X36MTI
Moderní technologie internetu

Ing. Pavel Bezpalec, Ph.D.

Katedra telekomunikační techniky
FEL ČVUT v Praze

Pavel.Bezpalec@fel.cvut.cz

© Pavel Bezpalec, 2009

IP telefonie

IP telefonie je **služba** založená na technologii VoIP.

- Alternativa ke klasické telefonii
  - POTS = *Plain Old Telephony Service*
  - POTS využívá principu přepojování okruhů (TDM)
- Internetová telefonie
  - varianta IP telefonie
  - pro přenosy dat využívá veřejný Internet

- Využití
  - veřejná služba
    - např. alternativní operátor
  - privátní služba
    - např. telefonování v rámci firmy
  - jako technologické řešení u operátorů
    - páteřních části svých sítí jsou budovány na principu VoIP a ne principem přepojování okruhů (TDM)
    - např. plán BT

© Pavel Bezpalec, 2009

VoIP – Voice over IP

- Obecné označení pro technologii
  - přenosu digitalizovaného hovoru v sítích s přepojováním paketů dle protokolu IP
- VoD (Voice over Data)
  - obecnější označení než VoIP
  - jakákoli další technologie pro přenos digitalizovaného hovoru po datových sítích
    - VoFR (Voice over Frame Relay)
    - VoATM (Voice over ATM)
    - CVoDSL (Channelized Voice over DSL)
- Realizována různými způsoby
  - proprietárně
    - Alcatel, Avaya, Cisco, Fayn, ICQ, Siemens, Skype ...
  - dle standardů ITU-T, IETF
    - H.323, SIP, MGCP
- Perspektiva VoIP
  - rychlejší rozvoj datových sítí
  - ekonomická výhodnost
  - nové aplikace a doplňkové služby
  - snaha o sjednocení komunikačních standardů a vytvoření sítí s konvergovanými službami

© Pavel Bezpalec, 2009

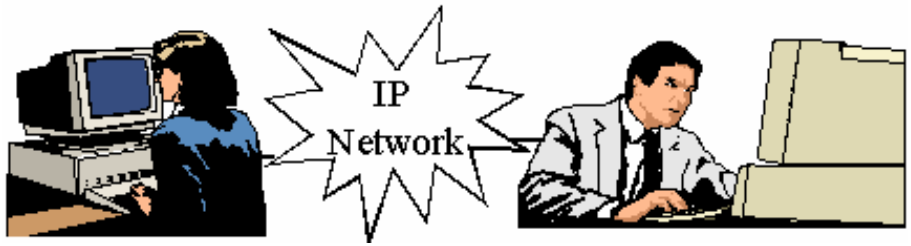
Vlastnosti protokolu IP

- Pro přenos dat nejužívanější protokol
- Paketový princip
  - multiplexování – přenos dat z více zdrojů
- Bezestavový protokol
  - neudržuje se spojení mezi odesílatelem a příjemcem
- Princip best-effort service
  - negarantuje odesílateli, že odeslaná data dojdou v pořádku, včas a ve správném pořadí adresátovi
- Problematická realizace řízení QoS
- Efektivnější využití poskytnutého pásma
  - oproti TDM systémům

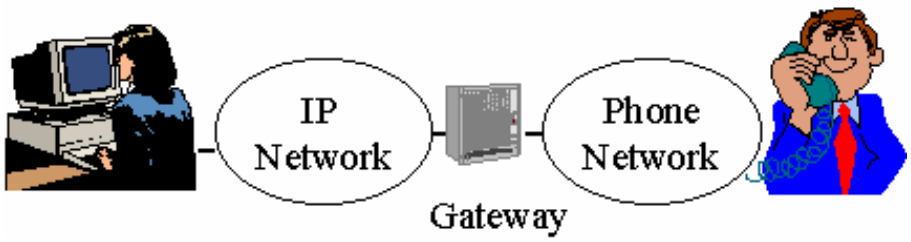
© Pavel Bezpalec, 2009

Scénáře použití IP telefonie

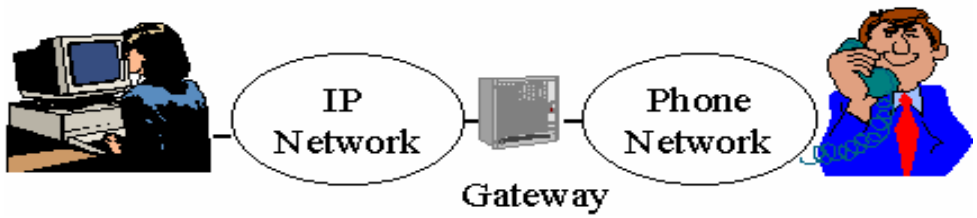
- **PC to PC**
  - komunikace mezi PC
  - označení účastníka IP adresou



- **PC to Phone**
  - komunikace mezi PC a telefonním systémem
  - označení účastníka tel. číslem

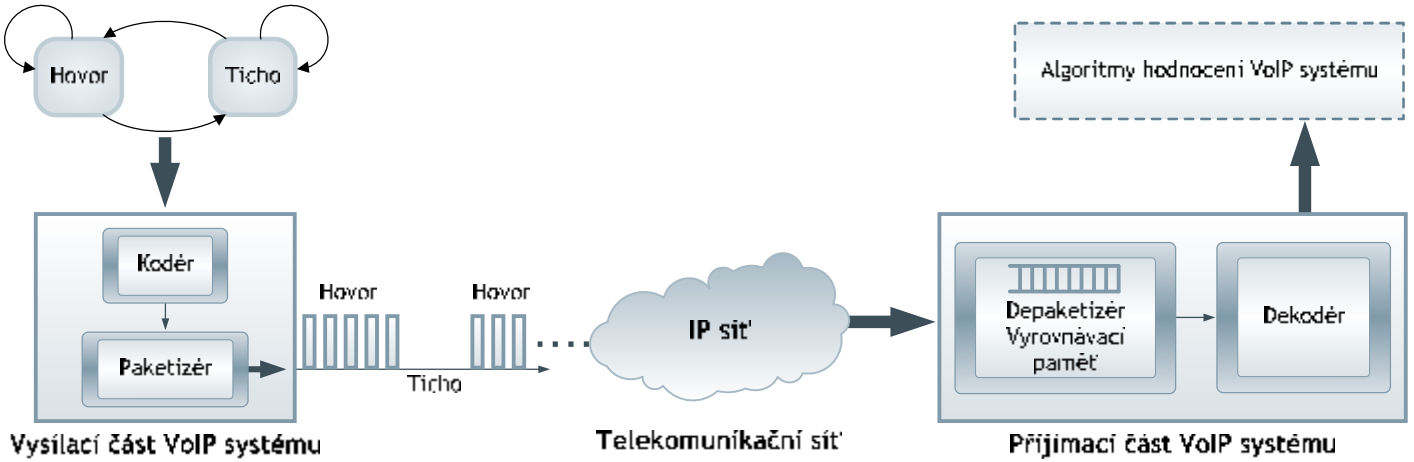


- **Phone to Phone**
  - komunikace mezi telefonními systémy prostřednictvím IP sítě
  - označení účastníka tel. číslem



© Pavel Bezpalec, 2009

VoIP systém

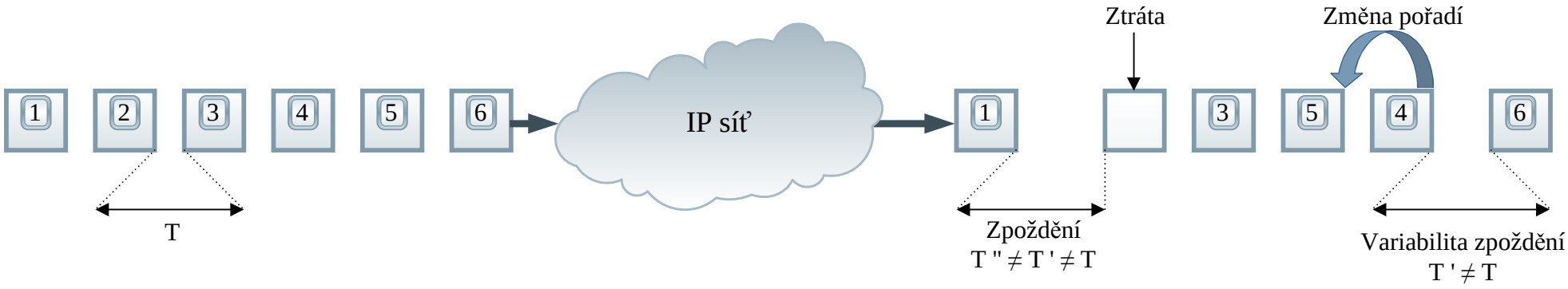


- Vysílací část
  - kodér
  - paketizér
  - řadič rozhraní sítě
- Telekomunikační síť
  - směrovače
  - přenosové prostředky
- Přijímací část
  - vyrovnávací paměť
  - depaketizér
  - dekodér

© Pavel Bezpalec, 2009

Základní úskalí při IP telefonním přenosu

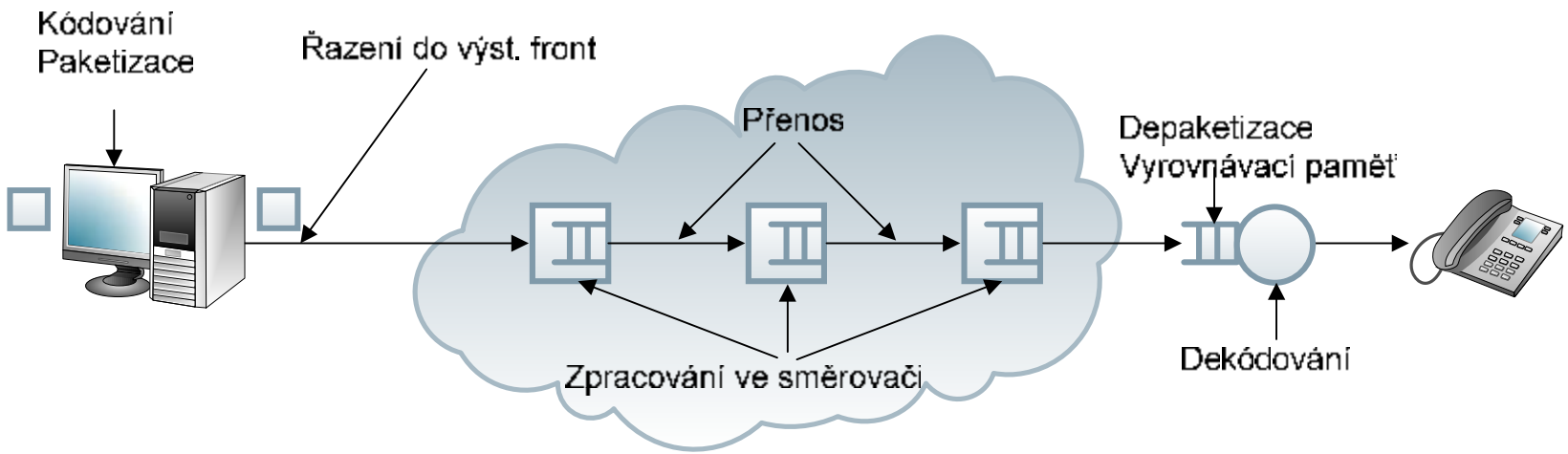
- **Zpoždění** – *Latency*
- **Ztráta paketů** – *Packet Loss*
- **Změna pořadí paketů** – *Packet Order*
- **Variabilita zpoždění** – *Delay Jitter*



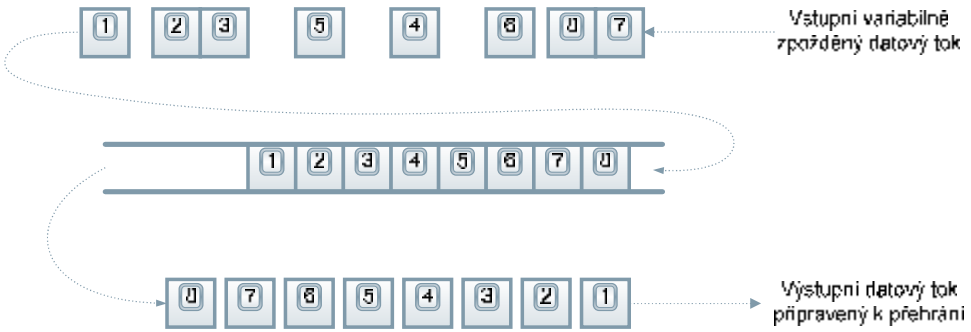
© Pavel Bezpalec, 2009

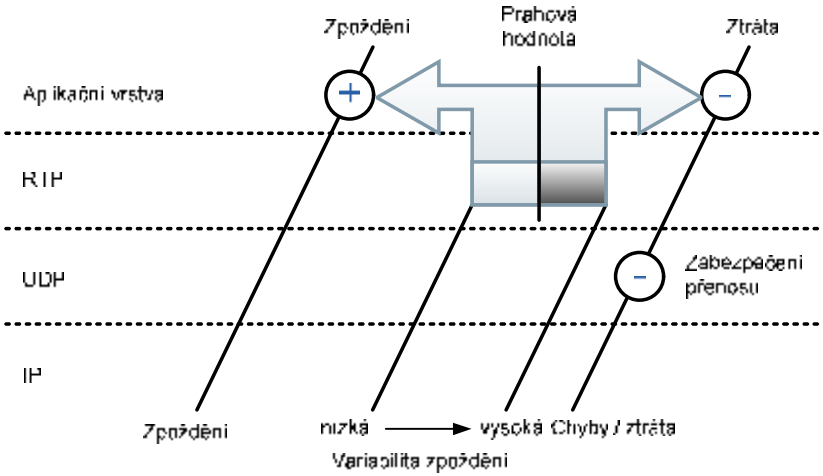
Zpoždění v IP telefonii

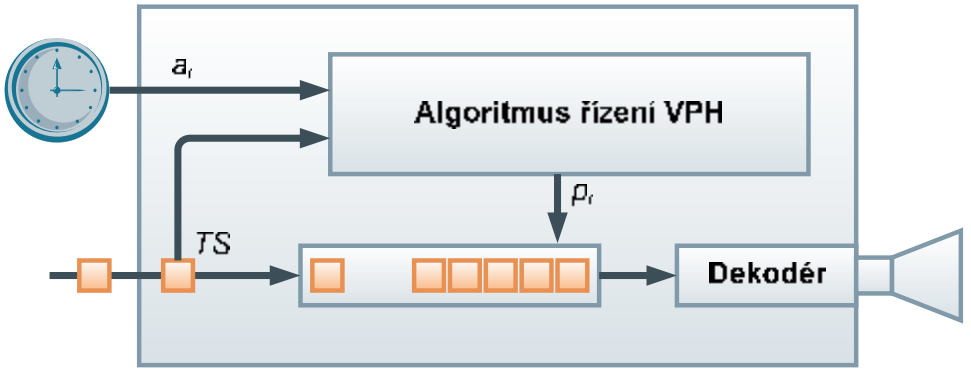
- Zdroje zpoždění ve vysílací části VoIP systému:
  - zpoždění v kodeku T_{CD} (*Coding Delay*)
  - zpoždění při paketizaci T_{PD} (*Packetization Delay*)
  - zpoždění při řazení do výstupní fronty T_{SER} (*Serialization delay*)
- Zdroje zpoždění v telekomunikační síti VoIP systému, platí pro *N* směrovačů na trase:
  - zpoždění při zpracování paketu ve směrovači T_R (*Queueing Delay in Routers*)
  - zpoždění při přenosu přenosovou trasou T_{PROP} (*Propagation Delay Line*)
- Zdroje zpoždění v přijímací části VoIP systému:
  - zpoždění při depaketizaci T_{DPD} (*Depacketization Delay*)
  - zpoždění ve vyrovnávací paměti T_{DJD} (*De-jitter Delay*)
  - zpoždění při dekódování T_{DCD} (*Decoding Delay*)



Variabilní zpoždění







- Kompenzace variabilního zpoždění (*jitteru*)
  - 1a zařazení paketu do vyrovnávací paměti hovoru (*playout buffer*)
  - 1b zahození paketu
  - 2 pozdržení paketu a následné jeho postoupení ke zpracování do dekodéru ve správném časovém okamžiku

© Pavel Bezpalec, 2009

Internet a kvalita služby

- Internet je síť „dobré vůle“
- Pravidla provozu Internetu (z r. 1970)
  - žádnému provozu nebude odmítnut přístup
  - se vším provozem se bude zacházet stejně
  - jediná garance – princip best effort
    - přenos co nejlepším způsobem s rovnou příležitostí
- Kvalita služby (QoS) dle ITU-T E.800
  - „soubor opatření, které zajistí určitý stupeň uspokojení koncového uživatele s danou službou “

© Pavel Bezpalec, 2009

Metody hodnocení kvality

- **Subjektivní měření**
  - statisticky pomocí ohodnocení dostatečně velké skupiny osob, které odpovídají na dotazník
    - uvedený v doporučení ITU-T P.82
  - parametr MOS-LQS *Mean Opinion Score – Listening Quality Subjective*
- **Objektivní měření**
  - na základě matematických modelů, které modelují lidský sluchový aparát
  - parametr MOS-LQO *Mean Opinion Score – Listening Quality Objective*
    - záleží na přesnosti matematického modelu
  - E-model
  - parametr R-faktor

Kvalita řečového vzorku		Hodnocení MOS
výborně	*excellent*	5
dobře	*good*	4
průměrně	*fair*	3
špatně	*poor*	2
nedostatečně	*bad*	1

Faktor R [-]	MOS [-]	Subjektivní spokojenost uživatele
100 – 90	4.5 – 4.34	velmi spokojený
90 – 80	4.34 – 4.03	spokojený
80 – 70	4.03 – 3.60	někteří uživatelé nespokojeni
70 – 60	3.60 – 3.10	mnoho uživatelů nespokojeno
60 – 50	3.10 – 2.58	téměř všichni uživatelé nespokojeni

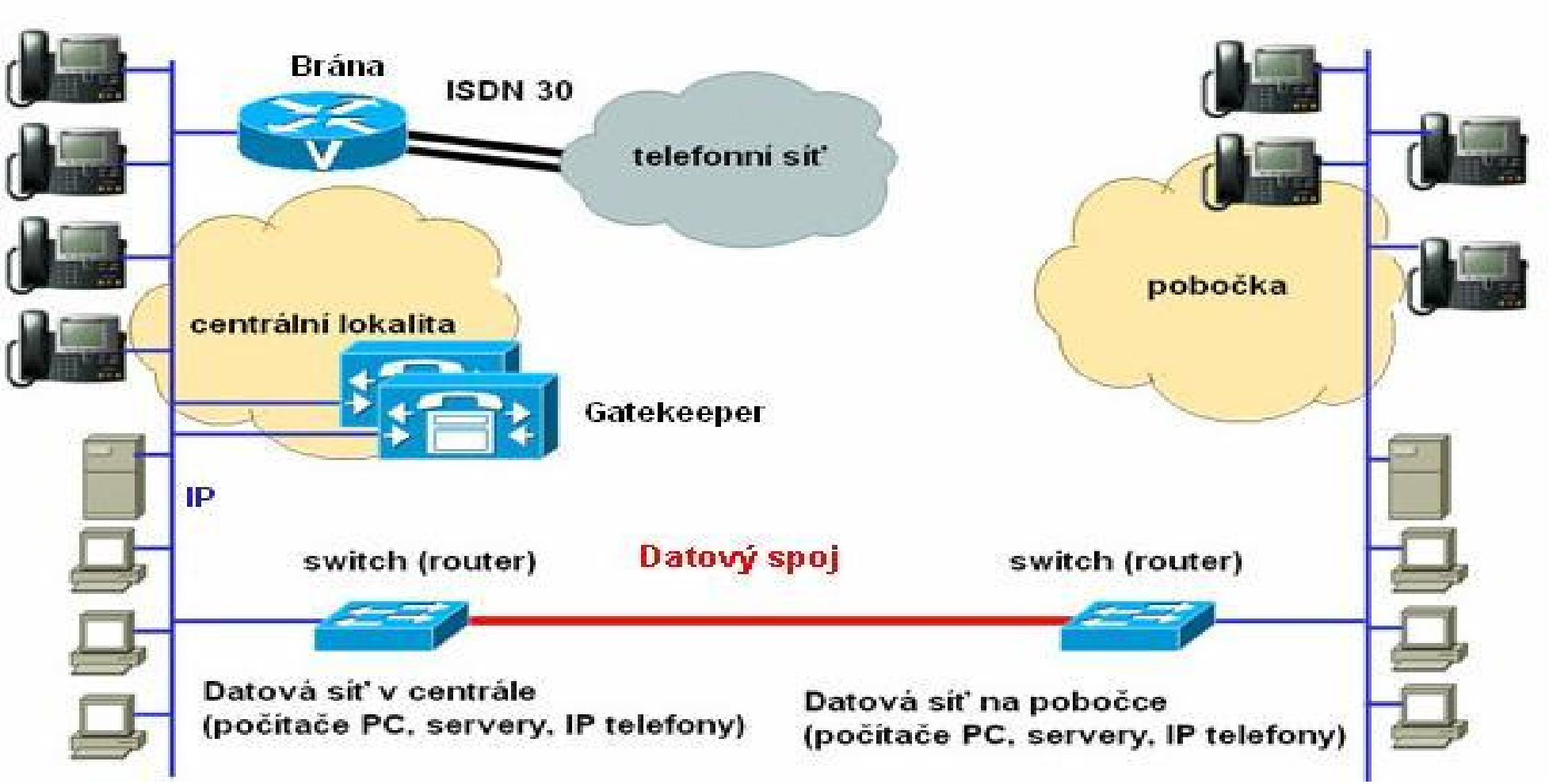
© Pavel Bezpalec, 2009

Obecné metody zajištění QoS

- Předimenzování spoje
  - 1Gbit, 10Gbit, 100Gbit ... ?Ethernet?
- Rezervace pásma
  - ATM
    - třídy služeb VBR, CBR, UBR
  - IntServ
    - rezervace pásma protokolem RSVP
- Použití prioritních schémat
  - ATM
    - třídy služeb CBR, VBR
  - 802.1p
    - prioritní třídy v rozšířeném Ethernetovém rámci
  - MPLS
    - pole *CoS* v záhlaví rámce
      - pole *Priority* v 802.1q
  - DiffServ
    - kód služby DSCP
      - pole *TOS* v záhlaví IPv4
      - pole *DS* v záhlaví IPv6

© Pavel Bezpalec, 2009

Topologie IP telefonního systému



Prvky IP telefonního systému ...

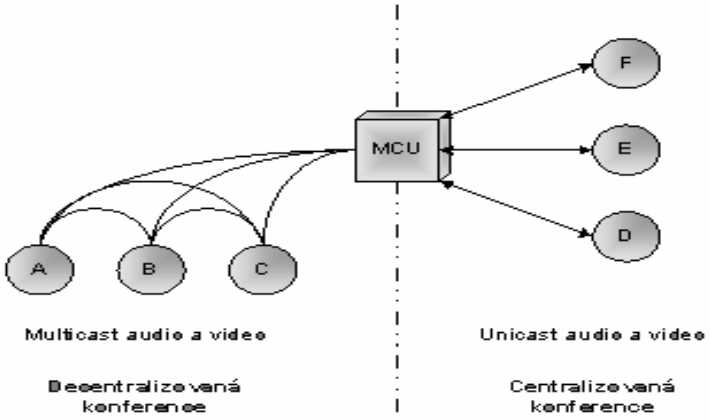
Terminál

nebo také UA (*User Agent*) ...

- Klient, koncová stanice
  - zajišťuje obousměrnou multimediální komunikaci v reálném čase
  - realizován SW na PC nebo specializovaným HW
- Řídící protokoly
  - std: H.323 nebo SIP
  - non std: Skype, firemní
- Audio komunikace
  - kodek G.711, G.723.1, G.729 ...
- Video komunikace
  - kodek H.261 a H.263
- Přenos dat
  - podle T.120

MCU

- Realizace konference mezi třemi a více terminály
- Podpůrné moduly
  - MC (***M**ultipoint **C**ontroller*)
  - MP (***M**ultipoint **P**rocessor*)
- Převod konverzace
  - multicast **ç è** unicast



© Pavel Bezpalec, 2009

Prvky IP telefonního systému

Brána *(gateway)*

- Konverze VoIP sítě se sítí jinou
- Není nutná pro komunikaci v rámci jedné datové sítě
- Konverzní funkce
  - na úrovni **fyzického rozhraní** a **multiplexních struktur**
    - Ethernet ↔ ATM
  - **formátů**
    - G.723 ↔ G.711 (PCM v telefonních sítích)
  - **protokolových sad**
    - H.323, SIP ↔ SS7 (signalizační systém použitý v telefonních sítích)

Správce zóny *(Gatekeeper)*

nebo také proxy, registrar ...

- Hlavní úkol
  - řídící funkce spojení
  - administrátor pro zaregistrované terminály
- Povinné služby GK
  - překlad adres
  - řízení přístupu
  - řízení přenosové kapacity
  - oblastní management
- Nepovinné služby GK
  - řízení signalizace
  - autorizace hovoru
  - správa hovoru

© Pavel Bezpalec, 2009

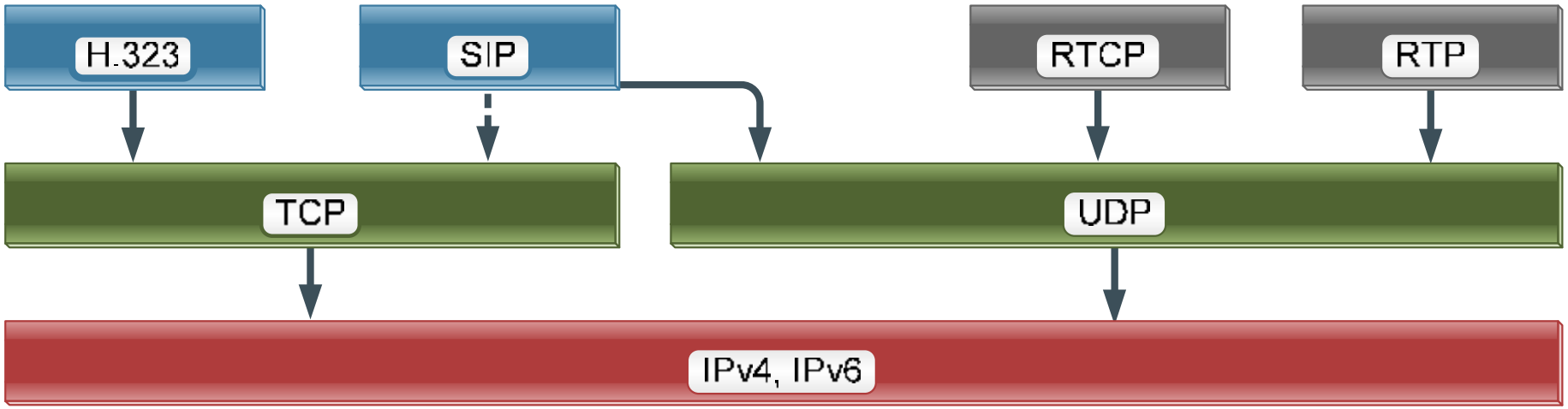
Standardizované protokoly v IP telefonii

- ü Signalizační protokoly
  - vzájemný kontakt a identifikace účastníků
  - dohodnutí způsobu, kvality a typu přenosu uživatelské informace
- ü Komunikační protokoly
  - vlastní přenos uživatelské informace (audio, video, data) mediálními toky
- ü Transportní protokoly
  - přenos signalizačních a komunikačních protokolů

ITU-T H.323, IETF SIP

RTP/RTCP

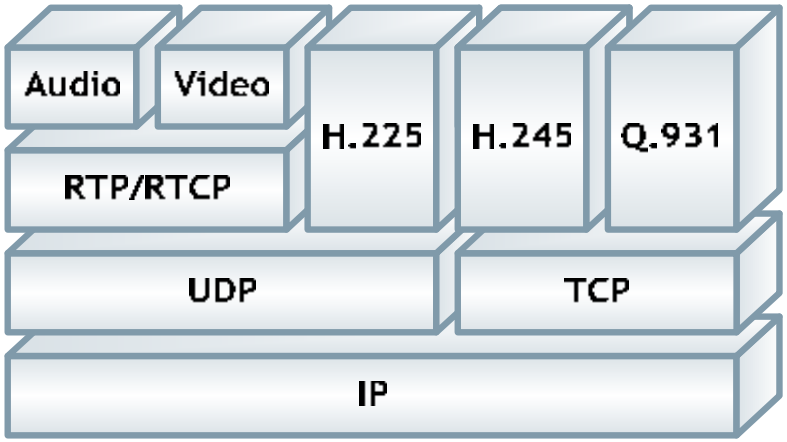
IP, UDP, TCP



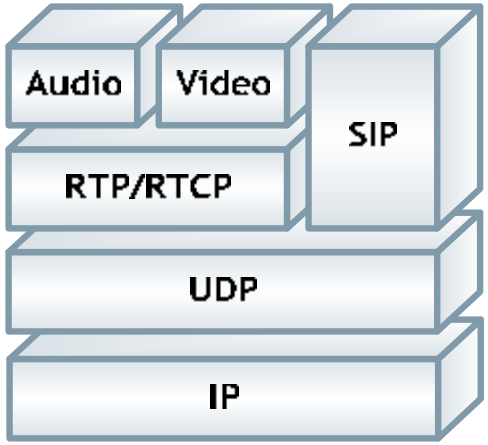
© Pavel Bezpalec, 2009

Signalizační protokoly v IP telefonii

- ITU-T H.323
  - zastřešující standard pro multimediální komunikaci v sítích LAN bez garance kvality služby (QoS), např. síť Internet
    - obsahuje H.225 (Q.931, RAS)
    - H.245 (popis multimediální relace)
    - RTP, RTCP (přenos hovoru)
  - binární protokol s reprezentací založenou na ASN.1

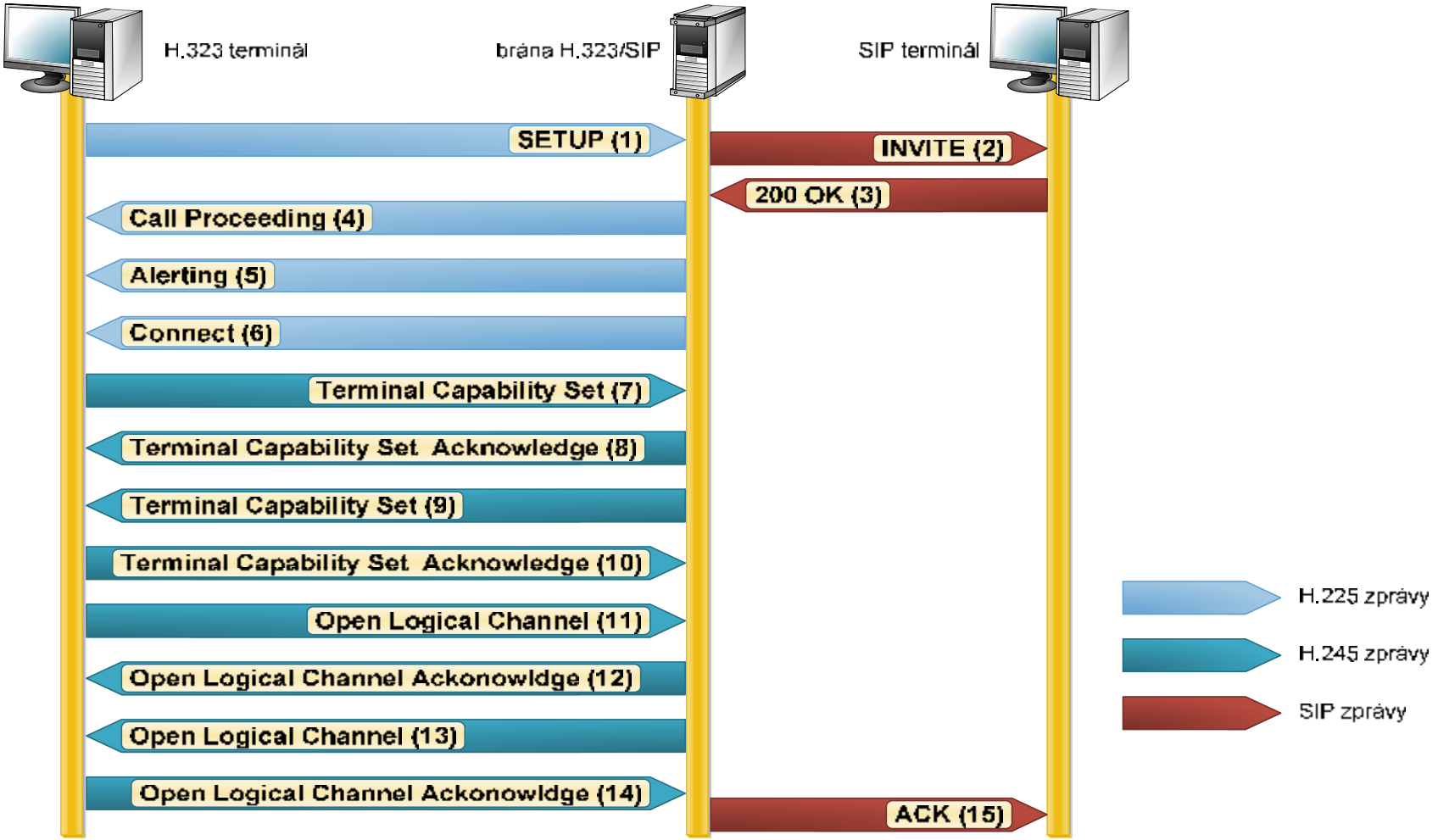


- SIP/SDP (IETF RFC 3261)
  - pouze *signalizační* protokol
  - textově orientovaný
    - jako HTTP
  - nespecifikuje transportní protokoly
    - používá RTP, RTCP, UDP, IP ...
  - subprotokol SDP
    - popis multimediální relace



© Pavel Bezpalec, 2009

Sestavení spojení: H.323 ´ SIP



© Pavel Bezpalec, 2009

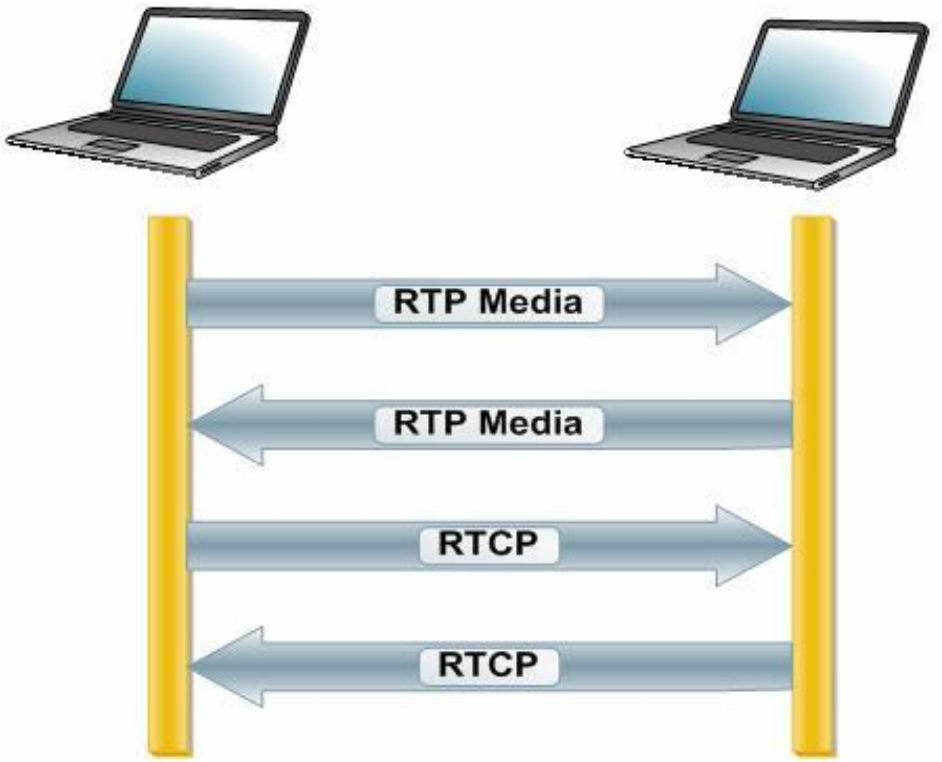
Porovnání H.323 ´ SIP

	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)	Registrar Server, Proxy Server, Redirect Server, Location Server
Transportní ptotokol	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

© Pavel Bezpalec, 2009

Komunikační protokoly RTP/RTCP

- RTP
  - protokolární prostředek k přenosu mediálních toků dat
    - video, audio, data
    - není zaručen přenos v reálném čase
    - zaručuje pouze přehrání dat v daný okamžik
    - používá UDP/IP pro zabezpečení vlastní komunikace
- RTCP
  - protokol pro řízení výkonnosti RTP a diagnostiku
    - informace o kvalitě vysílaných dat
    - identifikuje zdroj RTP
    - synchronizace více mediálních toků
    - provádí řízení intervalu vysílání RTCP
    - přenos minimální informace o řízení relace



© Pavel Bezpalec, 2009

RTP – přenos mediálního toku

- PT, *Payload Type* – Specifikace typu dat
  - použitý kompresní algoritmus
- SN, *Sequence Numbers* – Pořadové číslo
  - označení pořadí vysílaných paketů
- TS, *Time Stamp* – Časová značka
  - vysílač nastavuje č. značku paketu
  - přijímač použije č. značku k rekonstrukci originálního časování pro přehrání dat ve správný okamžik
  - RTP neodpovídá za synchronizaci

© Pavel Bezpalec, 2009

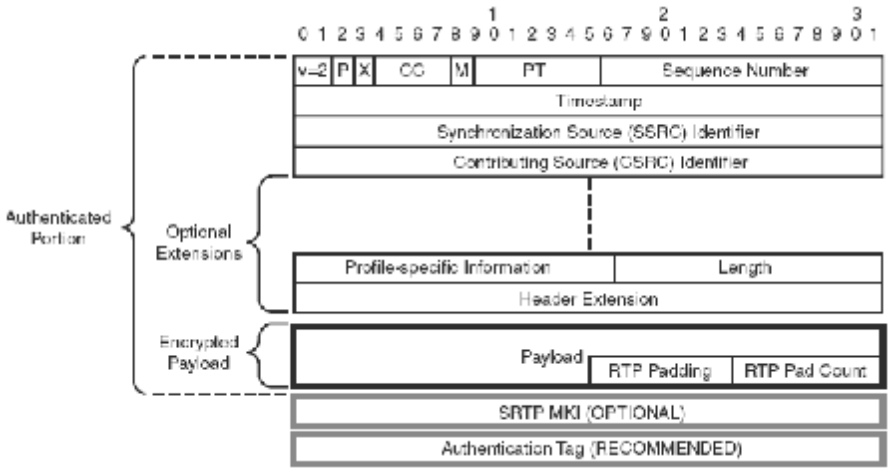
RTCP a rozšíření XR

- typy zpráv RTCP
  - SR – *Sender Report*
    - soubor statistik (o přijímaných i vysílaných datech) od odesílatelů
  - RR – *Receiver Report*
    - soubor statistik od příjemců
  - SDES – *Source DEScription*
    - vlastnosti odesílatelů RTP komunikace (jejich „vizitky“)
  - BYE
    - žádost o ukončení relace
  - APP – *Application*
    - funkce specifické jednotlivé aplikaci
- RFC 3611
- rozšíření RTCP XR
  - mechanismus pro monitorování parametrů QoS
  - lze implementovat do VoIP terminálů
  - firewall friendly
  - definice metrik
    - ztráta paketů
    - zpoždění
    - variabilní zpoždění
    - úroveň signálu, šumu a ozvěny
  - vyhodnocení QoS
    - R-faktor
    - MOS-LQ, MOS-CQ

© Pavel Bezpalec, 2009

Šifrování RTP

- sRTP – *secured RTP*
  - RFC 3711 z roku 2004
  - standard AES
  - klíč je získán z inicializačního vektoru IV
  - master klíč je distribuován přes SDP

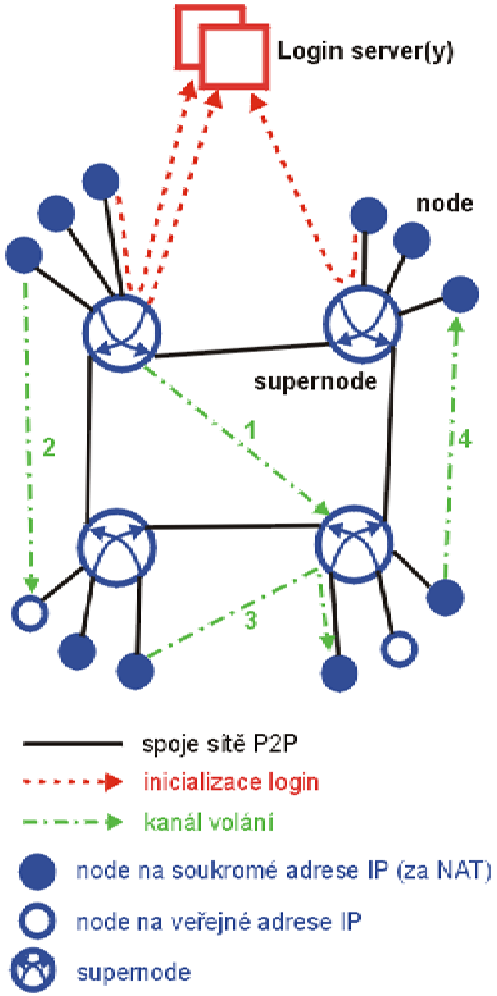


- zRTP – *Zimmermann RTP*
  - Diffie-Hellmanův algoritmus pro výměnu klíčů, dva různé módy:
    - 3072 bit Diffie-Hellman hodnoty
    - 4096 bit Diffie-Hellman hodnoty
  - obsahuje i detekci módu sRTP nebo zRTP

© Pavel Bezpalec, 2009

SKYPE – nestandardizovaný VoIP

- Neveřejná architektura
  - ? protokoly ? šifrování ?
- Peer-to-peer síť umožňuje
  - (video)hovor
  - přenos souborů a zpráv
- Parazituje na PC svých uživatelů
- Skype – entity
  - Login server
  - Supernode
  - Node – Skype client



© Pavel Bezpalec, 2009

Dotazy