# 3. přenáška

**Protokoly přenosu dat**

# Osnova přednášky

1. Protokoly RTP
2. Protokol RTCP
3. Protokoly cRTP, SRTP a ZRTP
4. Protokol SCTP

# 1. Protokol RTP

# Hlas je vzorkován kodekem a pak vkládán do rámců RTP

```
Internet Protocol Version 4, Src: 192.168.16.4 (192.168.16.4), Dst: 192.168.16.16 (192.168.16.16)
User Datagram Protocol, Src Port: clearvisn (2052), Dst Port: btpp2audctr1 (2536)
Real-Time Transport Protocol
⊞ [Stream setup by H245 (frame 22700)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  0... .... = Marker: False
  Payload type: ITU-T G.711 PCMU (0)
  Sequence number: 2
  [Extended sequence number: 65538]
  Timestamp: 320
  Synchronization Source identifier: 0x07fff4aa (134214826)
  Payload: 9d96929192969dabe92e1e18141214181e2c54b4a49d9998...
```

kodek

hlas

# Protokol RTP

RTP (Real-time Transport Protokol) je aplikační protokol, který byl navržen pro přenos audio/video dat přes Internet. Postaven je na protokolu UDP a jsou mu přidány některé vlastnosti pro zajištění lepšího přenosu mediálních dat. Zajišťuje seřazení jednotlivých paketů (sequence number), jejich časové značkování (timestamp – vzorkovací značka prvního oktetu v paketu) a multiplexování a demultiplexování. Záhlaví je velké obvykle 12 byte.

RTP nezajišťuje rezervaci kanálu a negarantuje QoS (Quality of Service).

Verze: 1996 – RFC 1889 a 1890 (verze 2),
2003 – RFC 3550 a 3551 (vylepšují především dohled nad RTP),
2004 – RFC 3711 (SRTP).

Doporučený zdroj:
Wiki Wireshark http://wiki.wireshark.org/SampleCaptures#SIP_and_RTP

# K čemu RTP slouží

Poskytuje mechanizmy pro koncové multimediální přenosy v reálném čase. Protokol podporuje přenos dat mezi dvěma i více účastníky.

- **Identifikace rámce** – Identifikuje začátek a konec rámce
- **Rekonstrukce správného pořadí paketů** na základě sekvenčních čísel
- **Synchronizace**: Určuje správný okamžik přehrávání dat na základě časových razítek, a to
  - Intermedia – Synchronizace více médií (audio-video-text)
  - Identifikace toku – Identifikuje typ médií a jeho kódování

# RTP v RFC 3550

Network Working Group
Request for Comments: 3550
Obsoletes: 1889
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
R. Frederick
Blue Coat Systems Inc.
V. Jacobson
Packet Design
July 2003

RTP: A Transport Protocol for Real-Time Applications

**Status of this Memo**

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

**Abstract**

This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

# RTP v RFC 3551

Network Working Group
Request for Comments: 3551
Obsoletes: 1890
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
July 2003

RTP Profile for Audio and Video Conferences
with Minimal Control

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

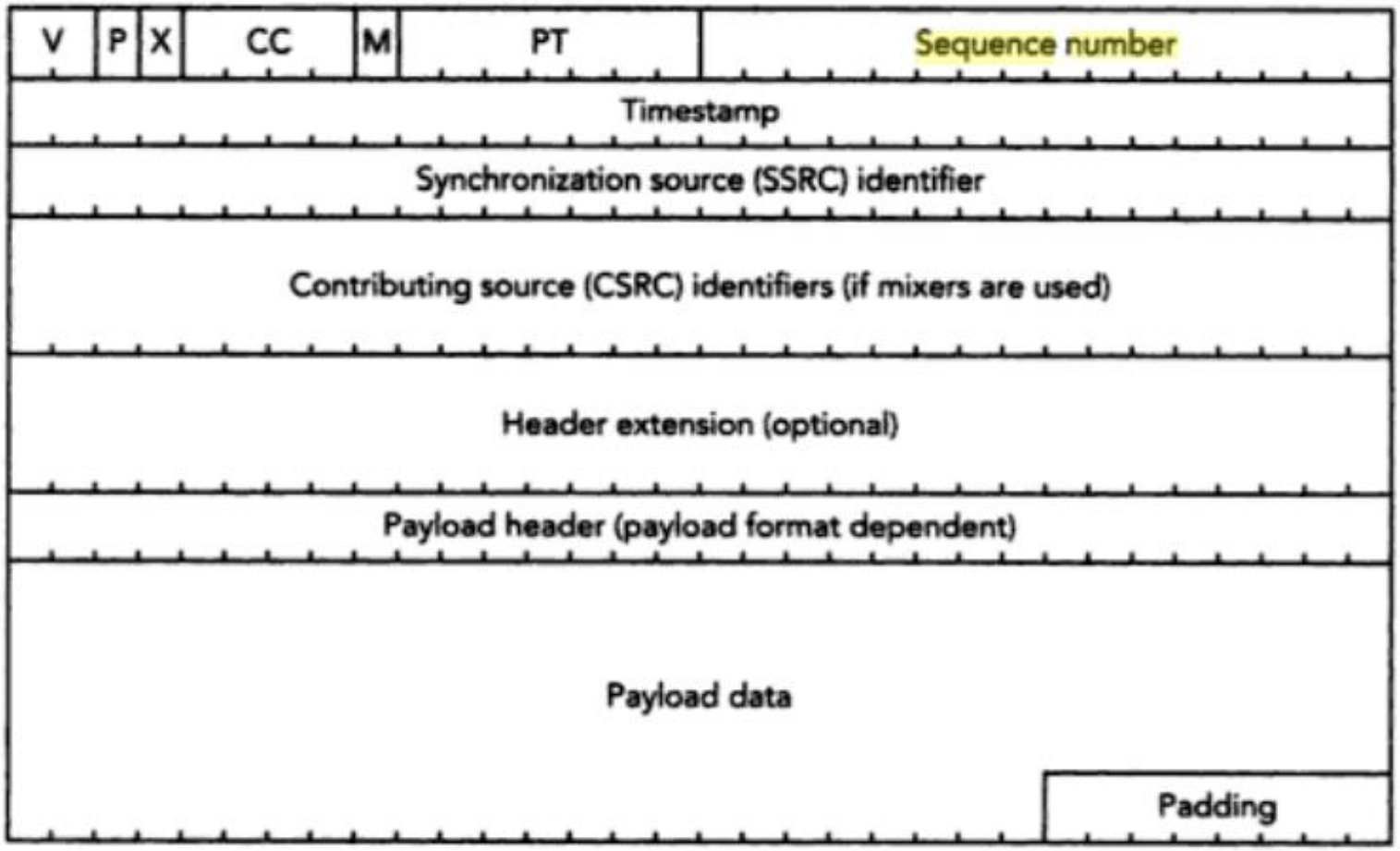
Abstract

This document describes a profile called "RTP/AVP" for the use of the real-time transport protocol (RTP), version 2, and the associated control protocol, RTCP, within audio and video multiparticipant conferences with minimal control. It provides interpretations of generic fields within the RTP specification suitable for audio and video conferences. In particular, this document defines a set of default mappings from payload type numbers to encodings.

This document also describes how audio and video data may be carried within RTP. It defines a set of standard encodings and their names when used within RTP. The descriptions provide pointers to reference implementations and the detailed standards. This document is meant as an aid for implementors of audio, video and other real-time multimedia applications.

This memorandum obsoletes RFC 1890. It is mostly backwards-compatible except for functions removed because two interoperable

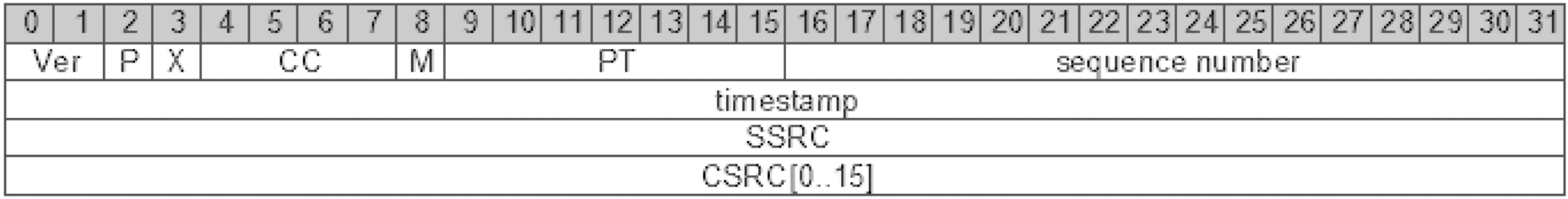
# Hrubá struktura RTP paketu



# Záhlaví rozšířené pro DTMF

```
User Datagram Protocol, Src Port: alchemy (3234), Dst Port: alchemy (3234)
Real-Time Transport Protocol
⊞ [Stream setup by SDP (frame 8)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  0... .... = Marker: False
  Payload type: DynamicRTP-Type-100 (100)
  Sequence number: 0
  [Extended sequence number: 65536]
  Timestamp: 5081566
  Synchronization Source identifier: 0xe2a51901 (3802470657)
RFC 2833 RTP Event
  Event ID: DTMF Zero 0 (0)
  0... .... = End of Event: False
  .1.. .... = Reserved: True
  ..10 0001 = Volume: 33
  Event Duration: 768
```

# Formát záhlaví

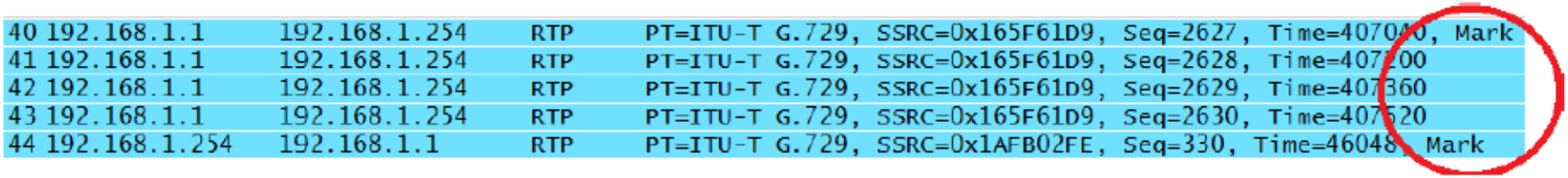




- ***Ver*** označuje verzi protokolu (dnes se používá verze 2),
- ***P*** (padding field) v případě P=1 označuje vycpávku v posledním paketu toku na dorovnání jednotné délky. Poslední oktet obsahuje informaci o tom, kolik oktetů bylo celkem přidáno,
- ***X*** (extension bit) v případě X=1 označuje, že za záhlavím následuje rozšíření paketu s CSRC
- **CC** (Contributing Source Identifier Counter) – počet zdrojů
  význam ***M*** (marker bit) počatek spřadani hovoru (talkspurt) → uprava zpožděni je dána aplikačním profilem (např. konec paketu v toku rámců).

RTP na rozdíl od UDP zavádí následující služby:

- ***PT*** – *payload type*, metoda kódování, může se během přenosu měnit;
- doručení ve správném pořadí, kontrola ztráty paketu (***sequence number***);
- zavedení časového razítka (***timestamp***);
- rozlišení synchronizačního zdroje – při přenosu více kanálů audio/video (**SSRC** – indikace synchronizačního zdroje, **CSRC** – identifikace příspěvkového (contribution) zdroje,

# Marker po klidovém úseku (volitelný)



| | | | | |
|---|---|---|---|---|
| 40 | 192.168.1.1 | 192.168.1.254 | RTP | PT=ITU-T G.729, SSRC=0x165F61D9, Seq=2627, Time=407040, Mark |
| 41 | 192.168.1.1 | 192.168.1.254 | RTP | PT=ITU-T G.729, SSRC=0x165F61D9, Seq=2628, Time=407200 |
| 42 | 192.168.1.1 | 192.168.1.254 | RTP | PT=ITU-T G.729, SSRC=0x165F61D9, Seq=2629, Time=407360 |
| 43 | 192.168.1.1 | 192.168.1.254 | RTP | PT=ITU-T G.729, SSRC=0x165F61D9, Seq=2630, Time=407520 |
| 44 | 192.168.1.254 | 192.168.1.1 | RTP | PT=ITU-T G.729, SSRC=0x1AFB02FE, Seq=330, Time=46048, Mark |

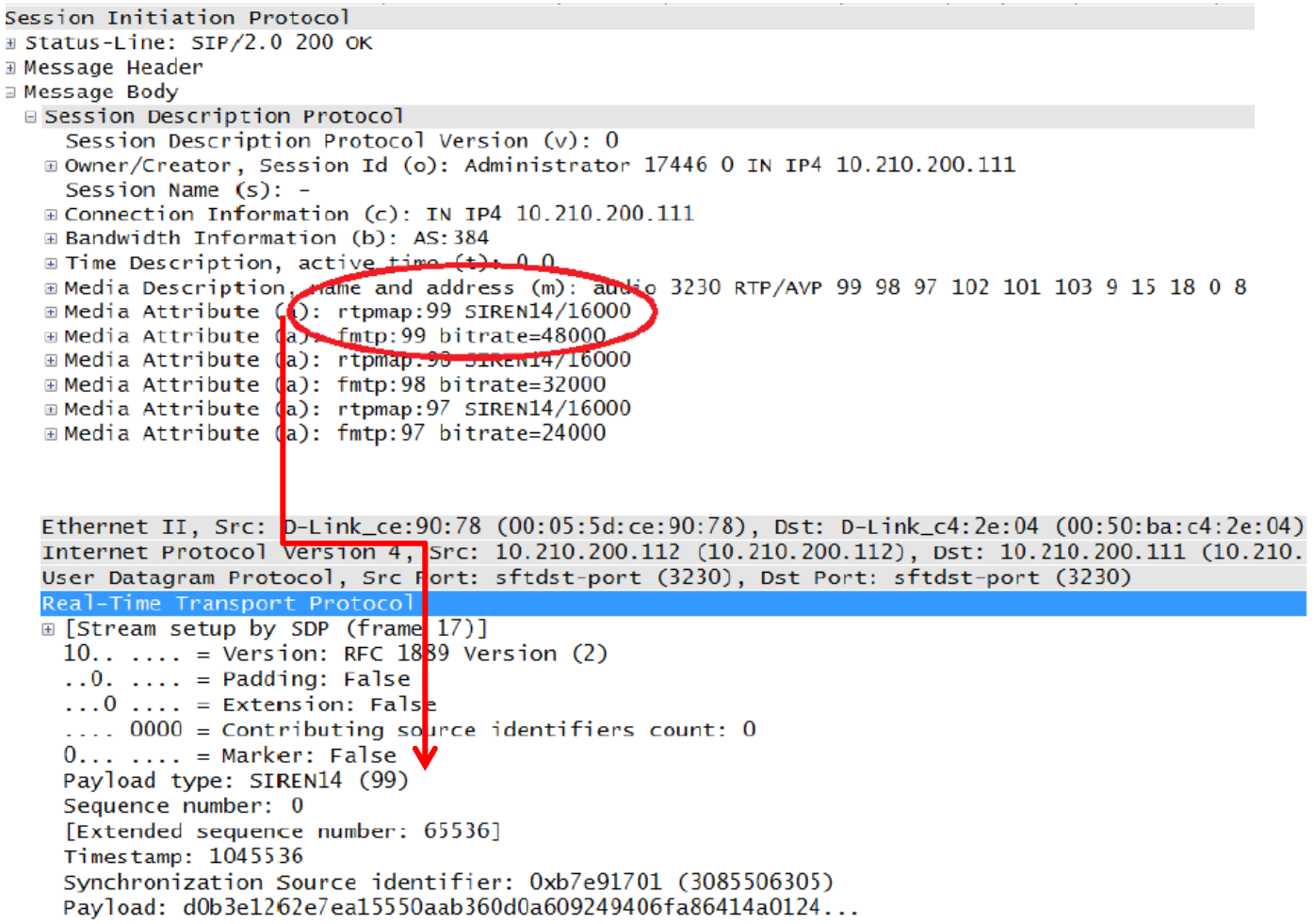
# Typy zátěže (PT) audio

| PT | encoding name | media type | clock rate (Hz) | channels |
|---|---|---|---|---|
| 0 | PCMU | A | 8,000 | 1 |
| 1 | reserved | A | | |
| 2 | reserved | A | | |
| 3 | GSM | A | 8,000 | 1 |
| 4 | G723 | A | 8,000 | 1 |
| 5 | DVI4 | A | 8,000 | 1 |
| 6 | DVI4 | A | 16,000 | 1 |
| 7 | LPC | A | 8,000 | 1 |
| 8 | PCMA | A | 8,000 | 1 |
| 9 | G722 | A | 8,000 | 1 |
| 10 | L16 | A | 44,100 | 2 |
| 11 | L16 | A | 44,100 | 1 |
| 12 | QCELP | A | 8,000 | 1 |
| 13 | CN | A | 8,000 | 1 |
| 14 | MPA | A | 90,000 | (see text) |
| 15 | G728 | A | 8,000 | 1 |
| 16 | DVI4 | A | 11,025 | 1 |
| 17 | DVI4 | A | 22,050 | 1 |
| 18 | G729 | A | 8,000 | 1 |
| dyn | G726-40 | A | 8,000 | 1 |
| dyn | G726-32 | A | 8,000 | 1 |
| dyn | G726-24 | A | 8,000 | 1 |
| dyn | G726-16 | A | 8,000 | 1 |
| dyn | G729D | A | 8,000 | 1 |
| dyn | G729E | A | 8,000 | 1 |

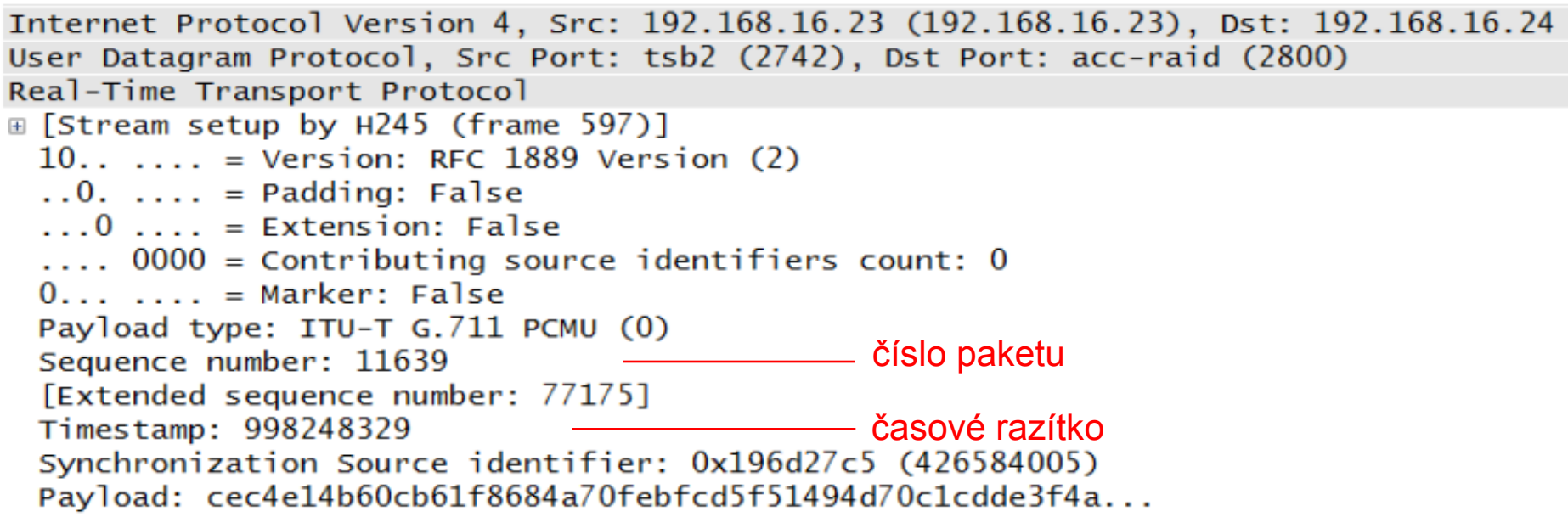
# Typy zátěže (PT) video

| PT | encoding name | media type | clock rate (Hz) |
|---|---|---|---|
| 24 | unassigned | V | |
| 25 | CelB | V | 90,000 |
| 26 | JPEG | V | 90,000 |
| 27 | unassigned | V | |
| 28 | nv | V | 90,000 |
| 29 | unassigned | V | |
| 30 | unassigned | V | |
| 31 | H261 | V | 90,000 |
| 32 | MPV | V | 90,000 |
| 33 | MP2T | AV | 90,000 |
| 34 | H263 | V | 90,000 |
| 35-71 | unassigned | ? | |
| 72-76 | reserved | N/A | N/A |
| 77-95 | unassigned | ? | |
| 96-127 | dynamic | ? | |
| dyn | H263-1998 | V | 90,000 |

# Dynamické porty je třeba předem dohodnout



# Číslo paketu a časové razítko



# Číslování paketů

První číslo je náhodně zvolené

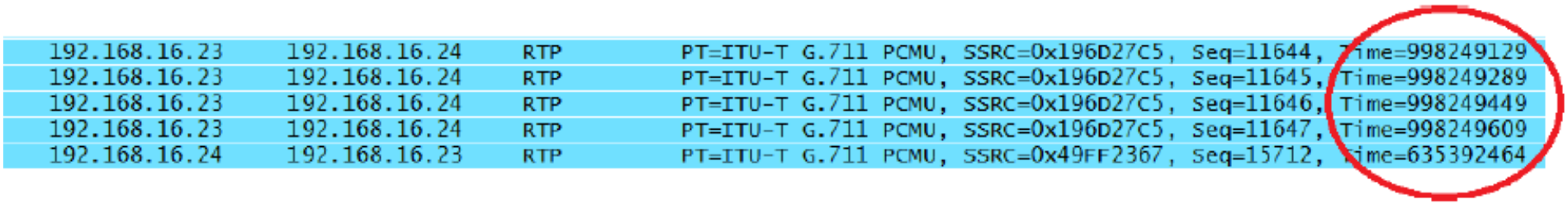
| | | | |
|---|---|---|---|
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11644, Time=998249129 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11645, Time=998249289 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11646, Time=998249449 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11647, Time=998249609 |
| 192.168.16.24 | 192.168.16.23 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x49FF2367, Seq=15712, Time=635392464 |

| | | | |
|---|---|---|---|
| 10.210.200.112 | 10.210.200.111 | RTP | PT=SIREN14, SSRC=0xB7E91701, Seq=0, Time=1045536 |
| 10.210.200.112 | 10.210.200.111 | RTP | PT=SIREN14, SSRC=0xB7E91701, Seq=1, Time=1045696 |
| 10.210.200.112 | 10.210.200.111 | RTP | PT=SIREN14, SSRC=0xB7E91701, Seq=2, Time=1045856 |
| 10.210.200.112 | 10.210.200.111 | RTP | PT=SIREN14, SSRC=0xB7E91701, Seq=3, Time=1046016 |

Polycom

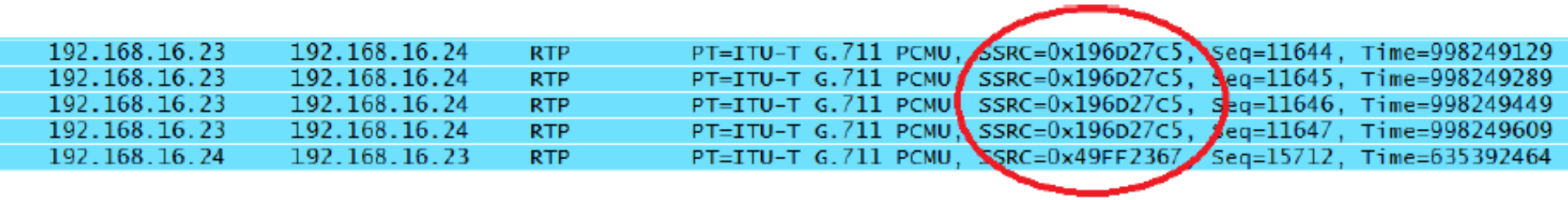
# Časové razítko

20 ms rámec G.711 obsahuje 160 vzorků

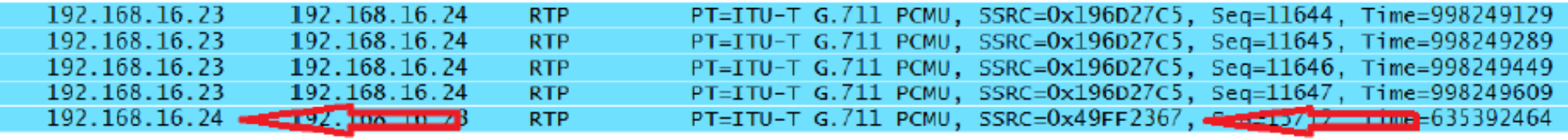


| | | | |
|---|---|---|---|
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11644, Time=998249129 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11645, Time=998249289 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11646, Time=998249449 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11647, Time=998249609 |
| 192.168.16.24 | 192.168.16.23 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x49FF2367, Seq=15712, Time=635392464 |

# Synchronizace pro playback

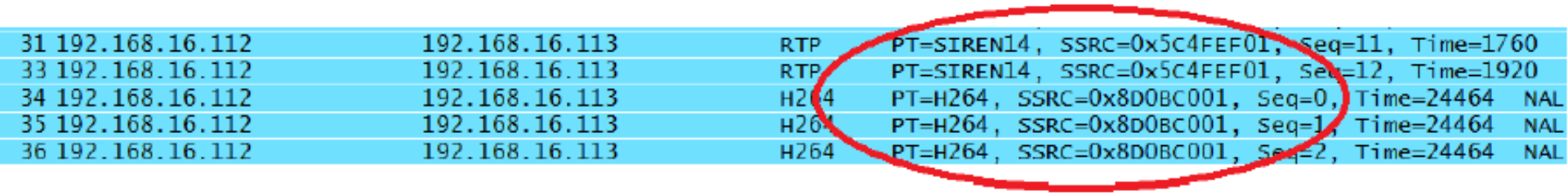


# Jak se mění zdroj, mění se i adresa synchronizačního zdroje

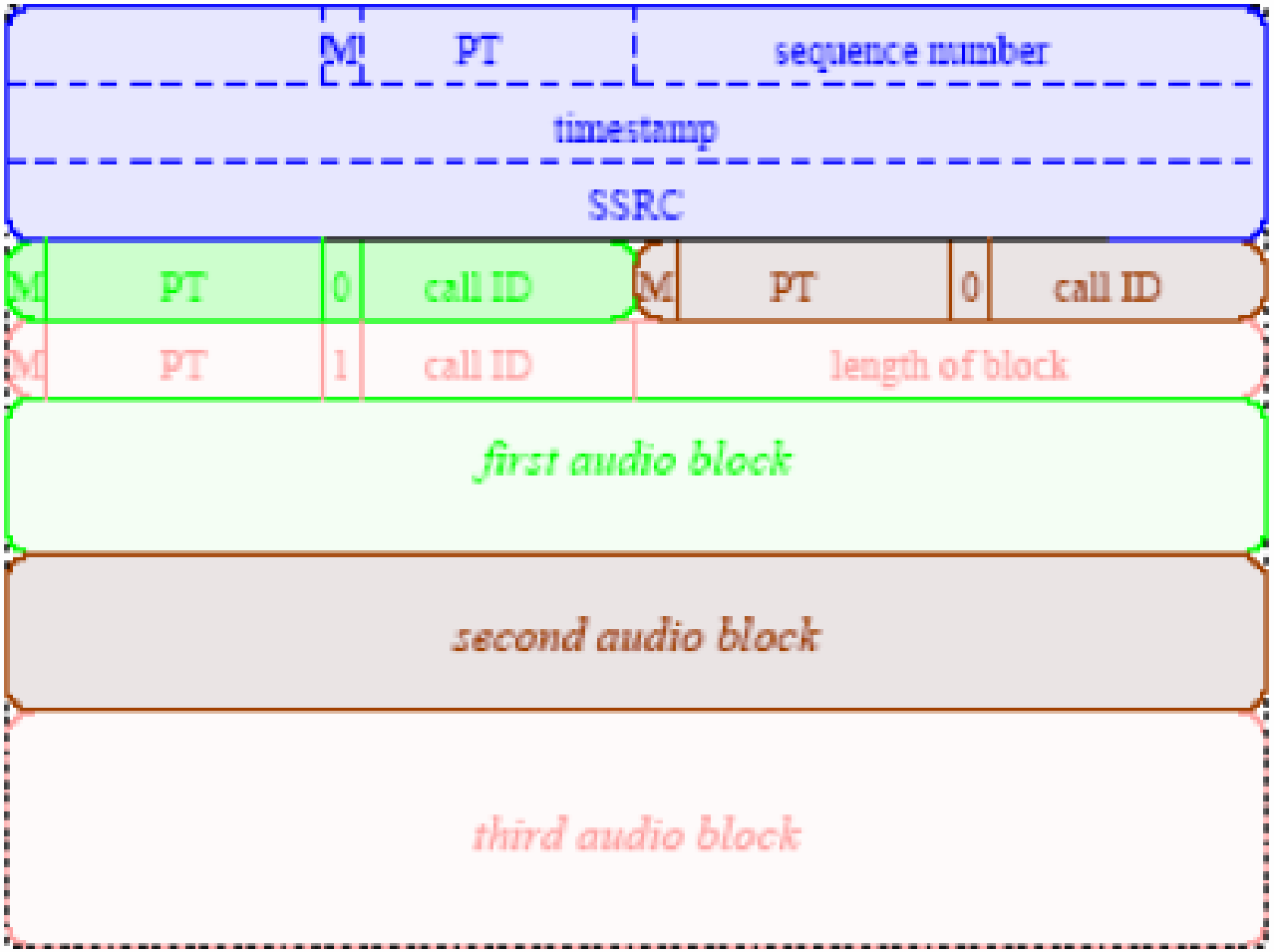


| | | | |
|---|---|---|---|
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11644, Time=998249129 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11645, Time=998249289 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11646, Time=998249449 |
| 192.168.16.23 | 192.168.16.24 | RTP | PT=ITU-T G.711 PCMU, SSRC=0x196D27C5, Seq=11647, Time=998249609 |
| 192.168.16.24 | [illegible] | RTP | PT=ITU-T G.711 PCMU, SSRC=0x49FF2367, [illegible] Time=635392464 |

# Skyping s web kamerou a mikrofonem (stejný zdroj)

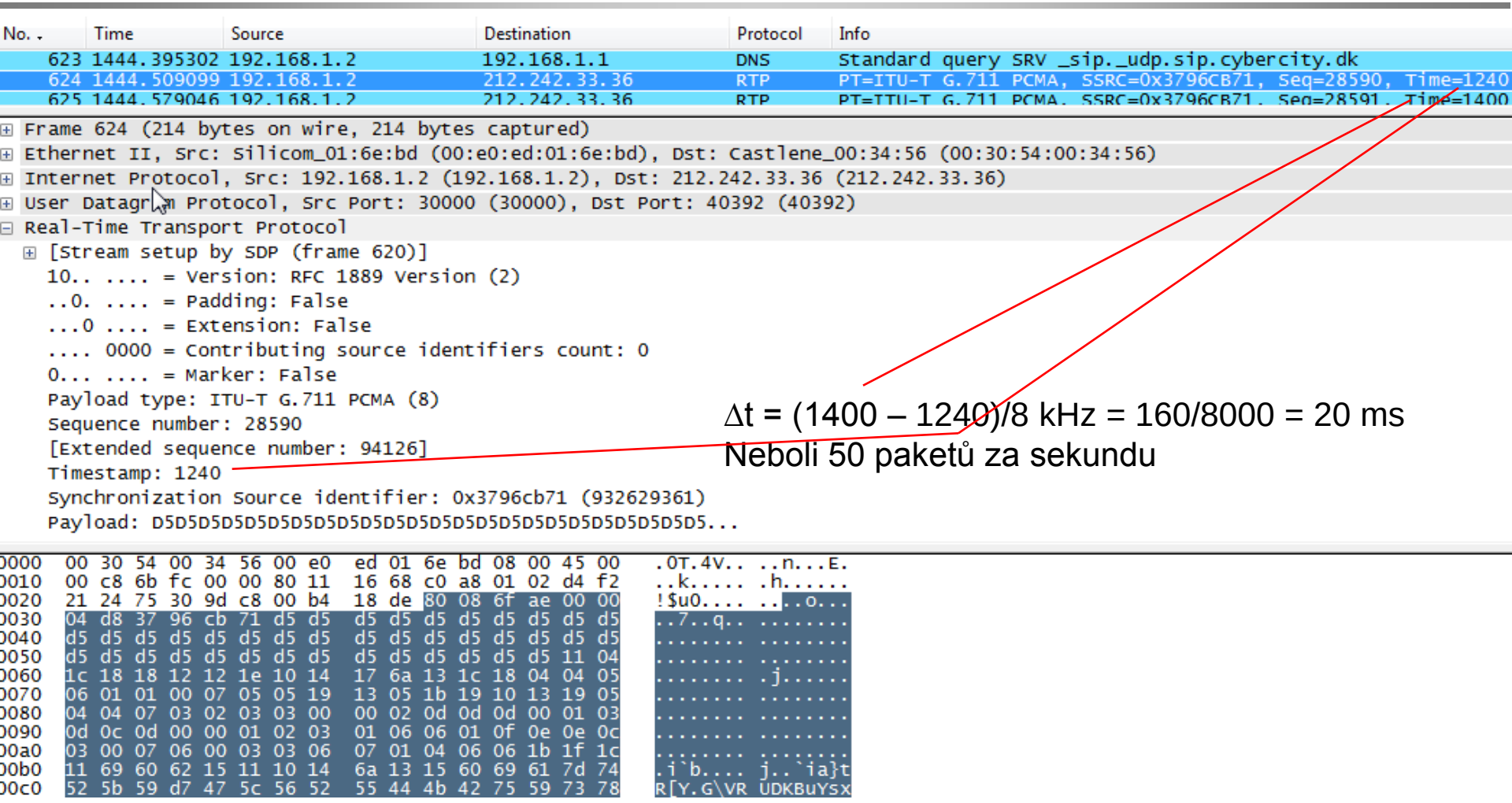


# Agregace dat




Pro 24 kanálů je využití pásma 89 %

# Jaké je časování odesílání paketů ze zdroje?




Δt = (1400 – 1240)/8 kHz = 160/8000 = 20 ms
Neboli 50 paketů za sekundu

# Přenosu DTMF a jiných tónů řeší RFC 2833

Network Working Group
Request for Comments: 2833
Category: Standards Track

H. Schulzrinne
Columbia University
S. Petrack
MetaTel
May 2000

RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This memo describes how to carry dual-tone multifrequency (DTMF) signaling, other tone signals and telephony events in RTP packets.

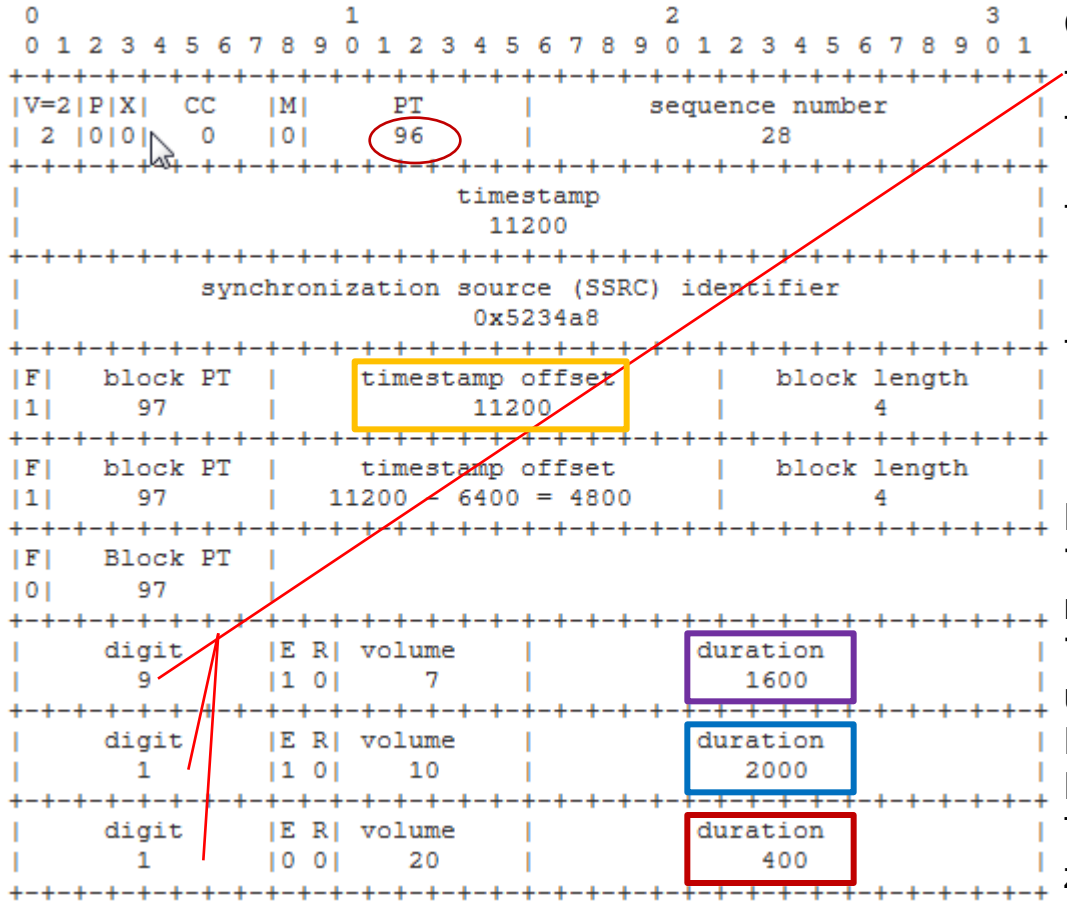
1 Introduction

This memo defines two payload formats, one for carrying dual-tone multifrequency (DTMF) digits, other line and trunk signals (Section 3), and a second one for general multi-frequency tones in RTP [1] packets (Section 4). Separate RTP payload formats are desirable since low-rate voice codecs cannot be guaranteed to reproduce these tone signals accurately enough for automatic recognition. Defining separate payload formats also permits higher redundancy while maintaining a low bit rate.

The payload formats described here may be useful in at least three applications: DTMF handling for gateways and end systems, as well as "RTP trunks". In the first application, the Internet telephony gateway detects DTMF on the incoming circuits and sends the RTP payload described here instead of regular audio packets. The gateway likely has the necessary digital signal processors and algorithms, as it often needs to detect DTMF, e.g., for two-stage dialing. Having the gateway detect tones relieves the receiving Internet end system

# Co zde z přenášených údajů o přenosu tónu DTMF podle RFC 2833 vyčteme?

Identifikace volajícího (DTMF):
- out-of-band (mimo hovorové pásmo): čísla, kmitočet…
- in-band: PCM, tóny v pásmu 300-3400 Hz digitalizované dle G.711.




Co se dovídáme:
- bylo voleno číslo 911
- **první číslice** „9“ je tón o délce trvání 200 ms (**1 600**/8 kHz) a začíná v čase 0 ms
- **druhé číslice** „1“ je tón o délce trvání 250 ms (**2 000**/8 kHz) a začíná v čase 800 ms (6 400/8 kHz) časových jednotek, timetamps)
- **třetí číslice** „1“ je tón o délce trvání 50 ms (**400**/8 kHz) a bylo stisknuto v čase1,4 s (11 200/8 kHz) časových jednotek, timetamps)

První generace Cisco IP telefonů (7902, 7905, 7910, 7912, 7940, 7960) RFC 2833 nepodporovala, druhá (7906, 7911, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975) a další už ano. U Cisco Unified Call Manager a je RFC 2833 podporováno od verze 5.0. Je dobré DTMF na branách řešit in-band pomocí Named Telephone Events, které RFC 2811 znají, např. out-of-band SIP signalizace ne.

# Obsah paketu (zátěž) v příkladu

| | | | | | |
|---|---|---|---|---|---|
| 96 - 127 | dynamic | | | | RFC 3551 |

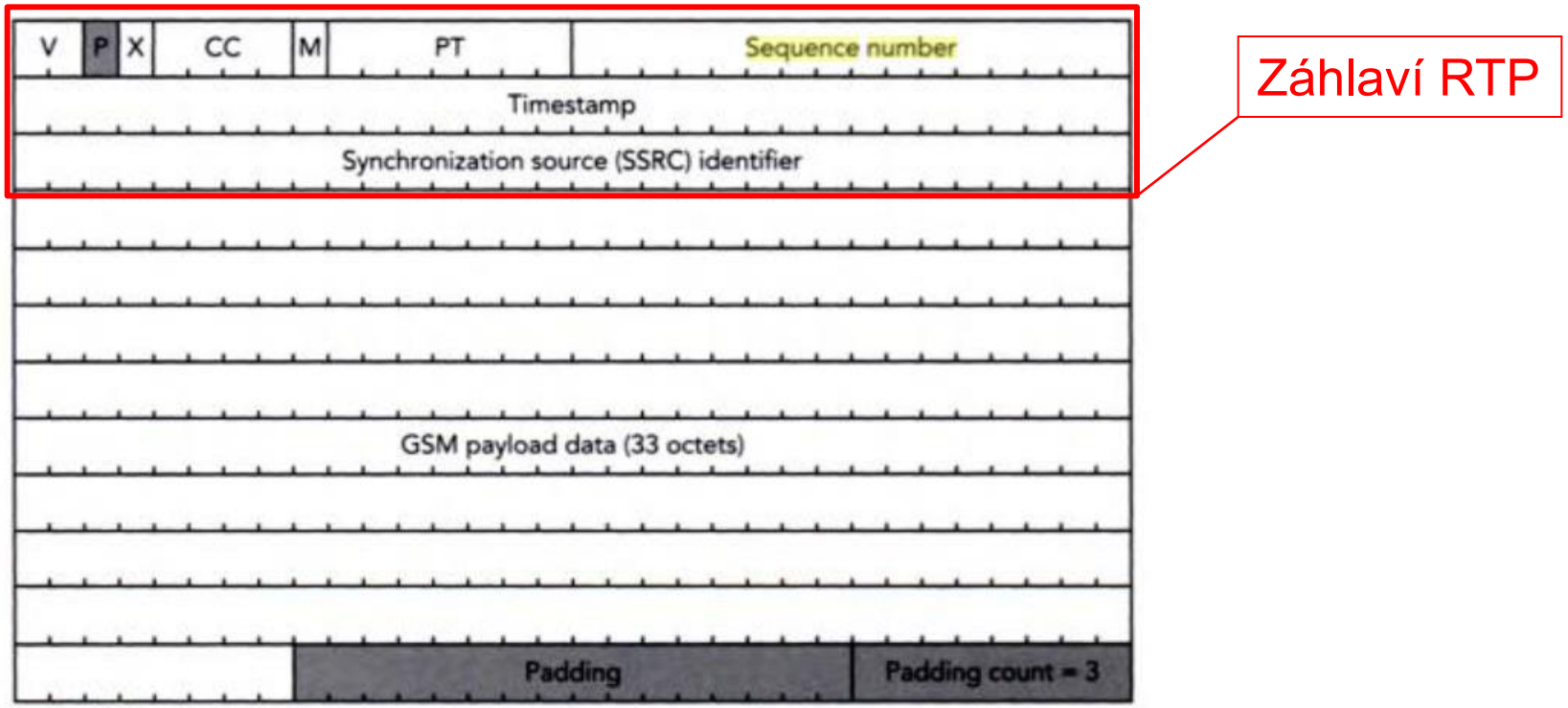
Network Working Group
Request for Comments: 3551
Obsoletes: 1890
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
July 2003

RTP Profile for Audio and Video Conferences
with Minimal Control

Status of this Memo

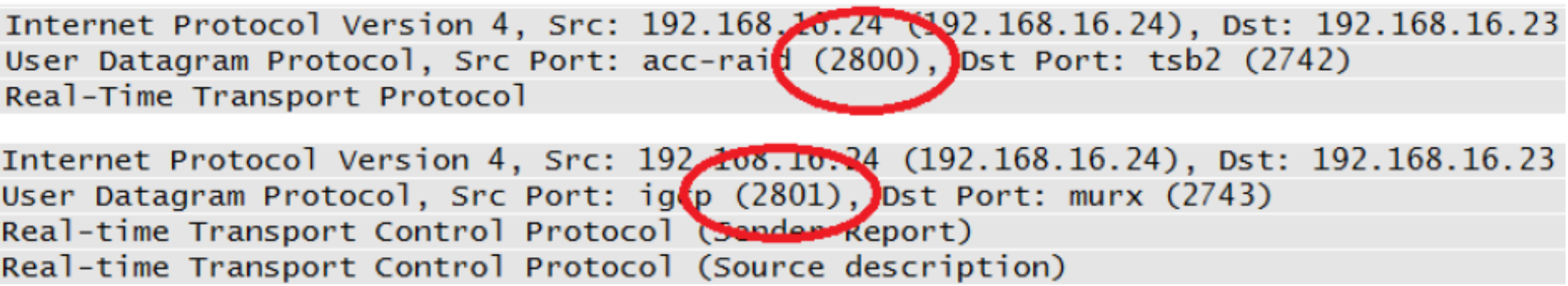
# Příklad – RTP pro GSM



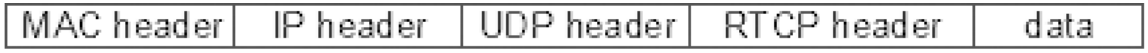

**K čemu může být užitečné doplnění na násobky 8?**

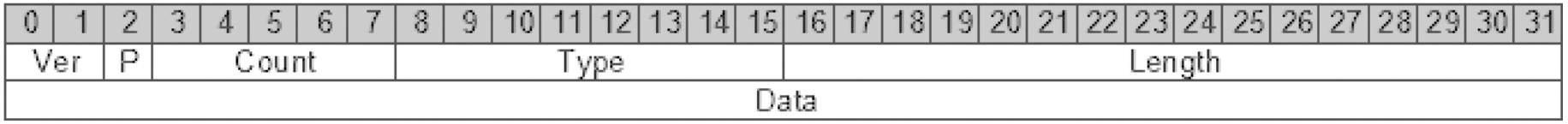
# 2. Protokol RTCP

# RCTP a RTP mají sousedící čísla portů a jsou přenášeny s frekvencí 5 paketů/s



# Protokol RTCP




RTP podporuje sloučení několika mediálních toků do jedné relace (session) za účelem podpory aplikací ,jako je pořádání konferenčních hovorů. Chybí mu však zpětná kontrola o tom, zda a v jakém stavu dorazily pakety k příjemci.

Z tohoto důvodu je pro protokol RTP implementován doplňkový protokol Real-time Transport Control Protocol (RTCP) zajišťuje odezvu od příjemce k odesílateli. Odesílatel tak může získávat informace o tom, v jaké kvalitě je signál přijímán, kolik paketů se cestou ztratilo nebo jaký byl rozkmit zpoždění (jitter) doručených paketů. Lze tedy s jeho pomocí sledovat úroveň kvality služby.

Periodické posílání mezi účastníky komunikace (na jiném portu než RTP – o jedna větší). Šířka pásma pro RTCP nesmí přesáhnout 5 % šířky pásma pro RTP spojení.

# Typy paketů RTCP

- SR – sender report: počet poslaných slabik → odhad rychlosti, časové značky → synchronizace
- RR – receiver report: Počet poslaných a očekávaných paketů → ztráty, jiter během přijmu, zpožděni oběhu
- BYE – explicitní ukončení – navíc (kromě timeoutu)
- SDES – source description: CNAME (canonical end-point identifier) – reálné jméno použité pro popis zdroje, EMAIL, PHONE, LOC (geografické umístění), TOOL (aplikace nebo jméno prostředku), NOTE – poznámka nebo stav – popisuje aktuální stav zdroje.
- APP – rozšíření – závislé na aplikaci

# Zpráva od zdroje – Send Report
## (soubor statistik o přijímaných a vysílaných datech)


identifikace zdroje dat

čas odeslání

odpovídající čas příjmu →synchronizace

čítač paketů odesílatele: celkový počet odeslaných paketů

čítač oktetů odesílatele: celkový počet odeslaných oktetů

vyhlazené „chvění“ mezi pakety

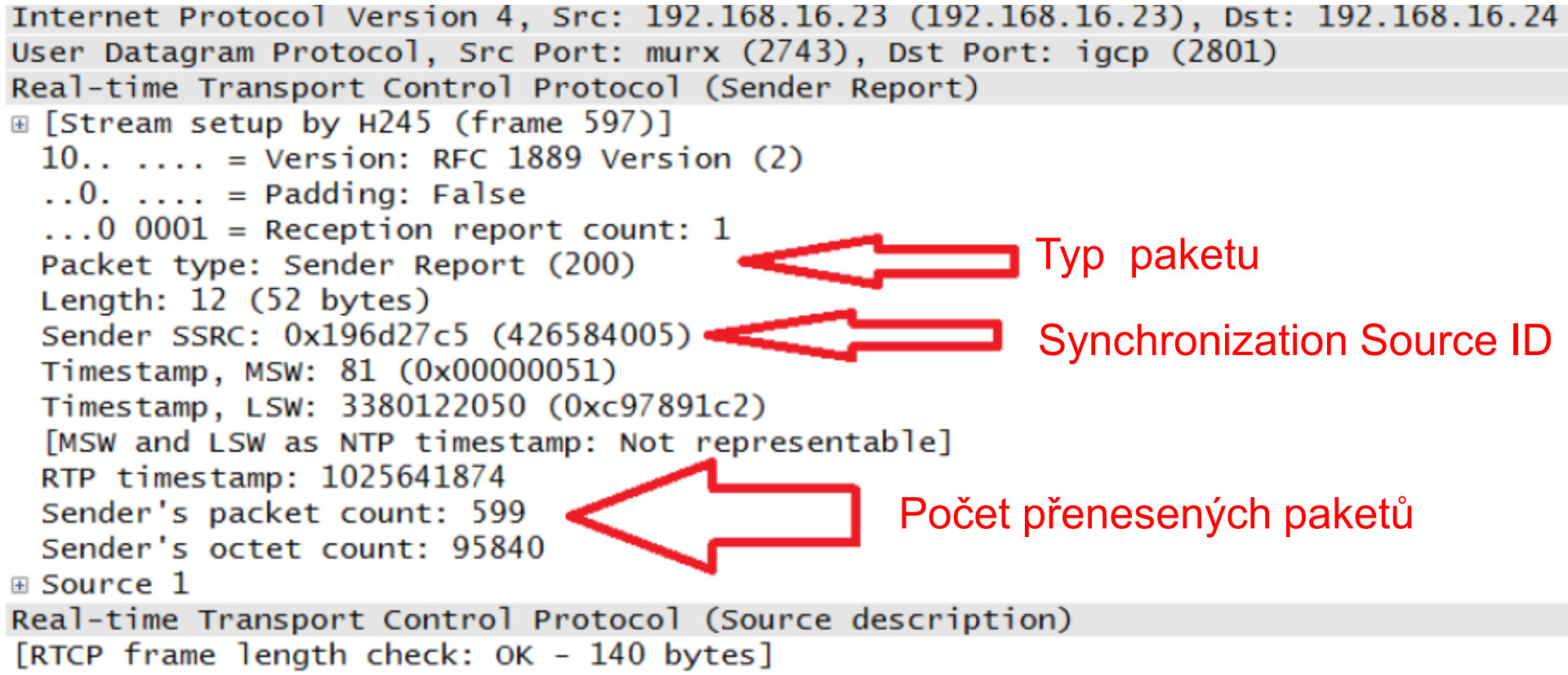
LSR – čas posledního přijmu SR

DLSR – zpoždění od posledního SR

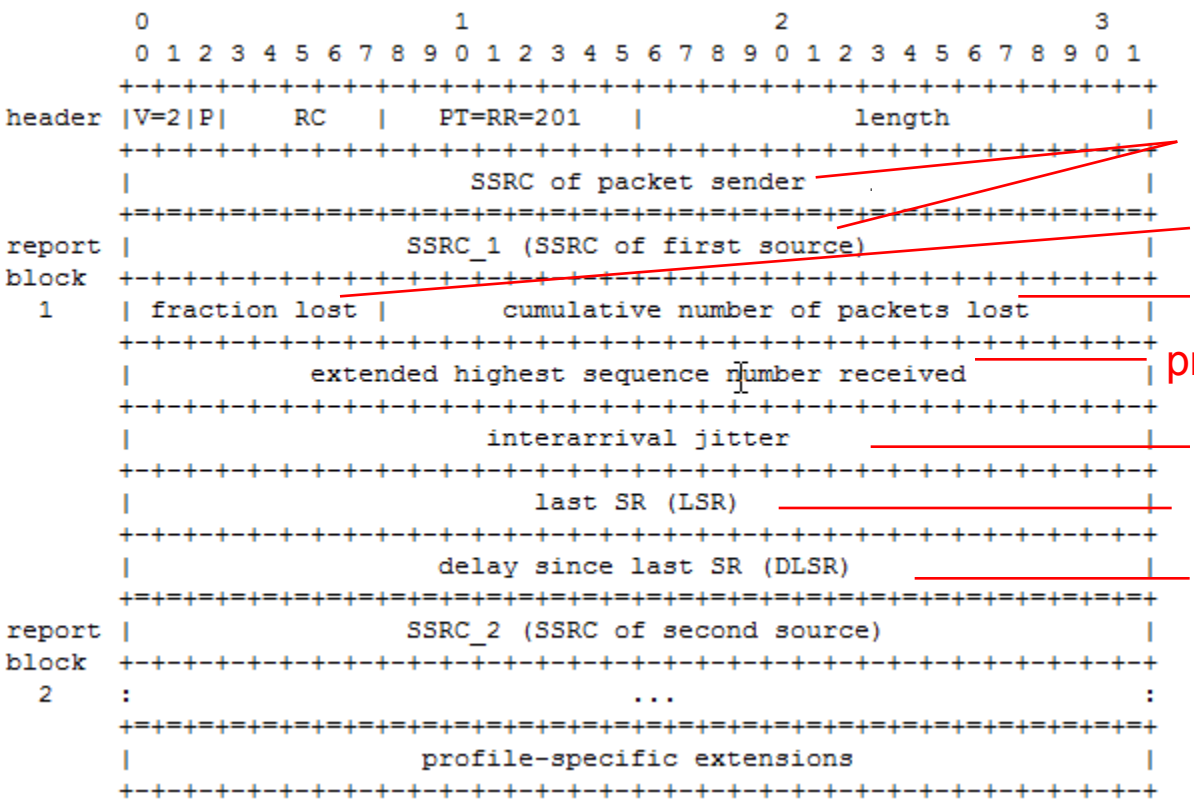
# Synchronizace

- Synchronizujeme různé streamy audio, video, snímky, …
- Časové značky jsou často umístěny v náhodných intervalech
- Nemusí tikat nominální rychlosti
- SR slouží ke korelaci reálného času za pomoci časových značek RTP

# Příklad


Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.24
User Datagram Protocol, Src Port: murx (2743), Dst Port: igcp (2801)
Real-time Transport Control Protocol (Sender Report)
[Stream setup by H245 (frame 597)]
10.. .... = Version: RFC 1889 Version (2)
..0. .... = Padding: False
...0 0001 = Reception report count: 1
Packet type: Sender Report (200)
Length: 12 (52 bytes)
Sender SSRC: 0x196d27c5 (426584005)
Timestamp, MSW: 81 (0x00000051)
Timestamp, LSW: 3380122050 (0xc97891c2)
[MSW and LSW as NTP timestamp: Not representable]
RTP timestamp: 1025641874
Sender's packet count: 599
Sender's octet count: 95840
Source 1
Real-time Transport Control Protocol (Source description)
[RTCP frame length check: OK - 140 bytes]
Typ paketu
Synchronization Source ID
Počet přenesených paketů

# Zpráva od příjemce – Received Report




identifikuje původce záznamu

krátkodobé ztráty

dlouhodobé ztráty

pro porovnání ztrát, přerušení spojení

vyhlazené „chvění“ mezi pakety

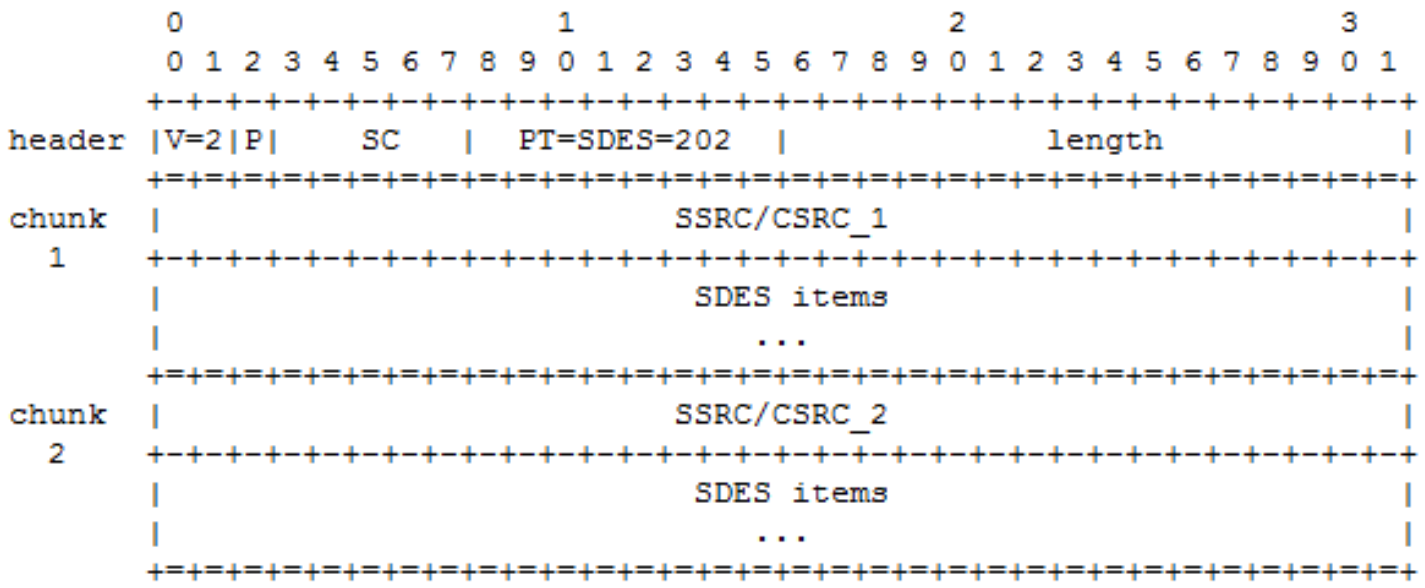
LSR – čas posledního přijmu SR

DLSR – zpoždění od posledního SR

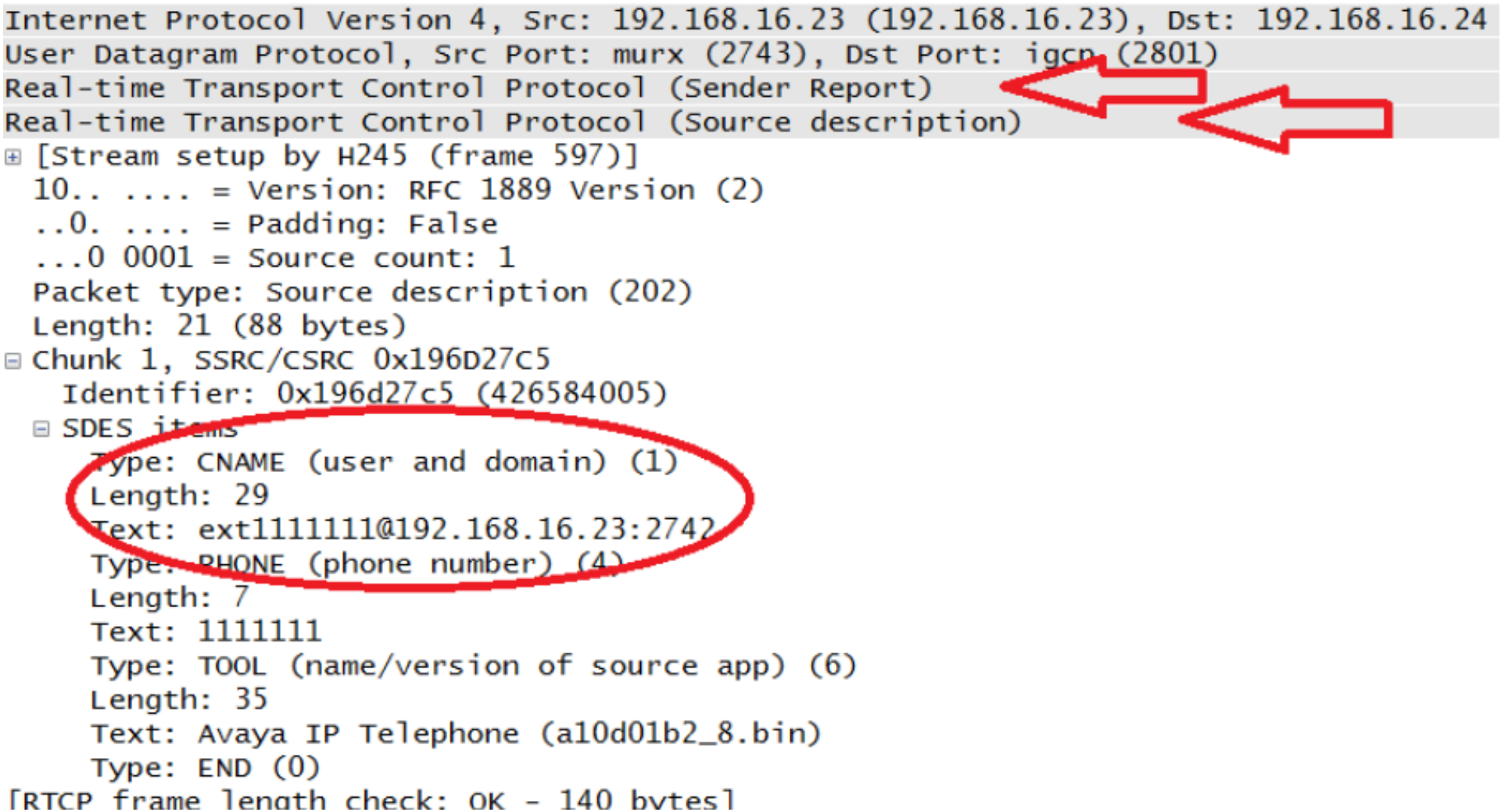
# Rozbalené pakety RR a BYE

```
Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.24
User Datagram Protocol, Src Port: murx (2743), Dst Port: igcp (2801)
Real-time Transport Control Protocol (Receiver Report)
⊞ [Stream setup by H245 (frame 597)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 0000 = Reception report count: 0
  Packet type: Receiver Report (201)
  Length: 1 (8 bytes)
  Sender SSRC: 0x196d27c5 (426584005)
Real-time Transport Control Protocol (Source description)
Real-time Transport Control Protocol (Goodbye)
⊞ [Stream setup by H245 (frame 597)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 0001 = Source count: 1
  Packet type: Goodbye (203)
  Length: 4 (20 bytes)
  Identifier: 0x196d27c5 (426584005)
  Length: 8
  Text: Teardown
[RTCP frame length check: OK - 116 bytes]
```

# Vizitky odesilatelů – Source DEScription
## (vlastnosti odesilatelů RTP komunikace)



# Příklad paketu SDES



# Typy SDES

| | | |
|---|---|---|
| END | End of SDES list | 0 |
| CNAME | Canonical name | 1 |
| NAME | Username | 2 |
| EMAIL | User's electronic mail address | 3 |
| PHONE | User's phone number | 4 |
| LOC | Geographic user location | 5 |
| TOOL | Name of application or tool | 6 |
| NOTE | Notice ab out this source | 7 |
| PRIV | Private extensions | 8 |

# Kolize

- dva zdroje mají stejné SSRC: pro 1000 členů relace souběžně spojených je pravděpodobnost asi 10-4

- Řešení kolize: poslání BYE, získání nového identifikátoru

# Packet RTCP s vizitkou SDES odchytený Wiresharkem

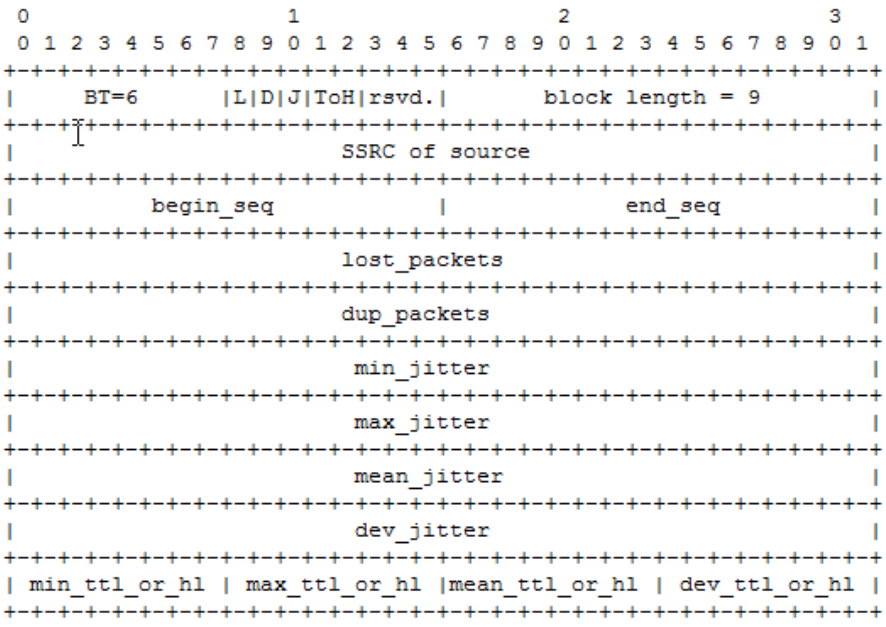
```
Real-time Transport Control Protocol (Sender Report)
    [Stream setup by H245 (frame 51)]
        [Setup frame: 51]
        [Setup Method: H245]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    Length: 12 (52 bytes)
    Sender SSRC: 0xbcdc0094 (3168534676)
    Timestamp, MSW: 11 (0x0000000b)
    Timestamp, LSW: 22544384 (0x01580000)
    [MSW and LSW as NTP timestamp: Feb  7, 2036 06:28:27,0052 UTC]
    RTP timestamp: 49823528
    Sender's packet count: 166
    Sender's octet count: 9960
    Source 1
        Identifier: 0xf5e33db0 (4125310384)
        SSRC contents
            Fraction lost: 0 / 256
            Cumulative number of packets lost: 0
        Extended highest sequence number received: 28620
            Sequence number cycles count: 0
            Highest sequence number received: 28620
        Interarrival jitter: 0
        Last SR timestamp: 0 (0x00000000)
        Delay since last SR timestamp: 0 (0 milliseconds)
Real-time Transport Control Protocol (Source description)
    [Stream setup by H245 (frame 51)]
        [Setup frame: 51]
        [Setup Method: H245]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Source count: 1
    Packet type: Source description (202)
    Length: 11 (48 bytes)
```

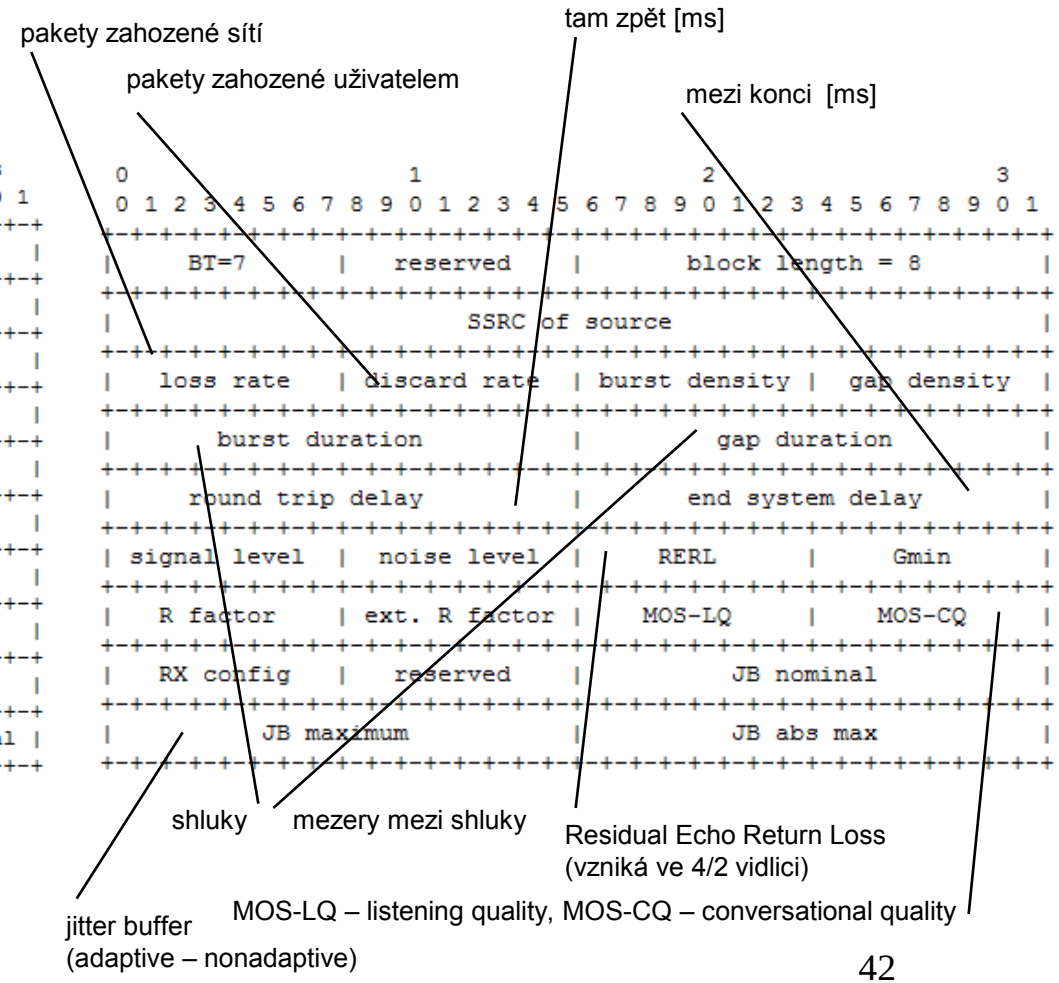
Verze 2

```
    Chunk 1, SSRC/CSRC 0xBCDC0094
        Identifier: 0xbcdc0094 (3168534676)
        SDES items
            Type: CNAME (user and domain) (1)
            Length: 14
            Text: IP200A@0.0.0.0
            Type: NAME (common name) (2)
            Length: 6
            Text: IP200A
            Type: TOOL (name/version of source app) (6)
            Length: 11
            Text: innovaphone
            Type: END (0)
[RTCP frame length check: OK - 100 bytes]
```

# Zasílání rozšířených zpráv dohledu dle RTCP XR

Rozšíření RTCP XR (Extended Reports) v RFC 3611 z roku 2003 umožňuje zasílání informace o kvalitě hovoru v MOS.
K výměně těchto zpráv se používají tzv. bloky oznámení (Report Blocks), např.:

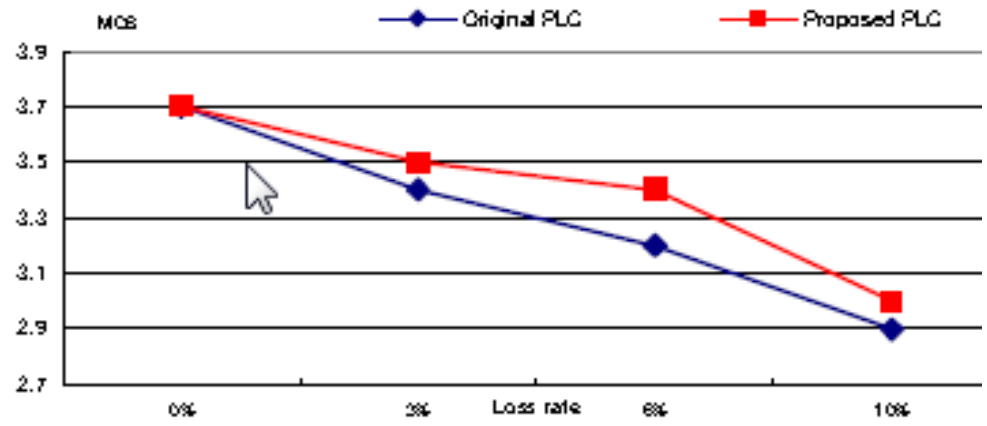


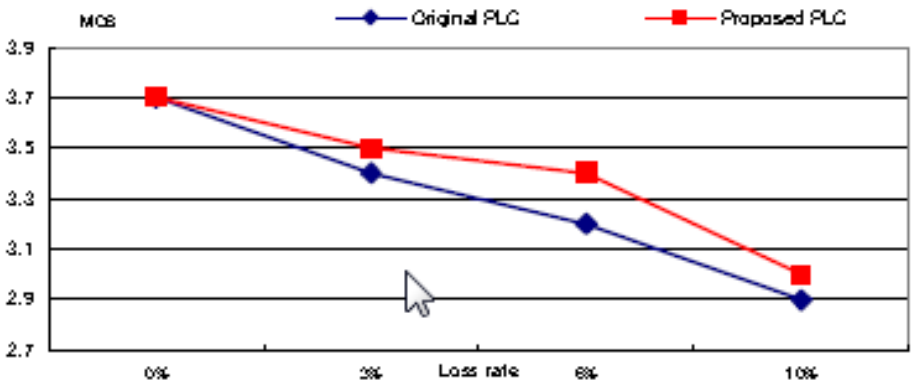



# Naměřen údaje lze použít pro vylepšování vlastností přenosu

Příklad: Použití Gilbert-Elliotova modelu pro vylepšování vlastností algoritmu PLC ( Packet Loss Concealment) použitého v kodeku G.729A.

Zdroj:
Jinsul Kim, Seung Ho Han, Hyun-Woo Lee, Won Ryu, and Minsoo Hahn: „QoS-Factor Transmission Control Mechanism for Voice over IP Network based on RTCP-XR Scheme“

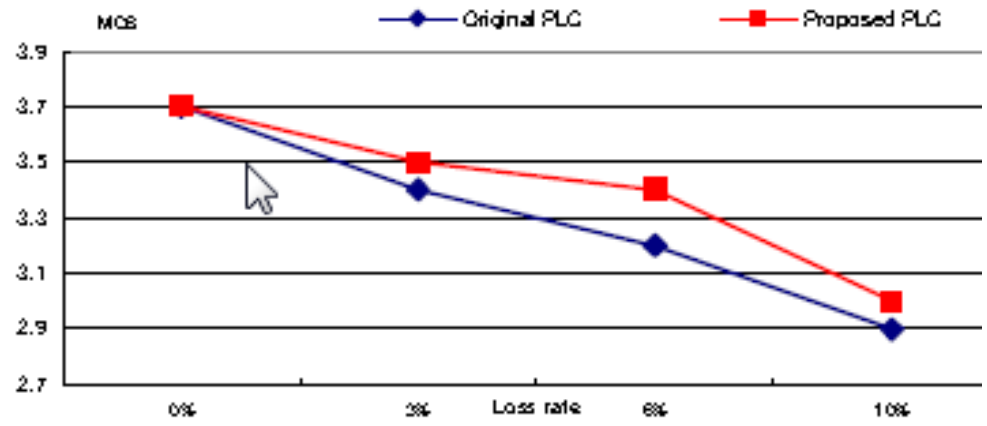


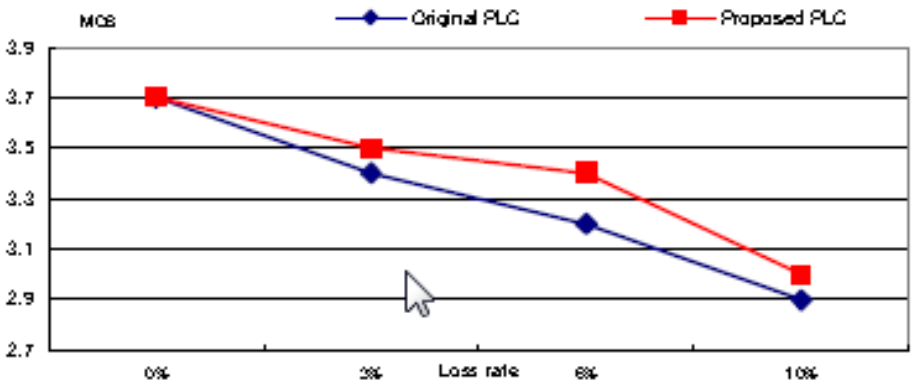



# Naměřen údaje lze použít pro vylepšování vlastností přenosu

Příklad: Použití Gilbert-Elliotova modelu pro vylepšování vlastností algoritmu PLC ( Packet Loss Concealment) použitého v kodeku G.729A.

Zdroj:
Jinsul Kim, Seung Ho Han, Hyun-Woo Lee, Won Ryu, and Minsoo Hahn: „QoS-Factor Transmission Control Mechanism for Voice over IP Network based on RTCP-XR Scheme“



# 3. Protokoly cRTP, SRTP a ZRTP

# cRTP

RFC 2508 – komprese záhlaví IP, UDP, RTP pro nízkorychlostní sériová připojení.
RFC 2509 – komprese záhlaví IP přes protokol PPP.
RFC 3545 – protokol ECRTP pro připojení s vysokým zpožděním, ztrátou paketů zpřeházenými pakety.

Podstata: nepřenáší se opakující se stejné údaje. Nevýhoda: Zátěž procesorů na směrovačích. Kalkulace:

G.711 - 160 B
IP/UDP/RTP 40 B, FR 4 B
Celkem 204 B * 50 p/s * 8b = 81 600 kb/s

G.711 - 160 B
IP/UDP/cRTP 5 B, FR 4 B
Celkem 169 B * 50 p/s * 8b = 67 600 kb/s

G.729 - 20 B
IP/UDP/RTP 40 B, FR 4 B
Celkem 64 B * 50 p/s * 8b = 25 600 kb/s

G.729 - 20 B
IP/UDP/cRTP 5 B, FR 4 B
Celkem 29 B * 50 p/s * 8b = 11 600 kb/s

# Enhanced Compressed RTP v RFC 3545

Network Working Group
Request for Comments: 3545
Category: Standards Track

T. Koren
Cisco Systems
S. Casner
Packet Design
J. Geevarghese
Motorola India Electronics Ltd.
B. Thompson
P. Ruddy
Cisco Systems
July 2003

Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document describes a header compression scheme for point to point links with packet loss and long delays. It is based on Compressed Real-time Transport Protocol (CRTP), the IP/UDP/RTP header compression described in RFC 2508. CRTP does not perform well on such links: packet loss results in context corruption and due to the long delay, many more packets are discarded before the context is repaired. To correct the behavior of CRTP over such links, a few extensions to the protocol are specified here. The extensions aim to reduce context corruption by changing the way the compressor updates the context at the decompressor: updates are repeated and include updates to full and differential context parameters. With these extensions, CRTP performs well over links with packet loss, packet reordering and long delays.

# Nástroje pro odposlech

## (VOIPSA – The Voice over IP Security Alliance)

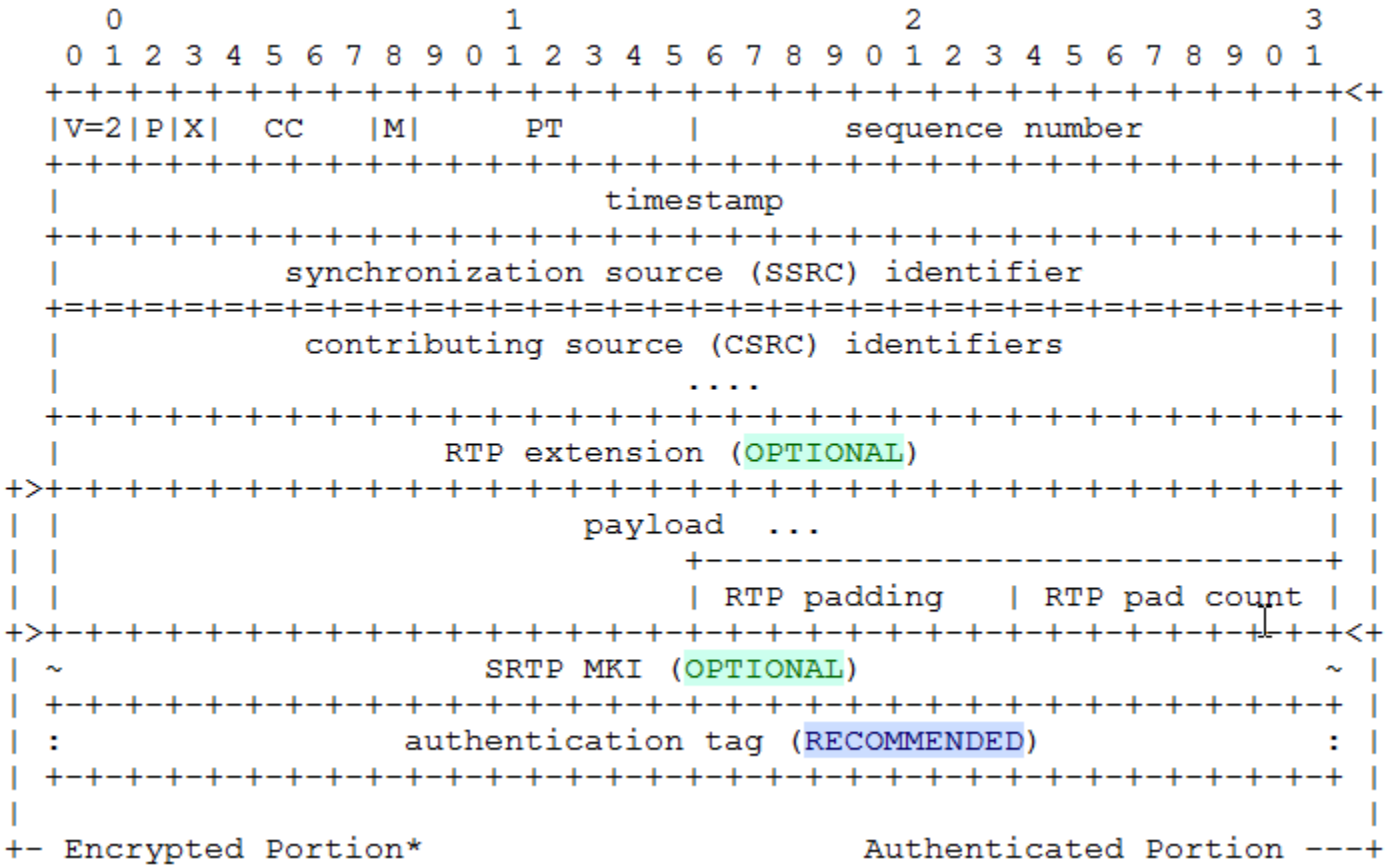
**VoIP Sniffing Tools**

- AuthTool - Tool that attempts to determine the password of a user by analyzing SIP traffic.
- Cain & Abel - Multi-purpose tool with the capability to reconstruct RTP media calls.
- CommView VoIP Analyzer - VoIP analysis module for CommView that is suited for real-time capturing and analyzing Internet telephony (VoIP) events, such as call flow, signaling sessions, registrations, media streams, errors, etc.
- Etherpeek - general purpose VoIP and general ethernet sniffer.
- ILTY ("I'm Listening To You") - Open-source, multi-channel SKINNY sniffer.
- NetDude - A framework for inspection, analysis and manipulation of tcpdump trace files.
- Oreka - Oreka is a modular and cross-platform system for recording and retrieval of audio streams.
- PSIPDump - psipdump is a tool for dumping SIP sessions (+RTP traffic, if available) from pcap to disk in a fashion similar to "tcpdump -w".
- rtpBreak - rtpBreak detects, reconstructs and analyzes any RTP session through heuristics over the UDP network traffic. It works well with SIP, H.323, SCCP and any other signaling protocol. In particular, it doesn't require the presence of RTCP packets.
- SIPomatic - SIP listener that's part of LinPhone
- SIPv6 Analyzer - An Analyzer for SIP and IPv6.
- UCSniff - UCSniff is an assessment tool that allows users to rapidly test for the threat of unauthorized VoIP eavesdropping. UCSniff supports SIP and Skinny signaling, G.711-ulaw and G.722 codecs, and a MITM ARP Poisoning mode.
- VoiPong - VoIPong is a utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. It supports SIP, H323, Cisco's Skinny Client Protocol, RTP and RTCP.
- VoIPong ISO Bootable - Bootable "Live-CD" disc version of VoIPong.
- VOMIT - The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.
- Wireshark - Formerly Ethereal, the premier multi-platform network traffic analyzer.
- WIST - Web Interface for SIP Trace - a PHP Web Interface that permits you to connect on a remote host/port and capture/filter a SIP dialog.

http://www.voipsa.org/Resources/tools.php

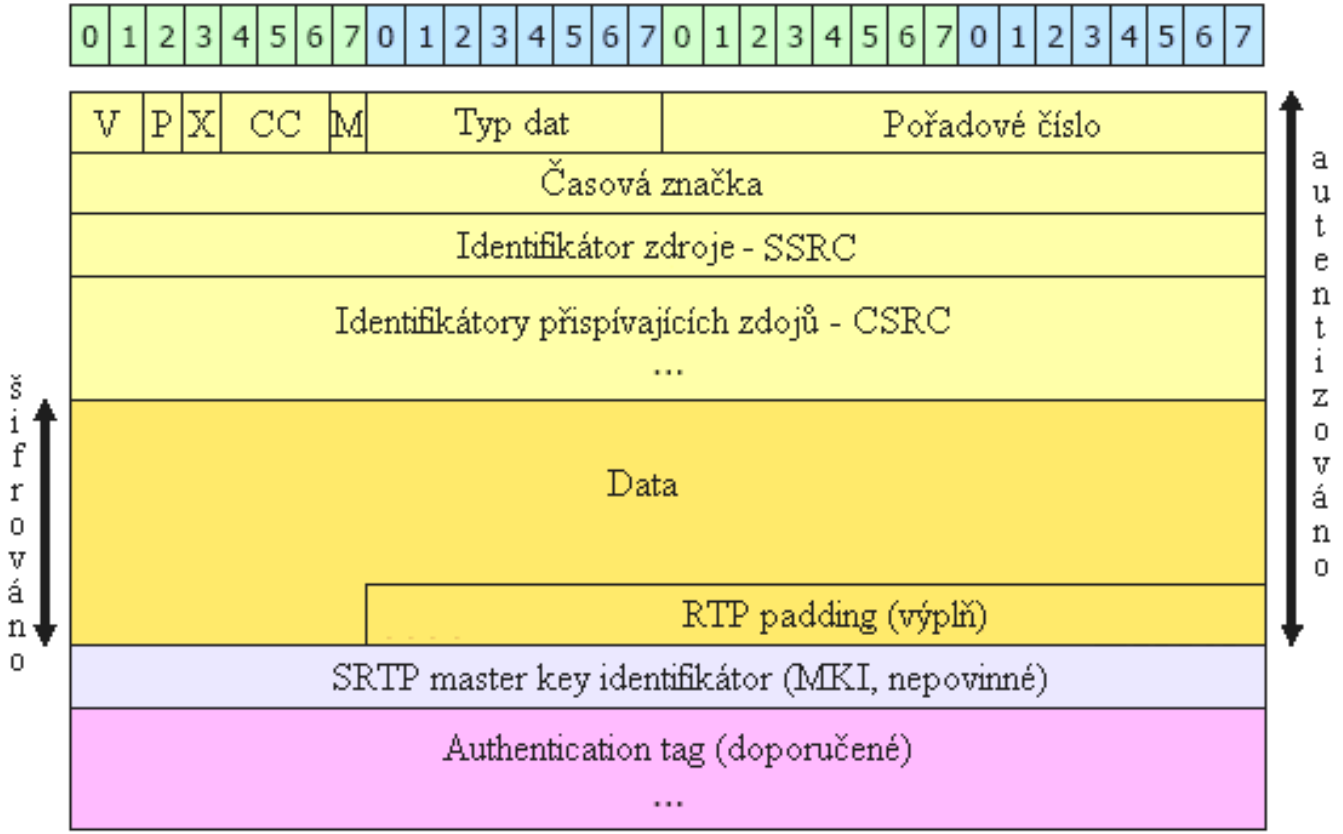
# Protokol SRTP

*(Secure Real-time Transport Protocol)*



# Formát SRTP paketu

*(zdroj http://realtimesecure.asp2.cz/srtp.aspx)*




Pole, která jsou navíc oproti RTP: MKI a Authentication tag.

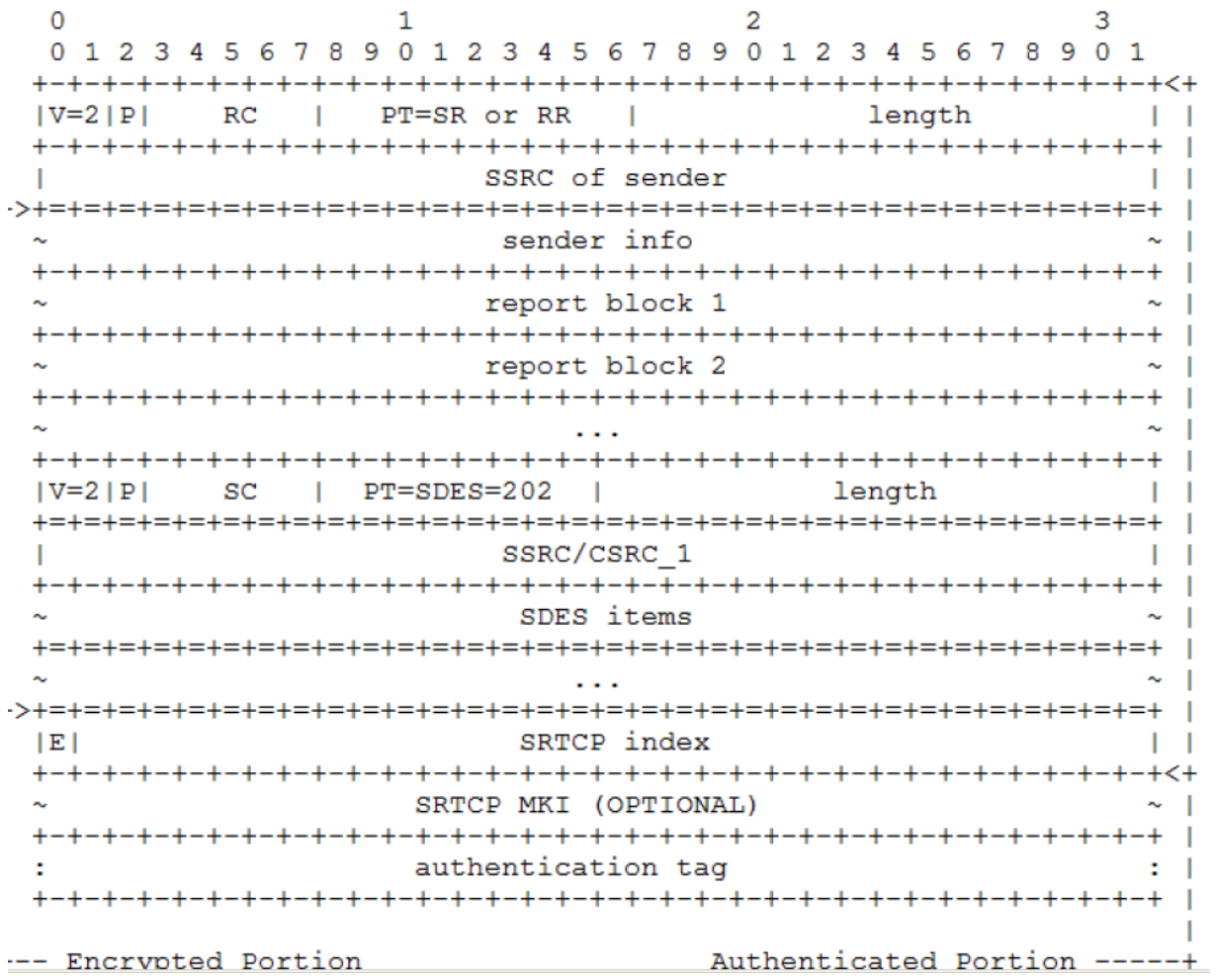
# Pole, která jsou navíc oproti RTP

**Master Key Identifier** (MKI) – nepovinné a identifikuje master key, od kterého jsou odvozeny tajné symetrické klíče session keys (klíče relace). Klíče relace jsou dohodnuty mezi uživateli hned po navázání spojení a po zbytek celé relace se jimi šifrují přenášená multimediální data. Nejdřív si ovšem komunikující strany musí vyměnit master key, pomocí kterého si pak vygenerují všechny potřebné klíče sezení.

K výměně master key se může použít protokol SDP (protokol pro inicializaci relací). Ten ale neposkytuje žádnou formu zabezpečení a tak je třeba navíc použít protokoly TLS nebo IPSec.

**Authentication tag** je šifrovaný kontrolní součet záhlaví a těla RTP paketu. Je doporučený a chrání pakety od neautorizované změny obsahu.

# Záhlaví protokolu SRTCP



# Porovnání IPSec a SRTP

## *G.711, 50 p/s*

| HDLC | MPLS | IP | IPSec | UDP | RTP | G.711 |
|---|---|---|---|---|---|---|
| 6 | 4 | 20 | 40–80 | 8 | 12 | 160 |

| HDLC | MPLS | IP | UDP | SRTP | G.711 |
|---|---|---|---|---|---|
| 6 | 4 | 20 | 8 | 12+4 (aut.) | 160 |

# Porovnání IPSec a SRTP

*G.729, 50 p/s*

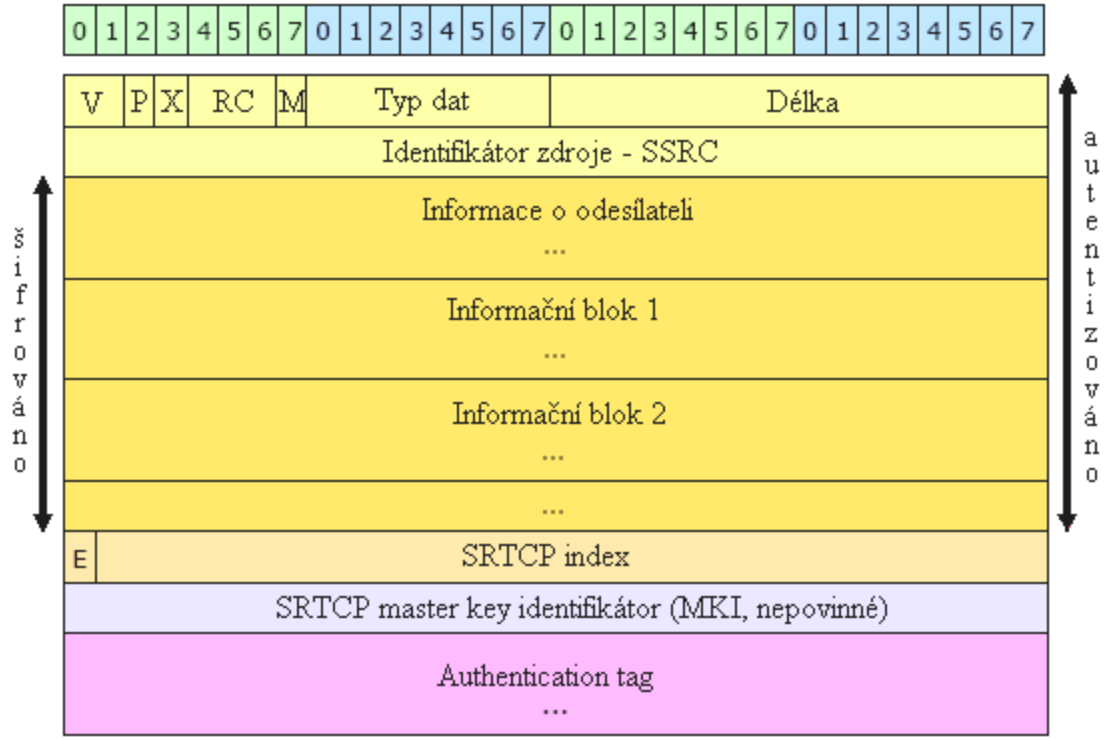
| HDLC | MPLS | IP | IPSec | UDP | RTP | G.729 |
|---|---|---|---|---|---|---|
| 6 | 4 | 20 | 60 | 8 | 12 | 20 |

**režie 85 %**

| HDLC | MPLS | IP | UDP | SRTP | G.729 |
|---|---|---|---|---|---|
| 6 | 4 | 20 | 8 | 12+4 | 20 |

**režie 73 %**

# Formát paketu SRTCP




SRTCP paket je chráněný obdobně jako SRTP paket, ale na rozdíl od SRTP je zde pole Authentication tag povinné. Jinak by bylo například možné ukončit spojení, kdyby útočník poslal paket BYE. Navíc je zde ještě pole SRTCP index, který se používá jako čítač pořadí SRTCP paketů a slouží k zabránění opakovaným útokům. První bit v tomto poli E se používá jako šifrovací značka (Encryption flag), která značí, jestli bylo tělo SRTCP paketu šifrováno.

# AES je v counter nebo F8 módu

1. counter mód E(k, IV) || E(k, IV + 1 mod 2^128) || E(k, IV + 2 mod 2^128)...
povinný pro šifrování a vyvozování klíčů relace z master key
Algoritmus umožňuje příjemci zpracovat přijaté pakety v nestanoveném pořadí, což je požadováno při použití real-time aplikací, kde pakety nemusí být vždy spolehlivě doručeny.

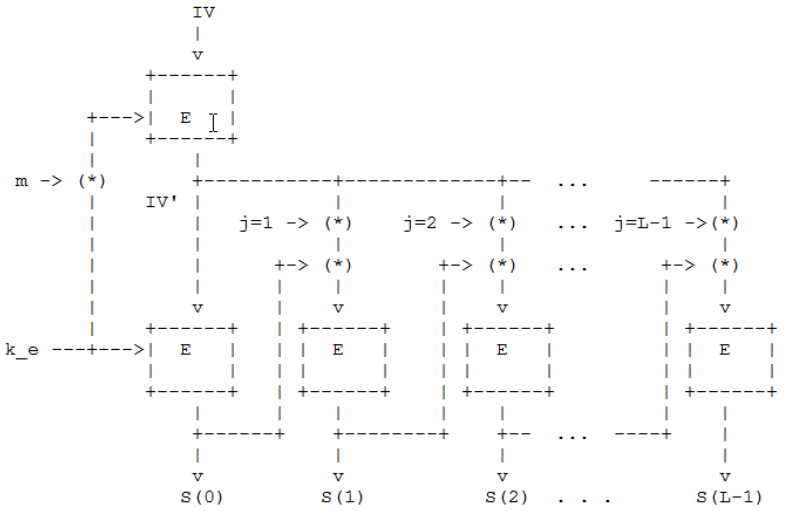
IV = (k_s * 2^16) XOR (SSRC * 2^64) XOR (i * 2^16)

Inicializační vektor IV', který se skládá z kontrolního součtu salt_key k_s, SSRC (náhodné číslo jednoznačně identifikující zdroj) a indexu paketu i.

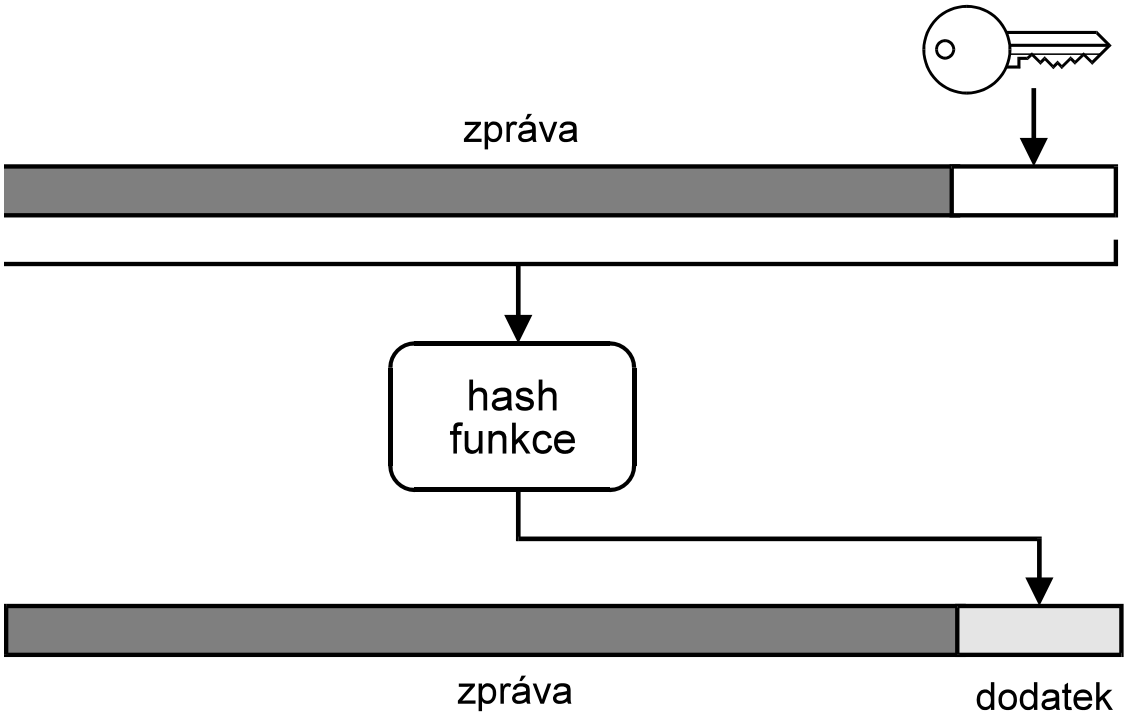
2. F8 mód (varianta OFB – Output Feedback Block

S(j) = E(k_e, IV' XOR j XOR S(j-1))

volitelný pro šifrování (určen pro pro UMTS 3G mobilní sítě)



# Generování dodatku pomocí hash funkce



# Zajištění autenticity a integrity v SRTP

HMAC – Hash Message Authentication Code

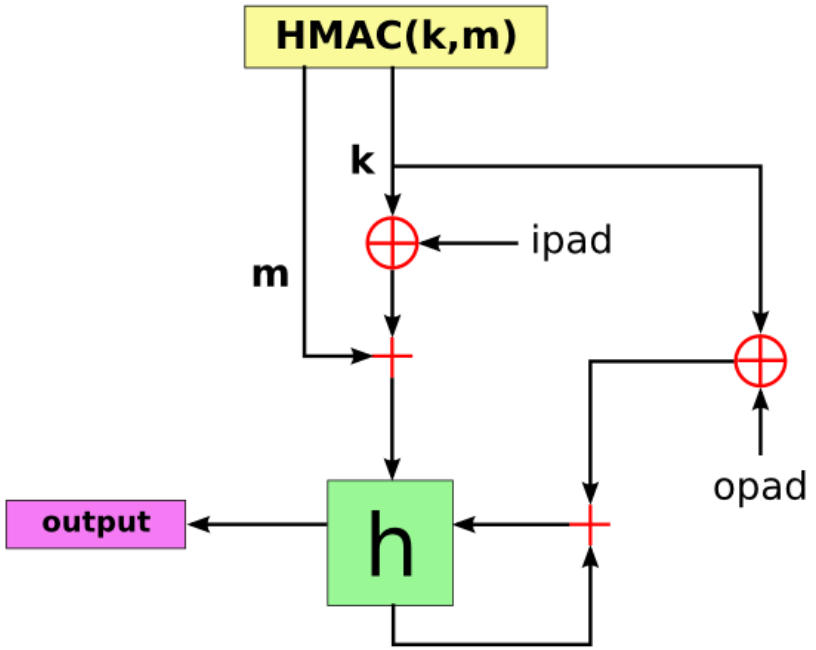
Jde o hash funkci nad zprávou *m* kombinovanou s klíčem *k*

HMAC(k,m) = H[(k ⊕ opad)||H[k ⊕ ipad)||m]]

ipad = 00110110 opakované 64x
opad = 01011100 opakované 64x

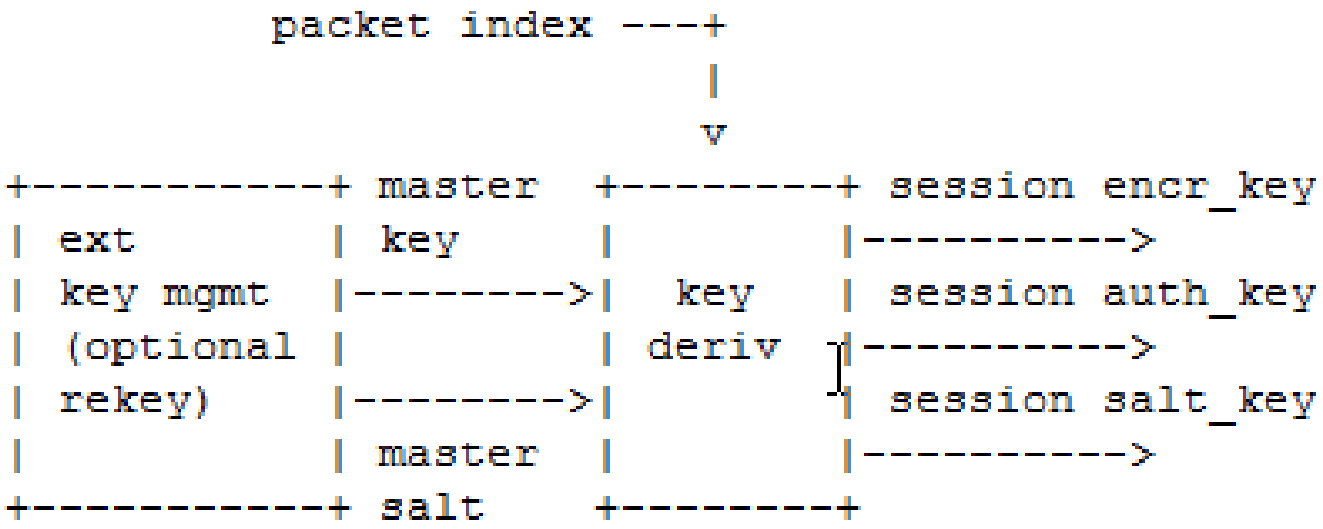
Je popsána v RFC 2104
V TLS a IP Sec se používá
HMAC-MD5 i HMAC-SHA-1,
V SRTP jen HMAC-SHA-1

2006: Úspěšný plný útok na MD4
a částečný na MD5




Vzhledem k tomu, že je při přenosu kladen důraz na co nejmenší šířku přenosového pásma, je výsledný kontrolní součet zkrácen na 80 nebo 32 bitů.

# Generování klíčů relace pomocí jednoho master key




Pro distribuci je použit protokol nechráněný protokol SDP (viz RFC 4566).

# ZRTP jako nástavba SRTP
## (Zimmermann Real-Time Transport Protocol)

Pro výměnu klíčů používá mechanismus Diffie-Hellmana (D-H hodnoty 3072 a 4096) a pak přepne do režimu SRTP.

Pro zamezení útoku typu MITM používá metody

- SAS (Short Authentication Key) – porovnávají se hashe sdíleného symetrického klíče

  M. Abdall: A Simple Threshold Authenticated Key Exchange from Short. ASIACRYPT 2005.

  S. Pasini and S. Vaudenay: SAS-Based Authenticated Key Agreement. http://lasecwww.epfl.ch/pub/lasec/doc/PV06b.pdf
  Pro WiFi patentováno v USA v roce 2009 (Luciana Costa (It))

- Retained secrets – porovnávají se hashe vytvořené z předchozího hashe a z nového sdíleného symetrického klíče.

  Blíže viz http://realtimesecure.asp2.cz/zrtp.aspx (2010, Vošec - Petr Otoupalík, pěkné)

# Příklad použití algoritmu D-H

1. Dohoda g = 11, n = 347, 1 < g < 347

2. Tajné klíče jsou x = 240, y = 39

3. A počítá $X = g^x \bmod n = 11^{240} \bmod 347 = 49$
   B počítá $Y = g^y \bmod n = 11^{39} \bmod 347 = 285$

4. A pošle B 49, B pošle A 285

5. A počítá $Y^x \bmod n = 285^{240} \bmod 347 = 268$
   B počítá $X^y \bmod n = 49^{39} \bmod 347 = 268$

A a B mají dohodnut společný klíč rovný 268, aniž by byl přenášen.

# Řešení problému s nechráněným přenosem master key v SDP použitím DTLS

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 5763
Category: Standards Track
ISSN: 2070-1721

J. Fischl
Skype, Inc.
H. Tschofenig
Nokia Siemens Networks
E. Rescorla
RTFM, Inc.

May 2010

Framework for Establishing a Secure Real-time Transport Protocol (SRTP)
Security Context Using Datagram Transport Layer Security (DTLS)

Abstract

This document specifies how to use the Session Initiation Protocol (SIP) to establish a Secure Real-time Transport Protocol (SRTP) security context using the Datagram Transport Layer Security (DTLS) protocol. It describes a mechanism of transporting a fingerprint attribute in the Session Description Protocol (SDP) that identifies the key that will be presented during the DTLS handshake. The key exchange travels along the media path as opposed to the signaling path. The SIP Identity mechanism can be used to protect the integrity of the fingerprint attribute from modification by intermediate proxies.

# Příklady řešení bezpečnosti RTP u softphonů

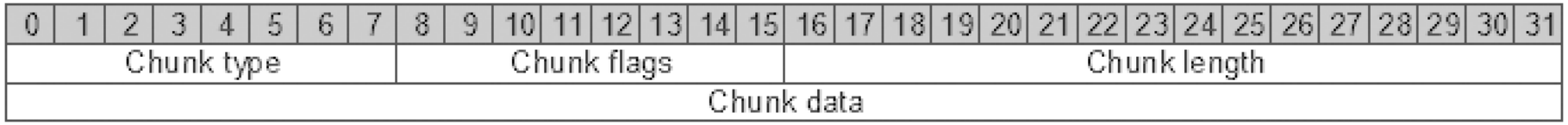
| Program | Protokoly | Bezpečnost |
|---|---|---|
| Cisco IP Communicator | SCCP (Skinny), SIP, TFTP | SRTP |
| Google Talk | XMPP | ZRTP |
| Mirial Softphone | SIP, H.323, RTSP | DTLS-SRTP |
| Mumble | CELT / Speex | TLS a OCB-AES128 |
| OctroTalk | SIP, (XMPP, STUN, ICE, Libjingle a RTP (media) | TLS a SASL |
| Revation Communicator | SIP/SIMPLE | TLS a SRTP |
| SFLphone | SIP, RTP, IAX2, STUN, SRV | Hlas (SRTP), signalizace (TLS), |
| SIP Communicator | SIP/SIMPLE, XMPP | Hlas (SRTP s potvrzováním zRTP), signalizace (TLS) |
| Zfone | SIP, RTP | SRTP, ZRTP |

Na téma penetračnícjh testů doporučuji http://www.cesnet.cz/akce/2010/vzdalena-spoluprace/p/voznak-penetracni-testy.pdf

# 4. Protokol SCTP

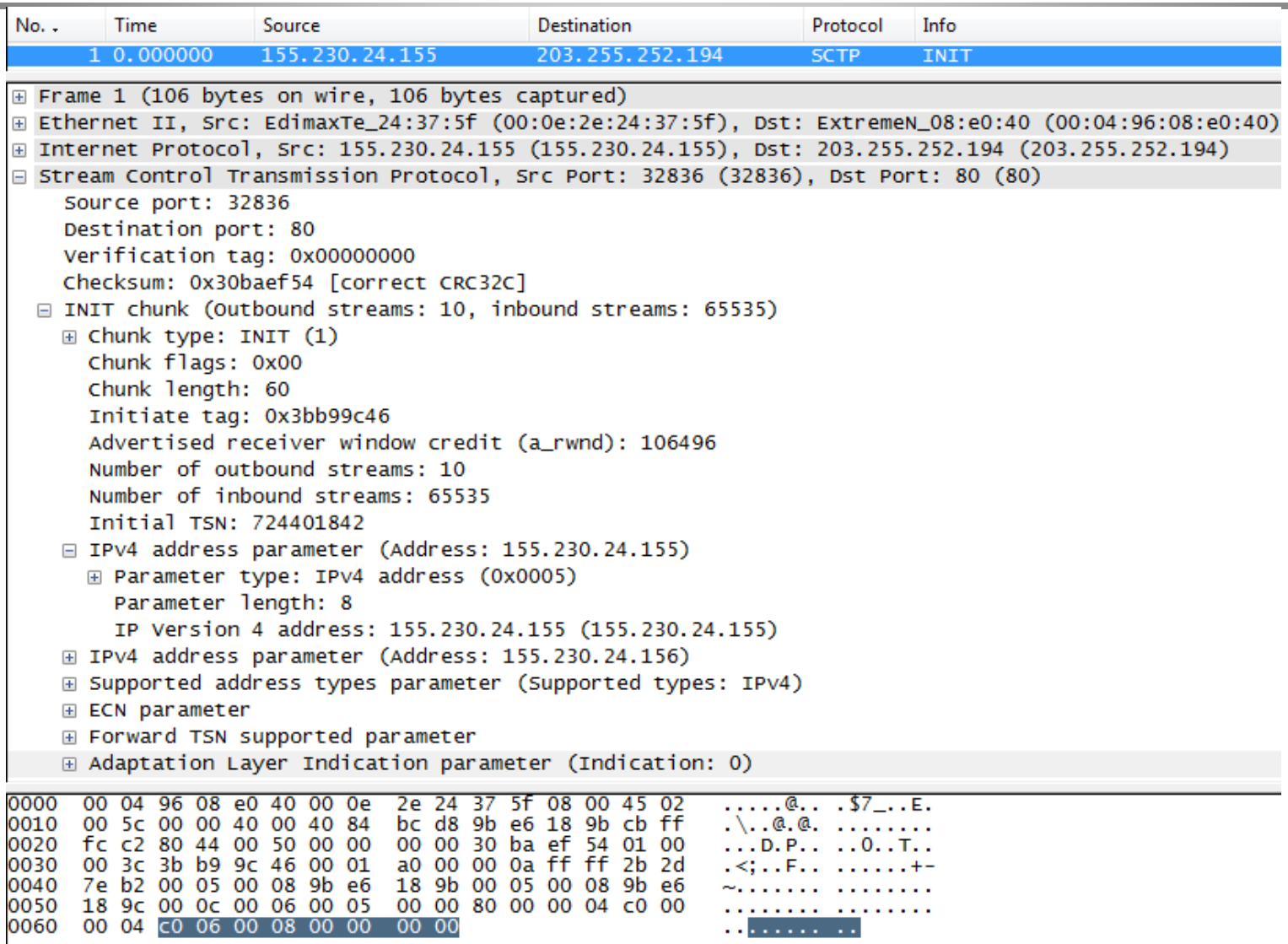
# Protokol SCTP






Protokol SCTP (Stream Control Transmission Protocol), je protokol, který se ve VoIP zatím ještě příliš neprosadil. Primárně byl navržen pro přenos PSTN signalizace přes sítě IP, lze jej však použít i pro přenos signalizačních protokolů. Jedná se o nespojovaný protokol, podobně jako UDP, ale na rozdíl od UDP je spolehlivý, doručuje pakety ve správném pořadí a má ochranu proti zahlcení.
Protokol rovněž zavádí podporu multihoming, kde se jeden (nebo oba) koncové body, mohou skládat z více IP adres.
Data jsou zde přenášena v dávkách zvaných chunk. Každý chunk je identifikován svým typem, osmibitové pole umožňuje definovat 255 typů, RFC 4960 jich zatím definovalo 15.

# Chunky v SCTP (Wireshark)



# Pěr dotazů

1. Pravda nebo lež: většina komunikačních systémů používá RTP při přenosu hlasu a videa.
2. Pravda nebo lež: RTP má stavět v kvalitě služeb mechanismu.
3. Pravda nebo lež: porty pro RTP a RTCP jsou náhodné.
4. Pravda nebo lež: RTCP je vázán na RTP stream s použitím stejného ID synchronizace zdroje.

# Odpovědi

1. Pravda nebo lež: většina komunikačních systémů používá RTP při přenosu hlasu a videa. T
2. Pravda nebo lež: RTP byl vytvořen s ohledem na QoS.
3. Pravda nebo lež: Porty pro RTP a RTCP jsou náhodné.
4. Pravda nebo lež: RTCP je vázán na RTP stream s použitím stejného ID synchronizace zdroje.

# Odpovědi

1. Pravda nebo lež: většina komunikačních systémů používá RTP při přenosu hlasu a videa. T
2. Pravda nebo lež: RTP byl vytvořen s ohledem na QoS. F
3. Pravda nebo lež: Porty pro RTP a RTCP jsou náhodné.
4. Pravda nebo lež: RTCP je vázán na RTP stream s použitím stejného ID synchronizace zdroje.

# Odpovědi

1. Pravda nebo lež: většina komunikačních systémů používá RTP při přenosu hlasu a videa. T
2. Pravda nebo lež: RTP byl vytvořen s ohledem na QoS. F
3. Pravda nebo lež: Porty pro RTP a RTCP jsou náhodné. Platí to jen pro RTP.
4. Pravda nebo lež: RTCP je vázán na RTP stream s použitím stejného ID synchronizace zdroje.

# Odpovědi

1. Pravda nebo lež: většina komunikačních systémů používá RTP při přenosu hlasu a videa. T
2. Pravda nebo lež: RTP byl vytvořen s ohledem na QoS. F
3. Pravda nebo lež: Porty pro RTP a RTCP jsou náhodné. Platí to jen pro RTP.
4. Pravda nebo lež: RTCP je vázán na RTP stream s použitím stejného ID synchronizace zdroje. F

# Jak lze RTP streamy odlišit od sebe?

# Jak lze RTP streamy odlišit od sebe?

Použitím synchronization source identifier.

# K čemu slouží protokol RTCP?

# K čemu slouží protokol RTCP?

Poskytuje zpětnou vazbu pro sledování výkonu toků RTP.

# Uveďte pět typů zpráv RTCP

# Uveďte pět typů zpráv RTCP

- Source Report
- Receiver Report
- Source Description
- Bye
- APP

# S jakou frekvencí jsou přenášeny toky RTCP?

# S jakou frekvencí jsou přenášeny toky RTCP?

5 paketů/s

# Ve kterém paketu naleznete kanonické jméno?

# Ve kterém paketu naleznete kanonické jméno?

Source Description

# Zdroje

**Wiki Wireshark http://wiki.wireshark.org/SampleCaptures#SIP_and_RTP**