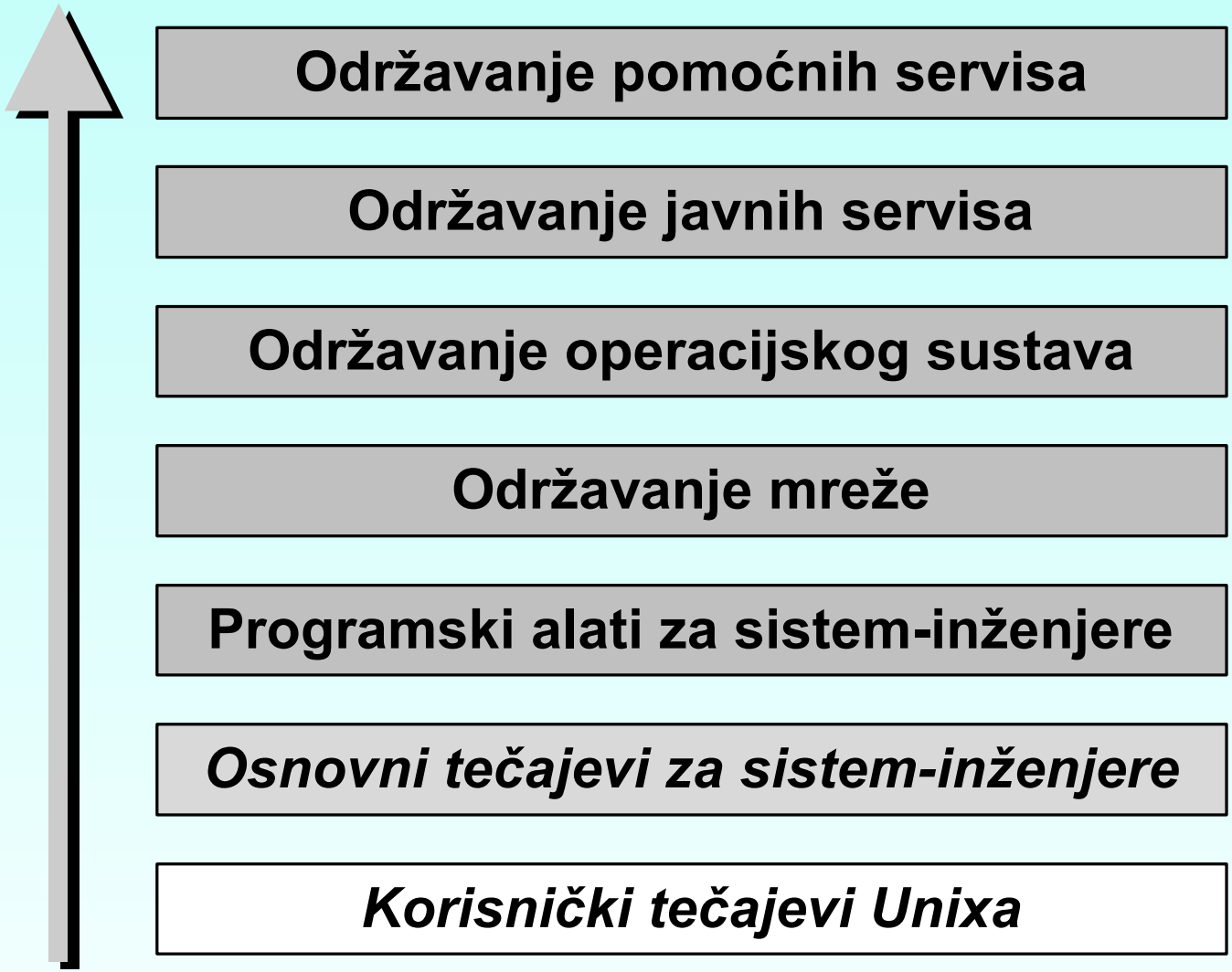
Održavanje mreže

autor: Boris Obradov (@fer.hr)

mentor: Mario Klobučar (@srce.hr)
recenzent: Vladimir Rabljenović (@srce.hr)


Održavanje pomoćnih servisa
Održavanje javnih servisa
Održavanje operacijskog sustava
Održavanje mreže
Programski alati za sistem-inženjere
Osnovni tečajevi za sistem-inženjere
Korisnički tečajevi Unixa

Ciljevi tečaja

- Upoznavanje s konceptom i strukturom TCP/IP mreža:
  - TCP, UDP, ICMP
  - IP
  - Ethernet
- Stjecanje potrebnih znanja za kvalitetno održavanje TCP/IP mreža:
  - Konfiguriranje sučelja, IP adresiranje, usmjeravanje
  - DNS

Potrebno predznanje

- poznavanje osnova Unixa
  - rad s datotekama
  - korištenje uređivača teksta
  - jednostavnije naredbe
- poželjno poznavanje
  - osnove računalnih mreža (ISO/OSI mrežni model)
  - osnove TCP/IP protokola

Sadržaj (1. dan)

Sadržaj (2. dan)

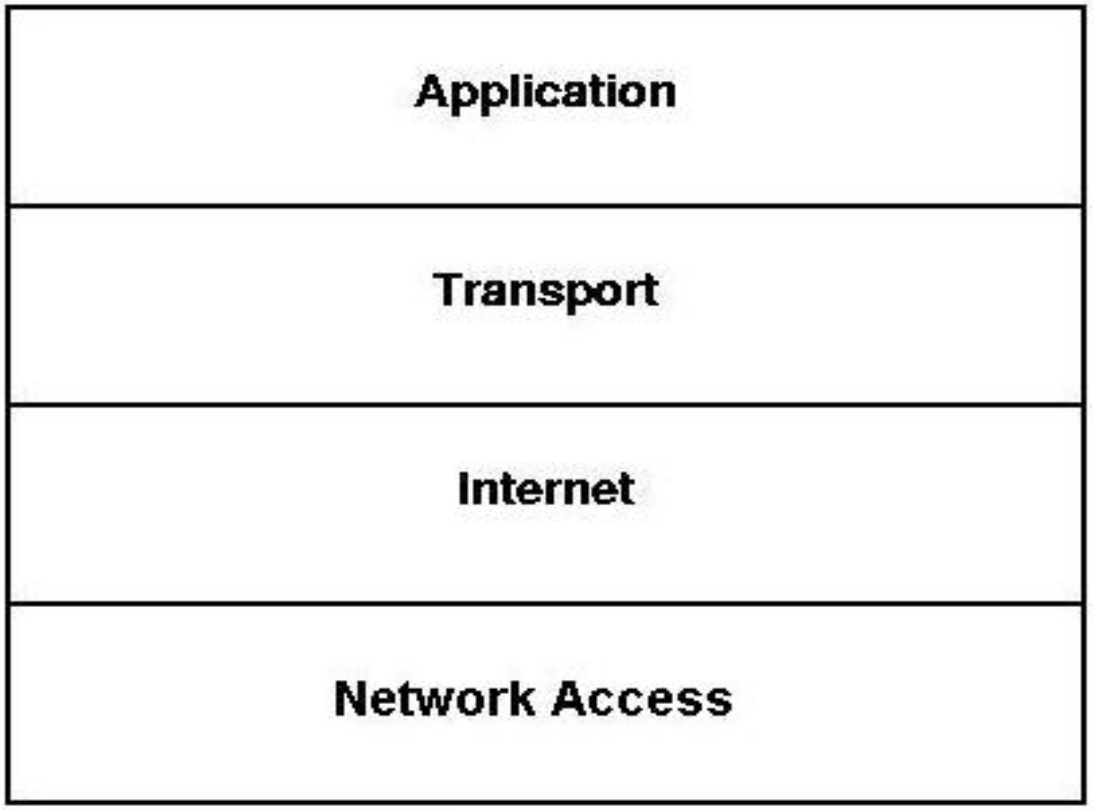
TCP/IP

Osnovni pojmovi - ISO/OSI mrežni model

Primjena	Application
Predočavanje	Presentation
Sjednica	Session
Prijenos	Transport
Mreža	Network
Podatkovni spoj	Data link
Fizički spoj	Physical

TCP/IP

Osnovni pojmovi – TCP/IP model



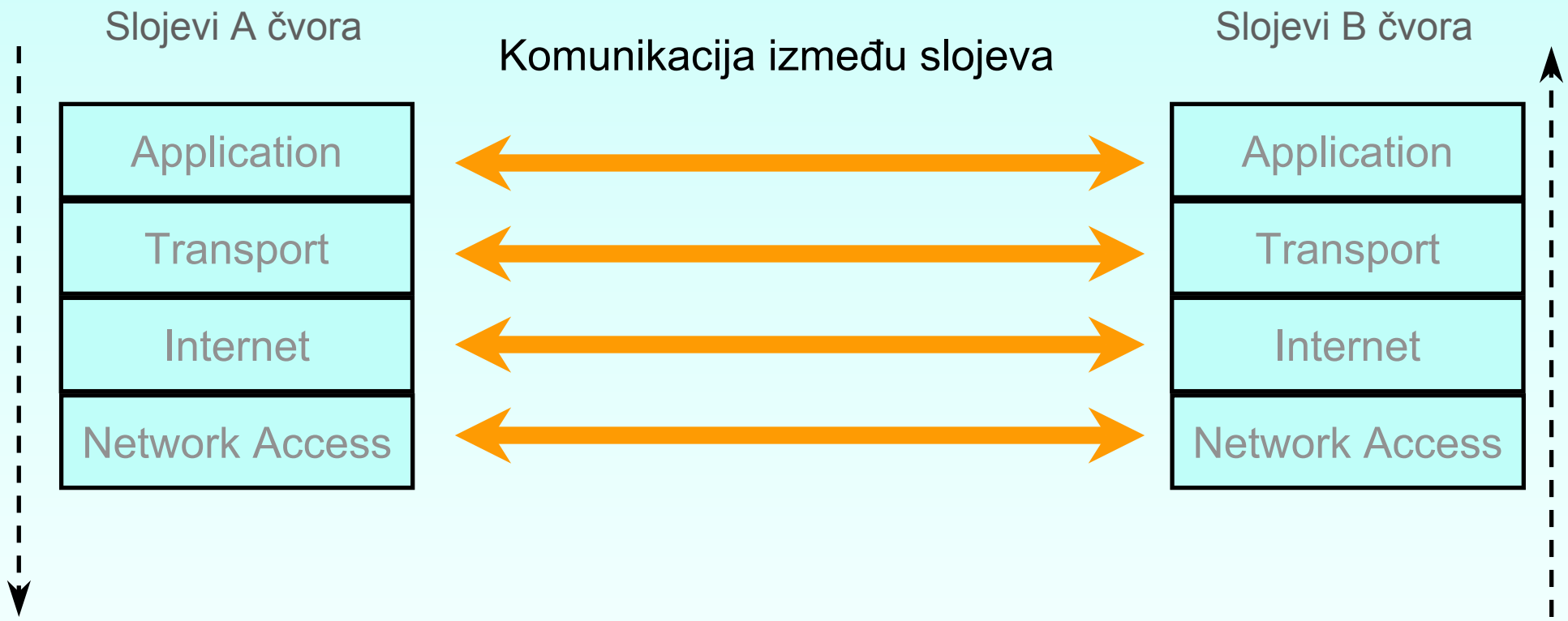
TCP/IP

Osnovni pojmovi – usporedba modela

OSI	TCP / IP
Application (Layer7)	Application
Presentation (Layer6)	
Session (Layer 5)	
Transport (Layer 4)	Transport
Network (Layer 3)	Internet
Data Link (Layer 2)	Network Access
Physical (Layer 1)	

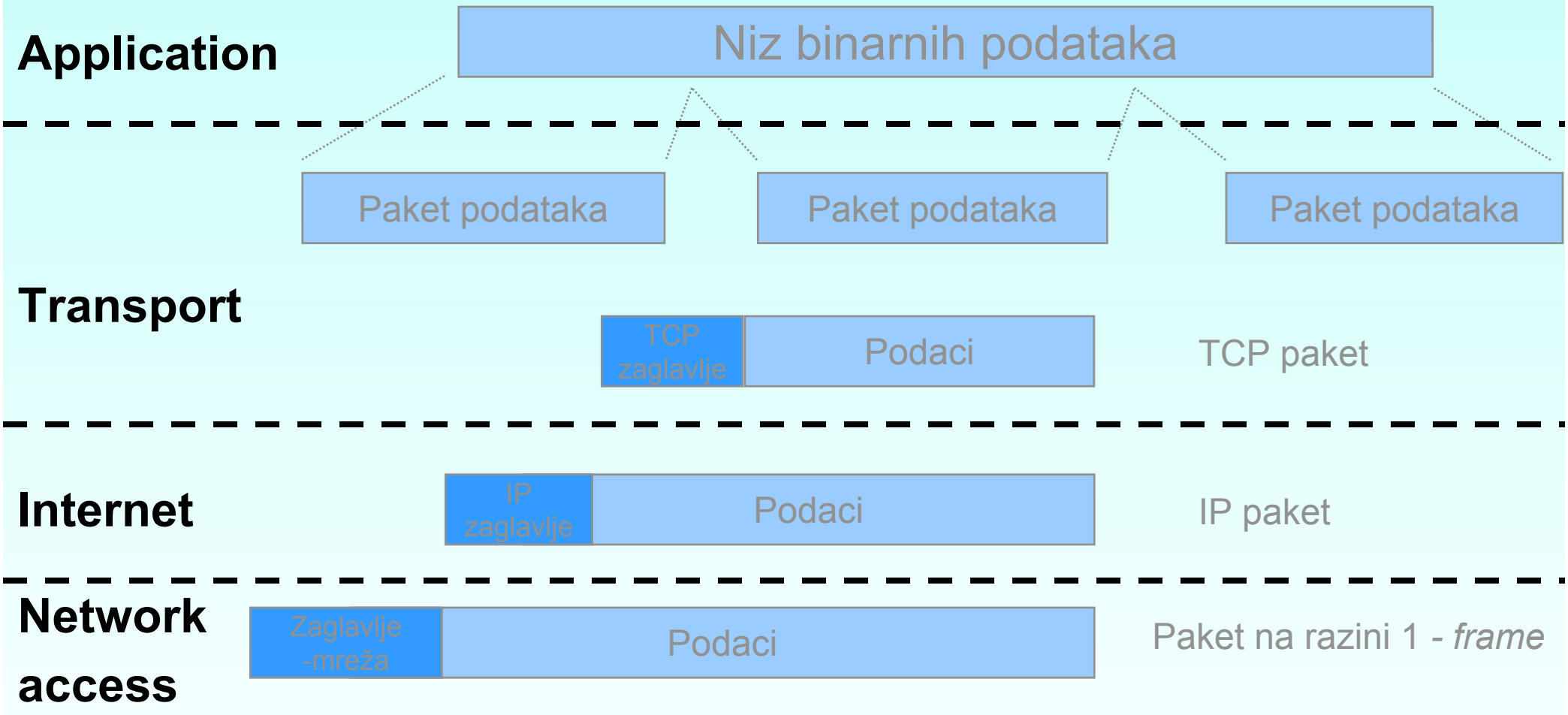
TCP/IP

Osnovni pojmovi – TCP/IP model (2)



TCP/IP

Osnovni pojmovi - enkapsulacija



TCP/IP

Osnovni pojmovi - aplikacijski sloj

- Povezan s korisničkim programima
- Vrši sinkronizaciju komunikacije između korisničkih aplikacija
- Provjerava mogućnost ostvarivanja komunikacije
- Priprema podatke za transportni sloj (niz bitova) – formatiranje, kompresija, enkripcija...
- Primjeri protokola aplikacijskog sloja: HTTP, FTP, SMTP...

TCP/IP

Transportni sloj

- Uspostavlja, koordinira i prekida komunikaciju između krajnjih IP čvorova
- Segmentiranje podataka s viših slojeva
- Multipleksiranje podataka od više aplikacija
- TCP - Transport Control Protocol
- UDP - User Datagram Protocol
- ICMP - Internet Control Message Protocol

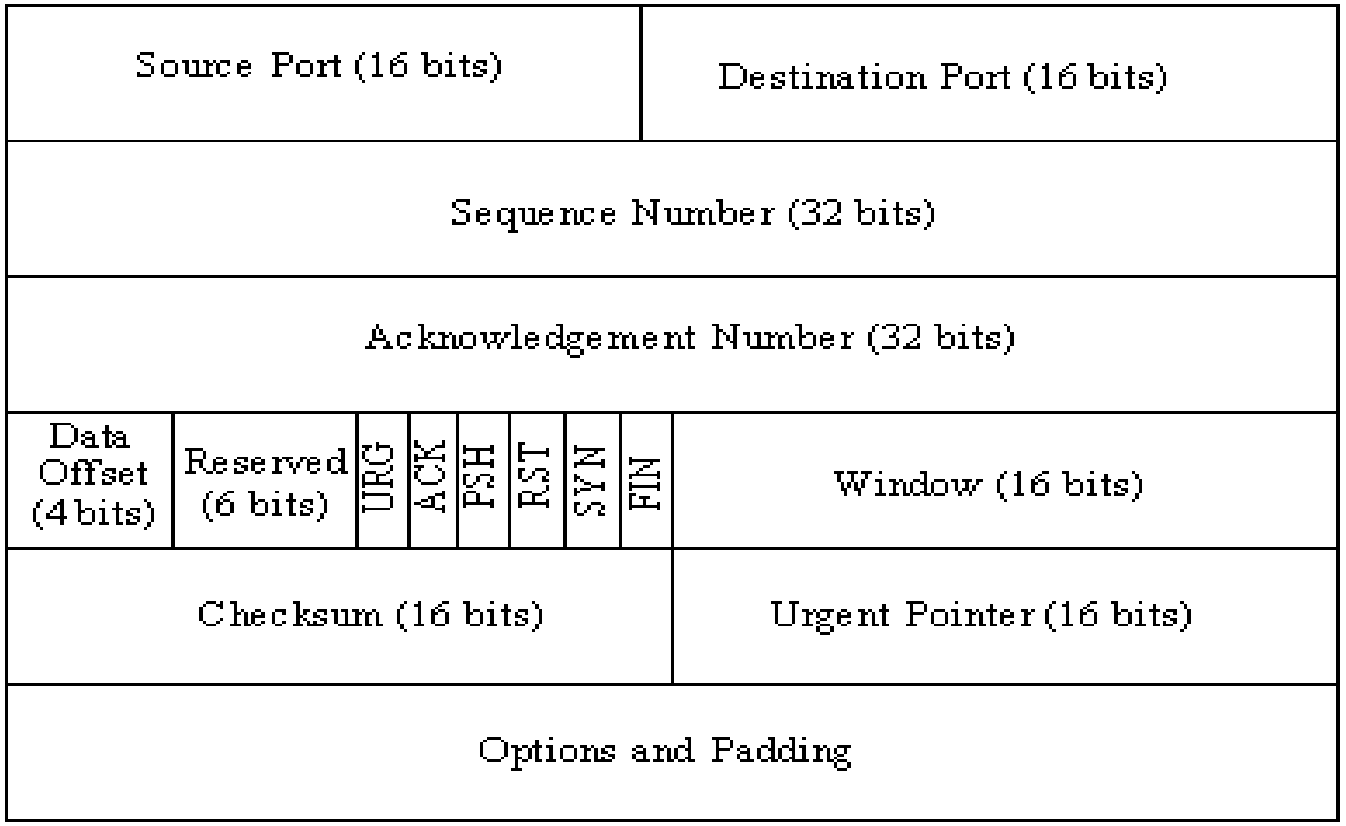
TCP/IP

Transportni sloj - TCP

- *Connection oriented*
- Detektiranje grešaka i retransmisija
- Segmentiranje i sastavljanje paketa
- Slaganje paketa po redoslijedu
- Kontrola toka podataka
- Potvrđivanje prijema paketa na prijamnoj strani
- “Siguran”, pouzdan, ali i složen protokol

TCP/IP

Transportni sloj - TCP (2)



TCP/IP

Transportni sloj - TCP (3)

- TCP komunikacija odvija se preko portova
- Tri grupe portova
  - 0 - 1023 – Well known ports
  - 1023 - 49151 – Registered ports
  - 49152 – 65525 – Dynamic or Private ports
- ICANN
- http://www.iana.org/assignments/port-numbers

TCP/IP

Transportni sloj - TCP (4)

- Više IP klijenata na jednom računalu (WWW, E-mail, FTP..) može se spajati istovremeno na IP servise
- Na jedan port servera može se istovremeno spajati više klijenata
- Za svaku aplikaciju na serveru potrebno je definirati TCP port na kojem aplikacija “sluša”

TCP/IP

Transportni sloj - TCP (5)

- /etc/services ili /etc/ports datoteka

```
% less /etc/services
```

- Pregled aktivnih portova (sesija):

```
% netstat -n
```

TCP/IP

Transportni sloj - TCP (6)

- Sequence Number – slijedni broj prvog okteta podataka u čitavoj poruci
- Acknowledgement Number – ako je ACK bit postavljen, ovaj broj označava Sequence Number kojeg primalac očekuje slijedećeg primiti – služi za potvrdu prijema

TCP/IP

Transportni sloj - TCP (7)

- Data Offset (4 bita) – broj 32-bitnih riječi u TCP zaglavlju
- Rsvd – 6 bitova je rezervirano za buduću uporabu, postavljaju se u 0
- Flags – URG, ACK, PSH, RST, SYN, FIN
  - URG – Urgent Pointer bit
  - ACK – Acknowledgment Number bit
  - PSH – Push funkcija - aplikacijski sloj traži “hitno” slanje paketa

TCP/IP

Transportni sloj - TCP (8)

- RST – Resetiranje TCP konekcije
- SYN – Služi za sinkronizaciju Sequence Number, koristi se pri uspostavi veze
- FIN - Indicira da pošiljalac nema više što slati - kraj transmisije

TCP/IP

Transportni sloj - TCP (9)

- Window
  - broj okteta počevši od okteta sadržanog u Acknowledgment Number polju koje primalac može primiti
  - pošiljalac može slati toliko okteta prije nego mora sačekati potvrdu prijema
  - ubrzanje komunikacije, kontrola toka, sprječavanje zagušenja

TCP/IP

Transportni sloj - TCP (10)

- Checksum
  - zbroj svih 16-bitnih riječi u TCP zaglavlju i podatkovnom dijelu TCP paketa – služi za provjeru ispravnosti prijenosa paketa
- Urgent Pointer
  - ako je URG bit postavljen, pokazuje na oktet koji bi primalac tog paketa trebao odmah (hitno) procesirati, npr. ako jedna strana pošalje kontrolni znak ili želi prekinuti sesiju

TCP/IP

Transportni sloj - TCP (11)

- Opcije
  - dodatni okteti koji mogu ići iza standardnog dijela TCP zaglavlja, a dužina im je n * 8 bitova, prenose neke dodatne informacije, npr. Maximum Segment Size
- Padding
  - ako duljina TCP paketa nije višekratnik od 32 bita, dodaju se dodatni bitovi bez značenja

TCP/IP

Transportni sloj - TCP (12)

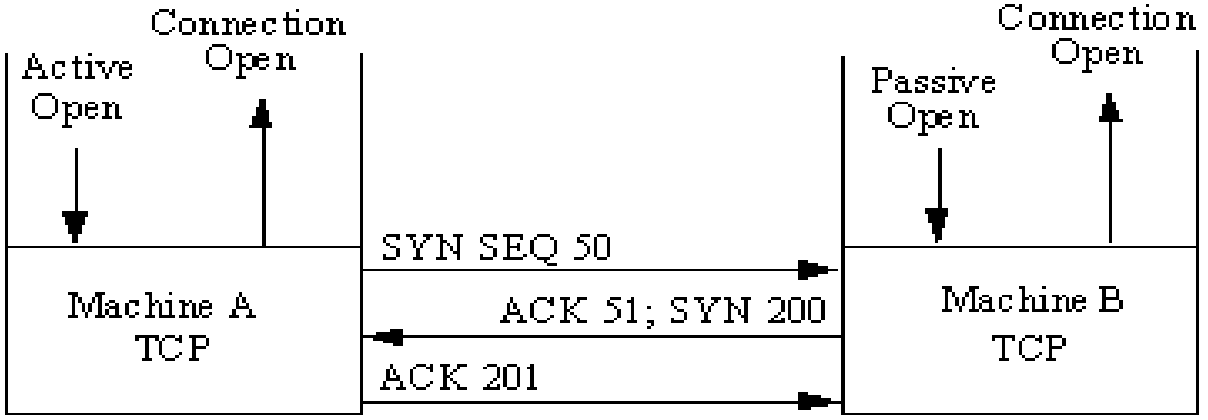
- TCP je konekcijski orijentiran, podaci se mogu prenositi tek kad je uspostavljena veza

- Uspostavljanje TCP sesije
- Razmjena paketa uz kontrolu toka podataka (Window, provjera, retransmisija, slaganje paketa, kontrolni *timeri...)*
- Zatvaranje TCP veze (sesije)

TCP/IP

Transportni sloj - TCP (13)

- **Uspostava veze (3-way handshake)**



TCP/IP

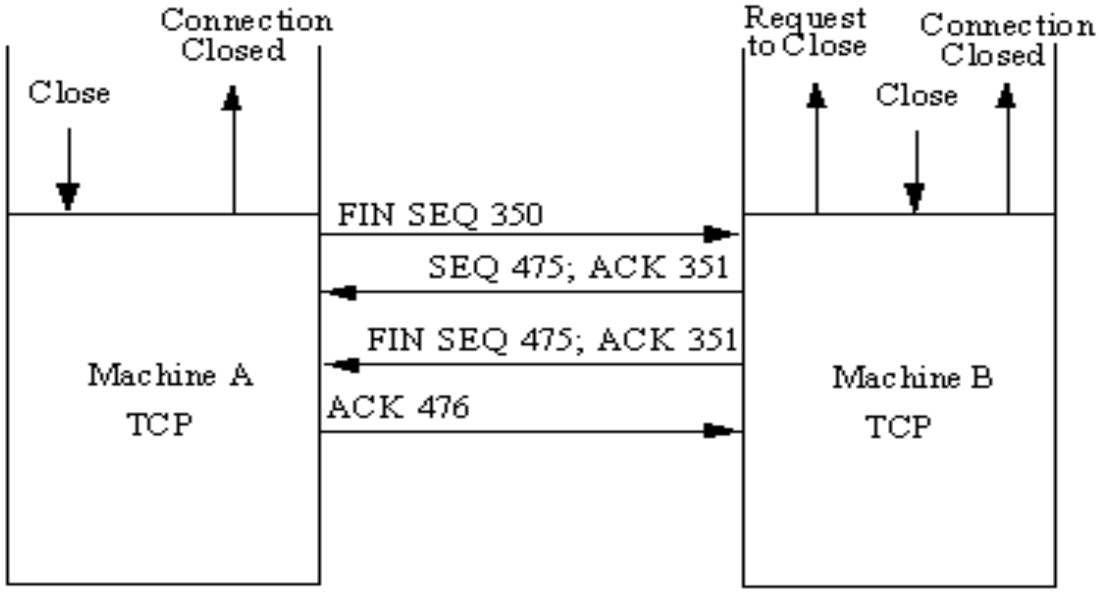
Transportni sloj - TCP (14)

- TCP šalje poruku s postavljenim SYN bitom i SEQ brojem (npr. 50), *source* i *destination port* brojem te drugim parametrima (*precedence, security, timeout*)
- Stanica B odgovara postavljenim ACK bitom i Ack. brojem 51 te SYN bitom i vlastitim SEQ brojem (200)
- Stanica A odgovora s ACK 201

TCP/IP

Transportni sloj - TCP (15)

- **Zatvaranje veze**



TCP/IP

Transportni sloj - TCP (16)

- A šalje poruku s postavljenim FIN bitom
- B šalje potvrdu stanici A i obavještava aplikaciju
- B šalje opet segment stanici A s postavljenim FIN bitom
- A šalje potvrdu

- Veze se mogu prekidati i “nasilno”, bez razmjene poruka

TCP/IP

Transportni sloj - UDP

- Jednostavniji od TCP-a
- *Connectionless oriented*
- Nepouzdaniji, ali “brži” od TCP-a, manje kašnjenje paketa
- Koriste ga prvenstveno aplikacijski protokoli koji nemaju velike pakete (DNS, SNMP...)
- Koriste ga i *real-time* aplikacije (video) zbog malog kašnjenja

TCP/IP

Transportni sloj - UDP (2)

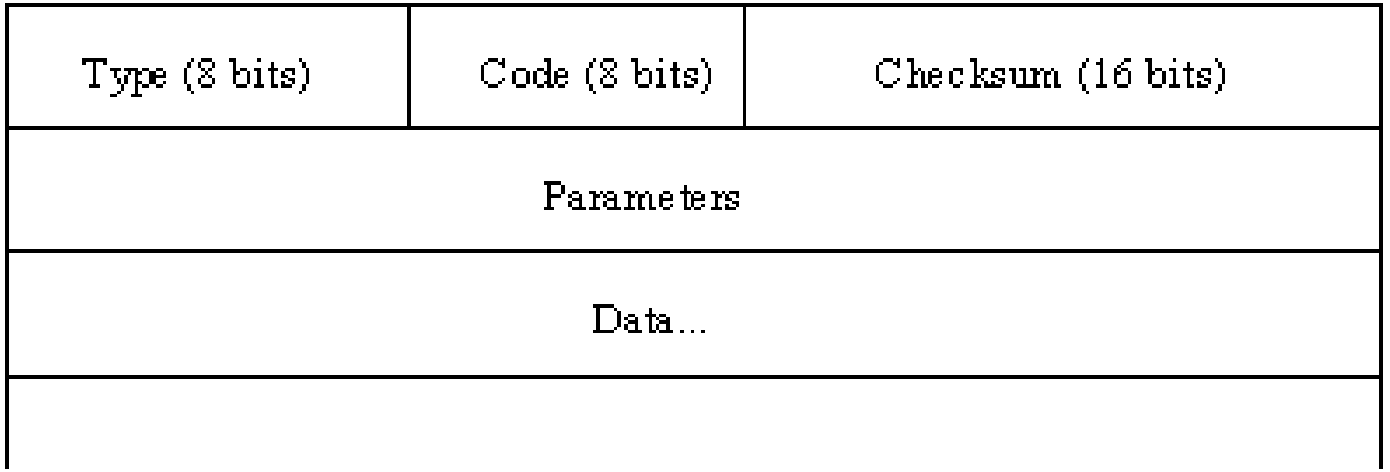
- UDP zaglavlje

Source Port (16 bits)	Destination Port (16 bits)
Length (16 bits)	Checksum (16 bits)
Data....	

TCP/IP

Transportni sloj - ICMP

- Protokol za dojavu grešaka
- Ostvaruje komunikaciju između IP slojeva, ne između aplikacija



TCP/IP

Transportni sloj - ICMP (2)

- Type – tip ICMP poruke
  - definirano 40-ak tipova (RFC 1700)
  - najčešći tipovi: Echo Reply, Destination Unreachable, Source Quench, Redirection Required, Echo Request, Time to Live Exceeded, Parameter Problem, Timestamp Request, Timestamp Reply, Address Mask Request, Address Mask Reply...

TCP/IP

Transportni sloj - ICMP (3)

- Pojedini tipovi mogu imati i kodove, koji ih pobliže opisuju
- Npr. kodovi za Time Exceeded tip ICMP poruke:
  - 0: Time to Live exceeded in Transit
  - 1: Fragment Reassembly Time Exceeded

TCP/IP

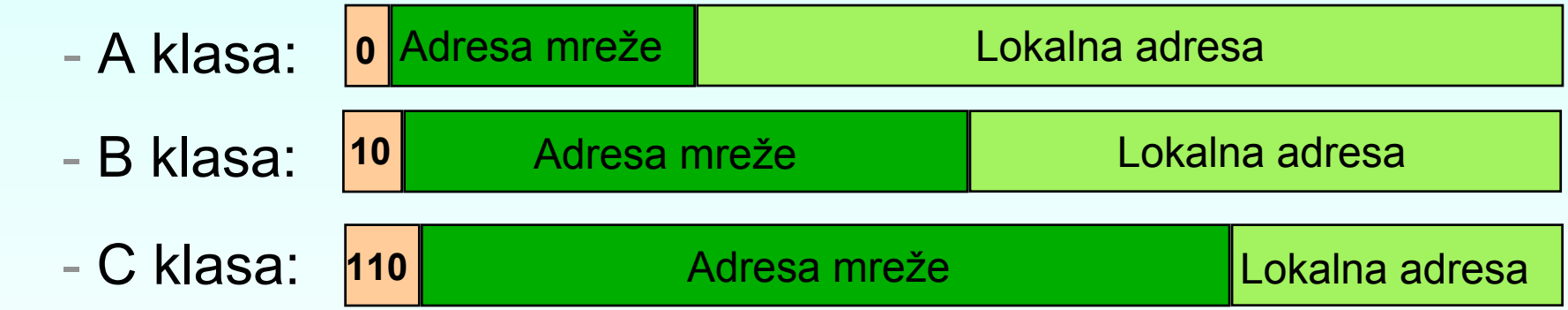
Internet Layer – IP adrese

- IP adrese – logičke adrese
- Sav IP promet se usmjerava i odvija preko IP adresa
- Jedno računalo ili IP uređaj može imati više IP adresa
- Dva ili više uređaja na povezanim IP mrežama ne mogu imati istu IP adresu, osim u posebnim slučajevima (NAT)

TCP/IP

Internet Layer – IP adrese (2)

- 32-bitni broj - *dotted-octet* notacija (X.Y.Z.T)
- dva dijela: adresa mreže i lokalna adresa
- tri osnovne klase IP adresa:



TCP/IP

Internet Layer – IP adrese (3)

- 1. adrese klase A,
  - oblika 1.x.x.x do 126.x.x.x,
- 2. adresa klase B,
  - oblika 128.0.x.x do 191.255.x.x,
- 3. adresa klase C,
  - oblika 192.0.0.x do 223.255.255.x,
- 4. adrese klase D
  - oblika 224.0.0.0 do 239.255.255.255,
  - multicast adrese

TCP/IP

Internet Layer – IP adrese (4)

- Privatne IP klase adresa:
- 10.X.X.X - A klasa
- 172.16-31.X.X - B klasa
- 192.168.0-255.X - C klasa

- Za pristup Internetu - NAT
- Nije moguć pristup s Interneta
  - moguće korištenjem statičkog NAT-a

TCP/IP

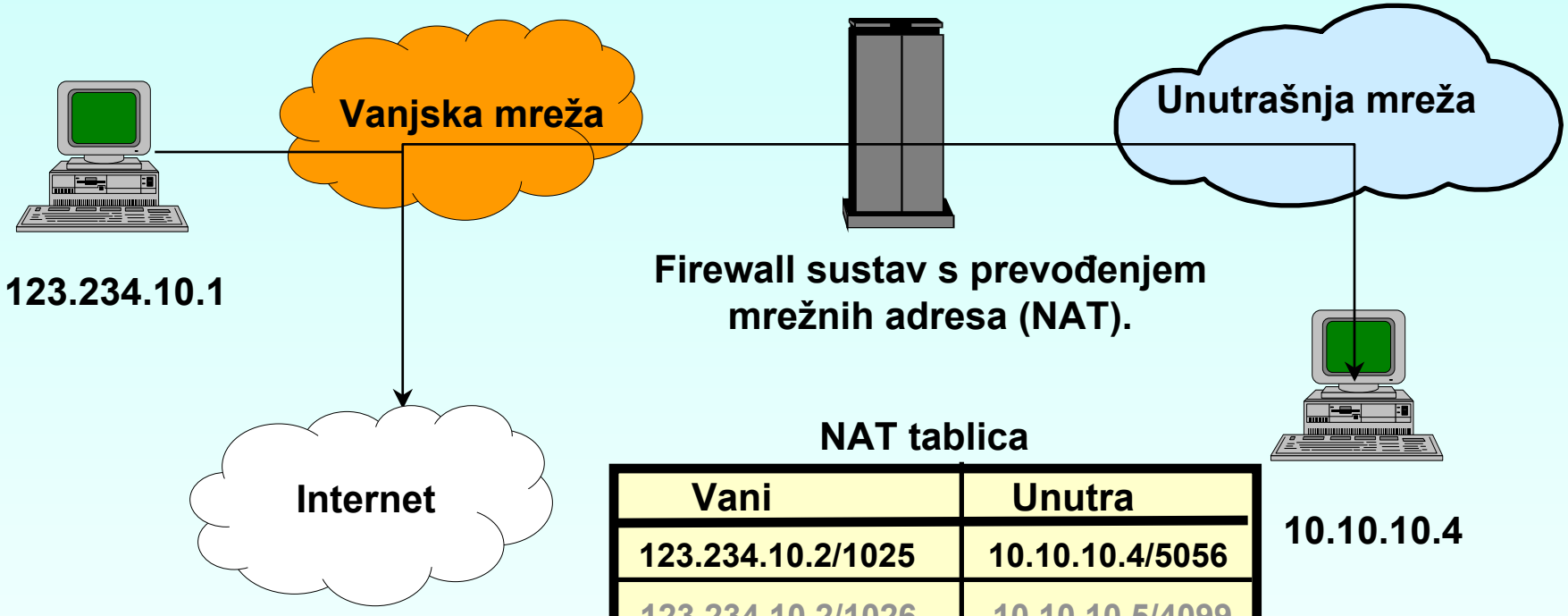
Internet Layer – IP adrese (5)

- Prevođenje mrežnih adresa (*Network Address Translation* - NAT)
  - sakriva adrese računala na internoj mreži
  - štedi IP adrese
  - povećava sigurnost privatnih mreža

  - neke *peer-to-peer* aplikacije ne rade ako je jedno ili oba računala iza NAT-a

TCP/IP

Internet Layer – IP adrese (6)



NAT tablica

Vani	Unutra
123.234.10.2/1025	10.10.10.4/5056
123.234.10.2/1026	10.10.10.5/4099
123.234.10.3/1027	10.10.10.6/5056

TCP/IP

Internet Layer – Interface

- Mrežno sučelje – svaki uređaj spojen na IP mrežu
- Mora imati najmanje jednu IP adresu
- Ne mora imati vlastitu adresu, može je preuzimati od drugog sučelja ili mu je dodjeljivati drugo sučelje (posebni slučajevi)
- Primjeri mrežnih sučelja: Ethernet mrežna kartica, serijsko modemsko sučelje

TCP/IP

Internet Layer – Interface (2)

```
% ifconfig -a
% ifconfig interface down
% ifconfig interface up
% netstat -I interface [interval]
```

- Pomoć:

```
% man ifconfig
% man netstat
```

- *ifconfig* naredba mora se izvršavati pri dizanju računala
  - napraviti /etc/hostname.* za svako sučelje
  - unijeti svako sučelje u /etc/hosts

TCP/IP

Internet Layer – Interface - vježbe

- Deaktivirati sučelje
- Aktivirati sučelje
- Pregledati statistiku prometa na LAN sučelju u intervalu od 30 sekundi
- Kreirati dva virtualna sučelja (slobodne IP adrese iz iste mreže) na jednom fizičkom sučelju

TCP/IP

Internet Layer – Interface – vježbe (2)

- Osigurati da se sučelja konfiguriraju automatski pri podizanju računala
  - Sučeljima dati proizvoljna imena iz nove domene (npr. kruska.kiki.hr, jabuka.kiki.hr...)
- Provjeriti dostupnost sučelja
  - `% ping` *`ip_adresa_sucelja`*
  - `% ping` *`ime_sucelja`* `(s drugog računala)`

TCP/IP

Internet Layer – Subnet mask

- Omogućava segmentiranje IP mreža na podmreže
- “1”-ce označavaju mrežni dio adrese, “0” host dio
- *Default* maska - prema klasi kojoj adresa pripada
- Npr. adresa 160.30.100.10 pripada B klasi, *default* maska je 255.255.0.0, adresa mreže je 160.30.0.0

TCP/IP

Internet Layer – Subnet mask (2)

- Adresa 160.30.100.10/255.255.192.0 znači da je klasa B segmentirana, adresa mreže je 160.30.64.0
- 255.255.192.0 = 11111111.11111111.11000000.0000000
- Prva dva bita trećeg okteta određuju adresu podmreže, 00 i 11 se ne koriste za adresu podmreže (adresa mreže i *broadcast* adresa)

TCP/IP

Internet Layer – Subnet mask (3)

- Broj nula u adresnoj maski određuje max. broj hostova na mreži
- U gornjem primjeru broj hostova je 16 384 -2
- Prva i zadnja adresa se ne koriste jer su to adresa podmreže i *broadcast* adresa podmreže

```
% ifconfig -a
```

- Koja je adresa ove mreže, maska, raspon IP adresa i *broadcast* adresa?

TCP/IP

Internet Layer – Subnet mask (4)

- Segmentiranje C klase

# Mask Bits	Subnet Mask	#Subnets	#Hosts
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

TCP/IP

Internet Layer – Subnet mask - vježbe

- Napraviti tablicu adekvatnu onoj na prethodnom *slideu* za B klasu

- Segmentirati dobivenu C klasu (npr. 193.198.155), ako želimo
  - jednu mrežu sa 40 računala
  - tri mreže sa 20 računala
  - napisati adrese mreža i maske za sve mreže (u binarnom i decimalnom obliku)

TCP/IP

Internet Layer – Adresiranje u CARNetu

- CARNet ima dva raspona adresa:
  - 161.53.x.x (B klasa)
  - 193.198.1.0 – 193.198.254.0 (C klasa)
- Na CARNetu se uglavnom koriste javne IP adrese
- Primjer FER-a:
  - svaki zavod ima jednu C podklasu nastalu segmentiranjem B klase 161.53.x.x, mrežna maska je 255.255.255.0
- Moguće koristiti privatne adrese + NAT

TCP/IP

Internet Layer – routing

- Usmjeravanje paketa na osnovi IP adrese
- Statičko i dinamičko usmjeravanje
- Statičko usmjeravanje
  - upisuju se rute do svih mreža + *default route*
  - manje mreže
  - mreže koje se ne mijenjaju često
  - ne troši se nepotrebno prijenosni pojas

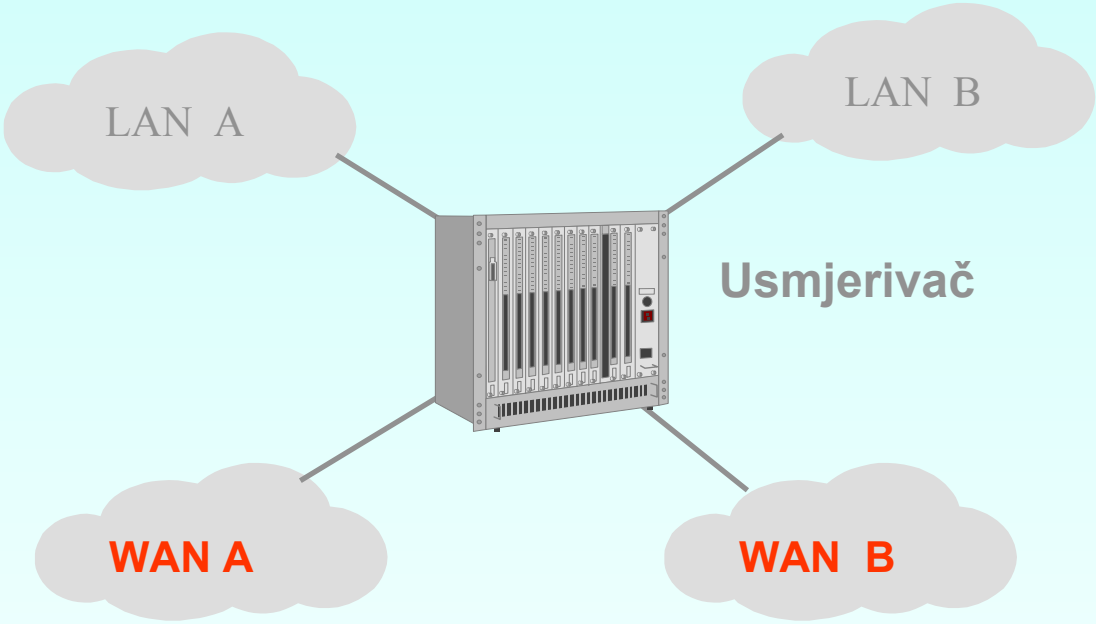
TCP/IP

Internet Layer – routing (2)

- Dinamičko usmjeravanje
  - *routeri* razmjenjuju *routing* informacije
  - promjene u mreži se automatski oglašavaju i mreža im se prilagođava
  - dodatno opterećenje linkova (prijenosnog pojasa)
  - nužnost za veće i “dinamičnije” mreže
  - nije preporučljivo na mrežama s dial-up vezama

TCP/IP

Internet Layer – routing (3)



- Uređaj za povezivanje IP mreža

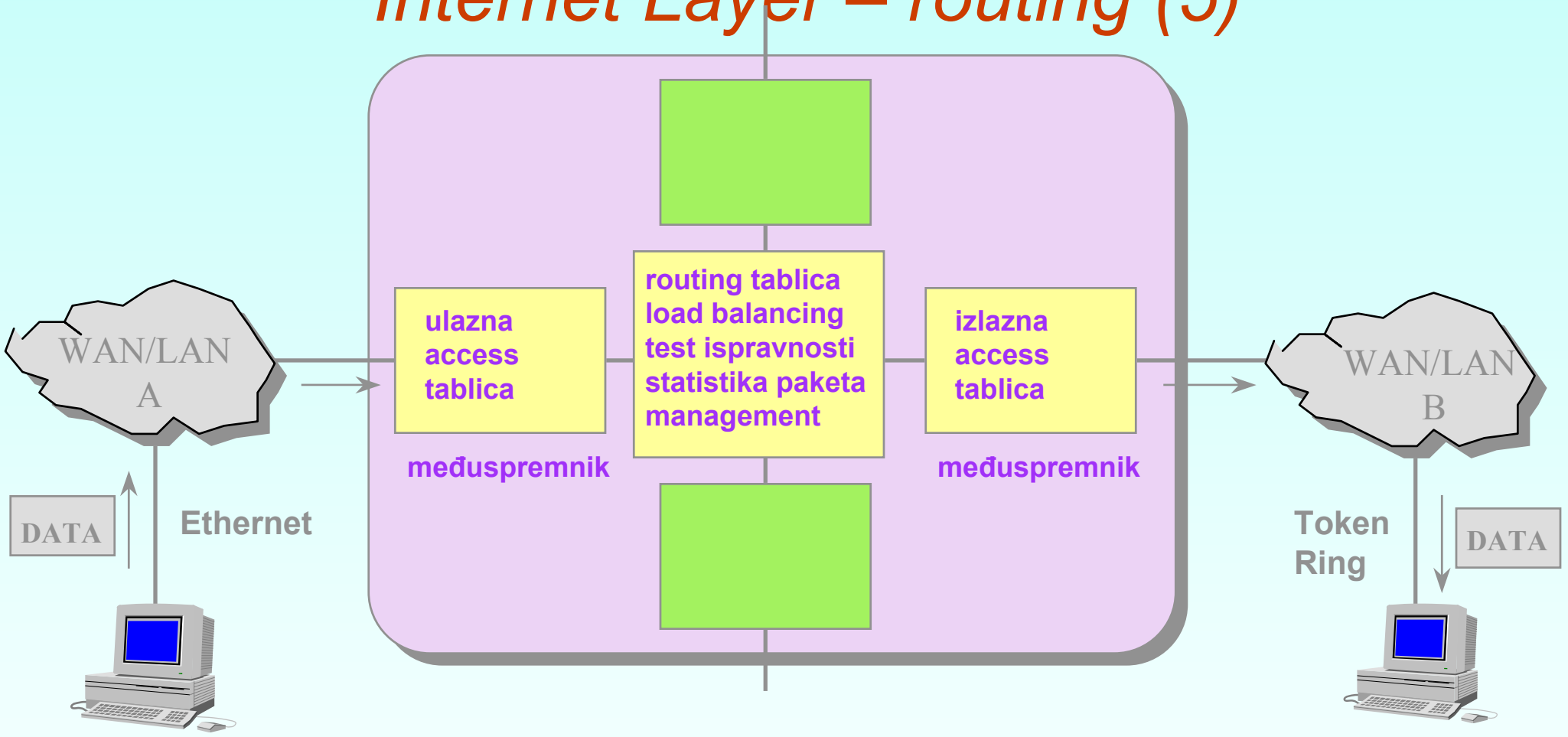
TCP/IP

Internet Layer – routing (4)

- Prilagođenje različitim medijima i protokolima
- Zbog složenijeg odlučivanja (programski) i veće funkcionalnosti sporije od preklapanja na Layeru 2
- WAN sučelja (serijska) i LAN (Ethernet)
- Računalo (npr. Unix radna stanica) s Ethernet i serijskim (modemskim) priključkom može vršiti usmjeravanje (IP *forwarding*)

TCP/IP

Internet Layer – routing (5)



TCP/IP

Internet Layer – routing (6)

- *Routing* tablica

```
% netstat -rn
```

```
  Destination     Gateway       Flags  Ref    Use    Interface
-------------------------------------------------------------
161.53.64.0     161.53.64.3     U      2     10562    hme0
224.0.0.0       161.53.64.3     U      2       0      hme0
default         161.53.64.1     UG     0     98906    hme0
204.36.8.0      204.36.8.15     UG      1    8251    ipdptp0
127.0.0.1       127.0.0.1       UH     0     13025    lo0
```

```
% route add -net 204.36.10.0 netmask
  255.255.255.0 204.36.8.15
```

TCP/IP

Internet Layer – routing - vježbe

```
% man route
% man netstat
```

- Pregledati *routing* tablicu na računalu
- Dodati statičke rute (npr. do 161.53.64.0/24)
- Izbrisati statičke rute
- Osigurati uspostavljanje statičkih ruta prilikom dizanja računala
  - dodati *route* komandu u *boot* datoteku (/etc/init.d/inetsvc, /rc2.d/Sxxxinetsvc)

TCP/IP

Internet Layer – routing (7)

- routing protokoli
  - interni: RIP, RIPv2, IGRP, OSPF, IGRP, IS-IS
  - eksterni: EGP, BGP, BGP4
- po načinu razmjene routing informacija:
  - *Distance Vector* protokoli: RIP, RIPv2, IGRP, EIGRP
  - *Link State* protokoli: OSPF, IS-IS
- Razmjena informacija između različitih *routing* protokola

TCP/IP

Internet Layer – routing (8)

- Distance Vector *routing* protokoli
  - razmjena cijelih *routing* tabela između susjednih routera
  - periodička razmjena *routing* tabela
  - sporo vrijeme konvergencije
  - opasnost od “petlji”
  - troše dosta *bandwitha*
  - lakša konfiguracija i održavanje mreže
  - pogodni za manje i statičke mreže

TCP/IP

Internet Layer – routing (9)

- Link State *routing* protokoli
  - svaki *router* ima mapu cijele mreže
  - oglašavaju se samo veze do susjednih *routera*
  - oglašavanje kod *reboota* i zatim samo kad se dogode promjene u topologiji mreže
  - podjela na *routing areas* - hijerarhijski model
  - oglasi ruta se šalju svim *routerima* u zoni [*area*]
  - puno brža konvergencija
  - troši se puno *bandwitha* samo pri konvergiranju
  - visoki zahtjevi na CPU i memoriju *routera*

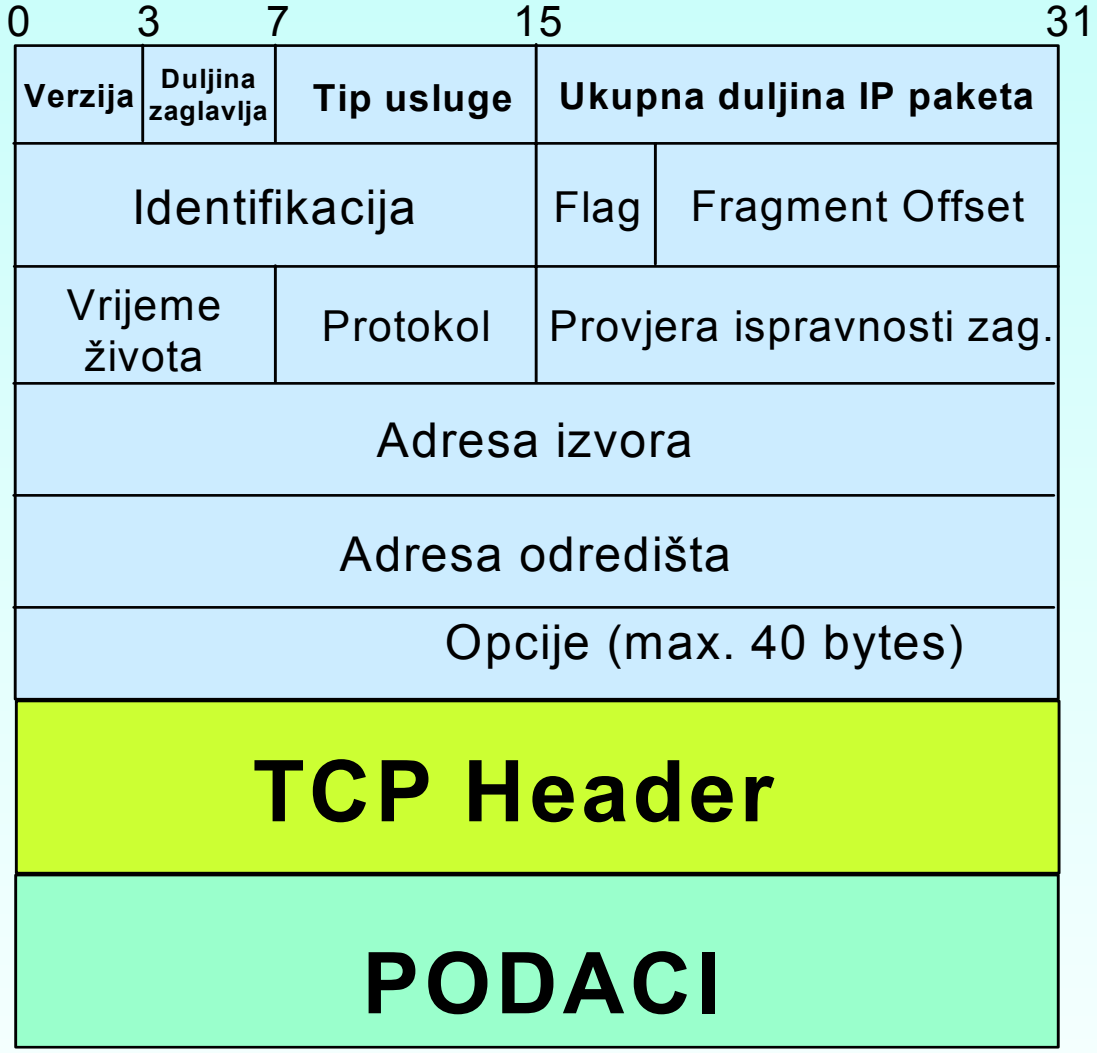
TCP/IP

Internet Layer – routing (10)

- Osobine usmjeravanja i usmjerivača
  - mogućnost dinamičkog biranja najboljeg puta
  - mogućnost segmentiranja vlastite mreže
  - praćenje i kontrola portova i aplikacija u upotrebi
  - kategorizacja prometa, *load balancing*
  - enkapsulacija (tunneling)
  - mrežna statistika
  - pristupne liste
  - usmjerivači su sporiji od preklopnika

TCP/IP

Internet Layer – IP datagram



TCP/IP

Internet Layer – IP datagram (2)

- Verzija - IPv4 ili IPv6
- Duljina zaglavlja - duljina IP zaglavlja izražena u 32-bitnim riječima, uključujući opcije
- Tip usluge - omogućava QoS
  - bitovi 7-5 - IP precedence - 8 klasa IP paketa
  - 4 - delay (0 - normal, 1 - malo kašnjenje)
  - 3 - throughput (0 - normal, 1 - velika propusnost)
  - 2 - pozdanost (0 - normal, 1 - velika pouzdanost)
  - 1,0 - ne koriste se

TCP/IP

Internet Layer – IP datagram (3)

- Duljina IP paketa - ukupna duljina IP paketa (u oktetima) => max. 65 535 okteta
- Identifikacija - jedinstveni broj kojeg dodjeljuje pošiljalac, služi za sastavljanje segmentiranih IP paketa
- Flags
  - bit 2: ne koristi se
  - bit 1: DF (*Don't fragment*) - ako je 1, paket se ne smije fragmentirati
  - bit 0: MF (*More fragments*) - ako je 1, ima još segmenata ove IP poruke

TCP/IP

Internet Layer – IP datagram (4)

- Fragment offset - sadrži poziciju segmenta u cijeloj poruci, tj. pomak (u oktetima) od početka poruke
- Vrijeme života (TTL) - broj sekundi prije otkazivanja IP datagrama. Svaki čvor smanjuje taj broj (po *defaultu* 15 ili 30) za vrijeme obrade datagrama, a min. za 1
- Protokol - označava Layer 4 protokol - najčešće TCP, UDP ili ICMP

TCP/IP

Internet Layer – IP datagram (5)

- Header Checksum - 16-bitni zbroj svih 16-bitnih riječi u IP zaglavlju, služi za provjeru ispravnosti prijenosa, računa se na svakom čvoru
- Adresa izvora i odredišta - 32-bitna IP adresa pošiljaoca i primaoca, ne mijenja se tijekom puta paketa od izvora do odredišta (osim u slučaju NAT-a)

TCP/IP

Internet Layer – IP datagram (6)

- Opcije - dodatni podaci u IP zaglavlju
  - počinju 8-bitnom riječi:
  - 1-bitni *copy flag*,
  - 2-bitna klasa opcija, trenutno su definirane 2 klase od četiri moguće
  - 5-bitni opcijski broj
- Padding - ako duljina IP zaglavlje nije višekratnik od 4 okteta, dodaju se dodatni okteti za popunjavanje

TCP/IP

Internet Layer – IP datagram (7)

Option Class	***Option Number***	***Description***
0	0	Marks the end of the options list
0	1	No option (used for padding)
0	2	Security options (military purposes only)
0	3	Loose source routing
0	7	Activates routing record (adds fields)
0	9	Strict source routing
2	4	Timestamping active (adds fields)

TCP/IP

Internet Layer – ICMP alati

- Služe za ispitivanje spojnosti između dviju točaka i provjeru mreže i puta paketa
- Ping - naredba koja inicira Echo Request/Reply sustav – ispituje spojnost između dvije točke
- Traceroute - pošiljalac dobiva ICMP odgovore i bilježi IP adresu svakog čvora kroz kojeg prođe paket do odredišta

TCP/IP

Internet Layer – ICMP alati (2)

- Osnovni oblik

```
% ping host [timeout]
```

- Prošireni oblik

```
% ping -s[drvRlLn] [-I interval] [-t ttl]
  [-i interface] host [data size]
  [npackets]
```

- Pomoć

```
% man ping
```

TCP/IP

Internet Layer – ICMP alati (3)

- Primjer:

```
% ping -s www.CARNet.hr
  PING gamma.carnet.hr: 56 data bytes
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=0.
    time=4. ms
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=1.
    time=1. ms
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=2.
    time=1. ms
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=3.
    time=1. ms
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=4.
    time=5. ms
  64 bytes from gamma.CARNet.hr (161.53.123.4): icmp_seq=5.
    time=1. ms
```

TCP/IP

Internet Layer – ICMP alati (4)

- Osnovni oblik

```
% traceoute host [timeout]
```

- Prošireni oblik

```
% traceroute [-dnrv] [-w wait] [-m
  max_ttl] [-p port#] [-queries] [-t tos]
  [-ssrc_addr] host [data size]
```

- Pomoć

```
% man traceroute
```

TCP/IP

Internet Layer – ICMP alati (5)

- Primjer:

```
% traceroute www.CARNet.hr
  traceroute to gamma.carnet.hr (161.53.123.4), 30 hops max, 40
    byte packets
   1  zemsgwy (161.53.64.1)  2 ms  1 ms  2 ms
   2  nsk-ro.CB4.CARNet.hr (161.53.113.73)  2 ms  2 ms  5 ms
   3  gamma.CARNet.hr (161.53.123.4)  5 ms *  1 ms
```

TCP/IP

Internet Layer – IPv6

- 128-bitni adresni prostor – 4x više od IPv4, nema potrebe za NAT-om
- Sigurnost uključena u osnovnu specifikaciju (Extension Headers)
  - ESP - Encapsulated Security Payload
  - AH - Authentication Header

TCP/IP

Internet Layer – IPv6 (2)

- Podrška *real-time* aplikacijama - *flowlabel*
- Plug and Play - automatsko spajanje uređaja na mrežu
- IPv6 zadržava dobre osobine IPv4, a odbacuje njegove lošije ili malo korištene stvari

TCP/IP

Internet Layer – IPv6 (3)

TCP/IP

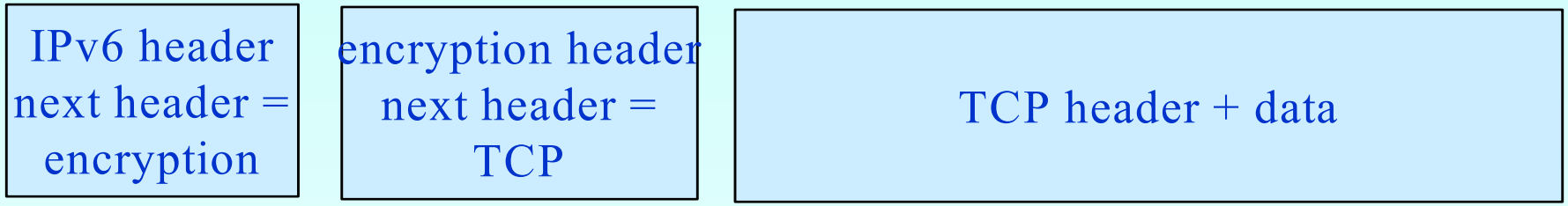
Internet Layer – IPv6 (4)

- Traffic Class - klasifikacija paketa po prioritetu
- Flow label - omogućava npr. *real-time* aplikacijama da svoj tijek poruka označe 24-bitnim brojem, a usmjerivači na osnovi tog broja i IP adrese izvora mogu proslijediti paket bez klasičnog usmjeravanja
- Hop Limit - max. broj čvorova koje paket može proći prije otkazivanja - svaki čvor umanjuje ovaj broj za 1

TCP/IP

Internet Layer – IPv6 (5)

- Extension Headers



- Samo krajnji čvor procesira ext. headere - manji *overhead* od IPv4
- Eliminirano IPv4 ograničenje opcija na 40 okteta

TCP/IP

Network Access Layer

- Odgovoran za prijenos poruka od točke do točke ili kroz “svoju” mrežu
- Fizičko adresiranje, detekcija (i korekcija) grešaka, kontrola toka podataka i zagušenja
- Logical Link Control (LLC) i Medium Access Control podslojevi (MAC)
- LAN i WAN Network Layer protokoli

TCP/IP

Network Access Layer (2)

- LAN, MAN
  - Ethernet
  - Token Ring, Token Bus
  - FDDI/CDDI
  - 100BaseVG AnyLAN
  - FibreChannel
  - bežični Ethernet,
  - ATM

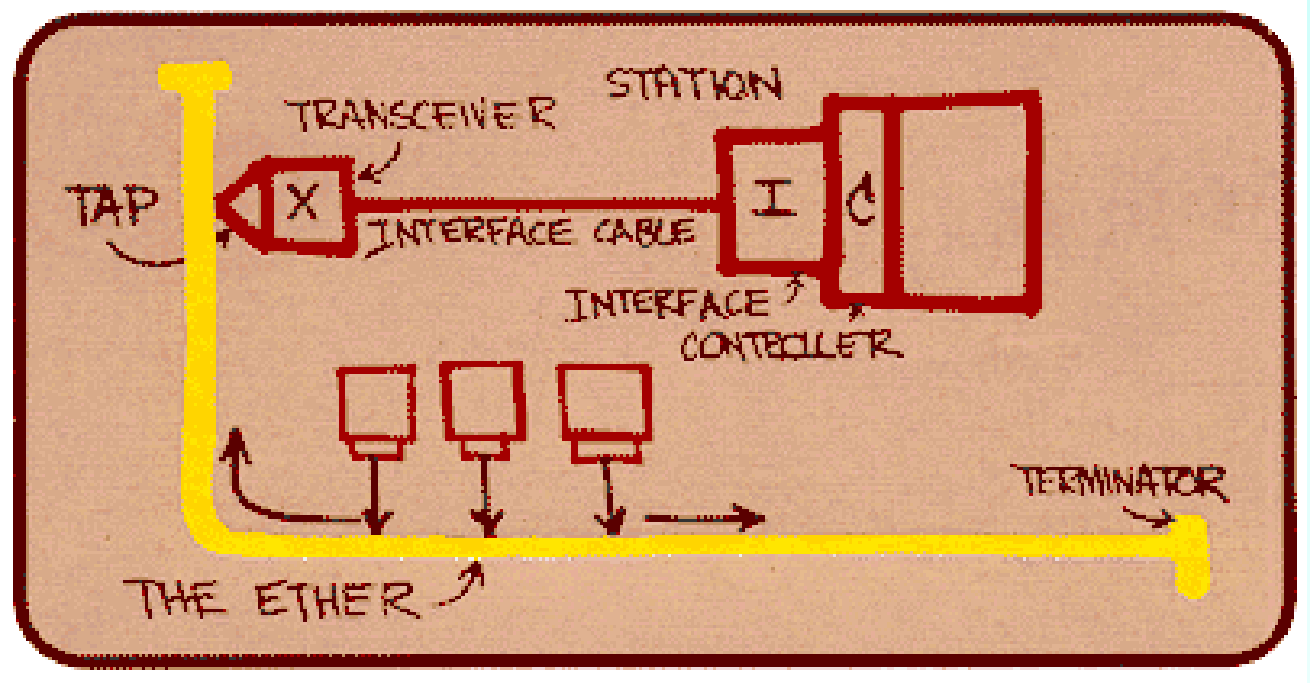
TCP/IP

Network Access Layer (3)

- WAN
  - Point-to-Point Protocol (PPP)
  - ATM
  - Frame Relay
  - X.25
  - Packet over Sonet/SDH (PoS)
  - Spatial Reuse Protocol (SRP)

TCP/IP

Network Access Layer - Ethernet



Skica prvog Ethernet sustava,
Dr. Robert M. Metcalfe, 1976.

TCP/IP

Network Access Layer - Ethernet (2)

- IEEE 802.3 CSMA/CD
- 10 Mbit/s
- CSMA/CD - Carrier Sence Multiple Access / Collision Detection - protokol koji regulira pristup dijeljenom mediju

TCP/IP

Network Access Layer - Ethernet (3)

- 10Base5 (thick koaks) - topologija sabirnice, Manchester kodiranje
- 10Base2 (thin koaks) - 500m, topologija sabirnice, Manchester
- 10BaseT (UTP, STP min. Cat.3) - 100m+ UTP, 500m STP, topologija zvijezde, Manchester
- 10BaseF (optika) - MM 2km max., SM 25km, topologija zvijezde, Manchester/on-off

TCP/IP

Network Access Layer - Ethernet (4)

- Fast Ethernet
  - IEEE 802.3u, definiran 1995.
  - 100 Mbit/s
  - 100BaseTX - UTP, STP Cat.5 i 5e, 100m, 4B/5B NRZI kodiranje
  - 100BaseT4 - UTP, STP Cat.3, 100m, 8B6T, NRZ
  - 100BaseFX - optika, MM 2km max., SM 20km 4B/5B NRZI kodiranje

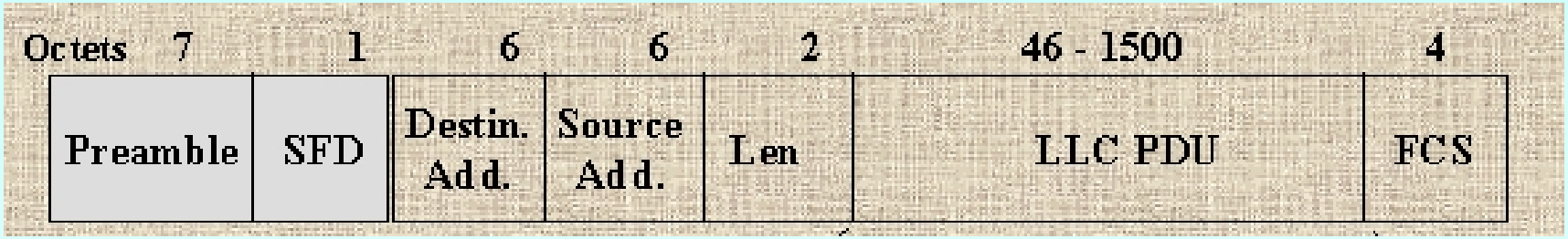
TCP/IP

Network Access Layer - Ethernet (5)

- Gigabit Ethernet
  - IEEE 802.3z - prijenos optičkim kabelom
  - IEEE 802.3ab - prijenos paričnim kabelom kategorije 5 (5e)
  - Standard usvojen 1998. Godine
  - 1 Gbit/s
  - 1000BaseSX - MM svjetlovodni kabel
  - 1000BaseLX - SM svjetlovodni kabel
  - 1000BaseCX - koaksijalni kabel
  - 1000BaseT - parični simetrični kabel kategorije 5

TCP/IP

Network Access Layer - Ethernet (6)

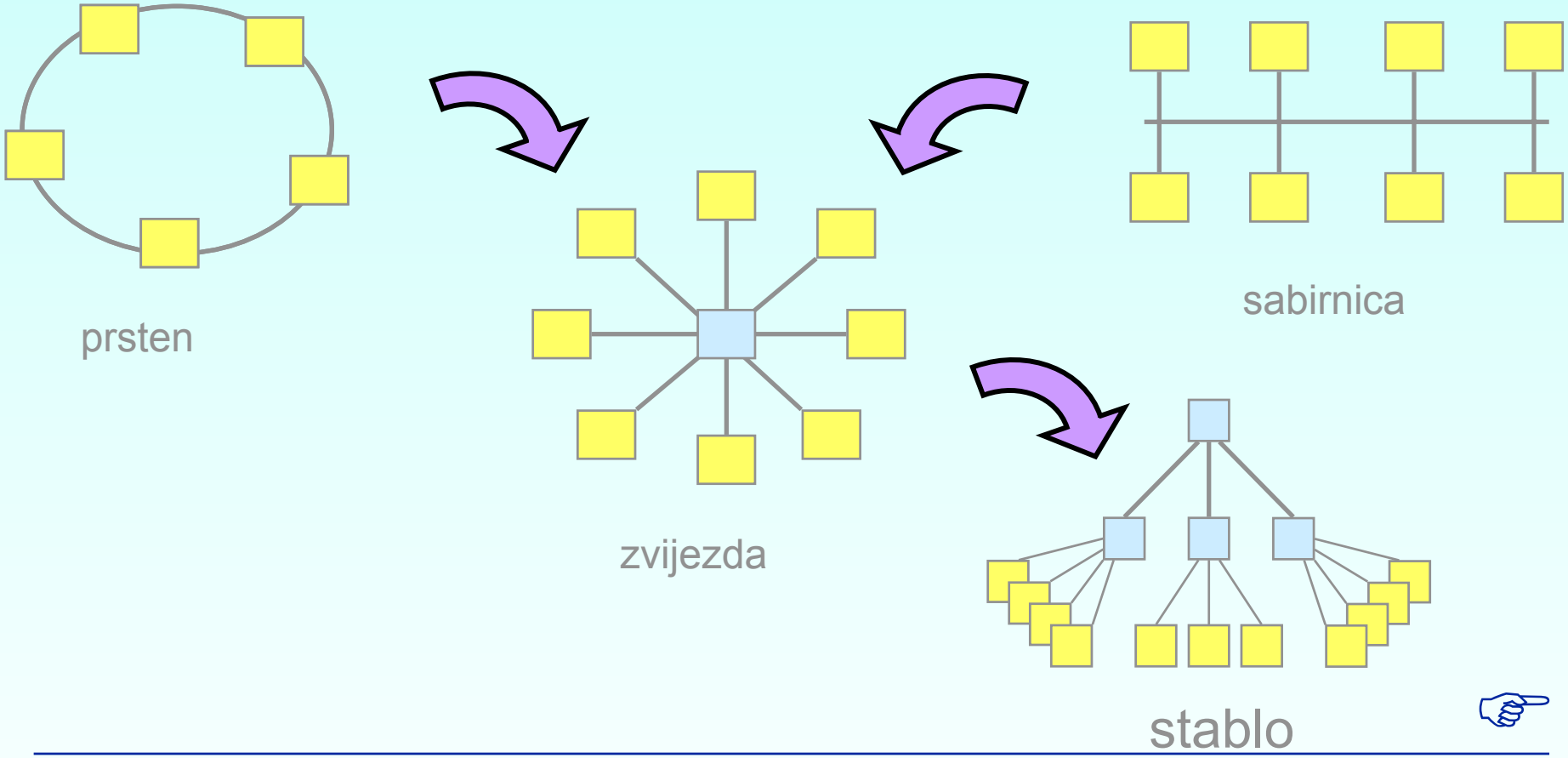


- Preamble – 7 * 10101010 – sinkronizacija prijamnika i predajnika
- SFD – Start-of-Frame delimiter
- Len – duljina *payload*-a (46 – 1500)
- Dest, Source Add. – MAC adrese prijamnika i predajnika
- FCS – Frame Check Sequence - CRC

TCP/IP

Network Access Layer - Ethernet (7)

- Topologije LAN-ova



TCP/IP

Network Access Layer - Ethernet (8)

- Učenje adresa
  - kad primi svaki paket, preklopnik zapisuje izvorišnu MAC adresu i pridjeljuje je portu na koji je paket došao
  - svaka stanica prilikom priključenja na mrežu i uključivanja emitira broadcast

TCP/IP

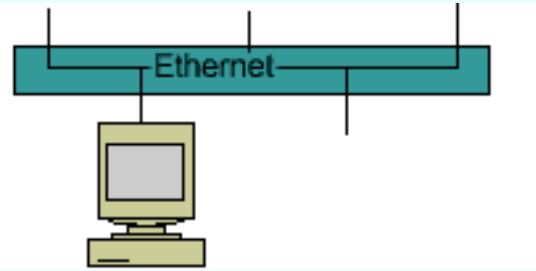
Network Access Layer - Ethernet (9)

- Prosljeđivanje paketa
  - SW po primitku pregleda odredišnu MAC adresu, ako je ima u tablici MAC adresa, šalje je na pripadajući port
  - ako je odredišna adresa nepoznata, switch šalje *frame* na sve portove

TCP/IP

Network Access Layer - Ethernet (10)

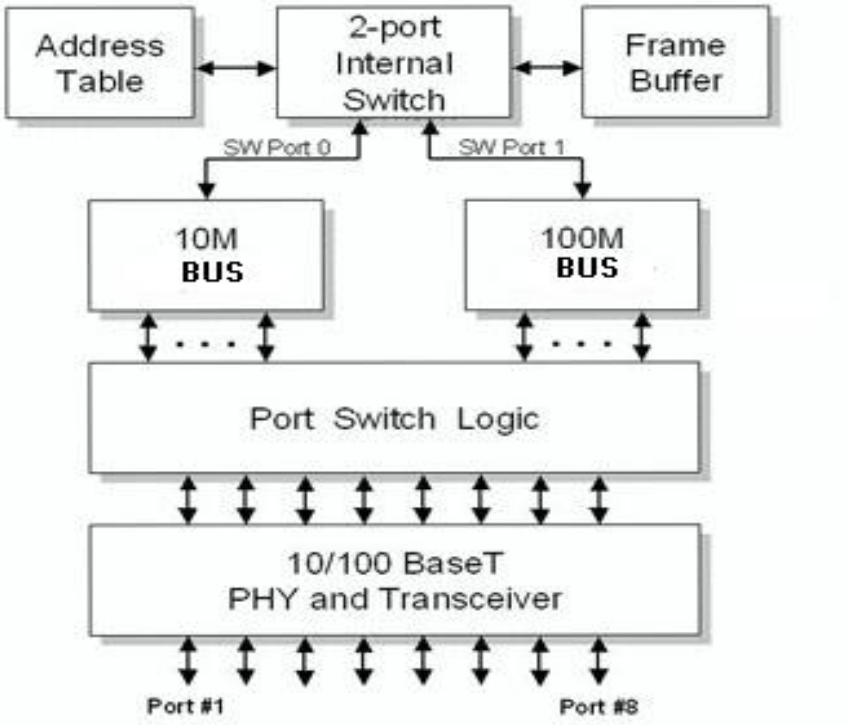
- Koncentrator - Hub
  - 10 i 100 Mbit/s uređaji
  - dijeljeni medij - shared media
  - interna sabirnička struktura kapaciteta 10 ili 100 Mbit/s



TCP/IP

Network Access Layer - Ethernet (11)

- Dual speed hub



FDS00DS "Dual Speed Hub" mode (Mode 0) functional block diagram

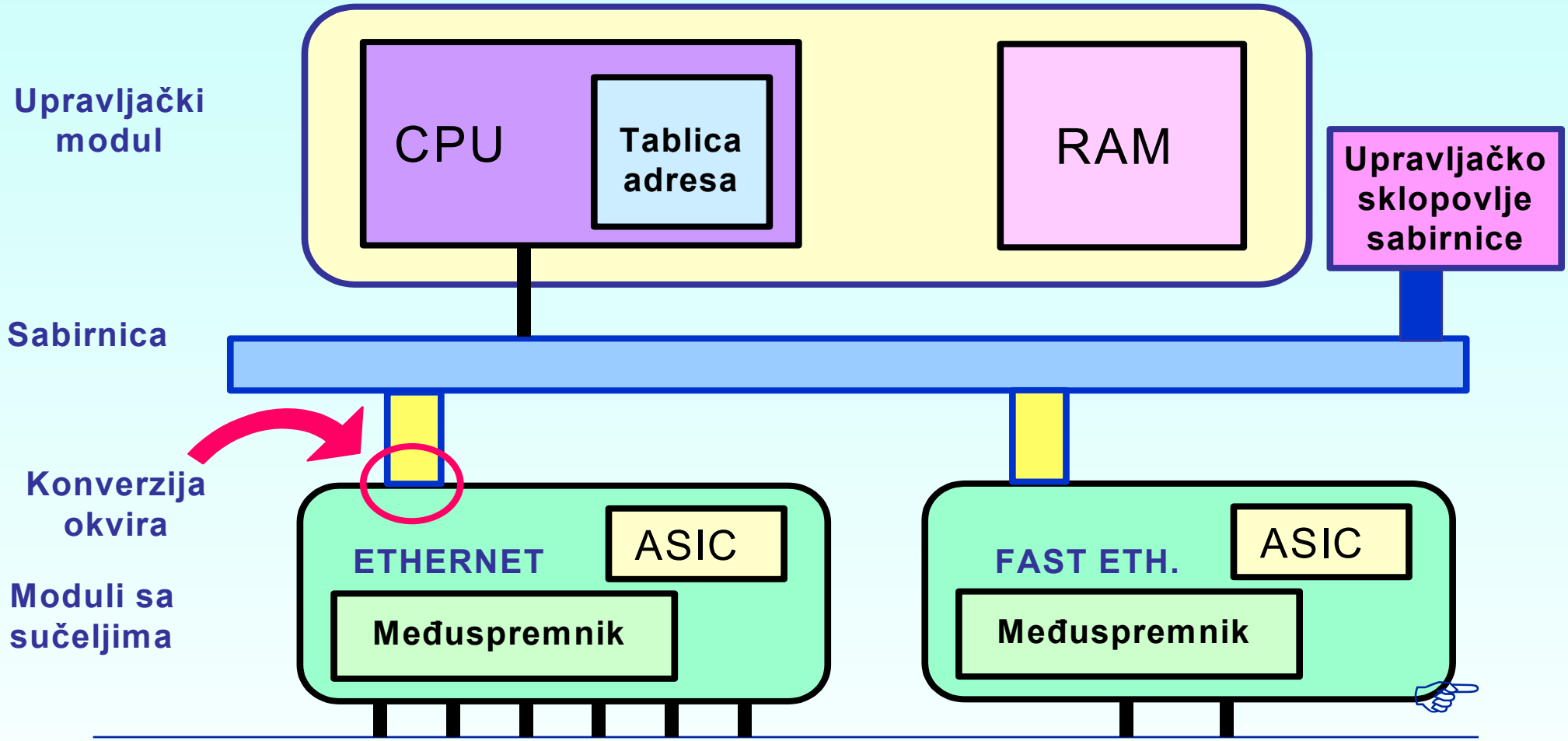
TCP/IP

Network Access Layer - Ethernet (12)

- Preklopnik
  - pregledava se odredišna i polazišna MAC adresa svakog dolaznog okvira, donosi se odluka kuda ga treba proslijediti, te ga se prosljeđuje
  - nije ga potrebno konfigurirati
  - moderni uređaji složeniji, posjeduju mnoštvo dodatnih funkcija
  - bitna karakteristika: kapacitet memoriranja MAC adresa
  - fiksni i modularni preklopnici

TCP/IP

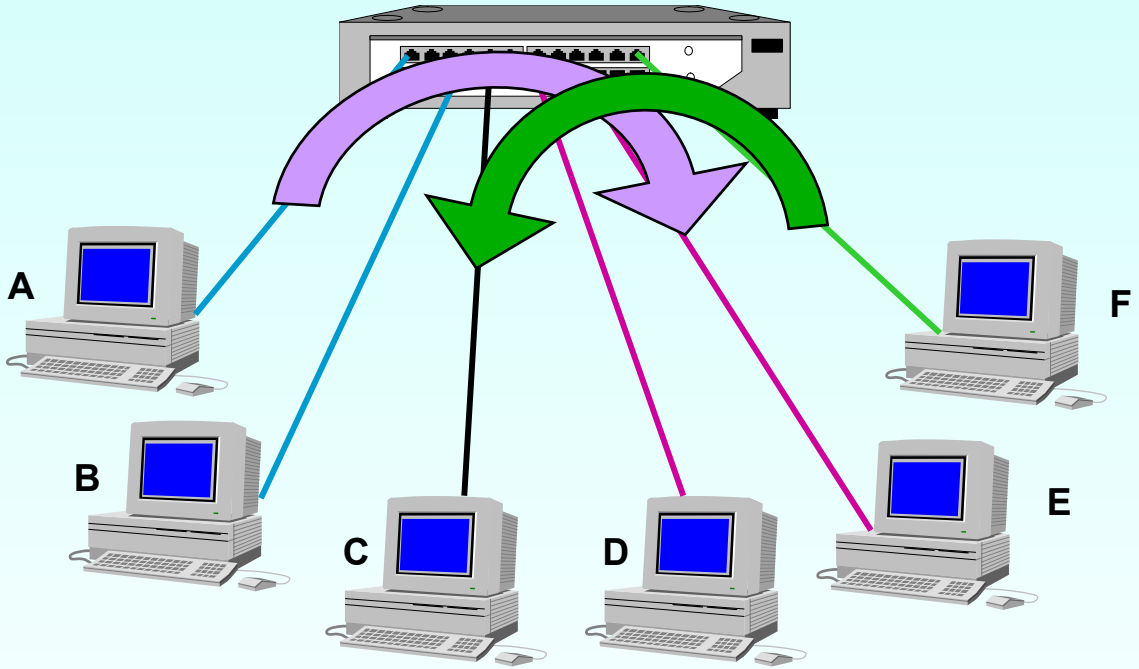
Network Access Layer - Ethernet (13)



TCP/IP

Network Access Layer - Ethernet (14)

- Tablica MAC adresa



Modul	Ulaz	MAC
1	1	A
4	3	E, G, H
2	3	F
3	5	C

TCP/IP

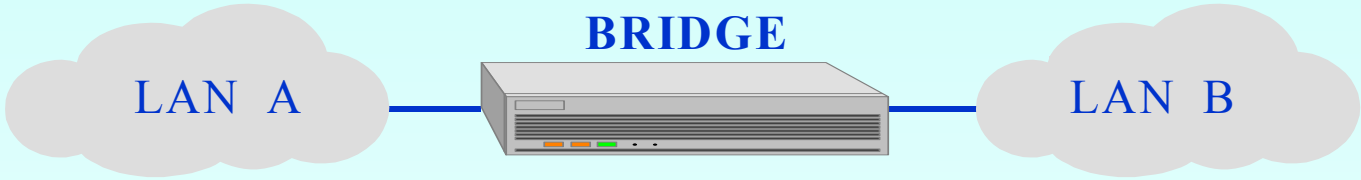
Network Access Layer - Ethernet (15)

- Osobine preklopnika:
  - kapacitet memorije MAC adresa
  - način preklapanja - *store and forward, cut-through, adaptive cut-through*
  - *Half duplex, Full duplex*
  - Autosense ulazi
  - brzina preklapanja - *packets per second* (pps)
  - mogućnost mrežnog upravljanja (SNMP, RMON)

TCP/IP

Network Access Layer - Ethernet (16)

- Premosnik - Bridge

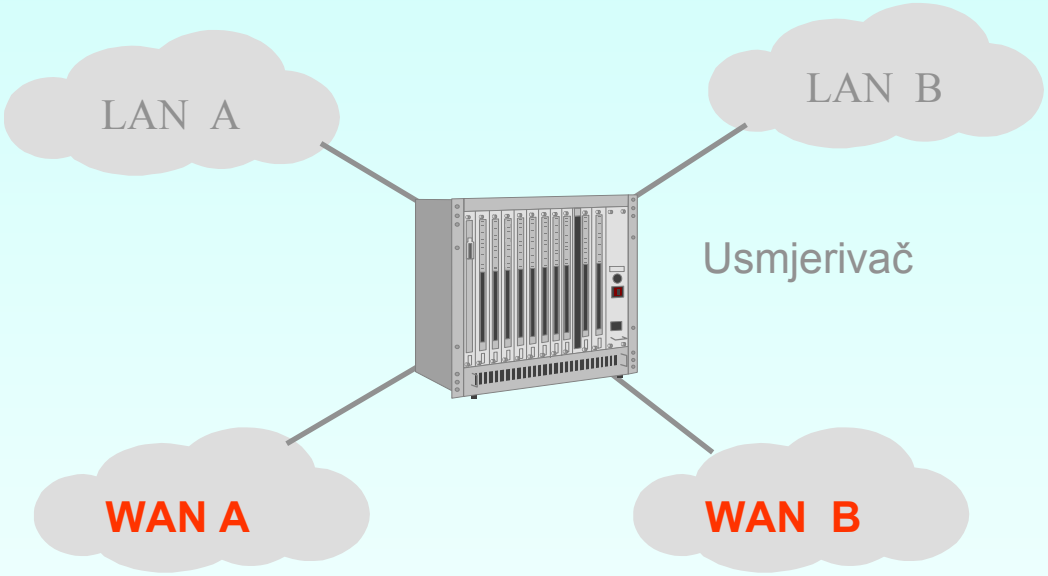


- povezuje dvije LAN mreže u jednu cjelinu
- funkcionira na razini MAC protokola
- separira mreže na toj razini
- ne prenosi kolizije i neispravne pakete
- povećava propusnost na oba segmenta
- prenosi *broadcast* i *multicast* poruke

TCP/IP

Network Access Layer - Ethernet (17)

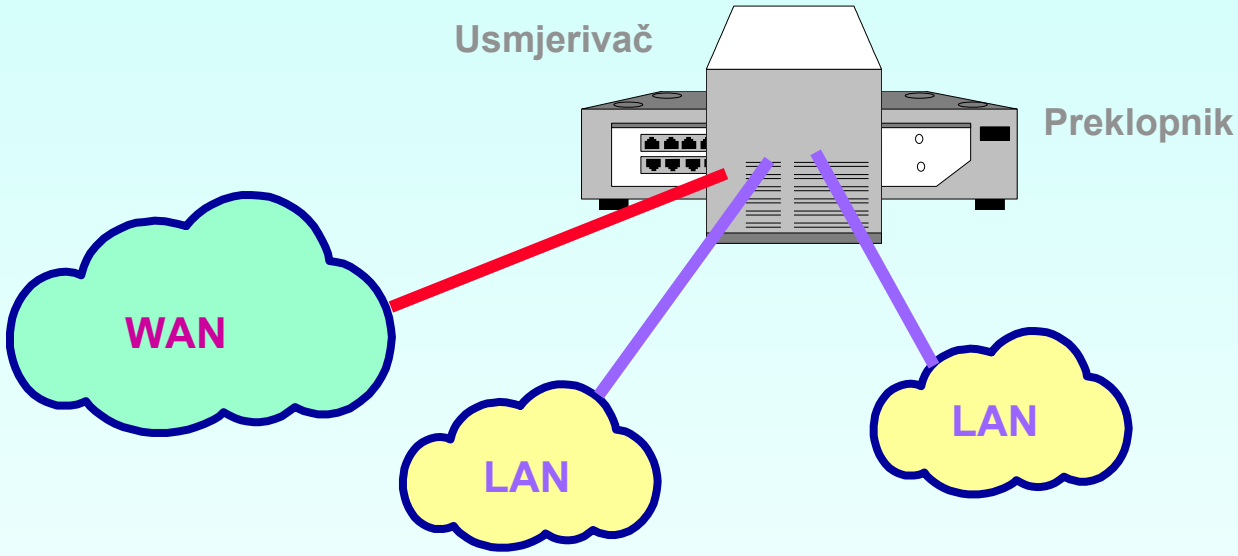
- Usmjerivač (*router*)



TCP/IP

Network Access Layer - Ethernet (18)

- Layer 3 preklopnici

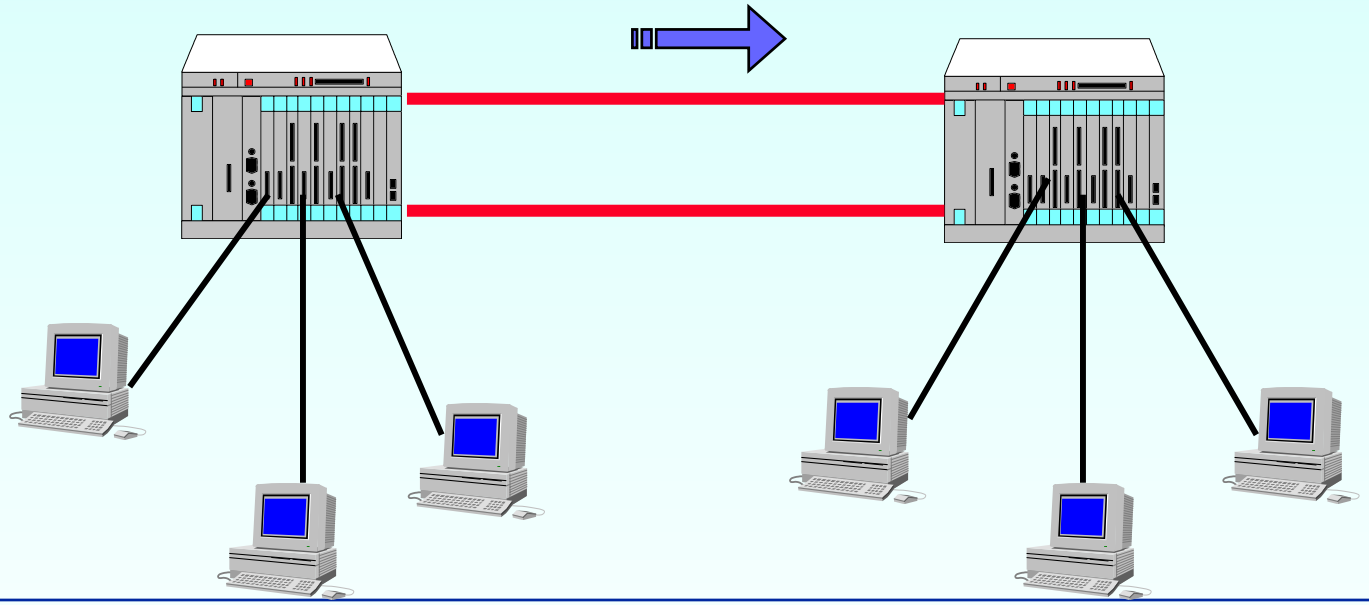


- funkcionalnost usmjerivača, brzina preklopnika

TCP/IP

Network Access Layer - Ethernet (19)

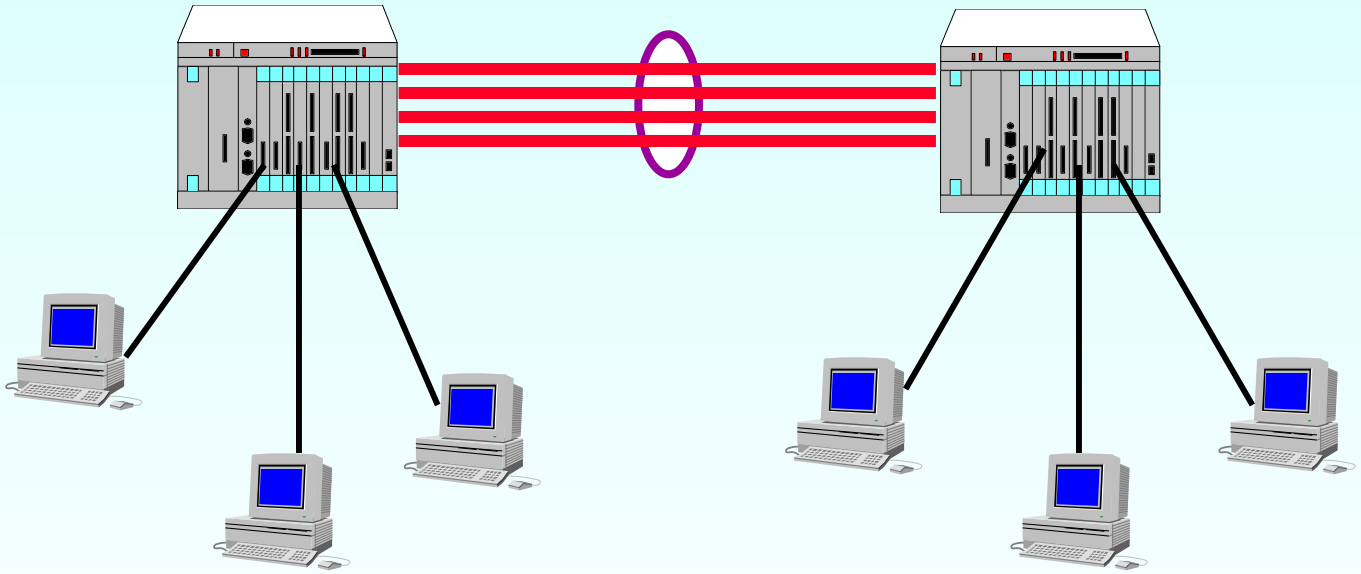
- Spanning tree
  - IEEE 802.1d
  - preklopnici razmjenjuju informacije o redundantnim vezama
  - aktivna je uvijek samo jedna (brža) veza



TCP/IP

Network Access Layer - Ethernet (20)

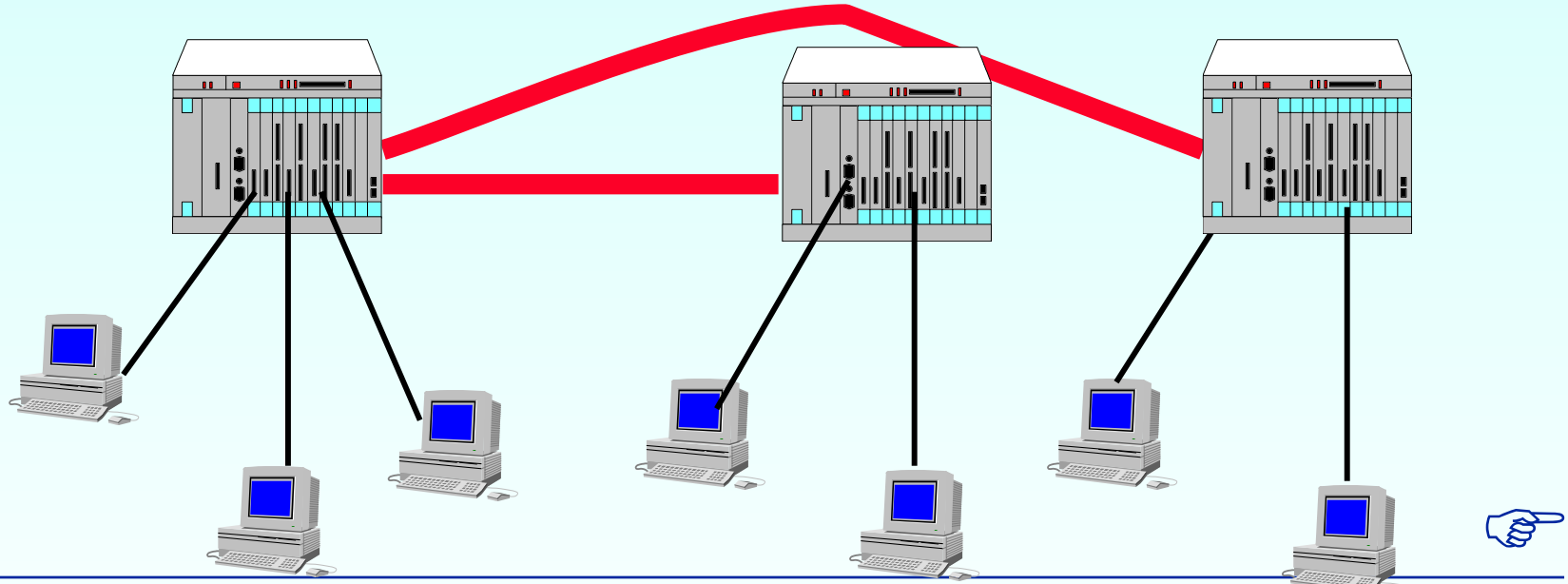
- Port (link) trunking (aggregation)
  - Multipliciranje kapaciteta veze između preklopnika



TCP/IP

Network Access Layer - Ethernet (21)

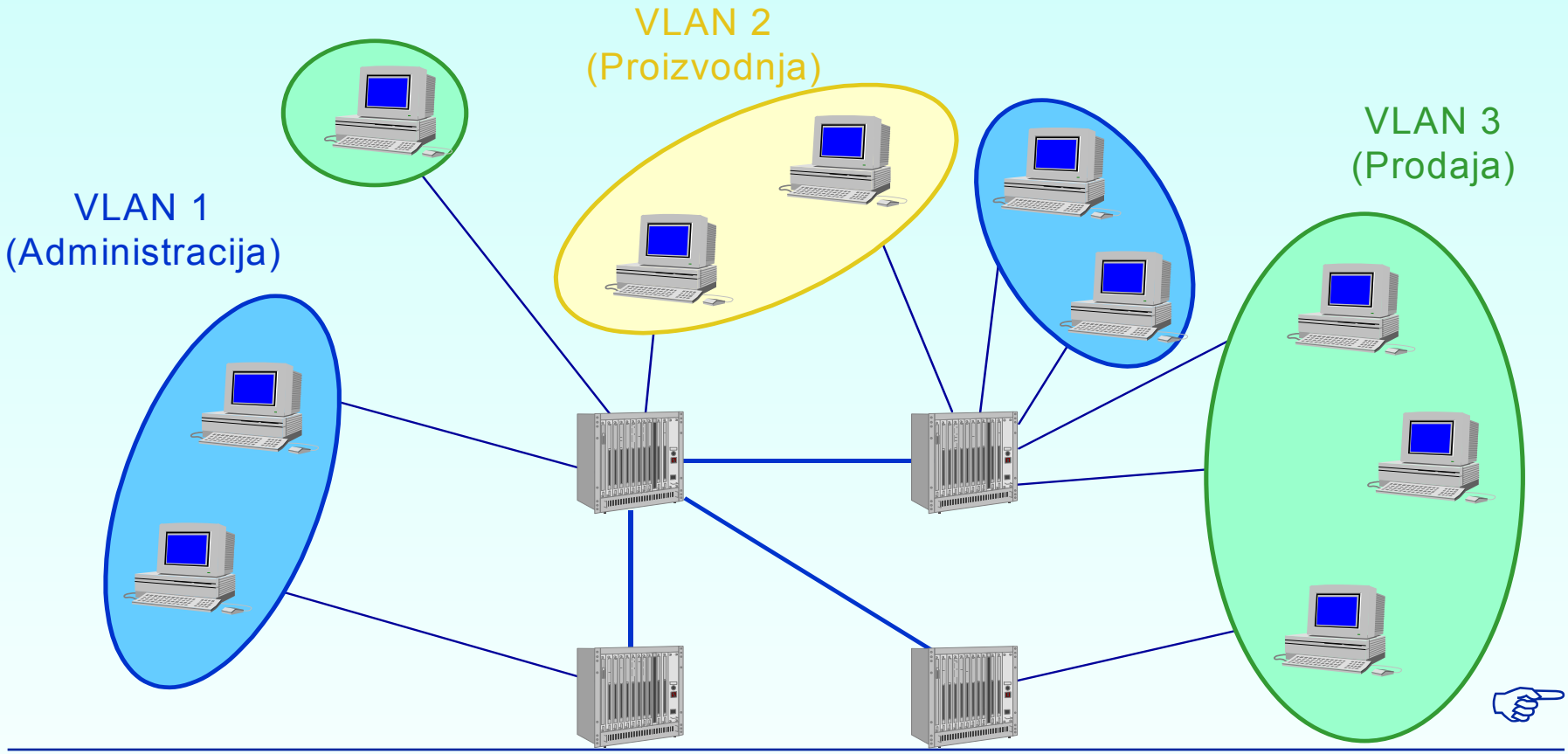
- Stack
  - Više preklopnika povezuje se posebnim kabelima
  - Mogu se promatrati i upravljati kao jedan preklopnik



TCP/IP

Network Access Layer - Ethernet (22)

- VLAN-ovi



TCP/IP

Network Access Layer - Ethernet (23)

- Ograničenje *broadcast* prometa na VLAN
- Povećana sigurnost mreže
- Povećane performanse mreže
- Olakšano održavanje (selidbe)
- Implementacije na OSI razinama 2 i 3
- Promet između VLAN-ova mora se *routati* (Layer 3 preklopnik ili usmjerivač)
- IEEE 802.1Q - VLAN *trunking*

TCP/IP

Network Access Layer - Ethernet (24)

- Povezivanje korisnika s određenom virtualnom LAN mrežom može se napraviti :
  - prema portovima preklopnika
  - prema MAC adresama
  - prema identifikatoru mrežne razine (IP adrese ili mrežni protokol)
  - prema korisnikovim identifikatorima (npr. lozinka)

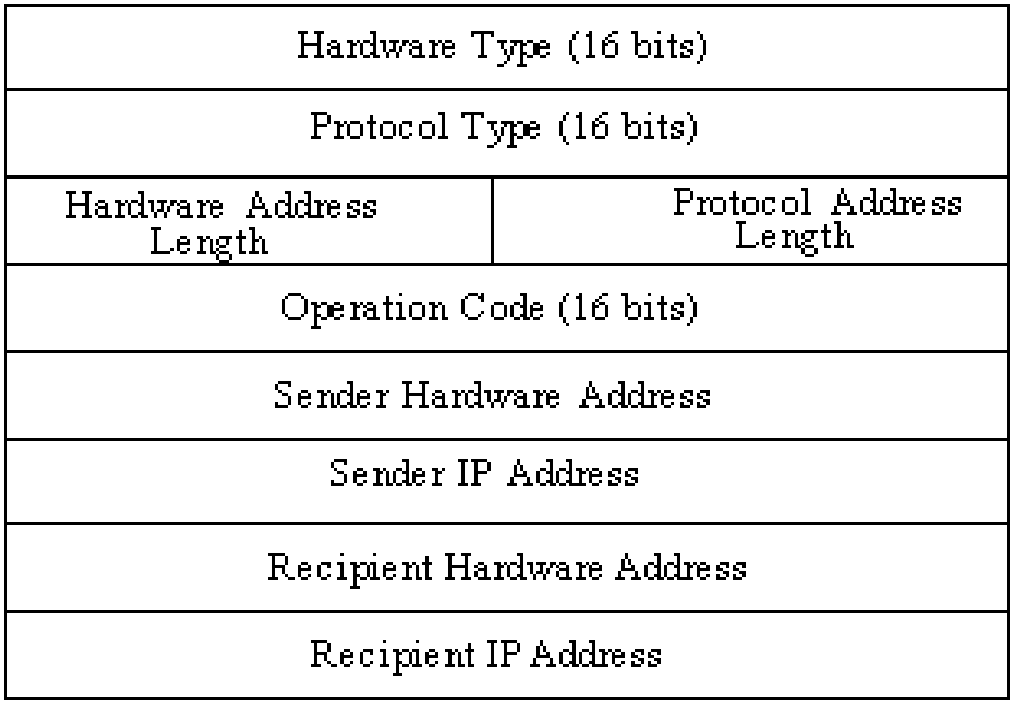
TCP/IP

Network Access Layer - ARP

- Address Resolution Protocol
- Prevođenje IP adresa u MAC adrese
- Pošiljalac mora znati fizičku (MAC) adresu primaoca
- Ako pošiljalac nema adresu u ARP *cacheu,* šalje *broadcast* u kojem traži MAC adresu za poznatu IP adresu
- Stanica koja ima traženu IP adresu odgovara svojom MAC adresom

TCP/IP

Network Access Layer - ARP (2)



TCP/IP

Network Access Layer - ARP (3)

- Osnovni oblik

```
% arp hostname
```

- Prošireni oblici

```
% arp -a
 arp -d hostname
 arp -s hostname ether_addr [temp][pub]
          [trail]
 arp -f filename
```

- Pomoć

```
% man arp
```

TCP/IP

Network Access Layer - ARP - vježbe

- Pregledati sve ARP zapise
- Pronaći MAC adresu za određenu IP adresu
  - 193.198.155.33, 193.198.155.53-58
- Izbrisati pojedine ARP zapise
- Kreirati ručno ARP zapise
- Kreirati *proxy* ARP zapise (*pub* opcija) za virtualna sučelja

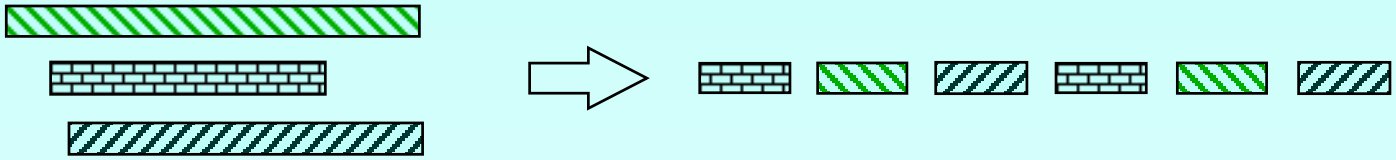
TCP/IP

Network Access Layer - ATM

- Na CARNet WAN mreži (okosnica) najviše se koristi ATM Layer 2 protokol
- Sučelje između Ethernet i ATM mreže je usmjerivač
- LAN Ethernet sučelje
- WAN ATM sučelje
- Usmjerivač šalje ATM ćelije prema ATM preklopnicima, koji čine okosnicu CARNet mreže

TCP/IP

Network Access Layer – ATM (2)



- Podaci se segmentiraju u pakete fiksne dužine 53 bytea - ćelije (engl. *cells*).
- ATM zahtijeva prethodno uspostavljanje spoja sugovornika (*engl. connection-oriented*).
- ATM je transparentan za sve tipove podataka - audio, video, računalni podaci ...
- Velik raspon brzina prijenosa, medija, područja primjene (LAN, WAN ...).

Sažetak

- TCP/IP, ISO/OSI mrežni model, aplikacijski sloj, Presentation, Session Layer
- Transport Layer, TCP, UDP, ICMP
- Internet Layer, adresiranje, sučelja, usmjeravanje, routeri, IP datagram, IPv6
- Network Access Layer, Ethernet, MAC adresa, preklopnici, koncentratori, topologija, ARP, ATM

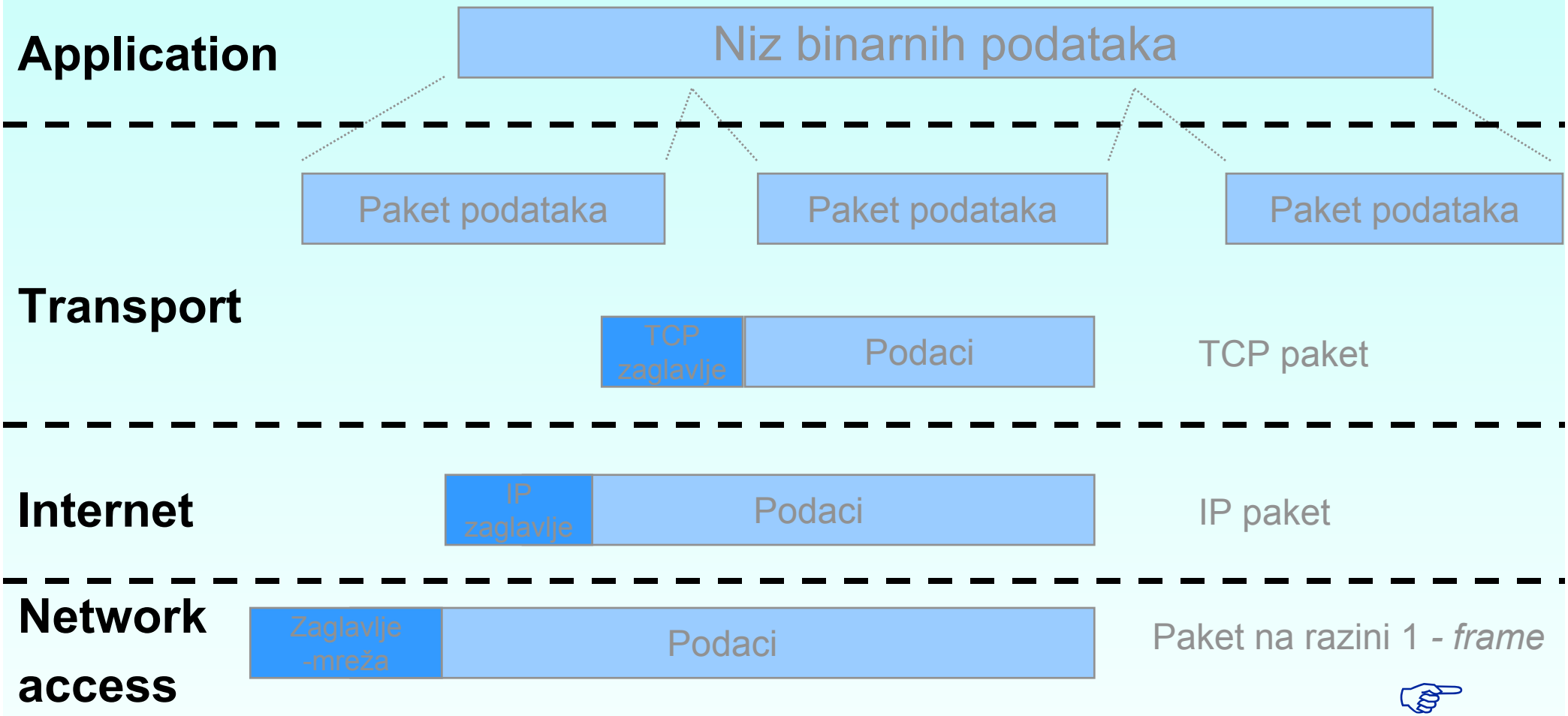
Literatura

- Knjige:
  - **Douglas E. Comer, David L. Stevens: "Internetworking with TCP/IP, Design, Implementation, and Intranets"**, Volume II, Prentice Hall, 1991.
- RFC standardi – 791, 793, 1180, 1146, 1072, 1693, 1827, 1883, 826...
- Internet

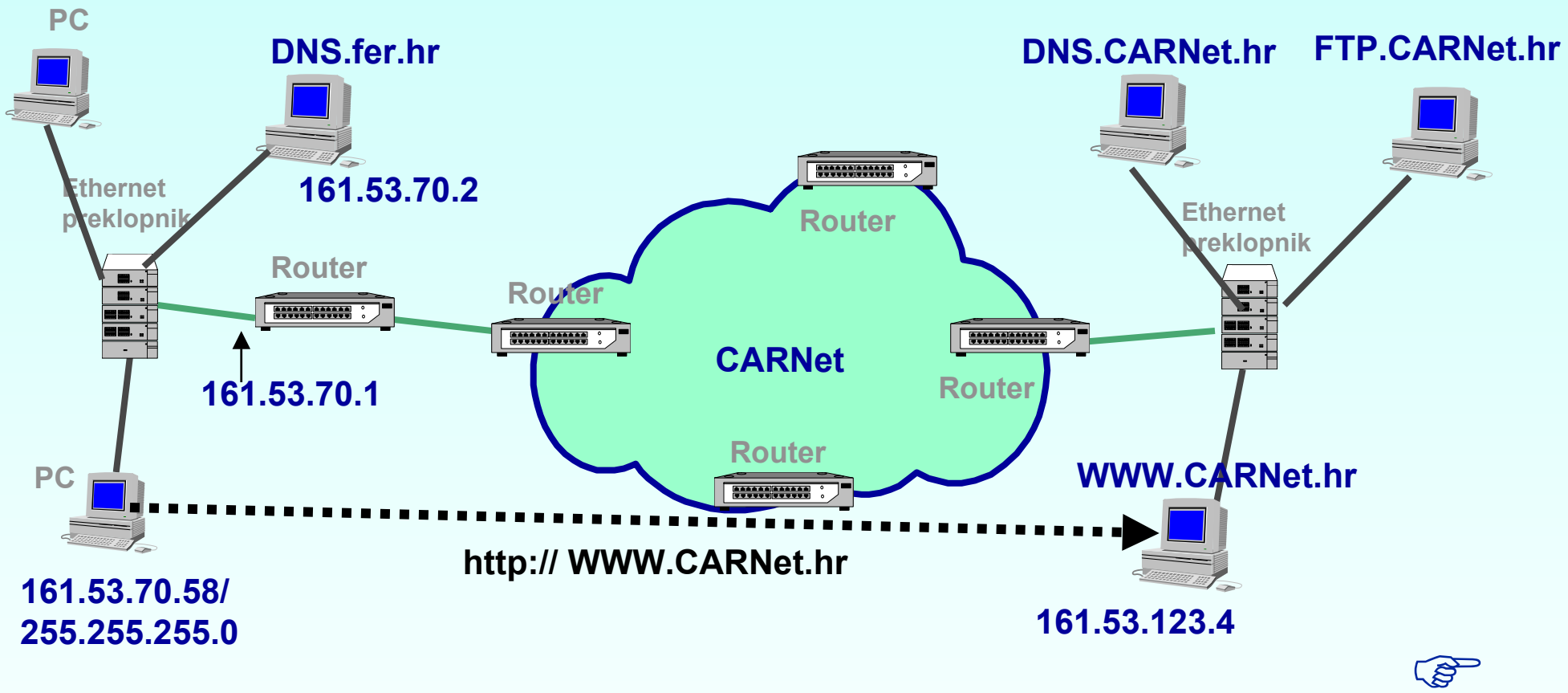
Sadržaj (2. dan)

TCP/IP - Komunikacija	35 min
Strukturno kabliranje - Bakreni kabeli, optički kabeli, općenito, arhitektura i terminologija, komponente, dimenzije, generičko kabliranje, zasićeno kabliranje, zaštita investicije	20 min
CARNet - Odnos CARNet – ustanova, veza CARNet – ustanova, CARNet oprema, primjer: LAN FER, adresiranje	20 min
Imena - Struktura dodjele imena, FQDN, hosts datoteka, DNS, lokalno razlučivanje, uloga u CARNet mreži	160 min
Sigurnost - DoS, DDoS	30 min

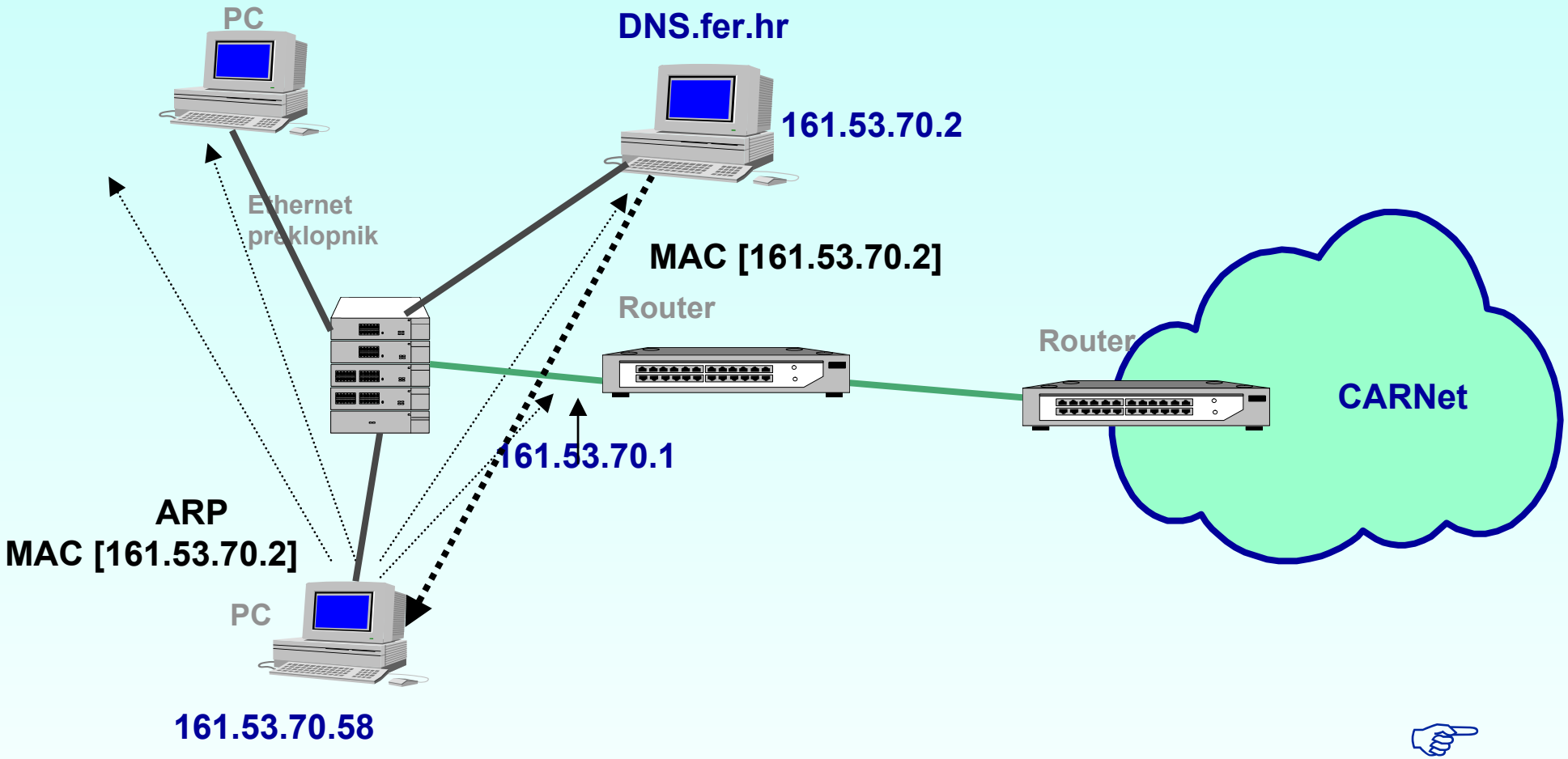
TCP/IP
Komunikacija



TCP/IP
Komunikacija (2)

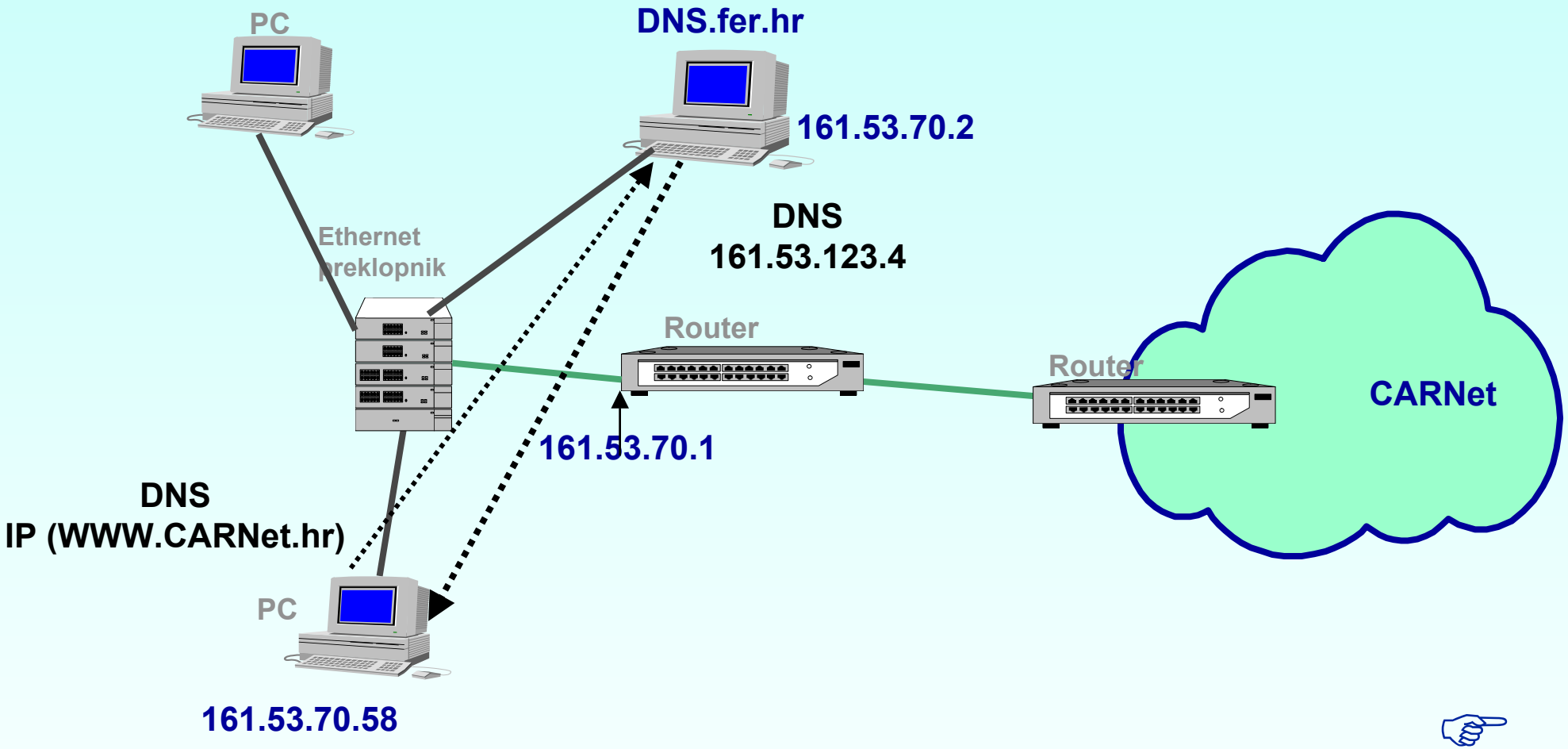


TCP/IP
Komunikacija (3)



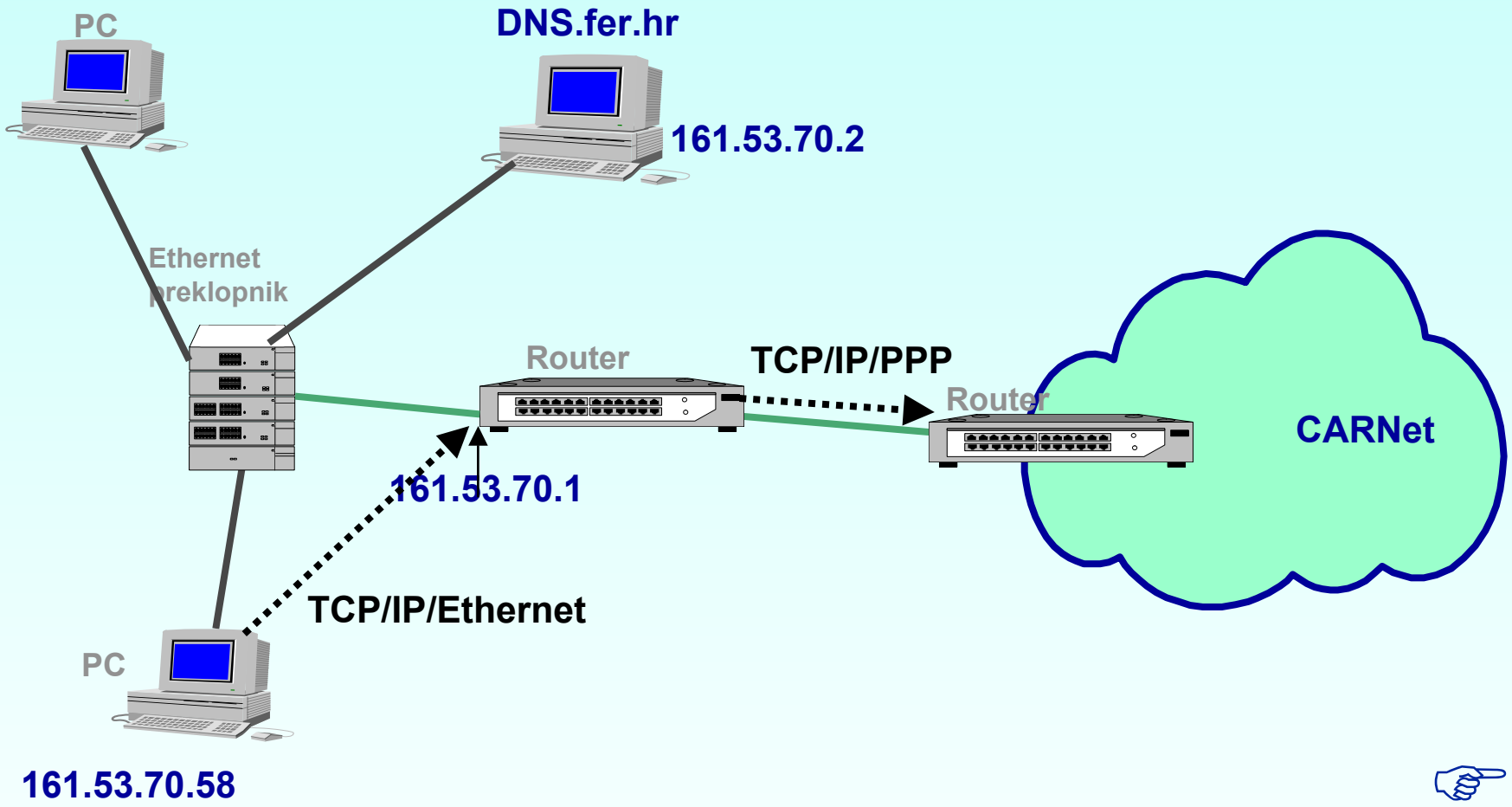
TCP/IP

Komunikacija (4)



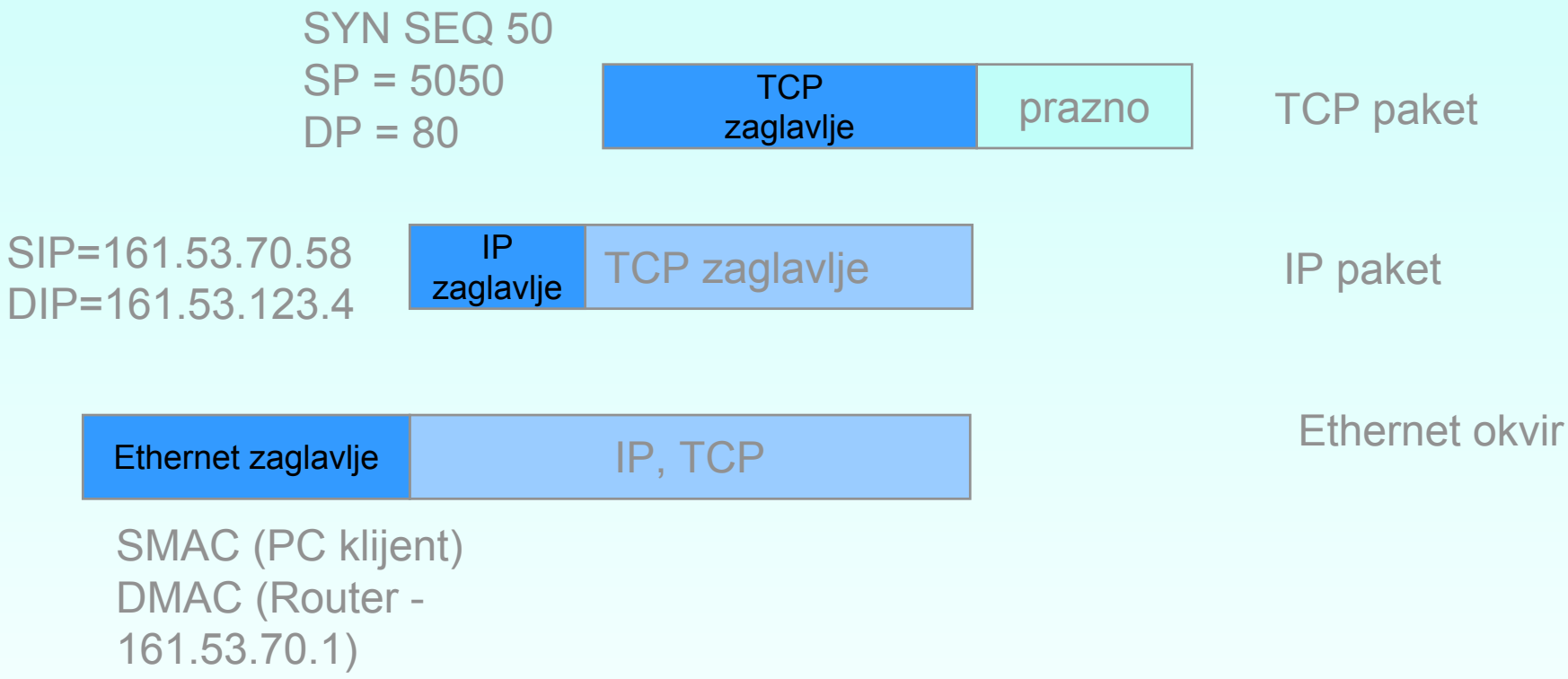
TCP/IP

Komunikacija (5)



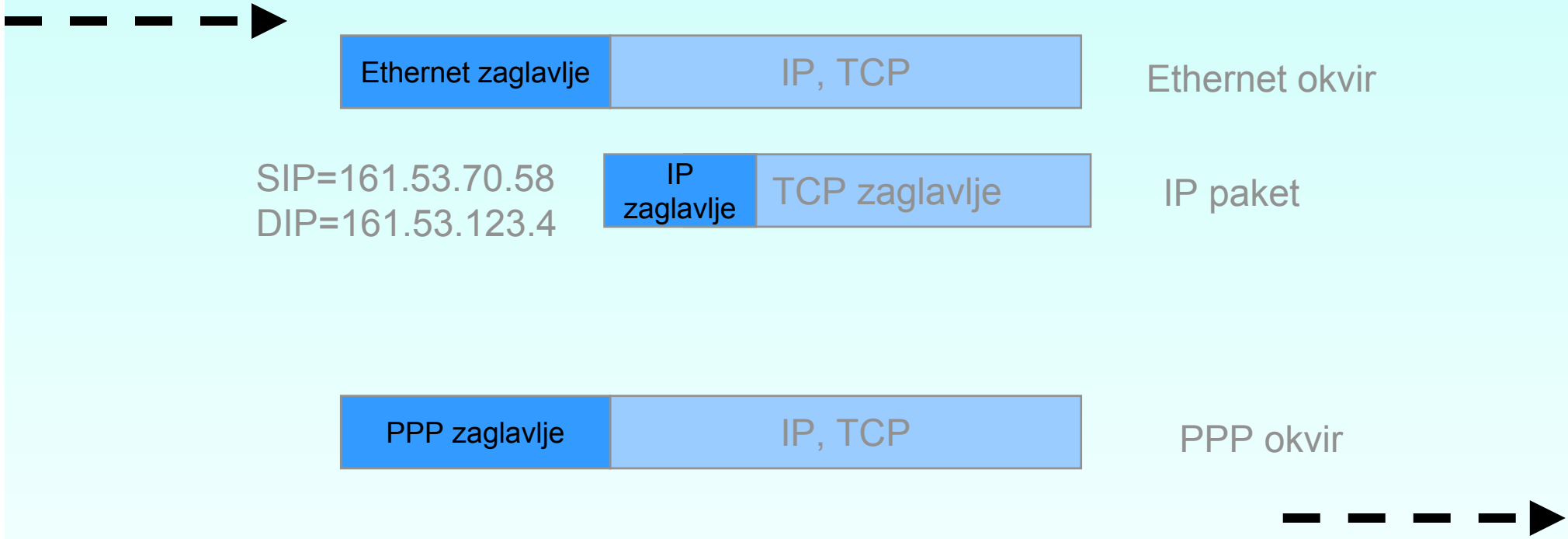
TCP/IP
Komunikacija (6)

- PC klijent - slaganje paketa

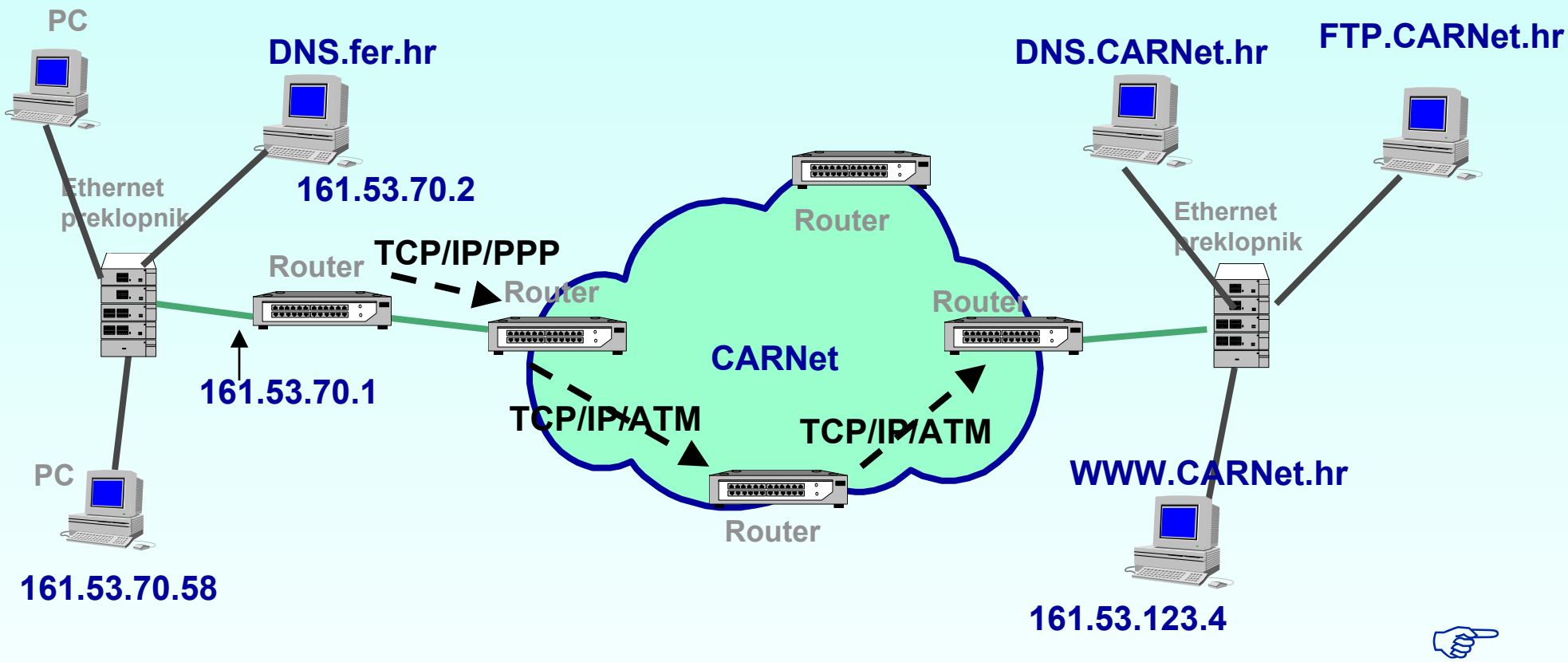


TCP/IP
Komunikacija (7)

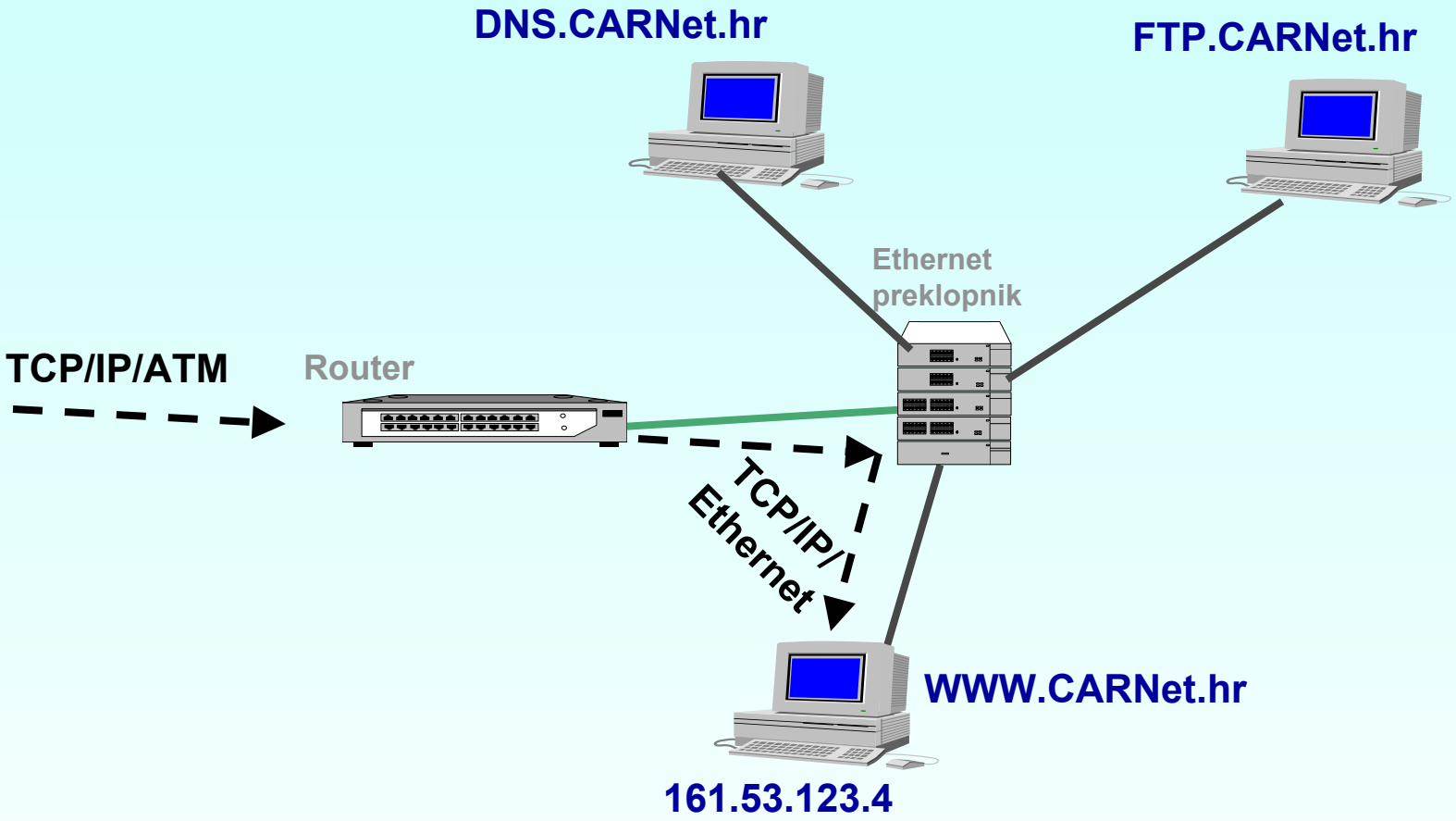
- Router - procesiranje paketa



TCP/IP
Komunikacija (8)

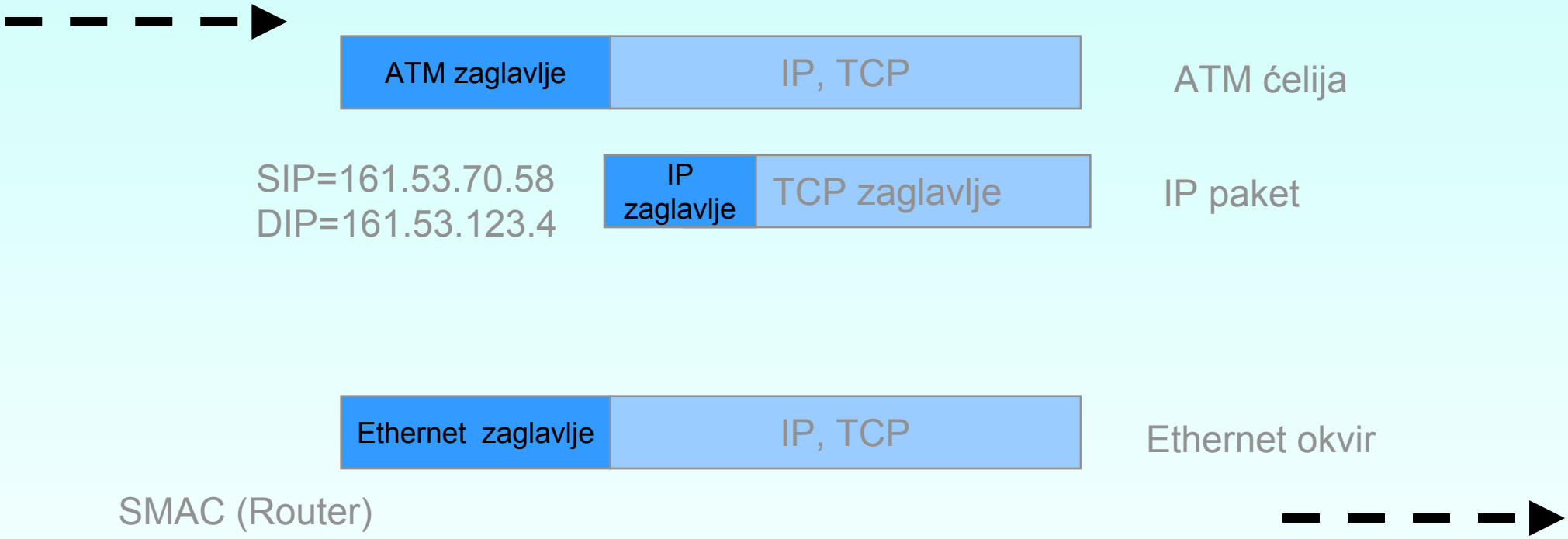


TCP/IP
Komunikacija (9)



TCP/IP
Komunikacija (10)

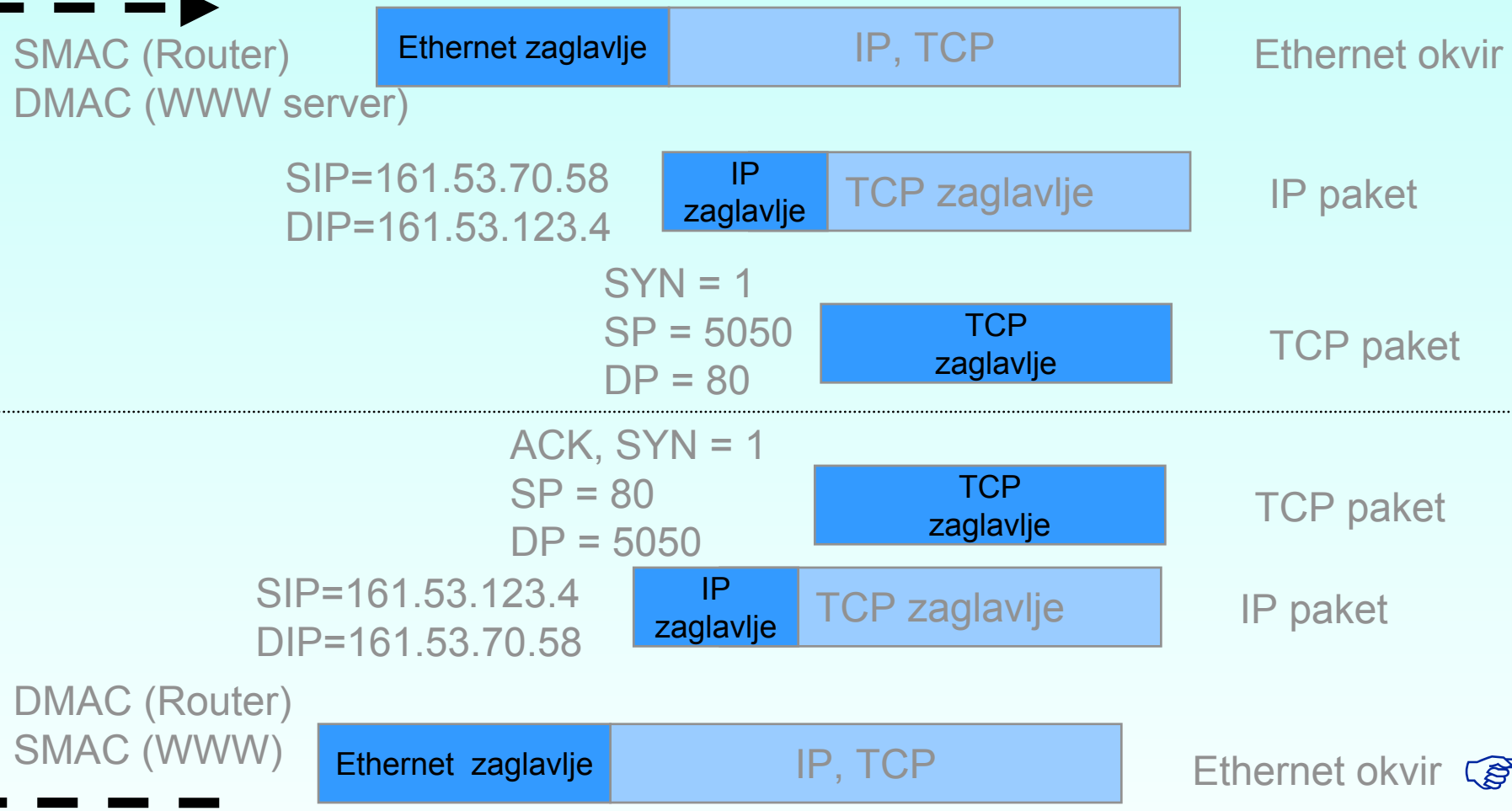
- *Router* - procesiranje paketa



TCP/IP

Komunikacija (11)

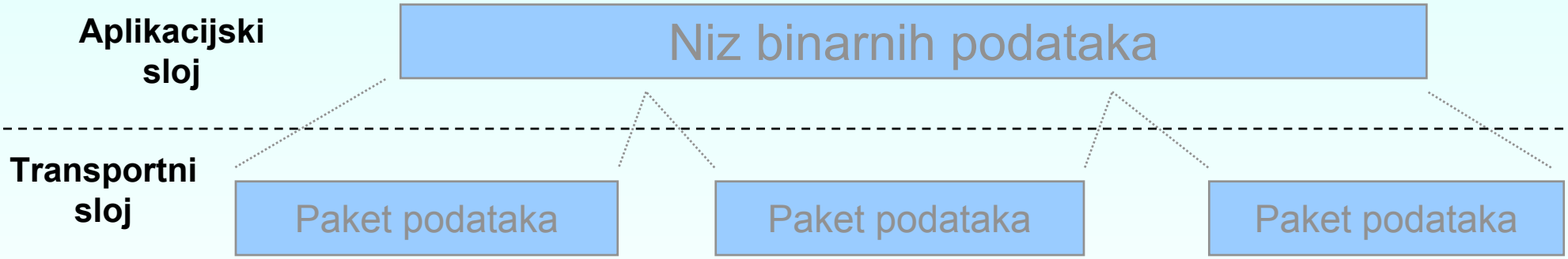
- WWW server - procesiranje paketa



TCP/IP

Komunikacija (12)

- Paket kojeg server šalje klijentu putuje na istovjetan način prema klijentu
- Sve je isto i za obične pakete s podacima, samo s viših slojeva stiže niz bitova (podaci), koje TCP segmentira, dodaje svoje zaglavlje...

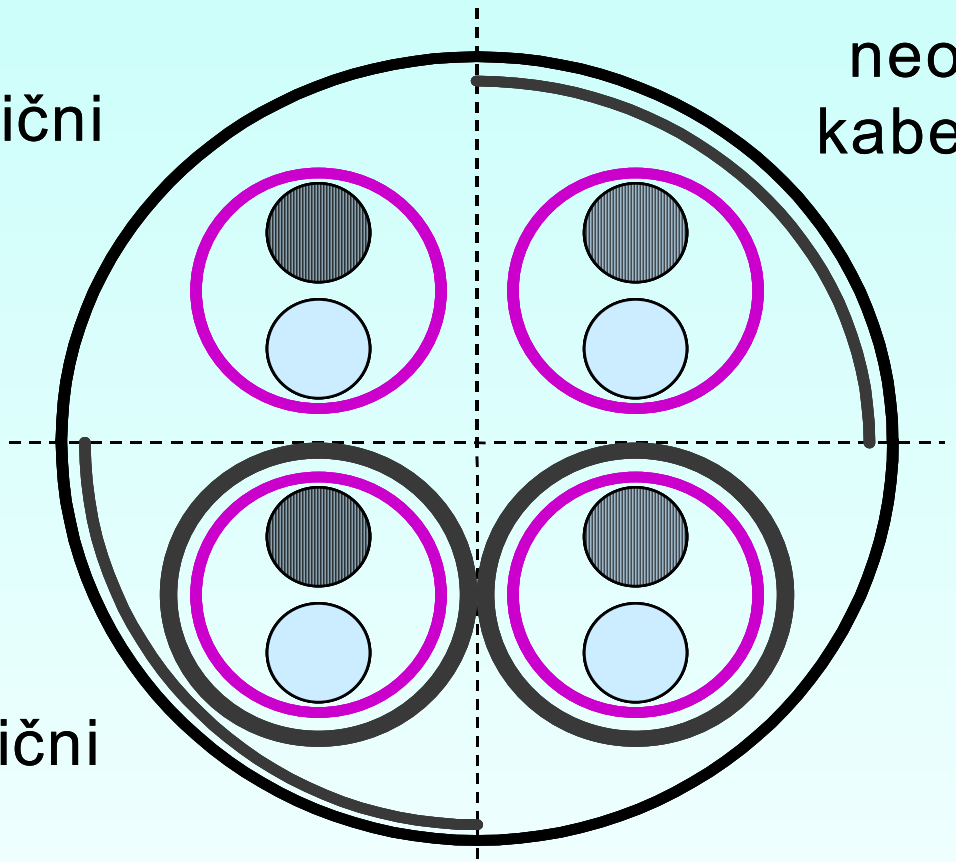


Strukturno kabliranje

Bakreni kabeli

neoklopljeni parični kabeli
UTP

neoklopljeni parični kabeli sa zajedničkim oklopom
S/UTP, FTP

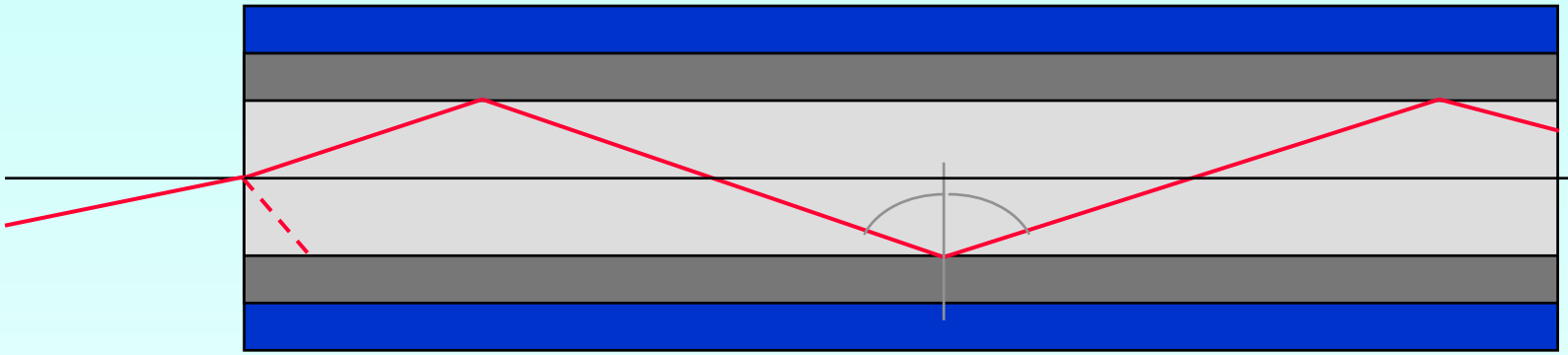


oklopljeni parični kabeli sa zajedničkom oklopom
STP

oklopljeni parični kabeli

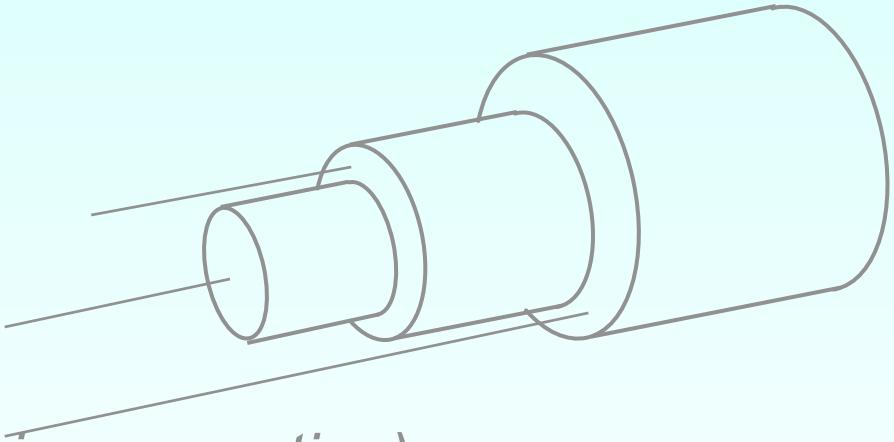
Strukturno kabliranje

Optički kabeli



n_1=1,48

n_2=1,46



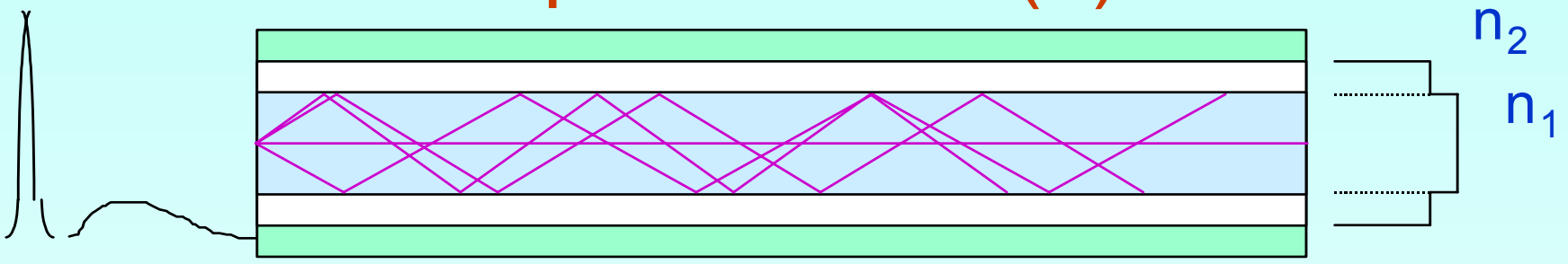
plašt (*engl. cladding*), n_2

jezgra (*engl. core),* n_1

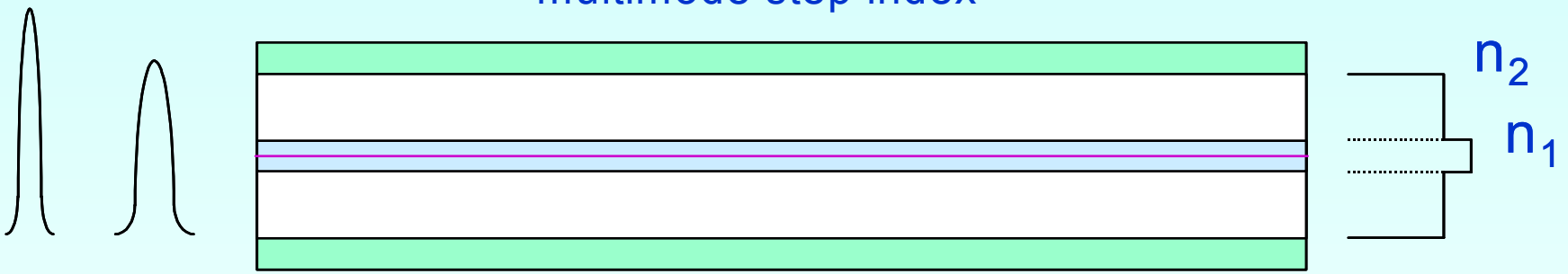
primarni omotač (*engl. primary coating)*

Strukturno kabliranje

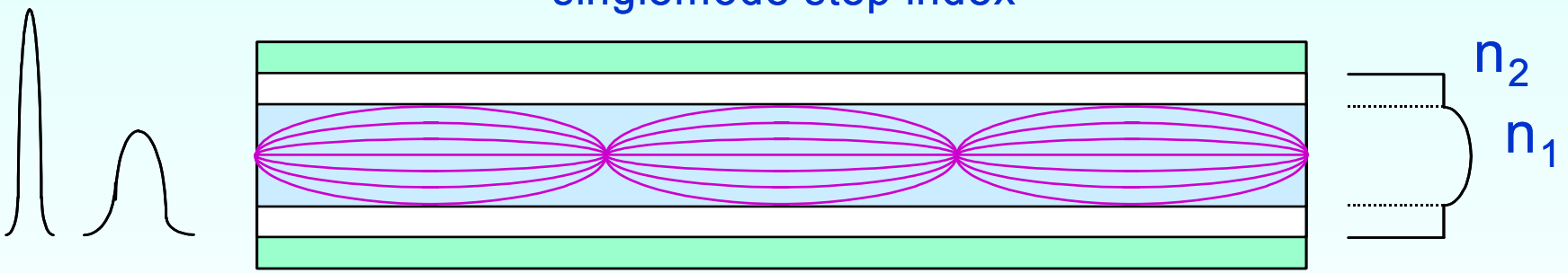
Optički kabeli (2)



multimode step index



singlemode step index



multimode graded index

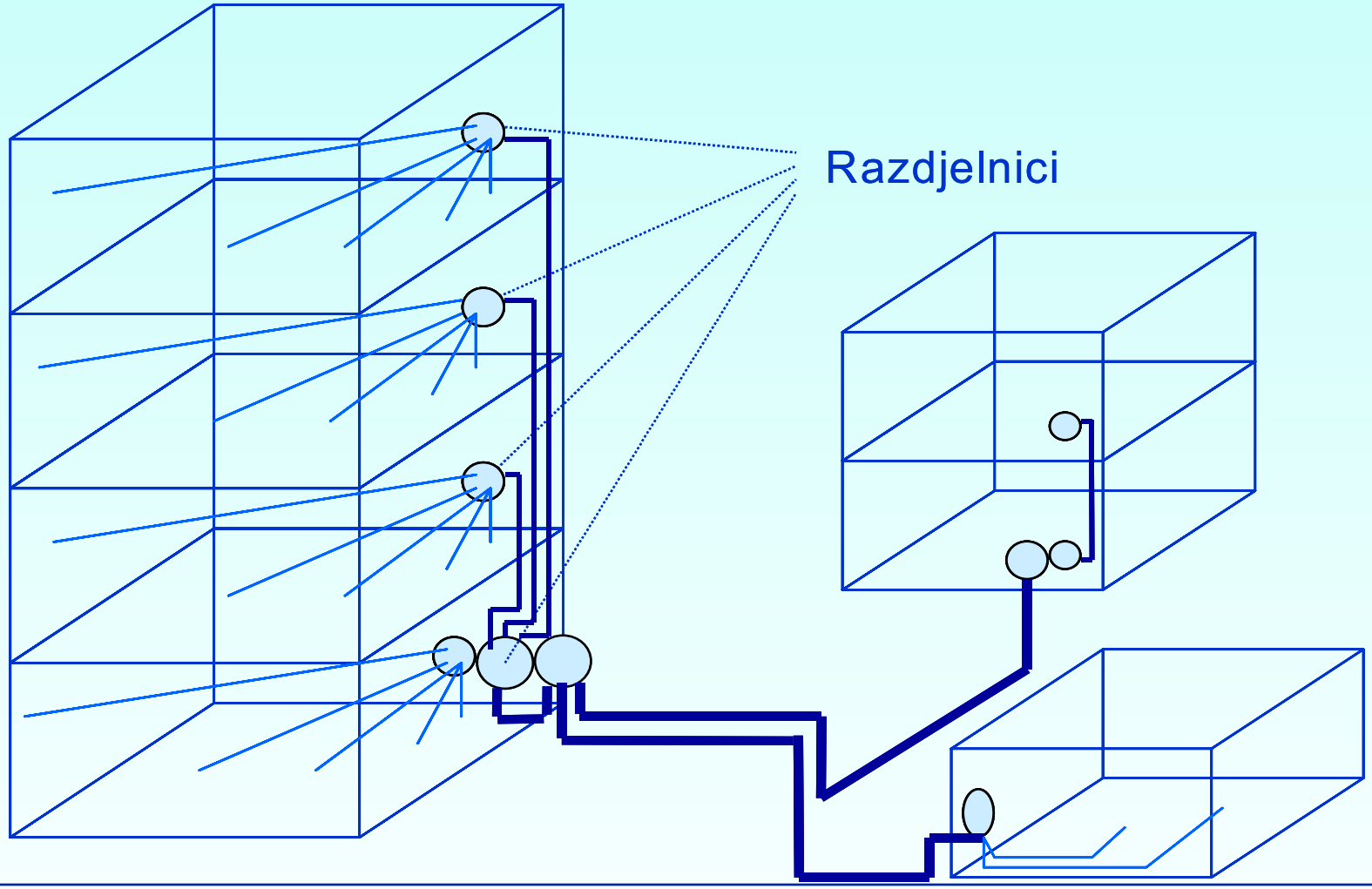
Strukturno kabliranje

Općenito

- Kabliranje računalnih mreža mora se smatrati dijelom zgrade isto kao i instalacije rasvjete i napajanja, grijanja ili telefonije!
- Raditi strukturno, a ne namjensko kabliranje
- Zajedničko kabliranje za računalnu i telefonsku mrežu
- Standardi i norme ISO11801, EIA/TIA568B, EN 50173...

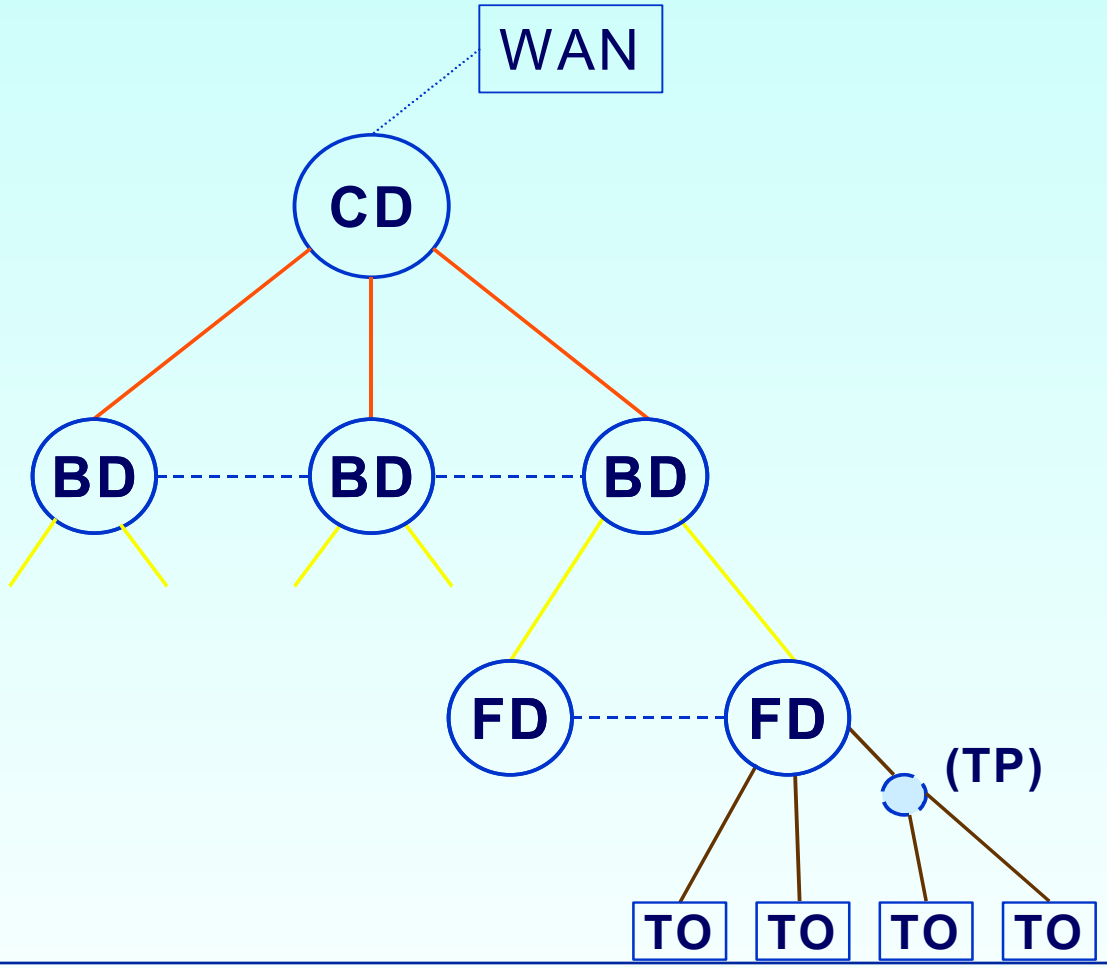
Strukturno kabliranje

Struktura



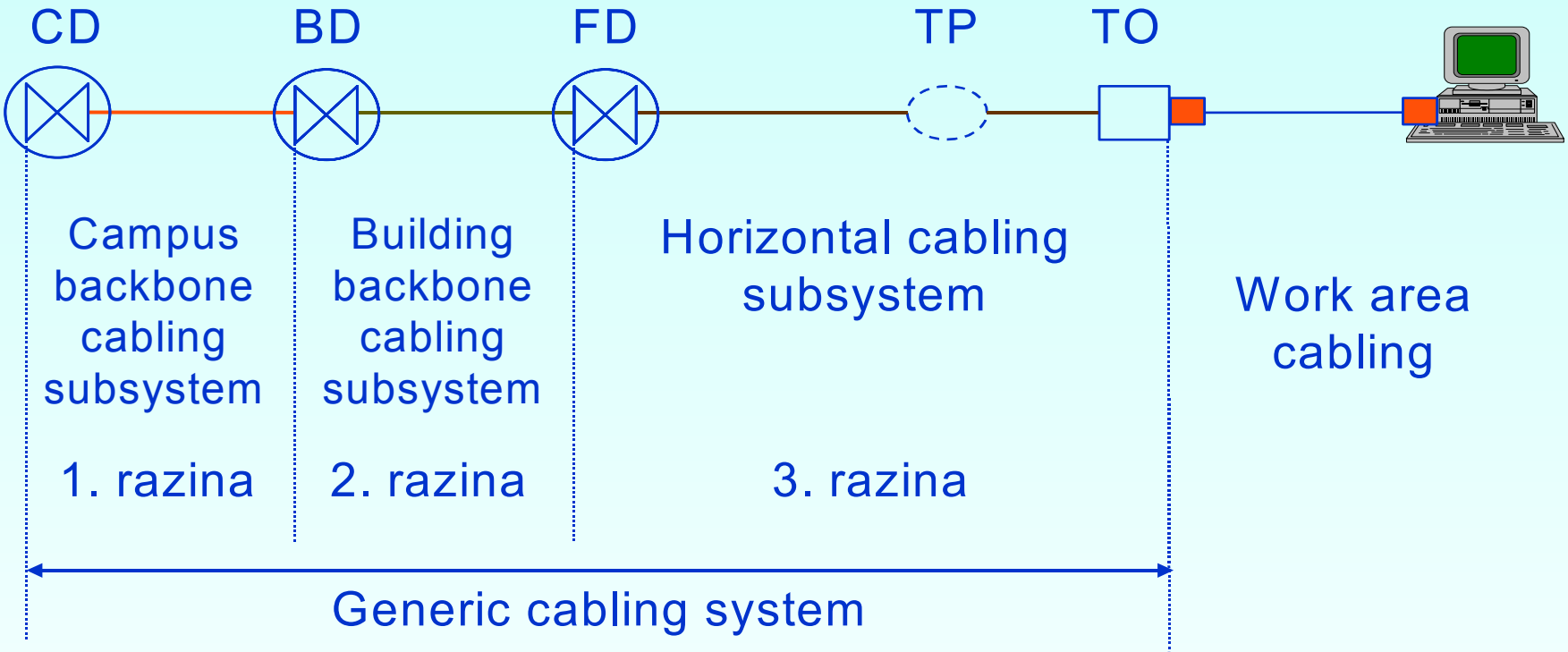
Strukturno kabliranje

Arhitektura i terminologija



Strukturno kabliranje

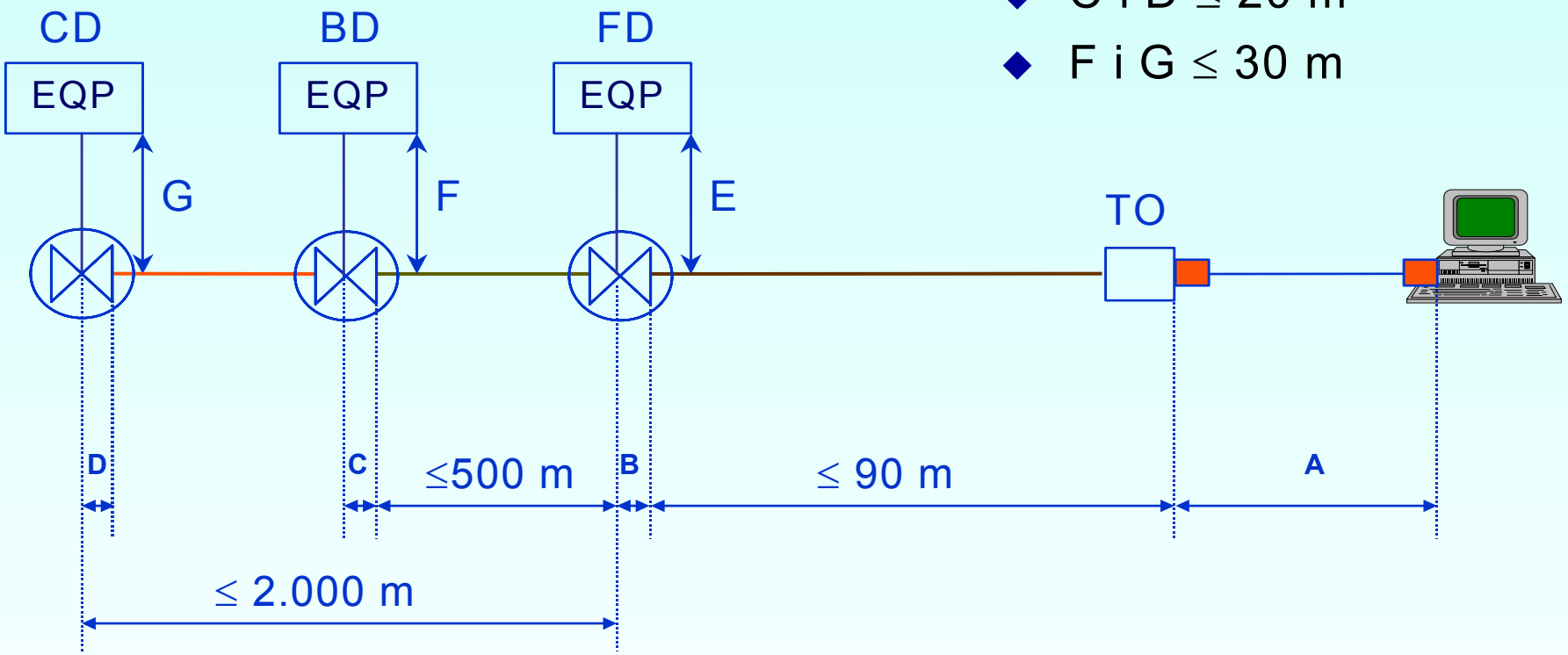
Komponente



Strukturno kabliranje

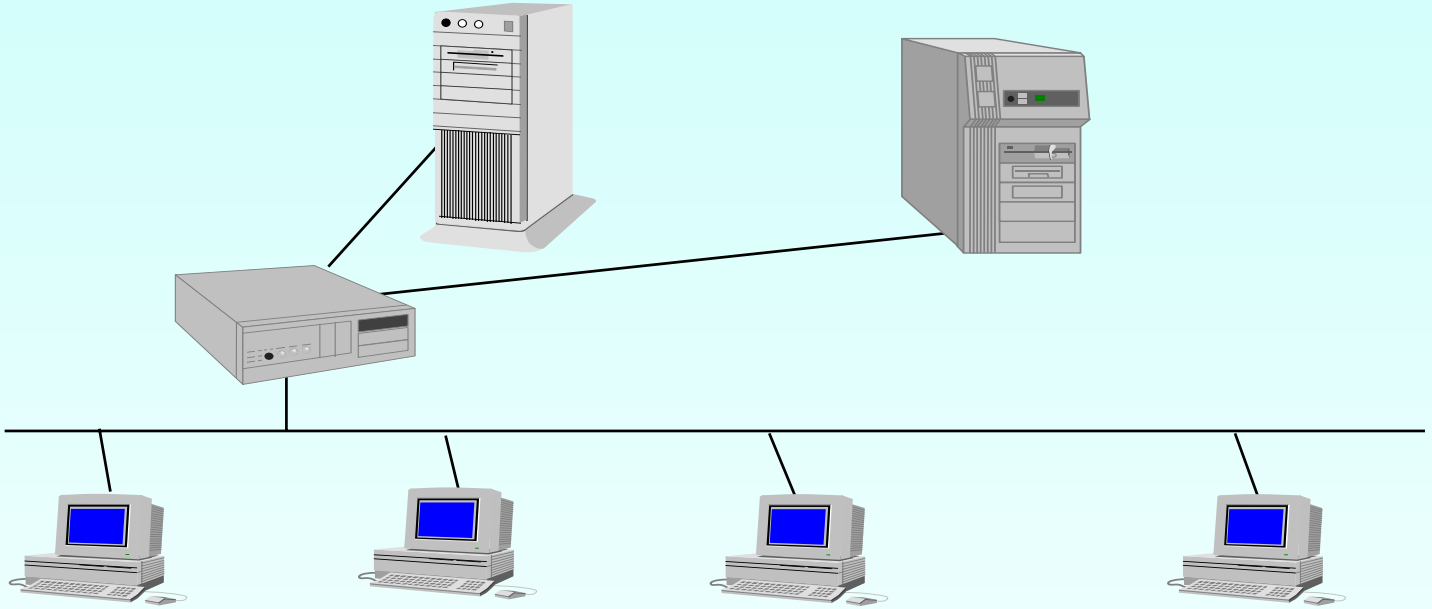
Dimenzije

- A+B+E ≤ 10 m
- C i D ≤ 20 m
- F i G ≤ 30 m



Strukturno kabliranje

Generičko kabliranje



- Različite tehnologije, ISTI kabeli!

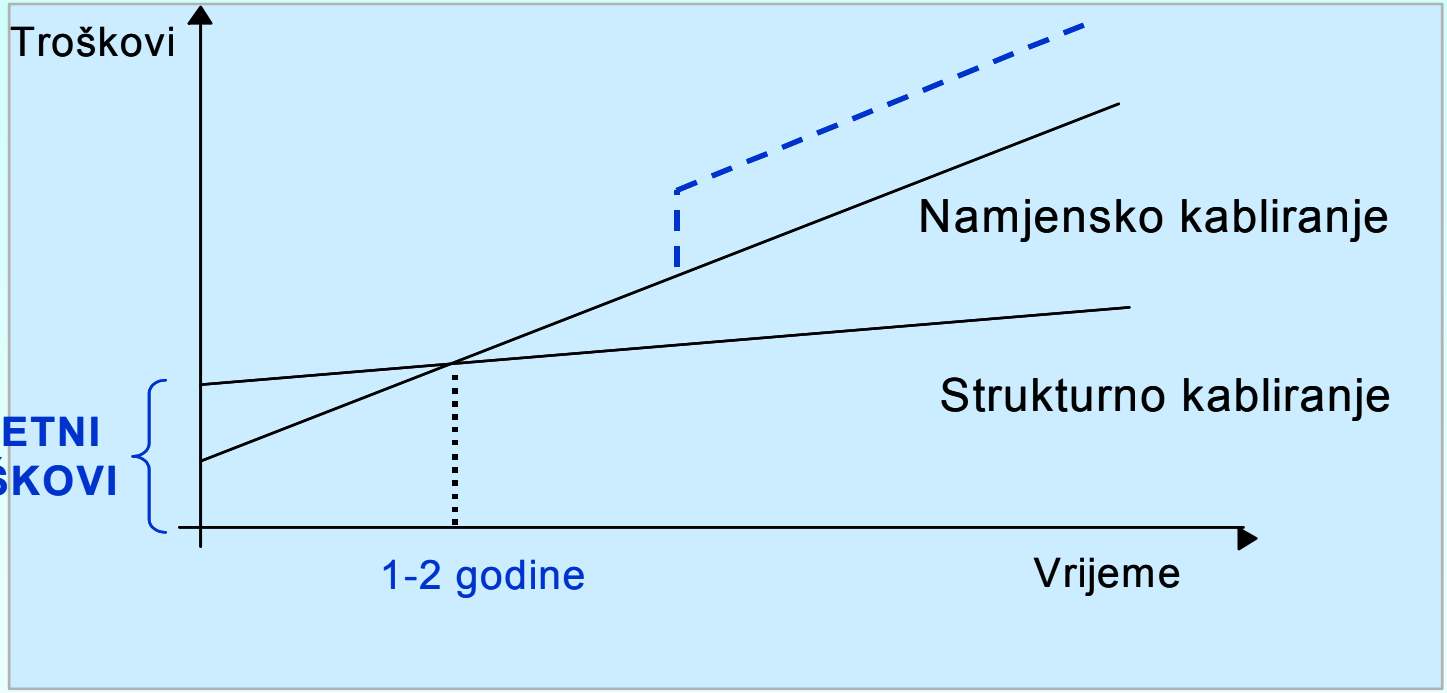
Strukturno kabliranje

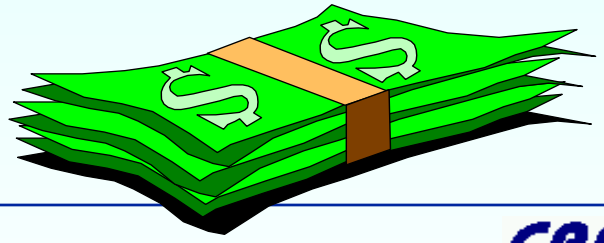
Zasićeno kabliranje

- Min. dva priključna mjesta na 10m^2 uredskog prostora
- Prosječna površina radnog mjesta – 6m^2
- Preporučena gustoća priključnih mjesta – 4m^2
- Dva priključka (RJ45) po priključnom mjestu

Strukturno kabliranje

Zaštita investicije





CARNet
Odnos CARNet - ustanova

- Tri kategorije članica CARNeta:
  - punopravne članice
  - pridružene članice
  - privremene članice
- “Naputak o stjecanju statusa i pravima korisnika CARNeta” (Min. znanosti)
- WWW.CARNet.hr/ustanova/clanice/spajanje.html

CARNet
Odnos CARNet - ustanova (2)

- CARNet najčešće osigurava uređaje za vezu na CARNet i samu vezu
- Za privremene članice osigurava se pristupna točka u CARNet mrežu
- Strukturno kabliranje, pasivnu i aktivnu opremu lokalne računalne i telefonske mreže osigurava sama ustanova (Min. znanosti)
  - u nekim slučajevima je i dio LAN opreme CARNetov

CARNet

Veza CARNet - ustanova

- ATM 155 ili 622 Mbit/s (velike ustanove, jezgra CARNet mreže)
- Unajmljene digitalne 2 Mbit/s komunikacijske linije
- MAN Ethernet veze 10, 100 Mbit/s, 1 Gbit/s
- Unajmljene bakrene parice do 2 Mbit/s
- Otvorene tel. linije do 56 kbit/s
- Bežične veze do 11 Mbit/s

CARNet
CARNet oprema

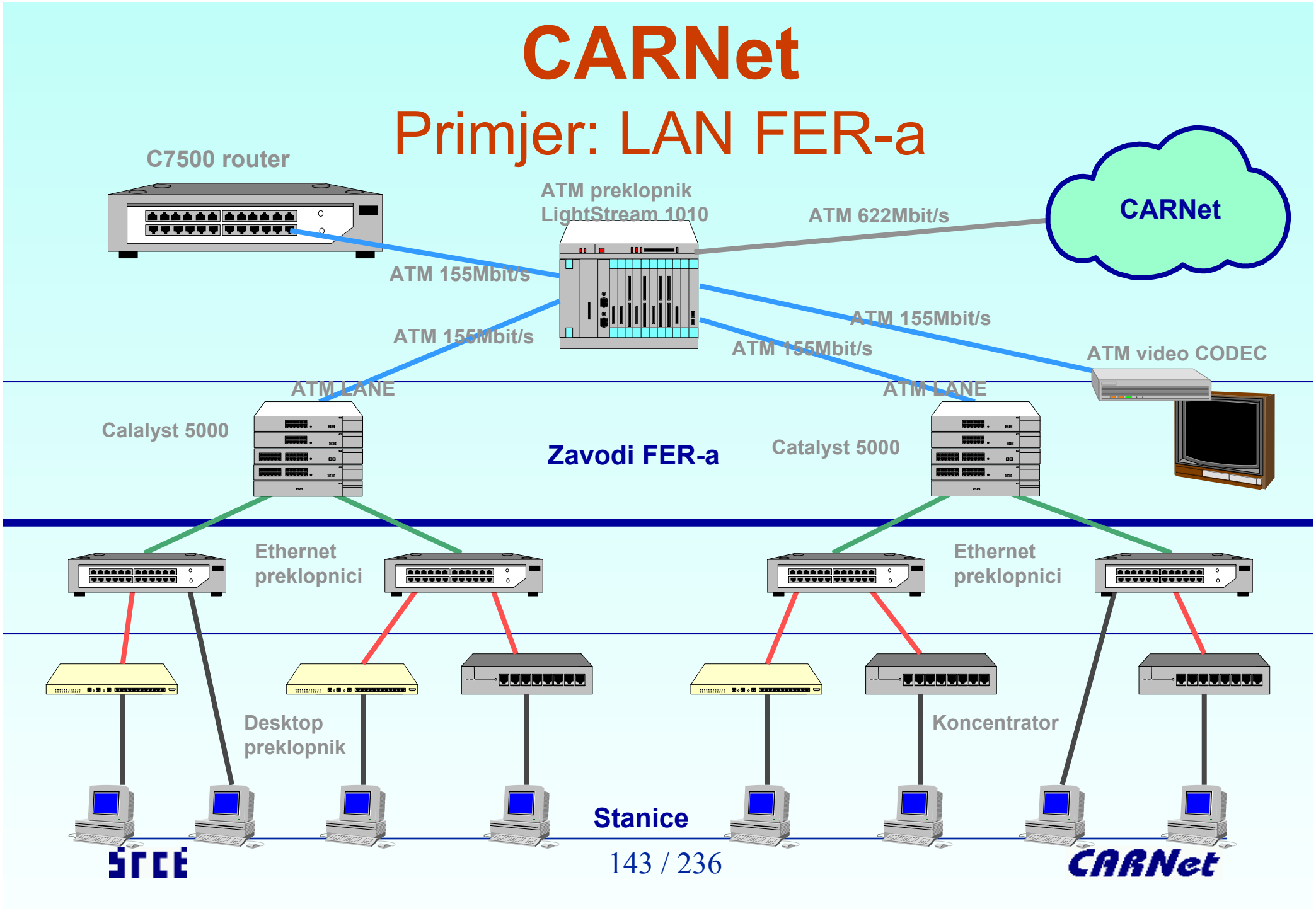
- Velike ustanove
  - ATM preklopnik (Cisco LightStream 1010)
  - usmjerivač s ATM sučeljem (najčešće Cisco 7500, 7200, 4700)
  - modemski pristupni poslužitelj
- Ostale ustanove
  - usmjerivač s Ethernet i serijskim sučeljem
  - pristupni uređaj (modem, CSU/DSU)
- Bežične veze
  - LAN bridge (IEEE 802.11b)

CARNet
CARNet oprema (2)

- Ustanove s 2Mbit/s digitalnom vezom dobivaju i HP Procurve 12 portni 10/100 Mbit/s *switch*
- U nekim ustanovama - računalni poslužitelji i dodatna mrežna oprema - preklopnici (Cisco Catalyst 5000…)
- Oprema za ostvarivanje video konferencija na ATM mreži
  - ATM videokoder/dekoder K-NET CellStack
- Svu CARNetovu opremu održava CARNet

CARNet

Primjer: LAN FER-a



CARNet
Adresiranje

- Svaka ustanova, prema iskazanim stvarnim potrebama, dobiva javne IP adrese iz raspodjele B ili C klase:
  - 161.53.X.X (B klasa)
  - 193.198.1.X - 193.198.254.X (254 C klase)
- Ustanova administrativno i tehnički upravlja dodijeljenim adresnim prostorom

CARNet
Adresiranje (2)

- Preporuka raspodjele adresa za C klasu:
  - 161.53.70.1 - *gateway* - LAN sučelje lokalnog usmjerivača
  - 161.53.70.2 - CARNet LAN oprema
  - 161.53.70.3-4 - primarni i sekundarni DNS poslužitelj
  - 161.53.70.4-10 - poslužitelji (E-mail, WWW, NT…)
  - 161.53.70.11-20 - aktivna mrežna oprema
  - 161.53.70.21-30 - modemski poslužitelj
  - 161.53.70.31-254 - računala (*hosts*)

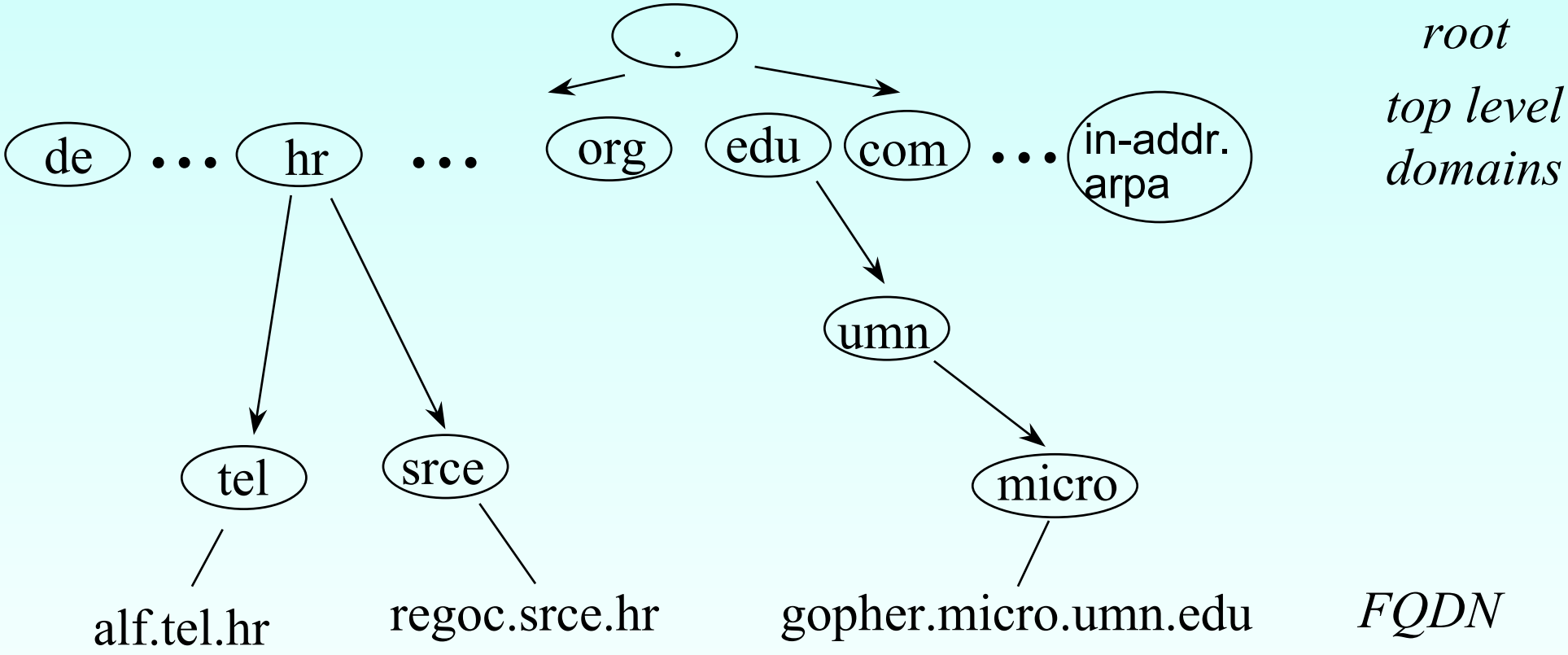
Imena

Uvod

- IP komunikacija zasnovana je na IP adresama
- Njih je teško pamtiti
- Zato se računalima i drugim IP uređajima dodjeljuju imena
- ICANN - Internet Corporation for Assigned Names and Numbers
- DNS prevodi imena u IP adrese (i obrnuto)

Imena

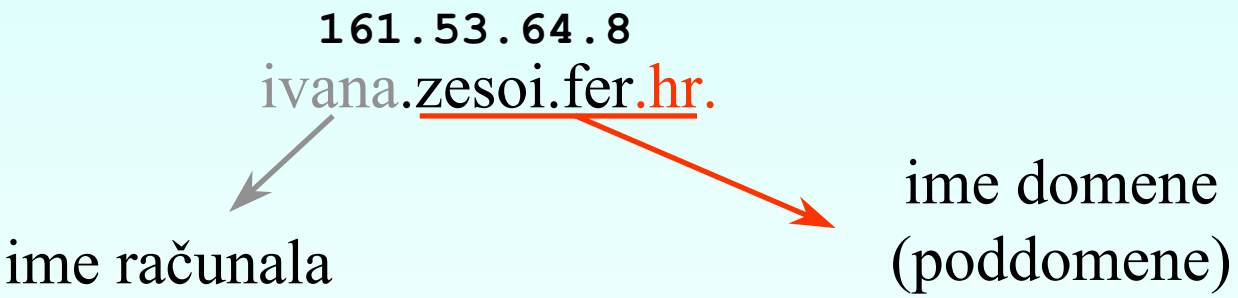
Struktura dodjele imena



Imena

FQDN

- (puni) naziv računala (FQDN - Fully Qualified Domain Name)
  - sastoji se od imena računala i odgovarajuće domene



- Broj poddomena nije ograničen

Imena

Hosts datoteka

- /etc/hosts Unix datoteka s podacima o imenima i IP adresama
- Pošiljalac odmah pomoću hosts datoteke vrši konverziju
- Koristila se na manjim mrežama gdje se imena i IP adrese ne mijenjaju često
- Na većim i dinamičnim mrežama - DNS

Imena

Hosts datoteka (2)

- Jedna IP adresa - moguće više imena odvojenih razmakom
- Korisna pri podizanju računala - čita se pri inicijalnoj konfiguraciji sučelja
- Korisna ako ne radi *name server* (*daemon named* na Unixu)
- Ako se sučelja konfiguriraju preko imena (*ifconfig*) onda u hosts datoteci trebaju biti adrese za ta imena!

Imena

Hosts datoteka (3)

- Loopback sučelje
  - služi za dijagnostiku
  - IP adresa 127.0.0.1
  - paket upućen na Loopback odmah se usmjerava nazad, ne ide niti na Ethernet ili serijsko sučelje
  - znači prvenstveno TCP/IP dijagnostika
  - većina OS-ova ima uključene Loopback drivere
  - Loopback se upisuje u /etc/hosts datoteku

Imena

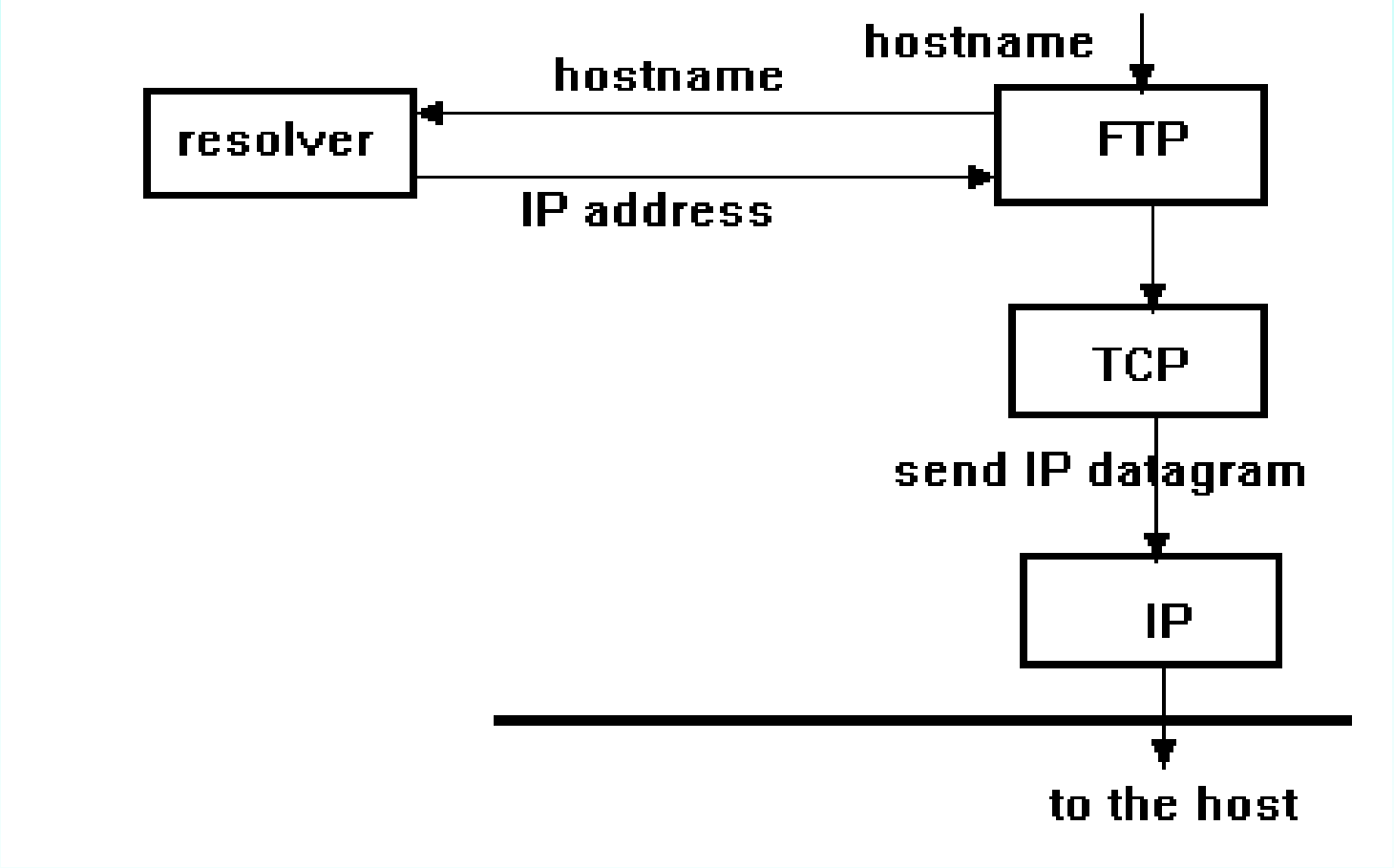
Hosts datoteka (4)

/etc/hosts

```
127.0.0.1          localhost local
161.53.64.5        maja
161.53.64.6        renata
161.53.64.254      marija
161.60.167.5       WWW.CARNet.hr
161.53.89.7        ftp.irb.hr
208.136.98.6       WWW.yahoo.com yahoo
```

Imena

DNS


hostname
hostname
resolver
FTP
IP address
TCP
send IP datagram
IP
to the host

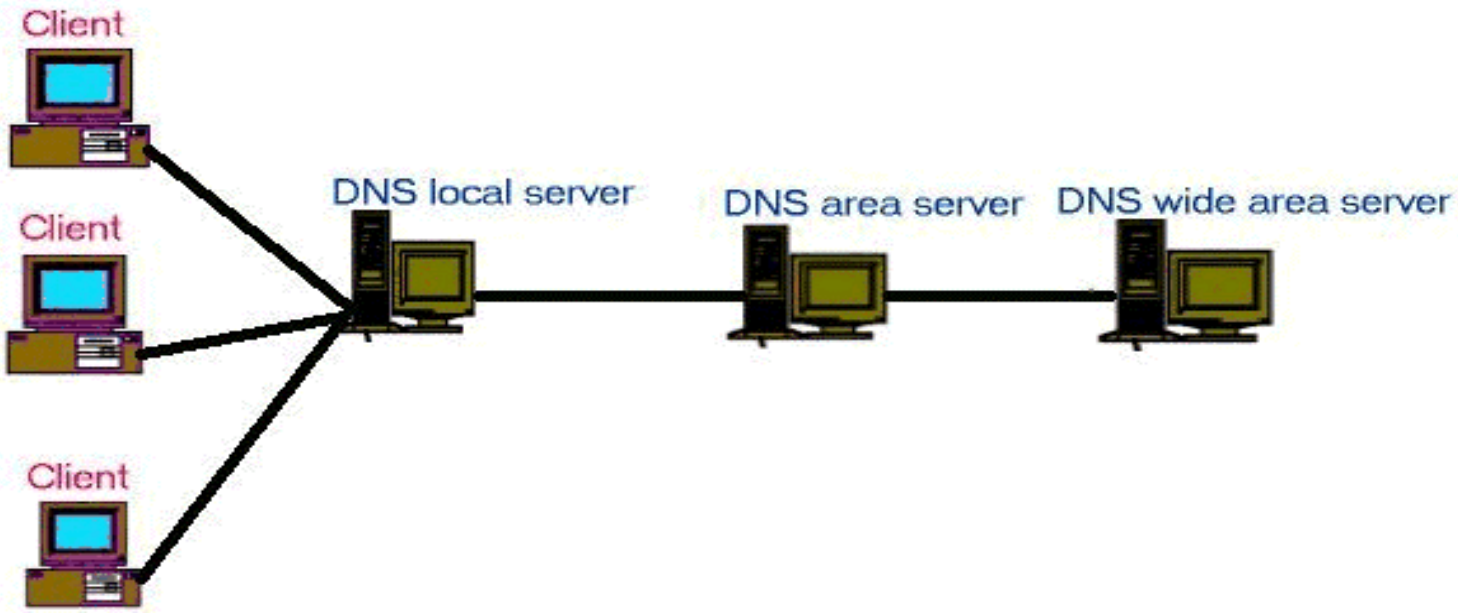
Imena

DNS (2)

- Domain Name System (Service)
- Distribuirani, hijerarhijski sustav koji jednoznačno povezuje IP adrese i nazive računala
- Razine u hijerarhiji određuju organizacijsku pripadnost računala - domenu
- Realiziran pomoću mreže DNS poslužitelja
- RFC 1034, 1035 ...

Imena

DNS (3)


Client
Client
Client
DNS local server
DNS area server
DNS wide area server

Imena

DNS (4)

- *Resolver* - programski kod na lokalnom stroju koji vrši interakciju s DNS-om
- *Name server* - DNS server (*daemon named* na Unixu)
- Resolver šalje upit serveru, koji odgovara IP adresom ako je zna, ako ne - pita se dalje:
  - nerekurzivnim načinom
  - rekurzivnim načinom

Imena

DNS - nerekurzivni način

- Ako server ne zna odgovor, šalje poruku *resolveru* da ne zna i adresu jednog ili više servera koji “možda znaju”
- Resolver zatim kontaktira te servere itd. dok ne dobije traženu adresu
- Slijedeći server može raditi u oba načina

Imena

DNS - rekurzivni način

- Ako ne zna odgovor, lokalni DNS server kontaktira sljedeći server i kad dobije odgovor šalje ga *resolveru*
- Lokalni server može kontaktirati server koji je isto u rekurzivnom modu - rekurzivni lanac
- Klijent (resolver) može zatražiti rekurzivnu uslugu
- U pravilu, resolver–server komunikacija je rekurzivna, a server–server nerekurzivna

Odgovor :

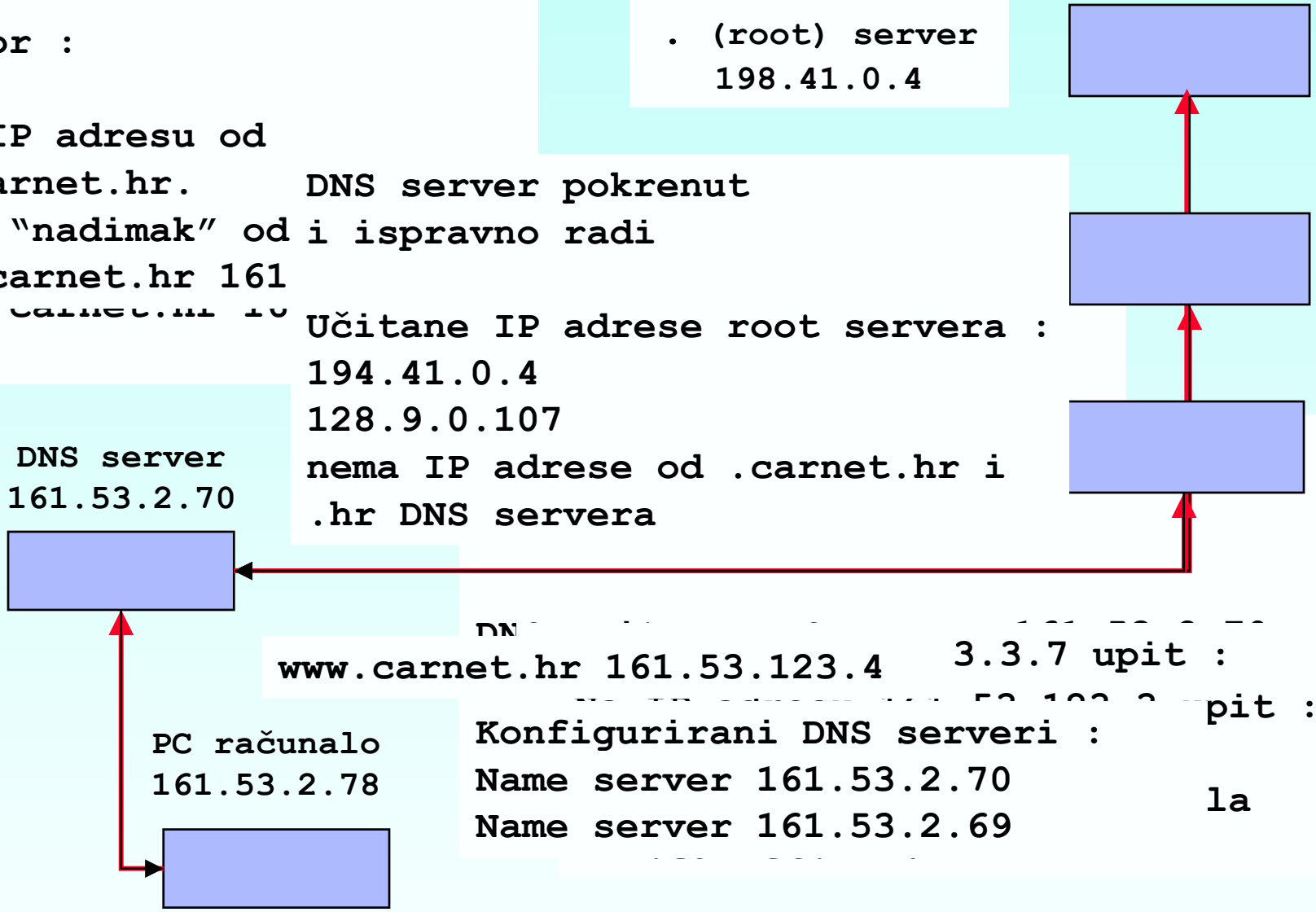
Odgovor :

Znam IP adresu od
www.carnet.hr.
To je "nadimak" od
beta.carnet.hr 161
.....

. (root) server
198.41.0.4

DNS server pokrenut
i ispravno radi

Učitane IP adrese root servera :
194.41.0.4
128.9.0.107
nema IP adrese od .carnet.hr i
.hr DNS servera



www.carnet.hr 161.53.123.4

3.3.7 upit :

pit :

Konfigurirani DNS serveri :
Name server 161.53.2.70
Name server 161.53.2.69

la

Imena

DNS - način rada

- Server prvo traži zapise za www.carnet.hr
- Ako ih nema, traži za carnet.hr
- Ako ih nema, traži za .hr
- Ako nema, traži adrese od *root* servera
- Unijeti u DNS bazu adrese hijerarhijski viših servera - do .hr servera
  - dns.srce.hr 161.53.3.7

Imena

DNS - *cache*

- Serveri (koji rade u rekurzivnom modu) održavaju *cache* tablicu
- *Resolveri* mogu raditi *cache* (/etc/nscd.conf)
- Kad dobiju tražene podatke, spremaju ime i adresu u *cache* tablicu
- Server koji šalje podatke kaže koliko se max. dugo smije zapis držati u *cacheu* da ne bi došlo do zastare (parametar TTL - Time to Live)

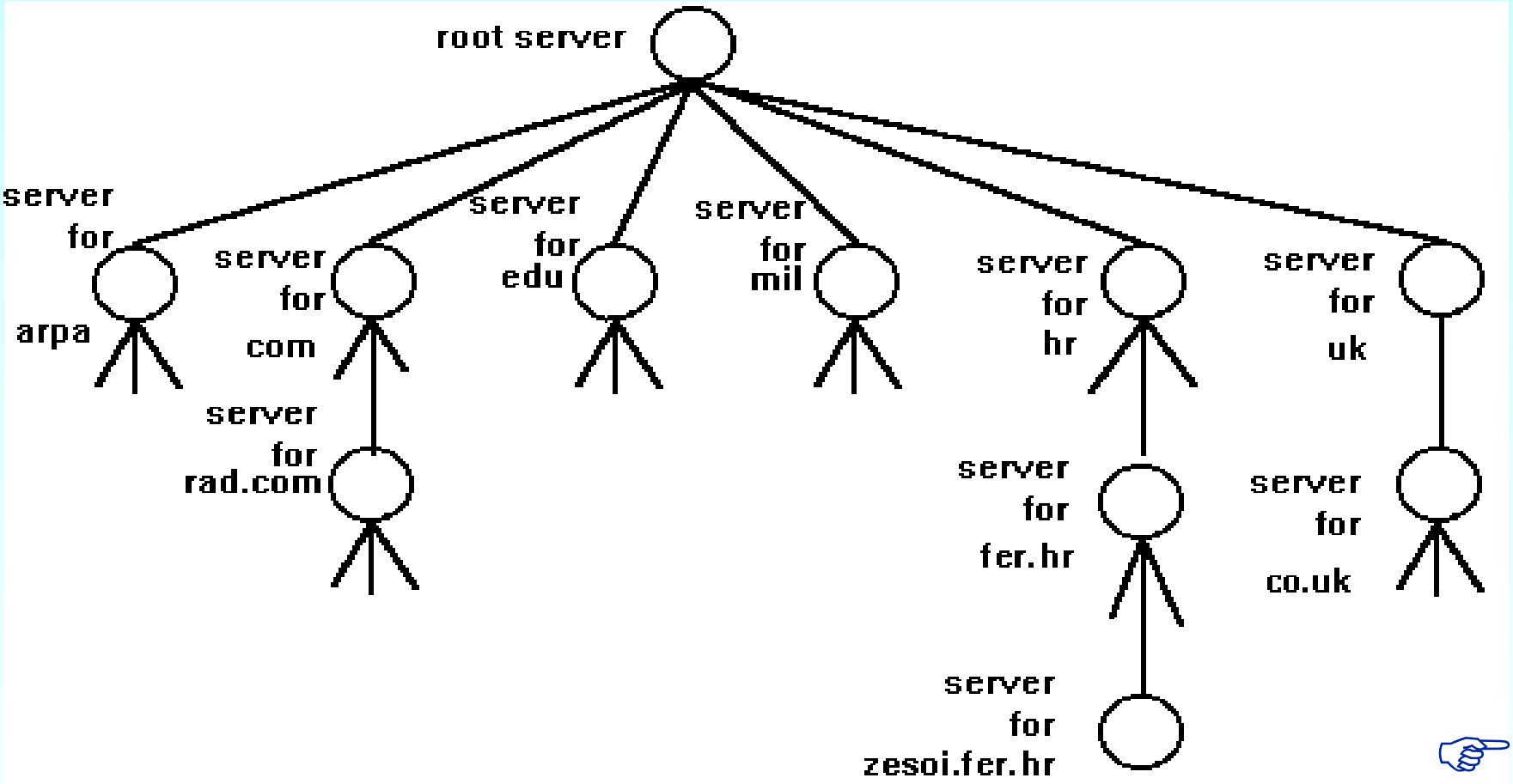
Imena

DNS - *address to name*

- Služi uglavnom za *debugiranje* i održavanje
- Adresni prostor sadržan u posebnoj domeni - IN-ADDR.ARPA
- Npr. 52.0.2.10 odgovara imenu 10.2.0.52.IN-ADDR.ARPA
- Ako netko želi saznati ime od 52.0.2.10, uputit će DNS zahtjev s parametrom 10.2.0.52.IN-ADDR.ARPA

Imena

DNS - struktura



Imena

DNS - struktura (2)

- Svaki DNS server je odgovoran (autoritet) za jednu mrežnu cjelinu (poddomena, zona)
- Jedan server može biti odgovoran za više zona
- DNS struktura je hijerarhijska
  - svaki server mora znati barem jednog servera hijerarhijski iznad sebe (root server je na vrhu)
  - server mora znati servere ispod sebe odgovorne za pojedine zone (ako postoje)

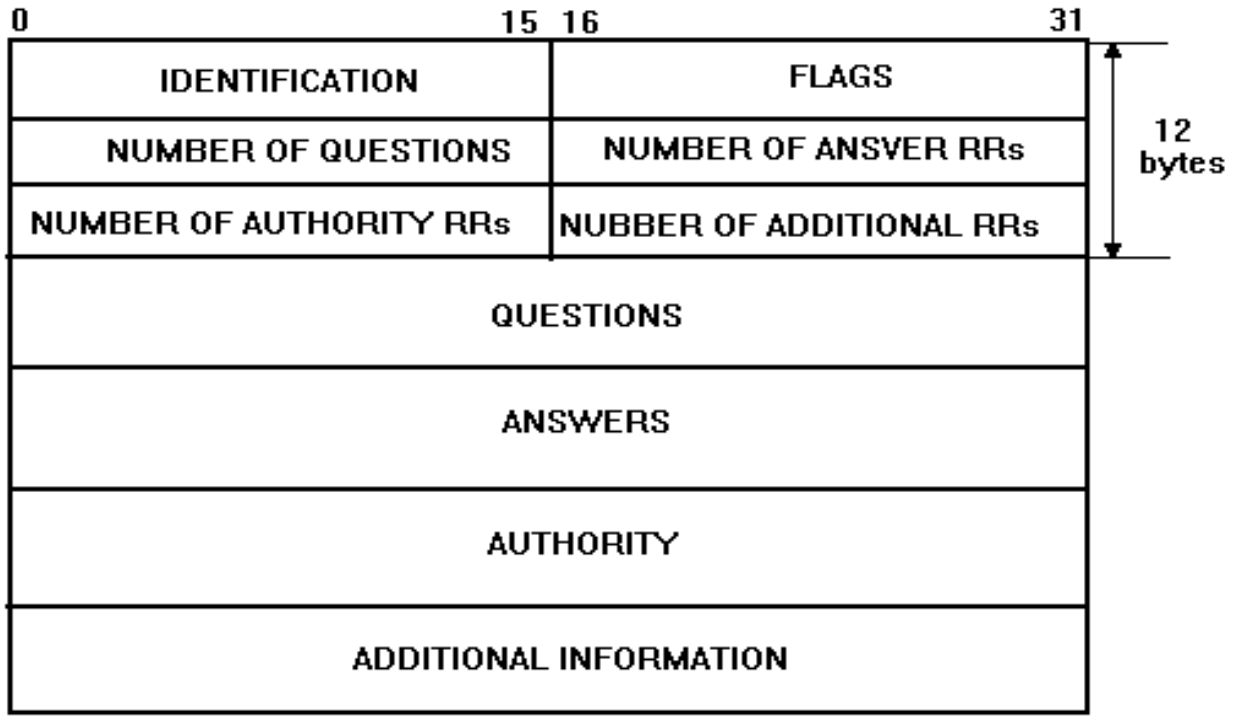
Imena

DNS - vježbe

- Kreirati i editirati datoteke:
  - /etc/hostname.*
  - /etc/defaultdomain (domainname)
  - /etc/defaultrouter
  - /etc/netmasks
  - /etc/hosts

Imena

DNS - poruke



The format of Dns queries and responses .

Imena

DNS - poruke (2)

- Identifikacija - postavlja klijent, a vraća server
- Flags (16 bita):
  - 0: QR: 0 - upit, 1 - odgovor
  - 1-4: Opcode: 0 - normal, 1 - inverzni upit, 2 - server status upit
  - 5: autoritativni odgovor: 1 - server je odgovoran za traženu domenu (ime)
  - 6: 1 - dio DNS poruke je odsječen
  - 7: 1 - rekurzivni mod je željen

Imena

DNS - poruke (3)

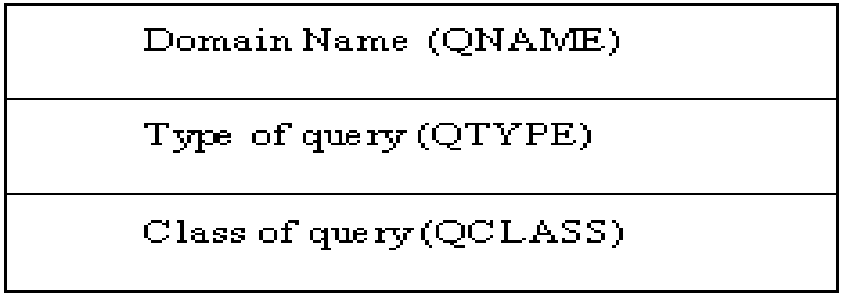
- 8: 0 - rekurzivni mod nije dostupan
- 9-11: uvijek 0
- 12-15. Return Code: 0 - nema greške, 3 - greška...

- Nr. of questions - broj pitanja u Questions polju
- Nr. of ans. RR - broj odgovora (Resource Records) u Answers polju
- Nr. of Authority RR - broj RR-a u Authority
- Nr. of Additional RR - broj RR-a u Additional

Imena

DNS - poruke (4)

- Questions

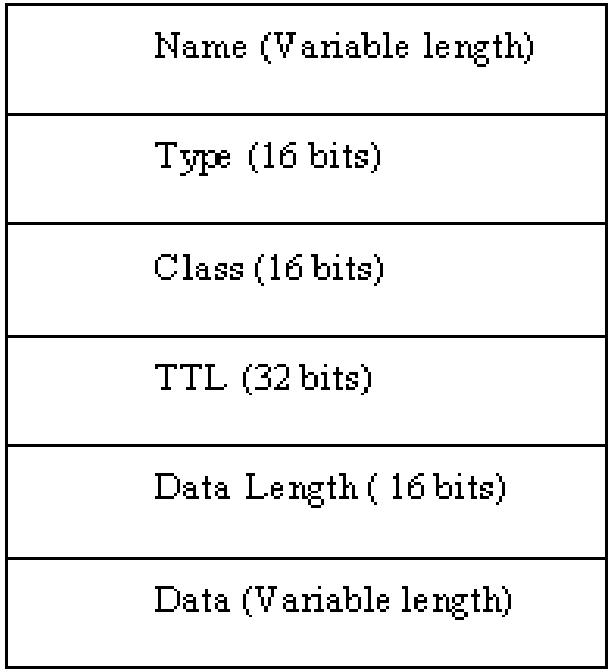


- Qname - ime za koje se traži IP adresa
- QType - tip RR-a koji se traži
- QClass - klasa traženog RR-a

Imena

DNS - poruke (5)

- Answers, Authority, Additional Information sadrže Resource Records (RR):



Imena

DNS - Resource Records

- Name (Owner) - *domain name* računala na koje se zapis odnosi, tj. “vlasnik” RR zapisa
- Type - tip RR-a (ima ih 21), najvažniji su:
  - SOA: Start of Zone Authority
  - NS: Authoritative Name Server
  - A: Network Address
  - MX: Mail Exchange
  - CNAME: Cannonical alias name
  - PTR: Domain name pointer

Imena

DNS - Resource Records (2)

- Class - klasa RR, najčešće IN za Internet Resource Record
- TTL - Time to Live - vrijeme (u sekundama) koliko RR može biti zadržan u *cacheu*
- Data Length - duljina Data polja
- Data - podaci o zapisu
  - varijabilne duljine
  - sadržaj ovisan o tipu zapisa (Type polje)

Imena

DNS - Resource Records (3)

- RR zapisi se unose na DNS server najčešće u tekstualne datoteke
- Na prethodnoj slici je izgled RR paketa, način zapisa u datoteci je sljedeći:
  - name ttl class type data
- ttl i class (IN) često se izostavljaju

```
maja    IN    A       161.53.64.5
5       IN    PTR     maja.zesoi.fer.hr.
```

Imena

DNS - Resource Records - SOA

Domain Name (MNAME)
Resp. Name (RNAME)
Serial
Refresh Time
Retry Time
Expiry Time
Minimum Time

Imena

DNS - Resource Records – SOA (2)

- MNAME – ime (*domain name*) servera koji je primarni za zonu (može ih biti više, najčešće primarni i sekundarni, tj. *master* i *slave*)
- RNAME – ime *mailboxa* administratora zone
  - mail adresa administratora, znak @ se zamjenjuje točkom – npr. DNSadmin.carnet.hr.
  - preporučljivo koristiti stalni *mail alias* (DNSadmin@carnet.hr)

Imena

DNS - Resource Records – SOA (3)

- Serial – 32-bitni broj koji označava verziju podataka u zoni
  - bitan podatak kojeg je potrebno osvježiti svaki put kad dođe do promjena u zonskoj datoteci
  - YYYYMMDDVV shema je preporučljiva
  - YYYYMMDD – godina-mjesec-dan
  - VV je redni broj verzije u danu (prva verzija u danu – 01)
  - vrijednosti se mogu mijenjati ručno ili automatizirano
  - ne smije biti = 0

Imena

DNS - Resource Records – SOA (4)

- Refresh – 32 bita, vrijeme (u sekundama) nakon kojeg treba obnoviti podatke u zoni
  - sekundarni server nakon tog vremena traži od primarnog kopiju SOA RR-a
  - ako je Serial broj manji nego na primarnom, sekundarni server traži zonski transfer
  - *default* vrijednost 3600 sekundi
  - ukoliko se planiraju neke veće promjene u konfiguraciji mreže (imena, adrese) - smanjiti prije TTL na što manju vrijednost

Imena

DNS - Resource Records – SOA (5)

- Retry – min. vrijeme nakon neuspjelog obnavljanja podataka prije novog pokušaja
  - sekundarni server ponovno traži zonski transfer nakon ovog vremena
  - *default*: 600 sekundi
- Expire – vrijeme nakon kojeg podaci o zoni više ne vrijede
  - sek. server (*slave*) nakon tog vremena proglašava svoje podatke nevažećim i ne odgovara na upite
  - *default*: 86400

Imena

DNS - Resource Records – SOA (6)

- Minimum – TTL vrijednost koju treba koristiti za svaki RR iz zone koji nema postavljen vlastiti TTL
  - *default*: 3600 sekundi
  - ukoliko se planiraju neke veće promjene u konfiguraciji mreže (imena, adrese) - smanjiti prije TTL na što manju vrijednost
  - nakon nekog vremena vratiti TTL na uobičajene vrijednosti

Imena

DNS - Resource Records – SOA (7)

- Primjer SOA RR zapisa:

```
@ IN SOA branka.zesoi.fer.hr. DNSAdmin.zesoi.fer.hr. (
          2000050201 ; Serial
          10800 ; Refresh - 3 hours
          3600 ; Retry - 1 hour
          432000 ; Expire - 5 days
          86400) ; Minimum - 1 day
```

Imena

DNS - Resource Records – NS

- Sadrži (u Data polju) ime autoriziranog (odgovornog) DNS servera za određeni dio DNS prostora
- NS RR se obavezno nalaze na serveru hijerarhijski iznad servera čije ime sadrži RR
- U Additional polju DNS odgovora server šalje RR-ove vezane uz autorizirani server

```
zesoi.fer.hr. IN NS ana.zesoi.fer.hr.
```

Imena

DNS - Resource Records – A

- Network Address
- Sadrži (u Data polju) 32-bitnu IP adresu pridruženu hostu na koji se odnosi RR
- Najčešće korišteni RR
- Ako DNS server zna IP adresu za traženo ime, tj. pronađe odgovarajući RR, šalje ga klijentu koji ga je tražio
- Primjer A RR zapisa:

```
maja    IN    A         161.53.64.3
```

Imena

DNS - Resource Records – MX

- Mail Exchange
- Data polje sadrži dva polja:
  - Preference (16 bitova)
  - Host Name
- Preference - prioritet
- Host Name - ime hosta (mail servera) koji će primiti *mail* za specificiranu domenu

Imena

DNS - Resource Records – MX (2)

- Može biti više MX RR-ova za istu domenu
- *Preference* vrijednosti u tom slučaju indiciraju prioritet *mail* servera - niže vrijednosti imaju veći prioritet
- DNS server u Additional polju vraća ostale RR-ove vezane uz mail servere koje šalje u MX polju
  - mora postojati A RR zapis za *mail* server
- Primjer MX RR zapisa:

```
zesoi.fer.hr. IN MX 10 ivana.zesoi.fer.hr.
```

Imena

DNS - Resource Records – CName

- Cannonical Alias Name
- Sadrži stvarno ime koje odgovara *aliasu*
- “Vlasnik” CNAME RR-a je *alias*, a u Data polju je pravo ime
- Primjer CNAME RR zapisa:

```
www IN CNAME solaris.fer.hr.
```

Imena

DNS - Resource Records – PTR

- Domain Name Pointer
- Koristi se kod reverznog DNS-a - pretvaranje IP adrese u ime
- Primjer PTR RR-a:

```
3       IN    PTR       maja.zesoi.fer.hr.
```

Imena

DNS - Alati - BIND

- Berkley Internet Name Domain
- U većinu Unix distribucija uključen je BIND DNS server alat
- Može se i zasebno instalirati
- 4.8.3, 4.9.3, 4.9.4, 8.Y.X, 9.Y.X
- 8.2.4
- www.isc.org

Imena

DNS - Alati - *nslookup*

- Alat za slanje upita prema DNS serverima
- Interaktivni i neinteraktivni mod
- Ulazak u interaktivni mod:

```
% nslookup
% nslookup - [nameserver]
```

- Izlazak: CTRL-D ili *exit*
- Neinteraktivni mod – jedna po jedna naredba

```
% man nslookup
```

Imena

DNS - Alati – *nslookup* - vježbe

- Ispitivati adrese različitih hostova (npr. www.carnet.hr) u interaktivnom modu
  - koristiti *default* DNS server
  - promijeniti DNS server – dns.srce.hr
  - tražiti različite podatke od DNS servera (npr. adrese *mail servera* za yahoo.com...)
- Raditi u neinteraktivnom modu
  - npr. pronaći imena i adrese DNS servera za zonu CARNet.hr, .hr...

Imena

DNS - Server

- Za konfiguraciju DNS servera potrebno je nekoliko tekst datoteka - baza podataka
- DNS server *daemon* (***named***) prvo konzutlira *boot* datoteku
- *Boot* datoteka usmjerava *daemona* na druge datoteke:
  - named.ca (*root* serveri)
  - private.hosts (računala u vlastitoj zoni)
  - private.rev (adresa u ime, vlastita zona)
  - private.local (*loopback*)

Imena

DNS - Server - *boot* datoteka

- /etc/named.conf ili /etc/namedb/named.conf

```
options {
        directory "/etc/namedb";
        forwarders { 161.53.100.2;
                     161.53.100.3;
                     };
             };
```

Imena

DNS - Server - *boot* datoteka *(2)*

```
zone "." {
        type hint;
        file "named.ca";
        };
zone "zesoi.fer.hr." {
        type master;
        file "hosts.db";
        allow-transfer { 161.53.64.3; };
                       };
```

Imena

DNS - Server - *boot* datoteka *(3)*

```
zone ”161.53.64.in-addr.arpa." {
        type master;
        file “hosts.rev";
        };
zone "0.0.127.in-addr.arpa." {
        type master;
        file “named.local";
        };
```

Imena

DNS - Server - *named.ca*

- /etc/namedb/named.ca

```
. 518400 IN NS A.ROOT-SERVERS.NET.
. 518400 IN NS D.ROOT-SERVERS.NET.
. 518400 IN NS B.ROOT-SERVERS.NET.
. 518400 IN NS C.ROOT-SERVERS.NET.

A.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.4
D.ROOT-SERVERS.NET. 3600000 IN A 128.63.2.53
B.ROOT-SERVERS.NET. 3600000 IN A 128.9.0.107
C.ROOT-SERVERS.NET. 3600000 IN A 192.33.4.12
```

Imena

DNS - Server – *hosts.db*

- /etc/namedb/hosts.db

```
@ IN SOA branka.zesoi.fer.hr. DNSAdmin.zesoi.fer.hr. (
        2000050201 ; Serial
        10800 ; Refresh - 3 hours
        3600 ; Retry - 1 hour
        432000 ; Expire - 1 week
        86400) ; Minimum - 1 day
fer.hr.    IN   NS   labs3.cc.fer.hr.
labs3.cc.fer.hr.    IN   A    161.53.70.2
hr.        IN   NS   dns.srce.hr.
```

Imena

DNS - Server – *hosts.db (2)*

```
dns.srce.hr.        IN   A    161.53.3.7
zesoi.fer.hr.       IN NS branka.zesoi.fer.hr.
;name   ttl class type       data
localhost     IN    A   127.0.0.1
branka        IN    A   161.53.64.3
maja          IN    A   161.53.64.3
renata        IN    A   161.53.64.6
ivona.zesoi.fer.hr.     IN   A    161.53.64.7
;-----------------------------------
marija        IN    A   161.53.64.254
```

Imena

DNS - Server – *hosts.db (3)*

```
; Aliases
;
mail IN CNAME solaris
www IN CNAME solaris
;
; Domain mailing addresses
;
zesoi.fer.hr. IN MX 10 branka.zesoi.fer.hr.
branka.zesoi.fer.hr. IN A 161.53.64.4
```

Imena

DNS - Server - *name to IP*

- /etc/namedb/hosts.rev

```
@ IN SOA branka.zesoi.fer.hr. DNSAdmin.zesoi.fer.hr. (
  2000050201 ; Serial
  10800 ; Refresh - 3 hours
  3600 ; Retry - 1 hour
  432000 ; Expire - 1 week
  86400) ; Minimum - 1 day
  IN NS ana.zesoi.fer.hr

  5       IN    PTR       maja.zesoi.fer.hr.
  6       IN    PTR       renata.zesoi.fer.hr.
  254     IN    PTR       marija.zesoi.fer.hr.
```

Imena

DNS - Server - *loopback*

- /var/named/named.local

```
@ IN SOA branka.zesoi.fer.hr. DNSAdmin.zesoi.fer.hr. (
  2000050201 ; Serial
  10800 ; Refresh - 3 hours
  3600 ; Retry - 1 hour
  432000 ; Expire - 1 week
  86400) ; Minimum - 1 day
  IN NS ana.zesoi.fer.hr.

;name      ttl class type      data
  1             PTR   A         localhost
```

Imena

DNS - startanje *named daemona*

- /usr/local/sbin/named
- Čita *named.conf* za svoje konfiguriranje i put prema drugim podacima
- Poželjno je *daemon* startati prilikom starta samog sistema
  - obično je dovoljno kreirati named.conf
  - modificirati /etc/init.d/inetsvc datoteku ili staviti zasebnu skriptu u /etc/rc2.d/ direktorij

Imena

DNS - Slave server

- Svaka zona može imati jedan *master* server i više *slave* servera
- Preporučljivo zbog pouzdanosti i redundantnosti imati barem jedan *slave*
- Prije se koristila terminologija primarni i sekundarni server
- *Slave* i *master* imaju iste podatke
- *Zone transfer protocol* (TCP)

Imena

DNS - Slave server (2)

- Transfer zone - prijenos DNS RR-a s *mastera* na *slave* server
- *Slave* periodički provjerava Serial broj na *masteru* i ako je manji zahtijeva transfer
- *Slave* može vršiti transfer i sa sekundarnih servera

Imena

DNS - Slave server (3)

- U named.conf datoteku upisati:

```
zone "fer.hr" {
  type slave;
  file "fer.hr/hosts.db";
  masters {
  161.53.72.21;
  161.53.67.2;
        };
};
```

Imena

Lokalno razlučivanje

- Svaki OS ima svoj način konfiguracije klijenta za DNS
- Uvijek se upisuje ime vlastite domene i IP adresa jednog ili više DNS servera
- Unixoidni OS-ovi:
  - /etc/nsswitch.conf
  - /etc/resolv.conf

Imena

Lokalno razlučivanje (2)

- /etc/nsswitch.conf

```
hosts:      files dns
```

- /etc/resolv.conf

```
domain zesoi.fer.hr
nameserver 161.53.64.3
nameserver 127.0.0.1
nameserver 161.53.72.21
nameserver 161.53.3.7
```

Imena

Uloga u CARNet mreži

- CARNet upravlja vršnom .hr domenom na osnovi ovlasti od ICANN
- “Pravilnik o organizaciji i upravljanju vršnom .hr domenom” (www.dns.hr/pravilnik.html)
- Registracija domena (www.dns.hr/registracija.html)
- Svaka članica treba imati barem jedan *slave* DNS server (bjesomar.srce.hr)
- WWW.DNS.HR

Imena

DNS - vježbe

- Provjeriti DNS konfiguraciju na stanici
- Kreirati server koji je *master* za infarkt.hr, kiki.hr i reverznu domenu ove mreže, a *slave* za zesoi.fer.hr (161.53.64.4)
- Kreirati i editirati datoteke:
  - named.conf, named.ca, hosts.db, hosts.rev, named.local
- Za napredne:
  - Kreirati jedinstvenu zonsku datoteku named.soa

```
$ include named.soa
```

Imena

DNS - vježbe (2)

- Dodati *aliase*,
- Dodati *mail exchanger*,
- Dodati još jedan rezervni *mail exchanger*,
- Dodati sve hostove za kiki.hr domenu,
- Za napredne:
  - Postati *slave* za još jednu reverznu domenu (161.53.64)

Imena

DNS - vježbe (3)

- (Re)startati *named daemon*
- Editirati nsswitch.conf i resolv.conf
- Mijenjati konfiguracije DNS servera
  - postaviti vlastiti host kao jedini DNS server (resolv.conf),
  - isprobavati konekcije lokalno i prema Internetu,
  - postaviti neki drugi lokalni host kao DNS server,
  - isprobavati konekcije na Internet i lokalno, testirati druge servere pomoću *nslookupa*
  - ...

Sigurnost
DoS

- *Denial of Service*
- Cilj ovih napada je zagušenje mreže i servera
- Nema krađe podataka
- Nanošenje materijalne štete dužim prekidima u radu ciljane mreže ili servera
- Teško se zaštiti od ovih napada
- Cilj: spriječiti da vlastita mreža posluži kao izvor DoS napada

Sigurnost
DoS - tipovi

- Denial of Service - DoS
  - napad s jednog računala na server ili drugi mrežni uređaj
  - relativno lako je identificirati odakle dolazi napad i blokirati (filtrirati) ga
  - lako je i otkriti napadača, iako se napad najčešće pokreće s nekog neutralnog računala
  - neefikasniji od DDoS napada, jer mogu generirati ograničenu količinu lažnih zahtjeva

Sigurnost
DoS - tipovi (2)

- Distributed Denial of Service - DDoS
  - kao i DoS napadi, šalju velike količine zahtjeva prema ciljanom serveru
  - u napad je uključen veći broj računala (klijenata)
  - program za generiranje napada se distribuira na neutralna računala (u formi virusa, crva, trojanskog konja)
  - znatno je teže braniti se od DDoS napada kao i identificirati izvorište napada

Sigurnost
DoS - tipovi (3)

- Remote system hogging
  - uzrokuje preopterećenost procesora napadnutog sistema
  - *mail* serveri su često mete
- Syn flood
  - generiraju se SYN paketi s lažnim ID-om na koje napadani server treba odgovoriti
  - napadani server čeka neko vrijeme odgovor na svoj paket s lažnim ID-om, prije oslobađanja resursa

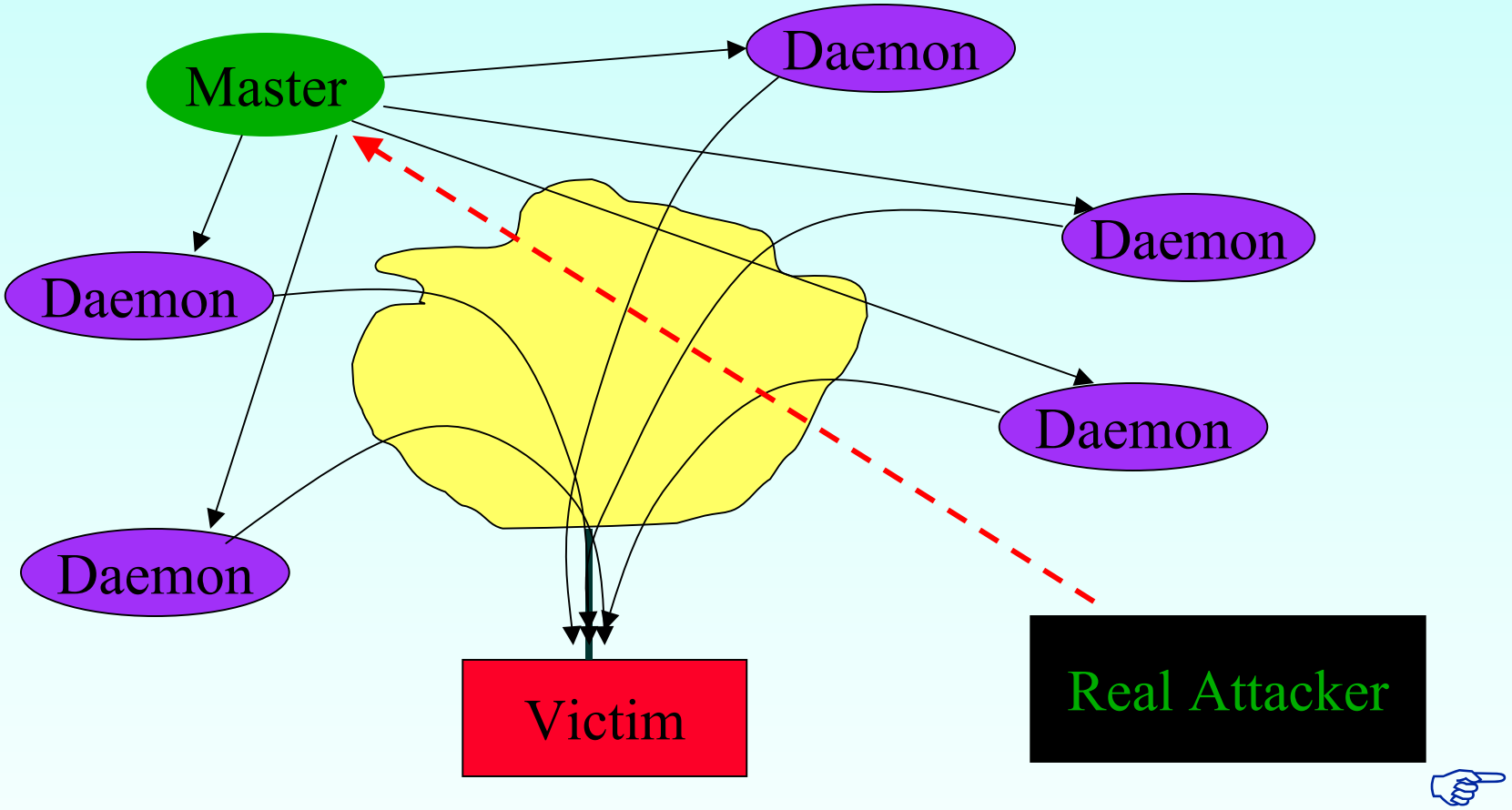
Sigurnost
DoS - tipovi (4)

- Ping of Death
  - koristi test pakete s Echo request zahtjevom
  - paketi su veće dužine od dozvoljene
  - to uzrokuje probleme mrežnim programima na napadanom uređaju i njegovo onesposobljavanje u krajnjem slučaju

- Ovo su bili osnovi tipovi DoS/DDoS napada, postoji i niz drugih

Sigurnost

DDoS

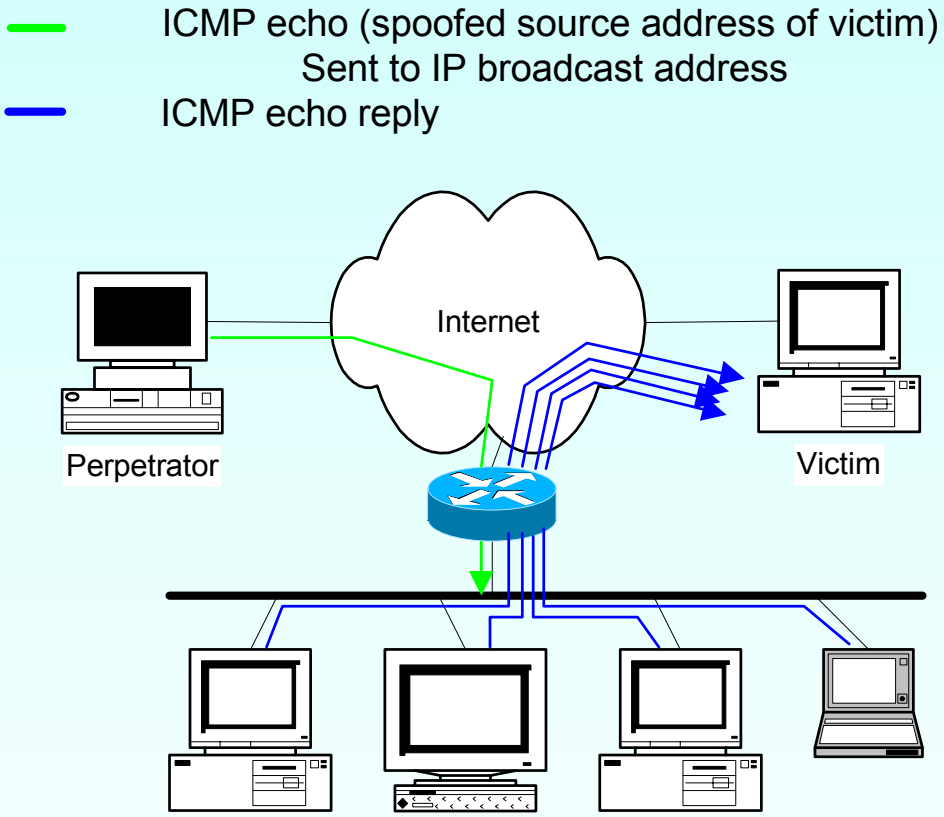


Sigurnost
DDoS (2)

- Attacker - napadač koji kriomice instalira Master i Daemon programe na dostupna računala
- Master - program koji kontrolira i koordinira agente
- Daemon (Agent) - provodi DoS napad
- Victim - ciljana žrtva DDoS napada (serveri, routeri …)

Sigurnost
DDoS (3)

- Smurf



Sigurnost
DDoS (4)

- Fraggle
  - isto kao Smurf, samo koristi UDP *echo* pakete
- Trinoo
  - komunikacija Attacker-Master-Daemon zaštićena lozinkama
  - agenti napadaju žrtvu UDP paketima velike duljine (npr. 1000 okteta)

Sigurnost
DDoS (5)

- Tribe flood network 2000 - TFN2K
  - napredni DDoS alat
  - sva komunikacija Attacker-Daemon-Master je kriptirana i kodirana te jednosmjerna
  - koristi više vrsta napada - SYN floods, UDP floods ping floods, broadcast ping floods
- Postoji još niz naprednih DDoS alata (Stacheldraht, Shaft, Mstream…)

Sigurnost
DoS - kako ih spriječiti

- Vrlo se teško braniti od DoS i posebice od DDoS napada
- Postoje opća pravila za zaštitu i mjere protiv pojedinih tipova napada
- Bitno je i moguće spriječiti da vlastita mreža postane izvor napada (mjesto instalacije Mastera i Daemona)

Sigurnost
DoS - kako ih spriječiti (2)

- Kvalitetno organizirati mrežnu zaštitu (firewall, IDS …)
- Zaštita na rubu mreže (routeri)
  - blokirati lažirane *source* adrese s vlastite mreže
  - spriječiti *broadcast* pakete izvana
  - spriječiti *broadcast* pakete iznutra prema van
  - ostale klasične metode zaštite...

Sigurnost
DoS - kako ih spriječiti (3)

- Zaštita javnih (Internet) servera
  - instalirati najnovije verzije programa i OS-a s odgovarajućim *patchevima*
  - deaktivirati sve nepotrebne servise
- Zaštita internih servera i računala
  - zaštiti ih vatrozidom od pristupa izvana
  - ako postoji potreba za pristupom izvana, strogo je ograničiti i kontrolirati

Sigurnost
DoS - kako ih spriječiti (4)

- Ublažavanje napada
  - kvalitetni i jaki usmjerivači i poslužitelji bolje podnose DoS napade
  - veći kapacitet veza teže je dovesti do zagušenja
  - fino podešavanje SW-a, čak i za vrijeme samih napada (npr. smanjivanje vremena čekanja na odgovor na TCP pakete)

Sigurnost
DoS - kako ih spriječiti (5)

- Poduzeti sve da se onemogući korištenje vlastite mreže kao izvora DoS napada
  - kontrolirano dodjeljivati prava instaliranja programa, mijenjati lozinke
  - koristiti nove inačice programa i OS-a sa sigurnosnim zakrpama
  - koristiti centralizirane anti-virus sustave i redovito ih osvježavati
  - zaštiti internu mrežu vatrozidom, onemogućiti izravnu komunikaciju izvana (telnet i sl.)

Sigurnost
DoS - kako ih spriječiti (6)

- blokirati lažirane *source* adrese s vlastite mreže
- deaktivirati sve nepotrebne servise
- spriječiti *broadcast* pakete iznutra prema van
- skenirati otvorene portove i provjeriti njihovu namjenu
- blokirati poznate portove koji se koriste za komunikaciju Attacker-Master-Daemon
- koristiti IDS sustave (skupi su i zahtjevni za održavanje)

Sigurnost
DoS - kako ih spriječiti (7)

- Detektiranje DoS napada
  - iznenadna velika količina prometa na mreži
  - iznenadno veliko opterećenje servera
  - korištenje IDS sustava (velike mogućnosti, ali skupi i zahtjevni za konfiguriranje i održavanje)
  - većina Firewalla ima mogućnosti detektiranja i odsijecanja DoS napada
  - postoje alati za detektiranje DoS napada na serverima

Sigurnost
DoS - kako ih spriječiti (8)

- Detektiranje DoS napada s vlastite mreže
  - praćenje zapisa na vatrozidu (pokušaj lažiranja *source* adrese)
  - blokiranje i praćenje aktivnosti na poznatim portovima koje koriste DoS alati (npr. 37337)
  - skeniranje otvorenih portova na mreži (noviji DoS alati ne odgovaraju na skeniranje)

Sigurnost
DoS - kako ih spriječiti (9)

- Što napraviti u slučaju DoS napada?
  - ne paničariti
  - bilježiti sve podatke i dokaze
  - obavijestiti nadležne ustanove i osobe (CARNet CERT, odgovorne u vlastitoj ustanovi)
  - koristiti tel. i fax komunikaciju
  - napraviti *backup* sistemskih datoteka
  - pokušati spriječiti ili ublažiti napad (po potrebi se odspojiti od mreže pri tome)

Sigurnost
DoS - kako ih spriječiti (10)

- Što napraviti u slučaju DoS napada s vlastite mreže?
  - ukloniti agente (*daemone*) (po potrebi se odspojiti od mreže)
  - obavijestiti nadležne osobe i ustanove
  - pronaći na koji način su agenti dospjeli na mrežu i blokirati tu mogućnost
  - pojačati sigurnosne mjere (instalirati programe za detektiranje promjena na računalima, IDS)

Sažetak

- TCP/IP, komunikacija, paketi
- Strukturno kabliranje, bakreni i optički kabeli, norme, osnovni zahtjevi
- CARNet ustanova, odnos i veza ustanove i CARNeta, CARNet oprema,
- Imena, potreba za imenima, definiranje domene, /etc/hosts datoteka, DNS, Resource Records, SOA, MX, lokalno razlučivanje, uloga u CARNet mreži
- Sigurnost, DoS, DDoS, kako ih spriječiti

Literatura

- RFC 1034
- RFC 1035
- Man Unix naredba
- Internet