Katedra softwarového inženýrství,
Matematicko-fyzikální fakulta,
Univerzita Karlova, Praha

Rodina protokolů TCP/IP,
verze 2.7

Část 11: VOIP, IP telefonie

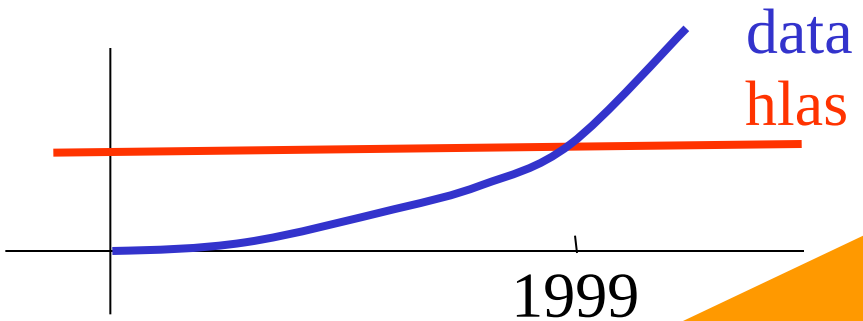
Jiří Peterka, 2011

terminologie

- VOIP (Voice over IP)
  - obecné označení pro technologii
    - přenosu zdigitalizovaného hlasu po protokolu IP
  - může být realizována různými způsoby
    - proprietárně
      - Skype, Fayn, …
    - dle standardu H.323
    - dle standardu SIP a MGCP
    - ….
  - může být využita k různým účelům
    - jako veřejná služba
    - jako služba pro privátní účely
      - např. telefonování v rámci firmy
    - jako technologické řešení u operátorů
      - v páteřních částech svých sítí přenáší data nikoli na principu přepojování okruhů, ale pomocí VOIP
  - může využívat různou přenosovou infrasktrukturu
    - veřejný Internet
    - privátní intranet
    - …..
- IP telefonie
  - obecné označení pro službu
    - většinou veřejná služba
  - využívá technologie VOIP
  - nedělá rozdíl mezi použitou přenosovou infrastrukturou
    - Internet, intranet
- internetová telefonie
  - varianta IP telefonie,
  - pro přenosy dat využívá veřejný Internet
- VOD (Voice over Data)
  - obecnější označení než VOIP
  - jakákoli technologie pro přenos zdigitalizovaného hlasu po datových sítích
  - např.:
    - VoFR (Voice over Frame Relay)
    - VoATM (Voice over ATM)
    - CVoDSL (Channelized Voice over DSL)

historie

- 1995:
  - izraelská firma Vocaltec představuje svůj Internet Phone
    - všeobecně považováno za začátek (běžně dostupné) internetové telefonie
    - značně nedokonalé, ale postupně se zlepšuje
- 1996:
  - ITU vydává doporučení **H.323**
    - jako standard IP telefonie "ze světa spojů"
    - 1998: první použitelná revize
- 1999:
  - objem datového provozu v telekomunikačních sítí se vyrovnává hlasovému provozu (v digitální podobě)
    - dále roste už jen datový provoz
    - hlasový provoz víceméně stagnuje
- 1999:
  - IETF schvaluje protokol **SIP**
    - Session Initiation Protocol
      - RFC2543 (17.3.1999)
      - RFC3261 až RFC 3265 (2002)
    - jako řešení IP telefonie "ze světa počítačů"
      - součást rodiny protokolů (TCP/IP)
- 1999:
  - v únoru 1999 v ČR zakázána služba Paegas Internet Call
  - v červenci liberalizovány hlasové služby na báziVOIP
    - generální povolení ČTÚ č. 22/1999



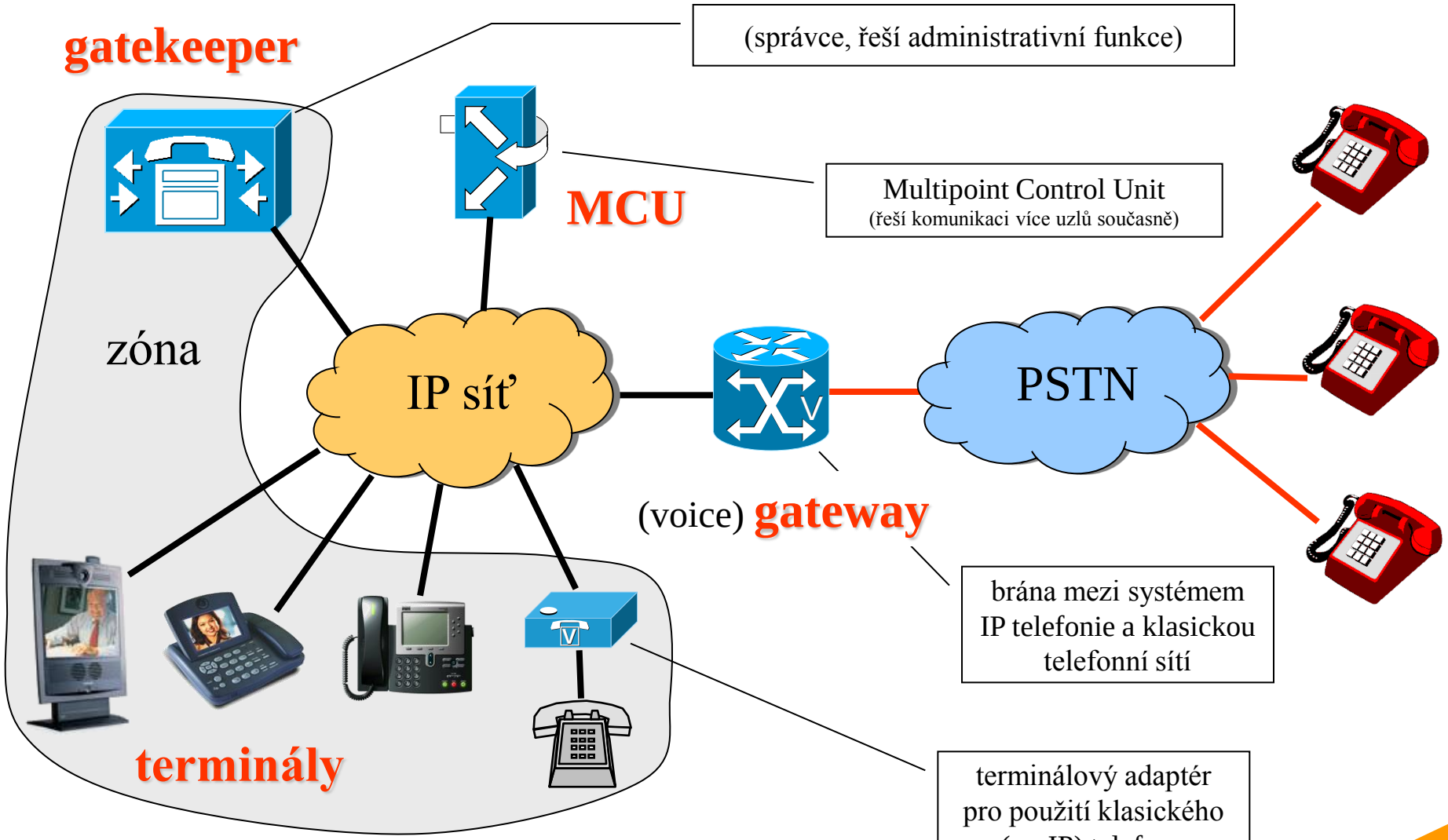
IP telefonie: co všechno se musí vyřešit

- jak digitalizovat (kódovat) hlas?
  - ve světě POTS (PSTN) je vše pevně dáno
    - PCM, 64 kbit/s na hovor
  - ve světě IP telefonie připadá v úvahu více možností
    - tyto možnosti musí být definovány
      - svými standardy
- jak se domluvit na schopnostech zařízení
  - v POTS: schopnosti jsou stejné
  - zde: mohou se i významně lišit
    - musí existovat mechanismy, prostřednictvím kterých se zúčastněné strany dohodnou na tom, co umí a co budou používat
- jak přenášet data
  - relativně nejsnazší
    - až na otázku kvality služeb
- jak propojit systémy IP telefonie s klasickou telefonní sítí
  - musí existovat vhodné **brány**
- jak "zařadit" telefon do sítě
  - ve světě POTS (PSTN) jsou telefony pevně přiřazené k telefonním ústřednám
    - a ty je "obsluhují" …
  - ve světě IP telefonie není předem dáno, "kam telefon patří"
    - musí existovat **správci**, kterým, se IP telefony přihlásí a které je "zařadí" a začlení do celé telefonní sítě
      - a umožní jejich dostupnost pro příchozí volání
- jak navazovat spojení
  - jak řešit adresaci
    - telefonní čísla, vs. IP adresy
  - jak hledat cestu k volanému
    - řeší **správci**
  - …….

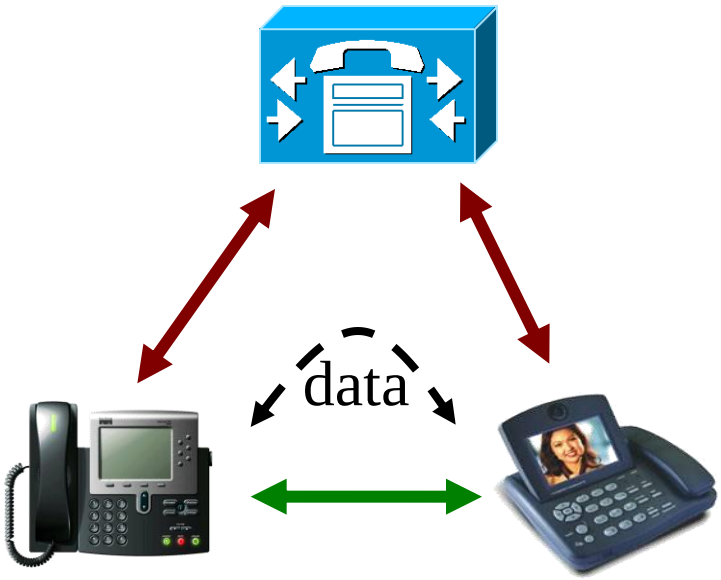
H.323

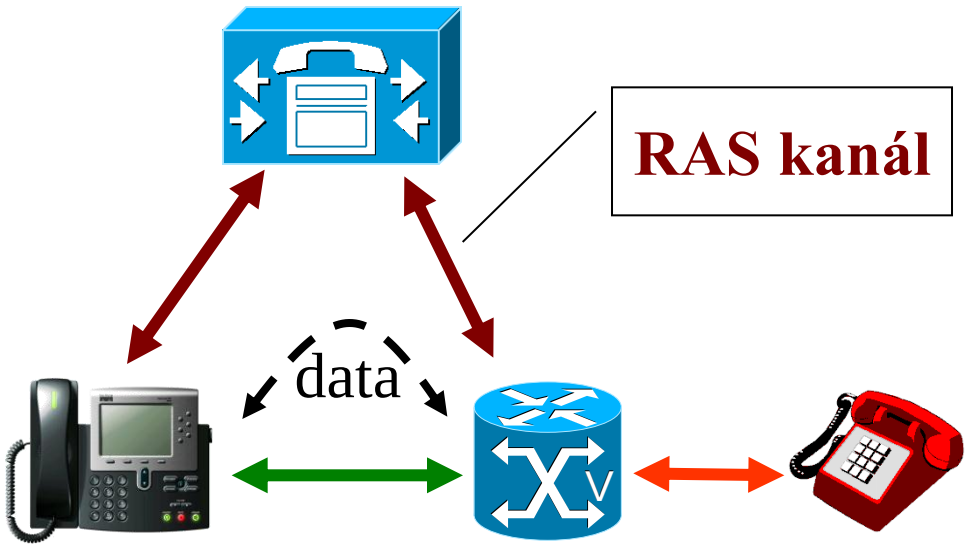
- plným jménem:
  - *"Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non Guaranteed Quality of Service"*
- pochází od ITU
  - Mezinárodní telekomunikační unie
- je "plnohodnotným" řešením
  - velmi komplexní, robustní
    - pokrývá všechny aspekty telefonie
    - dobře navazuje na klasickou telefonii
  - velmi drahé a komplikované řešení
    - ne vždy nutné realizovat v plném rozsahu
- dnes spíše ustupuje ve prospěch SIP-u
  - který je "odlehčený", flexibilnější, jednodušší
- H.323 je celkovou architekturou IP telefonie
  - nikoli jedním protokolem
  - obsahuje řadu konkrétních protokolů
- ale kromě IP telefonie řeší (volitelně) také:
  - videopřenosy a datové přenosy
- předpokládá:
  - přenosovou infrastrukturu bez podpory QoS
- pokrývá (zahrnuje protokoly pro):
  - správu terminálů a zóny
  - kódování hlasu
    - G.711, G.729 a řada dalších
  - řízení hovorů
  - signalizaci
  - přenos dat
    - používá UDP i TCP (nad IP)

architektura H.323



architektura H.323





- gatekeeper zprostředkuje "vyhledání volaného" + další ….
  - samotný hovor v datové podobě (a jeho řízení) probíhá přímo
    - na peer-to-peer bázi
- komunikace terminál-gatekeeper může být nespojovaná
  - nad protokolem UDP

- mezi terminály (terminálem a bránou) se vytváří "**hovorový kanál**" (call channel)
  - obvykle: spojovaný, nad TCP
- slouží potřebám:
  - signalizace
  - řízení hovoru

  } peer-to-peer komunikace
- vlastní data se přenáší "samostatně"
  - nespojovaně (RTP nad UDP)

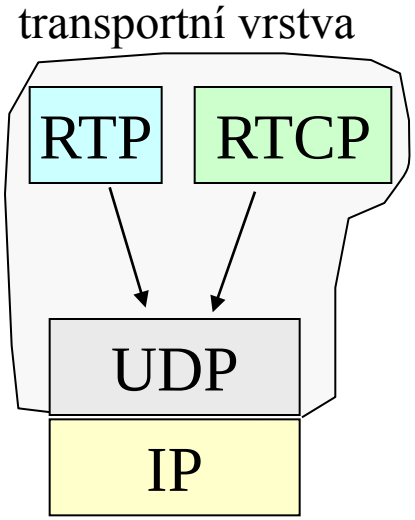
signalizace a řízení hovorů

- signalizace (Signalling)
  - řeší "*telekomunikační záležitosti*"
- týká se zřizování, vedení a ukončování spojení mezi A a B
  - zahrnuje např.:
    - překlad adres volaného/volajícího
    - zjištění, zda je k dispozici dostatečná přenosová kapacita
    - vyhledání cesty k volanému
    - identifikace volajícího vůči volanému
      - B se dozvídá, kdo je A
    - identifikace volaného vůči volajícímu
- v rámci H.323 řeší **H.225**
  - definuje formát zpráv pro své součásti
- součásti:
  - (telefonní) signalizace **Q.931**
    - signalizace převzatá z ISDN
  - komunikace s gatekeeperem
    - **RAS** (Registration/Admission/Status)

- řízení hovoru (Call Control)
  - řeší "*datové záležitosti*"
- týká se využití spojení mezi A a B pro potřeby přenosu hlasu (a ev. obrazu)
  - zahrnuje např.:
    - dohodu, které kodeky budou používány
    - dohodu na schopnostech obou zařízení
    - dohodu o portech pro media streamy
      - kam budou poslány
    - dohodu na dalších parametrech přenosů
- v rámci H.323 řeší hlavně **H.245**
  - Control Protocol for Multimedia Communication
    - může být tunelován skrze H.225
    - vhodná například kvůli firewallům

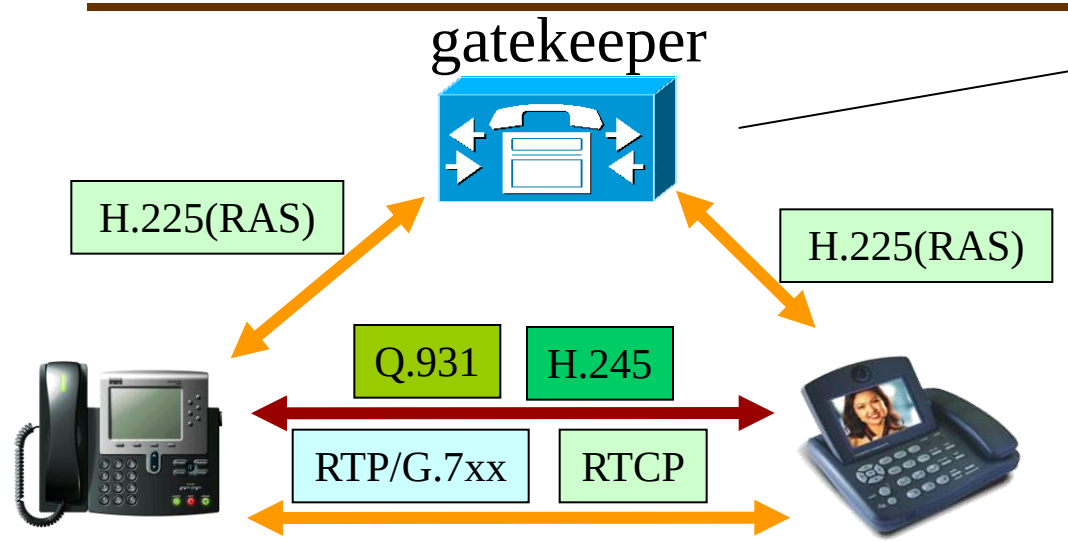
přenos dat v rámci H.323: RTP/RTCP nad UDP

- "čistě transportní" podpora QoS
  - standardizovaný způsob "balení" multimediálních dat do přenášených paketů, s podporou jejich multimediálního charakteru
  - ale bez vlivu na způsob jejich přenosu
    - ten je stále best effort!!!
- RTP (Real Time Protocol)
  - "balí" jednotlivé části multimediálních dat do vlastních bloků (paketů)
    - a ty vkládá do UDP paketů
  - připojuje informace
    - o typu multimediálního obsahu
      - Payload type 0: PCM, 64 kbps
      - Payload type 3, GSM, 13 kbps
      - Payload type 26, Motion JPEG
      - Payload type 33, MPEG2 video
      - ....
    - o pořadí paketu
      - jednotlivé pakety čísluje, usnadňuje detekci ztracených paketů
    - o čase vzniku dat (timestamp)
      - říká kdy přesně data vznikla
      - tím usnadňuje jejich bufferování na straně klienta
    - o konkrétním streamu (proudu)
      - v rámci jednoho RTP přenosu může být přenášeno více samostatných proudů (streamů)
  - podporuje multicast
- RTCP (Real Time Control Protocol)
  - zprostředkovává vzájemné informování zdroje a příjemců
    - např. o procentu ztracených paketů, o jejich zpoždění, o schopnostech příjemce apod.
    - přenáší popis RTP streamu, ….



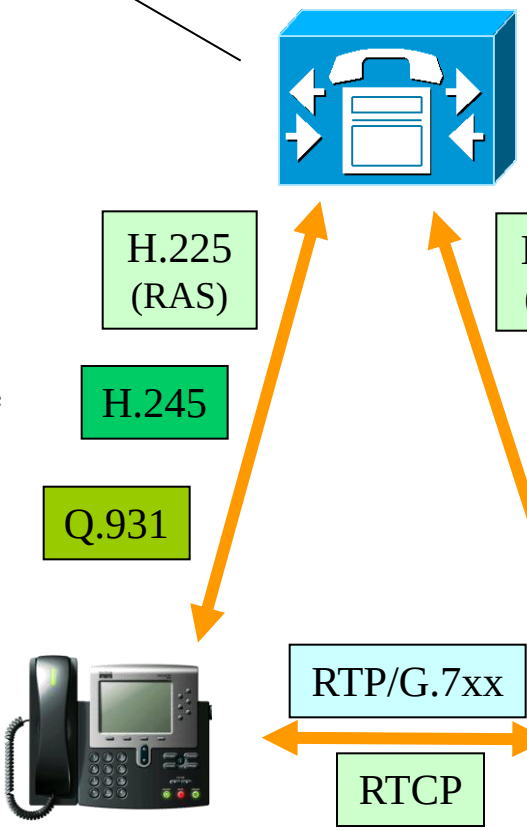
funguje spojovaně !!

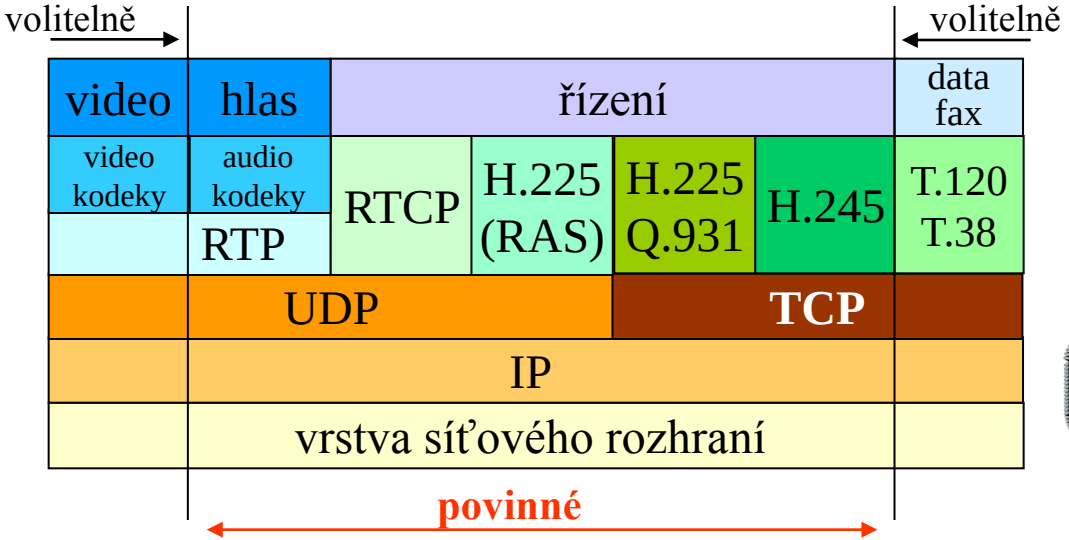
protokoly H.323



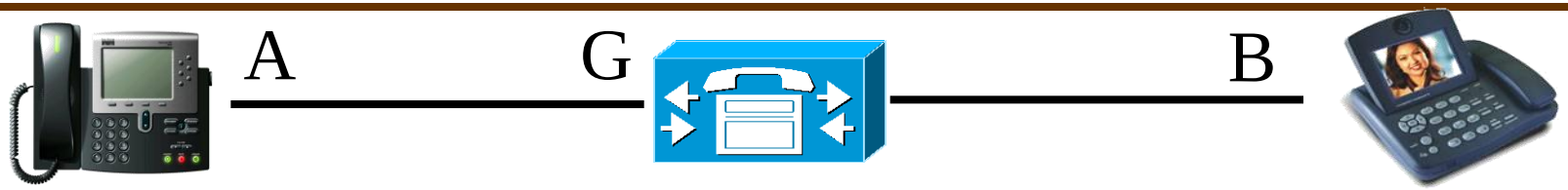
standardní řešení

volitelné řešení

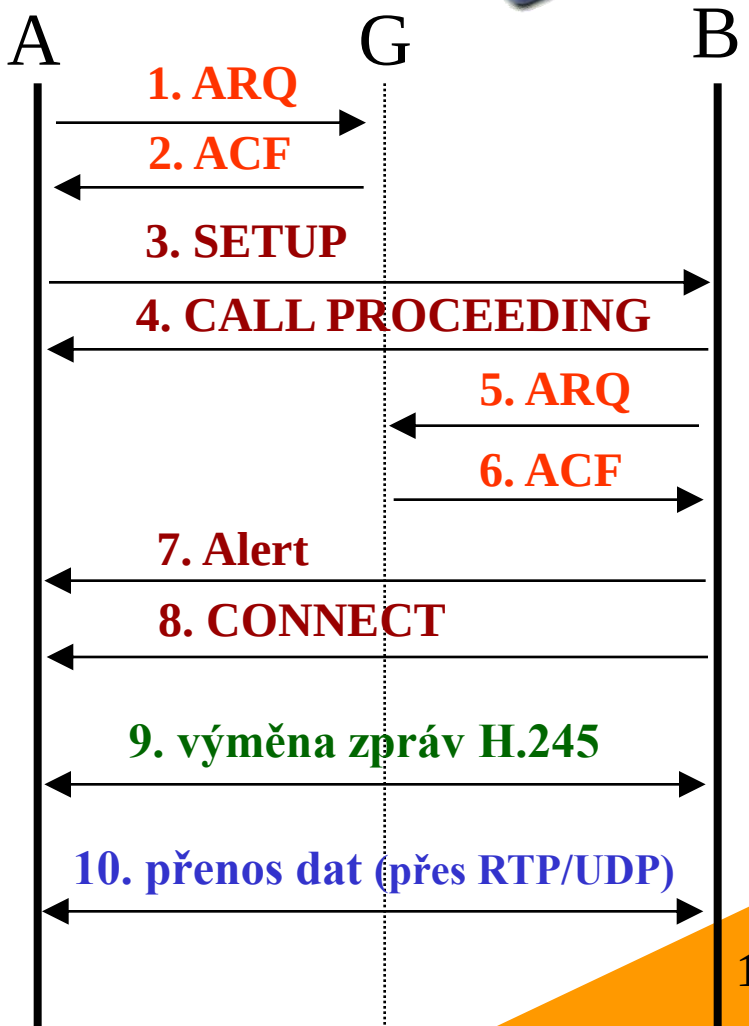




představa komunikace v H.323



  - A i B se již dříve zaregistrovali u gatekeeper-u G
- A žádá G o zprostředkování hovoru s B (1)
  - pomocí RAS zpráv
- G posílá A údaje, potřebné pro kontaktování B (2)
  - IP adresu
- A posílá B zprávu SETUP (3)
- B odpovídá A zprávou CALL PROCEEDING (4)
- B žádá G o souhlas (5)
  - G uděluje souhlas (6)
- B vrací A zprávu CONNECT (8)
  - mezi A a B existuje transportní spojení nad TCP
- A a B si vyměňují zprávy H.245 (9)
  - domlouvají se na svých schopnostech a vzájemné komunikaci
    - jaké kodeky, přes jaké porty si budou předávat data, …
- A a B si vyměňují data (10)
  - přes UDP, nespojovaným způsobem
  - *… probíhá hovor ….*

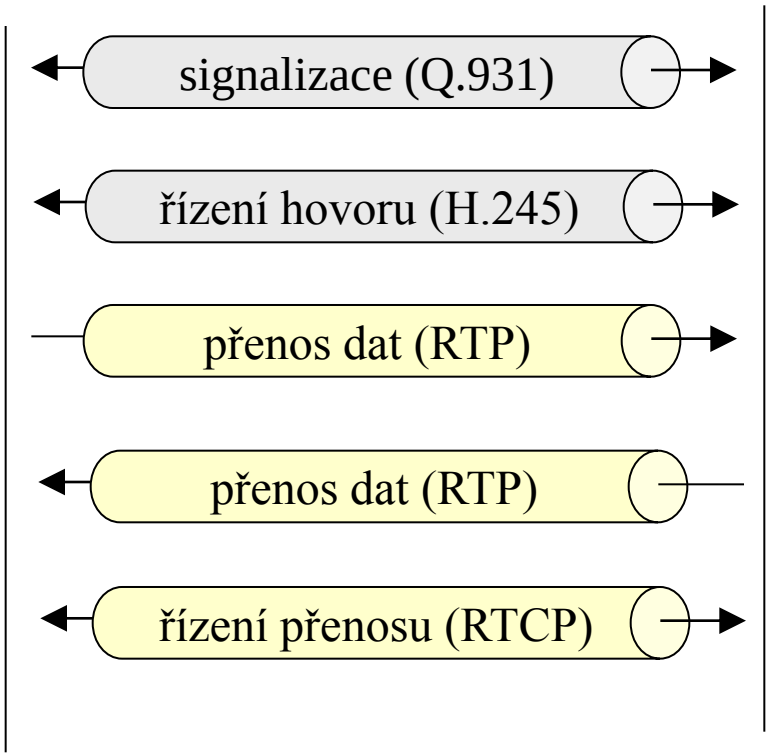


spojení mezi terminály

- komunikace terminálu s gatekeeperem je jednorázová
  - odehrává se na začátku hovoru, kdy se terminál dotazuje gatekeeperu
    - pak se může spojení zrušit
- další komunikace již probíhá přímo mezi terminály
  - mezi nimi existuje několik spojení:
  - 1x (obousměrně) pro signalizaci
    - nad TCP
    - pro protokol Q.931
      - musí přetrvat, aby terminály mohly ukončit svou komunikaci
  - 1x (obousměrně) pro řízení komunikace
    - nad TCP
    - pro protokol H.245
  - 1x dopředný datový kanál
    - RTP nad UDP
  - 1x zpětný datový kanál
    - RTP nad UDP

} mohou být asymetrické

  - 1x (obousměrně) datový řídící kanál
    - RTCP nad UDP



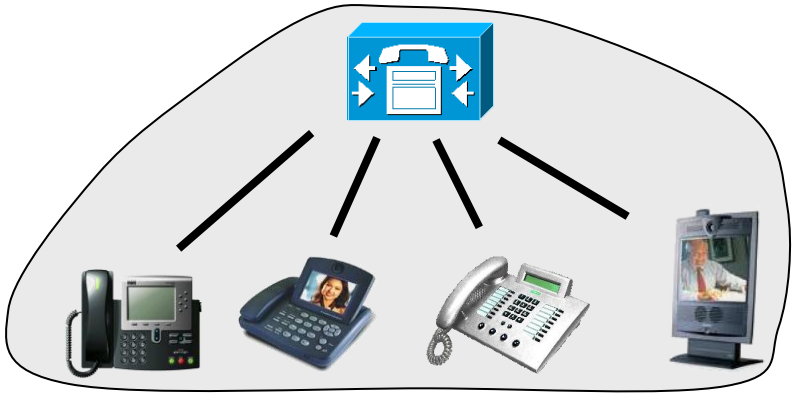
terminály v H.323

- terminály (koncová zařízení) jsou povinné
  - mohou to být jednoúčelová zařízení
    - IP telefony, videotelefony,
  - nebo běžná PC s multimediálním rozšířením
- povinná je podpora hlasových služeb
  - povinný je audiokodek G.771
    - odpovídá kódování PCM
  - další kodeky jsou volitelné
    - doporučeny jsou G.723.1 a G.729
- povinná je podpora:
  - H.225
    - signalizace
  - H.245
    - řízení hovoru
  - RTP/RTCP
    - přenos dat
- podpora videoslužeb je volitelná
  - doporučeny jsou videokodeky H.261 and H.263
- podpora datových a faxových služeb je volitelná
  - pokud je implementována, řeší se standardy z ISDN
    - T.120 – Data conferencing.
    - T.38 – Fax.

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

gatekeeper v H.323

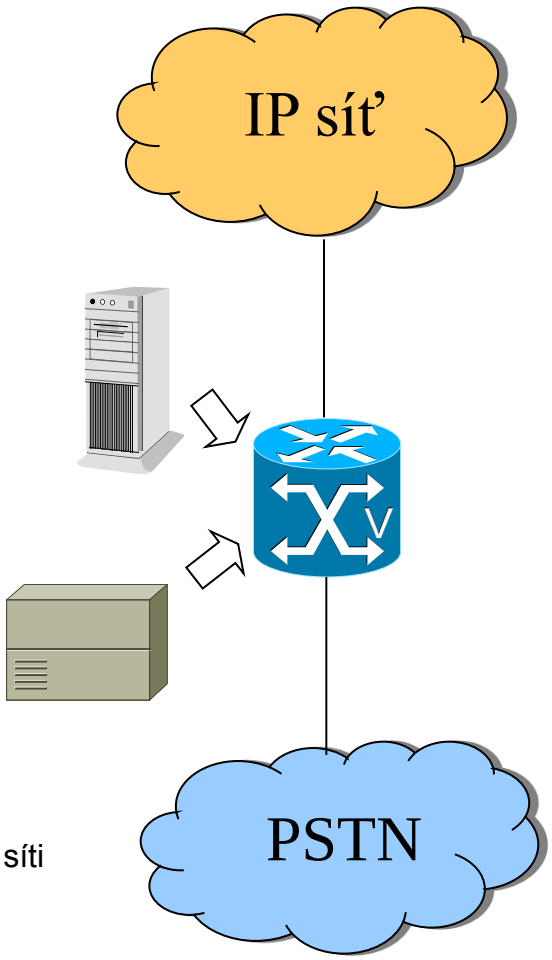
- funkce gatekeeper-u je v H.323 nepovinná
  - ale pokud gatekeeper existuje, musí se u něj všechny terminály zaregistrovat a musí používat jeho služby
- zóna:
  - všechny terminály, které "spadají do působnosti" gatekeeperu
    - které se u něj zaregistrovaly
    - terminál kontaktuje gatekeeper UDP broadcastem na port 1718



- gatekeeper zajišťuje:
  - překlady adres
    - např. mezi ITU-T E.164: 221092274 na IP/URL: 147.32.53.1:1700
  - správu zóny
    - kdo je členem, kdo ne, …
  - řízení přístupu
    - zkoumá, zda lze sestavit hovoru, přidělit přenosovou kapacitu atd.
  - řízení přenosové kapacity
    - přiděluje kapacitu na základě požadavků,
  - volitelně:
    - zajišťuje signalizaci a řízení hovorů
      - standardně si řeší terminály samy
    - zajišťuje správu přenosových kapacit
      - podpora QoS, změna přidělené kapacity atd.
    - autorizuje hovory
      - rozhoduje, zda smí být spojeny

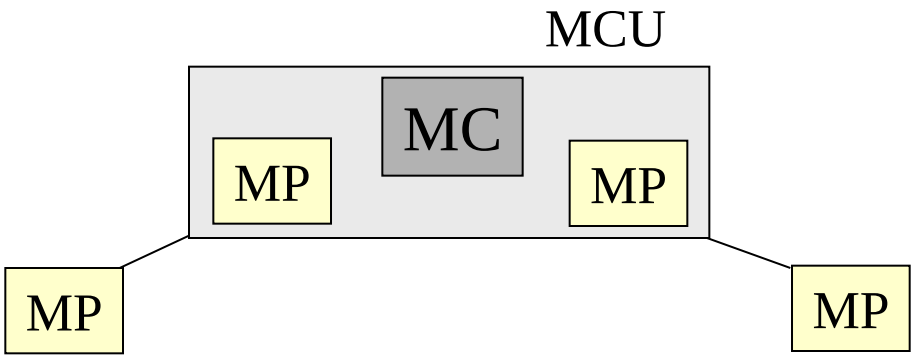
gateway (brána) H.323

- brána zajišťuje přechod (konverze) mezi systémy s různými protokoly
  - nejčastěji:
    - mezi systémem IP telefonie a klasickou telefonní sítí
  - ale také:
    - mezi jinak řešenými systémy IP telefonie
- představa:
  - brána (gateway) je z jedné strany telefonní ústředna, z druhé počítač
- konverzní funkce:
  - konverze na úrovni přenosu dat
    - Ethernet, ATM, …
  - konverze datového obsahu
    - převod mezi různé kódovaným hlasem
      - např. z/do G.711 (PCM), které se používá v klasické telefonní síti
  - konverze signalizačních protokolů
    - signalizace v H.323 a v klasické telefonní síti se liší
    - klasická telefonní síť používá signalizaci SS7, případně DSS1



MCU – Multipoint Control Unit v H.323 (jednotka pro řízení konferenčního spojení)

- slouží potřebám konferencí
  - současné komunikaci více terminálů
- zajišťuje:
  - domluvu na společných vlastnostech konference
    - jaké kodeky se budou používat
    - ….
  - vlastní průběh konference
    - distribuci konferenčních dat style point-to-multipoint
      - realizuje multicast



- MCU má dvě části:
  - MC (Multipoint Controller)
    - řídí sestavování konference
      - zjišťuje vlastnosti terminálů v konferenci,
      - inicializuje a ukončuje kanály pro audio, video a datové přenosy
  - MP (Multipoint Processor)
    - zpracovává multimediální data přenášená v konferenci
      - zajišťuje multicast
    - jde o volitelný modul
      - pokud je realizován, může být i samostatný (vzhledem k MCU).
    - jednotek MP může být i více

vývoj standardu H.323

- verze 1 (květen 1996)
  - definuje základní architekturu, včetně:
    - terminálu
    - gateway (brány)
    - gatekeeper (správce)
    - MCU (jednotky pro řízení konferenčního spojení)
  - ještě moc nepočítala s potřebami IP telefonie
    - spíše zaměřena na potřebu videokonferencí v počítačových sítích
- verze 2 (leden 1998)
  - větší podpora IP telefonie
    - např. rychlejší navazování spojení, podpora zabezpečení, integrace datových služeb, identifikace volajícího, přesměrování hovorů atd.
- verze 3 (září 1999)
  - přinesla hlavně rozšíření doplňkových služeb
    - parkování hovoru, čekající volání, čekající zprávy
  - rozšíření o mechanismy správy a dohledu
  - spolupráce mezi gatekeeperem a mechanismy rychlého sestavování spojení v paketových sítích
- verze 4 (listopad 2000)
  - větší spolehlivost
  - snazší rozšiřitelnost
  - možnost použití URL
    - pro adresy volaných
- verze 5 (květen 2003)
  - lepší návaznost na protokoly TCP/IP

SIP (Session Initiation Protocol)

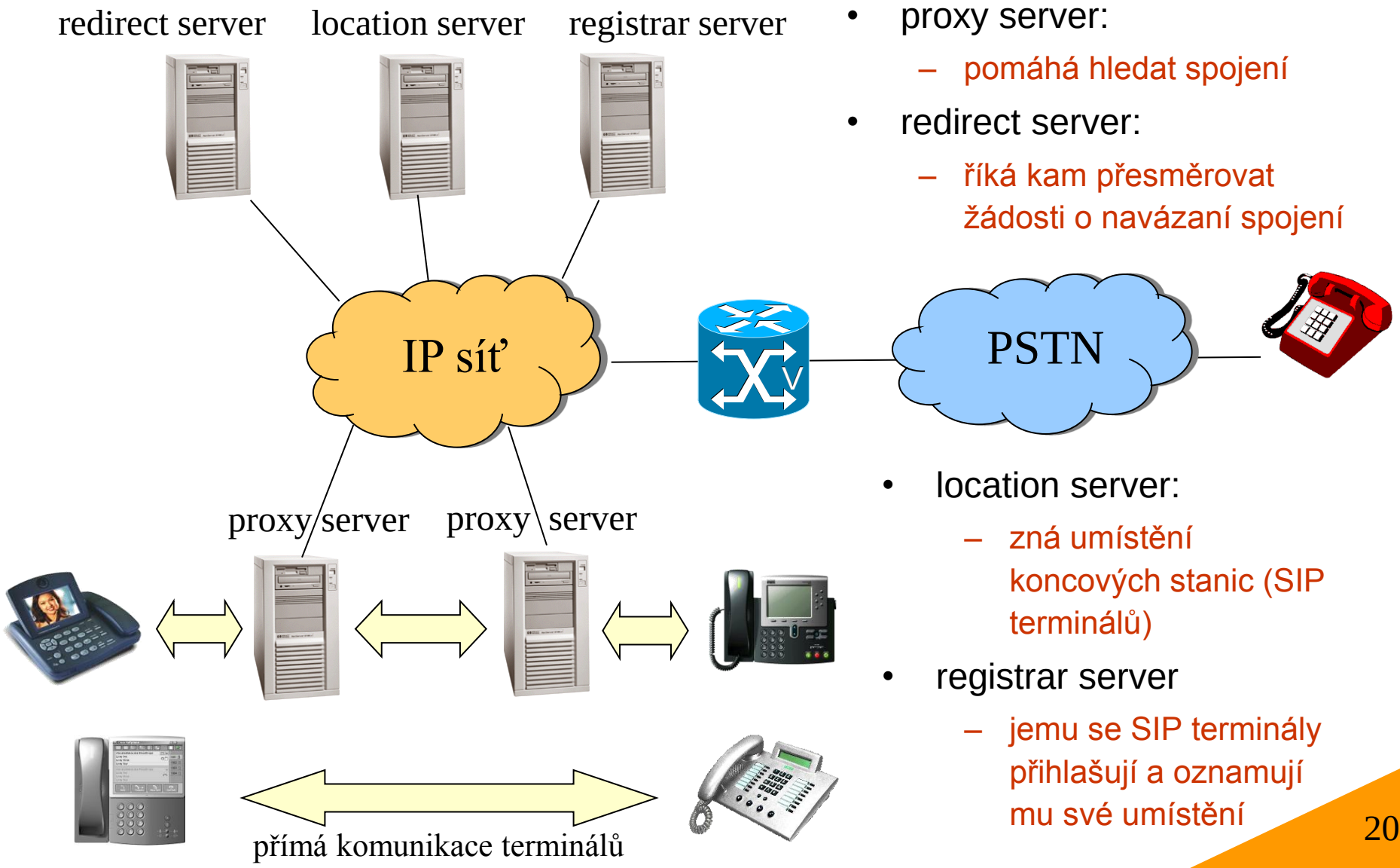
- řešení (nejen) pro IP telefonii ze světa TCP/IP
  - výstup pracovní skupiny MMUSIC v rámci IETF
    - práce započaly v roce 1995
    - první RFC přijato v roce 1999
    - další verze v roce 2002
- SIP je pouze signalizační protokol
  - řeší:
    - sestavení spojení (relace) mezi dvěma či více účastníky
    - dohled nad používáním tohoto spojení
    - rušení spojení (relace)
  - neřeší:
    - vlastní přenosy dat
    - řízení hovoru
      - dohadování na schopnostech zařízení, použitých kodecích atd.
- SIP lze využít například i pro Instant Messaging a další služby

- SIP je (jeden) protokol aplikační vrstvy
  - H.323 byl "deštníkem" nad řadou dalších protokolů
- SIP je jednoduchý textový protokol
  - blízký protokolu HTTP
  - jeho filosofie je blízká WWW
  - lze jej dobře integrovat s dalšími protokoly TCP/IP
- na SIP navazují další protokoly, které řeší řízení hovoru
  - nejčastěji SDP
    - Session Description Protocol
    - řeší:
      - kódování multimediálních dat
      - schopnosti zařízení
      - čísla portů pro datové přenosy
    - zprávy SDP jsou zapouzdřeny ve zprávách SIP !!!

filosofie SIP-u

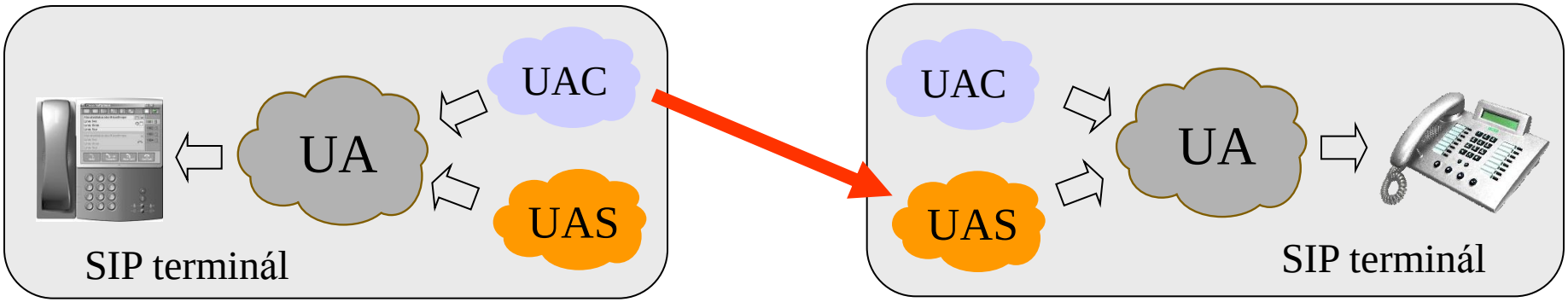
- účastníci se mohou dynamicky přemisťovat
- je třeba:
  - identifikovat je nezávisle na jejich poloze
    - vhodné SIP adresy
  - mít možnost zjistit kde se právě nachází
    - dát jim šanci oznámit jejich aktuální polohu
      - "operace REGISTER"
      - účastník se na novém místě zaregistruje
  - umět jim předávat pozvání k navázání spojení/relace
    - tak aby se volající nemusel sám zjišťovat kde se volaný nachází
      - "operace INVITE"
    - síť (SIP) se postará o správné vyhledání a předání výzvy

architektura SIP



- proxy server:
  - pomáhá hledat spojení
- redirect server:
  - říká kam přesměrovat žádosti o navázaní spojení
- location server:
  - zná umístění koncových stanic (SIP terminálů)
- registrar server
  - jemu se SIP terminály přihlašují a oznamují mu své umístění

architektura SIP



- **UA** (User Agent)
  - nachází se v každém SIP terminálu nebo bráně
    - včetně proxy serveru
  - obsahuje:
    - **UAC**: User Agent Client
      - žádá o spojení
    - **UAS**: Use Agent Server
      - přijímá žádosti o spojení

- styl komunikace mezi UAC a UAS je velmi podobný komunikaci WWW klienta a WWW serveru pomocí HTTP
  - posílají si požadavky formulované jako metody
    - v textové formě
    - a upřesněné hlavičkami
  - odpovědi jsou číselné
    - stejná konvence jako FTP, SMTP a HTTP
- komunikace může probíhat po UDP nebo TCP
  - není to předepsáno

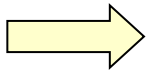
SIP – metody a odpovědi

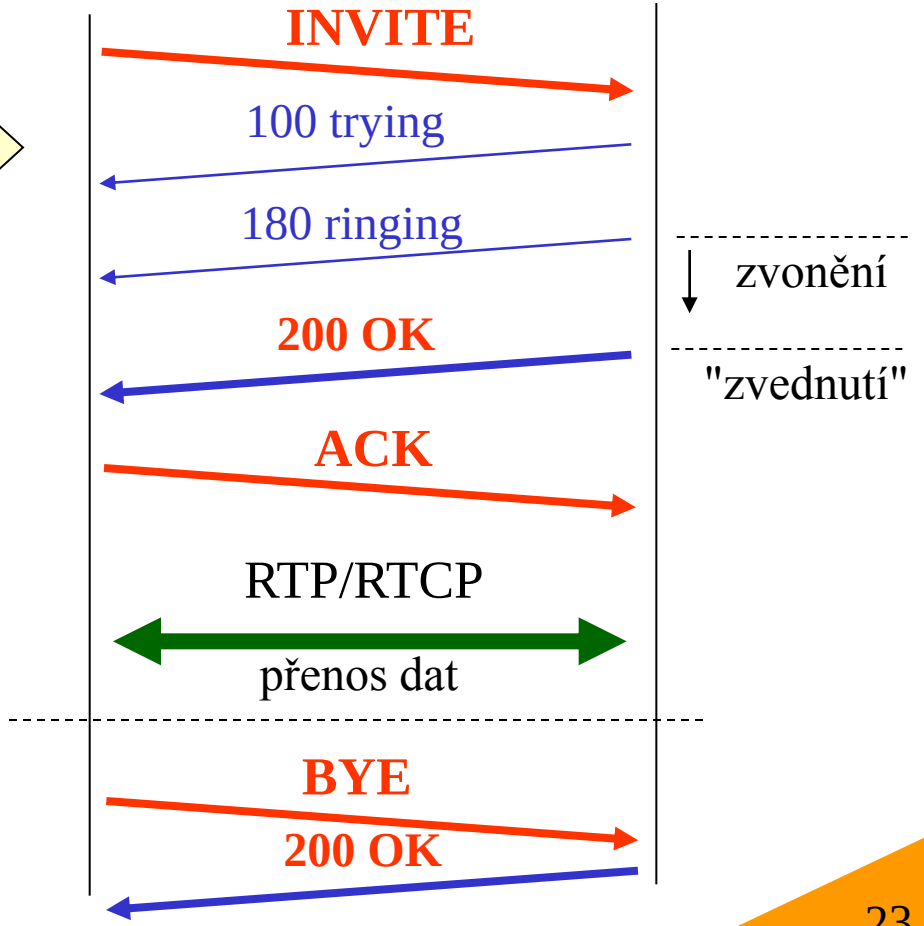
- INVITE
  - žádost o sestavení spojení
  - může být přijata, odmítnuta, přesměrována atd.
- ACK
  - potvrzení volajícího, že dostal odpověď na svou žádost INVITE
- BYE
  - ukončení spojení
- CANCEL
  - ukončení nesestaveného spojení
- REGISTER
  - registrace UA
- OPTIONS
  - dotaz na možnosti a schopnosti serveru

- 1XX
  - informační zprávy
    - např. 100 Trying, 180 Ringing
- 2XX
  - kladná odpověď - úspěšné vyřízení
    - např. 200 OK
- 3XX
  - přesměrování, dotaz je třeba směřovat jinam
    - 302 Moved Temporarily", "305 Use Proxy")
- 4XX
  - chybný požadavek
    - dotaz by se neměl ve stejné podobě opakovat
    - např. 403 Forbidden
- 5XX
  - chyba serveru
    - např. 500 Server Internal Error, 501 Not Implemented
- 6XX
  - globální (celková, zásadní) chyba
    - např. 606 Not Acceptable

SIP – navazování a rušení spojení

- nejjednodušší případ:
  - když volající koncové zařízení (UA) zná umístění volaného UA:
    - osloví jej přímo
    - navazování spojení představuje 3-fázový handshake
- jiné možnosti:
  - volající osloví proxy server
    - ten zajistí vyhledání volaného
    - sám předá žádost o navázání spojení dál
      - cílovému UA
  - volající osloví redirection server
    - server vrátí volajícímu adresu volaného UA, na kterou se má obrátit
      - obdoba ICMP redirect
- ukončení spojení:
  - může iniciovat kterákoli strana

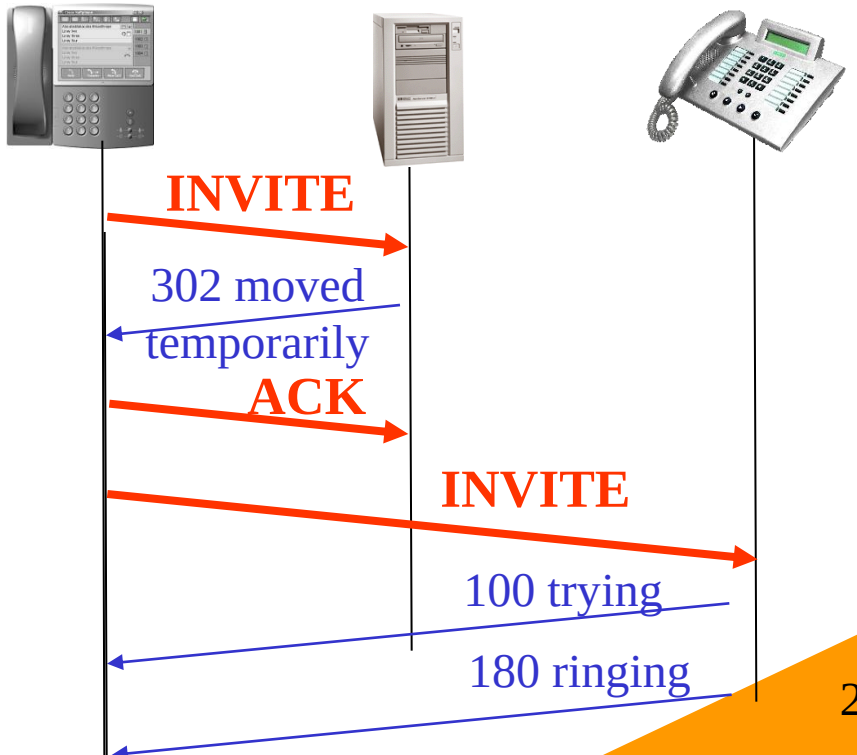




SIP – navazování a rušení spojení

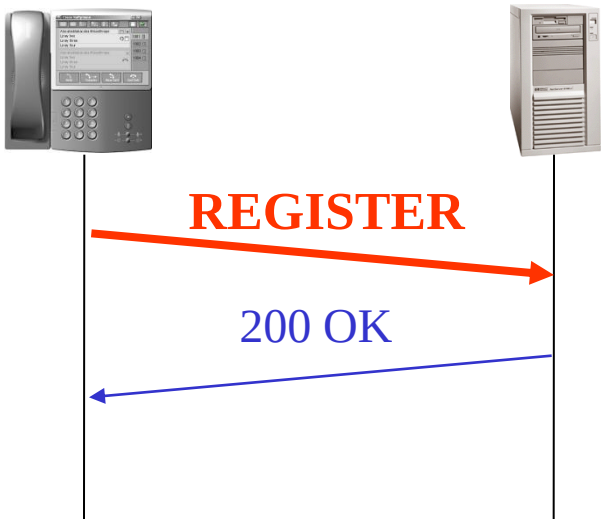
- když volající nezná přesnou adresu či cestu k volanému
  - může využít služeb proxy serveru nebo redirect serveru
- proxy server:
  - přijme žádost INVITE
  - určí komu ji předat dál
  - sám ji předá dál

- redirect server:
  - přijme žádost INVITE
  - určí komu ji předat dál
  - vrátí informace o správném směrování tomu, kdo zaslal výzvu INVITE
    - a ten by měl sám kontaktovat cíl

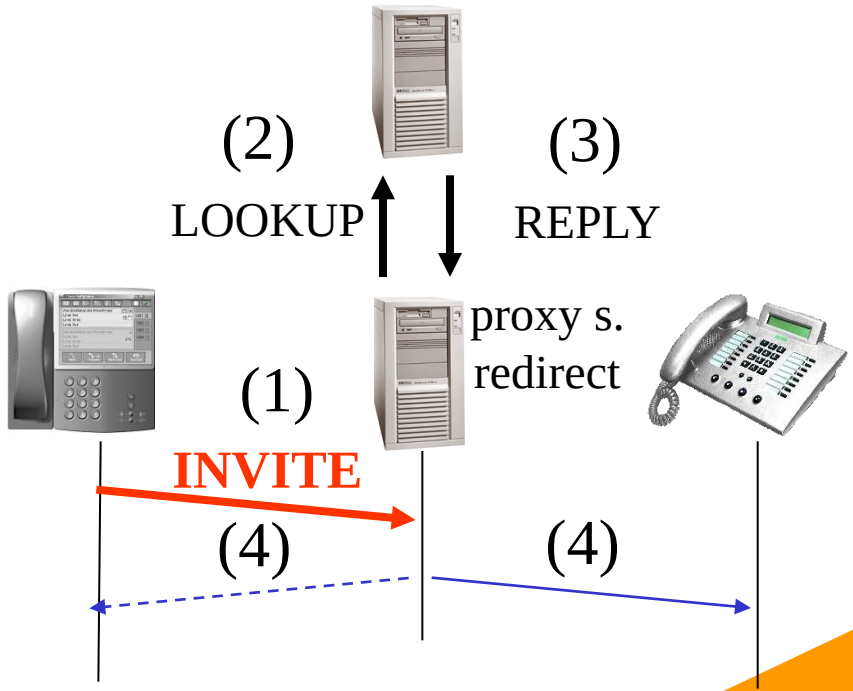


SIP – location a registrar server (oba servery obvykle splývají)

- registrar server:
  - přijímá metody REGISTER
    - registrace od klientů (UAC)
  - může podporovat autentizaci
    - terminál se musí prokázat že je tím za koho se vydává
- kdykoli je nějaký SIP terminál zapnut:
  - musí najít nejbližší registrar server a zaregistrovat se u něj



- location server:
  - pomáhá proxy serverům a redirect serverům hledat cestu k volanému
    - servery se ho dotazuji, on odpovídá
  - metody LOOKUP a REPLY nejsou součástí SIP-i

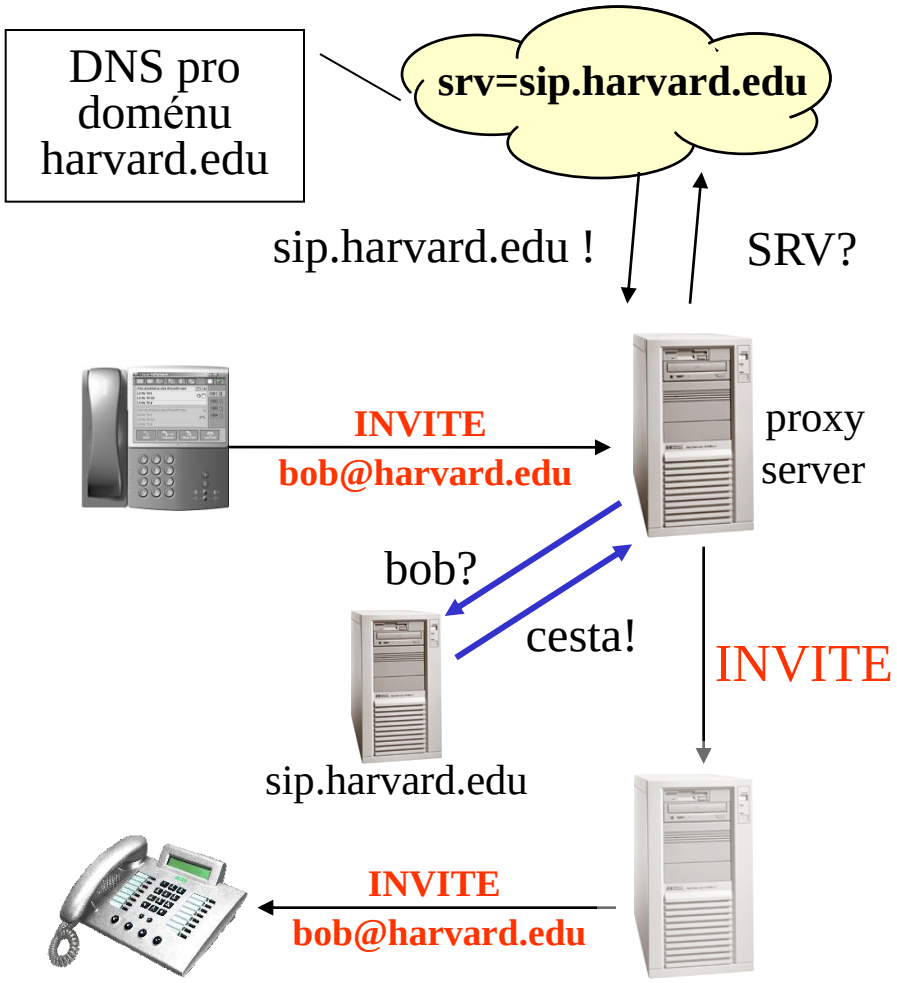


"vize SIP"

- protokol SIP vznikal s představou, že:
  - telefonní hovory a videokonferenční volání vznikají v Internetu
  - lidé jsou identifikováni jmény či emailovými adresami
    - a ne telefonními čísly
  - volaného je možné zastihnout bez ohledu na to, kde se právě nachází a jaké zařízení používá
- kvůli tomu SIP musí řešit i vhodné adresování a přesměrovávání
  - "nezávislost na umístění"
    - SIP by měl být schopen předat pozvání účastníkovi bez ohledu na to, kde se právě nachází
- SIP by měl fungovat v reálném čase
  - SIP by měl sloužit nejen IP telefonii, ale třeba i Instant Messagingu a dalším aplikacím
- SIP adresy:
  - obecně jde o jednu z variant URL adresy
    - <schema>:<specifická část>
  - konkrétně:
    - sip:user@host
    - sip:user@doména
  - například:
    - sip:**bob@192.168.10.1**
      - lze poslat INVITE přímo
    - sip:**bob@harvard.edu**
      - nutno řešit přes PROXY
- jak se SIP adresy překládají?
  - prostřednictvím DNS se vyhledá registrar a location server pro danou doménu

překlad SIP adres

- v DNS je nový typ RR záznamu:
  - SRV <IP adresa>
    - udává IP adresu (registrar) serveru pro danou doménu
- použití v praxi
  - pokud volající nezná IP adresu volaného:
    - pošle svůj INVITE nejbližšímu SIP proxy serveru
  - proxy server funguje jako DNS server a router
    - zjistí si SRV záznam příslušné domény
      - z něj zjistí adresu registrar serveru domény
    - zeptá se registrar serveru / location serveru
      - získá informace o tom, kudy má výzvu INVITE předat dál
      - pokud se uživatel přemístil někam jinam a tam se zaregistroval, měl by o tom mít registrar/location server informace
    - výzvu INVITE sám předá dál
  - obdobně funguje redirect server
    - který ale jen vrátí informace volajícímu
    - volající pak sám předává INVITE dál



hlavičky (SIP headers)

- obdobně jako u HTTP, mohou požadavky i odpovědi protokolu SIP obsahovat také doplňující hlavičky (headers)
  - slouží jako parametry
  - upřesňují požadavek/odpověď
- příklad:

  INVITE sip:Bob <bob@harvard.edu>

  FROM: sip:Alice <Alice@harvard.edu>

  Subject: chci s tebou mluvit kvuli …

  Content-type: application/SDP

  …….
- pro specifikaci datových typů se používá MIME typ
  - např. application/SDP
    - že jde o něco, co má zpracovávat aplikace registrovaná pro zpracování protokolu SDP (Session Description Protocol)
- součástí požadavku (i odpovědi) může být také část formulovaná v SDP
  - upřesňuje "technické parametry", například použité kodeky, schopnosti zařízení atd.
- příklady hlaviček:
  - FROM: <sip adresa>
    - od koho přichází žádost o spojení
      - povinné
  - TO: <sip adresa>
    - komu je výzva určena
      - stejné jako parametr u INVITE
      - povinné
  - VIA: <adresa>
    - informace o tom, kudy byl požadavek veden
      - přes který proxy server
  - CALL-ID: <identifikátor>
    - jednoznačný identifikátor požadavku
      - pro hovor: říká který hovor to je
        - » např. pro následné ukončení
        - » pro vyloučení opakovaných výzev apod.
      - pro registraci: vylučuje duplicitu
        - » každý uzel by (až do nového bootu) měl používat stejné ID
  - Content-Type: <MIME type>
  - Content-Length: <délka>
  - Content-Encoding: <id.>

příklad

```
-----------------------------------------------------------------
                        SIP Header
-----------------------------------------------------------------
INVITE sip:5120@192.168.36.180 SIP/2.0
Via: SIP/2.0/UDP 192.168.6.21:5060
From: sip:5121@192.168.6.21
To: <sip:5120@192.168.36.180>
Call-ID: c2943000-e0563-2a1ce-2e323931@192.168.6.21
CSeq: 100 INVITE
Expires: 180
User-Agent: Cisco IP Phone/ Rev. 1/ SIP enabled
Accept: application/sdp
Contact: sip:5121@192.168.6.21:5060
Content-Type: application/sdp
```

protokol SDP
(Session Description Protocol)

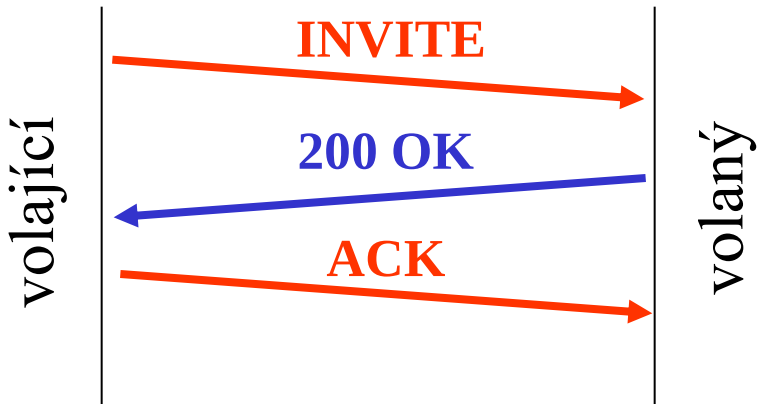
- pokud je v požadavku/odpovědi hlavička:
  - **Content-type: application/SDP**
- pak tělo "patří" protokolu SDP
  - podrobněji popisuje technické parametry
  - odděleno prázdnou řádkou od hlaviček
- SDP umožňuje odesilateli popsat svůj RTP/AVP
  - Audio/Video Profil a schopnosti přenosu dat
    - např. jaké kodeky podporuje
    - jaké metody šifrování
    - jakou vyžaduje šířku přenosového pásma
    - jakou latenci, rychlost atd.

- příklad:
  - m = audio RTP/AVP 0 3 4 5

Číslo	Kodek	Frekvence [Hz]
0	PCM	8000
1	Rezerva	
2	Rezerva	
3	GSM	8000
4	G.723	8000
5	DVI4	8000
…..	…..	…..

dialog protokolu SIP

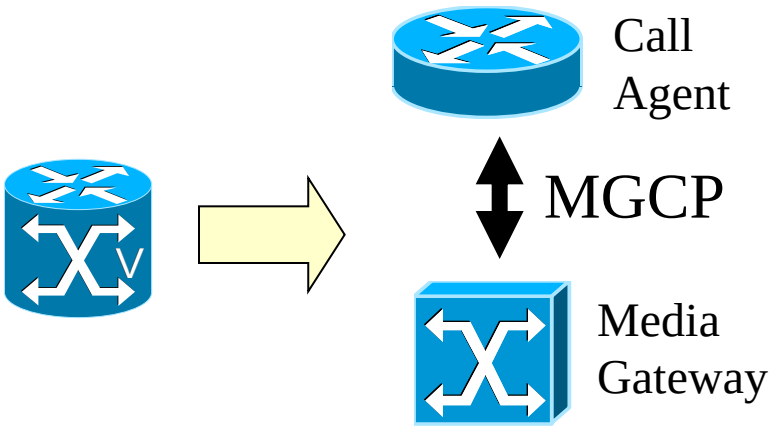
- výzvu INVITE může příjemce akceptovat
  - odpovědět 200 OK
    - a v rámci odpovědi poslat své schopnosti
    - jeho schopnosti se mohou týkat opačného směru komunikace
      - komunikace nemusí být symetrická, každý směr může být řešen jinak, např. s různou rychlostí / kapacitou, s jiným kódováním atd.
- problém:
  - volajícímu (odesilateli výzvy) to nemusí vyhovovat
    - nemusí na to mít schopnosti
  - proto je nutný 3-fázový handshake
    - aby volající mohl vyjádřit souhlas či nesouhlas se schopnostmi/požadavky příjemce výzvy



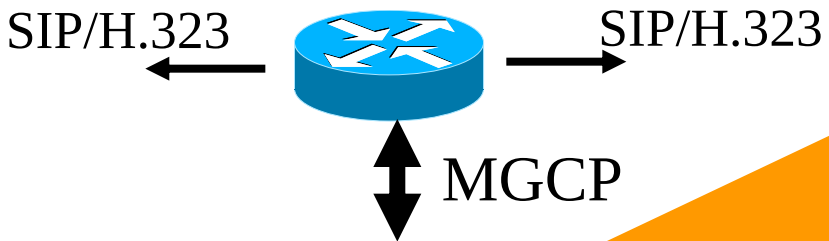
- příjemce může výzvu odmítnout:
  - 603 Decline
    - nechce ji přijmout
    - může navrhnout jiný termín
  - 606 Not Acceptable
    - nemůže ji přijmout
    - obvyklý důvod:
      - některé parametry navazovaného spojení (např. kodeky) nepodporuje
    - v odpovědi může popsat své možnosti
      - pomocí protokolu SDP
- průběh dalšího dialogu není předepsán
  - zda volající reaguje na odmítnutí zcela novou výzvou
    - nové Call-ID
  - nebo upřesňuje původní výzvu
    - stejné Call-ID

MGCP (Media Gateway Control Protocol)

- jde o řešení, které umožňuje oddělit
  - přepojování hovorů
    - ve smyslu "hloupé ústředny"
    - zajišťuje "Media Gateway"
  - rozhodování o směrování hovorů
    - obdoba centralizovaného směrování, s route serverem
    - zajišťuje "Call Agent"
      - resp. Media Gateway Controller
  - MGCP je protokol, prostřednictvím kterého spolu obě části komunikují



- vztah MGCP k H.323 a SIP-u
  - H.323 a SIP jsou protokoly pro komunikaci stylem peer-to-peer
    - mezi prvky na stejné úrovni
  - MGCP je protokol charakteru klient/server
    - Call Agent se chová jako server
      - poskytuje řídící informace pro Media Gateway
    - Media Gateway se chová jako klient
  - MGCP není náhrada pro SIP ani H.323
    - je spíše jejich doplňkem
    - Call Agent může komunikovat (spolupracovat) s ostatními "Call Agents" pomocí SIP nebo H.323

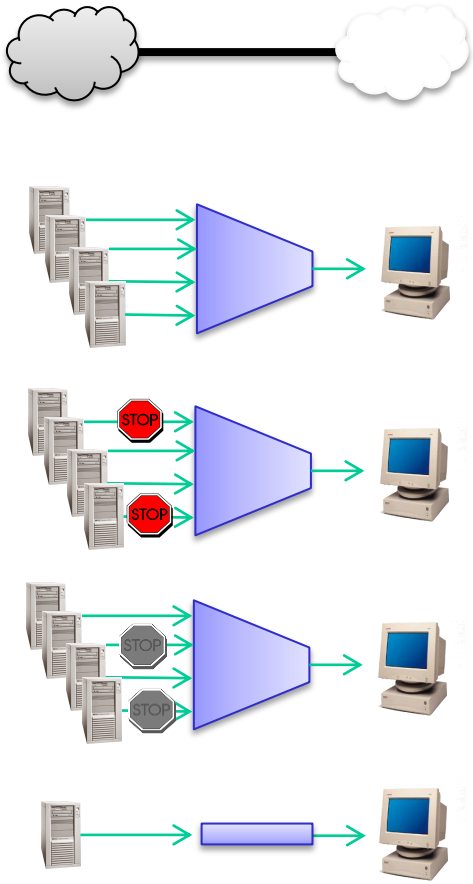


SIP vs. NAT/PAT

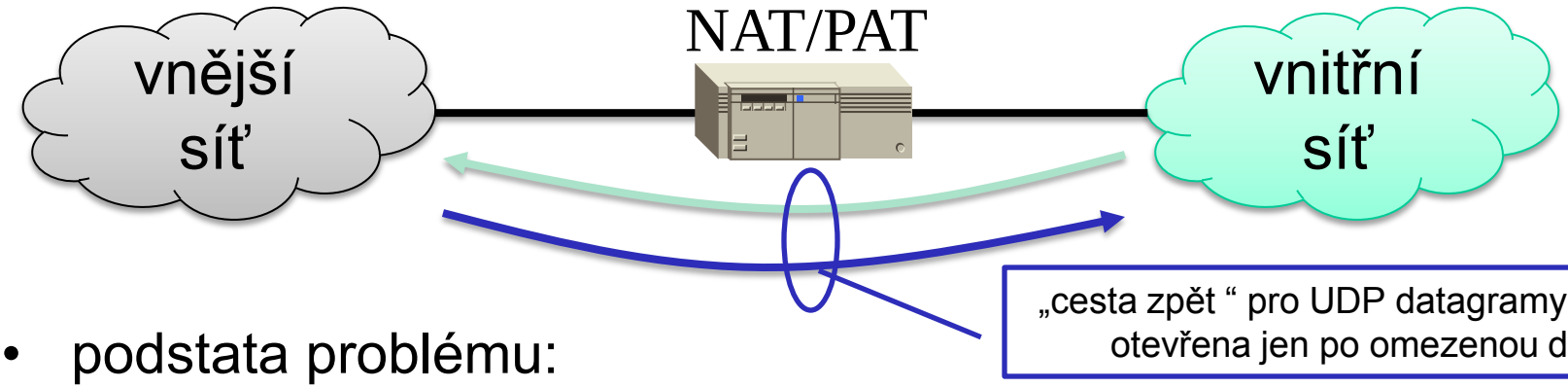
- nebezpečí (pro NAT obecně):
  - nelze navazovat spojení směrem dovnitř
  - pro některé aplikace/služby nemusí NAT fungovat vůbec
    - pro takové, které přenáší IP adresy i jinde než v hlavičce (kde o tom NAT neví a nemůže adresy měnit – např. IPSEC)
  - "inteligentní NAT"
    - snaží se rozpoznat konkrétní protokoly, které skrz něj prochází, a mění IP adresy i v těle IP paketů
- problémy SIP-u s NATem
  - zprávy REGISTER prochází (obvykle) bez problémů
    - jsou iniciovány z privátní sítě
  - zprávy INVITE se nedostanou „dovnitř“
    - mechanismus NAT je nepropustí do privátní sítě, jsou iniciovány „zvenčí“

jiná klasifikace NATů

- představa:
  - odeslání dat v vnitřní sítě vzniká „dočasný průchod“ skrze NAT
    - NAT si pamatuje vazbu mezi vnitřní a vnější adresou (i porty)
      - ale jen po omezenou dobu!!!!
  - klasifikace je založena na tom, kdo (z vnější strany) může využít tento dočasný průchod, pro přenos dat „dovnitř“
- full cone:
  - jakmile je „dočasný průchod“, může ho využít kterýkoli vnější uzel
- IP restricted cone:
  - „dočasný průchod“ mohou využít jen některé vnější uzly
    - podle IP adres, proto „IP restricted“
- port restricted cone:
  - „dočasný průchod“ mohou využít jen některé vnější uzly
    - podle čísel portů, proto „port restricted“
- symmetrical NAT
  - „dočasný průchod“ může využít jen vnější uzel, kterému byla odeslána původní data



technika “hole punching“, UDP keep-alive messages

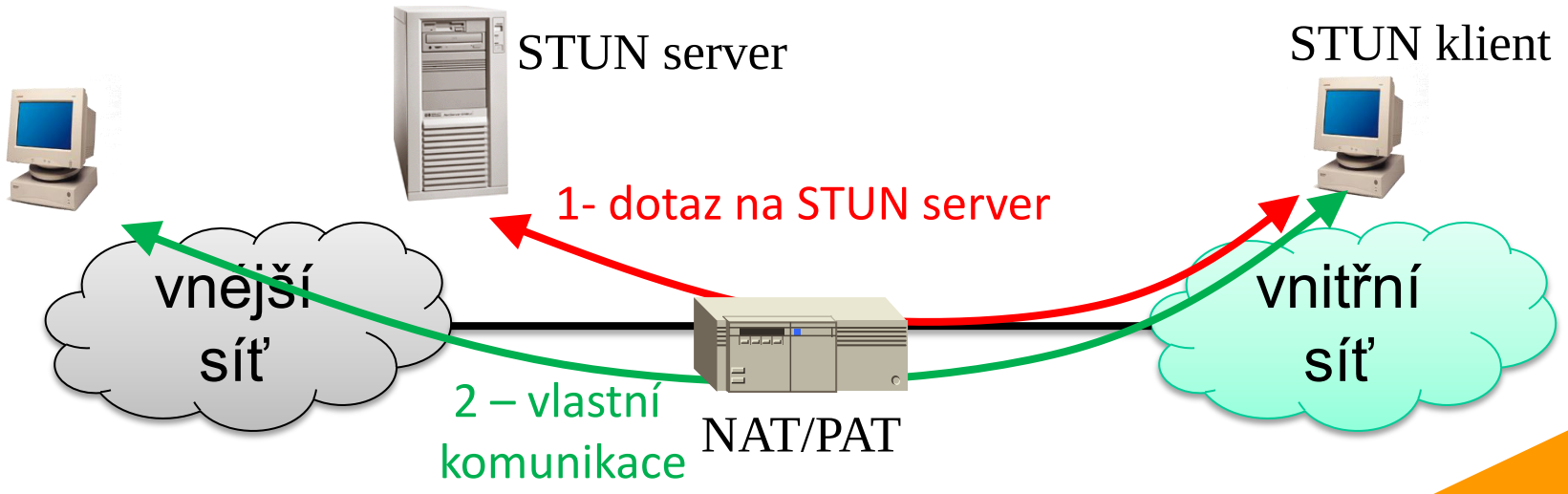


- podstata problému:
  - mechanismus NAT/PAT musí umožňovat odpověď na odchozí UDP datagramy
    - pamatovat si vazbu mezi vnitřními a vnějšími adresami a porty
      - tj. komu mají být předány ve vnitřní síti (IP:port)
  - ale jen po omezenou dobu
    - typicky 30 až 180 sekund
      - pro TCP: 30 až 60 minut !!!
    - pak možnost odpovědi expiruje
      - již není možné poslat UDP datagram „dovnitř“

- princip řešení (keep-alive):
  - „vnější“ uzel musí pravidelně posílat „dovnitř“ nějaká data (zprávu), aby nenechal expirovat možnost odpovědi
    - dříve než za 30 až 180 sekund
- problém:
  - narušuje to mechanismy pro šetření energií
    - u 3G/WCDMA roste spotřeba 3 až 16x !!!!

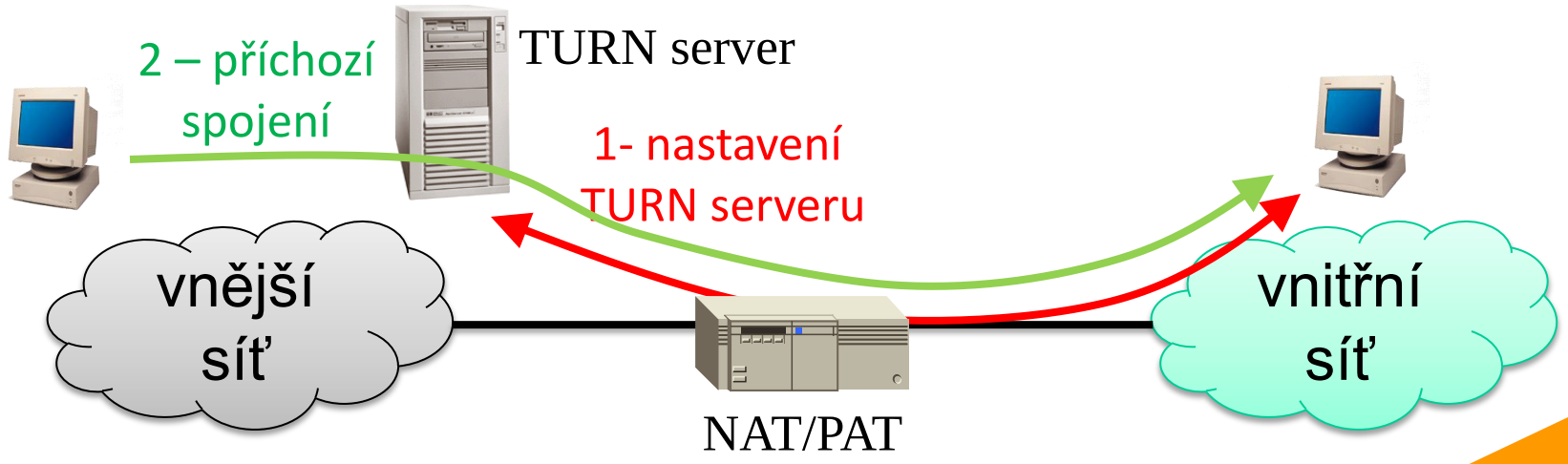
řešení pomocí protokolu STUN

- STUN
  - dříve: Simple Traversal of UDP through NAT,
  - dnes: Session Traversal Utilities for NAT
- princip:
  1. uzel/aplikace ve vnitřní síti se zeptá (STUN serveru) na to, za jakým typem NATu se nachází a jak je „vidět“ zvenku (pod jakou IP adresou)
     - STUN je protokol, prostřednictvím kterého je kladen dotaz a zasílána odpověď
  2. podle informací, které získá (od STUN serveru), se aplikace snaží „překonat“ NAT a komunikovat s vnějšími uzly



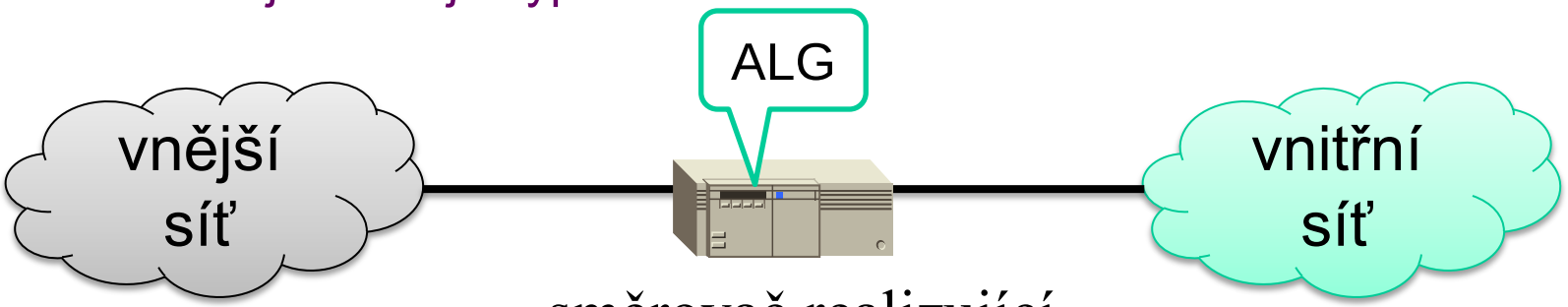
řešení pomocí protokolu TURN

- TURN
  - Traversal Using Relay NAT
- princip:
  - TURN server funguje jako proxy brána („otvor skrze NAT“), skrze kterou může být navázáno příchozí spojení od jednoho (konkrétního) vnějšího uzlu
    1. vnitřní uzel (klient) požádá TURN server o „zprůchodnění“
    2. příslušný vnější uzel může navázat příchozí spojení



SIP ALG (Application Level Gateway)

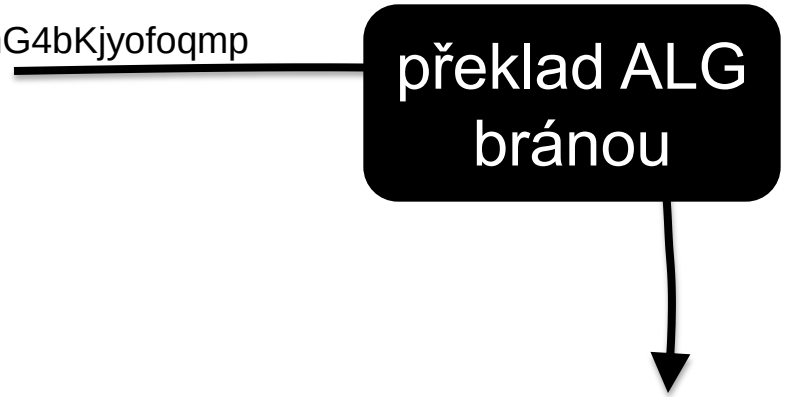
- řešení, zabudované do směrovačů realizujících NAT
- princip fungování:
  - ALG se „dívá dovnitř“ SIP zpráv a podle potřeby v nich přepisuje některé údaje
    - hlavně IP adresy a čísla portů, které se působením NATu mění
- častý problém s ALG:
  - jejich implementace je chybná a komplikuje (znemožňuje) fungování SIPu
  - ALG brány v různých směrovačích bývají často (defaultně) zapnuté
    - a je třeba je vypnout!!!



směrovač realizující NAT/PAT

představa fungování ALG

- INVITE sip:destino@example.com SIP/2.0
- Via: SIP/2.0/UDP **192.168.1.33:5060**;branch=z9hG4bKjyofoqmp
- Max-Forwards: 70
- To: <sip:destino@example.com>
- From: "Iñaki" <sip:ibc@example.com>;tag=nrrrx
- Call-ID: xetazdjyktlpsfo@192.168.1.33
- CSeq: 800 INVITE
- Contact: <sip:ibc@**192.168.1.33:5060**>
- Content-Type: application/sdp
- Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
- Supported: replaces,norefersub,100rel
- User-Agent: Twinkle/1.1
- Content-Length: 312



- INVITE sip:destino@example.com SIP/2.0
- Via: SIP/2.0/UDP **192.0.2.200:12345**;branch=z9hG4bKjyofoqmp
- Max-Forwards: 70
- To: <sip:destino@example.com>
- From: "Iñaki" <sip:ibc@example.com>;tag=nrrrx
- Call-ID: xetazdjyktlpsfo@192.168.1.33
- CSeq: 800 INVITE
- Contact: <sip:ibc@**192.0.2.200:12345**>
- Content-Type: application/sdp
- Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
- Supported: replaces,norefersub,100rel
- User-Agent: Twinkle/1.1
- Content-Length: 312

bridge mode vs. NAT

- NAT je řešení s překladem adres
  - jsou při něm odděleny dvě sítě, které používají různé síťové (IP) adresy
    - NAT mezi nimi překládá
  - sítě jsou propojeny routerem
    - mechanismus NAT je implementován v tomto routeru (směrovači)
- výhoda:
  - šetří IP adresami, umožňuje využít privátní IP adresy v privátní síti
- nevýhoda:
  - problém s NATem

- bridge mode je řešení bez překladu adres
  - nedochází při něm k oddělení dvou sítí
    - obě části (segmenty) jsou stále jednou sítí,
    - obě části používají stále stejné síťové (IP) adresy
  - segmenty jsou propojeny pomocí switche (přepínače)
- výhoda:
  - nejsou zde problémy. spojené s NATem
- nevýhoda:
  - v „privátním“ segmentu nelze použít privátní IP adresy