Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Bakalářská práce

2009 **Jindřich Křivohlávek**

Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Hlasová komunikace VoIP v hybridní internetové síti

Jindřich Křivohlávek

Bakalářská práce
2009

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Katedra informačních technologií
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Jindřich KŘIVOHLÁVEK**

Studijní program: **B2646 Informační technologie**

Studijní obor: **Informační technologie**

Název tématu: **Hlasové služby VoIP v hybridní internetové síti**

Zásady pro vypracování:

Komunikační sítě se v posledních desetiletích digitalizují, zároveň je znatelný sklon k využívání stejné infrastruktury a tím šetřit náklady a otvírat nové možnosti využití těchto sítí. Tento trend je označován jako konsolidace sítí. Jednou větví, která je v souvislosti s konsolidací zaznamenávána laickou veřejností je sdružování telefonních a datových sítí, který je symbolizován hlavně technologií VoIP (voice over Internet Protokol). V posledních letech je v oblasti počítačových sítí vyvíjen stále větší tlak na nasazování protokolu IPv6. Proto je vhodné vytvořit studii o stupni podpory VoIP v rámci hybridních IP sítí, které se pomalu stávají každodenní realitou. * v teoretické části práce student popíše proces digitalizace zvuku, různé přístupy k řízení v sítích VoIP a základní komunikační protokoly. * v praktické části práce bude provedena studie základní použitelnosti VoIP v hybridních sítích s protokoly IPv4 a IPv6.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

http://www.voip-info.org

Satrapa, Pavel: Internetový protokol IPv6,CZ.NIC, Praha, 2008, ISBN 978-80-904248-0-7

Vedoucí bakalářské práce: **Ing. Tomáš Fidler**
Katedra softwarových technologií

Datum zadání bakalářské práce: **15. ledna 2009**

Termín odevzdání bakalářské práce: **15. května 2009**

L.S.

doc. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Cegan
vedoucí katedry

V Pardubicích dne 31. března 2009

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 7. 8. 2009

Jindřich Křivohlávek

PODĚKOVÁNÍ

Tímto bych chtěl poděkovat vedoucímu práce Ing. Tomáši Fidlerovi za cenné rady a připomínky, které mi poskytl během vypracování mé bakalářské práce.

SOUHRN

Tématem této práce je hlasová komunikace VoIP v hybridní síti. Zkoumán je především SIP protokol v IPv4 a IPv6 síti. Práce obsahuje základní popis těchto protokolů včetně úvodu do oblasti telefonie a digitalizace zvuku.
Výsledkem práce jsou měření a vyhodnocení použitelnosti VoIP v současných a budoucích podmínkách. Součástí práce je i přiložené bootovatelné médium s operačním systémem, testovacími nástroji, VoIP softwarem (ústředna + klient) a návody na jejich použití.

KLÍČOVÁ SLOVA

IP, IPv6, IPv4, SIP, VoIP, telefonie

TITLE

VoIP voice communication in a hybrid Internet network

ANNOTATION

The topic of this work is the voice communications VoIP in the hybrid network. Studied is the SIP protocol in the IPv4 and IPv6 network. This work contains the basic description of these protocols, including the introduction to the field of telephony and the digitization of sound.
This work includes the measurement and evaluation of VoIP application in current and future conditions. Part of the work is attached bootable media operating system, testing tools, VoIP software (switchboard + client) and instructions for their use.

KEYWORDS

IP, IPv6, IPv4, SIP, VoIP, telephony

SEZNAM ZKRATEK

- **ATM (Asynchronous Transfer Mode)** – standard pro vysokorychlostní síťovou architekturu
- **B2BUA (Back To Back User Agent)** – zařízení obsahující více UA
- **DNS (Domain Name Server)** – hierarchický systém doménových jmen
- **DoS (Denial-of-service)** – způsob útoku na internetové služby
- **FR (Frame Relay)** – technologie přepínání paketů
- **HTML (HyperText Markup Language)** – značkovací jazyk pro vytváření hypertextových dokumentů
- **HTTP (HyperText Transfer Protocol)** – internetový protokol pro výměnu HTML dokumentů
- **HTTPS (HTTP Secure)** – zabezpečený HTTP
- **IP (Internet Protocol)** – protokol pro přenos dat v síti Internet
- **IPv4 (Internet Protocol version 4)** – Internet Protocol ve verzi 4
- **IPv6 (Internet Protocol version 6)** – Internet Protocol ve verzi 6
- **Kbps (Kilobit per second)** – kilobit za sekundu
- **MGCP (Media Gateway Control Protocol)** – protokol pro ovládání zařízení Media Gateway
- **NAT (Network Address Translation)** – překlad síťových adres
- **PSTN (Public Switched Telephone Network)** – veřejná telefonní síť
- **QoS (Quality of Service)** – termín zabývající se kvalitou služeb
- **RSVP (Resource ReSerVation Protocol)** – protokol k rezervaci síťových prostředků
- **SIP (Session Initiation Protocol)** – protokol pro signalizaci ve VoIP
- **SIPS (SIP Secure)** – zabezpečená verze SIP protokolu
- **SMTP (Simple Mail Transfer Protocol)** – protokol pro odesílání elektronické pošty
- **UA (User Agent)** – označení koncového zařízení ve VoIP
- **UAC (User Agent Client)** – UA odesílající požadavky
- **UAS (User Agent Server)** – UA odpovídající na požadavky
- **URI (Uniform Resource Identifikator)** – unikátní identifikátor zařízení
- **VoATM (Voice over Asynchronous Transfer Mode)** – přenos hlasu v sítí ATM
- **VoFR (Voice over Frame Relay)** – přenos hlasu v sítí FR
- **VoIP (Voice over Internet Protocol)** – přenos hlasu v síti IP
- **VoP (Voice over Packet)** – přenos hlasu paketovou technologií

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

1 Úvod

Cílem bakalářské práce je seznámení čtenářů s problematikou hlasové komunikace v rámci datových sítí používaných v současné době i blízké budoucnosti.

Po úvodní kapitole následuje druhá kapitola, která je určena pro seznámení čtenáře se základními pojmy a principy hlasové komunikace. Převážný obsah je tvořen samotným vývojem a principem hlasové komunikace.

Třetí kapitola obsahuje rozbor jednotlivých druhů telefonií v podrobnějším měřítku. Zde jsou vysvětleny pojmy jako analogová, digitální, bezdrátová, VoP či VoIP telefonie.

Čtvrtá kapitola je věnována digitálnímu přenosu, u kterého nesmí chybět samotný rozbor digitalizace.

Pátá kapitola obsahuje základní informace o protokolu IP, jenž je hlavní stavební jednotkou celosvětové sítě Internet. Čtenář zde nalezne základní pojmy a vývoj samotného protokolu.

Šestá kapitola je věnována přenosu hlasu po datových sítích. Pro přenos dat se nepoužívá pouze jedné technologie, proto jsou zde nastíněny ty nejčastěji používané. Nejrozšířenější je u koncových uživatelů protokol IP, tudíž celá práce bude zaměřena zejména na VoIP.

I přes tento výběr je oblast příliš rozsáhlá, práce je úzce zaměřena na použití signalizačního protokolu SIP. Ten totiž patří mezi nejoblíbenější jak mezi vývojáři, tak i v řadách uživatelů je velmi oblíbený. SIP protokolu je věnována kapitola sedmá.

V osmé kapitole jsou zahrnuty výsledky z měření a testování provozu SIP protokolu v hybridní síti. Kromě grafů jsou zde popsány i případné problémy v podpoře obou IP protokolů.

Devátá kapitola je věnována problémům, které se mohou v hybridních sítích objevit. Nastíněna jsou i některá možná řešení.

Desátou kapitolu tvoří závěr, kde je shrnut aktuální stav pro VoIP komunikaci pomocí SIP protokolu v hybridních sítích.

2 SEZNÁMENÍ S HLASOVOU KOMUNIKACÍ

Komunikace neboli dorozumívání je proces, při němž dochází k výměně informací mezi živými organismy. Samotná výměna probíhá pomocí různých signálů, mezi které můžeme zařadit například zvukové, obrazové apod. Pro přenos signálů je zapotřebí příslušné přenosové médium, ve kterém jsou signály šířeny od vysílače (odesílatele) k přijímači (příjemci). Pro bezproblémový průběh komunikace je nutné zajistit srozumitelné odeslání informace pomocí přenosového média a samotné porozumění příjemcem. To je zajištěno pomocí předem stanovených pravidel. Po příjmu informace může následovat její zpracování či předání dále.

Mezi lidmi je nejčastějším způsobem dorozumívání hlasové. Tento způsob je použitelný jak na velmi krátké vzdálenosti, tak i na vzdálenost v desítkách metrů. Někteří živočichové mohou pomocí zvukových vln komunikovat i v řádech kilometrů. Člověk tedy využil své inteligence k překonání tohoto limitu a za pomocí techniky je schopen předávat informace na vzdálenosti v řádech desítek tisíc kilometrů. Tento proces se pak nazývá telefonií, což je součást nadřazeného oboru telekomunikace. Telekomunikace zahrnuje kromě telefonie i telegrafii, což je přenos textových informací.

V současné době je stále populárnějším trendem kromě přenosu samotného zvuku i přenos obrazu, tedy videotelefonie. Rozšíření hlasové komunikace, založené na paketové technologii, o obrazové informace ve většině případů není problémem. Některé protokoly (například popisovaný SIP) jsou na to již připraveny. Proto nalezne tato práce částečné využití i v případě videotelefonie.

3 DRUHY TELEFONIÍ

Hlavní rozdělení telefonie je určeno podle způsobu, jakým je zvuková informace přenášena a zpracována. Přestože uvádím jako první způsob analogový přenos po metalickém vedení, principy samotné telefonie sahají ještě dále do minulosti. Příkladem takového předchůdce analogového aparátu může být trubkový telefon, jehož princip objevil čínský vynálezce Kung-Foo-Whing v roce 968 [11]. Komunikace u předchůdců dnešních analogových telefonů nebyla možná na velké vzdálenosti, proto se jimi nebudu nadále věnovat a přejdu tedy k prvnímu způsobu, který dokázal přenést hlas na větší vzdálenost.

3.1 ANALOGOVÝ PŘENOS

Při analogovém přenosu dochází k převodu zvukové informace na elektrický signál se spojitým průběhem. Tento signál pak může být šířen pomocí metalického vedení na větší vzdálenosti, které lze navyšovat pomocí zesilovacích členů.

Převod zvuku na elektrický signál je možný pomocí elektromagnetického mikrofonu, jehož princip je následující:

Zvuková vlna rozkmitá membránu s permanentním magnetem v cívce, při čemž je tento pohyb převáděn na elektrický proud. Princip reproduktoru je přesně opačný, k membráně je připevněna cívka, která je v magnetickém poli. Při průchodu elektrického proudu cívkou vznikne pohyb, který je membránou reprezentován v podobě zvuku.

Alexander Graham Bell byl dlouhou dobu považován za prvního objevitele telefonu, svůj první telefon vyrobil v roce 1876. V roce 2002 byl však uznán prvním vynálezcem telefonu Antonio Meucci jehož přístroj byl sestrojen již v roce 1849 [11].

Rozvoj analogové telefonie byl zpočátku velmi pomalý především kvůli vysokým nákladům na výstavbu infrastruktury. Dva komunikující body museli být totiž spojeny metalickým vedením s vhodnými parametry. S postupujícím časem se stávala analogová telefonie stále rozšířenější, protože umožnila rychlé předání informace na

větší vzdálenosti. První telefony se tak objevovaly ve větších či vládních institucích, mezi něž patří například poštovní úřady.

Analogový přenos má své nevýhody, díky kterým v současné době upadá do zapomnění. Hlavní nevýhodou je velká náchylnost na rušení, přeslechy a útlum. Kvalita reprodukce nemůže být zajištěna ve stejné podobě jako při vysílání. Další podstatnou nevýhodou je vyhrazení celého přenosového kanálu jedním hovorem. Jeden komunikační kanál tak může přenášet v daném okamžiku pouze jeden hovor. Naopak výhodou analogových zařízení jsou nižší náklady na výrobu a jednodušší návrh.

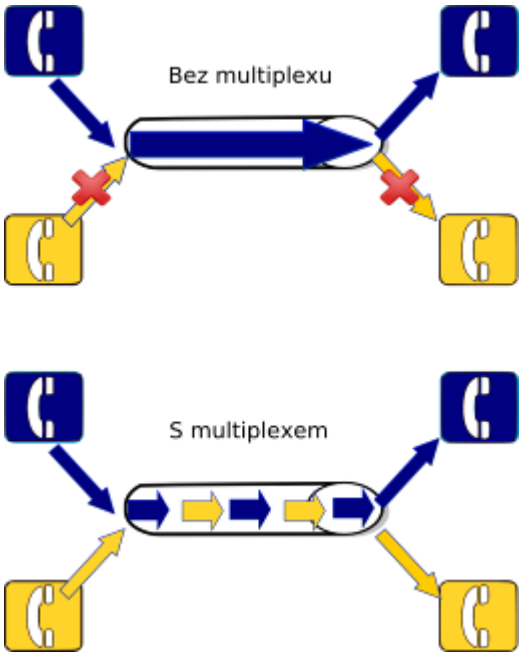
Díky uvedeným nedostatkům je analogová telefonie již několik let na ústupu.

3.2 DIGITÁLNÍ PŘENOS

Digitální přenos je nástupcem předchozího způsobu, jenž využívá k přenosu dat pouze diskrétního signálu. Pro převod je využíváno A/D a D/A převodníků, které zajišťují převod analogového (spojitého) signálu na digitální (diskrétní) a naopak. Samotnému způsobu digitalizaci zvuku je věnována samostatná kapitola níže.

Digitalizace v tomto odvětví odstranila nevýhody analogového formátu, snižuje tedy náchylnost na rušení, útlum a přeslechy. To je dáno nejen samotnými vlastnostmi digitálního vysílání, ale i přítomností samoopravných kódů apod. Digitální ústředny přináší možnost přepínání (multiplex) kanálů, po jednom vedení tak může probíhat více telefonních hovorů.

Nejčastěji je využíván časový multiplex (Time Division Multiplex – TDM). Tento způsob přepínání rozdělí jednotlivé hovory na velmi krátké části, které se v pravidelných intervalech střídají. Na druhé straně multiplexu jsou tyto části opět pospojovány do souvislého hovoru, který je odesílán ke koncovému zařízení.



OBRÁZEK 1 - VÝHODY MULTIPLEXU

3.2.1 BEZDRÁTOVÝ PŘENOS

Ačkoliv už byly základní problémy analogového přenosu vyřešeny, stále byla nutná instalace nákladné infrastruktury. Navíc metalické vedení nelze použít ve všech případech, problém nastává u vedení kabeláže poblíž napěťového vedení (velké rušení) či u historických budov (nemožnost vedení kvůli zásahu do budovy).

Pro tento problém bylo řešení v podobě bezdrátového přenosu. Mezi nejčastěji používanou technologii patří přenos pomocí rádiových vln. Pod pojmem bezdrátový telefon si může čtenář vybavit přenosný telefon, který je bezdrátově spojen se základní stanicí, jež je připojena k metalickému vedení. Dosah tohoto zařízení je ovšem omezen v řádech desítek metrů.

Druhou variantou, kterou si může čtenář vybavit pod pojmem bezdrátový telefon je řešení v podobě bezdrátové buňkové (celulární) sítě, tedy dnešní GSM (UMTS apod.). Zde už je dosah od základny v řádech kilometrů. V případě horšího signálu je možné okamžité přepojení k jiné buňce s lepším příjmem. GSM síť a jí podobné ovšem patří do kategorie následující.

3.2.2 PAKETOVÝ PŘENOS (VOP – VOICE OVER PACKET)

Všechny předchozí technologie vyžadovali po dobu hovoru neměnnou přenosovou cestou. V případě paketového přenosu je hovor rozdělen na malé části (podobně jako u použití multiplexu). Tyto částí jsou nazývány rámce (pakety). Zatímco v předchozích případech byl hovor přenášen po celou dobu jedinou cestou. V případě paketového přenosu může být a také často bývá tras více. Při paketovém přenosu mohou být části hovoru přenášeny paralelně, čímž dochází k lepšímu využití přenosových tras (rozložení zátěže). Ve výše uvedených případech tedy nemuselo docházet k efektivnímu využití přenosové soustavy jako v případě paketových technologií.

Výhodou paketového přenosu je především využití různých cest o různých kvalitách. Zatímco vyhrazené pásmo v předchozích případech zajistilo po celou dobu konstantní kvalitu, v případě paketového přenosu mají data různou trasu, tudíž se může kvalita v průběhu hovoru měnit. Garance kvality se zdá být největším problémem paketového přenosu.

Kvalita probíhajícího hovoru je závislá nejen na přenosové cestě, ale i na použitém protokolu. Jednotlivé pakety mohou být doručovány nespolehlivým protokolem (UDP), kde není kladen požadavek na 100% doručení. V případě, že se v průběhu hovoru ztratí pár paketů, nemusí to účastníci hovoru zaznamenat. Pakliže dochází ke ztrátám větším, hovor může být přerušován.

Existuje možnost zasílání dat spolehlivým způsobem (protokol TCP), který má ovšem větší požadavky na přenosové médium (režie spojená s potvrzováním a opakovaném zasílání dat) i systémové prostředky mezilehlých zařízení (kontrola paketu a případné žádání o opakované zaslání). I přesto, že data nakonec dorazí všechny, může nastat problém v jejich časové platnosti. Jinými slovy paket dorazí příliš pozdě.

Nejčastějším způsobem je přenos pomocí nespolehlivého protokolu UDP, drobné ztráty nejsou díky velmi krátkým úsekům, nedokonalosti sluchového ústrojí a vhodným kodekům postřehnutelné.

S tímto problémem souvisí i často používaný termín Quality of Service (QoS), což lze přeložit jako „kvalita služby“. Pro zajištění QoS jsou používány různé technologie, příkladem může být priorizace určitých služeb. Použít lze i RSVP. Díky různým implementacím QoS je možné vyhradit či zajistit vhodné podmínky pro danou službu. Přenos velkého množství souborů na jednom PC neomezí volání přes Internet na PC druhém. Bohužel potřeba priorizace vznikla až ve chvíli, kdy byla zapotřebí, takže se s ní u zrodu IPv4 protokolu nepočítalo. Implementace v IPv4 tedy není vždy zaručena a záleží pouze na provozovateli datové sítě a použitém HW. IPv6 a některé další protokoly s QoS již počítají.

Z výše uvedených odstavců by se mohlo zdát, že paketový přenos v oblasti telefonie spíše přináší nevýhody a bude tedy na ústupu. Kvalita datových sítí se ovšem neustále zlepšuje, provozovatelé nabízejí stále lepší rychlosti a kvalitu svých linek. Paketový přenos má hlavní výhodu v tom, že může probíhat na datových sítích. Zákazník tak nemusí platit zvlášť za vedení telefonní a datové linky. V případě paketového přenosu stačí pouze datová linka o vhodné kvalitě, díky tomu se sníží nejen náklady spojené s pronájmem dané linky, ale i administrativní (jak z hlediska společných faktur, tak z hlediska správy síťovými správci).

Samozřejmě existují i nevýhody, mezi které lze zařadit závislost na přívodu elektřiny a funkčnosti internetového připojení. Zatímco pevné linky a mobilní telefony počítají s výpadky energie, u poskytovatelů internetu tomu tak být nemusí. Taktéž ve VoP není realizováno nouzové volání. V nouzových situacích mají předchozí technologie stále výhodu.

O možnosti nasazení paketové telefonie mluví následující příklady:

- **Voice over Internet Protocol (VoIP)** – IP patří mezi nejpoužívanější technologie, což je dáno i tím, že jde o základní protokol celosvětové sítě Internet. Oblíbenost VoIP je tedy především v domácnostech a menších podnicích. To je mimo jiné důvod, proč bude této oblasti věnována zbývající část práce. Ve zkratce lze říci, že režie při přenosu hlasu je největší, na druhou stranu díky

velkému množství dostupných kodeků a rychlému vývoji lze telefonovat již na linkách s 28.8 kbps.

- **Voice over Frame Relay (VoFR)** – Frame Relay sítě jsou používány v podnikovém sektoru. Mezi hlavní výhody patří nízká režie ve srovnání s ostatními paketovými přenosy. Ve WAN (Wide Area Network) sítích může být úspora na režijních nákladech až 50% proti IP protokolu [28]. Mezi používané kodeky patří ITU G.723.1 a G.729A, které vyžadují pro kvalitní přenos hlasu pásmo o šířce 56/64 kbps.
- **Voice over Asynchronous Transfer Mode (VoATM)** – V síti ATM putují data v podobě buněk o velikosti 53 bytů, přičemž každá má příslušnou hlavičku o velikosti 5 bytů. Pevná a malá velikost buněk má velkou výhodu ve snadném a rychlém přepínání. Režie, která vzniká při přenosu hlasu, je v porovnání s předchozími na střední úrovni. V čistokrevných sítích ATM jsou používány kodeky založené na PCM, v případě hybridní ATM a Frame Relay sítě je kodek přizpůsoben dle FR.

4 DIGITALIZACE HLASU

Zvuk je z pohledu fyziky brán jako podélné mechanické vlnění v látce. V případě pevných látek jde o vlnění příčné. Tento jev pak v lidském uchu může vyvolat sluchový vjem. V případě analogového přenosu je pouze toto vlnění zaznamenáno mikrofonem a převáděno na elektrické. Elektrický signál je následně digitalizován, celý proces digitalizace je popsán v následující části (konkrétně bude popsána Pulse Coded Modulation – PCM).

4.1 VZORKOVÁNÍ

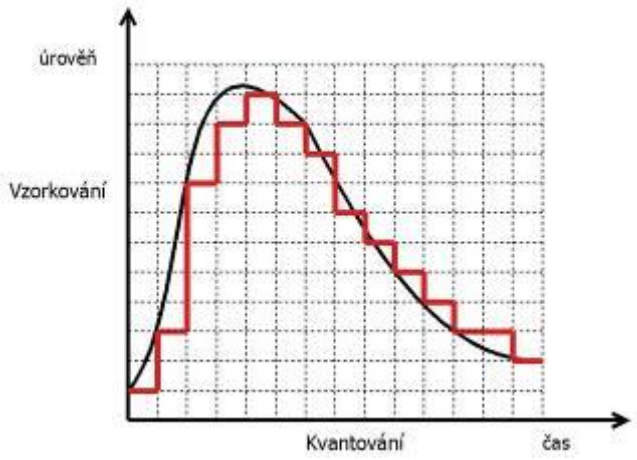
Vzorkování je snímání spojitého signálu v pravidelných intervalech. V případě PCM je vzorek měřen každých 125 mikrosekund, což je 8 000x za sekundu. Tyto pravidelné intervaly jsou nazývány jako vzorkovací frekvence, která je nejčastěji uváděna v kHz. Tedy u PCM je vzorkovací frekvence rovna 8 kHz. Čím vyšší vzorkovací frekvence, tím více je zachyceno detailů, ovšem s narůstající kvalitou narůstá i datová náročnost.

S výběrem vhodné frekvence souvisí Shannonův-Nyquistův-Kotělnikův teorém, který praví: „Přesná rekonstrukce spojitého, frekvenčně omezeného, signálu z jeho vzorků je možná tehdy, pokud byl vzorkován frekvencí alespoň dvakrát vyšší než je maximální frekvence rekonstruovaného signálu.“ [13]

4.2 KVANTOVÁNÍ

Aktuální úroveň vzorku lze opět zaznamenat pomocí omezeného počtu hodnot. Proto je aplikováno vzorkování v určitém rozsahu. Při samotném vzorkování může docházet k zaokrouhlování. U PCM je používáno číslo o velikosti 8 bitů.

Pakliže je snímána úroveň do podoby 8 bitového čísla 8000x za sekundu, pro samotný přenos hlasu je tedy vyžadována šířka pásma 64 kb/s.



OBRÁZEK 2 - PROCES DIGITALIZACE

4.3 KODEKY

Pojem kodek je složen z pojmů kodér a dekodér, respektive komprese a dekomprese. Kodek může být implementován jak v softwarové, tak hardwarové podobě a slouží k transformaci vstupních dat na výstupní. Tímto způsobem uložená data bývají méně náročná na kapacitu jak přenosového média, tak i úložného prostoru. Kodek ovšem může data i šifrovat a zabránit tak nevyžádaným odposlechům. O úspoře jednotlivých kodeků hovoří následující tabulka:

KODEK	ŠÍŘKA PÁSMA [KBPS]	ALGORITMUS
GSM	13	ACELP
G.711	64	PCM
G.722	48/56/64	SBADPCM
G.726	32	ADPCM
G.727	16-40	ADPCM
G.728	16	LD-CELP
G.729	8	CS-ACELP
G.723.1	5,3/6,3	ACELP/MPMLQ

TABULKA 1 - PŘEHLED KODEKŮ. ZDROJ: [2]

5 IP – INTERNET PROTOCOL

IP neboli Internet Protocol je protokol, který se využívá pro přenos dat v datových sítích. Současná podoba Internetu je postavena především na tomto protokolu a ani v blízké budoucnosti se to nezmění. Stejně jako ostatní technologie v informatice, i IP prošlo během své existence několika verzemi. Již od počátku roku 1983 se stal hlavním protokolem Internetu a nahradil tak Network Control Protocol (NCP). Experimentální provoz byl však započat v roce 1980. Zmínky o samotném vzniku jsou datovány k roku 1978, ve kterém se stal součástí TCP (Transfer Control Protocol). Později byl však vyčleněn jako samostatný protokol, který se v OSI modelu umístil na úrovni síťové vrstvy.

Hlavním úkolem IP protokolu je směrování a adresace v síti, přenášená data jsou rozdělena na jednotlivé datagramy. Odesílaná data nevyžadují předem vyhrazenou cestou a mohou tak putovat různými trasami dle aktuálního zatížení a dostupnosti. Samotné doručení dat není 100% zajištěno, proto je protokol označen jako nespolehlivý. Spolehlivost vyžaduje další režii, proto může být zajištěna až na úrovni vyšších vrstev (k tomu je často používán protokol TCP). Například u vysílání multimediálních dat není 100% spolehlivost vyžadována, jelikož samotnou ztrátu několika paketů nemusí samotný uživatel zaznamenat.

5.1 IPV4

5.1.1 ÚVOD

Jak je z názvu patrné, jedná se o čtvrtou verzi IP protokolu. O předchozích třech verzích je ovšem k dispozici velmi málo informací. Předchozí tři verze sloužili buď k laboratorním účelům, nebo byly součástí tehdejšího TCP protokolu. V 70. letech byl IP protokol oddělen od TCP protokolu. Ten byl v té době ve 4 verzi, proto i protokolu IP bylo přiděleno stejné číslo. Ačkoliv si toto označení nese protokol od svého počátku, v běžné komunikaci se zažilo používat pouze IP.

Na první pohled nejviditelnějším rozdílem mezi IPv4 a IPv6 jsou samotné adresy, změn je ovšem vícero.

5.1.2 ADRESY

Kromě adresy pro koncové zařízení je nutné i adresování samotné sítě, či všech uzlů v rámci dané sítě. Pro účely adresování sítě jsou používány adresy, které mají v hostitelské části samé nuly (například 192.168.1.0). V případě broadcastové adresy, jejímž účelem je zasílání dat na všechny uzly v dané síti slouží IP adresa s jedničkami v hostitelské části (například 192.168.1.255).

IPv4 adresa je dlouhá 32 bitů, nejpoužívanějším zápisem je čtveřice čísel s hodnotami od 0 do 255, jenž jsou zapsány v desítkové soustavě oddělené tečkou (například 192.168.1.1). Na první pohled by se mohlo zdát, že rozsah adres je nevyčerpatelný, opak je však pravdou. Hlavním problémem IPv4 se v posledních letech stává právě nedostatek adres, jehož příčinou bylo nevhodné rozdělování (vzhledem k jeho velké oblibě v pozdějších letech) hned v počátku zavedení. Celkový počet možných adres činí 2^{32}, což je přibližně 4×10^{9} možných kombinací.

Při zavedení IP protokolu byla adresa rozdělena na dvě části a to síťovou a hostitelskou. Zařízení, které mají stejnou síťovou část, patří do stejné sítě. Délka síťové adresy je dána podle tzv. tříd. Podle zvolené třídy bylo pak možné určit kolik má daná třída počítačů. Nejlepší ukázkou rozdělení je následující tabulka:

Třída	Hodnota 1. Bajtu	Binární začátek	Maska	Síťová část	Hostitelská část	Počet sítí	Počet hostů v každé síti
A	0 – 127	0	255.0.0.0	7	24	126	16 777 214
B	128 – 191	10	255.255.0.0	14	16	16 384	65 534
C	192 – 223	110	255.255.255.0	21	8	2 097 152	254
D	224 – 239	1110	Multicast				
E	240 – 255	11110	Experimentální				

TABULKA 2 - TŘÍDY IP ADRES. ZDROJ: [29]

Při pohledu do tabulky je vidět, že získáním síťové adresy z třídy A je přiděleno přes 16 milionů adres pro samotná zařízení v síti. To efektivně nedokáže využít žádná současná společnost, přesto tyto adresy byly přiděleny a počet dostupných adres se tak

znatelně ztenčoval. Adresy z třídy A získala například General Electric Company, IBM Corporation, Xerox Palo Alto Research Center, Apple Computer Inc. a spousta dalších.

Množství adres přidělených podle třídy C může být naopak příliš malé. Společnost, která by potřebovala připojit 300 zařízení, by musela vlastnit dvě síťové adresy, čímž by mohla přidělit adresy až 508 (4 adresy jsou obsazeny broadcastovými a sítě) zařízení. 208 by jich tedy zůstalo nevyužito. Jinou možností je přidělení síťové adresy z třídy B, ale v tomto případě by docházelo ještě k většímu plýtvání.

5.1.3 Maska - Classless Inter-Domain Routing

V počátečním návrhu nebylo s maskou sítě počítáno, tento způsob rozdělení se objevil až v pozdější době jako reakce na nepříliš variabilní způsob členění podle tříd. Díky VLSM – Variable Length Subnet Mask (neboli proměnlivá délka síťové masky) je možné rozdělit příliš velkou síť na menší či naopak malé sítě spojit do větších (takzvaných supersítí).

Pro využívání této techniky je zapotřebí příslušná podpora nejen v operačním systému, ale i ve směrovačích a směrovacích protokolech. Tato metoda se od roku 1993 úspěšně používá. Přesto byly již některé rozsahy rozdány a hrozilo vyčerpání stávajících adres, byly zavedeny další techniky. Více informací je k dispozici v RFC 4632 [30].

5.1.4 Privátní (neveřejné) adresy

Původním účelem IP protokolu bylo adresování v Internetu, ale návrh protokolu byl natolik dobrý, že se ujal i u sítí lokálních. Proto byl stanoven rozsah lokálních IP adres, které se v Internetu nepoužívají a tak nejsou ani ven směrovány směrovači. Používat lze některé z následujících rozsahů (x zastupuje rozsah od 0 – 255. Ve výsledku je tedy možné zvolit až 256 různých síti, kde v každé může být až 254 zařízení):

	Počáteční adresa	Koncová adresa	Počet sítí	Počet hostů v každé síti
Třída A	10.0.0.0	10.255.255.255	1	16 777 214
Třída B	172.16.0.0	172.16.255.255	1	65 534
Třída C	192.168.x.0	192.168.x.255	256	254
Lokální	127.0.0.0	127.255.255.255	1	16 777 214

Tabulka 3 - Rozsah privátních adres. Zdroj: [29]

Tyto rozsahy naleznou uplatnění nejen v lokálních sítích, které nejsou připojeny k Internetu, ale i v případě použití překladu adres (více v kapitole NAT).

5.1.5 Dynamické přidělování IP adres

Další metodou, jak lze snížit nedostatek veřejných IP adres je jejich dynamické přidělování. Ne každý počítač, který je připojen, k Internetu musí být připojen nonstop. Tohoto způsobu je využíváno především u telekomunikačních společností. Připojený klient tak může pokaždé získat jinou IP adresu. Poskytovatel díky tomu nepotřebuje stejný či větší počet IP adres jako má klientů. Pakliže by jeho služeb využívala v daný okamžik vždy pouhá polovina uživatelů, postačí mu i polovina IP adres, které budou dynamicky přidělovány.

5.1.6 NAT

Jelikož je rozsah IPv4 adres omezený a s každým dnem jich je volně dostupných méně a méně, byla vymyšlena technika nazývaná NAT (Network Adress Transaltion), což lze volně přeložit jako překlad síťových adres. Princip této technologie je jednoduchý a velmi často používaný. Velká část počítačů a zařízení, jenž využívá Internetové služby, se nejčastěji připojuje k nějakému serveru (webovému, streamovacímu, datovému atd.) a není tedy vyžadováno přímé připojení k těmto počítačům.

NAT v principu překládá privátní adresy na veřejné a zpět. Pakliže je odeslán požadavek z lokální sítě do Internetu, je na směrovači zaměněna zdrojová adresa lokálního PC za veřejnou adresu směrovače. Příslušný server odpovídá směrovači, který si pamatuje jednotlivé požadavky a díky tomu přesměruje příchozí datagram příslušnému PC. Z principu je tedy jasné, že komunikace nemůže být navazována v opačném směru. Směrovač totiž neví, k jakému zařízení by měl datagram směrovat.

Přestože patří tato technika mezi nejpoužívanější a znatelně pozastavila úbytek veřejných IP adres, jejím použitím vzniká mnoho problémů nejen v oblasti VoIP. Nejefektivnější komunikace je realizována pomocí přímého spojení. To je u dvou uživatelů, kteří jsou oba za jiným NATem velice problematické.

5.2 IPv6

5.2.1 Úvod

Především nedostatek IP adres má řešit nová verze, tedy IPv6. Nejjednodušším řešením bylo rozšířením adresného prostoru pouhým zvětšením IP adresy. IPv6 adresa má 128 bitovou délku, což je 4x více než u IPv4. Dohromady je tedy možné jednoznačně určit až 2^{128} uzlů, což je přibližně 3×10^{38} adres. Zatímco 4×10^{9} IP adres muselo v případě IPv4 vystačit celé planetě, v případě IPv6 lze použít 6×10^{23} IP adres na rozlohu 1 m² zemského povrchu.

5.2.2 Adresy

Díky natolik velkému adresnému prostoru je v IPv6 běžné přiřazování více adres jednomu síťovému rozhraní. Jednotlivé adresy mají svůj význam a mohou zjednodušovat komunikaci a správu sítě. Na druhou stranu mohou samotné uživatele zmást (díky délce a způsobu zápisu se nepočítá s tím, že by uživatelé pracovali přímo s adresami) a vnést chyby do komunikace při ruční konfiguraci.

5.2.3 Mobilita

Při návrhu tohoto protokolu bylo již počítáno s mobilními zařízeními, tudíž IPv6 podporuje mobilitu. Díky tomu je možná dostupnost na „jedné stálé“ IPv6 adrese, ať už se dané zařízení připojuje odkudkoliv. V oblasti IPv4 znamenala každá změna umístění i změnu adresy, tento problém musel být řešen pomocí přihlašování k určitému serveru a uvedením aktuální adresy (na obdobném principu je zajištěna mobilita i v IPv6). Výhoda spočívá v tom, že už tento problém nemusí řešit aplikace, protože je o to postaráno na úrovni síťové vrstvě.

Kromě výše uvedeného je dále k dispozici QoS pro zajištění kvality jednotlivých služeb. Výhod IPv6 je mnohem více (například automatická konfigurace), ale ostatní výhody se přímo netýkají této práce.

6 VoIP – Voice over Internet Protocol

Důvodů proč jsem práci věnoval právě VoIP je vícero a některé již byly zmíněny výše, přesto je zopakuji. Protokol IP je základním stavebním kamenem Internetu, pakliže bude na tomto protokolu postavena i hlasová komunikace, bude se možné dovolat kdekoliv po Internetu. Hovory mohou probíhat i rámci lokální sítě ve společnosti, přestože nebude připojena k Internetu.

Při vhodném návrhu VoIP infrastruktury je k dispozici mobilita. Pracovník se tak může připojit odkudkoliv přes Internet a další kolegové mu mohou volat na jedno služební číslo.

Samotný přenos může efektivně probíhat skrze vícero cest podle aktuálního vytížení. Přenosové trasy tak mohou být efektivně využívány. Při budování nové infrastruktury stačí pouhé vytvoření datové sítě, jelikož telekomunikační infrastrukturu zastoupí právě datová. Tento způsob může výrazně ušetřit náklady za pronájem příslušných okruhů.

Náklady mohou být ušetřeny i při pořizování samostatných zařízení, jelikož telefonní aparát může být zastoupen příslušně vybaveným počítačem (zvuková karta, reproduktory a mikrofon), či téměř každým notebookem s příslušnou aplikací (které často bývají zdarma).

6.1 Signalizační protokoly používané pro VoIP

Stejně jako v klasické telefonii, i v té paketové jsou používány speciální signály pro řízení jednotlivých akcí, mezi které lze zařadit například zahájení či ukončení hovoru a mnoho dalších. V případě VoIP samozřejmě nemluvíme o elektrických signálech, ale o signalizačních protokolech.

V současné době existují různé podoby těchto protokolů, které se mezi sebou často výrazně odlišují. Pro základní představu zde uvádím příklady standardizovaných protokolů, které patří mezi ty nejčastěji používané. Další kategorií jsou protokoly proprietární, které jsou nejčastěji používány v rámci jedné značky (příkladem může být SKINNY společnosti Cisco Systems, Inc.).

6.1.1 H.323

Za vývojem tohoto protokolu stojí Mezinárodní telekomunikační unie (ITU-T, International Telecommunication Union), která se zabývá standardy v oblasti telekomunikací. Signály tohoto protokolu jsou přenášeny v binární podobě a principy jsou velice podobné telefonním standardům. Výhodou binárního přenos mohou být nižší režijní náklady, nevýhodou však bývá těžší implementaci a případné ladění chyb.

H.323 mimo samotné signalizace (H.225.0) obsahuje RTP protokol pro přenos hlasu (G.7xx), videa (H.26x) a mnoho dalších. Jedná se tedy o celou rodinu protokolů, která může být nasazena samostatně (pro přenos hlasu není zapotřebí dalších protokolů, jelikož jsou všechny obsaženy). Zatímco zvukový kodek G.711 použitý v prvních verzích vyžadoval pro přenos hlasu datový tok o velikosti 64 kbps, v současné době používaný G.723 si vystačí již s datovým tokem o velikosti 8 kbps.

Praktické využití nalezl tento protokol v koncových aplikacích jako NetMeeting a Ekiga (implementace OpenH323). Zatímco dříve patřil tento protokol mezi nejpoužívanější, dnes ho již překonává SIP.

6.1.2 MGCP - Media Gateway Control Protocol

MGCP je jednou z implementací Media Gateway Control Protocol architektury. Tato architektura slouží k řízení tzv. media gateway, což je zařízení které slouží ke konverzi digitálního multimediálního streamu mezi různorodými telekomunikačními sítěmi. Nejčastějším případem je právě konverze mezi IP a PSTN (Public Switched Telephone Network – neboli veřejná telefonní síť) sítěmi.

6.1.3 SIP - Session Initiation Protocol

Zatímco H.323 protokol používal binární přenos, SIP využívá textovou formu. S tímto druhem přenosu se lze setkat například u protokolů HTTP (HyperText Transport Protocol) a SMTP (Simple Mail Transfer Protocol), kterým je velmi podobný (například čísla chybových hlášení), inspirací tedy byl svět sítí. Na rozdíl od H.323 nejsou dále specifikovány protokoly a kodeky pro samotný přenos hlasu. Je tedy pouze na vývojáři aplikace či samotném uživateli, jak bude hlas komprimován a kterých protokolů bude využíváno. S tímto souvisí i různorodost využití, protokol může sloužit i pro zasílání

rychlých zpráv (IM – Instant Messaging), hraní multiplayerových her apod. K přenosu audiovizuálních dat je nejčastěji využíváno RTP (**Real-time Transport Protocol**) protokolu.

Zatímco v případě H.323 byl telefonní hovor přenášen společně se signalizací, v případě SIP může probíhat signalizace odděleně od samotného hovoru. Na VoIP ústřednu jsou tak kladeny menší požadavky v oblasti systémových prostředků a síťového připojení (není nutné zpracovávat pakety s hovorem).

SIP protokol je podstatně mladším protokolem, jeho vznik se datuje k roku 1996 a za jeho vývojem stojí organizace IETF (Internet Engineering Task Force). Využití v současné době nalezne ve velkém množství aplikací, dokonce je podporován i některými mobilními telefony (Nokia, zařízení na platformě Windows Mobile).

7 SIP - SESSION INITIATION PROTOCOL

Jak již bylo zmíněno, základy tohoto protokolu vyplývají ze světa sítí, takže v SIP protokolu se můžeme setkat s přístupem klient-server, transakcemi, metodami, různými hlášeními apod. V této části uvádím pouze základní informace, ve skutečnosti jsou možnosti daleko širší a podrobnější. Výpis podrobných informací o protokolu SIP by několikanásobně přesahoval rozsah samotné práce.

7.1 FUNKCE PROTOKOLU

SIP zajišťuje pět základních činností, které jsou následující:

1) Lokalizace – zajišťuje nalezení vhodného spojení s cílovou stanicí
2) Zjištění stavu – slouží k zjištění schopnosti navázání spojení
3) Zjištění možností – výběr kodeku, zjištění maximální přenosové rychlosti, volba přenosu (audio/video)
4) Navázání vlastního spojení - RTP
5) Řízení probíhajícího spojení – přenos změn vlastností probíhajícího hovoru, případně samotné ukončení

7.2 METODY

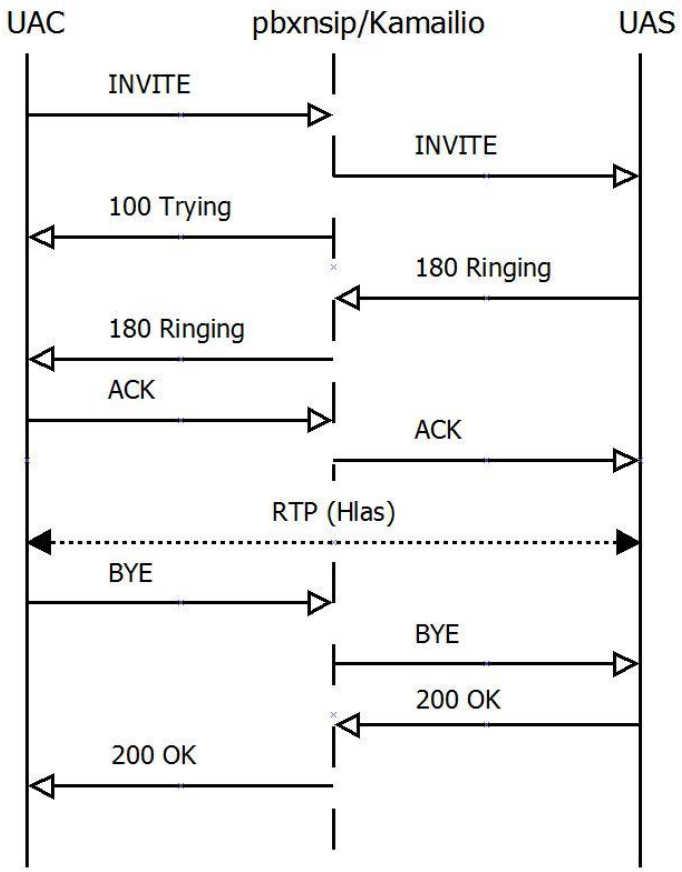
Jednotlivé metody SIP protokolu jsou zapisovány pomocí velkých písmen, tedy stejně jako u HTTP, ze kterého vychází.

- REGISTER – Tato metoda registruje adresu účastníka u SIP Proxy serveru.
- INVITE – Slouží k přizvání uživatele či služby ke komunikaci. Zpráva obsahuje popis spojení (relace).
- ACK – Je potvrzením na úspěšné přijetí dotazu INVITE.
- CANCEL – Ukončuje nevyřízené požadavky, které jsou identifikovány podle položek Call-ID, To, From a Cseq. Na již vyřízené požadavky tato metoda nemá vliv.
- BYE – Je používána pro ukončení probíhajícího hovoru, tato metoda může být zaslána jak volajícím tak volaným účastníkem.

7.3 HLÁŠENÍ

V případě hlášení jednotlivých stavů je shoda s protokolem HTTP ještě výraznější. Převzaty byly stejné kategorie i způsob rozlišení pomocí tříciferných čísel. Kromě samotných čísel je přenášena i textová informace, příkladem může 100 – Trying, či 200 – OK. Jednotlivá hlášení jsou rozdělena podle první číslice do následujících skupin:

- 1xx - informace o průběhu
- 2xx - úspěch
- 3xx - přesměrování
- 4xx - chyba na straně klienta
- 5xx - chyba na straně serveru
- 6xx - fatální chyba



OBRÁZEK 3 - PRŮBĚH KOMUNIKACE

7.4 Terminologie v SIP

Stejně jako každý obor má svou terminologii, i VoIP oblast používá specifické pojmenování jednotlivých prvků. V případě protokolu SIP jsou termíny a pojmenování jednotlivých prvků navíc odlišné i od H.323 a dalších VoIP protokolů. V následující části jsou uvedeny nejpoužívanější termíny, které budou v práci používány.

7.4.1 SIP URI

SIP URI (Uniform Resource Identifikator) slouží k adresaci jednotlivých uzlů. V SIP protokolu se nevyskytuje pouze jeden druh URI, jako tomu je u jiných protokolů. SIP URI je v těchto případech složeno z názvu protokolu, za nímž následuje dvojtečka. Po té je uvedena lokální část (může být složena jak z čísel, písmen případně jejich kombinací) a doména, jež jsou odděleny znakem @. Příkladem může být *sip:novak@test*, který nám říká, že existuje uživatel se jménem novak, který používá sip protokol a vyskytuje se v doméně test. Doména je vlastně adresa, na které se nachází ústředna, lokální část pak zastupuje adresu uživatele v dané doméně. V lokální části jsou rozlišovány velká a malá písmena, u domény již ne. Pakliže je používán standardní port, tedy 5060 nemusí být v adrese uveden. V případě, že je použit jiný port, musí být za SIP URI uvedena dvojtečka a číslo portu, například *sip:novak@test:5065*. Adresa je tedy velmi podobná těm používaných u e-mailové komunikace, což souvisí s inspirací u protokolu SMTP.

AOR (address of record) URI může sloužit k identifikaci osoby, skupin osob, služby či telefonního přístroje. Například skupina osob může být užitečná v případě použití ve velké společnosti, stačí tak jedna adresa pro celé oddělení. Při volání na tuto adresu se rozezvoní všechny telefony a odpovědět může kdokoliv z nich.

Contact URI posílá příslušná aplikace či zařízení (user agent) při registraci do domény. Příkladem může být *sip:novak@192.168.1.5*, čímž je řečeno, že uživatel novak je k zastižení na počítači s IP adresou 192.168.1.5. Zatímco AOR URI je dosažitelné odkudkoliv z Internetu, v případě Contact URI může být funkčnost omezena na lokální síť. Contact URI slouží pouze pro potřeby ústředny.

Protokol SIP umožňuje i šifrovaný přenos pomocí TLS, který lze poznat podle adresy začínající na *sips:*. Opět je zde vidět podobnost s protokolem HTTP (šifrovaná podoba HTTPS). Příkladem tedy může být *sips:novak@test*.

Kromě těchto adres může být adresa spojena s dalšími parametry, které mohou upřesňovat způsob přenosu či zasílat zprávu. Příkladem může být *sip:uzivatel@domena;transport=tcp*, což značí, že pro přenos dat se bude používat TCP protokol. Další možností je například *sip:uzivatel@domena?subject=Zprava*, kde se příjemci zobrazí text Zprava ještě před tím, než by hovor přijal (další shoda se zápisem e-mailové adresy).

7.4.2 User Agent (UA)

Je koncové zařízení, které může zahájit, přijímat a ukončit relaci. Toto označení lze použít jak pro software, tak hardware. V případě softwarové varianty se mluví o aplikaci, která je nainstalována na PC a slouží k telefonování. V případě hardwaru jde například o stolní VoIP telefon. Tedy přístroj, jenž se podobá klasickému telefonu, akorát pracuje na IP síti. Ačkoliv by se mohlo říci, že UA je vlastně telefon, není to celá pravda. V roli UA mohou být i hlasové automaty, záznamníky či zabezpečovací zařízení.

UA se navíc dále rozlišuje podle způsobu komunikace. UA zahajující spojení se nazývá **user agent client (UAC)** a zasílá požadavky serveru. V této roli lze používat následující metody INIVITE, ACK, OPTIONS, BYE, CANCEL, a REGISTER. UA odpovídající na požadavky se nazývá **user agent server (UAS)**. Tyto role jsou pouze v době, kdy probíhá daná transakce. Během samotného hovoru pak jsou role obou UA zařízení rovnocenné. Pro správnou funkčnost je tedy zapotřebí aby hardwarový i softwarový telefon uměl ovládat obě role.

7.4.3 Registrar Server

Jednotlivé UA jsou v síti identifikovatelné a dosažitelné podle svého Contact URI. O správu těchto adres se stará právě registrar server. Každý uživatel v dané doméně posílá tomuto serveru informaci (Contact URI) o svém jméně a IP adrese, na které se nachází. Tento server informace uloží a na vyžádání od proxy či redirect serveru je sdělí.

7.4.4 Proxy Server

Proxy server slouží ke směrování podle požadavků jednotlivých žadatelů. Jde vlastně o prostředníka, který zajišťuje komunikaci mezi dvěma UA. Díky proxy serveru může být dostupné více telefonů v lokální síti pomocí jedné veřejné adresy. Veřejnou adresu má právě proxy server, který se pak stará o přeposílání dat příslušným UA ve vnitřní síti. Proxy servery také mohou používat službu presence service, která slouží k zjištění, zda je uživatel dostupný či ne. Díky této službě pak můžete v telefonu vidět, zda je dotyčný u telefonu (online) či není (offline).

Funkci uvedu na příkladu, kdy účastník A chce uskutečnit hovor s účastníkem B. Účastník A zná číslo účastníka B, ale neví, kde se nachází. Nejdříve se tedy musí zeptat proxy serveru. Proxy server tento požadavek příjme a pošle ho registrar serveru pokud je účastník B ve stejné doméně. Pakliže je v doméně jiné, pošle požadavek proxy serveru v příslušné doméně, kde se stejným způsobem zjistí adresa účastníka B. Pakliže je adresa účastníka B nalezena, vrací se pomocí proxy serverů zpět k účastníku A. Nyní účastnící znají své adresy a mohou spolu komunikovat skrze proxy server(y). Hovor však může probíhat přímo a proxy server pak přenáší pouze signalizaci.

Proxy servery lze rozdělit na stavové (statefull) a bezstavové (stateless). Stavové servery zaznamenávají probíhající transakce, zatímco bezstavové ne. Výkon proxy serverů je měřen v počtu transakcí za sekundu.

Často lze narazit na softwarové produkty, jež spojují několik serverů dohromady, nejčastěji to bývá právě proxy, redirect a registrar v jednom. Pro zjednodušení budu nadále používat pojem ústředna pro kombinaci těchto serverů.

7.4.5 Redirect Server

Tento server přijímá SIP požadavky a přiřazuje buď nulové, nebo nové adresy, které následně vrací klientovy. Redirect server využívá služeb registrar serveru, od kterého zjišťuje nové adresy. Redirect server na rozdíl od proxy serveru nevytváří vlastní požadavky, kterými by kontaktoval požadovaný cíl. Místo toho vrátí požadavek klientovi s tím, že klient musí sám změnit cestu, aby dosáhl svého cíle.

7.4.6 B2BUA - Back to Back User Agent

Je zařízením, které obsahuje více UA. Díky těmto UA pak může toto zařízení fungovat podobně jako proxy server ke směrování požadavků. Zásadní rozdíl je v tom, že proxy server požadavky přeposílá, zatímco toto zařízení v roli UAS je zpracovává a jako UAC je odesílá dále. Pakliže je navázán hovor mezi dvěma koncovými body, ve skutečnosti probíhají hovory dva. První hovor probíhá mezi volajícím a ústřednou, druhý pak probíhá mezi ústřednou a volaným. Díky tomu může dojít k ukončení hovoru či změnám i ze strany ústředny (proxy server hovor ukončit nemůže). Nevýhodou jsou samozřejmě vyšší systémové nároky.

Příkladem takové ústředny je například často používaný Asterisk či v této práci testovaný pbxnsip.

8 PRAKTICKÁ ČÁST

Cílem praktické části bylo odzkoušet a odvodit závěry z použití SIP protokolu v sítích IPv4 a IPv6. V první řadě bylo nutné zajistit vhodné podmínky pro provoz těchto protokolů, provoz v rámci lokální sítě nepředstavoval žádný problém. To je dáno tím, že v sítí nebyl žádný směrovač, který by mohl způsobovat potíže. Dostupnost nativního IPv6 připojení je mezi poskytovateli velmi nízká (v mém případě nulová), tudíž jedinou možností by bylo tunelování. Toto řešení nebylo zvoleno, jelikož by mohlo přinést další problémy v měření a testování.

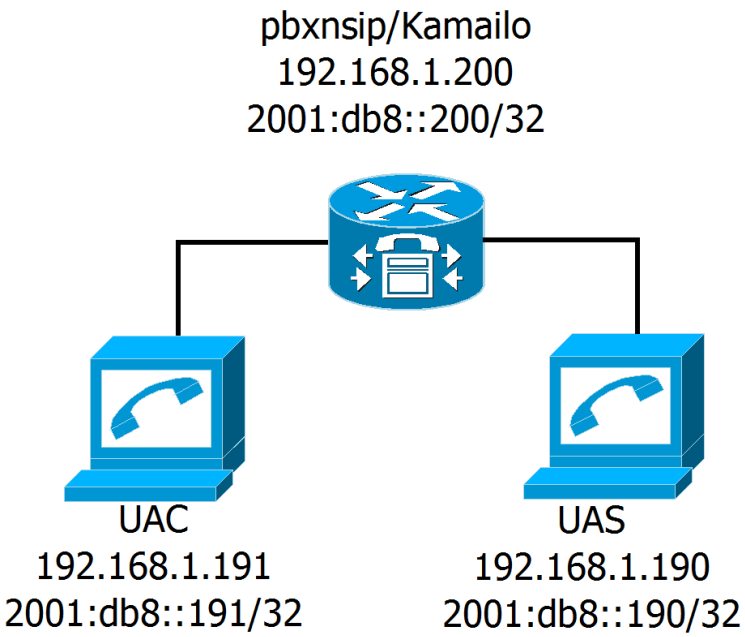
Dalším důležitým krokem byla volba operačního systému. Současné operační systémy již s podporou IPv6 počítají, pro testy byl konkrétně vybrán Debian 5.02, zkoušeno bylo i Ubuntu, které taktéž fungovalo bez problému (jediným problémem byla horší dostupnost některých nástrojů, proto byl zvolen právě Debian). Operační systém Debian byl mimo jiné zvolen díky snadné možnosti vytvoření tzv. live CD, které je součástí této práce. Na tomto CD je kromě operačního systému nainstalována VoIP ústředna včetně příslušných nástrojů pro sledování a testování komunikace. Dále pak byl zkoušen provoz na systémech Windows Vista Home Premium 64b, Windows 7 Ultimate RC 32b.

Hlavním krokem byla volba vhodné ústředny a testovacích nástrojů, jimž jsou věnovány následující podkapitoly.

8.1 TESTOVACÍ KONFIGURACE

Pro účely testování byly použity 3 počítače připojené do 100 Mb/s přepínače (switch). Konfigurace jednotlivých PC (CPU; RAM; OS) a jejich role je popsána níže:

- UAS – AMD Athlon X2 4850e (2 x 2,5 GHz); 1GB RAM; Debian 5.02
- UAC – Intel Core 2 Duo P8400 (2 x 2,26 GHz); 3GB RAM; Debian 5.02, Windows Vista Business, Windows 7 Ultimate Beta
- Pbxnsip/Kamailio – Intel Pentium Dual Core E2140 (2 x 1,6 GHz); 4GB RAM; Debian 5.02, Windows Vista Home Premium 64b, Windows 7 Ulitmate RC 64b



Obrázek 4 - Zapojení testovací konfigurace

8.2 SIP ústředna (PROXY + REGISTRAR + REDIRECT)

Na Internetu je v současné době velké množství SIP ústředen. Jejich výběr se ovšem velmi zužuje, pakliže je vyžadována podpora IPv6. Do této práce nakonec byly vybrány následující VoIP ústředny:

8.2.1 Kamailio (OpenSER) 1.5.1 - notls

Kamailio (dříve OpenSER) je opensource SIP ústředna, která vychází z projektu SIP Express Router (SER). Pro provoz na IPv6 je nutné v konfiguračním souboru přidat IPv6 adresu, na které má naslouchat, ve výchozím stavu totiž ústředna poslouchá pouze na IPv4 adresách. V této fázi je funkční signalizaci jak v sítích IPv4, IPv6 tak jejich kombinacemi.

8.2.2 pbxnsip (Windows - 3.3.1.3177, Debian – 3.4.0.3201)

Ústředna pbxnsip je zástupcem komerčního řešení, které je dostupné pro více operačních systémů. Podporovány jsou operační systémy Windows, Linux a Mac OS. Demoverze této ústředny umožňuje hovory o maximální délce 3 minut, což pro testování plně dostačovalo. Díky dostupnosti pro více platforem bude zajímavé sledovat, jak si poradí jednotlivé systémy s jednotlivými protokoly.

Konfigurace pbxnsip probíhá přes webové rozhraní a pro plnou funkčnost stačí pouhé zadání příslušného klíče. Tato ústředna byla testována na operačních systémech Debian 5.02, Windows Vista Home Premium a Windows 7 Ultimate RC.

8.3 SIP UA

Situace v oblasti softwarových telefonů je velmi podobná té s výběrem ústředny. Pakliže je kladen požadavek na funkčnost IPv6, výběr se výrazně zužuje. Nejlépe na tom je Linphone (použita byla verze 3.1.2 pro Windows, 2.1.1 pro Linux), který je dostupný jak pro operační systémy Linux, tak i Windows.

8.4 TESTOVACÍ NÁSTROJE

Existují sice nástroje, které by měli mít podporu IPv6, ale často jde o čistě komerční řešení (k dispozici nejsou ani demoverze - SIP Client-Server Traffic Generator od Valid8.com, PacketGen a PacketScan od GL Communications Inc.). K testování tedy bylo nakonec použito následujících nástrojů:

8.4.1 WIRESHARK 1.0.2

V testovacích nástrojích nesměl chybět Wireshark pro sledování síťového provozu, díky tomuto nástroji bylo možné identifikovat stranu, u které se chyba nacházela. Wireshark je dostupný pro operační systémy Windows, Linux a Mac OS.

8.4.2 SIPP 3.1

Pro testování samotného SIP protokolu byl zvolen nástroj SIPp. SIPp má však omezenou funkčnost při použití IPv6 protokolu (není zaručeno odesílání RTP) a ve Windows má některé funkce vypnuty. Proto byl používán výhradně v Debianu.

Při testu byl využit standardní scénář UAS a UAC v aplikaci SIPp, který simuluje uskutečnění hovoru a jeho následné zavěšení. Dalšími parametry scénáře bylo nastavení příslušného počtu uskutečněných hovorů (200, 400 a 1500) za sekundu po dobu 5 minut.

Při hodnotě 200 hovorů za sekundu dosahovalo zatížení CPU Intel Pentium Dual Core E2140 k 50-60% v závislosti na použitém protokolu. Dále byla zvolena hodnota 400, která simulovala plně zatíženou ústřednu. V této fázi již začalo docházet

k výpadkům některých hovorů, které byly následně vyhodnoceny jako chybné. Hodnota 1500 hovorů za sekundu byla zvolena kvůli propustnosti síťového rozhraní. V tomto případě je vidět jaký vliv mají různé protokoly při nedostatečném výkonu CPU, jako například při DoS útoku.

Při používání nástroje SIPp bylo vždy několik hovorů nevyhodnoceno, což je viditelné z tabulky (nejde ovšem o neúspěšné hovory, jelikož ty jsou zaznamenávány zvlášť). Měření bylo ukončeno po 6 minutách, kdy už byly všechny hovory odbaveny.

8.4.3 PJSIP 1.3

Jak se při pozdějším měření ukázalo, předchozí nástroj SIPp se jevil jako nedostatečný, tudíž došlo k výběru dalšího open source projektu, který umožňuje testovat SIP protokol a podporuje IPv6. Tento nástroj si navíc poradí i RTP protokolem v IPv4 i IPv6. Bylo tedy možné otestovat nejen chování signalizace, ale i přenos „hlasu“.

První test spočíval ve změření datové náročnosti jednotlivých protokolů. Pro měření přenesených dat byl použit vnStat a simulaci hovorů zajišťoval PJSIP. V této konfiguraci bylo současně provedeno 30 hovorů o délce 3 minut (omezení ze strany pbxnsip) a po té byly hodnoty přenesených dat zaznamenány. Výrazně větší počtu hovorů nebylo možné dosáhnout, jelikož PJSIP má při standardní kompilaci nastaven limit na 32. Ačkoliv jsem postupoval dle návodů pro kompilaci s podporou většího počtu hovorů, postup nebyl funkční. Postupnými pokusy jsem toto omezení navýšil, ale aplikace nebyla při větším počtu hovorů než 32 stabilní. Navíc ústředna přijímala maximálně 12 požadavků na nový hovor v krátkém okamžiku. Testovaných 30 hovorů jsem musel zahajovat postupně po 10. Díky tomu mohli být do výsledků měření vneseny chyby, tudíž další navyšování hovorů bylo ukončeno.

Druhý test měřil kvalitu hovoru pomocí vnitřních nástrojů PJSIP. Pro každou kombinaci spojení bylo provedeno sedm hovorů. Těchto sedm hovorů bylo následně zprůměrováno a zaznamenáno do příslušné tabulky. V tomto testu je použit termín jitter, což je nežádoucí odchylka jedné či více charakteristik periodického signálu v elektronice a telekomunikacích [31].

8.4.4 vnStat 1.6

Nástroj vnStat byl použit pro měření přenesených dat a přenosové rychlosti. Start a konec měření probíhalo ručním spuštěním testu UAC na jednom PC a spuštění měření na PC druhém. Čas byl sledován dle statistik UAC, čímž docházelo k maximální odchylce 2 sekund. Tento výsledek má minimální vliv na přesnost výsledků, jelikož parametrů ovlivňující toto měření bylo vícero (různé prodlevy a opakování jednotlivých hovorů). Údaje o přenesených datech a přenosových rychlostech jsou tedy spíše orientační.

8.4.5 htop 0.7

Nástroj htop sloužil ke sledování zatížení CPU, díky tomu bylo možné určit 100% zátěž dvoujádrového CPU Intel Pentium Dual Core E2140 při zpracovávání 400 hovorů za sekundu. Prováděny byly i další měření, ale v dalších případech docházelo k velkým odchylkám vůči naměřeným hodnotám. Proto jsou tyto výsledky reprezentovány pouze formou poznámky u jednotlivých scénářů. Tyto výsledky jsou však pouze orientační, jelikož mohli být ovlivněny systémovými službami apod.

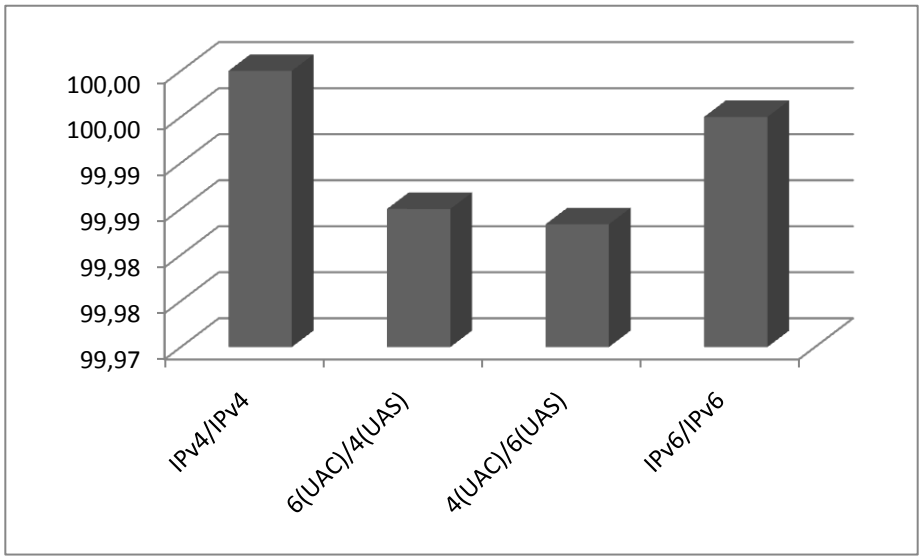
8.5 Kamailio

8.5.1 SIPp – 200 hovorů za sekundu

Tento test simuloval střední zátěž pro ústřednu Kamailio při použití různých IP protokolů. Pro testování byl použit SIPp, htop a vnStat. Důležité výsledky testů jsou shrnuty v následující tabulce:

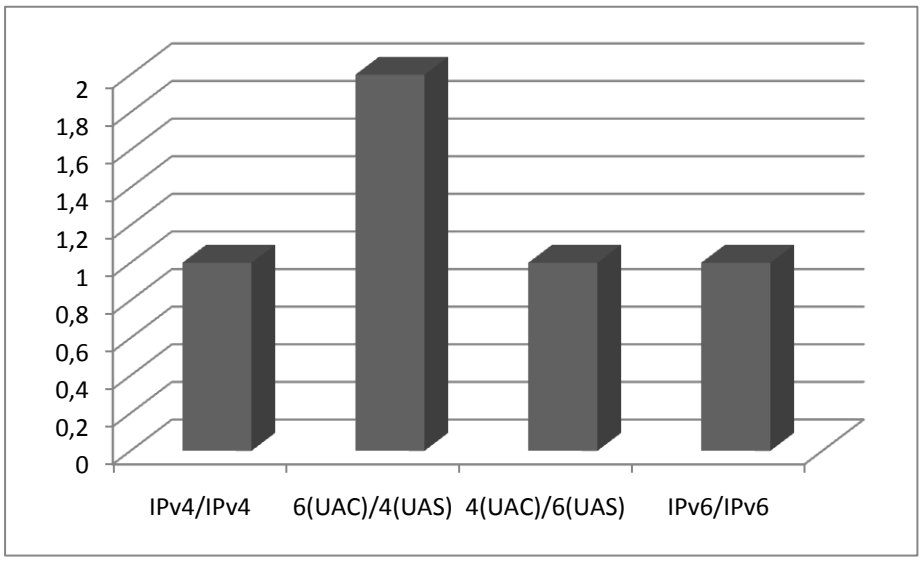
200	Počet hovorů			úspěch	odezva	Data [MB]		Maximální rychlost	
	celkem	úspěšné	Chybné	[%]	[ms]	upload	download	upload	download
IPv4 IPv4	59999	59999	0	100,00	1	444,3	480,8	1,47	1,6
6(UAC) 4(UAS)	59999	59990	8	99,98	2	482,7	503,3	1,63	1,69
4(UAC) 6(UAS)	59999	59989	6	99,98	1	445,6	495,3	1,52	1,67
IPv6 IPv6	59999	59996	3	99,99	1	483,3	524,7	1,62	1,76

Tabulka 4 - Kamailio/SIPp 200 hovorů za sekundu. Zdroj: vlastní měření



OBRÁZEK 5 - ÚSPĚŠNOST SPOJENÍ VYJÁDŘENÁ V PROCENTECH PRO 200 HOVORŮ ZA SEKUNDU

Jak je z výše uvedeného grafu vidět, rozdíly v úspěšnosti jsou v případě běžné zátěže z pohledu procentuální úspěšnosti nepatrné. Dále je vidět, že absolutním vítězem se 100% úspěšností se stala IPv4 síť. Ta je následována IPv6 podobou a na závěr se umístili hybridní varianty. Z pohledu počtu chyb jsou jasnými vítězi sítě, kde se používá pouze jeden z protokolů. U hybridních sítí musí docházet k překladu, což je dalším místem možného výskytu chyb.



OBRÁZEK 6 - PRŮMĚRNÉ ZPOŽDĚNÍ PŘI ZPRACOVÁNÍ POŽADAVKŮ PRO 200 HOVORŮ ZA SEKUNDU

Zajímavým číslem vypovídajícím o výkonu může být i průměrná doba zpoždění při zpracování jednotlivých požadavků. V tomto testu byl ovšem procesor vytížen pouze z poloviny, což se pozitivně projevilo na těchto hodnotách. Veškeré požadavky byly odbavovány ihned, ke drobnému zpoždění samozřejmě docházelo při překladu v hybridních sítích.

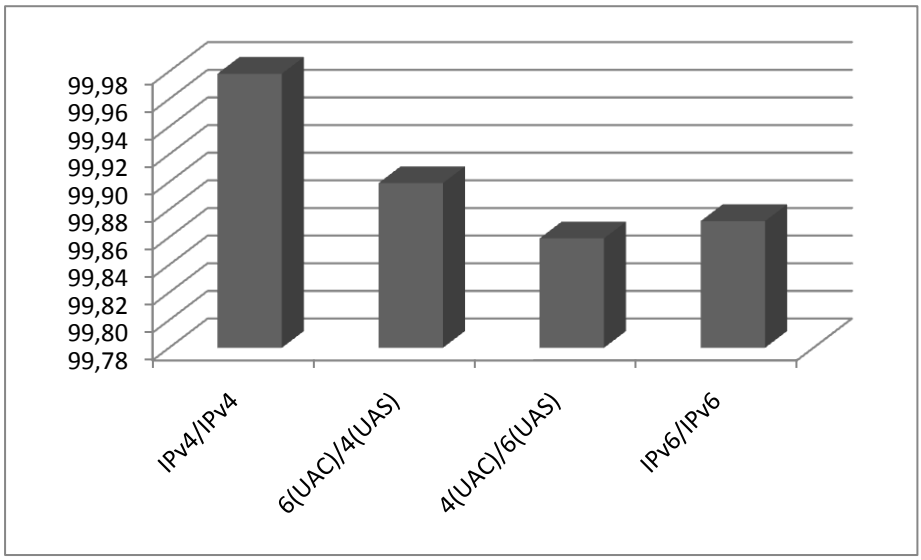
Při tomto testu bylo sledováno zatížení procesoru. V případě IPv4 docházelo k vytížení okolo cca 47%, v případě IPv6 cca 48%. Z toho plyne, že provoz v nativních sítích nemá vliv na výkon CPU a oba protokoly jsou si vyrovnané. V případě hybridní sítě ovšem vzniká režie při překladu, která se v případě UAS (s IPv4) a UAC (s IPv6) projevila 60% zatížením a v kombinaci UAS (s IPv6) a UAC (s IPv4) 50%. Rozdíly jsou dány nesouměrným rozložením požadavků na překlad adres z pohledu testované komunikace.

8.5.2 SIPp – 400 hovorů za sekundu

Účelem tohoto testu byla simulace vysoké zátěže pro ústřednu Kamailio při použití různých IP protokolů. Pro testování bylo použito následujících nástrojů: SIPp, htop a vnStat. Důležité výsledky testů jsou shrnuty v následující tabulce:

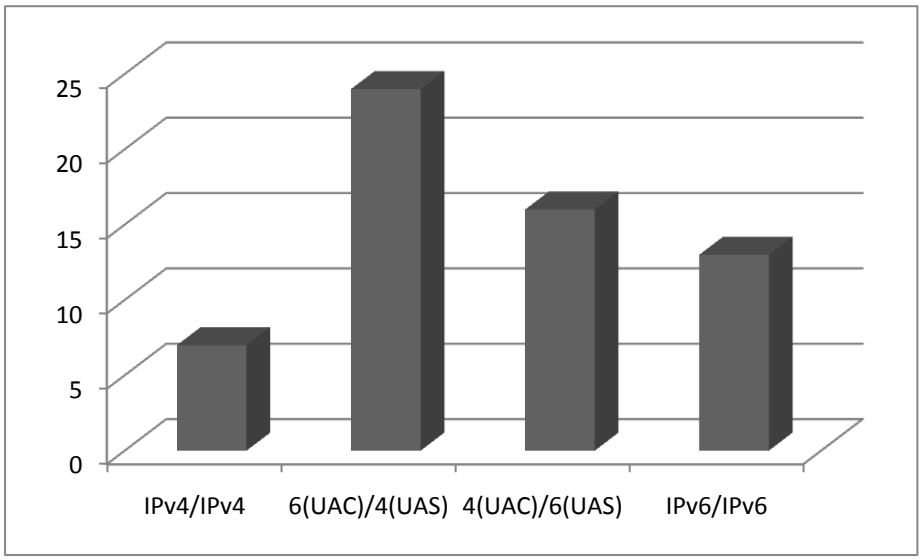
400	Počet hovorů			úspěch	odezva	Data [MB]		Maximální rychlost	
	celkem	úspěšné	chybné	[%]	[ms]	upload	download	upload	download
IPv4 IPv4	120000	119974	3	99,98	7	874,1	949,6	2,95	3,21
6(UAC) 4(UAS)	119996	119875	102	99,90	24	1410,0	951,0	3,3	3,53
4(UAC) 6(UAS)	119999	119830	146	99,86	16	884,1	993,8	3,05	3,42
IPv6 IPv6	119999	119845	3	99,87	13	958,4	1030,0	3,24	3,54

Tabulka 5 - Kamailio/SIPp 400 hovorů za sekundu. Zdroj: vlastní měření



OBRÁZEK 7 - ÚSPĚŠNOST SPOJENÍ VYJÁDŘENÁ V PROCENTECH PRO 400 HOVORŮ ZA SEKUNDU

Při 400 hovorech za sekundu již u některých protokolů přestával procesor plně obsluhovat všechny požadavky a docházelo tak ke zpoždění a chybám. Jak je z grafu vidět, IPv4 sít si vede stále nejlépe. Rozdíly jsou ovšem v řádu desetin procent, což může být i chybou měření. Chybu do měření může vnést právě SIPp, který nevyhodnocoval všechny hovory jako úspěšné či neúspěšné. Některé hovory totiž zůstávali pozastavené a z tohoto stavu se již nedostaly. Směrodatné tedy mohou být hodnoty neúspěšných hovorů, které jsou v případě sítí s jedním protokolem rovnocenné. V případě hybridních sítí jsou výsledky horší, příčinou je nutný překlad, který má vyšší nároky na systémové prostředky.



OBRÁZEK 8 - PRŮMĚRNÉ ZPOŽDĚNÍ PŘI ZPRACOVÁNÍ POŽADAVKŮ PRO 400 HOVORŮ ZA SEKUNDU

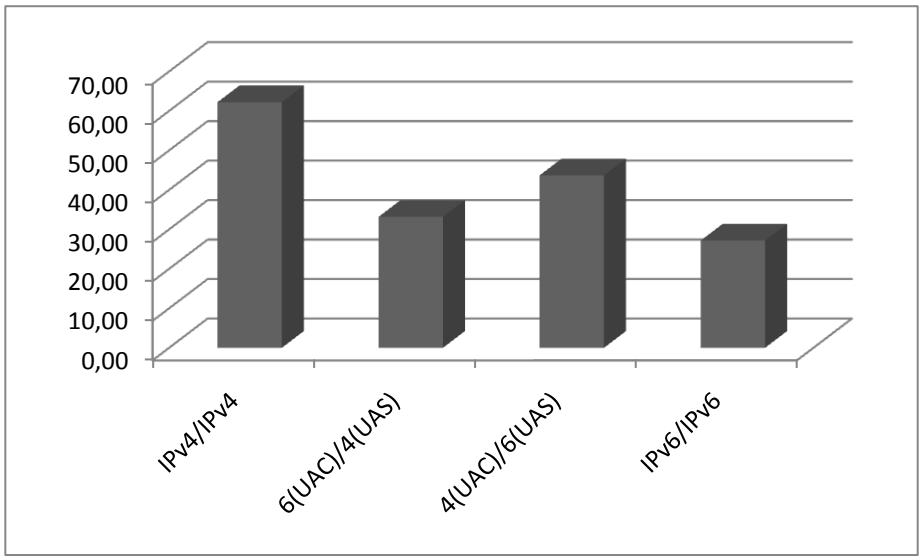
Výše popsané se projevilo i na zpoždění při zpracování požadavku. Jak je z grafu patrné IPv4 síť má nejnižší zpoždění. Téměř dvojnásobná doba je u IPv6 sítě. Hybridní sítě dosahují až 4x delších dob oproti IPv4.

8.5.3 SIPP – 1500 HOVORŮ ZA SEKUNDU

Poslední z testů pomocí nástroje SIPp byl test nadměrné zátěže pro ústřednu Kamailio při použití různých IP protokolů. Důležité výsledky testů jsou shrnuty v následující tabulce:

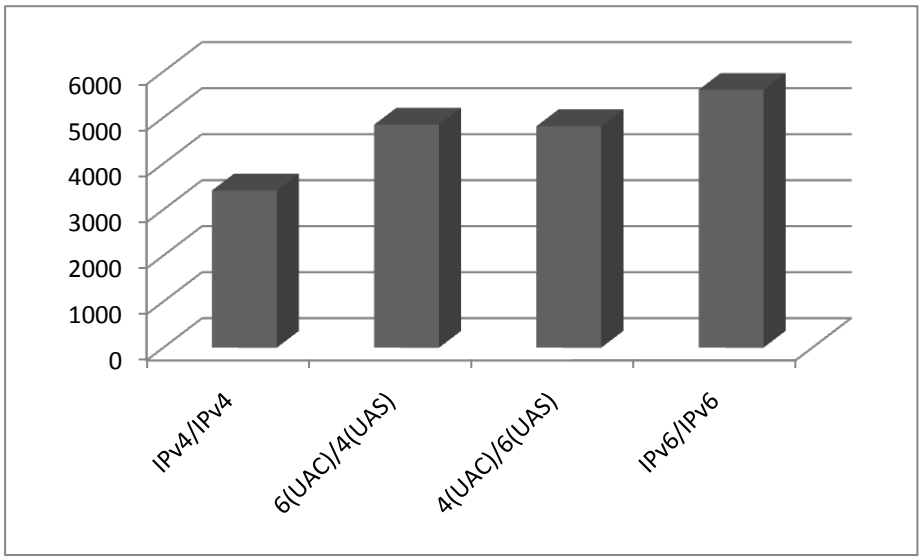
1500	Počet hovorů			úspěch	odezva	Data [GB]		Maximální rychlost	
	celkem	úspěšné	chybné	[%]	[ms]	upload	download	upload	download
IPv4 IPv4	450000	279909	160497	62,20	3417	2,46	3	8,86	10,88
6(UAC) 4(UAS)	449998	149235	293006	33,16	4848	1,69	2,61	8,07	10,81
4(UAC) 6(UAS)	449994	196530	243800	43,67	4814	1,76	2,75	7,37	10,83
IPv6 IPv6	449998	122211	316755	27,16	5605	1,78	2,38	8,85	11,37

TABULKA 6 - KAMAILIO/SIPP 1500 HOVORŮ ZA SEKUNDU. ZDROJ: VLASTNÍ MĚŘENÍ



OBRÁZEK 9 - ÚSPĚŠNOST SPOJENÍ VYJÁDŘENÁ V PROCENTECH PRO 1500 HOVORŮ ZA SEKUNDU

Tento test slouží pouze jako ukázka toho, jak se zachová ústředna, pakliže na ní bude kladeno příliš mnoho požadavků, což by mohlo simulovat například DoS útok. Z grafu je patrné, že 1500 hovorů za sekundu je příliš a CPU již nestíhá obsluhovat všechny požadavky. Zde se již projevují výrazné rozdíly mezi jednotlivými protokoly. Tento počet hovorů se již blíží i k limitu použité 100 Mb/s síťové karty. Největší propad je pozorovatelný u IPv6 sítě. U těchto sítí je totiž pracováno s delšími adresami, což se může projevit vyšší zátěži na procesor. Další příčinou může být větší velikost paketů, které pak hůře procházejí skrze vytížené linky (větší náchylnost na porušení). Hybridní sítě jsou umístěny uprostřed díky použití protokolu IPv4. Jelikož je nutný překlad, tak z tohoto grafu vyplývá, že limitem není procesor ale síťové rozhraní.



OBRÁZEK 10 - PRŮMĚRNÉ ZPOŽDĚNÍ PŘI ZPRACOVÁNÍ POŽADAVKŮ PRO 1500 HOVORŮ ZA SEKUNDU

Nejlepších výsledků dosahuje IPv4 síť, což je ve většině testů očekávané. IPv6 síť má podstatně větší zpoždění, než hybridní. Příčinou je nedostatečná propustnost síťového rozhraní.

8.5.4 LINPHONE

Praktická část bohužel nedopadla pro ústřednu Kamailio pozitivně. Ačkoliv předchozí testy prověřili signalizaci ve všech podmínkách, RTP protokol byl vyzkoušen až při použití UA Linphone. Samotný hovor bylo možné uskutečnit pouze ve spojení IPv4, pakliže byla podpora IPv6 vypnuta. Při zapnutí IPv6 byly funkční hovory pouze mezi IPv6 stanicemi, v ostatních případech byla funkční pouhá signalizace (s výjimkou kombinace IPv4 UAC a IPv6 UAS, kde nebyla funkční ani signalizace).

Problém spočívá v tom, že ústředna slouží pouze ke zpracování signalizace, u samotných hovorů pak počítá s přímým spojením. K dispozici je ovšem režim, který by měl umožnit i směrování RTP dat. Toho má být zajištěno například pomocí RTPproxy (testována verze 1.2.0), která sice podporuje protokoly IPv6 a IPv4, bohužel není popsán způsob jak sestavit most (bridge) mezi těmito sítěmi (popsány jsou pouze konfigurace IPv4 x IPv4 a IPv6 x IPv6, IPv4 x IPv6 chybí). Funkčnost tedy není 100% vyloučena, protože může existovat jiný RTP proxy server, který by tento nedostatek vyřešil.

8.5.5 PJSIP

Při použití tohoto nástroje byly samotné hovory v podobě RTP dat posílány přímou cestou, tedy bez účasti ústředny. Ústředna se podílela pouze na prvotním spojení, ukončení a zpracovávala pouze SIP požadavky. Jelikož SIP data jsou v případě VoIP telefonie využívány jenom při změnách, bylo jich tak malé množství z kterého nelze vyvodit jakýkoliv závěr.

8.6 PBXNSIP

8.6.1 SIPp

Jak již bylo řešeno výše, ústředna pbxnsip je založena na formě B2BUA, s tím souvisí jeden hlavní problém. Jelikož se pro testovací UAC chová jako odpovídající UAS, nebylo možné změřit jakékoliv reakce.

Naměřené výsledky by nemohli být rovnocenné, jelikož Kamailio využívá proxy serveru a pbxnsip B2BUA, náročnost by tedy v případě pbxnsip byla podstatně vyšší. Pakliže nebylo možné otestování pomocí SIPp, byl použit PJSIP, který se ukázal pro tuto ústřednu vhodnější.

8.6.2 LINPHONE

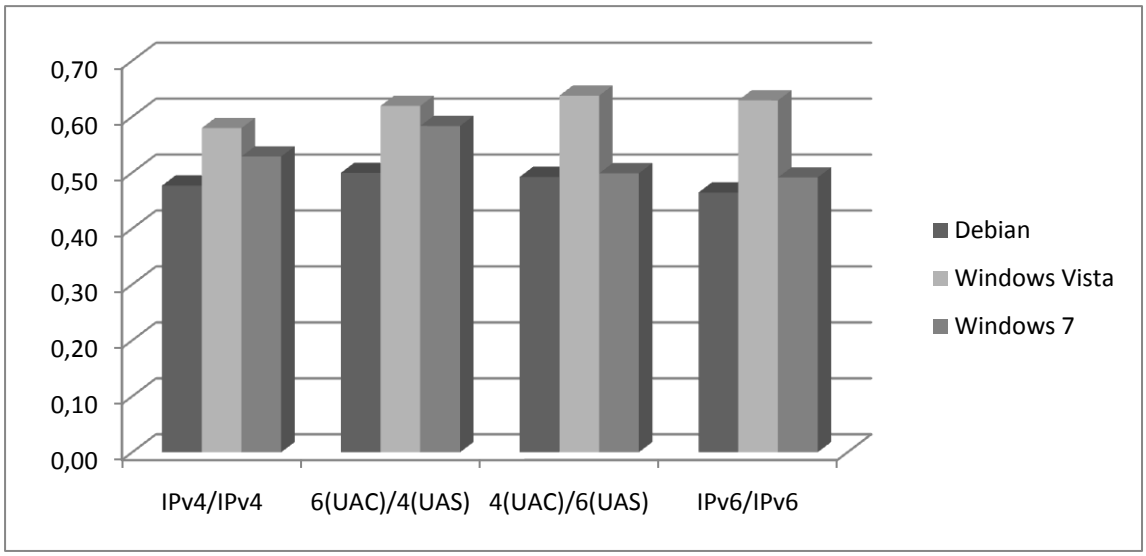
V praktickém využití je na tom pbxnsip podstatně lépe, všechny možné a testované možnosti byly funkční. Přenos hlasu tedy fungoval v následujících sítích: IPv4 x IPv4, IPv4 x IPv6 a IPv6 x IPv6. Veškerá komunikace (SIP + RTP) byly přenášeny skrze ústřednu. Při používání Linphone s ústřednou pbxnsip nebyl nalezen žádný problém.

8.6.3 PJSIP

Pomocí PJSIP bylo proměřena pbxnsip ústředna na třech operačních systémech. Testovány byly následující operační systémy ve standardní instalaci: Debian 5.02, Windows Vista Home Premium 64b, Windows 7 Ultimate RC 64b.

	Jitter - průměrná hodnota v ms		
	Debian	**Windows Vista**	**Windows 7**
IPv4/IPv4	0,48	0,58	0,53
6(UAC)/4(UAS)	0,50	0,62	0,58
4(UAC)/6(UAS)	0,49	0,64	0,50
IPv6/IPv6	0,46	0,63	0,49

TABULKA 7 - PJSIP/PBXNSIP SROVNÁNÍ OS. ZDROJ: VLASTNÍ MĚŘENÍ



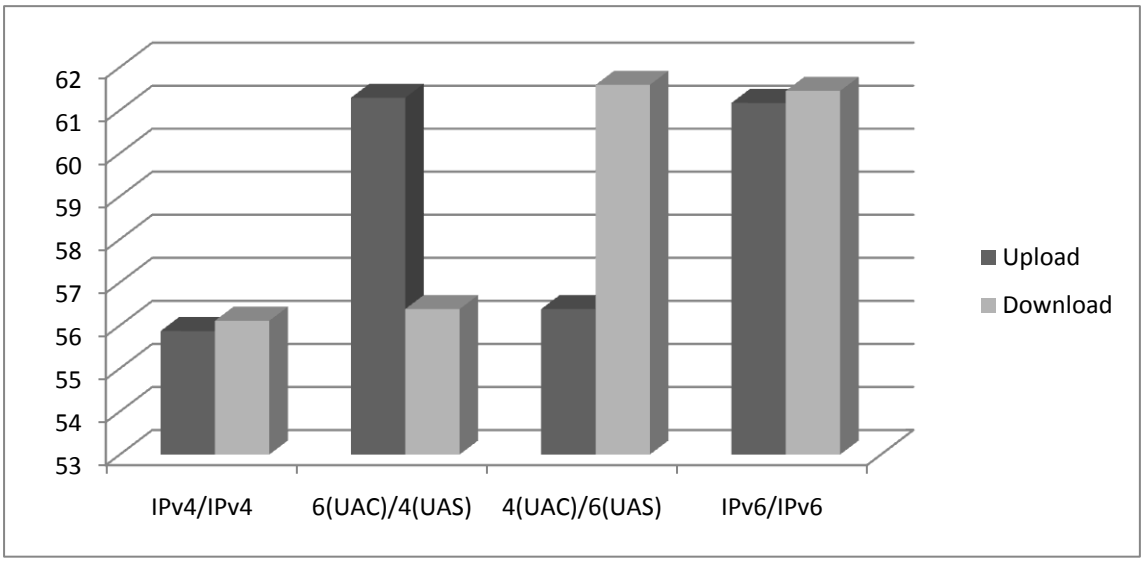
OBRÁZEK 11 - PJSIP/PBXNSIP SROVNÁNÍ OS

Jak je z výsledků vidět, mezi jednotlivými operačními systémy je odstup, který je podobný ve všech protokolech. Podle této tabulky je vidět, že všechny systémy mají oba protokoly velmi dobře zvládnuté. Jednotlivé rozdíly jsou dány optimalizacemi samotných operačních systémů. Zatímco zatížení Debianu bylo okolo 9%, jeho výsledky jsou nejlepší. Operační systém Windows Vista je znám vyššími systémovými nároky, což se projevilo na výsledcích, při kterých byl procesor využíván na 7%. Nejlépe na tom jsou Windows 7, které při zátěži 5% dosahovali výsledků podobných výsledkům Debianu.

Kromě těchto výsledků byl dále změřen datový objem nutný pro provedení 30 hovorů s délkou 3 minut. Výsledky jsou shrnuty v následujícím grafu a tabulce:

	Objem přenesených dat [MB]		Maximální rychlost [kB/s]	
	upload	download	upload	download
IPv4/IPv4	55,87	56,11	354,86	356,28
6(UAC)/4(UAS)	61,29	56,38	369,1	339,4
4(UAC)/6(UAS)	56,38	61,59	338,26	370,95
IPv6/IPv6	61,17	61,45	368,57	370,71

TABULKA 8 - OBJEM PŘENESENÝCH DAT PRO RŮZNÉ PROTOKOLY. ZDROJ: VLASTNÍ MĚŘENÍ



OBRÁZEK 12 - OBJEM PŘENESENÝCH DAT PRO RŮZNÉ PROTOKOLY

Naměřené výsledky jednoznačně hovoří ve prospěch IPv4 protokolu, který má nejnižší režii při přenosu. Z grafů je patrné, že protokol IPv6 má o cca 9,5% vyšší nároky na datový tok.

8.6.4 PJSIP – DEBIAN 5.02

Test byl prováděn na operačním systému Debian s použitím ústředny pbxnsip. Pro testování byl použit PJSIP a vnStat. Důležité výsledky testů jsou shrnuty v následující tabulce:

	Objem přenesených dat [MB]		Jitter [MS]	
	hovor	hovor + IP	průměr	max
IPv4/IPv4	1,36	1,70	0,48	13,64
6(UAC)/4(UAS)	1,35	1,69	0,50	20,48
4(UAC)/6(UAS)	1,36	1,70	0,49	6,71
IPv6/IPv6	1,35	1,69	0,46	12,57

TABULKA 9 - PJSIP/DEBIAN 5.02. ZDROJ: VLASTNÍ MĚŘENÍ

8.6.5 PJSIP – Windows Vista

Tento test je podobný tomu předchozímu, rozdílem je použitý operační systém. V tomto případě byl použit operační systém Windows Vista. Důležité výsledky testů jsou shrnuty v následující tabulce:

	Objem přenesených dat [MB]		Jitter [MS]	
	hovor	**hovor + IP**	**průměr**	**max**
IPv4/IPv4	1,35	1,69	0,58	23,60
6(UAC)/4(UAS)	1,35	1,69	0,62	26,34
4(UAC)/6(UAS)	1,35	1,69	0,64	26,54
IPv6/IPv6	1,35	1,69	0,63	27,18

Tabulka 10 - PJSIP/Windows Vista. Zdroj: vlastní měření

8.6.6 PJSIP – Windows 7

Poslední test byl prováděn na operačním systému Windows 7. Důležité výsledky testů jsou shrnuty v následující tabulce:

	Objem přenesených dat [MB]		Jitter [MS]	
	hovor	**hovor + IP**	**průměr**	**max**
IPv4/IPv4	1,36	1,70	0,53	26,08
6(UAC)/4(UAS)	1,35	1,69	0,58	27,89
4(UAC)/6(UAS)	1,35	1,69	0,50	28,27
IPv6/IPv6	1,35	1,69	0,49	32,36

Tabulka 11 - PJSIP/Windows 7. Zdroj: vlastní měření

8.7 Souhrn

Jak je z některých testů vidět, výkonnostní převahu mají sítě ve kterých je využíván pouze jeden protokol. Převahu má protokol IPv4, který je následován jeho novější podobou a to IPv6 protokolem.

V případě použití hybridního spojení je vždy nutné zajistit aktivní prvek, který bude na obou sítích komunikovat a překládat rámce mezi těmito sítěmi. Tímto prvkem může být RTP proxy, B2BUA či jiná forma překladače (translator). To je také příčinou, proč dochází k většímu zpoždění při spojení a vyšší zátěži ústředny (která minimálně pro SIP protokol hraje roli překladače). Nároky v případě signalizace nejsou nikterak vysoké. Problém může být u překladu RTP paketů, které jsou náročnější (podstatně větší množství) jak na zpracování procesorem, tak síťové připojení. Praktická část

ukázala, že by tyto nároky mohli být v případě IPv6 protokolu vyšší o cca 10%. U hybridního spojení je nutné přičíst ještě prostředky pro překlad.

Praktické využití testovaných ústředen shrnuje následující tabulka:

	IPv4 x IPv4	IPv4 x IPv6	IPv6 x IPv6
Debian – Kamailio	**Částečně**[1)]	**Ne**[2)]	**Částečně**[3)]
Debian – pbxnsip	**Ano**	**Ano**	**Ano**
Windows Vista – pbxnsip	**Ano**	**Ano**	**Ano**
Windows 7 RC - pbxnsip	**Ano**	**Ano**	**Ano**

TABULKA 12 - PRAKTICKÁ POUŽITELNOST S APLIKACÍ LINPHONE. ZDROJ: VLASTNÍ MĚŘENÍ

[1)] Ve výchozím nastavení, kdy funguje IPv4 je spojení funkční včetně přenosu hovoru mezi IPv4 účastníky. V případě povolení IPv6 funguje pouze signalizace - SIP. RTP požadavky ústředna nezpracuje.
[2)] Funkční je pouze signalizace v případě IPv6 UAC a IPv4 UAS. U opačné verze není funkční ani signalizace. Komunikace opět končí na straně ústředny.
[3)] V případě zapnutí IPv6 podpory je plně funkční pouze IPv6 spojení, v ostatních případech funguje pouze signalizace.

Z tabulky je tedy patrné, že Kamailio si poradí pouze při používání jednoho IP protokolu a k provozu v hybridním režimu potřebuje příslušnou RTP proxy. Samotná ústředna je tedy v hybridní síti prozatím nepoužitelná.

Ústřednu pbxnsip sice nebylo možné změřit v testech SIPp, ale v praktickém testu obstála výborně. Stejně tak testování pomocí PJSIP dopadlo pro 30 hovorů bez potíží. Veškeré ovládání je v podobě přehledného webového rozhraní, které je pro všechny OS stejné. Správce tak může ovládat ústřednu na jakémkoliv OS (nemusí se učit rozdíly v konfiguraci). Režim B2BUA má své výhody i nevýhody. Využití v hybridní síti je tedy použitelné. Jedinou nevýhodou může být cena při nákupu této ústředny a uzavřenost, která snižuje možnosti ladění chyb.

Testovací nástroj SIPp ještě není dokonalý ale na základní testy je velice užitečný. Mezi nevýhody lze zařadit problémy s podporou RTP přenosů v případě IPv6 protokolu. Jak je výše vidět, problémy mohou mít i samotné protokoly.

PJSIP má lepší podporu IPv6 a RTP protokolu, na druhou stranu má problémy s vyššími požadavky na náročné testování (maximální počet hovorů je 32). K dispozici je optimalizovaný nástroj pro testování SIP, ten ovšem neumí IPv6 protokol.

Aplikace Linphone sloužící k telefonování dokázala přenášet hovor na obou IP protokolech, díky podpoře více platforem ji nelze jinak než doporučit.

9 PROBLÉMY

Ačkoliv by se mohlo na první pohled zdát, že pro používání IPv6 protokolu stačí pouhé zadání IPv6 adresy a vše další už bude fungovat automaticky, opak je pravdou. Pro bezproblémový provoz IPv6 protokolu je zapotřebí splnění hned několika podmínek.

9.1 OPERAČNÍ SYSTÉM

Na podporu IPv6 protokolu musí být připraven především operační systém. V současné době jsou všechny běžně používané operační systémy s nativní podporou IPv6. Se staršími operačními systémy může nastat problém, je však možné že podpora lze dodatečně přidat. Mezi takový systém patří například oblíbené Windows XP. Pro operační systémy od společnosti Microsoft, které jsou starší než Windows XP podpora IPv6 neexistuje. V případě Linuxu je IPv6 podpora zahrnuta již od jádra 2.1.8 v experimentální podobě, finální podoba se objevila až v jádře 2.6.12. Postupy jak přidat podporu do operačního systému jsou podstatně složitější než u nativně podporovaných OS.

9.2 PODPORA SÍTĚ

Pakliže je požadována komunikace v rámci Internetu, je zapotřebí podpora ze strany poskytovatele a všech prvků, přes které do této sítě vstupujeme. Nevhodně nakonfigurovaný IPv4 směrovač tak může IPv6 pakety rovnou zahazovat, protože neví, co s nimi má dělat. V případě, že poskytovatel neposkytuje nativní IPv6 spojení, není vše ztraceno. Řešením může být například tunelování IPv6 paketů skrze IPv4 síť (Teredo, SixXs a další).

9.3 PODPORA APLIKACE

Dobře naprogramovaná aplikace může být nezávislá na použitém protokolu, v prostředí operačního systému Linux se k tomu používá služba getaddrinfo(). Častou praktikou ovšem bývá vynechání této služby a napsání aplikace na míru konkrétnímu protokolu, v takovém případě je pak nutné aplikaci přepsat pro protokol novější. Což

může být natolik náročné, že se toho výrobce vzdá, či za to může požadovat nějaký poplatek.

9.4 Adresování

V případě, že uživatel bude chtít použít lokální IPv6 adresu v síti Internet, tak ke spojení samozřejmě nedojde. IPv6 nabízí hned několik adres pro jedno rozhraní, což může být pro samotného uživatele velice matoucí. Řešení ovšem existuje ve službě getaddrinfo(), která by měla zaručit výběr vhodné adresy.

V případě zadávání adresy může dojít k dalším potížím kvůli zápisu. V IPv6 jsou používány jako oddělovače „:“, stejný znak je ovšem používán k oddělení adresy a portu jak v IPv4, tak v IPv6. Většina aplikací to tedy řeší tím, že IPv6 adresa je uzavřena hranatými závorkami []. Příkladem budiž [2001:db8::1] případně se specifikací portu [2001:db8::1]:5060.

Práce s IPv6 adresami nemusí být v aplikaci s podporou IPv6 vždy stoprocentní. Příkladem může být například pbxnsip, kde ve verzi 3.1.2.3120 (verze 3.3.1.3177 a 3.4.0.3201 fungují správně) nebylo možné vkládat IPv6 adresy do Access listu. Zpracování adresy bylo sice přijato, ale její reprezentace v seznamu neodpovídala realitě. Další problém má i Kamailio, kde není možné vložit IPv6 adresu pro daný kontakt ručně. Pro tento účel se musí zařízení pravidelně registrovat, aby ústředna věděla jeho adresu (i přestože je neměnná). Posledním případem je i testovací nástroj SIPp, kde adresy fungují správně s použitím hranatých závorek, ovšem prezentace bez závorek (jako například 2001:db8::1:5060) uvnitř programu může být pro neznalého uživatele matoucí a nežádoucí.

Konkrétní adresy ovšem často používány nebudou, jelikož jejich zapamatování a přepis by byl zbytečně složitý a mohl tak vnášet chyby. Tento problém je řešen pomocí DNS (Domain Name Server).

10 ZÁVĚR

Podle posledních předpovědí by měl být adresní prostor IPv4 vyčerpán přibližně na konci roku 2011. Do té doby se bude IPv6 rozvíjet velmi pomalu, podobným tempem jako nyní. Mnoho společností se do přechodu na IPv6 příliš nežene kvůli vysokým pořizovacím nákladům za nové vybavení a příslušné školení. To raději investují finance do nákupu IPv4 adres, které by se mohli později nakupovat od uživatelů, kteří je dostali přiděleny a nevyužívají jejich výhod.

Z výsledků této práce je vidět, že v současné době není problém zprovoznit VoIP komunikaci v hybridní síti. Největším problémem může být výběr vhodné ústředny, jelikož je značně omezen. Zatímco celkově je jich k dispozici v řádu desítek, s podporou IPv6 se počítá v řádu jednotek. Zajímavé je, že Asterisk jakožto nejpoužívanější SIP ústředna stále oficiálně IPv6 nepodporuje. Přitom byl před dvěma lety představen funkční port AsteriskIPv6, který komunikaci v sítích IPv4 a IPv6 umožňoval. Problém tedy nebude v náročnosti přidání IPv6 podpory, ale příčinou bude spíše malá poptávka ze strany zákazníků. V případě UA je situace velmi podobná ústřednám.

Další příčinou může být certifikace ze strany IPv6 protokolu, který totiž s nasazením SIPu počítá a jsou pro něj připraveny podmínky, které SIP IPv6 aplikace musí splnit, aby mohla použít příslušné logo. Je tedy možné, že již některé aplikace umožňují využití IPv6, ale veřejně to nedávají najevo kvůli nedostatkům z pohledu certifikace.

Z pohledu hardware je situace ještě horší, v současné době jsou k dispozici pouze IP kamery (VIVOTEK IP7160). Na žádné HW telefony s podporou IPv6 jsem v českých obchodech nenarazil.

Široké podpory IPv6 se pravděpodobně dočkáme až za pár let, pakliže tedy nepřijde na trh technologie či služba, která by striktně vyžadovala IPv6 a byla zajímavá pro velké množství uživatelů.

Pro VoIP provozovatele znamená příchod IPv6 nutnost veřejné IPv4 adresy a dostatečné konektivity pro překlad RTP paketů.

ZDROJE

1. Satrapa, Pavel: *Internetový protokol IPv6*, CZ.NIC, Praha, 2008, ISBN 978-80-904248-0-7
2. Minoli, Daniel: *Voice Over IPv6: architectures for next generation VoIP networks*, Elsevier Inc., United States of America, 2006, ISBN 978-0-7506-8206-0
3. Wikipedie: Otevřená encyklopedie: *Internet Protocol* [online]. 2009 [citováno 29. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Internet_Protocol>
4. Wikipedie: Otevřená encyklopedie: *IPv6* [online]. 2009 [citováno 29. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IPv6>
5. Wikipedie: Otevřená encyklopedie: *Session Initiation Protocol* [online]. 2009 [citováno 6. 08. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Session_Initiation_Protocol>
6. Wikipedie: Otevřená encyklopedie: *Voice over Internet Protocol* [online]. 2009 [citováno 6. 08. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Voip>
7. Wikipedie: Otevřená encyklopedie: *Telefonie* [online]. 2009 [citováno 1. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Telefonie>
8. Wikipedie: Otevřená encyklopedie: *Telekomunikace* [online]. 2009 [citováno 3. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Telekomunikace>
9. Wikipedie: Otevřená encyklopedie: *Vzorkování* [online]. 2009 [citováno 3. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Vzorkov%C3%A1n%C3%AD>
10. Wikipedie: Otevřená encyklopedie: *Kvantování (signál)* [online]. 2009 [citováno 5. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Kvantov%C3%A1n%C3%AD_(sign%C3%A1l)>
11. Wikipedie: Otevřená encyklopedie: *Telefon* [online]. 2009 [citováno 3. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Telefon>
12. Wikipedie: Otevřená encyklopedie: *Kodek* [online]. 2009 [citováno 3. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Kodek>
13. Wikipedie: Otevřená encyklopedie: *Shannonův teorém* [online]. 2009 [citováno 29. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Shannon%C5%AFv_teor%C3%A9m>
14. Wikipedia, The Free Encyclopedia: *Session Initiation Protocol* [online]. 2009 [citováno 7. 08. 2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Session_Initiation_Protocol>
15. Wikipedia, The Free Encyclopedia: *Voice over Internet Protocol* [online]. 2009 [citováno 5. 08. 2009]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Voip>
16. Wikipedia, The Free Encyclopedia: *H.323* [online]. 2009 [citováno 1. 08. 2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/H323>

17. PLÁNIČKA, Marek: *Úvod do protokolu SIP (1) - Základní kameny* [online]. 2009 [citováno 6. 08. 2009]. Dostupný z WWW: <http://www.telegro.cz/2009/05/05/uvod-do-protokolu-sip-1-zakladni-kameny>
18. CESNET: *SIP* [online]. 2007 [citováno 3. 08. 2009]. Dostupný z WWW: <https://sip.cesnet.cz/cs/protokoly/sip>
19. PUŽMANOVÁ, Rita: *Protokol SIP ve zkratce* [online]. 2004 [citováno 6. 08. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/protokol-sip-ve-zkratce/>
20. IT POINT: *TEORIE A PRAXE IP TELEFONIE* [online]. 2004 [citováno 6. 08. 2009]. Dostupný z WWW: <http://www.itpoint.cz/voip/>
21. PETŘÍK, Stanislav: *Signalizace v sítích VoIP* [online]. 2006 [citováno 6. 07. 2009]. Dostupný z WWW: <http://www.elner.sk/view.php?cisloclanku=2006010601>
22. PETERKA, Jiří: *Digitalizace hlasu* [online]. 2000 [citováno 16. 07. 2009]. Dostupný z WWW: <http://www.earchiv.cz/a008s200/a008s203.php3>
23. Hewlett-Packard: *SIP Components* [online]. 2007 [citováno 15. 07. 2009]. Dostupný z WWW: <http://docs.hp.com/en/5992-1950/ch01s02.html>
24. IETF: *Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6)* [online]. 2006 [citováno 19. 07. 2009]. Dostupný z WWW: <http://tools.ietf.org/html/draft-gurbani-sipping-ipv6-sip-03>
25. SIPp: *SIPp reference documentation* [online]. 2009 [citováno 23. 07. 2009]. Dostupný z WWW: <http://sipp.sourceforge.net/doc3.0/reference.html>
26. BITTO, Ondřej: *Jak se volá přes Internet: protokoly H.323 a SIP* [online]. 2007 [citováno 25. 07. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-se-vola-pres-internet-protokoly-h-323-a-sip/>
27. SOLNICKÝ, Ivo: IP Telefonie – co to je a jak vlastně funguje? [online]. 2002 [citováno 2. 07. 2009]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=152&clanekID=165>
28. FATIMA, Ahmed: *A Comparison of Voice Technologies (VoIP, VoFR, and VoATM)* [online]. 2003 [citováno 17. 07. 2009]. Dostupný z WWW: <http://www.developer.com/voice/article.php/3112781>
29. Wikipedie: Otevřená encyklopedie: *IP adresa* [online]. 2009 [citováno 29. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IP_adresa>
30. Request for Comments: 4632: *Classless Inter-domain Routing (CIDR):The Internet Address Assignment and Aggregation Plan* [online]. 2006 [citováno 19. 07. 2009]. Dostupný z WWW: <http://www.rfc-editor.org/rfc/rfc4632.txt>
31. Wikipedie: Otevřená encyklopedie: *Jitter* [online]. 2009 [citováno 29. 07. 2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Jitter>

PŘÍLOHY

Přílohou k této práci jsou dvě média (DVD, CD).

Na přiloženém bootovatelném DVD médium, je operační systém Debian s příslušnými aplikacemi (pbxnsip, Kamailio, Wireshark, SIPp, htop, Linphone) a návody na jejich obsluhu.

CD médium obsahuje výsledky měření, aplikace používané v prostředí Windows, vytvořené návody a tuto práci v digitální podobě.