Mendelova univerzita v Brně
Provozně ekonomická fakulta

Řízení síťového provozu v bezdrátovém spoji WAN sítě

Diplomová práce

Vedoucí práce:
Ing. Petr Zach Ph.D.

Bc. Martin Kučera

Brno 2017

Rád bych poděkoval svému vedoucímu práce, panu Ing. Petru Zachovi, Ph.D., za cenné rady, připomínky a čas strávený kontrolou a metodickým vedením při zpracování závěrečné práce. Dále bych chtěl poděkovat za podporu své přítelkyni a rodině.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Řízení síťového provozu v bezdrátovém spoji WAN sítě.**
vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 20. května 2017 _____

Abstract

Kucera, M. Managing network traffic on a wireless WAN network. Diploma thesis. Brno. 2017

The diploma thesis focuses on the issue of controll network traffic in wireless link. The requirements specification is suggested solution which is implemented and tested in laboratory conditions. The verification is carried out in the WAN network of TS-Hydro, s.r.o. The results are evaluated in the discussion.

Keywords

MikroTik, QoS, NV2, WMM, Queue Tree, IPTV

Abstrakt

Kučera, M. Řízení síťového provozu v bezdrátovém spoji WAN sítě. Diplomová práce. Brno. 2017

Diplomová práce se zaměřuje na problematiku řízení síťového provozu v bezdrátovém spoji. Po specifikaci požadavků je navrhnuto řešení, které je implementováno a otestováno v laboratorních podmínkách. Verifikace je provedena ve WAN síti firmy TS–Hydro, s.r.o. V diskuzi jsou zhodnocené výsledky.

Klíčová slova

MikroTik, QoS, NV2, WMM, Queue Tree, IPTV

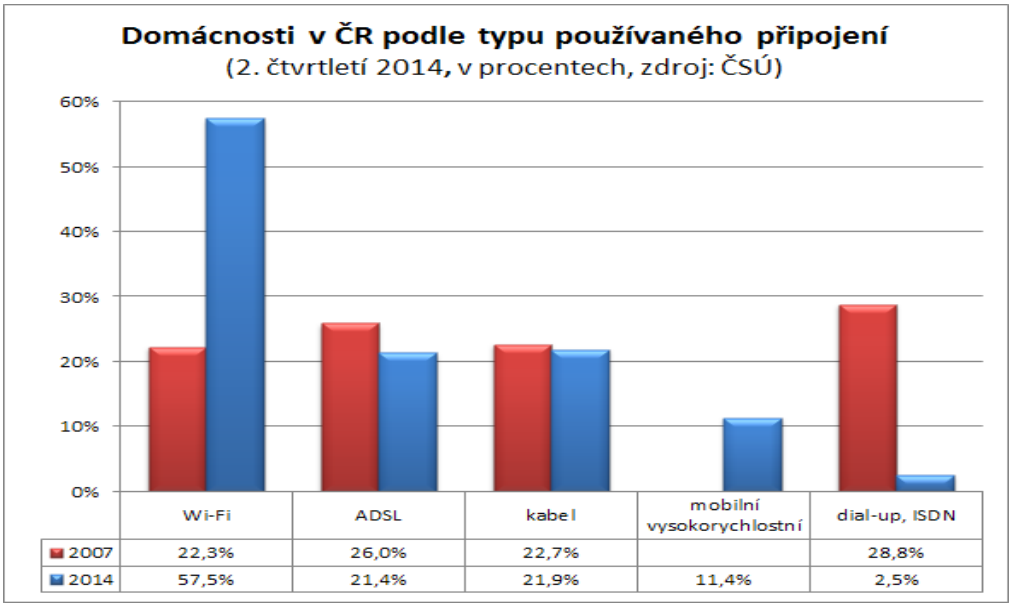
Obsah

1 Úvod

1.1 Motivace a cíl práce

Každé médium přenášející data má svoji limitovanou kapacitu. Při nedostatečné šířce pásma, může docházet k různým zpožděním v doručování paketů nebo doručení v jiném pořadí než bylo vysílání. Tento problém řeší transportní protokol TCP, který vše opraví, aniž by si uživatel všiml nějakých nedostatků. Problém nastává u přenosu multimediálních dat, která vyžadují výsledek v co nejkratším čase a nemá smysl provádět retransmise. Tím vznikají problémy s poruchou zvuku a obrazu. Do této skupiny patří – telefonní hovory (VoIP, Voice over IP), přenos videa (IPTV, Internet Protocol television), aj. Reakcí na tuto otázku vznikla komplexní technologie QoS (Quality of Service), která má zajistit uživateli doručení dat v potřebné kvalitě. Řízení síťového provozu je důležitou součástí počítačových sítí.

U bezdrátových sítí je řízení sítě složitější, protože přenos dat je ovlivněn vnějšími faktory jako např. počasí nebo rušení. Zmíněné vnější faktory lze ovlivnit, ale nikoliv eliminovat. V České republice se klade čím dál větší důraz na kvalitu přenosu dat u bezdrátových sítí a to z důvodu, že Česká republika je světová velmoc v počtu bezdrátových přípojek k Internetu.



Obr. 1 Domácnosti v ČR podle typu připojení k Internetu.
Zdroj: Lupa, 2014.

Většina těchto ISP (Internet Service Provider) poskytují své služby na lokální úrovni a to díky nízkým pořizovacím nákladům na provoz. Příliš mnoho poskytovatelů v bezlicenčních pásmech má negativní vliv na přenos dat. Omezený počet

šířky pásma způsobuje, že poskytovatelé se na daném kmitočtu překrývají a vzniká zmiňované rušení.

Pro použití bezdrátových sítí musíme dodržovat určitá pravidla, která stanovuje ČTU (Český telekomunikační úřad). Pro různá frekvenční pásma platí odlišná pravidla, která je před implementací potřeba nastudovat. V České republice se používá především bezlicenční pásmo 5 GHz a 10 GHz.

Tato práce je reakcí na potřeby firmy TS–Hydro, s.r.o., která se zabývá službami v oblasti počítačové techniky a především poskytováním Internetů. Firma vznikla v roce 2003 a během let má přibližně 400 připojených uživatelů včetně škol a firem. Infrastruktura je založena na platformách bezdrátových výrobců Alcoma, Ubiquity a především MikroTik. Firma je připojena na mezinárodní páteřní síť a bezdrátovými technologiemi poskytuje internetové připojení v různých vesnicích v okolí Brna. Z důvodu konkurenceschopnosti a vyšších nároků uživatelů je třeba rozšířit nabídku o poskytování služeb IPTV. Tato služba ovšem musí být naprosto spolehlivá, protože uživatel si všimne u sledování televize jakéhokoliv nedostatku (posun zvukové stopy, kostičkování, sekání obrazu). Distribuce těchto služeb by dala náskok firmě před konkurencí, která si netroufá poskytovat tyto služby na bezdrátových platformách.

1.2 Cíl práce

Cílem práce je zjistit, zda je možné využívat multimediální prostředky komunikace v bezdrátových sítích na různých frekvenčních pásmech. Díky spolupráci s firmou TS–Hydro, s.r.o., budou testy prováděny i v produkční síti. Závěrečné výsledky nám poskytnou dostatek informací, jestli bezdrátové technologie dosáhli úrovně, kdy lze poskytovat IPTV v outdoor bezdrátových sítích ISP.

1.3 Organizace práce

Na začátku diplomové práce je sepsána literární rešerše shrnující dostupnou literaturu v podobě závěrečných prací, vědeckých publikací a odborných knih. Cílem literární rešerše je získat aktuální přehled o stavu v dané oblasti. Současně je důležité získat teoretický přehled o problematice řízení sítě v bezdrátových sítích.

V úvodní kapitole teoretické části je podrobně popsána teorie bezdrátové komunikace. Obecně jsou popsány jevy, ke kterým dochází při šíření vlny prostředím. V práci nás budou zajímat frekvenční pásma 5 GHz, 10 GHz a 24 GHz. Pro každé frekvenční pásmo je popsán typ modulace, přístup náhodného přístupu k médiu CSMA (Carrier Sense Multiple Access), TDMA (Time Division Multiple Access) a protokoly, které zařízení mohou použít (802.11, NV2, Nstreme). V závěrečné kapitole bude popsána legislativa, která je součástí každého provozovatele bezdrátové komunikace.

Další kapitola se věnuje QoS, kde je popsán důvod vzniku, nasazení a jeho typ mechanismu pro řízení sítě. V bezdrátovém prostředí je jediným mechanismem pro QoS standard IEEE 802.11e. V teoretické části je popsán i původní 802.11 MAC, který používal přístupy DCF (Distributed Coordination Function) a PCF (Point Coordination Function). Protokol 802.11e vylepšuje oba tyto přístupy. Z důvodu

složitosti normy 802.11e byl vytvořen model WMM (Wireless MultiMedia), který má nutnou podporu EDCA přístupu (Zelinka, 2009). K řízení sítě jsou v teoretické části popsány druhy front a klasifikace provozu.

Jedna kapitola se bude věnovat srovnání různých platforem. Na základě specifikací (cena, výkon, funkčnost) zhodnotíme, který výrobce je nejvhodnější.
Kapitola praktické části začíná analýzou současného stavu sítě firmy TS–Hydro. Pochopení technologické filozofie firmy je nezbytnou součástí k další návrhové části. Možnosti konfigurace jsou nejprve testovány v laboratorních podmínkách na základě zvolené metodiky. Na základě výsledků zvolíme optimální řešení pro implementaci do produkční sítě.

Výsledky z laboratorního měření verifikujeme v síti ISP. Z důvodu vnějších faktorů, které ovlivňují bezdrátové technologie, tak mohou být výsledky v různých podmínkách odlišné.

1.4 Rešerše

Při vyhledávání podobných bakalářských a diplomových prací v univerzitním informačním systému[1] jsem nalezl bakalářskou práci „Využití QoS pro podporu VoIP a videotelefonie ve firemní síti“ (Drobný, 2014), která se zabývá implementací služby QoS. Disertační práce „Metodika sledování a hodnocení počítačové sítě podniku“ (Zach, 2015) se zabývá problematikou zajištění kvality hlasových služeb v počítačových sítí z pohledu QoS a QoE (Quality of Experience). Závěrečná práce Jakuba Konečného (Konečný, 2015) se jako jedna z mála prací zabývá problematikou VoWLAN (Voice over WLAN). Dále se práce zabývá optimalizací univerzitní bezdrátové sítě pro provoz hlasových služeb a podrobně popisuje metody pro vyhodnocování uživatelské spokojenosti QoE a MOS (Mean Opinion Score).

Pro vyhledávání různých prací z různých univerzit slouží portál theses.cz, kde jsem zadal klíčové slovo QoS a našel jsem spoustu prací zabývajících se tímto tématem. Závěrečná diplomová práce „QoS v síti VŠE“ (Kalina, 2013) se zaměřuje i na způsob řízení kvality služby na bezdrátových technologiích. Také zde nalezneme kvalitně popsány typy QoS a jejich možnosti. Další diplomová práce „Bezdrátové sítě v zarušených prostředích“ (Skipala, 2011) se zabývá tématem přenosu dat v zarušených prostředích na frekvenci 5 GHz s využitím platformy MikroTik. Diplomová práce „VoIP v bezdrátové síti VŠE“, má za cíl ověřit možnosti provozu VoIP v síti Vysoké školy ekonomické v Praze v dostatečné kvalitě. V práci jsou popsány principy VoIP a související technologie bezdrátových sítí nutných pro kvalitní a stabilní provoz. V závěru je řešení aplikováno v reálném prostředí ve Staré budově na Žižkově při roamingu a využití několika pokročilých standardů 802.11.

Webový portál sciencedirect.com, do kterého se přihlásíme přes univerzitní login, obsahuje několik vědeckých článků s podobným zaměřením jako tato práce. Publikace „Improving QoS of IPTV and VOIP over IEEE 802.11n“ (Saleh, Shah, Baig, 2014) je zaměřena na studii zlepšení přenosu IPTV a VoIP přes IEEE 802.11n

[1] is.mendelu.cz

WLAN. Výsledky zahrnují analytické a experimentální zkoumání. Autoři navrhují bezdrátové posílení pomocí TFMCC (TCP – Friendly Multicast Congestion Control) ke zvýšení kapacity a kvality přenosu. Další publikace „Network centric QoS performance evalutaion of IPTV transmission quality over VANETs“ (Oche, Noor, Aghinya, 2014) zjišťuje, jak nejlépe lze streamovat provoz přes VANETs (Vehicular ad hoc networks). Publikace konstatuje, že IPTV vyžaduje velkou šířku pásma a přísnou kvalitu služby.

K Seznámení s MikroTik RouterOS nám pomůže anglická literatura „Learn RouterOS“ (Burgess, 2009). Kniha představuje tento proprietární software, který je součástí všech prvků vyrobených lotyšskou firmou MikroTik. Autor popisuje možnosti nastavení i nevýhody tohoto operačního systému. Rigorózní práce z Masarykovy univerzity (Rebook, 2008) se věnuje problému QoS z pohledu aktivních programovatelných směrovačů. Práce rozšiřuje koncept QoS v IP sítích o problematiku kvality služby na programovatelných směrovačích, jako je prostorový čas, velikost volné paměti a další. Nasazením asymetrického QoS v bezdrátové síti se zabývá práce z University of Calgary (Hu, Wiliamson, Fapojuwo, 2011). Autoři nasazují QoS na přístupovém bodě z důvodu nedostatečného rozšíření standardu 802.11e v jednotlivých zařízeních.

Při vyhledávání podobných prací přes google.com jsem našel práci „Analýza závislosti komunikačních služeb na zpoždění a optimalizace QoS“ (Schön, 2015). Tato práce se zabývá řízením a optimalizací provozu. Teoretická část je dobře sepsána a autor popisuje nejen DCF a PCF, ale i mechanizmy EDCF (Enhanced Distribution Coordination Function), HCF (Hybrid Coordination Function) a především WMM. Praktická část je simulovaná v programu OPNET, kde si autor tvořil vlastní scénáře. Velice podobnou prací je „Analýza přenosu dat v konvergované síti“ (Menšík, 2011). V této práci je dobře popsána architektura Wi-Fi sítí. Praktická část je opět provedena v programu OPNET.

Závěrečných prací, které se zabývají řízením sítě s podílem multimediálních dat, je mnoho. Většina těchto prací je navržená v laboratorních podmínkách a testována na platformách, kterými škola disponuje. V této práci, díky spolupráci s firmou TS–Hydro, s.r.o., bude praktická část testována i v reálných podmínkách na frekvenčních pásmech, které studenti nemají k dispozici.

2 Teorie bezdrátové komunikace

Obecně bezdrátová komunikace je spojení dvou subjektů jiným než mechanickým způsobem. Podle typu nosného média můžeme rozlišovat mezi komunikací optickou, rádiovou a sonickou. Vzdálenost mezi komunikujícími body je od pár centimetrů do milionů kilometrů. Bezdrátové sítě dokáží pracovat ve frekvenčních pásmech od 900 MHz do 80 GHz. (Švarc, 2016). V České republice, stejně jako v celé Evropě, určuje použitelné frekvence organizace ETSI (European Telecommunications Standards Institute). V práci využíváme frekvenční pásma 5, 10 a 24 GHz, které patří podle ITU (International Telecommunication Union) do SHF (Super high frequency). SHF má rozmezí 3 GHz – 30 GHz. Tyto frekvence spadají do mikrovlnného pásma a patří sem bezdrátové sítě LAN, DSRC (Dedicated short-range communications), moderní radary, komunikační satelity, televizní vysílaní, amatérské rádio a další. Podle ITU se v článku 2 o poskytování uvádí, že rádiová spektra musí být rozdělena do devíti frekvenčních pásem. SHF využívá rozsah vlnové délky od 1 do 10 cm. (ITU, 2004).

V těchto frekvencích vyžadují spoje přímou viditelnost mezi anténami, kdy přímá spojnice mezi anténami není zastíněná žádnou překážkou (kopec, budova, stromy). Pokud se šířící signál dostává do antény odrazem od okolního prostředí, pak se jedná zpravidla o velmi nekvalitní a nestabilní spoj. (Skipala, 2011).

2.1 Přenosová soustava

Základní dělením spojů je podle počtu stanic účastnících se komunikace. Tedy bod–bod (PtP – Point to Point) nebo systém bod-multibod (PtMP – Point to Multipoint) s více stanicemi. Z hlediska přenosu signálu je vhodné nahlížet na každý spoj jako PtP a na PtMP pak nahlížíme jako na více spojů PtP (Skipala, 2011).

2.1.1 Typy bezdrátových sítí

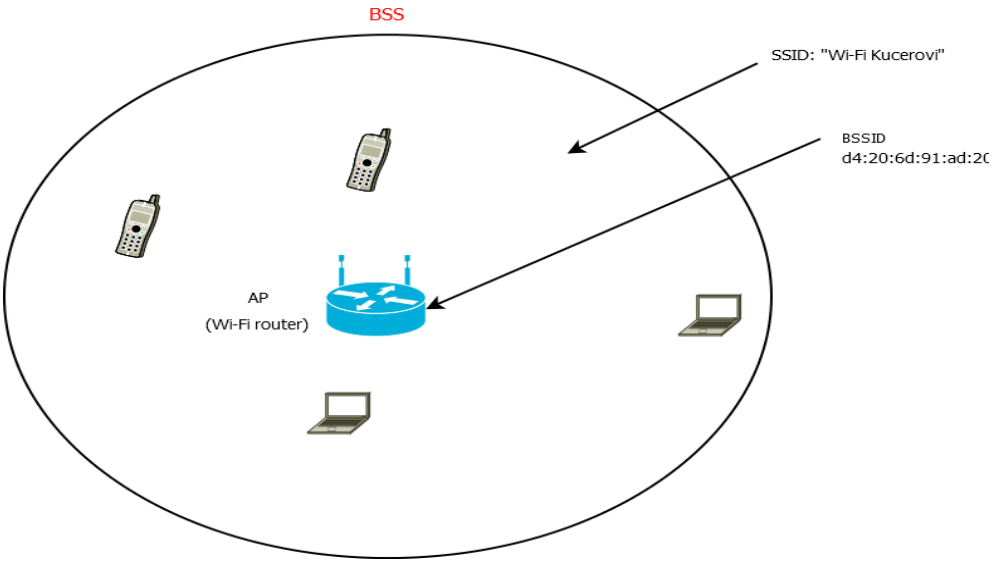
- **WPAN (Wireless Personal-Area Network)** – využívá vysílače s nízkým vyzařovacím výkonem a přenos je určen na krátké vzdálenosti (7–10 m). WPAN jsou založeny na standardu 802.15 a zahrnují technologie Bluetooth nebo ZigBee. (Hucaby, 2014).
- **WLAN (Wireless Local-Area Network)** – síť středního rozsahu, obvykle do 100 m. Spojení probíhá pomocí standardu IEEE 802.11 a přenos probíhá na bezlicenčních pásmech 2,4 GHz a 5 GHz. (Hucaby, 2014).
- **WMAN (Wireless Metropolitan-Area Network)** – z geografického hlediska se jedná o část nebo celá města. Frekvence jsou běžně licencované. Patří sem např. WiMAX, který využívá normy IEEE 802.16. Jde o standard pro bezdrátovou distribuci dat zaměřený na venkovní sítě. (Hucaby, 2014)
- **WWAN (Wireless Wide-Area Network)** – síť pokrývá velkou geografickou oblast. Patří sem např. mobilní sítě, ISP a další.

2.1.2 Módy bezdrátových zařízení

- **Přístupový bod** – neboli AP (Access Point) je zařízení, ke kterému se klienti připojují. Klienti spolu komunikují prostřednictvím AP, takže nemusí být spolu ve vzájemném rádiovém spojení. Komunikace mezi AP a klientem probíhá na jednom zvoleném. (Prasad, 2005).
- **Bezdrátový most** – plní funkci AP v pracovním režimu bridge mode. Propojení může mít podobu: PtP a PtMP. Bezdrátové mosty mohou pracovat ve čtyřech režimech (root, non-root, AP a repeater mode). Při propojení musí být jeden z mostů v režimu root mode. (Schön, 2015).
- **Repeater** – Používá se, když je potřeba pokrýt větší oblast a není možné použít kabelové rozvody. Zařízení přijme signál z AP a ten vysílá dál kolem sebe. (Hucaby, 2014). Nevýhodou této technologie je, že pokud zařízení přijme špatný signál a komunikace je ztrátová, tak zařízení připojena na repeater mají komunikaci také nekvalitní.
- **Klient** – je zařízení připojené k přístupovému bodu nebo mostu. V domácí síti je nejčastější topologii Wi-Fi router v modu přístupového bodu a mobily/notebooky jako klienti.

2.1.3 Bezdrátové topologie

Bezdrátová Wi-Fi síť může být vybudována různými způsoby dle potřeb uživatelů nebo podle požadovaných funkcí. Základním stavebním blokem Wi-Fi sítí je tzv. BSS (Basic Service Set), který je základním souborem služeb. V srdci každého BSS je bezdrátový přístupový bod (AP). (Hucaby, 2014). Daný AP pracuje v režimu infrastruktury, což znamená, že nabízí služby, které jsou nezbytné k připojení do bezdrátové sítě. Stanice komunikující v určité oblasti se říká BSA (Basic Service Area). Velikost BSA závisí na dosahu signálu jednotlivých členů BSS. (Lejtnar, 2012). AP slouží jako jediné kontaktní místo pro každé zařízení, které chce použít BSS. Inzeruje existenci BSS, takže zařízení ho mohou najít a připojit se k němu. Provádí to tak, že AP použijí unikátní BSS identifikátor (BSSID), který je založený na jeho vlastní MAC adrese. Kromě toho AP poskytuje logický textový řetězec SSID (Service Set Identifier), který slouží jako identifikace zařízení pro člověka. (Hucaby, 2014).

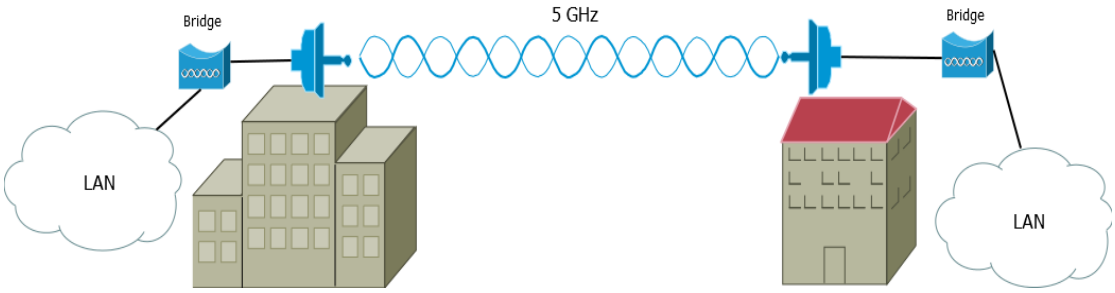


Obr. 2 BSS (Basic Service Set).
Zdroj: Převzato od Hucaby (2014).

Pokud je potřeba pokrýt větší oblast (nemocnice, univerzita, aj.), tak jeden AP nestačí. K pokrytí takové oblasti je potřeba několik AP. Problém nastane při přechodu do jiného sektoru v budově, kde se zařízení musí překonfigurovat a nastavit znovu pro nový AP. Tento problém řeší ESS (Extended Service Set). Různé BSS mají stejný SSID název, ale různé BSSID. (Hucaby, 2014). Klient, který přejde z jednoho AP na druhý, nemusí nic znovu konfigurovat, proběhne pouze změna BSSID. Pokud přenos proběhne bez větší ztráty dat, nazýváme tento přenos jako bezdrátový roaming.

Obecně se rozlišují dvě topologie Wi-Fi sítě na základě komunikace mezi členy BSS. První je na základě AP, přes kterého probíhá veškerá komunikace a je popsán výše. Druhý typ spojení se nazývá IBSS (Independent Basic Service Set). Ve světě je známý jako ad hoc. Principem je komunikace koncových zařízení přímo mezi sebou. Není tedy potřeba dostupnosti AP. Komunikaci tedy lze provést všude, kde jsou alespoň 2 počítače s Wi-Fi adaptéry. (Hucaby, 2014). Novinkou, která rozšiřuje ad hoc, je Wi-Fi direct. Opět není potřeba AP a přenos je mnohem rychlejší díky modulační technologii MIMO. Lze propojit libovolná zařízení a je prakticky nástupcem ad hoc. (TIEU, YE, 2014).

Při komunikaci mezi budovami nebo městy se používá topologie tzv. Outdoor Bridge. Spojení probíhá na dlouhé vzdálenosti. Zařízení mají povoleny větší vyzařovací výkon. Lze aplikovat spoje Point-to-Point nebo point-to-Multipoint. (Hucaby, 2014). Obr. 3 zobrazuje, jak by mohla vypadat topologie Outdoor Bridge.



Obr. 3 Topologie Outdoor Bridge.
Zdroj: Převzato od Hucaby (2014).

Mesh topologie se používá na pokrytí velké plochy. Není praktické mít kabeláž ke každému AP. Místo toho lze použít vícenásobné AP, které jsou nakonfigurovány v režimu mesh. AP mohou využívat i duální vysílání např. 2,4 GHz a 5 GHz. Každý mesh AP obvykle udržuje BSS na 2,4 GHz kanálu. V topologii mesh provozují AP dynamické routovací protokoly, které vyhledají nejlepší cestu v síti.

2.1.4 Šíření signálu

Síla signálu se uvádí v decibelech (dB), konkrétně v jednotkách dBi nebo dBm (kde 0 dBm = 1 mW). Vlivů, které ovlivňují šíření signálu, je celá škála. Drtivá většina z nich je negativních jako např. špatné počasí, pohlcování elektromagnetických vln a různé překážky (strom, budovy aj.). Při budování bezdrátové komunikace je důležité znát hodnoty efektivního izotropního vyzařovacího výkonu (EIRP, Equivalent Isotropically Radiated Power). Tyto hodnoty v Evropě spravuje mezinárodní organizace ETSI. (Švarc, 2016). EIRP se vypočítá podle vzorce:

$$\boldsymbol{EIRP = P_T - L_C + G_A}$$

kde P_T Výstupní výkon vysílače (dBm)
L_C Ztráta kabelu (dB)
G_A Zisk antény (dBi)

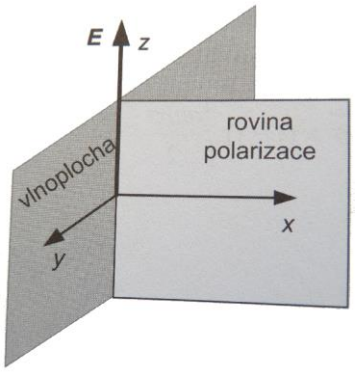
Indikátor síly přijatého signálu RSSI (Received Signal Strength Indication) je definovaná škála k určení úrovně signálu. Většinou se uvádí v dBm na stupnici od 0 do -100. (Švarc, 2016). Výrobci bezdrátových karet tyto hodnoty stanovují sami, což v praxi znamená, že různé karty výrobců mohou mít stejnou úroveň signálu, ale různé RSSI.

Poměr signálů a šumu SNR (Signal–to–Noise Ratio) vyjadřuje úroveň přijímaného signálu v porovnání s okolním šumem. Tuto hodnotu většina bezdrátových karet nedokáže zobrazovat, přestože může být při řešení problému důležitější než RSSI. (Švarc, 2013). Tento nedostatek lze vyřešit specializovaným zařízením jako např. AirCheck Wi-Fi Tester od společnosti FlukeNetworks2. Pokud bychom použili softwarové řešení, lze použít aplikaci Ekahau.

[2] http://www.fluketestery.cz/produkty/aircheck_wifi_tester.html

2.1.5 Polarizace

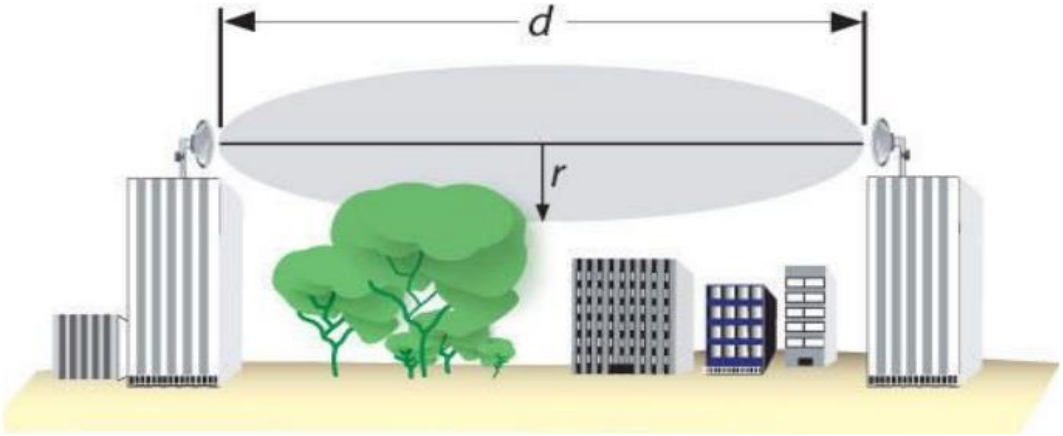
Při vysílání signálu do prostoru může anténa usměrnit signál do jedné ze dvou rovin (vertikální/horizontální). Pokud jednopolarizační vysílač má vertikální polarizací a přijímač horizontální pozici, tak v ideálním stavu je útlum nekonečný. (Pecháč, 2007) Polarizace antén se tedy musí shodovat. Aktuálně výrobci vyrábí dvoupolarizační antény, takže stanice proti sobě mohou být ve vertikálním i horizontálním stavu. (Kučera, 2015).



Obr. 4 Rovina polarizace.
Zdroj: Skipala, 2011.

2.1.6 Fresnelovy zóny

Dobře fungující spoj by neměl mít v přímé ani okolní spojnici žádné překážky. Této oblasti se říká Fresnelovy zóny. (Pecháč, 2007).



Obr. 5 Fresnelova zóna.
Zdroj: Novák, 2015.

Zachovat jen přímou viditelnost není pro účinné spojení dostačující. Zjednodušeně řečeno tvar podobný elipsoidu vymezuje oblast Fresnelovy zóny. V první Fresnelově zóně se přenáší 60 % energie mezi anténami. Je tedy nutné, aby v první

zóně nestála žádná překážka. Průměr Fresnelovy zóny v jejím nejširším místě (polovině) lze vypočítat dle vztahu: (Pecháč, 2007)

$$b_1 = \sqrt{\frac{d_1 d_2 \lambda}{d_1 + d_2}}$$

Na Internetu najdeme nespočet kalkulátorů, jež vypočítají Fresnelovy zóny. Většinou v praxi postačí tabulkové hodnoty.[3] N-tou Fresnelovu zónu v dané vzdálenosti lze vypočítat ze vztahu:

$$b_n = \sqrt{\frac{d_1 d_2 n \lambda}{d_1 + d_2}}$$

2.1.7 Výkonová bilance spoje

Správný výkon je nezbytným předpokladem pro dobře fungující spoj. Příliš slabý nebo přepálený signál způsobuje nejen omezení přenosové rychlosti, ale i kvality spoje. Pro bezdrátové spoje platí následující ideální přenosová rovnice (vyjádřeno v dB). (Skipala, 2011):

$$\mathbf{P_p = P_V + G_V + G_P - FSL(d) - L}$$

kde
- P_P je přijatý výkon (dBm), $P_{dBm} = 10\log\frac{P_w}{10^{-3}}$
- P_V výkon na vstupu vysílací antény
- G_V, G_P zisky antén (dB), $G_{dB} = 10\log G$
- FSL(d) ztráty volným prostorem (dB, $FSL(d)_{dB} = 10\log[(\frac{4\pi d}{\lambda})^2]$
- L ztráty šířením (dB) v daném prostředí, $L_{db} = 10\log L$

Podle Skipaly by pro frekvenci 5 GHz vypadala ztráta volným prostorem následovně:

[3] http://wiki.pvfree.net/index.php/Fresnelova_z%C3%B3na

Tab. 1 Ztráta volným prostorem v závislosti na vzdálenosti.

Vzdálenost	Útlum volným prostorem (FSL) [dB]	Síla signálu při použití xdBi antén (2dB ztráta na kabelu)[dBm]			
		10dBi	19dBi	24dBi	29dBi
50 m	80,98	-45,98	-36,98	-31,98	-26,98
100 m	87,00	-52,00	-43,00	-38,00	-33,00
200 m	93,02	-58,02	-49,02	-44,02	-39,02
300 m	96,54	-61,54	-52,54	-47,54	-42,54
500 m	100,98	-65,98	-56,98	-51,98	-46,98
1000 m	107,00	-72,00	-63,00	-58,00	-53,00
1500 m	110,52	-75,52	-66,52	-61,52	-56,52
2000 m	113,02	-78,02	-69,02	-64,02	-59,02
3000 m	116,54	-81,54	-72,54	-67,54	-62,54
4000 m	119,04	-84,04	-75,04	-70,04	-65,04
5000 m	120,98	-85,98	-76,98	-71,98	-66,98
7000 m	123,90	-88,90	-79,90	-74,90	-69,90
10 000 m	127,00	-92,00	-83,00	-78,00	-73,00
13 000 m	129,28	-94,28	-85,28	-80,28	-75,28
15 000 m	130,52	-95,52	-86,52	-86,52	-76,52
20 000m	133,02	-98,02	-89,02	-84,02	-79,02

Zdroj: Skipala, 2011.

2.2 Přístupy k médiu

2.2.1 CSMA

Jedná se o metodu náhodného přístupu k médiu, kde každá stanice před vlastním vysíláním kontroluje přítomnost signálu v médiu, zda není sdílené médium již využívané k přenosu jinou stanicí. Může nastat situace, kdy během krátkého intervalu chtějí dvě stanice po sobě zahájit vysílání. Jestliže je tento interval kratší než doba šíření signálu po médiu, druhá stanice pak nemůže v daném okamžiku zaznamenat, že médium je již obsazené a začne také vysílat, čímž způsobí kolizi. (Kučera, 2015).

V CSMA je nemožné zcela zabránit kolizím, avšak existují způsoby, jak se s nimi vypořádat:

1. **Metoda CSMA/CA**

   Uzel naslouchá aktivitě sítě a hledá nosný signál, který indikuje aktivitu na síti. Pokud uzel neslyší nosný signál a chce něco přenést, pošle RTS signál na síť. Jestliže se očekává přenos do určitého uzlu, čeká vysílací stanice na CTS signál. Pokud CTS signál není přijat, vysílací stanice předpokládá kolizi a celou akci v náhodných intervalech opakuje. Přijatý signál CTS znamená zahájení vysílá-

ní paketů na určitý uzel. Jedná-li se o zprávy, nečeká se na CTS signál. (Ručka, 2007).

2. **Metoda CSMA/CD**

   Nejrozšířenějším představitelem metody CSMA/CD je klasický Ethernet. V průběhu odesílání rámce si tato stanice sama zjišťuje, zda její signál nekoliduje se signálem jiné stanice, která začala vysílat ve stejné době. Tato vlastnost se nazývá detekce kolizí (Collision Detection – odtud zkratka CD). (Kučera, 2015).

Pro sítě WLAN jsou definovány dva typy koordinačních funkcí, distribuované a centralizované:

- **Distribuovaná koordinační funkce** (DCF – Distributed Coordination Function) je specifikována v standardu 802.11 a lze ji využít v BSS, ESS i IBSS. V tomto případě se využívá náhodná přístupová metoda a stanice soutěží o přístup k médiu. (Kučera, 2015).
- **Centralizovaná koordinační funkce** (Point Coordiantion Fuction) představuje přístupovou metodu bez soutěžení. U této přístupové metody se přístupový bod pravidelně dotazuje všech stanic a zjišťuje, zda nemají data k vysílání. (Kučera, 2015).

2.2.2 TDMA

TDMA (Time Division Multiple Access) je přístupová metoda k médiu pro sdílené sítě. V TDMA uživatelé využívají stejný rádiový přenosový kanál. Tento kanál je ale rozdělen v čase na jednotlivé časové díly (timesloty), jejichž určitý počet formuje TDMA rámec opakující se pravidelně v čase. Z důvodu sdílení frekvenčního kanálu více uživateli není telefonní hovor nebo přenos dat souvislý, daný uživatel má kanál přidělen jen po dobu trvání přiděleného časového dílu. (Kučera, 2015).

2.3 Bezdrátové sítě standardu IEEE 802.11

IEEE 802.11 je rozsáhlý průmyslový standard, jehož cílem bylo ujednotit protokoly pro bezdrátovou komunikaci a nabídnout celkovou interoperabilitu pro produkty různých výrobců (Carroll, 2008). Organizace IEEE přišla se standardem 802.11, který má sjednotit komunikaci a ustoupit od proprietárních protokolů různých výrobců. Pro standard IEEE 802.11 se časem vžil název Wi-Fi (Wireless Fidelity). První verze byla vydána v roce 1997. Organizace Wi-Fi Alliance (dříve WECA) je zodpovědná za certifikování produktů splňujících tyto standardy. Nejznámější standardy jsou srovnány v Tab. 2 .

Tab. 2 Přehled používaných standardů IEEE 802.11.

	802.11a	802.11b	802.11g	802.11n	802.11ac
Rok vydání	1999	1999	2003	2009	2013
Pásmo	5 GHz	2,4 GHz	2,4 GHz	2,4 a 5GHz	5 GHz
Šířka kanálu	20 MHz	22 MHz	20 MHz	20, 40 MHz	20, 40, 80, 160 MHz
Modulace	OFDM	DSSS	DSSS, OFDM	OFDM	OFDM
Modulační schémata	BPSK, QPSK, 16-QAM, 64 – QAM	DBPSK, DQPSK	DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64 – QAM	BPSK, QPSK, 16-QAM, 64 – QAM 256 - QAM
MIMO	-	-	-	až 4	až 8
Max. rychlost	54 Mbps	11 Mbps	54 Mbps	600 Mbps	6930 Mbps

Zdroj: Převzato od Konečný (2015).

2.3.1 IEEE 802.11

Jedná se o první standard. Pracuje na frekvenci 2,4 GHz a využívá modulace FHSS (Frequency-Hopping Spread Spectrum) a DSSS (Direct Sequence Spread Spectrum). Rychlost je pouze 1 až 2 Mbps. Tento standard je historický a v roce 1999 na něj navázal standard IEEE 802.11b (Caroll, 2008).

2.3.2 IEEE 802.11a

Tento standard byl vydán v roce 1999 a jeho hlavním přínosem bylo rozšíření Wi-Fi sítě do frekvenčního pásma 5 GHz. Rychlost byla až 54 Mbps s šířkou pásma 20 MHz. Díky modulaci OFDM (Orthogonal Frequency Division Multiplexing) a rozšířením modulačních schémat o 16-QAM, 64-QAM dosahuje tento protokol mnohonásobně vyšší rychlosti než původní standard 802.11. Výhodou je také využití pásma 5 GHz, který disponuje větším množstvím nepřekrývajících se kanálů. (Caroll, 2008).

V tomto pásmu lze použít i větší vyzařovací výkon, takže lze uskutečnit bezdrátovou komunikaci na větší vzdálenosti. Od povolení pásma 5 GHz ze strany ČTU (Český telekomunikační úřad) je Wi-Fi aktuálně nepoužívanější způsob připojení k Internetu v České republice. Nízké pořizovací náklady a jednoduchá instalace zvýšil mnohonásobný nárůst nových poskytovatelů, proto dnes najít ve městech nepřekrývající se kanál je téměř nemožné.

2.3.3 IEEE 802.11b

Vznik toho standardu se datuje k roku 1999 a navazuje na původní standard 802.11. Jeho maximální rychlost je až 11 Mbps a pracuje pouze v pásmu 2,4 GHz. Využívá modulaci DSSS pro šíření spektra namísto lepšího OFDM. Neméně dokonalé jsou i jeho modulační techniky (DBPSK a DQPSK). Šířka pásma je u standardu 802.11b 22 MHz, takže existují pouze 3 nepřekrývající se kanály (1, 6 a 11). Rychlost ovšem v době nasazení byla dostačující, kdy kabelové sítě dosahovaly rychlosti 10 Mbps. (Carroll, 2008).

2.3.4 IEEE 802.11g

Návrh byl vydán v roce 2003. Vznikl jako reakce na to, že v některých zemích bylo 5 GHz pásmo licencováno a standard 802.11b neměl dostatečnou přenosovou kapacitu. (Schön, 2015). Nově vzniklý standard dosahoval rychlosti až 54 Mbps. Pracoval v pásmu 2,4 GHz s šířkou pásma 22 MHz. Používá se modulace OFDM namísto staré DSSS. Vlivem zpětné kompatibility se 802.11g na nižších modulačních rychlostech chová stejně jako 802.11b. Klient připojený v normě 802.11b na AP v normě 802.11g znamená výkonnostní překážku. Způsobí degradaci výkonu klientů připojených v normě 802.11g na témže AP. Důvodem je, že AP přepne na modulaci DSSS a přejde na nižší modulační rychlost, aby mohli komunikovat i klienti s normou 802.11b, kteří normu 802.11g s modulací OFDM nepodporují. Proto většinou výrobci dávají uživatelům AP možnost nastavit: only 802.11g nebo kombinaci 802.11 b/g.

2.3.5 IEEE 802.11n

Aktuálně nepoužívanější standard, který vznikl v roce 2009. Tato norma jako první dokáže pracovat jak v pásmu 2,4 GHz, tak i 5 GHz. Díky tomu jsou tyto sítě kompatibilní se staršími normami a/b/g. (Carroll, 2008). IEEE 802.11 využívá modulace OFDM a modulačního schématu BPSK, QPSK, 16-QAM, 64-QAM. Šířka pásma může být 20 MHz nebo 40 MHz. Dvojnásobná šířka pásma má za následek zmenšení nepřekrývajících se kanálů. Nová technologie MIMO (Multiple-Input Multiple-Output) zvyšuje počet antén a lze tak provádět více simultánních přenosů dat. (Carroll, 2008). V souvislosti s tím je nutné zmínit pojem spartial stream, který představuje dílčí tok dat, přenášený některou z antén. Celkový počet dostupných spartial streamů je pak roven menšímu z počtu antén na přijímací či vysílací straně. Maximální potencionální rychlost je až 600 Mbps. (Konečný, 2015).

2.3.6 IEEE 802.11ac

Nejnovější standard, který vznikl v roce 2013. Rozšiřuje možnosti normy IEEE 802.11n. Tento standard ovšem už nepracuje ve frekvenčním pásmu 2,4 GHz a pracuje pouze pásmu v 5 GHz. Navýšení rychlosti se odvíjí od nastavené konfigurace. Při nastavení šířky pásma 80 MHz je rychlost až 1300 Mbps (MIMO 3x3).

Mnoho výrobců Wi-Fi poskytuje zařízení, která pracují v tzv. dvoupásmových přístupových bodech (dual-band). Tato zařízení operují v pásmu 2,4 GHz i 5 GHz

zároveň. Pásma 2,4 GHz využívá normu 802.11n a pásma 5 GHz normu 802.11ac. (Konečný, 2015).

Při použití šířky pásma 80 MHz se ještě více zaruší frekvenční pásmo a najít volný nepřekrývající se kanál bude ještě složitější než doposud.

2.3.7 IEEE 802.11ad

Standard IEEE 802.11ad je často přezdívaný jako WiGig. Měl by pracovat v pásmech 2,4 GHz, 5 GHz a nově i 60 GHz. Je určený pro přenos v rámci jedné místnosti s maximální teoretickou rychlostí až 7 Gbps. Zařízení s podporou této normy byla slibována už v roce 2014 a 2015. Článek Technet (2017) testoval první dostupný produkt v České republice od společnosti TP-Link. Během testů se dosáhlo 800 Mbps, ale při menší překážce je rychlost okamžitě snížena. Pokud mezi šířícím signálem a klientem stojí zeď, klient je odpojen. Velký útlum způsobuje i lidská překážka. Cena startuje na ceně 8059 Kč.

2.3.8 Protokol Nstreme

Tento proprietární protokol vytvořila firma MikroTik. Nstreme se využívá pro bezdrátové přenosy na vylepšení spojů PtP a spojů PtMP. Protokol lze využívat pouze pro spoje na platformě MikroTik a není tedy kompatibilní se zařízeními jiných výrobců.

Nstreme standardně využívá přístupovou metodu polling. Přístupný bod se postupně dotazuje klientů, zda mají nějaká data k vysílání. Tím odpadá problém skrytého uzlu a taktéž zařízení nemusí detekovat, zda je medium obsazené. (Skipala, 2011). Tímto mechanismem se zvedne odezva, ale jiter zůstane malý. (Vágner, 2013). Nstreme obsahuje ještě vylepšení, které upravuje velikosti přenášených rámců s funkcí best-fit. Ten pracuje tak, že čeká, až se naplní rámec a poté jej odešle. (Vágner, 2011). RouterOS umožňuje vypnout CSMA, což má za následek úplnou změnu z CSMA/CA na polling. Vypnutím CSMA se karta zbavuje povinnosti poslouchat médium před vysíláním, což může silně negativně ovlivnit soužití s jinými sítěmi na stejné frekvenci. (Skipala, 2011).

2.3.9 Protokol NV2

Nejnovějším protokolem z rodiny MikroTik je NV2 (Nstreme version 2). Tento protokol rozšiřuje původní Nstream a přidává podporu časového multiplexu TDMA. (Vágner, 2011). NV2 dělí čas do pevných úseků, které jsou dynamicky přidělovány pro downlink (od AP ke klientovi) a uplink (od klienta k AP). Uplink je pak dále rozdělen mezi klienty podle toho, jakou potřebují šířku pásma. Na začátku periody přístupový bod rozešle klientům informaci, kdy mají vysílat a jaký čas jim je k tomu přidělen. (Vágner, 2013)

Pro nově připojené klienty, kteří použili protokol NV2, je vyhrazen tzv. nespecifikovaný čas. Tento čas pak používá klient na registraci k přístupovému bodu. Ten pak odhaduje zpoždění šíření mezi nimi a začne jej zabudovávat do TDMA systému. TDMA řeší problém skrytého uzlu a zlepšuje využití přenosového kanálu, což

má za důsledek zlepšení propustnosti a latence, a to zejména v sítích Point-to-ManyPoint. NV2 je určený pro karty Atheros 802.11. Maximální limit u protokolu NV2 je 511 klientů. (MikroTik, 2015).

Protokol využívá proprietární řešení QoS pomocí variabilního počtu prioritních front. Přenos probíhá na základě pravidel 802.1D-2004. V praxi to znamená, že nejdřív jsou vyslána data s vyšší prioritou a teprve potom až další. QoS je řízené AP a klienti se přizpůsobují zásadám AP. V továrním nastavení je nastaven Nv2-qos=default a v tomto režimu je odchozí provoz kontrolován vestavěným algoritmem, který vybírá frontu na základě typu a velikosti paketů. Druhou možností je Nv2-qos = frame priority, kde je fronta klasifikována na základě pole s prioritou rámce. Fronta musí být nastavena explicitně podle firewall pravidla nebo implicitně přes ingress priority z forwarding procesu. Na základě Nv2-queue-count je vytvořen počet front. Maximální počet je 8. Minimální (default) jsou 2 fronty. Tab. 3 definuje mapování paketů do fronty na základě priority.

Tab. 3 Queue-count u protokolu NV2.

nv2-queue=2	**nv2-queue=4**	**nv2-queue=8**
priority 0,1,2,3 -> queue 0	priority 0,1 -> queue 0	priority 0 -> queue 0
priority 4,5,6,7 -> queue 1	priority 2,3 -> queue 1	priority 1 -> queue 1
	priority 4,5 -> queue 2	priority 2 -> queue 2
	priority 6,7 -> queue 3	priority 3 -> queue 3
		priority 4 -> queue 4
		priority 5 -> queue 5
		priority 6 -> queue 6
		priority 7 -> queue 7

Zdroj: Mum, 2013.

Dalším rozdílem mezi běžnými bezdrátovým QoS je, že priorita 1 a 2 je menší než 0. Viz Tab. 4 .

Tab. 4 Priorita fronty u NV2.

	Use Priority	Acronym	Traffic Type
Lowest	1	BK	Background
	2	./.	Spare
	0 (default)	BE	Best Effort
	3	EE	Excellent Effort
	4	CL	Controlled Load
	5	VI	Video
	6	VO	Voice
Highest	7	NC	Network Control

Zdroj: Mum, 2013.

2.3.10 Protokol airMAX

Proprietární protokol airMAX je vytvořený firmou Ubiquiti pro své platformy Wi-Fi produktů. Využívá metodu TDMA, takže ke každému připojenému klientovi je přiřazen časový úsek, respektive můžeme vzít kapacitu přístupového bodu a rozdělit ji pomocí časových úseků spravedlivě mezi všechny připojené stanice. Výrobce udává, že protokol airMAX zlepší parametry jakéhokoliv spoje, když bude tato funkce aktivována. Především zvětší přenosovou rychlost a odolnost vůči rušení. (Vágner, 2013).

2.4 Legislativa

Dodržování právních norem je součástí každého bezdrátového provozovatele. V České republice určuje pravidla organizace ČTU (Český telekomunikační úřad), která nás zastupuje na mezinárodních aktivitách ve věcech elektronických komunikací (ITU, ETSI aj.). ČTU v rámci své působnosti dané zákonem č. 127/2005 Sb., může udělovat pokuty při nedodržení platných norem. Zástupci ČTU celkem pravidelně navštěvují semináře pořádané pro ISP, kde informují o změnách legislativy a dalších novinkách. Největší důraz kladou na zapnutí funkce DFS (Dynamic Frequency Seletion), která skenuje meteoradary a zabrání vstupu do zakázaného kmitočtu. Mnoho výrobců nechává provozovatelích, zda tuto funkci zapnou či nikoliv. Tlak úřadů nevydržela firma MikroTik a od nového firmwaru 6.37.1 je tato funkce zapnuta bez možnosti změny, což má velice negativní vliv pro provozovatele. Scan DFS probíhá i 10 minut a často si změní vysílací kmitočet. To je pro drtivou většinu poskytovatelů nepřijatelné a používají starší firmware. Novinkou ČTU je

vytvoření „webu hříšníků“[4], kde nalezneme seznam zařízení, které ruší meteoradary. Dle slov ČTU mají provozovatelé několik dní na odstranění rušících elementů než budou pokutování. Podmínky provozu v pásmech 2,4 GHz - 66 GHz jsou definovány všeobecným oprávněním č. VO-R/12/06.2010-9. (viz Tab. 5).

Tab. 5 Všeobecné oprávnění V0-R/12/06.2010-9.

Ozn.	Kmitočtové pásmo	Vyzářený výkon	Maximální spektrální hustota e.i.r.p.	Další podmínky
A	2400,0-2483,5 MHz	100 mW e.i.r.p	10 mW/1 MHz	systémy s technikou DSSS nebo OFDM
			100 mW/100 kHz	systémy s technikou FHSS
B	5150-5250 MHz	200 mW střední e.i.r.p	10 mW/1 MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz).	pouze pro použití uvnitř budovy
C	5250-5350 MHz	200 mW střední e.i.r.p	10 mW/1 MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz).	pouze pro použití uvnitř budovy
D	5470-5725 MHz	1 W střední e.i.r.p.	50 mW/MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz).	-
E	17.1-17.3 GHz	100 mW střední e.i.r.p	-	-
F	57-66 GHz	40 dBm střední e.i.r.p	13 dBm/MHz (střední spektrální hustota)	stálé venkovní instalace jsou vyloučeny

Zdroj: ČTU, 2010.

[4] http://radar4ctu.bourky.cz/Ruseni.html

3 QoS

Mechanismus (technologie) QoS se používá tam, kde šířka pásma nestačí. Zajistí, že data budou roztříděna do kategorií a podle priority přenosu doručena v potřebné kvalitě. QoS lze aplikovat na různé vrstvy ISO/OSI, takže se jedná o rozsáhlý mechanismus. (Fraj, 2014). Většina zařízení dokáže pracovat na modelu ISO/OSI do 4. vrstvy a nejčastěji probíhá klasifikace provozu na síťové vrstvě. Vědecký článek „QoS and robustness of priority-based MAC protocols for the in-car power line communication" (Gehrsitz, Kellerer, 2016) aplikuje mechanismus QoS do automobilu, který je založen na MAC protokolu. Je tedy nemožné popsat v této práci veškerou problematiku tohoto mechanismu, který se používá nejen v klasických počítačových sítích. Kvalita sítě je hodnocena podle čtyř základních metrik, které charakterizují data přenášená v dané síti: (Cioara, Valentino, 2012).

- **Jednosměrné zpoždění (Delay)** – Zpoždění (latence), je doba mezi vysláním paketu od zdroje a jeho doručením k cílovému zařízení.
- **Časová nestabilita v síti (Jitter)** – Jitter je rozdíl v intervalech mezi přijímanými pakety. Často je způsobený zatížením jednotlivých síťových prvků nebo změnami topologie směrování sítí. To může mít negativní vliv na kvalitu přenosů v reálném čase. (Švec, 2011).
- **Ztrátovost paketů (Packet loss)** – Ztrátovost paketů uvádí relativní míru nedoručených paketů a celkové množství odeslaných paketů. Paket může být ztracen/zahozen při průchodu sítí. Ztrátovost paketů má významný vliv na kvalitu přenosu v reálném čase. (Kalina, 2013).
- **Dostupná šířka pásma (Bandwidth)** – V počítačových sítích se termín Bandwidth udává jako propustnost sítě, tedy množství dat, které určité médium dokáže přenést za jednotku času. Jednotkou propustnosti se udává bitrate.

Zajištění vysoké kvality služeb lze provést třemi způsoby. Prvním způsobem je naddimenzování (overprovision) a jedná se o nejjednodušší způsob. Není potřeba odborných znalostí, ale zvýšení prostupnosti ze 100 Mbps na 1 Gbps je ve WAN sítích často obrovsky nákladné. Druhou metodou je upřednostňovat provoz na základě priority. Takže při kapacitě 100 Mbps linky májí realtime datové toky přednost, ovšem pokud žádné nejsou, tak ostatní aplikace mohou využívat kompletně celou 100 Mbps linku. Posledním způsobem je vyhrazením zdrojů, nejčastěji šířky pásma. (Kalina, 2013). Tento způsob není příliš efektivní, protože pokud by v síti neprobíhal realtime provoz, ostatní aplikace využijí pouze 80 Mbps linku.

Jedním z problémů mechanismu QoS je negarantování šířky pásma. Pokud poskytovatel připojení nabízí agregovanou linku, nelze odhadnou maximální limit a rozdělování datových toků dle priorit je v tomto případě irelevantní. Příkladem může být, když určíme prioritu provozu pro IPTV 10 Mbps. Klesne-li konektivita od poskytovatele pod 10 Mbps, tak televize je nestabilní a navíc eliminujeme ostatní provoz.

3.1 Metody řízení provozu

QoS lze implementovat několika způsoby. Množina specifikací RFC 1812 (IETF, 1995), RFC 1633 (IETF, 1994), RFC 2474 (IETF, 1998b), RFC 2475 (IETF, 1998c) standardizovala trojici QoS modelů (Best-Effort, Integrated services a Differentiated services). (Zach, 2015).

3.1.1 Best-Effort

Jedná se o základní způsob zajištění kvality služeb. Tento model nemá aplikované žádné mechanismy QoS a provoz je obsluhován na bázi FCFS (First-come, first-served), kde dochází ke snaze doručit paket co nejrychleji k danému cíli. V okamžiku zaplnění šířky pásma se nové pakety začnou zahazovat (tail-drop). (Braun a další, 2008). Nepředvídatelnost takových sítí je důvodem, proč metoda Best-Effort není vhodná pro aplikace náročné na kvalitu sítě. (Cioara, Valentino, 2012). Model je tedy vhodné aplikovat pouze v sítích při dostatečné šířce pásma.

3.1.2 Integrated services model

Tato metoda je založena na principu dynamické alokace zdrojů přes všechny síťové prvky v cestě. Rezervaci pásma zajišťuje protokol RSVP (Resource Reservation Protocol), který je popsán v RFC 2205 a pracuje na čtvrté vrstvě ISO/OSI. Při přenosu dat se koncový uzel pokusí o vyhrazení šířky pásma, kterou potřebuje. (Cioara, Valentinon, 2012). Tento model jako jediný disponuje garancí zdrojů a jejich alokací pro každý tok zvlášť, takže po celou dobu přenosu je potřebné pásmo vyhrazeno pouze koncovému uzlu. V případě přílišného množství rezervací může dojít k tomu, že je kapacita sítě vyčerpána a protokol RSVP nedokáže alokovat potřebnou šířku pásma a žádný přenos se neuskuteční. (Konečný, 2015). Další nevýhodou je, že po cestě ke koncovému uzlu musí všechny síťové prvky podporovat protokol RSVP. (Kalina, 2013). Podle Kurose a Ross (2013) se integrované služby rozdělují na tři způsoby provozu:

- Best Effort service
- Controlled load service
- Guaranteed service

3.1.3 Differentiated services model

Differentiated services model je v současnosti nejrozšířenější QoS metoda v počítačových sítích. Lze ji považovat za následníka Integrated services modelu. Nepoužívá signalizační protokol, ale je založený na PHB (Per-Hop-Behaviour), kdy je každý provoz na uvedeném prvku označen (identifikován) a klasifikován do tříd. (Zach, 2015). Třídy mají určitou prioritu a na základě toho lze zajistit každé třídě různé požadavky na QoS. Tento model negarantuje rezervaci pásma, ale jeho nespornou výhodou je nenáročnost na systémové zdroje.

Proces modelu DiffServ je zpravidla složen z těchto částí: (Cisco Systems, 2005).

1. **Classification and Marking** – v této části se tvoří identifikace a klasifikace provozu. Paket lze zařadit do tříd pomocí údajů v záhlaví paketů označovaných jako Marking (značkování). Lze použít pole DSCP (Differentiated Services CodePoint), které se nachází v pozici TOS pro IPv4 respektive Traffic Class pro IPv6. (RFC 2474). Pole TOS v hlavičce IP paketu má 8 bitu. Klasifikace je možná také pomocí IP adres, transportního protokolu či signatur aplikačních dat (tzv. Multifield Identifier – MF). (Zach, 2015).
2. **Policing** – Tento mechanismus měří množství příchozího provozu a kontroluje, zda nepřesahuje povolenou horní mez. Provoz nad rámec limitů rychlosti je zahozen nebo přeznačkován na nižší prioritu. (Zach, 2015).
3. **Queuning and Scheduling** – Fáze Queuing (zařazování do front) a Scheduling (obsluha front). Při nedosažení maximální šířky pásma není aktivován mechanismus QoS. Až dojde k zahlcení linky, je QoS v aktivním stavu a pakety jsou odkládané do front, dle toho, jak jsou klasifikované. Délka každé fronty je omezena počtem paketů nebo bytu. Když dojde k úplnému zaplnění fronty, nový paket musí být zahozen (tail-drop). (Braun a další, 2008). U třídy multimediálních dat není vhodné zahazovat pakety a tento problém zajišťuje Scheduling (obsluha front). Scheduling je pověřen staráním se o to, jak bude s paketem zacházeno, když na vstupní rozhraní přichází data rychleji než je výstupní rozhraní schopné zpracovat. (Zach, 2015). Algoritmů, které definují, jakým způsobem jsou fronty obsluhovány při zahlcení, je celá řada. Základní mechanismy popisuje Koton (2014) a patří sem (FIFO, PQ, RRQ, WRRQ, WFQ, CBWFQ a LLQ). Ovšem někteří výrobci mají dokonce vlastní proprietární mechanismy, tudíž jejich struktura je nepublikována.
4. **Link-specific tools** – Patří sem metoda Shaping, která na rozdíl od Policingu, primárně nezahazuje pakety, ale zařazuje je do fronty.

4 QoS v bezdrátových sítích

Přenos na bezdrátovém mediu je náchylnější na chybovost způsobenou rušením, útlumem, šumem nebo dalším vnějším faktorem než klasický drátový spoj. Z důvodu zajištění kvalitnějšího přenosu u multimediálních dat vznikl standard 802.11e, který vylepšuje vrstvu MAC (Media Access Control) a rozšiřuje standard o podporu QoS. Sítě Wi-Fi pracují na principu vícenásobného přístupu, a proto je komunikace řízena metodou CSMA (u některých proprietárních standardů TDMA). V sítích 802.11 lze zvolit dvě funkce pro koordinaci přístupu k médiu - distribuovanou DCF nebo centralizovanou PCF, která se dnes prakticky nepoužívá. (Koton, 2014).

4.1 DCF

Distributed Coordination Function (DCF) doplňuje metodu CSMA/CA, která je běžně používaná při přenosu bezdrátových rámců. DCF zajišťuje službu best-effort bez podpory požadavku na QoS. Klient před vysíláním naslouchá, zda nevysílá jiný klient. Jako obrana proti kolizím se používá vkládání mezery mezi rámce IFS (InterFrameSpace) nebo odklad vysílání (backoff). (Menšík, 2011). Velikost mezer mezi rámci je rozdělena do 3 kategorií:

- **SIFS** (Short Interframe Space) – je nejkratší a zajišťuje nejpravděpodobnější přístup k médiu.
- **PIFS** (Point Coordination Function Interframe Space) – je středně dlouhá a používá se u PCF.
- **DIFS** (Distributed Coordination Function Interframe Space) – je nejdelší a používá se u DCF.

Stanice komunikující v síti DCF čeká minimálně DIFS interval, který určuje čas povinného čekání pro zjištění volného vysílacího kanálu, než začne stanice vysílat. Pokud v okamžiku začne vysílat nějaká jiná stanice, vysílání je odloženo. Interval odkladu je volen náhodně od 0 do velikosti CW (Contention Window). I přesto může dojít ke kolizi a to v případě, kdy se o vysílací kanál uchází více klientů. Velikost CW se v případě kolize zdvojnásobí (exponential backoof). Když interval odkladu uplyne a medium je volné, stanice začne vysílat. (Menšík, 2011). Podle Kotona je hodnota CW_{max} až 1023. (viz Tab. 6).

Tab. 6 Velikost mezirámcových mezer Wi-Fi sítí.

Technologie	SIFS [µs]	PIFS [µs]	DIFS [µs]	slot time [µs]	CW_{min} [µs]	CW_{max} [µs]
802.11a	16	25	34	9	15	1023
802.11b	10	30	50	20	31	1023
802.11g	10	30	50	20	15	1023
802.11n (2,4 GHz)	10	19/30	28/50	9/20	-	-
802.11n (5 GHz)	16	25	34	9	-	-
802.11ac	16	25	34	9	-	-

Zdroj: Koton, 2014.

4.2 PCF

Mechanismus PCF (Point Coordiation Function) je vymezen pro synchronní datové přenosy. Jedná se o volitelný mechanismus přístupu a nelze používat v ad-hoc sítích. (Menšík, 2011). AP vysílá periodicky beacon rámec, který vlastní informaci o síti (specifické parametry pro identifikaci a management) a mezi přenášením těchto rámců má dvě možnosti pro vysílání dat. První je *contentio-free*, která umožnuje vysílání bez ohledu na ostatní stanice. Pokud mám prioritní data a zažádám si právo vysílat, tak mohu vysílat. Druhá možnost je *contention,* což je standardní vysílání, kdy stanice začne vysílat, až jí jako první při čekání vyprší čas na volné médium. (Sliž, 2008). Stanice s prioritou vysílání využívá interval PIFS (PCF IFS), který je delší než SIFS a kratší než DIFS.

4.3 EDCF

EDCF (Enhanced Distribution Coordiantion Function) je rozšíření mechanismu DCF. Zajišťuje rezervování šířky pásma na základě kategorie provozu (CA – Category Access. Gachogu (2013) definuje čtyři kategorie přístupu a jsou odvozeny od DFC.

AC_VO (Voice)	$CW_{min} = (aCW_{min}+1)/4-1$	$CW_{max} = (aCW_{min}+1)/2-1$
AC_VI (Video)	$CW_{min} = (aCW_{min}+1)/2-1$	$CW_{max} = aCW_{min}$
AC_BE (Best Effort)	$CW_{min} = aCW_{min}$	$CW_{max} = aCW_{max}$
AC_BK (Background)	$CW_{min} = aCW_{min}$	$CW_{max} = aCW_{max}$

Výchozí hodnoty EDCA mechanismu pro standardy 802.11g/a/n jsou definovány jako:

Voice Queue	$CW_{min} = 3$	$CW_{max} = 7$
Video Queue	$CW_{min} = 7$	$CW_{max} = 15$
Best Effort Queue	$CW_{min} = 15$	$CW_{max} = 1023$
Background Queue	$CW_{min} = 15$	$CW_{max} = 1023$

Celkově má mechanismus až osm prioritních úrovní, které jsou kompatibilní se standardem 802.11D, který je používán v lokálních pevných sítích. (viz Tab. 7). Data s nejvyšší prioritou mají nejnižší čas AIFS (Arbitration Interframe Space). Tímto se docílí toho, že data s nejvyšší prioritou jsou upřednostněna před daty s nižší prioritou. Pokud nastane situace, že vysílají dvě stanice se stejnou prioritou, tak je před zahájením vysílání zařazen náhodný interval mezi nulou a EDCF. (Gachogu, 2013).

Tab. 7 Priority dle 802.11D na kategorii přístupu (AC).

Priorita dle 802.1D	Využití dle 802.11D	Kategorie	Využití dle 802.11e
1	přenos na pozadí	AC_BK (0)	přenos na pozadí
2	nedefinované	AC_BK (0)	přenos na pozadí
0	best-effort (výcho-	AC_BK (0)	best-effort
3	zí)	AC_BG (1)	best-effort
4	excellent-effort	AC_VI (2)	video
5	řízená zátěž	AC_VI (2)	video
6	video	AC_VO (3)	hlas
7	hlas	AC_VO (3)	hlas
	správa sítě		

Zdroj: převzato od Koton (2014).

4.4 HCCA

HCCA (HCF Controlled Channel Access) je rozšířením PCF. AP se zeptá v době contention free stanice, jestli vlastní nějaká prioritní data k vysílání. V případné kladné odpovědi jí přiřadí určitou dobu vysílaní a dobu trvání přenosu. (Sliž, 2008). Podle Zelinky (2009) se jedná o nejpokročilejší a nejkomplexnější koordinační funkci.

4.5 WMM

Z důvodu složitosti normy 802.11e a delší doby jeho standardizace byl vytvořen model WMM (Wireless MultiMedia), dříve WME (Wireless Multimedia Extensions). Funkce se zabývá QoS v sítích Wi-Fi a nahrazuje DCF v sítích CSMA/CA. Certifikovaná zařízení musí podporovat metodu řízení přístupu k médiu EDCA, zatímco podpora HCCA a ostatní funkcionality IEEE jsou volitelná. (Švarc, 2016).

WMM nedefinuje šířku pásma pro provoz, ale priorizuje multimediální data (VoIP, IPTV) nad ostatní provoz, který není náročný na ztrátovost či zpoždění. Pro plnou funkcionalitu WMM je nutné, aby byla funkce podporovaná a zapnutá na straně AP i na straně klienta. V rámci EDCA funkcionality jsou definované čtyři třídy provozu AC, které jsou ještě rozděleny na 7 levelů priorit. (viz Tab. 8).

Tab. 8 Priorita u modelu WMM.

Priority Level	Traffic Type
0 (lowest)	Best Effort
1	Background
2	Standard (spare)
3	Excellent Load
4	Controlled Load
5	Voice and Video
6	Layer 3 Network Control Reserved
7	Layer 2 Network Control Reserved

Zdroj: RFC 2597 & RFC 2598

5 Metody pro vyhodnocování QoE a MOS

Jedná se o metody, které vyjadřují kvalitu služby z pohledu uživatele. Nejde pouze o funkčnost, ale o komplexní vlivy, které ovlivňují výsledné hodnoty, jako jsou například dostupnost, cena, podpora, rychlost sítě aj. Hens a Caballero (2008) popisují tento mechanismus jako službu očima uživatele, čímž poskytuje provozovateli nebo výrobci zpětnou vazbu a usnadňuje mu komunikaci se zákazníkem.

QoE je rozsáhlá vědní disciplína a je spjata takřka s každým odvětvím. Snahou firem je poznat QoE uživatele co nejlépe a odhalit vztahy mezi QoS a QoE a tím docílit maximálního uspokojení uživatele za minimální náklady. (Zach, 2015). Příkladem může být zákazník, který reklamuje „sekající se obraz" u IPTV. Zákazník není schopen určit důvod výskytu časté anomálie na obrazu. Technická podpora se snaží určit, o který problém se může jednat. Většinou zákazník dostává otázky, kde na stupnici od 1 - 10 určuje závažnost chyb.

QoS a QoE je často mezi sebou zaměňován. QoS je tzv. *techno-centric*, což je skupina zabývající se technickými ukazateli (delay, jitter, packet loss, bandwidth), zatímco QoE je tzv. *subsciber-centric* skupina, která se zabývá subjektivním hodnocením. (Hens, Caballero, 2008). Konečný (2015) zobrazuje ukazatele QoS a QoE v Tab. 9 .

Tab. 9 Příklady QoS a QoE ukazatelů.

QoS ukazatelé	Delay (zpoždění) Jitter (kolísání zpoždění) Packet loss (ztrátovost) Bandwidth (šířka pásma)
Příklady QoE ukazatelů	Sekání hlasu Ozvěna Šum Celkový dojem z kvality hovoru

Zdroj: Převzato od Konečný (2015).

V dokumentu SLA (Service Level Agreement), který je často uzavíraný mezi dodavatelem a odběratelem služby, nalezneme několik parametrů, které souvisí s měřením a omezováním síťového provozu. Dle Molnára (2008) je nejčastější:

- Garantovaná přenosová rychlost (CIR, Commited Information Rate).
- Maximální přenosová rychlost (PIR, Peak Information Rate).

Pojmy QoS a QoE jsou rozdílné mechanismy, ale úzce spolu souvisí. Můžeme tedy říci, že QoS je jeden z prostředků umožňující dosažení optimálního QoE.

5.1 MOS

MOS (Mean opinion score) je stupnice sloužící pro vyjádření kvality nějaké služby. Hodnotu MOS lze získat různými metodami. Podle doporučení P.800 (ITU-T, 1996) a Kuiperse (2010) lze MOS rozdělit na subjektivní, objektivní a odhadové metody. Obecná stupnice MOS je znázorněná v Tab. 10 .

Tab. 10 Stupnice kvality MOS.

HODNOTA	KVALITA
5	Excellent (vynikající)
4	Good (dobrá)
3	Fair (průměrná)
2	Poor (špatná)
1	Bad (velmi špatná)

Zdroj: Převzato z ITU-T P.800 (1996).

Subjektivní metoda je založena participaci samotných uživatelů. Vybraní uživatelé reprezentují hodnotitele služby, kdy jim je služba představena a na různých úrovních kvality vyjadřují svoje preference. Subjektivní metoda poskytuje nejvyšší přesnosti, protože hodnocení je definováno od samotných uživatelů. Tato metoda je ovšem časově i finančně náročná, takže se používá především při zavedení nových služeb.

Objektivní metoda není finančně a časově náročná z důvodu nepotřebné účasti uživatelů. Kvalita služby je odhadována algoritmicky, avšak vychází z poznatků získaných subjektivním přístupem. Snaží se odhadnout, jak by reagovali koncoví uživatelé na službu.

Metoda odhadová nedisponuje žádnou znalostí obsahu originálních ani přenesených dat a pokouší se odhadnout QoE sledováním QoS parametrů. (Zach, 2015).

Stupnic MOS existuje celá řada a vzájemně se odlišují použitou metodou a cílem testu (ITU-T, 2006). Pokud aplikujeme MOS na konkrétní případ jako např. subjektivní testování poslechu, tak označujeme MOS jako MOS-LGS (Konečný, 2015). Konkrétní druh MOS lze také měřit podle frekvenčního pásma – narrow-band (úzké frekvenční pásmo), wide-band (široké frekvenční pásmo) a také podle typu kodeku.

Tato práce se vyhodnocováním služeb nezabývá, ale je dobré znát provázanost služeb QoS a QoE.

6 Použité technologie

6.1 MikroTik

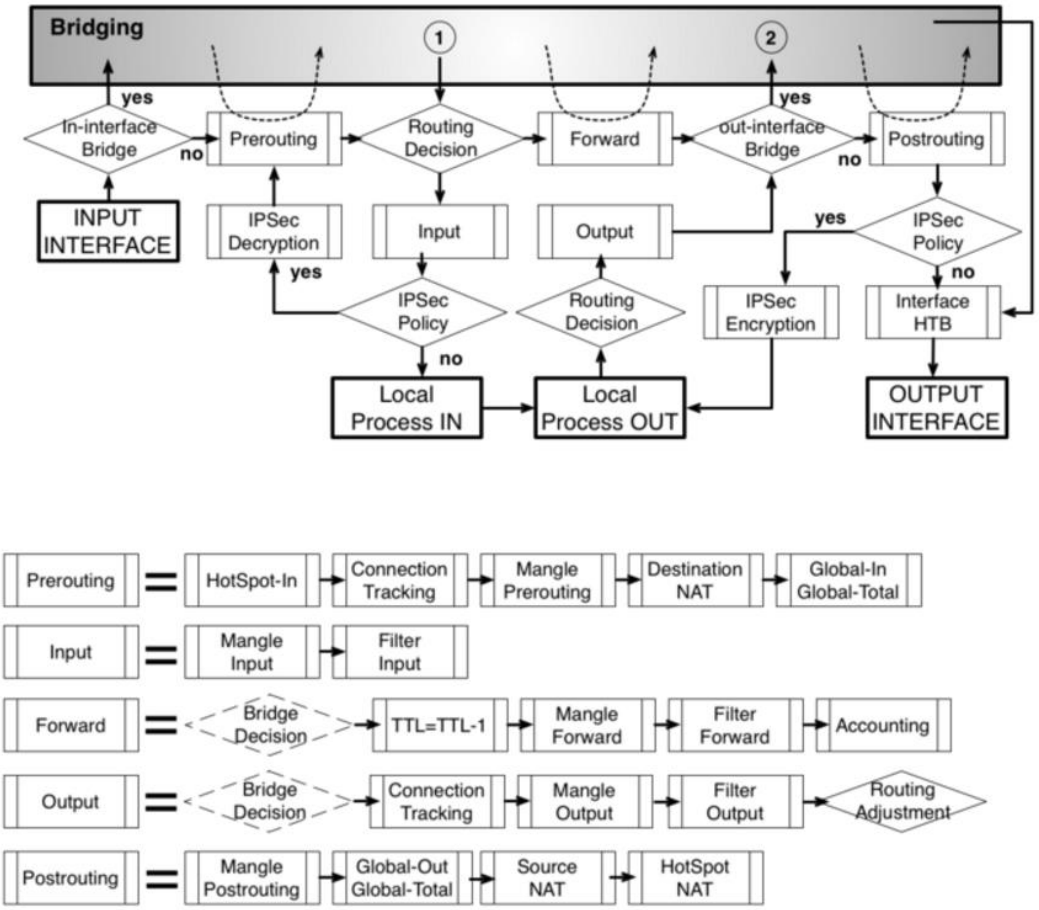
V práci se bude pracovat s prvky MikroTik. Nespornou výhodou této firmy je výborný operační systém RouterOS, který pracuje na Linuxové bázi. S prvky lze pracovat v GUI prostředí i přes terminál. Možnosti prvků omezují licence, které jsou rozděleny do 6 úrovní,[5] přičemž úroveň 6 je neomezena. Pro práci s datovými toky slouží nástroj Queue.

6.1.1 Firewall/Mangle

Mangle je nástroj, který označuje pakety příchozího nebo odchozího provozu. Paket dostane v systému speciální značku, která pak slouží pro další nástroje (queue tree, NAT, routing). Příchozí paket se identifikuje na základě jeho vlastností (IP adresa, port, protokol, DSCP aj.) a zpracuje ho odpovídajícím způsobem. Značky existují pouze v daném zařízení a nejsou přenášeny po síti. Nástroj Mangle se navíc používá k úpravě některých polí v hlavičce IP, jako jsou pole TOS (DSCP) a TTL, které pak může zpracovat jiné zařízení v síti.

Než přijde paket do zařízení, je důležité vědět, jak s ním bude zacházeno a kde přesně bude identifikován a dále zpracován. Podle dokumentace MikroTik (2017) je algoritmus pro průchod paketu až na výstupní rozhraní následující:

[5] https://wiki.mikrotik.com/wiki/Manual:License



Obr. 6 Průchod paketů na zařízení MikroTik.
Zdroj: MikroTik, 2017.

Jak můžeme vidět z obrázku, lze identifikovat paket v různém postupu na zařízení. Má-li být paket identifikován typem *prerouting*, *forward* a *postrouting*, musí být na *bridge* zapnutá funkce *Use IP Firewall*. Pokud tato funkce není zapnutá, prvek pracuje na 2. vrstvě ISO/OSI. Ve výchozím nastavení tato funkce není zapnutá a to z důvodu zvýšení nároku na prostředky zařízení. Podle pořadí routování a značkování dělíme tzv. řetězce (anglicky chain) na:

- **Prerouting** – paket je označen ještě před rozhodnutím o routingu. Chain je využívaný především když na zařízení není konfigurován NAT (maškaráda) nebo aktuální zařízení má více vnitřních rozhraní. Také se používá u značkování spojení a paketů pro následné statické routování.
- **Postrouting** – paket se označuje až těsně před tím, než opustí výstupní rozhraní. Často se využívá pro značkování uploudu.
- **Forward** – označuje paket bezprostředně po rozhodnutí o routingu. Jak můžeme vidět z Obr. 6, značkuje ještě před source-NATem, používá většinou tam, kde je přítomen i NAT.

V rozsáhlé síti může růst počet pravidel mangle. Pokud bychom měli 300 pravidel a paket byl zachycen až posledním pravidlem, může nastat zpoždění a navíc se zvyšují nároky na prostředky zařízení. Tento problém lze vyřešit funkci *Jump*, která při identifikaci paketu skočí na příslušné pravidlo. Další možností je použít *mark connection*, kdy se označený paket vztahuje na všechny pakety připojení. *Paket mark* (označení paketu) pak vychází z *mark connection*.

6.1.2 Queue

Queue (česky fronta) je nástroj v RouterOS, který slouží pro práci k řízení síťového provozu (QoS). Na základě parametrů lze omezovat a nastavovat priority pro různé datové toky. Lze použít i různé limity v závislosti na čase. Implementace Queue je založena na HTB (Hierarchical Token Bucket). Podle MikroTik (2017) wiki lze HTB strukturu připojit ke čtyřem různým rozhraním:

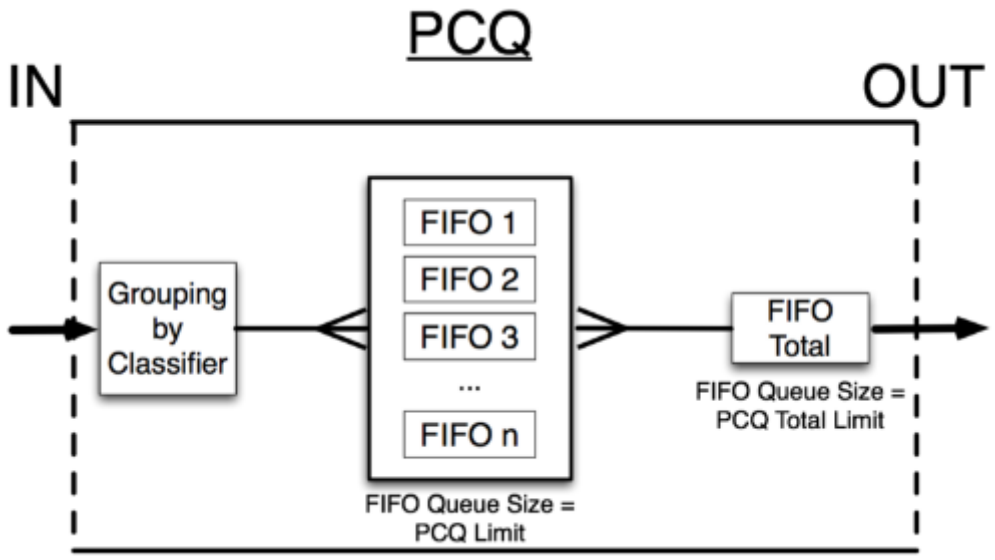
1. global-in – reprezentuje všechna vstupní rozhraní. Vztahuje se na provoz, který prvek přijímá před filtrováním paketů
2. global-out – reprezentuje všechna výstupní rozhraní
3. global-total – představuje všechna vstupní a výstupní rozhraní. Jinými slovy je to agregace globálních vstupů a výstupů
4. <interface name> - představuje jedno konkrétní fyzické rozhraní. Lze tedy pro různé rozhraní nastavit různé požadavky

K řízení provozu lze použít Simple Queue nebo Queue Tree. První zmíněný nástroj se používá pro základní stanovení pásma pro klienty. Priorita u Simple Queues označuje prioritu v rozdělování volného pásma pro *Max Limit.* Pokud není nastavený *Limit At*, jsou si všechny Queues rovny. Od nového firmwaru lze aplikovat Simple Queue i na jednotlivá rozhraní. Oproti tomu Queue Tree slouží ke složitějšímu řízení pásma. Jedná se o stromovou hierarchii. Lze nastavit šířku pásma, burst nebo garantovat minimální šířku pásma. Každé pravidlo má nadřazené rodičovské pravidlo (parent). (Fraj, 2014).

To, jak bude s pakety zacházeno a jak budou opouštět frontu, určuje queue type (česky typ fronty). RouterOS nabízí 6 druhů front:

- **PFIFO, BFIFO a MQ PFIFO** – Fronty pracují na principu algoritmu FIFO (First In First Out). Rozdíl mezi PFIFO a BFIFO je takový, že BFIFO je měřen v bajtech a PFIFO v paketech. Pokud se paket do fronty už nevejde, je zahozen. Velká velikost fronty může zvýšit latenci, ale zlepší se packet loss. MQ PFIFO funguje na stejném principu, ale používá více front současně.
- **RED** – Random Early Drop je mechanismus statického zahazování paketů. Zamezuje přetížení linky a zamezí špičkám.
- **SFQ** – Stochastic Fairness Queuing zajišťuje spravedlivé rozdělení pásma mezi jednotlivé relace (sessions), nepřiděluje tedy pásmo IP adresám. Používá se ve výchozím nastavení pro Wi-Fi. Celá fronta může obsahovat až 128 paketů a je k dispozici 1024 sub-streamů.

- **PCQ** – používá se u masivních QoS systémů. Nejprve používá vybrané klasifikátory k odlišení jednoho sub-streamu od druhého, potom použije velikost fronty a omezení fronty FIFO na každý sub-stream. Nakonec seskupí všechny sub-streamy dohromady a použije globální velikost fronty a omezení. Jednoduše řečeno, pokud máme např. rozsah zdrojových adres, může být použito jedno pravidlo, které bude omezovat každou IP z daného rozsahu. (MikroTik, 2017). Celý proces je zobrazen na Obr. 7. Další nespornou výhodou je spravedlivé rozdělení šířky pásma.



Obr. 7 PCQ mechanismus.
Zdroj: MikroTik, 2017.

6.2 IPTV

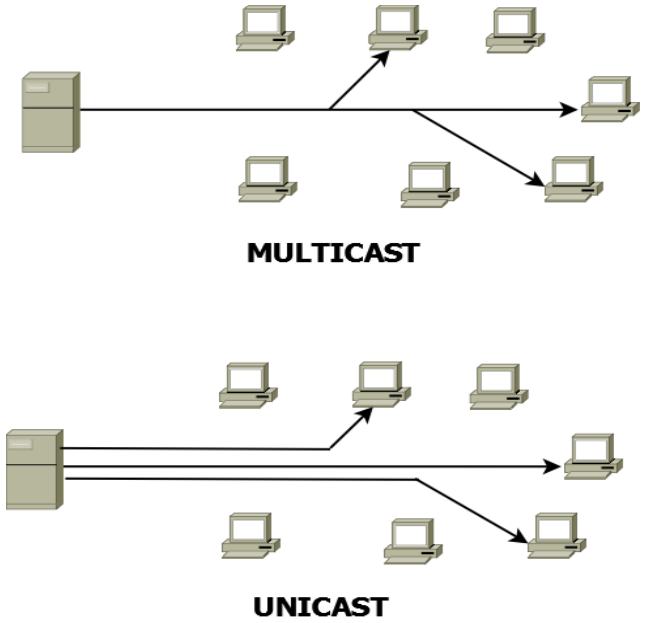
IPTV (Internet Protocol Television) je novodobé poskytování televizního vysílání. Televizní streamy jsou šířeny prostřednictvím IP protokolu přes počítačovou síť. K službě IPTV je potřeba internetové připojení. Lze použít zařízení jako osobní počítač, STB (Set-top box) nebo mobilní telefon. V roce 2005 bylo spuštěno první HDTV vysílání. Z důvodu vyšších nároků na HDTV kanály musí poskytovatelé zvyšovat kapacitu svých sítí. Rozdílem mezi terestriální formou přenosu televizního vysílání a IPTV je, že IPTV komunikují se zdrojem dat, zato u terestriálního vysílání uživatelé pouze přijímají vysílaný signál.

6.2.1 Typy komunikace

Unicast je typ komunikace, kde jsou pakety zasílané pouze jedinému cíli. Opakem je broadcast, který vysílá do všech uzlů v síti najednou. Unicast je nevhodný tam, kde je více zdrojů a více příjemců, jako např. televizní vysílání nebo videokonference. Zdroj musí vyslat data tolikrát, kolik je příjemců. Tato situace vede

k plýtvání šířky pásma a nároků na samotný zdroj dat, protože musí vysílat stejná data několikrát.

Mezi broadcastem a unicastem stojí multicast. Mutlicast je typ komunikace, který umožňuje vysílat data pouze jednou s tím, že kopie vyslaných dat jsou doručeny všem příjemcům. Kopie dat se vytváří vždy ve směrovačích umístěných nejblíže k danému příjemci, aby se šetřily přenosové prostředky sítě. (Slavíček, 2010).



Obr. 8 Multicastový a unicastový provoz.
Zdroj: Vlastní práce.

6.2.2 Zařízení Arris VIP 1113

Obr. 9 Arris VIP 1113
Zdroj: převzato od Selfnet (2017).

Výhodou dnešních IPTV je především možnost přehrávání kanálů zpětně i o několik dní. V základní nabídce IPTV od společnosti Smart Comp a.s. lze přehrávat všechny pořady 2 dny zpětně. Televizní stream distribuují nejen v mobilní a počítačové verzi, ale především v platformě Arris VIP 1113. Specifikace produktu jsou v Tab. 11 .

Tab. 11 Specifikace zařízení Arris VIP 1113.

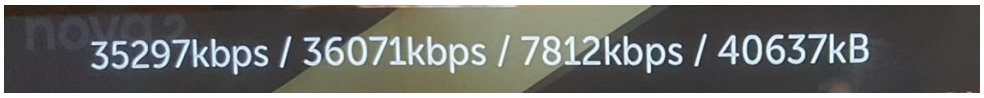
CPU	650 MHz
DRAM	265 (512) MB
FLASH	128MB
Výstupní rozlišení	576p, 720p, 1080i, 1080p60
Ethernet	10/100 Mbps
Hmotnost	150g
Audio kodeky	Dolby Digital, MP3, MPEG-1m, AAC LC, HE-ACC
Video kodeky	MPEG-4 AVC(H.264), MPEG-2
USB 2.0	ANO
OS	ARRIS KreaTV 4.6 nebo novější

Zdroj: Převzato od Selfnet (2017).

Cena STB produktu se pohybuje mezi 2000 - 3000 Kč. Jeho nasazení proběhlo i ve firmách DIGI CZ, T-Mobile a další. U služby Kuki TV[6] od společnosti Smart Comp a.s. vidí klient živé vysílání o několik sekund zpožděné. Zpožděné vysílání si načítá do bufferu, který zaručí, že i při větší ztrátě paketů nepozná uživatel žádný nedostatek. STB si udržuje 4 měnící se hodnoty:

1. Hodnota, která ukazuje velikost posledních načtených dat ze zdroje.
2. Hodnota, kterou propočítává algoritmus na výpočet rychlosti linky. Jedná se o rychlost šířky pásma, kterou STB disponuje. Dle hodnoty zařízení ví, jaký profil zvolit.
3. Nutná šířka pásma profilu, který je aktuálně zvolen. Nejvyšší profil má hodnotu 10 742 kbps a jedná se o nejvyšší kvalitu obrazu. Pokud se algoritmus na propočítávání rychlosti linky rozhodne, že linka nedosahuje minimální rychlosti 10 742 kbps, sníží profil, čímž se sníží kvalita obrazu, ale sníží se datová náročnost IPTV.
4. Poslední hodnota udává velikost načtených dat v bufferu. V případě, že je v bufferu 0 kB, tak se televizní stream zastaví. V živém vysílání si STB udržuje maximální hodnotu 20 000 kB. Při přehrávání ze záznamu má STB načteno v bufferu 40 000 kB.

   Hodnoty během vysílání mohou vypadat jako na Obr. 10.



Obr. 10 Datové hodnoty IPTV během provozu.
Zdroj: Vlastní práce.

Kuki TV nabízí své služby dvěma způsoby. První je typem unicast, který je doporučen používat v síti do 100 uživatelů. Druhý způsob je přes multicast, kde je potřeba dostat do sítě přibližně 600 Mbps trvalého provozu. STB si přehrávaný kanál vyžádá od nejbližšího aktivního prvku, na kterém je multicast. Komunikace probíhá přes IGMP (Internet Group Management Protocol).

6.2.3 Identifikace paketů

Řídit síť dle IP adres klientů, kteří využívají služeb IPTV, je značně neefektivní. Pakety IPTV jsou zaznamenány v hlavičce IP, respektive v poli DSCP. Pakety od dodavatele Kuki TV jsou označeny následujícím způsobem:

- **AF41** – multicast pro live-tv
- **CS4** – unicast pro nelineární vysílání
- **AF22** – STB signalizace (přepínání kanálů)

[6] https://www.kuki.cz/

Doporučení dle emailu od Kuki (2017) na QoS je následující:

1. priorita – VoIP provoz, VoIP signalizace, STB signalizace
2. priorita – multicast pro live-tv
3. priorita – unicast pro nelineární vysílání
4. priorita – zbývající provoz

Lineární provoz je klasické TV vysílání. Jeden pořad následuje druhý (oddělený znělkami, reklamami, upoutávkami apod.). Opakem je nelineární vysílání, kde uživatel vybírá, co bude sledovat a aktivně se podílí na jeho spuštění. (podcasting, různé videotéky, Video-On-Demand, TiVo, aj).

6.2.4 Požadavky na provoz

Požadavky na IPTV jsou vysoké především na šířku pásma. Z důvodu, že STB si načítá stream předem do velkého bufferu, nejedná se přímo o real-time provoz jako je VoIP. Požadavek na šířku pásma se odvíjí od stanoveného obrazového profilu. Podle wiki dodavatele jsou požadavky na datové profily následující: (Kuki, 2017).

Tab. 12 Specifikace zařízení Arris VIP 1113.

Profile	Encoding	Resolution	Video rate (kb/s)	Quality	Kuki bitrate (kb/s)
P1	ABR	616x462p25	600	SD	1000-1500
P1+	ABR	616X462p25	1000	SD	
P2	ABR	720X576p25	1500	SD	2000-2500
P2+	ABR	720X576p25	2000	SD	2000-3500
P2++	ABR	720X576p25	3000	SD	4000-4500
P3	ABR	1280x720p25	3000	HD ready	4000-4500
P3+	ABR	1280x720p25	4000	HD ready	5000-6000
P4	ABR	1920x1080p25	6000	HD full	8000-8500
P4+	1s	1920x1080i50	6000	HD full	8500
P5	1s	1920x1080i50	8000	HD full	10500-11005
P5+	1s	1920x1080i50	10000	HD full	13000-13500

Zdroj: Převzato od Kuki (2017).

Kuki bitrate udává maximální hodnotu datového toku streamu, včetně režie na ostatní stopy ve streamu (audio, titulky apod). Omezení bitrate pro konkrétní STB lze nastavit v portálu partner.kuki.cz.

Požadavky z pohledu delay, jitter a packet loss nejsou nikde zveřejněny. Pokud by packet loss přesahoval 10 %, lze předpokládat, že i když má STB dostatečnou rychlost, nedokáže načíst dostatek dat, protože se po cestě ztratila. STB načítá data tehdy, až je prázdnější buffer. Při profilu P5+ a garantované šířce pásma 40 Mbps si průměrně načítá data jednou za 4 sekundy.

7 Metodika

Postup vedoucí k dosažení specifikovaného cíle této diplomové práce lze shrnout do následujících kroků:

1. Stanovení cíle. Dosáhnout provozu IPTV v bezdrátovém prostředí nezávisle na zátěži provozu. Vyzkoušet různé varianty konfigurací a na základě testovacích výsledků zvolit optimální řešení.
2. Provedení analýzy prostředí TS–Hydro, ze kterého vychází problematika řízení sítě. Popsat strukturu a funkčnost sítě. Vytvořit souhrn působících platforem a srovnat s různými alternativami. (kapitola 8).
3. Vytvoření laboratorních podmínek (kapitola 9) a stanovení potřebné struktury (kapitola 7.1).
4. V kapitole 10 je popsána konfigurace prvků MikroTik, která vychází z teoretických znalostí popsaných v kapitole 6.1. Požadavky na provoz IPTV jsou interpretovány v kapitole 6.2.4.
5. Nejdůležitější částí této práce jsou měření výsledků jednotlivé konfigurace. Na základě různých protokolů a omezení změříme různá řešení. Na základě každé konfigurace, budeme provádět vždy několik druhů testů. Metodika měření je popsána v kapitole 7.3
6. Na základě hodnot měření zhodnotíme jednotlivé mechanismy QoS.
7. Dle výsledků zvolíme optimální řešení pro ISP síť.
8. V kapitole 13 provedeme implementaci a pro zvolené řešení provedeme verifikační testy.
9. V závěru zhodnotíme přínos nejen pro firmu, ale i pro praxi.

7.1 Struktura laboratoře

K měření výsledků je třeba vystavět laboratoř, která je postavená na platformách působících ve firmě TS–Hydro. V tomto případě se jedná o prvky značky MikroTik. V síti bude připojen souborový server, který bude sloužit k reálným zátěžovým testům. K monitoringu využijeme dva stolní PC. Fyzické propojení proběhne přes standard FastEthernet. Alespoň jedno spojení mezi klientem a serverem proběhne přes Wi-Fi standard. Laboratorní síť využije připojení k Internetu s kapacitou 100/100 Mbps. Podrobnější struktura je popsána v kapitole 9.

7.2 Konfigurace

Každý výrobce dává svým uživatelům různé možnosti konfigurace zařízení. V praxi může různé nastavení znamenat lepší výsledky. Je důležité, aby se síť v laboratoři co nejvíce přibližovala realitě. Budeme používat stejné firmwary (6.38.5) jako v síti ISP, protože v některých verzích mají prvky jiné možnosti nastavení a mohly by při implementaci do sítě ISP způsobovat problémy. U MikroTiku dává výrobce pro

použití k řízení sítě možnost Simple Queue a sofistikovanější Queue Tree. Oba přístupy jsou popsány v kapitole 6.1.2. V bezdrátových přenosech je alternativou WMM (kapitola 4.5) nebo proprietární protokol NV2 (kapitola 2.3.9). Na základě výsledků zvolíme optimální řešení.

7.3 Metodika měření

Měření lze provést dvěma způsoby - bez zátěže a se zátěží. Testování bez další zátěže je irelevantní, protože pouze při maximální zátěži se ukáže, zda řešení má přínos a je rezistentní proti datovým špičkám. Testování bez zátěže bude sloužit jen jako výchozí stav. Na základě kladných výsledků výchozího testu, provedeme další testy. Každý test bude proveden čtyřikrát. V práci bude publikováno pouze první měření. Ostatní měření jsou určena k tomu, aby odhalila případnou chybu prvního měření. Výsledky zátěžového měření odhalí optimální řešení pro poskytování IPTV bez ohledu na datový provoz.

VÝCHOZÍ STAV

Ve výchozím stavu bude IPTV vždy omezena na 15 Mbps. Toto omezení umožňuje provozovatel v portálu vm.kuki.cz, který slouží jako administrační systém pro ISP spolupracující ve velkoobchodním modelu. Na základě sériového čísla a MAC adresy je nastaven maximální bitrate v kbps.

DOBA MĚŘENÍ

Každé měření bude probíhat 2 minuty. Ukazatelem kvality přenosu jsou hodnoty STB, které definují kvalitu obrazu. (kapitola 6.2.2). Za 2 minuty každého testu dostaneme výsledky, které budou publikovány a graficky zobrazeny.

SIMULAČNÍ TESTY

Zátěžové simulační testy lze provést pomocí protokolů TCP nebo UDP. Simulační nástroj BTest umožňuje nastavení konstantní zátěže. Pro simulační testy nastavíme neomezenou přenosovou rychlost. Během každého testu je puštěn ping test. Testovány budou spojení TCP i UDP, ale v práci budou publikována pouze simulační data UDP. TCP spojení jsou publikována jako reálné testy.

REÁLNÉ TESTY

Reálné zatížení bude probíhat pomocí stažení dat ze souborového serveru. Přenosová rychlost je omezena rychlostí média. Spojení bude probíhat přes protokol TCP. Jako ukázka reálného testu se bude stahovat 3 GB soubor win7.iso, který byl stažen z MSDN AA. Zátěžový test nebude přerušen.

VELIKOST FRONTY

Velikost fronty ovlivňuje výsledek měření. Je třeba vhodně zvolit velikost fronty. Aplikovány budou fronty PCQ a SFQ. Jejich teoretické principy jsou popsány v kapitole 6.1.2. Pro ukázku vyzkoušíme, jak extrémní velikost fronty ovlivní výsledky měření. Maximální doba pobytu paketu ve frontě je pro nás 50 ms. Pro zjištění ideální velikosti PCQ fronty budeme testovat tyto hodnoty:

1. **50 MiB** – extrémní velikost fronty. RTT (Round-Trip Time) hodnoty by měly při zátěži dosahovat několika tisíc milisekund.
2. **50 KiB** – výchozí hodnota fronty v RouterOS.
3. **1 KiB** – minimální hodnota fronty.

Podle výrobce je výchozí hodnota nastavena ideálně. Jejich testy jsou zveřejněny na jejich wiki stránkách. (MikroTik, 2017).

MONITORING

Jako monitorovací prostředek pro stabilitu spoje je protokol ICMP (Internet Control Message Protocol), který vyhodnotí důležité aspekty. (RTT a packet loss).

7.3.1 Typy měření

Zátěž lze provést vícero způsoby a použít různé techniky. V této práci se budou používat simulační a reálné zátěže. Všechny typy měření proběhnou po dobu 2 minut. Do tabulky budou zaznamenány hodnoty STB vždy po 10 sekundách měření. IPTV vždy přehrává kanál ČT sport v režimu TimeShift, který využívá maximální profil P5+. Celkem proběhne 6 testů pro konfiguraci Queue Tree, NV2 a WMM.

TEST-1 (BEST EFFORT)

Tento test je bez aplikování mechanismu QoS. Proběhne reálný zátěžový test TCP. IPTV má výchozí hodnoty následující:

Tab. 13 Výchozí hodnoty IPTV v testu Best Effort.

15 000 kbps	15 000 kbps	10 742 kbps	40 000 kB

Po 10 sekundách proběhne z PC stažení dat ze souborového serveru. Měření probíhá vždy po 10 sekundách po dobu 2 minut.

TEST-2 (VÝCHOZÍ)

Jedinou datovou zátěží bude samotná IPTV. Pokud šířka pásma nedosahuje potřebných kvalit (alespoň 15 Mbps), nemá smysl tvořit zátěžové testy s touto konfigurací. Výchozí hodnoty STB jsou stejné jako v tabulce Tab. 13 .

TEST-3

IPTV má výchozí hodnoty stejné jako v tabulce Tab. 13 . V tomto případě ale proběhne reálné zatížení TCP ze souborového serveru po dobu 2 minut. Postup měření je následovný:

- 0 s – STB je zapnutý a má načtenou plnou kapacitu bufferu.
- 10 s – stahování dat ze souborového server a ping na hraniční prvek.
- 120 s – konec testu.

TEST-4

V TEST-4 probíhá simulační zátěžový test na hraniční prvek. STB začíná s bufferem v maximální kapacitě a po 10 sekundách bude spuštěn simulační test. Průběh 2 minutového testu je tedy následující:

- 0 s – STB je zapnutý a má načtenou plnou kapacitu bufferu.
- 10 s – simulační test a ping na hraniční prvek.
- 120 s – konec testu.

TEST-5

TEST-5 je nejpřísnější test, ve kterém je nejdříve spuštěn simulační a reálný test. Po 10 sekundách bude IPTV zapnutá, takže výchozí hodnoty bufferu budou na úplném minimu. Průběh 2 minutového testu je tedy následující:

- 0 s – na hraniční prvek je puštěn ping a simulační zátěžový test. Ze souborového serveru stahuje druhý PC soubor o velikosti 3 GB.
- 10 s – zapnutí STB.
- 120 s – konec testu.

TEST-6 (ICMP)

ICMP protokol bude prioritizován na úroveň IPTV. Při zátěžovém testu je to ukazatel kvality spojení. ICMP vyhodnotí klíčové aspekty – RTT a packet loss, které určí stabilitu spoje.

Srovnání (TEST-1 vs TEST-3)

Na závěr každé konfigurace je srovnán přístup Best Effort s QoS systémem. Oba testy jsou založeny na reálném TCP zatížení.

Verifikační TEST-1

Tento test je aplikován po implementaci řešení v síti ISP. Domácí síť je připojena k Internetu přes kabel do sítě ISP. Simulační zátěž UDP proběhne z 5 prvků působících ve vesnici. Cílem simulačního testu je hraniční prvek. IPTV bude zapnutá po 10 sekundách zátěžového testu. Průběh testů bude následující:

- 0 s – na hraniční prvek je puštěn ping a z 5 prvků na LAN síti je aplikován simulační zátěžový test. Bezdrátový spoj dosáhne své maximální přenosové kapacity.
- 10 s – zapnutí STB.
- 120 s – konec testu.

Verifikační TEST-2

V tomto testu bude domácí síť připojena k Internetu přes Wi-Fi Standard. Na AP bude celkem připojeno 5 klientů. Od 3 klientů bude aplikován simulační test TCP na hraniční prvek ISP sítě. IPTV bude zapnuta po 10 sekundách probíhajících simulačních testů. Průběh 2 minutového testu je následující:

- 0 s – na hraniční prvek je puštěn ping a od 3 klientů na AP je aplikován simulační zátěžový test. AP dosáhne své maximální přenosové kapacity.
- 10 s – zapnutí STB.
- 120 s – konec testu.

7.4 Výsledky

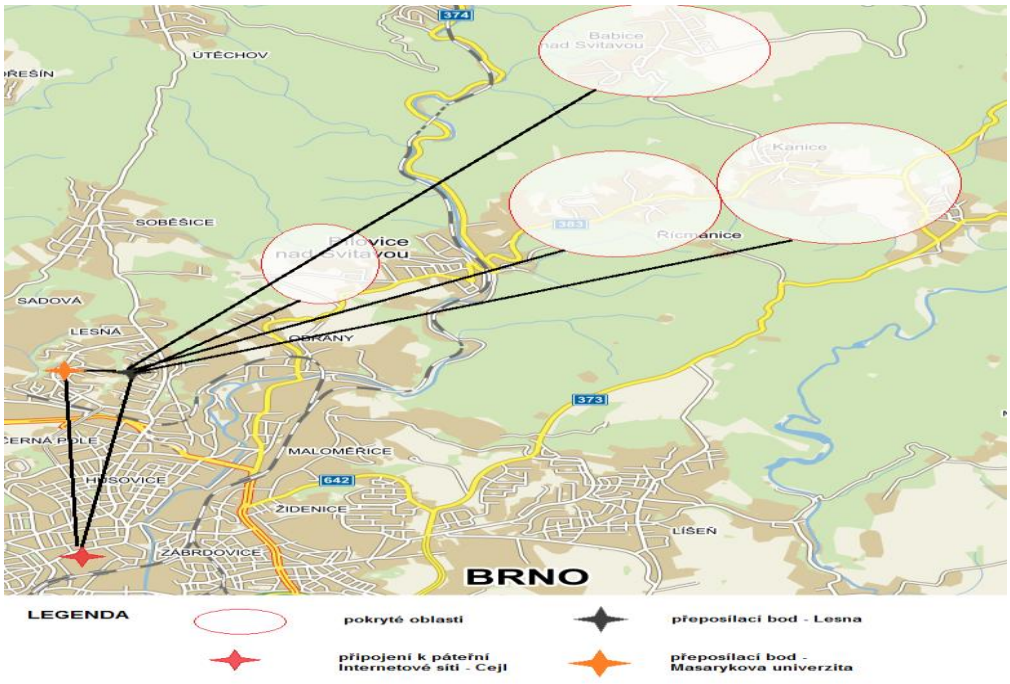
Výsledky měření srovnáme v kapitole 12. Grafem zhodnotíme rozdíl před a po nasazení QoS. Na závěr zhodnotíme všechna použitá řešení mezi sebou a zjistíme, zda základní řízení sítě bezdrátových technologií je na úrovni běžné kabelové sítě. Při pozitivních měřicích výsledcích provedeme implementace do produkční sítě.

8 Analýza

Počítačová síť společnosti TS–Hydro, s.r.o. vznikla v roce 2003. Dva studenti bydlící na stejné ulici si vytvořili ethernetovou síť na hraní her. Z důvodu nedostatečné kvality internetového připojení v obci se rozhodli pomocí bezdrátové technologie připojit vytvořenou ethernetovou síť k Internetu. Během pár let byla připojena pomocí bezdrátového spoje celá vesnice a založena firma TS-Hydro s.r.o.. Dnes má firma připojeno přes 400 koncových zákazníků včetně firem a dalších menších ISP.

8.1 Geografická poloha sítě

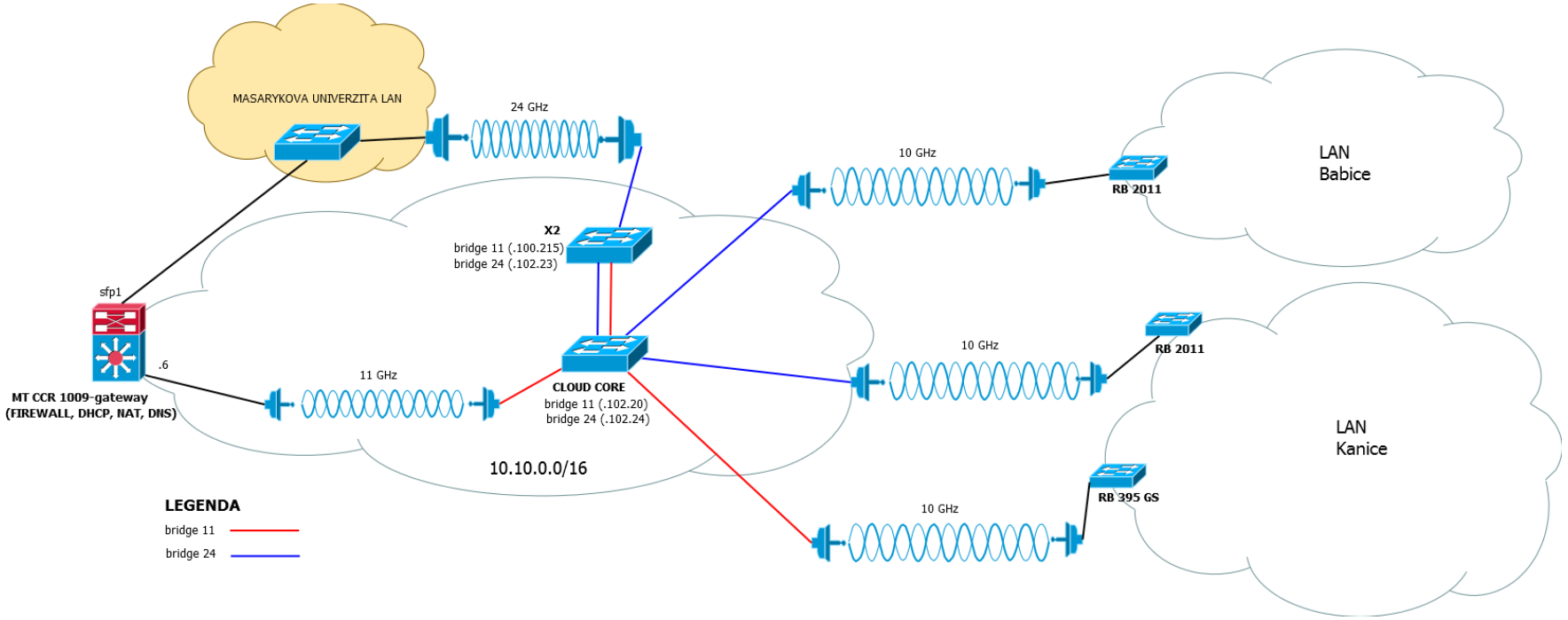
Poskytováním internetového připojení se firma zabývá především ve čtyřech vesnicích, které leží nedaleko Brna. Největší část klientu je připojena v Kanicích. Na Obr. 11 je zobrazena mapa sítě z geografického hlediska.



Obr. 11 Poloha sítě z geografického pohledu.
Zdroj: Vlastní práce.

8.2 Struktura sítě

Firma odebírá full duplexní konektivitu 1,5 Gbps od UPS z páteřní sítě v Brně na ulici Cejl. Ve špičce v neděli večer je maximální zatížení až 500 Mbps. Z důvodu rozsáhlosti sítě bude struktura popsána po částech a některé síťové prvky nezasahující do chodu sítě budou vynechány. Core vrstva je zobrazena na Obr. 12.



Obr. 12 Topologie core vrstvy.
Zdroj: Vlastní práce.

Celá síť včetně LAN ve vesnicích, pracuje na podsíti 10.10.0.0/16. Hraničním prvkem sítě je MT CRR 1009, který plní funkci brány, firewallu a NATu. Z tohoto prvku je na licencovaném pásmu 11 GHz přivedena konektivita na intermediální bod v Brně na Lesné. Spoj PtP přenese až 350 Mbps ve full duplexním režimu. Dodavatelem spoje je česká společnost Alcoma a.s.. Druhou a novou možností přenesení dat do lokality na Lesné je spoj z budovy Masarykovy univerzity přes pásmo 24 GHz. Spoj od americké firmy Ubiquiti přenese na krátkou vzdálenost až 1 Gbps ve full duplexním režimu. Z důvodu větší vzdálenosti mezi budovami je reálná rychlost 600 Mbps v obou směrech. Bezlicenční pásmo 24 GHz používá pouze 2 kmitočty. Pro RX (příjem) jeden a pro TX (odesílání) druhý kmitočet. Pokud by někdo v blízkosti aplikoval další 24 GHz spoj, pravděpodobně by nastalo degradování spoje. Jedná se však o novinku, která se během pár měsíců jeví jako skvělý spoj v poměru cena/výkon.

Z centrálního bodu na Lesné jsou do jednotlivých vesnic použity spoje Alcoma na frekvencích 10 GHz. Bezdrátový spoj Lesná – Kanice (RB 395GS) přenese přes 220 Mbps ve full duplexním režimu. Druhý spoj do Kanic přenese 140 Mbps v obou směrech. Do Babic nad Svitavou je konektivita 180Mbps full duplex. Všechny spoje jsou PtP a jedná se o velmi sofistikované spoje, které i při špatném počasí mají maximální datový útlum 10 Mbps.

V Kanicích má firma pokrytou téměř celou vesnici kabelovým připojením. Kabelové připojení je nově rozšířeno i v Babicích nad Svitavou, ale jedná se pouze o nově vystavěnou obytnou oblast. Zbytek klientů je připojen přes Wi-Fi na frekvenci 5 GHz, ve výjimečných případech 2,4 GHz.

8.2.1 Funkčnost

Síť firmy je pouze L2, takže se nepoužívají dynamické směrovací protokoly jako OSPF, BGP aj. Na síti jsou aplikované VLAN, pro menší ISP, které odebírají od firmy konektivitu. Jelikož se jedná o ISP, není aplikován téměř žádný firewall. Jedná se pouze o obranu před útoky na infrastrukturu. Firma poskytuje dva připojovací tarify. Tarif Mini (330 Kč/měsíc), který je omezen na 8/8 Mbps a dle smlouvy je nastaven FUP limit na 5 GB/měsíc. Omezení klientů probíhá na hraničním prvku na Cejlu. Z důvodů zkvalitňování služeb řešila firma nedostatečnou kapacitu spojů, nákupy nových bezdrátových spojů. Firma používá dva DHCP (Dynamic Host Configuration Protocol) servery. Jeden je implementován na hraničním prvku na Cejlu a je používán pro zákazníky s tarifem Speed. Druhý je na Lesné, používaný pro tarif Mini. Z důvodu bezpečnosti a častých broadcastových bouří, které vznikaly především z nekvalitních zařízení zákazníků, je každý zákazník oddělený pomocí NAT (Network Address Translation). V síti LAN ve vesnicích se používá protokol RSTP (Rapid Spanning Tree Protocol), který slouží k odstranění smyček a zároveň při výpadku automaticky aktivuje novou cestu. Prvky na Lesné mají 2 IP adresy. Jeden pro bridge11 a druhý pro bridge24. Tyto cesty jsou odděleny a není tedy zde implementován protokol RSTP. Redundance bran není prozatím v provozu, takže při výpadku brány je ručně aktivován prvek na Lesné, který je připojen k uživatelskému Internetu od UPS (100/100 Mbps). V nejbližších dnech by tento

problém měl vyřešit protokol VRRP (Virtual Router Redundancy Protocol). Funkci DNS (Domain Name Systém) má na starost hraniční prvek. Firma disponuje i veřejnými IP adresami, které poskytuje za poplatek 100 Kč/měsíc. Síť obsahuje přes 400 aktivních prvků, ze kterých je drtivá většina od firmy MikroTik. Při výpadku je aktivován na klíčových prvcích Netwatch, který při výpadku odešle SMS/email. Tento nástroj i sleduje stabilitu sítě. Pří ztrátě více paketů odešle informace o této ztrátě.

Je třeba brát při návrhu v potaz, že síť prochází restrukturalizací, takže řešení musí být kompatibilní s budoucími úpravami sítě.

8.2.2 Souhrn platforem v síti

Jak už bylo zmíněno, firemní politikou je nasazovat do sítě především MikroTiky. Je důležité znát i hardwarovou stránku zařízení, aby zvolené řešení zvládlo po výkonnostní stránce. Celkem je v síti 463 aktivních prvků z toho 441 prvků značky MikroTik (viz Tab. 14). Zařízení mají ještě rozdělení podle výkonu, typu vysílání a dalších funkci.

Tab. 14 Typy a počty zařízení MikroTik v síti.

Typ zařízení	**Počet**
RB SXT	140
RB 750	93
RB 951	38
RB 2011	38
Ostatní	24
RB OmniTik	21
RB 600	16
RB 711	13
RB 911	12
RB 433	12
RB 952	11
RB 951	10
RB 411	7
CCR + CRS	3
RB 953	3

Z hardwarové stránky dokáže provoz řídit pouze CCR nebo CRS, které disponují vícejádrovými procesory. Prvek od MikroTiku, jemuž CPU pracuje přes 50 %, je v sítí nepoužitelný a i když to není na první pohled poznat, tak způsobuje různé anomálie, které je velice těžké odhalit. Z vlastní zkušenosti to může být „sekající“ online stream videa. I když má klient dostačující rychlost i odezvu je video během přenosu nekvalitní.

Zbylých 22 zařízení jsou povětšinou páteřní spoje na kmitočtech 10 GHz. Největší zastoupení má platforma Alcoma a Ubiquiti. Přehled je zobrazen v Tab. 15 .

Tab. 15 Typy a počty ostatních zařízení v síti.

Typ zařízení	Počet
ALCOMA MP	12
Ubiquity M10	4
TP-Link	3
Ostatní	3

8.3 Srovnání různých výrobců

Výrobců síťových zařízení je nespočet. Mezi přední patří Cisco a Juniper. Je tedy důležité si srovnat různé platformy z hlediska funkčnosti, ceny a výkonu. U bezdrátových platforem je srovnání složitější. Někteří výrobci vyrábí pouze licencované spoje, ale ve spojích v bezlicenčních pásmech na frekvencích 5 GHz pro venkovní spoje je mimo MikroTik předním distributorem v České republice Ubiquiti. Oba distributoři mají na webu i4wifi.cz vlastní záložku pro nákup. Menší zastoupení má ještě Cambium Networks.

V pásmu 10 GHz, které slouží pro páteřní spoje, už MikroTik nepůsobí a největšími distributory v České republice jsou výrobci Alcoma, Ubiquiti a Summit Development. Spoje v pásmu 10 GHz byla velice nákladné (běžně 100 000 Kč za spoj). Tento trend narušil nový spoj M10 od společnosti Ubiquiti, jehož cena za spoj se začala pohybovat okolo 20 000 Kč. (Internetprovsechny, 2012).

Jako páteřní spoje jsou využívaná také frekvenční pásma 17 a 24 GHz. Podle vyhlášky popsané v kapitole 2.4 je rozsah frekvenčního pásma 17.1 – 17.3 GHz. Lze tedy použít pouze 200 MHz šířku pásma. Pásmo 24 GHz nespadá pod vyhlášku č. VO-R/12/06.2010-9. Tento frekvenční kmitočet je definován ve vyhlášce č. vo-r_10-04_2012-07 (ČTU, 2012). Rozsah volného použití pásma je 24, 15 – 24, 25 GHz, což je šířka pásma 100 MHz. Zvláštní přístup zvolila firma Summit Development, která stvořila mikrovlnnou komunikační jednotku pracující na obou zmíněných frekvencích. Zařízení na jednom kanále vysílá a přijímá v pásmu 17 GHz a na druhém kanále vysílá a přijímá v pásmu 24 GHz s kapacitou až 1Gbps s použitím šířky pásma 160 MHz.

Souhrn různých platforem pro umístění do jádra nalezneme v Tab. 16 . Core a distribuční switche od firmy Cisco jsou navrhované pro větší infrastruktury. Navíc je irelevantní srovnávat switche, které stojí několik stovek tisíc a jsou pro firmu absolutně nedostupné. Jsou tedy srovnány levnější verze těchto předních výrobců.

Tab. 16 Srovnání různých druhů platforem.

Výrobce	Typ	QoS	Gigabit portů	SFP portů	Počet jader	Frekvence CPU	OS	Cena (Kč)
MikroTik	CCR1036	ANO	12	4	36	1.2 GHz	RouterOS	24 000
TP-Link	T3700G-28TQ	ANO	24	6	-	-	-	50 000
Cisco	Catalyst 2960G 24	ANO	24	2	-	-	Cisco IOS	75 000
Juniper	EX4200-24T	ANO	24	6	-	1 GHz	Junos OS	85 000
HP	2920-24G	ANO	24	4	3	625 MHz	-	35 000

Jako nejlepší v poměru cena/výkon jasně dominuje MikroTik, který je zaměřený na menší poskytovatele. Někteří výrobci neposkytují informace o hardwarové stránce zařízení. Pokud by firma disponovala mnohonásobně větším kapitálem, je určitě lepší zvolit jiné řešení.

Firmy Cisco nebo Juniper se nezaměřují příliš na výrobu bezdrátových zařízení ve venkovním prostředí. V 5 GHz pásmu si vybírají poskytovatele zařízení, které má největší stabilitu a rychlost. Jsou to ovšem dvě subjektivní hodnoty. Rychlost přenosu se může v různých podmínkách pro různá zařízení lišit a teoretická rychlost udávaná od výrobců je prakticky nedosažitelná. Česká scéna bezdrátových ISP je rozdělena na dvě skupiny. Jedni vyznávají politiku platforem Ubiquiti a druzí MikroTik. V Tab. 17 jsou tedy porovnána zařízení z pohledu funkčnosti a ceny. Výkonnost není třeba porovnávat, protože se jedná o koncová zařízení.

Tab. 17 Srovnání různých platforem na frekvenci 5 GHz.

Výrobce	Typ	WMM	Proprietární QoS	Cena
MikroTik	SXT Lite5 ac	ANO	ANO	1500 Kč
Ubiquiti	LiteBeam5 ac	ANO	NE	1600 Kč
Cambium	ePMP Force 200	NE	ANO	3 300 Kč

Zařízení MikroTik mají ve výchozím nastavení WMM vypnuto a při použití proprietárního protokolu NV2 jsou aplikovány pouze dvě fronty. (MikroTik, 2017). Naproti tomu Ubiquiti má WMM ve výchozím nastavení zapnuto, ale musí být provoz předem definovaný, protože zařízení neumožňuje klasifikování a označení dat. Podle výrobce by měla být data klasifikována a roztříděna do tříd dle Tab. 18 .

Tab. 18 Třídy priorit u výrobce Ubiquiti.

802.1p Class of Service	TOS Range	DSCP Range	WME Category
0-Best-Effort	0x00-0x1f	0-7	Best-Effort
1-Background	0x20-0x3f	8-15	Background
2-Spare	0x40-0x5f	16-23	Background
3-Excellent Effort	0x60-0x7f	24-25,28-31	Best-Effort
4-Controlled Load	0x80-0x9f	32-39	Video
5-Video (<100ms latency	0xa0-0xbf	40-45	Video
6-Voice (<10ms latency)	0x68, 0xb8,0xc0-0xdf	26-27,46-47,48-55	Voice
7-Network Control	0xe0-0xff	56-63	Voice

Zdroj: Převzato od Ubnt (2015).

Bezdrátové klientské spoje od společnosti Cambium Networks (dříve Motorola Canopy) používají své proprietární QoS. Na základě DSCP nebo CoS (Class of Service) je provoz rozdělen do tří priorit – lowest, medium, highest. (Cambrium-Networks, 2016).

U bezdrátových mikrovlnných jednotek na frekvenci 10 GHz je srovnání v Tab. 19 . Hlavní rozdíl mezi zařízeními spočívá ve stabilní přenosové rychlosti. Podle diskutujících na ispforum.cz Alcoma přenese i ve špatném počasí téměř stejnou rychlost, zato Ubiquti M10 má přenosovou rychlost sníženou. Jedná se však o starší údaje. Velikost paraboly velice ovlivňuje stabilitu a přenosové rychlosti. V praxi platí čím větší tím lepší, a to z důvodu lepšího zisku antény. Spoj je odolnější vůči rušení a zvyšuje se tím potenciál do maximální propustnosti v závislosti na šířce pásma a modulaci. Je dobré si před koupí páteřního spoje propočítat, jakou přibližně parabolu je třeba aplikovat na vzdálenost spoje.

Tab. 19 Srovnání různých platforem na frekvenci 10 GHz.

Výrobce	Typ	QoS	Modulace	Cena
Alcoma	AL10D MP200	ANO	QPSK až 256QAM	94 900 Kč
Ubiquiti	PowerBridge M10	ANO	OFDM	24 494 Kč
Racom	Ray	NE	QPSK až 256QAM	65 000 Kč

Ceny spojů Alcoma a Racom jsou orientační, protože nejsou nikde zveřejněné a cena je u každého individuální. Jedná se o ceny pojítek zveřejněných na diskuz-

ních fórech. Nespornou výhodou spojů Alcoma je funkce, která při špatném počasí zvýší vysílací výkon, tím dosáhne podobných přenosových hodnot v jakémkoliv ročním období. Výrobci umožňují přenést svoje zařízení i do licenčního kmitočtu. Cena privátního kmitočtu 11 GHz stojí kolem 25 000 Kč za rok.

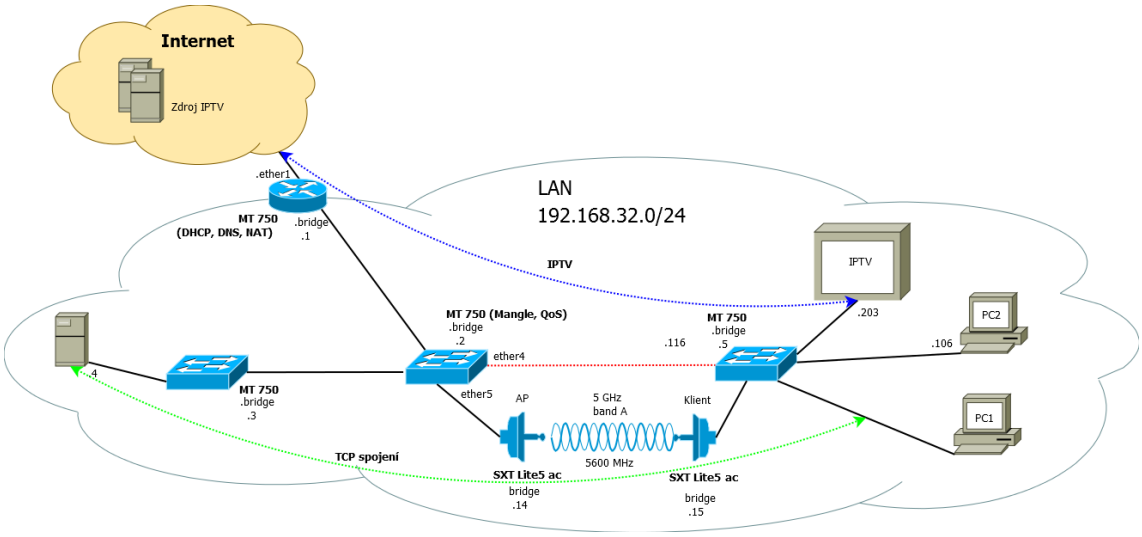
8.4 Požadavky ISP na řízení sítě

Nedostatečná šířka pásma je na bezdrátových spojích z Lesné do vesnic. Pokud má ISP poskytovat IPTV, jsou dalším slabým místem klienti připojení přes Wi-Fi. Šířka pásma AP se rozděluje rovnoměrně bez ohledu na prioritu. Při poskytování IPTV je nutnost mít IPTV pakety prioritizované před ostatním provozem.

Další potřeba poskytovatele je řízení datových toků v závislosti na poskytovaném tarifu. Na základě adresních prostorů je potřeba omezit zákazníky Speed a Mini. Veškerá práce s datovými toky musí probíhat pouze na jednom centrálním prvku. Tarif Speed je třeba omezit na rychlost 40/30 Mbps pro každého zákazníka a při nedostatečné kapacitě se bude šířka pásma rovnoměrně rozdělovat mezi uživatele tohoto tarifu. Tarif Mini by měl mít vyšší prioritu, protože menší šířka pásma je nedostačující pro běžné užití. Firma disponuje veřejnými IP adresami a dle smlouvy ji mohou využít pouze zákazníci tarifu Speed. Je tedy potřeba omezit veřejné IP stejně jako tarif Speed. Ostatní provoz jsou VLAN ISP, které kupují od firmy konektivitu.

9 Laboratoř

Laboratorní síť poskytne podmínky pro konfiguraci a testování. Výsledkem laboratorního experimentu bude obecné řešení pro problematiku s řízením bezdrátového provozu. Síť je z pohledu topologie zobrazena na Obr. 13.



Obr. 13 Topologie laboratoře.
Zdroj: Vlastní práce.

V topologickém obrázku č. 16 je zobrazena červená tečkována čára, která zobrazuje možnost připojení kabelem. Cesta je ve stavu *disable,* ale je možnost v rámci testování zaměnit cestu přes Wi-Fi za cestu kabelem. V laboratoři je připojen i souborový server a to z důvodu, že simulační data nemusí vždy odpovídat skutečnosti. Simulační data probíhají přes nástroj v RouterOS Bandwidth test nebo u PC BTest. Síť je připojena k Internetu konektivitou 100/100 Mbps. Přenosová kapacita kabelového propojení je standardu Fast Ethernet. Prvky jsou zapojeny jako *bridge*, což znamená, že všechna rozhraní v daném bridge vystupují pod jednou IP adresou. Na prvku MT 750 s bridge IP adresou 192.168.32.2 bude implementováno *Mangle* a *QoS.* Oba mechanismy jsou popsány v kapitole 6.1. Vzdálenost mezi AP a klientem je 6 m. Bezdrátový přenos funguje na standardu IEEE 802.11a. Použit je z důvodu, že poslouží k lepším testovacím informacím, které plynou z jeho menší přenosové kapacity. PC1 a PC2 pracují na operačním systému Windows 10.

10 Konfigurace

10.1 Mangle

Jak je popsáno v kapitole 6.1.1, nástroj Mangle pracuje s pakety na různých úrovních. V síti poskytovatele je třeba třídit pakety na základě multimediálních dat, tarifů, veřejných IP. Pracovat s RouterOS lze dvěma způsoby. První je přes GUI rozhraní, které poskytuje program Winbox nebo webový prohlížeč. Druhou možností je pracovat s terminálem. Z důvodu lepší přehlednosti zde budou ukázané příkazy namísto obrázků. Pokud chceme pracovat s pakety na L3 vrstvě, je potřeba zapnout funkci *Use IP Firewall*. Nutno podotknout, že zapnutí této funkce zvýší nároky na prostředky zařízení. Zapnutí provedeme příkazem:

```
/interface bridge settings set use-ip-firewall=yes
```

Už lze pracovat s funkcemi *prerouting, forward* a *postrouting*. Na příchozí provoz bude použit prerouting a na odchozí postrouting. Z důvodu ušetření nároku na zařízení bude před *mark-packet* proveden *mark-connection*.

IPTV pakety nám označuje dodavatel KukiTV a jsou označeny CS4 pro unicastový přenos dat a AF22 pro STB signalizaci. Podle Tab. 20 a Tab. 21 se jedná o decimální hodnoty 32 a 20.

Tab. 20 Skupina AF paketů.

	Class 1	Class 2	Class 3	Class 4
Low drop probability	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Med drop probability	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF11 (DSCP 36)
High drop probability	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF11 (DSCP 38)

Zdroj: Převzato od Wikipedia (2017).

Tab. 21 Skupina CS paketů.

DSCP	Binary	Hex	Decimal	Typical application	Examples
CS0 (default)	000 000	0x00	0		
CS1	001 000	0x08	8	Scavanger	Youtube, Gaming
CS2	010 000	0x10	16	OAM	SNMP, SSH
CS3	011 000	0x18	24	Signaling	SCCP, SIP
CS4	100 000	0x20	32	Realtime	TelePresence
CS5	101 000	0x28	40	Broadcast video	Cisco IPVS
CS6	110 000	0x30	48	Network control	OSPF, EIGRP
CS7	111 000	0x38	56		

Pakety jsou označené i za NATem, takže průchodem do privátní sítě neztrácejí svoji konzistenci. Identifikace a označení paketu pro Queue Tree bude následující:

```
/ip firewall mangle
add chain=prerouting dscp=32 action=mark-connection new-connection-
    mark=IPTV_C passthrough=yes
add chain=prerouting connection-mark=IPTV_C
    action=mark-packet new-packet-mark=IPTV passthrough=no
add chain=prerouting dscp=20 action=mark-connection new-connection-
    mark=IPTV_Signalizace_C passthrough=yes
add chain=prerouting connection-mark=IPTV_Signalizace_C
    action=mark-packet new-packet-mark=IPTV_S passthrough=no
```

Funkce *passthrough* značí, že i když je pravidlo provedeno, systém zkouší další pravidla. Pokud víme, že se jedná o paket IPTV, je zbytečné zkoušet další pravidla v seznamu. Další filtrování bude už pouze na základě IP adres v síti. Je vhodné si vytvořit *Address Lists* a to z důvodu možnosti budoucích měnících se požadavků. Je třeba filtrovat tarif mini, speed a veřejné IP. Následujícím příkazem na základě rozsahu vytvoříme address listy.

```
/ip firewall address-list add address=X.X.X.X list=name
```

Následná klasifikace pro odchozí a příchozí provoz bude vypadat následovně:

```
/ip firewall mangle
add chain=prerouting dst-address-list=nazev_listu action=mark-
    connection new-connection-mark=nazev_c passthrough=yes
add chain=prerouting connection-mark=nazev_c action=mark-packet new-
    packet-mark=nazev_znacky passthrough=no
add chain=postrouting src-address-list=nazev_listu action=mark-
    connection new-connection-mark=nazev_c passthrough=yes
add chain=postrouting connection-mark=nazev_c action=mark-packet
    new-packet-mark=nazev_znacky passthrough=no
```

Provoz je identifikován a roztříděn. Pro práci s datovými toky slouží v RouterOS nástroj Queue, který je popsán v kapitole 6.1.2.

10.2 Queue Tree

MikroTik podporuje několik mechanismů omezování a řízení síťového provozu. Pro omezování je nejvhodnější typ PCQ, který si na základě úpravy pcq-classifer omezí každou IP adresu a rovnoměrně rozdělí přidělenou šířku pásma. Pracovat s každou IP adresou ve WAN síti je nepraktické a časově náročné.

Ideálním modelem by mělo být prioritizování IPTV na úkor veškerého provozu. Pro souběžné poskytovatele je nutné garantovat linku pomocí *Limit At*, za kterou si platí. Tarif Mini má omezení 8/8 Mbps a snižování datového toku by už znamenalo přílišné omezení, které by zákaznici rozpoznali a mohli odejít ke konkurenci. Na druhou stranu to může být podnět k přechodu na vyšší tarif, takže tahle otázka je spíše pro manažerské pozice. Drtivá většina zákazníků využívá tarif Speed. Tento tarif využíval přístupu best-effort, který je ideální nahradit za omezení 40/30 Mbps pro každou IP zákazníka a při dosažení maximální šířky pásma rovnoměrně snižovat datový tok mezi zákazníky tarifu Speed.

RouterOS pracuje s datovými toky v mechanismu SQ (Simple Queue) nebo QT (Queue Tree). Rozdíly jsou popsány v kapitole 6.1.2. Na sofistikované řízení toku použijeme QT, který umožnuje vytvářet sdílené linky, upřednostňuje jednotlivé protokoly nebo služby běžící na určitých portech. Lze implementovat oba mechanismy naráz, je to ovšem nepraktické.

Pro jednotlivé třídy si vytvoříme PCQ, který bude omezovat každou dst IP určitou rychlostí. IPTV bude omezena rychlostí 30 Mbps z důvodu, že jeden zákazník má nárok až na dvě STB, takže při paralelním zapnutí by neměli STB dostatečnou rychlost. Pokud budeme pracovat s odchozím provozem, je třeba klasifikovat PCQ na základě src IP. V rámci laboratorní sítě nám postačí 15 Mbps. Zákaznicí na tarifu mini jsou omezování na hraničním prvku. Jedná se o dočasné řešení a je nutné připravit pro tento rozsah IP adres omezení. Zbylí zákaznici budou nahrazení za typ PCQ s rychlostí 40/30 Mbps. Ostatní ISP budou mít minimální garantovanou rychlost (Limit At). PCQ fronta má tyto vlastnosti:

- *Rate* – maximální rychlost jednotlivé IP adresy na základě klasifikátoru.
- *Limit* – velikost fronty jednotlivých sub-streamů (KiB).
- *Total Limit* – maximální množství dat ve frontě ze všech sub-streamů (KiB).
- *Burst Rate* – maximální rychlost uploudu/downloadu, kterého lze dosáhnout.
- *Burst Threshold* – hodnota po zapnuti/vypnuti burstu.
- *Burst Time* – periodické období v sekundách, ze kterého se vypočítává průměrná rychlost přenosu dat.
- *Classifier* – identifikátor sub-streamů. Zda se jedna o příchozí/odchozí provoz.

Nastavení velikosti fronty může radikálně ovlivnit výsledek při zátěži. Pokud nastavíme příliš velkou frontu, nastane obrovský delay pro cílový paket. Na druhou stranu bez fronty může nastat příliš vysoký packet loss, což má opět za následek nežádoucí účinek. V defaultním nastavení má PCQ *limit* velikost 50 KiB a *Total Limit* 2000 KiB. Je tedy vhodné otestovat, jaká je přibližně ideální velikost fronty pro danou síť. Vytvoříme fronty pro odchozí a příchozí provoz pro každou třídu, kterou jsme v Mangle klasifikovali. PCQ frontu pro IPTV vytvoříme následovně:

```
/queue type
add kind=pcq name=IPTV_D pcq-rate=15M pcq-classifier=dst-address
```

Nyní zbývá vytvořit QT a řízení provozu je implementováno. Pro jednotlivé rozhraní bude nastaven maximální limit, který je dané médium schopno přenést. Prioritní škála je v QT definována od 1-8, přičemž 1 je nejvyšší priorita. QT pro příchozí provoz lze vytvořit příkazem:

```
/queue tree
add name=DOWN_ether4 parent=ether4_Martin queue=default max-
    limit=30M
add name=IPTV parent=DOWN_ether4 packet-mark=IPTV queue=IPTV priori-
    ty=2
add name=SPEED parent=DOWN_ether4 packet-mark=SPEED queue=SPEED_DOWN
    priority=6
add name=OSTATNI parent=DOWN_ether4 packet-mark=no-mark que-
   ue=NEOMEZENO_D priority=6
```

Spojení bezdrátového spoje provedeme pouze na základě nejjednoduššího řešení. Přenos bude prozatím probíhat na standardu 802.11n a při testování bezdrátového QoS se přejde na standard 802.11a. AP s IP adresou 192.168.32.14 je připojen do rozhraní ether4_Martin a je tedy díky QT omezen na maximální přenosový limit 30Mbps. V laboratorním QT nejsou zahrnuty třídy MINI a VEREJKY z důvodu nepotřebnosti při testování.

10.3 Řízení v bezdrátových spojích

Wi-Fi systémy využívají pro řízení komunikace model WMM. MikroTik nebo Ubiquiti nabízí i proprietární řešení při použití svých protokolů. Jedná se ale pouze o jednoduchou práci s datovými toky.

10.3.1 Rádius

Aby se jednalo o centralizované řešení, na prvku 192.168.32.2 budeme příslušným paketům měnit DSCP (TOS) na hodnoty reprezentující prioritu WMM. Na AP nastavíme *set priority*, který lze nastavit ručně nebo na základě hodnot *from DSCP.* Zařízení pracující na frekvencích 2,4 a 5 GHz pracují v režimu Half duplex, takže při obrovské zátěži uploudu je celá šířka pásma využita a nezbývá pásmo pro download. Tenhle nedostatek lze vyřešit omezením přenosové rychlosti uploudu. Firma ovšem poskytuje symetrický upload/download a dle statistik je upload prakticky nezatížený. Téměř na všech AP je aplikován protokol NV2, který je popsán v kapitole 2.3.9.

Změnu v hlavičce paketů provedeme opět v Mangle. Je třeba si dát pozor, abychom nezměnili hodnotu DSCP pro IPTV před *mark-connection*. Musíme brát v úvahu, že pravidla v Mangle probíhají sekvenčně. Ve verzi firmwaru 6.38.5, který

je aplikován na všech zařízeních, je ve winboxu umožněno přesouvání jednotlivých Mangle pravidel. V některých verzích to umožněno není a je nutné dle toho přizpůsobit konfiguraci. Pro lepší výsledky měření si prioritizujeme protokol ICMP. Změnu DSCP(TOS) provedeme následujícím příkazem:

```
/ip firewall mangle
add chain=prerouting connection-mark=IPTV_C action=change-dscp new-
  dscp=5 passthrough=no
add chain=prerouting connection-mark=IPTV_Signalizace_C acti-
    on=change-dscp new-dscp=6 passthrough=no
add chain=prerouting protocol=icmp action=change-dscp new-dscp=7
    passthrough=no
```

10.3.2 NV2

NV2 pracující na TDMA přístupu je nový protokol, který je nadstavbou staršího protokolu nstreme. V základním režimu má aplikováno několik nepublikovaných nastavení, která velice ovlivňují přenos dat. Dle praktických zkušeností lépe rozděluje datové toky mezi klienty a je především vhodný pro spoje PtMP. Největší nevýhodou je zvyšování latence oproti protokolům 802.11 a nstreme.

AP je ve formě *bridge,* který disponuje IP adresou. Rozhraní Wi-Fi má následjící konfiguraci:

```
/interface wireless
set 1 mode=bridge band=5ghz-a frequency=5180 ssid=Vysilac wireless-
    protocol=nv2 country="czech republic" nv2-qos=frame-priority
    nv2-queue-count=8 tx-power=-30 tx-power-mode=all-rates-fixed
```

Protože jsme nastavili DSCP na hodnotu 7, nastavíme si *queue-count* na 8. QoS priority není defaultní, ale bude klasifikována na základě pole s prioritou rámce. Nastavit QoS lze i 2. vrstvě ISO/OSI. V záložce *bridge-filter* lze klasifikovat a rozdělit provoz bez zasáhnutí do vyšší vrstvy. Z důvodu, že chceme centralizované řešení, používáme DSCP pole, které je zabalené v hlavičce IP paketu. Musíme tedy zapnout na každém AP funkci *Use IP Firewall.* Příkaz k zapnutí je v kapitole 10.2.

Nyní je třeba nastavit obdobně rozhraní přijímacího zařízení. Výhodou je, že pokud nechceme řídit odchozí provoz, nemusíme nic dalšího nastavovat.

```
/interface wireless
set 1 mode=station-bridge band=5ghz-a/n ssid=Vysilac wireless-
    protocol=any country="czech republic" tx-power=-30 tx-power-
    mode=all-rates-fixed
```

Zbývá pouze nastavit v Mangle pravidlo, které bude na základě DSCP hodnot třídit pakety do fronty. Závěrečný krok se provede následující konfigurací:

```
/ip firewall mangle
add chain=prerouting action=change-dscp new-dscp=from-dscp
```

10.3.3 WMM

Model WWM se téměř neliší od proprietárního řešení NV2. Podle teoretické části je rozdíl především v tom, že u WMM je fronta 1 a 2 větší než defaultní 0. Konfigurace se téměř neliší a můžeme nechat stávající nastavení. Změníme pouze vysílací protokol a zapneme mechanismus WMM. Na straně AP provedeme následující konfiguraci:

```
/interface wireless
set 1 wireless-protocol=802.11 wmm-support=enable
```

Z důvodu, že v předešlé konfiguraci klienta jsme nastavovali *wireless-protocol* na *any*, klient se vždy přizpůsobí vysílacímu protokolu AP. Stačí tedy pouze zapnout WMM.

```
/interface wireless set 1 wmm-support=enable
```

11 Měření

Měření bude probíhat na základě konfigurací, které jsou popsány v předešlé kapitole. Jako první bude zvolena konfigurace s Queue Tree. Místo Wi-Fi spojení mezi prvky 192.168.32.2 a 192.168.32.5 zvolíme kabelovou cestu, která je v Obr. 13 zobrazena tečkovanou čarou.

11.1 Queue Tree

Vytvořený QT je nutné důkladně otestovat. Televize by měla mít garantovanou linku 15 Mbps bez ohledu zátěže ostatních uživatelů. Neoznačené pakety je nutné zahrnout do QT, aby i neklasifikovaný provoz v Mangle byl zahrnut pod maximální přenosový limit rozhraní. Způsob měření je popsán v kapitole 7.3.1. QT je navrhnuto i s podílem různých rozsahů, které mohou reprezentovat rychlostní tarify. Třída Speed je omezena na 23 Mbps pro každou IP. QT je zobrazeno na Obr. 14.

Name	Parent	Packet Marks	Priority	Limit At (bits...	Max Limit (b...	Avg. Rate	Queued Bytes	Bytes	Packets	Dropped
TOTAL_D	ether4_Martin		8		30M	14.3 Mbps	0 B	11.2 MiB	8 958	0
ICMP	TOTAL_D	ICMP	2	1	2	2.2 kbps	0 B	2658 B	23	0
IPTV	TOTAL_D	IPTV	2			14.1 Mbps	32.5 KiB	10.9 MiB	7 571	9
IPTV_SIGNALIZACE	TOTAL_D	IPTV_Signalizace	1	2M	5M	0 bps	0 B	0 B	0	0
OSTATNI	TOTAL_D	no-mark	7	5M	10M	262.4 kbps	0 B	316.2 KiB	1 386	0
SPEED	TOTAL_D	SPEED	6			0 bps	0 B	0 B	0	0

Obr. 14 QT v laboratorních podmínkách.
Zdroj: Vlastní práce.

U QT vidíme, že různé třídy s rozdílnou prioritou stahují příslušná data. Také můžeme vidět, kolik dat je právě ve frontě a kolik paketů daná třída zahodila (dropped).

11.1.1 Velikost fronty

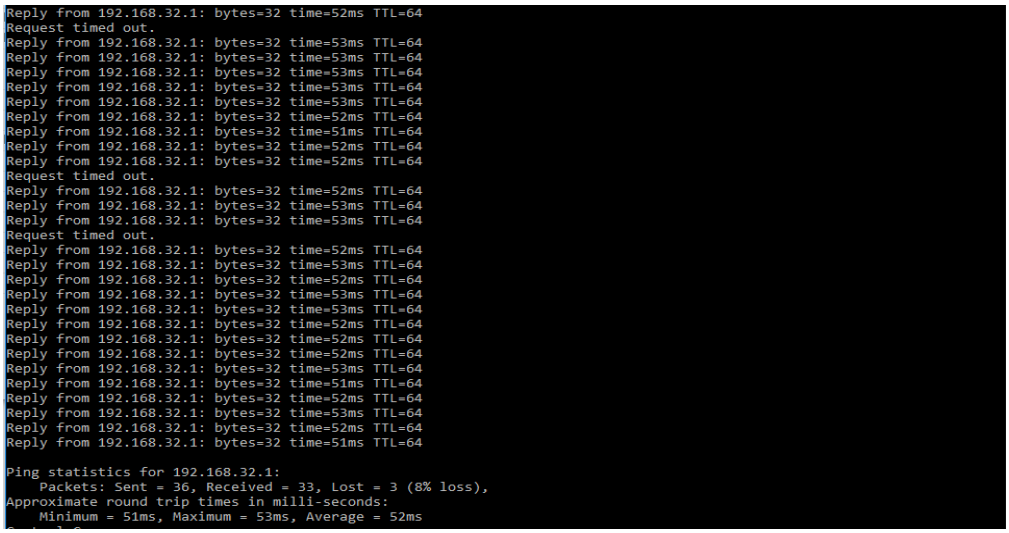
Velikost fronty je u HTB aplikována pouze u potomka. Zátěžový simulační test UDP proběhl z PC1. Fronta při zátěži ovlivňuje, jaký bude mít cílový paket delay, packet loss a jitter. Zvýšíme-li extrémně frontu (kapitola 7.3) a provedeme zatížení z PC1, dostaneme tyto výsledky:

```
Reply from 192.168.32.1: bytes=32 time<1ms TTL=64
Reply from 192.168.32.1: bytes=32 time<1ms TTL=64
Reply from 192.168.32.1: bytes=32 time=44ms TTL=64
Reply from 192.168.32.1: bytes=32 time=232ms TTL=64
Reply from 192.168.32.1: bytes=32 time=488ms TTL=64
Reply from 192.168.32.1: bytes=32 time=691ms TTL=64
Reply from 192.168.32.1: bytes=32 time=878ms TTL=64
Reply from 192.168.32.1: bytes=32 time=989ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1133ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1268ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1365ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1485ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1612ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1768ms TTL=64
Reply from 192.168.32.1: bytes=32 time=1934ms TTL=64
Reply from 192.168.32.1: bytes=32 time=2107ms TTL=64
Reply from 192.168.32.1: bytes=32 time=2307ms TTL=64
Reply from 192.168.32.1: bytes=32 time=2510ms TTL=64
Reply from 192.168.32.1: bytes=32 time=2735ms TTL=64
Reply from 192.168.32.1: bytes=32 time=2988ms TTL=64
Reply from 192.168.32.1: bytes=32 time=3233ms TTL=64
Reply from 192.168.32.1: bytes=32 time=123ms TTL=64
Reply from 192.168.32.1: bytes=32 time=32ms TTL=64
Reply from 192.168.32.1: bytes=32 time=25ms TTL=64

Ping statistics for 192.168.32.1:
    Packets: Sent = 24, Received = 24, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3233ms, Average = 1247ms
```

Obr. 15 RTT se zátěží při extrémní velikosti fronty.
Zdroj: Vlastní práce.

RTT dosahuje obrovských výsledků a pokud by se zátěžový test nezastavil, fronta by byla přeplněna a systémem FIFO zahazovala pakety. Fronta má sloužit k tomu, že i když je linka přeplněna, paket nezahodí a ponechá si ho a do cíle dorazí později v rozumném čase. RTT který je i přes několik tisíc milisekund, je v praxi horší než několikaprocentní packet loss. Při VoIP hovoru by se uživatele ani nedomluvili, protože by každý slyšel toho druhého v jiném čase. Stanovíme si tedy maximální možný RTT 55ms. Pokud by zdroj IPTV byl v dané LAN síti, mohlo by RTT být až 200 ms. Nastavíme hodnotu *Limit* na 50 KiB.



Obr. 16 RTT se zátěží při velikosti fronty 50 KiB pro jednotlivý sub-stream.
Zdroj: Vlastní práce.

Maximální delay ve frontě je 53 ms, což je ideální hodnota. *Total Limit* je třeba zvýšit ve WAN síti, kde je počet sub-streamu několikanásobně větší než v laboratorní síti.

11.1.2 QT TEST-1 (BEST EFFORT)

První test slouží k srovnání s mechanismem QoS. Zapnutý je pouze *maximální limit* rozhraní, pod který spadají všechna spojení. Ostatní konfigurace je vypnutá. Zátěžový test proběhne z PC1 pomocí reálného souboru. Spojovacím protokolem je TCP.

Tab. 22 Výsledky měření QT TEST-1 (BEST EFFORT).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 523	14321	P5+	41 056
20	9 643	14 145	P5+	37 065
30	8 700	10 203	P5+	34 161
40	9 144	9 987	P5+	28 792
50	8 100	9 203	**P4**	23 612
60	1378	8 500	**P4**	26 100
70	1650	8 930	**P4**	28 651
80	1500	8 692	**P4**	31 645
90	1983	9 671	**P4**	35 102
100	2012	9 136	**P4**	38 496
110	1293	8 148	**P4**	40 632
120	1581	9 139	**P4**	39 789

Reálný test zamezil STB, aby si načítal data tak, jak potřebuje. Propočet linky se pohybuje kolem 9 Mbps a nejvyšší profil P5+ potřebuje 10742 kbps. Po 50 vteřinách přeskočil STB na nižší profil, který není tak náročný. A až poté začal plnit svoji kapacitu v bufferu.

Při testování simulačního testu zátěž úplně degradovala komunikaci STB, který nedokázal ani propočítat novou rychlost linky, aby mohl skočit na nejnižší profil. STB je prakticky bez připojení k Internetu a během 20-30 sekund se IPTV obraz zastaví.

11.1.3 QT TEST-2 (VÝCHOZÍ)

Druhý test je výchozí a slouží k ověření správnosti konfigurace. Bez zátěžového testu naměříme tato data:

Tab. 23 Výsledky měření QT TEST-2 (VÝCHOZÍ).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 820	14 973	P5+	41 056
20	15 206	15 069	P5+	39 897
30	15 222	15 202	P5+	40 456
40	15 212	14 213	P5+	38 796
50	15 229	15 124	P5+	39 462
60	14 981	15 175	P5+	42 023
70	15 217	14 210	P5+	40 135
80	13 982	14 924	P5+	39 987
90	15 175	14 728	P5+	41 020
100	15 125	14 767	P5+	40 038
110	15 129	14 867	P5+	39 039
120	15 153	14 906	P5+	40 689

Přenos je stabilní a nemá žádné nedostatky. Lze tedy uskutečnit další testy.

11.1.4 QT TEST-3

Zátěž provedeme z PC1, který patří do třídy SPEED.

Tab. 24 Výsledky měření QT TEST-3.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	15 078	14 554	P5+	40 057
20	14 070	14 854	P5+	40 877
30	15 248	14 836	P5+	38 396
40	14 042	14 837	P5+	39 896
50	15 242	14 706	P5+	41 277
60	15 205	14 972	P5+	40 224
70	14 044	14 678	P5+	39 135
80	14 241	14 506	P5+	38 996
90	14 063	14 832	P5+	40 732
100	14 233	14 360	P5+	41 145
110	15 228	14 404	P5+	39 189
120	15 281	14 323	P5+	39 799

IPTV je naprosto stabilní při reálném zátěžovém testu pomocí spojení TCP. Prakticky nelze rozpoznat QT VÝCHOZÍ TEST-2 od QT TEST-3.

11.1.5 QT TEST-4

V tomto testu bude použita simulační zátěž UDP. Zátěž je provedena z PC1.

Tab. 25 Výsledky měření QT TEST-4.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	15 182	14 937	P5+	39 786
20	15 256	14 880	P5+	38 877
30	15 328	14 782	P5+	41 056
40	15 221	14 897	P5+	42 756
50	15 084	14 801	P5+	40 472
60	14 931	14 709	P5+	39 088
70	14 369	14 775	P5+	40 177
80	15 221	14 806	P5+	40 777
90	14 715	14 063	P5+	39 829
100	14 205	14 493	P5+	41 925
110	15 183	14 709	P5+	41 139
120	15 180	14 844	P5+	40 287

Žádný diametrální rozdíl zde není. Výsledky jsou obdobné jak u přechozích testů. Televize je stabilní a obraz nedisponuje žádnými anomáliemi.

11.1.6 QT TEST-5

Závěrečný zátěžový test je nejpřísnější. Z PC1 bude spuštěn reálný test. Z PC2 bude spuštěn simulační test. PC2 patří do třídy OSTATNÍ. Po 10 sekundách bude spuštěno STB, které nemá k dispozici žádná data v bufferu.

Tab. 26 Výsledky měření QT TEST-5.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	15 123	14 837	P5+	1080
20	15 772	15 123	P5+	4100
30	15 123	14 765	P5+	12 141
40	15 123	14 987	P5+	18 332
50	15 404	14 856	P5+	23 789
60	14 821	14 849	P5+	30 519
70	14 457	14 795	P5+	36 587
80	15 645	14 924	P5+	42 100
90	14 156	14 512	P5+	38 905
100	14 100	14 093	P5+	41 915
110	15 523	14 929	P5+	40 219
120	15 167	14 664	P5+	39 831

STB má přibližně po 70 vteřinách naplněn buffer do maximální kapacity. Pokud by IPTV byla omezena na více než 15 Mbps, proběhlo by načtení do bufferu rychleji. Můžeme ovšem konstatovat, že zatížení UDP a TCP nemá vliv na IPTV.

11.1.7 QT TEST-6 (ICMP)

STB nemá možnost testování klíčových hodnot delay, jitter a packet loss. Je ovšem nutno tyto hodnoty měřit. ICMP protokol dostane prioritu jako má IPTV. ICMP nám prokáže, jestli zátěžové testy nenarušují klíčové hodnoty IPTV. Cílová adresa ping testu je hraniční prvek laboratorní sítě.

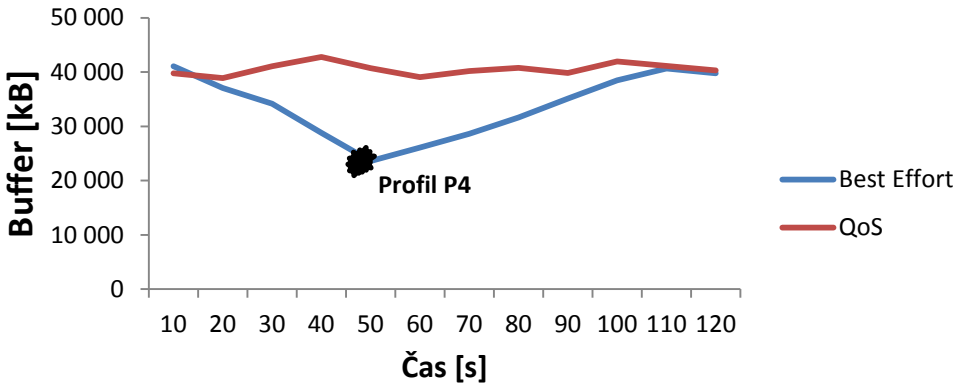
Tab. 27 Výsledky měření QT TEST-6 (ICMP).

Typ testu	Avg. RTT	Max. RTT	Packet loss
QT TEST-1 (BEST EFFORT)	2 ms	4ms	1 %
QT TEST-2 (VÝCHOZÍ)	0 ms	1 ms	0 %
QT TEST-3	1 ms	18 ms	0 %
QT TEST-4	0 ms	1 ms	0 %
QT TEST-5	0 ms	3 ms	0 %

Zátěžové testy nemají vliv na třídy s lepší prioritou. Nedochází k žádným ztrátám paketů. QT tedy pracuje dle očekávání.

11.1.8 QT Srovnání (TEST-1 vs TEST-3)

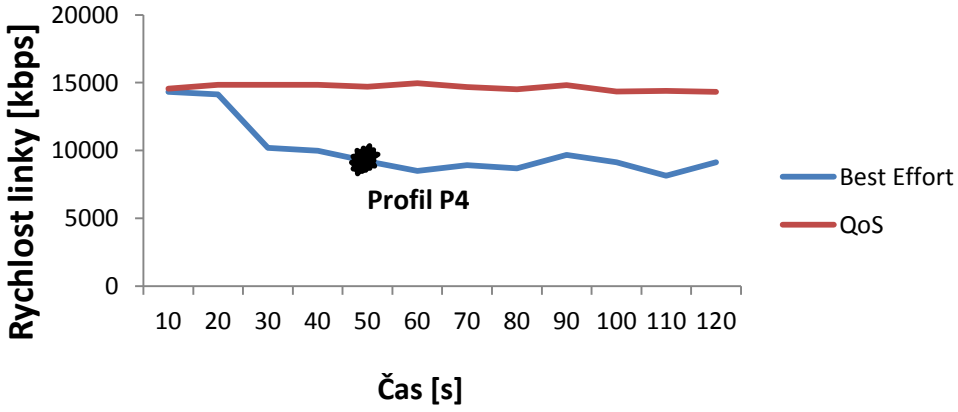
Provedeme srovnání dvou testů, které použily stejný zátěžový test. Na Obr. 17 je zobrazeno srovnání mechanismu QoS s běžným přístupem Best-Effort z pohledu kapacity bufferu.



Obr. 17 QT: srovnání z pohledu kapacity bufferu.
Zdroj: Vlastní práce.

Při aplikování QoS mechanismu prostřednictvím Queue Tree, má STB dostatek dat v bufferu i během zátěžového testu. Naproti tomu přístup Best Effort musí přeskočit na nižší profil, jinak by se obraz nakonec zastavil. Pokud by proběhla zátěž z více zařízení, muselo by STB přejít ještě na nižší profil než P4.

Na Obr. 18 vidíme jakou rychlostí STB disponuje během 2 minutového testu.



Obr. 18 QT: srovnání rychlosti linky.
Zdroj: Vlastní práce.

S nasazením QoS je stabilita rychlosti garantována na 15 Mbps. Rychlost linky je v mechanismu Best Effort nepředvídatelná a nelze předpokládat, že STB bude mít vždy dostatečnou rychlost pro načtení dat ze zdroje.

11.2 NV2

Proprietární protokol, který je popsán v kapitole 2.3.9 má vlastní QoS systém, který vychází z WMM. Konfigurace je popsána v kapitole 10.3.2. IPTV je přes portál vm.kuki.cz omezena na 15 Mbps. Přenos pracuje na 802.11a. Na prvku 192.168.32.2 jsou pakety identifikovány a dle Tab. 4 , přiřazeny hodnoty DSCP. Prioritní fronta bude mít následující podobu:

- ICMP – priorita 7
- IPTV Signalizace – priorita 6
- IPTV data – priorita 5
- OSTATNÍ – priorita 0

11.2.1 NV2 TEST−1 (BEST EFFORT)

Při tomto testu se jedná o klasické spojení PtP bez nasazení prioritních front.. Jelikož 802.11a má menší přenosovou kapacitu než FastEthernet, nemusíme nastavovat v tomto testu maximální limit pro rozhraní. Musíme ovšem konstatovat, že protokol NV2 má nepublikované funkce a nemusí se jednat přímo o mechanismus Best-Effort.

Tab. 28 Výsledky měření NV2 TEST-1 (BEST EFFORT).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 156	14 351	P5+	41 065
20	6 756	8 032	P5+	37 354
30	8 600	10 675	P5+	33 164
40	6 048	9 235	P5+	30 546
50	6 482	8 249	P5+	27 654
60	8 103	7 279	P5+	24 657
70	6 562	7 103	**P4**	23 320
80	7 958	9 873	**P4**	24 462
90	8 562	9 503	**P4**	30 564
100	10 486	10 309	**P4**	36 456
110	11 231	11 035	**P4**	38 895
120	6 806	8 830	**P4**	39 797

Výsledek testu je téměř stejný jako v kapitole 11.1.2. Poté, co je kapacita bufferu kolem 23 000 kB, tak podle rychlosti linky zvolí nižší obrazový profil. Při simulační zátěži dochází k poklesu dat v bufferu o něco rychleji a v jednom případě se profil snížil i na P3.

11.2.2 Nv2 TEST-2 (VÝCHOZÍ)

V tomto testu budeme pouze ověřovat, zda STB načítá stabilně datový tok 15 Mbps a je tedy zaručená minimální šířka pásma pro IPTV.

Tab. 29 Výsledky měření NV2 TEST-2 (VÝCHOZÍ).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 053	13697	P5+	40946
20	14 186	14468	P5+	41 798
30	14 208	13941	P5+	39472
40	13 776	14 460	P5+	38 245
50	13 797	14 100	P5+	40 109
60	15113	14372	P5+	40261
70	14154	14696	P5+	38 080
80	15106	14787	P5+	41 102
90	15127	14675	P5+	40828
100	15133	14458	P5+	42028
110	15091	14698	P5+	41319
120	14105	14698	P5+	39421

11.2.3 Nv2 TEST-3

Zátěžový test proběhne dle metodiky 7.4.1. Zátěž bude provádět PC1.

Tab. 30 Výsledky měření NV2 TEST-3.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 213	13 166	P5+	41 897
20	13 573	14 413	P5+	39 547
30	14 984	13 301	P5+	41 203
40	13 798	14 683	P5+	37700
50	14 366	13 538	P5+	40707
60	14 479	13 443	P5+	40872
70	14 267	13 306	P5+	41920
80	15 231	14 142	P5+	37595
90	14 098	13 306	P5+	38 220
100	15 097	14 389	P5+	40 568
110	15 091	13 736	P5+	38 845
120	14 139	13 851	P5+	41669

Výsledky testů dopadly výborně a STB měl během zátěže z PC1 dostatečné množství dat.

11.2.4 Nv2 TEST-4

Simulační test bývá tak náročný, že dochází až k rozpojení komunikace - často při testech na spojích, se špatnou kvalitou signálu. Nicméně i kdyby došlo k poklesu dat v bufferu, měl by si je STB dočerpat.

Tab. 31 Výsledky měření NV2 TEST-4.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14972	13541	P5+	41 262
20	14601	14715	P5+	38200
30	13705	13872	P5+	38213
40	14920	13471	P5+	36 123
50	12321	14341	P5+	40 562
60	15765	13354	P5+	37 795
70	13011	13751	P5+	39 080
80	15653	14622	P5+	39 832
90	13431	13910	P5+	41 568
100	12839	14081	P5+	37 842
110	13246	13465	P5+	39 879
120	14860	13492	P5+	38 315

Simulační test neovlivnil IPTV přenos a STB si během testu udržoval maximální kapacitu dat v bufferu. STB má stabilní rychlost linky.

11.2.5 Nv2 TEST-5

Poslední zátěžový test je nejpřísnější. PC1 bude provádět simulační test a PC2 stahovat data ze souborového serveru. Výsledky jsou zaznamenány v tabulce Tab. 32 .

Tab. 32 Výsledky měření NV2 TEST-5.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 003	13 879	P5+	174
20	15 006	13820	P5+	5678
30	13 971	13802	P5+	12 234
40	14 623	13803	P5+	17 652
50	14 624	13622	P5+	21 234
60	13984	13770	P5+	25 567
70	13 242	14770	P5+	31 567
80	11 227	13661	P5+	37 789
90	14040	13736	P5+	40 678
100	12170	13124	P5+	42 675
110	15 262	14423	P5+	40 357
120	13 657	14443	P5+	39 789

Při jednom ze čtyř testů byla na obrazovce vidět anomálie ve tvaru kostiček. Trvala 1-2s. Tato anomálie však mohla být způsobena STB zařízením nebo chybou někde po cestě ke zdroji dat.

11.2.6 Nv2 TEST-6 (ICMP)

Při špatné kvalitě signálu mezi AP a klientem často dochází k rozpojení komunikace, která má velmi negativní vliv na kvalitu přenosu. Dalším špatně odhalitelným jevem způsobujícím nekvalitní bezdrátový přenos je interference signálu z různých zdrojů (např. lednička, mikrovlnná trouba, atd.). V laboratoři před vyladěním Wi-Fi spoje docházelo také ke ztrátě dat. Např. protokol NV2 měl při zatížení maximální šířky pásma až 26 % packet loss. Je tedy nutné znát teorii bezdrátové komunikace, která je popsána v kapitole 2.

Výsledky zapnutého ICMP protokolu při testech jsou zobrazeny v tabulce 20. Jedná se o průměrné hodnoty během čtyř opakujících se měření.

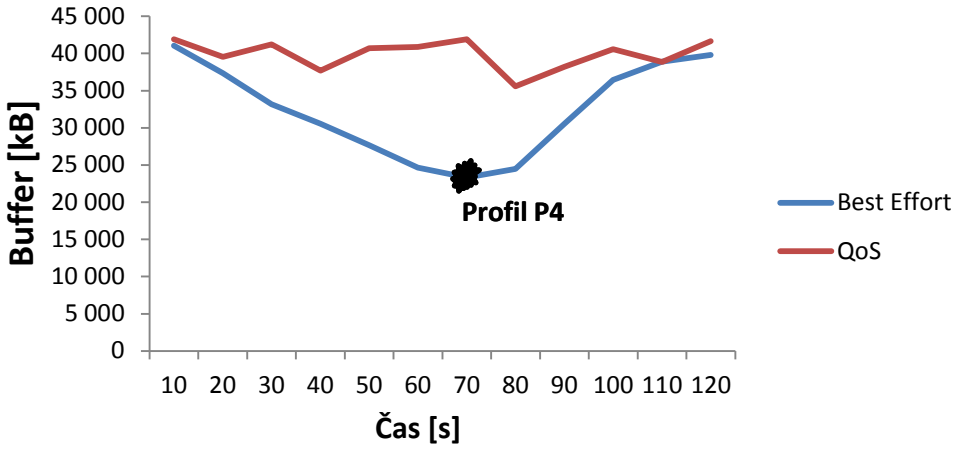
Tab. 33 Výsledky měření NV2 TEST-6 (ICMP).

Typ testu	Avg. RTT	Max. RTT	Packet loss
QT TEST-1 (BEST EFFORT)	10 ms	27 ms	1 %
QT TEST-2 (VÝCHOZÍ)	5 ms	12 ms	0 %
QT TEST-3	5 ms	12 ms	0 %
QT TEST-4	8 ms	18 ms	0 %
QT TEST-5	7 ms	19 ms	0 %

Jedná se o naprosto stabilní spojení. Nicméně přenos je uskutečněn v laboratorních podmínkách, které jsou často v realitě nedosažitelné z důvodu rušení nebo jiných vnějších faktorů. Lze konstatovat, že protokol NV2 splnil očekávání a dokáže prioritizovat provoz před druhým a je zároveň stabilní. I při testování přísného VoIP hovoru by tyto výsledky byly dostačující. Podle Cioary a Valentineho (2012) jsou doporučené hodnoty hlasových služeb následující: delay do 130 ms, jitter do 30 ms, packet loss do 1 % a šířka pásma závisí na kodeku.

11.2.7 NV2 Srovnání (TEST-1 vs TEST-3)

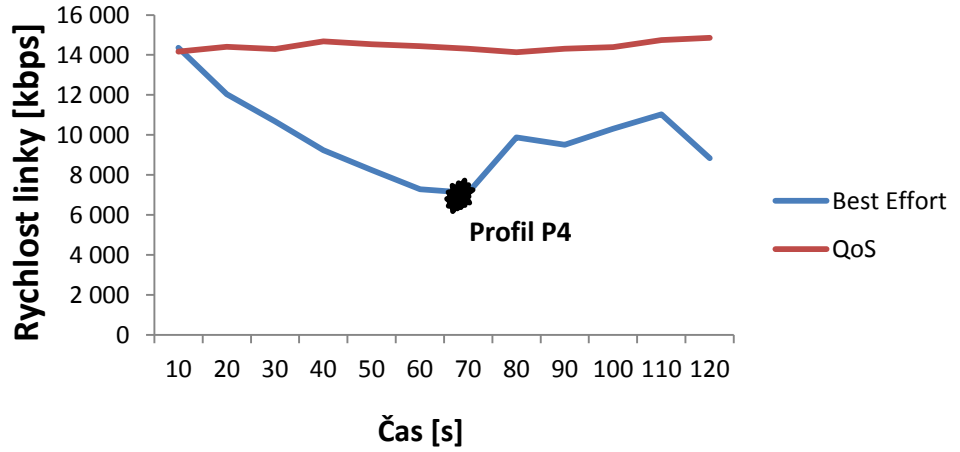
Na základě výsledků z kapitoly 11.2.2 a 11.2.5 si graficky srovnáme přínos QoS systému s běžným přístupem Best Effort.



Obr. 19 NV2: srovnání z pohledu kapacity bufferu.
Zdroj: Vlastní práce.

Výsledky jsou velice podobné z kapitoly 11.1.8. Nejvyšší profil má příliš vysoké požadavky na provoz a v závislosti na rychlosti linky musí přejít na profil P4.

Srovnání rychlosti linky před nasazením a po nasazení QoS systému je zobrazen na Obr. 20.



Obr. 20 NV2: srovnání rychlosti linky.
Zdroj: Vlastní práce.

Rychlost linky je diametrálně odlišná. Proprietární QoS systém protokolu NV2 poskytuje oproti systému Best Effort stabilní přenosovou rychlost.

11.3 WMM

Model WMM lze použít u MikroTiku při aplikování protokolu 802.11. Jedná se o obecný model, který je nadstavbou složitějšího standardu 802.11e. Konfigurace probíhá stejným způsobem jako u protokolu nv2. Priorita vychází z Tab. 4 .

11.3.1 WMM TEST-1 (BEST EFFORT)

V tomto testů je zátěž bez podpory WMM. Test je obdobný jak u NV2.

Tab. 34 Výsledky měření WMM TEST-1 (BEST EFFORT).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	13 221	12 899	P5+	42 212
20	5 157	4 432	P5+	35 458
30	6 598	4 230	P5+	30 879
40	7 428	6 059	P5+	26 789
50	5 128	4 688	**P3**	21 578
60	5 232	6 159	**P3**	23 879
70	6 189	5 722	**P3**	28 752
80	5 375	5 897	**P3**	32 878
90	5 898	4 856	**P3**	35 789
100	4 212	4 028	**P3**	36 824
110	4 138	3 845	**P3**	39 789
120	5 128	4 238	**P3**	39 697

Při běžném spojení bez podpory WMM, je při zátěži STB přinucen přejít na profil P3. U testování UDP protokolu nemá ani STB možnost přepočítat linku a je prakticky odpojen od zdroje dat.

11.3.2 WMM TEST–2 (VÝCHOZÍ)

Tab. 35 Výsledky měření WMM TEST-2 (VÝCHOZÍ).

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	13008	13894	P5+	42678
20	14569	14399	P5+	40298
30	14355	14095	P5+	39420
40	14241	14152	P5+	42029
50	14589	14389	P5+	38389
60	14658	13978	P5+	39652
70	14378	14343	P5+	41078
80	14427	14436	P5+	42008
90	14263	14349	P5+	40632
100	14275	14349	P5+	38765
110	14415	14375	P5+	38725
120	14357	14371	P5+	40272

11.3.3 WMM TEST-3

Tento zátěžový TCP test proběhne z PC1.

Tab. 36 Výsledky měření WMM TEST-3.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	14 623	14 322	P5+	39 452
20	13 607	14 276	P5+	37 165
30	11 060	12 567	P5+	38 752
40	14 319	13 953	P5+	39 421
50	12 035	13 233	P5+	36 485
60	11 727	21 960	P5+	37 984
70	11 832	13 215	P5+	39 752
80	11 879	12 683	P5+	36 482
90	12 813	12 039	P5+	39 422
100	11 777	12 468	P5+	40 821
110	14 631	12 807	P5+	41 582
120	12 587	13 092	P5+	38 423

STB nemá stabilní datový tok jako u Nv2. Rychlost linky se nedrží na garantovaných 15 Mbps, ale buffer je téměř pořád plný. Rozdíl mezi TEST-1 a TEST-3 při stejných podmínkách je značný.

11.3.4 WMM TEST-4

V tomto scénáři testu půjde o simulační zatížení přes protokol UDP.

Tab. 37 Výsledky měření WMM TEST-4.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	15452	14327	P5+	39654
20	12344	12976	P5+	37575
30	12500	12607	P5+	41248
40	12475	11863	P5+	41600
50	12957	12567	P5+	38123
60	12916	12930	P5+	36792
70	12044	12970	P5+	41586
80	13940	12176	P5+	40679
90	11100	12136	P5+	39782
100	12040	12934	P5+	39452
110	11954	12944	P5+	37892
120	11023	11031	P5+	40234

Zjistili jsme, že naměřené hodnoty jsou velice podobné jako u TEST-3. STB nedostává potřebný datový tok. Buffer se i přesto drží na plné kapacitě.

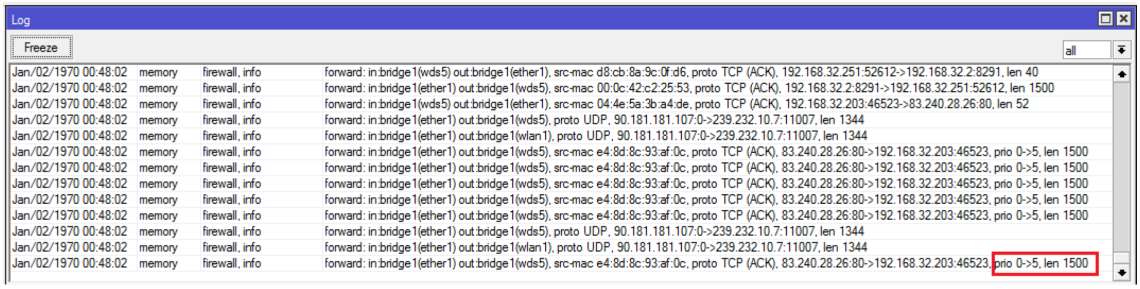
11.3.5 WMM TEST-5

V tomto testu proběhne zátěž z PC1 i PC2. Pokud dokáže STB dosáhnout maximálního bufferu s nejvyšším profilem, jedná se o test úspěšný. Naměřená data jsou v Tab. 38 .

Tab. 38 Výsledky měření WMM TEST-5.

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	8 135	9 505	**P4**	3 123
20	10 698	9 123	**P4**	8 246
30	8 432	9 218	**P4**	13 789
40	8 978	9 278	**P4**	18 979
50	9 423	8 532	**P4**	23 789
60	8 513	8 427	**P4**	27 462
70	9 135	9 072	**P4**	32 987
80	8 635	8 732	**P4**	36 752
90	8 982	9 189	**P4**	40 978
100	9 452	8 579	**P4**	39 725
110	8 578	8 975	**P4**	39 779
120	8 453	8 998	**P4**	40 892

STB po výpočtu rychlosti linky začal pracovat okamžitě na nižším profilu. Navíc průměrná rychlost se v tomto testu snížila. Při zapnutí WMM spoj rozděluje data rovnoměrně podle počtu spojení. Pokud proběhne zátěž z PC1, rychlost se rozdělí rovnoměrně mezi počítač a IPTV. Pokud zátěž přichází z více zařízení, rychlost STB se opět sníží, protože se o šířku pásma dělí s dalšími relacemi. Pokud by veškerá komunikace proběhla na stejné prioritě, rozdělování šířky pásma zajišťuje mechanismus SFQ. (popsán v kapitole 6.1.2) Je tedy třeba ověřit, zda jsou datové toky IPTV prioritizované.



Obr. 21 WMM nastavení priority - log.
Zdroj: Vlastní práce.

Jak můžeme vidět na Obr. 21, pakety IPTV mají prioritu 5. Ostatní pakety patří do fronty 0. ICMP protokol, který má prioritu 7, funguje dle očekávání. Rozdíl je zobrazen v Tab. 39 .

Tab. 39 Prioritizace protokolu ICMP.

Typ	Avg. RTT	Max. RTT	Packet loss
ICMP priorita 0	72 ms	173 ms	4 %
ICMP priorita 7	2 ms	9 ms	0 %

Rozdíl je značný. Nejen v packet loss, ale především v RTT. Prioritizace ICMP protokolu pracuje dle očekávání.

Identifikace na základě více údajů (protokol, port, IP) v Mangle neměla také žádný efekt. Celkově lze shrnout snahu o změnu fungování WMM následovně:

1. Identifikace na základě více údajů.
2. Změna firmwarů.
3. Komunikace AP a klienta na základě IP adresy rozhraní. (bez bridge).
4. Různé kombinace spojení (station bridge, stadion, station WDS).
5. Příspěvky ve fórech.
6. Přednášky MUM (MikroTik User Meeting).
7. Odeslání emailu výrobci.

Mnoho Wi-Fi poskytovatelů WMM mechanismus nevyužívá a bylo nalezeno pouze pár diskuzních témat, která se konfigurací WMM modelu zabývají. Jednalo se však o příspěvky několik let staré.

11.3.6 WMM TEST-6 (ICMP)

Protokol 802.11 má obecně lepší RTT než NV2. Výsledky ICMP protokolu při zátěžových testech je srovnány v Tab. 40 .

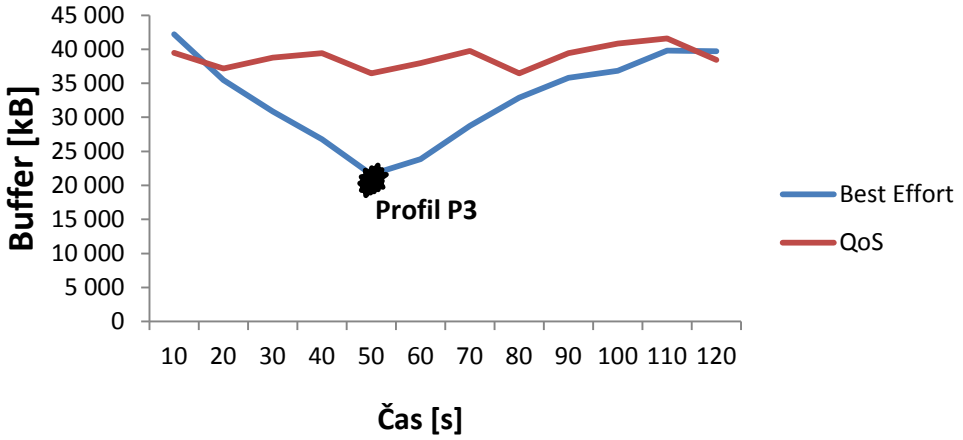
Tab. 40 Výsledky měření WMM TEST-6 (ICMP).

Typ testu	Avg. RTT	Max. RTT	Packet loss
QT TEST-1 (BEST EFFORT)	54 ms	750 ms	1 %
QT TEST-2 (VÝCHOZÍ)	0 ms	1 ms	0 %
QT TEST-3	3 ms	15 ms	0%
QT TEST-4	3 ms	8 ms	0%
QT TEST-5	4 ms	12 ms	0 %

Oproti protokolu NV2 je průměrný RTT nižší. Ovšem oba protokoly pracují na jiných přístupech k médiu.

11.3.7 WMM Srovnání (TEST-1 vs TEST-3)

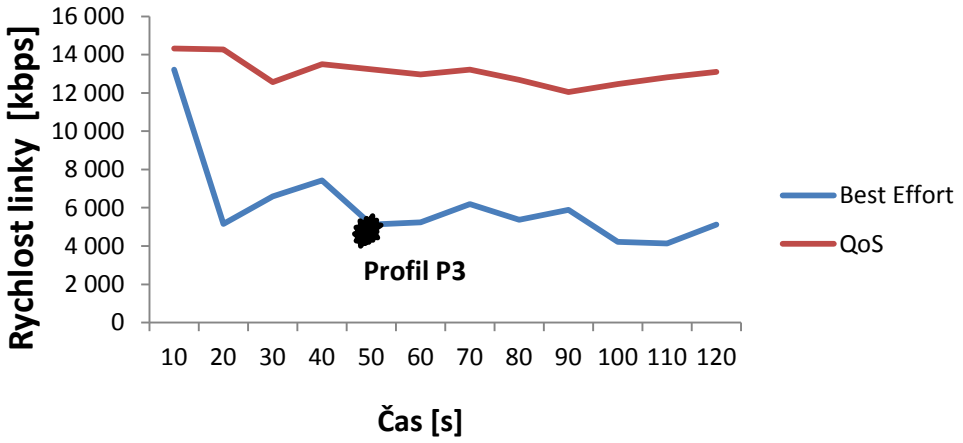
V této kapitole srovnáme WMM při jeho nasazení a při jeho absenci. Graficky je zobrazeno toto srovnání z pohledu velikosti bufferu na Obr. 22.



Obr. 22 WMM: srovnání z pohledu kapacity bufferu.
Zdroj: Vlastní práce.

U vysílacího protokolu 802.11 s absencí WMM musel STB přepnout až na profil P3. Při zapnutí WMM je buffer téměř vždy v plné kapacitě.

Pokud STB přepne na profil P3, musí být rychlost linky velice nízká. Požadavky na profil P3 jsou 4–4,5 Mbps. Srovnání rychlosti linky STB je zobrazen na Obr. 23.



Obr. 23 WMM: srovnání rychlosti linky.
Zdroj: Vlastní práce.

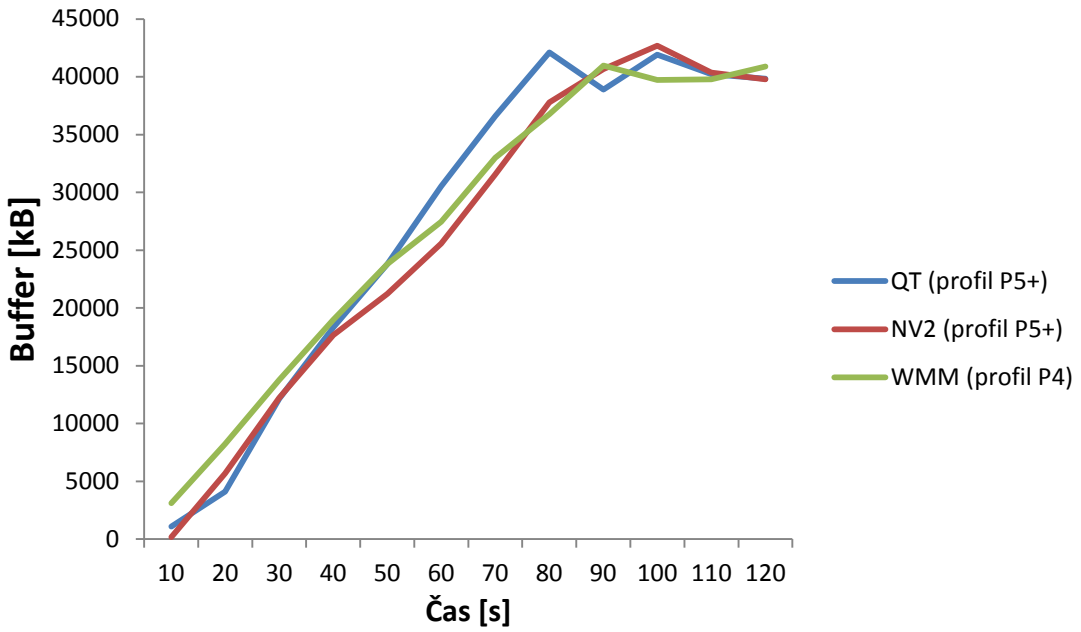
Absence modelu WMM je značná. STB si nedokáže udržovat stabilně rychlost linky a musí přepnout obraz až na profil P3. Při aplikaci WMM je rychlost stabilní kolem 13-14 Mbps. Je to ovšem z důvodu, že zatížení proběhlo pouze z PC1 a šířka pásma, která se pohybuje kolem 28 Mbps, je rovnoměrně rozložena mezi obě relace. WMM provoz rovnoměrně rozděluje, ale netřídí dle priority.

12 Výsledky

V této kapitole budeme srovnávat naměřené výsledky z kapitoly 11. Na základě výsledků zvolíme optimální řešení pro různé oblasti problematiky.

12.1 TEST-5 srovnání

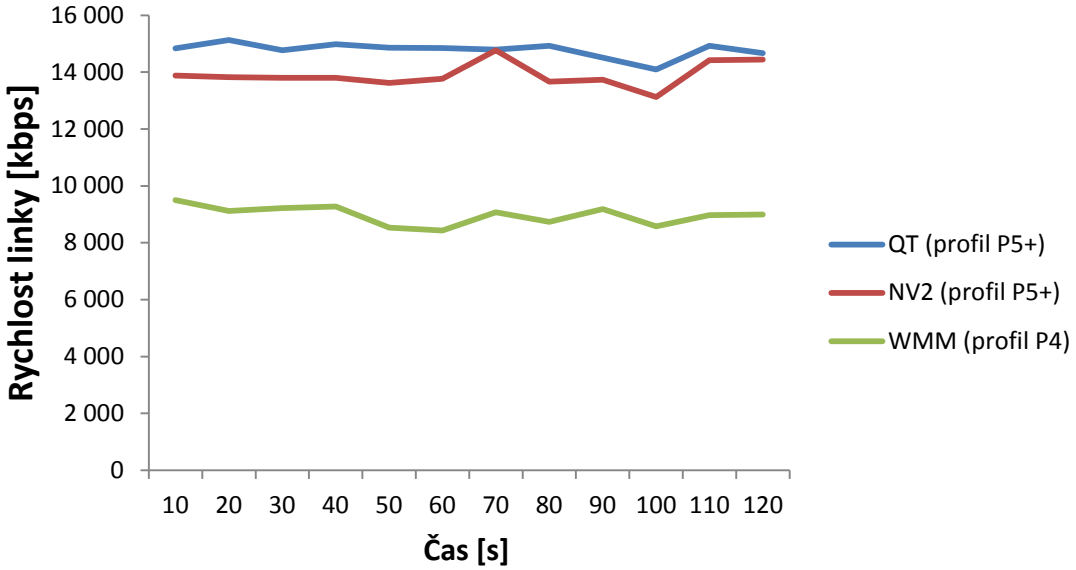
Jedná se o nejpřísnější test, který měl prokázat resistenci mechanismu QoS proti maximální zátěži média. Srovnání QT, NV2 a WMM z pohledu velikosti bufferu je zobrazeno na Obr. 24.



Obr. 24 Srovnání QT, NV2 a WMM z pohledu velikosti bufferu.
Zdroj: Vlastní práce.

Nejrychleji načetl data do bufferu QT. NV2 a WMM načetly do bufferu data přibližně stejnou rychlostí. Nutno však podotknout, že při konfiguraci WMM použil STB od počátku profil P4, který má téměř dvojnásobně nižší požadavky na profil než P5+.

Srovnání všech konfigurací z pohledu rychlosti linky pro STB je zobrazeno na Obr. 25.



Obr. 25 Srovnání QT, NV2 a WMM z pohledu rychlosti linky.
Zdroj: Vlastní práce.

Nejlepší výsledky dosahuje QT, který si udržuje stabilně 15 Mbps. Bezdrátové řešení QoS dopadlo také velice dobře. Nejslabším mechanismem je WMM, který neposkytl dostatečnou rychlost STB při zátěžích z PC1 a PC2.

12.2 TEST-6 (ICMP) srovnání

Protokol ICMP monitoroval při zátěžových testech stabilitu bezdrátového spoje. Při aplikacích typu VoIP je stabilita stejně důležitá jako garantovaná šířka pásma. IPTV od firmy Smart Comp a.s. nemá nikde publikované podmínky stability. Dle testů, které nejsou v práci publikované, zvládla IPTV i 20 % packet loss s průměrným RTT 100 ms. Vyšší ztrátovost už způsobuje obrazové anomálie nebo STB nestíhá načítat data do bufferu. Ovšem za předpokladu, že STB má omezenou datovou prostupnost 15 Mbps. Srovnání QT, NV2 a WMM stability při TEST-6 je zobrazeno v Tab. 41 .

Tab. 41 Srovnání stability prostřednictvím protokolu ICMP.

Konfigurace	Avg. RTT	Max. RTT	Packet loss
QT	0 ms	3 ms	0 %
NV2	7 ms	19 ms	0 %
WMM	4 ms	12 ms	0 %

Nejhorší avg. RTT má protokol NV2. Plyne to z jeho TDMA přístupu. Kabelové řešení QT, které lze implementovat i na bezdrátové spoje, má nejlepší RTT. Výhodou řešení kabelového QT je, že i v jiných prostředích má podobné výsledky, pro-

tože nepodléhá vnějším faktorům (počasí, rušení). Všechny testované mechanismy mají v laboratoři výborné výsledky stability a rozdíly jsou prakticky nepatrné, které běžný uživatel nepozná.

12.3 Obrazová kvalita

Obrazová kvalita a jeho plynulost je jediným aspektem, který běžného uživatele zajímá. Na Obr. 26 je zobrazeno srovnání obrazové kvality při použití QoS mechanismu NV2 proti přístupu Best Effort. Jedná se o obrazovou kvalitu při zátěžových testech z kapitoly 11.2.1a 11.2.3.

Obr. 26 Srovnání QoS a Best Effort z pohledu obrazové kvality.
Zdroj: Vlastní práce.

Jak lze rozpoznat, tak první 3 snímky jsou bez QoS. První 2 snímky jsou na nižším profilu (P4). U snímků č. 3 dochází k přechodu na profil P3, kdy uživatel přijde 1-2 sekundy o obraz. Zbylé snímky jsou s mechanismem QoS. Obraz má nejvyšší možnou kvalitu a nedochází k žádným anomáliím.

12.4 Shrnutí

Pro poskytování IPTV z hlediska řízení bezdrátového provozu je na základě výsledků nejlepší mechanismus QT. Jeho funkcionalita byla testována na kabelovém spojení, ale i na bezdrátovém (výsledky nejsou publikované). QT pracuje především na základě maximálních limitů, podle kterých pak rozděluje linku dle potřeb. Nevýhoda vzniká, pokud spojení není stabilní a v závislosti na vnějších faktorech mění svoji přenosovou kapacitu. Pokud spojení podléhá vnějším faktorům a nedokáže si udržet stabilní přenosovou kapacitu, je lepší využít mechanismy NV2 nebo WMM. Celkově lze každý mechanismus implementovat do různých podmínek.

12.4.1 QT

Je naprosto vhodný pro řízení provozu z různých hledisek požadavků. Dá se aplikovat na bezdrátové spoje PtP, kdy si na základě stabilní přenosové rychlosti stanovíme maximální limit pro rozhraní a dle kapacity třídíme provoz podle priority.

12.4.2 NV2

Proprietární protokol firmy MikroTik, který funguje při kvalitním spojení nadstandardně. Lze aplikovat na spojích PtMP a lze ho řídit centrálně na základě DSCP hodnot. Nevýhodou je, že bezdrátový QoS systém může být aplikován pouze mezi MikroTik platformami.

12.4.3 WMM

Obecný model QoS systému, který rozšiřuje 802.11e. Tento model se pro poskytování IPTV neosvědčil. Nicméně jeho rozdělování datových toků na základě relací je vhodné pro spoje PtMP. Na rozdíl od protokolu NV2 má nižší odezvu a dokáže pracovat i se zařízeními od jiných výrobců.

12.4.4 Ostatní

Mnoho bezdrátových výrobců poskytuje svoje proprietární řešení QoS. V teoretické části v kapitole 2.3.10 je popsán proprietární protokol airMAX, který funguje stejně jako NV2 na TDMA přístupu a pracuje pouze mezi platformami od firmy Ubiquti. Svoje proprietární řešení mají i spoje Alcoma, které prioritizují provoz na základě DSCP hodnot.

13 Návrh řešení – implementace

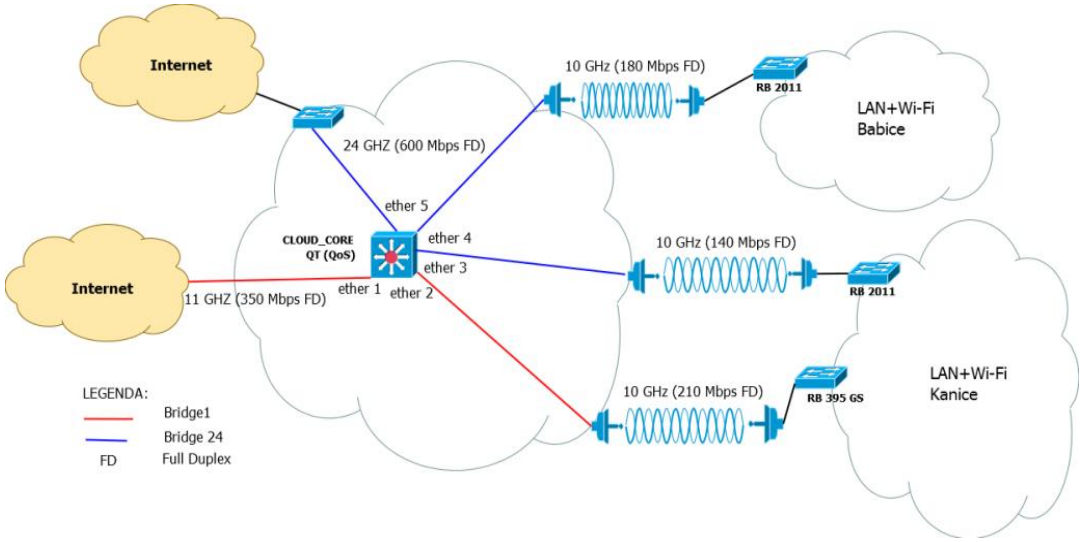
QoS mechanismus není potřeba nasazovat tam, kde je dostatečná šířka pásma. Po analýze z kapitoly 8 je nedostatečná šířka pásma na bezdrátových spojích do vesnic a na AP, které ve vesnicích vysílají. Síť trápí i omezování klientů podle různých tarifů. Celkově lze navrhnout dvě varianty provozu.

1. Na hraničním prvku sítě
2. Na CLOUD_CORE prvku na Lesné.

První varianta je všeobecně nejpoužívanější. V QT probíhá omezení a v Mangle se připraví DSCP hodnoty pro bezdrátové spoje. Na základě DSCP hodnot pouští AP prioritní provoz. Tato varianta je velice náročná na prostředky hraničního prvku, který plní mimo jiné další důležité funkce. Hraniční prvek ve firmě TS–Hydro má během večerního provozu vytížený procesor kolem 30 % a přidání dalších úkolů by mohlo být kritické.

Druhá varianta je nasazení řízení provozu na CLOUD_CORE prvek, který má lepší hardwarové specifikace. Před tímto intermediálním prvekem nejsou připojení žádní klienti. Další možností je vyměnit hraniční prvek za CLOUD_CORE. Tato změna by ale znamenala internetový výpadek pro celou síť a nutnost překonfigurování funkci z hraničního prvku na CLOUD_CORE.

Nejlepší a nejjednodušší variantou je implementovat veškeré řízení provozu na CLOUD_CORE. Pomocí QT se omezí adresní rozsahy na základě požadavků sítě z kapitoly 8.4. Maximální limit QT pro jednotlivé rozhraní bude definováno reálnou přenosovou kapacitou spoje do vesnice. Prioritu IPTV paketům pro AP nastavíme na CLOUD_CORE v Mangle na základě DSCP (TOS) hodnot. Vysílacím protokolem AP bude NV2. Kabelová LAN síť ve vesnicích má šířku pásma naprosto dostačují. Hlavní spoje mají přenosovou kapacitu 1 Gbps a konektivita zákazníků je 100 Mbps ve full duplexním režimu. Z pohledu topologie je návrh řešení zobrazen na Obr. 27.



Obr. 27 Návrh řešení z topologického pohledu.
Zdroj: Vlastní práce.

V topologickém návrhu jsou kvůli lepší přehlednosti vynechány spoje 24 GHz a 11 GHz. Konektivita z jednotlivých lokací je oddělena formou *bridge*, který funguje dost podobně jak VLAN, takže nevznikají v síti smyčky.

13.1 Konfigurace

Na základě znalostí z kapitoly 10 sestavíme sekvenci příkazu v poznámkovém bloku, kterou nakopírujeme do Terminálu CLOUD_CORE prvku. Omezení rychlost proběhne na základě PCQ mechanismu pro každou IP adresu. Před vytvořením konfiguračních příkazů musíme zahrnout podmínky ISP, které jsou pro příchozí provoz následující:

- priorita 1 – STB signalizace, rychlost 2 Mbps
- priorita 3 – data IPTV, rychlost 30 Mbps
- priorita 4 – technická PC, rychlost unlimited Mbps
- priorita 5 – tarif Mini, rychlost 8 Mbps
- priorita 6 – tarif SPEED, VEŘEJNE IP, 40 Mbps
- priorita 7 – ostatní ISP s nastavením *Limit At,* rychlost na základě smlouvy

U odchozího provozu nemusíme zahrnovat data IPTV. Jeho forma je následující:

- priorita 1 – STB signalizace, rychlost 2 Mbps
- priorita 4 – technická PC, rychlost unlimited Mbps
- priorita 5 – tarif Mini, rychlost 8 Mbps

- priorita 6 – tarif SPEED, VEŘEJNE IP, 30 Mbps
- priorita 7 – ostatní ISP s nastavením *Limit At,* rychlost na základě smlouvy

Z této hierarchie bude vycházet každé rozhraní. Pro AP je třeba nastavit hodnoty DSCP, podle kterých budou prioritizovat provoz. Struktura provozu vychází z Tab. 4 . V Mangle identifikujeme příslušné pakety a přenastavíme jejich hodnotu. I když Wi-Fi spoje na frekvencích 5 GHz pracují v režimu Half duplex, budeme prioritizovat pouze příchozí provoz. Forma priority je následující:

- priorita 7 – STB signalizace.
- priorita 5 – data IPTV.
- priorita 0 – ostatní provoz.

Na AP, které bude poskytovat IPTV, je třeba zapnout *Use IP Firewall* a v Mangle nastavit *set priority* a místo manuálního nastavení zvolíme *from DSCP.*

13.2 Implementace

Vytvořené příkazy v poznámkovém bloku (v příloze) nakopírujeme do Terminálu v nočních hodinách. Před nakopírováním příkazů je vhodné použít funkci *Safe Mode*, která zajistí, že při případném odpojení z konfiguračního prostředi, vrátí nastavení do původního stavu. Pokud provoz funguje i nadále, je nutné řešení otestovat a verifikovat. Část implementace QT v síti ISP je zobrazena na Obr. 28.

	Name	Parent	Packet Marks	Queue Type	Priority	Limit At...	Avg. Rate	Queued Bytes	Bytes	Dropped	PCQ Queues
—	B										
	B_SEVCIK_DOWN	ether4_Alcoma_Babice_180		default-small	7		107.6 Mbps	0 B	35.6 GiB	0	
	B_IPTV_SEV	B_SEVCIK_DOWN	IPTV	DOWN_IPTV	3		13.5 Mbps	7.4 KiB	6.9 GiB	46	5
	B_IPTV_SIGALIZACE_SEV	B_SEVCIK_DOWN	IPTV_SIGNALIZACE	DOWN_IPTV_SIGNALIZACE	1		4.8 Mbps	0 B	175.1 MiB	53	7
X	B_MINI_SEV	B_SEVCIK_DOWN	MINI_DOWN	DOWN_MINI	5		0 bps	0 B	0 B	0	
	B_NEOMEZENO_SEV	B_SEVCIK_DOWN	NEOMEZENO_DOWN	DOWN_NEOMEZENO	4		136 bps	0 B	94.5 KiB	0	1
	B_OSTATNI_SEV	B_SEVCIK_DOWN	no-mark	default-small	7	120M	39.1 Mbps	0 B	18.4 GiB	0	77
	B_SPEED_SEV	B_SEVCIK_DOWN	SPEED_DOWN	DOWN_40Mbps	6		39.9 Mbps	0 B	7.8 GiB	30	42
	B_VEREJKY_SEV	B_SEVCIK_DOWN	VEREJKY_DOWN	DOWN_40Mbps	6		10.0 Mbps	0 B	2349.3 MiB	9	2
	B_SEVCIK_UP	ether5_X2_Bridge_24GHZ		default-small	7		12.0 Mbps	0 B	2833.9 MiB	0	
	BU_IPTV_SIGNALIZACE_SEV	B_SEVCIK_UP	IPTV_SIGNALIZACE	UP_IPTV_SIGNALIZACE	1		0 bps	0 B	0 B	0	
X	BU_MINI_SEV	B_SEVCIK_UP	MINI_UP	UP_MINI	5		0 bps	0 B	0 B	0	
	BU_NEOMEZENO_SEV	B_SEVCIK_UP	NEOMEZENO_UP	UPLOUD_NEOMEZENO	4		136 bps	0 B	62.0 KiB	0	1
	BU_OSTATNI	B_SEVCIK_UP	no-mark	default-small	7	120M	9.6 Mbps	0 B	2127.2 MiB	4	
	BU_SPEED_SEV	B_SEVCIK_UP	SPEED_UP	UPLOUD_30Mbps	6		1888.9 kbps	0 B	552.3 MiB	0	87
	BU_VEREJKY_SEV	B_SEVCIK_UP	VEREJKY_UP	UPLOUD_30Mbps	6		518.7 kbps	0 B	154.2 MiB	0	7
—	K										
	K_BYTOVKA_DOWN	ether2_Alcoma_Kanice_220		default-small	7		174.9 Mbps	0 B	39.3 GiB	0	
	K_IPTV_BYT	K_BYTOVKA_DOWN	IPTV	DOWN_IPTV	3		8.7 Mbps	0 B	3772.1 MiB	52	6
	K_IPTV_SIGNALIZACE_BYT	K_BYTOVKA_DOWN	IPTV_SIGNALIZACE	DOWN_IPTV_SIGNALIZACE	1		6.7 Mbps	0 B	80.6 MiB	0	5
X	K_MINI_BYT	K_BYTOVKA_DOWN	MINI_DOWN	DOWN_MINI	6		0 bps	0 B	0 B	0	
	K_NEOMEZENO_BYT	K_BYTOVKA_DOWN	NEOMEZENO_DOWN	default	4		10.1 kbps	0 B	459.5 MiB	66 059	3
	K_OSTATNI_BYT	K_BYTOVKA_DOWN	no-mark	default	7	60M	49.6 Mbps	0 B	8.6 GiB	4 985	285
	K_SPEED_BYT	K_BYTOVKA_DOWN	SPEED_DOWN	DOWN_40Mbps	6		88.8 Mbps	0 B	19.9 GiB	32 167	67
	K_VEREJKY_BYT	K_BYTOVKA_DOWN	VEREJKY_DOWN	DOWN_40Mbps	6		21.0 Mbps	0 B	6.6 GiB	7 983	13
	K_BYTOVKA_UP	ether1_Alcoma_Cejl_350		default-small	7		3.1 Mbps	0 B	863.0 MiB	0	

Obr. 28 QT v ISP síti.
Zdroj: Vlastní práce.

Jak lze z obrázku vidět, datové toky jsou roztříděny do tříd. Součet všech datových toků tříd spadá pod HTB předka, který má definovaný maximální limit pro rozhraní. Když dojde kapacita, jsou datové toky rozděleny na základě priority a *Limit At*. Při řízení odchozího provozu je rodičem rozhraní, ze kterého paket opouští zařízení. U QT lze vidět, že za signalizaci IPTV se schovávají nějaké nedefinované aplikace.

Implementace Mangle pro IPTV provoz je zobrazena na Obr. 29. Pro pravidlo *change DSCP (TOS)* je nutné zaškrnout *passthrough* a to z důvodu, aby paket přešel i na pravidlo *mark packet.* Obě pravidla vychází z *mark connection.*

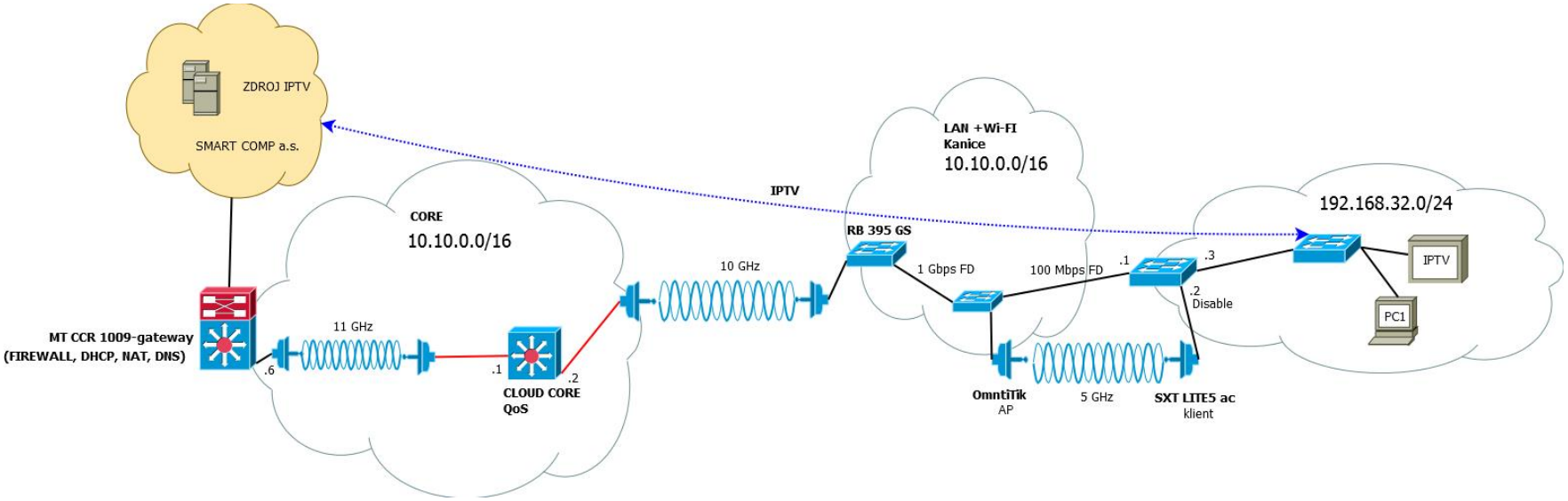
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; IPTV_SIGNALIZACE											
0	mark connection	prerouting								17.9 MiB	302 346
1	change DSCP (TOS)	prerouting								422.1 MiB	295 544
2	mark packet	prerouting								421.8 MiB	295 321
;;; IPTV											
3	mark connection	prerouting								621.4 MiB	434 586
4	change DSCP (TOS)	prerouting								655.2 MiB	544 571
5	mark packet	prerouting								654.7 MiB	544 205

Obr. 29 Mangle pro IPTV v ISP síti.
Zdroj: Vlastní práce.

Verifikací Mangle pravidla je informace ve sloupci *Packets*, kde je publikováno, kolik paketů patřilo do daného pravidla.

13.3 Měření

V této časti ověříme správnost navrženého řešení podle zvolené metodiky (kapitola 7.3.1). Na Obr. 30 můžeme vidět topologii sítě až ke zdroji dat. Proběhnou celkem 2 testy. Jeden při konektivitě přes kabel, druhý přes Wi-Fi připojení. Na základě zátěžových testů verifikujeme kapitolu 11.



Obr. 30 Průchod IPTV dat přes ISP.
Zdroj: Vlastní práce.

13.3.1 Verifikační TEST-1

Na základě metodiky provedeme zátěžový test. Prvky, které provádí simulační test, patří do třídy SPEED. Přestože není prioritizován ICMP protokol, datové toky by se měli rovnoměrné rozdělovat mezi účastníky třídy SPEED a nezvyšovat RTT. Výsledky měření jsou zaznamenány v Tab. 42

Tab. 42 Verifikační TEST-1

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	32 892	32 153	P5+	178
20	31 782	32 148	P5+	29 457
30	30 879	29 148	P5+	42 978
40	32 798	28 319	P5+	42 000
50	31 897	31 201	P5+	39 782
60	30 824	32 581	P5+	39 782
70	31 879	31 852	P5+	41 872
80	30 524	31 589	P5+	42 572
90	31 325	31 575	P5+	40 852
100	31 892	30 879	P5+	39 782
110	30 782	33 188	P5+	40 975
120	32 782	31 287	P5+	41 728

Buffer dosáhl maximální kapacity do 30 sekund. Je to z důvodu, že v ISP síti je omezení na 30 Mbps. IPTV stejně jak při laboratorních testech nepozná zátěž z jiné třídy. Avg. RTT z PC1 na hraniční prvek je 3 ms s packet loss 0 %. Měření z laboratorního prostředí z kapitoly 11.1 je verifikováno v prostředí ISP.

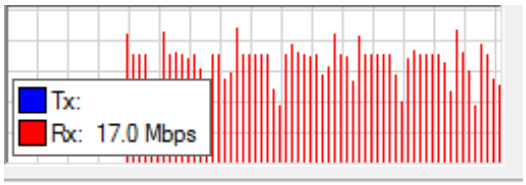
13.3.2 Verifikační TEST-2

Domácí síť s působností IPTV má konektivitu přes Wi-Fi. Vysílacím protokolem AP je NV2. Při testování výchozího testu se zjistilo, že STB načítá data kolem 24 Mbps. Simulační TCP test proběhne na hraniční prvek. STB bude zapnut po 10 sekundách.

Tab. 43 Verifikační TEST-2

Čas [s]	Poslední načtení dat [kbps]	Rychlost linky [kbps]	Profil	Buffer [kB]
10	17 895	19 824	P5+	634
20	18 165	19 275	P5+	13 003
30	20 384	21 857	P5+	21 928
40	22 785	24 875	P5+	25 782
50	19 276	20 185	P5+	34 879
60	21 636	23 875	P5+	41 879
70	27 256	25 789	P5+	39 725
80	25 278	26 272	P5+	42 185
90	20 872	21 875	P5+	40 857
100	24 320	19 872	P5+	41 879
110	20 875	20 789	P5+	39 782
120	20 442	21 028	P5+	40 952

STB si během 60 sekund dočerpal buffer do maximální kapacity a během testování si udržoval podobnou rychlost linky jako u výchozího testu. Klienti, ze kterých probíhal zátěžový test, si nedrží stabilní rychlost a v závislosti na požadavcích STB ustoupí z rychlostní kapacity. Viz Obr. 31.

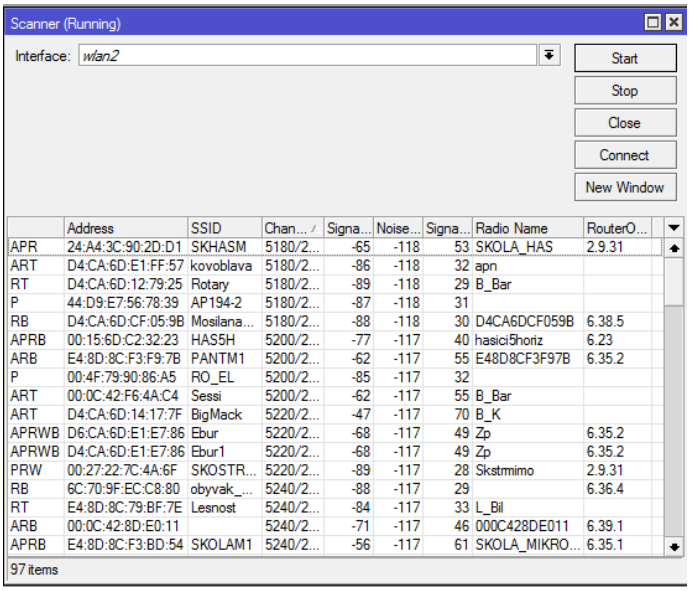


Obr. 31 Simulační zátěž z klienta.
Zdroj: Vlastní práce.

Ping z PC1 puštěný na hraniční prvek měl během simulačního zátěžového testu Avg. RTT 20 ms s packet loss 0 %. Můžeme tedy konstatovat, že výsledky NV2 jsme verifikovali v síti ISP a na bezdrátových spojích lze díky QoS mechanismu poskytovat IPTV.

14 Diskuze

Na základě verifikačních testů jsme dokázali, že zvolené řešení lze implementovat do sítě ISP. Výsledky však mohou být v různém prostředí jiné. V Babicích nad Svitavou, kde působí 5 Wi-Fi poskytovatelů, je frekvenční pásmo extrémně zarušené a je prakticky nemožné najít volný kanál. Místu ani neprospívá poloha, která je v nadmořské výšce 460 m n. m. Ukázka *Scan listu* je Obr. 32.



	Address	SSID	Chan...	Signa...	Noise...	Signa...	Radio Name	RouterO...
APR	24:A4:3C:90:2D:D1	SKHASM	5180/2...	-65	-118	53	SKOLA_HAS	2.9.31
ART	D4:CA:6D:E1:FF:57	kovoblava	5180/2...	-86	-118	32	apn	
RT	D4:CA:6D:12:79:25	Rotary	5180/2...	-89	-118	29	B_Bar	
P	44:D9:E7:56:78:39	AP194-2	5180/2...	-87	-118	31		
RB	D4:CA:6D:CF:05:9B	Mosilana...	5180/2...	-88	-118	30	D4CA6DCF059B	6.38.5
APRB	00:15:6D:C2:32:23	HAS5H	5200/2...	-77	-117	40	hasici5horiz	6.23
ARB	E4:8D:8C:F3:F9:7B	PANTM1	5200/2...	-62	-117	55	E48D8CF3F97B	6.35.2
P	00:4F:79:90:86:A5	RO_EL	5200/2...	-85	-117	32		
ART	00:0C:42:F6:4A:C4	Sessi	5200/2...	-62	-117	55	B_Bar	
ART	D4:CA:6D:14:17:7F	BigMack	5220/2...	-47	-117	70	B_K	
APRWB	D6:CA:6D:E1:E7:86	Ebur	5220/2...	-68	-117	49	Zp	6.35.2
APRWB	D4:CA:6D:E1:E7:86	Ebur1	5220/2...	-68	-117	49	Zp	6.35.2
PRW	00:27:22:7C:4A:6F	SKOSTR...	5220/2...	-89	-117	28	Skstrmimo	2.9.31
RB	6C:70:9F:EC:C8:80	obyvak_...	5240/2...	-88	-117	29		6.36.4
RT	E4:8D:8C:79:BF:7E	Lesnost	5240/2...	-84	-117	33	L_Bil	
ARB	00:0C:42:8D:E0:11		5240/2...	-71	-117	46	000C428DE011	6.39.1
APRB	E4:8D:8C:F3:BD:54	SKOLAM1	5240/2...	-56	-117	61	SKOLA_MIKRO...	6.35.1

Obr. 32 Scan List v Babicích nad Svitavou.
Zdroj: Vlastní práce.

Jak vidíme na obrázku, na každém kmitočtu vysílá minimálně 2 AP. Z toho vyplývá nízká přenosová kapacita spojů. Reálná rychlost je kolem 20–30 Mbps. Jediná možnost otestovat IPTV je v nočních hodinách, ale i přes dobré výsledky testů si firma nepřeje nasazovat náročnou IPTV v takovém prostředí.

Aplikovat QT na každý bezdrátový AP může zlepšit výsledky měření, ale nejednalo by se o centralizované řešení, které bylo požadavkem firmy.

Při lepší práci s datovými toky nemusí firma kupovat nové bezdrátové spoje s vyšší kapacitou a ušetří tím nákladů. Z důvodu poskytování IPTV v unicastovém režimu je otázkou, zda se firmě vyplatí poskytovat IPTV ve větší míře. Špatně zvolená strategie může způsobit klientům využívajícím Internet pomalé připojení, které může vyústit k odchodu ke konkurenci. V průběhu let určitě poroste kapacita bezdrátových spojů a jednou z klíčových služeb na konkurenčním trhu bude právě IPTV.

15 Závěr

Diplomová práce se zabývá problematikou řízení provozu v bezdrátovém spoji WAN sítě s podílem multimediálních dat. Na zvolené téma je v kapitole 1.4 provedena rešerše. Drtivá většina prací se zabývá VoIP provozem, který nemá vysoké požadavky na šířku pásma. IPTV je novým fenoménem, který poskytuje sledování televizního streamu v libovolném čase, a jeho popularita roste. Tato práce je reakcí na potřeby firmy TS–Hydro, která by chtěla poskytovat IPTV přes bezdrátové spoje a zajistit si tak výhodu před konkurencí.

Teorie bezdrátové komunikace z kapitoly 2 shrnuje nutné aspekty k vytvoření kvalitního bezdrátového spoje. Mechanismus QoS, který slouží k zajištění služeb dané aplikace, je popsán v kapitole 3 a 4. Na základě požadavků IPTV od společnosti Smart Comp a.s. je v laboratorních podmínkách vytvořena síťová infrastruktura, která bude sloužit k měření při zátěžových testech. Výsledky testů jednotlivých konfigurací jsou sepsány v kapitole 12.

Na základě analýzy sítě ISP je vytvořen návrh a implementace do síťové infrastruktury. Výsledky z laboratorního měření jsou verifikované ve WAN síti a zvolená konfigurace umožňuje firmě poskytovat IPTV na bezdrátových platformách.

16 Reference

BRAUN, T. -- DIAZ, M. -- ENRÍQUEZ-GABEIRAS, J. End-to-End Quality of Service Over Heterogeneous Networks. Berlin, Heidelberg. 2008. ISBN 9783540791201. URL: http://dx.doi.org/10.1007/978-3-540-79120-1.

BURGESS, Dennis. *Learn RouterOS*. Lexington: Dennis Burgess, 2009, 391 s. ISBN 978-0-557-09271-0.

CARROLLl, B. CCNA *Wireless Official Exam Certification Guide*. Indianapolis, USA: Cisco Press, 2008, xxviii, 473 s. ISBN 978-1-58720-211-7.

CIOARA, J., VALENTINE M. 2012. CCNA voice 640-461: Official Cert Guide. London: Pearson Education, 498 s. ISBN 978-158-7204-173.

CISCO SYSTEMS. *Enterprise QoS Solution Reference Network Design Guide* [online]. 2005 [cit. 2017-04-10]. Dostupné z: http://goo.gl/MNqUbR.

CAMBRIUMNETWORKS, *Quality of Service Mechanisms Explained*. 2016. Dostupné z: http://community.cambiumnetworks.com/t5/ePMP-Networking/Quality-of-Service-Mechanisms-Explained/td-p/52921

ČTU, *všeobecné oprávnění č. VO-R/12/09.2010-12 k využívání radiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat v pásmech 2,4 GHz až 66 GHz.* 2010. Praha. Dostupné z: http://www.ctu.cz/cs/download/oop/rok_2010/vo-r_12-09_2010-12.pdf

ČTU, *všeobecné oprávnění č. VO-R/10/04.2012-7 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu.* 2012. Praha. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2012/vo-r_10-04_2012-07.pdf

DROBNÝ, Jakub. *Využití QoS pro podporu VoIP a videotelefonie ve firemní síti.* Brno, 2014. Bakalářská práce. Mendelova univerzita v Brně, Provozně ekonomická fakutla. Vedoucí práce Jiří Balej.

FRAJ, Martin. *Řízení šířky pásma pomocí C# aplikace.* Jihlava, 2014. Bakalářská práce. Vysoká škola polytechnická Jihlava, Katedra elektrotechniky a informatiky. Vedoucí práce Antonín Přibyl

GACHOGU, Stephen. *Investigating whether the 802.11e wlan QoS standard provides optimal performance in converged networks.*2013. University of Nairobi. School of Computing and Informatics.

GEHRSITZ Thomas and KELLERER Wolfgang. *QoS and robustness of priority-based MAC protocols for the in-car power line communication.* 2016. Mnichov, Německo.

HENS, Franscisco J. CABALLERO M. Jose. *Triple Play: Building the Converged Network for IP, VoIP and IPTV.* Chichester, UK: Wiley, 2008. ISBN: 978-0-470-75367-5

HU, Qi Gang (William), WILLIAMSON, Carey and O. FAPOJUWO, Abraham. 2011. *Experimental evaluation of asymmetric QoS in IEEE 802.11g wireless networks.* New York, NY, USA : ACM, 2011. Q2SWinet '11.

HUCABY, Dave*. CCNA wireless 640-722 official cert guide*. ISBN 1587205629.

IETF.RFC 2597: *Assured Forwarding PHB Grou.* [online]. 1999 [cit. 2017-04-22]. Dostupné z: https://tools.ietf.org/html/rfc2597

IETF.RFC 2598: *An Expedited Forwarding PHB.* [online]. 1999 [cit. 2017-04-22]. Dostupné z: https://tools.ietf.org/html/rfc2598

IETF.RFC 3260: *New Terminology and Clarifications for Diffserv* [online]. 2002 [cit. 2017-05-05]. Dostupné z: https://tools.ietf.org/html/rfc3260

IETF.RFC 6405: *Voice over IP (VoIP) SIP Peering Use Cases.*[online].2011[cit.2017-04-29].

Dostupné z: https://tools.ietf.org/html/rfc6405

INTERNETPROVSECHNY: *soumrak-volneho-10-ghz-pasma-aneb-kdo-ma-zajem-na-jeho-zaruseni.* [online]. [cit. 2017-04-24]. Dostupné z: http://www.internetprovsechny.cz/soumrak-volneho-10-ghz-pasma-aneb-kdo-ma-zajem-na-jeho-zaruseni/

ITU.2004 [online]. 2017 [cit. 2017-03-31]. Dostupné z:

http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.16.48.en.101.pdf

ITU-T. P.800 : Methods for subjective determination of transmission quality. 1996.

ITU-T. P.800.1 : Mean Opinion Score (MOS) terminology. 2006

JITSI (SIP Communicator) [online]. 2017 [cit. 2017-04-08]. Dostupný z :

<http://www.jitsi.org/index.php/Main/HomePage>.

KALINA, Tomáš. *QoS v síti VŠE*. Praha: Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, 2013, 86 str. Dostupné z: <https://isis.vse.cz/auth/zp/index.pl?podrobnosti_zp= 35886>

KOKEŠOVÁ, Nikol. *Reálná prostupnost zařízení pracujících na standardu 802.11n*. [cit. 2017-03-27]. Brno, 2011. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Petr Münster.

KONEČNÝ, Jakub. *Optimallizace univerzitní bezdrátové sítě pro provoz hlasových služeb*. Brno: Mendelova univerzita v Brně, Provozně ekonomické fakulta, 2015. 80 str. Dostupné z: <http://theses.cz/id/tpuc8c/>

KOTON, J. 2014. Moderní síťové technologie. Vysoké učetní technické v Brně.

191 s. ISBN 978-80-214-5026-4.

KUČERA, Martin. *Renovace počítačové sítě ZŠ a MŠ Kanice.* 2015. Bakalářská práce. Mendelova univerzita v Brně. Provozně ekonomická fakulta. Vedoucí práce Jiří Balej.

KUKI, [cit. 2017-05-08]. Dostupné z: https://www.kuki.cz/

KUROSE, J. F. a ROSS, K. W. *Computer networking*: A Top-Down Approach. 6th

ed. Boston, USA: Addison-Wesley, 2013, xxiv, 862 s. ISBN 978-0-13-285620-1.

LEJTNAR, Michal. *Komparativní analýza ad hoc a direct spojení v bezdrátových sítích*. Bakalářská práce. České Budějovice: Jihočeská univerzita v Českých Budějovicích, Přírodovědecká fakulta, 2012

MENŠÍK, David. *Analýza přenosu dat v konvergované síti.* Brno, 2011. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologii. Vedoucí práce Vladislav Škorpil.

MICHAEL OCHE, RAFIDAH MD NOOR, JOHNSON IHYEH AGHINY, 2014. *Network centric QoS performance evaluation of IPTV transmission quality over VANETs.* Kuala Lumpur & Melbourne, Malaysia & Australia.

MIKROTIK. manual:Packet_Flow. [online]. 2017 [cit. 2017-04-26]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

MIKROTIK. manual:Queue. [online]. 2017 [cit. 2017-04-27]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Queue

MIKROTIK. manual:Queues_--PCQ. [online]. 2017 [cit. 2017-04-27]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ

MIKROTIK, manual: NV2 [online]. 2017. [cit. 2017-05-08]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Nv2

MIKROTIK, manual:Queue_Size [online]. 2017. [cit. 2017-05-12]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Queue_Size

Molnár, K. 2008*. Přednášky k předmětu Moderní síťové technologie*. FEKT VUT, Brno.

MUM.MIKROTIK. *Quality of Service in wireless Point-to-Point Links.*presenation.2013. Dostupné z: https://mum.mikrotik.com//presentations/US13/lutz.pdf

MUM.MIKROTIK. *Wireless QoS with WMM and DSCP – How to implement QoS on Wireless LAN*. 2010. Dostupné z: https://mum.mikrotik.com//presentations/PL10/grittini.pdf

NOVÁK, Tomáš. *Šíření vln: přednášky: otazka_09*. 2015. Vysoká škola báňská – Technická ta Ostrava. Fakulta eletrochtechniky a informatiky.

PECHÁČ, Pavel. *Šíření vln v zástavbě.* BEN – technická literatura, Praha 2006

PECHÁČ Pavel, ZVÁNOVEC Stanislav, *Základy šíření vln.* BEN – technická literatura, Praha 2007

PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualiz. vyd. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.

PRASAD R. Anand, PRASAD R. Neeli*, 802.11 WLANs and IP Networking: Security, QOS, and Mobility*, 2005, ISBN 1-58053-789-8

REBOOK, Tomáš. 2008. *QoS-enabled Distributed Active Router: rigorózní práce*. Brno : Masarykova univerzita, Fakulta informatiky, 2008.

RUČKA, Tomáš. *Simulace přístupové metody CSMA.* Praha, 2007. Bakalářská práce. České vysoké učení technické v Praze. Fakulta elektrotechnická. Vedoucí práce Jiří Douša.

SCHÖN, Martin.2015.*Analýza závislosti komunikačních služeb na zpoždění a optimalizace QoS.*Brno, 2015.Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologii. Vedoucí práce Jiří Hošek.

SELFNET. *Set-top-box Arris VIP1113 uživatelská příručka.* 2017. [cit. 2017-05-08]. Dostupné z: http://www.selfnet.cz/file/uzivatelsky-navod-stb-vip-1113.pdf

SKIPALA, Ondřej. *Bezdrátové sítě v zarušených prostředích.* Brno, 2011. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká.

SLANINA, Martin. *Moderní bezdrátová komunikace: přednášky*. Vyd. 1. V Brně: Vysoké učení technické v Brně, Fakulta elektrotechniky a informatiky, Ústav radioelektroniky, 2010, 169 s. ISBN 978-80-214-4156

SLAVÍČEK, Tomáš. *Optimalizace přístupových sítí pro multimediální služby.* 2010. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií.

SLIŽ, Vítězslav. *Technologie počítačových sítí: Projekt – konfiguraci a mechanismu QoS podle standardu IEEE 802.11e na přístupových bodech Cisco Airone.* 2008. VŠB: Katedra Informatiky.

ŠVARC, Lukaš. *VoIP v bezdrátové síti VŠE.* Praha, 2016. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Vedoucí práce Luboš Pavlíček.

ŠVARC, Lukáš. *Optimalizace bezdrátové sítě VŠE*. Praha, 2013. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky.

Švec, P. *Návrh a mplementácia IPv6 siete v akademickej sfére.* Ostrava, 2011. Dizertační práce. Ostravská univerzita v Ostravě.

TECHNET. *Jeden gigabajt za 10 sekund. Brutálně rýchlá Wi-Fi neprojde zdí ani masem.* 2017. Dostupné z: http://technet.idnes.cz/rychla-wi-fi-802-11-ad-tp-link-talon-ad7200-router-fe1-/hardware.aspx?c=A170424_082538_hardware_nyv

TIEU, Jimmy and YE, Sihan. *Wi-Fi Direct Services.* Master's Thesis. 2014. Department of Electrical and Information Technology. Lund University.

UBNT, *How is QoS and prioritization handle by airMAX?*. 2015. Dostupné z: https://help.ubnt.com/hc/en-us/articles/205231750-airMAX-How-is-QoS-and-prioritization-handled-by-airMAX-

VÁGNER, Adam. *Měření v bezdrátové síti 802.11N se skrytými uzly.* Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologii.

WIKIPEDIA: *Jitter.* [online]. [cit. 2017-03-25]. Dostupné z: https://en.wikipedia.org/wiki/Jitter

WIKIPEDIA: *Fresnel_zone.* [online]. [cit. 2017-03-20]. Dostupné z: https://en.wikipedia.org/wiki/Fresnel_zone

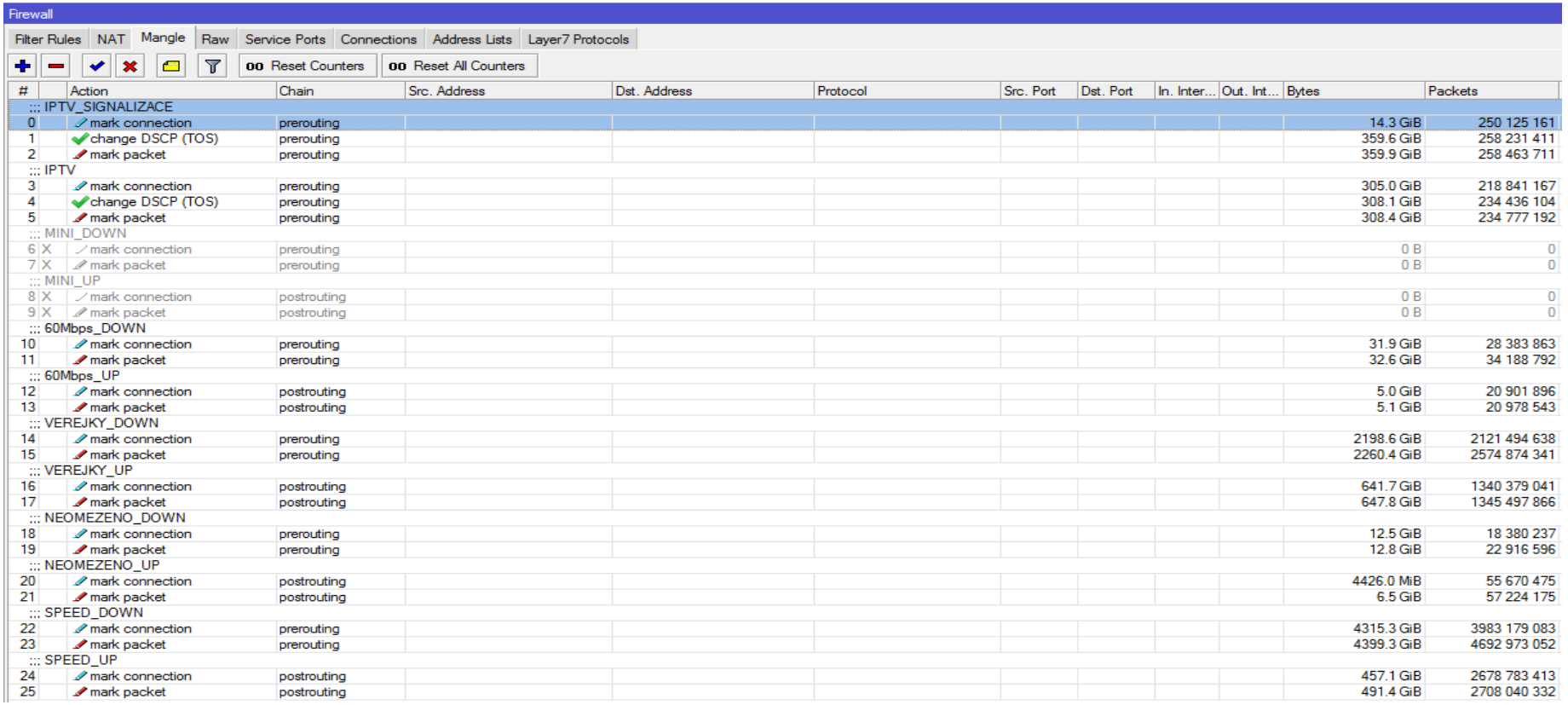
ZACH, Petr. *Metodika sledování a hodnocení počítačové sítě podniku.* Brno, 2015. Disertační práce. Mendelova univerzita v Brně, Provozně ekonomická fakutla. Vedoucí práce Arnošt Motyčka.

ZANDL, Patrick. *Bezdrátové sítě WiFi*: praktický průvodce. Brno: Computer Press, 2003, 190 str. ISBN 80-722-6632-2.

ZELINKA, Tomáš a SVÍTEK, Miroslav. 2009. *Telekomunikační řešení pro informační systémy síťových odvětví*. Praha : Grada Publishing, a.s., 2009. 978-80-247-3232-9.

Přílohy

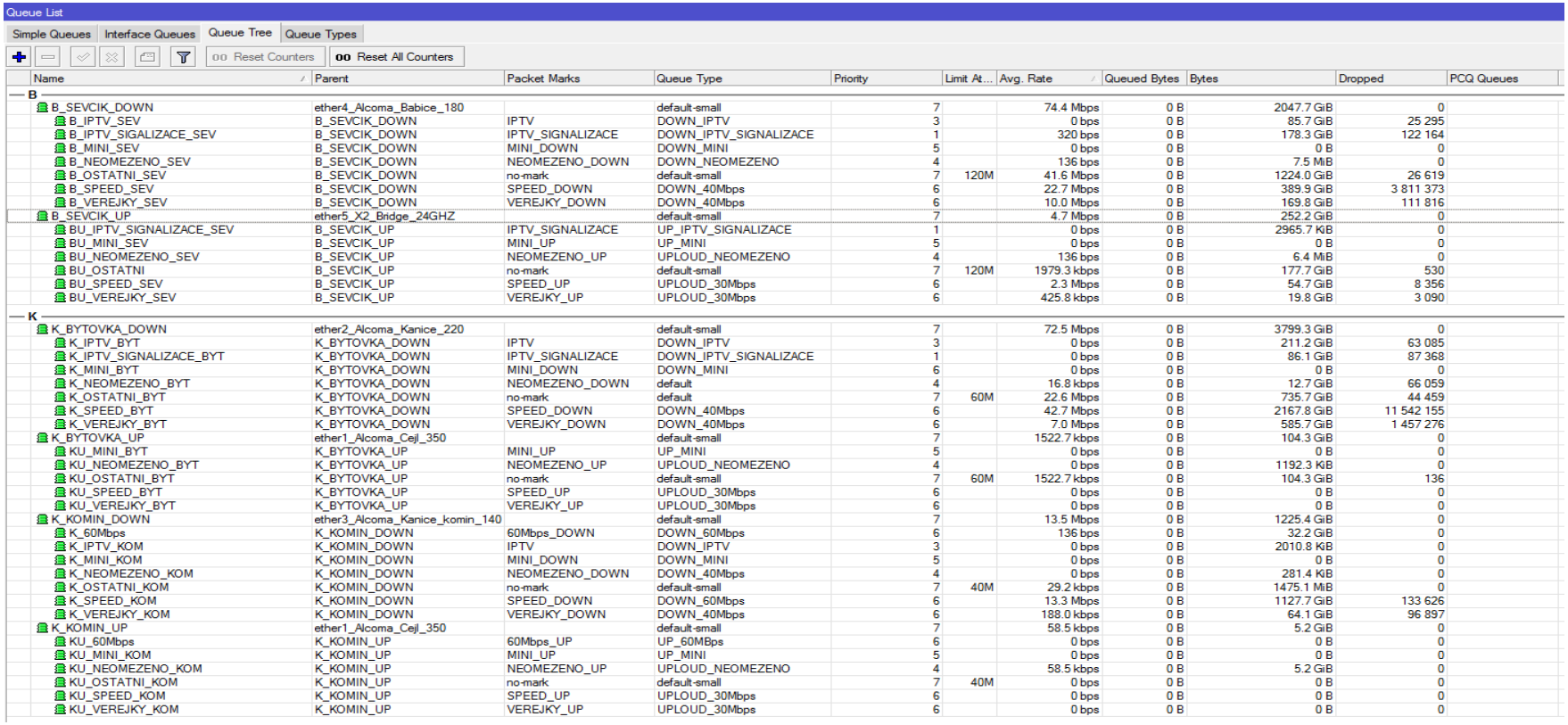
A CLOUD_CORE Mangle



#		Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; IPTV_SIGNALIZACE												
0		mark connection	prerouting								14.3 GiB	250 125 161
1		change DSCP (TOS)	prerouting								359.6 GiB	258 231 411
2		mark packet	prerouting								359.9 GiB	258 463 711
;;; IPTV												
3		mark connection	prerouting								305.0 GiB	218 841 167
4		change DSCP (TOS)	prerouting								308.1 GiB	234 436 104
5		mark packet	prerouting								308.4 GiB	234 777 192
;;; MINI_DOWN												
6	X	mark connection	prerouting								0 B	0
7	X	mark packet	prerouting								0 B	0
;;; MINI_UP												
8	X	mark connection	postrouting								0 B	0
9	X	mark packet	postrouting								0 B	0
;;; 60Mbps_DOWN												
10		mark connection	prerouting								31.9 GiB	28 383 863
11		mark packet	prerouting								32.6 GiB	34 188 792
;;; 60Mbps_UP												
12		mark connection	postrouting								5.0 GiB	20 901 896
13		mark packet	postrouting								5.1 GiB	20 978 543
;;; VEREJKY_DOWN												
14		mark connection	prerouting								2198.6 GiB	2121 494 638
15		mark packet	prerouting								2260.4 GiB	2574 874 341
;;; VEREJKY_UP												
16		mark connection	postrouting								641.7 GiB	1340 379 041
17		mark packet	postrouting								647.8 GiB	1345 497 866
;;; NEOMEZENO_DOWN												
18		mark connection	prerouting								12.5 GiB	18 380 237
19		mark packet	prerouting								12.8 GiB	22 916 596
;;; NEOMEZENO_UP												
20		mark connection	postrouting								4426.0 MiB	55 670 475
21		mark packet	postrouting								6.5 GiB	57 224 175
;;; SPEED_DOWN												
22		mark connection	prerouting								4315.3 GiB	3983 179 083
23		mark packet	prerouting								4399.3 GiB	4692 973 052
;;; SPEED_UP												
24		mark connection	postrouting								457.1 GiB	2678 783 413
25		mark packet	postrouting								491.4 GiB	2708 040 332

Obr. 33 CLOUD_CORE MANGLE
Zdroj: Vlastní práce.

B CLOUD_CORE Queue Tree



Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters

Name	Parent	Packet Marks	Queue Type	Priority	Limit At...	Avg. Rate	Queued Bytes	Bytes	Dropped	PCQ Queues
B										
B_SEVCIK_DOWN	ether4_Alcoma_Babice_180		default-small	7		74.4 Mbps	0 B	2047.7 GiB	0	
B_IPTV_SEV	B_SEVCIK_DOWN	IPTV	DOWN_IPTV	3		0 bps	0 B	85.7 GiB	25 295	
B_IPTV_SIGALIZACE_SEV	B_SEVCIK_DOWN	IPTV_SIGNALIZACE	DOWN_IPTV_SIGNALIZACE	1		320 bps	0 B	178.3 GiB	122 164	
B_MINI_SEV	B_SEVCIK_DOWN	MINI_DOWN	DOWN_MINI	5		0 bps	0 B	0 B	0	
B_NEOMEZENO_SEV	B_SEVCIK_DOWN	NEOMEZENO_DOWN	DOWN_NEOMEZENO	4		136 bps	0 B	7.5 MiB	0	
B_OSTATNI_SEV	B_SEVCIK_DOWN	no-mark	default-small	7	120M	41.6 Mbps	0 B	1224.0 GiB	26 619	
B_SPEED_SEV	B_SEVCIK_DOWN	SPEED_DOWN	DOWN_40Mbps	6		22.7 Mbps	0 B	389.9 GiB	3 811 373	
B_VEREJKY_SEV	B_SEVCIK_DOWN	VEREJKY_DOWN	DOWN_40Mbps	6		10.0 Mbps	0 B	169.8 GiB	111 816	
B_SEVCIK_UP	ether5_X2_Bridge_24GHZ		default-small	7		4.7 Mbps	0 B	252.2 GiB	0	
BU_IPTV_SIGNALIZACE_SEV	B_SEVCIK_UP	IPTV_SIGNALIZACE	UP_IPTV_SIGNALIZACE	1		0 bps	0 B	2965.7 KiB	0	
BU_MINI_SEV	B_SEVCIK_UP	MINI_UP	UP_MINI	5		0 bps	0 B	0 B	0	
BU_NEOMEZENO_SEV	B_SEVCIK_UP	NEOMEZENO_UP	UPLOUD_NEOMEZENO	4		136 bps	0 B	6.4 MiB	0	
BU_OSTATNI	B_SEVCIK_UP	no-mark	default-small	7	120M	1979.3 kbps	0 B	177.7 GiB	530	
BU_SPEED_SEV	B_SEVCIK_UP	SPEED_UP	UPLOUD_30Mbps	6		2.3 Mbps	0 B	54.7 GiB	8 356	
BU_VEREJKY_SEV	B_SEVCIK_UP	VEREJKY_UP	UPLOUD_30Mbps	6		425.8 kbps	0 B	19.8 GiB	3 090	
K										
K_BYTOVKA_DOWN	ether2_Alcoma_Kanice_220		default-small	7		72.5 Mbps	0 B	3799.3 GiB	0	
K_IPTV_BYT	K_BYTOVKA_DOWN	IPTV	DOWN_IPTV	3		0 bps	0 B	211.2 GiB	63 085	
K_IPTV_SIGNALIZACE_BYT	K_BYTOVKA_DOWN	IPTV_SIGNALIZACE	DOWN_IPTV_SIGNALIZACE	1		0 bps	0 B	86.1 GiB	87 368	
K_MINI_BYT	K_BYTOVKA_DOWN	MINI_DOWN	DOWN_MINI	6		0 bps	0 B	0 B	0	
K_NEOMEZENO_BYT	K_BYTOVKA_DOWN	NEOMEZENO_DOWN	default	4		16.8 kbps	0 B	12.7 GiB	66 059	
K_OSTATNI_BYT	K_BYTOVKA_DOWN	no-mark	default	7	60M	22.6 Mbps	0 B	735.7 GiB	44 459	
K_SPEED_BYT	K_BYTOVKA_DOWN	SPEED_DOWN	DOWN_40Mbps	6		42.7 Mbps	0 B	2167.8 GiB	11 542 155	
K_VEREJKY_BYT	K_BYTOVKA_DOWN	VEREJKY_DOWN	DOWN_40Mbps	6		7.0 Mbps	0 B	585.7 GiB	1 457 276	
K_BYTOVKA_UP	ether1_Alcoma_Cejl_350		default-small	7		1522.7 kbps	0 B	104.3 GiB	0	
KU_MINI_BYT	K_BYTOVKA_UP	MINI_UP	UP_MINI	5		0 bps	0 B	0 B	0	
KU_NEOMEZENO_BYT	K_BYTOVKA_UP	NEOMEZENO_UP	UPLOUD_NEOMEZENO	4		0 bps	0 B	1192.3 KiB	0	
KU_OSTATNI_BYT	K_BYTOVKA_UP	no-mark	default-small	7	60M	1522.7 kbps	0 B	104.3 GiB	136	
KU_SPEED_BYT	K_BYTOVKA_UP	SPEED_UP	UPLOUD_30Mbps	6		0 bps	0 B	0 B	0	
KU_VEREJKY_BYT	K_BYTOVKA_UP	VEREJKY_UP	UPLOUD_30Mbps	6		0 bps	0 B	0 B	0	
K_KOMIN_DOWN	ether3_Alcoma_Kanice_komin_140		default-small	7		13.5 Mbps	0 B	1225.4 GiB	0	
K_60Mbps	K_KOMIN_DOWN	60Mbps_DOWN	DOWN_60Mbps	6		136 bps	0 B	32.2 GiB	0	
K_IPTV_KOM	K_KOMIN_DOWN	IPTV	DOWN_IPTV	3		0 bps	0 B	2010.8 KiB	0	
K_MINI_KOM	K_KOMIN_DOWN	MINI_DOWN	DOWN_MINI	5		0 bps	0 B	0 B	0	
K_NEOMEZENO_KOM	K_KOMIN_DOWN	NEOMEZENO_DOWN	DOWN_40Mbps	4		0 bps	0 B	281.4 KiB	0	
K_OSTATNI_KOM	K_KOMIN_DOWN	no-mark	default-small	7	40M	29.2 kbps	0 B	1475.1 MiB	0	
K_SPEED_KOM	K_KOMIN_DOWN	SPEED_DOWN	DOWN_60Mbps	6		13.3 Mbps	0 B	1127.7 GiB	133 626	
K_VEREJKY_KOM	K_KOMIN_DOWN	VEREJKY_DOWN	DOWN_40Mbps	6		188.0 kbps	0 B	64.1 GiB	96 897	
K_KOMIN_UP	ether1_Alcoma_Cejl_350		default-small	7		58.5 kbps	0 B	5.2 GiB	0	
KU_60Mbps	K_KOMIN_UP	60Mbps_UP	UP_60MBps	6		0 bps	0 B	0 B	0	
KU_MINI_KOM	K_KOMIN_UP	MINI_UP	UP_MINI	5		0 bps	0 B	0 B	0	
KU_NEOMEZENO_KOM	K_KOMIN_UP	NEOMEZENO_UP	UPLOUD_NEOMEZENO	4		58.5 kbps	0 B	5.2 GiB	0	
KU_OSTATNI_KOM	K_KOMIN_UP	no-mark	default-small	7	40M	0 bps	0 B	0 B	0	
KU_SPEED_KOM	K_KOMIN_UP	SPEED_UP	UPLOUD_30Mbps	6		0 bps	0 B	0 B	0	
KU_VEREJKY_KOM	K_KOMIN_UP	VEREJKY_UP	UPLOUD_30Mbps	6		0 bps	0 B	0 B	0	

Obr. 34 CLOUD_CORE Queue Tree
Zdroj: Vlastní práce.

C CLOUD_CORE export

```
# may/21/2017 10:19:51 by RouterOS 6.38.5
# software id = 1FYS-2CDG
#
/interface bridge
add name=Bridge priority=0x7
add name=Bridge_24GHz priority=0x50
/interface ethernet
set [ find default-name=ether1 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full name=\
    ether1_Alcoma_Cejl_350 rx-flow-control=auto speed=1Gbps tx-flow-control=\
    auto
set [ find default-name=ether2 ] name=ether2_Alcoma_Kanice_220
set [ find default-name=ether3 ] name=ether3_Alcoma_Kanice_komin_140
set [ find default-name=ether4 ] name=ether4_Alcoma_Babice_180
set [ find default-name=ether5 ] name=ether5_X2_Bridge_24GHZ
set [ find default-name=ether6 ] name=ether6_RB600_vnitrni
set [ find default-name=ether7 ] name=ether7_Slatina_M10
set [ find default-name=ether8 ] name=ether8_RB911G_Bytovka_ricmanice
set [ find default-name=ether9 ] name=ether9_2011
set [ find default-name=ether10 ] name=ether_10_X2_Bridge_11GHZ
set [ find default-name=ether11 ] name=ether_11
set [ find default-name=ether12 ] name=ether_12
/queue tree
add max-limit=205M name=K_BYTOVKA_DOWN parent=ether2_Alcoma_Kanice_220 \
    priority=7
add max-limit=140M name=K_BYTOVKA_UP parent=ether1_Alcoma_Cejl_350 priority=7
add max-limit=180M name=B_SEVCIK_DOWN parent=ether4_Alcoma_Babice_180 \
    priority=7
add limit-at=120M max-limit=150M name=B_OSTATNI_SEV packet-mark=no-mark \
    parent=B_SEVCIK_DOWN priority=7
add name=B_SEVCIK_UP parent=ether5_X2_Bridge_24GHZ priority=7
add max-limit=100M name=K_KOMIN_UP parent=ether1_Alcoma_Cejl_350 priority=7
add max-limit=130M name=K_KOMIN_DOWN parent=ether3_Alcoma_Kanice_komin_140 \
    priority=7
add limit-at=40M max-limit=80M name=K_OSTATNI_KOM packet-mark=no-mark parent=\
    K_KOMIN_DOWN priority=7
add limit-at=120M max-limit=170M name=BU_OSTATNI packet-mark=no-mark parent=\
    B_SEVCIK_UP priority=7
add limit-at=60M max-limit=150M name=KU_OSTATNI_BYT packet-mark=no-mark \
    parent=K_BYTOVKA_UP priority=7
add limit-at=40M max-limit=120M name=KU_OSTATNI_KOM packet-mark=no-mark \
    parent=K_KOMIN_UP priority=7
```

```
/queue type
add kind=pcq name=DOWN_40Mbps pcq-burst-time=1s pcq-classifier=dst-address \
    pcq-dst-address6-mask=64 pcq-limit=100KiB pcq-rate=40M \
    pcq-src-address6-mask=64 pcq-total-limit=2000000KiB
add kind=pcq name=UPLOUD_30Mbps pcq-classifier=src-address \
    pcq-dst-address6-mask=64 pcq-rate=30M pcq-src-address6-mask=64
add kind=pcq name=DOWN_NEOMEZENO pcq-classifier=dst-address \
    pcq-dst-address6-mask=64 pcq-limit=500KiB pcq-src-address6-mask=64 \
    pcq-total-limit=200000KiB
add kind=pcq name=UPLOUD_NEOMEZENO pcq-classifier=src-address \
    pcq-dst-address6-mask=64 pcq-src-address6-mask=64
add kind=pcq name=DOWN_IPTV pcq-classifier=dst-address pcq-dst-address6-mask=\
    64 pcq-limit=100KiB pcq-rate=30M pcq-src-address6-mask=64 \
    pcq-total-limit=200000KiB
add kind=pcq name=UPLOUD_IPTV pcq-classifier=src-address \
    pcq-dst-address6-mask=64 pcq-rate=20M pcq-src-address6-mask=64
add kind=pcq name=DOWN_Wifi pcq-classifier=dst-address pcq-dst-address6-mask=\
    64 pcq-rate=19M pcq-src-address6-mask=64
add kind=pcq name=UP_wifi pcq-classifier=src-address pcq-dst-address6-mask=64
\
    pcq-rate=10M pcq-src-address6-mask=64
add kind=pcq name=DOWN_60Mbps pcq-classifier=dst-address \
    pcq-dst-address6-mask=64 pcq-rate=80M pcq-src-address6-mask=64
add kind=pcq name=UP_60MBps pcq-classifier=src-address pcq-dst-address6-mask=\
    64 pcq-rate=60M pcq-src-address6-mask=64
add kind=pcq name=DOWN_OTHER pcq-classifier=dst-address \
    pcq-dst-address6-mask=64 pcq-src-address6-mask=64
add kind=pcq name=UP_OTHER pcq-classifier=src-address pcq-dst-address6-mask=\
    64 pcq-src-address6-mask=64
add kind=pcq name=DOWN_MINI pcq-classifier=dst-address pcq-dst-address6-mask=\
    64 pcq-rate=9M pcq-src-address6-mask=64
add kind=pcq name=UP_MINI pcq-classifier=src-address pcq-dst-address6-mask=64
\
    pcq-rate=9 pcq-src-address6-mask=64
add kind=sfq name=TEST
add kind=pcq name=DOWN_IPTV_SIGNALIZACE pcq-classifier=dst-address \
    pcq-dst-address6-mask=64 pcq-rate=30M pcq-src-address6-mask=64
add kind=pcq name=UP_IPTV_SIGNALIZACE pcq-classifier=src-address \
    pcq-dst-address6-mask=64 pcq-rate=3M pcq-src-address6-mask=64
/queue tree
add name=K_SPEED_BYT packet-mark=SPEED_DOWN parent=K_BYTOVKA_DOWN priority=6 \
    queue=DOWN_40Mbps
add name=K_NEOMEZENO_BYT packet-mark=NEOMEZENO_DOWN parent=K_BYTOVKA_DOWN \
    priority=4 queue=default
add limit-at=60M max-limit=100M name=K_OSTATNI_BYT packet-mark=no-mark \
```

```
    parent=K_BYTOVKA_DOWN priority=7 queue=default
add name=K_VEREJKY_BYT packet-mark=VEREJKY_DOWN parent=K_BYTOVKA_DOWN \
    priority=6 queue=DOWN_40Mbps
add name=K_MINI_BYT packet-mark=MINI_DOWN parent=K_BYTOVKA_DOWN priority=6 \
    queue=DOWN_MINI
add name=K_IPTV_BYT packet-mark=IPTV parent=K_BYTOVKA_DOWN priority=3 queue=\
    DOWN_IPTV
add name=KU_MINI_BYT packet-mark=MINI_UP parent=K_BYTOVKA_UP priority=5 \
    queue=UP_MINI
add name=B_MINI_SEV packet-mark=MINI_DOWN parent=B_SEVCIK_DOWN priority=5 \
    queue=DOWN_MINI
add name=B_NEOMEZENO_SEV packet-mark=NEOMEZENO_DOWN parent=B_SEVCIK_DOWN \
    priority=4 queue=DOWN_NEOMEZENO
add name=B_VEREJKY_SEV packet-mark=VEREJKY_DOWN parent=B_SEVCIK_DOWN \
    priority=6 queue=DOWN_40Mbps
add name=B_SPEED_SEV packet-mark=SPEED_DOWN parent=B_SEVCIK_DOWN priority=6 \
    queue=DOWN_40Mbps
add name=B_IPTV_SEV packet-mark=IPTV parent=B_SEVCIK_DOWN priority=3 queue=\
    DOWN_IPTV
add  name=KU_VEREJKY_BYT  packet-mark=VEREJKY_UP  parent=K_BYTOVKA_UP  priority=6
\
    queue=UPLOUD_30Mbps
add name=BU_VEREJKY_SEV packet-mark=VEREJKY_UP parent=B_SEVCIK_UP priority=6 \
    queue=UPLOUD_30Mbps
add name=BU_SPEED_SEV packet-mark=SPEED_UP parent=B_SEVCIK_UP priority=6 \
    queue=UPLOUD_30Mbps
add name=BU_MINI_SEV packet-mark=MINI_UP parent=B_SEVCIK_UP priority=5 queue=\
    UP_MINI
add name=KU_SPEED_BYT packet-mark=SPEED_UP parent=K_BYTOVKA_UP priority=6 \
    queue=UPLOUD_30Mbps
add name=KU_NEOMEZENO_BYT packet-mark=NEOMEZENO_UP parent=K_BYTOVKA_UP \
    priority=4 queue=UPLOUD_NEOMEZENO
add name=BU_NEOMEZENO_SEV packet-mark=NEOMEZENO_UP parent=B_SEVCIK_UP \
    priority=4 queue=UPLOUD_NEOMEZENO
add name=KU_VEREJKY_KOM packet-mark=VEREJKY_UP parent=K_KOMIN_UP priority=6 \
    queue=UPLOUD_30Mbps
add name=KU_SPEED_KOM packet-mark=SPEED_UP parent=K_KOMIN_UP priority=6 \
    queue=UPLOUD_30Mbps
add name=KU_NEOMEZENO_KOM packet-mark=NEOMEZENO_UP parent=K_KOMIN_UP \
    priority=4 queue=UPLOUD_NEOMEZENO
add name=KU_MINI_KOM packet-mark=MINI_UP parent=K_KOMIN_UP priority=5 queue=\
    UP_MINI
add name=K_IPTV_KOM packet-mark=IPTV parent=K_KOMIN_DOWN priority=3 queue=\
    DOWN_IPTV
add name=K_MINI_KOM packet-mark=MINI_DOWN parent=K_KOMIN_DOWN priority=5 \
```

```
    queue=DOWN_MINI
add name=K_NEOMEZENO_KOM packet-mark=NEOMEZENO_DOWN parent=K_KOMIN_DOWN \
    priority=4 queue=DOWN_40Mbps
add name=K_SPEED_KOM packet-mark=SPEED_DOWN parent=K_KOMIN_DOWN priority=6 \
    queue=DOWN_60Mbps
add name=K_VEREJKY_KOM packet-mark=VEREJKY_DOWN parent=K_KOMIN_DOWN priority=\
    6 queue=DOWN_40Mbps
add name=K_60Mbps packet-mark=60Mbps_DOWN parent=K_KOMIN_DOWN priority=6 \
    queue=DOWN_60Mbps
add name=KU_60Mbps packet-mark=60Mbps_UP parent=K_KOMIN_UP priority=6 queue=\
    UP_60MBps
add name=B_IPTV_SIGALIZACE_SEV packet-mark=IPTV_SIGNALIZACE parent=\
    B_SEVCIK_DOWN priority=1 queue=DOWN_IPTV_SIGNALIZACE
add name=BU_IPTV_SIGNALIZACE_SEV packet-mark=IPTV_SIGNALIZACE parent=\
    B_SEVCIK_UP priority=1 queue=UP_IPTV_SIGNALIZACE
add name=K_IPTV_SIGNALIZACE_BYT packet-mark=IPTV_SIGNALIZACE parent=\
    K_BYTOVKA_DOWN priority=1 queue=DOWN_IPTV_SIGNALIZACE
/interface bridge port
add bridge=Bridge interface=ether1_Alcoma_Cejl_350
add bridge=Bridge interface=ether2_Alcoma_Kanice_220
add bridge=Bridge interface=ether3_Alcoma_Kanice_komin_140
add bridge=Bridge_24GHz interface=ether4_Alcoma_Babice_180
add bridge=Bridge_24GHz interface=ether5_X2_Bridge_24GHZ path-cost=90
add bridge=Bridge interface=ether6_RB600_vnitrni
add bridge=Bridge_24GHz interface=ether7_Slatina_M10
add bridge=Bridge interface=ether8_RB911G_Bytovka_ricmanice
add bridge=Bridge interface=ether9_2011
add bridge=Bridge interface=ether_10_X2_Bridge_11GHZ
add bridge=Bridge_24GHz interface=ether_11
add bridge=Bridge interface=ether_12
/interface bridge settings
set use-ip-firewall=yes use-ip-firewall-for-vlan=yes
/ip address
add address=10.10.102.20/16 interface=Bridge network=10.10.0.0
add address=10.10.102.24/16 interface=Bridge_24GHz network=10.10.0.0
add address=93.99.7.111/25 disabled=yes interface=Bridge network=93.99.7.0
/ip dns
set servers=10.10.0.34,10.10.192.34,8.8.8.8
/ip firewall address-list
add address=93.99.7.0/25 list=VEREJKY
add address=0.0.0.0/0 list=OSTATNI
add address=10.10.110.1-10.10.110.253 list=NEOMEZENO
add address=10.10.111.1-10.10.111.250 list=60Mbps
add address=10.10.192.1-10.10.193.254 list=MINI
add address=10.10.0.40-10.10.230.250 list=SPEED
```

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=IPTV_SIGNALIZACE dscp=20 \
    new-connection-mark=IPTV_SIGNALIZACE_C passthrough=no
add action=change-dscp chain=prerouting connection-mark=IPTV_SIGNALIZACE_C \
    new-dscp=7 passthrough=yes
add action=mark-packet chain=prerouting connection-mark=IPTV_SIGNALIZACE_C \
    new-packet-mark=IPTV_SIGNALIZACE passthrough=no
add action=mark-connection chain=prerouting comment=IPTV dscp=32 \
    new-connection-mark=IPTV_C passthrough=yes
add action=change-dscp chain=prerouting connection-mark=IPTV_C new-dscp=5 \
    passthrough=yes
add action=mark-packet chain=prerouting connection-mark=IPTV_C \
    new-packet-mark=IPTV passthrough=no
add action=mark-connection chain=prerouting comment=MINI_DOWN disabled=yes \
    dst-address-list=MINI new-connection-mark=MINI_DOWN_C passthrough=yes
add action=mark-packet chain=prerouting connection-mark=MINI_DOWN_C disabled=\
    yes new-packet-mark=MINI_DOWN passthrough=no
add action=mark-connection chain=postrouting comment=MINI_UP disabled=yes \
    new-connection-mark=MINI_UP_C passthrough=yes src-address-list=MINI
add action=mark-packet chain=postrouting connection-mark=MINI_UP_C disabled=\
    yes new-packet-mark=MINI_UP passthrough=no
add action=mark-connection chain=prerouting comment=60Mbps_DOWN \
    dst-address-list=60Mbps new-connection-mark=60Mbps_DOWN_C passthrough=yes
add action=mark-packet chain=prerouting connection-mark=60Mbps_DOWN_C \
    new-packet-mark=60Mbps_DOWN passthrough=no
add action=mark-connection chain=postrouting comment=60Mbps_UP \
    new-connection-mark=60Mbps_UP_C passthrough=yes src-address-list=60Mbps
add action=mark-packet chain=postrouting connection-mark=60Mbps_UP_C \
    new-packet-mark=60Mbps_UP passthrough=no
add action=mark-connection chain=prerouting comment=VEREJKY_DOWN \
    dst-address-list=VEREJKY new-connection-mark=VEREJKY_DOWN_C passthrough=\
    yes
add action=mark-packet chain=prerouting connection-mark=VEREJKY_DOWN_C \
    new-packet-mark=VEREJKY_DOWN passthrough=no
add action=mark-connection chain=postrouting comment=VEREJKY_UP \
    new-connection-mark=VEREJKY_UP_C passthrough=yes src-address-list=VEREJKY
add action=mark-packet chain=postrouting connection-mark=VEREJKY_UP_C \
    new-packet-mark=VEREJKY_UP passthrough=no
add action=mark-connection chain=prerouting comment=NEOMEZENO_DOWN \
    dst-address-list=NEOMEZENO new-connection-mark=NEOMEZENO_DOWN_C \
    passthrough=yes
add action=mark-packet chain=prerouting connection-mark=NEOMEZENO_DOWN_C \
    new-packet-mark=NEOMEZENO_DOWN passthrough=no
add action=mark-connection chain=postrouting comment=NEOMEZENO_UP \
    new-connection-mark=NEOMEZENO_UP_C passthrough=yes src-address-list=\
```

```
    NEOMEZENO
add action=mark-packet chain=postrouting connection-mark=NEOMEZENO_UP_C \
    new-packet-mark=NEOMEZENO_UP passthrough=no
add action=mark-connection chain=prerouting comment=SPEED_DOWN \
    dst-address-list=SPEED new-connection-mark=SPEED_DOWN_C passthrough=yes
add action=mark-packet chain=prerouting connection-mark=SPEED_DOWN_C \
    new-packet-mark=SPEED_DOWN passthrough=no
add action=mark-connection chain=postrouting comment=SPEED_UP \
    new-connection-mark=SPEED_UP_C passthrough=yes src-address-list=SPEED
add action=mark-packet chain=postrouting connection-mark=SPEED_UP_C \
    new-packet-mark=SPEED_UP passthrough=no
```