VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

# DIPLOMOVÁ PRÁCE

Brno, 2018 Bc. Adam Labuda


# 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


# ROAMING VE WIFI SÍTÍCH
ROAMING IN WIFI NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS


AUTOR PRÁCE
AUTHOR

Bc. Adam Labuda

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Ondřej Krajsa, Ph.D.



BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

# Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

***Student:*** Bc. Adam Labuda ***ID:*** 158182
***Ročník:*** 2 ***Akademický rok:*** 2017/18

**NÁZEV TÉMATU:**

## Roaming ve WiFi sítích

**POKYNY PRO VYPRACOVÁNÍ:**

Analyzujte možnosti roamingu u technologií 802.11. Porovnejte možnosti sítě VUT založené na prvcích HP a Vámi realizované sítě s prvky Mikrotik. Navrhněte a proveďte testování roamingu v těchto sítích.

**DOPORUČENÁ LITERATURA:**

[1]GAST, Matthew. 802.11 wireless networks: the definitive guide. 2nd ed. Sebastopol: O´Reilly, 2005, xxi, 630 s. : il. ISBN 978-0-596-10052-0

[2]CHI, Kuang-Hui, Chien-Chao TSENG a Ya-Hsuan TSAI. Fast Handoff among IEEE 802.11r Mobility Domains. Journal of Information Science and Engineering [online]. 2010, 26(4), 1345-1362 [cit. 2017-10-11]. DOI: 10.6688/JISE.2010.26.4.12. ISSN 1016-2364.

***Termín zadání:*** 5.2.2018 ***Termín odevzdání:*** 21.5.2018

***Vedoucí práce:*** Ing. Ondřej Krajsa, Ph.D.
***Konzultant:***

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

## ABSTRAKT

Táto práca sa zoberá problematikou roamingu vo WiFi sieťach. Preberá možnosti z pohľadu 802.11 štandardu. Možnostiach továrenských nastavení prvkov s rýchlim roamingom od firmy MikroTik a porovnaní s VUT siete z prvkov Hewlett-Packard. Navrhuje meranie a testovanie týchto sietí. Následne namerané výsledky zhodnotí.

## KĽÚČOVÉ SLOVÁ

802.11, 802.11a, 802.11g, 802.11h, 802.11n, 802.11ac, 802.11r, Beacon rámce, Probe rámce, Kanály 802.11, BSS, ESS, Asociácia, Aktívne a pasívne skenovanie, Fázy roamingu, Lokálny roaming, Globálny roaming, VUT, Hewlett-Packad, MikroTik, CAPsMAN

## ABSTRACT

This work deals with roaming issues in the WiFi network. Takes options from a 802.11 standard view. Factory setting options for fast roaming from MikroTik and BUT Brno network with Hewlett-Packard devices. It proposes to measure and test these networks. At the end is discusion about measured results.

## KEYWORDS

802.11a, 802.11g, 802.11g, 802.11n, 802.11n, 802.11n, 802.11n, 802.11n, 802.11n, 802.11n, 802.11n, 802.11n, Beacon frames, Probe frames, 802.11b, , BUT, Hewlett-Packard, MikroTik, CAPsMAN

LABUDA, Adam *Roaming vo WiFi sieťach*: diplomová práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2018. 77 s. Vedúci práce bol Ing. Ondřej Krajsa, Ph.D.

# PREHLÁSENIE

Prehlasujem, že som svoju diplomovoú prácu na tému „Roaming vo WiFi sieťach“ vypracoval(a) samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ..... .....

podpis autora(-ky)

# POĎAKOVANIE

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Ondřejovi Krajsovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.


Brno ..... .....

podpis autora(-ky)


Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

## POĎAKOVANIE

Výzkum popsaný v tejto diplomovej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

podpis autora(-ky)


EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

# OBSAH

# ZOZNAM OBRÁZKOV

# ZOZNAM TABULIEK

# ÚVOD

V dnešnom rýchlom modernom svete je nutné byť stále informovaný. Existujú rôzne prúdy informácií, ten najznámejší a najčastejšie používaný je Internet. Sieť zariadení, ktoré medzi sebou zdieľajú rôzne informácie. Pripojiť sa do tejto obrovskej siete dnes nie je problém. Máme smart telefóny, počítače, tablety a iné zariadenia pomocou, ktorých sa do siete dokážeme pripojiť. Tieto zariadenia sa stali vďaka modernizáciou doby pomerne prístupné každému. Ako sa svet posúva ďalej, vznikali nové a nové možnosti ako túto veľkú sieť zvanú Internet posúvať ďalej. Od klasických Ethernet káblov po optické siete, od EDGE po LTE, princípom je stále zvyšovať rýchlosť. Čo sa pred desiatkami rokov zdalo snom, je dnešnou realitou. Čo je dnes vrchol, zajtra nemusí byť. Kladú sa čoraz väčšie nároky a kto ich nesplní vypadáva z hry. Ruku v ruke ide aj pripojenie k Internetu. Samotné pripojenie nie je zložité, väčšinou ide o sadu rovnakých úkonov opakujúcich sa pre každé pripojenie. Po pripojení sa stávame súčasťou siete. Môžeme uploadovať, sťahovať súbory, informácie, aplikácie podľa nášho uváženia. Problém môže nastať ak sa chceme so zariadením pohnúť na iné miesto a zároveň ostať pripojený. Tento, na prvý pohľad jednoduchý úkon je omnoho zložitejší než sa môže zdať. Zariadenie je pripojené k prístupovému bodu a svojím pohybom sa dostane mimo dosah. Tým pádom postupne stráca signál, pripojenie. Túto situáciu možno vyriešiť tak, že sa po jeho ceste umiestnia ďalšie prístupové body. Koncové zariadenie následne preskočí z jedného prístupového bodu na druhý, bez toho aby došlo k viditeľnému prerušeniu komunikácie. Tento úkon sa volá roaming. Tejto problematike sa venujem v následujúcich sekciách práce. Na začiatok preberiem základy roamingu, následne preberiem riešenia u rôznych výrobcov, navrhnem riešenie a následne zmeriam parametre vytvorenej siete. Namerané hodnoty zapíšem do výsledkov merania, ktoré následne porovnám.

# 1 TEORETICKÁ ČASŤ ŠTUDENTSKEJ PRÁCE

## 1.1 Základy WiFi

WiFi je technológia, ktorá využíva rádiové vlny na prenos dát, respektíve pripojenie do siete. Názov je skratkou „Wireless Fidelity“ čo v doslovnom preklade zanemená bezdrôtová vernosť. Spojenie je možné pomocou bezdrôtového adaptéra, ktorý vytvorí prístupový bod vysielaný vďaka anténe. Následne tento vysielaný signál príjme koncové zariadenie vďaka sieťovej karte a pripojí sa. WiFi pracuje vo frekvenciách 2.4GHz a 5GHz podľa nastavenia. Táto technológia sa rýchlo rozšírila a umožnila väčšie pokrytie a zrýchlenie pripojenia. WiFi vychádza zo štandardu IEEE 802.11. Normy v IEEE projekte sú zamerané na fyzickú vrstvu a MAC (Medium Acess Control). V dobe, kedy bola WLAN (Wireless Local Area Network) vytváraná, zdalo sa, že bude ďalšou súčasťou fyzickej vrstvy už vytvorených štandardov. Prvým štandardom, ktorý sa zvažoval použiť bol najvýznamnejší štandard IEEE 802.3 a to teda Ethernet. Čoskoro bolo zrejmé, že rádiový prenos je veľmi odlišný od klasického drôtového. Z dôvodu obrovského útlmu na krátku vzdialenosť, detekciu kolízie nebolo možné použiť ako u drôtového prenosu. Preto nebolo možné použiť tento štandard. Ďalšia zvažovaná norma bola 802.4, ktorá funguje na princípe Token Ring. Avšak bolo zrejmé, že predávanie a prideľovanie Tokenu bude pri bezdrôtovom prenose obzvlášť náročná. Po neúspešných pokusoch IEEE zaviedlo samostatný štandard pre WLAN. Svetlo sveta uzrel v roku 1997 ako prvý 802.11 štandard. Na najnižšej fyzickej vrstve poskytuje frekvenčné skoky (FHSS), priame sekvenčné rozloženie spektra (DSSS). Na začiatku prenosová rýchlosť nebola tak vysoká ako dnes, 802.11 poskytovala len 1-2 Mb/s. Podobne ako u 802.3, základ 802.11 funguje na systéme listen-before-talk známi ako distribučná koordinačná funkcia (DCF). Implementuje viacnásobný prístup s vyhýbaním sa kolízii (CSMA/CA). Keďže kolíziu pri prenose nemožno zistiť v rádiovom prostredí, 802.11 čaká určitý interval pred vysielaním rámca. Toto je rozdiel od CSMA/CD kde interval čakania nastáva až po kolízii nie pred [1].

Po uverejnení 802.11 časom prišla spätná väzba. Zákazníci očakávali väčšiu kompatibilitu než v realite dostali. Napríklad správne nefungovala kryptovacia schéma WEP medzi zariadeniami rôznych výrobcov. Potreba pre odstránenie problémov viedla k vytvoreniu certifikovanom programu a vytvorenie WECA v roku 1999, premenovaná v roku 2003 na WiFi Alliancia (WFA). Stovky spoločností spolupracujú s týmto programom aby vyrábali zariadenie, ktoré odpovedajú aktuálnym normám[2].

### 1.1.1 802.11a/g/h

Prvé rozšírenie projektu 802.11 sa začalo v Septembri 1997. Dostalo názov 802.11a. Jeho hlavným prínosom bolo ortogonálny frekvenčný multiplex (OFDM), ktorý podporoval prenos až 54Mbit/s. 802.11a operuje v pásme 5GHz. V pásme 5GHz vytvára 12 samostatných neprekrývajúcich sa kanálov. Vďaka tomu môžete mať 12 prístupových bodov nastavených na každom kanáli bez toho aby sa medzi sebou rušili. Toto rozdelenie kanálov napomáha k výrazne vyššiemu prenosu, ktorú dokáže bezdrôtová sieť poskytnúť. Rušenie vysokofrekvenčného pásme je menej pravdepodobné kvôli menšiemu preplneniu. Problém nastáva ak chcem komunikovať napríklad so štandardmi 802.11b a 802.11g.. Tento dôležitý nedostatok viedol k vytvoreniu 802.11g štandardu, ktorý priniesol OFDM aj do pásam 2,4GHz. Vzhľadom na to, že poskytuje techniku priameho rozprestretého spektra (DSSS) bolo jednoduché prejsť z 802.11 na 802.11g[3].

Ide o rozšírenie 802.11b čo tvorí základ pre dnešné bezdrôtové siete. S vlastným paketovým binárnym konvolučným kódom (PBCC) boli podporované dátové rýchlosti 22Mbit/s a 33Mbit/s. Dnes zriedka používaný kód nastavil štandard a stal sa voliteľnou moduláciou a kódovacou schémou 802.11g. Ide o tretí modulačný štandard pre bezdrôtové siete. Pracuje v pásme 2,4GHz a s maximálnym prenosom 54Mbit/s. Použitím CSMA/CA maximálna prenosová rýchlosť sa pohybuje okolo 31Mbit/s pre pakety o veľkosti 1500bajtov. V praxi, prístupové body nemusia mať ideálnu implementáciu a preto nemusia byť schopné dosiahnuť tohto prenosu. Pakety o veľkosti 1500bajtov sú v sieti najpoužívanejšie, preto sa rýchlosti porovnávajú s týmto údajom. Menšie pakety poskytujú ešte menšiu teoretickú rýchlosť prenosu, pri 64bajtovom pakete okolo 3Mbit/s. Tento štandard je plne kompatibilný s 802.11b hardvérom [1], [3]

V záujme splnenia Európskych regulačných požiadavkou pre pásmo 5GHz, vytvorilo IEEE v roku na konci 2003, štandard 802.11h. Tento protokol rieši problémy ako rušenie satelitov a radarov v rovnakom 5GHz pásme. Tento štandard využíva

dynamický výber frekvencie (DFS) a riadenie výkonu vysielania. DFS detekuje ostatné zariadenia. Ktoré používajú rovnaký rádiový kanál a v prípade potreby prepne na iný kanál. Týmto princípom sa zabraňuje rušeniu s inými zariadeniami ako sú radarové a iné systémy. Prístupový bod iniciuje zmenu kanálu poslaním všetkým staniciam, ktoré sú s sním spojené a identifikuje nový kanál, kedy zmena nastane a či je možné komunikovať pred zmenou kanálu. Stanice, ktoré dostali správu o zmene kanálu, prepnú na nový po uplynutí času stanoveným prístupovým bodom [4].

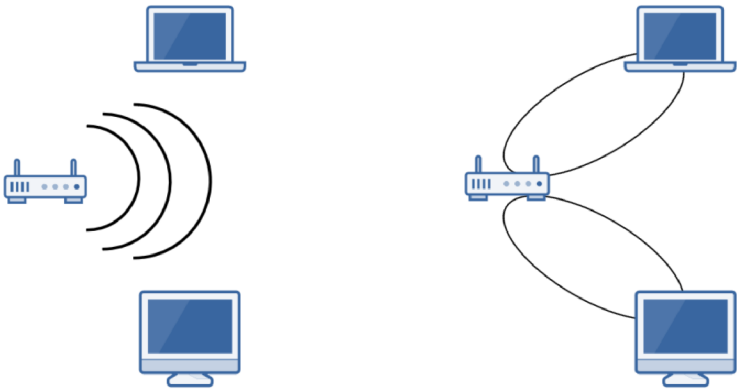
### 1.1.2 802.11n

Ide o normu pre bezdrôtové siete, ktoré používajú viacej antén pre zvýšenie dátových rýchlostí. Jeho najvýznamnejšou vlastnosťou je viacnásobný vstup a výstup (MIMO). Cieľom je zvýšiť rýchlosť prenosu predchádzajúcich dvoch štandardov 802.11a a 802.11g z 54Mbit/s na 600Mbit/s s použitím štyroch prenosov na kanále 40MHz. MIMO je technológia, ktorá využíva viac antén pre súvislé rozposlanie informácií než pri používaní jednej antény. Používa na to priestorové multiplexovanie (SDM), ktoré priestorovo multiplexuje viacero nezávislých dátových tokov, prenášaných súčasne v rámci jedného spektrálneho kanálu. Pri využívaní SDM môže výrazne zvýšiť prenos dát, pretože počet rozdelených samostatných dátových tokov sa zvyšuje. Táto technológia pre svoje fungovanie vyžaduje samostatný rádiofrekvenčný reťazec a analógovo-digitálny prevodník pre každú anténu zvlášť čo spôsobuje, že je finančne drahšia. Štandardizovaná podpora MIMO, zoskupenie rámcov a bezpečnostné vylepšenia a ďalšie vylepšenia. Môže byť využitá v 2,4GHz alebo 5GHz pásme. Problém môže nastať pri zvolení pracovného pásma na 2,4GHz, kde pri využívaní 40MHz pásma dochádza k rušeniu Bluetooth alebo ZigBee a iných zariadení [5].

### 1.1.3 802.11ac

Tento štandard vypĺňa návrhy, ktoré spĺňajú požiadavky Medzinárodnej telekomunikačnej únie (ITU) [6], [7]. Zaujímavosťou je, že medzi štandardom 802.11n a 802.11ac je šesť ročný rozdiel, to v technike zanemená doslova nekonečný čas čakania na vylepšenie štandardu 802.11n. Nie je prekvapenie, že teda prináša vysokú prenosovú rýchlosť viac ako 1Gbit/s pre pásma menšie 6GHz. Rozšírenie šírky pásma 40MHz, 80MHz a 160MHz. Kanál 160MHz je zložený z dvoch 80MHz kanálov, ktoré nemusia spolu susediť. Kanály 80MHz a 40MHz sa skladajú z dvoch susediacich frekvencii 40MHz a 20MHz. Podpora pásma 40MHz a 80MHz je povinná zatiaľ čo pásmo 160MHz je voliteľné. Technológia MIMO podporuje až osem prenosov čo je dva krát viac ako u štandardu 8702.11n. Podporovanie tohto štandardu systémom, umožňuje

kontinuálny prenos HD videa pre viacerých účastníkov v domácnosti, rýchlu synchronizáciu a zálohovanie veľkých dátových súborov či funkciu bezdrôtového displeja v reálnom čase. Ďalšou špecifikáciou tohto štandardu je vysielanie. To funguje na princípe vytvárania lúča. Zaradenie zistí kde sa v priestore koncový užívateľ nachádza a tým smerom vysiela, namiesto toho, aby vysielalo signál rovnomerne do všetkých smerov ako je zobrazené na obrázku 1.1.



Obr. 1.1: 802.11ac vytvorenie lúča

### 1.1.4 802.11r

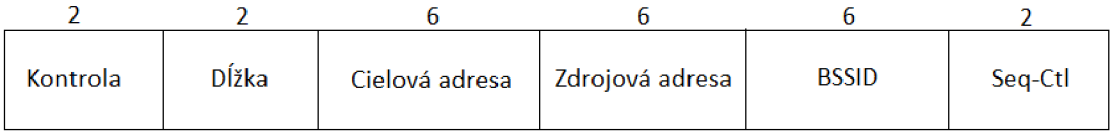
Tento štandard tiež známi ako rýchly roaming. Umožňuje nepretržitú konektivitu pre bezdrôtové zariadenia v pohybe, ktoré menia prístupové body počas svojej cesty. Na začiatku štandardu 802.11 boli autorizácie jednoduchšie. Na vytvorenie spojenia medzi koncovou stanicou a prístupovým bodom boli potrebné iba štyri správy, kroky. Postupom času sa pridávali nové a nové bezpečnostné štandardy, ktoré autorizačné kroky zvyšovali. Pokiaľ neprebehnú všetky kontrolné a autorizačné správy prenos dát nemôže byť uskutočnený. V niektorých podmienkach toto overovanie môže trvať aj niekoľko sekúnd, čo v prípade prenosu v reálnom čase môže spôsobiť výpadky. Štandard 802.11r bol vytvorený preto, aby tieto overenia dokázal zrýchliť. To dokáže pomocou rýchleho BSS prenosu. Tento mechanizmus umožňuje obnoviť už existujúce bezpečnostné parametre a pripojiť koncové zariadenie k novému prístupovému bodu. Vďaka tomu dokáže zrýchliť znovu pripojenie k prístupovému bodu v rámci jednej siete. Ak sa chceme pripojiť do inej siete, samozrejme musíme prejsť všetky kroky overenia lebo sa pripájame do „cudzej“ siete [8].

## 1.2 Základy štandardu 802.11

Priblížime si situáciu, kedy nadväzovať spojenie bude jedno koncové zariadenie a jeden prístupový bod [10]. Niektoré 802.11 manažment rámce sú dôležité pre základné pochopenie vytvorenia a udržania spojenia medzi koncovým zariadením a prístupovým bodom. Sú to tieto rámce:

- Beacons
- Probes
- Asociačné požiadavky
- Asociačné odpovede

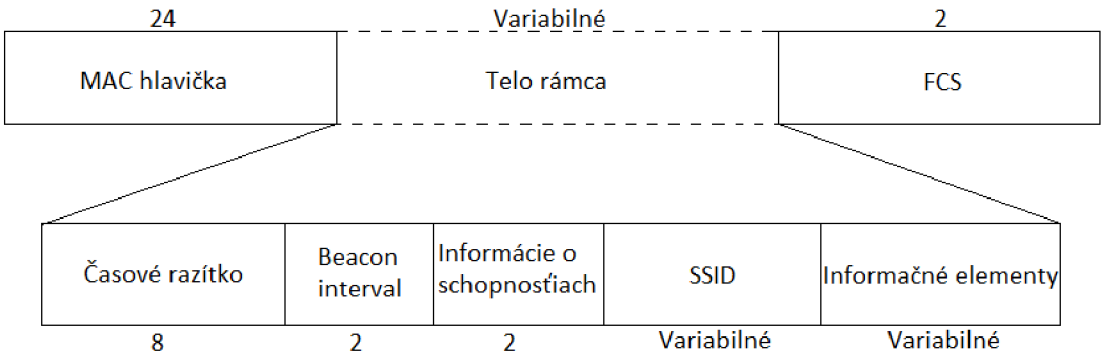
Všetky tieto rámce sú zakomponované na začiatku 802.11 MAC hlavičke ako je zobrazené na obrázku 1.2. Táto hlavička má šesť polí obsiahnutých v 24 bajtoch. Dva bajty sú na ovládanie rámca a dva bajty na dobu trvania. Po tých nasleduje šesť bajtov reprezentujúci cieľovú adresu a ďalších šesť bajtov reprezentujúcich zdrojovú adresu. Nasledujúcich šesť bajtov je venovaných základnému ID súboru služieb o ktorom budem hovoriť neskôr. Posledné dva bajty sú pre sekrečné riadenie. Všetky riadiace rámce končia dvomi bajtmi nazývanými sekvencia kontroly rámcov (FCS), ktoré sa používajú na kontrolu chýb.




Obr. 1.2: Hlavička 802.11

### 1.2.1 Beacons a Probes rámce

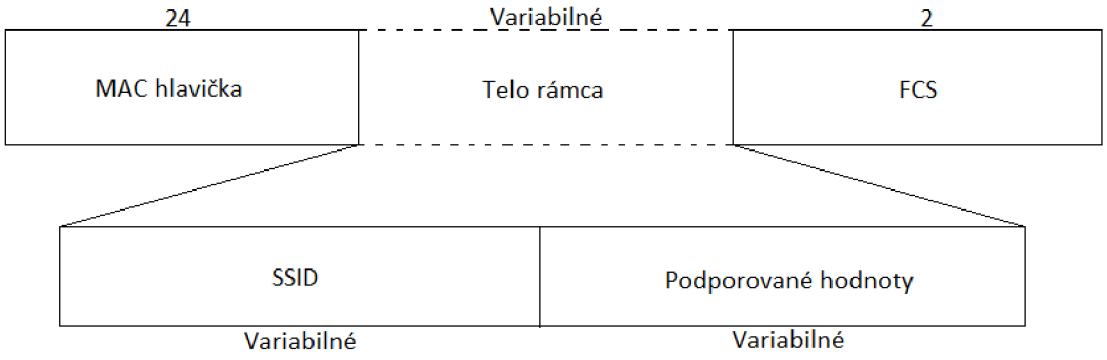
Beacon a Probes rámce sú dve samostatné mechanizmy prostredníctvom, ktorých sa koncové zariadenie môže dozvedieť o existencii prístupového bodu pracujúceho v danom kanáli. Je jedno či sa používajú Beacon alebo Probe rámce, dôležité je či je vybrané aktívne alebo pasívne skenovanie. Rámce Beacon sú vysielané prístupovým bodom aby ukázali svoju existenciu v danom kanáli. Informácie o spôsobilosti sú tiež zahrnuté v tomto rámci. Na obrázku 1.3 sú ukázané základné komponenty rámca Beacon. Všimnite si, že podobne ako aj hlavičky MAC všetkých ostatných riadiacich rámcov 802.11 predchádza telo rámca.




Obr. 1.3: Beacon rámec

Vidíme, že Beacon rámec nesie časovú počiatku vo veľkosti ôsmich bajtov, dvojbajtový interval, pole s informáciami o schopnosti a voliteľne dlhé pole so servisným set identifikátor (SSID) prístupového bodu vytvárajúceho Beacon rámec. Zbierka informačných prvkov zahrnutých v Beacon rámci sa v závislosti od možností a konfigurácie prístupového bodu výrazne líšia od ostatných.

Iba prístupové body prenášajú beacon rámce pokiaľ boli tak nastavené. V niektorých sieťach s cieľom urobiť war-driving je to trošku zložitejšie. Prístupové body sú nakonfigurované aby neposkytovali Beacon rámce. Ak prístupový bod nevysiela rámce Beacon, tento prístupový bod môže byť objavený pomocou výmeny Probe žiadostí a Probe odpovedí. Zatiaľ čo aktívne skenovanie je nevyhnutné pre objavenie prístupového bodu, ktoré nevysiela Beacon rámce. Aktívne skenovanie sa niekedy používa aj pri vysielaní Beacon rámcov pre zrýchlené zistenie či sú dostupné prístupové body v danom kanále. Rozloženie rámca Probe žiadosť je zobrazený na obrázku 1.4.




Obr. 1.4: Rámec Probe žiadosť

Pole SSID v tele rámca slúži na určenie, ktorý SSID požaduje koncové zariadenie. Tieto Probe žiadosti môžu vysielať na rôznych kanáloch, kým nebude prístupový bod načúvať na určitom kanále. Pole SSID má premennú dĺžku rovnako ako nasledujúce pole. Keď prístupový bod príjme Probe rámec na kanáli, na ktorom počúva, odpovie rámcom Probe odpoveď. Tento rámec je skoro identický ako Beacon rámec. Táto podoba je spôsobená tým, že rámce slúžia na rovnaký účel a to na propagáciu vysielacieho prístupového bodu. Rozdiel je v tom, že Beacon rámec je proaktívne vysielaný prístupovým bodom zatiaľ čo probe odpoveď je vyžiadaná koncovým zariadením [11].

### 1.2.2 Kanály v 802.11

Základným princípom architektúry bunkovej komunikácie je zvýšenie celkového využitia danej podmnožiny rádio frekvenčného spektra tým, že sa viacerým bunkám v rovnakej sieti umožní opätovne využiť rovnaká frekvencia alebo skupiny frekvencií. Táto technika vyžaduje aby bunky používali odlišné frekvencie od blízkych susedov ako aj obmedzený prenosový výkon. Tieto dva princípy uľahčujú opätovné používanie frekvencii v bunkových systémoch a tým aj zvýšenú agregovanú rádio frekvenčnú účinnosť týchto systémov. Aby sa zabezpečila vysoká odolnosť vysokofrekvenčnej signalizácie v rádio frekvenčnom spektre, v porovnaním s mnohými faktormi rušenia. Norma 802.11 špecifikuje použitie prenosu v rozprestretom spektre. S cieľom zabezpečiť rádio frekvenčnú signalizáciu, ktorá je veľmi robustná, táto technika bola implementovaná roky dozadu pre armádne ciele. Existujú tri technológie rozšíreného spektra, ktoré sa používajú v komerčne dostupných 802.11 zariadeniach. Sú to tieto:

- Frekvenčné skákanie (FH) používané v začiatkoch 802.11 štandardu
- Priame sekvencie (DS) používané v 802.11 štandarde
- Ortogonálne frekvenčne delený miultiplex (OFDM) používané v 802.11a a 802.11g štandarde

Pri metóde frekvenčné skákanie je užívateľský signál prenášaný cez set frekvencií. V každom okamihu sa signál prenáša iba na podskupinu množiny frekvencií, ktoré sú k dispozícii pre prenos. Vysielače a prijímače sú znalé kódu frekvenčného skákania, to dovoľuje vysielaču a prijímaču zosynchronizovať frekvencie, ktoré sa používajú v určitom časovom bode a vedieť kedy dôjde k prepnutiu na ďalšiu podmnožinu frekvencií.

Pri metóde priamej sekvencie je úzko pásmový signál rozložený na relatívne širokom frekvenčnom pásme a spätne získaný z tohto širokého pásma pomocou prijímača. Rozširovanie sa uskutočňuje pomocou matematickej transformácie signálu

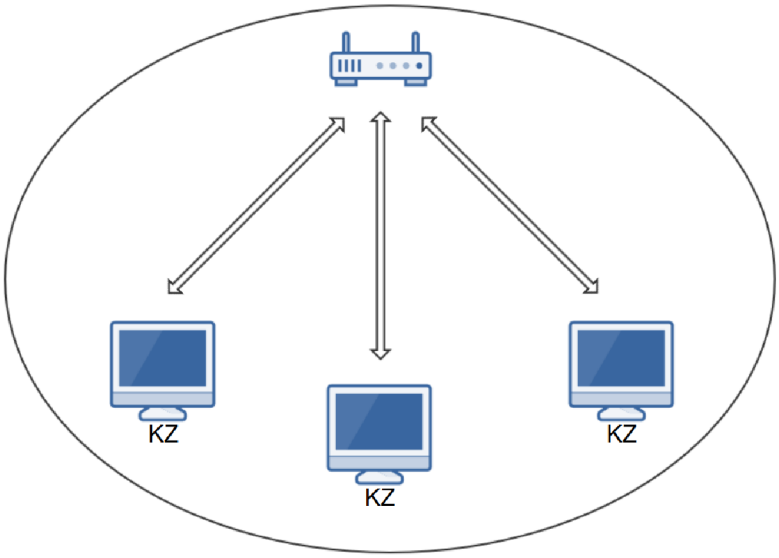
použitím numerického sekvenčného čipu na pôvodný signál. Sekvencia je tiež používaná u prijímačov na obnovenie signálu. Číselná sekvencia čipovania je binárny reťazec a niekedy sa nazýva aj pseudonáhodný šumový kód.

V prípade OFDM je široko frekvenčné pásmo použité na vysielanie, rozdelené na podkanály. Pojem prevádzkový kanál sa používa na rozlíšenie čísel kanálu, na ktoré odkazuje používateľ z podkanálov, ktoré tvoria prevádzkový kanál. Pôvodný prenos je kódovaný do týchto podkanálov, ktoré pracujú paralelne.

Štandard 802.11b DS má na fyzickej vrstve celkovo štrnásť kanálov aj keď nie všetky sa používajú. V spojených štátoch sú povolené iba kanály 1 – 11, v Európe sú to kanály 1-13. Každý kanál má šírku 5MHz a všetky sú v pásme 2,4GHz. Kanál 10 je dostupný vo všetkých hlavných regulačných doménach, často je to predvolený operačný kanál. V Prostredí s viacerými prístupovými bodmi by sa kanály v susediacich bunkách nemali prekrývať, aby sa minimalizovala interferencia. Tento požiadavok sa rieši pri umiestňovaní a nastavovaní prístupových bodov v priestore. V prípade DS používaného v 802.11b sú k dispozícií iba tri neprepúšťajúce kanály, 1, 6 a 11. Použitie týchto kanálov v 802.11b sa stalo štandardom. Štandard 802.11a s OFDM technológiou má na fyzickej vrstve 12 kanálov. Sú číslované 36, 40, 44, 48, 56, 60, 64, 149, 153, 157 a 161. Každý kanál má šírku pásma 20MHz a je v pásme 5GHz. Dostupnosť dvojitého režimu 11a/11g či dokonca trojitého režimu 11a/11b/11g čipov účinne zvýšila výber kanálov pri stanovení topológie buniek.

### 1.2.3 Služba Basic Servie Set (BSS)

V štandarde 802.11 táto technológia združuje skupinu koncových zariadení a prístupových bodov, ktoré komunikujú medzi sebou. V nezávislom BSS, ktorý sa tiež označuje ad hoc 802.11 sieť, stanice priamo komunikujú navzájom skôr ako prostredníctvom prístupového bodu. Takéto siete sa tiež nazývajú peer to peer. Siete v režime infraštruktúry, ktoré ovládajú všetky známe aplikácie a inštalácie štandardu 802.11, pozostávajú z infraštruktúry BSS. BSS označuje jediný prístupový bod a všetky koncové zariadenia, ktoré s týmto bodom komunikujú. Prístupové body a koncové zariadenia v BSS komunikujú na rovnakom 802.11 kanále. MAC adresa prístupového bodu sa používa na identifikáciu BSS a nazýva BSSID. Príklad je zobrazený na obrázku 1.5, kde vidíme tri koncové zariadenia (KZ) komunikujúce cez jeden prístupový bod. Service set ID (SSID), ktoré sme videli v kapitole vyššie, je názov skupine alebo jednému prístupovému bodu, ktoré poskytuje bezdrôtový prístup v danej podsieti IP.

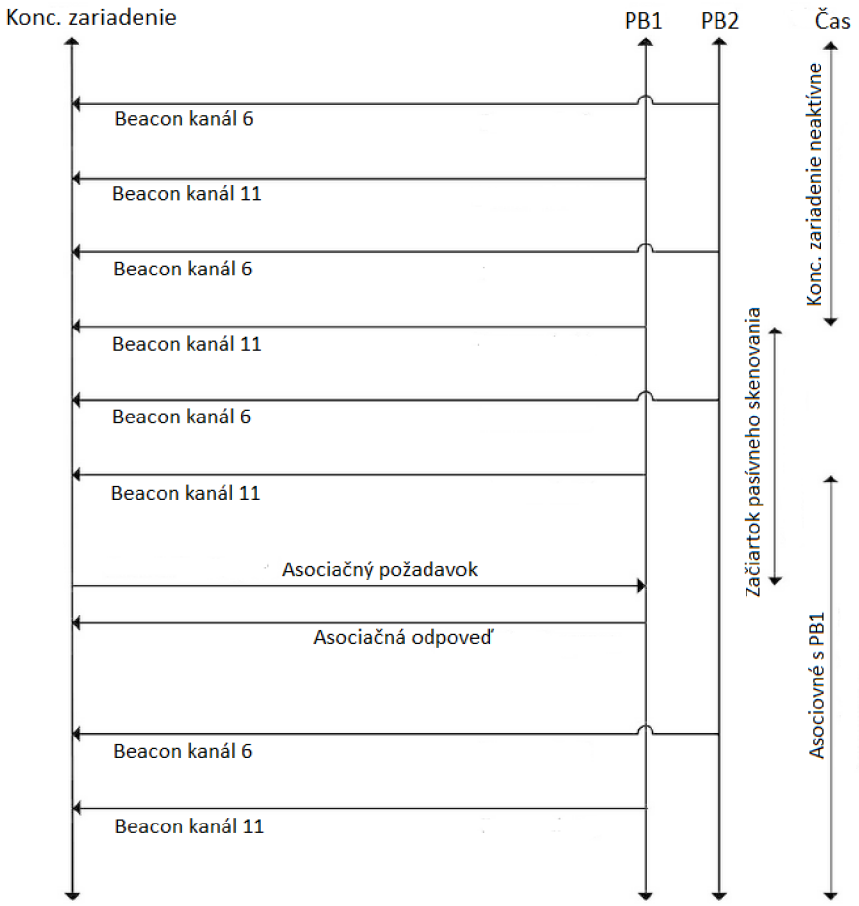



Obr. 1.5: BSS

### 1.2.4 Aktívne a pasívne skenovanie

Pri pasívnom skenovaní bude koncové zariadenie iteračne počúvať na všetkých dostupných kanáloch. Počas počúvania príjme koncové zariadenie beacon rámce od prístupového bodu s SSID. Koncové zariadenie zaznamená SSID, ktoré identifikuje. Je typické aby koncové zariadenie prijalo beacon rámce od prístupových bodov, ktoré vysielajú rôzne SSID ako aj rôzne prístupové body vysielajú rovnaké SSID. Na obrázku 1.6 sú dva prístupové body. Skratka PB1 a PB2 predstavujú prístupový bod 1 a 2.

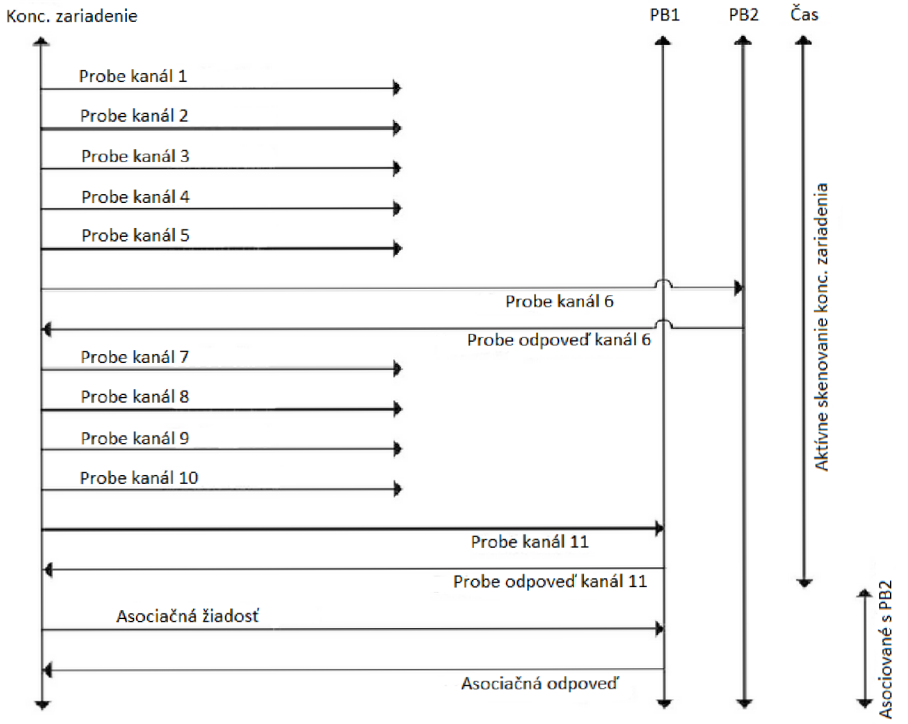
Proces odosielania rámca beacon pokračuje nezávisle na stave koncového zariadenia. V príklade vidíme, že koncové zariadenie začne pasívne skenovať v polovici diagramu. Napríklad začiatok pasívneho skenovania môže zodpovedať užívateľovi, ktorý povolí používanie 802.11 karty na zariadení. Toto skenovanie priamo nevedie k prenosu akýchkoľvek rámcov preto sa nazýva pasívne skenovanie. Počas tohto štádia, koncové zariadenie zhromažďuje informácie z prijatých beacon rámcov, jeden na kanáli 6 a druhý na 11. Pomocou týchto rámcov sa koncové zariadenie dozvie kanály, ktoré používa prístupový bod 1 a 2, identifikátor SSID, identifikátor o schopnostiach a informačné elementy. Ak toto koncové zariadenie chce vstúpiť do BSS jednej z týchto prístupových bodov, musí postupovať podľa asociačných krokov, ktoré preberám v kapitole Asociácia. Na obrázku 1.6 sa chce pripojiť ku prístupovému bodu 2, čo má za následok výmenu žiadostí a odpovedí. Aj keď je koncové zariadenie spojené s prístupovým bodom 2, beacon rámce sa stále vysielajú pretože, aktívne vysiela kvôli ďalším zariadeniam.




Obr. 1.6: Pasívny sken

Proces aktívneho skenovania sa líši od pasívneho tým, že koncové zariadenie aktívne vyhľadáva identifikátor SSID ku, ktorému sa chce pripojiť. Pre každý kanál, ktorý je aktívne skenovaný musí koncové zariadenie načúvať, aby predišlo kolízií, odoslať probe rámec a nakoniec počúvať určitý časový úsek či nepríde odpoveď alebo beacon rámec. Za účelom objavenia prístupového bodu s použitím konkrétneho SSID, vysielajú sa probe žiadosti na kanáli, ktoré sú k dispozícii pre koncové zariadenie, kým nezareaguje prístupový bod s rovnakým SSID ako má probe žiadosť. Probe žiadosť môže špecifikovať SSID vysielanie, v takomto prípade ide o wildcard probe na ktorú môže hocijaký prístupový bod reagovať. Wildcard probe sa tiež nazývajú nepriame probes rámce. Proces aktívneho skenovania je na obrázku 1.7.

Prvých päť probe rámcov nevedie k zodpovedajúcemu SSID identifikátoru. Probe žiadosti na kanáli 6 vedú k zhode na prístupovom bode 2, ten odpovie probe odpoveďou. Probe žiadosti na kanáloch 7 až 10 nevedú k zhode avšak probe žiadosť na kanáli 11 áno. Je to zhodný kanál vysielaný prístupovým bodom 1 a nastane to isté ako pri kanáli 6. Koncové zariadenie potom požiada o pridruženie, asociáciu k

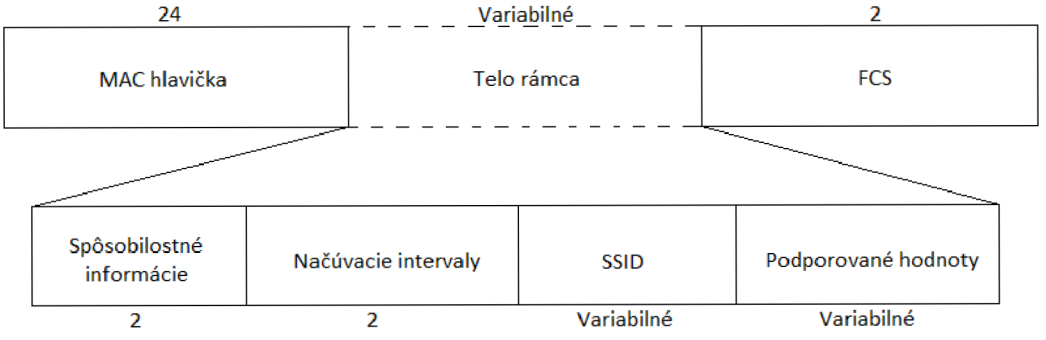



Obr. 1.7: Aktívny sken

prístupovému bodu 1 ten odošle asociačnú odpoveď.

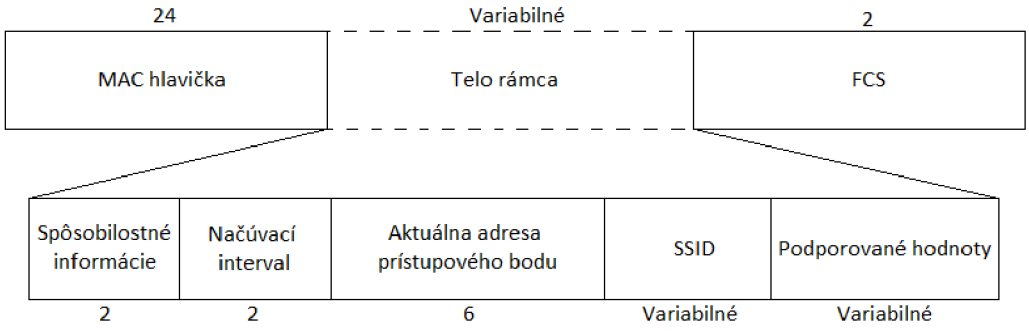
### 1.2.5 Asociácia

Keď koncové zariadenie identifikuje prijateľný prístupový bod, bude mať tendenciu asociovať sa s BSS tohto prístupového bodu odoslaním asociačnej žiadosti. Formát tohto rámca je na obrázku 1.8.



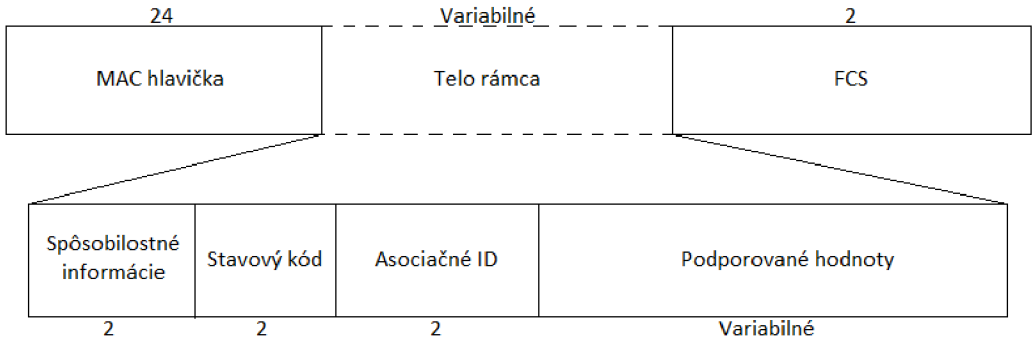

Obr. 1.8: Asociačná žiadosť

Rámec má dva bajty pre informácie o schopnostiach, dva bajty pre interval načúvania, SSID pole s premenlivou dĺžkou a pole s hodnotami rýchlostí. Rámec so žiadosťou reasociácie je na obrázku 1.8, ktorý je podobný ako asociačná žiadosť.




Obr. 1.9: Reasociačná žiadosť

Tento rámec sa používa keď koncový bod bol spojený s prístupovým bodom s rovnakým SSID, s ktorým sa koncové zariadenie pokúša spojiť. Rámec obsahuje dodatočné informácie, konkrétne šesť bajtov pre aktuálnu, teda starú adresu prístupového bodu. Táto informácia je potrebná pre dokončenie procesu handover, pripojenie sa k novému prístupovému bodu. Keď prístupový bod obdrží reasociačnú žiadosť, môže ho prijať alebo odmietnuť. Ak zvolí prijatie tejto žiadosti, zašle reasociačnú odpoveď vo forme, aká je na obrázku 1.8.



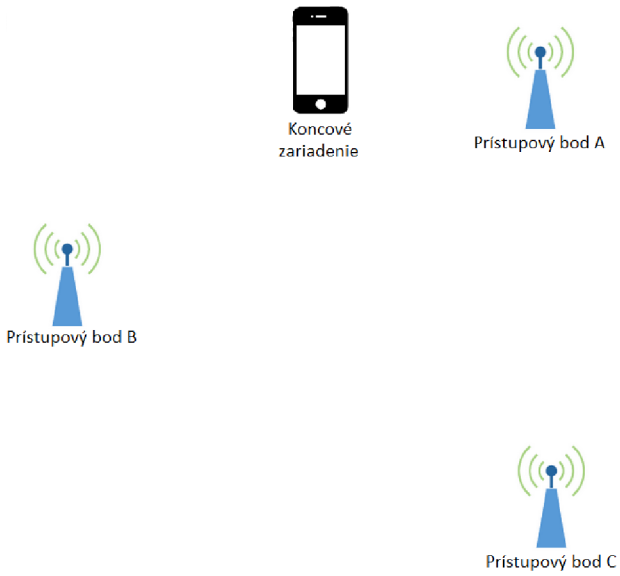

Obr. 1.10: Reasociačná odpoveď

Obsahuje dva bajty pre informácie o schopnostiach, dva bajty pre stavový kód, dva bajty pre asociačné ID a variabilnú dĺžku pre podporované hodnoty. V skutočnosti predtým ako sa koncové zariadenie spojí s prístupovým bodom, musí sa autentifikovať s prístupovým bodom, čo zahŕňa výmenu aspoň dvoch rámcov. Táto výmena musí nastať pred asociáciou, no vždy tak nemusí byť. To znamená, že autentifikácia môže nastať hocikedy pred asociáciou.

Počet autentifikačných rámcov pri výmenných pred asociáciou závisí od toho, aký režim autentifikácie sa používa. Ak sa používa zabezpečenie WEP, autentifikácia prebehne vo výmene štyroch rámcoch.

## 1.3 Základné vlastnosti roamingu

Ako som už spomenul v kapitolách hore, bezdrôtová sieť sa časom mení a zdokonaľuje. Princíp ale ostáva rovnaký [12]. Základom roamingu je teda proces odpojenia a pripojenia k novému prístupovému bodu. Tento proces sa zdá na prvý pohľad jednoduchý a v skutočnosti zaberie v ideálnom prípade pár milisekúnd je omnoho komplexnejší. Počas týchto milisekúnd musí koncové zariadenie rozhodnúť ku akému prístupovému bodu a pripojí, to býva na základe najsilnejšieho vysielaného signálu. Následne prebieha autorizácia a kontrola zo strany prístupového bodu. Primárne rozhodnutie o zmene prístupového bodu je len na koncovom zariadení, ktoré vydá pokyn k zmene. Toto rozhodnutie je vďaka mechanizmu, ktoré je zabudované v operačnom systéme zariadenia alebo v ovládači WiFi karty. Zároveň záleží aký operačný systém alebo WiFi kartu používame. Koncové zariadenie v periodických intervaloch zostavuje zoznam okolitých prístupových bodov a ich kvalitu resp. signál. Situáciu si môžeme popísať na obrázku 1.11.




Obr. 1.11: Rozloženie PB a KZ

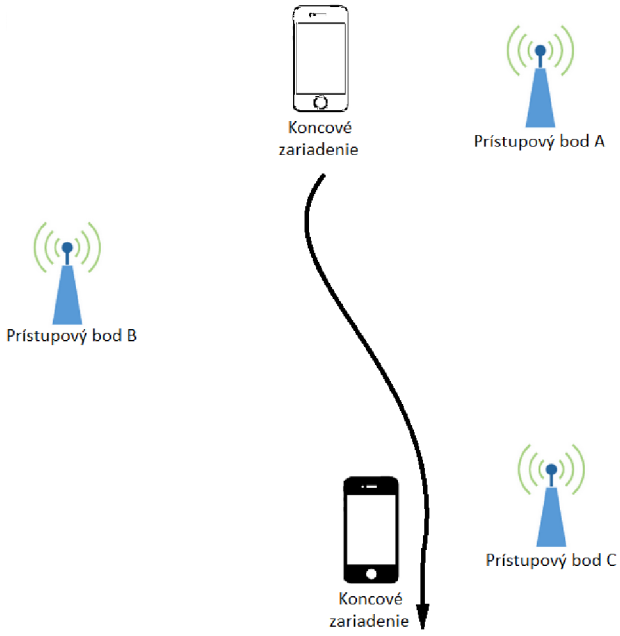
Koncové zariadenie sa nachádza v prostredí kde vysielajú tri prístupové body. Zoberme ideálny prípad, kedy nebudeme rušení okolím a nastavenie prístupových

bodov bude urobené tak aby boli všetky v tabuľke koncového zariadenia. Zjednodušená zoznam okolitých prístupových bodov bude vyzerať nasledovne tabuľky 1.1

| Identifikátor | Sila signálu |
|---|---|
| A | -50dBm |
| B | -60dBm |
| C | -75dBm |

Tab. 1.1: Zoznam príszupových bodov so silou signálu

Z tabuľky je teda evidentné, že najsilnejší signál má prístupový bod A. Zariadenie sa teda pripojí k tomuto bodu. Čo sa stane, ak sa koncové zariadenie začne hýbať smerom nadol obrázku 1.12




Obr. 1.12: Koncové zariadenie v pohybe

Samozrejme, aj tabuľka okolitých prístupových bodov sa zmenní podľa aktuálnej polohy koncového zariadenia. Zoznam bude vyzerať ako tabuľky 1.2.

Z tabuľky 1.2 je jasné, že lepší signál má prístupový bod C. Koncové zariadenie teda začne meniť pripojenie na kvalitnejšie.

| Identifikátor | Sila signálu |
|---|---|
| A | -75dBm |
| B | -65dBm |
| C | -50dBm |

Tab. 1.2: Zoznam príszupových bodov po pohybe koncového zariadenia

Pokiaľ kvalita aktuálneho prístupového bodu, teda bodu ku ktorému je zariadenia pripojené klesne pod určitú úroveň, zariadenie sa teda pripojí k aktuálne najkvalitnejšiemu prístupovému bodu v zozname. Táto úroveň sa samozrejme mení a záleží od toho, ako silné prístupové body sa v zozname nachádzajú. V podstate ak signál klesne pod určitú úroveň nie je vždy nutné sa pripájať ku najlepšej sieti v zozname ak táto sieť nie je dostatočne silná. Tento algoritmus funguje na týchto princípoch. Pre reálnu predstavu uvediem zjednodušený príklad:

1. Každých 50sekúnd vyhľadávaj signály okolitých prístupových bodov
2. Ak signál aktuálnej siete plesne pod -70dBm, nájdi v tabuľke najlepší signál prístupového bodu
3. Ak má kandidát lepší signál o 7dBm, pripoj sa na neho

Do tohto algoritmu vstupujú aj iné externé faktory ako napríklad rozmiestenie prístupových bodov a ich sila signálu. Ak umiestnime viac prístupových bodov v blízkosti s maximálnym výkonom signálu, bude dochádzať k rušeniu. Keďže prístupové body nie sú dobre rozmiestené budú teda pracovať na maximálny signál, bude dochádzať ku vzájomnému rušeniu a k výpadkom komunikácie čo nám ani tento algoritmus nedokáže vyriešiť. Správne rozmiestenie prístupových bodov a nastavenie sily signálu ale nemusí vždy zaručiť rýchly roaming z jedného prístupového bodu na druhý. Hlavnou podstatou je používanie správnych štandardov, ktoré som spomínal vyšiel.

Vysvetlili sme si ako roaming vníma koncové zariadenie. To je iba zlomok z procesov, ktoré zabezpečia kompletný roaming. Poďme sa pozrieť aké procesy nastávajú na strane prístupového bodu. Procesy, ktoré nastanú po tom ako sa koncové zariadenie rozhodne zmeniť prístupový bod môžeme nazvať handover. V literatúre sa môžeme stretnúť aj s názvami handoff alebo 4-way-handshake čo v preklade znamená štvorbodovú autorizáciu. Je dôležité nezabudnúť aj na úroveň zabezpečenia siete. Pre nezabezpečenú sieť roaming nepredstavuje žiadne overovacie procesy. Zariadenie sa jednoducho pripojí bez väčších problémov. Samozrejme nastane výmena údajov medzi koncovým zariadením a prístupovým bodom, no v skutočnosti neprebehne nijaké zložité overovanie prístupu. V realite sa stretávame väčšinou so zabezpeče-

nými prístupovými bodmi, preto sa nebudem tejto situácii venovať do hĺbky. Naopak pre zabezpečenú sieť, overovanie zariadenia a prístupu tvorí základ tejto problematiky. Cieľom je toto overovanie zrýchliť na čo najmenší čas, aby prenos dát nebol ovplyvnený.

Najčastejšie bezpečnostné riešenia prístupových bodov sú tieto:

1. WPA/WPA2-PSK (Pre-Shared Key)
2. WPA/WPA2-EAP (Extensible Authentication Protocol)

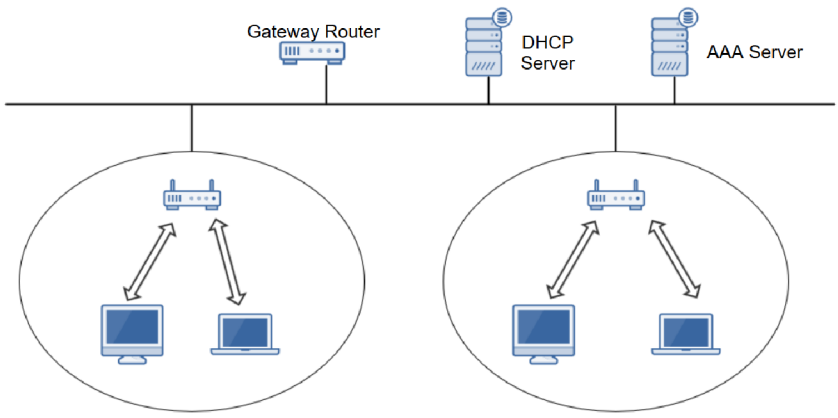
Nezahŕňam algoritmus WEP, ktorý je už zastaraný. Tieto bezpečnostné štandardy sú v širokom meradle najpoužívanejším zabezpečením bezdrôtových prístupových bodov.Prenos údajov je pomocou autentifikačných a asociačných rámcov. Tieto rámce preberám do detailu v kapitole Asociácia.

Je dôležité aby všetky zariadenia, ktoré sa pripájajú do siete, podporovali rovnaké štandardy a protokoly. Ak sa tak nestane, môže to spôsobiť komplikácie pri pripájaní a nasledovnej komunikácii či znemožniť pripojenie. V dnešnej dobe neustálych aktualizácii je jednoduché používať najnovšie technológie. Zastaraný software nemusí nutne znamenať, že sa nepripojíte k sieti. Môže ale znamenať, že procesy pripojenia, prenos dát a podobne budú trvať dlhšie a tým sa bude zdať, že je pripojenie pomalé. Táto problematika sa týka nie len koncového zariadenia ale aj prístupového bodu a ostatných častí siete smerom vyššie [9].

## 1.4 Roaming pomocou štandardu 802.11

### 1.4.1 Extended Service Set

Service Sets sú rozdielne, zatiaľ čo BSS sú jednotky zariadení pracujúce v rovnakom prístupovom prostredí ako frekvencie, kanály, modulácie a tak ďalej, ESS je logická jednotka jednej alebo viacerých BSS v rovnakom sieťovom segmente [10], [13]. Túto sieť si môžeme predstaviť na obrázku 1.13.




Obr. 1.13: ESS sieť

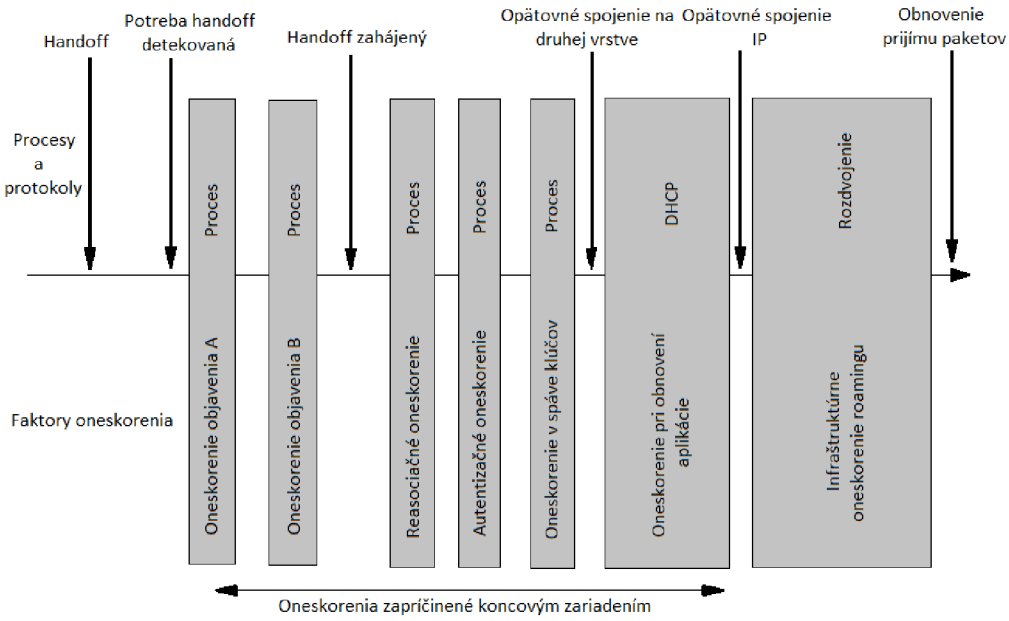
Každý z troch prístupových bodov propaguje rovnaké SSID v beacon rámcoch a probe odpovediach. Niektoré prístupové body vysielajú viaceré SSID v jedom beacon rámci. Táto multiplicita umožňuje jednému prístupovému bodu správať sa ako viacero virtuálnych prístupových bodov. Tejto funkcie sa využíva v prostredí kde jednotlivé virtuálne prístupové body poskytujú rozdielne zabezpečenia, kvalitu služieb alebo virtuálne LAN siete. Podsieť IP zodpovedajúca za SSID je často podobná sieti 802.3 eternetových portov s káblovým pripojením ku ktorému sú pripojené všetky prístupové body ktoré zdieľajú tento SSID. Prostriedky, vrátane servera DHCP a iných serverov, ako aj smerovač brány poskytujúci prístup k iným podsieťam a verejnému internetu, sú pravdepodobne pripojené k rovnakému eternetu a patria do rovnakej podsiete. Distribučný servis (DS) je termín 802.11, ktorý opisuje spájajúcu infraštruktúru prístupových bodov a EES. Štandard 802.16, zámy ako WiMAX, ktorý je bezdrôtová metropolitná sieť sa často navrhuje ako back-haul technológia spájajúca infraštruktúry prístupových bodov a ESS.

### 1.4.2 Fázy roamingu

Existuje veľa faktorov, ktoré skutočne prispievajú k oneskorenému roamingu. V tejto kapitole sa budem venovať jednotlivým oneskoreniam a ich vzájomnej kombinácii. Problém pri poskytovaní priamych meraní oneskorenia roamingu 802.11je, že sa oneskorenie môže líšiť obsahom. Je dôležité dobre odhadnúť situáciu a na základe, ktorej sa veci menia. Nič sa nedeje pre nič za nič. Proces rozhodovania či zmeniť prístupový bod môže trvať krátku aj dlhú chvíľu. Niektoré koncové zariadenia sa držia jedného prístupového bodu príliš dlho kým zistia, že bola možnosť pripojiť sa k lepšiemu.

Jednou z komplikácií je rozhodovanie sa, kedy zmeniť prístupový bod. Intuitívne by sme mohli zmeniť prístupový bod, vtedy keď nájdeme iný, so silnejším signálom. Táto stratégia však v praxi nefunguje. Rádio frekvenčné vlny podliehajú mnohým zmenám, i keď je koncové zariadenie bez pohybu. Keď pridáme pohyb koncového zariadenia a silu signálu prístupového bodu rušeného okolitými signálmi výsledok sa začne líšiť. Na začiatku sa v 802.11 sieťach volil prístup, odložiť roaming pokiaľ nepadne sila signálu pod určitú úroveň. Tento spôsob sa časom vyvíjal a boli pridávané sofistikovanejšie riešenia, ktoré brali v úvahu viacej faktorov. Ak by sa tak nestalo, zariadenie by mohlo jednoducho padnúť do nekončiacej špirály, kde by neustále menilo prístupový bod podľa sily signálu. Pozrime sa aké faktory roaming ovplyvňujú. Na obrázku 1.14 je zobrazených niekoľko udalostí, ktoré sa objavujú počas procesu roamingu. Ide o všeobecný príklad. V strede obrázku 1.14 sú šedé obdĺžniky označené dvomi názvami. Horná časť sú procesy alebo povedané protokoly. Spodná časť

obdĺžnikov označuje typ oneskorenia, ktorý predchádza pred ďalším. Oneskorenia na seba nadväzujú. Tieto oneskorenia preberieme do hĺbky.




Obr. 1.14: Oneskorenie v 802.11

**Oneskorenie objavenia** – proces zisťovania pozostáva zo skenovania a z iných meracích procesov potrebné pre koncový bod (A), aby zistil, že potrebuje využiť roaming (B) zároveň vybrať najlepší prístupový bod. Časť (A) ukazuje, že aktuálny prístupový bod nevyhovuje a je čas ho zmeniť. Existujú rôzne metriky, ktoré možno použiť pri tomto rozhodovaní. Patria sem nasledujúce:

- Zvýšený počet opakovacích pokusov kvôli chybám v prenose
- Zníženie prenosovej rýchlosti, v dôsledku neschopnosti komunikovať pri vyšších rýchlostiach
- Veľa zmeškaných beacon rámcov
- Veľa prijatých rámcov s chybou
- Pokles rádiovej sily signálu meranej pomocou RSSI parametra

Rôzne implementácie môžu využívať jednu alebo viacej týchto metrík aby zariadenie využilo roaming. Všetky tieto metriky priamo alebo nepriamo súvisia so silou signálu, preto ich nazvime signálovo založené metriky. Spúšťanie týchto metrík je na obrázku 1.14 zobrazené ako „Potreba handoff detekovaná“. Je potrebné poznamenať, že oneskorenie medzi „Handoff“ a „Potreba handoff detekovaná“ vychádza z reálneho scenára, kde začiatok roamingu nastane neskôr než je ten pravý okamžik. Táto

medzera je pravdepodobne nevyhnutná pretože rozhodnutie pre handoff musí byť na základe metrík a k ideálnemu času začatia sa dostaneme jedine retrospektívou.

**Reasociačné oneskorenie** – táto časová perióda je potrebná na dokončenie spojenia s novým prístupovým bodom. Zhŕňa výmenu dvojice autentifikačných rámcov 802.11 a výmeny asociačných žiadostí a odpovedí. Začiatok oneskorenia je definitívne ukončenie pripojenia s prístupovým bodom. V závislosti od toho na čo sa zameriame v časti oneskorenie objavenia A, aplikačné dáta nemusia byť schopné prejsť cez pripojený prístupový bod ešte pred začiatkom reasociačného oneskorenia no určite nie po jeho začiatku. Na obrázku 1.14 je znázornené meranie na základe času roamingu, po tom ako sa koncové zariadenie rozhodne pre zmenu. Toto trvanie zahŕňa časť B z oneskorenia objavenia a reasociačné oneskorenie, založené na slabom alebo žiadnom zabezpečení.

**Autentifikačné oneskorenie** - toto oneskorenie je priradené komunikácii medzi koncovým zariadením a AAA serverom (Authentication, Authorization, and Accounting). V závislosti od toho akú verziu zabezpečenia 802.11 používame, môže táto výmena obsahovať niekoľko rámcov. Väčšinou to býva 13 a viac, teoreticky to môže byť aj stovky pri použití network-admission teda kontrola prístupu.

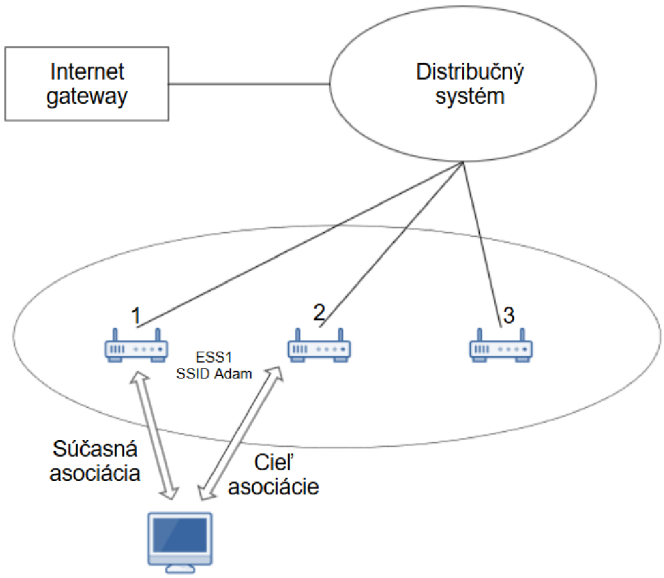
**Oneskorenie v správe kľúčov** - oneskorenie je spôsobené štvoritou výmenou kľúča v rámcoch, ktoré sa použijú na odvodenie hlavného kľúča pre šifrovanie spojenia. Na konci tejto fázy sa dostaneme do časti pohybu.

**Oneskorenie pri obnovení aplikácie** - keď sú 802.11 čipy naprogramované pomocou odvodzovania kľúča cez fázu oneskorenia v správe kľúčov, dôjde k určitému dodatočnému oneskoreniu, v prípade ak ovládač odošle LINK UP udalosť na protokoly vyššej vrstvy predtým, než zareagujú na obnovenie prenosu. Moderné koncové zariadenia odošlú ARP rámec na predvolenú gateway pre zistenie, či sa IP podsieť zmenila. V prípade, že prišlo k zmene IP podsiete, oneskorenie pri získavaní adresy od DHCP servera je súčasťou tejto fázy. Táto fáza je dôležitou časťou prečo sa globálny roming líši od lokálneho. Na konci tejto fázy opätovného spojenia IP.

**Infraštruktúrne oneskorenie roamingu** - táto posledná fáza oneskorenia zachytáva oneskorenie, ktoré sa môžu vyskytnúť v infraštruktúre po tom čo je koncové zariadenie a prístupový bod pripravený pokračovať v prenose. Na obrázku 1.14 je znázornené rozdvojenie v tejto fáze na lokálny roaming a mobilné IP. To predstavuje dva vrcholy v zložitosti infraštruktúry vzhľadom na dodatočné oneskorenie. V prípade lokálneho roamingu, aj keď je koncové zariadenie a prístupový bod pripravený pokračovať v prenose, musí byť presmerovaná cez nový prístupový bod. Kým infraštruktúra nezareaguje na túto zmenu, stále zariadenie nie je pripojené a nemôže prenos pokračovať. Doteraz sme si ale neopísali, ako infraštruktúra reaguje na túto zmenu. Podľa tohto vzoru infraštruktúra nevie, že sa koncové zariadenie pohlo k inému prístupovému bodu pokiaľ nedostane rámec od tohto prístupového bodu. Časť oneskorenia smerovania v infraštruktúre môže vzniknúť v dôsledku aplikačných timeoutoch, ktoré vyvrcholia s odoslaním paketov od koncového zariadenia do infraštruktúry. Príjem tohto rámca z nového portu prístupového bodu bude smerovať komunikáciu a tým infraštruktúru týmto smerom. V opačnom prípade, ak sa infraštruktúra pokusí nájsť koncové zariadenie, vyšle rámce na všetky porty pokiaľ nedostane odpoveď koncového zariadenia.

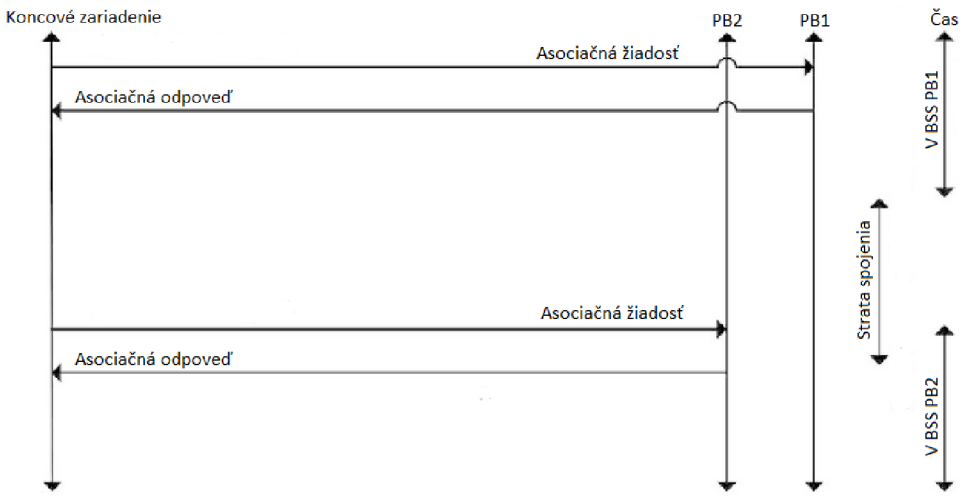
### 1.4.3 Lokálny roaming

Lokálny roaming je pre siete WLAN podobný mobilnému telefónu, ktorý sa pripája do ďalšej bunky poskytovanú rovnakým mobilným operátorom. Na obrázku 1.15 si môžeme ukázať príklad topológie, v ktorej si popíšeme základné princípy. Koncové zariadenie je pripojené ku koncovému zariadeniu číslo jedna a bude chcieť zmeniť prístupový bod na číslo dva. V sieťach kde prístupové body zdieľajú rovnaké SSID je opakom roamingu medzi bunkami mobilného operátora. V prípade lokálneho roamingu je podnetom k roamingu metódy merania sily signálu, ktoré vyvrcholia k zmene prístupového bodu v rovnakej ESS so silnejším signálom. V sieťach 802.11 sú všetky handoff sú hard handoff, s aktuálnym prístupovým bodom je prerušené spojenie pred tým, než prúd aplikačných paketov môže pokračovať na novom prístupovom bode. Doba handoff môže mať rôzne trvania v dôsledku náhodnej povahy skenovania a reasociačnej procedúry 802.11. Pri použití zabezpečenia 802.11i, čas hnadoff môže trvať niekoľko sekúnd.



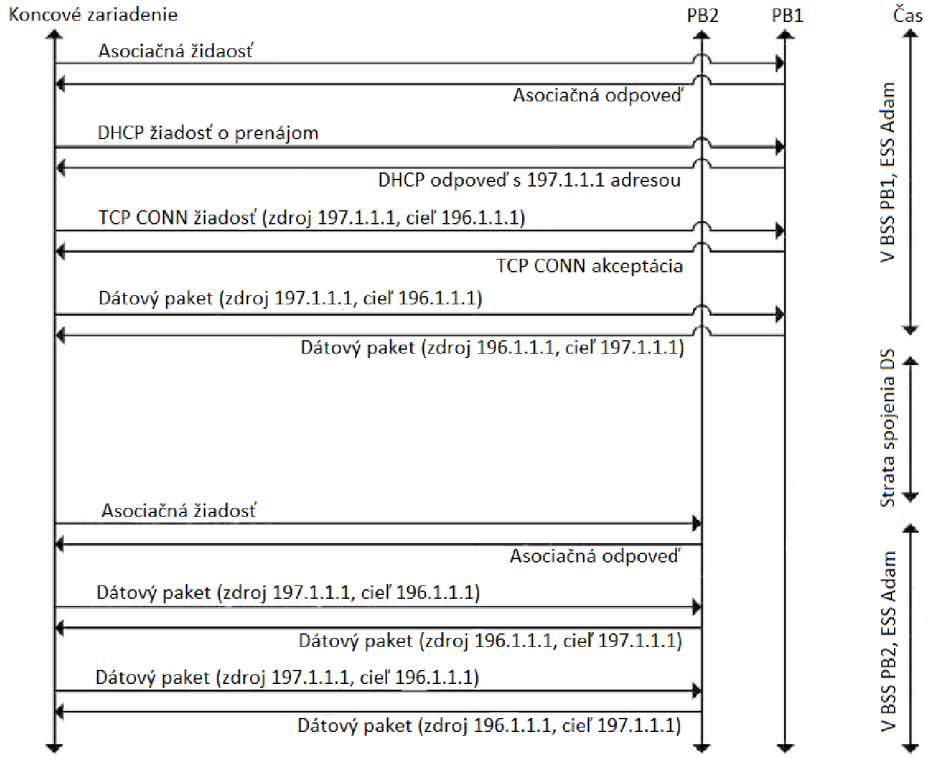

Obr. 1.15: Topológia pre lokálny roaming

V jednoduchosti, roaming v z jedného prístupového bodu na druhý v rámci EES zahŕňa len veľmi jednoduchú výmenu rámcov. Na obrázku 1.16 vidíme, že sa najskôr koncové zariadenie pripojilo k prístupovému bodu 1 (PB1) a po krátkej strate spojenia, pripojí na BSS prístupový bod 2 (PB2). Táto strata spojenie môže trvať rádovo milisekundy keď neberiem v úvahu zabezpečenie alebo kvalitu služieb. V skutočnosti strata môže trvať dlhšie v závislosti od rôznych faktorov spomenutých vyššie.




Obr. 1.16: Riadiace ráme v lokálnom roamingu

Je možne mať rôzne ESS v rovnakej posieti. Teoreticky by mohlo byť možné meniť ESS bez toho aby sa menila IP adresa. Globálny roaming môže mať oveľa väčší vplyv na užívateľa než lokálny roaming. Aby sme si ukázali tento rozdiel, musíme sa pozrieť na protokoly vyššej vrstvy. Pozrime sa ako by vyzerala komunikácia z obrázku 1.16, ak by sme pridali protokoly DHCP a TCP. Rozdiel vidíme na obrázku 1.17. Pre jednoduchosť, nie je to úplné zobrazenie zodpovedajúce týmto protokolom, ak by sme chceli reprezentovať skutočnosť, obrázok by sa stal nečitateľným a preplneným. Z tohto obrázku je vidno, že napriek spojeniu koncového bodu s novým prístupovým bodom sa podsieť nezmenila. IP stoh koncového zariadenia sa musel zresetovať a TCP spojenie pokračovalo nebolo však nutné toto spojenie obnoviť.

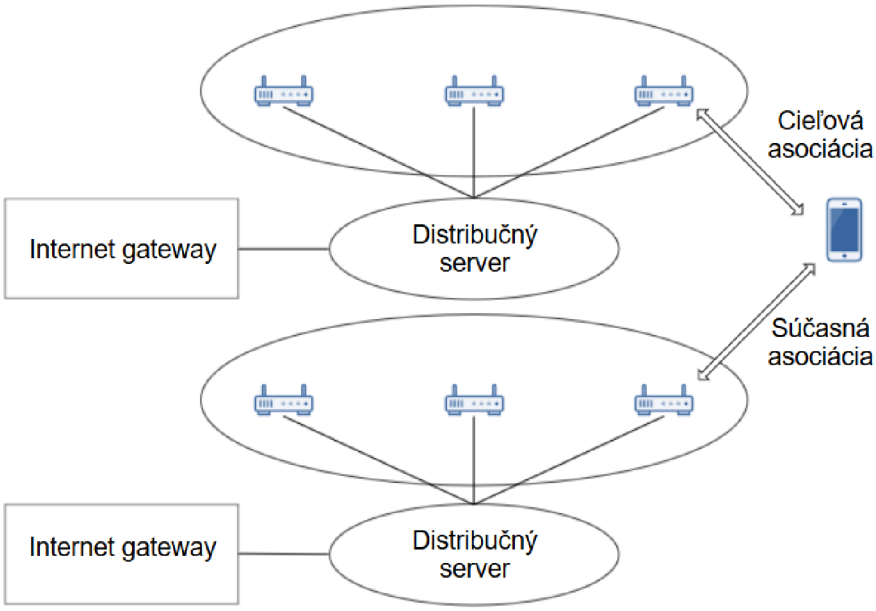



Obr. 1.17: Riadiace ráme v lokálnom roamingu s protokolmy DHCP a TCP

### 1.4.4 Globálny roaming

V predchádzajúcej časti sme preberali situáciu, kedy roaming bola jednoduchá voľba. Na obrázku 1.18 máme situáciu kde výber prístupového bodu nie je tak zrejmý. Koncové zariadenie je pripojené ku prístupovému bodu 3. Predpokladajme, že signál z tohto prístupového bodu stráca silu, preto lebo sa koncové zariadenie pohybuje alebo sa medzi nimi objaví prekážka. Koncové zariadenie príjme beacon rámce od

prístupového bodu 2 a 6. V prípade ak sú všetky ostatné faktory v normále , cieľom by mal byť prístupový bod 2, lebo nejde o zmenu SSID. Z rozloženia prístupových bodov, vyplýva, ak koncový bod prijme slabý signál od prístupového bodu 3, potom signál od prístupového bodu 2 bude ešte slabší. Z tohto uhla pohľadu môže byť prístupový bod 6 jediným kandidátom. Vzhľadom na to, že tento bod je v inej EES, roaming k tomuto prístupovému bodu bude globálnym. Keď sa pripájame k novému SSID vyplynú aj ďalšie problémy než sila signálu. Koncové zariadenie musí zistiť, či nové SSID ponúka určitý servis. To znamená, či SSID je súkromné alebo verejné. Užívateľ nemusí byť schopný splniť minimálne bezpečnostné požiadavky. Naopak, koncové zariadenie môže byť nastavené tak, že zakazuje pripojenie k týmto typom sietí.




Obr. 1.18: Topológia pre globálny roaming

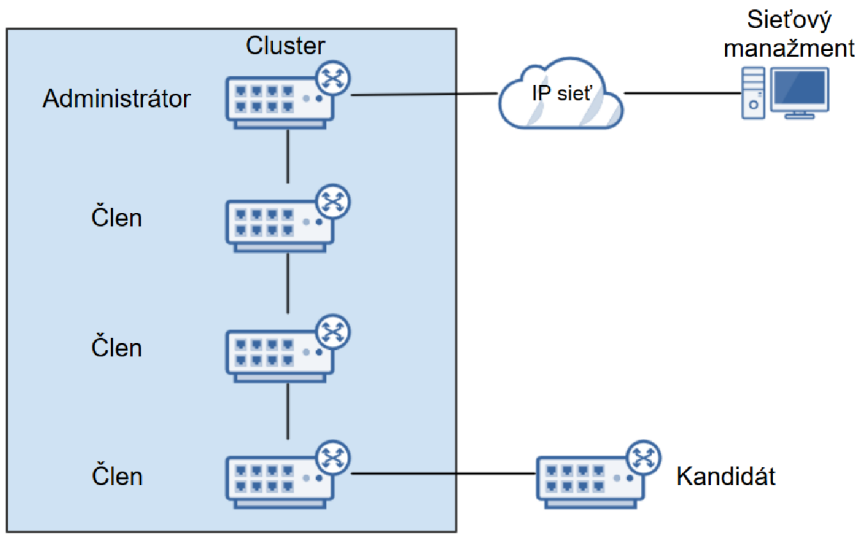
## 1.5 Hewlett-Packard

Skrátene HP, je medzinárodná firma zaoberajúca sa informačnými technológiami. Je to americká firma založené 1939 v jednej Kalifornskej garáži. Dnes je to najväčšia IT spoločnosť sveta. Zaoberá sa výrobou softwaru aj hardwaru. Ich vyrábaný sortiment siaha od tlačiarní až po sieťové prvky.

Spoločnosť HP pre kontrolovanie a manažment niekoľkých prístupových bodov využíva Cluster manažment [18]. Funguje na princípe pridávania koncových zariadení do vytvoreného systému správy. Zariadenia v tomto zoskupení majú tri rôzne funkcie podľa ich nastavenia:

- Administrator (Administrátor) - Zariadenie poskytuje manažment pre všetky prvky v skupine. Manažér v skupine môže byť len jeden. Každá konfigurácia, monitorovanie môže byť nastavené iba cez toto zariadenia. Ak máme nastaveného administrátora, toto zariadenie zhromažďuje informácie o ostatných zariadeniach pripojených do jeho skupiny
- Member (Člen) - Toto zariadenie býva väčšinou prístupový bod. Jednoducho je pripojené do skupiny a prijíma konfiguráciu od administrátora
- Candidate (Kandidát) - Nepatrí do žiadnej skupiny ale môže byť pridaný do skupiny. Zhromažďuje informácie a posiela ich administrátorovi ale nie je pridaný do skupiny

Pre zobrazenie možného zapojenia prvkov v skupine 1.19.




Obr. 1.19: HP cluster

Administrátor získava informácie od členov pomocou výmeny správ. Táto správa je implementovaná pomocou HGMPv2, ktorý sa skladá z týchto troch protokolov:

- NDP - Sa používa pre objavenie informácií o priamych susedoch vrátane názvu zariadenia, verzie softwaru a pripojovacieho portu týchto zariadení. NDP pracuje na dátovej vrstve a preto podporuje rôzne protokoly sieťovej vrstvy. Zariadenie posiela pravidelne NDP pakety svojim susedom, s týmito informáciami. Posiela aj správy o tom, ako dlho si príjemca tieto informácie bude uchovávať tak zvaný holdtime. V rovnakom čase prijíma NDP pakety od susedov. Tie pakety sa nepreposielajú, slúžia na komunikáciu medzi dvoma susedmi. Zariadenie vytvára tabuľku so susedmi a ich prenesenými informáciami. Ak zariadenie prijíme od suseda NDP paket s inou informáciu ako má uloženú v tabuľke, informácia a holdtime sa aktualizujú. Pokiaľ nedostanú informácie po vypršaní holdtime, táto informácia je vymazaná.
- NTDP - Pomocou NTDP sa prenášajú informácie potrebné pre cluster manažment. Zhromažďujú informácie o topológii a počte skokov. Podobne ako pri NDP, administrátor rozosiela NTDP pre získanie informácií o topológii, zachytáva NDP pakety v určitých sieťach pre vykreslenie topológie. Zhromaždené informácie budú použité administrátorom pri implementovaní potrebných úkonov. Ak člen clustra zistí zmenu u suseda vysielanú NDP paketom, informuje administrátora pomocou handshake pakety. Následne administrátor vyšle NTDP pre zistenie zmeny v sieti. NTDP sa administrátorom vysielajú periodicky. Keď zariadenie príjme NTDP od administrátora, odošle odpoveď administrátorovi a skopíruje NTDP na podporovaný port priľahlého zariadenia. Táto správ obsahuje základné informácie zariadení a jeho susedoch. Pracuje to na v podstate na princípe posielania a kopírovania NTDP správy po celej topológii v rámci dostupných skokov. V rovnakom čase sa posielajú a prijímajú NTDP správy čo vedie k zvýšeniu zaťaženiu zariadenia.
- Cluster - Slúži na pridávanie a komunikáciu v skupine. Pridávanie zariadenia prebieha pomocou administrátora, ktorý určí zariadenie pomocou NDP a NTDP protokolov. Následne je zariadenie pridané automaticky alebo manuálne. Po tom ako je pridané, dostane pridelené číslo a svoju IP adresu používanú v rámci skupiny. V skupine administrátor komunikuje s členmi poslaním handshake paketov pre obsluhu danej skupiny. Po pridaní člena do skupiny si administrátor uchová údaje o tomto zariadení a nastaví ho ako aktívne. To isté urobí aj pridaný člen. Následne si začnú vymieňať handshake pakety. Ak administrátor nedostane odpoveď od člena v intervale troch správ handshake, zmení jeho stav z aktívneho na pripojený. Keď člen odpovie do uloženého času holdtime, administrátor zmení jeho stav znova na aktívny, ak sa tak nestane,

stav sa zmení na odpojený. Pokiaľ sa obnoví komunikácia, administrátor znova pridá toto zariadenie do skupiny a zmení jeho stav na aktívny.

## 1.6 MikroTik

Ide o lotyšskú spoločnosť založenú v roku 1996 pre vývoj smerovačov a bezdrôtových ISP systémov. V dnešnej dobre, táto firma poskytuje hardware a software pre pripojenie do Internetu po celom svete. Od roku 2002 začali vyrábať vlastný hardware pod firemným názvom RouterBOARD.

### 1.6.1 CAPsMAN

Controled Acces Point systém Managment, v preklade kontrolovaný prístupový bod, umožňuje centralizáciu správ bezdrôtovej siete. V prípade potreby ho možno využiť aj na spracovanie dát. Pri použití tejto funkcie, sieť pozostáva z množstva kontrolovaných prístupových bodov nazývaných CAPs, teda pokiaľ sa sieť nezakladá z jedného zariadenia, ktoré poskytujú bezdrôtové spojenia a systémového správcu CAPsMAN. Tento správca iba konfiguruje prístupové body, ale aj o autentifikáciu klienta poprípade preposielanie dát. Keď je CAP kontrolovaný pomocou CAPsMAN vyžaduje iba minimálnu úroveň konfigurácie pre spojenie so správcom. Funkcie, ktoré robil prístupový bod ako napríklad kontrola prístupu či overovanie, teraz robí správca teda CAPsMAN. CAP, prístupový bod iba poskytuje bezdrôtové šifrovanie a dešifrovanie spojenia. V závislosti od konfigurácie, dáta si preposielané správcovi pre centrálnu správu alebo preposlané na samostatnú jednotku CAP. Existujú dve verzie tohto systému. Je nutné ale pripomenúť, že verzie medzi sebou nie sú kompatibilné. To znamená používanie iba jednej verzie v celej sieti aby sa predišlo problémom, staršiu verziu jednoducho aktualizujeme. Zaoberajme sa novšou verziou teda druhou generáciou. Tá prináša:

- Automatické aktualizácie všetkých CAP klientov
- Vylepšenú komunikáciu medzi CAP a CAPsMAN
- Pridané položky označenia „Name Format“ a „Name Prefix“ pre pravidlá poskytovania
- Zlepšené vstupy pre prípad roamingu koncového zariadenia medzi CAP
- Pridanie L2 Path MTU zistenia

CAPsMAN dokáže ovládať neobmedzený počet prístupových bodov. Aby systém CAPsMAN fungoval a poskytoval bezdrôtové pripojenie, CAP musí nadviazať spojenie s CAPsMAN. Toto spojenie môže byť vytvorené na základe protokolov MAC

alebo IP vrstvy zabezpečené funkciou DTLS (Datagram Transport Layer Security). Zariadenie CAP môže preposlať dáta o klientovom pripojení ale táto komunikácia bude nešifrovaná. Pri využití tejto služby, je nutné túto komunikáciu vhodne šifrovať napríklad IPSec alebo šifrovanými tunelmi. Prepojenie CAP a CAPsMAN sa dá vytvoriť pomocou dvoch transportných protokolov cez druhú a tretiu vrstvu. Prepojenie cez vrstvu MAC ponúka, CAP bez potrebnej konfigurácie IP a CAP a CAPsMAN musia byť v rovnakom segmente druhej vrstvy. Naopak pripojenie cez IP vrstvu ponúka, prerazenie NATu ak je potrebné, CAP musí byť schopná dočiahnuť na CAPsMAN cez IP protokol, ak nie sú v rovnakom segmente druhej vrstvy, musí byť dosiahnuteľná cez IP adresu.

Na vytvorenie spojenia, CAP iniciuje vyhľadávanie. Počas hľadania, CAP kontaktuje CAPsMAN a vytvorí zoznam. CAP sa následne pokúsi o kontakt pomocou zoznamu správcovských IP adries, zoznamu IP adries od DHCP servera alebo vysielaním nastavených rozhraniach pomocou protokolov IP a MAC vrstvy. Keď je zoznam vytvorený, CAP zvolí správcu podľa týchto pravidiel:

- Ak parameter caps-man-names špecifikuje povolené názvy správcov, CAP bude uprednostňovať toho správcu, ktorý je v zozname. AK je zoznam prázdny pripojí sa k hociktorému dostupnému správcovi
- Správca s pripojením na MAC vrstve je uprednostňovaný pred IP vrstvou

Po vybraní správcu, CAP sa pokúsi o vytvorenie DTLS spojenia. Existujú tieto autentifikačné režimy:

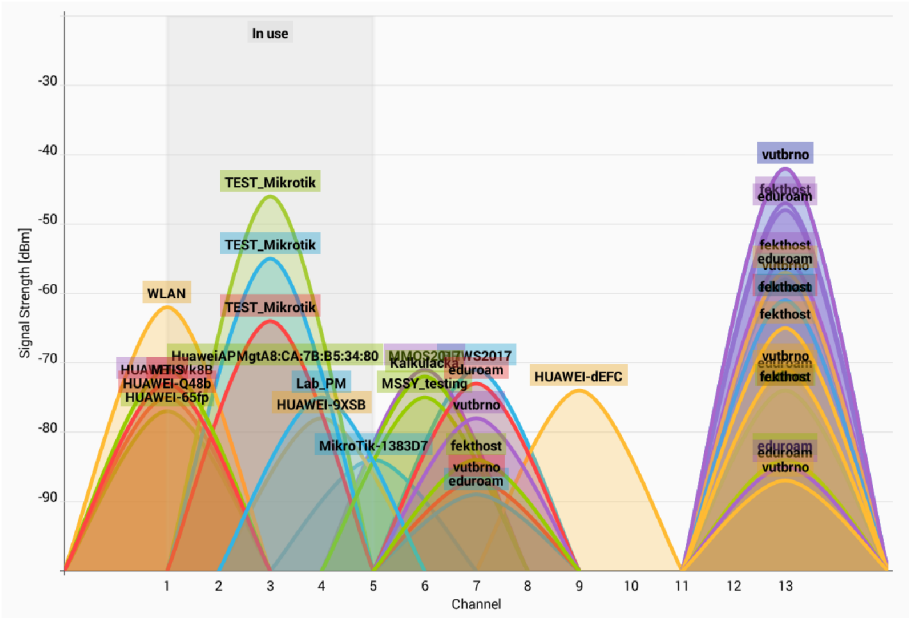
- Bez certifikátov, bez overovania
- Iba správca používa certifikát, CAP skontroluje správcov certifikát, no spojenie nezlyhá ak ide o nedôveryhodný certifikát. Správca musí byť nakonfigurovaný tak, aby dokázal vytvoriť spojenie s CAP bez certifikátu
- CAP aj správca používajú certifikát

Ak sa CAP odpojí od siete, správca začne odpočítavať interval po ktorom zariadenie ukončí spojenie [15].

# 2 RIEŠENIE DIPLOMOVEJ PRÁCE

## 2.1 Návrh merania

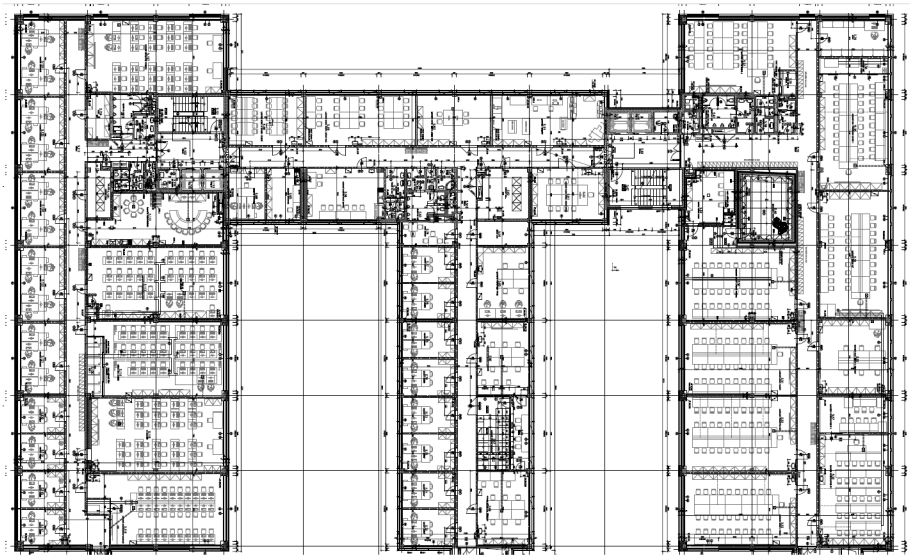
V predchádzajúcich kapitolách som popísal a rozobral problematiku roamingu vo WiFi sieťach. Ide o teoretické príklady a fakty. Ďalšou častou je vyskúšať nadobudnuté informácie na reálnych príkladoch a v reálnom prostredí. Pri vytváraní návrhu merania som bral do úvahy jeho opakovateľnosť pre obe siete a to Mikrotik a HP. Meranie by sa malo čo najviac podobať reálnemu používaniu siete. Je nutné počítať aj s tým, že sieť bude rušená inými prístupovými bodmi. Samozrejme ak sa nenájde voľné pracovné pásmo respektíve kanál v, ktorom môže prístupový bod bez rušenia pracovať. V mojom prípade situáciu vykresľuje obrázok 2.1, kde som sieť vytvoril na 3 kanáli. Ide teda nie o úplne ničím nerušené laboratórne meranie.




Obr. 2.1: Spektrum WiFi signálov

Testovanie siete prebieha na piatom nadzemnom podlaží budovy v časti C,D a E, fakulty elektrotechniky na T12. Pre lepšiu vizualizáciu prostredia pridávam obrázok podlažia 2.2. Keďže, časť budovy E a C majú veľmi rovnaký tvar, len sú zrkadlovo otočené, pri rozmiestňovaní prístupových bodov a vytváraní metodiky merania som pracoval v časti C. Na časť budovy E som aplikoval rovnaké rozloženie a metodiku ako v časti budovy C. V časti budovy D som pokračoval v podobnom spôsobe testovania ako u časti budovy C. Prechádzal som sa po celom poschodí a rozhodol som sa sieť vytvoriť na ôsmom kanáli v 2.4GHz pásme. V tomto kanáli je v

priemere 7 sietí. Svoju testovaciu sieť som pomenoval TEST_Miktorik pre testovanie prvkov od Mikrotiku a vutbrno ako zástupca výrobcu HP. Sieť vutbrno používa prístupové body HP J9845A 560. Metodika, nastavenia a výsledky, sú napísané v ďalších kapitolách.

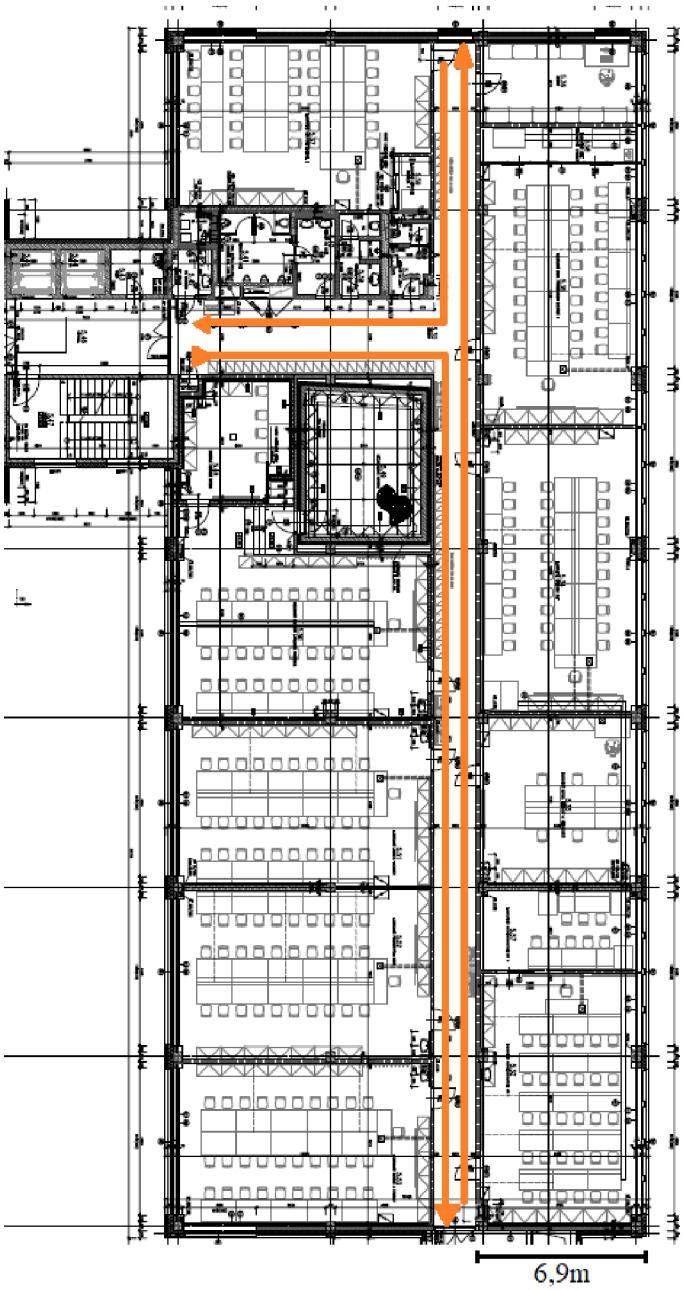


Obr. 2.2: Pôdorys piateho nadzemného podlažia

## 2.2 Metodika a kroky merania

V tejto kapitole preberieme testovanie, nastavovanie metodiky a kroky merania v sieti tak aby boli opakovateľné a splňovali parametre rýchleho roamingu. Pri testovaní používam dve zariadenia. Notebook so sieťovou kartou od výrobcu Intel Corporation. Ide konkrétne o typ Intel® Dual Band Wireless-AC 3165 s verziou ovládača 19.50.1.6. Druhé zariadenie je tablet, ktorý podporuje iba 2.4GHz pásmo a štandard IEEE 802.11b/g/n. Všetky merania prebiehajú na notebooku aj na tablete. Na meranie využívam programy a aplikácie ako SpeedTest, WiFi Survey, Wi-Fi Visualizer, Wi-Fi Heatmap, Wi-Fi Speed Test, Network Speed a podobné. Tieto aplikácie slúžia na zisťovanie informácií a parametrov testovanej siete. Využívajú aj grafické zobrazenie, ktoré používam v kapitolách. Aby bolo meranie presné, každý test opakujem 5 krát a následne spriemerujem namerané hodnoty. To platí pre testovanie s tabletom aj s notebookom. Ak chceme testovať parametre vo vytvorenej sieti je nutné najprv zistiť rozloženie prístupových bodov. Každý prístupový bod má svoje hranice a v uzavretom priestore to platí dvakrát viac. WiFi signál musí počas svojej cesty penetrovať rôzne objekty čím stráca na sile. Správnym rozmiestnením prístupových bodov, vieme hluché miesta eliminovať a zabrániť tak nechcenému výpadku

pripojenia. Všetky tieto podmienky som zvážil a navrhol metodiku a kroky merania. Najprv som po chodbe rozmiestňoval jeden router po druhom a meral jeho limity. Na základe týchto dát som zistil, ideálne rozmiestnenie prístupových bodov po chodbe, bez toho aby vznikli hluché miesta. Základom metodiky merania je pohyb po poschodí. Chôdza po vyznačenej trase, ktorú môžete vidieť na obrázku 2.3. Táto trasa sa najviac podobá bežnej chôdzi po uličke.



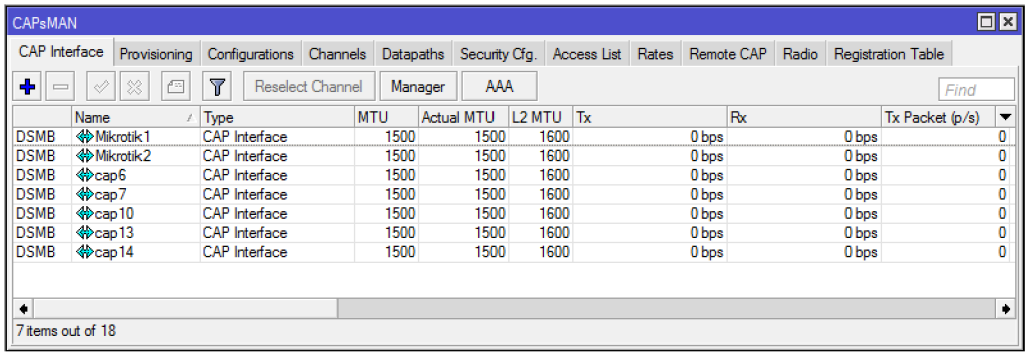

Obr. 2.3: Trasa merania roamingu

Princípom je pokryť chodby na celom piatom poschodí WiFi signálom bez hluchých miest. Roaming sa dá merať a testovať minimálne s dvoma prístupovými bodmi. Preto som meranie zameral hlavne na časť budovy C, odkiaľ sú výsledky možné aplikovať aj do ďalších častí budovy. Parametrami hlavného merania sú výpadky signálu pri downloade, sila signálu po vyznačenej trase a rýchlosť roamingu. Namerané hodnoty spriemerujem a použijem ako výsledok.

Ako download používam online stream a sťahovanie väčších súborov. Pri týchto procesoch meriam silu signálu a rýchlosť prenosu. Z tohto parametra je jednoducho vidieť, kedy nastal roaming. Na začiatku testujem samostatné časti budovy C následne prechod z časti E do časti C. To platí pre test prvkov Mikrotik a HP.

## 2.3 Nastavenie Mikrotik

Sieť zostavujem z prvkov Mikrotik s RouterBoard RB493 verziou 6.4.1. Mám k dispozícií 8 prístupových bodov rovnakého typu. Nastavenie siete je nakreslené na obrázku 2.4.

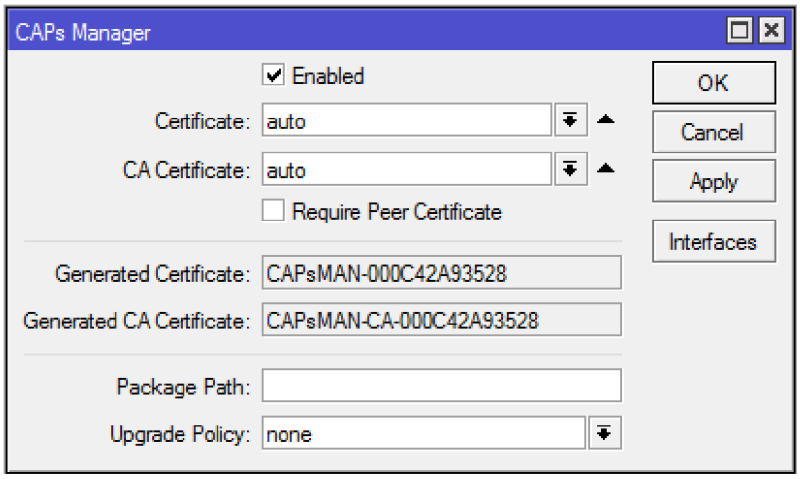



Obr. 2.4: Nastavenie prístupových bodov

Kde vidíme, že jeden prvok je nastavený ako manažér a ostatných 7 prvok ako prístupové body. Týchto 7 prvkov je pod správou manažéra. Toto nastavenie je možné vďaka centrálnemu manažmentu prvkov Mikrotik CAPsMAN. Toto nastavenie rozoberám v kapitole KAPITOLA. Pozrime sa ako sa nastavuje CAPsMAN tak aby sieť fungovala. Na začiatku je ideálne zariadenia zresetovať. Ako prvé nastavíme DHCP klienta na WAN port čím získame IP adresu, ktorá bude dôležitá pri nastavovaní CAPsMAN. Ďalej vytvoríme bridge kam pridáme všetky porty (aj wlan) okrem eth1. Vytvoríme adresy a pridelíme ich bridge. Používam adresy 10.254.X.0/24 kde X reprezentuje číslo zariadenia teda routra. Tieto adresy bude prístupový bod rozdávať koncovým zariadeniam, ktoré sa do siete pripoja. Následne nastavíme DHCP server na bridge. Povolíme NAT na eth1 a základné nastavenie routrov je hotové.

Toto nastavenie sa prevedie na všetkých 7 prvokoch. Ako ďalší krok nastavíme manažéra, ktorý bude spravovať prístupové body. Výhodou tohto manažéra je to, že ak chcem niečo zmeniť, stačí nastavenie zmeniť u manažéra a následne aplikovať na daný prístupový bod. Čiže nie je nutné nastavovať každý jeden prvok zvlášť čím sa dá ušetriť nemalý čas.

V záložke CAPsMAN ako prvé nastavíme router ako za manažéra podľa obrázku 2.5. Je dôležité nastaviť správne certifikáty a následne ich uložiť aby pri pripojení prístupových bodov nedošlo k nechcenému skopírovaniu. To by malo za následok, že by sa zariadenie nemohlo pripojiť tým pádom by nemohlo byť ovládané manažérom. Ak máme certifikáty vytvorené, jednoducho ich v kolonkách certifikátov nastavíme ručne.

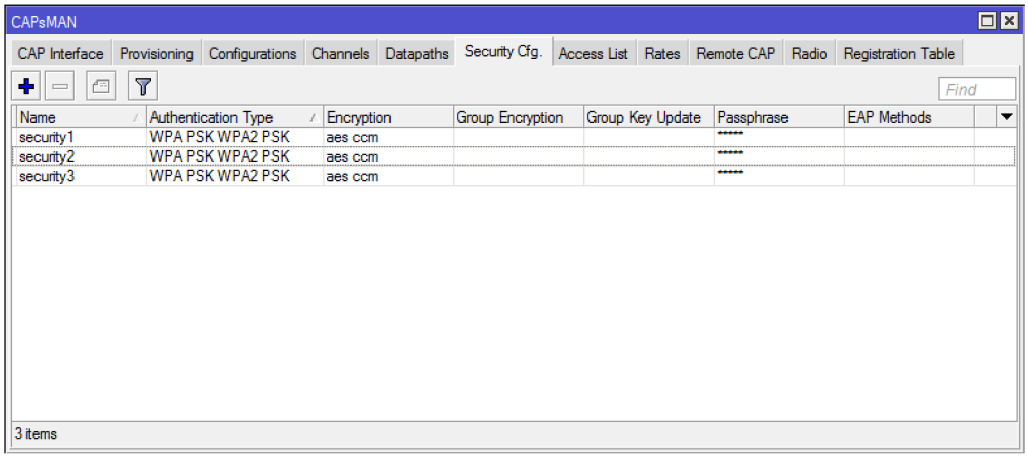



Obr. 2.5: Nastavenie manažéra CAPsMAN

Následne nastavuje ďalšie parametre v tomto okne 2.6. Pre správny chod CAPsMAN je nutné nastaviť najprv:

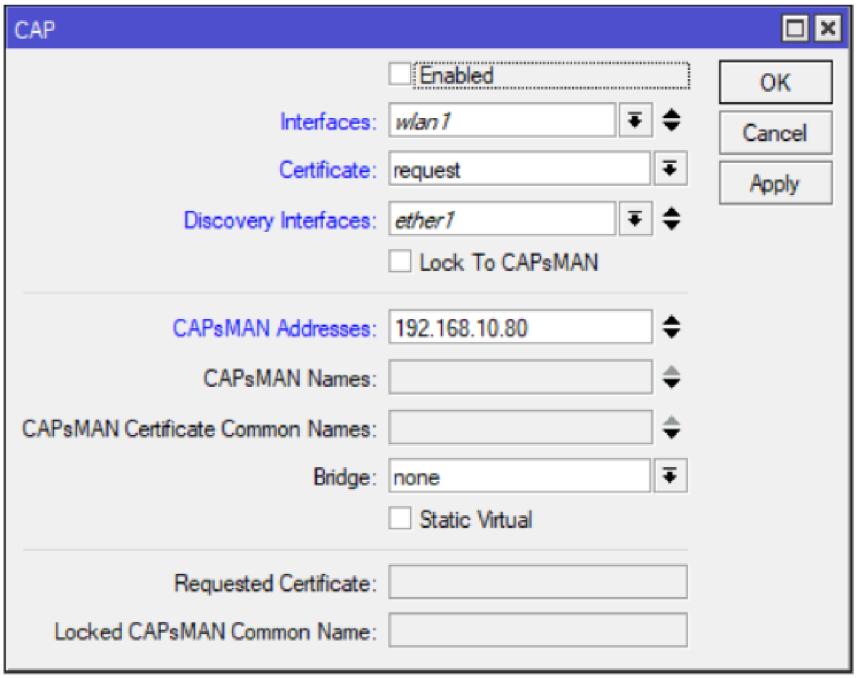
- Kanály siete v, ktorom bude naša sieť pracovať
- Datapath čiže smerovanie údajov
- Security config čo je nastavenie zabezpečenia siete
- Configuration samotnú konfiguráciu, konečné nastavenie siete
- Provisioning kde sa vytvárajú profily nastavení, ktoré sa aplikujú v záložke Radio

Všetky tieto nastavenie prebiehajú na manažérskom zariadení. Týmto zariadením sa na začiatku môže stať hociktorý router. Následná zmena manažéra nie je možná, je nutné celý systém CAPsMAN nastaviť znova s novo zvoleným manažérom.



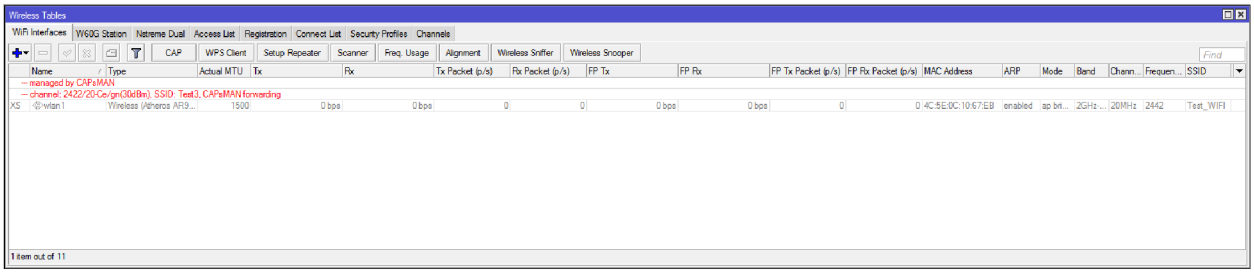

Obr. 2.6: Nastavenia pre fungovanie CAPsMAN

To je všetko z nastavenia manažéra. Je nutné nastaviť prístupové body tak, aby ich mohol manažér kontrolovať a spravovať. To urobíme v záložke Wireless a kliknutí na CAP. V ňom nastavíme parametre podľa obrázka 2.7.




Obr. 2.7: Nastavenie CAP

V parametri CAPsMAN Addresses zadáme adresu manažéra, aby prístupový bod vedel, kde má manažéra nájsť a následne sa spojiť s sním. Toto nastavenie prevedieme na všetkých prvkoch. Ak ich máme správne nastavené, uvidíme u manažéra všetky pripojené zariadenia ako na obrázku 2.4 a u prístupových bodoch skontrolujeme červený písmom napísaný výpis z obrázka 2.8. Ten hovorí o tom, že je zariadenie spravované manažérom a v druhom riadku vidíme akú ma nastavenú konfiguráciu.

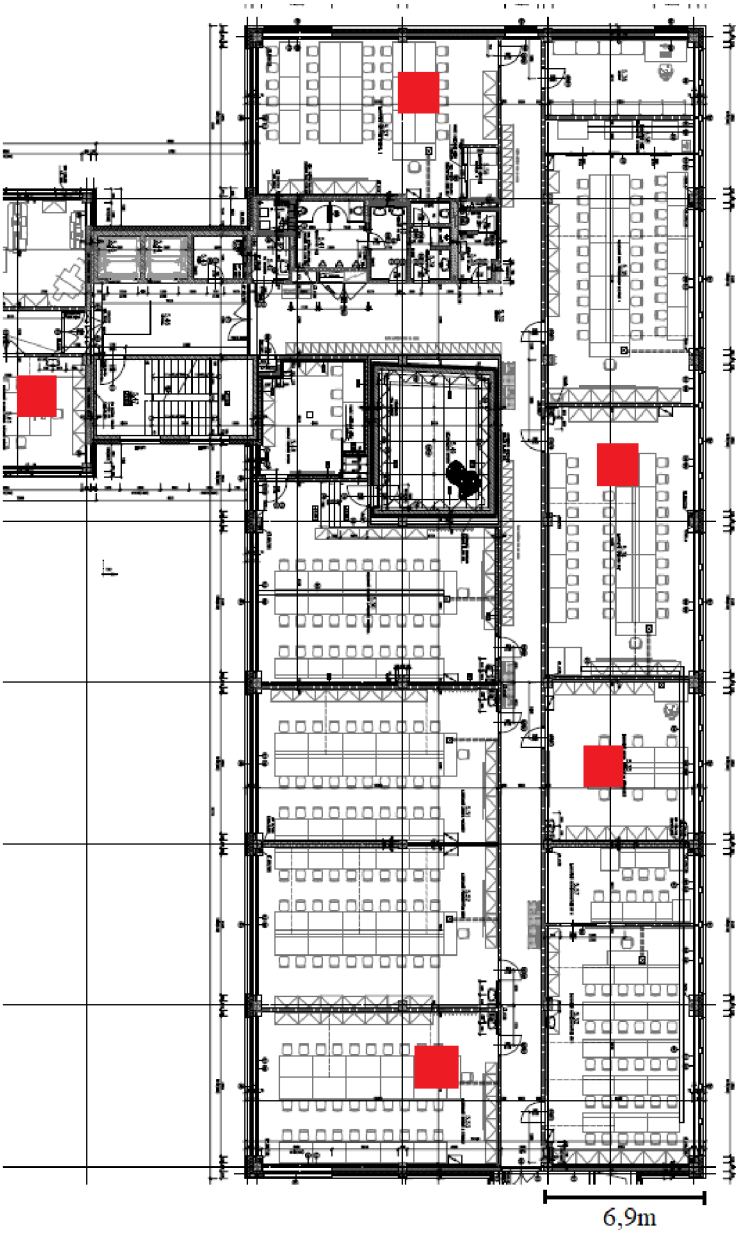



Obr. 2.8: Správny výpis CAP zariadenia

Pri nastavovaní je dôležité si uvedomiť, ako CAPsMAN pracuje. Nejde len o naklikanie nastavenia. Každý bod nastavenia má svoj zmysel. Bez správneho pochopenia nie je možné v prípade chyby dané zariadenie opraviť. Samozrejme Mikrotik má možnosť výpisu logov do konzole, ale nie sú vždy potrebné ak vieme kde môžeme chybu hľadať.

## 2.4 Meranie Mikrotik

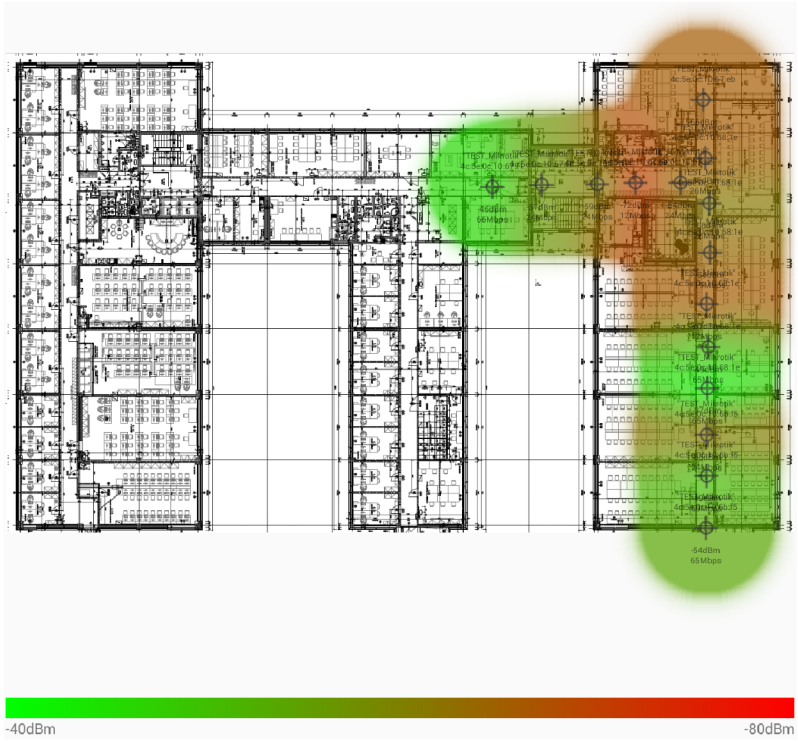
Meranie prebiehalo podľa hore spísaných postupov. Na začiatku som zisťoval limity dosahu jednotlivo rozmiestených prístupových bodov. Po zmeraní som prístupové body rozmiestnil podľa obrázku 2.9.




Obr. 2.9: Rozmiestnenie prístupových bodov

Tu môžeme vidieť, že na chodbe v budove C mám umiestnené štyri prístupové body a jeden na začiatku budovy D. Ten slúži k tomu, aby bolo možné pripojenie hneď po vystúpení z výťahu poprípade zo schodov.

Dosah a pokrytie chodby WiFi signálom zobrazuje obrázok 2.10.




Obr. 2.10: Mapa pokrytia signálu siete v budove C

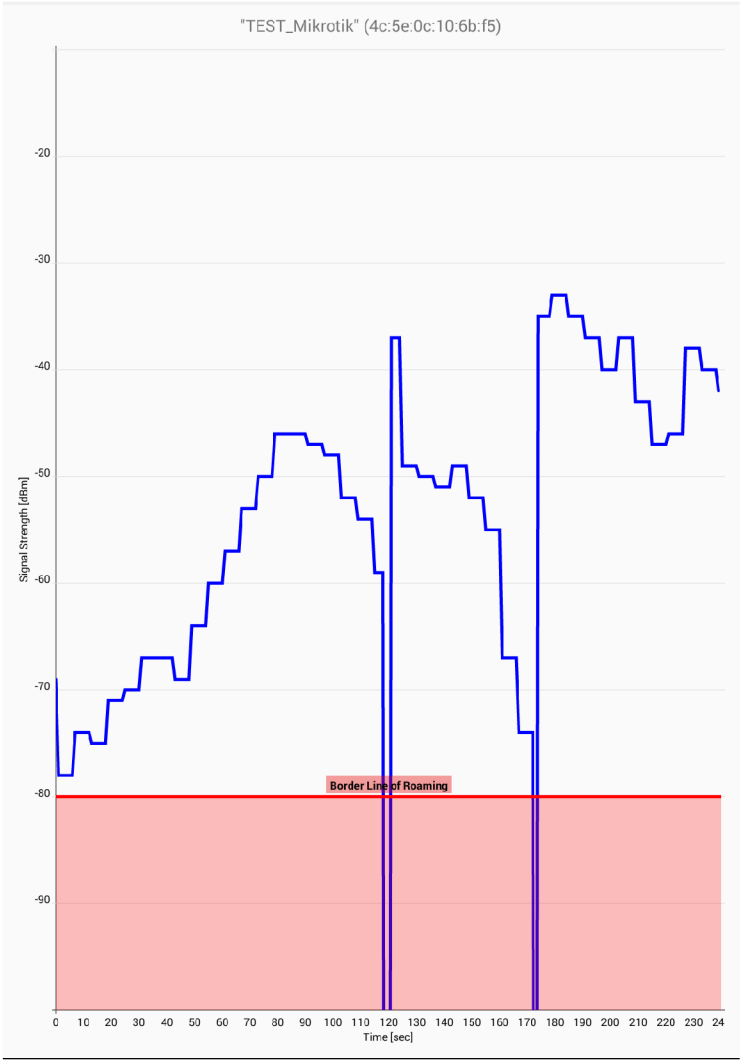
Môžeme vidieť, že signálom je pokrytá celá chodba. Čím zelenejší je signál tým silnejší a čím červenejší tým slabší signál. Miesta s červenejšími hodnotami nemusia hneď znamenať, že na danom mieste nie je WiFi signál. Signál sa tam nachádza len má menšiu silu. Menšia sila signálu nemusí z pravidla znamenať pomalú prenosový rýchlosť. Do prenosovej rýchlosti vstupujú aj ďalšie faktory, ktoré ju ovplyvňujú. Týmito faktormi môžu byť zaťaženosť siete, nízka výpočtová hranica hardware či pridelenie maximálnej rýchlosti na prístupovom bode alebo v topológii vyššie. V mojom prípade prístupové body nemajú rýchlosť nijak obmedzenú.

Po tom čo sa zariadenia rozmiestnia do učební, je nutné na manažérskom zariadení skontrolovať či sa k nemu pripojili. Pokiaľ nie, najčastejšie býva chyba v zadávaní adries. Ak sú zadané nesprávne, logicky sa zariadenia jedno k druhému pripojiť. Ideálne je použitie nástroja ping, ktorý ukáže, či sa prístupový bod dokáže dostať k manažérovi. Poprípade skontrolovať nastavenie cesty.

### 2.4.1 Výsledky pre Mikrotik

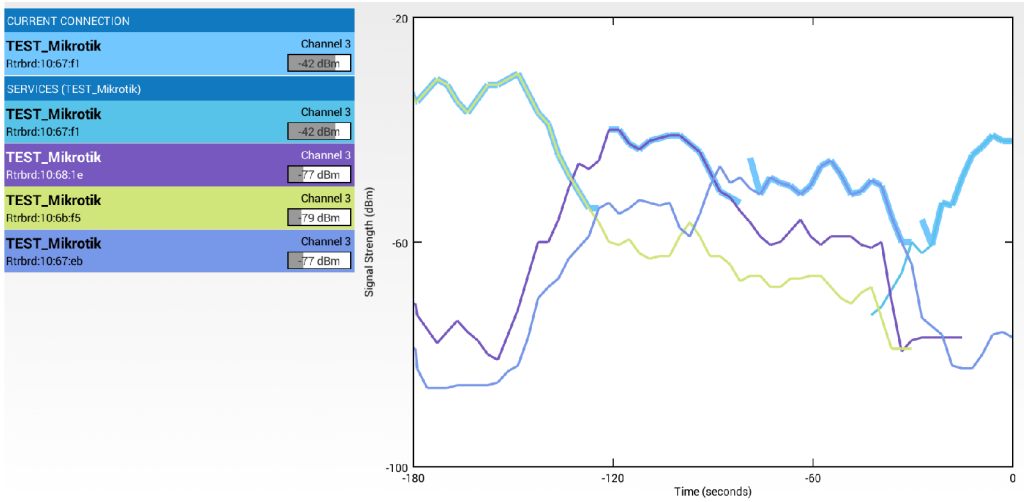
Keďže parametre roamingu sa dajú odmerať minimálne medzi dvoma zariadeniami, nie je teda pre test nutné, aby bolo celé podlažie pokryté WiFi signálom. Namerané hodnoty pre budovu C sú ľahko aplikovateľné aj na iné časti podlažia či priestory fakulty. Je z nich možné aj vychádzať pri tvorení a umiestňovaní prístupových bodov. Mnou vytvorená sieť je umiestená hlavne v budove C.

Ako prvý parameter, ktorý budem v sieti merať, je samostatný roaming a čas, za ktorý sa koncové zariadenie odpojí a znova pripojí k novému prístupovému bodu. V tomto meraní nebudem používať donwload. Pôjde len o čistý roaming bez zaťaženia prístupového bodu. Meranie bude bez zásahu do nastavenia sieťovej karty tabletu a notebooku. Pri chôdzi po chodbe som nameral tieto hodnoty. Na obrázku 2.11 vidíme graf silu signálu v čase.




Obr. 2.11: Graf sily signálu v čase

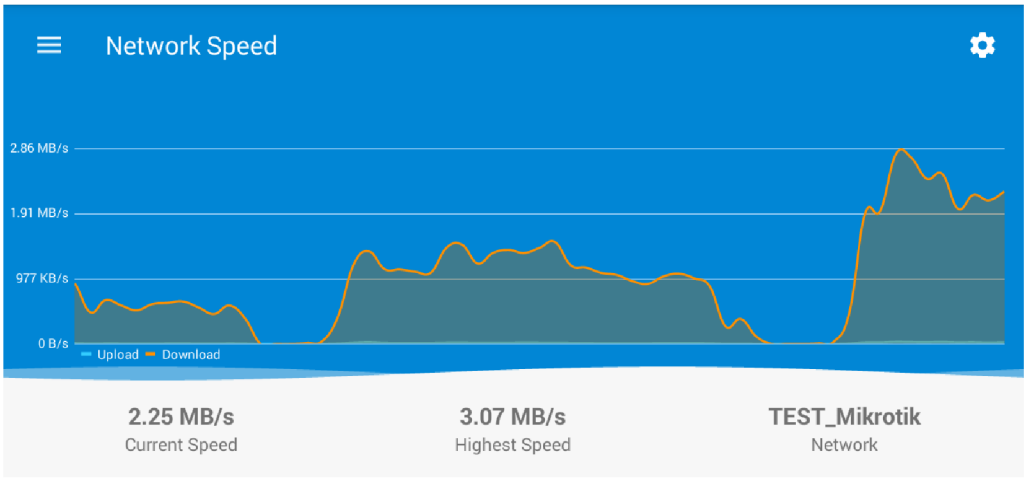
Na tomto grafe môžeme pekne vidieť, kedy koncové zariadenie prevedie roaming. Podnet zmeny prístupového bodu je založený na sile signálu, ktoré zaznamená koncové zariadenie. Vidíme, že koncové zariadenie previedlo roaming tri krát a pripojilo sa počas chôdze k trom prístupovým bodov. Posledná zmena nastala plynule bez výpadku signálu (nachádza sa v časovom rozmedzí 217-220sek). Ostatné procesy roamingu sú vidieť na úplnom výpadku signálu a následnom naskočení. V týchto bodoch zariadenie nemá prístup na internet a je prakticky nepripojené ku žiadnemu prístupovému bodu. Ako náhle sa pripojí, signál od nuly vystrelí nahor, v tej chvíli sme pripojený ku prístupovému bodu s najsilnejším signálom. Tento proces sa opakuje dva krát. Pri meraní a následnom spriemerovaní časových hodnôt roamingu som dospel k výsledku. U notebooku čas roamingu v priemere zabral 0.23sek a pri tablete 0.63sek. Sú to dobré časy keď si predstavíme aká výmena správ nastáva pri roamingu. Samozrejme nezabudnime na to, že v sieti neprichádza ku sťahovaniu väčších dát alebo uploadu, roaming by mal byť čo najrýchlejší. Ďalší proces roamingu je možné vidieť na obrázku 2.12.




Obr. 2.12: Graf signálov prístupových bodov v čase

Môžeme vidieť ako sa sily signálov prekrývajú a zariadenie si vyberá vždy prístupový bod s najsilnejším signálom. Vždy v určitom čase a mieste trasy sa nachádza prístupový bod s najsilnejším signálom ku, ktorému sa koncové zariadenie pripojí. Roaming a pripojenie ku prístupovému bodu reprezentuje hrubá čiara daného signálu prístupového bodu. Graf nám zároveň vykresľuje krivky signálov. Tieto krivky sa dajú použiť pri rozmiestňovaní prístupových bodov. WiFi signál som sa snažil udržať v rozmedzí -30dBm až -60dBm. Toto rozmedzie je ideálne prostredie pre pripojené koncové zariadenie.

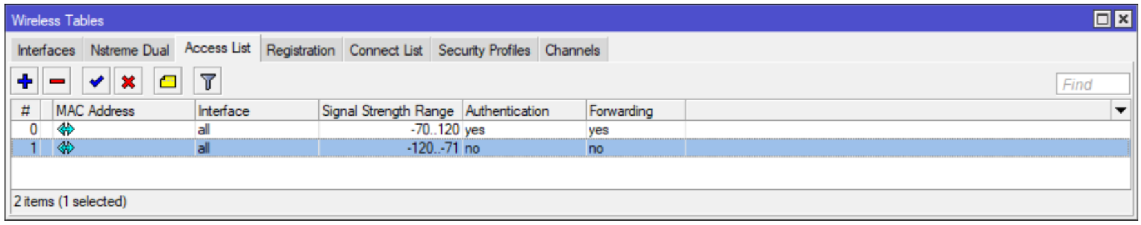
Ďalším testom bol download dát zo servera/cloud. V tomto prípade som na tablete sťahoval aplikáciu z Google play obchodu a na notebooku sťahoval film zo stránky uložto. Pri tomto teste budem sledovať prenosovú rýchlosť, čas roamingu a prípadné oneskorenie prenosu. Pri chôdzi sa prenosová rýchlosť pohybovala pri tablete v priemere na úrovni 1.73MB/s a pri notebooku na úrovni 2.15MB/s. Na obrázku 2.13 vidíme graf a výkyvy prenosovej rýchlosti. Miesta kde je prenosová rýchlosť nulová, nastáva roaming. V týchto častiach vypadne signál na dlhší čas než je ideálne.




Obr. 2.13: Graf rýchlosti prenosu

Tento čas výpadku sa v prípadoch líši. Pri tablete som nameral najvyššiu hodnotu 3.12sekundy a najnižšiu 0.76sekúnd. Priemerná hodnota vyšla 0.89sekundy. Na počítači som nameral lepšie hodnoty a to od 1.5sekundy do 0.16sekundy. V priemerná hodnota vyšla 0.51sekundy. Tieto rozdiely sú zrejme dané rokom výroby a verzou ovládača sieťovej karty. Ideálny roaming by mal nastať bez dlhšieho výpadku signálu, ktorý má za následok oneskorenie prenosu. Ak sa pohybujeme v stotinách sekúnd ide o človekom nepostrehnuteľný čas tým pádom ho hodnotíme ako rýchli roaming. Ako náhle je prekročená hranica a roaming trvá viac sekúnd, je výpadok siete nežiadúci. Pri downloade výpadok pár sekúnd nie je vec, ktorá by vadila. No ale napríklad pri používaní protokolu VoIP je takýto výpadok nedostatkom siete. Každopádne každé oneskorenie pri prenose dát je vec, ktorá by sa mala eliminovať ale nie vždy sa podarí. Existujú určité metódy a kroky, ktoré by mali pomôcť k rýchlejšiemu roamingu. Tieto možnosti overím v ďalších testoch. Toto nastavenie je ale nutné s niečim porovnať, preto v tejto časti meriam sieť bez podpôr rýchlejšieho roamingu, ktorú následne porovnám s úpravami podporujúce rýchly roaming.

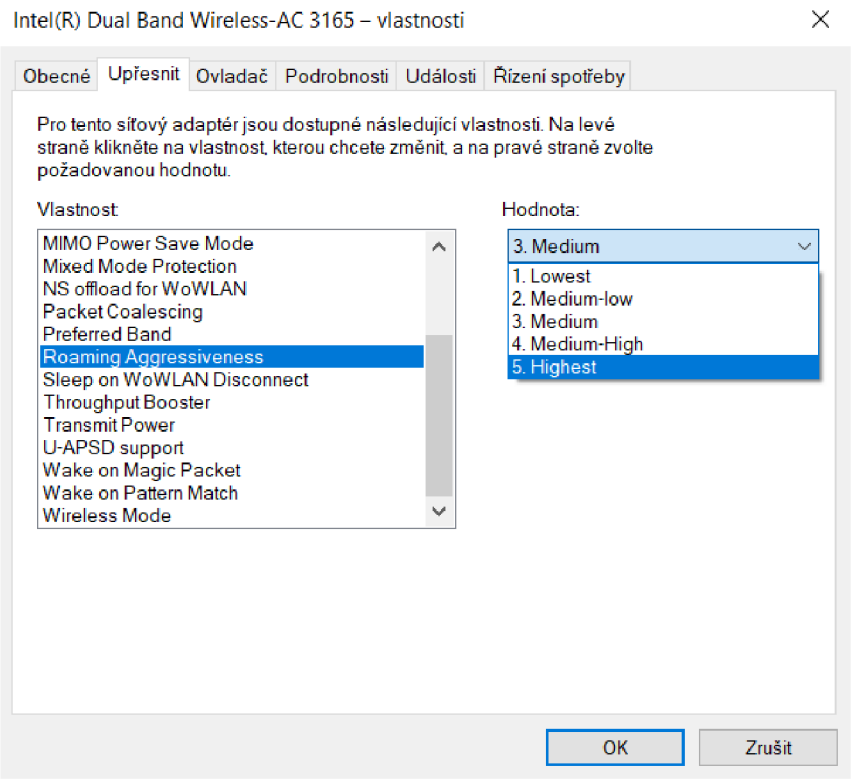
V tejto časti merania vyskúšam aplikovať nastavenia, ktoré pomáhajú rýchlejšiemu roamingu. Keďže impulz na roaming vytvára koncové zariadenie, je teda jasné, že bude hlavne záležať od jeho nastavenia. Existujú aj nastavenia prístupového bodu, ktoré tiež pomáhajú rýchlemu roamingu. Z pravidla to bývjú pravidlá pre pripojenie a odpojenie od siete. Nie všetky zariadenia majú túto možnosť podpory. Mikrotik má na to jedno nastavenie a to vidieť na obrázku 2.14.




Obr. 2.14: Nastavenie podpory rýchleho roamingu

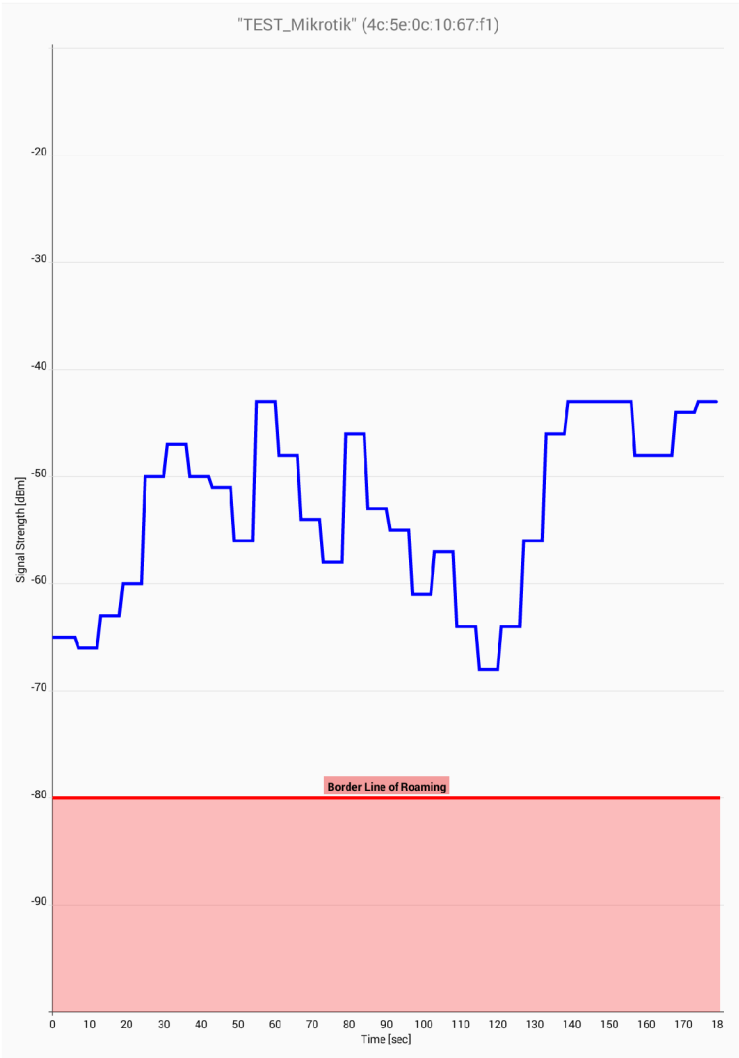
Ide o pravidlo, kde nastavujeme hodnoty sily signálu a následne pravidlo. Nastavené mám rozmedzie od 120dBm do -70dBm zariadenia prijať. Čiže nechať koncové zariadenie aby sa k prístupovému bodu pripojilo. Druhé pravidlo je opakom. Ak sila signálu na koncovom zariadení padne pod -70dBm, prístupový bod odpojí toto koncové zariadenie. Toto nastavenie je možné aplikovať aj na jednotlivé MAC adresy. Ja som pravidlo nechal aplikované na všetky koncové zariadenia. Toto je možnosť ako donútiť koncové zariadenie k procesu roamingu pred tým než sa zbytočne bude držať slabého signálu prístupového bodu. Ďalšia možnosť ako zrýchliť roaming je nastavenie sieťovej karty koncového zariadenia. Na tablete som využíval aplikáciu, v ktorej som si nastavil hranicu prijímaného signálu. Túto hranicu som nastavil na -55dBm. Ak sa sila signálu prístupového bodu dostane pod hranicu -55dBm, zariadenie automaticky prevedie proces roamingu. Na notebooku sa nastavenie mení trochu inak. Je treba si otvoriť vlastnosti sieťovej karty. Následne v záložke upresniť otvoriť nastavenie agresivity sieťovej karty ako je na obrázku 2.15.

Tieto nastavenie sú užitočné a pomáhajú rýchlejšiemu roamingu. Majú ale aj druhú stránku. Sieťová karta tým pádom častejšie sleduje silu signálu a okolité prístupové body. To má za následok väčšiu spotrebu baterky. Nejde o hrozivé čísla ale zmenu som pocítil na konci merania. Baterka vydrží asi o 20 -30minút kratšie.



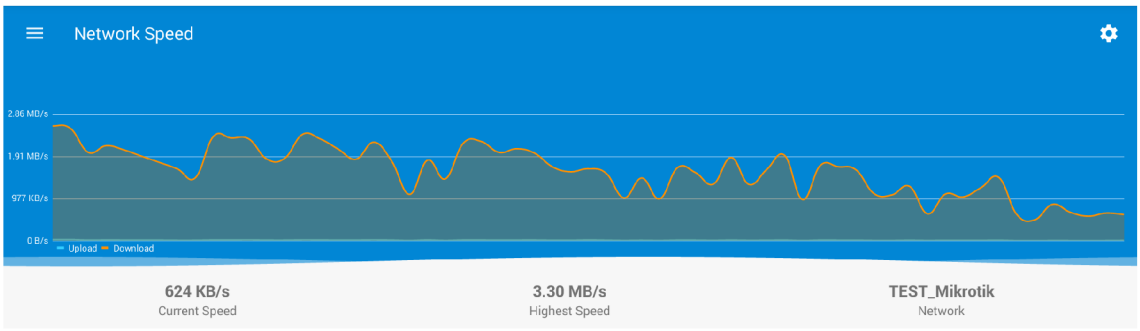

Obr. 2.15: Nastavenie sieťovej karty Intel

Následne som zopakoval testy chôdze zo zariadením bez downloadu a s downloadom. Namerané hodnoty boli podobné ako pri prvých testoch. Zmena sa prejavila v plynulejšom roamingu. Koncové zariadenia menili prístupové body hladšie a prediktívnejšie než u bežného nastavenia. Nenameral som situáciu kedy by koncové zariadenie držalo spojenie s prístupovým bodom príliš dlho a tým pádom stratilo silu signálu. Akonáhle prišla hranica sily signálu pod -55dBm až -65dBm tablet či notebook automaticky využili roaming a pripojili sa na silnejší prístupový bod. Je to zrejme dané dodatočným nastavením, ktoré podporuje rýchlejší roaming. S týmto nastavením sa mi podarilo namerať roaming bez značného výpadku signálu. Časové hodnoty roamingu bez downloadu boli 0,64 sekundy pri tablete a 0,24sekundy pri notebooku. Teda veľmi podobné ako bez dodatočného nastavenia. Počas downloadu sa časové hodnoty zmenili. Konkrétne na 0,5sekundy pri notebooku a 0,78sekundy pri tablete. Vidíme teda zlepšenie v porovnaní bez úprav sieťových kariet.




Obr. 2.16: Graf sily signálu bez výpadku

Pre vykreslenie bezvýpadkového roamingu vidíme na obrázku 2.16. V častiach poklesu vidíme ako koncové zariadenie roamuje z jedného prístupového bodu na druhý. Náhly kolmý vzostup sily signálu znamená pripojenie na ďalší prístupový bod. Toto nastavenie dokázalo, eliminovať viditeľné výpadku signálu. Prenosové rýchlosti sa o trošku zvýšili. Pri notebooku na hranicu 2.54MB/s a na tablete 1.88MB/s. Tieto rýchlosti sú vyššie ako pri meraní bez dodatočných nastavení. Pre lepšie predstavenie pridávam obrázok 2.17. Prenos síce v častiach roamingu miestami kolísal ale nevypadol na znateľne dlhú dobu. Primárne teda ide o najideálnejšie nastavenie prístupového bodu a koncového zariadenia z pohľadu roamingu.

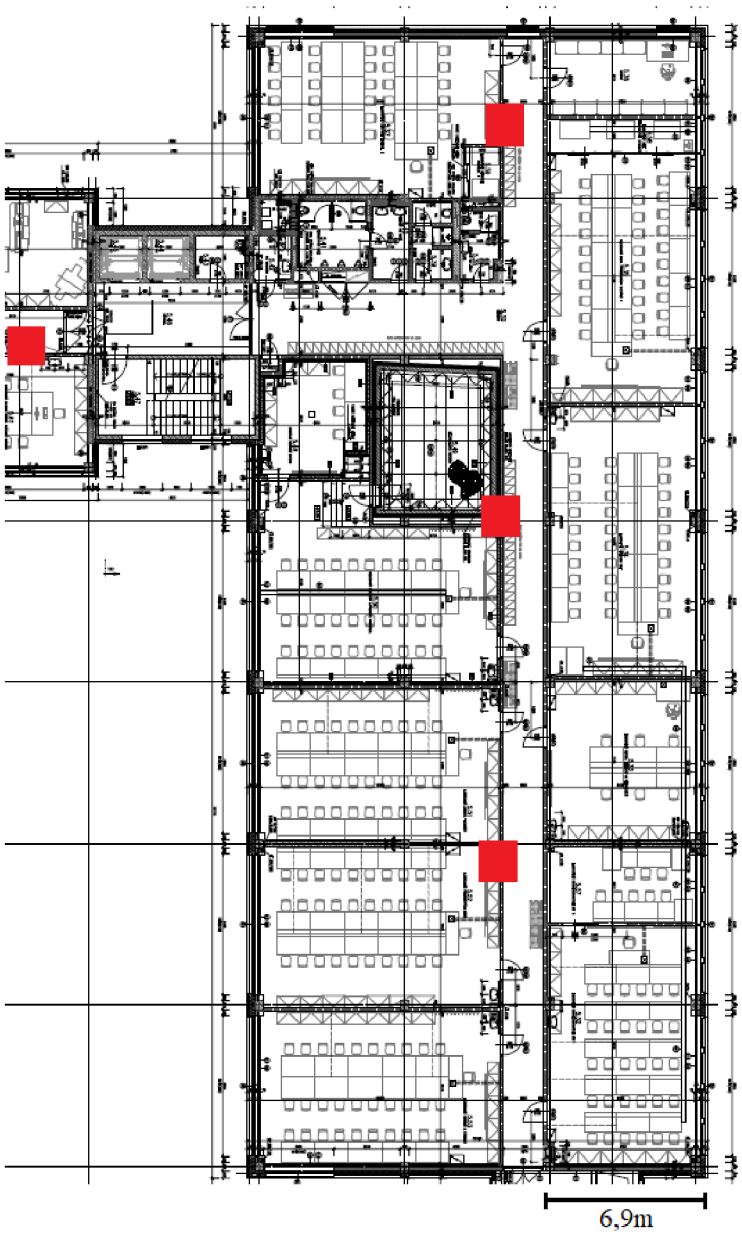



Obr. 2.17: Graf prenosovej rýchlosti bez výpadku

V ďalších kapitolách prevediem totožné meranie pre sieť vutbrno a následne porovnám výsledky.

## 2.5 Nastavenie siete vutbrno

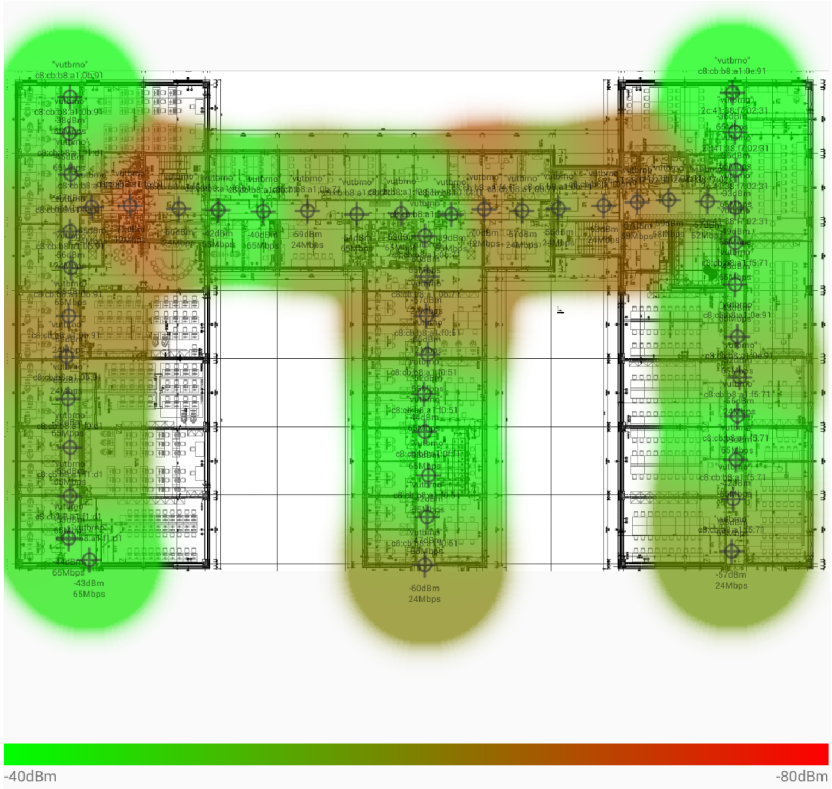
Nepodarilo sa mi zistiť aké nastavenie je aplikované na prístupových bodoch tejto siete. Myslím si, že sa využíva technika cluster popísaná v kapitole HP 1.5. Na týchto prístupových bodoch bežia aj virtuálne siete. Technika merania je rovnaká ako pri testoch so zariadeniami Mikrotik. Na chodbe v časti budovy C sa nachádzajú tri prístupové body. Ich umiestnenie je na znázornené na obrázku 2.18.




Obr. 2.18: Rozmiestnenie prístupových bodov siete vutbrno

Ako je vidieť z obrázku 2.18, prístupového bodu sú umiestené na chodbe.

Rozmiestnenie je ideálne pre pokrytie chodby signálom. Heat mapa pre túto sieť je na obrázku 2.19.

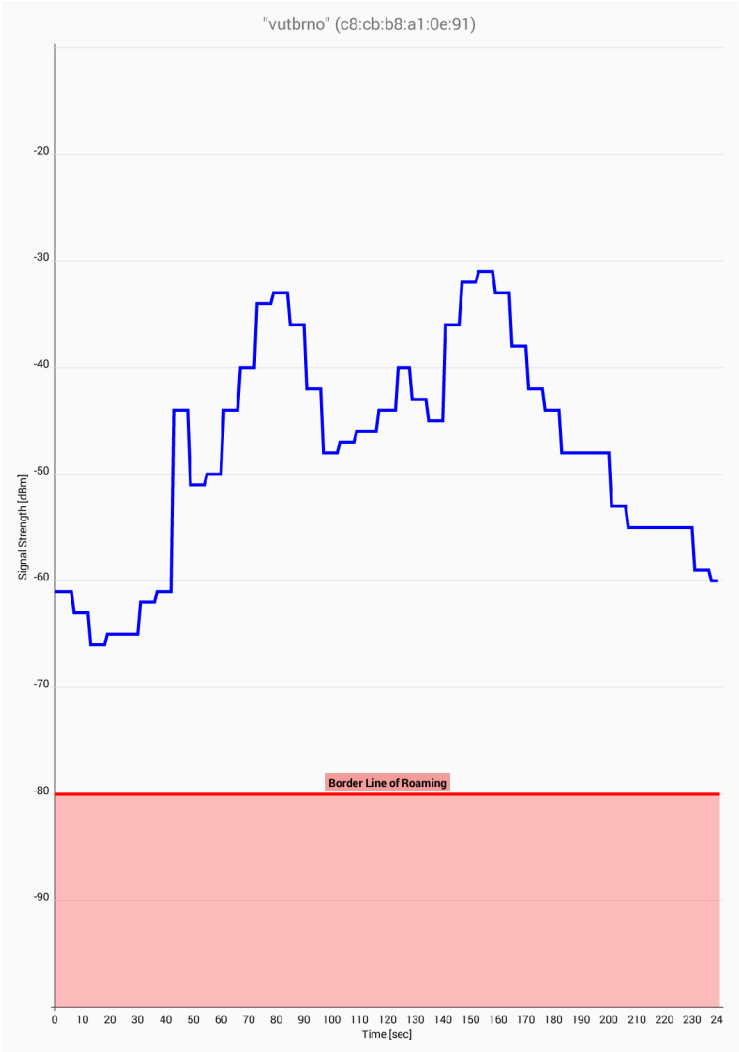



Obr. 2.19: Mapa pokrytia signálom siete vutbrno

Pokrytie signálom je skoro totožné ako pri sieti Mikrotik. Nastavenie siete vutbrno má jedno pravidlo, ktoré môže namerané hodnoty skresliť. Ide o prekročenie povoleného objemu dát. Táto hranica je nastavená na 250MB za sedem dní. túto hranicu som nepresiahol takže meranie je objektívne. Sieť je vytvorená na prvom kanáli. V tomto kanáli sa nachádza pätnásť ďalších sietí. Ako som spomínal väčšina týchto sietí je virtuálna. Meranie tejto siete je jednoduchšie preto, lebo nie je potrebné merať limity prístupových bodov a následne ich rozmiestňovať. Prístupové body sú už rozmiestnené a nevznikajú hluché miesta čím je dôkazom obrázok 2.19. Testovanie som sa snažil naplánovať v taký čas, kedy nebude veľa koncových zariadení pripojených na túto sieť. Keďže na sieti vytvorenej na prístupových bodoch Mikrotik boli pripojené len dve koncové zariadenia a to tablet a notebook. Je teda nutné v rámci objektívnosti merania, rovnaký test previesť aj na sieti vutbrno.

### 2.5.1 Výsledky pre sieť vutbrno

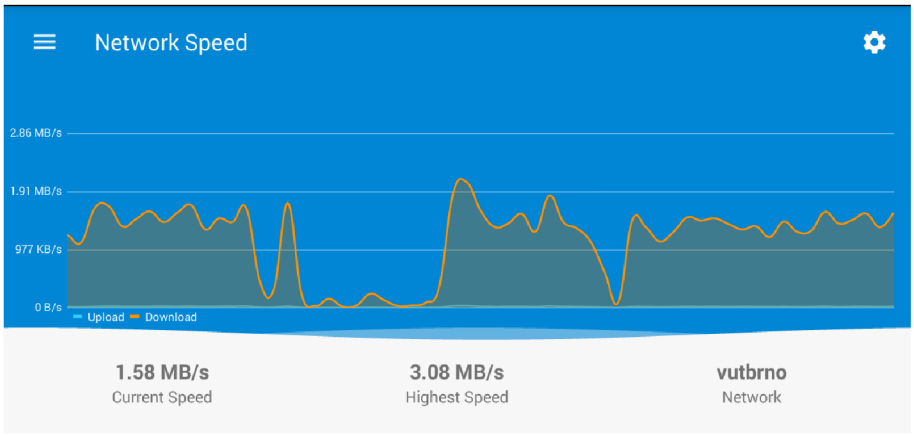
Ako aj pri časti merania prístupových bodov od firmy Mikrotik, tak aj tu prvé meranie bude chôdza po chodbe bez downloadu či uploadu. Sila signálu počas chôdze chodbou je vykreslená na obrázku 2.20.




Obr. 2.20: Graf sily signálu na čase pre sieť vutbrno

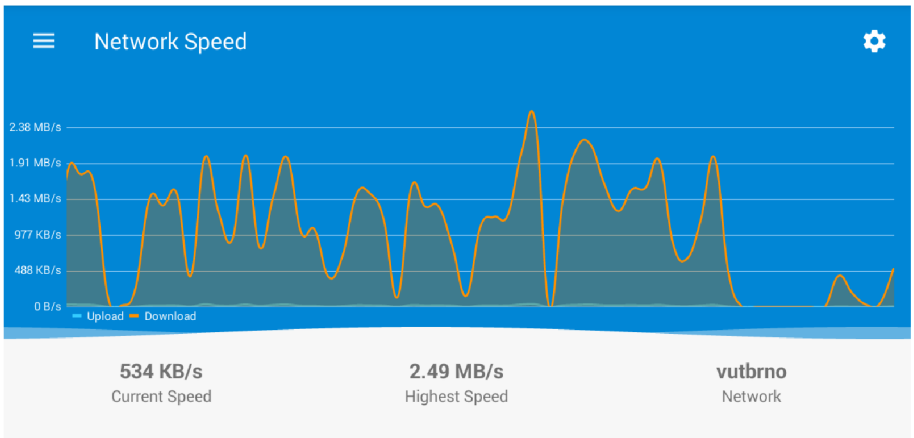
Na grafe vidíme podobné hodnoty ako sme namerali pri testoch Mikrotik s jedným rozdielom. Pri tomto meraní sa mi často stávalo, že sa koncové zariadenie nepripojilo na stredný prístupový bod. Jednoducho ho po ceste ignorovalo a pripojilo sa až k poslednému. Túto situáciu máme krásne vykreslenú na obrázku 2.20. Dva vrcholy nám ukazujú miesta po ceste kde má daný prístupový bod najsilnejší signál. Toto ignorovanie je zrejme dané tým, že sú prístupové body blízko pri sebe a signály sa prekrývajú. Rýchlosť roamingu na koncových zariadeniach bola veľmi

podobná ako pri meraní v kapitole 2.4.1. Pri tablete 0,65sekundy a pri notebooku 0,22sekundy.




Obr. 2.21: Graf prenosovej rýchlosti site vutbr

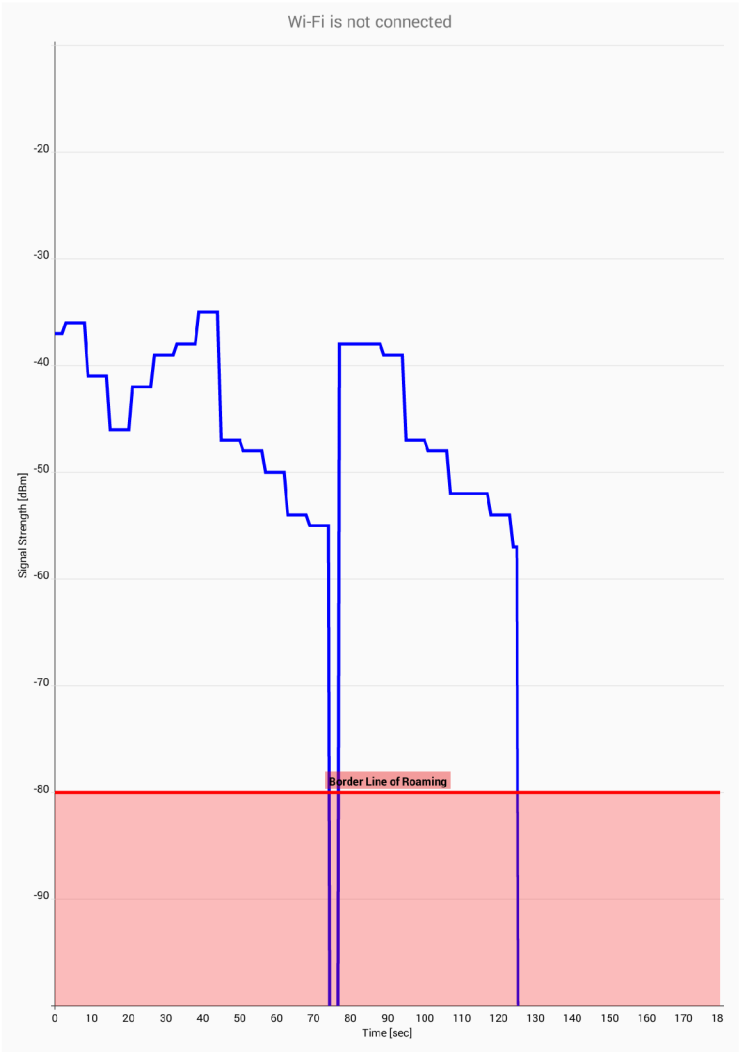
Nasledovalo meranie downloadu. Ako som spomínal, je dôležité neporušiť jedno z pravidiel VUT siete a to neprekročiť hranicu stiahnutých dát. Prenosová rýchlosť sa pohybovala 1,55MB/s na tablete a 1,97MB/s na notebooku. Časové hodnoty roamingu boli 0,84sekundy na tablete a 0,49sekuundy na notebooku. Pri meraní som sa stretol s častým kolísaním prenosovej rýchlosti pri chôdzi. Toto kolísanie je zobrazené na obrázku reffig:vutbrmiesto. Prenosová rýchlosť kolísal aj keď som stál na jednom mieste čo môžeme vidieť na obrázku 2.22.




Obr. 2.22: Graf prenosovej rýchlosti site vutbr

Toto kolísanie si neviem vysvetliť. Pri prenose nastávajú také výkyvy až miestami prenosová rýchlosť dosahuje iba niekoľko desiatok kB/s. Samozrejme sieť nie je stavaná na to aby sa cez ňu sťahovali veľké objemy dát na úkor ostatnej premávky.

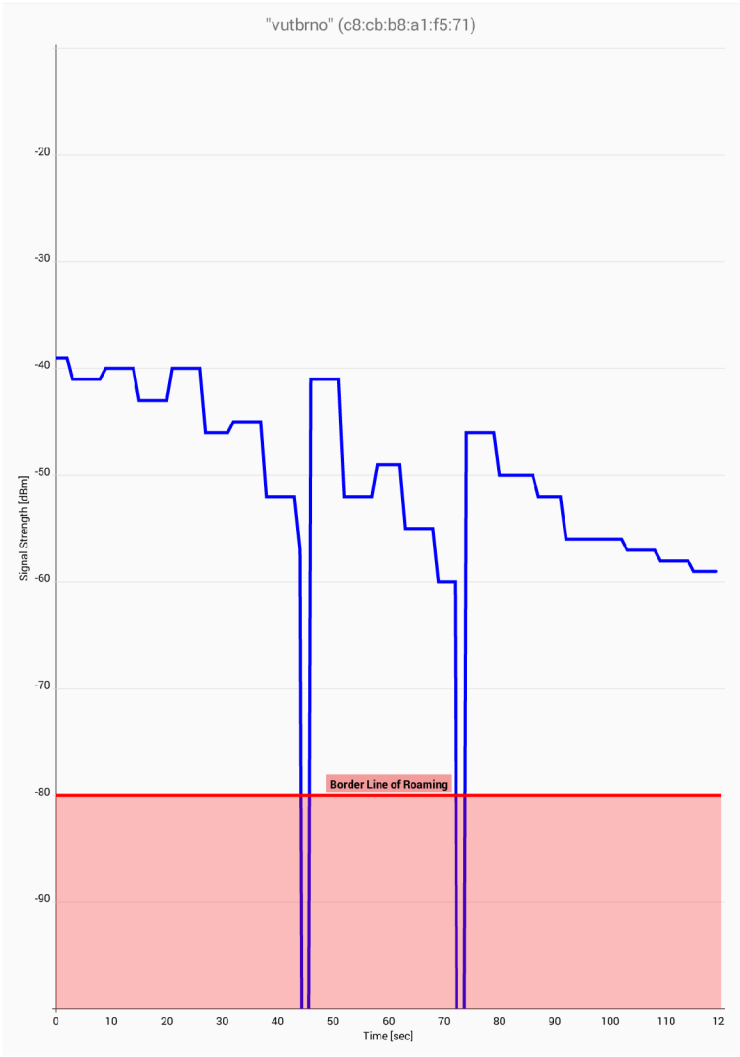
Aj tak je kolísanie príliš veľké. Pri chôdzi miestami sa nastala situácia výpadku signálu na dlhšiu dobu ako 5sekúnd. Miestami tento výpadok trval 17sekúnd. Tento razantný výpadok je možné vidieť na obrázku 2.23.




Obr. 2.23: Graf výpadku sily signálu siete vutbr

V tomto prípade ide o razantný výpadok pripojenia. Tento problém sa mi často vyskytoval na tablete. S notebookom nastal skôr zriedkavo. Je to možno dané staršou sieťovou kartou tabletu. Zrejme nastalo oneskorenie v overovaní pripojenia a prístupu. Problém môže byť aj v tom, že koncové zariadenie si nevedelo vybrať ku, ktorému prístupovému bodu sa má pripojiť. Ako som na začiatku kapitoly spomínal, miestami koncové zariadenie ignorovalo stredný prístupový bod a pripojilo sa až k poslednému. Zrejme situáciu nevyhodnotilo ako ideálny čas na roaming a čakalo až bolo neskoro a pripojilo sa k poslednému prístupovému bodu. Následne sa po dlhšom čase k prístupovému bodu koncové zariadenie pripojilo.

Pre zlepšenie roamingu som teda nastavil sieťové karty koncových zariadení tak ako pri teste so sieťou Mikrotik a meral či sa hodnoty zmenia. Nastavenie prístupových bodov som nemohol modifikovať. V tom bude rozdiel medzi meraniami. Po dodatočnom nastavení som nameral tieto hodnoty. Počas chôdze bez downloadu sa hodnoty roamingu moc nemenili. Priemerom som získal tieto hodnoty. Hodnota tabletu je 0,71sekundy pri notebooku 0,33sekundy. V tomto prípade graf sily signálu je zobrazený na obrázku 2.24. V sieti Mikrotik som dokázal eliminovať dlhší výpadok siete a graf bol plynulý. V sieti vutbr sa mi to nepodarilo. Vždy som nameral krátky výpadok, ktorý je znázornený aj na tomto obrázku. V podstate to nemalo žiaden vplyv na plynulosť prenosu a časy roamingu sú podobné ako pri sieti Mikrotik.




Obr. 2.24: Graf sily signálu siete vutbr po dodatočnom nastavení

Prenosová rýchlosť bola skoro totožná ako v meraní bez modifikácie sieťových kariet a to 1,62MB/s pri tablete a 2,01MB/s na notebooku. Rýchlosť prenosu sa

mi týmto nastavením nepodarilo zrýchliť. Roaming zabral v priemere 0,8sekundy tabletu a 0,53sekundy notebooku. Škoda je, že som sa nemohol pozrieť na zúbok siete vutbr a prípadne zmeniť nastavenia prístupových bodov tak ako u Mikrotiku. Každopádne som sa snažil meranie smerovať objektívne pre obe siete a výsledky okomentujem v kapitole nižšie.

## 2.6 Porovnanie výsledkov

V tejto časti porovnám výsledky merania siete vytvorenej z prístupových bodov Mikrotik a siete vutbr tvorenej z prístupových bodov HP. Výsledky merania vložím do tabuliek pre ľahšie porovnanie. V tabuľke 2.1 vidíme hodnoty prenosovej rýchlosti počas downloadu. Druhý riadok reprezentuje download s modifikáciou sieťových kariet na koncových zariadeniach. Ďalšia tabuľka 2.2 reprezentuje hodnoty pre sieť vutbr.

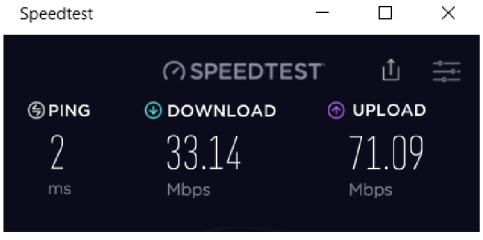
| | Tablet | Notebook |
|---|---|---|
| Download | 1,73MB/s | 2,15MB/s |
| Download s modifikáciou | 1,88MB/s | 2,54MB/s |

Tab. 2.1: Výsledky prenosovej rýchlosti siete vutbr

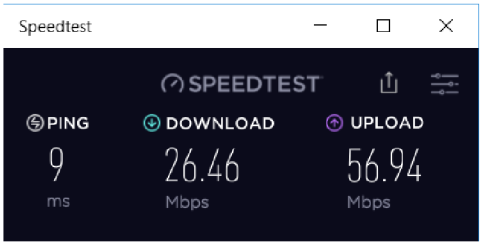
| | Tablet | Notebook |
|---|---|---|
| Download | 1,55MB/s | 1,97MB/s |
| Download s modifikáciou | 1,84MB/s | 2,2MB/s |

Tab. 2.2: Výsledky prenosovej rýchlosti Mikrotik

Z tabuliek 2.2 a 2.1 je vidieť, že rýchlejšia prenosová rýchlosť je na prístupových bodoch Mikrotik. Nejde o veľký rozdiel hodnôt no predpokladal som, že sieť Mikrotik bude mať vyššie hodnoty. Ikeď prístupové body siete vutbr majú vyššie výpočtové parametre ako Mikrotik, nedokázali nameranou prenosovou rýchlosťou prekonať Mikrotik. Procesor, RAM a pamäť týchto prístupových bodov je násobne väčšia ako u Mikrotiku. Je teda otázka prečo výsledky vyšli naopak. Zrejme ide o ďalšie obmedzenie premávky koncového zariadenia na určitú maximálnu prenosovú rýchlosť. Prístupové body sa líšia aj cenou. Drahšie zariadenia má sieť vutbr. Rýchlosť som zmeral aj pomocou SpeedTestu a výsledky sú na obrázkoch 2.25 a 2.26.




Obr. 2.25: SpeedTest siete Mikrotik




Obr. 2.26: SpeedTest siete vutbr

Aj toto overenie ukazuje, že skutočne sieť Mikrotik má vyššie hodnoty či už downloadu alebo uploadu ako sieť vutbr. Overenie som robil bez chôdze po chodbe.

Tabuľky 2.3 a 2.4 sú naplnené výsledkami meraní s časom roamingu. Všetky hodnoty boli merané počas chôdze po chodbe.

| | Tablet | Notebook |
|---|---|---|
| Bez downloadu | 0,63s | 0,23s |
| S downloadom | 0,83s | 0,51s |
| Upravené nastavenia | 0,64s | 0,24s |
| Upravené nastavenia download | 0,78s | 0,5s |

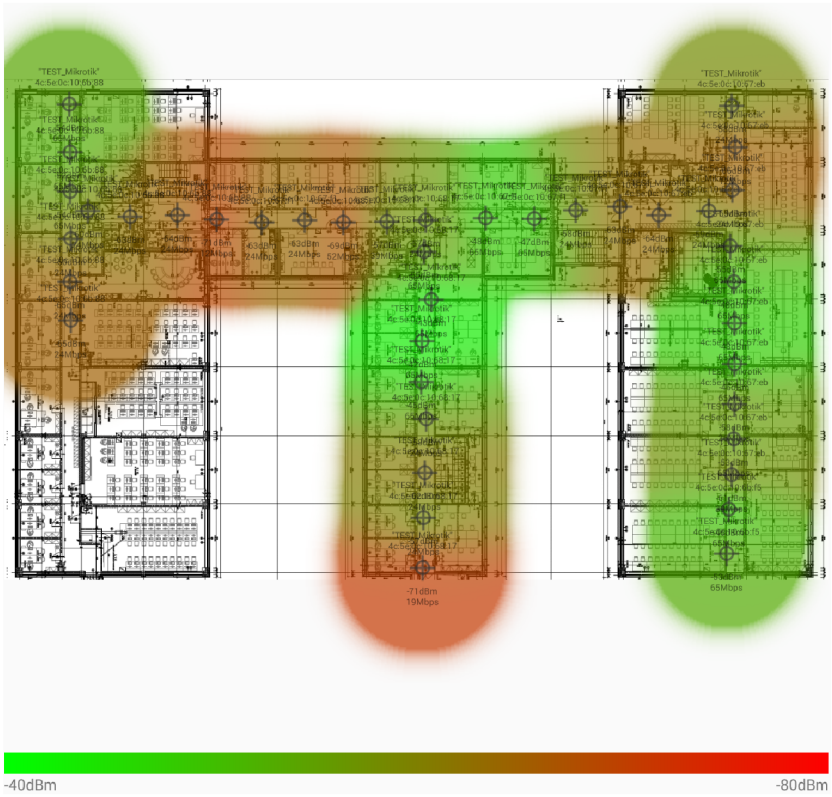
Tab. 2.3: Priemerné časové hodnoty roamingu v sieti Mikrotik

| | Tablet | Notebook |
|---|---|---|
| Bez downloadu | 0,65s | 0,22s |
| S downloadom | 0,84s | 0,49s |
| Upravené nastavenia | 0,71s | 0,33s |
| Upravené nastavenia download | 0,8s | 0,53s |

Tab. 2.4: Priemerné časové hodnoty roamingu v sieti vutbr

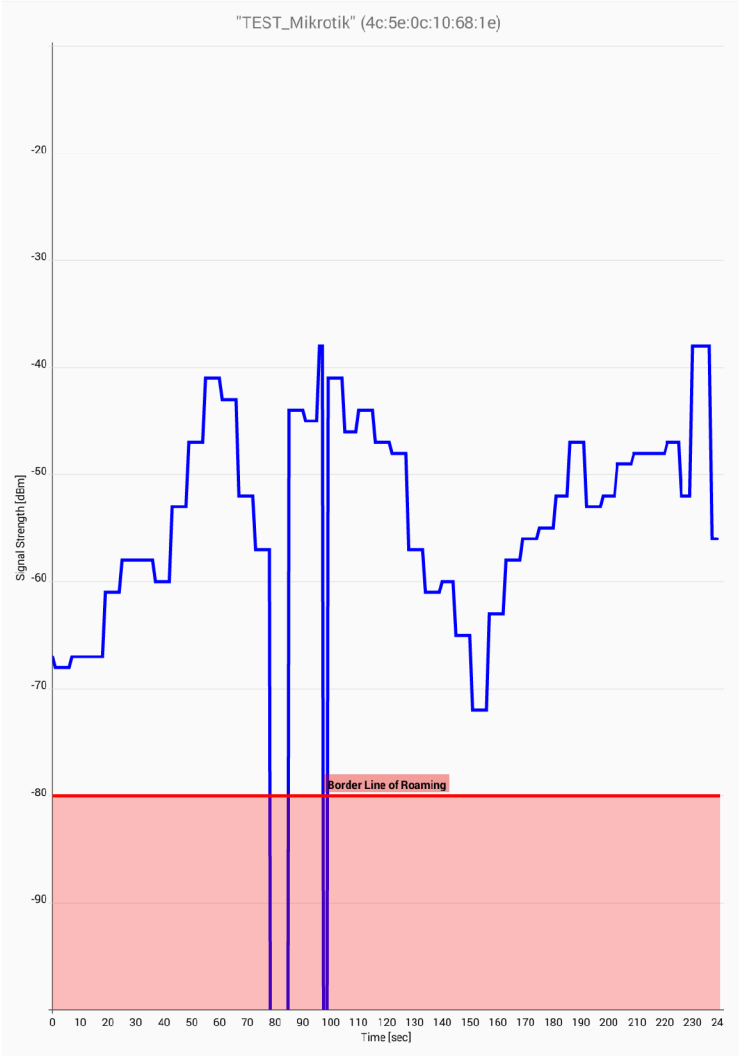
Hodnoty sú si veľmi podobné. Môžem povedať, že pri tomto meraní nie je žiaden výrazný rozdiel. Jediný rozdiel je medzi tabletom a notebookom. Tablet je skutočne pomalejší ako notebook. Je to zrejme dané ich sieťovými kartami. Tablet je o päť rokov starší ako notebook a ešte nepodporuje 5GHz pásmo WiFi signálu. Ide o prvú generáciu tohto tabletu. Za päť rokov sa výpočtová technika posunula o niečo ďalej. Je teda jasné, že má horšie výpočtové parametre ako notebook.

Záverečným testom bol prechod z časti budovy E do časti budovy C. Rotmiestnenie prítupových bodov site Mikrotik vidíme na obrázku 2.27 a pre siet vutbr na obrázku 2.19. Môžeme vidieť, že pokrytie signálom je podobné ako u siete vutbr.



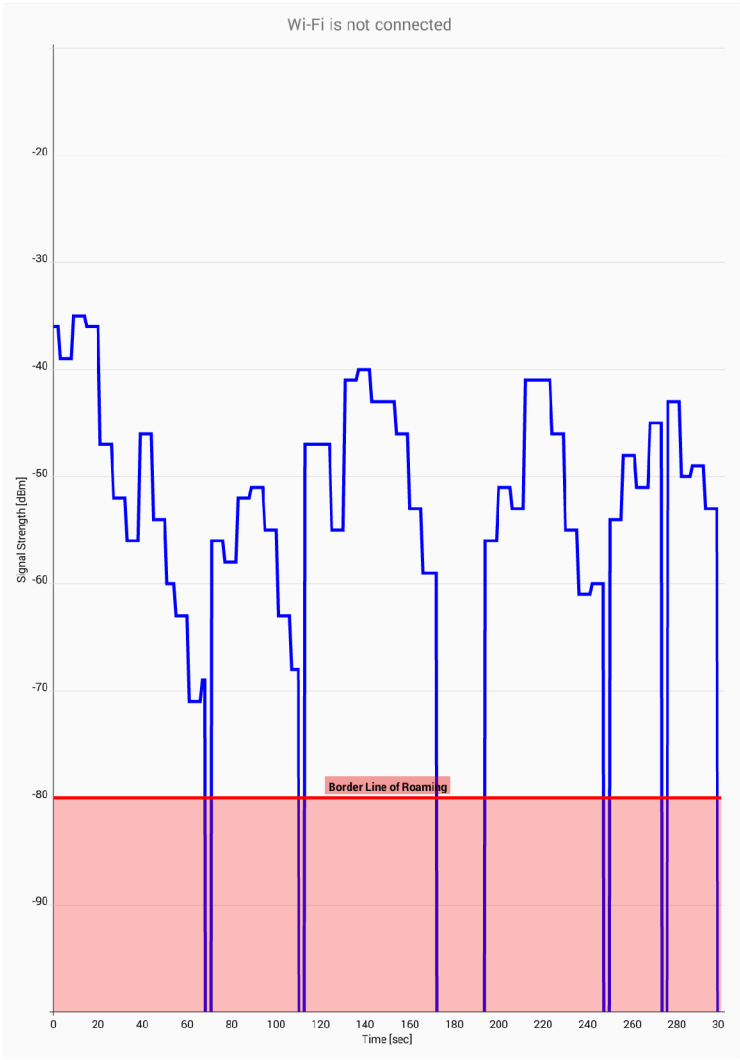

Obr. 2.27: Mapa pokrytia signálom siete Mikrotik na 5NP

Prenos prebiehal rovnako ako pri meraní v časti budovy C, tak ako som predpokladal. Pre názornú ukážku pridávam obrázky 2.28 pre sieť Mikrotik a obrázok 2.29 pre sieť vutbr. Tu vidíme rovnaké procesy prihlasovania a odhlásenia od prístupového bodu. Pri sieti Mikrotik, v niektorých situáciách je roaming tak plynulí, že som neevidoval výpadok dlhší ako 0,2sekundy. Zato pri sieti vutbr evidujem dlhšie výpadky počas roamingu. V niektorých prípadoch aj nad 2sekundy. Tieto hodnoty, ako som už spomínal nie sú ideálne.



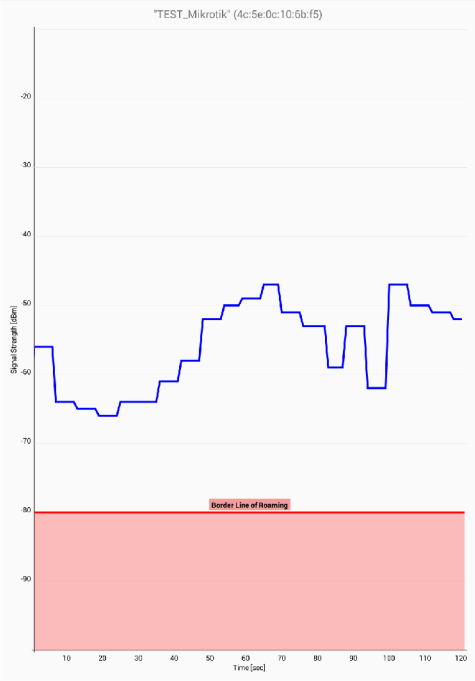

Obr. 2.28: Sila signálu siete Mikrotik pri chôdzi po 5NP

Pri nameraných hodnotách a výsledkoch, môžem skonštatovať sieť Mikrotik v meraní dopadla lepšie ako sieť vutbr. V tejto sieti zariadenie rýchlejšie a plynulejšie menilo prístupové body. Dokázalo vytvoriť prostredie s vyššou prenosovou rýchlosťou. Tieto parametre sú hlavným úskalím rýchleho roamingu.

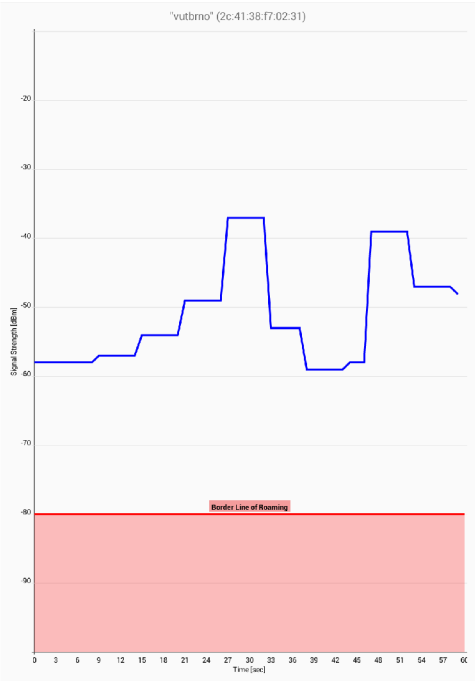



Obr. 2.29: Sila signálu siete vutbr pri chôdzi po 5NP

Pre zaujímavosť som previedol ešte jedno meranie. V tomto prípade som bežal po chodbe v časti C, z jednej strany na druhú. Dopadlo to tak ako som aj predpokladal. Koncové zariadenia v oboch sieťach ignorovali stredné prístupové body a pripojili sa až ku poslednému. To je krásne vidieť na obrázkoch 2.30 a 2.31. Je to dané rýchlosťou pohybu koncového zariadenia. To v určitých časových intervaloch kontroluje okolité siete a ich sily signálov. Za tento čas si koncové zariadenie zapamätalo silu signálu prvého prístupového bodu. Následne kontrolovalo okolie až keď som bol skoro úplne na konci chodby a pripojilo sa teda k poslednému prístupovému bodu.




Obr. 2.30: Sila signálu siete Mikrotik pri behu




Obr. 2.31: Sila signálu siete vutbr pri behu

# 3 ZÁVER

V tejto práci som rozobral problematiku a možnosti roamingu u technológie 802.11. Podrobne rozpísal procesy, ktoré nastávajú pri autorizácií a opätovnej autorizácií k prístupovému bodu počas roamingu. Naštudoval a otestoval možnosti nastavenie siete z prvkami Mikrotik. Následne testoval sieť s prvkami Mikrotik a HP. Z naštudovanej problematiky roamingu som vytvoril testovaciu metodiku a následne aplikoval pri meraní. Meranie niekoľkokrát opakoval aby výsledky dávali odpovedajúce hodnoty. Porovnal možnosti a výhody výrobcu MikroTik a siete vutbrno používané zariadenia HP. Namerané hodnoty zapísal do tabuliek a pre vykreslenie použil obrázky. Príslušne okomentoval tieto výsledky. Porovnal a zhodnotil namerané výsledky následne dospel k záveru. Sieť z prvkov Mikrotik mala najlepšie hodnoty. Roaming v tejto sieti prebiehal rýchlo a plynule. Neboli namerané veľké výpadky v porovnaní so sieťou vutbr. Prenosová rýchlosť dosiahla vyššie hodnoty ako sieť vutbr. Pri meraní som sa časti stretol s dlhým výpadkom pripojenie do siete vutbr. Ak ide o nastavenie sieťovej karty, oplatí sa meniť ak sa pohybujeme v kancelárskom priestore poprípade vo väčšej budove. Teda presúvame sa z jedného miesta na druhé, alebo meníme podlažia. Počas týchto procesov potrebujeme pripojenie na sieť. Roaming s tomto nastavení je plynulejší. Pre domáce použitie by som volil nastavenie menej agresívnejšie. Teda sieťová karta nekontroluje parametre siete a okolie v kratších časových intervaloch ale naopak. Optimalizácia chovania sieťovej karty napomáha k rýchlejšiemu a plynulejšiemu roamingu. Ide teda o preferencie koncového užívateľa a priestoru, kde chce využiť rýchli roaming. V meraní dopadla sieť z prvkov Mikrotik ako rýchlejšia vo všetkých smeroch. Znova pripomínam, že sieť vutbr má určité pravidlá. Ak by som vytvoril sieť z prvkov HP podľa seba, výsledky by sa mohli líšiť.

# LITERATÚRA


[1] The IEEE 802.11 universe [online]. Dostupné z URL: <http://ieeexplore.ieee.org/document/5394032/#full-text-section>.

[2] Wi-Fi Alliance [online]. Dostupné z URL: <https://www.wi-fi.org/>.

[3] Making the choice: 802.11a or 802.11g [online]. Dostupné z URL: <http://www.wi-fiplanet.com/tutorials/article.php/1009431>.

[4] 802.11h helps WLANs share spectrum [online]. Dostupné z URL: <https://www.networkworld.com/article/2323593/tech-primers/802-11h-helps-wlans-share-spectrum.html>.

[5] Next generation wireless LANs [online]. Dostupné z URL: <https://books.google.cz/books?hl=en&lr=&id=QZggAwAAQBAJ&oi=fnd&pg=PR19&dq=802.11n&ots=NVqkkqWeHR&sig=i5Y8jHM7rK4uZXtlj6dSEyKpdEs&redir_esc=y#v=onepage&q=802.11n&f=false>.

[6] 802.11ac vs 802.11n – What´s the difference between the Wi-Fi standards? [online]. Dostupné z URL: <http://www.trustedreviews.com/opinion/802-11ac-vs-802-11n-what-s-the-difference-2905251>.

[7] WiFi on steroids: 802.11ac and 802.11ad [online]. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6704471>.

[8] What is 802.11r? Why is this important? [online]. Dostupné z URL: <https://blogs.cisco.com/wireless/what-is-802-11r-why-is-this-important>.

[9] Fast handoff among IEEE 802.11r mobility domains [online]. Dostupné z URL: <https://pdfs.semanticscholar.org/f037/7411c2180d47cfb223b0bb553dc1912e8542.pdf?_ga=2.160357885.1954946331.1512323296-9123424.1512323296>.

[10] Secure roaming in 802.11 networks [online]. Dostupné z URL: <URL:https://ebookcentral.proquest.com/lib/vutbrno/reader.action?docID=305653&ppg=89>.

[11] A mobility for studying wireless communication and the complexity of problems in the model [online]. Dostupné z URL: <http://onlinelibrary.wiley.com/doi/10.1002/net.21452/abstract>.

[12] 802.11 wireless networks: The definitive guide, 2nd edition [online]. Dostupné z URL: <http://shop.oreilly.com/product/9780596100520.do>.

[13] Wi-Fi roaming 101 [online]. Dostupné z URL: <https://blogs.cisco.com/wireless/wi-fi-roaming-101>.

[14] 802.11 WLAN Roaming and Fast-Secure Roaming on CUWN [online]. Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html>.

[15] Manual CAPsMAN [online]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:CAPsMAN>.

[16] Why the 802.11k and Neighbor Report are Important? [online]. Dostupné z URL: <https://blogs.cisco.com/wireless/why-the-802-11k-and-neighbor-report-are-important>.

[17] Towards WiFi Mobility without FastHandover [online]. Dostupné z URL: <https://www.usenix.org/system/files/conference/nsdi15/nsdi15-paper-croitoru.pdf>.

[18] HP Configuration Guide [online]. Dostupné z URL: <https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02659218>.

# ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

AAA server - Authentication, Authorization, and Accounting server

ARP - Address Resolution Protocol

BSS - Basic Service Sets

BUT - Brno University of Technology

CAP - Controled Acces Point

CAPsMAN - Controled Acces Point system Manager

CCKM - Cisco Centralized Key Managment

CSMA/CA - Carrier-sense multiple access with collision avoidance

CSMA/CD - Carrier-sense multiple access with collision detection

dBm - decibel-milliwatts

DCF - Distributed coordination function

DFS - Dynamic Frequency Selection

DHCP - Dynamic Host Configuration Protocol

DS - Direct Sequence

DSSS - Direct-Sequence Spread Spectrum

DTLS - Datagram Transport Layer Security

EDGE - Enhanced Data rates for GSM Evolution

ESS - Extended Service Set

FCS - Frame Check Sequence

FH - Frequency Hopping

FHSS - Frequency-hopping spread spectrum

FTP - File Transfer Protocol

HD - High Definition

HP - Hewlett-Packard

HTTP - Hypertext Transfer Protocol

ID - Identity Document

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol

ISP - Internet Service Provider

ITU - International Telecommunication Union

KZ - Koncové Zariadenie

LAN - Local Area Network

LTE - Long Term Evolution

MAC - Mediam Access Control

MIMO - Multiple-Input and Multiple-Output

MSK - Master Session Key

OFMD - Orthogonal frequency-division multiplexing

PB1 - Prístupový bod 1

PB2 - Prístupový bod 2

PBCC - Packet Binary Convolutional Code

RAM - Random Access Memory

SDM - Spatial Division Multiplexing

SSID - Service Set Identifier

TCP - Transmission Control Protocol

VoIP - Voice over Internet Protocol

VUT - Vysoké Učení v Brně

WAN - Wide Area Network

WECA - Wi-Fi Alliance

WEP - Wired Equivalent Privacy

WFA - Wi-Fi Alliance

WiFi - Wireless Fidelity

WLAN - Wireless Local Area Network

WLC - Wireless LAN Controler

# ZOZNAM PRÍLOH

# A OBSAH PRILOŽENÉHO CD

Na priloženom CD sa nachádza elektronická forma práce v PDF.