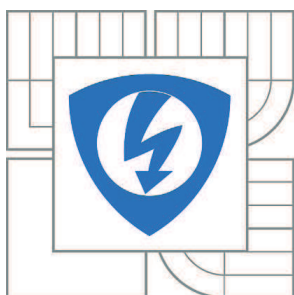


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MOŽNOSTI VIDEOKONFERENCÍ V PBX ASTERISK

VIDEOCONFERENCE POTENTIALS IN PBX ASTERISK

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

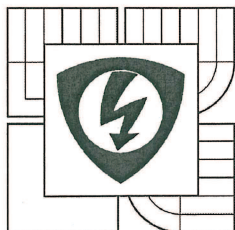
Bc. BRONISLAV VLK

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. ONDŘEJ KRAJSA

BRNO 2010



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Bronislav Vlk

Ročník: 2

ID: 74617

Akademický rok: 2009/10

NÁZEV TÉMATU:

Možnosti videokonferencí v PBX Asterisk

POKYNY PRO VYPRACOVÁNÍ:

Analyzujte možnosti videokonferencí v softwarové PBX Asterisk. Popište používané kodeky a jejich možné využití v PBX Asterisk. Vytvořte videokonferenční server s využitím PBX Asterisk a možností připojení klientů třetích stran.

DOPORUČENÁ LITERATURA:

- [1] Meggelen, J.V, Smith, J., Madsen, L. Asterisk™ The Future of Telephony. Sebastopol: O'Reilly Media, Inc., 2005. ISBN 0-596-00962-3.
- [2] Firestone, S., Ramalingam, T., Fry, S. Voice and Video Conferencing Fundamentals. Cisco Press; 1 edition, 2007. ISBN 1587052687.

Termín zadání: 29.1.2010

Termín odevzdání: 26.5.2010

Vedoucí práce: Ing. Ondřej Krajsa, Ph.D.

Konzultanti diplomové práce:


prof. Ing. Kamil Vrba, CSc.
předseda oborové rady



UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Anotace

Diplomová práce se zabývá možnostmi videokonferencí v PBX Asterisk a jejich použitím v praxi. Jsou zde popsány její eventuality a způsoby její konfigurace. Zvláštní pozornost je věnována protokolům SIP, IAX a H.323, které jsou popsány v jedné z kapitol. V rámci diplomové práce byla vytvořena PBX Asterisk, která demonstruje spolupráci s videokonferenčními klienty. V diplomové práci jsou popsány konfigurační soubory, pomocí kterých se ústředna nastavuje. Závěr práce hodnotí použití kodeků pro různé klienty.

Klíčová slova:

Asterisk, PBX, videokonference, protokoly, kodeky, H.323

Abstrakt

This thesis deals with the possibilities of video conferencing in Asterisk PBX and their use in practice. They also described the contingencies and how its configuration. Particular attention is paid to the protocols SIP, IAX and H.323, which are described in one of the chapters. The thesis was created by the Asterisk PBX, which demonstrates cooperation with videoconferencing clients. The thesis describes the configuration files so that the central set. Conclusion the work assesses the use of codecs for different clients.

Keywords:

Asterisk, PBX, video conference, protocols, codecs, H.323

VLK, B. *Možnosti videokonferencí v PBX Asterisk: diplomová práce*. Brno: FEKT VUT v Brně, 2010. 47 stran, 7 stran příloh. Vedoucí práce Ing. Ondřej Krajsa.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma Možnosti videokonferencí v PBX Asterisk jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 20.5.2010

.....

podpis autora

Poděkování

Děkuji vedoucímu práce Ing. Ondřeji Krajsovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

Obsah

1. Úvod.....	3
1.1 Videokonference – protokoly, kodeky	3
1.1.1 Protokoly	3
1.1.2 Audio kodeky	7
1.1.3 Video kodeky	10
1.1.4 MOS (Mean opinion score).....	11
1.2 Používané videokonferenční systémy	12
1.3 Zabezpečení multimediálních dat v reálném čase.....	16
1.3.1 Protokol SRTP	16
1.3.2 Protokol ZRTP	18
1.3.3 Protokolová sada IPsec	19
1.3.4 Protokol SIP – zabezpečení signalizace.....	20
1.3.5 Protokol H.323 a jeho zabezpečení.....	21
1.4 Asterisk – pobočková telefonní ústředna.....	23
1.4.1 Asterisk – možnosti konferenčních a videokonferenčních hovorů.....	25
1.4.2. Asterisk – video kodeky	26
1.4.3. Asterisk - zabezpečení hovorů.....	27
1.5 GNU Gatekeeper OpenH323	28
1.6 OpenMCU	29
1.7 Videokonference v praxi	30
1.8 Klienti s podporou videohovorů kompatibilní s PBX Asterisk	33
2. Instalace a technická část.....	35
2.1 Instalace a konfigurace Asterisku verze 1.6.2.9	35
2.2 Instalace a konfigurace klientů na podporu videohovorů	35
2.4 Testovací prostředí.....	35
2.5 Možnosti skriptování a vzdálené konfigurace	38
2.6 Videokonference pomocí protokolu ooh323, OpenMCU a gatekeeperu	40
2.7 Videokonference pomocí protokolu SIP a MCU Radvision	41
3. Závěr	44
Literatura.....	45
Seznam příloh	48
Příloha A - Klienti s podporou videohovorů	49

Příloha B - Postup instalace Ubuntu a aplikací.....	50
Příloha C - Diagram spojení SIP videokonference	52
Příloha D - Diagram spojení H.323 videokonference.....	53
Příloha E – Přílohy na CD	54

1. Úvod

Tato práce pojednává o možnostech využití videokonferenčních hovorů v počítačových systémech s operačním systémem Linux a Windows. V mém případě se jedná o rozšíření PBX Asterisk o možnost videokonferencí, porovnání možností mezi verzemi 1.6 a 1.8, zabezpečení multimediálních dat pomocí zabezpečovacích protokolů (SRTP, ZRTP, IPsec), vytvoření videokonferencí mezi více přípojnými body (počítači), nastavení jednotlivých klientů na stanicích s operačním systémem Windows a Unix a otestování videokonferenčních hovorů pro protokol SIP a OOH323.

V současné době je velký zájem o videokonference. Jako důvod uvádějí firmy a společnosti snížení nákladů, méně služebních cest, výdaje za diety, nocleh apod. Program Asterisk je z těchto důvodů vhodný videokonferenční nástroj, kde náklady na jeho provoz jsou minimální.

Program Asterisk využívá standardní protokoly a kodeky a vývojáři Asterisku vyvinuli i svůj vlastní protokol IAX.

V diplomové práci rozebírám používané protokoly, kodeky a jejich vývoj.

1.1 Videokonference – protokoly, kodeky

Voice over Internet Protocol (zkratkou VoIP) [1] je technologie pro přenos hlasové komunikace prostřednictvím počítačové sítě a protokolu IP. Protokol IP (Internet Protocol) pracuje na síťové vrstvě a poskytuje datagramovou službu.

1.1.1 Protokoly

Používají se tyto protokoly:

- IAX2
- SIP
- H.323
- MGCP
- Skinny/SCCP
- UNISTIM

IAX2

IAX2 (Inter-Asterisk eXchange protokol) je otevřený protokol pro přenos hlasu v PBX Asterisk. Tento protokol patří k jednodušším a používá jeden UDP port (4569) pro signalizaci a hlasový přenos. Dochází k snazšímu překladu adres NAT a snadnějšímu průchodu přes firewall.. Je jak zdrojový, tak i cílový. Signalizace je společně s datagramy UDP odesílána přes jeden port pomocí jednoho protokolu. Podporuje vestavěné šifrování AES (Advanced Encryption Standard) pro 128-bitové blokové šifry.

IAX umožňuje ověření třemi způsoby:

- nešifrovaným heslem
- MD5 hashování
- RSA výměna klíčů

SIP

SIP (The Session Initiation Protocol) [2] je podobný protokolům HTTP či SMTP. SIP je protokol aplikační vrstvy a používá ke komunikaci port 5060 a transportní vrstvu protokolu TCP či UDP. Nejčastěji se protokol SIP využívá pro telefonní hovory přes internet nebo k vytvoření a ukončení multimediálního přenosu. SIP se nepoužívá při přenosu média mezi samostatnými koncovými body. K této komunikaci se využívá protokol RTP (Real Time Protocol).

V Asterisku je protokol SIP začleněn do modulu s názvem chan_sip.so.

Protokol SIP používá k autentifikaci systém výzva/odpověď (Invite/Answer). Nejčastějším typem útoku je DoS (Denial of Service) útok. Vzniká posláním velkého množství INVITE paketů s cílem přetížit server.

Šifrování médií tzv. RTP stream je mimo rozsah SIP protokolu a musí být řešen samostatně.

Problém může vzniknout u protokolu SIP tehdy, když je vedena komunikace prostřednictvím NAT. Řešením je použít STUN server či proxy server (RTP proxy).

H.323

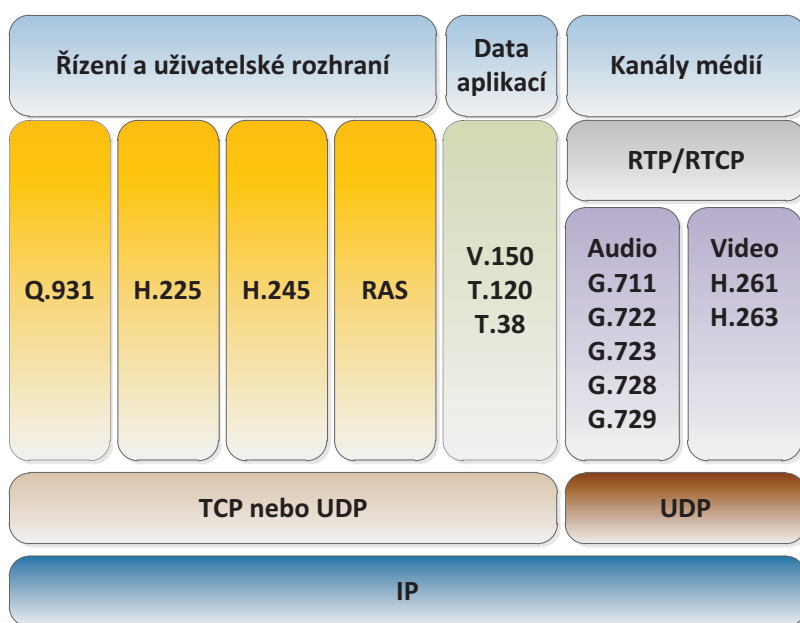
Protokol H.323 [3] je určen pro přenos audia a videa v reálném čase pomocí IP paketové sítě. Tento protokol podporuje sestavení hovoru, ukončení hovoru a také samotný hovor. Hlavním přínosem je tzv. QoS (Quality of Service), což je technologie

umožňující zvládnout v reálném čase složitost definování a dodržení síťové politiky. QoS zlepšuje kvalitu hlasových a multimediálních přenosů.

Protokol H.32x umožňuje komunikaci pro různé sítě:

- H.320 N-ISDN, úzkopásmová ISDN
- H.321 B-ISDN, širokopásmová ISDN (ATM)
- H.322 LAN s garancí QoS
- H.323 paketově založené multimediální systémy
- H.324 PSTN, veřejné analogové telefonní sítě s přepojováním okruhů
- H.324M rozšíření H.324 pro mobilní sítě 3GPP
- H.325 nově vyvíjený standard

Protokolový model [4] je zobrazen na obr. 1.1, kde všechny terminály H.323 musí podporovat audio a podpora videa a dat je volitelná. Pro řízení a uživatelské rozhraní je určen protokol RAS, H.225 či Q.931 (tzv. signalizace volání) a H.245 (protokol řízení médií).



Obr. 1.1: Protokolový model H.323

Signalizace protokolu H.323:

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

Následující protokoly zajišťují v rámci H.323:

- H.235 – zabezpečení a identifikace
- H.450 – doplňkové služby

Samotný protokol H.323 můžeme logicky rozdělit na dvě části:

- Koncový bod, koncové zařízení (Endpoint), což je MCU (Multipoint Control Unit) - multikonferenční jednotka a GW (Gateway) – brána, či terminál TE
- Řídící prvek sítě (Gatekeeper)

MCU (Multipoint Control Unit) je řídicí jednotka, která umožňuje podporu konference mezi třemi či více koncovými body. Jedná se o nejdražší část sítě. Výhodou MCU je, že umí transkódování (propojení terminálů s různými kodeky). MCU obsahuje řídicí jednotku MC (controller) a procesorovou jednotku, neboli audio mixér MP (media processor).

GW (Gateway) je nepovinným prvkem a poskytuje překlad mezi přenosovou částí (H.225) a komunikační částí (H.245). Dále umožňuje sestavit a ukončit hovor mezi dvěma terminály.

TE (Terminal) je koncové zařízení (SW pro Windows / Linux tzv. softphone, nebo HW terminál - IP telefon).

Gatekeeper (GK) je řídicím prvkem koncových bodů protokolu H.323 a zajišťuje podporu signalizace RAS, řízení přístupu, překlad adres mezi E.164 číslem a IP síťovou adresou, řízení přidělování kapacity pásma (Bandwidth Control), řízení spojení a řízení zón.

Gatekeeper podporuje autorizaci volání (Call authorization), optimalizaci směrování cestou nejnižších nákladů (Least Cost routing) nebo nastavení záložního GK (Standby GK).

Organizace ITU již začala pracovat na nástupci H.323, novém VoIP protokolu H.325 (AMS - Advanced Multimedia System). Protokol je zatím ve stádiu vývoje [21].

MGCP

MGCP (The Media Gateway Control) [4] protokol také pochází z IETF (Internet Engineering Task Force). Dříve byl tento protokol používán častěji, ale je vytlačován protokolem SIP a IAX2. Jeho cílem je, aby koncová zařízení (telefony) byla co nejjednodušší a aby provoz procházel přes hovorové brány a agenty. Na rozdíl od SIP, MGCP používá centralizovaný model. MGCP telefony nemohou přímo volat jiným MGCP telefonům.

Skinny/SCCP

Protokol Skinny (The Skinny Client Control Protocol) [5] je Cisco protokol pro Cisco VoIP zařízení. Tento protokol se používá pro VoIP telefonní přístroje či pracovní stanice, kde se použije tenký klient tzv. Skinny Client. Tento Skinny Client napomáhá minimalizovat náklady a složitost na VoIP koncové stanice. Hlasová komunikace mezi koncovými stanicemi využívá User Datagram Protocol (UDP) a IP (Internet Protocol).

UNISTIM

UNISTIM (Unified Networks IP Stimulus) [6] je protokol firmy Nortel (nyní ve vlastnictví firmy Avaya) pro IP telefony a IP PBX systémy.

1.1.2 Audio kodeky

Asterisk podporuje [1] následující širokopásmové (HD audio) kodeky: G.711 u-law (je používán v USA); G.711 a-law (je používán v Evropě); G.722 - 16 kHz širokopásmový kodek, přehrávání a nahrávání v Asterisk 1.4, plná podpora vč. překódování v Asterisk 1.6; G.723.1; G.726 - 32kbps pouze (16/24/32/40 kbps podporovány format_g726); G.729 - může vyžadovat licenci. Bezplatné verze jsou dostupné v zemích bez patentů nebo pro vzdělávací účely; GSM; iLBC; LPC10 (nedoporučuje se) a Speex - konfigurovatelné 4-48kbps, VBR, ABR, atd. viz chyba 2536. Pro Asterisk 1.4 je k dispozici patch 10519, který přidává podporu pro klientský software OpenWengo

G.711 u-law a G.711 a-law

G.711 je určen pro přenosové rychlosti (64 kb/s). Byl schválen jako ITU standard. V moderních digitálních telefonních sítích je považován jako nepostradatelný kodek.

Přestože byl formálně standardizován v roce 1988, je kodek G.711 PCM zaveden již na počátku 70. let 20. století firmou Bell Systems.

Existují dvě verze: a-law a u-law. U-law je původně standardem používaným v Severní Americe a Japonsku. A-law je norma používaná ve zbytku světa. Rozdíl je v kompresní charakteristice kompondoru.

Aplikací G.711 pro VoIP dostaneme velmi dobrou kvalitu hlasu. Využívá se logaritmická komprese. Pro přenos hlasu je využito 8 bitů a datový tok je 64 kbit/s. G.711 je podporován většinou poskytovatelů VoIP.

G.722

G.722 je používán pro vysoké přenosové rychlosti (48/56/64 kbit/s). Byl schválen jako ITU standard.

G.723.1

G.723.1 má rozumně nízkou přenosovou rychlost (6.3 kbit/s nebo 5.3 kbit/s) a je uplatňován v H.323 standardu. Pro používání tohoto kodeku je nutná licence od firmy Sipro Lab Telecom. Byl schválen jako ITU standard.

G.726

G.726 byl schválen jako ITU standard. Tento kodek aplikuje režim Adaptivní Diferenciální Pulse Code Modulation (ADPCM). Stejně jako G.711, G.726 má své kořeny v síti PSTN. V případě G.711 se používá 64 kbit/s, G.726 používá 32 kbit/s. Je to standardní kodek aplikovaný u bezdrátových telefonů DECT. Datový tok může být 16, 24, 32 nebo 40 kbit/s, ale 32 kbit/s je de facto standardem. Asterisk v současné době podporuje pouze běžný datový tok 32 kbit/s.

G.729

G.729 je ITU standard kodek. Má dvě hlavní varianty: variantu A a B. Nabízí nízký datový tok 8 kbit/s. Je to však poněkud "náročný" kodek z hlediska času zpracování procesoru, a proto některé VoIP telefony a adaptéry mohou zvládnout jeden G.729 hovor (kanál) najednou. Použití tohoto kodeku vyžaduje licenci od firmy Howler Technologies nebo Digium či VoiceAge.

GSM

Původně 'Full Rate' GSM kodek pro mluvené slovo je pojmenován RPE-LTP (Regular Pulse Excitation Long-Term Prediction). Tento kodek používá informaci z předchozích vzorků (tato informace se nemění). Řečový signál je rozdělen do bloků po 20 ms. Tyto bloky jsou pak převáděny na řečové, které mají rychlost 13 kbit/s a velikost bloků je 260 bitů.

iLBC

iLBC (Internet Low Bitrate Codec) je kodek zcela bezplatný a slouží pro mluvené slovo, což je vhodné pro robustní hlasové komunikace přes IP. Kodek je určen pro úzké řečové pásmo a výsledná bitová rychlost je 13,33 kbit/s, kódování rámce má délku 30 ms a 15,20 kbit/s s kódováním o délce 20 ms. U iLBC kodeku může dojít ke zhoršení kvality řeči v případě ztráty snímků, které se vyskytují v souvislosti se ztracenými nebo zpožděnými IP pakety.

LPC10

LPC10 (Linear predictive coding) se používá pro úzkopásmové připojení. Hlasový signál je jasný, ale má robotické zvuky, proto není moc vhodný a nedoporučuje se.

Speex

Speex je dobře přizpůsobitelný k internetovým aplikacím a poskytuje užitečné funkce, které nejsou přítomny ve většině ostatních kodeků. Kodek Speex je součástí projektu GNU a je k dispozici v rámci varianty Xiph.org BSD licence.

Speex je díky své flexibilitě výkonný kodek. Je však také dražší, protože se spotřebuje více CPU u kodeku G.729, G.726 i GSM a je téměř stejný jako iLBC. Vzhledem k tomu, že iLBC přichází s atypickými 30 ms pakety (není dobré pro IAX2) a PLC (má ztrátu paketů). Na rozdíl od jiných kodeků lze Speex přizpůsobit našim potřebám pomocí konfiguračního souboru `codecs.conf` v Asterisku.

1.1.3 Video kodeky

H.261

H.261 je ITU standard kodek z roku 1990 používaný ke kódování videa a je původně určen pro přenos přes ISDN linky, které mají přenosovou rychlost v násobcích 64 kbit/s. Kódovací algoritmus pro rychlost přenosu dat byl navržen tak, aby byl schopen pracovat mezi 40 kbit/s až 2 Mbit/s. Standardně podporuje video formát CIF a QCIF s rozlišením snímků 352x288 či 176x144.

H.261 byl prakticky první digitální video kodek. H.261 standard určuje dekódování videa.

H.263

H.263 je video kodek [1] navržený ITU-T pro videokonference. Jako první byl uplatněn v systémech H.324 (PSTN, videokonference a videotelefonie). Našel však použití i v systémech H.323 (RTP/IP videokonference) či v systémech H.320 (ISDN videokonference), RTSP (streaming media) a SIP (internetové konference).

H.263 byl vyvinut jako lepší verze kodeku H.261. Jeho první verze byla dokončena v roce 1995 a stala se náhradou za kodek H.261 ve všech přenosových rychlostech.

H.263p (ve verzi Asterisk 1.4)

H.263 + / h263p je vylepšená verze kodeku H.263 jenž podporuje Eyebeam Xten s lepší kvalitou videa.

H.264 (ve verzi Asterisk 1.4)

H.264/MPEG-4 AVC je ITU-T standard pro kompresi videa. První verze normy byla dokončena v květnu 2003.

H.264/AVC kodek vyvinutý podle standardu ITU-T Video Coding Experts Group (VCEG) spolu s ISO/IEC Moving Picture Experts Group (MPEG). ITU-T H.264 standard a ISO/IEC MPEG-4 AVC standard (formálně, ISO/IEC 14496-10 - MPEG-4 Part 10, Advanced Video Coding) jsou společně udržovány tak, že mají stejný obsah po technické stránce. H.264 je velmi populární pro své využití v technologiích Blu-ray, HD DVD a videí z iTunes Store.

Na začátku roku 1998 firma Video Coding Experts Group (VCEG - ITU-T SG16 Q.6) vydala výzvu k předkládání návrhů v rámci projektu H.26L s cílem zdvojnásobit efektivitu kódování (což znamená snížit přenosovou rychlost nezbytnou pro danou úroveň přesnosti).

H.264 video kodeku má velmi široké spektrum aplikací, které zahrnují všechny formy digitálního komprimovaného videa od nízkých bitových rychlostí až po streaming aplikace HDTV vysílání s téměř bezztrátovým kódováním. V satelitní digitální televizní kvalitě jsou dosahovány rychlosti max. 1,5 Mbit/s. U kodeku MPEG 2 jsou to rychlosti přibližně 3,5 Mbit/s.

Projekt Digital Video Broadcast (DVB) schválil používání H.264/AVC pro televizní vysílání na konci roku 2004. Ve Spojených státech normalizační orgán Advanced Television Systems Committee (ATSC) zvažuje možnost určit jeden nebo dva moderní video kodeky pro Enhanced-VSB (E-VSB) k využití v televizním vysílání v USA.

Vzhledem k tomu, že kodek H.264 vyžaduje značný výpočetní výkon, běží software pro kódování na procesorech CPU, které jsou obvykle pomalé, zejména týkající se HD rozlišení. Pro odlehčení CPU v reálném čase jsou zaměstnány hardwarové enkodéry.

Hardware H.264 enkodér lze použít ASIC a FPGA. FPGA je obecný programovatelný čip. Chceme-li použít FPGA jako hardwarový kodér, je nutný IP enkodér kodeku H.264. S postupujícím vývojem technologií může formát full HD (1080p, 30 snímků za sekundu) fungovat od roku 2009 na jednom nízkonákladovém FPGA čipu.

1.1.4 MOS (Mean opinion score)

MOS (Mean opinion score) [7] je subjektivní metoda, která stanovuje kvalitu přenosu hlasu kodeky. Mean opinion score je číslo, které stanoví kvalitu přenosu a vyjadřuje se, jako číslo v rozmezí 1 až 5, kde 1 je nejnižší vnímaná kvalita zvuku, a 5 je naopak nejvyšší možná naměřená kvalita zvuku. MOS testy pro hlasové kodeky jsou stanoveny podle doporučení ITU-T P.800.

<i>MOS</i>	<i>Kvalita</i>	<i>Zhoršení</i>
5	výborná	nepostřehnutelné
4	dobrá	patrné, ale ne nepříjemné
3	slušná	mírně nepříjemné
2	špatná	nepříjemné
1	slabá	velmi nepříjemné

Tab. 1.1: Tabulka hodnocení kvality MOS

MOS je aritmetický průměr ze všech jednotlivých výsledků, a může být v rozsahu od 1 (nejhorší) do 5 (nejlepší).

Kodek	Data rate [kbit/s]	Mean opinion score (MOS)
G.711 (ISDN)	64,0	4,30
iLBC	15,2	4,14
AMR	12,2	4,14
G.729	8,0	3,92
G.723 1r63	6,3	3,90
GSM EFR	12,2	3,80
G.726 ADPCM	32,0	3,80
G.729a	8,0	3,70
G.723 1r53	5,3	3,65
GSM FR	12,2	3,50

Tab. 1.2: Průměrné hodnoty výsledků pro různé kodeky

1.2 Používané videokonferenční systémy

S rozšiřujícím se využíváním internetu a datového spojení [8] se stále více uplatňuje videokonference v praxi. Náklady na provoz a údržbu videokonferenčních systémů jsou nižší a firmy či společnosti volí nejčastěji tuto variantu, než drahé výjezdy na konference, jednání či schůzky. Videokonference neboli tzv. multimediální přenos je de facto rozšířený telefonní hovor, kdy se kromě hlasu přenáší i obraz nebo i další informace.

Oproti telefonickému hovoru nabízí videokonference široké spektrum uplatnění. Díky možnosti přenášet video máme dojem, jako kdybychom mluvili s protějškem v jedné místnosti tváří v tvář (face to face), proto můžeme hovořit o tzv. virtuálních schůzkách, video setkáních, při kterých se může do debaty zapojit více účastníků.

Videokonferenční systémy můžeme rozdělit do několika kategorií:

Třídění podle účelu a zaměření

- Videokonferenční systémy pro jednotlivce a pracovní skupiny jsou určeny pro běžné využití v komunikaci s kolegy či obchodními partnery. Tyto se dále mohou rozdělit podle počtu účastníků videokonference na konference pro dva účastníky po síti IP, na konference pro více účastníků a na tzv. multicast konference. Využívají se multimediální počítače, vybavené aplikacemi MBone, Microsoft Netmeeting, Gnomemeeting a dalšími programy.
- Systémy, na něž je kladen značný důraz na kvalitní obraz. Uplatňují se pro přenosy mezi dvěma místy, např. velkých místností či videokonferenčních sálů. Jedná se o drahá zařízení a je využívána velká šířka přenosového pásma, např. zařízení AVA/ATV s technologií ATM.
- Broadcast, Media streaming. Video Demand a pro podporu on-line vzdělávání jsou určeny systémy s digitalizovanými záznamy uloženými na serveru, kde jsou k dispozici jak videa tak zvukové záznamy, či poznámkové texty. Pro tyto účely se využívají jako koncová zařízení multimediální počítače a aplikace např. Windows Media Player, Real Player či jiné multimediální přehrávače.

Třídění podle požadavku na šířku přenosového pásma

- Do 30 kb/s lze přenášet pouze zvuk. PC se zvukovou kartou a s aplikacemi Microsoft Netmeeting, MBone, Gnomemeeting a dalších programů.
- Do 300 kb/s lze přenášet obraz i zvuk s nižší kvalitou. Zařízení ISDN s aplikacemi Microsoft Netmeeting, MBone, Gnomemeeting a dalších programů.
- Do 3 Mb/s lze přenášet obraz i zvuk s vyšší kvalitou. Multimediální počítače s aplikacemi Microsoft Netmeeting, MBone, Gnomemeeting a dalších programů.
- Do 20 Mb/s lze přenášet obraz i zvuk ve velmi vysoké kvalitě. Např. koncová zařízení AVA/ATV, která využívají technologii ATM.

- Nad 20 Mb/s lze přenášet obraz i zvuk v té nejvyšší kvalitě. Např. multi point konference na sítích LAN.

Třídění podle technologie pro přenos

- Modem-telefonní linka má jen úzké přenosové pásmo, které je vhodné jen pro přenos zvuku. Koncovým zařízením bývá počítač se zvukovou kartou a aplikací např. Microsoft Netmeeting, MBone, Gnomemeeting a dalších.
- ISDN má šířku pásma 64 - 256 kb/s. Přenáší se audio, video i data.
- ATM je technologie s šířkou pásma 34 – 655 Mb/s a využívá se pro přenos videokonferenčních hovorů o vysoké kvalitě. Koncovým zařízením může být AVA/ATV s přenosovou technologií ATM.
- IP technologie má přenosové pásmo od 10 Mb/s do 10 Gb/s a lze využít videokonferenčních zařízení podobných ATM.

Třídění podle platformy (operačního systému)

- Linux je prostředí, v němž lze provozovat celou řadu videokonferenčních systémů. Využívají se multimediální počítače s aplikacemi Real Video, MBone, Gnomemeeting a další.
- Windows je prostředí, ve kterém lze provozovat celou řadu videokonferenčních systémů. Využívají se multimediální počítače s aplikacemi Microsoft Netmeeting, Real Video, MBone, Gnomemeeting a další.
- Sun - Solaris, SGI - Irix, FreeBSD pro tato prostředí se využívají multimediální počítače s aplikacemi MBone, VRVS a další.
- Hardwarové kodéry/dekodéry jsou specifická zařízení, jenž většinou pracují se stejnými modely na všech koncových místech a jejich vzájemná kompatibilita s jinými systémy nebývá velká. Jako koncová zařízení se používají AVA/ATV či ISDN zařízení v kombinaci s multimediálním počítačem nebo televizí.

Třídění podle počtu účastníků a směrovosti

- Jednosměrné – data jsou vysílána jedním směrem a přijímána jsou z jednoho nebo více míst najednou (např. přenos přednášek či lékařských operací do jiných míst). Využívají se multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, Gnomemeeting a další.

- Vícesměrné – data jsou vysílána i přijímána ze dvou nebo více míst současně (např. přenos přednášek nebo lékařských operací do jiných míst). Využívají se multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, Gnomemeeting a další.
- 1:1 – data jsou přenášena mezi dvěma účastníky. Využívají se multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, Gnomemeeting a další.
- 1:N – data jsou přenášena od jednoho účastníka k více účastníkům současně (např. přenos přednášek či lékařských operací do jiných míst). Využívají se multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, Gnomemeeting a další.
- N:M – data jsou přenášena mezi více vysílajícími i přijímajícími účastníky videokonferenčního hovoru. Jako koncová zařízení se využívají multimediální počítače s aplikacemi MBone a reflektoru či multicastu, VRVS a další.

Třídění podle časového zpoždění

- Přenosy v reálném čase bez možnosti zpoždění jsou systémy, jenž pracují se zpožděním menším jak 0,5 s. Používají se pro dva a více účastníků. Coby koncová zařízení se využívají multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, VRVS, Gnomemeeting a další.
- Přenosy v reálném čase s možností zpoždění jsou systémy, jež pracují se zpožděním 0,5 s. až několik sekund. Používají se pro jednosměrné přenosy přednášek nebo lékařských operací do jiných míst. Jako koncová zařízení se uplatňují multimediální počítače, specializované hardwarové kodéry/dekodéry, ISDN s aplikacemi Microsoft Netmeeting, Real Video, MBone, VRVS, Gnomemeeting, streamovací software či servery a další.
- Přenosy ze záznamu na vyžádání jsou tzv. systémy Video on Demand, jenž zpřístupňují na serveru uložená data, video či zvuk. Systémy jsou určeny pro on-line vzdělávací účely apod. Coby koncová zařízení se využívají multimediální počítače s aplikacemi Windows Media, Real Video, MPEG4IP a další.

1.3 Zabezpečení multimediálních dat v reálném čase

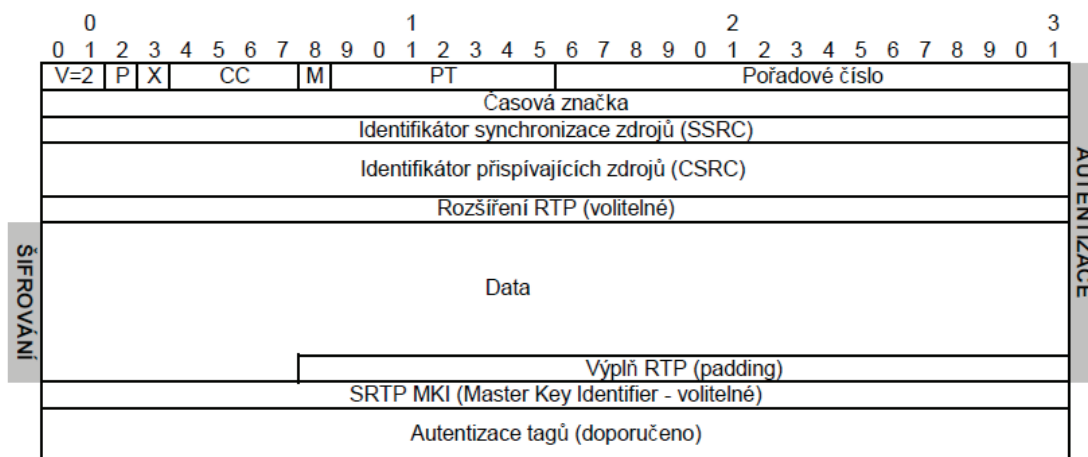
Pro zabezpečení vlastního multimediálního přenosu (přes SIP či H.323) lze použít zabezpečovací protokol SRTP a ZRTP.

Bezpečnostní prvky:

- Důvěrnost, kdy nikdo vyjma odesílatele a příjemce, nebude moci získat obsah přenášených multimediálních dat.
- Autentičnost má zaručit, že právě přenášená multimediální data jsou od odesílatele, se kterým právě komunikujeme.
- Integritu, což znamená, že informace bude doručena příjemci v takovém stavu, v jakém odešla od odesílatele.

1.3.1 Protokol SRTP

Protokoly RTP a RTCP nelze nijak zabezpečit, proto byly vyvinuty nové zabezpečovací protokoly SRTP (Secure RTP) a SRTCP (Secure RTCP), které umožňují zajistit důvěrnost, autentičnost a integritu přenášených dat.

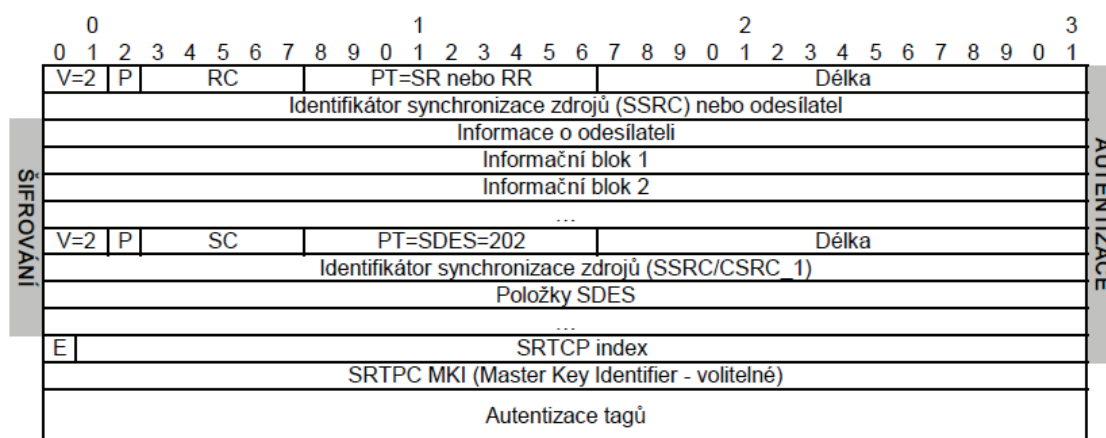


Obr. 1.2: Formát paketu SRTP

Pole SRTP MKI (Master Key Identifier) [9], viz obr. 1.2, je volitelné, nepovinné a slouží k identifikaci a správě hlavního klíče, tzv. master key. Klíč je definován již mezi uživateli (příjemcem i odesílatelem) multimediálního přenosu a je využíván po celou dobu přenosu. Napřed si však obě strany musí vyměnit klíče. Používá se k tomu protokol SDP (Session Description Protocol), což je protokol pro inicializaci relací, který však neumožňuje zabezpečený přenos. K tomu se používá protokol TLS či IPsec.

Autentizační tag (Authentication tag) má volitelnou délku, je doporučen, má autentizační značku, která ověřuje pravdivost zpráv. Skládá se z hlavičky RTP, pak následuje šifrovací část paketu SRTP. Pokud je tedy použito šifrování a autentizace, aplikuje se šifrování před autentizací na straně odesílatele, a na straně příjemce se použije autentizace před dešifrováním.

Pole SRTP MKI není celkově chráněno a neposkytuje zvláštní zabezpečení.



Obr. 1.3: Formát paketu SRTCP

Formát paketu SRTCP [10] na obr. 1.3 má dvě pole povinná (SRTCP index a autentizační tag) a jedno pole volitelné MKI (Master Key Identifier). Pole SRTCP index slouží jako čítač pořadí SRTCP paketů a zabraňuje opětovným útokům.

Pole E (E-flag) slouží k zjištění, zda je aktuální SRTCP paket šifrovaný či nešifrovaný.

Jestli jsou přenášena data důvěrná, ověřuje symetrická kryptografická metoda AES-CTR (AES-counter mode), která je vhodná k zabezpečení multimediálních přenosů. Pro autentičnost přenášených dat se používá algoritmus HMAC-SHA-1, kdy je vytvořen kontrolní součet hlavičky a obsahu SRTP paketu, který se uloží do pole autentizace tagů. Při přenosu se dbá, aby byla co nejmenší šířka přenosového pásma, a tedy výsledný kontrolní součet je 32 bitů.

Pro zabezpečení audio a video komunikace je možno použít např. program KPhoneSI ve verzi 1.1, který je určen pro operační systém Linux a protokol SIP. Pro autentizaci dat využívá algoritmus MD5 a zabezpečovací protokol SRTP.

Dalším programem pro zabezpečení VoIP komunikace je software Minisip [11] ve verzi 0.7.1, který je určen pro SIP User Agent (internetový telefon) a je využíván při telefonování, posílání zpráv či videohovorech v jedné síti SIP. Coby zabezpečovací protokol uplatňuje protokol SRTP a algoritmus MIKEY (DH, PSK, PKE).

1.3.2 Protokol ZRTP

Protokol ZRTP [12] byl vyvinut v roce 2006 Philem Zimmermannem. Má rozšířené mechanismy pro výměnu master key (symetrického klíče) při počátečním vytvoření spojení a samotnou distribuci klíčů. Jako zabezpečovací algoritmus je použita Diffie-Hellmanova metoda s hashovací funkcí. Algoritmus Diffie-Hellman je založen na tom, že si obě strany (vysílající i přijímající) vygenerují vlastní soukromý a veřejný klíč. Veřejný klíč si vzájemně vymění a pomocí matematických operací zjistí symetrický klíč, kterým se budou šifrovat a dešifrovat data. Vlastní komunikace mezi stranami probíhá pomocí protokolu RTP a není závislá na PKI, certifikačním klíči či různých potvrzujících autorit.

Nejčastěji používanou aplikací pro zabezpečení multimediálního přenosu je program ZFone viz obr. 1.4., který neslouží k samotnému přenosu dat, ale pouze k zabezpečení přenášených dat. Tento program musí být nainstalovaný na obou počítačích, na nichž probíhá komunikace např. videokonference.



Obr. 1.4: Program ZFone

Diffie-Hellmanův algoritmus je citlivý na útoky typu Man in the middle (MITM), proto se uplatňuje mechanismus SAS (Short Authentication String), či tzv. kontinuita klíčů.

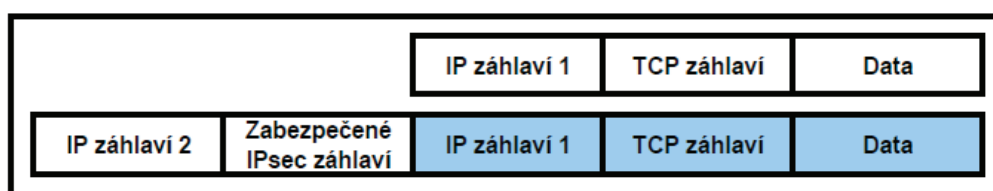
1.3.3 Protokolová sada IPsec

Na úrovni síťové vrstvy OSI modelu lze multimediální data zabezpečit pomocí protokolu IPsec (IP security). Tento protokol vznikl jako součást protokolu IPv6 a později byl začleněn i do protokolu IPv4.

IPsec můžeme rozdělit podle zabezpečení IP datagramů na tunelovací režim a transportní režim.

Tunelovací režim

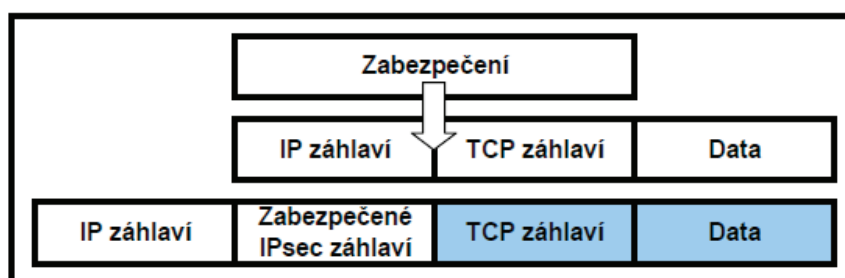
Je režim, kdy IP datagram je celý zajištěn a zapouzdřen. Zdrojový IP datagram se zabezpečí a vsune do nového IP datagramu a za novým IP záhlavím pokračuje zabezpečené záhlaví. V tomto režimu vzniknou dvě IP záhlaví vnitřní (IP1-původní) a vnější (IP2-nové). Na obr. 1.4 je zobrazen tunelovací režim, kde modrou barvou je označena zabezpečená část IP datagramu. U tohoto režimu lze vybudovat virtuální privátní síť (VPN-Virtual Private Network), již lze využít u VoIP.



Obr. 1.5: Tunelovací režim

Transportní režim

Je režim, který je oproti tunelovacímu režimu méně bezpečný, protože šifruje datovou část IP datagramu, který je zvětšen o bezpečnostní záhlaví. Je vložen mezi záhlaví datagramu a záhlaví TCP/UDP vrstvy. Z hlavičky lze určit, jak je IP datagram (datová část) zabezpečen. V transportním režimu se IPsec využívá k zabezpečení přenosu dat v rámci jedné sítě. Na obr. 1.5 je zobrazen transportní režim, kde modrou barvou je označena zabezpečená část IP datagramu.



Obr. 1.6: Transportní režim

Pro zabezpečení IP datagramů se používají dva protokoly. Je to protokol AH (Authentication Header) a protokol ESP (Encapsulated Security Payload). Protokol AH data nešifruje, pouze vkládá do IP paketu autentizační hlavičku, která zahrnuje hodnotu pro výpočet hešovací funkce (např. SHA-1 nebo MD5) z prvotního paketu a tajného klíče. Proto nelze zajistit důvěrnost dat. Protokol AH se téměř nepoužívá. Oproti tomuto protokolu ESP data šifruje a nezašifrovaná zůstávají pouze IP a ESP hlavička.

1.3.4 Protokol SIP – zabezpečení signalizace

Zprávy protokolu SIP [13] jsou lehce analyzovatelné, a proto je musíme pomocí kryptografických metod zabezpečit. Protokol SIP má shodné zásady jako protokol HTTP a SMTP. Tudíž pro něj lze použít podobné zabezpečení jako u HTTP. Musíme však dbát na bezpečnostní prvky, které protokol SIP má. Jedná se o zabezpečení pomocí IP Security (IPsec), Secure MIME (S/MIME), HTTP autentizace, SIP URI (TLS).

IP Security (IPsec)

Protokol IPsec pracuje na nižší vrstvě, a proto má menší nároky na chod SIP aplikací. Pro útočníka je obtížně zjistitelný. IPsec pracuje se všemi transportními protokoly, jenž využívá signalizace SIP (UDP, TCP a SCTP). Než vznikne samotné spojení, vytvoří se zabezpečený kanál, pomocí něhož protokol IPsec hromadně zabezpečí signalizační a multimediální data

Secure MIME (S/MIME)

Secure MIME zahrnuje, stejně jako protokol SMTP, MIME těla (MIME bodies – Multipurpose Internet Mail Extensions). Využívá jednoduché zprávy typu „application/pkcd7-mime“, která provádí podepisování a šifrování multimediálních dat. Pro autentizaci se používá metoda veřejných klíčů a šifrovací algoritmus DES, 3DES a AES.

HTTP autentizace

Mezi základní zabezpečení protokolu SIP patří ověření pomocí HTTP autentizace. Je zajištěna pomocí zásad „výzva – odpověď“ (challenge - response). Je použita hashovací funkce, kdy na začátek zabezpečených dat se vloží heslo a náhodný řetězec. Výsledek probíhá jak na straně příjemce tak na straně vysílajícího. Bývá

využita hashovací funkce SHA-1 nebo MD5. Tato technika ověřuje pouze autentičnost uživatele a neumožňuje šifrování obsahu datové zprávy ani integrity dat.

SIP URI (TLS)

Pro zajištění důvěrnosti dat se používá pro signalizační protokol SIP zabezpečovací protokol TLS (Transport Layer Security). Je umístěn mezi vrstvami aplikační a transportní. Data jsou šifrována pomocí šifrovacího algoritmu AES, DES, 3DES, DEA či RC4. Autentizace je zabezpečena pomocí výměny certifikátů a pro výměnu symetrického klíče je použit algoritmus RSA. Protokol TLS je využíván v celém průběhu přenášených dat sítí a pro transportní protokol je použit protokol TCP.

1.3.5 Protokol H.323 a jeho zabezpečení

Protokol H.323 [14] používá zabezpečení prostřednictvím protokolu H.235, který vymezuje a určuje několik profilů. Každý z těchto profilů využívá odlišný stupeň zabezpečení, jenž je volitelné. Poslední (čtvrtá) verze protokolu H.235 byla schválena v roce 2005 a sestává se z deseti částí (profilů), jež nesou název H.235.0 až H.235.9.

H.235.0 - H.323 zabezpečení: Série H pro multimediální systémy

Tento profil využívá bezpečnostní mechanismus založený na kryptografickém protokolu Diffie-Hellman.

H.235.1 - H.323 zabezpečení: Základní bezpečnostní profil

Mezi nejznámější patří Baseline security profile (základní bezpečnostní profil), který patří mezi nejvíce využívané. Používá zabezpečení protokolem H.235 a symetrické šifrování pomocí hashovací funkce založené na HMAC-SHA-1. Zabezpečuje autentičnost a celistvost právě přenášených dat pomocí společného tajného hesla.

H.235.2 - H.323 zabezpečení: Zabezpečení pomocí digitálního podpisu

Tento profil je založen na hashovací funkci SHA-1 či MD5 a digitálním podpisu či certifikátu. Protože však byly v roce 2004 zjištěny chyby u algoritmu MD5, přestal být aplikován pro jeho menší bezpečnost. Tento profil má zajištěnou tzv.

nepopiratelnost (non-repudiation). Protože se využívá digitální podpis a certifikát, je zatížení celého systému větší. Signature security profile je vhodný pro větší sítě.

H.235.3 - H.323 zabezpečení: Hybridní bezpečnostní profil

Profil vychází ze symetrické a asymetrické kryptografie. Je založen na bázi profilu Baseline security profile a Signature security profile. Na začátku výměny tajného klíče je použita asymetrická kryptografie (digitální podpis RSA a SHA1) a další ověřování probíhá pomocí symetrické kryptografie (Baseline security profile, HMAC-SHA1-96), která je více účinná. Tento profil je vhodný do velkých sítí. Opět je využita Diffie-Hellmanova metoda pro výměnu symetrického klíče.

H.235.4 - H.323 zabezpečení: Přímé a selektivní zabezpečení pomocí routování hovorů

Tento profil je založen na bezprostředním volání mezi dvěma Gatekeepery (terminály). Jeden z terminálů (volající nebo volaný) ustanoví oběma stranám tajný klíč pomocí metody uplatňující protokol Kerberos.

H.235.5 - H.323 zabezpečení: Bezpečná autentizace pomocí RAS a sdílených zpráv

Tento protokol je podobný předešlému protokolu (Direct and selective routed call security), kdy během zabezpečení datové komunikace mezi dvěma terminály se vymění RAS zprávy. Pro tuto komunikaci se používá bezpečná Diffie-Hellmanova metoda pomocí výměny veřejných klíčů.

H.235.6 - H.323 zabezpečení: Přenášení hlasové komunikace pomocí protokolu H.235/H.245 a šifrovacích klíčů

Je profil, který zabezpečuje přenášenou hlasovou komunikaci na základě výměny šifrovacích klíčů protokolu H.225 a generování klíče MSK (Media Stream Key) pomocí protokolu H.245. Výměna klíčů probíhá prostřednictvím Diffie-Hellmanovy metody a šifrování pomocí algoritmu AES (128 bitů), 3DES (168 bitů), DES (56 bitů) a RC2 (56 bitů). Využívá se algoritmus blokového CBC módu (Cipher Block Chaining) či proudového EFB módu (End of Facsimile Block).

H.235.7 - H.323 zabezpečení: Použití protokolu MIKEY a protokolu SRTP (Secure Real Time Transport Protocol)

Tento profil je nejčastěji využit v signalizačním protokolu SIP. Pracuje na principu proudového šifrování. Výměna klíče a autentizace probíhá především na základě domluvených tajných parametrů protokolom MIKEY (Multimedia Internet Keying). Tento profil můžeme rozdělit na dvě zcela jiné metody:

- Distribuce klíčů probíhá na základě dříve dohodnutých metod výměny klíče (MIKEY-PS-pre-shared, MIKEY-DHMAC).
- Security profile using asymmetric security techniques – výměna pomocí zabezpečení PKI

H.235.8 - H.323 zabezpečení: Výměna klíčů SRTP prostřednictvím zabezpečovacích kanálů

Výměna klíčů probíhá pomocí zabezpečovacích kanálů (TLS, IPsec).

H.235.9 - H.323 zabezpečení: Bezpečnostní brána pro H.323

Tento profil využívá Security Gatekeeper. Je včleněn mezi dvě sítě nebo i více IP sítí. V prostředí pracujícím s NAT a firewalý je nutno respektovat signalizační bezpečnost (autentizace a celistvost přenášených dat).

1.4 Asterisk – pobočková telefonní ústředna

Asterisk [1] je světově nejznámější softwarová pobočková ústředna, která se zabývá telefonními službami. Ve vývoji je již od roku 1999 a je bezplatná. Tento open source je plně vybavený hlasově komunikační server, tzv. PBX (Private Branch Exchange) neboli pobočková telefonní ústředna. Asterisk umožňuje snadno vytvářet a nasazovat širokou škálu telefonních aplikací a služeb.

Úvodní program pro Asterisk původně napsal Mark Spencer z firmy Digium. Na vývoji se dále podílelo mnoho softwarových inženýrů z celého světa. V současné době Asterisk používá více jak dva miliony uživatelů. Asterisk podporuje širokou škálu telefonních protokolů a kodeků. Má dobrou podporu pro zpracování a přenos hlasu přes tradiční telefonní rozhraní, včetně analogových linek, ISDN-BRI linek a digitálních T1/E1 svazků, včetně karet pro mobilní technologie (GSM a CDMA).

Asterisk se vyznačuje dobrou podporou pro široké spektrum protokolů VoIP, jako je např. SIP, IAX2, H.323 a další. Podporuje americké i evropské normy signalizace používané ve firemních telefonních systémech.

Asterisk je uvolněn jako open source pod licencí GNU General Public License (GPL) a je k dispozici při bezplatném stažení.

Asterisk zahrnuje všechny kompoziční bloky potřebné pro vytvoření systému PBX, IVR systémů (Interactive Voice Response) a ACD (Automatic Call Distribution) nebo jakýkoli jiný druh komunikačních řešení. IVR je zkratka pro automatický (interaktivní) hlasový odpovídač, jenž je ovládán převážně tónovou volbou (DTMF) nebo hlasem. IVR umožňuje volajícímu procházet informačním stromem a realizovat nabízené služby. Nejčastěji se používají v call centrech bankovních ústavů, telekomunikačních společnostech, objednávkových domech apod. ACD umožňuje automatické rozdělení hovorů dle nastavených pravidel, např. podle čísla volajícího či časových podmínek.

Asterisk obsahuje a umožňuje: kanály pro různé protokoly VoIP; hlasový kanál PSTN (standardní telefonní síť, kterou veřejnost využívá k realizaci místních, meziměstských i mezinárodních telefonních hovorů) - rozhraní karet a zařízení; směrování hovorů pro příchozí hovory; odchozí hovory a jejich směrování; řídicí funkce (záznam, přehrávání, generování tónu atd.); detail záznamu o hovoru pro účetnictví a fakturaci; webové služby v oblasti integrace pro přístup k datům pomocí standardních internetových protokolů; nahrávání hovorů a jejich sledování; integrovaný "dialplan" - skriptovací jazyk pro zpracování hovorů; vnější řízení hovorů v libovolném programovacím nebo skriptovacím jazyku prostřednictvím Asterisk Gateway Interface (AGI); upozorňování na události a CTI integraci prostřednictvím Asterisk Manager Interface (AMI); syntéza řeči ("text-to-speech") v různých jazycích a různých dialektech; rozpoznávání řeči rozdílných jazykových mutací prostřednictvím třetí strany;

Tato kombinace komponent umožňuje integrátorem (uživatel) nebo vývojáři rychle vytvářet hlasové aplikace. Otevřený charakter (open-source) programu Asterisk znamená, že není stanoven limit na to, co lze vytvořit. Program Asterisk umožňuje vytvořit systémy od velmi malých PBX až po velké hlasové servery.

Asterisk může být nakonfigurován jako hybridní pobočková ústředna umožňující přepínání hovorů, řízení linek, přepojení volajícího s okolním světem přes IP, analogové (POTS) a digitální (T1/E1) rozhraní.

Asterisk pracuje na celé řadě operačních systémů, včetně systémů Linux, Mac OS X, OpenBSD, FreeBSD a Sun Solaris a poskytuje všechny funkce, které očekáváme od PBX, včetně mnoha pokročilých funkcí, které jsou často spojovány s high-end (vysoké náklady) pobočkovými ústřednami (PBX). Asterisk architektura je navržena pro maximální flexibilitu a podporuje Voice over IP u mnoha protokolů, které mohou spolupracovat s téměř všemi standardy telefonních zařízení, využívajících poměrně levný hardware.

Asterisk je modulární telefonní architektura umožňující měnit širokou škálu komunikačních protokolů a multimediálních kodeků. Asterisk je vyjímečný tím, že nabízí tzv. server médií (vytváření streamovaných médií pomocí protokolu RTP).

Asterisk byl velmi dobře přijat v call centrech po celém světě díky jeho pružnosti. Call centra a kontaktní centra jsou plně vybavena systémem ACD na bázi Asterisku. Asterisk našel uplatnění v call centrech také díky schopnosti vzdálené správy IP agentů, pokročilému routingu a prediktivnímu a hromadnému vytáčení.

1.4.1 Asterisk – možnosti konferenčních a videokonferenčních hovorů

Od prvních verzí programu Asterisk [15] lze využívat konferenční volání pomocí funkce MeetMe. Tato komponenta je součástí aplikace Asterisk. Pro konferenční hovor se používá nadefinovaná klapka (tzv. extension), na kterou může uživatel zavolat a spojit se s několika uživateli, kteří se slyší navzájem. Volaným je právě Asterisk (přesněji určitá klapka), který hovor přijme, spojí a odešle zpět k uživatelům.

Od verze Asterisku 1.6.2 lze využívat pro audio konference funkci ConfBridge, která je podobná konferenci MeetMe. Rozdíl je v mixování zvuku (audia) pomocí DAHDI (Digium Asterisk Hardware Device Interface). U ConfBridge se toto mixování provádí přímo v programu Asterisk. Od verze Asterisku 1.8, ve funkci ConfBridge, odpadá přímá závislost na časovači.

Standardní podpora Asterisku pro videokonference je pomocí protokolů H.263 a H.264. Toto je vhodné max. pro 2 účastníky. Pro více účastníků (3 a více) je vhodné

použít MCU (Multipoint Control Unit), což je zařízení aplikované pro přenos videokonferenčního hovoru. Jedná se o koncový bod pro 3 a více terminálů a bran (gateway) k účasti pro vícebodové konference. MCU se skládá z povinné části Multipoint Controller (MC) a volitelné Multipoint procesor (MP).

Lze využít videokonferenčních zařízení či softwaru třetích stran. Mezi nejznámější dodavatele videokonferenčních zařízení a komunikačních programů patří firma Polycom. Produkty této firmy jsou na prvním místě na světě s videokonferenčními zařízeními. Tyto videokonference jsou však na profesionální úrovni a jejich cena je nemalá. Využívají se ve větších firmách, které často komunikují na dlouhé vzdálenosti. Ušetří tím nemalé finanční náklady za dopravu svých zaměstnanců na různá jednání, zasedání a konference.

Zaměřil jsem se na testování a využití videokonferencí pomocí volně šiřitelných programů a softwarových videotelefonů. Blíže se o nich zmiňuji v teoretické části diplomové práce.

1.4.2. Asterisk – video kodeky

Asterisk podporuje následující video kodeky:

- H.261
- H.263
- H.263p (od verze Asterisk 1.4)
- H.264 (od verze Asterisk 1.4)

Video funkce Asterisk 1.6 zahrnují:

- Přímé volání
- Přehrávání (očekává se určité zpoždění)
- Záznam
- Video na IVR
- Hlasová schránka (nahrávání a přehrávání, problémy s pozdravem zprávy)

Některé kanály mají podporu pro videohovory v Asterisk:

- SIP
- IAX2
- H.323

Aby Asterisk umožňoval video, musíme upravit sip.conf:

```
[general]  
videosupport=yes
```

Potom každému uživateli (SIP/osoba) musíme přidat podporované kodeky. Samozřejmě kodeky musí podporovat SIP telefon či aplikace pro videokonference, které jsou připojeny k Asterisku.

- **Video IVR pro Asterisk**

VXI VoiceXML prohlížeč – IVR video/mediální server pro Asterisk. Server spravuje interaktivní video pro standardní aplikace napsané v programovacím jazyku VoiceXML 2.0 +

- **Video konvertor pro Asterisk**

FF konvertor - generuje video obsah pro Asterisk. Umožňuje konverzi souborů MOV do video kodeku H.263 videa a souboru wav kompatibilních s Asteriskem.

- **Videokonferenční programy pro Asterisk**

- * Mediamixer - od firmy Sergia Murillo
- * App_conference - má určité omezené podpory videa
- * VMukti - Open Source VoIP řešení od firmy VMukti

1.4.3. Asterisk - zabezpečení hovorů

Nejčastějším způsobem zabezpečení audia a videa v Asterisku je ochrana prostřednictvím šifrovacích protokolů.

Pro zabezpečení šifrovaného kanálu mezi koncovými uživateli, nebo mezi Asteriskem a koncovými uživateli, se používá Zfone, což je projekt Phila Zimmermanna [20].

Důležitou funkcí v nové verzi Asterisku 1.8.x.x bude možnost šifrování hovorů. V Asterisku verze 1.6.x.x je k dispozici neoficiální patch. O tuto funkčnost se nejvíce zajímaly firmy a státní instituce. Zabezpečení SRTP se uskutečňuje pomocí

SDESencrptions a od algoritmu MIKEY se upustilo. Signalizace může být zabezpečena pomocí TLS, a je využívána již od verze Asterisku 1.6.

Zabezpečení pomocí SRTP je možno aktivovat v SIP.conf parametrem:

```
Encryption= yes
```

1.5 GNU Gatekeeper OpenH323

GNU Gatekeeper [16] je open-source projekt, který vznikl v roce 2001. Jde o svobodný software šířený pod licencí GNU GPL. Nejznámějším gatekeeperem je bezesporu GNU GK. Jedná se o plně H.323 kompatibilní gatekeeper (dále jen GK) dostupný na stránkách projektu <http://www.gnugk.org> a použitelný pod licencí GPL.

GNU GK je úspěšný projekt a existuje řada sítí, které jsou postaveny na GNU GK, v akademické komunitě je to například GDS (Global Dialing Scheme), což je síť pro videokonference a telefonii, který vznikl původně na anglických univerzitách a postupně byl rozšířen po celém světě.

Současným koordinátorem projektu je Jan Willamowius. Jelikož se jedná o open-source projekt, je možné se do samotného vývoje, případně testování, osobně zapojit. GnuGK gatekeeper je velmi stabilní, proto je komerčně využíván mnoha organizacemi poskytujícími VoIP služby. Autoři projektu poskytují GnuGK pro operační systémy: Linux, Windows, FreeBSD, Solária a MacOS X. Pod operačním systémem Windows může GnuGK běžet jako služba v pozadí.

Nabízí mnoho užitečných funkcí, jako například flexibilní směrování hovorů, široké možnosti autentizace a autorizace, plnou podporu H.323 proxy a NAT a rovněž podporu H.235 bezpečnostních mechanismů. Velkou výhodou je vzájemná kompatibilita GnuGK gatekeeperu s řadou zařízení pro VoIP služby.

Implementaci H.323 přináší i Asterisk v podobě oh323 či ooh323 kanálu a je možné propojit řešení GnuGK s Asteriskem.

V materiálech [22] doc. M. Vozňák zmiňuje „Příkladem nejrozsáhlejšího nasazení GnuGK v ČR je síť sdružení vysokých škol CESNET2. V současné době je v rámci IP telefonie sdružení CESNET2 přihlášeno zhruba padesát hlasových brán (dále jen VoGW), které jsou registrovány k vnitřnímu GK na platformě Cisco. K těmto VoGW jsou připojeny pobočkové ústředny institucí (dále jen PBX), které mohou volat v rámci sítě CESNET2 a subjekty mohou využívat i výstupu do veřejné sítě přes ČVUT.

Sdružení CESNET byl přidělen přístupový kód do neveřejné sítě sdružení ve tvaru 4209500. Na Gnu GK je provozován národní gatekeeper akademické sítě v ČR.“

Podle doporučení H.323 Gatekeeper poskytuje tyto služby: překlad adres; nastavení přístupu; nastavení zatížení; správu zón; signalizaci hovoru; autorizaci hovoru; správu zatížení a správu volání.

GNU Gatekeeper OpenH323 implementuje většinu těchto funkcí založených na protokolu OpenH323.

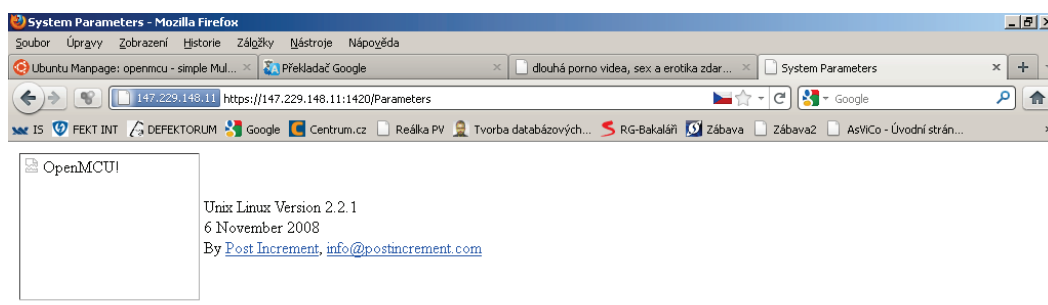
Aplikace Gatekeeper se spouští v cmd okně OS Windows příkazem:

```
telnet 147.229.148.11 7000
```

147.229.148.11 je IP adresa PC, kde je nainstalován Asterisk a samotný Gatekeeper. Číslo 7000 značí port, na kterém Gatekeeper naslouchá.

1.6 OpenMCU

OpenMCU [17] je jednoduchá multikonferenční jednotka, která pracuje s protokolem H.323. Ta má za úkol naslouchat příchozím hovorům. OpenMCU běží jako démon proces a je řízen přes webové rozhraní. Je směřován na port 1420 (<http://localhost:1420>).



System Parameters

Username

Password

Log Level 1=Fatal only, 2=Errors, 3=Warnings, 4=Info, 5=Debug

HTTP Certificate

HTTP Port

Gatekeeper Mode
☐ No gatekeeper
☒ Find gatekeeper
☐ Use gatekeeper

Interface

Enable video ☒

Video frame rate

Video quality

Disable codecs

Default room

Room time limit

Connecting WAV File

Entering WAV File

Leaving WAV File

Call log filename

Force split screen video ☐

Obr. 1.7: OpenMCUI – nastavení pomocí webového rozhraní

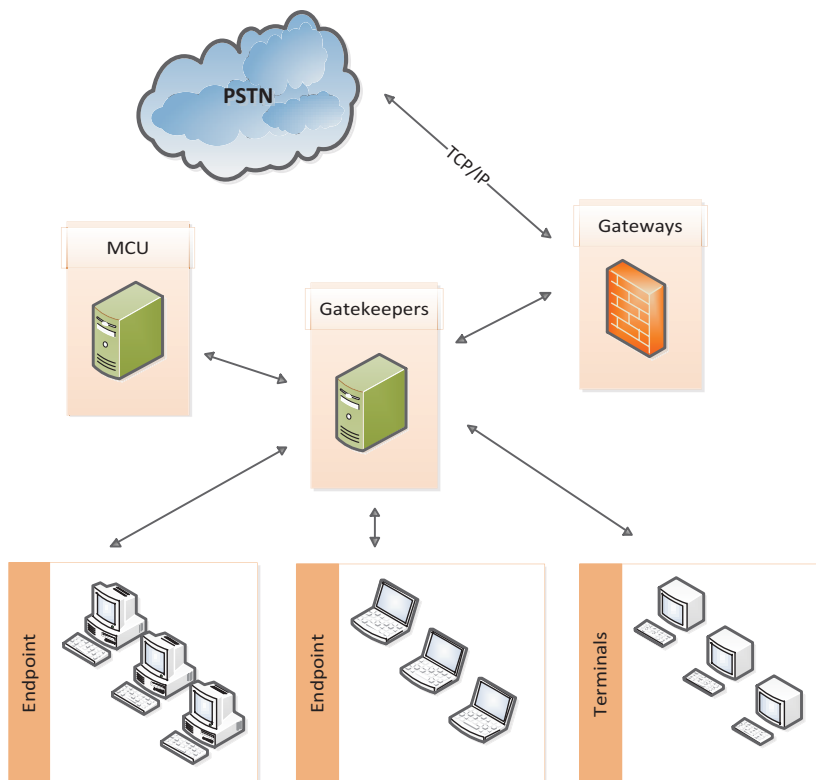
1.7 Videokonference v praxi

Videokonference můžeme rozdělit:

- dvoubodové (spojení dvou míst, jsou jednodušší s lepší kvalitou videohovoru)
- vícebodové (spojení více míst, jsou náročné s různou kvalitou přenosu)
- synchronní přenosy se signalizací (SCCP, MGCP, SIP, H.323)
- synchronní přenosy bez signalizace (MBONE Tools, VRVS, DVTS, AccessGrid, UltraGrid)

Pomocí protokolu H.323, komunikují tato zařízení:

- Terminál (Terminals, Endpoint)
- Správce (Gatekeepers)
- Brána (Gateways)
- MCU (Multipoint Control Units)



Obr. 1.8: Implementace IP řešení pro protokol H.323

Infrastruktura SIP

- SIP klient
- SIP server (Registrars, Redirects/Proxies, Location, Gateways)

Klienti H.323 a SIP

- softwarový klient
- hardwarové řešení (video telefon, all-in-one, set-top)

Softwarový klient pro svoji činnost může obsluhovat tyto komponenty: PC/notebook/server, USB kameru, náhlavní soupravu, externí audio, analogovou či digitální kameru pro zachytávání videa.

K nejznámějším softwarovým klientům patří: Ekiga, Microsoft NetMeeting, MyPhone, X-Lite, Windows Meeting Space, VCON point HD, Polycom PVX a další.

Pro kompaktní hardware jsou vhodná tato zařízení: se standardní kvalitou obrazu Polycom VSX 3000 a pro vysokou kvalitu obrazu HD je vhodná videokonference HDX 4002. Od firmy Tandberg je to kompaktní videokonference 1000 MXP či 1700 MXP.

K set-top zařízení patří Polycom HDX 7001, QDX 6000, HDX 8004, HDX 7002, HDX6004 a od Tandbergu Edge 95/85/75 MXP.



Obr. 1.9: Polycom HDX 4002



Obr. 1.10: Tandberg 1700 MXP

Mezi all-in-one videokonference bezesporu můžeme zařadit od Polycomu Executive Collection Floor systems a od Cisco TelePresence Profile 65 Dual.

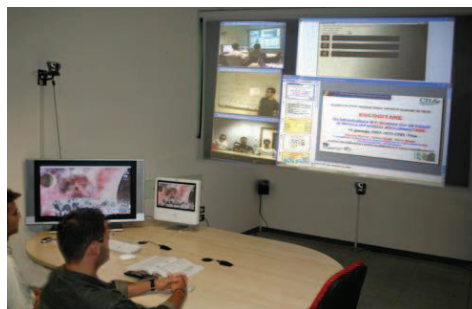


Obr. 1.11: Cisco TelePresence Profile 65 Dual

K zařízením, která využívají synchronní přenos bez signalizace, patří MBONE Tools, VRVS, DVTS, AccessGrid, UltraGrid).



Obr. 1.12: MBONE Tools



Obr. 1.13: AccessGrid

1.8 Klienti s podporou videohovorů kompatibilní s PBX Asterisk

- Leadtek produkty, jenž podporují SIP protokol např. GVSC SIP Carephone NCP3680, GCSC SIP IP Camera NSC3615, GVSC SIP PTZ IP Camera NSC3622, Videophone H.264 XTP8886
- Ekiga – podporuje protokoly SIP H.323, video H.261, MPEG4, H.263
- AuPix – podporuje protokoly SIP a H.323 video telefon
- Call Image Videotel - SIP videotelefony
- iFon – pro PDA s OS PocketPC
- Linphone pro PC s OS Linux – podporuje protokoly H.263p, Theora, Snow a MPEG4V. H.263p; produkty velmi dobře spolupracují s Asteriskem
- Microsoft Windows Messenger pro PC s OS Windows
- Wooksung WVP-2000- hardwarový SIP telefon
- Xten eyeBeam – pro OS s Windows a OSX
- Huawei ViewPoint 8220
- Kapanga Sip Video telefon
- GXV-3000 Grandstream H.264 and H.263 SIP video hardwarový telefon
- MyPhone - open source softwarový video telefon (H.323)

Obrázky viz příloha [\[Klienti s podporou videohovorů\]](#).

Kodek	TYP	Zkratka kodeku	CounterPath X-Lite 4.0 (build 58832)	CounterPath eyeBeam Enhanced v1.5.7.0	Ekiga 3.2.7	Linphone 3.4.1	MyPhone 02b12
(G.723.1)	audio	g723	X	X			X
(GSM)	audio	gsm	X	X	X	X	X
(G.711 u-law)	audio	ulaw	X	X	X	X	X
(G.711 A-law)	audio	alaw	X	X	X	X	X
(G.726 AAL2)	audio	g726aal2	X	X			X
(ADPCM)	audio	adpcm					
(16 bit Signed Linear PCM)	audio	slin	X				
(LPC10)	audio	lpc10					X
(G.729A)	audio	g729	X	X	X		X
(SpeeX)	audio	speex	X	X	X	X	X
(iLBC)	audio	ilbc	X	X	X	X	X
(G.726 RFC3551)	audio	g726	X	X	X		X
(G722)	audio	g722	X	X	X		
(H.261 Video)	video	h261			X		X
(H.263 Video)	video	h263	X	X	X	X	X
(H.263+ Video)	video	h263p	X	X	X	X	
(H.264 Video)	video	h264		X	X	X	

Tab. 1.3: Tabulka používaných kodeků pro jednotlivé klienty

2. Instalace a technická část

Vybral jsem si OS Linux Ubuntu verze 10.04, neboť Asterisk může pracovat pouze na linuxových platformách. Asterisk nelze provozovat na systémech s operačním systémem Windows. Použil jsem distribuci Asterisku verze 1.6.2.9, dále jsem nainstaloval OpenMCU verze 2.2.5 a Gatekeeper verze 2.3.2. Postup instalace serveru Ubuntu a aplikací je součástí příloh [\[Postup instalace Ubuntu a aplikací\]](#).

2.1 Instalace a konfigurace Asterisku verze 1.6.2.9

Instalace programu Asterisk je uživatelsky příjemná. Spouští se příkazem:

```
sudo apt-get install asterisk
```

Po stažení balíčku se spustí instalace. Pak se nastaví konfigurační soubory.

Aplikace Asterisk 1.6.2.9 se spouští příkazem:

```
asterisk -rvvvvvvvvvvvvvvvvvvv
```

2.2 Instalace a konfigurace klientů na podporu videohovorů

Pro testování jsem si vybral čtyři nejznámější softwarové klienty podporující videohovory. Jsou to COUNTERPATH X-Lite 4 ve verzi 4.1 (build 63214), Ekiga verze 3.2.7, Linphone verze 3.4.1 a MyPhone verze 0.2b12.

Asterisk může pracovat i s protokolem H.323, ale nemá Gatekeeper. Protokol H.323 je velmi rozšířený u videokonferencí. Proto jsem ho ověřil u klienta MyPhone a Ekiga.

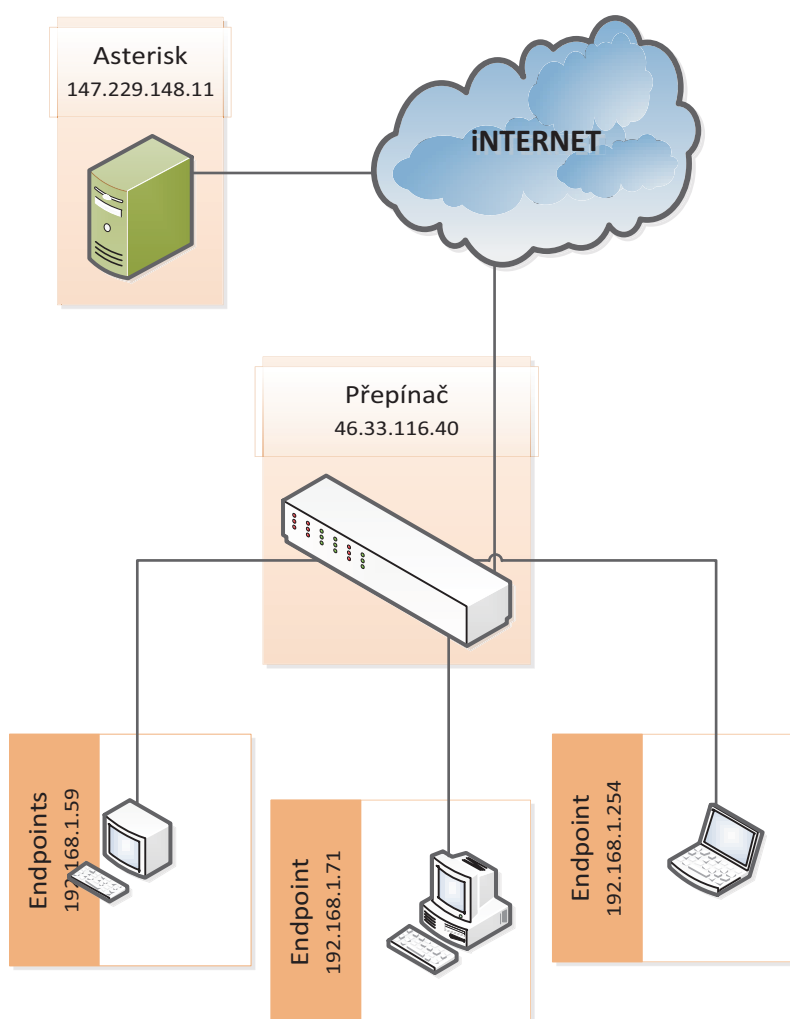
2.4 Testovací prostředí

Testoval jsem na počítačích s operačním systémem Windows XP Home SP3 a Windows Server 2003 Standard Edition SP2. Počítače byly zapojeny v lokální síti LAN. Lokální síti byla přidělena IP adresa 192.168.1.1. Měl jsem k dispozici tři počítače s těmito IP adresami:

PC 1 – 192.168.1.59
PC 2 – 192.168.1.71
PC 3 – 192.168.1.254

Asterisk byl nainstalován na PC fakultní sítě VUT Brno a byla mu přidělena IP adresa 147.229.148.11.

Počítače byly připojeny k přepínači (switch) viz obr. 2.1.



Obr. 2.1: Propojení PBX Asterisk s klienty

Softwarová pobočková ústředna Asterisk verze 1.6.2.9 byla na linuxové platformě Ubuntu 10.04 a byla jí přidělena IP adresa 147.229.148.11. Nadefinoval jsem si telefony pracující s protokolem SIP a H.323 (tab.2.2). Zapsal jsem je do konfiguračního souboru *Extensions.conf*, viz příloha *Extensions.conf*.

PC	IP	SIP	OOH323
PC 1	192.168.1.59	421	431
PC 2	192.168.1.71	422	432
PC 3	192.168.1.254	423	433

Tab. 2.1: Telefonní čísla pro protokol SIP a OOH323

Nainstaloval jsem GNU Gatekeeper verze 2.3.2 a upravil jsem konfigurační soubor *Gatekeeper.ini*, viz příloha Gatekeeper.ini.

Gatekeeper běží jako služba (daemon), kterou spustíme pomocí přepínače:

```
/etc/gnugk -r gatekeeper.ini
```

v případě požadavku lze monitorovat provoz:

```
gnugk - ttt
```

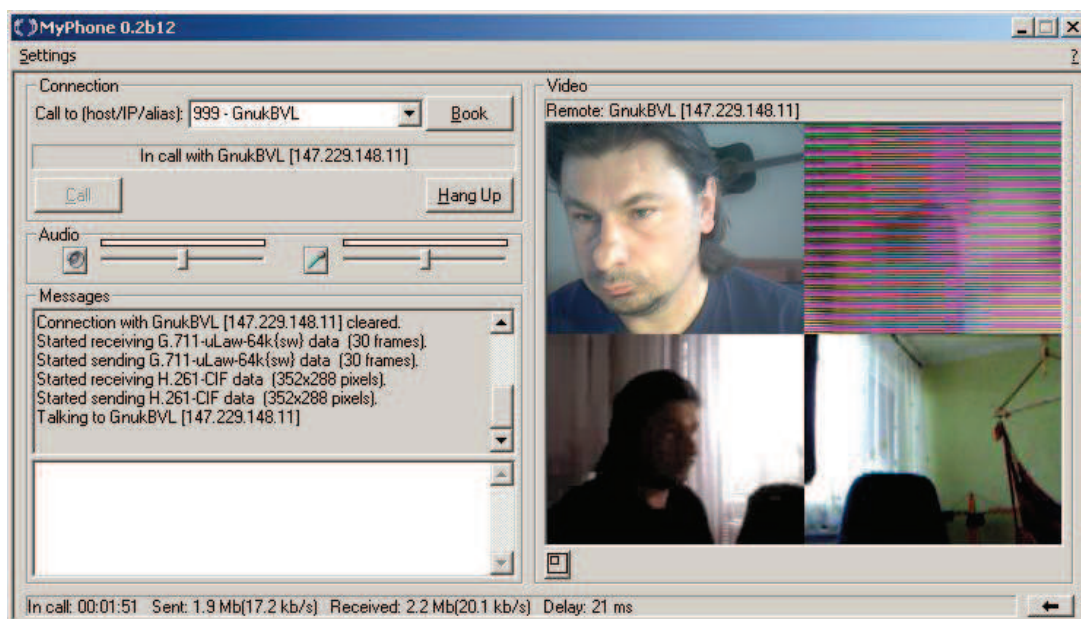
Další program, který jsem nainstaloval a spustil, je OpenMCU verze 2.2.5, což je multikonferenční jednotka, jež pracuje rovněž jako daemon a spouští se pomocí přepínače:

```
openmcu - d
```

Konfiguraci OpenMCU lze nastavit pomocí webového rozhraní:

<http://localhost:1420> nebo http://IP_adresa_serveru:1420

Protokol H.323 je standardně nainstalován s aplikací Asterisk. Upravil jsem konfigurační soubory *sip.conf* a *ooh323.conf* viz příloha sip.conf a soubor ooh323.conf. Po restartu aplikace Asterisk a Gatekeeper je testovací prostředí připraveno k prvnímu hovoru.



Obr. 2.2: Aplikace MyPhone

Room Name	Room Members					
	Name	Duration	Coder	RTP Packets/Bytes tx	RTP Packets/Bytes rx	TX Video frame rate/RX Video frame rate
999	431 [147.229.148.11]	7.05.554	G.711-uLaw-64k/G.711-uLaw-64k H.261-CIF/H.261-CIF	14186/3404640	10315/2475600	10.0007/7.93285
	434 [147.229.148.11]	4.519	G.711-uLaw-64k/G.711-uLaw-64k H.261-CIF/H.261-CIF	151/36240	130/31200	0/0
	433 [147.229.148.11]	5.38.549	G.726-40k/G.726-40k H.261-CIF/H.261-CIF	1410/1692000	33659/1682950	0/24.6807

Copyright ©2010 by [H323plus](http://H323plus.com), support@h323plus.com

Obr. 2.3: OpenMCU výpis uživatelů

2.5 Možnosti skriptování a vzdálené konfigurace

Program AsViCo (Asterisk Video Conferencing) vznikl na základě požadavku evidovat, monitorovat, dlouhodobě plánovat a obsluhovat videokonference. Software je naprogramován v programovacím jazyku PHP verze 5.3.5, konfigurován byl pro Apache verze 2.2.17 a spolupracuje s databází MySQL verze 5. Skripty php jsou přílohou diplomové práce, včetně konfiguračních souborů pro Apache, PHP a MySQL (apache2.conf, php.ini a my.cnf).

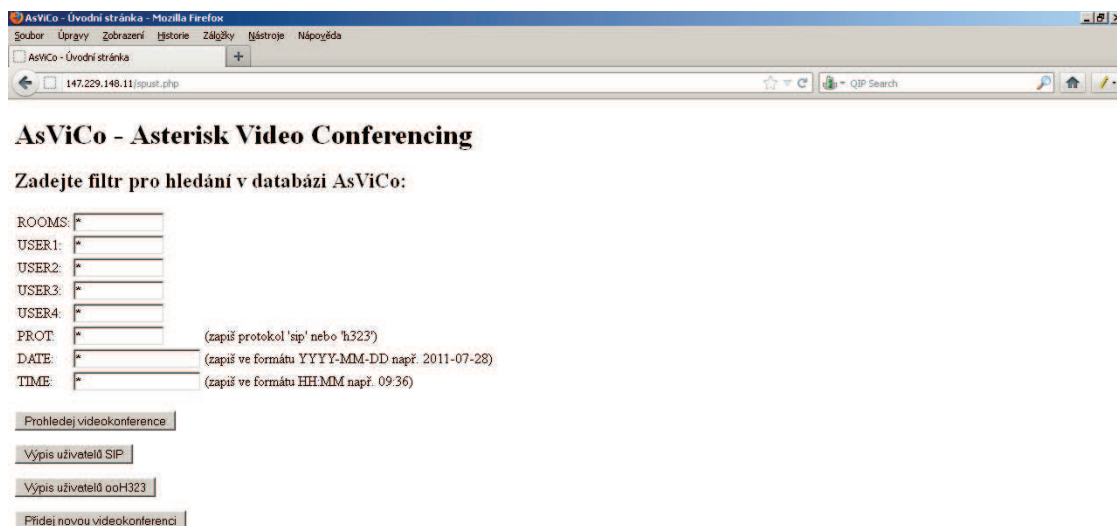
Výpis konfigurace Apache a PHP lze provést z webového rozhraní:

<http://147.229.148.11/ver.php>

Program AsViCo spustíme z webového rozhraní:

<http://147.229.148.11/spust.php>

zobrazí se nám úvodní stránka:



Obr. 2.4: Úvodní obrazovka programu AsViCo

Práce s programem AsViCo je intuitivní a přirozená. Při zakládání videokonference stačí znát název (číslo) místnosti (ROOMS). V mém případě to bylo číslo 999. Poté jsem zadal jednotlivé uživatele (SIP či H323). Nadefinujeme čas spuštění video konference. Na pozadí linuxu běží proces CRON s názvem automat, což je daemon, který spouští programy v určitý čas. Ten je umístěn v adresáři:

/etc/cron.d/automat

Proces se spouští každou minutu a kontroluje, zda není nutno spustit videokonferenci AsViCo, která postupně začne vytáčet jednotlivé klienty. Jakmile jsou klienti připraveni k videokonferenčnímu jednání, je zaznamenán do databáze čas videohovoru.

2.6 Videokonference pomocí protokolu ooh323, OpenMCU a gatekeeperu

Pro videokonference jsem zvolil klienta MyPhone verze 0.2b12. Tohoto klienta jsem nakonfiguroval postupně pro tyto kodeky: GSM, G.711 u-law, G.711 a-law a G.726. Prováděl jsem testovací volání mezi čtyřmi klienty a sledoval jsem zatížení serveru, kde byl nainstalovaný gatekeeper, pomocí aplikace htop. Výsledky jsem zaznamenal do tabulky.

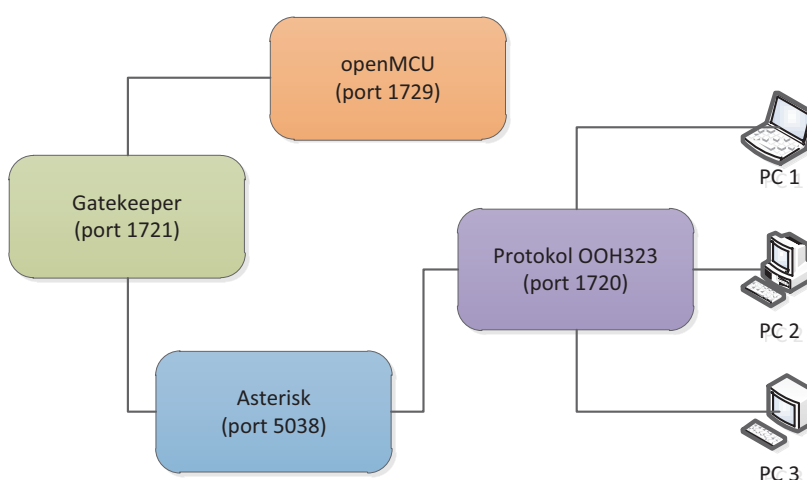
```

root@Asterisk-Vlk: ~
CPU[|||||] 12.1% Tasks: 200 total, 1 running
Mem[|||||] 177/1002MB Load average: 1.67 0.99 0.59
Swp[ ] 0/894MB Uptime: 01:43:31

  PID USER   PRI  NI  VIRT   RES   SHR  S  CPU%  MEM%   TIME+  Command
 1249 root    20   0  133M  114M  6376 S   1.0  11.4  0:11.13 asterisk
 1237 root    20   0  133M  114M  6376 S   0.0  11.4  0:03.74 asterisk
 1223 root    20   0  133M  114M  6376 S   0.0  11.4  0:00.12 asterisk
 1243 root    20   0  133M  114M  6376 S   0.0  11.4  0:00.12 asterisk
 1224 root    20   0  133M  114M  6376 S   0.0  11.4  0:00.16 asterisk
 1248 root    20   0  133M  114M  6376 S   0.0  11.4  0:00.12 asterisk
 1246 root    20   0  133M  114M  6376 S   0.0  11.4  0:00.18 asterisk

```

Obr. 2.5: Program htop



Obr. 2.6: Zapojení klientů v rámci videokonference pomocí openMCU

Kodeky	CPU (%)
GSM	12
G.711 uLaw	11
G.711 aLaw	13
G.726	40

Tab. 2.2: Kodeky a jejich serverová zatěž

Zjistil jsem, že nejmenší zátěž na systém má kodek G.711 uLaw a poté GSM. Přesto se doporučuje používat pro oblast Evropy kodek G.711 aLaw a nebo G.726.

2.7 Videokonference pomocí protokolu SIP a MCU Radvision

Další z možností, jak ověřit videokonference v Asterisku, je pomocí zařízení MCU Radvision SCOPIA 400, který je na Fakultě elektrotechniky a komunikačních zařízení v Brně. Zařízení je na adrese <http://147.229.149.29:8080> a výchozím prohlížečem je Internet Explorer.

Systém Radvision SCOPIA 400 se skládá z jednoho MCU modulu a dvou karet MVP (Media Video Processing), které slouží pro zpracování videa. Každá z karet MVP může obsloužit až 48 spojení pro maximální přenosovou rychlost 384 kbit/s. Při požadavku na vyšší kvalitu videa, jež odpovídá kvalitě SD (Standard Definition), může být využita přenosová rychlost do 2 Mbit/s, ale současně spojených uživatelů je maximálně 24. V případě použití kvality videa HD (High Definition) lze obsloužit pouze 12 uživatelů s přenosovou rychlostí do 4 MBit/s. Pro audio signál je využit kodek G.722.1 a pro video přenos může být aplikován kodek H.264, H.263 nebo H.261. K přenosu audio a video signálu slouží protokol RTP (Real-time Transport Protocol) [18].

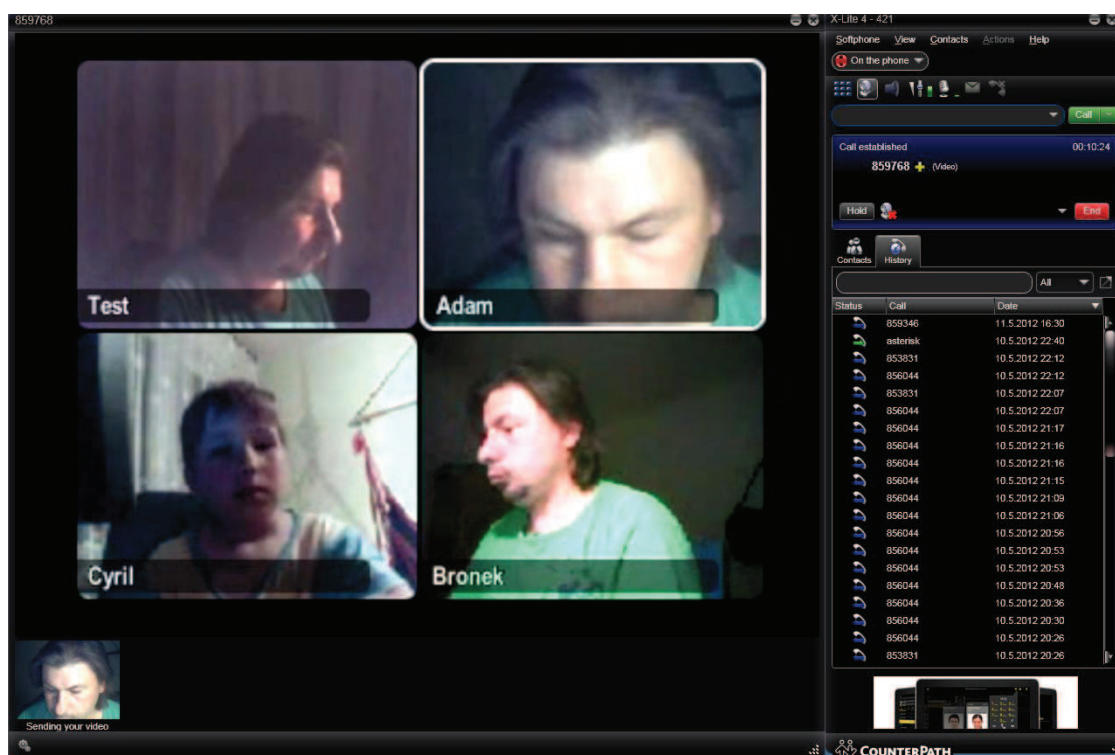
Pro správu a plánování videokonferencí je použit software iView Suite, který je stejně jako gatekeeper dostupný na webové adrese serveru a portu 8080. Zahrnuje iView Network Manager a iView Communications Manager. Společnost Radvision nabízí softwarové řešení terminálů SCOPIA Desktop. Skládá se ze dvou částí – serveru SCOPIA Desktop a terminálů SCOPIA desktop [19].

Nejprve jsem upravil konfigurační soubor *extension.conf* pro Radvision. Pomocí webové aplikace Radvision iView iCM v 7.5 si naplánujeme videokonferenci. Tato videokonference má své ID, které je šestimístné a začíná vždy 8. Pomocí aplikace X-Lite 4 (build 58832) vytvoříme konferenci (vytočíme ID videokonference Radvision). Můžeme však použít i integrovanou aplikaci SCOPIA Desktop, jež je součástí Radvisionu. Videokonferenci lze založit i pomocí aplikace AsViCo, která slouží k evidenci, plánování a k obsluze videokonferencí.

Postup při vytvoření videokonference pomocí Radvision SCOPIA 400:

a) aplikace X-Lite 4 a PBX Asterisk

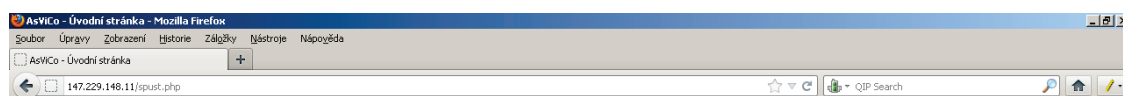
Vytvořil jsem SIP uživatelské účty v konfiguračním souboru SIP.conf (421-425) a nastavil extension.conf, což jsou konfigurační soubory PBX Asterisk. Jestliže se nachází uživatel za NATem, je nutno nakonfigurovat i klienta v sip.conf, který NAT podporuje. Po nakonfigurování aplikace X-Lite, jsem vytočil šestimístné ID videokonference Radvisionu. Spojení se uskutečnilo a mohl jsem začít využívat videokonferenční spojení ve spolupráci s aplikací SCOPIA Desktop viz obr. 2.7.



Obr. 2.7: Videokonference X-Lite a Radvision

b) Pomocí aplikace Asvico

Aplikace AsViCo je dostupná na adrese <http://147.229.148.11/spust.php>, kde naplánujeme novou videokonferenci. Tato se sama realizuje, když je dostupný videokonferenční klient na stanici viz obr. 2.8.



AsViCo - Asterisk Video Conferencing

Zadejte filtr pro hledání v databázi AsViCo:

ROOMS:

USER1:

USER2:

USER3:

USER4:

PROT: (zapiš protokol 'sip' nebo 'h323')

DATE: (zapiš ve formátu YYYY-MM-DD např. 2011-07-28)

TIME: (zapiš ve formátu HHMM např. 09:36)

[Prohledej videokonference](#)

[Vypis uživatelů SIP](#)

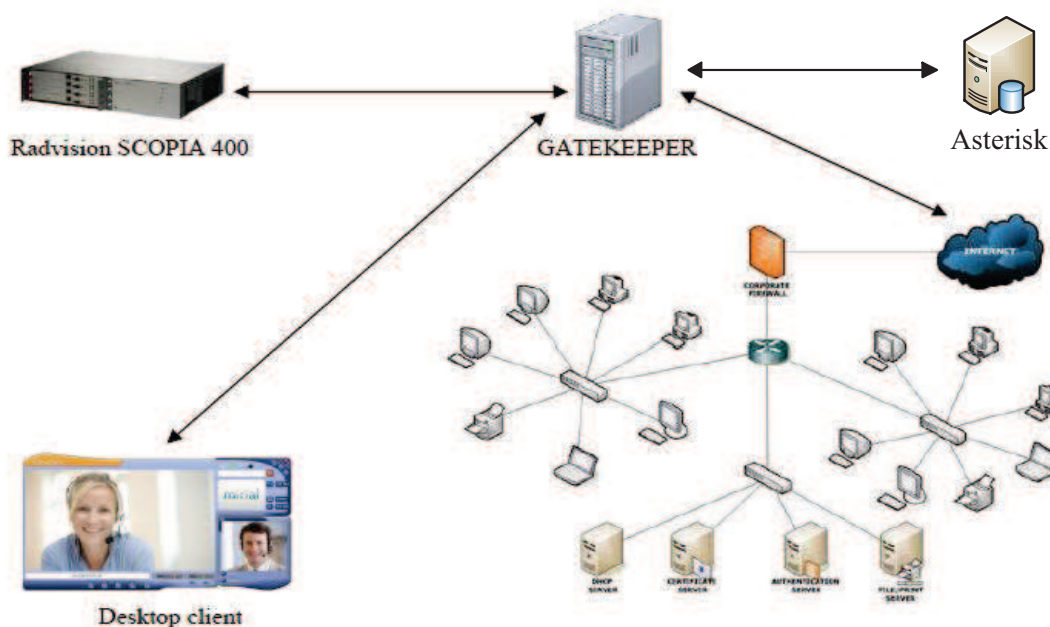
[Vypis uživatelů ooH323](#)

[Přidej novou videokonferenci](#)

Výsledky prohledávání v databázi AsViCo

ROOMS	USER1	USER2	USER3	USER4	PROTOCOL	DATE	TIME	CALLED	UPRAVIT	SMAZAT
859768	421	422	423		sip	2012-05-12	22:38:00		Upravit	Smazat

Obr. 2.8: Plánovaná videokonference pomocí aplikace AsViCo



Obr. 2.9: Zapojení Radvision SCOPIA 400 v rámci sítě LAN

3. Závěr

Neustálý vývoj v oblasti videokonferenčních hovorů je odrazem dynamického rozvoje komunikačních technologií. Uživatelé kladou stále vyšší požadavky na software, který využívají. Mezi ně mimo jiné patří i nízká finanční zátěž na pořízení programů.

V diplomové práci je obecně pojednáno o softwarové telefonní ústředně Asterisk. Jsou popsány signalizační protokoly, používané kodeky a programy pro videokonference.

Záměrem práce bylo sestavit videokonferenční hovor se softwarovým klientem, který podporuje protokoly SIP či H.323.

Byl vytvořen linuxový server Ubuntu verze 10.04, na kterém byla nainstalována softwarová telefonní ústředna Asterisk verze 1.6.2.9.

Po nakonfigurování telefonní ústředny Asterisk jsem testoval videokonferenční hovory v rámci sítě LAN a WAN. Na stanicích (počítačích) doporučuji používat stejného softwarového klienta, aby byl videokonferenční hovor kvalitní.

Ve spolupráci s Gatekeeperem verze 2.3.2 a openMCU verze 2.2.5 bylo zjištěno, že je kvalitnější podpora videa, nahrávání a přehrávání hovorů. Výhodnější je rovněž zpracování H.324 ISDN/3G videohovorů.

Na základě monitorování zátěže na procesor serveru s Asteriskem jsem došel k závěru, že největší zátěž je při použití kodeku G.726. Naopak nejmenší je při uplatnění kodeku G.711 uLaw a G.711 aLaw.

Dále byla vytvořena aplikace AsViCo, která slouží k evidenci, monitoringu, dlouhodobému plánování a obsluze videokonferencí.

Funkčnost byla ověřena u protokolu SIP (a aplikací X-Lite 4, Radvision SCOPIA 400 a Asterisk), i u protokolu H.323 (s aplikací MyPhone, Gatekeeper a Asterisk).

Z poznatků testování a instalace samotného softwaru je důležitá příprava konfiguračních souborů a následná implementace do provozu.

Na základě zkušebních hovorů je možné konstatovat, že kvalitnější přenos a obraz byly při použití protokolu SIP oproti užití protokolu H.323.

Literatura

- [1] DIGIUM, INC. About Asterisk [online]. c2009.
<<http://www.asterisk.org/support/about>>
- [2] OWEBU.CZ, VoIP, SIP protokol, 3.díl., c2009.
<<http://owebu.blogger.cz/PC-site/VoIP-SIP-protokol-3-dil>>
- [3] OWEBU.CZ, VoIP, H.323 protokol a ostatní, 4.díl., c2009.
<<http://owebu.blogger.cz/PC-site/VoIP-H-323-protokol-a-ostatni-4-dil>>
- [4] Mika, L., Knor. T., Protokol Media Gateway Control Protocol (MGCP) a jeho použití na Cisco IOS,
< <http://www.cs.vsb.cz/grygarek/TPS/projekty/0708Z/MGCP.pdf> >
- [5] searchunifiedcommunications.techtarget.com, Skinny Client Control Protocol (SCCP), c2005.
<<http://searchunifiedcommunications.techtarget.com/definition/Skinny-Client-Control-Protocol>>
- [6] astbook.asteriskdocs.org, VoIP Protocols - Chapter 8. Protocols for VoIP, c2005.
<http://astbook.asteriskdocs.org/en/2nd_Edition/asterisk-book-html-chunk/asterisk-CHP-8-SECT-2.html>
- [7] Vozňák, M., Zukal. D., Kvalita hovoru v prostředí VoIP, Praha, 2005
< http://homel.vsb.cz/~voz29/files/voz_71.pdf >
- [8] cesnet.cz , Videokonference [online], c2011.
<<http://www.cesnet.cz/videokonference/>>
- [9] packetizer.com, RFC 3711 - The Secure Real-time Transport Protocol (SRTP), c2004. <<http://www.packetizer.com/rfc/rfc3711/>>

- [10] networksorcery.com, The Secure Real-time Transport Protocol (SRTP), c2004.
<<http://www.networksorcery.com/enp/rfc/rfc3711.txt>>
- [11] minisip.org, Introduction, c2010.
<<http://www.minisip.org/>>
- [12] Zimmermann, P. ZRTP: Media Path Key Agreement for Unicast Secure RTP, c2011. <<http://zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-22.html>>
- [13] Steffen, A.; Kaufmann,D.; Stricker, A. SIP Security, 2004.
<http://security.hsr.ch/docs/DFN_SIP.pdf>
- [14] packetizer.com, H.323 Standards, c2011.
<<http://www.packetizer.com/ipmc/h323/standards.html>>
- [15] asteriskpbx-digium.blogspot.com, Asterisk cmd ConfBridge, c2010.
<<http://asteriskpbx-digium.blogspot.com/2010/10/asterisk-cmd-confbridge.html>>
- [16] gnugk.org, OpenH323 Gatekeeper - The GNU Gatekeeper, c2011.
<<http://www.gnugk.org/>>
- [17] sourceforge.net, OpenH323, c2010.
<<http://sourceforge.net/projects/openh323>>
- [18] Číka, P. , Balík, M., Systém pro efektivní komunikaci pracovníků výzkumných konsorcií. [Online] Elektrevue 2009/58 – 7.12.2009 str. 58-1
<<http://www.elektrevue.cz/cz/clanky/komunikacni-technologie/0/system-pro-efektivni-komunikaci-pracovniku-vyzkumnych-konsorcii/>> [cit. 18.5.2012]
- [19] Číka, P. , Balík, M., Systém pro efektivní komunikaci pracovníků výzkumných konsorcií. [Online] Elektrevue 2009/58 – 7.12.2009 str. 58-2
<<http://www.elektrevue.cz/cz/clanky/komunikacni-technologie/0/system-pro-efektivni-komunikaci-pracovniku-vyzkumnych-konsorcii/>> [cit. 18.5.2012]

- [20] Zfone, P. Asterisk PBX – Patches to support ZRTP [online]. c2006.
<http://zfoneproject.com/prod_asterisk.html>
- [21] PACKETIZER, INC. H.325 Papers and Presentations [online]. c2012.
<<http://www.packetizer.com/ipmc/h325/papers/>>
- [22] Vozňák, M.: Voice over IP [online]. c2012.
<http://homel.vsb.cz/~voz29/files/VOIP/VoIP_v5.pdf> [cit. 18.5.2012]

Seznam příloh

Příloha A - Klienti s podporou videohovorů

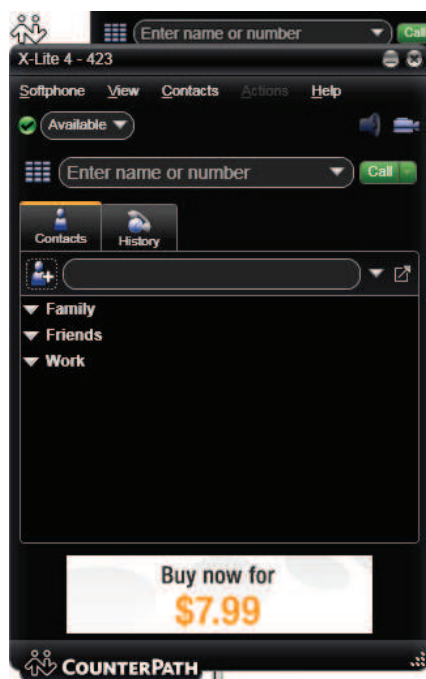
Příloha B - Postup instalace Ubuntu a aplikací

Příloha C - Diagram spojení SIP videokonference

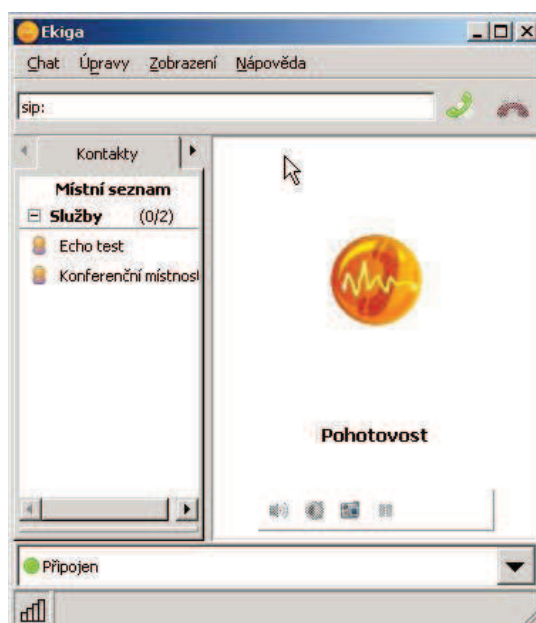
Příloha D - Diagram spojení H.323 videokonference

Příloha E - Přílohy na CD

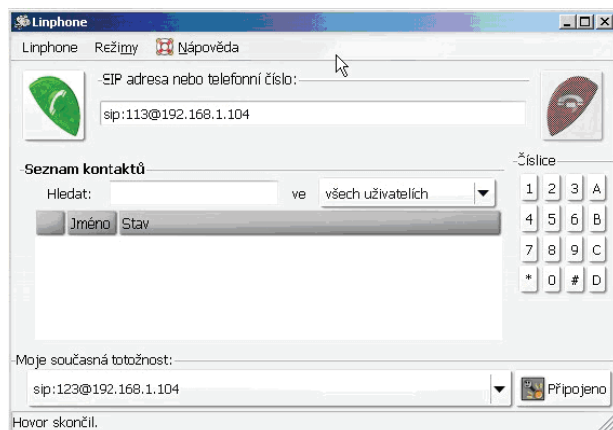
Příloha A - Klienti s podporou videohovorů



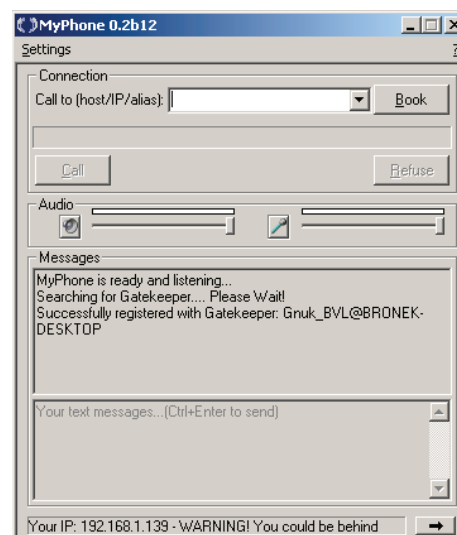
Obr. 3.1: CounterPath X-Lite 4
verze 4.1 (build 63214



Obr. 3.2: Ekiga verze 3.2.7



Obr. 3.3: Linphone verze 3.4.1



Obr. 3.4: MyPhone verze 0.2b12

Příloha B - Postup instalace Ubuntu a aplikací

Zvolil jsem instalaci Ubuntu 10.04 z instalačního média (ubuntu-10.04-server-i386.iso) ze serveru Ubuntu (<http://releases.ubuntu.com/10.04>). Zvolil jsem serverovou část, z důvodu lepší správy a aplikace jako byl Gnugk (Gatekeeper), OpenMCU, PHP či MySQL jsou určeny pro server. Konfigurace lze provádět i přes webové rozhraní (openMCU či MySQL).

Instalace Asterisk, kodeků, Gnugk, openMCU a PHPMyAdmin

- `apt-get update`
- `apt-get upgrade`
- `apt-get install asterisk`
- `apt-get install asterisk-ooh323c`
- `apt-get install libavcodec-extra-52 libx264-dev ffmpeg`
- `apt-get install libopal-dev libopal-dbg simpleopal`
- `sudo aptitude install libdc1394-dev bison flex libssl-dev libldap2-dev libexpat1-dev g++ autotools-dev libasound2-dev libavc1394-dev libraw1394-dev libdv-dev libsasl2-dev linux-libc-dev`
- `sudo aptitude install libspeex-dev libx264-dev libtheora-dev libavcodec-dev libavformat-dev`
- `sudo aptitude install gnome-common libsasl2-dev gettext libgnome2-dev libldap2-dev libgconf2-dev autoconf libgnomeui-dev libxv-dev intltool automake1.8 scrollkeeper libxml-parser-perl evolution-data-server-dev libavahi-common-dev libavahi-client-dev libavahi-glib-dev gnome-doc-utils libsigc++-2.0-dev libdbus-glib-1-dev libebook1.2-dev`
- `sudo aptitude install subversion`
- `apt-get install gnugk`
- `apt-get install openmcu`
- `apt-get install phpmyadmin`
- `apt-get update`
- `apt-get upgrade`

Nastavení cest s umístěním kodeků

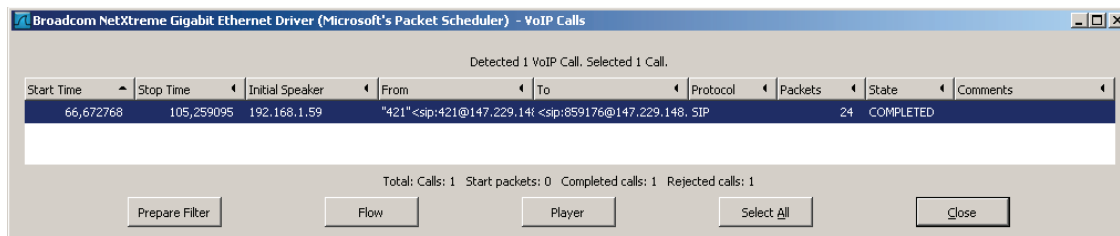
- `export PKG_CONFIG_PATH=/usr/lib/pkgconfig`
- `export LD_LIBRARY_PATH=/usr/lib`
- `export PTLIBPLUGINDIR=/usr/lib/opal-3.6.8`

Nahrání konfiguračních souborů

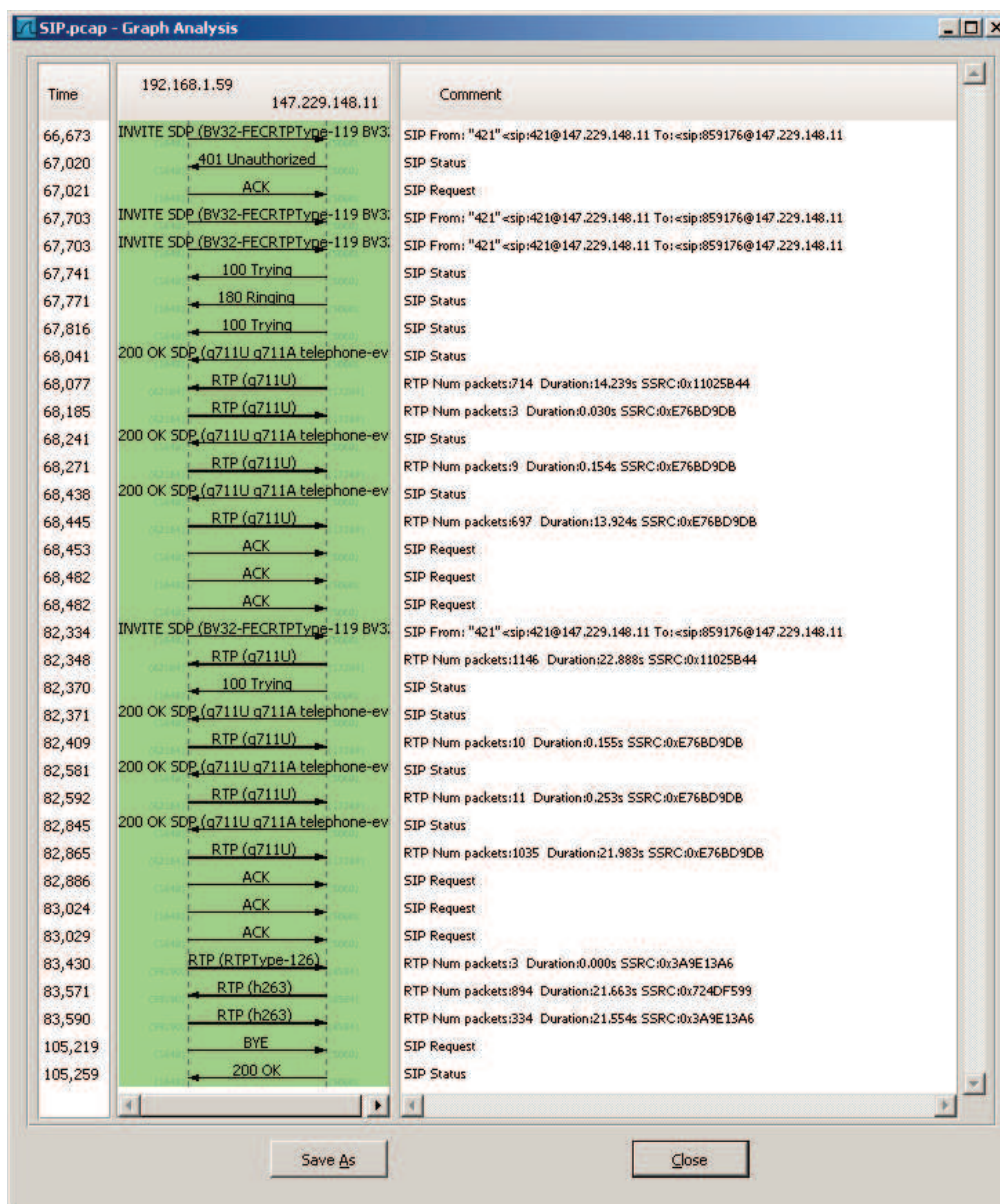
Aplikace	Soubory	Umístění Ubuntu (kam)
Apache	apache2.conf httpd.conf	/etc/apache2
Asterisk	asterisk.conf extensions.conf manager.conf ooh323.conf rtp.conf sip.conf	/etc/asterisk
AsViCo	automat.log automat.php mazani.php nova.php ooh323.php oprav.php pridani.php sip.php spust.php ver.php vyt_h323.php vyt_sip.php zmena.php	/var/www
Gatekeeper	gatekeeper.ini	/etc
MySQL	my.cnf	/etc/mysql
openMCU	openmcu.ini server.pem	/root/.pwlib_config
PHP	php.ini	/etc/php5/apache2

Příloha C - Diagram spojení SIP videokonference

Na obr. 3.5 a 3.6 je ukázaná komunikace mezi SIP spojením X-Lite 4 a MCU Radvision SCOPIA 400. Analýza spojení byla provedena pomocí program Wireshark 1.6.5.



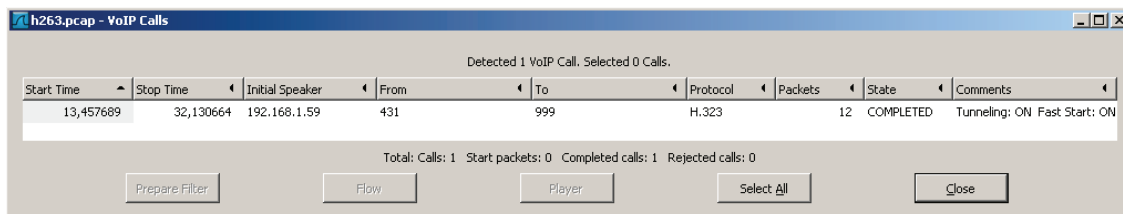
Obr. 3.5: Detekované SIP spojení X-Lite 4 a Radvision SCOPIA 400



Obr. 3.6: Graf SIP spojení X-Lite 4 a Radvision SCOPIA 400

Příloha D - Diagram spojení H.323 videokonference

Na obr. 3.7 a 3.8 je ukázaná komunikace mezi H.323 spojením MyPhone, openMCU a Asteriskem. Analýza spojení byla provedena pomocí program Wireshark 1.6.5.



h263.pcap - VoIP Calls

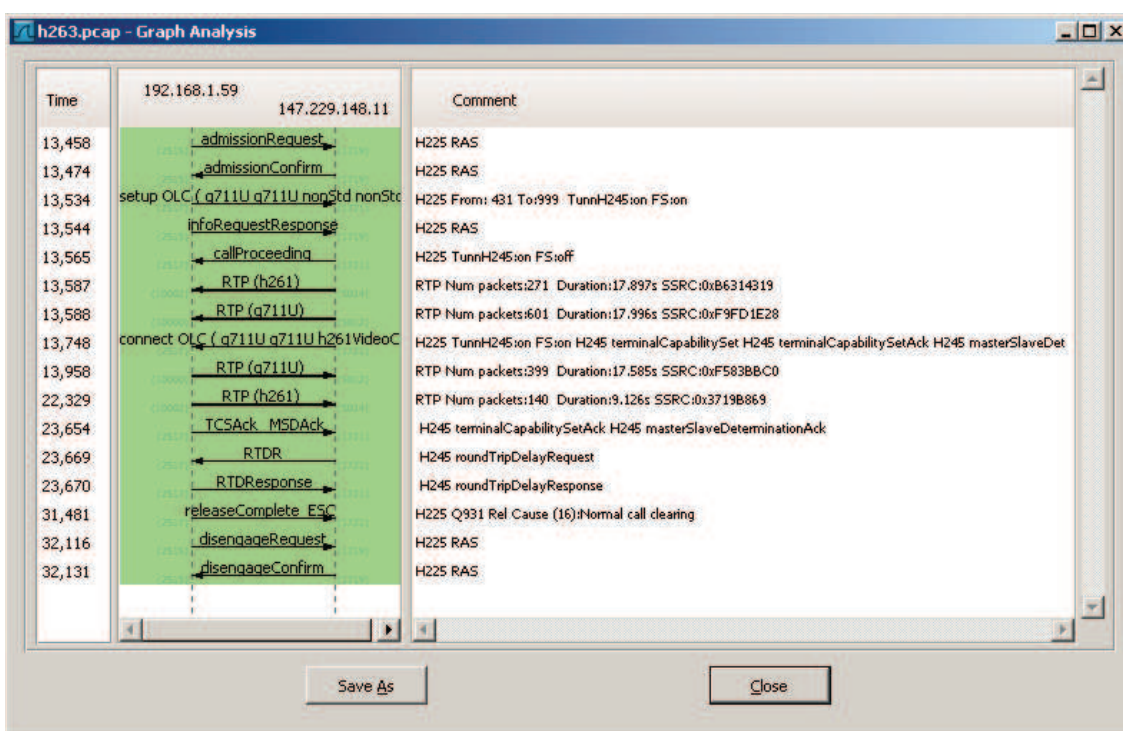
Detected 1 VoIP Call. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
13,457689	32,130664	192.168.1.59	431	999	H.323	12	COMPLETED	Tunneling: ON Fast Start: ON

Total: Calls: 1 Start packets: 0 Completed calls: 1 Rejected calls: 0

Buttons: Prepare Filter, Flow, Player, Select All, Close

Obr. 3.7: Detekované H.323 spojení MyPhone, openMCU a Asterisk



Obr. 3.8: Graf H.323 spojení MyPhone, openMCU a Asterisk

Příloha E – Přílohy na CD

Aplikace	Soubory
Apache	apache2.conf httpd.conf
Asterisk	asterisk.conf extensions.conf manager.conf ooh323.conf rtp.conf sip.conf
AsViCo	automat.log automat.php mazani.php nova.php ooh323.php oprav.php pridani.php sip.php spust.php ver.php vyt_h323.php vyt_sip.php zmena.php
Gatekeeper	gatekeeper.ini
MySQL	my.cnf
openMCU	openmcu.ini server.pem
PHP	php.ini