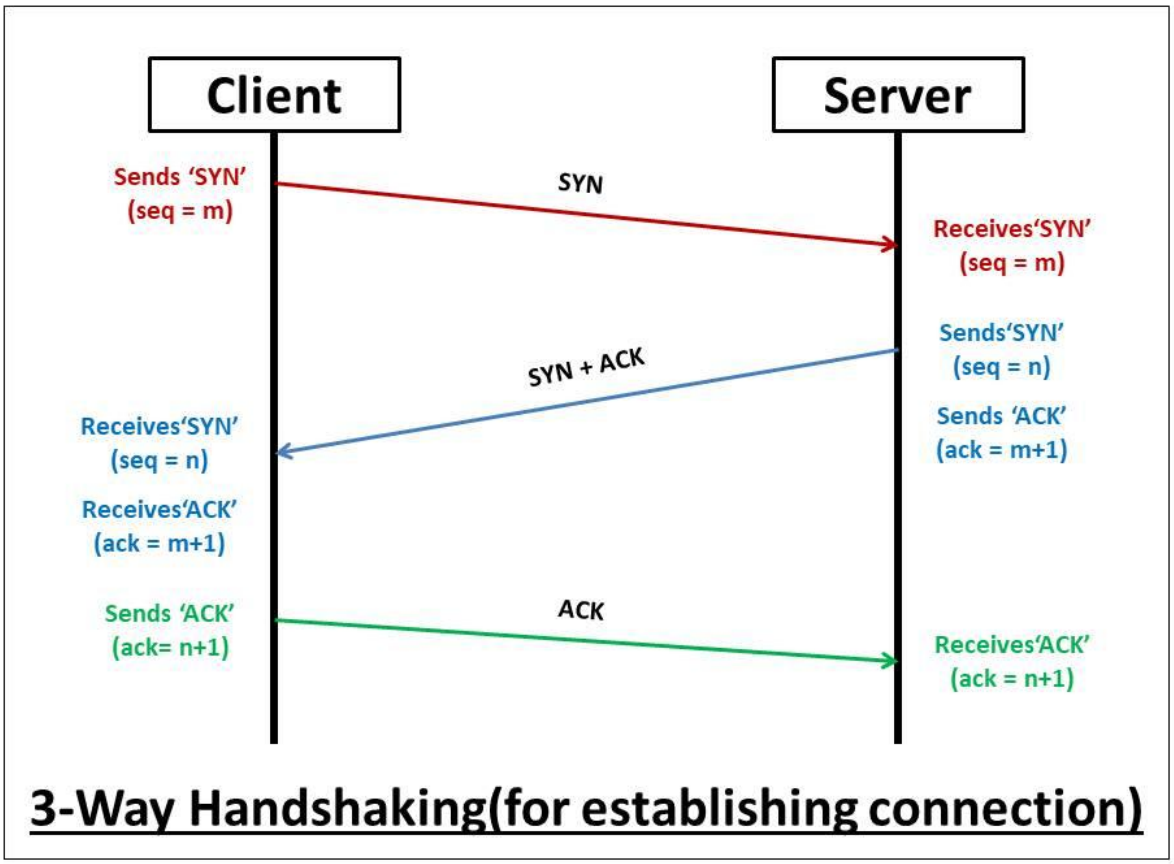


Šta je 3-way handshake?

3-way handshake je proces uspostavljanja veze u **TCP** (Transmission Control Protocol) komunikaciji. TCP je pouzdan protokol na transportnom sloju OSI modela, koji osigurava da podaci budu ispravno preneseni između dva krajnja uređaja (hosta).

Kada se koristi?

Koristi se svaki put kada se želi uspostaviti **pouzdana TCP veza** između dva uređaja (npr. klijent i server), pre nego što se prenesu podaci. Ovo je početni korak komunikacije u aplikacijama poput:

- **HTTP/HTTPS** (web stranice)
- **FTP** (prenos fajlova)
- **Telnet** (daljinski pristup)
- **SMTP** (e-pošta)

Kako funkcioniše 3-way handshake?

Proces ima tri koraka:

1. **SYN (Synchronize):**
    - Klijent šalje zahtjev za uspostavljanje veze serveru.
    - Ovaj zahtjev sadrži **SYN flag** (sinhronizacijski signal) i početni sekvencijalni broj (**Sequence Number**), npr. Seq = x.
2. **SYN-ACK (Synchronize-Acknowledge):**
    - Server odgovara potvrdom (ACK) klijentovog zahtjeva.
    - Server također šalje svoj vlastiti zahtjev za uspostavljanje veze s **SYN flagom** i svojim početnim sekvencijalnim brojem, npr. Seq = y i Ack = x+1.
3. **ACK (Acknowledge):**
    - Klijent potvrđuje serverov zahtjev.
    - Klijent šalje **ACK flag** s Ack = y+1, čime se završava uspostavljanje veze.

Vizuelni prikaz:

Klijent -> Server: [SYN, Seq = x]

Server -> Klijent: [SYN-ACK, Seq = y, Ack = x+1]

Klijent -> Server: [ACK, Ack = y+1]

Nakon ovoga, veza je uspostavljena i uređaji mogu razmjenjivati podatke.

Primjer:

Zamislimo da klijent otvara web stranicu:

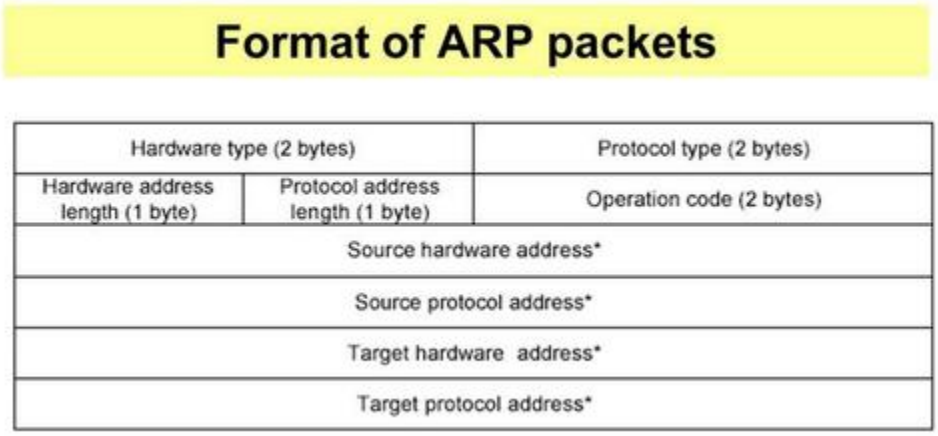
1. Klijent (npr. vaš računar) želi uspostaviti TCP vezu s web serverom.
2. **SYN:** Klijent šalje SYN paket serveru (početni broj: Seq = 1000).
3. **SYN-ACK:** Server odgovara sa SYN-ACK paketom (Seq = 500, Ack = 1001).
4. **ACK:** Klijent šalje ACK paket (Ack = 501).

Nakon ovoga, HTTP/HTTPS protokol počinje slati zahtjeve (npr. za stranicu ili fajlove).

Zašto je važan?

- **Osigurava pouzdanost:** Omogućava da obje strane potvrde spremnost za komunikaciju.

- **Provjera konekcije:** Provjerava dostupnost i spremnost klijenta/servera.
- **Upravljanje resursima:** Prije nego što veza počne, uređaji rezervišu resurse (portove, memoriju).



Format ARP paketa:

1. Hardware Type (2 bajta):

- Ovaj polje identificira tip hardverske adrese (MAC adrese) koja se koristi na Data Link sloju.
- **Primjer:**
    - **0x0001** označava Ethernet (najčešći slučaj).
    - Drugi tipovi mogu biti FDDI, token ring, itd.

2. Protocol Type (2 bajta):

- Identificira protokol za koji se traži razrješavanje adrese.
- **Primjer:**
    - **0x0800** označava IPv4.
    - Može biti i neki drugi mrežni protokol, npr. IPv6.

3. Hardware Address Length (1 bajt):

- Daje dužinu hardverske adrese u bajtovima.
- **Primjer:**
    - Za Ethernet, MAC adresa ima 6 bajtova (vrijednost će biti **6**).

4. Protocol Address Length (1 bajt):

- Daje dužinu protokolske adrese u bajtovima.
- **Primjer:**
    - Za IPv4 adresu, vrijednost će biti **4**.

5. Operation (2 bajta):

- Označava tip ARP poruke:
    - **1** – ARP Request (zahtjev za razrješavanje adrese).
    - **2** – ARP Reply (odgovor s razriješenom adresom).
    - **3** – RARP Request (zahtjev za reverzni ARP).
    - **4** – RARP Reply (odgovor na reverzni ARP).

6. Source Hardware Address:

- Hardverska (MAC) adresa pošiljaoca zahtjeva/odgovora.
- **Primjer:** Ako je uređaj na Ethernet mreži, ovdje je MAC adresa pošiljaoca ARP paketa.

7. Source Protocol Address:

- Protokolska (IP) adresa pošiljaoca.
- **Primjer:** IP adresa uređaja koji šalje ARP zahtjev ili odgovor.

8. Target Hardware Address:

- Hardverska (MAC) adresa odredišta.
- Kod ARP zahtjeva ovo polje je inicijalno **prazno** (nije poznato), dok kod ARP odgovora sadrži MAC adresu ciljanog uređaja.

9. Target Protocol Address:

- Protokolska (IP) adresa odredišta.
- Ovo je IP adresa uređaja čiju MAC adresu pokušavamo saznati.

Kako funkcioniše ARP u mreži?

1. **ARP Request:**
    - Kada uređaj (npr. računar A) želi poslati podatke drugom uređaju (računaru B) na istoj mreži, ali ne zna njegovu MAC adresu, šalje **ARP Request**. U njemu su:
        - **Source Hardware Address**: MAC adresa računara A.
        - **Source Protocol Address**: IP adresa računara A.

        - **Target Protocol Address**: IP adresa računara B.
        - **Target Hardware Address**: Prazno, jer se traži.
2. **ARP Reply:**
    - Uređaj B prima ARP Request, prepoznaje svoju IP adresu u polju **Target Protocol Address**, i odgovara sa:
        - **Target Hardware Address**: MAC adresa računara B.
        - **Target Protocol Address**: IP adresa računara B.
3. **Nakon ARP odgovora:**
    - Računar A sada ima MAC adresu računara B i može direktno slati Ethernet frejmove.

Primjer:

Pretpostavke:

- **Računar A**: IP 192.168.1.10, MAC AA:BB:CC:DD:EE:FF.
- **Računar B**: IP 192.168.1.20, MAC 11:22:33:44:55:66.

Koraci:

1. **ARP Request (poslat s računara A):**
    - Source Hardware Address: AA:BB:CC:DD:EE:FF.
    - Source Protocol Address: 192.168.1.10.
    - Target Hardware Address: Prazno.
    - Target Protocol Address: 192.168.1.20.
2. **ARP Reply (poslat s računara B):**
    - Source Hardware Address: 11:22:33:44:55:66.
    - Source Protocol Address: 192.168.1.20.
    - Target Hardware Address: AA:BB:CC:DD:EE:FF.
    - Target Protocol Address: 192.168.1.10.

Hajde da detaljno objasnimo pojmove **protokol** i **port**, kao i njihove funkcije, primjene, i razlike.

Šta je protokol?

Protokol je **pravilnik** ili skup pravila koja definišu kako uređaji međusobno komuniciraju u mreži. To uključuje pravila za:

1. **Razmjenu podataka**: Kako se podaci prenose.
2. **Formate**: Kako izgleda struktura paketa/podataka.
3. **Kontrolu grešaka**: Kako se greške detektuju i ispravljaju.
4. **Sekvenciranje**: Kako se podaci pravilno redaju.

Primjeri protokola:

1. **HTTP (HyperText Transfer Protocol)**: Koristi se za pregledavanje web stranica.
2. **FTP (File Transfer Protocol)**: Prenos fajlova između uređaja.
3. **TCP (Transmission Control Protocol)**: Pouzdan prenos podataka.
4. **UDP (User Datagram Protocol)**: Brz, ali nepouzdan prenos podataka.
5. **ICMP (Internet Control Message Protocol)**: Koristi se za dijagnostiku mreže, npr. kod pinga.
6. **ARP (Address Resolution Protocol)**: Pronalazi MAC adresu za datu IP adresu.

Zašto se koriste protokoli?

- Da bi komunikacija između uređaja bila standardizovana i kompatibilna.
- Svaki uređaj u mreži "razumije" pravila protokola.
- Omogućava različitim vrstama uređaja (računari, telefoni, serveri) da komuniciraju.

Gdje se koriste protokoli?

- U svakodnevnom radu s internetom i mrežama.
- Za slanje e-mailova, pregledavanje web stranica, skidanje fajlova, video konferencije itd.

Šta je port?

Port je **logički broj** (identifikator) koji aplikacije ili servisi koriste za razmjenu podataka na jednom uređaju. Možemo ga zamisliti kao "vrata" kroz koja podaci ulaze ili izlaze na određeni servis.

Primjeri portova:

- **Port 80**: HTTP (web stranice bez enkripcije).

- **Port 443**: HTTPS (web stranice s enkripcijom).
- **Port 22**: SSH (sigurno daljinsko povezivanje).
- **Port 25**: SMTP (slanje e-mailova).
- **Port 53**: DNS (prevođenje domena u IP adrese).

Zašto se koriste portovi?

- Da bi uređaj razlikovao različite servise koji rade na istoj IP adresi.
- Npr., računar može istovremeno koristiti:
    - **Port 80** za pregledavanje interneta.
    - **Port 22** za daljinsko povezivanje preko SSH-a.
    - **Port 25** za slanje e-mailova.

Kako rade portovi?

- Kada aplikacija želi komunicirati, koristi **specifičan port**.
- Na serverima, određeni servisi "slušaju" na specifičnim portovima.
- **Primjer:** Web server "sluša" na portu 80 (HTTP) ili 443 (HTTPS). Kada klijent šalje zahtjev, podaci stižu na taj port.

Razlika između protokola i portova:

Protokol	**Port**
Skup pravila za komunikaciju.	Logički broj koji identificira aplikaciju.
Primjer: HTTP, TCP, UDP.	Primjer: 80, 443, 22.
Određuje **kako** se podaci razmjenjuju.	Određuje **gdje** se podaci šalju.
Radi na više nivoa OSI modela.	Povezan je s Transportnim slojem (TCP/UDP).

Kada, gdje i kako se koriste protokoli i portovi?

Kada se koriste?

- Protokoli i portovi koriste se u svakodnevnoj komunikaciji preko mreže:
    - Pristup internetu (HTTP/HTTPS).
    - Slanje i primanje e-mailova (SMTP, IMAP, POP3).

- Online igre (koriste specifične portove i protokole).
- Video konferencije (UDP za brzinu, TCP za pouzdanost).

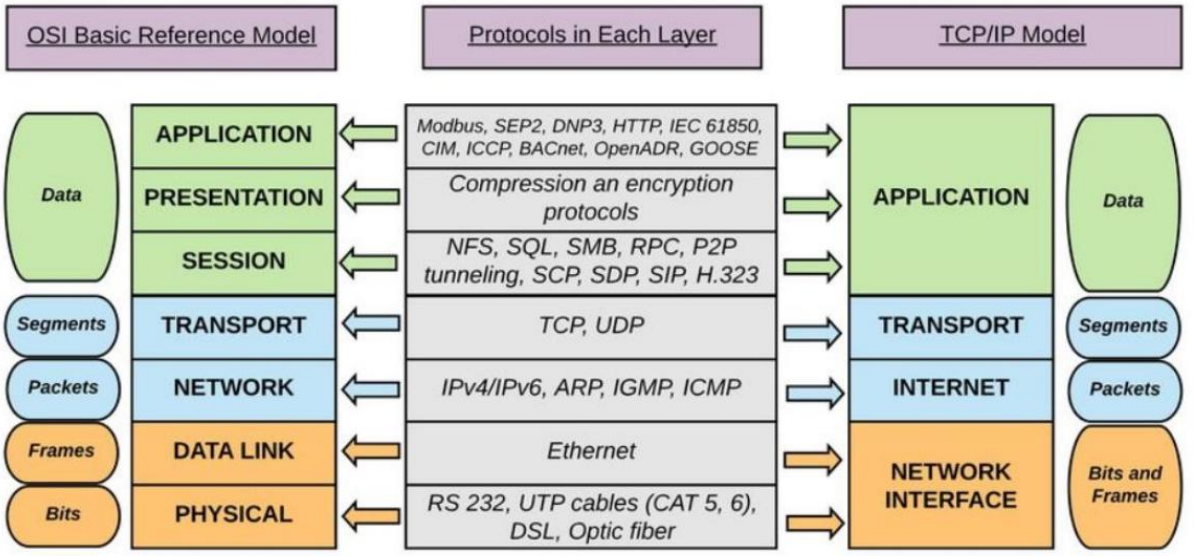
Gdje se koriste?

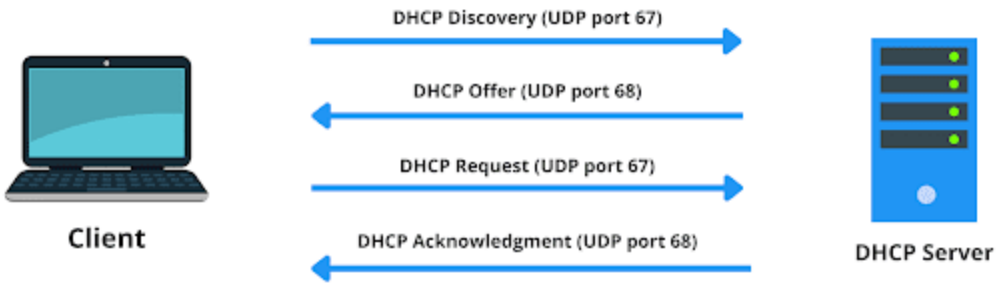
- Na svakom uređaju u mreži:
  - Klijent (računar, telefon) koristi portove da komunicira sa serverima.
  - Serveri "slušaju" na određenim portovima za različite servise.

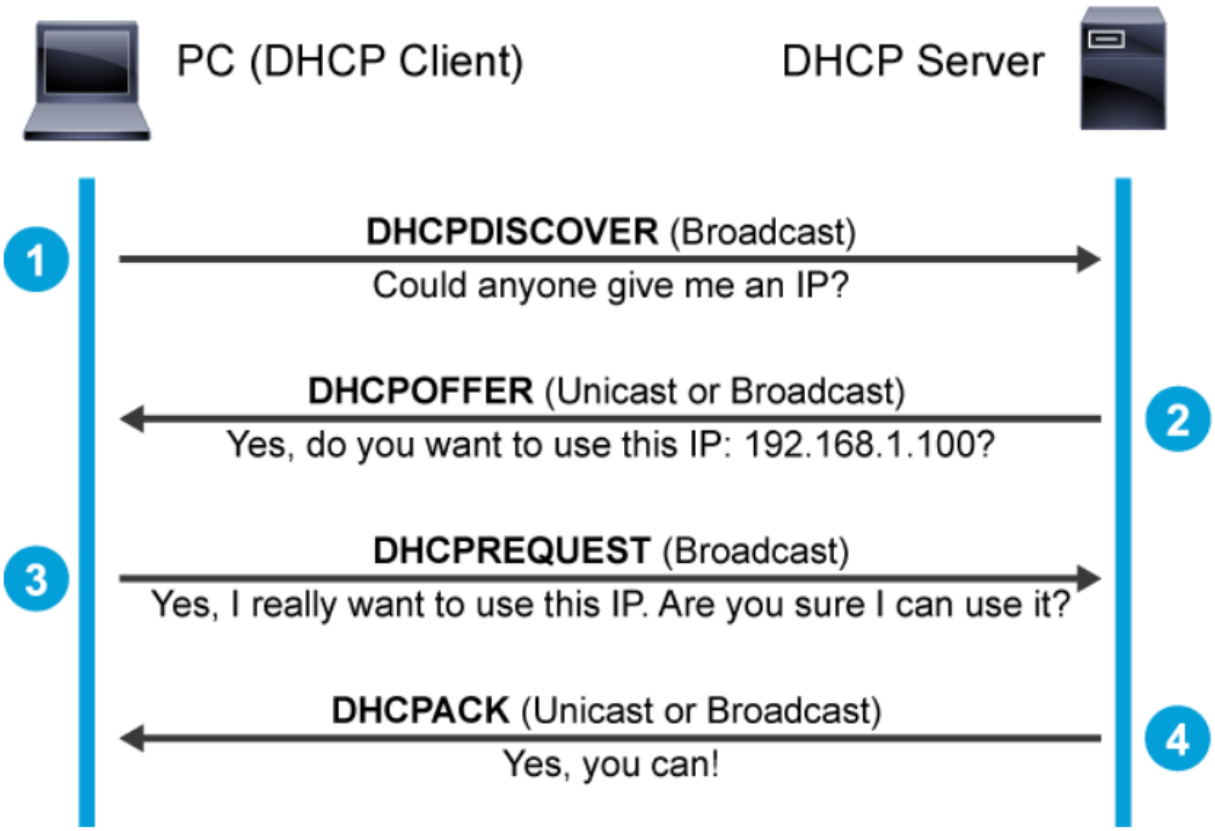
Kako funkcioniše?

1. **Komunikacija klijenta i servera:**
   - Klijent šalje zahtjev prema serveru koristeći **IP adresu** i **određeni port** (npr., HTTP zahtjev na port 80).
   - Server odgovara koristeći isti protokol i port.
2. **Primjer:**
   - Kada otvoriš web stranicu (npr. google.com):
     - Tvoj računar koristi **HTTP protokol**.
     - Podaci se šalju prema IP adresi Google servera.
     - Koristi se **port 80** ili **443** (za HTTPS).

Analiza mrežnog saobraćaja




DHCP Discovery (UDP port 67)
DHCP Offer (UDP port 68)
DHCP Request (UDP port 67)
DHCP Acknowledgment (UDP port 68)
Client
DHCP Server


PC (DHCP Client)
DHCP Server
1
DHCPDISCOVER (Broadcast)
Could anyone give me an IP?
DHCPOFFER (Unicast or Broadcast)
Yes, do you want to use this IP: 192.168.1.100?
2
3
DHCPREQUEST (Broadcast)
Yes, I really want to use this IP. Are you sure I can use it?
DHCPACK (Unicast or Broadcast)
Yes, you can!
4

Ethernet – fizički sloj

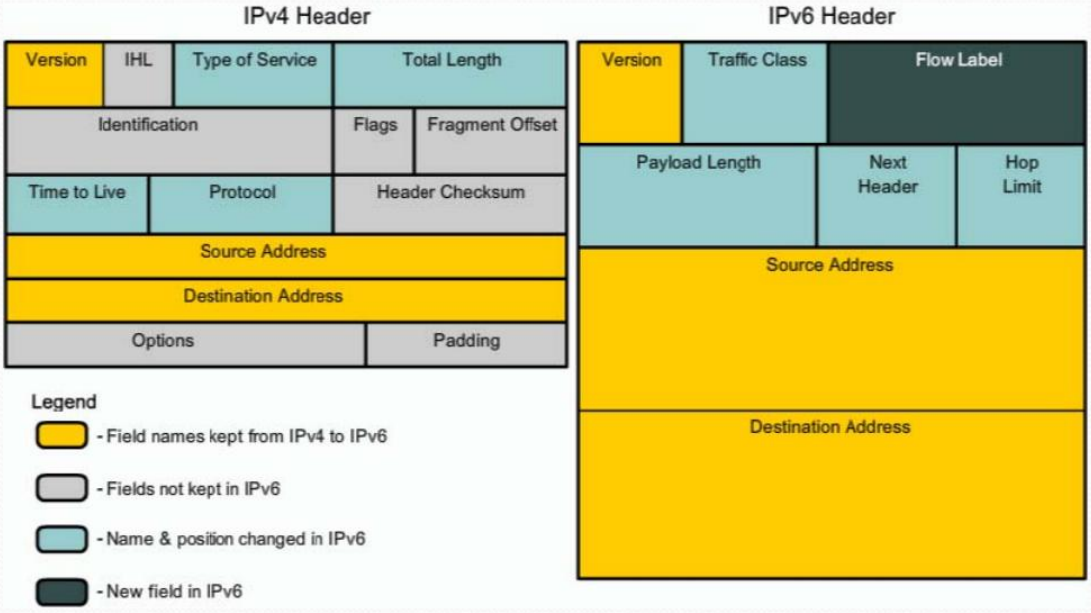
Types of Ethernet

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
100Base-FX	200 Mbps	Multimode Fiber	Full	2 km
1000Base-T	1 Gbps	Cat5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-CX4	10 Gbps	Twin-axial	Full	100 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km

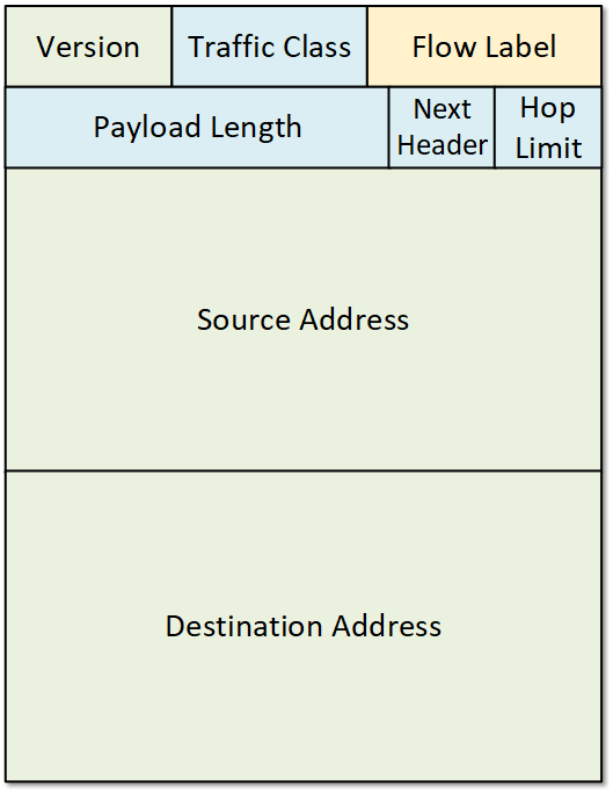
Types of Ethernet

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
100Base-FX	200 Mbps	Multimode Fiber	Full	2 km
1000Base-T	1 Gbps	Cat5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-CX4	10 Gbps	Twin-axial	Full	100 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km

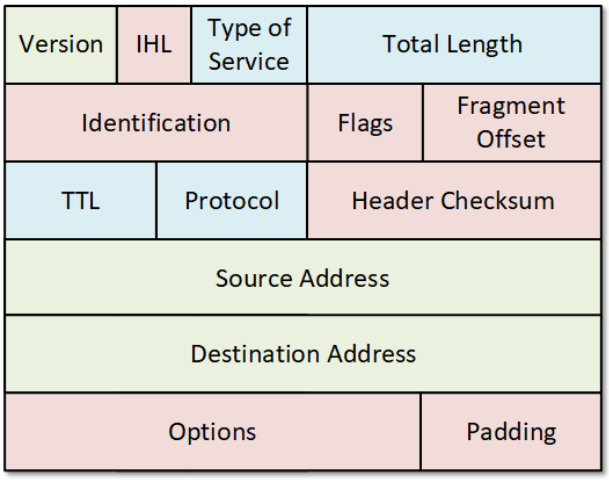
IPv4 header vs. IPv6 header



IPv6 Header

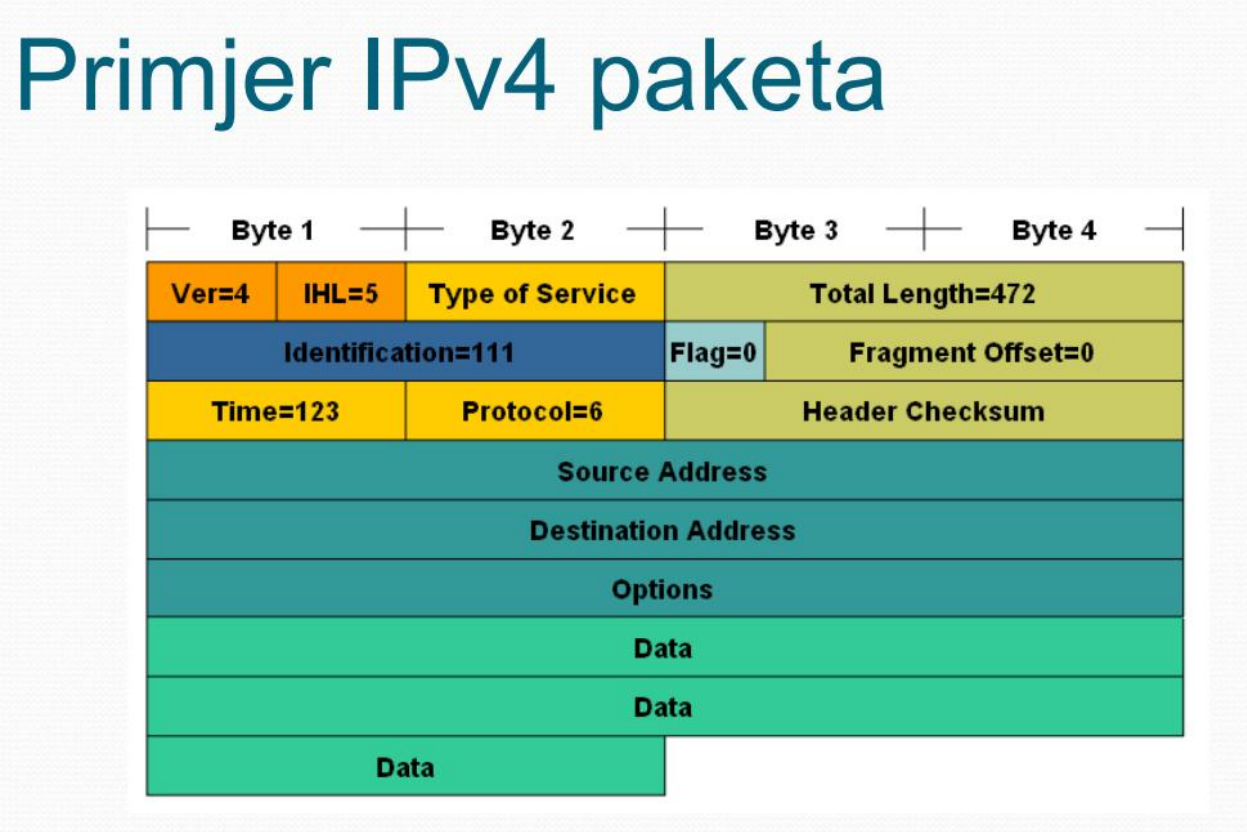


IPv4 Header



Legend

- Fields **kept** in IPv6
- Fields **kept** in IPv6, but name and position changed
- Fields **not kept** in IPv6
- Fields that are **new** in IPv6



Naravno, hajde da objasnimo **svako polje u IPv4 paketu** detaljno na osnovu tvoje slike:

---

1. Ver (Version)

- **Dužina:** 4 bita.
- **Funkcija:** Označava verziju IP protokola koji se koristi.
    - **Primjer:** 4 za IPv4, 6 za IPv6.
- **Kada se koristi:** Ovaj broj omogućava mrežnim uređajima da znaju kako da interpretiraju paket (npr. da li je IPv4 ili IPv6).

---

2. IHL (Internet Header Length)

- **Dužina:** 4 bita.
- **Funkcija:** Označava dužinu zaglavlja paketa u broju 32-bitnih riječi.
    - Vrijednost 5 znači da je zaglavlje dugačko 5 × 32 bita = 20 bajtova (minimalna dužina bez opcija).
- **Kada se koristi:** Koristi se za identifikaciju gdje počinju podaci (payload) u paketu.

---

3. Type of Service (ToS)

- **Dužina:** 8 bita.
- **Funkcija:** Označava prioritet paketa i klasu usluge (QoS - Quality of Service).
    - Koristi se za kategorizaciju saobraćaja, npr. video, glasovne podatke ili e-mail.
- **Kada se koristi:** Kod mreža koje imaju različite prioritete za različite vrste podataka.

---

4. Total Length

- **Dužina:** 16 bita.
- **Funkcija:** Označava ukupnu dužinu paketa (zaglavlje + podaci), izraženo u bajtovima.
    - Na primjer, vrijednost 472 znači da paket ima 472 bajta.
- **Kada se koristi:** Kada se podaci moraju segmentirati ili ponovo sastaviti.

---

5. Identification

- **Dužina:** 16 bita.
- **Funkcija:** Jedinstveno označava fragment paketa. Koristi se za identifikaciju fragmenata istog paketa kada je fragmentacija potrebna.
    - Vrijednost 111 u primjeru označava paket.
- **Kada se koristi:** Kada se paket dijeli na fragmente radi lakšeg prenosa preko mreže.

---

6. Flags

- **Dužina:** 3 bita.
- **Funkcija:** Kontrolišu fragmentaciju paketa.
    - **Bitovi:**
        - 1. bit: Rezervisan, uvijek 0.
        - 2. bit: **DF (Don’t Fragment):** Ako je postavljen, paket se ne fragmentira.
        -

3. bit: **MF (More Fragments):** Ako je postavljen, označava da slijedi još fragmenata.

    - Vrijednost 0 znači da nema fragmentacije.

- **Kada se koristi:** Kod upravljanja fragmentacijom podataka.

---

7. Fragment Offset

- **Dužina:** 13 bita.
- **Funkcija:** Označava mjesto fragmenta unutar originalnog paketa.
    - Vrijednost 0 znači da fragmentacija nije izvršena.
- **Kada se koristi:** Kod ponovnog sastavljanja fragmenata.

---

8. Time to Live (TTL)

- **Dužina:** 8 bita.
- **Funkcija:** Ograničava životni vijek paketa u mreži. Smanjuje se za 1 na svakom ruteru. Ako dostigne 0, paket se odbacuje.
    - Vrijednost 123 znači da paket može proći kroz 123 rutera prije odbacivanja.
- **Kada se koristi:** Da spriječi beskonačno kruženje paketa u mreži.

---

9. Protocol

- **Dužina:** 8 bita.
- **Funkcija:** Označava koji protokol se koristi za podatke unutar paketa.
    - Vrijednost 6 znači da je protokol **TCP**.
    - Ostali primjeri:
        - 1 za ICMP,
        - 17 za UDP.
- **Kada se koristi:** Ruteri koriste ovu informaciju za preusmjeravanje podataka ka odgovarajućem protokolu.

---

10. Header Checksum

- **Dužina:** 16 bita.

- **Funkcija:** Provjerava integritet zaglavlja paketa.
    - Ako je zaglavlje oštećeno, paket se odbacuje.
- **Kada se koristi:** Prilikom prolaska kroz svaki uređaj, kako bi se provjerila ispravnost zaglavlja.

---

11. Source Address

- **Dužina:** 32 bita.
- **Funkcija:** Označava IP adresu izvornog uređaja.
    - Npr., adresa uređaja koji šalje podatke.
- **Kada se koristi:** Ruteri koriste ovu adresu za odgovor nazad prema izvoru.

---

12. Destination Address

- **Dužina:** 32 bita.
- **Funkcija:** Označava IP adresu odredišnog uređaja.
    - Npr., adresa servera ili uređaja koji treba da primi podatke.
- **Kada se koristi:** Ruteri koriste ovu adresu za preusmjeravanje paketa.

---

13. Options

- **Dužina:** Promjenjiva.
- **Funkcija:** Sadrži dodatne opcije za specifične mrežne funkcije, kao što su sigurnosni podaci, vremenske oznake, itd.
- **Kada se koristi:** Ako su potrebne dodatne funkcionalnosti.

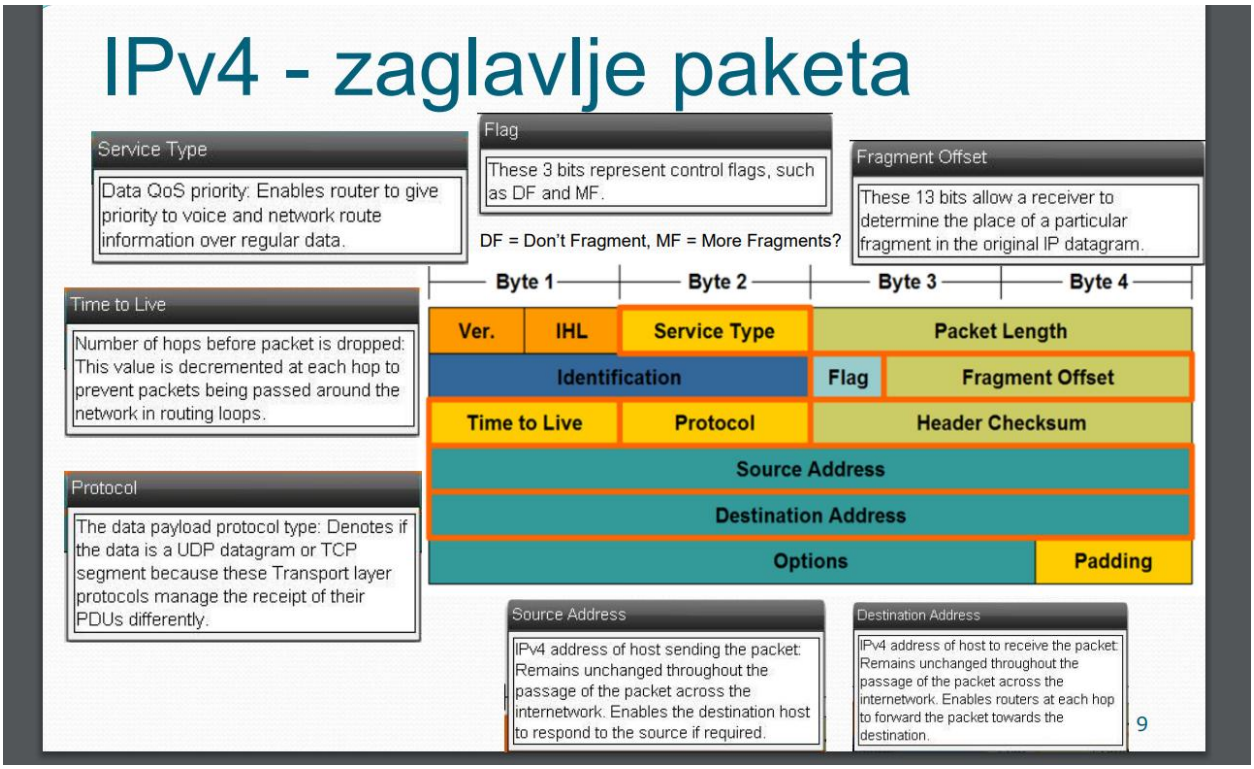
---

14. Data

- **Dužina:** Promjenjiva.
- **Funkcija:** Sadrži korisničke podatke (npr. HTTP zahtjev, fajl, e-mail).
- **Kada se koristi:** Ovo je glavni sadržaj paketa koji se šalje od izvora ka odredištu.

Sažetak:

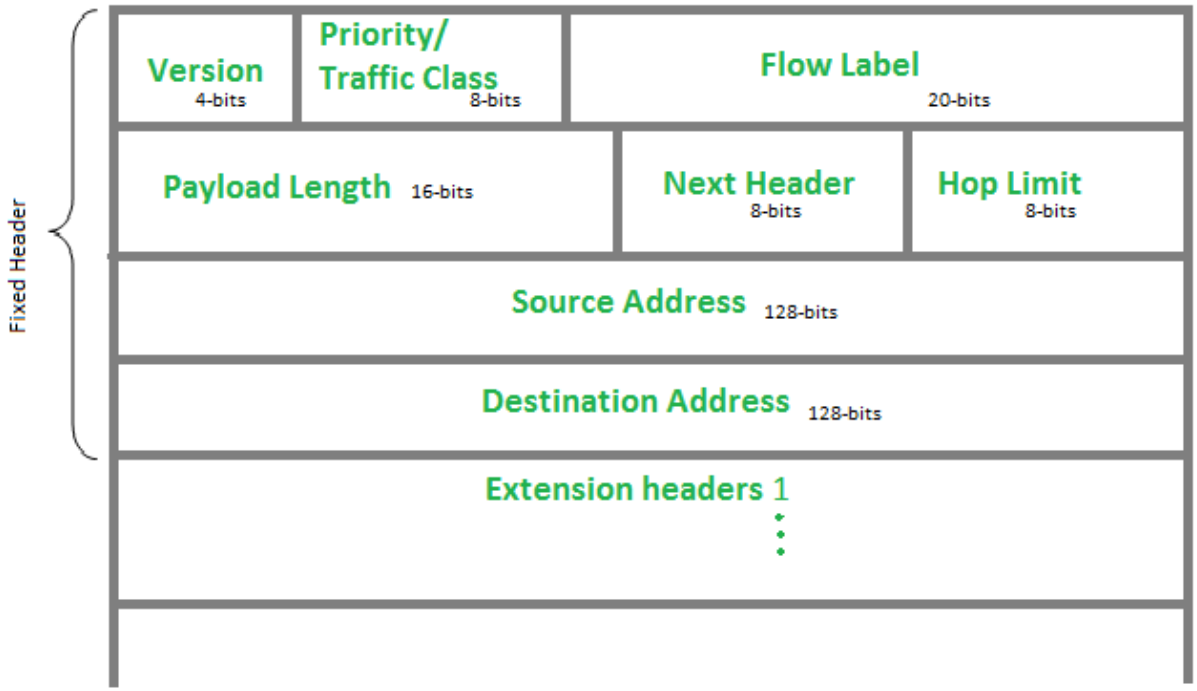
IPv4 paket je dizajniran da efikasno prenosi podatke kroz mreže, s detaljnim kontrolama fragmentacije, provjere grešaka, i usmjeravanja. Svako polje ima specifičnu ulogu kako bi komunikacija bila pouzdana i brza.



Klase IPv4 Adresa:

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			



Naravno, hajde da detaljno objasnimo svaki element **IPv6 zaglavlja** sa slike i čemu koje polje služi:

---

1. Version

- **Dužina:** 4 bita.
- **Funkcija:** Označava verziju IP protokola koji se koristi.
    - Vrijednost 6 znači da se koristi IPv6 protokol.
- **Kada se koristi:** Omogućava mrežnim uređajima da znaju kako interpretirati paket (IPv6 protokol).

---

2. Priority / Traffic Class

- **Dužina:** 8 bita.
- **Funkcija:** Sadrži dvije komponente:
    - **Traffic Class:** Označava prioritet paketa i koristi se za implementaciju QoS (Quality of Service).
    - Omogućava klasifikaciju saobraćaja (npr. video, glasovni podaci, e-mail).
- **Kada se koristi:** Kada mreža treba da upravlja prioritetima saobraćaja kako bi omogućila efikasniji protok podataka.

---

3. Flow Label

- **Dužina:** 20 bita.
- **Funkcija:** Identifikuje tok podataka koji pripadaju istom toku komunikacije između dva uređaja.
    - Koristi se za optimizaciju ruta i resursa za specifične tokove (npr. VoIP ili video strimovi).
- **Kada se koristi:** Kada je potrebno osigurati stabilan kvalitet komunikacije za specifične aplikacije.

---

4. Payload Length

- **Dužina:** 16 bita.
- **Funkcija:** Označava dužinu korisničkih podataka (payload) u bajtovima, ne uključujući osnovno zaglavlje (40 bajtova).
- **Kada se koristi:** Kada uređaji trebaju da znaju koliko podataka obrađuju ili prenose.

---

5. Next Header

- **Dužina:** 8 bita.
- **Funkcija:** Označava koji protokol dolazi poslije osnovnog IPv6 zaglavlja.
    - Vrijednosti:
        - 6 za TCP,
        - 17 za UDP,
        - 58 za ICMPv6.
- **Kada se koristi:** Za identifikaciju sadržaja paketa ili dodatnih zaglavlja (extension headers).

---

6. Hop Limit

- **Dužina:** 8 bita.
- **Funkcija:** Brojač koji ograničava broj rutera kroz koje paket može proći prije nego što se odbaci.
    - Vrijednost se smanjuje za 1 na svakom ruteru.
    - Ako dosegne 0, paket se odbacuje.
- **Kada se koristi:** Sprečava beskonačno kruženje paketa u mreži.

---

7. Source Address

- **Dužina:** 128 bita.
- **Funkcija:** Sadrži IPv6 adresu uređaja koji je poslao paket.
    - Koristi se za identifikaciju izvora podataka.
- **Kada se koristi:** Ruteri i drugi uređaji koriste ovu adresu za odgovaranje nazad pošiljaocu.

---

8. Destination Address

- **Dužina:** 128 bita.
- **Funkcija:** Sadrži IPv6 adresu odredišnog uređaja.
    - Koristi se za identifikaciju krajnjeg primatelja paketa.
- **Kada se koristi:** Ruteri koriste ovu adresu za isporuku paketa na ispravnu destinaciju.

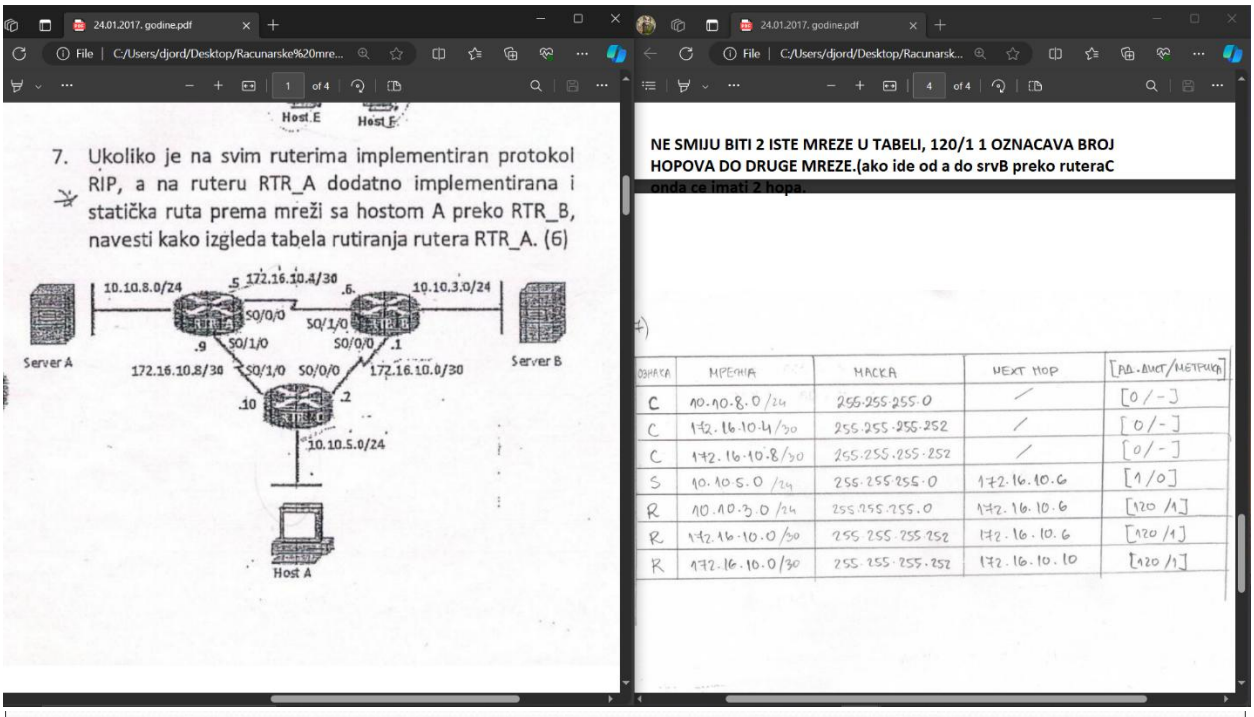
---

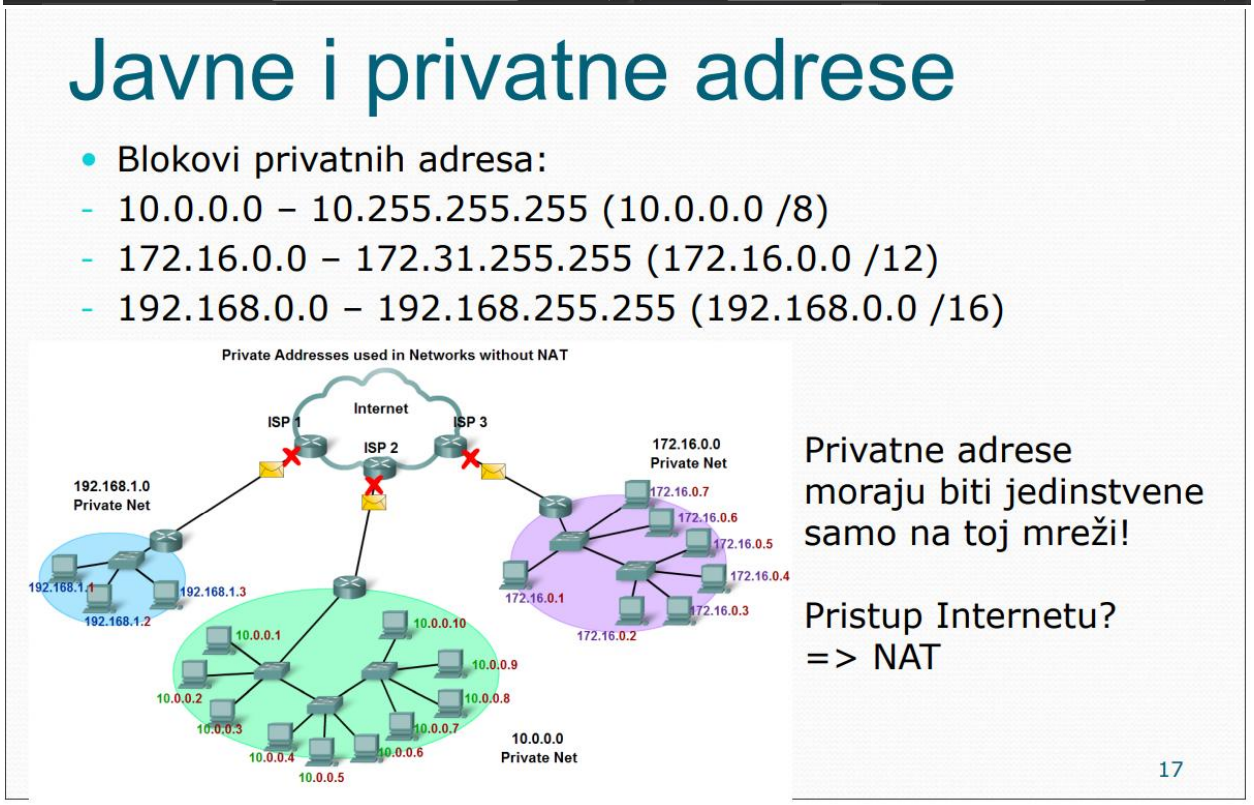
9. Extension Headers

- **Dužina:** Promjenjiva.
- **Funkcija:** Opcionalna zaglavlja koja omogućavaju dodatne funkcionalnosti, kao što su:
    - Sigurnost (IPSec),
    - Fragmentacija,
    - Informacije o stazi (routing),
    - Opcije za otklanjanje grešaka.
- **Kada se koristi:** Kada su potrebne napredne mrežne funkcionalnosti koje nisu pokrivene osnovnim zaglavljem.

Sažetak:

IPv6 paket ima pojednostavljeno osnovno zaglavlje u odnosu na IPv4, ali sadrži opcionalne **extension headers** za dodatnu fleksibilnost i funkcionalnost. Osnovno zaglavlje je uvijek **fiksne dužine od 40 bajtova**, što pojednostavljuje obradu paketa.





Na osnovu ove slike, objasniću razliku između **javnih** i **privatnih IP adresa**, njihove opsege, kao i gdje i kako se koriste. Takođe ću pojasniti ulogu NAT-a.

Šta su javne IP adrese?

- **Javne adrese** su one koje su dostupne na internetu i moraju biti **jedinstvene globalno**.
- Koriste ih uređaji ili mreže koje žele direktan pristup internetu.
- Dodeljuju ih organizacije poput IANA (Internet Assigned Numbers Authority) ili lokalni RIR-ovi (Regional Internet Registries).
- **Primjer:** Adresa rutera koji povezuje privatnu mrežu na internet.

Šta su privatne IP adrese?

- **Privatne adrese** su rezervisane za upotrebu unutar lokalnih mreža i nisu dostupne direktno na internetu.
- Ove adrese ne moraju biti jedinstvene globalno, ali moraju biti **jedinstvene u okviru jedne lokalne mreže**.
- Koriste se za identifikaciju uređaja u lokalnoj mreži (npr. računari, telefoni, štampači).

Blokovi privatnih adresa (prema RFC 1918):

1. **10.0.0.0 – 10.255.255.255** (10.0.0.0/8)
2. **172.16.0.0 – 172.31.255.255** (172.16.0.0/12)
3. **192.168.0.0 – 192.168.255.255** (192.168.0.0/16)

Ovi blokovi su jasno označeni na slici i koriste se za razne privatne mreže.

Zašto privatne adrese ne mogu direktno na internet?

- Privatne adrese nisu jedinstvene na globalnom nivou, pa bi došlo do konflikta ako bi se koristile na internetu.
- Ruteri na internetu **blokiraju privatne adrese**.

Kako privatne mreže pristupaju internetu?

- **NAT (Network Address Translation):**
    - NAT je tehnologija koja omogućava uređajima sa privatnim IP adresama da komuniciraju sa internetom.
    - Prevođenjem privatnih adresa u jednu ili više javnih adresa, NAT omogućava pristup internetu dok zadržava sigurnost lokalne mreže.
    - NAT se obično implementira na ruterima.

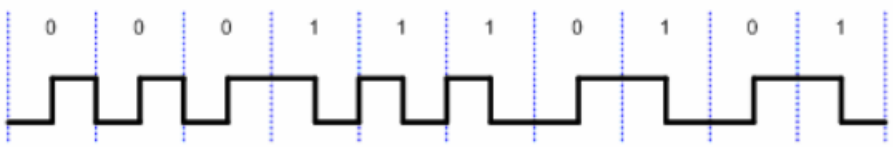
Prednosti privatnih adresa:

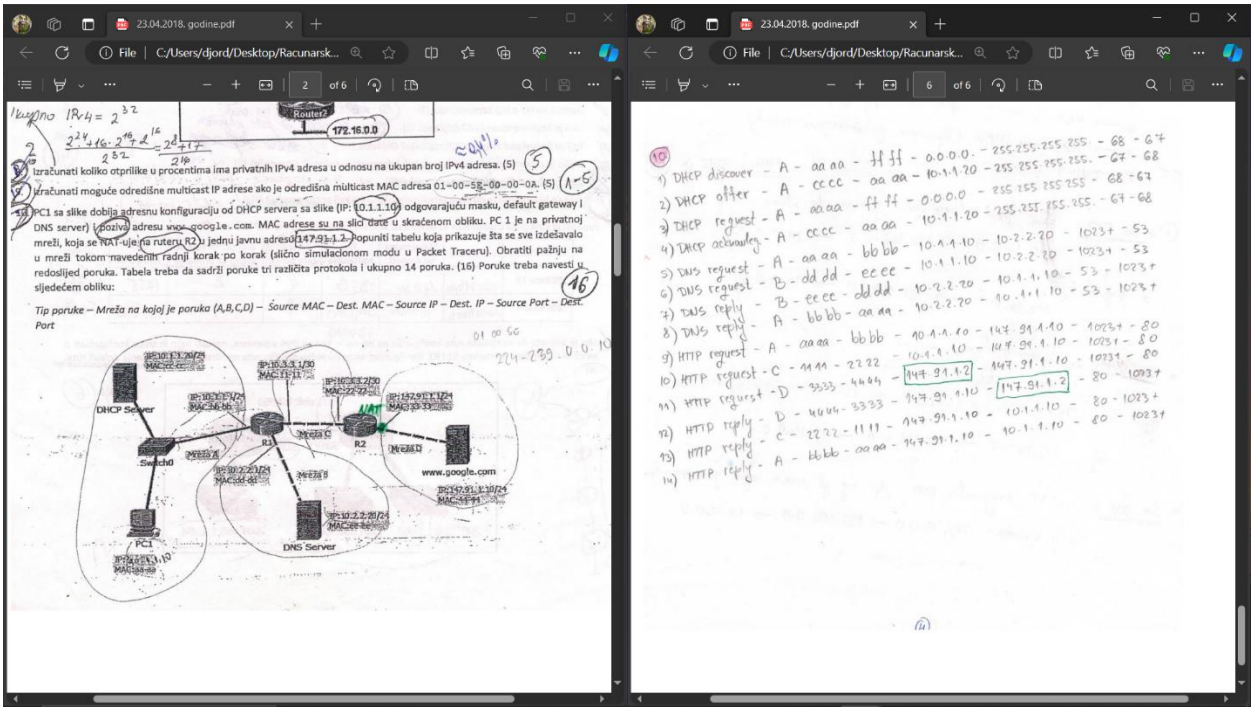
1. **Sigurnost:** Uređaji unutar privatne mreže nisu direktno izloženi internetu.
2. **Štednja IP adresa:** Koristeći privatne adrese, smanjuje se potreba za javnim adresama (što je ključno jer su IPv4 adrese ograničene).
3. **Fleksibilnost:** Administratori mreža mogu slobodno dodjeljivati adrese unutar svojih mreža.

Kada koristiti javne vs privatne adrese?

- **Privatne adrese:**
    - Kada se uređaji trebaju povezati samo unutar jedne mreže.
    - Primjer: Kancelarijski računari, kućni Wi-Fi uređaji.
- **Javne adrese:**
    - Kada se uređaj treba povezati direktno na internet.
    - Primjer: Web server, server e-pošte.

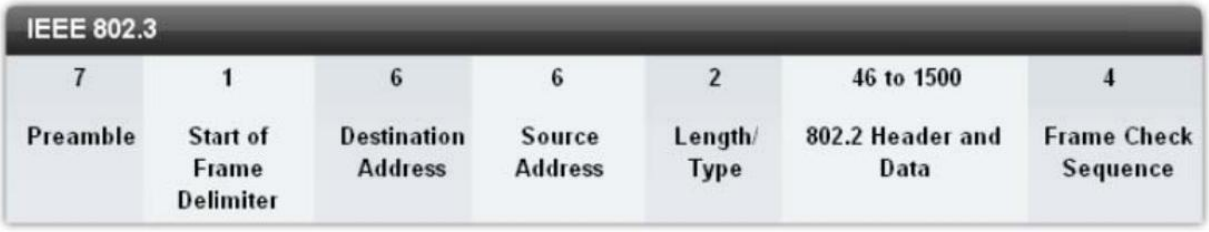
Manchester





7. Application	Sloj kojem krajnji korisnik pristupa
6. Presentation	Način reprezentovanja podataka
5. Session	Održavanje dijaloga
4. Transport	Adresiranje procesa i aplikacija, (ne)pouzdan prenos
3. Network	Određivanje puta i logičko adresiranje
2. Data Link	Priprema podataka za fizički prenos, fizičko adresiranje, otkrivanje grešaka
1. Physical	Fizički prenos bita pomoću signala

Polja Ethernet frame-a



IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length/ Type	802.2 Header and Data	Frame Check Sequence

- Preambula i SFD (7+1) – sinhronizacija
- ***Source*** i ***Destination*** MAC adresa (6+6)
- ***Length*** / ***Type*** (2) >= 0x0600 polje označava protokol, inače veličinu (bez preambule i SFD-a)
- ***Data*** & ***Pad*** (46-1500) – enkapsulirani paket sa višeg sloja; ukoliko je paket manji od minimalne dozvoljene veličine nadopunjuje se (***padding***)
- FCS (4) – detektovanje grešaka u frejmu, koristi CRC (***Cyclic Redundancy Check***), ne koristi preambulu i SFD u računanju

Reprezentacija adrese

- 128 bita
- x:x:x:x:x:x:x:x, x – 16-bitno heksadecimalno polje
- Vodeće nule su opcionalne
- Uzastopne nule mogu da se predstave kao ::, ali samo jednom u adresi!

- Primjeri:
  - 2031:0000:130F:0000:0000:09C0:876A:130B
    Ekvivalentno – 2031:0:130F::9C0:876A:130B,
    Ali ne može 2031::130F::09C0:876A:130B
  - FF01:0:0:0:0:0:0:1 → FF01::1
  - 0:0:0:0:0:0:0:1 → ::1
  - 0:0:0:0:0:0:0:0 → ::

Rezervisani adresni opsezi

- Ne mogu se koristiti sve adrese iz čitavog opsega (0.0.0.0 – 255.255.255.255)

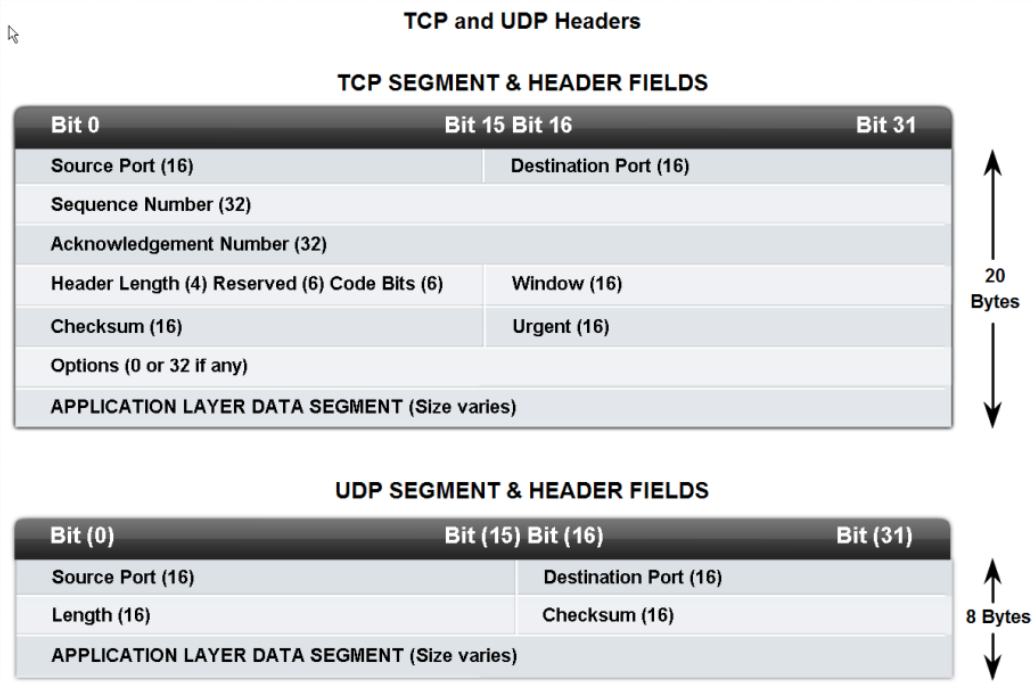
Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	• used for research or experimentation • cannot currently be used for hosts in IPv4 networks	240.0.0.0 to 255.255.255.254	1700 3330

Specijalne IPv4 adrese

- Ne mogu se dodijeliti hostovima:

1. Network i broadcast adrese – prva i posljednja adresa u mreži
2. Default route (0.0.0.0) – rezervisan cijeli blok 0.0.0.0/8
3. Loopback (127.0.0.1) – specijalna adresa za slanje samom sebi; rezervisan cijeli blok 127.0.0.0/8
4. Link-local adrese (169.254.0.0/16) – operativni sistem dodjeljuje ove adrese hostovima automatski kad nije dostupna IP konfiguracija; ne mogu se koristiti na javnoj mreži
5. TEST-NET adrese (192.0.2.0/24) – za svrhe učenja i predavanja; mogu se koristiti na javnoj mreži
6. Multicast i eksperimentalne adrese (na jednom od prethodnih slajdova)

TCP i UDP zaglavlja



Ova slika prikazuje **TCP** i **UDP zaglavlja** (header fields), koji su dio transportnog sloja u TCP/IP modelu. Svako polje ima svoju ulogu u uspostavljanju, upravljanju i prenošenju podataka.

TCP (Transmission Control Protocol):

TCP header je složeniji jer pruža pouzdanu komunikaciju. Ima minimalnu veličinu od **20 bajtova**, ali se može proširiti opcijama.

Polja TCP zaglavlja:

1. **Source Port (16 bita):**
   Identifikuje port na izvornoj strani (aplikaciji koja šalje podatke).
2. **Destination Port (16 bita):**
   Identifikuje port na odredištu (aplikaciji koja prima podatke).
3. **Sequence Number (32 bita):**
   Koristi se za redosled paketa. Oznaka početnog bajta u tekućem segmentu, pomaže u rekonstrukciji podataka.
4. **Acknowledgement Number (32 bita):**
   Ako je ACK bit postavljen, ovo polje pokazuje sledeći bajt koji se očekuje od prijemnika (potvrđuje prijem).

5. **Header Length (4 bita):**
   Ukazuje na dužinu TCP zaglavlja u 32-bitnim rečima (najmanje 5, što je 20 bajtova).
6. **Reserved (6 bita):**
   Rezervisano za buduću upotrebu. Uvek postavljeno na 0.
7. **Code Bits (6 bita):**
   Kontrolni bitovi (zastavice) za upravljanje vezom:
   - **URG:** Indikuje da je polje "Urgent Pointer" validno.
   - **ACK:** Pokazuje da je polje "Acknowledgement Number" validno.
   - **PSH:** Traži od prijemnika da odmah prosledi podatke aplikaciji.
   - **RST:** Resetuje vezu.
   - **SYN:** Koristi se za uspostavljanje veze.
   - **FIN:** Zatvara vezu.
8. **Window (16 bita):**
   Veličina prozora za kontrolu protoka. Pokazuje koliko bajtova prijemnik može da primi bez potvrde.
9. **Checksum (16 bita):**
   Proverava greške u zaglavlju i podacima.
10. **Urgent Pointer (16 bita):**
    Ako je **URG** zastavica postavljena, ukazuje na poziciju urgentnih podataka.
11. **Options (promenljive dužine):**
    Opcionalne informacije, kao što su maksimalna veličina segmenta (MSS).
12. **Application Layer Data Segment:**
    Podaci koji se prenose od aplikacije.

UDP (User Datagram Protocol):

UDP header je jednostavniji jer ne pruža pouzdanost, već fokusira na brzinu. Uvek ima fiksnu veličinu od **8 bajtova**.

Polja UDP zaglavlja:

1. **Source Port (16 bita):**
   Port izvora, može biti postavljen na 0 ako nije potreban.
2. **Destination Port (16 bita):**
   Port odredišta na kojem prijemnik sluša podatke.

3. **Length (16 bita):**
   Ukupna dužina UDP zaglavlja i podataka (u bajtovima).
4. **Checksum (16 bita):**
   Proverava greške u zaglavlju i podacima. Može biti opcionalno.
5. **Application Layer Data Segment:**
   Podaci aplikacije koja koristi UDP.

Ključne razlike između TCP i UDP zaglavlja:

- **TCP je složeniji** i koristi dodatna polja za pouzdanu komunikaciju, kontrolu toka i potvrdu.
- **UDP je jednostavniji**, nema potvrdu prijema i koristi se tamo gde je brzina važnija od pouzdanosti (npr. video streaming).

U Ethernet okviru (Ethernet Frame), nakon završetka **IPv4 paketa** (ili bilo kog protokola mrežnog sloja, npr. IPv6), počinje **transportni sloj**, što je obično **UDP** ili **TCP**.

Sekvenca slojeva unutar Ethernet okvira:

1. **Ethernet Frame Header:**
   - **Destinacijska MAC adresa (6 bajtova)**
   - **Izvorna MAC adresa (6 bajtova)**
   - **EtherType (2 bajta):** Oznaka koji protokol mrežnog sloja sledi (npr. 0x0800 za IPv4, 0x86DD za IPv6).
2. **IPv4/IPv6 paket:**
   - Počinje sa zaglavljem mrežnog sloja (npr. IPv4 ili IPv6).
   - Sadrži informacije o rutiranju i mrežnim adresama.
3. **TCP/UDP segment:**
   - Ovo je transportni sloj. Nakon mrežnog sloja, dolazi TCP ili UDP zaglavlje, koje se koristi za komunikaciju između aplikacija.
   - Prvi bajt posle IPv4 zaglavlja biće **Source Port** u TCP/UDP zaglavlju.
4. **Aplikacijski podaci:**
   - Nakon transportnog sloja dolaze podaci koji se prenose iz aplikacije (npr. HTTP, DNS, ili bilo koji drugi aplikacijski protokol).

Detaljniji primer (npr. za UDP preko IPv4 unutar Ethernet okvira):

- **Ethernet Header (14 bajtova):**
  - Destinacijska i izvorna MAC adresa + EtherType (0x0800 za IPv4).

- **IPv4 paket:**
    - Zaglavlje (20 bajtova ako nema opcija).
    - Sadrži protokolni broj u polju "Protocol" (npr. 17 za UDP, 6 za TCP).
- **UDP segment:**
    - UDP zaglavlje (8 bajtova).
    - Podaci aplikacije.

Ključni deo:

Protokolni broj u IPv4 zaglavlju (**Protocol field**) određuje šta dolazi nakon IPv4 paketa:

- **6 (TCP)** - Počinje TCP segment.
- **17 (UDP)** - Počinje UDP segment.

Dakle, nakon što mrežni sloj (IPv4/IPv6) završi, transportni sloj (TCP/UDP) preuzima prenos podataka prema aplikacijama.

Port	Protokol	Internet servis/aplikacija
20, 21	TCP	File Transfer Protocol (FTP)
22	TCP, UDP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP, UDP	Domain Name System (DNS)
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	HyperText Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP3)
123	UDP	Network Time Protocol (NTP)
143	TCP, UDP	Internet Message Access Protocol (IMAP)
161, 162	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP Secure (HTTPS)

Tipovi fizičkih medijuma

Physical Media - Characteristics

Ethernet Media

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX	1000BASE-ZX	10GBASE-ZR
Media	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 3, 4, 5 UTP, two pair	50/62.5 µm multi mode fiber	STP	EIA/TIA Category 3, 4, 5 UTP, four pair	62.5/50 micron multimode fiber	50/62.5 micron multimode fiber or 9 micron single mode fiber	9µm single mode fiber	9µm single mode fiber
Maximum Segment Length	100m (328 feet)	100m (328 feet)	2 km (6562 ft)	25 m (82 feet)	100 m (328 feet)	Up to 550 m (1,804 ft) depending on fiber used	550 m (MMF)10 km (SMF)	Approx. 70 km	Up to 80 km
Topology	Star	Star	Star	Star	Star	Star	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)				