VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

IMPLEMENTACE TRIPLE-PLAY SLUŽEB V HETEROGENNÍ SÍTI

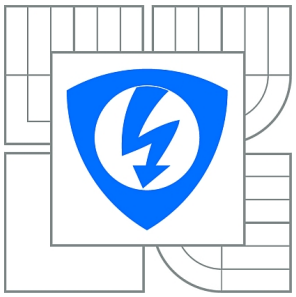
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. LUKÁŠ OBRŠLÍK
AUTHOR

BRNO 2014

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

IMPLEMENTACE TRIPLE-PLAY SLUŽEB V HETEROGENNÍ SÍTI

IMPLEMENTATION OF TRIPLE-PLAY IN HETEROGENEOUS NETWORK

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

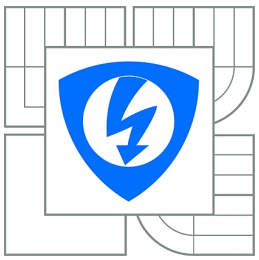
AUTOR PRÁCE — Bc. LUKÁŠ OBRŠLÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. RADKO KRKOŠ

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Lukáš Obršlík	***ID:***	130714
Ročník:	2	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Implementace triple-play služeb v heterogenní síti

POKYNY PRO VYPRACOVÁNÍ:

Popište problematiku heterogenních transportních a přístupových sítí a problematiku zabezpečení kvality služby pro přenos multimediálních toků a služeb pracujících v reálném čase po paketově komutovaných sítích. Analyzujte unicast vs. multicast transport pro přenos televizního vysílání, zejména dimenzování kapacity a škálování výkonu zařízení síťové infrastruktury. Popište problematiku poskytování triple-play služeb, vliv rezervace pásma a služeb s vysoce variabilním bitovým tokem na jiné toky v síti. Zrealizujte měření vytížení síťových prostředků a změnu parametrů kvality služeb v závislosti na počtu a bitovém toku provozovaných služeb a výsledky diskutujte. Navrhněte a implementujte plán zavedení podpory triple-play služeb do existující heterogenní datové sítě a popište jednotlivé etapy.

DOPORUČENÁ LITERATURA:

[1] HENS, Francisco J a Jose

Termín zadání:	10.2.2014	***Termín odevzdání:***	28.5.2014

Vedoucí práce: Ing. Radko Krkoš
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Diplomová práce se zabývá problematikou implementace triple-play slu- žeb a zabezpečení kvality služby v heterogenních komunikačních sítích. Vypracování je zaměřeno na ověření teoreticky nastudované problematiky na reálné situaci a existující síťové infrastruktuře. Součástí vypracování je tvorba technického řešení, které zajišťuje automatickou prioritizaci služeb na základě identifikace a rozdělení požadovaných služeb v síťovém provozu. Vytvořené technické řešení pro zajištění kvality služby bylo navrženo tak, aby bylo řešení možné v síti implementovat, do budoucna přizpůsobovat aktuálním požadavkům a zajistit tak škálovatelnost.

KLÍČOVÁ SLOVA

Triple-play, Kvalita služeb, Ethernet, Wi-fi, Unicast, Multicast, IPTV, VoIP, Perl, ISPadmin, RouterOS.

ABSTRACT

This master thesis deals with implementing triple-play services and providing it's quality of services in heterogenous comunnication networks. The aim of thesis is to apply theoretical methods in real case and existing network infrastructure. Practical part aims to create technical solution to prioritize network traffic based on classification of required services. The technical solution is created with conditions of being possible to add more functions and to provide scalability.

KEYWORDS

Triple-play, Quality of Service, Ethernet, Wi-fi, Unicast, Multicast, IPTV, VoIP, Perl, ISPadmin, RouterOS.

OBRŠLÍK, Lukáš *Implementace triple-play služeb v heterogenní síti*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 92 s. Vedoucí práce byl Ing. Radko Krkoš,

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Implementace triple-play služeb v heterogenní síti“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu semestrálního projektu panu Ing. Radkovi Krkošovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Technicka 12, CZ-61600 Brno
Czech Republic

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

PODĚKOVÁNÍ

Výzkum popsaný v této diplomové 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)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Tato práce se věnuje oblasti poskytování internetových služeb v síti internetového poskytovatele(ISP). Hlavní tématikou je poskytování multimediálního obsahu, který je v poslední době stále více vyžadován.

Obsahem teoretické části je popis problematiky poskytování triple-play služeb v transportních a přístupových sítích. Dále je věnována pozornost zabezpečení kvality služeb pracujících v reálném čase po paketově komutovaných sítích. Mezi témata teoretické části patří i popis využívaných přenosových médií v dnešních komunikačních sítích. Jednotlivý typy médií jsou porovnány a uvedeny jejich výhody a případné nevýhody. Dále jsou uvedeny technologie využité pro komunikaci v moderních sítích a konkrétní případy jejich použití.

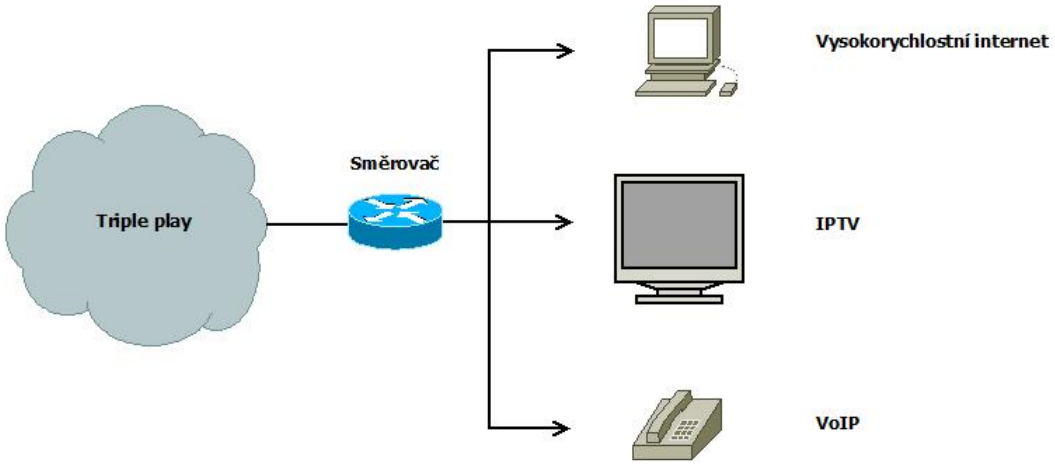
Nastudované teoretické informace o poskytování multimediálních služeb v heterogenních sítích jsou dále zkoumány v rámci praktické části na reálné infrastruktuře poskytovatele internetových služeb. Zde je analyzována použitá topologie a využité technologie v síti. Na základě požadavků a zjištěných faktorů následně sestaven plán pro implementaci triple-play služeb, který je následně realizován. Součástí implementace je vytvoření automatizovaného řešení pro zajištění požadované kvality služeb v heterogenní síti. V průběhu návrhu plánu a vytváření samotného technického řešení je kladen důraz na možnost reálného použití a do budoucna možnou škálovatelnost.

Výsledek práce je v závěru důkladně testován a jsou uvedeny zjištěné poznatky. Finální technické řešení je k dispozici v příloze a je umožněno jeho otestování. K tomu je určen návod v poslední části práce.

1 TECHNOLOGIE HETEROGENNÍCH SÍTÍ

1.1 Nové strategie

V současné době se v oblasti telekomunikací a moderních sítí nové generace stále častěji setkáváme s pojmem triple-play. Jedná se o poskytovaní datových a současně multimediální služeb. Samotné slovo triple zastupuje data, hlas a video. Ve výsledku si můžeme představit poskytování různých druhů služeb, používání více druhů zařízení a to vše s použitím jednoho dodavatele služeb (ISP). Více druhů služeb zastupuje poskytování běžného internetového připojení v kombinaci s multimediálními službami jako je přenos digitálního vysílání prostřednictvím IP sítí(IPTV) a hlasovými službami VoIP. [1]



Obr. 1.1: Poskytování triple-play služby

Koncept triple-play služeb není pouze novým komerčním produktem. Jedná se o reakci na změny a inovace v informačních technologiích a také ve společnosti. Uvedené faktory stále častěji přesvědčují operátory a poskytovatele služeb k tomu, aby nabízeli prostřednictvím svých sítí více, než jen klasickou internetovou přípojku. [2]

1.2 Přístupové sítě

Počítačové sítě pro podnikové i domácí použití mohou být vystavěny pomocí kabelů nebo také s využitím bezdrátové technologie Wi-fi. Před několika lety, kdy hromadně vznikaly počítačové sítě byla masově využita technologie klasického kabelového Ethernetu. Technologie využívá klasických UTP kabelů a síťového adaptéru na obou komunikujících stranách. Technologie byla vyvíjena desítky let a dnes ji lze

považovat za spolehlivou a s nízkými náklady. Nevýhodou kabelového ethernetu je větší náročnost na instalaci kabelů. V poslední době je stále více oblíbená technologie Wi-fi. Její nesporná výhoda je větší mobilita pro uživatele a také velmi jednoduchá instalace bezdrátové sítě. Není nutný žádný zásah do interiéru. Nevýhodou je nižší bezpečnost, je tak nutné dodržovat základní pravidla bezpečnosti jako je aktuální šifrovací protokol, dostatečně silný přístupový klíč apod. Dalším typem přístupové sítě je síť s využitím optického vlákna. Oproti metalickému kabelu nabízí optické vlákno větší šířku pásma, můžeme tedy dosáhnout větších přenosových rychlostí. Optické vlákno má menší útlum signálu než metalický kabel a není tak limitováno na zhruba 100 m, ale můžeme komunikovat na vzdálenost i několika kilometrů. Velkou výhodou optického vlákna je také odolnost proti elektromagnetickému rušení. Vzhledem k tomu, že optické vlákno nevyzařuje elektromagnetickou energii(mimo ohyb), je komunikace bezpečná a je obtížné ji odposlouchávat. Jedná se o nejbezpečnější médium pro přenos citlivých dat. Nevýhodou optického vlákna jsou vyšší pořizovací náklady. [3]
Přehledné porovnání jednotlivých typů přenosových médií, jejich výhody, a nevýhody, je uvedeno v tabulce 1.1

1.3 Transportní sítě

Z pohledu transportních sítí hraje poskytování triple-play služeb velkou roli. S nasazením multimediálních služeb do sítě poskytovatele se zvedají nároky na přenosovou kapacitu všech páteřních spojů a to velice znatelně. Pokud se dokonce poskytovatel rozhodne provozovat IPTV s využitím multicastu, samotná IPTV vyžaduje při vyšším zatížení kapacitu v řádu několika stovek Mb/s. Tento fakt je často spojen s tím, že je v dané síti nutno navýšit kapacity jednotlivých páteřních spojů. Pokud poskytovatel využívá optické trasy, má tak k dispozici dostatek kapacity. Situace je ovšem složitější v případě, kdy poskytovatel využívá mikrovlnné či bezdrátové spoje. Vzhledem k tomu, že výstavba optických tras je velice finančně a časově náročná záležitost, spousta poskytovatelů využívá ve svých infrastrukturách také různé typy bezdrátových spojů, ať už se jedná o mikrovlnné spoje s licencí, např. 11 nebo 17 GHz tak i bezdrátové spoje pracující ve volném frekvenčním pásmu, např. 5, 10 nebo 24 GHz. Použití těchto spojů typu bod-bod je pro poskytovatele výhodné v případě, že je nutné co nejrychleji pokrýt určitou lokalitu a je pro něj nevýhodné vybudovat optickou trasu, ať už časově nebo finančně. Mikrovlnné spoje také v dnešní době nabízí dostatečnou kapacitu na krátké vzdálenosti v řádu několika kilometrů. [4]

Tab. 1.1: Porovnání technologií pro přístupové sítě. [11]

Technologie	**Popis**
Kabelový Ethernet	**Výhody:** • Spolehlivost, • jednoduchá údržba, • rozšířenost, • cena. **Nevýhody:** • Náročnější instalace, • nutnost používat kabel, • omezená mobilita.
Bezdrátové Wi-fi sítě	**Výhody:** • Mobilita, • jednoduchá instalace. **Nevýhody:** • Bezpečnost, • spolehlivost, • interference mezi sítěmi.
Optické vlákno	**Výhody:** • Vysoká propustnost, • nízký útlum, • bezpečnost komunikace, • odolnost proti elektromagnetickému rušení. **Nevýhody:** • Cena výstavby optický tras, • odolnost optických vláken proti fyzickému namáhání.

1.4 Zabezpečení kvality služeb

Počítačové sítě tak jak je známe se v posledních letech významně změnily. Důležitým důvodem jsou jednoznačně nové služby, které koncoví uživatelé využívají. Jedná se zejména o sledování videa v reálném čase. Spolu s videem se v dnešní době také velice často využívá hlasových služeb, tzv. VoIP. Nasazením těchto služeb se automaticky setkáváme s problematikou zajištění kvality služeb, tzv. QoS (Quality of Service). Výzvou pro zajištění kvality poskytování služeb je také fakt, že se v současné době stále více využívají bezdrátové sítě. Bezdrátové sítě samy o sobě nenabízí takovou úroveň spolehlivosti a kvality přenosu jako např. sítě LAN. Zajištění kvality služeb (QoS) jejím uživatelům závisí na několika faktorech a entitách konkrétní uvažované sítě. Pro zjištění všech faktorů, které je třeba vzít v potaz ohledně zajištění kvality služeb musíme uvažovat specifika všechn technologií, které daný paket využije při cestě od zdroje k cíli. V následující části jsou popsány všechny důležité faktory pro zajištění kvality pro poskytování IPTV a VoIP služeb v heterogenních sítích. [12]

1.4.1 Důvod pro QoS?

Dnešní telekomunikační sítě jsou založené na protokolu IP. Protokol vznikl před více než 30 lety a má za sebou tedy mnoho let vývoje. Zajišťuje přenos paketů požadovanou strukturou aktivních prvků využitím IP adres. Naprostá většina dnešních aplikací je na protokolu IP založena. Sítě založené na protokolu IP jsou velmi efektivní, ale standardně negarantují maximální zpoždění jednotlivých paketů, které je nutné dodržet pro správne fungování služeb pracujících v reálném čase.

IP protokol poskytuje nespolehlivou a nespojovanou službu. Narozdíl od přepínání okruhů, kdy je před samotným přenosem sestaven komunikační okruh a po dobu přenosu mají přenášená data totožné podmínky, v případě přepínání paketů probíhá komunikace odlišným způsobem. Před komunikací není sestaven okruh, ale data jsou odesílána postupně a o směrování a doručení se starají aktivní prvky dané sítě. Každý paket nese informaci o cíli, kam má být doručen. Je tak možné, že všechny pakety nebudou doručeny stejnou cestou, ale v případě vytížení nebo poruchy linky na trase budou pakety směrovány záložní trasou. Odlišné trasy mají samozřejmě jiné parametry (zpoždění, jitter, ztrátovost apod.). Původní zpráva musí být na straně příjemce následně opětovně sestavena. V případě, že pakety došly v rozdílném pořadí, musejí být přeuspořádány. [13]

Z toho důvodu bylo nutné původní IP protokol aktualizovat a zavést podporu kvality služeb (QoS). Aktuální technologie používané v počítačových sítí přistupují k síťovému provozu ve dvou základních krocích:

- Roztřídění provozu.
- Řízení přetížení.

1.4.2 Roztřídění provozu

Ve fázi rozlišení, resp. roztřídění síťového provozu se celkový objem přenášených dat rozdělí na menší části. S jednotlivými částmi může být pak různě zacházeno. Rozlišení provozu probíhá ve dvou krocích:

1. **Klasifikace provozu**: Síťový provoz je rozdělen do tříd nebo více toků. V určitých případech je nutné označit provoz CoS (Class-of-Service) identifikátorem, který slouží pro označená druhu služby.
2. **Rozdílné zacházení s třídou provozu**: Pakety mají různé požadavky a nároky v průběhu přenosu. V určitém případě pakety vyžadují vyšší prioritu nebo přímo vyhrazení systémových prostředků pouze pro konkrétní službu.

Rozlišení služeb: O rozlišení služeb mluvíme v případě, kdy je s určitou částí provozu zacházeno prioritně oproti ostatnímu provozu. Tímto způsobem lze zajistit určitou úroveň kvality služeb. Tato metodika se nazývá také „Soft QoS“.

Garantování služeb: Garantování služeb je pokročilým krokem. Garantování je zaručeno vyhrazením systémových prostředků sítě pouze pro určité datové toky. Toto opatření je spolehlivější z hlediska zaručení kvality služby, vyžaduje ovšem větší šířku pásma. Garantování služeb je označované jako „Hard QoS“. [7]

S popsanými technikami jsou v praxi spojené termíny:

- **Intserv** – Metoda založena na pevné rezarvaci pásma v okamžiku navázání spojení. Představuje tak jistým způsobem okruhově orientovaný model v paketově orientovaných sítích. Pevná rezervace obnáší plýtvání přenosovým pásmem.
- **Diffserv** – Nezajišťuje pevnou šířku pásma, ale definuje zacházení s paketem dle informací uvedených v poli ToS, které se nachází v hlavičce paketu. Každé zařízení pracující na třetí vrstvě TCP/IP modelu musí poté nakládat s paketem na základě příslušných informací v poli ToS. [8]

1.4.3 Řízení přetížení

Přetížení znamená v síťovém provozu značnou degradaci propustnosti z důvodu vysoké zátěže. Efektivní správou síťových prostředků je možné efektivně směrovat

data i při vysoké zátěži. Vliv přetížení na síťový provoz je poté daný konfigurací QoS.

Existují dva způsoby jak se vypořádat s přetížením sítě:

1. **Řízení přetížení**: Jedná se o sadu mechanismů, které v případě detekce přetížení začnou zahazovat příchozí provoz podle daných podmínek.
2. **Předcházení přetížení**: Mechanismus, který se umí vypořádat s přetížením před tím, než nastane. Existují dva typy předcházení přetížení:
   - Prvním způsobem je kontrola na rozhraní sítě. Technika představuje limitování příchozího provozu na aktivním prvku který leží na rozhraní mezi vnitřní sítí a sítí sousedící(např. sousedící Autonomní systém). Toutu cestou zajistíme, aby síťové prvky v námi spravované síti danou kapacitu zvládnuli zpracovat.
   - Dalším způsobem je kontrola aktuálně využitých síťových prostředků v sítí.

Jako pasivní ochranu proti přetížení sítě může např. ISP aplikovat opatření dovolující urřitý objem přenesených dat za časový interval. Při překročení mohou být aplikovány příslušné politiky. Tímto opatřením může být nadbytečný provoz v síti zpracován bez zajištění kvality služeb, resp. bez garance. Konkrétní zacházení se síťovým provozem koncového účastníka je většinou specifikováno dohodou o garanci poskytovaných služeb, tzv SLA. Celková zátěž síťové infrastruktury by měla být přizpůsobena technickým možnostem sítě, aby byla zajištěna garance rychlého odbavení dat a optimálního využití sítě. Pokud je infrastruktura vytížena více, než dovolují možnosti dimenzování, výkon bude degradován z důvodu zahlcení aktivních prvků a nutnosti zahazování přenášených paketů. [1]

1.4.4 Parametry přenosu dat

Pokud chceme dodržovat určitou kvalitu poskytovaných služeb, je nutné sledovat patřičné parametry při přenosu dat. Je však důležité si uvědomit, že kvalita služeb je poskytována danou síťovou infrastrukturou, ale vnímána koncovými uživateli. Z toho důvodu je kvalita služby specifikována těmito parametry:

- "End-to-End" zpoždění.
- Bitová chybovost (BER).

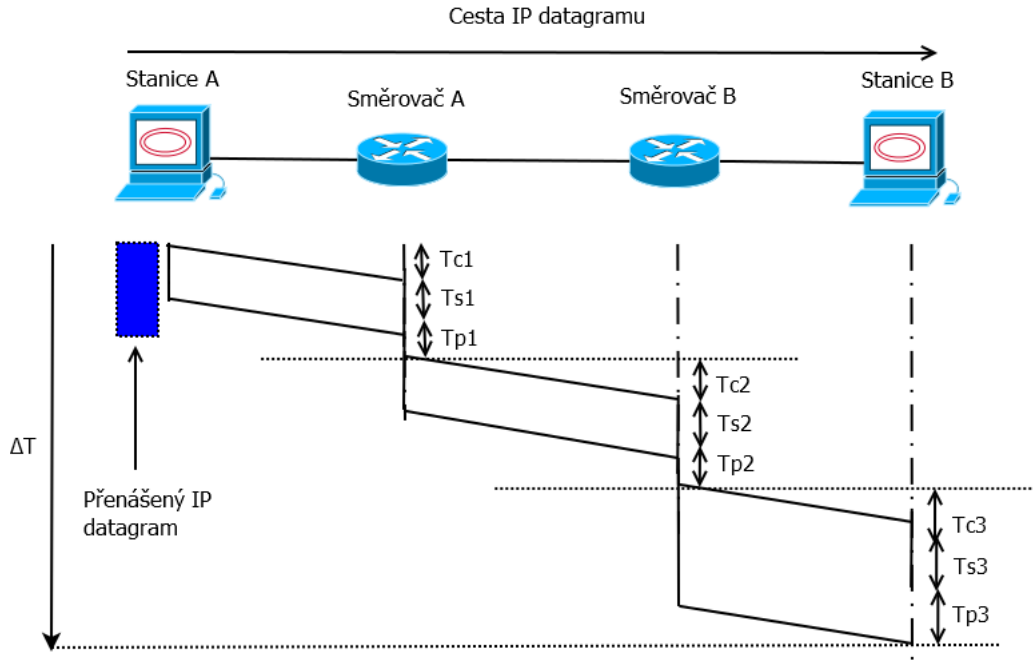
Tyto parametry udávají zpoždění přenášených dat od zdroje až k uživateli a procento přenášených dat, které není úspěšně doručeno.

Skupina parametrů IPPM (Internet Protocol Performance Metrics), vytvořená organizací IETF definuje způsob, jakým ohodnotit parametry přenášeného síťového provozu. Tyto parametry se využívají při návrhu sítě, výběru používaných technologií a také pro poskytování kvality služeb a dodržování SLA. [7]

- Zpoždění,
- Proměnlivost zpoždění,
- Ztrátovost,
- Šířka pásma.

Jednocestné zpoždění

Jednocestné zpoždění, resp. "One-way Delay" je čas, který je nezbytný pro přenos datového paketu od zdroje k cíli. Tento čas je součtem zpoždění na jednotlivých linkách a času nutného pro zpracování paketu příslušným síťovým prvkem, viz. obr. 1.2.



Obr. 1.2: Zpoždění paketu na cestě od zdroje k cíli

$$\Delta T = \sum T_{ci} + \sum T_{si} + \sum T_{pi} - T_p \tag{1.1}$$

Rovnice 1.1 uvádí součet všech položek, ze kterých se skládá celková doba nutná pro přenos paketu od zdroje k cíli.
Tyto položky jsou T_c – doba nutná k přenosu paketu přes konkrétní linku, T_s – zpoždění mezi přenosem prvního a posledního bitu konkrétního paketu a T_p – doba nutná ke zpracování paketu na směrovačích nebo přepínačích. Vzhledem k tomu, že při cestě paketu sítí se liší celkový počet linek a uzlů o 1, je nutné odečíst T_p ze sumy T_{pi}. Podrobnější popis jednotlivých parametrů:

- **Zpoždění zpracováním** – jedná se o čas vyžadovaný aktivním prvkem nutný pro přijetí paketu na příchozím rozhraní. Následně je paket zpracován a je vybráno odchozí rozhraní. Pokud je prvek aktuálně vytížen, může být paket zařazen do odchozí fronty, kde se doba zpracování ještě více prodlouží.
- **Zpoždění závislé na linkové rychlosti paketu** – toto zpoždění vzniká v době mezi přijetím prvního a posledního bitu paketu. Je závislé na typu zařízení. Některé aktivní prvky po přijetí prvního bitu čekají na přijetí celého paketu a následně ho zpracují a odešlou. Existují ovšem také přepínače, které jsou schopné jednotlivé rámce přeposlat ihned po zjištění cílové adresy.
- **Propagační zpoždění** – čas, který je vyžadován mezi odesláním prvního bitu na straně vysílače a přijmutím posledního bitu téhož paketu na straně přijímače. Tento čas je závislý na konkrétním přenosovém kanálu a je také přímo uměrný vzdálenosti, resp. délce konkrétní linky. [1]

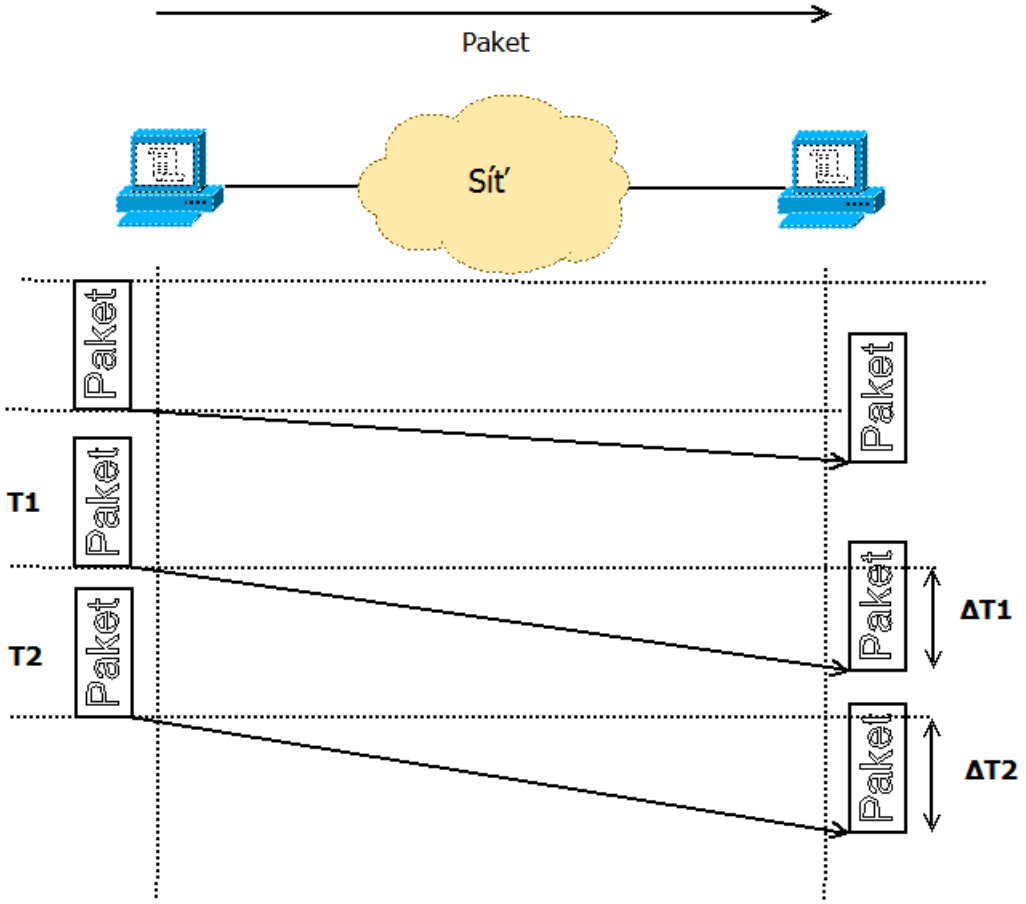
Odchylka zpoždění - Jitter

Představuje rozdíl ve zpoždění mezi odesláním a přijetím dvou po sobě následujících paketů při přenosu většího souboru, viz. obr. 1.3. Pokud však bereme v potaz pouze dva po sobě jdoucí pakety je taková hodnota často zanedbatelná. Z toho důvodu existuje několik dalších parametrů, které slouží ke zjištění odchylky zpoždění:

- **Jitter** – Velmi často používaný parametr. Pokud mluvíme o paketově přepínaných sítích, jedná se o parametr velice blízký odchylce zpoždění. Odchylka zpoždění může být ovšem i záporné číslo. Naopak Jitter je udávám v absolutní hodnotě.
- **Jednosměrný rozdíl zpoždění** – Parametr podobný odchylce zpoždění. V tomto případě je to nezáporné číslo a jedná se o statistickou hodnotu, která je průměrem rozdílů naměřených hodnot.
- **Špičková odchylka zpoždění** – Rozdíl mezi maximem a minimem při měření zpoždění.
- **Rozdíl doručení** – Měříme časový rozdíl mezi dvěma po sobě přijatými pakety. Není vyžadováno časové razítko nebo číslo sekvence. Z toho důvodu je tento parametr jednoduché změřit a je užitečný pokud zkoumáme odchylku zpoždění při přenosu. [5]

$$\Delta\Delta T = \Delta T_{d+1} - \Delta T_d \tag{1.2}$$

Rovnice 1.2 znázorňuje jednocestnou odchylku zpoždění. Odchylka je rovna rozdílu zpoždění prvního paketu T_d a rozdílu zpoždění následujícího paketu T_{d+1}.



Obr. 1.3: Měření rozdílu zpoždění

Ztrátovost paketů

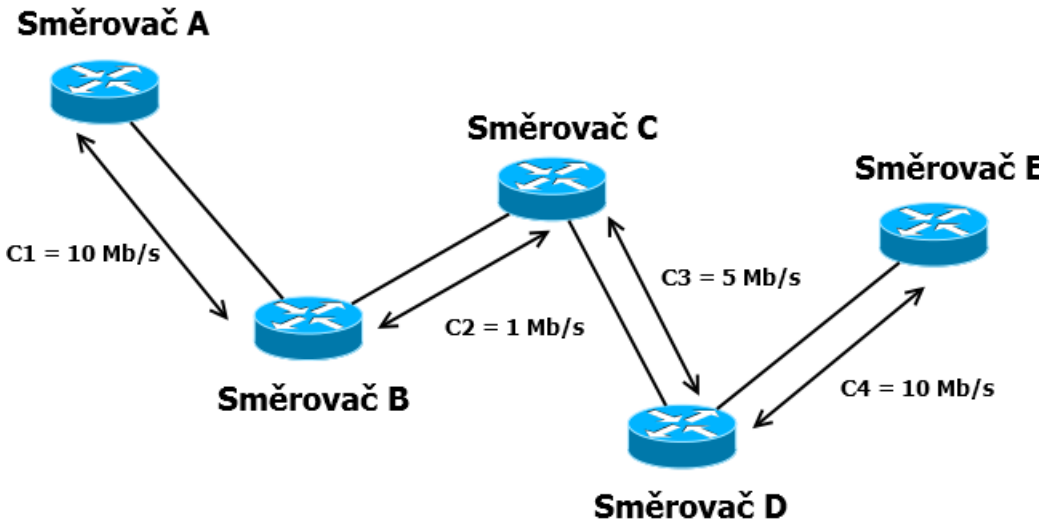
Údaj o ztrátovosti paketů udává poměr mezi počtem paketů, které nebyly správně přijaty na straně přijímače a celkovým počtem paketů. Pakety často nejsou přijaty správně pokud jsou zahozeny některým z aktivních prvků po cestě směrem k cíli, případně vyprší časový limit pro doručení na straně přijímače. Doručení paketů příliš pozdě má negativní vliv pokud se jedná a službu v reálném čase. V tomto případě je důležitější dodržet určitou hodnotu maximálního zpoždění, např. 150 ms. Doručení 100% všech dat není v tomto případě tak kritické. Mírné snížení kvality hovoru můžeme považovat za zanedbatelné, ale zpoždění hlasu např. o 1 vteřinu je kritické. [6]

Šířka pásma

Dalším velice důležitým parametrem je šířka pásma dané komunikační linky. Důležité parametry jsou:

- **Kapacita linky** – udává maximální objem dat, který lze linkou přenést za časový interval.
- **Dostupná šířka pásma** – dostupná šířka pásma na dané lince v určitý moment.

Pokud jsou na konkrétní komunikační trase stejné podmínky po dobu přenosu dat, kapacita daného kanálu je po tuto dobu konstantní. V případě bezdrátových sítí nebo sítí využívajících přenos dat po elektrické síti (PLC) se podmínky v čase mění a linková rychlost může následně kolísat. V závislosti na objemu přenášených dat se mění aktuální dostupná kapacita linky v daném čase, z toho důvodu je vhodné sledovat vytížení takové linky. Pokud máme složitější infrastrukturu v sítí, je nutné znát tzv. úzké hrdlo. Tak je většinou nazývána linka s nejnižší kapacitou, při vyšší zátěži bude tedy logicky vytížena na 100% jako první. Tuto situaci ilustruje obr. 1.4. Zde můžeme vidět, že linka mezi směrovačem 2 a 3 disponuje kapacitou pouze 1 Mb/s, při vyšší zátěži bude tedy pravděpodobně využita na 100%.



Obr. 1.4: Síťová infrastruktura s rozdílnou kapacitou linek

Při zajišťování kvality služeb (QoS) je nutné znát tzv. „úzka hrdla“ v síti. Pokud chceme zajistit garantovaní služby pro uživatele směrem od zdroje k jeho přijímači, můžeme zjistit, že na určitém místě v síti není možné požadovanou službu garantovat z důvodu nedostatečné kapacity linky. V takovém případě se může stát, že poskytovatel není schopen dodržet SLA a je tedy nutné kapacitu takové linky navýšit. [7]

1.5 Technologie přenosu dat

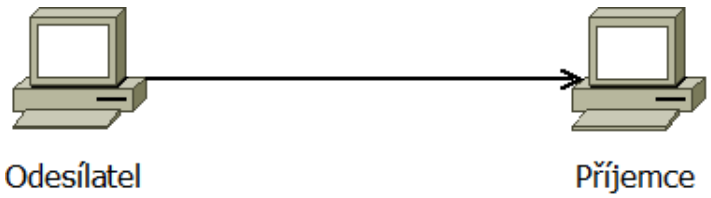
Cílem této kapitoly je popsat možnosti přenosu dat v počítačové síti včetně mechanismů pro skupinovou komunikaci. Technologie a mechanismy používané pro přenos dat v počítačové síti můžeme rozlišovat podle toho, kolik účastníků si vyměňuje informace v dané situaci. Pokud se jedná pouze o dva účastníky, můžeme takový typ komunikace brát jako speciální druh skupinové komunikace, standardně se typy komunikace rozlišují takto:

- Unicast (1:1).
- Multicast (1:n).
- Concast (m:1).
- Multipeer (m:n).

,kde m>1, n>1. Údaje v závorkách udávají počet účastníku na straně odesílatele a počet účastníků na straně příjemce. Speciální případ, pokud je příjemce, či odesílatel pouze jeden je označen číslem "1". [9]

1.5.1 Unicast

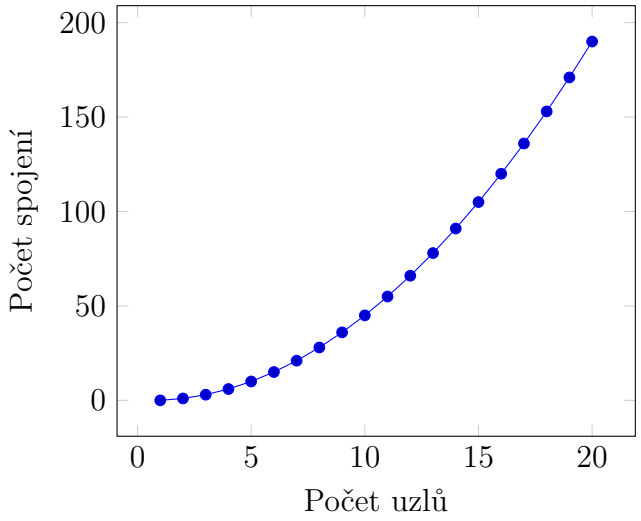
Unicast je standardní typ komunikace "bod-bod", resp. "uživatel-uživatel". Výměna uživatelských dat probíhá vždy jednosměrně, viz. obr. 1.5. Pokud si uživatelé vymě-



Obr. 1.5: Základní komunikace - Unicast

ňují data navzájem, musí existovat dvě unicast spojení. Vyjímkou jsou samozřejmě data nutná pro funkčnost samotného spojení, kontrola doručení apod. Tyto data jsou v rámci jednoho spojení odesílána obousměrně. Tento typ komunikace je vhodný pro výměnu dat pouze mezi dvěma uživateli. Pokud bychom použili unicast pro skupinovou komunikaci, je nutné vytvořit oddělené spojení mezi všemi členy skupiny. Celkový počet spojení roste kvadraticky s počtem uzlů a je dán rovnicí 1.3, kde c je celkový počet spojení a n počet uzlů. V případě, že uvažujeme větší skupinu uživatelů, je takový způsob komunikace neefektivní a obtížně realizovatelný. Graf roustoucího počtu spojení při 20 uzlech znázorňuje obr. 1.6. [10]

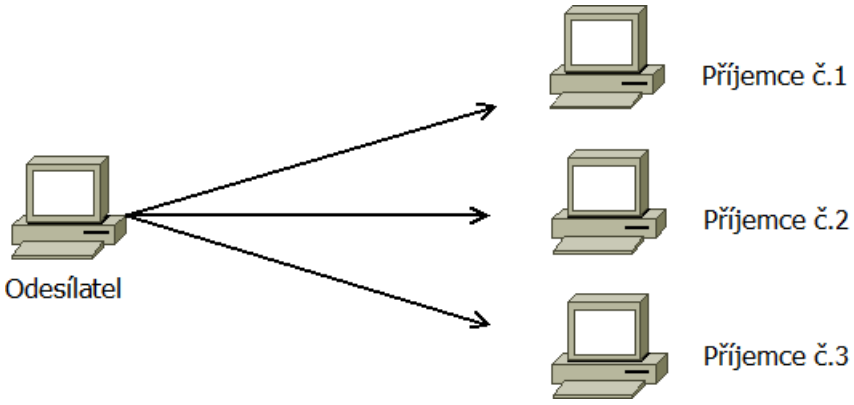
$$c = \frac{n(n-1)}{2} \tag{1.3}$$



Obr. 1.6: Nárůst počtu unicast spojení v závislosti na počtů uzlů

1.5.2 Multicast

V případě skupinové komunikace, tzv. „multicastu“ jsou data odesílána od zdroje jednomu a více příjemcům. Situace, kdy existuje pouze jeden příjemce představuje speciální případ unicastu. Schéma obr. 1.7 znázorňuje situaci, kdy jsou z jednoho zdroje odesílána data třem příjemcům. Všechny stanice přijímající data jsou schopny



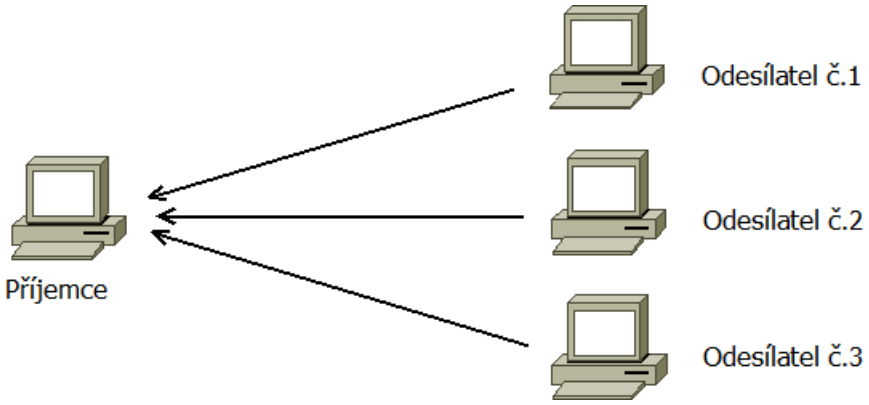
Obr. 1.7: Skupinová komunikace - Multicast

data pouze přijmout, nemohou žádné data odeslat zpět, v rámci jednoho multicast spojení odesílají zpět pouze řídící data pro správu přenosu uživatelských dat. Pokud bychom vyžadovali obousměrný přenos dat, je nutné vytvořit více multicast spojení. Počet těchto spojení odpovídá počtu stanic v dané síťové infrastruktuře.
Skupinová komunikace je výhodná pokud více stanic vyžaduje totožný obsah. Nemusíme tak přenášet na všech linkách totožná data vícekrát pro každého uživatele,

tím můžeme mnohem efektivněji využívat dostupnou šířku pásma. Nevýhodou je nutnost podpory síťovou infrastrukturou.

1.5.3 Concast

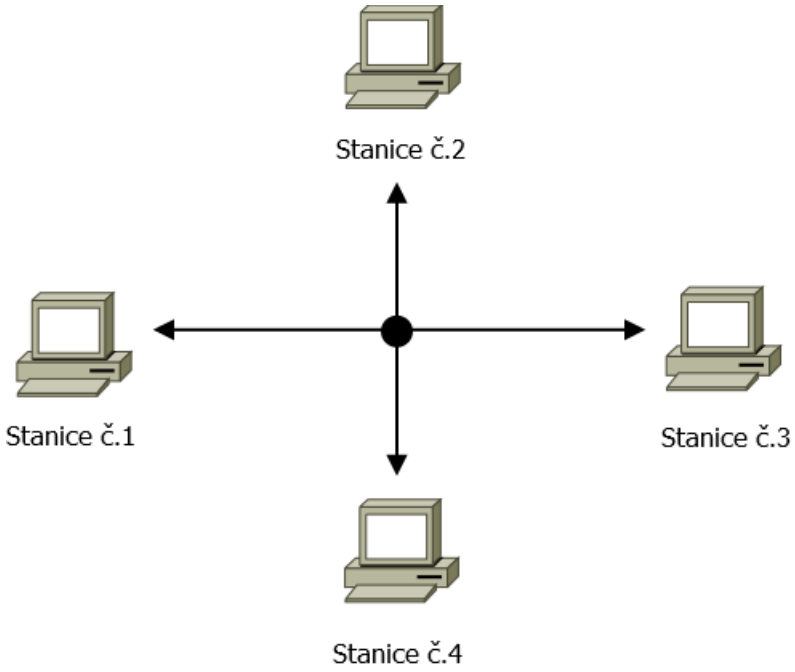
Tzv. “concast” komunikace se využívá v případě, kdy více stanic v síti odesílá data jednomu příjemci, je možné označit “m:1”. S tímto typem komunikace se můžeme setkat např. pokud velké množství stanic odesílá výsledky simulace na server, který tyto data shromažďuje, viz. obr. 1.8



Obr. 1.8: Shromažďování dat od více příjemců - Concast

1.5.4 Multipeer

Multipeer komunikace je vhodná v případě, kdy určitý počet účastníku potřebuje komunikovat navzájem, viz. obr. 1.9. Jako příklad se nabízí např. spolupráce na stejném projektu, sdílení informací apod. Tento typ komunikace je označován jako “m:n” a často je označován jako “peer-to-peer”. Multipeer je typ komunikace, který se pravděpodobně nejvíce odlišuje od ostatních typů skupinové komunikace, zároveň je často náročné tento typ komunikace implementovat. Většinou se využívá několik multicast spojení současně. [9]



Obr. 1.9: Vzájemná komunikace mezi více účastníky - Multipeer

1.6 Problematika poskytování triple-play služeb

Cílem této kapitoly je uvést souhrn problémů, se kterými je nutné se vypořádat pokud zvažujeme nasazení triple-play služeb do již existující sítě. Důležitým počátečním krokem, který je vhodné považovat za nezbytný, je detailní analýza existující síťové infrastruktury. Pokud máme k dispozici všechny nutné informace o síťové infrastruktuře, můžeme na základě dostupných dat navrhnout, které služby je možné v síti provozovat bez úprav sítě a služby, které vyžadují určitý zásah do infrastruktury.

1.6.1 Hlasové služby

Poskytování hlasových služeb patří ke službám, bez kterých se již dnes uživatelé neobejdou. Pro poskytovatele to znamená poskytnout koncovým zákazníkům internetové připojení s dostatečně krátkou odezvou a obsluhovat jej na všech aktivních prvcích prioritně před ostatními datovými službami. Hlasové služby nejsou příliš náročné na šířku pásma a není tak nutné budovat vysokokapacitní páteřní linky.

1.6.2 Video služby

Pokud jde o poskytování video služeb, zde je problematika zavedení těchto služeb, zejména IPTV složitější. Jsou-li v síti využívány bezdrátové spoje, u kterých se dy-

namicky mění odstup signálu od šumu (např. v případě špatného počasí) je vhodné zvážit, jaký typ IPTV je možné v takové síti úspěšně provozovat.

Unicast IPTV

Tento typ televizního vysílání je vhodným krokem pokud chceme implementovat IPTV v síti lokálního poskytovatele, kde nejsou všechny linky schopné poskytnout dostatečně kvalitní parametry a pro přenos multicastu (ztrátovost). V současné době je možné s využitím unicastu distribuovat komprimovanou IPTV, která vyžaduje šířku pásma v rozmezí 3-5 Mb/s. Při návrhu služby bylo počítáno s využitím na sítích s nižší přenosovou kapacitou a vyšší úrovní chybovosti. Služba poskytuje televizní vysílání ve standardní kvalitě z důvodu úspory přenosové kapacity. Výhodou tohoto typu IPTV pro menší lokální poskytovatele je fakt, že mohou začít poskytovat tuto službu včetně všech důležitých funkcí patřících k IPTV, jako je time-shift, pause, time-rewind, Video-on-Demand apod. Nevýhodou je, pokud bychom tuto službu chtěli poskytovat pro velký počet uživatelů. Vzhledem k tomu, že se jedná o přenos dat typu unicast, každý uživatel vyžaduje svoje vlastní spojení mezi serverem a přijímačem. Páteřní spoje mohou být tak značně vytížené. [13]

Multicast IPTV

Multicast IPTV je původní typ internetové televize, který ovšem vyžaduje komunikační linky s vysokou úrovní kvality parametrů jako je odezva, ztrátovost apod. Pokud nejsou tyto parametry poskytnuty na dostatečně kvalitativní úrovní, dochází k degradici kvality služby a v hodrším případě i k výpadku služby, pokud je chybovost na úrovni, kdy již nelze obraz na straně přijímače z přijatých dat sestavit ani s použitím samoopravných kódů. Multicast IPTV používá při přenosu protokol UDP na transportní vrstvě. Pokud nastane při přenosu chyba, neexistuje zde mechanismus, které by zajistil opětovné zaslání dat, které k příjemci nedorazili. V případě sítě, která se skládá z optických nebo standardních kabelových spojů (UTP) je nasazení Multicast IPTV vhodné, v opačném případě je nutné prověřit, zda je multicast možné na daných linkách provozovat. Standardní televizní kanál s využitím Multicast IPTV vyžaduje obvykle mezi 7-15 Mb/s. Služba je určena pro sítě s infrastrukturou využívající kabelové spoje, kde je k dispozici dostatečná šířka pásma a je tak možné přenášet vysílání ve vysoké kvalitě. Výhodou tohoto typu IPTV je vyšší kvalita vysílání a pro poskytovatele jednoznačně efektivnější využití šířky pásma na páteřních spojích. Nevýhodou IPTV jednoznačně zůstává fakt, že je obtížné provozovat multicast na linkách s nižší kvalitou parametrů (odezva, ztrátovost).

2 IMPLEMENTACE SLUŽEB V PRAXI

Obsahem této části práce je dokumentace jednotlivých etap, které bylo nutné absolvovat při implementaci triple-play služeb na reálné heterogenní síti. Jednotlivé etapy jsou přehledně uvedeny na obr. 2.1.
Pro minimalizování komplikací, které by se mohly vyskystnout při implementaci bylo rozhodnotu zvolit co možná nejvíce spolehlivou strategii. Zvolené etapy jsou částečně inspirované metodikou „Prepare-Plan-Design-Implement-Operate-Optimize“ (PPDIOO). Jedná se o šest fází návrhu a provozu telekomunikační sít navrhnutých společností Cisco. Tato metodika správy sítě určuje, jak by se mělo přistupovat při návrhu topologie, implementace požadovaných technologií a jejich následné údržbě. [14]

Obr. 2.1: Proces implementace služby do existující infrastruktury

Tab. 2.1: Stručný popis etap.[14]

Etapa	Popis
Stanovení požadavků	Určení požadavků organizace nebo podniku pro možnost následného návrh strategie, vhodných postupů a technologií k jejich dosažení.
Analýza infrastruktury	Technická analýza síťové infrastruktury na které je požadováno poskytovat dané služby. Zmapování důležitých parametrů infrastruktury, jako je propustnost, zpoždění a ztrátovost paketů.
Návrh řešení	Vytvoření návrhu konkrétního technického řešení na základě informací a požadavků z předchozích fází. Součástí návrhu řešení je tvorba časového plánu zpravování řešení a následné implementace.
Zpracování řešení	Jakmile je hotový návrh řešení, následuje zpracování samotného řešení, resp. realizace. Zpracování řešení zahrnuje přípravu konfigurace aktivních síťových prvků a dalších fyzických zásahů do síťové infrastruktury.
Implementace	Nasazení řešení vytvořeného v předchozí části na reálnou síťovou infrastrukturu. Tato část může zahrnovat fyzický zásah do infrastruktury a např. také změnu topologie, se kterou je nutné v předchozích bodech počítat aby výpadek služeb pro koncové uživatele byl co možná v nejmenším rozsahu. V případě potíží nebo situace, kdy narazíme na problém se kterým se v návrhu nepočítalo, musí existovat náhradní plán pro uvedení síťové infrastruktury do původního stavu.
Optimalizace	Fáze, kdy se řešení používá v běžném provozu. Získavají se zde provozní informace na základě monitorování síťového provozu, případě zpětné reakce uživatelů. Provádí se také údržba a odstraňují se případné chyby.

2.1 Stanovení požadavků

První částí praktické implementace triple-play služeb v heterogenní síti byla analýza potřeb poskytovatele služeb, který tuto síť provozuje. Tento poskytovatel působí jako regionální ISP a poskytuje internetovou konektivitu pro koncové domácí uživatele a firemní klienty. Prostřednictvím vlastní infrastruktury poskytuje koncovým uživatelům kromě datového připojení také služby IP telefonie (tzv. VoIP). K přenosu dat v rámci vlastní infrastruktury je využíváno více druhů přenosových médií, jako je např. optické vlákno, kroucená dvojlinka, bezdrátové a také mikrovlnné spoje. Jednotlivé uživatelské přípojky se od sebe také liší poskytovanou přenosovou rychlostí v Mb/s ve směru k (download) a od (upload) uživatele, viz. tab: 2.2

Požadavkem poskytovatele je nabídnout aktuálním a do budoucna dalším novým

Tab. 2.2: Poskytované tarify koncovým klientům.

Tarif	**Maximální rychlost stahování dat [Mb/s]**	**Maximální rychlost odesílání dat [Mb/s]**
1.	5	1
2.	10	2
3.	15	3
4.	20	5

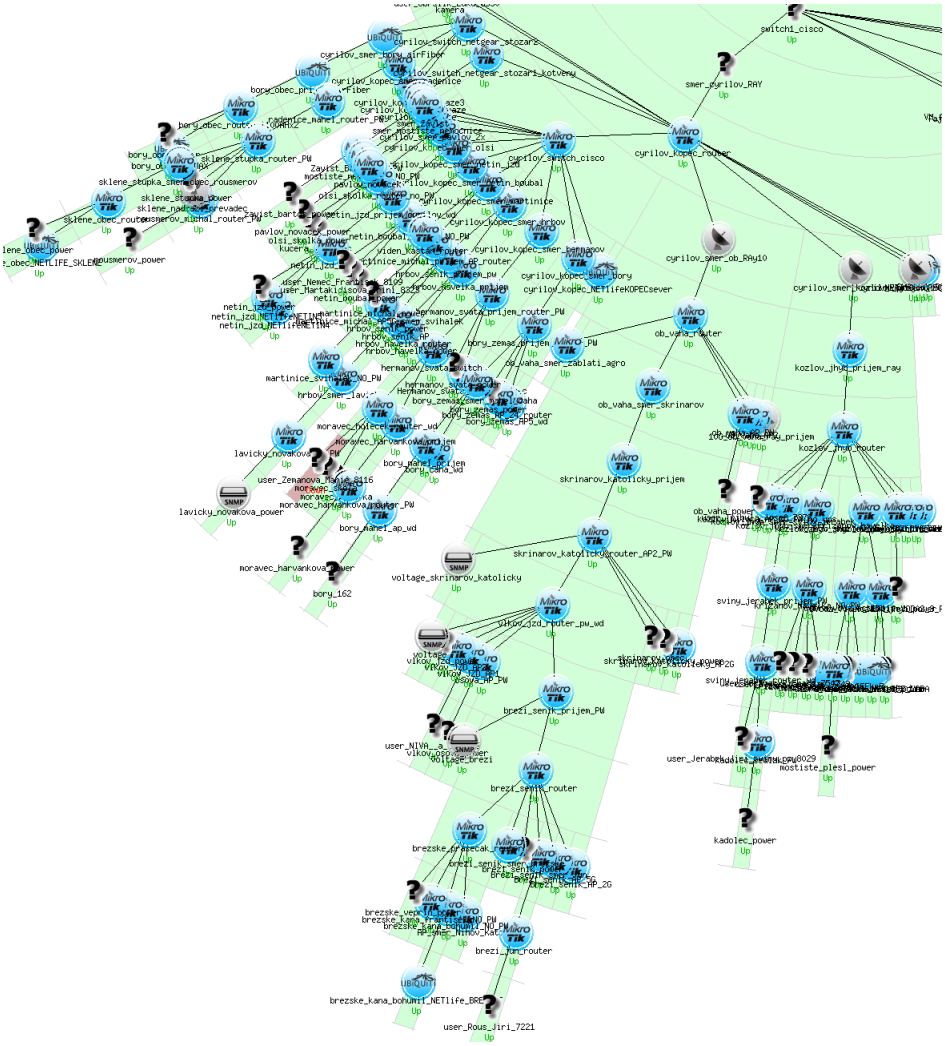
uživatelům mimo standardní internetové přípojky také nové doplňkové multimediální služby, primárně IPTV. Vzhledem k tomu, že v případě poskytování dalších multimediálních služeb zcela jistě narostou objemy přenášených dat v síti, dalším požadavkem je také poskytnutí kvality služeb pro časově kritické služby, jako je např. VoIP telefonie. Mezi další požadavky patří také to, že nasazení nových typů služeb musí probíhat na již fungující síti, pokud možno bez výpadku, aby uživatelé, kteří infrastrukturu již využívají nebyli omezováni.

2.2 Analýza infrastruktury

V rámci této části byla analyzována síťová infrastruktura, poskytovatelem používané technologie a také nástroje, které slouží k hromadné správě uživatelů a jim poskytovaných služeb.

2.2.1 Infrastruktura

Topologie zkoumané síťové infrastruktury se dá obecně klasifikovat jako strom, viz. obr. 2.2. Pro zachování alespoň částečné přehlednosti je níže zobrazena pouze část topologie pro získání základní představy. Kompletní mapa topologie je k dispozici na přiloženém DVD, viz B. Uvedený stromový graf byl získán pomocí síťového monitorovacího software Nagios. [15]



Obr. 2.2: Náhled části topologie zkoumané infrastruktury

Nagios je systém, který je využíván softwarem ISPadmin. Stará o správu síťové infrastruktury a koncových uživatelů, dále viz. 2.2.6. Ze zkoumané topologie vidíme, že existuje centrální místo, tzv. kořen stromu. Do tohoto místa je přivedena internetová konektivita optickým kabelem a následně je distribuována dále. Pro samotný přenos dat je využito několik typů přenosových médii, např. jednovidové optické vlákno, kroucená dvojlinka kategorie 5, $5E$, 6 a 7 UTP, případně FTP. Dále je využíváno také bezdrátových technologií, jako jsou mikrovlnné spoje pracující na kmitočtech 10, 17 a také 24 GHz. Kromě mikrovlnných spojů je také rozsáhle využíváno bezdrátových spojů využívajících kmitočtů $2,4$ a 5 GHz. Kompletní seznam používaných technologií je uveden v tab. 2.3. Jakákoli organizace,

Tab. 2.3: Používaná přenosová média a jejich přenosová kapacita

Typ přenosového média	**Technologie přenosu dat**	***Propustnost dle normy - [Mb/s]**
optické vlákno	IEEE 802.3 - Ethernet	1000
kroucená dvojlinka	IEEE 802.3 - Ethernet IEEE 802.3 - Ethernet	100 1000
mikrovlnný spoj 10 GHz – 28 MHz	IEEE 802.3 - Ethernet	170
mikrovlnný spoj 17 GHz – 56 MHz	IEEE 802.3 - Ethernet	360
mikrovlnný spoj 24 GHz – 100 MHz	IEEE 802.3 - Ethernet	700
bezdrátový spoj 2,4 GHz	IEEE 802.11b - 20 MHz IEEE 802.11g - 20 MHz IEEE 802.11n - 20 MHz	11 54 65
bezdrátový spoj 2,4 GHz	IEEE 802.11n - 20 MHz MIMO 2x2	130
bezdrátový spoj 5 GHz	IEEE 802.11a - 20 MHz IEEE 802.11n - 20 MHz	54 65
bezdrátový spoj 5 GHz	IEEE 802.11n - 20 MHz MIMO 2x2	130
*Údaje na základě použité technologie fyzické vrstvy.		

která používá telekomunikační síť a je připojena k síti internet, typicky tedy také poskytovatel internetových služeb, je povinen oznámit používaná datová rozhraní v jeho síti a jejich technické specifikace. Povinné oznámení rozhraní pro připojení

k veřejné komunikační síti vychází ze zákona dle §73 odst. 7 zákona č. 127/2005 Sb., o elektronických komunikacích. Specifikace rozhraní, která jsou využívána ve zkoumané sítí uvádí tab. 2.4 Na základě zjištěných parametrů používaných technologií,

Tab. 2.4: Zjištěná používaná rozhraní

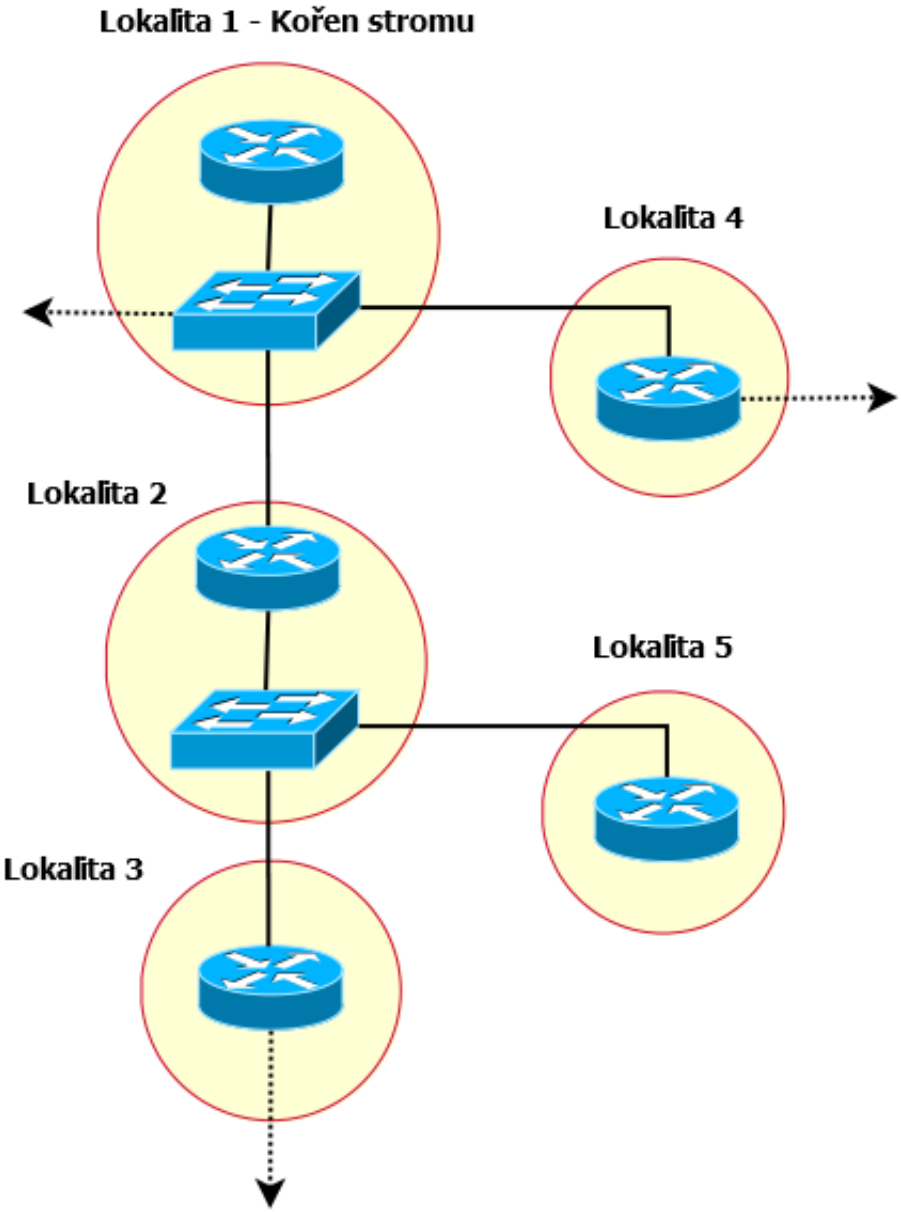
Rozhraní datových služeb		
Rozhraní	**Norma**	**Konektor / Poznámka**
Ethernet 10 Base-T	IEEE 802.3	RJ-45F
Ethernet 100 Base-TX		RJ-45F
Ethernet 1000 Base-T		RJ-45F
Ethernet 1000 Base-LX		SFP-LC
Wireless LAN	IEEE 802.11b	Wi-Fi 2,4 GHz
	IEEE 802.11g	Wi-Fi 2,4 GHz
	IEEE 802.11n	Wi-Fi 2,4 GHz
Wireless LAN	IEEE 802.11a	Wi-Fi 5 GHz
	IEEE 802.11n	Wi-Fi 5 GHz
Rozhraní hlasových služeb		
VoIP SIP	RFC 3261	RJ11, RJ45F

které jsou uvedeny v příslušných tabulkách se jedná o heterogenní síť využívající většinu běžných přenosových médií.

2.2.2 Síťový model

Pro možnost přistoupení k návrhu vhodného řešení pro implementaci triple-play služeb je nutné podívat se na síť jako logický celek. Pokud je možné topologii sítě zobecnit na nějaký obecný model např. hvězda, strom nebo kruh, získáme základní faktor, který bude hrát důležitou roli při dalším postupu. Zkoumaná topologie je, jak už bylo uvedeno výše rozvětvený strom, který má společný centrální bod, kterým je hlavní síťový prvek, přes který tečou všechna uživatelská data. Podrobnějším zkoumáním byly určeny další vlastnosti této topologie. V každé větší geografické lokalitě, kde se strom rozvětvuje a místo slouží k připojení dalších lokalit do páteřní sítě je umístěn aktivní prvek na síťové vrstvě – směrovač. Směrovač umožňuje přeposílání paketů mezi zařízeními, které patří do logicky oddělených sítí na základě IP adres a masky podsítě. Zde jsou to zařízení v jednotlivých geograficky oddělených lokalitách, které vyžadují směrovač pro vzájemnou komunikaci. Pokud daná lokalita slouží jako uzel pro připojení více lokalit a jedno zařízení nedisponuje dostatečným

počtem rozhraní, bývá na místě také často umístěn přepínač s dostatečným počtem portů pro připojení potřebných zařízení. Na základě výše uvedeného zkoumaní byl sestaven obecný typ síťové topologie, viz. obr. 2.3. Z tohoto modelu lze vyčíst



Obr. 2.3: Obecný model zkoumané topologie

všechny typy jednotlivých uzlů:

- **Kořen** – Centrální místo, ze kterého se celý strom rozvětvuje Lokalita 1.
- **Uzel** – Místo, kdy se jedna větev stromu rozvětvuje na dvě nebo více dalších větví. Lokalita 1, 2, 3 a 4.
- **Koncový bod** – Místo, které představuje koncový uzel, větev dále nepokračuje. Koncové body představují listy stromové struktury. Na těchto bodech

jsou poté připojení pouze koncoví uživatelé. Lokalita 5.
Vzhledem k tomu, že síťová infrastruktura obsahuje v každém uzlu aktivní prvek pracující na síťové vrstvě, můžeme tyto prvky využít ke správě síťového provozu a zajištění kvality poskytovaných služeb - QoS. [16]

2.2.3 Aktivní prvky

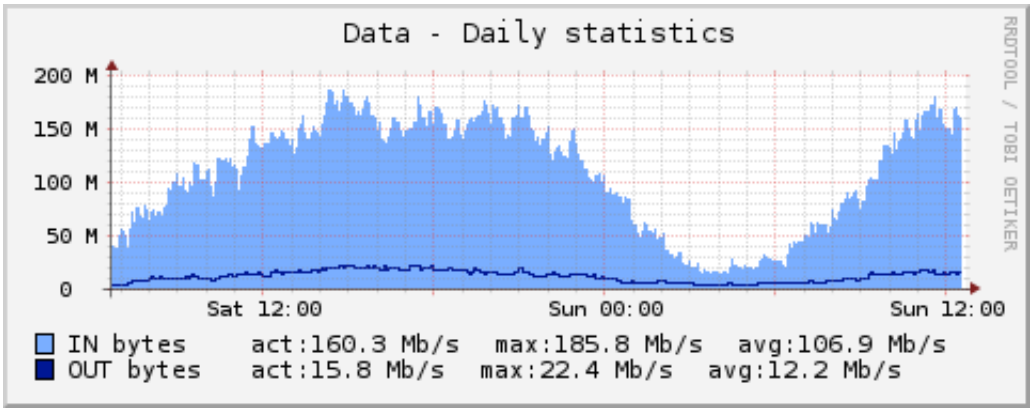
V rámci sítě jsou využívány z velké části aktivní prvky od jednoho výrobce, což považuji za výhodu pro následné plánování návrhu řešení. Poskytovatel zvolil síťové prvky od společnosti MikroTik, jedná se o zařízení, která jsou mezi regionálními poskytovateli telekomunikačních služeb velice rozšířená. Mezi důvody bezesporu patří široká nabídka zařízení pro realizaci bezdrátových spojů a také velice výhodný poměr ceny a nabízených parametrů, resp. funkcí. Zařízení od společnosti MikroTik, tzv. Routerboardy používají operační systém RouterOS, který si firma pro svoje zařízení sama vyvinula. RouterOS je založený na OS Unix. Mezi výhody RouterOS patří to, že je k dispozici také pro architekturu x86. Je tedy možné sestavit např. výkonné zařízení založené na běžných komponentách pro PC a s použitím výkonného procesoru získáváme výkonné zařízení s nízkou pořizovací cenou. Toto zařízení následně spravujeme stejně jako hardwarová zařízení firmy MikroTik. Mimo zařízení typu Routerboard jsou v síti použity také aktivní prvky od jiných výrobců, jako je např. Cisco. Seznam použitých zařízení, včetně specifikací, je uveden v tab. 2.5

Tab. 2.5: Seznam používaných aktivních síťových prvků

Typ zařízení	**Výrobce**	**Typ**	**Rozhraní Ethernet [RJ-45/SFP]**	**Operační systém**	**Procesor**	**Operační paměť**
směrovač*	MikroTik	CCR1036-12G-4S	12/4	RouterOS(x64)	36x1,2 GHz	2048 MB
směrovač	SuperMicro	5015A-EHF-D525	2/0	RouterOS	4x1,8 GHz	1024 MB
směrovač*	MikroTik	RB1100AHx2	13/0	RouterOS	2x1 GHz	2048 MB
směrovač*	MikroTik	RB1100AH	13/0	RouterOS	1 GHz	2048 MB
směrovač*	MikroTik	RB1100	13/0	RouterOS	800 MHz	512 MB
směrovač*	MikroTik	RB2011UiAS-RM	10/1	RouterOS	600 MHz	128 MB
směrovač*	MikroTik	RB2011iL-RM	10/1	RouterOS	600 MHz	64 MB
směrovač*	MikroTik	RB435G	3/0	RouterOS	680 MHz	256 MB
směrovač*	MikroTik	RB433AH	3/0	RouterOS	680 MHz	128 MB
přepínač*	MikroTik	CRS125-24G-1S-RM	24/1	RouterOS	680 MHz	128 MB
přepínač	Cisco	SG200-26	24/2	Proprietární	Nezjištěno	128 MB
* Směrovač obsahuje integrovaný hardwarový chip pro přepínaní rámců na linkové vrstvě. Lze tedy nakonfigurovat také jako přepínač.						

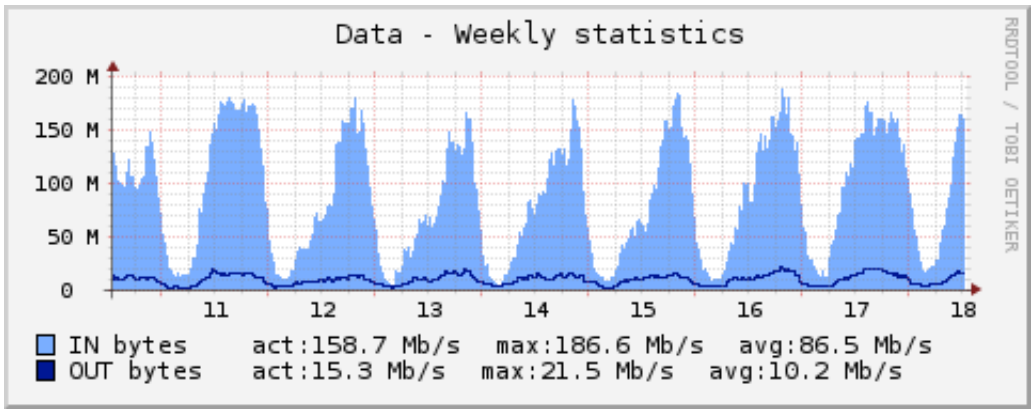
2.2.4 Vytížení síťě

V této fázi bylo zkoumáno vytížení síťové infrastruktury a to z toho důvodu, aby bylo zjištěno jaké kapacity jsou na jednotlivých spojích dostupné pro nasazení dalších služeb, které vyžadují větší objem přenesených dat. Mezi takové služby patří zejména ty, které přenášejí multimediální obsah, jako je požadovaná IPTV. Na hlavních linkách infrastruktury jsou použity mikrovlnné spoje, jejichž kapacity se pohybují v řádu několika stovek Mb/s za sekundu, viz. tab. 2.3 Všechny aktivní síťové prvky síťové infrastruktury jsou monitorovány systémem ISPadmin, viz. 2.2.6. Ze statistických dat, které jsou v systému k dispozici, je možné zjistit, jak jsou jednotlivé páteřní spoje vytížené během celého dne. Systém ISPadmin umožňuje z uložených dat vykreslení grafů pomocí nástroje RRDtool. Získané grafy slouží pro velice přehlednou analýzu přenášeného objemu dat. Grafy přenášených dat pro hlavní páteřní spoj (z kořene stromu do první lokality), který je nejvíce vytížený, jsou uvedeny na obr. 2.4 pro posledních 24 hodin a na obr. 2.5 za posledních sedm dní. Pro ověření reálné propustnosti téhož spoje byl proveden také test s využi-

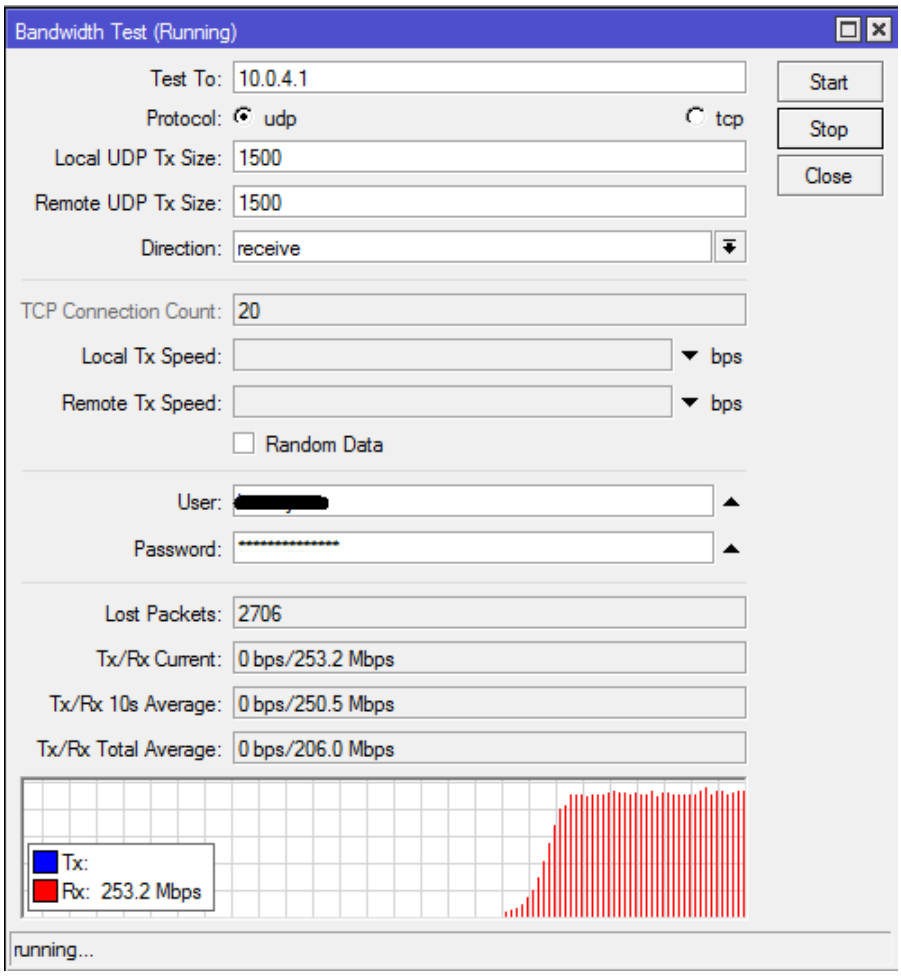


Obr. 2.4: Graf vytížení páteřního mikrovlnného spoje - 24 hodin

tím nástroje btest, který je volně k dispozici na webové stránce společnosti MikroTik: http://www.mikrotik.com/download/btest.exe. V době kolem 15. hodiny odpoledne, tedy době kdy je spoj zatížen odpolední špičkou, byl proveden test propustnosti. Výsledek tohoto testu je uveden na obr. 2.6. Dále na obr. 2.7 celkový zaznamenaný provoz na síťovém rozhraní v době testu. Z uvedených dat je patrné, že tento konkrétní datový spoj umožnuje přenášet zhruba 360 Mb/s uživatelských dat. Na základě hodnot vyčtených z grafu dlouhodobě přenášených dat, kdy se maximální hodnoty v době nejvyššího zatížení pohybují kolem 180 Mb/s, můžeme označit tuto linku za v současné době dostatečně nadimenzovanou. Podobně nadimenzovaná je většina testovaných páteřních spojů, kde je také k dispozici dostatečná kapacita pro další plánované služby. Obdobným zkoušením byly postupně otestovány všechny

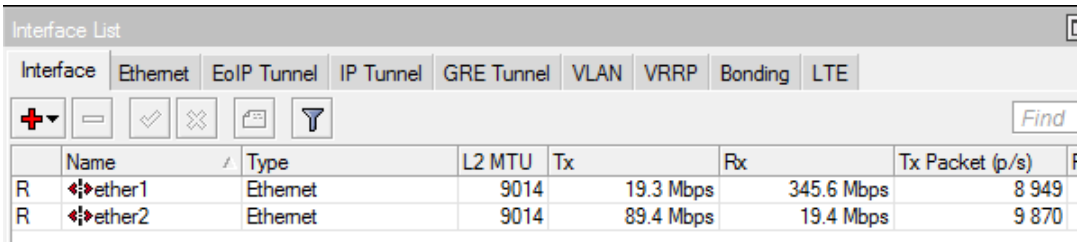


Obr. 2.5: Graf vytížení páteřního mikrovlnného spoje - 1 týden



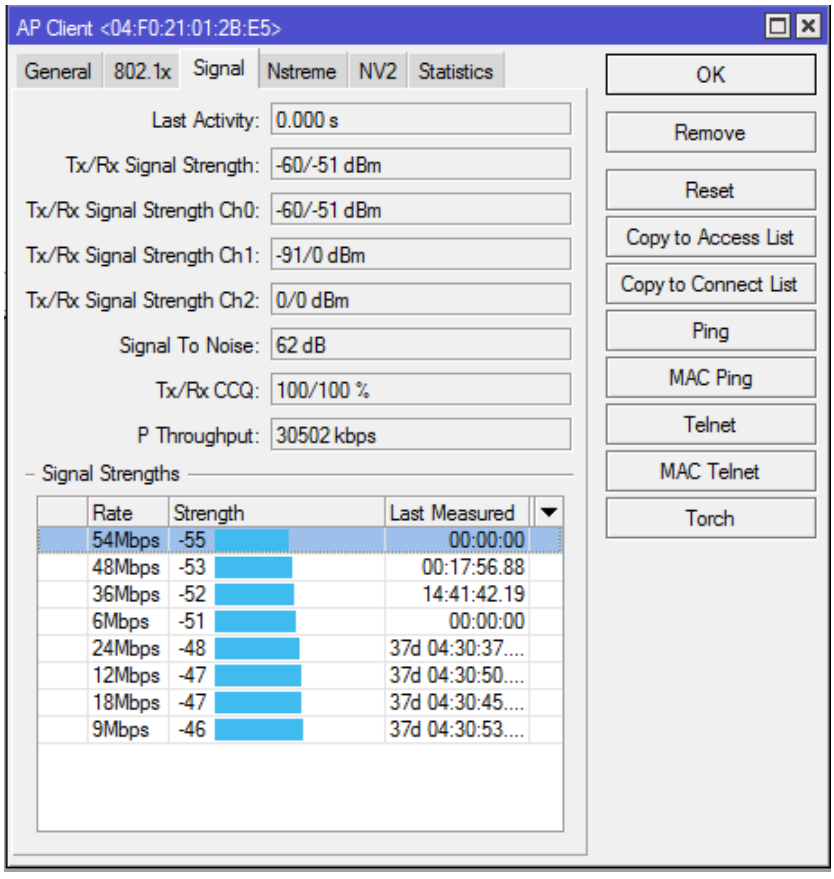
Obr. 2.6: Test propustnosti páteřního spoje

důležité lokality a byly také zjištěny místa, kde je dostupná kapacity spojů z větší části využívána již nyní. V případě požadavků na větší objem přenášených dat od kořene do některých posledních lokalit v topologii (typicky listy stromové topologie)



Obr. 2.7: Celkový provoz na síťovém rozhraní v době testu

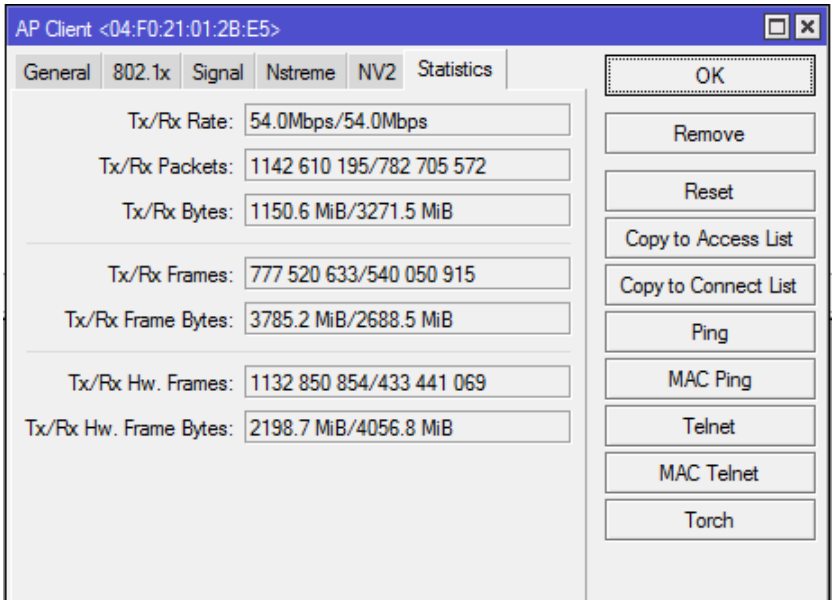
by spoje, které využívají bezdrátové technologie nemuseli již vyhovovat. Konkrétním příkladem je jedna z lokalit, která je připojena s využitím bezdrátového spoje technologií 802.11a v pásmu 5 GHz. Maximální teoretická přenosová rychlost této technologie v ideálních podmínkách je 54 Mb/s (cca 30 Mb/s pokud jde o reálná uživatelská data přenášená protokolem TCP). Úroveň signálu obou stran bezdrátového spoje je dostačující, viz. obr. 2.8. Jedna strana bezdrátového spoje indikuje



Obr. 2.8: Úroveň signálu bezdrátového spoje využívající technologii 802.11a

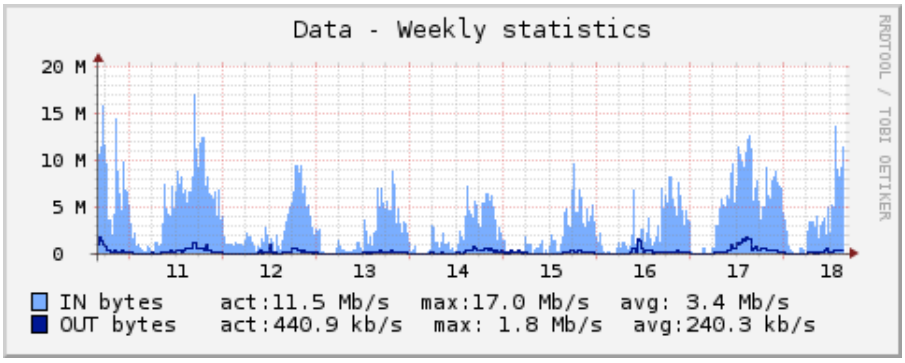
hodnotu přijímaného signálu nižší (-60 dBm) než druhá (-51 dBm). Tento rozdíl je dán typem bezdrátové karty na jednotlivých stranách přijímače a vysílače, kdy má

každá strana odlišný vysílací výkon. Lze si také všimnout ukazatele kvality připojení(CCQ) – 100 %, který určuje jak efektivně je využívána dostupná šířka pásma připojenou koncovou stanicí. Pokud spoj nefunguje tak jak by měl, z důvodu rušení nebo jiného, hodnoty bývají často mnohem nižší, i pod hranicí 50 %. Spoj poté umožňuje velmi omezenou kapacitu pro přenášená data. U zkoumaného spoje jsou hodnoty v pořádku a jak je vidět na obr. 2.9, spoj využívá nejvyššího režimu 54 Mb/s. [17] I když spoj samotný funguje v pořádku, tak na základě statických



Obr. 2.9: Automaticky zvolený režim rychlosti bezdrátového spoje

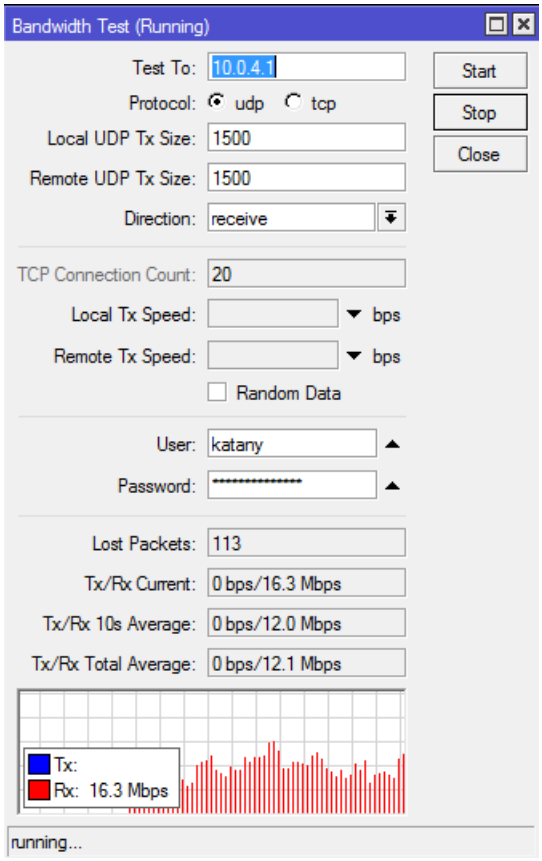
dat a z nich sestaveného grafu lze určit, že je jeho dostupná kapacita z větší části vytěžována již nyní, viz. obr. 2.10 Zde vidíme, že v době většího provozního zatí-



Obr. 2.10: Graf vytížení bezdrátového spoje – 1 týden

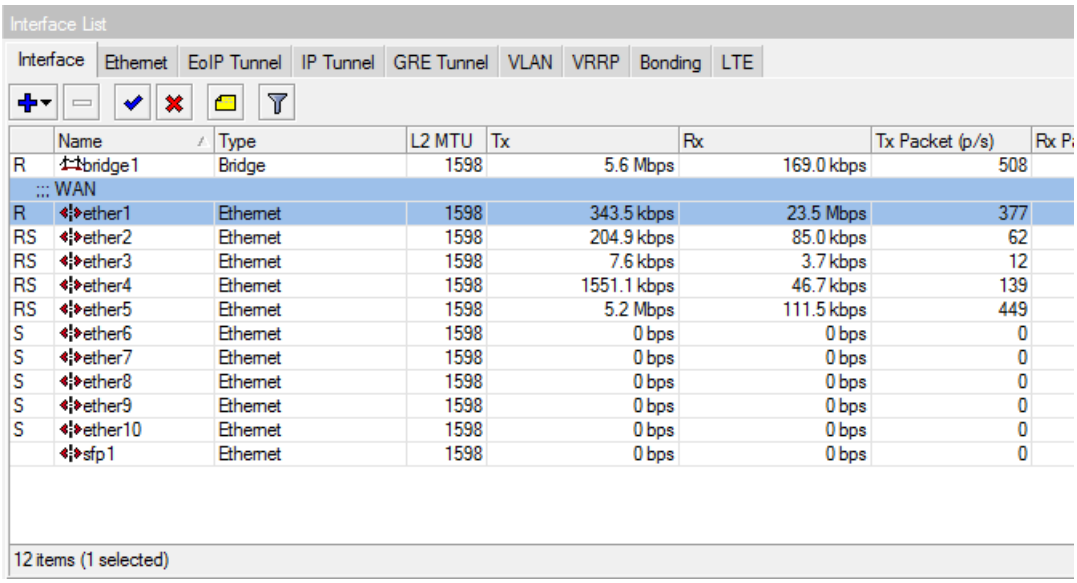
žení je na daném spoji využíváno kolem 15 Mb/s dostupné kapacity. To znamená, že ve špičce a době většího provozního zatížení má tato linka rezervu maximálně

10-15 Mb/s. Tento odhad je ověřen měřením dostupné šířky pásma mezi hlavním směrovačem (kořen stromu) a touto lokalitou (list stromu). Získané výsledky uvedené na obr. 2.11 a obr. 2.12 potvrzují správnost odhadu. Byla naměřena dostupná šířka pásma maximálně 16 Mb/s, která v průběhu testu navíc značně kolísala z důvodu vytížení spoje uživateli. Z provedeného zkoumání vytížení síťové infrastruktury



Obr. 2.11: Test propustnosti bezdrátového spoje

je důležité zmínit, že byly nalezeny důležité faktory pro následný návrh řešení pro implementaci triple-play služeb. Tímto faktorem je omezená dostupná šířka pásma v některých částech topologie.



Obr. 2.12: Celkový objem přenášených bezdrátovým spojem, který je připojen k rozhraní „ether1“

2.2.5 Správa uživatelů

V předchozích částech byla popsána síťová infrastruktura a analyzován síťový provoz. Tato část je zaměřena na analýzu způsobu správy sítě z hlediska evidence uživatelských služeb. Každému uživateli je poskytovaná služba, která je limitována:

1. Maximální rychlostí přenášených dat směrem k uživateli – **download**.
2. Maximální rychlostí přenášených dat směrem od uživatele – **upload**.

Kompletní evidence všech uživatelů a poskytovaných služeb je řešena pomocí systému ISPadmin.

2.2.6 ISPadmin

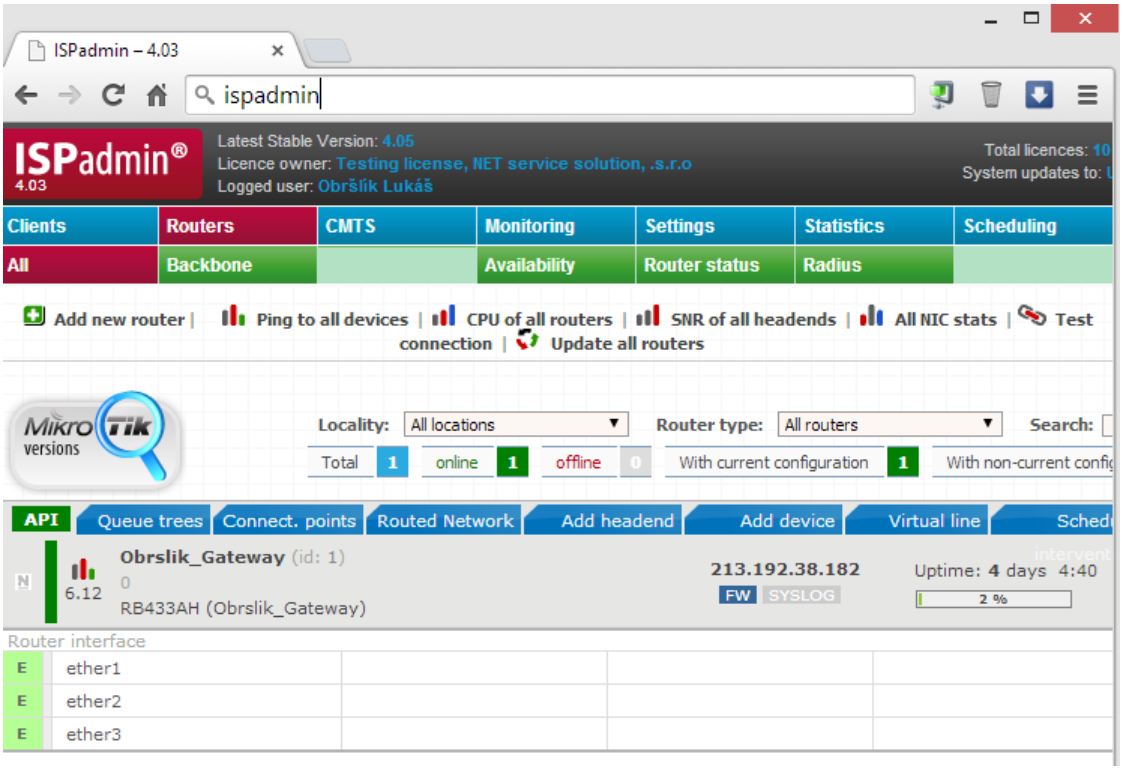
ISPadmin je administrační a informační systém vyvíjený českou firmou NET service solution od roku 2003. Je určený a přizpůsobený primárně pro společnosti a organizace poskytující telekomunikační služby. Dle tvrzení autora se jedná o nejrozšířenějších systému svého druhu nejen v České Republice ale i v zahraničí. Z hlediska velikosti cílových zákazníků je systém určen pro menší ale i rozsáhlejší sítě s větším počtem klientů. Hlavní funkce systému ISPadmin:

- Management zařízení v síti,
- Monitoring sítě,
- Podrobné statistiky sítě,
- Plánování činnosti servisních techniků,
- Klientský portál,

- Evidence klientů,
- Správa tarifů a služeb,
- Zálohování systému,
- Samostatné moduly(NETflow, Radius),
- Fakturace služeb.

Na obr. 2.13 zachycené webové rozhraní systému po přihlášení. Rozhraní obsahuje několik důležitých částí:

- **Clients** – Část pro správu klientů, jejich kontaktních údajů a přidělených služeb a nastavení parametrů fakturace.
- **Routers** – Zde je možné evidovat a monitorovat stav všechny zařízení v síti.
- **Monitoring** – Sledování činnosti modulu Nagios, který sleduje stav aktivních prvků v sítí.
- **Settings** – Nastavení hlavních funkcí systému ISPadmin.
- **Statistics** – Statistika využití systémových prostředků serveru, na kterém je systém nainstalován a také např. stav využití IP adres z přidělených adresních rozsahů. [18]



Obr. 2.13: Webové rozhraní systému ISPadmin

Veškerá data, která systém eviduje jsou spravována pomocí databáze MySQL. Systém používá vlastní databázi s názvem „ispadmin“, ve které jsou uloženy používané

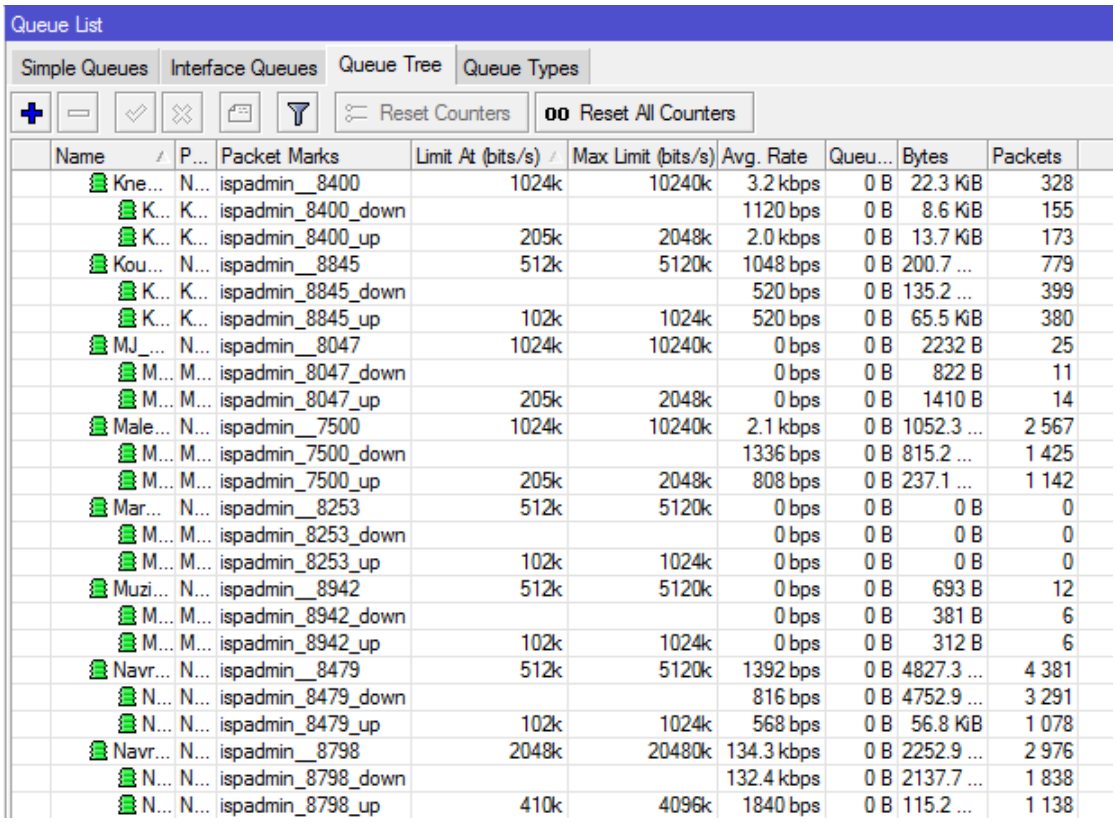
databázové tabulky. Z pohledu uživatelů, síťových prostředků a poskytovaných služeb jsou důležité tyto:

1. **cable_routers** – Tabulka, ve které jsou evidovány všechny aktivní prvky v síti. Každý záznam (aktivní prvek) je veden pod unikátním ID a dále je mu přiřazena používaná IP adresa, přihlašovací údaje pro komunikaci a vyčítání dat z daného zařízení.
2. **cable_users** – Údaje uživatelů, kde je každý odlišen svým identifikátorem, uvedeným jménem a jsou mu přiřazeny požadované údaje.
3. **cable_network** – Tabulka, která uchovává údaje pro všechny používané adresní rozsahy.
4. **sl_internet** – Zde jsou uloženy údaje o uživatelům poskytovaných službách. Každá služba je jako v ostatních tabulkách opět odlišena unikatním identifikátorem, který má přiřazeno jméno uživatele, IP adresu uživatele a také parametry služby, jako je maximální příchozí a odchozí rychlost.

V seznamu uvedené tabulky systém používá při komunikaci s požadovanými síťovými prvky. Systém umí komunikovat prostřednictvím rozhraní API, protokolu SSH a také vyčítat data využitím SNMP. Na zvolených aktivních prvcích umožňuje nakonfigurovat tyto parametry:

- **Firewall** – Nastavení pravidel pro firewall. Komunikace je povolena pouze pro IP adresy, ze kterých komunikují připojení uživatelé. Zbytek IP adres z přidělených adresních rozsahů je zakázán.
- **Mangle** – V části mangle je provoz procházející daným zařízením podle systémem definovaných pravidel odlišen na základě zdrojové a cílové adresy v každém paketu a poté označen. Takto označenému paketu je v rámci jednoho směrovače možné přidělit požadovanou prioritu ve frontě zpracování.
- **Queues** – Fronty (queues) systém používá pro sestavení tzv. stromu (Queue Tree), kde jsou uživatelům pro jednotlivé služby na základě hodnot v databázi nastavena omezení, viz. obr. 2.14. Jako příklad uvedeme situaci, kdy je poskytována služba s omezením rychlosti přenášených dat směrem k uživateli na 10 Mb/s a směrem od uživatele na 2 Mb/s. V tomto případě je aplikováno celkové omezení na přenášená data a pokud uživatel odesílá data rychlostí 2 Mb/s, tak v opačném směru, tedy k uživateli je povolena maximální rychlost přenášených dat 8 Mb/s. Pokud žádná data neodesílá, může využít 10 Mb/s.

Tyto parametry umožňuje systém ISPadmin nastavit pouze na zařízeních, které využívají operační systém **RouterOS**.



Name	P...	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queu...	Bytes	Packets
Kne...	N...	ispadmin__8400	1024k	10240k	3.2 kbps	0 B	22.3 KiB	328
K...	K...	ispadmin_8400_down			1120 bps	0 B	8.6 KiB	155
K...	K...	ispadmin_8400_up	205k	2048k	2.0 kbps	0 B	13.7 KiB	173
Kou...	N...	ispadmin__8845	512k	5120k	1048 bps	0 B	200.7 ...	779
K...	K...	ispadmin_8845_down			520 bps	0 B	135.2 ...	399
K...	K...	ispadmin_8845_up	102k	1024k	520 bps	0 B	65.5 KiB	380
MJ_...	N...	ispadmin__8047	1024k	10240k	0 bps	0 B	2232 B	25
M...	M...	ispadmin_8047_down			0 bps	0 B	822 B	11
M...	M...	ispadmin_8047_up	205k	2048k	0 bps	0 B	1410 B	14
Male...	N...	ispadmin__7500	1024k	10240k	2.1 kbps	0 B	1052.3 ...	2 567
M...	M...	ispadmin_7500_down			1336 bps	0 B	815.2 ...	1 425
M...	M...	ispadmin_7500_up	205k	2048k	808 bps	0 B	237.1 ...	1 142
Mar...	N...	ispadmin__8253	512k	5120k	0 bps	0 B	0 B	0
M...	M...	ispadmin_8253_down			0 bps	0 B	0 B	0
M...	M...	ispadmin_8253_up	102k	1024k	0 bps	0 B	0 B	0
Muzi...	N...	ispadmin__8942	512k	5120k	0 bps	0 B	693 B	12
M...	M...	ispadmin_8942_down			0 bps	0 B	381 B	6
M...	M...	ispadmin_8942_up	102k	1024k	0 bps	0 B	312 B	6
Navr...	N...	ispadmin__8479	512k	5120k	1392 bps	0 B	4827.3 ...	4 381
N...	N...	ispadmin_8479_down			816 bps	0 B	4752.9 ...	3 291
N...	N...	ispadmin_8479_up	102k	1024k	568 bps	0 B	56.8 KiB	1 078
Navr...	N...	ispadmin__8798	2048k	20480k	134.3 kbps	0 B	2252.9 ...	2 976
N...	N...	ispadmin_8798_down			132.4 kbps	0 B	2137.7 ...	1 838
N...	N...	ispadmin_8798_up	410k	4096k	1840 bps	0 B	115.2 ...	1 138

Obr. 2.14: ISPadmin – Omezení příchozí a odchozí rychlosti uživatelů.

2.3 Návrh řešení

V části návrh řešení je popsána příprava navrhovaného technické řešení pro implementaci požadovaných služeb na základě vyhodnocení všech faktorů získaných v předchozích částech.

2.3.1 IPTV

Jeden z hlavních požadavků je implementace doplňkových služeb, jako je IPTV. Vzhledem k tomu, že heterogenní infrastruktura poskytuje omezené možnosti dostupné šířky pásma, byly pro ověření možnosti implementace vybrány tyto tři služby:

- **sledovanitv.cz**,
- **UPC Business – IPTV**,
- **G.TV**.

Pro možnost otestovat tyto služby byli osloveni jednotliví poskytovatelé služeb, společnost SychrovNET, s.r.o (sledovanitv.cz), UPC Česká republika s.r.o. (UPC Business – IPTV) a Grape SC, a.s. (G.TV). Zástupci společností byli ochotni poskytnout možnost bezplatně otestovat jejich služby a v relativně krátké době zaslali i potřebný hardware, viz. obr. A.1
Služby byly otestovány na síťové infrastruktuře. Byly posouzeny nároky na požadovanou šířku pásma a ověřeno, zda infrastruktura nabízí dostatečné parametry pro zajištění bezproblémového poskytování.

2.3.2 sledovanitv.cz

Služba poskytovaná společností SychrovNET nabízí v současné době více než 30 televizních stanic, kompletní seznam je uveden v tab. 2.6. Mezi základní funkce patří:

- **Timeshift** – Časový posun ve vysílání. V tomto případě je umožněno přehrávat obsah 30 hodin zpětně.
- **Pause** – Pozastavení vysílání, limitem je 60 minut.
- **EPG** – Elektronický programový průvodce, který poskytuje informace o televizních pořadech.

Služba využívá transportního protokolu TCP. Televizní přenos je kódován kodekem H.264 a unicastový datový přenos se pohybuje mezi 1-2 Mb/s, viz. analýza využité kapacity šířky pásma pomocí zařízení s RouterOS obr. A.3, kde můžeme vidět realizovaný přenos dat v obou směrech (protokol TCP), kdy mimo přenos dat ze serveru poskytovatele služby probíhá i potvrzování přijatých dat (cca 50 kb/s). Nasazení služby v síti nevyžaduje zásah do používaného hardwaru nebo jeho konfigurace. Použití služby na koncovém zařízení je umožněno několika způsoby:

Tab. 2.6: Seznam TV stanic poskytovaných službou sledovanitv.cz

sledovanitv.cz – seznam TV stanic		
ČT1	Óčko Gold	TV Noe
ČT2	Šlágr TV	Óčko TA3
ČT24	musiq1	Prima Love
ČT Sport	FUN1	Prima ZOOM
ČT art	Polsat Sport	Prima Joj
ČT :D	Polsat	Prima
Nova	ORF eins	WAU
Nova Cinema	TV Barrandov	Retro
Filmbox	regionalnitelevize.cz	JOJ
Fanda TV	France 24	JOJ Plus
Smíchov	Jednotka	Doma
Relax	Dvojka	Dajto
Rebel	Markíza	

- **Webový prohlížeč** – Televizní vysílání je možné přijímat přímo na koncovém zařízení uživatele v libovolném webovém prohlížeči, viz. obr. A.2.
- **Aplikace** – Další možností je poskytovatelem služby nabízená aplikace pro platformu OS Android, Samsung Smart TV nebo využití softwaru pro zpracování video proudu (např. VLC player).
- **Set-top box** – Pokud je požadavkem zprovoznění televizního služby na televizoru uživatele, je k dispozici i set-top box. Jedná se o zařízení navržené přímo pro službu sledovanitv.cz, využívá OS Android. Set-top box disponuje rozhraními HDMI a RCA pro připojení digitálního i analogového zobrazovacího zařízení. K datové síti je možné připojit prostřednictvím bezdrátového rozhraní a kabelu (RJ-45).

2.3.3 UPC Business – IPTV

Tato služba je určena partnerům společnosti UPC. Služba byla představena v nedávné době a je pouze ve fázi testování. Seznam poskytovaných TV stanic je uveden v tab. 2.7. Nabízí stejně jako služba sledovanitv.cz příjem digitálního vysílání prostřednictvím IP sítě. Využívá unicastového přenosu dat pomocí transportního protokolu TCP. Jediným možným způsobem využití služby na straně uživatele je platforma Viera Cast vyvinutá společností Panasonic. Použít je tedy možné pouze moderní televizor vyrobený firmou Panasonic, který tuto platformu podporuje nebo

Tab. 2.7: Seznam TV stanic poskytovaných službou UPC Business – IPTV

UPC Business – IPTV – seznam TV stanic		
ČT1	Prima Love	Cinemax
ČT2	TV Barrandov	Cinemax 2
ČT24	Slovak Sport.TV2	CS Film
ČT Sport	Sport 1	Discovery Channel
ČT art	Eurosport	Disney Channel
ČT :D	Eurosport 2	Film+
Nova	Extreme Sports	Filmbox
Nova Cinema	Markíza	HBO2
Fanda	TV JOJ	HBO Comedy
Prima	Animal Planet	History Channel
Prima Family	AXN	JimJam
MGM	Minimax	National Geographic
Viasat History	Spektrum	Nickelodeon

multimediální přehrávače (např. Blu-ray) téhož výrobce. Toto řešení považuji za značně omezující. Společnost UPC zaslala k otestování služby Blu-ray přehrávač Panasonic DMP-BDT120. Součástí softwaru přehrávače je integrovaná platforma Viera Cast, která umožňuje instalovat dodatečné aplikace. Jednou z předinstalovaných aplikací je právě UPC.TV pro příjem digitálního televizního vysílání prostřednictvím IP sítě. Po zapnutí zařízení je nutné aplikaci nejprve spustit ze speciální nabídky a opakovat tento postup při každém spuštění považuji také za příliš komplikované. Pro zjištění náročnosti na objem přenášených dat byl proveden test pomocí nástroje ntop, který slouží pro zjištění podrobných informací o přenášeném síťovém provozu. Nástroj je k dispozici na přiloženém CD včetně návodu na instalaci pro platformu UNIX, kde byl testován na distribuci Debian. Nástroj slouží pro sběr a zpracování statistických dat. Data mohou být analyzována přímo na rozhraní systému, kde je ntop nainstalován nebo lze využít vzdálený sběr dat. Pro analyzování přenášených dat službou UPC Business – IPTV byl zvolen vzdálený sběr dat a využito zařízení MikroTik RB751G s nakonfigurovanou funkcí Traffic Flow, která obstarává periodické zasílání informací o přenášeném provozu na předem nadefinovaný port serveru s instalovaným nástrojem ntop. Výsledky testu jsou uvedeny na obr. A.4. Služba byla také testována nepřetržitě po dobu 18 hodin a na obr. A.5 je sestavena přehledná tabulka přenesených dat v jednotlivých hodinách. Ze získaných výsledků je patrné, že pokud služba běží nepřetržitě, za hodinu přenese zhruba 1 GB dat s odchylkou ±2 %.

Tab. 2.8: Seznam TV stanic poskytovaných službou G.TV

G.TV – seznam TV stanic		
Active TV	FashionBOX HD	ORF 1,2
Animal Planet	Fightbox HD	Playboy
Animax	Film+	Polsat
ARD	FilmBox Extra	Polsat Sport News
Arte	Filmbox Family	Prima(HD)
Astra 3D demo	Filmbox Plus	Prima Cool(HD)
AXN	FilmBox(HD)	Prima Love
AXN Black, White	Fine Living Network	Prima ZOOM
FANDA	Fish and hunting	R1
BabyTV	France24	Rádio Proglas
BBC Radio	FUN1	Rebel
BBC World	Golf Channel HD	regionalnitelevize.cz
Brazzers TV Europe	HBO(HD)	Relax
CBS Reality	HBO Comedy	RT Doc HD
Cinemax	HBO GO	Russia Today(HD)
Cinemax II	HBO II	SkyNews
CS Film, Mini	HD+	SMÍCHOV
Óčko	History Channel	Spektrum HD
ČT :D	JimJam	Sport 1,2,5
ČT Art	JOJ	STV I,II
ČT1(HD)	KiKA	Šlágr TV(HD)
ČT1 JM/SM	Kino CS	TA3
ČT2(HD)	Kino Svět	Telka
ČT24	Markíza	Travel Channel
ČT4 Sport(HD)	Metropol TV	TV Barrandov
Dajto	MGM	TV Doma
Deluxe Music	Minimax	TV FOOOR*
Discovery	MTV Europe	TV Harmonie
Disney Channel	Muzika CS	TV Lux
DocuBOX HD	Nat Geo Wild	TV NOE
Doku CS	National Geographic	TV Puls
Eurosport	Nova(HD)	TV 4,6,8
Eurosport 2	Nova Cinema	TVN (7)
Extreme Sport	Nova Sport(HD)	TVP 1,2
Fajn Rock TV	ZDF (neo,kultur)	

2.3.4 G.TV

Poslední testovanou službou je IPTV televize poskytovaná společnosti Grape SC, a.s. Tato společnost nabízí nejširší nabídku televizních stanic ze všech testovaných. Primárně je služba určená pro využití v metropolitních optických síti. Pro přenos dat mezi serverem a uživatelem je využit přenos dat typu multicast a datový proud není komprimován jako u předchozích služeb. To obnáší určité výhody a nevýhody. Mezi výhody služby patří konstantní bitový tok a vysoká kvalita obrazu. Nevýhody jsou velmi vysoké nároky na šířku pásmu a chybovost při přenosu, nutnost zásahu do síťové infrastruktury a příprava na přenášení několika set Mb/s multimediálního datového proudu. Služba poskytuje také další funkce, jako je pozastavení vysílání, posun zpět v čase vysílání(u služby G.TV až o 48 hodin). Služba byla vyzkoušena sestavením tunelu přenášejícího Ethernetové rámce mezi zařízením poskytovatele a přijímacím zařízením(EoIP), do kterého byl připojen set-top box Motorola VIP1003. Naměřená vyžadovaná šířka pásma je zachycena na obr. A.6 a obr. A.7. Na prvním zachyceném grafu vidíme využití zhruba 17 Mb/s, po celou dobu testování, kdy byl spuštěn přenos stanice HBO HD, která je ve vysokém rozlišení náročná na požadovanou šířku pásma. Druhý graf ukazuje využitou šířku pásma při spuštění stanice Nova, kde jsou nároky mnohem nižší (3 – 7 Mb/s). Výsledky tohoto měření ukazují, že pro použití na heterogenní síti je tato služba z hlediska požadované šířky pásma nevhodná. Nasazení by vyžadovalo kompresi datového toku při vstupu do síťové infrastruktury. Komprese by vyžadovala další dedikované zařízení, které by bylo nutné spravovat.

Výsledky testování IPTV služeb jsou shrnuty v tab. 2.9. Na základě výsledků získaných testování služeb lze říci, že vhodné služby pro implementaci jsou:

- **sledovanitv.cz**,
- **UPC Business – IPTV**.

Tyto služby vyžadují nižšími nároky na parametry síťové infrastruktury a je možné je reálně poskytovat. Služba sledovanitv.cz nabízí nějvětší uživatelský komfort, lze ji používat na kterémkoli koncovém zařízení prostřednictvím webového přihlížeče a také můžeme použít set-top box pro připojení k televizoru. Naopak služba G.TV není vhodná na použití v heterogenní síti z důvodu vysokých nároků na šířku pásma a nízkou chybovost. Tyto parametry nelze zaručit z důvodu použití bezdrátových spojů ve volně přístupném pásmu 5 GHz, kde je nutné počítat s možností rušení a zhoršení přenosových parametrů.

Tab. 2.9: Celkové porovnání IPTV služeb

Služba	**sledovanitv.cz**
Výhody	Nízké nároky na parametry síťové infrastruktury (šířka pásma, chybovost). Podpora Webového rozhraní. Kompaktní set-top box. Není nutný fyzický zásah do sítě. Mnoho doplňkových služeb.
Nevýhody	Průměrná kvalita obrazu.
Služba	**UPC Business - IPTV**
Výhody	Nízké nároky na parametry síťové infrastruktury (šířka pásma, chybovost). Není nutný fyzický zásah do sítě.
Nevýhody	Nutná platforma Viera Cast. Nižší kvalita obrazu. Ovládání aplikace na koncovém zařízení.
Služba	**G.TV**
Výhody	Vysoká kvalita obrazu. Rozsáhlá programová nabídka.
Nevýhody	Nároky na parametry síťové infrastruktury. Nutný fyzický zásah do sítě. Investice do nákupu nových zařízení.

2.3.5 Kvalita služeb

Nasazením multimediálních služeb, jako je např. IPTV vzroste postupem času objem přenášených dat. Abychom zajistili funkčnost služeb i v místech, kde je omezená šířka dostupného pásma, bude nutné aplikovat zajištění kvality služeb, tzv „QoS“. V rámci sítě, kde požadujeme zajištění kvality služeb jsou využívané zejména aktivní prvky MikroTik s operačním systémem RouterOS.

2.3.6 QoS v RouterOS

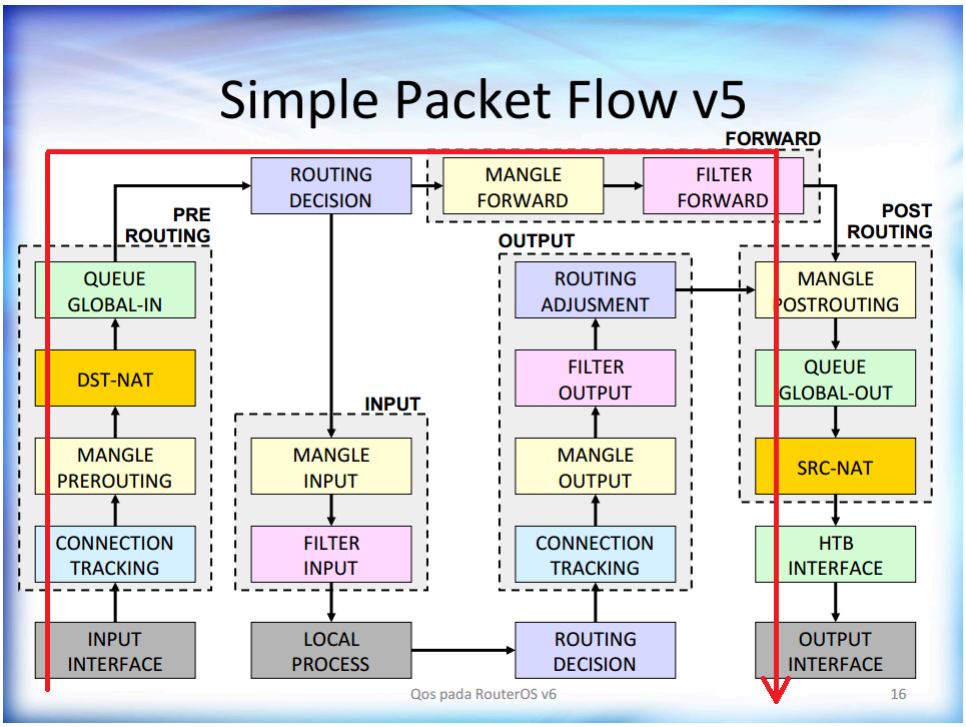
RouterOS nabízí široké spektrum možností pro zajištění kvality služeb. Základním principem pro zajištění kvality služeb lze popsat ve dvou částech:

- Mangle – V této části je veškerý provoz, který prochází daným zařízením rozlišen na základě nadefinovaných pravidel do kategorií. Jednotlivým paketům v každé kategorii je přiřazena značka, tzv. „packet mark“. Jakékoli značení

neprobíhá přímo do daného paketu, ale do interní databáze, která je k dispozici pouze v rámci konkrétního směrovače.

- Queue Tree – Pokud máme provoz rozlišen můžeme poté zacházet s každou nadefinovanou kategorií individuálně. Kategoriím můžeme přidadit priority a také nastavit maximální využitou šířku pásma apod. [19]

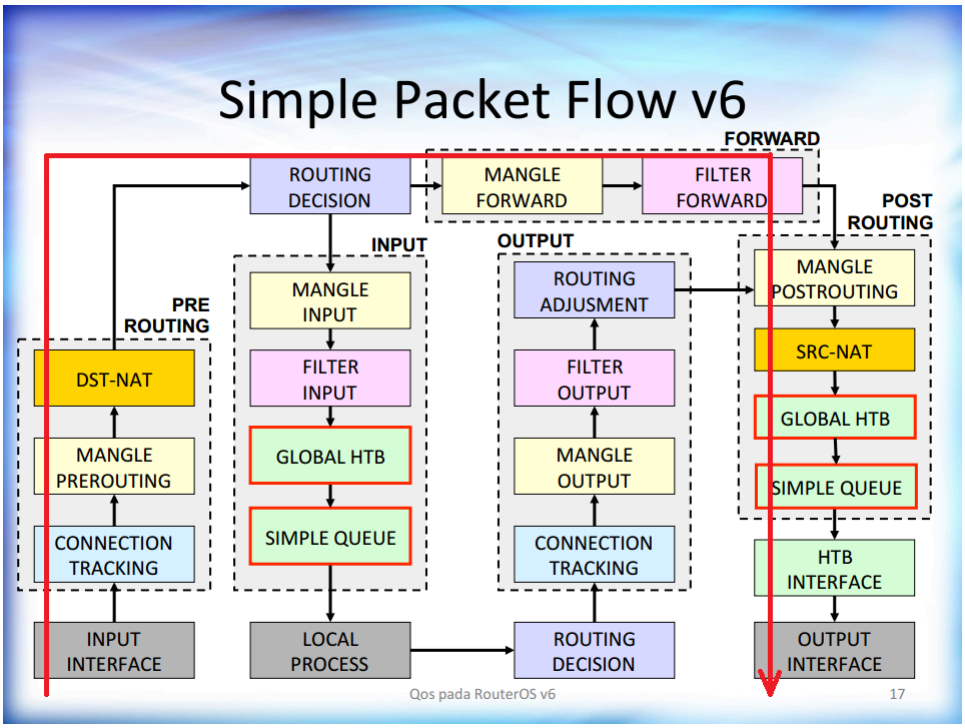
Do verze systému 5.X byl síťový provoz zpracováván, jak je uvedeno na obr. 2.15. Červená šipka znázorňuje zpracování paketu, který prochází směrovačem. Do verze 5.X bylo možné v části prerouting provést značkování (Mangle Prerouting) a poté přímo aplikovat požadovaná omezení (Queue Global-in) na jednotlivé třídy provozu. Stejný proces mohl následovat ještě jednou v části postrouting (Mangle Postrouting, Queue Global-out). Tímto způsobem bylo reálně možné rozlišit provoz podle jednotlivých tříd a na ty aplikovat první omezení v části prerouting a poté v části postrouting provést přeznačkování a rozlišit provoz konkrétních uživatelů dle IP adres a omezit kapacitu přenášených dat dle přidělených tarifů. Od verze RouterOS v6.0



Obr. 2.15: Zpracování síťového provozu – RouterOS v5.X a starší (převzato z [20])

došlo ke změně zpracovávání provozu. Metoda zpracování je znázorněna na obr. 2.16. Nyní je k dispozici v rámci jednoho směrovače pouze jedna globální fronta pro zpracování provozu (Global HTB). Můžeme tedy pouze jednou rozdělit provoz podle nadefinovaných pravidel a poté jednotlivým třídám provozu přidělit priority a aplikovat omezení maximální kapacity přenášených dat. Pokud potřebujeme garantovat určitou kvalitu služeb, jsme nuceni využít značkování (mangle) a globální frontu

(Global HTB) pro rozlišení jednotlivých služeb a přidělení požadovaných priorit. Pro omezení přenášených dat je nyní k dispozici speciální blok Simple Queue, který je navržen přímo pro omezení využité šířky pásma koncovými uživateli. Tento blok neumí rozeznávat označkované pakety, ale pouze IP adresy v hlavičce. Jeho výhodou je několikanásobně efektivnější zpracování oproti předchozímu způsobu(Mangle, Queue Tree) a tedy výrazně vyšší propustnost.



Obr. 2.16: Zpracování síťového provozu – RouterOS v6.0 a novější (převzato z [20])

V současné době v síti systém ISPadmin využívá většinu zařízení s operačním systémem RouterOS pro limitování uživatelských rychlostí, tzv. „shaping“. K samotnému omezení uživatelem využité šířky pásma využívá značkování paketů a poté aplikuje omezení na základě přidělených tarifů. Toto řešení znemožňuje aplikování kvality poskytovaných služeb pomocí RouterOS ve verzích RouterOS 6.X a novějších. Tento problém je možné vyřešit omezováním rychlostí uživatelů pomocí bloku Simple Queue a poté využít uvolněnou frontu Global HTB pro garantování požadovaných parametrů nadefinovaným službám, jak je popsáno v 2.4. [21]

2.4 Realizace řešení

Část realizace řešení obsahuje popis způsobu, jakým byl navržen komplexní systém pro zajištění kvality služeb v reálné heterogenní sítí tak, aby byla zajištěna možnost poskytovat triple-play služby. Při návrhu bylo zváženo několik faktorů, které jsou pro tuto konkrétní infrastrukturu klíčové:

- **Topologie** – Důležitým faktorem je uvažovaná topologie sítě pro implementaci triple-play služeb. Topologii, resp. struktuře zapojení aktivních šíťových prvků bylo nutné přizpůsobit návrh z důvodu co nejjednodušího nasazení.
- **ISPadmin** – Při analýze síťové infrastruktury bylo zjištěno, že systém ISPadmin nevyužívá možnosti aktivních prvků v síti efektivně. Pokud požadujeme zajistit kvalitu služeb na síti, kde jsou využívány jako směrovače zařízení s RouterOS, bylo nutné navrhnout nový způsob pro omezení využité šířky pásma jednotlivými uživateli a efektivněji tak využít síťové prvky.
- **Poskytované služby** – Pokud implementujeme kvalitu služeb, je vhodným postupem zjistit konkrétní používané služby v dané síti. Poté lze vytvořit technické řešení, které těmto službám přiřadí priority a upřednostní je naopak před službami, které natolik kritické nejsou.
- **Automatizace** – Z důvodu velké počtu uživatelů sítě (řádově několik tisíc) je nutné navrhnout řešení automatizované tak, aby systém automaticky změnil parametry pro kvalitu služeb pokud dojde ke změně tarifu uživatele.
- **Škálovatelnost** – Jedná se o jednu z žádoucích vlastností, které umožní navrhnutému řešení v budoucnu rozšiřitelnost a možnost přizpůsobit se změnám v síti.

2.4.1 Využití jazyka Perl

Po zvážení všech uvedených fakturů bylo přistoupeno k vytvoření skriptu v jazyce Perl pro zajištění kvality služeb na směrovačích v síti. Systém ISPadmin používá sadu skriptů právě v jazyce Perl pro komunikaci s jednotlivými zařízeními v síti. Použití stejného jazyka považuji za klíčové pro možnost do budoucna vytvořené řešení do systému ISPadmin integrovat v co možná nejvyšší možné míře. Skripty, který ISPadmin využívá jsou autory zašifrované a tak je nutné vytvořit od základu nový. Nově navržené řešení nahradí komunikaci se síťovými zařízeními a požadovaná je tato funkcionalita:

1. Připojit se na daný směrovač.
2. Zjistit jaké služby jsou na směrovači poskytované.
3. Povolit komunikaci pouze uživatelům evidovaným v systému a ostatním ji zakázat.

4. Nastavit limit pro omezení využité šířky pásma jednotlivými uživateli.
5. Nakonfigurovat na směrovači pravidla pro rozlišení síťového provozu.
6. Jednotlivé služby prioritizovat podle předem nadefinovaných pravidel.

Body 2.– 4. jsou implementovány z důvody kompatibility se systémem pro správu uživatelů (ISPadmin), který je v sití využíván.

2.4.2 Skript

Postupným vývojem byl vytvořen skript, který automaticky splní požadované úkoly. Využívá pro komunikaci se síťovými zařízeními rozhraní API a data, která jsou uložena v databázi MySQL. Nijak se tedy nemění způsob správy uživatelů a je možné je pohodlně ukládat a modifikovat původním způsobem pomocí systému ISPadmin. Pro vývoj skriptu a postupné testování byl nainstalován vyhrazený server, aby mohlo probíhat testování odděleně a nebylo zasahováno do reálných dat v databázi. Samotný skript je rozdělen na jednotlivé části. Řetězec na prvním řádku představuje cestu k interpretu, pro který je skript určen. Parametr **-w** aktivuje případná varování při kompilaci skriptu. Dále sdělímu skriptu používané moduly a externí knihovny parametrem **use**. V tomto případě používáme modul pro komunikaci s databází (DBI) a API klienta (Mtik), pro komunikaci s zařízením využívajícím RouterOS, který je dostupný na webové stránce http://http://wiki.mikrotik.com/wiki/API. Moduly **RouterOSFirewallMangle** a **RouterOSFwAddressList** obsahují externí vytvořené funkce, které jsou z důvodu lepší přehlednosti umístěné do zvláštního souboru pro moduly jazyka Perl s koncovkou **.pm**. Poslední řádek v první části zdrojového kódu 2.1 uloží do proměnné **routerid** identifikátor routeru a to je také jediný parametr, který skriptu předáme při spuštění, všechny ostatní potřebné údaje si zjistí automaticky z databáze.[22]

```
1 #!/usr/bin/perl -w
2 use DBI;
3 use Mtik;
4 use RouterOSFirewallMangle;
5 use RouterOSFwAddressList;
6
7 my $routerid=$ARGV[0];
```

Zdrojový kód 2.1: Perl – Definice základních parametrů skriptu

Zdrojový kód 2.2 využívá funkce modulu DBI pro získání požadovaný dat z databáze. Nejprve nadefinujeme přístupové údaje do databáze a také do proměnné **host** uvedeme adresu, kam se skript k databázi připojí, v našem případě localhost. Dále do proměnných **query** připravíme dotazy pro databázi, která na základě těchto údajů zašle požadovanou odpověď. Jako příklad je zde uvedeno zpracování dotazu

query_rtrid a **query_rtruserserv**. Dotaz query je po připojení k databázi příkazem **DBI->connect** zpracován příkazy **prepare** a poté **execute**, v případě že dotaz není správně vykonán, skript se ukončí příkazem **die**, protože bez potřebných dat nelze dále pokračovat. V případě, že je dotaz databází zodpovězen, uložíme z tabulky hodnoty z indexem 1 (ip adresa routeru) a 2 (nadefinovaný popis směrovače v databázi). Poté se vykoná i druhý dotaz, kdy získáme obdobným způsobem z další tabulky údaje o službě klienta:

- **userid** – Jedinečné ID uživatele,
- **usernames** – Jméno uživatele,
- **ipadresy** – IP adresa služby,
- **speed_down** – Limit pro přenos dat směrem k uživateli (download),
- **speed_up** – Limit pro přenos dat směrem od uživatele (upload).

Vzhledem k tomu, že na daném směrovači je většinou více, než jeden uživatel, konkrétní hodnoty jsou funkcí while načteny do polí, aby je bylo možné dále zpracovat. Po vykonání všech dotazů je komunikace s databází ukončena vykonáním příkazu **sqlQuery->finish**. [23]

```
## ------------------------------------------------------------
## Prace s DB MySQL - dotazy-----------------------------------
## ------------------------------------------------------------
$db ="ispadmin";
$user = "ispadmin";
$pass = "isp123";
$host="localhost";
$query_rtrid="SELECT * from cable_routers WHERE id=$routerid";
$query_rtruserserv="SELECT * from sl_internet WHERE rtrid=$routerid";
$query_rtrnetwork="SELECT * from cable_network WHERE rtrid=$routerid";
$query_rtrwanbw="SELECT * from mikrotik_queues WHERE rtrid=$routerid";
## ------------------------------------------------------------
## Prace s DB MySQL - zpracovani dotazu------------------------
## ------------------------------------------------------------
$dbh = DBI->connect("DBI:mysql:$db:$host", $user, $pass);
$sqlQuery  = $dbh->prepare(query_rtrid)
or die "Can't prepare query_rtrid: $dbh->errstr\n";
$sqlQuery->execute
or die "can't execute the query: $sqlQuery->errstr";
## ------------------------------------------------------------
## Prace s DB MySQL - vystup dat z DB--------------------------
## ------------------------------------------------------------
while (@row= $sqlQuery->fetchrow_array()) {
    $iprouteru = $row[1];
    $popisrouteru = $row[2];
}
my($mtik_host) = $iprouteru;
```

```
## ------------------------------------------------------------
## tabulka sluzeb: sl_internet
## row 0 = id
## row 1 = username
## row 2 = userip
## row 46 = user download
## row 47 = user upload
## row 69 = rtrid
$sqlQuery  = $dbh->prepare($query_rtruserserv)
or die "Can't prepare $query_rtruserserv: $dbh->errstr\n";
$sqlQuery->execute
or die "can't execute the query: $sqlQuery->errstr";
while (@row= $sqlQuery->fetchrow_array()) {
    push (@userid, $row[0]);
    push (@usernames, $row[1]);
    push (@ipadresy, $row[2]);
    push (@speed_down, $row[46]);
    push (@speed_up, $row[47]);
}
## ------------------------------------------------------------
## Prace s DB MySQL - ukonceni komunikace s DB----------------
##$------------------------------------------------------------
$sqlQuery->finish;
```

Zdrojový kód 2.2: Perl – Komunikace s databází MySQL

```
my($mtik_username) = 'admin';
my($mtik_password) = 'password';
print "Prihlasuji se do zarizeni: $mtik_host - $popisrouteru\n\n";
if (Mtik::login($mtik_host , $mtik_username, $mtik_password)) {
    print "Uspesne prihlaseno!\n";
##$ Mazani - Firewall Filter-----------------------------------
     print "Mazani aktualnich pravidel:\n";
     my @idlist = routeros_reading_rules('/ip/firewall/filter');
     my @result =
     routeros_removing_rules('/ip/firewall/filter', @idlist);
     #print @result;
     @idlist = ();
     undef @idlist;
```

Zdrojový kód 2.3: Perl – Mazání aktuálních pravidel firewallu

Zdrojový kód 2.3 popisuje mazání pravidel aktuálně nakonfigurovaných na síťovém zařízení. Před samotnou konfigurací aktuálních pravidel jsou vždy zcela smazány všechny pravidla ve firewallu (filter, mangle, address-list) a queue (simple Queue, queue Tree). Jedná se o preventivní opatření, protože kdykoli se někdo může k zařízení vzdáleně připojit a provést konfiguraci, která nemusí být správná nebo žádoucí,

proto skript nejprve pravidla smaže a nakonfiguruje znovu podle dat v systému ISPadmin. Příklad mazání je uveden pro pravidla firewallu. Nejprve je nutné do proměnných **mtik_username** a **mtik_password** uložit jméno a heslo pro možnost přihlásit se k zařízení. Poté je zavolána funkce **login** z knihovny **Mtik**, které je předáno přihlašovací jméno a heslo. Po úspěšném přihlášení je zavolána vytvořená funkce, které je předána cesta k sekci nastavení směrovače, kterou požadujeme smazat, tedy „**/ip/firewall/filter**“. Zdrojový kód 2.4 obsahuje funkci pro čtení jednotlivých řádků v sekci konfigurace, kterou jsme funkci předali. Nejprve je k cestě přidán řetězec „**/print**“ pro vypsání řádků v konfiguraci. Dále je zavolána funkce **get_by_key** v knihovně **Mtik**, která vypíše požadované řádky. Ty jsou uložené v proměné **ids**. Z celých řádků nám pro smazání postačuje pouze identifikátor konkrétního řádku. Proto je dále v cyklu pro každý řádek (pole **ids**) uložen identifikátor konkrétního řádku v paměti směrovače, tzv. „**.id**“. Seznam identifikátorů je funkcí push uložen do proměnné pole **@idlist**, která nově obsahuje pouze identifikátory řádků a ty předá zpět(**return @idlist**).

```
sub routeros_reading_rules
{
    @idlist = ();
    my($section)=$_[0] . "/print";
    my(%ids) = Mtik::get_by_key($section);
    if ($Mtik::error_msg eq '') {
            foreach my $id (keys (%ids))
            {
                foreach my $attr (keys (%{$ids{$id}}))
                {
                    if ($attr eq '.id') {
                    push (@idlist, $id . "\n");
                    #print "$ids{$id}{$attr}\n";
                    }
                }
            }
    }
    return @idlist;
}
```

Zdrojový kód 2.4: Perl – Čtení identifikátorů jednotlivých záznamů konfigurace

Ze zdrojového kódu 2.5 vidíme obdobný postup jako ve funkci čtení jednotlivých řádků. Opět je funkci předána sekce, kde pravidla smazat, ale nyní také proměnná **@idlist** obsahující seznam identifikátorů jednotlivých řádků v konfiguraci. Ke vstupnímu parametru, kde je uložena cesta, je přidán řetězec „**/remove**“, tentokrát tedy pro smazání. Za zmínku stojí jistě také použitý regulární výraz pro odstranění nežádoucích znaků před a za konkrétní hodnotou v poli **@idlist**. Bez odstranění těchto

nežádoucích znaků, konfigurované zařízení neakceptuje příkazy pro smazání jednotlivých řádků. Cyklem **for** je postupně vykonán příkaz pro smazání s uvedením konkrétních identifikátorů. Pro vyslání příkazu mazání každého řádku je využita upravená funkce v knihovně **Mtik**. Smazání každého řádku vrací hodnotu v proměnné **retval**, pokud je rovna 1 příkaz byl vykonán bez chybové hlášky, v opačném případě je vypsána chybová hláška. Pokud jsou obě funkce pro čtení i smazání vykonány správně, můžeme si nechat vypsat hodnotu v proměnné **result**, kde se nachází v případě úspěchu 1. Na závěr je smazán v paměti alokované pole **@idlist**. Tímto postupem je postupně smazáno nastavení firewallu a odchozích front, připravili jsme si tedy zařízení pro zápis pravidel nových.

```
1  sub routeros_removing_rules
2  {
3      @idlist = ();
4      my($section , @idlist)=@_;
5      $section = $section . "/remove";
6       my %operands;
7      for my $i (0 .. scalar @idlist-1){
8      $id = $idlist[$i];
9      $id =~ s/^\s*(.*?)\s*$/$1/;
10     $operands{'.id'} = $id;
11
12     my($retval,@results) = Mtik::mtik_cmd2($section,\%operands);
13         if ($retval != 1) {
14         print "removal of rule $idlist[$i] from $section failed. RC =
       $retval\n$Mtik::error_msg\n";
15         return $retval;
16         }
17         if ($retval == 1) {
18 #$         print "removal of rule $idlist[$i] DONE - RC = $retval\n";
19         }
20
21     }
22 print "OK.\n";
23 }
```

Zdrojový kód 2.5: Perl – Mazání pravidel v konfigurace směrovače

Jako názorný příklad konfigurace nových pravidel na základě aktuálních hodnot v databázi je uvedena ve zdrojovém kódu 2.6 konfigurace pravidla ve firewallu. Do pole proměnných **attrs_download** a **attrs_upload** jsou uloženy požadované parametry (i ty získané z databáze) pro konfiguraci:

- **chain** – Určuje fázi, ve které je pravidlem vyhodnocen síťový provoz. V tomto případě **forward** aplikuje dané pravidlo na veškerý provoz procházející daným síťovým zařízením. Pravidla nejsou aplikována na pakety které obsahují cílovou

adresu nakonfigurovanou na některém z rozhraní směrovače samotného.

- **dst-address** – Cílová adresa, je využita pro zapsání pravidla pro povolení komunikace ve směru k danému klientovi (download uživatele).
- **src-address** – Zdrojová adresa, je využita pro zapsání pravidla, které povolí komunikaci ve směru od klienta (uploadu uživatele).
- **action** – Určuje příslušnou akci, která je aplikována na pakety, které splňují podmínky definované pravidlem. Zde tedy povolíme přeposlání paketů (accept).
- **comment** – Popis pravidla slouží pro přehlednost.

Ve stavu, kdy máme připravené proměnné pro zápis pravidel je zavolána funkce **mti_cmd** z knihovny **Mtik**, které je obdobným postupem, jako při čtení nebo vymazání pravidel předána cesta pro zápis a pole proměnných se všemi potřebnými parametry (**attrs_network_download**, resp. **attrs_network_upload**). Funkce tedy zapíše nejprve pravidlo pro download a poté i upload jednoho uživatele. Celý tento proces je vykonán cyklem for tolikrát, kolik je počet identifikátorů v poli proměnné **@userid**, která obsahuje identifikátory všech uživatelů daného směrovače. Obdobným postupem jsou nakonfigurovány tyto sekce vybraného směrovače:

- **Firewall-Filter** – Pravidla pro konfiguraci firewallu.
- **Firewall-Mangle** – Konfigurace pravidel pro rozlišení jednotlivých služeb v síťovém provozu.
- **Firewall-Address list** – Přidány IP adresy používané pro rozlišení požadovaných služeb, jako je server poskytující IPTV služby nebo ověřené IP adresy, kterým je implicitně povolena komunikace (např. SSH whitelist).
- **Queues-Simple** – Omezení přenášených dat jednotlivými uživateli.
- **Queues-Tree** – Prioritizace provozu a zajištění kvality požadovaných služeb.

```
## ------------------------------------------------------
## Firewall - pravidla pro download i upload-------------
## ------------------------------------------------------
for my $i (0 .. scalar @userid-1){
      my(%attrs_download);
      $attrs_download{'chain'} = 'forward';
      $attrs_download{'dst-address'} = $ipadresy[$i];
      $attrs_download{'action'} = 'accept';
      $attrs_download{'comment'} = "Uzivatel $usernames[$i] - download"
   ;
      my(%attrs_upload);
      $attrs_upload{'chain'} = 'forward';
      $attrs_upload{'src-address'} = $ipadresy[$i];
      $attrs_upload{'action'} = 'accept';
      $attrs_upload{'comment'} = "Uzivatel $usernames[$i] - upload";
```

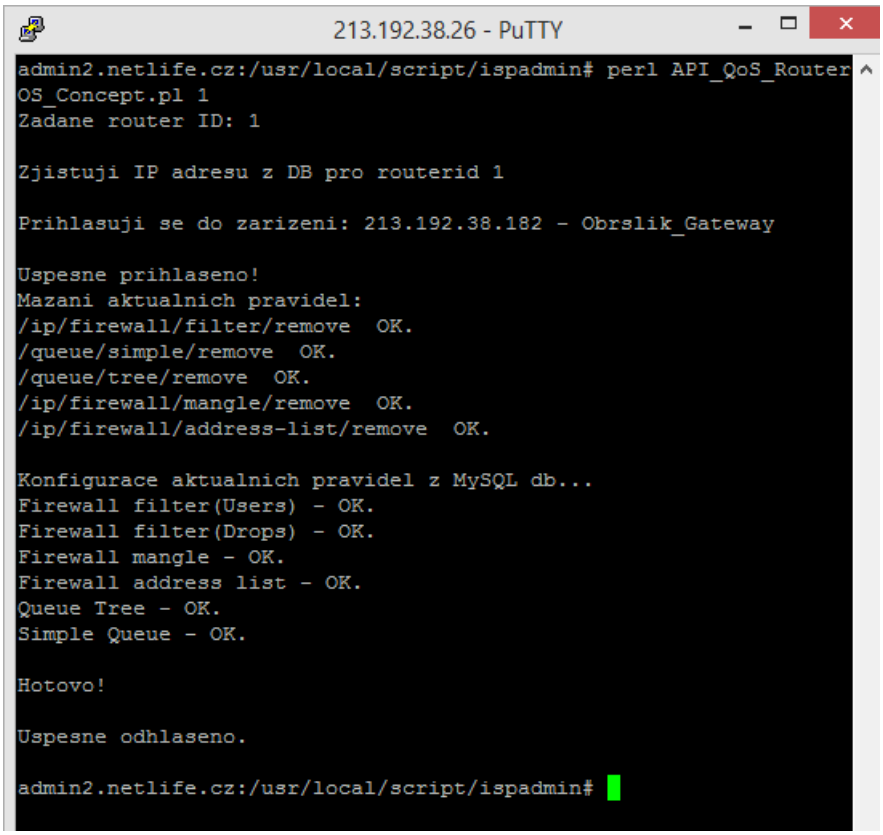
```
15      my($retval) = Mtik::mtik_cmd('/ip/firewall/filter/add',\%
    attrs_download);
16      if ($retval == 1)
17      {
18         #print "Pravidlo uzivatele $i zapsano.\n";
19      }
20      else
21      {
22         print "Unknown error: $Mtik::error_msg\n";
23      }
24      my($retval1) = Mtik::mtik_cmd('/ip/firewall/filter/add',\%
    attrs_upload);
25      if ($retval1 == 1)
26      {
27         #$print "Pravidlo uzivatele $i zapsano.\n";
28
29      }
30      else
31      {
32         print "Unknown error: $Mtik::error_msg\n";
33      }
34 }
35 print "Firewall filter(Users) - OK.\n";
```

Zdrojový kód 2.6: Perl – Zápis pravidel do konfigurace firewallu

Výše uvedené zdrojové kódy a jejich popis slouží k vysvětlení principu vytvořeného řešení. Kompletní zdrojový kód je k dispozici v příloze B.

2.5 Implementace

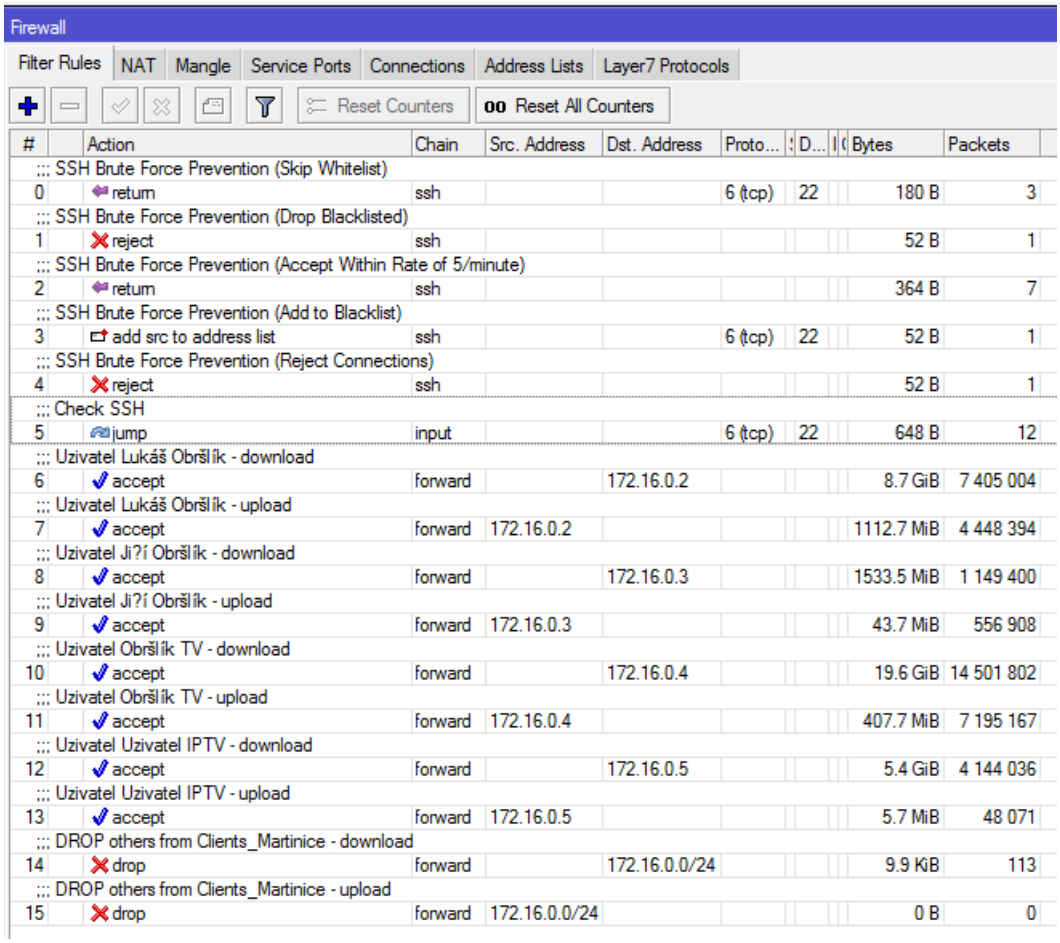
V rámci implementace bylo nejprve provedeno testování vytvořeného řešení. K testování byl využit dedikovaný server se systémem ISPadmin a na něm uložená data fiktivních uživatelů. Implementaci je nutné postupně provést tak, aby nebyli omezování uživatelé aktuálně využívající síťovou infrastrukturu. Výsledky získané testování popisují dále uvedené ilustrace. Uvedený obr. 2.17 byl zachycen po spuštění



Obr. 2.17: Lokálně spuštěný skript pro automatickou konfiguraci směrovače

skriptu na serveru se systémem ISPadmin. Jak je vidět ze zpráv systémem vypsaných do termínalu, byl spuštěn skript s koncovkou „**.pl**“ a parametrem (číslo 1). Skript si z databáze zjistil IP adresu zařižení s uvedeným ID. Poté se k zařízení připojil a smazal uvedené nastavení firewallu a front. Následně podle aktuálních hodnot v databázi nakonfiguroval kompletní konfiguraci. Stav firewallu na obr. 2.18 obsahuje tyto automaticky nakonfigurovaná pravidla:

- **SSH** – na prvních šesti řádcích (0-5) jsou pravidla pro ochranu směrovače před útokem hrubou silou (brute-force) využitím protokolu SSH. Prvních pět řádků bude aplikováno na všechny ssh připojení na daný směrovač. To je zajištěno pravidlem s indexem 5. Jeho podmínky splní připojení na portu 22 cílené na IP adresy nakonfigurované na směrovači (input). První z pěti pravidel povolí

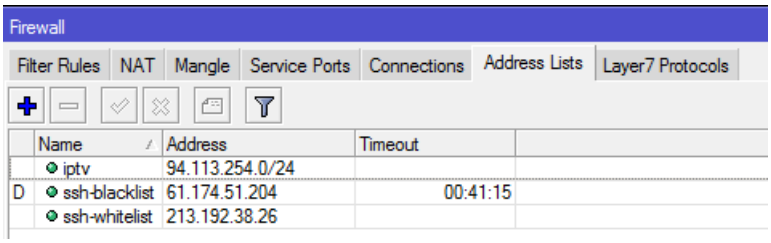


#	Action	Chain	Src. Address	Dst. Address	Proto...	D...	Bytes	Packets
;;; SSH Brute Force Prevention (Skip Whitelist)								
0	return	ssh			6 (tcp)	22	180 B	3
;;; SSH Brute Force Prevention (Drop Blacklisted)								
1	reject	ssh					52 B	1
;;; SSH Brute Force Prevention (Accept Within Rate of 5/minute)								
2	return	ssh					364 B	7
;;; SSH Brute Force Prevention (Add to Blacklist)								
3	add src to address list	ssh			6 (tcp)	22	52 B	1
;;; SSH Brute Force Prevention (Reject Connections)								
4	reject	ssh					52 B	1
;;; Check SSH								
5	jump	input			6 (tcp)	22	648 B	12
;;; Uzivatel Lukáš Obršlík - download								
6	accept	forward		172.16.0.2			8.7 GiB	7 405 004
;;; Uzivatel Lukáš Obršlík - upload								
7	accept	forward	172.16.0.2				1112.7 MiB	4 448 394
;;; Uzivatel Ji?í Obršlík - download								
8	accept	forward		172.16.0.3			1533.5 MiB	1 149 400
;;; Uzivatel Ji?í Obršlík - upload								
9	accept	forward	172.16.0.3				43.7 MiB	556 908
;;; Uzivatel Obršlík TV - download								
10	accept	forward		172.16.0.4			19.6 GiB	14 501 802
;;; Uzivatel Obršlík TV - upload								
11	accept	forward	172.16.0.4				407.7 MiB	7 195 167
;;; Uzivatel Uzivatel IPTV - download								
12	accept	forward		172.16.0.5			5.4 GiB	4 144 036
;;; Uzivatel Uzivatel IPTV - upload								
13	accept	forward	172.16.0.5				5.7 MiB	48 071
;;; DROP others from Clients_Martinice - download								
14	drop	forward		172.16.0.0/24			9.9 KiB	113
;;; DROP others from Clients_Martinice - upload								
15	drop	forward	172.16.0.0/24				0 B	0

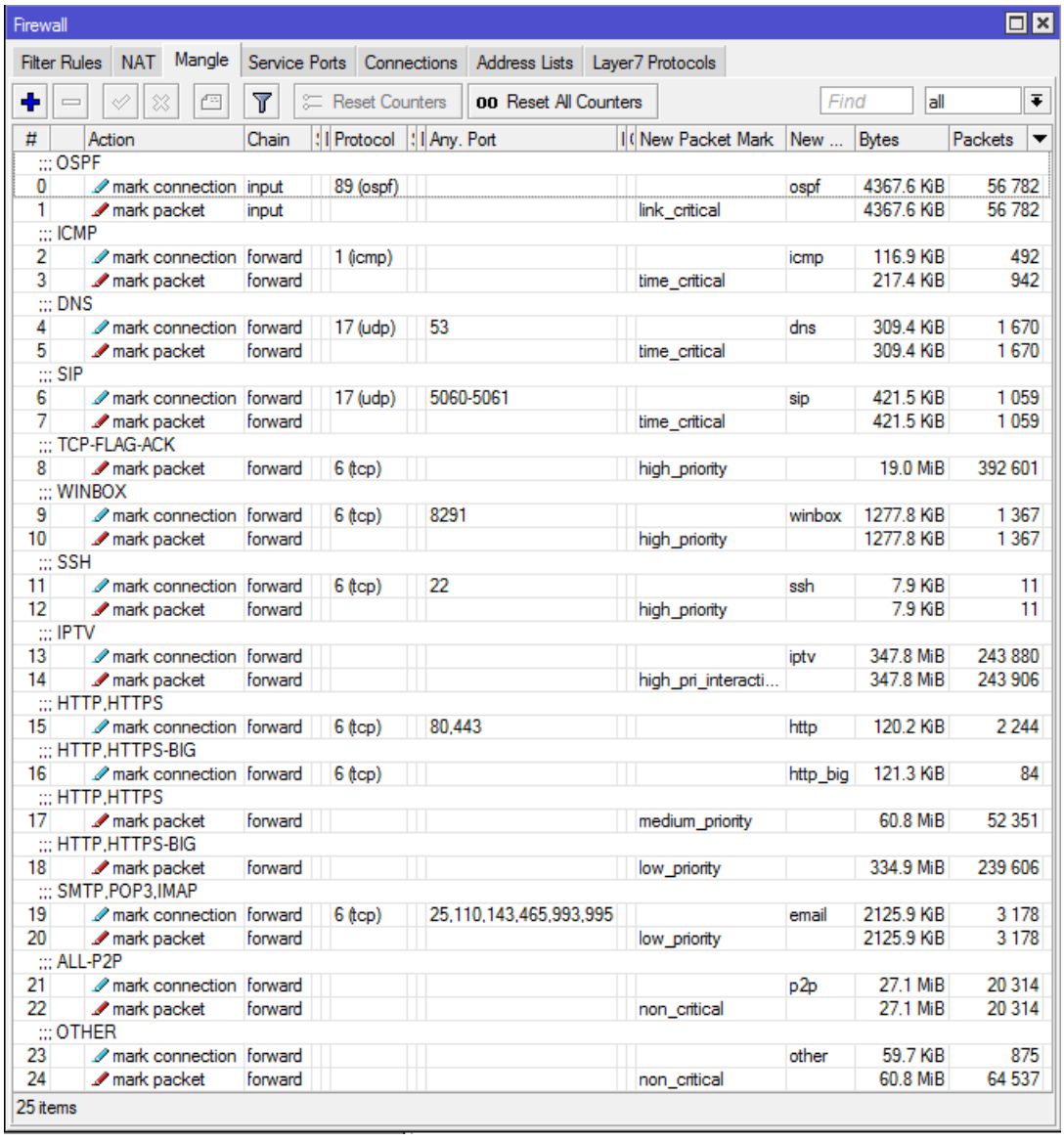
Obr. 2.18: Skriptem automaticky nakonfigurovaná pravidla firewallu

připojení pomocí SSH z IP adres patřících mezi důvěryhodné (whitelist). Další řádek zakáže připojení z IP adres, které již patří mezi blokované (blacklist). Pravidlo s indexem 2 povolí určitý počet připojení za daný interval, který se dá nakonfigurovat potřebnými parametry. Pokud nadefinovaný počet připojení za časový interval překročí daný limit, IP adresa potenciálního útočníka je přidána do seznamu adres (blacklist), viz. obr. 2.19 na předem nadefinovanou dobu(např. 1 hodina). IP adresám v seznamu zakázaných(blacklist) je implicitně zakázáno připojení na směrovač.

- **Povolené IP adresy** – Pravidla s indexem 6 až 12 povolují síťový provoz uživatelů, kteří jsou evidování v systému.
- **Zakázené IP adresy** – Poslední dvě pravidla zakáží provoz z IP adres (daných rozsahů), které nejsou v systému nijak evidované. Tyto IP adresy nejsou tedy využité pro poskytnutí služby. Potenciální nebezpečí stále hrozí, pokud by útočník zjistil IP adresy komunikujících účastníků metodou IP spoofingu. Mohl by zjištěné IP adresy použít ke komunikaci.



Obr. 2.19: Seznam adres využitých pro kontrolu SSH připojení a zajištění QoS



Obr. 2.20: Navržená a skriptem automaticky nakonfigurovaná pravidla pro rozlišení síťového provozu

Pravidla pro rozlišení síťového provozu jsou uvedená na obr. 2.20. Při konfiguraci je využito označení spojení (mark connection) a také značení paketů (mark-packet).

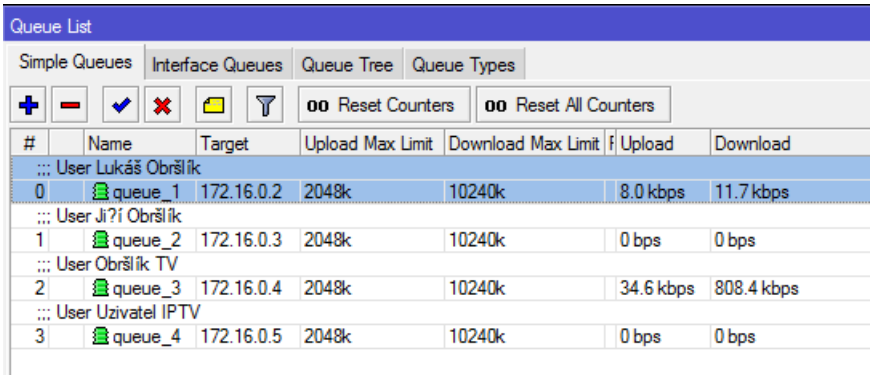
Funkce systému RouterOS pro značení spojení je velice efektivní, protože danou značku obdrží každý paket daného spojení a to v obou směrech (server-klient i klient-server). Značení slouží pouze pro interní použití v rámci směrovače, jak bylo popsáno v kapitole 2.3.6. Rozlišované služby jsou:

- **OSPF** – Komunikace protokolu OSPF zajišťující směrování v síti. Sledována je přímo komunikace protokolu OSPF (funkce RouterOS).
- **ICMP** – Velmi často využívaný protokol pro přenos řídících informací. Využita je opět funkce pro sledování protokolu ICMP integrovaná v systému RouterOS.
- **DNS** – Protokol pro překlad doménových názvů na IP adresy. Sledován je protokol UDP na portu 53.
- **SIP** – Signalizační protokol VoIP telefonie u spojení na portu 5060 a 5061 (UDP).
- **TCP** – Rozlišovány jsou v provozu potvrzení protokolu ACK (s omezenou délkou), které slouží pro potvrzení přijetí.
- **Winbox** – Komunikace nástroje Winbox, který slouží pro vzdálenou správu síťových zařízení s RouterOS. Využíván je protokol TCP a port 8291.
- **SSH** – Zabezpečený komunikační protokol pro správu síťových zařízení (TCP, port 22).
- **IPTV** – Přenos digitální IPTV televize, který je rozlišován na základě známé IP adresy serveru, který službu poskytuje.
- **HTTP** – Protokol pro přenos obsahu webový stránek. Rozeznáván je také přenos nezabezpečený i zabezpečený protokolu TCP na portech 80 (HTTP) a 443 (HTTPS). Dále je rozlišen provoz méně náročný na objem přenášených dat a delší přenosy, které většinou znamenají např. stahování většího objemu dat z internetu. Limit stanovuje objem přenesených dat daného spojení. V navrhnutém řešení po překročení hranice 5 MB je přenos zařazen do kategorie s nižší prioritou.
- **Poštovní protokoly** – Známé protokoly pro přenos elektronické pošty SMTP, POP3 (zabezpečený) a IMAP (zabezpečený) na portech 25, 110, 143, 465, 993 a 995.
- **P2P** – Datové přenosy vyhodnocené integrovanou funkcí systému RouterOS jako peer-to-peer spojení(typicky bittorrent).
- **Ostatní** – Do kategorie ostatní(other) je zařazen veškerý provoz, který nesplní předchozí podmínky. Lze tak efektivně oddělit provoz, který není jednoduché rozlišit (různé bittorrent spojení apod.) a přidělit mu nižší prioritu.

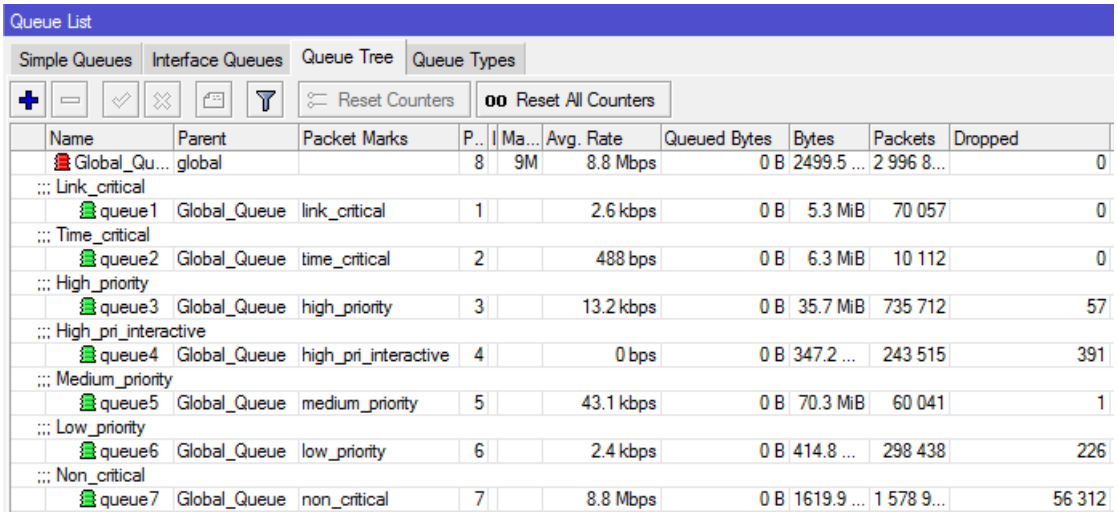
Popsaná technika rozdělení provozu je založena na rozlišení známých služeb a služby neklasifikované jsou přiřazeny do nejnižší kategorie. Prioritizujeme tak požadované služby před službami, které nejsou natolik kritické.

Podle zjištěných IP adres je dále skriptem nakonfigurováno omezení využité šířky

pásma jednotlivými uživateli, jak je znázorněno na obr. 2.21. Omezení šířky je prováděno na základě IP adresy uživatele a poskytovaného tarifu. Tyto údaje jsou zjištěny z databáze. Pro prioritizování jednotlivých služeb je nakonfigurována na směrovači také fronta provozu. Je vytvořeno sedm kategorií na základě rozlišeného provozu a všem dohromady je přidělena určitá šířka pásma. Tato hodnota je vyčtena z databáze, kde je u každého směrovače nutné vyplnit speciální pole hodnotou, která je skriptem vyhodnocena jako počet Mb/s a nastavena jako maximální využitá šířka pásma daným směrovačem (kapacity linky směřující k hlavnímu směrovači). Prakticky veškerý provoz v této stromové topologii je směrován na hlavní směrovač (kořen stromu) a dále do sítě internet. Směrovač, který jako první v topologii začne plně využívat přidělené pásmo bude tzv. úzkým hrdlem na cestě k hlavnímu směrovači. Vytvořené řešení začne v tuto chvíli prioritizovat požadované služby a zbytek provozu omezovat. Jednotlivé fronty provozu jsou uvedeny na obr. 2.22.



Obr. 2.21: Limitování přenášených dat jednotlivými uživateli



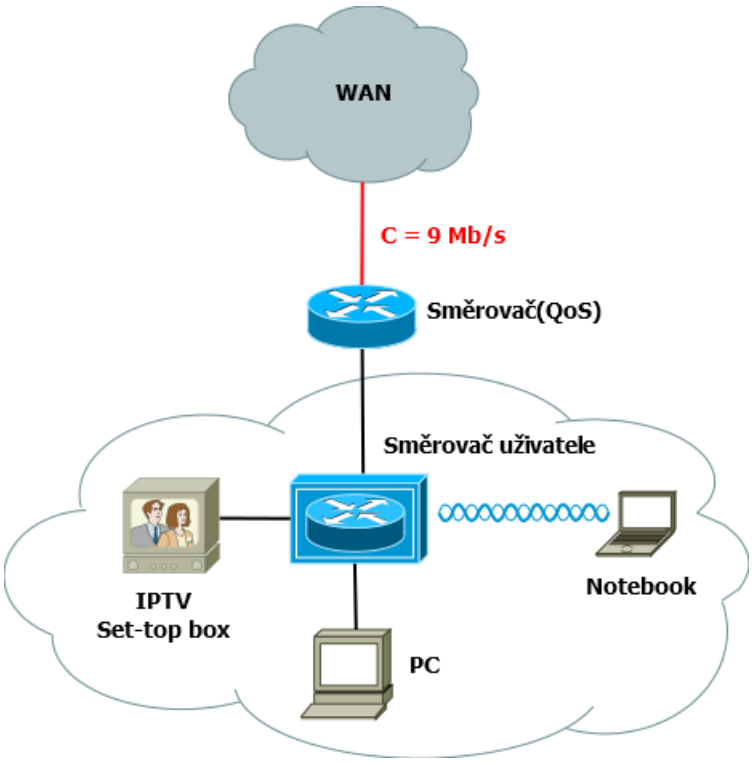
Obr. 2.22: Prioritizované datové toky rozlišovaných služeb

2.6 Optimalizace

Poslední část představuje optimalizaci nasazeného síťového řešení. V rámci optimalizace je myšleno odladění nově nasazeného řešení. Sestavená konfigurace byla nasazena na testovací server a vytvořený skript je testován na reálném síťovém provozu. Z výsledků získaných pomocí testování bude následně optimalizována konfigurace skriptu takovým způsobem, aby byla zajištěna co nejvyšší možná míra kvality poskytovaných služeb na síti. Skript byl navržen tak, aby bylo jednoduše možné přidat další služby, které bude v síťovém provozu rozpoznávat. Tyto požadované služby je možné zařadit do kategorie s požadovanou prioritou. V průběhu testování se mohou také vyskytovat doposud neodhalené chyby v konfiguraci, které bude následně nutné opravit.

2.7 Vliv řešení na poskytované služby

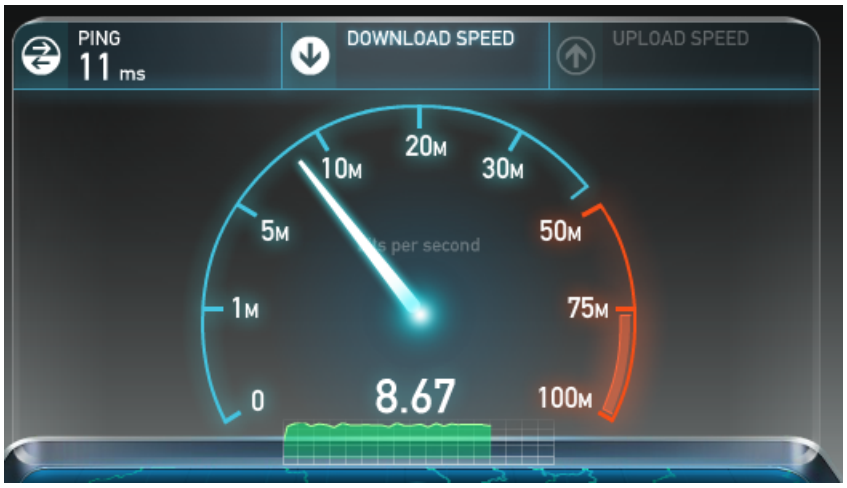
Po realizaci popsaného skriptu bylo provedeno testování na reálném síťovém provozu. Vytvořeným skriptem byl automaticky nakonfigurován směrovač a proveden experiment pro ověření vlivu přidělení priorit jednotlivým službám. Zapojení testované topologie je uvedeno na obr. 2.23. Topologie obsahuje směrovač MikroTik



Obr. 2.23: Topologie využitá pro testování prioritizace služeb

RB433AH nakonfigurovaný vytvořeným skriptem. Směrovač je připojen k síti Internet prostřednictvím síťové infrastruktury ISP (znázorněna jako WAN). Linka směrem do sítě internet má omezenou kapacitu. Dále k testovacímu směrovači připojen směrovač, který simuluje běžný směrovač, který se nachází u uživatele. Na tomto směrovači nejsou aplikována žádná pravidla pro zajištění kvality služeb. K tomuto uživatelskému směrovači je připojen testovací set-top box pro příjem IPTV, koncový počítač a také notebook prostřednictvím bezdrátové sítě. Síť uživatele používá adresní rozsah třídy C a všechny zařízení uživatele spolu tedy mohou komunikovat na linkové vrstvě (L2). Směrovač uživatele MikroTik RB751G má jedno rozhraní vyhrazené pro komunikaci s infrastrukturou poskytovatele (WAN rozhraní) a ostatní rozhraní (včetně bezdrátového) jsou logicky přemostěna a mají tak jednu společnou IP adresu, která je výchozí bránou pro všechna zařízení v síti. Komunikace do sítě internet je poté využitím technologie překládání IP adres (NAT), překládána za adresu na WAN rozhraní tohoto směrovače. Postup testování:

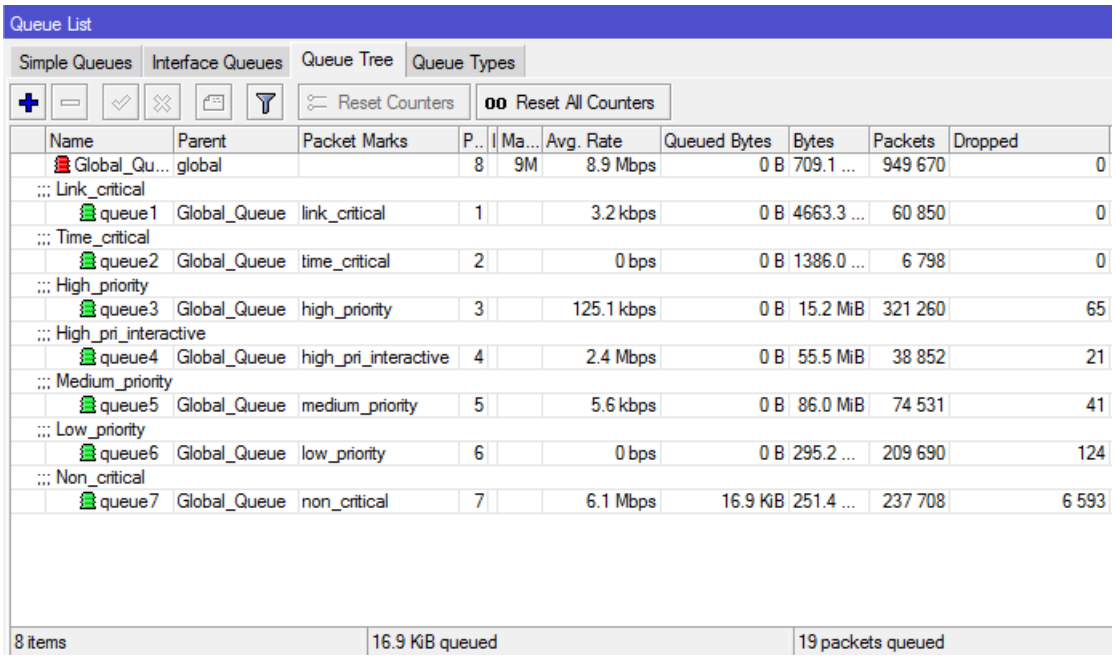
1. Nejprve byla na koncovém zařízení otestována dostupná kapacity linky do sítě internet. Obr. 2.24 uvádí test internetového připojení z koncového zařízení připojeného ke směrovači uživatele. Získaný výsledek je ovlivněný způsobem testování, kdy je využíváno protokolu TCP. Postupné narůstání rychlosti je náročné na režii(potvrzovací okénko). Výsledek 8,67 Mb/s odpovídá realitě při kapacitě linky 9 Mb/s.



Obr. 2.24: Dostupná kapacita linky do sítě internet

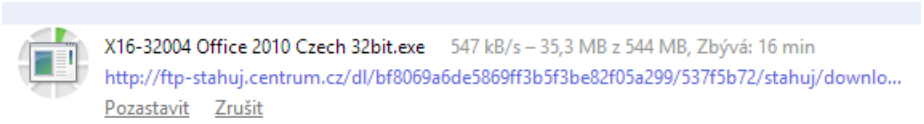
2. Následovalo spuštění softwaru uTorrent na koncové stanici a přenos dat ze sítě internet (bitové kopie unixové distribuce OpenSUSE). Stav prioritizace služeb je v tuto chvíli zachycen na obr. 2.22. Je vytížená celá šířká pásma (červená barva globální fronty) a přenos protokolem je klasifikován jako provoz s nejnižší prioritou (non_critical).

3. V průběhu přenosu souboru byl spuštěn set-top box pro příjem služby IPTV. Služba byla směrovačem pro zajištění kvality služeb správně vyhodnocena, jak ukazuje obr. 2.25. Přenosová rychlost služby s nižší prioritou (bittorrent) byla omezena, aby mohla být využita služba s vyšší prioritou (IPTV).



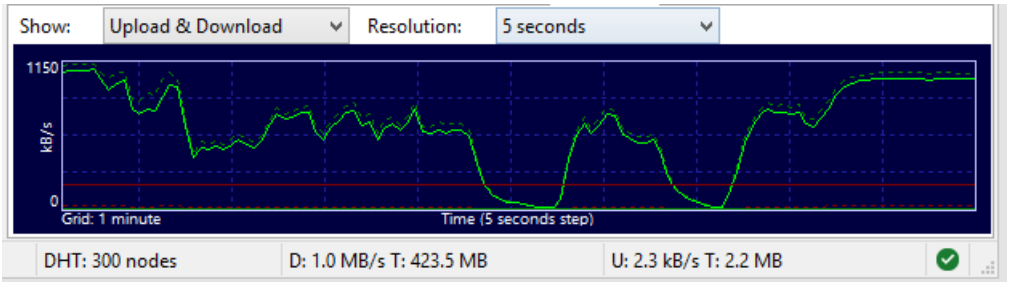
Obr. 2.25: Přenos IPTV vysílání a správné přidělení priorit

4. Navíc bylo ze serveru stahuj.cz spuštěno stahování souboru pro instalaci kancelářského software o velikosti 544 MB. Směrovač opět zareagoval a přehodnotil aktuální procházející provoz podle nadefinovaných pravidel. Stav v tuto chvíli zachycuje obr. 2.26.
   Přenos bitové kopie (non_critical) má nyní k dispozici ještě nižší přenosovou rychlost, protože se přenášejí služby s vyšší prioritou. Stahování prostřednictvím webového prohlížeče (low_priority) má přidělenou takovou šířku pásma, která je dostupná po využití službou IPTV (high_pri_interactive). Televizní vysílání tedy funguje stále a služby s nižší prioritou se přizpůsobily dostupné šířce pásma, dle nastavených priorit. V jednotlivých stavech je také počet zahozených paketů danou úrovní fronty. U služeb s nižší prioritou je více zahozených paketů, než u služeb s vyšší prioritou a jedná se o žádoucí stav navrhnutého řešení. K zahození paketu dojde, pokud nemá směrovač dostupnou kapacitu pro jeho zpracování.
5. V momentě, kdy byl set-top box vypnut a stahování souboru ze serveru stahuj.cz ukončeno, dostupná je opět celá šířka pásma i pro službu s nejnižší prioritou. Přenos bitové kopie prostřednictvím bittorrent protokolu využívá



Obr. 2.26: Přenos dat ze serveru prostřednictvím webového prohlížeče

opět celou šířku pásma. Graf využité šířky pásma protokolem bittorrent je uveden na obr. 2.27. V první části grafu je využitá šířka pásma 1150 kB/s (odpovídá přidělené kapacitě 9 Mb/s). Poté došlo v průběhu využívání služeb s vyšší prioritou k omezení využité šířky pásma protokolem bittorrent. V situaci, kdy služby s vyšší prioritou nejsou uživatelem již vyžadovány je opět dostupná šířka využita protokolem bittorrent. Na základě těchto výsledků testování lze říci, že navrhnuté řešení splňuje požadovaný cíl, kterým byla rezervace šířky pásma pro IPTV v závislosti na ostatních tocích v síti. Navrhnuté řešení se navíc dynamicky přizpůsobuje aktuálnímu síťovému toku a v případě, kdy není vyžadována služba s vyšší prioritou, mohou dostupnou šířku pásma využít ostatní služby. V situaci, kdy byla prioritizace služeb(Queue Tree) deaktivována využije dostupnou šířku pásma datový přenos protokolu bittorrent a služba IPTV je nepožitelná a je obtížné navázat pouze samotné spojení se serverem.



Obr. 2.27: Graf využití šířky pásma protokolem bittorrent

3 ZÁVĚR

Cílem diplomové práce bylo nastudování problematiky implementace triple-play služeb a zabezpečení kvality služby v heterogenních komunikačních sítích. Vypracování je zaměřeno na ověření teoreticky nastudované problematiky na reálné situaci a existující síťové infrastruktuře. Součástí vypracování je tvorba technického řešení, které zajišťuje automatickou prioritizaci služeb na základě identifikace a rozdělení požadovaných služeb v síťovém provozu.

V první části práce byly zkoumány technologie heterogenních sítí. Do práce jsou zahrnuty používaná přenosová média v transportních a přístupových heterogenních sítích. Dále se teoretická část věnuje implementaci triple-play služeb a zajištění kvality poskytovaných služeb pro přenos multimediálních toků pracujících v reálném čase po pakětově komutovaných sítích. V rámci zajištění kvality služby jsou zkoumány postupy pro klasifikaci síťového provozu a řízení přetížení. K přenosu dat jsou využívány odlišné technologie, v závislosti na druhu služby. Vypracování zahrnuje nejčastěji používané technologie typu unicast, multicast apod.

V rámci praktické části byly nastudované informaci a postupy aplikovány na reálné situaci. Pro implementaci triple-play služeb byla vybrána existující heterogenní síť regionálního poskytovatele internetových služeb(ISP). Prvním krokem bylo stanovení požadavků poskytovatele pro implementaci. Na základě požadavků byl sestaven plán a navrženy jednotlivé kroky implementace, podle kterých bylo dále postupováno. Počátečním krokem byla analýza existující síťové infrastruktury. Zkoumán byl používaný síťový model, aktivní prvky, vytížení síťové infrastruktury a způsob správy. Na základě vyhodnocení získaných informací bylo navrženo konkrétní technické řešení v závislosti na technických možnostech. Vybráno bylo několik typů IPTV řešení a ty následně prakticky testovány. Pro poskytované služby v síti bylo zpracováno řešení pro zajištění kvality služby na aktivních prvcích, které jsou v síti používány. Zajištění kvality služby bylo navrženo tak, aby bylo řešení možné v síti implementovat, do budoucna přizpůsobovat aktuálním požadavkům a zajistit tak škálovatelnost. Při vytváření byl využit skriptovací jazyk Perl z důvodu unifikace. Perl je již v rámci správy síťové infrastruktury využíván a je tak vhodným postupem, používat jeden druh programovacího, resp. skriptovacího jazyka v rámci jednoho systémového řešení.

Vytvořené řešení bylo na závěr testováno na několika aktivních prvcích infrastruktury a analyzován vliv řešení na poskytované služby v síti. Testováním bylo zjištěno, že vytvořené technické řešení dynamicky zajišťuje garanci přidělené šířky pásma, v závislosti na předem definovaných prioritách pro požadované služby. Díky vytvořenému řešení je nyní možné nabízet službu IPTV i v místech síťové infrastruktury, kde může ve špičce docházet k využití téměř veškeré dostupné přenosové kapacity.

V rámci dlouhodobějšího testování budou vyhodnocovány získané výsledky a na základě těchto výsledků optimalizováno vytvořené řešení pro co nejefektivnější práci se síťovým provozem a případně přidány další prioritizované služby. Pro možnost otestování vytvořeného řešení byl vytvořen návod pro instalaci požadovaného systému a konfiguraci síťových prvků.

LITERATURA

[1] HENS, Francisco J a José Manuel CABALLERO: HENS, Francisco J a José Manuel CABALLERO. *Triple play: building the converged network for IP, VoIP and IPTV*. Hoboken, NJ: Wiley, c2008, xiii, 401 p. ISBN 04-707-5367-6.

[2] LAMANAUSKAS, Tomas. Proposing a concept for regulating Triple Play bundling of services. In: *Telecoms Regulation & Competition Law* [online]. 2005 [cit. 2013- 12-31]. Dostupné z: `http://bit.ly/1cDGWOS`

[3] WILLIAMS, Chris. Wireless Networks vs. Ethernet Networks. Is there Still a Debate?. *Carousel Industries Inc.* [online]. 2011-06-22 [cit. 2014-05-16]. Dostupné z: `http://blogs.carouselindustries.com/wireless/wireless-networks-vs-ethernet-networks-is-there-still-a-debate/`

[4] BARBER, Matt. Advantages & Disadvantages With Optical Fibres. *Matt Barber's Fibre Optics Page* [online]. 2009 [cit. 2013-12-21]. Dostupné z: `http://services.eng.uts.edu.au/~akadi/ite/major_assignments/barber/advdisad.htm`

[5] WAN, Fengdan, Lin CAI, Emad SHIHAB a Aaron GULLIVER. Admission region of triple-play services in wireless home networks. *Computer Communications* [online]. 2010, vol. 33, issue 7, s. 852-859 [cit. 2013-12-31]. DOI: 10.1016/j.comcom.2009.12.006. Dostupné z: <`http://linkinghub.elsevier.com/retrieve/pii/S0140366409003429`>.

[6] ANDREWS, Matthew, Krishnan KUMARAN, Kavita RAMANAN, Alexander STOLYAR, Phil WHITING a Rajiv VIJAYAKUMAR. Providing Quality of Service over a Shared Wireless Link. In: *QOS AND RESOURCE ALLOCATION IN THE 3RD GENERATION WIRELESS NETWORKS* [online]. 2001 [cit. 2013-12-31]. Dostupné z: `http://ieeexplore.ieee.org.ezproxy.bib.hh.se/stamp/stamp.jsp?tp=&arnumber=900644`

[7] RÄISÄNEN, Vilho. *Implementing service quality in IP networks*. Chichester: John Wiley, c2003, xxvii, 325 s. ISBN 04-708-4793-X.

[8] XIPENG XIAO a L.M. NI. Internet QoS: a big picture. *IEEE Network* [online]. vol. 13, issue 2, s. 8-18 [cit. 2014-05-26]. DOI: 10.1109/65.768484. Dostupné z: `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=768484`

[9] WITTMANN, Ralph a Martina ZITTERBART. *Multicast communication: protocols and applications*. San Francisco: Morgan Kaufmann Publishers, 2001, 349 s. ISBN 15-586-0645-9.

[10] GROTH, David. *Network study guide*. 4th ed. London: SYBEX, 2005, xxxviii, 519 p. ISBN 07-821-4406-3.

[11] ALUWIHARE, Assaji, Jon BECKMAN, Robert FLASK, Eli KERCH, Jerome LAFERRIERE, Mirna MEKIC, Jim NERSCHOOK, Nisha PARBHAKAR, Thad WARD a John WILLIAMS. Triple-Play Service Deployment. In: *A Comprehensive Guide to Test, Measurement, and Service Assurance* [online]. 2007 [cit. 2013-12-30]. Dostupné z: `http://www.jdsu.com/noindexliterature/jdsu_tripleplay_book_1107.pdf`

[12] LEE, Hyo-Jin, Myung-Sup KIM, James W. HONG a Gil-Haeng LEE. QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring. In: *Distributed Processing & Network Management Lab* [online]. 2003 [cit. 2014-05-16]. Dostupné z: `http://www.knom.or.kr/knom-review/v5n2/4.pdf`

[13] DICK, Brad. What is IPTV: Unicast vs. multicast. BROADCAST ENGINEERING. *IPTV Pavilion* [online]. 2008 [cit. 2013-12-31]. Dostupné z: `http://iptvpavilion.com/features/iptv-unicast-multicast-0319/`

[14] OCCHIOGROSSO, Stephen. The Cisco PPDIOO Life Cycle. *CCIE or Null!* [online]. 2011-05-09 [cit. 2014-05-16]. Dostupné z: <`http://ccie-or-null.net/2011/05/09/the-cisco-ppdioo-life-cycle/`>.

[15] NAGIOS. NET SERVICE SOLUTION. *ISP admin Wiki* [online]. 2009 [cit. 2014-05-10]. Dostupné z: `http://wiki.ispadmin.eu/index.php/Documentation/Monitoring/NAGIOS/cs`

[16] DEAN, Tamara. *Network guide to networks*. 6th Ed. Clifton Park, NY: Course Technology, Cengage Learning, 2012, p. cm. ISBN 978-113-3608-196.

[17] Manual:Interface/Wireless. MIKROTIK. *Official MikroTik documentation* [online]. 2014 [cit. 2014-05-18]. Dostupné z: `http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless`

[18] Vlastnosti systému ISP admin. NET SERVICE SOLUTION. *Co je ISPadmin ?* [online]. 2009 [cit. 2014-05-18]. Dostupné z: `http://wiki.ispadmin.eu/index.php/Features`

[19] Traffic Priortization, RouterOS QoS Implemetation. MIKROTIK. *Official MikroTik documentation* [online]. 2009-04-30 [cit. 2014-05-20]. Dostupné z: http://wiki.mikrotik.com/wiki/Traffic_Priortization,_RouterOS_QoS_Implemetation

[20] RIYADI, Valens. QoS: RouterOS v6. In: *MikroTik User Meeting* [online]. 2013 [cit. [cit. 2014-05-10]]. Dostupné z: http://mum.mikrotik.com/presentations/HR13/valens.pdf

[21] MEGIS, Janis. New Obvious and Obscure: MikroTik RouterOS v6 features. MIKROTIK. *MikroTik User Meeting* [online]. 2012 [cit. 2014-05-20]. Dostupné z: http://mum.mikrotik.com/presentations/US12/megis.pdf

[22] VÁCLAVÍK, Jiří. Perl. *Linuxsoft* [online]. 2005-02-08 [cit. 2014-05-22]. Dostupné z: http://www.linuxsoft.cz/article_list.php?id_kategory=210

[23] How to access MySQL database using Perl. NIXCRAFT. *MYSQL* [online]. 2006-09-07 [cit. 2014-05-22]. Dostupné z: http://www.cyberciti.biz/faq/how-to-access-mysql-database-using-perl/

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

$\Delta\Delta T$ – Časový rozdíl mezi dvěma po sobě doručenými pakety.

ΔT – Zpoždění paketu na trase mezi vysílačem a přijímačem.

AAA (Authentication – Authorization – Accounting) – Protokol pro autentizaci uživatele, přidělení specifické služby (autorizace) a následné účtování (accounting).

API (Application Programming Interface) – Rozhraní pro komunikaci a konfiguraci zařízení.

BER (Bit error ratio) – Poměr mezi celkovým počtem přijatých bitů a chybně přijatými bity.

Btest – Název nástroje pro měření propustnosti mezi dvěma stanicemi počítačové sítě.

Blu-ray – Typ optického disku určeného pro ukládání velkého objemu digitálních dat.

CCQ (Client Connection Quality) – Hodnota udávaná v procentech, která značí, jak efektivně je využívaná dostupná šířka pásma pro přenos dat na bezdrátovém spoji.

CoS (Class-of-Service) – Zkratka používaná v oblasti kvality služeb QoS. Jedná se o identifikátor sloužící pro označení třídy provozu.

dBm – Jednotka hodnoty výkonu vztažená vůči 1 mW.

DNS (Domain Name Service) – Protokol sloužící k překladu doménových názvů na IP adresy.

Downlink – Přenos dat směrem ke koncovému zařízení uživatele.

DSSS (Direct-Sequence Spread Spectrum) – Modulační technika využívající rozprostřeného spektra. Vyslaný bit je modulací rozprostřen do více bitů, je tak odolný proti rušení, kdy při přenosu dojde ke změně přenášených dat.

EoIP (Ethernet over IP) – Jedná se o technologii zapouzdření Ethernetových rámců do IP protokolu, tzv. tunelování.

EPG (Electronic Program Guide) – Doplňková služba digitální televizního vysílání nabízející informace o vysílaných pořadech.

Ethernet – Technologie pro komunikaci v LAN síti.

FTP (Foil-Screened Twisted Pair) – Stíněná kroucená dvojlinka, kde jsou všechny páry obaleny jednou stínící kovovou fólií.

H.264 – Standard pro kompresi videa.

HDMI (High-Definition Multimedia Interface) – Rozhraní pro přenos obrazového a zvukového signálu v digitálním formátu.

ICMP (Internet Control Message Protocol) – Protokol pro přenos řídících informací v IP sítích.

IEEE 802.11 – Standard, který specifikuje bezdrátovou komunikaci v lokálních sítích.

IEEE 802.11a – Standard představený v roce 1999, který specifikuje bezdrátovou komunikaci využívající kmitočtové pásmo 5 GHz s využitím modulace OFDM.

IEEE 802.11b – Standard představený v roce 1999, který specifikuje bezdrátovou komunikaci využívající kmitočtové pásmo 2,4 GHz s využitím modulace DSSS.

IEEE 802.11g – Standard představený v roce 2003, který specifikuje bezdrátovou komunikaci využívající kmitočtové pásmo 2,4 GHz s využitím modulací OFDM a DSSS.

IEEE 802.11n – Standard představený v roce 2009, který specifikuje bezdrátovou komunikaci využívající kmitočtové pásmo 2,4 a 5GHz GHz, s využitím modulace OFDM a volitelně také technologie MIMO.

IEEE 802.3 – Standard společnosti IEEE, který určuje specifikace pro komunikaci na linkové a fyzické vrstvě.

IEEE (Institute of Electrical and Electronics Engineers) – Mezinárodní organizace zabývající se elektrotechnickým a elektronickým inženýrstvím.

IETF (Internet Engineering Task Force) – Organizace, vyvíjející síťové a telekomunikační protokoly.

IP protokol – Základní protokol pracující na síťové vrstvě.

IPPM (IP Performance Metrics) – Skupina parametrů definující parametry síťového provozu.

IPTV (Internet Protocol Television) – Televize přes IP protokol.

ISP (Internet Service Provider) – Poskytovatel internetových služeb.

ISPAdmin – Systém určený pro správu síťové infrastruktury a koncových uživatelů využívaný zejména regionálními ISP.

LAN (Local Area Network) – Lokální počítačová síť.

MIMO (Multiple-input Multiple-output) – Technologie využívaná v oblasti rádiové komunikace, kdy je na straně vysílače a přijímače využito více antén pro zvýšení propustnosti daného spoje.

Multicast – Technologie pro komunikaci. Jedná se o přeposílání IP paketů z jednoho zdroje skupině více koncových stanic.

MySQL – Multiplatformní databázový systém využívající jazyk SQL.

Nagios – Open-source systém pro monitorování počítačových sítí.

NETflow – Otevřený protokol vyvinutý společností Cisco. Jeho hlavním účelem je monitorování síťového provozu.

Ntop – Multiplatformní nástroj pro zjištění podrobných informací o síťovém provozu.

OFDM (Orthogonal Frequency-Division Multiplexing) – Modulační technika, kdy je frekvenční pásmo rozděleno do částí. Každá část má vlastní nosnou frekvenci, kde je přenášena část dat.

OS (Operating system) – Zkratka pro operační systém – programové vybavení počítače.

OSPF (Open Shortest Path First) – Jedná se o protokol pro dynamické sestavení směrovacích tabulek směrovačů v IP sítích.

P2P (Peer-To-Peer) – Typ komunikace mezi entitami, kdy mezi sebou komunikují přímo stanice. Není vyžadován centrální server.

PC (Personal Computer) – Označení pro osobní počítač, v současné době velice rozšířený termín.

PLC (Personal Computer) – Zkratka označující technologii pro přenos dat po elektrické síti.

PPDIOO (Prepare – Plan – Design – Implement – Operate – Optimize) – Jedná se o šest fází návrhu a provozu telekomunikační sít navrhnutých společností Cisco.

QoS (Quality of Service) – Technologie pro řízení a rezervaci datových toků v telekomunikačních a počítačových sítích.

Radius (Remote Authentication Dial In User Service) – Jedná se o AAA protokol pro autentifikování přístupu k síťovým prostředkům.

RCA – Standardizovaný konektor určený pro přenos obrazového a zvukového signálu.

RFC (Request For Comments) – Zkratka která se používá pro označení standardu popisující dokumentaci např. protokolu. Jednotlivé dokumentace jsou odlišeny číslem.

RJ-11 (Registered Jack – typ 11) – Typ koncovky, který je velmi často využíván u telefonních zařízení.

RJ-45F (Registered Jack – typ 45F) – Rozšířený typ koncovky, která je velmi často využíván v telekomunikačních sítích.

RouterOS – Operační systém pro síťové prvky. Pro svoji platformu aktivních síťových prvků RouterBOARD jej od roku 1995 vyvíjí litevská společnost MikroTik.

RRDtool (Round-robin database tool) – Výkonný open-source nástroj pro zpracování a ukládání časově závislých dat. Obsahuje také integrované nástroje pro zobrazení dat v grafické podobě.

Rx (Receive) – Zkratka, která se používá v telekomunikacích ve spojistosti s přijímačem.

SFP (Small Form-factor Pluggable) – Označuje typ konektoru používaného pro připojení přenosového média, např. optického kabelu k síťovému prvku.

SIP (Session Initiation Protocol) – Protokol určený pro přenos signalizace v internetové telefonii dle SIP architektury.

SLA (Service-level agreement) – Jedná se o dohodu o poskytnutí určité kvality služby mezi dodavatelem a zákazníkem.

SNMP (Simple Network Management Protocol) – Protokol pro sběr dat využívaný při správě sítě, umožňuje také autentizaci a šifrování.

Smart TV – Označení moderního televizoru, který disponuje doplňkovými funkcemi a připojením do sítě Internet.

SSH (Secure Shell) – Zabezpečený komunikační protokol pro komunikaci v počítačových sítích.

STP (Shielded Twisteded Pair) – Stíněná kroucená dvojlinka, kde jsou všechny páry zvlášť obaleny stínící kovovou fólií.

$\boldsymbol{T_d}$ – Čas nutný k doručení daného paketu.

$\boldsymbol{T_{d+1}}$ – Čas nutný k doručení paketu následujícího.

$\boldsymbol{T_c}$ – Doba nutná k přenosu paketu danou linkou.

$\boldsymbol{T_p}$ – Doba nutná ke zpracování paketů konkrétním aktivním prvkem (směrovačem nebo přepínačem).

$\boldsymbol{T_s}$ – Zpoždění mezi přenosem prvního a posledního bitu (stejného paketu).

Tx (Transmit) – Zkratka, která se používá v telekomunikacích ve spojistosti s vysílačem.

Unix – Operační systém. První verzi vyvinula společnost AT&T v roce 1969.

UTP (Unshielded Twisted Pair) – Nesťíněná kroucená dvojlinka.

VoIP (Voice over IP protocol) – Přenos hlasu přes IP protokol.

Upload – Přenos dat směrem od uživateli.

Wi-Fi – Technologie pro bezdrátovou komunikaci v počítačových sítích.

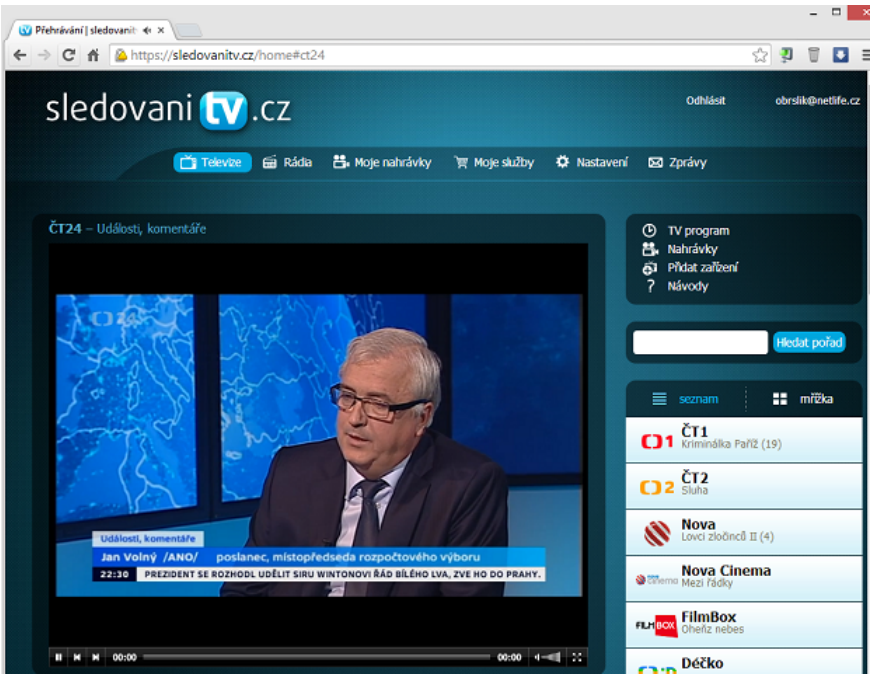
x64 – Označení představuje hardwarovou architekturu procesorů, které zpracovávají 64-bitové instrukce.

x86 – Označení představuje hardwarovou architekturu procesorů, které jsou odvozeny od 16-bitového procesoru Intel 8086, který původně podporoval pouze 16-bitové instrukce. Podpora 32-bitových funkcí byla přidána u procesoru Intel 80386, a je stále zachována zpětná kompatibilita.

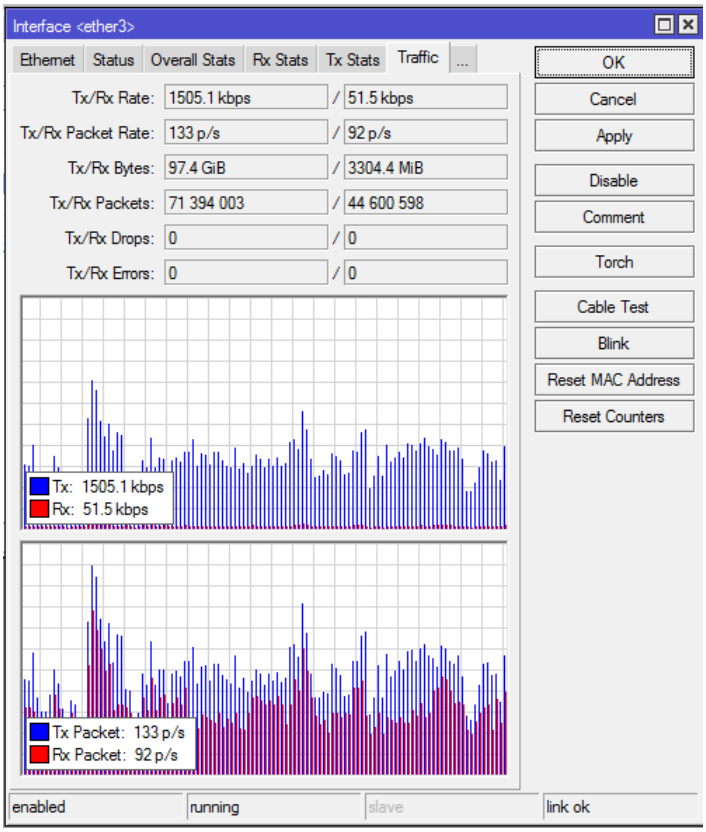
SEZNAM PŘÍLOH

A PŘÍLOHA - IMPLEMENTACE SLUŽEB V PRAXI

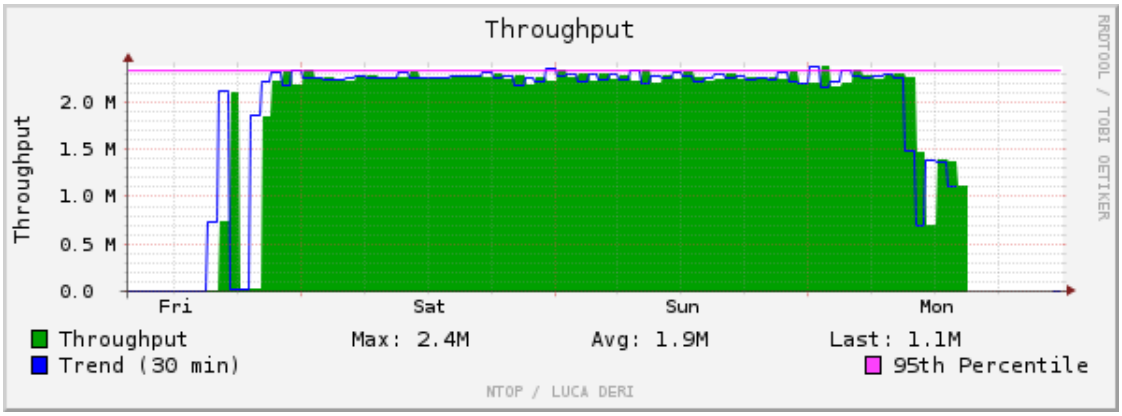
Obr. A.1: Hardware pro testování IPTV služeb



Obr. A.2: Příjem služby sledovanitv.cz využitím webového prohlížeče



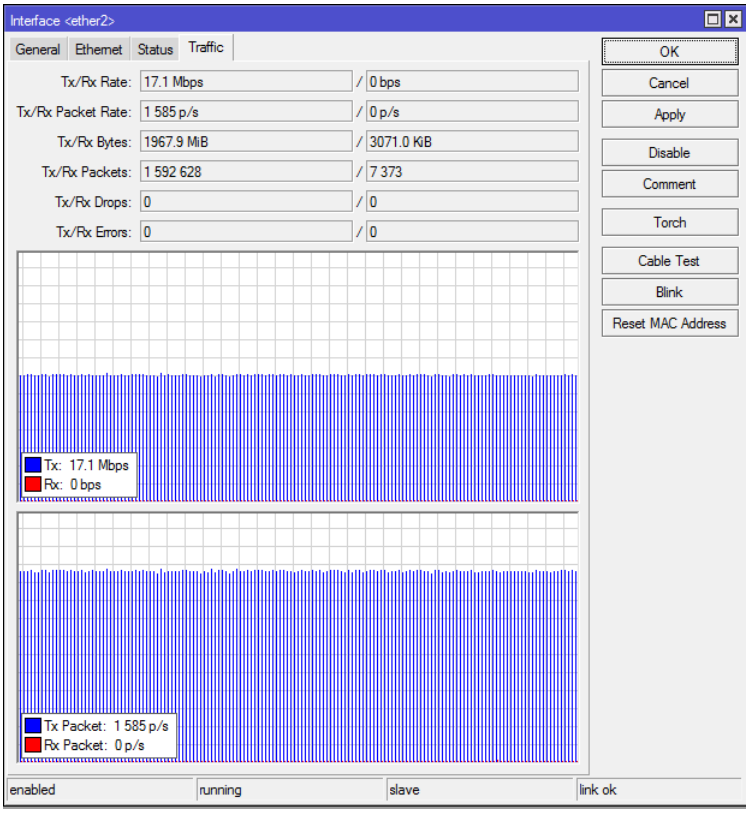
Obr. A.3: Využitá šířka pásma službou sledovanitv.cz



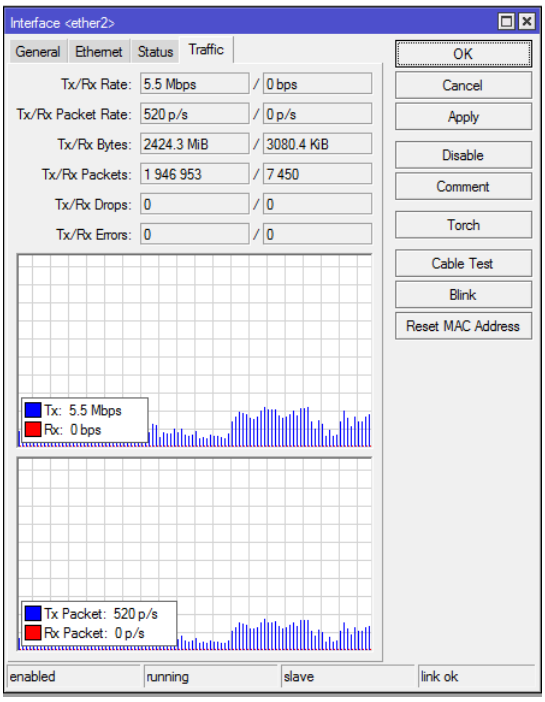
Obr. A.4: Využitá šířka pásma službou UPC Business – IPTV

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
10 AM	211.2 MBytes	1.2 %	5.4 MBytes	1.3 %
9 AM	985.1 MBytes	5.8 %	24.7 MBytes	5.8 %
8 AM	1001.6 MBytes	5.9 %	25.0 MBytes	5.8 %
7 AM	990.6 MBytes	5.8 %	25.2 MBytes	5.9 %
6 AM	981.6 MBytes	5.8 %	25.3 MBytes	5.9 %
5 AM	994.5 MBytes	5.9 %	25.3 MBytes	5.9 %
4 AM	1021.0 MBytes	6.0 %	25.6 MBytes	5.9 %
3 AM	962.3 MBytes	5.7 %	24.9 MBytes	5.8 %
2 AM	936.9 MBytes	5.5 %	23.9 MBytes	5.6 %
1 AM	1.0 GBytes	6.1 %	25.6 MBytes	6.0 %
12 AM	959.4 MBytes	5.7 %	24.2 MBytes	5.6 %
11 PM	965.5 MBytes	5.7 %	23.7 MBytes	5.5 %
10 PM	1008.8 MBytes	5.9 %	25.6 MBytes	6.0 %
9 PM	972.8 MBytes	5.7 %	25.4 MBytes	5.9 %
8 PM	986.9 MBytes	5.8 %	25.4 MBytes	5.9 %
7 PM	977.8 MBytes	5.8 %	24.6 MBytes	5.7 %
6 PM	987.5 MBytes	5.8 %	25.1 MBytes	5.8 %
5 PM	979.9 MBytes	5.8 %	24.9 MBytes	5.8 %
Total				

Obr. A.5: Objem přenesených dat službou UPC Business – IPTV v průběhu 18 hodin



Obr. A.6: Využívaná šířka pásma službou G.TV – stanice HBO HD



Obr. A.7: Využívaná šířka pásma službou G.TV – stanice Nova

B PŘÍLOHA - PŘILOŽENÉ SOUBORY NA DVD

Cesta k souboru	**Popis**
\software\winbox.exe	Nástroj pro konfiguraci zařízení s RouterOS.
\software\ispadmin-4.05-64bit-DVD.iso	Bitová kopie pro instalaci systému ISPadmin (Debian verze 6.0).
\skript\API_QoS_v1.pl	Vytvořený skript pomocí skriptovacího jazyka Perl.
\skript\RouterOSFirewallMangle.pm	Modul pro konfiguraci značkování směrovače.
\skript\RouterOSFwAddressList.pm	Modul pro konfiguraci firewallu směrovače.
\skript\Mtik.pm	Knihovna funkcí (API klient).
\diplomova_prace_130714.pdf	Přiložená práce v elektronické podobě.
\topologie.png	Existujicí heterogenní síť pro implementaci triple-play služeb a vytvořeného řešení pro zajištění kvality služeb.

Tab. B.1: Jednotlivé soubory přiložené na DVD

C PŘÍLOHA - NÁVOD K INSTALACE SYSTÉMU

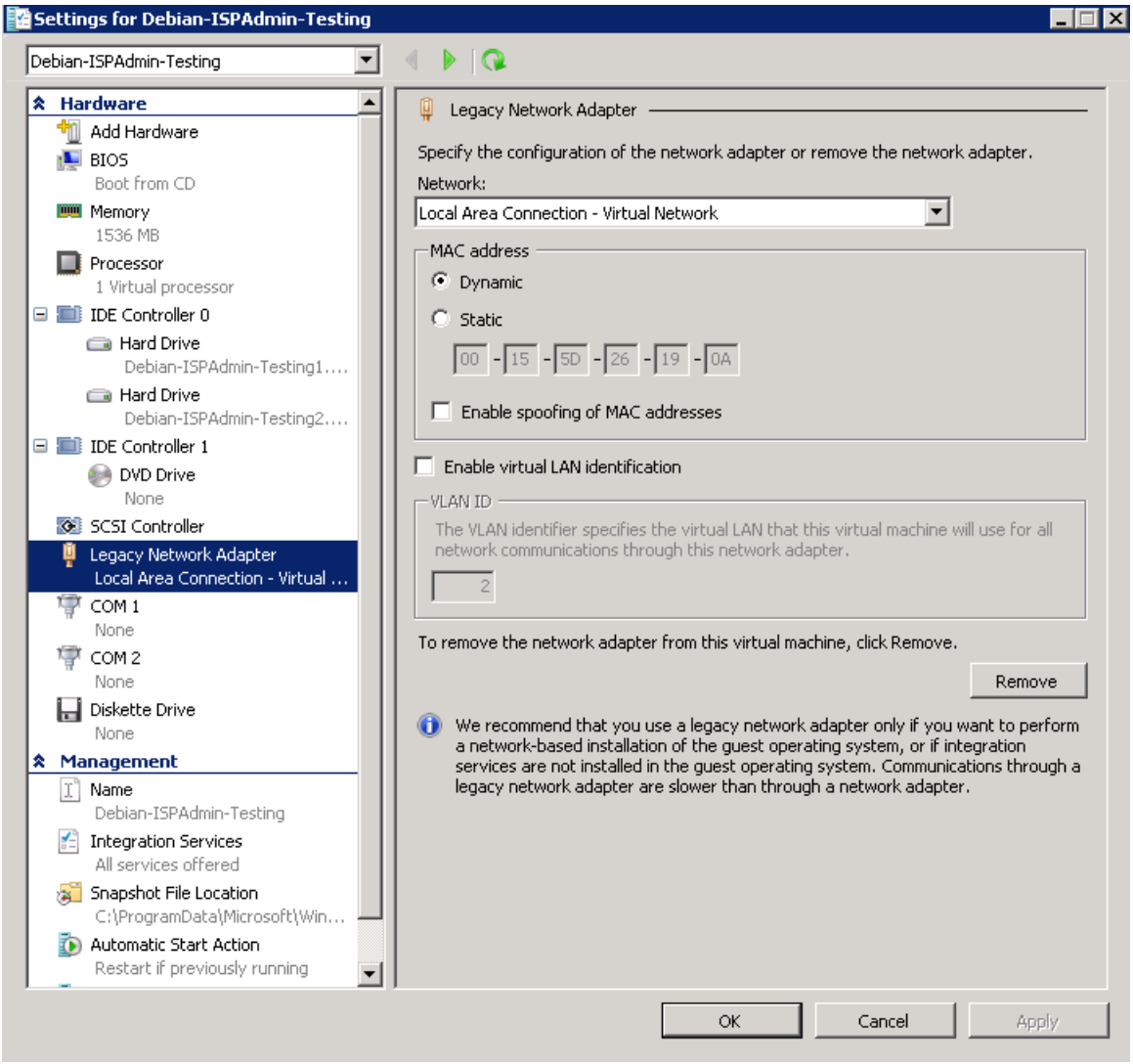
Pro možnost vyzkoušet funkčnost vytvořeného řešení, je v této příloze popsán postup pro zprovoznění serveru ISPadmin, který slouží jako zdroj dat následně využitých při konfiguraci směrovače poskytujícího kvalitu služeb. Dále je popsán postup pro využití skriptu k automatické konfiguraci síťového zařízení. Jako síťové zařízení lze využít libovolný síťový prvek výrobce MikroTik s operačním systémem RouterOS.

C.1 ISPadmin

Administrační systém ISPadmin pro správu uživatelů a síťových prvků je využíván poskytovatelem služeb (ISP), který provozuje síťovou infrastrukturu, na které bylo vytvořené řešení testované. Jedná se o komplexní systém založený na unixové distribuci Debian 6 a samotná instalace včetně potřebné konfigurace vyžaduje zhruba 1-2 hodiny času. Společnost NET Service Solution nabízí zkušební verzi systému ke stažení zdarma na svých webových stránkách:
http://download.ispadmin.eu/ispadmin-4.05-64bit-DVD.iso.
Zkušební verze je omezena limitem maximálně 10 uživatelů a 10 spravovaných směrovačů. Tento limit je pro vyzkoušení dostačující. Jako ideální volbu pro vyzkoušení považuji virtuální instalaci, např. VirtualBOX, VMware nebo ve Windows 8 Pro přímo integrované Hyper-V, které bylo využito i při tvorbě této práce. Nastavení virtuálního systému (Hyper-V):

1. Přidělenou operační pamět doporučuji nastavit alespoň 1,5 GB.
2. Kapacitu systémového disku(úložiště) minimálně 10 GB.
3. Při vytváření virtuálního systému doporučuji síťový adaptér změnit na „Legacy Network Adapter“, který nabízí vyšší kompatibilitu, viz.obr. C.1. Původně nastavený síťový adaptér vykazoval problémy při instalaci systému ISPadmin.
4. Po nastavení těchto hodnot můžeme inicializovat bitovou kopii (ISO soubor) a po zapnutí virtuálního systému uvidíme volby instalace systému ISPadmin.

Jednotlivé kroky instalace a konfigurace systému samotného jsou detailně popsány v dokumentaci připravené vývojáři systému na adrese:
http://wiki.ispadmin.eu/index.php/Documentation/Installation/Local/cs.
Pokud je instalace systému dle uvedeného návodu dokončena, doporučuji využít SSH klienta (např. putty) pro připojení k systému na IP adrese, které byla nakonfigurována na síťové rozhraní systémů v průběhu instalace. V případě, že instalace proběhla v pořádku, připojíme se k systému a uvidíme v okně terminálu uvítací zprávu, viz. obr. C.2. Pokud se nelze k systému klientem SSH připojit zkontrolujeme nastavení firewallu serveru pomocí příkazu „**iptables -L**“. Pokud firewall



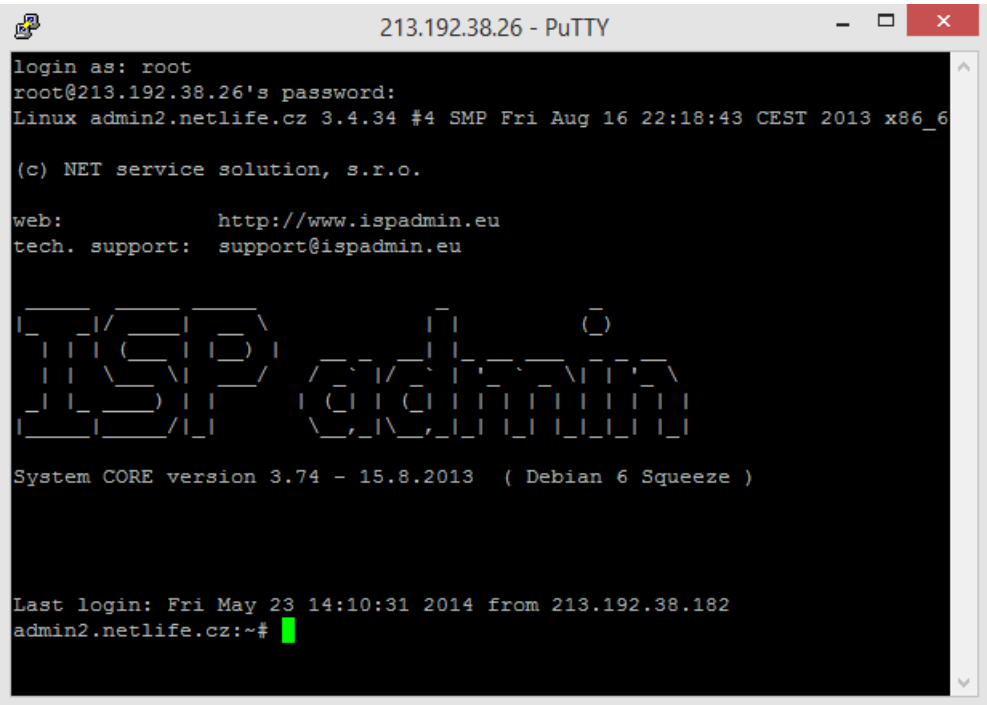
Obr. C.1: ISPadmin – Nastavení parametrů testovacího virtuálního systému.

implicitně obsahuje nakonfigurované pravidla po instalaci, doporučuji je smazat příkazem „**iptables -F**“.

Nyní by již nic nemělo bránit připojení pomocí SSH klienta. Po ověření funkčnosti serveru spustíme webové rozhraní a přihlásíme se pomocí přihlašovacích údajů uvedených v návodu pro instalaci.

Do systému je nutné vyplnit alespoň několik základních údajů:

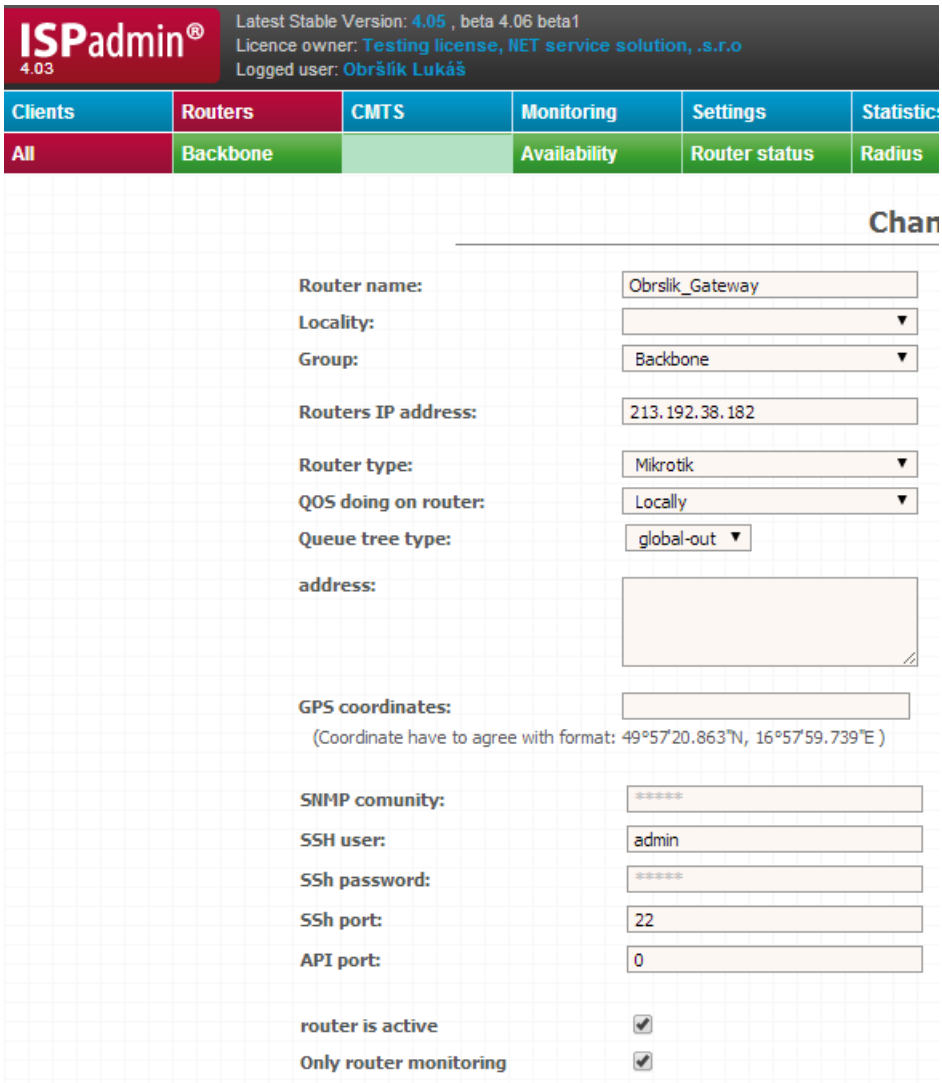
1. **IP rozsah** – Systému je nutné říci, jaký rozsah IP adres budou používat uživatelé na jednotlivých směrovačích.
   Nejprve je nutné v sekci „Settings/Codebooks/IP Ranges“ přidat námi zvolený rozsah IP adres (např. 172.16.0.0/24).
2. **Směrovač** – Do části „Routers“ přidáme směrovač. Vyplnit musíme IP ad-



Obr. C.2: ISPadmin – Terminálové okno po přihlášení k systém.

resu, typ směrovače a přihlašovací údaje nakonfigurované na síťovém zařízení a zaškrtneme pole „Only router monitoring“, viz. obr. C.3. Zajistíme tak, že nebude do zařízení systém zapisovat žádnou konfiguraci. ISPadmin bude tedy sloužit pouze jako zdroj dat pro konfiguraci. Pokud máme směrovač přidaný přiřadíme rozsah IP adres ke směrovači. Slouží k tomu druhá záložka na přidaném směrovači (Routed Network). V horní části nabídky zvolíme „Add IP range“ pro přidání rozsahu. V nabídce pro přidání vyplníme adresu sítě, masku, a pole „default router“, které určuje IP adresu, která bude nakonfigurovaná na rozhraní nastavovaného směrovače, tedy výchozí brána pro připojené uživatele. Také zvolíme typ (veřejný/privátní) a pro koho je vybraný rozsah určen (např. WIFI/LAN) viz. obr. C.4.

3. **Uživatel** – Máme-li v systému přidaný rozsah IP adres, směrovač a k němu daný IP rozsah přiřazen, můžeme vytvořit uživatele v části „Clients“. Vyplníme povinná pole označená hvězdičkou a ponecháme systémem vybrané unikátní identifikátor ID. Pokud je uživatel v systému první, bude ID rovno 1.
4. **Služba** – Dále otevřeme nabídku pro vytvořeného uživatele a zvolíme **Active services**. Vybereme **Add new service** a možnost „Internet“. Musíme zvolit typ fakturace (např. **don't invoice** pro vypnutí). Nastavíme parametry poskytovaného tarifu (download/upload) a vybereme z nabídky **Router** námi nadefinovaný směrovač a níže také IP adresu. Tímto jsme nadefinovali po-



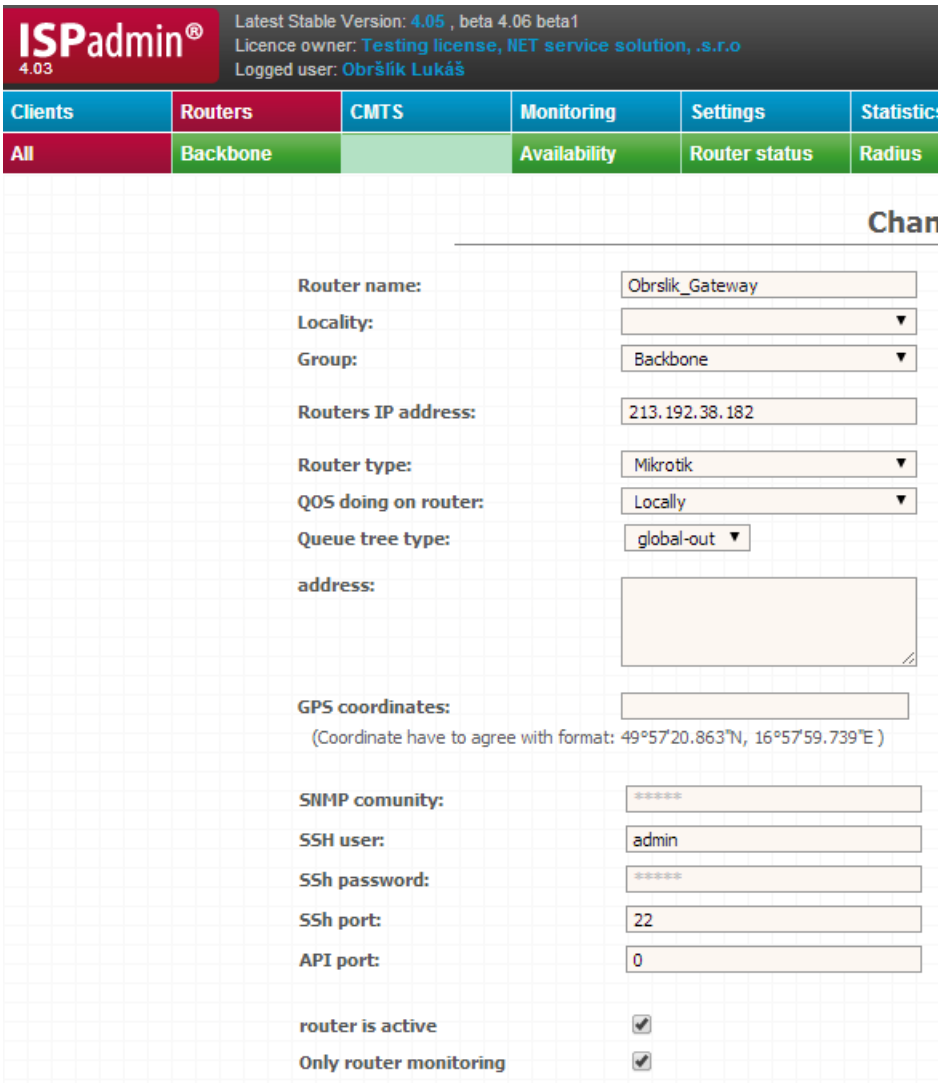
Obr. C.3: ISPadmin – Přidání směrovače do systému.

třebné údaje pro jednoho uživatele. Opakováním postupu tohoto posledního bodu můžeme přidat uživatelů více (není nutné).

5. **Kapacita linky** – Obdobně jako jsme přiřadili IP rozsah ke směrovači, nastavíme také kapacita linky směrovače směrem do internetu. Hodnotu je nutné zapsat do v záložce **Queue trees** do pole „Description“. Pole QueueID není prozatím využito.

C.2 Nastavení zařízení s RouterOS

K otestování zařízení potřebujeme připravený směrovač, přes který jsou přenášena data námi vytvořeného uživatele (nebo více uživatelů). Konfigurace směrovače je uvedena na přiloženém výpisu z konfigurace C.4. Nakonfigurovat je nutné IP adresu



Obr. C.4: ISPadmin – Přidání IP rozsahu ke směrovači.

rozhraní, výchozí bránu a překlad adres, protože privátní adresy by nebylo možné směrovat v internetu.

Do takto připraveného směrovače můžeme připojit libovolný směrovač s vlastním překladem adres, který bude představovat koncového uživatele. Na server ISPadmin přeneseme protokolem FTP vytvořený skript a knihovny (vše umístíme do stejného adresáře):

- API_QoS_beta.pl,
- Mtik.pm,
- RouterOSFirewallMangle.pm,
- RouterOSFwAddressList.pm.

Ve skriptu je nutné upravit přihlašovací údaje do databáze MySQL systému ISPadmin a údaje pro přihlášení ke směrovači pomocí API. Pokud jsme uvedený postup provedli správně, můžeme spustit skript s parametrem směrovače, který chceme konfigurovat, jak je uvedeno na obr. 2.17.

```
# may/24/2014 01:32:18 by RouterOS 6.12
# software id = Y4RM-7BPG
/ip address
add address=213.192.38.182/30 comment=WAN interface=ether3 network=\
    213.192.38.180
add address=172.16.0.1/24 comment=Clients interface=ether1 network
    =172.16.0.0
/ip dns
set max-udp-packet-size=512 servers=192.168.3.1,8.8.8.8
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether3
/ip route
add distance=1 gateway=213.192.38.181
```

Zdrojový kód C.1: RouterOS – Základní konfigurace.

Postup pro přídání uživatelů, směrovačů a dalších dat do systému ISPadmin je dostupný v dokumentaci vývojářů:
http://wiki.ispadmin.eu/index.php/Documentation/Implementation