K vytvoření tohoto textu nebylo použito žádného softwarového produktu společnosti MicroSoft. Text byl vysázen v typografickém systému LaTeX 2_ε a na zpracování obrázků byl použit program GIMP. Veškeré programové vybavení bylo provozováno nad operačním systémem LinuX.

Obsah

1 Druhy přenosu **3**
1.1 VoFR . . . 3
1.2 VoATM . . . 4
1.3 VoIP . . . 4

2 Vlastnosti protokolu TCP/IP **4**
2.1 Hardwarové prostředí . . . 5
2.2 IP . . . 6
2.3 TCP . . . 6
2.4 UDP . . . 6
2.5 Služební informace protokolů . . . 7
2.6 Možnosti zajištění QoS v IP síti . . . 7
2.7 Propojování sítí . . . 9

3 Kódování a komprimace hovorového signálů **9**

4 Protokoly pro přenos hlasu v IP síti **10**
4.1 Protokol H.323 . . . 10
4.1.1 Popis protokolu . . . 11
4.1.2 Adresace . . . 13
4.1.3 Spolupráce s tradiční telefonní sítí . . . 13
4.2 Protokol SIP . . . 14
4.2.1 Popis protokolu . . . 14
4.2.2 Adresace . . . 16
4.2.3 Spolupráce s tradiční telefonní sítí . . . 16
4.3 Srovnání protokolů . . . 16

5 Bezpečnost **17**

6 Závěr **18**

7 Seznam zkratek **19**

Úvod

Ve snaze kvalitnějšího využití přenosových tras a integrace technologií datových a telefonních sítí vznikají nové druhy přenosu mluveného slova, než na které jsme zvyklí v tradiční telefonii. K přenosu v takto integrovaných sítích se nevyužívá spojování okruhů (Circuit Switching), ale metoda paketového přenosu dat (Packet Switching) doposud používaná výhradně z datových a počítačových sítích. Tento způsob hlasové komunikace s sebou přináší řadu výhod jako například kvalitnější využití přenosových tras, nebo snížení nákladů na použitou technologii, jak již bylo zmíněno, ale také některé nevýhody, které omezují jakost poskytované služby. V dalším textu budou výhody i nevýhody tohoto druhu přenosu podrobně popsány.

1 Druhy přenosu

Podle typu hostitelké sítě se dnes využívá několik způsobů paketového přenosu hlasu. Jedná se o:

- **VoFR** - Přenos hlasu po prostředcích sítě s přepojováním rámců Frame Relay (Voice Over Frame Relay)
- **VoATM** - Přenos hlasu po prostředcích sítě s přepojováním buněk ATM (Voice Over ATM)
- **VoIP** - Přenos hlasu po prostředcích počítačové sítě postavené na službách protokolů rodiny TCP/IP (Voice Over IP)

1.1 VoFR

VoFR využívá k přenosu hlasu prostředků sítě Frame Relay. Mezi výhody patří poměrně nízké navýšení množství přenášených dat způsobené služebními informacemi přenosového protokolu. Jako hlavní nevýhodu je nutné zmínit poměrně obtížné propojování sítí různých provozovatelů a problémy se spoluprácí zařízení různých výrobců.

1.2 VoATM

VoATM - přenos hlasu po síti ATM. V síti ATM je minimální, respektive shodné jako u ostatních služeb v této síti, navýšení množství dat způsobené služebními informacemi přenosového protokolu, na rozdíl od VoFR a VoIP je však v síti ATM zajištěna jakost služby QoS (Quality Of Service).

1.3 VoIP

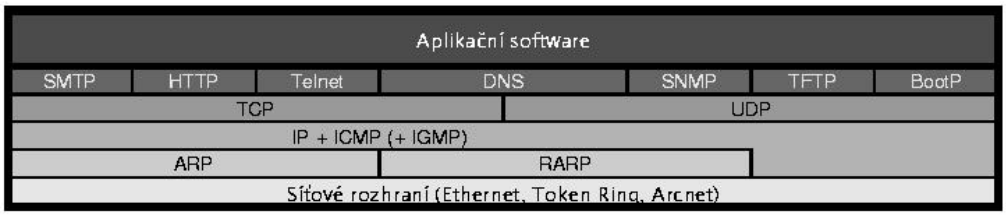
VoIP využívá k přenosu hlasové informace služeb počítačové sítě založené na službách protokolů rodiny TCP/IP. Ze všech zmíněných možností paketového přenosu má tento způsob největší navýšení přenášených informací způsobené služebními informacemi IP protokolu. Je poměrně značný problém v zajištění jakosti služby QoS. Velkou výhodou je ovšem jednoduché propojování sítí různých provozovatelů a poměrně minimální problémy při spolupráci zařízení různých výrobců.

VoIP

Následující text se zabývá možností využití počítačové sítě postavené na službách protokolů rodiny TCP/IP k přenosu hovorového signálu. Přenos hovorových signálů pomocí protokolu TCP/IP otevírá široké možnosti využití prostředí sítě Internet jako společného komunikačního média pro přenos dat z různých zdrojů, včetně telefonie.

2 Vlastnosti protokolu TCP/IP

Protokol TCP/IP je protokolem pocházejícím z dob, kdy přenosové rychlosti byly ve srovnání se současností poměrně nízké a chybovost přenosu 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



Obrázek 1: Vzájemná závislost základních protokolů rodiny TCP/IP

zpožděním, které jsou způsobeny možným přetížením sítě, ztrátou a následným opakováním paketů, odlišnou cestou paketů atd. 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 korespondují s modelem RM-OSI, z čehož vyplývá vysoké množství služebních informací pocházejících z protokolů jednotlivých vrstev. Na druhou stranu vrstvová filosofie zaručuje shodnost implementace protokolů a umožňuje jejich jednoduchý , přehledný a přesný popis. Jednotlivé protokoly z rodiny TCP/IP a jejich vzájemnou spolupráci ukazuje obrázek 1. V další části textu budou zjednodušeně popsány jednotlivé přenosové protokoly IP sítě, tj. IP, TCP UDP s ohledem na využití IP sítě pro přenos hovorových dat. Úplný a přehledný popis protokolů je uveden v [1].

2.1 Hardwarové prostředí

Protokoly rodiny TCP/IP jsou navrženy k zajištění komunikace mezi sítěmi v heterogenním prostředí. Protokoly zajišťují funkce síťové vrstvy a vrstev vyšších a nejsou nikterak vázány na přenosové médium případně na protokoly, které umožňují základní přenos informací po tomto médiu.

Protokoly rodiny TCP/IP je možné provozovat v podstatě na libovolném přenosovém prostředí od sériového spojení s protokolem V.24/V.28, přes telefonní modemy, sítě s protokolem X.21, Frame-Relay, Ethernet, Token-Ring až po současné moderní metody, jakými jsou například přenosové systémy SDH, kde se využívá progresivního způsobu (IP over SDH), který minimali-

4	4	8	16	
Verze	Délka záhlaví	ToS - typ služby	Celková délka paketu	
Identifikace			Návěští	Číslo fragmentu
Životnost		Číslo protokolu	Zabezpečení záhlaví	
Zdrojová IP adresa				
Cílová IP adresa				
Volitelné možnosti				
Data (maximálně 65535 - délka záhlaví bytů)				

Tabulka 1: Formát paketu IP

zuje množství přenášených řídících informací.

2.2 IP

Základním protokolem, tvořícím pilíř sítě, je protokol IP (Internet Protocol). Jedná se o protokol síťové vrstvy, na této vrstvě definuje datovou jednotku datagram. Na základě informací obsažených v záhlavích datagramů, které ukazuje tabulka, poskytuje síťová vrstva službu bez spojení. Každý datagram je samostatná jednotka a musí proto obsahovat všechny potřebné údaje pro jeho přesnou identifikaci. Formát záhlaví je zobrazen v tabulce 1.

2.3 TCP

Tento protokol realizuje přenos se spojením. Poskytuje službu virtuálního okruhu pro spolehlivý přenos dat mezi koncovými účastníky. TCP realizuje funkce jako navázání a rušení relace, segmentace dat, číslování paketů, detekce a oprava chyb atd. Formát záhlaví je zobrazen v tabulce 2.

2.4 UDP

Poskytuje transportní službu bez spojení. Je určena pro aplikace, které nepotřebují zabezpečení v takovém rozsahu, jako nabízí protokol TCP. Pakety UDP se dále nefragmentují, proto platí jednoznačné mapování do datagramu IP. Protokol UDP jen doplňuje informace přenášené již v datagramu IP tak,

16		**16**	
Zdrojový port		Cílový port	
Pořadové číslo			
Číslo potvrzení			
Délka záhlaví	Rezervováno	Funkce řízení	Šířka okna
Kontrolní součet		Označení urgentních dat	
Volitelné možnosti			
Data			

Tabulka 2: Formát paketu TCP

16	**16**
Zdrojový port	Cílový port
Délka	Kontrolní součet
Data	

Tabulka 3: Formát paketu UDP

aby mohl nabízet služby na vrstvě shodné s protokolem TCP. Záhlaví paketu UDP je uvedeno v tabulce 3.

2.5 Služební informace protokolů

Z uvedených tabulek obsahujících formáty záhlaví protokolů jednotlivých vrstev sítě TCP/IP je zřejmé, že užitečná informace bude doplněna o značné množství dat pocházejících ze záhlaví jednotlivých vrstvových protokolů. Vezmeme-li dále v úvahu, že při přenosu hovorového signálu se používá paketů o délce mezi 32 a 64 bytů, je zřejmé, že poměr celkového množství přenesených dat k užitečné informaci je značně nízký. S tímto je třeba uvažovat při návrhu technologického řešení systémů pro přenos hovorových dat.

2.6 Možnosti zajištění QoS v IP síti

Síťový protokol IP verze 4[1], nebyl stavěn tak, aby zajišťoval jakost služby. Protokol IP nabízí několik typů služeb (ToS - viz tabulka 1.), které jsou spe-

[1]Síťový protokol verze 4 s označením IPV4 je v současnosti standardem pro počítačové sítě založené na TCP/IP protokolech

cifikovány volitelně přímo v záhlaví datagramu. Podle tohoto pole v záhlaví se může řídit zpracování ve směrovačích. Této možnosti se však prakticky nevyužívá.

Řešení podpory QoS se dá rozdělit na dvě základní skupiny.

- **Struktura sítě** hraje důležitou roli v celkové jakosti služby IP sítě. Zvýšení jakosti služby je možné docílit například oddělením běžného provozu od VoIP, nebo posílením kapacity páteřních spojů.
- **Softwarové metody řízení toku použité ve směrovačích** jsou elegantnějsím přístupem ke zvětšení jakosti služby, avšak je nutné si uvědomit, že zvolenou metodu musí podporovat všechny směrovače, popřípadě i jiné síťové prvky.

V praxi se většinou oba uvedené přístupy vhodně kombinují a tím se dosahuje optimální QoS a zároveň ceny celého technologického zařízení.

Druhou skupinu opatření můžeme dále rozdělit do následujících tří podskupin

- **Prioritizace** - pakety nesou informaci o důležitosti a ve směrovačích jsou podle tohoto údaje tříděny a posílány v pořadí odpovídajícím důležitosti paketu.
  - **RSVP** - protokol sloužící k rezervaci potřebné šíře pásma pro konkrétní spojení dvou koncových bodů sítě. Popis protokolu je možno nalézt v [2] případně [1]
  - **Diff Serv** - nové doporučení IETF (Internet Engineering Task Force) definující tvz. diferencované služby, které slouží k rozdělení služeb podle jejich nároků na síť. Popis protokolu je opět popsán v [2] a [1], přesný popis protokolu je uveden v [7]
- **Segmentace** - pakety s vyšší důležitostí se segmentují do menších paketů o délkách mezi 23 až 64 bytů. Takto vzniklé pakety jsou odolnější při průchodu sítí proti ztrátě a sítí jsou přenášeny rychleji.

- **Vyrovnání toku paketů** - tato metoda se uplatňuje v koncových zařízeních pro přenos hovorového signálu. Používá se pro zajištění kontinuity přenosu a spočívá ve vyrovnání přenosového zpoždění pomocí zpožďovacích pamětí (buffer). Tento způsob zlepšení kvality je přímo součástí doporučení H.323.

Výše popsanými způsoby je možné zlepšit jakost služby pouze v síti jednoho provozovatele maximálně v několika málo sítích spolu sousedících. V současné době neexistuje metoda, kterou by bylo možné zajistit požadovanou jakost služby v celé síti Internet. Do budoucna jediné možné řešení tohoto problému je zavedení nové verze protokolu IP - IPV6. Ve verzi 6 IP protokolu je již řešení jakosti služby obsazeno v definici protokolu.

2.7 Propojování sítí

Propojování sítí různých provozovatelů je na úrovni protokolu IP přesně definováno. V současné době je téměř jediným standardem pro vzájemné propojování sítí směrovací protokol BGP4 viz. [4]. Vzájemná spolupráce sítí je jednoduchá[2] a spolehlivá, je proto také jednou z hlavních výhod technologie VoIP.

3 Kódování a komprimace hovorového signálů

Při přenosu hlasu pomocí protokolu IP se často využívá komprimace přenášených dat. Použitím DSP (Digital Signal Processing) je více či méně (podle použité metody) sníženo množství přenášených dat při minimální, nebo dokonce žádné ztrátě kvality přenosu (kvalita přenosu je opět závislá na použité metodě). Komprimace přenášených dat se provádí v kodecích, které jsou součástí koncového zařízení nebo brány[3] na rozhraní sítě.

[2]Slovo *„jednoduchá"* zde neznamená, ze konfigurace a provozování BGP by mohlo být v rukou začátečníků, či nezkušených techniků. Naopak problematika směrovacího protokolu BGP je jednou z nejobtížnějších věcí v prostředí sítí TCP/IP. Protokol je však jasně definován a výrobci přesně dodržován.

[3]Pojem *„brána"* bude vysvětlen v dalším textu.

Kodek	Přenosová rychlost (kb/s)	Způsob kódování
G.711	56/64	PCM (A-law, μ-law
G.722	48/56/64	ADPCM
G.726 - DECT	16/24/32/64	ADPCM
G.728	16	CELP
G.729	8/13	ACELP
G.723	5.3/6.3	ACELP
FR-GSM	13	RPE-LTP
HR-GSM	5.6	CELP
EFR-GSM	12.2	ACELP
EFR-IS 136	7.95	ACELP
FR-PDC	6.9	VSELP
HR-PDC	3.45	PSI-CELP
FR-IS 54	8	VSELP

Tabulka 4: Srovnání komprimačních metod

V tabulce 4, je uveden přehled komprimačních metod využívaných v doporučeních pro IP telefonii. Podrobný popis jednotlivých metod nalezne čtenář v jednotlivých doporučeních ITU-T.

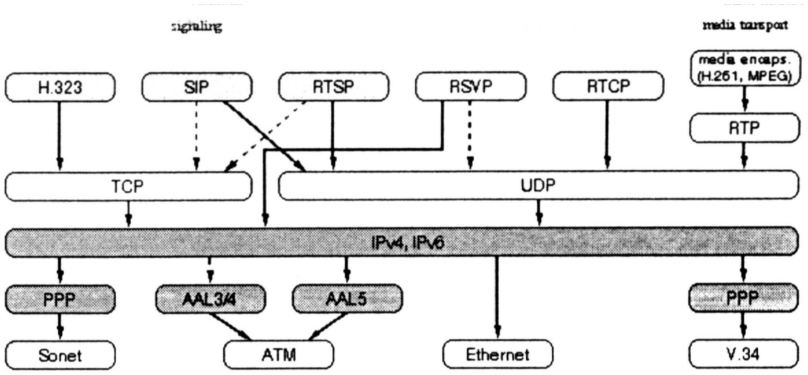
4 Protokoly pro přenos hlasu v IP síti

V současné době existují pro prostředí počítačových sítí založených na protokolu IP, tedy i pro Internet, dva diametrálně odlišné standardy pro přenos hlasového signálu sítí. Starší z nich a v současné době rozšířený standard H.323 pocházející od ITU-T a SIP poměrně nový, perspektivní standard od IETF. V následujícím textu budou stručně popsány oba protokoly s důrazem na odlišnosti a výhody či nevýhody obou protokolů.

Na obrázku 2 je znázorněna vazba protokolů sloužících k zprostředkování přenosu hlasových dat na protokoly rodiny TCP/IP.

4.1 Protokol H.323

H.323 je doporučení definující protokol pro přenos hovorových signálů IP sítí vzniklé na půdě ITU-T. Jedná se o komplexní protokol, který poskytuje



Obrázek 2: Vazby protokolů pro přenos hlasových dat na přenosové protokoly rodiny TCP/IP

všechny služby nutné pro přenos hovorového signálu. Tento protokol se stal prvním mezinárodně standardizovaným protokolem pro přenos hovorových signálů po IP sítích. Protokol H.323 je binárně orientovaným protokolem. Na diagnostiku spojení je proto nutné použití speciálních a to jak softwarových, tak hardwarových prostředků.

4.1.1 Popis protokolu

Protokol H.323 využívá pro přenos informací služeb protokolu TCP, jak ukazuje obrázek 2. To zajišťuje spolehlivý přenos mezi jednotlivými účastníky spojení[4]. 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 odprostit od tohoto modelu a celý systém

[4]Účastníky spojení jsou zde myšleny dva koncové body spojení H.323, to nemusí nutně znamenat totožnost s koncovými účastníky telefonní relace.

decentralizovat a tím zvýšit jeho odolnost proti proti možným poruchám. Na druhou stranu existence těchto center přináší řadu výhod, které umožňují například možnost adresace z využitím telefonních čísel[5], 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[6] (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.

[5] V telefonní síti zcela běžný způsob identifikace koncového účastníka využívaný již téměř sto let.

[6] Termín *„řadič spojení"* je převzat z [2] a autorovi se zdál býti výstižnější než například *„strážce brány"*

Přesná a úplná definice jednotlivých pojmů je součást 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 ne jen telefonní číslo volaného účastníka, ale i IP adresu cíle. V případě, že 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 (většinou podle finančních nákladů) bránu, 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.

4.1.2 Adresace

K adresaci účastníků v síti H.323 se používá běžných telefonních čísel, jako v tradiční telefonní síti dle doporučení ITU-T E.164. Přepočet na IP adresy provádí, pro menší sítě, sám koncový účastník (přesněji jeho koncové zařízení), nebo u sítí složitějších gatekeeper.

4.1.3 Spolupráce s tradiční telefonní sítí

Spolupráce s tradiční telefonní sítí není v případě H.323 téměř žádný problém. Při dodržení doporučení E.164 pro mezinárodní číslovací plán ISDN je

možné dosáhnout stavu, kdy koncoví účastníci nepoznají rozdíl mezi spojením v síti H.323 a v klasické telefonní síti[7].

4.2 Protokol SIP

Alternativní protokol pro přenos hovorových signálů k protokolu H.323 navržený odborníky z IETF.

4.2.1 Popis protokolu

Přístup k řešení problému tj. k přenosu hovorových signálů IP sítí je diametrálně odlišný od přístupu který je použit u protokolu H.323. Zatím, co ITU-T vyřešilo problém jedním protokolem poskytující veškeré potřebné služby pro realizaci přenosu hovorového signálu, IETF zvolilo cestu, běžnou z prostředí sítě Internet, kterou je vytvoření řady protokolů realizující pouze konkrétní část služeb nutných pro přenos hovorových dat, jako například signalizaci, či přenos multimediálních informací. To umožňuje v případě potřeby výměnu pouze jednoho elementárního protokolu a tím snadnou úpravu celého systému.

Protokol SIP vychází z osvědčených a praxí ověřených protokolů jako HTTP (Hyper Text Transfer Protocol), či SMTP (Simle Mail Transfer Protocol). Protokol je znakově orientovaný. To umožňuje použití (v IP síti) běžných technických prostředků pro diagnostiku přenosu, jako například softwarový nástroj tcpdump, známý z prostředí operačního systému Unix, k monitorování druhu a obsahu přenášených paketů. Není proto nutný nákup speciálního programového vybavení, případně zařízení pro diagnostiku provozu.

Na rozdíl od protokolu H.323 je použita strategie maximální decentralizace řízení, protokol nedefinuje žádná centrální místa v síti, komunikace probíhá výlučně mezi koncovými body. Tento přístup podstatně zvyšuje odolnost celého systému vystavěného na službách protokolu SIP jak proti výpadkům některých jeho částí, tak proti výpadkům IP sítě. Na druhou stranu je velký problém se sběrem údajů nutných pro zpoplatňování hovorů. Není téměř

[7] Myšleno tím rozdíl v průběhu sestavování spojení. V průběhu sestaveného spojení bude vždy patrný rozdíl v kvalitě přenášeného signálu.

možné využít systém zpoplatňování telekomunikačních služeb známý z prostředí tradičních telefonních sítí. Zpoplatňování telefonních hovorů je nutné převádět na platby za množství přenesených dat do okolních sítí, či paušální poplatky.

V doporučení IETF pro protokol SIP jsou definovány čtyři základní prvky sítě:

- **Uživatelský agent (User Agent)** - Uživatelská aplikace, umožňující koncovým účastníkům sítě obousměrnou komunikaci pomocí protokolu SIP. User Agent (UA) je dále rozdělen na dvě části:
  - **UA Client** - klientská část uživatelského agenta sloužící k sestavování a řízení odchozích relací
  - **UA Server** - serverová část uživatelského agenta sloužící k přijetí a řízení příchozích relací
- **SIP Proxy Server** - provádí funkce jako: hledání účastníka v koncové síti, směrování hovorů (spolupráce s Firewallem či NATem), zprostředkování styku s jinou sítí.
- **SIP Redirect Server** - směruje volání jiným serverům v síti.
- **SIP Registrar** - slouží k registraci koncových uživatelů (obdoba HLR u GSM)

Přesná definice pojmů je součástí patřičných doporučení RFC od IETF.

Při sestavování spojení se vždy využívá doménové jméno stroje v síti IP. V prvním kroku se provede hledání IP adresy koncového účastníka případně SIP serveru pomocí DNS (Domain Name Service). Dalším kroku se sestaví spojení s koncovým účastníkem, případně se využije služeb nějakého SIP serveru, není-li možné sestavit spojení přímo (například když je účastník umístěný za Firewallem či NATem, nebo je mobilní). Směruje-li se spojení mimo síť SIP protokolu, musí volající účastník vždy sám rozhodnout, kterou bránu pro spojení použije a znát její doménovou, případně IP adresu.

4.2.2 Adresace

K adresaci koncových účastníků v síti se využívá formátu zápisu shodného pro zápis e-mailových adres. Směrování v IP síti se pak provádí na základě IP adresy, která se určí využitím služby DNS.

4.2.3 Spolupráce s tradiční telefonní sítí

Spolupráce sítě, která využívá služeb protokolu SIP s běžnou telefonní síti je velice obtížné. Při odchozím spojení z IP sítě směrem k tradiční telefonní je možné využití odchozí brány[8]. Určení volaného se provede zápisem SIP adresy ve tvaru například: +420224531111@sipgw.praha.supertel.cz. Přesný formát, ve kterém bude uváděno před „zavináčem" není standardizován a je čistě v rukou provozovatele sítě. Telefonní číslo v uvedeném příkladu by proto mohlo být také ve tvaru 24351111, nebo 224351111 či 022435111 atd.

Spojení v opačném směru tj. ze sítě telefonní do sítě IP s protokolem SIP není možné jednoduše realizovat. Tuto velkou nevýhodu, která je způsobená použitým způsobem adresace, je možné částečně odstranit zavedením přepočtů na některém SIP proxy severu.

4.3 Srovnání protokolů

Při srovnání popsaných protokolů nutno konstatovat, že nelze jednoznačně prohlásit, který protokol je ten vhodný[9].

Protokol H.323 má nesporné výhody, které umožňují jednoduchou spolupráci s tradiční telefonní sítí, nabízí služby nutné pro zpoplatňování provozu a v současné době je již běžně implementován v síťových prvcích (například od firmy Cisco). Na druhou stranu se jedná o protokol, který se bude jen těžko dále vyvíjet, neboť je velice komplexní a úpravy by zcela určitě způsobovaly zpětné nekompatibility. Další nevýhodou je jeho binární orientace, která s sebou přináší řadu problémů při monitorování a měření provozu.

[8] Známe-li adresu brány pro oblast, kam se chceme dovolat. V opačném případě se nám volání sestavit nezdaří.

[9] Toto je názor autora, který vyplývá ze studia vlastností obou protokolů a praktických zkušeností se skutečným provozem.

Protokol SIP je jednoduchý, flexibilní a snadno implementovatelný protokol. Další jeho vývoj není problém, lze proto v brzké době očekávat řadu dalších vylepšení. Jeho implementace se začíná pomalu objevovat v nových verzích operačních systému pro síťové prvky (například je již součástí nových IOSů k zařízení firmy Cisco). Nutno však ukázat na dvě hlavní nevýhody:

1. Velice problematická spolupráce s tradiční telefonní sítí. Některé služby nelze dokonce obousměrně realizovat.

2. Problémy se sběrem tarifních informací, běžný model zpoplatňování služeb nelze na síť s protokolem SIP nasadit a je nutné hledat další metody, jak vhodně zajistit ocenění nabízených služeb.

Vážnou nevýhodou obou protokolů je poměrně složitá spolupráce s hraničními prvky privátních sítí, jako je FireWall a NAT. Jelikož je IP adresa jednotlivých konců spojení součástí obsahu paketu a ne jen jeho záhlaví není možné uskutečnit spojení přes výše uvedené prvky bez jejich úpravy, či bez pomocného proxy serveru. To může být značnou překážkou při nasazování uvedených protokolů do běžného provozu, kdy z důvodu nedostatku IP adres využívá většina podnikových sítí privátních rozsahů. Tento problém vyřeší nasazení protokolu IPV6[10].

5 Bezpečnost

Oba zmíněné protokoly hledisko síťové bezpečnosti téměř opomíjejí. Součástí protokolů není prostředek, který by zaručil jedinečnost koncového bodu v oblasti IP sítě. To může v praktickém provozu znamenat, že při útoku na systém může útočník zaměnit například bránu aniž by si toho účastník všiml. Presentovat se síti jako jiný účastník a využívat pak jeho telefonní číslo a volat na jeho účet není také nepřekonatelným problémem. Postačí pouze znalost hesla.

[10] Stále avizované nasazení protokolu IPV6 však není otázkou blízké budoucnosti, jak by se mohlo na první pohled zdát.

Je-li kladen důraz na vyšší síťovou bezpečnost je ji nutné řešit pomocí externích prostředků[11].

6 Závěr

Myšlenka přenosu hlasových dat pomocí běžné IP sítě je jistě velice zajímavá a přitažlivá. V současné době[12] však přináší nasazení VoIP do běžného provozu více problémů, než očekávaných výhod. Dojde-li k nasazení nové verze IP protokolu IPV6 do prostředí sítí propojených v síti Internet, k zajištění dostatečné síře pásma nejen u páteřních spojů, ale i u spojů ke koncovým uživatelům. Dojde-li dotažení standardizace protokolů tak, aby byla možná spolupráce se službami jak telefonní sítě, tak se službami sítě IP, stane se jistě tato progresivní forma přenosu hovorových dat vážnou konkurencí pro tradiční telefonii. Přinese nové možnosti přenosu nejen hovorových dat, ale i obrazu, videa a jejich možných kombinací.

[11] Ani toto řešení však není nikterak definováno, autor zatím nenašel kvalitní a funkční řešení tohoto problému.

[12] IP síť stojí na protokolech rodiny IPV4, není zajištěná potřebná šířka pásma, nelze zaručit jakost služby atd.

7 Seznam zkratek

ATM Asynchronous Transfer Mode

DNS Domain Name Service

GSM Global System for Mobile Communication

IETF Mezinárodní organizace definující pravidla sítě Internet (Internet Engineering Task Force)

HTTP Protokol pro přenos hypertextových informací (Hyper Text Transfer Protocol)

IP Internet Protocol

ITU Mezinárodní standardizační organizace (International Telecominication Union)

FR Datová síť s přepojováním rámců (Frame Relay)

PCM Pulsně-kódová modulace (Pulse Code Modulation)

QoS Jakost služby (Quality Of Service)

RM-OSI Sedmi vrstvový referenční model otevřeného síťového systému (Reference Model Open System Interconect)

RTCP Protokol umožnující zpětnou vazbu při použití RTP (Real-time Transfer Complimentary Protocol)

RTP Protokol pro přenos multimediálních informací v reálném čase podle ITU-T a převzat IETF (Real-time Transfer Protocol)

SIP Protokol pro přenos signalizace podle IETF (Session Initialization Protocol)

SMTP Protokol pro přenos elektronické pošty v IP sítích (Simple Mail Transfer Protocol)

TCP Tranfer Communication Protocol

ToS Typ služby (Type Of Service)

UDP User Datagram Protocol

VoATM Přenos hovorových dat po síti (Voice Over ATM)

VoFR Přenos hovorových dat po síti Frame Relay (Voice Over Frame Relay)

VoIP Přenos hovorových dat pomocí sítě s protokolem IP (Voice Over Internet Protocol)

Reference

[1] Rita Pužmanová, Pavel Šmrha: Propojování sítí s TCP/IP, Koop, České Budějovice, 1999

[2] Martin Tomek: Diplomová práce - Internet protokol telefonie, K332, Fel - ČVUT, Praha, 2000

[3] Jiří Kuthan, GMD Fokus: SIP Telephony, CVUT/CS Prague, Nov 6th, 2000

[4] Pavel Šmrha, Vladimír Rudolf: Internetworging pomocí TCP/IP, Koop, České Budějovice, 1995

[5] RFC2543

[6] RFC1889

[7] RFC2474

[8] http://www.openh323.org

[9] http://www.linuxtelephony.org

[10] http://www.cisco.com