Računalniške komunikacije

Transportna plast

Jurij Mihelič, UniLj, PeF

Vsebina

Plast	Podatkovna enota	Opis
aplikacijska	sporočilo	Visoko nivojski API.
predstavitvena		Predstavitev podatkov, kompresija, enkripcija/dekripcija.
sejna		Upravljanje sej (dvosmerna izmenjava informacij).
transportna	segment	Povezave med vozlišči, zanesljivost.
omrežna	datagram	Prenos med več vozlišči v omrežju, logično naslavljanje.
povezavna	okvir	Prenos okvirjev med dvema omrežnima napravama, povezanima s fizično plastjo, fizično naslavljanje.
fizična	bit	Prenos toka bitov po prenosnem mediju.

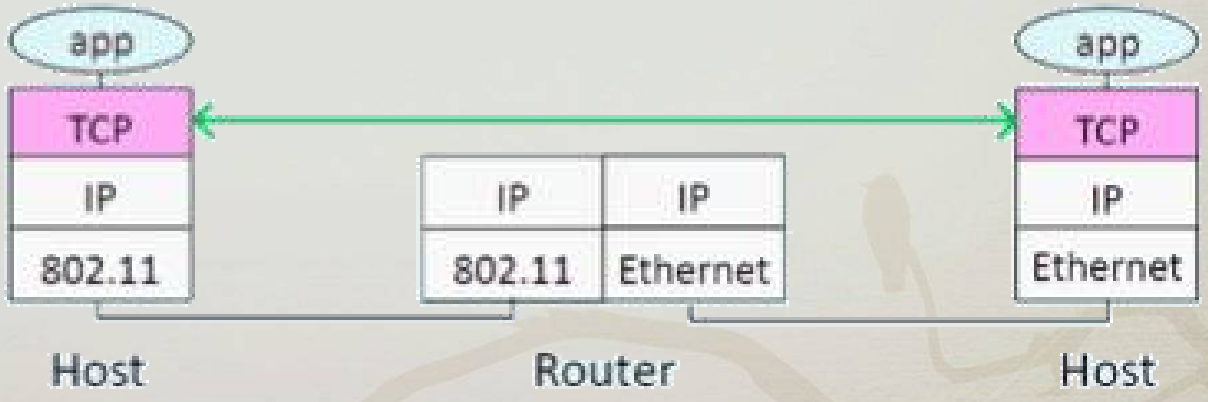
Vsebina

- Transportna plast
  - horizontalna komunikacija, naslavljanje procesov
  - vertikalna komunikacija, vtičnice
- UDP
- TCP

Transportna plast

- Storitve
  - povezovanje oddaljenih **procesov**
  - multipleksiranje / demultipleksiranje
  - zanesljiv prenos podatkov
  - nadzor pretoka
  - …

Omrežna plast povezuje končne sisteme

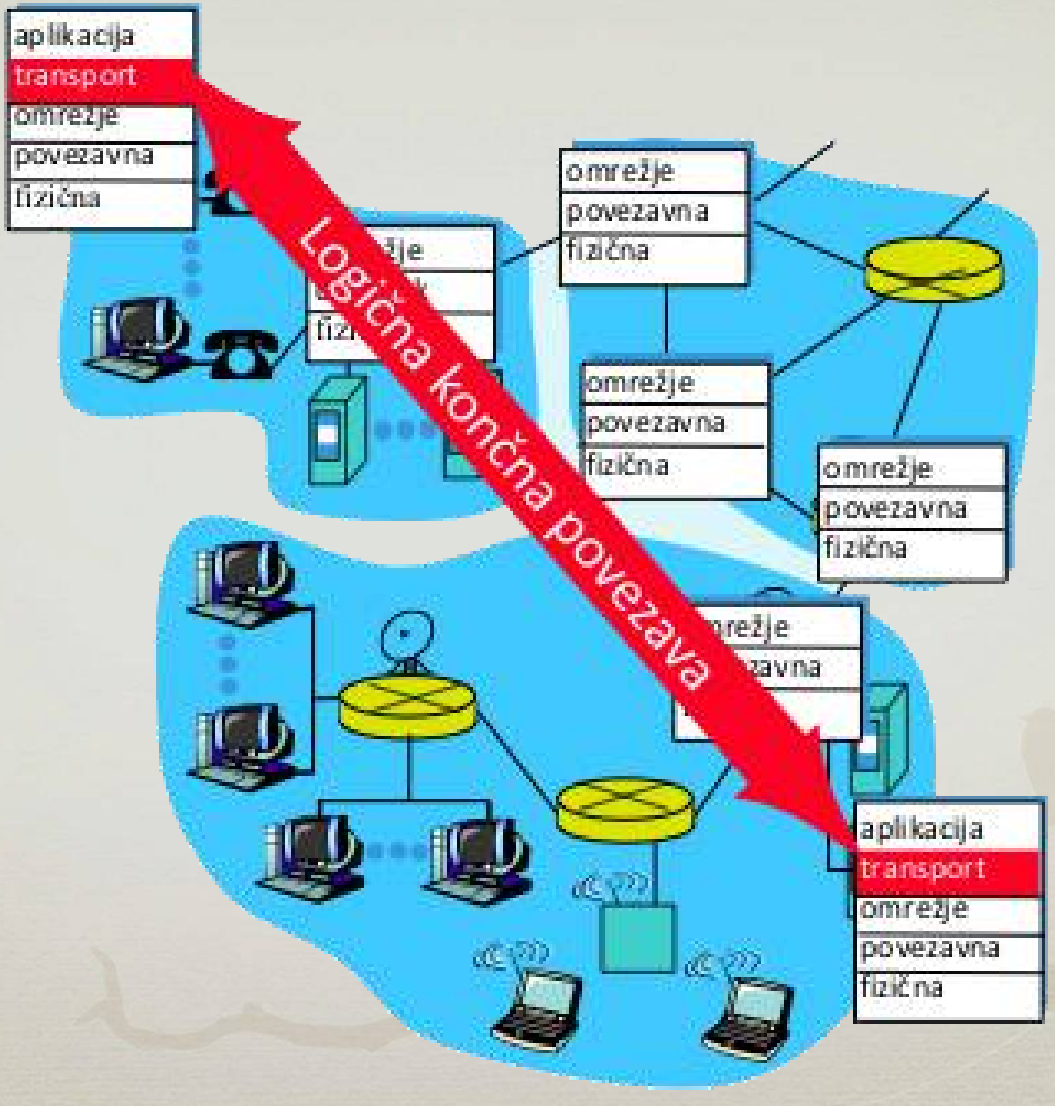


Transportna plast

- Horizontalna komunikacija
  - komunikacija med aplikacijskimi procesi
  - **pošiljatelj**
    - sporočilo razbije v segmente in jih posreduje v enkapsulacijo omrežni plasti
  - **prejemnik**
    - dekapsulira segmente iz paketov in jih združi v sporočila in posreduje aplikacijski plasti

Transportna plast

- Horizontalna komunikacija



Transportna plast

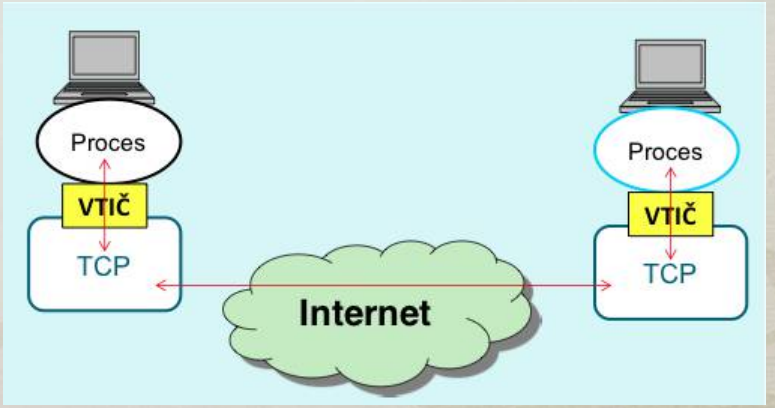
- Naslavljanje procesov
  - **vrata** (port)
    - 16 bitna številka
    - **vrata izvornega procesa**
    - **vrata ponornega procesa**
  - naslov procesa v končnem sistemu
    - **oblika**: *naslov končnega sistema:številka vrat*
      - 193.2.74.246:80
      - strežnik www.pef.uni-lj.si na vratih 80

Transportna plast

- Naslavljanje procesov
  - dobro znana vrata (well-known ports)
    - vrata od 0 do 1023
    - rezervirana za nekatere aplikacije
      - spletni strežnik (http): 80
      - poštni strežnik (smtp): 25
      - imenski strežnik (dns): 53
      - oddaljen dostop (telnet): 23
      - pogovorni strežnik (irc): 194
      - …

Transportna plast

- Vertikalna komunikacija
  - vtičnica (socket)
    - vmesnik med aplikacijsko in transportno plastjo
  - pristopna točka procesa
    - proces ustvari vtičnico preko katere nato komunicira



Transportna plast

- Vertikalna komunikacija
  - **multipleksiranje** – pošiljatelj
    - zbiranje sporočil iz ene ali več različnih vtičnic
    - enkapsuliranje sporočil v segmente
    - posredovanje omrežnemu sloju
  - **demultipleksiranje** – sprejemnik
    - zbiranje segementov od omrežnega sloja
    - dekapsuliranje sporočil iz segmentov
    - razpošiljanja sporočil iz segmentov ustreznim vtičnicam

Transportna plast

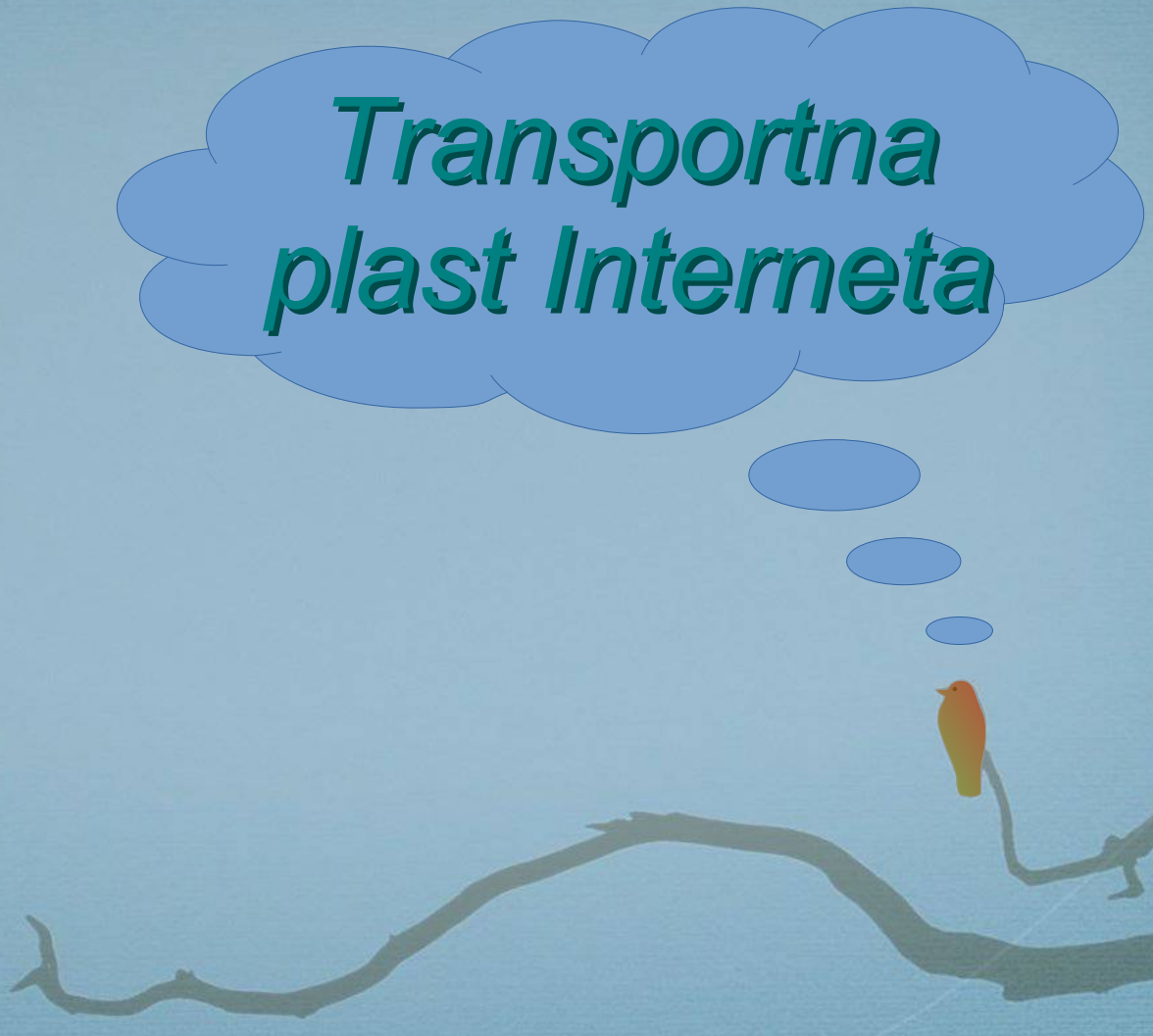
- Napad *portscan*
  - pregled vrat ciljnega končnega sistema
  - napadalec tako dobi vpogled v procese, ki tečejo na strežniku
    - lahko se nato nadalje osredotoči na posamezen proces

Transportna plast

- Različni protokoli
  - vsak protokol zagotavlja svoj nabor storitev
  - TCP
    - zanesljiva, povezavna storitev
    - nadzor pretoka in zasičenosti omrežja
  - UDP
    - nezanesljiva, nepovezavna storitev
  - v Internetu nimamo naslednjih storitev
    - zagotovljen čas dostave
    - zagotovljena pasovna širina

Računalniške komunikacije

Transportna plast Interneta



Jurij Mihelič, UniLj, PeF

UDP

- UDP, user datagram protocol
  - nepovezavna komunikacija

UDP

- Lastnosti
  - le „best-effort“ storitev
    - izgubljeni datagrami
    - ne zagotavlja vrstnega reda datagramov
  - majhna glava datagrama
    - samo 8 bajtov
  - nepovezavni
    - ni rokovanja
    - ni stanja povezave
  - brez nadzora pretoka

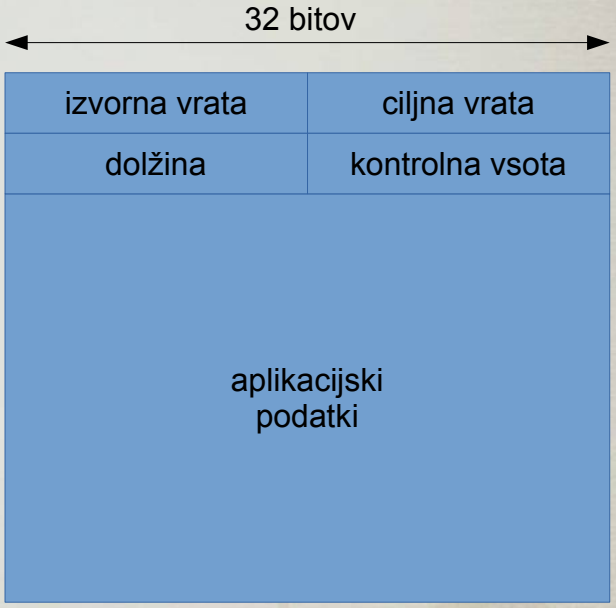
- Prednosti
  - enostaven protokol
    - brez dodatkov
  - hiter, učinkovit
    - manj režije
    - več možnih *povezav*
  - manjše zakasnitve
    - sporočilo se pošlje takoj
    - ni preverjanja zasičenosti itd.

UDP

- Namen
  - za aplikacije, ki
    - potrebujejo hitrost
    - vsebujejo poizvedbe tipa zahteva in odgovor
    - lahko tolerirajo delne izgube
  - dodatne lastnosti
    - mora zagotoviti aplikacija sama
  - primeri
    - DNS, SNMP, usmerjevalni protokoli (RIP), DHCP
    - avdio in video pretok v realnem-času

UDP

- Format segmenta
  - zmeda: UDP datagram – „paket“ UDP protokola
  - naslavljanje procesov
    - številka **izvornih** in **ciljnih** vrat
  - dolžina segmenta
    - vključno z glavo
  - kontrolna vsota
  - podatki



UDP

- Internetna kontrolna vsota (internet checksum)
  - pošiljatelj
    - komplement eniške vsote 16 bitnih besed
  - prejemnik
    - eniška vsota podatkov in kontrolne vsote
    - če dobi same enice potem je ok

podatki	1 0 1 1 0 1 1 0 0 0 1 1 1 0 0 0
vsota	1 1 1 0 0
eniška vsota	1 1 0 1
eniški komplement	0 0 1 0

UDP

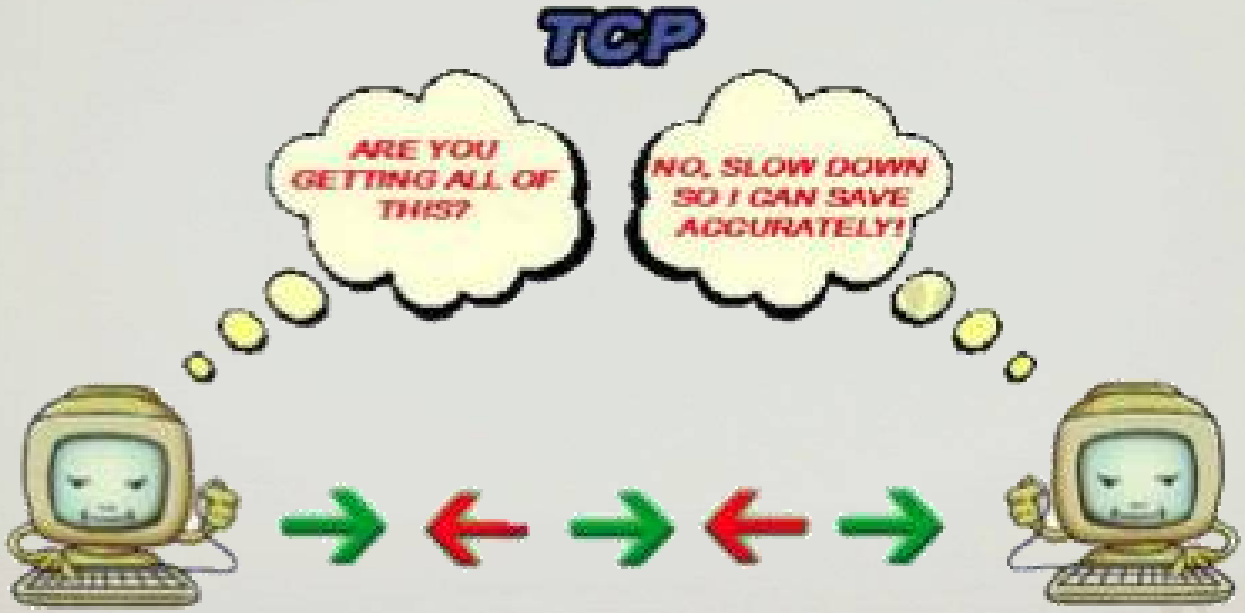
- Internetna kontrolna vsota
  - Zakaj zaznavanje napak na transportni plasti?
    - ni zagotovila, da protokoli na nižjih plasteh vsebujejo zaznavanje napak
      - npr., IPv6 ne vsebuje kontrolne vsote
    - do napak lahko pride tudi pri hranjenju datagrama v pomnilniku usmerjevalnika (in ne nujno pri prenosu)
    - zaznavanje napak med izvornim in ciljnim sistemom
      - princip končnih sistemov (end-to-end principle)

UDP

- Multipleksiranje / demultipleksiranje
  - nepovezavni protokol
  - identifikacija vtičnice
    - samo preko **cilja**: IP naslov in številka vrat
      - (dst_ip, dst_port)
  - posledica
    - posredovanje na vtičnico je odvisno le od cilja
    - izvor pa se ignorira
    - intuitivno
      - zahteve **različnih izvornih** procesov obdeluje **isti ciljni** proces

TCP

- Transfer control protocol
  - povezavna komunikacija, nadzor prenosa



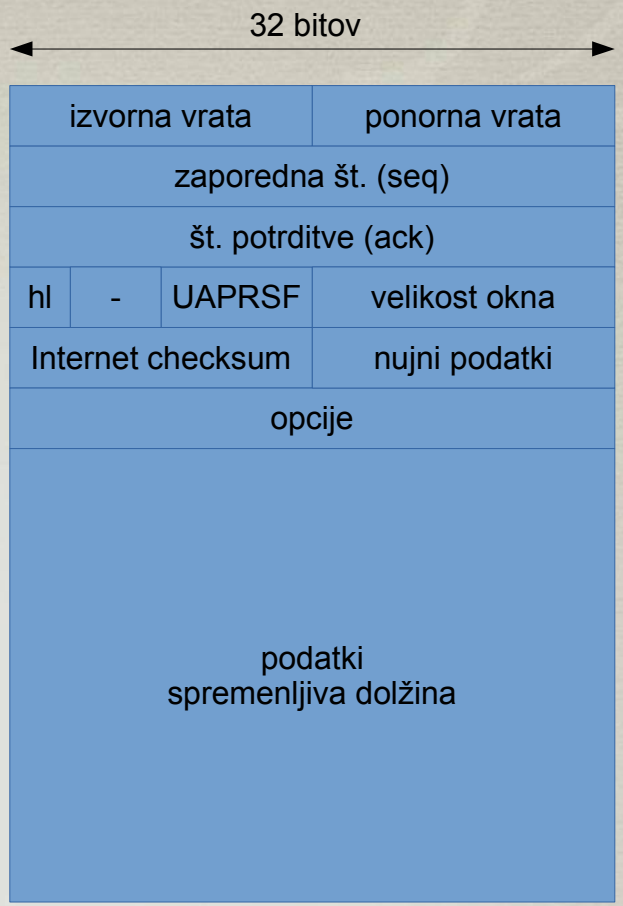
TCP

- Lastnosti
  - dvotočkovni protokol (point-to-point)
    - dve udeleženca: pošiljatelj in prejemnik
  - sočasno dvosmerna povezava (full duplex)
    - promet lahko v obe smeri poteka hkrati
  - povezavni protokol
    - vzpostavitev in rušenje zveze
  - zanesljiv prenos
    - potrjevanje segmentov
    - pozitivno potrjevanje, optimizirano potrjevanje

TCP

- Lastnosti
  - ohranja vrstni red segmentov
    - številčenje segmentov
  - tekoče pošiljanje z drsečim oknom
    - prilagodljiva velikost okna
      glede na nadzor pretoka in nadzor zamašitev
  - nadzor pretoka (flow control)
    - pošiljatelj ne preobremeni prejemnika
  - nadzor zamašitev (congestion control)
    - pošiljatelj ne preobremeni omrežja

TCP



- Format segmenta
  - hl … dolžina glave (4 bit)
    - v 32 bitnih besedah
  - zastavice UAPRSF
    - A … ACK
    - R … RST
    - S … SYN
    - F … FIN
  - zaporedne številke
    - seq … zaporedna številka prvega bajta v segmentu
    - ack … zaporedna številka naslednjega pričakovanega bajta

se ne uporablja: U … URG (nujni podatki), P … PSH (prioritetna obravnava)

TCP

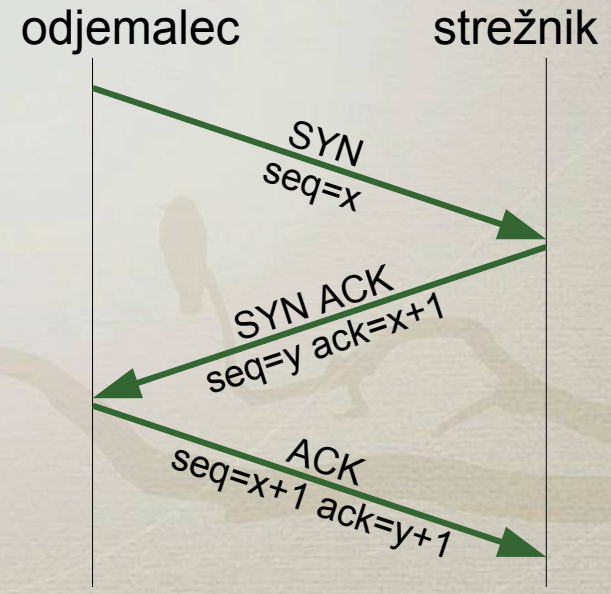
- Multipleksiranje / demultipleksiranje
  - povezavni protokol
  - identifikacija vtičnice
    - preko **izvora** in **cilja**: IP naslov in številka vrat
      - (src_ip, src_port, dst_ip, dst_port)
  - posledica
    - različni izvori (in cilji) se posredujejo na različne vtičnice

TCP: povezavni protokol

- Povezavna komunikacija
  - NE v smislu omrežnega sloja (navidezni vodi)
    - povezave v okviru paketnega omrežja
  - logična povezava
    - se tvori le v končnih sistemih (end-to-end)
    - vpletena končna sistema hranita stanje povezave
    - omrežje se povezave ne zaveda
      - usmerjevalniki procesirajo le datagrame
  - upravljanje s povezavo
    - vzpostavljanje povezave
    - rušenje povezave

TCP: povezavni protokol

- Vzpostavljanje povezave
  - udeleženca izvedeta rokovanje in izmenjata parametre povezave
    - začetne (naključne) zaporedne številke segmentov
    - velikosti medpomnilnikov (za nadzor pretoka)
  - **trojno rokovanje** (three-way handshake)
    1. odjemalec pošlje segment SYN in začetno številko segmenta
    2. strežnik vrne segment SYN ACK in začetno številko svojega segmenta
    3. odjemalec vrne ACK, lahko doda tudi že podatke

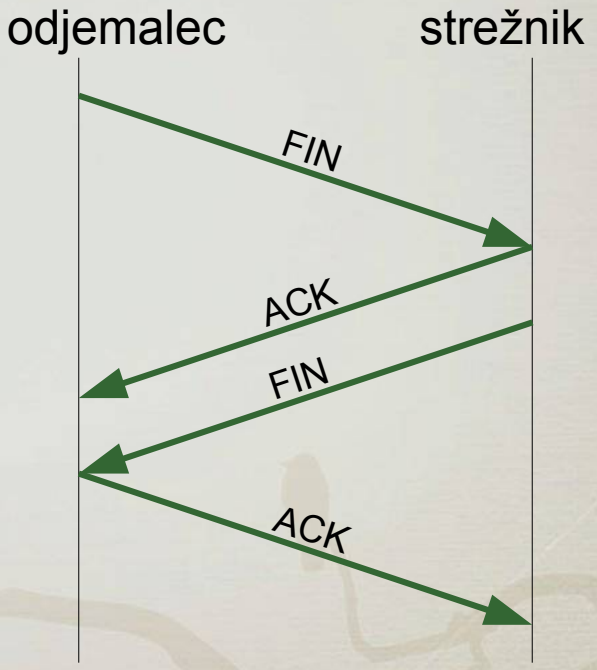


TCP: povezavni protokol

- Vzpostavljanje povezave
  - odzivi cilja izvoru na segment SYN
  - odgovor SYN-ACK
    - ciljni sistem je dosegljiv in
    - na podanih vratih teče nek proces
  - odgovor RST
    - ciljni sistem je sicer dosegljiv, vendar
    - na podanih vratih **ni** pripet noben proces
  - ni odgovora
    - ciljni sistem ni dosegljiv
      - morda je bil segment blokiran s strani požarnega zidu

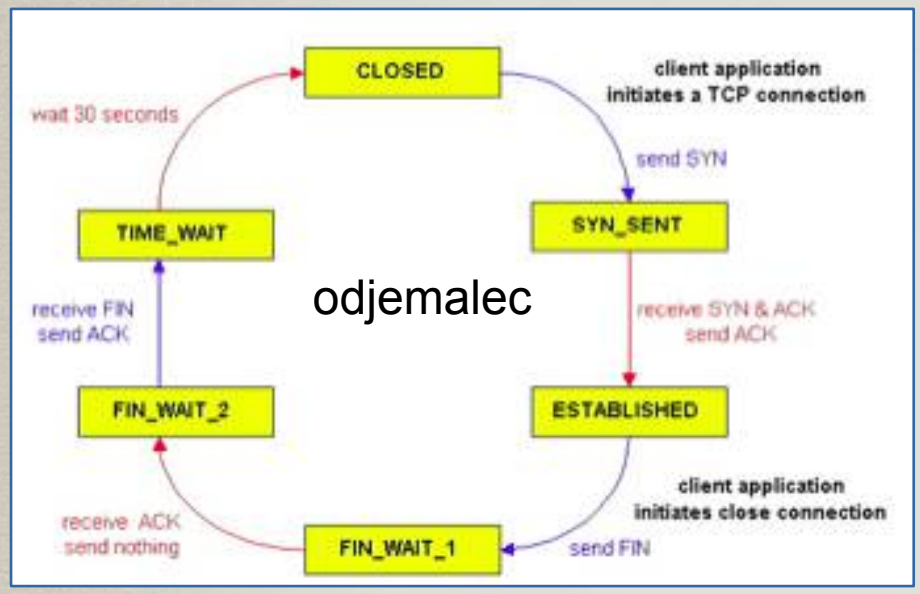
TCP: povezavni protokol

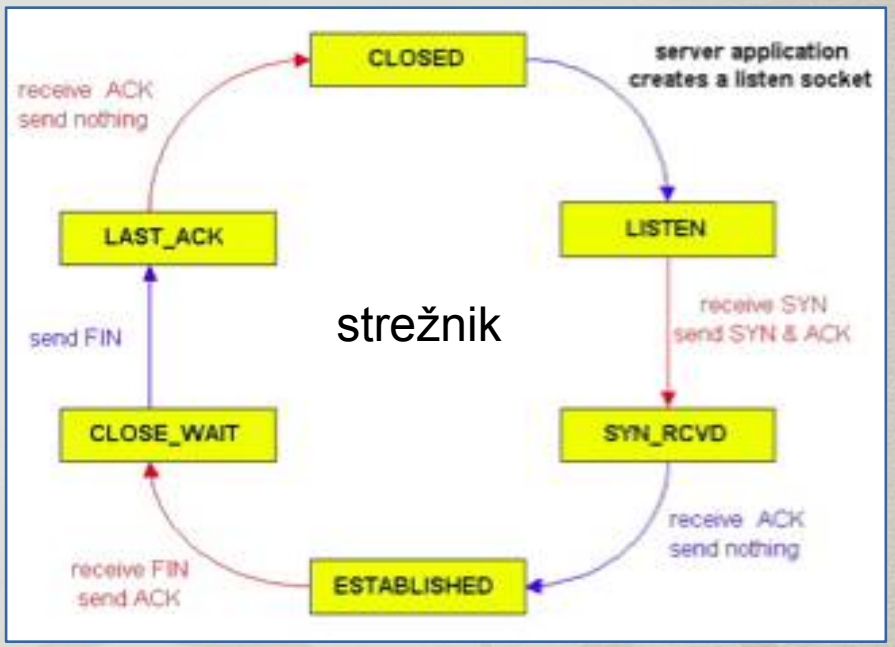
- Rušenje povezave
  - poljuben pobudnik: odjemalec ali strežnik
  - četvorno neodvisno rokovanje
    1. odjemalec pošlje FIN
    2. strežnik potrdi z ACK, zapre povezavo in pošlje FIN
    3. odjemalec prejme FIN in ga potrdi z ACK
    4. strežnik prejme ACK, končano



TCP: povezavni protokol

- Življenjski cikel udeležencev



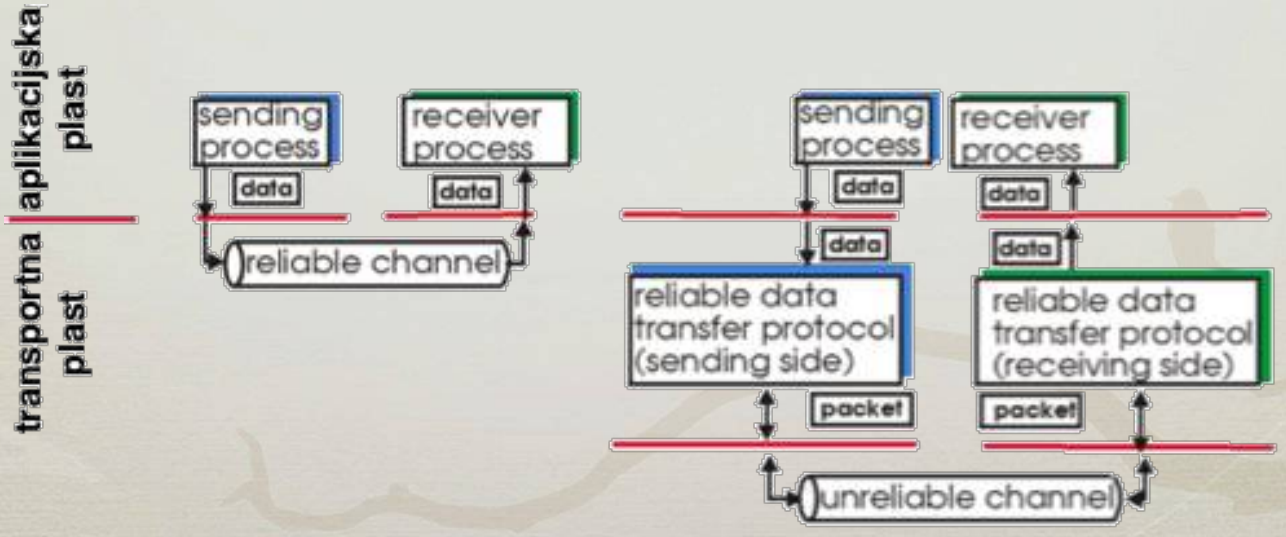


TCP: povezavni protokol

- Napad SYN flood
  - napadalec strežniku pošlje veliko segmentov SYN
  - strežnik vsakič rezervira del svojega medpomnilnika
  - napadalec ne zaključi rokovanja
  - medpomnilnik ostane rezerviran do izteka časovne kontrole
  - strežniku lahko zmanjka prostora in ne more več sprejemati novih povezav (DoS)

TCP: zanesljiv prenos

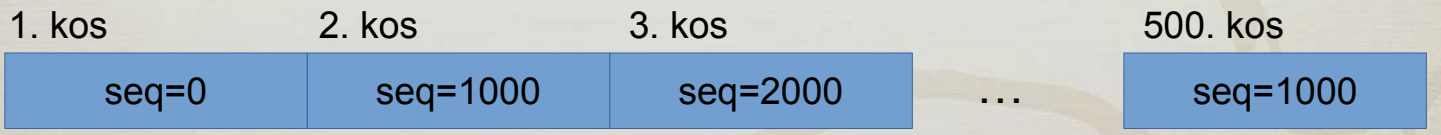
- Zanesljiv prenos
  - aplikacija predvideva zanesljivo povezavo
    - podatki se ne okvarijo
    - podatki se ne izgubljajo
    - podatki so dostavljeni v pravilnem zaporedju
  - prenos po omrežni plasti IP pa ni zanesljiv



Demo: http://www.ccs-labs.org/teaching/rn/animations/gbn_sr/

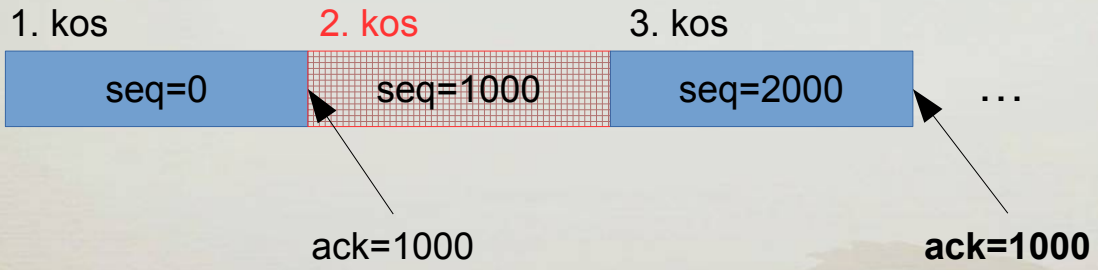
TCP: zanesljiv prenos

- Vrstni red segmentov
  - številčenje zaporedja poslanih bajtov
    - segment **vedno** vsebuje
      - *seq* … zaporedna številka prvega bajta v segmentu
  - primer
    - sporočilo dolžine 500 000 bajtov
    - razbijemo na 500 kosov velikosti 1000 ≤ MSS
      - MSS … maximum segment size



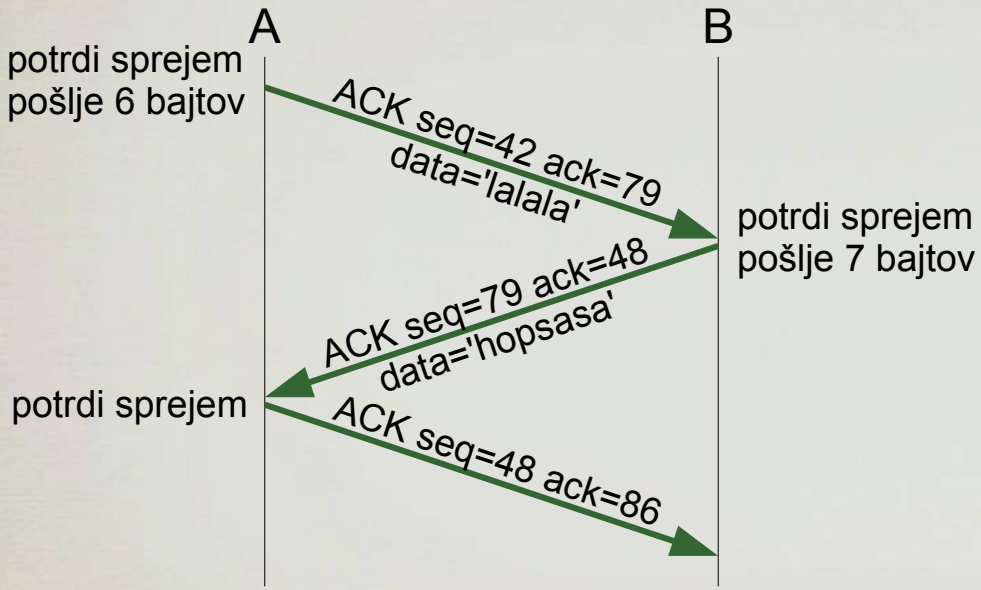
TCP: zanesljiv prenos

- Vrstni red segmentov
  - potrjevanje prejetih bajtov
    - segment **lahko** vsebuje še potrditev prejetega zaporedja
      - prižgana zastavica ACK
      - *ack* … zaporedna številka naslednjega pričakovanega bajta
    - **kumulativno potrjevanje**
      - potrdi se vse do prvega manjkajočega bajta iz prejetega toka



TCP: zanesljiv prenos

- Vrstni red segmentov



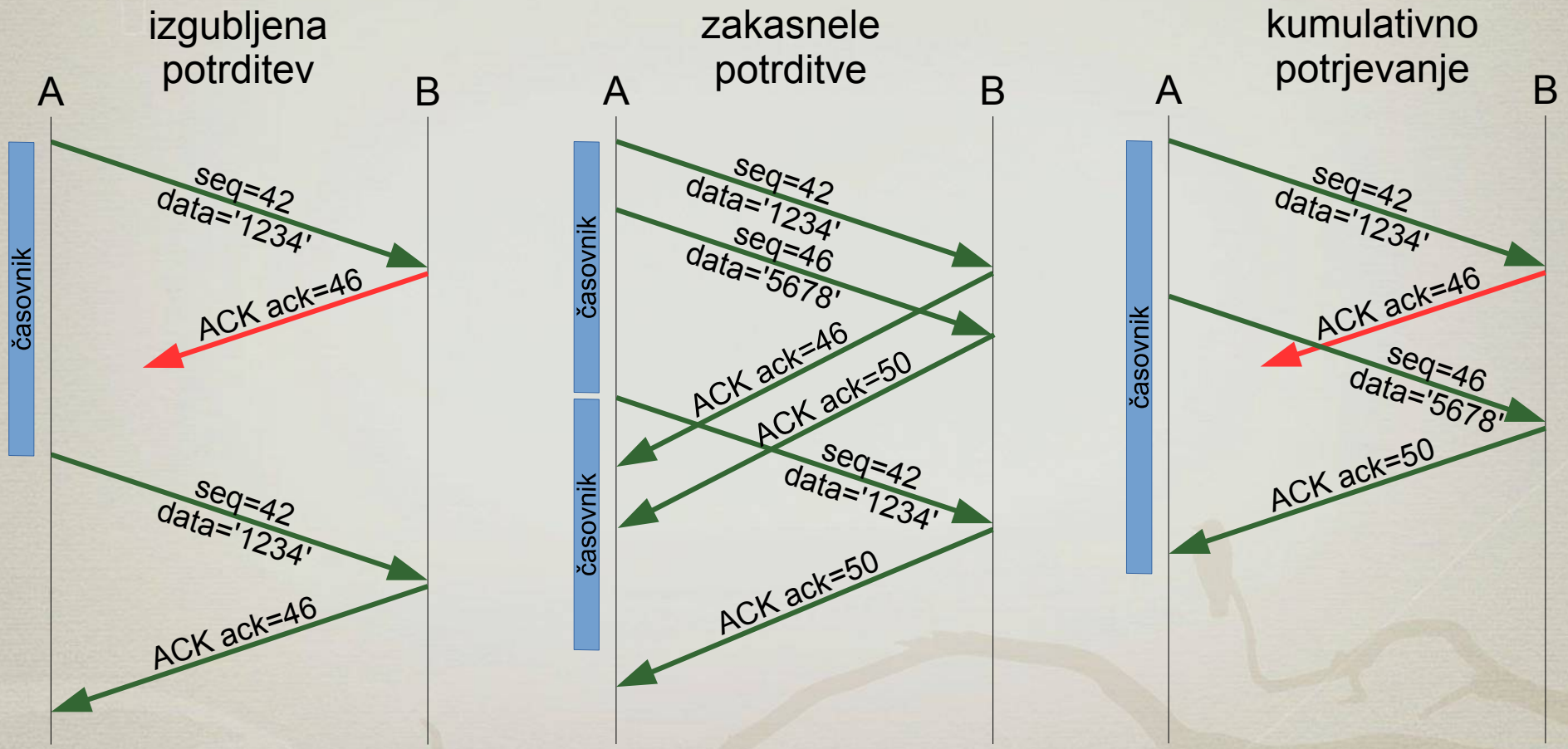
TCP: zanesljiv prenos

- Časovna kontrola
  - en časovnik (timer)
    - tudi v primeru več poslanih segmentov
    - se nanaša na najstarejši nepotrjeni segment
    - enostavnejše upravljanje

- **odposlan segment**
  - zagon časovnika, če ta še ne teče
- **prejeta potrditev**
  - ponoven zagon časovnika, če so še nepotrjeni segmenti
- **iztek časovnika**
  - nepotrjen segment (z najnižjo zap. številko) se ponovno pošlje
    - vzrok: izgubljen segment ali izgubljena potrditev
  - zagon časovnika

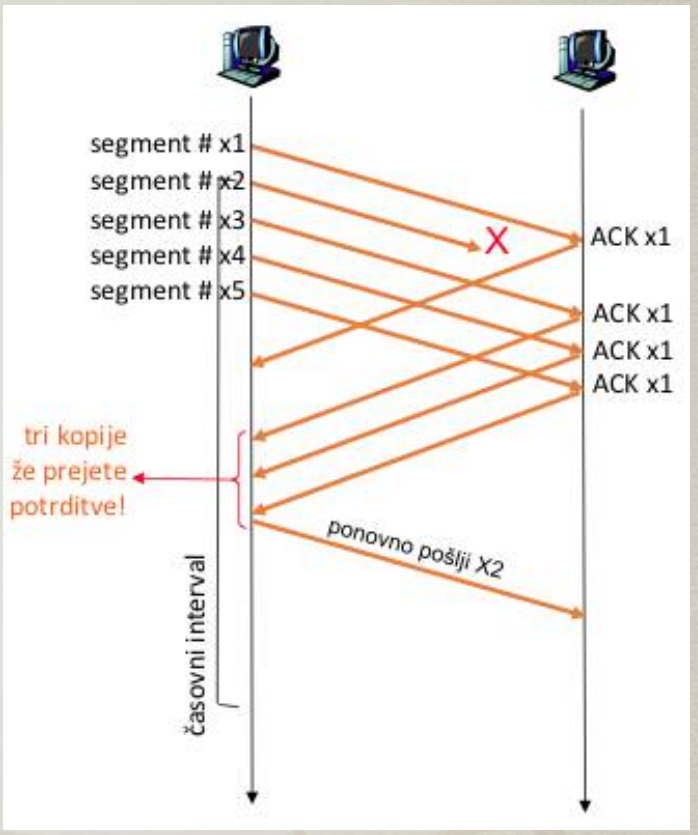
TCP: zanesljiv prenos

- Časovna kontrola



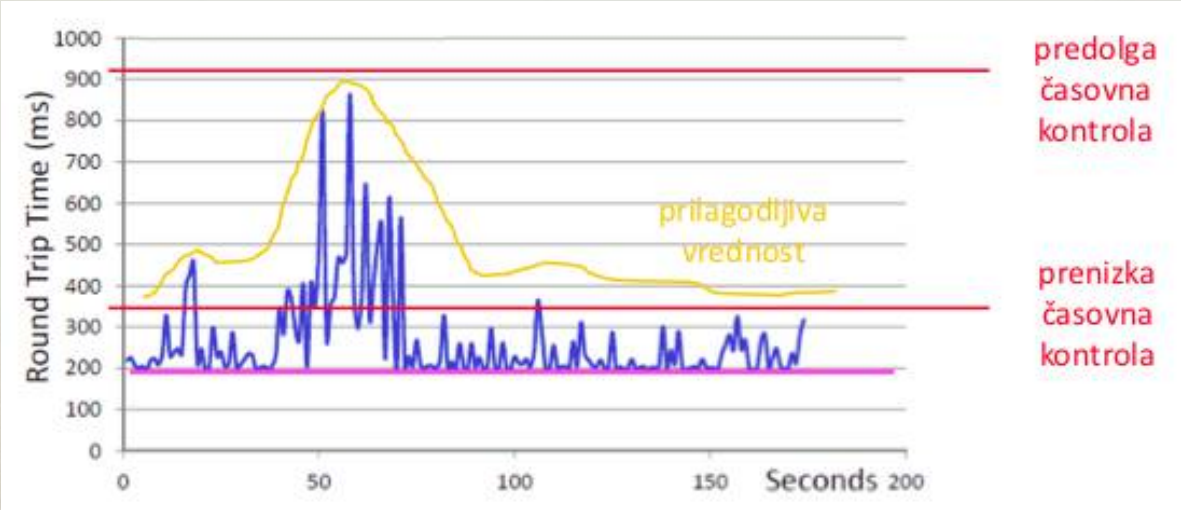
TCP: zanesljiv prenos

- Hitro ponovno pošiljanje
  - vrzel in tri enake potrditve
  - stanje na oddajni strani
    - nepotrjen segment, ki mu sledijo trije potrjeni
    - oddajnik sklepa, da je bil nepotrjeni segment izgubljen in
    - izvede ponovno pošiljanje pred iztekom časovnika



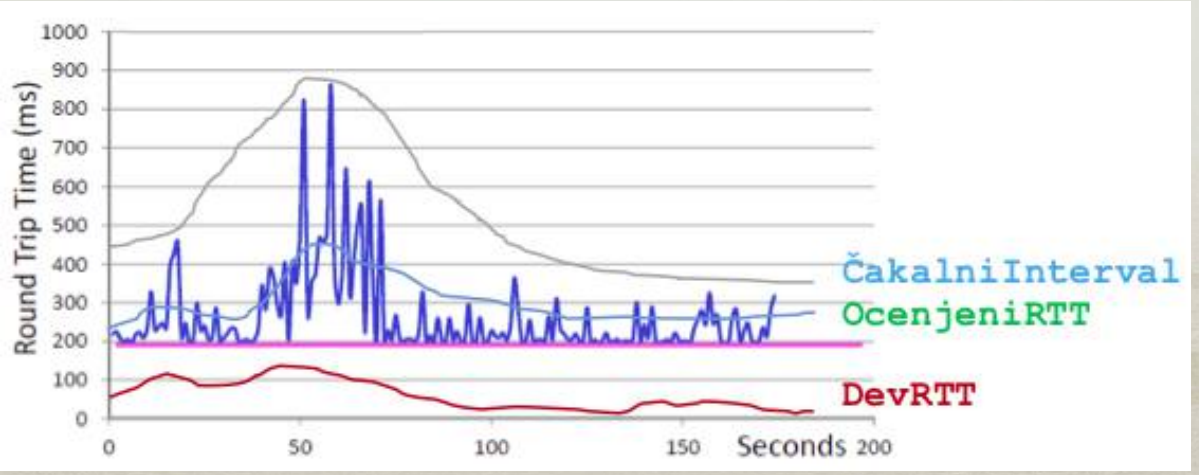
TCP: zanesljiv prenos

- Časovna kontrola
  - Kakšna je primerna dolžina čakalnega intervala?
    - prekratek: preveč ponovnih pošiljanj
    - predolg: prepočasno reagiranje na izgubljene pakete
    - daljši od časa vrnitve (RTT, round-trip time)



TCP: zanesljiv prenos

- Ocenjevanje RTT
  - gibajoče povprečje
    - $avg = (1-\alpha) * avg + \alpha * RTT$, npr. $\alpha = 0.125$
  - gibajoča razpršenost
    - $dev = (1-\beta) * dev + \beta * (RTT - avg)$, npr. $\beta = 0.25$
  - čakalni interval
    - ocena + rezerva, npr.: $avg + 4 * dev$



TCP: zanesljiv prenos

- Potrjevanje – dogodki pri prejemniku

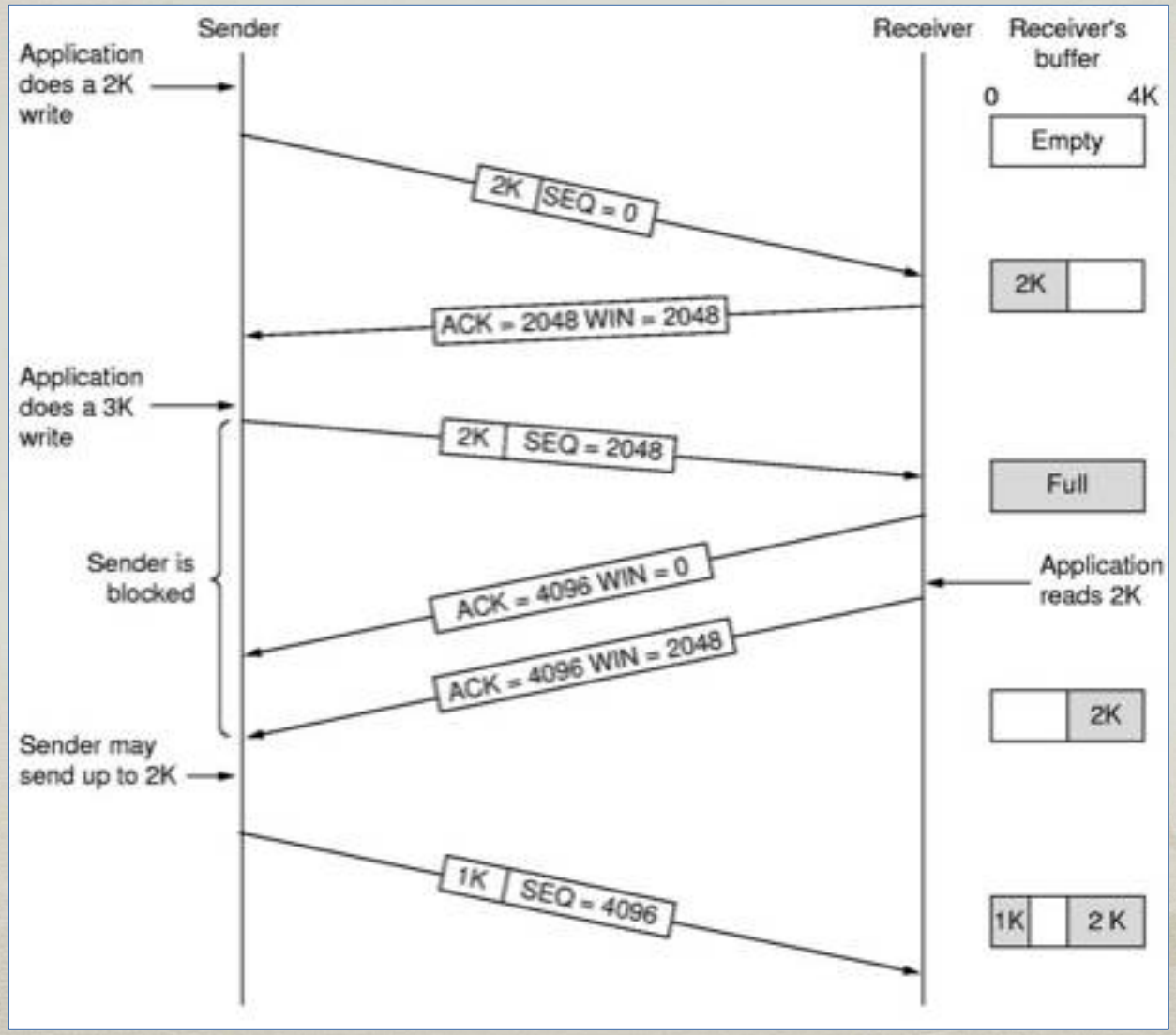
dogodek	odziv
• sprejem segmenta s pričakovano številko • vsi prejšnji že potrjeni	po preteku 500 ms pošlje zakasnjeno potrditev
• sprejem segmenta s pričakovano številko • prejšnji še ni potrjen	pošlji skupno potrditev obeh
zaznava vrzeli • sprejem segmenta s previsoko številko	takoj potrdi zadnji v zaporedju sprejeti segment (duplikat ACK)
polnjenje vrzeli • sprejem segmenta z najnižjo številko iz vrzeli	takoj potrdi segment

TCP

- Nadzor pretoka
  - usklajevanje „hitrosti“ prenašanja
    - preprečevanje prekoračitve medpomnilnika prejemnika
  - prejemnik sporoča pošiljatelju velikost razpoložljivega prostora v medpomnilniku
    - polje velikost okna v segmentu
    - pošiljatelj omeji število poslanih segmentov

TCP

- Nadzor pretoka



TCP

- Nadzor zamašitev
  - **zamašitev**
    - stanje preobremenjenosti omrežja
    - več virov sočasno **prehitro** pošilja **preveč** podatkov
  - posledice zamašitve
    - izgube segmentov
      - zaradi prekoračitve medpomnilnika v usmerjevalnikih
    - velike zakasnitve
      - zaradi dolgih čakalnih vrst v usmerjevalnikih