Analýza komunikace při realizaci VoIP spojení

Tomáš Mácha
Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií,
Ústav telekomunikací, Purkyňova 118, 612 00 Brno, Česká republika
email: tomas.macha@phd.feec.vutbr.cz

Článek popisuje podrobnou analýzu veškeré síťové komunikace realizovaných VoIP spojení experimentálního pracoviště. Pracoviště sloužilo pro přenos hlasu v datových sítích podle architektur H.323, SIP a Cisco. Pro analýzu komunikace mezi jednotlivými prvky při realizaci hovorového spojení byly použity protokolové analyzátory Wireshark a Observer. Je zde uveden přehledný výpis detailních informací jednotlivých paketů a diagramy sestavených spojení.

Úvod

Komunikační standardy a technologie jsou posledních několik let silně ovlivňovány Internetem jako základním komunikačním prostředím. Telefonní služba byla tak zcela logicky postavena do pozice služby poskytované na IP síti. V oblasti IP sítí je pro přenos telefonních hovorů nejrozšířenější technologie VoIP (Voice over IP). VoIP představuje vytvoření sítí s integrovanými službami umožňující 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.

Základní standardy, které jsou podmínkou pro úspěšné začlenění služeb v reálném čase do datových sítí jsou H.323, SIP a Cisco (SCCP). 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.

Na základě získaných poznatků o softwarových serverech, které zajišťují kontrolu nabízených služeb a podporu telefonních funkcí, 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.

S pomocí dostupných spojovacích systémů a koncových zařízení bylo navrženo integrované řešení hovorových služeb podle architektur SIP, H.323 a Cisco. IP architektury představovaly ústřednové řešení, kde spojovací jádro bylo 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. 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. Logickou topologii experimentálního pracoviště obsahující různé typy ústředen a IP telefonů znázorňuje Obrázek 1.

elektrorevue
ISSN 1213 - 1539

Obrázek 1 Logická topologie experimentálního pracoviště VoIP sítě

Analýza komunikace

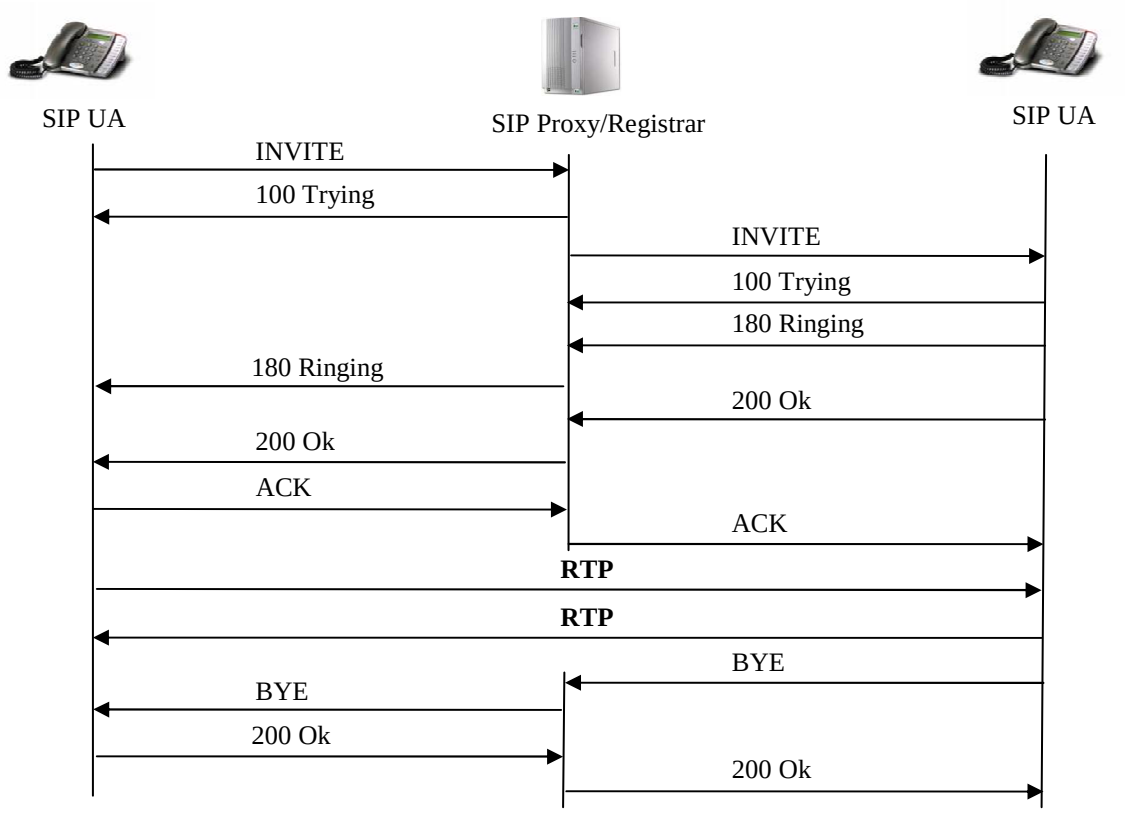
Pro podrobnou analýzu komunikace byly použity protokolové analyzátory Observer a Wireshark. Programy slouží k důkladnému sledování a analýzu veškeré síťové komunikace. Wireshark i Observer dokáží analyzovat jak komunikaci v reálném čase, tak vyhodnocovat uložené logy. Podávají přehledný výpis detailních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

Každý hlasový systém je třeba před samotnou realizací dobře navrhnout s ohledem na mnoho faktorů. Pozornost je věnována struktuře celého komunikačního systému v rámci jedné architektury. Důležitým předpokladem při nasazení různých signalizačních serverů v návrhu VoIP sítě je správná volba signalizačního protokolu. Diagnostika protokolů a sledování síťového provozu je tak zaměřena na jednotlivé architektury.

Signalizace SIP

Textová podstata protokolu SIP umožňuje jednodušší protokolovou analýzu. Zpráva nesená SIP protokolem je tvořena hlavičkou a vlastním tělem zprávy. Obrázek 2 znázorňuje příklad diagramu spojení SIP uživatelů pomocí SIP Proxy (Asterisk).

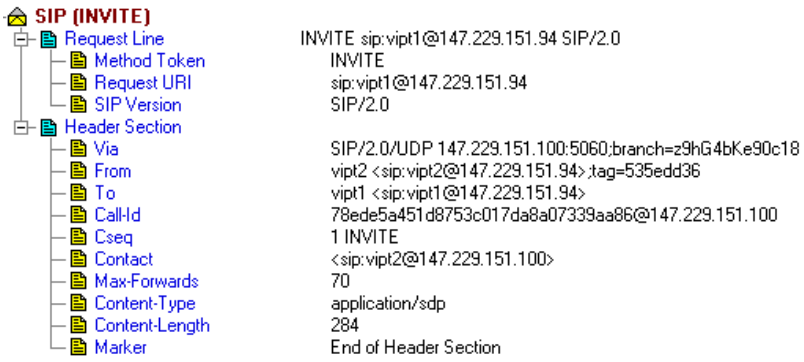
elektrorevue
ISSN 1213 - 1539



Obrázek 2 Diagram spojení SIP uživatelů přes SIP Proxy

Zahájení spojení

Navázání spojení mezi SIP účastníky se děje prostřednictvím ústředny Asterisk. Volající účastník má k dispozici SIP adresu volaného, tato adresa ovšem nevypovídá o aktuálním umístění volaného. Volající koncový bod odesílá žádost o navázání spojení INVITE na proxy server. Zpráva INVITE je přeposílána z jednoho proxy serveru na druhý, dokud nedojde k identifikaci volaného účastníka. Příklad zprávy INVITE ukazuje Obrázek 3.



Obrázek 3 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>

elektrorevue
ISSN 1213 - 1539

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

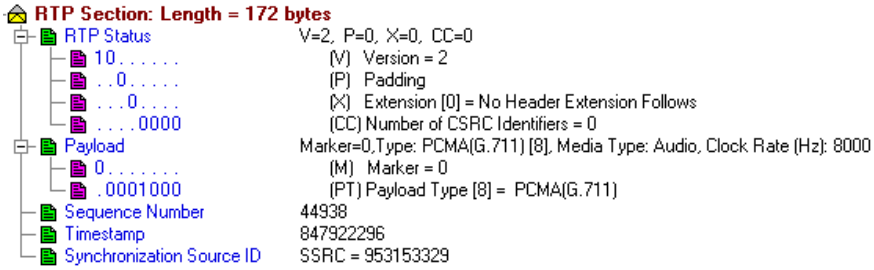
Uvnitř zprávy protokolu SIP pro navázání spojení je zapouzdřena zpráva jiného protokolu, který specifikuje použitá kódování pro multimediální data, jejich parametry a čísla portů, na kterých mají být data vysílána nebo přijímána. Obvykle je pro tento účel použit protokol SDP (Session Description Protocol),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

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)

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 ukazuje Obrázek 4.



Obrázek 4 Tělo RTP paketu detekované programem Observer

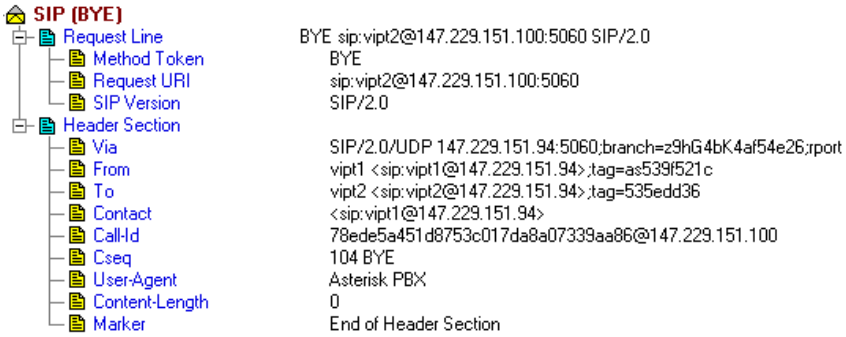
Pole nesoucí parametry protokolu RTP:

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

elektrorevue
ISSN 1213 - 1539

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. Podrobnosti zprávy BYE ukazuje Obrázek 5.



Obrázek 5 Tělo zprávy BYE detekované programem Observer

Signalizace H.323

Standard H.323 je zastřešující standard, kterému jsou podřazeny protokoly zajišťující signalizaci a zabezpečený přenos dat (H.225.0–RAS, H.225.0–Q.931, H.245, H.450, H.235) a protokoly pro přenos multimediálních dat (RTP, RTCP).

Zahájení spojení

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

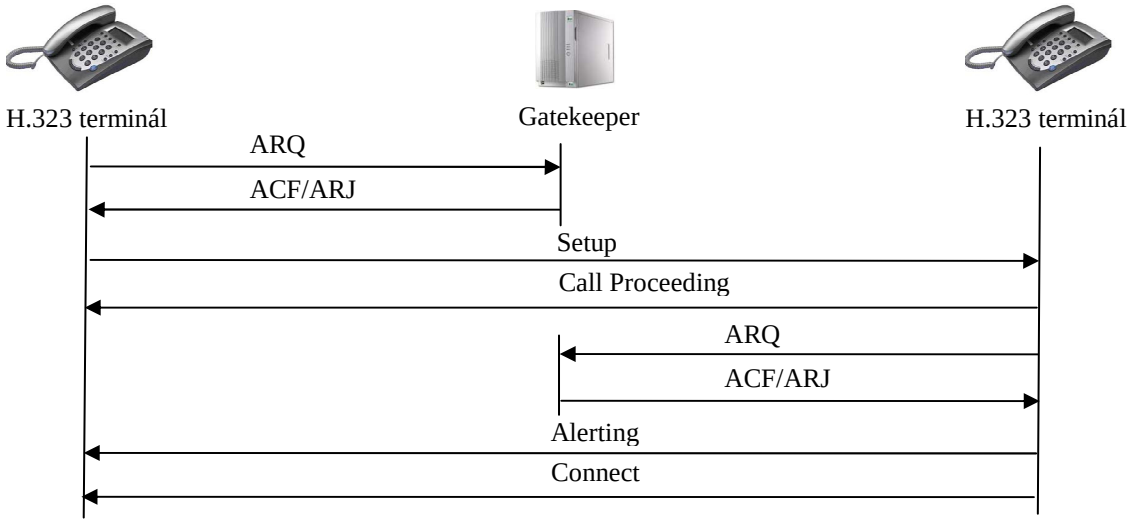
- přímá signalizace (direct call signalling),
- směrová signalizace (routed call signalling).

Pokud gatekeeper zvolí metodu přímého volání (Obrázek 6) pak volající terminál iniciuje signalizační spojení přímo s volaným terminálem. V případě směrového volání (Obrázek 7) je signalizační spojení nejprve navázáno s gatekeeperem a ten následně provede druhé spojení s volaným terminálem. V tomto režimu má gatekeeper větší kontrolu nad průběhem hovoru.

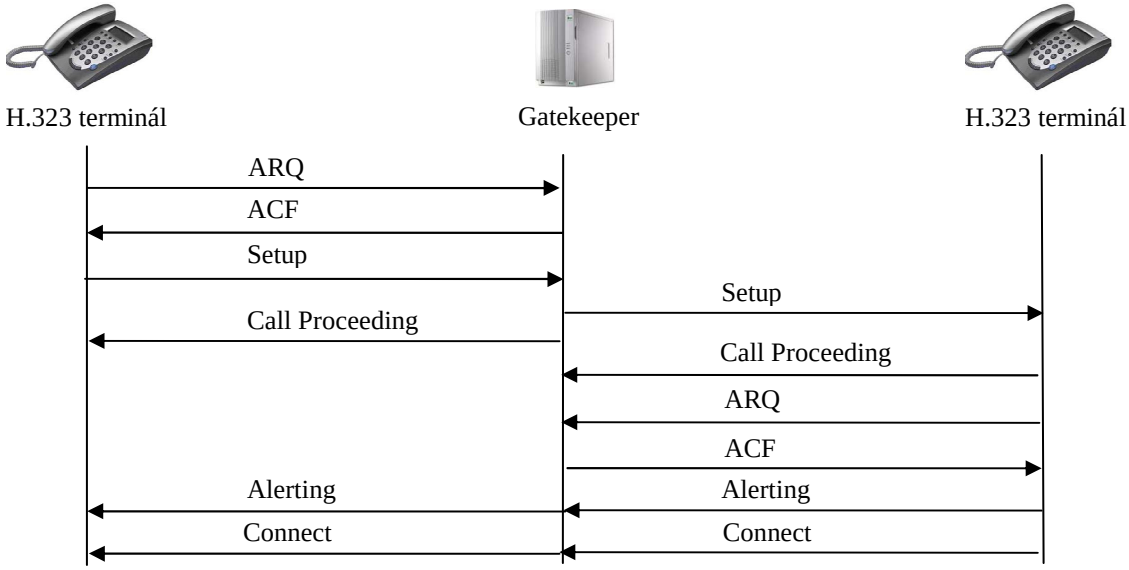
Pro komunikaci terminál–gatekeeper a gatekeeper–gatekeeper využívá standard H.323 protokolu H.225.0 označované jako H.225.0–RAS (Registration, Admission, Status). Protokol obsahuje zprávy určené pro registraci koncového H.323 uživatele na gatekeeperu, sestavení, udržování a ukončení relace. Zprávy protokolu H.225.0–RAS se přenášejí prostřednictvím protokolu UDP. Typické zahájení (Obrázek 6) 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 8) 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.

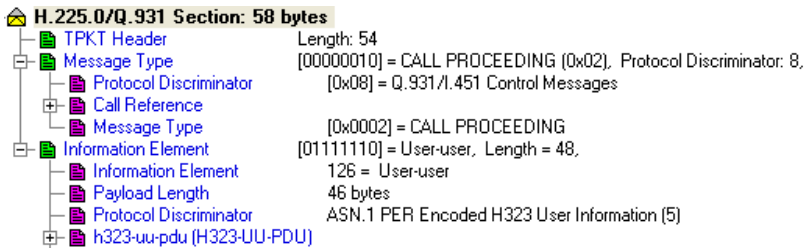
elektrorevue
ISSN 1213 - 1539



Obrázek 6 Diagram zahájení spojení H.323 uživatelů registrovaných ke gatekeeperu s využitím přímé signalizace



Obrázek 7 Diagram zahájení spojení H.323 uživatelů registrovaných ke gatekeeperu s využitím směrování



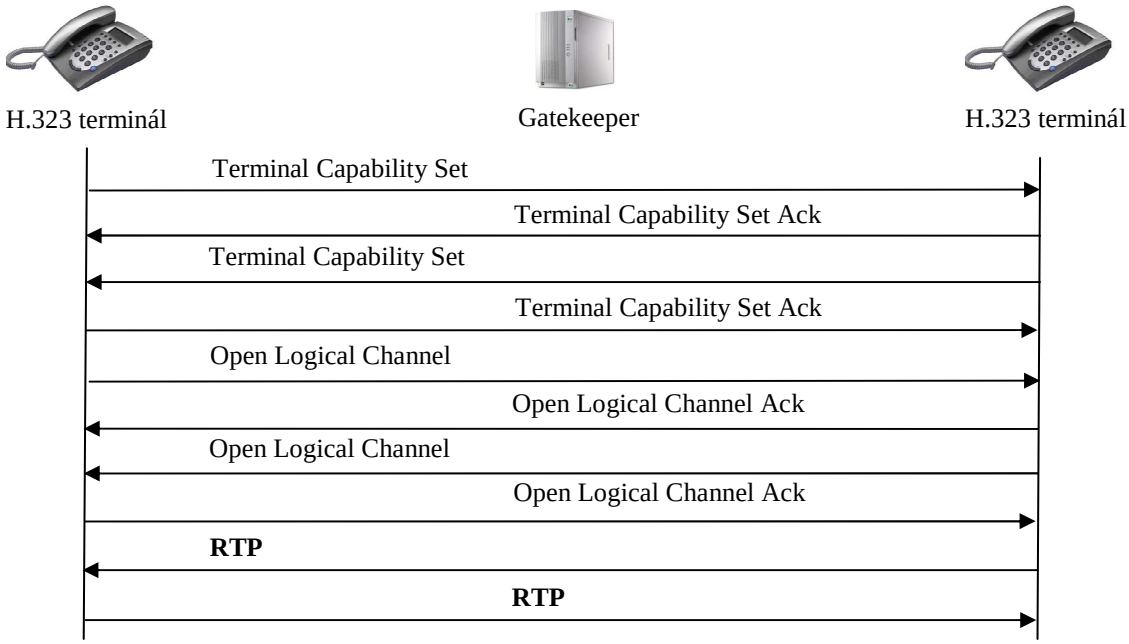
Obrázek 8 Tělo zprávy Call Proceeding detekované programem Observer

elektrorevue
ISSN 1213 - 1539

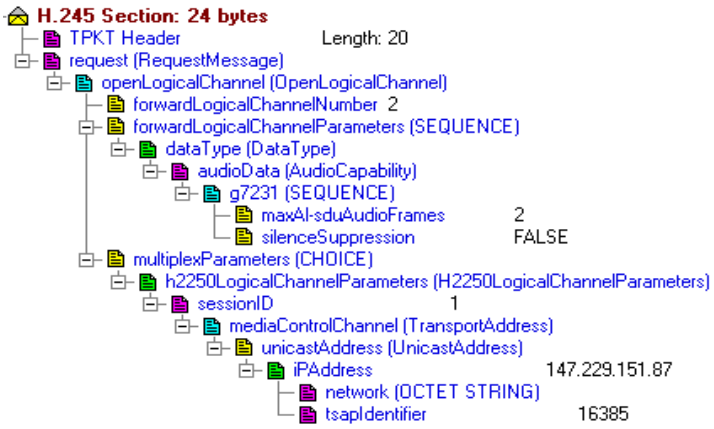
Průběh spojení

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 9 a princip 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 10).
3. Vlastní přenos multimediálních dat zprostředkovává protokol RTP na UDP. K řízení relace a sledování kvality toku slouží protokol RTCP.



Obrázek 9 Diagram průběhu spojení H.323 uživatelů registrovaných ke gatekeeperu



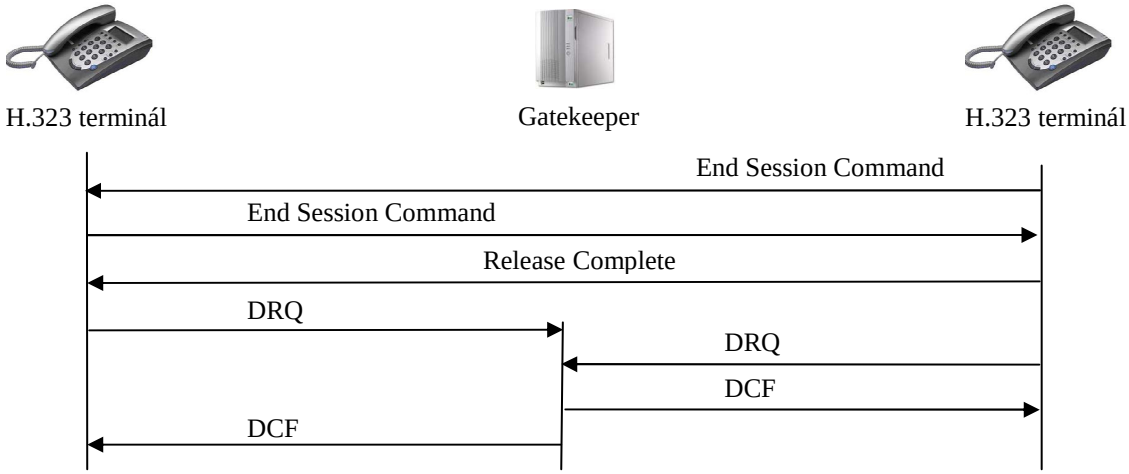
Obrázek 10 Tělo zprávy Open Logical Channel detekované programem Observer

elektrorevue
ISSN 1213 - 1539

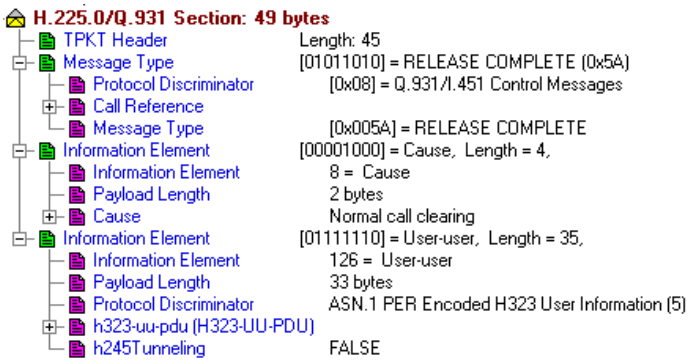
Ukončení spojení

Pro ukončení spojení (Obrázek 11) 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 12).
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 11 Diagram ukončení spojení H.323 uživatelů registrovaných ke gatekeeperu



Obrázek 12 Tělo zprávy Release Complete detekované programem Observer

Signalizace SCCP

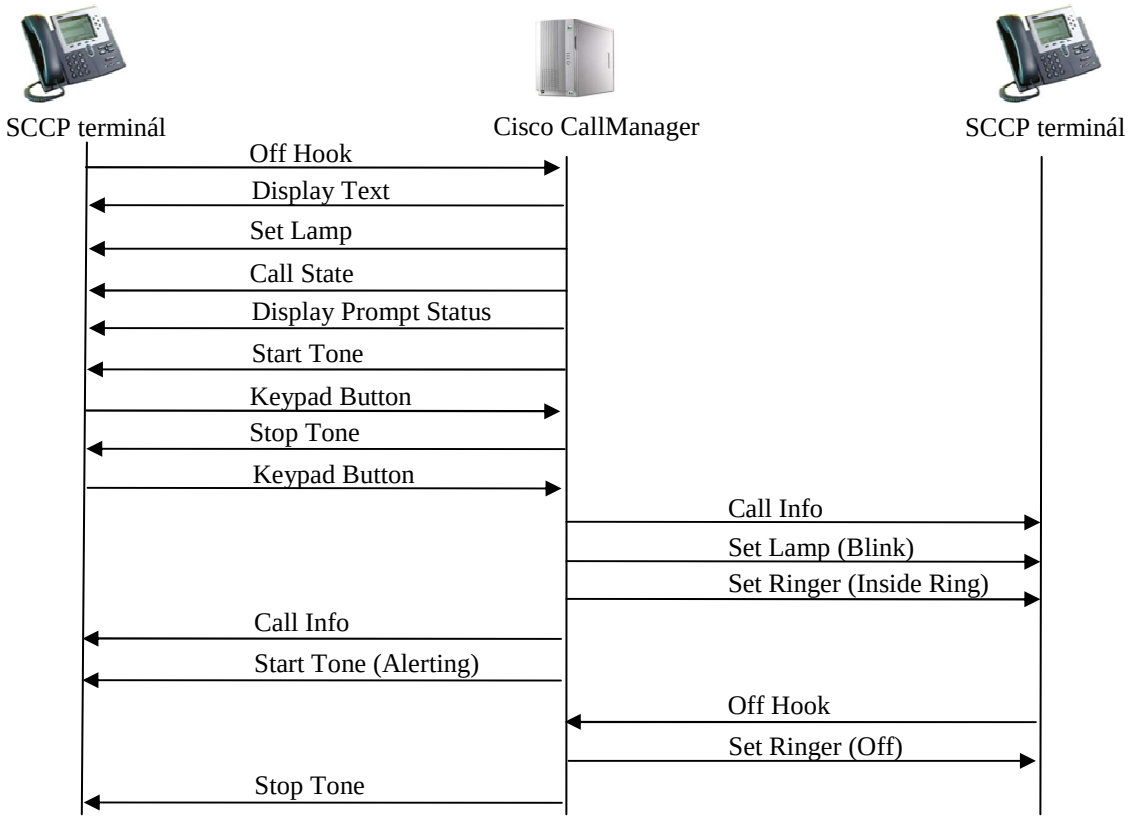
Následuje analýza spojení dvou SCCP uživatelů, kteří jsou zaregistrováni u Cisco CallManageru. Textová podstata protokolu SCCP umožňuje snadnou protokolovou analýzu. Jelikož jsou zprávy protokolu SCCP jednoduché, je nutné pro kompletní signalizaci přenést velké množství zpráv.

elektrorevue
ISSN 1213 - 1539

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 (Obrázek 13) vypadá následovně:

1. Po vyzvednutí sluchátka vysílá telefon zprávu Off Hook (Obrázek 14) 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 13 Diagram zahájení spojení SCCP uživatelů registrovaných u CallManageru

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

Obrázek 14 Tělo zprávy Off Hook detekované programem Wireshark

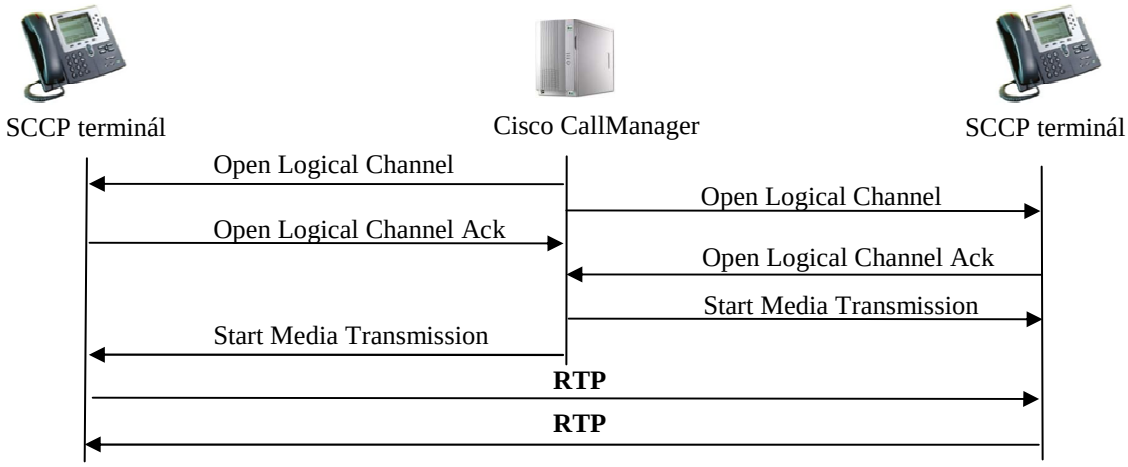
Průběh spojení

Po sestavení spojení následuje fáze otevření logických kanálů. Úkolem CallManageru je připravit obě strany na příjem RTP paketů. Typický průběh spojení dvou SCCP (Obrázek 15) klientů vypadá následovně:

1. CallManager posílá oběma SCCP klientům zprávu o otevření logického kanálu (Open Logical Channel).

elektrorevue
ISSN 1213 - 1539

2. Ve zprávě Start Media Transmission (Obrázek 16) 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 15 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)
```

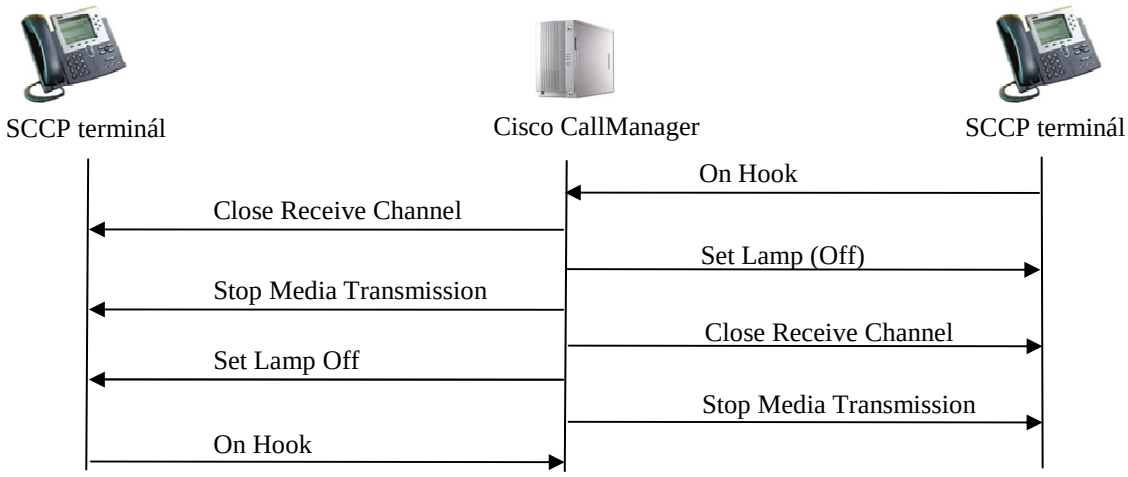
Obrázek 16 Tělo zprávy Start Media Transmission detekované programem Wireshark

Ukončení spojení

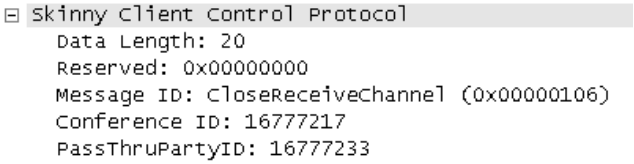
Obrázek 17 ukazuje příklad ukončení spojení dvou SCCP klientů registrovaných u CallManageru. Úkolem CallManageru je uzavírání logických kanálů a přerušení přenosu média. Následuje příklad ukončení spojení mezi SCCP uživateli:

1. Telefon signalizuje ukončení spojení zprávou zavěšení (On Hook).
2. CallManager uzavírá logické kanály vyhrazené oběma koncovým bodům zprávou Close Receive Channel (Obrázek 18) a zastavuje přenos pomocí zprávy Stop Media Transmission.
3. Posledním krokem je uvedení protistrany do zavěšeného stavu (On Hook).

elektrorevue
ISSN 1213 - 1539



Obrázek 17 Diagram ukončení spojení SCCP uživatelů registrovaných u CallManageru



Obrázek 18 Tělo zprávy Close Receive Channel detekované programem Wireshark

Srovnání protokolů SIP, SCCP a H.323

Signalizační protokoly 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.

Mezi výhody protokolů SIP a SCCP patří, že jsou textově orientovány, a tak je jejich čitelnost, zpracování a analýza jednodušší. Ovšem protokolová sada H.323 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. Následující tabulka (Tabulka 1) porovnává parametry protokolů SIP, SCCP, H.323: [4]

Tabulka 1 Srovnání parametrů protokolů SIP, SCCP, H.323

	SIP	SCCP	H.323
standard	otevřený, jednoduchý	otevřený, jednoduchý	uzavřený, složitý
organizace	IETF	Cisco	ITU
typ zpráv	textový	textový	binární
používané servery	SIP Proxy, Redirect, Registrar	CallManager	gatekeeper

elektrorevue
ISSN 1213 - 1539

Závěr

Článek se zabýval analýzou komunikace mezi jednotlivými prvky při realizaci hovorového spojení v IP síti. V práci je uveden přehledný výpis detailních informací paketů jednotlivých architektur. Jednotlivé signalizační postupy pro SIP, H.323 a Cisco při sestavení, průběhu a ukončení spojení jsou zobrazeny v detailních diagramech. Diagramy zajišťují snadnější pochopení principů síťové komunikace. Praktické zkušenosti s analýzou protokolu SCCP ukázaly, že pro kompletní signalizaci je nutné přenést velké množství zpráv, což činí celkovou analýzu nepřehlednou.

Literatura

[1] MÁCHA, T. *Konvergované řešení hovorových služeb*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 77 s. Vedoucí diplomové práce doc. Ing. Vít Novotný, Ph.D.

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

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

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