

SIGNALIZAČNÍ A KOMUNIKAČNÍ PROTOKOLY V IP TELEFONII

Ing. Pavel BEZPALEC

pracoviště: ČVUT FEL, Katedra telekomunikační techniky; mail: bezpalec@fel.cvut.cz

Abstrakt: Článek se zabývá signalizačními a komunikačními protokoly používanými v IP telefonii. Popisuje oba v současné době podporované a používané signalizační protokoly ITU-T H.323 a IETF SIP. Na příkladě ukazuje signalizační postup při sestavení a rušení spojení. Z komunikačních protokolů je uveden protokol RTP s řídicím protokolem RTCP a na příkladě je ukázán princip přenosu dat.

1 Úvod ke signalizačním a komunikačním protokolům v IP telefonii

Účastník A hodlá vyřídít vzkaz účastníkovi B. *Signalizačními protokoly* nejdříve účastník A kontaktuje účastníka B a vzájemně se identifikují, vymění si informace o způsobu, kvalitě a typu vlastního přenosu uživatelské informace, tedy audia, videa či dat (tzv. mediální tok). Po té prostřednictvím některého z *kunikačních protokolů* realizují vlastní přenos mediálního toku, tedy vyřízení vzkazu.

Signalizačními protokoly používanými v IP telefonii jsou

- ITU-T H.323
- IETF SIP

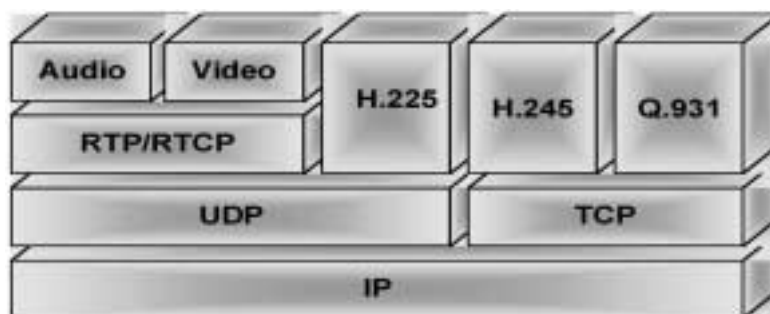
Mezi *kunikačními protokoly* používanými v IP telefonii patří

- Protokol RTP/RTCP

2 Protokol ITU-T H.323

2.1 Úvod k protokolu ITU-T H.323

Protokolový standard ITU-T H.323, viz [1], zastřešuje multimediální komunikaci v takových sítích, které nenabízejí žádnou garanci kvality služeb (QoS – *Quality of Service*), jako je např. síť Internet, typicky všechny sítě založené na protokolu IP. Protokol ITU-T H.323 přitom pokrývá nejen celkovou architekturu, definuje komponenty, ale specifikuje i použití protokolů nižších vrstev. Zabývá se poskytováním audio, video a datových služeb, přičemž povinné jsou pouze služby audio. Lze jej nasadit v jednoduchých segmentech sítí LAN, nebo i ve značně složitých soustavách vzájemně propojených sítích a podporuje i skupinový způsob přenosu (současné vysílání od jednoho zdroje k více příjemcům). Není vázán na žádnou systémovou platformu, a může tedy být nasazen skutečně kdekoli – nejen v klasických počítačových, ale také v různých zařízeních typu IP telefonů apod. Hlavním úkolem tohoto standardu je samozřejmě zajistit vzájemnou kompatibilitu systémů, které nabízejí multimediální přenosy (hlasu, volitelně i obrazu a dat). Je přitom poměrně pružný v tom smyslu, že umožňuje vzájemnou součinnost i mezi takovými systémy, které nemají stejné schopnosti a protokolově vyvrálý, autorsky velmi pečlivě vytvořen a otestován.



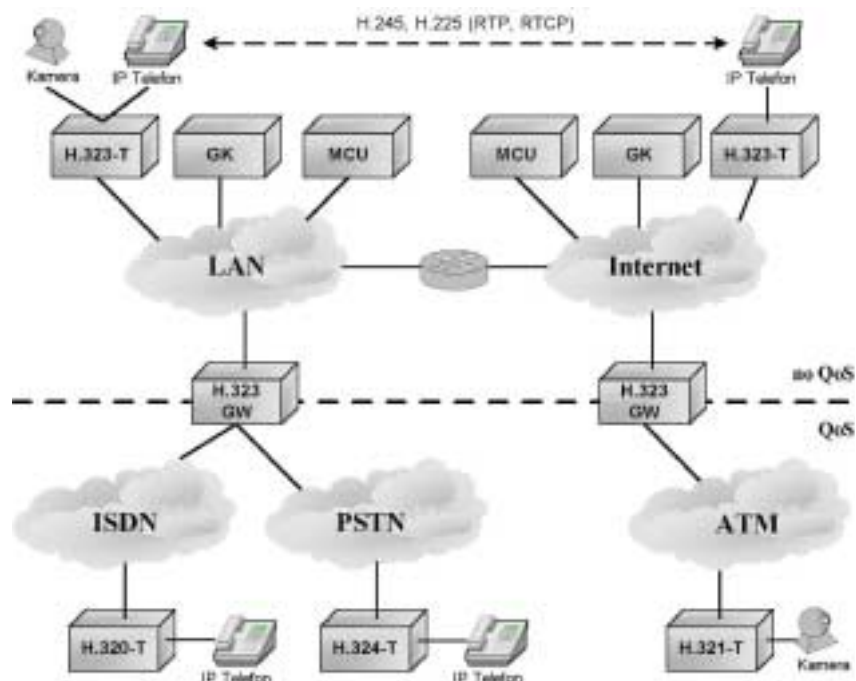
Obr. 1: Protokolová architektura dle ITU-T H.323

Náhled na protokolovou architekturu dle ITU-T H.323 poskytuje obr. 1. Standard H.323 je zastřešující standard, který se odkazuje na celou řadu dílčích standardů pocházejících z dílen ITU-T (Mezinárodní telekomunikační unie). Nejdůležitějšími dílčími standardy k ITU-T H.323 jsou:

- **H.225.0** – *Call signaling protocols and media stream packetization for packet based multimedia communication systems*
 - o Definiuje signalizační zprávy pro sestavení, dohled a rozpad spojení.
- **Q.931** – *ISDN user-network interface layer 3 specification for basic call control*
 - o Definiuje signalizační protokol pro sestavení, dohled a rozpad spojení v síti ISDN.
- **H.245** – *Control Protocol for Multimedia Communications*
 - o Definiuje signalizační zprávy pro vyjednání parametrů přenosového kanálu.
- **H.450.x** – *xxx supplementary service for H.323*
 - o Definiuje signalizaci doplňkových služeb H.323 terminálů.
- **RTP/RTCP** – Real Time Protocol / Real Time Control Protocol
 - o Definiuje vlastní multimediální přenos.
- **H.235** – *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*
 - o Definiuje bezpečnostní a šifrovací procedury pro protokol H.323.
- **E.164** – *The international public telecommunication numbering plan*
 - o Číslování koncových terminálů.

2.2 Architektura a komponenty dle ITU-T H.323

Celkovou možnou architekturu sítě podle standardu H.323 mohou tvořit směrovačem vzájemně propojené sítě LAN a Internet, které negarantují kvalitu přenosu (označeno *no QoS*), viz obr. 2. V tomto prostředí mohou audio/video terminály (*H.323-T*) komunikovat přímo nebo prostřednictvím pomocných uzlů (*GK, MCU*). Protokol ITU-T H.323 umožňuje komunikaci i s jinými typy audio/video terminálů sítí prostřednictvím externí brány (*H.323-GW*) s garantovanou kvalitou služby (*QoS*).



Obr. 2: Architektura sítě podle ITU-T H.323

Standard H.323 patří do rodiny standardů H.32x, které se zabývají multimediálními přenosy v sítích ISDN (H.320), ATM (H.321), v sítích LAN s garantovanou kvalitou služeb (H.322) a v telefonních sítích s negarantovanou kvalitou služeb (H.324).

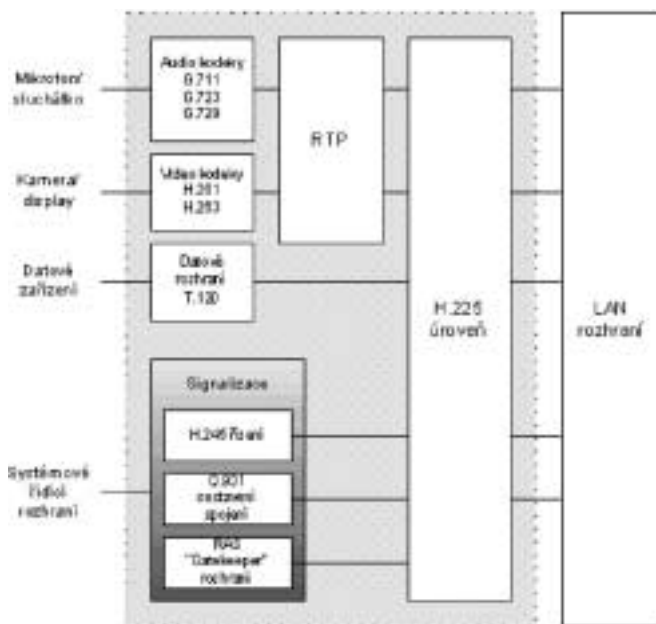
Jednotlivé komponenty sítě dle standardu H.323 jsou, viz obr. 2:

- terminál,
- brána,
- správce zóny,
- jednotka pro řízení konferenčního spojení.

Terminál

Terminál je koncový bod, který umožňuje obousměrnou multimediální komunikaci v reálném čase. Všechny terminály musí podporovat audio komunikaci. Video a datové přenosy jsou nepovinné. K audio zařízením se řadí různé mikrofonní systémy a telefonní zařízení produkující akusticky modulovaný signál. Ten se transformuje ve standardním kodeku G.711 (povinný).

- Doporučené další kodeky jsou G.723.1 a G.729 (pro sítě s užší šířkou pásma).
- Pro řízení komunikace a přenos zakódovaných dat mezi terminály H.323 slouží protokoly H.245 a H.225.
- Podpora pro přenos dat je volitelná dle T.120.
- Obrazové výstupy video zařízení jsou transformovány na data a zpět kodekem H.261.
- Nepovinné části terminálu jsou video kodeky H.261 a H.263.



Obr. 3: H.323 terminál

Terminál bývá implementován počítačem PC vybaveným audio/video zařízením (např. zvukovou kartou, kamerou), nebo přímo IP telefonem.

Brána (Gateway – GW)

Brána zabezpečuje přenos audio/video provozu mezi různými systémy s odlišným protokolovým vybavením, například audio/video terminály sítě garantující kvalitu spojení dle standardů H.320, H.321, H.322, H.324 a H.323.

Brány poskytují následující konverzní funkce mezi dvěma sítěmi:

- Konverze na úrovni fyzického rozhraní a multiplexních struktur – např. Ethernet ↔ ATM
- Konverze formátů – např. G.723 ↔ G.711 (používá se v telefonních sítích)
- Konverze protokolových sad – např. H.323 ↔ SS7 (signalizační systém použitý v telefonních sítích)

Brána může volitelně obsahovat jednotku MCU.

Správce zóny (*Gatekeeper – GK*)

GK provádí řídicí funkce spojení a působí jako administrátor pro zaregistrované terminály. Správci zóny v sítích nejsou nutní, ale pokud jsou použiti, koncové body musí používat jejich služby. Nejčastěji je GK realizován softwarem. GK může být integrován do kterékoli komponenty H.323.

Povinné služby definované doporučením H.323:

- **Překlad adres** – z telefonního čísla, dle ITU-T E.164 (např. 233090025) na IP adresu terminálu (např. 147.32.201.127:1720).
- **Řízení přístupu** – přístup terminálu ke GK může být založen na autorizaci, momentální přenosové kapacitě a několika dalších kritériích. Pokud je řízení přístupu vypnuto, tak jsou přijímány všechny požadavky na spojení.
- **Řízení přenosové kapacity** – zahrnuje provádění požadavků na šířku přenosového pásma. Způsob poskytování šířky pásma a správa šířky pásma závisí na poskytovateli. GK může probíhajícímu hovoru nařídít snížení používané šířky pásma. Všechna tato rozhodnutí závisí na poskytovateli této služby a jsou mimo vliv standardu H.323. Je-li řízení přenosové kapacity vypnuto, tak jsou přijímány všechny požadavky na změnu šířky pásma.
- **Oblastní management** – GK poskytuje doplňkové služby pro terminály, jednotky MCU a brány, které jsou registrovány uvnitř administrativní domény řízené gatekeeperem (tzv. zóna).

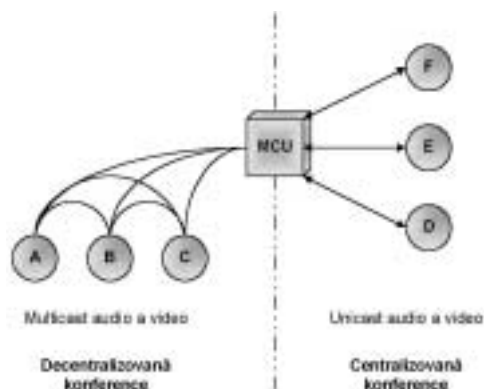
Nepovinné služby definované doporučením H.323:

- **Řízení signalizace spojení** – signalizace je buď realizována GK nebo přes GK transparentně prochází a je pouze monitorována.
- **Autorizace hovoru** – na základě pravidel GK rozhodne, zda potvrdí nebo odmítne daný hovor.
- **Správa hovoru** – GK může poskytovat inteligentní správu hovoru. Např. pokud je terminál obsazen hovorem může hovor přeměrovat, nebo se nebude pokoušet uskutečnit hovor s obsazeným terminálem a tím ušetří čas potřebný k sestavení hovoru. Správa hovorů může být založena na funkcích překladu adres, které poskytují monitorování hovorů, zasílání nebo přeměrování hovorů a směrování hovorů.

Jednotka pro řízení konferenčního spojení (*Multipoint Control Unit – MCU*)

Jednotka MCU umožňuje konferenci mezi třemi a více terminály a zároveň určuje přenosové vlastnosti konference (např. volba kodeku). Umožňuje převádět decentralizované konferenční spojení (data jsou určena skupině stanic) na spojení centralizované (data jsou určena právě jedné cílové stanici) a obráceně, viz obr. 4. Jednotka MCU se skládá z modulů MP a MC:

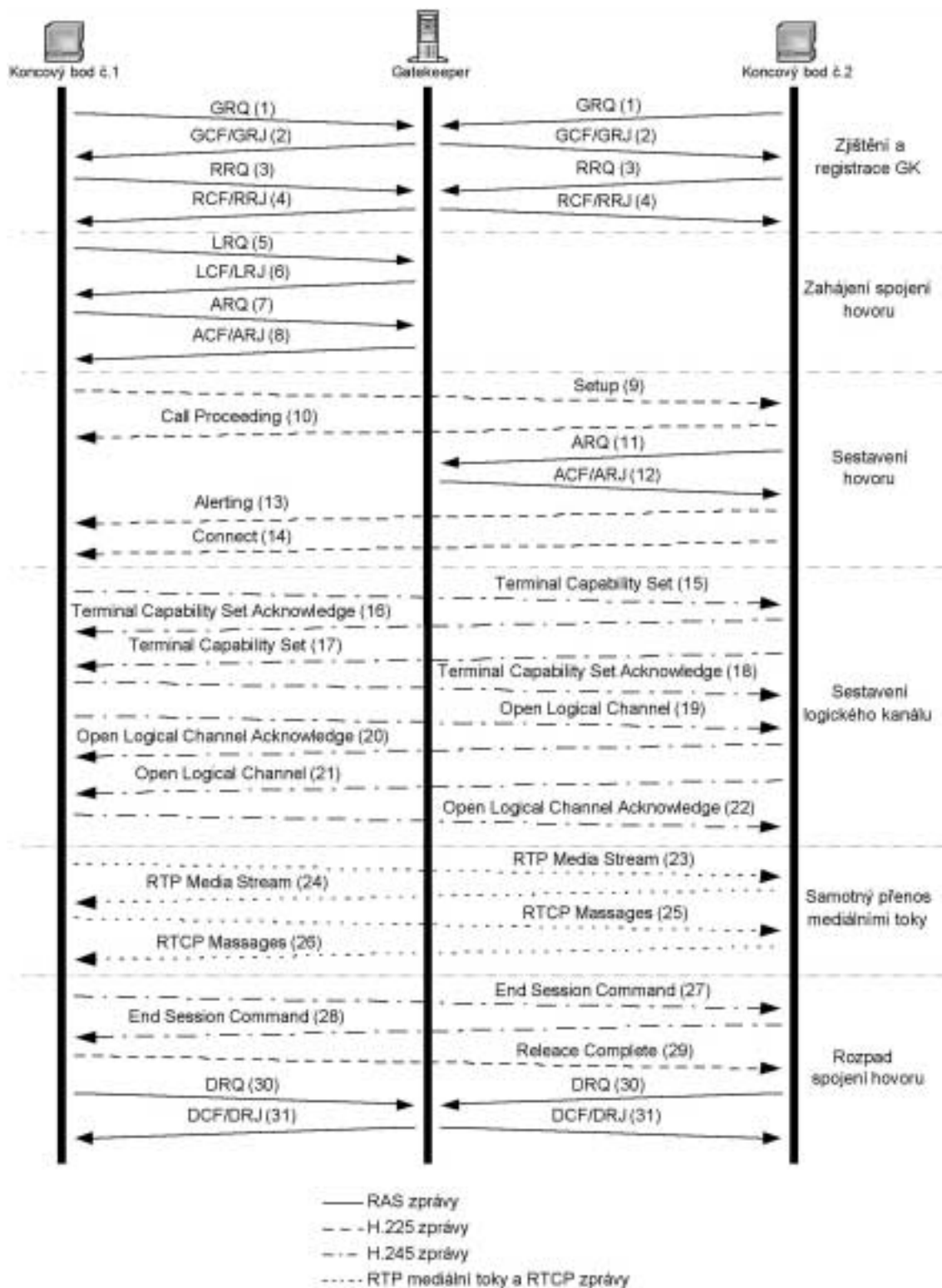
- **MC (*Multipoint Controller*)** – řídí sestavování konference tj. zjišťuje vlastnosti terminálů v konferenci, inicializuje a ukončuje kanály pro audio, video a datové přenosy.
- **MP (*Multipoint Processor*)** – zpracovává multimediální data přenášena v konferenci. MP je volitelný modul. Pokud jsou MP použity, tak mohou být umístěny samostatně v síti (i mimo jednotku MCU).



Obr. 4: Decentralizovaná a centralizovaná konference

2.3 Příklad signalizace dle ITU-T H.323

Příklad signalačního postupu při sestavení a rozpadu spojení dle protokolu standardu H.323 a jeho dílčích částí znázorňuje obr. 5.



Obr. 5: Signalační postup při sestavení a rozpadu spojení dle ITU-T H.323

2.4 Vývoj standardu H.323

První verze tohoto standardu byla schválena v roce 1996 Studijní skupinou č. 16 v rámci ITU-T pod názvem „*Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service*“. V lednu 1998 pak byla přijata již druhá verze tohoto standardu, s poněkud zjednodušeným a zpřesněným názvem „*Packet-based multimedia communication systems*“. Tato změna názvů napovídá, že standard H.323 původně vznikl odděleně od snah telefonie po Internetu, ale teprve později byl dopracován pro potřeby IP telefonie. Používá se však i pro potřeby vedení videokonferencí po počítačových sítích. Další verze, v pořadí již třetí byla schválena 30. září roku 1999 a přináší určitá vylepšení oproti druhé verzi. V současné době je aktuální jeho pátá verze ze srpna roku 2003.

H.323 – verze 1

Standard H.323v1 rozeznává čtyři hlavní části komunikačních systémů fungujících v síťovém prostředí:

- **Terminál** (*Terminal*) – koncový uzel umožňující oboustrannou komunikaci v reálném čase.
- **Brána** (*Gateway – GW*) – je nepovinná a slouží k propojení s principiálně odlišnými sítěmi.
- **Správce** (*Gatekeeper – GK*) – je nepovinný a jeho funkcí je řízení provozu v H.323 síti a překlad adres.
- **Jednotka pro řízení konferenčního spojení** (*Multipoint Control Unit – MCU*) – zajišťuje fungování přenosů konferenčního charakteru (tj. mezi více účastníky současně).

H.323 – verze 2

V první verzi standardu H.323 se příliš neuvažovalo o potřebách internetové telefonie, ale spíše o obecnějších potřebách videokonferencí v prostředí počítačových sítí. Později, když se internetová telefonie stala aktuální, bylo potřeba některé věci dopracovat. Konkrétně šlo o otázky *zabezpečení, zrychleného navazování spojení* či *větší integraci s datovými službami*. V otázce zabezpečení šlo například o autentifikaci volajících, utajení hovoru atd. Dalším problémem bylo zrychlené navazování spojení. V původní verzi se nejprve navázalo spojení mezi terminály a pak teprve se dohadovaly parametry multimediálního přenosu; ve verzi 2 se obojí děje paralelně. Dále verze 2 přináší rozšíření o přenosy faxu, kódování videa, konferenční spojení využívající všesměrového (broadcastového) adresování a doplňkové služby jako identifikace volajícího, přesměrování volání.

H.323 – verze 3

Verze 3 byla přijata v září 1999 a přinesla několik důležitých vylepšení do hlavního doporučení. Většina změn se týkala doplňkových služeb (parkování hovoru, čekající volání, čekající zprávy), rozšíření o potřeby správy a dohledu a spolupráce mezi GK a mechanismy rychlého sestavování spojení v paketových sítích.

H.323 – verze 4

Verze 4 přinesla mnoho vylepšení, týkající se zejména spolehlivosti, rozšiřitelnosti, pružnosti a dalšího rozšíření doplňkových služeb. Zavádí do H.323 konceptu rysy použité v protokolu HTTP (řízení, URL) Tato verze byla přijata v listopadu 2000.

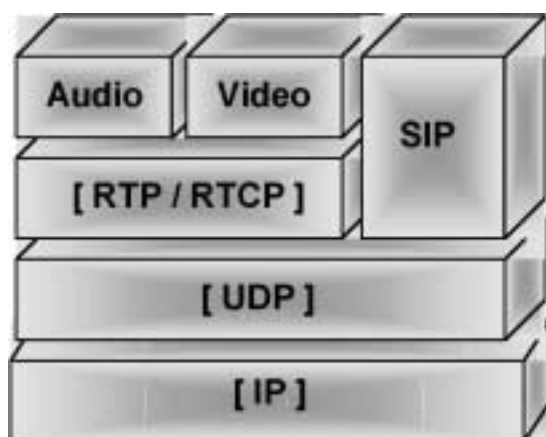
H.323 – verze 5

Verze 5 z května 2003 přináší změnu v sestavení, dohledu a rozpadu spojení dle H.225.0, vylepšenou spolupráci s GK (úprava časování) a obecné přihlašovací mechanismy.

3 Protokol SIP

3.1 Úvod do protokolu SIP

Protokol SIP (*Session Initiation Protocol*) [7] byl vytvořen pracovní skupinou MMUSIC v rámci organizace IETF (*Internet Engineering Task Force*). Je signalizačním protokolem pro sestavení, dohled a rozpad spojení mezi dvěma a více účastníky komunikace. Na rozdíl od protokolu dle standardu H.323 je SIP textově orientovaný, svojí strukturou podobný protokolu HTTP, používanému službou WWW.



Obr. 6: Protokolová architektura dle IETF SIP

Protokol SIP nespécifikuje jaký má být použit transportní protokol a není svázán s žádnými konkrétními komunikačními protokoly pro vlastní přenos multimediálních dat., viz obr. 6 – v hranatých závorkách jsou označeny obvykle používané protokoly RTP, RTCP, UDP a IP. Uvnitř signalizační zprávy protokolu SIP je proto 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 se pro tento účel používá protokol SDP (*Session Description Protocol*) [7], který je rovněž textový.

3.2 Architektura a komponenty sítě SIP

Celkovou možnou architekturu sítě podle IETF SIP mohou tvořit směrovači vzájemně propojené sítě, viz obr. 7. V tomto prostředí mohou audio/video terminály (*SIP terminál*) komunikovat přímo nebo prostřednictvím pomocných uzlů (*zástupný server*, *server přesměrování*).



Obr. 7: Architektura sítě dle IETF SIP

Protokol SIP obsahuje následující komponenty dle architektury zobrazené na obr. 7:

- **UAC** (*User Agent Client*) – klient v koncovém zařízení, který iniciuje SIP signalizaci.
- **UAS** (*User Agent Server*) – server v koncovém zařízení, který reaguje na SIP signalizaci od UAC, provádí přesměrování nebo odmítnutí hovorů.
- **UA** (*User agent*) – koncové zařízení SIP sítě. Stará se o navazování spojení s ostatními UA. Nejčastěji se jedná o SIP telefony nebo brány do jiných sítí. Obsahuje UAC a UAS.

- **SIP Terminál** – podporuje obousměrnou komunikaci s jinou SIP entitou v reálném čase. Podobně jako H.323 terminály SIP terminály podporují jak signalizační tak komunikační protokoly. Obsahuje UAC.
- **Zástupný server (Proxy Server)** – přijme žádost o spojení od UA nebo od jiného proxy serveru a předá ji dalšímu proxy serveru (pokud volanou stanicí nemá ve své správě) nebo přímo volanému UA pokud je tento v rámci jím spravované domény.
- **Server přesměrování (Redirect Server)** – přijímá žádosti o spojení od UA nebo proxy serverů, ale nepřeposílá je dále ve směru volaného, nýbrž posílá tazajícímu zpět informaci, komu má žádost poslat, aby se dostala k volanému.
- **Server umístění (Location Server)** – přijímá registrační žádosti od UA a aktualizuje podle nich databázi koncových zařízení, které jsou v rámci domény spravovány.

Jakkoliv jsou SIP servery definovány odděleně, v praxi se často jedná o jednu aplikaci, která přijímá registrace koncových uzlů a podle konfigurace se chová zároveň buď jako zástupný (*proxy*) nebo server přesměrování (*redirect*).

Klienti a servery si posílají požadavky pomocí takzvaných metod. Jedná se o zprávy v textovém formátu; šesti základními metodami jsou

- **INVITE** – slouží k žádosti o sestavení spojení
- **ACK** – potvrzení INVITE finálním příjemcem zprávy (volaným)
- **BYE** – ukončení spojení
- **CANCEL** – ukončení nesestaveného spojení
- **REGISTER** – registrace UA
- **OPTIONS** – dotaz na možnosti a schopnosti serveru

Další metody jsou předmětem samostatných RFC nebo draftů.

Odpovědi na SIP metody jsou zprávy uvedené číselným kódem. Systém kódů je převzat z HTTP protokolu. Číselné kódy odpovědí jsou členěny do šesti skupin:

- **1XX** – informační zprávy (např. *100 Trying*, *180 Ringing*)
- **2XX** – úspěšné ukončení žádosti (*200 OK*)
- **3XX** – přesměrování, dotaz je třeba směřovat jinam (*302 Moved Temporarily*, *305 Use Proxy*)
- **4XX** – chyba, dotaz by se neměl ve stejné podobě opakovat (*403 Forbidden*)
- **5XX** – chyba na serveru (*500 Server Internal Error*, *501 Not Implemented*)
- **6XX** – globální selhání (*606 Not Acceptable*)

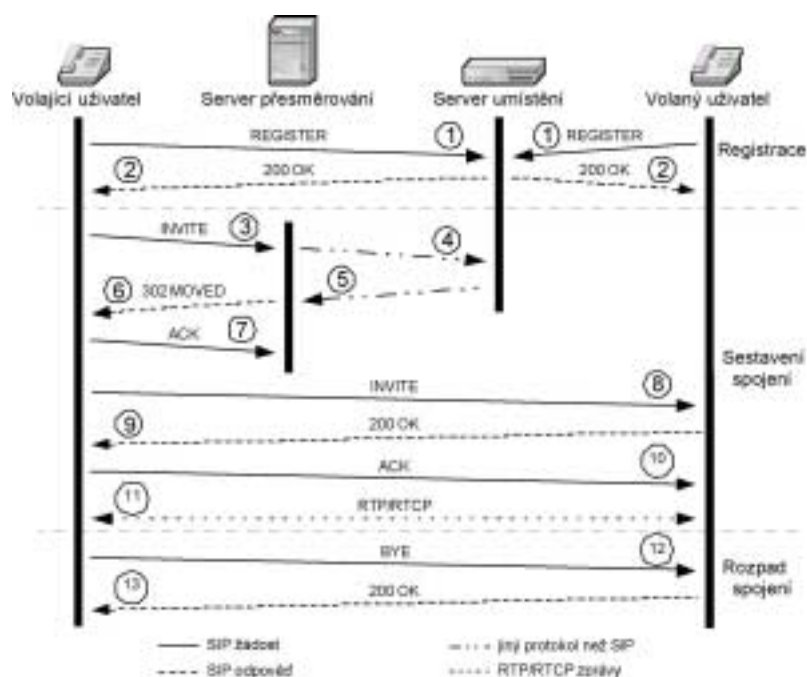
3.3 Příklad signalizace dle IETF SIP

Příklad signalizačního postupu při registraci, sestavení a rozpadu spojení dle protokolu IETF SIP je znázorněn na obr. 8.

3.4 Vývoj IETF SIP

Historický vývoj signalizačního postupu SIP lze shrnout do následujících bodů

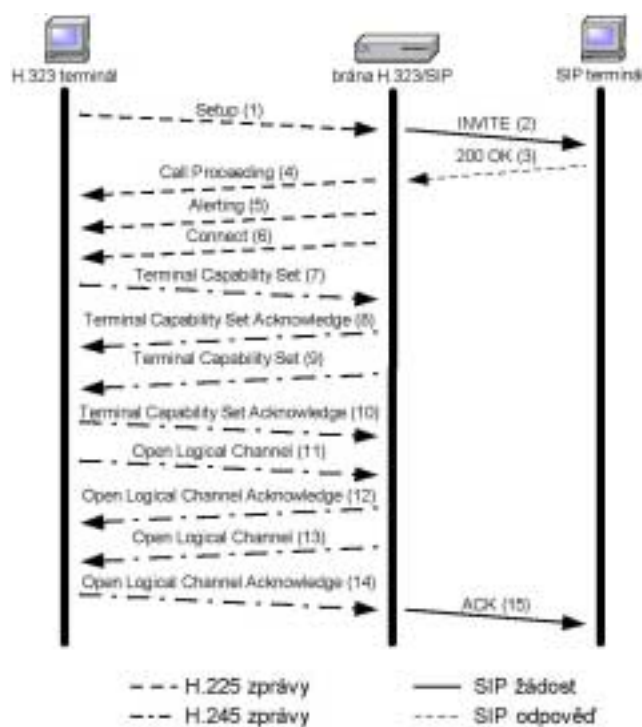
- 1995: počátek práce pracovní skupiny MMUSIC v rámci IETF
- 02/1996: první dokument „*draft-ietf-mmusic-sip-00*“: 15 stran textu, 1 metoda žádosti
- 12/1996: další dokumenty „*draft-ietf-mmusic-sip-01*“ 30 stran textu, 2 metody žádostí
- 01/1999: další dokumenty „*draft-ietf-mmusic-sip-12*“ 149 stran textu, 6 metod žádostí
- 03/1999: dokument RFC 2543, 153 stran textu, 6 metod žádosti
- 11/1999: založena pracovní skupina SIP
- 11/2000: další dokument „*draft-ietf-sip-rfc2543bis-02*“, 171 stran textu, 6 metod žádostí
- 04/2001: oznámeno proposal for splitting SIP WG into SIP and SIPPING
- 2001: široké rozšíření implementace SIPu



Obr. 8: Signalizační postup při sestavení a rozpadu spojení dle IETF SIP

4 Střet světů dle ITU-T H.323 a IETF SIP

Zařízení pracující s protokolem SIP mohou komunikovat se zařízeními pracujícími s protokolem H.323 pomocí brány SIP/H.323. Tato brána převádí signalizační zprávy obou protokolů. Protože pro vlastní přenos multimediálních dat používají zařízení typu H.323 i SIP obvykle protokol RTP, mohou po navázání spojení prostřednictvím brány dále komunikovat přímo. Obdobně mohou zařízení pracující s protokolem SIP komunikovat s telefony v telefonní síti (PSTN – *Public Switched Telephone Network*) pomocí brány SIP/PSTN. Porovnání signalizace pro sestavení spojení mezi H.323 terminálem a SIP terminálem prostřednictvím brány H.323/SIP ukazuje obr. 9.



Obr. 9: Spojení z H.323 terminálu na SIP terminál

Následující tabulka tab. 1 porovnává parametry výše zmíněných signalizačních postupů.

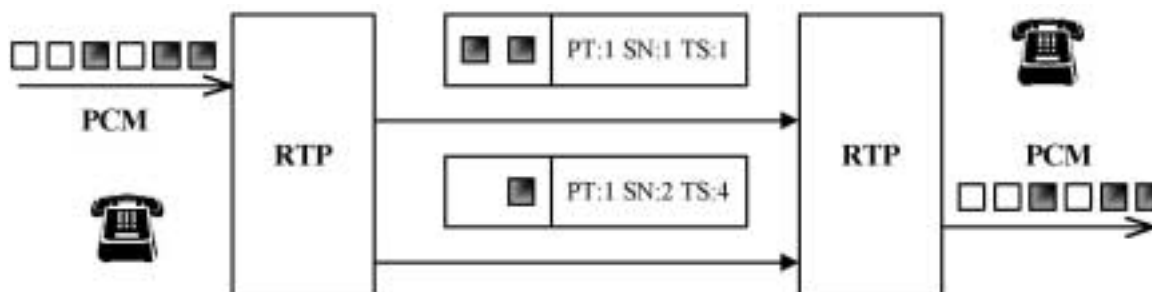
| | H.323 | SIP |
|----------------------|--|---|
| Standard, protokol | Uzavřený, složitý | Otevřený, jednoduchý |
| Organizace | ITU-T | IETF |
| Adresace | Vytvořený pro LAN – zaměřený na lokální provoz | Řešení adresace pro mezinárodní provoz |
| Typ zpráv | Binární, založené na ASN.1 | Textová typ žádost – odpověď |
| Používané protokoly | H.245, H.225 (Q.931, RAS) | SDP |
| Používané servery | Správce zóny (<i>Gatekeeper</i>) | Registrační server (<i>Registrar Server</i>) Zástupný server (<i>Proxy Server</i>) Přesměrovací server (<i>Redirect Server</i>) Server umístění (<i>Location Server</i>) |
| Transportní protokol | RTP s řídicím protokolem RTCP | RTP s řídicím protokolem RTCP |
| Zabezpečení | Nese odpovědnost za spolehlivost přenosu – zbytečná režie | Přenechává zabezpečení přenosu paketů nižším přenosovým vrstvám |
| Rozšíření protokolu | Rozšíření jsou závislá na specifikaci výrobce – nestandardní rozšíření | Povoluje rozšíření základu protokolu pro speciální funkce |

Tab. 1: Porovnání SIP a H.323

5 Protokoly RTP/RTCP

RTP (*Real Time Protocol*) je protokol sloužící pro přenos dat v reálném čase (RFC 1889) [7]. Obvykle se používá pro přenos audio a video provozu mezi koncovými procesy VoIP terminálů. Protokol sám o sobě nezaručuje přenos dat v reálném čase, disponuje jen procedurami, které umožňují rekonstrukci těchto vlastností na straně přijímacího procesu.

V záhlaví protokolu jsou přenášeny informace o typu přenášených dat, způsobu kódování, zdroji synchronizace, jakož i sekvenční číslo paketu a časová značka pro obnovu synchronizace a real-time vlastností. Příjemný proces prostřednictvím sekvenčních čísel paketů zabezpečuje interpretaci dat z paketů RTP ve správném pořadí. Podle definovaného prostředku synchronizace umožní časová značka v každém paketu načtení dat z paketů v odpovídajících časových intervalech.



Obr. 10: Příklad použití protokolu RTP při audio přenosu

Příklad činnosti protokolu RTP naznačuje obr. 10, na kterém je symbolicky vysvětlen přenos audio dat. Hlasový tok je transformován kodekem dle ITU-T G.711 do PCM vzorků s opakovací frekvencí 8000 Hz (v záhlaví RTP paketu to označuje pole *PT* – *payload type*). Vzorky jsou přenášeny ve dvou RTP paketech.

Časovou značkou je v tomto případě pořadové číslo prvního vzorku PCM v paketu RTP (*SN – sequence number*). V datové části se přitom prázdné vzorky PCM nepřenášejí, čímž se šetří šířka pásma sítě. Prostřednictvím časových značek (*TS – time stamp*) přijímač zabezpečuje synchronní načtení dat v přijímacím zařízení a doplnění prázdných vzorků.

Protokol RTP definuje i mezilehlé zařízení (tzv. RTP mixéry), umožňující multiplexování kanálů RTP a obnovování časových vlastností signálu mimo koncové body sítě.

RTCP (Real Time Control Protocol)

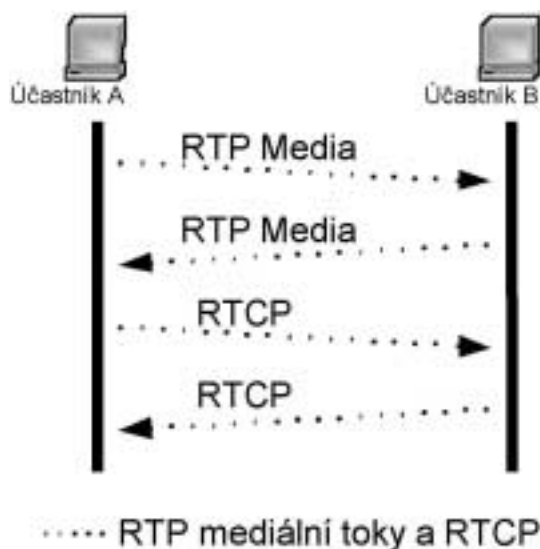
RTCP je řídicí protokol spolupracující s protokolem RTP, používající periodické vysílání paketů od každého účastníka relace RTP všem ostatním účastníkům za účelem řízení výkonnosti a pro diagnostické účely. RTCP vykonává následující služby:

- poskytuje informace aplikaci týkající se kvality vysílaných dat
- identifikuje zdroj RTP
- provádí řízení intervalu vysílání RTCP
- přenos minimální informace o řízení relace

Samotný přenos mediálními toky

Mediální toky jsou během VoIP spojení řízeny pomocí RTCP. Jedná se o řídicí protokol spolupracující s protokolem RTP, který se používá za účelem řízení výkonnosti a pro diagnostické účely. RTCP používá pro každý RTP mediální tok vyhrazený logický kanál.

Příklad přenosu mediálními toky RTP s jejich řídicími zprávami RTCP mezi dvěma komunikujícími uživateli znázorňuje obr. 11:



Obr. 11: Příklad přenosu mediálních toků pomocí RTP/RTCP

Literatura

- [1] ITU-T: *H.323 – Packet Based Multimedia Communication Systems*. ITU-T Study Group 16, červenec 2003.
- [2] ITU-T: *Q.931 – ISDN user-network interface layer 3 specification for basic call control*. ITU-T Study Group 11, květen 1998.
- [3] ITU-T: *H.225.0 – Call signaling protocols and media stream packetization for packet based multimedia communication systems*. ITU-T Study Group 16, červenec 2003.

- [4] ITU-T: *H.235 – Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*. ITU-T Study Group 16, srpen 2003.
- [5] ITU-T: *H.245 – Control protocol for multimedia communication*. ITU-T Study Group 16, červenec 2003.
- [6] ITU-T: *E.164 – The international public telecommunication numbering plan*. ITU-T Study Group 2, říjen 2003.
- [7] BERNERS-LEE, T. – FIELDING, R. – FRYSTYK H.: *Hypertext Transfer Protocol -- HTTP/1.0*. RFC 1945, IETF NWG, květen 1996.
- [8] ROSENBERG, J. et al.: *SIP: Session Initiation Protocol*. RFC3261, IETF STD 1, březen 1999.
- [9] HANDLEY, M – JACOBSON, V.: *SDP: Session Description Protocol*. RFC 2327, IETF STD 1, leden 1998.
- [10] SCHULZRINNE, H. et al: *RTP: A Transport Protocol for Real-Time Application*. RFC 1889, IETF STD 1, leden 1996.
- [11] SCHULZRINNE, H. et al: *Real Time Streaming Protocol (RTSP)*. RFC 2426, IETF NWG, duben 1998.
- [12] SCHULZRINNE, H.: *Internet Technical Resources* [online]. c1999-2003, poslední aktualizace 2003-09-25 [cit. 2004-05-03]. Dostupné z: <<http://www.cs.columbia.edu/~hgs/internet/>>.