

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

diplomová práce

Management výkonnosti a optimalizace VoIP technologie

Vedoucí práce: Ing. Jan Tyrychtr, Ph.D.

Autor práce: Bc. Petr Holubovský

© PRAHA 2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petr Holubovský

Informatika

Název práce

Management výkonnosti a optimalizace VoIP technologie

Název anglicky

VoIP Performance Management and Optimization

Cíle práce

Diplomová práce je zaměřena na optimalizaci VoIP technologie. Hlavním cílem práce je vytvoření procesu optimalizace konfigurace VoIP. Dílčí cíle diplomové práce jsou:

- vytvořit kritickou literární rešerši k problematice VoIP,
- provést měření kvality hovorů realizovaných pomocí VoIP technologie,
- provést měření kvality přenosů VoIP pro jednotlivé typy kodeků,
- navrhnout proces zavedení VoIP technologie prostřednictvím procesního diagramu.

Metodika

Řešení dané problematiky diplomové práce je založeno na studiu odborných informačních zdrojů a jejich analýze. Teoretická část bude obsahovat popis technologie VoIP a protokolů nezbytných pro provoz VoIP, přehled používaných kodeků a metody měření kvality přenosu hlasu. V praktické části bude provedeno měření kvality přenosu hlasu vybranými metodami pro dané typy kodeků. Na základě změřených hodnot bude vytvořen proces konfigurace reálného nasazení VoIP technologie, který bude vytvořen prostřednictvím modelovacího standardu BPMN. V závěru diplomové práce bude provedena syntéza dosažených výsledků práce a formulovány doporučení pro podnikovou praxi.

Doporučený rozsah práce

60-80 stran

Klíčová slova

VoIP, Asterisk, QOS, IP telefonie, SIP, DHCP, management výkonnosti VoIP

Doporučené zdroje informací

AHMED, Adeel; MADANI, Habib; SIDDIQUI, Talal. VoIP Performance Management and Optimization. Cisco Press, 2010.

BAZALA, David. Telekomunikace & VoIP telefonie I. 1. vydání. Praha: BEN, 2006. 222 s. ISBN 80-7300-201-9

HARTPENGE, Bruce. Packet Guide to Voice over IP: A system administrator's guide to VoIP technologies. 1. vydání. O'Reilly Media, 2013. 242 s. ISBN 978-1449339678

MADSEN, Leif – MEGGELEN Jim Van – BRIANT Russel. Asterisk: The Definitive Guide. 3. vydání. O'Reilly Media, 2011. 738 s. ISBN 978-0-596-51734-2

RAJAVELSAMY, Rajadurai, et al. Performance evaluation of VoIP over 3G-WLAN interworking system. In: Wireless Communications and Networking Conference, 2005 IEEE. IEEE, 2005. p. 2312-2317.

VOZŇÁK, Miroslav. Voice over IP. 1. vydání. Ostrava: VŠB – Technická univerzita Ostrava, 2008. 176 s. ISBN 978-80-248-1828-3

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Jan Tyrychtr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2016

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně pod vedením Ing. Jana Tyrychtra, Ph.D. a uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Poděkování

Rád bych poděkovat svému vedoucímu diplomové práce Ing. Janu Tyrychtrovi, Ph.D. za odborné vedení, za pomoc a rady při zpracování této práce.

Anotace

Diplomová práce se zaměřuje na optimalizaci a výkonnost VoIP technologie. V práci jsou představeny teoretické základy IP telefonie a měření jejich kvality. Práce se primárně zabývá praktickým měřením kvality hovorů realizovaných pomocí VoIP technologie. K měření je využito softswitch Asterisk, různé typy IP telefonů a umělé degradace signálu zprostředkované softwarovým Linuxovým směrovačem. Na základě těchto měření je navržen procesní diagram reálného nasazení VoIP technologie.

Abstrakt

The diploma thesis focuses on the VoIP technology optimization and performance management. The diploma thesis presents the theoretical basis of IP telephony and measurement of its quality. The thesis primarily deals with practical measurements of VoIP calls quality. Asterisk softswitch, various types of IP phones and simulated degradation of signal using Linux software router are used for measurements. Procedural diagram of VoIP technology real deployment is designed based on these measurements.

Klíčová slova

VoIP, Asterisk, QoS, IP telefonie, SIP, DHCP, management výkonnosti VoIP

Key words

VoIP, Asterisk, QoS, IP telephony, SIP, DHCP, VoIP Performance Management

Obsah

1	Úvod.....	11
2	Cíle práce	12
3	Metodika práce	12
3.1	Metody pro měření kvality řeči - objektivní	12
3.2	Testovací metodika	13
3.2.1	Objektivní testy.....	13
3.3	Typické rušivé jevy v prostředí VoIP a jejich vliv na MOS	14
3.3.1	Výpadky signálu	14
3.3.2	Neharmonické zkreslení	14
3.4	R – faktor.....	14
3.4.1	Přepoččet R-faktoru na parametr MOS	15
3.5	BPMN	16
3.5.1	Prvky BPMN.....	16
4	Teoretická část	17
4.1	VoIP	17
4.1.1	Přehled	17
4.1.2	Součásti sítě VoIP.....	19
4.1.3	Funkce VoIP	20
4.2	VoIP protokoly.....	21
4.2.1	Signalizační protokoly	21
4.2.2	Transportní protokol	23
4.3	Doplňující nástroje	24
4.3.1	IP protokol	24
4.3.2	TCP protokol (Transmission Control Protocol).....	25
4.3.3	UDP protokol.....	27

4.3.4	ICMP protokol (Internet Control Message Protocol)	27
4.3.5	DHCP protokol (Dynamic Host Configuration Protokol)	28
4.4	Kodeky	28
4.4.1	Standardy kódování a dekodování	28
4.4.2	Nejpoužívanější kodeky	31
4.4.3	Výpočet šířky pásma	31
4.5	Převod hlasu na digitální signál	35
4.5.1	Dělení hlasu na bajty	36
4.6	Kvalita řeči ve VoIP	39
4.6.1	Definice kvality řeči	39
4.6.2	Měření kvality řeči	41
4.6.3	Měření kvality přenosu - subjektivní metody	42
4.6.4	Subjektivní testy	43
4.7	Softswitch Asterisk	43
4.7.1	Moduly	44
4.7.2	Struktura souborů	45
4.7.3	Dialplán	45
4.7.4	Hardware	46
4.8	QoS (Quality of Service)	46
4.8.1	Aplikace QoS	46
4.8.2	Úrovně QoS	47
5	Praktická část	48
5.1	Příprava laboratoře	48
5.1.1	Popis procesu přípravy laboratoře	52
5.2	Měření kvality přenosů VoIP	54
5.2.1	Měření	55

5.3	BPMN schéma nasazení VoIP technologie.....	58
6	Závěr	61
7	Použitá literatura	62
8	Přílohy.....	65
8.1	Ukázka měření	65
8.2	Image systému ústředny Asterisk.....	66

Seznam obrázků

4.4.1.	Součásti sítě VoIP [7]	19
4.4.2.	SIP paket [1]	22
4.4.3.	H.225 paket [1]	22
4.4.4.	SCCP paket [1]	23
4.4.5.	RTP paket [1].....	23
4.4.6.	RTCP paket [1]	24
4.4.7.	Protokol TCP přenáší data pomocí portů [6].....	26
4.4.8.	Zpracování hlasu na straně odesílatele [4].....	32
4.4.9.	Jitter a jeho vliv na odstup mezi pakety [4].....	34
4.4.10.	Ukázka průběhu rozptylu zpoždění [4].....	34
4.4.11.	Zpracování na straně příjemce [4]	35
4.4.12.	Analogová a digitální vlnová křivka [3].....	35
4.4.13.	Aliasing [3]	36
4.4.14.	Převzorkování [3]	37
4.4.15.	Vzorkování [3].....	37
4.4.16.	Kvantizace [3].....	38
4.4.17.	PBX architektura vs. Asterisk [2].....	44
5.1.	Schéma zapojení laboratoře	49
5.2.	Schéma IP adres laboratoře.....	50
5.3.	Příprava laboratoře.....	51
5.4.	Stav připojených SIP účtů.....	54
5.5.	Průměrně dosažený R-Factor.....	57

5.6. Průměrně dosažené MOS scóre	58
5.7. BPMN schéma implementace VoIP	57
8.1. Ukázka měření	65

Seznam tabulek

4.4.1. Kodéry a jejich typy [4]	31
4.4.2. Hodnoty stupnice MOS [10]	40
4.4.3. Maximální MOS skóre jednotlivých kodeků [10]	41
5.1. Podporované kodeky	55
5.2. Originální signál	56
5.3. 1% ztrátovost paketů	56
5.4. 2,5% ztrátovost paketů	56
5.5. 5% ztrátovost paketů	56
5.6. 10% ztrátovost paketů	56
5.7. 15% ztrátovost paketů	57
5.8. 20% ztrátovost paketů	57
5.9. Průměrné hodnoty MOS a R-faktor	57
5.10. Výsledné pořadí kodeků	58

1 Úvod

S rostoucím rozvojem datových sítí stále více dochází k přechodu přenosu hlasu z analogových zařízení na digitální. Technologie VoIP využívá datových sítí pro přenos hovorů, telekonferencí apod. a klade nároky na srozumitelné a spolehlivé telefonní spojení (tzv. kvalitu služby). Služba VoIP využívá nejrůznější kódovací a dekodovací algoritmy (kodeky), které slouží k úspoře šířky pásma a zároveň mají za úkol zachovat dostatečnou kvalitu přenášeného hlasu.

Nalezení optimálního nastavení k dosažení nejlepšího zatížené sítě a kvality přenášeného hlasu je komplikované a nese s sebou řadu problémů, na které musí být brán zřetel. Ať už jde o nasazení několika zařízení v malém podniku, nebo rozsáhlé řešení v rámci lokálního poskytovatele služeb.

Tato diplomová práce se zabývá optimalizací nasazení VoIP technologie a nalezení optimálního poměru zatížení přenosové datové sítě a kvality přeneseného hlasu.

První část se zabývá teoretickými základy VoIP technologie a jakým způsobem dochází k přenosu hlasu po IP síti. Obsahuje popis VoIP protokolů, jak signalizačních, tak transportních a popis doplňujících nástrojů, které s telefonováním po datové síti souvisejí - jako např. IP, TCP, UDP a DHCP protokolů. Jsou popsány jednotlivé standardizované kodeky a metody měření přenosu hlasu objektivních i subjektivních, a to prostřednictvím kritické rešerše odborných zdrojů.

Druhá část se zabývá praktickým řešením managementu výkonnosti VoIP technologie a optimalizací jejího nasazení. Testovací prostředí je zrealizováno pomocí softwarové ústředny Asterisk, jako koncová zařízení jsou k dispozici IP telefony značky Grandstream, Well a Siemens.

2 Cíle práce

Diplomová práce se zabývá optimalizací technologií využívajících protokolu Voice over Internet Protocol (VoIP). Hlavním cílem práce je vytvoření procesu optimalizace konfigurace VoIP technologie. Dílčí cíle diplomové práce jsou:

- vytvořit kritickou literární rešerši k problematice VoIP technologie,
- provést měření kvality přenosů VoIP pro jednotlivé typy kodeků,
- navrhnout proces zavedení VoIP technologie prostřednictvím procesního diagramu.

3 Metodika práce

Řešení dané problematiky diplomové práce je založeno na studiu odborných informačních zdrojů a jejich analýze. Teoretická část obsahuje popis technologie VoIP a protokolů nezbytných pro provoz VoIP, přehled používaných kodeků a metody měření kvality přenosu hlasu. V praktické části je provedeno měření kvality přenosu hlasu vybranými metodami pro dané typy kodeků. Na základě změřených hodnot je vytvořen proces konfigurace reálného nasazení VoIP technologie, který je vypracován prostřednictvím modelovacího standardu BPMN. V závěru diplomové práce je pak provedena syntéza dosažených výsledků práce a formulovány doporučení pro podnikovou praxi.

3.1 Metody pro měření kvality řeči - objektivní

Objektivní metody jsou matematické algoritmy, které se snaží předpovídat subjektivní hodnocení signálu tím, že zkoumají průběh digitalizovaného poslechového signálu. Objektivní metody se dělí na:

- Intrusivní
- Neintrusivní

Podle toho, zda metoda vyžaduje nezkreslený originální signál, se dělí tyto metody na intrusivní a neintrusivní. Požadováním nezkresleného originálního signálu se sice omezuje rozsah využití metody, a to v případech, kdy neexistuje přístup ke zdroji. Na druhou stranu toto umožňuje postihnout jevů (např. zpoždění signálu), které není možné postihnout v neintrusivních metodách. Nasazení intrusivních metod může být problematické a může narušovat provoz testovaného systému. Z intrusivních metod se jedná například o PAMS, PSQM, PESQ atd. [10].

Zástupci neintrusivních metod jsou například ANIQUE, LCQA, 3SQM. Tyto metody jsou využitelné na straně přijímače telekomunikačního řetězce a slouží pro monitoring reálného provozu systému. V případě neintrusivních metod se můžeme setkat s přístupem, kdy kvalita nezávisí na signálu procházejícího telekomunikačním kanálem, ale odhaduje se pouze na základě síťových parametrů přenášeného řetězce. Jednou z takových metod je metoda VQMON.

Korelační koeficient vyjadřuje míru korelace mezi objektivními a subjektivními metodami. Tento koeficient je definován Pearsonovým vztahem (1) a může nabývat hodnot z intervalu 0 – 1.

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (1)$$

Koeficient y_i představuje výsledky objektivní metody a x_i představuje výsledky subjektivní metody u sobě si odpovídajících měření [10].

3.2 Testovací metodika

Realizace testování jak objektivních, tak i subjektivních metod je podmíněna důkladnou přípravou. Je výhodné vytvořit průnik podmínek pro objektivní a subjektivní testy a připravit si testovací vzorky (poslechové sekvence) tak, aby bylo možné realizovat oba typy testování. Tím je docíleno možnosti provést rozsáhlé objektivní testování, které je možné následně ověřit menším subjektivním testem [10].

3.2.1 Objektivní testy

Doporučení ITU-T P.563 definuje vzorkový signál pro metodu 3SQM jako 16-bit PCM signál, který má vzorkovací frekvenci 8 kHz. Signály, které mají vyšší vzorkovací frekvenci, musí být upraveny na frekvenci 8 kHz. Délka vzorku může být od 3 do 20 sekund. Z toho mluva by měla být zastoupena z 25 až 75 %.

Doporučení ITU-T P.862 - viz. [13] - definuje všechna kritéria, která má splnit testovaný signál. Jedním z nejdůležitějších je, že testovaný signál musí mít charakter signálu, který je běžně přenášen komunikační sítí. Testovací signál musí být složen z úseků mluvy s délkou od 1 do 3 sekund. Tyto mluvené úseky musí být odděleny pomlčkou s celkovou délkou od 40 do 80 % z testovaného signálu. Většinou se využívají testovací signály, které jsou

složeny ze dvou nebo tří úseků mluvy s celkovou délkou cca 8 sekund. Lze ale použít i věty, které jsou až 20 sekund dlouhé [10].

3.3 Typické rušivé jevy v prostředí VoIP a jejich vliv na MOS

Nástup VoIP prostředí přineslo zcela specifické typy rušení, které v prostředí POTS nemají žádnou analogii. Krom klasických rušivých jevů, zastoupených šumem a harmonickým zkreslením, lze potkat jevy, jako jsou například diskontinuita fáze signálu, neharmonické zkreslení nebo výpadky v signálu. Pro lepší představu je zde vysvětleno, jaký mají vliv na kvalitu řečového signálu dva typické druhy rušení [10].

3.3.1 Výpadky signálu

Výpadky signálu jsou jedním z typických jevů VoIP prostředí. V praxi se míra četnosti výpadků signálu pohybuje v rozmezí jednotek procent, až po extrémní hodnoty v řádu desítek procent. Toto je typická degradace řečového signálu. Vztaženo na hlásky, během kterých došlo k výpadku, je přenesený signál až nesrozumitelný [10].

3.3.2 Neharmonické zkreslení

„K neharmonickému zkreslení může dojít např. při saturaci řečového signálu. Parametr saturace udává poměr úrovní saturovaného a původního signálu“ [10].

3.4 R – faktor

Je známo mnoho objektivních faktorů ovlivňujících kvalitu volání skrze VoIP. Některé tyto faktory (packet delay variation, packet loss) je schopen daný softwarový analyzátor určit na základě měření. Nicméně tyto dané měřicí techniky nemají vypovídací hodnotu k subjektivnímu vnímání kvality hovoru uživatelem. „Metrika nazvaná R-faktor používá předpis pro zohlednění, jak uživatelského vnímání, tak celkového efektu znehodnocení zařízením pro dosažení numerického vyjádření hlasové kvality“ [10].

Doporučení G.107 [16] popisuje R-faktor a výpočetní model, který je znám jako E-model. Ten je osvědčeným prostředkem pro plánování přenosu, pro zhodnocení kombinovaných účinků variant různých přenosových parametrů, které ovlivňují kvalitu hovoru 3.1 kHz telefonie. Hlavním výstupem E-modelu je hodnotící faktor R (Rating Factor R) [10].

Doporučení G.107 popisuje jednotlivé komponenty pro výpočet R-faktoru. Vlastní výpočet vychází z E-modelu a je kombinací všech přenosových parametrů, které jsou důležité pro zvažované spojení. R-faktor se skládá z [15]:

$$R = R_O - I_S - I_D - I_{E-EFF} + A \quad (2)$$

kde

- R_O - základní koeficient signál-šum
- I_S - součet všech znehodnocení, která mohou nastat současně s přenosem hlasu
- I_D - faktor znehodnocení reprezentující všechny znehodnocení způsobené zpožděním signálů hlasu
- I_{E-EFF} - paketová ztráta, Efektivní faktor znehodnocení zařízením (Effective Equipment Impairment Factor)
- A - faktor zvýhodnění (přípustný rozsah 0 - 20)

3.4.1 Přepočítání R-faktoru na parametr MOS

Následuje jeden z možných způsobů, jak převést parametr R-faktor na parametr MOS [17].

$$MOS = \begin{cases} R \leq 6.5 & 1 \\ 6.5 \leq R \leq 100 & 1 - \frac{7}{1000} \cdot R + \frac{7}{6250} \cdot R^2 - \frac{7}{1000000} \cdot R^3 \\ R \leq 100 & 4.5 \end{cases} \quad (3)$$

Tento vzorec může být invertován v rozsahu $6.5 < R < 100$ pro výpočet R-faktoru z parametru MOS prostřednictvím následujícího vztahu:

$$R = \frac{20}{3} \cdot \left(8 - \sqrt{226} \cdot \cos\left(h + \frac{\pi}{3}\right) \right) \quad (4)$$

Předpoklady:

$$h = \frac{1}{3} \cdot \arctan 2\left(18566 - 6750 \cdot MOS, 15\sqrt{-903522 + 1113960 \cdot MOS - 202500 \cdot MOS^2}\right)$$

$$\arctan 2(x, y) = \begin{cases} \arctan(y/x) & \text{for } x \geq 0 \\ \pi - \arctan(y/-x) & \text{for } x < 0 \end{cases} \quad (5)$$

3.5 BPMN

Primárním cílem Business Process Model and Notation (BPMN) je poskytnout zápis procesu, který je snadno pochopitelný pro všechny účastníky životního cyklu procesu (technické vývojáře, business analytiku, analytiku monitorující procesy atd.). Slouží pro grafické modelování procesů za pomoci grafických objektů a pravidel. Vlastní realizace schémat je provedena v programu Yaoqiang, a to z důvodu podpory výstupů ve formátu png [18].

3.5.1 Prvky BPMN

Prostřednictvím BPMN vznikají diagramy, tyto diagramy jsou složeny z dílčích grafických prvků. Základní členění prvků BPMN je do 5 kategorií [18]:

- Tokové objekty (Flow objects)
 - Události (Events)
 - Aktivity / činnosti (Activities)
 - Brány (Gateways)
- Data
 - Datové objekty (Data objects)
 - Datové vstupy (Data inputs)
 - Datové výstupy (Data outputs)
 - Datové sklady / databáze (Data stores)
- Spojovací objekty (Connecting objects)
 - Sekvenční tok (Sequence flow)
 - Tok zpráv (Message flow)
 - Asociace (Association)
- Plavecké dráhy / kontexty (Swim lanes)
 - Bazény / kontext (Pool)
 - Dráhy / oddíly kontextu (Lane)
- Artefakty (Artefacts)
 - Skupiny (Group)
 - Anotace (Text annotation)

4 Teoretická část

V této části práce jsou nastíněny základní principy Voice over IP, VoIP protokoly, kodeky, převodu hlasu na digitální signál, kvality hlasu ve VoIP a pobočkovou ústřednou Asterisk.

4.1 VoIP

Voice over IP je technologie, která významně ovlivnila oblast telekomunikací, a pokud bychom hledali podobné milníky evoluce telefonie, pak lze IP telefonii postavit na stejnou úroveň jako digitalizaci. Voice over IP (VoIP se také označuje jako IP telefonie. Jednoduše řečeno se jedná o přenos hlasu po síti IP. Základní odlišnosti souvisejí s koncovými body, které jsou použity. Tradiční analogové a digitální okruhy v síti VoIP se připojují k síti IP, většinou prostřednictvím brány. Existují koncové body, které defaultně komunikují prostřednictvím protokolu IP.

V protokolu VoIP dochází ke směrování hlasové konverzace po IP síti včetně internetu. Díky tomu mohou firmy výrazně ušetřit, protože pro přenos hlasového hovoru i dat může být využita jejich stávající síť IP. Pokud firma nevyužívá kapacitu své sítě na maximum, může nevyužitou šířku pásma poskytnout pro přenos hlasu bez nutnosti investice do rozšíření datové sítě [4,7].

4.1.1 Přehled

Sítě IP využívající VoIP technologie poskytují hlasové aplikace jako jsou například telekonference, telefonování a zaslání rychlých zpráv. VoIP nedefinuje pouze způsob přenosu volání přes síť, ale zahrnuje také digitalizaci a paketizaci hlasu. Jednotlivé normy VoIP nabízejí možnost využití dalších funkcí (hlasová pošta, kontaktní centra, pokročilé směrování hovorů atd.).

Služby VoIP převedou hlas na digitální signál, který je pak přenášen přes síť založenou na protokolu IP. Pokud je voláno na standardní telefonní číslo, je signál před dosažením cíle převeden na standardní telefonní signál. Technologie VoIP umožňuje uskutečňovat volání z telefonu VoIP, ze standardního analogového telefonního přístroje připojeného přes zvláštní adaptér nebo přímo z počítače. Služby VoIP je možno navíc používat prostřednictvím bezdrátových přístupových míst (tzv. hot spotů) na místech, jako jsou letiště, parky a kavárny, umožňujících připojit se k Internetu [4,7].

4.1.1.1 Využívání technologií VoIP ve firmách

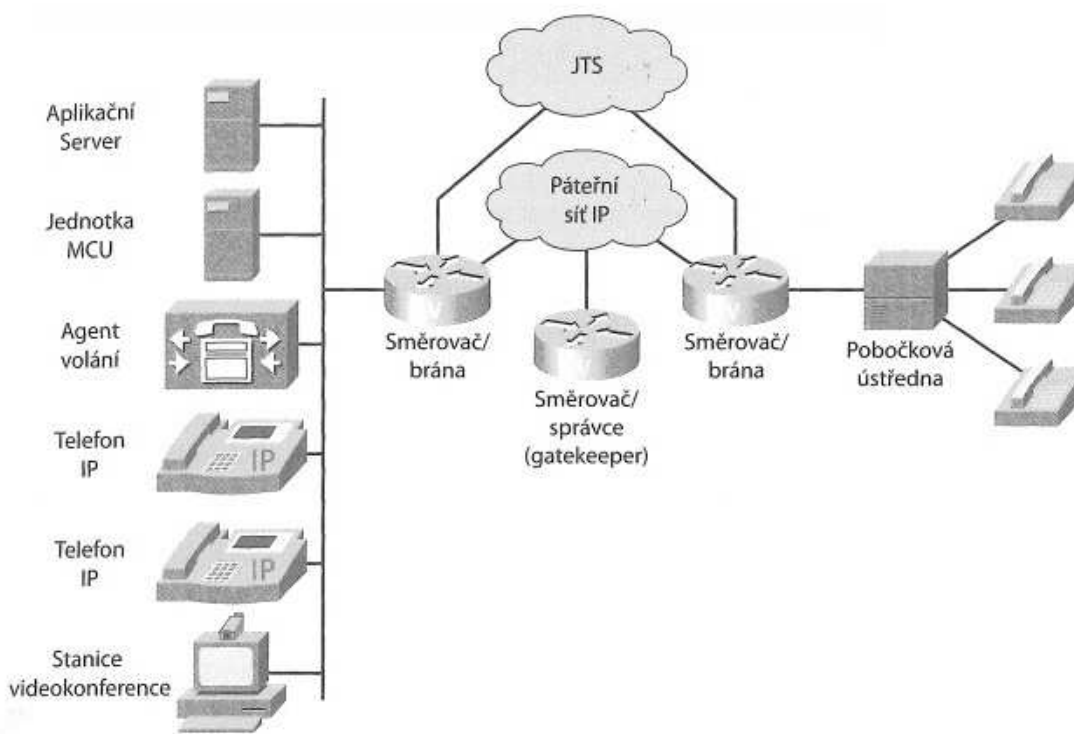
Původně se výhody implementace VoIP ve firmách se zaměřovaly na úspory spojené s neplacením telefonních poplatků a integrace sítě. To platí i dnes, avšak pokroky v hlasových technologiích umožňují poskytovatelům služeb nabízet ve svých produktech různé kombinace následujících výhod:

- ***Snížení nákladů***–TDM (time-division multiplexing), využívaný v sítích PSTN (Public Switched Telephone Network), vyhrazuje z celkové šířky pásma 64 kb/s na hlasový kanál. Pokud je použita tato metoda, je v případě, že neprobíhá žádná hlasová komunikace, tato vyhrazená šířka pásma nevyužita. Protokol VoIP sdílí šířku pásma. Výsledkem je efektivní využití šířky pásma, což v konečném důsledku znamená nižší požadavky na propustnost připojení. IP telefonie využívá k multiplexování hlasového přenosu souběžně s přenosem dat statistickou analýzu. Výsledkem této konsolidace jsou výrazné úspory z hlediska provozních nákladů a pracovního zařízení.
- ***Flexibilita*** – funkce IP sítí umožňují organizacím být flexibilní z hlediska toho, jaké typy služeb a aplikací nabízejí svým zákazníkům a uživatelům. Poskytovatelé služeb mohou snadno segmentovat zákazníky. To jim pomůže poskytovat různé vlastní služby, aplikace i sazby v závislosti na potřebách z hlediska objemu přenosu a dalších faktorech specifických pro jednotlivé zákazníky.
- ***Pokročilé funkce*** – několik nejpoužívanějších pokročilých funkcí:
 - ***Pokročilé směrování volání*** – v síti IP může existovat více tras pro spojení hovoru. Některé trasy jsou upřednostňovány s ohledem na vzdálenost, kvalitu, náklady, partnerské dodávky, zátěž z hlediska přenosu nebo různé další faktory.
 - ***Systém jednotného zasílání zpráv*** - jednotné zasílání zpráv zlepšuje produktivitu a komunikaci. Obsahuje uživatelské rozhraní například pro čtení e-mailů, hlasovou poštu a prohlížení faxových zpráv z jedné schránky doručené pošty.
 - ***Integrované informační systémy*** - pomocí technologie VoIP lze ovlivňovat transformaci obchodních procesů. Mezi tyto procesy patří virtuální kontaktní centra na různých geografických místech, centralizované řízené volání a přístup k prostředkům a samoobslužným nástrojům.

- **Zabezpečení** – IP technologie umožňuje šifrovat pakety proti neoprávněnému přístupu, útoku hackerů [7,19].

4.1.2 Součásti sítě VoIP

Na obrázku 4.1 jsou znázorněny základní součásti paketové hlasové sítě.



4.4.1. Součásti sítě VoIP [7]

Základní součásti:

- **IP telefony** – mají ethernetové síťové připojení, které slouží k zasílání a přijímání hlasových hovorů.
- **Správce (gatekeeper)** - zajišťuje řízení CAC (Call Admission Control), správu a řízení šířky pásma a překlad adres.
- **Brána (gateway)** - zajišťují překlad mezi sítí VoIP a sítěmi, které nejsou VoIP, například PSTN. Také umožňují fyzicky přístup pro lokální analogová a digitální hlasová zařízení, například telefony, faxová zařízení, sady klíčů a pobočkové ústředny.
- **Jednotky MCU (Multipoint Control Unit)** - zajišťuje připojení v reálném čase pro účastníky na různých místech světa, aby se mohli účastnit stejné videokonference nebo schůzky.

- **Agent volání** - umožňuje řídit volání pro telefony IP, řízení CAC, správu a řízení šířky pásma a překlad adres.
- **Aplikační servery** - zajišťují takové služby, jako je například hlasová pošta nebo jednotné zasílání zpráv.
- **Stanice videokonference** - zajišťuje přístup pro účast koncových uživatelů ve videokonferenci. Obsahuje zařízení pro mikrofon (pro vstup zvuku) a digitalizaci videa (pro vstup videa). Uživatel může poslouchat zvuk a sledovat datové proudy videa ze vzdálené stanice uživatele.

Další služby podle potřeb podniku zajišťují další komponenty, například softwarové hlasové aplikace, systémy IVR (interactive voice response) a softwarové telefony [3,7].

4.1.3 Funkce VoIP

V telefonní síti PSTN jsou všechny prvky nutné k uskutečňování volání koncovému uživateli transparentní. Pro migraci na VoIP technologie, je potřeba znát nutné prvky a důkladně pochopit princip protokolů a komponent, které zajišťují stejnou funkčnost v síti IP.

Povinné funkce VoIP:

- **Signalizace** - je schopnost generovat a vyměňovat informace o řízení, které budou použity k monitorování, navázání a uvolnění připojení mezi dvěma koncovými body. Hlasová signalizace vyžaduje možnost zajišťovat adresu, oznamování mezi dvěma uzly a supervizi. V síti PSTN se pro zprávy řízení přenosu využívá systém signalizace SS7 (Signaling System 7). Systém SS7 pro řízení volání využívá samostatný, vyhrazený kanál.
- **Databázové služby** - přístup ke službám, například ID volajícího nebo bezplatná čísla, vyžaduje možnost dotazovat se v databázi, aby bylo možné určit, zda lze volání uskutečnit nebo zda lze zpřístupnit informace. Databázové služby zahrnují přístup k službám databáze bezplatných čísel, doručování jména volajícího (CNAM), fakturačním informacím a službám volacích karet. Poskytovatelé služeb VoIP mohou odlišit své služby zajištěním přístupu k řadě jedinečných databázových služeb.
- **Řízení nosných služeb (bearer)** - slouží k přenosu hlasových volání. Je nutné, aby byla mezi koncovými zařízeními předávána odpovídající signalizace připojení a

odpojení volání. Správná signalizace zajišťuje, aby byl vyhrazen kanál pro aktuální hlasové volání a aby bylo správně zrušeno vyhrazení kanálu, když jeden z účastníků volání ukončí. Zprávy o připojení a odpojení jsou v síti PSTN přenášeny pomocí systému SS7. V síti IP jsou přenášeny pomocí protokolu SIP, H.323 nebo MSCCP.

- **Kodeky** - zajišťují převod kódování a dekódování mezi analogovými a digitálními zařízeními. Každý typ kodeku definuje mechanismus komprese a metodu kódování hlasu používané k převodu hlasu, viz [1,7,19].

4.2 VoIP protokoly

K dispozici jsou 2 typy VoIP protokolů: signalizační a transportní. Signalizační protokoly plní funkce, které obvykle plní tradiční protokoly, jako je digitální síť integrovaných služeb (ISDN) Q.931. Transportní protokoly se používají k zapouzdření nebo přenosu hlasové informace. Univerzální transportní protokol je Real-Time Protokol (RTP) [1,3].

4.2.1 Signalizační protokoly

I přesto, že VoIP architektura je zcela odlišná od použití klasické telefonie, existují stále základní požadavky na signalizaci. Telefony musejí vyzvánět, čísla musí být sdělena a trasování signálu musí být nastaveno. Všechny tyto funkce jsou zpracovány signalizačním protokolem. Nejběžnější typy jsou H.323, Skinny a Session Initiation Protocol (SIP) [1,3].

4.2.1.1 Session Initiation Protocol (SIP)

SIP je standardizovaný protokol od Internet Engineering Task Force (IETF). Formát SIP zprávy je velmi podobný paketu HyperText Transfer Protocol (HTTP). SIP měl pomalý start, ale dnes je používán po celém světě. Dokonce i Cisco přechází ze Skinny na SIP. Vzorek SIP paketu je vidět na obrázku 4.2. Z něj je patrné, že paket lze snadno přečíst. Má jasný cíl a zúčastněné strany jsou jasně definovány. Protokol je populární díky jednoduché integraci s adresováním TCP/IP [1,3].

```

Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112
Transmission Control Protocol, Src Port: sip (5060), Dst Port: sip (5060), Seq: 1, Ack:
Session Initiation Protocol
  Status-Line: SIP/2.0 180 Ringing
    Status-Code: 180
    [Resent Packet: False]
  Message Header
    v: SIP/2.0/TCP 10.210.200.112:5060;branch=z9hg4bk2965924072-14
    f: <sip:10.210.200.112>;epid=10021002000112;tag=plcm_2965924072-15
    t: <sip:10.210.200.111>;tag=plcm_1663913224-7
    i: 2965924072-13
    cSeq: 1 INVITE
    k: timer
    m: <sip:10.210.200.111:5060;transport=tcp>
    User-Agent: Polycom ViaVideo Release 8.0
    l: 0

```

4.4.2. SIP paket [1]

4.2.1.2 H.323

H.323 je standard od ITU-T, který se zaměřuje na videokonference. Tento standard byl vyvinut dříve, než ostatní zmíněné protokoly. Existuje několik subprotokolů (H.225, H.245, atd.). Vzorek H.225 paketu je vidět na obrázku 4.3.

```

  H.225.0 CS
    H323-UserInformation
      h323-uu-pdu
        h323-message-body: setup (0)
          setup
            protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
            sourceInfo
              terminal
                .0.. .... mc: False
                ..0. .... undefinedNode: False
                ...0 .... activeMC: False
            conferenceID: 00000000-0000-1000-0000-0000c0a81017
            conferenceGoal: callIndependentSupplementaryService (4)
            callType: pointToPoint (0)
            callIdentifier
            fastStart: 36 items
              1... .... mediawaitForConnect: True
              1... .... canOverlapSend: True
              0... .... h245Tunnelling: False

```

4.4.3. H.225 paket [1]

Na paketu H.225, ve kterém je zapouzdřen H.323 protokol je vidět sekce FastStart, která má 36 položek. Tato složitost je jedním z důvodů jeho klesající popularity [1,3].

4.2.1.3 Skinny Client Control Protocol

Skinny Client Control Protocol (SCCP) neboli skinny je produkt firmy Cisco. Je vysoce proprietární a jeho princip se značně liší od toho, co by mohlo být považováno za standardní nasazení VoIP. Nicméně Cisco mělo veliký úspěch s jeho produkty VoIP.

Vzorek Skinny paketu je vidět na obrázku 4.4.4. Jednou z předností protokolu Skinny je, že stejně jako SIP je velmi snadno čitelný. Nicméně Skinny je proprietární a má určité chování, které není vidět jinde, jako například v Real-Time Control Protocol (RTCP), doprovodném protokolu RTP [1,3].

```

Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 192.168.1.1 (192.168.1.1)
Transmission Control Protocol, Src Port: cisco-sccp (2000), Dst Port: 50202 (50202), Seq: 1205,
Skinny Client Control Protocol
Data Length: 88
Header version: Basic (0x00000000)
Message ID: StartMediaTransmission (0x0000008a)
Conference ID: 2
Pass-thru party ID: 0
Remote IP address: 192.168.1.3 (192.168.1.3)
Remote port: 27368
MS/packet: 20
Payload capability: G.711 u-law 64k (4)
Precedence: 0
Silence suppression: Media_SilenceSuppression_Off (0x00000000)
Max frames per packet: 0
G723 bitrate: Media_G723BRate_6_4 (2)

```

4.4.4. SCCP paket [1]

4.2.2 Transportní protokol

Real-Time Transport Protocol (RTP) je oblíbený prostředek pro přenos paketů obsahujících hlasová data. RTP je definován v RFC 3550, je to jednoduchý protokol, který používá zdrojová ID pro sloučení paketů ze stejného zdroje. Pakety se skládají ze dvou částí, z hlavičky a užitečného zatížení. Užitečné zatížení se identifikuje tak, aby přijímač mohl určit, který kodek byl použit pro vytvoření hlasového paketu. Vzorek RTP paketu je znázorněn na obrázku 4.4.5.

```

Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.24
User Datagram Protocol, Src Port: tsb2 (2742), Dst Port: acc-raid (2800)
Real-Time Transport Protocol
  [Stream setup by H245 (frame 597)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  0... .... = Marker: False
  Payload type: ITU-T G.711 PCMU (0)
  Sequence number: 11639
  [Extended sequence number: 77175]
  Timestamp: 998248329
  Synchronization Source identifier: 0x196d27c5 (426584005)
  Payload: cec4e14b60cb61f8684a70febfcd5f51494d70c1cdde3f4a...

```

4.4.5. RTP paket [1]

RFC 3550 také obsahuje Real-Time Control Protocol (RTCP), který poskytuje informace o toku RTP paketů. Jeho primární úkol je poskytnout zpětnou vazbu o kvalitě hovorových kanálů. RTCP paket viz obrázek 4.4.6.

```
User Datagram Protocol, Src Port: lot105-ds-upd (2053), Dst Port: upgrade (2537)
Real-time Transport Control Protocol (Sender Report)
  [Stream setup by H245 (frame 22700)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 0000 = Reception report count: 0
  Packet type: Sender Report (200)
  Length: 6 (28 bytes)
  Sender SSRC: 0x07fff4aa (134214826)
  Timestamp, MSW: 18560 (0x00004880)
  Timestamp, LSW: 1941307392 (0x73b60000)
  [MSW and LSW as NTP timestamp: Not representable]
  RTP timestamp: 148483616
  Sender's packet count: 2
  Sender's octet count: 320
Real-time Transport Control Protocol (Source description)
[RTCP frame length check: OK - 80 bytes]
```

4.4.6. RTCP paket [1]

Při porovnání paketů je zřetelné, že RTP paket obsahuje informaci o použitém kodeku, ID zdroje a samotná data. RTCP paket nic z toho neobsahuje. Místo toho RTCP sleduje časování a odeslané bajty mezi koncovými body. Podrobnosti viz kapitola 4 *Packet Guide Voice over IP* [1,3].

4.3 Doplnující nástroje

Pro plně fungující nasazení VoIP řešení je zapotřebí dalších protokolů a nástrojů.

4.3.1 IP protokol

Protokoly na 3 vrstvě modelu OSI mají primárně zajistit komunikaci mezi sítěmi. Při komunikaci v jediné síti na vrstvě 2 se používají MAC adresy. Obdobně vrstva 3 odpovídá za adresy, které umožňují komunikaci zařízení, která jsou umístěna v různých sítích. Tyto služby dokáže poskytnout několik protokolů, ale nejčastěji je možno se setkat s protokolem IP (definován v dokumentu RFC 791). IP protokol v zásadě představuje internetovou vrstvu. Další protokoly zde plní pouze pomocnou funkci. Protokol IP tvoří základní schéma a dá se říct, že „vše vidí“ v tom smyslu, že má informace o všech propojených sítích. Tato vlastnost je založena na tom, že všechny zařízení v síti mají SW neboli logickou adresu označovanou jako IP adresa [6, 21].

4.3.1.1 IP adresy

IP adresy jsou 32 bitové adresy, které umožňují jedinečně identifikovat zařízení připojené k síti. Bylo by příliš náročné pamatovat si sekvenci jedniček a nul dlouhou 32 znaků, takže se IP adresy zapisují v tečkové notaci. (dotted-quad notation). 32 bitů se dělí do 4 sekcí,

kteře se označují jako oktety nebo bajty, z nichž každý obsahuje 1 bajt (8bitů). IP adresu lze popsat jednou ze tří metod:

- Jako desítková čísla, např. 172.16.30.26
- Binárně, jako např. 10101100.00010000.00011110.00111000
- Hexadecimálně, jako např. AC.10.1E.38

Všechny tyto příklady označují stejnou IP adresu. Není náhodou, že se IP adresy dělí na 4 čísla. IP adresa je tvořena 2 částmi: adresou sítě (network address) a adresou hostitele (host address). Adresa sítě identifikuje lokální síť, do které je zařízení připojeno, a adresa hostitele označuje vlastní zařízení v síti. V praxi závisí na další adresní informaci, která se označuje jako maska sítě (network mask – netmask) nebo maska podsítě (subnet mask).

Maska podsítě je 32 bitová hodnota, která zařízení přijímacího paketu IP umožňuje rozlišit v IP adrese část adresy sítě a adresy hostitele. Tato 32 bitová maska podsítě se skládá z jedniček a nul. Hodnoty přitom reprezentují pozice, které se týkají síťových adres nebo adres podsítí.

IP adresy a masky sítě se často zapisují zkrácenou notací CIDR (ClassLess Inter-Domain Routing – beztřídní směrování mezi domény). V tomto formátu je uvedena celá IP adresa následovaná lomítkem a počtem bitů, které představují síťovou část IP adresy. IP adresu 10.10.1.22 a masku sítě 255.255.0.0 je například v notaci CIDR možné uvést jako 10.10.1.22/16 [6, 21].

4.3.2 TCP protokol (Transmission Control Protocol)

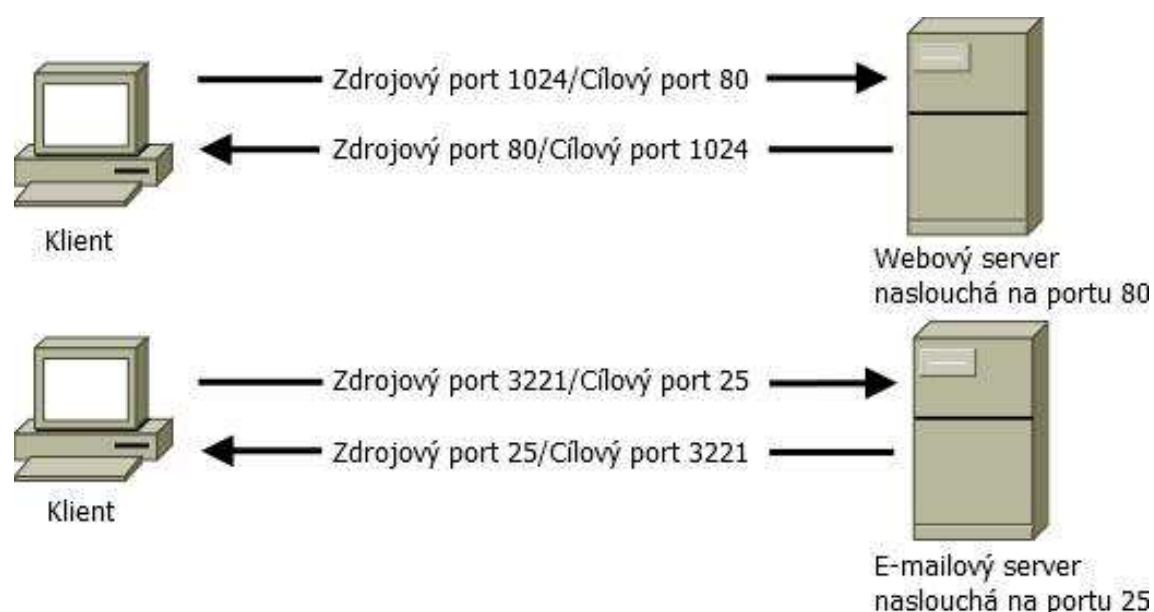
Úkolem protokolu TCP je zajistit spolehlivé doručování dat mezi koncovými body. Protokol TCP definovaný v dokumentu RFC 793 funguje na vrstvě 4 modelu OSI. Stará se řazení dat a opravu chyb a v konečném důsledku zajišťuje, že se data dostanou do určeného cíle. Při doručování paketů do cílového umístění se na protokoly TCP/IP spoléhá mnoho běžně používaných protokolů aplikační vrstvy. Protokol TCP je plně duplexní, spojovaný, spolehlivý a přesný, ale nastavení všech podmínek přenosu nad rámec kontroly chyb není rozhodně zadarmo. Protokol TCP je velmi komplikovaný a s ohledem na síťovou režii také poměrně nákladný [6, 21].

4.3.2.1 Porty TCP

Komunikace vrstvy protokolu TCP probíhá mezi zdrojovými a cílovými porty, které jsou uvedeny v každé hlavičce TCP. Port lze přirovnat k zástrčce ve staré telefonní ústředně.

Telefonní operátor tehdy sledoval panel se světélky a zásuvkami. Když se rozsvítila kontrolka, ozval se volajícím a zeptal se, s kým chce mluvit. Poté volajícího propojil s cílovou stanicí pomocí příslušného kabelu. Každé volání muselo mít svůj zdrojový port (volající) a cílový port (volaný). Porty TCP fungují obdobně.

Aby bylo možné přenášet data určité aplikaci na vzdáleném serveru nebo zařízení, musí paket TCP obsahovat informace o portu, na kterém vzdálená služba naslouchá. Pokud se pokusíte-li o přístup k aplikaci na portu, pro který není nakonfigurována, nebude komunikace úspěšná. Zdrojový port není v tomto postu příliš důležitý a lze jej vybrat náhodně. Vzdálený server zjistí, se kterým portem má komunikovat, jednoduše z původního paketu, který obdržel.



4.4.7. Protokol TCP přenáší data pomocí portů [6]

Klíčové protokoly a jejich čísla portů:

- Telnet 23,
- SMTP 25,
- http 80,
- SSH 22,
- DNS 53,
- FTP 20;21,
- HTTPS 443.

Ke komunikaci s protokolem TCP je k dispozici 65535 portů. Tyto porty se obvykle dělí do dvou skupin: standardních a dočasných [6, 21].

4.3.2.2 Skupina standardních portů

Skupina standardních portů začíná portem 1 a končí portem 1023 (port 0 se ignoruje, protože tato hodnota je vyhrazena). Se standardními porty pracují některé běžné služby. Tyto porty jsou definovány ve standardu RFC 3232 [6, 21].

4.3.2.3 Skupina dočasných portů

Skupina dočasných portů je omezena porty 1024 – 65535 (ačkoli některé operační systémy je definují odlišně). Na určitém portu může v danou chvíli komunikovat pouze jediná služba. Moderní operační systémy proto vybírají zdrojové porty náhodně, aby byla zajištěna jedinečnost komunikace. Tyto zdroje porty obvykle patří do rozsahu dočasných portů [6].

4.3.3 UDP protokol

Protokol UDP je druhý protokol 4 vrstvy, který se běžně používá v moderních sítích. Zatímco je protokol TCP navržen tak, aby díky integrované kontrole chyb zajistil spolehlivý přenos dat, účelem protokolu UDP je poskytnout rychlý přenos. Protokol UDP neřadí segmenty a nestará se o to, v jakém pořadí dorazí do cílového umístění. UDP segmenty prostě odešle a dále se jimi nezabývá. Nesleduje tyto segmenty, nekontroluje jejich stav, ani neposkytuje potvrzení bezpečného doručení. Vzhledem k tomu se označuje jako nespolehlivý protokol.

Vzhledem k tomu, že nespojovaný protokol nemůže zajistit spolehlivé služby, lze předpokládat, že přenos protokolem UDP bude značně nejistý. Teoreticky to platí, ale protokoly, které spoléhají na UDP, mají obvykle zabudovány vlastní služby spolehlivého přenosu nebo částečně zvyšují spolehlivost připojení pomocí některých funkcí protokolu ICMP. Například protokoly aplikační vrstvy DHCP a DNS, které značně závisí na rychlosti přenosu paketů po síti, sice používají protokol UDP jako svůj protokol transportní vrstvy, ale sami se starají o kontrolu chyb a časovače opakovaného přenosu [6, 21].

4.3.4 ICMP protokol (Internet Control Message Protocol)

Protokol ICMP funguje na síťové vrstvě a protokol IP pomocí něj zajišťuje mnohé služby. ICMP je obslužný protokol pro TCP/IP, který poskytuje informace o dostupnosti zařízení, služeb nebo tras v síti TCP/IP. Většina metod a nástrojů pro řešení potíží v síti je založena na běžných typech zpráv protokolu ICMP. Běžné události a zprávy, se kterými protokol ICMP souvisí:

- Ping
- Traceroute
- Hops/time exceeded (překročen počet přeskoků/časový limit)
- Destination unreachable

Protokol ICMP je definován v dokumentu RFC 792 [6, 21].

4.3.5 DHCP protokol (Dynamic Host Configuration Protocol)

Protokol DHCP nahrazuje starší BOOTP (Bootstrap Protocol). DHCP je protokol aplikační vrstvy, který zařízením umožňuje automaticky získat IP adresu (a adresu jiných síťových prostředků, jako jsou servery DNS a směrovače). Protokol DHCP se od protokolu BOOTP liší v tom, že protokol BOOTP přiřazuje adresu hostiteli, ale hardwarovou adresu hostitele je nutné zadat ručně do tabulky BOOTP. Většina serverů DHCP v současnosti klientům poskytuje i jiné parametry, např. adresy výchozí brány a serverů DNS používaných v síti [6,21].

4.4 Kodeky

Kodek lze označit jako algoritmus nebo zařízení, jehož hlavním úkolem je komprese velkého množství audiovizuálních informací. „Slovo kodek vzniklo složením slov kodér a dekodér, tj. zařízení, jež je na jedné straně schopné data zakódovat a na druhé straně opět rozkódovat“ [4]. Data získaná ze vstupu mikrofону, který je připojen ke zvukové kartě, kodér zpracuje a předá je Real Time Protocolu, který data přenese na druhou stranu. Na druhé straně se proces opakuje v opačném pořadí, akorát výstupem je reproduktor [8,9].

„Kodeky velmi často používají ztrátovou kompresi, a proto dekodovaná data nejsou totožná s daty, která byla zakódována“ [4].

4.4.1 Standardy kódování a dekodování

Jakmile se analogová vlnová křivka digitalizuje, je možno ušetřit šířku pásma komprimací těchto digitalizovaných vlnových křivek. Nejznámější a nejpoužívanější kodek je PCM [3,4]. Kódování PCM (Pulse Code Modulation) se sestává ze tří kroků [4]:

- Vzorkování - hodnoty spojitého analogového signálu se odečítají v diskrétním čase,
- Kvantování - ke každému vzorku získanému v předchozím kroku se přiřadí jedna z možných diskrétních úrovní,
- Zakódování - diskrétní hodnoty jsou reprezentovány pomocí n-bitových čísel; čím

více bitů jeden vzorek obsahuje, tím menší chyba při PCM kódování vzniká, ale na druhou stranu objem dat se zvětšuje.

4.4.1.1 Kódování DPCM (Differential Pulse Code Modulation)

DPCM vychází z kódování typu PCM a jejím hlavním účelem je snížit objem přenesených dat. „Nekódují se navzorkovaná data, ale jejich rozdíl oproti odhadnutému průběhu signálu. Průběh signálu je možné částečně předpovědět, protože po sobě následující vzorky jsou korelovány“ [4]. Toto je důsledkem parametrů hlasového traktu. Odhadnutý a navzorkovaný průběh mají minimální rozdíly, tudíž výsledný rozdíl má mnohem menší rozptyl a tedy je využito menšího počtu bitů k přenosu dat [4].

4.4.1.2 Kódování ADPCM (Adaptive Differential Pulse Code Modulation)

ADPCM je modifikací DPCM. V tomto typu kódování je generátor srovnávacího průběhu vylepšen tak, že je adaptivní a konkrétní kódované řeči se dokáže přizpůsobovat. To má za následek ještě menší rozptyl, než u kódování DPCM, a z toho plynoucí menší počet bitů k přenosu. Při tomto kódování dochází i ke změně vlastností kvantifikace pro charakteristiku konkrétní řeči. Mezi kodeky, které využívají ADPCM patří například kodek G.726 [3,4].

4.4.1.3 Kódování LPC (Linear Predictive Coding)

Princip fungování LPC je založen na úplně odlišném principu než předchozí dva způsoby kódování (DPCM, ADPCM). Jde o soustavu generátorů a filtrů, které mají za úkol snažit se kopírovat lidskou řeč. Tato metoda má za úkol definovat model hlasového ústrojí člověka. Jedním z předpokladů LPC kódování, je generování hlasového signálu bzučákem, umístěném na konci trubky. Bzukot definovaný frekvencí a hlasitostí vytváří šterbina mezi hlasivkami. Trubka definována svými rezonancemi, často označované jako formanty, modeluje ústa a krk. „LPC analyzuje řeč aproximováním formantů, odstraněním jejich působení z hlasového signálu a odhadem intenzity a frekvence zbývajících signálu, který je generován hlasivkami. Proces odstranění formantů se nazývá inverzní filtrování. Čísla reprezentující formanty mohou být uložena nebo odeslána jinam“ [4]. Řečový signál se vytváří inverzním procesem – nejdříve generátor vyprodukuje signál o určité frekvenci a hlasitosti. A filtr je vytvořen rezonancemi (formanty). Filtr zpracuje vygenerovaný signál a výsledkem je signál, který je podobný originálnímu signálu. Kvůli variabilitě vstupního signálu musí docházet k opakování tohoto procesu v krátkých časových intervalech –

rámců. 30 -50 rámců za sekundu jsou dostačující pro kvalitní úroveň řeči. Při použití metody LPC, v pásmu 2,4 kbit/s je již řeč srozumitelná [4, 20].

4.4.1.4 Kódování CELP (Code Excited Linear Prediction)

CELP zdokonaluje kódování LPC. Mezi hlavní problémy lineárně prediktivního kódování je skutečnost, že zbytek signálu po průchodu formantovým filtrem není pouze signál bzučáku. To je způsobeno tím, že součástí řeči je například složka reprezentující sykot. Takový sykot není jednoduché správně aproximovat pomocí kodeku LPC. Při odhadování formantů dochází k nepřesnostem, kdy některé informace o signálu zůstanou v takzvaném reziduu. LPC modelu neodpovídají například zvuky, které jsou generovány různým umístěním jazyka v ústech atd. Při použití kódování LPC, se informace o znělosti řeči obsažené v reziduum ztratí, a to z důvodu zakódování na základě dvou parametrů, amplitudy a frekvence signálu. Řešením lepšího zakódování rezidua bez navýšení šířky pásma a zachování důležitých informací je použití codebooku. V tabulce codebook jsou definovány typické průběhy rezidua. Kodér porovnává hodnoty v tabulce s průběhem rezidua a zvolí si tu, která má nejmenší odchylku. Poté se přenáší index této hodnoty z tabulky. Na opačném konci existuje stejná tabulka, která na základě přijatého indexu umí z codebook tabulky obnovit průběh rezidua. Tento průběh rezidua poté slouží jako generátor filtru aproximujícího formanty. Výsledkem použití codebook tabulky je zkvalitnění aproximace signálu než při použití lineárně prediktivního kódování. Aby CELP (Code Excited Linear Prediction) mohla správně fungovat, musí být tabulka codebook dostatečně rozsáhlá. Požití veliké tabulky má za následek velmi dlouhé vyhledávání. Součástí tabulky by měly být i vzorky pro různě vysoké hlasy, taková tabulka by byla ještě obsáhlejší a vyhledávání by bylo ještě delší. Řešením je rozložení informací do dvou menších tabulek místo jedné veliké. První tabulka obsahuje vzorky právě jednu výšku hlasu a je vytvořena při tvorbě kodeku. Druhá tabulka je nejdříve prázdná a plní se předešlými zpožděnými vzorky rezidua o konkrétní hodnotu, tedy je adaptivní. Tato hodnota latence určuje jakou bude mít hlas výšku. Při použití metody CELP, v pásmu 4,8 kbit/s je již řeč srozumitelná.

Existují další modifikace tohoto typu kódování. Mezi nejznámější můžeme zařadit LD-CELP (Low Delay Conjugate Excited Linear Predication) a ACELP (Algebraic Code Excited Linear Predication) [3,4].

4.4.2 Nejpoužívanější kodeky

Následuje výčet nejpoužívanějších kodeků [3,4]:

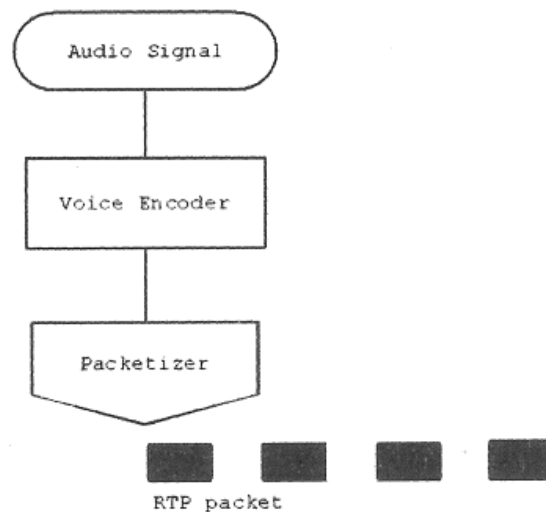
- G.711 patří mezi základní kodeky. Běžně se používá v PSTN (Public Switched Telephone Network). Kvalita hovoru je srovnatelná s kvalitou při běžném telefonním hovoru.
- G.723.1 je založen na kódování ACELP nebo MP-MLP. MP-MLP kódování vyžaduje šířku pásma 5.3 kbit/s, ACELP 6.3 kbit/s.
- G.726 patří do skupiny ADPCM kodeků. Má rozdílné nároky na šířku pásma a to 16, 24, 32 a 40 kbit/s. Na základě různé délky zpoždění zpracovává různě dlouhé bloky.
- G.728 je založen na LD-CELP kódování. BW je 16 kbit/s.
- G.729 je založen na CS-ACELP kódování - Conjugate Structure Algebraic Code Excited Linear Prediction. BW je 8 kbit/s.
- G.729a Při komprimaci paketů zaručuje nižší zátěž procesoru.
- GSM kodek, BW je 13 kbit/s. GSM je efektivnější nežli CELP (metody založené na slovníku).
- iLBC (Internet Low Bit Rate Codec) je kodek vyvinutý firmou Global IP Sound, BW je 13.33 kbit/s. V případě ztráty nebo zpoždění paketů umožňuje kodek elegantní snížení kvality přenášeného hlasu. K tomu využívá algoritmus Block Independent Linear Predictive Coding.

Kodek	Typ
G. 711	PCM
G. 723.1	MP-MLQ
G. 723.1	ACELP
G. 726	ADPCM
G. 728	LD-CELP
G. 729	CS-ACELP

4.4.1. Kodéry a jejich typy [4]

4.4.3 Výpočet šířky pásma

Signál musíme rozdělit na signalizaci a hlas. Signalizace je přenášena UDP nebo TCP protokolem. Oproti tomu hlas je přenášen RTP (Real Time Protocol), který je založen na UDP. Na obrázku 4.4.8 je znázorněn postup zpracování na straně odesílatele.



4.4.8. Zpracování hlasu na straně odesílatele [4]

Ke zpracování signalizace dochází odděleně a jedná se čistě o softwarovou záležitost. Jejím úkolem je hlavně mapování zpráv použitých protokolů (například H.323 pokud se jedná o hlasovou bránu, DSS1 atd.). Informace o signalizaci jsou vyhodnocovány a na základě jasně definovaných pravidel se tyto informace přidávají do paketů určených příjemci, nebo jsou generovány další dotazy na komponenty systému VoIP (na H.323 Gatekeeper nebo SIP Server). „Zpracování hlasu vyžaduje různou náročnost na procesorový výkon MIPS (Million Instructions Per Second), což je dáno kodekem. Pro efektivní využití IP sítí se používají většinou adaptivní metody komprese hlasu tak, aby bylo pásmo optimálně využito. Současné procesory jsou dostačující pro kompresi i dekompresi současně. V případě, že požadavků na kompresi více souběžných spojení se využívají signálové procesory DSP, které zároveň mohou provádět odečet ozvěny (echo-cancellation)“ [4].

Na straně odesílatele je hlas nejdříve kódován dostupným kodekem a poté paketizován do balíčků s užitečnou zátěží 20 až 160 oktětů a se standardní hlavičkou 40 oktětů. „Pakety jsou odesílány s časovými rozestupy, tento čas lze označit jako interval Δt_s . Ze znalosti Δt_s a použitého kodeku je možno definovat velikost užitečné zátěže v RTP paketu označené jako P_s “ [4]. Vztah mezi velikostí paketu a užitečné zátěže popisuje rovnice (6):

$$\Delta t = \frac{P_s}{C_R} \quad (6)$$

- Δt_s [ms] je sample time, rozestup mezi pakety se vzorky,
- P_s [oktět] užitečná zátěž, payload size,

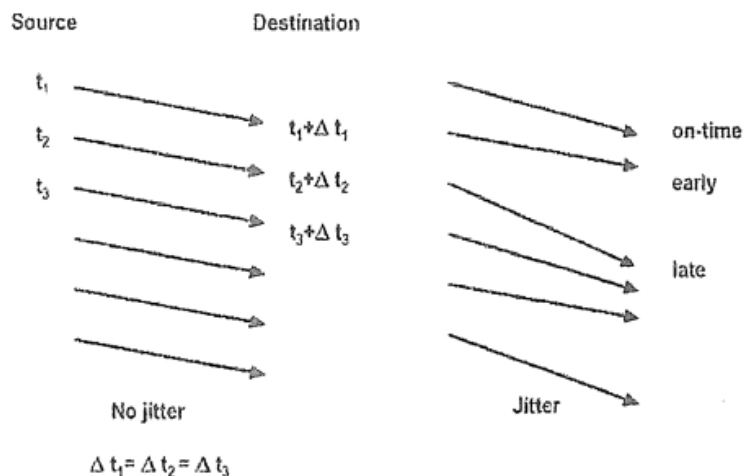
➤ C_R [kbit/s] codec rate, vlastnost kodeku, přenosová rychlost.

Ze znalosti formátu paketu a informaci o velikosti zátěže lze definovat režii přenosu pro konkrétní typ kódování podle vztahu (7), jehož součástí je i celková velikost paketu,

$$BW = \frac{(8 \cdot h + c_r \cdot \Delta t_s)}{\Delta t_s} \quad (7)$$

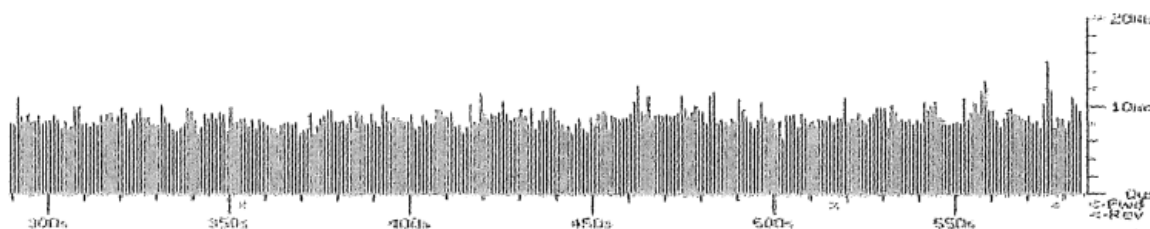
kde BW je nárokové pásmo (bandwidth), po dosažení Δt_s v ms vyjde BW v kbit/s a h je velikost hlavičky v bajtech, h je součet všech hlaviček. Pokud bychom chtěli spočítat pásmo na úrovni mezisíťové vrstvy, dosadí se 40 B a pokud v Ethernetu, tak 66 B bez VLAN a s použitím VLAN 68 B.

Pro kodek dle ITU-T G.711 je v plně duplexním Ethernetu potřeba zhruba 90 kbit/s oproti konvenčním 64 kbit/s v kanálově propojovaných sítích. U G.729 je to zhruba 35 kbit/s na hovor oproti tabulkovým 8 kbit/s a u G.723.1 5.3 kbit/s je výsledek 23 kbit/s a u G.723.1 6.3 kbit/s jsou nároky na hovor 24 kbit/s. U GSM kodeku (13.2 kbit/s) při typickém $P_s=33$ B nárokováno cca 40 kbit/s. Z uvedených rychlostí je možné si udělat obrázek, jak to v Ethernetu vypadá - pokud je třeba přenést současně 30 hovorů s kódováním PCM, pak lze očekávat tok RTP 2.7 Mbit/s. RTP pakety procházející IP sítí mohou být časově posunuty vlivem řazením ve frontách na routerech, na obrázku 4.4.9 vidíme příklad příchodů paketů s různým časovým zpožděním. Standard RFC 1889 pro RTP protokol již na toto pamatuje a hlavičky paketů obsahují položku *Timestamp* vyjadřující vzorkovací značku RTP paketu odvozenou od lineárního časovače. Tato značka přesně rozpoznává jitter a eliminuje jeho vliv [4,5].



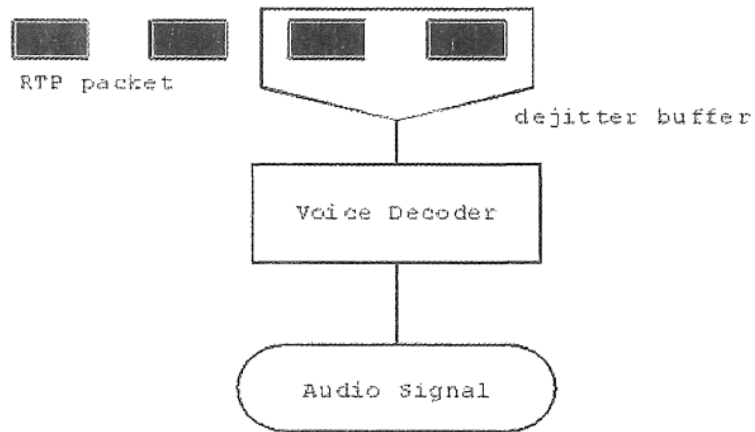
4.4.9. Jitter a jeho vliv na odstup mezi pakety [4]

Jitter označujeme jako rozptyl zpoždění a je to rozdíl mezi skutečným a očekávaným přijetím paketu. Na obr. 4.4.10 je zachycen příklad jeho průběhu během spojení.



4.4.10. Ukázka průběhu rozptylu zpoždění [4]

Na straně příjemce je přijatý paket zařazen do vyrovnávací mezipaměti (playout buffer neboli dejitter buffer), mající za úkol minimalizovat účinek rozptylu zpoždění. „Následně jsou data z mezipaměti předávány k dekódování, mezipaměť je vhodné nastavit na násobky dob trvání kódovaných hlasových fragmentů při paketizaci (např. 60 ms je nejvhodnější, neboť vyhovuje pro kódování G.711, G.729 i G.723.1), některá zařízení umožňují samokorekci velikosti mezipaměti a pomocí sofistikovaných algoritmů přizpůsobují její hodnotu aktuální situaci“ [4] (obr. 4.4.11.).



4.4.11. Zpracování na straně příjemce [4]

4.5 Převod hlasu na digitální signál

Hlas je ve své přirozené podobě analogový, tedy představuje plynule se měnící vlnovou křivku. V sítích VoIP se hlas naopak přenáší v digitální podobě pomocí binárního kódování, což znamená, že se přenáší série jedniček a nul, jak je ukázáno na obrázku 4.4.12. Jakmile se hlas převede na jedničky a nuly, a je připraven k zaslání po síti, je třeba se ujistit, že k přenosu všech svých hlasových hovorů není používána příliš velká šířka pásma [3].

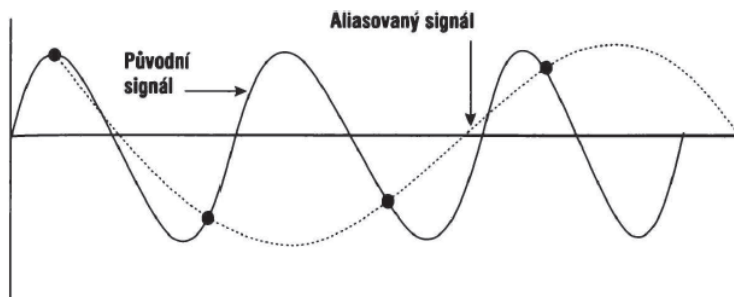


4.4.12. Analogová a digitální vlnová křivka [3]

4.5.1 Dělení hlasu na bajty

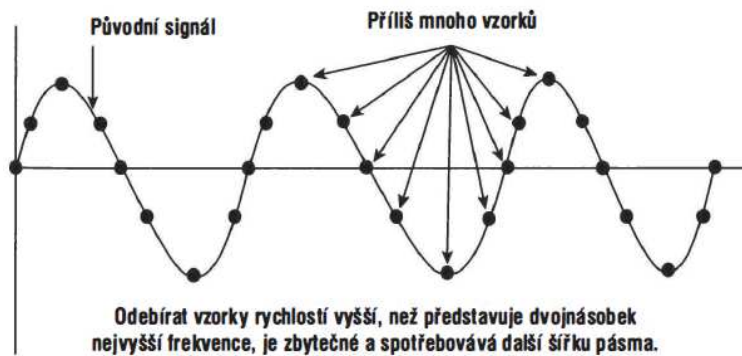
Úloha převodu analogového hlasu na digitální data začíná vzorkováním. Velmi často se odebírají „snímky“ nebo „vzorky“ analogové hlasové vlny. Tyto vzorky se následně digitalizují. Na druhém konci hlasové konverzace se tento digitalizovaný signál může následně převést zpět na analogovou vlnu, které dokáže posluchač porozumět.

Jedním z největších problémů u vzorkování je otázka, jak často by se měly tyto vzorky analogové vlny odebírat. Není žádoucí odebírat příliš malé množství vzorků za sekundu, protože když se zařízení na druhém konci telefonní linky pokusí znovu sestavit a porozumět těmto vzorkům, mohl by těmto vzorkům odpovídat také odlišný zvukový signál a posluchač by slyšel nesprávný zvuk. Toto označujeme termínem aliasing a je znázorněn na obrázku 4.4.13.



4.4.13. Aliasing [3]

Nepříznivé účinky podvzorkování nebo aliasingu, mohou svádět ke stanovisku „Odeberme raději mnohem více vzorků za sekundu, abychom se vyhnuli aliasingu“. Ačkoli tento přístup, někdy označovaný jako převzorkování, ve skutečnosti eliminuje problém aliasingu, přináší také jeden zásadní problém. Odebere-li za sekundu mnohem více vzorků, než je skutečně potřeba pro přesné obnovení původního signálu, spotřebuje se mnohem větší šířku pásma, než je nezbytně nutné.



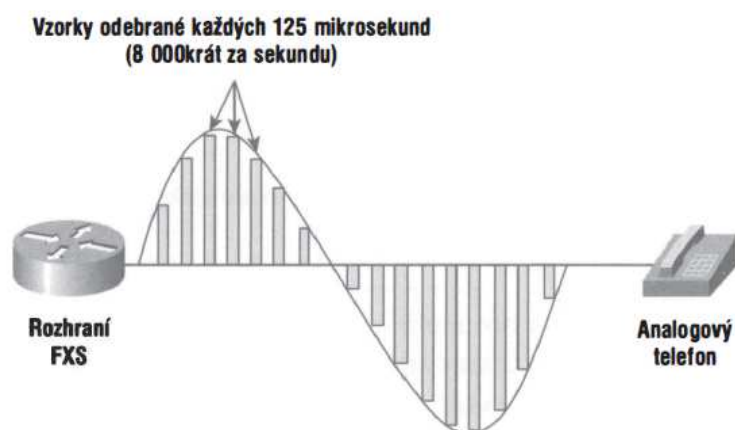
4.4.14. Převzorkování [3]

V tomto okamžiku je zřejmé, že nejde odebírat příliš málo ani příliš mnoho vzorků za sekundu.

Shannonův teorém udává, že vzorkovací frekvence musí být větší, nebo rovna, než je dvojnásobek maximální frekvence signálu.

$$f_v \geq 2f_{\max} \text{ [s}^{-1}\text{]} \quad (8)$$

Harry Nyquist uvedl, že rychlost odebírání vzorku musí být alespoň dvakrát tak vysoká jako největší vzorkovaná frekvence. Nejvyšší vzorkovaná frekvence pro hlas je teoreticky 4 kHz (to je 4 000 cyklů za sekundu). Na základě této informace Nyquistova věta udává, že je třeba odebrat 8 000 vzorků za sekundu, což znamená, že je třeba odebrat vzorek každých 125 mikrosekund, jak je znázorněno na obrázku 4.4.15.

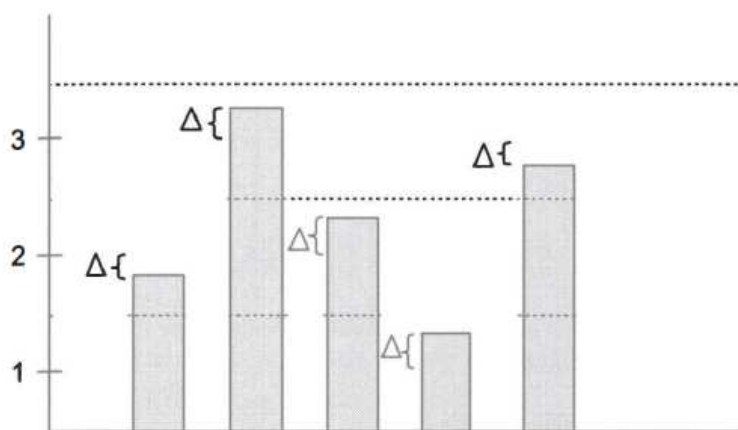


4.4.15. Vzorkování [3]

Počáteční proces vzorkování se označuje jako pulzně-amplitudová modulace (pulse amplitude modulation, PAM). Zajímavou skutečností však je, že po provedení pulzně-amplitudové modulace jsou vzorky stále v analogovém formátu. Tyto vzorky, jež jsou

tvořeny jedinou frekvencí, mají amplitudy (tj. intenzitu) odpovídající amplitudám vzorkované vlnové křivky.

V dalším kroku při digitalizaci vlnové křivky hlasu se vezmou tyto amplitudy a přiřadí se jim číslo, které lze poté přenášet v binární podobě. Proces přiřazování čísla k amplitudě se označuje termínem kvantizace, jak je znázorněno na obrázku 4.4.16.



4.4.16. Kvantizace [3]

Jakmile se vzorky pulzně-amplitudové modulace odeberou, je třeba je kvantizovat (přiřadit jim čísla, která budou představovat jejich amplitudy). Jestliže se však používá lineární stupnice (viz obrázek 4.16.), kvantizační chyba (označovaná deltami) způsobí deformaci hlasu. Deformace je patrná zejména při nižších intenzitách. Proto se používá raději logaritmická stupnice, která má při nižších intenzitách více měřicích intervalů.

Zajímavé je, že kvantizační chyba je patrnější u nižších amplitud. Nižší intenzity se přitom vyskytují většinou častěji než vyšší intenzity. Na základě těchto charakteristik je možno odebráním více vzorků při nižších intenzitách a méně vzorků při vyšších intenzitách překonat symptomy kvantizační chyby, aniž by se používala větší šířka pásma. K dosažení tohoto výsledku se místo lineární stupnice využívá logaritmická stupnice.

K definici logaritmické stupnice existují dva přístupy, u-Law a a-Law. u-Law je přístup, který se nejčastěji používá v Severní Americe a Japonsku, zatímco a-Law se vyskytuje spíše v jiných zemích. Nyní, když lze efektivněji měřit amplitudy pulzní modulace, se přiřadí k těmto vzorkům čísla.

V tomto okamžiku se hlas převede na řadu jedniček a nul. Podle pana Nyquista je zapotřebí odebrat 8 000 vzorků za sekundu. Každý vzorek používá 8 bitů.

8 000 vzorků za sekundu * 8 bitů za sekundu = 64 000 bitů za sekundu (to je 64 kb/s).

Tento výpočet udává, že je možno přenášet digitalizovaný hlas pomocí šířky pásma 64 kb/s. Kromě skutečného hlasu je však třeba přenášet i informace v hlavičkách paketů. Šířka pásma 64 kb/s představuje pouze hlasový provoz [3, 23].

4.6 Kvalita řeči ve VoIP

V době kdy se na poli klasických analogových sítích začaly objevovat technologie, které měly za úkol tyto klasické sítě nahradit, se začalo používat pojem kvalita hlasu, kvalita řeči. Tyto nové technologie byly založeny na mnoha typech vlastností spojení dvou koncových účastníků: mobility účastníků, kvalita služeb, levnější volání, přínos nových služeb atd. Kvalita služeb je úzce spjata s kvalitou řeči, který převažuje hlavně v sítích VoIP. Telefonování po internetu je dnes již zaběhlým standardem, ale i tak dochází ke zdokonalování komunikace mezi uživateli po celém světě a termín kvalita hovoru je stále klíčovou záležitostí [7,10].

Kvalitu řeči mohou ovlivňovat následující faktory[7,10]:

- Ozvěna
- Věrnost reprodukce zvuku
- Proměnlivé zpoždění (jitter)
- Ztráta paketů
- Vedlejší tón
- Hluk na pozadí

4.6.1 Definice kvality řeči

Termín kvalita řeči je velmi komplexní problém. Z tohoto důvodu je velmi obtížné definovat tento termín. Ať už je definována a vyhodnocována jakákoliv stupnice hodnocení kvality řeči, pro každého jedince bude vnímání této škály vždy subjektivní a nemusí se s ní ztotožnit. Je docela možné, že identický jedinec bude ten samí signál hodnotit různě v různou dobu. Na jeho hodnocení mají vliv okolnosti typu nemoc, dříve přehrávaný signál, nálada, okolní prostředí atd. Proto je téměř nemožné označit promluvu (úsek hovorového signálu) konkrétním ohodnocením, které bude pro každého za všech okolností stejné.

Doporučení ITU-T P.10 viz [11] upravuje terminologii měření kvality hlasu. V tomto doporučení se dají nalézt jednotlivé termíny související s měřením kvality přenosu hlasu a jejich stručnou charakteristiku. ITU-T P.10 má za cíl zabránit nesrovnalostem v interpretaci naměřených hodnot bez návaznosti na metody měření, které byly použity k jejich získání.

MOS je hodnotící systém pro kvalitu hlasu. Skóre MOS je generováno, když posluchači vyhodnocují předem nahrané věty, které jsou zpracovány různými způsoby, například kompresními algoritmy. Existuje několik druhů stupnic, které jsou definovány v doporučení ITU-Z P.800 viz [12]. Výběr stupnice závisí na typu prováděného experimentu. Nejpoužívanější stupnicí je stupnice kvality poslechu, která je popsána v tabulce 4.4.2. Tato stupnice má pětibodovou škálu s pevným celočíselným rozsahem 1,2,3,4 a 5, kdy 1 je nejhorší a 5 je nejlepší ohodnocení hlasového signálu. Každá hodnota je popsána slovním ohodnocením, které je přesně definované a neměnné. V některých případech je možné uvést zkrácená jednoslovná hodnocení. Toto hodnocení se označuje mean listening-quality opinion score, zkráceně Mean Opinio Score. Kombinací prvních písmen slov dostaneme označení jednotky MOS [10,22].

MOS	Kvalita	Popis
5	Vynikající	Neznamenatelné rušení
4	Dobrá	Rušení lze rozpoznat, ale není obtěžující
3	Průměrná	Rušení lze rozpoznat a mírně obtěžuje.
2	Nízká	Rušení obtěžuje, je nutno vyvinout úsilí při snaze porozumět.
1	Špatná	Rušení velmi obtěžuje, řeč je nesrozumitelná.

4.4.2. Hodnoty stupnice MOS [10]

Pro hodnocení kvality hovoru lze rozlišit tři základní kategorie. První kategorií je kvalita poslechu hodnocená uživatelem a je závislá především na použitém kódování. Dalším hlediskem je kvalita konverzace, kde se posuzuje schopnost vést rozhovor, zde se uplatňují vlivy jako je echo a zpoždění. Třetí kategorií je kvalita přenosu, která je vztažena ke schopnosti sítě přenášet hlas.

Každý průchod telekomunikační sítí generuje snižování kvality. Mezi základní jevy ovlivňující kvalitu hlasu patří zpoždění (delay), ozvěna (echo) a samozřejmě ztrátovost paketů (packet loss) v případě VoIP. Samozřejmě už při samotném kódování dochází k degradaci původního řečového signálu. V tabulce 4.4.3. jsou vypsány nejpoužívanější kodeky ve VoIP s jejich maximální naměřenou hodnotou MOS skóre [7,10,22].

Kodek	Datový tok [kbit/s]	MOS skóre
ITU-T G.711	64	4,2
iLBC	15,2	4,14
ITU-T G.729	8	3,92
GSM EFR	12,2	3,8
ITU-T G.729a	8	3,7
ITU-T G.728 LD-CELP	16	3,61
ITU-T G.729 x2	8	3,27
ITU-T G.729 x3	8	2,68

4.4.3. Maximální MOS skóre jednotlivých kodeků [10]

4.6.2 Měření kvality řeči

K určení kvalitu signálu lze používat několik metod, například:

- MOS (Mean Opinion Score)
- PSQM (Perceptual Speech Quality Measurement)
- PESQ (Perceptual Evaluation of Speech Quality)

Primárně se tato část zabývá metodou MOS.

MOS skóre se získává na základě testování vzorků (vzorku) řeči. Tyto testy se realizují pomocí již hotových metod. Tyto metody se dělí na dva základní typy. První typ testu se provádí za pomoci matematických algoritmů, nazývají se objektivní testy. Druhým typem jsou testy subjektivní, které jsou hodnoceny na základě několika testujících subjektů. Velkou nevýhodou subjektivních testů je náročná příprava měření, zdlouhavé měření a vlastní vyhodnocení. Jsou také velmi finančně náročné.

Každý testující subjekt se může zúčastnit měření pouze jednou, proto subjektivní metody potřebují mít k dispozici dostatečně velké množství testovacích subjektů. Každý subjekt nesmí být informován o jevech, které bude posuzovat. Pokud tyto základní podmínky nejsou splněny, může dojít ke zkreslení výsledků.

Na rozdíl od subjektivních metod mají objektivní metody několik výhod. Jednou z hlavních výhod je možnost kontinuálního běhu a vyhodnocování testu. Objektivní testy nejsou tak přesné jako subjektivní, protože nelze nahradit testování pomocí reálných subjektů. Primárně jsou určené k detekci zhoršení kvality hovoru a mají doplňkový informační charakter [7,10].

Objektivní metody měření, viz metodika práce.

4.6.3 Měření kvality přenosu - subjektivní metody

Základem subjektivních metod jsou konverzační a poslechové testy, během nichž posluchači hodnotí kvalitu přehrávaných sekvencí. Pro vyhodnocování subjektivních testů existují různé metodiky[10]:

- ACR (Absolute Category Rating)
- Quantal-Response Detectability Tests
- DCR - Degradation Category Rating method
- CCR - Comparison Category Rating Method
- The threshold method

Nejpoužívanější vyhodnocovací metodou je ACR. Tato metoda využívá ve svém principu přímé hodnocení kvality řeči tak, že každé testované poslechové sekvenci je testujícím subjektem přiřazeno hodnocení na stupnici MOS. MOS je v rozsahu od 1 do 5. Další test Quantal-Response Detectability Tests je využíván hlavně pro testování prahových úrovní. Metoda DCR je modifikovaná metoda ACR, pro své účely používá degradovaný a nedegradovaný signál (poslechovou sekvenci), a testuje, jak moc je degradace výrazná. Její hlavní využití je v systémech s převažující dobrou kvalitou. Metoda CCR je modifikovaná metoda DCR. Metoda The threshold method je využívána pro komparaci dvou systémů, kdy se hodnotí signály z porovnávaného a testovaného systému. Předmětem testu je pouze zjištění, který signál je lepší. Podrobnější informace o těchto metodách je možné nalézt v doporučení P.800 [12].

Nespornou výhodou těchto subjektivních testů jsou jejich výsledky, které lze považovat za téměř přesné. Pokud je zvolen dostatečně veliký soubor testerů (testující subjekty) a výstup ze statistického zpracování naměřených dat bude mít vysoký interval spolehlivosti, může být výsledek považován za referenční hodnoty, kterého nelze dosáhnout žádným jiným způsobem.

K testování existují dva typy přístupů. K poslechovému testu není v podstatě potřeba testovaný systém, protože se v tomto testu hodnotí jedna nebo více vlastností, které jsou specifické a dají se v systému izolovat (typickým příkladem je šum, rušení signálu typu výpadky paketů, harmonické zkreslení, diskontinuity fáze při navazování obnovených segmentů řeči, saturace řečového signálu atd.).

Při konvenčním testování se test provádí v rámci celého systému, kdy se hlasový signál degraduje všemi rušivými signály, které nelze zcela odstranit, ale jednotlivé rušivé vlivy se dají pouze cíleně eliminovat (typický příklad je odstraňování echa). Ve výsledném kvalitativním skóre se poté uplatní i všechna ostatní rušení (doba šíření, sidetone). S tímto je nutné počítat při zpracování výsledků [10].

4.6.4 Subjektivní testy

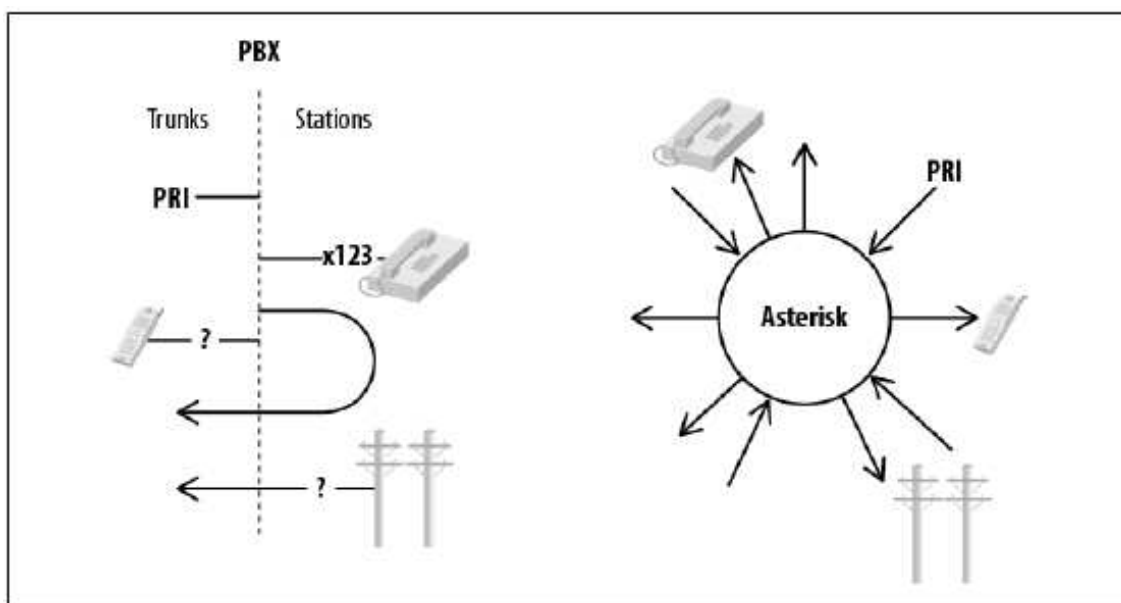
Doporučení ITU-T P.800 a ITU-T P.830 – viz. [14] - definují podmínky, které je nutno dodržet během realizace subjektivních testů. V prvním jmenovaném doporučení jsou definovány zejména požadavky vztahující se k vlastní realizaci testů. Doporučení obsahuje požadavky na testované subjekty, včetně instruktážních pokynů pro testované subjekty, a na testované prostředí. Dále obsahuje doporučení minimálního počtu posluchačů účastnících se poslechového testu. Druhé jmenované doporučení, ITU-T P.830 je zaměřeno hlavně na přípravu testovacích signálů, promluv pro poslechové testy. Toto doporučení dále definuje počet a výběr mluvčích, a způsob, jak se mají pořizovat a upravovat testovací signály (promluvy), které jsou určeny pro testování (vzorkování, úroveň signálu, formát dat atd.) [10].

4.7 Softswitch Asterisk

Asterisk (open source hybrid TDM and packet voice PBX) patří do skupiny softwarových pobočkových ústředen. Je velmi odlišný od jiných více tradičních pobočkových ústředen. Jeho dialplán ošetřuje v podstatě všechny příchozí kanály stejným způsobem. V tradiční PBX je logický rozdíl mezi stanicemi (telefonní přístroje) a trunky (zdroje, které se připojují k vnějšímu světu). To znamená např., že nelze nainstalovat externí bránu na port stanice a směrovat externí hovory bez nutnosti, aby nejdříve uživatel musel vytočit číslo pobočkové ústředny. Také koncept off-site zdroje (jako je recepce) je mnohem obtížnější na tradiční PBX, protože systém nedovolí externím prostředkům přistupovat k interním funkcím. Asterisk navíc nabízí naváděný automatický odpovídač (IVR – Interactive Voice Response), který je ovládán většinou tónovou volbou, nebo hlasem. Navíc obsahuje ACD systém automatického rozdělování hovoru dle stanovených pravidel [2,4].

Asterisk na druhé straně nemá vnitřní koncept trunků a stanic. V Asterisku vše, co přijde do systému nebo vyjde ze systému, prochází kanálem, který může být různého druhu. Existuje mnoho druhů vysílání, nicméně dialplán Asterisku zpracovává všechny kanály

podobným způsobem. To znamená, že interní uživatel může existovat na konci trunku (například mobilní telefon) a připojí se podle dialplánu přesně stejným způsobem jako uživatel na vnitřní síti. Porovnání klasické PBX architektury vs. Asterisk viz. obrázek 4.18. [2,4]



4.4.17. PBX architektura vs. Asterisk [2]

4.7.1 Moduly

Asterisk je postaven na modulech. Modul je zatížitelná komponenta, která poskytuje specifické funkce, například ovladač kanálu (`chan_sip.so`), nebo prostředek, který poskytuje připojení k externím technologiím (`func_od.bc.so`). Moduly Asterisk jsou definovány v `/etc/asterisk/modules.conf`. Asterisk je možné spustit bez jediného modulu, ale v tomto stavu nebude schopen nic dělat [2].

Typy modulů [2]:

- Bridging modules
- Call detail recording (CDR) modules
- Channel event logging (CEL) modules
- Channel drivers
- Codec translators
- Format interpreters
- Dialplan functions
- PBX modules
- Resource modules
- Addons modules
- Test modules

4.7.2 Struktura souborů

Asterisk je složitý systém, který se skládá z mnoha zdrojů. Tyto zdroje využívají souborového systému několika způsoby. Vzhledem k flexibilitě Linuxu je dobré pochopit, kde jsou uloženy konkrétní typy dat (hlasové zprávy, log soubory, atd.) [2].

- Konfigurační soubory
- Moduly
- Zdrojové knihovny
- Spool
- Logování

4.7.3 Dialplán

Dialplán je srdcem Asterisku. Všechny kanály, které vstupují do systému, jsou zpracovány prostřednictvím dialplánu, který obsahuje *call-flow* skripty, které určují jak zpracovat příchozí hovor. Dialplán může být zápsán jedním ze tří způsobů: [2]

- Tradiční dialplán Asterisku v */etc/asterisk/extensions.conf*
- Asterisk Extension Logic (AEL) v */etc/asterisk/extensions.ael*
- LUA v */etc/asterisk/extensions.lua*

4.7.4 Hardware

Asterisk je schopen komunikovat s obrovským množstvím různých technologií. Obecně platí, že tato spojení jsou zajištěna prostřednictvím síťového připojení. Nicméně spojení do tradičních telekomunikačních technologií, jako je PSTN (Public Switched Telephone Network), vyžadují specifický hardware. Tento hardware vyrábí mnoho společností (Digium, Sangome, Rehino, OpenVox, atd.). Autoři preferují karty od Digium a Sangome, nicméně nabízené produkty od jiných výrobců hardwaru mohou být vhodnější pro konkrétní řešení. Digium je hlavním vývojářem, sponzorem a majitelem Asterisku [2].

4.8 QoS (Quality of Service)

Quality of service je termín k definování schopnosti sítě poskytovat různé úrovně zajištění služeb různým formám provozu na síti. Toto umožňuje síťovým administrátorům přiřadit určitou prioritu daného typu provozu nad ostatní. Typická síť může mít jednu nebo více z následujících datových vrstev, pro které je povoleno QoS [24]:

- Frame Relay
- Ethernet
- Token Ring
- Point-to-Point Protocol (PPP)
- HDLC
- X.25
- ATM
- SONET

QoS byl dříve spojován pouze s definováním výkonnostních charakteristik pro přenos dat po síti. V současnosti se toto nevztahuje pouze k přenosu dat po síti, ale stejně tak i ke koncovému systému. Každá aplikace má jinou kvalitu servisních požadavků. Například pro aplikaci VOD (Video on demand) lze tolerovat mírné end-to-end zpoždění, ale vyžaduje vysokou propustnost a velmi nízkou chybovost. Oproti tomu VoIP potřebuje velmi nízké end-to-end zpoždění, ale toleruje horší propustnost a chybovost než je přijatelné VOD [24,25].

4.8.1 Aplikace QoS

V jakém okamžiku by se měla začít brát v úvahu kvalita služeb v síti? Následuje několik důvodů, proč nasadit QoS v topologii sítě [24]:

- Pokud chceme upřednostnit některé kritické aplikace před ostatními.
- Pro maximalizaci využití existujících investic do infrastruktury sítě
- Lepší výkon pro aplikace citlivé na zpoždění jako jsou hlas a video
- Chceme-li reagovat na změny v datovém provozu sítě

Nejjednodušším řeším přehlcení šířky pásma je navýšení šířky pásma připojení. V dnešní době gigabit ethernetu a optických sítí to není takový problém. Nicméně tímto přístupem se odsuzujeme k vyšším nákladům na provoz a není to vhodný přístup. Lepší je provést analýzu provozu sítě, definovat kritické protokoly a aplikace a na tomto základu vybudovat strategii nasazení řízení kvality služeb. QoS umožňuje správci sítě mít kontrolu nad šířkou pásma, zpoždění a jitter, a tím minimalizovat ztrátu paketů v rámci sítě [24,25].

4.8.2 Úrovně QoS

QoS je možné rozdělit do tří různých úrovní, jako modely služeb. Tyto modely popisují sady možností nastavení end-to-end QoS. End-to-end QoS je schopnost sítě poskytovat určitou úroveň služeb pro provoz v síti z jednoho konce na druhý. Úrovně QoS [24,25] :

1. Best-Effort Service

Služba nejlepšího úsilí zaručuje vynaložení veškerých možností sítě, aby paket dorazil na místo určení. Daná aplikace může posílat data v jakémkoliv množství, kdykoliv to potřebuje, bez nutnosti povolení nebo oznámení sítě. Některým aplikacím toto může vyhovovat (např. FTP a http). Naopak není vhodné pro aplikace, které jsou citlivé na zpoždění sítě, kolísání šířky pásma, a další měnící se podmínky v síti. Kolísání těchto parametrů by mohlo v případě VoIP vést k neúspěšnému hovoru, nebo k přerušení hovoru [24,25].

2. Integrated Services

Integrovaný model služeb poskytuje aplikacím garantovanou úroveň služeb tím, že vyjednává jednotlivé parametry přenosu sítí. Aplikace vždy žádá o potřebnou úroveň služeb, tak aby mohla bez problémů fungovat, a spoléhá na rezervační mechanismus QoS. Je důležité si uvědomit, že aplikace nezahájí síťovou komunikaci, dokud neobdrží signál, že jsou pro ni rezervovány požadované síťové prostředky.

K dosažení tohoto cíle je využíván proces řízení přístupu. Řízení přístupu je mechanismus, který brání síť před přetížením. Síť nebude přenášet signál pro zahájení provozu aplikace,

pokud dané pakety, řízené QoS, nemohou být doručeny. Jakmile aplikace zahájí přenos dat, vyhrazené síťové prostředky jsou udržovány po celou dobu provozu, nebo dokud rezervovaná šířka pásma přesahuje šířku pásma provozu aplikace. Síť bude zajišťovat své úkoly pro údržbu stavu toku dat, klasifikaci, dohled a inteligentní řízení paketových front pro splnění nastavených QoS [24,25].

3. Differentiated Service

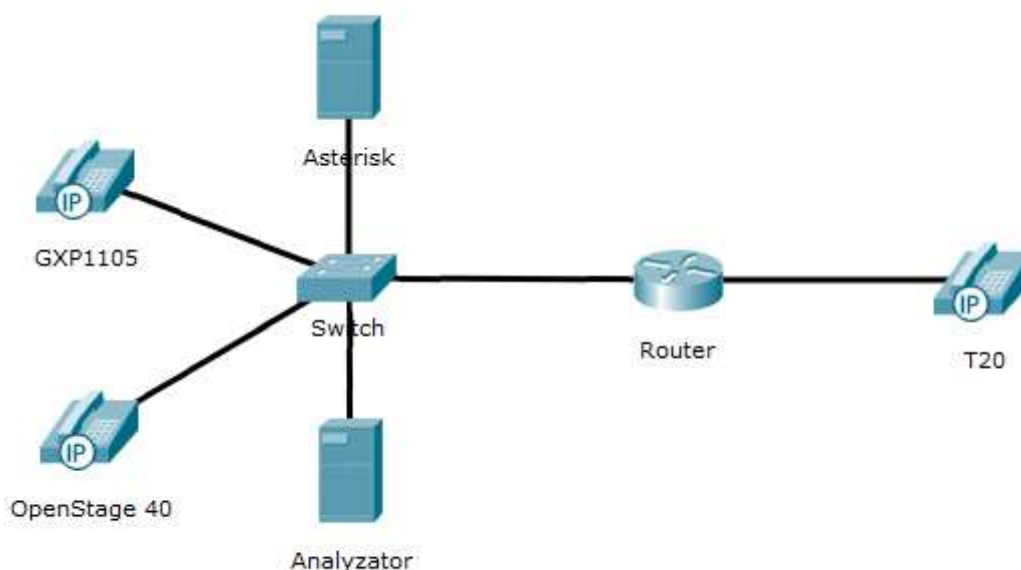
Posledním modelem pro QoS je model diferencovaných služeb. Diferencované služby zahrnují sadu klasifikačních mechanismů řazení do fronty, aby poskytly některým protokolům, nebo aplikacím přednost před ostatním síťovým provozem. Diferencované služby spoléhají na routery, které provádějí klasifikaci různých typů paketů procházejících sítí. Síťový provoz může být klasifikován prostřednictvím síťové adresy, protokolu nebo portu [24,25].

5 Praktická část

Praktická část se zabývá měřením kvality přenosů VoIP hovoru jednotlivých kodeků. Samotnému měření předchází definice a konfigurace laboratoře, které je nezbytná pro měření. Na základě změřených hodnot je vytvořeno schéma pro optimální nasazení VoIP prostřednictvím standardu BPMN 2.0.

5.1 Příprava laboratoře

Pro měření kvality hovoru byla postavena laboratoř skládající se ze dvou IP telefonů (Grandstream GXP1105 a Siemens OpenStage 40), softwarové telefonní ústředny a stanice, na které jsou k dispozici aplikace pro analýzu. Všechna tato zařízení jsou propojena PoE přepínačem (PoE – napájení IP telefonů). Výše zmíněná zařízení demonstrují LAN (Local area network). Tato síť je připojena ke směrovači, na jehož druhé straně je připojen třetí IP telefon (Well SIP-T20), který se tváří jako připojený z WAN sítě. Tento směrovač slouží k oddělení LAN a WAN a dále prostřednictvím aplikace netem (Network Latency and Packet Loss Emulation) generuje zatížení sítě. Viz schéma na obrázku 5.1.

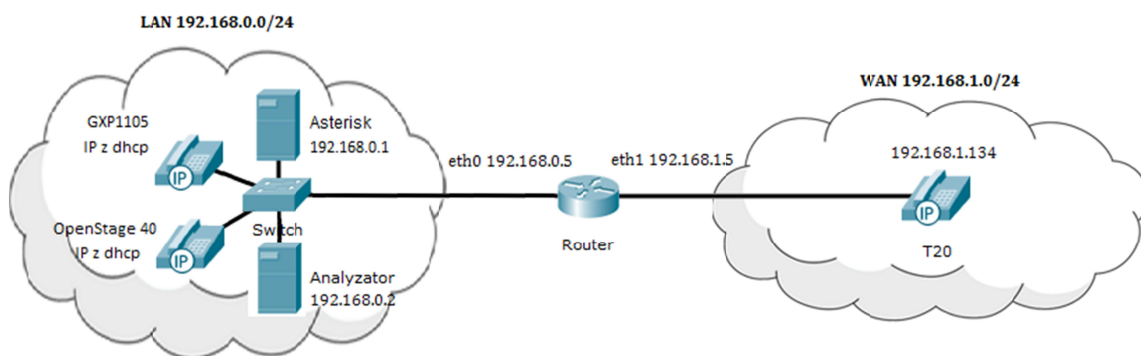


5.1. Schéma zapojení laboratoře

Pro realizaci telefonní ústředny byla použita open-source aplikace Asterisk verze 13.7.1. Tato aplikace je nainstalována na nejnovější stabilní verzi Linuxové distribuce Ubuntu 14.04.3server edition. Zároveň na tomto serveru je nainstalována DHCP server, který přiřazuje IP adresy všem IP telefonům v LAN. Asterisk server a server pro analýzu mají statickou adresu. Na stejné Linuxové distribuci je nakonfigurován směrovač.

V Asterisku je třeba nadefinovat číslovací plán, SIP účty 6000, 6001 a 6002 a povolit všechny dostupné kodeky.

LAN část laboratoře je v rozsahu 192.168.0.0 s maskou 255.255.255.0 (/24). V této síti mohou být zařízení pouze s adresami 192.168.0.1 – 192.168.0.254. Z tohoto důvodu má Asterisk server IP adresu 192.168.0.1 a server pro analýzu 192.168.0.2. IP telefonům přiřadí adresu dhcp server s range 50 – 150. WAN část laboratoře je v rozsahu 192.168.1.0 s maskou 255.255.255.0 (/24). Tento rozsah adres ve veřejné síti neexistuje, ale pro laboratorní účely to nevadí, protože laboratoř není připojena k internetu. Směrovač má dvě síťové karty, logicky označené eth0 a eth1. Port eth0 je připojen k LAN s adresou 192.168.0.5 a port eth1 představuje WAN s adresou 192.168.1.5. Telefon na straně WAN má statickou IP adresu 192.168.1.134, viz schéma IP adres.

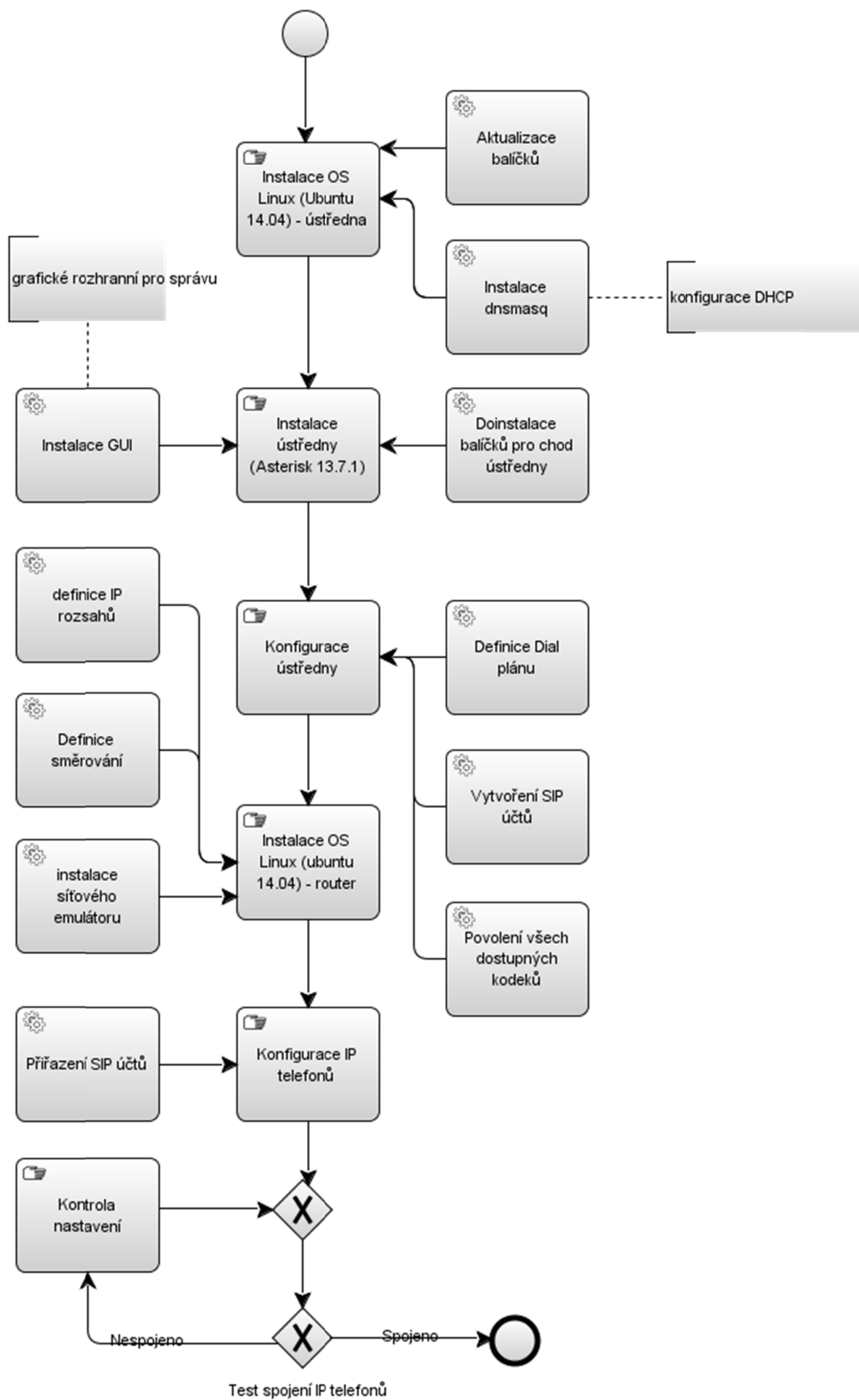


5.2. Schéma IP adres laboratoře

IP telefony jsou konfigurovány skrze jejich webové rozhraní, jejich přiřazené IP adresy jsou zapsány v souboru `/var/lib/misc/dnsmasq.leases`. Každému telefonu je potřeba nakonfigurovat:

- SIP účet,
- SIP heslo,
- SIP server (adresa Asterisku),
- Povolit vybrané kodeky.

Správnost nastavení se ověří testem spojení mezi jednotlivými telefony. Proces tvorby a instalace laboratoře je znázorněn na BPMN schématu, obrázek 5.2.



5.3. Příprava laboratoře

5.1.1 Popis procesu přípravy laboratoře

- Instalace OS Linux (Ubuntu 14.04)
 - Po instalaci OS následuje aktualizace balíčků:
 - `apt-get update`
 - `apt-get upgrade`
 - Následuje instalace role DHCP:
 - `apt-get install dnsmasq`
 - Konfigurace role DHCP. Do souboru `/etc/dnsmasq.conf` zapíšeme:
 - `dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h`
- Instalace ústředny (Asterisk 13.7.1)
 - Instalace balíčků pro Asterisk 13.7.1
 - `aptitude install gcc g++ oxygen libncurses5-dev libssl-dev libxml2`
 - `apt-get install uuid-dev libjansson-dev libsqlite3-dev`
 - Stažení a instalace Asterisku:
 - `wget`
`http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz`
 - `tar -xzf asterisk-13-current.tar.gz`
 - `./configure`
 - `make`
 - `make install`
 - `make samples`
 - `make config`
 - Instalace GUI:
 - `svn checkout http://svn.digium.com/svn/asterisk-gui/branches/2.0`
 - `./configure`
 - `make`
 - `make install`
 - `make checkconfig`
 - Po instalaci je nutný restart serveru.

➤ Konfigurace ústředny

- Upravení souboru `/etc/asterisk/http.conf`:
 - `enabled=yes`
 - `bindaddr=0.0.0.0`
 - `bindport=8088`
 - `enablestatic=yes`
- Upravení souboru `/etc/asterisk/manager.conf`:
 - `[general]`
 - `enabled=yes`
 - `webenabled=yes`
 - `[admin]`
 - `secret=admin`
 - `read=system,call,log,verbose,agent,user,config,dtmf,reporting,cdr,dialplan`
 - `write=system,call,user,agent,config,command,reporting,originate,message`
- Vytvoření dialplánu pro lokální volání a definování rozsahu SIP účtů.
- Vytvoření SIP účtů 6000,6001 a 6002
- Povolení kodeků u-law, a-law, GSM, ILBC, SPPEX, G.726, ADPCM, LPC10, G.729, G.723, H.263, H.263p,H.264

➤ Instalace routeru

- Základní balíčky – viz. instalace OS Linux výše mimo dhcp
- Definice IP rozsahů
 - LAN rozsah 192.168.0.0/24, port na routeru eth0 192.168.0.5
 - WAN rozsah 192.168.1.0/24, port na routeru eth1 192.168.1.5
- Definice směrování
 - `ip addr add 192.168.0.5/24 dev eth0`
 - `ip addr add 192.168.1.5/24 dev eth1`
- Obsah směrovací tabulky
 - `192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.5`
 - `192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.5`
- Instalace síťového emulátoru (ne tem)

- apt-get instar tc-netem.gz
- Konfigurace IP telefonů
 - Povolení DHCP v telefonu
 - Nastavení skrze webové rozhraní.
 - SIP účet
 - codeky
- Test spojení IP telefonů
 - Kontrola spojení s ústřednou viz obrázek 5.3.
 - Zkušební telefonní hovor mezi telefony

The screenshot shows the Asterisk web interface. On the left, the 'Extensions' section is active, displaying a table of SIP users. On the right, the 'System Info' section is visible, showing system details like hostname and OS version.

Status	Trunk	Type	Username	Port/Hostname/IP
Extensions [-]				
All Analog IAX SIP ● Free ● Ringing ● Busy ● UnAvailable				
Extension	Name/Label	Status	Type	
6000	6000	Messages : 0/0	SIP User	
6001	6001	Messages : 0/0	SIP User	
6002	6002	Messages : 0/0	SIP User	
-- *No Extension assigned	Check Voicemails		VoiceMailMain	
-- *No Extension assigned	Dial by Names		Directory	

Parking Lot [-]			
Caller ID	Channel	Extension	Timeout
No Parked Calls			

System Info [-]			
General	Network	Memory	Disk
Hostname: Asterisk			
OS Version: Linux Asterisk 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux			

5.4. Stav připojených SIP účtů

5.2 Měření kvality přenosů VoIP

Měření slouží pro výběr kodeku, který bude použit pro optimální nastavení VoIP nasazení, a to z toho důvodu, že kodek výrazně ovlivňuje kvalitu a výkonnost této technologie. Nekvalitní kodek může přinést nízké zatížení sítě a může se zdát, že je vše v pořádku, ale poslechová kvalita služby bude na nízké úrovni.

Měření kvality přenosů VoIP je založeno na objektivním přístupu. Kdy pro vlastní měření byl použit software Commview 6.5 [26], dostupný s licencí freeware. Pro měření byly vybrány kodeky u-law, a-law, G.726-32, G.729 a G.723. Kde u-law a a-law jsou někdy prezentovány jako pcmu a pcma. Tyto kodeky jsou výsledkem průniku podporovaných kodeků mezi ústřednou a dostupnými IP telefony viz tabulka č. 5.1. , kdy kodek musí být

podporován ústřednou a dvěma typy telefonů. Tyto jsou zároveň nejvíce používanými kodeky mezi bezplatnými.

Pro každý kodek bylo provedeno celkem pět měření. A to pro originální, nezkrácený signál a pro uměle degradovaný signál ztrátovostí paketů. Toto zkrácení bylo nastaveno na hodnoty ztráty paketů 1%, 2.5%, 5%, 10%, 15% a 20 %.

Ztrátovost paketů se v net em nastaví pomocí příkazu `# tc qdisc add dev eth0 root netem loss 1%` nebo změna nastavené hodnoty příkazem `# tc qdisc change dev eth0 root netem loss 2,5%`. Po zadání příkazu se změna nastavení projeví ihned.

Měření bylo prováděno pouze v jednom směru z A do B. RTP pakety spojení byly zachytávány na portu směrovače eth0. Tento port byl zrcadlen na port serveru pro analýzu. Tím byl zajištěn průchod degradujícím článkem naší laboratoře.

Aterisk	OpenStage 40	GXP1105	T20
u-law	G.711	G.723.1	pcmu
a-law	G.729	G.729A/B	pcma
GSM	G.722	Pcmu	G.729
ilbc		Pcma	G.722
speex		G.726-32	G.723_53
g.726		G.722 (wideband)	G.723_63
adpcm		Ilbc	G.726_16
lpc 10			G.726_24
G.729			G.726_32
G.723			G.726_40
H.263			
H.263p			
H.264			

5.1. Podporované kodeky

5.2.1 Měření

Následují změřené hodnoty pro jednotlivé typy kodeků a různé úrovně degradace originálního signálu. A to pro 0%, 1%, 2.5%, 5%, 10%, 15% a 20 % ztrátovosti paketů s 5% odchylkou ztrátovosti.

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	1,91	0	4	78,2
G.726-32	0,94	0	4,2	86,2
G.729	0,69	0	4,1	83,2
pcma	0,44	0	4,4	93,2
pcmu	0,83	0	4,4	93,2

5.2. Originální signál

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	1,85	14 (1,1%)	3,8	74
G.726-32	0,09	16 (1,0%)	3,9	78,1
G.729	0,6	14 (1,0%)	4	78,6
pcma	0,11	16 (1,0%)	4,2	84,4
pcmu	0,15	11 (0,9%)	4,2	85,7

5.3. 1% ztrátovost paketů

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	0,17	33 (2,4%)	3,6	69,5
G.726-32	0,09	26 (2,5%)	3,5	68,9
G.729	0,1	70 (2,4%)	3,7	72,7
pcma	0,15	37 (2,6%)	3,8	73,4
pcmu	0,1	30 (2,4%)	3,8	74,7

5.4. 2,5% ztrátovost paketů

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	1,82	80 (4,9%)	3,2	62,5
G.726-32	0,12	126 (5,0%)	2,9	57,1
G.729	0,11	117 (5,3%)	3,3	63,1
pcma	0,1	68 (5,1%)	3,2	61,3
pcmu	0,11	81 (4,8%)	3,2	62,3

5.5. 5% ztrátovost paketů

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	0,24	169 (10,7%)	2,6	50,4
G.726-32	0,14	176 (9,9%)	2,2	42,4
G.729	0,11	155 (10,4%)	2,6	51
pcma	0,1	139 (10,2%)	2,3	45,2
pcmu	0,61	199 (9,7%)	2,4	46,5

5.6. 10% ztrátovost paketů

Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	0,19	338 (15,2%)	2,2	43,7
G.726-32	0,09	228 (15,1%)	1,7	33,2
G.729	0,12	474 (15,4%)	2,2	42,8
pcma	0,13	425 (14,7%)	1,9	36,6
pcmu	0,13	353 (15,1%)	1,9	36,1

5.7. 15% ztrátovost paketů

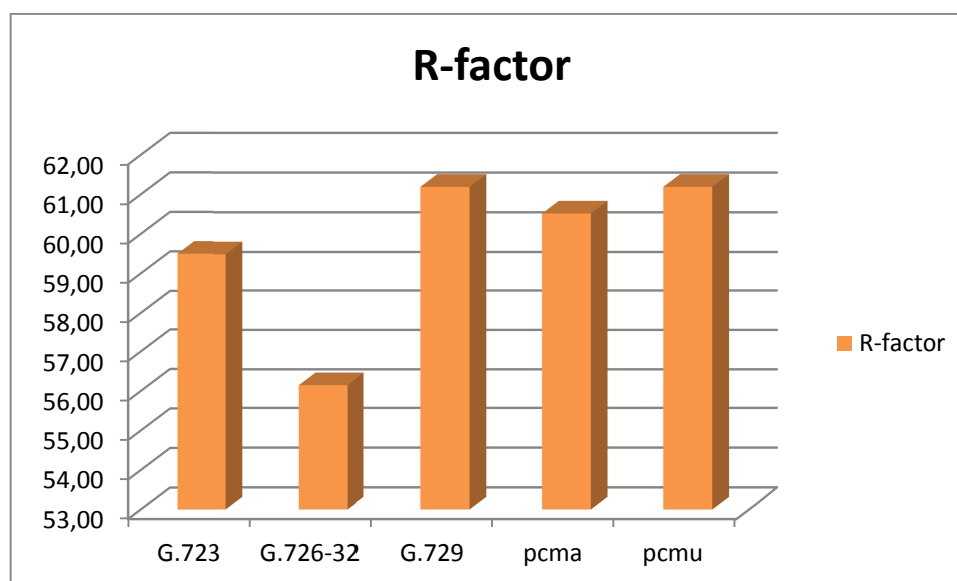
Kodek	Max Jitter (ms)	Lost Packets	MOS Score	R-factor
G.723	0,18	266 (20,0%)	2	38,2
G.726-32	0,11	291 (20,3%)	1,5	27,2
G.729	0,14	567 (20,2%)	1,9	37
pcma	0,08	240 (20,3%)	1,6	29,6
pcmu	0,12	1083 (20,0%)	1,6	29,9

5.8. 20% ztrátovost paketů

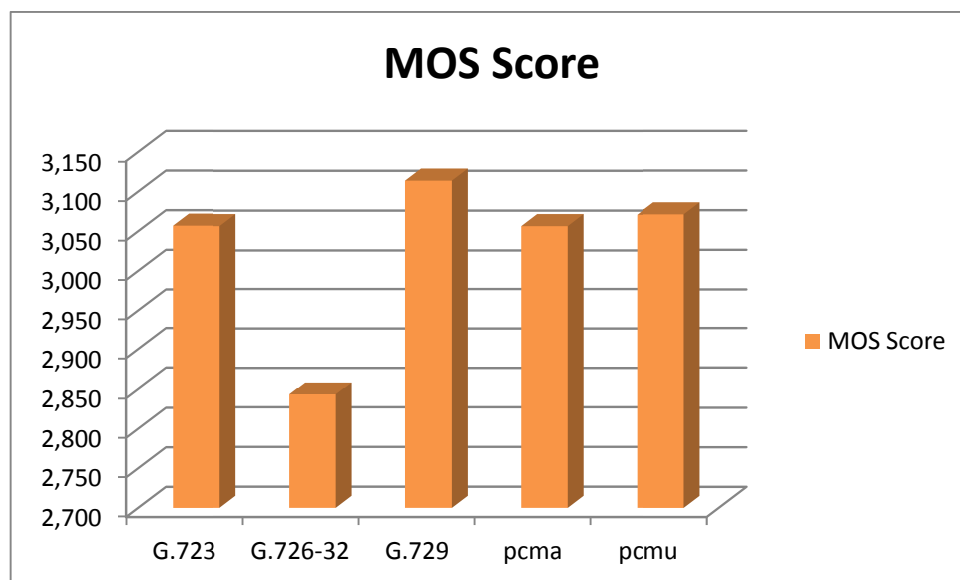
Kodek	Max Jitter (ms)	MOS Score	R-factor
G.723	0,91	3,057	59,50
G.726-32	0,23	2,843	56,16
G.729	0,27	3,114	61,20
pcma	0,16	3,057	60,53
pcmu	0,29	3,071	61,20

5.9. Průměrné hodnoty MOS a R-faktor

Na grafech 5.5 a 5.6 jsou znázorněny výsledné hodnoty z tabulky 5.9, které byly vypočítány jako prostý průměr změřených hodnot s nastavenou ztrátovostí paketu 0%, 1%, 2.5%, 5%, 10%, 15% a 20 % pro jednotlivé kodeky.



5.5. Průměrně dosažený R-Factor



5.6. Průměrně dosažené MOS scóre

Na základě pořadí vypočtených hodnot R-faktoru a MOS skóre jsme zjistili výsledné pořadí kodeků dle kvality přenosu hlasového signálu - viz tabulka 5.10.

Kodek	MOS Score	R-factor	Výsledné pořadí
G.729	1	1	1
pcmu	2	1	2
pcma	3	3	3
G.723	3	4	4
G.726-32	5	5	5

5.10. Výsledné pořadí kodeků

Na ústředně lze nastavit prioritu 5 kodeků pro jednotlivé SIP účty. Toto zjištěné pořadí tudíž definuje prioritu nasazených kodeků.

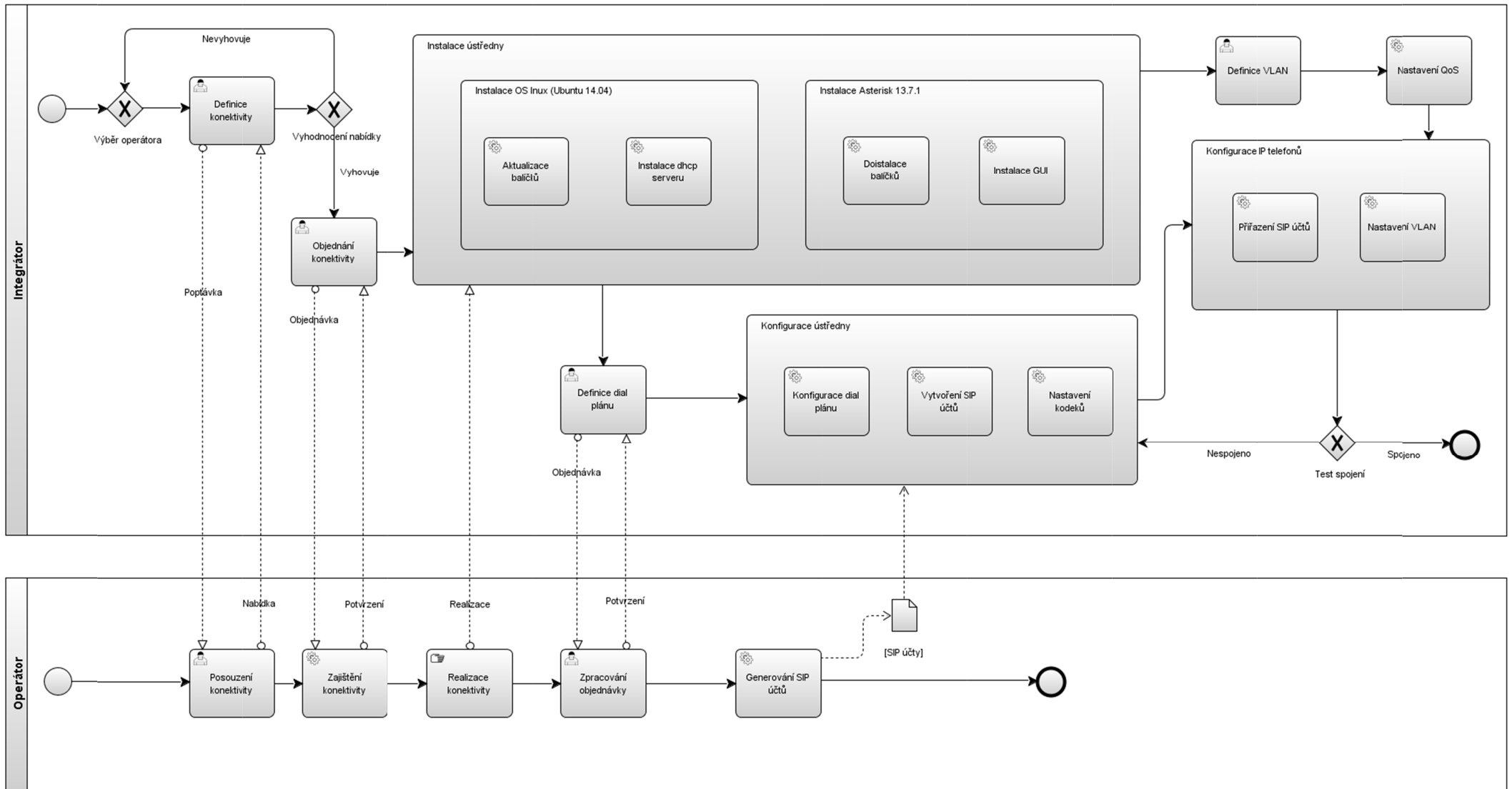
5.3 BPMN schéma nasazení VoIP technologie

Pro použití VoIP je nezbytné kvalitní a stabilní internetové připojení. Pro tyto účely je nutné neagregované a synchronní připojení s minimálně 99% garantované dostupnosti. Na základě počtu používaných telefonů a použitých kodeků (každý kodek zabírá různou šířku pásma) je potřeba definovat dostatečně velikou šířku pásma. Je zbytečné volit 100% z násobku šířky pásma kodeků a počtu telefonů, protože reálný provoz je mezi 10% a 20%. Jako dostačující proto bude připojení 30% požadované šířky pásma. Management výkonnosti VoIP je silně závislý na použitých kodecích. Ty totiž nejvíce ovlivňují kvalitu služby VoIP.

Instalace ústředny a Asterisku je shodné s již nainstalovanou ústřednou pro laboratorní účely. Rozdíl je pouze v nadefinovaném číselném plánu a SIP účty je nutno zajistit u poskytovatele telefonní služby. Poskytovatel dodá zároveň i číselný plán.

Je vhodné, aby provoz VoIP byl v LAN oddělen od ostatní provozu. Toho lze docílit nastavením VLAN pro tuto službu. Dále je vhodné nastavit QoS ve třídě 1 (Best-Effort Service). Díky této třídě bude VoIP komunikace mít přednost před ostatním provozem (http, HTTPS, FTP, atd.).

Konfigurace IP telefonů může být provedena ručně, nebo prostřednictvím provisioning serveru. Toto je závislé na počtu telefonů.



5.7. BPMN schéma implementace VoIP

6 Závěr

Jako první byla zpracována kritická literární rešerše týkající se VoIP technologie, se zaměřením, na měření kvality VoIP přenosů. Záležitost měření kvality VoIP přenosů je velmi komplexní a rozsáhlá. Díky této skutečnosti se práce zabývá pouze objektivními metodami, subjektivní metody jsou velmi náročné na přípravu (potřeba velkého počtu testerů, přesně definovaná testovací místnost atd.).

Pro účely měření byla vytvořena laboratoř, jejíž nezbytnou součástí byl generátor zatížení sítě. Simulována byla pouze ztrátovost paketů, šlo by simulovat i jiné negativní vlivy na přenos hlasového signálu.

Pro měření bylo vybráno 5 dostupných kodeků (u-law, a-law, G.723, G726-32 a G.729). Kodeků je mnohem více, ale výběr byl omezen dostupnými IP telefony a samotná ústředna nepodporuje všechny známé kodeky v bezplatné verzi. Na základě provedeného laboratorního měření byly stanoveny jednotlivé hodnoty R-faktoru a MOS skóre pro vybrané kodeky a hladiny ztrátovosti paketů 0%, 1%, 2.5%, 5%, 10%, 15% a 20 %. Z těchto hodnot byly vypočteny prosté průměry pro vybrané kodeky a srovnáním bylo stanoveno pořadí priorit nasazení těchto kodeků. A to v pořadí G.729, u-law, a-law, G.723 a G.726-32. Při reálném nasazení je nezbytné, aby ústředna i nasazené IP telefony tyto kodeky podporovaly.

Z výše provedené analýzy byl vytvořen procesní diagram zavedení VoIP technologie v praxi. Prvotní složkou je zajištění odpovídající a stabilní konektivity, zajištění číslovacího plánu u operátora. Další je instalace a konfigurace softswitche, konfigurace IP telefonů na základě dodaných SIP účtů a zjištěného pořadí kodeků. V neposlední řadě je vhodné oddělit VoIP provoz od ostatních služeb v síti pomocí VLAN a tento provoz privilegovat pomocí nastavení QoS. Poslední složkou je testování správnosti konfigurace celého řešení.

7 Použitá literatura

- [1] HARTPENGE, Bruce. *Packet Guide to Voice over IP: A system administrator's guide to VoIP technologies*. 1 vydání. O'Reilly Media, 2013. 242 s. ISBN 978-1449339678.
- [2] MADSEN, Leif, MEGGELEN Jim Van - BRIANT Russel. *Asterisk: The Definitive Guide*. 3 vydání. O'Reilly Media, 2011. 738 s. ISBN 978-0-596-51734-2.
- [3] WALLACE, Kevin. *VoIP bez předchozích znalostí*. 1 vydání. Brno: Computer Press, 2007. 232 s. ISBN 978-80-251-1458-2.
- [4] VOZŇÁK, Miroslav. *Voice over IP*. 1 vydání. OSTRAVA: VŠB – TECHNICKÁ UNIVERZITA OSTRAVA, 2008. 176 s. ISBN 978-80-248-1828-3.
- [5] VOZŇÁK, Miroslav. *VoIP Voice over IP and Jitter Avoidance on Low Speed Links*. International Conference Research in Telecommunication Technology. Žilina. 2002. ISBN 80-227-1934-X
- [6] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. 1. vydání. Brno: Computer Press. 2012. 288 s. ISBN 978-80-251-3718-5
- [7] WALLACE, Kevin. *Cisco VoIP Autorizovaný výukový průvodce*. 1 vydání. Brno: Computer Press, 2009. 527 s. ISBN 978-80-251-2228-0.
- [8] VOZŇÁK, Miroslav. *QoS Adaptation in Voice over IP*. International Conference Research in Telecommunication Technology. Brno, 2001. ISBN 80-214-1938-5
- [9] VOZŇÁK, Miroslav. *Výpočet šířky pásma pro hovor v sítích s protokolem IP*. IV. Seminář EaTT. Ostrava VŠB-TU, 2001. ISBN 80-248-0031-4
- [10] BRADA, Miroslav; ZELENKA Jan. *Posuzování kvality hlasu*. Kongresové centrum hotelu Olšanka, 2008. 64 s. (PDF) [cit. 2015-9-15]. Dostupné WWW: <http://www.ip-telefon.cz/data/download/40.pdf>
- [11] ITU-T P. 10: Vocabulary of terms on telephone transmission quality and telephone sets, 1998.
- [12] ITU-T P.800: Methods for subjective determination of transmission quality, 1996. CCITT: Handbook on Telephony, Geneva, 1992.

- [13] ITU-T P.862: Perceptual Evaluation of Speech Quality (PESQ): An Objective Method for End-to-end Speech Quality Assessment of Narrow-band Telephone Networks and Speech Codecs, 2001.
- [14] ITU-T P.830: Subjective Performance Assessment of Telephone-Band and Wideband Digital Codecs, 1996.
- [15] VOZŇÁK, Miroslav; ZUKAL David. *Vyhodnocení kvality hovoru pomocí R-faktoru v sítích VoIP*. 11 s. (PDF) [cit. 2015-8-5]. Dostupné z WWW: <<http://homel.vsb.cz/~voz29/files/voz49.pdf>>
- [16] ITU-T Recommendation G.107 (2003), The E-model, a computational model for use in transmission planning
- [17] Information about a new method for deriving the transmission rating factor R from MOS in closed form, ITU - Telecommunication Standardization Sector Temporary Document XX-E WP 2/12, Geneva, 27-31 May 2002
- [18] *Business Process Model and Notation*, 508 s. (PDF) [cit. 2015-10-4]. Dostupné z WWW: <<http://www.omg.org/spec/BPMN/2.0/PDF/>>
- [19] AHMED, Adeel; MADANI, Habib; SIDDIQUI, Talal. *VoIP Performance Management and Optimization*. 1 vydání. Indianapolis: Cisco Press, 2010. 448 s. ISBN 978-1-58705-528-7
- [20] PISKAČ, Richard. *Měření kvality hovoru v IP telefonii*. Praha, 2009. 96s. Diplomová práce. České vysoké učení technické, Fakulta elektrotechnická.
- [21] LAMMLE, Todd, *CCNA výukový průvodce*. 1 vydání. Brno: Computer Press, 2015. 1016 s. ISBN 978-80-251-4602-6
- [22] VOZŇÁK, Miroslav; ZUKAL David. *Kvalita hovoru v prostředí VoIP*. 9 s. (PDF) [cit. 2015-11-5]. Dostupné z WWW: <http://www.phonet.cz/archiv/dok_cizi/Cesnet_kvalita_hovoru.pdf>
- [23] BOULET, Benoit. *Fundamentals of Signals and System*. 1 vydání. Boston: Course Technology. 2005. 689 s. ISBN 9781584503811
- [24] FLANNAGAN, Michael E.; DURAND, Benoid. *Administering CISCO QoS for IP Networks*. 1. vydání. USA: Syngress Publishing. 2000. 561 s. ISBN 9780080481890

[25] SANJAY, Jha; MAHBUD, Hassan, *Engineering Internet QoS*. . 1. vydání. USA: Artech House. 2002. 346 s. ISBN 9781580535663

[26] SW Commview 6.5. dostupné z www 28.2.2016
<<http://www.tamos.com/download/main/index.php>>

8 Přílohy

8.1 Ukázka měření

The screenshot displays the CommView - Evaluation Version interface. The main window shows a table of RTP Streams with the following data:

Src IP	Dest IP	Src Port	Dest Port	Start Time	End Time	Duration	RTP Pa...	Avel...	Total Traffi...	Max J...	Lost Pa...	MOS S...	R-Factor	Duplic...	Sequen...
? 192.168.0.1	? 192.168.0.150	19812	5004	16:05:25	16:05:25	0:00:00.0	2	49.17	428	0.89	0	4.4	93.2	0	0
? 192.168.0.83	? 192.168.0.150	5010	5004	16:05:25	16:05:46	0:00:21.3	1069	83.63	228 766	0.83	0	4.4	93.2	0	0
? 192.168.0.150	? 192.168.0.1	19812	19812	16:05:25	16:05:47	0:00:21.3	36	3.37	9 216	2.41	0	4.4	93.2	0	0
? 192.168.0.150	? 192.168.0.83	5004	5010	16:05:26	16:05:46	0:00:20.4	1026	83.85	219 564	5.03	0	4.4	93.2	0	0
? 192.168.0.1	? 192.168.0.150	19004	5004	16:11:05	16:11:05	0:00:00.0	2	47.77	428	0.95	0	4.4	93.2	0	0
? 192.168.0.150	? 192.168.0.1	5004	19004	16:11:05	16:11:21	0:00:15.6	64	8.16	16 384	4.69	0	4.4	93.2	0	0
? 192.168.0.83	? 192.168.0.150	5010	5004	16:11:05	16:16:17	0:05:12.3	1630	5.79	231 528	1.02	0	4.1	83.2	0	0
? 192.168.0.150	? 192.168.0.83	5010	5010	16:11:06	16:16:17	0:05:11.4	1529	6.95	277 184	1.67	0	4.1	83.2	0	0
? 192.168.0.1	? 192.168.0.150	18048	5004	16:16:00	16:16:00	0:00:00.0	2	28.91	148	0.00	0	4.1	83.2	0	0
? 192.168.0.150	? 192.168.0.1	5004	18048	16:16:01	16:16:01	0:00:00.2	15	28.91	1 110	0.48	0	4.1	83.2	0	0

The detailed RTP Stream view shows the following information:

- Transport Information:** Src IP: 192.168.0.150, Src Port: 5004, Dest IP: 192.168.0.83, Dest Port: 5010, Protocol: UDP.
- Timing:** Start Time: 28.2.2016 16:05:26, End Time: 28.2.2016 16:05:46, Duration: 0:00:20.4.
- Packet Details:** Packet No, Time, SSRC, Seq..., RTP Times..., Payload Name, Jitter (ms), Marker, Content.

At the bottom of the window, the status bar shows: Capture: On, Pkts: 387 in / 1560 out / 5931 pass, Auto-saving: Off, Rules: Off, Alarms: Off, 3% CPU Usage.

8.1. Ukázka měření

8.2 Image systému ústředny Asterisk

Image je dostupná na přiloženém DVD. Soubor s názvem server.bz2.