8] *What does UTP, S/UTP, FTP, STP and SFTP mean?* [online]. [vid. 2019-04-17]. Dostupné z: https://www.universalnetworks.co.uk/faq/copper/what-does-utp-ftp-stp-or-sftp-mean

[9] BARAN, Ivo. *twisted pair utp cable* [online]. 22. říjen 2007 [vid. 2019-04-18]. Dostupné z: https://commons.wikimedia.org/wiki/File:UTP_cable.jpg

[10] WIKI, Ru. *S/FTP CAT 7* [online]. 20. duben 2011 [vid. 2019-04-18]. Dostupné z: https://commons.wikimedia.org/wiki/File:S-FTP_CAT_7.jpg

[11] VAN DER BURGT, Martin J. *Coaxial Cables and Applications* [online]. 2003 [vid. 2019-04-17]. Dostupné z: https://studylib.net/doc/8831583/coaxial-cables-and-applications

[12] APOLKHANOV. *English: Photo of RG-6 Coaxial cable* [online]. 5. leden 2014 [vid. 2019-04-18]. Dostupné z: https://commons.wikimedia.org/wiki/File:RG-6_coaxial_cable.png

[13] What is an Optical Fiber Cable? - Definition from Techopedia. *Techopedia.com* [online]. [vid. 2019-04-17]. Dostupné z: https://www.techopedia.com/definition/24918/optical-fiber-cable

[14] FREEBIE.PHOTOGRAPHY. *Free Stock Photo 11105 Fiber Optical Cable Isolated on White Background | freeimageslive* [online]. [vid. 2019-04-17]. Dostupné z: https://www.freeimageslive.co.uk/free_stock_image/fibre-optic-cable-jpg

[15] Microwave Technology. *CableFree* [online]. [vid. 2019-04-17]. Dostupné z: https://www.cablefree.net/wirelesstechnology/microwave/

[16] PIPERKOV, Lyuben. *Radioreléový spoj* [online]. 9. červen 2010 [vid. 2019-04-18]. Dostupné z: https://commons.wikimedia.org/wiki/File:Alcoma.bg_Radio_relay_link.jpg

[17] MARTINDALE, Jon. Wi-Fi helps connect all of our devices at high-speed, but what exactly is it? *Digital Trends* [online]. 16. únor 2019 [vid. 2019-04-17]. Dostupné z: https://www.digitaltrends.com/computing/what-is-wi-fi/

[18] Data Cabling FAQs | Data Cabling Q&As |Network Data Cabling FAQs. *Cabling Solutions* [online]. [vid. 2019-04-17]. Dostupné z: https://www.nmcabling.co.uk/data-cabling/data-cabling-faqs/

[19] FALES, Alexandr. Struktur. kabeláž horizontální a vertikální. In: [online]. B.m. [vid. 2019-04-17]. Dostupné z: https://docplayer.cz/6906580-Struktur-kabelaz-horizontalni-a-vertikalni.html

[20] BEAL, Vangie. *What is Cat-5e? Webopedia Definition* [online]. [vid. 2019-04-17]. Dostupné z: https://www.webopedia.com/TERM/C/Cat_5e.html

[21] FIREFOLD. Cat5 vs Cat6 Cables: What are the Differences? *FireFold* [online]. [vid. 2019-04-17]. Dostupné z: https://www.firefold.com/blogs/news/cat5-vs-cat6-cables-what-are-the-differences

[22] PALATINUS, Lukáš. *Topologie sítí | Blog.Banan.cz* [online]. 24. únor 2014 [vid. 2019-04-17]. Dostupné z: http://blog.banan.cz/Internet/Topologie-siti

[23] ZVONÍČEK, Josef. *Topologie sítí* [online]. [vid. 2019-04-17]. Dostupné z: http://pepa.zvonicek.info/inf/topologie.html

[24] LIBICH, Tomáš. Topologie firemní sítě. *Blog Tom Atom* [online]. 4. červen 2017 [vid. 2019-04-17]. Dostupné z: https://www.tomatom.cz/blog/topologie-firemni-site

[25] MCCLELLAND, Calum. What Is IoT? - A Simple Explanation of the Internet of Things. *IoT For All* [online]. 6. leden 2019 [vid. 2019-04-17]. Dostupné z: https://www.leverege.com/blogpost/what-is-iot-simple-explanation

[26] *Internet věcí - Vodafone.cz* [online]. [vid. 2019-04-17]. Dostupné z: https://www.vodafone.cz/firmy-a-korporace/internet-veci/

[27] ABU-ELKHEIR, Mervat, Mohammad HAYAJNEH a Najah Abu ALI. Data Management for the Internet of Things: Design Primitives and Solution. *Sensors*

(Basel, Switzerland) [online]. 2013, **13**(11), 15582–15612 [vid. 2019-04-18]. ISSN 1424-8220. Dostupné z: doi:10.3390/s131115582

[28] Co dokáže IIoT? *Vše o průmyslu* [online]. 28. září 2018 [vid. 2019-04-18]. Dostupné z: https://www.vseoprumyslu.cz/digitalizace/prumyslovy-internet-veci/co-dokaze-iiot.html

[29] What is Cloud Computing? - Amazon Web Services. *Amazon Web Services, Inc.* [online]. [vid. 2019-04-18]. Dostupné z: https://aws.amazon.com/what-is-cloud-computing/

[30] Co je IoT? *IoT portál* [online]. 27. červenec 2017 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/co-je-iot/

[31] REDAKCE. Kyberfyzikální systémy. *IoT portál* [online]. 22. srpen 2016 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/2016/08/22/kyberfyzikalni-systemy/

[32] *About LoRaWAN™ | LoRa Alliance™* [online]. [vid. 2019-04-18]. Dostupné z: https://lora-alliance.org/about-lorawan

[33] REDAKCE. LoRaWAN. *IoT portál* [online]. 29. únor 2016 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/2016/02/29/lorawan/

[34] REDAKCE. NarrowBand IoT. *IoT portál* [online]. 30. duben 2016 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/2016/04/30/narrowband-iot/

[35] IQRF About - IQRF. *About IQRF* [online]. [vid. 2019-04-18]. Dostupné z: https://www.iqrf.org/iqrfabout

[36] *Technology - IQRF* [online]. [vid. 2019-04-18]. Dostupné z: https://www.iqrf.org/technology

[37] REDAKCE. IQRF. *IoT portál* [online]. 27. listopad 2017 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/2017/11/27/iqrf/

[38] *Gateways* [online]. [vid. 2019-04-18]. Dostupné z: https://www.iqrf.org/products/gateways

[39] *Co je to firewall?* [online]. [vid. 2019-04-18]. Dostupné z: https://www.eset.com/cz/firewall/

[40] GEIER, Eric. 8 ways to improve wired network security. *Network World* [online]. 17. březen 2014 [vid. 2019-04-18]. Dostupné z: https://www.networkworld.com/article/2175048/8-ways-to-improve-wired-network-security.html

[41] *O Wi-Fi | Kybernetická bezpečnost SSPŠ* [online]. [vid. 2019-04-18]. Dostupné z: http://bezpecnost.ssps.cz/articles/detail/8

[42] BUDAI, David. *Nejčastější způsoby, kterými útočníci překonávají zabezpečení IT infrastruktury – ITBIZ – Vaše jednička mezi nulami* [online]. 17. listopad 2008 [vid. 2019-04-18]. Dostupné z: https://www.itbiz.cz/nejcastejsi-zpusoby-utoku-hackeru

[43] ŠKORNIČKOVÁ, Eva. Co je GDPR? *GDPR.cz* [online]. [vid. 2019-04-18]. Dostupné z: https://www.gdpr.cz/gdpr/

[44] ŠKORNIČKOVÁ, Eva. Jaká práva dává GDPR nám jako občanům. *GDPR.cz* [online]. [vid. 2019-04-18]. Dostupné z: https://www.gdpr.cz/gdpr/prava/

[45] REDAKCE. MQTT. *IoT portál* [online]. 24. květen 2016 [vid. 2019-04-18]. Dostupné z: https://www.iot-portal.cz/2016/05/24/mqtt/

[46] LIGHT, Roger. mqtt. *mosquitto.org* [online]. [vid. 2019-04-18]. Dostupné z: https://mosquitto.org/man/mqtt-7.html

[47] *Node-RED | Unipi* [online]. [vid. 2019-04-18]. Dostupné z: https://www.unipi.technology/cs/produkty/node-red-66

[48] SPURNÁ, Ivona. Bezdrátová inovace pro malá data jménem IQRF. *Root.cz* [online]. [vid. 2019-04-18]. Dostupné z: https://www.root.cz/clanky/bezdratova-inovace-pro-mala-data-jmenem-iqrf/

[49] *TR-72D RF Transceiver Module Series Data Sheet* [online]. 2018 [vid. 2019-04-18]. Dostupné z: https://iqrf.org/weben/downloads.php?id=337

[50] Download Raspbian for Raspberry Pi. *Raspberry Pi* [online]. [vid. 2019-04-18]. Dostupné z: https://www.raspberrypi.org/downloads/raspbian/

[51] ŠTRAUCH, Adam. Mikrotik: seznámení s Wi-Fi krabičkou. *Root.cz* [online]. 7. listopad 2008 [vid. 2019-04-18]. Dostupné z: https://www.root.cz/clanky/mikrotik-seznameni-s-wi-fi-krabickou/

[52] *Mikrotik RouterOS - About RouterOS* [online]. [vid. 2019-04-18]. Dostupné z: http://www.mikrotik-routeros.net/routeros.aspx

[53] SPINAR, Rostislav. install/rpi-board/GW-SbS-INSTALL.md · master · IQRF Alliance / IoT Starter kit. *GitLab* [online]. [vid. 2019-04-18]. Dostupné z: https://gitlab.iqrf.org/alliance/iot-starter-kit/blob/master/install/rpi-board/GW-SbS-INSTALL.md

[54] XECDESIGN. *NOOBS v2.2* [online]. 2. březen 2017 [vid. 2019-04-18]. Dostupné z: https://github.com/raspberrypi/documentation

[55] root_sudo [Ubuntu Česká republika]. *Root sudo - Ubuntu Wiki* [online]. 25. únor 2019 [vid. 2019-04-18]. Dostupné z: https://wiki.ubuntu.cz/root_sudo#myln%C3%A9_p%C5%99edstavy

[56] IQRF GW Daemon. *iqrf* [online]. [vid. 2019-04-18]. Dostupné z: https://www.iqrf.org/technology/iqrf-gw-daemon

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Střihavka Jakub	Arnultovice 106, Rudník - Arnultovice	I1600611

TÉMA ČESKY:

Integrace IoT do infrastruktury podniku

TÉMA ANGLICKY:

IoT integration into enterprise infrastructure

VEDOUCÍ PRÁCE:

Ing. Pavel Blažek - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem diplomové práce je prostudování typických firemních topologií počítačových sítí, jejich popis a následný návrh integrace IoT technologií s ohledem na jejich specifičnost.

SEZNAM DOPORUČENÉ LITERATURY:

1, Wireless network design : optimization models and solution procedures, Jeff Kennington, Eli Olinick, Dinesh Rajan. New York : Springer, (2011). ISBN 978-1-4419-6110-5 2, Designing for Cisco internetwork solutions (DESIGN), Diane Teare.Cisco Press, 2008. ISBN 978-1-58705-272-9 3, Mistrovství - počítačové sítě, Barrie Sosinsky. Computer Press, 2010. ISBN 978-80-251-3363-7 4, Možnosti a nebezpečenstvá internetovej komunikácie = Possibilities and dangers of internet kommunication, Eva Poláková, Alternativní metody výuky, Hradec Králové: Gaudeamus, 2009. 7. ročník mezinárodní konference Alternativní metody výuky 2009. 5, Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems, Eric Knapp, Joel Thomas Langill. Syngress, (2015), ISBN 978-0-12-420114-9

Podpis studenta: ..... **Datum:** 28.2.18

Podpis vedoucího práce: ..... **Datum:** 28.2.18