PRAKTIKUM IZ RAČUNARA

- OSNOVI MREŽNE KOMUNIKACIJE -

Transportni sloj

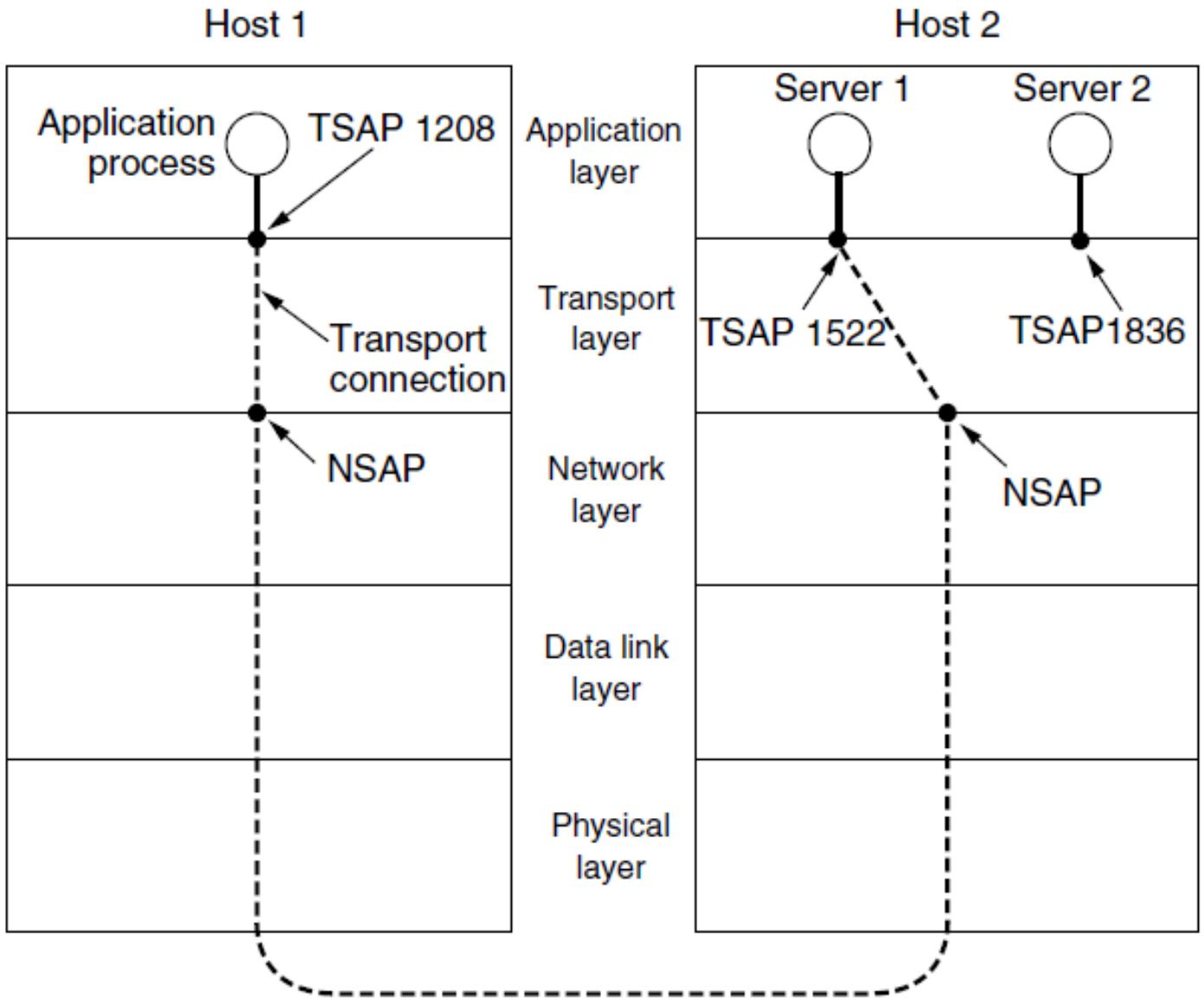
- Transportni sloj je zadužen da omogući prenos podataka između dva korisnička procesa koji se nalaze na udaljenim računarima.

- Zbog toga je pored mrežne (IP) adrese računara, koja je neophodna mrežnom sloju, da bi poruka ispravno bila preneta između udaljenih računara, potrebno uvesti i adresu procesa kojem je potrebno isporučiti pristiglu poruku.

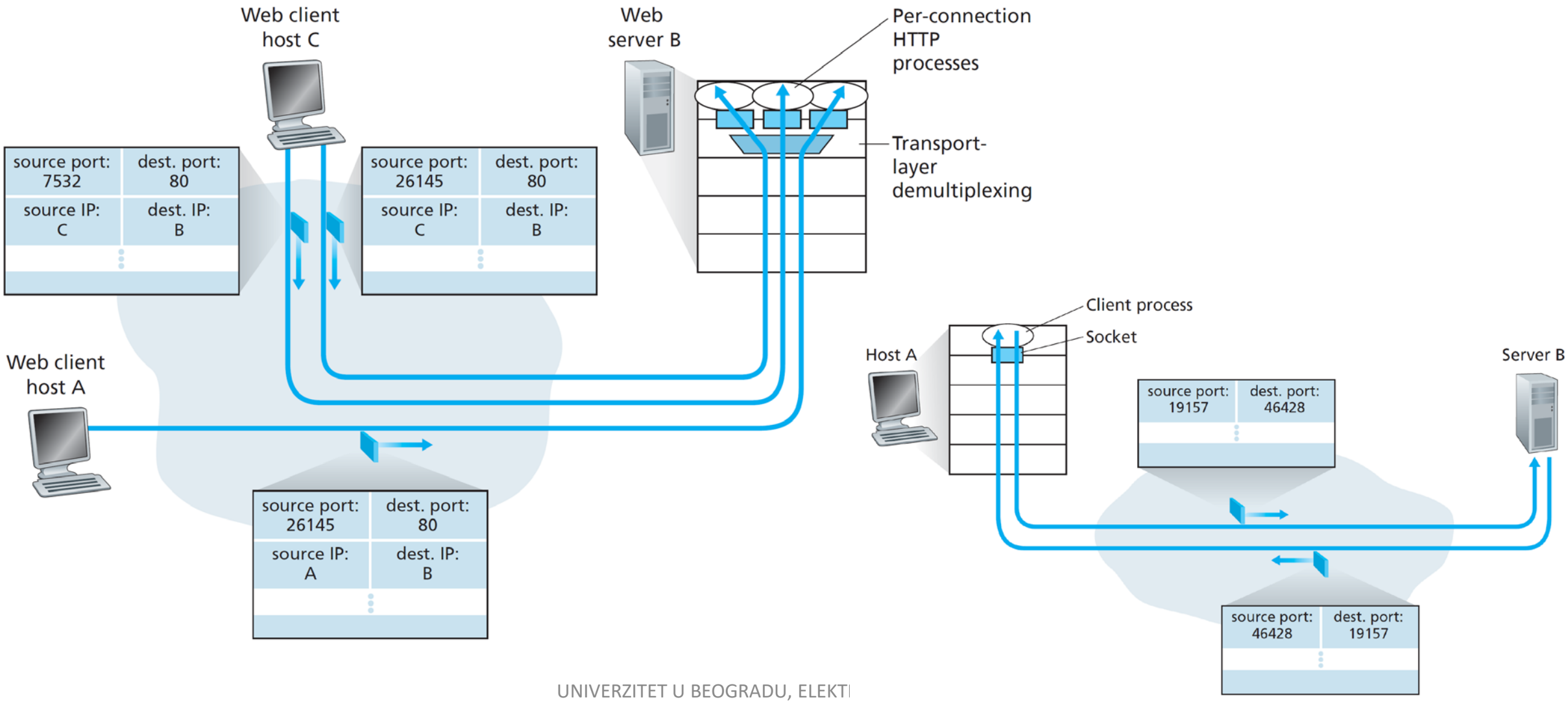
- U okviru transportnog sloja se definišu priključci (portovi). Korisnički proces koji očekuje prijem neke poruke, prijavljuje se da osluškuje odgovarajući port. Sve poruke koje pristignu se prosleđuju procesu koji osluškuje port na koji je poruka adresirana.

Transportni sloj

- TSAP – transportna pristupna tačka, adresa porta
- NSAP – mrežna pristupna tačka, IP adresa



Transportni sloj



Povezivanje na transportnom sloju - primer

- U prethodnom primeru na Web serveru postoji više procesa koji osluškuju port 80 koji je rezervisan za HTTP zahteve.
- Korisnički proces sa računara A i dva procesa sa računara C pristupaju ovom serveru i navode istu adresu porta pošto sva tri procesa zahtevaju pristup Web stranicama korišćenjem HTTPa.
- Dva procesa sa računara C imaju istu izvorišnu IP adresu ali im se izvorišne adrese porta razlikuju tako da će odgovor primljen sa servera B biti prosleđen na pravu adresu.
- S druge strane izvorišne adrese portova različitih procesa na različitim računaraima mogu biti iste. Ovo se vidi na primeru drugog procesa sa računara C i procesa sa računara A. Bez obzira što ova dva procesa imaju isti izvorišni port njihove izvorišne IP adrese se razlikuju tako da će poruka poslata sa servera B svakako biti isporučena na pravu adresu.

Adrese porta

- Adresa porta je dužine 16-bita i omogućava komunikaciju između procesa na udaljenim računarima.
- Prvih 1024 adresa portova je rezervisano za standarne servisa.
- Primer nekih standarnih servisa je prikazan u tabeli.

Port	Protocol	Use
20, 21	FTP	File transfer
22	SSH	Remote login, replacement for Telnet
25	SMTP	Email
80	HTTP	World Wide Web
110	POP-3	Remote email access
143	IMAP	Remote email access
443	HTTPS	Secure Web (HTTP over SSL/TLS)
543	RTSP	Media player control
631	IPP	Printer sharing

Transportni protokoli na Internetu

- Na Internetu se koriste 2 osnovna transportna protokola: UDP i TCP
- UDP (User Datagram Protocol) – predstavlja protokol bez uspostavljanja direktne veze. Koristi se u situacijama kada je važnija brzina komunikacije od pouzdanosti prenosa.
- TCP (Transmission Control Protocol) – predstavlja protokol sa uspostavljanjem direktne veze. Koristi se u većini aplikacija i garantuje ispravan prenos podataka uz opciju retransmisije u slučaju grešaka.

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

UDP karakteristike

- UDP ne pruža nikakve dodatne funkcionalnosti u odnosu na mrežni sloj osim adresa portova. Osim provere da li je pristigli paket ispravan (pomoću kontrolne sume) ne postoji mogućnost retransmisije i potvrđvanja prijema kojima se povećava pouzdanost komunikacije.

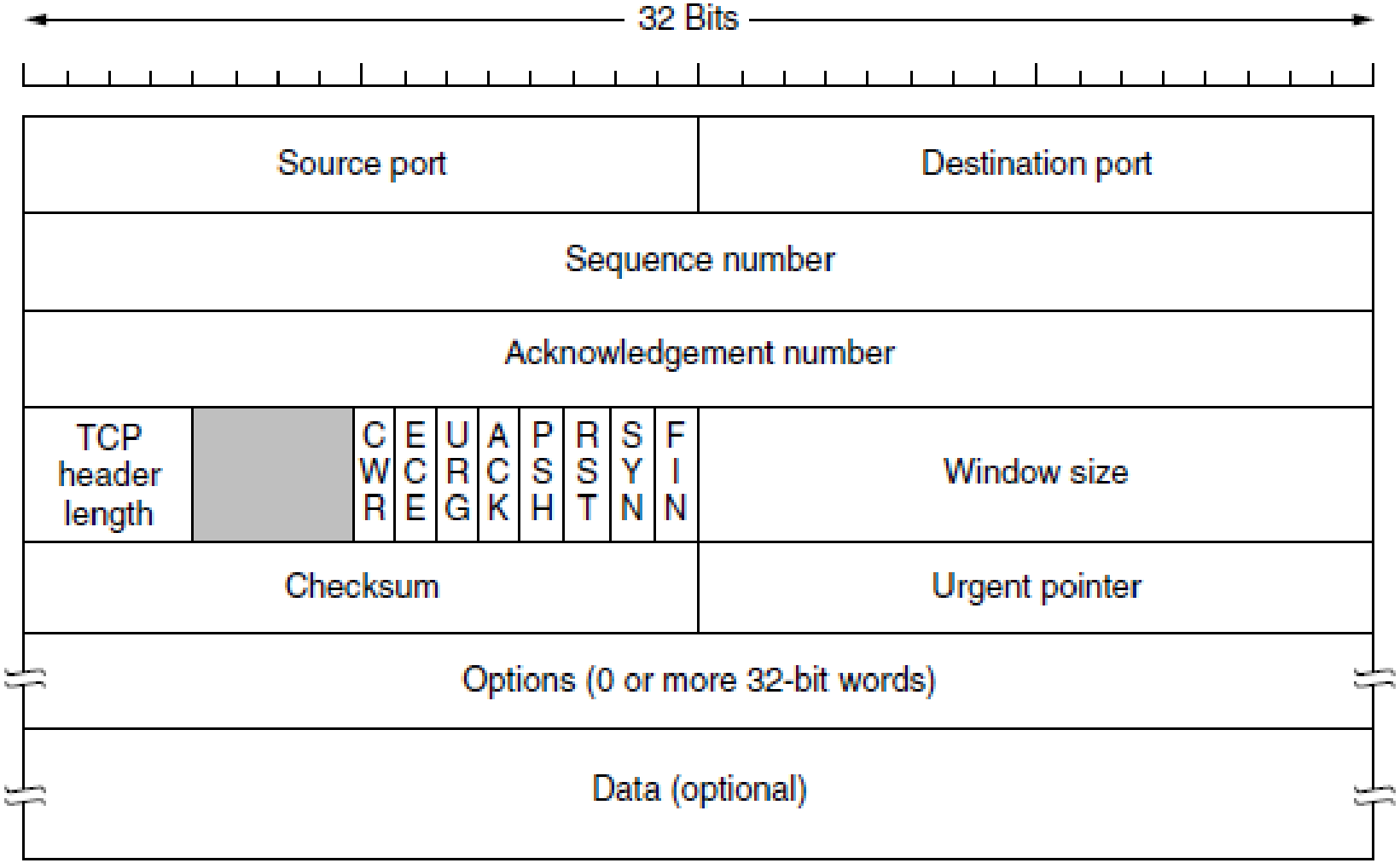
- UDP se koristi u situacijama gde je potrebno dobiti što brži odgovor ili obezbediti prenos sa što manjim kašnjenjem.

TCP karakteristike

- TCP obezbeđuje pouzdan prenos toka bajtova sa kraja na kraj veze kroz nepouzdanu mrežu.

- TCP funkcioniše po principu uspostavljanja direktne veze. Svaki bajt na TCP vezi ima jedinstveni 32-bitni redni broj koji se koristi za kontrolisanje koji podaci su zapravo preneti po uspostavljenoj vezi. Redni broj prvog bajta nije uvek 0 i određuje se prilikom uspostavljanja TCP veze.

TCP zaglavlje



Seq number – Redni broj prvog bajta u bloku koji se šalje.
Ack number – Redni broj bajta koji se sledeći očekuje. Ovim brojem se označava i da su ispravno primljeni svi bajtovi sa manjim rednim brojem - kumulativna potvrda.
SYN – kontorlni bit za uspostavljanje veze
FIN – kontorlni bit za raskidanje veze
ACK – kontorlni bit koji označava da paket sadrži potvrdu i tada se posmatra polje sa brojem potvrde
RST – kontorlni bit za resetovanje veze

Win size – Količina bajtova koja se može poslati u narednoj poruci, uključujući i potvrđeni bajt. Broj slobodnih mesta u prijemnom baferu.

Uspostavljanje TCP veze

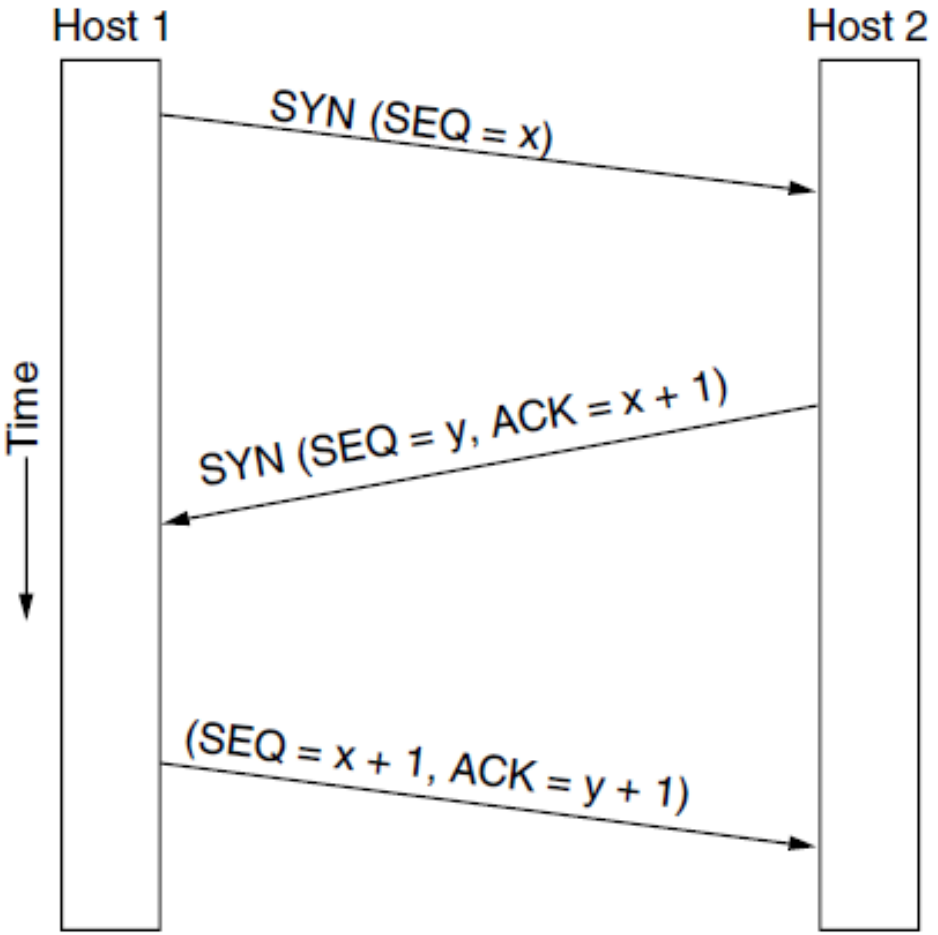
Uspostavljanje TCP veze se obavlja u 3 koraka:

1. Računar 1 koji inicira komunikaciju šalje TCP paket sa SYN=1 i ACK=0. SEQ = x predstavlja redni broj prvog bajta u prenosu (isn – initial sequence number).

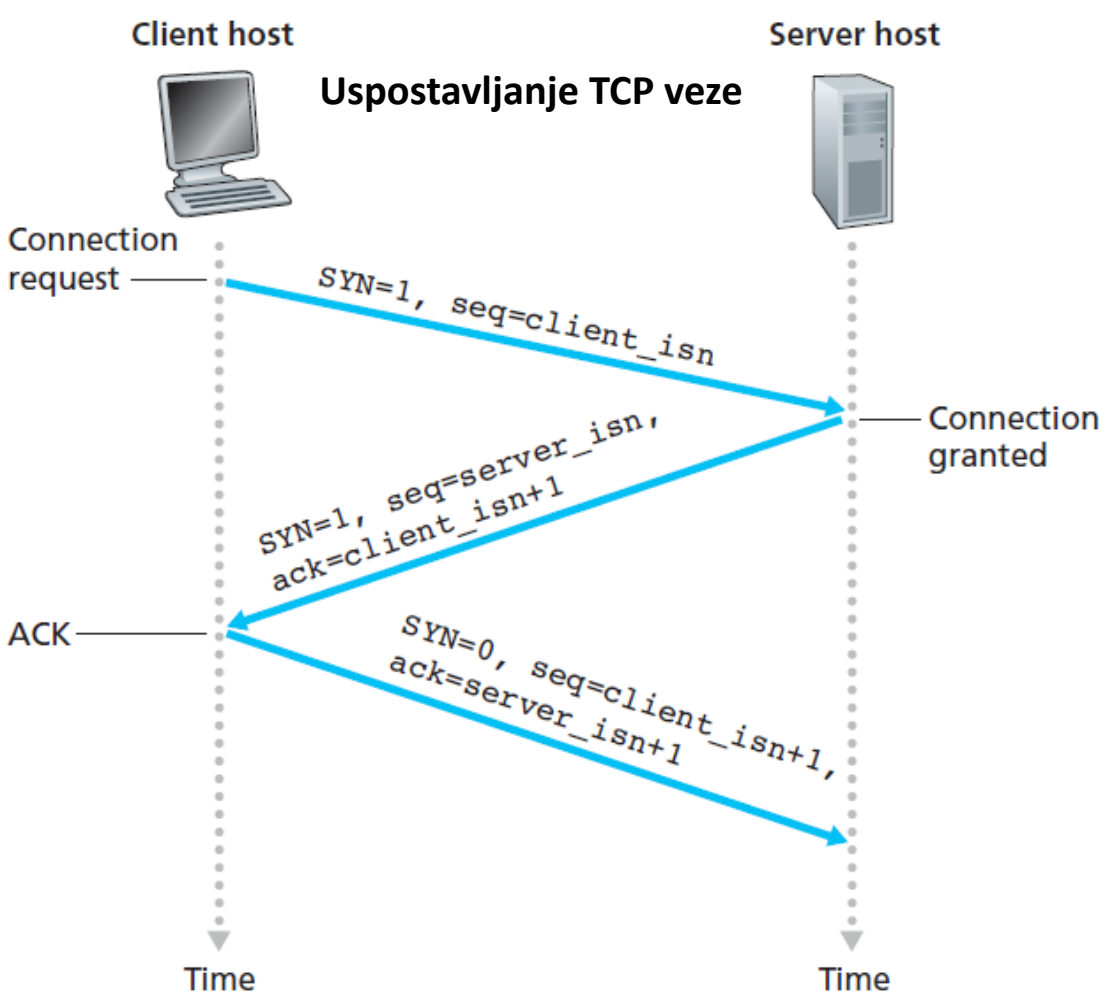
2. Računar 2 odgovara porukom sa SYN=1 i ACK=1. U ACK NUM upisuje x + 1 i definiše svoju početnu vrednost za numerisanje bajtova SEQ = y. Dakle ovom drugom porukom potvrđuje otvaranje veze od Račnuara 1 ka Računaru 2 i inicira otvaranje veze u suprotnom smeru.

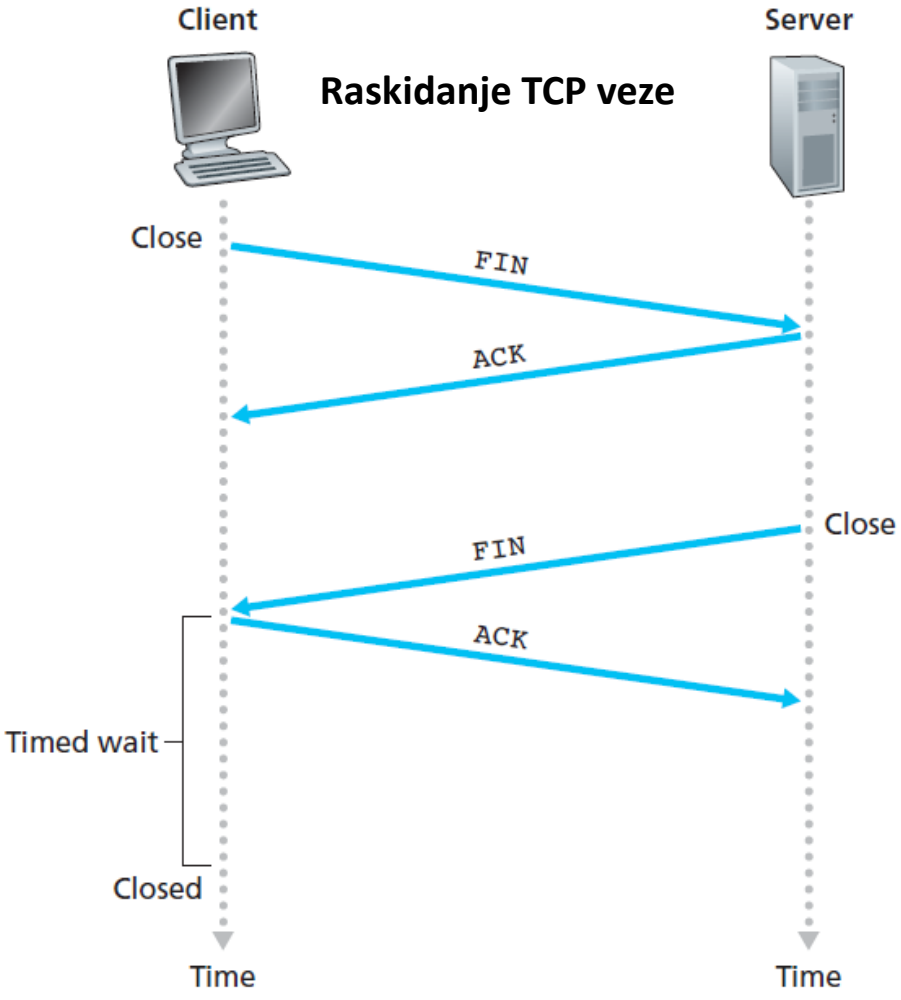
3. U narednoj poruci se potvrđuje se otvaranje veze od Računara 2 ka Računaru 1 (SYN = 0, ACK = 1) i šalje se prvi blok podataka od Računara 1 ka Računaru 2.

Raskidanje veze se realizuje na sličan način s tim što se umesto bita SYN koristi bit FIN. Prilikom raskidanja TCP veze čeka se određeni vremenski interval nakon signala potvrde pre nego što se veza označi zatvorenom. Time se osigurava da su svi paketi koji su pripadali ovoj TCP vezi nestali sa mreže.



Uspostavljanje i raskidanje TCP veze





Prenos podataka TCP vezom

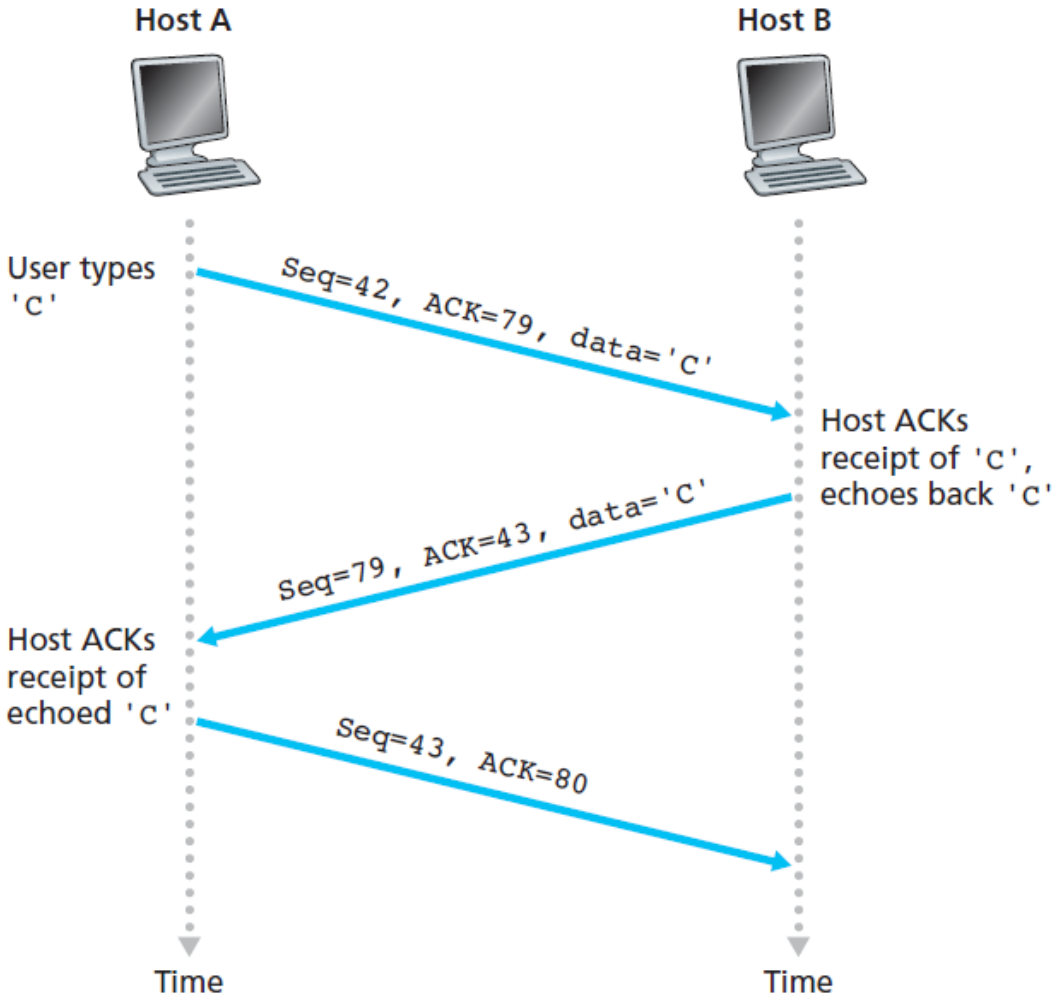
- Nakon uspostavljanja TCP veze podaci se šalju tako što se u svakoj poruci navodi jedinstveni broj prvog bajta trenutne poruke i u slučaju potvrde prijema redni broj narednog bajta koji se očekuje od pošiljaoca.

- Prilikom svake poruke se takođe navodi i maksimalan broj bajtova koji je primalac spreman da prihvati u narednoj poruci. Ovaj mehanizam je neophodan kako bi se sprečilo prepunjavanje ulaznih bafera podataka.

Primer TCP komunikacije

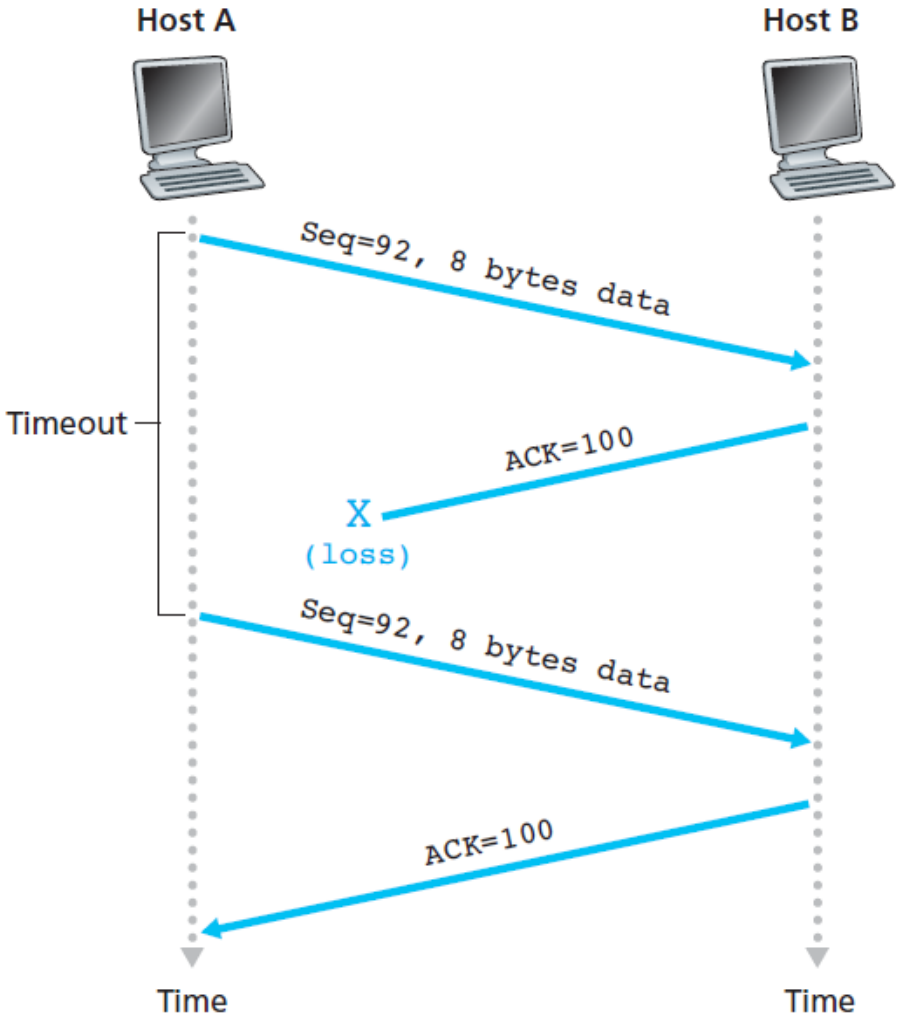
- Računar A šalje jedan bajt C računaru B. Ovaj bajt je označen brojem 42 i navodi da je sledeći bajt koji očekuje od računara B 79.

- Računar B šalje nazad bajt C računaru A i označava ga brojem 79. U isto vreme potvrđuje prijem prethodnog bajta tako što u ACK NUM polje upisuje broj 43. Ovim je naznačeno da naredni bajt koji očekuje ima redni broj 43 čime je potvrđen ispravan prijem bajta sa rednim brojem 42.



Primer TCP komunikacije

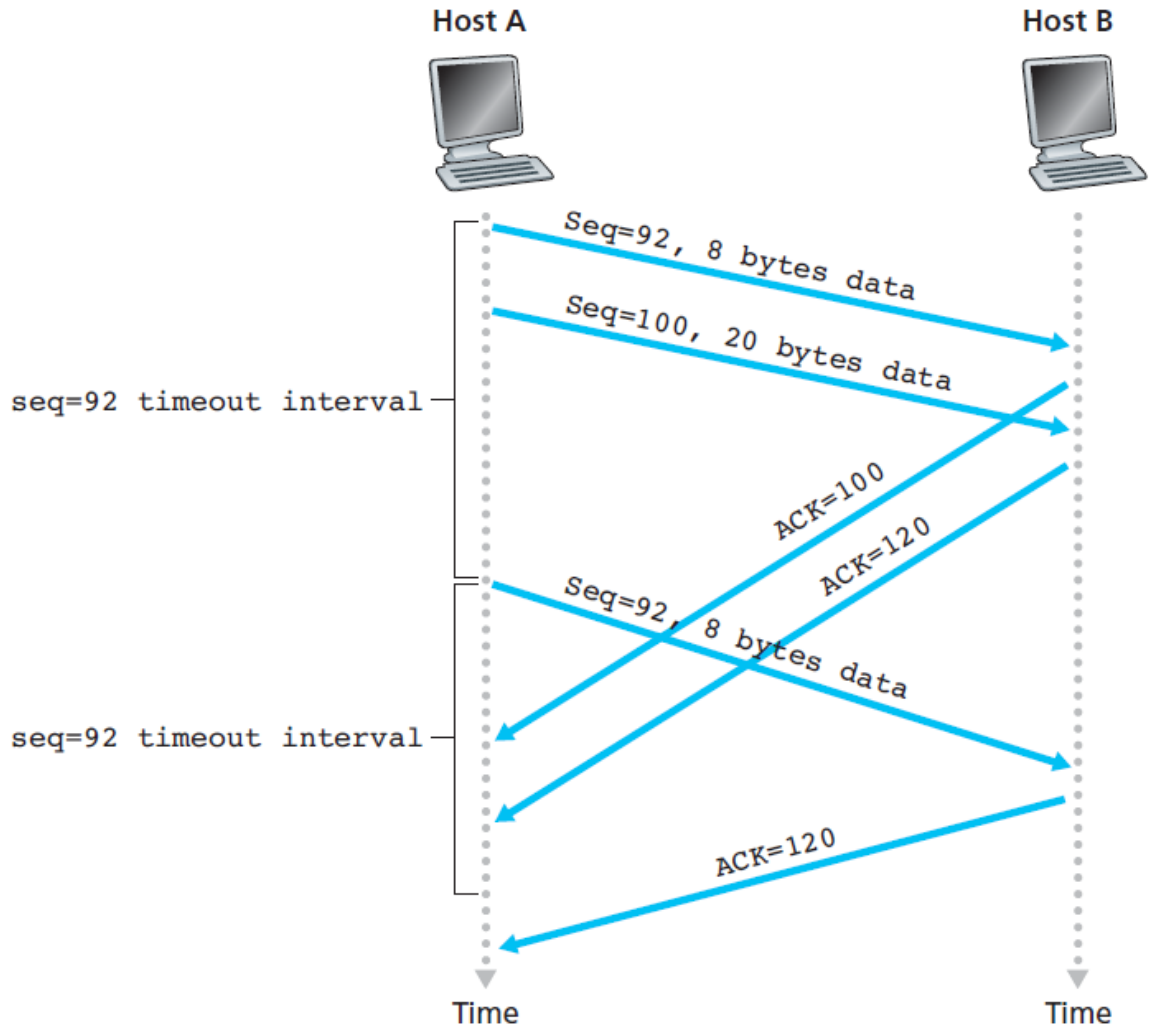
- U slučaju gubitka paketa sa podacima ili paketa sa signalom potvrde nakon određenog intervala vremena (timeout period) obavlja se retransmisija podataka.



Primer TCP komunikacije

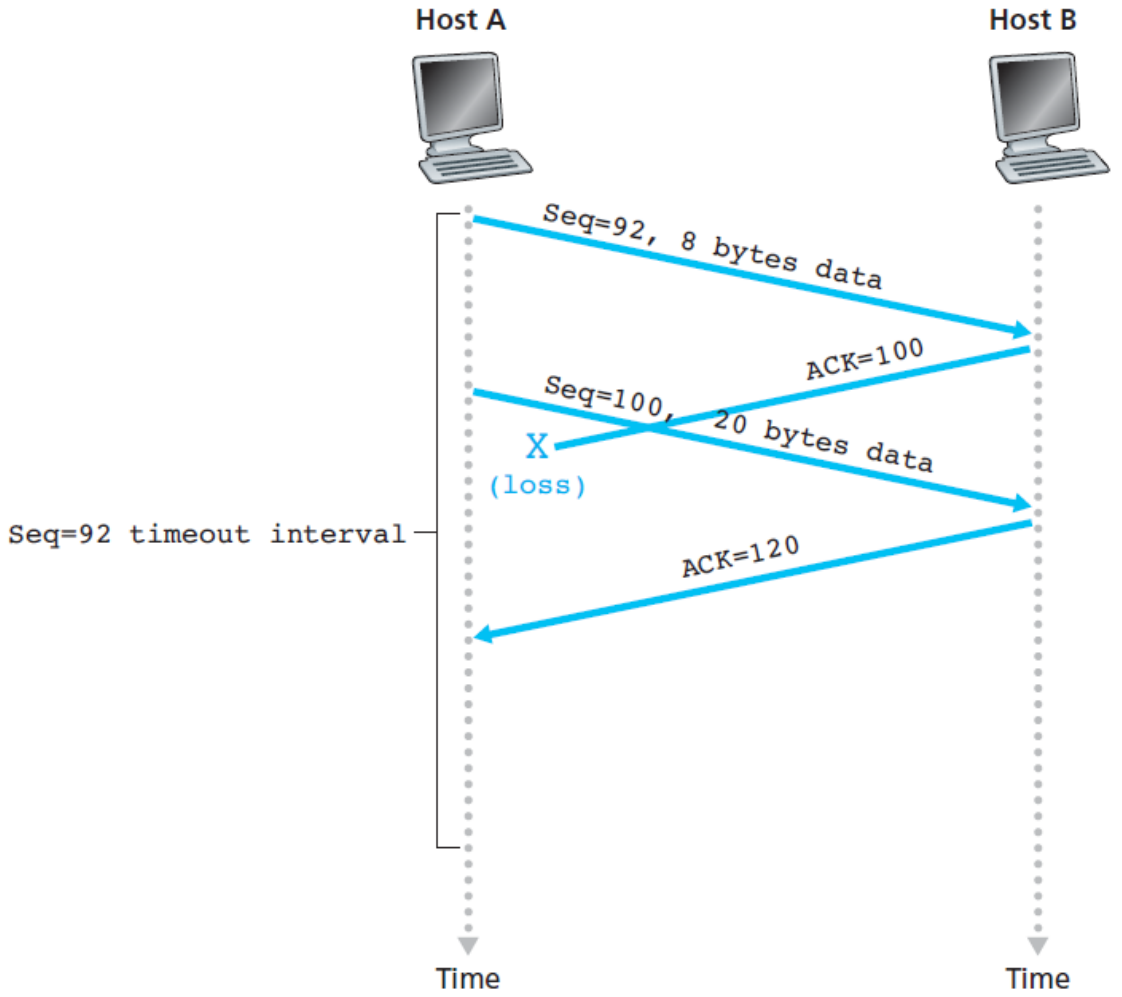
- Ukoliko signal potvrde stigne nakon isteka vremena čekanja, odgovarajući segment će biti poslat ponovo.

- Obratiti pažnju da se nakon prijema ponovo poslatog segmenta šalje signal potvrde sa rednim brojem bajta 120 čime se označava da je pored prvog ispravno primljen i drugi segment podataka.



Primer TCP komunikacije

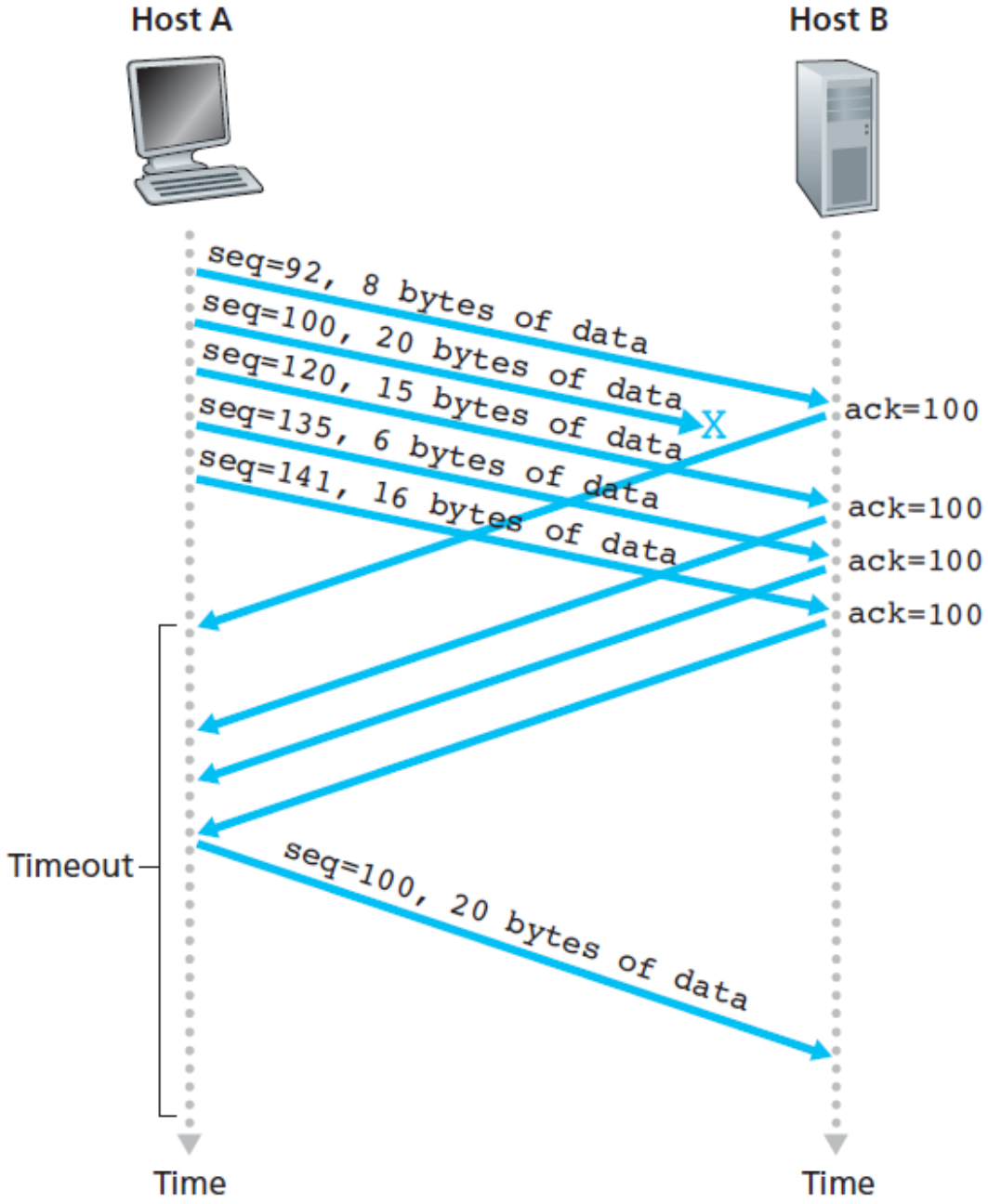
- U sledećem primeru potvrda za prvi blok podataka (Seq=92) je izgubljena ali je blok ispravno primljen.
- Naredni blok podataka je takođe ispravno primljen i računar B šalje poruku sa signalom potvrde da je prvi naredni bajt koji očekuje sa rednim brojem 120.
- Kako su poruke potvrde kumulativne ovo znači da su svi prethodni blokovi ispravno primljeni, uključujući u prvi blok podataka, tako da nema potrebe za retransmisijom.



Primer TCP komunikacije

- Postoje situacije kada se obavlja ponovo slanje bloka podataka i pre isteka intervala čekanja.

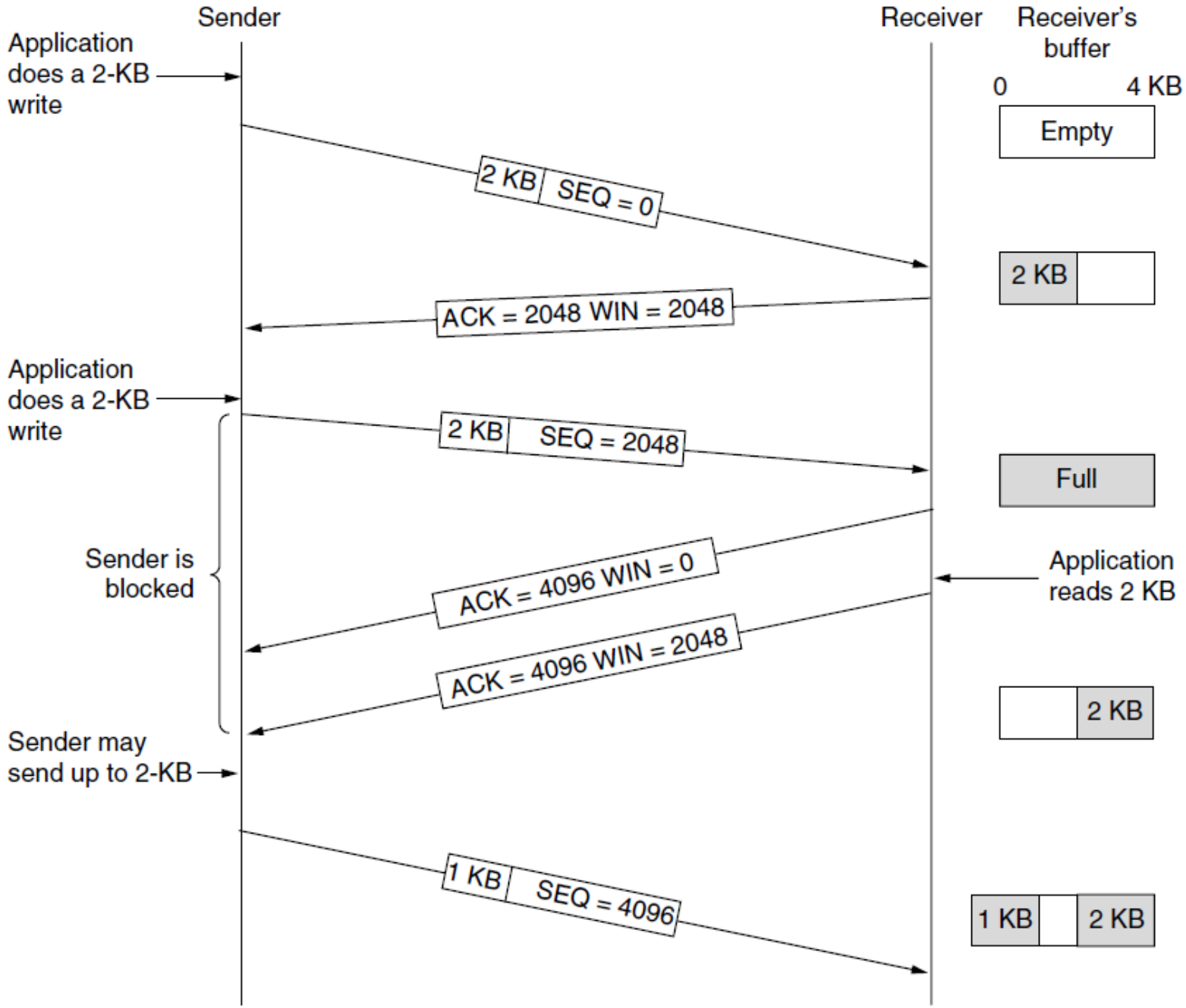
- Ukoliko se u više od 3 uzastopna paketa potvrde prepozna isti broj narednog očekivanog bajta, to zapravo znači da je taj blok podataka izgubljen. U tom slučaju se inicira ponovno slanje ovog bloka podataka.



Kontrola količine podataka

U slučaju punog ulaznog bafera, primalac signalizira pošiljaocu da ne može da prihvati nove podatke tako što postavlja vrednost **Win size** na 0.

Pošiljalac po prijemu ove poruke ne šalje nove podatke sve dok ne dobije poruku na validnom veličinom prozora.



Problem broja IP adresa

- IP adrese su predstavljene sa 32 bita, što čini skup od oko 2 milijarde adresa.
- Ogorman broj uređaja povezanih na je odavno prevazišao ovaj broj IP adresa.
- Kako onda Internet i dalje funkcioniše?

Dinamička dodela IP adresa

- Recimo da pružalac Internet usluga poseduje /16 blok IP adresa. Dakle ukupno 65534 korisnika može da se poveže na Internet.
- Broj korisnika se može povećati ako se IP adrese ne dodeljuju statički, tako da svaki korisnik ima svoju IP adresu kada pristupa Internetu, već dinamički.
- Dinamička dodela IP adresa podrazumeva da se IP adresa dodeljuje korisniku u trenutku pristupanja Internetu i oduzima mu se kada se raskine konekcija.
- Na ovaj način je sa blokom adresa /16 podržano ukupno 65534 aktivna korisnika dok ukupan broj korisnika može biti znatno veći.

IPv6 adresiranje

- Dinamička dodela IP adresa malo ublažava problem ali je daleko od rešenja. S obzirom da se danas očekuje da su uređaji stalno povezani na mrežu broj istovremeno aktivnih korisnika obično prelazi broj dostupnih IP adresa kod pružaoca Internet usluga.

- Dugoročno rešenje je drastično povećati broj dostupnih IP adresa prelaskom na IPv6 koji definiše 128-bitne adrese.

- Iako predstavlja dugoročno rešenje i iako je usvojen pre 20 godina proces prelaska na IPv6 i dalje traje i većina uređaja na mreži i dalje koristi IPv4. Kako?

NAT (Network Adress Translation)

- NAT (Network Address Translation) predstavlja međurešenje koje je trebalo da omogući funkcionisanje Interneta pre potpunog prelaska na IPv6. Ironija je da je upravo NAT značajno usporio prihvatanje IPv6.

- Osnovna ideja NAT-a je da se IP adrese podele na skup lokalnih i javnih IP adresa.

- Lokalne IP adrese se dodeljuju samo računarima u okviru lokalne mreže. Ove adrese ne moraju biti jedinstvene, što znači da dva različita uređaja mogu imati istu lokalnu IP adresu ukoliko pripadaju različitim lokalnim mrežama.

- Javne IP adrese se koriste za komunikaciju na Internetu. One su jedinstvene i svaki paket koji se nađe van lokalne mreže mora sadržati isključivo javne IP adrese.

Lokalne IP adrese

- Za lokalne IP adrese rezervisana su sledeća 3 opsega:

10.0.0.0/8 – 16 777 216 adresa

172.16.0.0/12 – 1 048 576 adresa

192.168.0.0/16 – 65 536 adresa

- **Lokalne adrese se koriste isključivo za adresiranje računara u okviru lokalne mreže i ne smeju se koristiti na Internetu.** Većina rutera na mreži zapravo odbacuje pakete koje sadrže adrese iz lokalnog opsega.

NAT - funkcionisanje

- Osnovna ideja NAT-a je da se svi računari unutar lokalne mreže adresiraju korišćenjem lokalnih IP adresa dok se javne IP adrese koriste samo za komunikaciju van lokalne mreže.

- Uloga NAT uređaja (koji obično predstavlja deo rutera) je da pre prosleđivanja paketa na Internet zameni adresu izvorišta javnom IP adresom koja je dobijena od pružaoca Internet usluga. Na ovaj način se obezbeđuje da veliki broj računara iz lokalne mreže pristupa Internetu preko malog broja javnih IP adresa.

NAT - vrste

- **Statički NAT** – obavlja se 1 na 1 translacija između lokalne i javne IP adrese. Na ovaj način je računaru koji pripada lokalnoj mreži zapravo pridružena jedinstvena javna IP adresa. Statički NAT se koristi za servere i uređaje kojima je potrebno inicirati komunikaciju sa lokacija van lokalne mreže.
- **Dinamički NAT** – prilikom uspostavljanja veze sa Internetom, lokalnom računaru se dodeljuje javna IP adresa. Nije moguće da više računara istovremeno koristi istu javnu IP adresu.
- **Preklapajući NAT (NAT overloading)** – omogućava da veliki broj računara komunicira na Internetu preko malog broja javnih IP adrese. U tu svrhu se koristi adresa TCP/UDP porta i zbog toga se ova vrsta NAT-a naziva i PAT (Port Address Translation).

NAT - funkcionisanje

- Kada adresirani računar primi poruku, odgovor šalje na javnu IP adresu odredišta.

- Na koji način ruter zna kom računaru u okviru loklane mreže treba da prosledi poruku ako svi oni pristupaju Internetu preko iste javne IP adrese?

- Rešenje: Dodatna informacija o adresi izvorišta je sadržana u adresi porta na transportnom sloju (TCP/UDP).

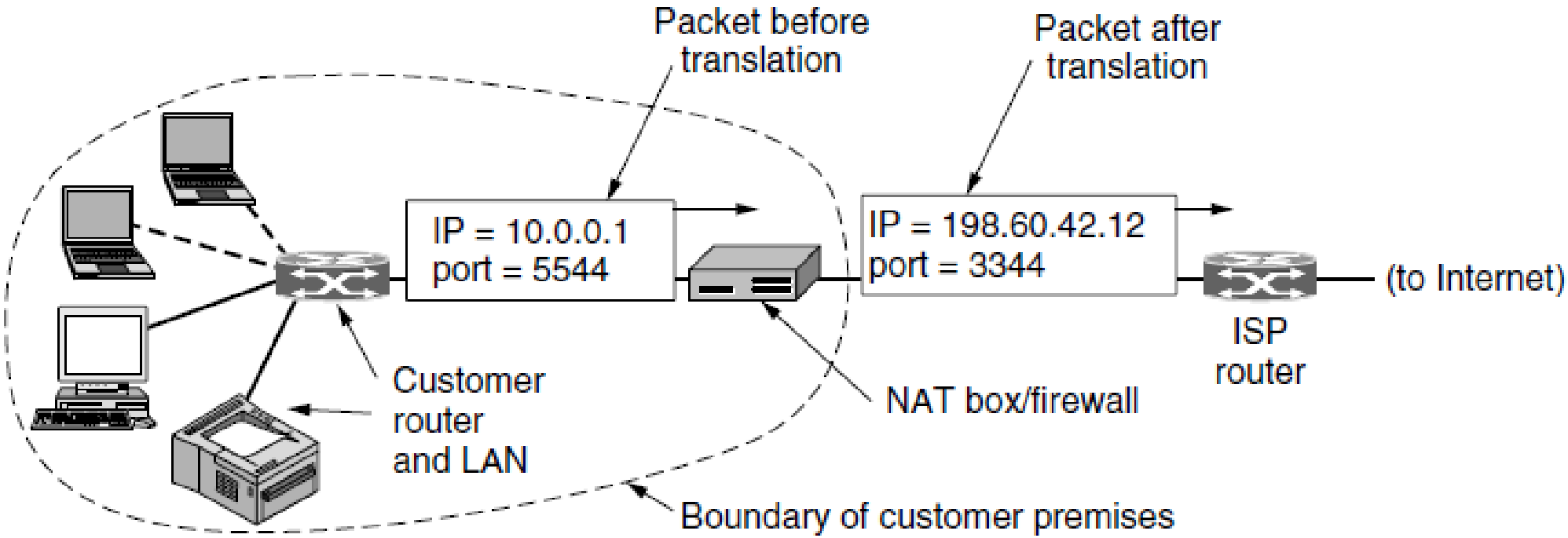
NAT/PAT - funkcionisanje

- Prilikom uspostavljanje komunikacije između dva procesa na transportnom sloju definiše se adresa porta koja će biti korišćena u komunikaciji. Adresa porta se predstavlja sa 16-bita.

- Prilikom napuštanja lokalne mreže, NAT uređaj umesto lokalne IP adrese i adrese porta u odlazni paket upisuje javnu IP adresu izvorišta i generiše novu adresu porta koja nije iskorišćena za neki drugi odlazni paket. Informacija o preslikavanju lokalne u javnu IP adresu se čuva u NAT uređaju kako bi se omogućilo ispravno prosleđivanje dolaznih paketa.

- Kako se sada za adresiranje koristi kombinacija IP adresa + adresa porta to se pomoću samo jedne javne IP adrese može ostvariti preko 60 000 konekcija (adresa porta 16 bita).

NAT/PAT - primer

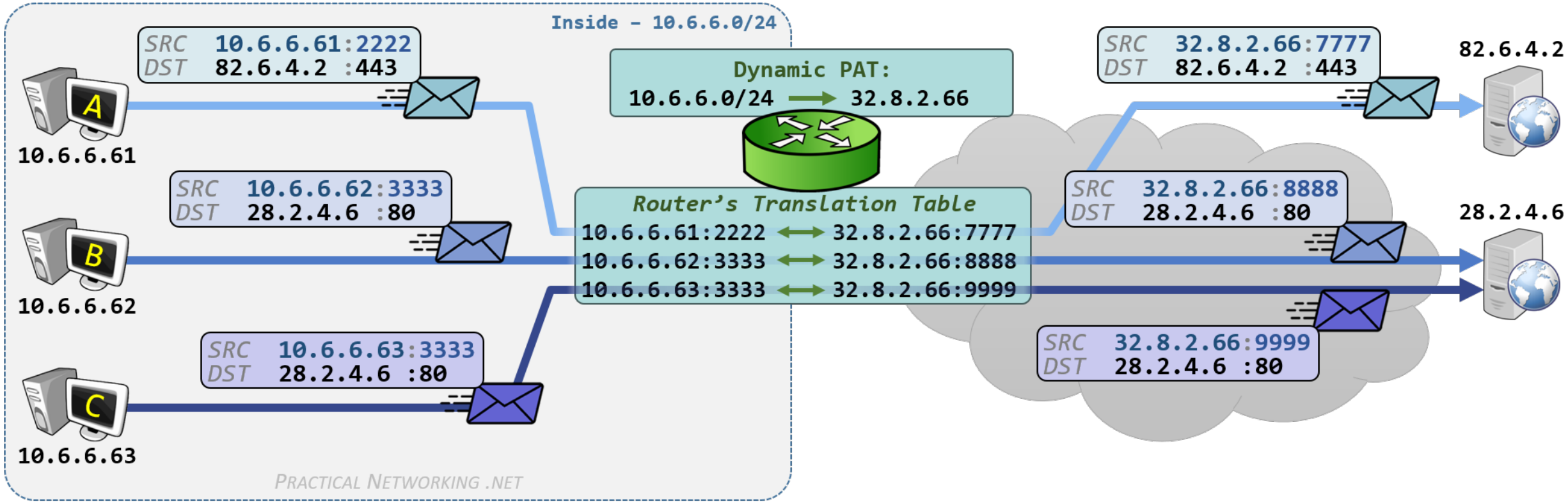


NAT/PAT - primer

- Računar iz lokalne mreže sa adresom 10.0.0.1 šalje poruku na Internet, pri čemu koristi adresu porta 5544. Prilikom prolaska kroz NAT uređaj ova izvoršna IP adresa i adresa priključka se menjaju javnom IP adresom 198.60.42.12 pri čemu se generiše i nova adresa porta 3344. **Generisanje nove izvorišne adrese priključka je neophodno kako bi se izbegla moguća preklapanja, jer procesi na različitim računarima unutar lokalne mreže mogu koristiti istu adresu izvorišnog porta.** Ova translacija adresa se čuva u NAT uređaju. Za svaki novi paket obavlja se identičan postupak.

- Server koji šalje odgovor u loklanu mrežu koristi za odredište javnu IP adresu 198.60.42.12 i adresu porta 3344. Nakon prolaska kroz NAT uređaj ove adrese se menjaju lokalnim adresama i poruka stiže na odgovarajuće odredište.

NAT/PAT primer 2



NAT/PAT

- Problemi sa NAT-om su mnogi.
- Uvođenjem lokalnih adresa izgubljena je jedinstvenost IP adresa koja predstavlja srž arhitekture Interneta.
- Lokalni korisnici pomoću NAT-a mogu pristupiti javnim serverima, međutim nije moguće inicirati komunikaciju sa računarom unutar lokalne mreže.
- Smanjena je pouzdanost s obzirom da sve konekcije zavise od tabele preslikavanja adresa koja se čuva u NAT uređaju. U slučaju gubitka ove tabele sve konekcije se automatski prekidaju.

DNS (Domain Name System)

- Sistem imenovanja domena DNS omogućava da se komunikacija između uređaja na mreži obavlja korišćenjem mnemoničkih umesto brojčanih adresa.

- Tako se na primer umesto korišćenjem adrese 147.91.14.197 stranici ETF-a može pristupiti pomoću adrese www.etf.bg.ac.rs.

- Pored lakšeg pamćenja same adrese, ukoliko se u budućnosti promeni IP adresa servera, pristup sajtu ETF se može obavljati preko iste mnemoničke adrese.

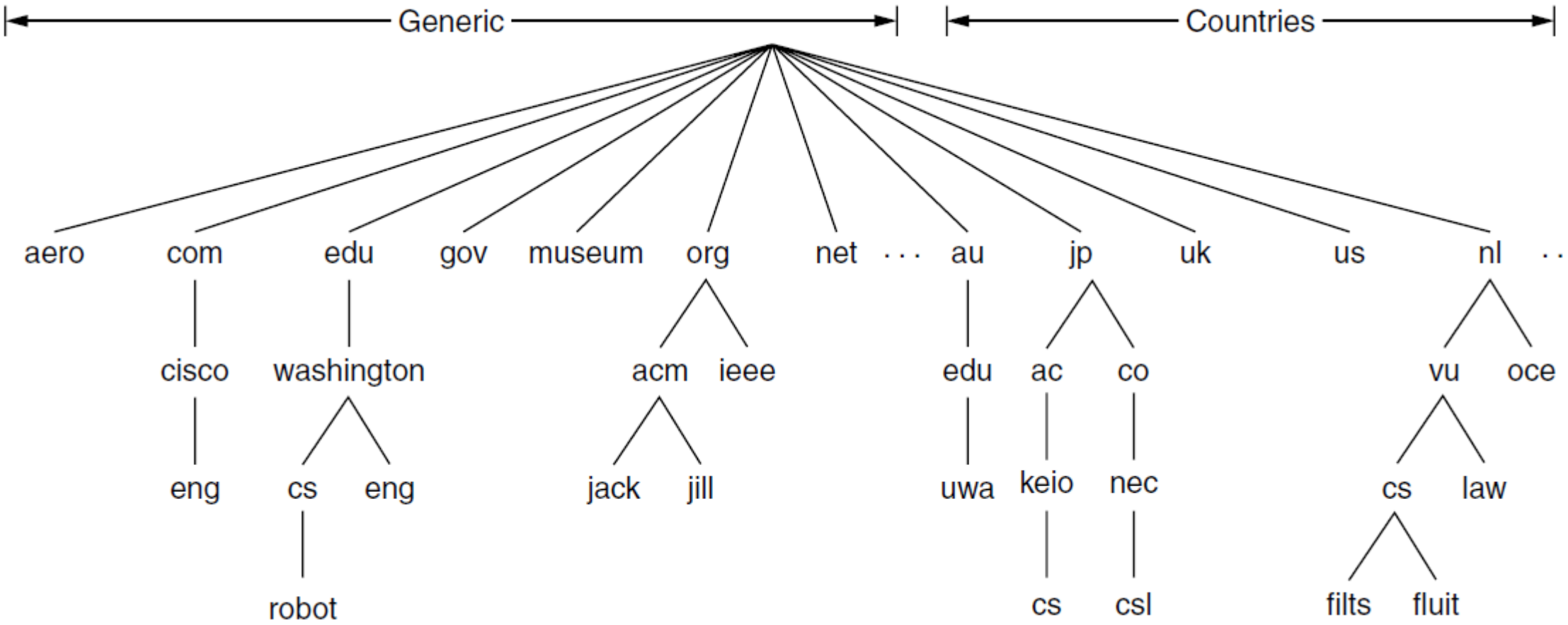
- DNS obezbeđuje preslikavanje mnemoničkih u mrežne IP adrese.

Organizacija imenskih domena

- Imenski domeni su organizovani hijerarhijski. Postoji preko 250 osnovnih domena koji označavaju određene delatnosti ili države. Ovi domeni se dele u poddomene i tako dalje.

- Na primer: etf.bg.ac.rs – Republika Srbija ima domen rs. Poddomen ac se koristi za akademske institucije. Poddomen bg u okviru domena ac označava da fakultet pripada Beogradskom Univerzitetu.

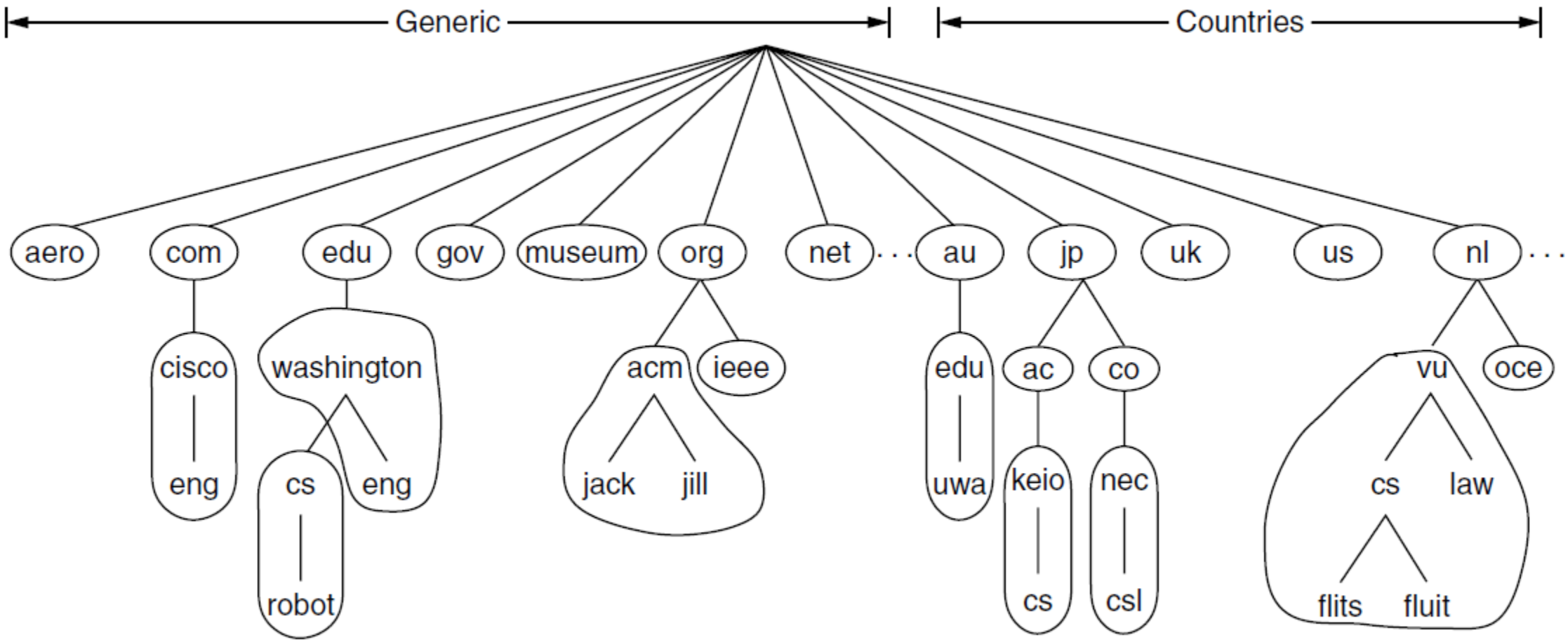
Organizacija imenskih domena



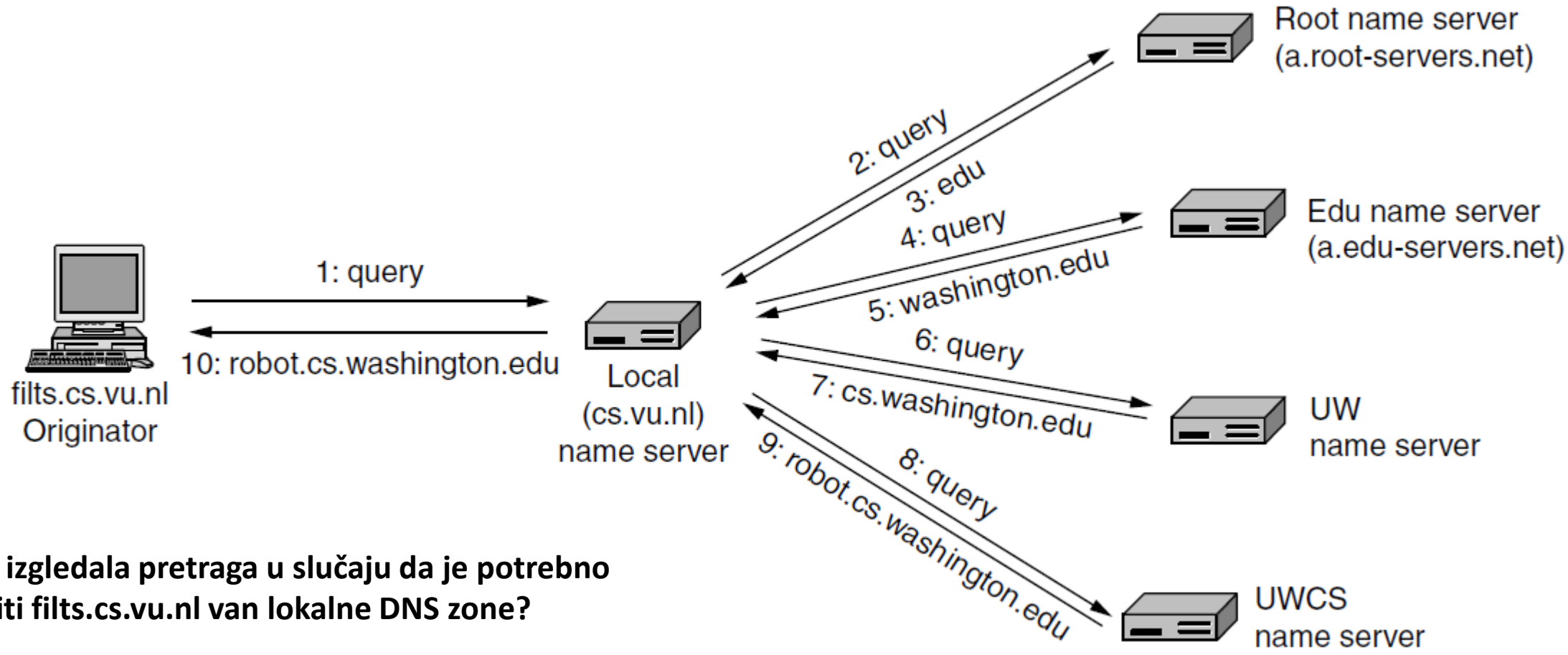
DNS serveri

- Kako bi se obezbedilo čuvanje velikog broja imena uređaja na mreži, imenski prostor je podeljenu više zona koje se međusobno ne preklapaju.
- Svaka zona ima primarni DNS server koji sadrži informacije na svom disku, a može imati i više sekundarnih DNS servera koji se obraćaju primarnom DNS serveru.
- **Svi računari koji koriste mnemoničke adrese moraju definisati adresu primarnog DNS servera.**
- Ukoliko traženi domen spada u zonu lokalnog DNS servera, odmah se šalje odgovor sa IP adresom. Ukoliko je domen van lokalne zone, DNS upit se šalje serveru imena osnovnog domena.

Primer podele na DNS zone



Razrešavanje adrese imena van lokalne zone



Kako bi izgledala pretraga u slučaju da je potrebno pristupiti filts.cs.vu.nl van lokalne DNS zone?

Razrešavanje adrese imena van lokalne zone

- Ukoliko je zahtevani domen van lokalne zone imena upit se šalje serveru osnovnog domena. Ovi serveri imaju adrese svih servera koji održavaju domene prvog nivoa poput: edu, com, gov, rs i sl. Svaki od servera u sebi sadrži adrese svih svojih poddomena. Na taj način se zapravo adresa razrešava hijerahijski kao što je prikazano na prethodnom primeru.

- Obratiti pažnju da DNS server ima informaciju o adresama svih svojih poddomena i svih domena u okviru lokalne zone.

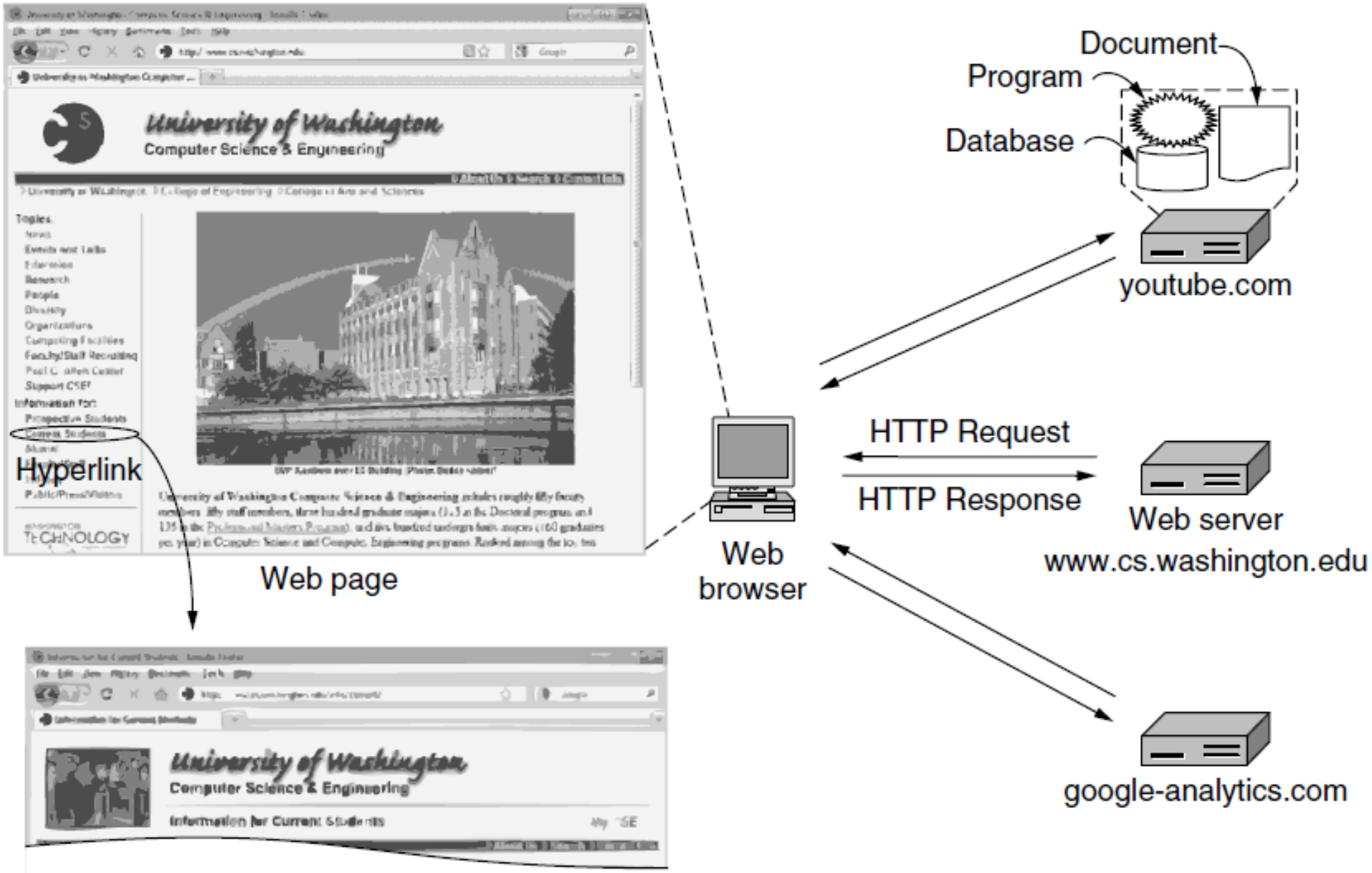
- Kako se razrešavanje adresa svodi na jednkoratno slanje zahteva i odgovora uspostavljanje veze bi predstavljalo gubitak vremena pa se u okviru transportnog sloja za DNS koristi UDP umesto TCP protokola.

World Wide Web

- Web predstavlja globalnu zbirku dokumenata zvanih Web strane. Na svakoj strani mogu postojati linkovi ka drugim stranama. Mogućnost da stranice pokazuju jedna na drugu naziva se hipertekst (*hypertext*).

- Za pristup stranicama koristi se HTTP protokol na sloju aplikacija. Kako je neophodno obezbediti da svi podaci ispravno budu prenesni da bi stranica bila ispravno prikazana u okviru transportnog sloje se koristi TCP protokol.

World Wide Web



URL – jedinstvene adrese resursa

- Svaka strana na Webu ima jedinstvenu adresu resursa URL (Uniform Resource Locator).

- U okviru ove adrese naveden je protokol na aplikativnom sloju koji se koristi, mnemonička adresa servera kao i adresa resursa u fajl sistemu servera.

- Primer: **http://tnt.etf.rs/~oe4pir/index.html**

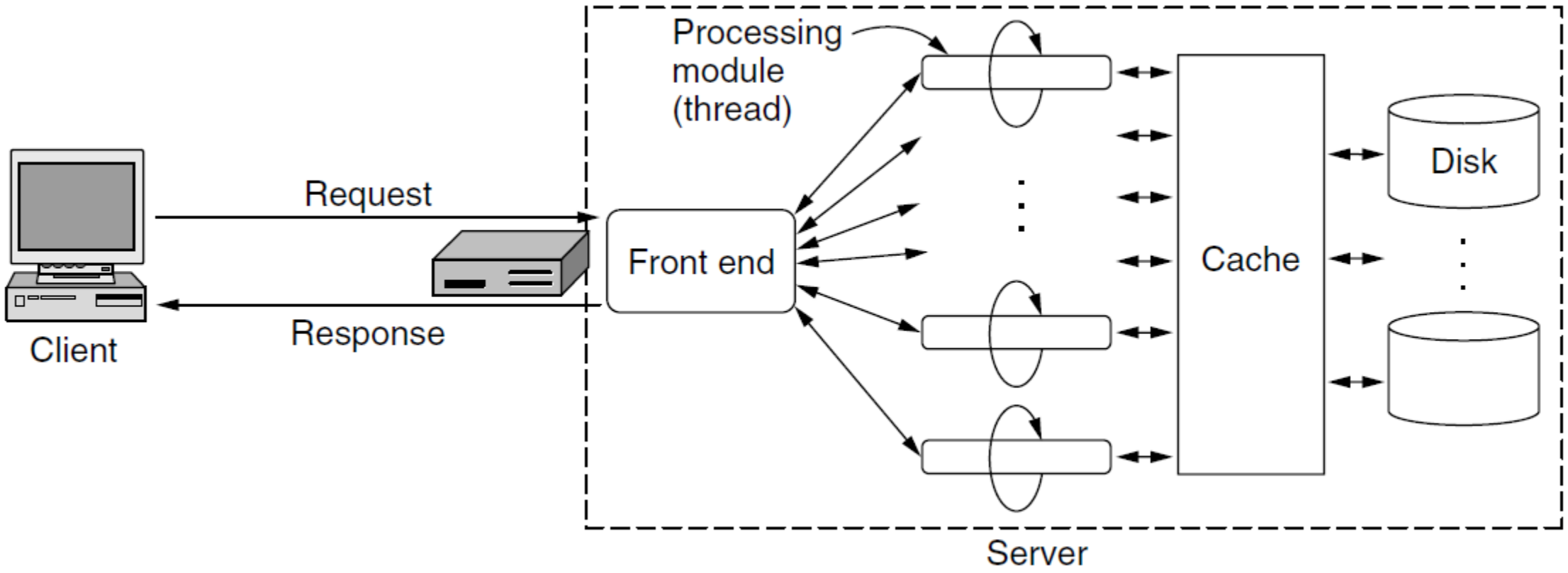
Pristup Web stranici sa strane klijenta

1. Najpre se upućuje zahtev DNS serveru kako bi se odredila IP adresa servera tnt.etf.rs.
2. DNS server vraća odgovor sa adresom 147.91.10.55.
3. Zatim se uspostavlja TCP veza sa portom 80 na računaru 147.91.10.55.
4. Nakon toga se šalje zahtev za fajl /~oe4pir/index.html
5. Server tnt.etf.rs šalje fajl /~oe4pir/index.html
6. TCP veza se raskida.
7. Čitač prikazuje sadržaj primljenog fajla.

Komunikacija sa strane servera

1. Server osluškuje odgovarajuće portove. U slučaju HTTP prenosa to je port 80.
2. Server prihvata uspostavljanje TCP veze inicirane od strane klijenta.
3. Prihvata podatak o lokaciji zahtevanog fajla.
4. Preuzima zahtevani fajl sa diska.
5. Šalje traženi fajl kiljentu.
6. Raskida TCP vezu.

Komunikacija sa strane servera



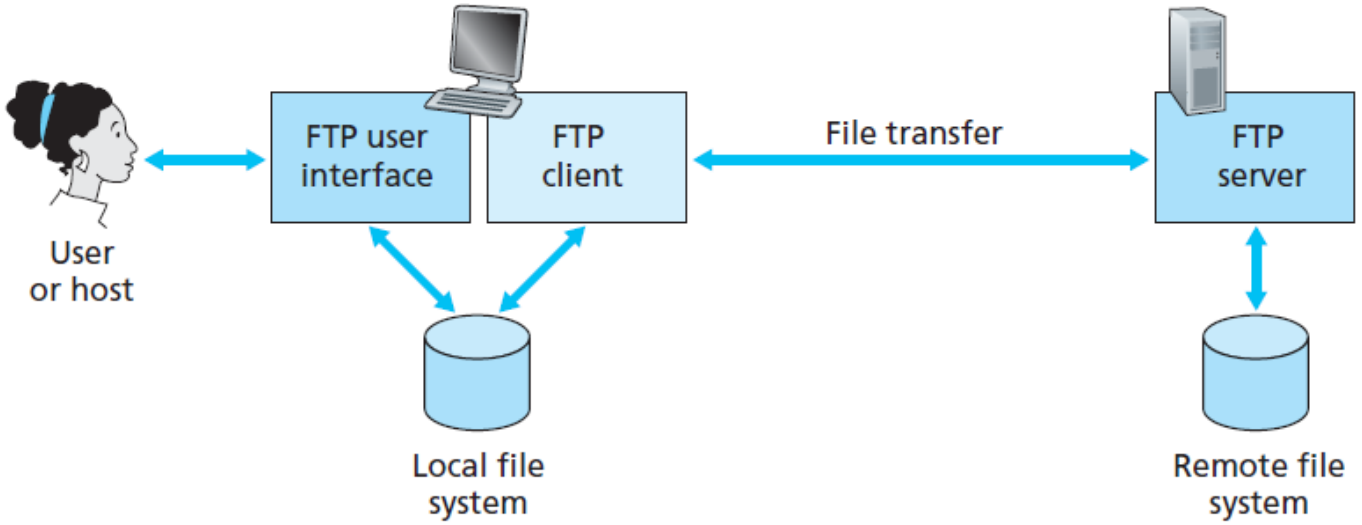
HTTP – privremene i trajne veze

- Nakon preuzimanja **index.html** stranice iz prethodnog primera klijent je u okviru ovog fajla naišao na linkove više fajlova koji sadrže slike. Kako bi se preuzele slike i ispravno prikazala stranica potrebno je ponovo uspostaviti vezu i obaviti prenos za svaki od navedenih fajlova.

- Prethodni pristup u kom se uspostavlja nova TCP veza za prenos svakog fajla naziva se privremena veza (non persistent connection). Problem sa ovim pristupom je taj što i za prenos najmanjih fajlova potrebno obaviti celokupnu proceduru uspostavljanja i raskidanja TCP veze što znatno usporava komunikaciju.

- HTTP protokol podržava trajne TCP veze. U ovom slučaju TCP veza ostaje otvorena i nakon ispravno primljenog fajla i na raspolaganju sa prenos ostalih fajlova. TCP veza se zatvara ukoliko neko duže vreme nije bilo razmene podataka po njoj, o čemu vode računa posebni tajmeri.

FTP (File Transfer Protocol)



FTP – protokol za prenos fajlova se koristi za razmenu fajlova između lokalnog računara i udaljenog servera.

Kako je neophodno obezbediti pouzdanu komunikaciju i prenos bez grešaka, FTP se na transportnom sloju oslanja na TCP.

FTP uspostavlja dve TCP veze. Veza na portu 21 se koristi za razmenu kontrolnih podataka. Kontrolna veza se prva uspostavlja i preko nje se šalju informacije poput korisničkog imena, šifre za pristup, komandi za prenos i sl. Veza na portu 20 se koristi za prenos podataka. Ova veza je privremenog tipa i raskida se nakon svakog prenesenog fajla.

FTP – tipične komande

- **USER** username – šalje se korisničko ime serveru
- **PASS** password – šalje se korisnička šifra serveru
- **LIST** – zahteva se da server pošalje listu fajlova u trenutno aktivnom direktorijumu
- **RETR** filename – zahteva se dohvatanje fajla sa servera
- **STOR** filename - zahteva se upisivanje fajla u trenutno aktivni direktorijum na serveru