Protokoli transportnog sloja TCP i UDP

Priprema za vježbu:

1) Koje su prednosti i nedostaci protokola TCP?

Prednosti TCP-a (Transmission Control Protocol) su:

Pouzdanost (TCP osigurava pouzdanu dostavu podataka, to znači da će sve poruke biti primljene ispravno, a ako dođe do gubitaka podataka, TCP će automatski retransmitirati izgubljene pakete)

Redoslijed (TCP održava redoslijed u kojem su podatci poslani i osigurava da će biti isporučeni u istom redoslijedu kako su poslani)

Kontrola zagušenja (TCP koristi različite algoritme za kontrolu zagušenja kako bi se osiguralo da se mrežni promet prilagođava trenutnim uvijetima mreže, smanjujući tako mogućnost zagušenja i gubitaka podataka

Potvrda primitka (acknowledgment) (TCP koristi mehanizam potvrde primitka kako bi osigurao da se podatci isporučuju na odredište i da je primatelj primio sve podatke)

Nedostatci TCP-a (Transmission Control Protocol) su:

Overhead (TCP dodaje dodatne zaglavlje informacija u svaki paket podataka radi osiguranja pouzdanosti i kontrole toka, što može dovesti do povećanog opterećenja mreže)

Sporiji od UDP-a (TCP je općenito sporiji od UDP-a (User Datagram Protocol), što je posljedica dodatne logike za kontrolu zagušenja, potvrde primitka i upravljanje vezama)

Veza uspostavljena (TCP zahtijeva uspostavljanje veze između pošiljatelja i primatelja prije nego što se mogu prenositi podatci, što može uzrokovati dodatno kašnjenje)

2) Koje su prednosti i nedostaci protokola UDP?

Prednosti UDP-a (User Datagram Protocol) su:

Brzina (UDP je brži od TCP-a jer nema složene kontrole toka, potvrde primitka ili mehanizama retransmisije podataka, što ga činim pogodnim za aplikacije koje zahtjevaju brzi prijenos podataka)

Manji overhead (UDP ima manje zaglavlje od TCP-a, što znači da troši manje resursa mreže, što ga čini učinkovitijim za prijenos malih paketa podataka ili aplikacija gdje je smajnje latencije važnije od pouzdanosti)

Jednostavnost (UDP je jednostavniji od TCP-a jer nema složenih mehanizama poput uspostavljanje veze, kontrole toka i retransmisije podataka)

Multicast i broadcast podrška (UDP podržava multicast i broadcast prijenos podataka, što omogućava slanje podataka jednom pošiljatelju koji ih zatim distribuira na više primatelja ili svim uređajima)

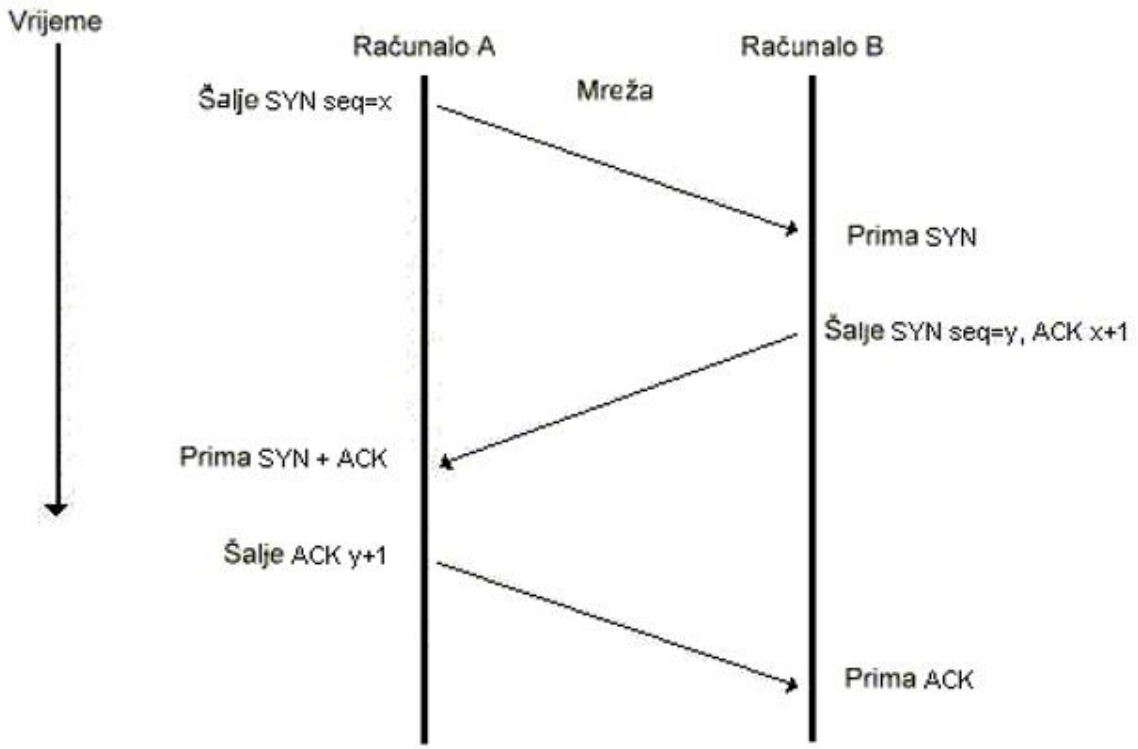
Nedostatci UDP-a (User Datagram Protocol) su:

Nepouzdanost (UDP ne generira pouzdanu dostavu podataka, što znači da podatci mogu biti izgubljeni ili isporučeni u pogrešnom redoslijedu bez upozorenja, a aplikacija je odgovorna za upravljanje tim problemima)

Nema kontrole toka (UDP nema mehanizme za kontrolu toka, što znači da primatelj ne može ograničiti brzinu prijenosa podataka, što može dovesti do preopterećenja mreže ili gubitka podataka u slučaju prevelikog opterećenja)

Nema potvrde primitka (UDP ne koristi potvrdu primitka, što znači da pošiljatelj ne zna je li primatelj primio podatke ili ne)

3) Skiciraj i objasni postupak uspostave TCP veze između klijenta i poslužitelja.



1. Zahtjev za uspostavu veze (TCP three-way handshake):

Klijent šalje paket prema poslužitelju (SYN) s postavljenim SYN bitom i određenim brojem sekvence (ISN - Initial Sequence Number) kako bi započeo uspostavu veze

Poslužitelj prima SYN paket, zatim odgovara klijentu s paketom koji sadrži potvrdu o SYN-u (SYN-ACK) s postavljenim SYN i ACK bitovima te s dodatnim brojem sekvence

Klijent prima SYN-ACK paket i potvrđuje potvrdu SYN-a poslužitelja (ACK). U ovom trenutku, veza je uspostavljena, a komunikacija može započeti

2. Rukovanje podacima:

Nakon uspostave veze, klijent i poslužitelj mogu početi razmjenjivati podatke. Podaci se šalju u paketima s postavljenim ACK bitovima kako bi se potvrdila ispravna primanja

3. Zatvaranje veze:

Nakon završetka komunikacije, bilo klijent ili poslužitelj može poslati FIN paket kako bi zatražio zatvaranje veze

Primatelj FIN paketa odgovara s ACK paketom kako bi potvrdio prijem FIN-a

Nakon toga, primatelj također šalje FIN paket kako bi zatražio zatvaranje veze sa svoje strane

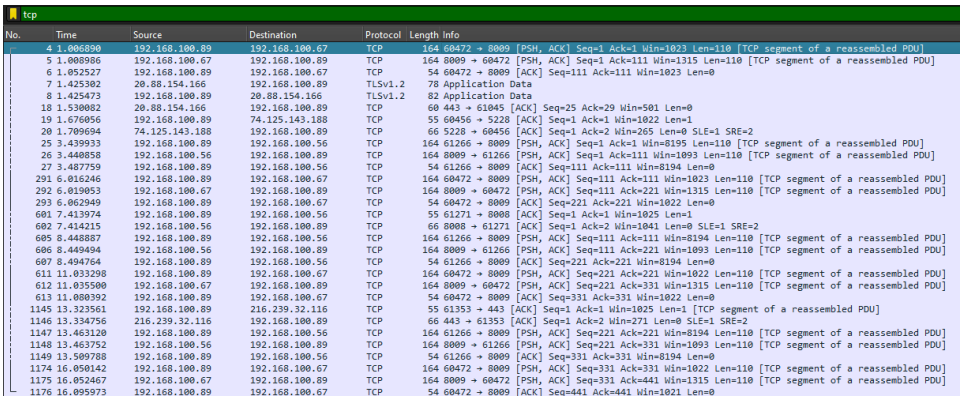
Po prijemu FIN paketa, pošiljatelj šalje ACK paket kao potvrdu zatvaranja veze

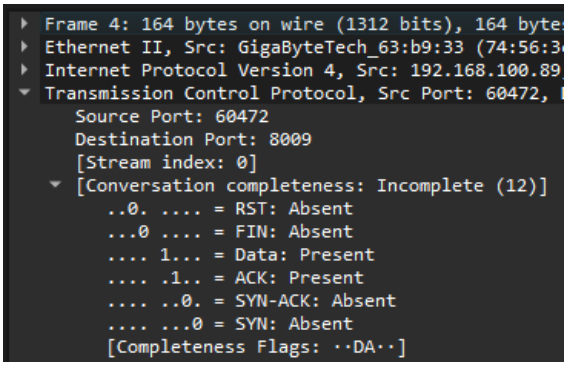
Veza je sada zatvorena

Izvođenje vježbe:

1) Analizirati zaglavlje odlaznih i dolaznih TCP segmenata

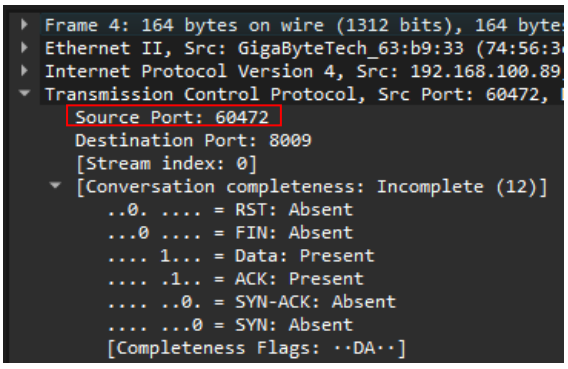
a) Pronaći segmente pomoću kojih se uspostavila veza između klijenta i poslužitelja (SYN, SYN-ACK, ACK).



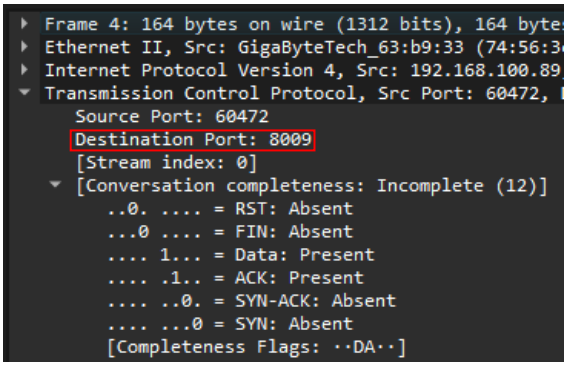


b) Pronađene segmente usporedite sa skicom iz pripreme, zadatak 3.

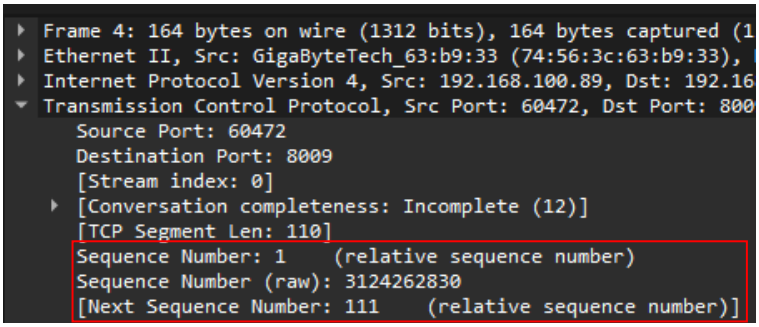
c) Koji je broj ishodišnog priključka (engl.port)?



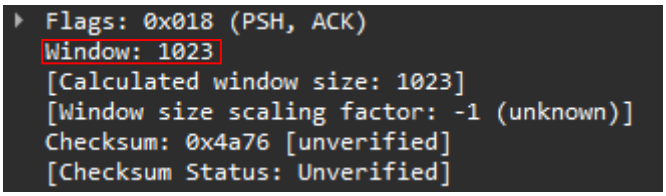
d) Koji je broj odredišnog priključka (engl.port)?



e) Pronađite brojeve koji označavaju redni broj segmenata (SEQ).

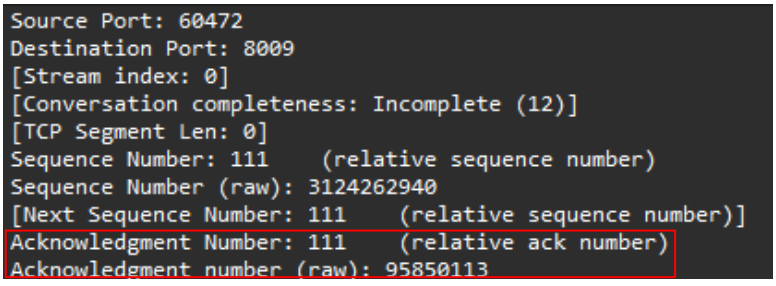


f) Čemu služi oznaka Win?



Primatelj koristi oznaku "Win" kako bi obavijestio pošiljatelja o trenutnom stanju prozora za prijem. Time se osigurava da pošiljatelj ne preplavi primatelja podacima koje ne može obraditi ili pohraniti odjednom

g) Pronađite brojeve koji označavaju potvrdu primljenog segmenta (ACK).



h) Koja su ostala polja TCP zaglavlja?

Osim polja za ACK i Win koje smo već spomenuli, TCP zaglavlje sadrži još nekoliko važnih polja koja pružaju različite informacije i funkcionalnosti

Source Port (Ishodišni priključak) (Ovo polje označava broj priključka s kojeg dolazi TCP segment, te taj broj pomaže primatelju da zna odakle dolazi podatak)

Destination Port (Odredišni priključak) (Ovo polje označava broj priključka na koji treba biti poslan TCP segment, te taj broj pomaže primatelju da zna na koji proces ili uslugu treba proslijediti podatak)

Sequence Number (Redni broj) (Ovo polje označava redni broj prvog bajta podataka u trenutnom TCP segmentu, te se koristi se za redoslijed i rekonstrukciju podataka na primatelju)

Header Length (Duljina zaglavlja) (Ovo polje označava duljinu TCP zaglavlja u riječima (4 bajta), te omogućuje primatelju da zna gdje završava zaglavlje i počinju podaci)

Reserved (Rezervirano) (Ovo polje je rezervirano za buduću uporabu i trenutno se postavlja na nulu)

Flags (Zastavice) (Ovo polje sadrži različite zastavice koje označavaju različite atribute ili stanja TCP segmenta. Primjeri zastavica uključuju SYN, ACK, FIN, RST, itd.)

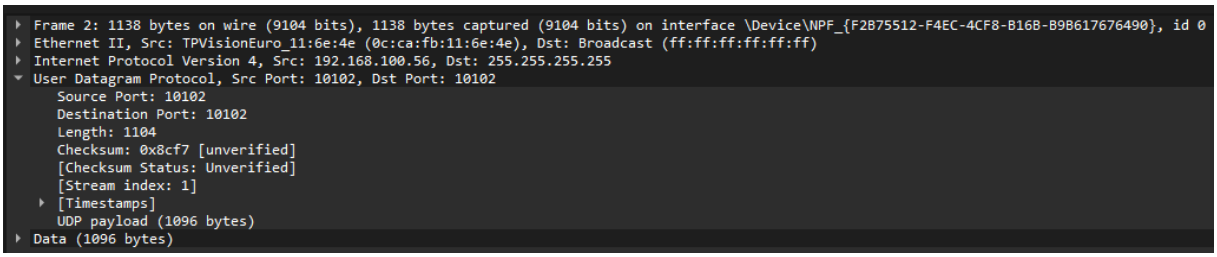
Window Size (Veličina prozora) (Ovo polje označava veličinu prozora za prijem, tj. koliko podataka primatelj može primiti prije nego što pošiljatelj mora pričekati potvrdu)

Checksum (Kontrolna suma) (Ovo polje sadrži vrijednost kontrolne sume koja se koristi za provjeru integriteta TCP segmenta, te to osigurava da podatci nisu bili oštećeni tijekom prijenosa)

Urgent Pointer (Pokazivač hitnosti) (Ovo polje označava položaj "hitnih" podataka unutar TCP segmenta, te se koristi za označavanje podataka koji zahtijevaju brzu obradu od strane primatelja)

2) Analizirati zaglavlje odlaznih i dolaznih UDP segmenata.

a) Pronaći UDP segmente.



b) Koje protokole enkapsulira UDP?

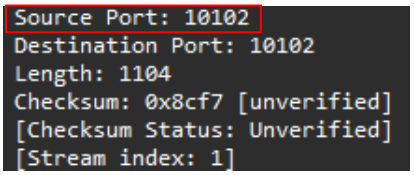
DNS (Domain Name System)

DHCP (Dinamic Host Configuration Protocol)

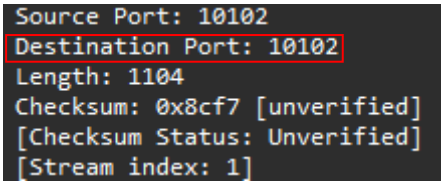
SNMP (Simple Network Management Protocol)

VoIP (Voice over IP)

c) Koji je broj ishodišnog priključka (engl.port)?



d) Koji je broj odredišnog priključka (engl.port)?



e) Koja su ostala polja UDP zaglavlja?

Ishodišni priključak (Source Port) (Ovo polje sadrži broj priključka (port) s kojeg dolazi UDP segment, te to omogućuje primatelju da zna odakle dolaze podatci)

Odredišni priključak (Destination Port) (Ovo polje sadrži broj priključka (port) na koji treba biti poslan UDP segment, te to omogućuje primatelju da zna kome su namijenjeni podatci)

Duljina (Length) (Ovo polje sadrži ukupnu duljinu UDP segmenta, uključujući i zaglavlje i podatke. Maksimalna vrijednost duljine je 65,535 bajtova, ali većina mrežnih implementacija ograničava stvarnu veličinu segmenta)

Checksum (Kontrolna suma) (Ovo polje sadrži vrijednost kontrolne sume koja se koristi za provjeru integriteta UDP segmenta. Kontrolna suma se izračunava na temelju sadržaja UDP segmenta i koristi se kako bi se osiguralo da podatci nisu oštećeni tijekom prijenosa)

3) Koja je uloga priključka u TCP i UDP segmentima?

U TCP i UDP segmentima, uloga priključka je identifikacija odredišnog i izvorišnog procesa na računalu

Ovo je važno za usmjeravanje podataka na pravo odredište na primateljskom računalu

Ishodišni priključak (Source Port):

U TCP segmentu (Označava priključak s kojeg dolazi TCP segment. Omogućuje primatelju da zna odakle dolaze podatci i na koji priključak treba poslati odgovor)

U UDP segmentu (Slično kao u TCP segmentu, ishodišni priključak označava priključak s kojeg dolazi UDP segment. Ovo omogućuje primatelju da zna odakle dolaze podatci i kako poslati odgovor)

Odredišni priključak (Destination Port):

U TCP segmentu (Označava priključak na koji treba biti poslan TCP segment. Omogućuje primatelju da zna kome su namijenjeni podatci i na koji priključak treba poslati odgovor)

U UDP segmentu (Slično kao u TCP segmentu, odredišni priključak označava priključak na koji treba biti poslan UDP segment. Ovo omogućuje primatelju da zna kome su namijenjeni podatci i kako poslati odgovor)

4) Za poznate protokole koje ste „ulovili“ navedite predefinirane brojeve priključaka (za TCP ili UDP)

HTTP (Hypertext Transfer Protocol):

TCP priključak: 80

HTTPS (Hypertext Transfer Protocol Secure):

TCP priključak: 443

DNS (Domain Name System):

UDP priključak: 53

FTP (File Transfer Protocol):

TCP priključak za kontrolu: 21

TCP priključak za podatke (aktivni način): 20

SSH (Secure Shell):

TCP priključak: 22

SMTP (Simple Mail Transfer Protocol):

TCP priključak: 25

POP3 (Post Office Protocol version 3):

TCP priključak: 110

IMAP (Internet Message Access Protocol):

TCP priključak: 143

Telnet:

TCP priključak: 23

SNMP (Simple Network Management Protocol):

UDP priključak: 161

Pitanja – Dodatno

1) Što je TCP?

TCP (Transmission Control Protocol) je jedan od glavnih protokola u Internet Protocol Suite (TCP/IP)

On omogućuje pouzdanu, uređenu i sigurnu komunikaciju između računala na mreži

TCP se koristi za većinu internetskih aplikacija koje zahtijevaju pouzdanu i sigurnu prijenos podataka, kao što su web preglednici, e-pošta, FTP (File Transfer Protocol) i mnoge druge

2) Koji protokoli aplikacijske razine koriste TCP?

HTTP (Hypertext Transfer Protocol) (Koristi se za prijenos web stranica i povezanih resursa preko interneta)

HTTPS (Hypertext Transfer Protocol Secure) (Sigurna verzija HTTP-a koja koristi SSL/TLS za šifriranje komunikacije)

FTP (File Transfer Protocol) (Koristi se za prijenos datoteka između računala na mreži)

SMTP (Simple Mail Transfer Protocol) (Koristi se za slanje e-pošte putem interneta)

POP3 (Post Office Protocol version 3) i IMAP (Internet Message Access Protocol) (Koriste se za pristup pošti na poslužitelju i preuzimanje e-pošte na klijentskom računalu)

SSH (Secure Shell) (Omogućuje sigurno upravljanje udaljenim računalima putem kriptirane veze)

Telnet (Omogućuje pristup udaljenom računalu putem terminala, ali nije siguran jer ne koristi enkripciju podataka kao SSH)

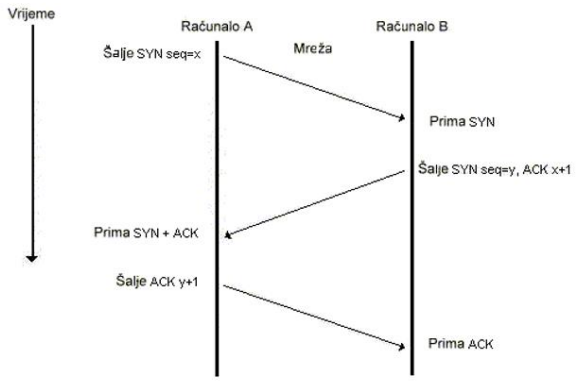
DNS (Domain Name System) (Koristi se za prevođenje domenskih imena u IP adrese i obrnuto)

3) Navedite dvije osnovne karakteristike TCP protokola?

Pouzdanost (TCP osigurava pouzdan prijenos podataka. To postiže segmentacijom podataka na manje dijelove, slanjem tih segmenata, praćenjem njihovog dolaska na odredište te ponovnim slanjem segmenata koji se izgube ili nisu ispravno primljeni. Ova karakteristika osigurava da podatci stignu na odredište bez grešaka i u pravilnom redoslijedu)

Kontrola toka (TCP kontrolira brzinu prijenosa podataka između pošiljatelja i primatelja kako bi spriječio preopterećenje mreže ili preopterećenje primatelja. To se postiže korištenjem mehanizma prozora, gdje primatelj šalje povratne informacije o tome koliko je podataka spreman primiti, a pošiljatelj prilagođava brzinu slanja podataka u skladu s tim. Ova kontrola osigurava učinkovit prijenos podataka i sprečava zagušenja u mreži)

4) Koje su faze procesa rukovanja kod TCP protokola? Opišite I nacrtajte dijagram.



1. Uspostavljanje veze:

Pošiljatelj šalje zahtjev za uspostavljanje veze (SYN)

Primatelj odgovara potvrdom (SYN-ACK) i također šalje zahtjev za uspostavljanje veze

Pošiljatelj potvrđuje prijem potvrde (ACK)

Sada je veza uspostavljena i podaci se mogu početi prijenositi

2. Prijenos podataka:

Pošiljatelj šalje segmente podataka

Primatelj potvrđuje prijem svakog segmenta

Ako neki segment nije primljen ili je oštećen, pošiljatelj ga ponovno šalje

Postupak se nastavlja sve dok svi podaci nisu preneseni

3. Zatvaranje veze:

Pošiljatelj šalje zahtjev za zatvaranje veze (FIN)

Primatelj potvrđuje prijem zahtjeva (ACK)

Primatelj zatim šalje svoj zahtjev za zatvaranje veze (FIN)

Pošiljatelj potvrđuje prijem zahtjeva (ACK)

Veza se sada zatvara

5) Što rade klijent i server tijekom postupka rukovanja? Što je ISN?

1. Klijent:

Inicira uspostavljanje veze slanjem zahtjeva za uspostavljanje veze (SYN)

Očekuje odgovor od poslužitelja (SYN-ACK)

Potvrđuje prijem SYN-ACK poruke (ACK)

Šalje podatke poslužitelju

Nakon završetka prijenosa podataka, može inicirati zatvaranje veze slanjem zahtjeva za zatvaranje veze (FIN)

Očekuje potvrdu od poslužitelja (ACK)

2. Poslužitelj:

Očekuje dolazak zahtjeva za uspostavljanje veze od klijenta (SYN)

Odgovara na zahtjev za uspostavljanje veze slanjem potvrde (SYN-ACK)

Očekuje potvrdu prijema SYN-ACK poruke od klijenta (ACK)

Prihvaća i obrađuje podatke koje šalje klijent

Može također inicirati zatvaranje veze slanjem zahtjeva za zatvaranje veze (FIN) nakon završetka komunikacije

Očekuje potvrdu od klijenta na svoj zahtjev za zatvaranje veze (ACK)

ISN (Initial Sequence Number) je početni broj sekvenca koji se koristi u TCP protokolu. To je slučajan broj koji se generira na početku svake TCP veze. ISN ima važnu ulogu u osiguravanju jedinstvenosti i pouzdanosti TCP veze. Slučajno generiran ISN pomaže u zaštiti od raznih napada, poput sinkronizacijskog napada (SYN flood attack), gdje bi napadač pokušao preplaviti poslužitelj velikim brojem SYN zahtjeva. Također pomaže u sprječavanju problema s redoslijedom paketa i duplikata tijekom prijenosa podataka

6) Objasnite generičke TCP parametre paketa.

Generički TCP (Transmission Control Protocol) paket sadrži nekoliko ključnih polja koja nose informacije potrebne za uspostavljanje i kontrolu komunikacije između klijenta i servera

1. Izvor (Source) i Odredište (Destination) IP adrese (Ova polja označavaju IP adrese pošiljatelja (klijenta) i primatelja (servera). Omogućuju usmjeravanje paketa preko mreže)

2. Izvorni (Source) i Odredišni (Destination) portovi (Portovi identificiraju odredišnu aplikaciju na računalu. Izvorni port označava port s kojeg paket dolazi, dok odredišni port označava port na koji je paket namijenjen na odredišnom računalu)

3. Sekvencijski broj (Sequence Number) (Ovo polje sadrži broj koji označava redni broj bajta u sekvenci podataka koji se prenose. To omogućuje primatelju da rekonstruira podatke u ispravnom redoslijedu)

4. Potvrdni broj (Acknowledgment Number) (Ovo polje sadrži broj koji označava sljedeći očekivani bajt koji će primatelj primiti. To omogućuje potvrdu primanja paketa i kontrolu toka)

5. Veličina prozora (Window Size) (Ova vrijednost označava broj bajtova koje primatelj trenutno može primiti bez potvrđivanja. To pomaže u kontroli toka i optimizaciji brzine prijenosa podataka)

6. Opcije (Ova polja mogu sadržavati dodatne informacije i opcije, poput maksimalne veličine segmenta (MSS), mogućnosti odgode potvrde (Nagle algoritam) i drugih parametara koji utječu na performanse i ponašanje veze)

7) Objasnite bar tri TCP zastavice.

SYN (Synchronize) (SYN zastavica se koristi tijekom procesa uspostavljanja veze između klijenta i servera. Kada klijent želi uspostaviti vezu s poslužiteljem, šalje paket s postavljenom SYN zastavicom. Ova zastavica signalizira poslužitelju da klijent želi uspostaviti vezu i obično sadrži i inicijalni sekvencijski broj (ISN) kako bi se započelo numeriranje podataka. Poslužitelj odgovara paketom koji također ima postavljenu SYN zastavicu, kao i ACK zastavicu (potvrda) i svoj inicijalni sekvencijski broj)

ACK (Acknowledgment) (ACK zastavica se koristi za potvrdu primljenih podataka. Kada primatelj primi TCP paket, postavlja ACK zastavicu u sljedećem paketu koji šalje natrag pošiljatelju. To signalizira pošiljatelju da je primljeno određeno potvrdno (ACK) polje u paketu i da je primatelj spreman primiti nove podatke ili potvrditi prijem sljedećeg paketa)

FIN (Finish) (FIN zastavica se koristi za zatvaranje veze. Kada jedna strana želi zatvoriti vezu, šalje TCP paket s postavljenom FIN zastavicom. To signalizira da je strana završila slanje podataka i da želi zatvoriti vezu. Primatelj odgovara ACK zastavicom kako bi potvrdio prijem FIN zahtjeva. Nakon toga, kada primatelj također završi slanje podataka i želi zatvoriti vezu, šalje paket s postavljenom FIN zastavicom. Ova razmjena zastavica omogućuje obe strane da sigurno zatvore vezu)