VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2018 Michal Řezáč

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

OPTIMALIZACE TRANZITU DAT V SÍTI
OPTIMIZATION OF DATA TRANSIT IN NETWORK

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Michal Řezáč

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Anna Kubánková, Ph.D.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Michal Řezáč ***ID:*** 186571
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Optimalizace tranzitu dat v síti

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte principy zajištění kvality služeb na linkové a sítové vrstvě ISO/OSI modelu a zajištění efektivity přenosu přepínané a směrované sítě. Analyzujte kvalitativní parametry stávající sítě a následně zdokumentujte zjištěné informace. Popište dostupné metody a funkce pro optimalizaci tranzitu dat dle výrobců síťových zařízení v definované síti. Na základě získaných podkladů zvolte nejvhodnější varianty pro optimální transit dat a navrhněte vhodnou metodiku testování. Aplikujte vybrané metody pro optimalizaci tranzitu dat. Postupným porovnáním výsledků získaných sledováním síťového provozu a optimalizaci konfigurace síťových prvků, určete nejvhodnější metodiku pro zajištění efektivního tranzitu dat sítí a porovnejte stav sítě před a po aplikaci zvolených postupů.

DOPORUČENÁ LITERATURA:

[1] WANG, Zheng. Internet QoS: architectures and mechanisms for quality of service. Morgan Kaufmann, 2001.

[2] MikroTik Wiki. Wiki.mikrotik.com [online]. Lotyšsko: MikroTik, 2005 [cit. 2017-09-05]. Dostupné z: wiki.mikrotik.com

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

Vedoucí práce: Ing. Anna Kubánková, Ph.D.
Konzultant: Ing. Lukáš Obršlík, NETlife, s.r.o.

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

ABSTRAKT

Bakalářská práce je rozdělena do dvou částí. První část se zabývá popisem nezbytných teoretických celků spolu s analýzou sítě ISP a dalšími vstupními informacemi. Tyto poznatky jsou dále využity v druhé části bakalářské práce. Praktická část se zabývala ověřením optimalizačních mechanismů v laboratorní síti. Následně širším testováním optimalizačních mechanismů, založených na různých způsobech značení datových toků a místě nasazení těchto pravidel. Dále byly zhodnoceny výhody a porovnání těchto metod.

KLÍČOVÁ SLOVA

DSCP, IPTV, QoS, reálný čas, zatížení, ztrátovost

ABSTRACT

This bachelor thesis is divided into two parts. The first part deals with and describes necessary teorethical units, together with analyse of ISP network and other input informations. These findings are further used in second part of bachelor thesis. The practical part dealt with testing of optimization mechanisms in the laboratory network. Thereafter has been done a wider tests of optimization mechanisms based on different ways of marking data streams and deploying these rules. The advantages and comparision of these methods were further evaluated.

KEYWORDS

DSCP, IPTV, QoS, real-time, load, packet loss

ŘEZÁČ, Michal. *Optimalizace tranzitu dat v síti*. Brno, 2017, 60 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Anna Kubánková, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Optimalizace tranzitu dat v síti“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Mé poděkování patří vedoucímu bakalářské práce, paní Ing. Anně Kubánkové Ph.D. za odborné vedení, zajímavé náměty a přínosné konzultace řešené problematiky. Neméně velké poděkování náleží kolektivu společnosti NETlife s.r.o, u které byla bakalářská práce vykonávána, především pak panu Ing. Lukáši Obršlíkovi, konzultantovi této bakalářské práce. Dále děkuji všem, kteří mě při tvorbě bakalářské práce a studiích motivují a podporují.

Brno ....

podpis autora(-ky)

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

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

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno ....

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM VÝPISŮ

ÚVOD

Nekončící trend, kdy je vyžadováno stále vyšších přenosových kapacit datových sítí, při co nejnižší odezvě a nulové ztrátovosti nutí poskytovatele datových služeb investovat značné sumy do robustních přenosových systémů. Aby byly sníženy náklady a zároveň zachována vysoká kvalita přenášených dat, tedy maximálně zefektivněn přenos dat, byla vytvořena disciplína zabývající se optimalizací přenášených dat *(Quality of Service)*. Díky rozlišení žádané velikosti kvality konkrétně poskytovaných služeb, je možné upravit datový tok takovým způsobem, že služby žádající okamžitou odezvu, respektive pracující v reálném čase budou přednostně odbaveny a méně časově náročné služby budou částečně potlačeny.

Metodikou zajištění kvality služeb se zabývá tato bakalářská práce. Cílem je prostudování možností zajištění kvality služeb, jak obecně, tak následně v definované síti poskytovatele internetu (ISP).

První část bakalářské práce uvádí teoretické celky spojené s optimalizací tranzitu dat v síti. Paralelně s popisem teoretických celků jsou uvedeny výsledky analýzy sítě ISP, které se optimalizace týká.

Druhá část práce přejímá teoretické poznatky o síti i problematice a aplikuje konkrétní mechanismy na otestování zvýšení efektivity tranzitu dat v síti. Po otestování daných metod byly vyřčeny hlavní výhody a nevýhody při použití konkrétních způsobů optimalizace. V posledním bodě byla vybrána nejvhodnější metoda pro optimalizovanou datovou síť.

1 TECHNOLOGIE PRO TRANZIT DAT

1.1 Služby regionálního ISP

Síť regionálního poskytovatele internetového připojení (dále ISP), která je předmětem této bakalářské práce zajišťuje datové připojení, bez limitů přenesených dat a času. Tato heterogenní síť, jejíž celky byly podrobně analyzovány v této práci nabízí služby *triple-play*, charakterizované spojeným přenosem dat, obrazu a zvuku. Všeobecně známé pod kombinací Internet, VoIP a IPTV.

Tyto služby jsou poskytovány, ve většinovém podíle za pomocí mikrovlnné technologie v členitém kraji Vysočina. Vzhledem k potřebám zákazníků z celého spektra, které odpovídají aktuálním trendům, konkrétně co nejvyšší propustnosti, společně s co nejnižší ztrátovostí dat a zpožděním, byl vytvořen tento projekt optimalizace datového provozu. Cílem optimalizace je zefektivnit využití přenosového pásma úpravou a priorizací datového provozu na 2. a 3. vrstvě, dle *International Standards Organization/Open Systen Interconnection* (dále ISO/OSI) modelu. Tato technika omezuje do značné míry nutnost tvorby nadbytečných přenosových kapacit.

1.2 Základní síťové architektury

Zaměřením problematiky na optimalizaci tranzitu dat na 2. a 3. vrstvu ISO/OSI modelu jsou v této kapitole uvedeny základní síťové architektury, které se využívají pro síťovou komunikaci, což je základní pilíř fungování komunikace každé sítě, každého síťového zařízení.

Síťová architektura je koncept, který svými funkcemi utváří možnou realizaci komunikační sítě. Tento celek sestává z fyzických prvků sítě, spolu s jejich funkčním uspořádáním, zvolenou konfigurací a dodržováním sady postupů a zásad, které jsou pro daný model v určité kombinaci specifické. Mimo model samotný jsou definovány i služby, které jsou skrze komunikační sítě distribuovány, tedy používány. Komunikační architektura nasazená v Internetu je lépe specifikována spíše sadou protokolů, jež spolu navzájem spolupracují, než přímo konkrétní komunikační architekturou, nebo využíváním určitého typu zařízení, případně metodami využívanými při jejich použití.

Referenční model ISO/OSI je koncepční model síťové architektury, shrnující definice postupů a standardy fungování komunikační sítě, případně jiného výpočetního zařízení s ohledem na jeho technologické provedení. Cílem tohoto souboru pravidel je maximálně efektivní kooperace diverzních komunikačních stanic, respektive systémů.

Díky složitosti síťové komunikace je i u modelu TCP/IP jeho architektura rozdělena do vrstev, které si vzájemně vyměňují informace. Vrstvy fungují na hierarchickém principu, kdy pro svoji činnost využívají vrstvy nižší a poskytují své vlastní služby vrstvě vyšší. Probíhající komunikace mezi jednotlivými systémy je řízena komunikačním protokolem. Architektura umožňuje variaci různých protokolů na určité vrstvě bez dopadu na celkovou komunikaci, tedy na vrstvy ostatní. TCP/IP komunikační model se skládá z pouze 4 vrstev, z nichž každá principiálně odpovídá jedné, nebo více vrstvám modelu ISO/OSI. Díky faktu, že tento model obsahuje 4 vrstvy, je komplexnější, co se vrstev týče. Implementace je levnější a díky vládní podpoře ve Spojených státech amerických, které iniciovaly vznik této architektury, nabýval v jeho počátcích rychleji na oblíbenosti, než model ISO/OSI. TCP/IP tak zaštiťuje svou protokolovou sadou celosvětovou síť Internet.[1][7]

Mezi hlavní rozdíl těchto architektur patří, že ISO/OSI je nyní spíše koncepční, reálně nevyužívaný model, zde zmíněný z výukového hlediska díky jeho jasnému popisu fungování a rozdělení na více vrstev.

I přes naznačení paralely mezi modely ISO/OSI a TCP/IP z hlediska složení jednotlivých vrstev a jejich funkcí jsou výjimky. Příkladem může být protokol *Transport Layer Security* (dále TLS) zajišťující zabezpečení komunikace. TLS protokol nespadá z hlediska abstraktních vrstev modelu ISO/OSI pouze do jedné vrstvy, ale díky metodice jeho fungování ho lze zařadit hned do několika vrstev (2, 5, případně 7).[1]

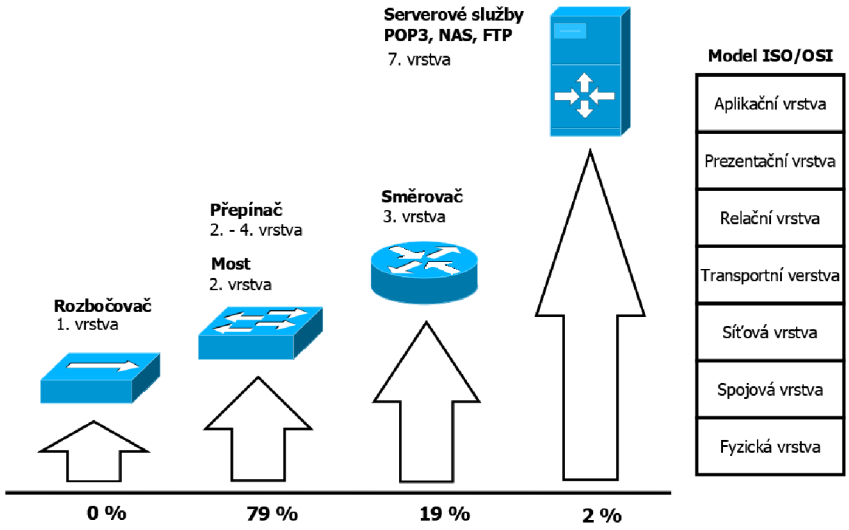
1.2.1 Rozdělení sítě ISP

Při rozlišování datového provozu a potažmo jeho optimalizaci z pohledu vrstvy spojové a síťové, modelu ISO/OSI dochází k úpravám přenášených dat vkládáním dodatečných informací do polí *Class of Service* (dále CoS) na vrstvě spojové a *Type of Service* (dále ToS) na vrstvě síťově. Možnosti těchto polí jsou popsány u kapitoly 1.4.3, která popisuje metodu diferencovaných služeb, používající ke své funkci značení priorit průchozího datového provozu, dále pak jeho optimalizaci.

Pro úpravu v přepínané síti, tedy na spojové vrstvě je využíván protokol 802.1Q. Díky kterému je možné rozdělení provozu do virtuálních lokálních sítí, takzvaných *virtual local area network* (dále VLAN) s konfigurovatelnou prioritou pomocí protokolu 802.1p.[9]

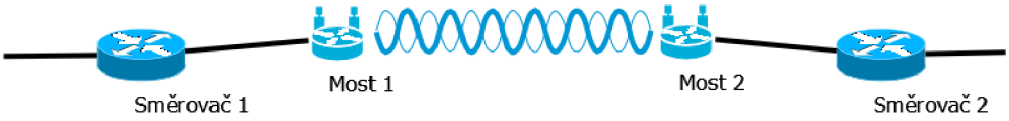
Samotné rozdělení sítě ISP, podle vrstvy na které operují použitá zařízení je znázorněno na obrázku 1.1. Z toho vyplývá, že 79 % prvků pracuje na 2. vrstvě. Na vrstvě 3. pak pracuje pouhých 19 % zařízení, zbylá 2 % jsou zastoupena zařízeními operujícími na 7. vrstvě. Tohoto zjištění bylo dosaženo při analýze sítě ISP.

I přes relativně nízký podíl prvků pracujících na 3. vrstvě, je síť z převážné části



Obr. 1.1: Rozdělení prvků, podle operační vrstvy ISO/OSI

směrovaná a optimalizace byla provedena právě na 3. vrstvě. Síť ISP je koncipována modelem jednoho centrálního prvku na jednom přístupovém bodu do sítě ISP, provádějícího směrování, s dalšími připojenými síťovými zařízeními, které jsou k jeho síťovým rozhraním připojeny již v režimu mostů. Tato metoda je demonstrativně znázorněna na obrázku 1.2.Tímto modelem vznikl velký podíl zařízení v režimu mostu, ale byl tím zjednodušen přenos po síti.



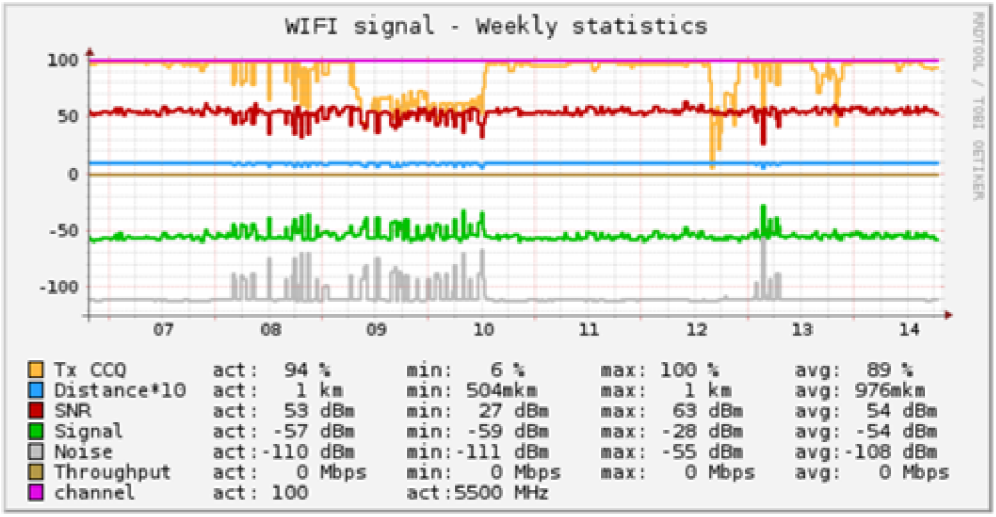
Obr. 1.2: Propojení směrovačů s využitím prvků v režimu mostu

1.3 Parametry ovlivňující přenos dat v rádiové komunikaci

Před řešením optimalizace datového toku je nutné uvést základní parametry, které díky specifické situaci mohou fatálně ovlivnit fungování celé sítě. Do takové míry, že optimalizační metody situaci již neovlivní. Tato kapitola popisuje možné problémové faktory v rádiovém prostředí, které musí být vyřešeny před další optimalizací

tranzitu dat.

Existuje celá řada faktorů dopadajících na přenos dat a kvalitu spojů v rádiovém prostředí. Kvalita a stabilita závisí na okolnostech, jako je členitost terénu, použitá vysílací a přijímací zařízení, využívané frekvenční pásmo a dalších, které budou rozepsány dále. V tomto případě, jsou uváženy pouze faktory s vlivem směřujícími k mikrovlnné komunikaci, nikoli optické a sonické komunikaci, kde je také využito bezdrátové prostředí, ale způsob využití technologie, klíčové parametry a úskalí zcela jiná a netýkají se tohoto případu. Obrázek 1.3 zachycuje záznam podstatných informací týkajících se kvality rádiového spoje. Byl pořízen monitorovacím softwarem Munin, jež pro svou funkci využívá *object identifier* (dále OID), které reprezentují jednotlivé informace, jako úroveň signálu a aktuální frekvenční kanál. Hodnoty jsou ze zařízení vyčítané za pomocí *Simple Network Management Protocol* (dále SNMP).



Obr. 1.3: Monitorovaná data mikrovlnného spoje za pomocí softwaru Munin

Soubor činitelů, které ovlivňují fungování mikrovlnného spojení lze dělit na dvě základní skupiny:

- Faktory, kterým se nedá vyhnout a je nutné je akceptovat. U těchto negativních vlivů můžeme pouze minimalizovat jejich dopad, nikoliv jim kompletně zamezit.
- Řešitelné vlivy, které lze zcela eliminovat úpravou konfigurace, inovací a dalšími postupy.

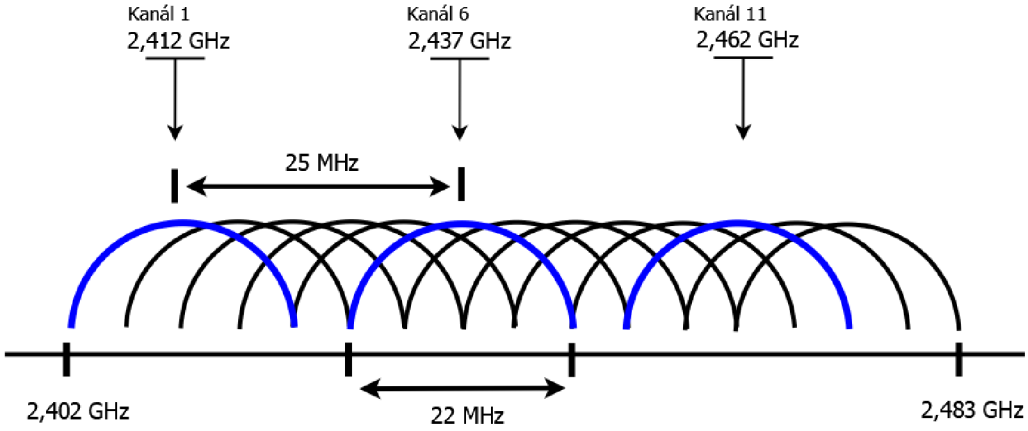
1.3.1 Konkrétní parametry rádiového prostředí

Jednotlivé parametry s dopadem na kvalitu mikrovlnného spoje, tedy přenosové vlastnosti jsou:

- **Fyzické překážky** – Mikrovlnné signály mají problémy pronikat skrze materiály. Dle typu překážky dochází k degradaci přenosových vlastností až k neschopnosti spojení sestavit. Překážky zahrnují vyvýšené body, budovy a mimo jiné i vegetaci. Čím větší je počet překážek mezi vysílačem a přijímačem, tím více bude signál ovlivněn, tudíž je žádoucí dodržení přímé viditelnosti mezi komunikujícími body. Obecně platí, že čím nižší frekvenční pásmo je využito, tím lepší jsou penetrační charakteristiky elektromagnetických vln, tedy signálu.[10]

- **Vyzařovací úhel signálu a vzdálenost mezi zařízeními** – Velikost vyzařovacího úhlu se výrazně liší u spojů bod-bod (dále P2P), kde je úhel menší, někdy v řádově jednotkách stupňů, aby nedocházelo k jeho zbytečnému rozptylu a interferencím s dalšími signály. Naopak u stanice, v roli bod-více bodů (dále P2MP)je úhel standardně větší, to až 360 stupňový, to u antén všesměrových, kde ovšem dochází k podstatnému zarušení celého okolí, nejen v určitém směru. Obecně tedy platí, že čím menší vyzařovací úhel je, tím méně interferuje s ostatními signály a má menší rozptyl. Tyto vlastnosti, jako rozptyl a interference dále rostou se vzdáleností komunikačních bodů, čím je tedy vzdálenost větší, tím více klesá úroveň signálu.
- **Frekvenční interference** – Díky narůstající oblíbenosti mikrovlnných zařízení dochází ke stále většímu zarušení bezlicenčních pásem 2,4 GHz a 5 GHz. Demonstrativně je zmíněno frekvenční pásmo 2,4 GHz. U tohoto pásma, jak lze

vidět na obrázku 1.4, je možné využití pouze 3 kanálů bez interference. S přibývající hustotou provozu a obsazením jednotlivých kanálu dochází ke snižování odstupu signál-šum, parametru známého jako *signal-noise-ratio* (dále SNR), tedy zvýšení šumu na pozadí. Mimo nelicencovaná frekvenční pásma jsou také privátní frekvenční pásma, které draží v České republice Český telekomunikačního úřad (dále ČTU). Právě zmíněný ČTU provádí kontrolu elektronických komunikací a vyhledává rušení ve frekvenčním pásmu 6 kHz až 300 GHz, kde působí jako regulační autorita.[2]



Obr. 1.4: Frekvenční překrývání u pásma 2,4 GHz

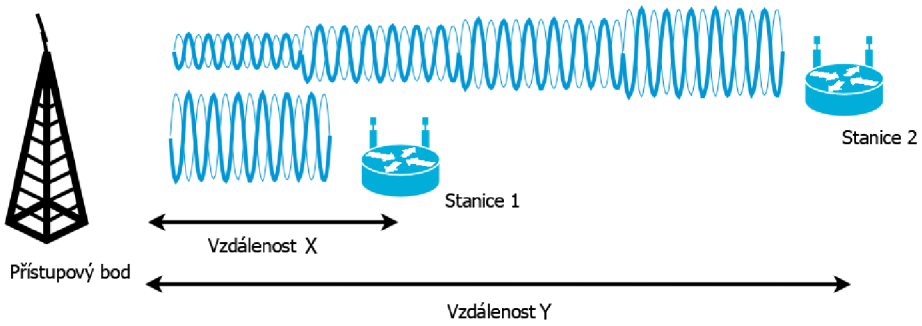
- **Sdílení signálu** – Mikrovlnné sítě v mnoha případech umožňují připojení P2MP, díky této možnosti musí přístupový bod zorganizovat rozvrh přenosu, kdy se jednotlivé stanice střídají v přenosu, tuto problematiku řeší MikroTik proprietárním protokolem Nstreme verze 2 (dále Nv2), který je zvláště popsán dále v této kapitole.

- **Lokální enviromentální faktory** – Faktor založen na výkyvech a extrémech počasí v oblasti realizace mikrovlnného spojení. Pro případný pokles signálu je implementována funkce *Auto Power Control* (dále ATPC), která monitoruje úroveň signálu a případně dočasně zvýší výstupní výkon vysílače za cílem zachovat předdefinovanou úroveň signálu.[10]

- **Odraz signálu** – Tento parametr je podstatný v husté zástavbě, tedy městech, kde může docházet až k několikanásobnému odrazu především od budov. Díky odraženému signálu u těchto "pozemních přenosů"dochází k špatné klasifikaci přijatých dat a jejich částečnému znehodnocení, tento problém může vyřešit

například vhodná modulace, jako *orthogonal frequency division multiplexing* (dále OFDM), používaná v mikrovlnných sítích standardem 802.11a.

- **Výkonové omezení vysílače** – Předpisy stanovené ČTU určují maximální možný výstupní výkon vysílače. Hodnoty jsou specifické, dle pásma, ve kterém se vysílací prvek nachází. Pro pásmo 5,470-5,725 GHz definuje omezení ČTU podle VO-R/12/09.2010-12 na maximální vyzářený výkon W při použití automatické regulace výkonu, bez regulace je maximální povolený vyzářený výkon pouze 0,5W. Mimo přímo nastavený výstupní výkon antény jsou podstatné další faktory, jako vyzařovací úhel vysílače a zisk přijímací antény. Všeobecně platí, že s přesnějším, tedy menším vyzařovacím úhlem se snižuje úroveň výstupního výkonu vysílače. Tyto regulace výkonu jsou velmi podstatné pro správné fungování sítě. Při modelové situaci, kdy bude mít vysílač blíže postavený k přijímacímu bodu příliš vysoký výstupní výkon, degraduje úroveň signálu ostatních připojených zařízení, jež mají nižší úroveň signálu způsobenou geografickou polohou, eventuálně průchodem prvků, které stíní cestu signálu, modelově zobrazeno na obrázku 1.5. Zde Stanice 2 díky své poloze vzhledem k vysílači dosahuje horší propustnosti, situaci zhoršuje i neadekvátně nastavený výstupní výkon ze Stanice 1, u které by bylo vhodné zvolit nižší úroveň výstupního výkonu, která by nijak zvláště nezhoršila propustnost Stanice 1, ale méně by degradovala signál Stanice 2.[2]



Obr. 1.5: Rozdíl geografického rozložení stanic vzhledem k síle signálu

- **Zpětná kompatibilita využívaných standardů** – V sítích pracující na standardu 802.11 má zásadní vliv na fungování verze standardů, jenž přenosové zařízení používají. Pokud má síť využít plný potenciál nových technologických norem, modelově 802.11ac, je nezbytné zajistit, aby síť obsahovala pouze zařízení kompatibilní s tímto standardem.

- **Polarizace signálu** – Při výstupu signálu z vysílače dochází k jeho polarizaci, základní metodika polarizace použitá u mikrovlnných spojů je polarizace vertikální a horizontální. Pro správné fungování přenosu je nutné, aby antény vysílaly i přijímaly shodně polarizovaný signál. V opačném případě dochází k jeho vysoké degradaci

- **Režie přenosu** – Vzhledem k nezbytnosti využití šifrování, překladů IP adres aj., dochází k omezení maximální přenosové rychlosti těmito režijními kroky prováděnými při zpracování přenášených dat. Někteří výrobci však deklarují rychlosti „reálného světa“ kde se již počítá s režií a udávaná rychlost se více blíží reálně dosažitelné.

1.3.2 Nstreme verze 2 (Nv2)

Nstreme verze 2 (dále Nv2), proprietární protokol společnosti MikroTik, nadstavba pro sadu 802.11 je založen na *Time Division Multiple Access* (dále TDMA), zahrnuje metodu *Carrier Sense Multiple Acces with Collision Avoidance* (dále CSMA/CA), která zjišťuje klidový stav ve využívaném rádiovém prostředí, využívaném prvky podporující standardy 802.11.

Pokud je síťová struktura založena na protokolu Nv2, je řízena přístupovým bodem, ten vytvoří časové rámce, které periodicky přiděluje. Tyto časové rámce se dynamicky rozdělí podle aktuální potřeby na vysílání dat *Transmitting* a přijímání dat *Recieving*.

Čas datového příjmu přístupového bodu se dále rozděluje jednotlivým stanicím na základě jejich přenosových požadavků. Na začátků každé vysílací smyčky, respektive periody, vyšle přístupový bod časový rozvrh, ve kterém deklaruje, kdy a po jakou dobu má která stanice vysílat.

Pro případ, že se do sítě vstoupí další stanice, přijímá přístupový bod po určitý čas provoz od nespecifikované stanice. V tomto čase se nově připojená stanice zaregistruje k přístupovému bodu. Během této komunikace se přístupový bod snaží vypočítat vzdálenost nově přiřazené stanice, jelikož tato vzdálenost je posléze zahrnuta v novém časovém rozvrhu vysílání.

Pro implementaci kvality služeb má Nv2 vložen proměnný počet prioritních front s předvoleným plánovačem kvality služeb.[5]

1.4 Kvalita služeb (QoS)

S přibývajícími požadavky ze strany uživatelů, co se objemu přenášených dat týče a zároveň na druhé straně ISP s tendencí využít poskytované zdroje co nejefektivněji, vznikla nutnost vytvoření metodik, které by dokázaly řídit datový provoz efektivněji než doposud.

Díky obeznámení a úpravou konfigurace síťových prvků vyplývající z předešlé kapitoly, zabývající se parametry ovlivňujícími kvalitu přenosu dat v rádiovém prostředí lze řešit kvalitu služeb (dále QoS) s dostatečnou efektivitou. V případě nevhodně zvolených, eventuálně dosažených parametrů týkajících se přenosu dat v rádiovém prostředí by nebylo možné docílit požadovaných výsledků, ani za pomocí QoS.

Za pomoci QoS lze kategorizovat provoz do jednotlivých skupin, které budou odbaveny dle jejich priority, respektive nasmlouvaných podmínek známých jako *service-level agreement* (dále SLA). Tím lze dojít k zjednodušení poskytování služeb s garantovanou kvalitou, a to i v sítích, u kterých je přístup k přenosovému médiu řešen na bázi konkurenčního přístupu, jako jsou sítě mikrovlnné. U podstatné části IP sítí je stále běžnou metodou zajištění QoS pomocí metody Best-Effort, který nehledí na ztrátovost a případné zpoždění dat.[8]

Při nasazování metodik zajištující kvalitu služeb, se hledí na několik klíčových parametrů:

- Přenosové pásmo – *Bandwith* [Mbit/s]
- Datové zpoždění – *Delay* [ms]
- Rozptyl zpoždění – *Jitter* [ms]
- Ztrátovost – *Packet loss* [%]

Dané parametry mají vliv na výslednou kvalitu služeb, ovšem jsou nadstavbou po zajištění dostatečně kvalitního datového spojení s klíčovými parametry a faktory, popsanými v kapitole 1.3.

1.4.1 Best-Effort

Síť optimalizovaná pomocí metody Best-Effort (RFC 5290), nazývaná i jako *lack of QoS* se sice řadí mezi metody QoS, ovšem nezahrnuje žádné postupy a politiky při tranzitu dat sítí, které by uživateli zajišťovali určitou prioritu jeho služeb, jako prioritu specifických dat, případně datové zpoždění. Aplikace zasílají data a ty jsou sítí přenášena s maximálním možným využitím rezervovaných síťových prostředků.[9]

Mezi hlavní výhody sítí typu Best-Effort je režie přenosu dat, jenž je ve srovnání s IntServ i DiffServ minimální. Díky jednoduché a nulové nutnosti implementace této metody při porovnání se službami se zaručenou spolehlivostí, dobré funkčnosti při stavu nepřetížené síťové infrastruktury je tato metoda QoS stále často nasazována.[6]

Na tomto principu přenosu dat je založen veškerý datový provoz v IP sítích, který nebyl nijak dále optimalizován, tudíž se s touto metodou běžně setkáváme například v domácích, respektive lokálních sítích.

1.4.2 Integrované služby (IntServ)

Model IntServ (RFC 1633), známý také jako *Hard QoS* model, je prvním průkopníkem, který si již od roku 1994 klade za cíl zajištění zaručené služby v IP sítích. U IntServ definuje své požadavky aplikace žádající o přenos dat. Základní model IntServ obsahuje:

- Kontrola přístupu (*Admisson Control*)
- Rezervační protokol (*Resource Reservation Protocol*)
- Klasifikátor (*Packet Claesifier*)
- Plánovač paketů (*Packet Scheduler*)

Provoz rozdělený dle IntServ se dělí do kategorií:[7]

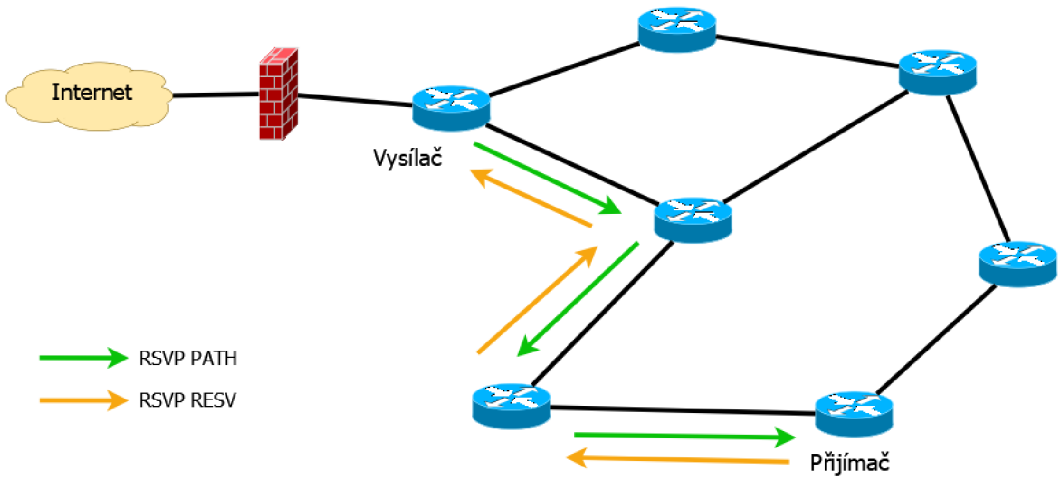
- *Real Time Intolerant* (RTI) – Kategorie s garantovanými prostředky, sem spadají hlasové služby.
- *Real Time Tolerant* (RTT) – Varianta pro aplikace s vyššími požadavky, než Best-Effort, data jsou v drtivé většině doručena, většina z nich dosahuje minimálního zpoždění, služby s přenosem obrazu .
- *Elastic multimeda application* – Provoz bez požadavku na doručení, tedy Best-Effort, služby využívající tuto kategorii přenosu dat jsou nepatrně, eventuálně nezávislé na časovém zpoždění a procentu doručených dat.

Ve chvíli, kdy aplikace žádá o vysílání dat, požaduje jisté parametry přenosu dat, jako jsou šířka přenosového pásma a stupeň důležitosti dat. V tomto okamžiku probíhá kontrola přístupu *Admission Control*, během které se na základě zachování konzistence dříve stanovených záruk rozhodne o vyhovění, případně odmítnutí

přenosu. V případě odmítnutí požadavku o sestrojení nového spojení má iniciátor požadavku na nové spojení možnost zvážit své nároky a případně je snížit.

Pokud dojde k přijetí požadavku, je nutné informovat síťové zařízení, které mají spojení zprostředkovat. Tento úkol plní rezervační protokol, běžně RSVP. Rezervace spojení je poněkud komplikovaná. Musí se rozšířit informace o navázání nového spojení včetně jeho nároků, to vše se děje během dynamicky se měnící situace v síti.

Zařízení vyžadující spojení vyšle zprávu PATH směřující k požadovanému příjemci. Po přijetí zprávy PATH přijímač odpovídá zprávou RESV. RESV rezervuje prostředky ve směrovací trase určené předchozí zprávou PATH. Pokud některý ze směrovačů narazí na nedostatek svých kapacit, vyšle PATH-ERR ze strany vysílače a RESV-ERR ze strany přijímače, proces navázání spojení je naznačen na obrázku 1.6.



Obr. 1.6: Vytváření rezervací na přenosové trase pomocí RSVP

Proces rezervování je periodicky opakovaný, což generuje další datový provoz. Při konci relace ze strany přijímače, nebo směrovače jsou vyslány zprávy PATH TEAR, RESV TEAR. Další RSVP zprávy:[6]

- PATH – Nese data od vysílače dat *sender* k přijímači dat *receiver*, označuje cestu, kterou budou procházet požadovaná data.
- RESV – Rezervační požadavek od příjemce dat.
- PATH-ERR – Indikace záporné odpovědi na zprávu typu PATH.
- RESV-ERR – Indikace záporné odpovědi na zprávu typu RESV.
- PATH-TEAR – Odstranění stavu PATH – cesty, mezi vysílačem a přijímačem dat.
- RESV-TEAR – Zrušení rezervace na trase mezi vysílačem a přijímačem dat.

- RESV-CONF – V případě, že příjemce dat vyžaduje potvrzení, vysílač dat zašle tuto zprávu.

Po sestrojení přenosové trasy za pomoci rezervačního protokolu dochází ke klasifikaci dat *Packet Clasifier*, u těchto dat se upravuje port a IP adresa přijímače. Změněným hodnotám odpovídá služba s dohodnutou třídou. Tento proces probíhá u vysílače i jednotlivých směrovačů v trase k příjemci.

Při odesílání dat je provoz řazen podle jeho priority do front a následně odesílán pomocí nakonfigurovaných vah, tuto úlohu plní plánovač paketů *Packet Scheduler*.

Tento typ zajištění služeb najde své využití spíše v telefonii, kde utváří End-to-End spojení pro jednotlivé hovory, v globálním měřítku se od něj ustupuje. Hlavní příčiny jsou neefektivní hospodaření s přenosovým pásmem a režie pro celou síť, před sestavením spojení a rezervací zdrojů, ale i během probíhajícího přenosu stavovými zprávami o spojích.[4]

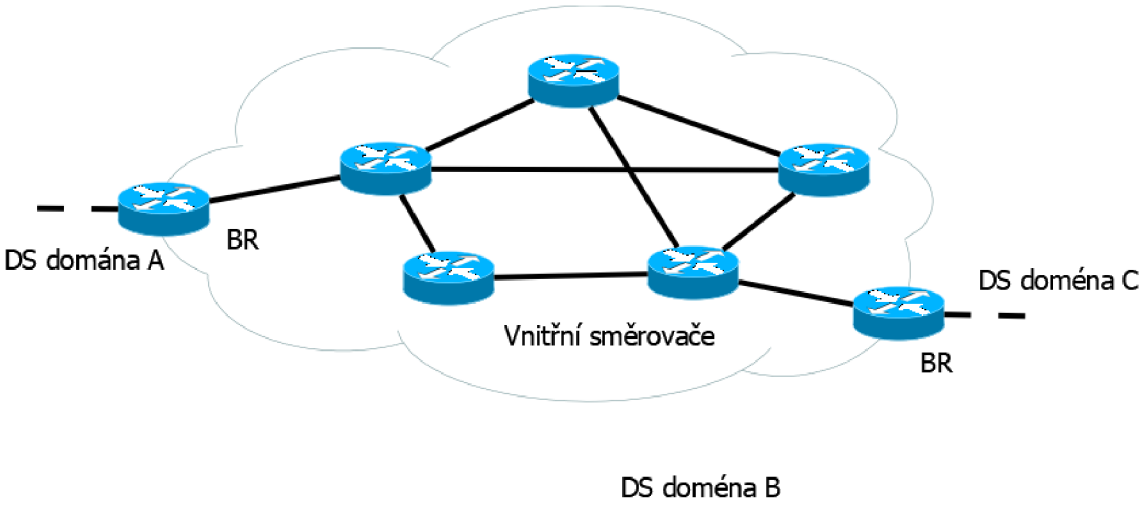
1.4.3 Diferencované služby (DiffServ)

První definice Diferencovaných služeb (dále DiffServ), označované také *Soft QoS* modelem byla roku 1998 (RFC 2475), po níž následovaly další úpravy v hned několika RFC.

Zde je veškerá datová filtrace a úprava na hraničním směrovači, takzvaném *Border Router* (dále BR) jednotlivých DiffServ domén (dále DS), zobrazených na obrázku 1.7, z kterého je patrné složení sítě, respektive BR a vnitřních uzlů, v případě sítě ISP směrovačů. DS doména reprezentuje určitou část IP domény, která nabývá schopností diferenciovaných služeb. Na BR dochází k dělení jednotlivých dat podle jejich nároků na doručení. V síti DiffServ jsou nejprve deklarovány požadavky QoS. Aplikace, které by v modelu IntServ žádali o přidělení daných prostředků, jsou této role zbaveny.

Nasazení architektury DiffServ spočívá v principiálně jednoduché metodice skládající se z těchto kroků:

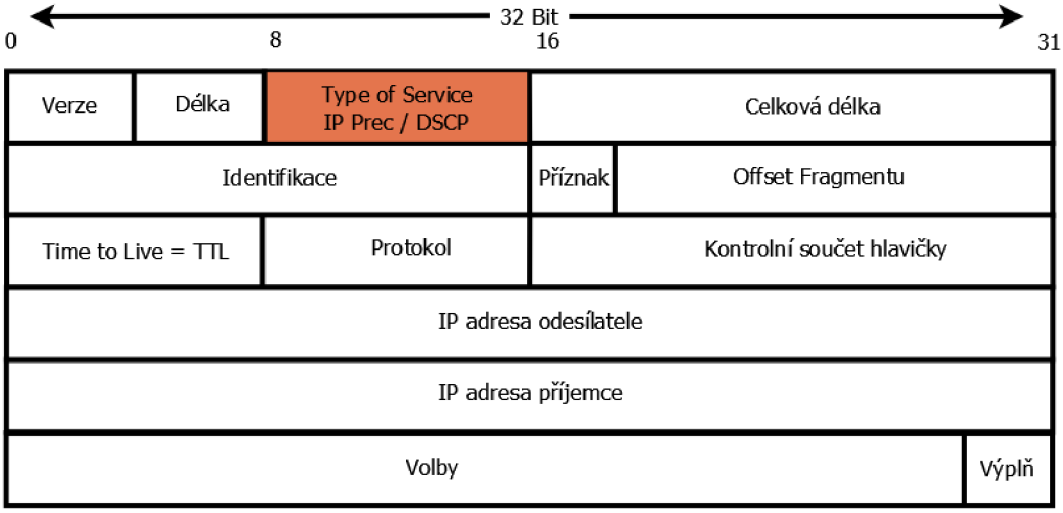
- Klasifikace provozu (*Classification*)
- Značení paketů (*Packet Marking*)
- Měření (*Traffic mettering*)
- Tvarování (*Traffic Shapping*)
- Definování politik pro jednotlivé třídy (*PHB*)



Obr. 1.7: DS doména

Ke klasifikaci (*Classification*) je využito pole CoS v hlavičce rámce na 2. vrstvě ISO/OSI – rozšířením hlavičky rámce o 4 bajty. CoS sestává ze 3 bitů a nabývá hodnot priority 0 až 7.

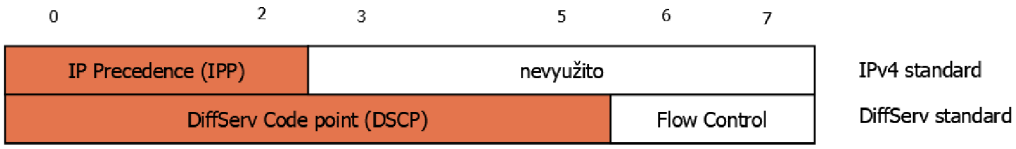
Pro 3. vrstvu ISO/OSI se používá pole ToS, které je 8 bitů dlouhé. V poli ToS je vložena hodnota *Differentiated Services Code Point* (dále DSCP), využívající 6 bitů z 8 bitů tohoto pole. Pole ToS lze vidět na obrázku 1.8, reprezentující hlavičku IP paketu s jejím rozdělením.[8]



Obr. 1.8: Hlavička IP paketu

DSCP nabývá hodnot mezi 0 a 63, toto pole se překrývá s IP Precedens (dále IPP) jak je naznačeno na obrázku 1.9. IPP má shodnou velikost, jako na 2. vrstvě

ISO/OSI, tedy 3 bity a nabývá hodnoty 0 až 7. Doporučené rozdělení úrovní tříd v IPP a DSCP jsou znázorněny v tabulce 1.1. Před rozšířením o DSCP, které bylo vytvořeno na míru DiffServ se využíval výhradně IPP, ten je konvertibilní s DSCP.



Obr. 1.9: Pole ToS a jeho využití při IPP a DSCP

Data, rozdělena (*Packet Marking*) podle nároků, změní své pole CoS, respektive ToS dle tříd, které jim byly přiřazeny. K správnému označení paketů slouží u IPv4 pole DSCP a IPP (možno využít IP toku, formát, port, DNS a jiných). Hodnotu DSCP a IPP můžeme najít v hlavičce paketu. Roli ToS u IPv6 převzal oktet TRAFFIC_CLASS.[4]

Díky funkci omezení rychlosti *(rate limiting)*, která se provádí na směrovačích podél celé trasy přenosu, na nichž jsou obsaženy funkce pro tvarování (*Traffic Shaping*), využívající metody *Token bucket*, *Leaky bucket* a TCP plovoucí okno. Tvarovače odesílají data konstantní rychlostí a urovnávají přenosové špičky provozu za pomocí zvoleného frontování. Nevýhodou frontování je, že může dojít k zahození i garantových dat, to záleží na zvoleném mechanismu front, jednotlivé fronty využívané na platformě MikroTik jsou popsány v kapitole 1.3.6. Data směřující od zdroje, respektive od BR, se po změření (*Traffic Metering*) porovnávají s dohodnutými podmínkami mezi zákazníkem a ISP, tedy dle SLA. Data, která těmto kritériím nevyhovují jsou přetvarována, upravena, respektive přeznačena, nebo zahozena.[8]

Směrovače v DS se zachovají dle *Per Hop Behaviors* (dále PHB), jenž se na nich nakonfiguruje. Bez konfigurace PHB by samotné označení na BR nemělo žádný efekt. Zde je definováno, jak se bude s danou hodnotou ToS zacházet, dokud nedorazí ke svému cíli, který leží v této síti, nebo neopustí síť, kde jsou hraničním směrovačem přetypovány hodnoty ToS, za předpokladu, že má síť, do které data vstupují jinak nastavené priority QoS, nebo funguje na jiném modelu QoS.[5]

Tab. 1.1: Přiřazené hodnoty CoS, IPP, DSCP a PHB odpovídající typu dat[5]

COS/IPP	DSCP	PHB	Typ dat
7	56	CS7	Řízení sítě
6	48	CS6	Vnitrosíťové řízení
5	46	EF	Zvukové služby
5	40	CS5	Vysílání videa
4	36	AF41	Multimediální konference
4	32	CS4	Reálný čas
3	28	AF31	Multimediální vysílání
3	24	CS3	Hovorová signalizace
2	20	AF21	Transakční data
2	16	CS2	Nárazový provoz
1	12	AF11	Nízká priorita
1	8	CS1	Služby na pozadí
0	0-7	BE	Základní nastavení

Rozdíly mezi modely QoS

Charakteristické rozdíly mezi jednotlivými optimalizačními metodami, v tabulce 1.2.

Tab. 1.2: Rozdíly modelů QoS [7]

Metoda	Best-Effort	Diferencované služby	Integrované služby
Služba	Spojení bez garance	Garance toku	Garance pro spojení
Orientace	End-to-End	Doména	End-to-End
Rozsah	NA	Nastavení pro DS	Nastavení pro spojení

Používané typy front

- BFIFO, PFIFO, MQ PFIFO – Fronty založené na frontě typu FIFO, první do fronty vstoupí – první bude odbaven. Liší se dle typu měření mezi PFIFO a BFIFO (pakety, bajty). MQ PFIFO má navíc podporu pro vícenásobné fronty.[5]

- RED (*Random Early Drop*) – Fronta, která zahazuje příchozí data, dle aktuální velikosti fronty, při nízkém naplnění nezahazuje žádná data, mezi minimem a maximem zaplnění zahazuje náhodně vybraná data. Nad hranicí maxima fronty zahazuje veškerá příchozí data.[5]

- SFQ (*Stochastic Fairness Queuing*) – 4 FIFO logické fronty s Round-robin algoritmem využívající informace o procházejících datech jako jsou porty a IP adresy, tyto data pak člení až do 1024 dílčích toků. Celé SFQ může obsahovat 128 paketů v možných 1024 dílčích frontách.[5]

- PCQ (*Per Connection Queuing*) – Tento mechanismus frontování je detailněji popsán, protože se v analyzované síti využíval před optimalizací.[5]

Per Connection Queue, (dále PCQ) frontové systém byl navržen pro optimalizaci již masově využívaných QoS systémů, kde jsou v mnoha případech fronty pro různé toky identické. PCQ tyto fronty seskupuje a zjednodušuje tak jejich komplexní fungování.

PCQ využívá klasifikátory pro identifikaci jednotlivých podkanálů, poté jsou přiděleny individuální délky front typu FIFO na každý podkanál. Následně jsou všechny podkanály sloučeny a globálně nastaveny finálními parametry, omezením velikosti pro tuto frontu.

Díky PCQ není nutné mít 50 obdobných front s danými parametry, ale pouze jednu PCQ, zahrnující 50 podkanálů.
Parametry PCQ:

- Klasifikátor (*pcq-classifier*) - Výběr podkanálu

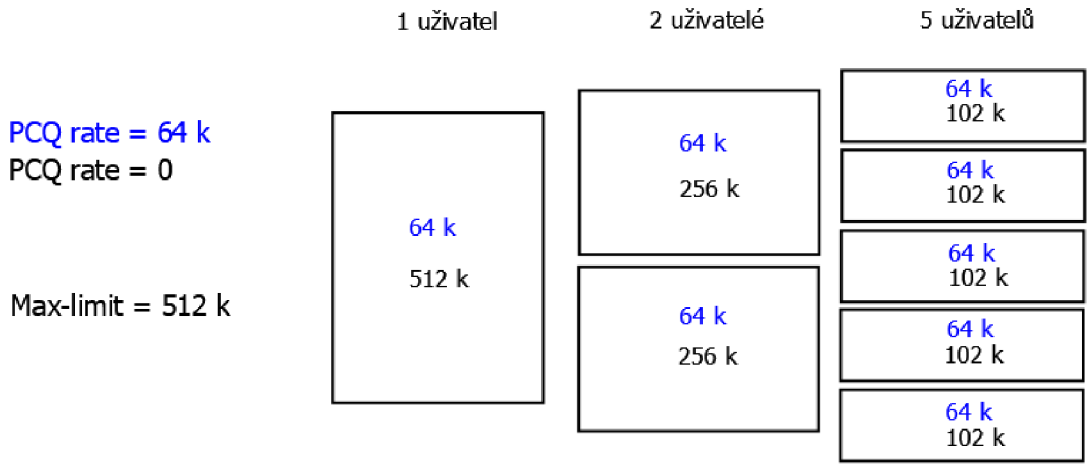
- Datový tok (*pcq-rate*) - Maximální možný datový tok všech podkanálu

- Limit (*pcq-limit*) - Velikost fronty jednotlivých podkanálů

- Celkový limit (*pcq-total-limit*) - Maximální množství dat ve všech podkánálech

Klíčový parametr PCQ Rate umožňuje nastavení velikosti přenášených dat. Při volbě PCQ Rate = 0, bude v situaci celkového datového toku 512k rozdělen pro

všechny uživatele rovným dílem z celkové velikosti. Pokud je zvoleno PCQ Rate = 64k, dojte k definici maxima datového tuku. Při 1 uživateli poté bude 80 % pásma nevyužito, kdežto v případě Rate = 0 bude využito 512/512, tedy celá kapacita. Situace přidělování minimálního pásma je na obrázku 1.10.[5]



Obr. 1.10: Vliv parametru PCQ Rate

Mimo tyto metody frontování jsou obecně známe i fronty WFQ, CBWFQ, WRED a LLQ.[5]

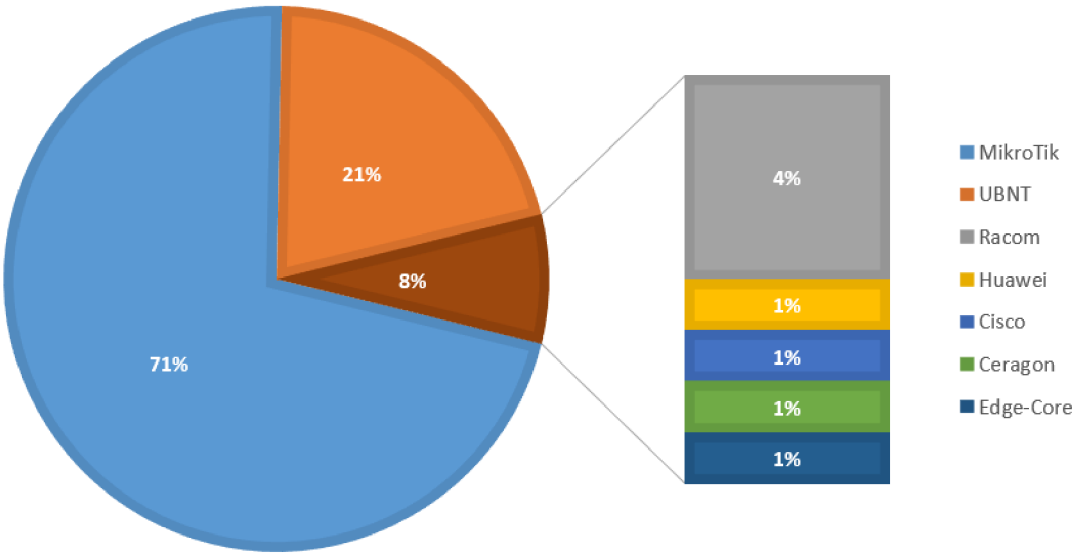
1.5 Nasazené platformy

Po analýze sítě regionální ISP bylo dosaženo závěru, že majoritní podíl síťových prvků používaných v sítí pro přenos dat na úrovni transportní části sítě je v 71 % značky MíkroTik. Druhé nejpočetnější zastoupení tvoří síťové prvky firmy UBNT s podílem 21 %. Zbylých 8 % spadá pod Racom, Huawei, Cisco, Ceragon a Edge-Core, jak vyplývá z obrázku 1.11.

K analýze sítě byl využit administrační a dohledový systém ISPadmin, který ISP využívá ke své činnosti.

1.5.1 Podpora optimalizace dat

Směrovače, které zprostředkovávají optimalizaci přenosu dat podporují práci s polem ToS, v němž jsou definovány jednotlivé hodnoty IPP a DSCP. Hodnoty DSCP byly využity pro značení provozu na BR a dále byly v rámci celé sítě ISP využívány k selekci provozu. Využití DSCP pole bylo upřednostněno před polem IPP, z důvodu většího množství klasifikovatelných tříd.[3][4][5]



Obr. 1.11: Zařízení v transportní části sítě dle výrobce

1.5.2 Páteřní prvky sítě ISP

Klíčovými prvky sítě ISP byly shledány zařízení MikroTik, konkrétně prvky provádějící směrování přes hlavní datové linky ISP. Vysílací antény jsou pak připojeny k rozhraním směrovačů a zprostředkovávají fyzický přenos dat, jsou nakonfigurovány v režimech mostů.

Jednotlivé modely provádějící směrování na hlavních datových linkách ISP jsou:

- MikroTik CCR1036-12G-4S-EM
- MikroTik RB3011UiAS-RM
- MikroTik RB2011UiAS-RM

Parametry páteřních směrovačů jako jsou rozhraní, výpočetní výkon, RAM paměť a pracovní teplotní rozsah, při kterém mohou být prvky použity jsou vypsány v tabulce 1.3.

Téměř všechny parametry se zdají podstatné - velkokapacitní rozhraní nutné pro přenos s možností datového toku i 1 Gbps vyžadují pro zpracovávaná data dostatečný výpočetní výkon a velikost RAM mezipaměti. Vedle těchto parametru se zdá teplotní rozsah poněkud nepodstatný, ovšem pokud se uváží, v jakých prostředích jsou tyto zařízení umístěna, tedy často ve venkovních podmínkách, kde může

Tab. 1.3: Parametry páteřních směrovačů[5]

Zařízení	MikroTik CCR1036-12G-4S-EM
Rozhraní	4x SFP, 12x 10/100/1000 Eth, Sériové rozhraní
Procesor	TLR4-03680CH-12CE-A3c, 36 jader / 36 vláken, 1,2 GHz
RAM	4 GB
Teplotní rozsah	-20 °C až 60 °C
Zařízení	MikroTik RB3011UiAS-RM
Rozhraní	1x SFP, 10x 10/100/1000 Eth, Sériové rozhraní
Procesor	IPQ-8064-0-519FCBAGA-TR-01-0, 2 jádra / 2 vlákna, 1,4 GHz
RAM	1 GB
Teplotní rozsah	-30 °C až 70 °C
Zařízení	MikroTik RB2011UiAS-RM
Rozhraní	1x SFP, 5x 10/100/1000 Eth, 5x 10/100 Eth, Sériové rozhraní
Procesor	AR9344, 1 jádro / 1 vlákno, 600 MHz
RAM	128 MB
Teplotní rozsah	-35 °C až 65 °C

v každém ročním období docházet k extrémním teplotám blížícím se hranicím jejich pracovního rozsahu.

Jak je patrné z uvedených dat v tabulce 1.3, každé z těchto zařízení dosahuje jiných přenosových výsledků. Pro přiblížení byly vybrány 4 rozlišné kombinace, 2 měření v režimu mostu, 2 měření v režimu směrovače. FastPath nastavení značí zvolení průchodu zařízení, bez firewallové filtrace a případných dalších úprav dat. U dvou zbylých měření byly využity právě zmíněné filtrace toku za pomocí 25 pravidel, pro 2. měření. U 4. měření byl proveden průchod dat skrze 25 front. Jaké dopady má konkrétní konfigurace při různých velikostech zpracovávaných dat lze vidět v tabulkách 1.4, 1.5, 1.6.

Tab. 1.4: Datová propustnost CCR1036-12G-4S-EM[5]

Režim	Nastavení	1518 bajtů Kpps/Mbps	512 bajtů Kpps/Mbps	64 bajtů Kpps/Mbps
Přemostění	FastPath	1300/15792	3759/15399	28808/14750
Přemostění	25 filtrovacích pravidel	1300/15792	3760/15403	5164/2644
Směrování	FastPath	1300/15792	3762/15411	28808/14750
Směrování	25 front	1300/15792	3762/115411	7643/3913

Tab. 1.5: Datová propustnost RB3011UiAS-RM[5]

Režim	Nastavení	1518 bajtů Kpps/Mbps	512 bajtů Kpps/Mbps	64 bajtů Kpps/Mbps
Přemostění	FastPath	325/3947	940/3849	1530/784
Přemostění	25 filtrovacích pravidel	325/3947	384/1574	349/179
Směrování	FastPath	325/3947	940/3849	1438/736
Směrování	25 front	325/3947	420/1719	420/215

Tab. 1.6: Datová propustnost RB2011UiAS-RM[5]

Režim	Nastavení	1518 bajtů Kpps/Mbps	512 bajtů Kpps/Mbps	64 bajtů Kpps/Mbps
Přemostění	FastPath	122/1482	232/950	270/138
Přemostění	25 filtrovacích pravidel	84/1015	86/352	88/45
Směrování	FastPath	122/1482	210/860	227/116
Směrování	25 front	101/1221	104/426	107/55

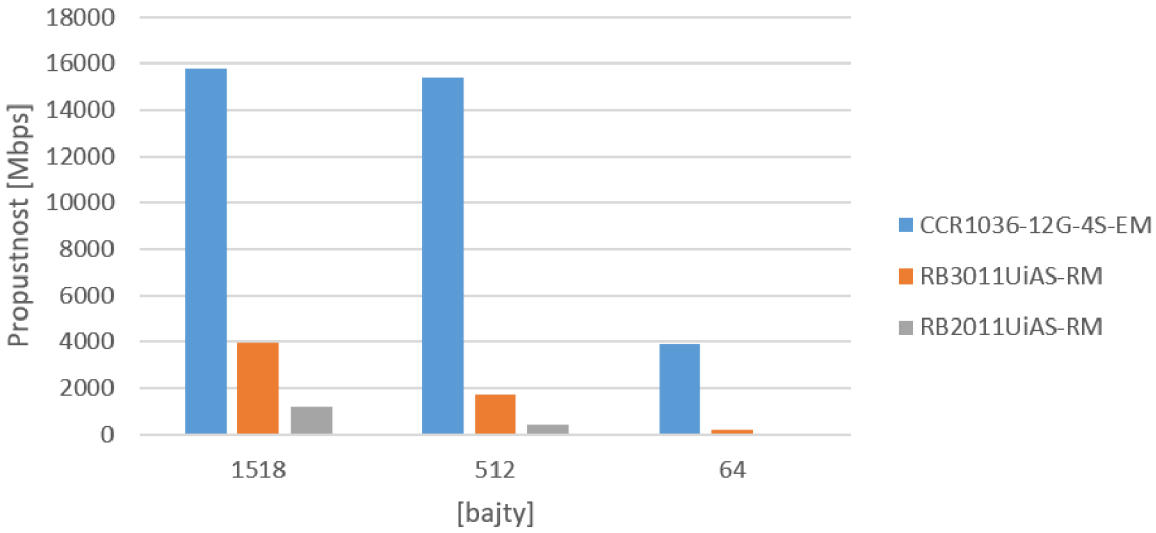
Porovnání propustnosti těchto směrovačů je na obrázku 1.12. U tohoto srovnání byla vybrána varianta směrování s 25 frontami, z důvodu využití obdobného frontování při optimalizaci tranzitu dat v síti ISP. Obrázek znázorňuje 3 směrovače a jejich propustnost při různých velikostech datových jednotek, konkrétně přenos při 1518, 512 a 64 bajtech.

1.5.3 MikroTik

Vzhledem k faktu, že společnost MikroTik tvoří majoritní část sítě ISP (71 %), která bude tvořit drtivou většinu optimalizace provozu, tato kapitola stručně popisuje tuto společnost a jejím zaměřením.

Litevská firma vznikla roku 1995, za účelem vývoje mimo jiné routerů a mikrovlnných systémů pro ISP. Po dvouleté zkušenosti s hardwarem především industriálního rázu se rozhodlo pro vytvoření vlastního operačního systému RouterOS. RouterOS poskytuje rozsáhlou kontrolu, flexibilitu a stabilitu pro veškeré datové rozhraní a směrování.[5]

V roce 2002 přidala ke svému vývoji RouterOS i výrobu vlastního hardware, známého pod označením RouterBOARD. Nyní má tato firma zaměstnávající zhruba 160 zaměstnanců zákazníky po celém světě.



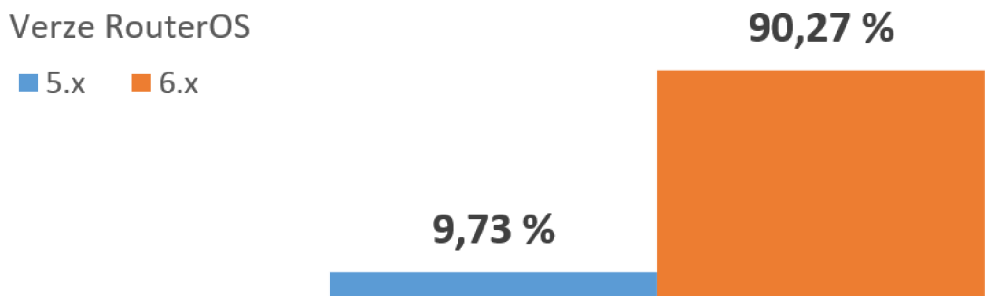
Obr. 1.12: Propustnost páteřních směrovačů[5]

RouterOS

RouterOS je operační systém pracující na zařízeních RouterBOARD, tedy MikroTik. Mimo platformy MikroTik RouterBOARD ho lze nasadit i na počítač, resp. server s architekturou x86, kde je schopný plnit standardní síťové úkony jako směrování, firewall, nebo VPN server, mimo jeho další možnosti. Operační systém RouterOS je založen na základu operačního systému Linux v2.6.[5]

RouterOS je vyvíjen a rozšiřován od roku 1997, nyní je aktuální verze 6.x. Postupně se upravovaly jak základní funkce, jako *print* (pro zobrazení položek), tak i podstatnější funkce, charakteristicky *Fast Path*. V tomto případě, jak lze vidět na obrázku 1.13, jsou v síti nasazeny verze:

- RouterOS 5.x - vyvíjeno v období 2011-2013
- RouterOS 6.x - uveden roku 2013, stále se inovuje a postupně jsou uvolňovány balíčky obsahující aktuální změny a nadstavby

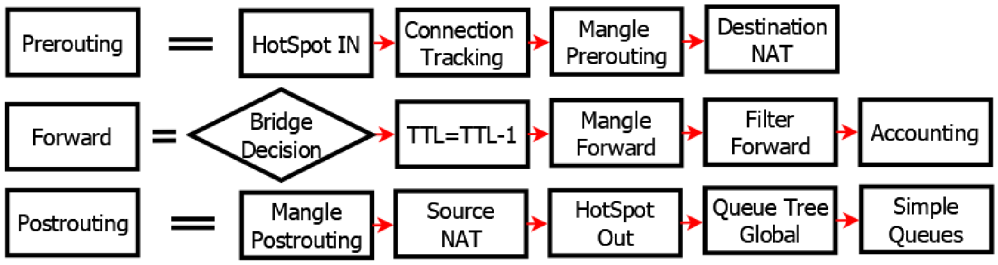


Obr. 1.13: Používané verze RouterOS v sítí ISP

Packet Flow

RouterOS je navržen pro intuitivní ovládání v různých konfiguračních režimech. Tento koncept je otevřen pro velké množství úprav jako jednoduchému vytváření a úpravě základních funkcí, jako IP rozsahů, překladů IP adres, vlastně *Network Address Translation* (dále NAT), *Dynamic Host Configuration Protocol* (dále DHCP), tyto a podobné úkony lze jednoduše zvládnout pár jednoduchými úkony v konfigurační řádce, nebo v příslušném menu ve Winboxu, bez řešení a znalostí o tom, jak jsou ve směrovači pakety zpracovány.

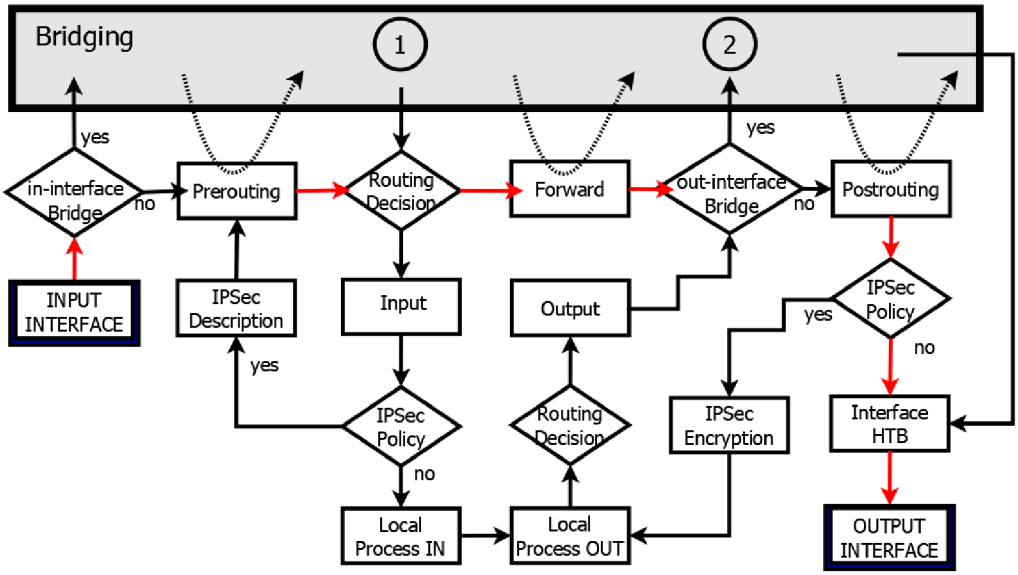
Ovšem pro náročnější konfigurace, jako vytváření směrovacích pravidel, nebo optimalizace datového toku, kde jsou nutné komplexní operace, je nutné vědět která interní operace náleží v určitém úseku práce s daty, několik úseků je znázorněno na obrázku 1.14.



Obr. 1.14: Operační schéma Packet Flow[5]

Z tohoto důvodu byla vytvořena schémata cest paketů *Packet Flow* v jednotlivých situacích. V případě této práce bylo hojně využíváno schématu směrování Ethernet-to-Ethernet, schéma s červeně vyznačenou cestou je na obrázku 1.15. Výčet schémat Packet Flow obsahuje:

- *Bridging with use IP firewall* – Přemostění s použitím IP firewallu
- *Routing – from Ethernet to Ethernet interface* – Směrování z ethernetového na ethernetové rozhraní
- *Routing form one Bridige interface to different Bridge interface* – směrování z jednoho přemostěného rozhraní na jiné přemosstěné rozhraní
- *IPsec encryption* – IPsec šifrování
- *IPsec decryption* – IPsec dešifrování



Obr. 1.15: Směrování Ethernt-to-Ethernet[5]

1.5.4 Minoritní síťové zařízení v síti ISP

Druhou nejpočetnější skupinou v síti ISP jsou síťové zařízení společnosti *Ubiquiti Networks* (dále UBNT) v zastoupení 21 %. Mikrovlnné prvky značky UBNT mají podstatně menší možnosti konfigurace, než je tomu u zařízení MikroTik. Tyto zařízení mají obdobně proprietární nadstavbu 802.11 jako má MikroTik Nv2, zde AirMAX. AirMAX monitoruje parametry spojení a podle parametrů jednotlivých klientů přiděluje časové rámce, reprezentující přidělenou povolenou dobu přenosu s přístupovým bodem. Tato metoda pomůže klientům s horším mikrovlnným spojením, naopak sníží možnosti vysílání u ostatních klientů, na které tím pádem připadá méně potenciálního vysílacího času.[3]

2 KVALITA SLUŽEB V DEFINOVANÉ SÍTI

Spolu s analýzou vstupních dat, jako je obsah sítě ISP a datový provoz, byla rozebrána teorie související s problematikou optimalizace přenosu dat.

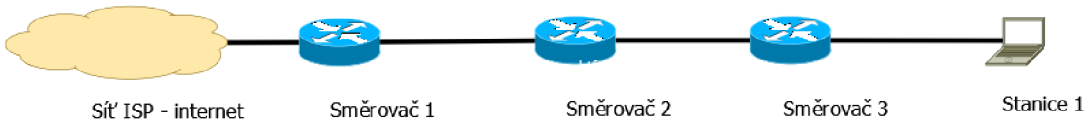
V této části práce jsou popsány testy s laboratorní sítí, ve které byly aplikovány konfigurační kroky směřující k optimalizaci dat a následně optimalizace sítě samotné. Model zvolený pro nasazení do sítě je DiffServ, využívající značení paketů a toků dle parametrů popsaných v kapitole 1.4.3, teoretické části práce. Tento model má nejlepší teoreticky předpoklady a vlastnosti pro správnou funkci v optimalizované síti ISP. Proto jsou zde použity jeho možné způsoby aplikace porovnávající výhody a možnosti konkrétních konfigurací.

2.1 Laboratorní testy

Před nasazením nové konfigurace přímo do sítě ISP bylo nutné provést několik testů a ověření funkčnosti žádané konfigurace. V případě nasazení neotestovaných a potenciálně nefunkčních pravidel a úprav tvarujících provoz přímo do sítě ISP by mohlo negativně ovlivnit fungování, v neznámém rozsahu. Vzhledem k uvedeným rizikům bylo realizováno dvouúrovňové laboratorní testování:

- Virtualizované prostředí RouterOS
- Fyzická laboratorní síť

První laboratorní testování proběhlo ve virtualizovaném prostředí programu Oracle VM Virtualbox, na který byl nainstalován operační systém RouterOS. Virtualizací bylo možné otestovat a prověřit funkce jednotlivých částí operačního systému RouterOS před realizací fyzického spojení konkrétních síťových prvků. Druhým bodem byla fyzická laboratorní síť z prvků MikroTik RB951Ui-2HnD, reprezentované `Směrovačem 2` a `Směrovačem 3` na obrázku 2.1.



Obr. 2.1: Zapojení laboratorní sítě

`Směrovač 1` zastupoval funkci výchozí brány z laboratorní sítě, zde byl nasazen prvek MikroTik RB333, který měl dostatečné parametry pro procesy testované v laboratorní síti stejně jako směrovače RB951Ui-2HnD. Konfigurace laboratorní sítě

proběhla pomocí `Stanice 1`, pomocí které byly prováděny i testy ověřující funkčnost konfigurace.

V sestavené laboratorní síti bylo testováno značení datového provozu z internetu, ale také přímo ze sítě ISP. Proběhlo ve třech variantách klasifikace výstupních dat. První test značení proběhl pomocí statických seznamů IP adres. Následující pomocí portů. Třetí varianta optimalizace fungovala na základě hlubší paketové inspekce pracující např. s video formáty *(také nazývanou jako layer 7)*. Těmito metodami bylo ověřeno fungování členění, značení a omezování provozu, bez nutnosti nasazení konfigurace na BR.

Statické IP adresy - v tomto případě byly zachytávány datové toky náležící:

- FTP server
- seznam.cz
- google.com

Pro značení portů byly použity dvě dvojice portů z rozsahu známých portů *(well known ports)* proběhlo pro služby fungující na portech:

- 80, 443 *(webové stránky)*
- 20, 21 *(FTP přenos)*

Poslední varianta založená na pravidlech pracující na 7 vrstvě ISO/OSI zachytával provoz obsahující:

- video (mp4, flv)
- hlas (sip, h323)

Těmito metodami byly vytvořené filtry, použité pro značení provozu. Celá sít ISP využívá vnitřní, respektive neveřejné IP adresy a rozsahy. Na BR dochází k překladu na veřejné IP adresy. Proto bylo nezbytné provádět značení na základě rozsahů IP adres, přímo na BR, ukázkové znázornění značení zvolených služeb je znázorněno na obrázku 2.2.

Laboratorní síť je stejně jako sít ISP za několika překlady, tudíž pro laboratorní síť nebyly relevantní veřejné IP adresy pro značení datového provozu. Proto v tomto bodě bylo provedeno DSCP přeznačení již na BR sítě ISP. U DSCP byla využita vlastnost konzistentnosti v celé DS. Tímto způsobem bylo dosaženo rozlišení datových toků, kterých bylo použito v laboratorní síti i následně při implementaci do sítě ISP.

```
/ip firewall mangle
add action=change-dscp chain=prerouting comment="zmena DSCP - Youtube" new-dscp=40 src-address-list=\
    Youtube
add action=mark-packet chain=postrouting comment="znaceni paketu - Youtube" dscp=40 new-packet-mark=\
    YoutubePacketMark
add action=change-dscp chain=prerouting comment="zmena DSCP - FTP-local" new-dscp=15 src-address-list=\
    FTPserver_local
add action=mark-packet chain=postrouting comment="znaceni paketu - FTP-local" dscp=15 new-packet-mark=\
    FTPlocalPacketMark
add action=change-dscp chain=prerouting comment="zmena DSCP - Twitch" new-dscp=42 src-address-list=\
    Twitch
add action=mark-packet chain=postrouting comment="znaceni paketu - Twitch" dscp=42 new-packet-mark=\
    TwitchPacketMark
add action=change-dscp chain=prerouting comment="zmena DSCP - SledovaniTV" new-dscp=41 \
    src-address-list=SledovaniTV
add action=mark-packet chain=postrouting comment="znaceni paketu - SledovaniTV" dscp=41 \
    new-packet-mark=SledovaniTVPacketMark
```

Obr. 2.2: Značkování provozu

Vzhledem k teoretickým podkladům popsaných v kapitole 1.4.3 a otestování v laboratorní síti byly zvoleny frontové mechanismy typu PCQ. Frontové mechanismy PCQ dosahovaly statisticky nejlepších výsledků, podle zpoždění dat a jejich ztrátovosti.

2.1.1 Rozlišení typů datových toků pomocí vytvořených záznamů IP

Aby bylo možné značení dat pomocí IP adres, které pozorované webové služby využívají, je nutné provést evidenci a přiřazení jednotlivých IP adres, či rozsahů. Tyto IP adresy byly získány 2 způsoby.

Jeden způsob získání těchto IP adres, respektive IP rozsahů, byl pomocí programu Wireshark, který zaznamenává provoz na síťových rozhraních koncových stanic. Tato metoda tvoření adresových listů pro konkrétní webové služby je poněkud pomalá a časové náročná. Navíc nezaručuje, že budou zanalyzovány všechny IP adresy, které webová služba používá.

Druhá, efektivnější metoda spočívala ve vyhledání IP adres na relevantních webových stránkách, jako jsou webové stránky poskytovatele služby, nebo webové stránky vedoucí databáze s informacemi o veřejných IP adresách, jako `db-ip.com`. Příklad vytvoření pravidla, které na základě listu IP adres přeznačí DSCP na hodnotu 49. V dalším kroku značí jednotlivé pakety s hodnotou DSCP 49 na značku IPTV_IP. Značení paketů `mark-packet` je určeno pro lokální zpracování, jako řízení odbavování ve frontách. Příklad je zobrazen kódem 2.1.

Výpis 2.1: Ukázka zdrojového kódu - značení s IP

```
chain=forward action=change-dscp new-dscp=49
passthrough=no src-address-list=IPTV log=no
log-prefix=""

chain=postrouting action=mark-packet
new-packet-mark=IPTV_IP passthrough=no
dscp=49 log=no log-prefix="
```

2.1.2 Rozlišení typů datových toků pomocí portů a podružných parametrů

Pro zachytávání provozu podle portů a následně i podružných parametrů, zajišťujících přesnější rozlišení jednotlivých typů přenášených služeb bylo nezbytné zjištění, na kterých portech operují optimalizované služby. Velká část obecných služeb operuje v rozsahu známých portů *(well know ports)* 0-1024. Příkladem mohou být v laboratorní síti nasazené - optimalizované služby přenášející webový obsah (80, 443) a FTP přenos (20, 21). Dále v rozsahu registrovaných portů, tedy 1024-49151. Registrované porty jsou přiřazeny k méně běžným službám a aplikacím. Zbylé porty v rozsahu 49152-65535 náleží do skupiny dynamických a privátně využívaných portů. Porty z posledních dvou skupin jsou různými aplikacemi často náhodně otevírány a používány pro jejich přenos.

Právě pro velkou neurčitost, jinými slovy dynamickou volbu používaných portů čím dále větším množstvím aplikací tato metoda pro značkování provozu obsahuje podružné parametry, které mají přesněji specifikovat, o jaký provoz konkrétně jde. Mezi podružné parametry byly zařazeny:

- Typ spojení *(Connection Type)*
- Rychlost spojení*(Connection Rate)*
- Velikost paketu *(Packet Size)*
- Limit spojení *(Connection Limit)*

Parametry byly nastaveny v zařízeních MikroTik při tvorbě Mangle pravidel pro zachycení provozu. Příklad zachycení provozu na základě zdrojového portu je vypsán zdrojovým kódem 2.2. Kde paketům obsahující zdrojový port 20 nebo 21 byly přeznačeny DSCP značky na hodnotu 43. Následně byly pakety obsahující DSCP značku 43 značeny jako FTP_Port, toto značení je určeno pro lokální zpracování.

Výpis 2.2: Ukázka zdrojového kódu - značení s porty

```
chain=forward action=change-dscp new-dscp=43
protocol=tcp src-port=20,21
passthrough=no log=no log-prefix=""

chain=postrouting action=mark-packet
new-packet-mark=FTP_Port passthrough=no
dscp=43 log=no log-prefix="
```

2.1.3 Rozlišení typů datových toků podle pravidel vyšších vrstev

Při tvorbě pravidel na základě vyšších vrstev dochází k hledání shodného přednastaveného schématu *(pattern)* a procházejících paketů. Speciálně u této metody je velký předpoklad vysokého využití paměti a především výpočetního výkonu směrovače.

Jednotlivá schémata pro sestavení pravidel na vyšších vrstvách (dále L7) lze nalézt v MikroTik dokumentaci, nebo pomocí filtrování provozu nástroji jako Wireshark. Použitá schémata pro klasifikaci provozu na základě L7 byly získány oběma variantami. Každý použitý filtr provozu byl zvlášť testován, aby se potvrdila jeho funkčnost. Níže je uveden příklad podmínky hledaných formátů pomocí regexp *(Regular Expressions)* se syntaxí podle standardu POSIX, až na několik vyjímek dohledatelných v dokumentaci MikroTik.

```
regexp="\"^.*get.+\\\\(mov|mpeg3|mp4|flv|avi)
```

Příklad zdrojového kódu 2.3 jako v předchozích dvou případech kdy bylo prováděno zachytávání datových spojení na základě listů IP adres, nebo portů. V prvním kroku této ukázky je na základě `regexp`, neboli pravidla L7 vyhledán datový provoz obsahující video obsah. Následně jsou zdrojové IP adresy splňující toto pravidlo dočasně uloženy a dále přeznačeny jejich hodnoty DSCP. Pro lokální prioritní zpracování a další úpravy těchto dat s odpovídající značkou DSCP jsou označeny jako video_L7.

Výpis 2.3: Ukázka zdrojového kódu - značení s L7

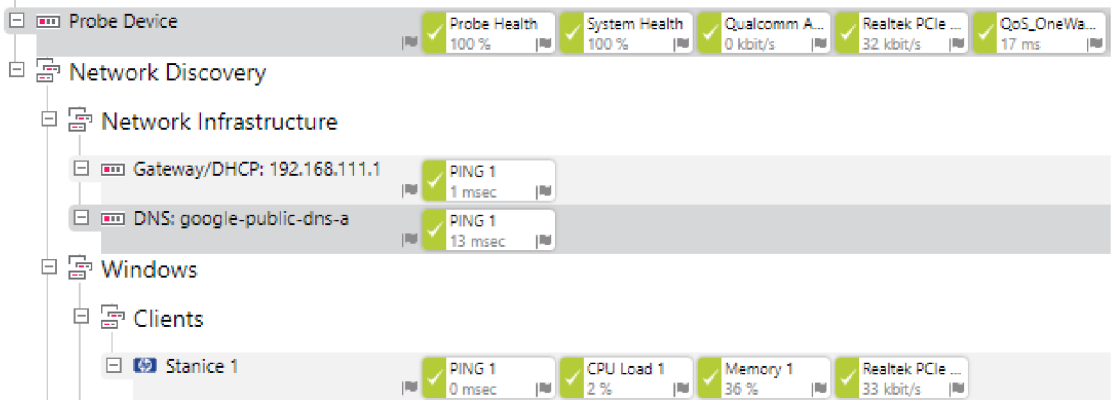
```
chain=forward action=add-dst-to-address-list
layer7-protocol=video_L7 address-list=videoList_L7
address-list-timeout=30m log=no log-prefix=""

chain=forward action=change-dscp new-dscp=45
passthrough=no src-address- list=videoList_L7
log=no log-prefix=""

chain=postrouting action=mark-packet
new-packet-mark=video_L7 passthrough=no
dscp=45 log=no log-prefix="
```

2.1.4 Monitorování a generovaná data

Zaznamenávání funkčnosti laboratorní sítě při generování datového provozu a testování funkčnosti konfigurací bylo provedeno pomocí monitorovacího nástroje PRTG tool. Na obrázku 2.3 jsou zachyceny základní senzory monitorující stav laboratorní sítě. Tento software, monitorující parametry jako je zatížení procesoru, datový tok na jednotlivých síťových rozhraních, odezvu, případně ztrátovost dat, byl využit i u monitorování sítě ISP.



Obr. 2.3: Senzory PRTG tool pro laboratorní síť

Datové toky byly generovány z globální sítě Internet, ale i sítě ISP, kde byla k těmto účelům vytvořena služba FTP serveru na virtualizovaném serveru Windows 2012. Všechny toky, které byly využity pro generování dostatečně objemného provozu, zatěžující linku do meze rozpadu spojení, jsou:

- Internetová televize - IPTV *(zdroj v Internetu)*
  - odpovídající 16,7 % datového provozu

- Video na vyžádání (VoD) - YouTube.com *(zdroj v Internetu)*
  - odpovídající 12,7 % datového provozu

- Streamovací server - Twitch.tv *(zdroj v Internetu)*
  - odpovídající 47,3 % datového provozu

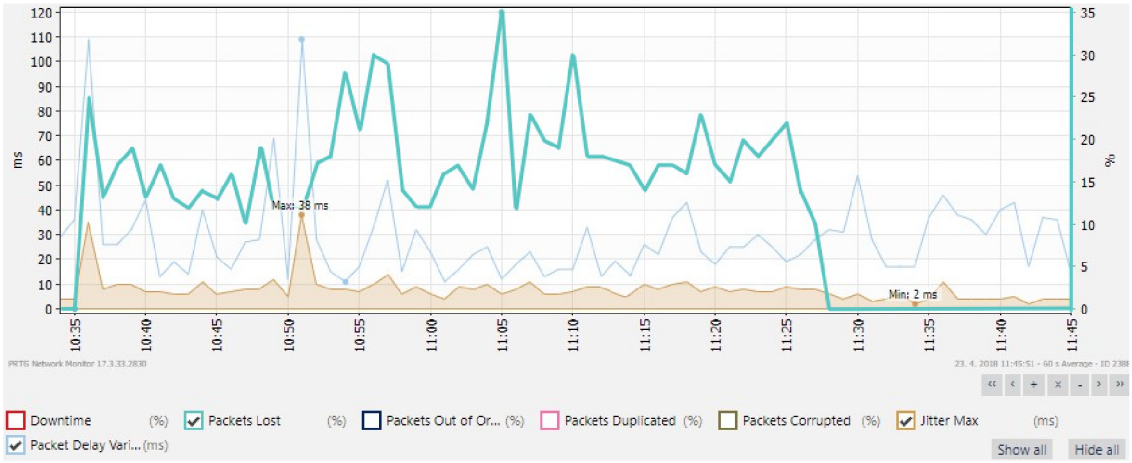
- FTP server *(zdroj v síti ISP)*
  - odpovídající 23,3 % datového provozu

Tab. 2.1: Celkový generovaný datový provoz

Typ datového provozu	Název služby	Přenášené rozlišení	Přenesená data za 10 minut/ za vteřinu	Zatížení [%]
IPTV	Kuki IPTV	1080p50FPS	435,5 MB/5,81 Mbps	16,7
VoD	YouTube	1080p60FPS	329,8 MB/4,40 Mbps	12,7
Stream	Twitch.tv	1080p60FPS	606,7MB /8,09 Mbps	23,3
FTP	FTP přenos	NA	1230,8 MB/16,41 Mbps	47,3

2.2 Testování v reálném prostředí

Po úspěšném ověření očekávaných funkcí v laboratorní síti bylo přistoupeno k širším implementacím konfigurací do sítě ISP. Testované implementace potvrdily své funkce na větším vzorku klientů ISP. Dále se projevilo chování, respektive vliv zatížení síťových prvků při větším objemu značeného datového provozu a frontování dat.

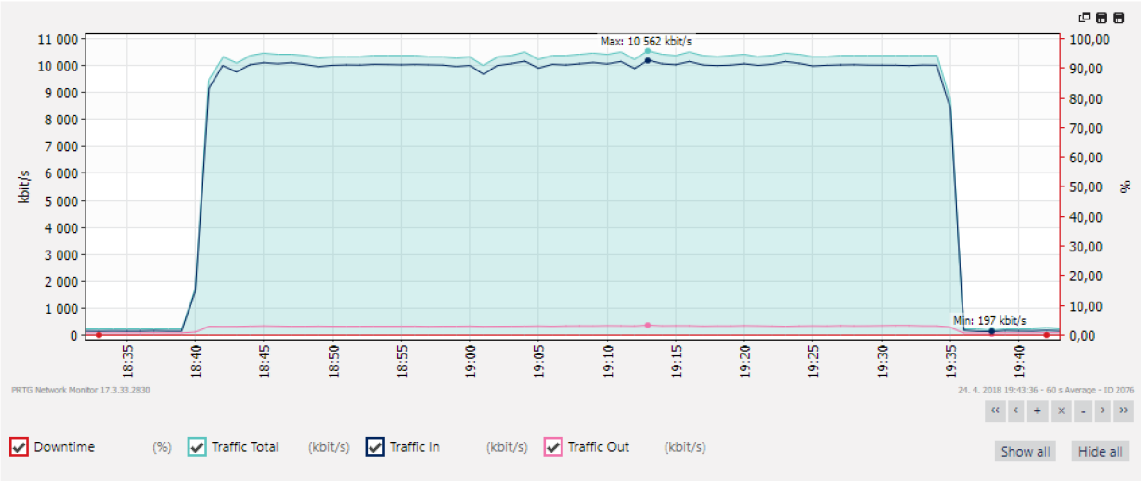


Obr. 2.4: Ztrátovost na testované lince před optimalizací

Před vložením samotných úprav do konfigurace směrovačů v síti ISP byly zaznamenány klíčové parametry sítě při zatížení spoje do míry rozpadů spojení IPTV a streamovaných přenosů, respektive služeb vyžadujících nízkou odezvu. Při tomto testu byl kladen největší důraz na co nejpřesnější zaznamenání ztrátovosti datového toku. Parametr ztrátovosti byl zobrazen na grafu 2.4. Parametry korelují s mírou zatížení přenosové linky, zobrazené v grafu 2.5. Jednotlivé, výše zmíněné grafy jsou ze dvou různých měření, ovšem přesně reflektují dění na datovém spojení. Spojení bylo omezeno nesymetricky na rychlost 10 Mbps pro rychlost stahování dat, neboli *downlink* a 1 Mbps rychlost nahrávání dat, *uplink*.

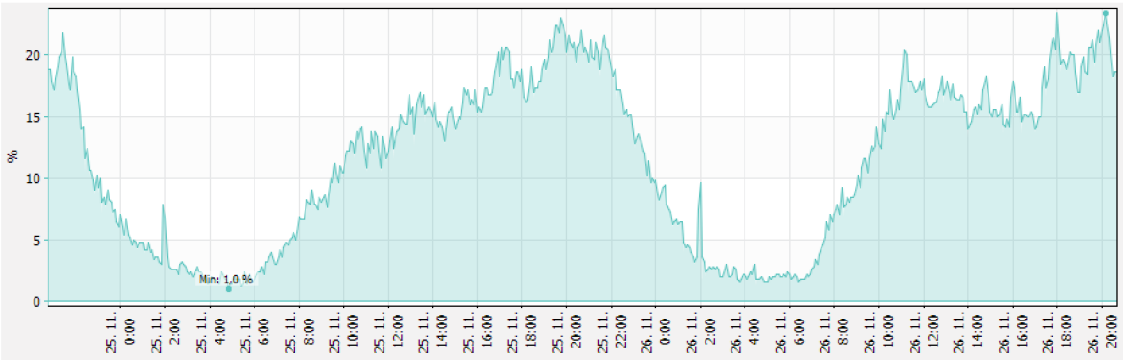
Při snímání těchto parametrů bylo periodicky, každých 60 s zasíláno 1000 UDP datagramů o velikosti 172 B. Mezi jednotlivými pakety byl zvolen 20 ms rozestup. Pro zachycení i velmi přetíženého datového spoje měl každý z těchto paketů zvolený čas expirace 60 s. Tato konfigurace monitorovacího programu vytvářela nejlépe zpracované grafy, odpovídající reálnému dění při srovnání s pozorováním datových přenosů a úzkého hrdla - sekání a rozpady časově citlivých spojení. Proto byla ponechána i na všechny následující měření v síti.

Takto monitorovaná linka dosahovala špičkové ztrátovosti až 35 %. Při nízkém zatížení, respektive bez faktorů limitujících přenosovou linku ztrátovosti 0 %. Podstatným parametrem je zatížení výpočetních jednotek na hlavních směrovačích, zobrazené na obrázku 2.6. Zatížení výpočetních jednotek je přímo úměrné s množstvím



Obr. 2.5: Datový provoz na testované lince před optimalizací

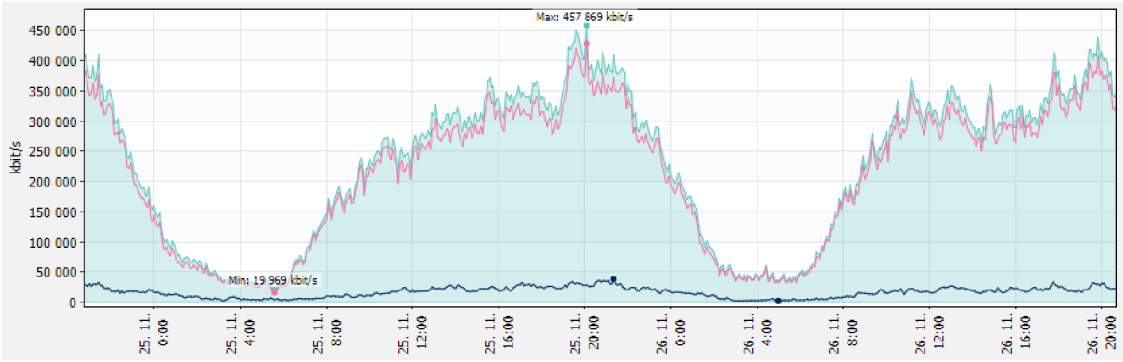
přenesených dat, na obrázku 2.7.



Obr. 2.6: Zatížení procesoru na páteřním směrovači před optimalizací

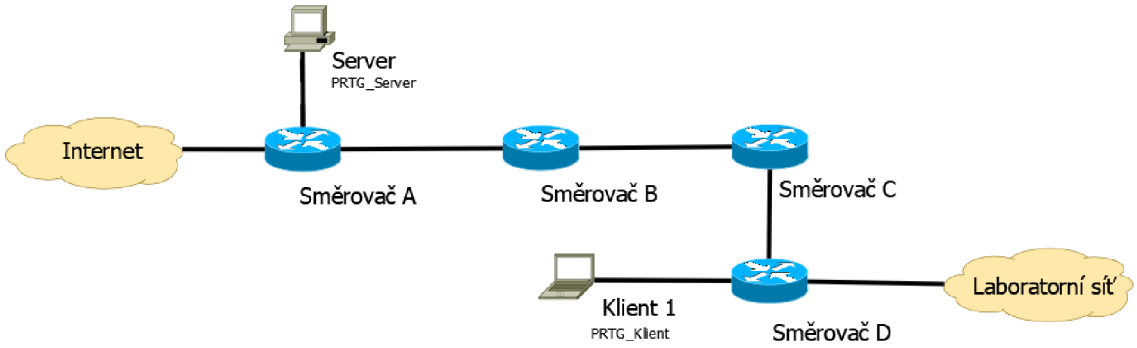
Záznam linky odpovídající 70 minutám, u obrázku 2.4 a 2.5, byly záměrně zvoleny v kratším časovém úseku, aby se zabránilo průměrování zaznamenaných dat. Datový provoz a zatížení procesorů na páteřním směrovači, zobrazené v 2 denním záznamu, na obrázcích 2.6 a 2.7 je nutné brát s přihlédnutím na nezbytné průměrování snímaných hodnot v čase, mohlo tak dojít k nepatrnému zkreslení charakteristiky. Cenou tohoto zkreslení je záznam, na kterém lze dobře identifikovat periodicky se opakující dobu s vyšším vytížením sítě.

Implementace, testující značení a frontování při větším vzorku klientů a větším množství zpracovaných dat, zprvu neobsahovala žádné limitující faktory jako kapacita front. Přiřazovala zvolené hodnoty DSCP specifikovaným datovým tokům, které se vážou k poskytovateli určité služby na internetu. Značení DSCP bylo na BR ISP nasazeno již u laboratorní sítě, kde bylo pro menší datové toky úspěšně ověřeno zaznamenávání a značení dat služeb. Implementovány tak byly značkovací a fron-



Obr. 2.7: Datový provoz na páteřním směrovači před optimalizací

tovací mechanismy podél testované trasy, která je znázorněna na obrázku 2.8. Zde je naznačeno i zasazení laboratorní sítě v rámci celé sítě ISP. Na obrázku jsou také server s klientem monitorovacího programu PRTG tool, zaznamenávající chování v síti během testování změn v konfiguraci jednotlivých směrovačů.

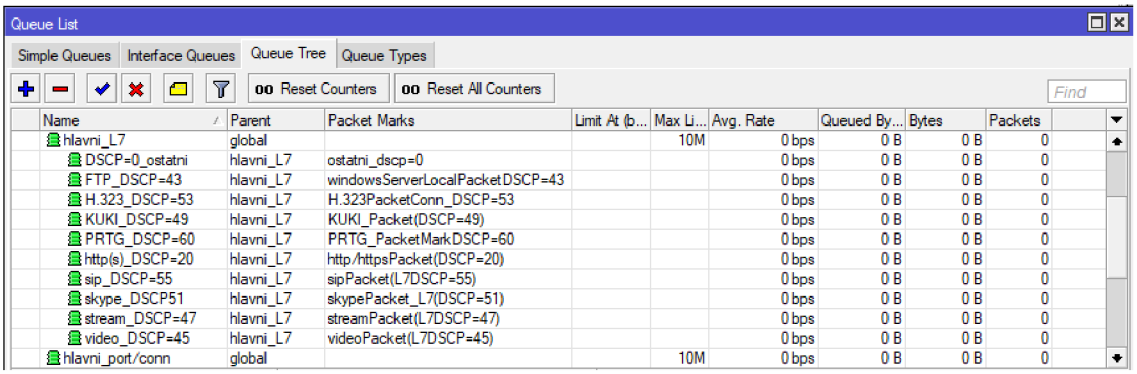


Obr. 2.8: Monitorovaná část sítě ISP

Nakonfigurované fronty, kterými prochází přeznačený datový provoz jsou znázorněny na obrázku 2.9. Fronty je možné hierarchicky členit stromovou strukturou, toho bylo využito i u této implementace, kde je zaštiťující fronta s názvem `hlavni` provázána se síťovým rozhraním `ether1`, které je v roli vstupního rozhraní. Pod toto síťové rozhraní pak náleží následující fronty jednotlivých služeb. Celou strukturu lze specifikovat minimální i maximální propustností pro jednotlivé fronty, také velikosti zásobníků a priority fronty.

2.2.1 Metody optimalizace a jejich nasazení

Dosavadní vložené úpravy do konfigurace v síti laboratorní, ale i na BR prováděly pouze rozlišení několika testovacích datových zdrojů popsaných v kapitole 2.1, je-



Obr. 2.9: Použité fronty v síti ISP

jich značení pomocí DSCP a odchytávání na CPE*(Customer-provided equipment)*, neboli směrovači ISP umístěného u zákazníka. Vytvořené fronty, přes které procházely rozlišné datové toky s rozlišnými značkami DSCP fungovaly pouze pro ověření správného zaznamenání značených dat v jiné části sítě. Kompletní testy provádějící upřednostnění konkrétních služeb byly popsány v této kapitole.

Zvolené metody byly zaměřené na prověření přenosových parametrů, kdy stěžejní proměnnou, mimo standardní QoS parametry, byla velikost zatížení výpočetního výkonu (CPU) páteřních a hraničních směrovačů. Tento parametr značně ovlivňuje možné množství firewallových pravidel i filtrů pro rozlišení jednotlivých typů datových přenosů. Vzhledem k tomu byla volena optimalizace rozlišená do níže vypsaných kategorií.

Metody podle místa nasazení:

- hraniční směrovač (BR) - *centralizovaně*
- směrovač ISP u klienta (CPE) - *decentralizovaně*

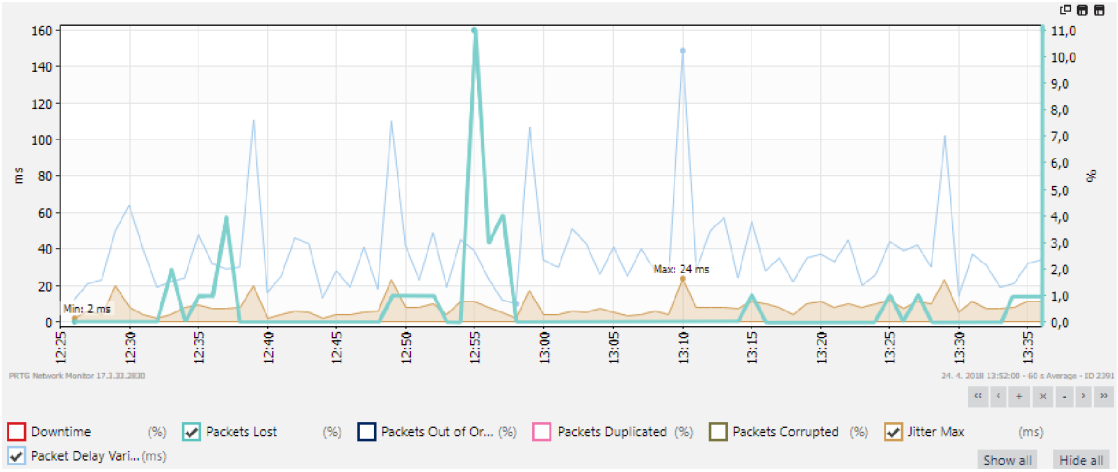
Metody podle způsobu členění datových toků:

- Statické záznamy IP adres
- Porty a podružné parametry
- Pravidla vyšších vrstev - *regexp/content*

Značení datových toků podle statických IP záznamů

První testovanou metodou reálně omezující a tvarující datový provoz proběhla na základě uložených IP záznamů, jejichž získání bylo popsáno v kapitole 2.1.1. Klasifikace byla provedena na hraničním směrovači, kde byl datový provoz přeznačen odpovídajícími hodnotami v poli DSCP. Přiřazené hodnoty pro konkrétní optimalizované služby jsou v tabulce 2.3. Kde jsou mimo zvolené DSCP hodnoty zobrazeny i následně použité priority zpracování provozu. Princip třídění datového provozu spočíval ve staticky uložených IP záznamech.

Po otestování roztřídění provozu na BR bylo řešeno třídění decentralizovaně na CPE, kde bylo očekáváno rozptýlení nezbytného výpočetního výkonu z hraničního směrovače. Mimo rozlišné zatížení výpočetních jednotek mezi BR a CPE bylo dosaženo totožných optimalizačních výsledků vynesených v grafu 2.10. Zde je pozorovatelné zlepšení parametrů, mimo jednu špičkovou ztrátovost přenášených dat. Souhrn klíčových parametrů je obsažen v tabulce 2.2. Po analýze vzniklé situace bylo stanoveno, že krátkodobě zvýšená ztrátovost, dosahující 11 % byla zapříčiněna nevykrytím všech nezbytných IP adres, které komunikovaly se zařízením realizujícím sledovaný datový přenos. Dostatečně obsáhlé záznamy IP adres jsou úskalím této metody.



Obr. 2.10: Vliv optimalizace pomocí staticky přiřazených IP

Metoda založená na staticky vedených záznamech IP adres nese výhody jednoduché datové inspekce a s tím související nepříliš velkou náročnost na výpočetní výkon na síťovém prvku provádějící třídění datových toků. Velkou nevýhodou této metody bránící širšímu nasazení spočívá v pracnosti vytvoření odpovídajících IP záznamů. IP adresy jednotlivých služeb se navíc mohou dynamicky měnit. Proto je tato metoda vhodná především pro jednodušší optimalizaci, jako může být omezení datového přenosu pro služby poskytované přímo od ISP, nebo IPTV přenášené ze

Tab. 2.2: Klíčové parametry zachycené při testování QoS - podle IP

Typ klasifikace	Packets Lost [%]	Jitter [ms]	Delay Variation [ms]
	min/prům/max	min/prům/max	min/prům/max
IP - centrálně	0/1/12	3/10/26	15/37/145
IP - necentrálně	0/1/11	2/11/24	17/40/150

známých, pevně stanovených IP adres partnerské služby. V opačném případě může dojít k situaci zobrazené v grafu 2.10, nekontrolovaným negativním kolísáním ztrátovosti díky nedostatečné databázi statických adres.

Tab. 2.3: Přiřazené hodnoty DSCP a priority odbavování přenášených dat v síti ISP

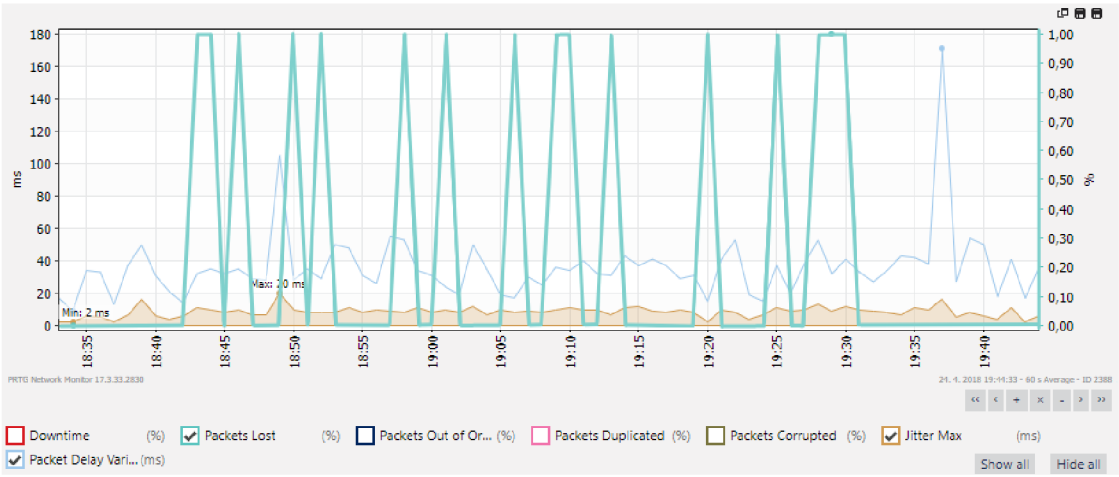
Typ datového provozu	DSCP hodnota	Priorita zpracování
SIP	55	1
H323	53	2
Skype	51	3
IPTV	49	4
Stream	47	5
VoD	45	6
Ostatní	0	7
FTP	43	8

Značení datových toků podle portů a podružných parametrů

Tato sada testování byla založena na tvarování provozu pomocí zdrojových portů a podružných parametrů. Rozdělení rozsahů portů a jednotlivé podružné parametry upřesňující typ a náročnost jednotlivých datových toků byly popsány v kapitole 2.1.2. Kde došlo k přiřazení konkrétních aplikací a služeb k jimi využívaným portům a pozorováním chování těchto datových toků byly určeny podružné parametry.

Stejně jako při optimalizaci na základě statických seznamů IP adres, i zde bylo testování provedeno při koncentraci pravidel na BR a následně na CPE. Pozorované datové spojení dosahovalo lepších vlastností, znázorněných na grafu 2.11. Linka nabývala maximální datové ztrátovosti 1 %, ovšem v průměru méně než 1 %, jak je vyobrazeno v tabulce 2.4.

Při použití této metody docházelo k vyššímu zatížení výpočetní jednotky, než u předešlé metody založené na statických záznamech adres. Nejvyšší rozdíl nabýval



Obr. 2.11: Vliv optimalizace pomocí portů a podružných parametrů

10 % při maximálním datovém toku na BR. Obdobný trend byl pozorován i na CPE, ovšem opět s lepšími výsledky ztrátovosti, vůči pouhým statickým IP seznamům. Souhrn pozorovaných parametrů je znázorněn v tabulce 2.4.

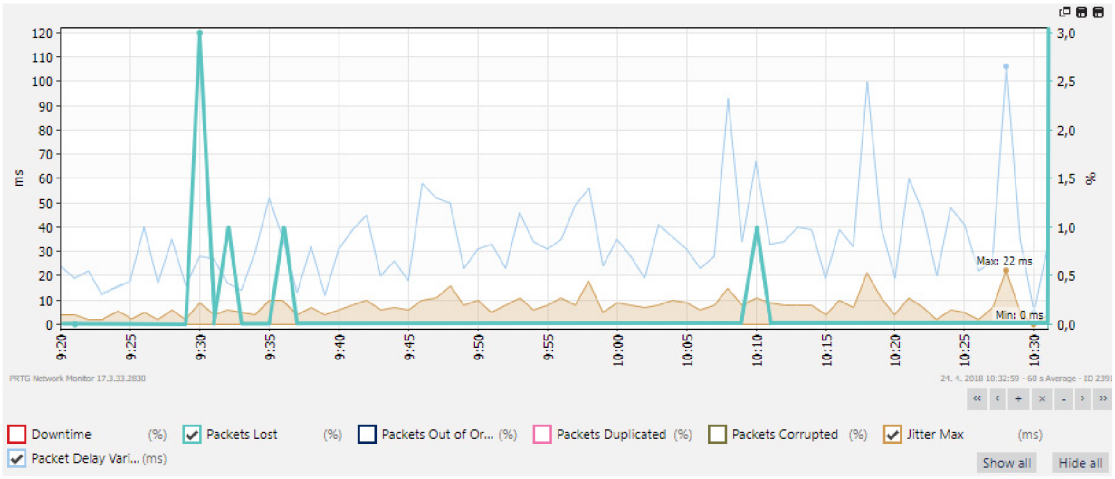
Tab. 2.4: Klíčové parametry zachycené při testování QoS - podle Portů

Typ klasifikace	Packets Lost [%]	Jitter [ms]	Delay Variation [ms]
	min/prům/max	min/prům/max	min/prům/max
Port - centrálně	0/<1/2	5/8/19	18/23/105
Port - necentrálně	0/<1/1	3/9/20	16/25/105

Značení datových toků podle vyšších vrstev (L7)

Testování, u kterého byly hledány regulární výrazy *(regexp)*, nebo specifické textové obsahy paketu *(content)*. Metoda byla obecně popsána v kapitole 2.1.3. Jde o nejjemnější prohledávání přenášených dat, ovšem tato hloubková inspekce dat *(deep packet inspection)* vyžaduje vysoký výpočetní výkon. Při nasazení 2 pravidel L7 procházející veškerý vstupní provoz na BR došlo k znatelnému navýšení využití výpočetní jednotky, odpovídající až 10 %, což je při použití pouhých 2 filtrů pro značení provozu velké zatížení. Při aplikaci všech filtrů třídících vstupní datový provoz vypsaných v tabulce 2.3 vzrostlo zatížení výpočetní jednotky při nejvyšším datovém provozu na 64 %. Mimo vysoké nároky na síťový prvek provádějící filtraci pomocí L7 dosahuje tato metoda nejlepších výsledků, vynesených v grafu 2.12.

Graf zobrazuje test provedený při aplikaci L7 filtračních pravidel na CPE, ovšem jeho výsledky jsou identické s chováním datové linky při testování s centralizovanými



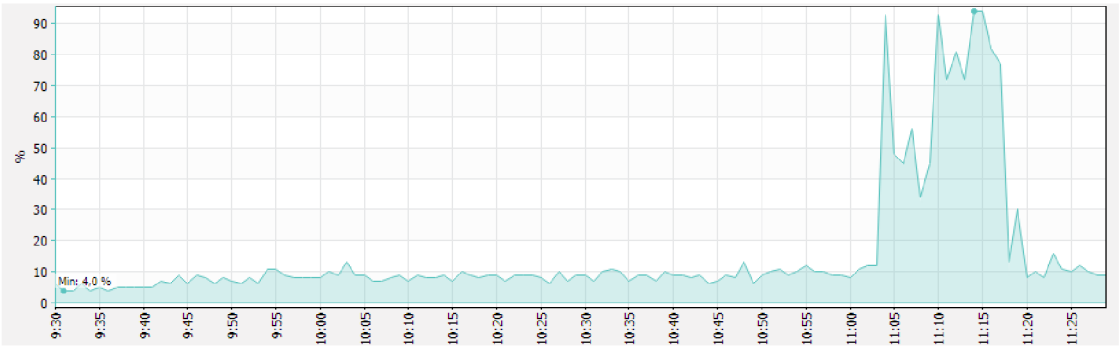
Obr. 2.12: Vliv optimalizace pomocí vyšších vrstev

pravidly na BR, proto byl vynesen pouze jeden graf. Nepatrné rozdíly mezi oběma testy jsou stejně jako u předchozích metod uvedeny v tabulce 2.5. I z tabulky vyplývá že oba testy mají téměř identické výsledky.

Tab. 2.5: Klíčové parametry zachycené při testování QoS - podle L7

Typ klasifikace	Packets Lost [%]	Jitter [ms]	Delay Variation [ms]
	min/prům/max	min/prům/max	min/prům/max
L7 - centrálně	0/1/2	3/10/19	10/35/105
L7 - necentrálně	0/1/3	4/9/18	12/32/107

Bylo otestováno nasazení většího množství `mangle`- značkovacích pravidel operujících s L7, nad rámec aplikací a služeb vypsaných v tabulce 2.3. Zahrnující vyhledávání klient-klient (peer-to-peer) přenosů, konkrétně torrentů. Cílem rozšíření bylo omezit přenosy tohoto charakteru a přenášet je pouze na "pozadí"v nevyužitém přenosovém pásmu. Zde bylo dosaženo limitů výpočetních zdrojů BR. Rapidní nárůst zatížení procesoru je znázorněno v grafu 2.13. Rozšiřující test nesl jasné znamení, vypovídající o nebezpečně vysoké spotřeby výpočetních zdrojů a případnému zahlcení síťového prvku, které by mělo v případě sítě typu stub fatální následky na síťový provoz. Během tohoto krátkodobého spotřebování veškerých výpočetních zdrojů se v celé síti zhoršila odezva až o 400 ms.



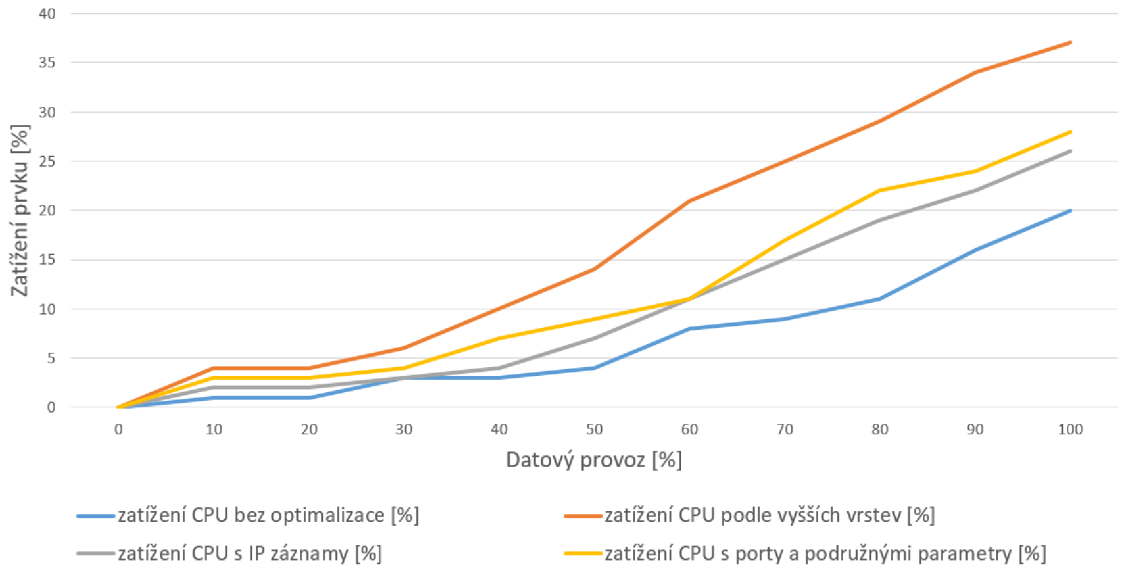
Obr. 2.13: Špičkové vytížení výpočetní jednotky BR

Během optimalizačních testů založených na značení datových toků podle seznamů IP adres, portů s podružnými parametry a vyšších vrstev byl monitorován stav velikosti parametru jitter. Parametr byl v optimalizačních metodách všeobecně zlepšen. V neoptimalizované síti docházelo k nárazovému kolísání odezvy až 40 ms. U optimalizovaných metod došlo ke snížení nárazového kolísání o téměř polovinu, v nejhorším případě na 24 ms.

Dále byly pozorovány maximální hodnoty Packet Delay Variation (PDV), uvádějící dobu [ms] od doručení předchozího rámce. Všechny optimalizační metody nabývaly maximální hodnoty PDV = 110 ms, mimo optimalizace založené na statických seznamech IP adres, zde hodnoty dosahovaly až 150 ms. Tato veličina nedosáhla žádného výrazného zlepšení, to vzhledem k vlivům rádiového prostředí a výrazným paketových shlukům při datovém přenosu.

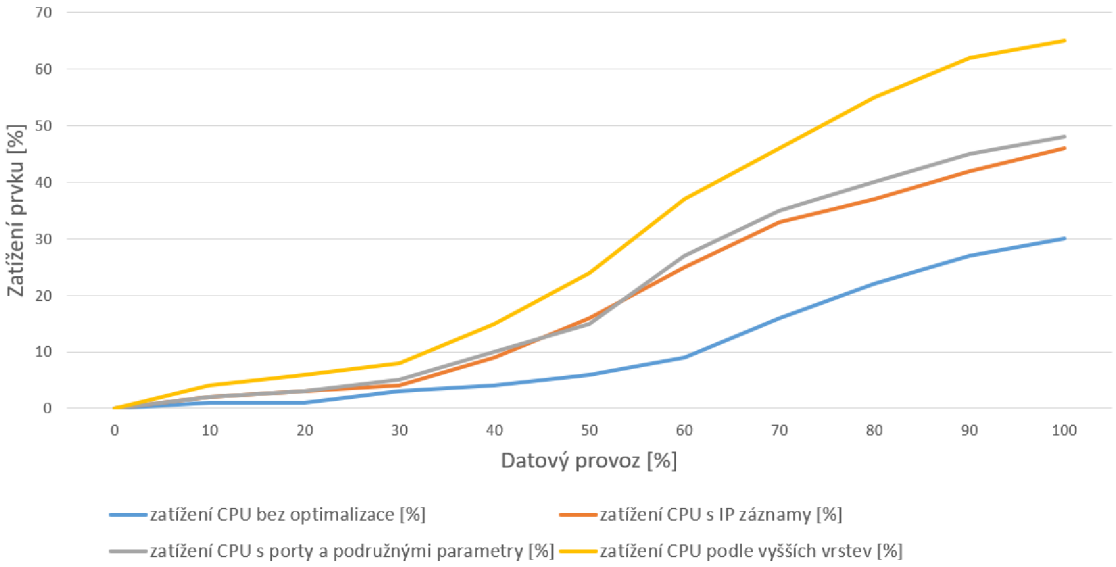
Zatížení výpočetních jednotek(CPU)

Každá ze tří nasazených metod vykazovala odlišné zatížení výpočetní jednotky. Shrnutí charakteristik pro všechny tři metody i zatížení před zásahem do konfigurace jsou shrnuty v grafu 2.14 pro zatížení výpočetní jednotky při koncentraci optimalizačních pravidel na BR. Graf 2.15 vypovídá o zatížení výpočetní jednotky při koncentraci optimalizačních technik na CPE. Grafy znázorňují velikost `zatížení prvku`, reprezentovaným zatížením výpočetní jednotky v závislosti na `datový provoz`, značící velikost procházejícího datového provozu přes síťový prvek.



Obr. 2.14: CPU v závislosti na velikosti datového provozu na BR

Grafy 2.14, 2.15 jasně potvrzují, že nejnáročnější metoda je metoda operující na vyšších vrstvách. V případě koncentrace filtračních mangle pravidel na BR i rozprostření na CPE. V síti plní roli CPE hned několik druhů a verzí síťových zařízení. Některé tak nemusí dostačovat požadavkům vyšších datových toků při aplikací QoS, vzhledem k jejich výpočetním jednotkám. Při centralizaci pravidel na BR dochází k výraznému zatížení výpočetní jednotky, ovšem do nižší míry, než v případě rozprostření pravidel na jednotlivá CPE. Proto byla vyhodnocena jako lepší varianta koncentrace těchto optimalizačních metodik na BR. Co se týče jednotlivých testovaných optimalizačních metodik, nejlepších výsledků dosáhla metoda vyšších vrstev. Metoda založená na databázích IP adres a metodě založené na portech a podružných parametrech dosahovaly obdobných výsledků, ale s nižším zatížením výpočetních jednotek. Ideální variantou mezi těmito metodami je kombinace všech tří metod. Příkladem může být zvolení statických záznamů IP adres u služeb poskytovaných přímo ISP, či jeho partnerů, jako VoIP a IPTV. Volba portů s podružnými parametry může plnit funkci například u služeb fungujících v rozsahu známých portů, které



Obr. 2.15: CPU v závislosti na velikosti datového provozu na CPE

jsou trvale přiděleny určitým aplikacím. Metodiku značení datových toků podle vyšších vrstev lze použít pro filtraci zbylého multimediálního přenosu z internetu, jako jsou video streamy, či videa na vyžádání.

3 ZÁVĚR

V bakalářské práci byly popsány nezbytné teoretické celky o datové komunikaci, základních parametrech ovlivňujících datový přenos v rádiových systémech, jako předstupeň následně popsaných globálně využívaných optimalizačních technik (QoS) - diferencovaných a integrovaných služeb. Bez dodržení parametrů ovlivňujících datový přenos v rádiovém prostředí by následná optimalizace pomocí technik QoS byla nedostatečná. Průběžná analýza sítě poskytovatele internetu (ISP) formovala dále popisovanou teorii, související s konkrétními síťovými zařízeními a jejich možnostmi. Díky znalosti majoritní platformy v síti, náležící 71 % výrobci MikroTik byly popsány konkrétní možnosti a kompatibilita s ostatními síťovými prvky.

Síť v předešlém konfiguračním provedení fungovala jako Best-Effort, nepodnikající žádné aktivní kroky k optimalizaci datového provozu. Vzhledem k topologii sítě ISP a teoreticky popsaným vlastnostem byla zvolena metoda diferencovaných služeb. Optimalizační metoda integrovaných služeb se hodí spíše do telefonních sítí, charakteristické rezervování zdrojů nemá příliš efektivní využití v síti triple-play.

Po volbě optimalizačního modelu byla vytvořena laboratorní síť ověřující teoreticky popsané skutečnosti. První test proběhl ve virtualizovaném prostředí s operačním systémem RouterOS. Následně vytvořená laboratorní fyzická síť z prvků MikroTik byla použita k hledání nejoptimálnější variace testovaných metod. Zvolené optimalizační konfigurace byly postupně vloženy na hraniční směrovač a zařízení na straně klienta (CPE), kde byly již za nepřetržitého provozu testovány na větším datovém toku. Před upravením konfigurace přímo v síti ISP byla pro srovnání zaznamenána kvalita přenosu dat v sítí.

Poté byly provedeny tři rozlišné optimalizační testy (založené na IP adresách, portech s podružnými parametry a pravidlech vyšších vrstev). Realizace jednotlivých konfigurací byly vždy provedeny variantou na hraničním směrovači s centralizováním veškeré klasifikace datového toku a druhou variantou s rozprostřením klasifikačních pravidel na jednotlivých CPE. Provedení s rozprostřením pravidel a jejich koncentrací mělo za cíl zjištění velikosti zatížení výpočetních jednotek a velikost optimalizace.

Nedostatečných optimalizačních výsledků bylo dosaženo při použití optimalizace založené na záznamech IP adres. Tato metoda byla velmi neefektivní. Vyžadovala náročné prvotní filtrování provozu a zjišťování, do které kategorie datových služeb náleží konkrétní IP adresy. Docházelo tak k neklasifikovaným datovým přenosům, které zhoršovali funkci celého modelu. Metoda byla však nejméně náročná na zatížení výpočetních jednotek. Její využití lze shledat ve službách poskytovaných organizující spravující datovou infrastrukturu, či jejich partnerů, jako může být IPTV a VoIP.

Lepších výsledků dosáhla metoda založená na klasifikaci podle portů a para-

metrech jako jsou typ spojení a datový tok. Jednodušeji konfigurovatelná a efektivnější metoda. Tato optimalizační metoda žádá vyšší zdroje výpočetní jednotky, než metoda předchozí, ale kombinací služeb v rozmezí známých portů spolu s definicí podružných parametrů lze efektivně optimalizovat datový provoz. Úskalím této metody je fakt, že velké množství aplikací používá náhodně otevírané porty.

Poslední metoda, rozlišující typ datového provozu podle vyšších vrstev dosáhla nejlepších optimalizačních výsledků. Metoda hledající nakonfigurované schéma, kterým může být například specifická posloupnost znaků v procházejícím datovém toku, je vysoce náročná na výpočetní jednotku. Kladné využití této vysoce efektivní metody závisí na výkonu síťového zařízení, určujícího možné množství filtračních pravidel. Tato optimalizační metoda byla zvolena jako nejvhodnější ze všech testovaných.

Při porovnání těchto metod a výběru nejlepší varianty pro optimalizovanou síť je nejvhodnějším řešením kombinace všech tří metod. Nasazení při vhodné kombinaci optimalizačních pravidel bylo zvoleno na hraniční směrovač, tedy centrálně. Vyvaruje se tak ojedinělým, ale možným potížím s nedostatkem výpočetního výkonu na CPE. Hraniční směrovač má navíc dostatek výpočetních zdrojů pro vhodně kombinované řešení optimalizačních metod.

LITERATURA

[1] *IEEE* [online]. IEEE [cit. 2017-09-07]. Dostupné z: ieee.org

[2] *Český telekomunikační úřad* [online]. Český telekomunikační úřad [cit. 2017-09-07]. Dostupné z: ctu.cz

[3] *UBNT Support* [online]. Ubiquiti Networks [cit. 2017-09-07]. Dostupné z: https://help.ubnt.com/hc/en-us

[4] *Cisco support* [online]. Cisco Systems [cit. 2017-09-07]. Dostupné z: cisco.com/c/en/us/support

[5] *MikroTik Wiki* [online]. MikroTik [cit. 2017-09-05]. Dostupné z: wiki.mikrotik.com

[6] *Microsoft TechNet* [online]. Microsoft [cit. 2017-11-24]. Dostupné z: technet.microsoft.com

[7] *THE ELECTRICAL ENGINEERING HANDBOOK*. 2. 84 Theobald's Road, London WC1X 8RR, Velká Británie: Elservier, 2005. ISBN 0-12-170960-4.

[8] *Utility-based resource and QoS optimization in packet networks: link and network level ptimization*. 1. Saarbrücken, Německo: VDM Verlag Dr. Mueller E.K., 2008. ISBN 978-3-639-04446-1.

[9] *Internet QoS: Architectures and Mechanisms for Quality of Services*. 1. Spojené státy americké: Morgan Kaufmann publishers, 2001. ISBN 1-55860-608-4.

[10] *Exam Cram: CompTIA Network+*. 3. Pearson IT Certification, 2009. ISBN 978-0-7897-3796-0.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

BE	Best-Effort
BFIFO	Packets First-In, First Out
BR	Border Rrouter
CS	Class Selector
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CoS	Class of Service
CPE	Customer-provided equipment
DHCP	Dynamic Host Configuration Protocol
DS	DiffServ Domain
DSCP	Differentiated Services Code Point
DiffServ	Differentited Services
EF	Expedited Forwarding
FIFO	First In, First Out
IETF	Internet Engineering Task Force
IP	Internet Protokol
IPP	IP Precedence
IPsec	IP security
IPv4	Internet Protokol verze 4
IPTV	Internet Protokol television
ISO/OSI	International Standards Organization/Open System Interconnection
ISP	Poskytovatel internetového připojení
IntServ	Integrated Services
L7	Layer 7
MAC	Media Access Control
MQ PFIFO	Multiple Queues Packets First-In, First Out
NA	Not applicable
NAT	Network Address Translation
Nv2	Nstreme version 2
OS	Operating System
PCQ	Per Connection Queue
PDV	Packet Delay Variation
PFIFO	Byte First-In, First Out
PHB	Per-Hop Behaviors
PRTG	Paessler Router traffic Grapher
QoS	Quality of Service
RED	Random Early Detection
RFC	A Request for Comments

RSVP	Resource ReSerVation Protocol
RTI	Real Time Intolerant
RTT	Real Time Tolerant
SFQ	Stochastic Fairness Queueing
SLA	Service-Level Agreement
TCP/IP	Komunikační model Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
ToS	Type of Service
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protokol
VPN	Virtual Private Network
WRED	Weighted Random Early Detection

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- Elektronická verze bakalářské práce