

6. Internet protokoli

Prof.dr Igor Radusinović

igorr@ucg.ac.me

dr Slavica Tomović

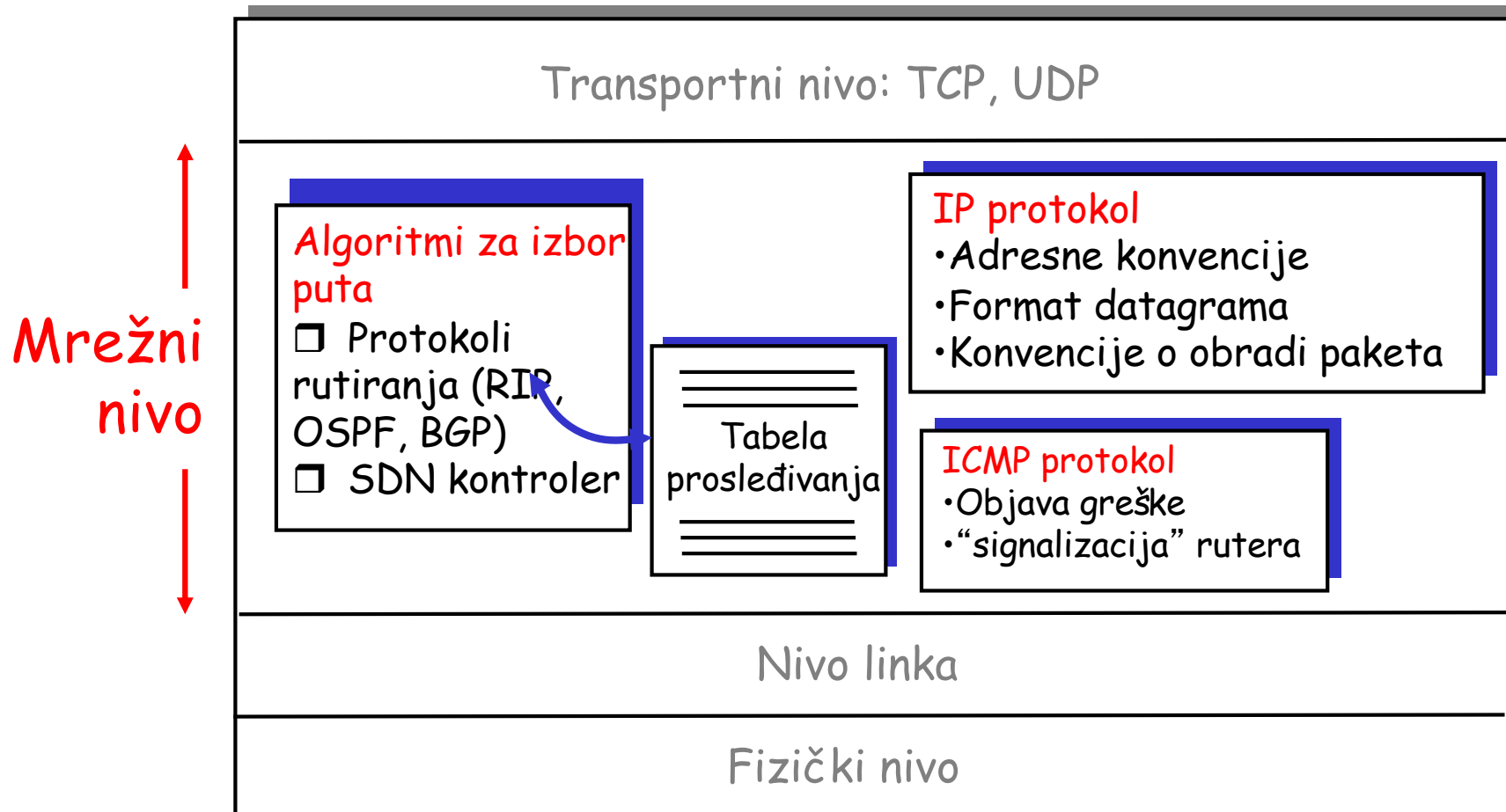
slavicat@ucg.ac.me

Internet protokoli

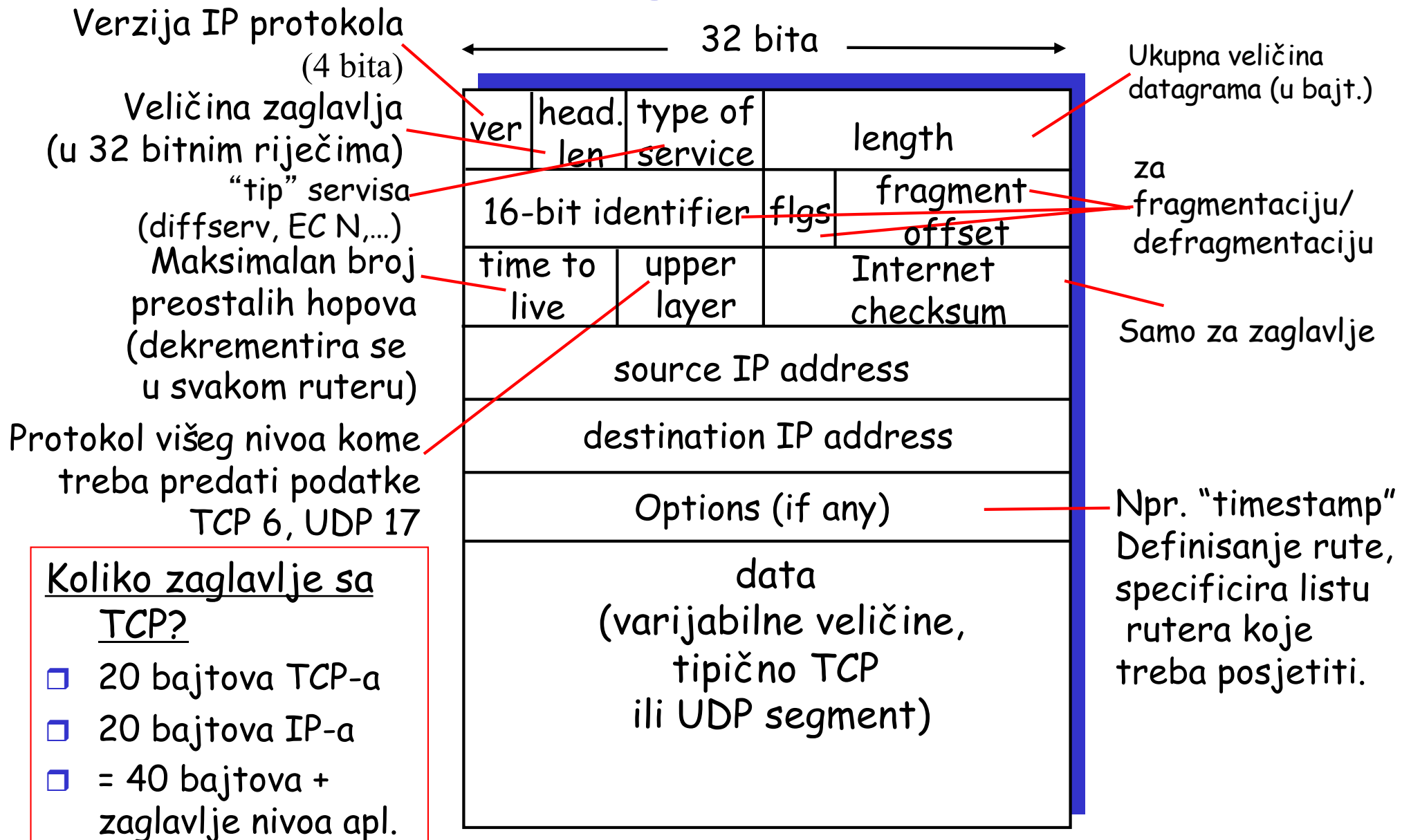
- ❑ IP (Internet Protocol)
- ❑ IP adresiranje
- ❑ IP rutiranje
- ❑ Ruter

Internet mrežni nivo

Host, ruter funkcije mrežnog nivoa:



Internet v4 datagram

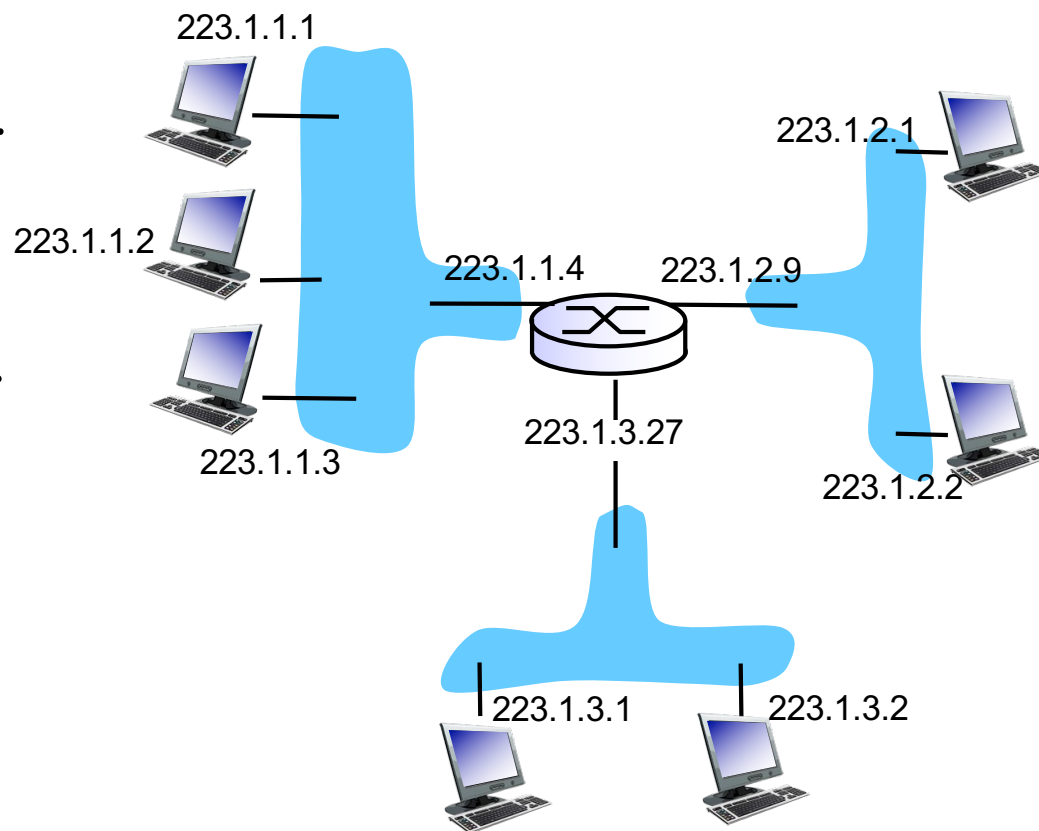


Koliko zaglavlje sa TCP?

- 20 bajtova TCP-a
- 20 bajtova IP-a
- = 40 bajtova + zaglavlje nivoa apl.

IPv4 adresiranje

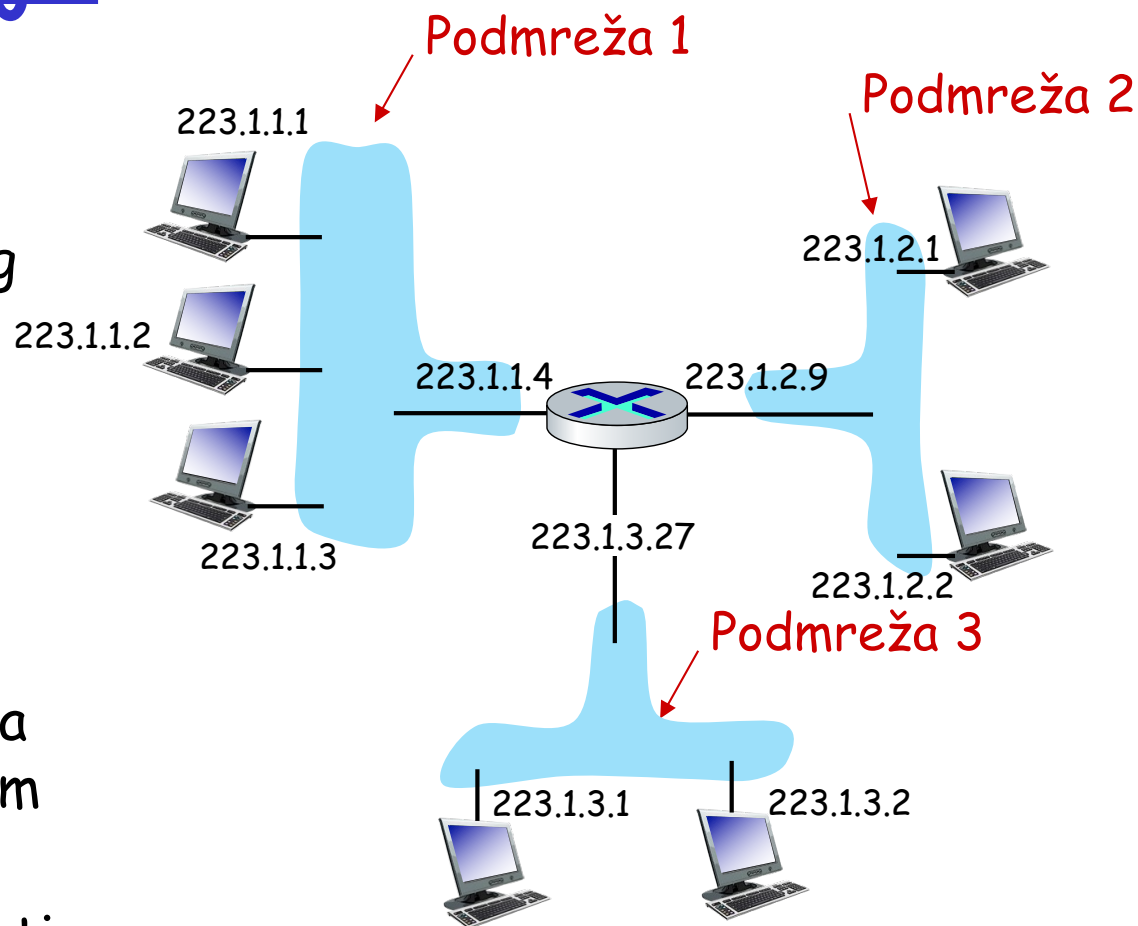
- IP adresa: 32-bitni identifikator za host ili ruter *interfejs*
- *interfejs*: veza između host/rutera i fizičkog linka
 - Ruteri imaju više od jednog interfejsa
 - i host može imati više interfejsa
 - IP adrese su vezane za svaki interfejs



$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{1}$$

IPv4 adresiranje

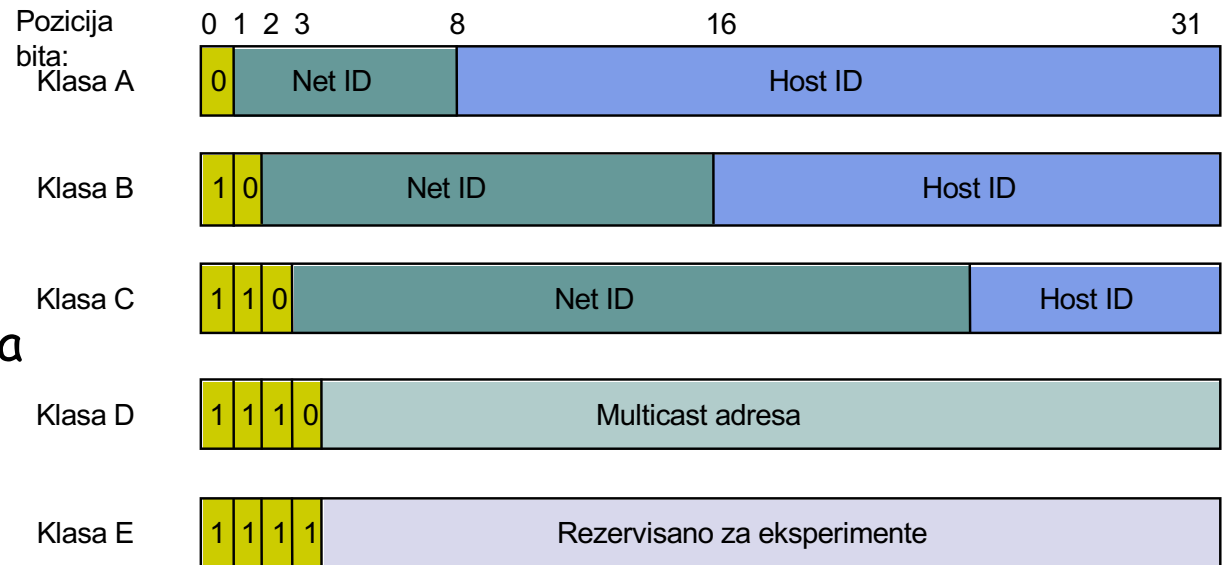
- IP adresiranje:
 - Mrežni dio (biti višeg reda)
 - Dio hosta (biti nižeg reda)
- *Šta je mreža?* (iz perspektive IP adrese)
 - Interfejsi uređaja sa istim mrežnim dijelom IP adrese
 - mogu fizički dosegnuti jedni druge bez učešća rutera



Mreža se sastoji od 3 IP podmreže (prvih 24 bita su mrežna adresa)

IPv4 classful adresiranje

- IPver4 adresna struktura je podijeljena na pet adresnih klasa: A, B, C, D i E, identifikacijom najznačajnijih bita adrese kao što je prikazano na slici.
- Na primjer klasa A ima 7 bita za mrežni ID i 24 bita za host ID, što znači $2^7 - 2 = 126$ mreža i $2^{24} - 2 = 16777214$ hostova. U klasu A spadaju adrese čiji je prvi bit uvijek 0. Ova klasa je namijenjena velikim organizacijama. Opseg validnih mrežnih adresa klase A je od 1.0.0.0 do 126.0.0.0.

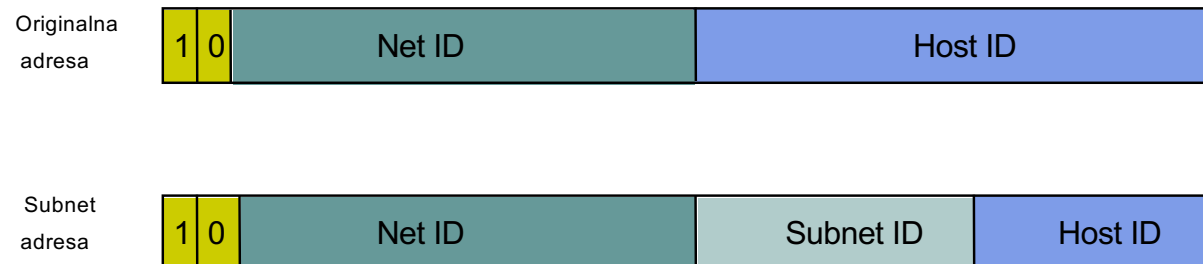


IPv4 classful adresiranje

- ❑ ID koji imaju sve jedinice i sve nule imaju specijalnu namjenu.
- ❑ Host ID koji se sastoji od svih jedinica znači da se paket *broadcast*-uje svim hostovima mreže čiji je mrežni ID specificiran.
- ❑ Ako se mrežni ID sastoji od svih jedinica to znači da se paket *broadcast*-uje svim hostovima lokalne mreže.
- ❑ Host ID koji se sastoji od svih 0 odgovara adresi mreže.
- ❑ Određeni opsezi adresa su namijenjeni za privatne mreže (RFC1918).
- ❑ Ove adrese se koriste unutar mreža koje se ne vezuju direktno na Internet ili u mrežama u kojima je implementiran NAT.
- ❑ Ove adrese nijesu registrovane i ruteri na Internetu moraju odbacivati pakete sa ovakvim adresama. Opsezi privatnih adresa su: 10.0.0.0 - 10.255.255.255 (A klasa), 172.16.0.0 - 172.31.255.255 (B klasa) i 192.168.0.0 - 192.168.255.255 (C klasa - najčešće se primjenjuje u kućnim mrežama)

IPv4 classful adresiranje

- ❑ Opisano IP adresiranje ima više nedostataka.
- ❑ Ovo adresiranje može biti vrlo neefikasno. Na primjer, dodjela B klase jednoj akademskoj instituciji koja ima jednu ili više lokalnih računarskih mreža je besmislena.
- ❑ Rješenje ovog problema je razvijeno 1980-tih kada je usvojen koncept podmreže (subnetting) kada sa dodaje još jedan hijerarhijski nivo subnet (podmreža).
- ❑ Sjajna stvar ovog koncepta je njena transparentnost na Internetu. Naime, Internet "vidi" i dalje samo dva nivoa hijerarhije. Unutar intraneta mrežnom administratoru se ostavlja mogućnost kombinovanja veličina subnet i host polja.



IPv4 classful adresiranje

- To znači da dodijeljena mrežna adresa može biti podijeljena na više podmreža. Tako na primjer, 172.16.1.0, 172.16.2.0 i 172.16.3.0 predstavljaju podmreže mreže 172.16.0.0.
- Adresa podmreže se dobija "posuđivanjem" bita iz dijela koji se odnosi na host i njihovo dodjeljivanje podmreži.
- Broj "posuđenih" bita iz dijela koji se odnosi na host varira i zavisi od maske podmreže (subnet mask).
- Maska podmreže ima isti format i koncepciju kao i IP adrese. Razlika je u tome što sve jedinice označavaju polja koja pripadaju mreži i podmreži, dok 0 specificiraju polje adrese koje pripada hostu.



Maska podmreže 255 • 255 • 255 • 0

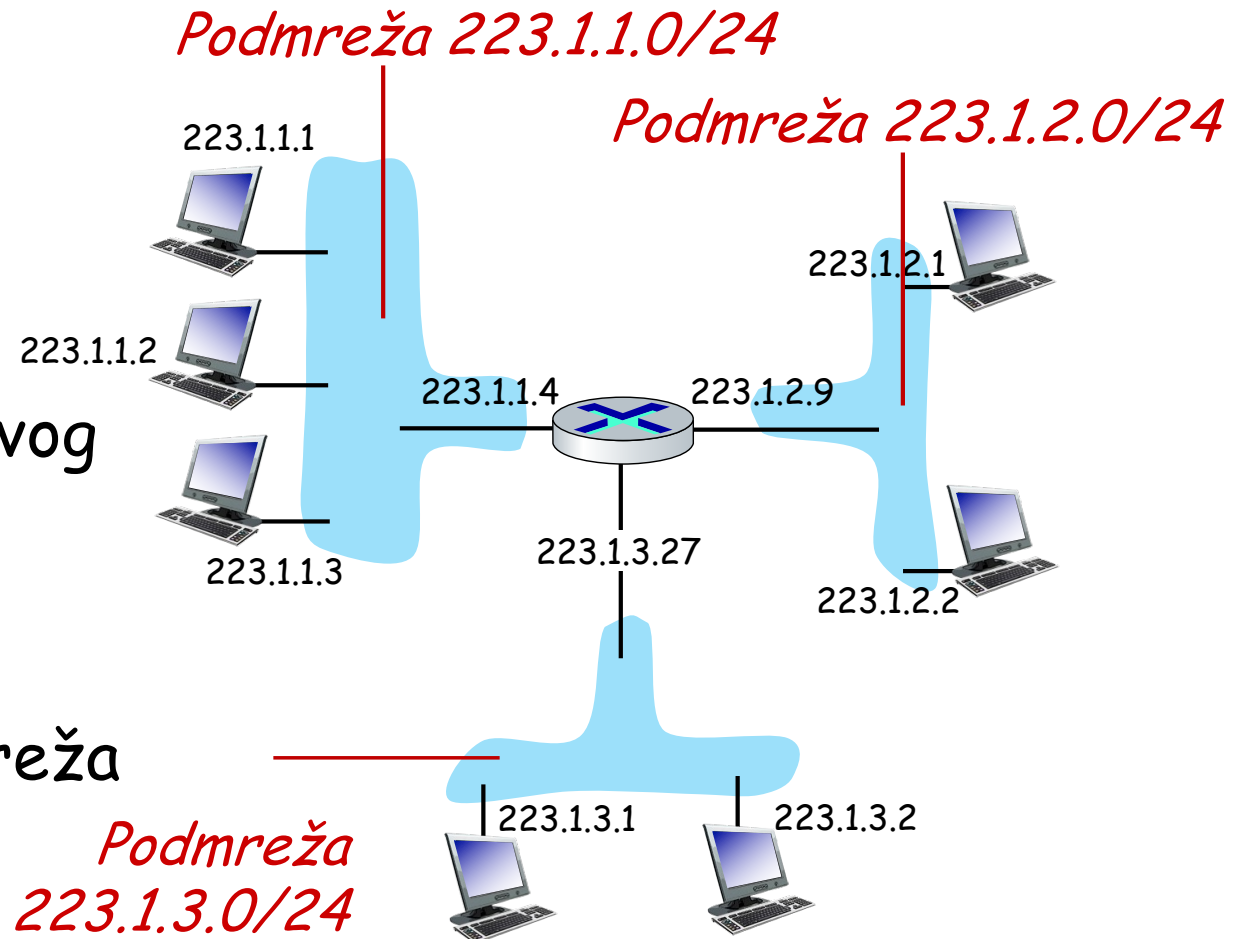
Binarna
reprezentacija
maske podmreže 1 1 1 1 1 1 1 1 • 1 1 1 1 1 1 1 1 • 1 1 1 1 1 1 1 1 • 0 0 0 0 0 0 0 0



IPv4 classful adresiranje

Podmreža

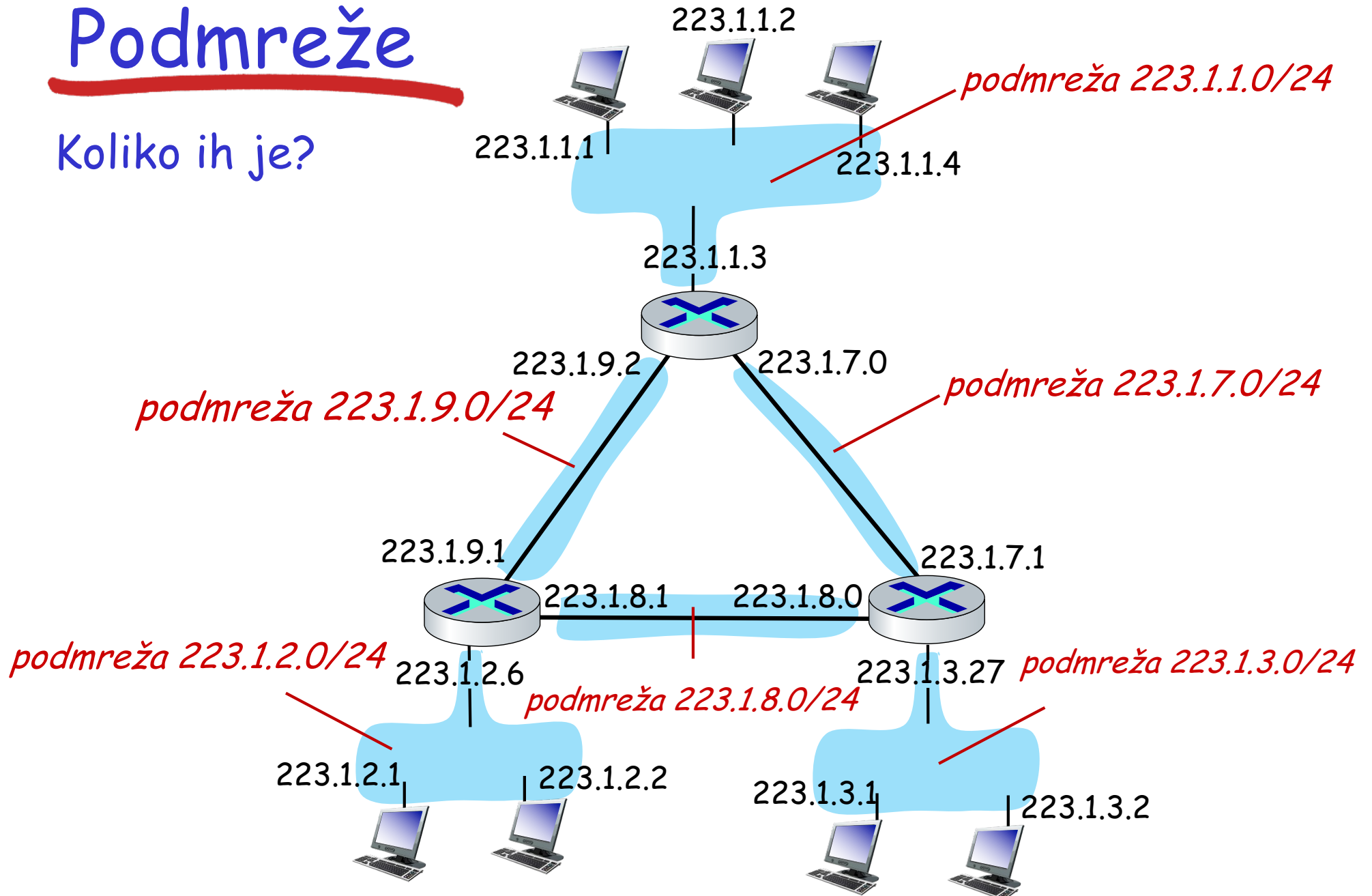
- Da bi odredili podmreže, treba razdvojiti svaki interfejs od njegovog hosta ili rutera, kreirajući ostrva izolovanih mreža. Svaka izolovana mreža se zove **podmreža**.



Maska podmreže: /24

Podmreže

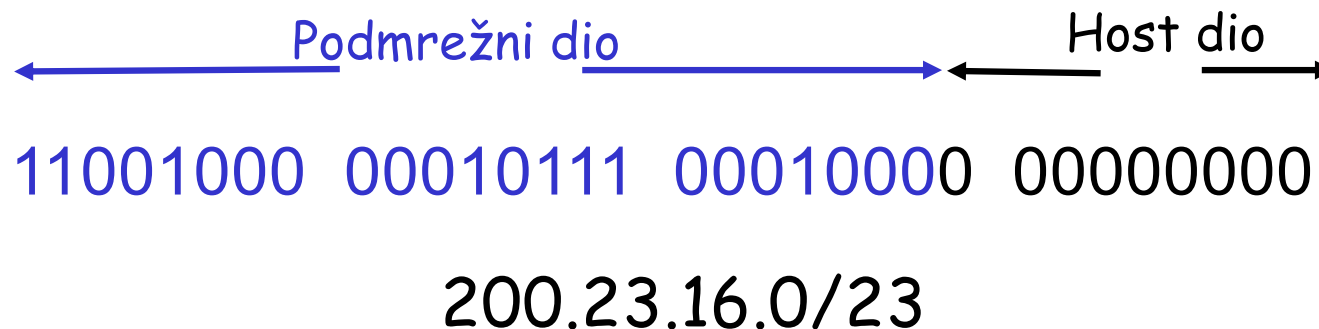
Koliko ih je?



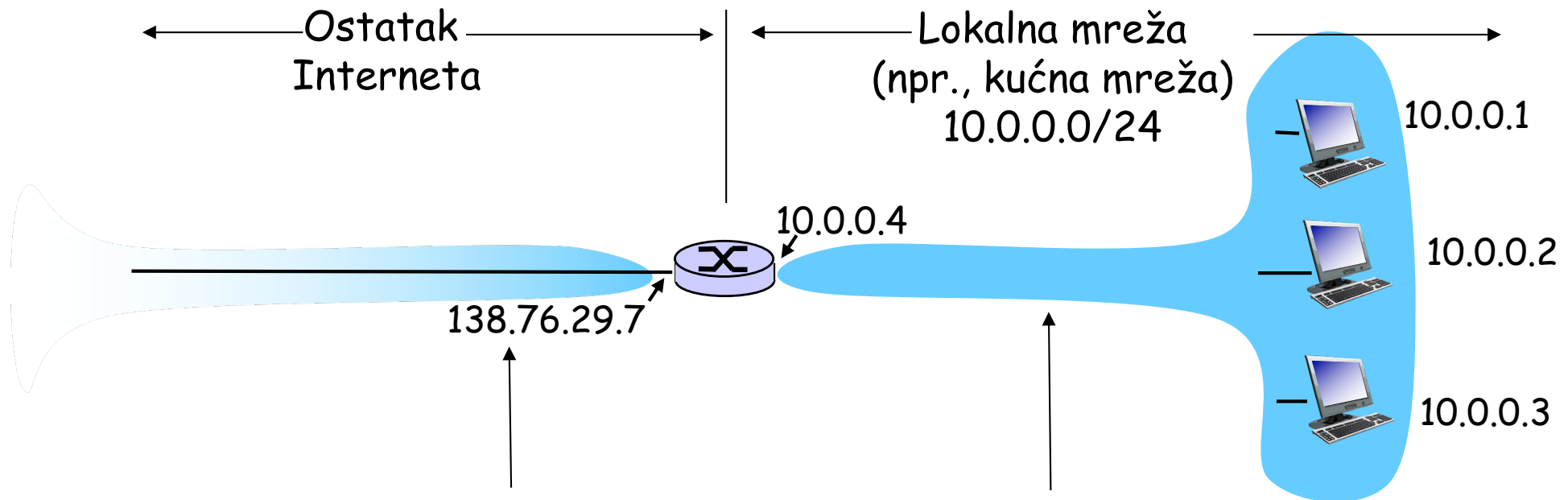
IPv4 classless adresiranje

□ CIDR: Classless InterDomain Routing

- Podmrežni dio adrese je proizvoljne veličine
- Format adrese: **a.b.c.d/x**, gdje je x broj bita u mrežnom dijelu adrese



NAT: Network Address Translation



Svi datagrami *napuštaju* lokalnu mrežu imajući *istu* jedinstvenu izvorišnu adresu NAT IP: 138.76.29.7, Različiti brojevi izvorišnih portova

Datagrami sa izvorima ili destinacijama u ovoj mreži imaju 10.0.0.0/24 adresu za izvor, destinaciju (kao što je uobičajeno)

NAT: Network Address Translation

- **Motivacija:** lokalna mreža koristi samo jednu IP adresu:
 - Nema potrebe za dodjelu opsega adresa od strane ISP (samo jedna IP adresa se koristi za sve uređaje)
 - Mogu mijenjati adrese uređaja u lokalnim mrežama bez obavještenja "ostatku svijeta"
 - Mogu mijenjati ISP bez mijenjanja adresa uređaja u lokalnim mrežama
 - Uređaji unutar mreže se eksplicitno ne adresiraju, na vidljiv način "ostatku svijeta" (plus u smislu zaštite).

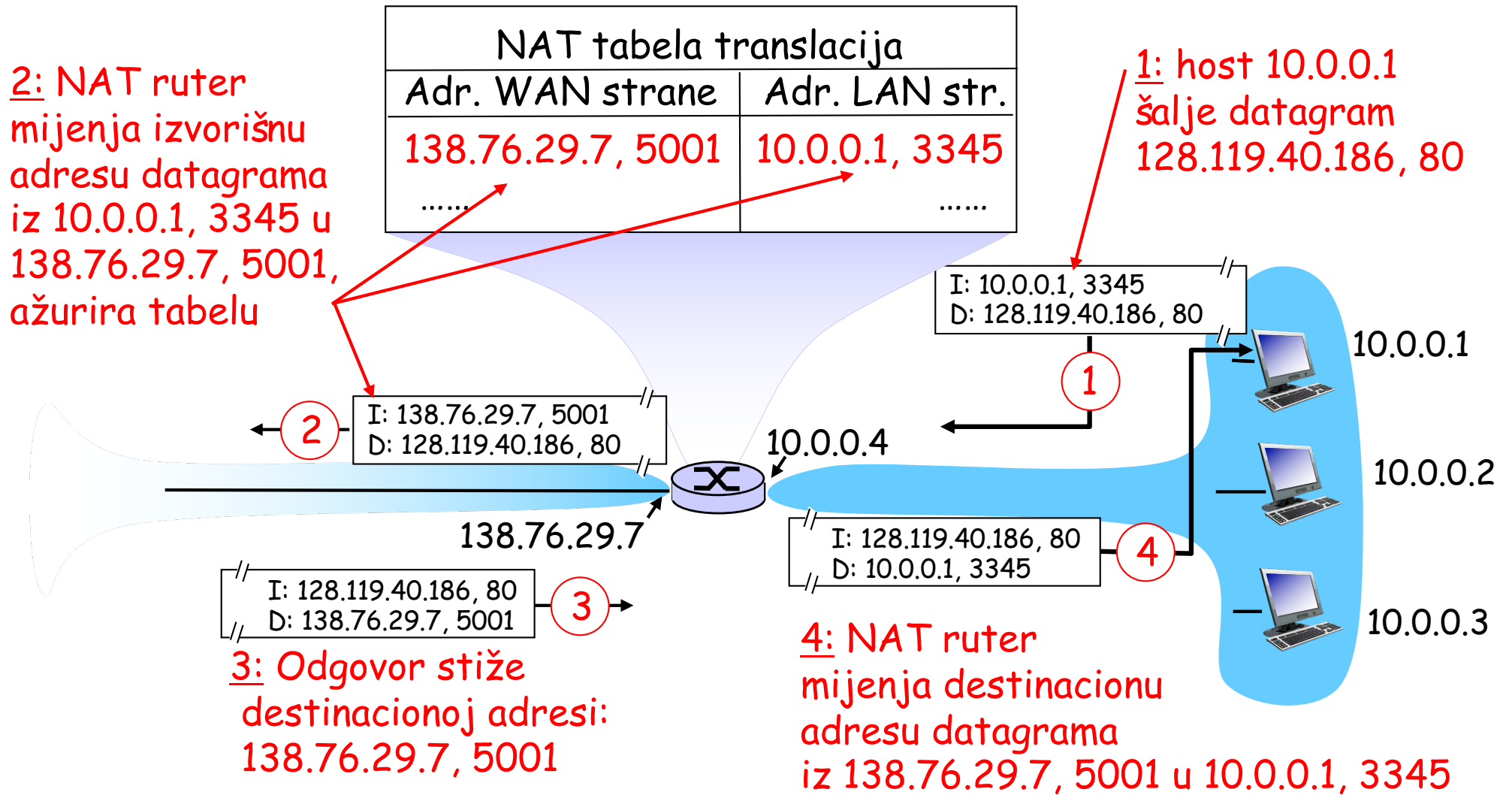
NAT: Network Address Translation

Implementacija:

NAT ruter mora:

- *odlazni datagrami: zamijeniti* (izvorišnu IP adresu, broj port) svakog odlaznog datagrama sa (NAT IP adresom, novim brojem porta)
 - ... udaljeni klijenti/serveri će odgovoriti korišćenjem (NAT IP adrese, novi broj porta) kao adrese destinacije.
- *zapamtiti (u NAT tabeli translacija)* svaki (izvorišna IP adresa, broj porta) i (NAT IP adresa, novi broj porta) u vidu translacionog para
- *dolazeći datagrami: zamijeniti* (NAT IP adresu, novi broj porta) u polju destinacije svakog dolaznog datagrama sa odgovarajućim (izvorišna IP adresa, broj porta) smještenim u NAT tabeli

NAT: Network Address Translation



NAT: Network Address Translation

- 16-bitno polje broja porta:
 - 65536 simultanih veza sa jednom adresom sa LAN strane!
- NAT je kontraverzan:
 - Ruteri bi trebali vršiti obradu samo do nivoa 3
 - Narušava prirodu od kraja do kraja
 - NAT mora biti uzet u obzir od strane dizajnera aplikacija, npr., P2P aplikacija
 - Oskudica adresa se može ublažiti i prije upotrebe IPv6
 - Broj porta se posredno koristi za adresiranje računara
- NAT se intenzivno koristi u praksi

IPv6

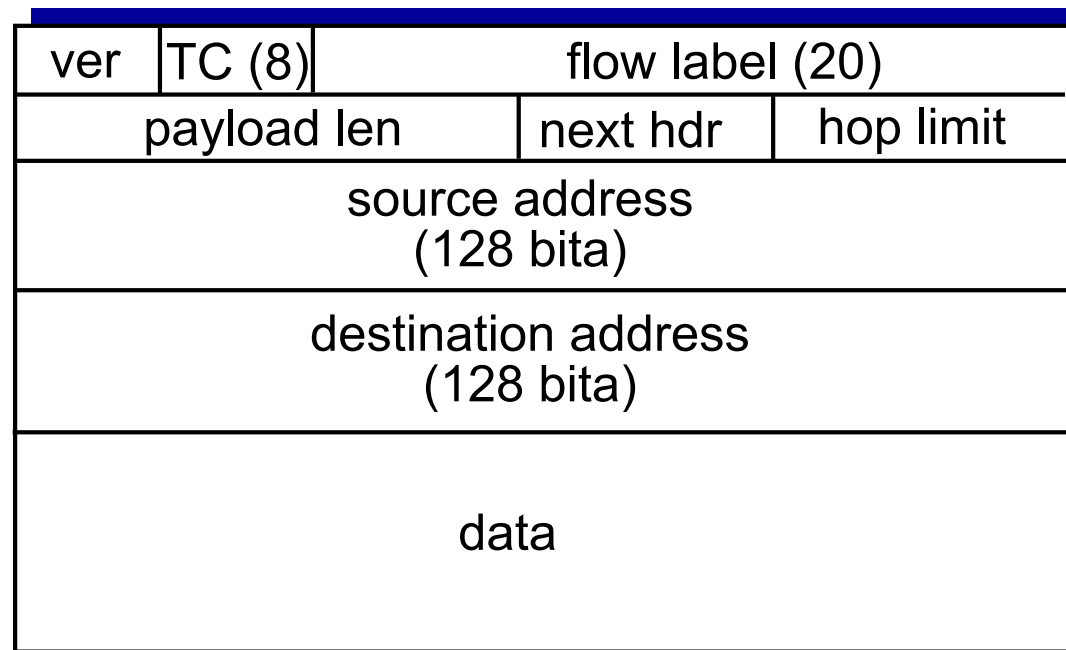
- ❑ **Inicijalna motivacija:** 32-bitni adresni prostor će vrlo brzo u potpunosti biti dodijeljen.
- ❑ **Dodatna motivacija:**
 - Format zaglavlja pomaže obradi/prosleđivanju
 - Promjene zaglavlja uključuju QoS
- ❑ **IPv6 format datagrama:**
 - Zaglavlje fiksne-dužine od 40B
 - Nije dozvoljena fragmentacija

IPv6

Priority: identifikuje prioritet između datagrama u "toku"

Traffic class: identifikuje datagrame u istom "toku".
(koncept "toka" nije precizno definisan).

Next header: identifikuje protokola višeg nivoa za podatke



← 32 bita →

IPv6

- *Checksum*: potpuno uklonjena kako bi se smanjila obrada na svakom hopu
- *Options*: dozvoljene, ali van zaglavlja, indicirano sa “Next Header” poljem
- *ICMPv6*: nova verzija ICMP
 - dodatni tipovi poruka, npr. “Packet Too Big”
 - funkcija upravljanja multicast grupama

IPv6 adresiranje

Format:

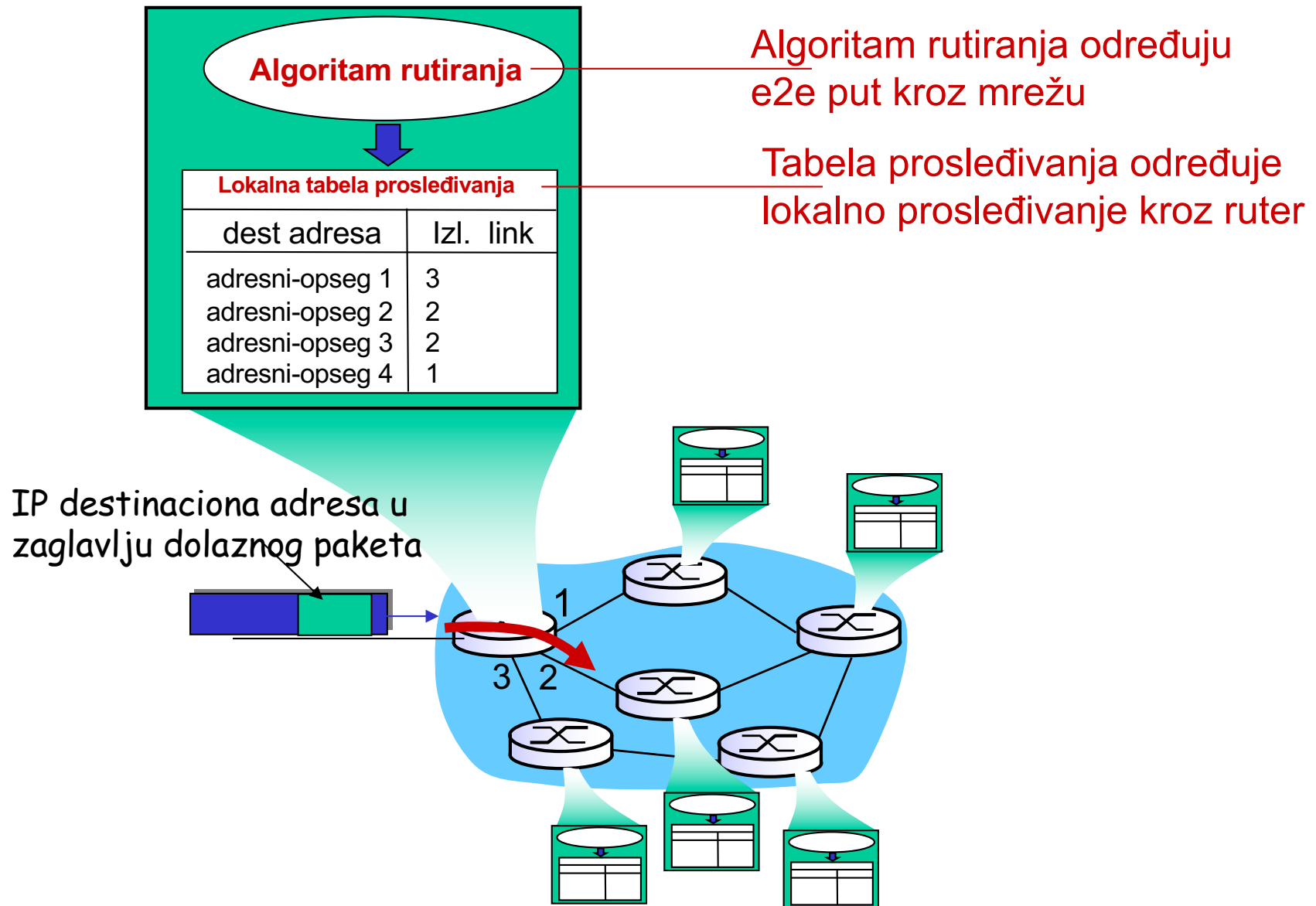
- ❑ *RFC 4291 (Februar 2006)*
- ❑ *128 bita*
- ❑ *Predstavlja se u vidu 8 grupa po četiri heksadecimalna broja*
- ❑ *X:X:X:X:X:X:X:X*
- ❑ 1111111000011010 0100001010111001 00000000000011011
000000000000000000 000000000000000000 0001001011010000
0000000001011011 0000011010110000
- ❑ FE1A:42B9:001B:0000:0000:12D0:005B:06B0
- ❑ FE1A:42B9:001B:0:0:12D0:005B:06B0 (grupa od četiri 0 se može prikazati jednom 0)
- ❑ FE1A:42B9:1B::12D0:5B:6B0 (više susjednih grupa od četiri 0 se prikazuje sa ::, koja se može pojaviti samo jednom)
- ❑ 2001:4C::50:0:0:741
- ❑ 2001:004C::0050:0000:0000:0741
- ❑ 2001:004C:0000:0000:0050:0000:0000:0741

IPv6 adresiranje

IPv6 prefiks:

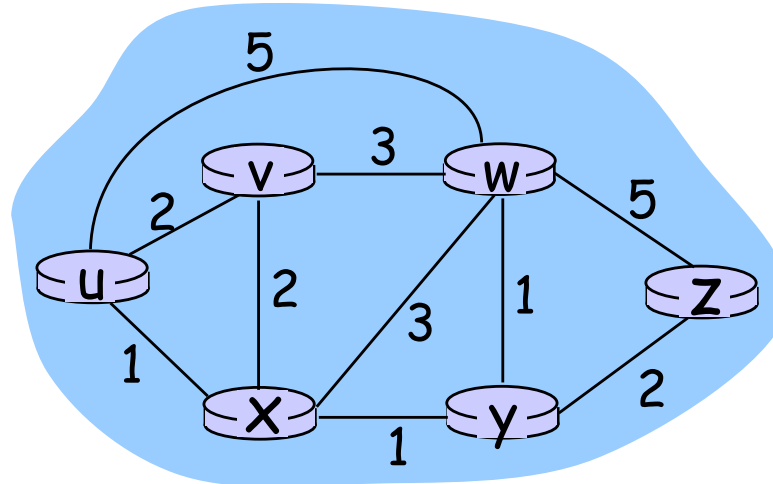
- ❑ Slično kao kod IPv4: IPv6adresa/dužina prefiksa
- ❑ 200C:001b:1100:0:0:0:0:0/40 ili 200C:1b:1100::/40
- ❑ Koristi se CIDR rutiranje

IP rutiranje



IP rutiranje

Abstrakcija pomoću grafa



Graf: $G = (N, E)$

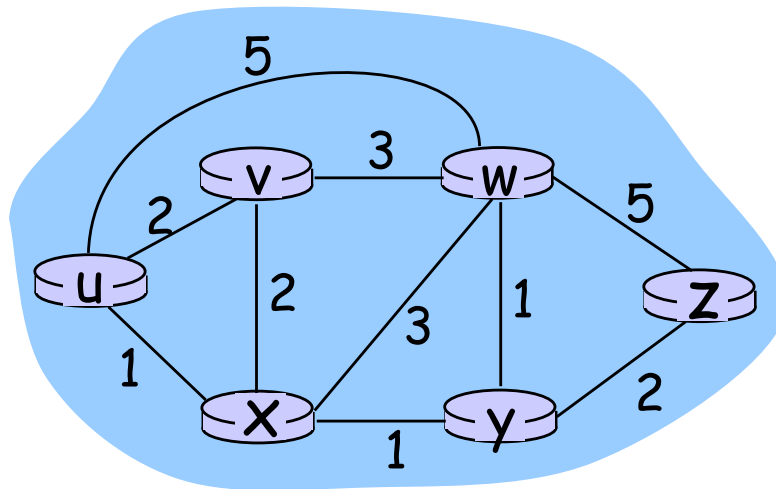
$N = \text{skup rutera} = \{ u, v, w, x, y, z \}$

$E = \text{skup linkova} = \{ (u,v), (u,x), (v,x), (v,w), (x,w), (x,y), (w,y), (w,z), (y,z) \}$

Napomena: Abstrakcija pomoću grafa je korisna i u drugim mrežnim kontekstima.

Primjer: P2P, gdje je N skup peer-ova, a E skup TCP konekcija

IP rutiranje



- $c(x,x')$ = težinski faktor (cost) linka (x,x')
 - npr., $c(w,z) = 5$
- težinski faktor može biti uvijek 1, ili recipročan protoku, ili recipročan zagušenju

Težinski faktor puta $(x_1, x_2, x_3, \dots, x_p) = c(x_1, x_2) + c(x_2, x_3) + \dots + c(x_{p-1}, x_p)$

Pitanje: Koji je put sa najmanjim težinskim faktorom između u i z ?

Algoritam rutiranja: algoritam koji pronalazi put sa najmanjim težinskim faktorom

Klasifikacija algoritama rutiranja

Globalna ili decentralizovana informacija?

Globalna:

- ❑ svi ruteri posjeduju kompletnu topologiju mreže sa informacijama o težinskim faktorima linkova
- ❑ “link state” algoritmi

Decentralizovani:

- ❑ ruter poznaje fizički povezane susjede i težinske faktore linkova do susjeda
- ❑ iterativni proces izračunavanja, razmjena informacija sa susjedima
- ❑ “distance vector” algoritmi

Statički ili dinamički?

Statički:

- ❑ Rute se sporo mijenjaju

Dinamički:

- ❑ Rute se mijenjaju mnogo brže
 - periodični update
 - kao odgovor na promjene težinskih faktora linkova

Dijkstra algoritam rutiranja

- Link state
- Mrežna topologija, težinski faktori linkova poznati svim čvorištima
 - Dobijeno preko “link state broadcast”
 - Sva čvorišta imaju istu informaciju
- Proračunava puteve najmanjih težinskih faktora od jednog čvorišta (“izvor”) do svih ostalih čvorova
 - generiše **tabelu rutiranja** za to čvorište
- iterativni: poslije k iteracija, poznat je put sa najmanjim težinskim faktorom do k destinacija
- OSPF

Notacija:

- $c(A,B)$: težinski faktor linka od čvorišta A do B su beskonačni ukoliko čvorišta nijesu susjedi
- $D(A)$: trenutna vrijednost težinskog faktora puta od izvorišta do destinacije A
- $p(A)$: sledeće čvorište duž puta od izvorišta do čvorišta A, koje je susjed A
- N' : skup čvorišta čiji su najniži težinski faktori puta poznati

Dijkstra algoritam rutiranja

1 *Inicijalizacija:*

2 $N' = \{u\}$

3 Za sva čvorišta A

4 Ako je A susjedno čvorište u

5 tada $D(A) = c(u,A)$

6 else $D(A) = \infty$

7

8 *Petlja*

9 Pronađi B koje nije u N' tako da je $D(B)$ minimalno

10 dodati B skupu N'

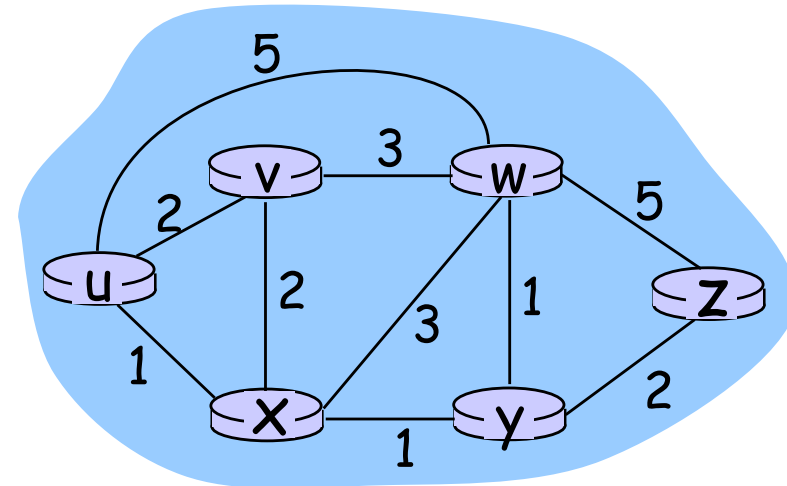
11 update $D(A)$ za sve A susjede B koji nijesu u N' :

12 $D(A) = \min(D(A), D(B) + c(B,A))$

13 /* novi težinski faktori za A su ili stari težinski faktori za A ili su poznati

14 najmanji težinski faktori puta do B plus težinski faktori od B do A */

15 *dok sva čvorišta ne budu u N'*

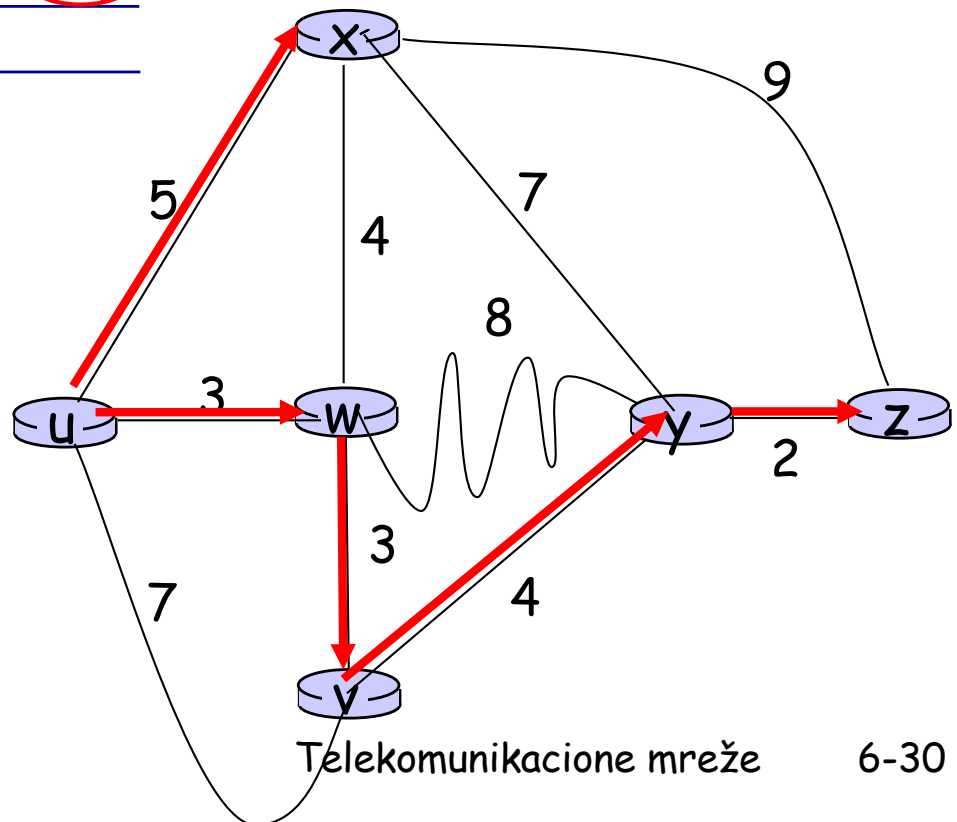


Dijkstra algoritam rutiranja

Step	N'					
0	u	7,u	3,u	5,u	∞	∞
1	uw	6,w		5,u	11,w	∞
2	uwX	6,w			11,w	14,x
3	uwXv				10,v	14,x
4	uwXvy					12,y
5	uwXvyz					

Napomene:

- ❖ Konstruisati najkraći put praćenjem prethodnih čvorišta
- ❖ Linkovi mogu biti prekinuti



OSPF (Open Shortest Path First)

- ❑ Interior Gateway Protocol (IGP)
- ❑ “open”: javno dostupan
- ❑ Verzija 2 (RFC 2328) iz 1998
- ❑ Verzija 3 (RFC2740) iz 1999 podržava IPv4 i IPv6
- ❑ Koristi se u velikim kompanijskim mrežama zbog brze konvergencije, rješavanja problema petlji i balansiranja saobraćaja, dok operatori koriste IS-IS koji je pogodan za stabilne mreže
- ❑ Koristi “Link State” algoritam
 - LS širenje paketa
 - Mapa topologije na svakom čvorištu
 - Proračun rute korišćenjem Dijkstra algoritma
 - Broadcast svakih 30min
- ❑ OSPF oglašavanja nose po jednu informaciju po susjednom ruteru
- ❑ Širenje oglašavanja preko **čitavog** AS (“flooding”)
 - Nose se u OSPF porukama direktno preko IP (a ne preko TCP ili UDP) pri čemu potrebne kontrole obavlja OSPF
- ❑ Radi smanjenja saobraćaja može se koristiti koncept DR (designated router) i multicasta tabele.

Hijerarhijsko rutiranje

Prethodna analiza je bila - idealizacija

- ❑ Svi ruteri su identični
- ❑ “flat” mreža

... praksa je drugačija

veličina: nekoliko stotina miliona
destinacija:

- ❑ ne mogu se sve destinacije smjestiti u tabele rutiranja!
- ❑ razmjena tabela rutiranja može oboriti linkove!
- ❑ LS može izazvati potiskivanje saobraćaja na račun broadcasta tabela
- ❑ DV teško može konvergirati

administrativna autonomija

- ❑ internet = mreža svih mreža
- ❑ svaki mrežni administrator želi
 - kontrolu rutiranja u svojoj sopstvenoj mreži
 - Sakriti mrežnu organizaciju od ostalih

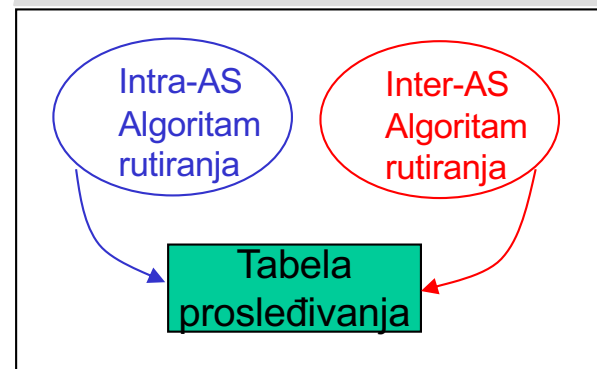
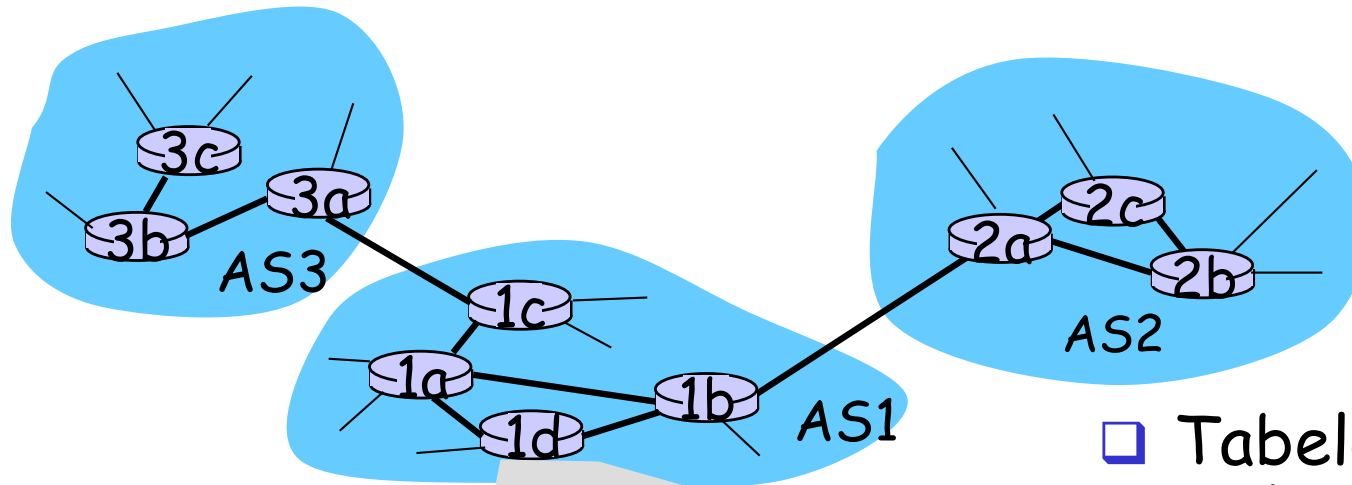
Hijerarhijsko rutiranje

- ❑ grupe rutere u regione, “autonomni sistemi” (AS)
- ❑ ruteri u istom AS izvršavaju isti protokol rutiranja
 - “intra-AS” protokol rutiranja se slično ponaša objašnjenim idealizovanim modelima
 - ruteri u različitim AS mogu izvršavati različite intra-AS protokole rutiranja

Gateway ruter

- ❑ Prosleđuje datagrame van AS

AS medupovezivanje



□ Tabela prosleđivanja se konfigurira i sa intra- i sa-AS algoritmom rutiranja

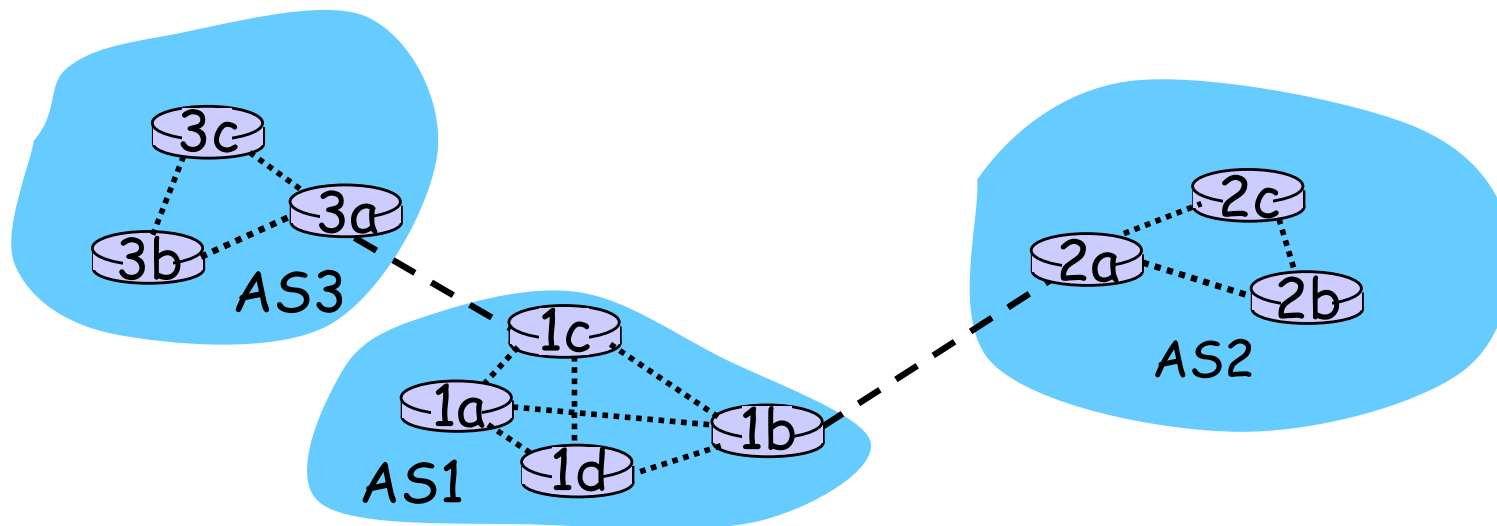
- Intra-AS setuje sadržaje za interne destinacije
- Inter-AS & Intra-AS setuje sadržaje za eksterne destinacije

Internet inter-AS rutiranje: BGP

- ❑ **BGP (Border Gateway Protocol):** *de facto* standard
- ❑ Verzija 4 (RFC1771) iz 1994 je doživjela preko 20 korekcija, pri čemu je zadnja RFC4271 (iz 2006)
- ❑ CIDR i agregacija ruta
- ❑ Naslijedio EGP čime je napravljena potpuna decentralizacija Interneta
- ❑ Mogu ga koristiti i kompanije kada OSPF nije dovoljno dobar i kada se radi o multihomed mreži (bolja redundansa).
- ❑ BGP omogućava svakom AS:
 1. Dobijanje informacije o dostižnosti sa susjednih AS-ova.
 2. Prosleđivanje prethodne informacije svim ruterima u okviru AS.
 3. Utvrđivanje “dobre” rute do podmreža baziranih na informaciji o dostižnosti i politici.
- ❑ Dozvoljava podmreži oglašavanje svog prisustva ostatku Interneta: *“Ovdje sam”*

Internet inter-AS rutiranje: BGP

- Parovi rutera (BGP peer-ovi) razmjenjuju informaciju rutiranja preko semi-permanentne TCP konekcije (port 179): **BGP sesije**
- Svakih 60s šalje **keep alive** poruku
- **Napomena:** BGP sesije ne odgovaraju fizičkim linkovima.
- Kada AS2 oglasi prefiks do AS1, AS2 **obećava** da će proslijediti bilo koji datagram koji je adresiran do tog prefiksa preko sebe.
 - AS2 može agregirati prefikse u oglašavanjima

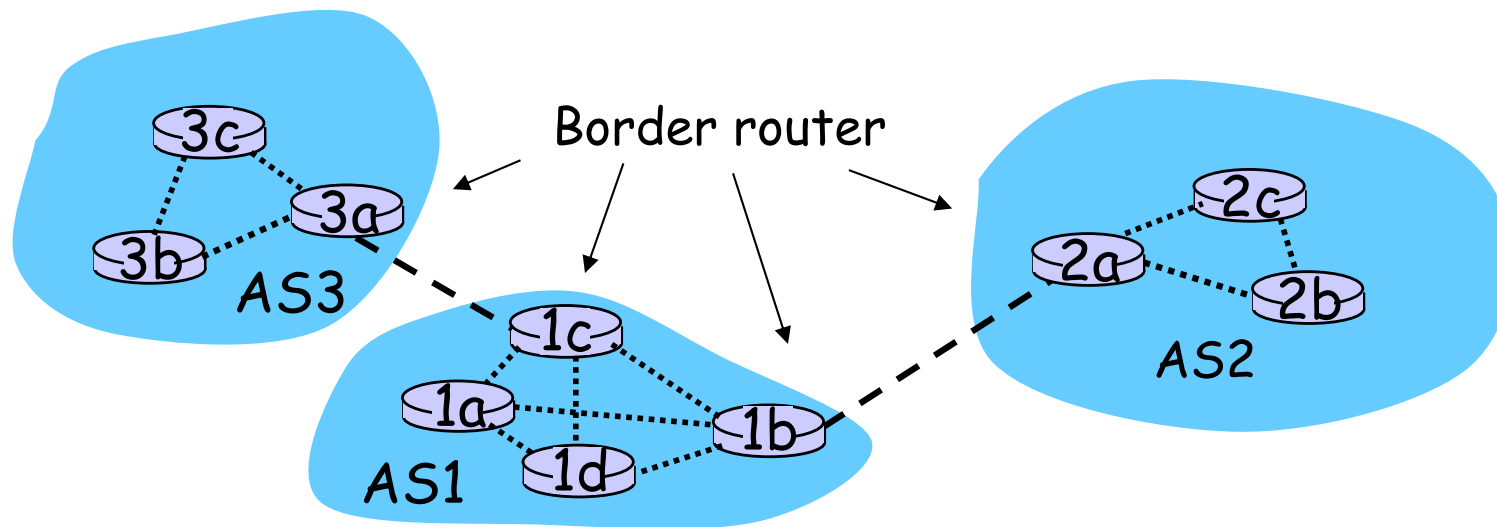


----- eBGP sesija

..... iBGP sesija

Internet inter-AS rutiranje: BGP

- ❑ Sa eBGP sesijom između 3a i 1c, AS3 šalje informaciju o dostižnosti prefiksa do AS1.
- ❑ 1c može tada koristiti iBGP za distribuciju ove nove informacije o dostizanju prefiksa do svih rutera u AS1
- ❑ 1b može tada ponovo oglasiti novu informaciju o dostizanju do AS2 preko 1b-2a eBGP sesije
- ❑ Kada ruter stekne znanje o novom prefiksu, kreira sadržaj za taj prefiks u tabeli rutiranja.



----- eBGP sesija

..... iBGP sesija