

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

SIMULAČNÍ MODEL IPTV SLUŽBY S PROTOKOLEM RTP

DIPLOMOVÁ PRÁCE  
MASTER'S THESIS

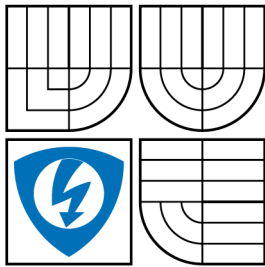
AUTOR PRÁCE  
AUTHOR

BC. ALEŠ LEŽÁK

BRNO 2008



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

## SIMULAČNÍ MODEL IPTV SLUŽBY S PROTOKOLEM RTP IPTV MULTICAST MODEL WITH RTP PROTOCOL

DIPLOMOVÁ PRÁCE  
MASTER'S THESIS

AUTOR PRÁCE  
AUTHOR

BC. ALEŠ LEŽÁK

VEDOUCÍ PRÁCE  
SUPERVISOR

ING. MILAN ŠIMEK

BRNO 2008

# Diplomová práce

magisterský navazující studijní obor  
Telekomunikační a informační technika

**Student:** Ležák Aleš, Bc.

**Ročník:** 2

**ID:** 88538

**Akademický rok:** 2007/08

**NÁZEV TÉMATU:**

## Simulační model IPTV služby s protokolem RTP

**POKyny PRO VYPRACOVÁNÍ:**

Seznamte se s možnostmi simulace multicastových operací ASM a SSM v prostředí Opnet Modeller a navrhnete model služby IPTV. V zadaném simulačním nástroji vytvořte simulační model IPTV služby z multicastovým přenosem dat. Simulujte RTP/RTCP relaci s velkým počtem uživatelů a na výstupních charakteristikách prezentujte závislost frekvence přenosu kontrolních RTCP paketů na počtu uživatelů. Pro simulaci použijte reálné parametry IPTV služby. Pro simulační model také vytvořte aplikační blok IPTV služby.

**DOPORUČENÁ LITERATURA:**

- [1] M.A. SPORCTAK, Směrování v sítích IP, ComputerPress, a.s., 2004, ISBN: 80-251-0127-4
- [2] Opnet Technologies Inc., "Opnet Modeller", [online], Opnet Technologies Inc. 2001, dostupné na <www.opnet.com>

**Termín zadání:** 11.2.2008

**Termín odevzdání:** 28.5.2008

**Vedoucí projektu:** Ing. Milan Šimek

prof. Ing. Kamil Vrba, CSc.  
předseda oborové rady



**UPOZORNĚNÍ:**

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

ZDE VLOŽIT PRVNÍ LIST LICENČNÍ  
SMOUVY

Z důvodu správného číslování stránek

## **ABSTRAKT**

Tato diplomová práce se zabývá především problematikou simulace multicastových přenosů ASM v prostředí Opnet Modeler a simulací služby IPTV. V simulačním nástroji byl vytvořen simulační model IPTV s multicastovým přenosem dat. Tento způsob přenosu dat podporuje skupinové vysílání. To si lze představit jako komunikaci jednoho zdroje dat s velkým počtem příjemců stejných dat. Hlavním cílem této technologie je zmenšení zátěže zdrojového uzlu a přenosové soustavy při distribuci dat skupině příjemců. Nejčastěji se používá multicast v oblasti distribuce vysílání audio a video signálu. Známe dva druhy multicastu - ASM a SSM. Zde je však použit pouze model ASM. Simulována je relace RTP/RTCP s větším počtem uživatelů a je sledován interval zasílání kontrolních RTCP paketů. Toho je docíleno dvěma způsoby, které jsou v závěru srovnány. A to sice teoretickým výpočtem podle vzorce a praktickou simulací v nástroji Opnet Modeler.

## **KLÍČOVÁ SLOVA**

ASM, Multicast, IPTV, RTP/RTCP, Opnet Modeler, Simulace.

## **ABSTRACT**

This diploma thesis contains questions of simulation data transfer by ASM multicast. In simulation tool Opnet Modeler is proceed design of service IPTV. IPTV means television which is transfered in network by IP protocol. Data of IPTV service are sending by multicast transfer. Multicast is a technology which uses a group transfer. It is actually communication of a one source of data with many users. These users are receiving the same data. A main target of this technology is to decrement loading of source node and transference system in distribution of data towards group of users. Most often is multicast used in distribution of audiovisual data. Relation RTP/RTCP is simulated with a different numbers of users. Observed is interval of transmission of control RTCP packets. This will be reached by two methods which will be confront in the end. One is a theoretic calculation by course of a equation and second is a practical simulation in Opnet Modeler.

## **KEYWORDS**

ASM, Multicast, IPTV, RTP/RTCP, Opnet Modeler, Simulation.

LEŽÁK A. *Simulační model IPTV služby s protokolem RTP*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 53 s. Vedoucí diplomové práce Ing. Milan Šimek..

## PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Simulační model IPTV služby s protokolem RTP“ 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 jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne .....

.....

(podpis autora)



# OBSAH

<b>1</b>	<b>Úvod</b>	<b>12</b>
<b>2</b>	<b>Multicast</b>	<b>13</b>
<b>3</b>	<b>Adresy pro multicast</b>	<b>14</b>
<b>4</b>	<b>Modely multicastu a protokoly podporující multicastové vysílání</b>	<b>16</b>
4.1	ASM . . . . .	16
4.1.1	PIM-SM . . . . .	16
4.1.2	IGMP . . . . .	17
4.2	SSM . . . . .	21
4.2.1	PIM-SSM . . . . .	21
4.2.2	IGMPv3 . . . . .	22
<b>5</b>	<b>Způsob směrování v multicastu</b>	<b>24</b>
5.1	Požadavky na efektivní skupinové vysílání . . . . .	24
5.2	Průběh směrování . . . . .	24
<b>6</b>	<b>Multimediální protokol RTP/RTCP</b>	<b>26</b>
6.1	Služby RTP . . . . .	27
6.2	Architektura RTP . . . . .	27
6.3	Datový paket . . . . .	27
6.4	Kontrolní paket . . . . .	28
<b>7</b>	<b>Zajištění QoS IPTV</b>	<b>30</b>
<b>8</b>	<b>Simulace v prostředí OPNET Modeler</b>	<b>32</b>
8.1	Seznámení s OM . . . . .	32
8.2	Vytvoření modelu sítě . . . . .	33
8.2.1	Nastavení síťových prvků . . . . .	35
8.2.2	Nastavení aplikací . . . . .	38
8.2.3	Přiřazení aplikace na straně příjemce . . . . .	38
8.2.4	Nastavení aplikace na straně odesílatele - serveru . . . . .	39
8.3	Simulace modelu IPTV služby s multicastovým přenosem dat . . . . .	39
8.4	Porovnání výstupu simulace zpoždění RTP protokolu s výpočtem dle vzorce 6.1 . . . . .	42
8.5	Zatížení páteřní linky při přenosu dat multicastem a unicastem . . . . .	43
<b>9</b>	<b>Závěr</b>	<b>48</b>

<b>Literatura</b>	<b>49</b>
<b>Seznam symbolů, veličin a zkratk</b>	<b>51</b>

# SEZNAM OBRÁZKŮ

2.1	Multicast	13
4.1	Any Source Multicast	17
4.2	IGMP protokol v datagramu IP	18
4.3	IGMPv1	18
4.4	IGMPv2	19
4.5	Source Specific Multicast	21
5.1	Vytvoření multicastového okruhu	25
5.2	Odstranění multicastového okruhu pomocí RPF	25
6.1	Architektura protokolu RTP	26
6.2	Formát záhlaví datového paketu RTP	28
8.1	Navržená síť	33
8.2	Podsít Brno	34
8.3	Podsít Praha	34
8.4	Podsít Maleč	35
8.5	Povolení multicastového provozu na uživatelské stanici	35
8.6	Povolení RIP protokolu na rozhraních směrovače	36
8.7	Nastavení parametrů IGMP protokolu na směrovačích	36
8.8	Povolení protokolu PIM-SM	37
8.9	Nastavení módu a verze protokolu PIM	37
8.10	Konfigurace RP na směrovači	38
8.11	Objem přijatých a vyslaných dat protokolem RTP. Výstup z programu Opnet Modeler.	41
8.12	Nastavení aplikace IPTV.	41
8.13	Zpoždění protokolu RTP pro 20 uživatelů. Výstup z programu Opnet Modeler.	43
8.14	Grafická závislost intervalu odesílání RTCP Feedback Report paketů na počtu uživatelů	44
8.15	Propustnost linky ve směru Brno - Maleč, přenos unicastem. Výstup z programu Opnet Modeler.	45
8.16	Propustnost linky ve směru Brno - Maleč, přenos multicastem. Výstup z programu Opnet Modeler.	46
8.17	Propustnost linky ve směru Brno - Praha, přenos unicastem. Výstup z programu Opnet Modeler.	47
8.18	Propustnost linky ve směru Brno - Praha, přenos multicastem. Výstup z programu Opnet Modeler.	47

## SEZNAM TABULEK

3.1	Adresy třídy D . . . . .	15
8.1	Parametry simulace . . . . .	40
8.2	Vypočítané hodnoty zpoždění RTCP paketu . . . . .	42
8.3	Nasimulované hodnoty zpoždění RTCP paketu . . . . .	43

# 1 ÚVOD

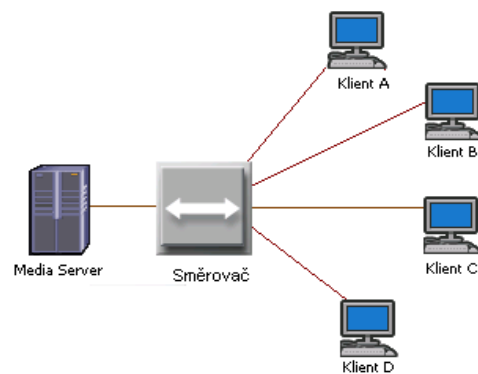
Tato diplomová práce se zabývá službou IPTV, tzn. streamovaným vysíláním audiovizuálních dat přes internetovou síť s podporou protokolu RTP. Toto vysílání je realizováno multicastovým přenosem, což je vlastně technologie skupinového vysílání. Tato technologie byla vyvinuta především pro podporu aplikací obsahujících komunikaci jednoho zdroje s velkým počtem příjemců stejných dat. Hlavním cílem této technologie bylo zmenšení zátěže zdrojového uzlu a přenosové soustavy při distribuci dat skupině příjemců. Nejčastěji se používá multicast v oblasti distribuce vysílání audio a video signálu, videokonference, vyhledávání služeb, či distribuované simulace.

Jsou zmíněny i druhy multicasu, jakými jsou ASM (Any Source Multicast) a SSM (Source Specific Multicast) a možnost jejich simulace v nástroji Opnet Modeleru. Další část bude věnována multicastovému protokolu PIM (Protocol Independent Multicast), díky kterému se uživatelé přihlašují k příjmu multicastového vysílání, a který se využívá mezi směrovači k směrování multicastového provozu přes IP síť. Další nezbytnou součástí multicastového přenosu dat je protokol zajišťující sestavení multicastových skupin IGMP (Internet Group Management Protocol). Ten se využívá mezi klienty a LAN a dále ke směrovači, umožňuje tak klientům přihlásit se do multicastové skupiny.

Hlavním předmětem zájmu je však multimediální protokol RTP (Real Time Protocol), který je určen pro multimediální přenosy a RTCP (Real Time Control Protocol) protokol pro přenos signalizace a synchronizace toku dat. Vlastnosti tohoto protokolu jsou zkoumány na navrženém simulačním modelu služby IPTV v simulačním nástroji Opnet Modeler. U RTCP protokolu je sledována frekvence přenosu kontrolních paketů v závislosti na počtu uživatelů v navrženém modelu sítě. Je zde porovnáno i zatížení páteřní linky mezi přenosem podporovaným multicasem a unicastem.

## 2 MULTICAST

Multicast [3] je mechanismus směrování IP paketu, který zabezpečí, že paket vyslaný odesílatelem bude doručený každému příjemci z dané skupiny (jedná se o princip tzv. „best effort“ - viz obr. 2.1). Tato skupina se nazývá multicastová skupina. V rámci jedné multicastové skupiny jde například přijímat video vysílané do této skupiny streaming serverem. Aby mohl uzel přijímat data poslané do multicastové skupiny, musí být jejím členem.



Obr. 2.1: Multicast

Multicast je integrální součástí protokolu IP (Internet Protocol). Internet Protocol Multicast je technologie, která slouží k efektivnímu využití šířky pásem pro situace, kdy jeden vysílač distribuuje informaci (např. internetové rádio, videokonference, IP TV atd.) tisícům příjemců.

### 3 ADRESY PRO MULTICAST

Když chce stanice vyslat data více uživatelům, například pěti, jedním z řešení by bylo vytvořit pět nezávislých spojení a poslat data každé stanici zvlášť. Ale stejně tak, jako roste počet příjemců, snižuje se efektivita. Proto se zavedl nový typ adresy - skupinová adresa, která označuje všechny členy dané skupiny. Na první pohled se multicastový paket v ničem neliší od běžného unicastového. Jediný rozdíl je v tom, že pro tyto multicastové adresy jsou vyhrazené adresy z třídy D: 224.0.0.0 až 239.255.255.255. Tyto adresy se poznají tak, že první čtyři bity 1110 identifikují multicastový paket a dalších 28 bitů určuje, pro kterou multicastovou skupinu je daný uzel určený. Tyto adresy jsou určeny pouze pro cílovou adresu datagramu nesoucího data pro členy multicastové skupiny. Zdrojová adresa je běžná unicastová směrovatelná IP adresa. Zdroj nemusí být členem skupiny, což znamená, že stanice může poslat paket do jakékoliv skupiny a nezáleží na tom, jestli je, nebo není jejím členem. Takovéto skupiny nazýváme otevřené. Členství ve skupině je dynamické, stanice se můžou přihlásit a odhlásit ze skupiny podle potřeby a stanice může patřit do více skupin najednou. Počet členů ve skupině není omezený.

Organizace IANA rozdělila adresní prostor pro multicast následovně:

- 224.0.0.0 až 224.0.0.255 jsou určeny pro lokální použití, například 224.0.0.5 je adresa všech lokálních OSPF směrovačů.
- Pro globální použití jsou potom určeny adresy z rozsahu 224.0.10.0 až 238.255.255.255.

Následující tabulka 3.1 je částečný záznam dobře známých adres třídy D, které jsou rezervované pro IP multicasting registrované v organizaci IANA (Internet Assigned Numbers Authority).

Multicast adresy	Popis
224.0.0.0	Základní adresa
224.0.0.1	Všichni uživatelé multicastové skupiny na stejném síťovém segmentě
224.0.0.2	Všechny směrovače multicastové skupiny na stejném síťovém segmentě
224.0.0.5	OSPF směrovače
224.0.0.6	Používá se na posílání OSPF směrovacích informací na OSPF vyhrazené směrovače v síťovém segmentě
224.0.0.9	RIP v.2 skupinová adresa. Používá se k zaslání RIP směrovacích informací do všech RIP v.2 směrovačů v síťovém segmentě
224.0.0.10	EIGRP skupinová adresa. Používá se k zaslání EIGRP směrovacích informací do všech EIGRP směrovačů v síťovém segmentě
224.0.0.22	IGMP v3

Tab. 3.1: Adresy třídy D

Kompletní seznam rezervovaných IP multicastových adres, přidělených organizací IANA je k dispozici na [13].

## 4 MODELY MULTICASTU A PROTOKOLY PODPORUJÍCÍ MULTICASTOVÉ VYSÍLÁNÍ

Existují dva druhy modelů skupinového vysílání - multicastu. Jsou jimi ASM, SSM. Tyto modely budou popsány v následující kapitole. Dále budou zmíněny protokoly užívající se pro daný druh multicastu - ASM, či SSM.

### 4.1 ASM

Pro multicastové přenosy ASM [5] je nutno vytvořit složitou strukturu směrování. Multicastový provoz je rozdělený do skupin a to pomocí protokolu IGMP. Ten to ohlásí nejbližšímu směrovači, který spolupracuje s ostatními směrovači a zabezpečí vytvoření distribučního stromu. Stanice pošle pouze data se skupinovou adresou směrovači a ten musí zařídit nasměrování. Stanice se můžou přihlašovat a odhlašovat ze skupiny kdykoliv. Odesílatelů může být i více a nemusí být členy skupiny.

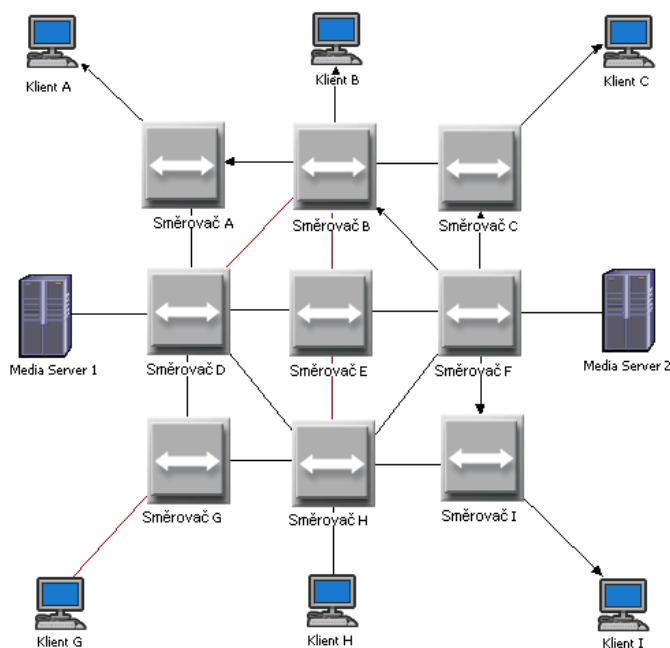
ASM používá sdílený strom, který má kořen v porovnání se zdrojovým stromem, vždy na jednom místě nezávisle na tom, kdo data posílá, tedy na zdroji. Strom tu popisuje tok dat skupině. Někdy se kořen označuje jako RP - Rendezvous Point a je realizovatelný na nějakém směrovači v síti. Proto se tyto stromy nazývají RP stromy. Vysílající posílá pakety na RP a každý zájemce o příjem dané multicastové skupiny si prostřednictvím svého nejbližšího směrovače pošle žádost o zasílání paketů z RP. Pakety jsou posílány pouze tam, kde je o ně zájem. S prvním přijatým paketem zjistí směrovač příjemců, odkud se vysílá a může žádat o příjem optimální cestou přímo od zdroje a zrušit příjem přes RP. Rendezvous Point v tomto případě může sloužit pouze k oznámení, tzn. příjemcův směrovač se dozví, odkud se vysílá. Tento mechanismus vytváří z multicastu ASM (viz obr. 4.1) složitý a nesnadno realizovatelný systém.

Tento způsob přenosu je vhodný pro on-line hry, hlasové a video konference, sdílení elektronických tabulí, tj. kdy se někteří z účastníků střídají jako zdroje dat.

V dalších několika odstavcích se budeme zabývat protokoly, které se pro daný druh multicastu (ASM) užívají. Jsou jimi PIM-SM a dvě verze protokolu IGMP - IGMPv1 a IGMPv2.

#### 4.1.1 PIM-SM

Protokol PIM-SM (Protocol Independent Multicast - Sparse Mode) patří mezi sparse mode protokoly [5]. V těchto protokolech jsou využity sdílené stromy, které jsou zde užity pro rozesílání multicastových dat. Tyto stromy využívají tzv. pull model, který předpokládá, že se data nesmějí poslat do sítě, aniž by si je někdo vyžádal. Pro připojení uživatele do multicastové skupiny musí jeho příslušný router poslat zprávu



Obr. 4.1: Any Source Multicast

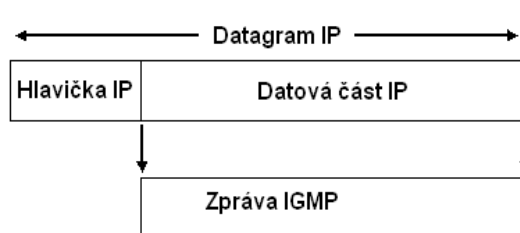
join a to sice směrem ke kořenu stromu. Toto je způsob, jakým je sestavena další větev stromu a díky tomu mohou data proudit dále. Důležitou vlastností zprávy join je, že je časově omezena. Musíme ji proto obnovovat. Jestliže dojde k situaci, že se v dané větvi nenachází žádný příjemce skupiny, router vyšle zprávu graft, kterou větev „odřízne“.

Díky zavedení sparse mode protokolů se šetří vypočetní výkon routerů. Když dojde k situaci, že se vyskytne více přispěvovatelů do skupiny, musí dense mode protokoly počítat strom pro každého zvláště. Toto se však u sparse mode protokolů nemusí, avšak může být jejich směrování méně efektivní, a proto je tedy za potřeby velice pečlivě volit Rendezvous Point.

### 4.1.2 IGMP

V této kapitole se budeme zabývat obecně protokolem IGMP [6]. Budou nás zajímat jeho verze 1 a 2, které jsou používány pro tento druh multicastu - ASM. IGMP je protokol, který spravuje členy skupin mezi klienty a nejbližším směrovačem. Rovněž zajišťuje šíření adresných oběžníků (tj. multicastu). IGMP je využíván systémy, které pracují s protokolem IP verze 4 a to pro oznámení svého členství ve skupině multicastového přenosu okolním směrovačům. Směrovač může být buďto členem multicastové skupiny, anebo může zajišťovat multicastové přenosy pro jiné skupiny.

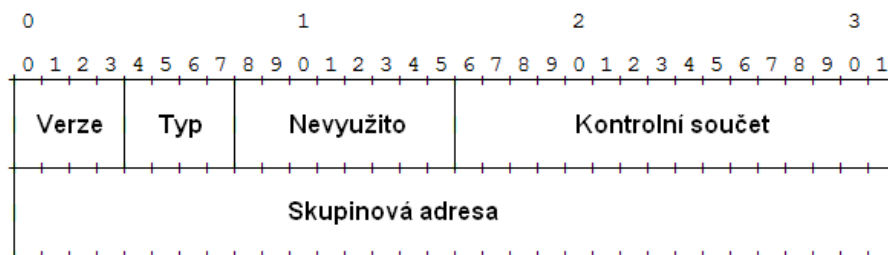
Zprávy protokolu IGMP jsou před odesláním zahrnuty do datagramů IP, jak je znázorněno na následujícím obrázku 4.2



Obr. 4.2: IGMP protokol v datagramu IP

### IGMPv1

Formát IGMPv1 zprávy je na následujícím obrázku 4.3. Tato sekvence osmi bitů následuje hned po IP hlavičce:



Obr. 4.3: IGMPv1

Význam jednotlivých políček v obrázku 4.3:

- Verze - aktuální verze protokolu (1),
- Typ - verze 1 podporuje pouze dva typy zpráv a to:
  - Membership Query, kód 1,
  - Membership Report, kód 2.
- Nevyužito - při posílání by mělo být nastaveno na 0 a při příjmu ignorováno,
- Kontrolní součet - kontrolní součet IGMP zprávy,

- Skupinová adresa - u zprávy Membership Report obsahuje toto pole multicastovou adresu, jinak by mělo být nastaveno na 0.0.0.0..

Tento protokol má jednoduché schéma Query-Report. Klient musí pro připojení do multicastové skupiny udělat následující. Nejdříve musí poslat zprávu typu Membership Report s vyplněným číslem skupiny na adresu té skupiny. Příslušný router by ji měl zachytit a postarat se i o zprostředkování. Router si rovněž průběžně kontroluje členství klientů ve skupinách a jednou za 60 sekund pošle zprávu typu Membership Query a to na adresu 224.0.0.1. a dále čeká na Reporty od klientů. Existuje možnost, že se v síti vyskytne více klientů pro jednu skupinu. Proto byl navržen mechanismus, jenž zaručí to, že pro každou skupinu dorazí jenom jeden Report. Každý z klientů, který zachytí Query, si zvolí náhodné číslo z rozsahu 0 až 10. Toto číslo vyjadřuje číslo v sekundách. Je to doba, za kterou chce poslat Report. Zároveň ale poslouchá, jestli nějaký jeho kolega Report pro danou skupinu pošle. Je-li tomu tak, klient už nic neposílá.

Nastane-li případ, že klient danou skupinu opustí, dojde k tomu, že přestane odpovídat na Query. Když router neobdrží pro skupinu třikrát po sobě žádný Report, dále ji neposílá. Query se posílá obvykle jednou za 60 sekund. Tzn., že v nejhorším případě router odesílá data ještě další tři minuty potom, co už nejsou žádaná. Tento mechanismus je vhodné použít zejména, pokud klient často mění své členství ve skupinách.

## IGMPv2

Zprávy IGMPv2 vypadají poněkud odlišně, než v předchozí verzi, protože obsahují jiná políčka. To je vidět na obr. 4.4:



Obr. 4.4: IGMPv2

Jejich význam je následující:

- Typ - hodnoty pole se volí tak, aby bylo možné rozeznat zprávy IGMPv1, které na tomto místě mají dvě políčka a to verzi a typ. Protokol rozeznává následující typy zpráv:
  - Membership Query - vlastně jsou dvě, General Query a Group-specific Query, rozlišení se dělá podle obsahu políčka Skupinové adresy, číselný kód zprávy je 11, tedy zpráva vypadá podobně jako IGMPv1 Query,
  - IGMPv1 Membership Report - pro zpětnou kompatibilitu, kód zprávy 12,
  - IGMPv2 Membership Report, kód 16,
  - Leave Group, kód 17,
- Max. doba odezvy - používá se u Query zprávy a označuje maximální čas na zaslání reportu v desetinách sekundy. Mechanismus je stejný jako u IGMPv1,
- Kontrolní součet - kontrolní součet IGMP zprávy,
- Skupinová adresa - u zpráv Membership Report, Leave Group a Group-specific Query obsahuje toto pole multicastovou adresu, jinak by mělo být 0.0.0.0. Z toho je vidět, že zpráva General Query u IGMPv2 je až na pole Max. doba odezvy shodná s Membership Query u IGMPv1.

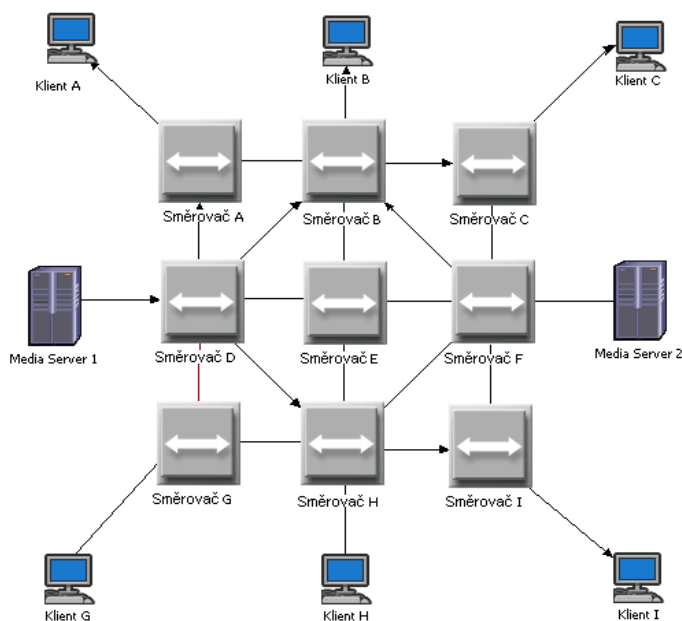
Signalizace přihlášení do multicastové skupiny je podobná jako u verze IGMPv1. Liší se pouze procesem pro opuštění skupiny. Klient posílá zprávu Leave Group. Router na ni zareaguje posláním Group-specific Query do dané skupiny. Maximální doba odezvy je obvykle nastavena na 1 sekundu. Zůstal-li ještě někdo ve skupině, tak odpoví a router pokračuje v posílání dat.

Další odlišností je volba routeru, který posílá Query. Pro posílání Query sítě je vybrán router s nejvyšším IP. Ostatní mohou jenom naslouchat a být připravený pro převzetí jeho role. Mechanismus funguje tak, že když router uslyší Query zprávu od routeru s vyšším IP, tak přestane ty své sám posílat. Čeká dále 400 sekund, jestli nepřijde další. Nepřijde-li, vyhodnotí situaci tak, že vybraný server již nadále nefunguje a začne posílat Query sám, což má za následek nové volby. V IGMPv2 se Query pošle jednou za 125 sekund.

IGMPv2 je zpětně kompatibilní s IGMPv1. Pokud dojde k situaci, že klienti rozpoznají IGMPv1 router podle jeho Query, začnou rovněž odesílat zprávy taky v IGMPv1 a nastaví si časovač na 400 sekund. Po uplynutí nastaveného intervalu začnou opět posílat IGMPv2. Naopak server je schopný obsloužit směsicí IGMPv1 i IGMPv2 klientů. Je tomu tak, protože dokáže rozlišit jejich zprávy. IGMPv1 klienti nepoznají žádný rozdíl. Detekuje-li router IGMPv1 klienty na síti, ignoruje Leave Group zprávy.

## 4.2 SSM

Tento způsob přenosu (viz obr. 4.5) je odvozen od ASM. Lze jej použít pouze v případě, kdy je v síti přesně definován zdroj dat (např. při příjmu již zmíněného internetového rádia či televize). Případný jiný zdroj vysílající na stejnou multicastovou adresu (např. jiná rádiová stanice) není přijímán. Toto je zajištěno na straně příjemců dat tak, že poskytnou dva typy adres: multicastovou adresu (adresa multicastové skupiny, ze které chce příjemce přijímat data) a unicastovou adresu (adresa konkrétního zdroje). Unicastovou adresu zdroje lze například provést výběrem na webové stránce rádiového vysílání. SSM má výhodu ve své jednoduchosti a v menší realizační náročnosti. Více na [4].



Obr. 4.5: Source Specific Multicast

V této kapitole budou dále zmíněny protokoly podporující SSM. Jsou jimi PIM-SSM a IGMPv3.

### 4.2.1 PIM-SSM

PIM-SSM je rozšířením PIM protokolu [8]. Užitím SSM může klient přijímat multicastové vysílání přímo od zdroje. PIM-SSM používá funkčnost PIM-SM k vytvoření SPT (Shortest Path tree) mezi příjemcem a zdrojem. Avšak tento strom s nejkratší cestou bude bez RP (Rendezvous Point). Dle standardu SSM skupinová multicast

adresa je omezená jistým rozsahem IP adres a to od 232.0.0.0 do 232.255.255.255. Nicméně lze jej rozšířit na adresy skupiny D.

Užití je snadné. Je potřeba nakonfigurovat pouze PIM-SM na všech rozhraních směrovače a otázka nutnosti SSM příkazů, které zahrnují specifikaci IGMPv3 v síti příjemce. Není-li PIM-SM explicitně nakonfigurován na obouh (zdrojových a skupinových) rozhraních uživatele, pakety multicastu nebudou přeposlány. Tabulka se seznamem zdrojů, podporována IGMPv3 je užitá v PIM-SSM. Zdroji se stanou aktivními a odesílají multicastové pakety. Příjemci zahrnutí v SSM skupině přijímají multicastové pakety.

## 4.2.2 IGMPv3

Tato verze protokolu IGMP [7] se snaží řešit následující problém. Uživatel je členem jisté multicastové skupiny a dojde k tomu, že nechce přijímat data od všech zdrojů, ale pouze od těch, jež si vybere. Následkem toho je, že se v IGMPv3 nepřihlašuje pouze do skupiny, ale i k odběru dat od určitého zdroje, který se nachází v dané skupině. Díky tomu se pochopitelně změní i formát zpráv. Tyto zprávy již nebudou mít konstantní délku, jak tomu bylo u předchozích verzí. Přesným popisem se zde nebudeme zabývat. IGMPv3 má své dvě vlastní zprávy a pro zpětnou kompatibilitu rozumí dalším třem:

- Membership Query - kód 11,
- IGMPv3 Membership Report - kód 22,
- IGMPv1 Membership Report - kód 12,
- IGMPv2 Membership Report - kód 16,
- IGMPv2 Leave Group - kód 17.

Význam zpráv je stejný jako u předchozích verzí, pouze se přidávají políčka pro členství ve skupinách. Také se trochu změnil význam políčka Max. doba odezvy. Nyní se jmenuje Max. kód odezvy a pokud je jeho hodnota nižší než 128, význam se nemění. IGMPv3 Report se také neposílá do příslušné skupiny, ale na adresu 224.0.0.22..

Prvních 8 bytů Query zprávy je stejný jako u přechozích verzí. Tzn., že klienti s nižší verzí protokolu nepoznají rozdíl a odpoví zprávou typu Report v odpovídající verzi protokolu. Router potom zachází s každou skupinou podle toho, jaké verze mají přihlášení klienti. Uvedme si názorný příklad. Pokud se do stejné skupiny na stejné síti přihlásí IGMPv2 i IGMPv3 klient, pak nebude router provádět filtrování

zdrojových adres a bude posílat všechny data skupiny. Naopak, dostane-li klient zprávu délky 8 bytů, ví, že jeho router používá IGMP nižší verze a přizpůsobí se mu.

Tento druh multicastu - SSM, byl však rozebrán pouze teoreticky a neobjeví se v praktické části. Je to z toho důvodu, že jeho podpora není implementována v simulačním nástroji Opnet Modeler. K provozu SSM multicastu je zapotřebí protokol PIM-SSM, který v OM bohužel definován není. OM umí pracovat pouze s PIM-SM, jež podporuje multicast typu ASM.

## 5 ZPŮSOB SMĚROVÁNÍ V MULTICASTU

### 5.1 Požadavky na efektivní skupinové vysílání

Cílem skupinového vysílání [1], které musí realizovat směrovače s příslušnou podporou skupinových směrovacích protokolů, je efektivita práce v síti, která spočívá v následujících požadavcích:

- každý člen skupiny dostane právě jednu kopii paketu určenou pro jeho skupinu,
- nečlenové skupiny paket nedostanou,
- cesta od zdroje ke každému cíli musí být optimální (nejkratší cesta).

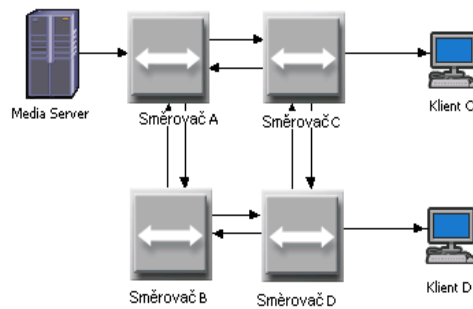
Paket do skupiny může být obecně odesláný ze stanice, která sama není členem dané skupiny a může být směrován přes sítě, které nemají připojené žádné členy dané skupiny. Optimální skupinové směrování musí zaručit dosažitelnost všech členů a to tak, aby se paket neocítl na jedné síti vícekrát. Nesmí tedy dojít k zacyklení směrovací smyčky. K tomu slouží informace vyplývající ze zdrojové adresy. Z toho též vyplývá, že v případě skupinového směrování jde vlastně o jakési obrácené směrování, z čehož plyne, že hledání optimální cesty není od zdroje směrem k cíli, ale naopak.

### 5.2 Průběh směrování

Směrování v unicastovém světě je poměrně jednoduché. Směrovač si pomocí dynamického směrovacího protokolu nastaví směrovací tabulku, nebo mu jí v jednodušším případě nastaví ručně operátor. Pokud bude tomuto směrovači doručen paket na libovolný interface, sníží tomuto paketu nejdříve parametr TTL (Time To Live) o jedničku a pokud je tento parametr stále vyšší než nula, prozkoumá směrovací tabulku. Když v ní pro cílovou adresu paketu najde příslušný řádek, přepośle paket na daný interface následujícímu směrovači.

Při multicastu je však skupinová adresa tím, co znamená více příjemců v různých sítích. Jednoduchá metoda je poslat takovýto multicastový paket na všechny rozhraní, kromě toho odkud přišel. Toto však vytváří v jistých situacích kruhy (viz obr. 5.1) Protože se paket duplikuje, je nutné spolehlivě kontrolovat, aby těchto duplikací nebylo příliš a aby paket k příjemcovi došel pouze jednou a ne víckrát. Pokud by se toto stalo, zátěž sítě by mohla být i vyšší než u obyčejného unicastu.

Jak je vidět na obr. 5.1, paket se neustále množí. Díky neustálému snižování parametru TTL (Time To Live) by se dále nemnožil, ale rozhodně by spotřeba

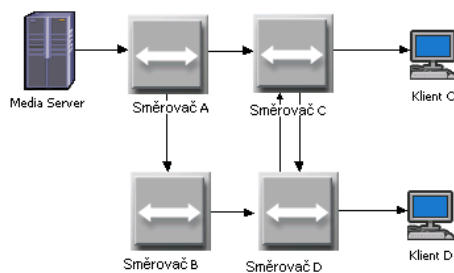


Obr. 5.1: Vytvoření multicastového okruhu

pásma byla několikanásobně vyšší, než je nutné. Stejně tak koncové zařízení dostane svoji zprávu několikrát, čímž se zbytečně zatěžují.

Technika, která zabraňuje této situaci se nazývá RPF - Reverse Path Forwarding (viz. obr. 5.2). Směrovač si stále drží unicastovou směrovací tabulku. Tuto tabulku získává buď od operátora, z klasických směrovacích protokolů, případně si ji sestavuje pomocí speciálních multicastových protokolů (například DVMRP). Často se může jednat i o více tabulek dohromady.

Jestliže směrovači přijde multicastový paket, zjistí si jeho zdrojovou adresu a interface, z kterého byl vyslán. Potom otestuje, zda-li by stejným směrem poslal i unicastový paket, jehož cílová adresa by byla stejná jako zdrojová u multicastového. Pokud nebude test pozitivní, bude paket zahozen. V opačném případě paket pokračuje k dalšímu zpracování. Toto výrazně snižuje zátěž.

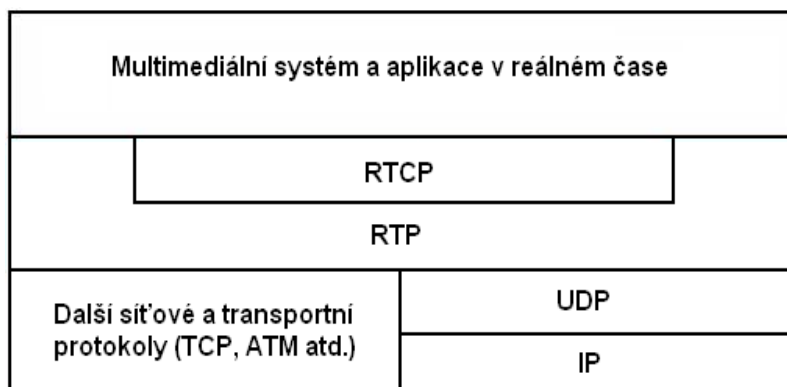


Obr. 5.2: Odstranění multicastového okruhu pomocí RPF

## 6 MULTIMEDIÁLNÍ PROTOKOL RTP/RTCP

Tento multimediální protokol [9] nám umožňuje uskutečnění živého vysílání po internetu, např. videokonferenci, nebo již zmiňovanou službu IP televize. Pro realizaci tohoto vysílání je nutné přijímat i vysílat multimediální data v reálném čase. Jedním z požadavků pro přenos těchto dat je samozřejmě výkonost komunikační sítě. Pod tímto pojmem si lze představit to, že musí splňovat jisté nároky na přenosovou rychlost, zpoždění a kvalitu služeb. V tom je hlavní rozdíl mezi přenosem statických dat a přenosem dat v reálném čase. Z toho lze vyvodit, že je třeba pro tento přenos v reálném čase užít speciální protokoly. Protokoly vhodné pro spolehlivý přenos dat v síti s malou šířkou pásma jsou dobře známé HTTP a FTP. Tyto jsou založené na protokolu TCP/IP. Dojde-li ke ztrátě, či poškození paketu, je tento znovu vyslán od zdroje k příjemci. To je jeden z důvodů, proč se k přenosu v reálném čase používají jiné protokoly než TCP. Jedním z takových je protokol UDP (User Datagram Protocol). UDP je však nespolehlivý protokol, který není schopen zaručit, aby byl každý vyslaný paket doručen k cíli a to ani ve správném pořadí.

Internetovým standardem, používaným pro přenos dat v reálném čase, je protokol RTP (obr. 6.1), který využívá zejména protokolu UDP. RTP umožňuje uživateli přenos dat od zdroje směrem k cíli v reálném čase. RTP je nezávislý na typu sítě a na přenosovém protokolu.



Obr. 6.1: Architektura protokolu RTP

Protokol RTP lze použít jak pro unicastové (tzn. pro každý cíl je vyslána ze zdroje jedna kopie), tak i pro multicastové (data vyslána ze zdroje pouze jednou a síť zajišťuje přenos dat do ostatních míst) služby sítě. Multicasting je však daleko výhodnější pro přenos multimediálních dat.

## 6.1 Služby RTP

RTP dokáže před samotným zahájením přenosu rozpoznat, o jaký typ dat se jedná. Poté určí pořadí paketů, v jakém budou data zasílána a synchronizuje datové toky z různých zdrojů. U datových paketů RTP není zaručeno to, že dorazí v pořadí, v jakém byly vyslány ani to, jestli k cíli dorazí všechny. To už je úkolem adresáta, aby pořadí rekonstruoval a provedl kontrolu toho, zda mu dorazily všechny data. To se děje pomocí informací v záhlaví paketů. Samotný protokol RTP nám neposkytuje žádné zajištění včasného doručení, nebo poskytnutí záruky kvality služeb (QoS). Tyto mechanismy nám poskytne kontrolní protokol RTCP. Ten umožňuje sledování kvality distribuce dat. RTCP dále poskytuje kontrolní a identifikační mechanismus pro přenosy RTP.

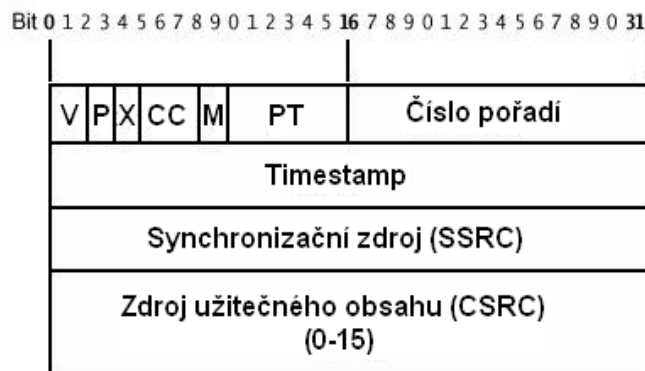
## 6.2 Architektura RTP

Vytvoření RTP spoje je vlastně asociace skupiny aplikací, komunikujících s RTP. Spoj se identifikuje pomocí síťové adresy a páru portů. Jeden port je určen pro samotný přenos dat a ten druhý je pro RTCP řídicí data. Jako účast ve spojení lze brát jednak pasivní příjem dat, stejně tak ale i vysílání dat, nebo dokonce obojí, tzn. příjem i vysílání dat. Při přenosu se rozlišuje jaký typ dat bude přenášen. Rozdílné typy jsou přenášeny zvlášť jiným spojem. Vhodným příkladem je videokonference. Je-li přenášen zvuk i video zároveň, musí se jeden spoj vyhradit pro přenos audio dat a druhý pro přenos video dat. Tímto se umožní účastníkovi vybrat si, jaký typ dat chce přijímat. Pokud se nachází v síti, kde je nízká šířka pásma, může si zvolit pouze příjem audio dat z konference.

## 6.3 Datový paket

Záhlaví datového paketu RTP (obr. 6.2) obsahuje následující položky:

- Verze RTP protokolu (V): 2 bity.
- Doplnění (P): 1 bit. Pokud je tento bit nastaven, je na konci paketu jeden nebo více bytů, které nejsou součástí užitečného obsahu. Úplně poslední byte v paketu indikuje počet doplněných bytů. Doplnění je využíváno některými šifrovacími algoritmy.
- Rozšíření (X) : 1 bit. Jestliže je tento bit nastaven, následuje za pevným záhlavím jedno rozšíření záhlaví. Tento mechanismus umožňuje vložení rozšiřujících informací do záhlaví RTP.



Obr. 6.2: Formát záhlaví datového paketu RTP

- Počet CSRC (CC) : 4 bity. Počet CSRC identifikátorů, které následují za pevným záhlavím. Jestliže je počet CSRC roven nule, je zdrojem synchronizace zdroj užitečného obsahu.
- Záložka (M) : 1 bit. Záložkový bit, definovaný konkrétním profilem média.
- Typ užitečného obsahu (PT) : 7 bitů. Index z tabulky profilu média, který popisuje formát užitečného obsahu.
- Číslo pořadí: 16 bitů. Jedinečné číslo paketu, které popisuje pozici paketu v pořadí paketů. Číslo paketu je inkrementováno po každém odeslaném paketu.
- TIMESTAMP: 32 bitů. Vyjadřuje moment odebrání vzorku prvního bytu užitečného obsahu.
- SSRC : 32 bitů. Identifikuje synchronizační zdroj. Jestliže je počet CSRC roven nule, je zdroj užitečného obsahu zdrojem synchronizace. Jestliže je CSRC nenulové, SSRC identifikuje mixér.
- CSRC : 32 bitů každý. Identifikuje zdroje přispívající do užitečného obsahu. Počet přispívajících zdrojů je určen polem počtu CSRC (CC). Celkem může být 16 přispívajících zdrojů. Jestliže je více přispívajících zdrojů, je výsledný užitečný obsah sloučením těchto zdrojů.

## 6.4 Kontrolní paket

K multimediálním datům jsou jako dodatek připojeny pakety kontrolních dat (RTCP). Ty jsou pak zasílány všem účastníkům spojení. RTCP pakety mohou v sobě obsahovat informace o kvalitě služeb pro účastníky spojení. Dále pak informaci o zdroji

dat na datovém portu a statistiky k datům, které byly přenášeny.

Je několik typů RTCP paketů :

- zpráva odesílatele,
- zpráva příjemce,
- popis zdroje,
- BYE,
- specifikace aplikace.

RTCP pakety je možné sloučit a zaslat je skupinově. Všichni účastníci, kteří jsou členy daného spojení vysílají RTCP pakety. Takový účastník, který odeslal paket, vydá zprávu odesílatele. Tato zpráva obsahuje celkový počet odeslaných paketů a bytů stejně tak, jako informaci, která může být užita pro synchronizaci toků medií z jiných spojů. Účastníci, jenž jsou spojeni, posílají zprávu příjemce v pravidelných intervalech. Ta je určena pro ostatní zdroje, z kterých přijímají datové pakety. Zpráva příjemce obsahuje informaci, která udává počet ztracených paketů, nejvyšší číslo pořadí a `TIMESTAMPu`, jenž může být užítý k odhadu obousměrného zpoždění, ke kterému dochází mezi odesílatelem a příjemcem. Ve skupině paketů musí být tím prvním paket zprávy a to i v případě, že nebyla přijata či odeslána žádná data. Všechny skupiny RTCP paketů musí obsahovat popis zdroje (`SDES`), který obsahuje kanonické jméno (`CNAME`), které identifikuje zdroj. Popis zdroje může obsahovat i další informace, kterými jsou jméno zdroje, telefonní číslo, emailová adresa, název aplikace, zeměpisná poloha nebo zprávu popisující aktuální stav zdroje. Dojde-li k tomu, že zdroj přestane býti aktivním, vyšle protokol RTCP paket `BYE`. V tomto oznámení lze nalézt důvod, proč zdroj opouští spojení. Paket specifikace aplikace poskytuje aplikacím mechanismus pro definici a zasílání uživatelských informací přes RTP řídicí port.

RTP aplikace lze dělit na ty, které potřebují přijímat data ze sítě (RTP klienti) a ty jenž potřebují vysílat data do sítě (RTP servery). Některé aplikace dělají obojí, např. aplikace pro konference získávají a vysílají data do sítě v tom samém okamžiku kdy přijímají data ze sítě.

Nás však v této práci bude nejvíce zajímat výpočet délky intervalu Feedback Report paketu, který se vypočítá podle následujícího vztahu:

$$c = \frac{8 \cdot RTCP_{size}}{0,75 \cdot 0,05 \cdot sess_{bw}} \cdot n, \quad (6.1)$$

kde  $RTCP_{size}$  je průměrná velikost Receiver Report paketu,  $sess_{bw}$  je využívaná šířka pásma a  $n$  je počet uživatelů.

## 7 ZAJIŠTĚNÍ QOS IPTV

Internetová televize - IPTV [12] znamená digitální vysílání, které je realizované přes internet a to díky protokolu IP [11]. IPTV sice využívá stejnou distribuční síť jako vysokorychlostní připojení k internetu, nejde ale o klasické internetové vysílání. IPTV putuje po privátní IP síti, která není dostupná široké veřejnosti, ale pouze těm zákazníkům, kteří si ji předplatili. Přináší proti klasickému televiznímu vysílání hned několik vylepšení.

IPTV se v podstatě skládá ze dvou komponent – internetového protokolu (IP) a televize (TV). Protokol IP specifikuje formát datových paketů a adresování v síti. Ve většině sítí se kombinuje IP protokol s protokolem vyšší úrovně. Nejčastěji je to protokol UDP (User Datagram Protocol), který je využit při navázání virtuálního spojení mezi příjemcem a zdrojem dat. Protokol IP umí pouze adresovat tok dat, ale už nedokáže sestavit přímé propojení mezi odesílatelem a příjemcem.

Služba poskytuje daleko vyšší rozlišení obrazu. Tzn. jemnější rastr scén. Pro provoz této služby však potřebuje uživatel využít daleko větší šířku pásma v přístupové síti.

Pro snížení nároků na šířku pásma [15] při náročných video přenosech se dnes používají normalizované kodeky (kompresor/dekompresor). Nejmodernější z nich, kompresní formát z pera skupiny ISO Motion Picture Experts Group, MPEG-4 AVC (Audio Video Coding), vytvořený ve spolupráci s ITU (International Telecommunication Union), jako doporučení H.264 AVC v roce 2003. Ve srovnání s populárním MPEG-2 (rok 1994), nabízí o polovinu lepší kompresní výkonnost.

Nicméně ani MPEG-4 AVC nemusí dlouhodobě vyřešit problém, jak přenášet video ve vysoké kvalitě po sítích DSL. S MPEG-4 mohou provozovatelé sítí DSL poskytovat služby IPTV v běžném rozlišení, s čímž mohou konkurovat dalším poskytovatelům, ale nebude stačit na obsah s vysokým rozlišením (HDTV). S MPEG-4 AVC postačí pro běžné rozlišení (SDTV) v reálném čase 1,5-2 Mbit/s. HDTV ale potřebuje – na každý kanál – minimálně 4-8 Mbit/s (systém 720p/25 potřebuje 4 Mbit/s a systém 1080i/50 s prokládaným řádkováním vyžaduje 5 Mbit/s), v závislosti na spolehlivosti videotoku. K tomu ještě je třeba připočítat kapacitu pro další internetové služby a hlas a rázem potřebujeme přípojku DSL o takové kapacitě, která u nás není zcela běžná.

V oblasti IPTV služeb přes DSL budou mít proto poskytovatelé značné problémy obstát vedle konkurence kabelových, satelitních a hlavně optických přípojek, kde se s kapacitou a poskytováním HDTV služeb nepotýkají.

Asi je zbytečné zde rozebírat vlastnosti televize, ale i přesto se nad tím pozastavme. Tento komunikační prostředek umožňuje přenos obrázků a zvuků. Nás však budou zajímat služby, jakými jsou lineární nabídka programů a nabídka programů

na vyžádání. V privátní síti, navržené specificky pro IPTV, může operátor zaručit uživatelům potřebnou kvalitu služby (QoS). QoS souvisí s přidělením vyšší priority. Pod tímto si lze představit to, že se přenos IPTV upřednostní před jinými službami poskytovanými v IP sítích. Tyto služby však budou poskytovány současně s IPTV, ale s nižší prioritou. To však neplatí pro VoIP, protože tato hlasová služba má ve všech případech nejvyšší prioritu.

Nejvýznamnějšími parametry, které definují QoS v síti jsou:

- Ztrátovost paketů - jaké množství paketů nedorazí od vysílače k cíli.
- Přenosová kapacita - objem přenesených dat za čas.
- Zpoždění doručení paketů - je definováno dobou potřebnou k přenosu od odesílatele k adresátovi.
- Proměnné zpoždění tzv. Jitter - je definováno změnou zpoždění jednotlivých paketů během přenosu.

IPTV je služba s okamžitým přenosem. Nezahrnuje tedy žádný „download“ obsahu jak lineárního, tak i na vyžádání. IPTV umožňuje dodávat všechny rádiově i kabelově šířené programy, včetně pořadů vysílaných „naživo“, tzn. v reálném čase. Rovněž může nabídnout i službu video na vyžádání VoD, což je něco jako videotéka. Tato služba umožňuje provozovateli širokopásmových služeb vyvíjet nové, unikátní služby, díky kterým bude konkurenceschopná. Více např. v [12].

Obecně je známo, že i dnes při velmi vysoké rychlosti připojení, může být dosti nepříjemné sledovat sportovní přenosy (např. kopaná) přes IPTV. Dynamika obrazu je velmi vysoká a scény se mění velmi rychle díky pohybu hráčů, což zapříčiňuje časté rozostření obrazu. Toto může způsobit velmi nepříjemnou bolest očí a sportovní požitek je „ten tam“. Proto lze tuto službu doporučit spíše pro sledování filmů, kde je více statických scén. Existuje však možnost, že v budoucnu bude poskytovatel nabízet takovou QoS a prodejce monitory, či LCD displeje s velmi krátkou dobou odezvy, že i sledování sportovních utkání se stane „méně bolestivé“ pro naše oči.

## 8 SIMULACE V PROSTŘEDÍ OPNET MODELER

### 8.1 Seznámení s OM

Opnet Modeler [14] je simulační program, který je vhodný zejména pro návrh a analýzu komunikačních sítí. Vyvinula ho americká firma OPNET Technologies. Toto prostředí usnadňuje návrh komunikačních sítí. Nabízí zejména dimenzování sítí, návrh a simulaci protokolů, simulaci chování aplikací s velkou možností flexibility.

OM je hierarchicky a objektově orientován, grafické prostředí odráží reálné rozmístění jednotlivých síťových komponent a na nejnižší úrovni je chování jednotlivých komponent zapsáno v jazyce C/C++. Dále obsahuje široké možnosti v oblasti simulace a analýzy výsledků. OPNET Modeler již v sobě obsahuje řadu knihoven jednotlivých síťových komponent převážně pro Ethernet, FDDI, IP, TCP, ATM, HTTP, UMTS atd. Tyto knihovny mají dostupný zdrojový kód, takže jej lze dále podle potřeby upravovat.

OM poskytuje širokou možnost tvorby statistik z dané simulace vytvořené sítě. Lze jej proto použít tam, kde chceme prověřit chování reálného objektu v různých extrémních podmínkách (např. vysoká zátěž serveru atd.). Lze tak předejít jistým nežádoucím stavům. OM poskytuje možnost generovat výsledky statistik do zpráv ve formátu XML, nebo HTML, či data uložit do tabulek. Ba dokonce umí aplikaci i naopak z těchto formátů načíst vstupní data. OM obsahuje i prohlížeč animací, takže můžeme názorně vidět průběh běžící simulace. Ta probíhá se zrychlením. To znamená, že můžeme nastavit dobu simulace např. několik dní a simulace proběhne během několika minut.

Základní prvky OM:

- subnet - podsíť (propojené servery, stanice, huby, switche apod.),
- node model – model uzlu (modely stanice, serveru, hubu, switche apod.),
- process model – model procesu zde jsou definovány jednotlivé procesy modelu uzlu.

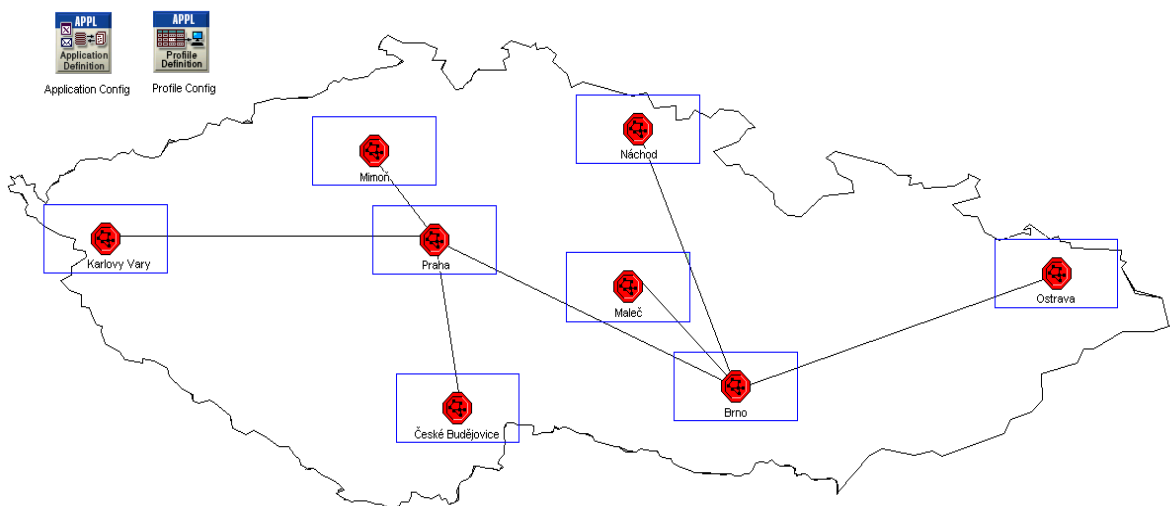
OM je „jednoduchý“ hierarchický editor, který přesně popisuje spojení struktur reálné sítě a protokolů. OM je tvořen ze třech základních editorů:

- Project Editor - editor projektu je grafický editor modelující topologii a komunikaci v síti.

- Node Editor - editor uzlu představuje rozhraní nižší úrovně než editor projektu. Ukazuje např. architekturu síťového zařízení, nebo systému a vzájemné vztahy mezi funkčními moduly a volanými funkcemi.
- Process Editor - editor procesu je rozhraní nejnižší úrovně, obsahuje kód v C/C++. Slouží pro tvorbu konečného stavového automatu. Stavů a přechodů jsou definovány v grafickém editoru.

## 8.2 Vytvoření modelu sítě

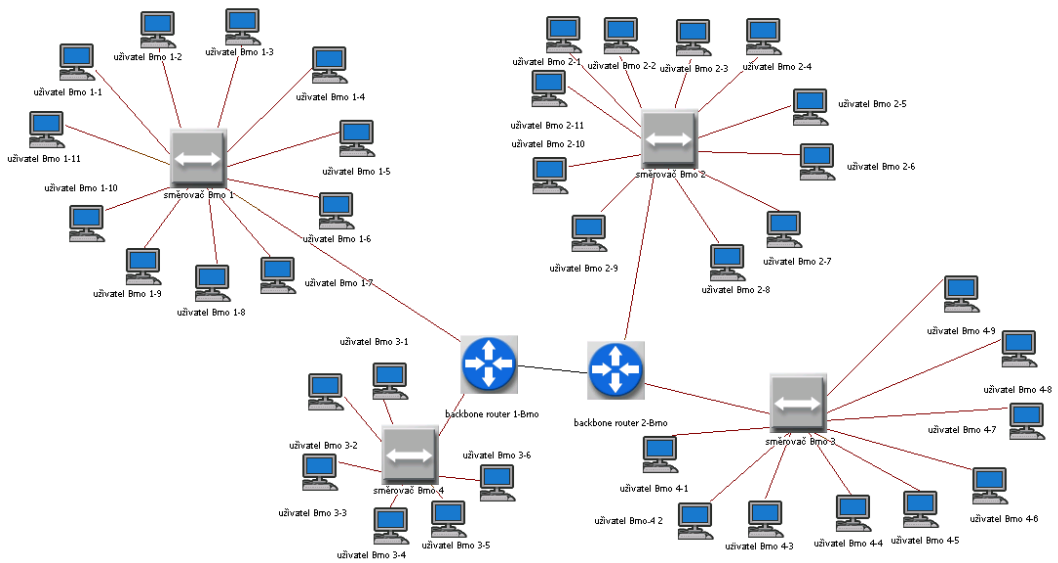
Úkolem bylo navrhnout a ověřit chování sítě podporující multicastový přenos služby IPTV. Byla navržena síť v rámci České republiky a jako podsítě několik vybraných měst. Těmi jsou: Praha, Brno, Ostrava, Karlovy Vary, České Budějovice, Náchod, Mimoň a malebná vesnička v podhůří Železných hor - Maleč (viz obr. 8.1).



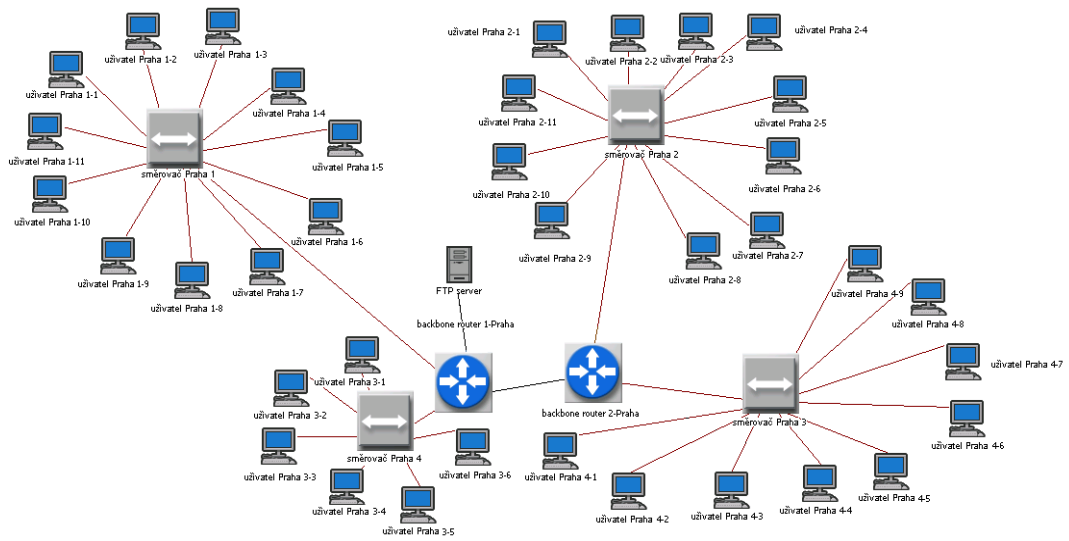
Obr. 8.1: Navržená síť

Každá podsíť je svou velikostí, co se počtu uživatelů týče, úměrná reálné velikosti těchto měst. Tzn., že pro zjednodušení je podsíť Praha shodná s podsítí v Brně (viz obr. 8.2), Ostravě, Karlových Varech a Českých Budějovicích.

V těchto větších podsítích se nachází další dílčí sítě, které jsou navzájem propojeny pomocí směrovačů. Jednotlivé uživatelské stanice jsou k těmto směrovačům připojeny ethernetovou linkou **100BaseT**. Celkový počet uživatelů v posítí činí 37, čtyři směrovače a dále pak dva backbone routery, kterými jsou propojena jednotlivá města a to sice linkou s označením **PPP\_DS3**, jejíž přenosová rychlost je 44,736 Mbit/s. V Praze je ještě navíc server vysílající službu IPTV (obr. 8.3).

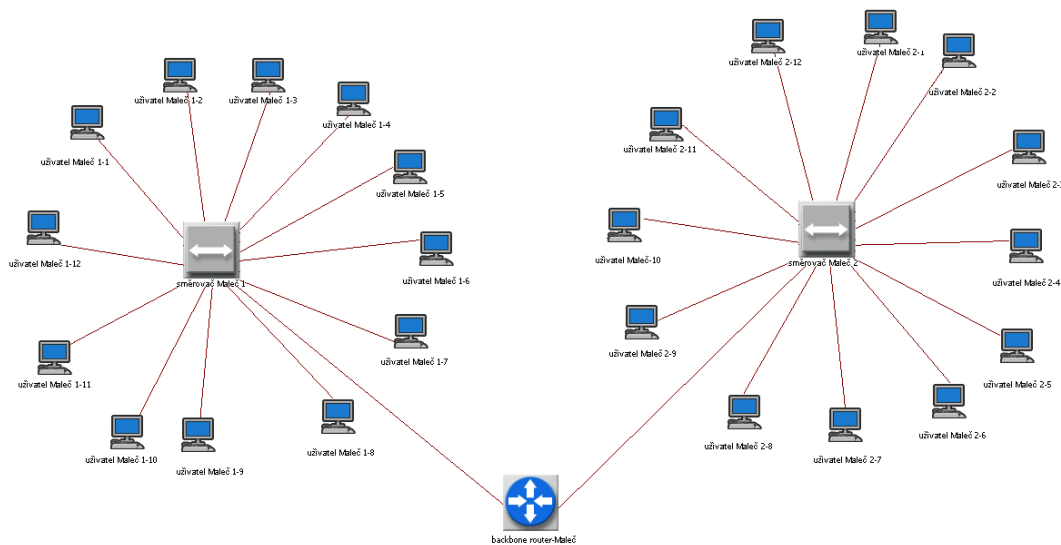


Obr. 8.2: Podsít' Brno



Obr. 8.3: Podsít' Praha

Dále se svou topologií shodují podsítě Mimoň, Maleč a rovněž Náchod (viz obr. 8.4). V těchto sítích se nachází 24 uživatelských stanic, dva směrovače a jeden backbone router se stejnou funkcí jako viz. výše.

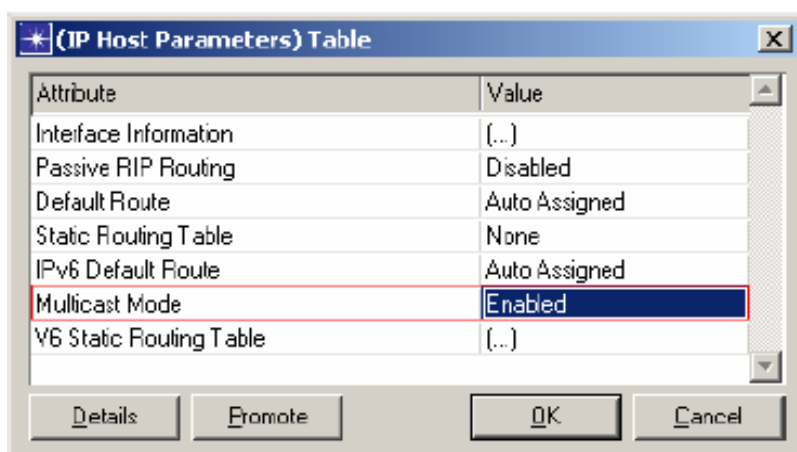


Obr. 8.4: Podsít' Maleč

## 8.2.1 Nastavení síťových prvků

Aby bylo dosaženo správných výsledků v simulaci multicastového přenosu dat, musí být každý prvek v síti správně nakonfigurován.

1. Jako první bylo nastavení klientských stanic, které byly součástí multicastového provozu. Je zapotřebí povolit v jejich nastavení položku **Multicast Mode** na **Enabled** (viz obr. 8.5).



Obr. 8.5: Povolení multicastového provozu na uživatelské stanici

2. Dalším krokem je nastavení multicastu na směrovačích. Zde je nutné povolit multicast a zároveň směrovací protokoly na jeho rozhraních. Ty je potřeba

i správně určit a nastavit RP. Nastavení směrovače dle následujícího obrázku nalezneme v položce *Edit Attributes - IP Routing Protocols -RIP Parameters - Interface Information - Staus - Enabled*.

Name	Status	Silent Mode	Advertisement Mode	Cost
IF15	Enabled	Disabled	Split Horizon with ...	1
IF16	Enabled	Disabled	Split Horizon with ...	1
IF17	Enabled	Disabled	Split Horizon with ...	1
IF18	Enabled	Disabled	Split Horizon with ...	1

Obr. 8.6: Povolení RIP protokolu na rozhraních směrovače

3. Nezbytnou součástí provozu je i správná funkce protokolu IGMP. Ten zajistí, aby směrovač rozpoznal, zda jsou v jeho podsíti připojení členové multicastové skupiny. Nastavení je následující: *Edit Attributes - IP Multicasting - IGMP Parameters - Interface Information*, jak je patrné z obrázku 8.7.

Name	Status	Version	Membership Groups	Fast-Switch Groups
IF7	Enabled	2	Not Configured	Not Configured
IF8	Enabled	2	Not Configured	Not Configured
IF9	Enabled	2	Not Configured	Not Configured
IF16	Enabled	2	Not Configured	Not Configured
IF1	Enabled	2	Not Configured	Not Configured

Obr. 8.7: Nastavení parametrů IGMP protokolu na směrovačích

4. Povolit multicast musíme i na směrovači a to následujícím způsobem: *Edit Attributes - IP Multicasting - IP Multicast Parameters - Multicast Routing - Enabled*.
5. Dalším bodem je nastavení PIM parametrů pro rozhraní, které zabezpečují komunikaci mezi směrovači: *Edit Attributes - IP Multicasting - IP Multicast Parameters - Interface information*.

Name	Status	Routing Protocol(s)	TTL Threshold	Subinterface Infor...
IF7	Enabled	PIM-SM	0	Not Configured
IF8	Enabled	PIM-SM	0	Not Configured
IF9	Enabled	PIM-SM	0	Not Configured
IF16	Enabled	PIM-SM	0	Not Configured
IF1	Enabled	PIM-SM	0	Not Configured

Obr. 8.8: Povolení protokolu PIM-SM

6. Povolení PIM protokolu na směrovači: *Edit Attributes - IP Multicasting - PIM Parameters - Status – Enabled.*
7. Nakonfigurování PIM parametrů pro rozhraní: *Edit Attributes - IP Multicasting - PIM Parameters - Interface Information.* Jak již bylo zmíněno výše, PIM protokol pracuje ve 3 různých módech. A to sice Dense, Sparse a Sparse-dense. Zvolíme typ módu, dle obrázku 8.9 a to z důvodu, že je multicastový provoz směrován na toto rozhraní pokud nejméně jeden z PIM rozhraní je explicitně připojený do multicastového stromu. Verzi zvolíme 2.

Name	Mode	Version	Priority	Hello Interval (millis...)
IF7	Sparse	2	0	30000
IF8	Sparse	2	0	30000
IF9	Sparse	2	0	30000
IF16	Sparse	2	0	30000
IF1	Sparse	2	0	30000

Obr. 8.9: Nastavení módu a verze protokolu PIM

8. Dalším důležitým krokem je konfigurace Rendezvous Pointu na směrovači: *Edit Attributes - IP Multicasting - PIM Parameters - Static RP Configuration.* Adresa RP směrovače je běžná unicastová adresa třídy C, viz. obr. 8.10. Ve sloupci *Version* znamená verzi PIM protokolu, který běží na rozhraní.

Address	Override	Version	Group Filter Config...	Bidirectional
192.0.1.1	Disabled	2	(...)	Disabled
192.0.1.1	Disabled	2	(...)	Disabled
192.0.1.1	Disabled	2	(...)	Disabled

Obr. 8.10: Konfigurace RP na směrovači

V tomto stejném okně přejdeme do nabídky *Group Filter Configuration*, která je potřebná pro nastavení skupin, využívajících RP (nastavený pro všechny skupiny). Objeví se okno, v kterém je nutné přiřadit cílovou multicastovou adresu i s maskou podsítě (*Destination Address/Mask*). V našem případě to bude **224.0.6.1**.

## 8.2.2 Nastavení aplikací

Nastavení aplikací se v OM provádí pomocí bloků *Application Config* a *Profile Config*. V *Application Config* se zvolí jednotlivý typ aplikace a její parametry. Těmi mohou být např. u videokonference počet snímků za sekundu, rozlišení snímku, priorita aplikací, nebo rezervace šířky pásma. V OM jsou definovány aplikace jako např. Database Access, Email, File Transfer, File Print, Telnet Session, Video Conferencing, Voice Over IP Call, Web Browsing, či Custom - vlastní aplikace. Blok *Profile Config* nastavuje průběh aplikace v době simulace. A to např. start aplikace, konec aplikace, počet opakování, či offset.

## 8.2.3 Přiřazení aplikace na straně příjemce

Každý klient v síti, který chce využívat danou aplikaci, musí ji mít jistým způsobem přiřazenu. Nastavení klienta je následující:

1. Rozvineme roletové menu na objektu, *Edit Attributes - Application: Multicasting Specification*. V kolonce *Application Name* vybereme aplikaci podporovanou multicastem, tzn. náš profil definovaný v bloku *Application Config*.
2. Položka *Membership Addresses* udává podporované multicastové adresy z rozsahu 224.0.1.0 – 239.255.255.255. Pro naši síť bude použita adresa **224.0.6.1**.

3. Dalším parametrem, který se musí na klientovi nastavit je ***Application: Supported Services***. Pravým kliknutím na objekt nastavujeme: ***Edit Attributes - Application - Application: Supported Services*** a vybereme podporovanou, námi definovanou službu v kolonce ***Name*** na námi definovanou aplikaci ***IPTV***.

#### 8.2.4 Nastavení aplikace na straně odesílatele - serveru

V síti, která je použita pro simulaci, je nastaven zdroj dat (server) v podsíti Praha. Tento server, s nímž budou komunikovat klienti, musí podporovat aplikaci a symbolické cílové jméno (***Destination Name***), které bude představovat příjemce.

1. Pravým kliknutím rozbalíme nabídku nastavení serveru: ***Application - Application: Destination Preferences***. Jako ***Symbolic Name*** zvolíme ***Multicast Receiver***, což představuje multicastový přijímač. V ***Actual Name*** nastavit kolonku ***Name*** v ***Table*** na adresu ***224.0.6.1***, představující multicastovou adresu klienta.
2. Ve stejném menu rozbalíme nabídku ***Application: Supported Profiles*** a do ***Profile Name*** přiřadíme náš předem vytvořený profil z ***Profile Config***, tedy IPTV.

A nyní můžeme přistoupit k nastavení výstupu simulace sítě.

### 8.3 Simulace modelu IPTV služby s multicastovým přenosem dat

Na navržené síti byl vytvořen model služby IPTV s multicastovým přenosem dat v nástroji OM. Zde však aplikace zajišťující provoz služby IPTV není přímo definována, a tak byla vytvořena modifikací služby VOIP. Možná by se zdála pro úpravu vhodnější videokonference, jelikož je její podobnost se službou IPTV velká, z hlediska přenosu audiovizuálních dat. Bohužel má ale OM poněkud zvláště definované aplikace, pro které lze realizovat simulaci vlastností multimediálního protokolu RTP. Podporuje ho totiž pouze pro službu VOIP, nikoli však pro videokonferenci. Pro tu lze simulovat pouze vlastnosti protokolu UDP, jež je protokolem transportní vrstvy a zajišťuje nám tedy pouze „nespolehlivý“ přenos dat.

Daná služba byla modifikována tak, že se v bloku ***Application Config*** zvětšila šířka pásma na 2 Mbit/s . Tato hodnota odpovídá šířce pásma reálné IPTV typu SDTV (Standard-definition television)[15]. Šířka pásma se musí zvětšit především

proto, že služba IPTV přenáší kromě audio dat i data obsahující video. Tuto hodnotu lze měnit v nabídce **RSVP Parameters**, který slouží pro rezervaci šířky pásma. V tomto okně (obr. 8.12), lze ještě změnit typ služby. Pro IPTV byl zvolen typ **Streaming Multimedia**. Tímto nastavením se lze službě IPTV přiblížit asi nejvíce.

Pro zobrazení výsledku simulace, se musí na každém sledovaném objektu (server, klient, směrovač, linka) přiřadit sledované parametry simulace. Jedním způsobem přiřazení je globální. V tomto přiřazení pro celou síť, tzn. pro každý prvek v síti, se přiřadí stejná sledovaná charakteristika. Tou druhou možností je lokální přiřazení, kde sledujeme vybrané parametry pouze na určitém objektu v síti. Postup je následující:

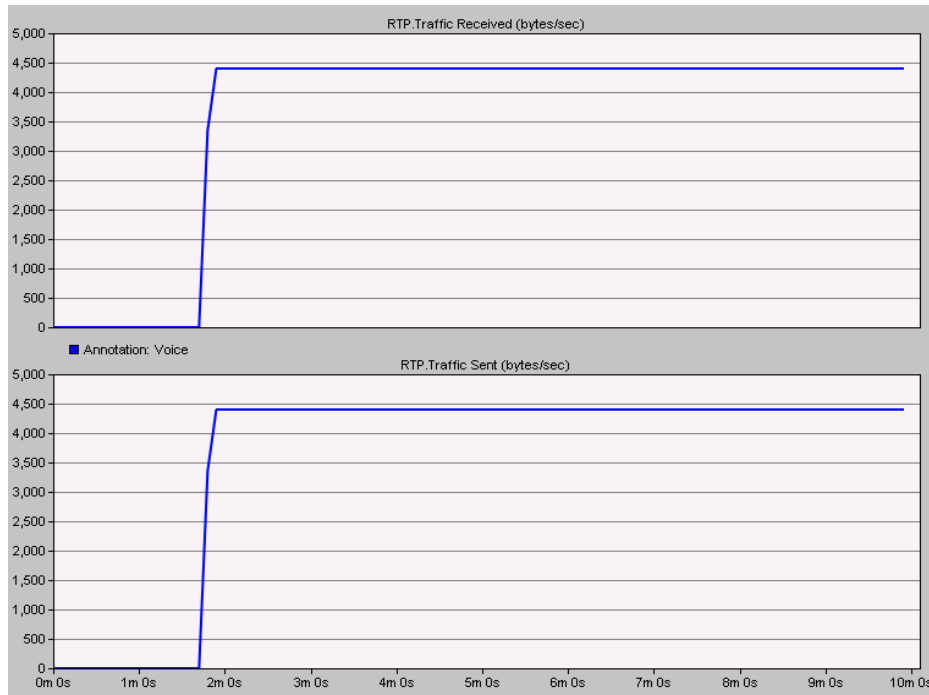
1. Pravým kliknutím na sledovaný objekt: **Choose Individual DES Statistics**, zobrazí se nám nabídka s množstvím statistik, které lze objektu přiřadit. My zvolíme např. sledování protokolu RTP.

Zde jsou pro přehlednost uvedeny všechny parametry simulace, které byly pro danou síť nastaveny:

Počet snímků	10 snímků/s
Rozlišení	128 x 100 pixelů
Typ služby	Streaming multimedia
Doba simulace	10 minut

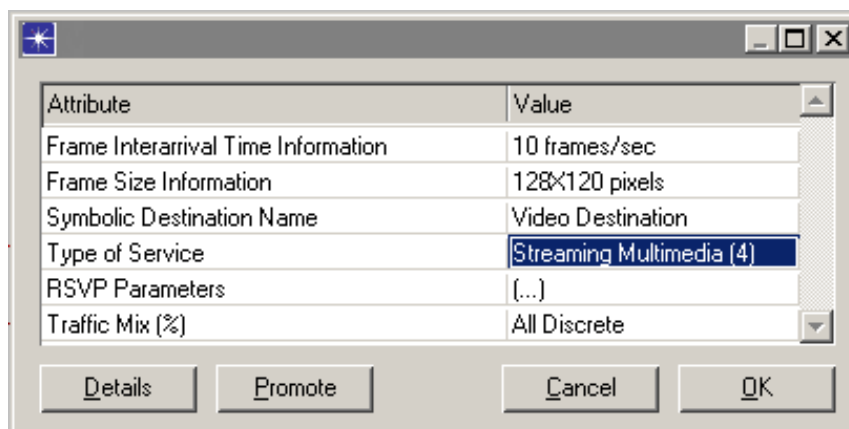
Tab. 8.1: Parametry simulace

Je-li celá síť nastavená dle našich představ, můžeme zahájit samotnou simulaci. Tu lze spustit pomocí ikony na hlavním panelu s názvem **Configure/Run Discrete Event Simulation (DES)**. Zobrazí se nám okno **Configure/Run DES**, kde se nastavují parametry simulace, jakými jsou doba simulace, generátor náhodného čísla, či počet naměřených hodnot k vykreslení charakteristiky.



Obr. 8.11: Objem přijatých a vyslaných dat protokolem RTP. Výstup z programu Opnet Modeler.

Zobrazeny jsou charakteristiky propustnosti jednotlivých linek v páteřní síti navrženého modelu mezi vybranými podsítěmi (městy). Nás však především budou zajímat vlastnosti protokolu RTP. Zkoumám je objem vyslaných a přijatých dat (obr. 8.11) a jeho zpoždění (obr. 8.13). V následující kapitole jsou porovnány dva způsoby, kterými lze zjistit zpoždění zasílání RTCP paketů. Prvním je výpočet dle vzorce 6.1 a tím druhým je výstup simulace z OM.



Obr. 8.12: Nastavení aplikace IPTV.

## 8.4 Porovnání výstupu simulace zpoždění RTP protokolu s výpočtem dle vzorce 6.1

Nabízejí se nám hned dva způsoby, jak zjistit interval zasílání RTCP Feedback Report paketů, jimiž se přenášejí řídicí informace o daném spojení.

1. Tím prvním je teoretický výpočet dle vzorce 6.1. Naznačený postup výpočtu je níže. Je zde zobrazena i tabulka 8.2 výsledků pro různý počet uživatelů v modelu navržené sítě. Počet uživatelů byl zvolen od 10 do 247 a to v 7 krocích. 247 je celkový počet uživatelů v modelu sítě navrženém v OM, jedná se tedy o maximum zatížení, jež je síť schopná poskytnout.

Počet uživatelů	10	20	50	100	150	200	247
Zpoždění [s]	0,11	0,22	0,54	1,07	1,60	2,14	2,64

Tab. 8.2: Vypočítané hodnoty zpoždění RTCP paketu

Vzorec 6.1 má tvar:

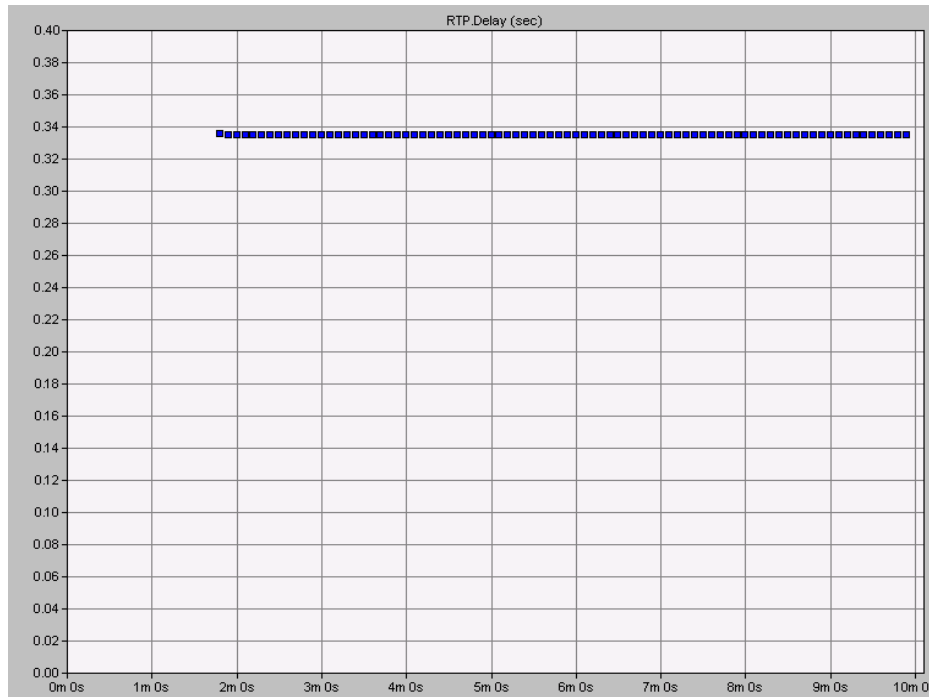
$$c = \frac{8 \cdot RTCP_{size}}{0,75 \cdot 0,05 \cdot sess_{bw}} \cdot n, \quad (8.1)$$

kde  $RTCP_{size}$  je průměrná velikost Receiver Report paketu, kterou zde zvolíme 100 bytů. To odpovídá reálné hodnotě, jež v praxi velikost Receiver Report paketu skutečně dosahuje. Číslo 8 v čitateli nám tuto hodnotu převádí na bity.  $sess_{bw}$  je využívaná šířka pásma, kterou jsme zvolili 2 Mbit/s. Z násobení číslem 0,05 je patrné, že RTCP pakety zabírají 5% z celkové šířky pásma. A  $n$  je počet uživatelů. Tato hodnota se nám mění pro jednotlivá měření dle tabulky 8.2.

Příklad výpočtu pro 100 uživatelů:

$$c = \frac{RTCP_{size}}{0,75 \cdot sess_{bw}} \cdot n = \frac{8 \cdot 100}{0,75 \cdot 0,05 \cdot 2000000} \cdot 100 = 1,07s \quad (8.2)$$

2. Dalším způsobem je simulace provozu IPTV služby v Opnet Modeleru. Klikneme na plochu páteřní sítě pravým tlačítkem myši a vybereme nabídku **View Results** a zobrazíme si požadovanou charakteristiku. Závislost zasílání RTCP Feedback Report paketů na počtu uživatelů lze realizovat tak, že v navrženém modelu sítě měníme počet připojených uživatelů. Provedeno je to tak, že uživatelé byly postupně odpojovány a připojovány do páteřní sítě v jednotlivých podsítích a to pro 7 různých hodnot (viz. tab. 8.3). Na obrázku 8.13 je příklad charakteristiky pro 20 uživatelů.



Obr. 8.13: Zpoždění protokolu RTP pro 20 uživatelů. Výstup z programu Opnet Modeler.

Počet uživatelů	10	20	50	100	150	200	247
Zpoždění [s]	0,17	0,34	0,50	0,90	1,30	1,78	2,20

Tab. 8.3: Nasimulované hodnoty zpoždění RTCP paketu

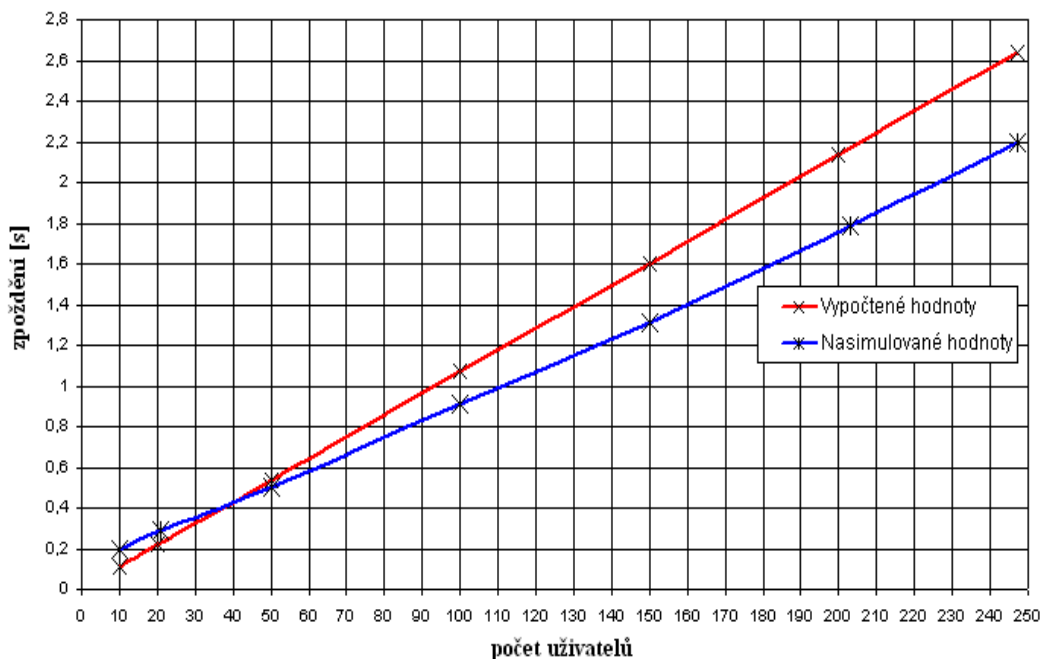
Tyto oba způsoby jsou porovnány v grafické závislosti, jež je zobrazena na obrázku 8.14. Nárůst zpoždění zasílání RTCP Feedback Report paketu v závislosti na počtu uživatelů je lineární. Obě křivky se však zcela neshodují a nasimulované hodnoty vykazují menší zpoždění, než ty vypočtené.

## 8.5 Zatížení páteřní linky při přenosu dat multicastem a unicastem

Důležitou vlastností multicastových přenosů je to, že zmenší zátěž zdrojového uzlu a přenosové soustavy při distribuci dat skupině příjemců. Porovnány jsou proto propustnosti linek multicastového a unicastového přenosu dat v navrženém modelu sítě.

Zobrazeny jsou charakteristiky propustnosti linek mezi městy (podsítěmi) Brno

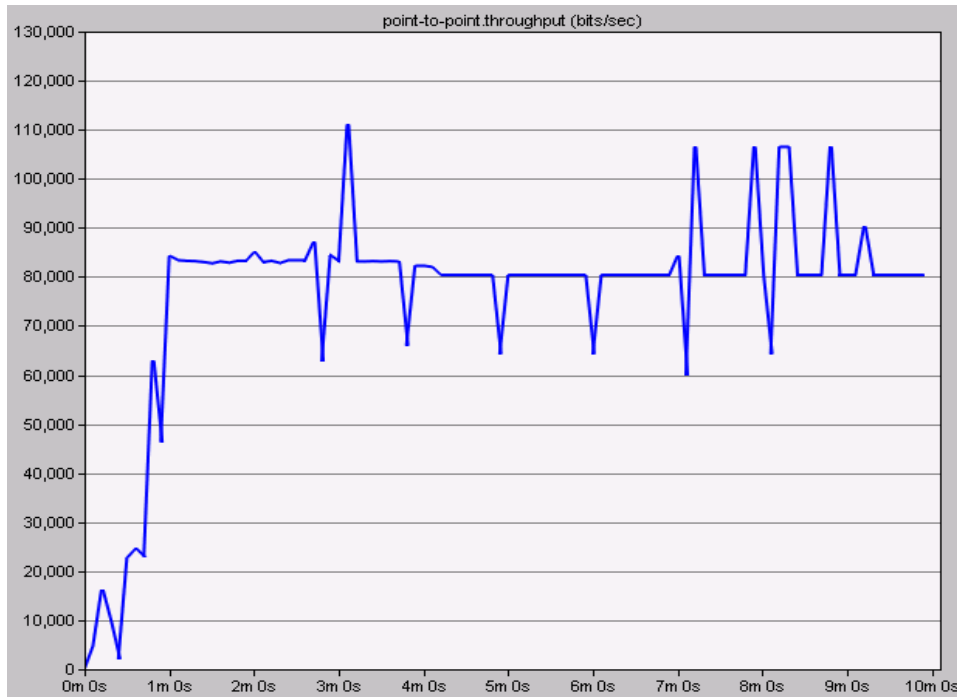
Závislost intervalu odesílání RTCP Feedback Report paketů na počtu uživatelů



Obr. 8.14: Grafická závislost intervalu odesílání RTCP Feedback Report paketů na počtu uživatelů

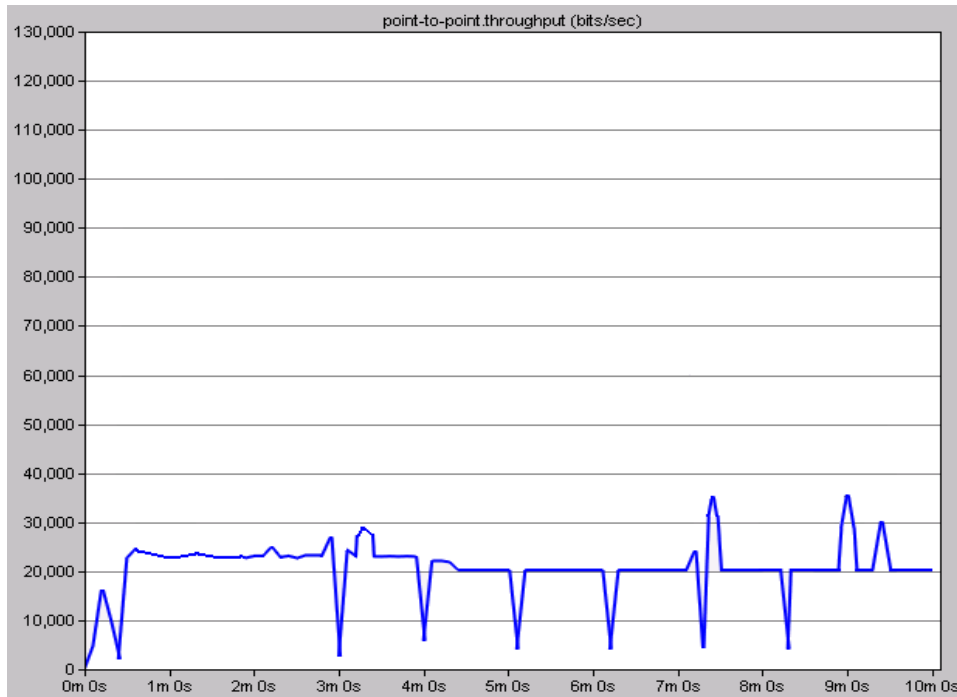
a Maleč, dále pak mezi Prahou a Brnem. Zvoleny jsou tedy dvě větší města a jedno menší, ve kterém je připojeno méně uživatelů. Z toho plyne, že by linka měla vykazovat menší propustnost, což je ověřeno simulací. Výstupem simulace je několik následujících charakteristik.

Tou první je propustnost linky mezi podsítěmi Brno a Maleč s přenosem dat unicastem (obr. 8.15). Při porovnání s obr. 8.16, kde je zobrazena propustnost linky při multicastovém přenosu, je patrné, že menší propustnost a tudíž i zátěž vykazuje komunikace pomocí multicastu. Při unicastu dosahuje maximum propustnosti hodnoty až 110000 bits/s a u multicastu je toto maximum pouze 35000 bits/s. Tato skutečnost odpovídá teoretickým předpokladům.



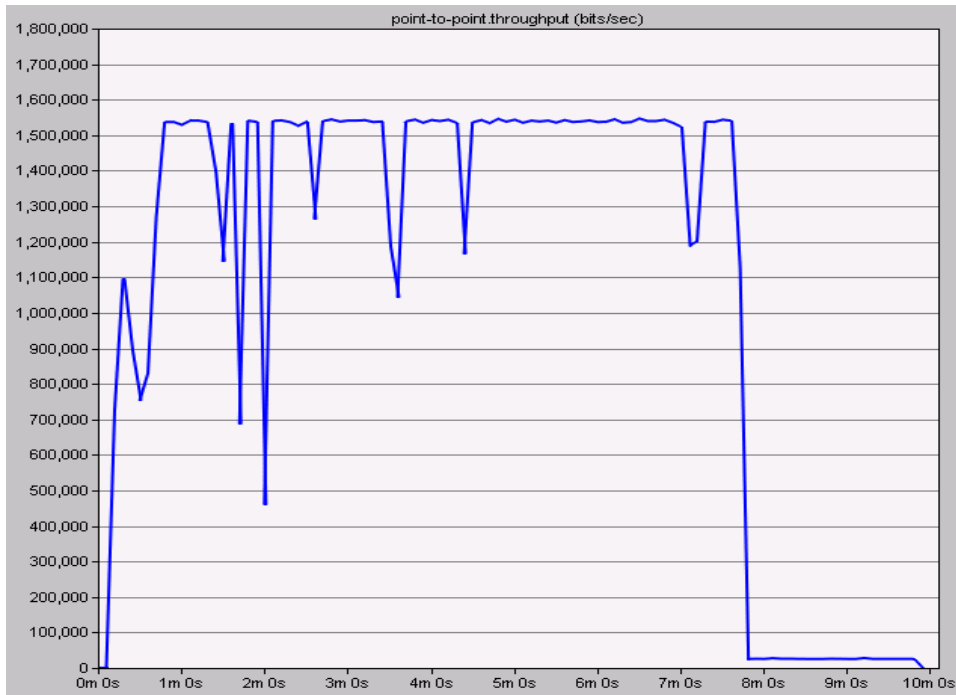
Obr. 8.15: Propustnost linky ve směru Brno - Maleč, přenos unicastem. Výstup z programu Opnet Modeler.

Na následujících charakteristikách 8.17 a 8.18, je opět porovnán přenos unicastem a multicastem. U sítě s multicastem dosahuje maximum propustnosti pouze k hodnotě 750000 bits/s, kdežto unicastová síť až k 1550000 bits/s. Opět se tedy potvrzuje to, že multicast vykazuje menší zatížení přenosové soustavy.

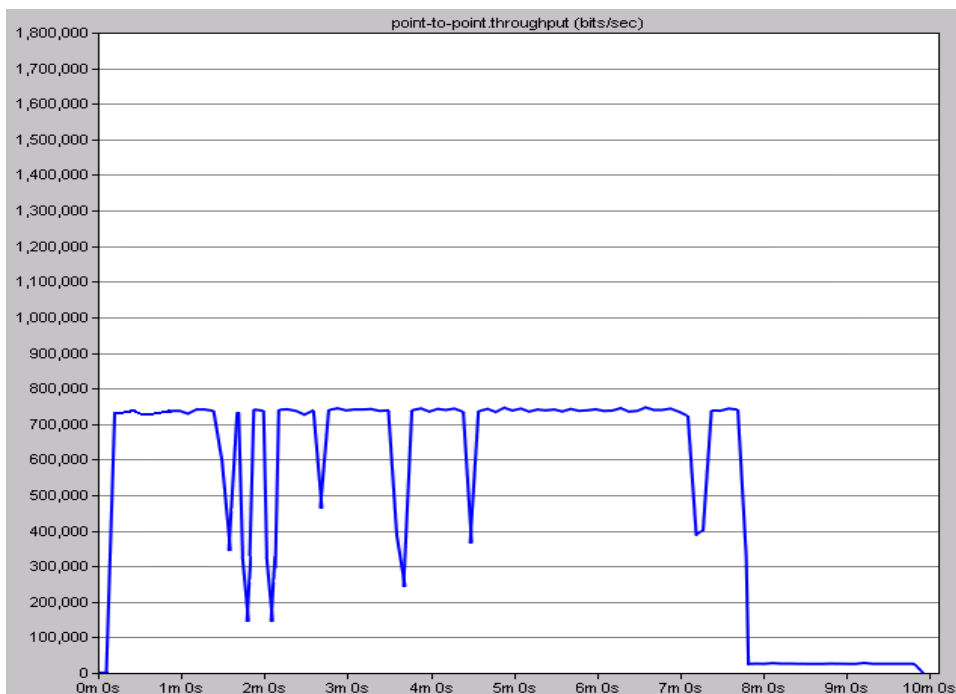


Obr. 8.16: Propustnost linky ve směru Brno - Maleč, přenos multicastem. Výstup z programu Opnet Modeler.

Lze ještě vzájemně porovnat propustnost linek mezi většími městy - Brnem a Prahou a mezi menší Malčí. Je patrné, že na lince mezi Prahou a Brnem je dosaženo, např. při přenosu unicastem (obr. 8.17), více než desetkrát větší propustnosti linky než na obr. 8.15. A to z důvodu větší zátěže, která je zapříčiněna větším počtem uživatelů.



Obr. 8.17: Propustnost linky ve směru Brno - Praha, přenos unicastem. Výstup z programu Opnet Modeler.



Obr. 8.18: Propustnost linky ve směru Brno - Praha, přenos multicastem. Výstup z programu Opnet Modeler.

## 9 ZÁVĚR

V této práci byly popsány principy a jednotlivé druhy multicastu - ASM a SSM. Simulace však byla provedena pouze pro multicast typu ASM, jelikož OM nepodporuje multicast typu SSM.

V simulačním nástroji byl navržen model aplikace IPTV s multicastovým přenosem dat. Tato síť byla navržena v rámci České republiky a jako podsítě byly vybrána některá města, či menší městečka. Jako rozsáhlejší síť byla zvolena Praha, Brno, Ostrava, Karlovy Vary a České Budějovice a jejich topologie jsou pro jednoduchost naprosto totožné. Stejně tak tomu je v případě Náchoda, Mimoně a Malče. Tyto sítě byly však navrhnuty s menší počtem uživatelských stanic.

Služba využívající multicast - IPTV byla navržena v OM a postup návrhu byl popsán. Nezbytnou součástí přenosu služby IPTV je protokol RTP/RTCP, který zaručuje přenos multimediálních dat v reálném čase. Zkoumána však byla především signalizační část tohoto protokolu a to interval odesílání RTCP Feedback Report paketů v závislosti na rostoucím počtu uživatelů. Porovnávány byly dvě metody a to sice praktická (simulace v OM) a teoretická (výpočet dle vzorce 6.1). Z vypočtených hodnot byly vyneseny grafy, jež znázorňuje obrázek 8.14. Obě závislosti jsou lineárně rostoucí ke vzrůstajícímu počtu uživatelů. Z grafu je patrné, že v OM nedosahuje zpoždění tak velkých hodnot, jak je tomu u teoretického výpočtu. Pro maximální hodnotu účastníku v síti, která činí 247 uživatelských stanic, je mezi těmito dvěma metodami rozdíl zhruba 0,5 sekundy. Se zvyšujícím počtem uživatelů by se tento interval i nadále zvyšoval. Lze tedy konstatovat, že protokol RTP není příliš vhodný pro velmi rozsáhlé sítě, které mohou mít až stovky tisíc uživatelů. V tak rozsáhlé síti by mohl interval zasílání RTCP Feedback Report paketů dosáhnout až několik minut, což by značně znepříjemnilo sledování jakéhokoliv programu, kdyby byla signalizace zasílána s tak velkým zpožděním.

Simulována byla i propustnost páteřní linky v závislosti na použité přenosové technologii. První byl přenos multicastem a druhým byl unicastový přenos. Potvrdila se zde významná vlastnost multicastu a to, že daleko méně zatěžuje přenosovou soustavu než unicast. Těmito charakteristikami byla ověřena další vlastnost přenosu. A to tak, že byly porovnány maxima propustnosti linky mezi několika městy. Bylo to mezi Prahou a Brnem a Malčí a Brnem. Potvrdil se tak předpoklad, že čím je linka méně zatížena, tzn. má menší počet připojených uživatelů, tím menší propustnost je linkou vykazována.

## LITERATURA

- [1] SPORCTAK, M. A. *Směrování v sítích IP*. Computer Press, a.s., 2004, ISBN 80-251-0127-4.
- [2] Opnet Technologies Inc. *Opnet Modeller* [online]. Opnet Technologies Inc. 2001, poslední aktualizace 12. 12. 2007 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.opnet.com>>.
- [3] KOMOSNÝ, D. *Nové směry vývoje protokolu RTP/RTCP pro rozsáhlé konference v Internetu* [online]. 2004, poslední aktualizace 27. 10. 2004 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.elektrorevue.cz/clanky/04052/index.html>>.
- [4] HRUBÝ, P. *Source Specific Multicast - nástroj pro zajištění multicastingu v Internetu* [online]. 2002, poslední aktualizace 19.11. 2002 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.isdn.cz/clanek.php?cid=4461>>.
- [5] FILIP, O. *Úvod do IP multicastu (díl třetí)* [online]. 2004, poslední aktualizace 8. 10. 2004 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.lupa.cz/clanky/uvod-do-ip-multicastu-dil-treti/>>.
- [6] MICROSOFT TechNet. *Protokol IGMP (Internet Group Management Protocol)* [online]. 2007, poslední aktualizace 21. 1. 2005 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/cs/library/ServerHelp/ffa6231a-bf9b-4691-a63d-81c9cf66a34e.mspx?mfr=true>>.
- [7] FILIP, O. *Úvod do IP multicastu (díl čtvrtý)* [online]. 2004, poslední aktualizace 29. 10. 2004 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.lupa.cz/clanky/uvod-do-ip-multicastu-dil-ctvrty/>>.
- [8] Juniper Networks, Inc. *PIM-SSM* [online]. 2007, poslední aktualizace neuvedena [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.juniper.net/techpubs/software/junos/junos60/swconfig60-multicast/html/pim-overview13.html>>.
- [9] HUJKA, P. *Real - Time Transport Protocol a aplikační rozhraní RTP Java Media Framework* [online]. 2003, poslední aktualizace 27. 5. 2003 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.elektrorevue.cz/clanky/03018/index.html>>.
- [10] HABRMAN, R. *Síťové protokoly (XXI. část), Protokol OSPF* [online]. 2007, poslední aktualizace 20. 3. 2007 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.owebu.cz/pc-site/vypis.php?clanek=1596>>.

- [11] Extra PC IPTV, *seznamte se prosím!* [online]. 2007, poslední aktualizace 14. 3. 2007 [cit. 28. 5. 2008]. Dostupné z URL: <<http://styl.finance.cz/zpravy/finance/101597-iptv-seznamte-se-prosim-/>>.
- [12] Sdělovací Technika - [www.stech.cz](http://www.stech.cz) *IPTV aneb televize po Internetu* [online]. 2006, poslední aktualizace 18. 7. 2006 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.stech.cz>>.
- [13] IANA *Internet multicast addresses* [online]. 2007, poslední aktualizace 28. 11. 2007 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.iana.org/assignments/multicast-addresses>>.
- [14] MOLNÁR, K., ZEMAN, O. *Moderní síťové technologie* Návod do počítačových cvičení, VUT Brno. 2006, Brno.
- [15] Články o aDSL - Svět.DSL.cz *IPTV vyžaduje nejen šířku pásma, ale vysokou kvalitu I.* [online]. 2007, poslední aktualizace 9. 11. 2007 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.dsl.cz/clanky-dsl/clanek-891/IPTV-vyzaduje-nejen-sirku-pasma,-ale-vysokou-kvalitu-I.>>.
- [16] BOLDIŠ, P. *Bibliografické citace dokumentů podle ČSN ISO 690 a ČSN ISO 690-2* [online]. 2001, poslední aktualizace 11. 11. 2004 [cit. 28. 5. 2008]. Dostupné z URL: <<http://www.boldis.cz/citace/citace.html>>.

# SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

- ASM Model multicastu využívající více zdrojů dat pro skupinové vysílání – Any Source Multicast
- ATM Asynchronní přenosový mód – Asynchronous Transfer Mode
- DVMRP Směrovací protokol podporující skupinové vysílání – Distance Vector Multicast Routing Protocol
- EIGRP Rozšířený vnitřní směrovací protokol (Cisco) – Enhanced Interior Gateway Routing Protocol
- FDDI Distribuované datové rozhraní s optickými vlákny – Fiber Distributed Data Interface
- FTP Protokol pro přenos souborů – File transfer protocol
- HTTP Protokol podporující prohlížení webů – Hyper Text Transfer Protocol
- IANA Organizace na rezervování a přidělování IP adres – Internet Assigned Numbers Authority
- IGMP Protokol podporující skupinové vysílání v rámci internetu – Internet Group Management Protocol
- IP Internetový protokol – Internet Protocol
- IPTV Televizní vysílání přes internet – Internet Protocol TeleVision
- LAN Lokální počítačová síť s menším počtem počítačů – Local Area Network
- LCD Moderní technologie pro zobrazovací prvky – Light Crystal Device
- LSA Link State Advertisement – Zpráva obsahující informace o změně v síti
- OM Simulační program firmy OPNET – OPNET Modeler
- OSPF Směrovací protokol – Open Shortest Path First
- PIM-SM Protokol nezávislý na skupinovém vysílání – Protocol Independent Multicast - Sparse Mode
- PIM-SSM Směrovací protokol nevyužívající Rendezvous Point – Protocol Independent Multicast - Source Specific Multicast
- QoS Kvalita služeb – Quality of Service

RIP Směrovací protokol, využívající metriku – Routing Information Protocol

RP Kořen stromu multicastu – Rendezvous Point

RPF Technika zabráňující tvorbě multicastového okruhu – Reverse Path Tree

SPF Nalezení nejkratší cesty – Shortest Path Find

SPT Nejkratší cesta ve stromě – Shortest Path Tree

SSM Model multicastu využívající jediný zdroj dat pro skupinové vysílání – Source Specific Multicast

TCP/IP Nejznámější internetový protokol – Transmission Control Protocol/Internet Protocol

TTL Zbývající doba „životnosti“ paketu – Time To Live

UDP Protokol sestavující spojení – User Datagram Protocol

UMTS Univerzální mobilní telekomunikační systém – Universal Mobile Telecommunications System

VoD Video na vyžádání – Video on Demand

VoIP Hlasová služba v sítích IP – Voice Over IP

XML Rozšířitelný značkovací jazyk – Extensible Markup Language