

Domáci VoIP ústředna s připojením do GSM sítí

Home VoIP platform with GSM interface

Martin Ludík

Bakalářská práce
2009



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav aplikované informatiky

akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin LUDÍK**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační technologie**
Téma práce: **Domácí VOIP ústředna s připojením do GSM sítě**

Zásady pro vypracování:

1. Prostudujte systém VOIP serveru Asterisk.
2. S použitím GSM brány nebo GSM telefonu připojeného ke zvukové kartě realizujte propojení VOIP serveru se sítí GSM.
3. Nakonfigurujte VOIP server dle následujícího zadání: Předpokládejte, že máte SIM kartu s tarifem pro neomezené bezplatné volání mezi členy rodiny (např. T-Mobile Rodina), známé jako virtuální privátní síť (dále jen VPN). Nastavte směrování hovorů tak, aby při volání z čísla z rozsahů čísel VPN, které jsou zdarma, VOIP server hovor přijal a přes vytočení klapky nechal volajícího uživatele zavolat kamkoli dál přes síť VOIP, popř. přes další GSM zařízení, instalované v systému.
4. Prostudujte možnost následující: při volání z GSM čísla člena rodiny, které je mimo rozsah VPN, by mohl Asterisk vyhodnotit, jestli náhodou pro volání člen-Asterisk neexistuje levnější spojení než toto GSM (např. přes VOIP nebo přes jinou GSM SIM kartu) a pokud existuje, tak hovor odmítnout, zavolat členovi zpátky a sestavit hovor nejlevnější a neoptimálnější cestou.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. JIM, Van Meggelen, LEIF, Madsen, JARED, Smith. Asterisk : The Future of Telephony. Mike Loukides; Robert Romano and Jessamzn Read. 2nd enl. edition. Sebastopol : O'Reilly Media, 2007. xxv, 574 s. ISBN 978-0-596-51048-0.
2. SYSEL, Martin. Operační systémy GNU/Linux. 1. vyd. Zlín : Univerzita Tomáše Bati Academia centrum, 2006. 77 s. ISBN 80-7318-489-3.
3. Asterisk :: The Open Source PBX & Telephony Platform [online]. Digium, Inc, c2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.asterisk.org> .
4. [IpTelWikil] : Asterisk PBX [online]. [2005] , 2008/10/31 [cit. 2009-01-30]. Dostupný z WWW: <https://sip.cesnet.cz/cs/start> .
5. Celliax: eigenbau GSM anbindung per Daten/Audiokabel Asterisk Allgemein [online]. 2000-2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.ip-phone-forum.de/showthread.php?t=142983> .
6. V100 - GSM VoiP ATA brána, 1x WAN, 1x FXS, 1x PSTN, 1x SIM, H.323/SIP [online]. c2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.i4wifi.cz/?cls=stoitem&stiid=1156> .
7. ICamp SIP server [online]. [2006] [cit. 2009-01-30]. Dostupný z WWW: <http://sip.icamp.eu> .

Vedoucí bakalářské práce:

Ing. Tomáš Dulík

Ústav aplikované informatiky

Datum zadání bakalářské práce:

20. února 2009

Termín odevzdání bakalářské práce:

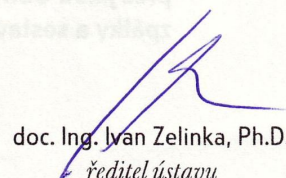
27. května 2009

Ve Zlíně dne 13. února 2009



prof. Ing. Vladimír Vašek, CSc.

děkan



doc. Ing. Ivan Zelinka, Ph.D.

ředitel ústavu

ABSTRAKT

Bakalářská práce je zaměřena na téma možnosti použití serveru Asterisk ve spojení s GSM bránou. Vymezuje problematiku propojení VPN GSM sítí s VoIP systémem. Umožňuje služby směrování hovorů s minimálními náklady na spojení.

Klíčová slova:

Asterisk, telefonie, IP telefonie, hlasové služby, směrování hovorů, propojení GSM, levné volání, nízké náklady, privátní síť.

ABSTRACT

This bachelor thesis is focused on using Asterisk server in conjunction with a GSM gate. It deals with the problem of interfacing VPN GSM networks with a VoIP system. Our solution routes the calls between GSM and fixed/VOIP lines in a way which guarantees minimal or no fees/charges for the user's phone bill.

Keywords:

Asterisk, telephony, IP telephony, voice services, call routing, GSM, cheap calling, low cost, private networks.

Na tomto místě je mou milou povinností poděkovat Ing. Tomáši Dulíkovi za vedení této práce. Dále děkuji firmám HS Logic s r.o. Přerov za poskytnutí potřebného hardware a firmě Emos s r.o. Přerov za poskytnutí infrastruktury. Nejvíce však děkuji mé manželce Pavlíně za její trpělivost, bez které by tato práce nevznikla.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval.

V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	11
1 VOIP, SIGNALIZAČNÍ A TRANSPORTNÍ PROTOKOLY	12
1.1 VYMEZENÍ POJMU IP TELEFONIE	12
1.2 PŘENOS HLASU V SÍTÍCH IP	12
1.3 PŘENOS SIGNALIZAČNÍCH INFORMACÍ V SÍTÍCH IP	13
1.4 VOICE OVER IP	13
1.5 SIGNALIZAČNÍ PROTOKOL H323	14
1.5.1 Standard H.323	14
1.5.2 Prvky H.323	14
1.5.3 Koncepce komunikace v H.323	14
1.6 SIGNALIZAČNÍ PROTOKOL SIP	15
1.6.1 Vlastnosti SIPu	15
1.6.2 Adresace	15
1.6.3 SIP proxy server	15
1.6.4 Metody a odpovědi	16
1.6.4.1 Typy požadavků	16
1.6.4.2 Typy odpovědí	17
1.6.5 Důležité hlavičky SIP	18
1.6.6 Navázání a ukončení spojení	18
1.7 SIGNALIZAČNÍ PROTOKOL IAX	19
1.7.1 IAX obecně	19
1.7.2 Přednosti IAX oproti SIP/RTP	19
1.7.3 Rámce protokolu IAX	19
1.7.4 Adresace	20
1.8 TRANSPORTNÍ PROTOKOL RTP	20
1.8.1 Popis RTP	20
1.8.2 Šifrovaný přenos SRTP	21
1.8.3 Protokol ZRTP	21
1.8.4 Tóny DTMF v RTP	21
1.9 KODEKY	21
1.9.1 Kvalita hovoru v interakci s VoIP	22
1.9.2 Používané kodeky	22
2 VOIP SERVER ASTERISK	24
2.1 CO JE ASTERISK?	24
2.1.1 Vlastnosti Asterisku	24
2.1.2 Doplnkové služby	24
2.1.3 Rozhraní a kanály	25
2.1.4 Instalace Asterisku	26
2.1.5 Konfigurace	26
2.1.6 Ovládání	26

2.2	KONFIGURACE A UKÁZKY NASTAVENÍ	27
2.2.1	Context a extension.....	27
2.2.2	Práce s řetězci.....	28
2.2.3	Konfigurace účtů	29
2.2.4	Základní konfigurace.....	29
II	PRAKTICKÁ ČÁST.....	31
3	PŘIPOJENÍ GSM ROZHRANÍ K ASTERISKU	32
3.1	SOUNDWIN - V100	32
3.1.1	Konfigurace V100 pro připojení k Asterisku	32
3.1.2	Konfigurace ústředny Asterisk pro použití brány V100.....	37
3.2	VOICEBLUE - 2N.....	38
3.2.1	Doplnění konfigurace VoiceBlue brány	38
3.2.2	Nastavení ústředny Asterisku s VoiceBlue.....	39
4	POUŽITÍ VPN SÍTĚ A SERVERU ASTERISK.....	40
4.1	SMĚROVÁNÍ HOVORŮ ČLENŮ VPN.....	40
4.1.1	VPN volání mezi uživateli	40
4.2	SCHÉMA ROUTOVACÍHO ALGORITMU ÚSTŘEDNY	40
4.3	ZAPOJENÍ TESTOVACÍ HW ČÁSTI SERVERŮ ASTERISK	41
4.4	TESTOVACÍ ZAPOJENÍ TELEFONNÍ SÍTĚ.....	42
4.5	ZÁKLADNÍ NASTAVENÍ SMĚROVÁNÍ HOVORŮ	43
4.5.1	Konfigurace účtů	44
4.5.1.1	Konfigurace sip.conf.....	44
4.5.1.2	Konfigurace iax.conf.....	45
4.5.2	Číslovací plán v souboru <i>extensions.conf</i>	46
4.5.2.1	Odchozí volání.....	46
4.5.2.2	Příchozí volání	47
4.5.2.3	Normalizace čísel z GSM sítě.....	47
4.5.2.4	Ověření VPN mobilního uživatele	48
4.5.2.5	Hlasové menu	48
4.5.2.6	Ověření neznámého uživatele	49
5	ALTERNATIVA VOLÁNÍ UŽIVATELŮ MIMO VPN ROZSAH.....	50
5.1	SPOJENÍ MEZI HOSTITELSKÝMI ÚSTŘEDNAMI	50
5.1.1	ENUM.....	50
5.2	VYUŽITÍ ENUMU MIMOROZSAHOVÉ VPN	51
5.3	NASTAVENÍ ASTERISKU POUŽITÍ ENUM / VPN	52
5.3.1	Odchozí volání.....	52
5.3.2	Příchozí volání	52
5.4	MOTIVACE ENUM.....	52
	ZÁVĚR	53
	ZÁVĚR V ANGLIČTINĚ	CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.
	SEZNAM POUŽITÉ LITERATURY	55

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	57
SEZNAM OBRÁZKŮ.....	58
SEZNAM TABULEK	59

ÚVOD

Voice over IP (VoIP) je technologie, která významně ovlivnila oblast telekomunikací a pokud bychom hledali podobné milníky evoluce telefonie, tak bychom IP telefonii mohli postavit na stejnou úroveň jako digitalizaci. Přenášet hlas v paketových sítích má své nesporné výhody, které jsou ve dvou rovinách. Jednak je to využití jediné přenosové infrastruktury a tím zefektivnění jejího užití a jednak zavedení nových pokročilých služeb, které v klasické přepínané telefonní síti jsou podstatně složitěji realizovatelné anebo zcela nemožné. Každopádně pohlížíme na telefonii jako na službu v sítích s protokolem IP a hovoříme o IP telefonii jako o aplikaci, která využívá standardní transportní protokoly Internetu.

Dal jsem si za cíl využít těchto možností VoIP, a realizovat přenosovou infrastrukturu propojenou s mobilními sítěmi GSM operátorů se vzájemným provázáním koncových uživatelů těchto sítí jako možnost zavedení nových pokročilých služeb. Snažil jsem se dosáhnout co nejmenší pořizovací ceny použitého hardware a nízké nebo nulové náklady na provoz při zachování patřičného komfortu při používání telefonních služeb. Jako pokrokovou technologii k zavádění nových služeb jsem použil také technologii doménových záznamů ENUM.

V tomto textu je několikrát zmíněn open source projekt Asterisk. Jednou je použit přívlastek „ústředna Asterisk“, podruhé „server Asterisk“. Vycházel jsem z praxe, kdy pro služby týkající se hlasových služeb se více hodí název ústředna, kdežto pro služby spojené s IP a sítěmi spíše název server. Obojí je správně, protože Asterisk je server poskytující služby telefonní ústředny.

I. TEORETICKÁ ČÁST

1 VOIP, SIGNALIZAČNÍ A TRANSPORTNÍ PROTOKOLY

V současnosti je klasická telefonní služba stále více nahrazována řešením na bázi IP telefonie, označené často anglickou terminologií Voice over IP - VoIP. Vzniká velké množství nových operátorů, ať už se jedná o velké a zavedené telekomunikační společnosti, které své portfolio služeb rozšiřují o VoIP, nebo o společnosti lokálního významu, které nabízejí připojení k síti Internet a hlasovou službu vidí spíše jako doplňkovou [23].

Pro přenos hlasu se používá na třetí vrstvě OSI modelu protokol IP, na čtvrté vrstvě protokol UDP (někdy i TCP). [8].

Díky levnému přenosovému médium jménem Internet lze pomocí implementace relativně jednoduchých signalizačních protokolů a pravidel vytvořit systémy vzájemně hlasově propojených uživatelů.

1.1 Vymezení pojmu IP telefonie

IP telefonii chápeme jako službu založenou na technologii VoIP (Voice over IP), která umožňuje přenos hlasu v sítích s přepojováním paketů založených na protokolu IP. VoIP tak tvoří další alternativu ke klasické telefonii, založené na použití sítí s přepojováním okruhů přes veřejnou telefonní síť. Tato alternativa je velice perspektivní a to hned z několika důvodů. Datové sítě se v současnosti rozvíjejí a šíří mnohem rychleji než telefonní síť. Přenos hovorů v datových sítích je ekonomicky výhodný, protože rozsáhlé a geograficky rozdělené společnosti mohou uskutečňovat hlasový provoz po vlastních datových sítích, jimiž většina společností disponuje. Připojení operátora poskytujícího na IP konektivitu i hlasové služby logicky vede k nižším cenám, neboť jsou redukovány náklady na komunikační infrastrukturu.

Dalším aspektem IP telefonie jsou nové aplikace a doplňkové služby využívající informační technologie. Právě v propojení s oblastí IT je ukrytý dosud nevyužívaný potenciál IP telefonie. Další důvod zavádění VoIP je snaha o sjednocení komunikačních standardů a vytvoření sítí s integrovanými službami, které jsou schopny nad jedinou infrastrukturou přenášet data, hlas nebo video [9].

1.2 Přenos hlasu v sítích IP

V sítích s protokolem IP se hlas přenáší v paketech RTP (Real Time Protocol), které na transportní vrstvě používají protokol UDP (User Datagram Protocol) a na síťové vrstvě protokol IP. Výjimkou je pouze protokol IAX, který má vlastní řešení přenosu hlasových paketů. Formát RTP paketu je dán doporučením IETF z roku 1996 s označením RFC 1889/1890 pro RTP/RTCP, přičemž RTP řeší vlastní přenos hlasové informace a RTCP (Real Time Control Protocol) je kontrolní mechanismus pro RTP.

Hlavička IP 20 oktetů	Hlavička UDP 8 oktetů	Hlavička RTP 12 oktetů	Užitečná informace 20 až 160 oktetů
--------------------------	--------------------------	---------------------------	--

Tab. 1 – Paket RTP a jeho hlavičky (40 oktetů)

Na obrázku je znázorněn formát paketu RTP a je možné si všimnout, že užitečná informace má omezenou velikost v rozsahu 20 až 160 oktetů. Důvodem je fakt, že pakety s menší velikostí způsobují mnohem menší zpoždění na směrovačích při odesílání do WAN sítí [9].

1.3 Přenos signalizačních informací v sítích IP

Obdobně, jako v sítích s přepínáním okruhů, je každý hovor provázen signalizačními informacemi při sestavení spojení v jeho průběhu a ukončení. V sítích s protokolem IP se signalizační informace mohou přenášet v transportních protokolech UDP nebo TCP. Tak vzniká otázka, kterému transportnímu protokolu dát přednost. V sítích IP se používá více protokolových modelů, a to H.323, SIP nebo IAX.

V případě protokolu SIP je to opravdu jedno, protože je schopen signalizační informace variabilně přenášet na obou protokolech dle konfigurace daného zařízení, ale standardně používaný je protokol UDP, konkrétně port UDP **5060** [9], [10], [11].

H.323 využívá obou protokolů UDP i TCP pro signalizační informace k hovoru, standardně na portu UDP **1719** a případně i na **1718**, hovorová signalizace spojení se přenáší na portu TCP **1720**. Protokolový model H.323 je robustní a je precizně navržen, pro výrobce zařízení VoIP znamená ovšem jeho složitost komplikaci a v praktických implementacích se využívá zhruba 10 % jeho možností a mnohem blíže je tvůrcům aplikací protokol SIP [9], [13].

Protokol Inter Asterisk Exchange IAX získává v poslední době na důležitosti. Jeho nejčastějším využitím je propojení IP telefonních ústředěn. Komunikuje pouze na jediném UDP portu, včetně hlasového přenosu, a tím je obvykle **4569**. Jeho specifikace do značné části odporuje trendům, které striktně oddělují signalizační a hovorová data. Paradoxně právě proto je tak často nasazován [12].

Existují i jiné méně rozšířené protokoly jako je třeba MGCP (Media Gateway Control Protocol) a další.

1.4 Voice over IP

Jak už bylo zmíněno výše, pro přenos hlasu se používá na třetí vrstvě OSI (Open System Interconnection) modelu protokol IP, na čtvrté vrstvě protokol UDP (User Datagram Protocol). V těle jednotlivých UDP datagramů se kromě dalších údajů přenáší malý úsek telefonního hovoru, zakódovaný podle určitého algoritmu k dosažení úspory objemu přenášených dat. Kódovací a dekodovací algoritmy, zkráceně kodeky, mají různá označení (G. 711, G.722, G.723, G.726, G.729, iLBC, T38, ..) a jsou standardizovány a v mnoha případech i patentovány.

Kromě UDP datagramů, nesoucích v paketech protokolu RTP zapouzdřené úseky vlastního hovoru, zahrnuje VoIP přenos ještě další pakety. Jsou to např. STUN (Simple Traversal UDP through NAT), ICE (Interactive Connectivity Establishment) nebo TURN (Traversal Using Relay NAT) určené pro techniky tunelování NATu (překlady síťových adres). Dalšími pakety jsou ICMP (Internet Control Message Protocol) a popř. pakety TCP (Transmission Control Protocol). Ty řídí přenos, nesou telefonní signalizaci, ověřují dostupnost komunikujících zařízení atd.

Rozbor protokolů samozřejmě nekončí na čtvrté vrstvě. Jak bylo naznačeno, na páté vrstvě obsahují hovorové UDP datagramy protokol RTP (Real Time Protocol) a ten teprve ve své datové části obsahuje zakódované kousky hovoru (obvykle 20 nebo 30 ms fragmenty).

Celá rodina VoIP protokolu není jediná, ale má řadu variant (implementací), lišících se podle standardu, použitého pro VoIP spojení [8].

Zajímavým protokolem je IAX2 – preferovaný protokol softwarové ústředny Asterisk. Obecně lze říct, že má podobný přenos hovoru pomocí proudu krátkých úseků nesených v RTP, ale liší se ve službách a signalizaci.

1.5 Signalizační protokol H323

1.5.1 Standard H.323

Standard H.323 od ITU-T byl prvním doporučením, které popisovalo komunikaci v paketových sítích. Od roku 1995 urazil Internet závratný kus cesty a H.323 se dostala do své známé poslední verze 6 z roku 2006. Vývoj stále pokračuje, v roce 2009 má vyjít již sedmá verze H.323v7 [13].

1.5.2 Prvky H.323

Prvky sítě H.323 tvoří koncové body EP (endpoints) a řídicí prvky GK (GateKeeper). Množina EP registrovaná ke stejnému GK tvoří zónu. Zónu můžeme chápat jako logickou oblast spravovanou GK, v jedné zóně nemůžeme provozovat více GK [13].

GK je řídicím prvkem H.323 koncových bodů (terminal, gateway, ...). Dle standardu musí zajišťovat následující:

- Podporu signalizace RAS (Registration/Administration/Status), která realizuje řízení přístupu k prostředkům sítě
- Řízení přístupu (Admission Control), zajišťuje autorizovaný přístup
- Překlad adres (Address Translation) mezi E-164 číslem a sítovou adresou
- Řízení přidělování kapacity pásma (Bandwidth Control)
- Řízení spojení (Call Control)
- Řízení zón (Zone Management)

1.5.3 Koncepce komunikace v H.323

Hovor je přenášen na RTP/RTCP protokolech. RTP přenáší hovor a RTCP přenáší stavové a řídicí informace. Signalizace, s výjimkou RAS, je přenášena spolehlivě přes TCP. Následující protokoly se zabývají signalizací:

- RAS – řídí registraci, přístup a stav
- Q.931 – řídí nastavení volání a jeho ukončení
- H.245 – určí využití kanálu a jeho kapacitu

Jak již bylo uvedeno, v případě H.323 jsou signalizační informace k hovoru dány doporučením H.225.0, které využívá obou protokolů UDP i TCP. Standardně řídicí prvek sítě (Gatekeeper) naslouchá signalizaci H.225.0/RAS na portu UDP 1719 a případně i na 1718 (pro multicast 224.0.1.41), hovorová signalizace spojení H.225.0/Q.931 se přenáší na portu TCP 1720. Navíc je tu další část signalizace dle ITU-T H.245 pro vyjednávání

parametrů audio/video, která je postavena na TCP. Od verze H.323v2 je pomocí metody Fast Connect schopná většinu informací přenést v H.225.0/Q.931 [13].

1.6 Signalizační protokol SIP

1.6.1 Vlastnosti SIPu

SIP byl vyvíjen od roku 1996 v rámci IETF (Internet Engineering Task Force). V roce 1999 byl předložen ve formě navrhovaného standardu (Proposed Standard) v RFC 2543. Téhož roku na popud IETF vznikla nová pracovní skupina, nazvaná příznačně SIP (Session Initiation Protocol), která převzala vývoj hlavního jádra protokolu. Její práce v květnu roku 2002 vyústila v nový standard RFC 3261. SIP je signalizační protokol pracující na aplikační vrstvě. Tento protokol byl navržen tak, aby byl snadno implementovatelný, rozšiřitelný a dostatečně flexibilní. Specifikace je dostupná ve formě několika doporučení RFC. Nejdůležitější je RFC3261, jež obsahuje jádro protokolu. Protokol je užíván pro sestavení, modifikaci a ukončení spojení s jedním nebo více účastníky.

SIP není jediný protokol, který je potřebný pro komunikující zařízení. Ve spojení se SIPem jsou nejčastěji používány ještě dva další protokoly, RTP a SDP (Session Description Protocol). RTP protokol je užíván k přenosu multimédií v reálném čase (real-time). Tento protokol umožňuje přenášet hlas nebo video v paketech pomocí IP [13].

1.6.2 Adresace

SIP je vázán k doméně, což respektuje adresace. Uživatel existuje v konkrétní doméně, kterou obsluhuje SIP proxy server. SIP entity jsou identifikovány použitím SIP URI (Uniform Resource Identifier). SIP URI má formát:

sip:user@host:porturi-parameters

Jak můžeme vidět, SIP URI se skládá z části user a z části host, obě části jsou oddělené znakem @. SIP URI je podobná e-mailové adrese, je doporučeno používat stejnou adresu pro e-mail i SIP, takže URI může být snadné si zapamatovat. Část user identifikuje uživatele v doméně prezentované v části host, která může být zadána pomocí jména nebo IP adresy. Pokud není uvedeno číslo portu, tak se předpokládá použití všeobecně známého portu 5060. Parametry mohou nést další volitelné informace. Doménová část URI je adresována s využitím DNS, což dává adresaci vysokou flexibilitu [10], [13].

1.6.3 SIP proxy server

SIP umožňuje vytvořit infrastrukturu sítě hostitelů nazývaných jako proxy server. Koncové terminály (UA – User Agents) mohou odesílat zprávy na proxy server. Proxy servery jsou důležité entity v SIP infrastruktuře, zajišťující směrování žádostí o spojení dle aktuálního umístění adresáta, autentizaci, účtování a spoustu dalších důležitých funkcí. Nejdůležitější úloha proxy serveru je směrovat žádosti o sestavení spojení blíž k volanému. Při inicializaci sestavení spojení bude obvykle prohledávat řadu proxy serverů, dokud

nenajde nějaký, který zná aktuální umístění volaného. Pak proxy přesměruje žádost o spojení přímo k volanému a volaný akceptuje nebo odmítne žádost o spojení [10], [13].

Jedním z mnoha proxy serverů, kterým je i softwarová ústředna Asterisk umožňující tyto služby, se budeme zabývat v této práci.

1.6.4 Metody a odpovědi

Komunikace užívající SIP (signalizaci) je tvořena zprávami, které jsou obvykle přenášeny v samostatných UDP datagramech. Každá zpráva obsahuje hlavičku zprávy (header) a vlastní obsah (body). V prvním řádku zprávy je identifikován její typ. Známe dva typy zpráv:

- žádost (metoda)
- odpověď

Žádosti jsou obvykle užívány k inicializaci procedury (sestavení, ukončení spojení) nebo oznamují příjemci požadavek na něco. Odpovědi jsou užívány k potvrzení, že žádost byla přijata a zpracována a obsahuje stav zpracování [10], [11], [13].

Příklad části SIP zprávy INVITE

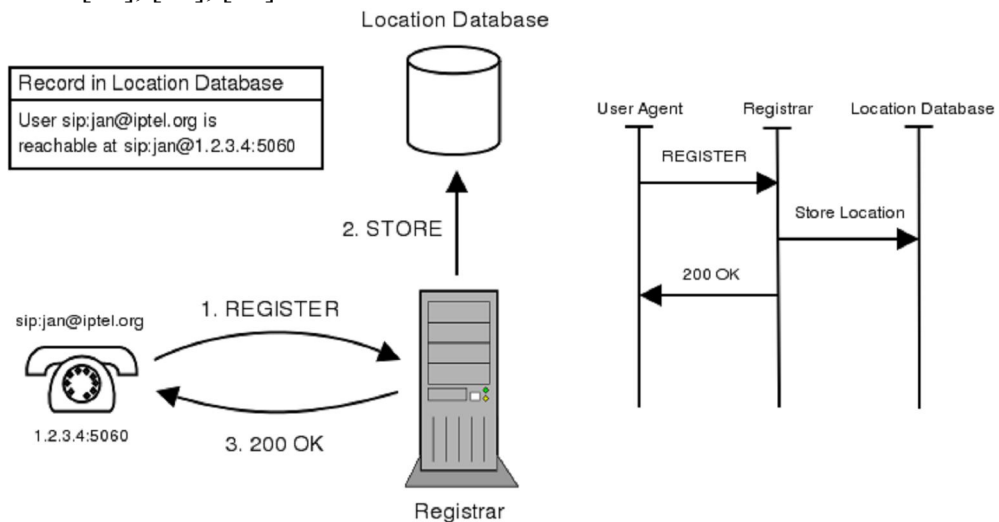
```
INVITE sip:mamut@iptel.org SIP/2.0.
Max-Forwards: 10.
Record-Route: <sip:195.113.222.3;ftag=5DAA94E7;lr=on>.
Via: SIP/2.0/UDP 195.113.222.3;branch=z9hG4bK0a5d.90580ee2.0.
Via: SIP/2.0/UDP 195.113.134.233:5062;branch=z9hG4bK2E1FD348.
CSeq: 262 INVITE.
To: <sip:mamut@iptel.org>.
Proxy-Authorization: Digest username="bbb", realm="ces.net",
nonce="43788e90381194d66364fced4dc7097828391e81", uri="sip:mamut@iptel.org",
cnonce="abcdefghi", nc=00000001, response="ed4adec8Content-Type:
application/sdp.
From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.
Call-ID: 379332994@195.113.134.233.
Subject: sip:bbb@ces.net.
Content-Length: 234.
User-Agent: kphone/4.2.
Contact: "Franta Vomacka" <sip:bbb@195.113.134.233:5062;transport=udp>.
P-hint: outbound.
Remote-Party-ID: "Franta Vomacka" <sip:950070101@ces.net>;party=calling;id-
type=subscriber;privacy=off; screen=yes.
```

1.6.4.1 Typy požadavků

První položka požadavku obsahuje jeho typ, označovaný jako metoda, označení klienta nebo serveru, kterému je požadavek adresován (Request-URI) a verzi protokolu. Důležité jsou následující požadavky:

- Metoda **INVITE** slouží k přivvání uživatele nebo služby k podílení se na relaci. Tělo zprávy obsahuje popis relace (spojení).
- Metoda **ACK** potvrzuje, že klient v pořádku přijal odpověď na INVITE dotaz.
- Klient používá metodu **BYE** k oznámení protistraně, že hodlá ukončit hovor. Metoda **BYE** může být vyslána jak volaným, tak volajícím.
- Metoda **CANCEL** ukončuje nevyřízený požadavek se stejnou identifikací, tedy položkami Call-ID, To, From a pořadovým číslem požadavku Cseq.
- Metoda **REGISTER** je používána k registraci současné adresy klienta u SIP serveru, který ji předá lokalizační službě.

Další žádosti pokročilých služeb a vylepšení SIPu jsou: **PRACK**, **UPDATE**, **REFER**, **MESSAGE** [11], [13], [24].



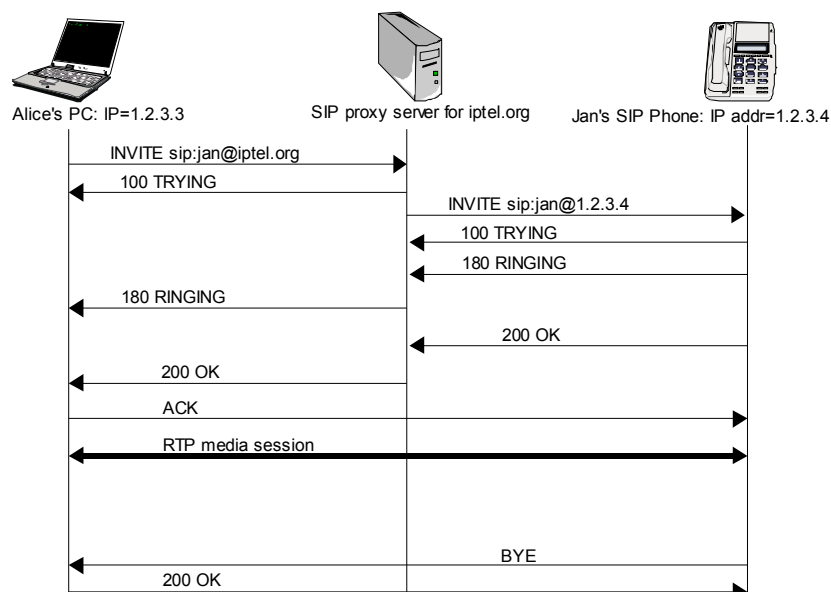
Obr. 1 – Použití metody REGISTER

1.6.4.2 Typy odpovědí

Odpovědi se dělí do uvedených kategorií podle kódu odpovědi na:

- 1xx:** Prozatímní odpovědi jako požadavek přijat, vyzvání
- 2xx:** Úspěch. Požadavek je přijat, pochopen a akceptován
- 3xx:** Přesměrování. Je třeba vytvořit nový upravený požadavek
- 4xx:** Chyba klienta. Požadavek nemůže být proveden, nebo jeho syntaxe je špatná
- 5xx:** Chyba serveru. Server není schopen provést platný požadavek
- 6xx:** Globální chyba. Požadavek nelze provést na žádném serveru

Odpovědi s kódem 200 a výše jsou konečné, jejich přijetí ukončuje transakci.



Obr. 2 – Ukázka metod a odpovědí

1.6.5 Důležité hlavičky SIP

Níže uvedené položky jsou tím podstatným výběrem z mnoha možných hlaviček [10], [11].

To: Adresa volaného

From: Adresa volajícího klienta

Via: Adresa klienta, který vysílá požadavek nebo adresa serverů, přes něž požadavek prošel a kudy se bude vracet odpověď

Call-Id: Unikátní identifikace volání

Contact: Aktuální skutečná adresa klienta

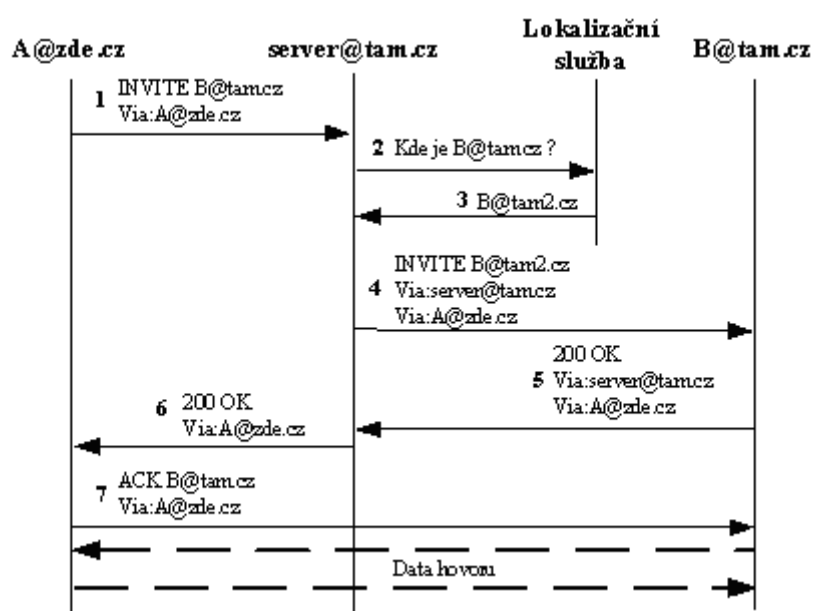
Record-Route: Seznam adres serverů, které chtějí dostávat veškerou komunikaci náležející k hovoru

Route Posloupnost adres serverů, přes které je požadavek směřován na klienta, ke kterému má požadavek dorazit.

Request-URI: Aktuální adresát požadavku.

1.6.6 Navázání a ukončení spojení

Obvykle probíhá spojení za účasti SIP proxy serverů, aby volající nemusel znát aktuální IP adresu volaného UA. Předpokládejme, že účastník je zaregistrován na serveru, který odpovídá za určitou oblast. Volající se tedy požadavkem INVITE dotazuje serveru SIP, ke kterému podle adresy zadané uživatelem přísluší volaný. Server se snaží zjistit aktuální polohu volaného. Polohu je možno zjistit například dotazem do databáze kontaktů, kterou může server spravovat. Po obdržení místa nebo míst, kde by se klient B mohl nacházet, zašle SIP server tuto informaci zpět klientovi A (server vystupuje v redirect módu) a je na klientovi samotném, aby spojení navázal. Nebo server zprávu INVITE upraví a posílá směrem ke klientovi B sám (proxy mód). Přijetí hovoru 200 OK se vrací zpět na server a od něj pokračuje k volajícímu. Pokud není použit mechanismus Record-Route, putuje potvrzení ACK a všechny další zprávy mezi klienty A a B již přímo [11], [13], [24].



Obr. 3 – Navázání spojení pomocí SIP serveru

1.7 Signalizační protokol IAX

1.7.1 IAX obecně

Na rozdíl od univerzálního protokolu SIP byl protokol IAX navržen s ohledem na maximální jednoduchost a snadnost implementace. Jeho cílovou platformou měla být velmi jednoduchá a levná koncová zařízení. Jedná se o binární protokol, který sdružuje signalizaci i hlasová data v jednom kanálu a umožní tak lépe využít šířku pásma a snadno přechází mezi sítěmi s překladem adres (NAT). Nakonec se protokol IAX vyprofiloval na řešení, které je určeno pro přímé propojení dvou ústředen Asterisk.

IAX je zaveden do ústředny Asterisk od samého počátku vývoje. Od Asterisk 0.5 (současná verze 1.6) začala být podporována vylepšená verze protokolu, nazývaná IAX2. IAX je orientován na přenos peer-to-peer a je určen pro přenos signalizačních i hlasových dat. Pomocí protokolu IAX lze provést registraci vzdálených systémů, vytvářet, udržovat a ukončovat multimediální přenosy. Protokol je navržen a vytvořen speciálně pro využití s IP protokolem [12].

1.7.2 Přednosti IAX oproti SIP/RTP

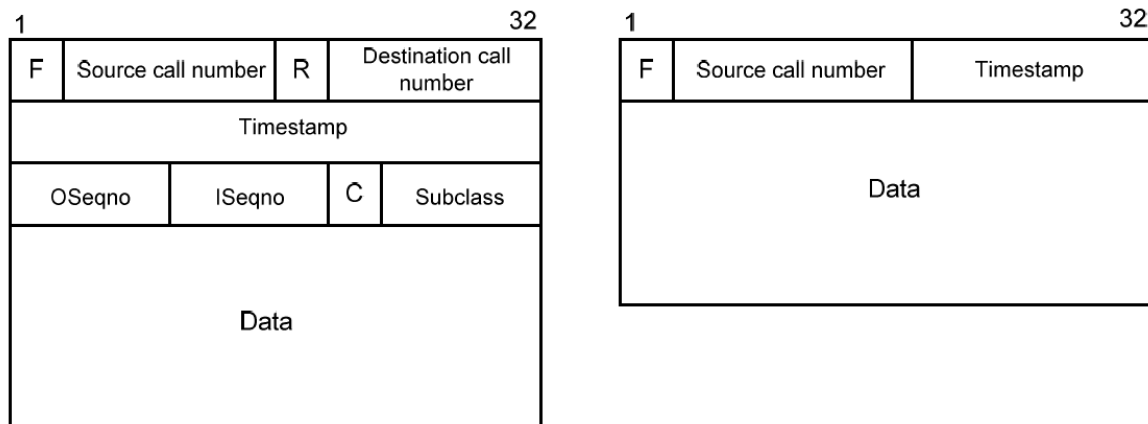
Základní myšlenkou protokolu IAX2 je využití jediného kanálu pro přenos signalizace i samotných multimediálních dat, jako je hlas a video. Základní myšlenkou je také multiplex více hovorových i signalizačních dat do jednotného datového toku. Pro přenos je využíván pouze jeden UDP port - tím je obvykle port 4569, patřící do seznamu „registrovaných“ portů.

IAX je binárně orientovaný protokol. Díky tomu může být mnohem efektivnější při hospodaření s přenosovou šířkou přiděleného pásma. Díky využití binárního protokolu je systém, který jej využívá, také mnohem odolnější proti útokům typu „buffer overrun“.

Využití binárního protokolu a sloučení signalizace a dat do jednoho toku sice zmenšuje srozumitelnost celého procesu a zároveň jde proti současnému trendu, který striktně odděluje signalizační a hovorová data, na druhou stranu ovšem umožní snadnější průchod přes firewall a NAT, přičemž, jak již bylo řečeno, nezanedbatelná je i snížená režie celého přenosu [12].

1.7.3 Rámce protokolu IAX

Základní komunikační jednotkou protokolu IAX je IAX rámec. Existuje více typů rámců, přičemž základní a nesoucí hovorová i signalizační data je tzv. „Full Frame“. Pro přenos multimediálních dat je využit tzv. „Mini Frame“. Již při pouhém přenosu multimediálních dat lze identifikovat značné rozdíly oproti protokolu RTP, který vyžaduje 12 bajtů, protože hlavička rámce „Mini Frame“ má velikost pouhé 4 bajty. Je samozřejmé, že stranou nemohlo zůstat ani zabezpečení, proto je autentizace zabezpečena protokolem RSA. Bezpečnost je důležitá hlavně v případech, kdy dochází k propojení dvou pobočkových ústředen prostřednictvím Internetu.



Obr. 4 - IAX rámce - FullFrame a MiniFrame

Jak již bylo zmíněno, protokol IAX využívá dva typy rámců MiniFrame a FullFrame (viz Obr.):

- MiniFrame má hlavičku pouze 4 bytovou, která obsahuje posledních 16 bitů časové značky, zdrojové číslo volajícího a bit F, který rozlišuje typ rámce.
- FullFrame má hlavičku 12 bajtů. Obsahuje stejné informace jako MiniFrame, včetně plné časové značky TimeStamp. Navíc obsahuje číslo volaného, OSeqno (OutBound stream sequence number), které udává číslo odchozích rámců. ISeqno (InBound stream sequence number) obsahuje stejnou informaci jako OSeqno, ale tentokrát pro příchozí rámce. Frame Type, určuje typ rámce (DTMF signalizace, hlasová data, video, řídicí rámec, IAX řízení, atd...). Pole C určuje, jak bude interpretováno pole nazývané Subclass [12].

1.7.4 Adresace

Protokol IAX využívá pro adresaci standardních formátů typu podle doporučení. Základní schéma *URI* protokolu IAX je následující:

iax2:uživatelské_jméno@host:port/identifikátor?kontext

Položky jsou podobné jako u protokolu SIP a doplněné o některé další údaje, jako je např. kontext, sloužící k určení části systému, na kterém je služba provozována, využitá u Asterisk serveru [12].

1.8 Transportní protokol RTP

1.8.1 Popis RTP

Především zajišťuje seřazení zaslaných paketů a jejich časové značkování (Timestamp), další vlastnost je multiplexování a demultiplexování. Kromě vlastního přenosu RTP obsahuje komunikace i kontrolní mechanismus v doručování RTCP, který během přenosu dostává informace o počtu ztracených paketů a proměnném zpoždění. RTP je protokol přenosu v reálném čase, je tedy vhodný pro audio, video a jiné.

Hlavička RTP může být komprimována ze 40B na 2-3B s použitím kompresního protokolu cRTP (compressed RTP). Jelikož je vyžadována podpora na obou stranách, je použití víceméně omezeno na dvoubodové spoje. Typickým portem RTP je 5004, pro RTCP je port 5005, ale lze využít jakýkoliv port větší než 1024 [13].

V tomto protokolu během času došlo k několika rozšíření doporučení RFC xxxx (xxxx – číslo doporučení), která řeší změnu pravidel a algoritmů, např.:

- SR (Sender Report) soubor statistik od odesílatelů
- RR (Receiver Report) soubor statistik od příjemců
- APP funkce specifické jednotlivé aplikace
- XR (Extended report) rozšířené posílání zpráv, které obsahuje
 - Packet Loss (ztráty) a Discard Metric (vyřazené pakety)
 - Delay Metrics (zpoždění)
 - Signal Related Metrics (parametry signálu)
 - Jitter Buffer Parameters (parametry mezipaměti)
 -

1.8.2 Šifrovaný přenos SRTP

V roce 2004 byl standardizován protokol umožňující šifrování obsahu real-time komunikace RTP v IP síti. Použitím nešifrovaného přenosu zvyšujeme riziko odposlechu hovoru. SRTP rozšiřuje protokol RTP o bezpečnostní mechanismy.

Důvěrnost přenášených dat zajišťuje kryptografický primitiv AES (Advanced Encryption Standard), který funguje jako generátor pseudonáhodných klíčů.

Při použití je nutné, aby všechny strany komunikace znaly tajný symetrický klíč, tzv. session key. Objevuje se problém, jak klíč generovat a distribuovat. Pro distribuci se používá protokol SDP, ten ale není chráněn proti případným útokům [13].

1.8.3 Protokol ZRTP

Protokol ZRTP (Zimmermann RTP) je nástavba SRTP. ZRTP rozšiřuje mechanismy pro počáteční výměnu symetrických klíčů. K výměně klíčů se zde používá Diffie-Hellmanův algoritmus [13].

1.8.4 Tóny DTMF v RTP

RFC 2833 specifikuje, že lze přenášet tóny způsobem:

- Out-of-band, čili mimo hovorové pásmo, tóny popsány určitou formou
- In-band, přenos tónu v digitalizované podobě

1.9 Kodeky

Kodek je zařízení nebo algoritmus, který slouží ke zmenšení jinak zbytečně velkého objemu audiovizuálních dat. Vzniklo složením slov kodér a dekodér, tj. zařízení, jež je na jedné straně schopné data zakódovat a na druhé straně opět dekodovat. Kodeky velmi často

používají ztrátovou kompresi, a proto dekodovaná data nejsou totožná s daty, která byla zakódována.

1.9.1 Kvalita hovoru v interakci s VoIP

Z hlediska kvality hovoru přináší VoIP používání různých metod kódování, které mají odlišnou hodnotu parametru MOS (Mean Opinion Score). MOS je stanoven subjektivní metodou hodnocení. Může dosáhnout maximálně hodnoty 5. V tabulce jsou uvedeny používané standardy kódování, názvy algoritmů, náročnosti na zpracování vyjádřené parametrem MIPS (počet milionů instrukcí za sekundu), přenosové rychlosti kodeků a jejich kvalita ohodnocená parametrem MOS [13], [15].

Standard	Algoritmus	MIPS	Přenosová rychlost [kbit/s]	MOS[ACR]
G.711	PCM	0	64	4,1
G.726	ADPCM	1	32	3,85
G.728	LD-CELP	30	16	3,61
GSM 06.10	RPE-LTP	10	13	3,5
G.729	CS-ACELP	20	8	3,92
G.723.1	MP-MLQ	16	6,3	3,9
G.723.1	ACELP	20	5,3	3,65
SILK	-	-	12 -40	3,22
Spex	-	-	5,3	2,74

Tab. 2 - Tabulka kodeků a hodnot MOS

Nejpoužívanějším kodekem je jednoznačně pulzní kódová modulace PCM dle standardu ITU-T G.711. Ačkoliv pohledem do tabulky se může zdát, že G.729 bude oproti G.711 osmkrát úspornější na pásmo v IP sítích, tak po vytvoření paketů a započtení jejich hlaviček, si G.729 nárokuje v síti Ethernet zhruba 35 kbit/s a G.711 až 90 kbit/s! [14].

1.9.2 Používané kodeky

- **G.711** - Kodek, který je použit i v klasické telefonní síti. Kvalita přenášeného hlasu je totožná s kvalitou hlasu běžného telefonního hovoru, MOS = 4,1. Existují dva typy G.711. μ -law používaný v Americe a v Japonsku a A-law využívaný v Evropě a zbytku světa.
- **G.723.1** - Používá buď kódování MP-MLQ nebo ACELP. První typ kódování vyžaduje šířku pásma 6.3 kbit/s, druhý typ 5.3 kbit/s. Doba trvání jednoho rámce je 30 ms a MOS = 3,9 při kódování MPMLQ a MOS = 3,65 při použití ACELP.
- **G.726** - Kodek používá kódování ADPCM, proměnná šířka pásma je 16, 24, 32 a 40 kbit/s. Kodek může zpracovávat bloky různé délky podle toho, jak velké zpoždění je požadováno.
- **G.728** - Kódování LD-CELP. Potřebná šířka pásma je 16 kbit/s, MOS = 3,61.

- **G.729** - Použité kódování je CS-ACELP. Potřebná šířka pásma je 8 kbit/s, kvalita je podobná jako 32 kbit ADPCM. G.729a je dodatek k G.729. Tento kodek snižuje nároky na výpočetní výkon asi o 20%, ale je zhoršena kvalita hovoru.
- **GSM** - Kodek, šířka pásma je 13 kbit/s. GSM je rychlejší než metody založené na slovníku (CELP).
- **iLBC** - Internet Low Bit Rate Codec, potřebná šířka pásma je 13.33 kbit/s, délka rámce je 30 ms. Kodek umožňuje elegantní snížení kvality přenášeného signálu v případě zpoždění nebo ztráty paketů.
- **SILK** – Super Wideband Audio Codec, zpracovává hlasové pásmo 50 až 12000 Hz, MOS = 3,22 [15].
- **SPEEX** - svobodný zvukový kodek pod licenci BSD. Ke kompresi lidské řeči. MOS = 2,74.

2 VOIP SERVER ASTERISK

2.1 Co je Asterisk?

Asterisk (open source hybrid TDM and packet voice PBX) je softwarová pobočková ústředna umožňující provoz IP, tak digitální ISDN i analogové telefonie. Navíc nabízí služby IVR (Interactive Voice Response) a Automatic Call Distribution (ACD). IVR je zkratka pro naváděný automatický odpovídač, který je ovládán většinou tónovou volbou (DTMF) anebo hlasem. ACD je systém automatického rozdělování hovorů dle stanovených pravidel (např. čísla volajících, časových podmínek, definovaných schémat).

Asterisk je open-source softwarová PBX běžící na platformách Linux, Unix. Existuje řada praktických nasazení, kde Asterisk dokázal nahradit komunikační systémy renomovaných výrobců. Pokud se při výběru komunikačního systému objeví nabídka s Asteriskem a dokáže splnit kladené technické nároky, pak je pro konkurenci Asterisku velmi těžké soutěžit proti této nabídce, neboť software je zcela zdarma a placena jsou pouze práce na Asterisku či případné úpravy [17].

2.1.1 Vlastnosti Asterisku

Systém je navržen tak, aby vytvořil rozhraní telefonnímu hardwaru, softwaru a libovolné telefonní aplikaci a může být mimo jiné použit v těchto aplikacích [13], [17]:

- Různorodá VoIP gateway (MGCP, H.323, SIP, IAX)
- Pobočková ústředna (PBX)
- Voicemail služby s adresářem
- Interaktivní hlasový průvodce (IVR)
- Softwarová ústředna (Softswitch)
- Konferenční server (včetně videa)
- Packet voice server
- Šifrování telefonních nebo faxových spojení
- Překlad čísel
- Prediktivní volič (Predictive dialer)
- Řazení volání do front se vzdáleným zprostředkovatelem
- Vzdálené „kanceláře“ pro existující PBX

2.1.2 Doplnkové služby

Asterisk nabízí veliké množství jak klasických doplnkových služeb, tak i pokročilých, které jsou obvykle poskytovány pouze špičkovými TDM PBX. Jako doplnkové služby a funkce si uvedeme jen některé nejzajímavější následující příklady [17]:

- ACCOUNT CODE, pro tarifkaci hovoru. Volající před volbou čísla vloží svůj kód.
- AUTOMATED ATTENDANT, automatická spojovatelka.
- BLACKLIST, seznam nežádoucích příchozích čísel.
- CALL TRANSFER, jedná se o předání hovoru.
- CALL FORWARDING ON BUSY, ON NO ANSWER, UNCONDITIONALLY přesměrování volání za různých podmínek.

- CALL RECORDING, umožňuje zaznamenávat hovory, zaznamenané hovory jsou uloženy v požadovaném formátu (např. PCM či GSM).
- CALL ROUTING, je provolení na pobočku (DDI – Direct Dialing In, provolba).
- CALLER ID, je funkce zobrazení čísla volajícího a jména volajícího.
- CALLER ID BLOCKING, hovor je odmítnut na základě identifikace volajícího.
- CONFERENCE BRIDGING, vytvoří konferenci mezi terminály různých typů, jako lokální pobočkou, vzdálenou linkou, mobilním účastníkem, VoIP spojením, apod.
- DATABASE STORE / RETRIEVAL, ukládá informace o hovorech do DB pro pozdější využití.
- DIAL BY NAME, namísto čísla je možné volit i jméno (jako alias).
- DUNDI (Distributed Universal Number Discovery), je distribuovaný systém směrování, který v síti Asterisků umožní jednak rozložení zátěže mezi různé servery a jednak zvýšení odolnosti při výpadku některého z Asterisk serverů.
- ENUM, Asterisk podporuje vyhledávání telefonních čísel přes DNS, kde je realizováno mapování telefonních čísel na jmenné identifikátory (URI), pokud je spojení na vyhledanou URI adresu nedostupné, tak se použije další pravidlo (např. směrování přes PSTN).
- IVR je pokročilý systém pro obsluhu příchozích volání.
- MUSIC ON HOLD, hudba na přidržené lince, přičemž audio soubory lze vytvářet jednoduchým způsobem.
- PROTOCOL CONVERSION, umožňuje spojení mezi sítěmi používajícími rozdílné protokoly.
- REMOTE OFFICE SUPPORT, umožňuje přihlásit telefon z jiné PBX tak, že má vlastnosti lokální pobočky.
- ROUTE BY CALLER ID, hovor je směrován na základě čísla volajícího na pobočku, do fronty nebo do skupiny účastníků (Ring Group).
- SMS MESSAGING, Asterisk umožňuje pomocí SMS upozorňovat např. zmeškaná volání a zanechané vzkazy, SMS se posílají přes SMS
- SPELL/SAY, funkce umožňuje přečíst text, např. email.
- TRANSCODING, Asterisk umožňuje konverzi mezi různými kodeky.
- TRUNKING, je funkce připojení do klasické telefonní sítě pomocí interní karty v Asterisku.
- VOICEMAIL, umožňuje nahrát vzkaz pro volaného, zpřístupnit nahrané vzkazy z telefonu přes web anebo odeslat vzkaz do poštovní schránky uživatele jako email.

2.1.3 Rozhraní a kanály

Architektura systému je v podstatě velmi jednoduchá, ale zcela odlišná od nejčastěji používaných telefonních produktů. Asterisk vystupuje v podstatě jako středový prvek spojující telefonní technologie na jedné straně s telefonními aplikacemi na straně druhé.

Asterisk je navržen tak, aby umožňoval použití nových rozhraní a snadné rozšíření o nové technologie. Podporuje veškeré možné typy současných i budoucích technologií pro telefonii.

Obecně jsou rozhraní rozdělena do tří základních skupin [16]:

- Zaptel hardware, je nativně podporován Asteriskem,
- non-Zaptel hardware, doplněn bez podpory výrobce PBX,
- packet voice, tato skupina nevyžaduje HW, jedná se o již zmíněné různé VoPI protokoly.

Prostřednictvím kanálů vstupují do systému různé druhy komunikace. Kanály jsou logická spojení s různými přenosovými a signalizačními cestami, které může Asterisk využívat k vytváření a spojování jednotlivých hovorů. Asterisk nedělá žádný rozdíl mezi typem kanálu FXO (Foreign eXchange Office) a FXS (Foreign eXchange Station), nerozlišuje tedy mezi telefony a telefonními linkami. Každé volání je na odlišném kanále. Asterisk se všemi kanály zachází jako s přípojnými body, jejichž vzájemná interakce se definuje v souboru *extensions.conf*. Je důležité si uvědomit, že i kdyby se kanály lišily v rámci použité technologie a konektivity, Asterisk umožňuje zacházet se všemi téměř stejně.

V případě kanálů/klientů IAX se konfigurace provádí modifikací souboru *iax.conf*. Konfigurace SIP kanálů/klientů se provádí modifikací souboru *sip.conf*. Zap kanálový modul poskytne mezivrstvu mezi Asteriskem a Zaptel. Konfigurace ZAP kanálů se provádí modifikací souboru *zapata.conf*. Dialplan je konfigurován v souboru *extensions.conf*. Je to nejdůležitější konfigurační soubor systému. Řídí způsob ovládání a směrování příchozích a odchozích hovorů. Toto je místo, kde kontrolujete chování všech spojení provedených prostřednictvím PBX [13], [16].

2.1.4 Instalace Asterisku

Instalace se může lišit u každé linuxové distribuce, a proto je nejvhodnější vyhledat informace ke konkrétní verzi v odborné literatuře nebo internetu. Nejjednodušším způsobem instalace je distribuce softwarové ústředny s operačním systémem nazvaná Asterisk NOW v aktuální verzi 1.5.0. Takto instalovaná ústředna pracuje pod operačním systémem CentOS. Lze použít i jiné linuxové distribuce, např. se systémem Debian a další [2].



2.1.5 Konfigurace

Nastavení se provádí v konfiguračních souborech, které vznikly instalací. Každý soubor má své specifické umístění a funkci:

- /etc/zaptel.conf*, fyzické rozhraní ZAPATA telephony,
- /etc/asterisk/zapata.conf*, konfigurace ZAPTEL rozhraní (např. ISDN PRI),
- /etc/asterisk/extension.conf*, konfigurace číslovacího plánu,
- /etc/asterisk/sip.conf*, konfigurace sip kanálu,
- /etc/asterisk/iax.conf*, konfigurace iax kanálu,
- /etc/asterisk/h323.conf*, konfigurace h323 kanálu,
- /etc/asterisk/meetme.conf*, doplňková služba - konferenční místnost,
- /etc/asterisk/voicemail.conf*, doplňková služba - hlasová pošta,
- /etc/asterisk/followme.conf*, doplňková služba – přesměrování,
- /etc/asterisk/dundi.conf*, směrovací protokol pro cluster s Asterisk servery,
- /etc/asterisk/enum.conf*, pro podporu mapování E.164 na URI (tzv ENUM).

2.1.6 Ovládání

Ústředna se ovládá z konzole, označenou v Asterisku jako CLI>. Příklady nejpoužívanějších příkazů:

asterisk -r	spuštění konzole s parametrem
help	vypíše všechny známé příkazy
reload	znovu načte konfiguraci po změně konfigurace
restart when convenient	restartuje ústřednu po uvolnění všech obsazených kanálů
sip show peers	detailní informace o SIP stanicích
iax show registry	zobrazení registrace stanic IAX
dialplan show	zobrazení celého dialplánu

2.2 Konfigurace a ukázky nastavení

2.2.1 Context a extension

Asterisk je koncepčně obdobou klasické telefonní ústředny, ke které jsou všechna zařízení připojena do "zásuvek", zvaných extensions. Extensions mohou používat různé technologie. Nejčastější je to protokol SIP, ale je možné použít i protokol H323, speciální kartu pro připojení analogových telefonů, ISDN atd. Každá extension má vlastnost *context*, která určuje, jaká část konfiguračního souboru *extensions.conf* se použije pro hovory, které z ní přicházejí [13], [17].

```
[services]

exten => 348,1,Answer()
exten => 348,n,Playback(demo-echotest)
exten => 348,n,Echo()
exten => 348,n,Hangup()

[sipusers]

exten => 331,1,Dial(SIP/stul,20)
exten => 332,1,Dial(SIP/client)
exten => 333,1,Dial(SIP/host1)
```

Tab. 3 – Ukázka kontextů

V tomto případě jsou definovány dva kontexty. Jeden s názvem *services* a druhý s názvem *sipusers*. Jména kontextů jsou vždy v hranatých závorkách. Rozdělení do dvou kontextů umožňuje nastavit odlišné chování ústředny pro volání.

Extension Dialplan mohou být jednoduchá čísla jako „421“ nebo „0“. Mohou to být také alfanumerické znaky jako „honza“ nebo „klara08“. Často může logický Dialplan zahrnovat skoky z jedné extension do jiné extension a pro tyto skoky mohou být definována extension jména s jakýmkoliv názvem.

Konfigurace v každém kontextu se skládá z jednotlivých pravidel. Každé pravidlo začíná klíčovým slovem *exten* a má tvar [13], [18]:

```
exten => name,priority,application
```

Tab. 4 – Pravidla extensions

name

Pravidlo se použije, odpovídá-li volané číslo hodnotě name. Nejjednodušší možnost je použít přímo telefonní číslo. V praxi se často využívají šablony, které umožňují jedním pravidlem ošetřit celou skupinu hodnot. Šablony se liší od obvyklých hodnot tím, že začínají znakem podtržítka. Například `_XXX` odpovídá všem trojčíferným číslům. Některé hodnoty name mají speciální význam, většinou jde o samostatná písmena jako:

- i – Invalid – neplatný, jakákoliv hodnota mimo ostatní definované extension
- s – Start – začátek, hodnota bez upřesnění čísla provádějící nějakou funkci
- t – Timeout – kontrolovaná hodnota časového limitu

priority

Priorita určuje pořadí zpracování záznamů. Asterisk během zpracování hovoru postupně probírá pravidla a řadí je přitom podle priority. Nejprve hledá odpovídající pravidlo s prioritou 1, potom hledá pravidlo s prioritou 2, atd. Žádné číslo nesmí být vynecháno. Pokud by kontext obsahoval jen pravidla s prioritami 1, 2 a 4, pak by Asterisk zpracoval priority 1 a 2, následně by nenašel pravidlo s prioritou 3 a v hledání dalších pravidel by už nepokračoval. Na pravidlo s prioritou 4 by nikdy nedošlo. Místo čísla se používá proměnná „n“ a znamená prioritu o jedničku větší než předešlá.

application

Application je příkaz, který se má provést. Aplikací neboli příkazů, jsou desítky. Seznam použitelných příkazů závisí na tom, jaké moduly byly nahrány při startu asterisku. Některé příkazy mají parametry, které se píšou do kulatých závorek za příkaz (například `Wait (2)` čeká 2s před skokem na další prioritu).

```
exten => s,n,Wait(2)
exten => s,n,Answer()
```

2.2.2 Práce s řetězci

Syntaxe řetězců vracejících hodnotu dle nastavení:

```

${123456789:1}    - vrací řetězec 23456789
${123456789:-4}   - vrací řetězec 6789
${123456789:0:3}  - vrací řetězec 123
${123456789:2:3}  - vrací řetězec 345
${123456789:-4:3} - vrací řetězec 678

```

Jména extension nejsou tedy omezena na jednotlivé specifické extension „čísla“. Jednotlivé extension mohou rovněž odpovídat vzorům. V souboru `extension.conf` se jméno extension stává vzorem, jestliže začíná znakem „podtržítka“. V extension vzorech mají následující znaky speciální smysl [16]:

```

X    odpovídá některé z číslic 0 – 9
Z    odpovídá některé z číslic 1 – 9
N    odpovídá některé z číslic 2 – 9

```

[17-9] odpovídá některé číslici nebo písmenu uvedenému v závorkách (v tomto případě tedy 1,7,8,9)

Práci s řetězci ukazuje následující příklad:

```
exten => _606ZXXXXX,1,Dial(${EXTEN:3})
```

Tab. 5 – Práce s řetězci

Vzor čísla `_606ZXXXXX` znamená, že se čeká na volbu 9-ti místného čísla začínajícího na 606. Na druhé pozici se nesmí objevit číslo 0, což signalizuje znak „Z“. Syntaxe „`${EXTEN:3}`“ provede odříznutí prvních tří čísel. Vrácená hodnota je 6-ti místné číslo nezačínající číslem „0“ [16].

2.2.3 Konfigurace účtů

Konfigurační soubor `sip.conf` obsahuje konfigurace uživatelů na protokolu SIP. Popisy ukázkového nastavení jsou na stejném řádku, označené jako komentář.

```
[general]
port = 5060                ;UDP port
context = sipusers        ;Default context pro prichozí volání
disallow = all            ;Zakázání všech kodeků
allow = alaw              ;Povolení vybraných kodeků
allow = ulaw
allow = gsm
dtmfmode = auto          ;Default DTMF rfc2833
language = cz             ;Výchozí jazyk

[stul]
type = friend             ;Overení v obou směrech
username = stul           ;Uživatelské jméno
userid = Stul <331>       ;Zobrazování jména na displeji
host = dynamic            ;Dynamické přidělení IP adresy
allow = ulaw              ;Použitý kodek

[client]
type = user               ;Overení uživatele směrem k ústředně
username = client
userid = Client <332>
host = dynamic
```

Tab. 6 – Konfigurace účtů

2.2.4 Základní konfigurace

Konfigurační soubor `extensions.conf` je základním souborem systému Asterisk. Zjednodušeně se jedná o definování číslovacího plánu daného systému. Právě tento soubor definuje jakým způsobem budou ovládána jednotlivá volání.

```
[general]
static = yes
writeprotect = yes ;zamezeni prepisovani diaplan z CLI

[globals] ;=====

[services] ;=====

exten => 348,1,Answer() ;Prijmuti hovoru Asteriskem
exten => 348,n,Playback(demo-echotest) ;Prehrava se hlaska "demo..."
exten => 348,n,Echo()
exten => 348,n,Hangup() ;Zaveseni hovoru

[sipusers] ;=====

include => services ;Vlozeni jineho contextu

exten => 331,1,Dial(SIP/stul,20) ;Volba 331, po 20s skok na
dalsi priritu
exten => 331,n,Dial(SIP/v100/777573684,,r) ;Presmerovani pres gate v100
exten => 332,1,Dial(SIP/client)
exten => 333,1,Dial(SIP/host1)

exten => 337,1,Dial(IAX2/iaxclient) ;Volba stanice 337, tentokrat IAX
exten => _4XX,1,Dial(IAX2/iaxtrunk2:heslo@82.114.208.81/${EXTEN:0})
;Volba stanice 4xx druhe ustredny
```

Tab. 7 – Ukázka konfiguračního souboru

Příklad, vyjmutý z nastavení konfigurace této bakalářské práce, ukazuje tabulka. Jednoduché vysvětlení syntaxe je v komentářích za znakem “;”.

PRAKTICKÁ ČÁST

3 PŘIPOJENÍ GSM ROZHRAŇÍ K ASTERISKU

GSM brána jako další Zeptel rozhraní, kterou lze k systému připojit, obnáší relativně velkou investici. Proto se naskytá možnost připojení externí GSM brány (gate) přes některá podporovaná softwarová rozhraní (LAN, Bluetooth, zvuková karta). Cena některých GSM bran, připojitelných pomocí VoIP protokolu k ústředně Asterisk již dosáhla 1/5 ceny nejlevnější ceny brány určené pro Zeptel rozhraní.

3.1 Soundwin - V100

Jedna z těchto GSM bran je zařízení V100 od firmy Soundwin. Brána je vybavena čtyřpásmovým mobilním GSM modulem, má rozhraní FXS, FXO a ethernetové rozhraní WAN. Některé vybrané vlastnosti brány:

- Volání z mobilního telefonu přes VoIP
- Volání z VoIP na mobilní telefon
- SMS Server pro příjem a zaslání SMS
- Směrování, restrikce a úprava volaných čísel
- Zobrazení stavu hlasových kanálů
- Dynamický jitter buffer
- Podpora SIP i H.323



GSM brána Soundwin V100 v sobě kombinuje GSM a VoIP - ATA bránu. Brána umožňuje příjem volání z mobilního telefonu a dále směrování hovoru přes VoIP nebo obráceně. Také umožňuje směrování volání přes klasickou telefonní linku. Konfigurace brány se provádí pomocí grafického menu přes webové rozhraní [6].

3.1.1 Konfigurace V100 pro připojení k Asterisku

Před samotným nastavením brány je nutné ve vlastnostech síťového připojení konfiguračního PC nastavit IP adresy dle obrázku 5. Výchozí IP adresa brány je 192.168.1.1, kterou zadáme do prohlížeče, a po zadání brána vyzve k zadání jména a hesla. Oba údaje jsou „admin“.

Začneme s nastavením GSM modulu, kde se nastavují parametry GSM části. Přejdeme na položku **System Configuration >> GSM Setup >> GSM Parameter**. Zde nastavíme parametry mobilní části (Obr. 6).

<input checked="" type="radio"/> Použít následující adresu IP:	
Adresa IP:	192 . 168 . 1 . 2
Maska podsítě:	255 . 255 . 255 . 0
Výchozí brána:	192 . 168 . 1 . 1
<input type="radio"/> Získat adresu serveru DNS automaticky	
<input checked="" type="radio"/> Použít následující adresy serverů DNS:	
Upřednostňovaný server DNS:	192 . 168 . 1 . 1
Náhradní server DNS:	.

Obr. 5 – Vlastnosti TCP/IP v PC

GSM Parameter Table	
GSM Parameter table	
PIN Code Protection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable PIN: <input type="text"/>
Failsafe Mechanism (FXS rely on PSTN)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Baby Call	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Delay Time: <input type="text"/> Calling Number: <input type="text"/>
FXS Battery Reverse	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Talking Time Limit	<input type="text"/> mins
GSM Frequency	<input checked="" type="radio"/> 900/1800 <input type="radio"/> 850/1900
CLI Presentation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
CLI Detection	<input type="radio"/> Disable <input type="radio"/> Enable <input checked="" type="radio"/> Asterisk 1.3 <input type="radio"/> IDT
Answer Supervision	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
GSM Receive Gain	<input type="radio"/> -18db <input checked="" type="radio"/> -10db <input type="radio"/> -8db <input type="radio"/> -6db <input type="radio"/> -4db <input type="radio"/> -2db <input type="radio"/> 0db <input type="radio"/> +2db <input type="radio"/> +4db <input type="radio"/> +6db
GSM Transmit Gain	<input type="radio"/> +30db <input checked="" type="radio"/> +33db <input type="radio"/> +36db <input type="radio"/> +39db <input type="radio"/> +42db
GSM Answer Mode	<input type="radio"/> Auto Answer <input checked="" type="radio"/> Connecting Answer
VoIP TO GSM Hot line	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Calling Number: <input type="text"/>

Obr. 6 - GSM parametry

V záložce **GSM parametr** vložte PIN kód SIM karty v případě, že je vyžadován. **Baby Call**, **FXS Battery Reverse**, **Answer Supervision**, **Talking Time Limit** pro spojení s Asteriskem nevyužijeme. Další parametr, důležitý pro správnou funkci ústředny **GSM frequency**, je ve výchozím nastavení aktivována pro české podmínky, tedy 900/1800 MHz. **CLI Presentation** zobrazuje číslo v odchozím směru. **CLI Detection** při volbě Asterisk 1.3, bude přeneseno číslo volajícího přes Asterisk proxy server. Jsou-li potíže s příjmem nebo vysíláním GSM signálu, lze položkou **GSM Receive, Transmit Gain** nastavit úroveň signálu. Ostatní parametry je doporučeno nechat v defaultních hodnotách. Další parametry >> **GSM Setup** >> nejsou potřeba nastavovat.

V síťové části **Advance Setup** >> **Network Setup** >> **WAN Setting** je doporučeno pro spojení s Asteriskem nastavit statickou adresu, kde bude ústředna hledat spojení s GSM modulem.

Nejdůležitější část komunikace s gsm bránou nastavují parametry **Advance Setup** >> **VoIP Setup** >> **VoIP Basic**. Bohužel se nepodařilo bránu k Asterisku zaregistrovat, což ovšem neovlivňuje funkci komunikace. Nelze tedy použít zabezpečenou registraci pomocí hesla, ale vzhledem k instalaci ústředny a gsm brány ve stejné (lokální zabezpečené síti) není tento krok potřeba. Na záložce **VoIP Basic** vybereme protokol SIP dle obrázku 7.

VoIP Protocol Setting SIP

Port Number / Password Setting(MAX 20 digit) :

No.	Number	Reg	Account	Password	Register Status	Reason
1(FXS)	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		
2(GSM)	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		

Use Public Account (PORT 1) Enable Disable

SIP Hunting Table :

No.	Hunting Member
1	<input checked="" type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2
2	<input type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2

SIP Proxy Setting :

Domain/Realm	<input type="text" value="192.168.0.103"/>
SIP Proxy Server	<input type="text" value="192.168.0.103/5060"/>
SIP User Agent	<input type="text" value="192.168.0.103"/>
Register Interval (seconds)	<input type="text" value="900"/>
SIP Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Outbound Proxy Server	<input type="text" value="192.168.0.103/5060"/>

Obr. 7 – VoIP parametry I

Do pole **SIP Proxy Server** vložíme IP adresu Asterisk ústředny včetně komunikačního portu. Tuto adresu použije gsm brána pro sestavení spojení GSM >> VoIP. Ještě jednou je potřeba nastavit komunikační port (pro SIP pravděpodobně 5060, ale může být i vyšší).

Local port Setting:

Local SIP Port	<input type="text" value="5060"/>
----------------	-----------------------------------

Obr. 8 – VoIP parametry II

Advance Setup >> VoIP Setup >> Dialing Plan určuje nastavení routovacích parametrů dle čísel (Obr. 9).

Outgoing Dial Plan: (maximun 50 entries, maximun length of prefix digits is 16 digit, maximun length of number is 20 digit)

Item	Outgoing no.	Length of Number	Delete Length	Prefix no.	Destination IP/DNS	Destination SIP Port	Operation
		~					ADD

DELETE Outbound Dial Plan From To

Incoming Dial Plan: (maximun 50 entries, maximun length of prefix digits is 16 digit, maximun length of number is 20 digit):

Item	Incoming no.	Length of Number	Delete Length	Prefix no.	Destination	Operation
1	6x	9 ~ 9	0	None	GSM	
2	7x	9 ~ 9	0	None	GSM	
		~			<input type="radio"/> FXS <input type="radio"/> GSM	ADD

DELETE Inbound Dial Plan From To

Obr. 9 – Dial plán

Jedná se o odchozí směr volání z VoIP >> GSM, zde označen jako „incoming“ (myšleno přicházející z VoIP). V tabulce jsou nastavena čísla, která mohou být směrována do GSM sítě. Nastavení, zobrazené na obrázku 6, vychází z číslovacího plánu České republiky. Mobilní sítě začínají číslem 6 a 7. V národním formátu mají pevnou velikost 9 číslic. Parametr „6x“, v poličku **Incoming no.** znamená volba 6 a cokoliv dalšího. **Length of Number** je minimální a maximální délka voleného čísla. Zpracování čísel necháme na ústředně Asterisk a proto předradit **Prefix no.** a umazat **Delete Length** volené číslo není potřeba.

Na kartě **Advance Setup >> VoIP Setup >> Advance Setting** se v záložce „VoIP Advance“ nastavuje způsob odesílání DTMF tónu. Doporučen je standard RFC 2833, který je dále využit k možnosti volby čísla po sestavení spojení s Asteriskem.

Advance Setting

Advance Setting Select VoIP Advance Select

DTMF Relay for SIP	<input type="radio"/> Inband <input checked="" type="radio"/> RFC2833 <input type="radio"/> SIP Info
RFC2833 Payload	101 (from 96 to 127)
Watchdog	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VoIP Encryption	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VoIP Encryption Port	8888
MWI	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Apply

Obr. 10 – Nastavení DTMF

Velmi důležitý parametr brány V100 se nachází **Advance Setup >> VoIP Setup >> Advance Setting** v záložce „Telephone Advance“. Jmenuje se „**Silence Compression Voice Activity Detection**“. Česky to znamená detekce ticha. V době, kdy se nepřenáší žádný zvuk (ticho), nepřenáší se ani data. S tímto parametrem si ústředna Asterisk nerozumí a musí být vypnut nastavením „VAD disable“! Při nenastavení parametru na hodnotu disable, neuvolní Asterisk kanál, i když volající účastníci ukončí hovor. Na stejné kartě je i možnost nastavení kodeku. G.711 se jeví jako správná volba. Má malou kompresi (tudíž i zkreslení) a na vnitřní rychlé síti, šířka pásma 64 kbit/s (90 kbit/s reálných) nevadí.

Příchozí hovor je řešen jako hotline číslo. Znamená to, že příchozí hovor z GSM je předán na toto „hotline“ číslo. Nastavuje se v **Advance Setup >> VoIP Setup >> Hot Line Setting**.

Hotline Delay	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Hotline Delay Time(Max. 20 sec)	<input type="text" value="3"/> sec
Port 1 number	<input type="text" value="None"/>
Port 2 number	<input type="text" value="343"/>
<input type="button" value="Apply"/>	

Obr. 11 – Hotline číslo

Zde je potřeba nastavit číslo, které bude v Asterisku voláno. Musíme použít port 2 (port 1 je pro PSTN GSM brány). Volání z GSM brány v protokolu SIP pak vypadá následovně:

```
Request-Line: INVITE sip: 343@192.168.0.103
SIP/2.0
```

} žádost o spojení
 } protokol
 } volaný
 } IP adresa ústředny
 } verze

Volané číslo se převezme z tabulky „hotline“ řádku **port 2 number** a sestaví se adresa volajícího z IP adresy serveru, která je na kartě **VoIP Basic**, položka SIP Proxy Server.

Všechny provedené změny je potřeba uložit a provést reboot celého zařízení. Doba potřebná pro tuto operaci je cca 90s (GSM jednotka se musí nalogovat do sítě).

Pro ladění nastavení poskytuje grafické rozhraní GSM brány V100 sledování příchozích a odchozích volání s následným routováním. Nachází se v nabídce **Advance Setup >> VoIP Setup >> Port Status**, jak ukazuje obrázek 12 a 13.

Port Status:										
Port No.	Type	Status	Codec	Direction	Dial No.	Caller No.	Dest/Source	IN	OUT	Duration
1	FXS	onhook	none	none	none	none	none	0	0	0
2	GSM	connected	G.711(μ-law)	Outbound	343		192.168.0.103	1	3	3

Obr. 12 – Port Status, příchozí volání z GSM do Asterisku

Port Status:										
Port No.	Type	Status	Codec	Direction	Dial No.	Caller No.	Dest/Source	IN	OUT	Duration
1	FXS	onhook	none	none	none	none	none	0	0	0
2	GSM	connected	G.711(μ-law)	Inbound	777573684	stul	192.168.0.103	2	3	3

Obr. 13 – Port Status, odchozí volání z Asterisku do GSM

3.1.2 Konfigurace ústředny Asterisk pro použití brány V100

Nastavení připojení gsm brány V100 k Asterisku vyžaduje doplnění údajů účtu do souboru *sip.conf*, dle následující tabulky.

```

;=====GSM gate Sounwin V100=====
[v100]
type = friend ;Identifikace
host = 192.168.0.119 ;Overení v obou smerech
;secret = gsm ;IP adresa umistení GSM gate
fromdomain = 192.168.0.119 ;IP v tele SIP-From
disallow = all ;Zakazani vseh kodeku
allow = ulaw ;Povoleni vybranych kodeku
allow = gsm
permit = 192.168.0.119/255.255.255.0 ;Kontrola IP s maskou
qualify = yes ;Periodicke odesilani NOTIFY
canreinvite = no ;Prenos DTMF pres Asterisk
context = incoming ;Prirazeny kontext prichoziho hovoru

```

Tab. 8 – Nastavení účtu v100

Brána GSM funguje jako vnější přenašeč připojený přes rozhraní SIP k PBX Asterisk. V telekomunikační terminologii se označuje tento přenašeč jako „trunk“. Aby při dalším nastavování nebylo třeba uvádět cestu (IP adresu) a další registrační údaje, v těle konfiguračního řádku extension, použije se název účtu. V tomto případě trunk [v100].

```

exten => _7XXXXXXXX,1,Dial(SIP/v100/${EXTEN:0},,r)
exten => _7XXXXXXXX,1,Dial(SIP/${EXTEN:0}@192.168.0.119,,r)

```

Tab. 9 – Zápis odchozího volání

Tabulka ukazuje dva totožné zápisy odchozího volání přes GSM gate, uložené v souboru *extension.conf*. První zkrácený zápis používá odkazování na registrační údaje

v *sip.conf* souboru, druhý sestaví adresu volání přímo z IP adresy GSM brány. Tabulka také ukazuje použití gsm brány pro odchozí volání. Syntaxe prvního řádku znamená. Volba jakéhokoliv devítimístného čísla začínajícího znakem 7, volba do přenašeče (trunku) SIP, extension (účet) [v100], „ $\$ \{EXTEN:0\}$ “ neodeber žádnou číslici. Znak „r“ přidává ihned za provedenou volbou vyzváněcí tón (alert). Tímto způsobem lze nastavit další čísla, která se mohou volit přes GSM bránu.

Příchozí volání je realizováno volbou extension „343“. Aby bylo volání ústřednou správně zpracováno, je u účtu [v100] nastaven kontext „incoming“, který nasměruje hovor do tohoto kontextu v souboru *extension.conf*. Další zpracování hovoru bude popsáno dále.

3.2 VoiceBlue - 2N

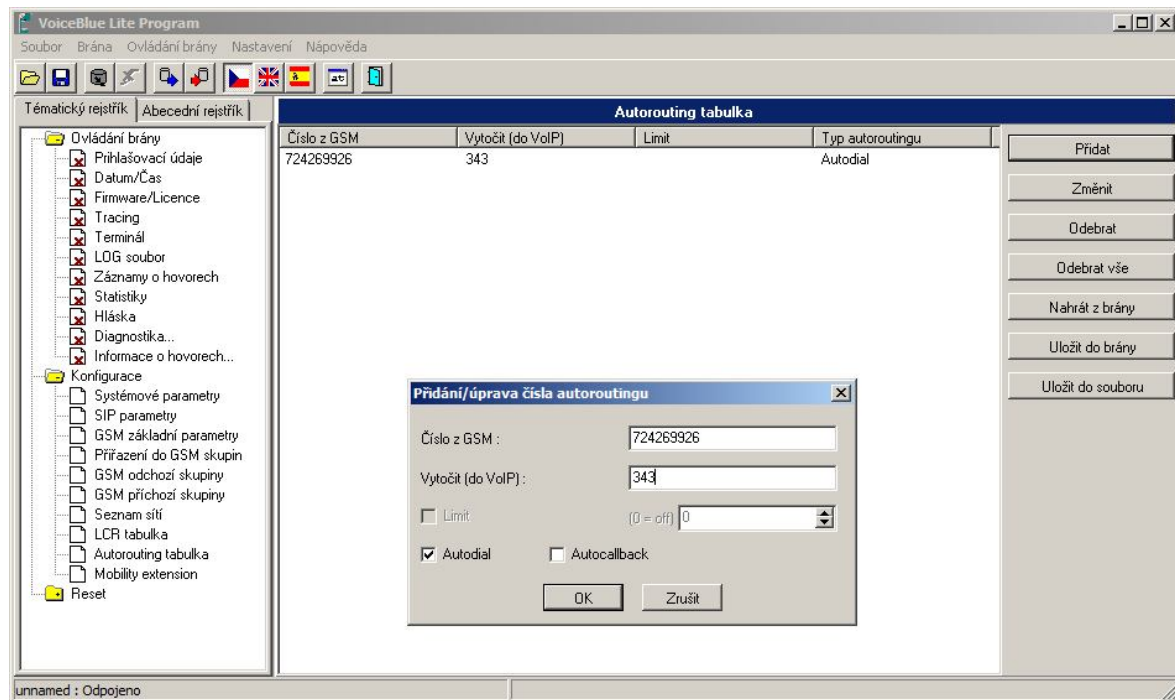
Brána 2N Ateus VoiceBlue je vhodná alternativa brány Soundwin V100. Lze ji také připojit pomocí protokolu SIP k ústředně Asterisk. Detailní popis konfigurace a připojení této GSM brány lze najít [20]. Při použití této brány je však potřeba myslet na několik odlišností:

1. Cena této GSM brány je 5tinásobkem brány V100.
2. Samotná brána má mnoho možností nastavení, včetně silného routovacího algoritmu, který z 70% je schopen nahradit ústřednu Asterisk.
3. Velice kvalitní provedení s možností použití více SIM karet.
4. Delší skladba mezinárodního identifikačního čísla (CLIP používá před číslem přestupný znak 420(v ČR)).
5. Příchozí volání odbavuje hlasový průvodce (pokud není číslo volajícího uloženo v databázi brány), zvýšené náklady na hovor.
6. Přísná licenční politika (vysoká cena licence).

3.2.1 Doplnění konfigurace VoiceBlue brány

Jak již bylo zmíněno, příchozí volání do GSM brány zpracovává hlasové návštějí DISA. Znamená to, že příchozí hovor brána vyzvedne, přehraje hlášku a čeká na volbu čísla od volajícího uživatele. Aby se předešlo tomuto chování je potřeba dát GSM bráně vědět, která příchozí čísla má propustit a nasměrovat přímo do Asterisku. Protože potřebujeme zařídit toto chování jen pro určitou skupinu příchozích čísel (VPN), není problém toto nastavit.

Nastavení se provádí v konfiguračním nástroji GSM brány VoiceBlue, změnou v Autorouting tabulce.



Obr. 14 – Autorouting tabulka VoiceBlue

Stisknutím tlačítka „Přidat“ vložíme příchozí gsm číslo člena VPN skupiny. Parametr „Vytočit (do VoIP)“ je číslo, kterým se volá dovnitř Asterisku z gsm sítě, obdobně jako hotline parametr u brány Soundwin v100.

3.2.2 Nastavení ústředny Asterisku s VoiceBlue

Nastavení účtu k připojení GSM brány VoiceBlue k Asterisku se příliš neliší od nastavení brány Soundwin v100. Opět je potřebné doplnění údajů účtu do souboru *sip.conf*, dle následující tabulky.

```

;=====GSM gate 2N VoiceBlue=====
[voiceblue]                                ;Identifikace
type = peer                                ;Overeni v obou smerech
host = 192.168.0.131                        ;IP adresa umisteni GSM gate
username = gsm                              ;Uzivtelske jmeno
secret = gsm                               ;Heslo
fromdomain = 192.168.0.131                 ;IP v tele SIP-From
disallow = all                             ;Zakazani vseh kodeku
;allow = alaw
allow = ulaw                               ;Povoleni vybranych kodeku
allow = gsm
permit = 192.168.0.131/255.255.255.0      ;Kontrola IP s maskou
qualify = yes                              ;Periodicke odesilani NOTIFY
context = incoming                         ;Prirazeni kontextu

```

Tab. 10 – Nastavení účtu VoiceBlue

4 POUŽITÍ VPN SÍTĚ A SERVERU ASTERISK

4.1 Směrování hovorů členů VPN

Princip propojení je založen na připojení GSM brány k Asterisku, která používá SIM kartu členů GSM skupiny VPN (viz 4.1.1). To znamená vzájemné propojení mobilních uživatelů a všech služeb ústředny Asterisk.

Můžeme tedy sestavit spojení hovoru mobilního uživatele, patřícího do skupiny VPN, s libovolným uživatelem pevné VoIP sítě a naopak. Server Asterisk je v tomto případě jako zprostředkovatel spojení mezi účastníky. Asterisk komunikuje s uživateli přes jednoduché hlasové menu.

4.1.1 VPN volání mezi uživateli

Díky službě mobilních operátorů nazvané VPN (Virtual Private Network – možnost volání mezi uživateli skupiny s nízkými nebo žádnými náklady na spojení) a možností připojení GSM brány k ústředně Asterisk, lze vytvořit zapojení telefonní sítě, které umožní stanicím připojeným k této ústředně a mobilními uživateli, komunikaci s nízkými náklady. Tuto službu poskytují v ČR tyto operátoři: O2, T-Mobile, Vodafone.

4.2 Schéma routovacího algoritmu ústředny

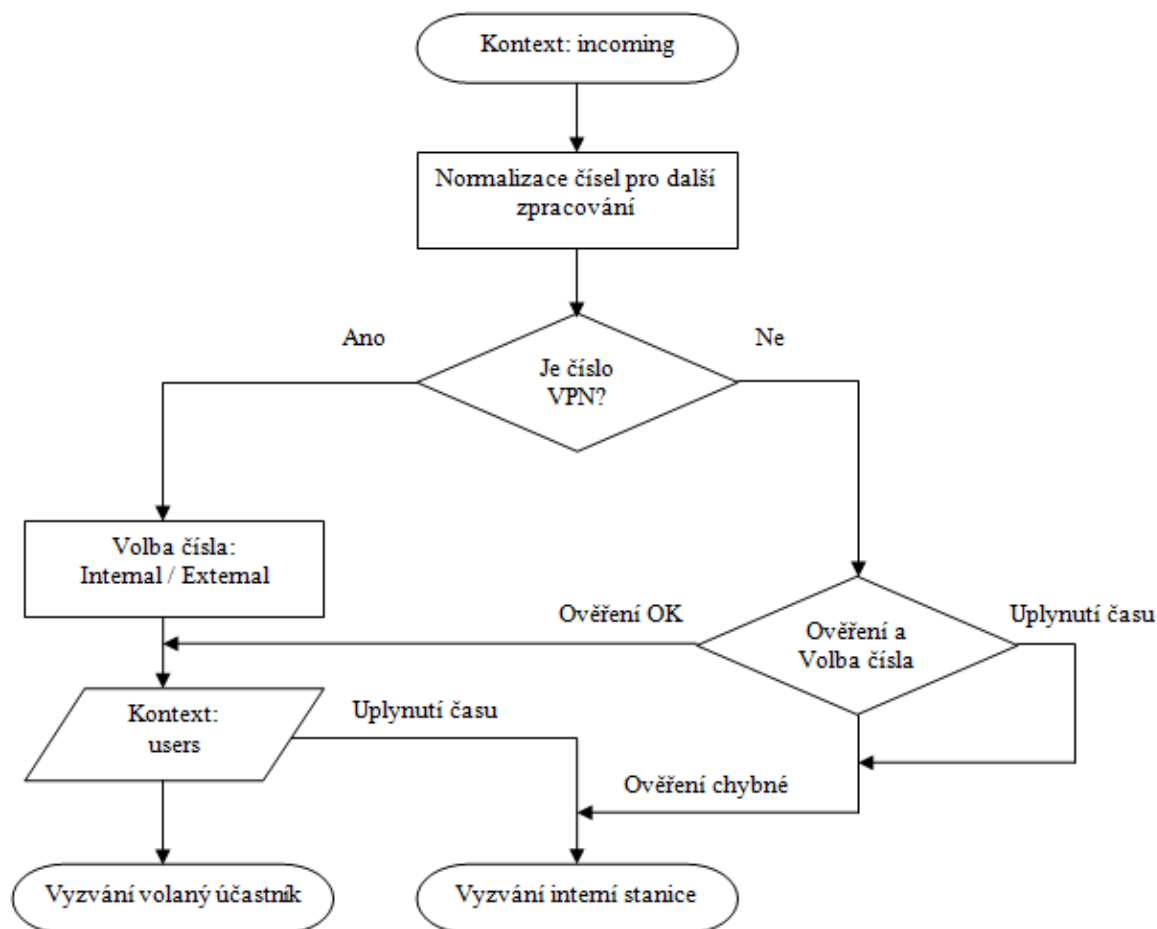
Začátek příchozího volání začíná v kontextu „incoming“. V našem případě je to volání na extension 343. Pro zpracování příchozího hovoru algoritmus upravuje identifikační číslo z mezinárodního na národní formát. To znamená na číslo délky 9 znaků. Tato normalizace je potřeba ošetřit jen na GSM branách, kde se používá číslo v mezinárodním formátu. Pevní poskytovatelé telefonních služeb předávají číslo již v národním formátu.

Následuje porovnání čísla volajícího. Pokud je volající členem sítě VPN, předá algoritmus hovor do menu, kde je možná jak volba interních, tak externích uživatelů, přes kontext „users“. Jestliže člen sítě VPN neprovede žádnou volbu v menu, po uplynutí časového intervalu, přejde volání na defaultně nastaveného uživatele, v našem případě na extension 331.

Jiná situace nastane, není-li volající členem VPN skupiny. Algoritmus jej vyzve k zadání hesla, které mu umožní přístup do menu a následně libovolné volbě. Zde mohou nastat tři situace:

1. Uživatel zná heslo – pokračuje ve volbě čísla stanice, se kterou chce hovořit.
2. Uživatel nezná heslo – po vypršení časového intervalu zvoní defaultní stanice.
3. Uživatel zadá špatné heslo - zvoní ihned defaultní stanice (má dva pokusy).

Grafické znázornění funkce routovacího algoritmu, přibližuje více vývojový diagram na obrázku 12.



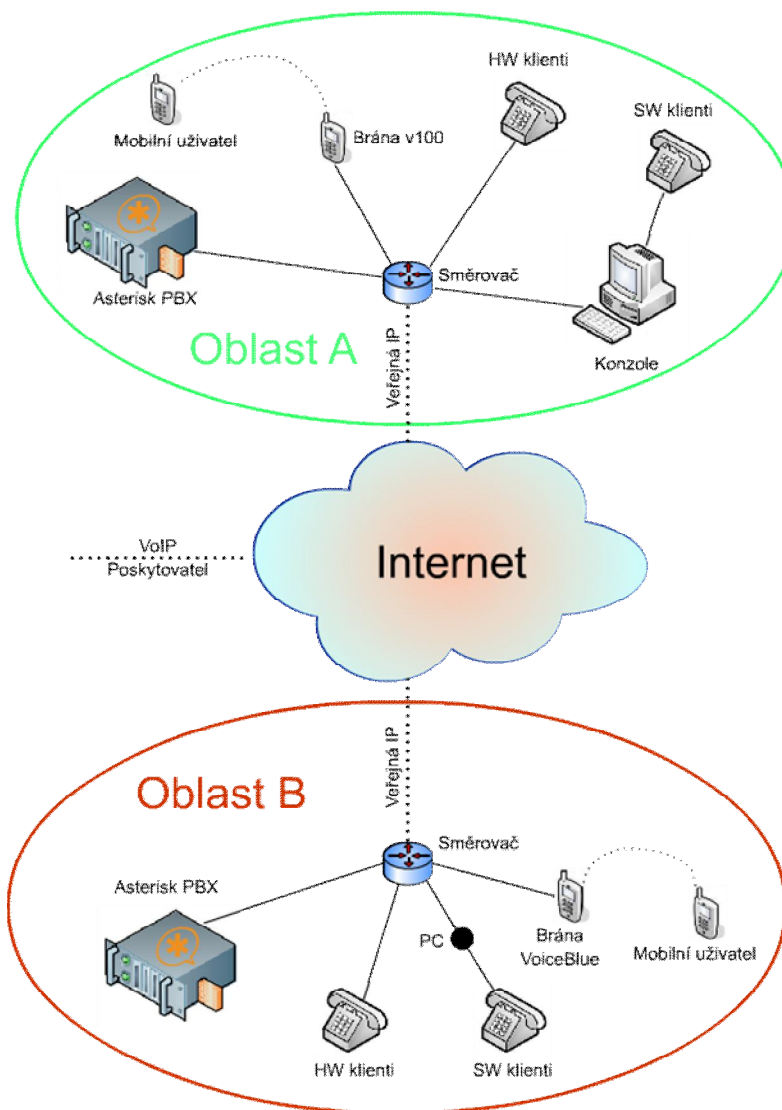
Obr. 15 – Schéma routovacího algoritmu

4.3 Zapojení testovací HW části serverů Asterisk

Pro testovací účely, bylo vytvořeno zapojení s dvěma oblastmi. Oblast A znázorňuje hlavní ústřednu, na které byly všechny zde popisované funkce vyzkoušeny. Tato oblast obsahuje i uživatele mobilní VPN skupiny. Všechny komponenty zapojení, ústředna Asterisk, HW a SW klienti, VoIP brána a konzole jsou pomocí směrovače s přepínačem zapojení na malé lokální síti. Směrovač je připojen k běžné internetové síti. Oblast B obsahuje podobné zapojení, a je odlehčená o některé prvky.

Obě oblasti jsou od sebe vzdáleny cca 10km. Směrovače na portech WAN používají veřejnou IP adresu. Jsou nastaveny tak, aby směrovaly příchozí spojení na portech 5060 (SIP), 4569 (IAX) a 22 (konzole přes SFTP) na server Asterisk.

Konzole je servisní počítač, kterým se lze připojit k oběma ústřednám Asterisk, pro jejich zprávu a konfiguraci (Putty, WinSCP).



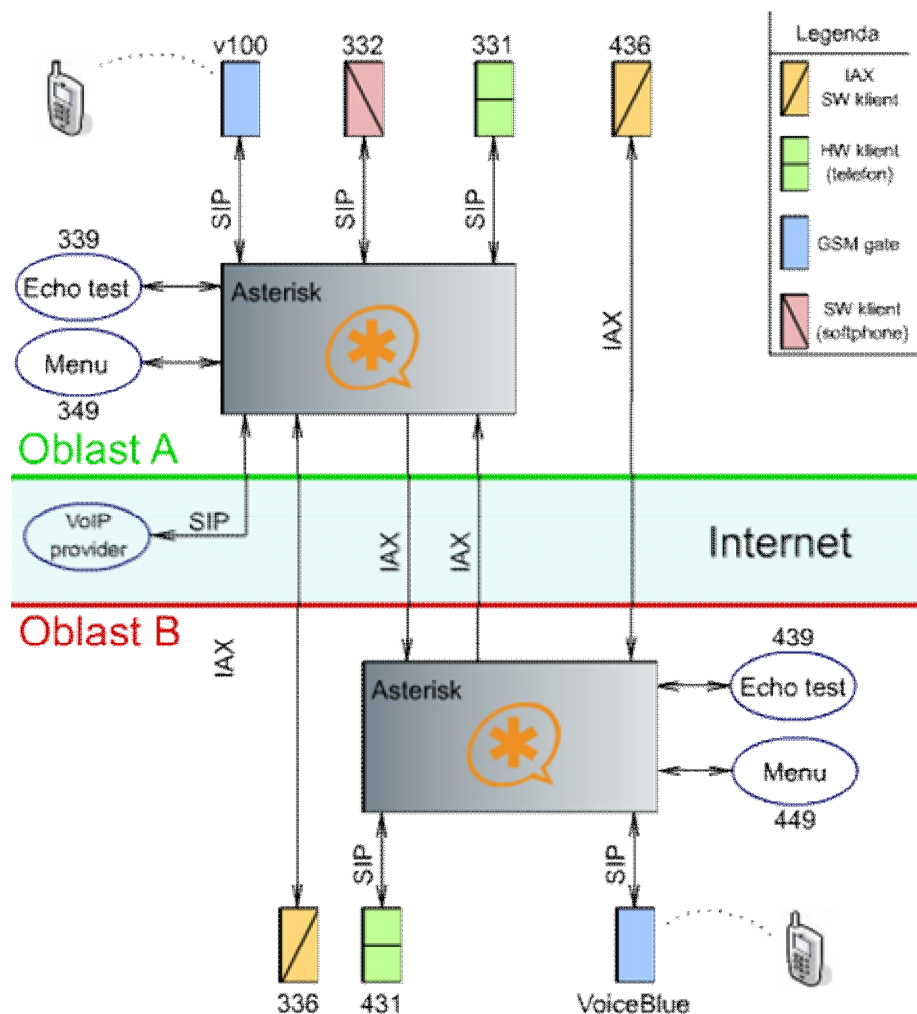
Obr. 16 – Síťové testovací zapojení HW

Jsou použity standardní HW klienti (VoIP telefony), např. Linksys, Gradnstream, atd. Jako SW klienti jsou použity: eyeBeam vycházející z projektu x-Lite (podpora SIPu) a Zoiper (podpora IAXu i SIPu). Brány do GSM sítí: Soundwin V100 a Ateus 2N VoiceBlue.

Servery Asterisk jsou nainstalovány na vyřazených PC platformy Pentium. Použitá instalace AsteriskNOW, běžící pod operačním systémem Linux Centos.

4.4 Testovací zapojení telefonní sítě

Ke každé ústředně je připojeno několik klientů (extension), pro základní ověření funkce. Každá z ústředěn používá vlastní číslovací plán. Pro oblast A jsou to extensions začínající číslicí 3xx, pro oblast B číslicí 4xx. Pro snazší kontrolu a testování sítě, je do každé oblasti přihlášen klient druhé ústředny (436 a 336), používající protokol IAX. Obě ústředny mají připojenou SIP/GSM bránu a jsou navzájem hlasově propojeny opět protokolem IAX. Ústředna oblasti A je připojena k veřejnému poskytovateli VoIP služeb.



Obr. 17 – Zapojení telefonní sítě

V tomto testovacím zapojení, slouží servery Asterisk i jako brány mezi jednotlivými protokoly (SIP-IAX, IAX-SIP).

4.5 Základní nastavení směrování hovorů

Všechny možnosti směrování (volání), vychází z číslovacího plánu Asterisku, uloženém v souboru *extensions.conf*. Použitá rozhraní (trunkky nebo účty) se konfiguruje v *sip.conf* a *iax.conf*. Popis konfigurace se vždy vztahuje k oblasti A. Na konfigurační soubor jiné oblasti bude vždy upozorněno.

Směrování hovorů vždy začíná v souboru *extensions.conf* volbou čísla (lze použít i jméno). Podle typu čísla se použije příslušný algoritmus, provede se patřičná funkce nebo se pokračuje do dalšího kontextu.

4.5.1 Konfigurace účtů

4.5.1.1 Konfigurace sip.conf

Konfigurace účtů pro připojení GSM brány již byla popsána. Následující výpis ukazuje globální nastavení a nastavení účtu veřejného poskytovatele a klientů (extensions) používající SIP protokol.

```
[general]
port = 5060
context = users
disallow = all
allow = alaw
allow = ulaw
dtmfmode = auto
language = cz

register => 581111799:heslo@212.71.146.175:5060/581111799

[stul]
type = friend
username = stul
userid = Stul <331>
host = dynamic
allow = ulaw

[client]
...

;=====Fixed provider=====
[my_802_provider]
type = friend
host = hlas.802.cz
username = 581111799
fromuser = 581111799
secret = heslo
fromdomain = hlas.802.cz
context = incoming
dtmfmode = rfc2833
disallow = all
allow = alaw
allow = ulaw
deny = 0.0.0.0/0
permit = 212.71.146.175/32
insecure = invite
```

Tab. 11 – Konfigurace sip.conf

Kontext [general] popisuje použité porty pro SIP komunikaci, použité kodeky, mód DTMF, výchozí jazykovou sadu pro texty na displeji a jazykové hlášky a odkaz na výchozí kontext `context = users`, kde začíná práce s číslovacím plánem. Položka `register =>` říká serveru Asterisk, aby provedl registraci účtu k poskytovateli VoIP ve tvaru: uživatelské jméno, heslo, doména poskytovatele, komunikační port a „exten“ pro příchozí hovor.

Konfigurační soubor také obsahuje i kontexty uživatelů, definující registrační a upřednostňující nastavení uživatelů např. [stul].

Nastavení účtu poskytovatele VoIP má kontext `[my_802_provider]`, ve kterém je definováno uživatelské jméno, heslo, doména, výchozí DTMF a kodek. Ověřovací parametr `type` je hodnoty `friend` určující směr ověřování v obou směrech. Parametr `deny` zakazuje přístup ze všech IP adres v síti nulovou hodnotou IP adresy a masky, proto je potřeba registračnímu serveru umožnit přístup parametrem `permit`, kde je definovaná jeho IP včetně masky. Parametr `insecure = invite` slouží pro příchozí autentifikaci, vycházející z parametru `INVITE` v SIP hlavičce volání. Kontext, bez kterého by nefungovalo příchozí volání, odkazující se na hodnotu `incoming` v číslovacím plánu `extensions.conf`.

4.5.1.2 Konfigurace `iax.conf`

Následující výpis ukazuje globální nastavení, nastavení účtů (trunků) a klientů (extensions) používající IAX protokol.

```
[general]
Bindport = 4569
bindaddr = 192.168.0.103
iaxcompat = yes
delayreject = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm

[iaxclient]
type = friend
username = iaxclient
userid = Client <337>
host = dynamic
secret = heslo
context = users

[iaxtrunk]
type = user
username = iaxtrunk
host = dynamic
secret = heslo
context = users
```

Tab. 12 - Konfigurace `iax.conf`

Standardní výchozí nastavení kontextu `[general]` obsahuje nastavení komunikačního portu, IP adresy serveru, komunikačních kodeků, kompatibility mezi Asterisky `iaxcompat=yes` a použití zpoždění `delayreject = yes` pro odeslání odmítnutí při zadání nesprávného hesla.

Nastavení účtů klientů je stejné, jako v konfiguraci `sip.conf`. Zajímavý je účet `[iaxtrunk]`, sloužící k vzájemnému propojení Asterisků. Opět musí být nastavena důležitá položka `context` určující přiřazení kontextu v číslovacím plánu.

4.5.2 Číslovací plán v souboru *extensions.conf*

4.5.2.1 Odchozí volání

Konfigurace v každém kontextu se skládá z jednoduchých pravidel. Každé pravidlo začíná klíčovým slovem *exten*. Pro snadnější orientaci bylo zvoleno číslování jednotlivých řádků.

Celý číslovací plán začíná v kontextu `[users]`, kde je definováno celé jádro volacího systému. Řádek 2 až 9 definuje standardní uživatele. Uživatel 331 má nastavené přeměrování volání po 20s vyzvánění na mobilní telefon (po 20 s skok na další prioritu).

Programový krok 10 definuje odchozí volání začínající číslicí 4xx do ústředny v oblasti B. Použita je registrace ke vzdálené ústředně při sestavování spojení, s předáním celé adresy systémem INVITE.

```

1. [users]

2. exten => 331,1,Dial(SIP/stul,20)
3. exten => 331,n,Dial(SIP/v100/777573684)
4. exten => 332,1,Dial(SIP/client)
5. exten => 333,1,Dial(SIP/host1)
6. .
7. .
8. .
9. exten => 337,1,Dial(IAX2/iaxclient)
10. exten => _4XX,1,Dial(IAX2/iaxtrunk2:psw@82.114.208.81/${EXTEN:0})
11. exten => _4XX,n,Hangup()

12. exten => _7XXXXXXXX,1,GotoIf($[${EXTEN:0}=724269926]?4:2)
13. exten => _7XXXXXXXX,2,Dial(SIP/v100/${EXTEN:0},,r)
14. exten => _7XXXXXXXX,4,Goto(second_pbx,724269926,1)
15. exten => _6XXXXXXXX,1,Dial(SIP/v100/${EXTEN:0},,r)
16. exten => _2XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
17. exten => _3XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
18. exten => _4XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
19. exten => _5XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
20. exten => _8XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
21. exten => _0XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)

22. include => services

23. [services]

24. exten => 348,1,Answer()
25. exten => 348,n,Playback(demo-echotest)
26. exten => 348,n,Echo()
27. exten => 348,n,Hangup()

28. exten => 349,1,LookupCIDName
29. exten => 349,2,goto(menu,s,1)

30. exten => 343,1,LookupCIDName
31. exten => 343,2,goto(virtual_net,s,1)

```

Tab. 13 – Odchozí volání

Na řádku 12 až 21 jsou definována odchozí čísla do národní telekomunikační sítě. Řádek 12 kontroluje čísla do mobilních sítí začínajících číslem 7... Dále porovnává, není-li volené číslo, číslem vzdálené ústředny (VPN oblasti B). Jestliže se číslo shoduje s číslem pro porovnání, pokračuje se na prioritu 4 (řádek 14), kde dojde ke skoku do kontextu „sekond_pbx“ s předáním čísla. Volba pokračuje již v ústředně s využitím GSM brány a VPN systému oblasti B. Pokud se volané číslo neshoduje, řádek 12 pokračuje na prioritu 2, zde se volané číslo předá gsm bráně pomocí kontextu [v100], na trunk přenašeč. Parametr „r“ na konci řádku určuje generování prvního vyzváněcího tónu ústřednou Asterisk. Mezi řádkem 13 a 14 chybí prioritizované číslo 3. Zde lze doplnit další číslo hostitelské ústředny.

Podobný algoritmus volání platí i pro ostatní volená čísla, jen s rozdílem použití trunk přenašeče řádek 15 až 21.

Výpis řádku 22 vkládá kontext „services“ do kontextu „users“ a stává se jeho součástí. V kontextu „services“ se nalézají: testovací volání 348 s echo testem, skok do menu s číslem 349 řádek 29 a skok do databáze mobilních VPN uživatelů číslem 343 řádek 31.

4.5.2.2 Příchozí volání

Definice příchozích volání se nachází v kontextu [incoming]. Sem jsou odkazovány hovory z definovaných účtů. Řádek 2 zpracovává volání od VoIP poskytovatele, po 15s pokračuje na další prioritu s číslem 2, kde dojde ke skoku do již zmíněné databáze mobilních VPN uživatelů. Řádek 4 definuje skok do kontextu pro normalizaci čísel, použitý u příchozího volání z GSM brány.

```
1. [incoming]
2. exten => 581111799,1,Dial(SIP/stul,15)
3. exten => 581111799,2,Goto(virtual_net,s,1)
4. exten => 343,1,goto(normalizing,s,1)
```

Tab. 14 – Příchozí volání

4.5.2.3 Normalizace čísel z GSM sítě

Jelikož je potřeba ošetřit vstupní informace o volajícím čísle (CLIP), které GSM brány předávají v mezinárodním formátu, tzn. s prefixem státu (u nás 420), je vytvořen kontext, v kterém probíhá úprava identifikace čísla volajícího na národní formát.

Jednoduchý algoritmus vychází z délky národního (9 znaků) a mezinárodního (12 znaků) čísla. Na řádku 2 se převezmeme číslo z GSM brány CALLERID(num) odstraní

```
1. [normalizing]
2. exten => s,1,SetCallerID(${CALLERID(num):3})
3. exten => s,n,NoOp(${CALLERID(num)})
4. exten => s,n,goto(virtual_net,s,1)
```

Tab. 15 – Normalizace čísel

první tři číslice a uloží do proměnné `SetCallerID`. Zvláštní příkaz „NoOp“ vlastně nedělá nic důležitého. Tento příkaz zobrazuje v konzolovém výpisu již upravené číslo. Takto upravené číslo pokračuje na další kontext, nazvaný `[virtual_net]`, kde je algoritmus pro volbu mobilních VPN uživatelů.

4.5.2.4 *Ověření VPN mobilního uživatele*

Kontext `[virtual_net]` porovnává příchozí čísla a hledá shodu. Zde je využito podmíněných skoků pomocí příkazu `GotoIf`. Jeli číslo `CALLERID(num)` stejné s číslem za porovnávacím znakem “=” dojde ke skoku priority na hodnotu 10, která se nachází na řádku 7. Není-li nalezena shoda, pokračuje se na další řádek. Takto se prohledává databáze čísel, která mohou používat rozšířené funkce a služby ústředny Asterisk. Čísel může být libovolné množství, jen je potřeba správně zvolit hodnotu priority určující kladnou hodnotu porovnání.

Řádek 6 odkazuje do kontextu k dalšímu ověření volajícího uživatele, který v předcházejících řádcích nenašel shodu. Řádek 7 odkazuje po úspěšném ověření identifikace volaného do kontextu, kde již může provést další volbu požadovaného účastníka.

```

1. [virtual_net]

2. exten => s,1,NoOp(${CALLERID(num)}) ;overeni delky cisla
3. exten => s,2,GotoIf($[${CALLERID(num)}=777573685]?10:3)
4. exten => s,3,GotoIf($[${CALLERID(num)}=777573684]?10:4)
5. exten => s,4,GotoIf($[${CALLERID(num)}=581111784]?10:5)
6. exten => s,5,Goto(verify,s,1)

7. exten => s,10,Goto(menu,s,1)

```

Tab. 16 – Ověření VPN

4.5.2.5 *Hlasové menu*

Byla-li kontrola volajícího mobilního uživatele úspěšná, pokračuje volání do kontextu `[menu]`. Z důvodu kompletního zpoždění je volajícímu indikován vyzváněcí tón do doby, než dojde k přehrávání menu, aby nedošlo k useknutí začátku přehrávání zprávy. Tento čas nastavuje parametr `wait(2)`. Řádek 4 provádí vyzvednutí hovoru Asteriskem (`connect`), a řádek 7 spouští přehrávání hlášky na pozadí. Parametr `TIMEOUT` nastavuje důležitý čas (`digit`)=3 určující dobu mezi zadáním jednotlivých znaků v DTMF.

```

1. [menu]

2. exten => s,1,Ringing()
3. exten => s,n,Wait(2)
4. exten => s,n,Answer()
5. exten => s,n,Set(TIMEOUT(digit)=3)
6. exten => s,n,BackGround(menu)
7. include => users
8. exten => s,n,WaitExten(10)

```



```
9. exten => s,n,Dial(SIP/stul)
```

Tab. 17 – Menu

Následuje přehrání hlášky `BackGround(menu)`, která se nachází v adresáři operačního systému `/var/lib/asterisk/sounds`.

Syntaxe `include => users` vloží číslovací plán do menu, a tím umožní uživatelům kompletní využití tohoto plánu. Není-li voleno žádné číslo, nastane čekání 10s pomocí příkazu `WaitExten(10)`. Po uplynutí času přejde systém k automatické volbě defaultní stanice určené řádkem 9.

4.5.2.6 *Ověření neznámého uživatele*

Tato možnost byla přidána pro přístup uživatelů, kteří nejsou součástí VPN, ale jsou oprávněni použít celý volací systém. Kontext `[verify]` musí ošetřit všechny tři již zmíněné stavy. Začátek je stejný jako v kontextu `[menu]`, zpožděné vyzvednutí před přehráním hlášky. Následuje příkaz `Authenticate(0000, j)` s parametrem „0000, j“. Číslo v závorce určuje hodnotu hesla a znak „j“ doplňuje příkaz o skok na prioritu `n+101` v případě chybného zadání. Nežadá-li uživatel heslo do defaultně nastaveného času, je hláška několikrát opakována a chování je stejné jako při chybném zadání.

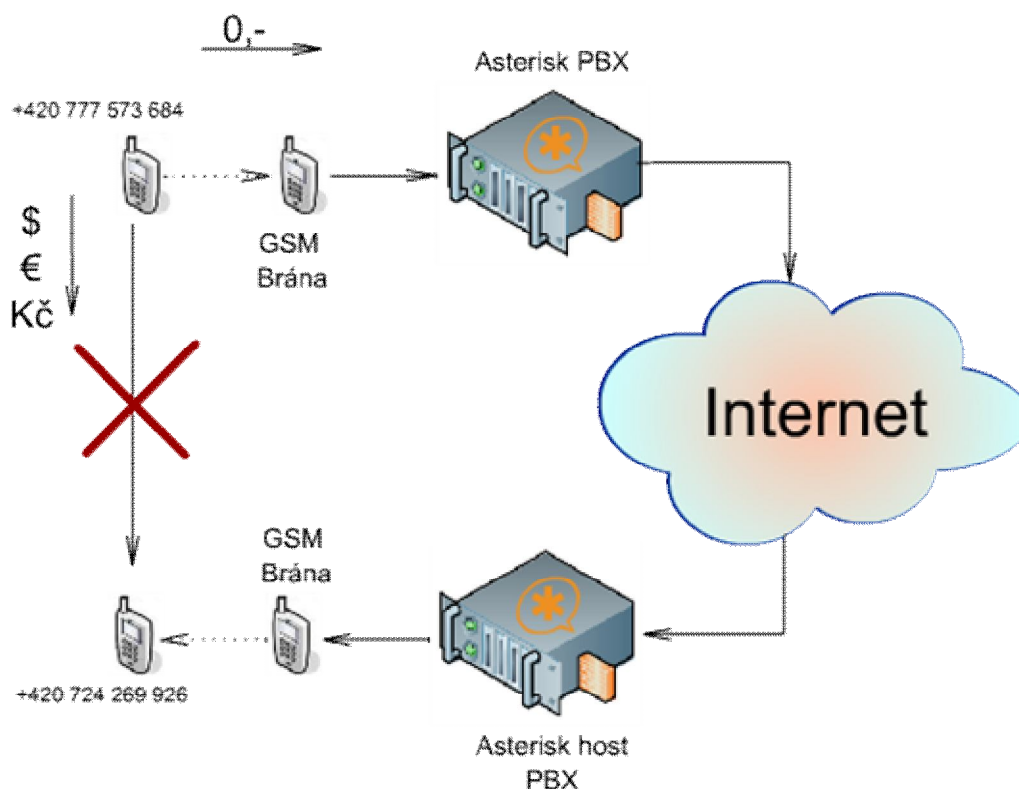
```
1. [verify]
2. exten => s,1,Ringing()
3. exten => s,n,Wait(2)
4. exten => s,n,Answer()
5. exten => s,n,Authenticate(0000,j)
6. exten => s,n,Goto(menu,s,1)
7. exten => s,105,Dial(SIP/stul)
```

Tab. 18 – Ověření uživatele

5 ALTERNATIVA VOLÁNÍ UŽIVATELŮ MIMO VPN ROZSAH

5.1 Spojení mezi hostitelskými ústřednami

Aby mobilní uživatel měl bezplatné spojení na jiného mobilního uživatele mimo rozsah VPN, při použití svého systému Asterisk nakonfigurovaného jako předcházející popis, musí uživatel mimo rozsah VPN použít stejný systém Asterisk (viz 4.5.2.1). Pro odchozí volání stačí do kontextu `[users]` definovat číslo mobilního uživatele mimo rozsah VPN.



Obr. 18 – Cesta levnějšího spojení

Cestu sestavení spojení ukazuje obrázek. Mobilní uživatel vytočí číslo své GSM brány připojené k systému Asterisk, po úspěšném ověření přejde volání do hlasového menu, kde může volit číslo mobilního uživatele mimo rozsah VPN. Je-li číslo v seznamu, dojde k sestavení volání Asterisk – Asterisk a dále přes GSM bránu hostitelské ústředny na mobilní telefon uživatele hostitelské ústředny.

Tento systém se opírá o znalost čísel, uložených v konfiguračním souboru `extensions.conf`. Nebude-li volané číslo systém Asterisk znát, spojí hovor běžným způsobem. Proto se zde naskýtá použití systému ENUM.

5.1.1 ENUM

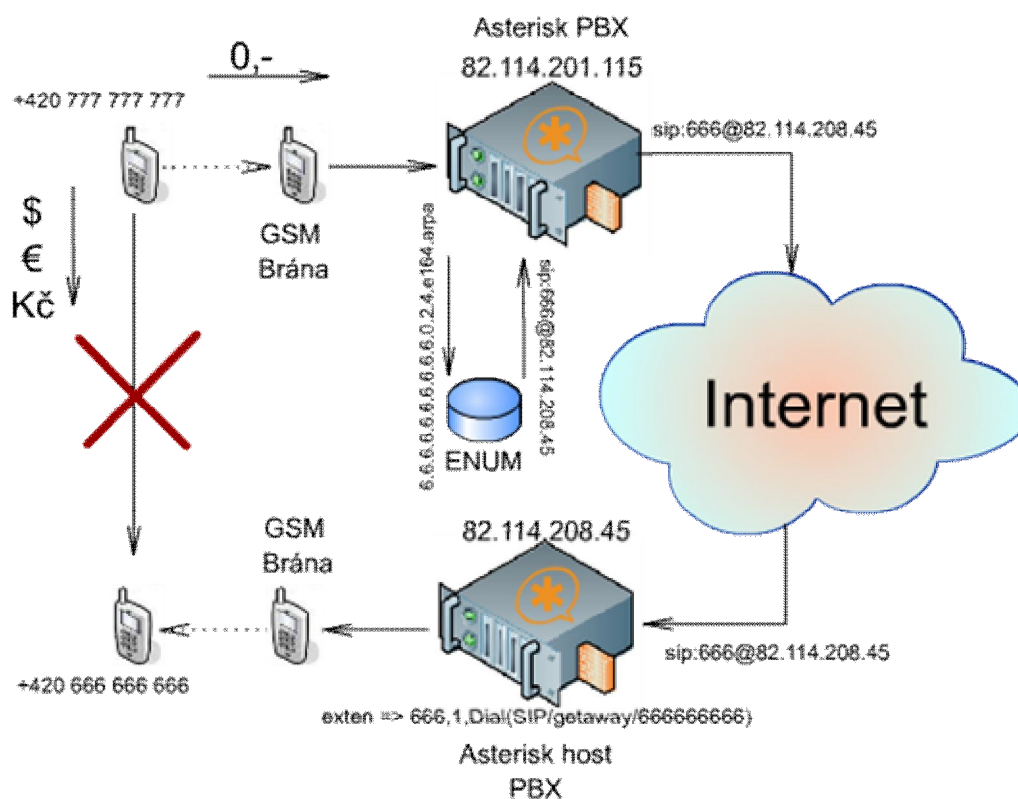
Telephone Number Mapping (anglicky *mapování telefonních čísel*, zkráceně ENUM) je soubor protokolů, které mají za cíl sjednotit telefonní systém s internetem za použití adres E.164 s DDNS a DNS. ENUM také označuje „E164 Number Mapping“. ENUM je

protokol založený na DNS, který poskytuje vhodné služby, které pomáhají uskutečnit hovor, ale rozšiřuje i možnosti spojení o další DNS služby.

ENUM dovoluje zveřejnit k telefonnímu číslu informaci, jak se na něj dovolat přes internet. Zbytek již obstará telekomunikační infrastruktura podporující ENUM, která při vytočení telefonního čísla vždy nejprve zjistí, zdali se může spojit s telefonem volaného účastníka přes internet. Pokud ano, hovor je spojen tímto způsobem a je zdarma. V případě, že propojení přes internet není možné, hovor proběhne běžnou cestou po telefonních linkách veřejné telefonní sítě (PSTN) a je zpoplatněn dle aktuálních cenů telefonních operátorů.

5.2 Využití ENUMu mimorozsahové VPN

Této skutečnosti se dá využít při spojení na číslo mimo rozsah VPN, kdy ústředna Asterisk vznese požadavek na ENUM server. Jestliže ENUM najde vhodný záznam, Asterisk jej použije k sestavení spojení. Schéma je na následujícím obrázku.



Obr. 19 – Využití ENUMu

Volající uživatel sestaví spojení se svým serverem Asterisk. V hlasovém menu volí číslo 666 666 666 požadovaného mobilního uživatele. Asterisk předá dotaz na ENUM server v požadovaném formátu `6.6.6.6.6.6.6.6.0.2.4.e164.arpa`. ENUM server vrátí adresu sip `sip:666@82.114.208.45`, kterou Asterisk použije a sestaví odchozí volání. V hostitelské ústředně Asterisk přijme volání a vytočí požadované číslo do GSM brány (`exten => 666,1,Dial(SIP/getaway/666666666)`).

5.3 Nastavení Asterisku použití ENUM / VPN

5.3.1 Odchozí volání

Je vhodné vytvořit vlastní kontext např. `[enum]`, na který bude v systému asterisk odkazováno. Před použitím je potřeba vytvořit normalizační tabulku, pro úpravu čísel na mezinárodní formát, vyžadovaný ENUM systémem.

```
[enum]
exten => _00420.,1,Set(ENUM=${ENUMLOOKUP(+${EXTEN:2}|sip|||e164.arpa)})
exten => _00420.,2,Dial(SIP/${ENUM})
exten => _00420.,3,HungUp()
```

Tab. 19 – odchozí volání přes ENUM

Volbou čísla se do proměnné `${ENUM}` nastaví hodnota získaná příkazem `ENUMLOOKUP`. Předtím se přestupné znaky prefixu „00“ nahradí znakem „+“ `+${EXTEN:2}`. Požadavek na server ENUM je, aby byla vrácena pouze sip adresa. Takto získaná adresa se použije v příkazu `Dial(SIP/${ENUM})`. Není-li nalezený záznam, dojde k ukončení hovoru, znamenající nedostupnost jakékoliv alternativy použití systému levného volání.

5.3.2 Příchozí volání

V hostitelské ústředně už je jen třeba ošetřit příchozí volání. V tabulce je syntaxe umístěná v kontextu `[incoming]`, volající přímo mobilního uživatele.

```
exten => 666,n,Dial(SIP/gsm_gateway/666666666)
```

Tab. 20 – příchozí volání z ENUM

5.4 Motivace ENUM

Z nastíněné situace plyne skutečnost, že pro správnou funkci je potřeba provést ENUM registraci (záznam v registru ENUM). I když tento systém neumožňuje identifikaci volajícího, umožní ostatním uživatelům bezplatné volání, bez znalosti telefonních čísel jiných takto zapojených systémů. Při registraci několika čísel tohoto systému, vznikne rozsáhlá síť umožňující oboustranné bezplatné volání, aniž by se uživatelé těchto systémů vzájemně znali.

ZÁVĚR

Asterisk se v dnešní době jeví mnohem pružněji k telefonním službám. Lze ho v podstatě naprogramovat dle libovolného nápadu, funkce a služeb proti TDM ústřednám, kde lze nastavit jen to, co výrobce implementuje dle svého uvážení, které je samozřejmě ovlivněno trhem. Zatímco Asterisk má svůj programovací jazyk syntaxi souborů *conf*. Ten nám umožní „vyrobit“ jakoukoliv funkcionalitu dle aktuálních požadavků. Velká síla ústředny Asterisk je v propojení databází a to jak vlastního formátu databázového systému, tak možnost použití relačních databází (MySQL). Proto můžeme začlenit telefonní službu do rychle se rozvíjejících sítí (Internetu) a integrovat tak jakoukoliv službu s libovolnou službou na bázi protokolu IP.

CONCLUSION

Asterisk seems to be more flexible to the phone services nowadays. Basically it is possible to programme it according to any idea, function and service in comparison with TDM exchange, where you can set up only at the discretion of the producer who is impressed with the market of course. Whereas Asterisk has its own programming language syntax of files *conf*. This makes us possible to „make“ any functionality according to actual requirements. The great power of Asterisk is in his connected databases both own database system and the possibility of using related database (MySQL). That's why we can incorporate the phone service to the quickly developing internet networks and so we can integrate any service with optional service based on IP protocol.

SEZNAM POUŽITÉ LITERATURY

- [1] JIM, Van Meggelen, LEIF, Madsen, JARED, Smith. Asterisk : The Future of Telephony. Mike Loukides; Robert Romano and Jessamzn Read. 2nd enl. edition. Sebastopol : O'Reilly Media, 2007. xxv, 574 s. ISBN 978-0-596-51048-0.
- [2] SYSEL, Martin. Operační systémy GNU/Linux. 1. vyd. Zlín: Univerzita Tomáše Bati Academia centrum, 2006. 77 s. ISBN 80-7318-489-3.
- [3] Asterisk :: The Open Source PBX & Telephony Platform [online]. Digium, Inc, c2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.asterisk.org> .
- [4] [IpTelWiki] : Asterisk PBX [online]. [2005], 2008/10/31 [cit. 2009-01-30]. Dostupný z WWW: <https://sip.cesnet.cz/cs/swahw/asterisk>.
- [5] Celliax: eigenbau GSM anbindung per Daten/Audiokabel Asterisk Allgemein [online]. 2000-2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.ip-phone-forum.de/showthread.php?t=142983> .
- [6] V100 - GSM VoIP ATA brána, 1x WAN, 1x FXS, 1x PSTN, 1x SIM, H.323/SIP [online]. c2009 [cit. 2009-01-30]. Dostupný z WWW: <http://www.i4wifi.cz/?cls=stoitem&stiid=1156> .
- [7] ICamp SIP server [online]. [2006] [cit. 2009-01-30]. Dostupný z WWW: <http://sip.icamp.eu>
- [8] *Voice over Internet Protocol* [online]. Wikipedia, 2009 , Editováno 28. 4. 2009 v 14:57 [cit. 2009-05-10]. Dostupný z WWW: <<http://cs.wikipedia.org/wiki/Voip>>.
- [9] VOŽŇÁK, Miroslav. TECHNICKÉ PRINCIPY IP TELEFONIE. *Teorie a praxe IP telefonie* [online]. 2004 [cit. 2009-05-10]. Dostupný z WWW: <http://www.ip-telefon.cz/archiv/dok_osta/ipt-2004_Principy_IPtel.pdf>.
- [10] VOŽŇÁK, Miroslav. SIGNALIZACE SIP. *Teorie a praxe IP telefonie* [online]. 2006 [cit. 2009-05-10]. Dostupný z WWW: <http://www.ip-telefon.cz/archiv/dok_osta/ipt-2006_Signalizace_SIP.pdf>.
- [11] *SIP* [online]. Cesnet, [2006] , Poslední úprava: 2007/03/19 16:42 [cit. 2009-05-10]. Dostupný z WWW: <<https://sip.cesnet.cz/cs/protokoly/sip>>.
- [12] PETR, Kovář, KAROL, Molnár. Využití protokolu IAX pro spojení mezi ústřednami. *Elektrorevue* [online]. 2008 [cit. 2009-05-10]. Dostupný z WWW: <<http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/vyuziti-protokolu-iax-pro-spojzeni-mezi-ustrednami/>>. ISSN 1213-1539.
- [13] MIROSLAV, Vožňák. *Voice over IP*. 1. vyd. Ostrava : VŠB-TU Ostrava, 2008. 176 s. ISBN 978-80-248-1828-3.
- [14] VOŽŇÁK, M., ZUKAL, D.. *Kvalita hovoru v prostředí VoIP* [online]. V 0.1 Released. Praha : Cesnet, 2005 [cit. 2009-05-16]. Dostupný z WWW: <<http://www.cesnet.cz/doc/techzpravy/2005/voip/kvalitahovoru.pdf>>.
- [15] *SILK* [online]. SKYPE, [2008] [cit. 2009-05-16]. Dostupný z WWW: <<https://developer.skype.com/silk?action=AttachFile&do=get&target=SILKDataSheet.pdf>>.
- [16] WIJA, Tomáš, ZUKAL, David, VOŽŇÁK, Miroslav. *Asterisk a jeho použití* [online]. verze 0.2. Praha : Cesnet, 2005 [cit. 2009-05-16]. Dostupný z WWW: <<http://www.cesnet.cz/doc/techzpravy/2005/voip/asterisk.pdf>>.
- [17] VOŽŇÁK, Miroslav. *TELEFONNÍ ÚSTŘEDNY ASTERISK* [online]. 2008 [cit. 2009-05-16]. Dostupný z WWW: <http://www.ip-telefon.cz/archiv/dok_osta/ipt-2008_Telefonni_ustredny_Asterisk.pdf>.

- [18] HRUŠKA, Petr. *Konfigurace Asterisku (3) - extensions.conf* [online]. 2009 [cit. 2009-05-16]. Dostupný z WWW: <<http://www.telegro.cz/2009/04/12/konfigurace-asterisku-3-extensionsconf>>.
- [19] *Soundwin V100 : GSM GATEWAY User Manual* [online]. Version: 1.07. Sounwin, 2008 [cit. 2009-05-16]. Dostupný z WWW: <<http://www.i4wifi.cz/img.asp?attid=97586>>.
- [20] *VoiceBlue with Asterisk IP PBX - How to* [online]. Praha : 2N, c2007 [cit. 2009-05-16]. Dostupný z WWW: <http://www.2n.cz/news/press_releases/voiceblue_with_asterisk.html>.
- [21] *Telephone Number Mapping* [online]. Wikipedia, [2008] , 18. 2. 2009 [cit. 2009-05-16]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Telephone_Number_Mapping>.
- [22] *Co je ENUM* [online]. CZ.NIC, [2007] [cit. 2009-05-16]. Dostupný z WWW: <<http://enum.nic.cz/page/270/co-je-enum/>>.
- [23] KOVÁŘ, Petr, MOLNÁR, Karol, NOVOTNÝ , Vít. *Současnost a budoucnost VoIP sítí* [online]. Brno : VUT Brno, 2007 [cit. 2009-02-04]. Dostupný z WWW: <<http://www.elektrorevue.cz/cz/download/soucasnost-a-budoucnost-voip-siti/>>. ISSN 1213-1539.
- [24] DULÍK, Tomáš. *Open Source and Open Standards VOIP communication : iCamp project internal technical report*. [s.l.] : [s.n.], 2007. s. 1-17.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TDM	Označení klasických telefonních ústředen na bázi přepínání okruhů.
PBX	Private Branch Exchange - telefonní ústředna.
PSTN	Standardní telefonní síť, kterou veřejnost používá k realizaci místních, meziměstských i mezinárodních telefonních hovorů.
DNS	Domain Name System je hierarchický systém doménových jmen. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
DDDS	Dynamic Delegation Discovery System je způsob uložení dat (adres) používaný v systému ENUM. Záznamy uložené v DDDS obsahují informaci o tom, jak telefonní číslo E.164 převedené na název domény následovně převést na číslo (resp. adresu) libovolného VoIP operátora.
CLIP	Calling Line Identification Presentation - zobrazení identifikačního čísla volajícího.

SEZNAM OBRÁZKŮ

Obr. 1 – Použití metody REGISTER	17
Obr. 2 – Ukázka metod a odpovědí.....	17
Obr. 3 – Navázání spojení pomocí SIP serveru.....	18
Obr. 4 - IAX rámce - FullFrame a MiniFrame	20
Obr. 5 – Vlastnosti TCP/IP v PC	32
Obr. 6 - GSM parametry.....	33
Obr. 7 – VoIP parametry I.....	34
Obr. 8 – VoIP parametry II.....	34
Obr. 9 – Dial plán	35
Obr. 10 – Nastavení DTMF	35
Obr. 11 – Hotline číslo.....	36
Obr. 12 – Port Status, příchozí volání z GSM do Asterisku.....	37
Obr. 13 – Port Status, odchozí volání z Asterisku do GSM.....	37
Obr. 14 – Autorouting tabulka VoiceBlue.....	39
Obr. 15 – Schéma routovacího algoritmu	41
Obr. 16 – Síťové testovací zapojení HW	42
Obr. 17 – Zapojení telefonní sítě	43
Obr. 18 – Cesta levnějšího spojení.....	50
Obr. 19 – Využití ENUMu.....	51

SEZNAM TABULEK

Tab. 1 – Paket RTP a jeho hlavičky (40 oktetů)	12
Tab. 2 - Tabulka kodeků a hodnot MOS	22
Tab. 3 – Ukázka kontextů.....	27
Tab. 4 – Pravidla extensions.....	27
Tab. 5 – Práce s řetězci.....	29
Tab. 6 – Konfigurace účtů	29
Tab. 7 – Ukázka konfiguračního souboru.....	30
Tab. 8 – Nastavení účtu v100.....	37
Tab. 9 – Zápis odchozího volání	37
Tab. 10 – Nastavení účtu VoiceBlue	39
Tab. 11 – Konfigurace sip.conf.....	44
Tab. 12 - Konfigurace iax.conf.....	45
Tab. 13 – Odchozí volání.....	46
Tab. 14 – Příchozí volání	47
Tab. 15 – Normalizace čísel.....	48
Tab. 16 – Ověření VPN	48
Tab. 17 – Menu	49
Tab. 18 – Ověření uživatele	49
Tab. 19 – odchozí volání přes ENUM.....	52
Tab. 20 – příchozí volání z ENUM	52

PŘÍLOHA : SOUBOR *EXTENSIONS.CONF*

```
[general]
static = yes
writeprotect = yes ;zamezeni prepisovani diaplan z CLI

[globals] ;=====

[services] ;=====

exten => 348,1,Answer() ;Prijmuti hovoru Asteriskem
exten => 348,n,Playback(demo-echotest) ;Prehrava se hlaska "demo..."
exten => 348,n,Echo()
exten => 348,n,Hangup() ;Zaveseni hovoru

exten => 349,1,LookupCIDName
exten => 349,2,goto(menu,s,1)

exten => 343,1,LookupCIDName
exten => 343,2,goto(virtual_net,s,1)

include => test_exten

[users] ;=====

include => services ;Vlozeni jineho contextu

exten => 331,1,Dial(SIP/stul,20) ;Volba stanice 331, po 20s skok na
dalsi priritu
exten => 331,n,Dial(SIP/v100/777573684) ;Volba mobilni stanice GSM pres gate
v100
exten => 332,1,Dial(SIP/client)
exten => 333,1,Dial(SIP/host1)
exten => 334,1,Dial(SIP/host2)
exten => 335,1,Dial(SIP/mobile)
exten => 336,1,Dial(SIP/mobile2)
exten => 337,1,Dial(IAX2/iaxclient) ;Volba stanice 337, tentokrat IAX
exten => _4XX,1,Dial(IAX2/iaxtrunk2:emos@82.114.208.81/${EXTEN:0})
;Volba stanic druhe ustredny
exten => _4XX,n,NoOp(IAX2/iaxtrunk2:emos@82.114.208.81/${EXTEN:0})
exten => _4XX,n,Hangup()

exten => _7XXXXXXXX,1,GotoIf(${${EXTEN:0}=724269926}?4:2)
exten => _7XXXXXXXX,2,Dial(SIP/v100/${EXTEN:0},,r)
exten => _7XXXXXXXX,3,NoOp(${CALLERID(num)})
exten => _7XXXXXXXX,4,Goto(second_pbx,724269926,1)
exten => _6XXXXXXXX,1,Dial(SIP/v100/${EXTEN:0},,r)
exten => _2XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
exten => _3XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
exten => _4XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
exten => _5XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
exten => _5XXXXXXXX,n,NoOp(${CALLERID(num)})
exten => _8XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)
exten => _0XXXXXXXX,1,Dial(SIP/my_802_provider/${EXTEN:0},,r)

include => enum_00

[virtual_net] ;=====

exten => s,1,NoOp(${CALLERID(num)})
exten => s,2,GotoIf(${${CALLERID(num)}=777573685}?10:3)
exten => s,3,GotoIf(${${CALLERID(num)}=777573684}?10:4)
exten => s,4,GotoIf(${${CALLERID(num)}=581111784}?10:5)
exten => s,5,Goto(verify,s,1)

exten => s,10,Goto(menu,s,1)

[incoming] ;=====

exten => 581111799,1,NoOp(${CALLERID(num)})
```

```

exten => 581111799,2,Dial(SIP/stul,15)
exten => 581111799,3,LookupCIDName
exten => 581111799,4,Goto(virtual_net,s,1)
exten => 343,1,goto(normalizing,s,1)

[normalizing] ;=====

exten => s,1,NoOp(${CALLERID(num)})
exten => s,n,SetCallerID(${CALLERID(num):3})
exten => s,n,NoOp(${CALLERID(num)})
exten => s,n,goto(virtual_net,s,1)

[menu] ;=====

exten => s,1,Ringing()
exten => s,n,Wait(2)
exten => s,n,Answer()
exten => s,n,Set(TIMEOUT(digit)=3)
;exten => s,n,Set(TIMEOUT(response)=20)
exten => s,n,BackGround(menu)
include => users
exten => s,n,WaitExten(10)
exten => s,n,Dial(SIP/stul)

[verify] ;=====

exten => s,1,Ringing()
exten => s,n,Wait(2)
exten => s,n,Answer()
exten => s,n,Authenticate(2699,j)
exten => s,n,Goto(menu,s,1)
exten => s,105,Dial(SIP/stul,20)
exten => s,106,Dial(SIP/v100/777573684,,r)

[second_pbx] ;=====

exten => 724269926,1,Dial(IAX2/iaxtrunk2:emos@82.114.208.81/${EXTEN:0})
exten => 724269926,n,NoOp(IAX2/iaxtrunk2:emos@82.114.208.81/${EXTEN:0})

[enum_00] ;=====

exten => _00420.,1,Set(ENUM=${ENUMLOOKUP(+${EXTEN:2}|sip||e164.arpa)})
exten => _00420.,2,NoOp(+${EXTEN:2})
exten => _00420.,3,Dial(SIP/${ENUM})
exten => _00420.,4,Dial(SIP/my_802_provider/${EXTEN:2},,r)

[test_exten] ;=====

exten => bobanl,1,Dial(SIP/${EXTEN:0}@sip.icamp.eu,,r)
exten => 339,1,Dial(SIP/bobanl@sip.icamp.eu,,r)

```