URM ISHODI 3 I 4

Kućar 2018

„Kratki“ sadržaj:

Transportni sloj

Transportni sloj je četvrti sloj OSI modela a treći sloj TCP/IP modela. On definira uloge i metode za uspostavu krajnje komunikacije između procesa pokrenutih na uređajima u mreži.

- Osnovne funkcije transportnog sloja su podjela poruke na segmente i prosljeđivanje tih segmenata procesima na aplikacijskom sloju. Podjela veće poruke na manje dijelove naziva se **segmentacija**. Transportni sloj prima podatke s aplikacijskog sloja, segmentira ih, enkapsulira sa zaglavljem protokola transportnog sloja i prosljeđuje na režu. Na primateljevoj strani transportni sloj spaja segmente ponovno u cjelinu i prosljeđuje podatak procesu na aplikacijskom sloju.
- Na računalu može biti pokrenuto više aplikacija istovremeno a kako bi se znalo o kojoj aplikaciji odnosno procesu se radi koristimo portove:
    - Well known ports - standardni poslužiteljski portovi nalaze se u **0-1023** rangu. Namijenjeni su standardnim Internet servisima. Protokoli HTTP, FTP, SMTP, POP, IMAP, Telnet etc.
    - Reserved ports – rezervirani portovi su unutar raspona **1024-49151.** Ovi portovi su namijenjeni vlasničkim servisima kojima se nudi mogućnost registracije. To su aplikacijski protokoli pojedinih programa i servisa na internetu stvorenih od strane privatnog poduzeća.
    - Dynamic ports – dinamički portovi su portovi unutar raspona **49152-65535.** Ovi portovi se ne mogu registrirati i namijenjeni su za slobodno korištenje po potrebi.

Na transportnom sloju prepoznajemo dva osnovna protokola, **TCP** i **UDP**.

UDP – User Datagram Protocol je jednostavniji od TCP protokola. Ne uspostavlja vezu (connectionless je) i ne garantira isporuku (unreliable). Prijenosi podataka poput video konferencija zahtijevaju primarno brzinu a pouzdanost nije toliko bitna i u takvim slučajevima se koristi UDP. Također se koristi i kod protokola DNS i DHCP jer je potrebna brzina a količina podataka je premala da bi se brinulo o uspostavi veze i provjere ispravnosti tijeka podataka.

TCP – Transmission Control Protocol je jedan od najčešće korištenih protokola transportnog sloja. Temeljna zadaća mu je uspostava krajnje komunikacije između aplikacija (Connection oriented) odnosno servisa aplikacijskog sloja. TCP je pouzdan protokol koji uspostavlja i održava vezu između krajnjih uređaja. Provjerava ispravnost i upravlja tijekom prijenosa podataka. Cijena pouzdanosti je brzina.

Mrežni sloj

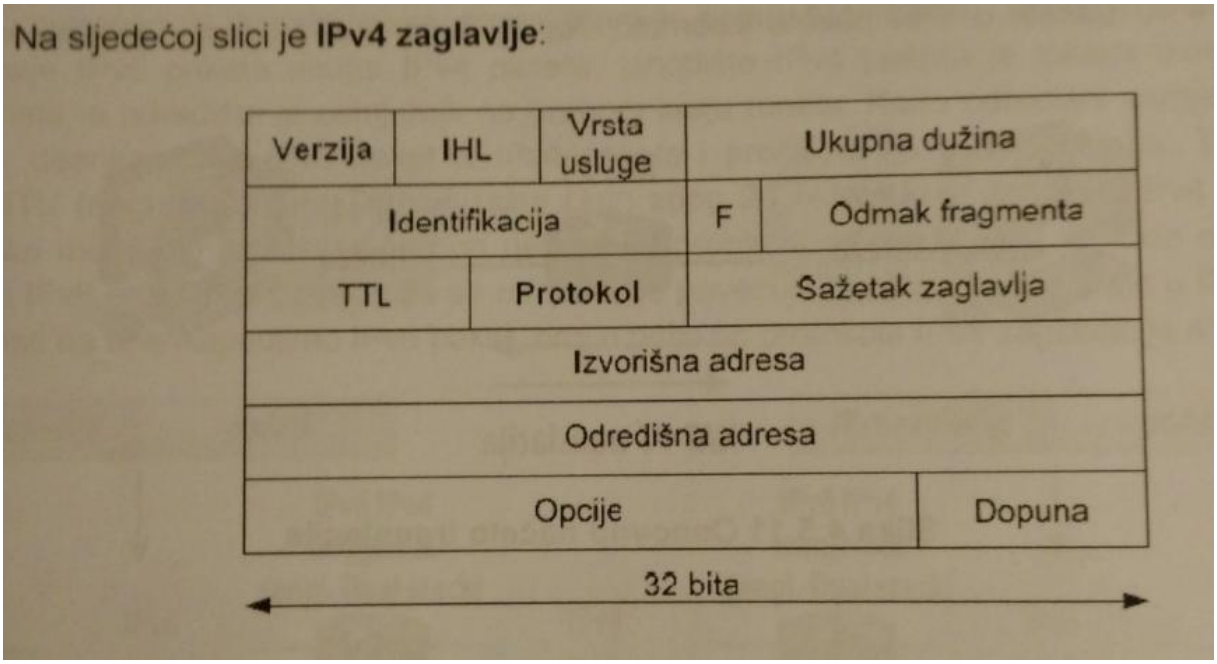
Mrežni sloj obavlja sljedeće zadatke:

- adresiranje paketa pomoću ishodišne 1 odredišne IP adrese
- enkapsulacija, odnosno dodavanje IP zaglavlja
- usmjeravanje paketa (engl toutłng) ili pronalaženje najboljeg puta do odredišta
- deenkapsulacija, odnosno skidanje IP zaglavlja na odredištu.

Protokol IPv4 opisuje strukturu zaglavlja kojim se enkapsuliraju UDP TCP segmenti transportnog sloja

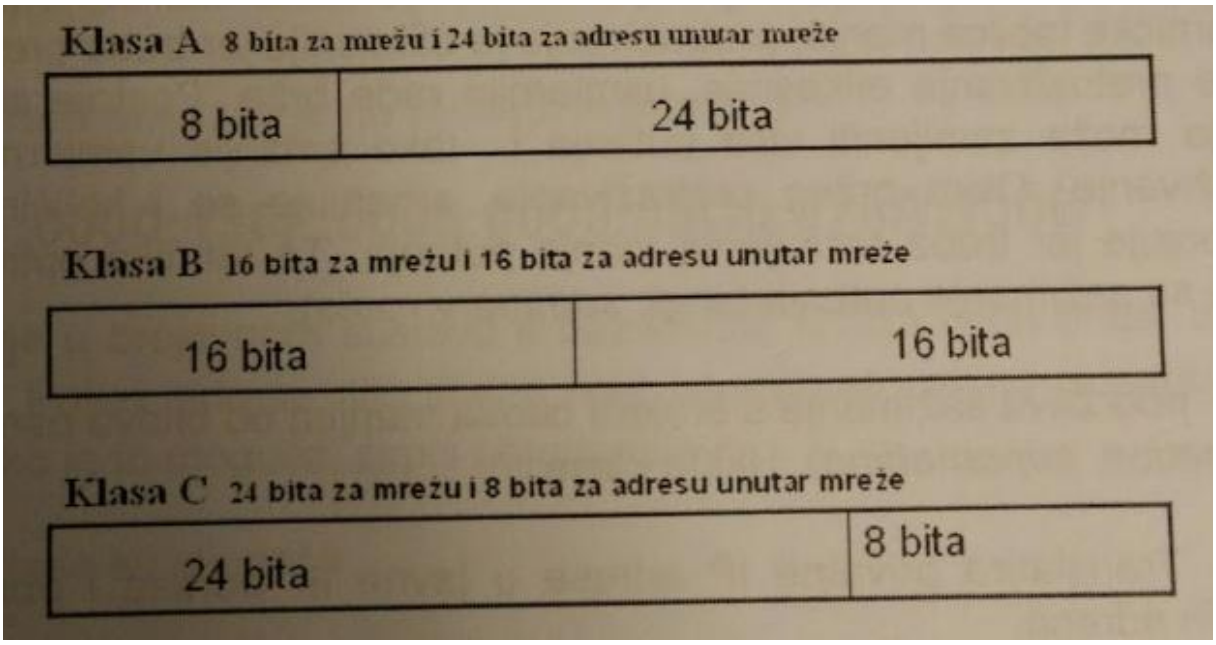
Osnovne značajke protokola IPv4 su:

- Ne uspostavlja se veza između ishodišta i odredišta prije slanja paketa (engl connectionless)
- Najbrža moguća usluga (engl. Best effort) — nema dodatnih kontrolnih paketa koji bi garantirali isporuku paketa. To mu omogućuje najbrži mogući način, prijenosa paketa od ishodišta do odredišta. Cijena brzine je nepouzdanost
- Nezavisan od vrste medija za prijenos podataka (engl. Media indepedent).



Fragmentiranje paketa - hardverske osobine uređaja na mreži definiraju između ostalog i najveću količinu podataka koju neki uređaj smije poslati na mrežni medij za prijenos podataka unutar jednog okvira (engl. Frame). Ova veličina naziva se Maximum Transmission Unit — MT U i ovisi o mrežnoj tehnologiji drugog sloja. Ako je paket veći od dozvoljene veličine, fragmentira se, odnosno cijepa na više manjih paketa. Na odredištu se opet fragmenti spajaju u izvorni paket.

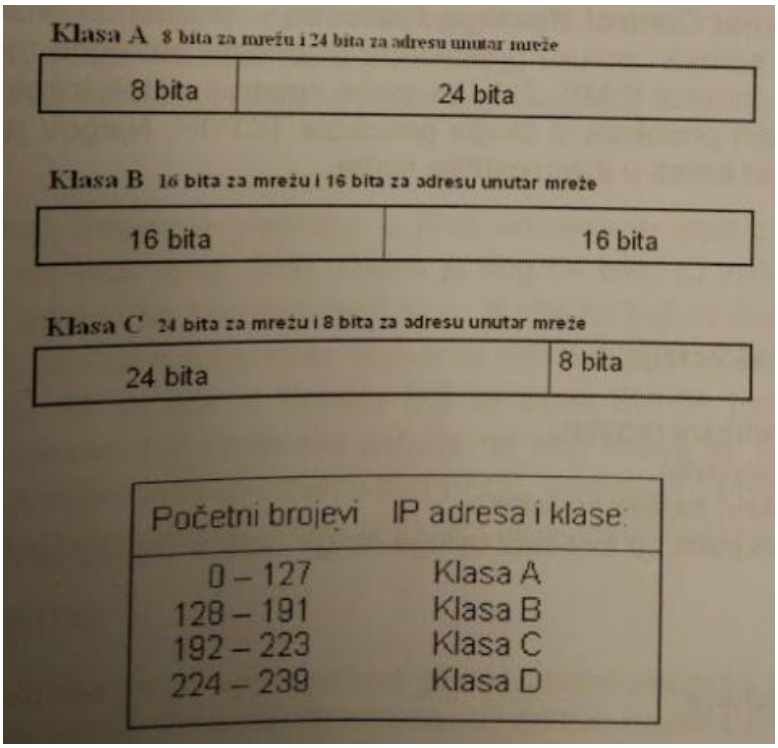
IP adresa - svaki uređaj u mreži mora biti jednoznačno definiran, odnosno mora imati svoju adresu. Ta adresa se u TCP/IP skupu protokola zove IP adresa. Sastoji se od četiri broja odvojena točkom. Brojevi mogu biti u intervalu od O do 255. Primjer IP adrese je 192.120.234.11. Dužina IP adrese u binarnom obliku je 32 bita. Svakih osam bita je jedan broj. IP adresa sastoji se od mrežnog dijela i tzv. host dijela. Mrežni dio definira logičku mrežu u kojoj se uređaj nalazi, a host dio definira adresu unutar mreže. Osnovna podjela mrežnog i host dijela je podjela na klase. Podjelu na klase prikazuje sljedeća slika:



Postoje tri osnovna tipa IP adresa.

- Jednoodredišne adrese (engl unicast) adrese,
- broadcast adrese,
- grupne adrese (engl. Multicast)

Mreže unutar Interneta su podijeljene na klase: A,B,C,D i E. Ovisno u kojoj klasi se IP adresa nalazi, određeni broj bitova se dijeli na mrežni dio adrese i dio za adresu računala u toj mreži. Dakle, klasa definira mrežni dio adrese.



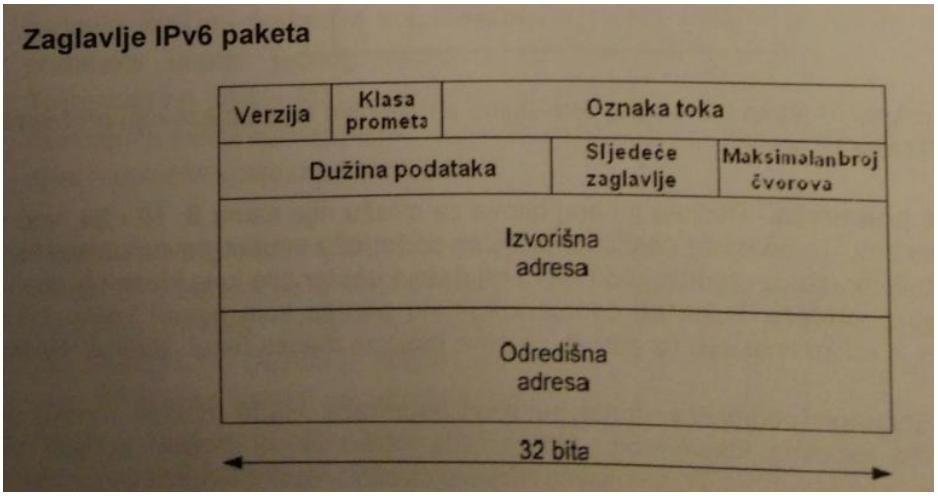
Da bi se potrošnja IP adresa smanjila, osmišljene su tehnike koje ublažavaju probleme koji uzrokuje prekratka IP adresa.

- **Stvaranje podmreža** - Podjela na broj bitova za mrežu nije samo 8, 16 i 24, već može biti bilo koji broj. To se može postići stvaranjem podmreža unutar glavne mreže klase A, B ili C. Bitovi mreže se produžuju od lijevo na desno unutar bilo koje klase i pomoću njih se stvaraju podmreže. Sada se dodaje još jedna adresa koja govori koliko bitova je mrežni dio, a koliko host dio. Ta adresa se zove mrežna maska (engl. Subnet maska).
- **VLSM** — Stvaranje podmreža unutar neke od podmreža. Sada mrežne maske unutar neke mreže osnovne klase mogu biti različite. Kako bi se mogao koristiti VLSM, usmjernički protokoli moraju dozvoljavati različite mrežne maske u mreži. Sloj podatkovne veze
- **Sažimanje putanja** - poželjno je da usmjernićke tablice budu što manje. Sto su usmjernitke tablice manje, pretraživanje je efikasnije jer treba pretraživati manje putanja. Ako je pretraživanje efikasnije, usmjernici rade brže Postoje situacije u kojima jedna putanja može zamijeniti više putanja i tako smanjiti usmjerničku tablicu te ubrzati pretraživanje. Osim bržeg pretraživanja, smanjuje se i količina informacija koja se razmjenjuje jer treba razmijeniti manje putanja, Ta tehnika optimiziranja broja putanja naziva se sažimanje putanja (engl. summary route).
- **CIDR** - podržava sažimanje s brojem bitova manjim od bitova osnovne klase (engl. route aggregation, supernetting). Ukida klase.
- **NAT** — Translatira privatne IP adrese u javne IP adrese i obrnuto. Na slici je skup privatnih adresa.
- **ICMP (engl. Internet Control Message Protocol) -** Budući da protokol IP nema ugrađen sustav kontrolnih poruka i poruka grešaka pri prijenosu, potrebna mu je pomoć. Taj posao za njega obavlja protokol ICMP. Zato se može smatrati potprotokolom protokola IP. ICMP je jedan od važnijih protokola iz skupa protokola TCP/IP. Njegov je posao slanje poruka. Zbog toga se često koristi u dijagnostičke svrhe.

IPv6

Bitne novosti IPv6 verzije su:

- mnogo veći adresni prostor,
- novi format zaglavlja,
- ugrađeni sustavi zaštite podataka, poboljšana podrška za kvalitetu usluge (engl. QoS — Quality of Service),
- proširivost.



Sloj podatkovne veze

Na OSI sloju veza dolazi do enkapsulacije paketa s trećeg sloja u okvir i naravno, u obrnutom slučaju, deenkapsulacije okvira u paket trećeg sloja. Na sloju veza, oblik okvira definira odabrana mrežna tehnologija.

Sloj podatkovne veze (engl. Data Link Layer) upravlja pristupom mediju. U računalnim mrežama postoje dva osnovna načina povezivanja uredaja: točka prema točki (engl. Point to Point), dijeljeni medij (engl. Shared Medium).

Komunikacija između dva mrežna uredaja je obično dvosmjerna i ta dvosmjernost može biti izvedena na dva načina:

- Half Duplex,
- Full Duplen

Half Duplex komunikacija je izvedba u kojoj se komunikacija Odvija uvijek u jednom smjeru bez obzira na dvosmjerne medije za prijenos podataka za svaki smjer. Full duplex je komunikacija u oba smjera istodobno.

Mrežna Topologija je način povezivanja uređaja i kablova u računalnu mrežu. Kada govorimo 0 topologiji, bitno je razlikovati fizičku topologiju od logičke topologije.

- Fizička topologija prikazuje kako su uređaji fizički spojeni medijem (fizički izgled).
- Logička topologija prikazuje na koji način uređaji komuniciraju, točnije prikazuje protok podataka mrežom.

Ethernet je standard za lokalne mreže.

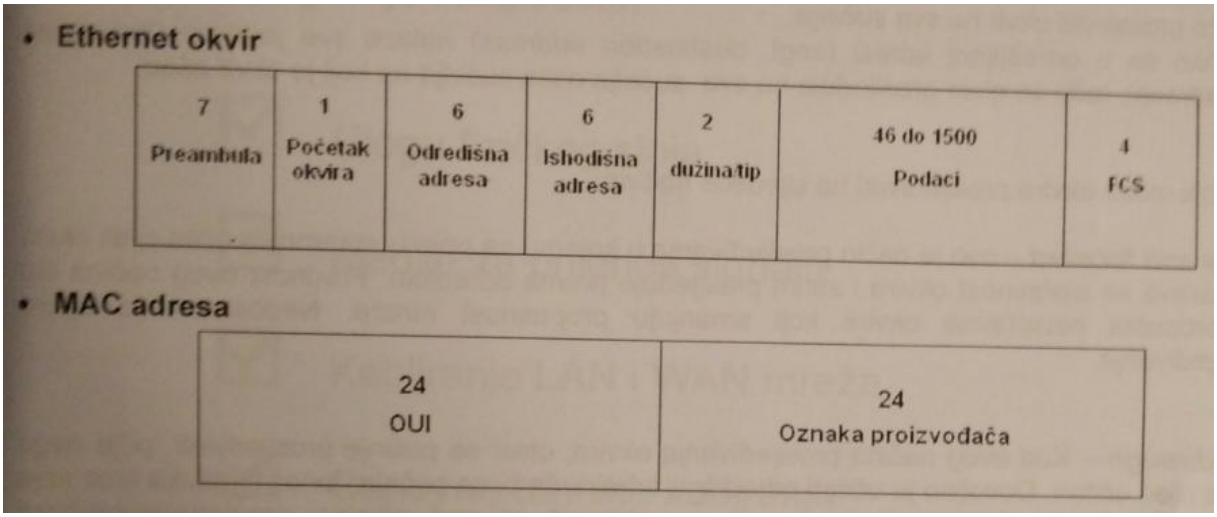
CSMA/CD - Logička topologija Ethernet mreže je broadcast. Svi uredaji koji se nalaze u mreži natječu se za prijenos podataka. Svaki uredaj osluškuje signale na mediju za prijenos podataka i ako je medij slobodan šalje podatke. Ostali uređaji uočavaju da je medij zauzet i čekaju da se medij oslobodi. Zbog dužine medija za prijenos podataka i realnog vremena potrebnog da signal s jednog kraja medija dode do drugog kraja, može doći do situacije u kojoj dva ili više uređaja misle da je medij za prijenos podataka slobodan. U tom slučaju istodobno šalju podatke na medij i dolazi do kolizije signala. Ako dode do kolizije, mrežni adapteri koji su pokušali slati podatke uočavaju koliziju i povlače se s medija. Nakon toga u različitim vremenima unutar predefiniranog vremenskog intervala pokušavaju ponovno. Sustav koji upravlja slanjem podataka na medij za prijenos podataka i rješavanjem kolizije (ako se dogodi) zove se CSMA/CD (engl. carrier sense multiple access/collision detect).

Kolizijska domena - Vjerojatnost da dode do kolizije signala povećava se s brojem uredaja na jednom Ethernet segmentu. Ethernet segment unutar kojega može doći do kolizije zove se kolizijska domena.

Broadcast domena - To je područje unutar kojega se razmjenjuju broadcast poruke. Preklopnik kao uređaj smanjuje kolizijske domene, ali dozvoljava broadcast promet. Preklopnik nije granica za broadcast promet. LAN mreža s preklopnicima je jedna broadcast domena (pod uvjetom da se ne stvaraju VLAN mreže).

U mrežama s preklopnicima moguće su tri vrste komunikacije: unicast, multicast, broadcast.

Unicast komunikacija je kad samo jedan uredaj šalje podatke i samo jedan uređaj podatke. Primjeri unicast komunikacije su HTTP, SMTP, Telnet i drugi protokoli. **U multicast** komunikaciji jedan uredaj šalje podatke, a grupa uredaja prima podatke. Primjer multicast komunikacije je slanje slike i zvuka na više odredišta u mreži. **Broadcast komunikacija** je kada jedan uređaj šalje podatke svim uredajima na mrežnom segmentu. Primjer broadcast komunikacije su protokoli ARP i DHCP.



Kašnjenje u mreži

Kašnjenje u Ethernet mreži (engl. network latency) je vrijeme potrebno Ethernet okviru da stigne od ishodišnog mrežnog adaptera do odredišnog mrežnog adaptera. Do kašnjenja dolazi zbog tri uzroka: -

- Vrijeme potrebno da ishodišni mrežni adapter postavi signal na medij za prijenos podataka i vrijeme potrebno da odredišni mrežni adapter interpretira te signale.
- Vrijeme potrebno da signal prijede put od ishodišnog mrežnog adaptera do Odredišnog mrežnog adaptera.
- Kašnjenje u uređajima kroz koje signal prolazi

Zagušenje u mreži

Najčešći uzroci zagušenja u mreži su:

- Današnja tehnologija u krajnjim uređajima (procesori, sabirnice, periferni uredaji...) šalje sve veću količinu podataka u određenom vremenu u mrežu.
- Broadcast poruke kao što su poruke protokola ARP imaju utjecaja na rad mrežnih uređaja i krajnjih uređaja u mreži. Uredaji moraju otvoriti broadcast poruke, kada i nisu namijenjene njima.
- Mrežne aplikacije zahtijevaju sve veću širinu pojasa (engl. bandwidth) jer moraju otvoriti sve veću količinu podataka. Primjeri takvih aplikacija su video aplikacije (engl. video on deman), učenje preko mreže (engl. e-learning) i mnoge druge.

Osnovna načela rada preklopnika

Ako preklopnik primi okvir na nekom od portova. napravit će sljedeće:

- Pročitat će ishodišnu adresu u okviru.
- Ako se adresa ne nalazi u MAC tablici, upisat će u MAC tablicu ishodišnu MAC adresu i broj sučelja na koji je okvir ušao (engl. frame) Na taj način dinamički popunjava tablicu i ući koje su adrese na kojem sučelju.
- Pročitat će odredišnu adresu u okviru
- Potražit će tu adresu u MAC tablici i pogledati koje sučelje je pridruženo toj adresi. Proslijedit će okvir samo na to sučelje.
- Ako u MAC tablici ne postoji adresa koja je jednaka odredišnoj adresi u okviru, preklopnik de proslijediti okvir na sva sučelja.
- Ako se u odredišnoj adresi (engl. destination address) nalaze sve jedinice (broadcast adresa), tada se okvir prosljeđuje na sva sučelja osim sučelja na koji je okvir ušao.

Preklopnik može okvire prosljeđivati na sljedeće načine:

Store and forward — ovo je način prosljeđivanja u kojemu se prvo u spremnike učita cijeli okvir, provjerava se ispravnost okvira i zatim prosljeđuje prema odredištu. Prednost ovog načina što ne propušta neispravne okvire koji smanjuju propusnost mreže. Nedostatak je sporo prosljeđivanje.

Cut-through — Kod ovog načina prosljeđivanja okvira, okvir se počinje prosljeđivati prije nego što je cijeli učitan. Dovoljno je učitati odredišnu adresu da bi se počela donositi odluka kroz koje sučelje proslijediti okvir. Kod ovog načina preklopnik ne radi nikakvu provjeru ispravnosti prijenosa. Propušta neispravne okvire koji dalje putuju mrežom i uništava ih tek mrežni adapter na odredištu. Prednost mu je brzina, a nedostatak propuštanje neispravnih okvira. Postoje dvije varijante ovog načina prosljeđivanja okvira:

Fast forward — tipična cut-through metoda. Okvir se prosljeđuje odmah nakon učitane odredišne adrese. To je najbrža metoda, ali loša strana joj je što prosljeđuje i neispravne okvire.

Fragment free — ova metoda je kompromis između store and forward i cut-through metode. Preklopnik učita prva 64 okteta okvira prije nego počne prosljeđivati. Razlog zašto prosljeđivanje počinje nakon 64 okteta leži u činjenici da je većina grešaka u okviru u prva 64 okteta.

Postoje dvije vrste preklapanja:

Simetrično preklapanje — kod simetričnog preklapanja sva sučelja preklopnika imaju istu brzinu prijenosa podataka. Takvo preklapanje koristi se kod primjerice peer to peer mreža u kojima su svi članovi mreže ravnopravni.

Asimetrično preklapanje — Kod asimetričnog preklapanja sva sučelja nemaju istu brzinu prijenosa podataka. Sučelja veće brzine se obično dodjeljuju poslužiteljima.

ARP (engl. Address Resolution Protocol) je protokol koji povezuje IP adresu i MAC adresu. Uređaj šalje broadcast poruku u mrežu s upitom koji uređaj na segmentu ima određenu IP adresu. Traži da mu se taj uređaj javi i pošalje mu svoju MAC adresu. adresa je logička adresa, a MAC adresa je fizička adresa i ona nam treba da bi u konačnici poslali podatke nekom uređaju na mrežnom segmentu.

OSI fizički sloj

OSI fizički sloj osigurava prijenos podataka fizičkim medijem. Sam prijenos okvira na mediju zahtijeva od fizičkog sloja slijedeće elemente:

- Fizički medij i konektore
- Reprezentaciju bita na mediju
- Kodiranje podataka i upravljačkih informacija
- Sklopove predajnika i prijemnika na mrežnim uređajima

Tri su osnovna tipa fizičkih medija:

- Bakrena žica
- Optički kabel
- Bežična veza

Pri planiranju kabliranja LAN mreže treba uzeti u obzir 4 područja:

- Radno područje (work area)
- Telekomunikacijska soba
- Horizontalno kabliranje (horizontal cabling)
- Vertikalno kabliranje (vertical cabling)

UTP kabeli:

- **Straight-through**
    - Spajanje preklopnika i ethernet sučelja usmjernika
    - Računalo i preklopnik
    - Računalo i koncentrator
- **CrossOver**
    - **Preklopnik i preklopnik**
    - **Preklopnik i koncentrator**
    - **Koncentrator i koncentrator**
    - **Računalo i računalo**
    - **Računalo i ehternet sučelje usmjernika**

WAN veze spajaju velike udaljenosti. Te veze mogu biti izvedene različitim protokolima i sučeljima na fizičkom sloju.

Kodiranje je metoda pretvorbe niza podataka u unaprijed dogovoreni kod. Kod čine grupe bitova s predvidivim uzorkom koje se mogu raspoznati na obje strane komunikacijske veze. Na ovaj način uređaji koji sudjeluju u komunikaciji mogu razlikovati podatkovne od upravljačkih bitova.

Signali na fizičkom sloju – fizički sloj mora generirati električne, svjetlosne ili bežične signale koji će predstavljati računalu razumljive jedinice i nule. Metoda kojom se predstavljaju ove jedinice i nule naziva se signalizacija. Standardi fizičkog sloja moraju definirati kakav tip signala predstavljaju logičku nulu a kakav logičku jedinicu.

Ispitna pitanja 1:

1. koja je uloga transportnog sloja u komunikaciji izmedu dva računala, opiši?
Uloga transportnog sloja između dva računala je da definira uloga i metode za uspostavu komunikacije između procesa pokrenutih na uređajima u mreži te da segmentira i proslijeđuje poruke procesima ostalih slojeva OSI modela.

[Short]
Definira uloge i metode za uspostavu komunikacije između procesa pokrenutih na uređajima.

2. koja je razlika imedu UDP i TCP protokola opiši
[TCP] Transmition Control Protocol protokol podržava pouzdan prijenos podataka, kontrolu toka, upravljanje zagušenjima, segmentaciju te multipleksiranje/demultipleksiranje. Ove mogućnosti TCP protokola osiguravaju sigurnu i pouzdanu komnunikaciju te integritet podatka.

Primjeri: Hyper Text Transfer Protocol (HTTP), Hyper Text Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), Telnet

[UDP] User Datagram Protocol je protokol transportnog sloja koji ne uspostavlja vezu i ne garantira isporuku. Zadaće UDP-a segmentacija i multipleksiranje/demultipleksiranje. Korisiti se kod onih vrsta prometa gdje potrebna brzina i kod onih vrsta prometa koji mogu podnijeti gubitke.

Prijmeri: Audio/Video prijenosi, VoIP, promet računalnih igara.

[Short]
TCP sporiji, ali pouzdan. UDP brz, ali ne garantira pozdanost.

3. koja je uloga portova na transportnom sloju u komunikaciji opiši
[Full] Port number služi se adresiranje aplikacija. Svaka aplikacija koji pristupa internetu ima određeni broj porta kako bi računalo znalo koji aplikaciji treba proslijediti dolazni promet.

[Short]
Port number služi se adresiran aplikacija.

4. koja je uloga sequence numbera u komunikaciji opiši
Slijedni broj (Sequence Number) - 32-bitni broj odabran slučajnim izborom koji označava prvi oktet u podaktovnom dijelu TCP segmenta. Ovo je ključna informacija za praćenje komunikacije između dva proces na uređajima koji komuniciraju.

[Short]
Služi za praćenje komunikacije između uređaja.

5. opiši i skiciraj 3-way handshake mehanizam i čemu služi

3-way handshake je moda koju koristi TCP kako bi uspostavio konekciju putem IP.

[Dijagram događaja]

==Početak==

<Host A> - šalje TCP paket s SYN zastavicom prema host-u B

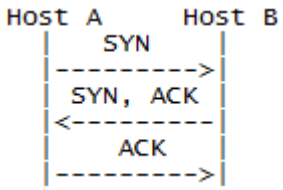
<Host B> - prima paket od host-a A

<Host B> - šalje TCP paket s SYN i ACK zastavicama prema host-u A

<Host A> - prima paket od host-a B

<Host A> - šalje TCP paket s ACK zastavicom

==Kraj==



6. kako djelimo portove (u koje grupe)

- Standardni poslužiteljki portovi (Well known ports)

>Raspon: 0-1023

>Primjeri: HTTP(80), HTTPS(443), FTP(20 i 21), POP(110/995)

- Rezervirani portovi (Reserved Ports)

>Raspon: 1024-49151

>Primjeri: League of Legends (5000-5500), Steam client traffic defaut (27015), TS3 default server port (9987)

-Dinamički portovi (Dynamic Ports)

>49152-65535

>Ovi portovi se ne mogu registirati i namijenjeni su za slobodno korištenje

7. koja je uloga TTL polja u IP zaglavlju

Time To Live (TTL) je broj koji ograničava životni vijek paketa u mreži. Svrha mu je kako bi onemogućio beskonačno kruženje (routing petlje) paketa u mreži.

8. koji su rasponi privatnih IP adresa

A klasa > 10.0.0.0-10.255.255.255

B klasa > 172.16.0.0-172.31.255.255

C klasa > 192.168.0.0 - 192.168.255.255

9. sto je mac adresa i kako se koristi

MAC adresa je adresa je fizička adresa mrežnog uređaja ili mrežne kartice. Služi za komnikaciju u mreži

10. koja je uloga preklopnika u mrezi, a koja usmjerenika

Preklopnik (switch) je uređaj koji služi za razgranavanje mreže.
Usmjernik (router) je uređaj koji služi za usmjerivanje prometa u mreži.

11. koja vrsta komunikacije postoje i kratko ih usporedite

Unicast - komunikacija jedan-na-jedan
Multicast - komunikacija jedan-na-više
Broadcast - komunikacija jedan-na-sve

12. koja UTP/STP kategorija kabela bi kupili u trgovini i zasto

Za male do srednje lokalne mreže dovoljno je Cat5e, jer omogućava gigabitne veze i PoE.
Recommended and tested by Jura (trust Jura.)

13.sto je to cyber secutity

Cyber security je sigurnost u kontekstu IT tehnologija možemo definirati kao kontinuirani proces zaštite digitalnih informacija i IT resursa od unutarnjih i vanjskih zlonamjernih ili slučajnih prijetnji. Ovaj proces obuhvaća detekciju, prevenciju i odgovor na prijetnje kroz korištenje sigurnosnih politika, programskih alata i IT servisa.

14.koje bi bile 4 posljedice hakerskih napada – opišite

Krađa osobnih podataka, novaca, informacija, pad mreže/servisa (sve ovisi o vrsti napada)...

15. kad govorimo o podacima u kontekstu sigurnosti koje 3 stvari su vazne opisite

[1.] Povjerljivost (Confidentiality) - Privatnost podataka. Povjerljivost podataka bi trebala biti zajamčena propisanim korporativnim politikama koje ograničavaju pristup podacima neovlaštenim osobama

[2.] Integritet (Integrity) - Ovo bi bila konzistentnost podataka i vjerodostojnost podatak tijekom životnog ciklusa podataka. Podaci se ne smiju mijenjati prilikom prijenosa

[3.] Dostuponost (Availability) - Održavanje opreme, operativnih sustava i softwarea up-to-date kao i izrada backupa osigurava dostupnost podataka u slučaju njihovog gubitka uzrokovanog ljudskim faktorom ili višom silom. Za povrat podataka moraju postojati pripremljene procedure

Ispitna pitanja 2:

HTTP: Kada i gdje je nastao World Wide web, što je hipertekst?
1991 u CERNU - izumio ga Tim Bernrs Lee, međusobno povezan sadržaj korištenjem poveznica(linkova)

HTTP: Od čega se sastoji URL? Pokaži na primjeru.
protokola, domenskog imena i file patha - http:// net.hr /zabava

HTTP: Navedi tipove HTTP odgovora (1xx, 2xx, 3xx, 4xx i 5xx) i navedi primjer svakog tipa:
1xx - informacijski(informational), 2xx - uspješni(success), 3xx - preusmjeravanje(redirect), 4xx - klijentska greška(client error), 5xx - poslužiteljska greška(server error)
100-continue, 200-OK,300-Multiple choices, 404 - Not found, 502 - Bad Gateway

HTTP: Što se događa s HTTP cookieom kada koristimo Private browsing opciju?
on se ne zapisuje

HTTP: Koji je temeljni nedostatak HTTP Autentikacije. Kako se taj problem rješava?
temelji se na plaintext slanju zaporke što nije sigurno. rješava se https-om - http preko secure socket layer-a, kreira se SSL kanal preko kojega se komununicira HTTP-om, sigurnost je gurnuta u sesijski sloj

HTML: Što znači da je HTML markup jezik? Koja je aktualna verzija HTML jezika?
Znači da koistimo običan tekst dokument u kojem određenim markup oznakama ograđujemo dijelove teksta koji dobivaju određenu funkciju

HTML: Pod čijem se okriljem danas nalazi standardizacija HTTP protokola?
W3C

FTP: Pojasni svrhu kontrolne i podatkovne konekcije u FTP komunikaciji?
kontrolnom konekcijom uspostavljamo konekciju između klijenta i poslužitelja, a podatkovna se stvara kada iniciramo prijenos podataka(za prijenos podataka)

P2P: Kako BitTorrent protokol identificira sadržaj, te zašto se podaci dijele u blokove?
identificira pomoću torrent filea u kojem je Distributed hash table za exact-match podataka, podaci u blokovima da se mogu skidati od većeg broj poslužitelja na distribuiran način te to ujedno daje otpornost na ispadanje poslužitelja iz mreže

TCP/UDP: Kojim parametrom razlikujemo različite aplikacije na transportnom sloju?
port

TCP/UDP: Kako klasificiramo portove u kategorije te za što se koja od tih kategorija koristi?
well-known, reserved, dynamic

TCP/UDP: Navedi 5 važnih funkcija TCP protokola.
pouzdan prijenos, kontrola toka(flow control), upravlajnje zagušenjem(congestion control), segmentacija, multipleksiranje i demultipleksiranje

TCP/UDP: Kakve aplikacije koriste TCP ili UDP protokol na transportnom sloju?
UDP - one aplikacije koje trebaju brz prijenos ali ne i ispravnost, connectionless komunikacija(bazirana na porukama), audio i video, DNS, DHCP,TFTP
TCP - one koje trebaju ispravnost, SMTP, FTP, HTTP, telnet

TCP/UDP: Kako TCP protokol osigurava pouzdani prijenos? Koja polja se za to koriste?
u slijedni broj(SEQ) upišemo redni broj okteta koji šaljemo, s druge strane vraćamo potvrdni broj(ACK) koji predstavlja broj sljedećeg okteta kojeg očekujemo i tako potvrđujemo da smo sve primili

TCP/UDP: Čemu služi checksum polje u zaglavljima protokola? Što njime možemo otkrit?
Služi za otkrivanje pogreške u prijenosu - bit errora.

TCP/UDP: Što su i koja je razlika u funkciji upravljanja toka i upravljanja zagušenjem?
upravljanje toka regulira brzinu prijenosa s strane primatelja, a upravljanje zagušenjem s strane pošiljatelja