KOMUNIKACIJSKE MREŽE

⇒ komunikacijska mreža ⇒ povezan komunikacijski sustav na koje se spaja druga korisnička oprema (npr. računala)

⇒ klasična podjela mreža - gorna mreža
- podatkovna mreža
↳ danas ta podjela više nije aktualna ⇒ se koristi pojam INTEGRIRANA MREŽA

⇒ danas se mreže dijele po:
- rasprostranjenosti
- namjeni (javna / privatna)
- vrsti informacije (slika / zvuk / podatak / ...)
- načinu komuniciranja (kanal / paket)
- topologiji (povezanost čvorova)
- pokretljivosti korisnika

⇒ zvuk i govor se bolje prenose preko kanala jer je kanal rezerviran cijelo vrijeme za trajanje komunikacije te je time osigurana komunikacija bez kašnjenja, u stvarnom vremenu
↳ no, kanal nije dobro rješenje za podatke jer se podaci prenose u paketima, a ne kontinuirano, pa je odviše skupo rezervirati kanal na tako dugo vrijeme (npr. DIAL-UP je koristio kanal)

⇒ dalnji nedostatak paketa je ta da se dio kapaciteta troši na upravljačku informaciju koja se naziva ZAGLAVLJE PAKETA (eng. packet header)

↳ informacija koja se prenosi kanalom ne treba zaglavlje jer se točno zna od kuda do kuda je kanal uspostavljen

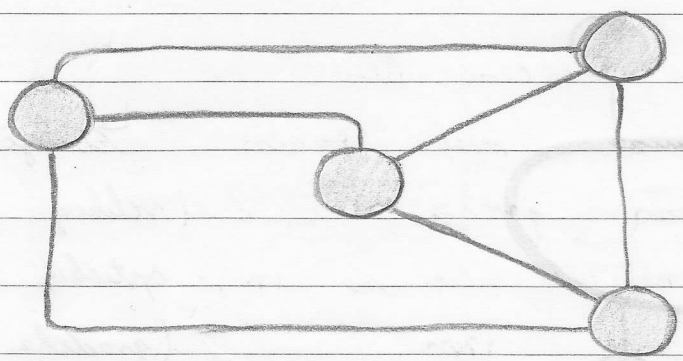
⇒ u mreži koja komunicira paketima, moguće je uspostaviti VIRTUALNE KANALE i tako pakete slati uvijek istim putem

↳ time možemo izvedbu kašnjenja paketa i tako osigurati bolji prijenos govora

⇒ paket koji se ne šalje odredenim putem, već se šalju zasebnim putevima, medijima i čvorovima nazivaju se DATAGRAM

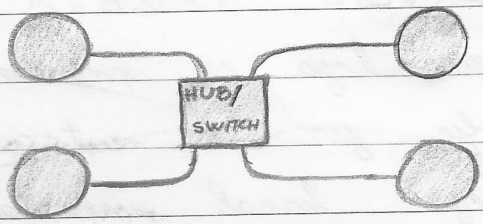
⇒ RAZLIČITE TOPOLOGIJE:

a) potpuna povezanost - izravna povezanost svaka dva čvora u mreži (otporno na kvarove, ali skupo!)



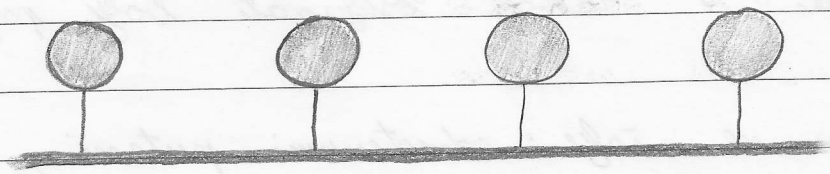
↳ prilagođena na mreže s manjim brojem čvorova

b) **zvijezda** - na središnji čvor su spojeni ostali čvorovi (npr. hotspot)



↳ primjena za lokalne mreže

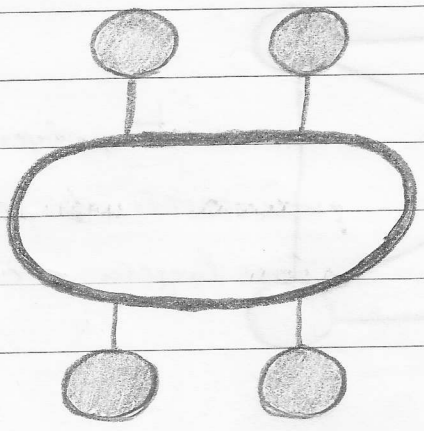
c) **sabirnica** („bus") - svi čvorovi priključeni na zajednički prijenosni medij
- potrebni su mehanizmi dodjele prava komuniciranja (protokoli)



↳ ojačalo na kraju
↳ lokalne mreže

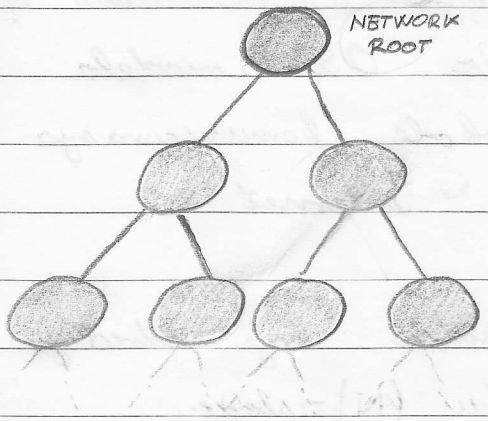
⇒ NAPOMENA: danas su računala najčešće spojena u zvijezdu preko, ali i dalje logički funkcioniraju kao sabirnice

d) **prsten** - svi čvorovi spojeni na zajednički medij koji stvara zatvoren put



↳ najčešće za mreže velikog kapaciteta i optičkih kabela (gradske mreže)

c) stablo - hijerarhijska struktura komunikacije



↳ koristi se kod regionalnog umrežavanja i pobrežnih mreža

⇒ ARHITEKTURA MREŽE:

a) DIJELOVI MREŽE

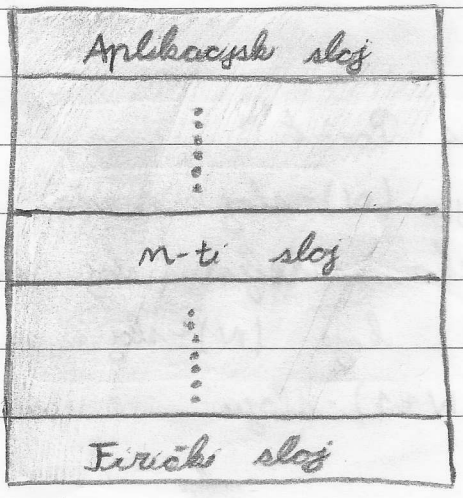
1) pristupna mreža - preko nje se korisnici priključuju

2) jezgrena mreža - povezuje sustave u pristupnoj mreži i omogućuje komunikaciju

b) SLOJEVI MREŽE

↳ najviši sloj - usluge pružene korisniku

↳ najniži sloj - prijenos informacija medijem



↳ niži sloj uvijek pruža usluge višem sloju

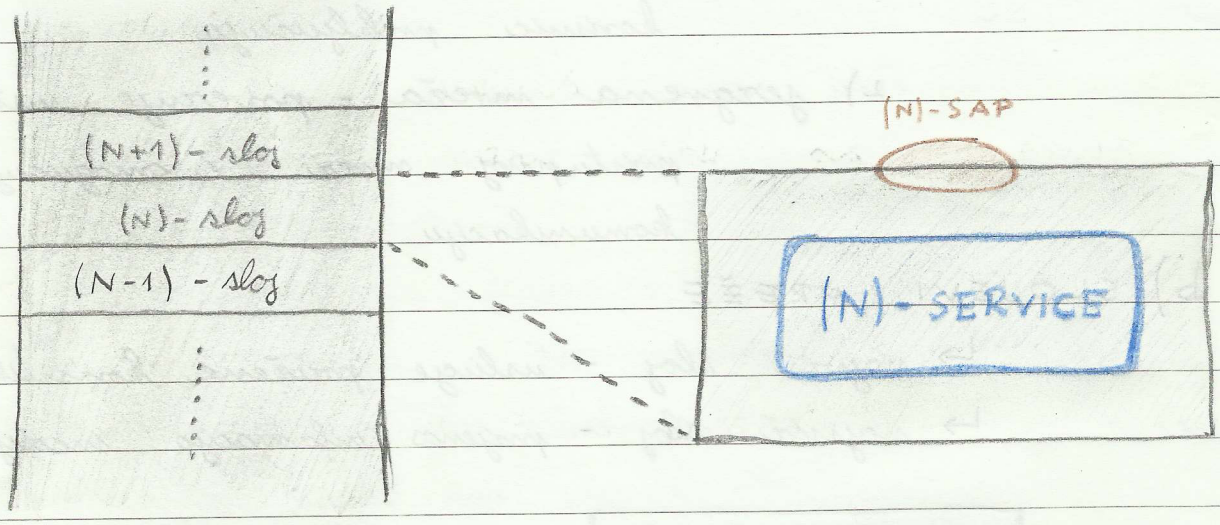
⇒ OSNOVNI MODELI:

a) OSI ⇒ „Open System Interconnection Reference Model"
⇒ otvoreno rješenje, neovisno o proizvođaču opreme

b) TCP/IP ⇒ nastao iz OSI modela i definirao protokole komuniciranja te je uveo naziv Internet

⇒ protokol ⇒ skup pravila i formata koji određuju komunikacijsko ponašanje u (N)-sloju

⇒ spojna usluga realizira se nekom vrstom kanala, a nespojna usluga realizira se kao datagram
↳ Internet je nespojna usluga



- (N)-SAP ⇒ „Service Access Point"
⇒ točka u kojoj (N)-sloj pruža (N)-usluga sloju iznad preko sučelja (sloj iznad je (N+1)-sloj)
- (N)-SERVICE ⇒ mogućnost koje (N)-sloj i slojevi ispod njega pružaju (N+1)-sloju

REFERENTNI MODEL OSI

⇒ „Open System Interconnection"

⇒ model se sastoj od 7 slojeva

7.	Aplikacijski sloj (Application Layer)
6.	Prezentacijski sloj (Presentation Layer)
5.	Sjednički sloj (Session Layer)
4.	Transportni sloj (Transport Layer)
3.	Mrežni sloj (Network Layer)
2.	Sloj podatkovne poveznice (Data Link Layer)
1.	Fizički sloj (Physical Layer)

1) FIZIČKI SLOJ:

- komunikacija nekim fizičkim medijem
- odvija se na razini **bita**

2) SLOJ PODATKOVNE POVEZNICE:

- odvija se na razini **okvira**
- promatra komunikaciju između dva direktno povezana čvora
- koristi MAC adresu mrežne kartice
- osnovna funkcija je prijenos okvira od jedne do neke druge točke

3) MREŽNI SLOJ

- on gleda komunikaciju na dva krajnja čvora i bira mreže za put paketa (odvija se na razini **paketa**)

4) TRANSPORTNI SLOJ:

- osigurava prijenos bez pogrešaka i nepotrebno kašnjenje
- odvija se na razini **segmenata**

5) SJEDNIČKI SLOJ:

- usklađuje sustave za zajedničku komunikaciju

6) PREZENTACIJSKI SLOJ:

- osigurava pravilan prikaz i značenje informacija

7) APLIKACIJSKI SLOJ:

- pruža aplikacije i usluge za korisnike
- skup protokola za korisničke aplikacije

INTERNETSKI MODEL (TCP/IP)

4.	Aplikacijski sloj	
3.	Transportni sloj	TCP
2.	Mrežni sloj, Internetski sloj	IP
1.	(nije definiran, ali je fizičke razine)	

2) MREŽNI SLOJ, INTERNETSKI SLOJ:

- koristi se IP (Internet Protocol) i dodatni protokol za usmjeravanje
- međusobno povezivanje mreža i podmreža
- na razini paketa i svaki paket se usmjerava zasebno (svojim putem) → **datagram**
- stare usluge se često koriste IP-om:
  - a) IP over X (IPoX)
  - b) X over IP (XoIP)

3) TRANSPORTNI SLOJ:

- koriste se dva protokola:
  - a) TCP (Transmission Control Protocol)
    - ↳ provjerava pogreške i redoslijed
    - ↳ nešto sporiji od UDP-a
  - b) UDP (User Datagram Protocol)
    - ↳ ne garantira isporuku i pravilan redoslijed

4) APLIKACIJSKI SLOJ:

- korisnički protokol (SMTP, HTTP, ...)

KVALITETA VEZE

⇒ MREŽNE PERFORMANSE:

a) ŠIRINA POJASA („bandwidth")

↳ maksimalni broj bita koji se može prenijeti u jedinici vremena

↳ izražava se u bit/s

b) PROPUSNOST („throughput")

↳ broj korisnih bitova prenesen u jedinici vremena

↳ manja je od širine pojasa jer se uz informaciju prenosa i dodatne bitove vezane uz protokole i slično

c) KAŠNJENJE („latency")

↳ vrijeme potrebno da bit stigne s izvora na odredište

↳ izražava se u „ms"

FIZIČKI SLOJ 1
PRIJENOSNI MEDIJ

⇒ fizički sloj omogućava prijenos na određenu udaljenost i radi na bitu kao jedinici podataka

⇒ kapacitet komunikacijskog kanala određuju:
- širina prijenosnog pojasa (B)
- odnos signal / šum (S/N)

⇒ PRIJENOSNI MEDIJI:

a) OMEĐENI MEDIJI:
- parica (UTP - „Unshelded Twisted Pair")
- koaksijalni kabel
- optičko vlakno

b) NEOMEĐENI MEDIJI:
- radijski frekvencijski spektar
- bežični prijenos
- infracrveni, optički, laserski, mikrovalni, ...

⇒ PARICA (UTP - kabel):

↳ brzina prijenosa ovisi o:
- debljini žica, duljini žica, načinu upredanja, ...

↳ postoje kategorije parica:
- CAT 5 (brzina do 100 Mbit/s)
- CAT 6 (brzina do 1 Gbit/s)

↳ npr. ADSL radi do 5.5 km od centrale

⇒ OPTIČKO VLAKNO („fiber optics")

↳ svjetlo se šalje kroz staklast medij

↳ jednomodno vlakno ⇒ veća brzina prijenosa uz prijenos na veće udaljenosti (50 Gbit/s, 100 km), ali ima skuplju opremu

↳ višemodno vlakno ⇒ jednostavnija i jeftinija oprema i nešto manja brzina (10 Gbit/s, 500 m)

↳ prednosti nad bakrom:

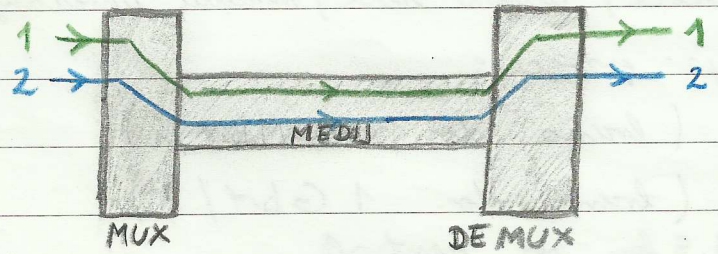
- veća brzina
- malo gušenje signala
- neosjetljivost na elektromagnetske smetnje
- neosjetljivost na korozju
- tanki i lagani kabel
- prisluškivanje teško izvedivo

⇒ VIŠESTRUKA UPOTREBA PRIJENOSNOG MEDIJA:

↳ želimo raditi **multipleksiranje** - više korisnika može koristiti isti prijenosni medij istodobno

↳ podjela po komponentama informacijskog volumena:

- **frekvencija** (najčešće) il valna duljina
- vrijeme
- valna duljina
- kod



SLOJ PODATKOVNE POVEZNICE

⇒ bavi se prijenosom između dva direktno povezana čvora
⇒ odvija se na razini okvira
⇒ obrađuju se pogreške u prijenosu jer mrežni sloj očekuje da se prijenos između svaka dva direktno povezana čvora odradio ispravno
⇒ brine se o toku podataka (kontrolira zagušenje)

⇒ OBLIKOVANJE PODATKOVNE POVEZNICE:
↳ to oblikovanje definira očekivano ponašanje (jedinica podataka, otkrivanje ili ispravljanje pogrešaka, ...)

⇒ OKVIR:
- polje podataka
- polje upravljačkih podataka (zaglavlje, završetak)
- fiksna il varijabilna duljina okvira
  ↳ fiksna duljina se koristi za bežični prijenos
  ↳ varijabilna se često koristi za žični prijenos

⇒ USLUGE SLOJA PODATKOVNE POVEZNICE:

a) nespojna usluga bez potvrde

↳ izvor šalje neovisne okvire

↳ odredište ne potvrđuje prijem (gubitak moguć)

↳ primjena: za lokalne mreže, za komunikaciju u stvarnom vremenu

b) nespojna usluga s potvrdom

↳ izvor šalje neovisne okvire

↳ odredište potvrđuje prijam

↳ ukoliko izvor ne primi potvrdu, ponovno se šalje okvir (retransmisija)

↳ primjena: prijenos za jako izraženim smetnjama (npr. bežični)

c) spojna usluga s potvrdom

↳ uspostavlja se logička veza između izvora i odredišta

↳ svaki okvir je označen brojem i okviri se šalju točnim redoslijedom

↳ izvor treba potvrdu prijema

↳ primjena: u mrežama koje trebaju veliku pouzdanost

⇒ upravljanje pogreškama: mjera je BER ("Bit Error Rate")

↳ dobro je ako imamo vjerojatnost pogreške oko 10^{-9} (optički kabel)

PROTOKOLI PODATKOVNE POVEZNICE

⇒ PROTOKOL ⇒ skup pravila i formata za postupak razmjene informacija u mreži kako bi predajnik i prijamnik bili usklađeni

⇒ sloj podatkovne poveznice treba osigurati:
- razmjenu okvira
- upravljanje pogreškama
- upravljanje tokom

⇒ MODELI PROTOKOLA (jednostavni):

a) jednosmjerni protokoli:
1) jednosmjerni protokol bez ograničenja
2) jednosmjerni protokol „Stani i čekaj"

b) dvosmjerni protokoli:
1) dvosmjerni protokol „Stani i čekaj"

⇒ MODELI PROTOKOLA (složeni):

↳ „okvir po okvir" je prilično neučinkovito, pa se je razvio „KLIZEĆI PROZOR":
- šaljemo nekoliko okvira bez potvrde
- ratin, kako dobivamo potvrde, šaljemo nove okvire
- broj okvira se dinamički mijenja („prozor klizi")

LOKALNA MREŽA

⇒ standard: Ethernet, IEEE 802.3

⇒ danas se najčešće lokalne mreže rade pomoću dvanaestom (engl. „hub", „switch") u topologiji zvijezde

⇒ imamo problem dodjeljivanja fizičkog medija računalima koje istodobno žele komunicirati

⇒ sloj podatkovne poveznice dijelimo na dva podsloja kada govorimo o lokalnim mrežama:

a) SLOJ UPRAVLJANJA PRISTUPNOM MEDIJU

↳ engl MAC ⇒ „Media Access Layer"

↳ **dinamička** dodjela medija

↳ izvodi se na mrežnim karticama

↳ upravljanje pristupa mediju s distribuiranom

↳ **slučajni pristup mediju:**

• protokol ALOHA

↳ stanica šalje podatke kada ih ima

↳ ako više stanica pošalje podatke, dolazi do „sudara" i okviri su uništeni

↳ ponavlja se slanje okvira

↳ stoga, mrežne kartice imaju različita vremena retransmisije kako bi se izbjegli uzastopni sudari

↳ danas se još uvijek koriste u nekim slučajevima

- protokol CSMA/CD
  - ↳ prije slanja, ustanovljava se je li medij zauzet mjerenjem napona
    - ↳ engl. „Carrier Sense Multiple Access / Collision Detect"
      - ↳ rad s Ethernetom do 100 M bit/s

b) SLOJ UPRAVLJANJA LOGIČKOM POVEZNICOM

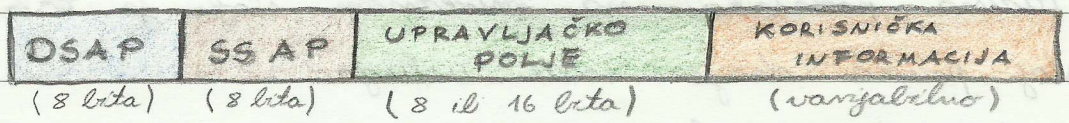
↳ omogućuje protokolima mrežnog sloja da dijele podatkovnu poveznicu (multipleksiranje)

↳ izveden je kao upravljački program

↳ razmjena okvira između stanica lokalne mreže

⇒ struktura jedinice podataka

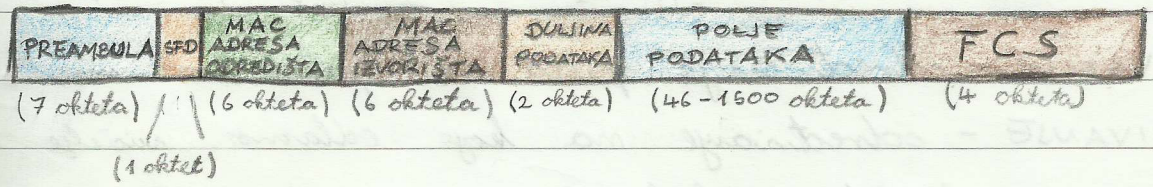
↳ PDU: „Packet Data Unit"



DSAP ⇒ odredišna točka pristupa usluzi („Destination SAP")

SSAP ⇒ izvorišna točka pristupa usluzi („Source SAP")

⇒ struktura okvira na IEEE 802.3:



↳ imamo minimalnu veličinu okvira (72 okteta) jer time na udaljenost do 100m imamo sigurnu detekciju sudara

BITNO!

MREŽNI SLOJ

⇒ Zadaća mrežnog sloja:
↳ komunikacija između dva krajnja (korisnička) čvora u mreži (to se rad izravno ili preko niza međučvorova)

⇒ da bi mrežni sloj to izvršio, on treba slijedeće funkcionalnosti:
- adresiranje
- usmjeravanje
- upravljanje tokom, pogreškama i zagušenjem
- povezivanje mreža i podmreža

⇒ osnovna razina podataka na mrežnom sloju je PAKET
⇒ mrežni sloj pruža dvije vrste usluga:
a) spojna usluga
b) nespojna usluga (INTERNET)
↳ izvedba usmjeravanja u mrežama s komutacijom paketa:
a) datagram (INTERNET)
b) virtualni kanal

⇒ USMJERAVANJE - određivanje puta za paket kroz mrežu
⇒ PROSLJEĐIVANJE - određivanje na koje odlazno sučelje proslijediti paket
↳ druge naziv: a) routing
b) forwarding

⇒ NAČELO OPTIMALNOSTI:

↳ ako je J na optimalnom putu od usmjeritelja I do odredišta K, onda je put od J dó K dionica tog puta

⇒ <u>algoritmi usmjeravanja</u> (PODJELA):

a) neadaptivni (statički)

- unaprijed izračunati puteve na temelju nekih kriterija (npr. udaljenost, cijena, ...)
- putevi se postavljaju prilikom prvog pokretanja čvora i više se ne mijenjaju

b) adaptivni (dinamički)

- donose odluke na temelju mjerenja ili procjena stanja u mreži

1) USMJERAVANJE NAJKRAĆIM PUTEM:

⇒ statički algoritam

⇒ računa se najkraći put od svih čvorova prema zadanom čvoru u grafu

↳ to se računa Dijkstrinim algoritmom (pogledaj slajdove!)

2) PREPLAVLJIVANJE:

⇒ statički algoritam

⇒ prosljeđuje se paket na svako odlazno sučelje, osim onog od kojeg je pristigao paket (viđen paket se odbacuje)

⇒ uvijek dođe najkraći put

3) USMJERAVANJE VEKTOROM UDALJENOSTI:

⇒ dinamički algoritam

⇒ svaki usmjerivač ima tablicu (vektor) koji daje najbolju „poznatu udaljenost" za svako odredište i prvi korak ka njemu

⇒ algoritam sporo reagira na loše vijesti, ali brzo reagira na dobre

4) USMJERAVANJE STANJEM POVEZNICE:

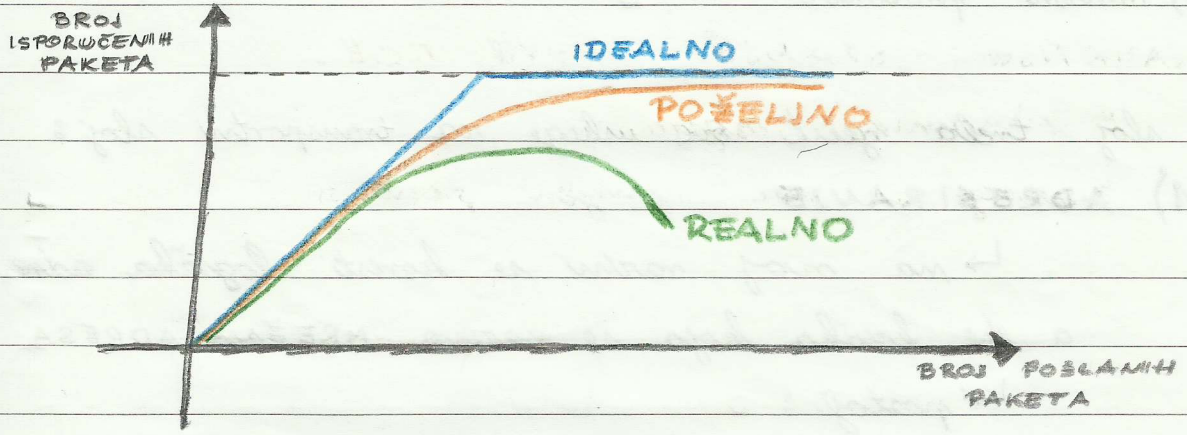
⇒ dinamički algoritam

⇒ temelji se na razmjeni podataka u topologiji

PROBLEMI I MOGUĆNOSTI MREŽNOG SLOJA

⇒ ZAGUŠENJE:

↳ degradacija performansi mreže zbog prevelikog broja paketa u mreži



↳ stvara se red čekanja na čvorovima te se paket spremaju u spremnik

↳ upravljanje zagušenjem:

a) rješenja otvorenim pojmom
   - ograničeni prihvat korisnika
   - upravljanje prometom

b) rješenja zatvorenim pojmom
   - modeliranje veličina spremnika

POVEZIVANJE MREŽA I PODMREŽA

⇒ svaka mreža ima:

a) organizaciju
b) adresiranje
c) mrežni protokol

} ARHITEKTURA MREŽE

⇒ mrežni sloj treba ponuditi ove usluge na transportni sloj:

1) ADRESIRANJE

↳ na ovoj razini se koristi **logička adresa**, a ne fizička koja se naziva MREŽNA ADRESA

↳ postoji:

a) dinamička mrežna adresa
- dodjeljena tijekom pružanja usluge
- npr. IP-adresa

b) statička mrežna adresa
- dodjeljena trajno
- plaća se jer se rauzima adresa

2) FRAGMENTACIJA

↳ jedinica je PDU - „Packet Data Unit"

↳ svaka podmreža ima različitu veličinu **fragmentacije** (transparentna fragmentacija) il je ta veličina **fragmentacije** fiksna (netransparentna fragmentacija) - internet je netransparentan

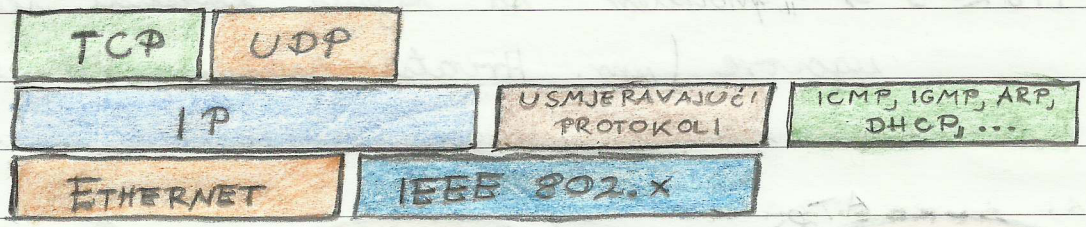
3) POVEZIVANJE MREŽA

MREŽNI SLOJ U INTERNETU

⇒ IP ⇒ „Internet Protocol"

⇒ rad adresiranje, format datagrama i fragmentacije

⇒ načelo datagrama ⇒ svaki paket se usmjerava zasebno



⇒ organizacija Interneta:

- puno povezanih mreža raznoraznih na TCP/IP arhitekturi i protokolima

⇒ AUTONOMNI SUSTAV ⇒ skup IP mreža i usmjeritelja pod zajedničkom upravom i sa zajedničkom politikom usmjeravanja (npr. CARNet, on dijeli adrese „providerima", a IANA je dodijelila tu titulu CARNet-u)

⇒ unutar autonomnog sustava, koriste se protokol za UNUTARNJE USMJERAVANJE

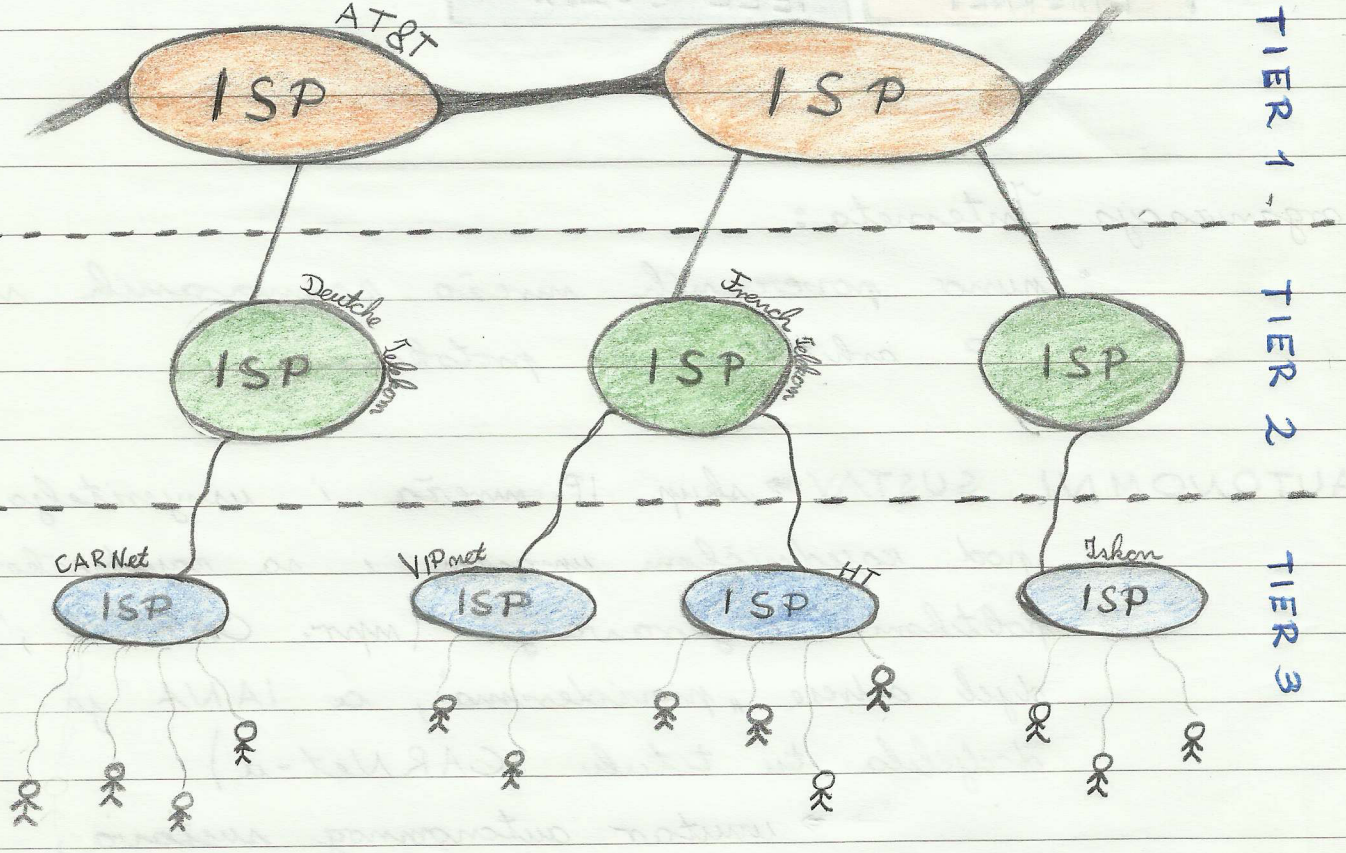
↳ npr. OSPF („Open Shortest Path First")

⇒ HIJERARHIJA INTERNETA

a) TIER 1 ⇒ „provideri" koji povezuju mreže najviše razine i postoji ih desetak (npr. AT&T) te su gotovo svi u Americi

b) TIER 2 ⇒ „provideri" više telekomunikacijske razine koji uzimaju usluge od TIER 1 (npr. Deutsche Telekom)

c) TIER 3 ⇒ „provideri" sa kojima korisnici sklapaju ugovore (npr. Hrvatski Telekom, VIPnet)



⇒ideja Interneta je da je standardizacija minimalna tako da se omogući povezivanje

↳ postoji mnogo protokola, ali se zna koji su „Best Practice"

↳ svatko može predložiti neko poboljšanje nekog protokola ili druge funkcionalnosti Interneta

PROTOKOL IP

⇒ standardni protokol

⇒ odlike:

- neovisan o nižim protokolima
- datagramsko načelo
- nespojna usluga
- nepotvrđena usluga
- nema garancije očuvanja redoslijeda datagrama

⇒ glavna uloga jest OMATANJE:

↳ uzima podatke od višeg sloja i dodaje mu IP-zaglavlje i daje taj cijeli omotan podatak nižem sloju

⇒ IP protokol jest **netransparentan** što znači da se podaci sastavljaju tek na cilјnom čvoru, a ne na svakom međučvoru

⇒ IP ADRESA ⇒ identifikator koj globalno i jednoznačno određuje mrežno sučelje

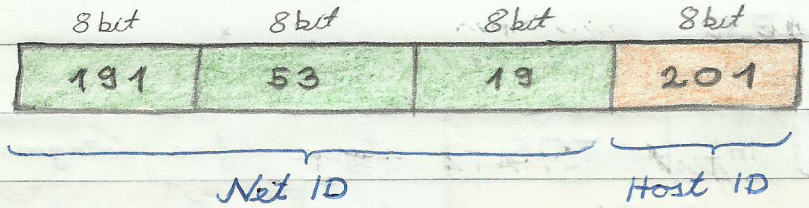
↳ krajnji čvor ima jednu, a mrežni čvor više IP adresa

⇒ DIJELOVI IP - ADRESE:

a) identifikator mreže („Net ID") ⇒ određen broj bitova koji identificira mrežu u kojoj se nalazi krajnji čvor

b) identifikator krajnjeg računala („Host ID") ⇒ određen broj bitova koji identificira krajnji čvor u mreži

⇒ primjer adrese:



↳ no, problem je ovih 24 bita za Net ID jer previše vremena trošimo da pretražimo 2^{24} mreža da nađemo pravu, pa se to još dijeli na podmreže i koristi se maskiranje

⇒ besklasno adresiranje:

195.24.0.0/13

/13 ⇒ definira se broj bitova za identifikator mreže

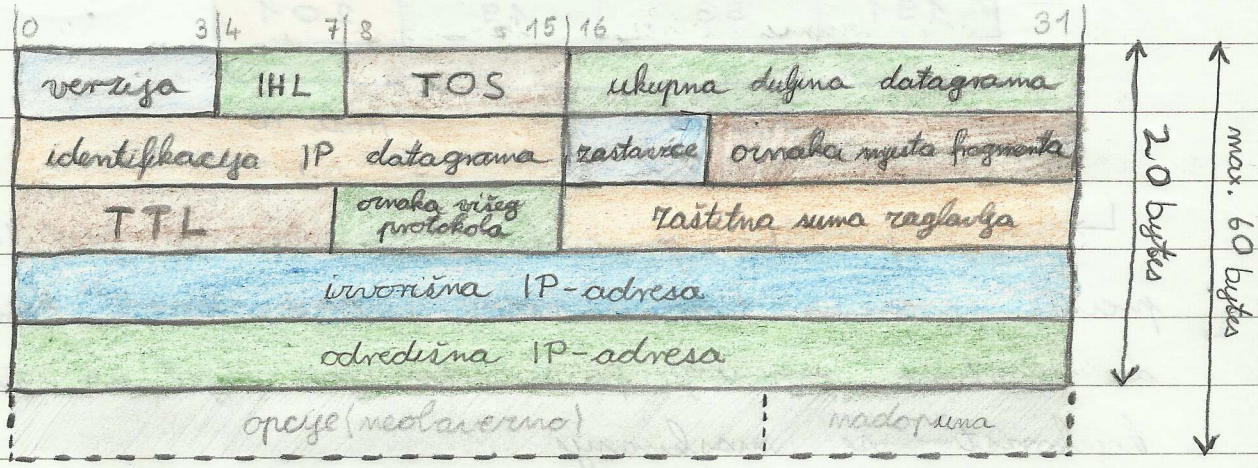
↳ danas se sve više koristi besklasno adresiranje jer je učinkovitije definirati određen broj bitova za Net ID za gotovo sve primjene

⇒ DODJELA IP-ADRESA:

a) statička ⇒ uvijek ista IP-adresa
⇒ koristi se za poslužitelje / servere

b) dinamička ⇒ adresa i postavke se od „providera"
⇒ koristi se za osobna računala
⇒ prilikom povezivanja na Internet, DHCP našeg „providera" nam dodjeli adresu

⇒ IP-ZAGLAVLJE:



- IHL ⇒ „Internet Header Length"
  ⇒ broj 32-bitnih riječi u zaglavlju
- ukupna dužina datagrama ⇒ veličina cijelog paketa, uključujući zaglavlje i podatke u bajtovima
- TTL ⇒ „Time to Live"
  ⇒ brojač koji se smanjuje na svakom čvoru kako bi se spriječilo beskonačno kruženje paketa Internetom
- identifikacija ⇒ jedinstvena oznaka datagrama koja se koristi kako bi se prepoznali fragmenti jednog datagrama
- oznaka mjesta fragmenta ⇒ koristi se za sastavljanje fragmenata

USMJERAVANJE NA INTERNETU

⇒ usmjeravanje - postupak pronalaženja puta od izvorišta do odredišta, izravno ili preko niza usmjerivača

⇒ prosljeđivanje - odluka unutar usmjerivača

⇒ usmjeravanje se vrši korištenjem odredišne IP-adrese
↳ ako su izvor i odredište u istoj mreži, onda on komunicira izravno, a ako nisu, onda preko niza usmjerivača

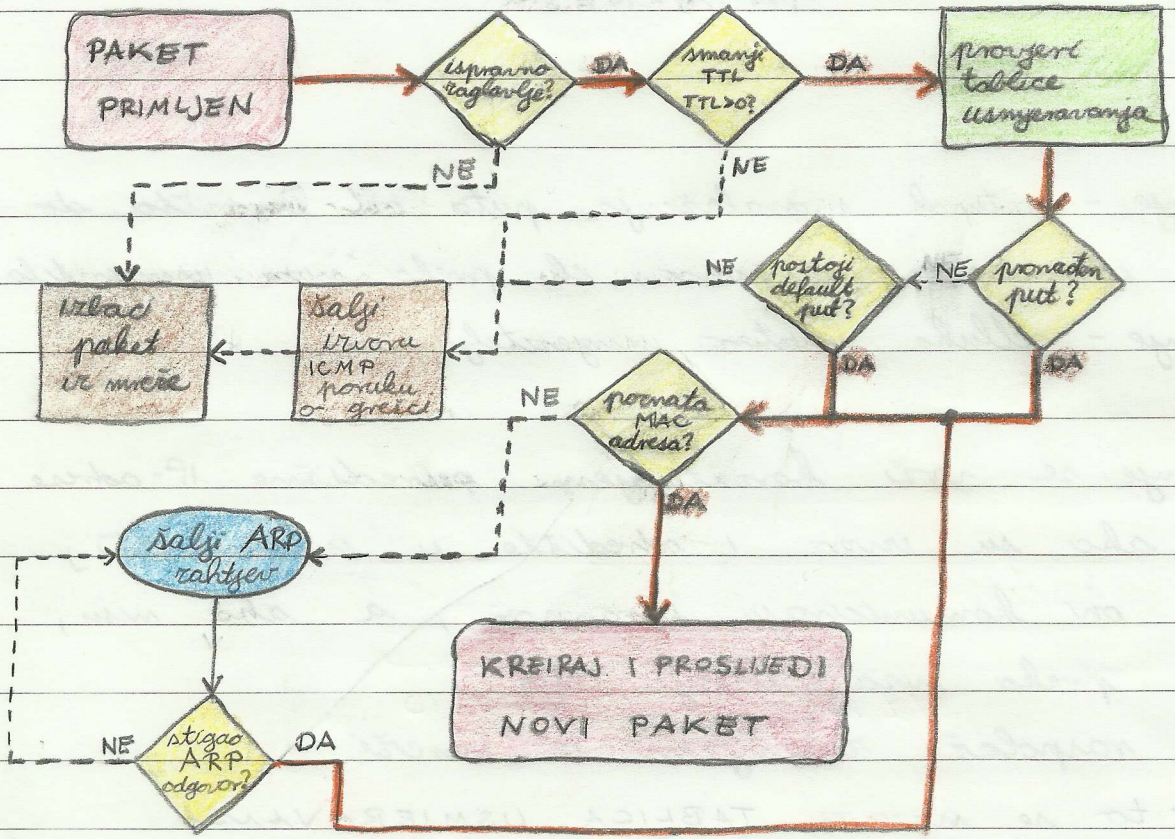
⇒ usmjerivač raspolaže znanjem o mreži
↳ to se naziva TABLICA USMJERAVANJA
↳ ta se tablica ažurira (kod dinamičkih algoritama usmjeravanja)

⇒ GLAVNA PODJELA USMJERAVANJA:
a) unutar autonomnog sustava
b) izvan autonomnog sustava
} algoritme se razlikuju

⇒ glavni podaci paketa za usmjeravanje:
- izvorišna adresa
- odredišna adresa
- TTL

Destination	Gateway	Netif
default	163.51.19.1	eth2
127.0.0.0	127.0.0.0	elk1
...	...	...

⇒ PROCES USMJERAVANJA PAKETA:



↳ ovaj proces je vrlo slično izveden u svim usmjeravačima današnjice

↳ stoga, korisno je imati na umu shemu u svakom trenutku rada sa routerima.

↳ ovdje nije objašnjeno popunjavanje tablice usmjeravanja i učenje usmjeritelja o mreži (tzv. RIP protokol) no o tome će biti riječi kasnije

⇒ ICMP protokol:

↳ „Internet Control Message Protocol"

↳ služi za dijagnosticiranje i kontroliranje trenutnog stanja u mreži

↳ primjeri naredbi: a) Echo Request / Echo Reply

↳ piše se u komandnu liniju pomoću naredbe **ping** IP

b) Trace Route IP

↳ ispisuje put od našeg računala do odredišta

↳ temelji se na polju TTL

MEĐUSOBNO POVEZIVANJE MREŽA

⇒ ARP protokol: BITNO!

↳ protokol razlučivanja adrese

↳ on ima radaću pronaći računalo sa radnom MAC adresom - to radi na način:

1) rad „broadcast" sa upitima
2) očekuje odgovor od računala sa odgovarajućom MAC adresom
3) po primanju, sprema se zapisuje u spremnik

⇒ domena sudara ⇒ dio mreže unutar koje su mogući sudari ako više stanica istodobno šalje okvire

⇒ javlja se samo u lokalnoj mreži

⇒ LAN-komutator ⇒ uređaj koj djeluje na sloju podatkovne poveznice

⇒ služi za razdvajanje domene sudara

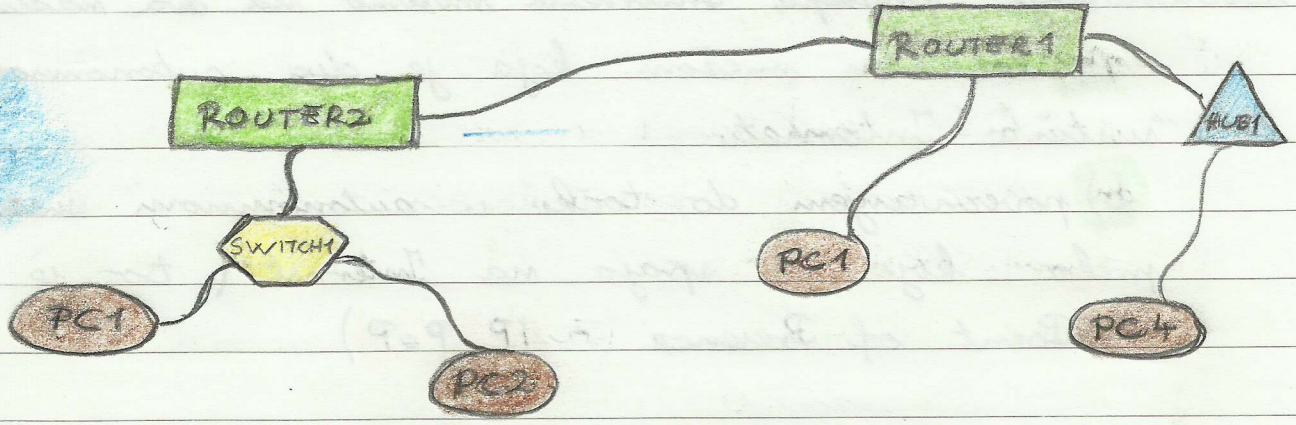
⇒ sve funkcionalnost leži na sklopovlju

⇒ VIDI PROBLEM BESKONAČNE PETLJE!

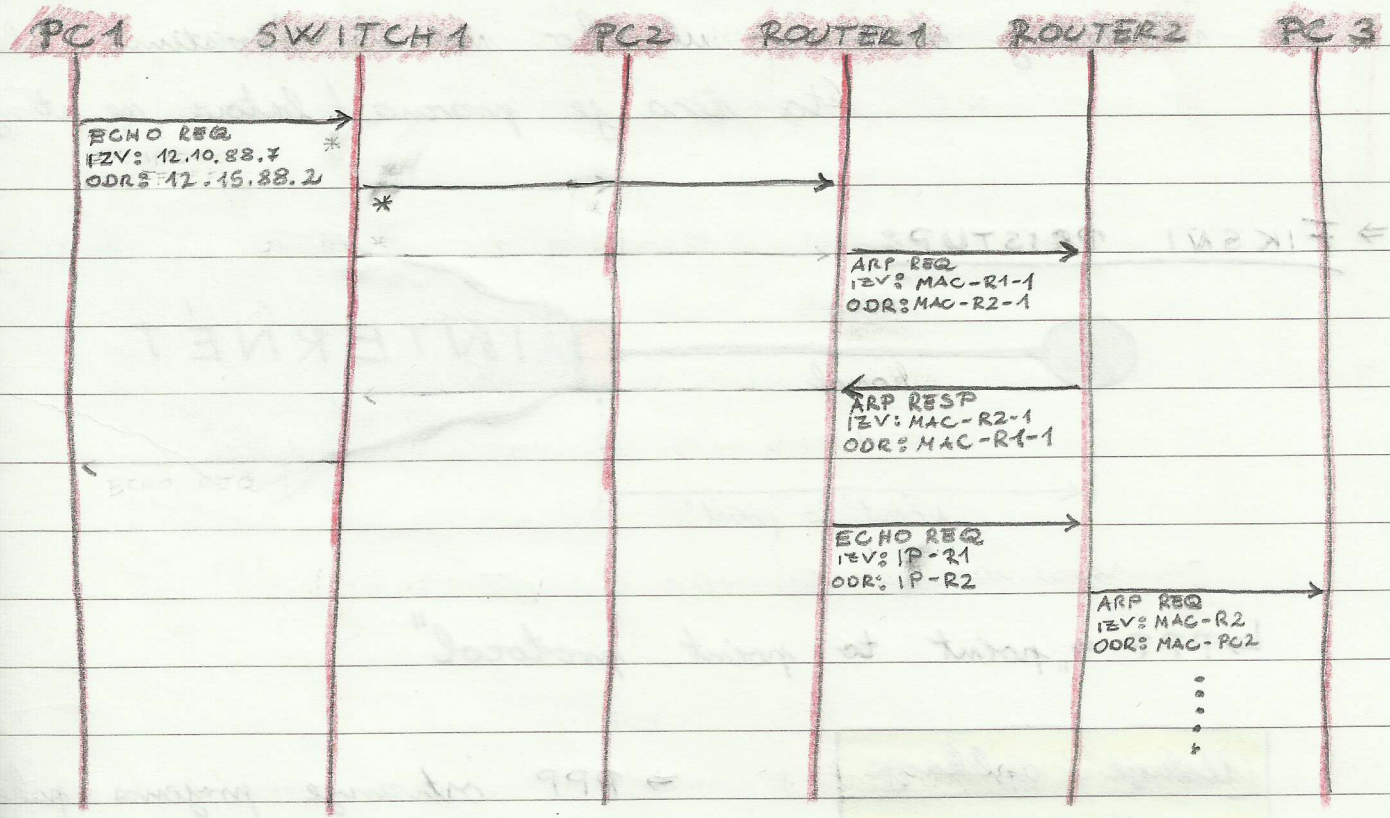
↳ pomoću protokola STP se rješava ta problem redundantnih veza (one se jednostavno ne koriste za raspršivanje)

⇒ Router (usmjerivač) ⇒ razdvaja domene sudara i raspršivanja

ZAD: Računalo 1 šalje „ping" na računalo 3?
Prikaži vremenski dijagram? Na početku su sve
priručne memorije prazne.



b)



PRISTUP INTERNETU

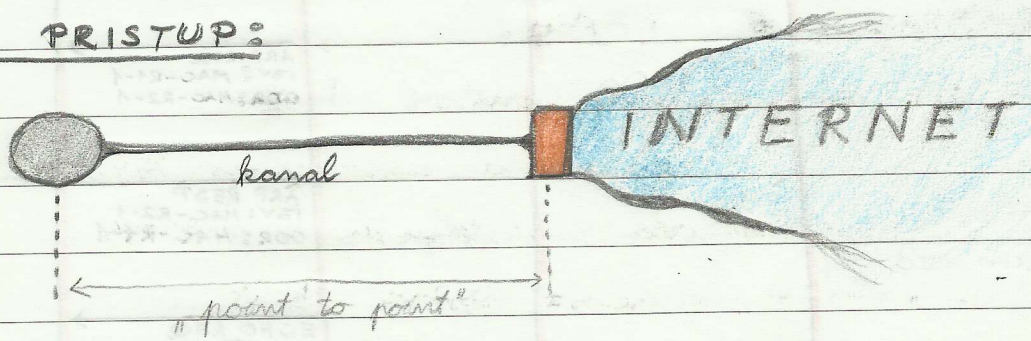
⇒ ostvarivanje pristupa Internetu možemo na dva načina:

a) lokalnom mrežom koja je dio autonomnog sustava Internetu

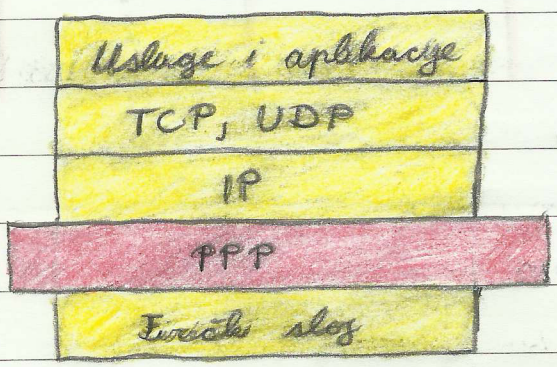
b) povezivanjem do točke u autonomnom sustavu preko koje se spaja na Internet (to je IP Point of Presence - IP PoP)

⇒ svak od nas ima vlastitu žicu od PoP-a (centrale) do vlastitog doma - ukoliko mi ne koristimo Internet, ta žica je prazna (bitovi ne struje)

⇒ FIKSNI PRISTUP:



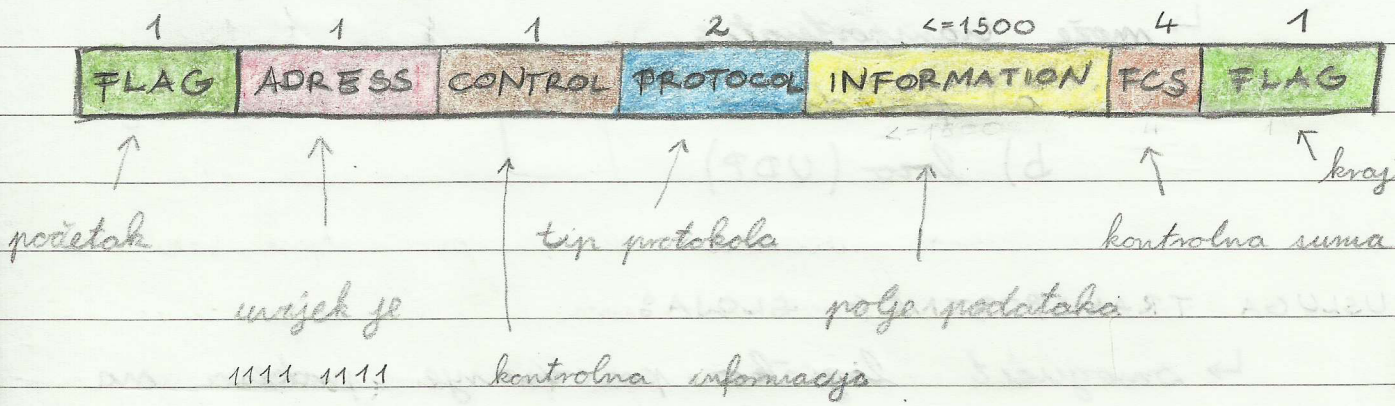
↳ PPP ⇒ „point to point protocol"



⇒ PPP ostvaruje prijenos paketa kanalom od krajnjeg sustava do točke u autonomnom sustavu kod koje se ostvaruje pristup Internetu

⇒ PPP zapravo ima ulogu sloja podatkovne poveznice, ali samo za komunikaciju između krajnjeg čvora i prve točke Interneta

⇒ PPP pakira pakete u svoj poseban okvir; ali u suštini funkcionira identično paketu sloja podatkovne poveznice:



⇒ **KOMPONENTE PPP-a:**

a) LCP ⇒ „Link Control Protocol"

⇒ konfigurira, uspostavlja, ispituje i raskida podatkovnu poveznicu

b) NCP ⇒ „Network Control Protocol"

⇒ brine se o enkripciji, fragmentaciji i slično

⇒ komunikacija s PPP-om:

1. uspostava poveznice i pregovaranje o konfiguraciji (LCP)
2. upravljanje kvalitetom
3. pregovaranje o konfiguraciji mrežnog sloja (NCP=IPCP)
4. komunikacija na mrežnom sloju
5. raskidanje poveznice (LCP)

⇒ pristup Internetu se razlikuje, ovisno o opremi (vidi slajdove za „dial-up", ADSL i bežičnu mrežu)

TRANSPORTNI SLOJ

⇒ zadaća transportnog sloja:

↳ provesti transparentan prijenos transportnih jedinica podataka od izvora do odredišta

↳ taj prijenos je „s kraja na kraj"

↳ može transportirati:

a) pouzdano (TCP) } teška može obje

b) brzo (UDP)

⇒ USLUGA TRANSPORTNOG SLOJA:

↳ omogućit logičko povezivanje procesa na krajnjim računalima

↳ usluga može biti spojna i nespojna

⇒ ADRESIRANJE:

↳ na sučelju transporta i mreže (N-SAP):

• IP - adresa

↳ na sučelju transporta (T-SAP):

• adresa vrata (engl. „port")

⇒ par (IP-address, port) jednoznačno odredjuje vezu koju nazivamo SOCKET:

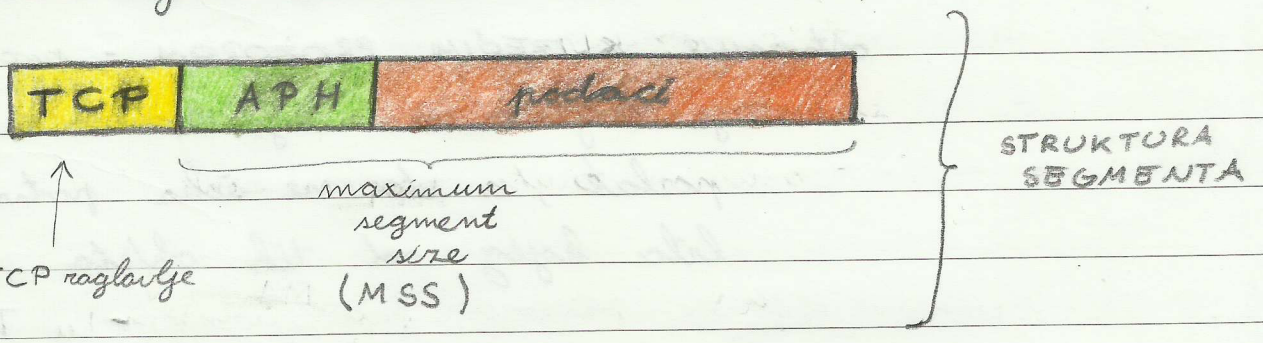
(IP-address, port) <--------> (IP-address, port)

⇒ KLJUČNE ZNAČAJKE TRANSPORTNOG SLOJA:

a) dvosmjerna komunikacija
b) pouzdanost transporta
c) kontrola toka
d) transfer poruka tk. niza okteta

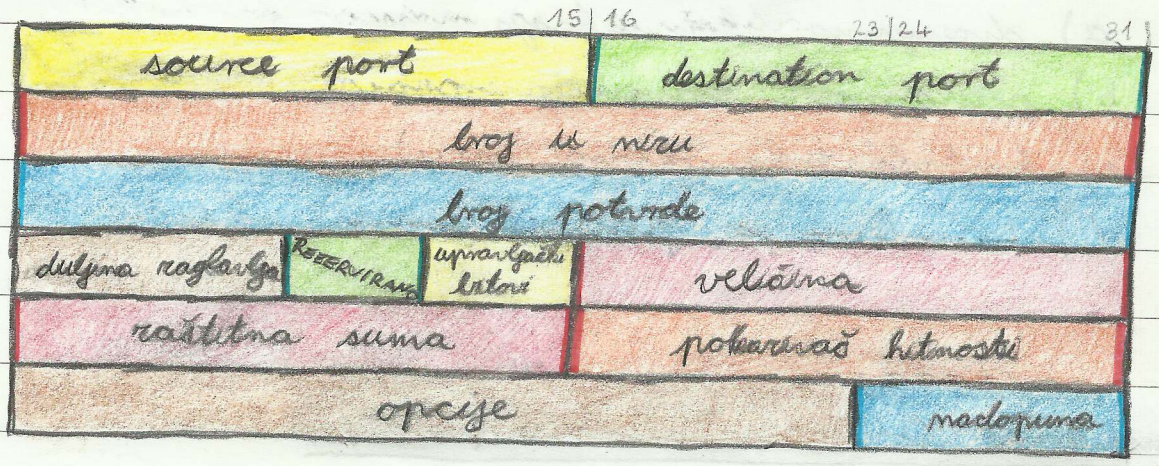
⇒ „Transmission Control Protocol" (TCP):

↳ pruža spojnu uslugu povh nespojnog IP-a
↳ mehanizam potvrde i retransmisije uz očuvanje redosljeda struje okteta
↳ logička veza između procesa definirana je parom 16 bitnih transportnih adresa (PORTOVI)
↳ PDU se na ovom sloju naziva SEGMENT
↳ TCP može obaviti puno stvari, pa nam olakšava rad na višim slojevima, što nije slučaj sa UDP-om



↳ ideja pouzdanosti: numeriraj segmente, primatelj potvrđuje primljene segmente (potvrđuje se veća skupina segmenata - kumulativna potvrda) al se potvrđuje samo do prvog pogrešnog segmenta

↳ struktura TCP zaglavlja:



↳ TCP se ostvaruje konačnim automatom:

- definiraju se stanja i prijelazi te se pomoću toga možemo vratiti u stanje sustava kada je greška nastala i ispravit grešku (npr. slanje retransmisija)

↳ TCP ima dobro ostvarenu vremensku kontrolu na način da se dinamički određuje RTO (Retransmission Time Out)

- dinamička vremenska kontrola se ostvaruje KLIZEĆIM PROZOROM - prozor je broj okteta koji se može poslati, a da ne čeka potvrdu bilo kojeg od tih okteta

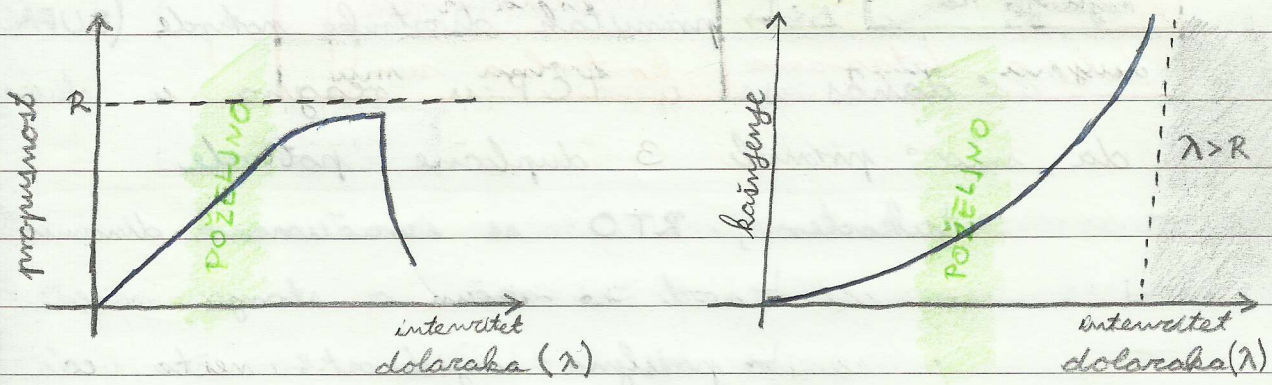
- u TCP-u, veličina klizećeg prozora se mijenja ovisno o stanju mreže (algoritme za to ćemo vidjeti kasnije)

↳ znači, TCP nam osigurava pouzdan prijenos s kraja na kraj (svi segmenti u pravilnom redoslijedu)

↳ MSS - „Maximum Segment Size"

- odredujemo se prilikom uspostave aplikacije, ali se obično prilagođava maksimalnoj veličini okvira (MTU)

↳ upravljanje zagušenjem:



- ideja upravljanja - kada detektiraš da dolazi do zagušenja, naglo smanji intenzitet slanja, pa ga postupno povećavaj
- zagušenje detektiramo učestalim gubicima i učestalim istekom RTO-a
- razlog za takvu dinamičku kontrolu jest to da niti jedan pošiljatelj ne može unaprijed odrediti svoj udio kapaciteta
- MEHANIZAM:
  - ↳ svatko za sebe povećava brzinu slanja i prati stanje
  - ↳ pošiljatelj uvodi još jedan prozor:

PROZOR ZAGUŠENJA

- ↳ on promatra gubljenje paketa
- ↳ efektivni prozor pošiljatelja:

min{oglašeni prozor primatelja, prozor zagušenja}

- **cwnd** - „Congestion window"
- **rwnd** - „Receiver advertised window"
- **swnd** - „Sender window"
- ustanovljavanje gubitaka:
  - ↳ istek RTO
  - ↳ primitak dvostruke potvrde (DUPACK)
- danas se u TCP-u reagira u slučaju da smo primili 3 duplicane potvrde
- također, RTO se izračunava dinamički:
  - ↳ vodi se računa o stanju mreže
  - ↳ početna vrijednost: nešto veća od prosječnog RTT-a
  - ↳ koristi se izraz:

$$RTO = RTT + 4 \cdot D \quad (1)$$

D → srednja devijacija RTT-a

↳ ovisno o veličini skoka RTT-a i duljini mjerenja RTT-a odredujemo težinu trenutnog izračuna RTO-a

↳ nadalje, on segmente koji su poslani ponovno (retransmisija) imaju posebnu formulu za računanje RTO-a (KARNOV ALGORITAM):

$$RTO_2 = 2 \cdot RTO_1 \quad (2)$$

RTO_1 → izračunat RTO po izrazu (1)

• cwnd se uvijek postavlja na 1 na početku i povećava se na dvostruku vrijednost

• kada dođe do isteka RTO-a, drastično se smanjuje prozor zagušenja

↳ prozor zagušenja se postavlja početno na 1 MSS

↳ prag polaganog početka ssthresh se postavlja na polovicu veličine prozora zagušenja prije gubitka segmenta

• **dodatni mehanizmi:**

a) BRZA RETRANSMISIJA

↳ odmah pošalji segment nakon 3 DUPACK

b) BRZI OPORAVAK

↳ ne smanjuj prozor zagušenja na 1, već na polovicu veličine prilikom detekcije zagušenja

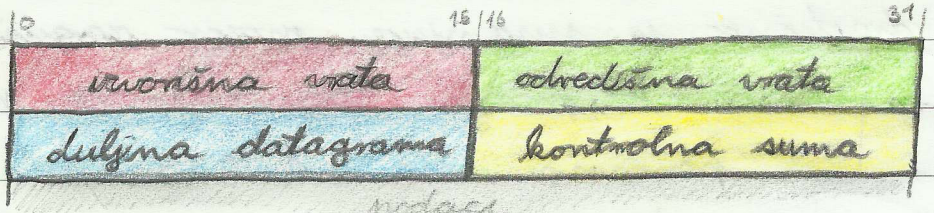
↳ postoje razne izvedbe TCP-a koj koriste razne mehanizme kontrole toka i kontrole zagušenja

↳ TCP nema mehanizme za sigurnost i privatnost podataka, ne vodi računa o gravicama poruka i ne garantira isporuku (ali se jako potrudi)

⇒ „User Datagram Protocol" (UDP):

↳ nema nikakve kontrole (ima raštitnu sumu, ali se u praksi ne rabi)

↳ struktura UDP zaglavlja:



↳ koristi se za multiplayer igre, video prijenos, prijenos govora, ... ⇒ BRZINA JE KLJUČNA!

↳ aplikacija koja koristi UDP mora voditi računa o izgubljenim podacima (najčešće ih jednostavno zanemaruje)

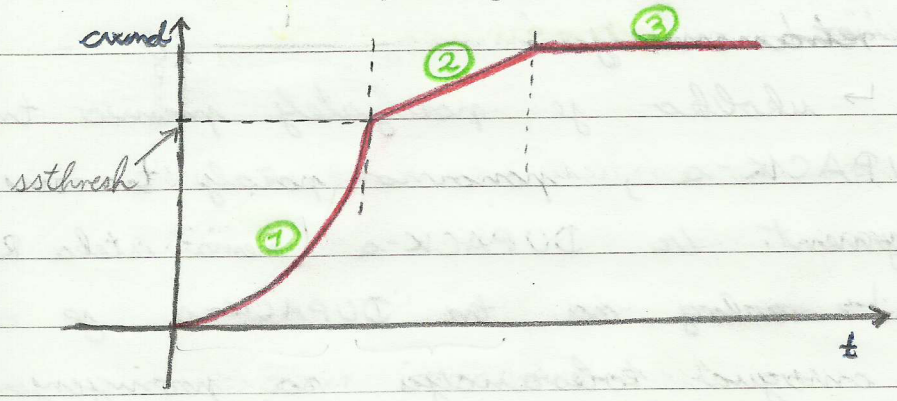
↳ UDP ne uspostavlja vezu prije komunikacije kao što to radi TCP

- UDP - nespojna usluga
- TCP - spojna usluga

↳ UDP ne osigurava pravilan redoslijed isporuke podataka

TCP UPRAVLJANJE ZAGUŠENJEM (ponavljanje)

⇒ cilj je približiti se maksimalnoj propusnosti mreže bez zagušenja



① **Polagani početak** ⇒ po primitku svih potvrda, „cwnd" se udvostručuje

⇒ u slučaju isteka RTO-a, dosli smo u zagušenje, smanji „ssthresh" na polovicu vrijednosti i kreni ponovno u polagani početak (smanji „cwnd" na 1)

② **Izbjegavanje zagušenja** ⇒ „cwnd" je nadišao „ssthresh" što znači da smo bliu zagušenja te treba povećavati „cwnd" linearno (oličino po 1)

⇒ u slučaju isteka RTO-a, radimo ista kao u ①

③ **Dosegnuta oglašena veličina prozora primatelja:**

↳ dalje ne povećavamo jer primatelj ne može više od toga primati

⇒ **problem ovog mehanizma:**

- prilikom gubitka jednog segmenta, istječe RTO i smanjujemo „cwnd" na jedan, a znamo da smo blizu željene vrijednosti „cwnd"-a ☹

⇒ rješenje gornjeg problema nude dva podmehanizma:

a) **brza retransmisija:**

↳ ukoliko je pošiljatelj primio tri DUPACK-a, ponovno počalj traženi segment iz DUPACK-a (nema isteka RTO-a ☺)

↳ razlog za tri DUPACK-a je da se omogući tolerancija na promijenjen redoslijed paketa

b) brzi oporavak:

↳ umjesto resetiranja „cwnd"-a na 1 nakon brze retransmisije, postavljamo „cwnd" na polovicu svoje vrijednosti

APLIKACIJSKI SLOJ U INTERNETU

⇒ najviši sloj u TCP/IP referentnom modelu
↳ on obuhvaća aplikacijski, prezentacijski i sjednički sloj referentnog OSI modela

⇒ aplikacijski sloj pruža aplikacijske protokole:
a) SUSTAVSKI:
↳ DNS → „Domain Name System"
b) KORISNIČKI:
↳ HTTP, STTP → „... Text Transfer Protocols"

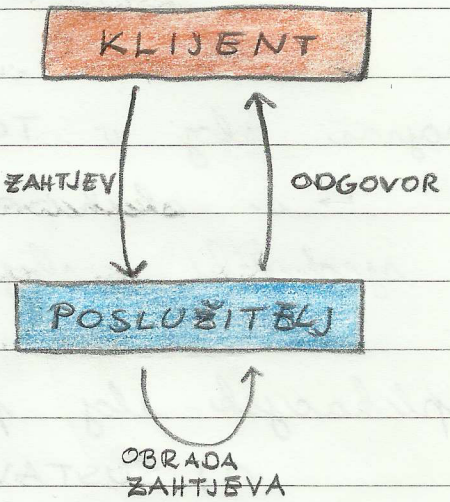
⇒ osnove internetskih usluga:
- aplikacijski protokol - obuhvaća raščlanjivanje vrste poruka, raščlanjivanje sintaksu poruka, te raščlanjivanje semantiku
- model izvedbe usluge - **klijent/poslužitelj**
- ravnopravni sustav („peer-to-peer")

⇒ kod modela klijent/poslužitelj moraju postojati dva programa:
↳ program klijenta (npr. web-stranica)
↳ program poslužitelja (npr. program koji dodatne razne zahtjeve od klijentskih programa)

⇒ MODEL KLIJENT - POSLUŽITELJ

↳ najčešći oblik izvedbe usluge

↳ rad poslužitelja može biti:



PO MEMORIJI

a) memorijski
- obrada ovisi o prethodnim obradama (npr. reklame na temelju prethodnih narudžbi)

b) bezmemorijski
- svaka obrada je neovisna o drugoj

PO PARALELNOSTI

a) iterativni
- obrađuje se jedan po jedan zahtjev u jednom poslužiteljskom procesu

b) konkurentni
- obrađuje se više zahtjeva odjednom u više zasebnih procesa

↳ ASOCIJACIJA – uspostavljen odnos između procesa klijenta i procesa poslužitelja putem jedne transportne veze (TCP ili UDP)

↳ PRONALAŽENJE USLUGA:
- kako klijent odabere prava vrata na poslužitelju?
- postoje dobro-poznata vrata za neke usluge, pa klijent može znati kamo slati

↳ PROGRAMSKO SUČELJE („socket API"):

- socket (priključnica) je apstrakcija krajnje točke komunikacije između klijenta i poslužitelja
- to je programska apstrakcija koja standardizira komunikaciju

↳ GDJE SU USLUGE SMJEŠTENE?

a) na poslužitelju
   - npr. web-stranice, e-trgovine

b) djelomično na klijentu
   - npr. Java, JavaScript, AJAX, ...

c) negdje između
   - npr. proxy serveri (posrednici)

⇒ uloge posrednika (PROXY):

a) „klasična" posrednička uloga
   - dohvaćanje podataka za klijenta od nekog drugog poslužitelja
   - prikupljanje podataka sa više poslužitelja

b) međuspremnička uloga
   - „caching" za ubrzavanje

c) nadzor i ograničenje pristupa
   - „firewall"

SUSTAV DOMENSKIH IMENA

⇒ DNS → „Domain Name System"

⇒ ovaj sustav se još naziva i „imenik Interneta"
jer povezuje ime sa IP adresom

↳ to je potrebno jer je ljudima lakše pamtiti i baratati sa simboličkim imenima nego sa brojevima

⇒ u početku Interneta, to nije bio problem jer je bilo malo računala, no 1980-ih se je moglo da će trebat **skalabilno** rješenje te se razvio DNS

⇒ ideja je da nema svaki DNS-poslužitelj informaciju o svim već on zna koga treba pitati ukoliko nema podatke za uneseno simboličko ime

↳ razlučitelj („resolver") je aplikacijski program koji se vrti u pozadini koji šalje upit DNS-poslužitelju

⇒ također, DNS-poslužitelj je u većini slučajeva u lokalnoj mreži računala

⇒ HIJERARIJSKI SUSTAV:

↳ domena ⇒ skupina računala koje pripadaju određenoj organizaciji

⇒ može imati pod-domene

⇒ primjer: .hr , .fer.hr, .tel.fer.hr

↳ potpuno kvalificirano domensko ime ⇒ daje jedinstvenu identifikaciju krajnjeg mrežnog sučelja (preslikava se u IP adresu)

⇒ općeniti oblik potpuno kvalificiranog domenskog imena:

host.poddomena.domena

↳ na primjer: www.unizg.hr

⇒ postoji 13 vrhovnih („root") poslužitelja, oko 400 manjih DNS-poslužitelja

⇒ ZAPIS O DOMENI (u DNS-poslužitelju):

↳ svaki zapis ima rok trajanja te se obnavlja

↳ vrste zapisa:

- tip A → zapis za krajnje računalo
- tip NS → zapis za DNS-poslužitelj („Name Server")

⋮

⇒ NAČIN RAZLUČIVANJA ADRESE:

a) iterativan ⇒ klijent uzastopno ispituje traženi DNS-poslužitelje i sam dolazi do odredišnog računala

b) rekurzivan ⇒ klijent pošalje jedan zahtjev za razlučivanje, a DNS-poslužitelj rekurzivno dolazi do odredišnog računala i vraća IP-adresu klijentu

↳ danas se u Internetu koristi miješani način:

- klijent pita lokalnog DNS-poslužitelja, a on sa drugim DNS-om iterativno nalazi odredišnu IP-adresu (VIDI SLAJDOVE ☺)

INTERNETSKE USLUGE

⇒ najvažnije Internetske usluge:
- World Wide Web (WWW)
- Elektronička pošta (E-mail)

WORLD WIDE WEB

↳ usluga se naziva globalni hipermedijski informacijski sustav
↳ koristi HTTP aplikacijski protokol
↳ koristi model klijent - poslužitelj
↳ program klijenta:
- koristi se za pregledavanje Weba
- često služi kao univerzalno sučelje za sve vrste usluga (npr. transfer datoteka, pošta, ...)

↳ program poslužitelja:
- poslužuje informacijske resurse

↳ OSNOVNI ZAHTJEV ⇒ omogućiti transparentni pristup informacijskom sustavu hipermedijskih izvora
↳ HIPERTEKST ⇒ aktivni dio teksta koj omogućuje skok na drugo mjesto
↳ HIPERMEDIJ ⇒ stranice hipersteksta obogaćene drugim medijima (npr. slike, video, audio, ...)
↳ nad-pojam pojmu hipermedij je RESURS - to je bilo što na Webu što daje informaciju i može se identificirati (URI → „Unique Resource Identifier")

↳ problemi koje treba riješiti za implementaciju Weba:

HTML

a) jedinstveno opisivanje i prikaz određenog sadržaja na Webu

⇒ RJEŠENJE: HTML → „Hypertext Markup Language"
↳ → jednostavan jezik za prikaz hipertekst-a

XML → podržava dodatne stvari

URL

b) jedinstven način identificiranja sadržaja

⇒ RJEŠENJE: URL → „Uniform Resource Locator"

URN → „Uniform Resource Name"

URI → može biti ime, lokacija ili oboje!

HTTP

c) protokol za prijenos komunikacije na Webu

⇒ RJEŠENJE: HTTP → „Hypertext Transfer Protocol"
→ pet vrsti poruka (ključni su zahtjev (GET) i odgovor (OK, not found))

ELEKTRONIČKA POŠTA

↳ jedna od najstarijih Internetskih usluga

↳ koristi se nekoliko aplikacijskih protokola:

- SMTP → „Simple Mail Transfer Protocol" } SLANJE
- POP → „Post Office Protocol" } ČITANJE
- IMAP → „Internet Mail Access Protocol"

↳ opet se koristi arhitektura klijent-poslužitelj, ali na principu **pohrani i proslijedi**:

- klijent ima Mail User Agent (MUA)
- poslužitelj ima Mail Transport Agent (MTA)

↳ stoga, poruka prolazi niz e-mail poslužitelja na putu do krajnjeg korisnika

→ TIJELO: poslani podaci

ZAGLAVLJE: vidi ga korisnik (opisuje from, to, Bcc, received, ...)

OMOTNICA: nju korisnik ne vidi (služi samo MTA-u)

↳ MIME ⇒ „Multi-purpose Internet Mail Extensions"

⇒ cilj je riješiti problem internacionalnih znakova (više se ne koristi 7-bitni ASCII)

⇒ to je danas standard

↳ PROTOKOLI:

a) SMTP ⇒ služi za slanje poruke do odredišnog poslužitelja

⇒ ne ovisi o nižim protokolima

⇒ definira sintaksu

b) POP ⇒ služi za čitanje elektronske poruke
⇒ služi krajnjem korisniku za pristup poslužitelju sa elektronskom poštom
⇒ relativno star protokol koj je imao probleme sa sigurnošću

c) IMAP ⇒ moderniji protokol koj se većinom koristi i nastoj ukloniti nedostatke POP-a

OSNOVE SIGURNOSTI MREŽA

⇒ SIGURNOST ⇒ sposobnost mreže da se suprotstavi slučajnim događajima i zlonamjerali

⇒ temeljni zahtjevi sigurnosti:

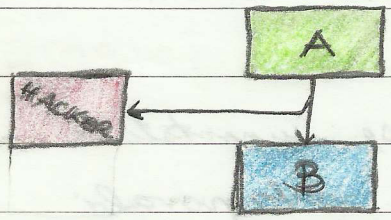
- povjerljivost (CONFDENTIALITY)
  ↳ poruke su razumljive samo pošiljatelju i primatelju poruke
- integritet (INTEGRITY)
  ↳ jamstvo da su informacije primljene onakve kakve su i poslane
- raspoloživost (AVAILABILITY)
  ↳ informacije moraju biti raspoložive usprkos neočekivanim događajima
- autentičnost (AUTHENTICITY)
  ↳ provjera identiteta korisnika
- neporecivost (NONREPUDIATION)
  ↳ ukoliko je korisnik sudjelovao u nekoj radnji, on to kasnije ne može opovrgnuti

↳ prevladavajuće uvjete... = CIA

⇒ važno je predvidjeti što više mogućih scenarija u kojima se sustav ne ponaša onako kako je inicijalno namišljeno

⇒ tipične sigurnosne prijetnje:

- presretanje, prisluškivanje:

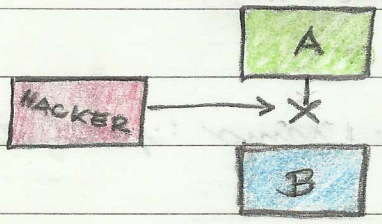


↳ preuzima se informacija, gubi se povjerljivost informacije

↳ ilegalna akcija

↳ moguće rješenje je šifriranje

- prekidanje, uskraćivanje:

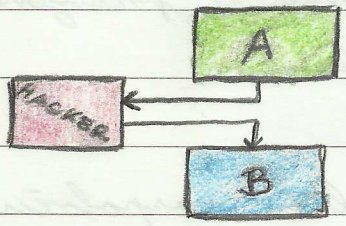


↳ „denial of service", „interruption"

↳ također ilegalno

↳ izaziva se velikim i dugotrajnim preopterećenjem poslužitelja

- promjena, kažnjavanje:

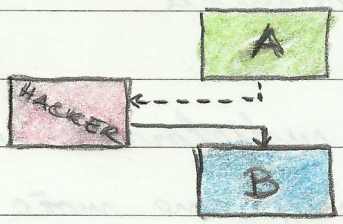


↳ promjena ili umetanje informacije

↳ ovo se naziva „man in the middle attack"

↳ danas vrlo čest napad protiv kojeg ima malo efikasnih rješenja

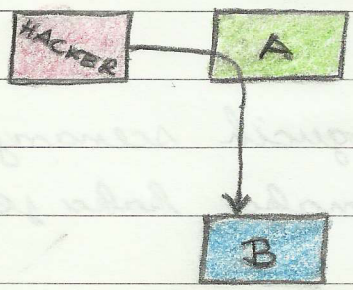
- fabrikacija, ponavljanje:



↳ ubacivanje izmanipulirane informacije u komunikacijski kanal

↳ ubacuje se informacija prethodno presretnuta presretanjem

- lažno predstavljanje:



↳ napad kod kojeg se izmanipulirani korisnik maskira (utjelovljuje) kao sudionik komunikacije

↳ narušava se autentičnost

⇒ problem sigurnosti u Internetu je, zbog velik jer protokol koji se koriste su nastali u doba kada sigurnost nije bila jedan od prioriteta

⇒ MJERE KONTROLE:

a) fizička - kamere, blindirana vrata, ...

b) tehnička - vatrozid, kriptiranje, ...

c) administrativne - politika, pravilnici, ...

⇒ na nas su najbitnije tehničke mjere kontrole

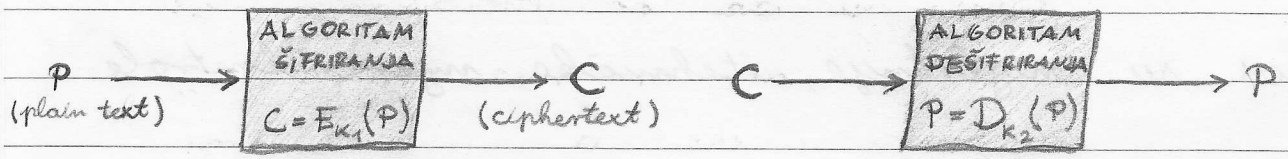
TEHNIČKE MJERE KONTROLE

⇒ KRIPTOLOGIJA:

↳ znanost koja se bavi šifriranjem i obuhvaća dvije komplementarne discipline

a) kriptografija - šifrira

b) kriptoanaliza - dešifrira



↳ „K_1" i „K_2" su ključevi za šifriranje i dešifriranje

↳ <u>simetrični algoritmi</u>:

- koriste isti ključ za šifriranje i dešifriranje
- javno poznati algoritmi
- tajnost se temelji na tajnosti ključa
- algoritam je još što je ključ veći
- ako je ključ fiksne dužine, to je onda blok algoritam (npr. 56 bita, 112 bita, 192 bita)

⇒ 2 standarda simetričnih blok algoritama:

a) DES ⇒ „Data Encryption Standard"

⇒ dužina ključa samo 56 bita, pa se danas više ne koristi

b) AES ⇒ „Advanced Encryption Standard"

⇒ veće dužine ključa (npr. 256 bita)

⇒ može se ostvariti sklopovski, pa se puno koristi

⇒ problem simetrične kriptografije je upravo distribucija ključa na drugu stranu (VIDI SLAJDOVE ▽!)

↳ asimetrični algoritmi:

- svaki sudionik ima dva ključa:
  - javni ključ
  - privatni ključ
- sudionik objavljuje javni ključ i koristi ga sa privatnim ključem
- postupak šifriranja i dešifriranja je složen i iziskuje veće korištenje nego simetrični algoritmi, ali pruža neštu veću pouzdanost
- vid postupak šifriranja i dešifriranja na slajdu 30 ▽!

⇒ ŠIFRIRANJE U PRAKSI:

↳ za razmjenu ključeva koriste se asimetrični algoritmi, a za samo šifriranje teksta se koriste simetrični algoritmi

⇒ za neke svrhe se koriste i SAŽECI („Hash")

↳ npr. download datoteka:

- skinemo datoteku i njen sažetak
- OS izračunava „Hash" datoteke
- uspoređuje se skinuti i izračunati „Hash"

⇒ PROBLEM DISTRIBUCIJE KLJUČA:

↳ kako znamo da „man-in-the-middle" nije presreo ključ i podmetnuo svoj?

• ne možemo znati, pa se uvode CERTIFIKACIJSKA TIJELA kojoj svi vjeruju

BITNO

↳ točan način tijeka komunikacije i distribucije ključeva vodi na slajdovima!

↳ izdavanje certifikata se naplaćuje

SIGURNOST U INTERNETU

⇒ ovo je zanatan problem jer su gotovo svi protokoli relativno stari i nemaju značajne sigurnosne mjere

↳ stoga, dodaju se novi protokol:

a) IPsec

b) TLS („Transport Layer Security")

⇒ IPsec:

- ima dva načina rada
  - ↳ transportni - štiti podatke viših slojeva (od transportnog nadalje)
  - ↳ tunelski - štiti se cijeli IP-datagram
- ima široku primjenu za virtualne mreže (VPN)
- nije od početka ramišljen, pa je implementacija dosta složena i skupa

⇒ TLS:

- koristi se za sigurnost transportnog sloja
- umjesto direktnih poziva funkcija za primanje i slanje podataka, prvo se pozivaju funkcije za šifriranje
- koriste se prethodno spomenuti certifikati od tijela kojima se vjeruje
- vidi postupak uspostavljanja TLS sjednice na slajdu 51!
- https koristi TLS!

⇒ SIGURNOST ELEKTRONIČKE POŠTE:

a) S/MIME („Secure MIME")

b) PGP („Pretty Good Privacy")

⇒ VATROZID: („Firewall")

↳ uređaj koj radi na mrežnom sloju, osigurava **sigurnost krajnjih sustava**, al ne i komunikacije

↳ pažnji skup pravila koja svak paket mora zadovoljit kako bi paket „ušao" u našu mrežu il računala

↳ može bit sa stanjima il bez stanja

POVEZIVANJE MREŽA U INTERNETU

⇒ usmjeravanje između AUTONOMNIH SUSTAVA:

- iBGP - „internal Border Gateway Protocol"
  - održava tablice usmjeravanja routera unutar autonomnog sustava
- eBGP - „external Border Gateway Protocol"
  - održava tablice usmjeravanja routera koji povezuju autonomne sustave

⇒ Network Address Translation (NAT):

↳ prevođenje prežnih adresa

↳ uvedena zbog nedostataka IP adresa (IPv4)

↳ više računala iz privatne (lokalne) mreže komunicira u Internetu preko jedne ili nekoliko javnih IP-adresa

- ukratko, jedna adresa za LAN, a druga adresa za WAN

⇒ Port Address Translation (PAT):

↳ radi isto što i NAT, samo za vrata transportnog sloja

⇒ NAT i PAT se u praksi rijetko koriste i ovi zbog toga donekle štede IP-adresa

DODATNO O SIGURNOSTI U INTERNETU

⇒ SIGURNOST PODATKOVNOG SLOJA:

↳ Ethernet je nesiguma mreža jer su do sada su sigurnosni mehanizmi bili na višim slojevima

↳ problem 1: netko neautoriziran se može priključiti u mrežu i prisluškivati prilikom broadcasta u lokalnoj mreži

- rješava se naprednijim LAN komutatorima

↳ problem 2: preusmjeravanje komunikacije pomoću nerazumljivog ARP-a (na ARP zahtjev, napadač odgovori svojom IP-adresom)

- rješava se pomoću ARP-a na višim slojevima sa sigurnosnim rješenjima

⇒ SIGURNOSNA STIJENA (vatrozid, firewall):

↳ ključan element računalne

↳ u osnovi, to je jednostavan filter paketa

↳ često se kombinira sa usmjerivačem i NAT-uređajem

PROTOKOL IPv6

⇒ standardiziran 1998. godine

⇒ novosti u IPv6:

- duljina adrese je 128 bita što omogućuje 2^{128} adresa (ne trebamo imati skrivene mreže, računala što rad NAT)
- učinkovitije usmjeravanje (jednostavnije zaglavlje)
- podrška za QoS (omogućuje tokove, prepoznaje vrstu paketa)

⇒ notacija IPv6 adrese:

↳ 8 blokova od po 4 heksadekadske znamenke

↳ UNICAST → jednoodredišna adresa (identificira se jedno računalo)

↳ MULTICAST → više računala se odjednom adresira

↳ ANYCAST → novost za IPv6 (GOOGLAJ!)

⇒ **dodjela IPv6 adrese:**

a) **bez poslužitelja** - izračunava se na temelju MAC adrese

b) **sa poslužiteljem** - standardni način

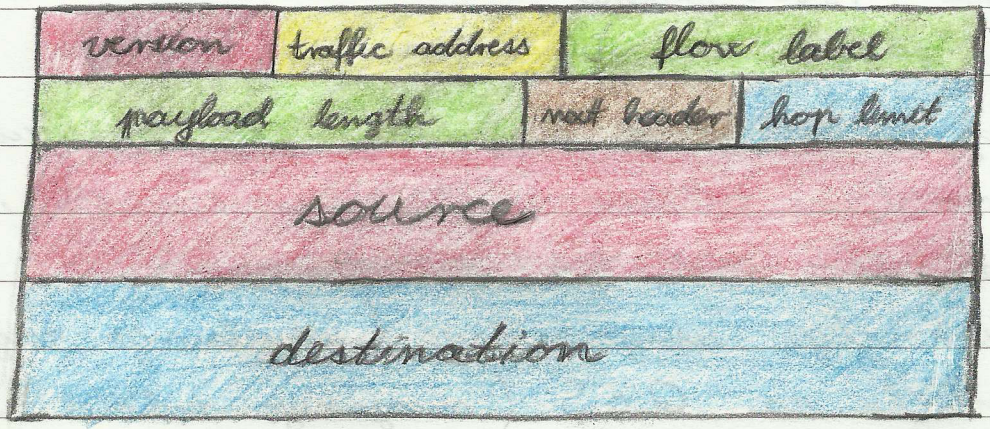
- jednako kao sa IPv4

sama što poslužitelj dodjeljuje IPv6 adrese

⇒ IPv6 ZAGLAVLJE:

↳ sada je fiksne veličine (40 okteta)

↳ drastično pojednostavljeno



↳ TTL je promijenio ime u nešto prikladnije „hop limit"

↳ ostala polja imaju razumljiva imena

↳ fiksna veličina zaglavlja omogućava brži obradu paketa

⇒ kod IPv6 nema protokola ARP već se vježava funkcionalnost rješava na višim slojevima što pospješuje sigurnost mreže