Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra fyziky

Hlasové přenosy po Internetu – internetová telefonie

bakalářská práce

Autor: **Martin Kuška**

Vedoucí bakalářské práce: **Ing. Michal Šerý**

ČESKÉ BUDĚJOVICE 2006

Anotace

Tato bakalářská práce se zabývá základy hlasových přenosů po Internetu a datových sítí založených na IP protokolu. Cílem práce je seznámení se základními principy, podmínkami a způsobem jejich zajištění pro přenos hlasu.

Synopsis

This bachelor's thesis is about the bases of voice transmission over Internet and IP protocol based networks. The objective of this thesis is to introduce the main rules of voice transmission, required conditions and ways to guarantee them.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, a že jsem uvedl veškerou použitou literaturu.

……

Martin Kuška

Obsah

Úvod

Dnešní Internet se stal určitou samozřejmostí pro většinu z nás. Celosvětová síť se neustále vyvíjí a nabízí svým uživatelům stále nové služby a technologie. Takovou technologií, která v posledních letech dobývá stále větší počet běžných uživatelů Internetu je internetová telefonie nebo-li přenos hlasu po Internetu (VoIP). Internetová telefonie není sice žádnou novinkou, ale největšího rozšíření mezi běžné uživatele zažívá v posledních několika letech.

Tato práce, zabývající se seznámením s touto technologií, má čtenáři přiblížit a vysvětlit základy přenosu hlasu po Internetu a datových sítí založených na IP protokolu.

1 Co to je internetová telefonie

1.1 Historie Internetu

V šedesátých letech se americká armáda snažila najít způsob, jak zajistit, aby armádní počítače rozmístěné po celém území USA mohly spolu bez problému komunikovat, a to i v případě, že část této sítě bude vyřazena z provozu. Pracovníci RAND Corporation přišli s unikátním řešením - vybudování sítě bez centrálního uzlu. Pokud bude některá linka zničena, informace bude ihned vedena k příjemci jinou trasou.

"Are you receiving this?" - první věta, která byla v srpnu 1969 poslána z University of California v Los Angeles po síti složené ze čtyř uzlů: UCLA, Stanford Research Institute, UC Santa Barbara a University of Utah v Salt Lake City. Tak vznikl Arpanet.

Postupně se k Internetu připojovali další instituce, především university. V této době byl Internet čistě nekomerční záležitostí. Na jeho vybudování přispívala americká armáda a různé vládní agentury. Podnikatelé o něj ani nestáli, protože nenacházeli způsob jak jej využít.

V roce 1989 vymyslel Tim Berners-Lee nový způsob komunikace (původně pro vnitřní potřebu laboratoří CERN, kde pracoval) - hypertextové dokumenty. Texty, které obsahují odkazy na další dokumenty a které mohou být umístěny na jiném počítači, třeba na druhém konci světa. Díky jednoduchému a intuitivnímu ovládání se tento způsob komunikace rozšířil i za brány CERNu a dnes jej známe pod jménem World Wide Web. Zanedlouho byly k dokumentům připojeny i obrázky. Vzhled dokumentů byl přirozenější a umožnil ještě lepší komunikaci. Právě existence WWW spolu s masovým rozšířením osobních počítačů přilákala na Internet miliony nových uživatelů a

Internet začal být zajímavý i pro podnikatele. Komerční provoz na Internetu se datuje od roku 1992, kdy National Science Foundation, která do této doby spravovala páteřní síť Internetu, umožnila připojení i komerčním subjektům.

1.2 Internet včera a dnes

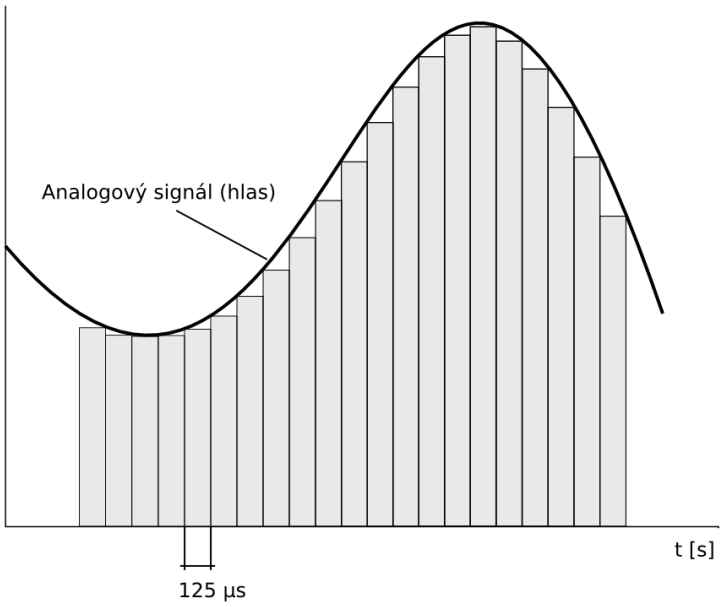
Dnešní Internet je celosvětovou sítí určenou pro přenos dat - mezi jednotlivými počítači, které jsou do něj zapojeny, dokáže přenášet skutečně libovolná data. Například data představující krátké textové zprávy (v rámci elektronické pošty) nebo obrázky a texty v jazyku HTML (*HyperText Markup Language*), v rámci dnes tolik populární služby WWW (*World Wide Web*). Tak proč by Internet nemohl přenášet také data představující zdigitalizovaný lidský hlas - když to samé vlastně dělá i digitální část veřejné telefonní sítě? Poměrně dlouhou dobu byli lidé přesvědčeni, že Internet něco takového nedokáže. Důvodem tohoto přesvědčení byl samotný způsob fungování Internetu, který není nakloněn přenosu „živého“ lidského hlasu, resp. tomu co je pro přenos hlasu zapotřebí zajistit.

Postupem času došlo k výraznému navýšení přenosových kapacit, čímž vzrostla i rezerva, kterou lze využít v případě špičkového souběhu více požadavků. Díky tomu se snížila i pravděpodobnost, že dojde k prodlevě a data dorazí později než je zapotřebí.

K nynějšímu přenosu hlasu po Internetu a IP sítích též přispěl významný pokrok v oblasti digitalizace a komprese hlasu. Způsob, jakým je digitalizován hlas ve veřejné telefonní síti, patří mezi nejméně efektivní a úsporné. Na každý uskutečněný hovor v telefonní kvalitě je vyčleněno pásmo o šířce 64 kb/s. V současnosti používané kompresní metody a techniky v Internetu umožňují tuto hodnotu několikanásobně snížit a dokáží vystačit s pásmem s hodnotami kolem 10 kb/s.

1.3 Přenos hlasu po Internetu: VoIP

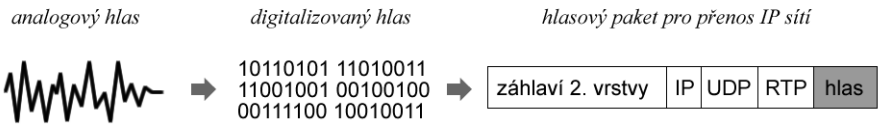
Jak již bylo naznačeno, internetová telefonie je vlastně přenos zdigitalizovaného lidského hlasu po Internetu nebo obecně v datových sítích založených na službách protokolů rodiny TCP/IP (*Transmission Control Protocol / Internet Protocol*). Tento druh přenosu nazýváme VoIP (*Voice Over Internet Protocols*) Toto řešení s sebou přináší řadu výhod, ale i nevýhod, které si přiblížíme dále.



Obrázek 1.3.1 – Princip vzorkování analogového signálu

Zdigitalizovanou podobu lidského hlasu získáváme vzorkováním analogového signálu (lidského hlasu). Znamená to, že v pravidelných intervalech jsou snímány vzorky analogového signálu (obvykle 8000-krát za vteřinu) a jejich hodnoty jsou převáděny do digitální podoby, neboli vyjádřeny jako číselné hodnoty. Tato čísla jsou pak přenášena přenosovou sítí a na druhém konci nastává opačný proces k „digitalizaci“ - podle hodnot

jednotlivých vzorků je zpětně generována původní podoba lidského hlasu. Co je ale velmi podstatné je to, aby jednotlivé vzorky (resp. jejich hodnoty) byly přenášeny dostatečně pravidelně tak, aby na straně příjemce mohly být dostatečně pravidelně použity k rekonstrukci původní řeči. Pokud by pravidelnost nebyla dostatečná a odstupy mezi jednotlivými vzorky byly příliš nerovnoměrné, pak by rekonstruovaný hlas musel být tu „zrychlován“, tu „zpomalován“, neboli celkově zkreslován. Nakonec by při určité míře zkreslení už nebylo rekonstruovanému hlasu rozumět nebo by rekonstrukce nebyla vůbec možná.



Obrázek 1.3.2

Pokud se uskutečňuje přenos hlasu ve veřejné telefonní síti, tak je pro takový hovor vyhrazen přenosový kanál, který má pevně stanovenou šířku pásma. Tato konstantní šířka pásma garantuje pravidelnost přenosu jednotlivých vzorků hlasu a zároveň tím garantuje určitou kvalitu služby QoS (*Quality of Service*). Přenosový kanál s pevně danou šířkou si můžeme představit jako souvislou rouru, která vede od volajícího k volanému, ve všech místech má stejný průměr a přenášená data se nikde nezpožďují.

Naproti tomu Internet a s ním prakticky všechny IP sítě fungují na jiném principu. Jednotlivé části dat se zapouzdří do paketů, které jsou opatřeny hlavičkou, kde je uvedena adresa odesílatele a příjemce, a následně jsou předány síti k doručení. Tyto sítě používají systém přepojovacích uzlů, kde se podle adresy v záhlaví paketu rozhoduje, kudy dál paket poslat, aby se dostal k příjemci. Celý takto fungující přenosový systém se snaží být maximálně efektivní a spravedlivý ke všem došlým požadavkům a snaží se přistupovat ke

všem rovnoměrně. Pokud ovšem dojde k momentálnímu souběhu více požadavků a tudíž není možno vyhovět všem a okamžitě, jsou tyto požadavky rovnoměrně kráceny. Toto krácení může znamenat například i to, že je nějaký paket v tomto uzlu na chvíli pozdržen do doby, než ho bude možno zpracovat. Délka této prodlevy není dopředu známa a nelze ji shora omezit. V důsledku těchto prodlev negarantuje Internet, za jakou dobu dorazí jednotlivé části dat ke svému příjemci, v jakém pořadí ani jaká bude mezi nimi prodleva.

Aby se zamezilo nepříjemnému kolísání zpoždění hlasových paketů, musí se pakety u příjemce ukládat do vyrovnávací paměti, aby se mohly přehrávat konstantní rychlostí. K tomu slouží dva transportní protokoly: RTP (*Real-time Transport Protocol*) a RTCP (*Real-time Transport Control Protocol*). Oba protokoly ale neredukují celkové zpoždění dat ani negarantují QoS.

Digitalizovaný hovor je před odesláním komprimován v některém z dnes existujících kodeků (některé jsou uvedeny v tabulce 1.3.3), aby bylo množství odesílaných dat co nejméně.

kodek	kompresní poměr	vlastnosti	zpoždění
G.711	1:1	PCM rychlostí 64 kbit/s	0,75 ms
G.726	2:1	ADPCM rychlostí 32 kbit/s	1 ms
G.728	4:1	LD-CELP rychlostí 16 kbit/s	5 ms
G.729A	8:1	CS-CELP rychlostí 8 kbit/s	10 ms

Tabulka 1.3.3 – Některé dnes používané kodeky

Dalším neméně důležitým aspektem je signalizace v síti. Signalizace je v telefonních systémech klíčový mechanismus pro navázání a ukončení

spojení. Signalizace také umožňuje další služby, jako jsou služby pobočkových ústředen, apod. Přenos hlasu po IP sítích vyžaduje, aby se IP síť s přepojováním paketů chovala pro přenos hlasových paketů podobně jako tradiční síť s přepojováním okruhů. Pro signalizaci je třeba zajistit dostatečnou šířku pásma a pásmo pro hlasovou konverzaci dobře dimenzovat, protože podcenění v tomto směru vždy vede ke snížení kvality hlasového přenosu.

Právě signalizace umožňuje potřebnou kvalitu komunikace mezi koncovými terminály a sítí a ověřuje potřebu bezpečného spojení s garantovanou úrovní QoS.

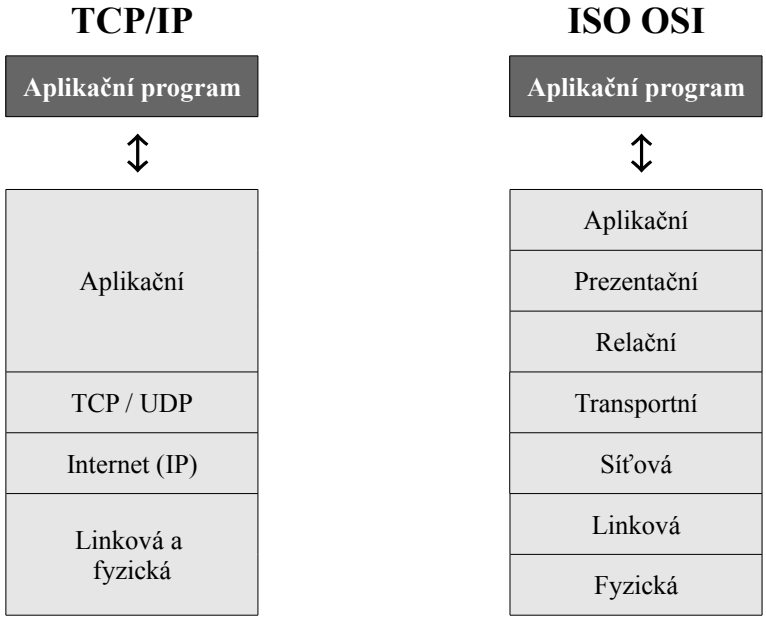
2 Protokoly

2.1 TCP/IP protokol

Protokol TCP/IP je protokolem pocházejícím z dob, kdy přenosové rychlosti byly ve srovnání se současností poměrně dost nízké a chybovost přenosu dat naopak vysoká. Protokol byl navržen pro přenos dat pocházejících z počítačových systémů, proto při vývoji tohoto protokolu nebyly kladeny požadavky na minimální zpoždění při přenosu. Při přenosu paketů sítí může docházet ke zpožděním, která jsou způsobena možným přetížením sítě, ztrátou a následným opakováním paketů, odlišnou cestou paketů, apod. Výše zmíněné vlastnosti nezpůsobují žádné problémy při běžné datové komunikaci. Při přenosu hovorových signálů mohou však znamenat degradaci vlastností přenosu nebo dokonce naprostou nepoužitelnost sítě pro tento druh komunikace.

Protokoly TCP/IP jsou navrženy k zajištění komunikace mezi sítěmi v heterogenním prostředí. Protokoly zajišťují funkce síťové vrstvy a vrstev vyšších a nejsou nijak vázány na přenosové medium případně na protokoly, které umožňují základní přenos informací po tomto médiu. Protokoly TCP/IP je tedy možné provozovat prakticky v jakémkoli přenosovém prostředí od sériového spojení přes telefonní modemy, Frame-Relay, Token-Ring, Ethernet až po současné moderní metody, jakými jsou například přenosové systémy SDH, kde se využívá progresivního způsobu (IP over SDH), který minimalizuje množství přenášených servisních (řídících) informací.

Protokoly TCP/IP korespondují s modelem ISO-OSI, z čehož vyplývá vysoké množství služebních informací pocházejících z protokolů jednotlivých vrstev. Naopak výhodou vrstvové filosofie je jednoduchý, přehledný a přesný popis.



Obrázek 2.1.1 – Porovnání síťových modelů TCP/IP a ISO OSI

2.1.1 Internet Protokol verze 4

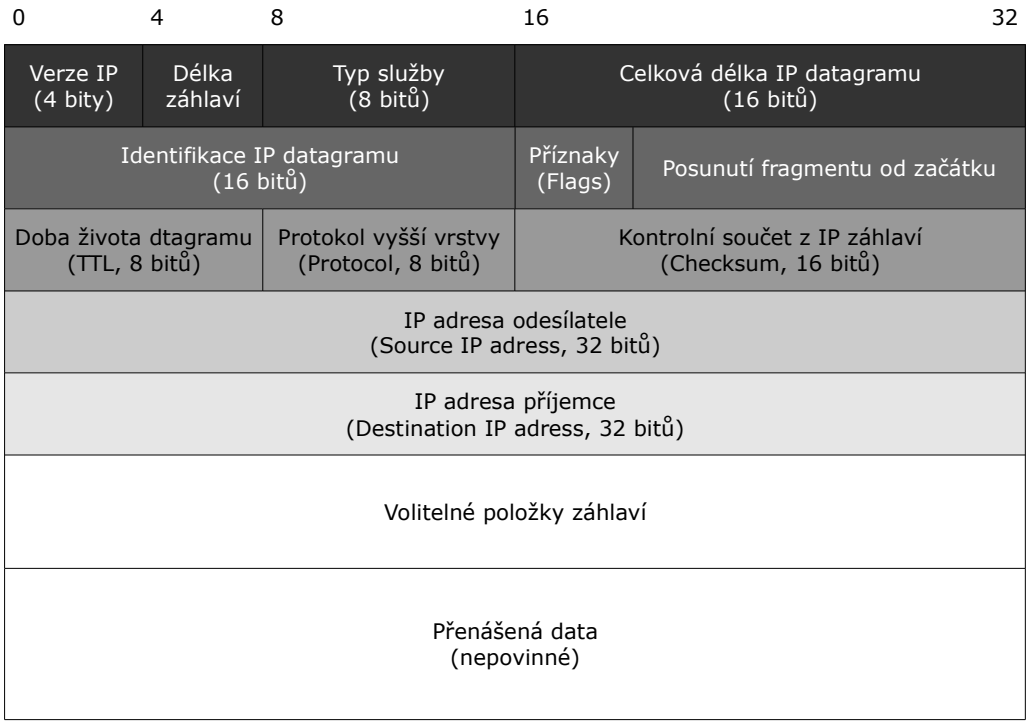
IP protokol (*Internet Protocol*) prakticky odpovídá síťové vrstvě. IP protokol přenáší tzv. IP-datagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese informaci o adrese příjemce, což je úplná směrovací informace pro dopravu IP-datagramu k adresátovi. Síť tedy může přenášet každý IP-datagram samostatně. Na základě informací uvedených v záhlavích datagramů poskytuje síťová vrstva službu bez spojení.

IP protokol je protokol umožňující spojit jednotlivé lokální sítě do celosvětového Internetu. Od protokolu IP dostal také Internet své jméno Zkratka IP totiž znamená IterNet Protocol, tj. protokol propojující jednotlivé sítě. Později se místo InterNet začalo psát Internet a Internet byl na světě.

Data jsou od odesílatele k příjemci dopravována (směrována) přes směrovače (router). Na cestě od odesílatele k příjemci se může vyskytnout celá řada směrovačů. Každý takový směrovač řeší pro každý IP-datagram směrování k následujícímu směrovači samostatně. Data jsou tudíž předávána od směrovače k směrovači. V důsledku to znamená, že IP-datagramy mohou dorazit v úplně jiném pořadí, než v jakém byly od odesílatele odeslány.

IP protokol je tvořen několika dílčími protokoly:

- vlastním protokolem IP
- služebním protokolem ICMP sloužícím zejména k signalizaci mimořádných stavů
- služebním protokolem IGMP sloužícím pro dopravu adresných oběžníků
- služebními protokoly ARP a RARP, které jsou často vyčleňovány jako samostatné, na IP nezávislé protokoly, protože jejich rámce nejsou předcházeny IP záhlavím



Obrázek 2.1.1.1 - Struktura IP datagramu

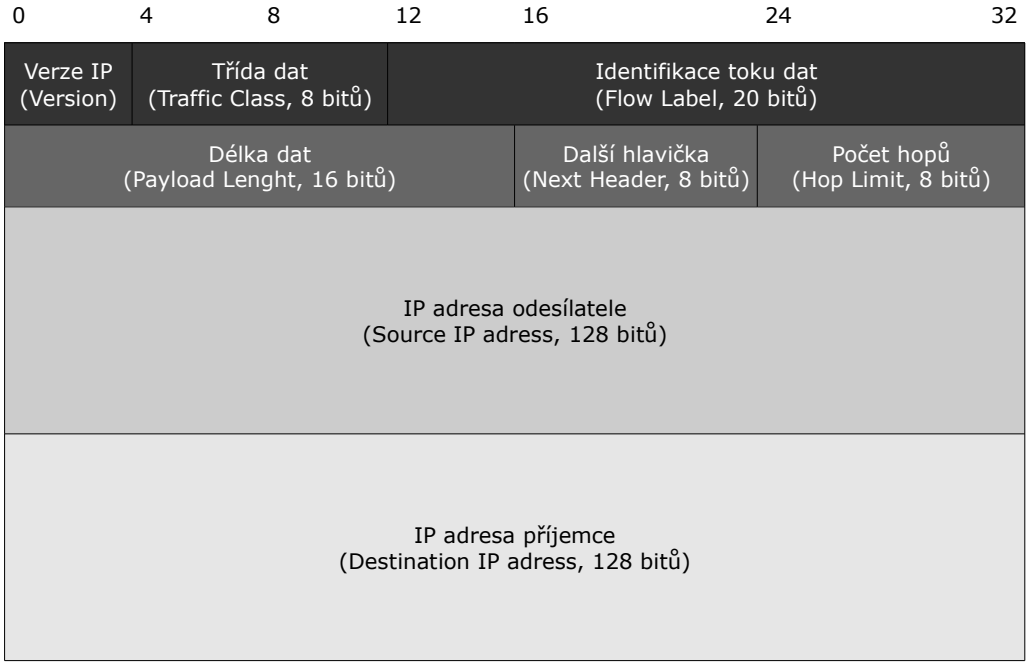
2.1.2 Internet Protokol verze 6

IP protokol verze 6 (*IPv6*) se často označuje jako protokol nové generace (*IP Next Generation*) odkud je i zkratka IPng.

IP verze 6 přináší nejen zvětšení IP adresy ze čtyř na šestnáct bajtů, ale i fyziologicky zcela nový pohled na stavbu IP datagramu. V záhlaví IP datagramu chybí kontrolní součet záhlaví a mnohá další málo využívaná pole jsou přesunuta ze základního záhlaví do nepovinných dalších hlaviček.

IP datagram verze 6 se skládá ze 320 bitů dlouhého základního záhlaví nasledovaného rozšířeními. 320 bitů základního záhlaví se může zdát hodně,

ale je třeba si uvědomit, že jen IP adresy odesílatele a příjemce zaberou 256 bitů.



Obrázek 2.1.2.1 - Struktura základního záhlaví IP datagramu verze 6

Nyní si přiblížíme význam některých polí základního záhlaví.

Pole **verze IP** obsahuje hodnotu 6 pro IP protokol verze 6.

Pole **třída dat** se skládá ze čtyř bitů (nabývá hodnoty 0 až 15). Specifikuje přenášená data pro případ rozhodování v okamžiku zahlcení sítě. V okamžiku zahlcení sítě musí směrovač IP datagramy zahazovat. V tomto poli se specifikuje, které datagramy je možné zahodit dříve než jiné.

Interval 0-15 je rozdělen na dvě části:

- 0-7 je určeno pro klasický provoz
- 8-15 je určeno pro přenosy v reálném čase, jako jsou přenosy videa a hlasu. Datagramy s nižší hodnotou si uživatel přeje zahodit dříve než datagramy s vyšší hodnotou. To však platí pouze v tomto intervalu (8-15), protože interval 0-7 a interval 8-15 se zpracovávají odděleně.

Pole **identifikace toku dat** spolu s adresou odesílatele jednoznačně identifikuje jeden dílčí tok dat v Internetu. Doposud se směrování provádělo výhradně na základě adresy příjemce. Myšlenka spočívá v tom, že datagramy jednoho toku dostanou svou identifikaci. Směrovač pak řeší úlohu směrování (do jakého rozhraní datagram předat) pouze jednou, a to pro první datagram toku a do paměti si poznamená výsledek. Pro další datagramy se nejprve podívá do paměti, a pokud tam nenajde poznamenaný tok, tak teprve potom řeší úlohu směrování. Další datagramy stejného toku tedy bude předávat do stejného rozhraní, aniž by pro každý datagram řešil úlohu směrování (pouze na základě údajů v paměti). Tok je určen adresou odesílatele a polem identifikace toku dat.

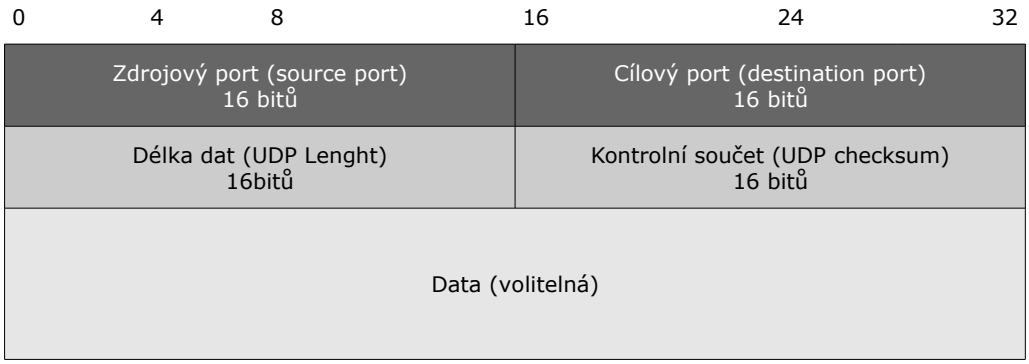
Další možností využití identifikace toku dat je zajištění šířky přenášeného pásma. Směrovače na cestě od odesílatele k příjemci se nakonfigurují tak, aby pro datový tok o jisté identifikaci zajišťovaly určitou šířku pásma. Datagramy docházejí na směrovač, kde se umisťují do vyrovnávací paměti. Za normálních okolností se jedná o frontu datagramů, která z jednoho konce přibývá a z druhého konce se datagramy odebírají (odesílají). Směrovač však nemusí frontu zpracovávat sekvenčně, ale může přednostně vybírat datagramy tak, aby zajistil dohodnutou šíři pásma.

2.1.3 TCP

Protokol TCP (*Transmision Control Protocol*) je spojovanou službou, tj. službou, která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášené bajty jsou číslovány. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena kontrolním součtem. Toto zabezpečení je účinné pouze proti poruchám technických prostředků.

2.1.4 UDP

Protokol UDP (*User Datagram Protocol*) je jednoduchou alternativou protokolu TCP. Protokol UDP je nespojovaná služba (na rozdíl od protokolu TCP), tj. nenavazuje spojení. Odesílatel odešle UDP datagram příjemci a už se nestará o to, jestli datagram k příjemci dorazil nebo jestli se cestou náhodou neztratil. O to se musí v tomto případě postarat aplikační protokol.



Obrázek 2.1.4.1 - Formát UDP datagramu

Z obrázku je patrné, že záhlaví UDP protokolu je velice jednoduché. Obsahuje čísla zdrojového a cílového portu (čísla portů protokolu UDP nesouvisejí s čísly portů protokolu TCP, protokol UDP má svou nezávislou sadu čísel portů). Pole délka dat obsahuje délku UDP datagramu (součet délky záhlaví a délky dat), minimální délka UDP datagramu je tedy 8 bytů (64 bitů), tj. UDP datagram obsahující pouze záhlaví a žádná data. Pole kontrolní součet nemusí být povinně vyplněné. Výpočet kontrolního součtu je tak v protokolu UDP nepovinný.

Zvláštností protokolu UDP je skutečnost, že adresátem nemusí být pouze jednoznačná IP adresa konkrétního síťového rozhraní, ale adresátem může být i skupina síťových rozhraní (stanic), tzn. adresovat lze i oběžník.

Adresovat lze všeobecné oběžníky (*broadcast*), ale podstatně zajímavějším případem je adresování adresných oběžníků (*multicast*). To lze využít třeba u aplikací, kde jsou všem uživatelům poskytována v daném čase stejná data. Příkladem takové aplikace je šíření zvukového záznamu internetem (vysílání rádia do internetu). Tím, že se data šíří pomocí adresných oběžníků, dochází k ohromné úspoře kapacity přenosových cest.

2.2 RTP a RTCP

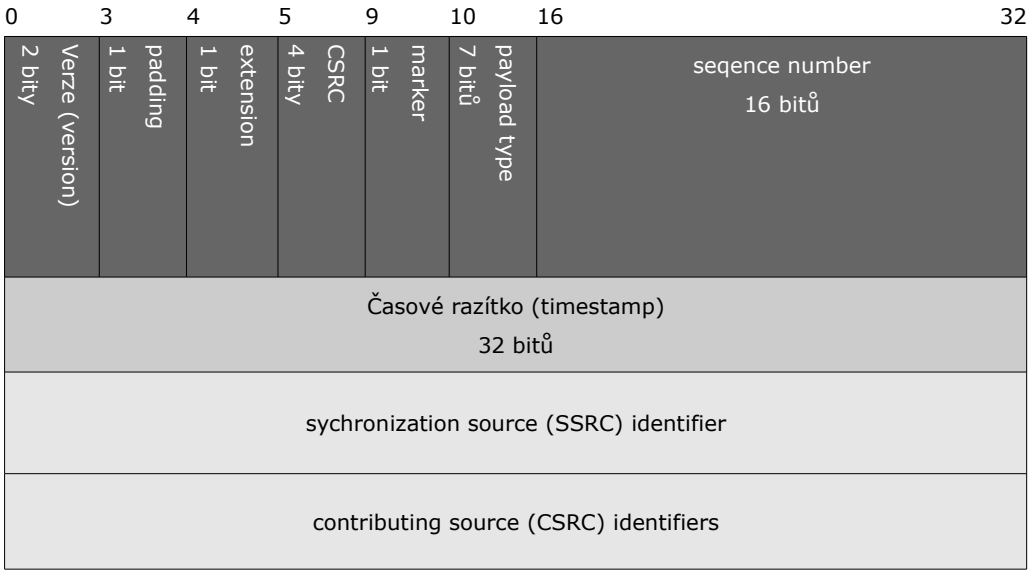
RTP (*Real Time Protocol*) a RTCP (*Real Time Control Protocol*) jsou transportní protokoly užívané IP telefonií. Oba protokoly jsou určeny pro přenos dat v reálném čase. RTP přenáší digitalizované části informací v reálném čase, zatímco RTCP poskytuje zpětnou vazbu, co se týče kvality přenosového spoje.

Služby RTP protokolu:

- identifikace přenášených dat (audio a video kodek)
- kontrola pořadí doručených paketů, v případě potřeby seřazení přeházených paketů
- kódovací/dekódovací synchronizační informace
- sledování informací o doručení

RTP protokol využívá protokol nižší vrstvy UDP k navázání spojení mezi dvěma entitami a ke kontrole integrity dat (kontrolní součet – *checksum*). Samotný RTP protokol negarantuje žádnou kvalitu služby.

Obrázek 2.2.1 zobrazuje záhlaví RTP protokolu. Prvních 12 bytů je v každém RTP paketu, poslední byty obsahující CSRC (*Contributing Source* – zdroj dat) jsou přítomny pouze v případě průchodu dat tzv. směšovačem (termín směšovač označuje v tomto případě systém, který přijímá dva nebo více datových proudů RTP, tyto slučuje a posílá dál).



Obrázek 2.2.1 - Hlavička RTP protokolu

Protokol RTCP využívá ty samé protokoly nižších vrstev jako protokol RTP k periodickému zasílání kontrolních paketů do všech navázaných spojení. Ke každému RTP kanálu běžícím na portu číslo N je přiřazen také kanál RTCP protokolu, který má číslo portu N+1.

Služby RTCP protokolu:

- zpětná vazba kvality distribuce dat, zpětná vazba pro kontrolu aktivních kodeků
- zasílání identifikátoru pro zdroj RTP a je zdrojem pro synchronizaci audio, video datového toku
- průměrný počet spojení a velikost datového toku
- informace o spojení použité k identifikaci spojení

2.3 Provozní informace protokolů

Z obrázků popisující formáty záhlaví protokolů jednotlivých vrstev sítě TCP/IP je patrné, že samotná užitečná informace bude doplněna o značné množství dat pocházejících ze záhlaví jednotlivých protokolů vrstev. Tímto se značně snižuje poměr přenesených dat k užitečné informaci. Je tedy třeba již při návrhu technologického řešení systémů pro přenos hlasových dat s tímto počítat.

3 Kvalita služby (QoS) v IP síti

V tradiční telefonní síti má každý hovor vyčleněnou určitou šířku pásma, zatímco v IP síti, kde sice VoIP vystačí s podstatně menší šířkou pásma, se musí pakety o dostupnou šířku pásma dělit. Hlasové pakety pak mohou na cestě sítí nabírat různá zpoždění a mohou přicházet v intervalech odlišných od intervalů jejich vysílání. Tyto odlišnosti v souvislosti s momentálním stavem IP sítě mají přímý dopad na smysly koncového uživatele, čili posluchače. Do určité hodnoty je kvalita dobrá až únosná, při překročení určitých limitů se ale telefonní hovor stává nepříjemným až nerealizovatelným. Pro zajištění potřebných parametrů pro hlas v IP síti je většinou nutností nasadit nástroje pro zajištění kvality služby, které jsou souhrnně označovány jako QoS (*Quality of Service*). QoS samo o sobě nezamezuje zahlcení sítě, ale zajišťuje upřednostnění určitého druhu přenosu před ostatním. Například zajistí, aby data aplikace jako hlasové služby citlivé na zpoždění, byly vždy na začátku fronty k odbavení.

Mezi nejvýznamnější parametry kvality služby patří:

- Šířka pásma přenosové trasy - objem dat přenesený za jednotku času.
- Ztrátovost paketů - kolik procent paketů nedorazí od odesilatele k adresátovi.
- Zpoždění - doba potřebná k přenosu paketu od odesilatele k adresátovi.
- Změna (proměnné) zpoždění - jak se mění zpoždění jednotlivých paketů během přenosu; přesně lze definovat různými způsoby.

Cílem nástrojů zajišťující QoS je dosáhnout co nejlepších hodnot těchto parametrů. Především:

- poskytnout aplikaci konstantní kapacitu

- minimalizovat zpoždění doručení
- minimalizovat proměnné zpoždění

Důvody, které vedou k nasazení QoS jsou:

Zpoždění (latence) v síti (*delay*)

- zpoždění v přepínání, šíření signálu a serializaci, frontování (*buffering, queuing*) při přetížení

Proměnné zpoždění v síti (*jitter*)

- přetížení způsobí zachycení paketů ve výstupní frontě směrovače/přepínače, doba doručení paketů se mění v závislosti na aktuálním zatížení směrovačů/přepínačů

Ztráta paketů (*packet loss*)

- výstupní ztráty (*output drops*), vyčerpání front směrovačů/přepínačů
- vstupní ztráty (*input drops*), přetížení procesoru/přepínacího systému zařízení

3.1 QoS z pohledu aplikace

QoS je schopnost sítě sloužit dané aplikaci efektivně bez omezení její funkce či výkonu. Aplikaci, která má přísné nároky na QoS nazýváme jako kritickou.
QoS je sada nástrojů sloužící k ovládání:

- šířky pásma přenosové trasy (*Bandwith*)
- zpoždění (*Delay*)
- proměnného zpoždění (*Jitter*)
- ztráty paketů (*Packet loss*)

3.2 QoS z pohledu provozu

Šířka pásma, zpoždění a ztráty mohou být chápany jako zdroje, protože každé aplikaci lze přidělit jen aktuálně dostupné množství dle situace. QoS z pohledu provozu je pokročilé řízení zdrojů sítě.

3.3 Důsledky provozování kritických aplikací bez Quality of Service

Vedlejší provoz může zabrat pásmo kritickým aplikacím, především se jedná o přenos velkých objemů dat generující dlouhé pakety (protokol FTP). Problém se objevuje ve většině sítí WAN, kde dochází při saturaci linek k vytváření front na hraničních směrovačích. Neřešení QoS má dopad na kvalitu provozování Real-time aplikací jakou VoIP je. Zatímco tradiční IP aplikace jako web, e-mail, atd. se dokáží se saturovaným provozem na linkách WAN vyrovnat, tak aplikace v reálném čase ztrácejí neúnosně mnoho informací, především díky nadměrnému zpoždění. Při VoIP může být hovor trhaný, chvílemi se může zcela přerušit, případně dojde k rozpadu navázaného spojení.

IP telefonie je kritickou aplikací. S rozvojem Internetu a hektickým zvyšováním výkonů výpočetní techniky trh vyvinul značný tlak na vývoj standardů pro IP telefonii a v posledních letech především na mechanismy, které umožňují kontrolu pásma v IP sítích. Hovor může mít relativně skromné nároky na pásmo, ale nikoliv na zpoždění. Aplikace tedy požaduje zabezpečení kvality služby QoS.

ToS	→	CoS	→	QoS
označení paketu (hlavička IP)	→	roztřídění paketů	→	kvalita služby

Obrázek 3.2.1 - Mechanizmus zajištění QoS

Základním cílem QoS je dosáhnout pásma a zpoždění pro konkrétní aplikaci. CoS (*Class of Service*) umožňuje roztřídit do skupin různé toky paketů které mají odlišné požadavky na zpoždění a pásmo. ToS (*Type of Service*) je pole v hlavičce protokolu IP umožňující nastavit CoS. V současné době ToS používá tři bity, jenž dovolují vyčlenit osm skupin, neboli CoS (0-7), což je označováno jako IP Precedence. Novější mechanizmy označované jako DiffServ používají v ToS šest bitů a další dva pro řízení toku.

3.4 Způsoby dosažení QoS v IP síti

Při implementaci QoS na úrovni protokolu IP existují dva hlavní přístupy řešení: integrované služby (*Integrated services*, ve zkratce *Intserv*) a rozlišované služby (*Differentiated services*, ve zkratce *Diffserv*).

3.4.1 Intserv

U přístupu intserv aplikace přímo požadují od počítačové sítě zajištění určitých kvantitativních parametrů spojení, například jistou minimální propustnost. K zajištění těchto parametrů se používají rezervační protokoly, například RSVP (*Resource ReSerVation Protocol*) [RFC2205]. Tento přístup se

ukazuje jako příliš restriktivní vzhledem k využití kapacity počítačové sítě a přináší značnou režii - směrovače musí udržovat stavovou informaci o každém procházejícím spojení.

Intserv rozšiřuje základní model služby v IP, tj. best-effort, o další typy služeb podle vzoru QoS v ATM: zaručené služby (*Guaranteed Services*) a služby s řízeným zatížením (*Controlled-Load Services*). Záměrem je rozšířit IP o možnosti provozu v reálném čase. Základní nevýhodou je, že intserv vyžaduje přizpůsobení všech aplikací signalizaci RSVP a dále spolupráci síťových prvků, které musí každý datový tok zpracovat izolovaně. To klade značné nároky na výkon síťových prvků. Pro široké použití je intserv nepraktický.

Služby s řízeným zatížením zajišťuje pro datový tok stejnou kvalitu služeb, jako nezatížená síť best-effort. Nezaručují se explicitně žádné vlastnosti týkající se zpoždění. Služby s řízeným zatížením zajišťuje, ze dohodnuté datové toky nezahltí síťové prvky. Pakety nesplňující dohodnuté podmínky jsou zpracovány neprivilegovaně na úrovni služby best-effort.

Zaručené služby zaručují hodnotu maximálního zpoždění při dané přenosové rychlosti a to, že paket nebude zahozen z důvodu přeplnění některé fronty. Cílem naopak není minimalizovat rozdíly zpoždění (*jitter*). Služba je popsána tzv. fluid modelem, jehož analogií je dedikovaný kanál stejné přenosové rychlosti. Vychází se při tom z faktu, že lze vypočítat maximální zpoždění datového toku v uzlu při znalosti rychlosti výstupní linky a parametrů datového toku.

QoS pro konkrétní tok dat:

- použitelnost v rozsáhlých sítích
- jedná se o mechanizmus pro dynamickou změnu QoS
- aplikace provede požadavek rezervace trasy pro přenos

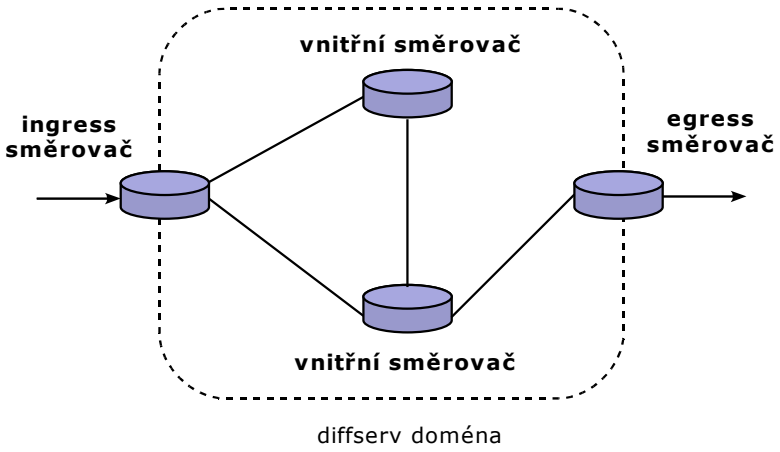
Používá se signalizační protokol RSVP (*Resource ReSerVation Protocol*), rezervace se provádí krok za krokem po celé cestě daného přenosu od příjemce k odesílateli. Umožňuje vytvoření , změnu a obnovení rezervace. Podporován je na IP verze 4 (*IPv4*) i IP verze 6 (*IPv6*).

3.4.2 Diffserv

Architektura definuje třídy služeb založené na klasifikaci toků. Označení paketů je provedeno pomocí vzorků v oktetu TOS u IPv4 nebo nastavením parametru třídy provozu u IPv6 (*Traffic Class Octet*). Smyslem je umožnit provozování rozdílných tříd služeb na společné síťové infrastruktuře. Každý tok je kontrolován a označen v souladu s profilem služby. K označení se používá TOS pole v hlavičce IP paketu čímž dochází k priorizaci hlasového provozu před datovým.

Každý IP paket vstupující do počítačové sítě je označen značkou, která říká, jak má být s paketem zacházeno - neboli určuje třídu přenosu poskytnutou paketu. Místo v hlavičce IP paketu určené pro tuto značku se nazývá DSCP (*Differentiated Services CodePoint*). Toto označení probíhá jen na vstupu do počítačové sítě na tzv. ingress směrovači. Během přenosu paketů počítačovou sítí další směrovače pouze přečtou značku každého paketu a řídí se podle ní při zpracování paketu. Počet různých značek je relativně malý, v současném návrhu diffserv jich je 64. Směrovače přidělí určité prostředky každé třídě přenosu a zajišťují určitý vztah mezi jednotlivými třídami. Například může být

stanoveno, že pakety s určitou značkou mohou být poslány dále jen pokud nejsou ve frontě čekající pakety s jinou značkou. Takto fungující síť se nazývá diffserv doména. Rozlehlá počítačová síť může být rozdělena na několik propojených diffserv domén. V každé z nich probíhá zpracování paketů samostatně. Struktura diffserv domény je znázorněna na obrázku 3.4.2.1.



Obrázek 3.4.2.1 - Struktura diffserv domény

4 Protokoly a kodeky používané pro přenos hlasu v IP síti

V IP telefonii v současnosti existují dva hlavní protokoly pro signalizaci SIP a H.323. Protokol SIP (*Session Initiation Protocol*) je určený pro navazování interaktivních relací zahrnující nejrůznější média, včetně hlasu. Uživatele lze prostřednictvím SIP lokalizovat a komunikovat s nimi bez hledu na konkrétní koncová zařízení, která právě používají. Základní výhodou

protokolu SIP je jeho jednoduchost.

Protokol H.323 podporovaný organizací ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*) je skupina protokolů vyvinutá a podporovaná ze strany telekomunikačních provozovatelů, protože přenáší koncepci signalizace známou z telefonní sítě. H.323 zastřešuje řadu nových protokolů (H.225.0, H.245, H.450.x), ale mnohem více jich přímo přebírá (RTP, RTCP, G711, ...). Implementace jsou zpravidla stabilní a dobře pracující. Velkou výhodou je jeho protokolová vyzrálost. Při jeho vývoji se autoři snažili zachytit, definovat a ošetřit všechny možné stavy. Standard H.323 je robustní a další rozšiřování nebo přidávání nových funkcí je komplikované a monolitický charakter znesnadňuje zásahy uživatele-vývojáře do prvků sítě H.323.

4.1 Protokol H.323

Protokol H.323 využívá pro přenos informací služeb protokolu TCP, což zajišťuje spolehlivý přenos mezi jednotlivými účastníky spojení. Vlivem výše zmíněných nedostatků IP sítě však může využití služeb protokolu TCP s sebou přinést i problémy, které se projeví velkým zpožděním relací protokolu H.323.

Na vlastnostech protokolu se výrazně projevila skutečnost, že tvůrci protokolu měli velice blízko k technologiím telefonních sítí a poněkud opomněli výhodné vlastnosti a zvyklosti ze sítí počítačových. Protokol definuje v síti několik center a na jejich existenci a funkčnosti je závislá funkčnost celého systému. Tento přístup vnáší do celého systému potenciální nebezpečí selhání celku z důvodu poruchy pouze jedné z jeho částí. Odborníci z prostředí

počítačových sítí se snaží maximálně oprostit od tohoto modelu a celý systém decentralizovat a tím zvýšit jeho odolnost proti možným poruchám. Na druhou stranu existence těchto center přináší řadu výhod, které umožňují například možnost adresace z využitím telefonních čísel, sběr dat nutných pro tarifikaci provozu, definovat centrálně brány pro určité směry atd.

Logická topologie sítě pro přenos hlasových dat s využitím protokolu H.323 je definovaná pomocí několika základních pojmů:

Entita	Každá komponenta H.323, včetně terminálů, bran (*Gateway*), řadičů spojení (*Gatekeeper*), řadičů konferencí (*Multipoint Controller*) a dalších jednotek nutných pro zajištění spojení.
Koncový bod (*Endpoint*)	Jedná se o koncové terminály, brány (*Gateway*) a řadiče konferencí (*Multipoint Controler*). Každý koncový bod sítě H.323 může sestavovat a rušit spojení, případně být volán. Každé hovorové spojení v síti H.323 začíná a končí vždy koncovým bodem.
Brána (*Gateway*)	Bránou se rozumí rozhraní mezi sítí H.323 a jinými sítěmi. Brána je koncovým bodem H.323 sítě a zajišťuje v reálném čase dvoucestnou komunikaci mezi koncovými body H.323 a koncovými body jiných sítí.
Řadič spojení (*Gatekeeper*)	Řadič spojení je H.323 entita zajišťující překlad adres a řízení přístupu pro všechny H.323 koncové body tj. terminály, brány a ostatní příslušenství. Řadič spojení může pomocí signalizace dohlížet nad všemi službami, které síť nabízí koncovým účastníkům, včetně řízení, dohledu a sběr tarifních informací.
Řadič konference (*Multipoint Controler*)	Řadič konference (zkráceně označovaný MC) je stanicí, která řídí v reálném čase konferenci více uživatelů.

Přesná a úplná definice jednotlivých pojmů je součástí doporučení ITU-T H.323.

Celý systém je možno provozovat ve dvou možných režimech:

1) Sestavení spojení se provede přímo s koncovým účastníkem, nebo s bránou

   V tomto případě musí koncový bod, který spojení sestavuje znát nejen telefonní číslo volaného účastníka, ale i IP adresu cíle. V druhém případě, kdy hovor má být směrován mimo IP síť musí volající sám rozhodnout o použití určité brány, přes kterou bude hovorové spojení sestaveno. Tento způsob je použitelný pouze pro malé sítě u kterých není potřebný celkový ohled a tarifní údaje.

2) Sestavení spojení provádí každý účastník sítě pomocí gatekeeperu

   V tomto případě postačuje k realizaci spojení znalost cílového telefonního čísla a IP adresa gatekeeperu. Volající účastník osloví gatekeeper, předá mu telefonní číslo se kterým chce sestavit hovorové spojení. Gatekeeper disponuje údaji, podle kterých zjistí IP adresu kam má být volaní směrováno, případně určí vhodnou bránu (většinou podle finančních nákladů), přes kterou bude hovor dále směrován mimo IP síť. Gatekeeper také vyhodnotí, zda má účastník na dané spojení kategorii a zaznamená údaje nutné pro zpoplatnění služby.

4.2 Protokol SIP

4.2.1 Popis protokolu

Protokol SIP je určen pro spojování, rozpojování a dohled nad spojením mezi dvěma nebo více účastníky. Není svázán s žádnými konkrétními protokoly pro vlastní přenos multimediálních dat. Uvnitř zprávy protokolu SIP pro navázání spojení je proto zapouzdřena zpráva jiného protokolu, která specifikuje použité kódování pro multimediální data, jejich parametry a čísla portů, na kterých mají být data vysílána nebo přijímána. Obvykle se pro tento účel používá protokol SDP (*Session Description Protocol*), který je rovněž textový.

Zařízení pracující s protokolem SIP mohou komunikovat se zařízeními pracujícími s protokolem H.323 pomocí brány SIP/H.323. Tato brána převádí signalizační zprávy obou protokolů. Protože pro vlastní přenos multimediálních dat používají zařízení typu H.323 i SIP obvykle protokol RTP, mohou po navázání spojení prostřednictvím brány dále komunikovat přímo.

SIP je protokol typu klient-server. Klient navazuje spojení se serverem. Jedno zařízení může pracovat současně jako klient i server. Například telefon pracuje jako klient pro odchozí volání a jako server pro příchozí volání. Zprávy protokolu SIP jsou dvojího druhu – Request a Response (žádosti a odpovědi).

Seznam zpráv žádostí (Message Requests):

INVITE	žádost o navázání spojení nebo o změnu parametrů existujícího spojení
BYE	žádost o rozpojení spojení
ACK	klient potvrzuje, že obdržel odpověď na žádost INVITE
REGISTER	žádost o registraci klienta na registračním serveru
CANCEL	žádost o zrušení probíhající žádosti INVITE
OPTIONS	žádost o zaslání podporovaných funkcí na serveru
INFO	přenos informací během hovoru

Seznam zpráv odpovědí (Message Responses):

1xx (Trying, Ringigng, Call is being forwarded, Queued)	Informační odpověď, žádost obdržena, její zpracování probíhá. Posílá proxy nebo redirect server trvá-li směrování hovoru delší dobu.
2xx (OK)	Úspěšné provedení žádosti
3xx (Multiple choices, Moved permanently, Moved temporarily, See other, Use proxy, Alternative service)	Přesměrování (odpověď od redirect serveru)
4xx (Bad request, Unauthorized, Payment required, Forbidden, Method not allowed, Not acceptable, ...)	Chyba způsobená klientem (například špatná syntaxe žádosti)
5xx (Internal server error, Not implemented, Bad gateway, Service unavailable ...)	Chyba způsobená serverem
6xx (Busy everywhere, Decline, Does not exist anywhere)	Obecná chyba, žádost nemůže být provedena ani na jiném serveru

Hlavička zpráv specifikuje číslo volajícího, volaného, cestu spojení a typ zprávy. Krátké vysvětlení nejdůležitějších je uvedeno níže.

Některé hodnoty SIP hlaviček:

To		Volaný uživatel nebo adresa, která má být registrována na registračním serveru.
From		Původní odesílatel žádosti (volající nebo registrující se uživatel).
Subject		Popisuje typ volání.
Via		Indikuje cestu zprávy, každý proxy server směrující žádost vloží svoji adresu na začátek této hlavičky. Při přenosu odpovědi zpět servery opět své adresy vyjímají. Proxy server musí vždy ověřit, zda následující adresa, na kterou posílá žádost již není v této hlavičce, tím se zabrání smyčkám.
Call-ID		Identifikace hovoru nebo registrace, kterou pro každý hovor resp. registraci vygeneruje klient. Následující žádosti INVITE, které pouze mění parametry již existujícího hovoru mají stejnou hodnotu Call-ID jako původní žádost INVITE, ale vyšší hodnotu CSeq.
CSeq		Pořadové číslo žádosti v rámci jednoho hovoru, je-li stejná žádost opakována, protože na ní nepřišla odpověď, má stejnou hodnotu Cseq. Následné žádosti INVITE pro stejný hovor posílané pro změnu parametrů existujícího hovoru mají vždy vyšší hodnoty CSeq.
User Agents - uživatelé jsou typu:	**UAC**	(UA Clients), inicializuje zprávy Request (žádosti)
	UAS	(UA Servers) , přijímá žádosti a vrací Response (odpovědi)
	UA	Většina SIP aplikací je schopna fungovat obousměrně (např. IP SIP telefon), a proto budeme používat označení UA

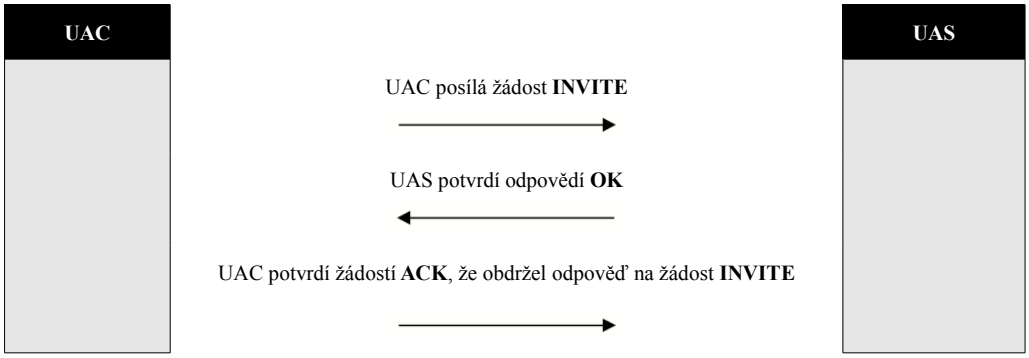
Síťové servery

Používají se dva typy:

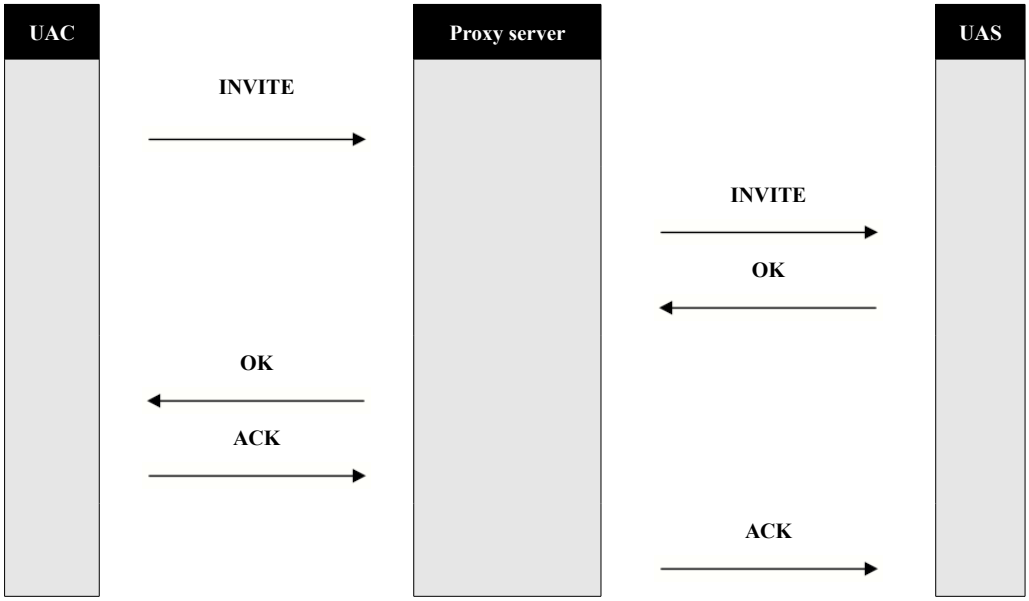
Proxy server	Obsahuje funkce klienta a serveru. Dokáže interpretovat a přepisovat hlavičky žádostí.
Redirect server	Akceptuje SIP žádosti a přeposílá klientovi zpět přesměrované odpovědi obsahující adresu dalšího serveru. Nedokáže přijímat a zpracovávat volání.
SIP Server	Protože většina aplikací síťových SIP serverů umožňuje režim Proxy i Redirect serveru (navíc je často doplněna o lokalizační a autorizační službu – většinou s LDAP), budeme hovořit o SIP serveru.

4.2.2 Popis signalizačních procedur

UAC (klient, který inicializuje zprávy) může kontaktovat UAS (klient, který přijímá žádosti) přímo nebo prostřednictvím jiného serveru, který pracuje jako tzv. proxy nebo redirect server. Přímé volání se používá, pokud klient zná IP adresu serveru, u kterého se nachází volaný uživatel. Možný průběh signalizačních zpráv mezi UAC a UAS je následující:



Častější je případ, kdy klient nezná IP adresu serveru, u kterého se volaný uživatel nachází. V tomto případě klient naváže spojení s proxy nebo redirect serverem. Ten nejprve prostřednictvím lokalizační služby zjistí IP adresu serveru volaného uživatele. Uživatelé mohou totiž požádat svůj telefon (který pracuje jako SIP klient i server), aby se registroval u registračního serveru. Registrační server předá informaci o tom, kde se uživatel právě nachází lokalizační službě. Proxy server potom sám naváže spojení se serverem volaného uživatele a potvrdí navázání spojení volajícímu klientu.



Základní adresa uživatele má tvar e-mailové adresy (jmeno@domena.cz), lze ji též zapsat jako URL ve tvaru sip:jmeno@domena.cz . Adresa může obsahovat i další údaje popisující způsob kontaktu uživatele. Úplný tvar adresy je následující:

sip:[username[:heslo]@]hostname [:port] [;parametr;parametr …][?hlavička&hlavička …]

Hranaté závorky označují nepovinné části. Jediným povinným údajem je ve skutečnosti jméno zařízení (počítače, telefonu, atd.). Místo jména může být

uvedena přímo IP adresa zařízení. Před jméno zařízení lze volitelně uvést jméno uživatele případně heslo na tomto zařízení. Pracuje-li zařízení jako brána do klasické telefonní sítě, ve které se uživatelé označují telefonními čísly, uvádí se místo jména uživatele jeho telefonní číslo. Za jménem zařízení může následovat seznam parametrů a hlaviček. Parametry určují jaký protokol má být použit v transportní vrstvě (UDP nebo TCP), zda je uvedeno jméno nebo telefonní číslo uživatele a další údaje. Hlavičky se potom stávají přímo součástí signalizační zprávy.

4.3 Protokol IAX

Protokol IAX je po protokolu SIP dalším krokem ve zjednodušení komunikačních VoIP protokolů. IAX je zkratka „*Inter-Asterisk eXchange*“ protokolu používaného softwarovou open-source PBX ústřednou Asterisk firmy Digium. Hlavním použitím je udržování VoIP spojení mezi Asterisk servery. V současnosti se již začíná také prosazovat v oblasti spojení mezi servery a klienty používajícími tento protokol. Jedná se o jediný protokol sdružující vlastnosti signalizačního a přenosového protokolu.

Primárním cílem protokolu bylo minimalizovat nezbytnou šířku pásma určenou pro signalizaci a vlastní přenášené médium (v našem případě „hlas“). Dalším důležitým cílem bylo poskytnou přirozenou podporu pro NAT (*Network Address Translation*) transparentnost . Pro vynucení průchodu přes NAT firewally není již při použití IAX potřebná žádná další konfigurace. Protokol je vytvářen s ohledem na pozdější rozšiřitelnost a vylepšení.

IAX je obecně velmi robusní a plnohodnotný protokol, zároveň je však jednoduchý. Typově je to protokol typu peer-to-peer, koncové body udržují stavy asociované s protokolovými operacemi. IAX lze použít jako transportní protokol prakticky pro všechny typy přenášených dat. U hlasového přenosu

protokol nerozeznává používané kodeky. IAX design byl vytvořen na základě zkušeností s mnoha dnešními řídícími a přenosovými standardy včetně *Session Initiation Protocol* (SIP), *Media Gateway Control Protocol* (MGCP) pro řízení a *Real-time Transfer Protocol* (RTP) pro streamování média přenosu.

Základní vlastností IAX je multiplexování signalizace a vícenásobných média streamů do jediného UDP toku mezi dvěma počítači. Namísto použití RTP protokolu využívá pro komunikaci mezi koncovými body protokol UDP (obvykle jediný port 4569) a to jak pro vlastní data, tak pro signalizaci. Hlasový provoz je přenášen uvnitř pásma, což vytváří předpoklad pro překonání firewallů a je tak vhodnější pro práci za NAT (*Network Address Translation*). Tato skutečnost je hlavním rozdílem oproti protokolu SIP, který pro přenos informací používá RTP tok mimo pásmo a proto se potýká s problémem překonání NAT. Uvádí se, že protokol IAX může ztrojnásobit počet volání přenášených přes jediný megabit. Při použití kompresního kodeku G.729 lze například přes 1 MB pásmo uskutečnit až 103 volání.

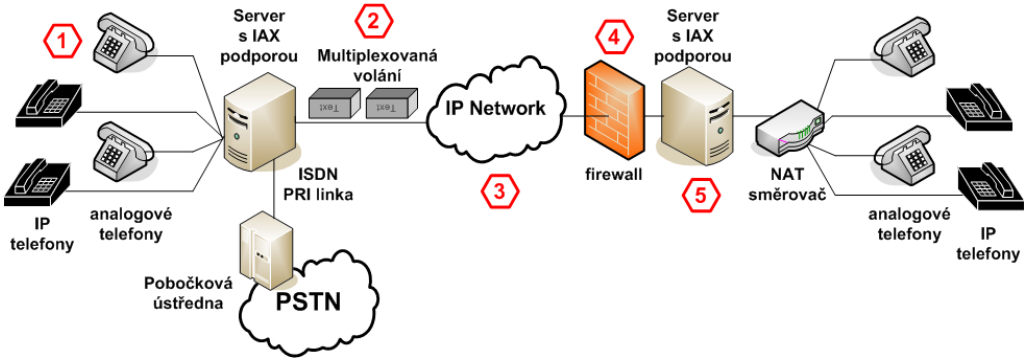
Data jsou tedy z vícenásobných volání sloučena do jednotného souboru paketů, jeden IP datagram může doručit současně informace pro více než pouze jedno volání. Zároveň je prováděno redukování efektivní IP režie bez generování dalšího nežádoucího zpoždění. Tato skutečnost je velkou výhodou pro VoIP uživatele (IP záhlaví je procentuálně větší než pásmo využité pro vlastní přenášený hovorový datový tok.

IAX je binárním protokolem, je navržen a uspořádán způsobem určeným pro redukci nadbytečných dat a to speciálně v hlasovém streamu. Důvodem binární formy protokolu je jednak jeho zjednodušení a jedna skutečnost, že binární forma je základní formou komunikace používané technikou (počítače, IP telefony, …). Binární struktura protokolu byla zvolena také s ohledem na efektivnost šířky přenosového pásma. Kromě toho je IAX specificky optimalizován pro vytvoření větší efektivity využití šířky

přenosového pásma pro individuální volání. Efektivnost šířky přenosového pásma pro jiné typy datových toků je do určité míry obětována pro individuální volání.

Veškerá signalizace je umístěna uvnitř odpovídající 2 vrstvy (data, link). Tóny dvoutónové multifrekvenční volby (DTMF - *Dual-tone multi-frequency*) jsou vždy vysílány stejnou cestou jako zbývající signalizační data, tím jsou spolehlivě přeneseny na druhý konec konkrétního spojení.

IAX protokol přenáší audio pakety pouze s 4 bytovým záhlavím a na vlastní příkazy použijí pouze velmi malou část přenosového pásma. Pro vícenásobná volání redukuje IAX režii každého kanálu kombinováním dat několika kanálů do jednoho paketu, neredukuje tím tedy pouze počet záhlaví, ale také počet paketů (výhodné pro bezdrátové sítě).



Obrázek 4.3.1 - Principiální schéma možností IAX protokolu

Popis k obrázku 4.3.1:

1) Generovaný hovor je vyslán přes Server s IAX podporou (v našem případě Asterisk), který plní funkci pobočkové ústředny, softwarové ústředny (*softswitch*) a brány (*gateway*). Server může zakódovat hovor do IAX formátu a to jak hovor z klasické PSTN připojené

prostřednictvím PRI linky, tak hovor v některém z VoIP protokolů.

2) Server s IAX podporou zapouzdří volání do IAX protokolu a multiplexuje vícenásobná volání do jednoho kanálu, eliminuje tím nadbytečné paketové záhlaví.
3) Volání je směrováno přes IP síť.
4) Volání prochází bez problémů přes firewall. Důvodem je skutečnost, že komunikace probíhá přes UDP port.
5) Server s IAX podporou rozlišuje na který telefon dané volání směrovat. Důvodem je skutečnost, že multiplexované IAX médium obsahuje také signalizaci.

4.4 Kodeky

Má-li se přenést hlas IP prostředím, je potřeba nejen navázat spojení, ale i spojení opět ukončit. Základním pilířem celého hovoru je přenos vlastního telefonního hovoru. A aby bylo možno převést hlas na data, data na hlas, případně správně vyměnit data mezi dvěma IP telefony, bylo potřeba ustanovit i různé způsoby převodu – kodeky. Přenést hlas sítí je vcelku jednoduché, nezáleží-li na kvalitě a rychlosti. Pro potřeby IP telefonování je však vhodné, aby byly splněny některé požadavky, mezi něž patří co nejmenší nutná šířka přenosového pásma a co nejmenší zpoždění při přenosu. Velkou měrou obě kritéria ovlivňují právě použité kodeky, které se starají o převod analogového hlasu do datové podoby a jeho kompresi (a samozřejmě i o opačný směr převodu).

Čím kvalitnější je komprese, tím déle trvá, a tím větší blok dat může potřebovat pro svoji funkci. Nejkvalitnější by komprese byla v tom případě,

kdyby se nahrál celý hovor a poté se teprve zkomprimoval. To však není vhodné pro hovory, kdy obě strany chtějí spolu aktivně mluvit, a ne pouze poslouchat nahrané myšlenky a postřehy protistrany. Naopak, nejrychlejší je převést hlas do nějaké jednoduché datové podoby a okamžitě poslat sítí. Takový přístup má však zase veliké nároky na šířku pásma přenosu.

Tento problém je známý, a proto se objevilo hned několik různých kodeků. Navzájem se liší několika parametry – kvalitou komprese, nutným datovým tokem pro kvalitní přenos a velikostí jednotlivých paketů. Některé kodeky jsou volně k dispozici, za používání jiných je třeba platit.

Kodek	Datový tok [kb/s]	Délka paketu [ms]	Komentář
G.711	64	10 - 20	Výborná kvalita nejnižší zpoždění
G.726	16 - 40	20	Dobrý kompromis
G.729	8	20	Licencovaný, nejlepší kompromis
G.723@6.3	6,3	30	Licencovaný, nízká šířka pásma
GSM-EFR	12,2		Mobilní telefony (pro srovnání)

Tabulka 4.4.1 – Přehled nejznámějších kodeků

U hodnoty datového toku je zároveň nutné počítat s tím, že maximální možný výsledný proud dat bude větší. Je to dáno skutečností, že každý paket obsahuje navíc IP a UDP hlavičky, což připočtu a velikosti odesílaných paketů už hraje nezanedbatelnou roli. Všechny kodeky naštěstí počítají s tím, že přenést ticho je zbytečným zatěžováním datové linky nulovou informací, proto se používá i detekce a potlačení ticha (silence suppression), při kterém se po

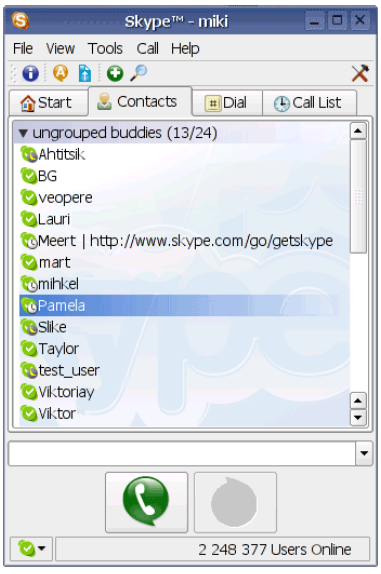
síti nic neposílá. A ideální kodek? Neexistuje. Ale dá se říci, že mezi nejčastěji používané a doporučované patří G.711, pokud není nutné použít co nejmenší šířku pásma.

5 Softwaroví klienti pro VoIP po Internetu

Aplikací pro provozování VoIP přes Internet je nepřeberné množství, od freeware přes open source až po komerční. V této kapitole si v krátkosti představíme několik aplikací pro internetovou telefonii. Zaměříme se především na aplikace, které jsou distribuovány zdarma a jejich běžné používání také není nijak zpoplatněno.

5.1 Skype

Softwarový klient Skype je nejenom programem určeným pro internetovou telefonii, ale je také instant messengerem. Skype je mezi běžnými uživateli pravděpodobně nejrozšířenějším programem pro VoIP po Internetu a mezi jeho přednosti patří především dobrá průchodnost přes firewally a NAT (překlad adres) v síti, snadné ovládání, ukládání kontaktů do adresáře a komunikace zabezpečená šifrováním. Jak jsem se již zmínil, tak je



Skype také instant messenger a umí tedy posílat i textové vzkazy (obdoba ICQ, Jabber, AIM). Hlavní předností je velmi vysoká kvalita přenosu hlasu, která je limitována pouze kapacitou internetového připojení.

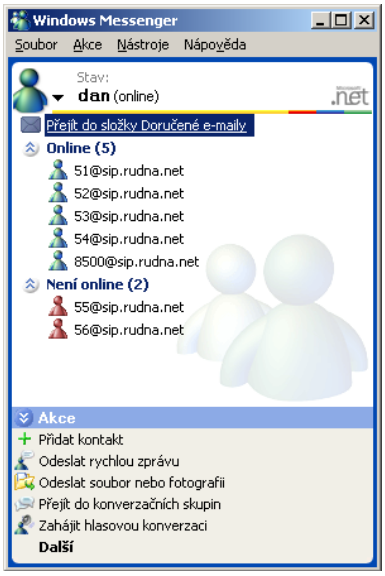
Program je portován nejen na všechny nejrozšířenější operační systémy osobních počítačů (Microsoft Windows, Linux, Mac OS) ale též na systém Pocket PC a dokonce někteří výrobci mobilních telefonů ho chtějí použít ve svých přístrojích.

Nevýhodou tohoto programu je uzavřenost jeho zdrojového kódu a též uzavřenost samotného protokolu, který používá k vlastní komunikaci s klienty a servery. Dalším negativem této aplikace je centrální řízení. Důsledkem toho, při výpadku centrálních serverů dojde k nefunkčnosti celé sítě. Skype od verze 2.x podporuje kromě přenosu hlasu, též přenos obrazu.

Přehled funkcí:

- veškeré funkce běžného telefonu
- videohovory
- konferenční hovory
- správa kontaktů (přidávání/odebírání kontaktů, organizování skupin, import z adresáře, hledání)
- filtr a rychlá volba pro hledání v kontaktech
- zobrazení kontaktů z aplikace Microsoft Outlook
- základní chat
- skupinový chat

5.2 Windows Messenger



MSN Messenger, který je součástí systémů Microsoft Windows, byl původně určený pouze pro textovou komunikaci, později byl vylepšen i o hlasovou a video komunikaci. Pro hlasovou komunikaci podporuje SIP protokol

Přehled funkcí:

- hlasové služby
- správa kontaktů
- posílání souborů
- posílání textových zpráv

5.3 Windows NetMeeting

Jedná se o jednoduchý program, který je součástí systému Microsoft Windows pro volání nejen po Internetu ale také po lokální počítačové síti. Kontakty je možno vyhledávat v lokálním adresáři nebo po zaregistrování v internetovém adresáři, kde jsou uvedeny všichni uživatelé. Program podporuje též video hovory, konference, sdílení plochy, textovou konverzaci a posílání souborů. Není zde podpora volání do klasických telefonních sítí, tudíž je možné volat pouze mezi počítači v lokální síti nebo Internetu.

5.4 X-lite

Neplacený softwarový telefon s mnoha užitečnými funkcemi. K jeho výhodám patří podpora volání přes firewall/proxy. Lze použít na systémech Windows i Linux. I přesto, že je dostupný zdarma, obsahuje mnoho funkcí, např.: 3 linky na volání, přidržení hovoru, zobrazení volajícího a mnoho dalších.

Přehled funkcí:

- tónová volba (DTMF)
- 3 linky pro volání
- podržení hovoru
- redial
- identifikace volajícího
- zobrazení délky hovoru
- vypnutí mikrofonu při hovoru – Mute
- ovládání hlasitosti mikrofonu i reprodukoru
- Push-To-Talk (Pocket PC)
- pamět přijatých čísel
- pamět volaných čísel
- přehledné menu
- adresář
- zkrácené vytáčení

6 Závěr

Přenos hlasu po Internetu a IP telefonie s sebou přináší pro běžné uživatele mnoho výhod, převážně to jsou náklady na samotné telefonování. Nyní můžeme pozorovat poměrně značné nasazení služeb založených na VoIP u komerčních telefonních operátorů i zprostředkovatelů Internetu pro své klienty. Díky dostatečným přenosovým kapacitám mnoho ISP zprostředkovává i hlasové služby, které jsou založeny na VoIP a tím začínají konkurovat tradiční telefonii. Někteří z nich zacházejí ještě dál a pomalu nabízejí i přenos videa a televize. Pro velké firmy a korporace mohou VoIP služby být také ekonomicky zajímavé, vzhledem k možnosti využít stávající datové rozvody a kapacity pro přenos hlasu a hlasové služby v rámci firmy.

Literatura

[1] Rita Pužmanová: *Širokopásmový Internet.* Brno, Computer Press, 2004

[2] Stanislav Puffler: *Skype - internetová telefonie na GNU/Linuxu.* URL: http://www.abclinuxu.cz/clanky/show/64859

[3] Michal Křenek: *VoIP - Telefonování přes internet pro každého* URL: http://www.abclinuxu.cz/clanky/site/voip-telefonovani-pres-internet-pro-kazdeho

[4] Martin Řehůřek: *IP telefonie*

[5] Miroslav Vozňák: *Voice over IP.* URL: http://homel.vsb.cz/~voz29/voip.html

[6] Petr Hrubý: *Protokol SIP (I) - Architektura, typy zpráv a identifikace.* URL: http://www.isdn.cz/clanek.php?cid=4990

[7] Gary Audin: *Základy Voice over IP (VoIP) pro IT techniky*

[8] Jiří Peterka: *Internetová telefonie, IP telefonie, VOIP a konvergence sítí* URL: http://www.earchiv.cz/i_iphone.php3

[9] Jiří Peterka: *Proč Internet dříve nemohl, ale dnes už může?* URL: http://www.earchiv.cz/a98/a805t602.php3

[10] Martin Saidl: *Telefonie v prostředí sítí TCP/IP*

URL: http://saidl.tone.cz/text/html/VoIP/node1.html

[11] Digium - *The Asterisk Telephony Company.* URL: http://www.digium.com

[12] Skype, URL: http://www.skype.com/intl/cs/

[13] Counterpath, URL: http://www.xten.com

[14] Cesnet: *VoIP – přenos hlasu* URL: http://www.cesnet.cz/iptelefonie/voip-principy.hrml

[15] Wikipedie - *Protokoly VoIP.*

URL: http://cs.wikipedia.org/wiki/VoIP#Protokoly_VoIP

[16] Voip Wiki - *a reference guide to all things VOIP.*

URL: http://voip-info.org/wiki/

[17] RFC 791, RFC 2460, RFC 2205