Stvarni čas in komunikacije

KOMUNIKACIJSKI PROTOKOLI IN OMREŽNA VARNOST

VSEBINA

- primeri rabe in zajem podatkov
- omrežni čas
- osnovni protokol za promet v stvarnem času
- protokol za upravljanje s tokom podatkov
- varna inačica protokola

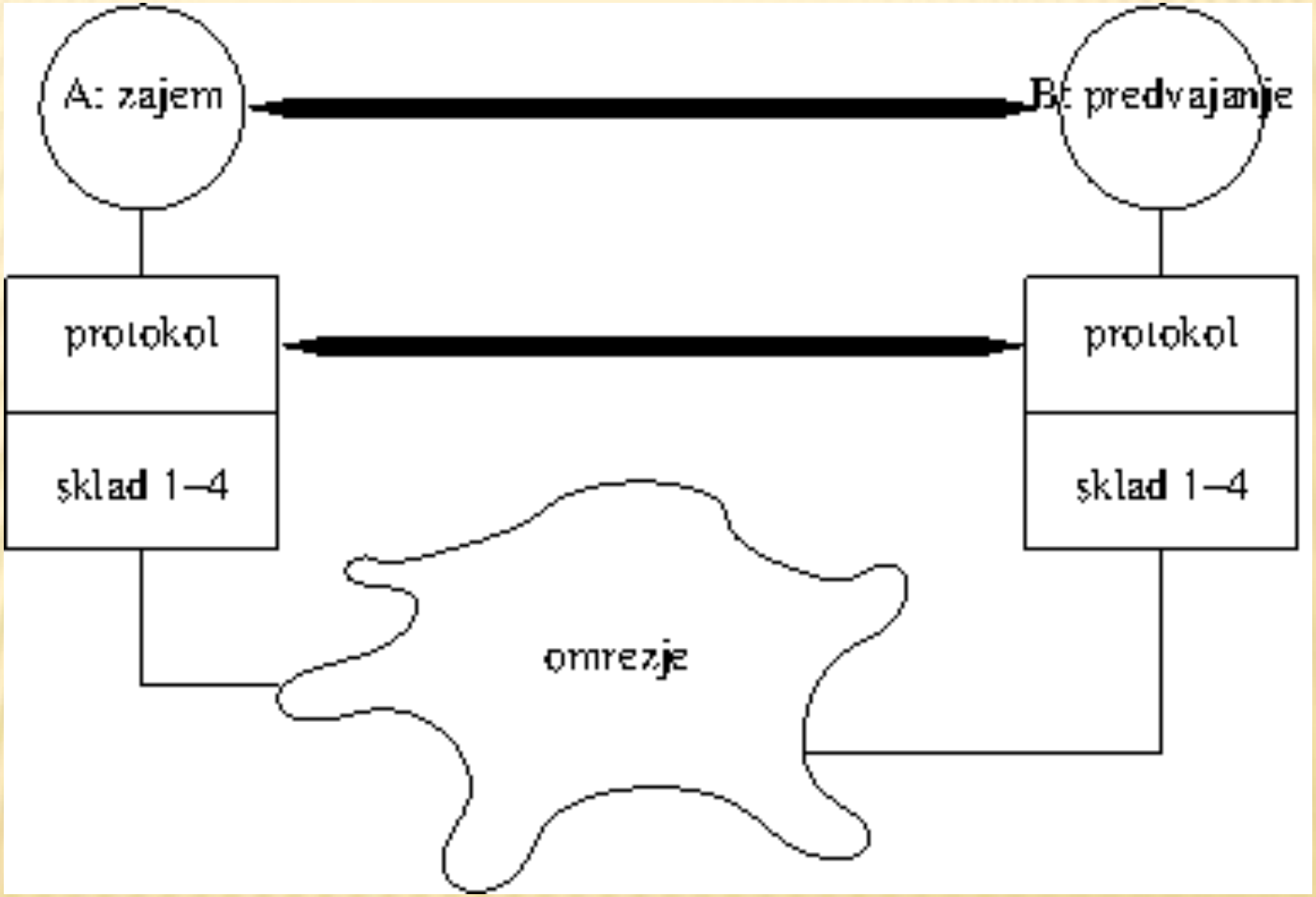
PRIMERI RABE

- kaj je stvarni čas (realni čas, *real-time*)
  - (čas dospetja, čas začetka izvajanja, potreben čas za izvajanje, rok zaključka izvajanja)
  - sistemi strogo in mehko v stvarnem času (*hard* in *soft real time*)
  - izziv: ali običajni operacijski sistemi FreeBSD, Linux in MS Windows omogočajo delo v stvarnem času? Utemeljite odgovor.

PRIMERI RABE

- mi se ne bomo ukvarjali s takšno definicijo stvarnega časa
- scenarij:
  - imamo stran A in stran B in med njima omrežje
  - na strani A se dogajajo različni dogodki, ki se zajemajo in o tem poroča strani B preko omrežja
  - opazovalec, ki opazuje dogodke na strani B, mora imeti čim bolj veren občutek opazovanja dogodkov
- vsebino dogodkov lahko nekako prenesemo, težava je prenos učinka časa med dogodkoma

SCENARIJ


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

PRIMERI RABE

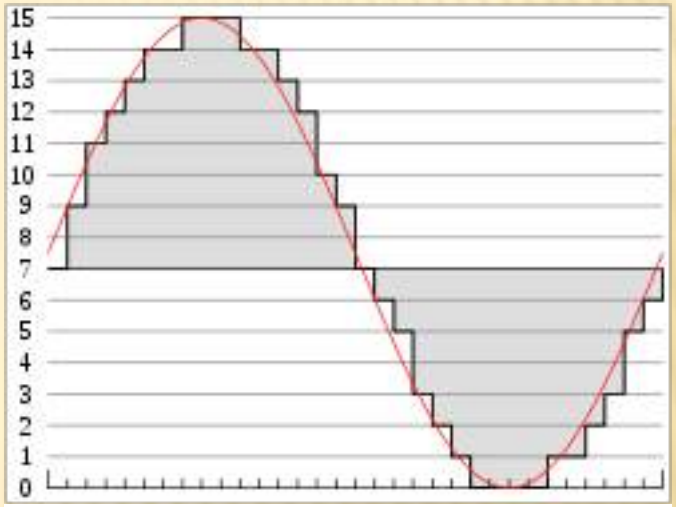
- Enosmerna komunikacija:
  - prikazovanje prosojnic, diapozitivov, ...
  - predvajanje zvoka (oddaljeni CD) in predvajanje filma (oddaljeni VCR)
  - združevanje slike in zvoka ob prenosu
  - predvajanje radijskega ali TV programa
- Dvosmerna komunikacija:
  - pogovor preko spleta (VoIP)
  - video telefonija

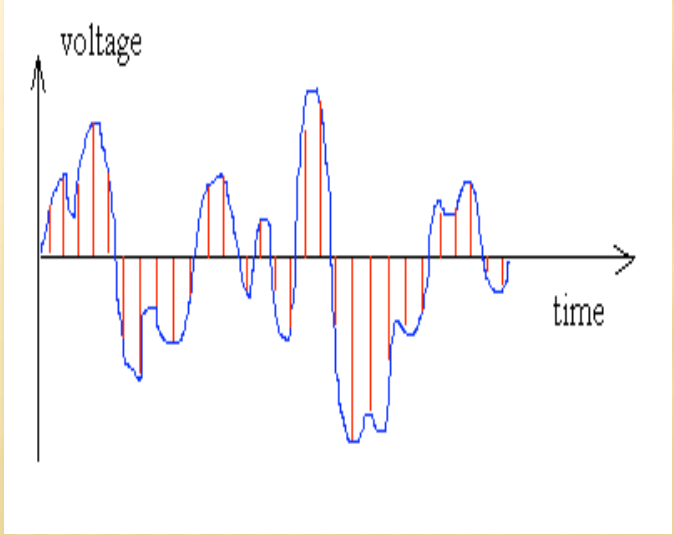
ZAJEM PODATKOV – ZVOK

- zvok je *analogen* pojav spreminjanja zračnega pritiska, ki ga zaznava (človeško) uho
- preddigitalno:
  - zajem zvoka smo preko mikrofona analogni signal spremenil v analogni električni signal
  - električni signal smo uporabili za proizvajanje zvoka preko zvočnika

ZAJEM PODATKOV – ZVOK

- digitalno:
  - še vedno zajamemo zvok, a le v diskretnih trenutkih – zajamemo odmik (amplitudo, jakost, energijo)
  - amplitudi pretvorimo v n-bitno številko
  - izziv: poiščite program audacity, ga namestite in v njem zajemite ter obdelajte zvok.



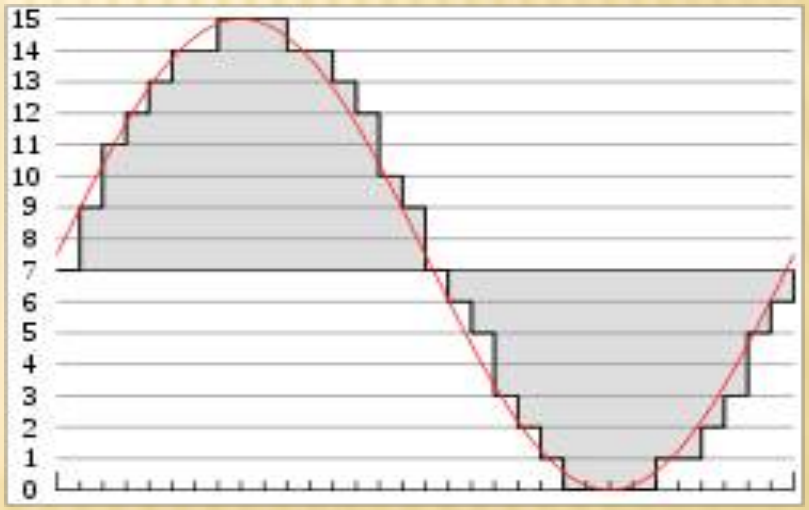


ZAJEM PODATKOV – ZVOK

- zvok seveda ni preprost sinusen pojav, ampak je linearna kombinacija večih sinusnih signalov: vsota

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

- digitalni zajem ne sme izgubiti (preveč) informacije o signalih



ZAJEM PODATKOV – ZVOK

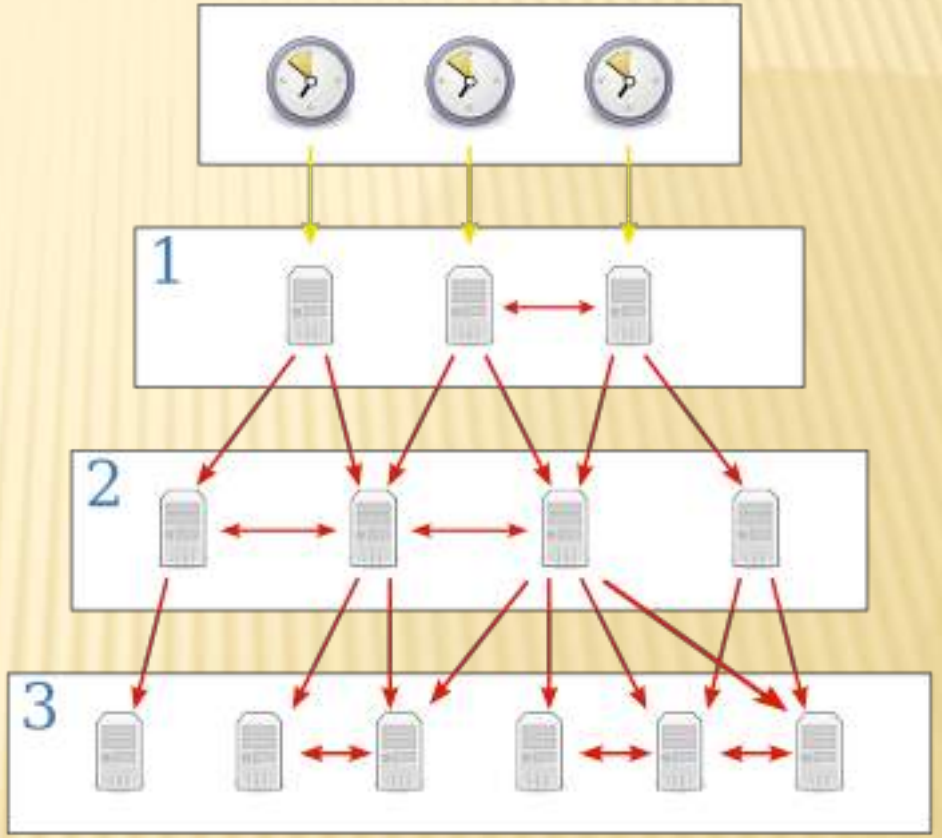
- problem vzorčenja (Nyquist-ova frekvenca)
  - izziv: zakaj se vrtijo v filmih kolesa včasih nazaj, avto ali voz pa se premika naprej?
- človeško uho zaznava frekvence približno od 20Hz do 22kHz
  - izziv: kakšna je frekvenca vzorčenja za wav datoteke?
- človeško uho ne zazna določene kombinacije signalov
  - mp3 stiskanje
  - izziv: poiščite program z vmesnikom z ukazne vrstice za mp3 stiskanje za Unix in ga namestite?

ZAJEM PODATKOV – SLIKA

- problem digitalizacije ene slike in nato filma
- digitalizacija slike:
  - vsaka točka na zaslonu ima svojo vrednost, ki je tri razsežnostni vektor
  - izziv: katere so lahko tri razsežnosti vektorja (več možnosti)? Kaj pomenijo?
  - izziv: preverite različne standarde kot so jpg, gif, pgn, bmp in jih komentirajte. Kako je s pretvorbo med njimi?
- tako digitalizirana slika predstavlja primer ene amplitude pri zvoku
- problem časovne digitalizacije je podoben / enak kot pri zvoku
  - človeško oko zazna neprekinjeno premikanje, če mu posredujemo vsaj med 23 do 25 slikic na sekundo
  - izziv: kakšne so standardne hitrosti vzorčenja? Jih je več in kje se uporabljajo? Zakaj so različne?
  - izziv: preverite različne standarde zapisov filma in jih komentirajte. Kako je s pretvorbo med njimi?

OMREŽNI ČAS

- včasih moramo uskladiti čas med večimi oddaljenimi sistemi
- problem zakasnitve prenosa podatka
- uporabimo lahko več sistemov hkrati



PROTOKOL NTP

- definiran v RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*
  - *obvezno: poiščite ga na spletu ter ga preberite – literatura!*
  - izziv: poiščite še ostale RFC dokumente, ki se ukvarjajo z ntp ter preverite, kaj piše v njih. Poiščite opis Marzullovega algoritma.

PROGRAMSKA OPREMA

- na FreeBSD: ntpd
- konfiguracija v /etc/ntp.conf

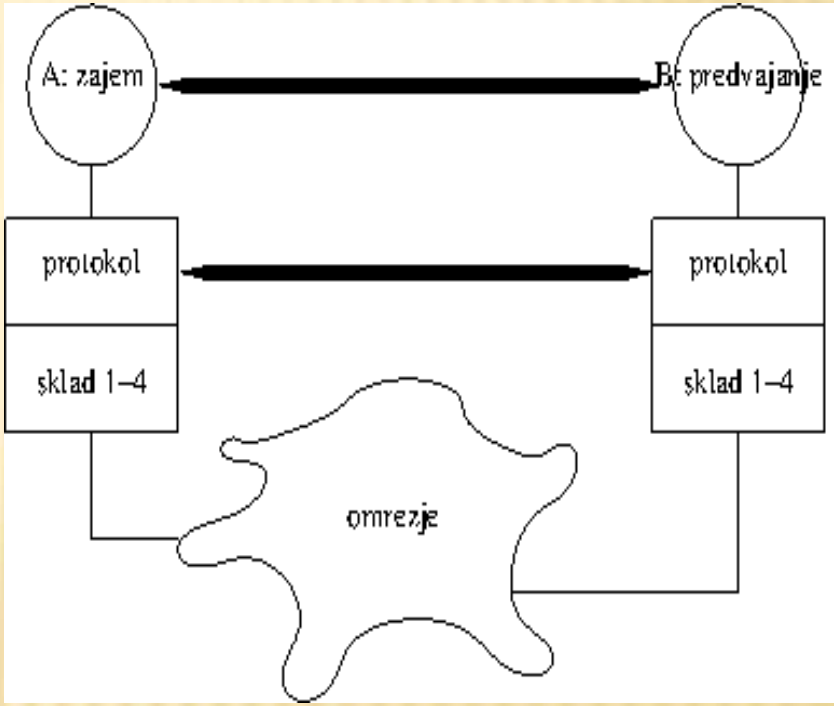
```
server ntplocal.example.com prefer
server timeserver.example.org
server ntp2a.example.net

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

- izziv: poiščite ntp strežnike v Sloveniji?

- izziv: poiščite priročnik ter poženite odjemalca. Ročno premaknite čas in opazujte, kaj se dogaja.
- izziv: kako uporabljati ntp na OS Windows?

PRENOS OD A DO B

- možne rešitve:
  - A posname dogodke in časovne značke in pošlje datoteko B
  - A, ko posname dogodek, ga opremi s časovno značko in ga takoj pošlje B
  - nekaj vmes
- osnovni vir težav je omrežje

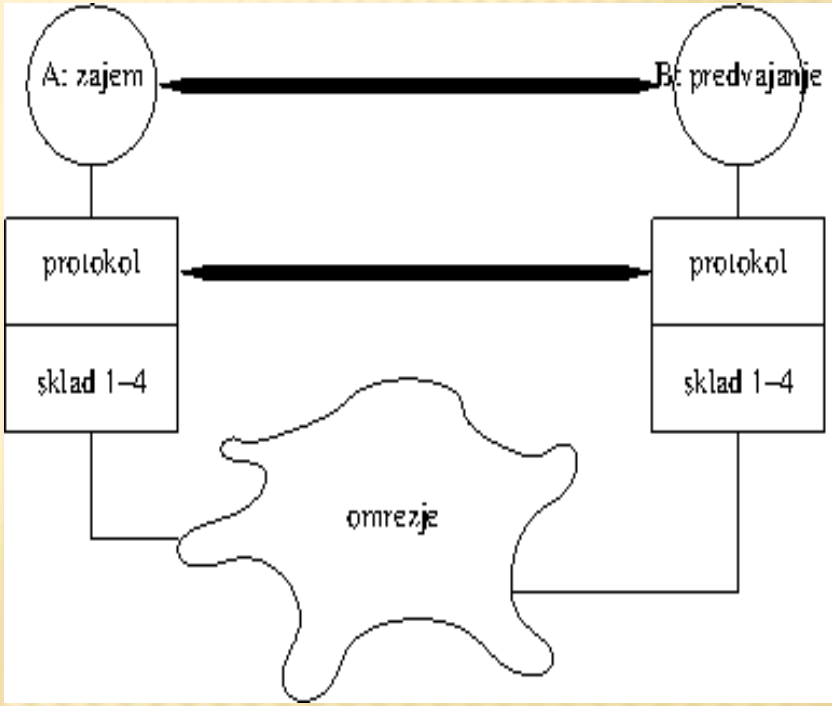


VPLIV OMREŽJA

- naše omrežje je paketno
  - vsak paket lahko potuje po drugi poti
  - vsak paket lahko potuje različno dolgo
    - problem latence – ni tako velik pri enosmernem prometu
  - nekateri paketi se lahko izgube
- dva problema:
  - kaj narediti z izgubljenimi paketi
    - povezavna prenosna plast ali aplikacija skrbi za izgubljeno
  - kaj narediti z neenakomerno prihajajočim paketi
    - nekateri paketi preprosto zamudijo

VPLIV OMREŽJA

- dva problema:
  - kaj narediti z izgubljenimi paketi
  - kaj narediti z neenakomerno prihajajočim paketi
- rešitev:
  - zamujene pakete obravnavati kot izgubljene
  - protokol naj poskrbi za časovno izravnavo
  - aplikacija naj poskrbi za izgubljene pakete



PROTOKOL RTP

- definiran v RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*
  - *obvezno: poiščite ga na spletu ter ga preberite – literatura!*
  - izziv: poiščite še ostale RFC dokumente, ki se ukvarjajo s tftp ter preverite, kaj piše v njih.
- osnovne funkcionalnosti:
  - skrbi za pravo zaporedje paketov
  - skrbi za časovne značke dogodkov

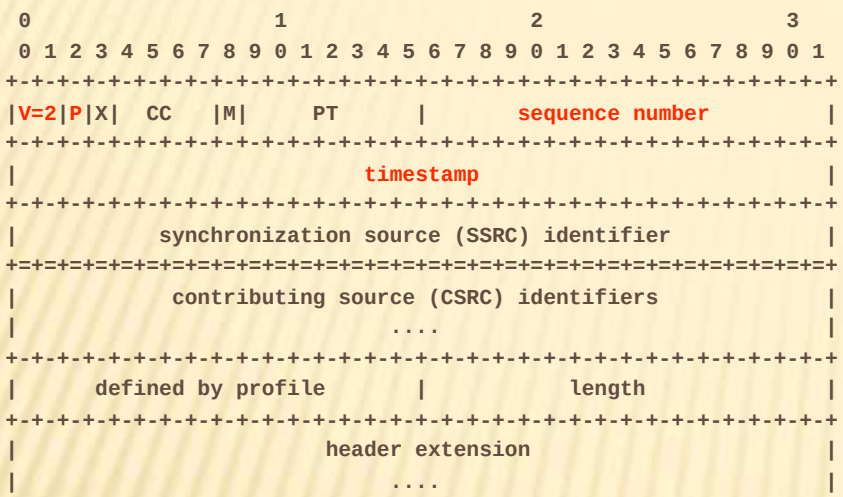
PROTOKOL RTP

- dodatne funkcionalnosti:
  - ena povezava lahko prenaša več podatkovnih tokov (virov dogodkov): zvok levi, zvok desni, ...; slika desnega očesa, slika levega očesa; podnapisi, ...
  - identifikator vira / seje in njegov sinhronizacijski vir
  - poseben element – mešalec (*mixer*), ki lahko združuje več sej v eno sejo
  - v združeni seji, komu v resnici pripada poslani paket

RTP – NEKAJ PODROBNOSTI

- rtp protokol je prenosni protokol, ki služi prenosu podatkov
  - ne vključuje ukazov za začetek povezave in vzdrževanje povezave
- rtp protokol omogoča aplikacijam prenos posebnih podatkov (za predvajanje zvoka, filma, ...) – profil
- za nadzor delovanja rtp protokola uporablja protokol rtcp (*RTP Control Protocol*) – isti RFC
- rtp na prenosni plasti uporablja nepovezavni način – UDP protokol

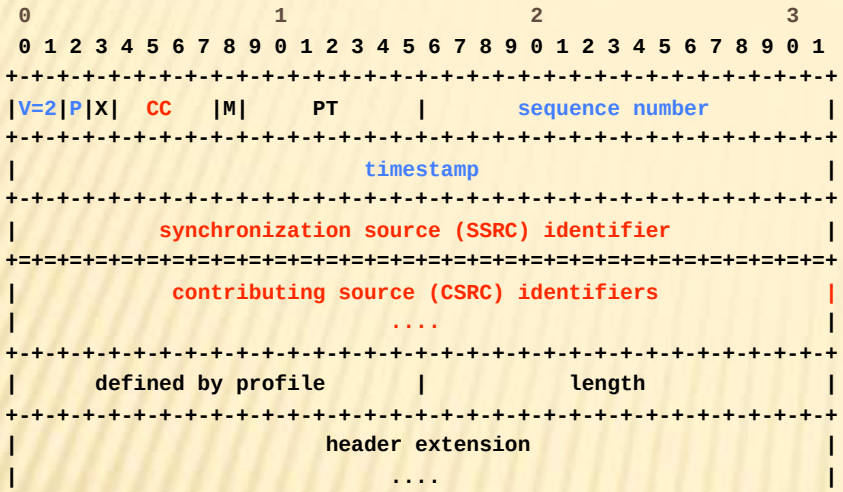
RTP – OBLIKA PAKETA



Osnova:

- V – verzija; 2
- P – zapolnitev (*padding*)
- sequence number – številčenje paketov poslanih v toku
- timestamp – časovna značka dogodka

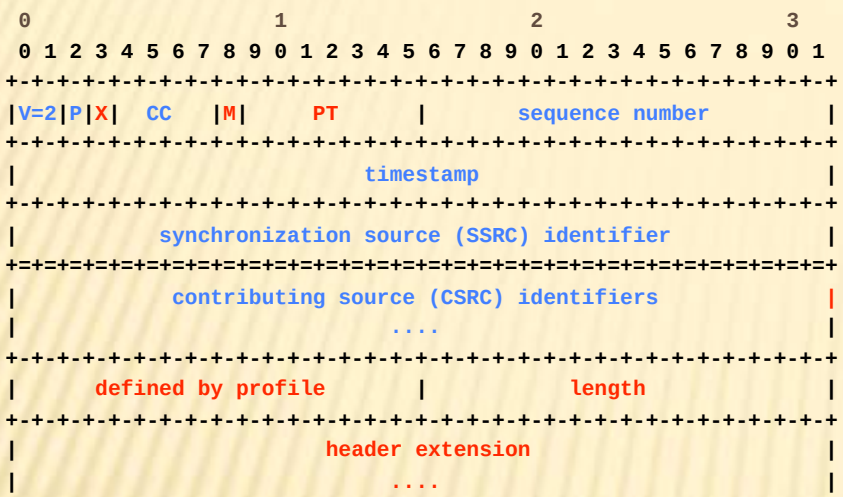
RTP – OBLIKA PAKETA



dodatne funkcionalnosti:

- SSRC – identifikator vira (*Synchronization source*)
- CC – število mešanih virov
- CSRC – identifikatorji mešanih virov (*Contributing source*)

RTP – OBLIKA PAKETA



višji protokol/aplikacija:

- PT – identifikacija protokola
- M – poseben bit za potrebe protokola
- X – ali je prisotna razširitev glave
- zadnji del je razširitev glave
- izziv: poiščite RFCje za opis posameznih protokolov (vrst prometa), ki uporabljajo RTP in jih primerjajte (npr. zvok, film, besedilo!, ...)

NADZORNI PROTOKOL RTCP

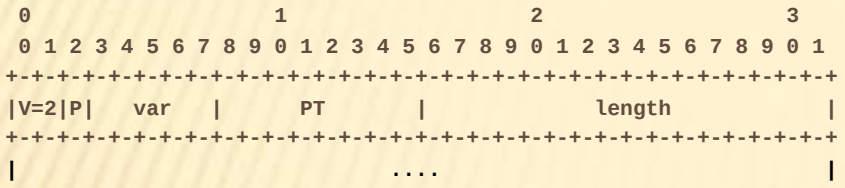
- primerjaj analogijo med IP in IPCP
- opravlja štiri funkcije:
  1. sporoča o kakovosti prenašanega prometa (*RR*: *receiver report* in *SR*: *sender report*
  2. dodaten opis vira toka dogodkov (*SDES*: *Source description items*)
  3. skrbi za pravilno gostoto pošiljanja sporočil o kakovosti prenosa
  4. prenaša lahko še dodatne podatke za potrebe aplikacije (*APP: Application-specific functions*)

NADZORNI PROTOKOL RTCP

- za potrebe RTCP je uprabljena stalna pasovna širina
- če je veliko sodelujočih strank (*multicast*), potem je gostota poročanja manjša

- izziv: kakšne vse podatke lahko prenaša RTCP o viru dogodkov? Kaj je to CNAME?
- izziv: kako izgleda poročilo o kakovosti prometa? Kakšne podatke vključuje?

RTCP – OBLIKA PAKETA



- izziv: kakšna je vrednost var pri SR ukazu in kaj pomeni?
- izziv: Peter Zmeda je med branjem spletnih strani opazil, da obstaja nekakšna povezava med besedami RTP, freebsd in mplayer? Kakšna? Namestite mplayer in preizkusite njegovo delovanje.

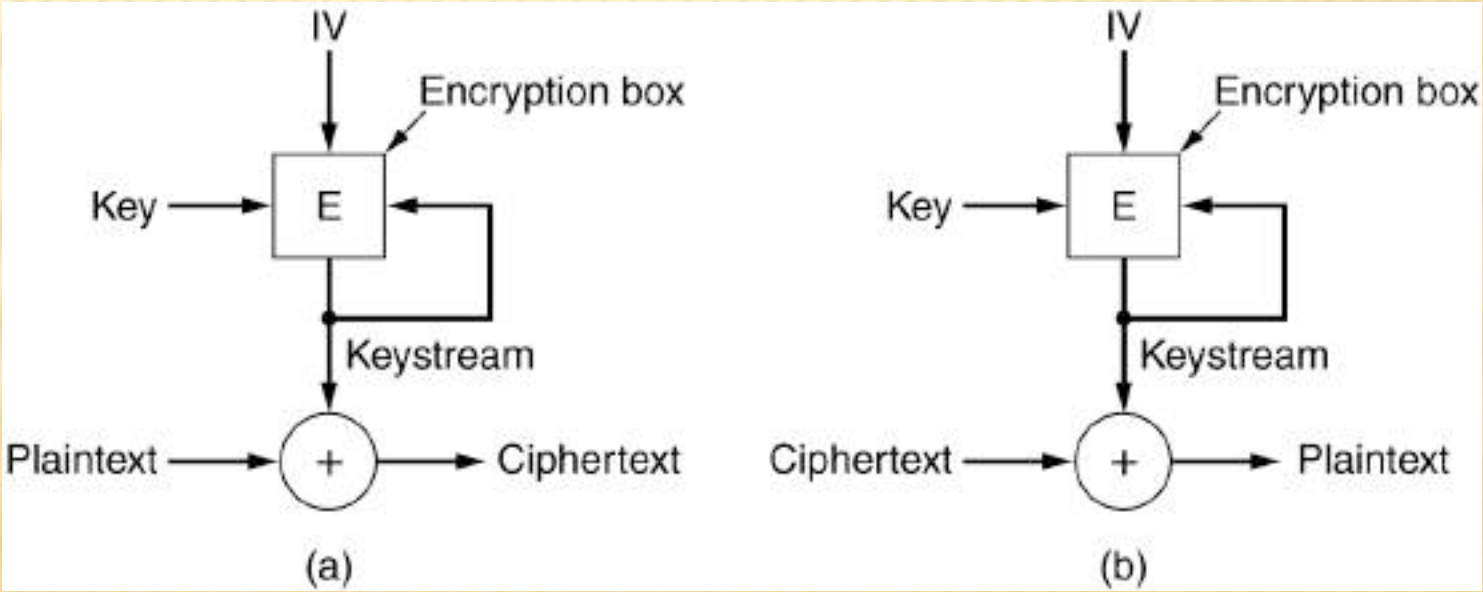
- V – verzija; 2
- P – zapolnitev (*padding*)
- PT – ukaz: SR, RR, SDES, BYE, APP
- var – različne vrednosti v odvisnosti od ukaza

VARNI RTP

- RTP protokol uporablja UDP prenos, ki nima ssl plasti
- zato moramo varnost za RTP dograditi sami
- nekako izmenjamo ključe, toda paketi se izgubljajo
- drugačen način kriptiranja: kriptiranje s tokom šifer

KRIPTIRANJE S TOKOM ŠIFER

- začetna vrednost (IV) je poznana obema stranema
- obema stranema je poznan tudi ključ
- vsak paket se ločeno zakriptira
- + je preprosti xor ali kakšen podoben algoritem
- če se paket izgubi, samo v prazno zavrtimo E



PROTOKOL SRTP

- definiran v RFC 3711, The Secure Real-time Transport Protocol (SRTP)
  - *obvezno: poiščite ga na spletu ter ga preberite – literatura!*
  - izziv: poiščite še ostale RFC dokumente, ki se ukvarjajo s srtp ter preverite, kaj piše v njih.
- zasnovan na RTP
- varnost dodana z kriptiranjem s tokom šifer
- izziv: kako si obe strani izmenjata ključe?
- izziv: v RFC je omenjena HMAC funkcija (tudi RFC 2104); kako deluje in kako se uporablja? Kaj je to f8, ki je omenjena v standardu?

UPORABNIKI PROTOKOLA RTP

- beleženje dogodkov v (oddaljenih) laboratorijih (gridcc)

- IP telefonija – SIP
- oddaljeni VCR ali VoD
  - uporablja protokol RTSP

PROTOKOL RTSP

- definiran v RFC 2326, Real Time Streaming Protocol (RTSP)
  - *obvezno: poiščite ga na spletu ter ga preberite – literatura!*
  - izziv: poiščite še ostale RFC dokumente, ki se ukvarjajo s RTSP ter preverite, kaj piše v njih.
- osnovni ukazi: nastavi (*SETUP*), igraj in/ali snemaj (*PLAY*, *RECORD*), počakaj (*PAUSE*) in zaključi (*TEARDOWN*)
- še dodatni ukazi za nastavljanje in branje parametrov
- primer uporabe na spletnih straneh:

prelep slovenski film

- ,,sorodnik'' protokola http: podobna struktura ukazov (MIME)
  - izziv: eno od polj, ki jih odjemalec nastavi v zahtevi strežniku je *transport*. Kako izgleda, kaj pomeni in čemu služi?
  - izziv: kje se vidi povezava med RTSP in RTP – na primer pri RTP smo imeli v glavi SSRC polje; ali obstaja tudi pri RTSP in če da, kje ter kako izgleda?

PROGRAMSKA OPREMA

- eden prvih odprtokodnih strežnikov je Darwin
- kaj pa odjemalec?
  - izziv: poiščite strežnik in si ga namestite na vašem FreeBSD/Linux sistemu. Dodajte spletno stran za ponudbo filmov iz vaše filmoteke.

ZAKLJUČEK

- ogledali smo si, kaj to pravzaprav pomeni ,,stvarni čas'' in kako nastavljamo čas na svojem računalniku
- kaj je to dogodek in kaj praktično pomeni prenos podatkov o dogodkih v stvarnem času
- spoznali smo RTP/RTCP protokol ter njegovo varno inačico SRTP
- ogledali smo si še uporabo RTP protokola za primer VoD, ki uporablja protokol RTSP

- Naslednjič: razpošiljanje (*multicasting*)

- Uh, kako pa aplikacija rokuje z izgubljenimi paketi (glej naloge prepuščene aplikaciji)?