

---

# Mrežni sloj: podatkovna ravnina

Poglavlje 6 — Skripta kolegija *Računalne mreže*

---

doc. dr. sc. Sandi Baressi Šegota

Fakultet informatike Sveučilišta Jurja Dobrile u Puli

## Poglavlje 6

# Mrežni sloj: podatkovna ravnina

Mrežni sloj prenosi pakete od jednog hosta do drugog kroz mrežu rutera. Njegove se funkcije dijele na dvije *ravnine*: **podatkovnu** (koja svaki paket prosljeđuje s ulaza na ispravni izlaz rutera, vrlo brzo i po paketu) i **upravljačku** (koja računa tablice prosljeđivanja, tj. obavlja usmjeravanje). Ovo se poglavlje bavi podatkovnom ravninom: protokolom IP, adresiranjem, mehanizmima DHCP i NAT, protokolom IPv6 te **generaliziranim prosljeđivanjem** i SDN-om.

### Ishodi učenja

Po završetku poglavlja student će moći: razlikovati podatkovnu i upravljačku ravninu te prosljeđivanje i usmjeravanje; opisati IPv4 datagram i IP adresiranje (podmreže, CIDR, longest prefix match); objasniti DHCP i NAT; te opisati IPv6 i model „uvjet+akcija”.

## 6.1 Uloga mrežnog sloja i ruter

Dvije ključne funkcije mrežnog sloja jesu **prosljeđivanje** — lokalna radnja premještanja paketa na ispravni izlazni port jednog rutera — i **usmjeravanje** — globalni proces određivanja puta paketa kroz cijelu mrežu. Na Internetu je usluga *best-effort*: nema jamstva dostave, redoslijeda ni kašnjenja.

Iznutra, ruter čine *ulazni portovi* (koji obavljaju pretragu tablice prosljeđivanja), *sklopna mreža* (koja fizički premješta pakete) te *izlazni portovi* (s redovima čekanja). Kada promet prema nekom izlazu premaši njegov kapacitet, paketi se nakupljaju u redovima, a pri prepunjenom međuspremniku dolazi do gubitka. Ako se paketi drže u redovima na *ulazu*, može nastati *blokiranje čela reda* (*head-of-line blocking*): paket na čelu, koji čeka zauzeti izlaz, koči i pakete iza sebe iako bi oni mogli proći na slobodne izlaze. Zbog toga se u praksi teži brzim sklopnim mrežama i redovima na izlaznim portovima.



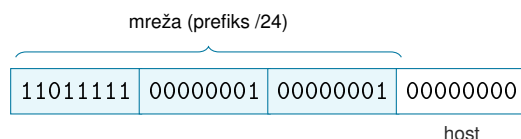
Figure 6.1: Pojednostavljena arhitektura rutera.

## 6.2 IP i adresiranje

**IPv4 datagram** nosi, uz podatke, zaglavlje s poljima kao što su verzija, ukupna duljina, identifikator i offset (za *fragmentaciju*), **TTL** (koji ograničava životni vijek paketa), oznaka

protokola višeg sloja te izvorišna i odredišna **IP adresa** (svaka 32 bita). Ako datagram premašuje *MTU* nekog linka, fragmentira se i ponovno sastavlja na odredištu.

IP adresa pripada *sučelju*, a ne uređaju, pa ruter ima više adresa (po jednu za svako sučelje). Skup sučelja koja se mogu doseći bez prolaska kroz ruter čini **podmrežu**, koja ima zajednički *prefiks*. U **CIDR** notaciji zapis  $223.1.1.0/24$  znači da je prvih 24 bita *mrežni dio*, a ostatak identificira host; ekvivalentna maska je  $255.255.255.0$ .



**Figure 6.2:** CIDR: adresa  $223.1.1.0/24$ , mrežni dio i dio za host.

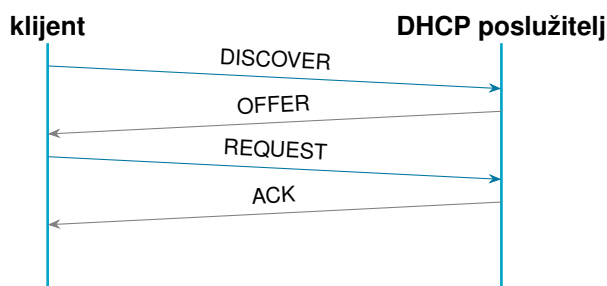
Pri prosljeđivanju ruter primjenjuje pravilo **longest prefix match**: među svim prefiksima koji odgovaraju odredišnoj adresi bira *najduži* (najspecifičniji). To omogućuje *agregaciju* ruta i finu kontrolu. Blokovi adresa dodjeljuju se hijerarhijski: ICANN → regionalni registri (RIR) → ISP-ovi → organizacije.

#### Primjer podjele na podmreže

Mrežu  $192.168.1.0/24$  (256 adresa) možemo podijeliti na četiri jednake podmreže povećavši prefiks na  $/26$  (64 adrese svaka):  $192.168.1.0/26$ ,  $192.168.1.64/26$ ,  $192.168.1.128/26$  i  $192.168.1.192/26$ . U svakoj je jedna adresa mrežna, jedna broadcast, a preostale su iskoristive za hostove. Posebne su još adrese poput  $127.0.0.1$  (loopback) te privatni rasponi  $10.0.0.0/8$ ,  $172.16.0.0/12$  i  $192.168.0.0/16$ .

### 6.3 DHCP i NAT

Host adresu može dobiti ručno ili automatski putem protokola **DHCP**. Klijent emisijom šalje poruku DISCOVER, poslužitelj odgovara OFFER-om, klijent traži ponuđenu adresu REQUEST-om, a poslužitelj potvrđuje ACK-om. Uz IP adresu, DHCP daje i mrežnu masku, adresu *gatewaya* te adrese DNS poslužitelja. Budući da host u početku nema adresu, poruke putuju *emisijom* (broadcast) preko UDP-a; kada DHCP poslužitelj nije u istoj podmreži, posao preuzima *relejni agent* koji prosljeđuje zahtjeve. Adresa se dodjeljuje na *ograničeno vrijeme* (lease) te se povremeno obnavlja.



**Figure 6.3:** DHCP izmjena poruka (DISCOVER, OFFER, REQUEST, ACK).

**NAT** (*Network Address Translation*) omogućuje da cijela privatna mreža dijeli *jednu* javnu IP adresu. NAT ruter pri odlasku prepisuje izvorišnu privatnu adresu i port u svoju javnu adresu i novi port, bilježeći preslikavanje u *tablicu prijevoda*; pri povratku obavlja obrnuti postupak. NAT štedi javne adrese i skriva unutarnju mrežu, ali krši načelo kraj-do-kraja i

otežava dolazne veze (npr. P2P), zbog čega se koriste tehnike poput prosljeđivanja porta i STUN/TURN.

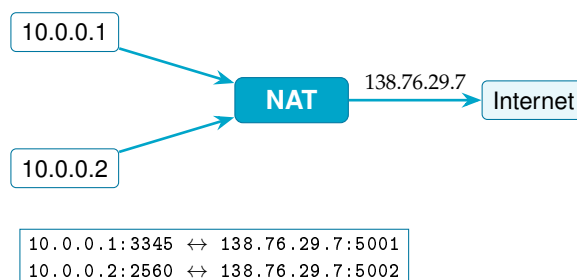


Figure 6.4: NAT preslikava (privatna adresa, port) u (javna adresa, novi port).

## 6.4 IPv6 i generalizirano prosljeđivanje

IPv4 raspolaže s „tek“  $2^{32}$  adresa, koje su zbog rasta broja uređaja iscrpljene. **IPv6** adresu širi na 128 bita, uvodi fiksno zaglavlje od 40 bajtova (bez kontrolnog zbroja i bez fragmentacije u ruterima) i dodaje oznaku toka. Adrese se zapisuju heksadecimalno u osam skupina, uz skraćivanje nula (2001:db8::ff00:42:8329). Budući da prijelaz ne može biti trenutačan, koristi se **tuneliranje**: IPv6 paket „umota“ se u IPv4 dok prolazi kroz IPv4 područja, uz čest dvostruki stog na uređajima.

|                                                 |
|-------------------------------------------------|
| verzija · klasa prometa · oznaka toka           |
| duljina tereta · sljedeće zaglavlje · hop limit |
| izvorišna adresa (128 bita)                     |
| odredišna adresa (128 bita)                     |

Figure 6.5: IPv6 zaglavlje: fiksnih 40 bajtova, adrese od 128 bita.

Suvremeni ruteri sve više koriste **generalizirano prosljeđivanje** po modelu *uvjet + akcija*: pravilo uspoređuje više polja (IP, TCP/UDP portovi, MAC) i primjenjuje akciju (prosljedi, odbaci, preusmjeri, prepriši). Ista apstrakcija tako objedinjuje ruter, vatrozid, NAT i balanser opterećenja. U pristupu **SDN** (*software-defined networking*) logički *centralizirani* upravljač postavlja te tablice u uređaje, npr. protokolom OpenFlow, čime se mreža programira softverski.

| uvjet (match)   | akcija (action) |
|-----------------|-----------------|
| dst=10.0.0.0/24 | izlaz 2         |
| tcp dport=22    | odbaci          |
| src=1.2.3.4     | kontroleru      |

Figure 6.6: Generalizirano prosljeđivanje: tablica „uvjet + akcija“.

### Sažetak poglavlja

Mrežni sloj ima podatkovnu (prosljeđivanje) i upravljačku (usmjeravanje) ravninu. **IP** nudi best-effort prijenos; adresa pripada sučelju, a **CIDR** i podmreže organiziraju adresni prostor uz longest prefix match. **DHCP** dinamički dodjeljuje adrese, a **NAT** štedi javne adrese dijeleći jednu javnu adresu. **IPv6** trajno rješava iscrpljenje adresa, a *uvjet+akcija* model sa SDN-om generalizira i programira prosljeđivanje.