3. přenáška

Protokoly přenosu dat

Osnova přednášky

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

1. Protokol RTP

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

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.

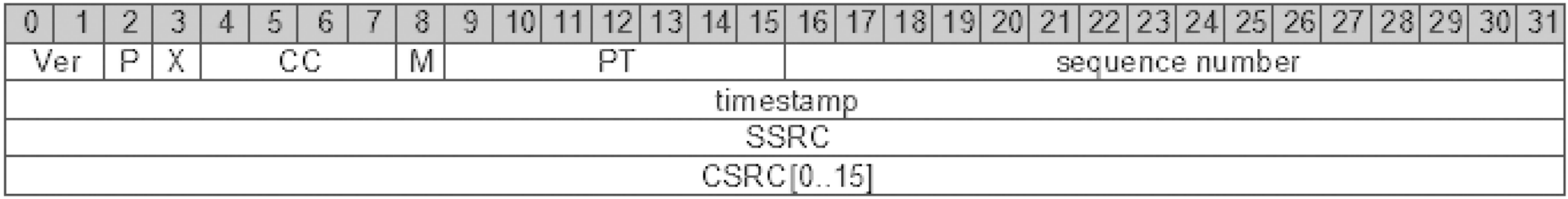
Abstract

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

Formát záhlaví



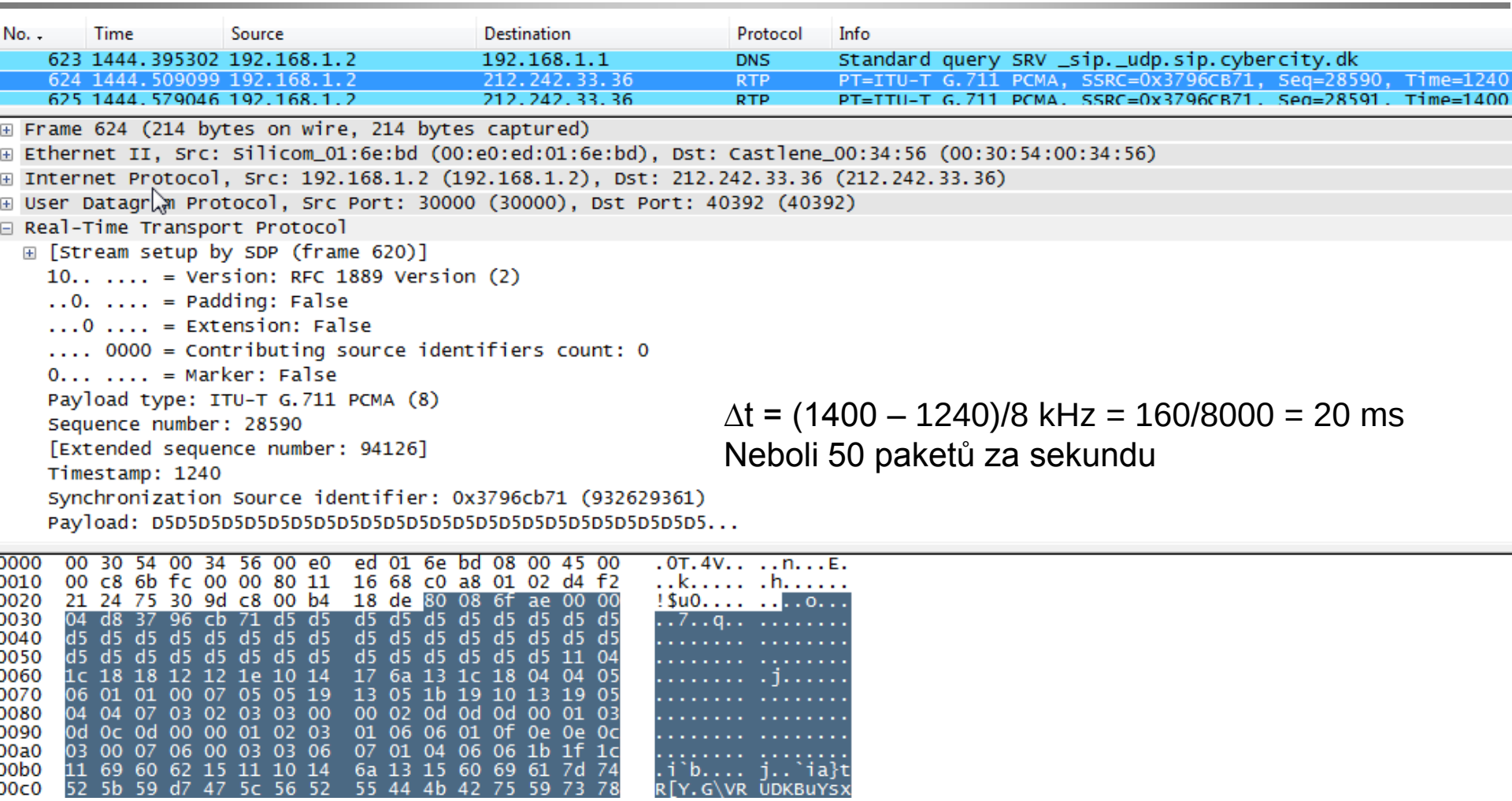
- *Ver* označuje verzi protokolu (dnes se používá verze 2),
- *P* (padding field) v případě P=1 označuje vycpávku v posledním paketu toku
- na dorovnání jednotné délky,
- *X* (extension bit) v případě X=1 označuje, že za záhlavím následuje rozšíření paketu s CSRC
- význam *M* (marked field) je dán aplikačním profilem (např. konec paketu v toku rámců).

RTP na rozdíl od UDP zavádí následující služby:
- identifikace obsahu paketu (*PT – payload type*);
- 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, používaná při mixování zdrojů).

Typy zátěže (PT)

Typ	kódování	médium	taktovací kmitočet	počet kanálů
0	PCMU	Audio	8,000	1
1	1016	Audio	8,000	1
2	G726-32	Audio	8,000	1
3	GSM	Audio	8,000	1
*4	G723	Audio	8,000	1
5	DVI4	Audio	8,000	1
6	DVI4	Audio	16,000	1
7	LPC	Audio	8,000	1
8	PCMA	Audio	8,000	1
9	G722	Audio	8,000	1
10	L16	Audio	44,100	2
11	L16	Audio	44,100	1
*12	QCELP	Audio	8,000	1
13	Reserved			1
14	MPA	Audio	90,000	1
15	G728	Audio	8,000	1
*16	DVI4	Audio	11,025	1
*17	DVI4	Audio	22,050	1
*18	G729	Audio	8,000	1
19	Reserved			1
20	Unassigned			1
21	Unassigned			1
22	Unassigned			1
23	Unassigned			1
*dyn	GSM-HR	Audio	8,000	1
*dyn	GSM-EFR	Audio	8,000	1
*dyn	L8	Audio	Variable	1
*dyn	RED	Audio	Conditional	1
*dyn	VDVI	Audio	Variable	1

Jaké je časování odesílání paketů ze zdroje?



No.	Time	Source	Destination	Protocol	Info
623	1444.395302	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.sip.cybercity.dk
624	1444.509099	192.168.1.2	212.242.33.36	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3796CB71, Seq=28590, Time=1240
625	1444.579046	192.168.1.2	212.242.33.36	RTP	PT=ITU-T G.711 PCMA, SSRC=0x3796CB71, Seq=28591, Time=1400

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.

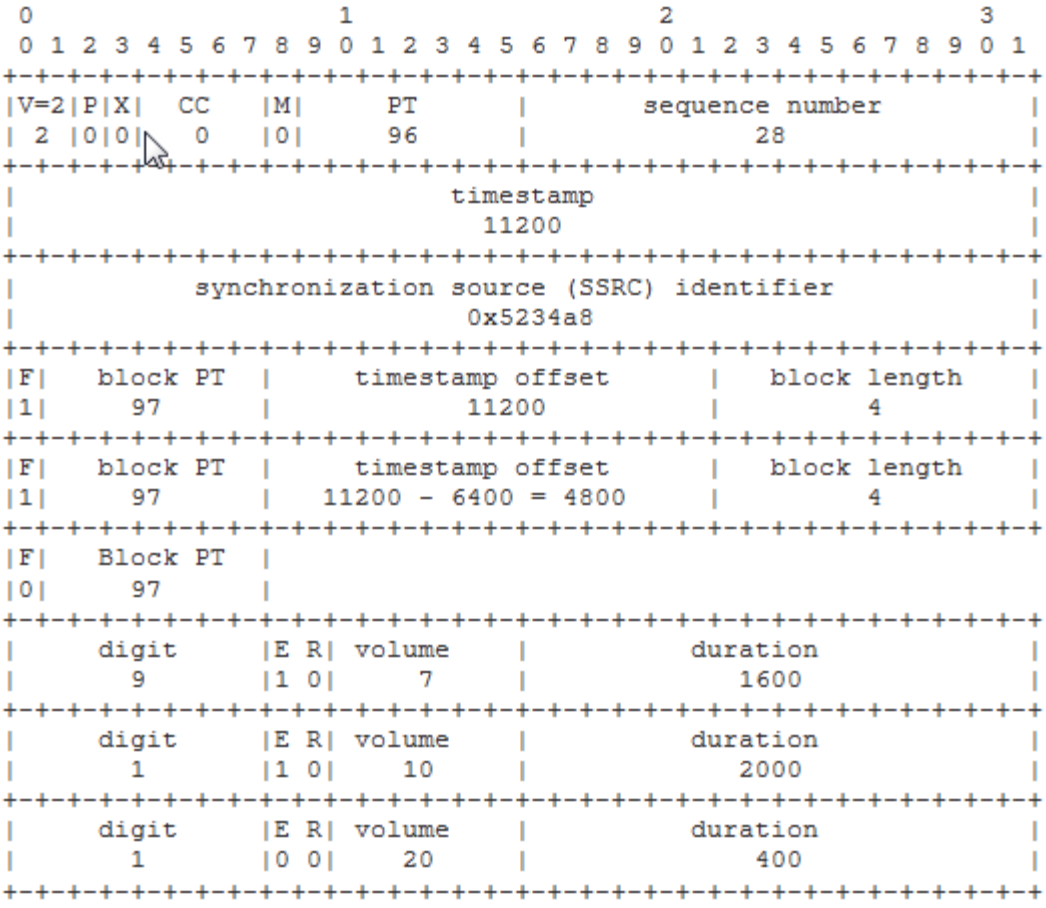
1 Introduction

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.

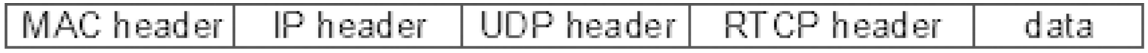


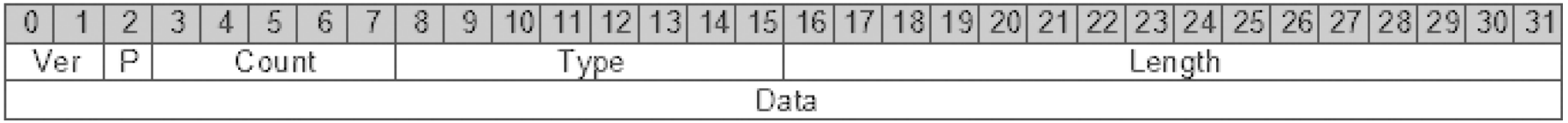
Co se dovídáme:
- bylo voleno číslo 911
- první číslice „9“ je tón o délce trvání 200 ms (1 600/8 kHz) a začíná v čase 0
- druhé číslice „1“ je tón o délce trvání 250 ms (2 000/8 kHz) a začíná v čase 800 (6 400/8 kHz) časových jednotek, timetamps)
- třetí číslice „1“ je tón o délce trvání 50 ms (400/8 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 28833 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.

2. Protokol RTPC

Protokol RTCP

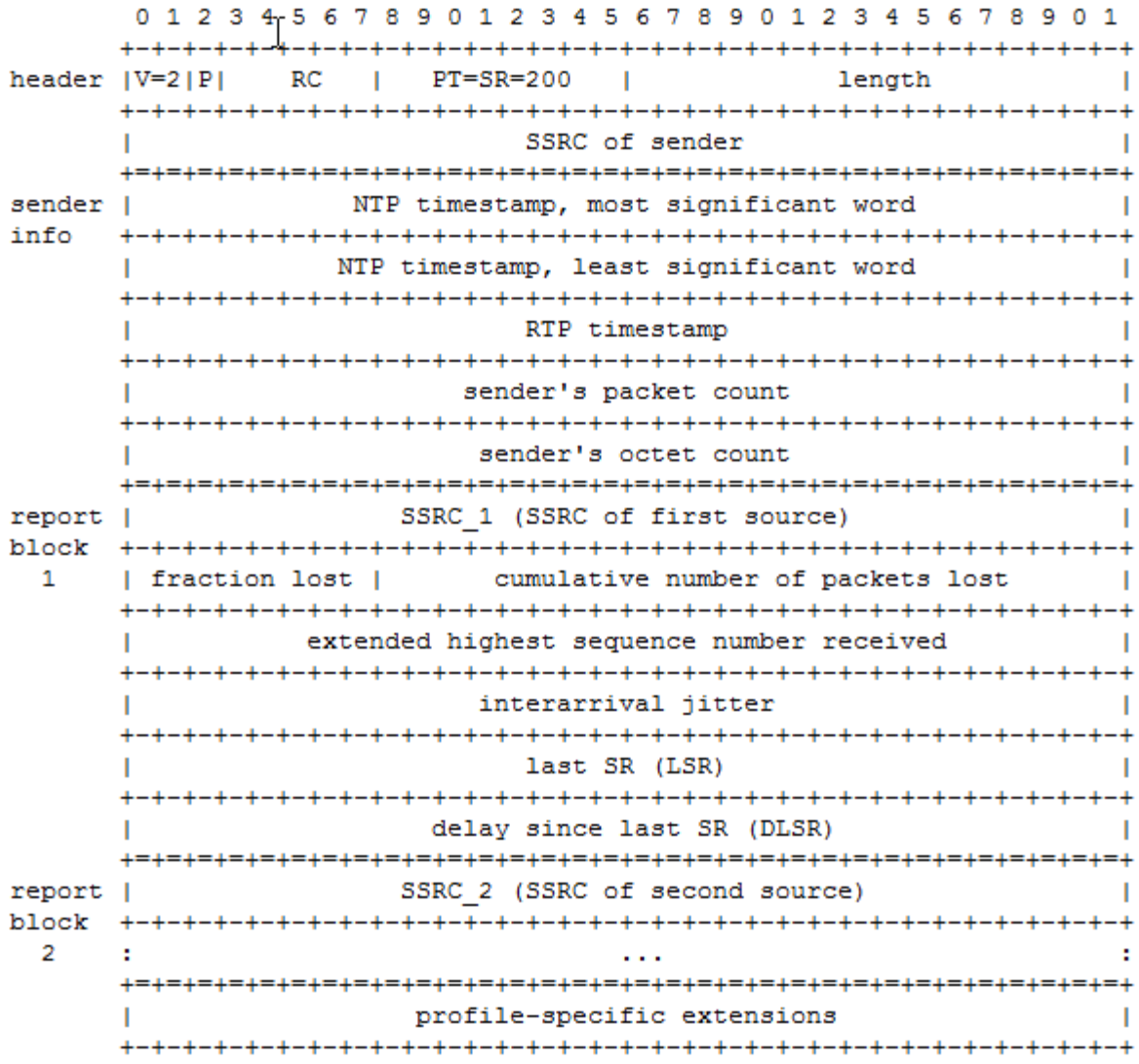




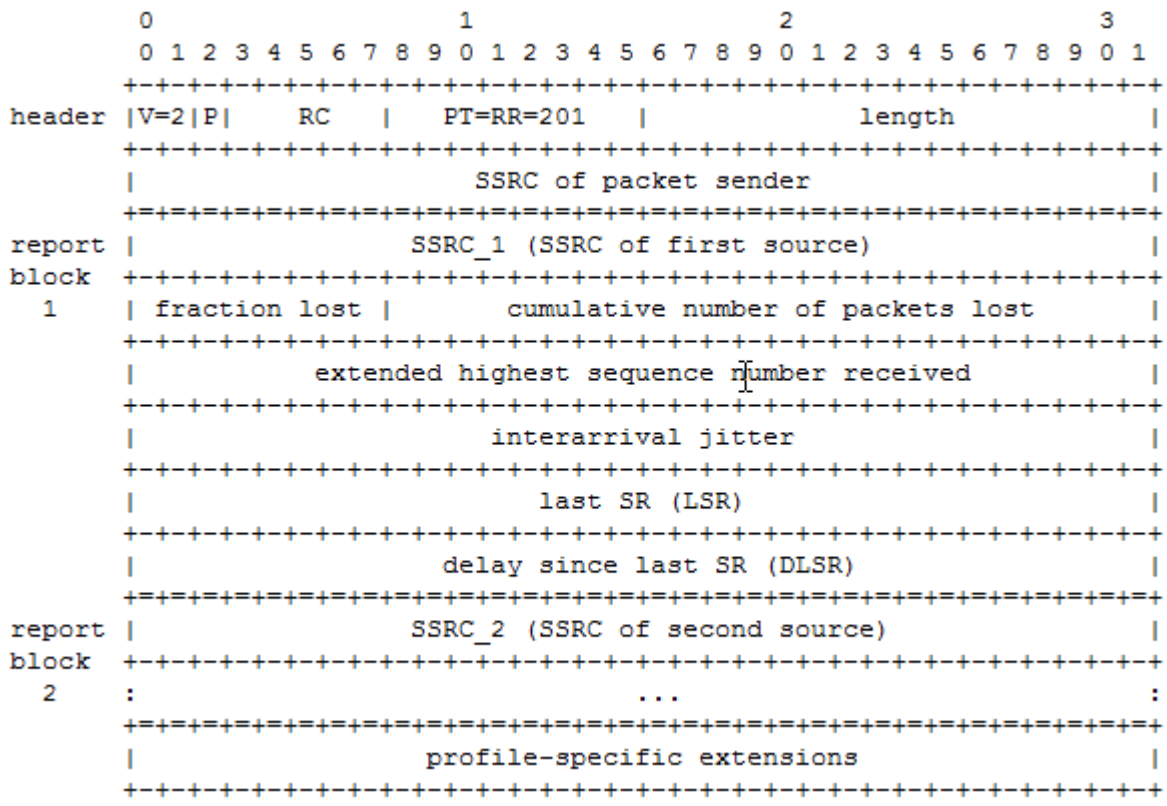
RTP podporuje sloučení několika mediálních toků do jedné relace (session) za účelem podpory aplikací ‚jako je pořádání konferenčních hovorů. Chybí mu však zpětná kontrola o tom, zda a v jakém stavu dorazily pakety k příjemci.

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.

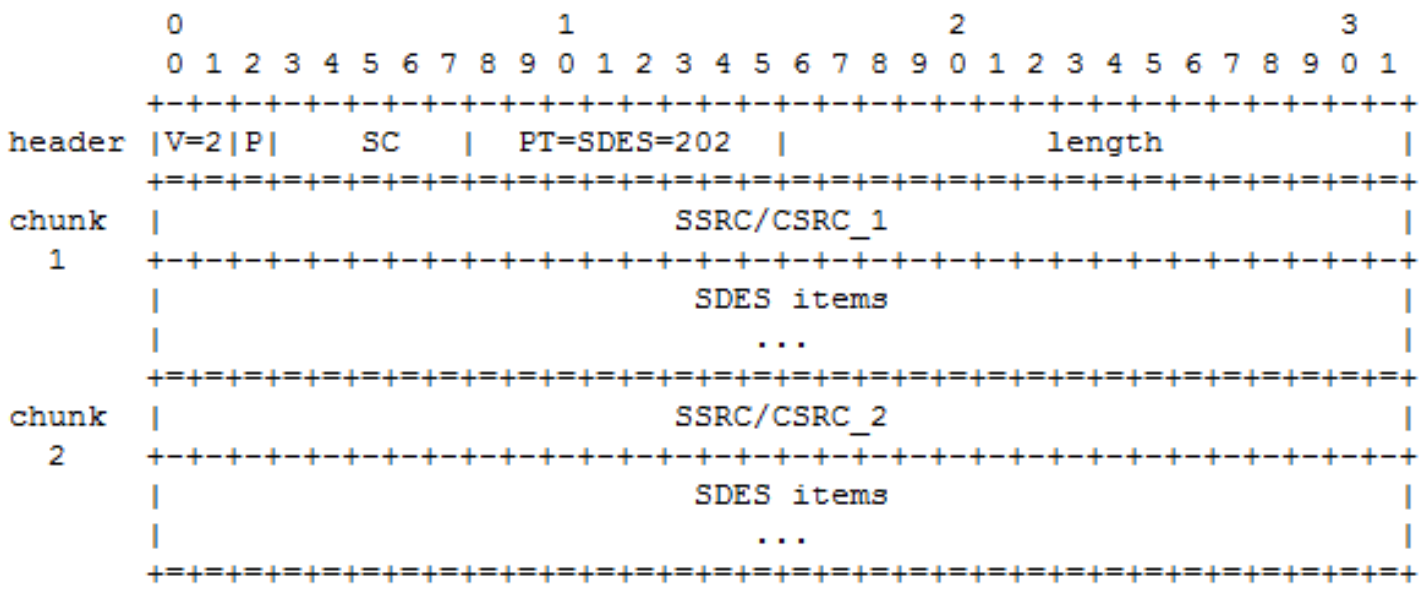
Zpráva od zdroje – Send Report
(soubor statistik o přijímaných a vysílaných datech)



Zpráva od příjemce – Received Report



Vizitky odesilatelů – Source DEScription
(vlastnosti odesilatelů RTP komunikace)



Packet RTCP s vizitkou SDES odchycený Wiresharkem

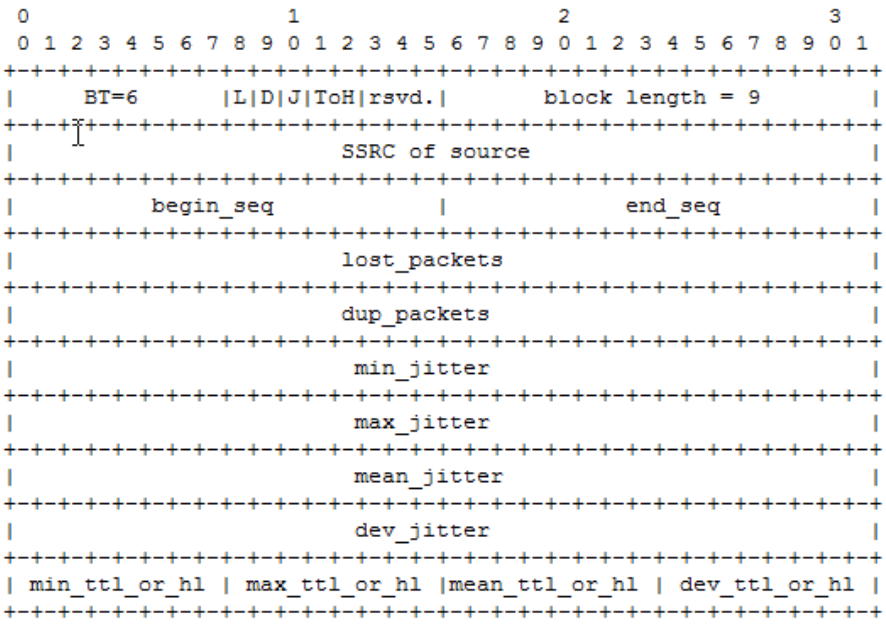
```
Real-time Transport Control Protocol (Sender Report)
    [Stream setup by H245 (frame 51)]
        [Setup frame: 51]
        [Setup Method: H245]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    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)
```

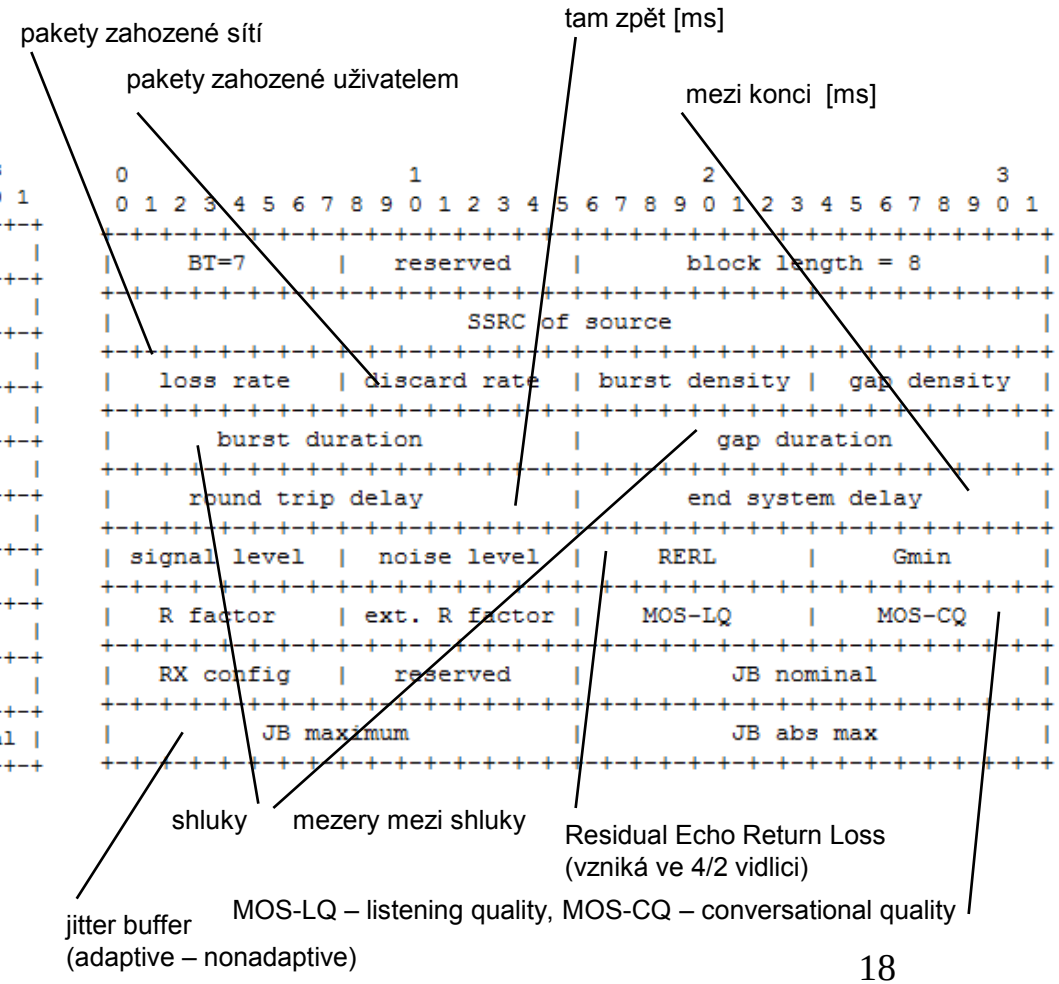
```
    Chunk 1, SSRC/CSRC 0xBCDC0094
        Identifier: 0xbcdc0094 (3168534676)
        SDES items
            Type: CNAME (user and domain) (1)
            Length: 14
            Text: IP200A@0.0.0.0
            Type: NAME (common name) (2)
            Length: 6
            Text: IP200A
         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

Verze 2

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.:

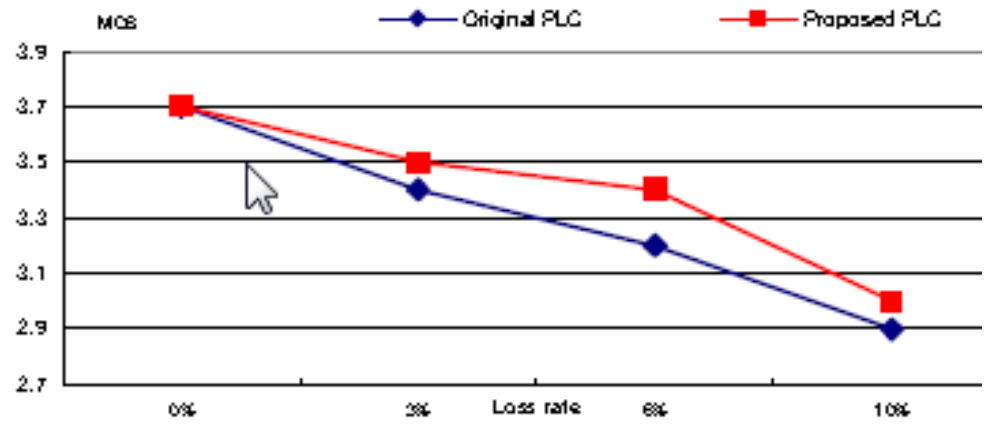


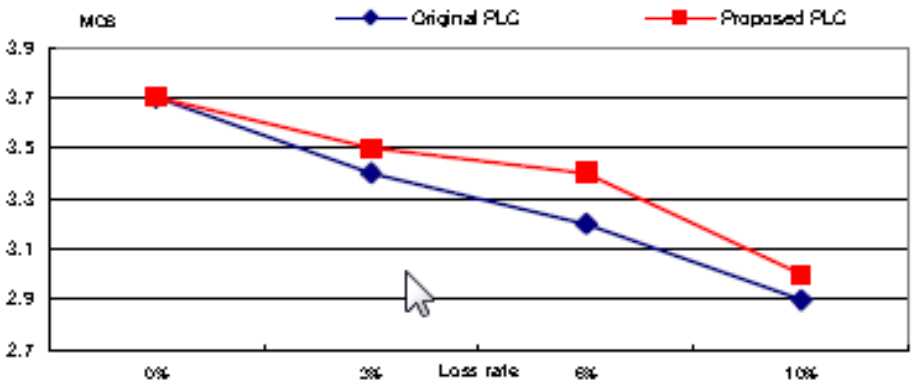


Naměřen údaje lze použít pro vylepšování vlastností přenosu

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“

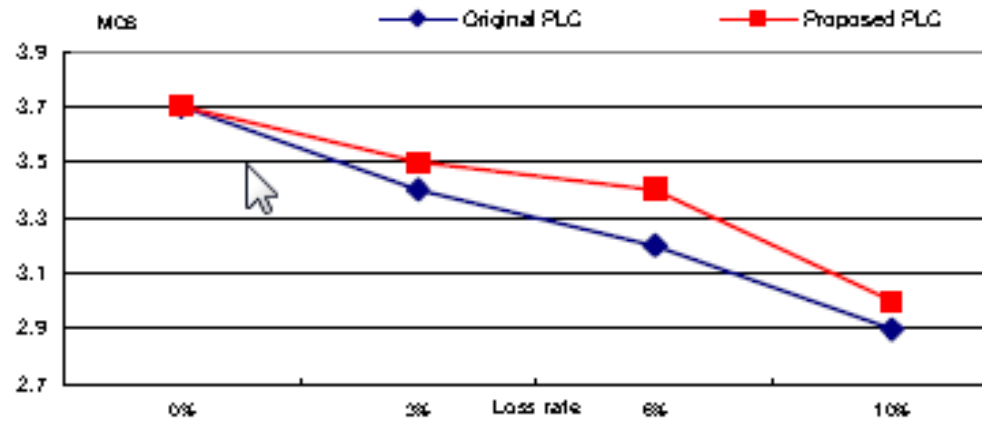


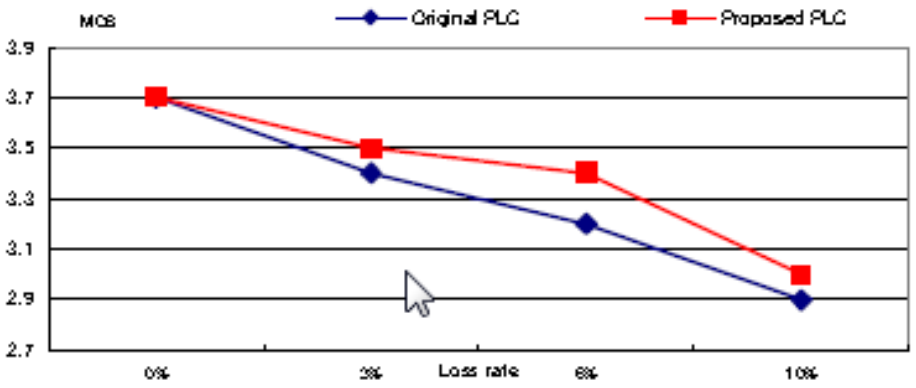


Naměřen údaje lze použít pro vylepšování vlastností přenosu

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

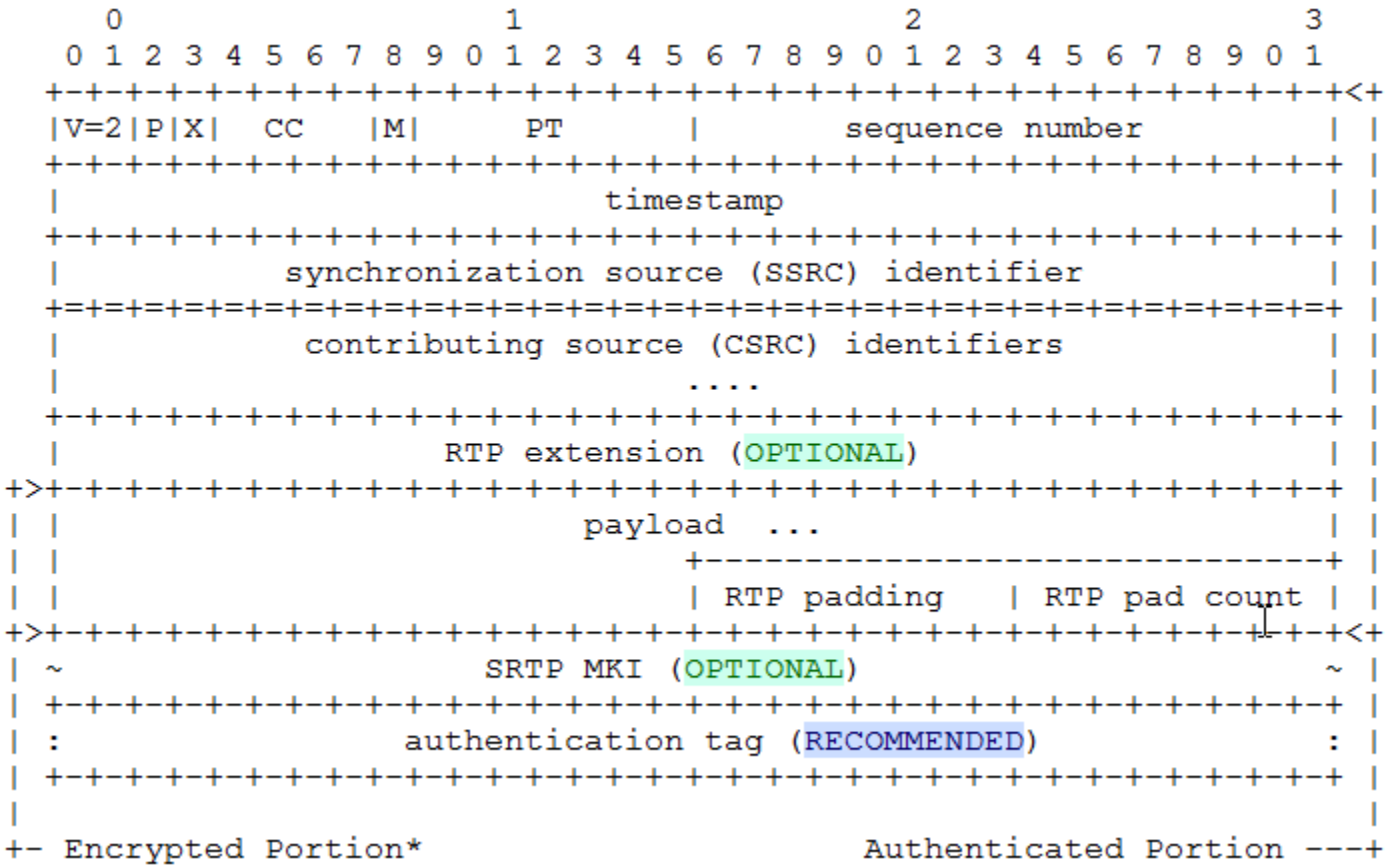
(VOIPSA – The Voice over IP Security Alliance)

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

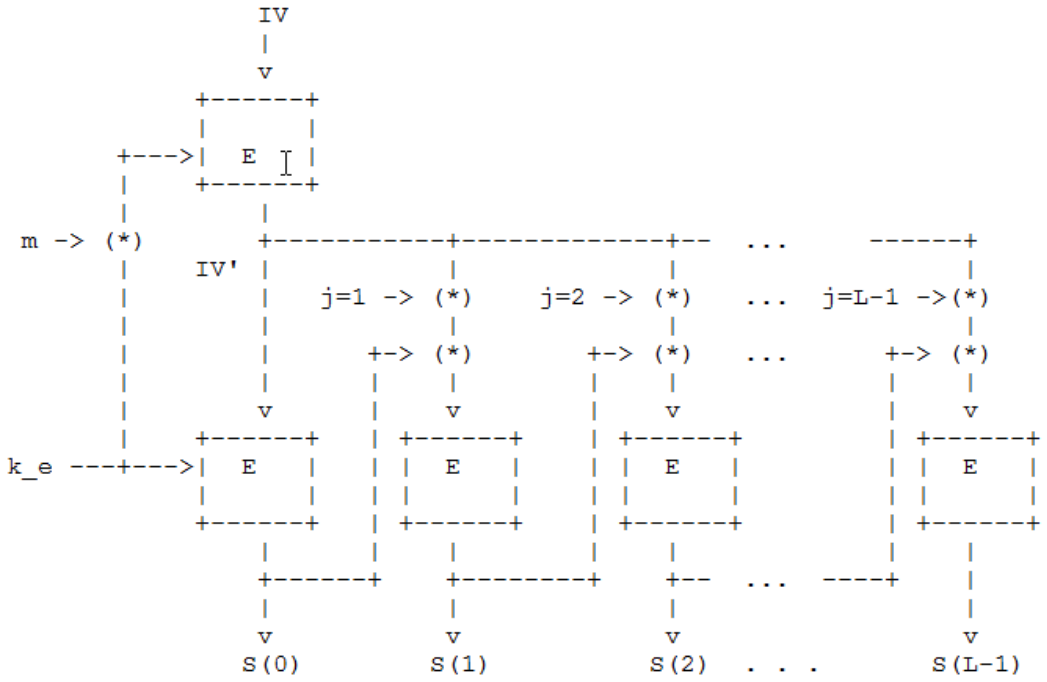
Protokol SRTP



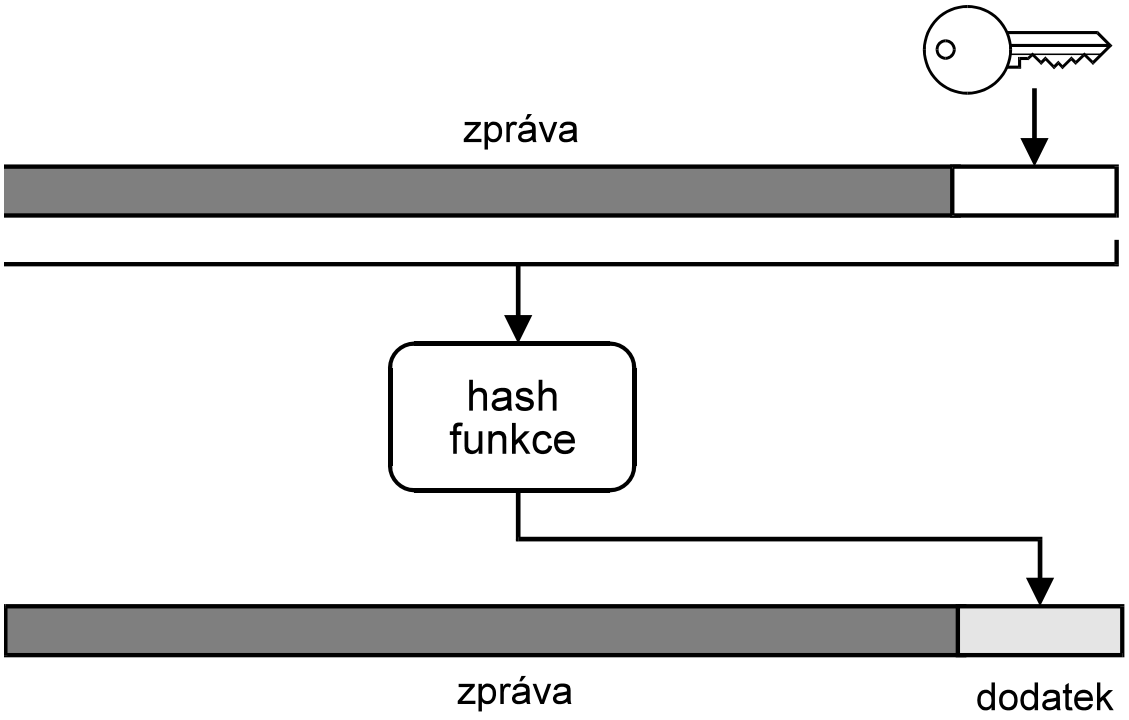
AES je v counter nebo F8 módu

1. counter mód E(k, IV) || E(k, IV + 1 mod 2^128) || E(k, IV + 2 mod 2^128)...
   IV = (k_s * 2^16) XOR (SSRC * 2^64) XOR (i * 2^16)
   povinný pro šifrování a vyvozování klíčů relace z master key

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

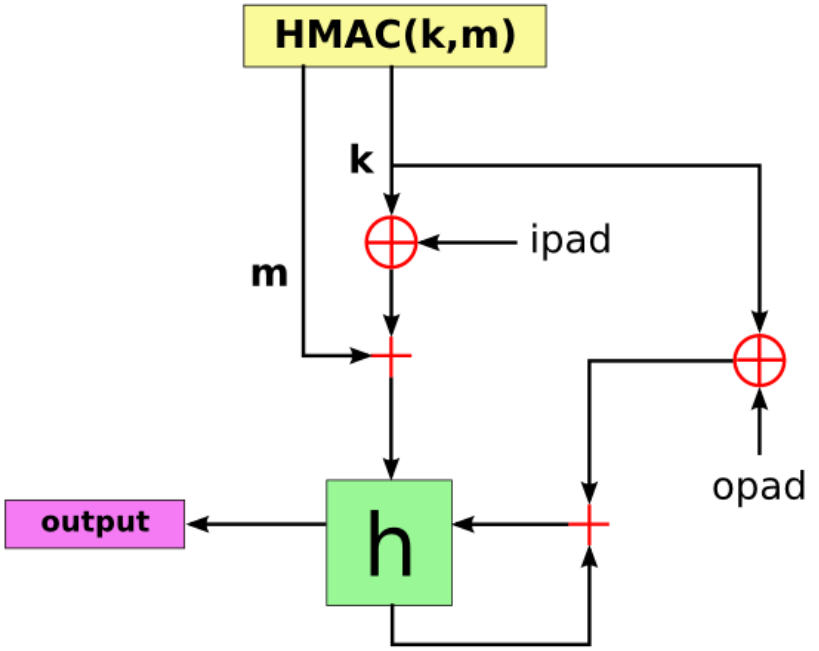
Jde o hash funkci nad zprávou *m* kombinovanou s klíčem *k*

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

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

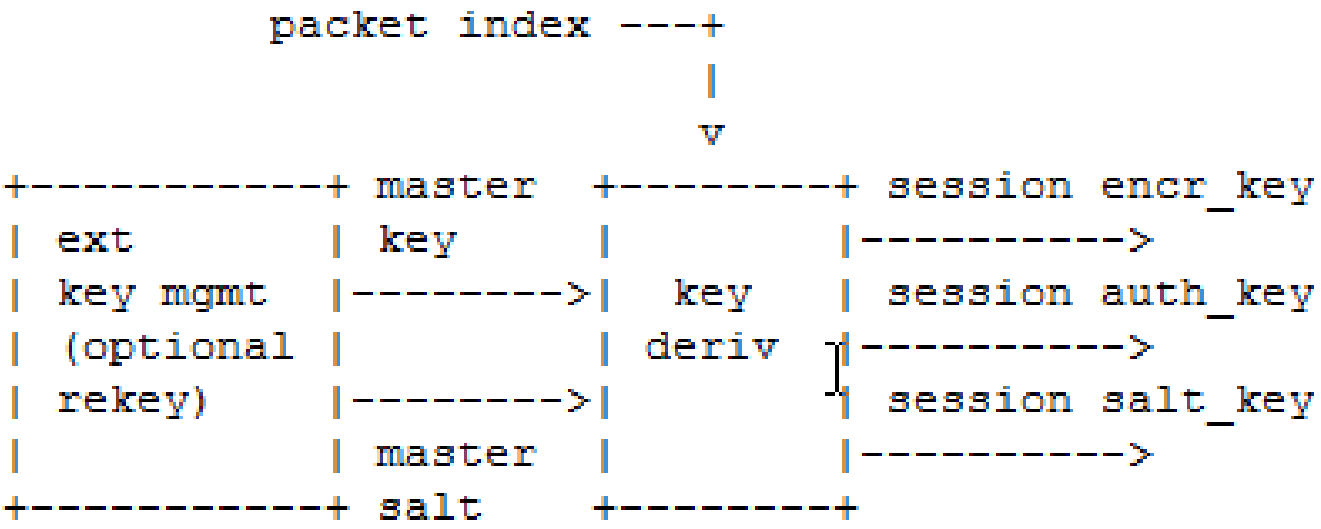
Je popsána v RFC 2104
V TLS a IP Sec se používá
HMAC-MD5 i HMAC-SHA-1,
V SRTP jen HMAC-SHA-1

2006: Úspěšný plný útok na MD4
a částečný na MD5



Povinná je i implementace režimu
nulové šifry (zajišťují se alespoň tyto vlastnosti)

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.

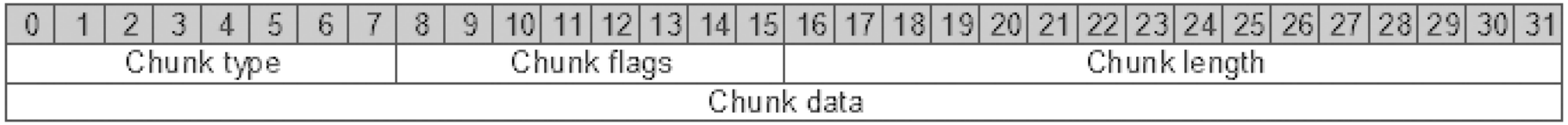
Příklady řešení bezpečnosti RTP u softphonů

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

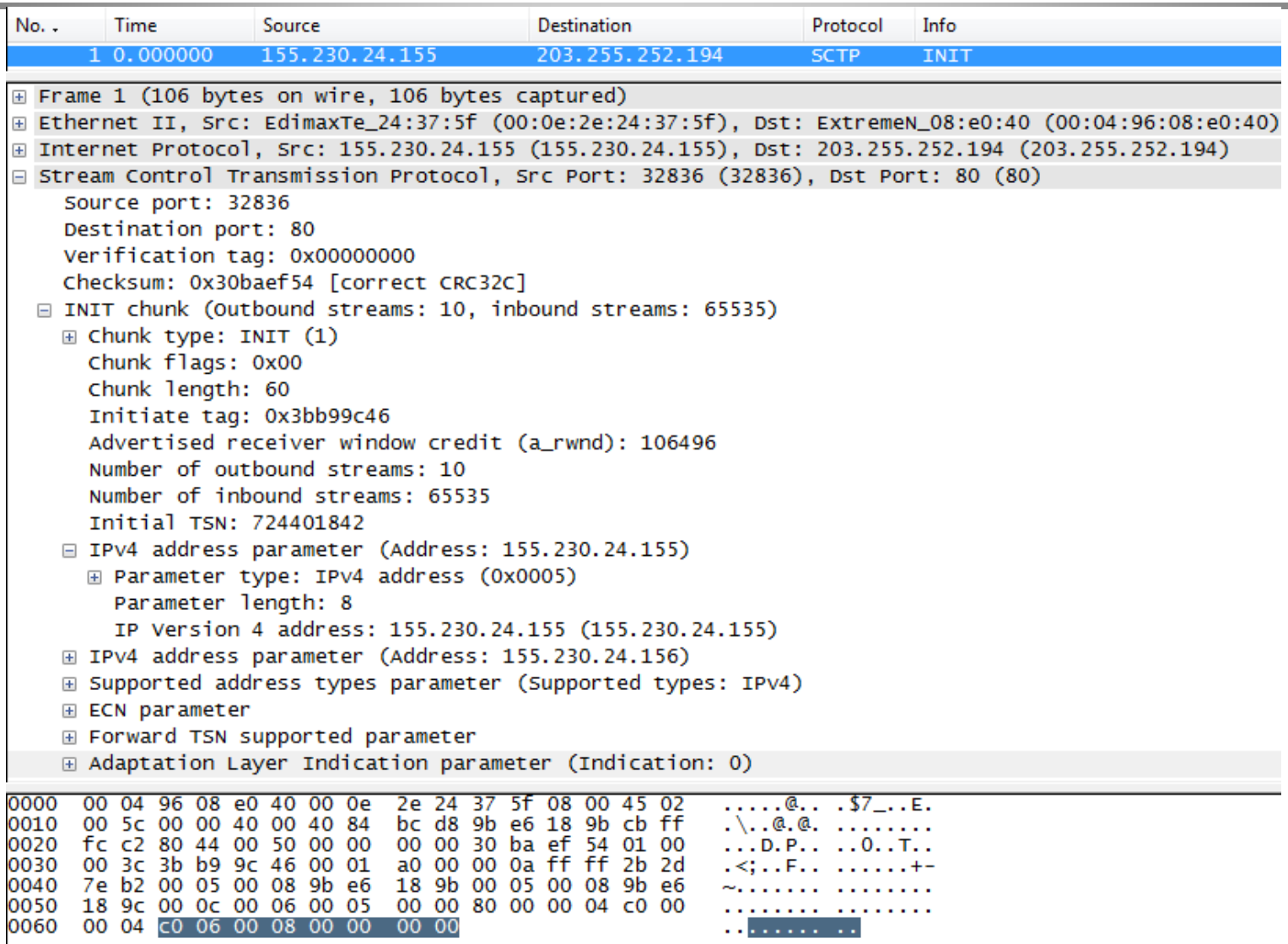
4. Protokol SCTP

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)



Zdroje

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