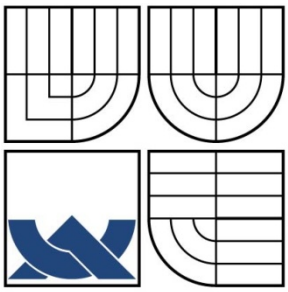
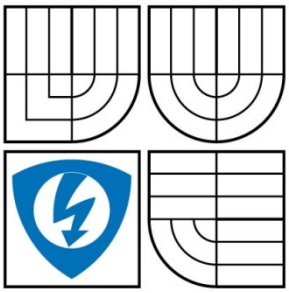


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

KONVERGOVANÉ ŘEŠENÍ HOVOROVÝCH SLUŽEB

CONVERGED SOLUTION OF SPEECH SERVICES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. TOMÁŠ MÁCHA
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÍT NOVOTNÝ, Ph.D.
SUPERVISOR

BRNO 2008

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bc. Tomáš Mácha

Bytem: Na Rybníčku 421, 739 24, Krmelín

Narozen/a (datum a místo): 29.7.1984, Frýdek-Místek

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - □ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP: Konvergované řešení hovorových služeb

Vedoucí/ školitel VŠKP: doc. Ing. Vít Novotný, Ph.D.

Ústav: Ústav Telekomunikací

Datum obhajoby VŠKP:

VŠKP odevzdal autor nabyvateli v*:

- □ tištěné formě – počet exemplářů 2
- □ elektronické formě – počet exemplářů 2

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….. ……

Nabyvatel Autor

ANOTACE

Rozvoj technologie VoIP je neodmyslitelně spojen s faktory rychlého růstu kvality a rychlosti připojení k Internetu. Nasazení technologie VoIP se stalo jednou z klíčových oblastí konvergence komunikačních a informačních systémů.

Mezi cíle diplomové práce patřilo prostudovat problematiku IP telefonie, přenosu hlasu v datových sítích, podle architektur H.323, SIP a Cisco. Dále navrhnout a zprovoznit experimentální pracoviště zmíněných architektur a podle možností vybavení laboratoře zajistit jejich vzájemné propojení.

V první části diplomové práce jsou podrobně popsány zmíněné architektury včetně jejich porovnání. Tématem dalších částí jsou návrh a implementace řešení VoIP síťové infrastruktury. Jsou zde uvedeny řídicí a zprostředkující systémy pro VoIP a hardwarové i softwarové IP telefony. Následně je řešena problematika návrhu VoIP sítí pro experimentální ověření oboustranné komunikace v datové síti různými VoIP terminály. S pomocí dostupných spojovacích systémů a koncových zařízení bylo navrženo experimentální pracoviště architektur SIP, H.323 a Cisco včetně jejich konvergovaných řešení.

Součástí práce je podrobná analýza veškeré síťové komunikace realizovaných spojení. Je zde uveden přehledný výpis detailních informací jednotlivých paketů a diagramy sestavených spojení.

Na základě získaných poznatků jsou navrženy dvě laboratorní úlohy zabývající se realizací hlasových služeb v prostředí datových sítí. Účelem těchto úloh je praktické seznámení studentů s principy fungování IP telefonie prostřednictvím zmíněných architektur.

KLÍČOVÁ SLOVA

VoIP, konvergence, hlas, přenos, signalizace

ABSTRACT

Development in VoIP technology is connected with the rapid growth of quality and data rate of the Internet connection. The application of the VoIP technology has become one of the key areas in telecommunication and networking.

The main task of this thesis was to explore the questions of IP telephony and voice transmission over data networks according to H.323, SIP and Cisco architectures. Next focus was on designing and implementing experimental workplaces of mentioned architectures and their converged solutions.

The purpose of the first chapter is to introduce the theory background of architectures required for implementation of real-time services in data networks and their comparison. The key objectives of the second and third part are to design and implement experimental workplaces containing signaling and proxy servers and hardware or software IP phones of several architectures. Illustration examples of different network topologies are included to demonstrate designed and realized VoIP solutions.

Several tests of established communication are done using a packet analyzer. These tests examine duplex data transmission over IP.

This article also contains two laboratory exercises designed according to gained practical experiences. The laboratory exercises provide an overview of theory and clearly indicate the possibilities of IP telephony.

KEYWORDS

VoIP, convergency, voice, transmission, signaling

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Konvergované řešení hovorových služeb jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s využitím 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 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 .....

.....
podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc. Ing. Vítu Novotnému, Ph.D., za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne .....

.....
podpis autora

SEZNAM ZKRATEK

ACF	Admission Confirm
ARJ	Admission Reject
ARQ	Admission Request
AVVID	Architecture for Voice Video and Integrated Data
CLI	Command Line Interface
DCF	Disengage Confirm
DHCP	Dynamic Host Configuration Protocol
DRQ	Disengage Request
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
HTTP	Hyper Text Transfer Protocol
IAX	Inter – Asterisk eXchange
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
MEGACO	MEdium GAteway COntrol Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
NAT	Network Address Translation
PBX	Private Branch eXchange
POTS	Plain Old Telephone Service
QoS	Quality of Service
RAS	Registration, Admission, Status
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SCCP	Skinny Call Control Protocol
TDM	Time Division Multiplexing
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
XML	eXtensible Markup Language

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Internet se v současnosti stává stále masovějším prostředkem pro přenos informací rozmanitých typů. Hovorová služba není v tomto výjimkou. Pro nasazení telefonní služby do prostředí sítí IP vznikla řada technologií, avšak proprietárních, a tedy vzájemně nekompatibilních. To vyústilo v potřebu standardizovaného řešení. V současnosti existují dvě standardizované architektury, a to SIP a H.323. Implementace technologie VoIP představuje zavedení podpory integrovaných služeb do IP sítí umožňující tak přenos dat, hlasu a videa nad jedinou infrastrukturou. Návrh a následná realizace VoIP sítí vyžaduje pečlivé plánování k zajištění efektivní činnosti a požadované kvality přenášeného hlasu.

Cílem práce je osvětlení problematiky hovorových služeb v sítích IP. V úvodu pojednávám o základních standardech, které jsou podmínkou pro úspěšné začlenění služeb v reálném čase do datových sítí. V současné době nejperspektivnějším standardem v oblasti multimediálních komunikačních služeb je signalizační protokol SIP. Obliba protokolu stoupá díky jeho struktuře, jednoduchosti a pružnosti. Protokolová sada H.323 představuje další významný standard pocházející z rodiny doporučení organizace ITU pro přenos obecně multimediálních dat po IP sítích. Dále je popsán protokol SCCP, proprietární protokol firmy Cisco, sloužící pro komunikaci mezi Cisco CallManagerem a Cisco VoIP telefony. Posledním zmíněným protokolem je také proprietární řešení, a to protokol IAX, původně určený pro softwarovou pobočkovou ústřednu Asterisk.

Dále je zde zmíněno o hardwarových a softwarových řídicích zařízeních, zprostředkujících systémech a terminálech pro VoIP. Na základě získaných poznatků o softwarových serverech je pro realizaci experimentálního pracoviště vybráno jedno efektivní řešení každého standardu. Softwarová pobočková ústředna Asterisk zastupuje doménu SIP, GNU Gatekeeper je řídicím prvkem domény H.323 a CallManager je aplikačním serverem pro doménu Cisco.

V projektu je navrženo VoIP řešení hovorových služeb pro experimentální ověření oboustranné komunikace v datové síti různými VoIP terminály jednotlivých architektur. Dále je navrženo řešení pro konvergenci SIP a H.323 sítě, kde GNU Gatekeeper je využíván ve funkci gatekeeperu potřebného pro kontrolu H.323 kanálu v softwarové ústředně Asterisk. Součástí práce je i návod na konfiguraci Cisco CallManageru pro uskutečnění telefonního hovoru s koncovými body v doméně SIP i H.323.

V neposlední řadě je popsáno propojení dvou SIP domén s řídicím prvkem Asterisk a propojení dvou H.323 domén s řídicím prvkem GNU Gatekeeper. Při návrhu je kladen důraz na stanovené požadavky na VoIP síť.

S pomocí dostupných nástrojů je analyzována veškerá síťová komunikace jednotlivých architektur i jejich vzájemného propojení. Jednotlivé signalizační postupy pro SIP, H.323 a Cisco při sestavení, průběhu a ukončení spojení jsou zobrazeny v detailních diagramech.

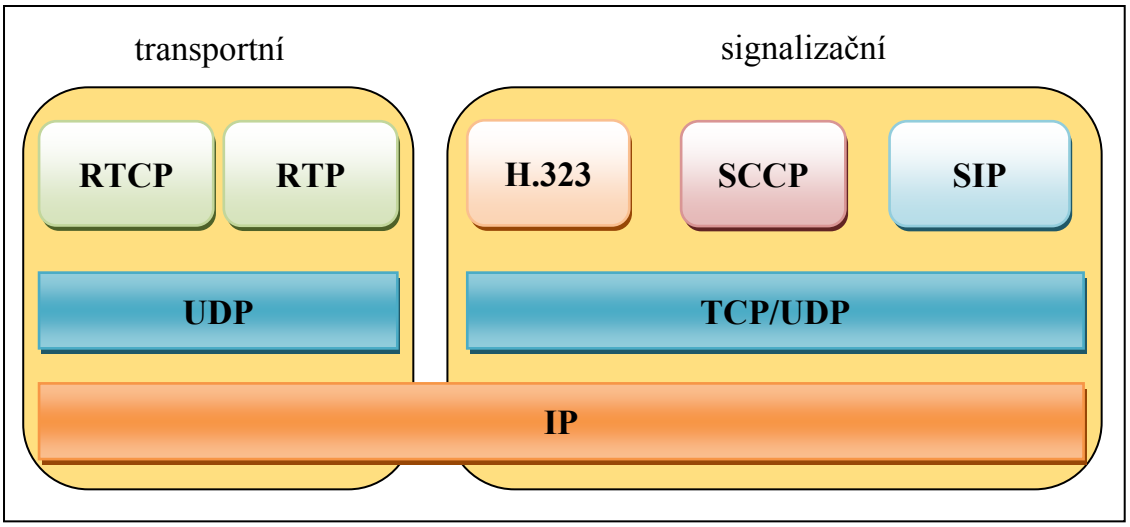
V závěru jsou navrženy dvě laboratorní úlohy zabývající se realizací hlasových služeb v prostředí počítačových sítí. Účelem úloh je praktické seznámení studentů s principy fungování IP telefonie prostřednictvím standardů SIP a H.323. Studenti budou mít možnost analýzy hovorových spojení díky protokolovému analyzátoru Wireshark. Součástí laboratorních úloh jsou kontrolní otázky sloužící k prověření pochopení principu VoIP.

1 ARCHITEKTURY PRO VOIP

Technologie VoIP umožňuje přenos digitalizovaného hlasu prostřednictvím sítí pracujících na bázi IP protokolu. Tvoří alternativu ke klasické telefonii, založené na použití sítí s přepojováním okruhů. Nasazení technologie VoIP vyžaduje implementaci nových funkčních prvků a komunikačních protokolů definující pravidla přenosu dat. Protokoly zajišťující hlasovou službu v prostředí IP jsou rozděleny na signalizační a transportní.

Navázání spojení mezi účastníky, řízení toku a jeho ukončení je realizováno prostřednictvím signalizačních protokolů. Signalizační protokoly můžeme dělit na standardizované (H.323, SIP, IAX2, MGCP, MEGACO, atd.) nebo proprietární (SCCP, IAX2, aj.).

Úlohou transportních protokolů (typicky RTP, RTCP) je dopravit multimediální obsah (hlas, video) od vysílače k přijímači a opatřit tento signál informacemi, které umožní přijímači co nejvěrnější reprodukci informace vyslané protějším koncovým uzlem. Architektury standardů používaných VoIP zachycuje Obrázek 1.1.



Obrázek 1.1 Architektura standardů používaných VoIP

1.1 ARCHITEKTURA SIP (SESSION INITIATION PROTOCOL)

Architektura SIP je řešení VoIP založené na hlavním signalizačním protokolu SIP, který vyvinula organizace IETF. Protokol SIP slouží k sestavení, modifikaci a ukončení relací mezi dvěma a více účastníky v IP sítích. SIP je textově orientovaný protokol využívající principy známé z internetových protokolů HTTP. Je to protokol typu klient – server. Často jedno zařízení (například telefonní přístroj) může současně pracovat jako klient i server (tzv. agent).

Jedná se o aplikační protokol, takže pro úspěšnou realizaci služeb vyžaduje spolupráci s nižšími vrstvami. Zejména protokoly SDP (Session Description Protocol), SAP (Session Annoucement Protocol), RTSP (Real-Time Streaming Protocol), protokoly pro řízení bran MGCP (Media Gateway Control Protocol) a MEGACO (MEdia GAteway Control Protocol) a protokoly pro přenos multimediálních dat RTP (Real-time Transport Protocol) a RTCP (Real-time Transport Control Protocol).

1.1.1 SIP komponenty

Protokol SIP definuje architekturu, která se skládá z následujících komponentů:

- SIP User Agent,
- SIP servery.

SIP User Agent

User Agent představuje koncové zařízení sítě SIP. Nejčastěji se jedná o softwarové či hardwarové telefony.

V rámci SIP User Agent se rozlišují User Agent Client (UAC), který iniciuje spojení a User Agent Server (UAS), který reaguje na příchozí žádosti a posílá odpovědi na tyto žádosti. V koncovém zařízení je implementován jak UAS tak UAC.

SIP servery

SIP servery umožňují zprostředkování hovorů mezi koncovými účastníky. Rozlišujeme tři základní druhy SIP serverů:

SIP Proxy server – server analyzuje příchozí zprávy. Přijímá žádosti o spojení od UA nebo jiných proxy serverů a přeposílá je dalšímu proxy serveru nebo přímo UA, pokud se nachází v jím řízené doméně.

Redirect server – server přijímá žádosti o spojení od UA nebo jiných proxy serverů a prostřednictvím lokalizační služby zjistí žádanou adresu a předá ji zpět klientskému UA.

Registrar server – server přijímá registrační žádosti od UA a aktualizuje podle nich databázi koncových zařízení.

1.1.2 SIP zprávy

Protokol SIP používá zprávy Request a Response (žádost a odpověď), pomocí kterých mezi sebou komunikují klienti a servery. Struktura zprávy nesená SIP protokolem je tvořena hlavičkou a vlastním tělem zprávy. [7] Typické využití zpráv protokolem SIP potřebných k sestavení, řízení a ukončení spojení znázorňuje Obrázek 4.1.

Requests (žádosti)

Žádosti jsou obvykle užívány k inicializaci procedury (sestavení, ukončení spojení) nebo oznamují příjemci konkrétní požadavek.

- **INVITE** – žádost o navázání spojení nebo o změnu parametrů existujícího spojení,
- **BYE** – žádost o rozpojení spojení,
- **ACK** – klient potvrzuje, že obdržel odpověď na žádost INVITE,
- **REGISTER** – žádost o registraci klienta na registrar serveru,
- **CANCEL** – žádost o zrušení probíhající žádosti INVITE,
- **OPTIONS** – žádost o zaslání podporovaných funkcí na serveru,
- **INFO** – přenos informací během hovoru. [7]

Responses (odpovědi)

Odpovědi jsou třímístné kódy označující výsledek žádosti. Lze je rozdělit do šesti skupin podle první číslice.

- **1xx** (informační) – požadavek byl přijat a zpracovává se,
- **2xx** (úspěch) – činnost byla úspěšně realizována, pochopena a akceptována,
- **3xx** (přesměrování) – musí být realizovány další procedury pro úplnost požadavku,
- **4xx** (chyba klienta) – požadavek obsahuje nesprávný syntax,

- **5xx** (chyba serveru) – server selhal při zpracování správného požadavku,
- **6xx** (obecná porucha) – žádost nebude provedena ani na jiném serveru.

Další dvě číslice jsou pro každou třídu jednoznačně definovány a vyjadřují příslušné stavy v dané třídě. [7]

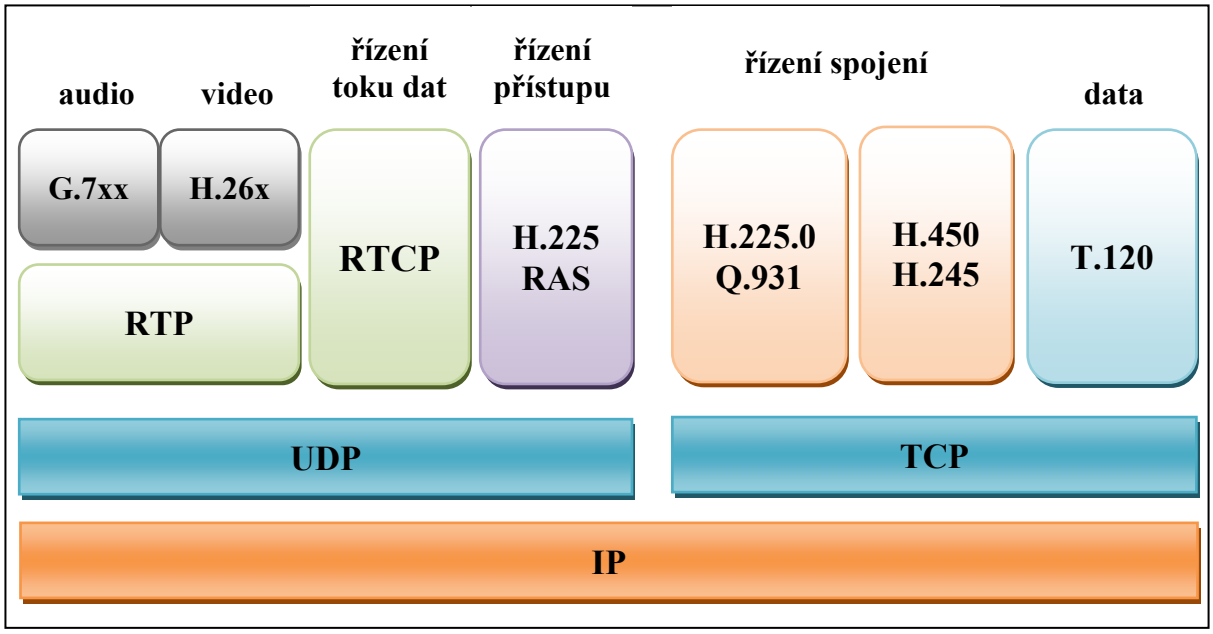
1.1.3 Adresace v SIP

Základní adresa uživatele má tvar e-mailové adresy, nazývá se URI (Uniform Resource Identifier). Příkladem SIP URI je zápis ve tvaru ***sip:jméno@doména***. Toto je adresa, kterou normálně použije volající, když chce navázat relaci s druhou stranou. Adresa však může obsahovat i další doplňující údaje. Úplný tvar adresy je ve tvaru ***sip:[uživatel[:heslo]@]hostname[:port][;parametry][?hlavičky]***.

Obsah hranatých závorek označuje nepovinné části. Jediným povinným údajem je jméno nebo IP adresa domény.[1]

1.2 Architektura H.323

Organizace ITU definuje protokolovou sadu H.323 spravující protokoly pro přenos dat, hlasu a videa (obecně multimediální informace) v IP sítích. H.323 představuje součást protokolové série ITU-T H.32x komunikačních doporučení pro různé typy transportních sítí. Protokolová sada zahrnuje řízení spojení, management přenosu a zpracování multimediálních dat. Protokolovou výbavu H.323 zobrazuje Obrázek 1.2. [6]



Obrázek 1.2 Protokolová sada architektury H.323

1.2.1 H.323 komponenty

Protokolová sada H.323 rozlišuje čtyři následující komponenty:

- terminál,
- gateway,
- gatekeeper,
- konferenční jednotka (MCU).

Terminál

Terminál představuje softwarový nebo hardwarový koncový bod umožňující obousměrnou multimediální komunikaci. Jedná se o jedinou povinnou složku H.323 sítě. Povinnou službou terminálu je hovorová služba, případně video nebo datové služby.

Terminál musí podporovat:

- protokoly pro přenos multimediálních dat v IP síti (RTP) a pro kontrolu tohoto přenosu (RTCP),
- protokol pro zprostředkování informací o použitém přenosovém kanálu a jeho vlastnostech (H.245),
- protokol zajišťující signalizaci a navazování spojení mezi koncovými uživateli (H.225.0Q.931),
- protokol zajišťující signalizaci s gatekeeperem (H.225.0 – RAS),
- audio kodek G.711.

Terminál může podporovat:

- video kodeky (H.261, H.263),
- další typy audio kodeků,
- protokol zajišťující datový přenos (T.120). [3]

Gateway

Představuje nepovinnou součást H.323 sítě zajišťující spojení s jinými druhy sítí (ISDN, PSTN). Gateway (brána) sestává z MGC (Media Gateway Controller) obsluhující hovorovou signalizaci a z MG (Media Gateway), který provádí konverzi audio a video formátů. Terminál pro komunikaci s bránou používá protokoly H.225.0 – Q.931, H.225.0 – RAS a H.245.

Gatekeeper

Nepovinná, avšak pro plnou funkčnost architektury nezbytná komponenta poskytující řídicí služby pro brány a terminály. Provádí překlad adres do tvaru použitelného v H.323 a řídí přenosové kapacity. Obě tyto funkce jsou definovány v RAS (Registration, Admission, Status). Pro překlad aliasové adresy na transportní adresu je využívána překladová tabulka. Řízení přístupu může být ovlivněno na základě autorizace, momentální kapacity a dalších kritérií. Řízení přenosové kapacity zahrnuje provádění požadavků na šířku přenosového pásma. Gatekeeper nabízí i volitelné služby, jako jsou vzdálený přístup, číslovací plán, uživatelský profil atd.

Konferenční jednotka MCU

Konferenční jednotka zajišťuje konferenci mezi třemi a více uživateli a zároveň určuje přenosové vlastnosti konference. Jednotka MCU se skládá povinně z MC (Multipoint Controller) a volitelně z MP (Multipoint Processor). MC řídí sestavování konference a MP zpracovává přenášená data v konferenci.

1.2.2 H.323 zprávy

Zprávy protokolové sady H.323 jsou binárně zapouzdřeny v dílčích protokolech a jsou přenášeny prostřednictvím TCP i UDP. Typické využití zpráv protokolem H.323 potřebných k sestavení, řízení a ukončení spojení znázorňuje Obrázek C. 1. Významné jsou zprávy protokolu H.225.0 – RAS (Registration, Admission, Status) zajišťující sestavení, průběh a ukončení hovoru mezi koncovým bodem a gatekeeperem. Přenášejí se protokolem UDP a gatekeeper standardně poslouchá na portu 1719. Mezi RAS zprávy patří:

- **ARQ** (Admission Request) – požadavek k povolení hovoru,
- **ACF** (Admission Confirm) – schválení a povolení požadavku,
- **ARJ** (Admission Reject) – odmítnutí požadavku,
- **DRQ** (Disengage Request) – ohlášení ukončení hovoru,
- **DCF** (Disengage Confirm) – schválení a povolení ukončení hovoru.

Zprávy protokolu H.225.0 – Q.931 slouží k signalizaci mezi terminály. Přenášejí se protokolem TCP a standardní port, na kterém terminály očekávají spojení, je 1720. Příklady zpráv H.225.0 – Q.931 jsou následující:

- **Setup** – požadavek volající strany o ustanovení spojení,
- **Call Proceeding** – odpověď protistrany na zprávu Setup, požadavek se zpracovává,
- **Alerting –** protistrana vyzvání,
- **Connect –** protistrana přijala žádost o spojení,
- **Disconnect –** hovor je odmítnut a ukončen,
- **Release –** odezva na zprávu Disconnect o uvolnění spojení,
- **Release Complete –** uvolnění spojení dokončeno.

Zprávy protokolu H.245 slouží k signalizaci mezi dvěma koncovými body (End – to – End signalizace), pomocí níž jsou vyměňovány informace o vlastnostech terminálů a je řízen přenos multimediálních informací prostřednictvím logických kanálů. [8] Příklady zpráv H.245 jsou následující:

- **Terminal Capability Set** – každý terminál informuje protistranu o druhu informace, kterou je schopen přijímat nebo vysílat.
- **Open Logical Channel** – otevření logických kanálů, které multiplexují přenosové cesty mezi terminály. Zpráva obsahuje číslo logického kanálu a typ přenášené informace.
- **End Session Command** – terminál uzavírá logický kanál a zahájí ukončení hovoru.

1.2.3 Adresace v H.323

Adresace v H.323 využívá zpráv definovaných v kódu protokolu H.225.0. Procedura adresování může mít několik podob:

- **síťová adresa** – každý koncový bod sítě je identifikován IP adresou.
- **aliasová adresa** – koncový bod sítě může být specifikován jednou nebo více aliasovými adresami. Převod na IP adresy řeší gatekeeper pomocí RAS.
- **URL adresa** – URL adresa musí být sestavena podle standardního URL schématu. Skládá se ze dvou částí: ***user*** a ***hostport*** (***ras://jméno@doména:port***). [6]

1.3 Architektura SCCP (Skinny Call Control Protocol)

Cisco Systems nabízí ucelené řešení nejen pro IP telefonii, ale i ostatní multimediální přenosy, jako jsou videokonference nebo distribuce videosignálu. Celkově je koncept nazýván AVVID (Architecture for Voice Video and Integrated Data).

SCCP je proprietární protokol firmy Cisco sloužící pro komunikaci mezi Cisco CallManagerem a Cisco VoIP telefony. CallManager je software fungující jako signalizační server. Skinny klient využívá TCP/IP k přenosu a příjmu hovorů, zprávy protokolu jsou přenášeny prostřednictvím TCP na portu 2000. [5]

1.3.1 SCCP zprávy

Komunikace mezi jednotlivými stranami probíhá na principu žádosti a odpovědi. Příklad řídicích zpráv používaných protokolem SCCP ukazuje Tabulka 1.1.

Tabulka 1.1 Příklad řídicích zpráv protokolu SCCP

Code	Station Message ID Message
0x0000	Keep Alive Message
0x0001	Station Register Message
0x0002	Station IP Port Message
0x0003	Station Key Pad Button Message
0x0004	Station Enbloc Call Message

1.4 ARCHITEKTURA IAX (INTER – ASTERISK EXCHANGE)

Protokol IAX je signalizační protokol v síťových prostředích pracujících na bázi IP protokolu, který zároveň podporuje přenos dat s multimediálním obsahem. Jedná se o binárně orientovaný, otevřený protokol původně určený pro softwarovou pobočkovou ústřednu Asterisk. Veškerá signalizace probíhá nad protokolem UDP. Protokol IAX může být použit pro vzájemné propojení Asteriskových serverů nebo IAX klientů pomocí tzv. trunků. Princip trunkování spočívá ve spojení dat souběžných spojení mezi koncovými body stejného typu do jednoho paketu. Výrazně se tak sníží přenosová kapacita díky eliminaci hlaviček. IAX se odkazuje na protokol IAX2, což je druhá verze protokolu IAX. [10]

1.4.1 IAX zprávy

Zprávy protokolu IAX jsou rozděleny do dvou kategorií:

- spolehlivé,
- nespolehlivé.

Úkolem spolehlivých zpráv je zajistit signalizaci a řízení spojení, zatímco nespolehlivých je přenos multimediálních dat. Všechny druhy zpráv IAX protokolu definuje Tabulka 1.2. [10]

Tabulka 1.2 Specifikace všech druhů zpráv protokolu IAX

Typ	Popis	Popis podtřídy	Popis dat
0x01	DTMF	0 – 9, A – D, *, #	nedefinováno
0x02	audio	formát audio komprese	data
0x03	video	formát video komprese	data
0x04	řídicí	typy řídicích zpráv	mění se s typem
0x05	nulový	nedefinováno	nedefinováno
0x06	řídicí IAX	typy řídicích IAX zpráv	základní informace
0x07	text	vždy 0	nezpracovaný text
0x08	obraz	formát komprese obrazu	nezpracovaný obraz
0x09	HTML	typy HTML zpráv	specifikace zpráv
0x0A	komfortní zvuk	úroveň zvuku v decibelech	nedefinováno

1.4.2 Adresace v IAX

Adresování v IAX může být provedeno podle doporučení ITU E.164. Tuto adresu si volí účastník sám v číslovacím plánu. Další možností je použití IAX URI. Úplná syntaxe IAX URI je ve tvaru: ***iax:[uživatel@]host[:port][/číslo[?kontext]]***.

1.5 Srovnání SIP, SCCP, H.323 a IAX

Signalizační protokoly IAX, SIP (IETF), SCCP (Cisco) i protokolová sada H.323 (ITU) slouží pro navázání komunikace mezi koncovými účastníky, správu a modifikaci parametrů hovoru. Přes tyto protokoly se přenáší jak citlivé uživatelské údaje, tak informace které se týkají parametrů spojení.

Protokoly SIP a SCCP jsou textově orientovány, a tak je jejich čitelnost, zpracování a analýza jednodušší. H.323 a IAX používá zprávy kódované v binárním formátu. Jelikož je SIP podobný protokolu HTTP, lze na něj uplatnit bezpečnostní mechanismy pro HTTP. Standard H.323 má bezpečnostní mechanismy definované podle protokolu H.235. Cílem H.235 je poskytnout autentičnost, důvěrnost a integritu přenášených dat.

Struktura protokolu SIP umožňuje zapouzdření dalších protokolů, například SDP. Protokol SDP implementovaný do SIP specifikuje všechna potřebná konfigurační data. Protokoly zabezpečující signalizaci a zabezpečený přenos dat pro H.323 jsou H.245, H.225 – RAS a H.225.0 – Q.931.

Mezi výhody protokolu IAX patří podpora NAT (Network Address Translation), menší režie spojení a jednodušší použití za firewally. Za nevýhodu IAXu lze považovat jeho menší rozšířenost v hardwarových a softwarových telefonech a jeho nízkou podporu ze strany VoIP provozovatelů.

Následující tabulka (Tabulka 1.3) porovnává parametry protokolů SIP, SCCP, H.323 a IAX: [4][8][10]

Tabulka 1.3 Srovnání parametrů protokolů SIP, SCCP, H.323 a IAX

	SIP	SCCP	H.323	IAX
standard	otevřený, jednoduchý	otevřený, jednoduchý	uzavřený, složitý	otevřený, jednoduchý
organizace	IETF	Cisco	ITU	–
typ zpráv	textový	textový	binární	binární
používané servery	SIP Proxy, Redirect, Registrar	CallManager	gatekeeper	Asterisk
adresace	URI	IP adresa	IP, aliasová, URL adresa	URI, IP adresa

2 VoIP IMPLEMENTACE

Pro návrh celkového řešení VoIP síťové infrastruktury je důležitá správná volba komunikačních zařízení a softwaru. Nezbytným základem každé VoIP sítě jsou VoIP koncová zařízení a síťová infrastruktura (kabeláž a spojovací prvky – přepínače a směrovače). V praxi však přistupují další zařízení nebo softwarové moduly umožňující rozšíření funkcí a dostupnost podporovaných služeb. Mezi řídicí a zprostředkující zařízení se řadí telefonní server, konferenční jednotka a telefonní brána. Koncové body jsou zastoupeny hardwarovými či softwarovými IP telefony.

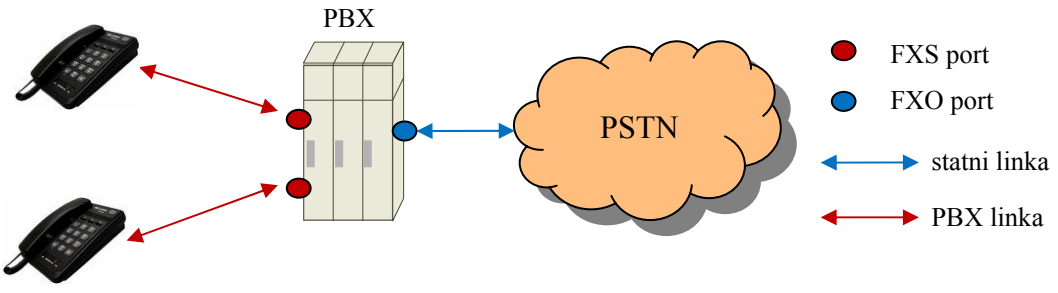
2.1 ŘÍDICÍ A ZPROSTŘEDKUJÍCÍ SYSTÉMY PRO VoIP

Kontrolu nabízených služeb a hovorů, podporu telefonních funkcí, autentizaci a autorizaci volajících a další doplňkové služby zabezpečují komunikační servery. Úlohou konferenčních jednotek je zajistit realizaci konferencí. Gatekeeper představuje řídicí prvek VoIP sítě s architekturou H.323, SIP telefonní server zase řídicí prvek architektury SIP a CallManager pro Cisco. Jejich přítomnost v síti není povinná, avšak realizace uceleného řešení jej vyžaduje. Další hardwarové vybavení, které může být součástí VoIP sítě je brána. Brána provádí všechen nezbytně nutný překlad fyzických adres a hlasovou kompresi. Hlasová brána poskytuje tyto následující funkce:

- integrace telefonů, faxů a modemů různých sítí (PSTN, ISDN,VoIP, atd.),
- kódování a dekódování hlasu v reálném čase,
- zpracování signalizačních informací.

Telefonní rozhraní analogové telefonní linky, známé jako POTS (Plain Old Telephone Service), představují dva druhy portů FXO (Foreign eXchange Office) a FXS (Foreign eXchange Subscriber). Příklad telefonních rozhraní FXO a FXS ukazuje Obrázek 2.1.

- **FXO** – port přijímá analogovou linku, očekává napájení a indikuje vyvěšení a zavěšení. Jedná se o zásuvky analogového telefonního systému, telefonu nebo faxu. Port FXO je zdrojem signálu přihlášení a odhlášení.
- **FXS** – port generuje analogovou linku předplatiteli, poskytuje napájení, generuje oznamovací tón a signalizuje vyzvánění. Jedná se o zásuvky, do kterých se připojují telefony a faxy. V IP telefonii jsou těmito porty vybaveny hlasové brány pro připojení klasických telefonů.



Obrázek 2.1 Příklad telefonního rozhraní FXO a FXS

2.2 SOFTWAROVÁ POBOČKOVÁ ÚSTŘEDNA ASTERISK

Asterisk je kompletní open source pobočková ústředna (PBX) na softwarové bázi. Ústředna operuje primárně na platformách Linux, ale lze ji použít i pod operačními systémy Mac OS X, OpenBSD, FreeBSD a Sun Solaris. Asterisk tvoří rozhraní telefonnímu hardwaru, softwaru a libovolné telefonní aplikaci. Systém podporuje protokoly SIP, H.323, IAX, MGCP, SCCP a VoFR. Asterisk vystupuje jako středový prvek mezi telefonními technologiemi a telefonními aplikacemi. Telefonní technologie zahrnují VoIP služby (SIP, H.323, IAX a MGCP brány a telefony) a tradiční TDM technologie (POTS, PSTN, ISDN BRI, atd.). Ústřednu je možno získat zdarma na www.asterisk.org. [2]

Asterisk nabízí následující základní služby:

- pobočková ústředna PBX,
- VoIP gateway (MGCP, H.323, SIP, IAX),
- softwarová ústředna,
- konferenční server,
- překlad čísel,
- interaktivní hlasový průvodce.

Asterisk jádro ovládá následující položky:

- PBX přepojování – přepojovací systém pobočkové ústředny, spojovací volání mezi různorodými uživateli,
- spouštěč aplikací – spouštění služeb jako hlasová pošta, přehrání souboru,
- překladač kodeků – používá kodeky pro kódování a dekódování zvukových kompresních formátů.

Asterisk nedělá rozdíly mezi přenosovými cestami, které využívá k vytvoření a spojení jednotlivých hovorů. Každé volání je umístěno na odlišném kanále. Operace s jedním kanálovým typem je stejná jako s ostatními kanálovými typy. Díky tomuto způsobu zacházení s kanály je Asterisk velice flexibilní PBX. [2]

2.2.1 Technologie podporované Asteriskem

Výhodou Asterisku je jeho flexibilnost a s tím související přizpůsobení novým technologiím. Asterisk v současné době podporuje všechny používané typy technologií v telekomunikacích. Rozhraní ústředny jsou rozdělena do tří skupin:

- Zaptel rozhraní,
- Non – Zaptel rozhraní,
- Packet voice protokoly.

Zaptel rozhraní – rozhraní zajišťující konektivitu ke klasické telefonní síti pracující na časovém dělení kanálů (TDM).

Non – Zaptel rozhraní – rozhraní umožňující konektivitu ke klasickým telefonním službám jako jsou například ISDN4Linux a Linux Telephony Interface.

Packet voice protokoly – jedná se o standardní protokoly pro komunikaci přes datové sítě IP (SIP, H.323, MGCP, VoFR). Asterisk nabízí i podporu vlastního komunikačního protokolu IAX2. Tato rozhraní nevyžadují specializovaný hardware.

2.2.2 Kanály Asterisku

Kanál představuje logické spojení, které Asterisk využívá k vytváření a spojování relací. Každé volání je umístěno na samotném kanále. Konfigurace kanálu se provádí v adresáři ***/etc/asterisk*** úpravou textu požadovaného konfiguračního souboru. Prostřednictvím kanálu vstupují do systému různé formáty komunikace:

- fyzické telekomunikační okruhy (FXO, FXS, PRI, BRI),
- softwarově založené spojení,
- síťově připojitelné entity (SIP, IAX),
- vnitřní kanály Asterisku (Agent, Console). [2]

Typy kanálů

Asterisk poskytuje následující typy kanálů:

- Agent,
- Console,
- H.323,
- IAX,
- MGCP,
- SIP,
- Skinny,
- atd.

2.2.3 Spuštění a základy práce s Asteriskem

Ovládání Asterisku se provádí přes příkazový řádek. Asterisk je spuštěn do CLI (Command Line Interface). Při odchodu z konzoly zůstane Asterisk běžet na pozadí. Syntaxe je následující:

```
# asterisk –g

# asterisk –r
```

Příkaz s parametrem ***g*** spouští Asterisk a parametr ***r*** zpřístupní již běžící Asterisk na pozadí daného zařízení.

Je důležité umět použít příkazy, které mají vliv na chod ústředny. Příkladem mohou být následující užitečné příkazy:

`*CLI># stop now`	ihned ukončí program,
`*CLI># restart now`	provede restart programu,
`*CLI># reload sip`	obnoví informace o nastavení konfiguračního souboru ***sip.conf***,
`*CLI># reload extensions`	obnoví informace o nastavení číslovacího plánu z konfiguračního souboru ***extensions.conf***,
`*CLI># sip/iax2 show peers`	vypíše přehled SIP/IAX2 uživatelů s aktuální IP adresou, maskou sítě a portem,
`*CLI># sip/iax2 show users`	vypíše informace o daném uživateli.

2.2.4 Instalace podpory H.323 kanálu pro Asterisk

Softwarová ústředna Asterisk je primárně podporována operačním systémem Linux. Vhodná varianta distribuce Linuxu pro instalaci H.323 podpory je Debian. Implementace je však pouze jako H.323 gateway, nikoliv jako gatekeeper. Jedná se o kanál ***oh323***, který je vydán pod licencí GNU GPL. Instalace balíčku prostřednictvím internetu je možná pomocí příkazu:

```
apt-get install oh323
```

Další varianty jsou kanály ***h323*** nebo ***ooh323***. Asterisk – ooh323 je součástí asterisk – addons balíčků. Tento svazek je vyvinut v jazyce C a obsahuje pouze kód potřebný k nastavení H.323 signalizačních kanálů.

2.3 OpenH323 Gatekeeper – The GNU Gatekeeper

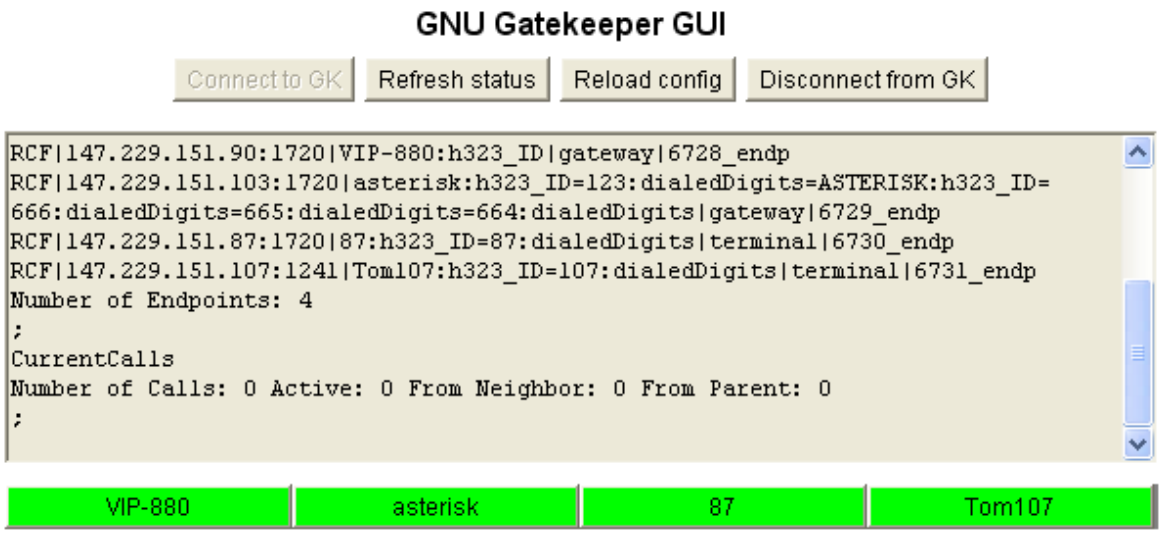
GNU Gatekeeper je plně funkční gatekeeper pro VoIP. Jedná se o stabilní open – source projekt, který nabízí řídicí služby pro koncové H.323 uživatele. Poskytuje spustitelné soubory pro Linux, Windows, FreeBSD, Solaris a MacOS. Gatekeeper je chráněn licencí GNU GPL (GNU General Public Licence), která umožňuje kopírovat, volně šířit nebo upravovat software. GNU gatekeeper nabízí následující služby:

- překlad adres,
- H.323 proxy,
- řízení hovorů,
- flexibilní směrování hovorů,
- podporu pro NAT,
- zabezpečení H.235,
- grafické uživatelské rozhraní,
- atd. [9]

2.3.1 Instalace a základy konfigurace GNU Gatekeeperu

GNU Gatekeeper je dostupný na www.gnugk.org. Konfigurace gatekeeperu se provádí změnou textu v textovém souboru ***gatekeeper.ini***. Pro znovunačtení konfigurace slouží příkaz ***Reload***. Konfigurační soubor s komentářem se nachází v příloze C. Monitoring H.323 sítě je umožněn přes telnet nebo pomocí Java appletu přes webový prohlížeč. Uživatelské rozhraní Java appletu ukazuje Obrázek 2.2. Následující příkazy pro práci s GNU Gatekeeperem se provádějí v telnetu:

`rv`	seznam aktivních registrací,
`reload`	provede reload konfigurací,
`s`	celková statistika gatekeeperu,
`cv`	seznam všech aktuálních hovorů,
`gk`	vypíše informace o gatekeeperu.



Obrázek 2.2 Java Applet pro GNU Gatekeeper

2.4 OpenH323

OpenH323 je plně H.323 kompatibilní gatekeeper dostupný na www.openh323.org. Jedná se o open – source implementaci standardu H.323. Představuje součást většiny IP systémů založených na H.323 standardu. OpenH323 nabízí následující služby:

- překlad adres,
- řízení přístupu,
- management zón,
- řízení přenosové kapacity,
- autorizace,
- videokonference,
- atd.

2.4.1 Instalace a základy konfigurace OpenH323

OpenH323 pro Linux nebo Windows společně s manuály a zdrojovým kódem lze získat na www.openh323.org/code.html. Následující příkazy se provádějí v příkazovém řádku pro Windows:

`opengk debug`	spustí soubor pro rychlé otestování,
`opengk`	provede spuštění programu a chod na pozadí,
`opengk install`	spustí konfiguraci programu a jeho chod na pozadí.

Veškerá konfigurace se provádí přes HTTP prohlížeč. Do prohlížeče se píše adresa ***http://uživatel:1719***, kde ***uživatel*** představuje IP adresu zařízení, na kterém běží gatekeeper. Po zadání hesla nabízí prohlížeč uživateli dvě položky:

- Parameter,
- Status.

V sekci ***Status*** probíhá monitoring H.323 klientů a jejich relací. Stránka se sama aktualizuje každých třicet sekund. Obrázek 2.3 ukazuje dva registrované H.323 IP telefony a současně i jejich vzájemnou komunikaci. Monitoring H.323 klientů nabízí následující parametry:

- End Point Identifier,
- Call Signal Addresses,
- Aliases,
- Application,
- Active Calls.

Monitoring relací H.323 klientů nabízí tyto parametry:

- Call Identifier,
- End Point,
- Source/Destination Signalling Address,
- Last IRR,
- Connected.

Sekce ***Parametres*** umožňuje konfiguraci gatekeeperu. Všechny důležité položky pro správnou funkci gatekeeperu jsou přednastaveny.

End Point Identifier	Call Signal Addresses	Aliases	Application	Active Calls	
47cc5c8a:1	ip$147.229.151.88:1720	147 H.323	*Name:* PA168S *Version:* 1.45 *Vendor:* 181/42	1	Unregister
47cc5c8a:2	ip$147.229.151.107:1044	Tom107 107	*Name:* SJ Labs□ SJphone *Version:* 1.65.377a *Vendor:* 0/0	1	Unregister

Call Identifier	End Point	Source/Destination Signalling Addresse	Last IRR	Connected	
7fc00428-23fc-214d-b515-6048eb4b1e24	47cc5c8a:1	10#@ip$147.229.151.107:1060 147@ip$147.229.151.88:1720	21:17:05		Clear
7fc00428-23fc-214d-b515-6048eb4b1e24	47cc5c8a:2	107@ip$147.229.151.107:1038 147@ip$147.229.151.88:1720	21:17:04		Clear

Obrázek 2.3 OpenH323 gatekeeper se zaregistrovanými IP telefony

2.5 H.323 HARDWAROVÉ ŘÍDICÍ SYSTÉMY

Při realizaci praktické části byly také zprovozněny hardwarové ústředny a brány. Systémy sloužily pro doplnění VoIP sítě o analogovou telefonní síť.

2.5.1 H.323 hlasová ústředna

K praktickému odzkoušení byla použita H.323 telefonní ústředna IPX – 1000 (Obrázek 2.4), produkt společnosti Planet. Jedná se o plně funkční analogovou telefonní ústřednu, bránu pro realizaci volání po internetu, ochranný firewall pro připojení k internetu a 100Mbit/s přepínač. IPX – 1000 mimo jiné nabízí čtyři pobočkové linky FXS, dvě linky FXO a čtyřikrát LAN 10/100Mbps. Více informací o telefonní ústředně lze nalézt na www.planet.com.tw/news/productnews/IPX-1000.htm.

Obrázek 2.4 IPX-1000, VIP-880

2.5.2 H.323 gateway

VIP – 880 (Obrázek 2.4) je osmiportová brána pro snadné umožnění VoIP volání. Poskytuje připojit do FXO portů čtyři vnější linky nebo připojit se na stávající ústřednu. Nabízí další čtyři porty pro běžné telefonní přístroje. Brána umožňuje vytvořit síť pro neomezený počet účastníků a slouží pro vstup do běžné lokální telefonní sítě. Zařízení podporuje protokoly SIP a H.323, přičemž uživatel provádí volbu vybraného standardu. Umožňuje spolupráci s H.323 gatekeeperem nebo SIP Proxy serverem v síti. Detailní popis produktu se nachází na www.planet.com.tw/news/productnews/VIP-880_882_880FO.htm.

2.6 CISCO CALLMANAGER

Softwarová telefonní ústředna CallManager je základním prvkem IP telefonie systému Cisco, využívající především signalizační protokol SCCP. Jedná se o řídicí aplikaci běžící na serverovém počítači s operačním systémem Windows nebo Linux. Jeden server Cisco CallManager dokáže obsloužit až 2500 IP telefonů umístěných na libovolném místě IP sítě. CallManager funguje pouze jako signalizační server, samotný hovor je po síti spojen vždy nejkratší cestou přímo mezi koncovými zařízeními (dvěma telefony nebo telefonem a hlasovou bránou). CallManager servery mohou být sdruženy do clusteru až o pěti členech, který pak slouží pro rozložení zátěže a zálohování výpadku. CallManager lze vzdáleně ovládat přes webové rozhraní (Obrázek 2.5), což umožňuje spravování systému z kteréhokoli počítače v síti. Cisco CallManager zabezpečuje:

- konfiguraci a správu IP telefonů,
- řízení hovorů,
- správa číslovacího plánu,
- správa uživatelů,
- atd. [12] [13]

2.6.1 Základy konfigurace CallManageru

Konfigurace systému se provádí v administrační části prostřednictvím webového rozhraní. V internetovém prohlížeči se napíše následující adresa pro spuštění uživatelského rozhraní: ***http://<IP_Adresa_CallManageru>/CCMAdmin/***. Základní nastavení vlastností CallManageru se provádí v sekci ***System***. Číslovací plán systému lze nakonfigurovat v oddíle ***Route Plan***. Sekce ***Service*** umožňuje nastavení různých parametrů služeb pro vybrané servery. Oddíl ***Feature*** nabízí konfiguraci nadstandardních vlastností. Příkladem může být nastavení mobility zařízení. V oddíle ***Device*** lze přidat a konfigurovat nové zařízení jako jsou telefony, gatekeepery, brány a trunky (SIP, H.323). Přidání nového uživatele a jeho práv lze provést v záložce ***User***. Instalace a konfigurace Plug – in se nachází v ***Application***.

Obrázek 2.5 Webové rozhraní aplikace Cisco CallManager

2.7 VoIP TERMINÁLY

Z pohledu uživatele jsou nejvýznamnější koncové body označované jako terminály. Terminálem pro VoIP je IP telefon. Existuje několik řešení VoIP telefonu v datových sítích:

- **hardwarový telefon** – speciální zařízení připomínající klasický telefon, avšak s odlišným technickým vybavením přizpůsobeným do datových sítí. V přístroji je implementována protokolová sada TCP/IP, dále H.323, SCCP nebo SIP a audio kodeky. Pro správnou funkci telefonu bývá nedílnou součástí softwarová výbava umožňující dálkový dohled a konfiguraci a download aktuálního firmware. [1]
- **softwarový telefon** – představuje speciální aplikaci podporující alespoň jeden z protokolů SIP, H.323, IAX, atd. Program může být instalován na počítač a fungovat jako IP telefon. Nutnou výbavou počítače je zvuková karta. Softwarové IP telefony mohou podporovat i přenos videa. Výhodou softwarových telefonů je jejich cenová dostupnost. [1]

2.7.1 Vybrané hardwarové IP telefony

VIP–101T (H.323)

VIP – 101T (Obrázek 2.6) je zařízení s přímou podporou přenosu hlasu po IP sítích standardem H.323. Jedná se o IP telefon od společnosti Planet. Telefonní přístroj je nezávislý na operačních systémech počítačů a pro konfiguraci není zapotřebí speciálního softwaru. VIP – 101T podporuje konfiguraci IP adresy staticky a dynamicky pomocí DHCP. Vzdálená administrace se provádí přes telnet nebo prohlížeč web. Více informací o IP telefonu se nachází na www.planet.com.tw/product/product_dm.php?product_id=192&menu_id=3.

NT–320 VoIP telefon (H.323)

Zcomax NT – 320 je VoIP telefon splňující standardy SIP, H.323, MGCP a Net2phone. Telefon podporuje DHCP pro připojení přes LAN nebo kabelový modem. Nastavení telefonu je možné provést přes webové rozhraní nebo přes telnet. Více informací o telefonu se nachází na www.zcomax.cz/Nt3202.aspx. IP telefon zachycuje Obrázek 2.6.

Obrázek 2.6 VIP-101T, NT-320 VoIP telefon

VIP – 155PT (SIP)

Telefonní přístroj společnosti Planet s přímou podporou standardu SIP (Obrázek 2.7). Podporuje konfiguraci IP adresy jak staticky, tak dynamicky pomocí DHCP. Telefon podporuje SIP Proxy a umožňuje autorizaci vůči SIP Proxy. Vzdálený management přístroje se provádí přes webový prohlížeč nebo telnet, lokální management přes klávesnici a menu na LCD displeji. Informace o zařízení se nacházejí na www.planet.com.tw/news/productnews/VIP-155PT.htm.

VIP – 153T (SIP)

IP telefon VIP – 153T (Obrázek 2.7) společnosti Planet podporuje protokol SIP pro přenos hlasu po síti. Pomocí protokolu DHCP se konfiguruje statická, případně dynamická IP adresa. Vzdálená správa se provádí přes webový prohlížeč nebo telnet a lokální pomocí klávesnice. Implementovanou vlastností pro přenos hlasu po SIP je podpora SIP Proxy.
Další popis IP telefonu se nachází na www.planet.com.tw/news/productnews/VIP-153PT.htm.

Obrázek 2.7 VIP-153T, VIP-155PT

Cisco IP Phone 7960 (SCCP)

Telefon Cisco IP Phone 7960 (Obrázek 2.8) je IP telefon druhé generace s komplexní funkční výbavou. Telefon podporuje protokol SCCP a je kompatibilní s H.323 a Microsoft NetMeeting. Telefon je vybaven Ethernetovým switchem pro připojení počítače, telefon i PC tak sdílí jednu datovou zásuvku. IP telefon nabízí softwarová programovatelná tlačítka a umožňuje provozování XML aplikací. Více informací o telefonu Cisco IP Phone 7960 se nachází na http://www.cisco.com/en/US/products/hw/phones/ps379/ps1855/index.html.

Obrázek 2.8 Cisco IP Phone 7960

2.7.2 Porovnání hardwarových IP telefonů

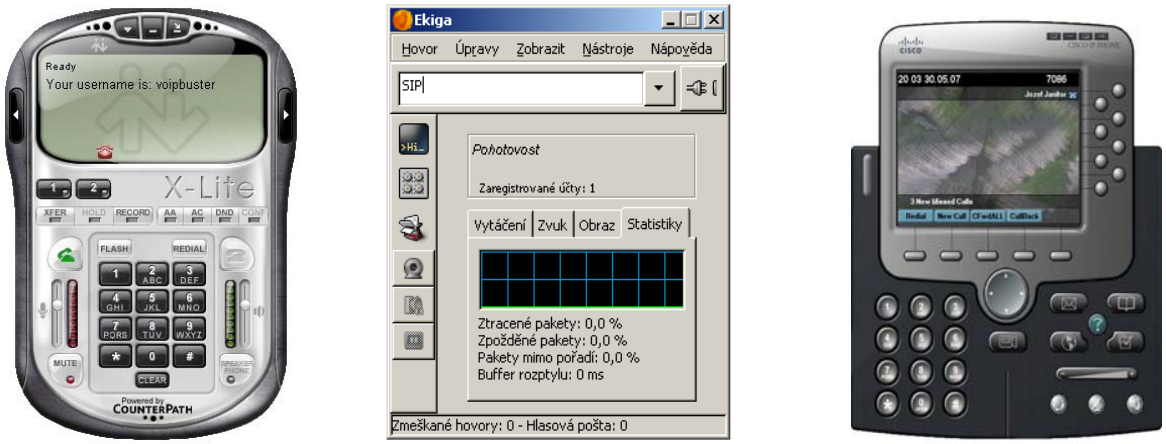
Společnost Planet nabízí pro VoIP telefony řady VIP – 150 (VIP – 155PT a VIP – 153T) podporující protokol SIP. Telefon VIP – 101T je zaměřen pouze na protokol H.323. Nejflexibilnější je telefon Zcomax NT – 320, který je kompatibilní jak se SIP, tak i s H.323. Cisco IP Phone 7960 podporuje proprietární signalizační protokol firmy Cisco, a to protokol SCCP. U Cisco IP telefonu 7960 lze provést konverzi z protokolu SCCP na SIP. Instalační a konfigurační proces konverze umožňuje příslušný TFTP server. Vzdálená správa telefonů se provádí přes webový prohlížeč nebo telnet a lokální pomocí klávesnice. Přístroje nabízejí širokou sadu funkcí, které mohou být doplňovány pomocí upgradu programového vybavení.

2.7.3 Vybrané softwarové IP telefony

Jsou zde zmíněni zástupci z prostředí SIP, H.323 a Cisco. Seznam dalších softwarových telefonů se nachází na www.voip-info.org.

X–Lite (SIP)

X – Lite je produktem CounterPath. Pro řízení spojení využívá protokol SIP. Tento SIP User Agent běží pod operačními systémy Microsoft Windows, MAC OS, PocketPC a Linux. Volná verze produktu je na stránce www.xten.com. Uživatelské rozhraní programu představuje Obrázek 2.9. Instalace této aplikace je jednoduchá a uživatelské rozhraní a menu je srozumitelné. Program X – Lite nabízí mnoho funkcí, jako jsou tři linky na volání, přidržení hovoru, paměť přijatých i volaných čísel, adresář, zkrácené vytáčení, automatické odmítnutí i přijetí příchozích hovorů, přesměrování hovoru, atd.



Obrázek 2.9 Uživatelské rozhraní X – Lite, Ekiga a Cisco IP Communicator

Ekiga (H.323)

Jedná se o open source komunikační program pro VoIP. Je kompatibilní s protokoly SIP a H.323 a podporuje videohovory. Běží pod platformami Linux, Microsoft Windows, MAC OS a OpenSolaris. Ekiga obsahuje podporu STUN za účelem hladkého provozu za routery a firewally. Ekiga nabízí podobné funkce jako X – Lite. Download programu je možný na www.ekiga.org. Uživatelské rozhraní ukazuje Obrázek 2.9.

Cisco IP Communicator (SCCP)

Cisco IP Communicator je softwarová aplikace podporující protokol SCCP a SIP. Běží pod platformou Microsoft Windows. Vizuálně je tato aplikace podobná IP telefonu Cisco 7960 (Obrázek 2.9) a nabízí uživateli stejné funkce. Kromě obvyklých funkcí umožňuje telefon dynamické ovládání hovoru prostřednictvím softwarových tlačítek nebo možnost videokonference. Více informací o telefonu se nachází na www.cisco.com.

2.7.4 Porovnání softwarových IP telefonů

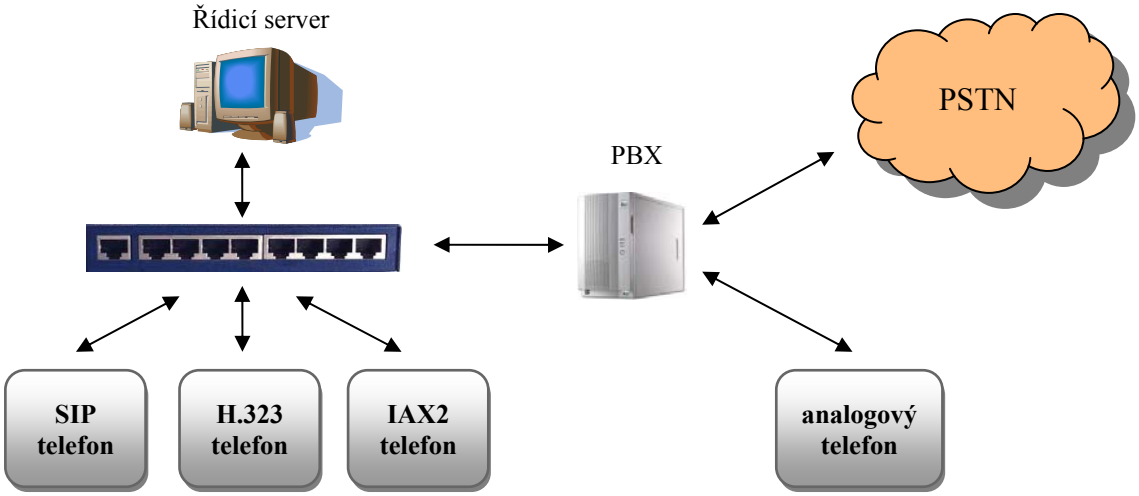
X – Lite, Ekiga i Cisco IP Communicator jsou kvalitní IP telefony pro internetové telefonování. X – Lite pro řízení spojení využívá protokol SIP, zatímco Ekiga je kompatibilní se SIP i H.323 a Cisco IP Communicator je kompatibilní s SCCP a SIP. Nástroje mohou ve spojení s některým ze SIP operátorů sloužit jako plnohodnotná náhrada pevné linky. Softwarové telefony nabízí mnoho využitelných funkcí včetně videokonference. U IP telefonu X – Lite je uživatelské rozhraní srozumitelnější a jednodušší než u programu Ekiga. Výhodou programu Cisco IP Communicator je podobnost s hardwarovým telefonem Cisco IP Phone 7960.

3 NÁVRH VOIP SÍTĚ

Každý hlasový systém je třeba před samotnou realizací dobře navrhnout s ohledem na mnoho faktorů. Důležitým faktorem je návratnost investice. IP telefonie nabízí nemalé úspory spojené s telefonními poplatky a správou systému, ale není to pravidlem. Stávající telefonní infrastruktura musí být také brána v úvahu. V neposlední řadě je kladen důraz na kvalitu zprostředkujících prvků sítě a na podporu kvalitativních požadavků (QoS) ze strany technologie VoIP. Cílem je tedy navrhnout a v laboratorních podmínkách zrealizovat požadované řešení VoIP ústředny. Logickou topologii systému obsahující různé typy IP telefonů s možností připojení k PSTN znázorňuje Obrázek 3.1.

Při návrhu byly stanoveny následující požadavky:

- připojení dostatečného množství IP telefonů (SIP, H.323, SCCP, IAX2),
- podpora starších analogových telefonů,
- podpora komunikačních standardů,
- volání na základě číslovacího plánu,
- flexibilita ústředny a případný upgrade firmware,
- možnost propojení více ústředen,
- vysoká stabilita a funkčnost ústředny.



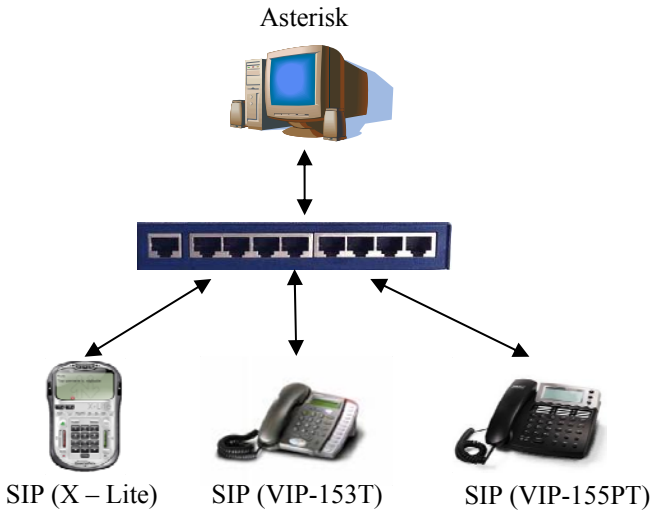
Obrázek 3.1 Příklad logické topologie VoIP sítě

3.1 REALIZACE EXPERIMENTÁLNÍCH PRACOVIŠŤ JEDNOTLIVÝCH ARCHITEKTUR

Vytvořit fungující systém využívající VoIP technologie a nabízející možnosti telefonování podobné klasické telefonní síti není až tak jednoduché. Pozornost je věnována struktuře celého komunikačního systému v rámci jedné architektury. Při realizaci experimentálního pracoviště je návrh IP sítě omezen prostředky, které jsou v laboratoři k dispozici. Při realizaci komunikačních systémů je kladen důraz na vyladění a konfiguraci pro možnost dlouhodobého využití (například pro účely laboratorních cvičení).

3.1.1 Implementace IP řešení pro SIP

Samotná implementace IP řešení pro SIP vede k pochopení principu ústředny Asterisk. Jednou z možností, jak do sítě začlenit ústřednu Asterisk, ukazuje Obrázek 3.2. Pro realizaci a zprovoznění experimentálního pracoviště byly vybrány výše zmíněné zařízení. Hardwarovými zástupci IP telefonů pro SIP jsou VIP – 153T a VIP – 155PT a softwarový IP telefon X – Lite. Softwarová pobočková ústředna běží pod operačním systémem Fedora.



Obrázek 3.2 Implementace IP řešení pro SIP

Konfigurace Asterisku

Nakonfigurování Asterisku spočívá v úpravě textu konfiguračních souborů. Definice uživatelských účtů se provádí v adresáři ***/etc/asterisk***. Klienti jsou definováni v příslušném typu konfiguračního souboru. V případě kanálu SIP je jím ***sip.conf***. Jedná se o konfigurační soubor se seznamem uživatelů, kteří s Asteriskem komunikují prostřednictvím SIP.

Dalším důležitým krokem je definice příkazů v souboru ***extensions.conf***, které řídí způsob ovládání a směrování příchozích a odchozích relací.

Konfigurace klientů Asterisku

Příklad nastavení konfiguračního souboru ***sip.conf*** pro koncové zařízení využívající protokol SIP:

```
[general]                       ;definice hlavních voleb
port=5060                       ;nastavení portu
disallow=all                    ;zakázání všech audio kodeků
allow=alaw                      ;povolení audio kodeku

[XLite]                         ;definice uživatele XLite
type=friend                     ;uživatel může volat i přijímat hovory
context=SIPskupina              ;jméno context pro tohoto uživatele
callerid=jmeno                  ;jméno zobrazující se volanému
host=dynamic                    ;dynamické přidělení IP adresy
nat=no                          ;uživatel se nenachází za NATem
secret=heslo                    ;pro zabezpečenou registraci klientů
qualify=yes                     ;kontrola stavu uživatele
```

Definice uživatelů komunikujících s Asteriskem prostřednictvím jiného typu kanálu je obdobná. Například zápis IAX klientů se provádí v souboru ***iax.conf*** umístěném v ***/etc/asterisk.***

Konfigurace extension

Definice jednotlivé extension obsahuje jeden nebo více příkazů určených k provedení. Každý příkaz je uveden na samostatném řádku v následujícím formátu: ***exten=>extension,priorita,příkaz***.

Charakteristika jednotlivých parametrů je následující:

- **extension** – číselné nebo alfanumerické vyjádření extension,
- **priorita** – určuje pořadí pro vykonání příkazů příslušející k dané extension,
- **příkaz** – název prováděného příkazu.

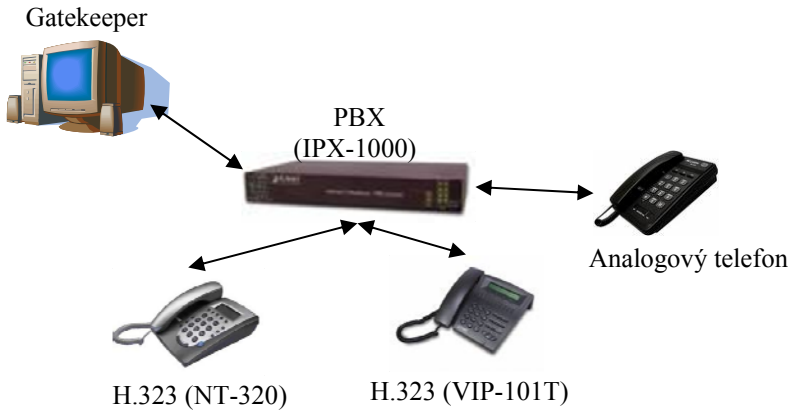
Jednoduchý příklad nastavení konfiguračního souboru ***extensions.conf***:

```
[general]                          ;definice hlavních voleb

[SIPskupina]                       ;jméno context
exten=>123,1,Dial(SIP/XLite)       ;definice extension
```

Pokud Asterisk obdrží informaci o vytočení účastnického čísla 123, pak s nejvyšší prioritou provede příkaz pro vytvoření spojení s uživatelem XLite. Podrobný popis konfigurace Asterisku se nachází na www.voip-info.org/wiki.

3.1.2 Implementace IP řešení pro H.323

Topologie H.323 sítě experimentálního pracoviště vychází ze dvou hlavních komponent – gatekeeper a terminál. Gatekeeper je jedna z nejdůležitějších komponent H.323 infrastruktury. Protože Asterisk neumožňuje funkci gatekeeperu, je pro odzkoušení spuštěn GNU Gatekeeper. Zástupci hardwarových IP telefonů pro H.323 síť jsou NT – 320 a VIP – 101T. Dále je využito hlasové ústředny IPX – 1000. Ústředna umožňuje připojit čtyři IP telefony H.323, čtyři stávající analogové telefony a připojení pevné telefonní linky PSTN. Topologii H.323 sítě ukazuje Obrázek 3.3.



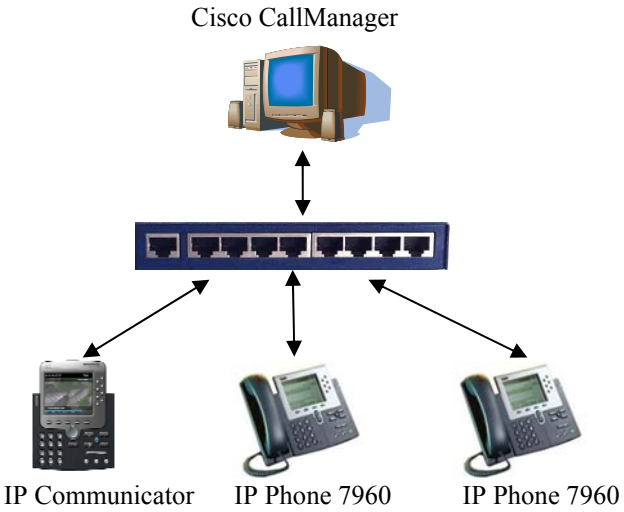
Obrázek 3.3 Implementace IP řešení pro H.323

Konfigurace gatekeeperu

Po instalaci GNU gatekeeperu je program zcela připraven plnit funkci gatekeeperu. Další možné nakonfigurování gatekeeperu spočívá ve změně souboru ***gatekeeper.ini***. Jedno z možných nastavení se nachází v příloze C. Signalizační zprávy mohou být přenášeny dvěma způsoby. První metodou je Direct Endpoint Call Signalling. V tomto případě jsou zprávy přenášeny přímo mezi jednotlivými koncovými body. Druhou metodou je Gatekeeper Routed Call Signalling. Při použití této metody jsou jednotlivé zprávy směrovány přes gatekeeper.

3.1.3 Implementace IP řešení pro Cisco

Vytvořený telefonní systém se skládá z jednoho Cisco CallManageru, který představuje řídicí komunikační server. Dále ze dvou hardwarových telefonů Cisco IP Phone 7960 a jednoho softwarového zástupce Cisco IP Communicator. Topologii stabilního a funkčního systému Cisco ukazuje Obrázek 3.4.



Obrázek 3.4 Implementace IP řešení pro Cisco

Konfigurace CallManageru

Konfigurace Cisco CallManageru (kapitola 2.6.1) se provádí pomocí webového rozhraní na adrese ***http://<IP_Adresa_CallManageru>/CCMAdmin/***.

Před vytvořením nového uživatele je vhodné začlenit nové komunikační zařízení, jako jsou například Cisco IP telefony, do systému. Prvním způsobem je automatická registrace komunikačního zařízení, kdy je CallManager nastaven na automatické připojení zařízení do sítě. V menu ***System → Cisco Unified CallManager*** se vybere požadovaný CallManager a v části ***Auto – registration Information*** musí být vyplněna políčka ***Starting Directory Number*** a ***Ending Directory Number***. Zde se nastavuje rozsah telefonních čísel určených pro autoregistraci. Druhým způsobem je přidání komunikačního zařízení do sítě manuálně. Manuální registrace se prování v menu ***Device → Phone → Add a New Phone***. Po vybrání typu telefonu následuje zadání MAC adresy telefonu a telefonního čísla.

Pro vytvoření nového uživatele je nutné spustit menu ***User → Add a New User***. V aplikaci CallManager je integrována adresářová služba DC Directory. Tato služba poskytuje a spravuje databázi uživatelských účtů. Po nastavení jména, hesla a telefonního čísla se přiřazuje vlastní komunikační zařízení tohoto uživatele (***Device Association***). Uživatel může konfigurovat svůj uživatelský účet, a to prostřednictvím webového rozhraní na adrese ***http://<IP_Adresa_CallManageru>/CCMUser/***. Po přihlášení do uživatelského rozhraní CallManager serveru, je potřeba vybrat komunikační zařízení, které se bude konfigurovat. Není však povolena veškerá konfigurace, je možné nastavit přesměrování hovorů, rychlou volbu, vlastní adresář, heslo atd. Nastavení se potvrdí stisknutím tlačítka ***Update***.

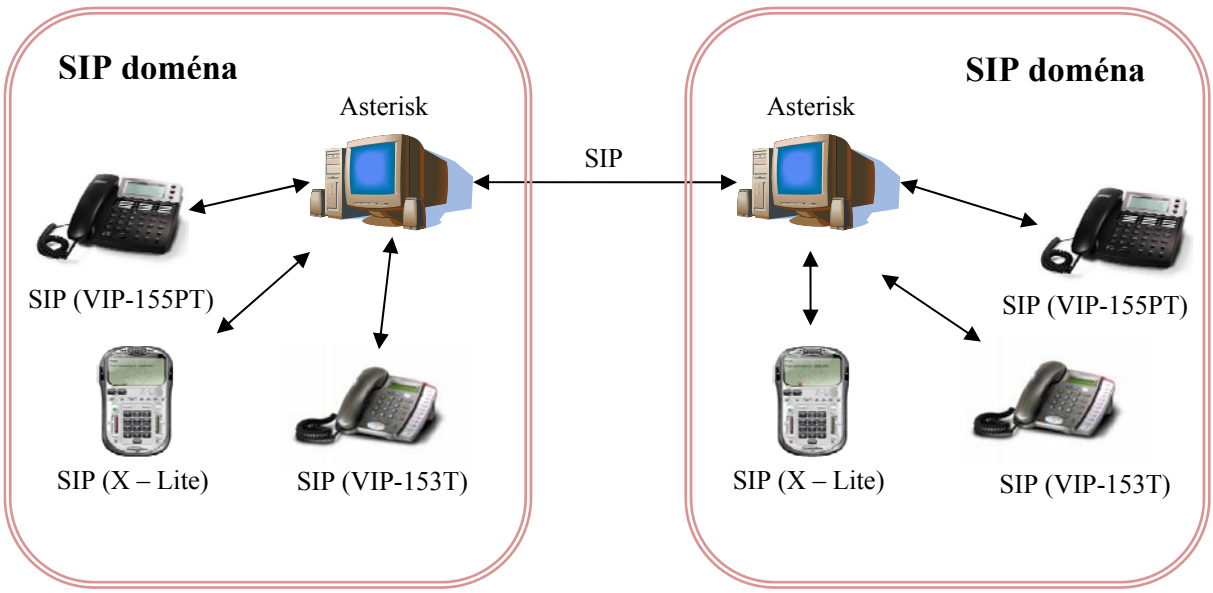
3.2 REALIZACE EXPERIMENTÁLNÍCH PRACOVIŠŤ KONVERGOVANÝCH ŘEŠENÍ

IP architektury představují ústřednové řešení, kde spojovací jádro je tvořeno datovou sítí s protokolovou sadou TCP/IP a komunikačními servery. Pro řízení a směrování volání se do sítě řadí tzv. komunikační server. Server zároveň zajišťuje předcházení kolizím, a tedy i co nejmenší výsledné zpoždění. Zařízení pracující například s protokolem SIP mohou pracovat se zařízeními pracujícími s protokolem H.323 také pomocí brány SIP/H.323. Tato brána převádí signalizační zprávy obou protokolů. Softwarová pobočková ústředna Asterisk, GNU Gatekeeper i Cisco CallManager implementují funkci brány. Jejich kombinace vede k účelnému využívání nabízených výhod a představuje tak konvergovaná řešení těchto architektur. IP telefonie od společnosti Cisco nabízí kromě systému Cisco CallManager pro realizaci hlasových služeb i další systémy a možnosti pro zvýšení komfortu uživatele. Jelikož všechny tři architektury používají pro vlastní přenos multimediálních dat obvykle protokol RTP, mohou koncoví uživatelé po navázání spojení komunikovat přímo. Podobně mohou komunikovat koncové body SIP, H.323 nebo Cisco s telefony v síti PSTN.

3.3 PROPOJENÍ DVOU SIP DOMÉN S ŘÍDICÍM PRVKEM ASTERISK

Softwarová ústředna Asterisk lze také nakonfigurovat pro propojení s jinými ústřednami Asterisk. Trunk představuje spojení mezi dvěma ústřednami, ať už se jedná o jedinou linku nebo více linek.

Nejvýhodnější řešení pro propojení dvou ústředen Asterisk je pomocí protokolu SIP. Asterisk dokáže pracovat i jako SIP klient. Konfigurace kanálu se provádí modifikací souboru ***sip.conf*** v adresáři ***/etc/asterisk***. Příklad zapojení sítě dvou Asterisků ukazuje Obrázek 3.5. Diagram spojení uživatelů přes SIP kanál ukazuje Obrázek 4.19. Druhý způsob představuje propojení dvou ústředen pomocí proprietárního protokolu IAX2. Výhodou protokolu je možnost vytvoření trunku při více hovorech vedených zároveň mezi dvěma body a tím ušetřit přenosovou kapacitu.



Obrázek 3.5 Logická topologie VoIP sítě se dvěma Asterisky

3.3.1 Konfigurace SIP kanálu pro propojení dvou Asterisků

Pro možnost propojení dvou ústředen Asterisk je nutná modifikace konfiguračních souborů ***sip.conf***. Na obou stranách se definují noví uživatelé, pomocí kterých budou ústředny vzájemně komunikovat. Pro ústřednu Asterisk1 je definován uživatel asterisk2, který slouží k propojení ústředny Asterisk2 k ústředně Asterisk1. Příklad nastavení konfiguračního souboru ***sip.conf*** na ústředně Asterisk1:

```
[general]                              ;definice hlavních voleb
autokill=yes                           ;zabránění přerušení hovoru pokud
                                       nedojde k potvrzení paketů do 2 sekund

register=>asterisk1:heslo@<IP_adresa_Asterisk2>

[asterisk2]
type=friend                            ;uživatel může volat i přijímat hovory
host=<IP_adresa_Asterisk2>             ;IP adresa serveru Asterisk2
secret=heslo
context=incoming_Asterisk
trunk=yes                              ;pro úsporu přenosové kapacity
```

Příklad nastavení konfiguračního souboru ***sip.conf*** na ústředně Asterisk2:

```
[general]                              ;definice hlavních voleb
autokill=yes                           ;zabránění přerušení hovoru pokud
                                       nedojde k potvrzení paketů do 2 sekund

register=>asterisk2:heslo@<IP_adresa_Asterisk1>

[asterisk1]
type=friend                            ;uživatel může volat i přijímat hovory
host=<IP_adresa_Asterisk1>             ;IP adresa serveru Asterisk1
secret=heslo
context=incoming_Asterisk
trunk=yes                              ;pro úsporu přenosové kapacity
```

Prostřednictvím dialplanu (***extensions.conf***) se provádí směrování z jedné ústředny na druhou. Příklad nastavení konfiguračního souboru ***extensions.conf***:

```
[incoming_Asterisk]                        ;jméno context
exten=>124,1,Dial(SIP/XLite)
```

Na tomto příkladu je předvedeno přesměrování hovoru na druhou ústřednu při příchozím volání čísla 124.

3.3.2 Konfigurace IAX kanálu pro propojení dvou Asterisků

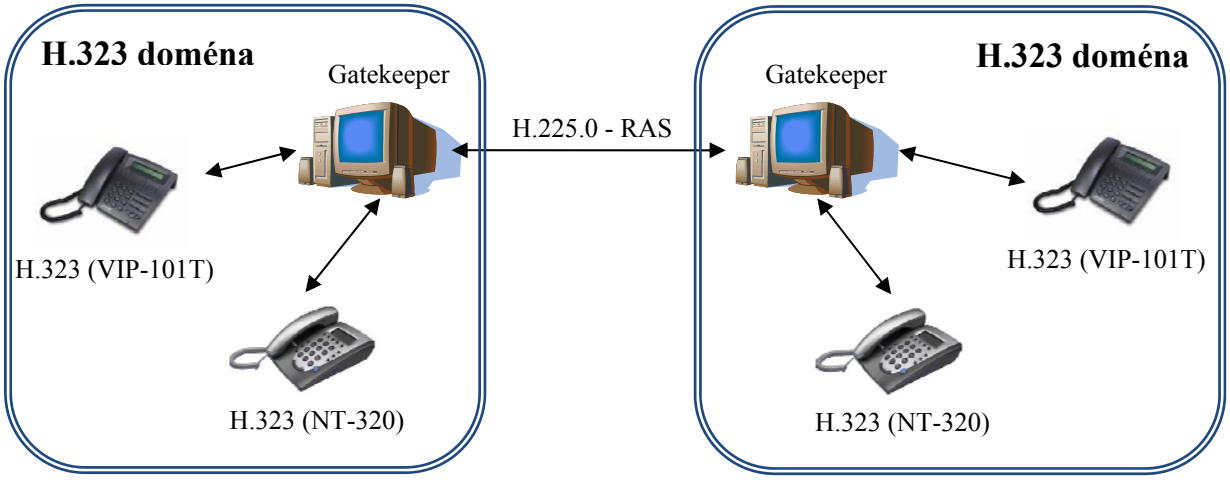
Další možný způsob pro vytvoření trunku je pomocí protokolu IAX2. Jedná se o vnitřní protokol Asterisku, který podporuje vzájemnou kompatibilitu ústředen. Konfigurace souboru ***iax.conf*** je podobná s předchozím příkladem konfigurace souboru ***sip.conf***. Při správné konfiguraci není nutná vzájemná registrace ústředen. Příklad nastavení konfiguračního souboru ***extensions.conf***:

```
[incoming_Asterisk]                        ;jméno context
exten=>_1XX,1,Dial(IAX2/asterisk1:heslo@<IP_adresa_Asterisk2>/${EXTEN})
```

Na tomto příkladu je předvedeno přesměrování hovoru na druhou ústřednu prostřednictvím IAX kanálu bez registrace ústředen.

3.4 PROPOJENÍ DVOU H.323 DOMÉN S ŘÍDICÍM PRVKEM GNU GATEKEEPER

Pro propojení dvou H.323 sítí je nejvýhodnější použít GNU Gatekeeper. Příklad zapojení sítě se dvěma gatekeepery ukazuje Obrázek 3.6. Diagram sestaveného spojení ukazuje Obrázek 4.20.



Obrázek 3.6 Logická topologie VoIP sítě se dvěma gatekeepery

3.4.1 Konfigurace GNU Gatekeeperů pro propojení dvou H.323 domén

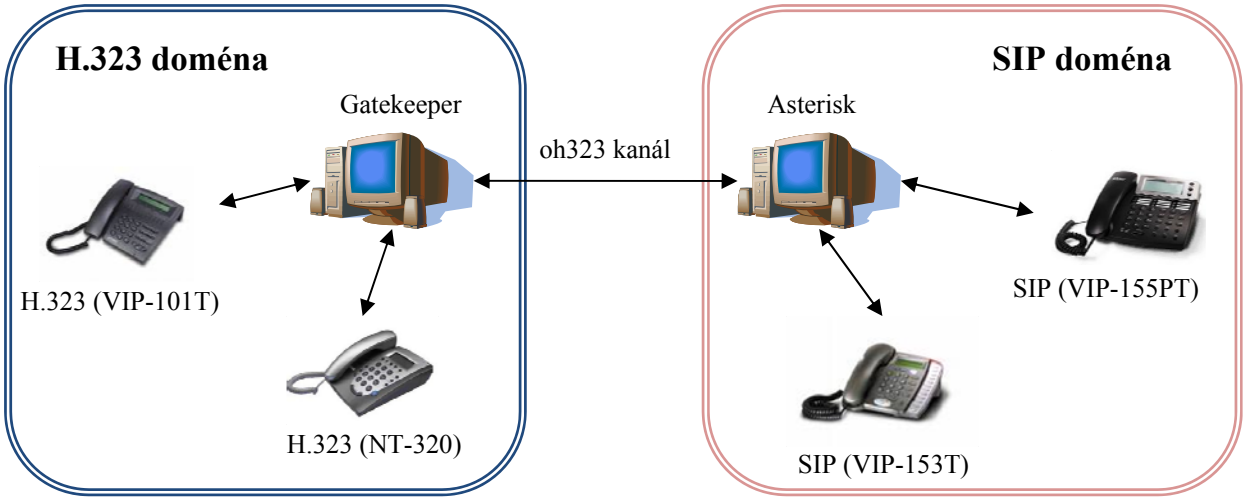
Následuje příklad nastavení konfiguračního souboru ***gatekeeper.ini*** pro propojení dvou H.323 domén. Po požadované změně je důležité provést reload. Konfigurace gatekeeperu GK1 jako souseda gatekeeperu GK2 vypadá následovně:

```
[Gatekeeper::Main]
FortyTwo=42                          ;zjištění přítomnosti konfig. souboru
Name=GK1                             ;identifikace gatekeeperu
Home=<IP_adresa_gatekeeper1>         ;IP adresa gatekeeperu
TimeToLive=300                       ;nastavení limitu pro registraci

[GkStatus::Auth]                     ;definice pravidel
rule=allow                           ;povolení jakéhokoli připojení
<IP_adresa_gatekeeper1>=allow ;pro možnost monitorování

[RoutedMode]
GKRouted=1                           ;mód směrování signalizace
H245Routed=0                         ;přenášení zpráv H.245 přes gatekeeper

[RasSrv::Neighbors]                  ;definice sousedů
GK2=GnuGk

[Neighbor::GK2]                      ;konfigurace souseda
GatekeeperIdentifier=GK2             ;identifikátor
Host=<IP_adresa_gatekeeper2>         ;nastavení IP adresy serveru
SendPrefixes=*                       ;prefixy vysílané gatekeeperem
AcceptPrefixes=*                     ;prefixy akceptované gatekeeperem

[RasSrv::LRQFeatures]                ;definice LRQ
NeighborTimeout=2                    ;nastavení časového limitu
```

Nastavení druhého gatekeeperu je inverzní, takže se zamění pouze IP adresa a identifikátory.

3.5 Propojení SIP a H.323 domén pomocí Asterisku a GNU Gatekeeperu

IP architektura je ústřednové řešení, kde ústřednou pro síť SIP je Asterisk a pro síť H.323 je GNU Gatekeeper. GNU Gatekeeper je využíván ve funkci gatekeeperu potřebného pro kontrolu H.323 kanálu v softwarové ústředně Asterisk. Nevýhodou tohoto spojení jsou velké zpoždění a nižší stupeň spolehlivosti sítě díky serverům, na jejichž bezproblémovém chodu závisí funkčnost celé sítě. Logickou topologii sítě využívající jak gatekeeperu, tak SIP Proxy serveru ukazuje Obrázek 3.7. Typické využití zpráv protokolem H.323 a SIP potřebných k sestavení, řízení a ukončení spojení znázorňuje Obrázek 4.18.



Obrázek 3.7 Propojení domén SIP a H.323 prostřednictvím oh323 kanálu

3.5.1 Konfigurace kanálu oh323 ústředny Asterisk

Pro možnost propojení dvou různých standardů, jako jsou SIP a H.323 prostřednictvím Asterisku, je dodatečně nutné instalovat podporu pro H.323. Implementace je však pouze jako H.323 gateway, nikoliv jako gatekeeper. Vhodnou variantou je kanál ***oh323***. Konfigurace souboru ***oh323*** spočívá v modifikaci textu souboru ***oh323.conf*** v adresáři ***/etc/asterisk***.

Příklad nastavení konfiguračního souboru ***oh323.conf***:

```
[general]                              ;definice hlavních voleb
listenport=1720                        ;nastavení portu
tcpStart=10000                         ;rozsah TCP portů používaných H.323
tcpEnd=20000
udpStart=10000                         ;rozsah UDP portů používaných H.323
udpEnd=20000

outboundMax=10                         ;maximální počet odchozích spojení
inboundMax=10                          ;maximální počet příchozích spojení
simultaneousMax=10                     ;maximální počet současných spojení

gatekeeper=<IP_adresa_gatekeeper>      ;IP adresa GNU Gatekeeperu
gatekeeperTTL=600                      ;nastavení timeout pro registraci
context=h323                           ;nastavení kontextu pro H.323 volání

[register]                             ;konfigurace aliasů a prefixů
context=h323
gwprefix=00                            ;prexix volený z H.323 terminálu
```

Příklad nastavení konfiguračního souboru ***extensions.conf***:

```
[sip]                                   ;pro kontext sip
exten=>_87,1,Dial(OH323/87,30)
exten=>_87,2,Hangup()
```

Volbou čísla 87 je s nejvyšší prioritou vytočen účastník 87 pomocí oh323 kanálu. Pokud volaný neodpoví, tak po třiceti sekundách dojde k zavěšení hovoru.

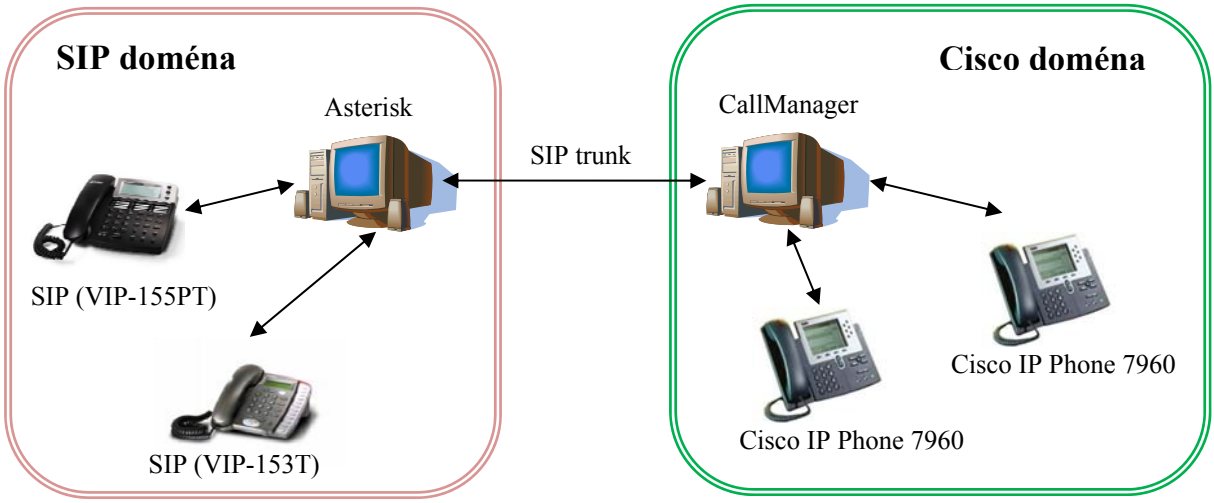
3.5.2 Konfigurace GNU Gatekeeperu pro propojení se SIP doménou

Konfigurace gatekeeperu se provádí změnou textu v textovém souboru ***gatekeeper.ini***. Po požadované změně je důležité provést reload. Nastavení umožňující přihlášení libovolného terminálu se nachází v příloze 0. Pro propojení s doménou SIP je konfigurace souboru následující:

```
[RasSrv::Neighbors]                     ;směrování
GK1=asterisk

[Neighbor::GK1]                         ;konfigurace souseda
GatekeeperIdentifier=GK1                ;identifikátor
Host=<IP_adresa_Asterisk>               ;nastavení IP adresy serveru
SendPrefixes=*                          ;prefixy akceptované Asteriskem
AcceptPrefixes=*                        ;prefixy akceptované gatekeeperem
```

3.6 Propojení Cisco a SIP domén pomocí CallManageru a Asterisku

Jedná se o ústřednové řešení, kde ústřednou pro síť Cisco je CallManager a pro síť SIP je Asterisk. Domény jsou mezi sebou spojeny pomocí SIP trunku. Logickou topologii sítě využívající jak Asterisku, tak CallManager serveru ukazuje Obrázek 3.8. Diagram spojení domény Cisco a SIP ukazuje Obrázek 4.22.



Obrázek 3.8 Propojení domén Cisco a SIP prostřednictvím SIP trunku

3.6.1 Konfigurace CallManageru pro spojení se SIP doménou

Na adrese ***http://<IP_Adresa_CallManageru>/CCMAdmin/*** je zvoleno menu ***Device → Trunk → Add a New Trunk*** za účelem zřízení nového trunku. V sekci ***Trunk type*** se vybere možnost ***SIP Trunk*** a ***Device Protocol*** je ***SIP***. Po zadání IP adresy Asterisku a jména trunku se zvolí možnost ***UDP*** protokolu jako ***Outgoing Transport Type***. Dalším krokem je konfigurace Asterisku pro spojení s doménou Cisco.

3.6.2 Konfigurace Asterisku pro spojení s doménou Cisco

Na Asterisk serveru v souboru ***sip.conf*** se vytvoří nový účet pro Cisco CallManager.

```
[callman]                       ;definice uživatele pro CallManager
type=friend                     ;uživatel může volat i přijímat hovory
context=cisco                   ;jméno context pro tohoto uživatele
host=<IP_adresa_CallMan>        ;nastavení IP adresy CallManageru
secret=heslo                    ;pro zabezpečenou registraci
disallow=all                    ;zakázání všech audio kodeků
allow=alaw                      ;povolení audio kodeku
allow=ulaw                      ;povolení audio kodeku
nat=no                          ;uživatel není za NATem
canreinvite=yes                 ;povolení vysílání zpráv INVITE
qualify=yes                     ;kontrola stavu uživatele
```

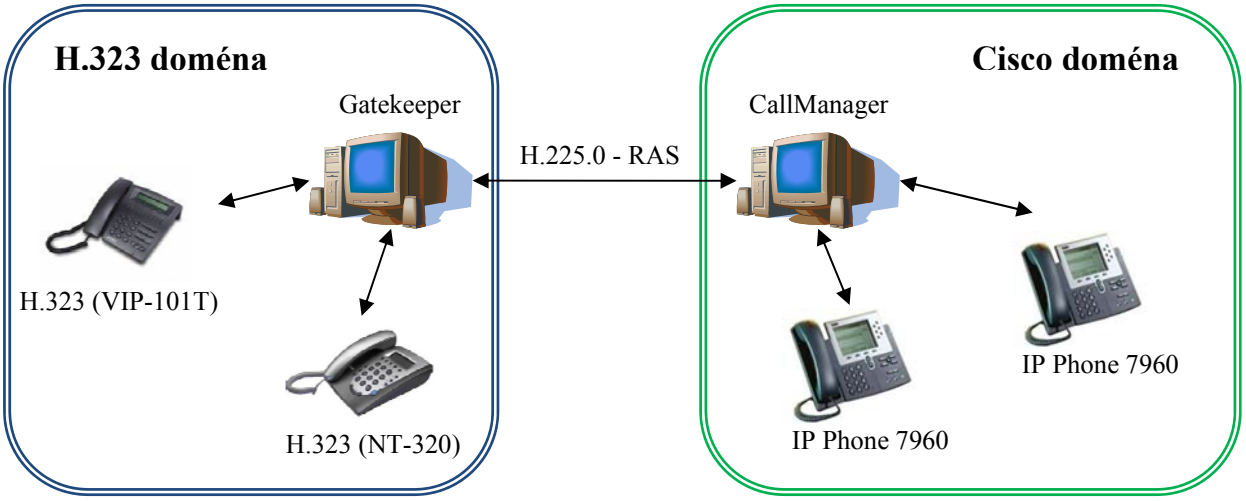
Příklad nastavení konfiguračního souboru ***extensions.conf***:

```
[cisco]                                 ;pro kontext cisco
exten=>_2000,1,Dial(SIP/callman/2000,30)
exten=>_2000,2,Hangup()
```

Volbou čísla 2000 je s nejvyšší prioritou vytočen Cisco účastník 2000 pomocí SIP kanálu. Pokud volaný neodpoví, tak dojde po třiceti sekundách k zavěšení hovoru.

3.7 Propojení Cisco a H.323 domén pomocí CallManageru a GNU Gatekeeperu

IP architektura je opět ústřednové řešení, kde ústřednou pro síť Cisco je CallManager a pro síť H.323 je GNU Gatekeeper. Jednotlivé domény jsou mezi sebou spojeny pomocí trunku H.225.0 – RAS. Každý Cisco CallManager může registrovat jeden nebo více gatekeeperů. Logickou topologii sítě využívající jak gatekeeperu, tak CallManager serveru ukazuje Obrázek 3.9. Diagram spojení domén Cisco a H.323 ukazuje Obrázek 4.21.



Obrázek 3.9 Propojení domén Cisco a H.323 prostřednictvím trunku H.225.0 - RAS

3.7.1 Konfigurace CallManageru pro spojení s H.323 doménou

Konfigurace Cisco CallManageru spočívá ve dvou krocích, přidání nového gatekeeperu a přidání nového trunku.

Na adrese ***http://<IP_Adresa_CallManageru>/CCMAdmin/*** se zvolí menu ***Device → Gatekeeper*** za účelem zřízení nového gatekeeperu. Po zadání IP adresy a časových limitů je možné povolit gatekeeperu kontrolu nad vzniklým spojením. Dalším krokem je přidání nového trunku. To se provádí v sekci ***Device → Trunk → Add a New Trunk***. Jako typ trunku se zvolí ***H.225.0 Trunk*** a protokol zařízení ***H.225.0***. Dále je možné nastavit jméno trunku a vlastnosti příchozích a odchozích hovorů. V oddíle ***Gatekeeper Information*** je pro správnou funkci trunku nutné vybrat požadovaný gatekeeper.

3.7.2 Konfigurace GNU Gatekeeperu pro spojení s doménou Cisco

Konfigurace souboru ***gatekeeper.ini*** je popsána v příloze C. Pro propojení s doménou Cisco je konfigurace souboru následující:

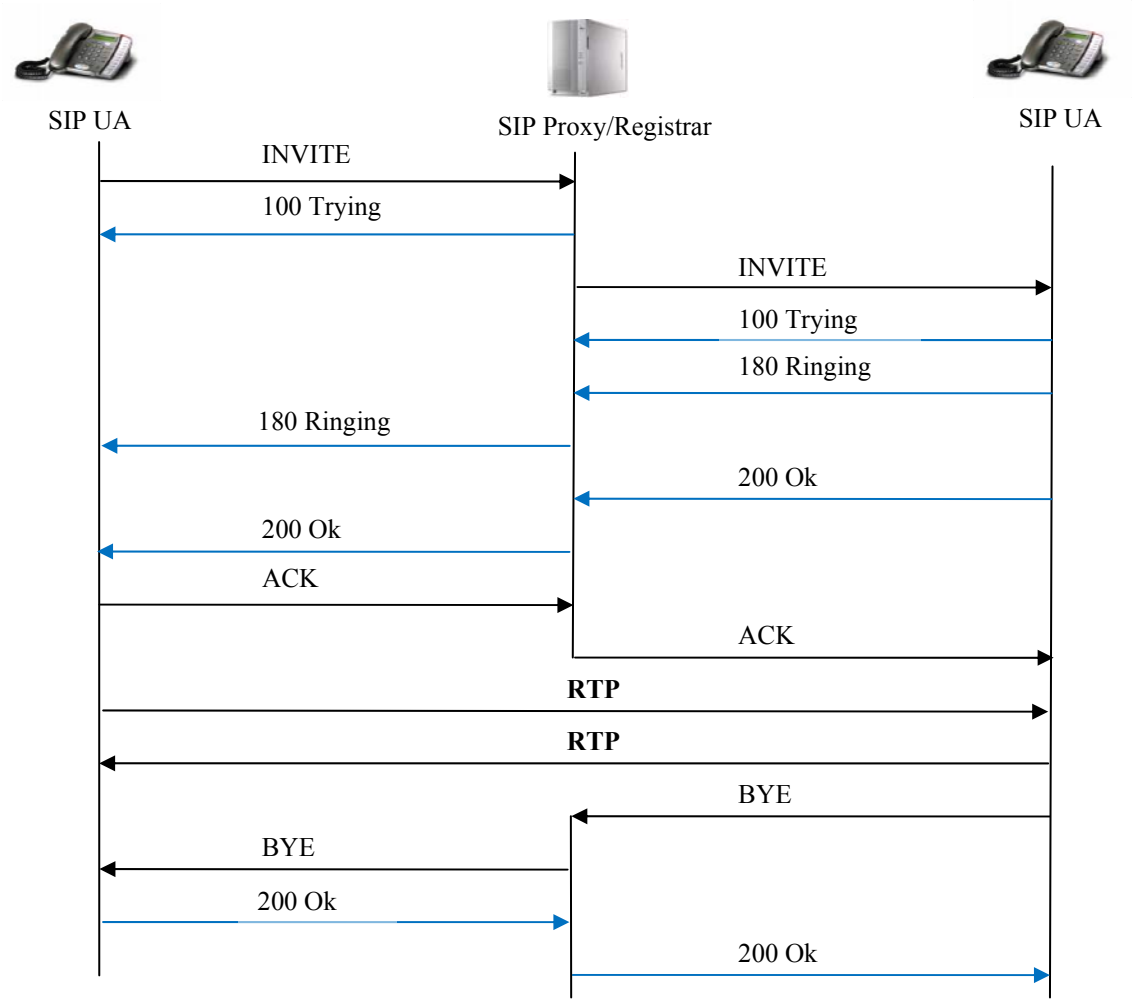
```
[RasSrv::Neighbors]                    ;definice sousedů
GK3=CiscoGk

[Neighbor::GK3]                        ;konfigurace souseda
Host=<IP_adresa_CallManager>           ;nastavení IP adresy serveru
SendPrefixes=*                         ;prefixy vysílané gatekeeperem
AcceptPrefixes=*                       ;prefixy akceptované gatekeeperem
```

4 ANALÝZA KOMUNIKACE PŘI REALIZACI SPOJENÍ

Pro podrobnou analýzu komunikace jsou použity protokolové analyzátory Observer a Wireshark. Programy slouží k důkladnému sledování a k analýze veškeré síťové komunikace. Wireshark i Observer dokáží analyzovat jak komunikaci v reálném čase, tak vyhodnocovat uložené logy. Podávají přehledný výpis detailních informací o jednotlivých paketech. Program Wireshark lze získat zdarma na www.wireshark.org/download.html.

4.1 SIGNALIZACE SIP

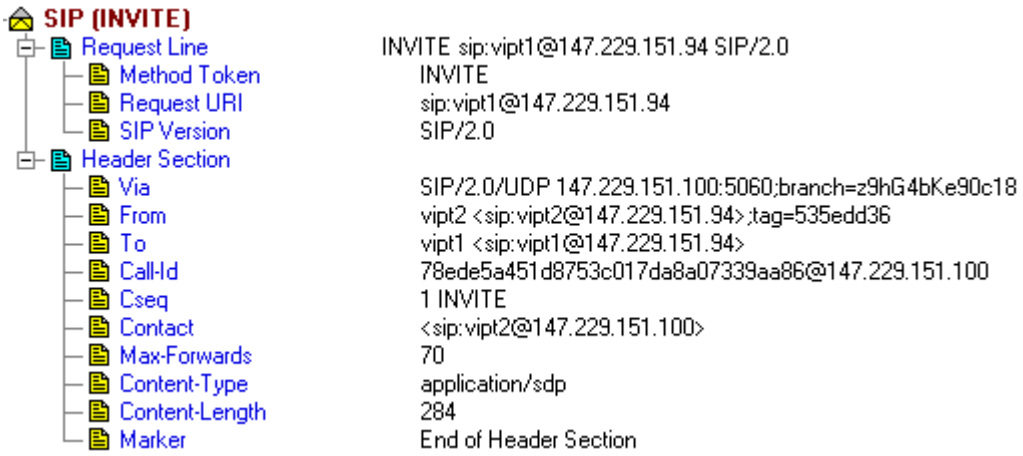
Textová podstata protokolu SIP umožňuje jednodušší protokolovou analýzu. Zpráva nesená SIP protokolem je tvořena hlavičkou a vlastním tělem zprávy. Obrázek 4.1 znázorňuje příklad diagramu spojení SIP uživatelů pomocí SIP Proxy (Asterisk).



Obrázek 4.1 Diagram spojení SIP uživatelů přes SIP Proxy

4.1.1 Zahájení spojení

Navázání spojení mezi SIP účastníky se děje prostřednictvím ústředny Asterisk. Volající účastník má k dispozici SIP adresu volaného, ale tato adresa nevypovídá o jeho lokalizaci. Volající koncový bod odesílá žádost o navázání spojení INVATE na proxy server. Zpráva INVITE je přeposílána z jednoho proxy serveru na druhý, dokud nedojde k identifikaci volaného účastníka. Příklad zprávy INVITE ukazuje Obrázek 4.2.



Obrázek 4.2 Tělo zprávy INVITE detekované programem Observer

Pole nesoucí žádost INVITE protokolu SIP:

INVITE	sip:Request URI SIP/2.0
Via:	SIP/2.0/UDP IP adresa serveru:port
From:	”jméno” <sip:jméno@doména:port>
To:	<sip:jméno@doména:port>
Contact:	<sip:jméno@IP adresa>
Call-ID:	identifikátor@IP adresa
Cseq:	identifikátor INVITE
User-Agent:	User Agent Server
Date:	datum
Allow:	pole podporovaných metod
Content-Type:	specifikace vnitřního protokolu
Content-Length:	délka těla v bajtech
Marker:	konec hlavičky

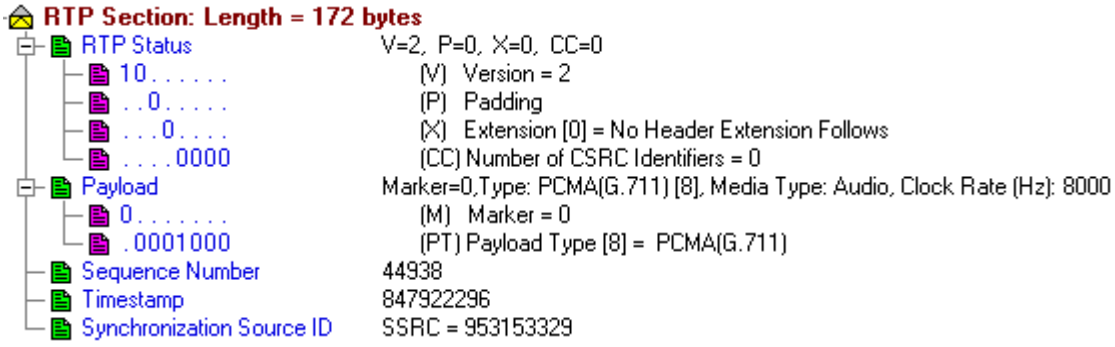
Uvnitř zprávy protokolu SIP pro navázání spojení je zapouzdřena zpráva jiného protokolu, který specifikuje použitá kódování pro multimediální data, jejich parametry a čísla portů, na kterých mají být data vysílána nebo přijímána. Obvykle je pro tento účel použit protokol SDP (Session Description Protocol), který je rovněž textový. Nejčastěji je používán ve zprávě INVITE a odpovědi na ni. Příklad těla zprávy protokolu SDP ukazuje Obrázek C. 5.

Pole nesoucí žádost INVITE protokolu SDP:

v:	číslo verze (SIP nedefinuje)
o:	identifikace zdroje žádosti o spojení
s:	jméno spojení
c:	typ spojení
t:	čas spojení (SIP nedefinuje)
m:	typ přenášených dat (typ, port, RTP/AVP profil)
a:	atributy spojení (profil, kodek)

4.1.2 Průběh spojení

Vlastní přenos multimediálních dat je realizován s využitím protokolů RTP (Real – time Transport Protocol), RTCP (Real – time Transport Control Protocol) a nepotvrzovaným přenosovým mechanismem UDP. Protokoly však neredukují celkové zpoždění dat, ani negarantují QoS (Quality of Service). Protokol RTP zajišťuje pružnost a je navržen tak, aby byl oddělen přenos uživatelských dat od řídicích funkcí. Příklad RTP paketu znázorňuje Obrázek 4.3.



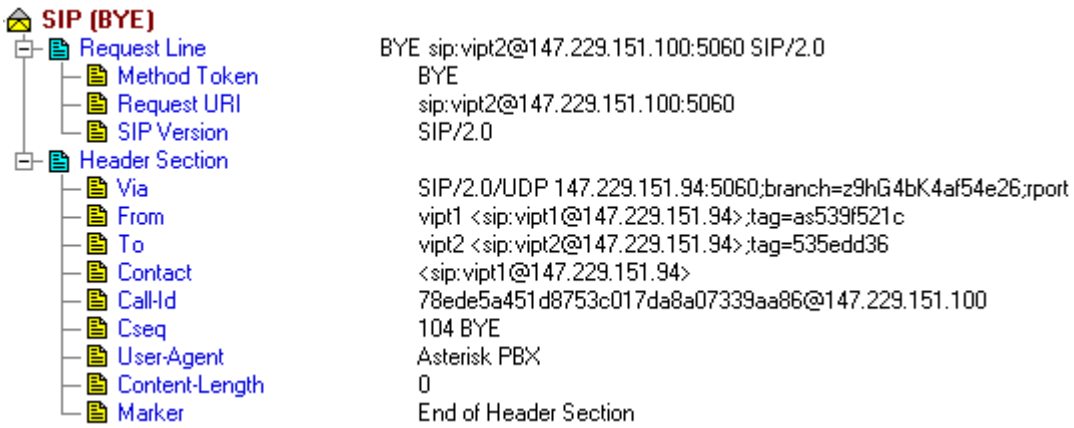
Obrázek 4.3 Tělo RTP paketu detekované programem Observer

Pole nesoucí parametry protokolu RTP:

V (Version):	verze protokolu
P (Padding):	informace o přidání výplně
X (eXtension):	rozšiřovací bit
M (Marker):	bit pro hlasovou a video komunikaci
Payload type:	kódovací metoda pro audio/video
Sequence Number:	pořadové číslo datového segmentu
Timestamp:	časová značka
Synchronization S. ID:	číslo jednoznačně identifikující zdroj

4.1.3 Ukončení spojení

Spojení je ukončeno odesláním žádosti BYE v dialogu zahájeného zprávou INVITE. Účastník spojení, který zavěsí, odesílá zprávu BYE a protistrana posílá odpověď 200 OK, kterou potvrzuje zprávu BYE a spojení je ukončeno. Zprávu BYE ukazuje Obrázek 4.4.



Obrázek 4.4 Tělo zprávy BYE detekované programem Observer

4.2 SIGNALIZACE H.323

Standard H.323 je zastřešující standard, kterému jsou podřazeny následující protokoly:

- protokoly zajišťující signalizaci a zabezpečený přenos dat (H.225.0 – RAS, H.225.0 – Q.931, H.245, H.450, H.235),
- protokoly pro přenos multimediálních dat (RTP, RTCP).

4.2.1 Zahájení spojení

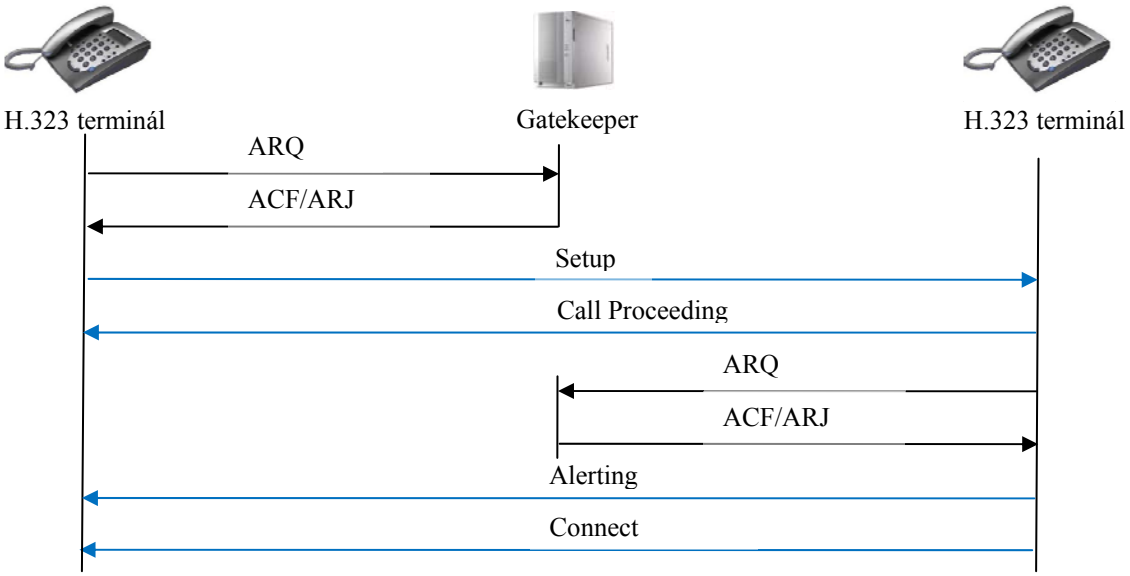
Následuje analýza zahájení spojení dvou H.323 telefonů, které jsou úspěšně zaregistrovány u GNU Gatekeeperu. Existují dva modely navázání hovorové signalizace:

- přímá signalizace (direct call signalling),
- směrová signalizace (routed call signalling).

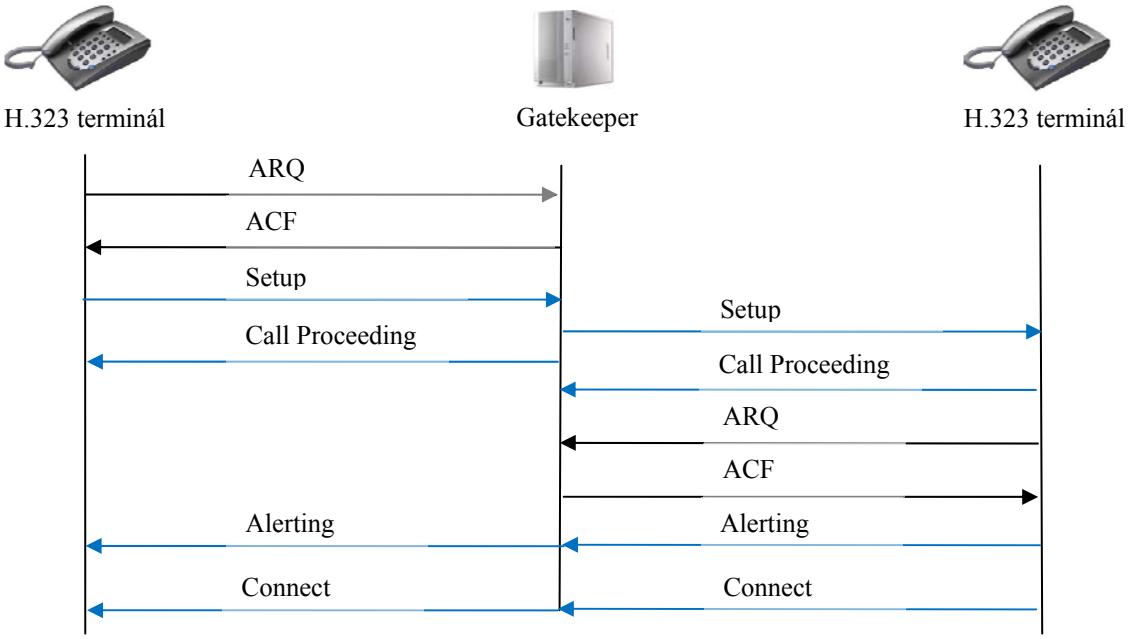
Pokud gatekeeper zvolí metodu přímého volání (Obrázek 4.5), pak volající terminál iniciuje signalizační spojení přímo s volaným terminálem. V případě směrového volání (Obrázek 4.6) je signalizační spojení nejprve navázáno s gatekeeperem, a ten následně naváže druhé spojení s volaným terminálem. V tomto režimu má gatekeeper větší kontrolu nad průběhem hovoru.

Pro komunikaci terminál – gatekeeper a gatekeeper – gatekeeper využívá standard H.323 protokolu H.225.0 označované jako H.225.0 – RAS (Registration, Admission, Status). Protokol obsahuje zprávy určené pro registraci koncového H.323 uživatele na gatekeeperu, sestavení, udržování a ukončení relace. Zprávy protokolu H.225.0 – RAS se přenášejí prostřednictvím protokolu UDP. Typické zahájení (Obrázek 4.5) hovoru s využitím přímé signalizace vypadá následovně:

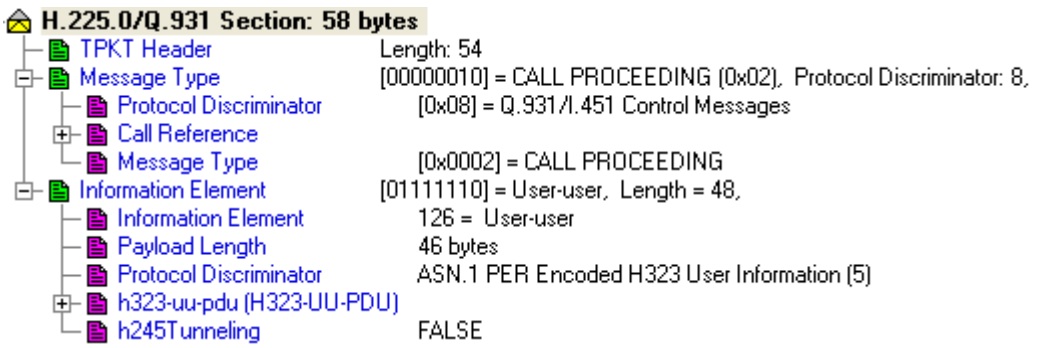
1. Volající terminál zasílá gatekeeperu žádost o povolení hovoru (ARQ – Admission Request) přes RAS kanál.
2. Gatekeeper posílá potvrzení žádosti o spojení ve zprávě ACF (Admission Confirm) zpět volajícímu terminálu. Odmítnutí žádosti je v podobě zprávy ARJ (Admission Reject).
3. Pomocí protokolu H.225.0 – Q.931 vysílá volající terminál zprávu nutnou k domluvě parametrů spojení (Setup).
4. Volaný terminál odpovídá zprávou Call Proceeding (Obrázek 4.7) o zpracování žádosti.
5. Nyní se musí volaný terminál dotázat gatekeeperu o povolení hovoru zprávou ARQ.
6. Gatekeeper potvrzuje žádost o spojení (ACF).
7. Po úspěšném přijetí potvrzení vysílá volaný terminál zprávu o vyzvánění (Alerting).
8. Spojení je zahájeno vysláním zprávy Connect.



Obrázek 4.5 Diagram zahájení spojení H.323 uživatelů registrovaných ke gatekeeperu s využitím přímé signalizace



Obrázek 4.6 Diagram zahájení spojení H.323 uživatelů registrovaných ke gatekeeperu s využitím směrování

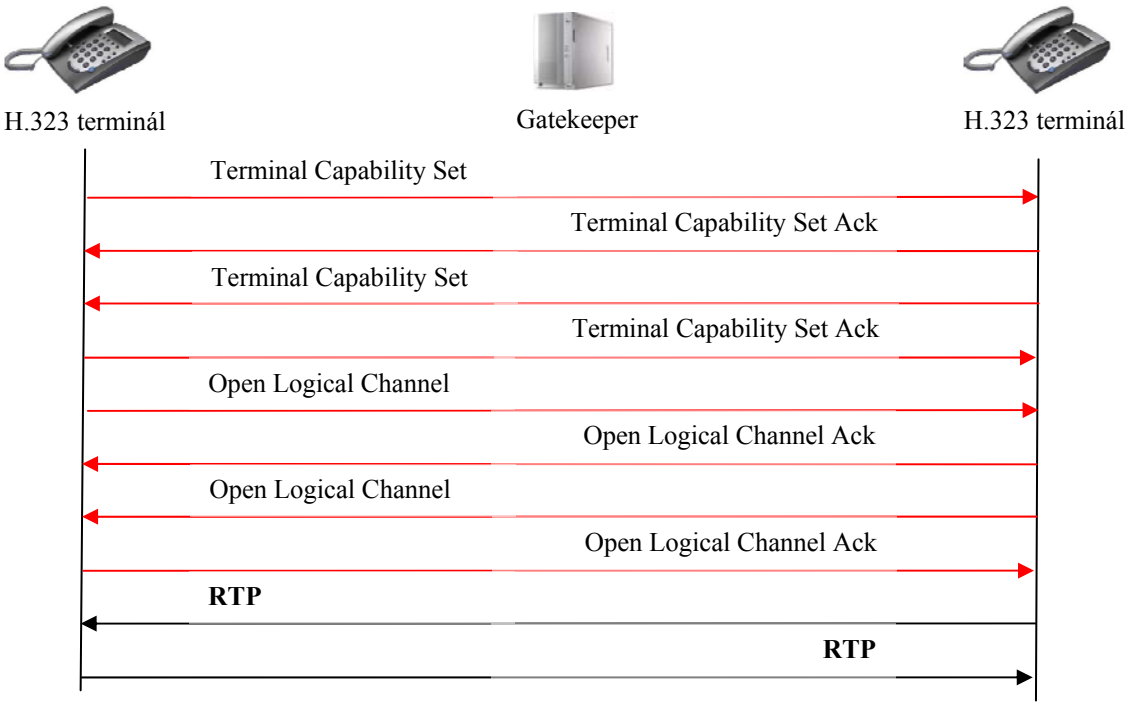


Obrázek 4.7 Tělo zprávy Call Proceeding detekované programem Observer

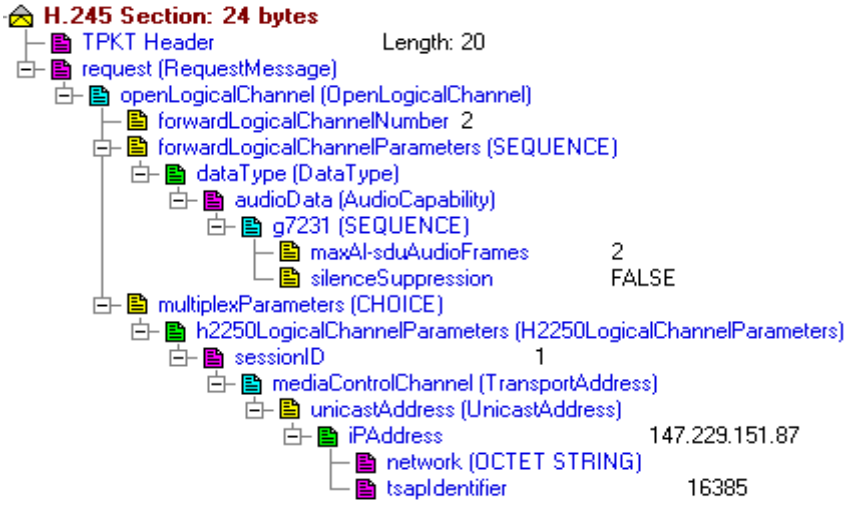
4.2.2 Průběh spojení

Po sestavení spojení následuje fáze nastavování komunikačních parametrů (vytváření logických kanálů), která je řešena pomocí signalizace mezi multimediálními koncovými zařízeními a zabezpečuje ji protokol H.245. Pro přenos multimediálních dat v reálném čase slouží protokol RTP, popřípadě RTCP. Pro videokonferenci se používá video kodek H.263. Průběh H.323 spojení ukazuje Obrázek 4.8. Průběh H.323 spojení vypadá následovně:

1. Dochází k vytvoření řídicího kanálu mezi terminály. Pomocí zprávy Terminal Capability Set protokolu H.245 si terminály mezi sebou vymění informace o způsobilosti přijímat nebo vysílat.
2. Následuje otevření mediálního kanálu prostřednictvím zprávy Open Logical Channel (Obrázek 4.9).
3. Vlastní přenos multimediálních dat zprostředkovává protokol RTP na UDP. K řízení relace a sledování kvality toku slouží protokol RTCP.



Obrázek 4.8 Diagram průběhu spojení H.323 uživatelů registrovaných ke gatekeeperu

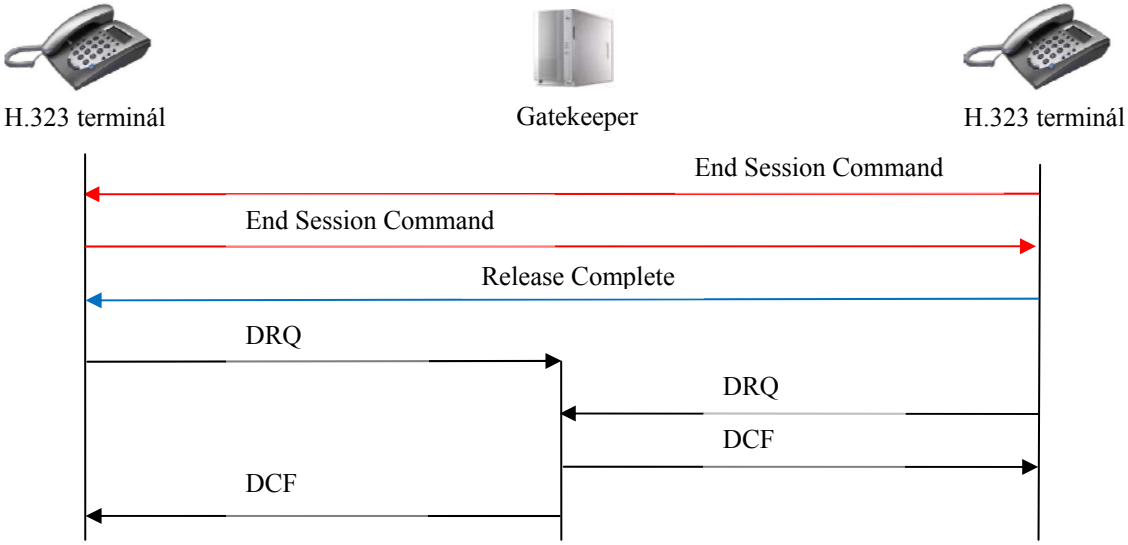


Obrázek 4.9 Tělo zprávy Open Logical Channel detekované programem Observer

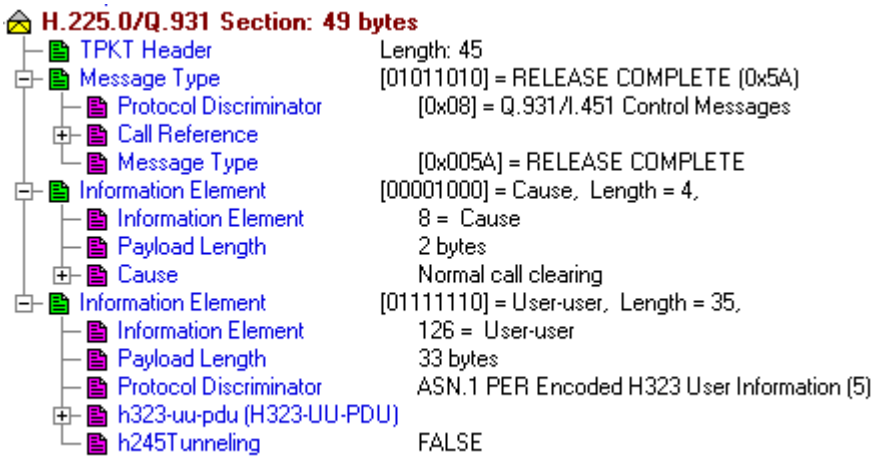
4.2.3 Ukončení spojení

Pro ukončení spojení (Obrázek 4.10) v H.323 síti se zpravidla využívá třech protokolů. Jedná se o protokoly H.225.0 – RAS, H.225.0 – Q.931 a H.245. Typické ukončení hovoru vypadá následovně:

1. Nejprve dochází k ukončení signalizačního spojení mezi koncovými body. Jeden z terminálů iniciuje ukončení spojení. Vysílá zprávu End Session Command druhému terminálu.
2. Protistrana potvrdí požadavek o ukončení spojení vysláním zprávy End Session Command.
3. První terminál dokončí spojení mezi koncovými body zprávou Release Complete (Obrázek 4.11).
4. Následuje ukončení signalizačního spojení koncových bodů s gatekeeperem. Oba terminály požádají gatekeeper o uvolnění prostřednictvím zprávy DRQ.
5. Gatekeeper uvolní oba koncové body a vyšle zprávu o potvrzení DCF.



Obrázek 4.10 Diagram ukončení spojení H.323 uživatelů registrovaných ke gatekeeperu



Obrázek 4.11 Tělo zprávy Release Complete detekované programem Observer

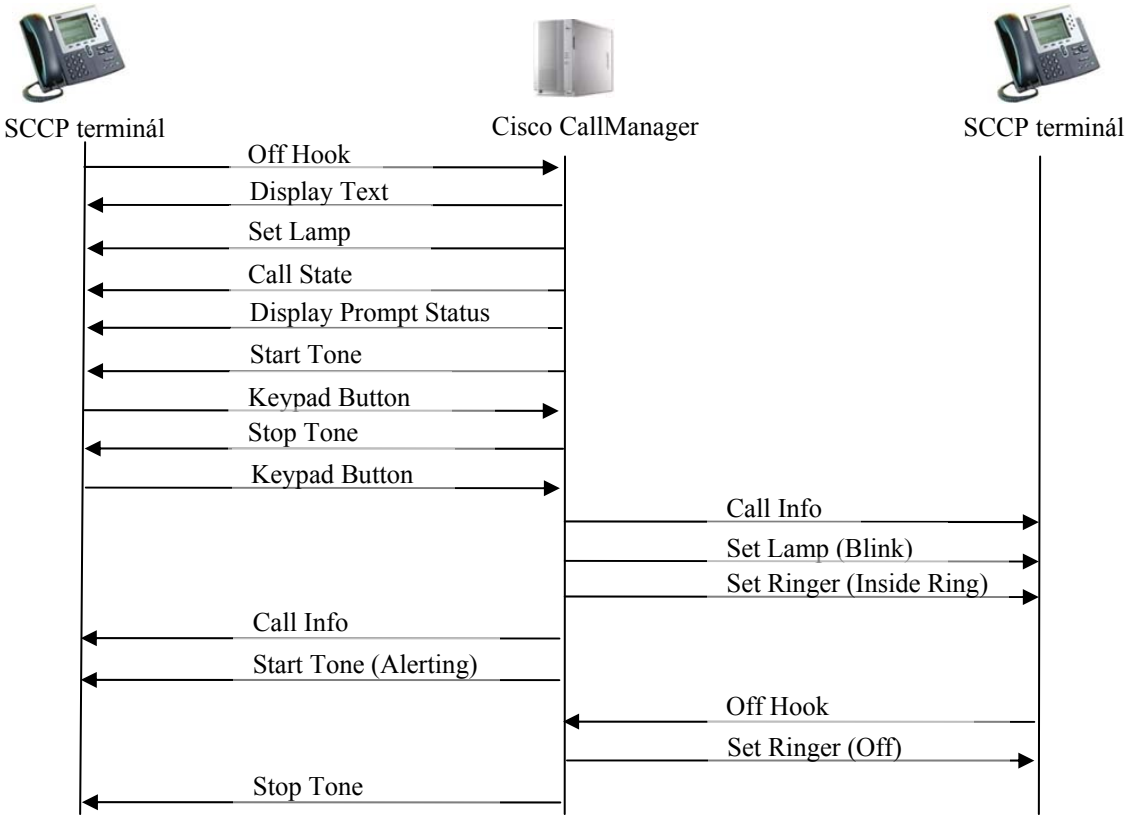
4.3 SIGNALIZACE SCCP

Následuje analýza spojení dvou SCCP uživatelů, kteří jsou zaregistrováni u Cisco CallManageru. Textová podstata protokolu SCCP umožňuje snadnou protokolovou analýzu. Jelikož jsou zprávy protokolu SCCP jednoduché, je nutné pro kompletní signalizaci přenést velké množství zpráv, což činí celkovou analýzu nepřehlednou.

4.3.1 Zahájení spojení

Základní formát SCCP zprávy zastupuje pole o velikosti čtyři bajty pro jednodušší procesy na straně telefonu. Je zřejmé, že zprávy přenášejí minimum informace a systém je nehospodárný. Běžné zahájení spojení vypadá následovně:

1. Po vyzvednutí sluchátka vysílá telefon zprávu Off Hook (Obrázek 4.13) CallManageru.
2. CallManager posílá volajícímu zpět zprávy s přesným nastavením průběhu komunikace. Například identifikaci, časový limit, vyzváněcí tón, atd.
3. Následně CallManager přeposílá veškeré informace o dohodnuté komunikaci druhému účastníkovi pomocí zprávy Call Info.
4. Po přijetí zprávy o vyvěšení protistrany (Off Hook) zruší CallManager vyzváněcí tón volajícího účastníka zprávou Stop Tone.



Obrázek 4.12 Diagram zahájení spojení SCCP uživatelů registrovaných u CallManageru

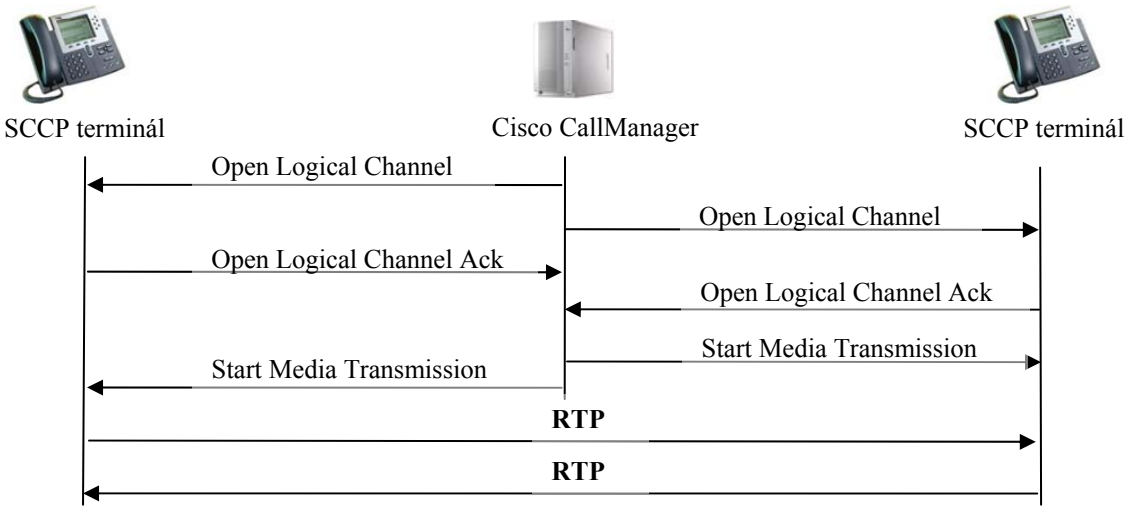
```
⊟ Skinny Client Control Protocol
    Data Length: 12
    Reserved: 0x00000000
    Message ID: OffHookMessage (0x00000006)
```

Obrázek 4.13 Tělo zprávy Off Hook detekované programem Wireshark

4.3.2 Průběh spojení

Po sestavení spojení následuje fáze otevření logických kanálů. Úkolem CallManageru je připravit obě strany na příjem RTP paketů. Typický průběh spojení dvou SCCP (Obrázek 4.14) klientů vypadá následovně:

1. CallManager posílá oběma SCCP klientům zprávu o otevření logického kanálu (Open Logical Channel).
2. Ve zprávě Start Media Transmission (Obrázek 4.15) jsou uloženy informace o nadcházejícím End – to – End spojení. Jedná se hlavně o IP adresy koncových bodů a dohodnuté audio kodeky.
3. K vlastnímu přenosu multimediální informace slouží RTP protokol



Obrázek 4.14 Diagram průběhu spojení SCCP uživatelů registrovaných u CallManageru

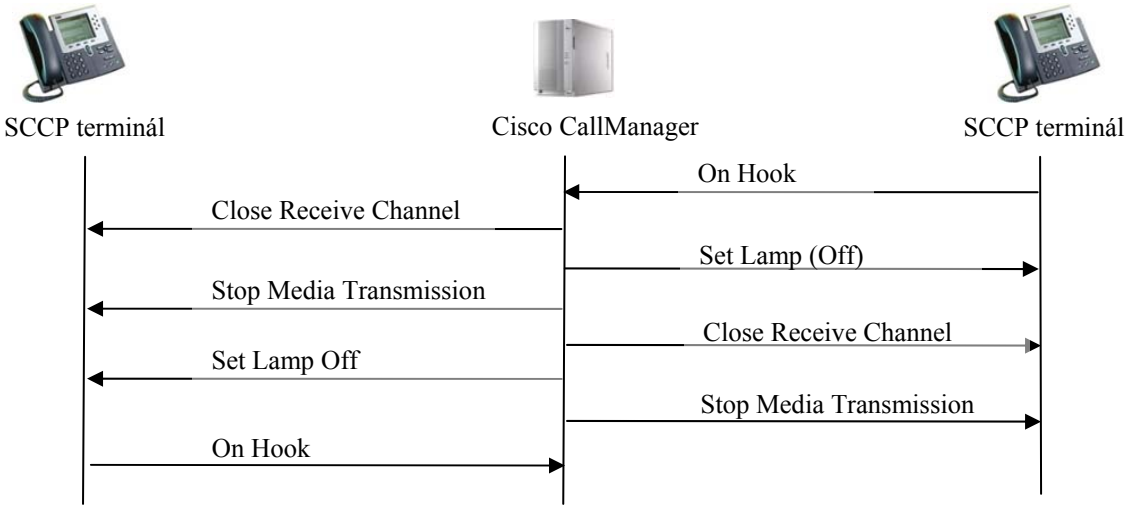
```
⊟ Skinny Client Control Protocol
    Data Length: 108
    Reserved: 0x00000000
    Message ID: StartMediaTransmission (0x0000008a)
    Conference ID: 16777218
    PassThruPartyID: 16777249
    Remote Ip Address: 147.229.151.116 (147.229.151.116)
    Remote Port: 27426
    MS/Packet: 20
    PayloadCapability: G.711 u-law 64k (4)
    Precedence: 184
    Silence Suppression: Media_SilenceSuppression_Off (0x00000000)
    MaxFramesPerPacket: 0
    G723 BitRate: Unknown (0)
```

Obrázek 4.15 Tělo zprávy Start Media Transmission detekované programem Wireshark

4.3.3 Ukončení spojení

Obrázek 4.16 ukazuje příklad ukončení spojení dvou SCCP klientů registrovaných u CallManageru. Úkolem CallManageru je uzavírání logických kanálů a přerušení přenosu média. Následuje příklad ukončení spojení mezi SCCP uživateli:

1. Telefon signalizuje ukončení spojení zprávou zavěšení (On Hook).
2. CallManager uzavírá logické kanály vyhrazené oběma koncovým bodům zprávou Close Receive Channel (Obrázek 4.17) a zastavuje přenos pomocí zprávy Stop Media Transmission.
3. Posledním krokem je uvedení protistrany do zavěšeného stavu (On Hook).



Obrázek 4.16 Diagram ukončení spojení SCCP uživatelů registrovaných u CallManageru

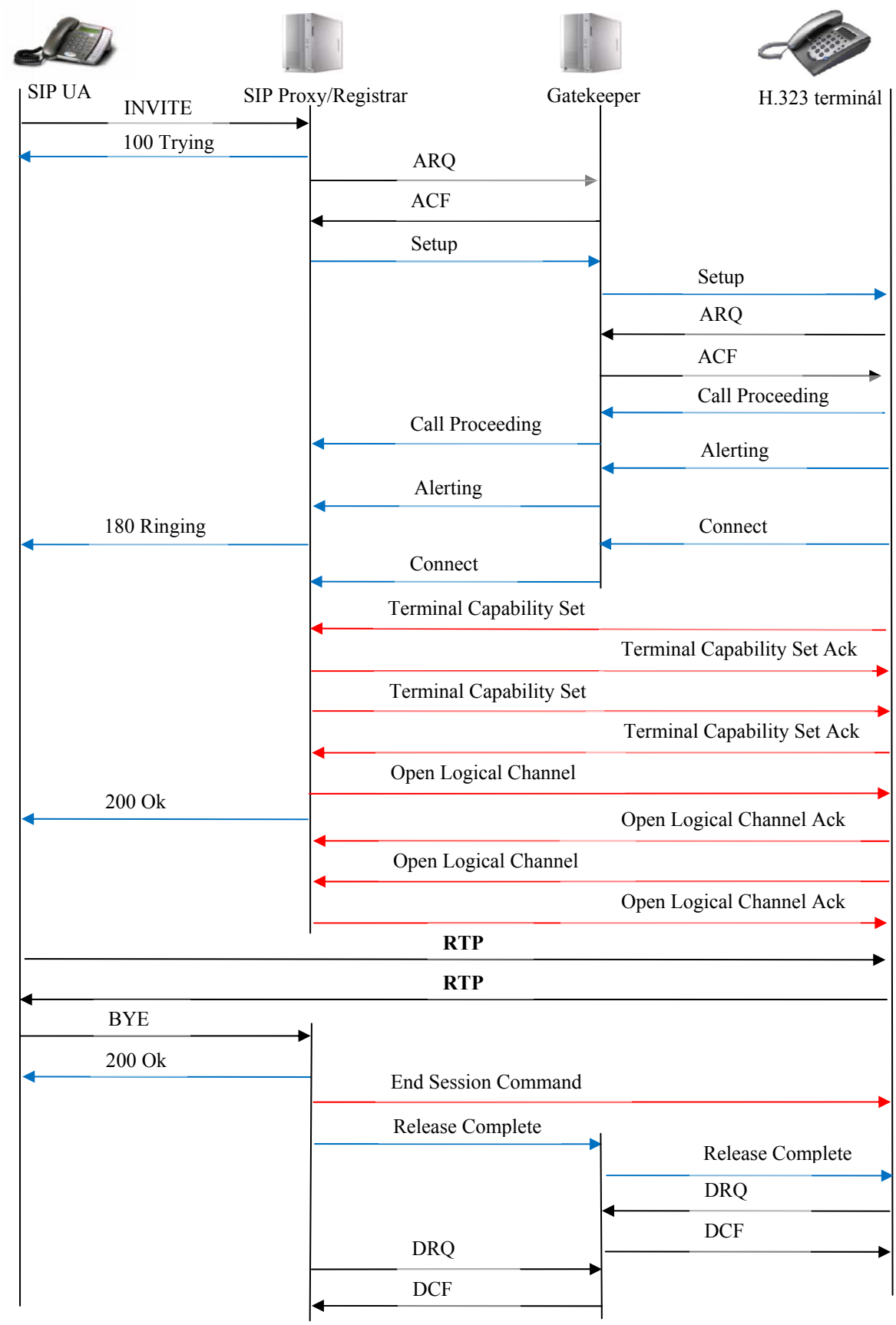
```
⊟ Skinny Client Control Protocol
    Data Length: 20
    Reserved: 0x00000000
    Message ID: CloseReceiveChannel (0x00000106)
    Conference ID: 16777217
    PassThruPartyID: 16777233
```

Obrázek 4.17 Tělo zprávy Close Receive Channel detekované programem Wireshark

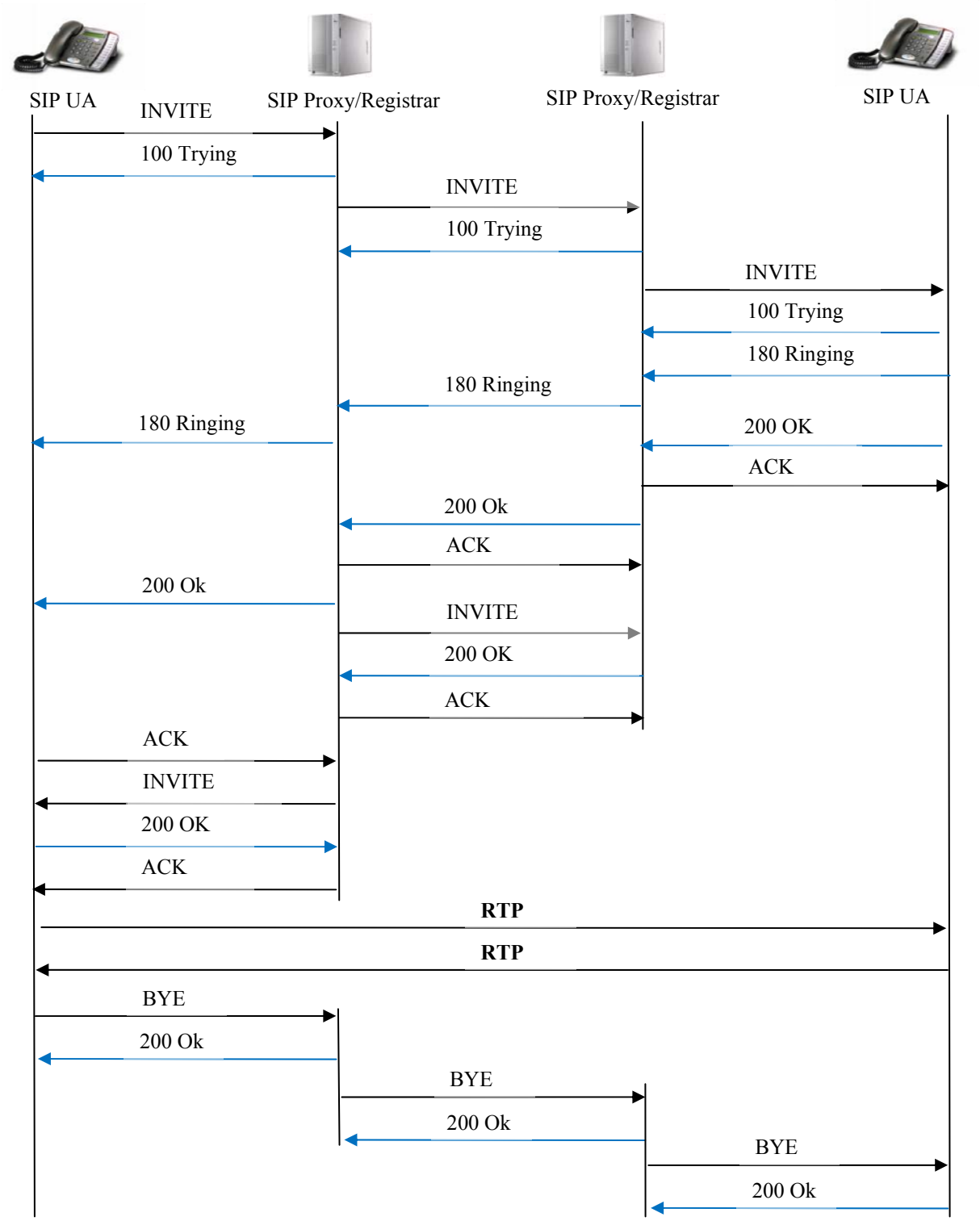
4.4 SIGNALIZACE KONVERGOVANÝCH ŘEŠENÍ

Důležitým předpokladem při nasazení různých signalizačních serverů v IP telefonii je správná volba signalizačního protokolu. Většina VoIP systémů podporuje více signalizačních protokolů, ať už standardizovaných nebo proprietárních, což umožňuje vytvořit konvergovaná řešení těchto systémů.

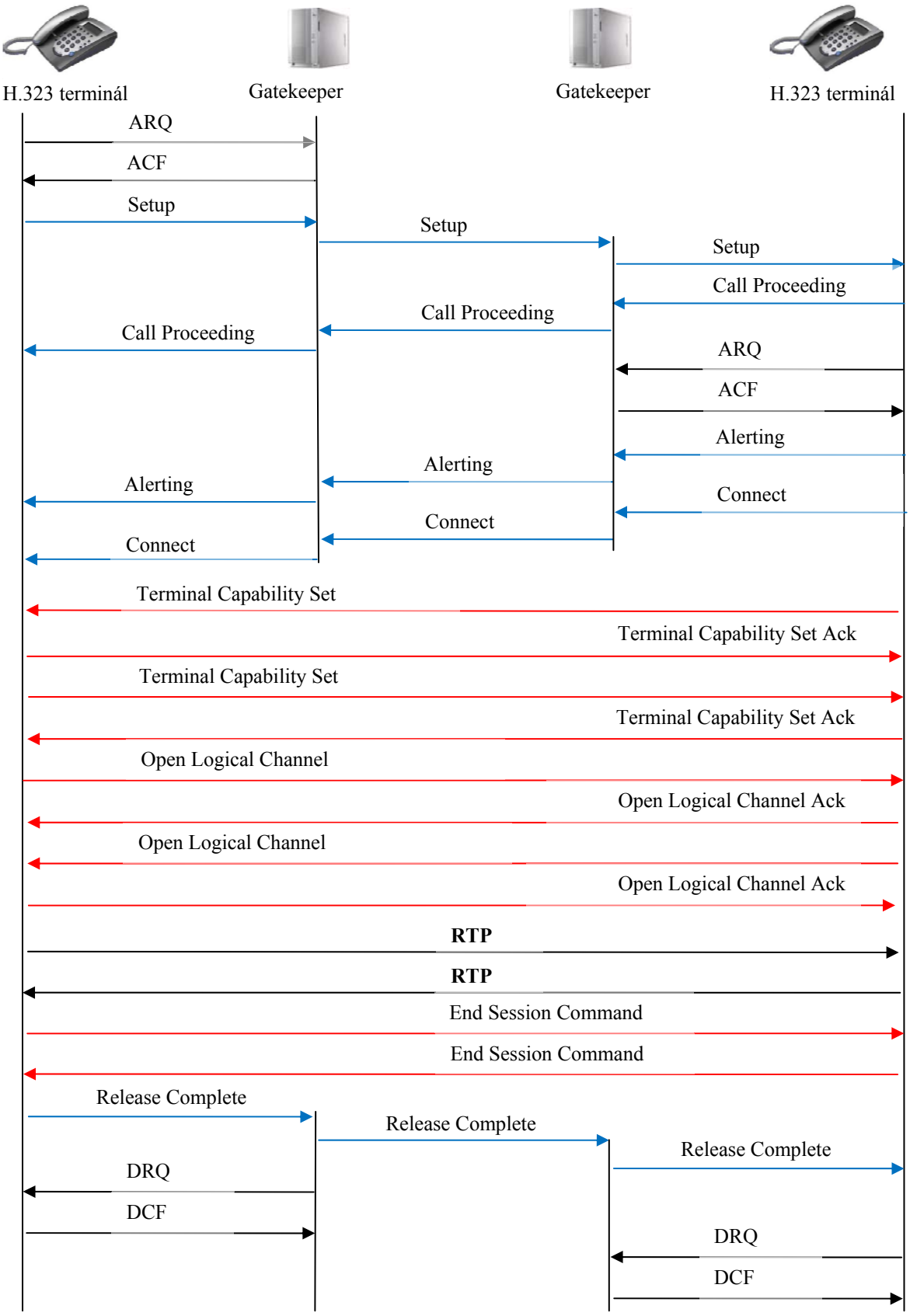
Jednotlivé signalizační postupy pro SIP, H.323 a Cisco při sestavení, průběhu a ukončení spojení jsou zobrazeny v následujících diagramech.



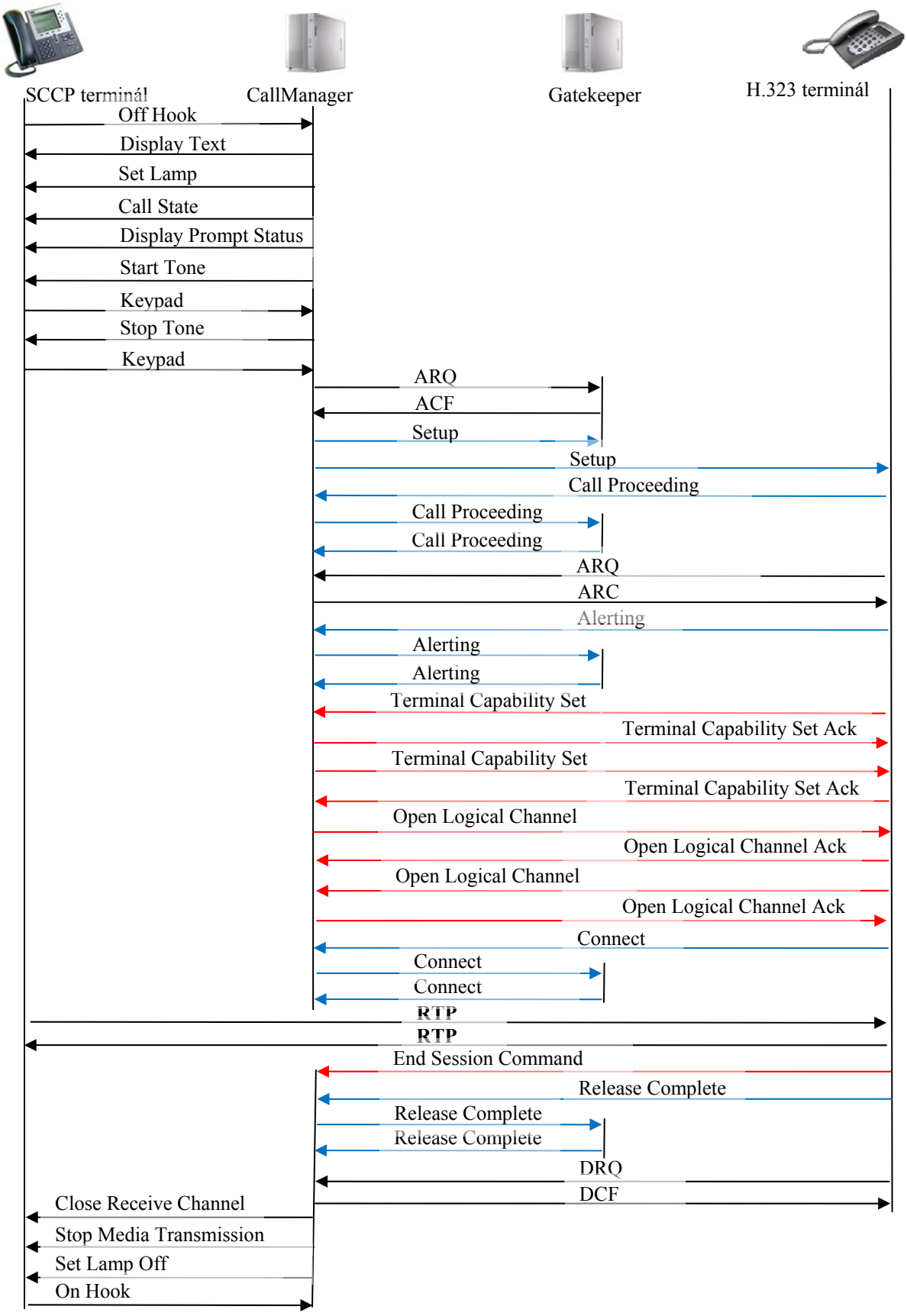
Obrázek 4.18 Diagram spojení domény SIP a H.323 s řídicími prvky Asterisk a GNU Gatekeeper



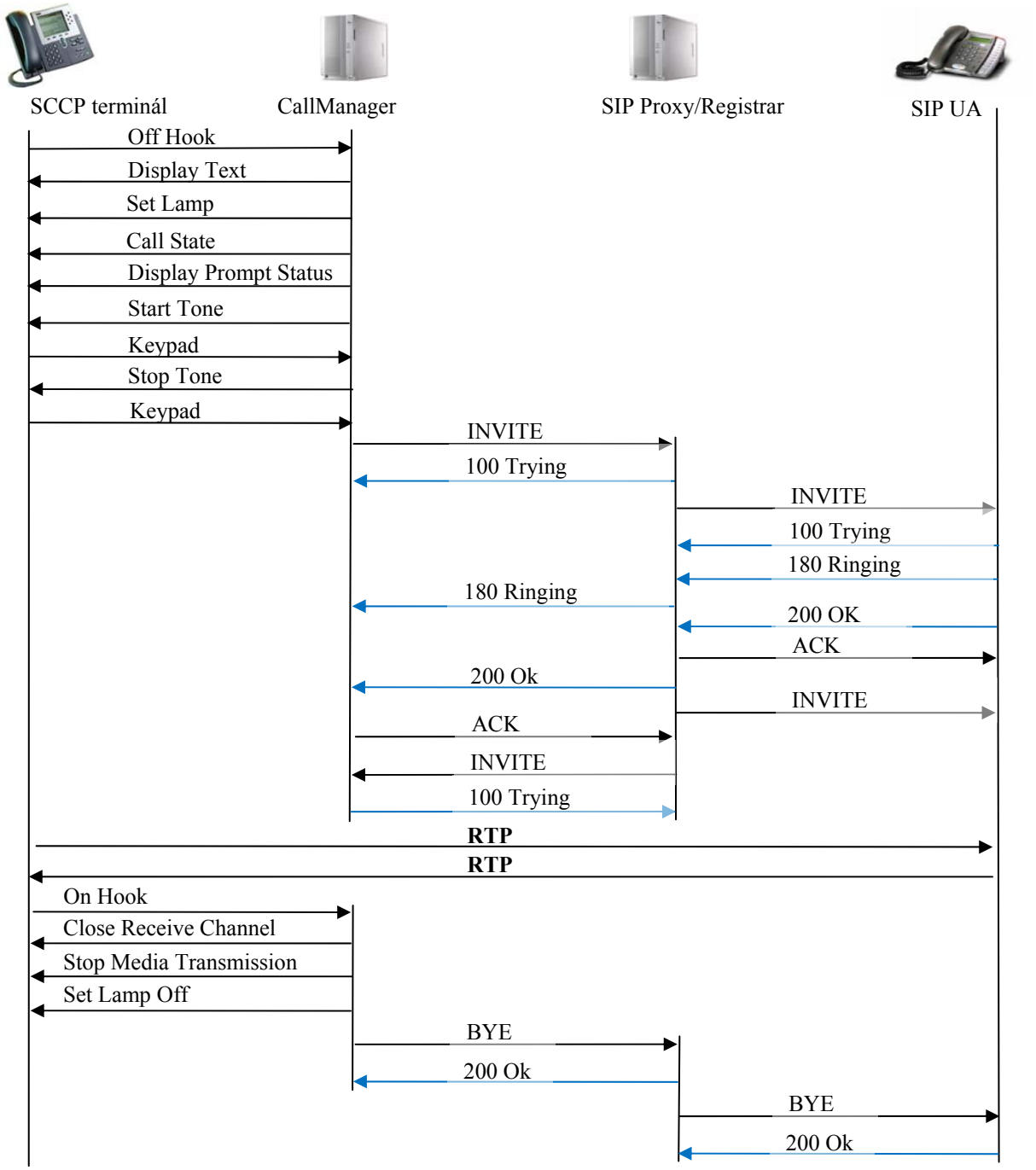
Obrázek 4.19 Diagram spojení dvou SIP domén s řídicím prvkem Asterisk



Obrázek 4.20 Diagram spojení dvou H.323 domén s řídicím prvkem GNU Gatekeeper



Obrázek 4.21 Diagram spojení Cisco a H.323 domén s řídicími prvky CallManger a GNU Gatekeeper



Obrázek 4.22 Diagram spojení Cisco a SIP domén s řídicími prvky CallManger a Asterisk

ZÁVĚR

Rozvoj technologie VoIP je neodmyslitelně spojen s faktory rychlého růstu kvality a rychlosti připojení k Internetu. Nasazení technologie VoIP se stalo jednou z klíčových oblastí konvergence komunikačních a informačních systémů moderních společností.

V práci je podrobně popsána struktura, vlastnosti a funkce architektur SIP, H.323 a Cisco. V dnešní době se více upřednostňuje protokol SIP ve spojení s transportním protokolem RTP před H.323, i když je tato sada v současnosti již velmi propracovaná. Důvodem je jednoduchost, flexibilita a srozumitelnost protokolu SIP. Cisco nabízí efektivní architekturu, která díky otevřeným rozhraním a protokolům (SCCP) nabízí možnost integrace s aplikacemi dalších výrobců.

Součástí práce bylo navrhnout a zrealizovat integrované řešení hovorových služeb v laboratoři. S pomocí dostupných spojovacích systémů a koncových zařízení bylo navrženo experimentální pracoviště architektur SIP, H.323 a Cisco a zajištěno jejich vzájemné propojení pomocí VoIP bran, takže je nyní možné realizovat hovory mezi libovolnými terminály těchto architektur.

Na základě laboratorních experimentů bylo zjištěno, že pro VoIP telefonii lze využít softwarové telefonní ústředny, které se vyrovnají hardwarovým řešením, s výhodou cenové dostupnosti. V rámci experimentálního pracoviště byla ústředna Asterisk úspěšně odzkoušena na dvou serverech. Dále byl využit GNU Gatekeeper jako řídicí prvek H.323 sítě, a také jako gatekeeper potřebný pro podporu H.323 kanálu v softwarové ústředně Asterisk. Jako řídicí telefonní ústředna systému Cisco sloužila aplikace CallManager. Byla realizována celá řada pokusných hovorů. Systémy se představily jako plně funkční a názorně tak demonstrovaly možnosti IP telefonie a softwarových ústředen. Nevýhodou těchto spojení jsou velké zpoždění a nižší stupeň spolehlivosti sítě díky serverům, na jejichž bezproblémovém chodu závisí funkčnost celé sítě.

Důležitým předpokladem při nasazení různých signalizačních serverů v návrhu VoIP sítě je správná volba signalizačního protokolu. Cisco CallManager i Asterisk podporují více signalizačních protokolů, ať už standardizovaných nebo proprietárních, což umožňuje vytvořit konvergovaná řešení těchto systémů a implementaci H.323. Jednotlivé signalizační postupy pro SIP, H.323 a Cisco při sestavení, průběhu a ukončení spojení jsou zobrazeny v podrobných diagramech.

Na základě získaných poznatků a zkušeností byly vytvořeny dvě laboratorní úlohy. Cílem cvičení je prakticky seznámit studenty s možností realizace hlasových služeb v prostředí počítačových sítí. Součástí laboratorních úloh jsou kontrolní otázky, jejichž zodpovězení by po absolvování těchto úloh nemělo činit problémy. K úlohám je přiložen vypracovaný manuál pro instalaci a konfiguraci jednotlivých řešení.

Pro analýzu komunikace mezi jednotlivými prvky při realizaci hovorového spojení byly použity protokolové analyzátory Wireshark a Observer. Programy sloužily pro důkladné sledování a analýzu veškeré síťové komunikace. V práci je uveden přehledný výpis detailních informací jednotlivých paketů a protokolů. Praktické zkušenosti s analýzou protokolu SCCP ukázaly, že pro kompletní signalizaci je nutné přenést velké množství signalizačních zpráv, což činí celkovou analýzu nepřehlednou.

Myšlenka konvergence, neboli sjednocení oddělených telekomunikačních a datových sítí, je založena na jednoduchosti a přímočarosti celkového řešení. V tomto pohledu je protokol IP zásadním zástupcem v oblasti přenosových sítí.

POUŽITÁ LITERATURA

[1] NOVOTNÝ, V. *Účastnická koncová zařízení*. Brno: FEKT VUT Brno, 2002

[2] WIJA, T., ZUKAL, D., VOZŇÁK, M. *Asterisk a jeho použití.* 2005

[3] Úvod do VoIP. MB DATA. 10/2007. www.mbdata.cz.

[4] voip-info.org. 10 2007. www.voip-info.org.

[5] H.323. *International Telecommunication Union*. 11/2007. www.itu.int/net/home/index.aspx.

[6] SIP. *IETF*. 11/2007 www.ietf.org.

[7] H.323 versus SIP: A Comparison. *Packetizer*. 12/2007. www.packetizer.com.

[8] KOMOSNÝ. D., NOVOTNÝ. V. Doporučení H.323. *Elektrorevue*. 4.9.2002. www.elektrorevue.cz.

[9] GNU Gatekeeper. *OpenH323 Gatekeeper - The GNU Gatekeeper*. 2/2008. www.gnugk.org.

[10] SPENCER. M. *IAX:Inter-Asterisk eXchange Version 2*. 4/2008. www.ietf.org/internet-drafts/draft-guy-iax-04.txt.

[11] MILLER, M.A. *Voice over IP technologies - Building a Converged Network*. M&T Books, ISBN 0-7645-4907-3, New York, USA, 2002.

[12] Svět sítí. *Cisco IP telefonie – nosná část architektury AVVID*. 4/2008. http://www.svetsiti.cz/view.asp?rubrika=Technologie&temaID=&clanekID=140

[13] KEJHA, T. *Řešení hlasových služeb v IP sítích*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2007. 84 s. Vedoucí diplomové práce doc. Ing. Vít Novotný, Ph.D.

[14] VAN MEGGELEN, J., MADSEN L., SMITH J. *Asterisk: The Future of Telephony*. O'Reilly, ISBN 978-0-596-51048-0, Sebastopol, USA, 2007.

PŘÍLOHY

PŘÍLOHA A: LABORATORNÍ CVIČENÍ 1 – KONVERGOVANÉ ŘEŠENÍ SIP A H.323

Cíl

Cílem cvičení je seznámit studenty s možností realizace hlasových služeb v prostředí počítačových sítí. Studenti budou prakticky seznámeni s principy fungování IP telefonie prostřednictvím standardů SIP a H.323. Dále seznámit studenty s analýzou provozu jak v síti SIP, tak i H.323.

Vybavení pracoviště

Pracoviště sestává ze čtyř počítačů (dva s operačním systémem Windows, dále Fedora a Debian), hardwarových a softwarových IP telefonů a dvou H.323 videotelefonů podle následující tabulky:

	H.323	SIP
HW koncové body	VIP – 101T, NT – 320	VIP – 155T, VIP – 153T
SW koncové body	NetMeeting	X – Lite
videotelefon	NetMeeting	
servery	GNU Gatekeeper	Asterisk

Úkoly

1. Seznamte se s pracovištěm (Obrázek A. 1).
2. Uskutečněte hovor v doméně SIP a následně v doméně H.323.
3. Realizujte videohovor mezi účastníky H.323.
4. Nakonfigurujte Gatekeeper 1 jako souseda Gatekeeperu 2 a prověřte funkčnost nastavení.
5. Realizujte hovor mezi dvěma Asterisky pomocí trunku SIP a navrhněte řešení pro propojení pomocí IAX2 kanálu.
6. Uskutečněte hovor mezi oběma architekturami prostřednictvím oh323 kanálu.
7. Seznamte se s funkcemi a možnostmi analyzátoru Wireshark.
8. Zachyťte průběh spojení paketovým analyzátorem a z dekódovaných zpráv určete IP adresy všech terminálů a gatekeeperu.
9. Uskutečněte spojení mezi H.323 terminály a pomocí diagramu spojení zjistěte, zda byl hovor signalizován mezi koncovými body nebo prostřednictvím gatekeeperu.
10. Proveďte rekonstrukci VoIP hovoru prostřednictvím nástroje Stream Analysis.

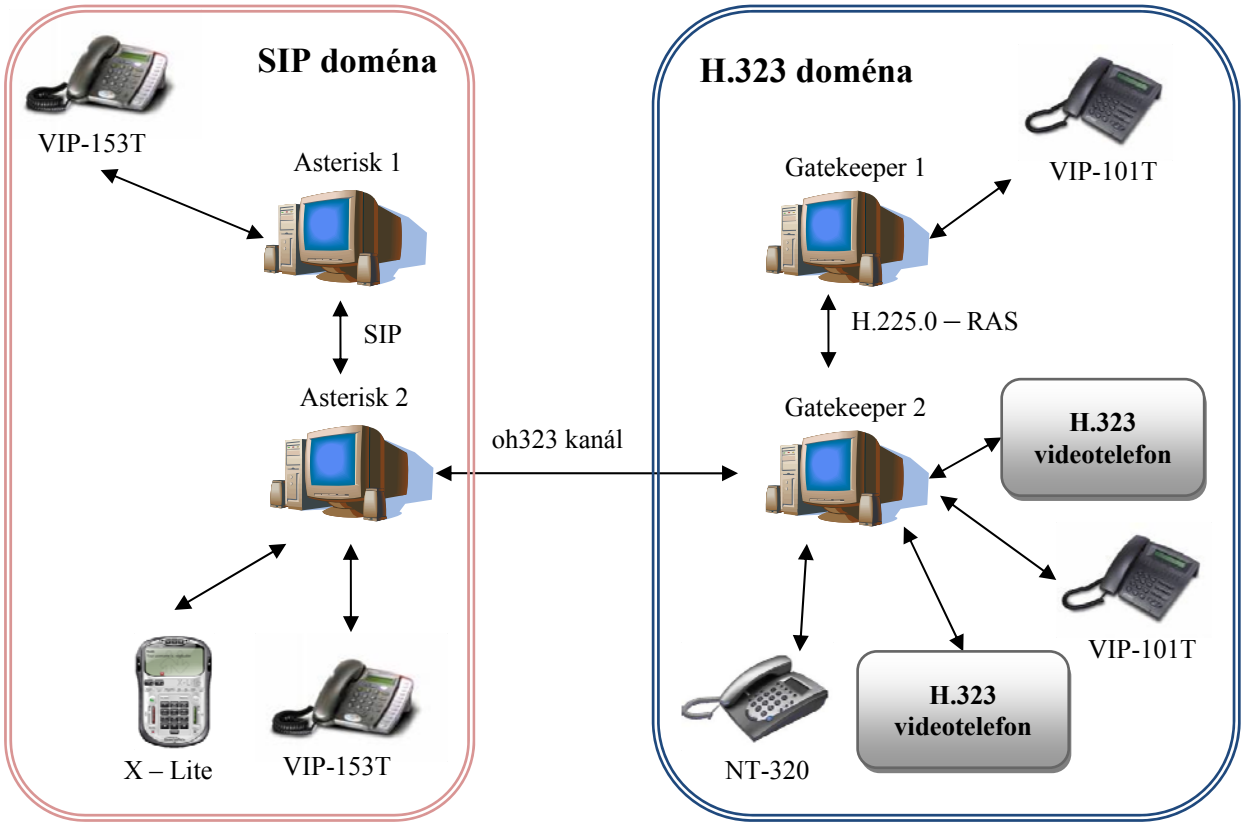
Teoretický úvod

VoIP představuje souhrn technik nutných pro přenos hlasu po sítích s přepojováním datových jednotek potřebných k přenosu digitalizovaného hlasu. Základem této technologie jsou protokoly, kterými se VoIP řídí. V současnosti jsou nejběžnější H.323 a SIP. Pro realizaci pracoviště je vybráno jedno řešení pro SIP doménu, a to softwarová pobočková ústředna Asterisk. Jedná se o kompletní open source softwarovou PBX, která je kompatibilní s mnoha telekomunikačními standardy. Asterisk využívá kanály jako logické spojení k vytvoření relací. Kanál SIP umožňuje Asterisku fungovat jako SIP klient, proxy server i registrar. SIP může být také použit pro vzájemné propojení Asteriskových serverů pomocí tzv. trunků. Princip trunkování spočívá ve spojení dat souběžných spojení mezi koncovými body stejného typu do jednoho paketu. Asterisk však nevystupuje jako

registrační server pro H.323 koncová zařízení, ale pouze jako gateway. Další možností je využití protokolové sady H.323. Řídicím serverem H.323 domény je GNU Gatekeeper. Jde o otevřené řešení pro implementaci H.323 gatekeeperu a koncových zařízení. Je využíván ve funkci gatekeeperu potřebného pro kontrolu H.323 kanálu v softwarové ústředně Asterisk. Tento kanál nese název oh323 a je aplikován do systému za účelem implementace H.323 komponent. Kombinace architektur SIP a H.323 vede k účelnému využívání jejich výhod a představuje tak konvergovaná řešení těchto architektur.

Technologie VoIP přináší celou řadu nových možností:

- efektivní využití počítačové sítě,
- nižší náklady,
- integrace služeb.



Obrázek A. 1 Schéma zapojení laboratorní úlohy 1

Architektura SIP

SIP (Session Initiation Protocol) je signalizační protokol pro řízení spojení v IP síti. Jedná se o textově orientovaný protokol navržený organizací IETF. Textová podstata SIP umožňuje jednodušší analýzu paketů. Protokol zabezpečuje mobilitu účastníka použitím logické adresy namísto fyzické. Zprávy protokolu SIP jsou tvořeny hlavičkou a vlastním tělem zprávy.

Architektura H.323

Standard H.323 je produktem telekomunikační unie ITU. Jedná se o zastřešující protokol, což znamená podřazenost jiných protokolů zajišťujících řízení spojení, management přenosu a zpracování multimediálních dat. Tento protokol je orientován binárně, takže pro jeho analýzu je zapotřebí kvalitních analyzátorů. Zprávy protokolové sady

H.323 jsou binárně zapouzdřeny v dílčích protokolech a jsou přenášeny prostřednictvím TCP i UDP. Adresování v H.323 využívá zpráv definovaných v kódu protokolu H.225.0. Většinou se jedná o síťovou adresu, kde identifikátorem je IP adresa.

Postup

Realizace spojení

Realizujte hovory mezi všemi účastníky SIP domény registrovanými u Asterisku 1 a následně mezi H.323 IP telefony registrovanými u Gatekeeperu 1. Posuďte a porovnejte kvalitu přenášeného hlasu mezi oběma doménami a také mezi softwarovým a hardwarovým koncovým bodem v doméně SIP.

Realizujte videohovor pomocí programu NetMeeting v doméně H.323. Spusťte program NetMeeting přes ***Start → Spustit → conf***. Zvolte ***Nástroje → Možnosti → Možnosti volání***. Do pole ***Server gatekeeper*** zapište IP adresu Gatekeeperu 2 (147.229.151.107) a rovněž vyplňte jméno nebo číslo účtu. NetMeeting se automaticky zaregistruje ke GNU Gatekeeperu. Nyní je možné vytočit číslo volaného. Posuďte a porovnejte kvalitu přenášeného videohovoru.

Uskutečněte hovor mezi dvěma Asterisky v rámci domény SIP. Asterisky jsou propojeny pomocí kanálu SIP. Konfigurace kanálu spočívá v nastavení konfiguračního souboru ***sip.conf*** v adresáři ***/etc/asterisk*** na serveru Asterisk 1:

```
[general]                          ;definice hlavních voleb

register=>asterisk1:heslo@<IP_adresa_Asterisk2>

[asterisk2]
type=friend                        ;uživatel může volat i přijímat hovory
host=<IP_adresa_Asterisk2>         ;IP adresa serveru Asterisk2
secret=heslo
context=incoming_Asterisk
trunk=yes                          ;pro úsporu přenosové kapacity
```

Na serveru Asterisk 2 je zřízen účet pro uživatele Asterisk 1. Při propojení dvou ústředen pomocí IAX2 je situace velmi podobná jako při využití SIP. Při správné konfiguraci není nutná vzájemná registrace ústředen.

Konfigurace sousedního gatekeeperu se provádí v souboru ***gatekeeper.ini***, který otevřete po zvolení ***Start → Programy → GNU Gatekeeper → Configuration***. Definice Gatekeeperu 1 jako souseda Gatekeeperu 2 je následující:

```
[RasSrv::Neighbors]                ;definice souseda
GK1=GnuGk

[Neighbor::GK1]                    ;konfigurace souseda
GatekeeperIdentifier=GK1           ;identifikátor
Host=<IP_adresa_gatekeeper1>       ;nastavení IP adresy serveru
SendPrefixes=*                     ;prefixy vysílané gatekeeperem
AcceptPrefixes=*                   ;prefixy akceptované gatekeeperem
```

Nezapomeňte provést reload systému a to přes ***Start → Programy → GNU Gatekeeper → Reload***.

V rámci konvergovaného řešení realizujte hovor mezi účastníkem domény SIP a domény H.323. Posuďte vzniklé zpoždění.

Analýza spojení

Analýza spojení se provádí prostřednictvím programu Wireshark. Před samotnou analýzou je nutné nastavit parametry programu pro správnou funkci. V menu ***Capture*** → ***Options*** → ***Interface*** se provádí volba síťové karty. Ostatní položky jsou přednastaveny pro správnou funkci programu.

Zachytávání paketů lze spustit tlačítkem ***Start***. Ukončení zachytávání paketů lze provést klávesovou zkratkou ***Ctrl + E***.

Celkové množství zachycených paketu můžeme pro naše účely zpracovat nejlépe s využitím nástroje ***VoIP Calls***, který se nachází v menu ***Statistics***. Po jeho otevření se objeví okno se seznamem všech VoIP hovorů, které proběhly v průběhu zachytávání. Pro zobrazení tzv. flow graph spojení slouží tlačítko ***Graph***.

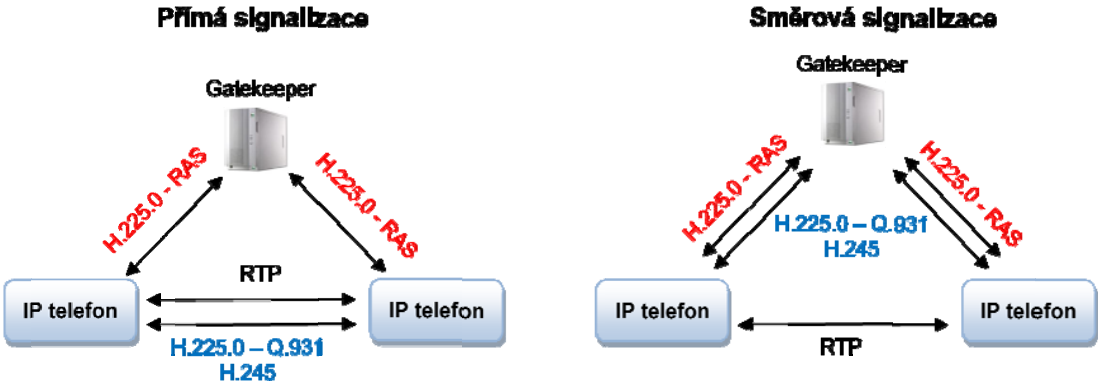
Vlastní přenos hlasových dat je realizován prostřednictvím protokolu RTP. Program Wireshark umožňuje rekonstrukci uskutečněných hovorů prostřednictvím payloadů zachycených RTP paketů. Rekonstrukce hovoru přeneseného protokolem RTP je následující. V hlavním okně je nutné označit jeden z RTP paketů hovoru určeného pro rekonstrukci. Dále volba menu ***Statistics*** → ***RTP*** → ***Stream Analysis*** otevře okno zobrazující dopředný (Forward) i zpětný (Reserved) směr přenosu. Uložení a následné přehrání payloadu lze provést stisknutím tlačítka ***Save payload***. V novém okně se zvolí cesta a formát ukládaných dat. Soubory s příponou ****.au*** si můžeme přehrát v programu Windows Media Player.

Hovorová signalizace v H.323 doméně

Existují dva modely navázání hovorové signalizace v H.323:

- přímá signalizace (direct call signalling),
- směrová signalizace (routed call signalling).

Pokud gatekeeper zvolí metodu přímého volání (Obrázek A. 2**Chyba! Nenalezen zdroj odkazů.**), pak volající terminál iniciuje signalizační spojení přímo s volaným terminálem. V případě směrového volání (Obrázek A. 2) je signalizační spojení nejprve navázáno s gatekeeperem, a ten následně naváže druhé spojení s volaným terminálem. V tomto režimu má gatekeeper větší kontrolu nad průběhem hovoru.



Obrázek A. 2 Diagramy rozdílnosti přímé a směrové signalizace

Kontrolní otázky

1. Jaká je funkce proxy serveru?
2. Jaká je funkce gatekeeperu?
3. Jaký je rozdíl mezi přímou a směrovou signalizací?
4. Čím je dáno zpoždění při realizaci hovoru konvergovaného řešení?

PŘÍLOHA B: LABORATORNÍ CVIČENÍ 2 – KONVERGOVANÉ ŘEŠENÍ CISCO – SIP A CISCO – H.323

Cíl

Cílem laboratorní úlohy je experimentální ověření oboustranné komunikace v počítačové síti s CallManagerem jako řídicím prvkem a následnou analýzou komunikace při realizaci hovorového spojení.

Vybavení pracoviště

Pracoviště sestává ze tří počítačů (dva s operačním systémem Windows a jeden s Debianem) a hardwarových a softwarových IP telefonů podle následující tabulky:

	Cisco	H.323	SIP
HW koncové body	Cisco IP Phone 7960	VIP – 101T, NT – 320	VIP – 153T
SW koncové body			X – Lite
servery	CallManager	GNU Gatekeeper	Asterisk

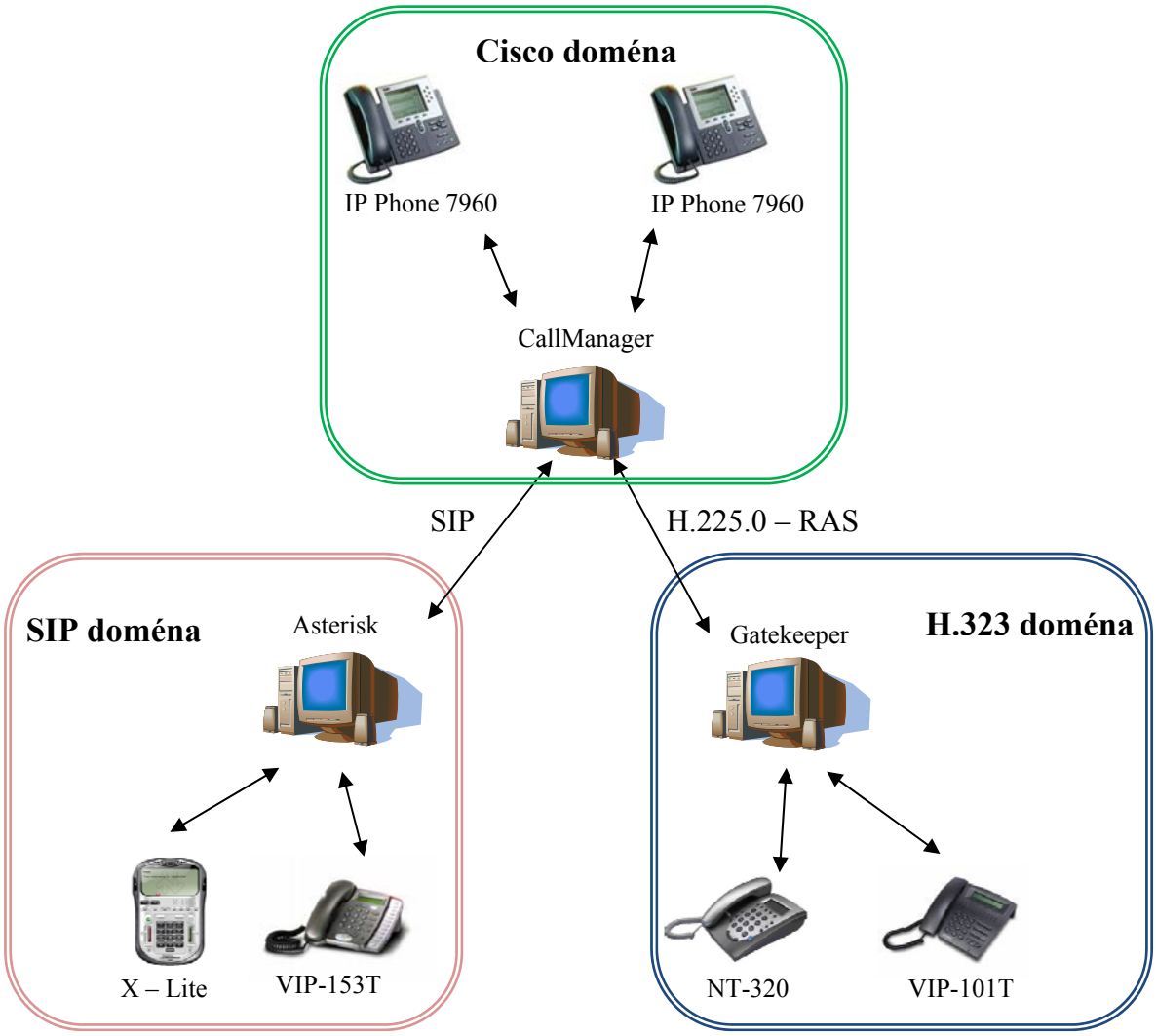
Úkoly

1. Seznamte se s pracovištěm (Obrázek B. 1).
2. Nakonfigurujte IP telefon NT – 320 a uskutečněte hovor v doméně H.323.
3. Nakonfigurujte IP telefon VIP – 153T a uskutečněte hovor v doméně SIP.
4. Realizujte hovor mezi doménou Cisco a SIP.
5. Realizujte hovor mezi doménou Cisco a H.323.
6. Zachyťte a analyzujte pomocí programu Wireshark komunikaci mezi jednotlivými zařízeními. Analyzujte průběh signalizace při budování a ukončení komunikace.

Teoretický úvod

VoIP představuje souhrn technik nutných pro přenos hlasu po sítích s přepojováním datových jednotek potřebných k přenosu digitalizovaného hlasu. Základem této technologie jsou protokoly, kterými se VoIP řídí. V současnosti jsou nejběžnější H.323 a SIP. V neposlední řadě také vystupuje protokol SCCP. Jedná se o proprietární protokol firmy Cisco sloužící pro komunikaci mezi Cisco CallManagerem a Cisco VoIP telefony.

Pro realizaci pracoviště je vybráno jedno řešení pro SIP doménu a to softwarová pobočková ústředna Asterisk. Jedná se o kompletní open source softwarovou PBX, která je kompatibilní s mnoha telekomunikačními standardy. Asterisk využívá kanály jako logické spojení k vytvoření relací. Kanál SIP umožňuje Asterisku fungovat jako SIP klient, proxy server i registrar. Další možností je využití protokolové sady H.323. Řídicím serverem H.323 domény je GNU Gatekeeper. Jde o otevřené řešení pro implementaci H.323 gatekeeperu a koncových zařízení. Softwarová telefonní ústředna CallManager je základním prvkem IP telefonie systému Cisco. Jedná se o řídicí aplikaci využívající především signalizační protokol SCCP. Kombinace architektur Cisco – SIP a Cisco – H.323 vede k účelnému využívání jejich výhod a představuje tak konvergovaná řešení těchto architektur.



Obrázek B. 1 Schéma zapojení laboratorní úlohy 2

Postup

Realizace spojení

Konfigurace IP telefonu NT – 320 se provádí dvěma způsoby. Jednak pomocí webového prohlížeče nebo přes klávesnici a menu na LCD displeji. Do webového prohlížeče zadejte IP adresu telefonu NT – 320, login se nepíše a heslo je ***1234***. Pro správnou funkci telefonu v H.323 síti je důležité vyplnit sekci ***H.323 Protocol Settings***. Do pole ***Gatekeeper*** napište IP adresu gatekeeperu a zaškrtněte možnost ***use service***. Nyní se přesvědčte, zda se IP telefon zaregistroval ke GNU Gatekeeperu a zda je připraven k použití v H.323 síti. Na počítači s nainstalovaným GNU Gatekeeperem zvolte ***Start → Programy → GNU Gatekeeper → Monitor***. Do otevřeného okna napište příkaz ***rv*** pro zobrazení aktivních registrací. Uskutečněte hovor s registrovanými účastníky v H.323 doméně.

Konfigurace IP telefonu VIP – 153T se provádí opět dvěma způsoby. Pomocí webového prohlížeče nebo přes klávesnici a menu na LCD displeji. Do webového prohlížeče zadejte IP adresu telefonu VIP – 153T, napište login ***admin*** a heslo ***123***. Pro správnou funkci telefonu v SIP síti je důležité vyplnit sekci ***SIP Configuration***. Vyplňte jméno, číslo a heslo uživatele. Tyto údaje se musí shodovat s údaji uživatele nadefinovaného pro Asterisk. Do pole ***SIP Domain Name*** zapište IP adresu Asterisku. Změny uložte. Nyní

se přesvědčte, zda se IP telefon zaregistroval k Asterisku a zda je připraven k použití v SIP síti. Na počítači s nainstalovaným Asteriskem otevřete terminál a zadejte příkaz ***asterisk –r***. Zobrazí se konzole Asterisku běžícího na pozadí počítače. Napište příkaz pro zobrazení SIP účastníků ***sip show peers***. Uskutečněte hovor s registrovaným účastníkem X – Lite.

Realizujte hovor mezi jedním účastníkem domény Cisco a SIP doménou. Následně realizujte hovor mezi účastníkem domény Cisco a H.323 IP telefony. Posuďte a porovnejte kvalitu přenášeného hlasu mezi oběma doménami.

Analýza spojení

Analýza spojení se provádí prostřednictvím programu Wireshark. Před samotnou analýzou je nutné nastavit parametry programu pro správnou funkci. V menu ***Capture → Options → Interface*** se provádí volba síťové karty. Ostatní položky jsou přednastaveny pro správnou funkci programu.

Zachytávání paketů lze spustit tlačítkem ***Start***. Ukončení zachytávání paketů lze provést klávesovou zkratkou ***Ctrl + E***.

Celkové množství zachycených paketu můžeme pro naše účely zpracovat nejlépe s využitím nástroje ***VoIP Calls***, který se nachází v menu ***Statistics***. Po jeho otevření se objeví okno se seznamem všech VoIP hovorů, které proběhly v průběhu zachytávání. Pro zobrazení tzv. flow graph spojení slouží tlačítko ***Graph***.

Kontrolní otázky

1. Porovnejte protokoly SCCP a SIP.
2. Jaká je funkce aplikace CallManager?
3. Jakými kanály je spojen CallManager s Asteriskem a Gatekeeperem?

PŘÍLOHA C: DETEKOVANÉ DIAGRAMY SPOJENÍ

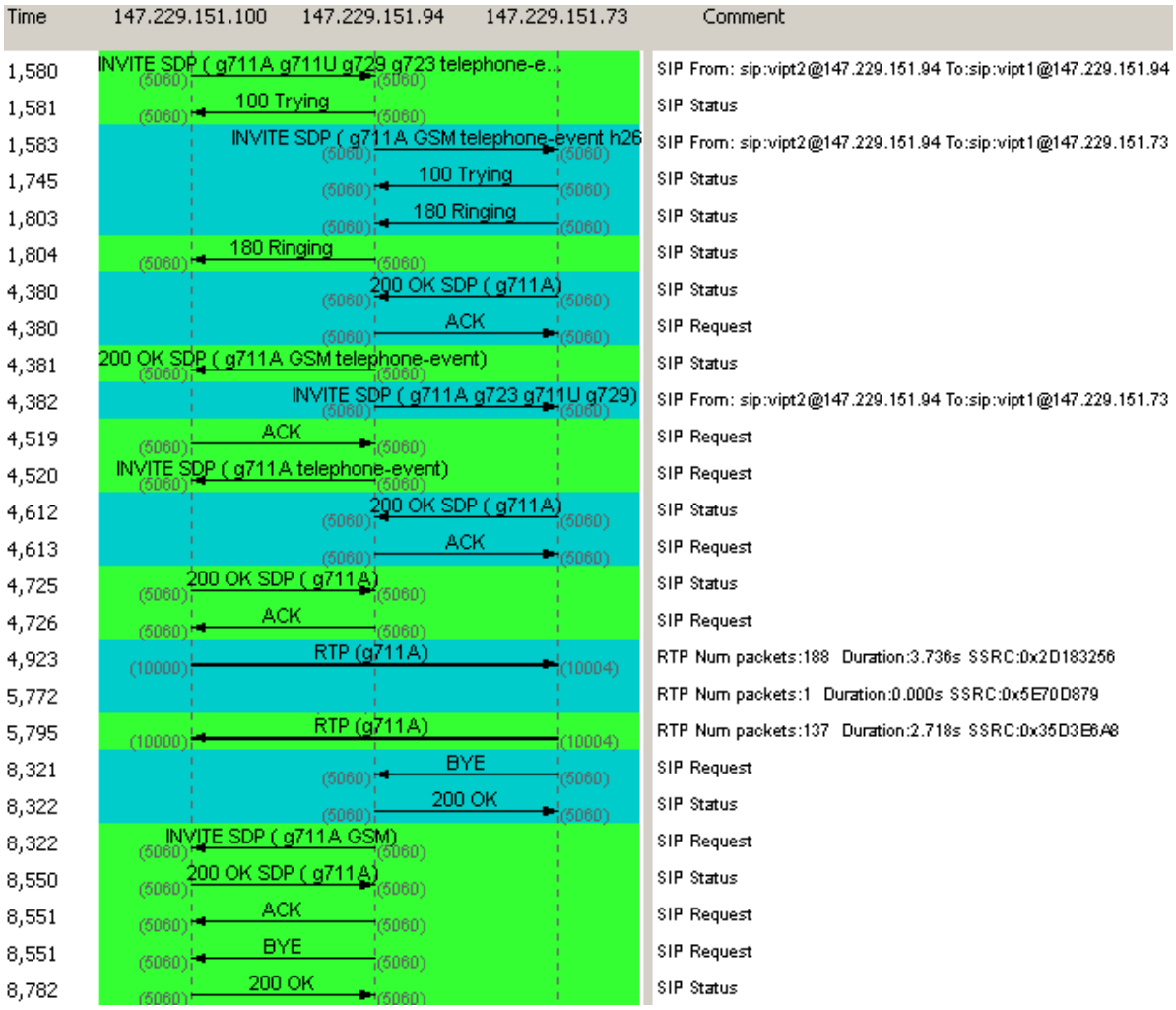
Diagram spojení dvou terminálů v H.323 síti prostřednictvím gatekeeperu

Následující diagram (Obrázek C. 1) ukazuje propojení dvou H.323 koncových bodů s využitím gatekeeperu jako středového prvku. Podle zpráv protokolu H.245 je vidět, že byla zvolena přímá signalizace.

Obrázek C. 1 Detekovaná komunikace pomocí programu Wireshark v síti H.323

Diagram spojení dvou terminálů v SIP síti prostřednictvím Asterisku

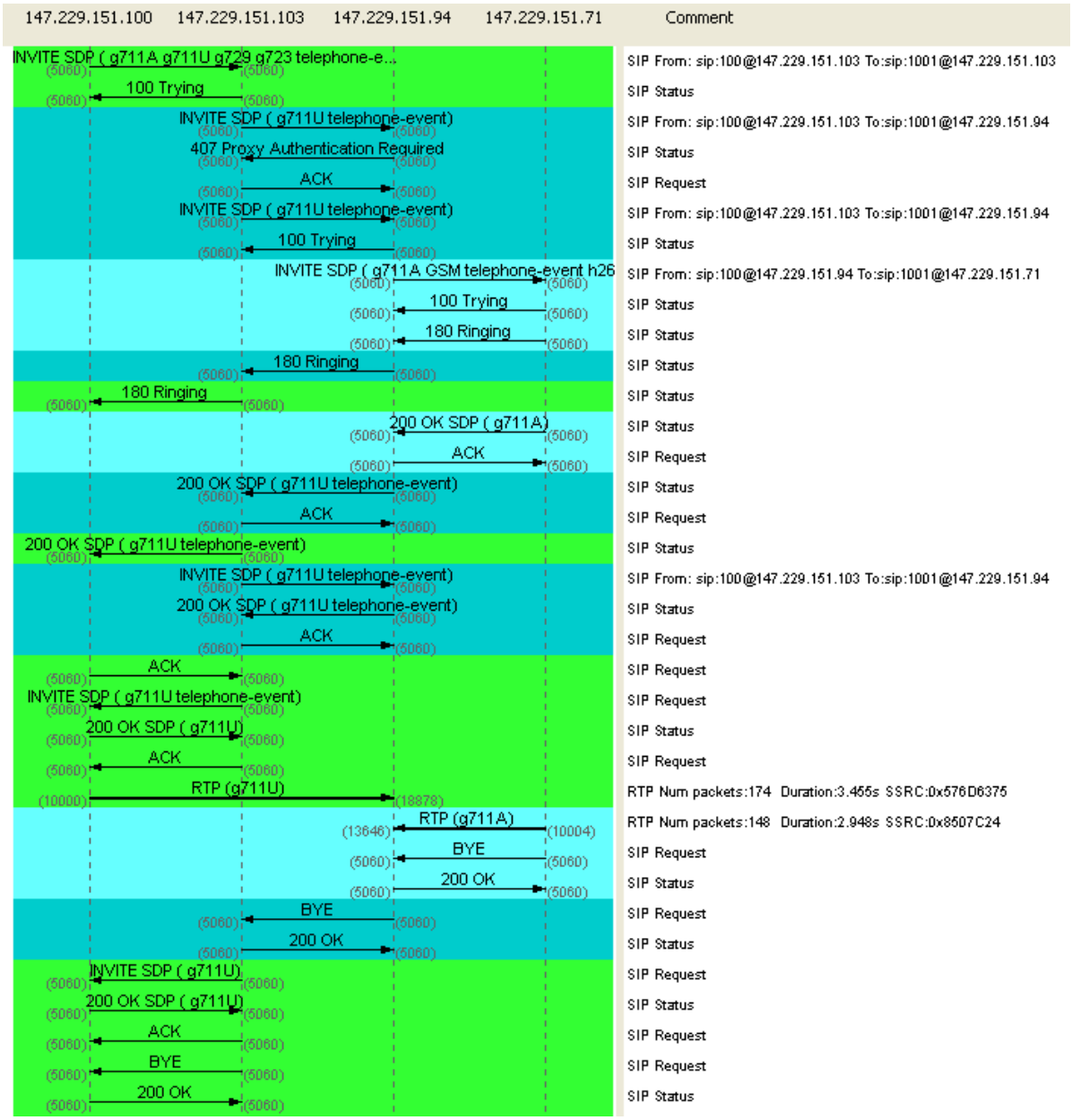
Obrázek C. 2 znázorňuje situaci, kdy volající i volaný jsou registrováni ke stejnému serveru v rámci společné domény. Kdyby byl volaný účastník registrovaný u jiné domény, zobrazený proxy server by směroval zprávu INVITE na další proxy server.



Obrázek C. 2 Detekovaná komunikace pomocí programu Wireshark v síti SIP

Diagram spojení dvou Asterisků prostřednictvím kanálu SIP

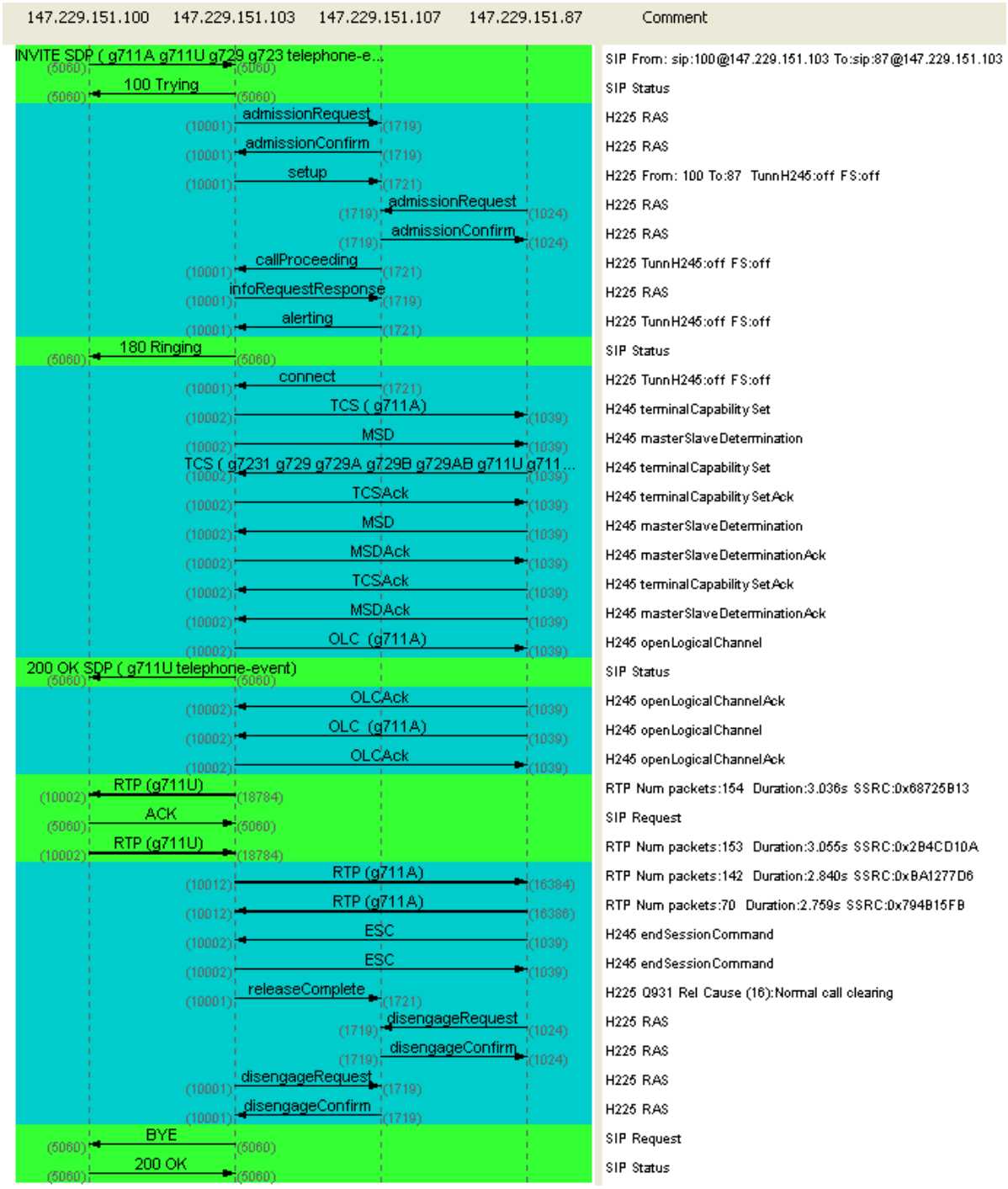
Obrázek C. 3 ukazuje propojení dvou SIP domén pomocí softwarových pobočkových ústředen Asterisk. Spojení dvou Asterisků je zabezpečeno kanálem SIP.



Obrázek C. 3 Propojení SIP domén detekované pomocí programu Wireshark

Diagram spojení sítě SIP a H.323

Tento diagram spojení detekovaný analyzátorem Wireshark ukazuje propojení dvou různých architektur SIP a H.323. SIP telefon (147.229.151.100) vyslal žádost o spojení směrem k ústředně Asterisk (147.229.151.103). Ústředna pomocí implementovaného oh323 kanálu komunikuje s gatekeeperem (147.229.151.107) přes zprávy protokolu H.225.0 – RAS. Gatekeeper prostřednictvím zprávy H.245 získává informace o vybavení z hlediska multimediálních funkcí s H.323 IP telefonem (147.229.151.87). Po otevření logického kanálu dochází k přenosu dat (RTP). Z diagramu je vidět, že Asterisk slouží také jako překladač audio kodeků (A – law, μ – law).



Obrázek C. 4 Propojení SIP a H.323 domén detekované pomocí programu Wireshark

Tělo zprávy protokolu SDP

SDP je vnitřní protokol standardu SIP. Obrázek C. 5 ukazuje tělo zprávy protokolu SDP obsažené v žádosti INVITE.

Obrázek C. 5 Příklad těla zprávy protokolu SDP detekované pomocí programu Observer

Konfigurační soubor gatekeeper.ini

Následující nastavení konfiguračního souboru umožňuje programu GNU Gatekeeper bezproblémově plnit funkci gatekeeperu. Dále je zde zmíněno nastavení spojení s pobočkovou ústřednou Asterisk, sousedním gatekeeperem a CallManagerem.

Příklad nastavení konfiguračního souboru ***gatekeeper.ini***:

```
[Gatekeeper::Main]
FortyTwo=42                          ;zjištění přítomnosti konfig. souboru
Name=GnuGkA                          ;identifikace gatekeeperu
Home=<IP_adresa_gatekeeperu>         ;IP adresa gatekeeperu
EndpointSuffix=_GnuGk                ;definice přípony
TimeToLive=600                       ;nastavení timeout pro registraci
UnicastRasPort=1719                  ;nastavení portu pro RAS

[GkStatus::Auth]                     ;definice pravidel
rule=allow                           ;povolení jakéhokoli připojení
<IP_adresa_gatekeeperu>=allow        ;pro možnost monitorování
default=forbid

[RoutedMode]
GKRouted=1                           ;mód směrování signalizace
H245Routed=0                         ;přenášení zpráv H.245 přes gatekeeper
CallSignalPort=1720                  ;port pro signalizaci
AcceptNeighborCalls=1                ;akceptování volání
AcceptUnregisteredCalls=1            ;akceptování neregistrovaných volání
DropCallsByReleaseComplete=1         ;uvolnění kanálu po ukončení hovoru
SupportNATedEndpoints=1              ;podpora koncových bodů za NATem

[RoutingPolicy]                      ;definice politiky směrování
default=explicit,internal            ;explicitní a interní požadavek

[RasSrv::Neighbors]                  ;směrování
GK1=asterisk
GK2=GnuGk
GK=CiscoGk

[Neighbor::GK1]                      ;konfigurace souseda
GatekeeperIdentifier=GK1             ;identifikátor
Host=<IP_adresa_Asterisku>           ;nastavení IP adresy serveru
SendPrefixes=2                       ;prefixy akceptované Asteriskem
AcceptPrefixes=*                     ;prefixy akceptované gatekeeperem

[Neighbor::GK2]                      ;konfigurace souseda
GatekeeperIdentifier=GK2             ;identifikátor
Host=<IP_adresa_gatekeeperu>         ;nastavení IP adresy serveru
SendPrefixes=1                       ;prefixy vysílané gatekeeperem
AcceptPrefixes=*                     ;prefixy akceptované gatekeeperem

[Neighbor::GK3]                      ;konfigurace souseda
Host=<IP_adresa_CallManageru>        ;nastavení IP adresy serveru
SendPrefixes=*                       ;prefixy vysílané gatekeeperem
AcceptPrefixes=*                     ;prefixy akceptované gatekeeperem

[RasSrv::LRQFeatures]                ;definice LRQ
AcceptNonNeighborLRQ=1               ;akceptování    LRQ    neregistrovaných
                                     ;sousedů
 [RasSrv::RRQFeatures]               ;definice parametrů RRQ
AcceptEndpointIdentifier=1           ;akceptování v úplné RRQ zprávě
AcceptGatewayPrefixes=1              ;registrace prefixů s gatekeeperem
```

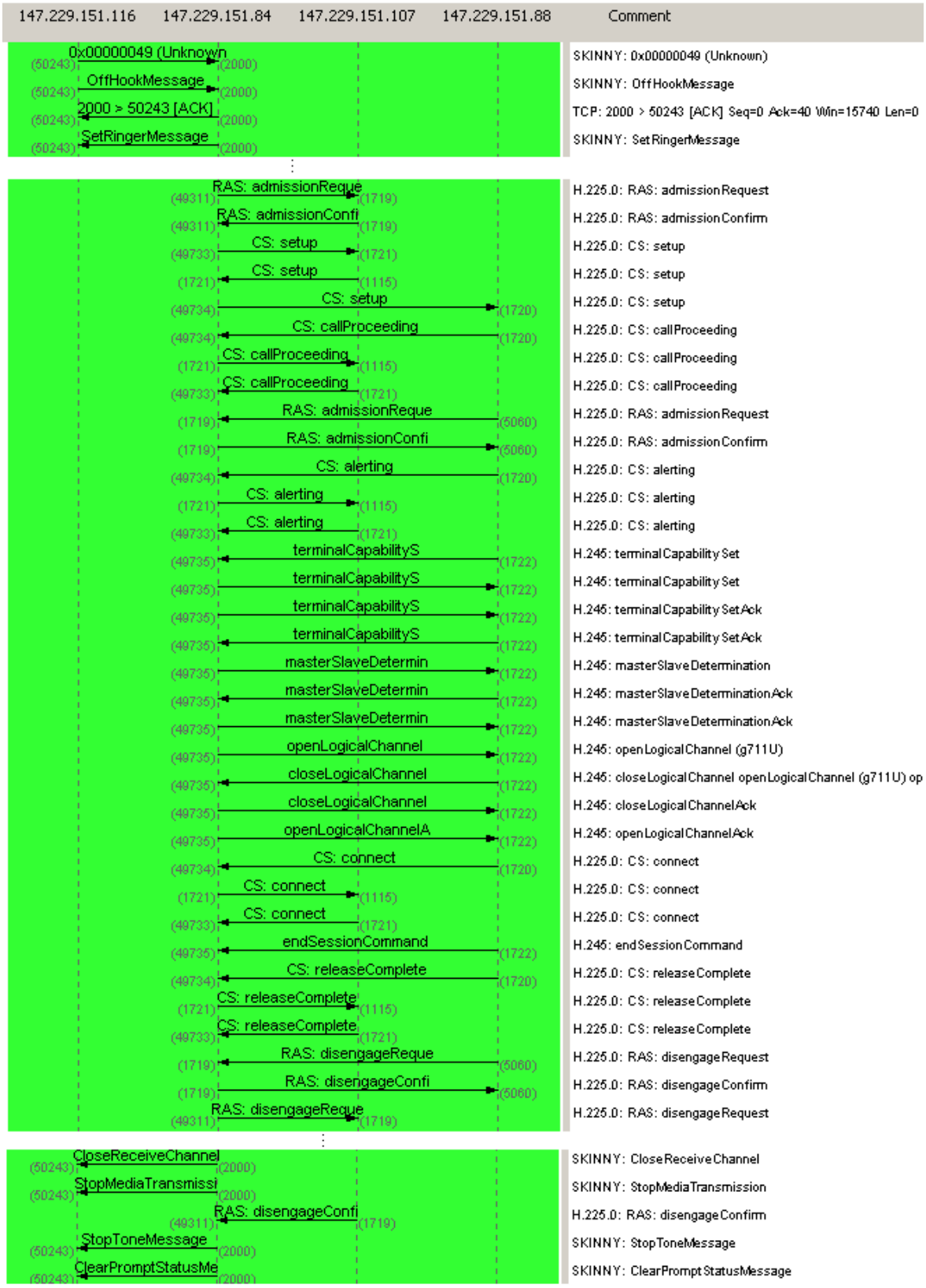
Diagram spojení dvou GNU Gatekeeperů

Následující diagram (Obrázek C. 6) ukazuje propojení dvou H.323 koncových bodů registrovaných u odlišných gatekeeperů. Podle zpráv protokolu H.245 je vidět, že byla zvolena přímá signalizace.

Obrázek C. 6 Propojení H.323 domén detekované pomocí programu Wireshark

Diagram spojení Cisco a H.323

Obrázek C. 7 ukazuje propojení Cisco a H.323 domén pomocí Cisco CallManageru a GNU Gatekeeperu. Jelikož protokol SCCP využívá při navázání a ukončení spojení velké množství zpráv, je diagram zjednodušen.



Obrázek C. 7 Propojení Cisco a H.323 domén detekované pomocí programu Wireshark

Diagram spojení Cisco a SIP

Obrázek C. 8 ukazuje propojení Cisco a SIP domén pomocí Cisco CallManageru a ústředny Asterisk. Jelikož protokol SCCP využívá při navázání a ukončení spojení velké množství zpráv, je diagram zjednodušen.

Obrázek C. 8 Propojení Cisco a SIP domén detekované pomocí programu Wireshark