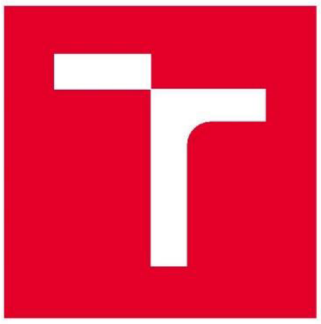


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH LOKÁLNÍCH BEZDRÁTOVÝCH SÍTÍ
WIRELESS LOCAL AREA NETWORK DESIGN

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Marek Šenkyřík

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. Jaroslav Koton, Ph.D.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Marek Šenkyřík ***ID:*** 177378
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Návrh lokálních bezdrátových sítí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou lokálních bezdrátových sítí určených pro pokrytí jak vnitřních tak vnějších prostor v definovaném perimetru. V souladu se stávající legislativou pak diskutujte podmínky nastavení a provozování takových sítí, a také pak jejich správu. Na reálných příkladech ukažte kroky návrhu funkční bezdrátové sítě provozované uvnitř budov a ve volném prostoru.

DOPORUČENÁ LITERATURA:

[1] Z. Long, X. Song, L. Zhang, Y. Xiao: Design and Implementation of Wireless Local Area Network Videophone, Advances in Intelligent and Soft Computing, vol 133. Springer, Berlin, Heidelberg, 2012, ISBN: 978-3-642-27-51-7.

[2] Campus LAN and Wireless LAN Design Guide, Cisco Validated Design [online], 2016, [cit: 2017-10-01] Dostupné z:
www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-Campus-LAN-WLAN-Design-2016OCT.pdf

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 29.5.2018

Vedoucí práce: doc. Ing. Jaroslav Koton, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato práce seznamuje s tématem bezdrátových lokálních sítí a jejich realizací. Úvod teoretické části se věnuje fyzikálnímu principu elektromagnetické vlny a přenosu vlny volným prostorem, dále otázce legislativy a omezení výkonu. Následně je v práci rozebrán princip a využití WLAN sítí. Jako příklad WLAN sítí je zrealizovaná síť pro pokrytí budov a jejího okolí. Druhý scénář sítě rozebírá vzdálenější spoje, jak páteřní, tak i koncové.

KLÍČOVÁ SLOVA

Bezdrátové lokální sítě, elektromagnetická vlna, WLAN sítě, legislativa bezdrátových sítí, PTP spoj, PTMP spoj, IEEE802.11

ABSTRACT

This work explores the topic of wireless local networks and their implementation. The introduction of the theoretical part is dedicated to physical principle of electromagnetic wave, air wave transfer, legislation of wireless networks and transmit power limitations and regulations. The thesis also presents WLAN networks functionality and their application. The practical part of the thesis contains the WLAN network for covering buildings and their surroundings. The second network scenario for remote connections, both backbone and endpoints.

KEYWORDS

Wireless local networks, electromagnetic waves, WLAN networks, legislation of wireless networks, PTP connection, PTMP connection, IEEE802.11

ŠENKYŘÍK, M. *Návrh lokálních bezdrátových sítí.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 65 s. Vedoucí bakalářské práce doc. Ing. Jaroslav Koton, Ph.D..

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Návrh lokálních bezdrátových sítí“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následku porušení ustanovení § 11 a následujících autorského zákona c. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonu (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce doc. Ing. Jaroslavu Kotonovi, Ph.D. za metodickou, pedagogickou a odbornou pomoc při zpracovávání. Dále děkuji za podporu ve firmě Brnet.cz v získávání nejen praktických znalostí v oboru bezdrátových telekomunikacích a přístupu k technologiím. Děkuji také přítelkyni Mgr. Lucii Novákové za kontrolu textu, trpělivost a projevenou podporu při tvorbě bakalářské práce. Poděkování patří též lidem v mém okolí, rodině, a především Bohu za podporu nejen v dosavadním studiu, ale i v budoucím.

V Brně dne ....

podpis autora

OBSAH

OBSAH **5**
SEZNAM OBRÁZKŮ **7**
SEZNAM TABULEK **9**
ÚVOD **10**
1 TEORETICKÁ ČÁST **11**
1.1 ELEKTROMAGNETICKÁ VLNA 11
1.1.1 Popis EM vlny 11
1.1.2 Rychlost EM vln 12
1.1.3 Spektrum EM vln 12
1.1.4 Vliv prostředí na šíření EM vlny 13
1.1.5 Fresnelova zóna 13
1.1.6 Digitální modulace 15
1.2 STANDARDY 17
1.3 LEGISLATIVA 19
1.3.1 DFS 20
1.4 VÝKON A LEGISLATIVA 20
1.5 TYPY ANTÉN 21
1.6 TECHNOLOGIE MIMO 21
2 BEZDRÁTOVÉ SÍTĚ WLAN **23**
2.1 IP ADRESACE 23
2.2 SMĚROVAČE A SMĚROVÁNÍ IP 24
2.3 FIREWALL 24
2.4 NAT – NETWORK ADDRESS TRANSLATION 25
2.5 DHCP – DYNAMIC HOST CONFIGURATION PROTOCOL 25
2.6 DNS 26
2.7 ZABEZPEČENÍ WI-FI 26
2.7.1 Hide SSID 27
2.7.2 MAC address filter 27
2.8 NSTREME A NV2 27
2.9 ROAMING 27
2.10 TEORETICKÝ ROZBOR NÁVRHU WI-FI SÍTĚ 28
3 REALIZACE BEZDRÁTOVÉ SÍTĚ WI-FI V OBJEKTU SOKOLOVNY **30**
3.1 ANALÝZA ZADÁNÍ A SITUACE 30
3.2 VÝPOČET PŘÍVODNÍ LINKY DO SOKOLOVNY. 31
3.3 TEORETICKÝ NÁVRH 31
3.3.1 Konfigurace sítě 32
3.3.2 Zařízení objektu sokolovny 34
3.3.3 Zařízení přívodu a rozvodny 34
3.4 KONFIGURACE SÍTĚ 35
3.4.1 Konfigurace bezdrátového a síťového rozhraní 35

3.4.2 Konfigurace Wi-Fi sítí ... 36
3.4.3 Konfigurace PTP spoje ... 36
3.5 SESTAVENÍ SÍTĚ ... 37
3.6 MĚŘENÍ PARAMETRŮ REALIZOVANÉ SÍTĚ ... 37
3.6.1 Síť sokolovny ... 37
3.6.2 Síť rozvodny ... 40
4 REALIZACE VENKOVNÍ WI-FI SÍTĚ ... 41
4.1 TEORETICKÝ POPIS A NÁVRH ... 41
4.1.1 Síťová topologie a konfigurace ... 41
4.2 HLAVNÍ ROUTER – MT-MAINROUTER ... 43
4.2.1 Popis zařízení ... 43
4.2.2 Konfigurace ... 43
4.2.3 Umístění Rack – Šumavská Tower – A ... 45
4.3 PTP SPOJ METROLINQ IGNITE ... 46
4.3.1 Popis zařízení ... 46
4.3.2 Montáž a zaměření spoje ... 47
4.3.3 Umístění Rack – Hotel Continental ... 49
4.3.4 Konfigurace PTP spoje Metrolinq Ignite ... 49
4.3.5 Parametry sestaveného spojení ... 52
4.3.6 Měření parametrů ... 53
4.3.7 Diskutabilní 802.11ad ... 54
4.4 PTMP SPOJ MIKROTIK ... 54
4.4.1 Popis zařízení ... 55
4.4.2 Konfigurace síťového rozhraní ... 55
4.4.3 Konfigurace bezdrátového rozhraní ... 55
4.4.4 Sestavení spojení ... 56
4.4.5 Měření ... 57
5 ZÁVĚR ... 59
LITERATURA ... 60
SEZNAM POUŽITÝCH ZKRATEK, VELIČIN A SYMBOLŮ ... 63
SEZNAM PŘÍLOH ... 64
PŘÍLOHA Č.1 – SEZNAM MASEK SÍTĚ ... 65

SEZNAM OBRÁZKŮ

Obr. 1.1: Obecný přenosový kanál EM vlny. 11
Obr. 1.2: EM vlna [16] 12
Obr. 1.3: Elektromagnetické spektrum [17] 13
Obr. 1.4: Fresnelova zóna [19] 14
Obr. 1.5: QAM zobrazení, reálná osa - fáze, imaginární osa - amplituda [20] 16
Obr. 1.6: BPSK [21] 16
Obr. 1.7: QAM - IQ diagram [22] 17
Obr. 1.8: Pásmo 2,4 GHz [25] 18
Obr. 1.9: Pásmo 5 GHz 19
Obr. 1.10: MIMO [29] 22
Obr. 3.1: Půdorys areálu s objektem, včetně vyznačených prostor pro pokrytí signálem 30
Obr. 3.2: Rozvržení AP pro pokrytí požadovaných oblastí objektu 32
Obr. 3.3: Topologie celé sítě objektu, včetně připojení sítě do sítě poskytovatele k síti Internet 33
Obr. 3.4: Rack v objektu se switchem a napájením 37
Obr. 3.5: Měření úrovně signálu v objektu a areálu pomocí Wi-Fi Visualizer 38
Obr. 3.6: Měření úrovně signálu v objektu a v areálu pomocí Ekahau Heatmapper 39
Obr. 4.1: Mapa realizovaného spojení mezi budovami A – Šumavská, B – Hotel, C – Veveří 41
Obr. 4.2: Topologie venkovní Wi-Fi sítě, včetně IP adresace 42
Obr. 4.3: Načtení konfigurace DHCP klienta 44
Obr. 4.4: IP adresy hlavního routeru definované pro interface bridge1 a ethernet9 44
Obr. 4.5: Routovací tabulka hlavního routeru 44
Obr. 4.6: Firewall a definovaná pravidla NATu 45
Obr. 4.7: Konfigurace uživatele pro přístup do administrace 45
Obr. 4.8: Konfigurace názvu hlavního routeru 45
Obr. 4.9: Rack telekomunikačního operátora, Šumavská Tower – A 46
Obr. 4.10: Jednotka PTP spoje Metrolinq Ignite umístěna na budově A Šumavská se zaměřovacím dalekohledem 46
Obr. 4.11: Doladění pomocí dalekohledu – anténa Master 48
Obr. 4.12: Doladění rádia na straně Hotelu pomocí Aiming tool 48
Obr. 4.13: Jemné doladění rádia s vyznačenými šrouby 49

Obr. 4.14: Rack telekomunikačního operátora na budově B – Hotel Kontinental 49
Obr. 4.15: Konfigurace jednotky 50
Obr. 4.16: Nastavení bezdrátové části rádia Metrolinq Ignite 52
Obr. 4.17: Parametry 60GHz spojení ze strany rádia klient na budově A 53
Obr. 4.18: Topologie sítě PTMP spoje v pásmu 5 GHz s IP adresací 55
Obr. 4.19: Konfigurace bezdrátového rozhraní klientské strany 56
Obr. 4.20: Sken ostatních sítí při výběru vysílacího kanálu 56
Obr. 4.21: Parametry sestaveného spojení PTMP spoje, strana bridge 57
Obr. 4.22: Parametry sestaveného spojení PTMP spoje, strana routeru 57

SEZNAM TABULEK

Tab 1.1: Fresnelova zóna [12] 14
Tab 1.2: Přehled IEEE standardů pro Wi-Fi [5] [25] 17
Tab 1.3: Porovnání 802.11ac a 802.11n [27] 19
Tab 3.1: Počet návštěvníků objektu a teoretický počet připojených návštěvníků k síti 31
Tab 3.2: Kontrola přenosové rychlostí omezená routerem a kontrolérem 39
Tab 4.1: Volitelné možnosti MCS Rate 51
Tab 4.2: Volitelné možnosti výkonu 52
Tab 4.3: Úroveň RSSI při změně kanálu 53
Tab 4.4: Měření úrovně RSSI, MCS a rychlostí při snižování výkonu na obou stranách spoje 54
Tab 4.5: Měření reálné přenosové rychlosti v málo rušeném kanále, bridge CCQ 89/90 %, router CCQ 85/89 % 57
Tab 4.6: Měření reálné přenosové rychlosti v rušeném kanále, bridge CCQ 29/20 %, router CCQ 35/22 % 58
Tab 4.7: Měření reálné přenosové rychlosti v rušeném kanále a vlivu Nv2 a Nstreme, bridge CCQ 25/9 %, router CCQ 28/14 % 58

ÚVOD

Bezdrátové sítě jsou nyní součástí každodenního života člověka, který jde s moderní dobou. Ještě před několika desítkami let byly jen snem a postupem času jsou naší nezbytnou součástí. Pod pojmem bezdrátové si můžeme představit mobilní služby, které se v průběhu času zdokonalují. Například zkratky GSM, UMTS, HSPDA, CDMA jsou nám známé a stále mají své místo ve světě, ale mnohdy převažují 3G, nebo 4G – LTE, popřípadě aktuálně značně diskutované téma v oboru bezdrátových sítí – IoT (Internet of Things). Pod pojem bezdrátové sítě dále můžeme zahrnout i televizní vysílání, satelitní anebo rádiové.

Práce se zabývá problematikou návrhu a realizace lokálních bezdrátových sítí, které slouží k připojení koncových klientů přenosných zařízení, domácností a také radiových spojů. V teoretické části je rozebrána stavba a přenos EM vlny, vlastnosti přicházející s přenosem vlny prostorem, prací s výkonem a frekvenčním pásmem, což jsou dva parametry důležité pro legislativu, a tudíž i pro legální provoz těchto sítí v České republice. Druhá kapitola se věnuje samotné síti WLAN, což značí propojení bezdrátových zařízení se síťovou infrastrukturou. Pro správné pochopení propojení těchto dvou částí je první podkapitola věnována spíše bezdrátové části a druhá podkapitola síťové infrastruktuře a způsobu přenosu dat a jejich zpracování.

V dalších kapitolách se práce zabývá realizací WLAN sít dle standartu IEEE802.11 (tj. Wi-Fi sítě) v objektu a mimo něj, s definováním parametrů bezdrátové sítě a síťovou konfigurací pro více skupin uživatelů s různým omezením rychlosti. Druhá část realizace se zabývá sítí složenou primárně ze spoje PTP v 60 GHz pásmu a PTMP v 5 GHz pásmu dle standartu IEEE802.11.

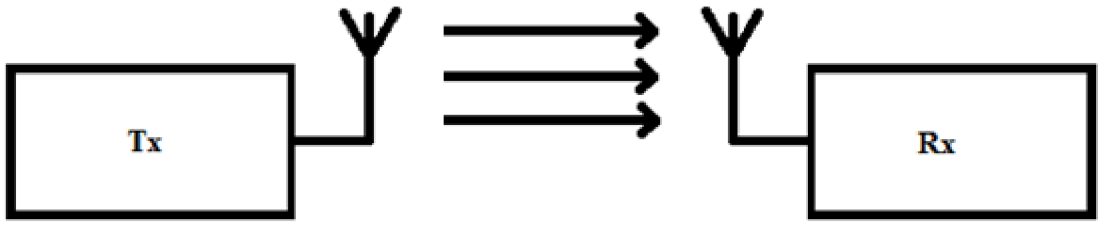
Jelikož pracuji pro menšího bezdrátového a optického poskytovatele internetu, jsou v práci uvedeny příklady, kterých se mi podařilo dosáhnout, popřípadě pro dokreslení informací s označením „Příklad z praxe“.

1 TEORETICKÁ ČÁST

1.1 Elektromagnetická vlna

S elektromagnetickou (dále jen EM) vlnou se setkáváme na každém kroku – rádiové vlny, mikrovlny, rentgenové záření, nebo i světlo. U přenášení radiového signálu řešíme tří základní vlastnosti: [12] [24]

- Antény – vysílací a přijímací, které mění EM vlnu šířící se prostorem na energii, která se dále šíří po vedení a opačně přeměnu energie z vedení na EM vlnu vyzařovanou do prostoru
- Vedení – způsob přenosu energie přijímané nebo vysílané mezi anténou a vysílačem či přijímačem
- Prostředí pro přenos – prostor mezi vysílačem (Tx) a přijímačem (Rx) [12]



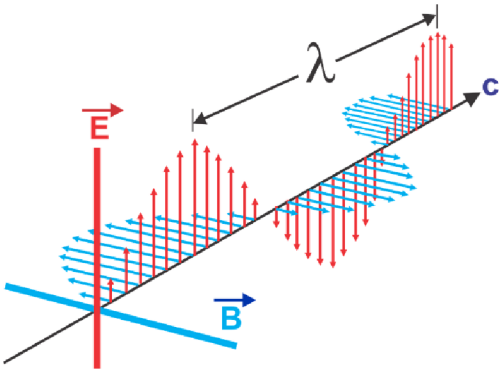
Obr. 1.1: Obecný přenosový kanál EM vlny.

U anténních systémů a přenosu Wi-Fi signálu je mnoho různých požadavků. Například pro přenos na velké vzdálenosti je žádoucí připojení bod – bod – tzv. PTP (Point To Point) a proto je nutné snížit úhel přenášeného záření. [5] [12] [24]

1.1.1 Popis EM vlny

U EM vln se zvětšuje a zmenšuje elektrické a magnetické pole, přičemž nekmitají, ani se nehýbají žádné další částice. Elektrické pole – vlnu elektrické intenzity E [$V.m^{-1}$] můžeme na obrázku 1.2 pozorovat jako červenou vlnu a magnetické pole – vlnu magnetické indukce B [T] jako modrou vlnu. Jedná se o zobrazení šíření vlny volným prostorem, kde vektory E a B kmitají ve stejné fázi a oba tvoří příčné vlnění. Ze směrů vektorů E, B a fázové rychlosti vf zjistíme, že soustava souřadnic je pravotočivá v každém okamžiku, kromě nulových bodů. Můžeme k tomu využít pravidlo pravé ruky, kdy použijeme tři prsty. Ukazováček ukazuje rovně, na který je palec kolmý a prostředníček zahneme a uděláme kolmici na předchozí dva prsty. Ukazováček nám představuje vektor E, prostředníček vektor B a palec vektor vf. Pokud palec a vektor vf

mají souhlasný směr, pak je tato soustava pravotočivá, pokud mají opačný směr, pak je levotočivá. [26]



Obr. 1.2: EM vlna [16]

1.1.2 Rychlost EM vln

Rychlost EM vlny je rovna ve vakuu rychlosti, kterou známe jako rychlost světla. Touto rychlostí se šíří všechny druhy elektromagnetických vln. Označujeme ji písmenem *c*. [26]

$$c = 299\,792\,458\ \mathrm{m} \cdot \mathrm{s}^{-1}, \tag{1.1}$$

kde *c* je rychlost světla.

Pro elektromagnetické vlnění platí závislost mezi frekvencí a vlnovou délkou [26]

$$c = \lambda f\ [\mathrm{m} \cdot \mathrm{s}^{-1}], \tag{1.2}$$

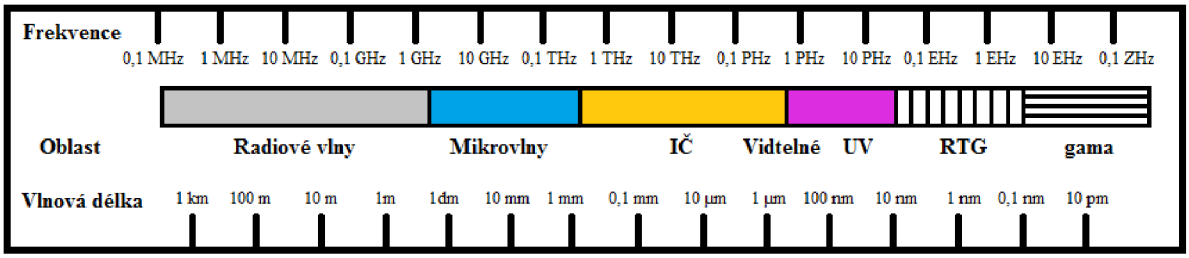
kde λ je vlnová délka a *f* je frekvence.

Známe-li alespoň jednu veličinu a jelikož rychlost světla *c* je konstanta, tak snadno můžeme dopočítat druhou veličinu. Mezi veličinami λ a f platí nepřímá úměra. Roste-li frekvence, klesá vlnová délka a naopak. [26]

1.1.3 Spektrum EM vln

Elektromagnetické vlny dělíme podle vlnové délky. Základní typy dělení můžeme vidět dále na obrázku, kde na vrchní ose máme vynesenou frekvenci *f* a na spodní vlnovou délku λ. [17]

K rádiovým vlnám můžeme přiřadit vlny o vlnové délce cca od 1 cm až po 1 km. Například televizní signál má vlnovou délku od 0,1 m po 1 m. Mobilní signál 16 cm nebo 33 cm. Rentgenovému záření RTG má vlnovou délku mezi 10 nm a 1 pm. [17]



Obr. 1.3: Elektromagnetické spektrum [17]

Pro mikrovlnný Wi-Fi signál používáme frekvence 2,4 GHz, 5 GHz a 60 GHz. Dle rovnice pro vztah rychlosti světla s frekvencí si můžeme dopočítat jednotlivé vlnové délky: [18]

$$\lambda = \frac{c}{f} = \frac{c}{2.4\ \text{GHz}} = 0{,}125\ \text{m} = 12{,}5\ \text{cm} \tag{1.3}$$

$$\lambda = \frac{c}{f} = \frac{c}{5\ \text{GHz}} = 0{,}06\ \text{m} = 6\ \text{cm} \tag{1.4}$$

$$\lambda = \frac{c}{f} = \frac{c}{60\ \text{GHz}} = 0{,}005\ \text{m} = 0{,}5\ \text{cm}\,, \tag{1.5}$$

Infračervené vlny s rozsahem mezi 1 mm a 770 nm můžeme přiřadit tělesům s vyšší teplotou, přičemž se zvyšování teploty stoupá i vlnová délka. Pomocí infračerveného záření můžeme sledovat teplejší předměty mezi studenějšími, například infračerveným dalekohledem, nebo kamerou založenými na změně spektra z neviditelné části na viditelné. Například lidské tělo má teplotu 310 K a viditelné záření můžeme pozorovat při teplotě cca od 900 K, například u kutí kovu. [17]

Samotný člověk dokáže vnímat jen velmi úzké spektrum (s porovnáním s ostatními na obrázku 1.3) od 390nm do 770nm, které je označeno jako viditelné spektrum od barvy červené po fialovou. Lidské oko je nejcitlivější na barvu žlutozelenou s vlnovou délkou cca 550nm. Vlnová délka 10^{-14} odpovídá gama záření, které vzniká rozpadem atomových jader. [17]

1.1.4 Vliv prostředí na šíření EM vlny

Vlivů na šíření EM vlny a její efektivní přenos v prostředí ovlivňuje mnoho faktorů a jevů, z kterých základní jsou: [18]

- **Absorbce signálu** – dochází ke snížení velikosti amplitudy vlny díky průchodu signálu skrze překážku, kterou mohou být například zdi, lidé, nebo koberce.
- **Odrazy signálu** – způsobující dělení signálu do více směrů a příchod signálu na přijímací anténu s časovým zpožděním, nebo s horší kvalitou (tzv. rozptyl signálu).
- **Frekvenční rušení** – jelikož kanálů ve frekvenčním spektru Wi-Fi pásem 2,4 a 5 GHz je méně, než je jejich využití, vznikají situace, kdy je více vysílacích zařízení na stejné frekvenci a vzájemně se ovlivňují. V potaz je potřeba vzít i sousední kanály, které do sebe zasahují. [18]

1.1.5 Fresnelova zóna

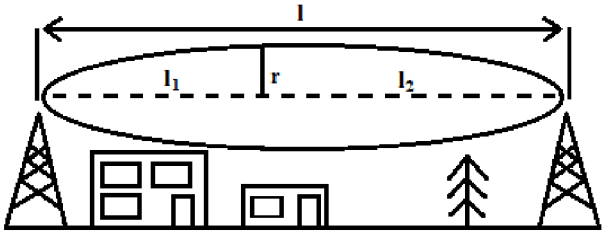
Fresnelova zóna je nezbytným pojmem v radiokomunikacích a je nutností mít o ní alespoň

minimální povědomí. Jedná se o prostor v tvaru elipsoidy v podélném řezu a kruhový tvar v příčném řezu, který se mění v celé délce. Fresnelova zóna je důležitým prvkem, protože prakticky uvnitř tohoto prostoru se odehrává celý přenos signálu. [12] [19]

Poloměr kruhu ve Fresnelově zóně můžeme spočítat vztahem: [12] [19]

$$r = 17{,}3\sqrt{\frac{l_1 l_2}{l_1 f_{\mathrm{GHz}}}}\ [\mathrm{m}], \tag{1.6}$$

kde $l = l_1 + l_2$ znační vzdálenost mezi stožáry, l_1 vzdálenost od první antény a l_2 vzdálenost od druhé antény.



Obr. 1.4: Fresnelova zóna [19]

Pro Fresnelovu zónu v praxi platí, že stačí zajistit průchodnost skrze 60 % prostoru pro minimalizování ztrát. V tabulce 1.1 jsou uvedené hodnoty velikosti Fresnelovy zóny pro Wi-Fi pásma 2,4 a 5 GHz. [12] [19]

Tab 1.1: Fresnelova zóna [12]

60 % rozsahu Fresnelovy zóny [m]		
Délka rádiového spojení [km]	2,4 GHz	5 GHz
0,1	1,1	0,7
0,2	1,5	1,0
0,5	2,4	1,6
1	3,4	2,3
2	4,7	3,3
3	5,8	4,0
4	6,7	4,6
5	7,5	5,2
6	8,2	5,7
7	8,9	6,1
8	9,5	6,6
9	10,1	7,0
10	10,6	7,3

Pokud uvažujeme vyšší vzdálenosti radiového spoje, musíme počítat i se zakřivením země. Například u 5 km roste výška překážek o 1 m a u 10 km o 4 m. [12] [19]

1.1.6 Digitální modulace

Při modulaci v radiokomunikacích dochází k ovlivňování 3 parametrů nosného signálu modulačním signálem – amplituda (ASK), kmitočet (FSK) a počáteční fáze (PSK). Modulačním signálem je digitální signál, který může nabývat pouze hodnot log.1 a log.0. Díky změně okamžité hodnoty digitálního signálu, se mění skokově i namodulovaná nosná vlna. [8] [10] [20]

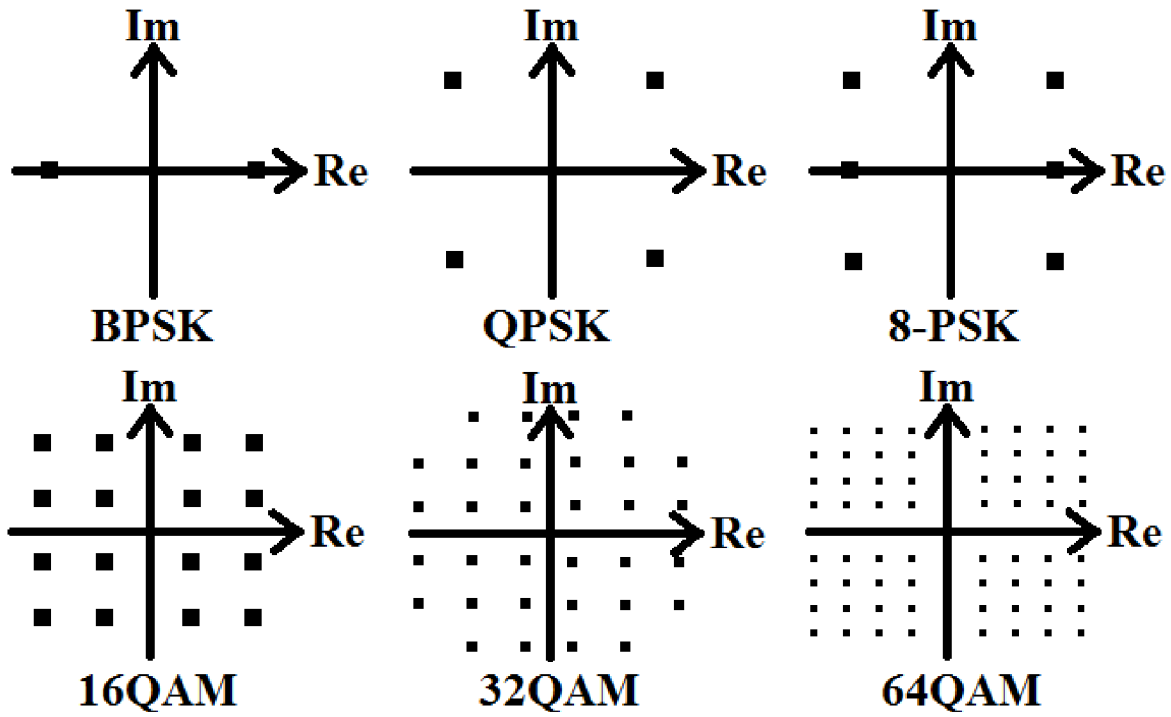
Modulace můžeme rozdělit na dvoustavové a vícestavové. U dvoustavových modulací je pro každý bit modulačního signálu přiřazen 1 stav nosné vlny – Symbol. Pro vícestavovou modulaci platí vztah: [8] [10]

$$M = 2^n\ [-], \tag{1.7}$$

kde M je počet stavů nosné a n je počet bitů.

Například M=4 – čtyřstavová modulace vyjadřuje každý stav nosné určitou dvojbitovou hodnotu n=2, kterou nazýváme dibit. U osmistavové modulace M=8 vyjadřujeme 3 bitovou hodnotu n=3 a dále. [8] [10] [20]

Graficky můžeme tyto stavy zobrazit ve stavovém diagramu se dvěma složkami, jako je na obrázku 1.6. *In-phase* – synfázní složka a *Quadrature* – kvadraturní složka, mezi kterými jsou zakresleny koncové body vektorů nacházející se pouze na kružnici, které značí velikost amplitudy nosné vlny. Toto zobrazení se též nazývá *IQ*. [8] [10] [20]

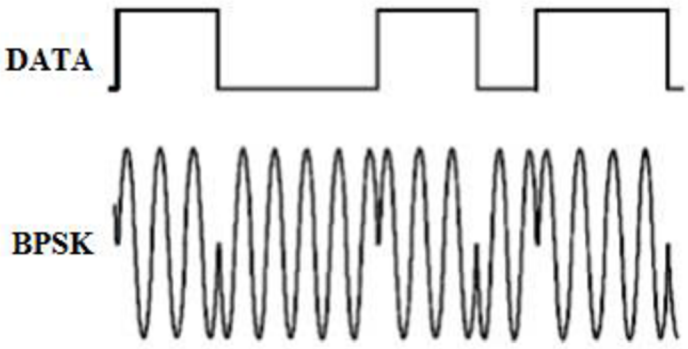


Obr. 1.5: QAM zobrazení, reálná osa – fáze, imaginární osa – amplituda [20]

Samostatné modulace ASK a FSK se ve Wi-Fi technologiích téměř nepoužívají. Využívají se hlavně modulace s označením BPSK – 2QAM, QPSK – 4QAM, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM a 256QAM. Můžeme se též setkat s vyššími modulacemi, často ale mimo standart 802.11. [8] [10] [20]

BPSK (Binary Phase Shift Keying)

Tzv. binární modulace s klíčováním fáze je základní modulací založená na posunutí fáze o 0° nebo 180° nosné vlny pro určení náběžné či sestupné hrany logické z digitálního modulačního signálu. [10] [21]



Obr. 1.6: BPSK [21]

QAM (Quadrature Amplitude Modulation)

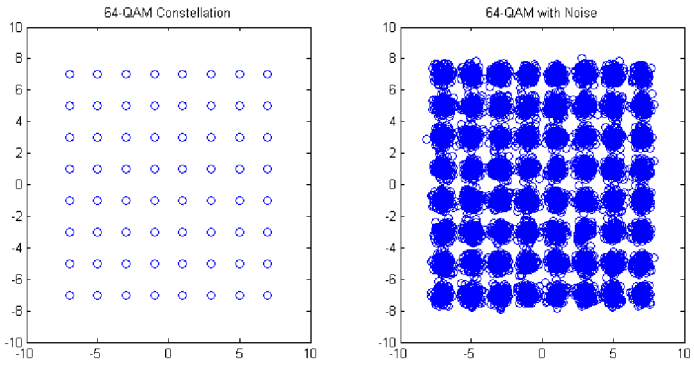
Pro ještě lepší výsledky diagramu *IQ* využíváme kvadraturní modulace QAM s funkcí nejen

klíčování počáteční fáze, ale i amplitudy nosné vlny. Na Obr. 1.5 jsou znázorněny stavové diagramy 16QAM, 32QAM a 64QAM modulace. Výhoda této modulace spočívá hlavně v efektivním využití frekvenčního pásma a navýšení přenosové rychlosti. Počet koncových bodů nám určuje počet stavů nosné a dle rovnice (1.7) můžeme spočítat počet možných přenesených bitů. Například pro označení 256QAM, které slouží jako vyjádření nosné, kde M=256 je výsledkem osmibitová kombinace n=8, tudíž vyšší přenosová rychlost. [] [9] *Webinář Alternetivo – vysokokapacitní wifi* [online]. 20.10.2015 [cit. 2018-05-29]. Dostupné z: https://youtu.be/1VBsKbaYo5g

[] []

Srovnáme-li dvě různé modulace, např. 256QAM a BPSK a je-li konstantní symbolová rychlost, tak je vícestavová modulace 256QAM 8x rychlejší než dvoustavová modulace BPSK. [8] [10] [22]

Jelikož v reálném prostředí působí na signál různá rušení a šum, tak pro vícestavové modulace jsou kladeny vyšší nároky na přijímač a jeho schopnost rozlišovat menší změny amplitudy, frekvence nebo fáze. Na obrázku 1.8 můžeme pozorovat příklad, jak se rušení projevuje na signálu s modulací 64QAM. S vyšší modulací automaticky přichází i nutnost náročnějšího zpracování signálu. [8] [10] [22]



Obr. 1.7: QAM – IQ diagram [22]

1.2 Standardy

Standardy IEEE802.11 (tj. Wi-Fi), byly definované pro určitá pásma. V Tab 1.2 je zobrazen výpis základních standardů. [5] [25]

Tab 1.2: Přehled IEEE standardů pro Wi-Fi [5] [25]

IEEE standart	rok	f. pásmo	t. propustnost	MIMO
802.11b	1999	2,4 GHz	11 Mb/s	-
802.11g	2002	2,4 GHz	54 Mb/s	-
802.11a	2002	5 GHz	54 Mb/s	-
802.11n	2007	2,4 (5)	600 Mb/s	MIMO
802.11ad	2011	60 GHz	7 Gb/s	-

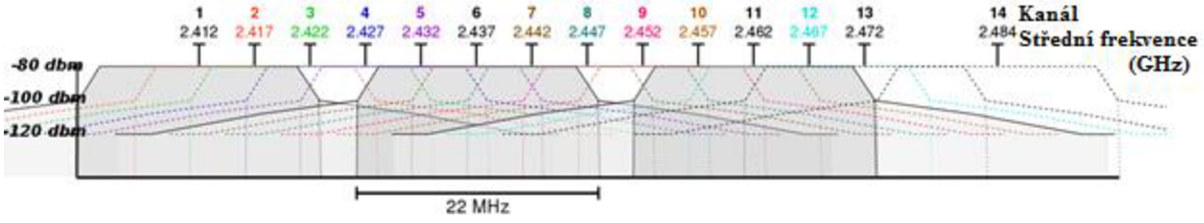
802.11ac	2012	5 GHz	1 Gb/s	MU-MIMO

Pásmo

V pásmu 2,4 GHz máme definovaných 11 až 14 kanálů, v závislosti na území. [5] [25]

- EU kanály 1-13
- US kanály 1-11
- JPN kanály 1-14

Odstup kanálů mezi dvěma nejbližšími je 5 MHz a šířka jednoho kanálu 20-22 MHz. Díky velké šířce kanálu a malému odstupu můžeme pozorovat vzájemné překrývání kanálů na obrázku 1.9, kde námi volený kanál ovlivňuje dva sousední na vyšším a nižším kmitočtu, tudíž 4 kanály. Existují tedy pouze 3 kanály, 1,6 a 11, které se vzájemně nepřekrývají a tím pádem nedochází k vzájemnému rušení tzv. mezikanálové interferenci. [5] [25]



Obr. 1.8: Pásmo 2,4 GHz [25]

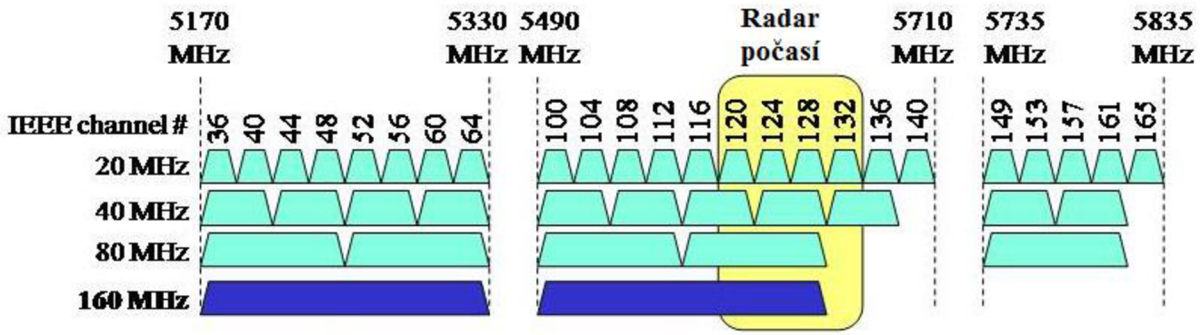
Příklad z praxe: V US, jsou definovány pouze kanály 1-11, díky čemuž jsou zde občas vyráběny zařízení bez podpory kanálů 12 a 13, které jsou povoleny v EU. Při dovozu zařízení z US mohou tedy nastat problémy s připojením k AP vysílajícím na kanálech 12 nebo 13. V takovém případě je jedinou cestou přenastavit vysílací AP na kanál nižší (podporovaný) a to v rozsahu 1-11. [5] [25]

Pásmo 2,4 GHz sdílejí i další služby a zařízení, které mohou narušit chod Wi-Fi. [5] [25]

- 2,402 až 2,480 GHz Bluetooth
- 2,4 GHz Bezdrátová sluchátka
- 2,45 GHz Mikrovlnná trouba

Tyto služby a zařízení mohou ovlivnit chod dat v pásmu 2,4 GHz. Například u bezdrátových sluchátek je problémem technologie „Clear“ pro ostrý zvuk, protože funguje jako širokopásmová rušička v pásmu 2,4 GHz. [5] [25]

V pásmu 5 GHz máme definovaných více kanálů než v pásmu 2,4 GHz a to 36-64, přičemž kanály 36-48 by mělo podporovat každé zařízení, ale není to pravidlem. V tomto pásmu jsme schopni využít MIMO. [5] [25]



Obr. 1.9: Pásmo 5 GHz [30]

802.11ac

Standart 802.11ac je určen pouze v 5 GHz pásmu kvůli vyžití více kanálů. V pásmu 2,4 je méně kanálů a standart ac by zde nemělo smysl uplatňovat. Standart 802.11ac funguje na slučování kanálů, přičemž se vejde méně těchto sloučených kanálů do spektra. Například 160 MHz kanál u standartu 802.11ac se do spektra vejdou dva. [27] [29]

Tab 1.3: Porovnání 802.11ac a 802.11n [27]

Počet streamů	Šířka kanálu [MHz]	802.11ac	802.11n
1	20	86,7 Mbps	72,3 Mbps
1	40	200 Mbps	150 Mbps
2	40	400 Mbps	300 Mbps
4	40	800 Mbps	600 Mbps
1	80	433 Mbps	N/A
2	80	867 Mbps	N/A
3	80	1,3 Gbps	N/A
4	80	1,69 Gbps	N/A
1	160	867 Mbps	N/A
4	160	3,39 Gbps	N/A
8	160	6,77 Gbps	N/A

1.3 Legislativa

Pro stanovení a dohled nad legislativou a dodržováním norem nejen bezdrátových sítí máme v České republice Český telekomunikační úřad. Tento úřad definoval kmitočty a podmínky jejich využívání ve všeobecných oprávněních. [2] [4] [5] [7]

Kmitočtové pásmo standard IEEE, 2,4 GHz a 5GHz je definováno v tabulkách všeobecném oprávnění č. VO-R/12/09.2010-12 z roku 2010 dostupné v literatuře. [2] [4] [5] [7]

Pásmo 2,4 GHz (2400 – 2483,5 Hz) je hojně využívané pásmo, nejen právě pro bezdrátový internet, ale i pro bluetooth, kamerové systémy, dálkové ovládání elektroniky, aj. [2] [4] [5] [7]

Oblast 5 GHz rozdělujeme na více částí:

- Pásmo 5,15 – 5,35 GHz – pouze pro vnitřní pokrytí budov
- Pásmo 5,47 – 5,725 GHz
- Pásmo 5,725 – 5,875 GHz – pouze s použitím malého výkonu 25mW (EIRP) [2] [4] [5] [7]

Dohledu státu nad elektronickými komunikacemi často docházejí stížnosti a udání a při kontrolách měřícími vozy narážejí na nedodržování zákonu 127/2005 Sb. o elektronických komunikacích. Kvůli zlepšení parametrů jako zvýšení signálu, nebo vyhnutí se rušení je častým problémem používání frekvenčních kanálů pro vnitřní pokrytí budov ve venkovním prostředí, nebo nedodržení velikosti vysílacího výkonu definovaného ve všeobecném oprávnění. [2] [4] [5] [7]

Výrobce zařízení pro bezdrátový přenos internetu je povinen v návodu sdělit podmínky pro použití zařízení v ČR ve shodě s všeobecným oprávněním a uživatel je povinen dle tohoto manuálu a opět v souladu s všeobecným oprávněním provozovat. Častým případem bývá použití zařízení určeného pro všesměrovou anténu s malým ziskem na směrovou s velkým ziskem, následně nezregulování, popřípadě automatického nastavení maximálního výkonu EIRP a tím nedodržení celkového vysílacího výkonu. [2] [4] [5] [7]

V pásmu 2,4 a 5 GHz se jedná o sdílená kmitočtová pásma a stanice nemají zajištěnou ochranu proti rušení jinou stanicí. Pokud dojde ke sporu dvou stran při využívání volně licencovaných pásem, spor se řeší nejprve dohodou. Pokud se strany nedohodnou, řeší se spor dle zákona § 100 o elektronických komunikacích, popřípadě uživatel, který spustil službu později ji zastavuje. [2] [4] [5] [7]

1.3.1 DFS

V České republice jsou dva meteorologické radary pracující v pásmu 5 GHz [4] [7]

- Brdy; pracující na frekvenci 5630 MHz
- Skalky; pracující na frekvenci 5645 MHz

Tyto radary v ČR dodávají data pro zajištění bezpečnosti civilnímu i vojenskému letectvu a dle regulací „Radio regulations“ vydanými „International Regulation Union“ ustanovující povinnost členským státům [4] [7]

Funkce DFS spočívá v zjišťování komunikace služby s vyšší prioritou. Pokud takováto komunikace bude zjištěna, tak automaticky přeladí AP na jiný kanál. [4] [7]

1.4 Výkon a legislativa

Pro dodržení maximálního výkonu stanoveným legislativou ve Wi-Fi pásmu je nutné

správně korigovat maximální vysílací výkon rádiové jednotky. V pásmu 2,4 GHz je výkon omezen na 100 mW (20 dBm) EIRP. V pásmu 5 GHz, kde 5150-5250 na 200 mW (23 dBm) EIRP, 5250-5350 na 100 mW (20 dBm) EIRP a 5470-5725 na 1 W (30 dBm) EIRP. V pásmu 60 GHz je omezení stanoveno na 10 W (40 dBm) EIRP. [2] [5]

EIRP je hodnota výkonu, která je vyzářena anténou. Prakticky je EIRP roven součtu vysílacího výkonu karty a zisku antény s odečtením ztrát, které se často zanedbávají. Nejdůležitější hodnotou pro nepřekročení maximálního výkonu definovaném legislativou je výkon EIRP. [2] [5]

1.5 Typy antén

Ve Wi-Fi pásmu je důležité se zaměřit na výběr antény, která je volena dle použití. V potaz bereme dva parametry, a to vzdálenost od koncových stanic a úhel pokrytí prostoru, dle kterého antény dělíme na: [5]

- **Směrové** – s velikostí vysílaného úhlu kolem 30° se ziskem i přes 25 dB, díky malému vyzařovacímu úhlu. Vhodnost použití u klientské stanice, nebo spoje PTP a další.
- **Sektorové** – s úhlem vysílání s úhlem vysílání od 45° až 120° se ziskem až kolem 22 dB. Použití na vykrytí určité oblasti.
- **Všesměrové** – s úhlem 360° a ziskem od jednotek dB po cca 20 dB v závislosti na výšce paprsku. Vhodnost použití pro domácí AP, nebo pokrytí menších lokalit s menším rušením. [5]

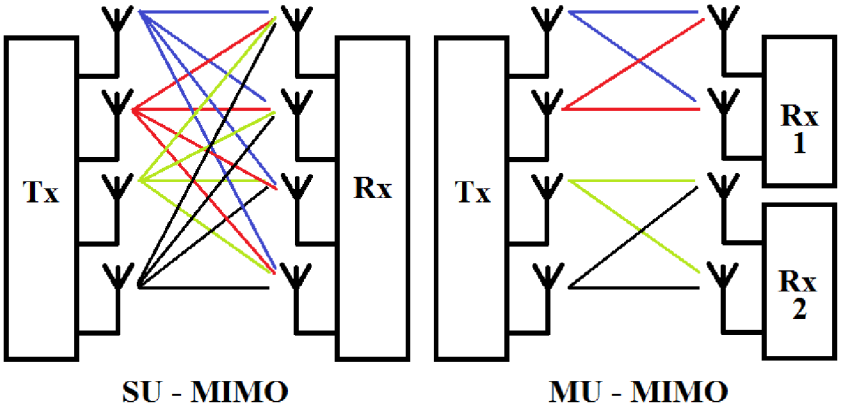
1.6 Technologie MIMO

SU-MIMO (single user – MIMO)

Na vysílači je určitý počet antén a určitý počet antén na přijímači. Za pomocí časové analýzy zjistíme, jaký tok ke kterému toku patří. Nevýhoda spočívá při připojení zařízení, které dokáže využít pouze jeden stream (1x1), načež i ostatní zařízení se tomu musí podvolit a využívat pouze jeden stream a zbytek leží ladem. [29]

MU-MIMO (multi user – MIMO)

V daném čase dokážeme obsloužit více klientů, tím pádem šetříme čas a spektrum. [29]



Obr. 1.10: MIMO [29]

2 BEZDRÁTOVÉ SÍTĚ WLAN

Předchozí kapitola seznamovala s teorií a principem fungování bezdrátových zařízení, přenosem signálu v prostředí a základními otázkami, které je nutno řešit při stavbě bezdrátové sítě. V této kapitole je popsán způsob fungování LAN sítí, propojení s bezdrátovými zařízeními, jejich vlastnostmi a možnostmi.

2.1 IP adresace

Historicky byly definován model ISO/OSI a jemu konkurenční TCP/IP z kterého jsou v následující kapitole uvedeny základní informace týkající se Wi-Fi sítí.

Model TCP/IP je rozdělen na čtyři vrstvy, kde první je Vrstva síťového rozhraní, která definuje přenosové médium, které pro stavbu jednoduché bezdrátové sítě z pravidla bývá vzduch a kroucený ethernetový kabel. Na síťové vrstvě je také pro komunikaci definovaná MAC adresa jako fyzický identifikátor konkrétního rozhraní zařízení.

Druhou vrstvou je Síťová (IP), která pracuje s IP adresami, které slouží ke komunikaci jednotlivých zařízení. Protokoly definované na Síťové vrstvě jsou IPv4, v dnešní době stále primárně využívaný, s tím, že nástupce IPv6 již je často implementován do systémů.

Dalšími dvěma vrstvami je řešen protokol TCP s kontrolou a UDP bez kontroly dat a porty které se přiřazují k IP adresám pro definování služby. Příkladem využívaných portů je port 80 pro protokol http, 443 pro https, 67 a 68 pro DHCP služby, aj. [13] [28]

IPv4 – IP adresa

IP adresa dle protokolu IPv4 nabývá velikosti 32 bitů, jak je znázorněno v tabulce 2.1. Pro lepší práci ji rozdělujeme na 4 hodnoty nabývající velikosti 0–255 oddělené tečkou, například 192.168.1.101. IP adresa je součástí sítě definované maskou sítě například 255.255.255.0 Maska sítě určuje počet IP adres použitelných pro danou konkrétní síť. Příklady masek sítě jsou uvedeny v Příloha č.1 – Seznam masek sítě, kde Prefix zastupuje počet bitů velikosti masky a Počet hostů definuje počet použitelný IP adres v rámci definované sítě.

Příklad z praxe: Náš poskytovatel internetové konektivity nám přiděluje veřejný adresní rozsah velikosti /24, což je 254 volných adres. Tyto adresy my dále dělíme buď na malé bloky s prefixem /29, nebo konkrétní adresu přiřadíme konkrétnímu klientovy, či stanici.

Organizace IANA predikovala nedostatek adres, a proto byl zaveden systém veřejných adres, které již byly rozdělovány a privátních adres. Aby privátní adresy mohly fungovat s veřejnými, byl zaveden překlad adres NAT (kapitola č. 2.4). [28]

IPv6

Protože je čím dál větší nárok na přístup z veřejné sítě ke koncovým zařízením a veřejné adresy postupně dochází, tak se přechází postupně na protokol IPv6. Protokol IPv4 obsahoval teoreticky 2^{32} adres, zatímco protokol IPv6 disponuje 2^{128} počtem adres, což je mnohonásobně vyšší číslo a s touto možností by i odpadla nutnost překladu adres NAT. [28]

Příklad z praxe: Protokol IPv6 jsme začali implementovat před několika měsíci na žádost zákazníků a není jednoduché tuto síť přenastavit, i když téměř všechna zařízení tento protokol

podporují. Plný přechod na IPv6 a jeho využití vidíme nejdříve za několik let. [28]

2.2 Směrovače a směrování IP

Internet a všechna zařízení v internetu pracují s IP adresami (kapitola 2.1). Jelikož zařízení, a tedy i IP adres je v sítí internetu nespočet, a protože je nutný udržet funkčnost, pořádek a efektivnost práce s IP adresami, je nutné mít nástroje pro řízení této sítě. [28]

Směrování (routing) nám zajišťují aktivní síťové prvky – směrovače (routery), které jsou použity pro správu malých sítí, například v domácnosti pro jednotky zařízení až po mezinárodní sítě sčítající statisíce záznamů. Cílem směrování je určování cesty (směru) paketům v síti a jejich rozesílání či přijímání. [28]

Směrovač (router) je zařízení s operačním systémem o jednom a více síťových portech, které přiděluje do jedné či více sítí a tyto sítě propojuje a zajišťuje práci s pakety. Když paket dorazí na určitý port routeru, tak ten následně rozhoduje, jestli a kam paket bude odeslán (nebo zahozen), k čemuž využívá směrovací tabulku. [28]

Směrovací tabulka

Routery mají svojí směrovací tabulku, dle které se rozhodují o příchozích paketech. Jakmile dorazí paket na rozhraní směrovače, směrovač zjistí, jestli patří mezi jeho sítě ve směrovací tabulce a odešle ho správnému zařízení. Pokud směrovač tento záznam nenalezne v tabulce, nebo má jiná definovaná pravidla, tak odesílá paket na výchozí bránu. [28]

Směrovací tabulka může skýtat jednotky záznamů pro malou síť anebo i statisíce pro velkou síť. [28]

Statické směrování

Statické směrování je nejjednodušší forma směrování, která je vhodná pouze pro malé sítě nebo několika málo sítí, z důvodu ruční konfigurace. Administrátor sítě tyto cesty nastavuje ručně ve směrovacích tabulkách jednotlivých zařízení. Nevýhoda statické směrování přichází při změnách směrovací tabulky, při které musí administrátor opět ručně změnit či opravit tabulku. Nevýhodou opět ale nemusí být u malých sítí (často hvězdicové topologie), v kterých právě statické směrování zajišťuje jednoduchost a přehlednost a také menší nároky na hardware samotného směrovače. [28]

Dynamické směrování

Dynamické směrování využívá protokolů ke směrování jednotlivých paketů. Směrovače mezi sebou komunikují a zasílají si automaticky zprávy o změnách ve směrovacích tabulkách. Oproti statickému směrování je jeho použití výhodné ve velkých sítích s mnoha směrovači, čím částečně odpadne práce administrátora sítě upravovat směrovací tabulky a následně i se snižuje lidský faktor zásahu do sítě, čímž i riziko vzniku chyby. [28]

2.3 Firewall

Firewall slouží k zabezpečení a řízení toku dat v síti, dle definovaných pravidel pro komunikaci. Základem je identifikace zdrojové, cílové adresy, cílového portu a také rozšířením se zkoumáním paketů, znalosti protokolů a informacích o stavu spojení. [31]

Firewally můžeme rozdělit:

- **Paketové filtry** – obsahuje zdrojovou a cílovou IP adresu a port, rychlý, ale nízká úroveň kontroly, při které se dle pravidel umožňuje, nebo neumožňuje doručení paketu
- **Aplikační brány** – schování IP adresy skrze proxy za IP brány, jako NAT popsán níže
- **Stavové paketové filtry** – provádějí kontrolu paketů a ukládají si tyto informace
- **Stavové paketové filtry s kontrolou protokolů**– kontrola paktů včetně hloubkové kontroly spojení a zda obsahuji korektní požadavky, například na základě signatur [31]

2.4 NAT – Network Address Translation

NAT, jako součást firewallu, představuje systém překladu síťových adres. V kapitole 2.1 byla naznačena nutnost rozdělit adresní rozsah IPv4 na veřejný a privátní, přičemž je nutnost zajistit komunikaci mezi těmito dvěma systémy, a to pomocí NATu, který z pravidla je součástí směrovače (routeru). [14]

Funkce NAT obsahuje seznam pravidel, definovaných administrátorem, kterými se řídí: [14]

- **Source NAT** – zdrojová IP adresa nebo protokol
- **Destination NAT** – cílová IP adresa nebo protokol
- **Příkaz** – který se má vykonat při splnění podmínek

Základní příkazy funkce NAT jsou: [14]

- **Maškaráda** – jakmile dojde paket z vnitřní sítě, změní se mu IP adresa (z pravidla na vnější adresu routeru) a port a je odeslán. Zároveň si uchová informaci v dynamické tabulce.
- **NAT 1:1** – v NAT tabulce je napevno definováno, co se s příchozími pakety z určité IP nebo portu stane, kam budou přesně odeslány či nebudou zahozeny.

2.5 DHCP – Dynamic Host Configuration Protocol

DHCP se používá pro automatické dělení IP konfigurace v síti, čím je centralizována, ale hlavně velmi zjednodušena práce s IP adresami a konfigurací v sítích v které se často mění nejen, ale hlavně koncové stanice. [5]

DHCP server zejména přiděluje parametry:

- IP adresa
- maska sítě
- výchozí brána
- DNS server/y

Přidělování adres serverem DHCP probíhá skrze broadcast, který kontroluje a jakmile přijme žádost o přidělení DHCP adresy, odesílá zpět návrh IP konfigurace a po následném

schválení si zapisuje k sobě pronájem vybrané IP adresy. [5]

Pronájem IP

IP adresa přidělená DHCP serverem má stanovený čas pronájmu pro určitou stanici. Stanice, která dostala IP adresu a chce si ji uchovat déle, než je stanovený čas pronájmu serverem DHCP, musí zaslat žádost o prodloužení, jinak o tuto adresu přichází. Tímto způsobem může mít více stanic stejnou IP adresu v síti. [2] [5]

Adresy DHCP server může přidělovat několika způsoby: [5]

- **Statická alokace** – DHCP server disponuje seznamem konkrétních MAC adres, které jsou ručně (administrátorem) přirazeny permanentně k IP adresám
- **Dynamická alokace** – Ve vymezeném rozsahu (administrátorem) DHCP server vybere IP adresu a přidělí ji na žádost stanici, pokud IP adresa není pronajata jiné stanici.

2.6 DNS

DNS slouží k převodu doménových jmen a IP adres serverů a uzlů sítě. Obsahují také informace o IP telefonii, nebo emailové komunikaci. DNS servery jsou hierarchicky organizovány, kde kořen je označován tečkou a za ním jsou TLD servery – Top Level Domain – spravují rozdělení domén za tečkou - .com, .cz, .eu, .org. O úroveň níže je strom rozdělen do zón, kde jsou autoritativní servery s informacemi o spravovaných doménách. [6]

DNS servery můžeme rozdělit dle rolí na:

- **Autoritativní server** – trvale uloženy záznamy ke spravované doméně
- **Rekurzivní server** – klientská zařízení odesílají požadavky na rekurzivní server, který odesílá požadavky na autoritativní server a informace ukládá do vlastní cache, na dočasnou dobu [6]

2.7 Zabezpečení Wi-Fi

K základnímu zabezpečení bezdrátové sítě Wi-Fi pro neoprávněný přístup cizího uživatele k vstupu do uzavřené sítě se mezi nejběžnější prostředek řadí šifrování. Dva základní typy zabezpečení jsou: [2] [3]

WEP – Wired Equivalent Privacy

Starší WEP šifrování se řadí k nejméně bezpečné formě zabezpečení i tak v dnešní době stále občas používaným. Pomocí crackovacích programů a s dostatečnými zkušenostmi, lze WEP prolomit, a proto je doporučeno používat WPA2 viz dále. [2] [3]

WPA – WiFi Protected Access

WPA je nástupcem WEP, často dostupném na zařízeních, s možností výběru obou typů šifrování s protokolem **TKIP** (Temporal Key Intergrity Protocol), který částečně řeší problémy WEP a zavádí dynamickou správu šifrovacích klíčů pro bezpečný přenos na začátku komunikace i během ní. Pro domácnosti a kanceláře, kde je sdílené heslo, je vytvořeno **PSK** (Pre-shared key), kdy uživatel pro přístup do sítě musí zadat heslo o velikosti od 8 do 63 znaků z tabulky ASCII. [2] [3]

WPA2

WPA2 obsahuje vše ze standardu použitým v šifrování WPA a rozšiřuje ho o algoritmus, založeným na **AES** (Advanced Encryption Standard).

Některá zařízení podporují současné použití WPA a WPA2 – WPA2 mixed. [2] [3]

2.7.1 Hide SSID

Název sítě – SSID, lze veřejně vysílat, nebo jej skrýt před běžným skenováním Wi-Fi pásma. Připojit se lze k němu jen po zadání přesného SSID a hesla. Tuto metodu nelze považovat za velké zabezpečení, protože skryté SSID lze odhalit během krátké chvíle. [11]

2.7.2 MAC address filter

Každé zařízení má své unikátní výrobní číslo (kapitola 2.1.2) a dle tohoto čísla můžeme nastavit oprávnění připojení zařízení na bezdrátový vysílač. Pokud se MAC adresa neshoduje se zadanou administrátorem, zařízení i když zná heslo není povoleno připojení. [11]

2.8 Nstreme a nv2

Společnost Mikrotik na svých HW vyvinula protokol Nstreme pro zrychlení linky mezi dvěma zařízeními nejen pracující na RouterBoard v pásmu 5GHz. Princip spočívá v nepřenášení kontrolních rámců a ve sdružování vícero rámců, čím sice zvyšujeme propustnost linky, ale vzniká také nutnost využívat kvalitní hardware pro snížení ztrát a chybovosti. [15]

Operační módy Nstreme: [15]

- **PTP mode** – spoj dvou antén
- **Dual radio PTP** – s použitím dvou antén na jedné straně, jedna jako přijímací a druhá vysílací, nazýváme Nstreme2
- **PTMP** – spoj jednoho vysílacího bodu a více přijímacích bodů

Příklad z praxe: Při použití Nstreme protokolu na zařízení Mikrotik již nelze připojit ostatní zařízení pracující na standartu 802.11n, ale pouze zařízení s nastaveným protokolem Nstreme. Konkurence společnosti Mikrotik – Ubiquiti Networks vyvinula vlastní obdobný protokol Airmax. Tyto dva protokoly nejsou navzájem kompatibilní. [15]

2.9 Roaming

Pojem Roaming je známý v GSM sítích, kdy operátor při přecházení přes hranice země řeší funkci GSM sítě pro daný telefon a účtování. Ve Wi-Fi technologii roaming řeší přechod zařízení mezi jednotlivými přístupovými body AP. Přechod zařízení na jiné AP z původního rozhoduje samotné zařízení dle své vnitřní konfigurace politiky, načež u každého zařízení se toto chování liší. [9]

Zařízení si pravidelně sestavuje seznam dostupných AP a pokud signál AP ke kterému je aktuálně připojen poklesne pod určitou úroveň a v seznamu je AP které zná, je zařízení přepojeno. [9]

Z pohledu sítě je více AP s totožným SSID a propojeno skrze aktivní prvky pro správu sítě z pravidla k směrovači. Cílem při přechodu klientského zařízení mezi AP je, aby klient výpadek nezaznamenal, proto samotná reakce na přepojení musí být rychlá. Důležitým požadavkem je zajištění funkcionality IP vrstvy, když si na prvním AP vyžádalo zařízení IP konfiguraci z DHCP serveru. DHCP server si musí zapamatovat toto zařízení při přechodu mezi AP a přidělit mu stejnou IP adresu. [9]

2.10 Teoretický rozbor návrhu Wi-Fi sítě

Pro stavbu lokální bezdrátové sítě při zadávání projektu existují základní požadavky na chování a parametry. Z pohledu technické správy dostaneme požadavky od zadavatele, jako [2] [3]

Pokrytí

Prvním požadavkem je pokrytí vymezeného prostoru od těch nejmenších po velké. U pokrývání několika menších prostor, nebo jednoho většího prostoru hledíme na možnosti fyzického umístění AP a vedení kabeláže k rozvodně a určení počtu zařízení v pokrývané oblasti s ohledem na minimální velikost signálu pro klientské stanice. [2] [3]

Při pokrývání Wi-Fi pásmem 2,4 GHz můžeme využít tři nepřekrývající se kanály 1, 6 a 11 pro jednotlivá AP. Proto je vhodné zvolit umístění jednotlivých AP v prostoru tak, aby se v pořadí vždy opakovaly tyto kanály a zároveň aby AP se stejným kanálem byli vždy od sebe v maximální možné vzdálenosti kvůli vzájemnému nežádoucímu rušení. [2] [3]

Velikost pokrytého prostoru můžeme též ovlivňovat nastavením hranice minimálního signálu klientského zařízení. Jakmile klient se vzdálí od AP natolik, že není přepojen na jiné AP (roaming kapitola 2.9), a signál klesne pod minimální hodnotu, je klient odpojen. [2] [3]

Rychlosti a agregace

Způsob řízení rychlosti a agregace v síti můžeme rozdělit na tři skupiny:

- **Společná** – kdy rychlost a agregace jsou definovány pro celou síť již na směrovači nebo od našeho dodavatele a dále již není nijak řízena
- **Na klienta** – každý klient má definovanou určitou rychlost a agregaci dle nastavení na směrovači, či jiném aktivním prvku
- **Skupinová** – jednotlivým skupinám klientů je přiřazena určitá rychlost a agregace a podle přihlášení klientského zařízení k určité skupině (například dělením dle SSID) jsou parametry klientu nastaveny. [2] [3]

Agregace se udává jako poměr X:Y, kdy X je minimální podíl a Y maximální podíl z rychlosti. Čím vyšší je Y, tím vyšší je sdílení vyhrazené rychlosti. Například agregace 1:10 při rychlosti 100Mb/s znamená rozdělení rychlosti 100Mb/s mezi 10 účastníků, takže při plném zatížení sítě výsledná rychlost bude jen 10Mb/s. U agregace 1:1 je sdílení sítě nulové.

Počet klientů

Maximální počet klientů může být definován parametry:

- **DHCP pool** – maximální počet IP adres, které může DHCP server pronajmout klientům. V případě nedostatku adres již další klienti neobdrží IP adresu a nejsou připojeni do sítě.

- **AP** – samotný přístupový bod má omezenou kapacitu. Při připojení více klientů, než je schopen zvládnout může AP omezovat klienty s menším signálem, popřípadě všechny.
- **LAN síť** – s propustností směrovače (portů, zpracování dat), nebo samotnou přivedenou konektivitou je nutno počítat v nastavení a při dosažení určité hranice buď odmítnout připojení dalších zařízení, nebo omezit ostatní zařízení [9]

Příklad z praxe: Každoročně na jaře na Brněnském výstavišti stavíme dočasnou bezdrátovou síť pro Fantu a Coca-Colu. V zadání klienta jsou vždy jasné jen parametry celkové přivedené konektivity 100/100 Mb/s s agregací 1:1 a rychlostmi pro klientské stanice 5 Mb/s pro stahování a 2 Mb/s pro nahrávání. Průměrný počet klientů se pohybuje okolo 150 klientských stanic, většinou mobilní telefony. Při jednoduché matematice 150 klientů * 5/2 Mb/s rychlost se dostáváme na teoretickou maximální požadovanou rychlost 750/300 Mb/s, což je několikanásobek přivedené konektivity. Existují klientské stanice (klienti), využívající síť skoro ve 100 % připojeného času a klientské stanice využívající síť jen minimálně. Proto je vhodné počet klientů korigovat, v našem případě odpojováním a změnou maximální rychlosti. Díky správnému a pečlivému nastavení mnoha parametrů sítě jsme schopni zajistit efektivní využití a minimalizovat problémy

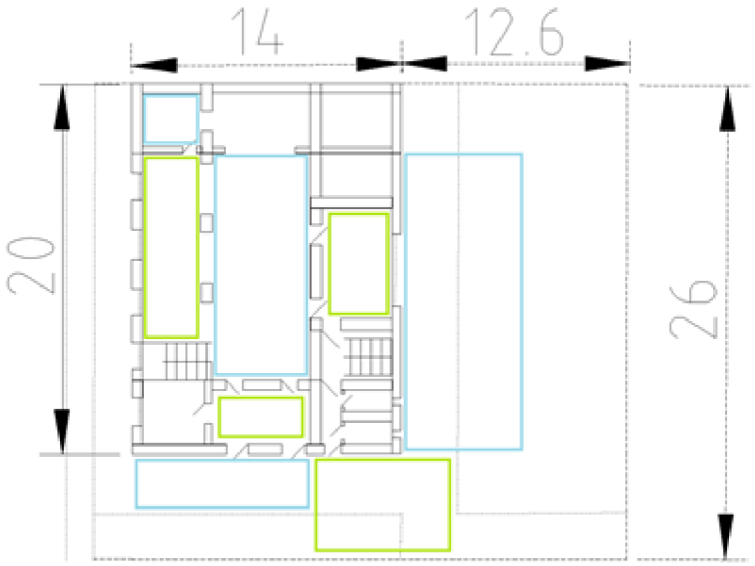
.

3 REALIZACE BEZDRÁTOVÉ SÍTĚ WI-FI V OBJEKTU SOKOLOVNY

V následující části je popsána realizace bezdrátové sítě v a vně objektu sokolovny, Doubravník 156, 592 61 Doubravník, kde pokrytí signálem pro návštěvníky je požadováno ve frekventovaných prostorách. Požadavkem je veřejný hotspot s heslem, Wi-Fi síť pro organizátory a ethernetovou přípojku do pracovny s přiměřenými rychlostmi a agregací.

3.1 Analýza zadání a situace

Pro správný výběr technologie s dostatečnými parametry pro splnění zadání bylo nutné analyzovat zadání a celou konkrétní situaci v objektu. Prvotním bodem pro analýzu je samotný objekt a vymezení prostor, které bylo nutné pokrýt dostatečnou úrovní Wi-Fi signálu. Nejvíce frekventované prostory, které bylo nutné pokrýt, jsou vyznačené na půdorysu objektu, viz Obr. 3.1, zelenou barvou. Další prostory v a vně objektu mohli být pokryty s nižší úrovní signálu, označené na půdorysu modrou barvou. Pro zbytek prostor objektu a areálu není požadované pokrytí, avšak je vítané.



Obr. 3.1: Půdorys areálu s objektem, včetně vyznačených prostor pro pokrytí signálem

Parametr počet návštěvníků je důležitým ukazatelem pro využití a vytíženost jednotlivých přístupových bodů a sítě, z pohledu kapacitního a IP adresace. Počet návštěvníků sokolovny se pohyboval mezi 20 až 400 lidmi, dle Tab 3.1 sestavené na základě zkušenosti majitele objektu. Největší kapacitní zatížení sítě bude při akci Sportovní turnaj, kde počet připojených návštěvníků je 30. Další ukazatel je počet přihlášených návštěvníků na AP, kteří nejeví aktivitu, ale mají zapnutou Wi-Fi na zařízení a již tím zatěžují AP, kde pravděpodobně největší zatížení sítě je na akci Skautský ples.

Tab 3.1: Počet návštěvníků objektu a teoretický počet připojených návštěvníků k síti

Akce	Maximální počet návštěvníků objektu	Teoretický počet návštěvníků připojených k síti
Skautský ples	400	20
Sokolský ples	150	7,5
Hodová zábava	300	15
Divadelní představení	100	10
Sportovní turnaj	100	30
Trénink	20	5

Třetí parametry, který je nutné vzít v potaz je primární činnost návštěvníků, resp. jejich připojených zařízení k síti Wi-Fi. Zde v objektu je konkrétně primární činností nahrávání fotek a videí, posílání zpráv skrze email a sociální sítě. Z tohoto důvodu omezení rychlosti stahování i nahrávání na klientské zařízení volíme symetrické a to 5 Mb/s pro stahování a 5 Mb/s pro nahrávání, kde rychlost je volena dle dostupné kapacity od poskytovatele internetu, která je v maximu 70/70 a tak aby dělení rychlosti v maximu dosáhlo přiměřené agregace popsané v kapitole 2.10.

3.2 Výpočet přívodní linky do sokolovny.

Budeme-li uvažovat, že na jednoho klienta připadá 5/5 Mb/s a klientů při největším zatížení bude 30, jednoduchým vynásobením získáme rychlost 150/150 Mb/s. Protože v jednu chvíli ale linku využívá jen část klientských zařízení, není nutné, aby byla přivedena takto velká rychlost. K tomuto účelu se využívá agregace rychlosti popsaná v kapitole 2.10.

Při standartní agregaci 1:5 dostačuje linka 30/30 Mb/s, při agregaci 1:10 15/15 Mb/s.

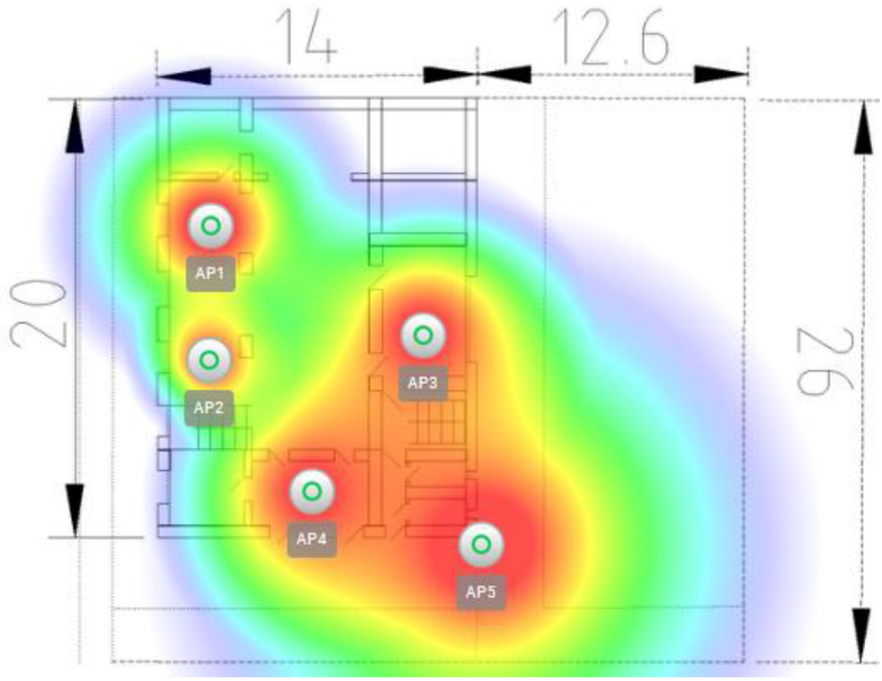
Součtem agregované linky pro organizátory 15/15 Mb/s + neagregovaný přívod pro majitele 10/10 Mb/s + agregovaný přívod pro návštěvníky 30/30 Mb/s (nebo 15/15 Mb/s), vychází výsledek přívodní linky pro sokolovnu 55/55 Mb/s (40/40 Mb/s). Zvolena byla agregace 1:5, tzn 55/55 Mb/s.

3.3 Teoretický návrh

V teoretickém návrhu řešení sítě objektu byl zjištěn počet a rozmístění zařízení pro splnění požadavků, způsob jejich propojení a konfigurace sítě. Na základě analýzy a návrhu byly zvoleny vhodné prvky s dostatečnými parametry pro zajištění chodu sítě.

Návrh počtu AP je potřeba počítat z parametru počtu přihlášených zařízení a počtu aktivních zařízení v síti. Jelikož těchto zařízení dle tabulky je málo a není to problémem i pro levnější varianty řešení Wi-Fi sítě, budeme brát v potaz pouze podmínku, aby prostory k pokrytí definované v kapitole č. byly pokryty dostatečnou úrovní signálu. Pro zajištění dostatečného signálu v těchto menších prostorech byl výpočet AP spočten z počtu prostor,

abychom předešli velkému útlumu zdí. Místnosti jsou dvě menší, jeden venkovní prostor a jedna větší, která byla rozdělena na poloviny pro dvě AP. Výsledkem je pět AP pro pokrytí prostor objektu a areálu rozvrženými na půdoryse objektu, viz Obr. 3.2, pomocí aplikace kontroléru.

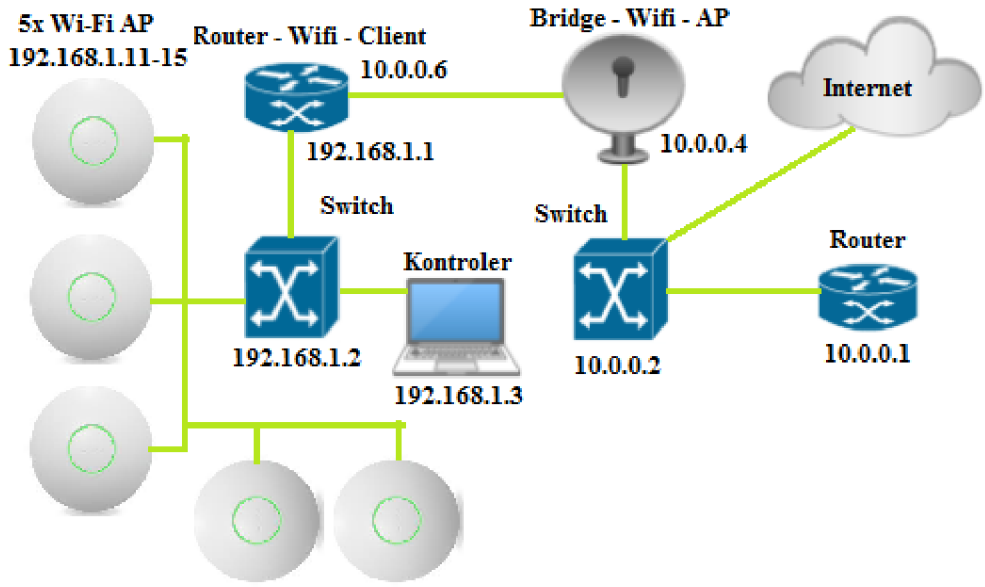


Obr. 3.2: Rozvržení AP pro pokrytí požadovaných oblastí objektu

Důležitou volbou je výběr frekvenčního pásma. Jelikož byla uvažována Wi-Fi bezdrátová síť, jsou prakticky schůdné pouze pásma 2,4 GHz a 5 GHz. Výhodou 5 GHz pásma oproti 2,4 GHz pásmu je hlavně větší počet kanálů a vyšší přenosová rychlost. Jelikož počet aktivních klientů byl nízký a přenesená data malá, bylo zvoleno použití pásma pouze 2,4 GHz se standardem 802.11 b/g/n. Pásmo 5GHz pro koncové AP je sice čím dál více využívanější, ale pro naše účely bylo nadbytečné.

3.3.1 Konfigurace sítě

V následující kapitole je sestavena topologie celé sítě včetně přivedení přívodu Internetu od poskytovatele a vnitřní bezdrátové sítě objektu. Topologie byla sestavena tak, aby byla využita zařízení poskytovatele Internetu, v síti rozvodny jako router a switch, do kterého byl připojen PTP spoj pro připojení objektu sokolovny, kde jednotka PTP spoje na straně sokolovny zastávala i funkci routeru a obstarávala celou vnitřní síť sokolovny, kde do připojeného switche byly připojena všechna AP včetně kontroléru.



Obr. 3.3: Topologie celé sítě objektu, včetně připojení sítě do sítě poskytovatele k síti Internet

Síť sokolovny pro zařízení:

Počet hostů: 8

Síť: 192.168.1.0/24 (255.255.255.0)

VLAN: 1 – tzn. bez VLAN sítě

Brána – Router: 192.168.1.1

Switch: 192.168.1.2

Kontrolér: 192.168.1.3

AP: 192.168.1.11-192.168.1.15

Majitel: 192.168.1.200

Omezení: 10/10 Mb/s na majitelovu IP

Síť klientů – SSID: Sokolovna-Hotspot:

Počet hostů aktivních na Hotspotu je cca 30 dle odhadů, pasivních může být mnohonásobně více. Pro předejití problémům automaticky byl volen vyšší počet možných hostů, i z nepředvídatelných důvodů.

Síť: 192.168.4.0/23 (255.255.254.0)

VLAN: 202

Brána – Router: 192.168.4.1

Omezení: 30/30 Mb/s pro rozsah sítě

Síť klientů – SSID: Sokolovna-Organizace:

Počet hostů připojených k síti Organizace je cca 10.

Síť: 192.168.2.0/24 (255.255.255.0)

VLAN: 200

Brána – Router: 192.168.2.1

Omezení: 15/15 Mb/s pro rozsah sítě

Síť rozvodny pro připojení přívodu:

Počet hostů: 4+

Síť: 10.0.0.0/24 (255.255.255.0)

Brána – Router: 10.0.0.1

Switch: 10.0.0.2

Vysílající anténa – bridge: 10.0.0.5

Přijímací anténa – router: 10.0.0.6

Hlavní přívod: DHCP client, VLAN100 – skrze switch do routeru

3.3.2 Zařízení objektu sokolovny

Jako přístupový bod AP bylo zvoleno zařízení od společnosti Ubiquity a to UniFi s podporou pouze 2,4 GHz pásma. Výhodou AP UniFi je především napájení skrze PoE, možnost rychlého a přehledného ovládání skrze kontrolér a cenová dostupnost. Jako switch byl použit TP-Link s dostatečným počtem portů, možností administrace skrze webové rozhraní a podporou VLAN, která nebyla v tomto případě využita. Kontrolérem systému pro UniFi AP je softwarová aplikace pro Windows běžící na podpoře Javy. Jako kontrolér byl zvolen Notebook Lenovo s operačním systémem Windows 7.

Parametry AP

Název: UniFi AP

Frekvenční rozsah: 2,4 GHz

Antena: 1dBm

Maximální vysílací výkon: 24 dBm

Switch

Název: TP-Link

Počet portů: 16

Kontrolér – Notebook Lenovo

Operační systém: Windows 7

LAN: 1x 1Gb/s

3.3.3 Zařízení přívodu a rozvodny

Pro propojení budovy rozvodny s objektem sokolovny byl zvolen PTP spoj od společnosti Mikrotik z důvodu využití 5 GHz pásma pro přenos v prostředí v celku s malým rušením. Pro připojení spoje do sítě Internet byla využita již nainstalovaná technologie poskytovatele internetu, a to switch TP-Link a Router od společnosti Mikrotik.

PTP spoj

Název: RB SXT 5HnD

Frekvence: 5 GHz

Zisk: 14 dBi

Maximální výkon: 30 dBm

Switch

Název: TP-Link

Porty: 16x 1 Gb/s

Router – MT-MainRouter

Název: RouterBoard

Porty: 1x 1Gb/s

Kabeláž

Značka: Belden, cat5e

Patch kabely: DataCom, cat5e

3.4 Konfigurace sítě

3.4.1 Konfigurace bezdrátového a síťového rozhraní

Veškeré konfigurace bezdrátové sítě objektu byla provedena skrze kontrolér až na IP adresaci, omezení rychlosti pro IP rozsahy a služby routeru, které byly prováděny na routeru.

Kontrolér jednotek UniFi umožňuje možnosti konfigurace bezdrátového rozhraní jednotlivých AP v tomto nastavení:

- Šířka pásma (Channel width)
  - HT20 – 20 MHz
  - HT40 – 40 MHz
- Kanál (Channel)
  - 1-13 – pásmo 2,4 GHz
- Vysílací výkon (Transmit Power) - EIRP
  - Vysoký (High) – 20 dBm
  - Střední (Medium) – 14dBm
  - Nízký (Low) – 8dBm
  - Vlastní (Custom) – 0 až 23 dBm (možnost překročit 100mW)
- Minimální RSSI (Minimum RSSI)
  - -1 až -94

Konfigurace bezdrátového rozhraní probíhá pro každou jednotku zvlášť. V základním nastavení jsou jednotky nastaveny na šířku kanálu HT20, automatický kanál vysílání a automatická velikost vysílacího výkonu.

Nastavení velikosti vysílacího výkonu probíhá pro čtyři úrovně, kde pro jednotlivé možnosti Low, Medium, High jsou určeny velikosti dBm, vypočítaných kontrolérem, dle vybraného státu v nastavení a jeho legislativních podmínkách o použití bezdrátových sítí a omezení vysíleného výkonu popsaným v kapitole 1.4 . Kontrolér do výpočtu výkonu zahrnuje i zisk antény. V České republice je povolen maximální vysílací výkon 100mW, což je rovno 20dBm při volbě možnosti High.

Kanály pro jednotlivé AP byly zvoleny dle rozmístění a aby se střídaly konkrétní kanály 1, 6 a 11, kvůli vzájemnému překrývání a rušení popsaným v kapitole 1.2. Vysílací výkon byl volen tak, aby byla dostatečná velikost signálu v požadovaných oblastech a aby zároveň si AP navzájem nezasahovaly do pokrývaných oblastí.

AP1 – Kanál č. 1, Výkon: Medium

AP2 – Kanál č. 6, Výkon: Low

AP3 – Kanál č. 1, Výkon: Medium

AP4 – Kanál č. 11, Výkon: Medium

AP5 – Kanál č. 6, Výkon: High

Síťové rozhraní jednotlivých AP bylo nakonfigurováno dle návrhu konfigurace v kapitole 3.3.1. Konfigurace probíhá ve stejné záložce kontroléru jako konfigurace bezdrátového rozhraní.

3.4.2 Konfigurace Wi-Fi sítí

Bezdrátové sítě byly nakonfigurovány dle návrhu popsaném v kapitole 3.3.1. Samotná konfigurace se provádí v kontroléru v nastavení [./nastavení/bezdrátové sítě]. Byla zde vytvořena dvě SSID s VLAN sítí pro správné přidělování IP adres klientským zařízením přihlášeným k síti.

Základní konfigurace zabezpečení sítě může být provedena pomocí těchto čtyř možností:

- Otevřená síť (Open) – bez hesla
- WEP
- WPA
- WPA2

Pro všechny sítě byla zvolena zabezpečení WPA/WPA2, které je považováno za bezpečné.

VLAN síť zde slouží k zajištění komunikace mezi routerem a koncovými klienty, primárně z důvodu přidělování IP adres určených pro dané SSID, a tedy i k omezení maximální rychlosti pro rozsah IP.

Konfigurace Skupiny (User group), která se provádí v nastavení [./nastavení/user group] slouží ke konfigurace omezení rychlosti stahování a nahrávání na klienta. Tyto skupiny byly nakonfigurovány dle návrhu v kapitole č. a přiřazeny jednotlivým SSID.

SSID: Sokolovna-Hotspot

VLAN: 202

Heslo: bakalarka223

Skupina: Sokolovna-Hotspot – s omezením 5/5 Mb/s na jednoho klienta

SSID: Sokolovna-Organizace

VLAN: 200

Heslo: bakalarka223

Skupina: Sokolovna-Organizace– s omezením 10/10 Mb/s na jednoho klienta

3.4.3 Konfigurace PTP spoje

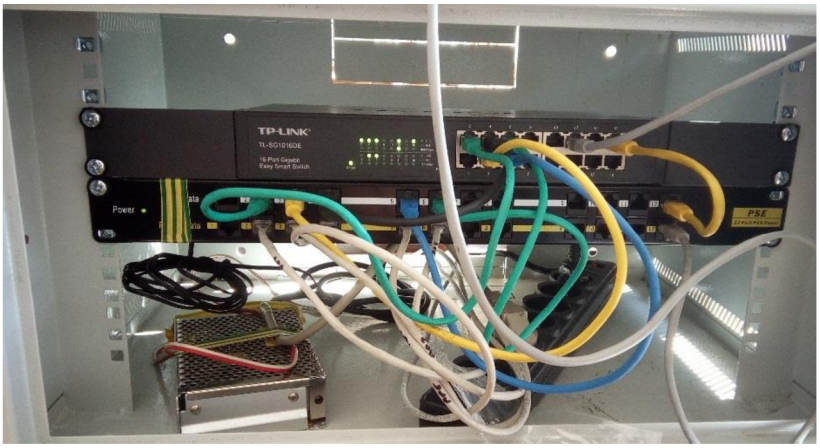
Konfigurace PTP spoje, kterým byl zvolen Mikrotik se provádí skrze systém RouterOS, který vyžaduje určité znalosti pro správnou konfiguraci, kterou lze provádět několika způsoby. Nejpoužívanějším nástrojem pro konfiguraci je aplikace pro Windows, zvaná WinBox. Skrze WinBox lze přehledně konfigurovat všechny parametry zařízení.

Síťová konfigurace jednotek byla nakonfigurována dle návrhu v kapitole 3.3.1, tak aby komunikovala se síti rozvodny, kde byla jednotka na straně rozvodny zapojena do switche a na straně objektu provedena konfigurace routeru. Na routeru byly nastaveny VLAN sítě pro

jednotlivé SSID s omezením pro IP rozsahy přidělované DHCP serverem. Router také plnil funkci NAT – masquerade mezi WLAN rozhraním a LAN. Způsob konfigurace systému RouterOS je více popsán v kapitole 4.2.2.

3.5 Sestavení sítě

Dle návrhu byla síť sestavena v budově sokolovny a rozvodny a realizována spojení mezi těmito dvěma budovami. V budově sokolovny byla uschován switch, kontrolér a veškeré napájení sítě, do racku, viz Obr. 3.4 odkud vedly jednotlivé kabely k AP rozmístěným v objektu.

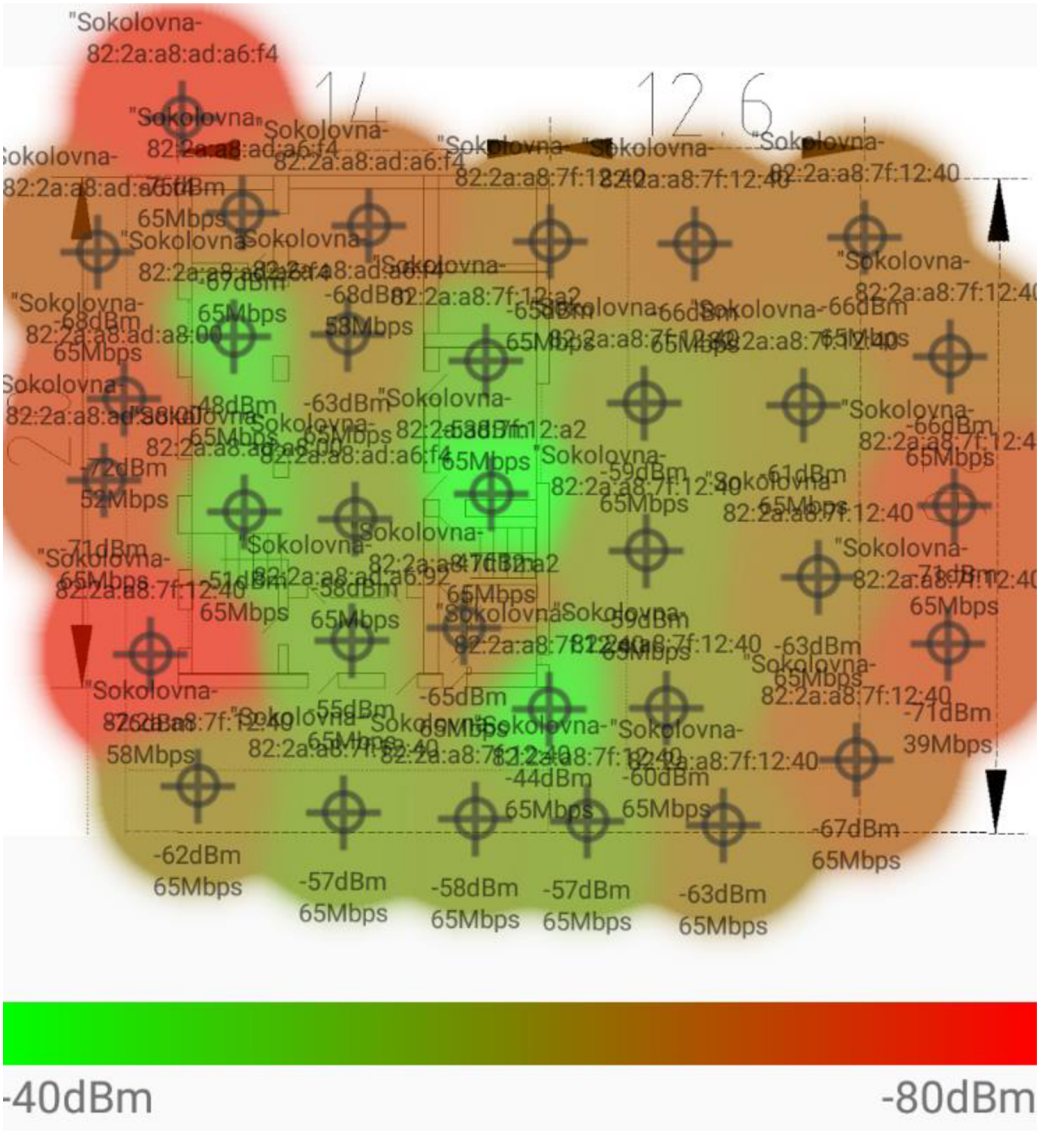


Obr. 3.4: Rack v objektu se switchem a napájením

3.6 Měření parametrů realizované sítě

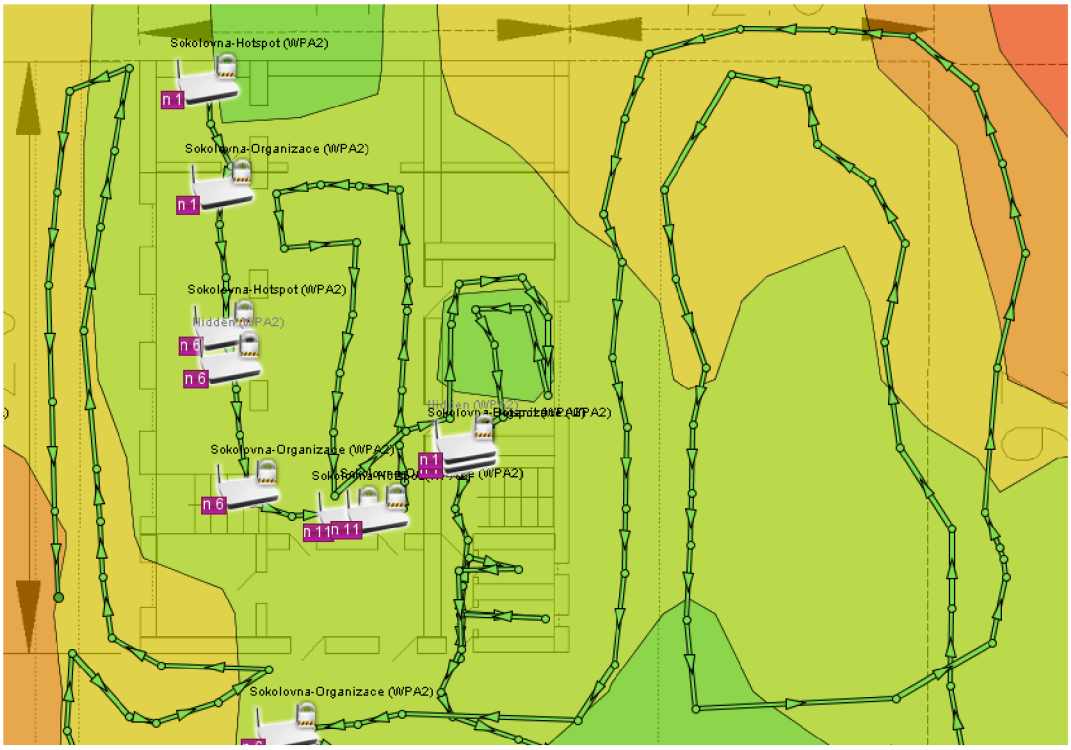
3.6.1 Síť sokolovny

Primárním cílem bylo pokrytí vymezených prostor dostatečnou úrovní signálu. Měření (viz Obr. 3.5)proběhlo pomocí aplikace Wi-Fi Visualizer, skrze kterou byly změřeny velikosti signálu mobilním zařízením ZoPo. Měření proběhlo v požadovaných oblastech v a vně budovy, včetně měření i mimo tyto oblasti. Na obrázku je možno vidět jednotlivé úrovně v bodě měření značené barvou kde barva světle zelená značí cca -40 dBm až -50, tmavě zelená -50 až -60, hnědá -60 až -70 a červená -70 a více.



Obr. 3.5: Měření úrovně signálu v objektu a areálu pomocí Wi-Fi Visualizer

Pro porovnání prvního měření bylo provedeno druhé měření v programu Ekahau HeatMapper, kterým byly změřeny velikosti signálů. Velikost těchto signálů je znázorněna na Obr. 3.6, kde zelená barva značí nevyšší signál s úrovní -45dBm a oranžová barva s úrovní -80dBm. Oba obrázky si vzájemně přiměřeně odpovídají s jistou chybou měření, primárně způsobenou nepřesností měření, měřením jen určitých prostor a ploch.



Obr. 3.6: Měření úrovně signálu v objektu a v areálu pomocí Ekahau Heatmapper

Dalším výstupem měření je možnost upravení minimálního RSSI, kde pro docílení ještě lepší konfigurace sítě, můžeme nastavit hodnotu minimum RSSI jednotlivých AP, pro odpojování klientů s nižší hodnotou RSSI než je definována. Hraniční hodnotu při usuzování z měření pro síť objektu a areálu byla cca -70dBm, kterou lze následně snižovat či zvyšovat dle potřeby.

Měření parametru rychlosti a omezení rychlosti:

Kontrola přenosové rychlosti a jeho omezení nastaveným globálně na routeru a pro každého uživatele je znázorněna v tabulce. Měření proběhlo pomocí příkazu iperf, kde jedna strana je vždy server a druhá strana klient, který vysílá data. Jde o průměrná data několika měření.

Tab 3.2: Kontrola přenosové rychlostí omezená routerem a kontrolérem

Typ měření	Stahování (Download) Mb/s	Nahrávání (Upload) Mb/s
Hotspot bez omezení	28	27,7
Hotspot s omezením	4,9	4,8
Organizace bez omezení	14,8	14,1
Organizace s omezením	10	9,9
Majitel	9,8	9,9

Jednotlivé hodnoty se vcelku blíží hodnotám nadefinovaným v omezovačích a šlo je považovat za použitelné, jelikož zde není až takový požadavek na přesnost jednotlivých rychlostí.

3.6.2 Síť rozvodny

Bylo provedeno základní měření skutečné rychlosti na spoji a přívodu od poskytovatele. Poskytovatelem byla dodána kapacita sítě s parametry 70/70 Mb/s, bez agregace. Po měření této přívodní konektivity v dopoledních hodinách, tudíž ne ve špičce, bylo dosáhnuto průměrné rychlosti 67/64 Mb/s, což je pro naše potřeby popsané v návrhu v kapitole č. dostačující.

Měření hlavního přívodu

Velikost přívodní rychlosti: 67/64 Mb/s

Parametry spoje PTP

Úroveň signálu: -56

CCQ:

Průměrná přenosová rychlost: 72/70 Mb/s.

Výsledkem měření sítě rozvodny je, že tato síť je dostačující pro splnění požadavků pro přenos rychlosti 55/55 Mb/s s rezervou 12/9 Mb/s na přívodní konektivitě a 17/15 na přenosu dat PTP spojem mezi rozvodnou a objektem. Veškeré hodnoty byly měřeny za dobrého počasí a v hodinách kdy nebyla špička. Při zhoršení počasí nebo ve špičce může dojít k mírnému zhoršení těchto hodnot, přičemž vypočtená rezerva by měla postačit k vykrytí těchto anomálií. Další měření v 5 GHz pásmu se spoji Mikrotik jsou popsány v kapitole č. při sestavování venkovní sítě.

4 REALIZACE VENKOVNÍ WI-FI SÍTĚ

4.1 Teoretický popis a návrh

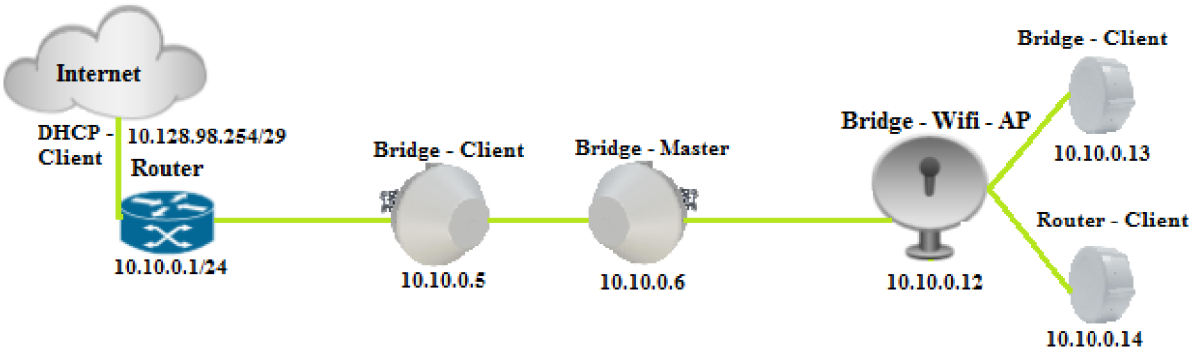
Venkovní Wi-Fi síť je realizována v Brně na vzdálenosti ve stovkách metrů. Cílem bylo propojit tři budovy bezdrátovou Wi-Fi technologií v Brně, kde síť byla sestavena v reálném prostředí s rušením a dalšími nežádoucími vlastnostmi. Dalším cílem je i otestovat zajímavé vlastnosti jednotlivých bezdrátových technologií.

Základní bod sítě byl na budově A – Šumavská Tower A, Šumavská 525/33 602 00 Brno, kde je umístěna přívodní konektivita do sítě internet od poskytovatele internetu. Budova Šumavské má být spojena s budovou B – Hotel Continental, Kounicova 680/6 602 00 Brno, na vzdálenost 1,33km, kde jsou další dva spoje s budovou C – Veveří 6, 602 00 Brno, na vzdálenost 104 m.

Obr. 4.1: Mapa realizovaného spojení mezi budovami A – Šumavská, B – Hotel, C – Veveří

4.1.1 Síťová topologie a konfigurace

Topologie sítě je vyobrazena na Obr. 4.2, kde pro připojení přívodu sloužil router, který prováděl NAT popsaný v kapitole č. a obstarával síť pro připojení jednotlivých bezdrátových zařízení. Jako hlavní router byl zvoleno zařízení Mikrotik – RouterBoard 3011, popsán v kapitole 4.2, jelikož má dostatečné vlastnosti pro sestavení této sítě jako 1 Gb/s porty, kterých je více jak dva.



Obr. 4.2: Topologie venkovní Wi-Fi sítě, včetně IP adresace

Konfigurace celé sítě byla volena tak, aby byl dostatek místa pro všechna zařízení a byla přiměřeně flexibilní. Konfigurace přívodní sítě, pro připojení do Internetu, bylo volena formou DHCP serveru a klienta, kde byla přidělována konkrétní IP adresa od poskytovatel Internetu s velikostí sítě /29, branou a DNS adresami, které v naší síti nevyužijeme.

Síť přívodu

Způsob konfigurace: DHCP klient

Počet hostů: 1

Síť: 10.128.98.240/29 (255.255.255.248)

Brána: 10.128.98.241

MT-MainRouter: 10.128.98.254

DNS: 10.128.0.0, 10.128.0.1

Pro vzdálený přístup skrze veřejný IPv4 rozsah byla poskytovatelem pro vnitřní IP adresu 10.128.98.254, která byla přidělena routeru pomocí NAT přidělena veřejná IP adresa 213.175.51.204, díky které je umožněna komunikace s routerem, ale také s dalšími zařízeními v síti, buď přes router, například skrze SSH tunel, nebo pomocí přidělených portů, které byly překládány v routeru (NAT, viz kapitola 2.4).

Páteřní síť

Pro páteřní síť byl zvoleno statické přidělování IP adres, kde síť obhospodařoval hlavní router. Velikost sítě byla volena /24, což odpovídá 256 hostům, což bylo plně dostačující. Číselný rozsah byl volen pro jednoduché zapamatování 10.10.0.0/24, kde zařízení dostala přiřazeny IP adresy ze spodní části rozsahu.

Způsob konfigurace: Statické IP

Počet hostů: 6+

Síť: 10.10.0.0/24 (255.255.255.0)

Brána MT-MainRouter: 10.10.0.1

Dell – testovací notebook: 10.10.0.2

Metrolinq Client: 10.10.0.5

MetroLinq Master: 10.10.0.6

Lenovo – testovací notebook: 10.10.0.10

MT-AP5GHz: 10.10.0.12

SXT-bridge: 10.10.0.13

SXT-router: 10.10.0.14

DNS: 8.8.8.8, 8.8.4.4 (Google)

Domácí síť SXT-router

Pro domácí síť byl zvolen router s DHCP serverem a funkcí NAT, pro oddělení vnitřní sítě od páteřní, primárně z důvodu bezpečnosti. Vnitřní síť je volena v rozsahu 192.168.0.0./24.

Způsob konfigurace: DHCP server, NAT

Počet hostů: jednotky až desítky

Síť: 192.168.0.0/24 (255.255.255.0)

Brána SXT-router: 192.168.0.1

DNS: 8.8.8.8, 8.8.4.4 (Google)

4.2 Hlavní Router – MT-MainRouter

Na rozhraní páteřní sítě byl umístěn router pro překlad adres a komunikaci mezi sítí páteřní a sítí poskytovatele pro přístup k Internetu. Jako router byl zvolen Mikrotik RouterBoard 3011, z důvodu většího počtu gigabitových portů pro připojení přívodu, rádia a testovacího notebooku.

4.2.1 Popis zařízení

Název: RB3011UiAS-RM

CPU: 2x 1,4 GHz

Porty: 10x 1Gb/s

SFP port: 1x

PoE In: port 1

PoE Out: port 10

Vstupní napětí 10V – 30V

Operační systém: RouterOS

USB: USB 3.0

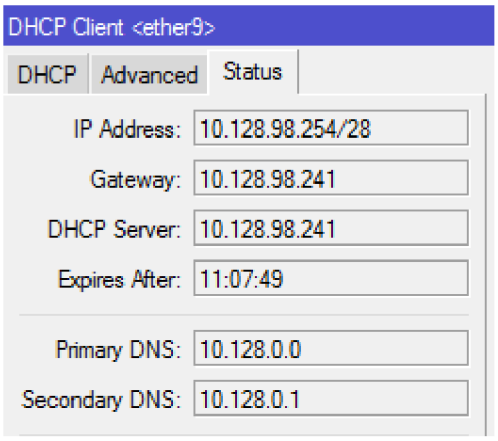
Seriál port: RJ45

4.2.2 Konfigurace

Konfigurace WAN rozhraní:

Konfigurace RB3011 probíhá skrze operační systém RouterOS, který již byl popsán v kapitole č. při konfiguraci vnitřní sítě Wi-Fi.

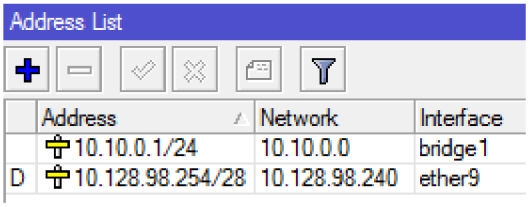
Přívod byl připojen na interface ethernet9, pro který byl nastaven DHCP klient [./IP/DHCP client], který si nechal přidělit adresy od DHCP serveru poskytovatele Internetu. Výsledné adresy jsou vidět na Obr. 4.3 Systém RouterOS automaticky přidělené adresy zpracoval a přidal do adresy [./IP/Adresses] viz. Obr. 4.4 a doplnil routovací tabulku [./IP/Routes] obrázek Obr. 4.5.



Obr. 4.3: Načtení konfigurace DHCP klienta

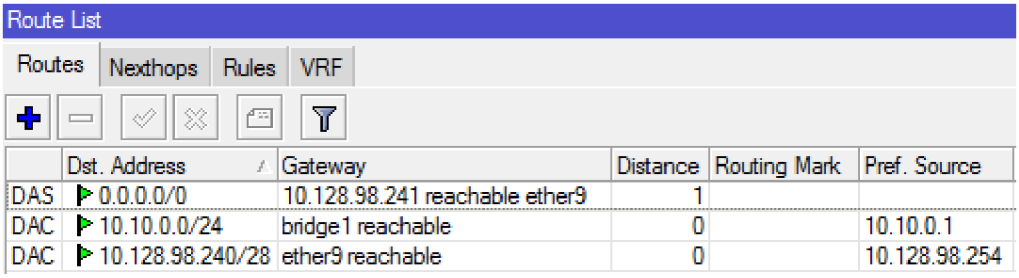
Konfigurace LAN rozhraní:

Pro páteřní síť byl vytvořen v systému RouterOS most – bridge1, který spojuje porty 2 až 7 (ethernet2 až ethernet7), pro které je přidělena stejná síť. Jako síť páteřní dle návrhu v kapitole 4.1.1 byla zvolena 10.10.0.0/24, kde první adresa je přidělena routeru. Veškerá konfigurace IP adres v páteřní síti probíhá staticky.



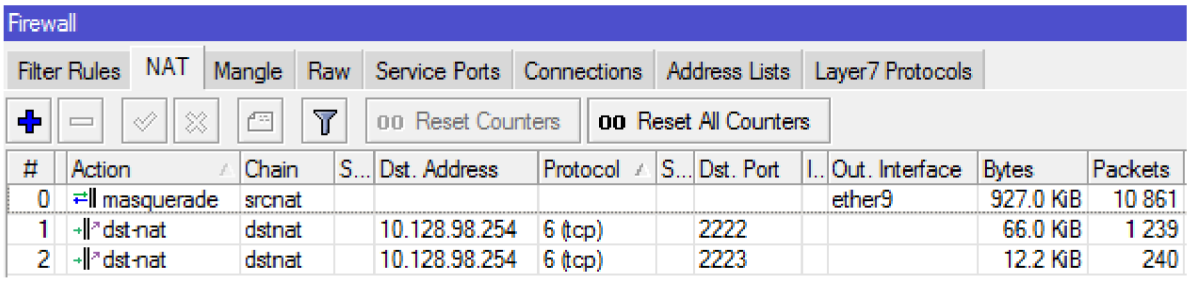
Obr. 4.4: IP adresy hlavního routeru definované pro interface bridge1 a ethernet9

Routovací tabulka slouží k rozhodovaní routeru, kam má posílat pakety (Gateway), které přijdou z adres Dst. Address. Rozhodování se dělá i v závislosti na vzdálenosti – velikosti parametru Distance, což je v této síti nevyužitelné.



Obr. 4.5: Routovací tabulka hlavního routeru

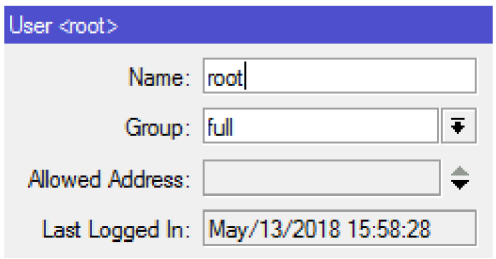
Firewall je popsán v kapitole 2.4, kde na routeru je využitá funkce NAT. První funkcí označenou na Obr. 4.6 jako „0“ je srcnat s akcí masquerade, která slouží k převzetí všech dat z vnitřní sítě a odesílá je do sítě poskytovatele, dle routovací tabulky za IP adresou, přidělenou na WAN rozhraní. Další dvě pravidla s funkcí dst-nat slouží k přístupu z veřejné části sítě skrze veřejnou IP definovanou v kapitole 4.1.1 k jednotlivým zařízením sítě skrze porty 2222 a 2223, které jsou automaticky překládány na port 80 (http protokol) pro správu dvou páteřních zařízení.



Obr. 4.6: Firewall a definovaná pravidla NATu

Konfigurace systému:

Pro přihlášení bylo v nastavení systému [./system/user] nakonfigurován uživatel root s heslem bakalarka223 pro přístup do administrace. Na Obr. 4.7 je vidět i poslední čas přihlášení uživatele.



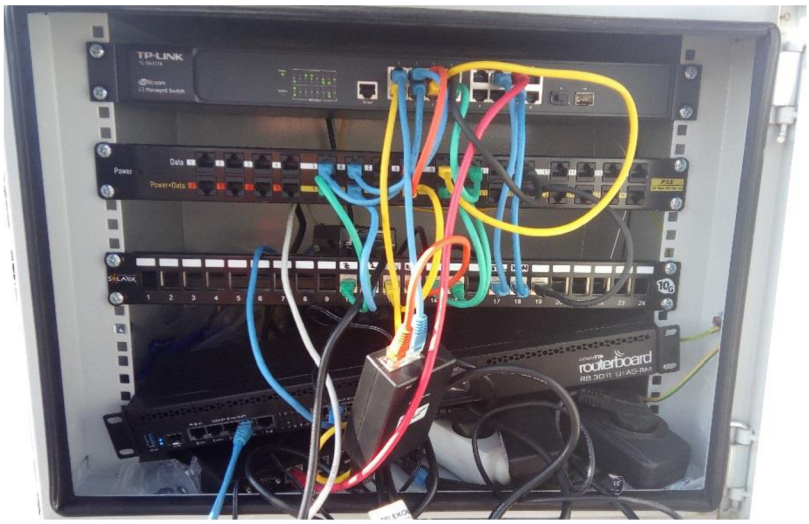
Obr. 4.7: Konfigurace uživatele pro přístup do administrace

Hlavní router byl pojmenován MT-MainRouter, dle návrhu a nakonfigurován v systému [./system/identity], možno vidět na Obr. 4.8.

Obr. 4.8: Konfigurace názvu hlavního routeru

4.2.3 Umístění Rack – Šumavská Tower – A

Hlavní router – MT-MainRouter byl umístěn do racku telekomunikačního operátora, viz obrázek Obr. 4.9, s jeho souhlasem, včetně napájecích zdrojů k routeru a k bezdrátovému rádiu. Jelikož v racku telekomunikačního operátora nebylo dostatek místa pro přehledné namontování, bylo nutné umístit zařízení nepřehledně do spodní části racku.



Obr. 4.9: Rack telekomunikačního operátora, Šumavská Tower – A

4.3 PTP spoj Metrolinq Ignite

Jako PTP spoj mezi budovou A Šumavská a budovou B Hotel byl zvolen spoj Metrolinq Ignite, viz Obr. 4.10, pracujícím v 60 GHz pásmu, dle standartu 802.11ad. Spoj byl volen z důvodu svých vlastností, kde přední vlastností spoje je velká šířka kanálu, díky které je spoj schopen zajistit vysokou přenosovou kapacitu.

Obr. 4.10: Jednotka PTP spoje Metrolinq Ignite umístěna na budově A Šumavská se zaměřovacím dalekohledem

4.3.1 Popis zařízení

Název: MetroLinq 60-35 PTP/Client

- Standart: 802.11ad
- Pásmo: 60GHz

Hardware:

- 2x Gigabit Ethernet Port (1x PoE IN)
- 1x USB 2.0 Port

LED žárovky:

- Napájení (Power), Ethernet, Wireless (60/5GHz), Stav (Health/Status), Zaměřování (Aiming)

Rozměry:

- 350x350x200mm

Váha:

- 3,5 Kg

Napájení (Power):

- 24V/1A Gigabit PoE (pasivní/passive)

Pracovní prostředí:

- Pracovní a skladovací teplota: -30 až +55 °C
- Vlhkost vzduchu: 10 až 90 % (nekondenzující)

Dosah:

- Do 1,5km (v závislosti na umístění)

RF výkon (TX):

- 60 GHz: 14dBm
- 5GHz: 24dBm

RF výkon (RX):

- Zisk: 42dBi
- 60GHz: -74dBm@MCS1, -65@MCS5, -60dBm@MCS9
- 5GHz: -94dBm@MCS0, -64cBm@MCS15

Šířka pásma:

- 60GHz: 2GHz
- 5GHz: 80/40/20MHz

Další vlastnosti:

- Management VLAN
- Cloud kontrolér

4.3.2 Montáž a zaměření spoje

Montáž:

Jelikož anténa je citlivá na přesné zaměření, bylo nutností ji přidělat na pevný stožár pomocí držáku. Pro tento typ antény se vyrábí dva typy držáků – bez jemného doladění a s jemným doladěním, který byl použit právě pro svoji vlastnost na obou stranách spoje.

Zaměření:

Existují tři způsoby zaměření vysokofrekvenčního spoje s úzkým hlavním lalokem, které je potřeba vykonat všechny pro získání co nejlepších parametrů:

1. Zaměření od oka – provedeno při montáži
2. Zaměření dalekohledem – přiměřeně přesné zaměření antény namontovaným dalekohledem dodávaným výrobcem pomocí jemného ladění, kde výsledek lze pozorovat na Obr. 4.11, kde dalekohled míří přesně na protější rádio v zaměřovacím čtverci.

Obr. 4.11: Doladění pomocí dalekohledu – anténa Master

3. Zaměření pomocí zaměřovacího nástroje, skrze webové rozhraní rádia – Aiming Tool pomocí jemného ladění, díky kterému byl zaměřen spoj pro co nejlepší parametry. Porovnáním metod zaměření dalekohledem a pomocí nástroje Aiming Tool je zjištěn několikametrový rozdíl v zaměření spoje. Úroveň RSSI v Aiming tool při zaměření dalekohledem byla -70, po zaměření s Aimning tool -49.

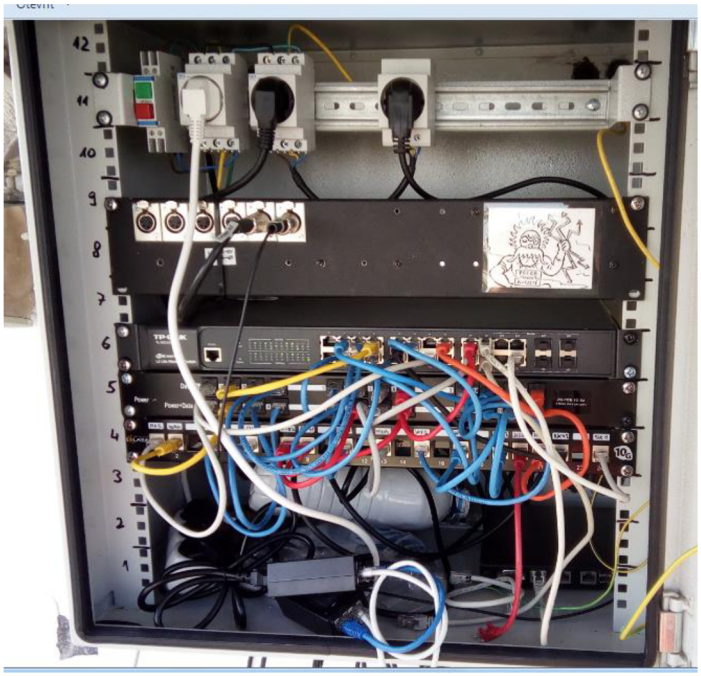
Obr. 4.12: Doladění rádia na straně Hotelu pomocí Aiming tool

K jemnému ladění se využívá dalších šroubů na držáku rádia, vyznačenými na Obr. 4.13, kde pomalým otáčením, dotáčíme anténu o několik stupňů. Pro vertikální ladění je nutné mít mírně povolené šrouby 1-4 a provádí se šroubem č. 5. Horizontální ladění se provádí šroubem č. 6. Při doladění je potřeba brát v potaz poslední dotažení, jelikož zde se může anténa trochu pohnout a můžeme získat ztrátu až několik dB, kvůli špatnému směrování rádia.

Obr. 4.13: Jemné doladění rádia s vyznačenými šrouby

4.3.3 Umístění Rack – Hotel Continental

V racku telekomunikačního operátora, jak je vyobrazeno na Obr. 4.14, je umístěn napájecí zdroj pro rádio Metrolinq Ignite a zdroj pro MT jsou umístěny 2x napájecí zdroj 2x Gigabit PoE pro napájení anténa Metrolinq a AP v 5 GHz pásmu MT-AP5GHz, pro připojení budovy C popsaném v kapitole 4.4.



Obr. 4.14: Rack telekomunikačního operátora na budově B – Hotel Kontinental

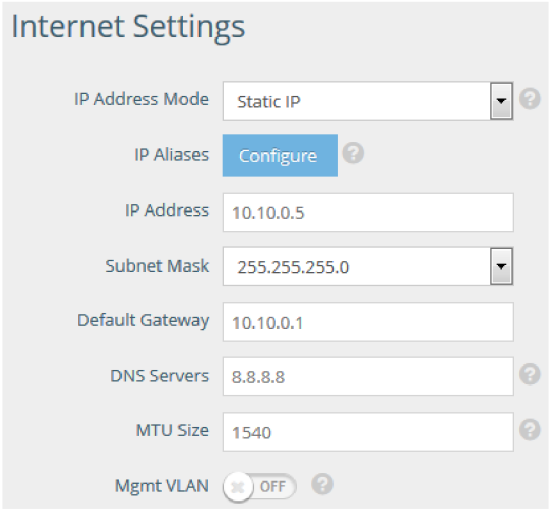
4.3.4 Konfigurace PTP spoje Metrolinq Ignite

Síťové rozhraní (Internetové):

Webová aplikace umožňuje konfiguraci statickou a dynamickou s podporou pouze IPv4. Byla zvolena konfigurace statická, což je možné vidět na Obr. 4.15, dle návrhu sítě v kapitole 4.1.1

a nastaveny příslušné adresy, včetně masky sítě a DNS. Velikost MTU je možné nastavit od 1400 do 7912 bytů, kde jsme ponechali defaultní nastavení 1540 bytů.

Další funkcí v konfiguraci síťového rozhraní je Mgmt VLAN (Management VLAN), jak je zobrazeno na Obr. 4.15. Funkce Mgmt VLAN slouží k zařazení nastaveného rozhraní zařízení do VLAN sítě, a tedy i komunikaci se zařízením skrze nastavenou VLAN síť. Standardně je tato možnost využita pro přístup k webové aplikaci skrze VLAN síť, kde výhodou může být, při výpadku komunikace routeru, dostupnost zařízení například přes VLAN switch.



Obr. 4.15: Konfigurace jednotky

Bezdrátové rozhraní 60 GHz (Wi-Fi):

V konfiguraci bezdrátového rozhraní v pásmu 60 GHz je možné volit, zda spoj, který sestavujeme je PTP, anebo PTMP a zda nastavovaná jednotka je Master, anebo Slave. Aby spoj byl funkční, je podmínkou, aby na jedné straně byla jednotka Master a na druhé Slave. U PTP spoje není až tak důležité, na které straně je která funkce, ale u PTMP je nutné mít na jednotce, ke které jsou připojeny další jednotky funkci Master. U realizovaného spoje byl volen Master na Hotelu a Slave na Šumavské.

Dostupné kanály v 60 GHz pásmu pro tuto jednotku, kde šířka kanálu je fixní na 2000 MHz (2 GHz) jsou:

- Kanál 1 – 58,32 GHz
- Kanál 2 – 60,48 GHz
- Kanál 3 – 62,64 GHz
- Kanál 4 – 64,80 GHz

Zvolen byl kanál 4 (64,80 GHz) z důvodu, že ze zjištěných informací se na budově Hotelu nachází další spoj v 60 GHz pásmu na kanále č. 1, který by mohlo mít teoreticky vliv na náš spoj. Ovládací rozhraní neumožňuje skenování kanálů pro zjištění rušení, což by nemuselo být až takovým problémem, protože použité antény jsou úzce směrové a využití pásma 60 GHz je prozatím v dnešní době minimální.

Název vysílané sítě SSID byl definován jako Bak60. Pro zabezpečení spoje pro připojení jednotky jsou možnosti:

- Bez zabezpečení
- WPA
- WPA2

Byla volena možnost Bez zabezpečení, jelikož právě pásmo 60 GHz je využívané minimálně a spoj byl sestavován pouze pro testovací účely.

MCS Rate (Modulation and coding set), neboli modulační a kódovací sada, slouží k volbě jednotlivých MCS 1-9, kde pro každý je definovaná jiná modulace s teoretickou přenosovou rychlostí, jak je možno vidět v Tab 4.1. Volbou konkrétního MCS, se nastaví napevno přenos. Pokud jednotky mají dostatečnou úroveň signálu a dostatečně přívětivé podmínky spoj pojede v pořádku i když by teoreticky mohl fungovat na vyšší rychlost. Pokud ale spoj má horší signál a špatné podmínky, kterými nedosáhne na dostatečné parametry voleného MCS, tak se rozpadá, je nestabilní a neumožňuje komunikaci. U tohoto spoje, jako i u dalších vysokofrekvenčních spojů jsou odchylky a pokud to jen jde, spoj se pokusí spojit i na menším MCS. Pro realizovaný spoj bylo voleno MCS auto, pro jeho flexibilnost a vhodnost použití při měření.

Tab 4.1: Volitelné možnosti MCS Rate

Název	Modulace	Teoretická rychlost Mbps
MCS1	BPSK	385
MCS2	BPSK	770
MCS3	BPSK	962,5
MCS4	BPSK	1155
MCS5	BPSK	1251,25
MCS6	QPSK	1540
MCS7	QPSK	1925
MCS8	QPSK	2310
MCS9	QPSK	2502,5

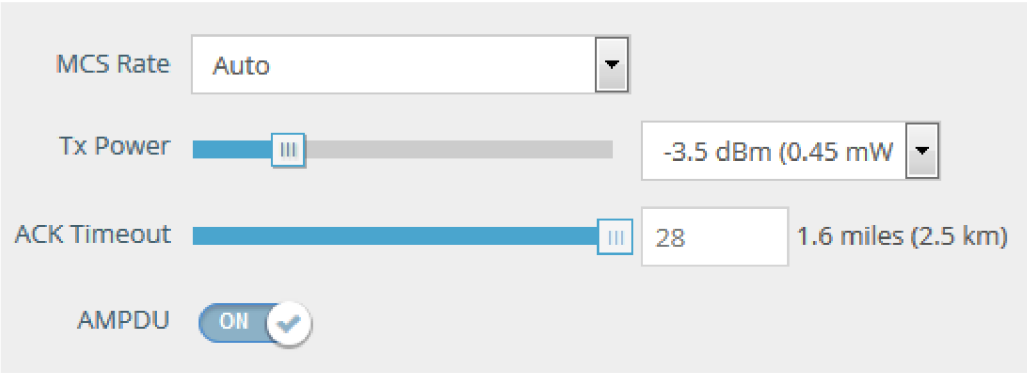
Vysílací výkon (Tx power) je možné regulovat od -8,5 dBm do 14 dBm, jak vidět v

Tab 4.2, kde k jednotlivým výkonům jsou přiřazeny hodnoty výkonu v miliwattech.

Tab 4.2: Volitelné možnosti výkonu

Výkon dBm	Výkon mW
14	25
11,5	14
9	7
6,5	4
4	2
1,5	1
-1	0,79
-3,5	0,45
- 6	0,25
- 8,5	0,14

Dalším nastavením je ACK Timeout, který má za úkol definovat maximální vzdálenost spoje a to hodnotami 10-28. Spoj byl realizován na vzdálenost 1,33 km, kde teoreticky by postačilo definovat hodnotu na 1,5km, ale protože bylo zjištěno při sestavování spojení již v minulosti, že je lepší volit vyšší hodnotu, tak automaticky byla volena maximální hodnota 28, což odpovídá maximální vzdálenost 2,5 km, jak je vidět na Obr. 4.16. AMPDU slouží k teoretickému navýšení rychlosti, díky snížení režijních dat, která je ve výchozím nastavení zapnutá.

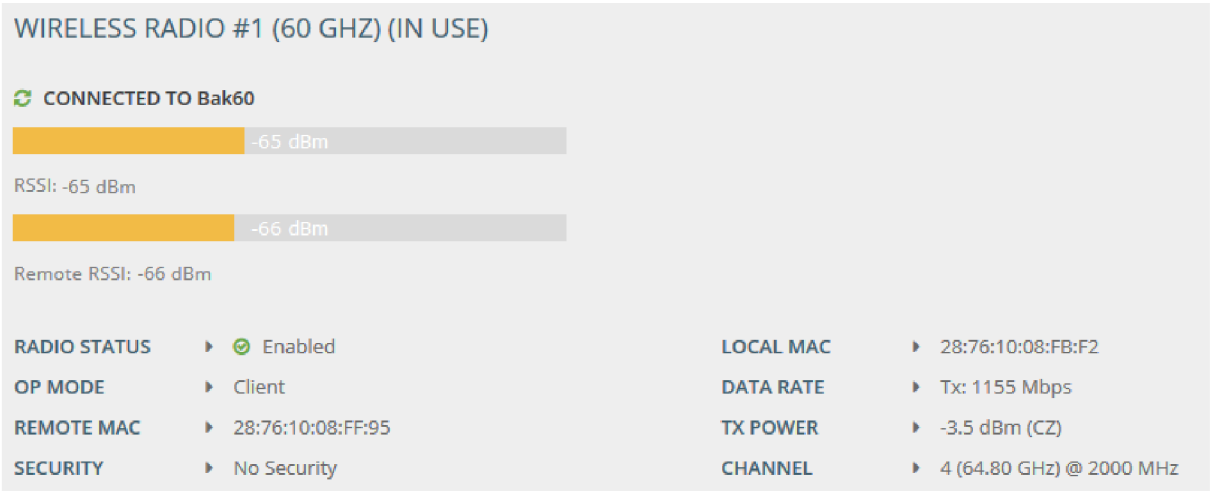


Obr. 4.16: Nastavení bezdrátové části rádia Metrolinq Ignite

4.3.5 Parametry sestaveného spojení

Spojení mezi budovami pomocí spoje Metrolinq Ignite bylo sestaveno s parametry, které

můžeme pozorovat na Obr. 4.17, s vysílacím výkonem -3,5 dBm, fixní šířkou kanálu 2000 MHz, na kanále č. 4 (64,80 GHz). Signál RSSI na straně klienta – budova A byl -48 dBm a na straně Mastera – budova B -50 dBm s teoretickou přenosovou rychlostí 2502,5/2502,5 Mb/s při nejvyšším možném MCS. Počasí při sestavování bylo pěkné, bez deště, nebo jiných nežádoucích a neočekávaných vlivů.



Obr. 4.17: Parametry 60GHz spojení ze strany rádia klient na budově A

4.3.6 Měření parametrů

Měření vlivu změny frekvence na signál

Změna frekvence u vysokorychlostních spojů může být problémem, a to primárně ve změně charakteristiky vysílacího diagramu – změnu směru vysílání hlavního laloku, až o několik stupňů. V tabulce jsou uvedeny hodnoty RSSI při změnách kanálu při zaměřeném spoji na kanále č. 4. V praxi změna kanálu může být nutná například při zarušení spoje. Je lepší se změně kanálů vyhnout, popřípadě je nutné spoj opět doladit.

Tab 4.3: Úroveň RSSI při změně kanálu

Kanál	Client RSSI	Master RSSI
4	-65	-66
3	-67	-69
2	Spoj rozpojen, nestabilní	
1	-67	-68

Test snižování výkonu na obou stranách z pohledu klienta:

Pro otestování chování spoje v 60 GHz pásmu byl spoj sestaven na vzdálenost, 1,33km s výkonem Tx Power -3,5 dBm dle legislativy, který v následujících měřeních budeme snižovat a zvyšovat pro obě strany spoje, viz Tab 4.4.

Tab 4.4: Měření úrovně RSSI, MCS a rychlostí při snižování výkonu na obou stranách spoje

Výkon	Client RSSI	Master RSSI	MCS	Teoretická rychlost Tx/Rx Mb/s	Změřená rychlost Tx/Rx Mb/s
14 dBm (25mW)	-48	-50	9/9	2502,5/2502,5	750/658
11,5 dBm (14mW)	-51	-53	9/9	2502,5/2502,5	710/587
9 dBm (7mW)	-54	-56	9/9	2502,5/2502,5	680/540
6,5 dBm (4mW)	-55	-57	9/9	2502,5/2502,5	569/518
4 dBm (2mW)	-58	-60	9/8	2502,5/2310	541/480
1,5 dBm (1mW)	-60	-62	9/7	2502,5/1925	528/440
-1 dBm (0,79 mW)	-63	-65	5/3	1251,25/962,5	490/398
-3,5 dBm (0,45 mW)	-65	-66	5/2	1155/770	483/187
-6 dBm (0,25 mW)	-67	-68	4/1	770/385	138/68
-8,5 dBm (0,14 mW)	-68	-69	1/1	385/385	25/1,05

Výsledkem měření je zjištění, že spoj se při poklesu signálu jedné strany na úroveň RSSI -69 začíná výjimečně rozpojovat, popřípadě dochází k většímu snížení teoretické a reálné rychlosti a při poklesu na -70 a více se již spoj rozpojuje a je nepoužitelný. Při hodnotách RSSI -48 až – 67 byl spoj stabilní.

Při dodržení legislativních podmínek, omezení vysílacího výkonu na 40 dBm ERIP, dle kapitoly č. je nastavený maximální vysílací výkon – 3,5 dBm. Při tomto výkonu lze dosáhnout stabilního spoje s průměrnými změřenými rychlostmi 483/187 Mb/s.

4.3.7 Diskutabilní 802.11ad

V případě spoje Metrolinq Ignite je diskutabilní, jestli se zařazuje do standartu 802.11ad. Výrobce a prodejci udávají u zařízení standart 802.11ad. Odborníci v ČR se dělí na dva skupiny s protichůdným názorem, primárně z důvodu dosahu. Na portálech a dokumentech jsou uváděny informace pro vzdálenost od jednotek metrů až po desítky, včetně uzavírání i neuzavírání maximální vzdálenosti. Jelikož praktické využití spoje Metrolinq Ignite je na vzdálenosti desítek až stovek metrů, je ho tedy možné považovat za zařaditelné do standartu 802.11ad.

4.4 PTMP spoj Mikrotik

Spojení budovy B Hotelu a budovy C Veveří 6 na vzdálenost cca 100 m bylo zvoleno zařízení společnosti Mikrotik pracující v 5 GHz pásmu, z důvodu dostatečných parametrů pro přenos dat.

4.4.1 Popis zařízení

Standart: 802.11n s využitím nv2 protokolu

Pásmo: 5GHz

AP – Mikrotik RB912UAG-5HPnD

Anténa citlivost: 15 dBi

Porty: 1x Gb/s

PTP spoj

Název: RB SXT 5HnD

Frekvence: 5 GHz

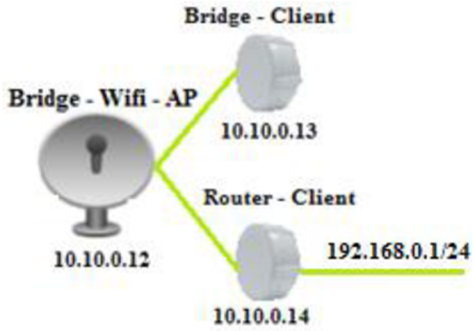
Zisk: 14 dBi

Maximální výkon: 30 dBm

Port : 1x 100 Mb/s

4.4.2 Konfigurace síťového rozhraní

Konfigurace síťového rozhraní na AP a dvou klientech, viz. obrázek Obr. 4.18, byla provedena obdobným způsobem jako konfigurace routeru, viz kapitola 4.2.2, jelikož se jedná o stejný systém RouterOS. Konfigurace byla provedena dle návrhu v kapitole 4.1.1,

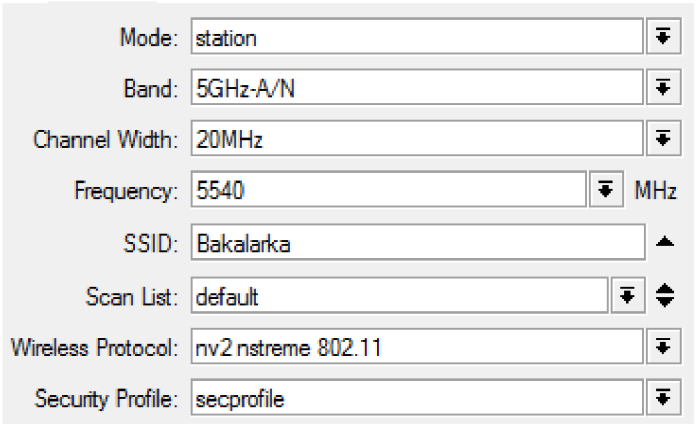


Obr. 4.18: Topologie sítě PTMP spoje v pásmu 5 GHz s IP adresací

4.4.3 Konfigurace bezdrátového rozhraní

U konfigurace bezdrátového rozhraní, viz obrázek Obr. 4.19, je důležitá volba kanálu a jeho šířky. Jelikož realizovaný spoj PTMP byl sestaven v městě, tak konfigurace bezdrátového rozhraní byla provedena nadvakrát. Poprvé dle odhadu byl zvolen kanál, dle odhadu a splnění legislativních podmínek pro bezdrátové spoje ve venkovním prostředí. Šířka kanálu byla volena na 20 MHz jak nejužší kanál. Když byl spoj sestaven mezi budovami, byly skenovány další sítě a úroveň signálu, jak na straně klienta, tak i AP, které mohou rušit spoj. Ze skenu, který je vyobrazen na Obr. 4.20 byl vybrán kanál s frekvencí 5540 MHz, jelikož úroveň signálu ostatních sítí na stejném či blízkém kanálu byla nejmenší.

Název SSID byl volen „Bakalarka“ s podporou 802.11a/n a security profile byl vytvořen s WPA/WPA2 Personal s heslem „bakalarka223“ a nv2 protokol popsaný v kapitole 2.8.



Obr. 4.19: Konfigurace bezdrátového rozhraní klientské strany

UPC Wi-Free	5500/20-Ceee/ac	-77
UPC34ED29D	5500/20-Ceee/ac	-77
internety500	5500/20-Ceee/ac	-79
UPC Wi-Free	5500/20-Ceee/ac	-80
UPC Wi-Free	5500/20-Ceee/ac	-83
UPC1A4E5C8	5500/20-Ceee/ac	-83
UPC Wi-Free	5500/20-Ceee/ac	-84
Pohadkova_WiFi	5500/20-Ceee/ac	-85
UPC Wi-Free	5500/20-Ceee/ac	-85
666net1	5500/20-Ceee/ac	-85
UPC504729898	5500/20-Ceee/ac	-89
Brandlova	5500/20/ac	-79
CZFree.Net.Lidicka	5540/20-Ce/an	-75
AjMdaN	5540/20/a	-75
Bakalarka	5540/20/an	-50
UPC Wi-Free	5560/20-eeeC/ac	-75
private residence	5560/20-eeeC/ac	-75
UPC Wi-Free	5560/20-eeeC/ac	-85
yolo	5560/20-eeeC/ac	-86
test25	5560/20/a	-88
typocapku	5580/20-Ce/an	-88

Obr. 4.20: Sken ostatních sítí při výběru vysílacího kanálu

4.4.4 Sestavení spojení

Montáž a zaměření spoje v 5 GHz pásmu je jednodušší než ve vyšších pásmech, díky širšímu hlavnímu laloku antén a lepším vlastnostem průchodu signálu prostředím. Zaměření antén se provádí primárně pomocí velikosti úrovně signálu sestaveného spojení. U klientského zařízení bridge se podařilo dosáhnout úrovně signálu -49/-50 dBm, viz obrázek Obr. 4.21 a u routeru -52/-54 dBm viz obrázek Obr. 4.22.

Hodnota CCQ (Client Conection Quality) nám ukazuje kvalitu sestaveného spojení. CCQ u spojení PTMP bylo použitelné pro dostatečnou rychlost přenosu, s ohledem, že spoj je realizován ve městě, kde rušení je velké.

Status	connected to ess
AP MAC	E4:8D:8C:01:27:3E
Network Name	Bakalarka
Tx/Rx Signal Strength	-49/-50 dBm
Tx/Rx CCQ	89/90 %

Obr. 4.21: Parametry sestaveného spojení PTMP spoje, strana bridge

Status	connected to ess
AP MAC	E4:8D:8C:01:27:3E
Network Name	Bakalarka
Tx/Rx Signal Strength	-52/-54 dBm
Tx/Rx CCQ	85/89 %

Obr. 4.22: Parametry sestaveného spojení PTMP spoje, strana routeru

4.4.5 Měření

Měření byla provedena pro ověření rychlosti v málo rušeném a rušeném prostředí, kde rušení bylo pozorována primárně na hodnotě CCQ.

Tab 4.5: Měření reálné přenosové rychlosti v málo rušeném kanále, bridge CCQ 89/90 %, router CCQ 85/89 %

Název měření	Rychlost stahování Mb/s	Rychlost nahrávání Mb/s
Měření reálné rychlosti mezi AP a bridgem	43	48
Měření reálné rychlosti mezi AP a routerem	38	42
Měření reálné rychlosti mezi bridgem a routerem	25	28

Tab 4.6: Měření reálné přenosové rychlosti v rušeném kanále, bridge CCQ 29/20 %, router CCQ 35/22 %

Název měření	Rychlost stahování Mb/s	Rychlost nahrávání Mb/s
Měření reálné rychlosti mezi AP a bridgem	14	8
Měření reálné rychlosti mezi AP a routerem	13	10
Měření reálné rychlosti mezi bridgem a routerem	5	6

V dalším měření bylo provedeno srovnání Nv2 a Nstreme v zarušeném prostředí. Protokol Nv2 byl již použit při měření vlivu rušení na CCQ.

Tab 4.7: Měření reálné přenosové rychlosti v rušeném kanále a vlivu Nv2 a Nstreme, bridge CCQ 25/9 %, router CCQ 28/14 %

Název měření	Rychlost stahování Mb/s	Rychlost nahrávání Mb/s
Měření reálné rychlosti mezi AP a bridgem - Nstreme	9	8
Měření reálné rychlosti mezi AP a routerem - Nstreme	7	9
Měření reálné rychlosti mezi bridgem a routerem - Nstreme	4	3

Výsledkem měření je zjištění, že kvalita spojení je velmi ovlivněna rušením v 5 GHz bezlicenčním pásmu. Z měření vlivu CCQ na rychlost a vlivu protokolu Nv2 a Nstreme na CCQ a reálnou přenosovou rychlost lze usuzovat, že mají přiměřený vliv a je vhodné použít Nv2 který je vyvíjen společností Mikrotik, zatím co Nstreme není plně akutalizován. Spoje byly sestaveny v centru města, kde rušení v 5 GHz pásmu je velké a jeho použití vyžaduje správnou konfiguraci protokolu, výkonu, a především výběr kanálu, který je nejméně zarušen a zároveň splňuje legislativní podmínky České republiky.

5 ZÁVĚR

Cílem této práce bylo seznámit se s problematikou lokálních bezdrátových sítí určených pro pokrytí jak vnitřních, tak vnějších prostor a legislativou spojenou s provozem těchto sítí. V rámci teoretické části byla rozebrána elektromagnetická vlna, skrze kterou se přenáší datový signál, její samotný přenos a zpracování. Dále byl rozebrán vztah legislativy České republiky k frekvenčnímu využití pásma a povolenému vysílacímu výkonu a výpočet a práce s výkonem. Rozebrány byl provoz WLAN sítí, IP adresace s protokoly a službami na ní běžící.

V rámci praktické části bakalářské práce byly realizovány dvě Wi-Fi sítě dle standardu 802.11, které byly navrženy z praktického hlediska i s připojením do sítě Internet. V rámci 2,4 GHz sítě bylo navrženo a otestováno řešení pokrytí objektu a venkovního areálu Wi-Fi sítí s více SSID a možností omezení datového toku jak pro jednotlivé zařízení, tak i pro skupiny zařízení. V rámci venkovní bezdrátové sítě byl otestován spoj v 60 GHz pásmu na vzdálenost 1,33 km, kde se změnou výkonu bylo pozorován pokles teoretické rychlosti a měřena skutečná rychlost spoje. V případě 60 GHz spoje s ohledem na legislativu a dodržení maximálního vysílacího výkonu EIRP byly naměřeny průměrné hodnoty přenosové rychlosti 483/187 Mb/s. Pro dosáhnutí plného potenciálu zařízení bylo nutné zvýšit výkon. Vhodnou alternativou je využití rádiových spojů mimo standard 802.11 například nelicencovaném 10 GHz, 24 GHz nebo 80 GHz pásmu. Další částí venkovní sítě byl spoj PTMP s dvěma klientskými zařízeními, kde byl otestován vliv rušení na přenos a možnost využití protokolů Nstreme a nv2 pro větší odolnost spoje. Při použití protokolu Nv2 a volbě nejméně rušeného kanálu se podařilo dosáhnout rychlostí 43/48 pro zařízení bridge a 38/42 Mb/s pro router. Rozdíl těchto rychlotí dvou zařízení na stejnou vzdálenost je dán rozdílem signálu a složitostí operace NAT definované na routeru.

LITERATURA

[1] Z. Long, X. Song, L. Zhang, Y. Xiao: Design and Implementation of Wireless Local Area Network Videophone, Advances in Intelligent and Soft Computing, vol 133. Springer, Berlin, Heidelberg, 2012, ISBN: 978-3-642-27551-7.

[2] Campus LAN and Wireless LAN Design Guide, Cisco Validated Design [online], 2016, [cit: 2017-10-01] Dostupné z: www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-Campus-LAN-WLAN-Design-2016OCT.pdf

[3] BEČVÁŘ, Zdeněk, P. MACH a I. PRAVDA. *Mobile networks*. Prague: Czech Technical University, 2013. ISBN 978-80-01-05306-5.

[4] Všeobecné oprávnění č. VO-R/12/09.2010-12 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu. Portál ctu.cz [online]. 29.9.2010 [cit. 10.11.2017]. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2010/vo-r_12-09_2010-12.pdf

[5] MILAN, Klement. *Technologie bezdrátových sítí - základní principy a standardy* [online]. Křížkovského 8, 771 47 Olomouc: Univerzita Palackého v Olomouci, 2017 [cit. 2018-05-29]. ISBN 978-80-244-5156-5, dostupné z https://www.researchgate.net/publication/316987268_Technologie_bezdratovych_siti_-_zakladni_principy_a_standardy

[6] *Introduction to the Domain Name System* [online], 8 [cit. 2018-05-29]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_registrar/9-0/dns/guide/DNS_Guide/DNS_Guide_chapter_00.pdf

[7] INTERNATIONAL TELECOMMUNICATIONS UNION. *Radio regulations*. Edition of 2012. Geneva: ITU, 2012. ISBN 9789261140212.

[8] SAMEK, Martin. *Linux Days 2014 - Není WiFi jako WiFi* [online]. 6.10.2014 [cit. 2018-05-29]. Dostupné z: https://www.youtube.com/watch?v=ChfCr0A79rY

[9] *Webinář Alternetivo – vysokokapacitní wifi* [online]. 20.10.2015 [cit. 2018-05-29]. Dostupné z: https://youtu.be/1VBsKbaYo5g

[10] HANUS, CSC., Doc. Ing. Stanislav. *Bezdrátové a mobilní komunikace*. , 135. ISBN 80–214–1833 –8.

[11] *Jak zabezpečit WiFi síť* [online]. [cit. 2018-05-29]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-zabezpecit-wifi

[12] I4WIFI A.S. *Jak na instalaci WLAN* [online]. [cit. 2018-05-29]. Dostupné z: https://files.i4wifi.cz/inc/_doc/Pdf/wlan-info-01-cz.pdf

[13] PETERKA, Jiří. *Rodina protokolů TCP/IP* [online]. 2013, 10 [cit. 2018-05-29]. Dostupné z: http://www.earchiv.cz/l225/gifs/TCPIPv3_5print.pdf

[14] MIKROTIK. *NAT* [online]. [cit. 2018-05-29]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT

[15] MIKROTIK. *Nv2* [online]. [cit. 2018-05-29]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Nv2

[16] *Elektromagnetické vlny – Vlnová délka* [online]. [cit. 2018-05-29]. Dostupné z: https://pixabay.com/p-1526374/?no_redirect

[17] *Elektromagnetické spektrum* [online]. [cit. 2018-05-29]. Dostupné z: http://www.wikiwand.com/cs/Elektromagnetick%C3%A9_spektrum

[18] OK1PD. *Šíření rádiových signálů* [online]. 2006 [cit. 2018-05-29]. Dostupné z: http://www.crk.cz/SIRENIC

[19] RACOM S.R.O. *Implementační poznámky* [online]. [cit. 2018-05-29]. Dostupné z: http://www.racom.eu/cz/products/m/ray/calcul.html

[20] *Comparsion of QAM* [online]. [cit. 4.11.2017]. Dostupné z: https://www.headendinfo.com/32qam-64qam-128qam-256qam/

[21] *Binary Phase Shift Keying (BPSK) Modulation* [online]. [cit. 2018-05-29]. Dostupné z: http://www.evalidate.in/lab2/pages/BPSK-mod/BPSK/BPSK_I.html

[22] JOHN (YA). *M-QAM Bit Error Rate in Rayleigh Fading* [online]. 2012 [cit. 2018-05-29]. Dostupné z: http://www.raymaps.com/index.php/m-qam-bit-error-rate-in-rayleigh-fading/

[23] COMA S.R.O. *Standard 802.11ac* [online]. 28.2.2016 [cit. 2018-05-29]. Dostupné z: http://www.raymaps.com/index.php/m-qam-bit-error-rate-in-rayleigh-fading/

[24] *Elektromagnetické vlnění* [online], 8 [cit. 2018-05-29]. Dostupné z: https://www.e-fyzika.cz/kapitoly/24-elektromagneticke-vlneni.pdf

[25] *IEEE 802.11* [online]. 23.5.2018 [cit. 2018-05-29]. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.11

[26] *Vlastnosti elektromagnetického vlnění* [online]. [cit. 2018-05-29]. Dostupné z: https://sps-cl.cz/public/MatFyz/Soubory/Fyzika/10_elmg_zareni/vlastnosti_elmg_vln.htm

[27] *Here Comes Multi-Gigabit Wi-Fi* [online]. 05.05.2014 [cit. 2018-05-29]. Dostupné z: http://www.blog.beldensolutions.com/here-comes-multi-gigabit-wi-fi/

[28] *Internet of things--from hype to reality*. New York, NY: Springer Berlin Heidelberg, 2016. ISBN 978-3-319-44858-9.

[29] *IEEE 802.11ac Migration Guide* [online]. 05.05.2014 [cit. 2018-05-29]. Dostupné z: https://enterprise.netscout.com/content/white-paper-ieee-80211ac-migration-guide

[30] *802.11ac Channelization* [online]. [cit. 2018-05-29]. Dostupné z:

http://rfmw.em.keysight.com/wireless/helpfiles/n7617/Content/Main/802.11ac%20Channelization.htm

[31] *Firewall* [online]. [cit. 2018-05-29]. Dostupné z: http://home.zcu.cz/~afrouzov/

SEZNAM POUŽITÝCH ZKRATEK, VELIČIN A SYMBOLŮ

AES	Advanced Encryption Standard
AMPDU	Aggregated MAC Protocol Data Unit
AP	Access Point
ASCII	American Standard Code for Information Interchange
ASK	Amplitude-shift keying
BPSK	Binary-Phase Shift Keying
DFS	Dynamic Frequency Selection
DNS	Domin Name System
EIRP	Equivalent Isotropically Radiated Power
MAC	Media access control
MIMO	Multiple-input and multiple-output
MT	Mikrotik
MTU	Maximum transmission unit
NAT	Network address translation
RSSI	Relative received signal strength
SSID	Service set identifier
VLAN	Virtual LAN
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fiber
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

SEZNAM PŘÍLOH

Tab A. 1: Seznam masek sítě [29]..... 65

PŘÍLOHA Č.1 – SEZNAM MASEK SÍTĚ

Tab A. 1: Seznam masek sítě [29]

Prefix	Počet IP	Použitelné IP	Maska sítě
/4	268435456	268435454	240.0.0.0
/5	134217728	134217726	248.0.0.0
/6	67108864	67108862	252.0.0.0
/7	33554432	33554430	254.0.0.0
/8	16777216	16777214	255.0.0.0
/9	8388608	8388606	255.128.0.0
/10	4194304	4194302	255.192.0.0
/11	2097152	2097150	255.224.0.0
/12	1048576	1048574	255.240.0.0
/13	524288	524286	255.248.0.0
/14	262144	262142	255.252.0.0
/15	131072	131070	255.254.0.0
/16	65536	65534	255.255.0.0
/17	32768	32766	255.255.128.0
/18	16384	16382	255.255.192.0
/19	8192	8190	255.255.224.0
/20	4096	4094	255.255.240.0
/21	2048	2046	255.255.248.0
/22	1024	1022	255.255.252.0
/23	512	510	255.255.254.0
/24	256	254	255.255.255.0
/25	128	126	255.255.255.128
/26	64	62	255.255.255.192
/27	32	30	255.255.255.224
/28	16	14	255.255.255.240
/29	8	6	255.255.255.248
/30	4	2	255.255.255.252