

# Optimalizace metod pro multimediální aplikace v geodézii v prostředí IP sítí

Milan Berka <sup>1</sup>

## *Optimization of Methods for Geodetic Data for Multicast in IP Networks*

*This paper deals with possibilities of using RTP and RTPC protocols for defining different schemes of broadcast multimedia multiplex and ways of its distribution in telecommunication networks. The effectiveness of different variants of signal distribution is compared through this simulation experiment. Some defined tasks, which could be eventually solved in this area, are also presented. A simulation is applied to theoretical and real networks and the results on each particular network could differ significantly.*

**Key words:** Multicast, unicast, control hierarchy, system simulation, RFC 1350, RFC 1351, optimization techniques, signal distribution, multimedia multiplex.

## Úvod

Není daleko doba, kdy poměrně velké množství uživatelů bude moci současně využívat informace o terénu a objektech na něm v reálném čase. Jednou současnou aplikací, která poskytuje alespoň představu o tom, jak by to v budoucnu mohlo vypadat je Google Earth. Z pohledu geodetických potřeb je to ovšem dle mého názoru v současné době sice efektivní, ale stále pouze dětská hračka. Možná moje představy jsou v této oblasti trochu podobné Sci-Fi, ale promítání změn do map a modelů terénu v reálném čase a jejich získávání také v reálném čase dříve nebo později bude realitou. Dnes považujeme za úspěch stažení souboru prostřednictvím sítě, zítra možná, se budeme pohybovat nad terény v 3D v reálném čase.

V této oblasti existují některé docela zajímavé práce např. „Tourism information based on visualisation of multimedia geodata – ReGeo“, kolektivu *Department Remote Sensing and Landscape Information Systéme a Albert-Ludwigs-University Freiburg i.Brsrg., Germany*, i když daná tematika nějak v roce 2004 usnula...

## Současný stav

### MPEG-1

Standard MPEG byl vyvinut na základě požadavku průmyslu, který potřeboval kvalitní způsob ukládání a získávání audio a video informací na digitální záznamová média (Digital Storage Media – DSM). CD-ROM je levný nosič poskytující přenosovou rychlost přibližně 1.2 Mbps. MPEG standard byl vyvíjen s cílem dosáhnout podobnou přenosovou rychlost. "Constrained Parameters bitstream" (datový rok s omezenými parametry), jsou podmnožina všech přístupných bitových toků, u kterých se očekává, že budou široce využívány. Jsou omezeny na datovou rychlost až do 1.856 Mbps. Nicméně je třeba podotknout, že standard není omezen jen touto hodnotou, a že může být použit i pro vyšší datové rychlosti.

Během práce na standardu MPEG videa byly vyvinuty další dva závažné mezinárodní standardy: H.261 od společnosti CCITT zaměřený na telekomunikační aplikace a ISO 10918 od výboru ISO JPEG zaměřený na kódování obrázků. Základy obou těchto standardů byly začleněny do standardu MPEG Video, ale výsledkem další práce výboru byly prvky, které nebyly obsaženy ani v jednom z výchozích standardů (H.261 a ISO 10918).

Standard MPEG Video definuje formát pro kompresi digitálního videa a možnosti, jak může být video kódováno a dekódováno. Ačkoliv je tento standard flexibilní, základní algoritmy byly laděny tak, aby dobře pracovaly v datové rychlosti od 1 do 1.5 Mbps, při rozlišení okolo 350 x 250 a snímkovací frekvencí mezi 24 a 30 snímky. Použití slova "obraz", jako protiklad ke slovu "rám", je záměrné. Kódy MPEG Video postupně snímají vyobrazení a nerozpoznávají způsob proplétání. Prokládané místo videa musí být před kódováním převedeno na neprokládaný formát. Po dekódování může dekóder libovolně vytvořit pro zobrazení nějaký prokládaný formát.

Standard MPEG Video je navržen k povolení několika metod, aby sledovaly kódování videa, které normálně souvisí s VCR: přehrávání, pozastavení obrazu, rychlé převíjení vpřed, rychlé převíjení zpět

<sup>1</sup> doc. RNDr. Milan Berka, CSc., GTS Novera a.s., Výstaviště 1, BRNO,, tel.: 420 602 244 751, Česká Republika, [Milan.Berka@gtsnovera.cz](mailto:Milan.Berka@gtsnovera.cz)  
(Recenzovaná a revidovaná verzia dodaná 6. 2. 2007)

a zpomalené přehrávání. Navíc je možný i libovolný přístup. Schopnost dekóderu realizovat tyto režimy záleží na rozsahu povahy digitálního paměťového média, ve kterém je zakódované video uloženo.

#### MPEG video - kompresní techniky

Video je představováno jako posloupnost jednotlivých obrázků, a každý obraz je považován za dvojrozměrné pole obrazových prvků (pixelů). Barva každého pixelu se skládá ze tří složek: hodnoty Y (jasu) a dvou barevných složek.

Komprimace digitalizovaného videa je možná díky několika technikám:

- vzorkování barevné informace vzhledem k citlivosti lidského zraku,
- kvantizaci,
- kompenzaci pohybu (Motion Compensation),
- transformaci frekvence pomocí
- diskrétní kosinové transformace (Discrete Cosine Transform - DCT),
- kódování VLC (Variable Length Coding) a obrazové interpolaci.

#### MPEG-2

Definitivní schválení ISO/IEC 13818-1 (MPEG-2 systémy), ISO/IEC 13818-2 (MPEG-2 video) a ISO/IEC 13818-3 (MPEG-2 Audio) jako mezinárodních standardů, bylo dáno 29. setkáním ISO/IEC JTC1/SC29/WG11 (MPEG), konaném v Singapuru v listopadu 1994.

MPEG-2 koncepce je podobná jako u MPEG-1, ale zahrnuje zaměření na širší použitelnost. Základní aplikace je zaměřena na plně digitální přenos videa v přenosových rychlostech mezi 4 a 9 Mbps.

Nicméně bylo zjištěno, že syntaxe MPEG-2 nachází uplatnění také pro aplikace s vyšší vzorkovací frekvencí a bitrate (jako např. HDTV). Nejvýraznějším zlepšením, oproti MPEG-1, je přidání syntaxe pro účinné kódování prokládaného videa (např. kompenzace pohybu pro bloky 16x8, Dual Prime, a další).

Mnoho dalších jemných zlepšení (jako např. 10-bitová diskrétní kosinová transformace s dvojitou přesností, nelineární kvantizace, tabulky VLC kódování a další) přispívá ke zlepšenému výkonu kódování a to dokonce i pro progresivní video. Dalšími klíčovými vlastnostmi standardu MPEG-2 jsou rozšiřitelné dodatky, které umožňují dělení kontinuálního video signálu do dvou nebo více kódovaných datových toků, které mohou reprezentovat video s různým rozlišením, kvalitou obrazu nebo snímkovací frekvencí.

#### MPEG-4

Na rozdíl od \*.MPG, žádný souborový formát \*.MPEG4 neexistuje. Tedy otázka: *“Jak si vytvořím MPEG-4 soubor?”* nemá smysl.

Lze vytvořit soubor AVI, ve kterém je obraz zkomprimován technikou MPEG-4. MPEG-4 je mnohem variabilnější formát pro kompresi pohyblivých obrázků, než jakým je MPEG-1. Na rozdíl od MPEG-1 může mít téměř libovolné rozměry obrazu, počet snímků za sekundu a vzdálenost mezi klíčovými snímky (KeyFrame, IFrame). Navíc nemá pouze konstantní datový tok (CBR: constant bitrate), ale proměnný datový tok (VBR: variable bitrate), což snižuje výslednou velikost videa. Co však MPEG-4 nemá, je široká podpora výrobců stolních DVD/VCD přehrávačů. To znamená že v tuto chvíli pro MPEG-4 video neexistuje žádný CD standard. Tudíž ani není možné říci jaký formát mají mít CD ve formátu MPEG-4 a tedy je nemožné taková CD ve stolních přístrojích přehrávat, pokud ovšem tyto zařízení nejsou vlastně PC...

#### Problémy

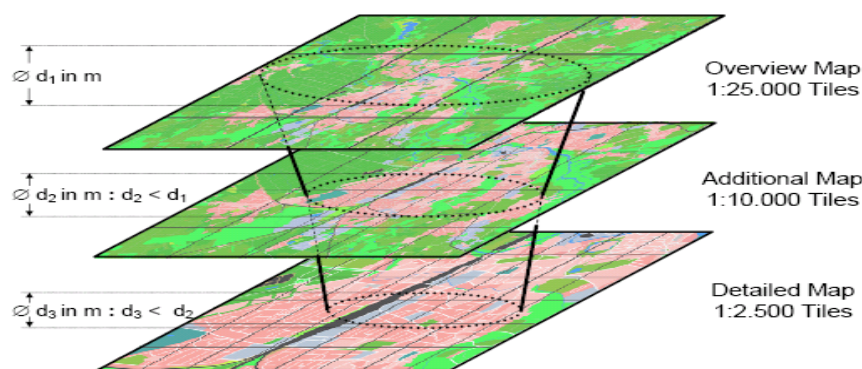
Z hlediska technologie přenosu je třeba říci, že rozumným způsobem pro živé vysílání je využití protokolů IP, nad ním protokolu UDP a nad ním pak protokolu RTP/RTCP [3]. Z hlediska způsobu distribuce signálu k odběratelům (klientům) se pak rozlišuje především unicast a multicast. Unicast při vysílání z jednoho zdroje je silně omezen kapacitou přenosové trasy. Např. při vysílání se šířkou pásma 2 Mbps pro jednu relaci se kapacita spoje u vysílacího serveru při 1 000 klientech vyšplhá na úctyhodných 2 Gbps, což je běžná kapacita jednoho optického vlákna. Je třeba si také uvědomit, že pro digitální kvalitu 2 Mbps není použitelná šířka pásma, ale spíše 10-20x tolik...

Z tohoto pohledu unicast, který by docela dobře splňoval požadavky na možnost zabezpečení přenosu od vysílače ke klientovi, se jeví jako perspektivně nepoužitelný. Protože ke každému klientovi jde separátní kanál, není problém tento kanál šifrovat či proudově podepisovat. Přitom podepisování živého proudového vysílání není zase až tak triviální záležitostí (protože při příjmu signálu a jeho zobrazení máme vždy k dispozici pouze „kousek“ celé informace). Je to věc ovšem řešitelná. Problém s omezeným počtem uživatelů je problém zásadní.

Existuje celkem známá cesta, jak z tohoto problému ven. Tou cestou je použití technologie multicastu, kde z vysílacího serveru jde pouze jeden proud dat a ten se postupně na jednotlivých směrovačích rozvětluje

ke klientům. Díky této technologii se zátěž páteřní sítě nezvyšuje s narůstajícím počtem klientů. Mohlo by se zdát, že problém je vyřešen.

Mimo unicast a multicast existuje ještě technologie broadcast v této oblasti je zajímavá publikace "Location-Based Geodata Broadcast", kde jsou popsány technologie Terrestrial digital video broadcast DVB (DVB-T) pro lokalizaci pohybujících se objektů. Systém postupného zjemňování mapových podkladů ukazuje následující převzatý obrázek



Obr.1. Zjemňování lokalizačních map.  
Pic.1. Transition to detailed map.

Existují i technologie, které umožňují postupné zjemňování přechodu mezi jednotlivými měřítky a odpovídající technologie pro přesnost takovýchto dat.

Vznikají však některé další problémy (viz [1]):

1. Není možné jednoduše zabezpečit trasu mezi serverem a zvláště každým klientem.
2. I pro protokol RTP/RTCP existují „množstevní“ omezení pro počet klientů, nad kterým se výrazně omezí dostupnost vysílání i pro multicast. Toto si ukážeme níže. Pro protokol RTP existuje také bezpečná varianta a to protokol SRTP (Secure Real-time Transport Protocol), který je upraven prostřednictvím standardu RFC 1711. V tomto případě jde vlastně o zašifrování určité porce dat v rámci paketu definovaného dle RFC 3550. V normě je šifrování definováno prostřednictvím 128 bitových bloků AES-f8. Zpětnou signalizaci pak provádí analogicky zabezpečený protokol SRTPC. Mandatorně je používán AES-CM pro šifrování, HMAC-SH1 pro integritu a AES-CM pro odvozené klíče. V každém fixním proudu může být klíč použit maximálně jedenkrát. Master keys mohou být použity i napříč streamy. Tímto způsobem je bezpečnost limitována. Při rychlosti např. 200 SRTPC paketů za sekundu je maximální možná doba streamu asi 4 měsíce. Protokol může být použit i při ochraně proti opětovnému přehrávání audia nebo videa.
3. Dalším rozšířením protokolu SRTP je pak protokol ZRTP, který k definici v normě přidává mechanismy pro počáteční výměnu klíčů. Produkt, který využívá tuto technologii je např. ZPHONE. Reálně to funguje tak, že pod vlastní VoIP je vnořena vrstva (něco jako SSL PROXY), která zajišťuje bezpečnost. Toto je ovšem řešení spíše pro systémy komunikace jeden s jedním.
4. Nefunguje rozumný přenos multicasu mezi operátory, takže můžeme předpokládat, že dané vysílání uvidíme pouze u „svého“ poskytovatele připojení, pokud je bude poskytovat. Nějaké celo Internetové multicastové vysílání nebude možné bez další specifikace přenosových technologií a standardů
5. Není rozumně možné individuálně zabezpečit přenos signálu zvláště pro každého klienta. Vydání stejného klíče všem klientům není zrovna nejlepší řešení zabezpečení. Na takto zabezpečené satelitním vysílání vyrostli celé generace hackerů a celý průmysl, který se zabývá prolamováním ochrany šifrovaných kanálů...

### Možná řešení

Aby dopad multimediálního vysílání zcela neparalyzoval infrastrukturu, je pochopitelně třeba použít něco jiného než unicast. Možná není v sítích implementováno odpovídající řešení, ale teoretický problém v této oblasti není.

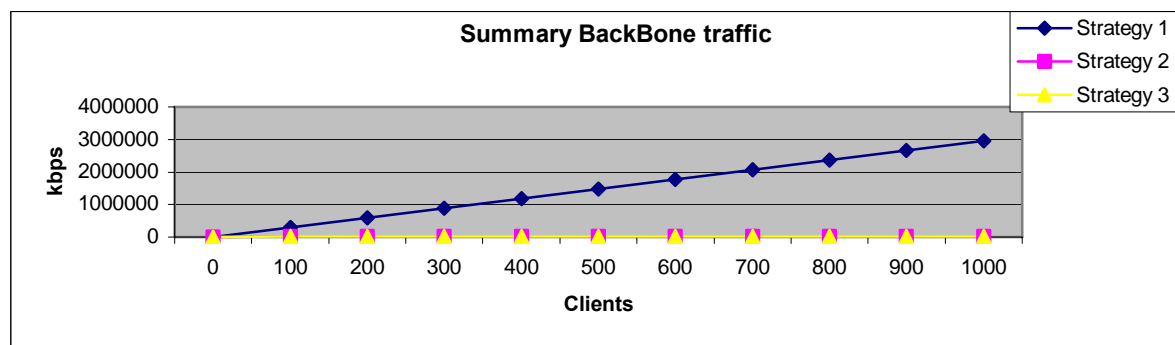
Řešením je zde SSM - Specific Source Multicast, ale pouze v oblasti šíření datového obsahu. Existují však i jiné problémy. Ty spočívají v samotném protokolu RTP/RTCP, kde dle definice zpětné odezvy protokolu, kterou se např. poskytují informace o kvalitě přeneseného signálu, vychází, že podle klasických vzorců dle RFC 1350 a 1351 je interval reportu přímo úměrný počtu klientů. Např. při 100 000 divácích (což pro klasické televizní vysílání není žádné velké číslo) bude tento interval už 33 minut. Kromě modulace kvality však tento protokol může sloužit ke zprostředkování interaktivní zpětné vazby. Např. Ovlivnění

obsahu streamu, což pro oblast geodezie a mapových informací může být záležitost zásadního významu. Taková odezva je prakticky nepoužitelná.

Existuje několik možných řešení tohoto problému. Jednou je modifikace šíření signálu o koncentraci zpětných vazeb na síťových prvcích. Tato cesta má některá úskalí. Ta spočívají v tom, že síťový prvek by musel řešit řadu úloh, které mu nejsou vlastní, muselo by dojít k implementaci těchto algoritmů výrobcem apod. Z krátkodobého hlediska se jedná o dostatečně neprůchozí variantu.

Druhou variantou je, že roli koncentrátorů zpětného toku převezmou někteří klienti. V takovém případě, velmi zjednodušeně řečeno, vznikne jakási reverzní situace k technologii CDN. To vyžaduje malou úpravu protokolu, ale teoretická rychlost odezvy pro 100 000 klientů klesne z výše uvedených 33 minut na cca 30 sekund a to je snížení docela podstatné. Pro 1 000 000 klientů pak teoreticky klesne z úctyhodných 5 hodin na 50 sekund.

Vývoj nárůstu potřeby páteřní kapacity ukazuje následující graf, ze kterého je zřejmé, že při zátěži koncových linek uživatelů je potřeba růstu kapacity páteře při SSM multicastu minimální. Rostoucí křivka odpovídá unicastu.



Obr. 2. Růst zátěže sítě.

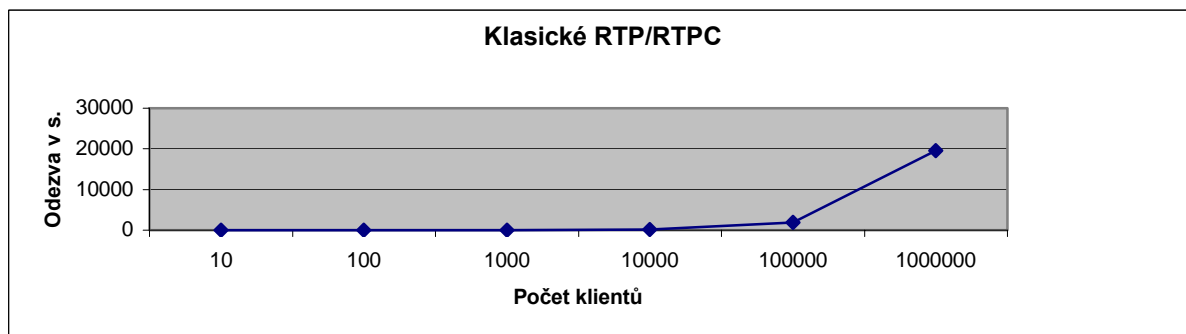
Pic. 2. Accumulation of network traffics.

Následující dva grafy srovnávají interval odezvy pro klasické RTP/RTCP s metodou agregace ve dvou hierarchických úrovních. Otázka vhodného počtu úrovní pro optimální odezvu je momentálně otázkou teoretické analýzy. Z hlediska praktické použitelnosti se do 1 000 000 klientů jeví počet dvou úrovní dostatečný. Klasické schéma dle RFC 1350, 1351 vypadá následovně:

Tab. 1. Odezvy.

Tab. 1. Response times.

Počet klientů	Sekund odezvy	Minut odezvy	Hodin odezvy
10	0,196267	0	0
100	1,962667	0	0
1 000	19,62667	0	0
10 000	196,2667	3	0
100 000	1962,667	33	1
1 000 000	19 626,67	327	5



Obr. 3. Závislost odezvy na počtu klientů.

Pic. 3. Dependences between clients and the response time.

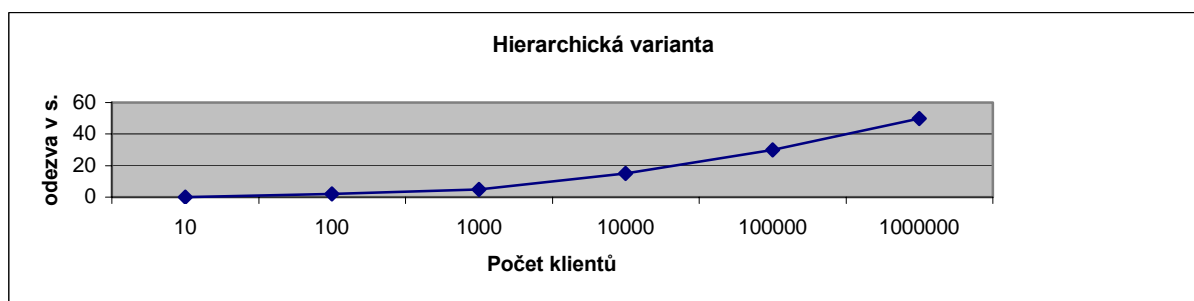
Při použití hierarchie se situace dost podstatně vylepší. Následující tabulka ukazuje pouze dvouúrovňovou hierarchii. V této struktuře se dokonce dá podle požadované odezvy navrhnout potřebná hierarchie.

I v případě, kdy se nesnažíme nějak minimalizovat dobu odezvy, je vidět, že situace je rozhodně optimističtější.

Tab. 2. Odezvy při hierarchii druhé úrovně.  
Tab. 2. Response times in the two level model.

Počet klientů	Počet uzlů	Počet respondentů ve skupině	Sekund odezvy
10	1	10	0,19
100	10	10	1,96
1 000	31	32	5
10 000	255	39	15
100 000	510	196	30
1 000 000	1019	981	50

Situace je dosti podobná technologii CDN, ale jaksí v reverzní podobě. Uzly nerozdělují tok dat, ale naopak jej integrují. Případně se to dá chápat jako P2P naopak.



Obr. 4. Odezvy při hierarchii druhé úrovně.  
Pic. 4. Response times in the two level model.

Co říci k obsahu tohoto obrázku? Možná jenom to, že ani multicast sám o sobě není schopen řešit problém velkého počtu respondentů multimediálního vysílání. Metody, které v této oblasti nastupují, v mnohém připomínají metody řešení problémů s pomocí neuronových sítí [2].

#### Analytické řešení

Mimo simulace sítí je možné popsat řadu parametrů protokolu RTP/RTCP matematicky [4] a dobrat se k podobným výsledkům.

$$\text{PočetKlientů} = \frac{0.75 - \text{Rychlost} \cdot \text{Odezva}}{\text{VelikostPaketu}};$$

Z tohoto vzorce pak můžeme bez problémů vyjádřit dobu odezvy a získat hodnotu, která byla uvedena v předchozí tabulce.

$$10^5 = \frac{0.75 \cdot 5 \cdot 10^4 \cdot x}{736}; x = 1963 \text{ s} = 33 \text{ minut};$$

Teoretickým řešením je, jak bylo uvedeno již výše, použití hierarchie. Pro zjednodušení řešení přijmeme některé předpoklady. V podstatě ne všichni klienti budou odesílat informace serveru, ale informace budou sdružovány po skupinách a budou existovat specializovaní klienti, kteří informace budou slučovat a odesílat dále. Budeme předpokládat, že:

- skupiny mají stejný počet členů,
- odezvy všech skupin a všech klientů jsou stejné,
- délky všech paketů protokolu RTCP jsou stejné,
- strom hierarchie je vyvážený.

V takovém případě bude platit následující vzorec

$$PočetKlientů = \left( \frac{0.75 \cdot Rychlost}{VelikostPaketu} \right)^i \cdot X^i;$$

Následně doba odezvy jedné skupiny klientů v hierarchii se dá vyjádřit následujícím způsobem

$$X_i = \sqrt[i]{PočetKlientů} \cdot \frac{736}{5 \cdot 10^4 \cdot 0.75};$$

A následně celková doba odezvy ode všech klientů k centrálnímu serveru bude vypadat následovně

$$X = \left\{ i \cdot \sqrt[i]{PočetKlientů} \cdot \frac{736}{5 \cdot 10^4 \cdot 0.75} \right\};$$

Problém tohoto vzorce je ten, že obsahuje parametr „i“, který odpovídá úrovni hierarchie. Možná usít se zjistit, zda existuje něco, jako je optimální úroveň hierarchie pro daný fixní počet klientů. Jinými slovy je třeba najít hodnotu optimálního „i“ a to „i<sub>0</sub>“

$$i_0 = Arg \min \left\{ i \cdot \sqrt[i]{PočetKlientů} \cdot \frac{736}{5 \cdot 10^4 \cdot 0.75} \right\};$$

Pokud si odmyslíme konstanty, které na hodnotu argumentu minima nemají vliv, pak vlastně hledáme minimum parametrické funkce

$$f(i) = i \cdot \sqrt[i]{n};$$

A řešením je hodnota

$$i_0 = \ln(n);$$

Optimální úrovně hierarchie jsou uvedeny v následující tabulce

Tab. 3. Optimální úrovně dle počtu klientů.  
Tab. 3. Optimal levels of hierarchy.

Počet klientů	Optimální úroveň hierarchie
10	2
100	5
1000	7
10000	9
100000	12
1000000	14

Docela poučné může být zjištění, jak se s úrovní hierarchie obecně mění velikost odezvy a zhodnotit, zda řízení hierarchických úrovní stojí za přínos v oblasti odezvy protokolu.

Minima jsou označeny silně a rozumné hodnoty jsou zvýrazněny šedým pozadím. Minima jsou totiž velmi plytká a jejich dosažení bude náročné z hlediska řízení celé struktury hierarchie.

Situace velmi připomíná situaci, která funguje v p2p sítích, ale jaksi naopak, zde prostřednictvím takové hierarchie se nešíří obsah, ale sbírají se zpětné informace o vysílání od klientů k vysílacímu serveru. Pochopitelně tato strategie je použitelná, ale vyžaduje odpovídající úpravu protokolu RTP/RTCP a speciálně vytvořené klienty, z nichž někteří budou plnit roli sumarizačních center. Plánování takových služeb není jednoduché a bude vyžadovat logiku podobnou fungování výměnných sítí.

Tuto situaci zobrazuje následující tabulka.

Tab. 4. Minima a rozumný kompromis.

Tab. 4. Minimum of response time and a rational compromise between the response time and the levels of hierarchy.

Hierarchie/ počet klientů	10	100	1000	10000	100000	1000000
1	0.2	1.96	19.63	196.27	1962.67	19626.67
2	<b>0.12</b>	0.39	1.24	3.93	12.41	39.25
3	0.13	0.27	0.59	1.27	<b>2.73</b>	<b>5.89</b>
4	0.14	0.25	0.44	0.79	1.4	2.48
5	0.16	<b>0.25</b>	0.39	0.62	0.98	1.56
6	0.17	0.25	0.37	0.55	0.8	1.18
7	0.19	0.27	<b>0.37</b>	0.51	0.71	0.99
8	0.21	0.28	0.37	0.5	0.66	0.88
9	0.23	0.29	0.38	<b>0.49</b>	0.63	0.82
10	0.25	0.31	0.39	0.49	0.62	0.78
11	X	0.33	0.4	0.5	0.61	0.76
12	X	0.35	0.42	0.51	<b>0.61</b>	0.74
13	X	0.36	0.43	0.52	0.62	0.74
14	X	0.38	0.45	0.53	0.63	<b>0.74</b>
15	X	0.4	0.47	0.54	0.63	0.74

## Literatura - References

- [1] Berka, M. a kol.: Bezpečná počítačová síť, Verlag Dashofer, Praha, 2004 (doplňené vydání 2006), 1230 str.
- [2] Berka, M.: The Optimization of Methods for Multicast in IP Networks, *Konference for Management, Economics and Business Development in the New European Conditions*, Brno, 2006, p. 46-51.
- [3] Perkins, C.: RTP Audio and Video for the Internet, Addison-Veslay, New York, 2005, 414 str.
- [4] Fletcher, R.: Practical Methods of Optimization, Wiley, New York, 1987, 436 str.