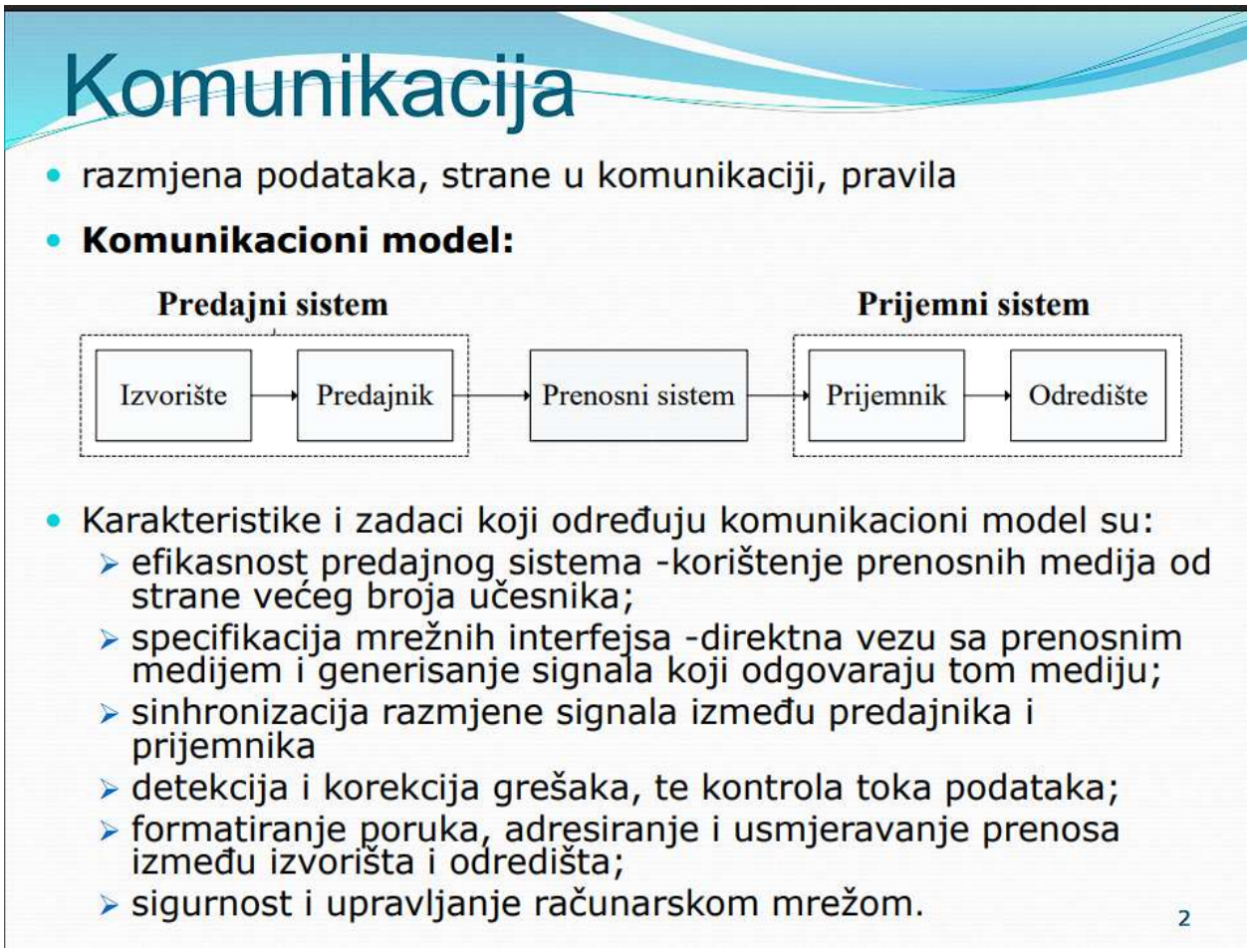
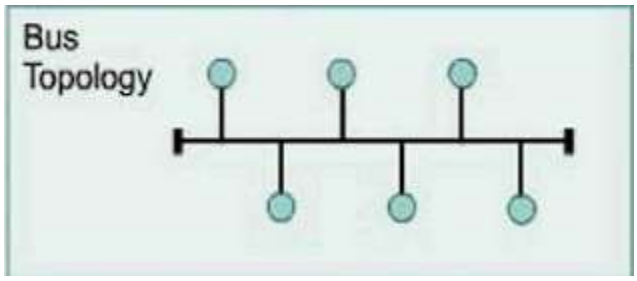
1. Fizičke/Mrežne topologije (stranica 4)



Topologija Magistrale (eng. Bus topology) predstavlja najjednostavniji način povezivanja uređaja ili komunikacionih čvorova. Na sljedećoj slici prikazan je jedan primjer topologije magistrale:



Kod ove topologije, svaki uređaj ili čvor je posebnim kablom povezan na zajednički prenosni kabal.

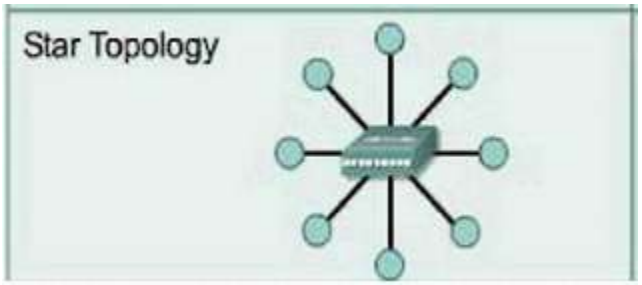
Zajednički prenosni kabal, najčešće zovemo „kičmom(eng. Backbone)“.

Krajevi zajedničkog prenosnog kabla se uglavnom završavaju posebnim uređajem koji se uglavnom naziva „terminator“.

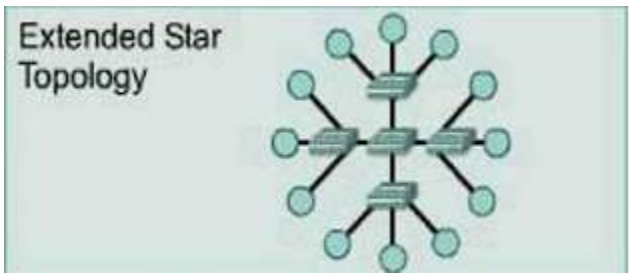
Kada jedan urađaj želi da komunicira sa drugim, on svim uređajima šalje emisionu poruku

(eng. Broadcast message) o namjeri za uspostavljanje komunikacije.
Veza se uspostavlja samo sa jednim, željenim, krajnjim uređajem i prenos podataka između čvorova se obavlja u jednom pravcu.
Zbog toga ovu topologiju karakteriše degradacija performansi jer u nekom trenutku samo jedan uređaj može slati podatke i česte su pojave kolizije.
Takođe, ukoliko dođe do prekida zajedničkog prenosnog kabla -onemogućena je komunikacija između krajnjih uređaja.

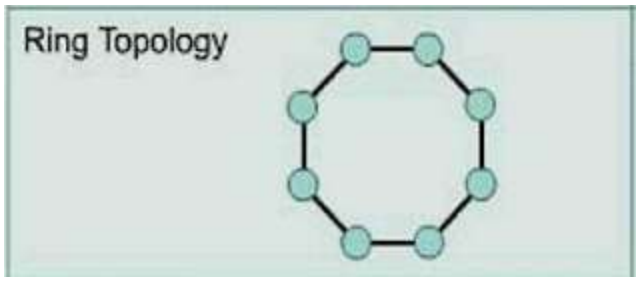
Topologija zvijezde (eng. Star topology) se najčešće koristi u računarskim mrežama zasnovanim na paketskom prenosu podataka.
Na sljedećoj slici, prikazan je jedan primjer topologije zvijezde:



Centralni uređaj, može biti Router/Switch i u zavisnosti od izbora istog zavisi i način prenosa podataka između čvorova.
Ukoliko dođe do prekida rada centralnog uređaja -onemogućena je komunikacija između krajnjih uređaja.
U praksi, moguće je realizovati i primjer „proširene zvijezde“ gdje se na željenim pozicijama umjesto krajnjih uređaja, postavlja neki od centralnih uređaja na koji se dalje povezuju krajnji uređaji.

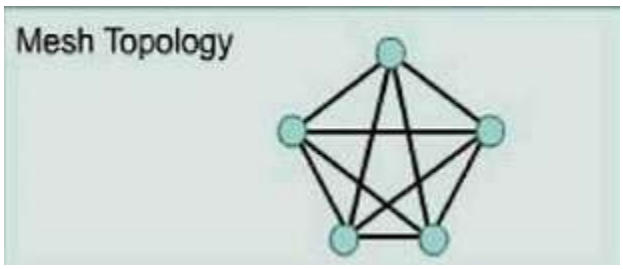


Topologija prstena podrazumijeva povezivanje čvorova u prsten, pri čemu svaki čvor ima dva susjedna čvora.
Jedan primjer takve topologije, prikazan je na sljedećoj slici:



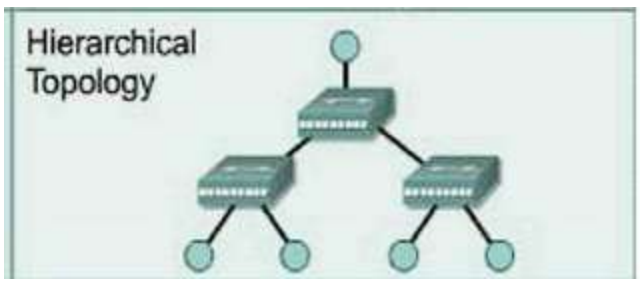
Podaci se prenose u jednom ili drugom smjeru, pri čemu svaki čvor indirektno ima zadatak da prosljeđuje podatke prema odredištu.
Svaki čvor je potencijalna kritična tačka, ukoliko dođe do prekida prstena na trasi između izvorišta i odredišta, dolazi do prestanka njihove međusobne komunikacije.

Potpuno povezana topologija (eng. Mesh topology) prikazana je na sljedećoj slici:



Na slici vidimo da između bilo koja dva čvora u topologiji -postoji direktna povezanost i omogućen prenos podataka.
Mana ove topologije jeste cijena, broj veza raste sa kvadratom broja povezanih uređaja.
Da bi se smanjili troškovi, moguće je modifikovati topologiju tako da se svaki od uređaja povezuje samo sa onim uređajima sa kojima ima čestu komunikaciju.
Takva topologija se inače naziva ***"parcijalni meš"***.

Hijerarhijska topologija (eng. Tree topology) prikazana je na sljedećoj slici:



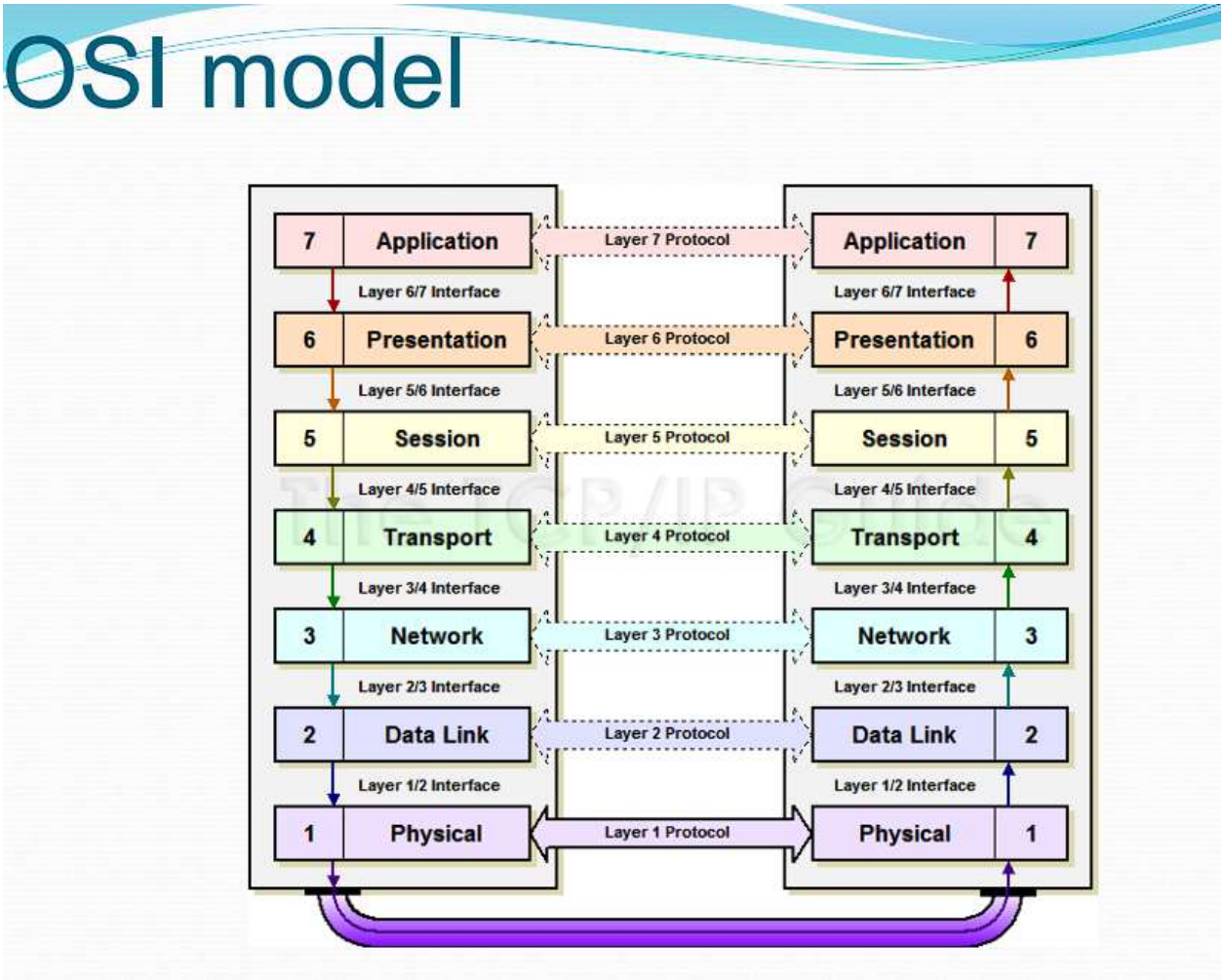
Ova topologija predstavlja varijaciju topologije zvijezde koja obezbjeđuje hijerarhijski tok podataka.
Vidimo jedan **„centralni uređaj"** na koji mogu biti povezani drugi krajnji ali i centralni uređaji.

Prednosti: imamo više nivoa prioriteta uređaja, omogućena direktna ili indirektna povezanost velikog broja uređaja, korišćenje različitih tipova hijerarhijskih linkova.

Kao i kod obične topologije zvijezde, ukoliko dođe do prestanka rada centralnog uređaja, komunikacija također biva onemogućena..

Rezime:
Bus, Star, proširena zvijezda, Ring, Mesh, partMesh, Hierarchical –opiši od čega se sastoji topologija, način odvijanja komunikacije, odlike i mane.

2. **PDU OSI/TCP modela** (19. stranica u knjizi..)



Aplikativni sloj je sloj kome pristupa krajnji korisnik i kojim se definiše interfejs između aplikacija koje se izvršavaju na krajnjim uređajima.
Veliki broj protokola(HTTP, FTP, Telnet,..) koji se svakodnevno koriste u računarskim mrežama svoju funkcionalnost, u značajnom mjeri vežu za ovaj sloj.
Rezultat izvršenja ovih programa su podaci koji se prenose između aplikacija ili uslužnih programa i operativnog sistema nekog krajnjeg uređaja.

Prezentacioni sloj je zadužen za način reprezentovanja podataka što uključuje formatiranje, kompresiju i šifrovanje podataka u kontekstu obezbjeđivanja potpune funkcionalnosti aplikacija koje učestvuju u komunikaciji.
Podatke koje prezentacioni sloj dobije od aplikacionog sloja na predajnoj strani treba kompresovati radi efikasnijeg prenosa, a zatim na prijemnoj strani prvo dekompresovati pa proslijediti aplikacionom sloju.
Dakle, karakteristične funkcije ovog sloja jesu kompresija i dekompresija podataka.

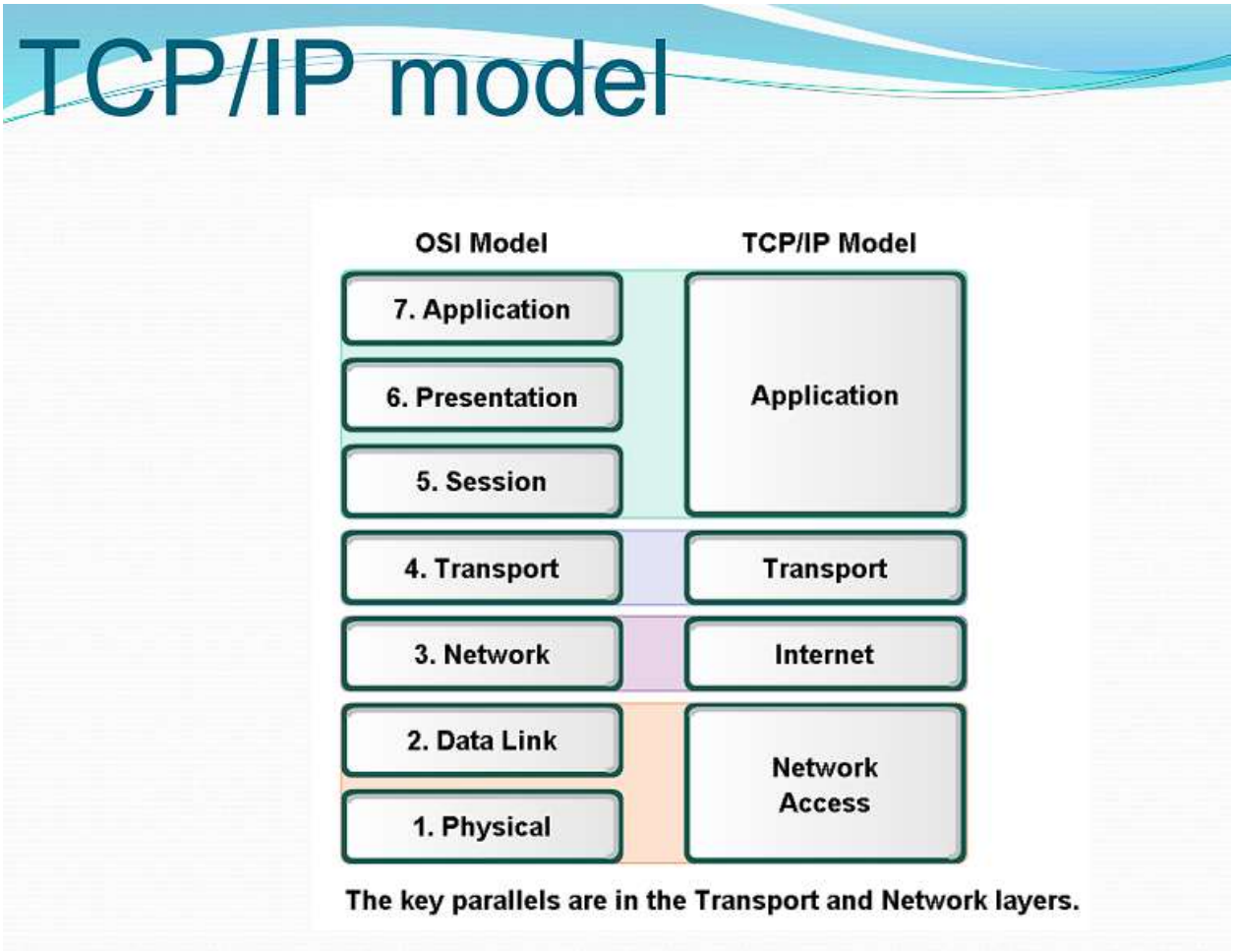
Sloj sesije ima ulogu održavanja dijaloga između krajnjih hostova, odnosno između učesnika u komunikaciji.

Transportni sloj ima zadatke da obezbjedi adresiranje procesa i aplikacija, te da realizuje prenos korisnih podataka koji su dobijeni od viših slojeva (eng. Payoad data).
(Dalje ide priča o prenosu podataka TCP/UDP..)

Mrežni sloj ima zadatak da obezbijedi prenos paketa od izvorišta do odredišta vodeći računa o putanjama između mrežnih čvorova, sve dok se paketi ne isporuče krajnjem uređaju.
Mrežni sloj se često naziva i internet sloj, a najpopularniji protokol koji se koristi na ovoj sloju je IP(Internet protocol) protokol.
Na ovom sloju se identifikuju i adresiraju krajnji hostovi upotrebom IP adresa.
Na putanji od izvorišta do odredišta, svakom čvoru dodjeljena je IP adresa, zbog toga se na ovom sloju koriste odgovarajući protokoli rutiranja, kojima se definiše najbolja putanja za prenos paketa.
Funkcionalnost protokola zavisi i od veličine paketa, neki paketi imaju veličinu koja prevazilazi maksimalno dozvoljeno fragmentiranje i iz tog razloga ih je potrebno fragmentirati prije slanja. U tom slučaju, fragmenti se na prijemnom strani kombinuju u izvorni paket.

Sloj veze podataka ima zadatak da podatke predstavi odgovarajućim okvirima ili frejmovima, koji se sastoje od bajtova, a zatim obezbjedi njihov prenos preko prenosivog fizičkog medija.
Često korišteni protokoli ovog sloja su Ethernet i WiFi koji definišu prenos prenos preko žičanih ili bežičnih medija, respektivno.

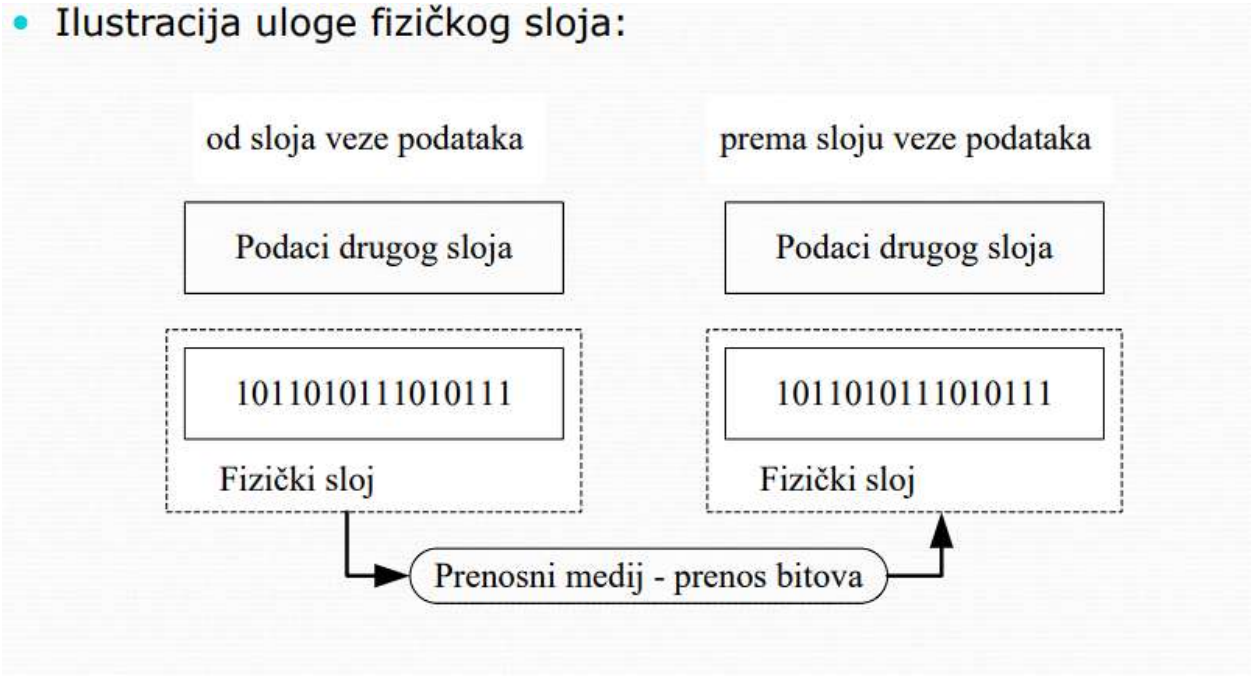
Fizički sloj je zadužen za slanje bitova(nula i jedinica) preko fizičkog medija pomoću odgovarajućih signala. Bitovi se mogu slati preko radio talasa ili materijalnih medija.
Na ovom sloju se standardima definiše koliki napon predstavlja jedinicu, a koliki nulu, te koliki vremenski interval traje jedan *bit*.



Kod TCP-a, 5-6-7 se posmatraju kao Aplikacioni sloj..

3. **Funkcije na fizičkom sloju** (31. stranica..)

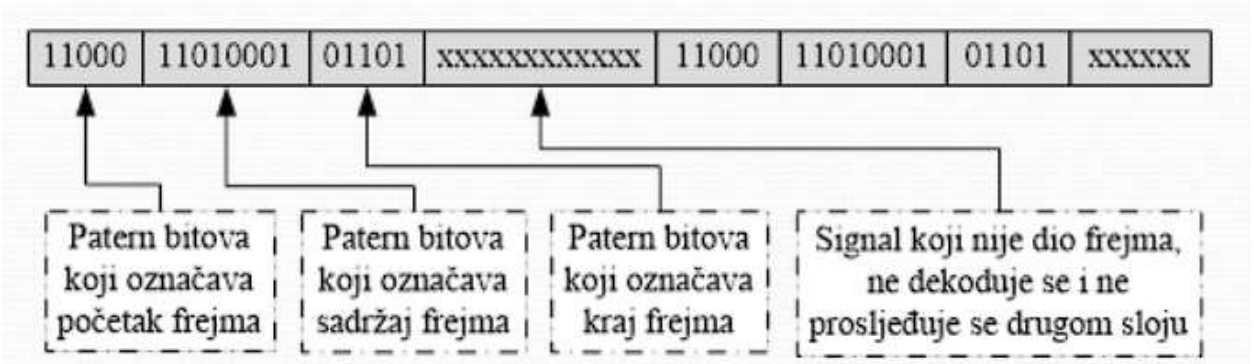
Na slici je ilustrovan process kojim fizički sloj realizuje preuzimanje okvira od sloja veze podataka i prosljeđivanje *bita* na prenosni medij.



Da bi se obezbjedio potpuno funkcionalan komunikacioni link, na fizičkom sloju je potrebno realizovati sljedeće funkcije:

-**Veza sa slojem veze podataka kroz vertikalnu komunikaciju između slojeva i enkapsulacija podataka.** Okviri preuzeti od sloja veze podataka koji sadrže niz bitova predstavljenih 0 ili 1, trebaju se predstaviti u obliku koji odgovara fizičkom mediju koji se koristi za transmisiju.

-**Kodovanje.** Niz bitova dobijen sa drugog sloja se konvertuje u precizno definisane kodne grupe. Na slici je prikazana ilustracija upotrebe paterna za identifikaciju početka i kraja okvira:



-Reprezetacija bitova na prenosnom mediju. Sekvence bitova je potrebno predstaviti odgovarajućim električnim, optičkim ili radio signalima koji će predstavljati 1 ili 0 na transmisionom mediju.

-Prenos bitova preko komunikacionog medija.
Važan parametar prenosnog medija u kontekstu paketskog prenosa računarskim mrežama je **propusni opseg (eng. Bandwidth)**.
Kada je riječ o paketskom prenosu podataka ovaj parametar se izražava brojem bitova u sekundi **[b/s]**.
Propustnost ili **protok (eng. Throughput)** predstavlja količinu podataka koja se prenese u jedinici vremena u realnim uslovima.

-Specificiranje karakteristika mrežnih interfejsa.
Na fizičkom sloju je potrebno standardizovati i precizno definisati fizičke karakteristike interfejsa koji obezbjeđuju vezu između mrežnog uređaja ili hosta i transmisionog medija.

4. **Budžet slabljenja optičkog linka** (54. stranica)

Prilikom projektovanja, izgradnje i održavanja optičkih linkova u oblasti računarskih komunikacija neophodno je voditi računa o gubicima i slabljenju signala koji se prenosi. Gubici snage signala kod optičkih linkova zavise od više činioca.

Ako je P_1 ulazna snaga na predajnoj strani optičkog linka i P_2 izlazna snaga na prijemnoj strani optičkog linka, tada je slabljenje $\boldsymbol{\alpha}$ predstavljeno sljedećim logoritamskim izrazom:

$\boldsymbol{\alpha = 10log_{10}\frac{P_2}{P_1}[dB]}$, B-Bel -osnovna jedinica za interpretaciju i mjerenje slabljenja optičkih linkova.

Slabljenje izraženo decibelom predstavlja relativnu vrijednost slabljenja optičkog linka.
Veoma često je teško odrediti snagu na predajnoj strani jer se mjerenjem utvrđuje samo snaga na prijemnoj strani.
U tom slučaju se za definisanje vrijednosti slabljenja koristi izraz u kojem se umjesto snage na predajnoj strani koristi fiksna, referentna snaga od *1mW*, što je usvojeno i standardima.
U tom slučaju dobija se izraz:

$\boldsymbol{\alpha = 10log_{10}\frac{P_2}{1mW}[dBm]}$

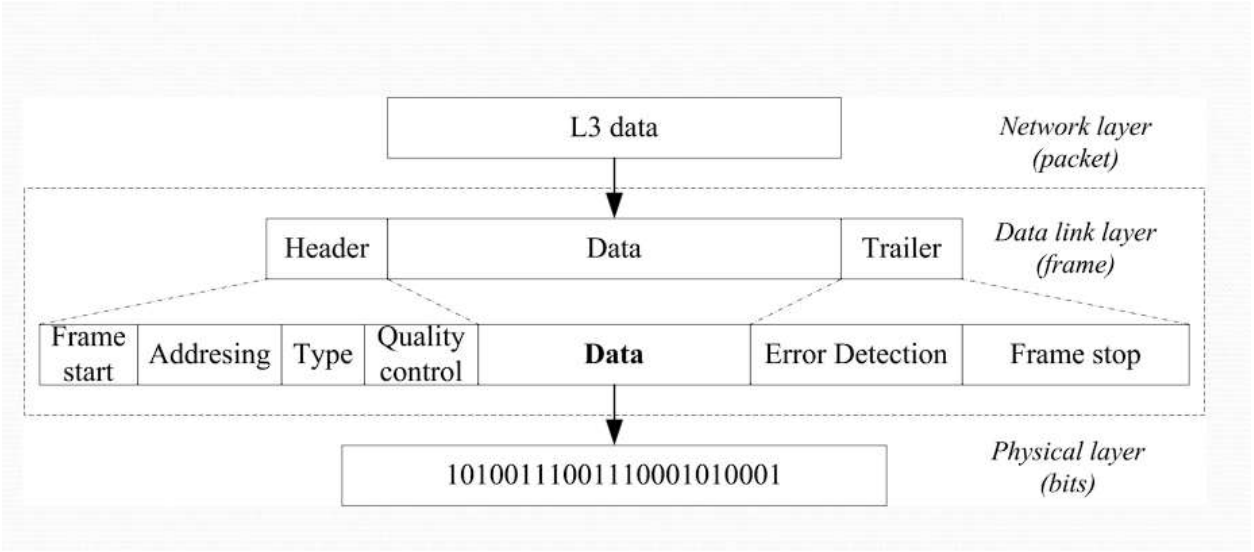
Dobijena jedinica *dBm* označava decibel u odnosu na milivat što eksplicitno ukazuje na to da je slabljenje izraženo u odnosu na referentnu snagu od *1mW*.

Prvi i neophodan zadatak prilikom planiranja i izgradnje optičkog linka je proračun kvaliteta linka ili budžeta slabljenja optičkog linka.
Pod pojmom budžeta slabljenja optičkog link se podrazumijeva ukupno slabljenje s kraja na kraj posmatranog linka.
Realna vrijednost budžeta treba da bude između teorijski maksimalne i minimalne vrijednosti slabljenja za koje je moguć prenos optičkog signala i uspostavljanje komunikacije preko optičkog linka.

Za proračun budžeta slabljenja je potrebno uzeti u obzir sva slabljenja koja unose pasivne ali i aktivne komponente optičke mrežne infrastukture.
Osim slabljenja komponenti optičkog linka uzima se u obzir i preporučena margina slabljenja.
Margina slabljenja je definisana razlikom između industrijske specifikacije i očekivanih stvarnih vrijednosti slabljenja što obezbjeđuje proračun budžeta optičkog linka sa dovoljnom preciznošću i projektovanom pouzdanosti

5. **Ilustrovati i objasniti princip enkapsulacije i uokvirivanja na sloju veze podataka** (64.str)

Jedan od prvih zadataka sloja veze podataka je formiranje okvira.
Paketi koji se preuzimaju od trećeg sloja se smiještaju u polje okvira koje se naziva polje za korisničke podatke ili payload.
Ispred polja u kojem su smješteni podaci se dodaje zaglavlje sloja veze podataka, a iza se dodaje završni blok okvira ili trejler(eng. Frame trailer).
Na sljedećoj slici je predstavljen princip enkapsulacije i uokviravanja na sloju veze podataka.



-**Polje za identifikaciju početka okvira (Frame Start),** ovo polje koristi poseban patern bitova kojim se određuje početak okvira.

-**Polje za adresiranje (Addressing)** se koristi za adresiranje izvorišnog i odredišnog čvora na drugom sloju veze podataka. Adresiranje na sloju veze podataka direktno zavisi od logičke topologije mreže.

-**Polje za tip podataka (Type)**. Sadržaj ovog polja ukazuje koji protokol trećeg sloja je upotrijebljen za formiranje paketa koji su enkapsulirani u polje korisničkih podataka.

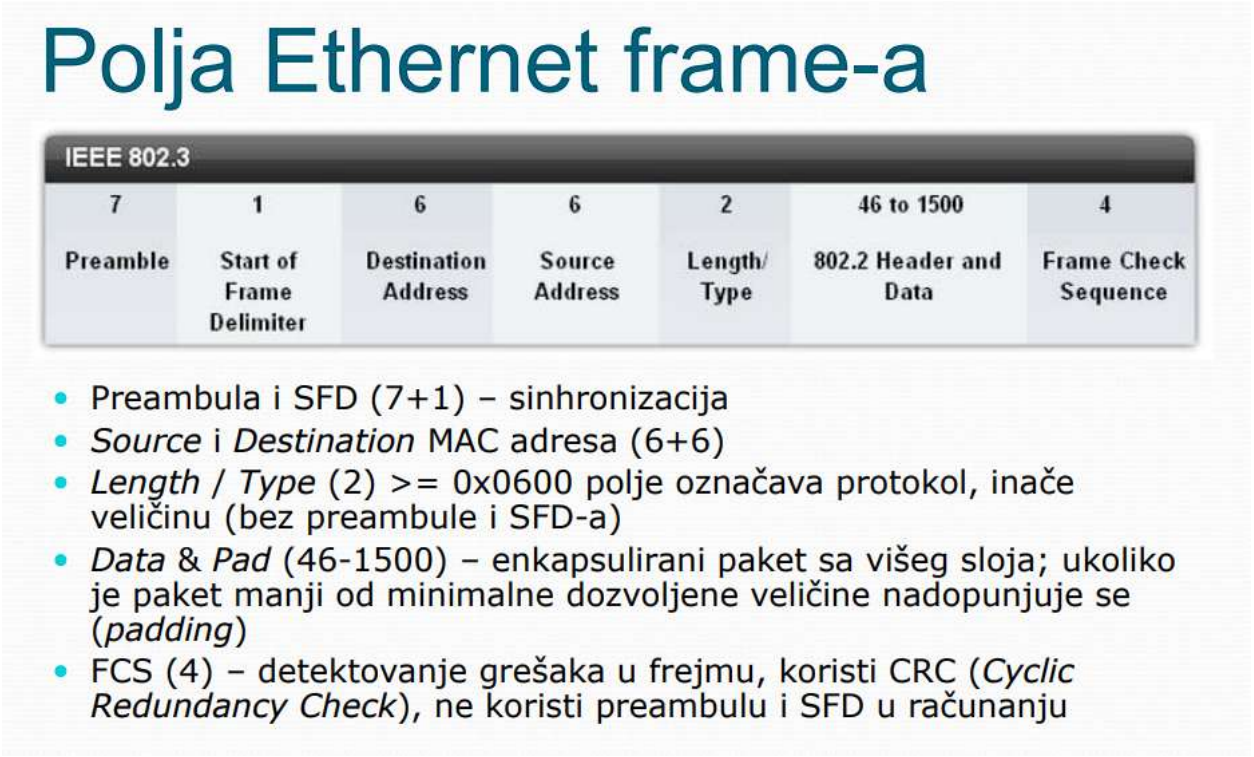
-**Polje za kontrolu prenosa (Quality Control),** obezbjeđuje kontrolu prenosa i identifikaciju posebnih kontrolnih servira kao što je kvalitet servisa.

-**Polje korisničkih podataka (Data),** sadrži korisničke podatke, odnosno podatke dobijene od trećeg sloja.

-**Polje za detekciju grešaka (Error Detection)** ubacuje se nakon korisničkih podataka i predstavlja dio trejlera.

-**Polje za identifikaciju završetka okvira (Frame Stop),** dio trejlera, čini ga poseban patern bitova pomoću kojeg se identifikuje kraj okvira.

6. **Ethernet Frame nacrtati i objasniti polja** (78. stranica)



-Preambula(Preamble) je polje kojim započinje svaki Ethernet Frame. Ovo polje je postavljeno na sedam bajtova čija vrijednost je identična 10101011. Promjenom vrijednosti 0 i 1 se onemogućuje uspostavljanje sinhronizacije između prijemnika i predajnika.

-SFD(Start Frame Delimiter) sadrži jedan bajt koji je predstavljen sekvencom 10101011. Ima poseban značaj zbog toga što je dužina Ethernet okvira promjenjiva i potrebno je identifikovati početak okvira. SFD zajedno sa Preamble očigledno predstavlja zaglavlje fizičkog sloja.

-Destination/Source Address polja.

-Length/Type. Ukoliko mu je vrijednost manja od 1500(decimalno) tada ima značenje dužine, a u suprotnom ima značenje tipa podataka.
Tip podataka ukazuje na protokol višeg sloja čiji paket se nalazi u polju podaci.

-**Pad,** omogućuje prevazilaženje problema koji se javlja ukoliko je dužina data polja manja od 46 bajtova.

-**FCS(Frame Check Sequence),** na bazi algoritma za izračunavanje kontrolne sume se detektuju greške nastale u prenosu.

7. ICMP/PING/TRACEROUTE (103. stranica)

IP protokol omogućuje prenos podataka između hostova koji su jednoznačno određeni izvorišnom i odredišnom IP adresom. Karakteristika IP protokola je da ne zathtijeva prethodno uspostavljanje konekcije i riječ je o beskonekcionom protokolu.

Zbog toga je potreban mehanizam koji će obezbijediti informaciju da li je isporuka paketa bila uspješna ili je došlo do djelimičnog ili potpunog gubitka paketa.

Osim toga, često je potrebno utvrditi da li je udaljeni host ili neki mrežni uređaj dostupan što nije podržano od strane IP protokola.

Upravo to može da obezbijedi ICMP(internet Control Message Protocol).
Postoje dvije verzije ICMP protkola, verzija 4 i verzija 6.

ICMP protokol je protokol **mrežnog sloja**.
ICMP poruke se **enkapsuliraju unutar IP paketa**, pri čemu se odgovarajuće polje u zaglavlju IP paketa postavlja na vrijednost koja označava da se koristi ICMP protokol.

- **Ping** služi za provjeru dostupnosti odredišnog uređaja, koristeći **ICMP Echo Request** i **ICMP Echo Reply** poruke. Osim dostupnosti, ping također mjeri vrijeme potrebno za putovanje paketa do odredišta i natrag.
- **Traceroute** služi za detekciju broja skokova i putanje paketa između izvorišnog i odredišnog uređaja. Korištenjem **TTL** (Time to Live) polja u IP paketu i **ICMP Time Exceeded** poruka, traceroute identificira svaki usmjerivač na putu paketa, prikazujući njegovu IP adresu i vrijeme odziva.

8. ARP protokol (108. stranica)

Osnovna uloga ARP protokola je mapiranje IP adresa u fizičke, hardverske adrese sloja veze podataka, odnosno MAC adrese.

Zahvaljujući funkcijama IP protokola i ARP protokola moguće je utvrditi MAC adrese mrežnih interfejsa uređaja koji su povezani u okviru posmatranog mrežnog segmenta.

Na osnovu dobijenih parova IP adresa i MAC adresa formira se baza podataka koja daje uvid u mapiranje lokalnih IP adresa u MAC adrese, odnosno ARP tabela.

U toku prenosa podataka od izvorišta do odredišta IP adresa je poznata od strane aplikacije i viših slojeva, transportnog i mrežnog sloja. U trenutku kada se paket treba proslijediti na jedan od odlaznih interfejsa potrebno je odrediti odredišnu adresu sloja veze podataka, odredišnu MAC adresu odgovarajućeg interfejsa. Na osnovu podataka iz ARP tabele bira se odlazni mrežni interfejs na koji će se proslijediti IP paket. Popunjavanje ARP tabele se realizuje automatski ili, u određenim slučajevima, nakon određenih aktivnosti mrežnog administratora. (Objasni dinamički/statički način popunjavanja ARP tabela..)

9. Uspostavljanje TCP konekcije, TCP proces komunikacije, koraci (142. stranica)

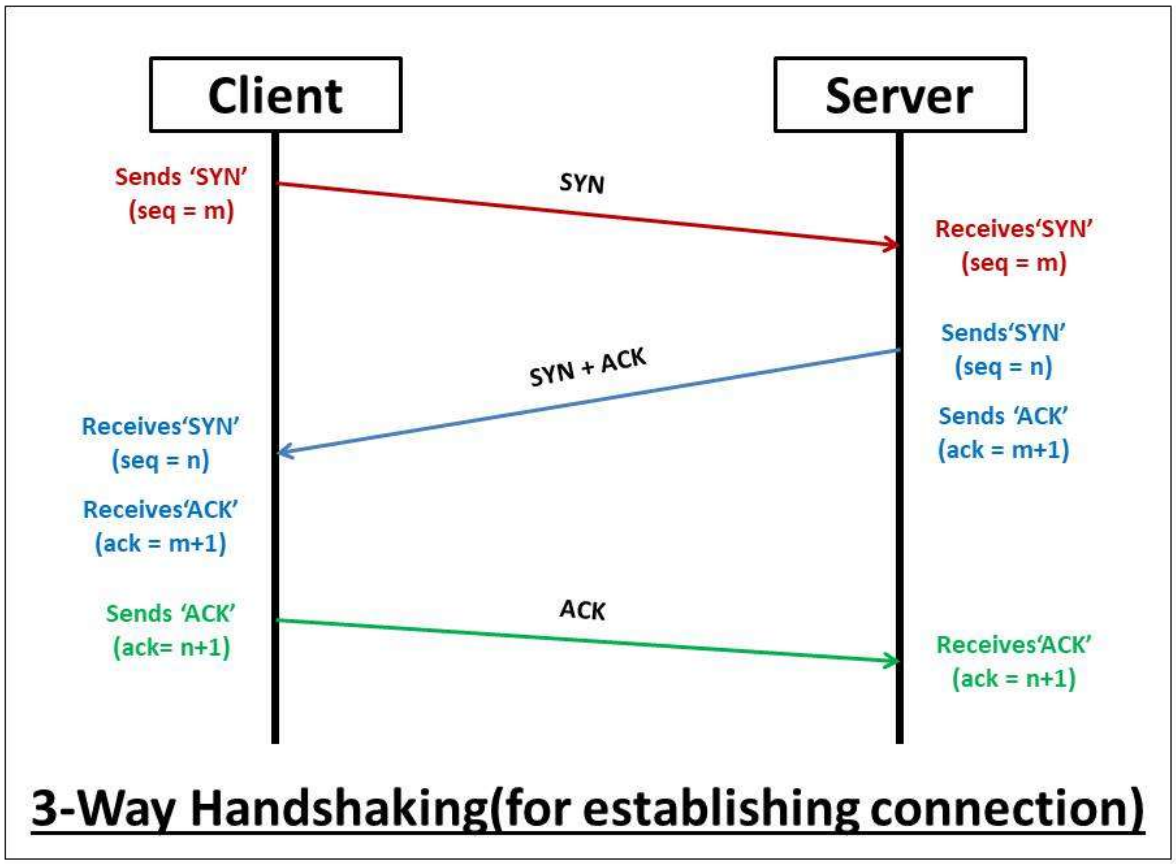
TCP(Transmission Control Protocol) je transportni protokol koji obezbjeđuje pouzdan prenos podataka uspostavljanjem veze i potvrđivanjem prijema podataka.

TCP podržava *full-duplex* komunikaciju *point-to-point* tipa, što znači da se komunikacija uvijek odvija između maksimalno dva učesnika i to u oba smjera istovremeno.
Dok jedna strana šalje podatke, druga može da ih prima i istovremeno šalje podatke.
Nije moguće istovremeno slanje podataka na više adresa(*multicast* ili *broadcast*).

Uspostavljanje veze (Three-way handshake):

- **Korak 1:** Inicijator šalje segment na odredišnu IP adresu i port. U zaglavlju tog segmenta aktivira se **SYN (Synchronize)** bit i šalje se početni redni broj, npr. **SEQ = M**.
- **Korak 2:** Odredišni uređaj, ukoliko je spreman za vezu, odgovara segmentom sa aktiviranim **SYN i ACK (Acknowledge)** bitovima. U ovom segmentu, on šalje svoj vlastiti početni redni broj (**SEQ = N**) i potvrđuje prijem inicijalnog segmenta tako što u polje za potvrdu (ACK) postavlja vrijednost **M+1**, čime signalizira da očekuje sljedeći bajt sa rednim brojem M+1.
- **Korak 3:** Inicijator prima SYN/ACK segment od odredišta i šalje posljednji segment za potvrdu. U njemu aktivira samo **ACK** bit, a u polje za potvrdu postavlja vrijednost **N+1**, čime potvrđuje prijem segmenta od odredišta.

Nakon ovog trećeg koraka, veza je uspostavljena i podaci se mogu razmjenjivati u oba smjera. Svi ovi redni brojevi (M, N, M+1, N+1) osiguravaju da svi paketi stignu na svoje mjesto i budu ispravno sortirani.



Kada neki učesnik u komunikaciji nema više podataka za slanje, on može da prekine vezu slanjem segmenata sa aktivnim FIN bitom. Nakon potvrdesegmenta od druge strane, ovaj smjer komunikacije se zatvara.

10. DNS -domeni, poddomeni, zone, primjeri dns zapisa (169. stranica)

DNS(Domain Name System) predstavlja jedan od ključnih servisa i protokola na internetu. Ovaj sistem je u suštini distribuirana baza podataka imena koja se koriste na internetu i odgovarajućih IP adresa, koja je raspoređena na DNS serverima širom svijeta.

Za komunikaciju na internetu ljudi mnogo lakše koriste i pamte imena, dok su za stvarnu komunikaciju između hostova na mreži potrebne IP adrese.
DNS omogućava preslikavanje imena u IP adrese i na taj način omogućava da se za ljudsku potrebu koriste imena umjesto IP adresa.
DNS omogućava da se jednom imenu dodjeli više IP adresa, ili da se promijeni fizički uređaj i njegova IP adresa, a da njegovo ime i dalje ostaje nepromjenjeno.

DNS je zasnovan na Client-Server arhitekturi.
DNS Client je aplikacija koja inicira komunikaciju i zahtijeva podatke od DNS servera.
Sa druge strane, DNS server je softver koji očekuje zahtjeve DNS klijenata i odgovara im podacima kojima raspolaže.

Komunikacija između DNS klijenta i servera uobičajeno se odvija korišćenjem UDP protkola, DNS-Client je na portu 1024+, a DNS-Server koristi port 53.

Kada bilo koji host u mreži ima potrebu da za dato ime drugog hosta dobije njegovu IP adresu, on mora da se obrati DNS serveru. Da bi se obratio DNS serveru, host mora da zna njegovu IP adresu. Zbog toga je IP adresa sastavni dio parametra konfiguracije svakog hosta u mreži koji ima potrebu da radi sa imenima hostova.
Obično se u konfiguraciji hosta navode IP adrese dva DNS servera.

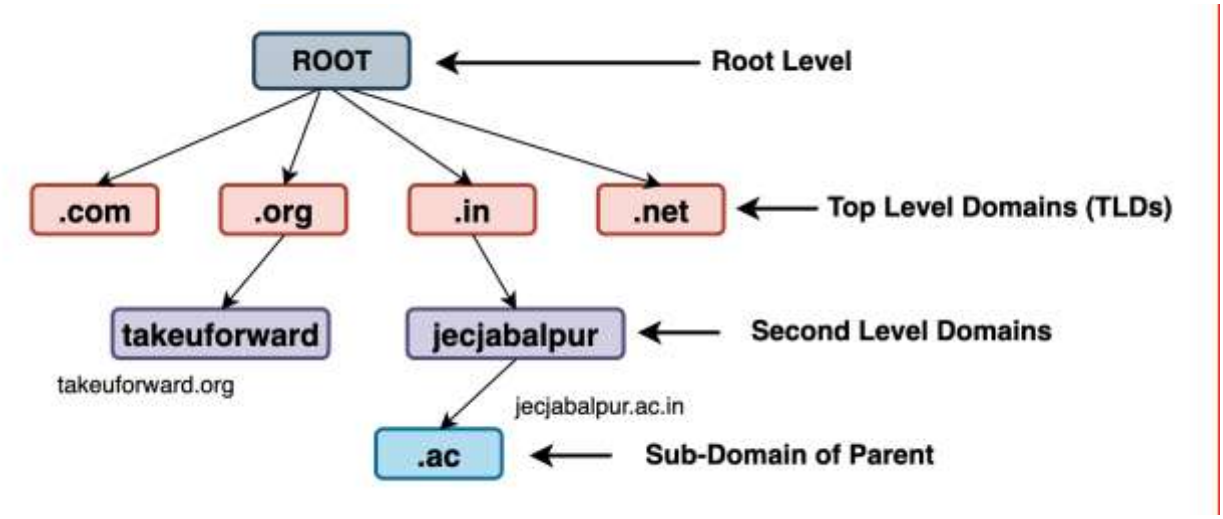
(DNS Querry, DNS Response ..)
DNS Resolver ima ulogu da u ime neke aplikacije šalje upite DNS serveru i vraća odgovor aplikaciji.

Domeni, poddomeni i zone

Radi lakše organizacije i upravljanja imenima na internetu, uvedena je hijerarhijska struktura imena koja omogućava da se adresni prostor imena na internetu podijeli u određene zone ili domene odgovornosti, kao i da se upravljanje imenima delegira različitim organizacijama.

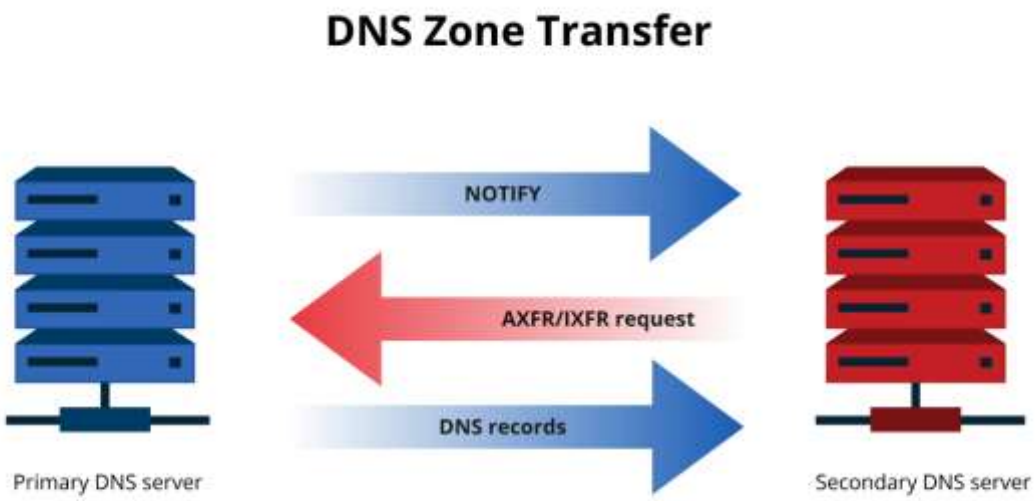
Jedan dio tog prostora, koji čini logičku ili organizacionu cjelinu, naziva se *domen*(eng. Domain).

Domenski prostor na internetu je organizovan hijerarhijski, u formi korijenog stabla, sa početkom u korijenu(eng. Root) koji nema poseban naziv.
Zatim slijede TOP(Top Level Domains) ili ti domeni prvog nivoa, zatim Secondary Level Domains, itd.
Svaki domen može da ima svoje poddomene, koji takođe mogu da imaju svoje poddomene i da formiraju hijerarhiju od nekoliko nivoa.
Domeni prvog nivoa se mogu podjeliti na generičke ili opšte domene poput domena com, net, org, te domene država poput ba, rs, mn, ..



Pošto je broj hostova i domena na internetu prilično veliki, nije praktično da se podaci o domenima čuvaju na jednom mjestu, pa je odgovornost za upravljanje domenskim prostorom distribuirana na veći broj entiteta koji imaju svoje zone odgovornosti.

DNS zone su segmenti DNS sistema koji predstavljaju područje odgovornosti nad određenim domenom ili poddomenom.
U njima se nalaze DNS zapisi koji određuju kako se imena domena prevode u IP adrese i obrnuto. Postoje **primarne zone** (gdje se zapisi kreiraju i mijenjaju), **sekundarne zone** (kopije primarne, služe za raspodjelu opterećenja i rezervu) i **reverse zone** (za mapiranje IP adresa na domene). Na ovaj način DNS je decentralizovan, stabilan i skalabilan, jer odgovornost nije na jednom mjestu nego raspodijeljena između više servera.



Primarni DNS server je glavni izvor podataka za određenu zonu, a sekundarni se koriste za raspodjelu opterećenja i u slučaju kad primarni nije dostupan.

Podaci na serverima se čuvaju u formi DNS zapisa:
{naziv} {TTL} klasa tip podaci

naziv -DNS ime na koje se zapis odnosi, ako se izostavi onda dobija vrijednost prethodnog zapisa.

TTL -vrijeme trajanja keširanih podataka DNS servera, iskazano u sekundama.

klasa -klasa adresa zapisa

tip -Tip DNS zapisa, tipovi:

A – Address record – povezuje domen sa IPv4 adresom.

AAAA – IPv6 Address record – povezuje domen sa IPv6 adresom.

CNAME – Canonical Name record – alias, preusmjerava jedan domen na drugi.

MX – Mail Exchange record – određuje mail servere za primanje e-pošte.

NS – Name Server record – definiše autoritativne DNS servere za zonu.

PTR – Pointer record – koristi se u reverse DNS zoni za mapiranje IP adrese na domen.

SOA – Start of Authority record – sadrži osnovne informacije o zoni (primarni server, serijski broj, interval osvježavanja...).

TXT – Text record – omogućava upisivanje proizvoljnog teksta (često za SPF, DKIM, verifikacije).

SRV – Service locator record – specificira servere za određene servise (npr. VoIP, IM).

CAA – Certification Authority Authorization – definiše koje sertifikacione kuće mogu izdavati SSL/TLS certifikate za domen.

podaci -podaci specifični za određeni tip zapisa

11. HTTP (186. stranica)

HTTP(Hyper Text Transfer Protocol) se koristi za prenos podataka između veb klijenata i veb servera. (Slobodno malo opštirnije, napomeni kako je to protokol aplikativnog sloja OSI modela, portovi koje se koriste,..)

GET – Zahtjev za dobijanje resursa od veb servera.

POST – Zahtjev za slanje reursa veb serveru, obično se odnosi na izmjenu postojećih resursa na serveru.

PUT – Zahtjev za slanje resursa veb serveru, obično se odnosi na kreiranje novih resursa na serveru.

DELETE – Zahtjev za brisanje resursa na veb serveru

HEAD – Zahtjev za dobijanje samo zaglavlja od veb servera, bez konkretnog sadržaja.

OPTIONS – Zahtjev za dobijanje dodatnih informacija od strane veb servera.

HTTP kodovi:
HTTP 200 - uspješno slanje zathtjeva i slanje odgovora od servera.
HTTP 204 – uspješno slanje zahtjeva ali nema slanja odgovora od servera.
HTTP 301 – obavještenje da je resurs preusmejeren.
HTTP 404 – resurs nije pronađen na serveru, pogrešno generisanje zahtjeva.
HTTP 500 - Interna greška u usluživanju aplikacije na serveru.

12. TFTP vs FTP (205. stranica)

TFTP(Trivial File Transfer Protocol) je još jedan protkol koji se može koristiti za prenos fajlova.

Baziran je na Client-Server arhitekturi, kao FTP i većina protokola aplikacionog sloja.
TFTP klijent je često u sastavu OS-a, a na nekim sistemima ga je potrebno posebno uključiti ili instalirati.
Nudi samo elementarne funkcionalnosti za prenos fajlova, koristi UDP protkol i port 69 za servesku stranu i 1024+ za klijentsku stranu.

TFTP je dosta zastupljen u administraciji računarskih mreža kao jednostavan mehanizam za prenos konfiguracionih fajlova sa mrežnih uređaja na administratorske radne stanice i obrnuto.

FTP (File Transfer Protocol) je standardni mrežni protokol koji se koristi za prenos fajlova sa jednog računara na drugi preko TCP/IP mreže, poput interneta.

Za razliku od TFTP-a, FTP je mnogo kompleksniji i nudi naprednije funkcije. Njegova osnovna svrha je omogućavanje efikasnog i sigurnog prenosa većih količina podataka. Zbog svoje složenosti i bogatih funkcija, FTP se smatra "punokrvnim" protokolom za prenos fajlova.

FTP koristi **TCP (Transmission Control Protocol)** na transportnom sloju, što mu omogućava pouzdanost i kontrolu toka podataka. Uspostavlja dvije odvojene konekcije: kontrolnu konekciju na **portu 21** za slanje komandi i primanje odgovora, te konekciju za prenos podataka na dinamičkom portu ili na **portu 20**.

Baziran je na **klijent-server arhitekturi**, kao i većina protokola aplikacionog sloja. FTP klijent se obično koristi za pristup FTP serveru i upravljanje fajlovima.

FTP je i danas široko rasprostranjen u administraciji servera i web sajtova, a koristi se i za prenos fajlova unutar internih mreža. Zbog nedostatka enkripcije, za sigurniji prenos se često koriste njegove varijante, poput **FTPS (FTP Secure)** i **SFTP (SSH File Transfer Protocol)**.

13. Telnet, SSH (206. stranica..)

Telnet je mrežni protokol i komandni interfejs koji se koristi za dvosmjernu, tekstualnu komunikaciju s udaljenim računarima.

Baziran je na **Client-Server arhitekturi**, a u OSI modelu pripada sloju aplikacije.

Telnet klijent je često uključen u operativne sisteme, mada ga na novijim sistemima treba naknadno omogućiti.

Telnet pruža **terminalsku funkcionalnost** za pristup i izvršavanje komandi na udaljenom serveru. Podaci se prenose u **nekriptiranom tekstualnom obliku**, što ga čini nesigurnim. Koristi TCP protokol i **port 23**.

Zbog svoje jednostavnosti, Telnet je bio široko rasprostranjen u ranijim fazama razvoja interneta, ali ga je zbog nedostatka enkripcije danas u velikoj mjeri zamijenio SSH.

SSH(Secure Shell) je kriptografski mrežni protokol koji pruža sigurnu, šifriranu komunikaciju između dva računara. Koristi se za udaljenu prijavu na server, izvršavanje komandi i siguran prijenos datoteka.

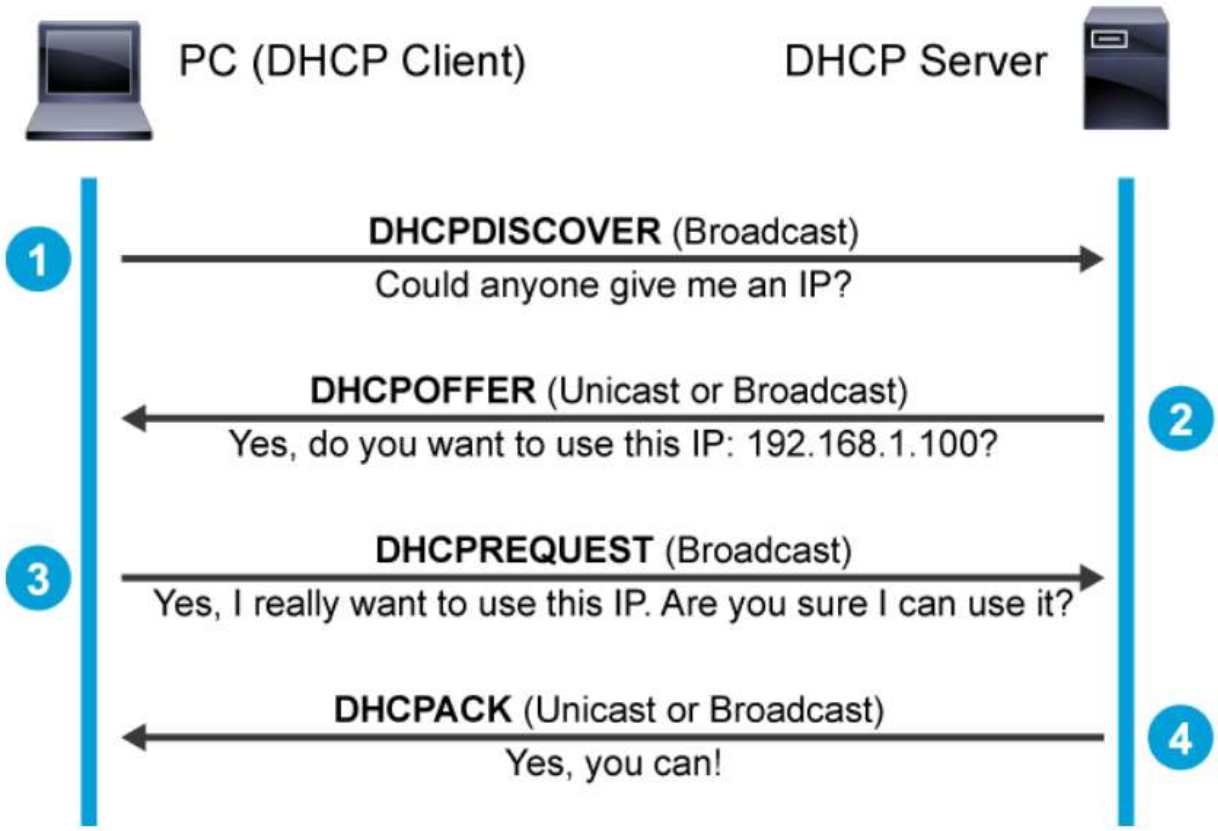
Kao i većina mrežnih protokola, SSH je baziran na **Client-Server arhitekturi** i pripada sloju aplikacije.

SSH klijent je ugrađen u većinu operativnih sistema (npr. Linux, macOS, Windows 10/11), dok SSH server treba instalirati na serveru kojem se želi pristupiti.

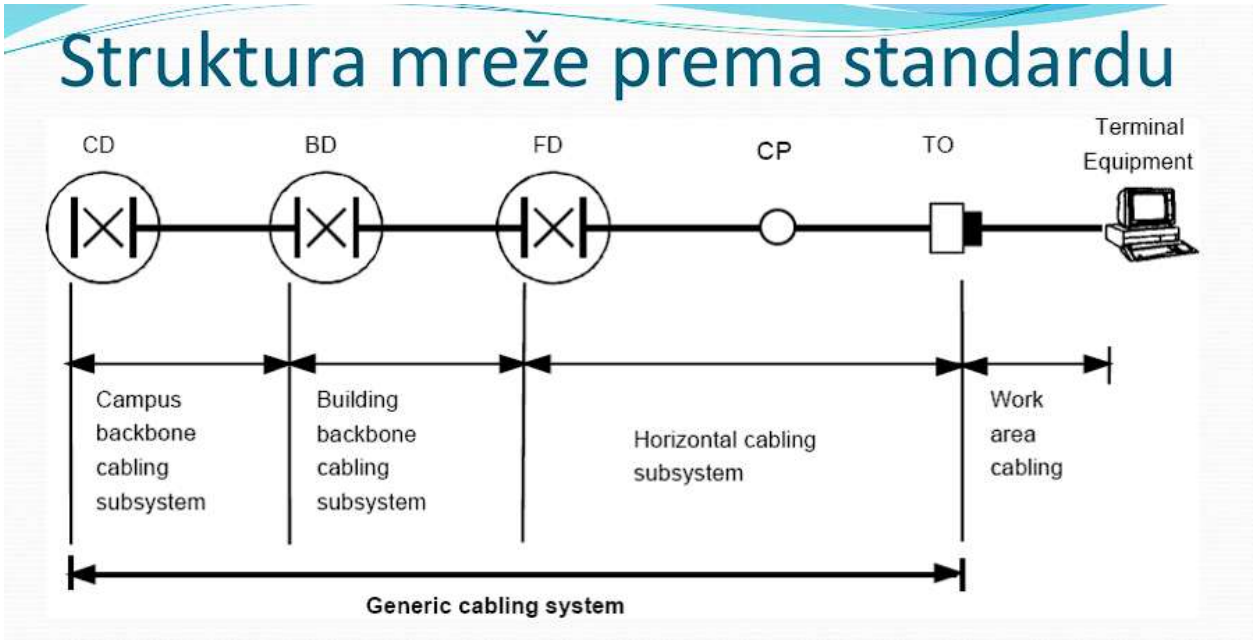
SSH nudi **siguran i šifriran** kanal za komunikaciju. Za autentifikaciju korisnika koristi korisničko ime i lozinku, ili javne/privatne ključeve. Podržava i tuneliranje portova te prosljeđivanje X11 sesija. Koristi TCP protokol i standardno **port 22**.

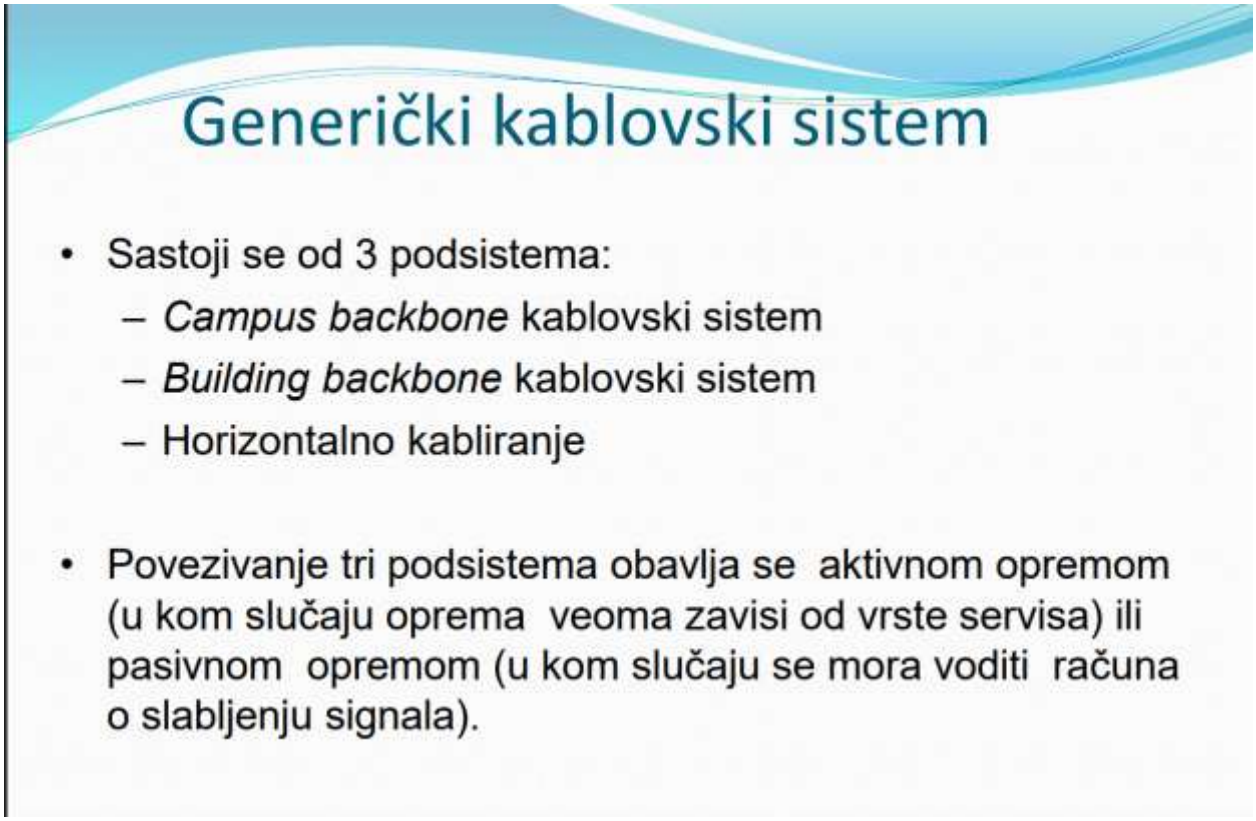
SSH je danas **standard za udaljenu administraciju** mrežnih uređaja i servera, pružajući neophodnu sigurnost koja je nedostajala kod protokola poput Telnet-a.

14. Ilustrovati i opisati komunikaciju DHCP Client-Server (210. stranica..)

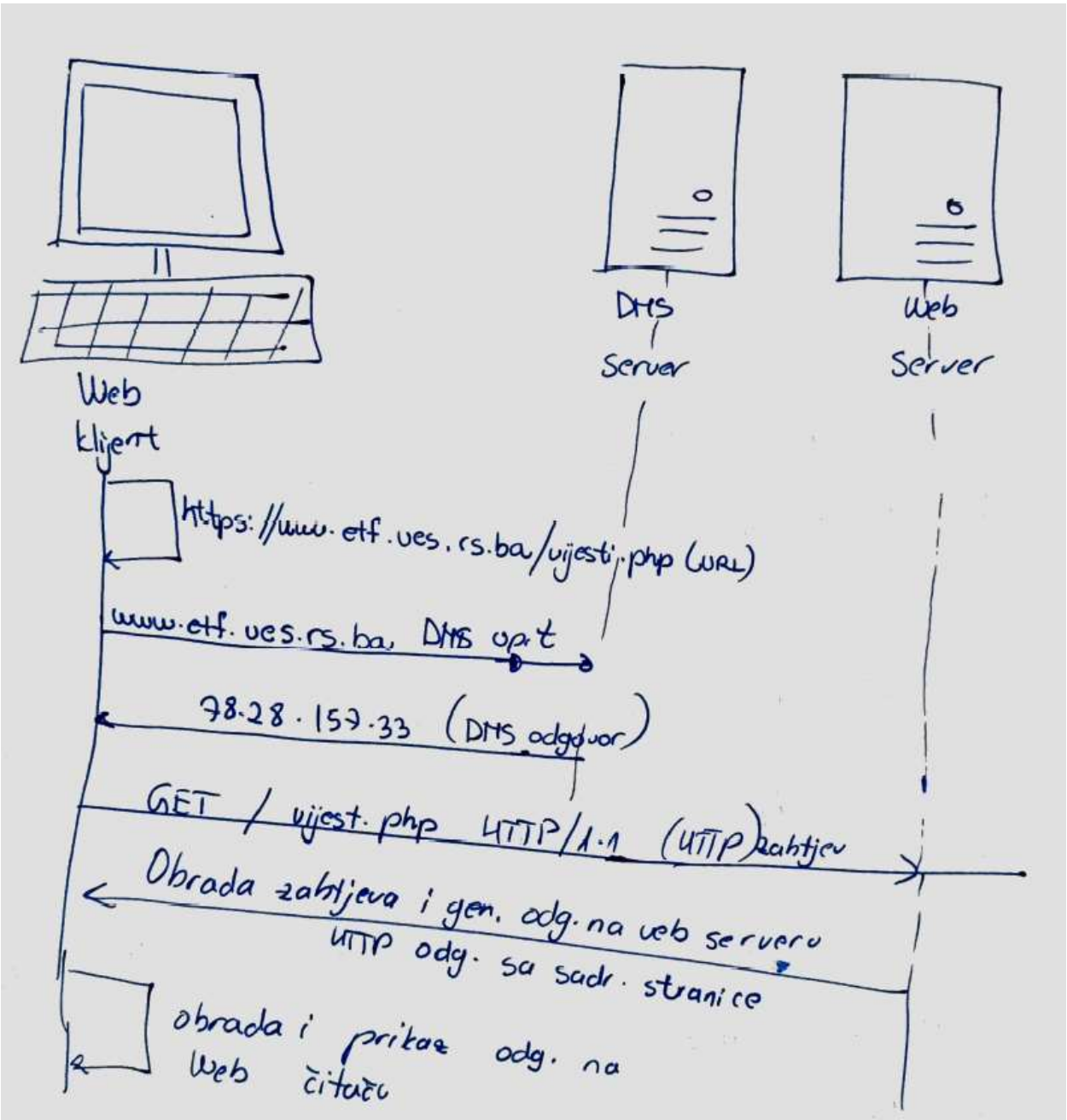


15. generički kablovski sistem, nacrtati i objasniti (stranica 224.)





16. Objasniti Komunikaciju (260. stranica)..zada ti neki primjer i ti onda prepričaš..

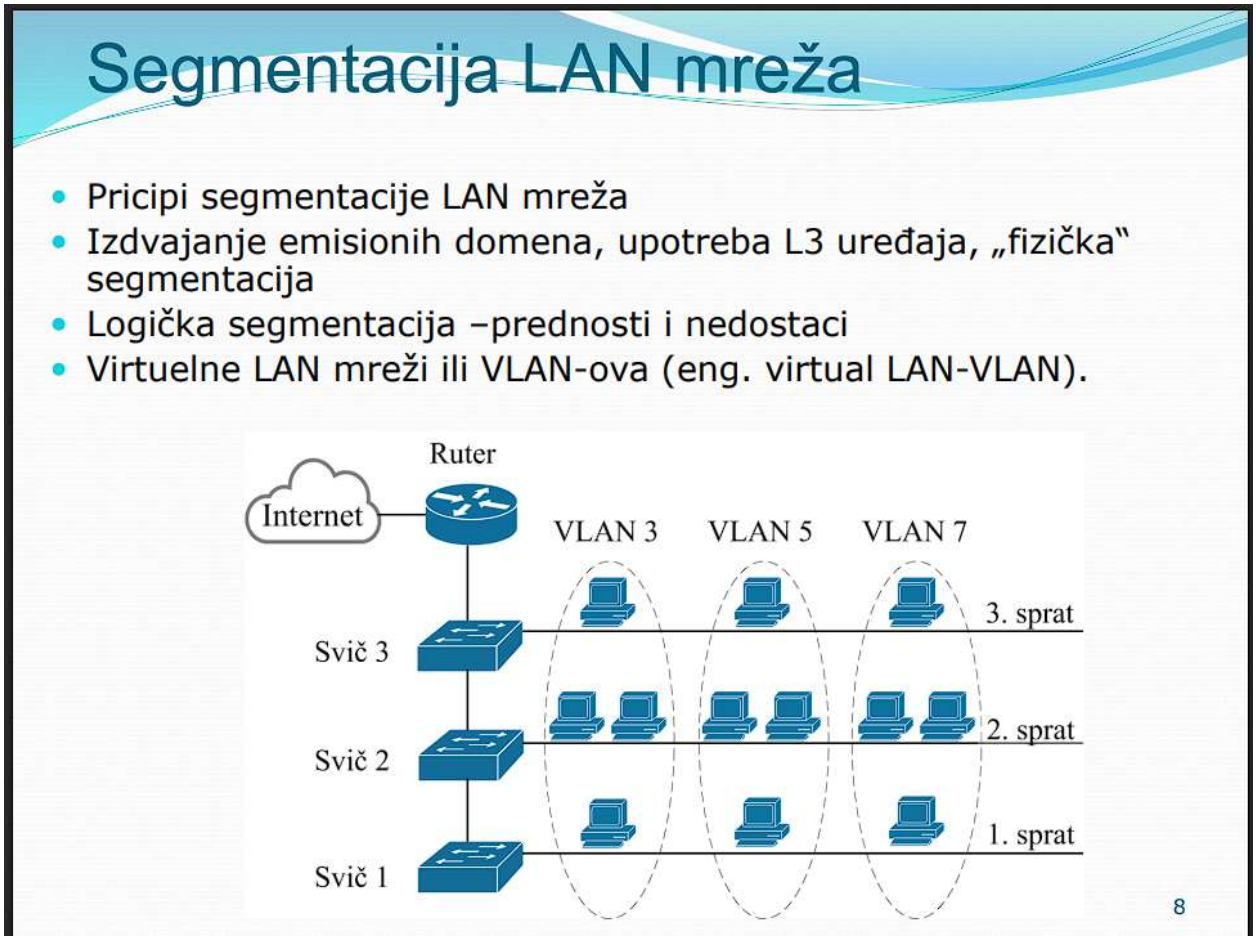


17. Principi segmentacije (237. stranica)

Jedan od važnih zadataka prilikom projektovanja LAN mreža je da se mreža podijeli u manje funkcionalne cjeline, odnosno da se obavi segmentacija mreže.

Ruteri, kao L3 uređaji, omogućuju segmentaciju LAN mreža tako da se dobije više manjih LAN mreža.
Veza prema svakom od segmenata se ostvaruje preko jednog od interfejsa rutera.
Ruteri koji se koriste za segmentaciju LAN mreža uglavnom softverski obrađuju i prosljeđuju saobraćaj.
Saobraćaj između tako dobijenih mrežnih segmenata se mora adekvatno rutirati.

Logička segmentacija LAN mreža se bazira na definisanju virtuelnih LAN mreža ili VLAN-ova.
Može se kazati da svi uređaji koji se nalaze u jednom VLAN-u pripadaju jednom emisionom domenu.
VLAN se definiše kao logička grupa portova jednog sviča i na njih povezanih krajnjih uređaja.
Na sljedećoj slici je ilustrovan princip logičke segmentacije LAN mreža upotrebom VLAN-ova.



Prednosti:

-Fleksibilnost upotrebe LAN mreže koja se ogleda u tome da korisnici mogu da mijenjaju fizičke lokacije radnih mjesta, a da zadrže pripadnost istom VLAN-u.

-Segmentacija i particionisanje resursa LAN mreže.

-Performanse LAN mreže i brzine prenosa paketa se značajno poboljšavaju.

-Sklabilnost LAN mreže je olakšana upotrebom VLAN-ova.

-Mogućnost kreiranja VLAN mreža koje imaju privremeni karakter ili mreža koje imaju specifičnu namjenu.

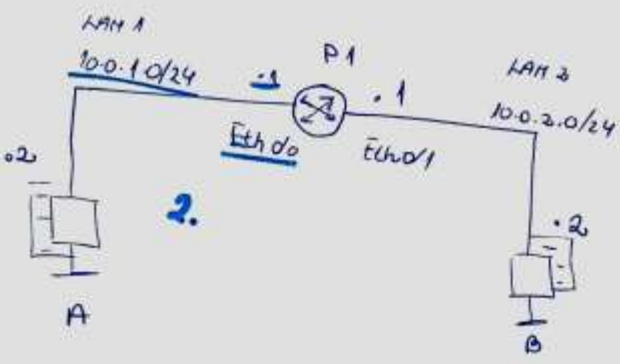
18. Комуникација између хостова у различитим логичким мрежама

Хостови који комуниц. са хостовима изван своје логичке мреже морају да одаберу посредник. индиректно, преко неког мрежног уређаја (посредник).
У случају ове комуникације потребно је да хостови осим своје IP адресе и мрежне маске знају и IP адресу свог подразумјеваног гејтвеја (default gateway) у својој IP конфигурацији.
IP адреса гејтвеја мора да припада истој лог. мрежи као и адресе хостова те мреже, да би се могла остварити директна веза хоста и гејтвеја.
На хосту се може подесити и више гејтвеја, али се подразумјевани користи као крајња инстанца, када нема бољег рјешења.
Као IP адреса гејтвеја узима се прва или задња адреса из распона, опсега логичке мреже, али је могуће користити и било коју др. из тог опсега. Нр:

IP address: 10.0.1.2
Subnet mask: 255.255.255.0
Gateway: 10.0.1.1

Улога гејтвеја је да прихвати пакете из локалне мреже ~~да их~~ који су намијењени хостовима у др. мрежама и да те пакете упути ка одг. одредишту

Као уређај се најчешће користи рутер или рач. са одг. софтвером.
са мин. 2 интерфејса



- У пракси хостови и рутер се повезују на свич, ова веза је овде због поједностављења топологије
- Интерф. рутера не могу имати IP адресе из исте логичке мреже.

Приказане су двије логичке мреже са мрежним адресама 10.0.1.0/24 и 10.0.2.0/24. За IP адресе интерфејса рутера је резервисана прва адреса из расположивог одг. опсега адреса мреже

Када хост A из мреже LAN1 иницира комуникацију са хостом B у LAN2, на основу своје IP конфигурације и одредишне IP он закључује да се хост B не налази у истој логичкој мрежи

Хост A не може директно послати Eth оквир хосту B, већ мора адр. оквир користећи MAC слој деф. гејтвеја.
- У Eth. оквир ће бити смешт. пакет са IP адресом хоста A и IP адресом хоста B.

Комуник. на нивоу везе се одвија између хоста А и његовог гејтвеја (Eth 0/0 R1 на LAN1).

Комуник. на мрежном нивоу се одвија између хост А и В.

МАС адресу гејтвеја хост А може сазнати из своје ARP табеле или користећи ARP протокол, на исти начин као што ради и са др. хостовима у својој мрежи.

Када сазна МАС гејтвеја, хост А енкапс. IP пакет у Eth оквир и шаље га на мрежу.

Пакет стиже до рутера, а врши деенкапсулацију и из оквира извуче IP пакет са изворном IP и одредишном IP.

Рутер доноси одлуку где да прослеђи пакет на основу инф. добијених као резултат изв. ф-ја рутирања (табели рутирања)...

У овом случ. LAN 2 је једина мрежа позната рутеру 1 јер се и један његов интерф. налази у тој мрежи.

А то закључује на основу одр. IP адресе, IP адресе и маске локалног интерфејса Eth0/1 у LAN2.

Све мреже на које је рутер повезан су директно повезане.

Даља комуник. између R2 и B је иста као и у сличном примеру комуник. између хоста у истој лок. мрежи.

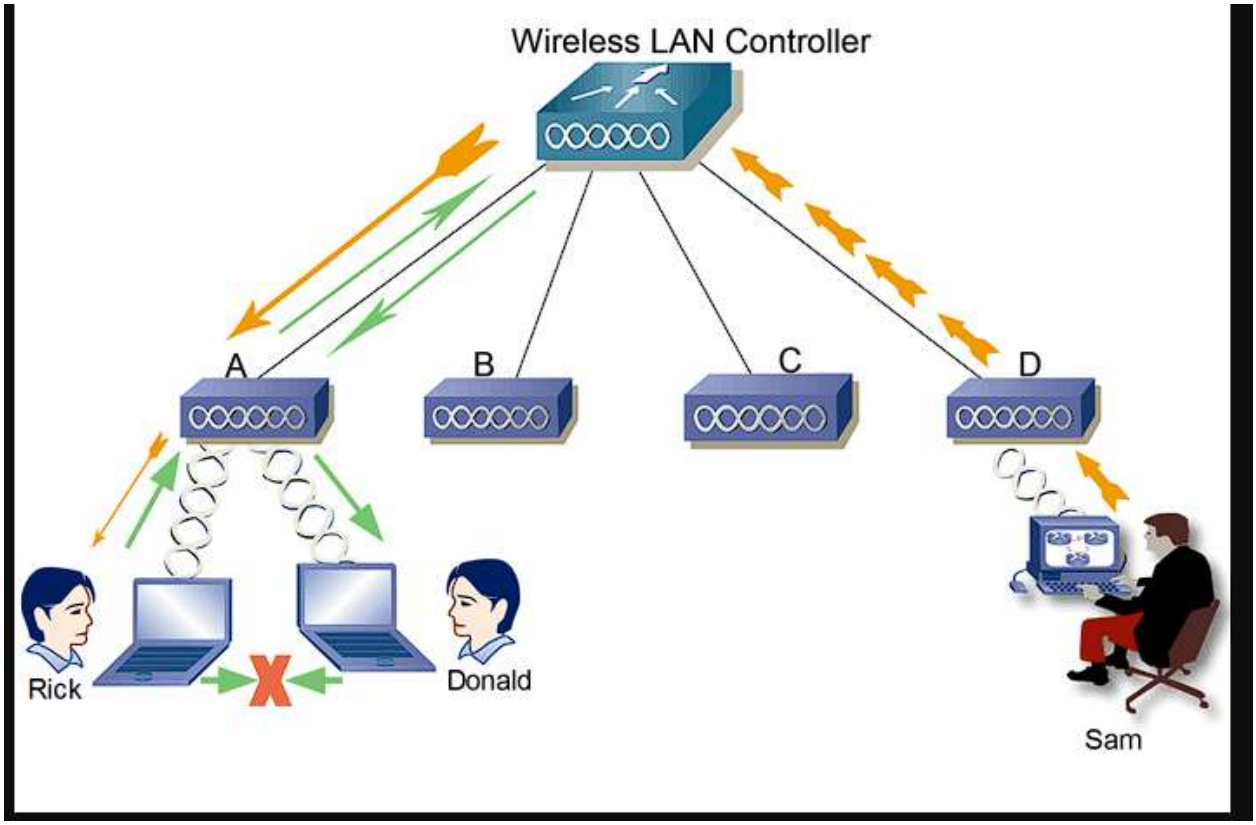
Уколико у обратном смеру тече исто

WLAN kontroler

WLAN kontroler je centralizovani hardverski ili softverski uređaj koji upravlja i kontroliše više bežičnih pristupnih tačaka (**AP - Wireless Access Points**). Njegova glavna svrha je pojednostavljivanje implementacije, upravljanja i obezbjeđivanja sigurnosti u velikim Wi-Fi mrežama. Omogućava administratorima da sa jedne lokacije nadgledaju, konfigurišu i optimizuju čitavu bežičnu mrežu, osiguravajući dosljedne performanse i nesmetano korisničko iskustvo na svim povezanim uređajima.

Ključne funkcije i prednosti

- **Centralizovano upravljanje:** WLAN kontroler funkcioniše kao centralno komandno mjesto, što pojednostavljuje administraciju velikog broja pristupnih tačaka.
- **Pojednostavljena implementacija:** Mrežni administratori mogu lako implementirati, konfigurisati i održavati bežične mreže, smanjujući ukupnu složenost.
- **Poboljšana sigurnost:** Kontroleri mogu automatizovati distribuciju pravila pristupa i sigurnosnih postavki na nivou mreže, čime se poboljšava opšta sigurnost i smanjuju ranjivosti.
- **Optimizacija performansi:** Kontroleri prate pristupne tačke i upravljaju mrežnim saobraćajem kako bi spriječili zagušenja i osigurali dosljedne performanse, posebno za aplikacije koje zahtijevaju visoke performanse kao što su glasovne i video aplikacije.
- **Skalabilnost:** WLAN kontroleri su ključni za velike ili distribuirane bežične mreže, omogućavajući organizacijama da upravljaju stotinama, pa čak i hiljadama pristupnih tačaka.
- **Nadgledanje mreže:** Pružaju uvid u mrežu, što omogućava administratorima da prate status pristupnih tačaka, povezanih klijenata i opšte stanje mreže.
- **Otkrivanje neovlaštenih pristupnih tačaka:** Kontroleri mogu otkriti i reagovati na neovlaštene pristupne tačke (**rogue APs**) u mreži.
- **Besprekorno roming iskustvo:** U okruženjima sa više pristupnih tačaka, kontroler pomaže u omogućavanju nesmetanog rominga, održavajući stabilnu vezu i performanse dok se korisnik kreće mrežom.


Wireless LAN Controller
A
B
C
D
Rick
Donald
Sam

OBAVEZNO PREĐI SVE PRAKTIČNE PRIMJERE IZ KNJIGE!!