

Úvod do VoIP

VoIP systémy patří k nejnovějším technologiím v oblasti komunikace. Kapacita internetových spojů se každoročně zdvojnásobuje a tak VoIP se dostává z laboratoří do běžného života. Připravili jsme pro vás úvod, který vás seznámí s možnostmi a principy VoIP technologií.

Co je to VoIP

[Využití IP telefonie](#)

Přenos hlasu a kodeky

Architektura a protokoly

[Architektury sítí VoIP](#)

[Protokoly využívané ve VoIP](#)

Protokol H.323

[Komponenty definované protokolem](#)

[Propojení komponent](#)

[Struktura protokolu](#)

[Příklady průběhu spojení](#)

Protokol SIP

[Komponenty](#)

[Komunikace komponent a identifikace](#)

Porovnání protokolů H.323 a SIP

Protokol RTP a RTCP

Hardware

[Hlasová brána](#)

[Call Manager](#)

[IP telefony](#)

Implementace v distribuovaném prostředí

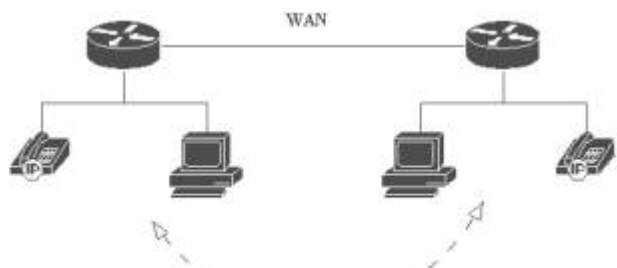
Co je to VoIP

VoIP umožňuje přenos hlasu v sítích s přepojováním paketů založených na protokolu IP. VoIP tak tvoří alternativu ke klasické telefonii, založené na použití sítí s přepojováním okruhů přes veřejnou telefonní síť. Tato alternativa je velice perspektivní a to hned z několika důvodů.

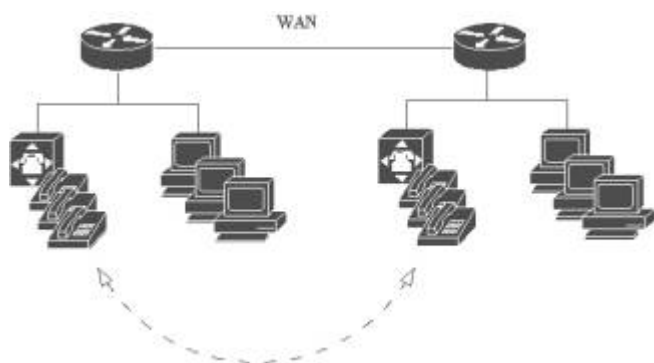
Datové sítě se v současnosti rozvíjejí a šíří mnohem rychleji než telefonní sítě. Přenos hovorů v datových sítích je ekonomicky výhodný, protože rozsáhlé a geograficky rozdělené společnosti mohou uskutečňovat hlasový provoz po vlastních datových sítích, jimiž většina společností disponuje. Připojení operátora poskytujícího na IP konektivitu i hlasové služby logicky vede k nižším cenám, neboť jsou redukovány náklady na komunikační infrastrukturu.

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

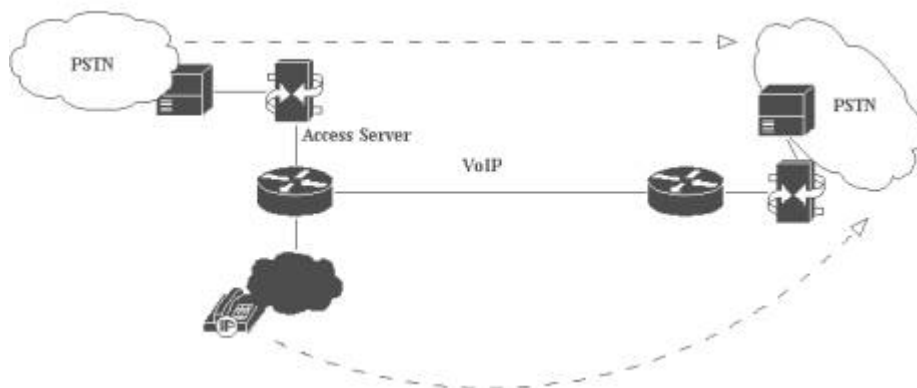
Využití IP telefonie



Toto využití lze označit jako scénář IP-Phone to IP-Phone, vlastní IP telefon je realizován jako SW aplikace pro PC nebo hardware v podobě IP telefonu. Tento scénář je používán nejvíce pro vnitřní komunikaci.

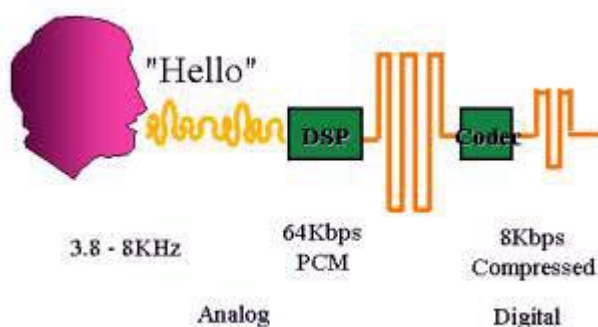


Toto využití lze označit jako scénář PSTN to PSTN. Dochází k propojení sítí PSTN (Public Switched Telephone Network - klasická analogová telefonní síť) přes IP síť. PSTN je připojeno do IP sítě pomocí bran zajišťujících převod. Tento scénář je využíván také v rámci podniků mající PSTN síť, je také využíván operátory a je nabízen za cenově zvýhodněných volání.



Scénář IP-Phone to PSTN (resp. PSTN to IP-Phone) je v podstatě analogií předchozího scénáře. Objevuje se ve veřejné síti a realizuje výstup z IP sítě v určitém bodě a nabízí přístup do PSTN jako službu VoIP to PSTN (nebo naopak).

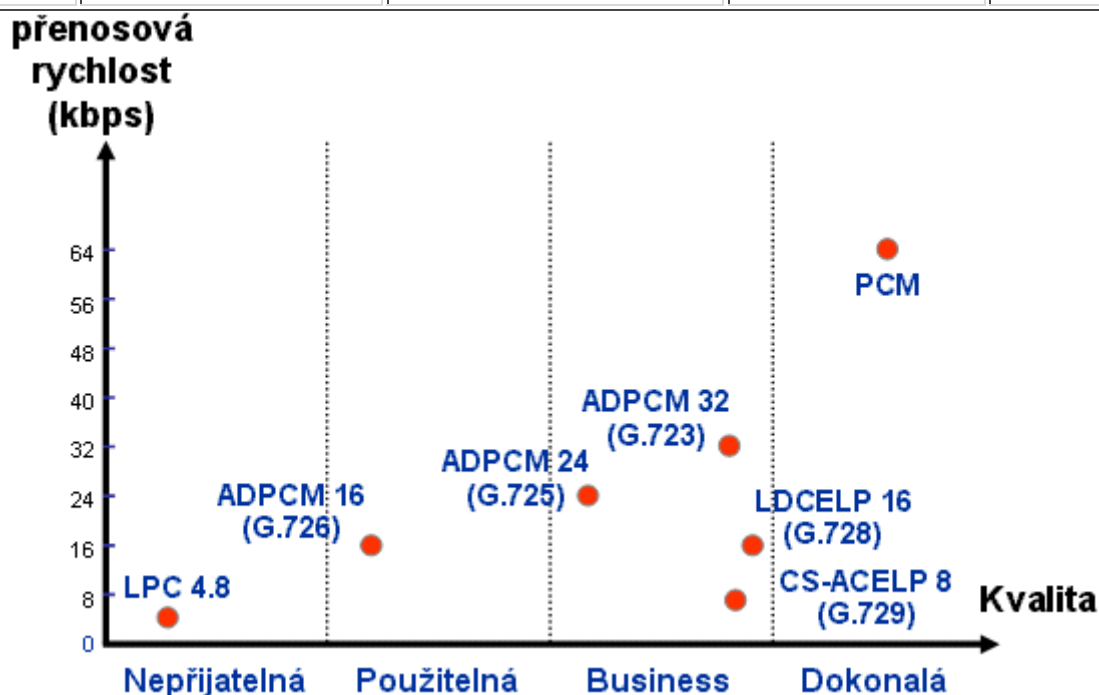
Přenos hlasu a kodeky



VoIP pro převod hlasu na data využívá různých kodeků. Kodeky jsou uzpůsobeny pro přenos lidského hlasu (pásmo přibližně od 300Hz - 3,4KHz). Základní používaná metoda digitalizace je PCM, která potřebuje přenosovou rychlost 64 kbit/s. Jelikož je lidské ucho nedokonalé využívá se kodeků snižující kapacitu (analogie s MP3-nepřenášet "zbytečné informace", nemusí se přenášet ticho, apod.). Kodeků existují desítky a liší se poměrem kvality a vyžadovaného pásma pro přenos. V následující tabulce a grafu je porovnání některých kodeků.

| Technika | Přenosová rychlost (Kbps) | Nároky na výpočetní kapacitu | Výsledná kvalita hlasu | Způsobené zpoždění |
|-----------|---------------------------|------------------------------|------------------------|--------------------|
| G.711 PCM | 64 (bez komprese) | žádné | vynikající | N/A |

| | | | | |
|-------------------|----------|--------------|----------------------------|------------|
| G.723 MP-MLQ | 6.4/5.3 | střední | Dobrá (6.4) Slabá (5.3) | vysoké |
| G.726 ADPCM | 40/32/24 | nízké | dobrá (40) slabá (24) | velmi malé |
| G.728 LD-CELP | 16 | velmi vysoké | dobrá | nízké |
| G.729 CS-ACELP | 8 | vysoké | dobrá | nízké |



Některé komplikace použití VoIP:

- ozvěna - je eliminována aktivním potlačením v DSP;
- zpoždění - je nepříjemné a musí být zajištěna prioritizace hlasových paketů; pro vysokou kvalitu hovoru je určeno max. 150 ms na dobu doručení informace od odesílatele k příjemci.
- Kolísání zpoždění (jitter) - je nutné vyrovnávat proměnné zpoždění příchodu hlasových paketů jejich ukládáním do bufferů; to samozřejmě přináší určité zpoždění.
- ztráta- opravnými mechanismy nemá občasná ztráta paketů vliv na kvalitu hlasu.

Má-li komunikační síť poskytovat nové druhy služeb, musí umožňovat poskytování těchto služeb v požadované kvalitě. Zde se zavádí pojem kvalita služeb (Quality of Service, QoS). Koncept QoS je ve skutečnosti značně široký a může zahrnovat velmi mnoho různých oblastí, parametrů a veličin, kterých se může týkat. V současnosti lze provozovat v sítích s protokolem IP hlasovou komunikaci v požadované kvalitě díky třem faktorům :

- pokrokům v kompresních technikách snižujících nároky na přenosové pásmo
- navyšování přenosové kapacity v Internetu
- zavedením nástrojů QoS v IP síti

Architektura a protokoly

Architektury sítí VoIP

Centralizovaná architektura

- analogie ke klasickým veřejným telefonním sítím
- centralizované řízení sítě a „hloupá“ koncová zařízení

Výhody:

- centralizované řízení hovorů, management a zajištění
- kopíruje principy klasických telefonních sítí

Nevýhody:

- potlačení inovace koncových zařízení
- obtížná implementace jiných VoIP služeb, než přenos hlasu

Distribuovaná architektura

- filosofie IP sítí
- inteligence sítě (sestavování hovorů, směrování, billing) je rozprostřena do koncových bodů
- koncové body mohou být VoIP brány, IP telefony, media servery nebo jakékoliv zařízení schopné iniciovat a ukončit VoIP hovor.
- využití v sítích WAN, komplexní řešení

Výhody:

- flexibilita
- možnosti sítě závisí na koncových zařízeních – snadné přizpůsobení konkrétním aplikacím (ICQ Phone, NetMeeting)

Nevýhody:

- komplikovaná struktura sítě

Protokoly využívané ve VoIP

VoIP využívá dva druhy protokolů:

- **Signalizační** - slouží navazování spojení, řízení toku a jeho ukončování. Mezi signalizační protokoly patří H.323, SIP, MGCP, Megaco. H.323 a SIP se využívá v distribuované architektuře. MGCP a Megaco se využívají v architektuře centralizované. Od H.323 a SIP se liší v tom, že je ideální pro centrální řízení jednoduchých koncových přístrojů, kdy řídicí servery mezi sebou dále komunikují prostřednictvím H.323 nebo SIP.
- **Komunikační** - slouží k vlastnímu přenosu hlasu. Využívá se protokolu RTP a RTCP.

Protokol H.323**Komponenty definované protokolem**

H.323 má 4 základní komponenty:

- terminál
- gateway
- gatekeeper
- multipoint control unit

Terminál je základní a jedinou povinnou komponentou H.323 sítě. Používá se pro obousměrnou komunikaci v reálném čase. Může to být PC nebo specializované zařízení, na kterém běží H.323 stack. Závazně musí podporovat audio služby, video a data jsou volitelné. Je schopen komunikovat s jinými multimediálními terminály v jiných sítích.

Gateway - GW (brána) zabezpečuje spojení H.323 sítě s jinou sítí (např. ISDN), slouží jako překladač protokolů mezi různými sítěmi. Je volitelnou komponentou.

Gatekeeper - GK (správce zóny) - Tuto komponentu si můžete představit jako mozek sítě. Ačkoli je to volitelná komponenta, má na starosti velice důležité služby jako autorizaci, autentifikaci, překlad telefonních čísel na IP adresy, účtování služeb, směrování hovorů apod. Jedná se vlastně o analogii inteligentní ústředny. 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).

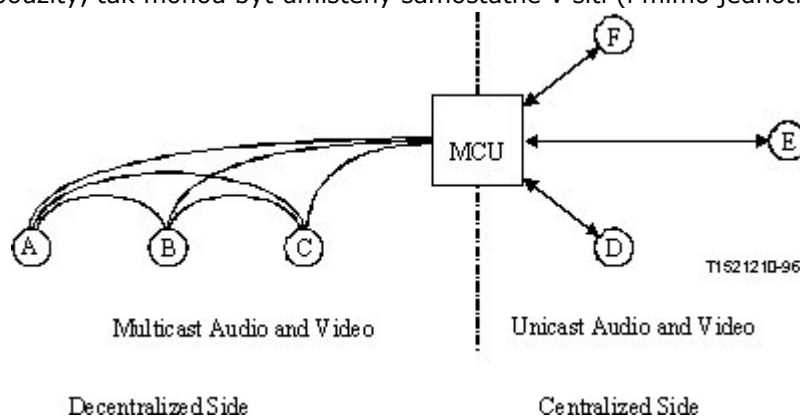
Nepovinné služby definované doporučením H.323 :

- 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 přesměrovat, 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, zasilání nebo přesměrování hovorů a směrování hovorů.

Multipoint Control Unit - MCU (jednotka pro řízení konferenčního spojení) zajišťuje komunikaci tří a více terminálů (konferenční hovory). Umožňuje převádět decentralizované konferenční spojení (data jsou určena skupině stanic) na spojení centralizované (data jsou určena právě jedné cílové stanici) a obráceně

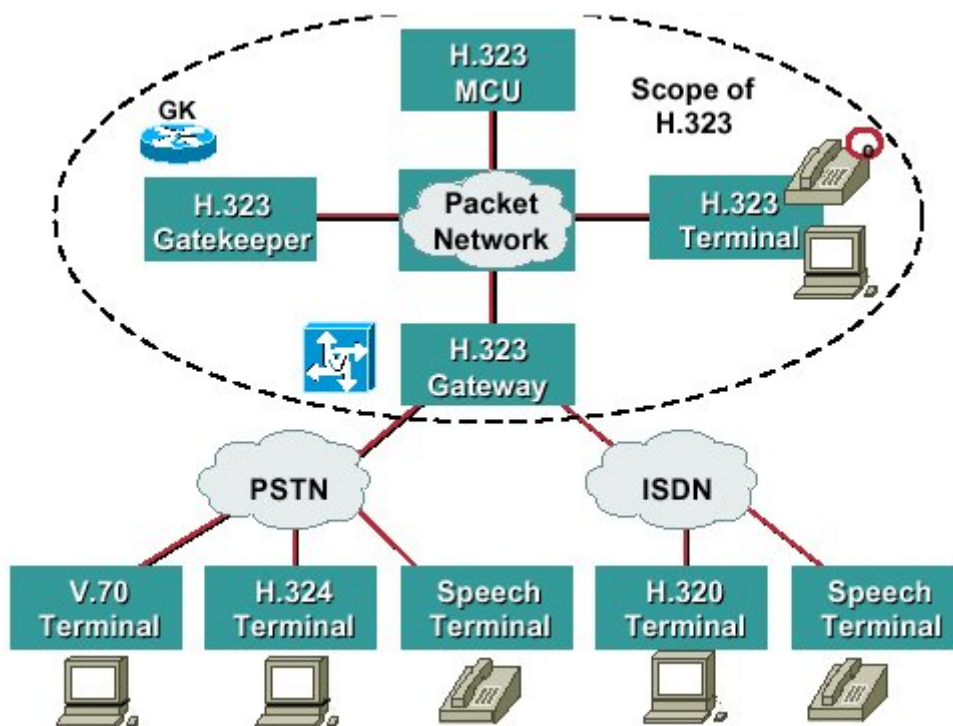
Jednotka MCU se skládá z modulů MP a MC :

- 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 přenášená v konferenci. MP je volitelný modul. Pokud jsou MP použity, tak mohou být umístěny samostatně v síti (i mimo jednotku MCU).

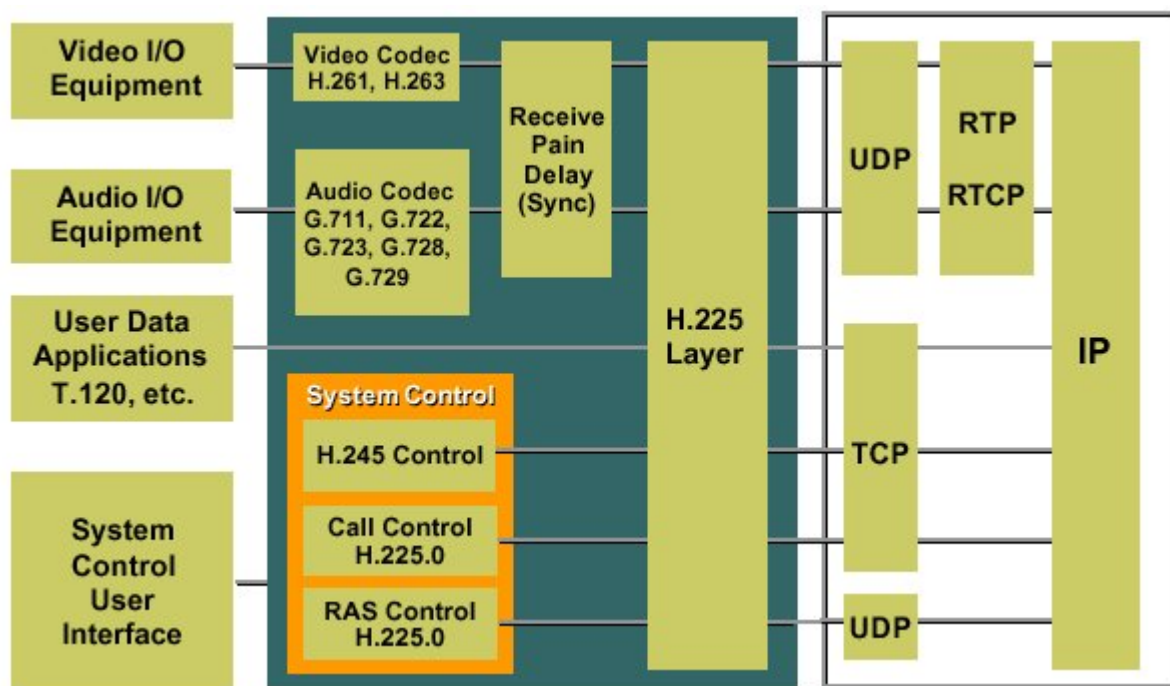


Doplnění: H.323 síť může obsahovat libovolné množství terminálů, MCU a brán, vždy však pouze jednoho gatekeepera. Mluvíme pak o H.323 zóně. Rovněž je potřeba zdůraznit, že toto dělení je pouze logické. Jednotlivé komponenty pak mohou být a často také bývají integrovány do jednoho produktu. Například funkce MCU může být integrována přímo v terminálu nebo v gateway.

Propojení komponent



Struktura protokolu



Protokol H.323 v sobě zahrnuje (viz obrázek):

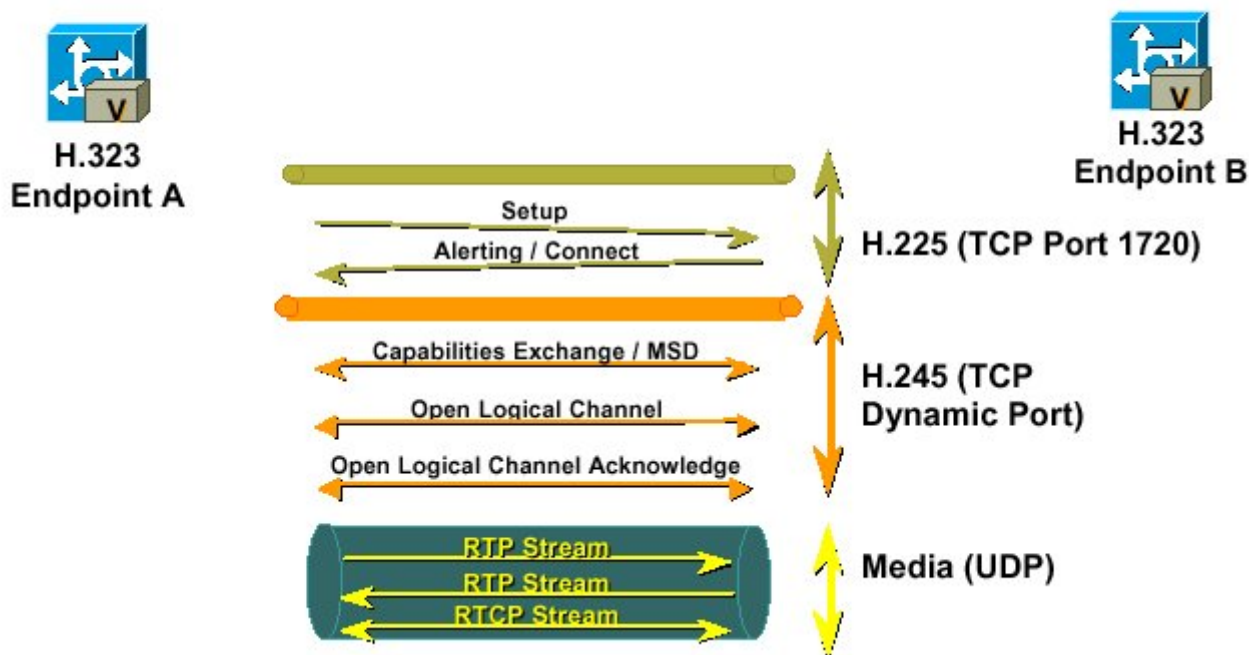
- **kódování zvuku** - tj. zakódování zvuku na vysílajícím terminálu a jeho dekódování na přijímající straně. Protože podpora zvuku je povinná, každý terminál musí podporovat kódování podle G.711 (PCM, 64 Kbps) a volitelně pak G.722 (64, 56 a 48 Kbps), G.723.1 (5,3 a 6,3 Kbps), G.728 (16 Kbps) nebo G.723 (8 Kbps)
- **kódování obrazu** - podpora videa je volitelná. Pokud je zahrnuta, musí splňovat standard H.261.
- **H.255 signalizace volání a H.255 RAS** (Registration, Admission, Status). Slouží pro sestavení spojení mezi dvěma koncovými body. K sestavení slouží výměna zpráv na signalizačním kanále, a to buď přímo mezi koncovými zařízeními, nebo mezi koncovým zařízením a gatekeeperem. RAS protokol zabezpečuje komunikaci mezi koncovými zařízeními sítě (terminál, gateway) a gatekeeperem. Má na starosti procedury jako je registrace, správa šířky pásma apod.
- **řídící signalizace H.245** Tyto řídicí zprávy zajišťují:

- výměnu vlastností mezi koncovými body (co vše terminály podporují)
 - otevření a uzavření logických kanálů pro přenos
 - řízení toku dat
 - všeobecné příkazy a indikace stavu
- **RTP a RTCP** - RTP zajišťuje samotný přenos zvuku a videa v reálném čase mezi koncovými body sítě. Přesněji zajišťuje doručení paketů ve správném pořadí pomocí časových razítek (timestamp), sekvenčních čísel apod. Při komunikaci přes IP používá protokol UDP. RTCP je analógie RTP pro řídicí služby, tj. slouží pro synchronizaci audia i videa.

Příklady průběhu spojení

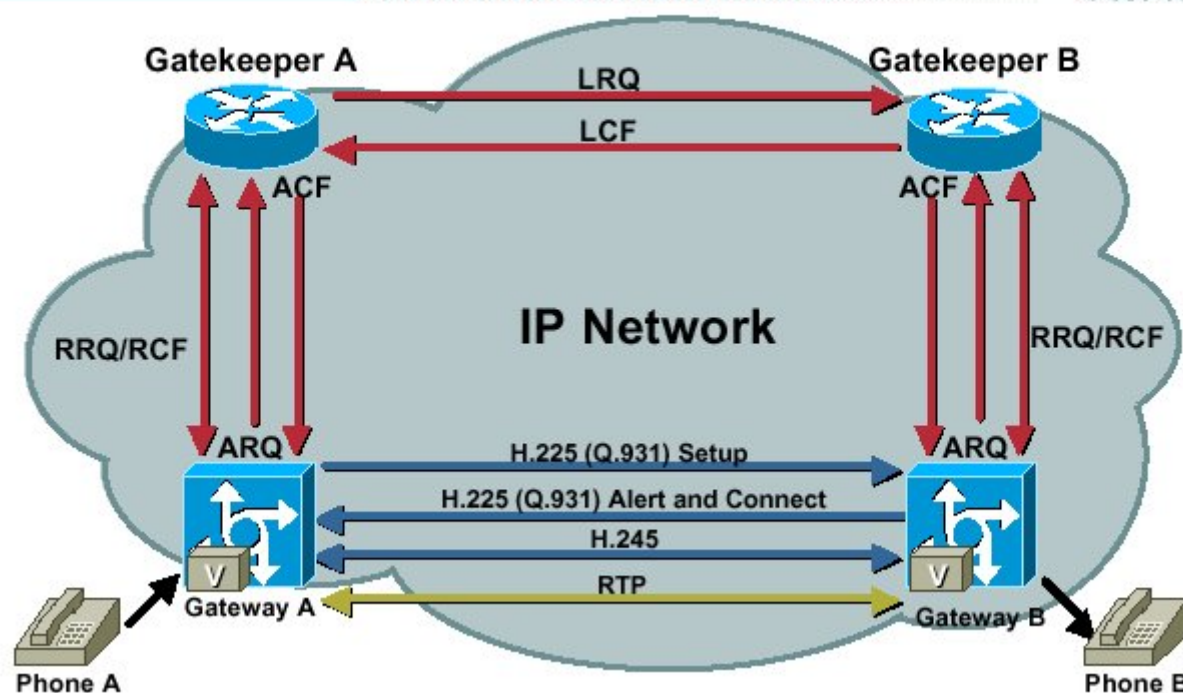
H.323 Signaling

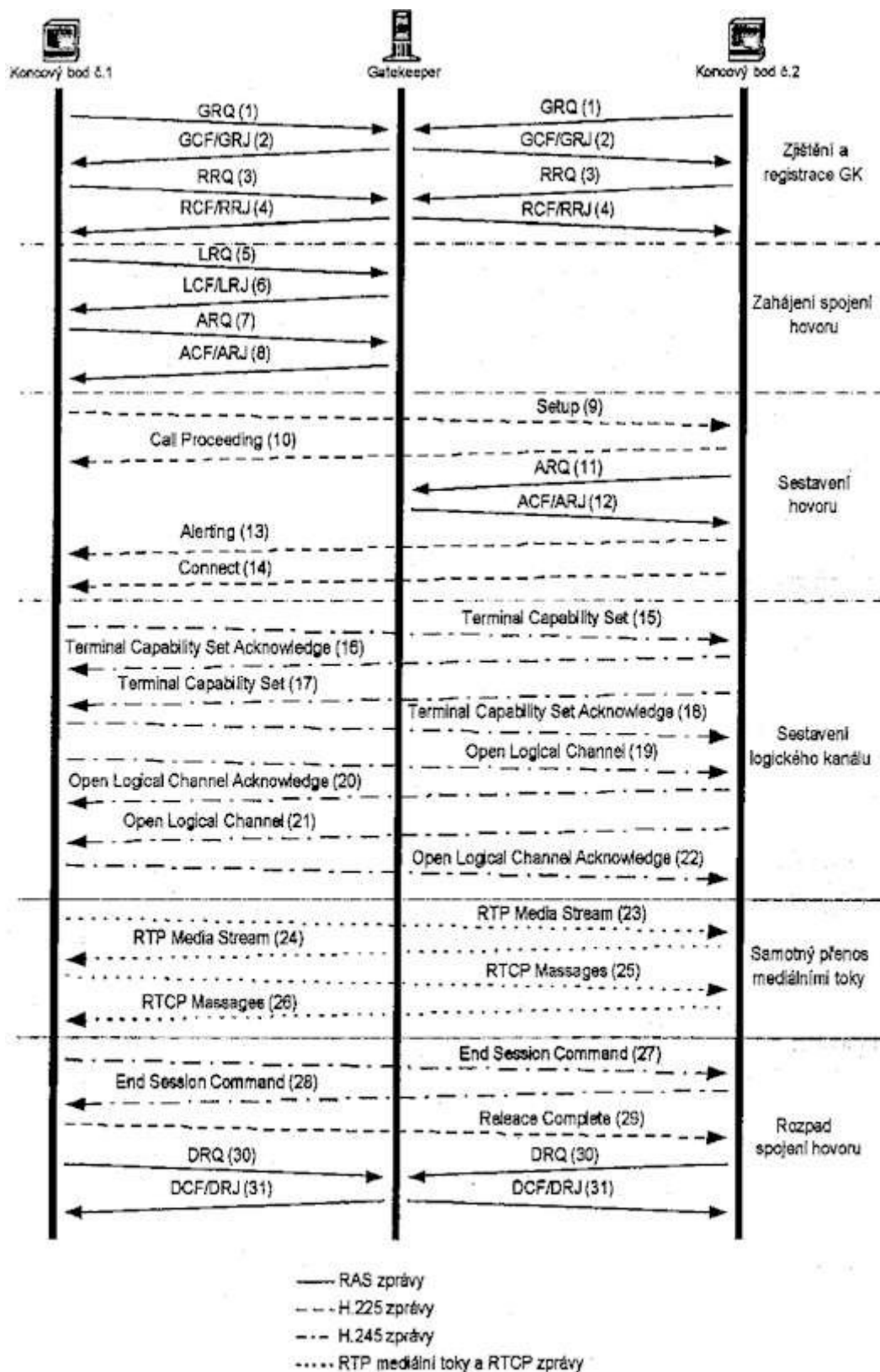
Cisco.com



Basic H.323 Call

Cisco.com





Signalizační postup při sestavení a rozpadu spojení dle ITU-T H.323

Protokol SIP

SIP (Session Initiation Protocol) 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. Protokol SIP nespécifikuje jaký má být použit transportní protokol a není svázán s žádnými konkrétními komunikačními protokoly pro vlastní přenos multimediálních dat. 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).

Komponenty

Podobně jako H.323 i SIP definuje architekturu v rámci které funguje a která sestává z následujících komponent:

User Agent

User agents (UA) jsou koncovými zařízeními SIP sítě. Starají se o navazování spojení s ostatními UA. Nejčastěji se jedná o SIP telefony (ať už fyzické nebo ve formě aplikací běžících na PC) a brány do jiných sítí, typicky do PSTN. V rámci UA rozlišujeme ještě User Agent Client (UAC), což je část UA která má na starosti iniciaci spojení a User Agent Server (UAS), která reaguje na příchozí žádosti a posílá odpovědi. V koncovém zařízení (SIP telefonu) je implementován jak UAC, tak i UAS.

Servery

Servery jsou v SIP architektuře zařízení, jejichž úkolem je zprostředkovat kontakt mezi volajícími a volanými (tedy mezi UA), což ale nevylučuje přímý kontakt koncových zařízení bez účasti serverů. Rozlišujeme tyto tři typy SIP serverů:

1. Proxy server.

Tento 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.

2. Redirect server.

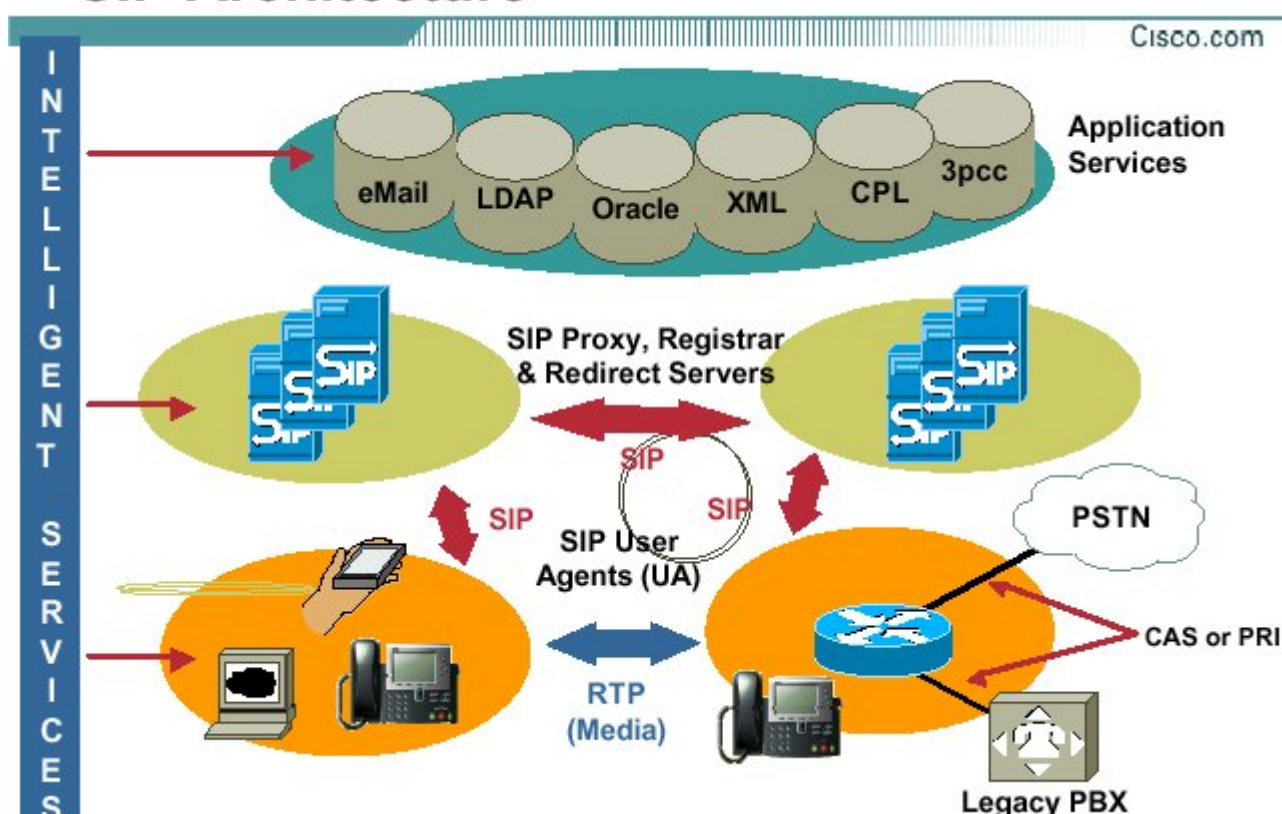
Stejně jako proxy přijímá žádosti o spojení od UA nebo proxy serverů, ale nepřeposílá je dále ve směru volaného, nýbrž posílá tázajícímu informaci, komu má žádost poslat, aby se dostala k volanému. Je pak na dotazujícím se, aby žádost na takto získanou lokalitu (další proxy/redirect server nebo volaný UA) poslal.

3. Registrar server.

Registrar server přijímá registrační žádosti od UA a aktualizuje podle nich databázi koncových zařízení (location service), které jsou v rámci domény spravovány.

Jakkoliv jsou tyto servery definovány odděleně, v praxi se často jedná o jednu aplikaci, která přijímá registrace koncových uzlů a podle konfigurace se chová zároveň buď jako proxy nebo redirect server (určitá analogie s gatekeeperem z H.323).

SIP Architecture



Komunikace komponent a identifikace

Metody a odpovědi

O komunikaci mezi komponenty SIP architektury jsem se zatím zmínil pouze v obecné rovině. Agenti a servery si posílají požadavky pomocí takzvaných metod. Jedná se o zprávy v textovém formátu a šesti základními metodami jsou

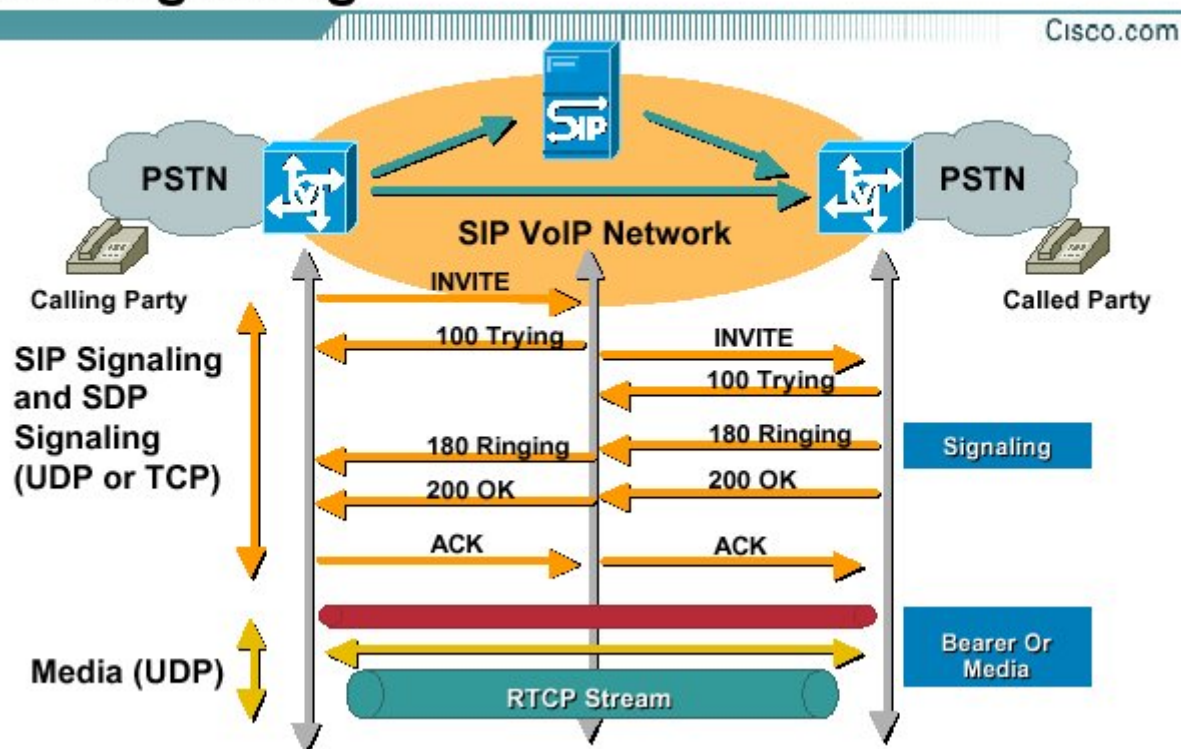
- INVITE - slouží k žádosti o sestavení spojení
- ACK - potvrzení INVITE finálním příjemcem zprávy (volaným)
- BYE - ukončení spojení
- CANCEL - ukončení nesestaveného spojení
- REGISTER - registrace UA
- OPTIONS - dotaz na možnosti a schopnosti serveru

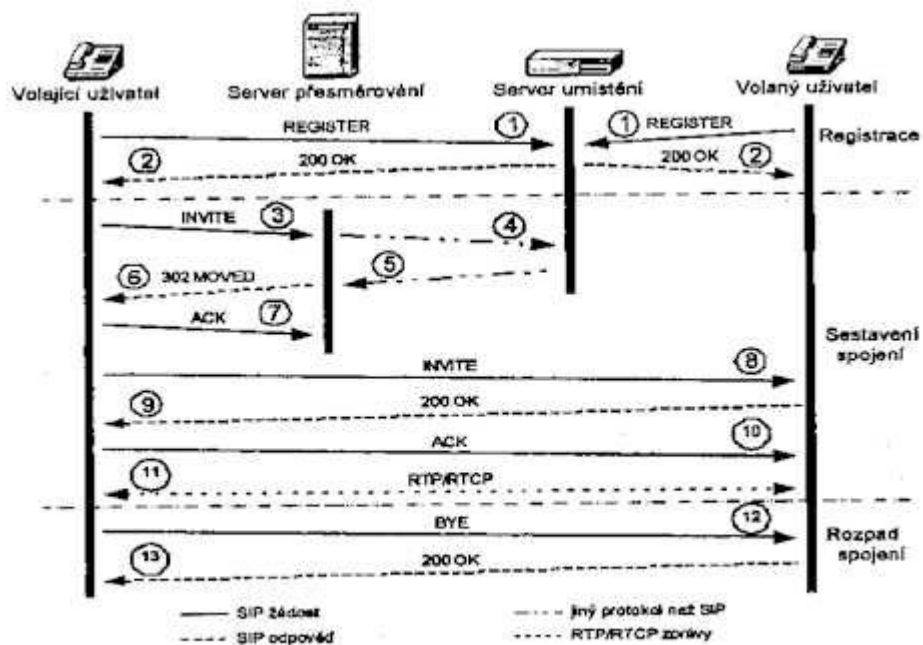
Další metody jsou předmětem samostatných RFC nebo draftů.

Odpovědi na SIP metody jsou zprávy uvedené číselným kódem. Systém kódů je převzat z HTTP protokolu. Např. SIPovská odpověď "404 Not Found" je velmi podobná té, které se objeví na web prohlížeči při přístupu na neexistující stránku. 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")

SIP Signaling





Signalizační postup při sestavení a rozpadu spojení dle IETF SIP

Identifikace volaného v síti SIP

Zatímco v běžné telefonní síti jsme zvyklí identifikovat jednotlivé účastníky pomocí telefonního čísla (E.164), v rámci SIP se používá Uniform Resource Identifier (URI) resp. Universal Resource Locator (URL), což je další ukáзка toho, jak SIP využívá již existující standardy. Zde jsou to standardy pro popis zdrojů vyskytujících se v Internetu.

Tímto způsobem jsou identifikováni samozřejmě nejen koncoví účastníci ale i hlasové záznamníky, brány do jiných sítí, skupina účastníků, atd.

Telefonovat můžeme např. na takovéto adresy:

- sip:jan.novotny@nejakafirma.cz
- sip: "Milkman Dan" dan@redmeat.com
- sip:123456@jinafirma.cz
- tel:+420244470645

Ukázka zprávy SIP se zapouzdřeným SDP

```
INVITE sip:ty@tam.cz SIP/2.0
Via: SIP/2.0/UDP 195.113.147.120:1912
Date: Tue, 17 Apr 2001 10:56:34 GMT
From: <sip:ja@tady.>
To: <sip:ty@tam.cz>
Subject: Hovor 1
Priority: normal
Expires: 3600
CSeq: 1691095645 INVITE
Call-ID: 884664559@195.113.147.210
Contact: <sip:ja@195.113.147.120:5060>
Content-Type: application/sdp
Content-Length: 143
v=0
o=ja 987504994 987504994 IN IP4 195.113.147.120
s=Hovor 1
c=IN IP4 195.113.147.120
t=3196493794 3196497394
m=audio 10000 RTP/AVP 0
```

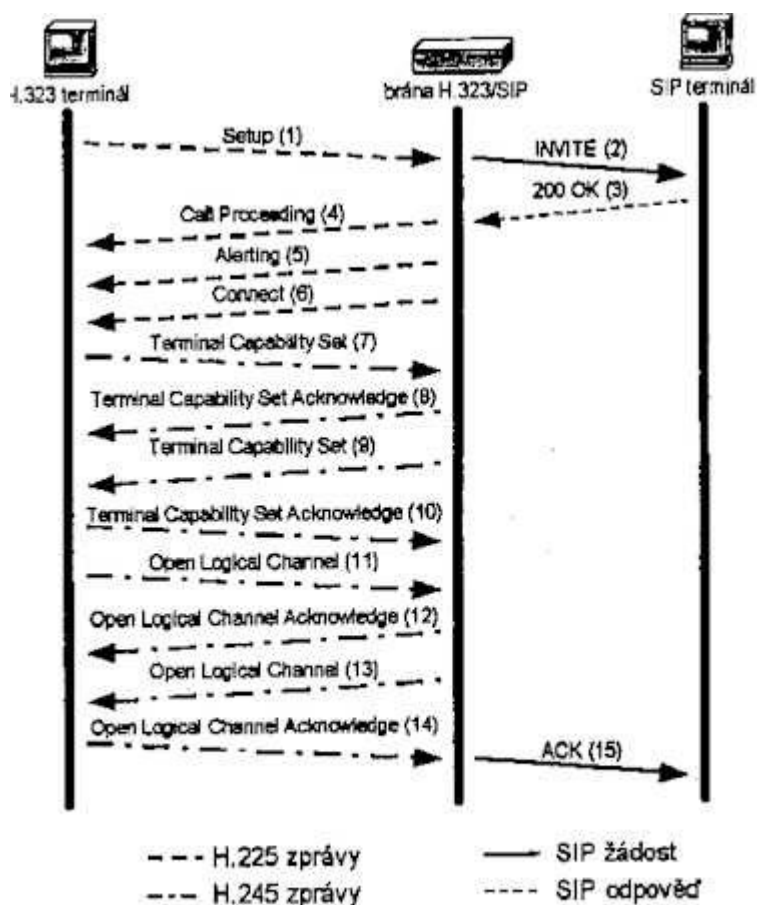
Poznámka k protokolu SDP

Protokol SDP slouží k specifikaci kódování a dalších parametrů přenosu multimediálních dat během komunikace. Zpráva protokolu SDP je obsažena v těle zprávy protokolu SIP a sestává z posloupnosti řádků ve tvaru typ=hodnota. Typ je vždy zapsán jen jedním písmenem a říká, jaký parametr komunikace je popisován. Nejprve jsou vždy uvedeny řádky týkající se celého spojení nebo všech toků přenášených dat. Potom následují řádky popisující jednotlivé toky dat. Nejvýznamnější typy a jejich význam jsou následující:

- v - verze protokolu SDP
- o - původce (originator) spojení, udává jeho uživatelské jméno, identifikátor spojení a IP adresu
- s - jméno (subject) spojení
- c - adresa spojení (connection), na kterou mají být posílána data, obvykle jde o multicastovou IP adresu, za kterou může následovat lomítko a hodnota TTL (Time To Live) definující rozsah šíření paketů v síti
- a - atribut přenášející doplňkové informace, může být ve tvaru hodnota nebo jméno:hodnota, například recvonly znamená, že odesílatel této zprávy bude pouze přijímat data
- m - popis toku dat (media), udává typ dat (audio, video, atd.), číslo portu na adrese udané řádkem c, na kterém bude tento proud dat posílán, transportní protokol (RTP, UDP, atd.) a kódování, obvykle jako číslo definované jako typ dat v protokolu RTP

Porovnání protokolů H.323 a 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 následující obrázek.



Spojení z H.323 terminálu na SIP terminál

Následující tabulka 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 (Gatekeeper) | Registrační server (Registrar Server) Zástupný server (Proxy Server) Přesměrovací server (Redirect Server) Server umístění (Location Server) |
| 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 |

Protokol RTP a RTCP

RTP (Real Time Protocol) je protokol sloužící pro přenos dat v reálném čase. 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. Příjímací 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.

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

Hardware

Hlasová brána

Hlasová brána VoGW (Voice Gateway) je klíčovou částí služeb IP telefonie, neboť umožňuje spojení mezi telefonní a paketovou sítí, to znamená, že provádí všechny nezbytně nutné fyzický překlad a hlasovou kompresi a tím dovoluje volání mezi těmito dvěma prostředími. Hlasová brána poskytuje tyto následující funkce :

- kódování a dekódování hlasu v reálném čase s kompresními algoritmy
- paketizaci a depaketizaci komprimovaného hlasového signálu
- komunikaci s PBX(pobočková telefonní ústředna), PSTN nebo jiným telefonním zařízením
- zpracování signalizačních informací
- komunikaci se sítí s protokolem IP

Hlasová brána může být realizována na PC formou karet s příslušným rozhraním a SW aplikací nebo formou směrovače doplněného o hlasové moduly.



Call Manager

Call Manager (správce volání) udržuje a spravuje konfigurace a je schopen směrovat hovory v rámci telefonní sítě. Call Manager má návaznost na celopodnikovou adresářovou strukturu a umožňuje tak zadávat a udržovat informace o uživateli na jednom místě. Call manager může být pouze software jako je například systém SIPSTAR, běžící na serveru nebo specializovaný kus hardwaru. Prostřednictvím Call Managerů je zajištěna poměrně zajímavá škálovatelnost řešení. Zatímco v případě klasické ústředny je nutná výměna šasi za větší když to stávající firma „přeroste“, v případě IP telefonie se přidávají jednotky pouze uživatelské licence nebo Call Manager.



IP telefony

IP telefony jsou koncová zařízení pro uživatele. Plní dvě funkce:

- hlasové dorozumívání s protějškem - vlastnost obvyklá u klasického telefonního světa
- nové funkce – komunikace s aplikačními servery v datové síti - telefony jsou vybavené xml prohlížečem a poměrně velkým displayem umožňujícím provoz textově orientovaných aplikací, příp. aplikací s jednoduchou grafikou. Technologie XML umožňuje vyvíjet pro IP telefony zcela nové aplikace podle individuálních potřeb uživatelů.

IP telefony nemusí být jen ve formě zařízení, ale mohou být také ve formě softwarových aplikací (hardphone - softphone)

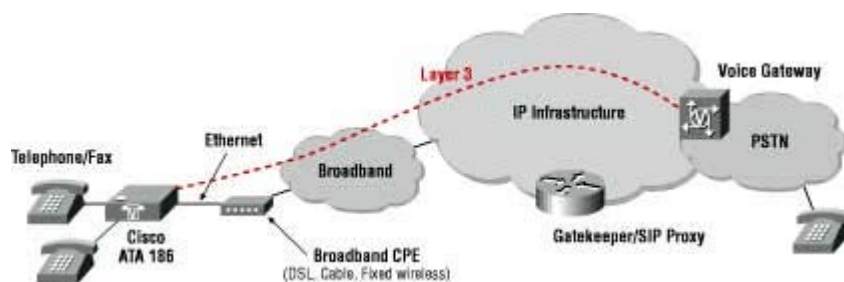


Implementace v distribuovaném prostředí

V rámci distribuovaného prostředí WAN lze v závislosti na množství uživatelů na jednotlivých lokalitách volit model založený na:

- distribuovaných Call Managerech – každá lokalita vlastní Call Manager
- centralizovaném Call Manageru – Call Manager pouze v centru
- kombinaci – Call Manager je centralizovaný, nicméně na velkých pobočkách existuje vlastní Call Manager

Každá lokalita se může skládat z většiny prvků uvedených v následujícím obrázku:



Call Manager je jednou z nejdražších komponent v celém systému. Jeho použití v každé lokalitě distribuovaného modelu je samozřejmě poměrně neefektivní. Na druhou stranu v případě toho, že IP telefony nemají Call Manager dostupný, je ohrožena možnost telefonovat. Z tohoto důvodu bývají vzdálené firemní pobočky vybaveny vlastními Call managery.