Real time and comunications

COMMUNICATION PROTOCOLS AND NETWORK SECURITY

CONTENT

- Examples of use and data capture
- Network time
- Basic protocol for real-time traffic
- Protocol for the management of data flow
- Secure version of the protocol

EXAMPLES OF USE

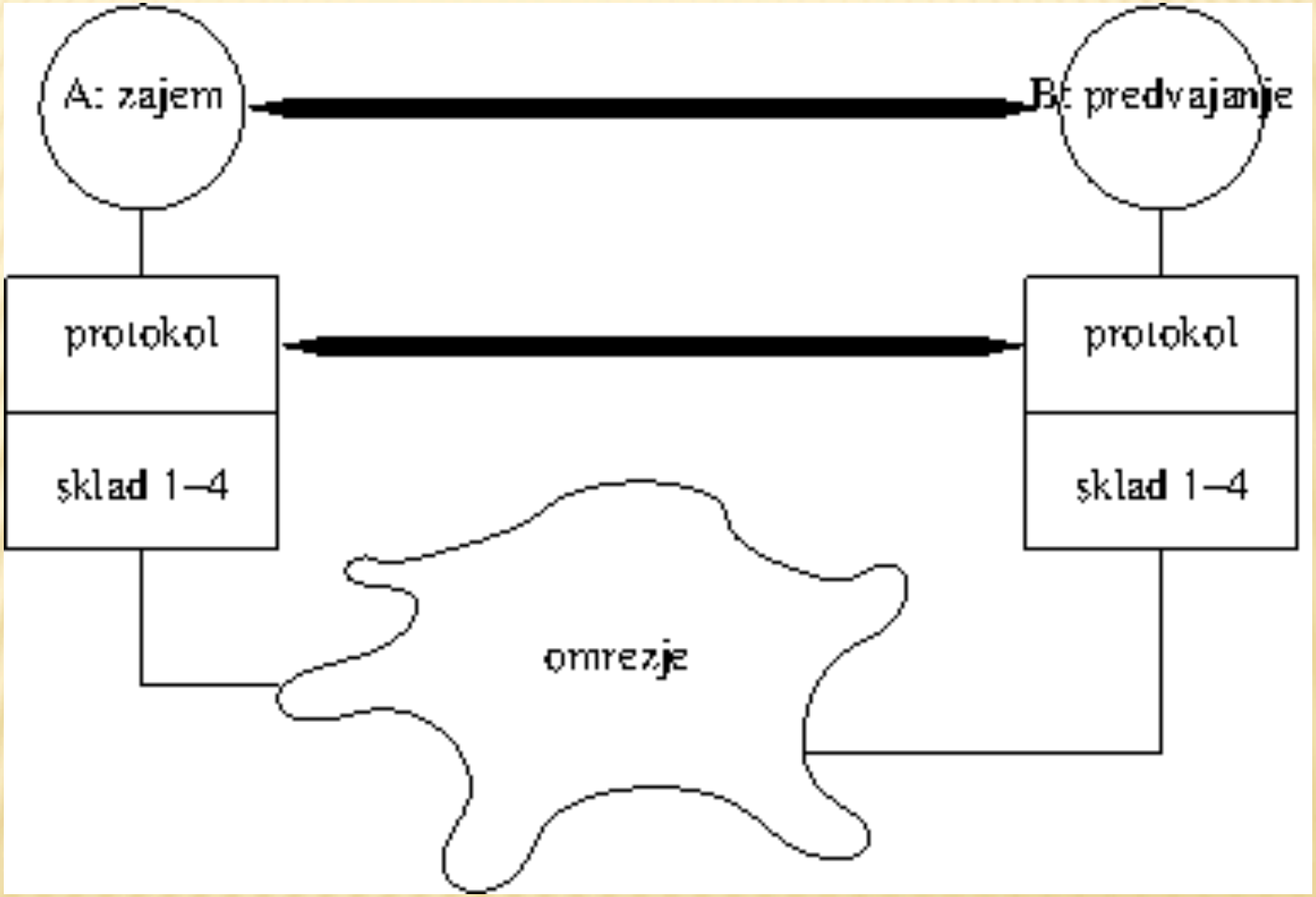
- What is real-time
  - (time of arrival, time of implementation, the time required to implement, deadline for completion of performance)
  - Systems *hard* and *soft real time*
  - Challenge: Do normal opperating systems FreeBSD, Linux in MS Windows allow work in real time?

    Justify the answer.

EXAMPLES OF USE

- We will not deal with such a definition of the real-time.
- Scenarios:
  - We have page A and page B, and between the two, we have the network.
  - On page A we have differen events, that caputre themselves and report to page B through the network.
  - Observer, observing events on page B, must have trust in what he sees.
- We can transfere the content of the events, the problem is to transfer the effect of time between the events.

SCENARIOS


A: zajem
B: predvajanje
protokol
protokol
sklad 1–4
sklad 1–4
omrezje

EXAMPLES OF USE

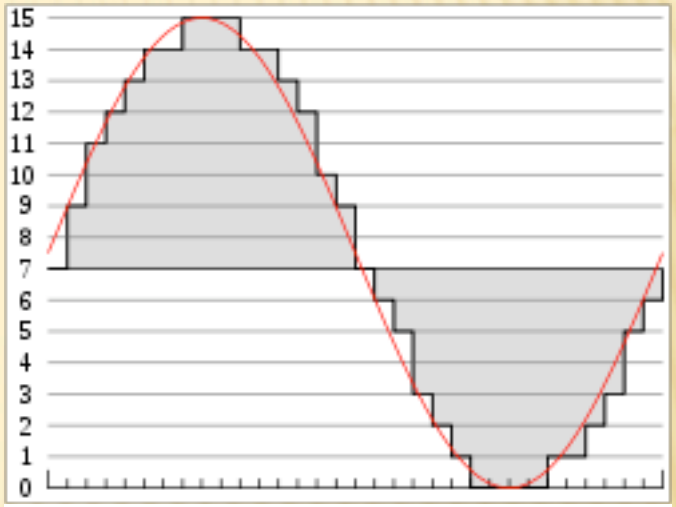
- One way communication:
  - Presentation of slides, …
  - Playing sound (remoteCD) and playing movie(remote VCR)
  - Combining picture and sound at transfer.
  - Broadcasting radio or TV program.
- Two way communication
  - Chatting via internet(VoIP)
  - video telephony

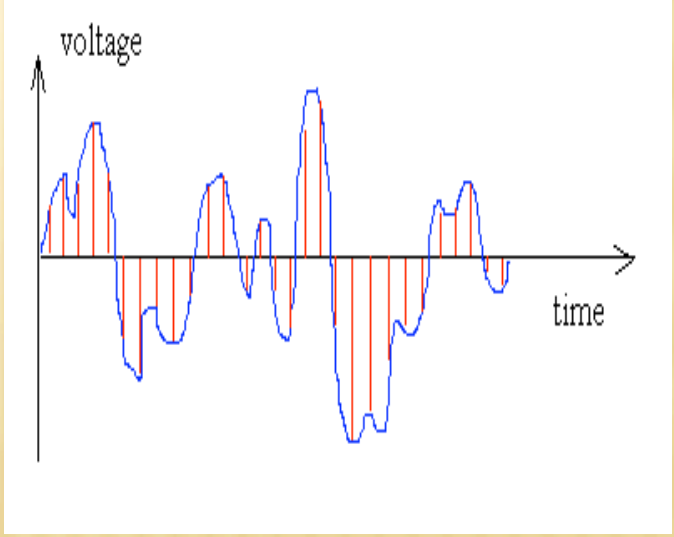
CAPTURE OF DATA – SOUND

- Sound is an analog phenomenon of changing air pressure, perceived by the human ear.
- Before digital:
  - We changed analog audio signal via microphone into an analog electrical signal.
  - Electrical signal was then used for the production of sound through the speaker.

CAPTURE OF DATA – SOUND

- Digital:
  - We still capture sound but only in discreete moments – We capture deviation (amplitude, intensity, energy)
  - Amplitude is then transformed into n-bit number
  - Challenge: find the audacity program, install it, and then capture and process the sound.



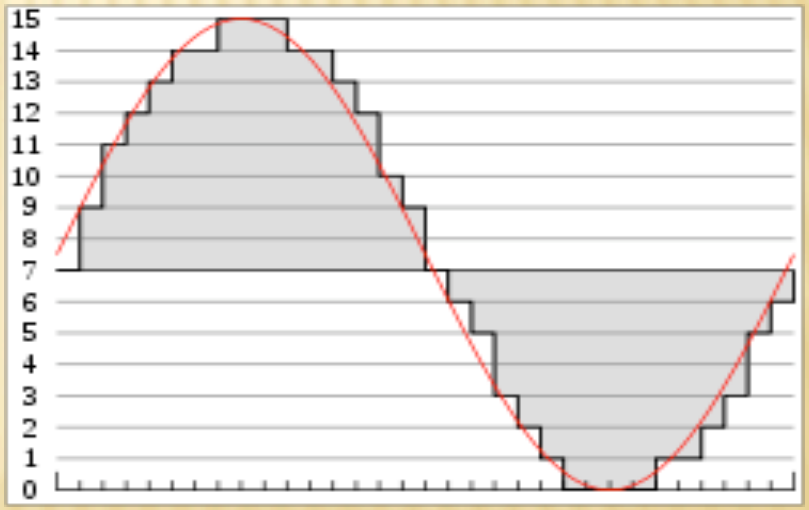


CAPTURE OF DATA – SOUND

- Sound, of course, is not a simple sine phenomenon, but it is a linear combination of multiple sinusoidal signals: the sum of

$$a_k \sin(k\omega)$$

- Digital capture of signal must notloose (to much) singal information.



CAPTURE OF DATA – SOUND

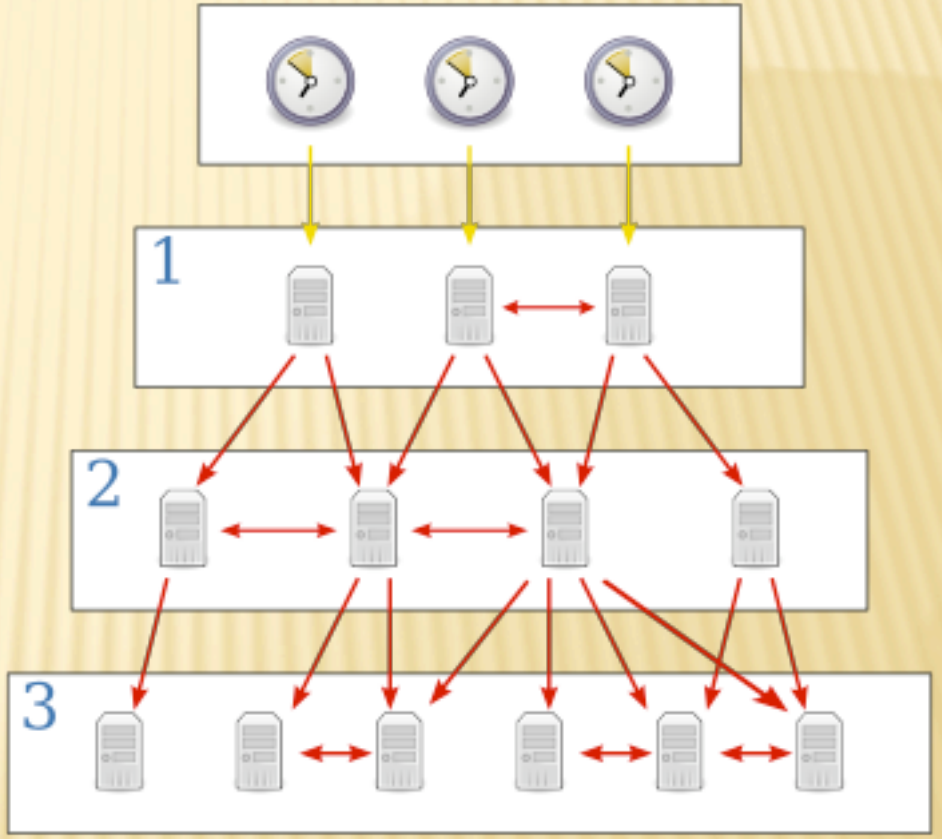
- Sampling problem(Nyquist-ova frequency)
  - Challenge: Why are cars rotating wheels in the movies go sometimes back, while car or wagon is moving forward?
- The human ear perceives frequencies of approximately 20Hz do 22kHz
  - Challenge: What is the sampling frequency for wav files?
- The human ear can not detect certain combinations of signals
  - mp3 compressing
  - Challenge: Search program with the command line interface for mp3 compression for Unix and install it?

CAPTURE OF DATA – PICTURE

- Problem of digitizing one picture and then the movie.
- Digitizing picture:
  - each point on the screen has a value that is three dimensional vector
  - Challenge: Which can be the three dimenssions of vector (more options)? What do they mean?
  - Challenge: Check different standards like jpg, gif, pgn, and comment them. How is the conversion between them?
- So digitized image represents an example of one amplitude of sound
- The problem of time digitizing equals / is the same as it is in sound
  - Human eye can sense movement if he receives at least between 23 to 25 pictures of the second
  - Challenge: What are the standard sampling speeds? Are there more, where are they beeing used? Why are they different?
  - Challenge: check out the different standards of movie records and comment them. How is the conversion between them?

NETWORK TIME

- Sometimes we must synchronise time between multiple remote systems.
- Problem of data transfer delay.
- You can use multiple systems simultaneously.



PROTOCOL NTP

- Defined in RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*
  - *Mandatory: Find it on the internet and read it – literature!*
  - Challenge: Find other RFC documents, dealing with ntp and check, what is written in them. Find description of Marzullov algorythm.

SOFTWARE

- On FreeBSD: ntpd
- Configuration in /etc/ntp.conf

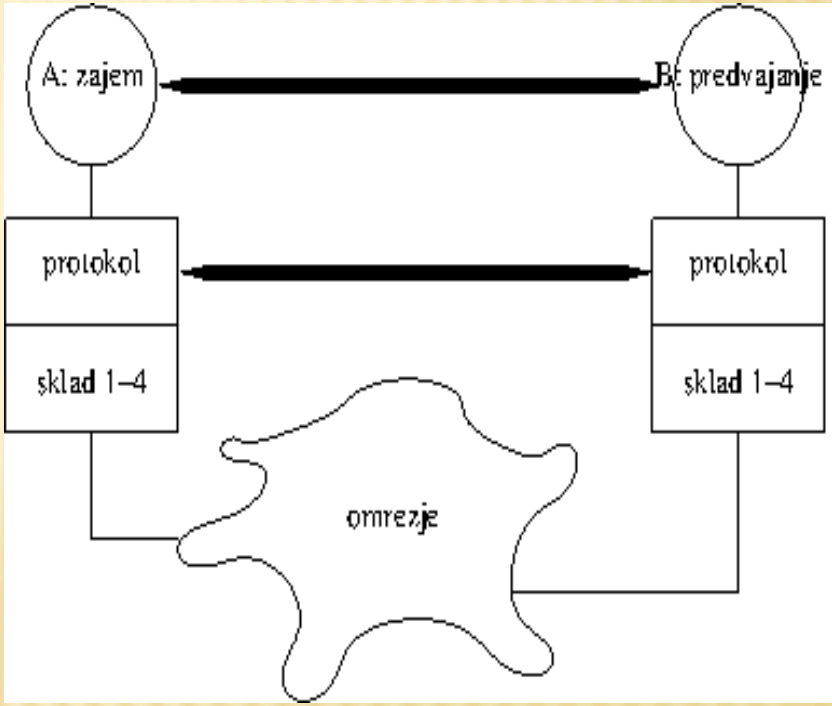
```
server ntplocal.example.com prefer
server timeserver.example.org
server ntp2a.example.net

driftfile /var/db/ntp.drift
```

- Challenge: Find servers in Slovenia?

- Challenge: find manual and run client. Manually change the time and watch what will happen.
- Challenge: How to use ntpd on OS Windows?

TRANSFER FROM A TO B

- Possible solutions:
  - A records the events and time stamps and sends the file to B.
  - A, when he records the event, he puts stamp on the record and sends it to B.
  - Somethin in between.
- Main problem is network.



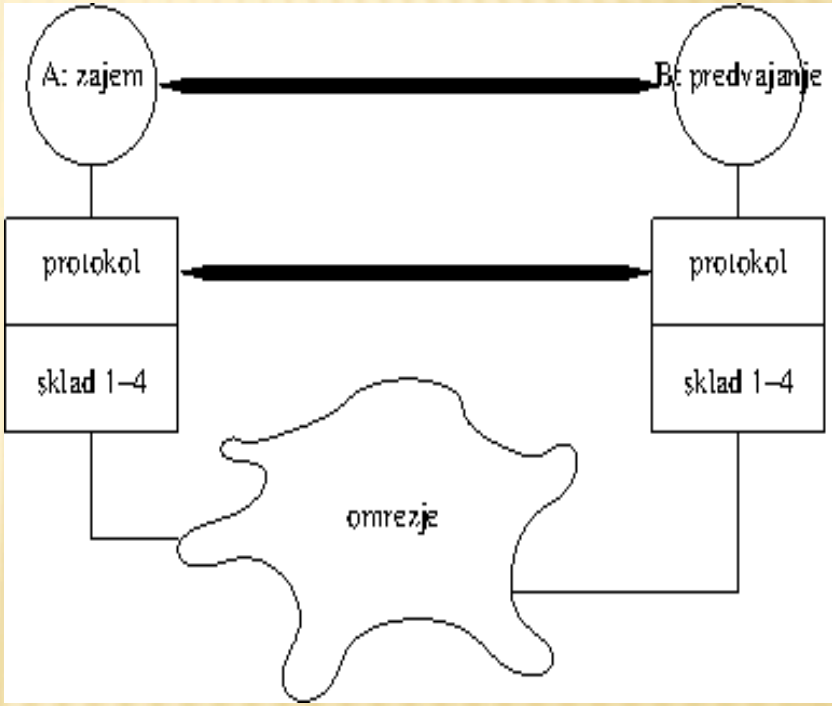
THE IMPACT OF NETWORK

- Our network is packet based
  - Each packet can travel on different route
  - Each packet can arrive in different time
    - latency problem– is not so big in one-way traffic
  - Some packets can get lost

- Two problems:
  - What to do with lost packages
    - Network transport layer or aplication layer handles lost packets
  - What to do with uneven packet arrival
    - Some packets can simply be late

THE IMPACT OF NETWORK

- Two problems
  - What to do with lost packages.
  - What to do with uneven packet arrival
- Solution:
  - Late packages adress as lost
  - Protocol should provide a time balance
  - Application should arrange packet loss



PROTOCOL RTP

- Defined in RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*
  - *Mandatory: Find it on the internet and read it – literature!*
  - Challenge: Find other RFC documents, dealing with tftp and check, what is written in them.
- Basic funcionality:
  - ensures the correct sequence of the packets
  - concern for time stamp events

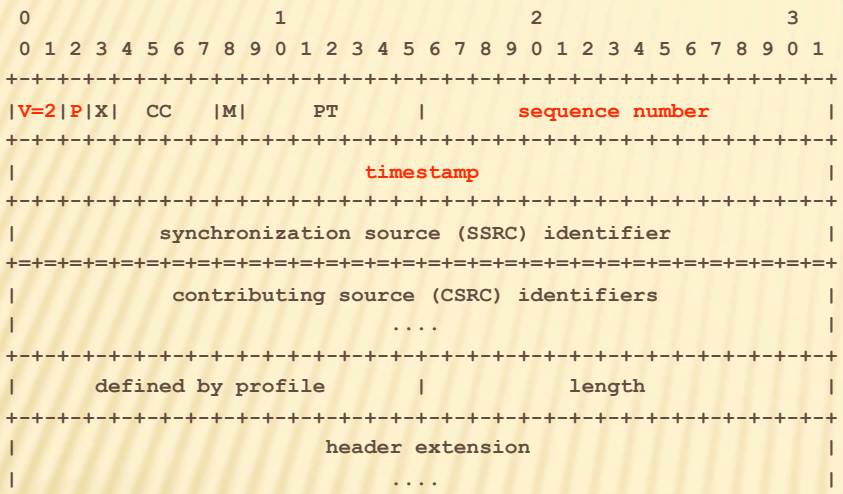
PROTOCOL RTP

- Additional functionality:
  - On connection can have multiple data flows (sources of events): soud left, sound right, ...; picture from right eye, picture from left eye; subtitles, ...
  - Identificator of source / session and his synchronization source
  - Special element– mixer, that can combine more sessions to one.
  - In combined session, whom the package belong to.

RTP – SOME DETAILS

- rtp is transport protocol, that serves for data transfer.
  - does not include commands to initiate connections and maintain connections
- rtp protocol allows application to transport special data (for playing sound, music, ...) – profile
- For control of RTP protocol, it uses RTCP protocol(*RTP Control Protocol*) – same RFC
- rtp uses on transport layer connectionless mode – UDP protocol

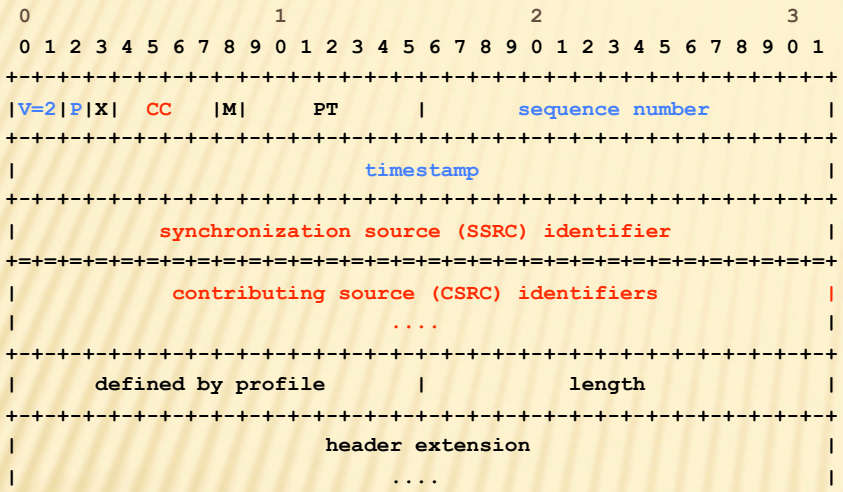
RTP – PACKAGE FORM



Basis:

- V – version; 2
- P – *padding*
- sequence number – sequencing packages sent in flow.
- timestamp – Time stamp of the event.

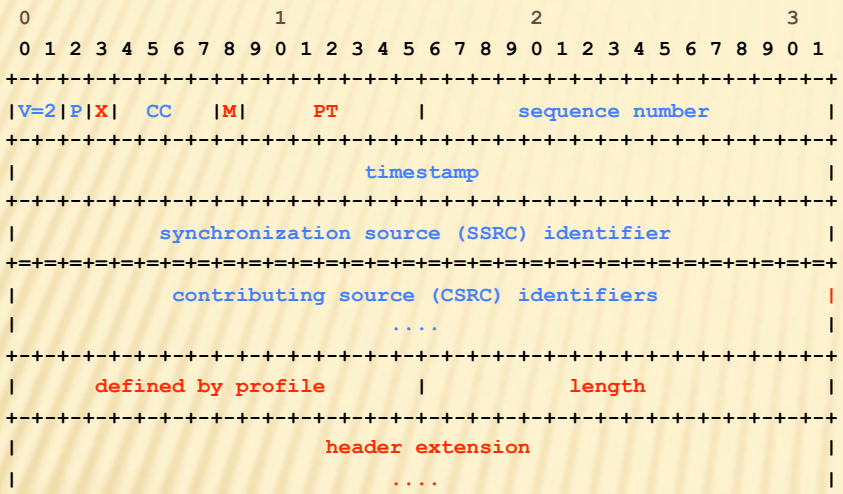
RTP – PACKAGE FORM



Additional functionalities:

- SSRC –*Synchronization source*
- CC – number of mixed sources
- CSRC –*Contributing source*

RTP – PACKAGE FORM



Higher protocol/application:

- PT – protocol identification
- M – special bit for needs of protocol
- X – presence of header extension
- Last part of header extension
- Challange: Find RFC for protocol description (modes of transport), that use RTP and compare them (sound, movie, text!, ...)

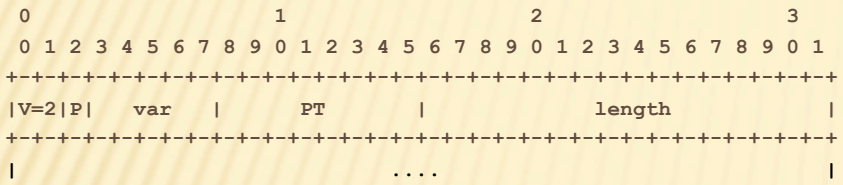
THE CONTROL PROTOCOL RTCP

- Compare analogy between IP and IPCP
- Has four funcions:
  1. Reports on the quality of traffic(*RR*: *receiver report* and *SR*: *sender report*
  2. Extra description of event flow(*SDES*: *Source description items*)
  3. responsible for the proper density messaging on quality of transport
  4. Can transport other application packets (*APP: Application-specific functions*)

THE CONTROL PROTOCOL RTCP

- For use of RTCP we must maintain stable bandwidth
- If there are a lot of partys (*multicast*), then the density of reporting is smaller
- Challenge: What kind of data can RTCP send about event source? What is CNAME?
- Challenge: How does traffic quality report look like?What kind of data does he have?

RTCP – PACKAGE FORM



- Challenge: What is the value of var in SR command and what does it mean?
- Challenge: Peter Zmeda has found out that there is connection between RTP, freebsd and mplayer? What kind? Install mplayer and try it.

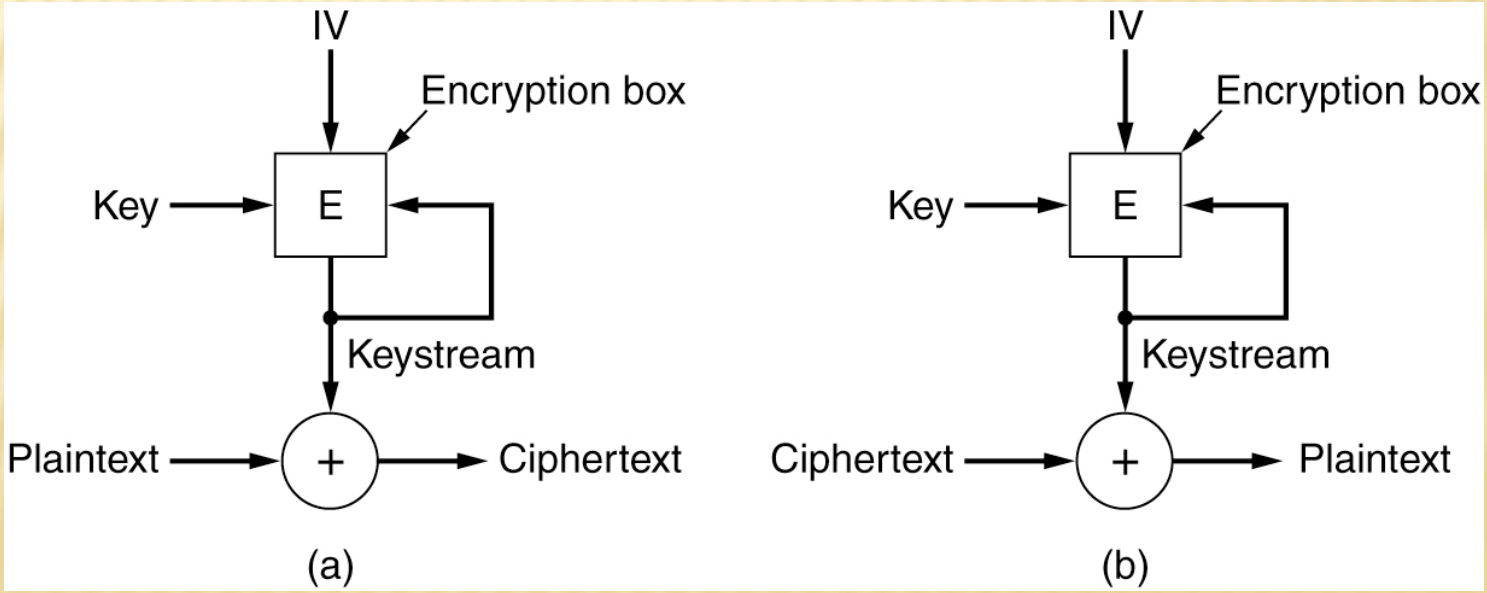
- V – verison; 2
- P – *padding*
- PT – command: SR, RR, SDES, BYE, APP
- var – different values, depends on command.

SAFE RTP

- RTP protocol uses UDP transfer, who do not have sll layer.
- So we must implement saftey in RTP by our self
- We exchange keys, but packages get lost
- Different way of encryption: encryption with cypher flow

ENCRYPTION WITH CYPHER FLOW

- Starting values(IV) is know to both sides
- Both sides also know the key
- Each packed is separately encrypted
- + is simple xor or something similar
- If packet is lost, we swirl emty E



PROTOCOL SRTP

- Defined in RFC 3711, The Secure Real-time Transport Protocol (SRTP)
  - *Mandatory: Find it on the internet and read it – literature!*
  - Challenge: Find other RFC documents, dealing with srtp and check, what is written in them.
- based on RTP
- Security added with cyphering a flow of cyphres
- Challenge: How do they exchange keys?
- Challenge: In RFC there is mention about HMAC function(RFC 2104); how does it work and how we use it? What is f8, which is mentioned in standard?

USERS OF RTP PROTOCOL

- Event Logging in (distant) laboratories (gridcc)

- IP telephony– SIP
- Remote VCR or VoD
  - Uses protocol RTSP

PROTOCOL RTSP

- Defined in RFC 2326, Real Time Streaming Protocol (RTSP)
  - *Mandatory: Find it on the internet and read it – literature!*
  - Challenge: Find other RFC documents, dealing with RTSP and check, what is written in them.
- Basic commands: set (*SETUP*), play and/or record(*PLAY*, *RECORD*), wait(*PAUSE*) and stop(*TEARDOWN*)
- additional commands for setting and reading parameters
- Example of use on websites:

prelep slovenski film

- ,, relative'' of protocol http: same structure of commands (MIME)
  - Challenge: on of fields, that client sets in server request is *transport*. How does it look like and what does it do?
  - Challenge: Where can we see connection between RTSP in RTP – for example in RTP we had in header SSRC field; does it exist in RTSP and if yes where is it and how does it look like?

SOFTWARE

- One of first opensource servers is Darwin
- What about the client?
  - Challenge: find server and install it on yourFreeBSD/ Linux system. Add a site that offers your movies.

CONCLUSION

- We looked at what really means “real time" and how to adjust time on your computer.
- We looked RTP/RTCP protocol and its safe version SRTP
- We looked the use of RTP protocol for VoD, that uses protocol RTSP

- Next time: *multicasting*

- Ufff, how does application handles lost packets(look at the tasks left to application)?