VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Filip Krulich

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

POKROČILÝ ROAMING VE WI-FI SÍTÍCH
ADVANCED ROAMING IN WI-FI NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Filip Krulich**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Ilgner**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Filip Krulich ***ID:*** 187201
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Pokročilý roaming ve Wi-Fi sítích

POKYNY PRO VYPRACOVÁNÍ:

Analyzujte možnosti rychlého roamingu umožňující rychlé přepojení klienta bezdrátové sítě IEEE 802.11 k přístupovému bodu se silnějším signálem. Zaměřte se na standardy IEEE 802.11k, 802.11r a 802.11v. Vysvětlete jejich princip, vzájemnou koexistenci a zjistěte jejich podporu u majoritních klientských operačních systémů a bezdrátových karet.
Do operačního systému OpenWrt pro vestavěná zařízení přidejte programové vybavení, které umožní využívat rychlý roaming i na této platformě. Umožněte snadnou správu z grafického rozhraní LuCi. Případné úpravy systému distribuujte jako opkg balíček. Na několika zařízeních se systémem OpenWrt vytvořte testovací topologii, která bude umožňovat rychlý roaming. Na ní testujte provedená opatření v různých scénářích. Změřte rychlost připojení před a po nasazení uvažovaných standardů na různých klientských zařízeních. Porovnejte hodnoty s implementací v bezdrátových zařízeních Mikrotik.

DOPORUČENÁ LITERATURA:

[1] GORANSSON, P. a R. GREENLAW. Secure Roaming in 802.11 Networks. Oxford: Elsevier Science & Technology, 2011. ISBN 9780750682114.

[2] IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2. USA: IEEE, 2008. DOI: 10.1109/IEEESTD.2008.4573292.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Petr Ilgner
Konzultant:

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

UPOZORNĚNÍ:
Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Tato práce se zabývá problematikou Wi-Fi roamingu. Popisuje a přibližuje jak k této problematice přistupují doplňky standardu 802.11 zaměřující se na podporu roamingu, tedy doplňky 802.11r, 802.11k a 802.11v. Součástí této práce je sestavení topologie založené na sytému OpenWrt, na které je testován roaming před a po nasazení těchto standardů. Po testování je ukázán kratší čas roamingu, kterého je dosaženo díky použití těchto standardů. Rovněž je zde sestavena identická testovací topologie založená na zařízeních Mikrotik, na které je otestováno, že zařízení Mikrotik tyto standardy nepodporují.

KLÍČOVÁ SLOVA

802.11k, 802.11r, 802.11v, OpenWrt, Roaming, Wi-Fi, WLAN

ABSTRACT

This work deals with the issues of Wi-Fi roaming. It describes, how amendments of IEEE 802.11 focused on roaming, namely 802.11r, 802.11k and 802.11v, deal with these issues. Part of this work is designing a topolgy based on OpenWrt system, on which to test roaming before and after using these amendments. After testing, lower roaming times are exhibited, thanks to using these standards. There is also designed an identical topolgy based on Mikrotik devices, on which it's demonstrated, that Mikrotik devices do not support these standards.

KEYWORDS

802.11k, 802.11r, 802.11v, OpenWrt, Roaming, Wi-Fi, WLAN

KRULICH, Filip. *Pokročilý roaming ve Wi-Fi sítích*. Brno, Rok, 44 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Petr Ilgner

Vysázeno pomocí balíčku `thesis` verze 3.03; `http://latex.feec.vutbr.cz`

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Pokročilý roaming ve Wi-Fi sítích“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Petru Ilgnerovi, za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Obsah

Seznam obrázků

Úvod

Masový nárůst bezdrátových sítí, který se v posledních pár letech objevil, s sebou přináší i různá úskalí. Jak se zvyšovaly přenosové rychlosti, zvyšovaly se i nároky na sítě kladené.

Jedním z nejvýraznějších výhod bezdrátových sítí je mobilita. Možnost přesunout se z místa na místo bez ztráty konektivity do sítě, je nespornou výhodou oproti kabelovému připojení. Tato práce se zabývá právě problematikou tohoto přemisťování a zaměřuje se na procesy, které nastanou v moment, kdy klientské zařízení začne s vyšší vzdáleností od přístupového bodu ztrácet signál a nastane nutnost připojit se na bližší přístupový bod se signálem lepším.

Jak se technologie bezdrátových sítí rozrůstala, bylo zapotřebí lepšího a lepšího zabezpečení, což způsobilo v přepojení k lepšímu přístupovému bodu větší zpoždění. Aby byla zachována bezpečnost komunikace a šifrovaného spojení, musí totiž zařízení při přepojení k tomuto přístupovému bodu opět projít celým procesem autentizace. Z tohoto důvodu byl vyvinut standard IEEE 802.11r, který tento proces značně zlehčuje a kterým se zabývá tato práce.

Spolu s 802.11r se tato práce také zaměřuje na standardy IEEE 802.11k a IEEE 802.11v, které přináší do problematiky roamingu další funkce a mechanismy, které pomáhají celkovému výkonu a stabilitě bezdrátových sítí.

Pro praktické testování těchto standardů je tato práce zaměřená zejména na platformu OpenWrt. Jedná se o volně šiřitelný operační systém určený pro síťová zařízení. Tento systém může použít kdokoliv jak ve své domácnosti tak v náročnějším firemním prostředí, proto můžou mít tyto standardy implementované na těchto zařízení velký dopad na bezdrátové sítě po celém světě.

1 Teoretická část práce

1.1 IEEE 802.11 a Wi-Fi

IEEE 802.11 je standard, bez kterého si dnešní svět představíme už jen velmi těžko. Původně byl publikován v roce 1997 organizací IEEE (Institute of Electrical and Electronics Engineers) jako řešení problematiky fyzické vrstvy a podvrstvy řízení přístupu k médiím (MAC, Medium Access Control) vrstvy linkové OSI modelu pro právě vznikající bezdrátové sítě [1]. Standard je organizací IEEE dále spravován. Do dnešního dne byl rozšířen o mnoho dalších dodatků, které řeší například různé technologické problémy, či přímo přidávají další funkcionalitu, potřebnou pro budoucí aplikace.

Na IEEE 802.11 a jeho dodatcích je založena technologie Wi-Fi. Jak již bylo naznačeno, je to technologie bezdrátová a jako fyzické médium pro přenos dat používá rádiové vlny. Přímo pojem Wi-Fi vznikl v roce 1999 organizací, tehdy známou jako Wireless Ethernet Compatibility Alliance, jako ochranná známka pro tzv. Wi-Fi certifikované produkty, které úspěšně projdou certifikačním procesem[1]. Organizace byla přejmenována v roce 2004 na Wi-Fi Alliance a pod tímto názvem dodnes funguje [2]. Jejím cílem je zajištění kompatibility mezi zařízeními různých výrobců, docílenou právě pomocí certifikací a přiblížení těchto technologií veřejnosti. Na základě těchto myšlenek jsou například vytvářena generační označení Wi-Fi kompatibilních zařízení, místo uvádění přímo podporovaných standardů (Wi-Fi 4 podporuje standard 802.11n, Wi-Fi 5 podporuje 802.11ac atd.) [2].

Standard IEEE 802.11 a technologie Wi-Fi měly od jejich vzniku ohromný dopad na budoucí technologický vývoj a na používání počítačových sítí v komerčním i soukromém sektoru. Na světě je momentálně více než devět miliard Wi-Fi certifikovaných zařízení a více než polovina veškerého internetového provozu je zprostředkována Wi-Fi sítěmi[2]. Dá se tedy bezpochyby říci, že tyto technologie stále více ovlivňují náš každodenní život a vše naznačuje tomu, že tento trend bude přinejmenším v blízké budoucnosti stále narůstat.

1.2 Doplňky 802.11

1.2.1 802.11-1997

Původní verze standardu, také často nazývána jako 802.11 legacy, se v praxi už téměř nevyužívá a byla velmi rychle nahrazena novějšími verzemi, historicky však pomohla nastartovat budoucí masový nárůst bezdrátových zařízení a zavedla principy, které jsou dodnes používány.

802.11 legacy nabízí rychlosti 1 Mb/s a 2 Mb/s a představuje tři různé technologické možnosti, jak data na fyzické vrstvě přenášet [1]. První z nich je posílat data pomocí infračerveného záření. Tato možnost stále zůstává součástí standardu, ačkoliv nemá žádnou konkrétní implementaci. Další možností je přenášet data pomocí radiových vln v pásmu 2,4 GHz, za použití buď metody frekvenčních skoků (FHSS), nebo metodou přímého rozprostření spektra (DSSS).

Kromě metod fyzických vrstev řeší 802.11 legacy také problematiku přístupu k médiu. Používá k tomu metodu vícenásobného přístupu k médiu, s vyhýbáním kolizí (CSMA/CA)[1]. Tato metoda byla použita právě z důvodu nemožnosti kolize detekovat. Zařízení tedy čekají náhodný časový interval před, odesláním každého rámce, na rozdíl např. od metody vícenásobného přístupu k médiu s detekcí kolizí (CSMA/CD), kdy zařízení čeká až v případě kolize.

1.2.2 802.11a/b/g

Jako vůbec první byl představen v roce 1999 doplněk s označením 802.11a [1]. Na rozdíl od 802.11 legacy pracuje v pásmu 5 GHz, což přináší určité výhody i nevýhody. Jedním z přínosů je například menší pravděpodobnost rušení jinými zařízeními. Ve 2,4GHz pásmu totiž operuje velké množství jiných služeb, mimo jiné například bluetooth, bezdrátové telefony nebo třeba i mikrovlnné trouby. Kromě toho nabízí 5GHz pásmo dvanáct různých nepřekrývajících se kanálů, na kterých může zařízení operovat. Ve 2,4GHz pásmu jsou oproti tomu nepřekrývající se kanály pouze tři. Za nevýhodu lze poté považovat nižší dosah, jelikož vyšší frekvence hůře proniknou fyzickými objekty. Hlavní nevýhodou je však nemožnost komunikovat se zařízeními v 2,4GHz pásmu a tudíž nekompatibilita se staršími zařízeními.

Velký posun přinesl tento doplněk také v maximální přenosové rychlosti, která zde dosahuje až 54 Mb/s [3]. Toho bylo možno docílit zejména díky použití modulace OFDM (Ortogonální multiplex s frekvenčním dělením).

Zároveň s rozšířením 802.11a byl také představen doplněk 802.11b a naopak od předchozího byl koncipován spíše jako pokračování předchozí technologie, než jako představení nových možností. Pracuje ve 2,4GHz, čímž zajišťuje pro 802.11a chybějící interoperabilitu se staršími zařízeními.

IEEE 802.11b dosahuje rychlostí až 11 Mb/s [3]. Každý kanál zde vyžaduje stejnou šířku pásma jako za použití 802.11 legacy s modulací DSSS. Vyšší rychlosti je pak dosaženo díky implementaci nového modulačního schématu nazvaného Doplňkové klíčování kódu (v angličtině známé pod názvem Complementary Code Keying, zkráceně CCK)[3].

Z výše uvedených důvodů zařízení implementující 802.11a našla využití spíše v korporátním a podobném prostředí, kde nebyla překážkou vyšší cena a dominantním standardem běžných komerčních produktů se stalo využití 802.11b.

K celé této problematice přistupuje poté další doplněk, označený, jako 802.11g. Ačkoliv byl ratifikován v červnu roku 2003, v komerční sféře se objevuje už o něco dříve. Přináší možnost použití stejné modulační techniky jako 802.11a, tedy OFDM ve 2,4GHz pásmu, čímž je tato technologie schopna dosáhnout přenosové rychlosti do 54 Mb/s [3]. Kromě modulace OFDM používá 802.11g i modulaci DSSS, čímž zajišťuje možnost připojení starších zařízení, používajících 802.11b. Doplňek tedy přináší stejné přenosové rychlosti jako 802.11a a zároveň řeší problém interoperability který, zde stále přetrvával. Tou větší nevýhodou tu stále zůstává hlavně možnost rušení v relativně přeplněném 2,4GHz pásmu.

1.2.3 802.11n

Další velkou změnou byl v roce 2009 publikován standard 802.11n. Je schopen pracovat jak v 2,4GHz, tak i v 5GHz pásmu a jako vůbec první bezdrátový standard byl schopen konkurovat technologii Fast Ethernet (802.3u). Maximální rychlost, které tento doplňek dosahuje je totiž 600 Mb/s [3].

Významným přínosem této technologie je možnost využití více antén pro přenos dat současně, neboli metoda známá jako MIMO (multiple-input multiple-output). Tento koncept umožňuje použití až čtyř antén, které pak vytváří více datových toků souběžně ve stejném pásmu, použitím prostorového multiplexování [4].

Velkou a také částečně kontroverzní inovací se stala eventualita vyšší šířky pásma. Konkrétně se tu vyskytuje možnost rozšířit šířku pásma z 20 MHz na 40 MHz. Tato funkce je sice schopna zdvojnásobit rychlost přenosu dat na fyzické úrovni, ale ve 2,4GHz pásmu způsobí ještě daleko větší problémy s interferencí, než se tu již vyskytují. Tato funkcionalita je proto omezena zejména na použití v 5GHz pásmu a v 2,4GHz pásmu by se měla používat až s jistotou, že nebude ovlivňovat jiné bezdrátové zařízení, využívající například technologie jako Bluetooth nebo Zigbee.

1.2.4 802.11ac

Postupným rozšiřováním technologických možností, zvyšováním rychlostí a obrovským uplatněním na trhu, se WiFi sítě přežily, jako pouhý nástroj pro základní

konektivitu k místní síti a k internetu. Zejména díky přínosům 802.11n se začaly na bezdrátové sítě klást vyšší nároky. Dalším zvyšováním rychlostí se nejen zlepší komfort koncových uživatelů, ale některé služby jako například streaming multimédií, pro své kvalitní fungování přímo vyžadují větší kapacity. Mimo jiné byl proto v roce 2013 publikován standard 802.11ac.

IEE 802.11ac navazuje hodně na 802.11n a snaží se zejména rozšířit kapacity pro možnost vyšších přenosových rychlostí. Jeden ze způsobů jak toho dociluje je třeba další rozšíření šířky pásma. Kromě 20 MHz a 40 MHz nyní je nyní přidána možnost využít i šířku pásma 80 MHz a 160 MHz [5]. Z tohoto důvodu také operuje 802.11ac pouze v 5GHz pásmu.

Standard také rozšiřuje možnosti technologie MIMO. Kromě navýšení současných přenosů ze 4 na 8, se také připojuje možnost vysílat tyto proudy na více koncových zařízení najednou (tzn. Multiple Users MIMO)[5].

1.3 Pokročilý roaming

Jak už bylo naznačeno, s postupným zlepšováním a evolucí bezdrátových sítí, se zároveň začaly zvyšovat nároky na tyto sítě. Jedním z těchto faktorů se postupem času stala mobilita. Automatizovaný přechod z jednoho přístupového na druhý, s lepší sílou signálu, je při pohybu uživatele často kruciální, pro udržení dobré kvality služeb.

Velkým technickým problémem se u tohoto tématu časem ukázalo zpoždění vznikající právě změnou stávajícího přístupového bodu a asociací k novému. Různé služby jsou pak na toto zpoždění velmi citlivé a někdy může dojít i ke kompletnímu výpadku spojení. Typicky je to služba typu VoIP (Voice over Internet Protocolo), kde je jako maximální možné zpoždění uváděno 150 ms [6]. Zde se ale bere v potaz i možné zpoždění, způsobené průchodem přes internet. V lokálních sítích je proto uváděno maximální možné zpoždění většinou kolem 50 ms [6]. Mimoto způsobuje VoIP službám také velký problém kolísání zpoždění na síti, neboli tzn. jitter. Ten je rovněž nežádoucím vlivem procesu asociace klientského zařízení k jinému přístupovému bodu. Z těchto důvodů je nutné snažit se tyto faktory omezit, jak je to jen možné.

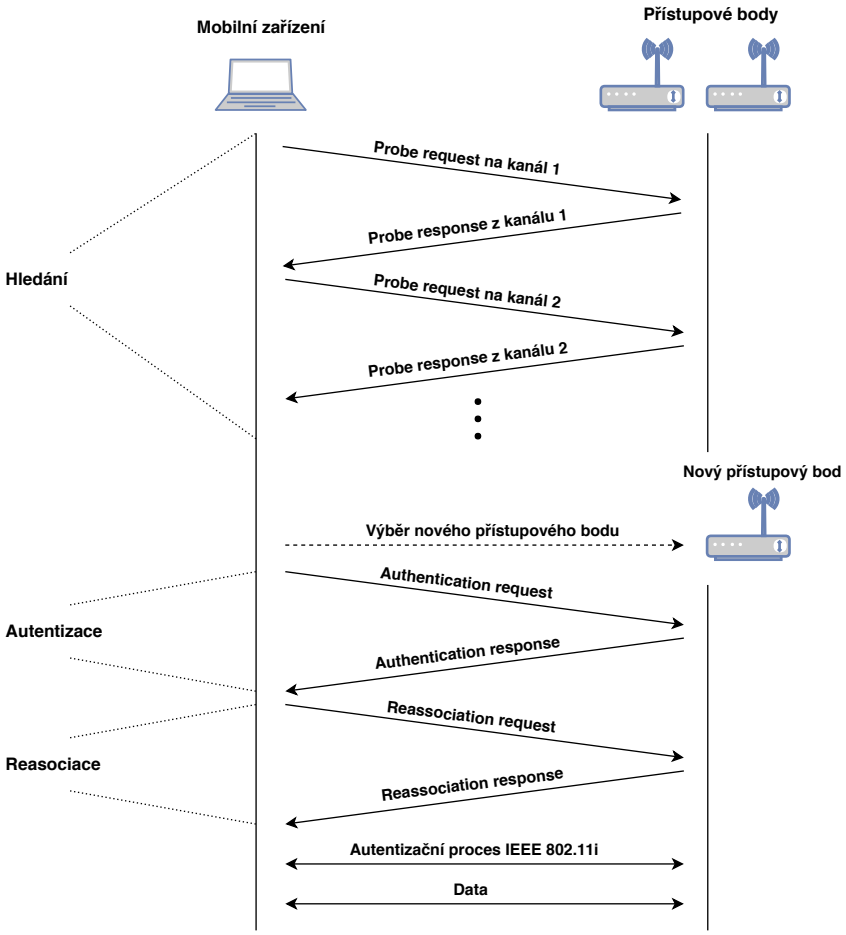
Funkcionalita změny přístupového bodu byla už v 802.11 sítích zavedena. V původních typických scénářích stačilo pro připojení k novému přístupovému bodu vyměnit pouze 4 zprávy [7]. S budoucím rozšiřováním tohoto standardu však počet řídících zpráv drasticky narostl. Jednou z částí tohoto procesu se stala např. tzv. EAP (Extensible Authentication Protocol) reautentizace, tedy při každé změně přístupového bodu musí klientské zařízení znovu projít krokem autentizace. Na takto

vzniklé problémy se zaměřuje doplněk označený 802.11r, který se snaží snížit počet řídících zpráv a zjednodušit proces reautentizace.

1.3.1 Handoff proces

V situaci, kdy se mobilní klientské zařízení příliš vzdálí od přístupového bodu, ke kterému je aktuálně připojené, musí se připojit na přístupový bod s lepším signálem, jinak hrozí riziko výpadku konektivity. Proces který se v takovéto situaci spustí se nazývá Handoff. Jedná se v podstatě o sérii zpráv, které si mezi sebou vymění klientské zařízení, původní přístupový bod a nový přístupový bod. Během tohoto procesu není klientské zařízení schopné datové komunikace. Výsledkem úspěšného zakončení všech potřebných kroků, je navázání spojení a asociace s novým přístupovým bodem a pokračování datových toků.

Handoff proces můžeme rozdělit celkově na čtyři fáze: detekce, hledání, autentizace a reasociace [8][9]. Jednoduchý příklad tohoto procesu je zobrazen na obrázku 1.1



Obr. 1.1: Handoff proces

První z těchto kroků, tedy detekce, je fáze, kdy koncové zařízení determinuje potřebu změnit svůj aktuální přístupový bod. Dle jakých podmínek se klient rozhoduje, záleží přímo na konkrétním zařízení a implementaci výrobce [2]. Může se jednat o jednoduché porovnání signálu aktuálního přístupového bodu s předem definovanou hodnotou, ale někteří výrobci implementují i řešení hodnotící poměr signálu k šumu nebo třeba i ztrátovost paketů. Krom těchto faktorů taky často zařízení bere v potaz, zda se v dosahu nachází jiný přístupový bod s lepším signálem.

Jako další krok po rozhodnutí ke změně aktuálního přístupového bodu, nastává fáze hledání. Tento proces může mít dvě podoby a to jako tzv. pasivní skenování nebo aktivní skenování. V případě pasivního skenování klientské zařízení naslouchá a čeká na zachycení beacon rámce. Ten je periodicky rozesílán přístupovými body, obvykle s prodlevou kolem 100 ms [9]. Jednou z nevýhod tohoto postupu je delší doba hledání, oproti použití aktivního skenování. Další je možnost nezachytit některé beacon rámce. Zařízení totiž musí postupně naslouchat na všech kanálech a v případě, kdy nenaslouchá dostatečně dlouhou dobu, může beacon rámec minout [2].

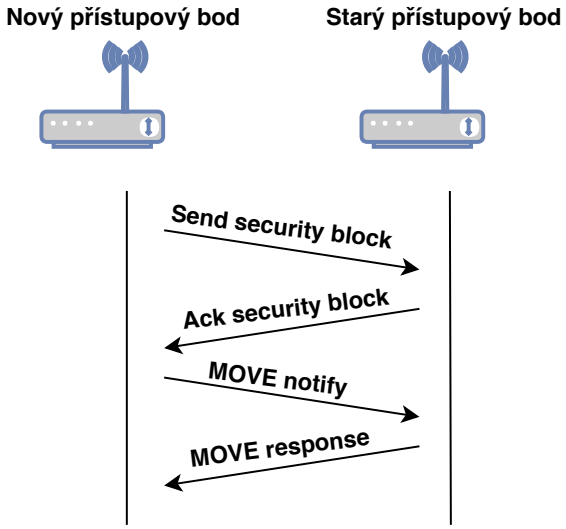
Při použití aktivního skenování koncové zařízení zjišťuje, zda se na daném kanálu nachází nějaký přístupový bod. Toho docílí odesláním probe request rámce a následným naslouchánímpředem daného času. Pokud tento rámec nějaký přístupový bod zachytí, odešle zpět zprávu ve formě probe response rámce. Čas, po který trvá proces aktivního skenování závisí na počtu kanálů, které klient skenuje. Můžou to být všechny používané kanály, v takovém případě se jedná o tzv. full-scan, ale mohou to být i jen předem vybrané určité kanály, tvz. short-scan [9].

Po vyhledání všech potenciálně budoucích přístupových bodů, si klientské zařízení vybere, ke kterému se připojí, na základě nejlepšího signálu. Samozřejmostí je předpoklad, že signál tohoto přístupového bodu by měl být vyšší, než signál stávajícího, aby nedocházelo ke zbytečnému přepojování.

Když si klientské zařízení vybere nový přístupový bod, nastane fáze autentizace. Ta je nutnou podmínkou následné asociace. Ačkoliv tuto fázi upravuje pro větší bezpečnost standard IEEE 802.11i, na obrázku 1.1 je pro názornost předvedena jednoduchá výměna za použití autentizačního procesu známého jako open authentication.

Finálním krokem, tedy reasociace, rozumíme přenesení asociace koncového zařízení z jednoho přístupového bodu na druhý. Klientské zařízení nejdříve odešle novému přístupovému bodu zprávu reasociation request, obsahující mimo jiné informace o své MAC adrese, MAC adrese stávajícího přístupového bodu a identifikátor ESS (Extended Service Set). Po této zprávě si stávající a budoucí přístupový bod vymění bezpečnostní informace roamujícího klientského zařízení, například pomocí protokolu IAPP (Internet Access Point Protocol) známého také jako IEE 802.11f. Jednoduchá reprezentace tohoto procesu je vidět na obrázku 1.2. Po přeposlání

security bloku je potřeba, aby starý přístupový blok přeposlal všechny potřebné informace o pobíhajících spojeních klientského zařízení. Nový přístupový bod proto odešle stávajícímu přístupovému bodu žádost známou jako MOVE notify, na kterou stávající přístupový bod odpoví zprávou MOVE response. Tato komunikace je samozřejmě z bezpečnostních důvodů zašifrovaná. Po těchto krocích odešle nový přístupový bod klientskému zařízení zprávu reasociation response, čímž je proces handoff ukončen.



Obr. 1.2: IAPP

Aby se zabránilo různým bezpečnostním rizikům, bylo ve standardu IEEE 802.11i implementováno použití mechanismů standardu 802.1X [8]. Využívá se tu principu, při kterém se mezi klientským zařízením a autentizačním serverem vygeneruje klíč, nazývaný Pairwise Master Key (PMK). Tento klíč by měl vydržet během celé komunikace a měl by být na síti vystavován co možná nejméně. Aby si mohly přístupový bod i klientské zařízení ověřit, že tento klíč znají a nemusely ho přitom dále vystavovat na síti, byl implementován tzv. four-way handshake, během kterého je z PMK dále odvozen klíč s názvem Pairwise Transient Key (PTK). Four-way handshake sestává celkově ze čtyř zpráv, které jsou odesílány použitím protokolu EAPOL (Extensible Authentication Protocol Over LAN).

1.3.2 802.11r

Každá z fází handoff procesu způsobuje zpoždění a zvyšuje prodlevu, během které klientské zařízení nemůže komunikovat. Na některé z těchto procesů se zaměřuje standard IEEE 802.11r, někdy nazýván Fast BSS transition nebo také Fast roaming. Představuje tři různé způsoby, jak docílit nižší prodlevy a to: integrace four-way handshake zpráv do fází autentizace a asociace, před-rezervací QoS (Quality

of Service) zdrojů a efektivní distribuce bezpečnostních klíčů. IEEE 802.11r také přidává nové pole do určitých zpráv, nutné pro správnou funkci protokolu. Jedním z nich je například Mobility Domain Information Element (MDIE), které dodává informace o mobilní doméně, ve které se nachází daný přístupový bod. Dalším je Fast Transition Information Element (FTIE), který se stará o bezpečnostní politiku a rezervací zdrojů [8].

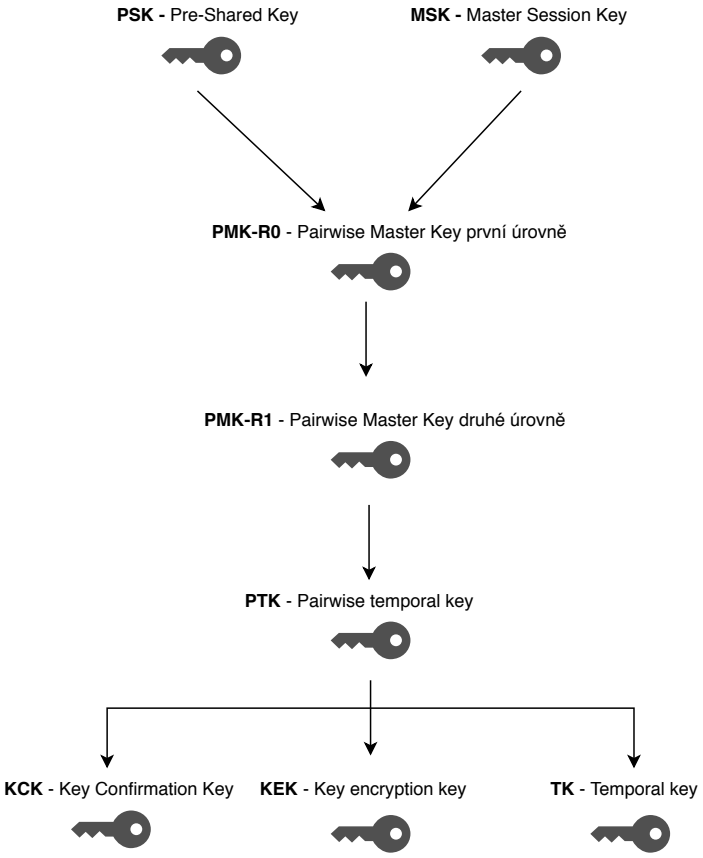
Jak bylo řečeno výše, první ze způsobů jak 802.11r zjednodušuje handoff proces, je integrace různých informací do již existující komunikace. Největších výsledků v tomto ohledu pravděpodobně dosahuje obsažení čtyř EAPOL zpráv, ze kterých se skládá four-way handshake do autentizačních a asociačních žádostí a odpovědí, přidáním polí, které nesou bezpečnostní informace. Stejně tak jsou například pole MDIE a FTIE integrovány do beacon rámců, probe rámců, asociačních žádostí a asociačních odpovědí, místo vytváření nových rámců obsahující tyto informace. Tato metoda se ukázala jako velmi efektivní ve snižování prodlevy u handoff procesu, jelikož snižuje celkový počet zpráv, které si mezi sebou musí přístupový bod a klientské zařízení vyměnit a odpovídá tak na jeden z největších problémů zpoždění vznikajícího při roamingu [8].

Druhý problém, na který se 802.11r zaměřuje, je vstupní kontrola QoS, tedy kontrola zda má daný přístupový bod dostatek zdrojů k zajištění uspokojivé kvality služeb. Tento problém se tu řeší tzv. před-rezervací. Jedná se o princip, díky kterému může klientské zařízení provést vstupní kontrolu QoS s novým přístupovým bodem ještě před autentizací nebo asociací. U tohoto principu lze použít dva způsoby. Prvním z nich je komunikace přes tzv. distribuční servis (Over the Distribution Service, OTD). V tomto případě komunikuje klientské zařízení s budoucím přístupovým bodem prostřednictvím aktuálně připojeného přístupového bodu, využitím infrastruktury, kterou jsou mezi sebou přístupové body propojeny. Toto řešení, je z pohledu omezení prodlevy preferované, jelikož díky použití distribučního servisu nebude narušen stávající provoz klientského zařízení. Druhým způsobem je komunikace bezdrátová (Over the Air, OTA), kdy zařízení komunikuje přímo z budoucím přístupovým bodem.

Největším problémem celého roamingového procesu se časem staly režijní náklady spojené se zvyšujícím se zabezpečováním bezdrátových sítí. Krom zrychlení procesu autentizace se 802.11r zabývá také distribucí bezpečnostních klíčů v dané mobilní doméně. S použitím 802.11r stačí, aby se klientské zařízení asociovalo s jedním přístupovým bodem a PMK klíč může být dále distribuován po všech přístupových bodech, které se nacházejí ve stejné mobilní doméně. Když se poté klientské zařízení pokusí o připojení k jinému přístupovému bodu v této doméně, klíč je tu jíž přítomný. Tím se zbavíme nutnosti komunikace s autentizačním serverem, čímž se výrazně sníží zpoždění spojené s reautentizací [8].

1.3.3 Hierarchie klíčů v 802.11r

Na obrázku 1.3 je zobrazeno, jak řeší hierarchii klíčů standard 802.11r. Model sestává ze dvou úrovní držitelů klíčů. Držitel klíče R0 odvodí Pairwise Master Key první úrovně (PMK-R0) z tzv. Pre-shared klíče (PSK) a tzv. Master Session klíče (MSK), když se klientské zařízení poprvé připojí na některý z přístupových bodů dané mobilní domény a projde plným procesem autentizace. Na jednu mobilní doménu připadá jeden držitel klíče první úrovně a jeden PMK-R0 pro každé klientské zařízení [8]. Klíč druhé úrovně (PMK-R1) je pak odvozen pro asociaci klientského zařízení s novým přístupovým bodem. Zde připadá jeden PMK-R1 na každý různý pár klientského zařízení a přístupového bodu. Držitelem klíče může být přímo jeden z přístupových bodů, ale může to být separátní zařízení. Přístupové body v sobě také uchovávají tzv. Pairwise Transient Key (PTK). Ten se skládá celkově ze tří dalších klíčů, které se používají pro další šifrování provozu.



Obr. 1.3: Hierarchie klíčů v 802.11r

1.3.4 802.11k

V roce 2008 byl představen doplněk IEEE 802.11k nazvaný také jako Radio Resource Measurement (RRM) enhancements, neboli zdokonalení měření rádiových zdrojů[10]. Tento doplněk definuje nové mechanismy a způsoby měření, které výrazně přispívají informovanosti účastníků bezdrátové komunikace o svém okolí. Zařízení implementující 802.11k si vedou databázi s informacemi o ostatních známých okolních účastnících bezdrátové komunikace, jak o přístupových bodech, tak i klientských zařízeních. Tyto informace jsou pak schopny na základě žádostí schopny poskytovat pomocí standardního Management Information Database (MIB) rozhraní[10]. Mimo jiné jsou takto typicky poskytovány statistiky klienta o používané lince, jako počet přijatých a odeslaných paketů nebo rychlost přenosu dat, a informace o rádiovém kanálu, jako informace o šumu či vytíženosti tohoto kanálu.

Pro účely poskytování těchto informací definuje 802.11k několik zpráv, odesílaných většinou na bázi žádost/odpověď. Jsou to zprávy[11]:

- Beacon Request/Report
- Frame Request/Report
- Channel Load Request/Report
- Noise Histogram Request/Report
- Station Statistics Request/Report
- Location Configuration Information (LCI) Request/Report
- Transmit Stream/Category Measurement Request/Report
- Link Measurement Request/Report
- Neighbor Report Request/Report
- Measurement Pause Request
- Measurement Pilot Report

Pokud dotazované zařízení disponuje požadovanými informacemi, je po přijetí příslušné žádosti ihned odeslána odpověď. V opačném případě započne přijatá žádost měřící interval, po jehož konci je teprve odeslána odpověď obsahující příslušné informace. Speciálním případem je zpráva Measurement Pause, která nedefinuje žádost a odpověď, nýbrž pouze informuje o začátku a konci měřícího intervalu, ve kterém zařízení neodpovídá na případné další žádosti[10]. Další vyjímkou je zpráva Measurement Pilot, kterou periodicky rozesílají přístupové body. Tato zpráva obsahuje část informací, obsažených v běžném beacon rámci a rozesílá se častěji než beacon rámce, za účelem asistování ostatním účastníkům komunikace se skenováním[10].

Pro výměnu těchto zpráv jsou definovány dva typy rámců. Zprávy Link Measurement a Neighbor Report jsou definovány jako samostatné action rámce, protože nepožadují započetí samotného měření, ale pouze požadují informace, které má dotazované zařízení již k dispozici[10]. Všechny ostatní zprávy jsou odesílány

jako MeasurementRequest a Measurement Response rámce, přičemž Measurement request rámce obsahují pole Type, které rozlišuje, o jaký typ žádosti se jedná.

Zprávy beacon request používají koncové zařízení pro požadování seznamu přístupových bodů, dostupných na předem specifikovaných kanálech od jiného koncového zařízení. Tyto informace lze zjišťovat třemi možnými způsoby, tedy v pasivním módu, v aktivním módu nebo v módu beacon tabulky[11]. V pasivním módu (pasivní skenování) zařízení spustí měřící interval, ve kterém sleduje požadované kanály a zaznamenává beacon, probe response a measurement pilot rámce u kterých zároveň měří výkonové úrovně (RCPI, Received Channel Power Indicator). Při použití aktivního módu (aktivní skenování) probíhá proces téměř identicky, jen na počátku měřícího intervalu odešle měřící zařízení na požadovaném kanálu probe request rámec. V módu beacon tabulky dotazované zařízení žádné měření neprovádí, ale pouze odešle veškeré relevantní uložené informace[11].

Na frame request odpovídá dotazované zařízení informacemi o provozu na daném kanálu. Poskytovány jsou statistiky o všech přijatých rámcích, průměrných výkonových úrovní (RCPI) a BSSID všech známých unikátních adres[11].

Channel load report vrací vytíženost daného kanálu z pohledu dotazovaného zařízení[11].

Noise histogram poskytuje výkonový histogram šumu, způsobeného jinými zdroji než, 802.11 zařízeními[11]. Dotazované zařízení tento šum měří vzorkováním kanálu, když na sledovaném kanálu neprobíhá žádný provoz a měřící zařízení nevysílá ani nepřijímá žádný provoz.

Station statistics report obsahuje hodnoty a statistiky přímo spojené s komunikací dotazovaného zařízení. Rozdělují se na dvě skupiny. První z nich, STA counters, obsahuje různé statistiky o úspěšnosti odesílaných a přijímaných rámců mimo jiné například počet úspěšně a neúspěšně odeslaných multicast rámců nebo celkový počet zaznamenaných FCS (Frame Check Sequence) chyb. Druhá skupina se nazývá BSS avarage access delay a obsahuje hodnoty průměrných zpoždění při komunikaci s asociovaným přístupovým bodem, počet asociovaných koncových zařízení k tomuto přístupovému bodu a vytíženost příslušného kannálu[11].

LCI request může být dotaz na lokaci tázajícího (tzv. dotaz Where am I?) i dotazovaného (dotaz Where are you?) zařízení[11]. Jedná se o lokaci v rámci souřadnic délky, šířky a výšky s tím, že hodnota výšky je typicky definovaná jako patro umístění zařízení.

Transmit stream/category measurement umožňuje dvěma QoS zařízením výměnu informací o stavu probíhajícího komunikačního proudu mezi nimi. Report zde obsahuje výkonové metriky měřeného komunikačního proudu ze strany odesílatele[11].

Link measurement poskytuje aktuální informace o radiofrekvenčních charakteristikách na lince dvou konvích zařízení, což indikuje kvalitu této linky[11].

Neigbor report je pro roaming z těchto zpráv asi nejdůležitější. Request odesílá koncové zařízení přístupovému bodu, který poté odešla jako odpověď informace o známých sousedních přístupových bodech, které si udržuje v tabulce dot11RRMNeighborReportTable v MIB[11]. Tyto informace poté koncové zařízení může použít pro informovanější rozhodování při výběru nového přístupového bodu při roamingu.

Díky mechanismům 802.11k jsou nyní přístupové body i koncové zařízení daleko informovanější o svém okolí. Bez použití těchto možností jsou zařízení odkázaná pouze na svou přímou komunikaci a mají povědomí jen o svém nejbližším okolí. V moderním prostředí se ale bude bezdrátová síť častěji skládat z více různých přístupových bodů, ke kterým bude asociováno více zařízení. Díky možnosti vyměňovat si mezi informace a statistiky, jsou zařízení schopná mít daleko komplexnější přehled o prostředí, ve kterém se nachází a učinit tak lepší rozhodování při roamingu.

Je zde několik informací, které lze vzít v úvahu, když se koncové zařízení rozhoduje k jakému přístupovému bodu se asociuje. Lze například použít Neighbor report, který obsahuje informace o aktuálním vytížení jednotlivých přístupových bodů[10]. Koncové zařízení se tak může rozhodnout, jestli přístupový bod s lepším signálem, ale větším zatížením může být stále schopen poskytnout požadovanou kvalitu připojení nebo jestli je lepší zůstat připojen na stejném místě.

Další z pomocných informací je, na kterých kanálech se nachází uvažované přístupové body. Díky této informaci nemusí koncové zařízení skenovat zbytečně všechny kanály, čímž se sníží doba skenování.

Jedna z možností, které lze také využít, je Location Configuration Information. Na základě informací o lokaci jednotlivých zařízení a síly signálů těchto zařízení, je teoreticky možné předpokládat směr pohybu koncového zařízení a vzít tyto informace v úvahu při roamingu[10].

Tyto mechanismy mohou mít velký dopad na kvalitu rozhodování při roamingu a teoreticky i na celkovou výkonnost bezdrátové sítě, nicméně nutno zmínit, že implementace těchto mechanik a zejména rozhodovacích procesů využitých při roamingu je plně v gesci výrobce zařízení.

1.3.5 802.11v

Podobně jako IEEE 802.11k nabízí doplněk IEEE 802.11v také známý jako Wireless Network Management (WNM), prostředky pro výměnu informací mezi koncovými zařízeními, pro zlepšení celkového výkonu bezdrátových sítí. Zařízení pak mají lepší přehled o celkové topologii a momentálním stavu sítě. Dále 802.11v umožňuje výměnu informací o lokaci, podporuje možnosti více přístupových bodů v jedné síti, efektivní doručování skupinových rámců a umožňuje tzv. WNM-Sleep mode, díky kterému může být koncové zařízení déle nečinné, bez přijímání dalších rámců od přístupového bodu. Seznam funkcionalit, které 802.11 přináší je[12]:

- BSS Max idle period management
- BSS transition management
- Channel usage
- Collocated interference reporting
- Diagnostic reporting
- Directed multicast service (DMS)
- Event reporting
- Flexible multicast service (FMS)
- Location services
- Multicast diagnostic reporting
- Multiple BSSID capability
- Proxy ARP
- QoS traffic capability
- SSID list
- Triggered STA statistics
- TIM broadcast
- Timing measurement
- Traffic filtering service
- U-APSD Coexistence
- WNM-Notification
- WNM-Sleep mode

První z těchto funkcí, tedy BSS Max idle period management přináší možnost definovat dobu, ve které přístupový bod neodpojí asociované zařízení z důvodu nepřijetí žádné komunikace, což napomáhá řízení zdrojů přístupového bodu a šetření energie klientského zařízení, které nemusí tak často odesílat tzv. keep-alive rámce[12].

BSS transition management je funkce, díky které může příliš zatížený přístupový bod odeslat žádost koncovému zařízení o reasociaci k jinému specifikovanému přístupovému bodu, či alespoň seznam preferovaných přístupových bodů k reasociaci.

Channel usage jednoduše poskytuje informace o zatížení jednotlivých kanálů.

Tyto informace odesílá přístupový bod koncovým zařízením a můžou být použity například jako doporučení při sestavování komunikace mimo danou síť[12].

Při použití Collocated interference reporting se dotazuje koncové zařízení jiného koncového zařízení na rušení způsobené překrýváním přenosových pásem[12]. Tyto informace pak lze použít pro načasování přenosu k minimalizaci tohoto rušení.

Diagnostic reporting obsahuje informace o hardwaru, konfiguraci a možnostech koncového zařízení. Tyto informace mohou být na žádost odeslány jinému koncovému zařízení a dále použity pro diagnostiku problémů, které mohou v síti nastat[12].

DMS používá koncové zařízení, když potřebuje vyžádat od přístupového bodu odeslání skupinově adresovaného rámce, jako rámec individuálně adresovaný[12].

Event reporting se používá k předávání informací v reálném čase na základě předem daných událostí. První z nich je tzv. transition event, dojde k němu po úspěšně proběhlém roamingu a používá se k diagnostice problémům, které mohou při roamingu nastat. Další událostí je tzv. RSNA (Robust Security Network Associations) event, který popisuje použitý způsob autentizace a používá se pro diagnostiku problémů spjatých s bezpečností a autentizací. Třetí událost je WNM Log event a umožňuje na žádost odeslat WNM Log, do kterého si zařízení ukládá informace spjaté s používáním 802.11v funkcionalit. Poslední událostí je Peer-to-Peer link event, která se vyvolá ustanovením nové Peer-to-Peer linky, což je použito pro monitorování Peer-to-Peer linek v síti[12].

FMS také napomáhá nižší spotřebě energie koncových zařízení. Koncové zařízení může totiž díky této službě požádat o jiný DTIM (Delivery traffic indication message) interval, tedy interval, ve kterém jsou pravidelně odesílány informační rámce na skupinové adresy[12]. To umožňuje nastavit si jednotný čas, ve který bude koncové zařízení tyto zprávy přijímat a nemusí se tzv. budit v při každé skupinově odeslané DTIM zprávě.

Location services funkce obsahuje rámce Location Configuration Request a Response, pro výměnu informací o prostorovém rozpoložení zařízení[12].

Multicast diagnostic reporting poskytuje statistiky o přijatých multicast rámcích přijatých od jednotlivých adres, což dále může požít přístupový bod pro diagnostiku multicastového provozu[12].

Multiple BSSID capabilty umožňuje v síti s více přístupovými body použít jen jeden beacon rámec eventuelně jen jeden probe response rámec pro všechny známé přístupové body[12]. Tato funkce může celkovému zatížení sítě velice uvolnit oproti odesílání těchto rámců každým jednotlivým přístupovým bodem, obzvláště v rozsáhlejších sítích s vyšším počtem přístupových bodů.

Proxy ARP pomáhá přístupovému bodu nadefinovat koncové zařízení, kterým nebudou odesílány ARP rámce, což opět napomáhá šetřit energii u koncových zařízení[12].

QoS traffic capability umožňuje zařízení oznámit svoji schopnost podpořit provoz definovaný s určitou prioritou[12].

O SSID list může požádat koncové zařízení jiného účastníka komunikace. Jedná se jednoduše o seznam známých SSID[12]. Účelem těchto informací je omezit počet probe request zpráv odesílaných při seknování.

TIM broadcast je periodicky odesílná zpráva, rozesílaná častěji než beacon rámce. Obsahuje informace o individuálně adresovaném provozu připraveným v bufferu přístupového bodu. Koncové zařízení tak může ve stand-by módu kontrolovat, zda bude přijímat nějakou komunikaci a nemusí se tzn. probouzet s každým beacon rámcem, což napomáhá šetřit energii.

Timing measurement poskytuje možnost srovnat případné nesrovnalosti nastaveného času mezi účastníkky komunikace. Je zde definován tzv. Timing Measurement action rámec, použitím kterého jsou zařízení schopná zjistit nesrovnalosti mezi nastaveným časem odesílatele a příjemce a případné výchylky kompenzovat[12].

Traffic filtering service je služba filtrování provozu. Koncové zařízení může přístupovému bodu dodat pravidla, podle kterých bude provoz filtrován. Přístupový bod poté bude kontrolovat jednotlivé rámce, směřované na toto konceové zařízení a pokud rámec neodpovídá žádným z definovaných pravidel, je tento rámec zahozen[12].

U-APSD je funkcionalita doplňku, IEEE 802.11e určená pro šetření energie koncových zařízení. U-APSD coexistence umožňuje koncovým zařízením nadefinovat přístupovému bodu pracovní interval ve kterém budou přijímat datovou komunikaci, což snižuje pravděpodobnost nepřijetí odeslaných rámců[12].

Pomocí WNM-Notification může zařízení upozornit jiné zařízení na řídící události, nicméně definovaná událost je zatím pouze jedna a to firmware update[12].

WNM-Sleep mode, neboli režim spánku, je definován pro koncová zařízení, která mohou odeslat zprávu přístupovému bodu, ve které specifikují dobu, po kterou se do tohoto režimu přepnou. Tato funkce výrazně napomáhá šetřit spotřebu energie, bez nutnosti odpojit se od přístupového bodu, když zařízení neplánuje odesílat ani přijímat žádná data[12].

Principy, které přináší 802.11v nejsou primárně určeny pro samotné snížení celkového času roamingu, ale přesto mohou být velmi účinné ve zlepšení celkového výkonu bezdrátové sítě. Stejně jako u 802.11k, jsou nyní účastníci komunikace schopní být informovanější o svém okolí a uplatnit tyto znalosti při další komunikaci v síti.

Jednou velkou výhodou je poskytnutí přístupový bodům mechaniky pro tzv. load-balancing. V moment, kdy už přístupový bod není dále schopný obsloužit všechny připojená koncové zařízení, může několika koncovým zařízením odeslat žádsoti o reasociaci k jinému přístupovému bodu a tím rovnoměrně rozložit možné prostředky bezdrátové sítě.

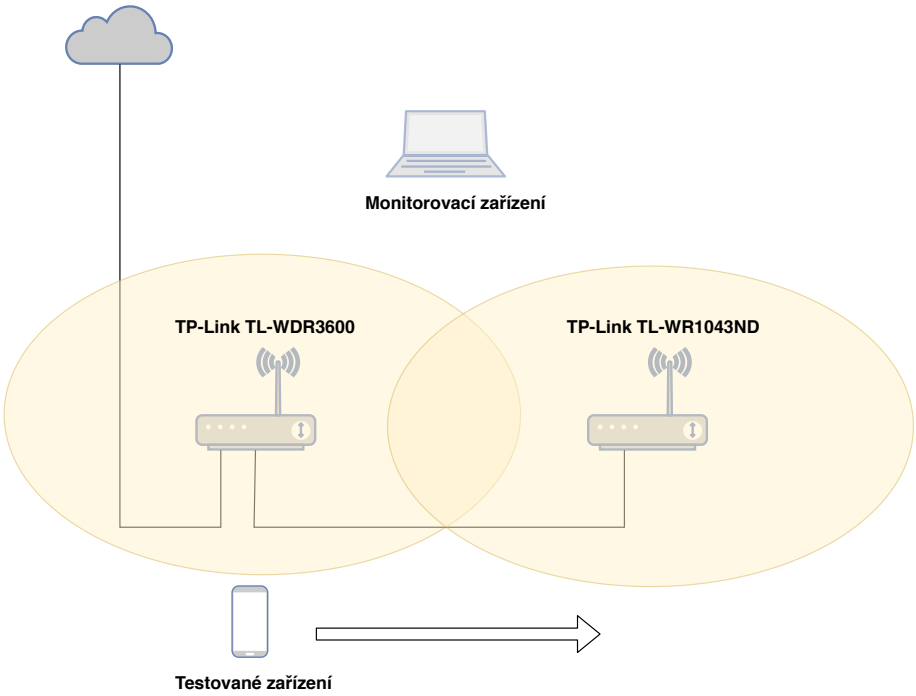
Dalším velkým přínosem jsou široké prostředky pro šetření spotřeby energie. Tyto mechanismy jsou zejména důležitá pro mobilní zařízení, jako chytré telefony a tablety, které jsou k bezdrátové síti připojeny takřka stále a spotřeba energie je u nich také zásadním parametrem.

2 Řešení práce

2.1 Testovací topologie

2.1.1 OpenWRT

Základem testovací topologie jsou dvě zařízení značky TP-link, konkrétně TP-link TL-WDR3600 verze 1.2 a TP-link TL-WR1043ND verze 1.6. Tato zařízení byla zvolena z důvodu dobré podpory systému OpenWrt. Schéma testovací topologie je zobrazeno na obrázku 2.1.



Obr. 2.1: Testovací topologie pro OpenWrt

Na obou zařízeních běží již zmíněný operační systém OpenWrt verze 18.06.1. Jedná se o open source linuxový operační systém, určený pro síťová zařízení[13]. Místo klasického statického firmwaru nabízí OpenWrt plně zapisovatelný souborový systém s možností rozšíření pomocí balíčků. Toto umožňuje vysokou míru přizpůsobení zařízení, jelikož zde člověk není odkázaný na operační systém, dodávaný výrobcem přímo se zakoupeným zařízením. O správu balíčku se na tomto systému stará systém opkg (open package management), ketrý je zde výhodný zejména z důvodu malého využití kapacity paměti, což by v opačném případě mohl být u síťových zařízení potenciální problém. OpenWrt používá pro ovládání z příkazové řádky Almquist shell. Konfigurace zařízení pak lze provádět přímo úpravou konfiguračních

souborů, ale systém také pro zjednodušení konfigurace poskytuje sadu skriptů, nazvaných UCI (unified configuration interface), díky kterým lze provádět konfiguraci použitím zjednodušených příkazů, podobně jako například u systémů jako Cisco IOS nebo RouterOS od společnosti Mikrotik. Systém lze také v omezené míře konfigurovat pomocí webového rozhraní, z nichž nejrozšířenější je pravděpodobně balíček LuCI, ale lze použít i jiné balíčky webového rozhraní.

Zařízení Tp-link TL-WDR3600 je nakonfigurováno, aby plnilo funkci hlavního směrovače a výchozí brány testovací sítě. Zařízení pracuje i jako DHCP server pro konfiguraci IP adres na koncových zařízeních. Jedním ethernetovým rozhraním je toto zařízení připojeno k internetu, z důvodu další konfigurace obou zařízení, stahování potřebných balíčků a podobně. Na druhém ethernetovém rozhraní je nastavena IP adresa, která slouží právě jako výchozí brána testované sítě. S tímto rozhraním jsou dále pomocí bridge propojena všechna ostatní nevyužitá ethernetová rozhraní spolu s rozhraním bezdrátové síťové karty. Před toto rozhraní je také k síti připojeno druhé zařízení TP-link TL-WR1043ND. To plní v síti pouze úlohu přístupového bodu a žádné další důležité služby zde nejsou spuštěny.

Obě zařízení jsou nastavena jako přístupové body testovací sítě a pracují v 2,4GHz pásmu. Pro správu bezdrátových služeb je zde použitý balíček wpad. Při běžné instalaci systému OpenWrt je většinou použitý balíček wpad-mini, nicméně ten neobsahuje veškeré funkce potřebné pro tuto testovací síť. Samotná konfigurace bezdrátové sítě zde byla provedena pomocí webového rozhraní LuCI. Jako ESSID sítě zde bylo zvoleno zvoleno OpenWrt_Roaming. Oba přístupové body operují na prvním kanálu, tedy na frekvenci 2412 MHz s šířkou pásma 20 MHz. Síť používá protokol 802.11n. Jako bezpečnostní protokol je zde použitý WPA2-PSK, tedy WPA2 s předsdíleným klíčem. Další nastavení se mění vždy podle charakteru měření, tedy měření bez použití 802.11r a s použitím 802.11r. Samotná konfigurace rychlého roamingu (Fast BSS Transition), je velmi jednoduchá. V aktuální verzi LuCI stačí pouze v záložce Wireless Security zaškrtnout možnost 802.11r Fast Transition a všechny ostatní pole lze nechat na původních hodnotách. Jediná další možnost, která se zde bude měnit, je pole FT protocol, ve kterém lze vybrat, zda bude použita metoda 802.11r OTA nebo OTD.

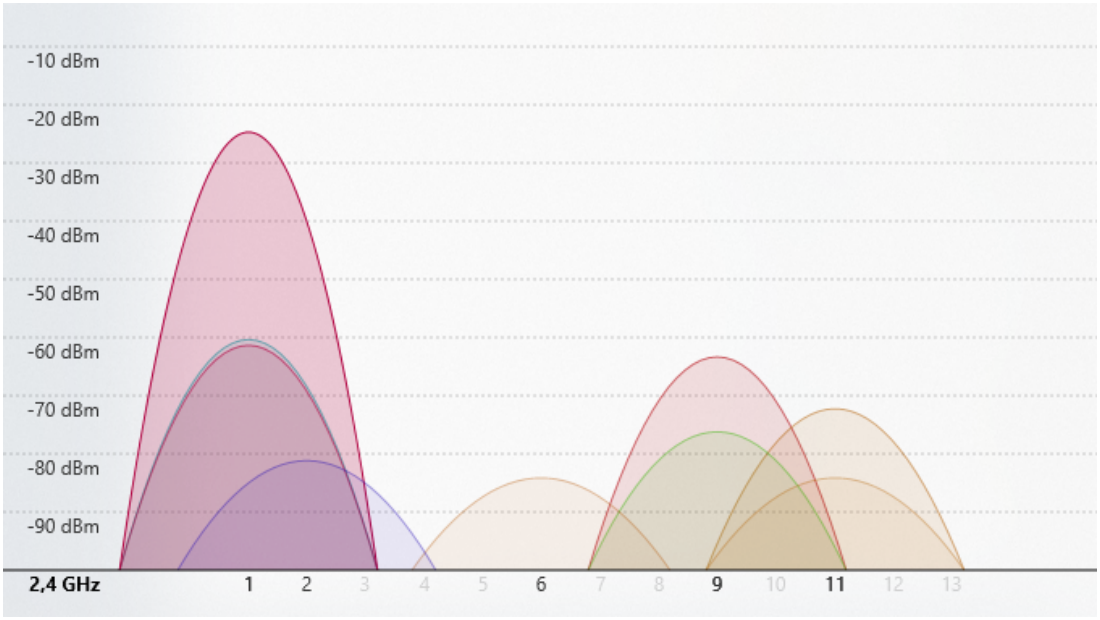
Pro sledování bezdrátového provozu je zde nutné použít nezávislé zařízení pro monitorování bezdrátového provozu. Jako toto monitorovací zařízení je zde použitý notebook s operačním systémem Kali Linux. Tento systém byl zvolen, protože už v základní konfiguraci nabízí spoustu nástrojů pro testování a diagnostiku sítě, používá se proto často například při penetračních testech různých zařízení, sítí a systémů. Pro samotný monitoring je použita USB bezdrátová síťová karta TP-link TL-WN722N, která umožňuje přepnutí do takzvaného monitorovacího módu. V monitorovacím módu je síťová karta schopná sledovat veškerý provoz na předem daném

kanálu. Při sledování bezdrátového provozu lze také využít možnsoti takzvaného channel-hoppingu, kdy je průběžně v časových intervalech sledován provoz na různých kanálech. Tato možnost není ale vhodná pro dlouhodobé sledování provozu určitých zařízení, místo toho se spíše používá pro zjištění, na kterém kanálu se nachází požadované zařízení. Z tohoto důvodu jsou zde oba přístupové body nastaveny na stejném kanálu. Takto lze efektivně sledovat a diagnostikovat komunikaci obou zařízení. Softwarově je poté pro zachytávání a vizualizaci provozu použitý program Wireshark, který také patří mezi základní programové vybavení systému Kali Linux.

Jako testované zařízení byly vybrány dva chytré telefony, Apple iPhone 8 s operačním systémem Apple iOS 12.2 a Samsung Galagy S9+ s operačním systémem android. Tato zařízení byla pro testovaní vybrána, protože implementace rychlého roamingu se chytrých telefonů dotýká pravděpodobně nejvíce. Obě tato zařízení mají také deklarovanou podporu standardů 802.11r, 802.11k i 802.11v[14][15]. Dle dokumentace obou výrobců obě dvě zařízení plně podporují možnost rychlého roamingu. Standardu 802.11k využívá Apple k vytvoření a udržování seznamu kanálů, na kterých se nachází přístupové body, ke kterým se může koncové zařízení potenciálně připojit. Samsung ze standardu 802.11k implementuje zprávy Beacon request/report a Neighbor request/report. Těchto zpráv pak využívá ke snížení času skenování a ke kvalitnějšímu vybírání přístupového bodu při roamingu. Ze standardu 802.11v implementují Apple i Samsung funkcionalitu BSS transition management, díky které mohou jejich koncová zařízení brát v úvahu zatížení jednotlivých přístupových bodů.

Podpora standardů podporujících roaming vždy závislá na několika faktorech. Operační systémy Windows podporují standardy 802.11r, 802.11k a 802.11v od systému Windows 10, nicméně podpora je vždy závislá na použité síťové kartě a ovladačích této karty[16]. Z velkých výrobců mají deklarovanou podporu těchto standardů na vybraných zařízení například síťové karty od firmy Intel[17]. U linuxových systémů záleží na použité distribuci, Ubuntu například mají deklarovanou podporu za předpokladu použití balíčku wpa-supplicant[18]. Zařízení firmy Apple podporují 802.11r a 802.11k od operačního systému iOS 6, standard 802.11v podporují nicméně až od verze iOS 7[14]. U systému Android je podpora vždy závislá na konkrétním zařízení, z velkých výrobců mají podporu deklarovanou například právě vybraná zařízení firmy Samsung[15].

Měření je prováděno za běžného provozu a v blízkém okolí se nachází jiné přístupové body. Vzhledem k tomu, že se nacházíme na 2,4GHz pásmu, lze očekávat nějaké rušení. Situace v čase testování byla zachycena pomocí programu WiFi Analyzer a je zobrazena na obrázku 2.2.



Obr. 2.2: Spektrum WiFi signálů ve 2,4GHz pásmu

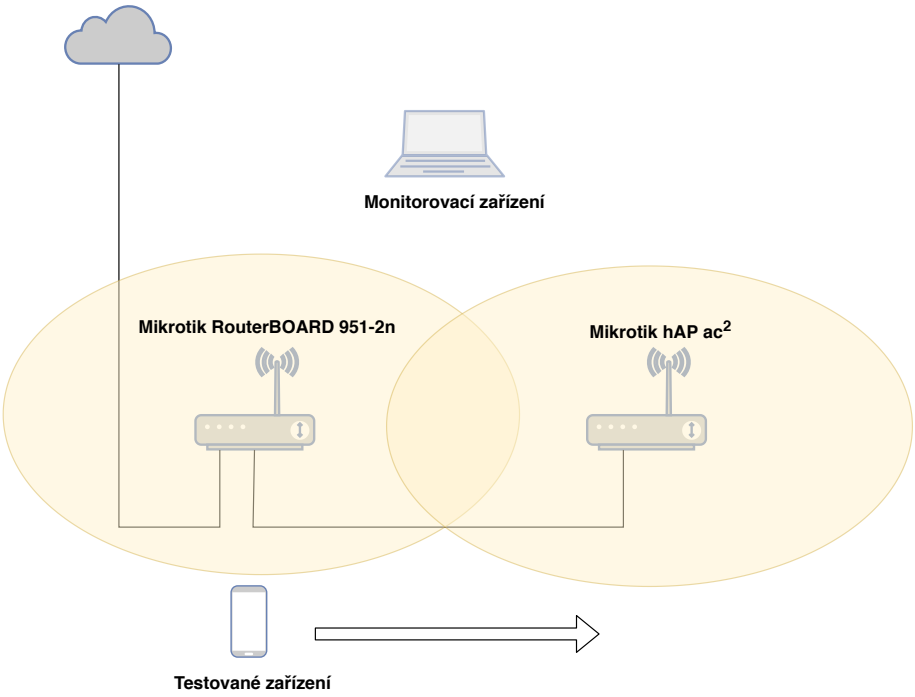
2.1.2 Mikrotik

Testovací topologie pro zařízení Mikrotik je prakticky identická s topologií pro OpenWrt, jsou zde pouze vyměněné přístupové body za zařízení firmy Mikrotik, jak je ukázáno na obrázku 2.3. Konkrétně se jedná o zařízení Mikrotik RouterBOARD 951-2n (RB 951-2n) a Mikrotic hAP ac^2

Obě zařízení Mikrotik používají operační systém RouterOS. Tento systém je založen na linuxovém jádře a je určený pro síťové prvky. RouterOS je vyvíjen firmou Mikrotik a je volně šiřitelný, nicméně k odemčení funkcionalit systému je definováno několik úrovní licencí, poskytovaných právě firmou Mikrotik. Systém lze spravovat tradičně pomocí příkazové řádky nebo pomocí grafického webového rozhraní. Lze také použít aplikaci Winbox, která poskytuje také zprávu pomocí grafického rozhraní. Aplikace Winbox také poskytuje možnost použít takzvaný MAC-Telnet, tedy připojení přes druhou vrstvu OSI modelu, na základě MAC adresy spravovaného zařízení, například v momentě, kdy zařízení nemá nakonfigurovanou IP adresu.

Zařízení RB951-2n je nastaveno podobně jako v topologii pro OpenWrt, jako hlavní směrovač a výchozí brána testované sítě. Stejně tak je zde spuštěna služba DHCP. Jedním ethernetovým rozhraním je zařízení připojeno k internetu, druhým je k síti připojeno zařízení hAP ac^2, které opět plní pouze úlohu přístupového bodu.

Pro konfiguraci bezdrátové sítě lze použít v RouterOS dvě možnosti, a to přímo nastavením jednotlivých bezdrátových rozhraní do módu přístupového bodu, nebo použitím funkce Controlled Access Point system Manager (CAPsMAN). Při použití CAPsMAN lze nadefinovat jedno zařízení jako server (tzv. system Manager), a neo-



Obr. 2.3: Testovací topologie pro Mikrotik

mezený počet dalších zařízení jako přístupové body (Controlled Access Points)[19]. System manager se pak centralizovaně stará o konfiguraci všech takto připojených přístupových bodů a o autentuzaci klientů, kteří se připojují do sítě. Pro testovací síť byli vyzkoušeny oba typy konfigurace.

Nastavení bezdrátové sítě je tu stejné, jako u OpenWrt, tedy obě zařízení pracují ne frekvenci 2412 MHz a využívají šířku pásma 20 MHz. Bezpečnostní protokol je opět zvolen jako WPA2-PSK a je zde opět podpora pouze 802.11n zařízení. ESSID sítě je zde nastaveno jako Roaming_Mikrotik.

Monitorovací a testavaná zařízení jsou použita stejná, jako u OpenWrt.

2.2 Výsledky měření

Při měření času roamingu lze použít několik metodik. V rámci této práce bude použité měření od probe request rámce a měření od authentication request rámce. První z těchto metod začíná momentem, kdy se zařízení rozhodne, že zahájí handoff proces a zahájí skenování odesláním prvního Probe Request (PR) rámce. Konec roamingu se zde liší podle toho, zda je v síti použitý rychlý roaming. Bez použití 802.11r indikuje konec tohoto procesu úspěšné odeslání poslední EAPOL zprávy, tedy ukončeí tzv. four-way handshaku, po kterém je zařízení dále schopné pokračovat v komunikaci. Za použití 802.11r jsou tyto zprávy integrovány do předchozí komunikace,

takže ukončení roamingu zde indikuje úspěšně odeslaný rámec reasociation response. Nevýhodou této metody je, že čas skenování je ovlivněn mnoha různými faktory a může se lišit například dle výrobce zařízení nebo podle použitého ovladače. Z tohoto důvodu je zde použita ještě druhá metoda, při které se jako počátek roamingu považuje Asociation Request (AR) rámec, odeslaný romaujícím zařízením. Konec roamingu je zde uvažovaný stejně jako v předchozí metodě. Při použití této metody měříme „čistý“ čas roamingu, tedy čas který zabere koncovému zařízení projít autentizačním a asociačním procesem. Obě metody jsou použity právě proto, že použití druhé metody opomíjí celý proces skenování a změřením obou těchto časů lze omezit nevýhody použití samostatných jednotlivých metod a tím demonstrovat chování testovaných zařízení při roamingu.

2.2.1 OpenWrt

V tabulkách 2.1 a 2.2 jsou zaznamenány výsledky měření časů roamingu obou testovaných zařízení.

	Apple					
	Čas Bez použití FT [ms]		FT Over the Air [ms]		FT Over DS [ms]	
Číslo měření	od AR	od PR	od AR	od PR	od AR	od PR
1	68,62	89,62	45	64,5	18,37	38,11
2	19,74	40,24	13,62	35,41	12,12	31,87
3	22,12	42,62	12,37	34,07	13,87	33,65
4	22,05	40,87	12,37	34,24	16	37,74
5	26,24	46,86	12,5	34,12	14	35,64
6	19,99	40,62	13,49	33,87	12,95	34,57
7	22,74	43,21	31,35	50,48	13,24	33,18
8	21,49	41,99	13,36	34,73	14	33,88
9	23,98	44,34	12,37	33,99	15,87	35,74
10	20,77	41,24	12,5	33,99	17,37	37,37

Tab. 2.1: Časy roamingu zařízení Apple

První čeho si lze všimnout je, že časy bez použití rychlého roamingu se u obou zařízení poměrně drasticky liší. V ideálních situacích dosahoval čas roamingu zařízení Apple 20–22 ms, přičemž u zařízení Samsung se tyto časy pohybovaly kolem 55–65 ms. U obou zařízení je také vidět, že dochází v měřených časech k poměrně velkým výchylkám od časů, kterých jsou zařízení schopná běžně dosáhnout, u zařízení Samsung jsou však tyto výchylky daleko častější a výraznější. Tyto výchylky lze vysvětlit použitým médiem. Jak bylo řečeno, tato bezdrátová technologie je velice

	Samsung					
	Čas Bez použití FT [ms]		FT Over the Air [ms]		FT Over DS [ms]	
Číslo měření	od AR	od PR	od AR	od PR	od AR	od PR
1	60,13	88,99	17,75	47,74	13,37	43,46
2	100	128,87	16,5	46,37	12,12	42,37
3	101,45	130	13,99	44,36	13,24	43,25
4	146,62	174,87	19,75	49,74	11,99	42,07
5	54,82	83,69	17,74	47,74	13,24	43,25
6	57,87	84,87	13,24	43,37	26,87	57,24
7	78,24	107,12	15,12	44,99	13,45	43,32
8	65,37	94,12	14,23	44,1	12,12	43,25
9	67,31	96,06	11,87	41,87	13,75	43,75
10	116,12	144,11	13,39	43,35	15,37	45,6

Tab. 2.2: Časy roamingu zařízení Samsung

náchylná na rušení, obzvláště na zaplněném 2,4GHz pásmu. Z tohoto důvodu není tato technologie v těchto podmínkách plně spolehlivá a může zde docházet k takovýmto excesům. Jak bylo zmíněno, pro služby VoIP je maximální povolené zpoždění v lokální síti uváděno na 50 ms[6], lze zde tedy poznamenat že zařízení Samsung by zde neuspělo ani s nejnižší naměřenou hodnotou, která dosáhla 54,82 ms. Časy naměřené u zařízení Apple by zde byly dostačující, nicméně nejvyšší výkyv hodnoty tu dosáhl 68,62, kdy by tento čas mohl být pro službu VoIP také kritický. Zde se ale ještě nebere v úvahu čas naměřený s předchozím skenováním sítě počínající rámcem Probe Request.

Časy naměřené od Probe Request rámce se od časů naměřených od Asociation Request rámce u zařízení Apple liší stabilně o 19–21 ms při měření všech konfiguracích testované sítě. U zařízení Samsung se tyto hodnoty liší také stabilně o 28–30 ms. Zde se jedná o čas, který zabere zařízení skenování sítě a výběr nového přístupového bodu, něž takto vybranému bodu odešle zprávu Asociation Request. Jak bylo řečeno, tyto mechanismy implementuje sám výrobce dle svého uvážení, čímž lze vysvětlit rozdílný čas skenování mezi testovanými zařízeními. Zařízení Apple může mít například lépe zacílený výběr kanálů, na které vyšle zprávu Probe Request nebo může mít nastavenou kratší dobu čekání na zprávy Probe Response a podobně.

S aplikací rychlého roamingu naměřené časy dle očekávání klesly. U zařízení Apple jsou časy při použití módů OTA i ODA srovnatelné a pohybují se v ideálních situacích 12–14 ms. U zařízení Samsung jsou tyto hodnoty velmi podobné, v ideálních podmínkách se v obou módech pohybují mezi 12–14 ms. U obou zařízení se opět vyskytují v naměřených hodnotách výchylky. U zařízení Apple je takto maximální

naměřená hodnota 45 ms při metodě OTA, u zařízení samsung 26,87 ms při metodě OTD.

Naměřená data metodikou měření od AR rámce jsou vizualizována na grafech 2.13, 2.14 na straně 37. Na grafech 2.15 a 2.16 na straně 38 jsou zobrazena naměřená data metodou od PR rámce a navíc je zde vykreslena maximální hladina zpoždění, pro službu VoIP v lokální síti. Z grafů je patrné, jak obě zařízení mohou benefitovat ze zavedení rychlého roamingu. Ačkoliv stále dochází k excesům, při kterých může dojít k ohrožení výpadku služeb náchylných na zpoždění v síti, lze konstatovat, že s nižšími časy roamingu, které rychlý roaming zajišťuje, se pravděpodobnost výpadku těchto služeb velmi snižuje. Obzvláště to lze říci o zařízení Samsung, které podle dostupných naměřených dat z tohoto standardu velmi benefituje z důvodu nevyhovujících časů naměřených bez použití rychlého roamingu. Zařízení Samsung se také zdá z naměřených časů být po zavedení rychlého roamingu méně náchylné k větším výkyvům časů roamingu a tím stabilnější, než bez použití tohoto standardu.

2.2.2 Analýza zachycené komunikace

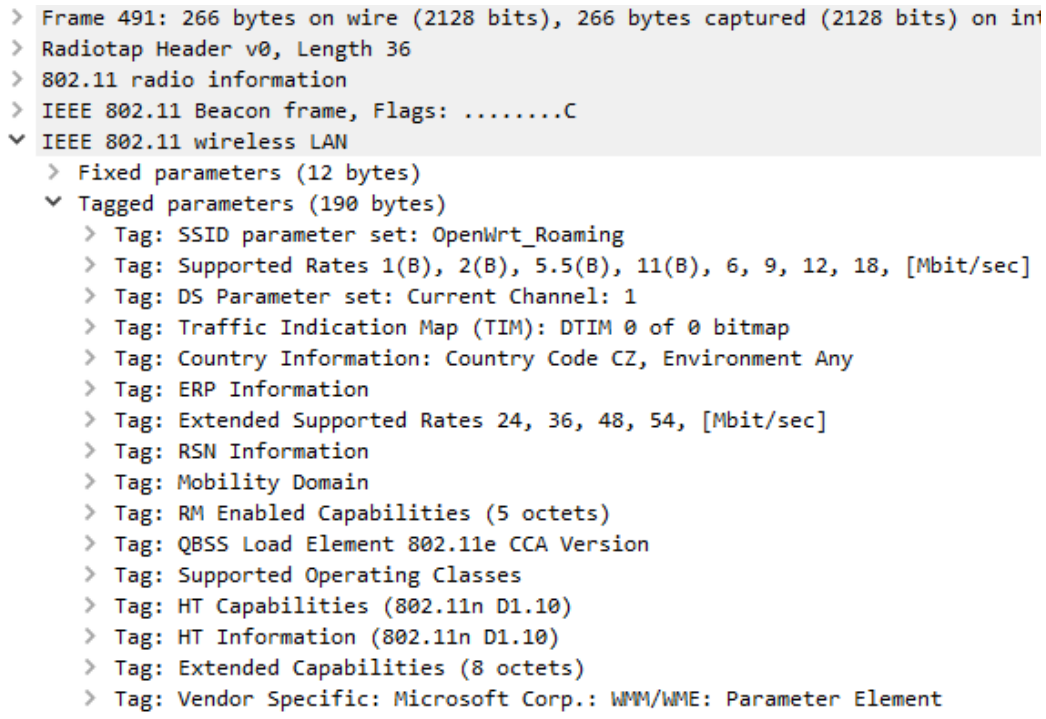
No.	Time	Source	Destination	Protocol	Length	Info
5555	*REF*	Apple_a3:76:87	Broadcast	802.11	172	Probe Request, SN=186, F
5567	0.018825660	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	802.11	94	Authentication, SN=189,
5570	0.021735477	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	802.11	70	Authentication, SN=3958,
5572	0.023999051	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	802.11	208	Reassociation Request, S
5574	0.026251656	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	802.11	179	Reassociation Response,
5576	0.029499682	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	EAPOL	173	Key (Message 1 of 4)
5578	0.032999343	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	EAPOL	195	Key (Message 2 of 4)
5581	0.038377450	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	EAPOL	229	Key (Message 3 of 4)
5583	0.040874129	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	EAPOL	173	Key (Message 4 of 4)

Obr. 2.4: Zachycená komunikace při roamingu bez 802.11r

Na obrázku 2.4 je zachycený proces roamingu bez použití 802.11r. Je zde vidět první rámec Probe Request, nastavený jako časová reference, po něm nachází výměna autentizačních a reasociačních rámců po které následuje four-way-handshake.

Na obrázku 2.5 je zachycený beacon rámec po aktivaci rychlého roamingu na přístupovém bodě. Oproti běžnému beacon rámci je zde přítomné pole Mobility Domain, které informuje uživatele o mobilní doméně, kterou je tento přístupový bod součástí. Také je zde navíc přítomné pole RM (Resource Measurement) enabled capabilities, které informuje ostatní zařízení o podpoře funkcionalit standardu 802.11k.

Na obrázku 2.6 je poté zachycený roaming proces s použitím rychlého roamingu v módu OTA. Proces začíná opět Probe Request rámcem, ale následuje opět autentizace a reasociace. Proces ale tentokrát končí Probe Response rámcem. Na obrázku si



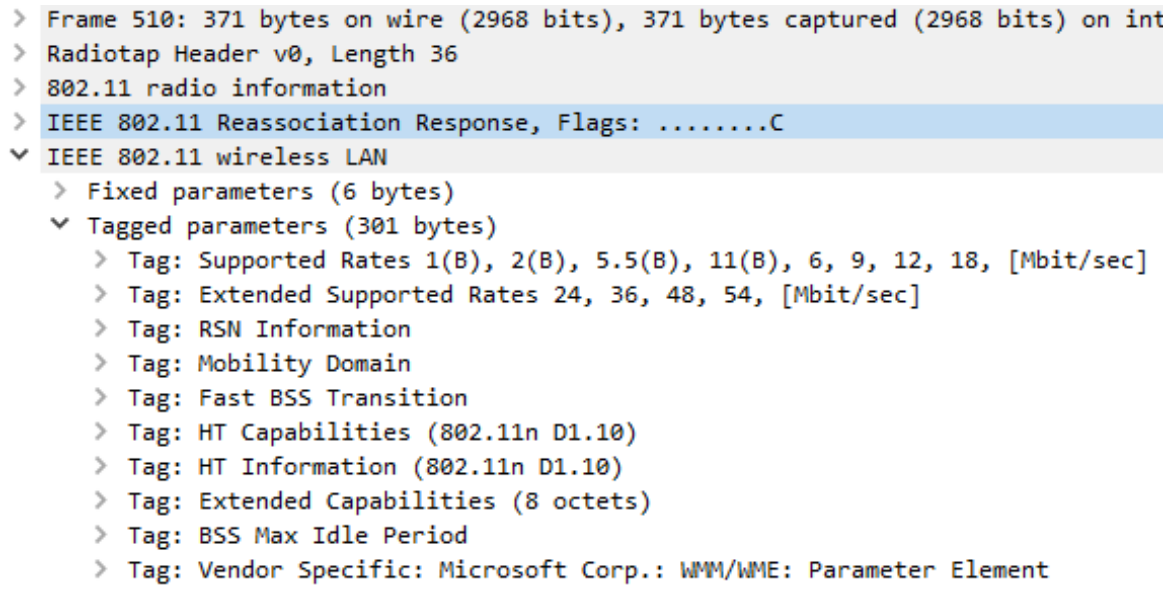
Obr. 2.5: Beacon rámec po aktivaci rychlého roamingu

No.	Time	Source	Destination	Protocol	Length	Info
492	*REF*	Apple_a3:76:87	Broadcast	802.11	172	Probe Request, SN=178,
504	0.021493489	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	802.11	237	Authentication, SN=181,
506	0.025869647	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	802.11	225	Authentication, SN=825,
508	0.029621979	Apple_a3:76:87	Tp-LinkT_4c:c3:8b	802.11	344	Reassociation Request,
510	0.033998008	Tp-LinkT_4c:c3:8b	Apple_a3:76:87	802.11	371	Reassociation Response,

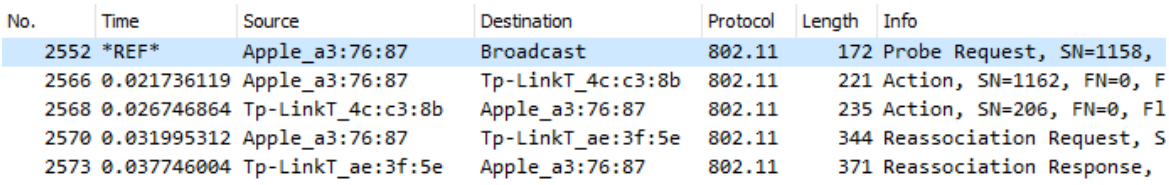
Obr. 2.6: Zachycená komunikace s použitím rychlého roamingu v módu OTA

lze všimnout, že autentizační a reasociační rámce jsou větší, než při komunikaci bez rychlého roamingu. Je to proto, že jsou právě v těchto rámcích zakomponovaná pole Mobility Domain a Fast BSS transition, díky kterým již není potřeba dále provádět klasický four-way-handshake. Pro demonstraci je na obrázku 2.7 zobrazena zpráva reasociation response, kde se tyto dvě pole nachází. Navíc si zde lze všimnout pole BSS Max Idle period. Toto pole je odesíláno v Reasociation Response zprávách při podpoře standardu 802.11v a dává klientovi informaci, jakou dobu nemusí odesílat keep-alive rámce bez odpojení od přístupového bodu.

Při použití rychlého roamingu v módu OTD je proces o něco rozdílnější. Jak je zachyceno na obrázku 2.8, po skenování sítě je místo asociačního rámce novému přístupovému odeslaný Action rámec, který informuje původní přístupový bod o tom, že dojde k reasociaci zařízení. Autentizační informace si následně přístupové body vymění přes distribuční systém. Roaming proces je poté ukončen tradiční výměnou



Obr. 2.7: Reasociation response po aktivaci rychlého roamingu

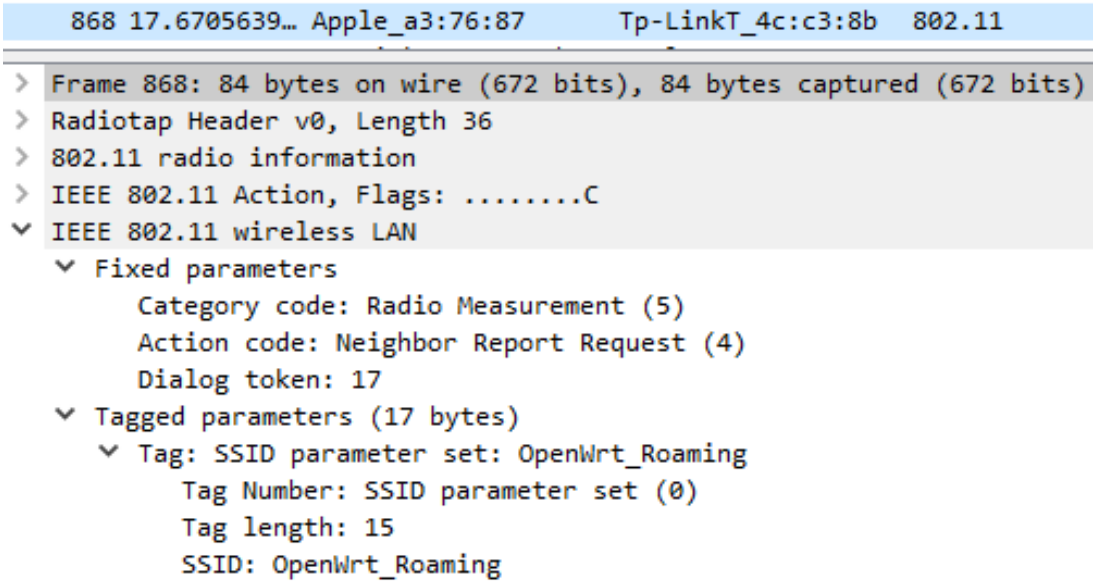


Obr. 2.8: Zachycená komunikace s použitím rychlého roamingu v módu OTD

reasociačních zpráv mezi roamujícím klientem a novým přístupovým bodem.

Na obrázku 2.9 je dále zachycený příklad komunikace protokolu 802.11k. Je zde zobrazen Action rámec Neighbor Report Request. Pole SSID parametr set je zde nastaveno na aktuálně používané SSID, tedy OpenWrt_Roaming. Zařízení Apple tedy odesílá svému přístupovému bodu dotaz na informace o známých sousedních přístupových bodech ve stejné síti. Tyto informace poté může zařízení využít při případném budoucím roamingu.

V této topologii s aplikací rychlého roamingu bylo ještě referenčně otestováno několik zařízení, které nemají podporu rychlého roamingu deklarovanou. Byly to konkrétně telefony Xiaomi redmi 5 plus se systémem Android 8.1.0, Honor 5x se systémem Android 6.0.1 a dva notebooky s operačním systémem Windows 10, jeden se síťovou kartou Intel Centrino Advanced-N 6205 a jeden se síťovou kartou Qalcom Atheros QCA61x4. Všechny tyto zařízení rychlý roaming nepodporují a testování proběhlo jako běžná komunikace ukázaná při testování této topologie bez podpory 802.11r.



Obr. 2.9: Neighbor Request

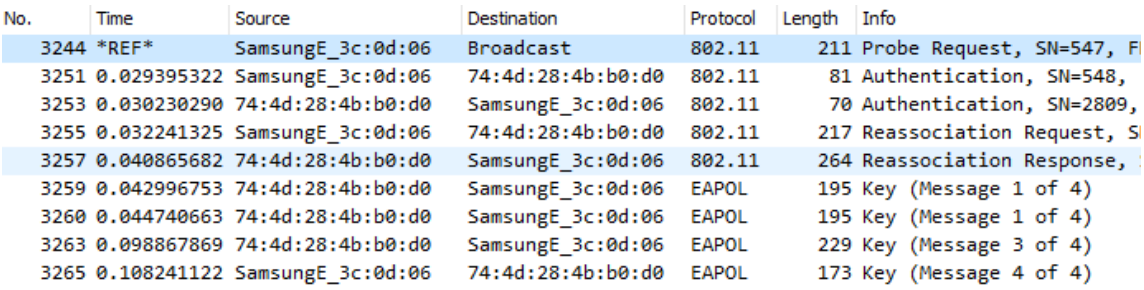
2.2.3 Mikrotik

Samotná zařízení Mikrotik se systémem RouterOS nikde v technické dokumentaci podporu 802.11r, 802.11k a 802.11v nezmiňují. V samotné konfiguraci zařízení se žádná možnost nastavit parametry těchto standardů také nenachází. Referenční testování v topologii s přístupovými body Mikrotik bylo tedy provedeno v identických podmínkách, jako předchozí měření v konfiguraci bezdrátové sítě pomocí CAPsMAN i pomocí přímé konfigurace bezdrátových rozhraní.

No.	Time	Source	Destination	Protocol	Length	Info
1124	*REF*	Apple_a3:76:87	Broadcast	802.11	173	Probe Request, SN=1146, F
1134	0.020807579	Apple_a3:76:87	74:4d:28:4b:b0:d0	802.11	94	Authentication, SN=1149,
1136	0.021459064	74:4d:28:4b:b0:d0	Apple_a3:76:87	802.11	70	Authentication, SN=830, F
1138	0.023426039	Apple_a3:76:87	74:4d:28:4b:b0:d0	802.11	199	Reassociation Request, SN
1140	0.025185858	74:4d:28:4b:b0:d0	Apple_a3:76:87	802.11	264	Reassociation Response, S
1165	0.030467992	74:4d:28:4b:b0:d0	Apple_a3:76:87	EAPOL	195	Key (Message 1 of 4)
1167	0.034104820	Apple_a3:76:87	74:4d:28:4b:b0:d0	EAPOL	195	Key (Message 2 of 4)
1169	0.035174700	74:4d:28:4b:b0:d0	Apple_a3:76:87	EAPOL	229	Key (Message 3 of 4)
1171	0.038405153	Apple_a3:76:87	74:4d:28:4b:b0:d0	EAPOL	173	Key (Message 4 of 4)

Obr. 2.10: Roaming Mikrotik bez použití CAPsMAN se zařízením Apple

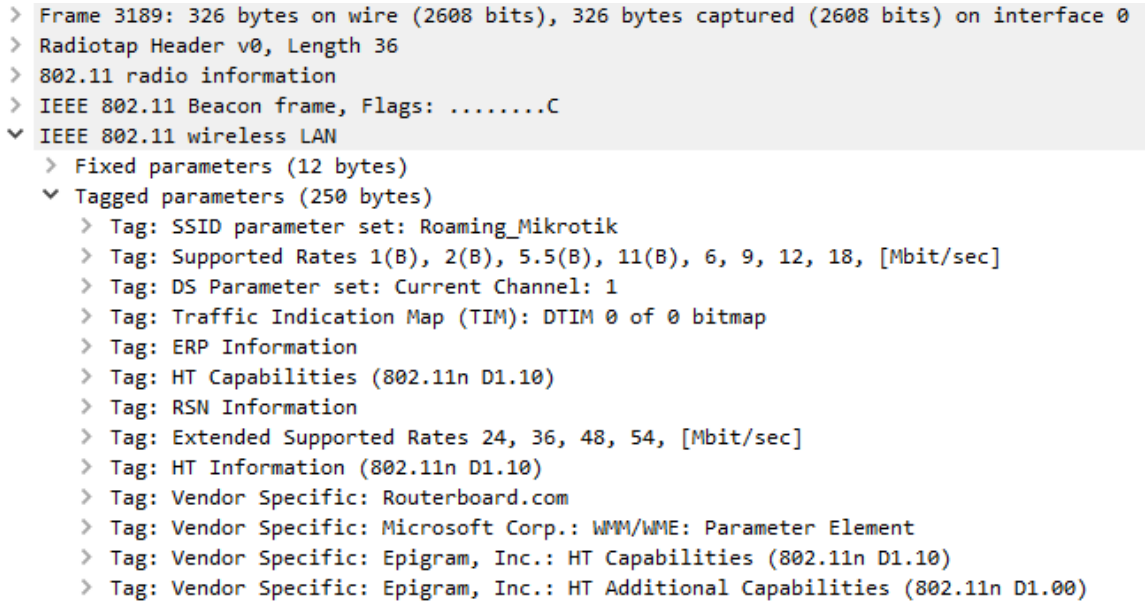
Na obrázku 2.10 je zachycený proces roamingu v této testovací topologii, při ručním nastavení bezdrátové sítě. Z komunikace je vidět, že zde probíhá běžný proces autentizace a asociace bez použití rychlého roamingu. Měření bylo se stejným zařízením několikrát opakováno i v konfiguraci pomocí funkce CAPsMAN, vždy s identickým výsledkem. Čas roamingu naměřený na této topologii je tedy také srovnatelný s časem na OpenWrt bez použití rychlého roamingu. Na obrázku 2.11 je pak



No.	Time	Source	Destination	Protocol	Length	Info
3244	*REF*	SamsungE_3c:0d:06	Broadcast	802.11	211	Probe Request, SN=547, F
3251	0.029395322	SamsungE_3c:0d:06	74:4d:28:4b:b0:d0	802.11	81	Authentication, SN=548,
3253	0.030230290	74:4d:28:4b:b0:d0	SamsungE_3c:0d:06	802.11	70	Authentication, SN=2809,
3255	0.032241325	SamsungE_3c:0d:06	74:4d:28:4b:b0:d0	802.11	217	Reassociation Request, S
3257	0.040865682	74:4d:28:4b:b0:d0	SamsungE_3c:0d:06	802.11	264	Reassociation Response,
3259	0.042996753	74:4d:28:4b:b0:d0	SamsungE_3c:0d:06	EAPOL	195	Key (Message 1 of 4)
3260	0.044740663	74:4d:28:4b:b0:d0	SamsungE_3c:0d:06	EAPOL	195	Key (Message 1 of 4)
3263	0.098867869	74:4d:28:4b:b0:d0	SamsungE_3c:0d:06	EAPOL	229	Key (Message 3 of 4)
3265	0.108241122	SamsungE_3c:0d:06	74:4d:28:4b:b0:d0	EAPOL	173	Key (Message 4 of 4)

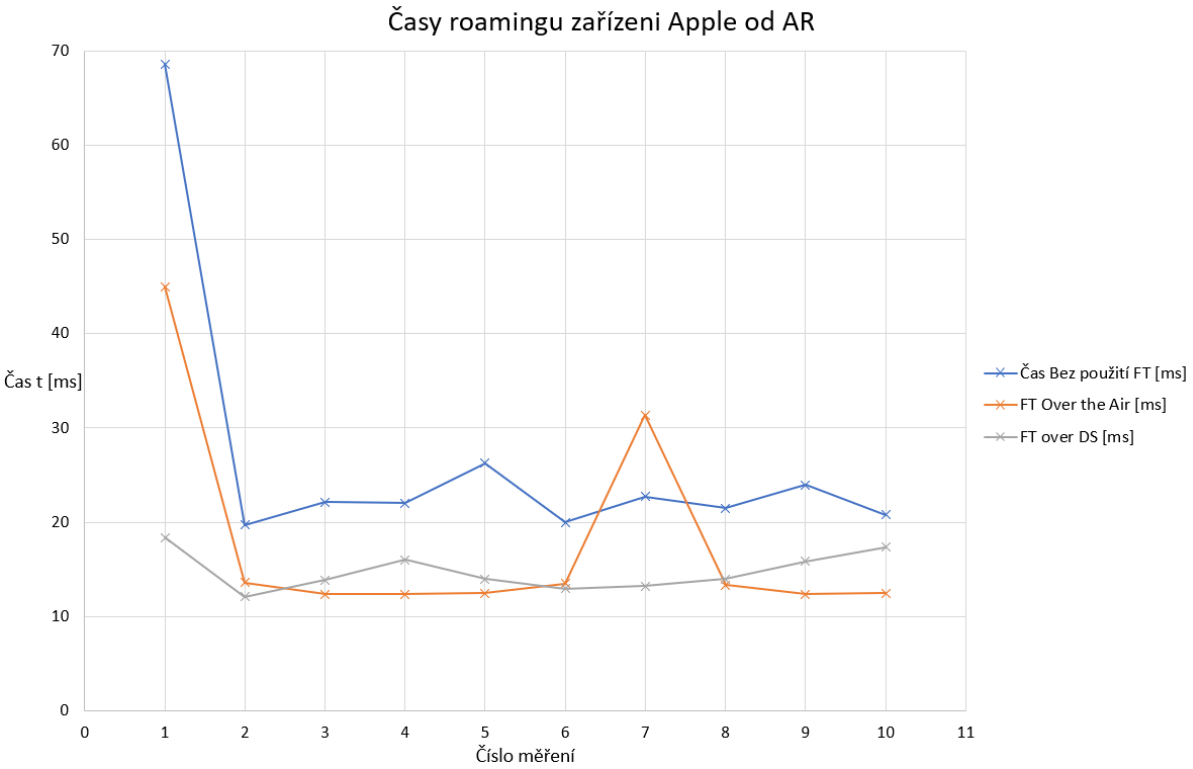
Obr. 2.11: Roaming Mikrotik s použití CAPsMAN se zařízením Samsung

komunikace s testovaným zařízením Samsung za použití konfigurace CAPsMAN. Výsledek je nicméně opět stejný a čas opět srovnatelný s naměřeným časem v předchozí testovací topologii.

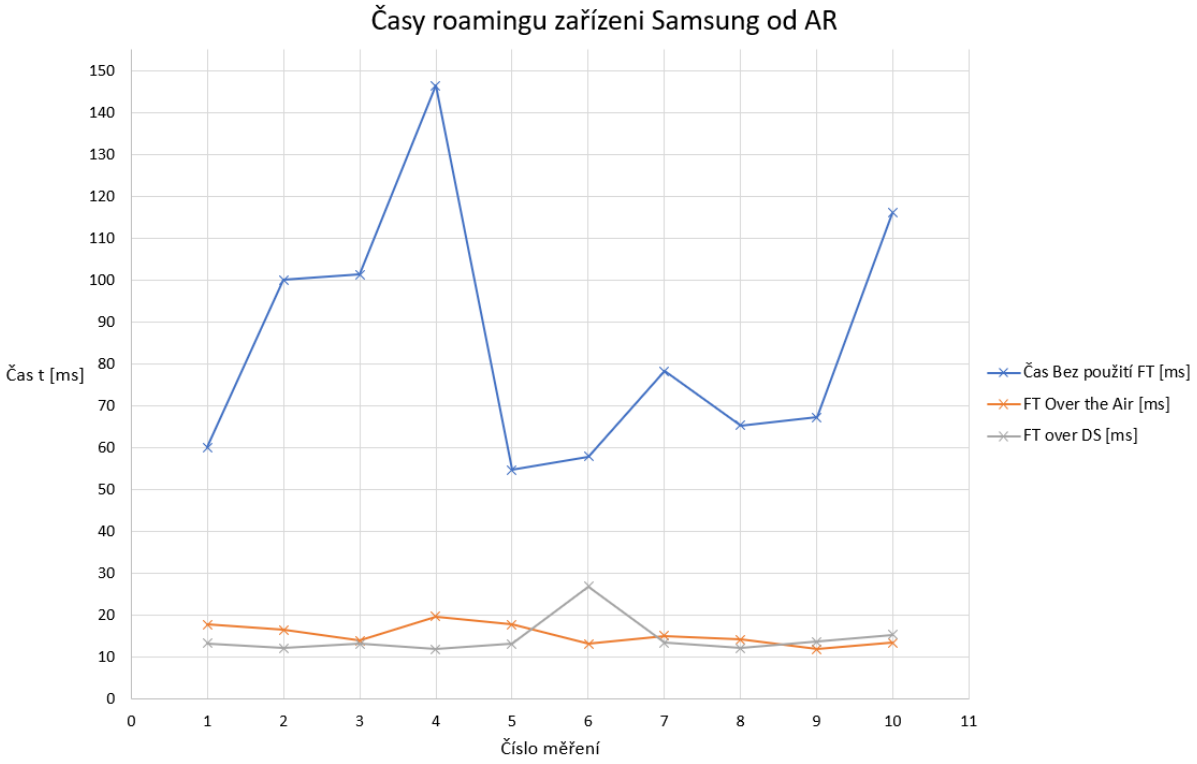


Obr. 2.12: Beacon rámec zařízení Mikrotik

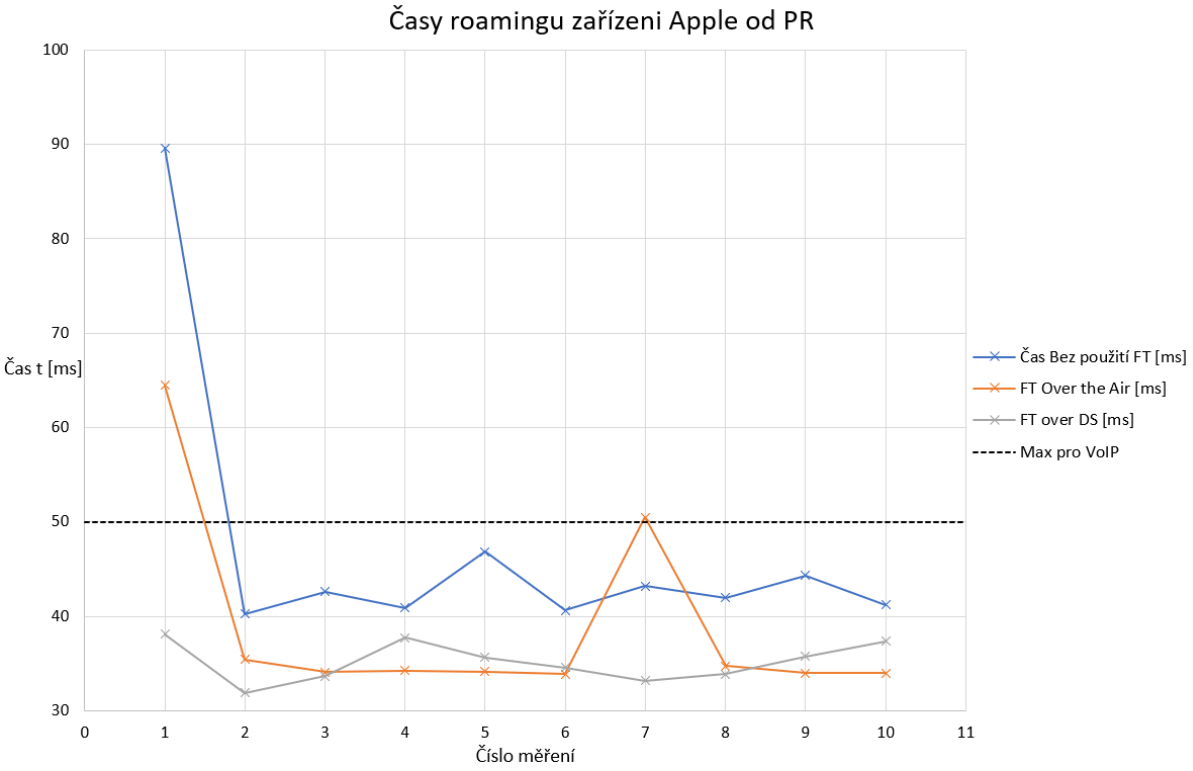
Na obrázku 2.12 je zobrazený zachycený beacon rámec zařízení RouterBOARD 951-2n. Zde můžeme také vidět absenci jakýchkoliv polí, která by značila podporu rychlého roamingu. Na základě těchto informací a výsledků testových měření v této topologii lze předpokládat, že zařízení mikrotik moderní standardy pro podporu roamingu nepodporuje. Dle srovnatelných časů roamingu naměřených v této topologii a naměřených časů v topologii OpenWrt bez podpory rychlého roamingu a dle identické komunikace při procesu roamingu lze také předpokládat, že zařízení Mikrotik ani neimplementují žádné proprietární řešení pro tuto problematiku, jak činí například firmy Cisco[20], nebo Ubiquiti[21].



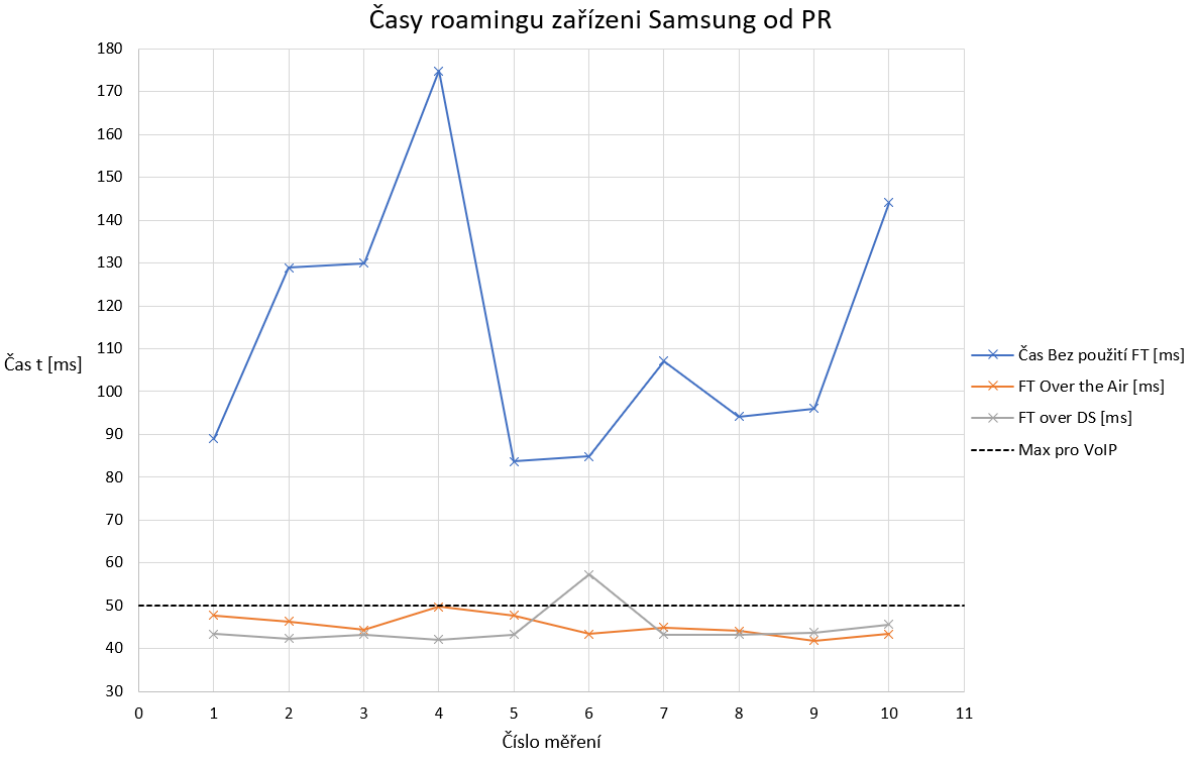
Obr. 2.13: Testování času roamingu zařízení Apple od AR



Obr. 2.14: Testování času roamingu zařízení Samsung od AR



Obr. 2.15: Testování času roamingu zařízení Apple od PR



Obr. 2.16: Testování času roamingu zařízení Samsung od PR

3 Závěr

Jedním z cílů této práce je efektivně popsat proces roamingu, tedy proces při němž se zařízení připojené k bezdrátové síti připojí k přístupovému bodu stejné sítě s lepším signálem. V úvodu této práce je tedy přiblížena celková problematika Wi-Fi sítí, na kterou navazuje popis, jak celý roaming proces probíhá, jaké jsou fáze tohoto procesu a jak tyto fáze ovlivňují prodlevu, během které roamující zařízení nemůže komunikovat. Práce je zaměřená na moderní doplňky standardu 802.11 podporující roaming, tedy 802.11r, 802.11k a 802.11v. V teoretické části jsou tedy dále popsané mechaniky a funkce, které tyto doplňky přináší a jaké benefity mohou tyto doplňky přinést k celkovému fungování bezdrátových sítí.

Pro testování těchto služeb byla vytvořena topologie založená na zařízeních OpenWrt, která tyto moderní standardy pro podporu roamingu podporuje. Na této topologii proběhlo testován na zařízení Apple a zařízení Samsung před a po zavedení těchto standardů. Testovaná zařízení se v této topologii chovala přesně dle očekávání a popsané teorie. Z naměřených výsledků je také vidět, jak tyto zařízení benefitují z implementace těchto standardů. Zde testované standardy mohou být velmi důležitá zejména při použití služeb citlivých na zpoždění a výpadky komunikace. Je zde demonstrováno, že podle naměřených dat by zařízení Samsung mohlo mít před zavedením těchto mechanismů velký problém při používání služby VoIP, kdyby v průběhu komunikace došlo k roamingu. Je zde také demonstrováno, jak reálný proces roamingu probíhá na konkrétně zachycené komunikaci.

Cílem práce bylo rovněž otestovat roaming na zařízeních Mikrotik s operačním systémem RouterOS. Pro tyto účely zde byla vytvořena identická topologie, jako pro měření prvků OpenWrt. Pro testování zde byli použity stejná koncová zařízení jako v předchozí topologii. Testování zařízení Mikrotik ukázalo, že tyto přístupové body standardy pro podporu roamingu neimplemetují a pravděpodobně ani neimplementují žádné proprietární řešení této problematiky.

Literatura

[1] HIERTZ, G.;denteneer. The IEEE 802.11 universe. *Communications Magazine, IEEE* [online]. USA: IEEE, 2010, **48**(1) [cit. 2018-12-14]. DOI: 10.1109/MCOM.2010.5394032. ISSN 0163-6804. Dostupné z: https://ieeexplore.ieee.org/document/5394032#full-text-section

[2] *Wi-Fi Alliance* [online]. [cit. 2019-05-22]. Dostupné z: https://www.wi-fi.org/

[3] STALLINGS, W. IEEE 8O2.11: wireless LANs from a to n. *IT Professional* [online]. USA: IEEE, 2004, **6**(5), 32-37 [cit. 2018-12-14]. DOI: 10.1109/MITP.2004.62. ISSN 1520-9202. Dostupné z: https://ieeexplore-ieee-org.ezproxy.lib.vutbr.cz/document/1362623

[4] SOSINSKY, Barrie. *Mistrovství — počítačové sítě*. Computer Press, 2010. ISBN 978-80-251-3363-7.

[5] VERMA, Lochan;fakharzadeh. Wifi on steroids: 802.11AC and 802.11AD. *Wireless Communications, IEEE* [online]. USA: IEEE, 2013, **20**(6), 30-35 [cit. 2018-12-14]. DOI: 10.1109/MWC.2013.6704471. ISSN 1536-1284. Dostupné z: https://ieeexplore-ieee-org.ezproxy.lib.vutbr.cz/document/6704471

[6] *QOS: VOIP QoS Requirements* [online]. [cit. 2018-12-14]. Dostupné z: https://www.voip-info.org/qos/

[7] MACHAN, P.;wozniak. Proactive handover for IEEE 802.11r networks. In: *Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP* [online]. IEEE Publishing, 2011, s. 1-7 [cit. 2018-12-14]. DOI: 10.1109/WMNC.2011.6097242. ISBN 9781457711923. Dostupné z: https://ieeexplore-ieee-org.ezproxy.lib.vutbr.cz/document/6097242

[8] KHAN, K.n.;rehana. Wireless handoff optimization: A comparison of IEEE 802.11r and HOKEY. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* [online]. 2010, **6164**, s. 118-131 [cit. 2018-12-14]. DOI: 10.1007/978-3-642-13971-0_12. ISBN 3642139701. ISSN 03029743.

[9] CHUNG-SHENG LI, YUNG-CHIH TSENG a HAN-CHIEH CHAO. A Neighbor Caching Mechanism for Handoff in IEEE 802.11 Wireless Networks. In: *Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on* [online]. IEEE, 2007, s. 48-53 [cit. 2018-12-14]. DOI: 10.1109/MUE.2007.32. ISBN 0-7695-2777-9. Dostupné z: https://ieeexplore-ieee-org.ezproxy.lib.vutbr.cz/document/4197248

[10] GORANSSON, Paul a Raymond GREENLAW. *Secure roaming in 802.11 networks*. Boston: Newnes/Elsevier, c2007. ISBN 978-0-7506-8211-4.

[11] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1. New York, USA: IEEE, 2008. DOI: 10.1109/IEEESTD.2008.4544755.

[12] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8. USA: IEEE, 2011. DOI: 10.1109/IEEESTD.2011.5716530.

[13] *OpenWrt* [online]. [cit. 2019-05-24]. Dostupné z: https://openwrt.org/

[14] Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS. *Apple Support* [online]. Cupertino, Kalifornie: Apple, c2019 [cit. 2019-05-25]. Dostupné z: https://support.apple.com/en-us/HT202628

[15] Knox Platform in-depth articles: Enhanced Roaming Algorithm. *Samsung Knox* [online]. Seoul, Jižní Korea: Samsung, c2018, 2019-03-20 [cit. 2019-05-25]. Dostupné z: https://support.samsungknox.com/hc/en-us/articles/115013403768-Enhanced-Roaming-Algorithm

[16] Fast Roaming with 802.11k, 802.11v, and 802.11r. *Hardware Dev Center* [online]. Redmond, Washington: Microsoft, c2019, 2017-04-20 [cit. 2019-05-25]. Dostupné z: https://docs.microsoft.com/en-us/windows-hardware/drivers/network/fast-roaming-with-802-11k–802-11v–and-802-11r

[17] Support for Fast BSS Transition Roaming on Windows® 10 with Intel® Wireless Adapters. *Support Intel* [online]. Santa Clara, California: Intel Corporation, 2017-04-12 [cit. 2019-05-25]. Dostupné z: https://www.intel.com/content/www/us/en/support/articles/000021562/network-and-i-o/wireless-networking.html

[18] About wpa-supplicant. *Ubuntu documentation* [online]. Canonical [cit. 2019-05-25]. Dostupné z: https://docs.ubuntu.com/core/en/stacks/network/wpa-supplicant/docs/

[19] Manual:CAPsMAN. *Mikrotik Documentation* [online]. Riga, Litva: Mikrotik, 2019-04-23 [cit. 2019-05-25]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:CAPsMAN

[20] 802.11 WLAN Roaming and Fast-Secure Roaming on CUWN. *Cisco Support* [online]. San Jose, Kalifornie: Cisco Systems, 2018-08-29 [cit. 2019-05-25]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html

[21] UniFi - Fast Roaming. *UBNT Support* [online]. New York City, New York: Ubiquiti Networks, c2019 [cit. 2019-05-27]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/115004662107-UniFi-Fast-Roaming

Seznam symbolů, veličin a zkratek

VoIP	Voice over Internet Protocolo
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
WLAN	Wireless Local Area Network
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
OFDM	Ortogonální multiplex s frekvenčním dělením
CCK	Complementary Code Keying
MIMO	multiple-input multiple-output
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
IAPP	Internet Access Point Protocol
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
EAPOL	Extensible Authentication Protocol Over LAN
QoS	Quality of Service
MDIE	Mobility Domain Information Element
FTIE	Fast Transition Information Element
OTD	Over the Distribution Service
OTA	Over the Air
PSK	Pre-Shared Key
PTempK	Pairwise Temporal Key
MSK	Master Session Key
RRM	Radio Resource Measurement
MIB	Management Information Database
RCPI	Received Channel Power Indicator
FCS	Frame Check Sequence
LCI	Location Configuration Information
WNM	Wireless Network Management
DMS	Directed multicast service
RSNA	Robust Security Network Associations
FMS	Flexible multicast service
DTIM	Delivery traffic indication message
opkg	open package management
UCI	unified configuration interface

CAPsMAN Controlled Access Point system Manager
AR Asociation Request
PR Probe Request