

1.

Djelovanje u mrežnom sloju OSI modela

- 1.1. Zadaće i djelovanje u mrežnom sloju OSI modela**
- 1.2. Adresiranje IPv4**
- 1.3. Podmrežavanje u IPv4**
- 1.4. Adresiranje IPv6**

1.1.

Zadaće i djelovanje u mrežnom sloju OSI modela

o Nakon ove nastavne teme moći ćeš:

- o opisati komunikaciju na mrežnom sloju OSI modela
- o opisati funkcije mrežnog sloja
- o objasniti usmjeravanje paketa u računalnoj mreži
- o opisati dijelove paketa i njihovu ulogu u procesu usmjeravanja
- o objasniti načela i funkcije IP protokola
- o objasniti pojam fragmentacije
- o objasniti ICMP protokol
- o usporediti ARP i RARP protokole.

Komunikacijom računala i mrežnih uređaja u istoj mreži upravljaju samo njihove mrežne kartice. Komunikacija se odvija samo na razini fizičkih, MAC adresa pa u komunikaciji mrežnim uređajima ne sudjeluju protokoli mrežnog sloja. Kako bi se mogla odvijati komunikacija između uređaja koji se nalaze u različitim računalnim mrežama, potrebne su usluge protokola mrežnog sloja OSI modela.

Mrežni sloj OSI modela, kao i internetski sloj TCP/IP modela pruža tri osnovne funkcije:

- adresiranje
- enkapsulaciju ili dekapulaciju u pakete
- usmjeravanje.

Ako promatramo TCP/IP model komunikacije računalnom mrežom, internet sloj prihvaća podatke od sloja pristupa mreži te ih predaje transportnom sloju. Isto tako, u OSI modelu mrežni sloj prihvaća podatke od sloja podatkovne poveznice i predaje ih transportnom sloju. **Osnovna jedinica podataka** na ovoj razini komunikacije jest **paket**.

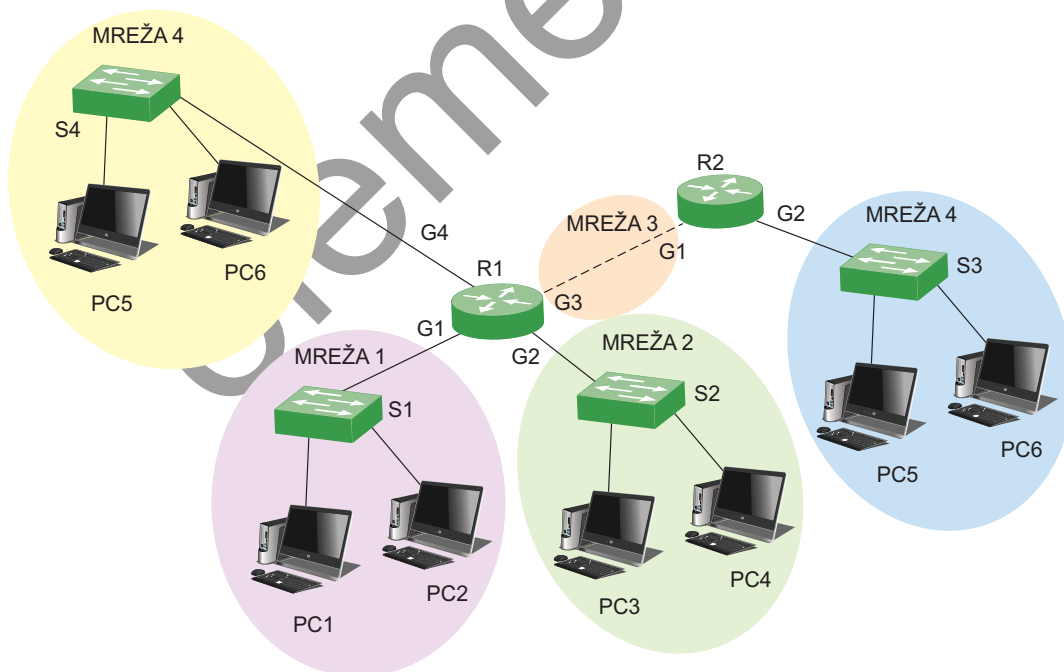
Na uređaju primatelju podataka **mrežni sloj** OSI modela **dekapsulira okvire u pakete** podižući razinu komunikacije s fizičkih u **logičke adrese**. Na uređaju pošiljatelju **segmente enkapsulira u pakete**, pripremajući dijelove korisničke poruke za put mrežom i uspostavljaajući logičke veze između dvaju uređaja koja komuniciraju.

Funkcije mrežnog sloja su dakle:

- jedinstveno i hijerarhijsko adresiranje svih hostova
- utvrđivanje ruta i procjena njihove učinkovitosti
- nalaženje optimalnog puta do odredišta
- učinkovito adresiranje i upravljanje mrežnim adresama
- hijerarhijsko strukturiranje mrežnih adresa
- slanje paketa do odredišta prema načelu da usmjernik „daje sve od sebe” (engl. *best effort*) da paket stigne do odredišta.

U drugom razredu, u predmetu Uvod u računalne mreže, naučili ste da **protokoli mrežnog sloja isporučuju pakete od izvora do odredišta kroz više mreža ili podmreža, usmjeravajući signal** kroz različite kanale iz jednog čvora u drugi.

Usmjernik, uređaj mrežnog sloja OSI modela, **povezuje mreže i pri tome odlučuje koja je najbolja putanja za slanje podataka. Svaki priključak** usmjernika pripada **različitoj mreži, zasebna je kolizijska i zasebna sveodredišna domena**. Proces usmjeravanja i osnovnu konfiguraciju usmjernika ponovit ćemo detaljnije u 2. poglavlju i zatim proširiti znanje novim nastavnim sadržajima.



Slika 1.1. Usmjernici R1 i R2 i njihove izravno povezane i udaljene mreže

Komunikacijom na mrežnoj razini, neposredno i posredno, upravljaju protokoli:

- **IP** (engl. *Internet Protocol*)
- **ICMP** (engl. *Internet Control Message Protocol*)
- **ARP** (engl. *Address Resolution Protocol*)
- **RARP** (engl. *Reverse Address Resolution Protocol*)
- **DHCP** (engl. *Dynamic Host Configuration Protocol*)
- **dinamički protokoli usmjeravanja** kao što su na primjer **RIPv1** (engl. *Routing Information Protocol version 1*) i **RIPv2** (engl. *Routing Information Protocol version 2*) te **OSPF** (engl. *Open Shortest Path First*) konfiguriraju se na usmjerniku. Dinamičkim protokolima usmjeravanja bavit ćemo se detaljnije u zasebnom poglavlju ovog udžbenika.

1.1.1. IP

IP (engl. *Internet Protocol*), standardiziran standardom RFC 791 temeljni je protokol **mrežnog sloja OSI modela**, kao i **internetskog sloja** modela TCP/IP.

U računalnoj je mreži **logičko adresiranje** ostvareno na razini mrežnog sloja primjenom **IP protokola**.

Trenutačno se primjenjuju dvije inačice IP protokola:

- **IPv4**
- **IPv6**.

Adresni prostor postao je daleko premalen za sve potrebe. Danas je područje mobilne telefonije integrirano s internetom, različiti uređaji kao kućanski aparati, razni uređaji u industriji i prometu koriste se internetom za razmjenu i prikupljanje informacija, komunikaciju, upravljanje na daljinu i sl.

Inačica protokola IPv6 razvijena je zbog nedostatka adresa u inačici IPv4. Kako se **IPv4 adresa** sastoji od **32 bita**, a **IPv6 adresa** od **128 bitova**, njome je moguće adresirati puno više uređaja nego u IPv4-u. U IPv4 maksimalni broj različitih adresa je 2^{32} ili približno $4,3 \cdot 10^9$, a u IPv6 ukupno 2^{128} , odnosno $3,4 \cdot 10^{38}$. Danas se primjenjuju oba protokola, a tako će biti i u nekoliko idućih godina jer su u instalacijama interneta u mnogim dijelovima svijeta još uvijek u funkciji usmjernici koji rade s adresama u protokolu IPv4. Postupnim obnavljanjem instalacija bit će zamijenjeni uređajima koji rade u IPv6.

Adresiranjem u inačicama IPv4 i IPv6 bavit ćemo se u poglavljima 1.2 i 1.3 ovog udžbenika.

Osnovne funkcije IP protokola su:

- definiranje sheme adresiranja na internetu
- definiranje IP paketa
- prosljeđivanje podataka između podatkovne i transportne razine
- prosljeđivanje paketa do određene mreže ili podmreže.

Da bi dva hosta komunicirala s pomoću IP protokola, ne moraju uspostaviti sesiju. Uspoređivanjem IP adrese odredišnog hosta s izvorišnom IP adresom, IP protokol utvrđuje može li se paket izravno poslati odredišnom hostu ili usmjernik treba propaći putanju.

Podsjetimo se, host je računalo ili mrežni uređaj koji komunicira s ostalim računalima i mrežnim uređajima na mreži preko sučelja na kojima je konfigurirana IP adresa. Svaki host može u računalnoj mreži biti konfiguriran kao korisnik i poslužitelj.

IP je **bespojni** (engl. *connectionless*) protokol, što znači da se uređaj pošiljatelj i uređaj primatelj ne dogovaraju o početku ili završetku prijenosa podataka. **Pošiljatelj** pošalje paket i **nema potvrde** primitka paketa. Kako IP protokol ni na koji način ne provjerava isporuku paketa i nema mehanizme kojima bi se informacija sigurno prenijela na odredište, **nema niti garancije pouzdane isporuke informacije**. Tako paketi mogu biti izgubljeni ili stići nepredviđenim redoslijedom.

Zato protokoli viših razina obavljaju:

- **otkrivanje pogrešaka u prijenosu**
- **otklanjanje pogrešaka u prijenosu**
- **kontrolu protoka**
- **kontrolu redoslijeda paketa.**

IP paket sastoji se od dvaju osnovnih dijelova:

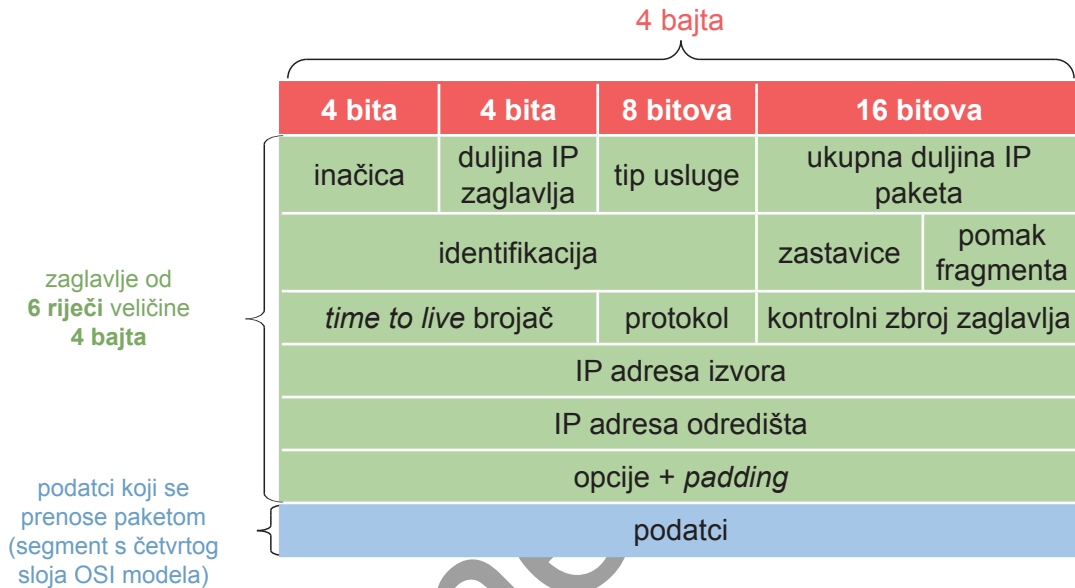
- **IP zaglavljaja**
- **IP tijela.**

IP zaglavljaje može imati duljinu do 6 riječi po 32 bajta, a nakon njega u IP tijelu slijede podatci koji se prenose mrežom. Ti **su podatci zapravo segment** enkapsuliran na transportnoj razini OSI modela.

Na mrežnoj razini OSI modela paketi se usmjeravaju do odredišta na osnovi IP adrese odredišta. U slučaju da količina podataka koja se treba prenijeti paketom prijeđe dopuštenu veličinu mrežnog paketa, paket mora biti **fragmentiran**. Ako je segment prevelik za prijenos jednim paketom, on se dijeli u više dijelova, fragmenata i prenosi s pomoću više paketa. Taj se proces razlaganja segmenta na nekoliko paketa naziva

fragmentacija. Dolaskom na odredište uspostavlja se ispravan redosljed i cjelovitost informacije svakog pojedinog paketa s pomoću podataka iz zaglavlja.

Na slici 1.2 prikazana je struktura paketa u IPv4. Sastoji se od sljedećih polja bitova:



Slika 1.2. Struktura IP paketa

Značenja polja IP paketa su:

- **inačica** (duljine 4 bita) – ukazuje na trenutačno korištenu inačicu IP-a, određuje format zaglavlja.
- **duljina IP zaglavlja** (duljine 4 bita) – označava koliko 32-bitnih riječi sadržava IP zaglavlje; omogućava određivanje početka podatkovnog dijela paketa; minimalna duljina ispravnog zaglavlja je 5.
- **tip usluge** (duljine 8 bitova) – označava vrstu prometa te željenu razinu usluge, ovo polje je bitno ako imamo prioritetni promet u mreži, omogućava usmjernici-ma različit tretman pojedinih paketa u cilju postizanja zadovoljavajuće kvalitete usluge (engl. *Quality of Service*, QoS), a s obzirom na dopušteno kašnjenje, količinu prometa i zahtijevanu pouzdanost. Zadaća QoS-a je i pružanje prioriteta prilikom izbora jednoga ili više protoka podataka tako da ostali protoci podataka trpe propuste, to jest pruža im se smanjena propusnost. Suvremene podatkovne mreže nude različite usluge, uključujući glasovne poruke, video-zapise, streaming glazbe, *web*-stranice i e-poštu. Mnogi od predloženih mehanizama QoS koji su omogućili koegzistenciju ovih usluga bili su složeni i nisu uspješni odgovoriti na zahtjeve javnog interneta.

- **ukupna duljina IP paketa** (duljine 16 bitova) – određuje duljinu cijelog IP paketa, uključujući podatke i zaglavlje, u bajtovima; najveća duljina paketa je 65 535 okteta (s obzirom na 16-bitno polje u koje se ta duljina upisuje).
- **identifikacija** (duljine 16 bitova) – sadržava cijeli broj koji identificira trenutačni paket, a rabi se za rekonstrukciju fragmenata paketa pri povezivanju svih fragmenata u paket.
- **zastavice** (duljine 4 bita; jedan se ne koristi) – kontroliraju dopušta li se usmjerenicima fragmentacija paketa i označava dijelove paketa za primatelja.
- **pomak fragmenta** – definira mjesto fragmenta u originalnom paketu, mjereno u jedinicama od 8 okteta; odstupanje prvog fragmenta je nula.
- „**Time to Live**”, TTL (duljine 8 bitova) – brojač koji označava vrijeme postojanja paketa u mreži; predstavlja broj čvorova koje paket može prijeći do odredišta. Pritom se uzima u obzir trajanje obrade paketa od strane svakog čvora, u dijelovima sekundi. Čvor koji obrađuje paket umanjuje vrijednost brojača za najmanje 1, a kad vrijednost polja dosegne nulu, paket se odbacuje, uklanja s mreže. Time se sprječavaju beskonačne petlje paketa do kojih može doći uslijed poremećaja u tablicama usmjeravanja.
- **protokol** (duljine 8 bitova) – označava kojem se protokolu više razine podatci prosljeđuju.
- **kontrolni zbroj zaglavlja** (duljine 16 bitova) – pomaže osigurati integritet IP zaglavlja; ponovno se obračunava i provjerava pri svakoj promjeni podataka u zaglavlju.
- **IP adresa izvora** (duljine 32 bita) – određuje IP adresu hosta pošiljatelja paketa.
- **IP adresa odredišta** (duljine 32 bita) – određuje IP adresu hosta primatelja paketa.
- **opcije** + **padding** (duljine 32 bita) – opcije, sadrže kontrolne informacije o usmjeravanju, sigurnosne parametre i sl. *Padding* je nadopuna bitova u registru nulama do duljine 32 bita. Oba su dijela varijabilne duljine.
- **podatci** (polja duljine 32 bita) – sadržavaju podatke gornjeg sloja, najveće duljine $65\,535 - 6 = 65\,529$ okteta.

Na slici 1.3 prikazano je bojom označeno zaglavlje IP paketa.

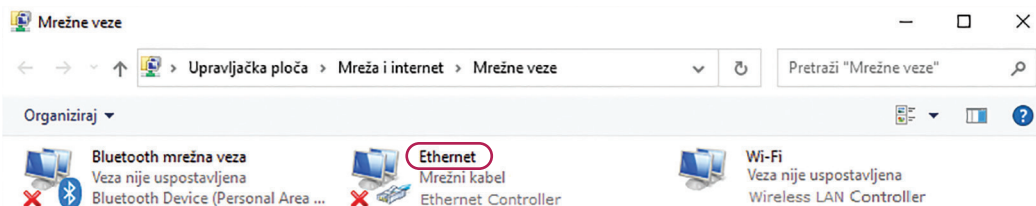
```

Internet Protocol Version 4, Src: 172.20.1.31 (172.20.1.31), Dst: 172.20.1.32 (172.20.1.32)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capab
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 60
  Identification: 0x5887 (22663)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (1)
  Header checksum: 0x5eaa [correct]
  Source: 172.20.1.31 (172.20.1.31)
  Destination: 172.20.1.32 (172.20.1.32)

0000 00 30 64 25 f4 00 00 91 05 6c 5b 08 00 45 00  .Od%o... ..][..E.
0010 00 3c 58 87 00 00 80 01 5e aa ac 14 01 1f ac 14  .<X.... ^.....
0020 01 20 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66  ..MZ.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdfgh hi
  
```

Slika 1.3. Zaglavlje IP paketa

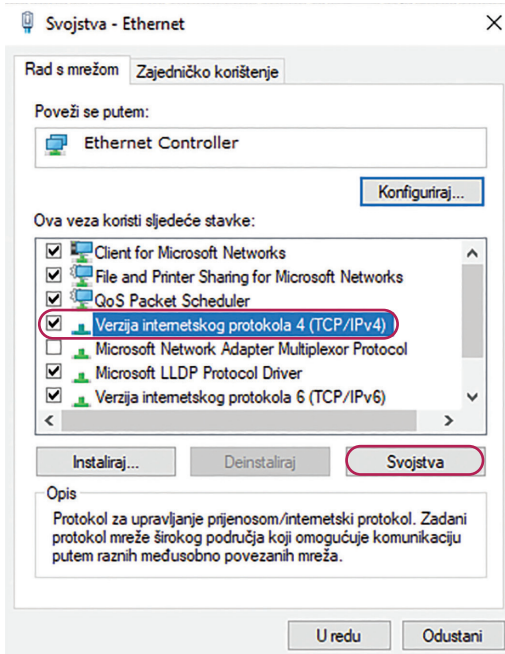
Iskazuje li neko računalo probleme pri povezivanju s internetom i ako dijagnostika računala i nakon ponovnog pokretanja usmjernika nije ukazala na neki drugi problem, ponekad je potrebno **ponovno namjestiti automatsko dobivanje IP adrese računala te IP adrese glavnog i rezervnog DNS poslužitelja**. U većini kućnih mreža u normalnim okolnostima usmjernik će dodijeliti adrese uređajima kako se spajaju. Ne dobiju li valjanu IP adresu, to može biti uzrokom problema. Adresa DNS poslužitelja može se i promijeniti ako je primijećeno da je internetska veza usporena, a pružatelj internetskih usluga (ISP) i korisnik uklonili su sve druge moguće razloge. U sučelju „**Mrežne veze**” odabrana je **Ethernet veza** (slika 1.4), a desnim klikom na nju odabrano je sučelje „**Svojstva**” (slika 1.5).



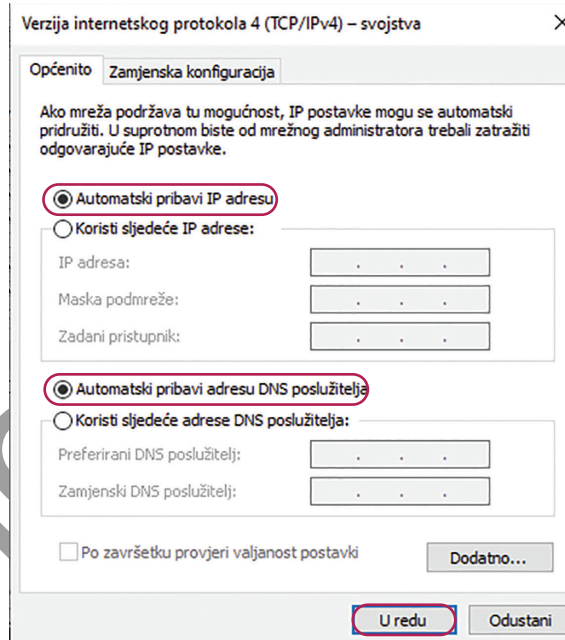
Slika 1.4. Sučelje „Mrežne veze”, odabir sučelja „Svojstva” Ethernet veze

U otvorenom prozoru „Svojstva – Ethernet” odabire se „Inačica internetskog protokola 4 (TCP/IPv4)”. (slika 1.5).

Na kraju se u otvorenom prozoru odabire „Automatski pribavi IP adresu” te „Automatski pribavi adresu DNS poslužitelja”. Na kraju se klikne na gumb „U redu” (slika 1.6).



Slika 1.5. Prozor „Svojstva – Ethernet”



Slika 1.6. Automatsko pribavljanje IP adrese i adrese DNS poslužitelja

Ako opet nema IP adrese ili je internetska veza vrlo spora, korisno je poduzeti još tri koraka:

1. resetirati neke od datoteka koje Windows koristi za pristup internetu upotrebljavajući u naredbenom retku niz naredbi redom:

- netsh winsock reset
- netsh int ip reset

2. obnoviti IP adresu u naredbenom retku nizom naredbi redom:

- ipconfig /release
- ipconfig /renew

pri čemu će prvom naredbom računalo otpustiti IP adresu, a drugom će ju obnoviti

3. osvježiti postavke DNS-a u naredbenom retku naredbom:

- ipconfig /flushdns.

Nakon toga, ako opet nema rezultata, može se pokušati dobiti navedene adrese na sljedeće načine:

1. isključiti i ponovo uključiti mrežnu karticu
2. isključiti i ponovo uključiti mrežni kabel iz mrežne kartice
3. ponovo pokrenuti računalo.

IP fragmentacija

IP fragmentacija je proces internetskog protokola (IP) koji razbija pakete na manje dijelove (fragmente) tako da rezultirajući dijelovi mogu proći putem veze s manjom jedinicom za prijenos od izvorne veličine paketa. Prijamni domaćin ponovno sastavlja fragmente. Kada host pošalje IP paket na mrežu, paket ne može biti veći od maksimalne veličine koju podržava ta lokalna mreža. Ta je veličina određena mrežnom podatkovnom vezom (engl. Maximum Transmission Units, MTU) i IP-om koji su obično isti. Tipična suvremena Ethernet mreža ureda, kampusa ili podatkovnog centra imat će veličinu MTU-a od 1500 bajta.

Međutim, paketi koji se inicijalno prenose putem mreže koja podržava jedan MTU možda će se morati usmjeriti na mreže (kao što je WAN ili VPN tunel) s manjim MTU-om. U slučajevima kada veličina paketa premašuje niži MTU, podatci u paketu moraju biti fragmentirani (ako je moguće). To znači da je paket razbijen na dijelove koji se prenose unutar novih paketa (fragemnata) koji su jednaki ili manji od nižeg MTU-a. Taj se proces naziva fragmentacija, a podatci u tim fragmentima obično se ponovno sastavljaju kada stignu na svoje odredište. Fragmentacija se može dogoditi kod izvornog pošiljatelja ili na usmjernicima koji se nalaze između pošiljatelja i primatelja. Ako je IP datagram fragmentiran, prvo ga ponovno sastavlja primatelj ili eventualno interventni vatrozidi koji su konfigurirani za izvršavanje tzv. ponovno sastavljanje prije prosljeđivanja podataka. Ako je potrebno, paket koji je već fragmentiran može se **dodatno fragmentirati** (npr. kada se promijeni tehnologija prijenosa).

Svaki fragmentiran IP datagram dobiva novo zaglavlje na temelju izvornog zaglavlja i posebnih ažuriranih polja. U novim IP zaglavljima fragmenata pomak fragmenta označava položaj podataka koji se šalju u ovom paketu u odnosu na izvorni paket. Svi fragmenti osim posljednjeg imaju postavljenu **zastavicu Više fragmenata**. Duljina dotičnog fragmenta upisuje se u polje duljine IP zaglavlja za sve fragmente, a kontrolni zbroj IP zaglavlja izračunava se zasebno za svako zaglavlje, dok ostatak zaglavlja odgovara izvornom zaglavlju prije fragmentacije.

Prijamni host ima zadatak ponovno sastaviti izvornik iz informacija prisutnih u zaglavljima paketa uzimajući sve fragmente s istim IP zaglavljem (osim zasebnih informacija za svaki fragment) i stavljajući ih u ispravan redoslijed koristeći se njihovim pomacima. Budući da svaki pojedini fragment predstavlja samostalan paket, može se dogoditi i da ti pojedinačni dijelovi ne stignu u redu. Također je moguće da su po-