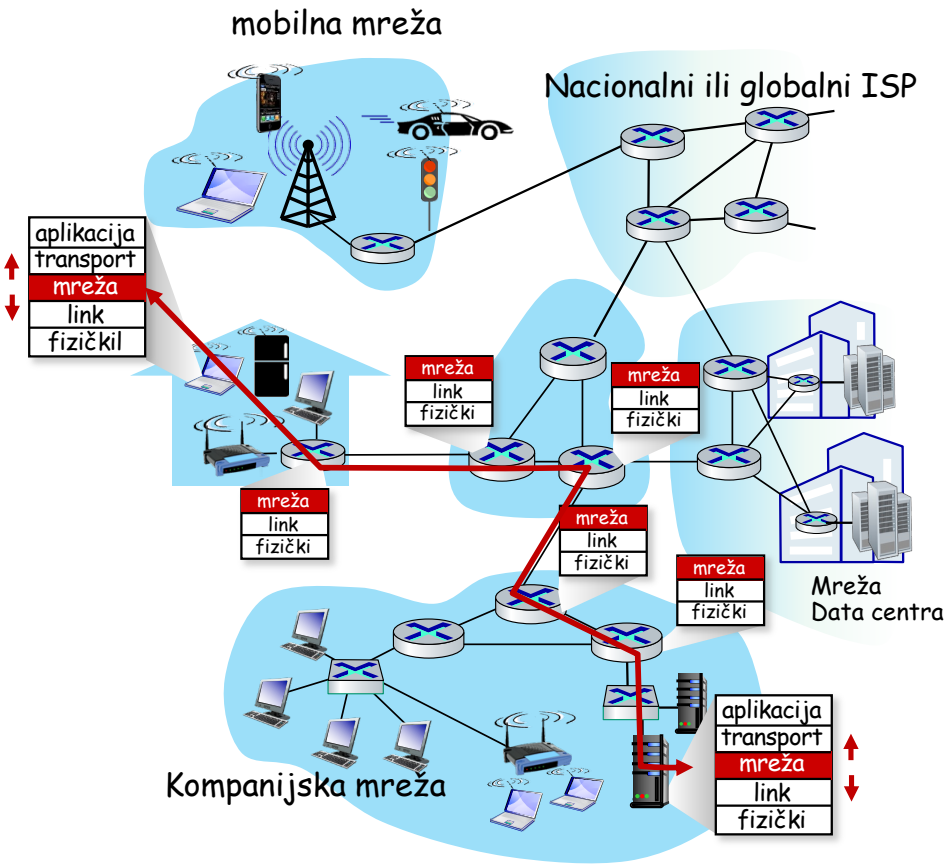
Glava 4: Mrežni nivo

- Principi nivoa mreže
- IPv4 (Internet Protocol)
  - DHCP
  - NAT
  - ICMP
- IPv6
- Protokoli rutiranja
- Mrežni menadžment

Mrežni nivo

- Prenos segmenta od pošiljaoca do odredišta
  - Na predajnoj strani se enkapsuliraju segmenti u datagrame
  - Na prijemnoj strani segmenti se predaju transportnom nivou
- Protokoli mrežnog nivoa su implementirani na svakom hostu, ruteru, firewall-u, IDS, IPS, *content layer* komutatoru
- Ruter ispituje polja zaglavlja svakog IP datagrama kojeg prosleđuje sa ulaza na izlaz prateći rutu od izvora do destinacije



Ključne funkcije mrežnog nivoa

- prosleđivanje: prenos paketa sa ulaza rutera na odgovarajući izlaz (RAVAN PODATAKA)
- rutiranje: izbor rute kojom se paketi prenose od izvora do destinacije (KONTROLNA RAVAN)

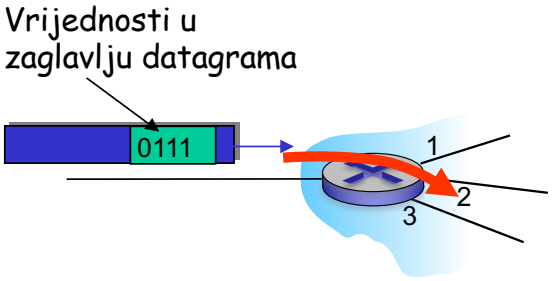
prosleđivanje

rutiranje

Mrežni nivo: ravan podataka, ravan kontrole

Ravan podataka

- Lokalna funkcija rutera
- Određuje kako se datagram koji dolazi na ulazni port rutera prosleđuje na izlazni port
- Funkcija prosleđivanja

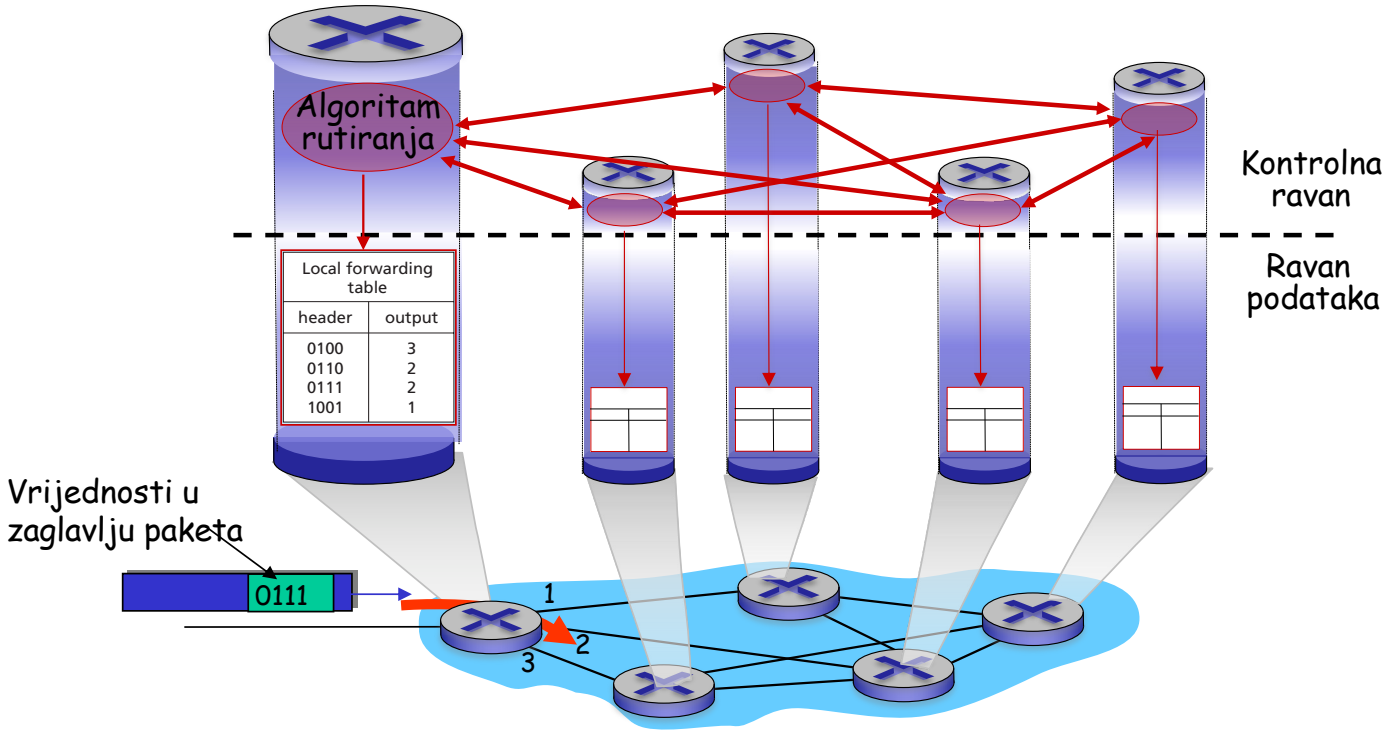


Kontrolna ravan

- Mrežna logika
- Određuje kako se datagram rutira duž putanje od kraja do kraja od izvorišnog do odredišnog hosta
- Dva pristupa:
  - Tradicionalni algoritmi rutiranja: implementirani u ruterima
  - *Software-Defined Networking* (SDN): implementirani u udaljenim serverima

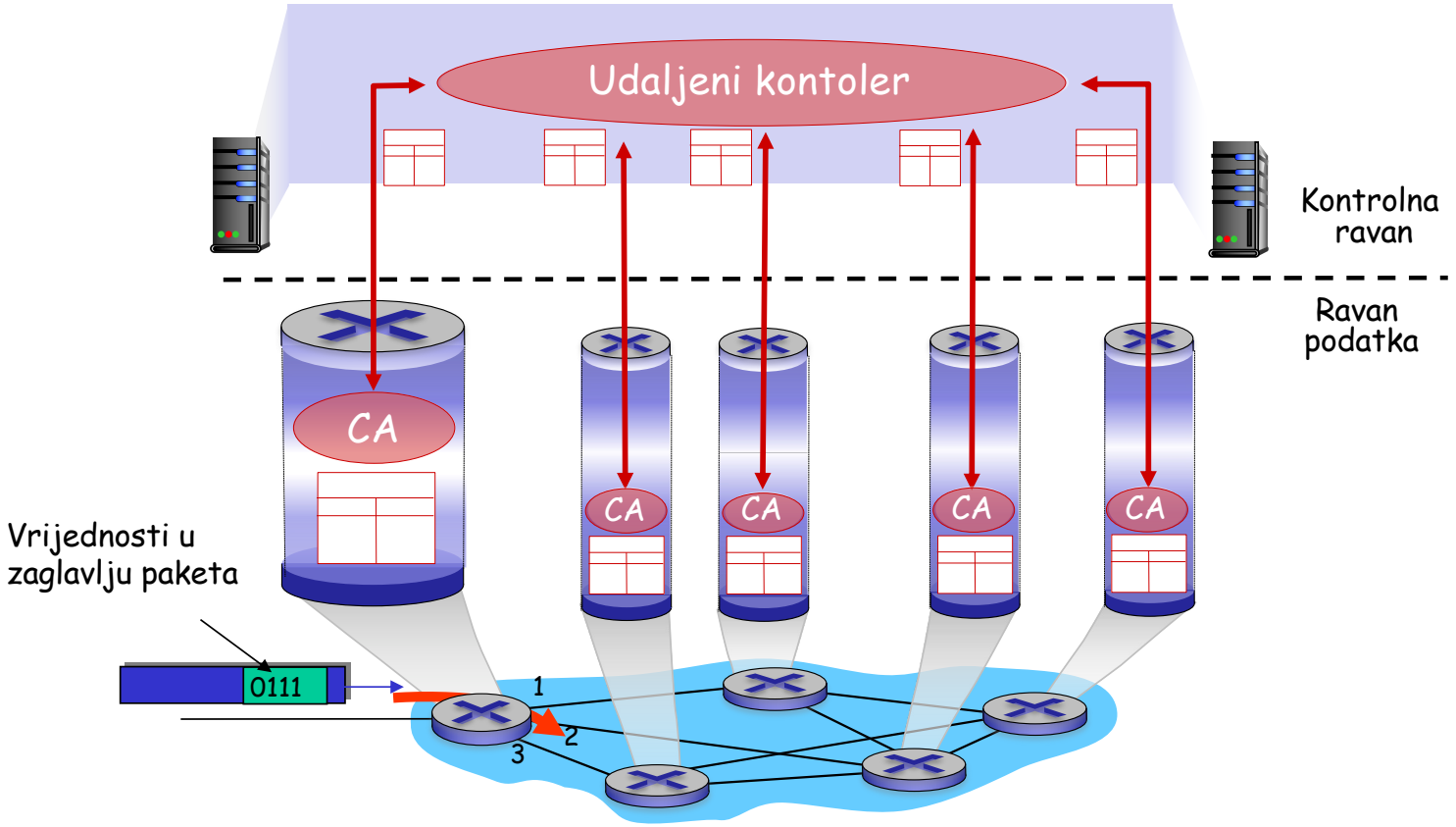
Distribuirana kontrolna ravan

Individualni algoritmi rutiranja se izvršavaju samostalno u svakom ruteruvi međusobno interaguju u kontrolnoj ravni



Centralizovana kontrolna ravan

Udaljeni kontroler utvrđuje i šalje tabele prosleđivanja ruterima



Mrežni servisni model

Koji *servisni model* nudi "kanal" koji transportuje datagrame od pošiljaoca do prijemnika?

Primjer servisa za individualne datagrame:

- Garantovana predaja
- Garantovana predaja sa kašnjenjem manjim od određene vrijednosti (recimo 40ms)

Primjer servisa za tok datagrama:

- Redosledna predaja datagrama
- Garantovani minimalni protok toka
- Ograničene promjene u međupaketskim intervalima
- Nivo zaštite

Modeli servisa mrežnog nivoa:

Mrežna arhitektura	Model Servisa	QoS garancije ?			
		Brzina prenosa	Gub.	Red.	Tajm.
Internet	best effort	bez	ne	ne	ne
ATM	CBR	konstantna brzina	da	da	da
ATM	VBR	garantov. brzina	ne	da	ne
Internet	Intserv	da	da	da	da
Internet	Diffserv	moguće	moguće	moguće	ne

Best-effort servis

- Jednostavnost dozvoljava masovno korišćenje Interneta
- Obezbjeđivanje dovoljnog kapaciteta mreže omogućava da *real time* aplikacije budu dovoljno kvalitetne veći dio vremena
- Distribuirani i replicirani servisi nivoa aplikacije (data centri, CDN) koji su blizu klijentskih mreža nude servise sa više lokacija
- Kontrola zagušenja "elastičnih" servisa pomaže

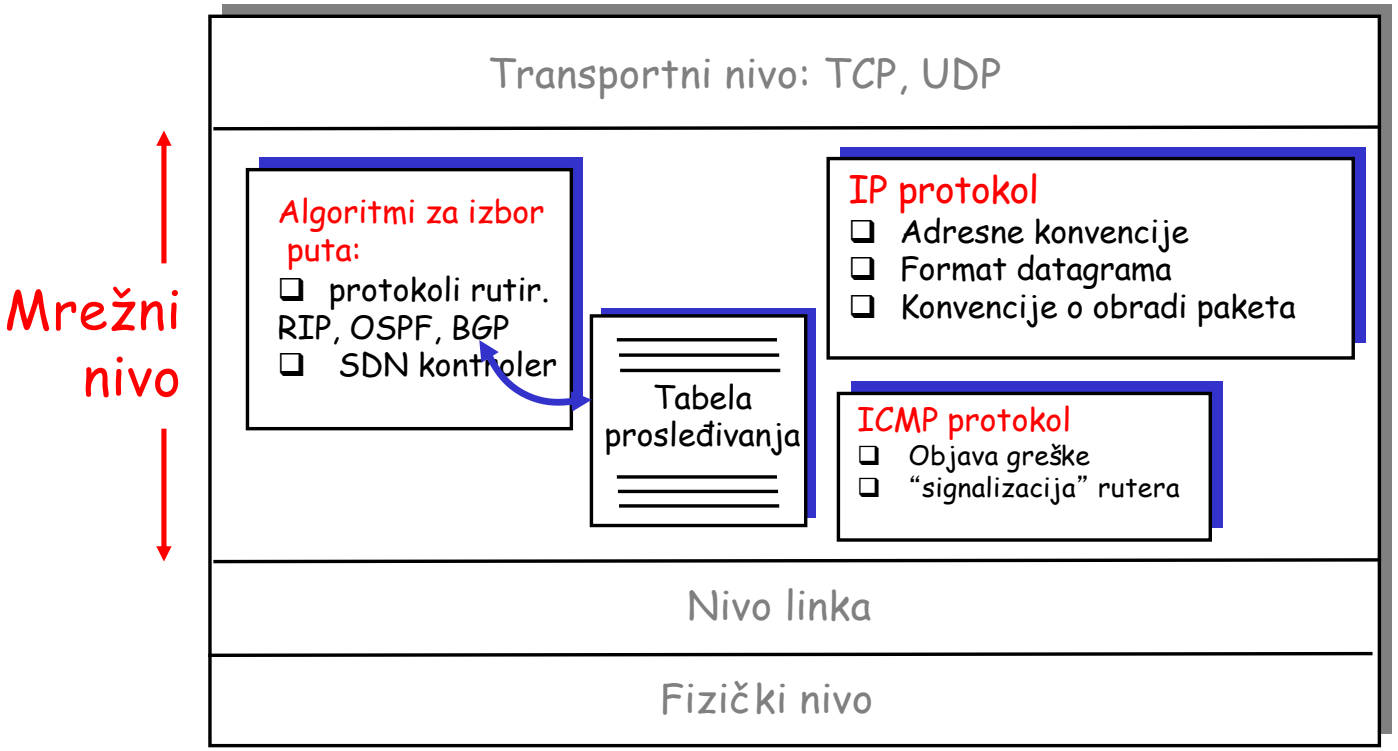
Teško je osporiti uspjeh *best-effort* servisa.

Glava 4: Mrežni nivo

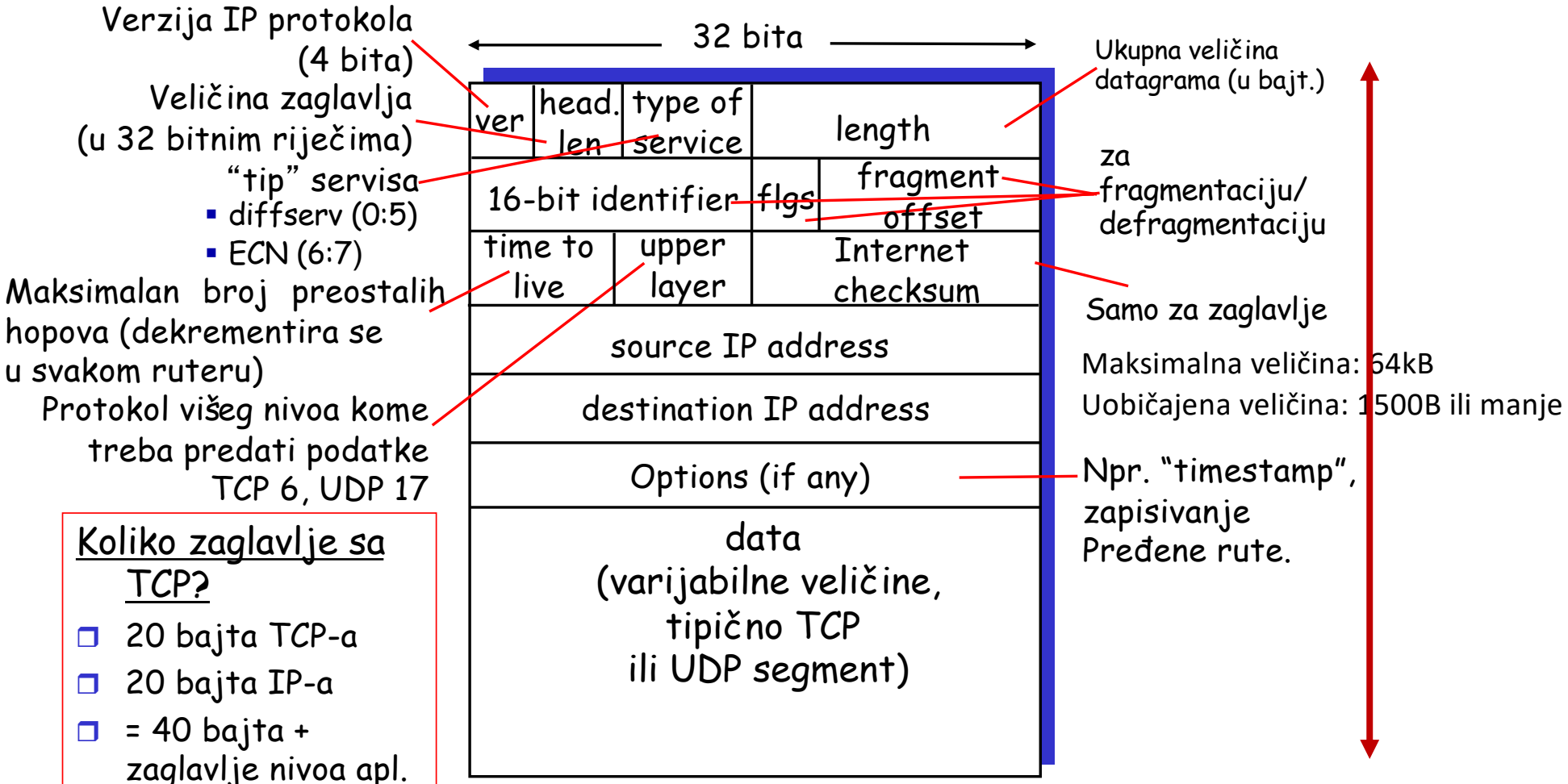
- Principi nivoa mreže
- IPv4 (Internet Protocol)
  - DHCP
  - NAT
  - ICMP
- IPv6
- Protokoli rutiranja
- Mrežni menadžment

Internet mrežni nivo

Host, ruter funkcije mrežnog nivoa:



Format IP datagrama

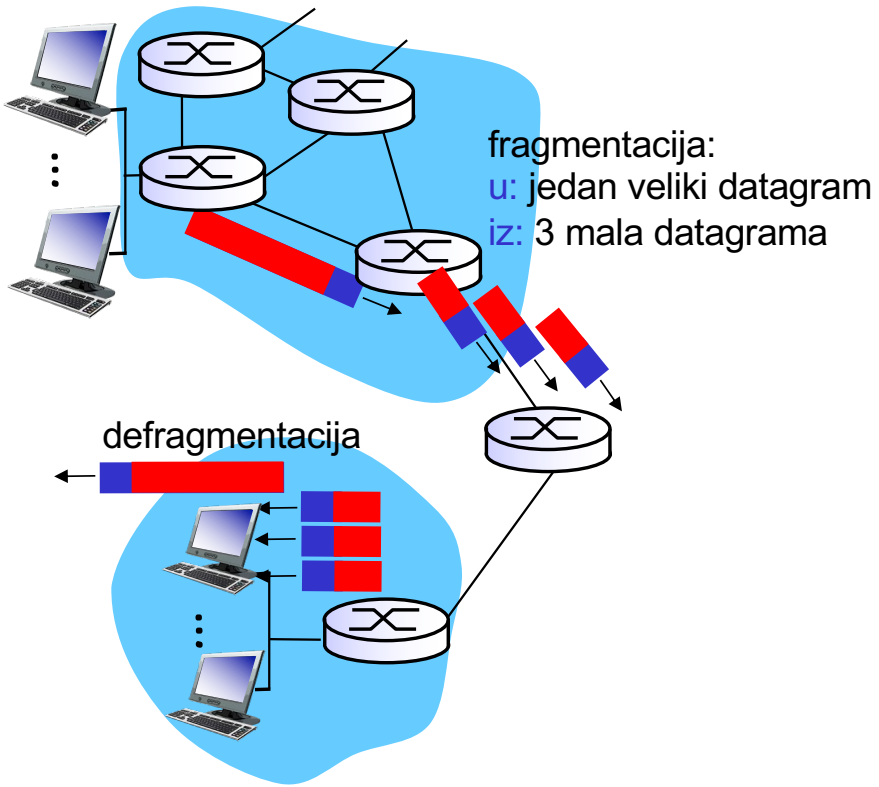


Koliko zaglavlje sa TCP?

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

IP Fragmentacija & Defragmentacija

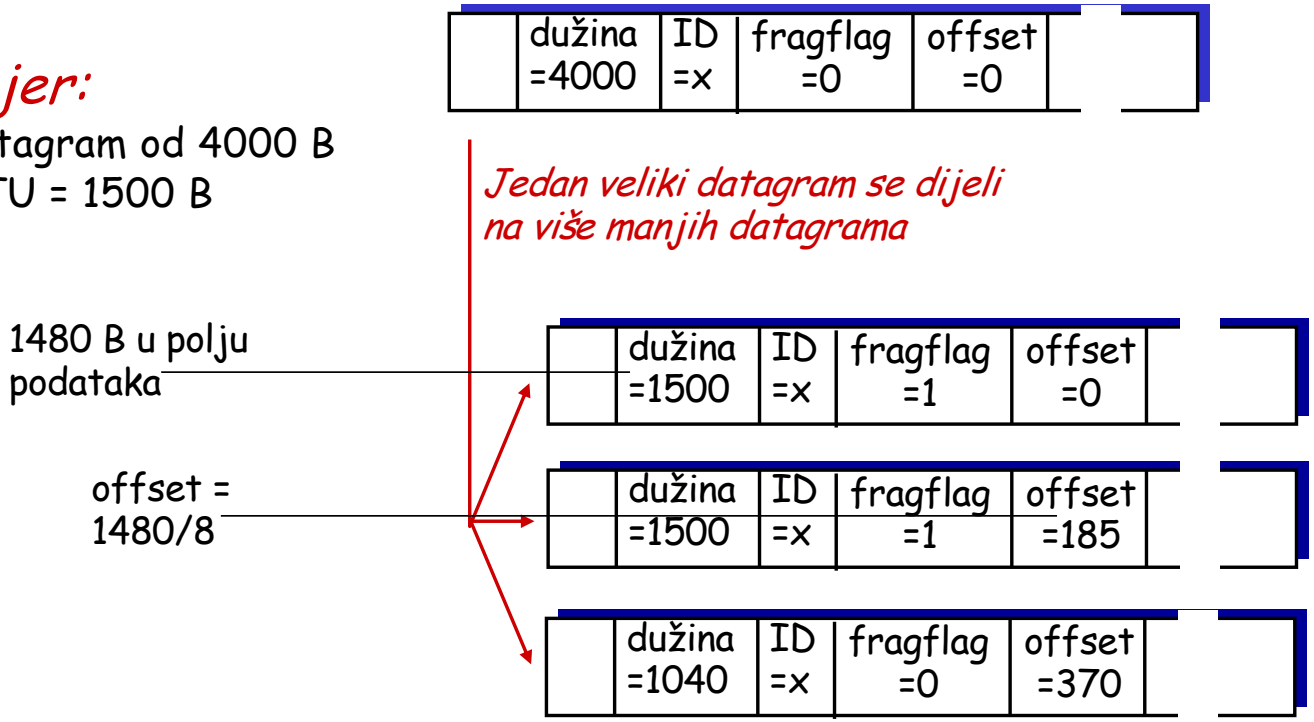
- Mrežni linkovi imaju MTU (max.transfer size) – najveći mogući okvir nivoa linka.
  - Različiti tipovi linkova, različiti MTU-ovi
- veliki IP datagram se dijeli ("fragmentira") u okviru mreže
  - jedan datagram postaje više datagrama
  - "defragmentira" se samo na krajnjoj destinaciji
  - IP biti zaglavlja se koriste za identifikaciju redosleda vezanog za fragment



IP fragmentacija, defragmentacija

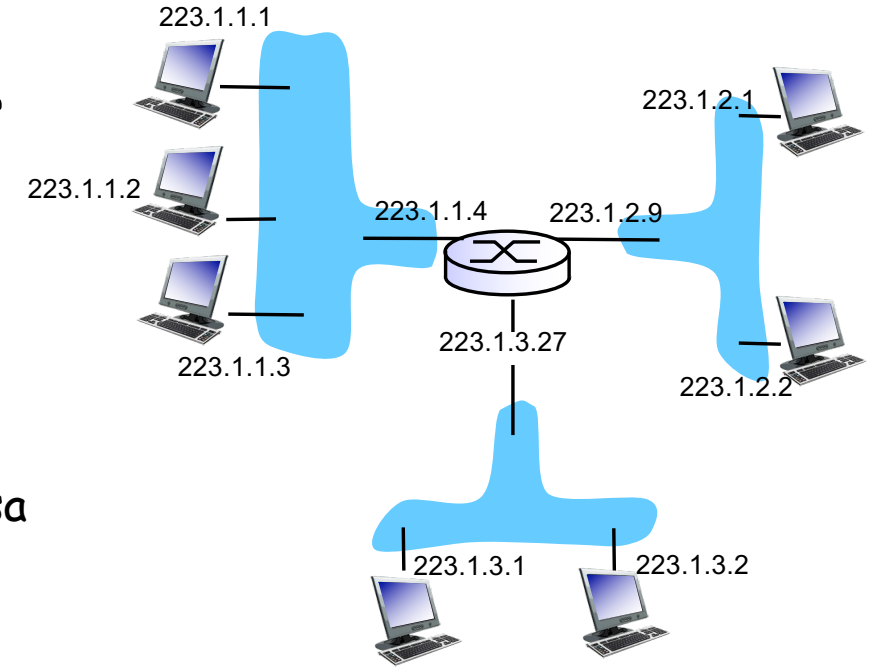
Primjer:

- Datagram od 4000 B
- MTU = 1500 B



IP Adresiranje: uvod

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

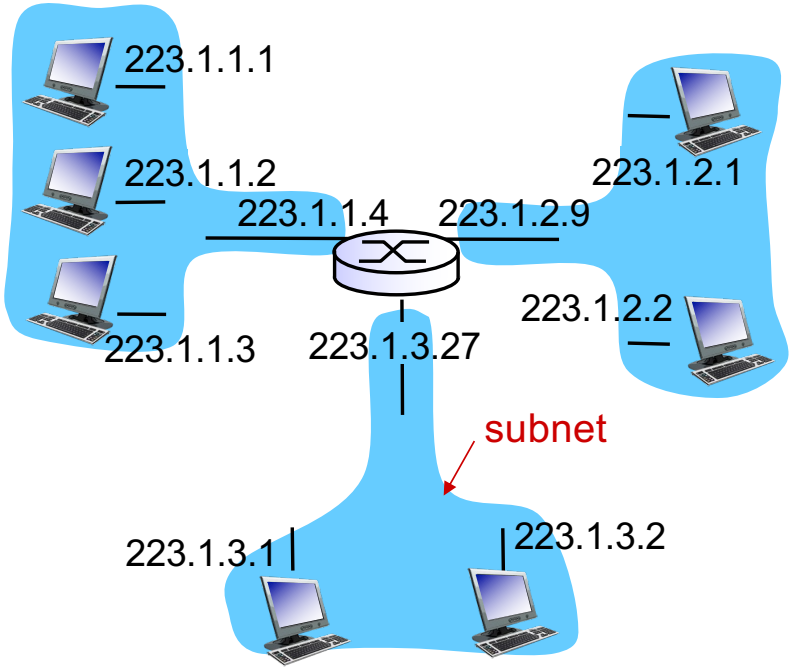


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

IP Adresiranje

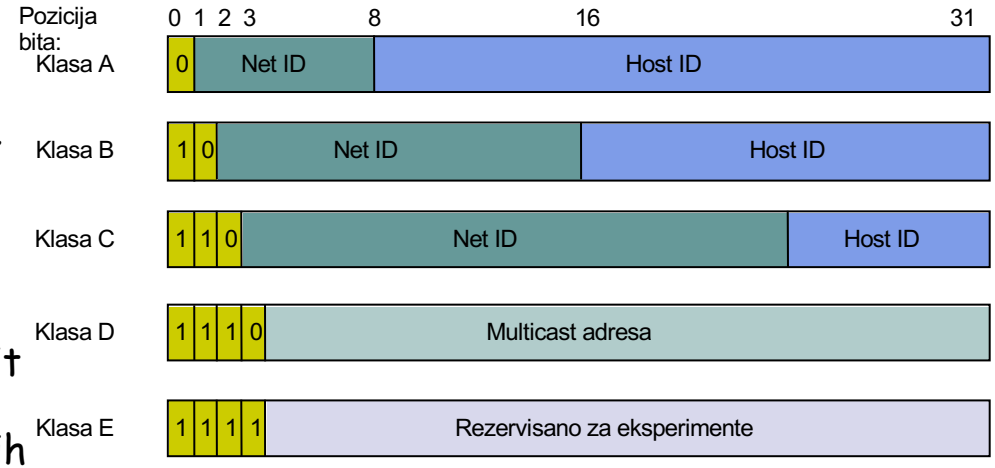
- IP adresiranje:
  - Mrežni dio (biti višeg reda)
  - Dio hosta (biti nižeg reda)
- *Šta je subnet?* (iz perspektive IP adrese)
  - Interfejsi uređaja sa istim mrežnim dijelom IP adrese
  - Interfejsi koji mogu fizički dosegnuti jedni druge bez učešća rutera



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

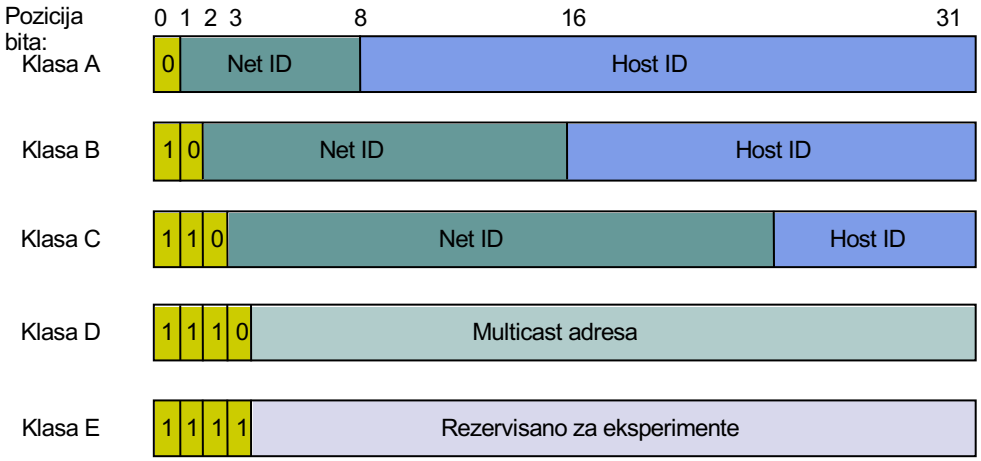
Classful IP Adresiranje

- 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.
- Klasa A ima 8 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.



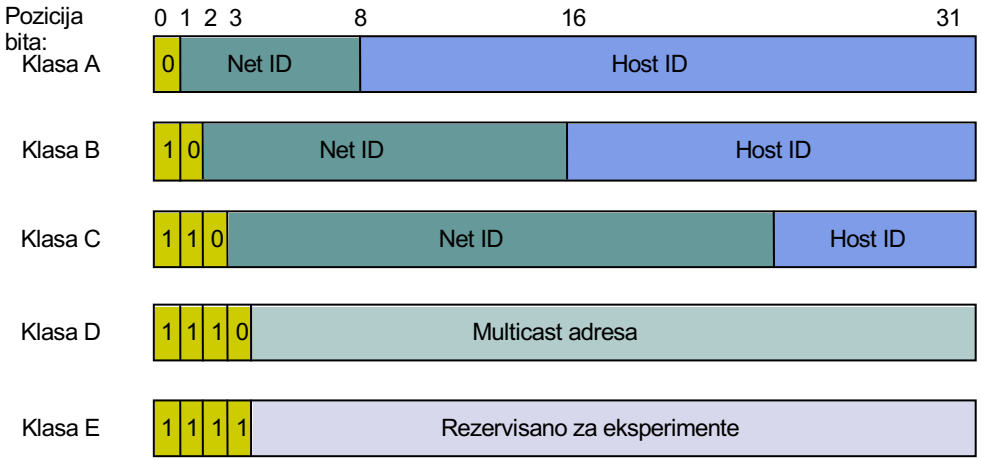
Classful IP Adresiranje

- Klasa B ima 16 bita za mrežni ID, što znači 2^{14}-2=16382 mreža i 2^{16}-2=65534 hostova. U klasu B spadaju adrese čija su prva dva bita uvijek 10. Ova klasa je namijenjena organizacijama srednje veličine. Opseg validnih mrežnih adresa klase B je od 128.1.0.0 do 191.254.0.0.
- Klasa C ima 21 bit za mrežni ID i 8 bita za host ID, što znači 2^{21}-2=2097150 mreža i 2^{8}-2=254 hostova. U klasu C spadaju adrese čija su prva tri bita uvijek 110. Ova klasa je namijenjena malim organizacijama. Opseg validnih mrežnih adresa klase C je od 192.0.1.0 do 223.255.254.0.



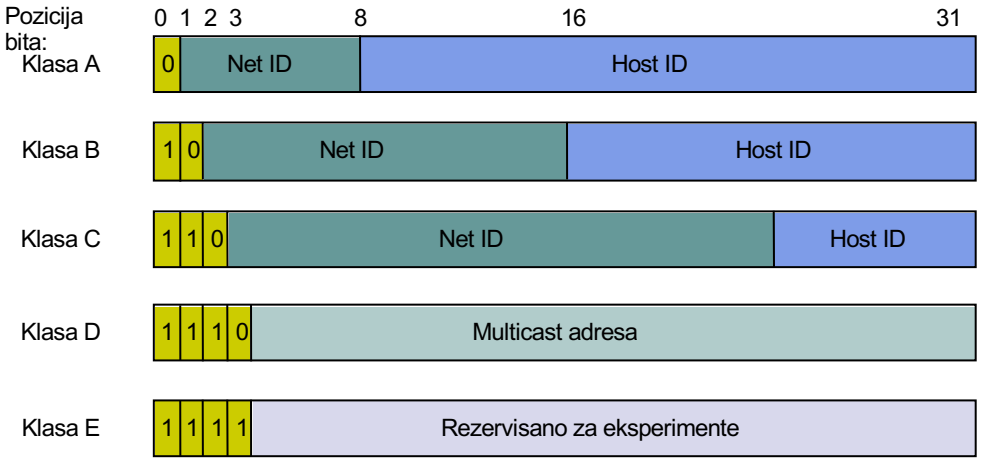
Classful IP Adresiranje

- Klasa D se koristi za multikast servis koji omogućava da host šalje paket grupi hostova koji pripadaju istoj multikast grupi. U klasu D spadaju adrese čija su prva četiri bita uvijek 1110. Ova klasa je namijenjena za multicast grupe. Opseg adresa koji pripadaju ovoj klasi je od 224.0.0.0 do 239.255.255.255. Ove adrese nijesu za komercijalnu upotrebu.
- Klasa E je rezervisana za eksperimente. U klasu E spadaju adrese čiji su prvih pet bita uvijek 11110. Ova klasa je namijenjena za multicat grupe. Opseg adresa koji pripadaju ovoj klasi je od 240.0.0.0 do 254.255.255.255. Ove adrese takođe nijesu za komercijalnu upotrebu.



Classful IP 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.



Classful IP Adresiranje

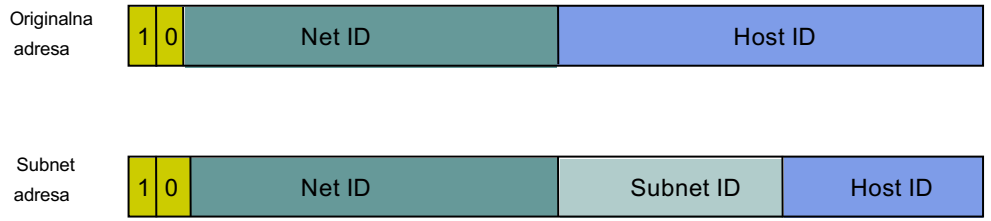
- IP adrese se najčešće pišu u formi tačka-decimalnog zapisa koji je pogodan za korišćenje od strane čovjeka. Adresa se dijeli na četiri bajta, pri čemu svaki bajt predstavlja decimalni broj, koji su razdvojeni tačkama. Na primjer adresa
- 10000000 10000111 01000100 00000101
  - 128 . 135 . 68 . 5
- Klasa adrese se lako određuje ispitivanjem prvog okteta adrese. U IP adresi 128.135.68.5 prvi oktet je 128. Kako 128 pada između 128 i 191, jasno je da je ovo IP adresa klase B.

Classful IP Adresiranje

- 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)

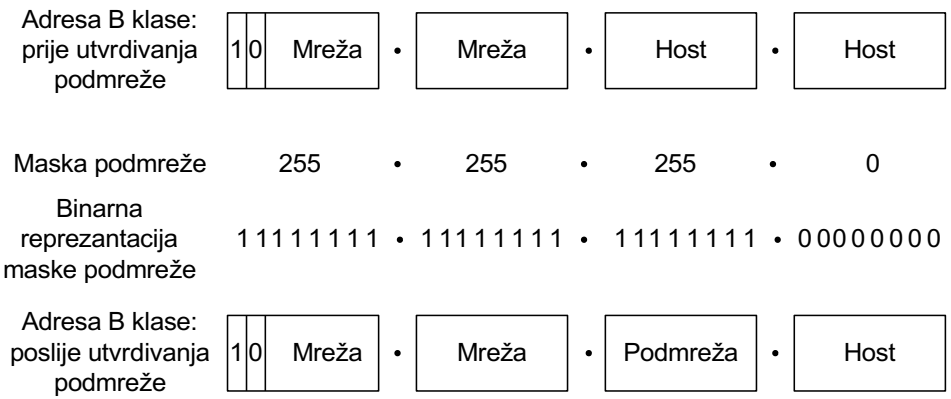
Classful IP Adresiranje

- 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.



Classful IP 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 171.16.0.0.
- 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.



Classful IP Adresiranje

U tabeli je prikazana je veza između binarne i decimalne reprezentacije maske podmreže.

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240
1	1	1	1	1	0	0	0	248
1	1	1	1	1	1	0	0	252
1	1	1	1	1	1	1	0	254
1	1	1	1	1	1	1	1	255

- Default maske podmreža su:
- - 255.0.0.0 (A klasa)
- - 255.255.0.0 (B klasa)
- - 255.255.255.0 (C klasa)

Classful IP Adresiranje

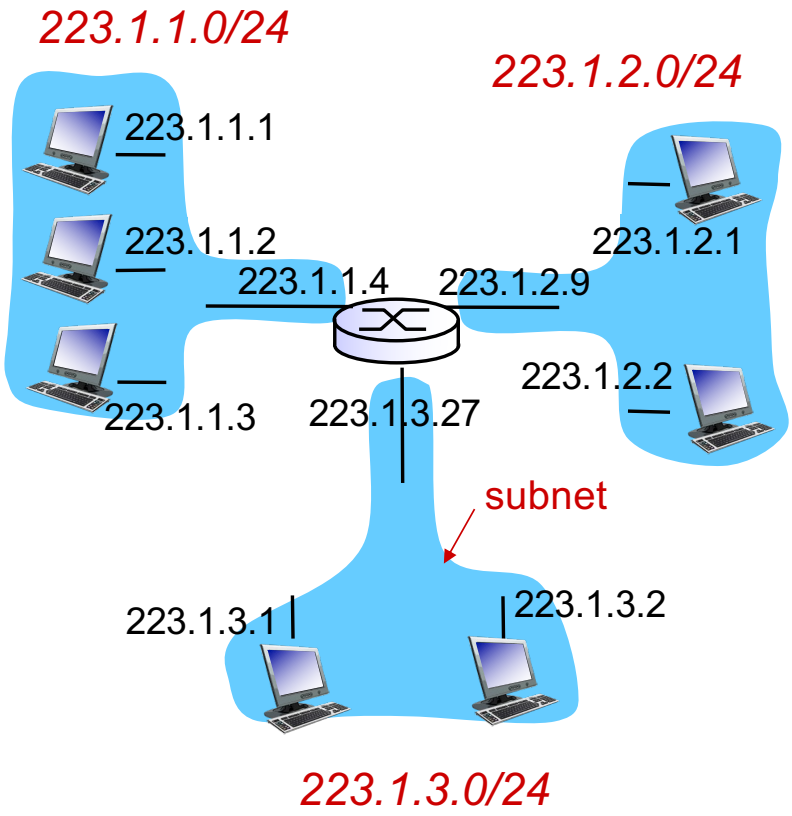
172	16	125	1	zadata adresa u decimalnom formatu
10101100	00010000	01111101	00000001	zadata adresa u binarnom formatu
255	255	0	0	default maska podmreže u decimalnom formatu
11111111	11111111	00000000	00000000	default maska podmreže u binarnom formatu
10101100	00010000	0	0	adresa mreže u binarnom formatu
172	**16**	**0**	**0**	**adresa mreže u decimalnom formatu**

172	16	125	1	zadata adresa u decimalnom formatu
10101100	00010000	01111101	00000001	zadata adresa u binarnom formatu
255	255	224	0	zadata maska podmreže u decimalnom formatu
11111111	11111111	11100000	00000000	zadata maska podmreže u binarnom formatu
10101100	00010000	01100000	00000000	adresa podmreže u binarnom formatu
172	**16**	**96**	**0**	**adresa podmreže u decimalnom formatu**

Broadcast adresa u ovoj podmreži je 172.16.127.255 (10101100.00010000.01111111.11111111). Opseg adresa koje pripadaju ovoj podmrežije od 172.16.96.1 (10101100.00010000.01100000.00000001) do 172.16.127.254 (10101100.00010000.01111111.11111110).

Podmreža

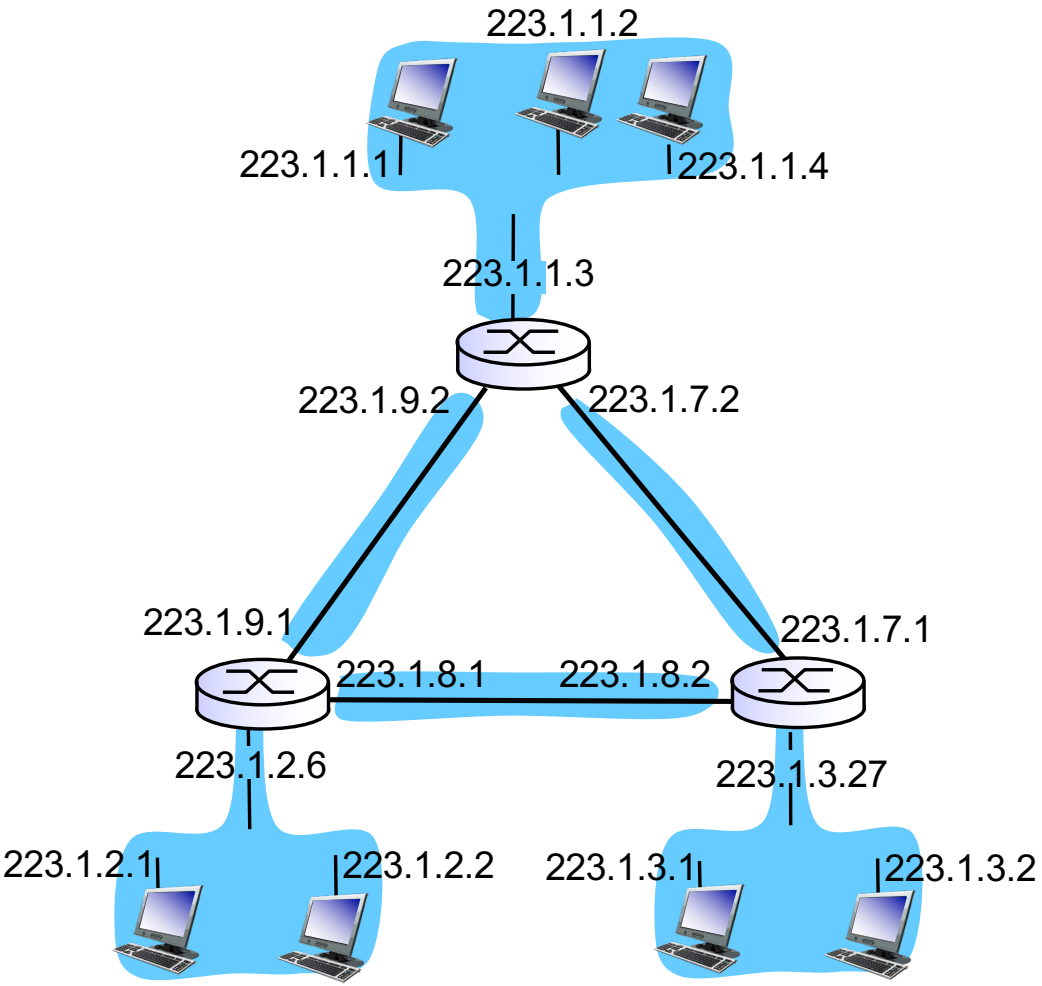
Da bi odredili podmreže, treba razdvojiti svaki interfejs od njegovog hosta ili rutera, kreirajući ostrva izolovanih mreža. Svaka izolovana mreža je podmreža.



Maska podmreže: /24

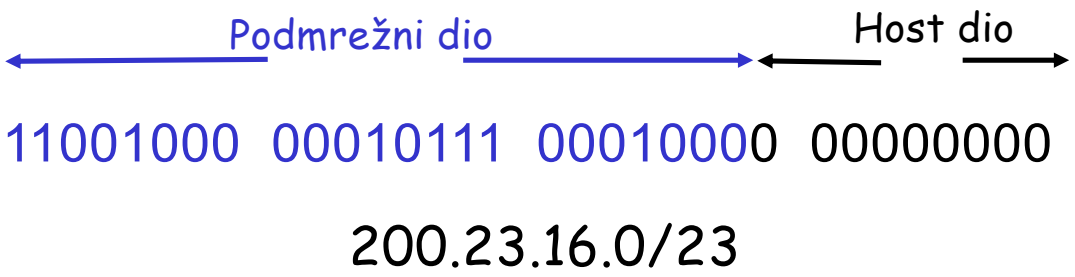
Podmreže

Koliko je podmreža?



IP adresiranje: CIDR

- 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



IP adrese: kako dobiti IP adresu?

Kako *host* dobija IP adresu?

- "hard-coded" od strane sistem administratora u fajlu
  - Winl: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- Dynamic Host Configuration Protocol (DHCP) server dinamički dodjeljuje adresu
  - "plug-and-play"

DHCP: Dynamic Host Configuration Protocol

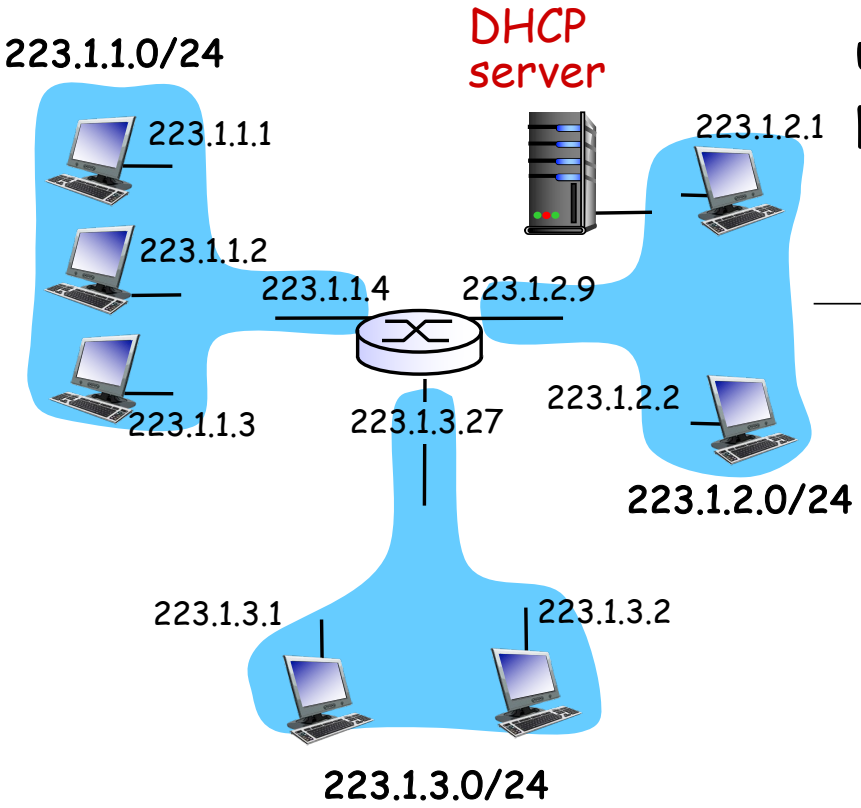
Omogućava hostu dinamičko dobijanje adresa sa mrežnog servera kada se poveže na mrežu

- Može obnoviti adresu koju je već koristio
- Omogućava "reuse" adresa (host zadržava adresu sok je uključen)
- Olakšava pristup mobilnim korisnicima koji se pridružuju mreži

DHCP:

- host svima šalje "DHCP discover" poruku (UDP segment na port 67)
- DHCP server odgovara "DHCP offer" porukom
- host zahtijeva IP adresu: "DHCP request" porukom
- DHCP server šalje adresu: "DHCP ack" porukom

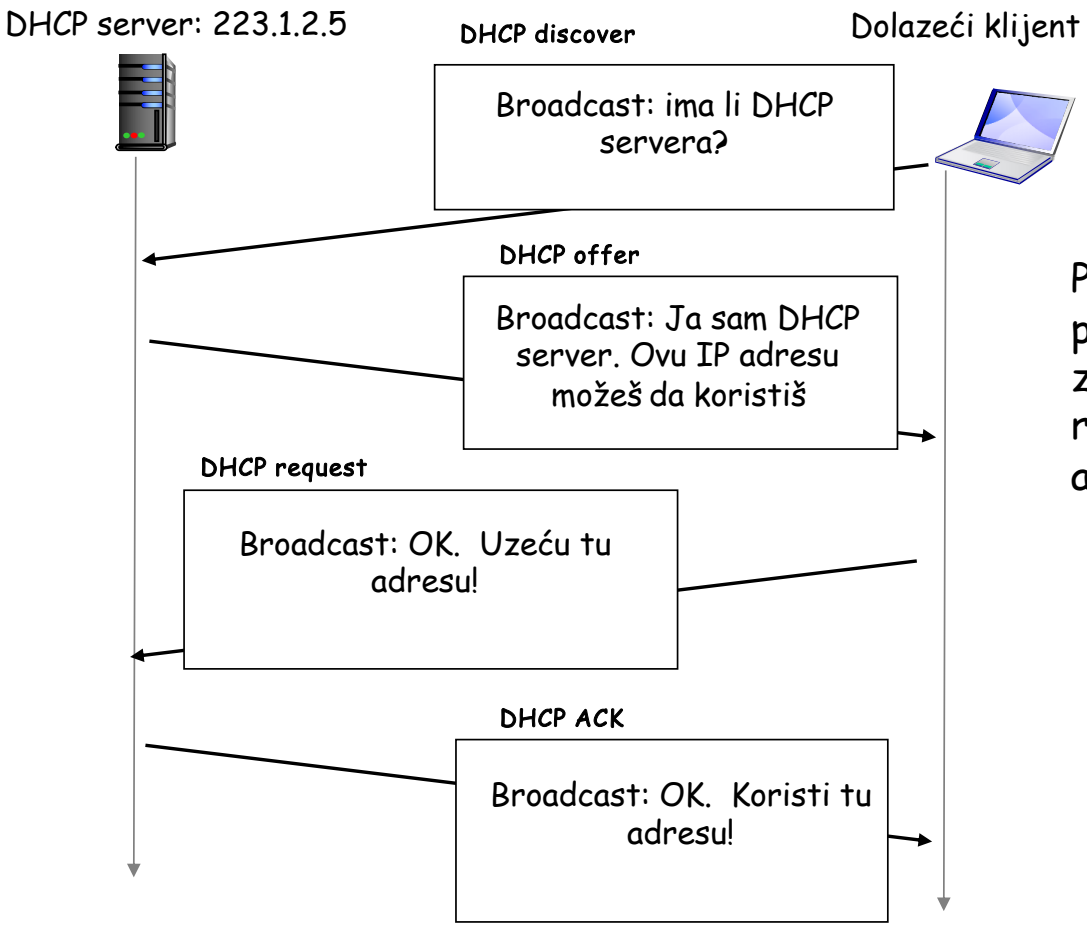
DHCP klijent-server scenario



Tipično je DHCP server lociran u ruteru, opslužujući sve podmreže na koje je povezan.

DHCP klijent treba adresu u novoj mreži

DHCP client-server scenario



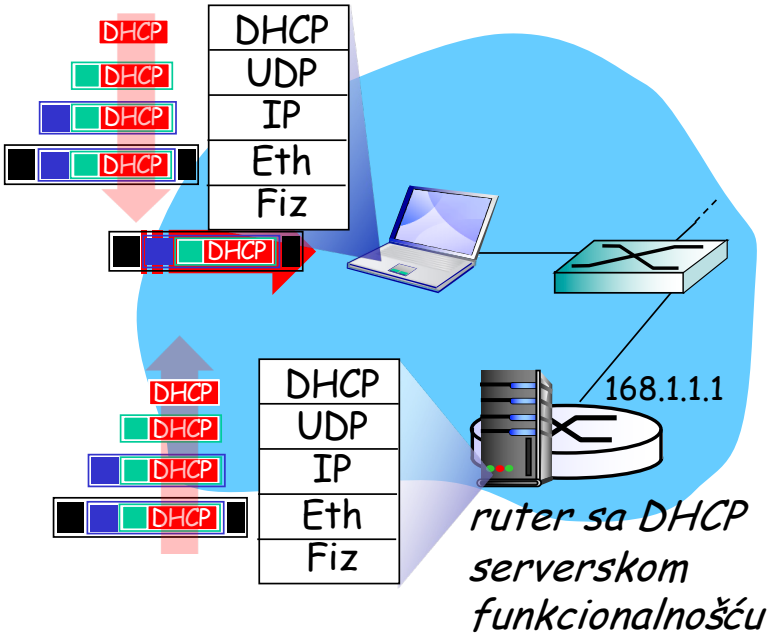
Prva dva koraka mogu biti preskočena "ako je klijent zapamtio i želi da koristi ranije alociranu mrežnu adresu" [RFC 2131]

DHCP: više od IP adrese

DHCP pored same alokacije IP adresa u podmreži obezbjeđuje:

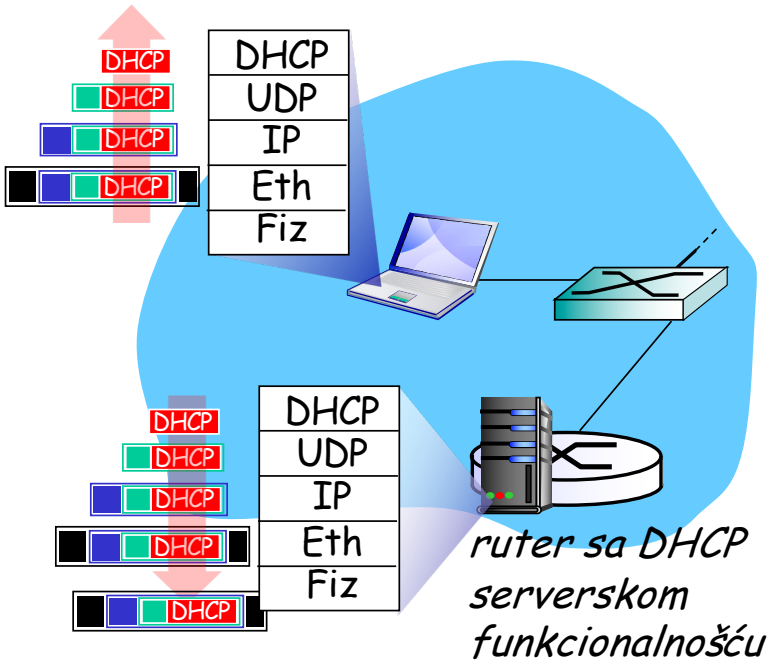
- Adresu gateway-a podmreže
- Ime i IP adresu DNS servera
- Subnet masku (indicira mrežni dio adrese)

DHCP: primjer



- Laptopu je potrebna IP adresa, adresa gateway-a, adresa DNS servera: koristi DHCP
- DHCP zahtjev se enkapsulira u UDP segment, pa u IP datagram, pa u 802.3 Ethernet frejm
- Ethernet frejm se šalje svim (dest: FFFFFFFFFFFF) interfejsima u LAN-u i prima od strane DHCP servera
- Na DHCP serveru se obavlja suprotan proces enkapsulaciji

DHCP: primjer



- DHCP server kreira DHCP potvrdu koja sadrži klijentsku IP adresu, IP adresu gateway-a, ime & IP adresu DNS servera
- Frejm se prosleđuje do klijenta koji ga raspakuje
- Klijentu je poznata IP adresa, ime i IP adresa DNS servera, IP adresa gateway-a

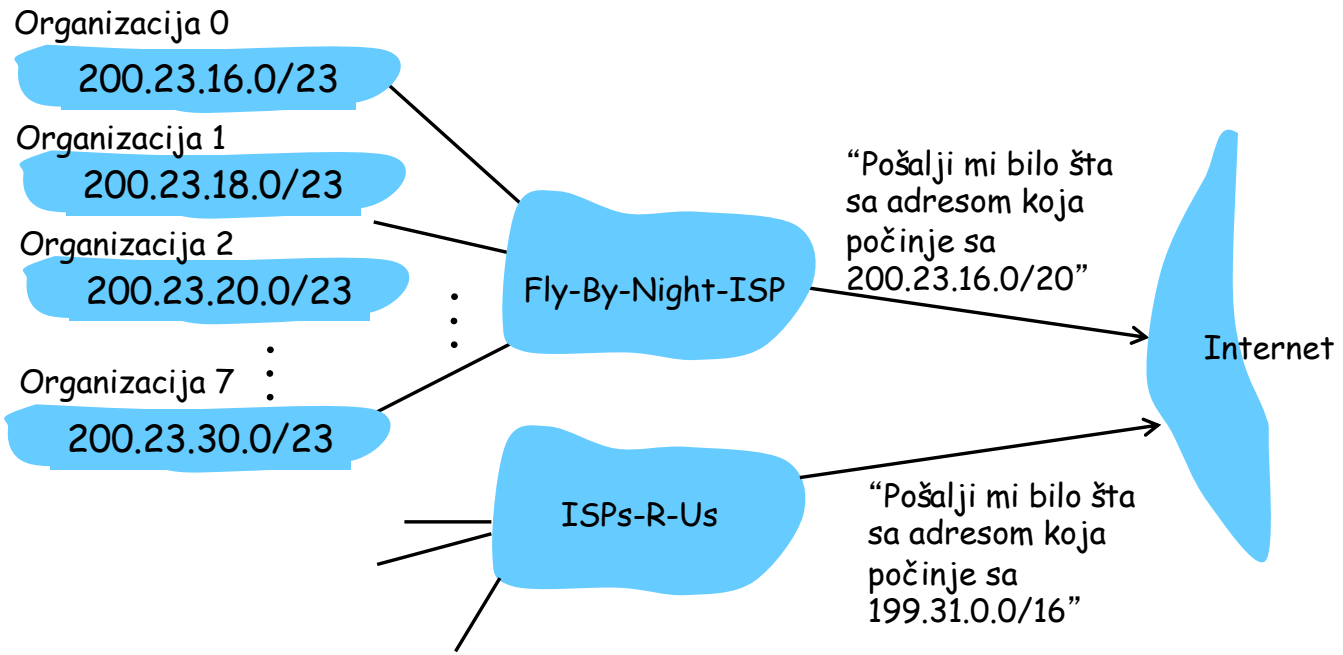
IP adrese: kako dobiti IP adresu?

Kako mreža dobija podmrežni dio IP adrese?

ISP-ov blok	11001000 00010111 00010000 00000000	200.23.16.0/20
Organizacija 0	11001000 00010111 00010000 00000000	200.23.16.0/23
Organizacija 1	11001000 00010111 00010010 00000000	200.23.18.0/23
Organizacija 2	11001000 00010111 00010100 00000000	200.23.20.0/23
...	....	....
Organizacija 7	11001000 00010111 00011110 00000000	200.23.30.0/23

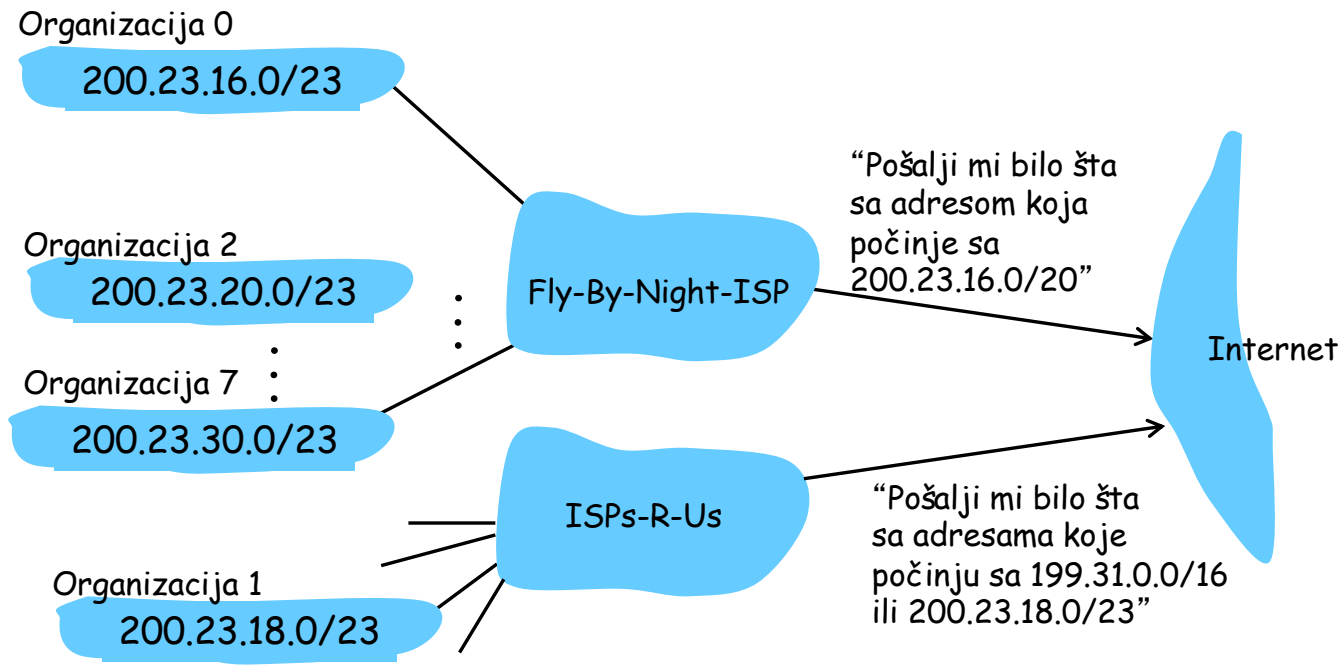
Hijerarhijsko adresiranje: agregacija ruta

Hijerarhijsko adresiranje dozvoljava efikasno oglašavanje informacije potrebne za rutiranje:



Hijerarhijsko adresiranje: specifičnije rute

ISPs-R-Us ima više specifičnih ruta do Organizacije 1



IP adresiranje: poslednja riječ...

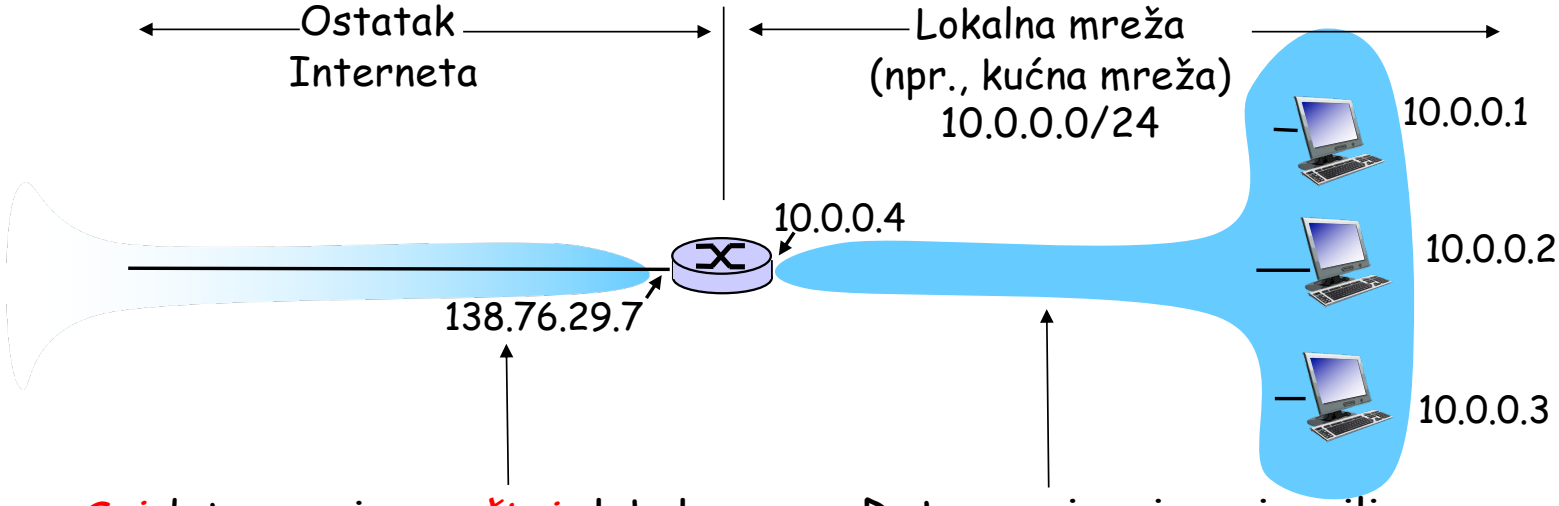
Kako ISP dobija svoj blok adresa?

ICANN: Internet Corporation for Assigned Names and Numbers

- http://www.icann.org
- Dodjeljuje adrese
- Upravlja DNS
- Dodjeljuje imena domena, razrješava sporove
- Dodjeljuje adrese lokalnim regionalnim Internet registrima (ARIN, RIPE, APNIC, LACNIC i AFRINIC)
- Poslednji skup IPv4 adresa je dodijeljen 2011. godine

NAT: Network Address Translation

NAT: svi uređaji lokalne mreže dijele samo jednu IPv4 adresu dok god to ostatku Interneta ne zasmeta



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

Lokalna mreža koristi samo jednu javnu IP adresu

- Nema potrebe za dodjelu opsega adresa od strane ISP (samo jedna IP adresa se koristi za sve uređaje)
- Mogu se 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

NAT ruter mora:

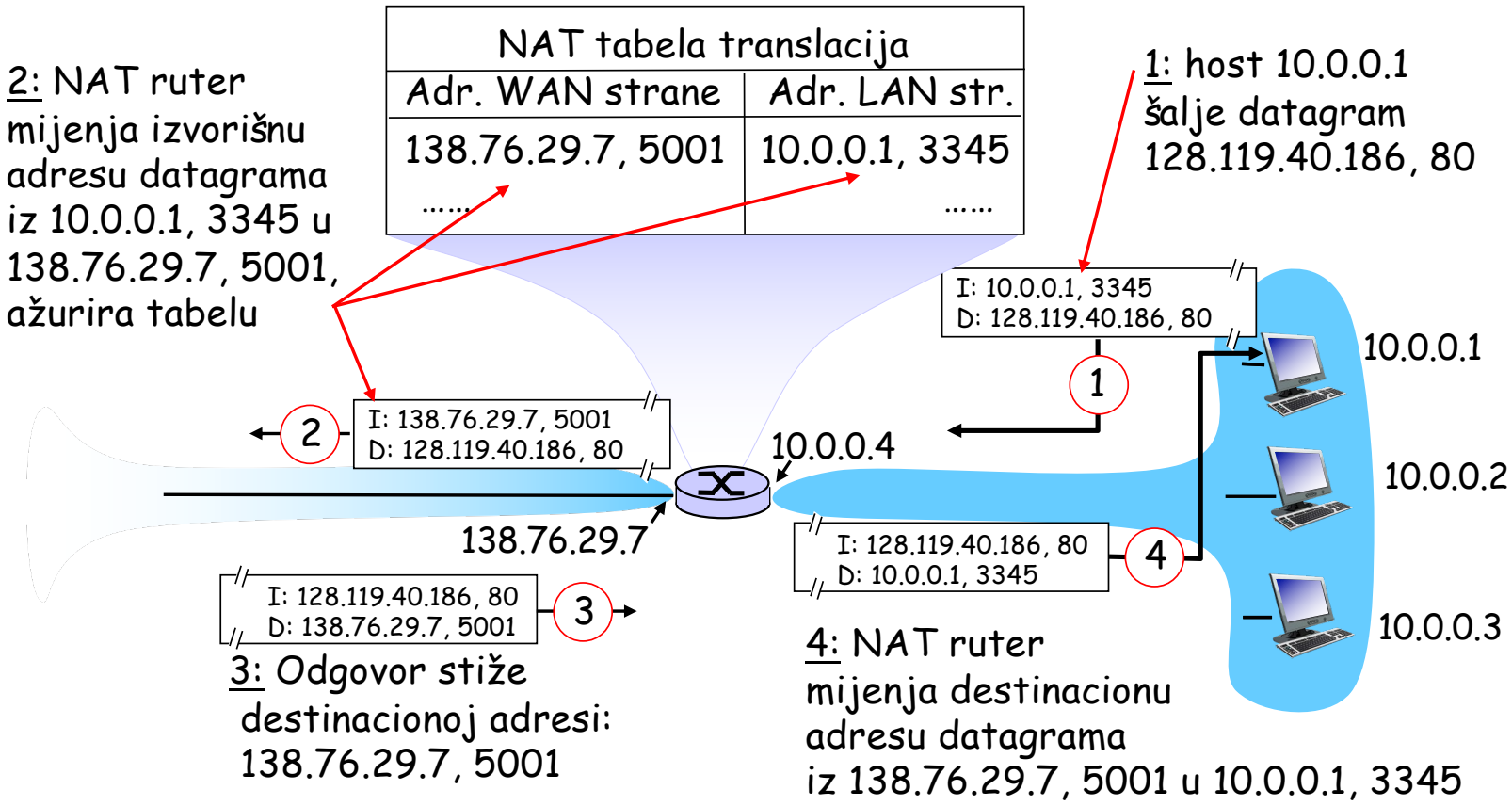
- *odlazni datagrami:* zamijeniti (izvorišnu IP adresu, broj port) svakog odlaznog datagrama sa (NAT IP adresom, novim brojem porta)

  . . . 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 translaticionog 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 masovno koristi u kućnim, kompanijskim, 4G/5G mrežama,...

ICMP: Internet Control Message Protocol

- koriste hostovi, ruteri, "gateway" za prenos informacija nivoa mreže
  - obavještenje o greški: nedostižan host, mreža, port, protokol
  - echo zahtjev/odgovor (koristi ga ping)
- Mrežni nivo "iznad" IP:
  - ICMP poruke se nose u IP datagramima
- ICMP poruke: tip, kod i prvih 8 bajtova IP datagrama koji je izazvao grešku

Tip	Kod	Opis
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute i ICMP

- Izvor šalje serije UDP segmenata do destinacije
  - Prva trojka ima TTL =1
  - Druga trojka ima TTL=2, itd.
  - Nepoželjni broj porta
- Kada n-ti datagram stigne na n-ti router:
  - ruter odbacuje datagram
  - šalje izvoru ICMP poruku (tip 11, kod 0)
  - poruka uključuje ime rutera & IP adresu
- Kada ICMP poruka stigne, izvor izračunava RTT
- Traceroute to ponavlja 3 puta

Kriterijum zaustavljanja

- UDP segment eventualno stigne do destinacionog hosta
- Destinacija vraća ICMP "port unreachable" paket (tip 3, kod 3)
- Kada izvor dobije ovaj ICMP, zaustavlja se.

Glava 4: Mrežni nivo

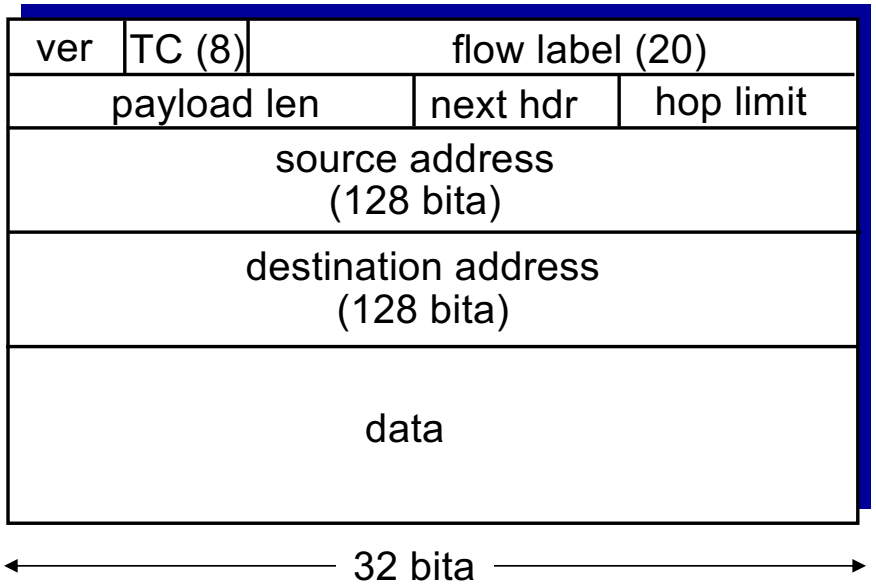
- Principi nivoa mreže
- IPv4 (Internet Protocol)
  - DHCP
  - NAT
  - ICMP
- IPv6
- Protokoli rutiranja
- Mrežni menadžment

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 zaglavlje (nastavak)

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



Druge izmjene u odnosu na IPv4

- *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 0000000000011011 0000000000000000 0000000000000000 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

IPv6 adresiranje

Tri tipa adresa:

- *unicast* – označava adresu jednog interfejsa na uređaju
- *multicast* – označava grupu interfejsa (uglavnom na različitim računarima) tako da paket poslat na ovu adresu stiže **do svih** adresiranih interfejsa koji pripadaju istom multicast stablu
- *anycast* –paket poslat na *anycast* adresu stiže **do jednog od interfejsa** opisanih ovom adresom (po pravilu najbližeg definisano pojmom rastojanja u protokolu rutiranja)

  Nema više broadcast adrese. Njenu funkciju preuzima multicast adresa, čime se stvara mogućnost korišćenja adresa koje se sastoje od svih nula i jedinica.

IPv6 adresiranje

Dodjela IPv6 adresa:

- Kombinacija alokacije i automatske dodjele.
- Prvih nekoliko bita (Format prefiks) se koriste za alokaciju adresa.

Tip adrese	Binarni prefiks	IPv6 notacija
Unspecified	00...0 (128 bita)	::/128
Loopback	00...1 (128 bita)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Global Unicast	(sve ostalo)	

IPv6 adresiranje

Unspecified Adresa

- Adresa sa svim nulama: 0:0:0:0:0:0:0:0.
- Označava da IPv6 adresa nije definisana za interfejs. Datagrame sa ovom odredišnom adresom ne prosleđuje IPv6 ruter.

Loopback Adresa

- IPv6 loopback adresa je 0:0:0:0:0:0:0:1.
- Njeno korišćenje je slično korišćenju IPv4 loopback adrese 127.0.0.1.

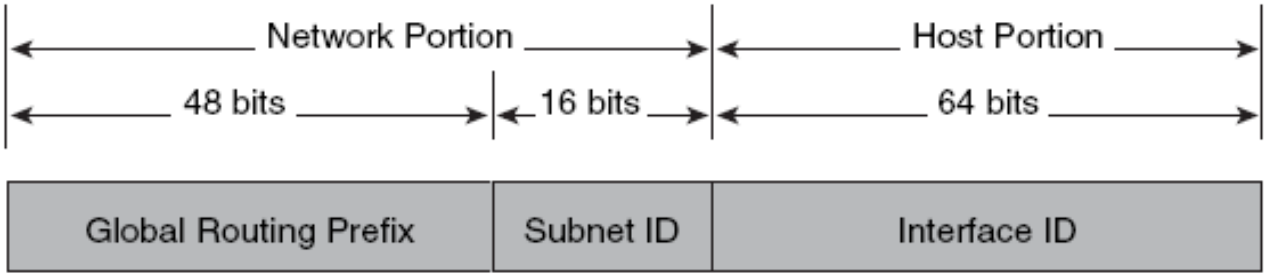
IPv4 mapirane adrese:

- Prvih 80 bita su nule
- Sledećih 16 bita su jedinice
- Ostalih 32 bita su jednaki bitima odgovarajuće IPv4 adrese
- 100.1.1.1 = 01100100 00000001 00000001 00000001=6401:0101
- 0000:0000:0000:0000:0000:FFFF:6401:0101 ili
- 0:0:0:0:0:FFFF:6401:0101 ili
- ::FFFF:6401:0101 ili čak ::FFFF:100.1.1.1

IPv6 adresiranje

IPv6 globalna adresa

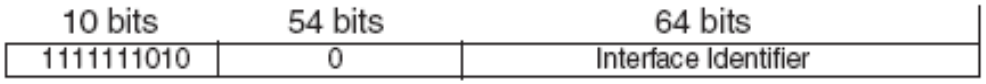
- Koristi se za povezivanje na javnu mrežu.
- Ove unicast adrese su jedinstvene i na bazi njih ruteri mogu prosleđivati pakete.
- RFC 2374, RFC 3587
- Globalni prefiks rutiranja (generalno je dužine 48 bita), identifikator subneta (dužine 16 bita) i identifikator interfejsa (dužine 64 bita)



IPv6 adresiranje

IPv6 *link-local* adresa

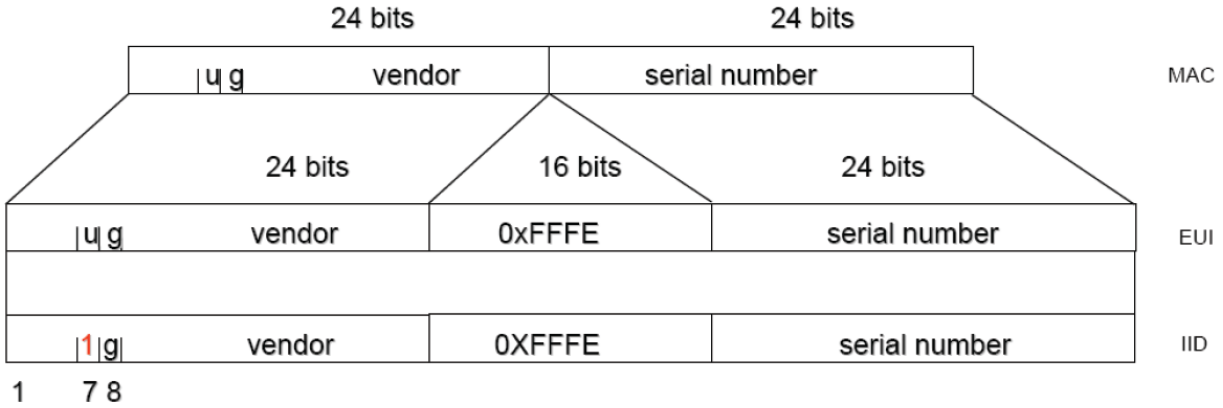
- Koriste se za adresiranje na jednom linku (mrežni segment bez rutera, npr. LAN).
- Značajne samo za čvorišta u okviru jedne LAN mreže.
- Ruteri ne prosleđuju pakete sa ovim izvorišnim ili odredišnim adresama van LAN-a.
- Koriste se za automatsko dodjeljivanje adresa, otkrivanje susjeda ili kada nema rutera u mreži.
- Ove adrese su identifikovane sa FE8 heksadecimalnim brojevima (10 bita) na početku.
- Konfigurišu se automatski ili manuelno.
- 1111111010 + 54 nule i 64-bitni identifikator interfejsa.
- Identifikator interfejsa se dobija automatski, komunikacijom sa drugim čvorištem na linku.



IPv6 adresiranje

Identifikator interfejsa

- U modifikovanom EUI-64 formatu
- Jedinstven unutar jedne podmreže

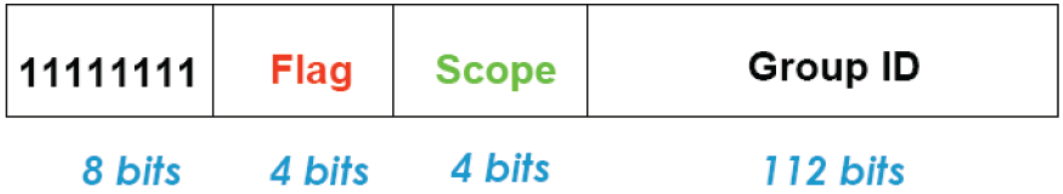


- u=1, adresa se formira na bazi MAC adrese (global scope)
- u=0, adresa se formira na slučajan način (local scope)

IPv6 adresiranje

IPv6 *multicast* adresa

- Ista funkcija kao IPv4 multicast adresa



FF00::/8 addresses are multicast addresses

Flag bits: 0 R P T

T = 0 *permanent addresses (managed by IANA)*

T = 1 *transient multicast addresses*

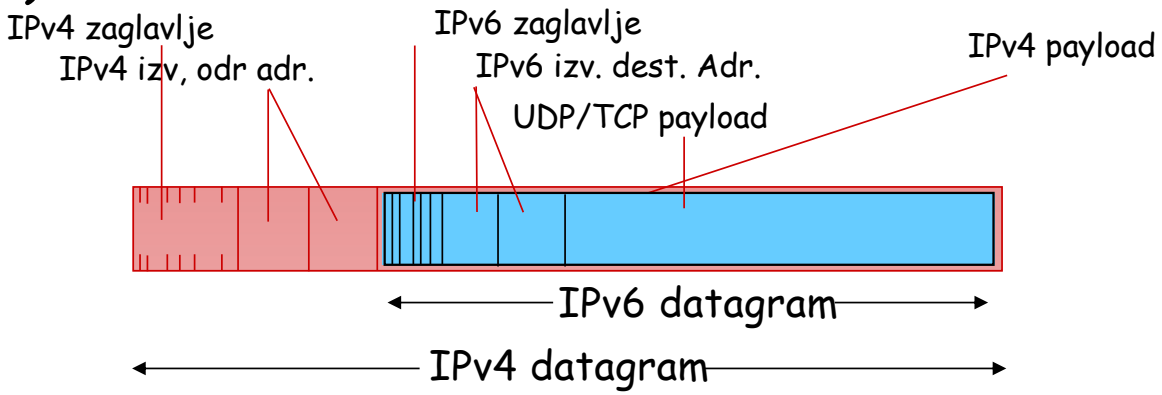
- P = 1 *derived from unicast prefix (RFC3306)*
  - R = 1 *embedded RP addresses (I-D)*

Scope

0 : Reserved
1 : Interface-local
2 : Link-local
3 : Subnet-local
4 : Admin-local
5 : Site-local
8 : Organization-local
E : Global
F : Reserved

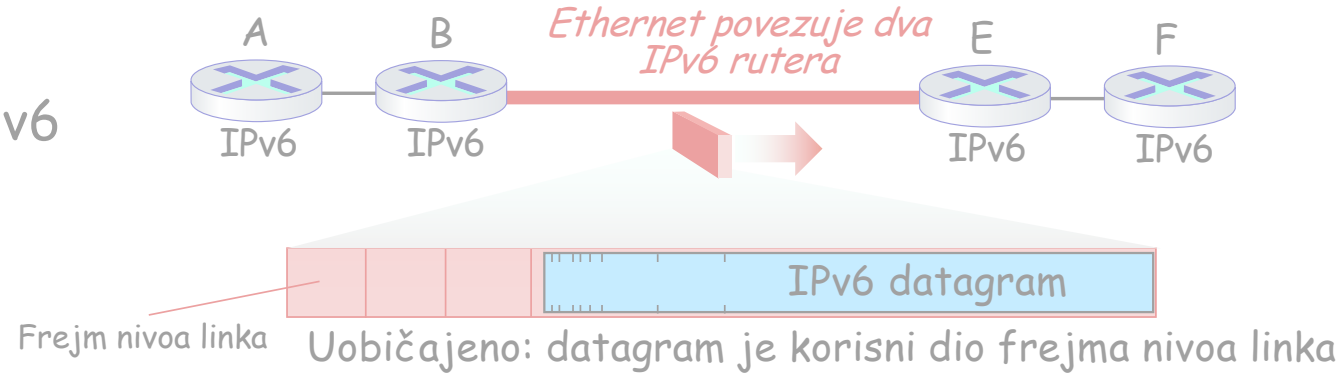
Tranzicija sa IPv4 na IPv6

- Ne mogu svi ruteri biti jednovremenovano nadograđeni sa IPv6 funkcionalnostima
  - nema "dana D"
  - Kako može da funkcioniše mraža IPv4 i IPv6 rutera?
- tunelovanje: IPv6 datagram se prenosi kao korisni sadržaj IPv4 datagrama ("paket u paketu")
  - Tunelovanje se često koristi u telekomunikacionim mrežama (4G/5G)

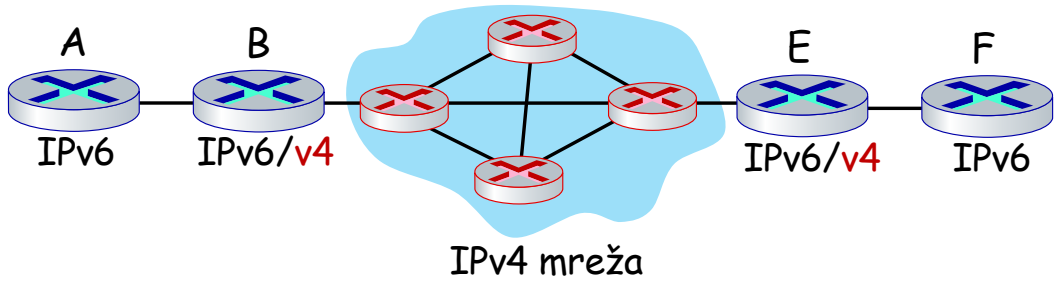


Tunelovanje i enkapsulacija

Ethernet povezuje dva IPv6 rutera:

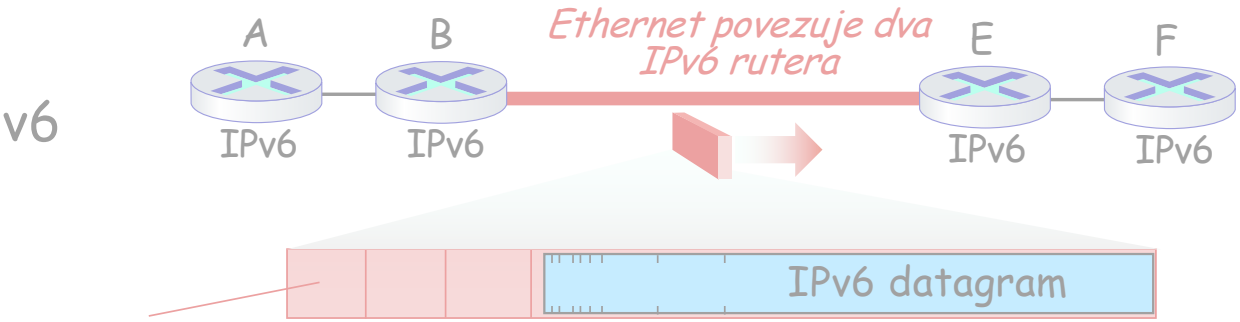


IPv4 mreža povezuje dva IPv6 rutera



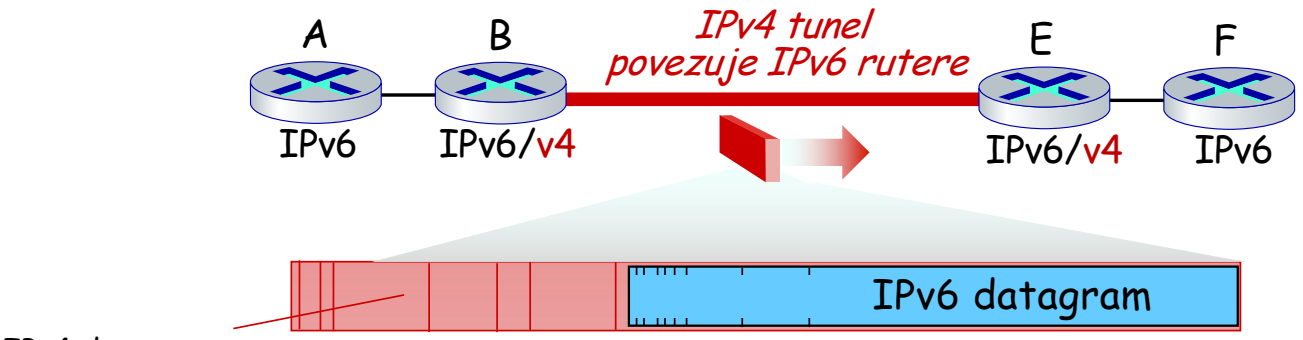
Tunelovanje i enkapsulacija

Ethernet povezuje dva IPv6 rutera



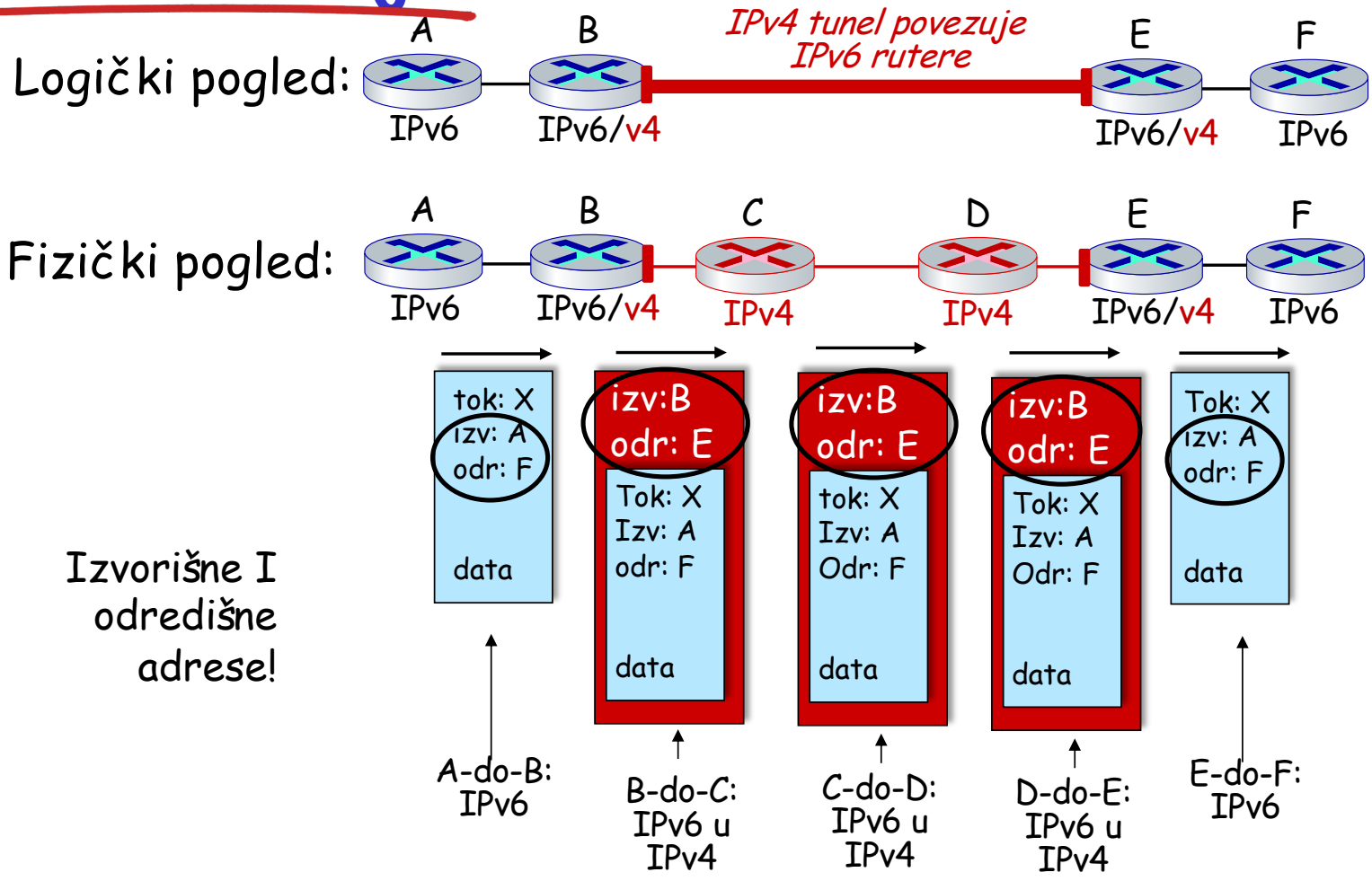
Uobičajeno: datagram se prenosi kao korisni dio frejma nivoa linka

IPv4 tunel povezuje dva IPv6 rutera



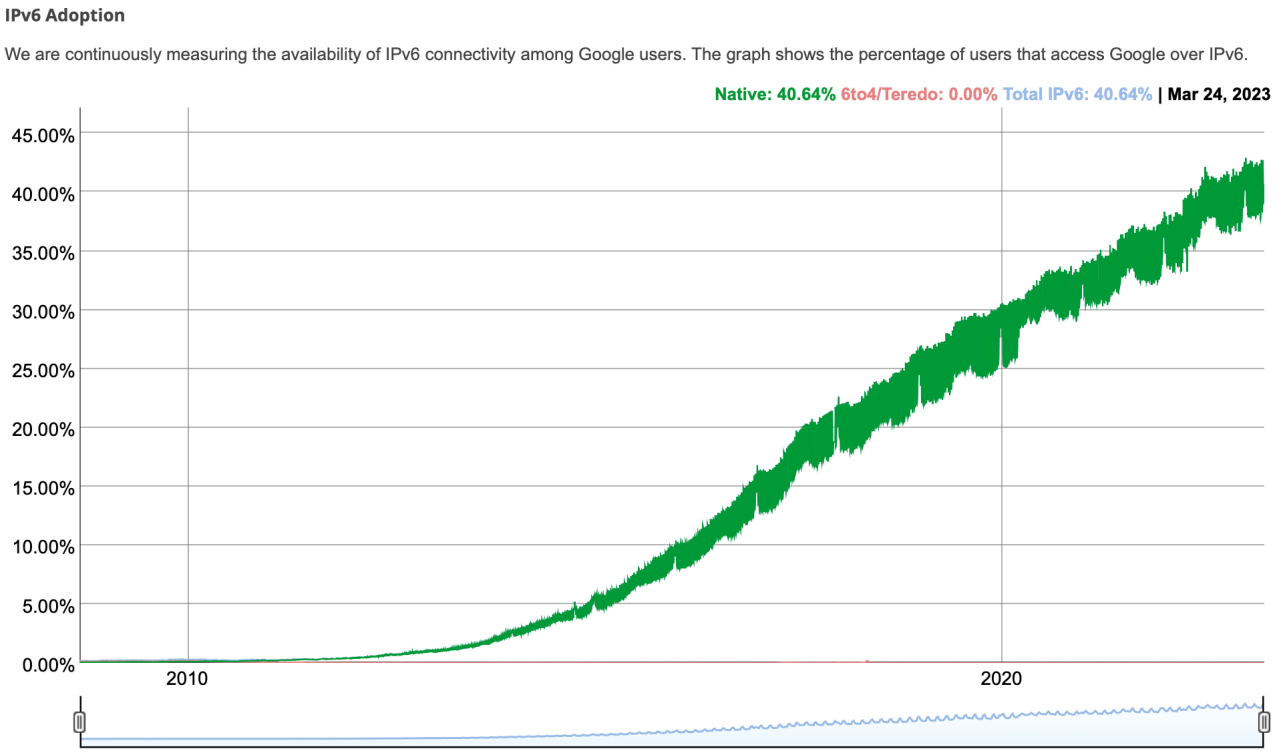
tunelovanje: IPv6 datagram je korsni dio IPv4 datagrama

Tunelovanje



IPv6: uvođenje

- Google[1]: ~ 40% klijenata pristupa preko IPv6
- NIST: 1/3 svih US državnih domena podržavaju IPv6



1 https://www.google.com/intl/en/ipv6/statistics.html

IPv6: uvođenje

- Google[1]: ~ 40% klijenata pristupa preko IPv6
- NIST: 1/3 svih US državnih domena podržavaju IPv6
- Predugo traje
  - 25 godina i …
  - Promjene na nivou aplikacije u poslednjih 25 godina: WWW, društvene mreže, streaming media, igrice, telepresence, …
  - *Zašto tolika razlika?*

[1] https://www.google.com/intl/en/ipv6/statistics.html

Glava 4: Mrežni nivo

- Principi nivoa mreže
- IPv4 (Internet Protocol)
  - DHCP
  - NAT
  - ICMP
- IPv6
- Protokoli rutiranja
- Mrežni menadžment

Intra-AS Rutiranje

- Poznato kao Interior Gateway Protocols (IGP)
- Najpozantiji Intra-AS protokoli rutiranja:
  - RIP: Routing Information Protocol
  - OSPF: Open Shortest Path First
  - IGRP: Interior Gateway Routing Protocol (vlasništvo kompanije Cisco)
  - IS-IS: Intermediate system to intermediate system

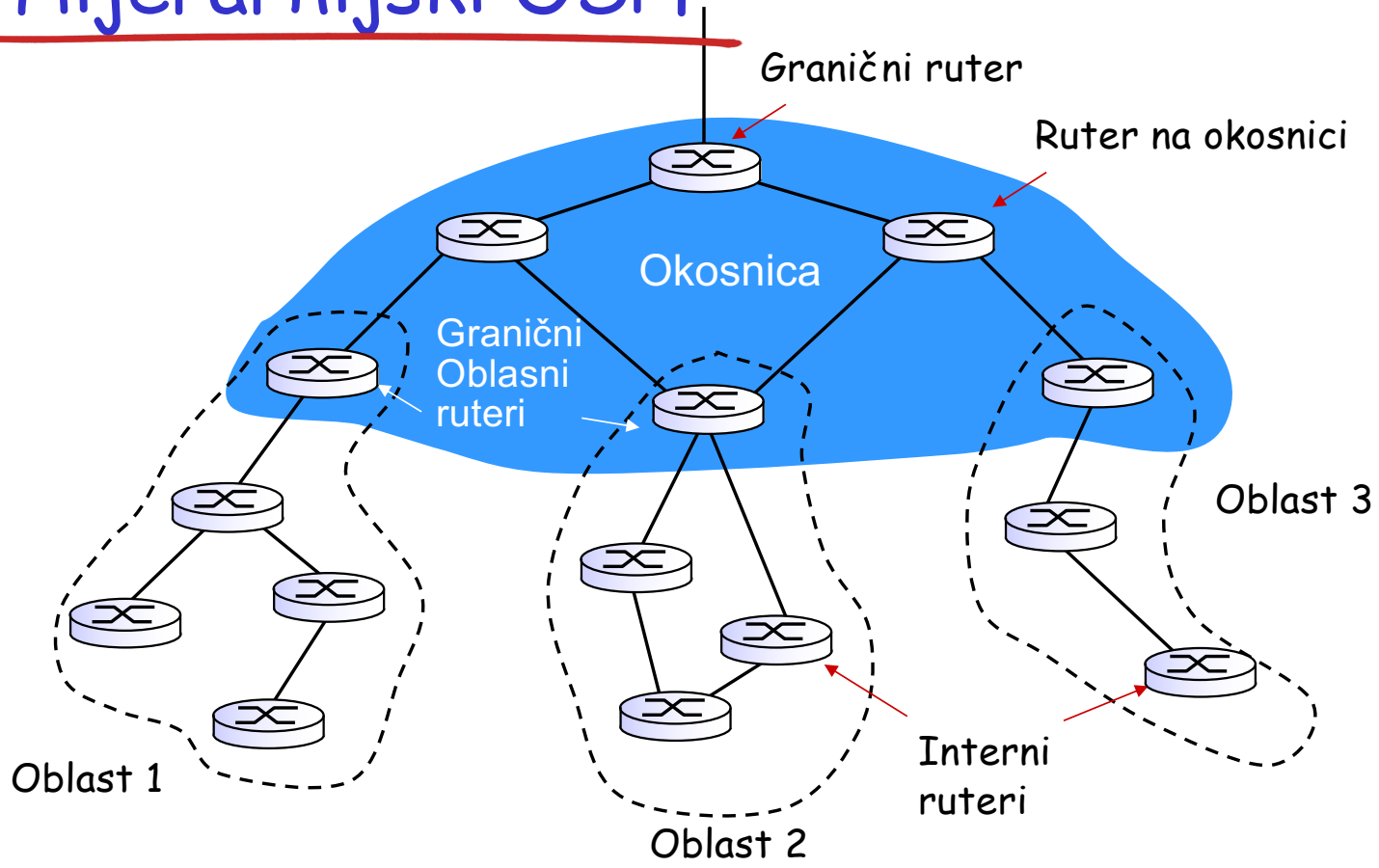
OSPF (Open Shortest Path First)

- 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 multicast tabela.

OSPF "advanced" karakteristike (ne u RIP)

- Sigurnost: za sve OSPF poruke se mora znati izvor (prevencija malicioznih aktivnosti) pri čemi se koriste lozinke ili MD5 kodiranje
- Više puteva sa istim troškovima je dozvoljeno (RIP dozvoljava samo jedan put)
- Za svaki link, više metrika troškova za različiti TOS (npr., troškovi satelitskog linka su podešeni na "nisko" za best effort; visoko za servis u realnom vremenu)
- Integrisana uni- i multicast podrška:
  - Multicast OSPF (MOSPF) koristi istu bazu podataka o topologiji kao OSPF
- Hijerarhijski OSPF u velikim domenima.

Hijerarhijski OSPF



Hijerarhijski OSPF

- Hijerarhija u dva nivoa: lokalna mreža i okosnica.
  - Oglašavanja o stanju linka samo u lokalnoj mreži
  - Svako čvorište ima detaljnu topologiju mreže; samo poznaje najkraći put do mreža u drugim mrežama.
- **Ruter na granici lokalne mreže:** "sumira" rastojanja do mreža u sopstvenoj zoni odgovornosti i to oglašava drugim ruterima na granicama lokalnih mreža.
- **Ruteri okosnice:** izvršavaju OSPF rutiranje samo na okosnici.
- **Granični ruteri:** povezivanje na druge AS.

IS-IS (Intermediate system to intermediate system)

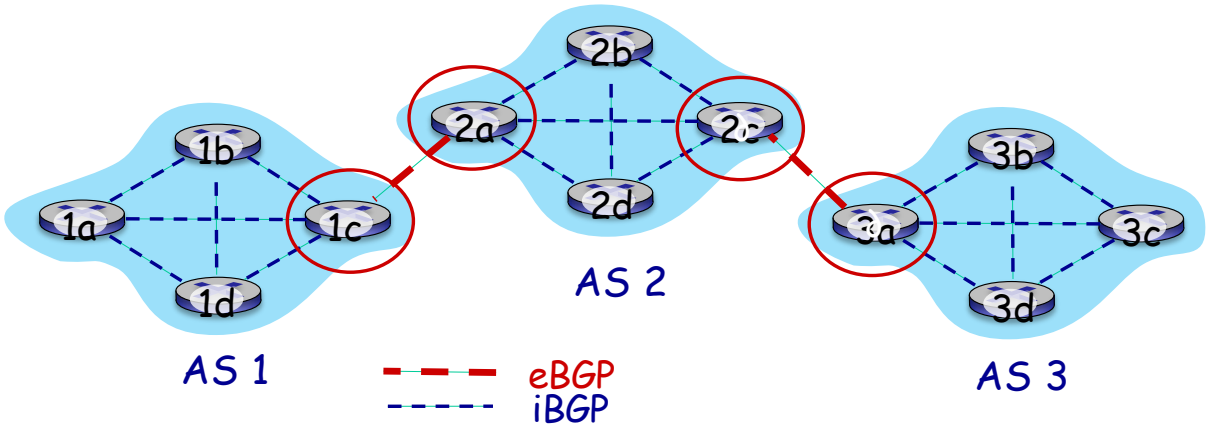
- Interior Gateway Protocol (IGP)
- Koristi "Link State" algoritam
  - LS širenje paketa
  - Mapa topologije na svakom čvorištu
  - Proračun rute korišćenjem Dijkstra algoritma
- OSI referentni model (protokol mrežnog nivoa)
- Poslednjih nekoliko godina je potisnuo OSPF iz operatorskih mreža
- Multicast prenos LSA
- CIDR adresiranje
- Ne koristi usluge IP tako da je samim tim indiferentan u odnosu na verzije IP protokola
- Zbog jednostavnosti generiše manji saobraćaj od OSPF tako da je pogodan za velike mreže
- Integrated IS-IS je predložen u TCP/IP arhitekturi
- IS-IS ruter pripada samo jednoj oblasti (Level 1, Level 2 i Level1-2)
- Nema okosnice

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"*

BGP osnove

- 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 AS3 oglasi prefiks do AS2, AS3 *obećava* da će proslijediti bilo koji datagram koji je adresiran do tog prefiksa preko sebe.
  - AS3 može agregirati prefikse u oglašavanjima



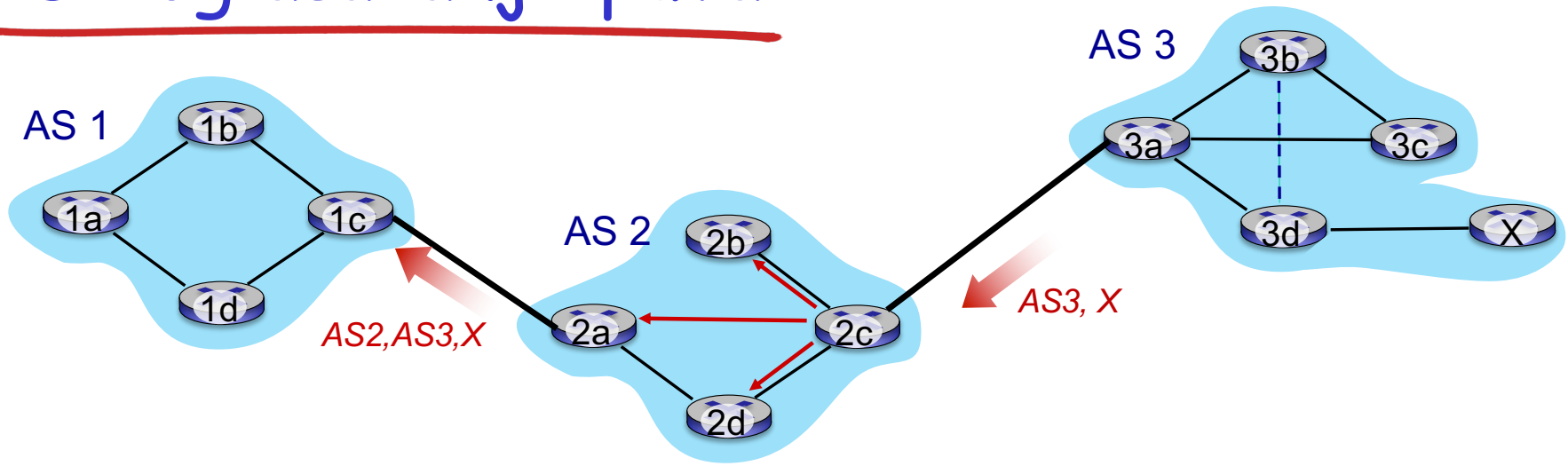
Atributi puta & BGP rute

- Kada oglašava prefiks, oglašavanje uključuje BGP atribute.
  - prefix + atributi = "ruta"
- Dva važna atributa:
  - AS-PATH: sadrži AS-ove preko kojih je oglašavanje prefiksa prošlo: AS 67 AS 17
  - NEXT-HOP: Indicira specifični interni-AS ruter do next-hop AS. (Može biti više linkova od trenutne AS do next-hop-AS.)
- Kada gateway ruter primi oglašavanje rute, koristi politiku importovanja za potvrdu/odbijanje rute. Ova politika takođe određuje hoće li neka ruta da se oglasi susjednim AS.

BGP izbor rute

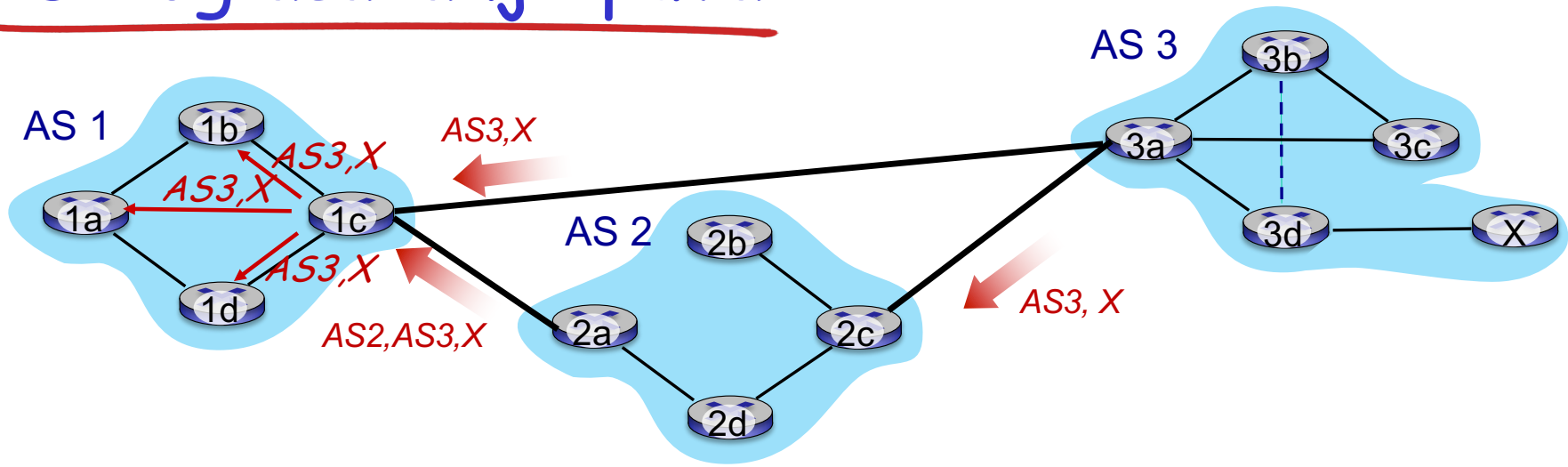
- Ruter može naučiti više od jedne rute do istog prefiksa. Ruter mora odabrati rutu.
- Pravila eliminacije:
  1. Vrijednost atributa lokalne reference: odluka politike
  2. Najkraći AS-PATH
  3. Najbliži NEXT-HOP ruter: "vrući krompir" rutiranje
  4. Dodatni kriterijum

BGP oglašavanje puta



- AS2 ruter 2c dobija oglašavanje puta AS3,X (preko eBGP) od AS3 rutera 3a
- Na bazi AS2 politike, AS2 ruter 2c prihvata put AS3,X, šaljući ga (preko iBGP) svim AS2 ruterima
- Na bazi AS2 politike, AS2 ruter 2a oglašava (prekoa eBGP) put AS2, AS3, X do AS1 rutera 1c

BGP oglašavanje puta



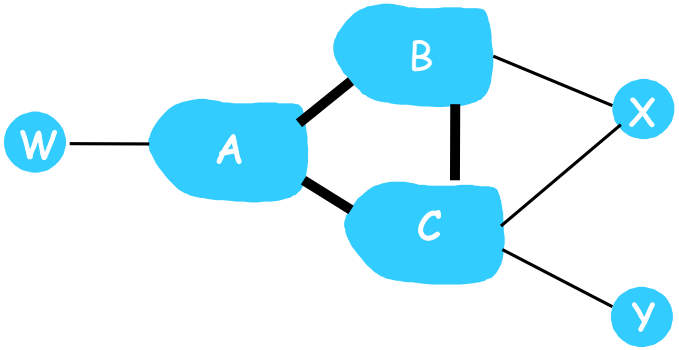
gateway router može naučiti više puteva do destinacije:

- AS1 gateway ruter 1c uči put *AS2,AS3,X* od 2a
- AS1 gateway ruter 1c uči put *AS3,X* od 3a
- Na bazi *politike,* AS1 gateway ruter 1c bira put *AS3,X* i oglašava ga unutra AS1 preko iBGP

BGP poruke

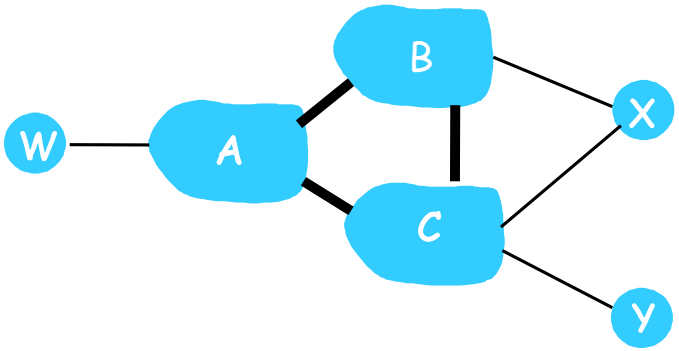
- BGP poruke se razmjenjuju preko TCP.
- BGP poruke:
  - OPEN: otvara TCP vezu sa peer i vrši identifikaciju pošiljaoca
  - UPDATE: oglašava novi put (ili odbacuje stari)
  - KEEPALIVE održava vezu u odsustvu UPDATE-ova; takođe potvrđuje OPEN zahtjev
  - NOTIFICATION: izvještava o greškama u prethodnoj poruci; takođe se koristi za raskidanje veze

BGP politika rutiranja



- A,B,C su mreže provajdera
- x,w,y su korisnici (mreža provajdera)
- x je "dual-homed": povezan na dvije mreže
  - x ne želi da se saobraćaj rutira od B preko x do C
  - .. tako x neće oglašavati B rutu do C

BGP: kontroliše ko rutira do tebe



- A oglašava B put Aw
- B oglašava X put BAw
- Da li će B oglašavati C put BAw?
  - Nema šanse! B ne dobija "profit" za rutiranje CBAw pošto w i C nisu B-ovi korisnici
  - B želi da prinudi C da rutira do w preko A
  - B želi da rutira *samo* do/od njegovih korisnika!

Zašto različito Intra- i Inter-AS rutiranje ?

Politika:

- Inter-AS: administrator želi kontrolu nad načinom rutiranja saobraćaja i time ko rutira kroz njegovu mrežu.
- Intra-AS: jedan administrator, nema potrebe za političkim odlukama

Veličina:

- hijerarhijsko rutiranje čuva veličinu tabele, smanjuje saobraćaj koji se odnosi na ažuriranje

Performanse:

- Intra-AS: može se fokusirati na performanse
- Inter-AS: politika može dominirati u odnosu na performanse

Glava 4: Mrežni nivo

- Principi nivoa mreže
- IPv4 (Internet Protocol)
  - DHCP
  - NAT
  - ICMP
- IPv6
- Protokoli rutiranja
- Mrežni menadžment

Mrežni menadžment

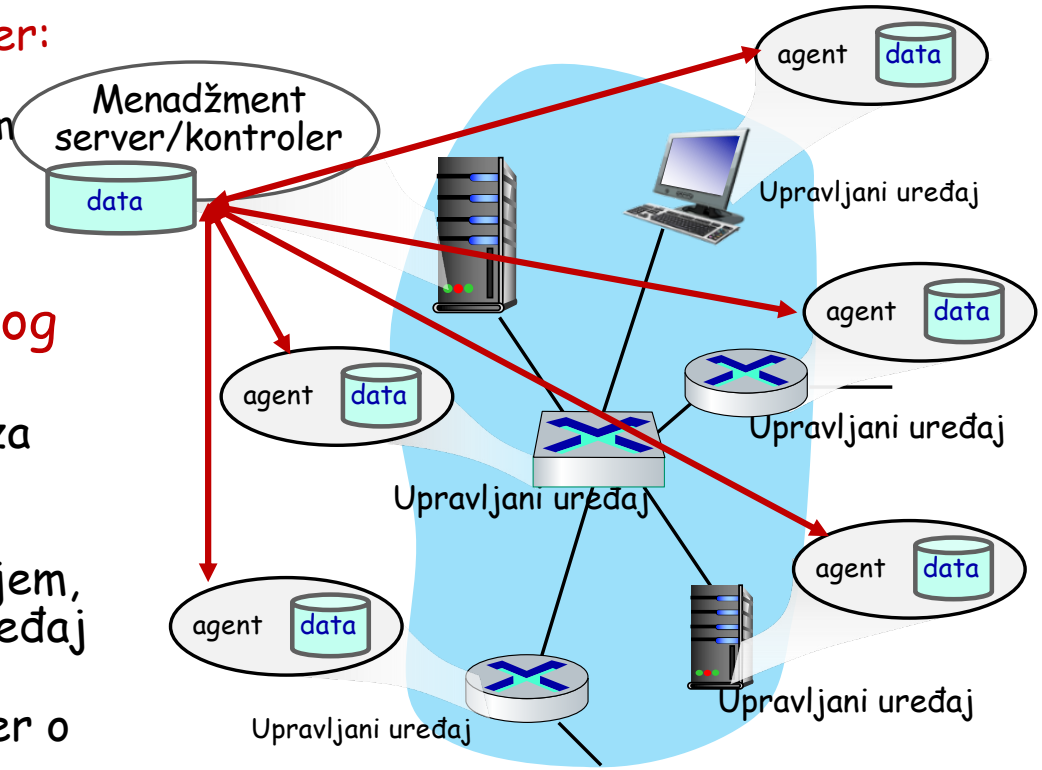
- autonomni sistemi (mreže): hiljade sofverskih i hardverskih komponeni koje međusobno interaguju
- ovako kompleksni sistemi zahtijevaju monitoring, konfiguraciju, kontrolu

Mrežni menadžement uključuje implementaciju, integraciju i koordinaciju hardvera, softvera, i čovjeka radi praćenja testiranja, konfigurisanja, analize, evaluacije i kontrole mreže i resursa mrežnih elemenata u realnom vremenu kako bi se postigle željene performanse i *Quality of Service* zahtjevi po razumnoj cijeni.

Komponente mrežnog menadžmenta

Menadžment server: aplikacija, tipično povezana za mrežnim menadžerom

Protokol mrežnog menadžmenta: koristi ga server za pozivanje, konfigurisanje i upravljanje uređajem, kao i upravljani uređaj da informiše menadžment server o podacima, događajima,...



Upravljani uređaj: oprema sa upravljivim i konfigurabilnim HW i SW komponentama

Podaci: podaci o konfiguraciji, operativni podaci, statistike

Pristup operatora mrežnom menadžmentu

CLI (*Command Line Interface*)

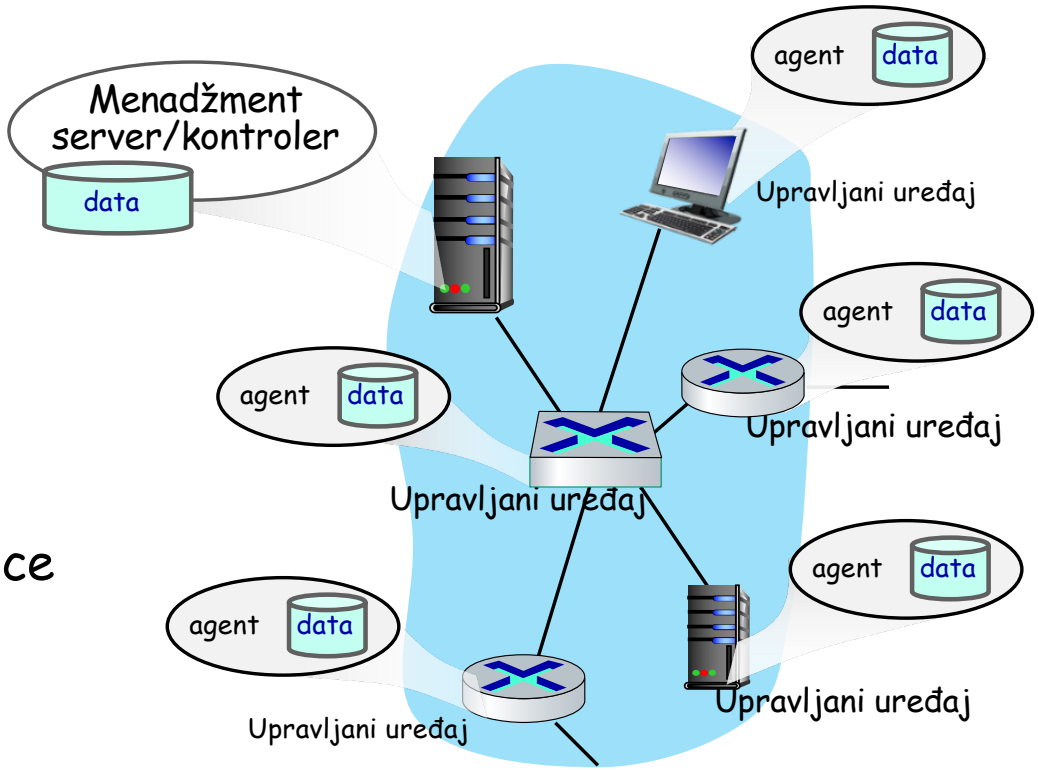
- Operator unosi komande direktno na pojedinačne uređaje (npr., ssh)

SNMP/MIB

- operator poziva/setuje podatke uređaja Management Information Base (MIB) korišćenjem Simple Network Management Protocol (SNMP)

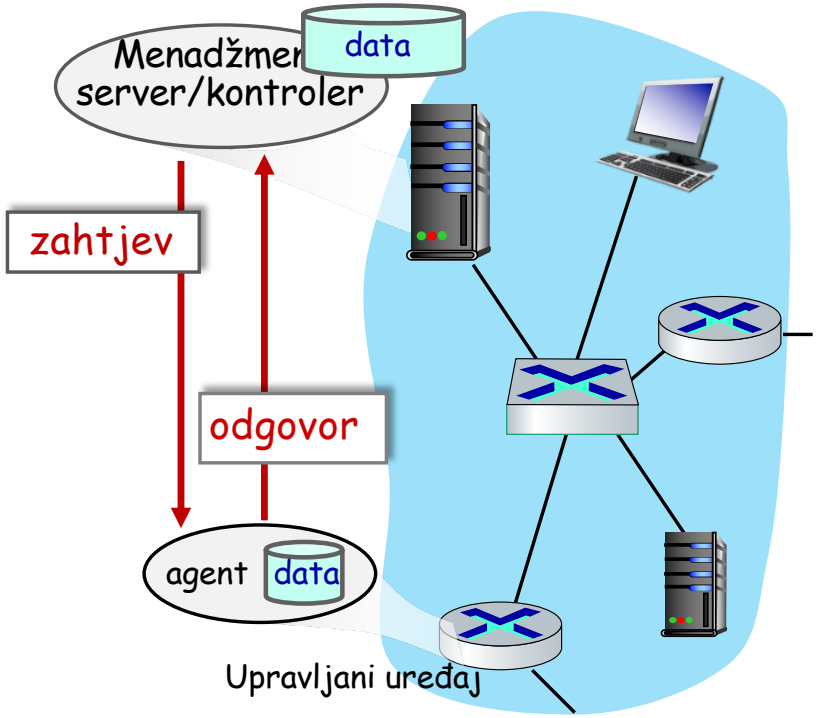
NETCONF/YANG

- abstraktan, holistički
- namijenjen menadžmentu multi-device konfiguracija.
- YANG: data modeling jezik
- NETCONF: komunicira YANG-kompatibilnim akcijama/podacima ka/od/između udaljenih uređaja

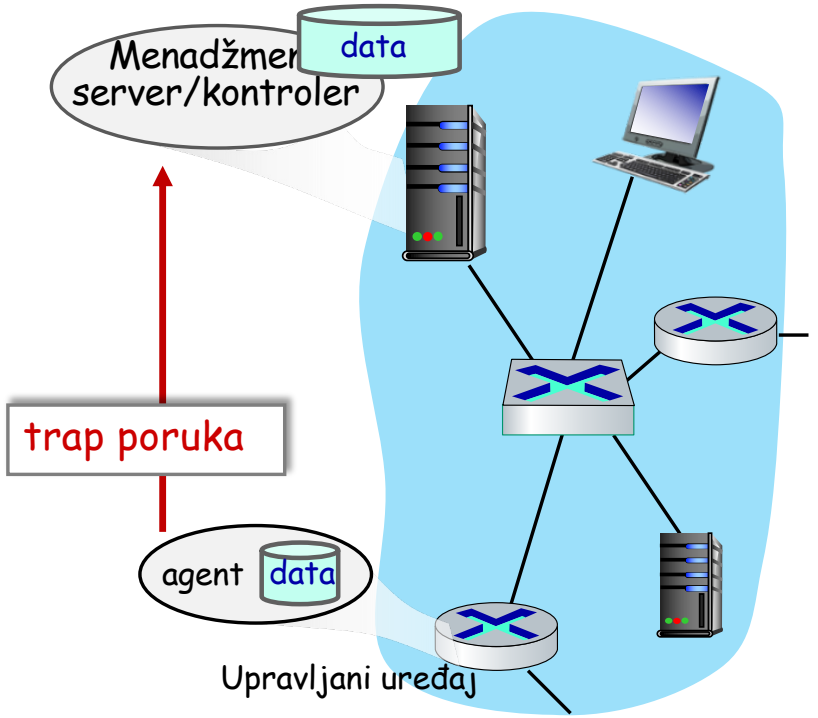


SNMP protokol

Dva načina za prenos MIB info, komandi:



request/response mod



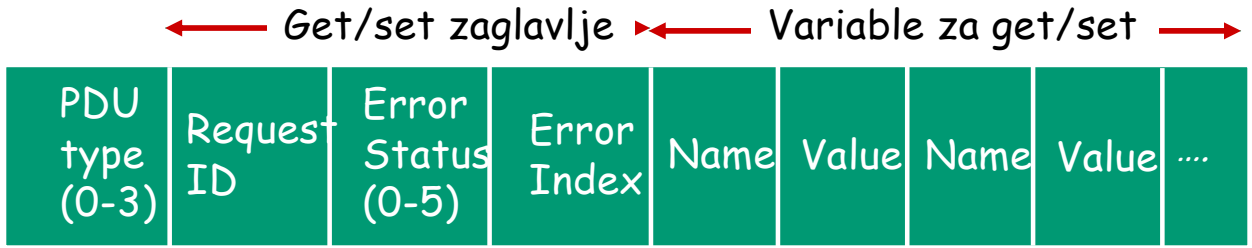
trap mod

SNMP protokol: tipovi poruka

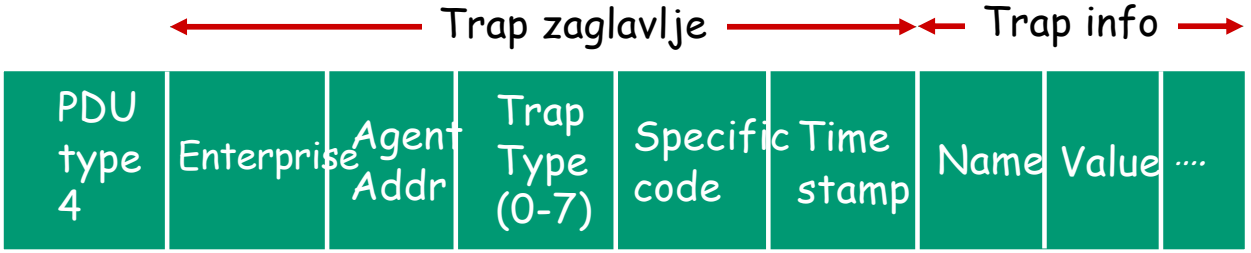
Tip poruke	Funkcija
GetRequest GetNextRequest GetBulkRequest	manager-to-agent: "pošalji mi podatke" (data instance, next data in list, block of data).
SetRequest	manager-to-agent: postavi MIB vrijednost
Response	Agent-to-manager: vrijednost, odgovor na zahtjev
Trap	Agent-to-manager: informiše menadžera o vanrednom događaju

SNMP protokol: formati poruka

Tipovi poruka 0-3

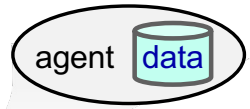


Poruka tip 4



SNMP: Management Information Base (MIB)

- Podaci upravljanog uređaja (operativni i nešto konfiguracionih)
- Prikupljeni u uređajevom MIB modulu
  - 400 MIB modula je definisano u RFC-ovima pri čemu je mnogo više proizvođačkih MIB-ova
- Structure of Management Information (SMI): data definition jezik
- primjer MIB varijabli za UDP protokol:

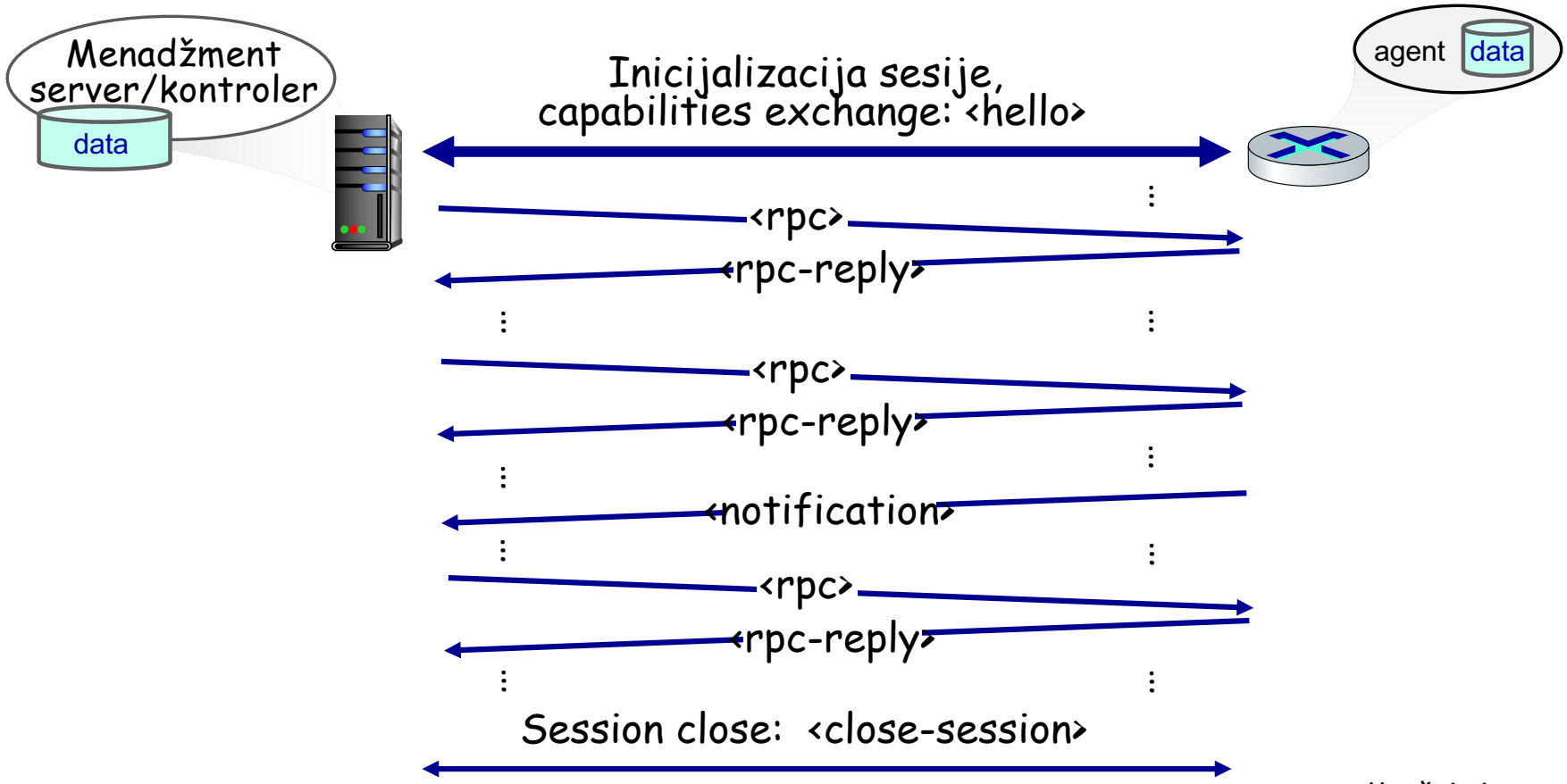


Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	32-bit counter	total # datagrams delivered
1.3.6.1.2.1.7.2	UDPNoPorts	32-bit counter	# undeliverable datagrams (no application at port)
1.3.6.1.2.1.7.3	UDInErrors	32-bit counter	# undeliverable datagrams (all other reasons)
1.3.6.1.2.1.7.4	UDPOutDatagrams	32-bit counter	total # datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port currently in use

NETCONF

- cilj: aktivno upravljanje/konfiguracija uređaja u mreži
- funkcioniše između menadžment servera i upravljanog uređaja
  - akcije: povuci, setuj, modifikuj, aktiviraj konfiguracije
  - atomic-commit akcije preko više urađaja
  - Ispitivanje operativnih podataka i statistika
  - Notifikacije od uređaja
- *Remote Procedure Call* (RPC) paradigma
  - Poruke NETCONF protokola su pisane u XML
  - Razmjenjuju se preko sigurnog i pouzdanog transportnog (npr TLS) protokola

NETCONF inicijalizacija, razmjena, zatvaranje



Neke NETCONF operacije

NETCONF	Opis operacije
<get-config>	Povlačenje svih djelova date konfiguracije. Uređaj može imati više konfiguracija.
<get>	Povlačenje svih ili dijela podataka o stanju konfiguracije i operativnom stanju.
<edit-config>	Promijeni specificiranu (vjerovatno aktivnu) konfiguraciju upravljanog uređaja. <rpc-reply> upravljanog uređaja sadrži <ok> ili <rpcerror>.
<lock>, <unlock>	Zaključaj (otključaj) bazu konfiguracije na upravljanom uređaju (zaključati INETCONF, SNMP ili CLI komande sa drugih izvora).
<create-subscription>, <notification>	Omogućiti notifikaciju događaja sa upravljanih uređaja

Primjer NETCONF RPC poruke

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <rpc message-id="101"                    note message id
03   xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
04   <edit-config>          Promijeni konfiguraciju
05     <target>
06       <running/>         Promijeni aktivnu konfiguraciju
07     </target>
08     <config>
09       <top xmlns="http://example.com/schema/
         1.2/config">
10         <interface>
11           <name>Ethernet0/0</name>     promijeni MTU Ethernet
12           <mtu>1500</mtu>               0/0 interfejsa na 1500
13         </interface>
14       </top>
15     </config>
16   </edit-config>
17 </rpc>
```

YANG

- Jezik modelovanja podataka koji se koristi da specificira strukturu, sintaksu, semantiku NETCONF podataka mrežnog menadžmenta
  - built-in data tipove, kao SMI
- XML dokument koji opisuje uređaj, mogućnosti mogu biti generisane iz YANG opisa
- Može izraziti ograničenja u podacima koja moraju biti zadovoljena u validnoj NETCONF konfiguraciji
  - Obezbjeđuje da NETCONF konfiguracije zadovoljavaju ograničenja u pogledu korektnosti i konzistentnosti