



Preddiplomski studij

Računarstvo

Komunikacijske mreže

13.

Povezivanje mreža u Internetu

Evolucija mreže i izazovi Interneta: odabrane teme
iz tehnologija Interneta

Ak.g. 2014./2015.



slobodno smijete:

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
 - **remiksirati** — prerađivati djelo
- pod sljedećim uvjetima:**

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencijske uvjete ovog djela. Najbolji način da to učinite je poveznicom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

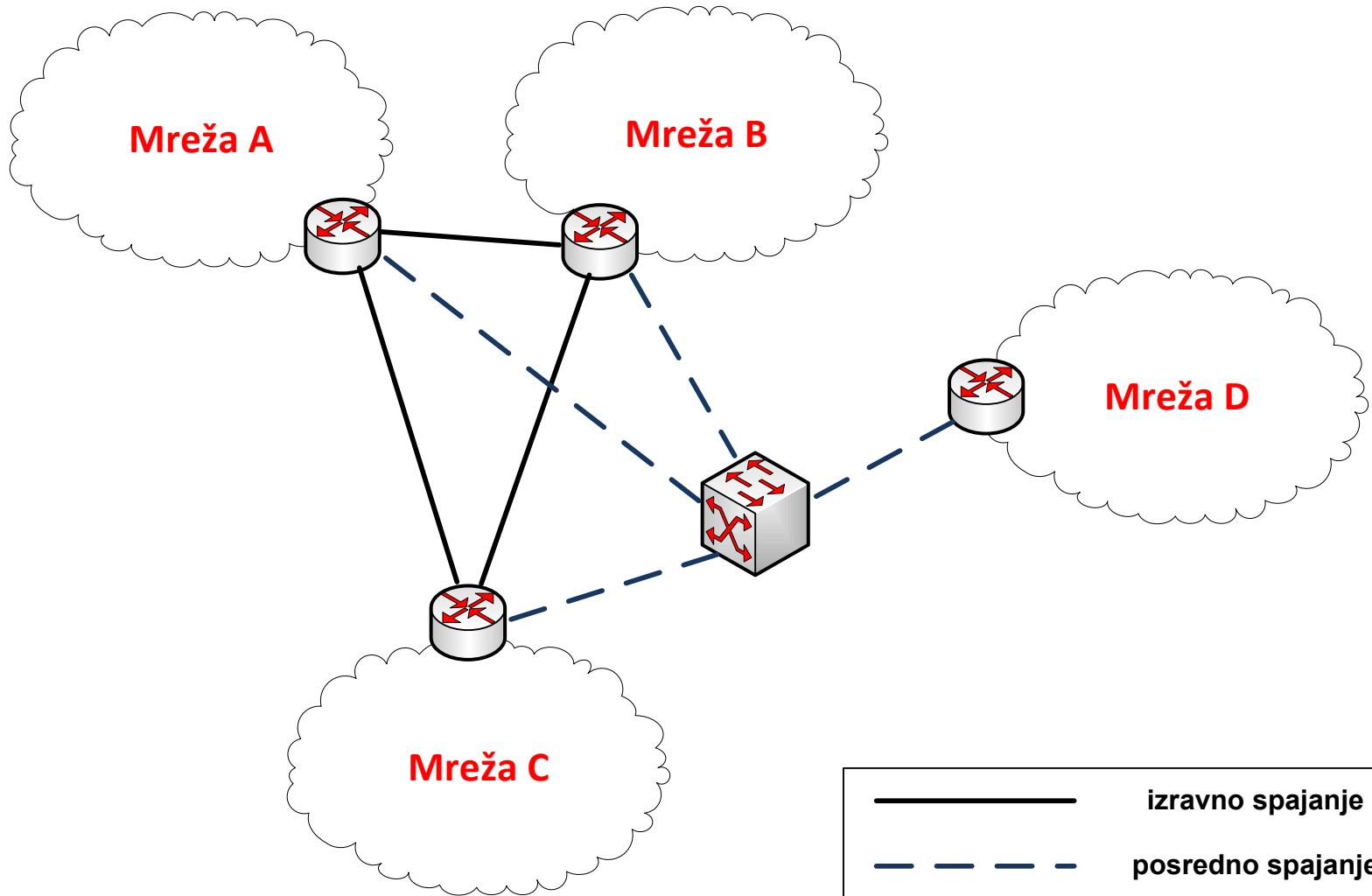
Tekst licencije preuzet je s <http://creativecommons.org/>.

Sadržaj predavanja

- ◆ Povezivanje mreža u Internetu
 - Primjer: akademska i istraživačka mreža CARNet
- ◆ Odabrane teme iz tehnologija Interneta
 - Sigurnosni izazovi protokola sloja podatkovne poveznice; sigurnosna stijena (engl. *firewall*)
 - Protokol IPv6

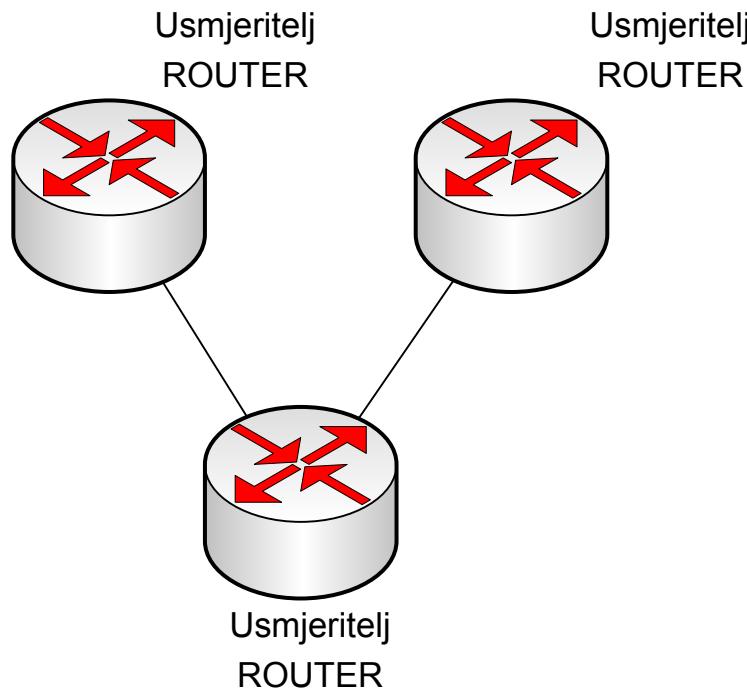
Povezivanje mreža u Internetu

Kako međusobno povezati mreže?



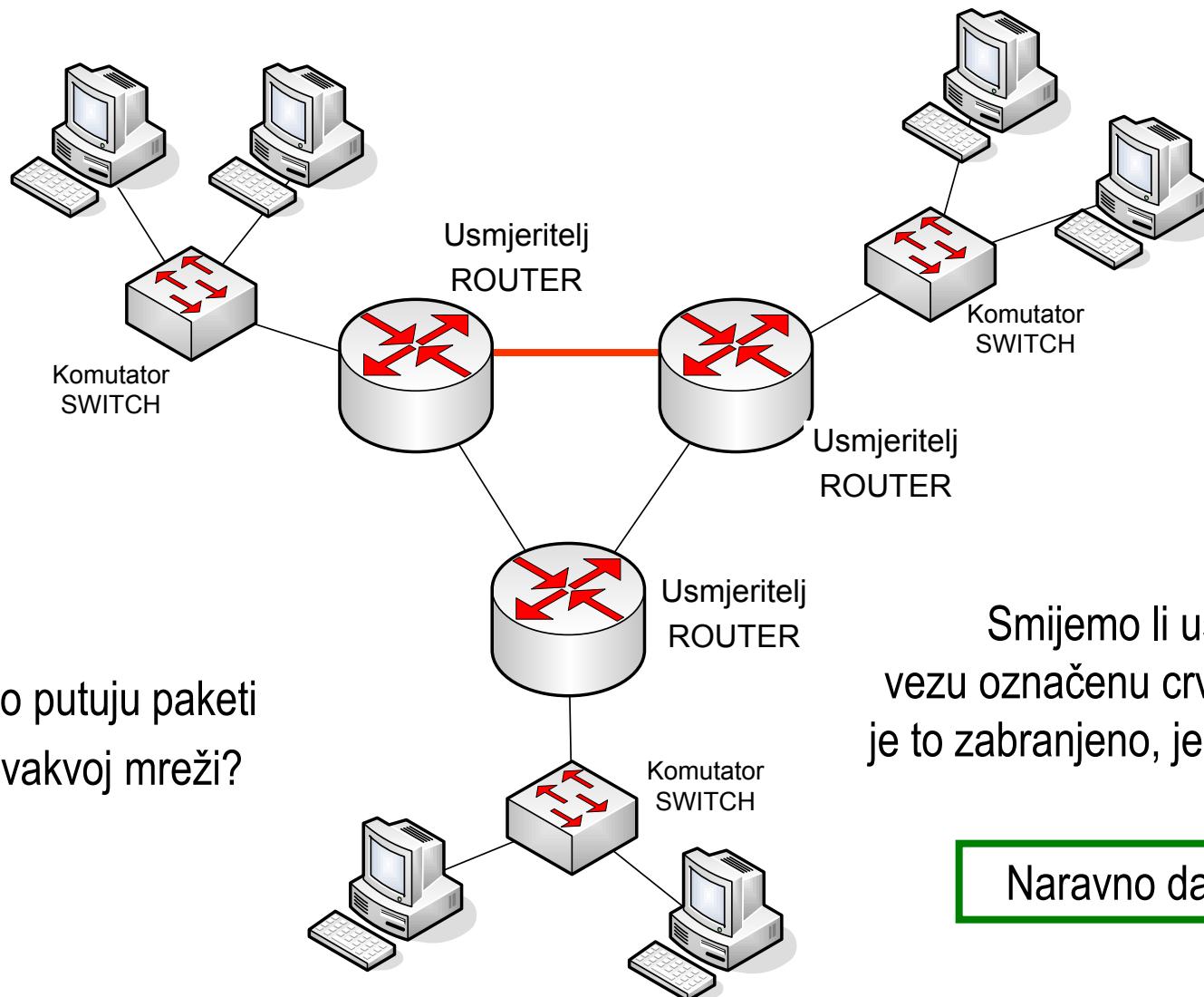
Povezivanje mrežnih uređaja (1)

Je li ovo realna topologija?



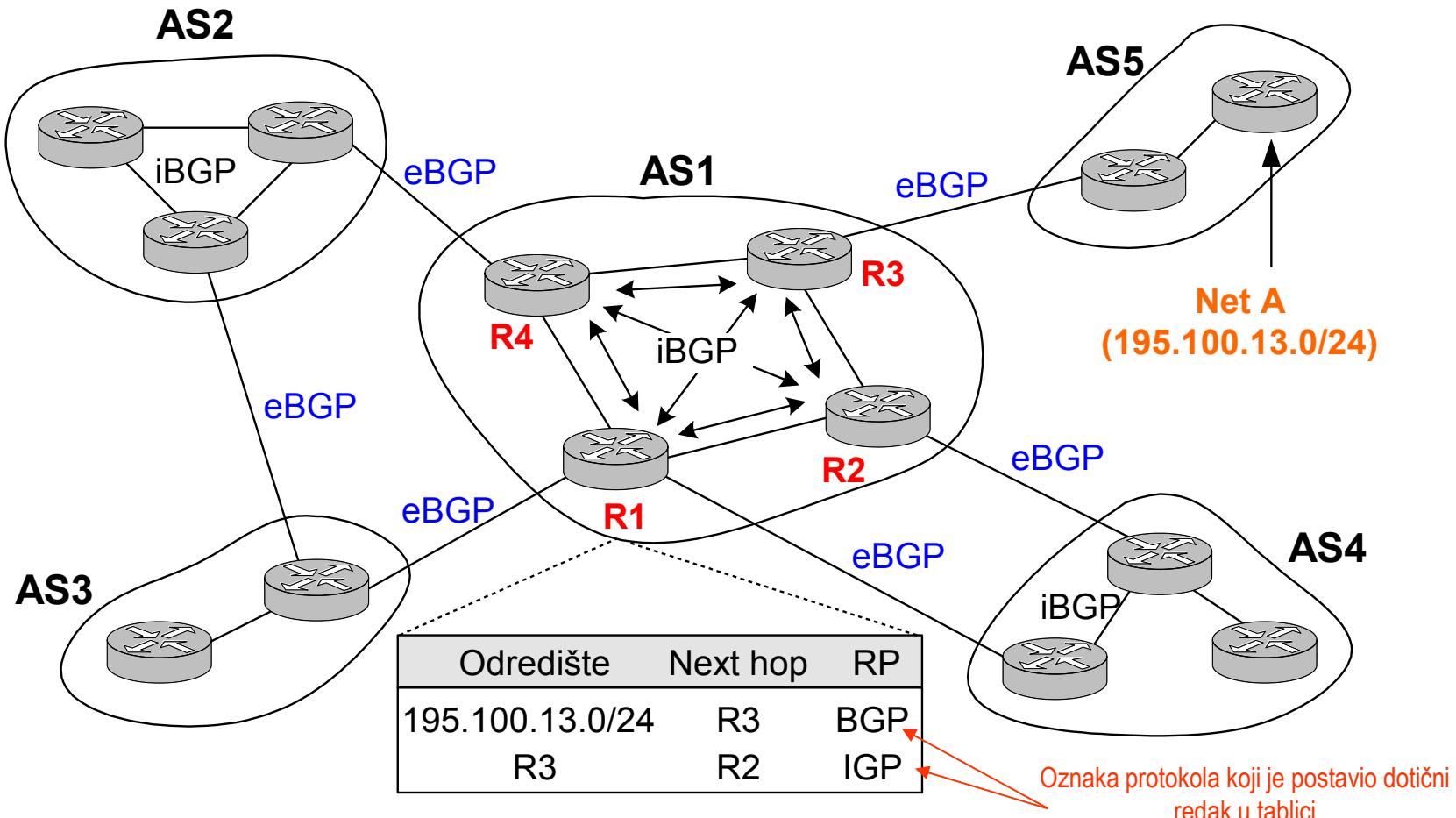
Da! Često se usmjeritelji povezuju izravno kod međusobnog povezivanja dviju ili više mreža.

Povezivanje mrežnih uređaja (2)

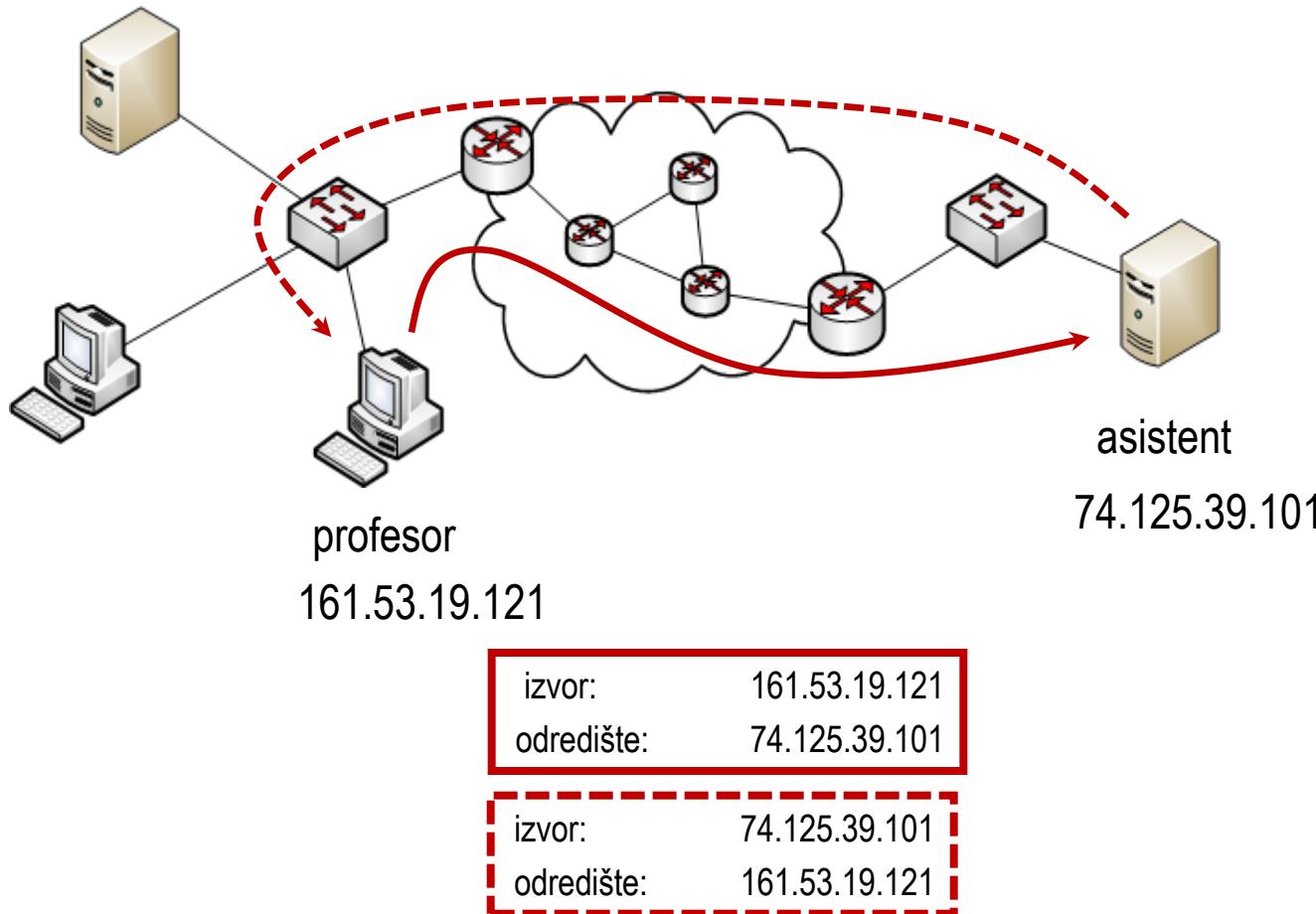


Usmjeravanje između AS-ova – protokol BGP

Svi autonomni sustavi (AS) koriste Border Gateway Protocol (BGP) verzije 4



Usmjeravanje datagrama (javne, statičke adrese)



NAT – Network Address Translation (1)

- ◆ Prevođenje mrežnih adresa (engl. *Network Address Translation*)
- ◆ Izvorno uvedeno radi nedostatka IP-adresa u IPv4
 - Odvojiti adresiranje unutar privatne mreže (npr. intranet) od onog u Internetu
- ◆ Najčešće se privatna adresa pretvara u javnu i obratno
- ◆ Više računala iz privatne (lokalne) mreže komunicira u Internetu preko jedne ili nekoliko (javnih) IP-adresa
- ◆ Vrste prevodenja:
 - NAT pretvara IP-adrese, a PAT (*Port Address Translation*) pretvara vrata (*port*)
 - Kombinacija NAT + PAT → NAT s pretvaranjem vrata:
 - Izvorišni NAT - pretvara izvorišnu adresu (koja je inicirala komunikaciju)
 - Odredišni NAT - pretvara odredišnu adresu (koja prihvaca komunikaciju)
 - U praksi se koriste obje istovremeno, uz praćenje konekcija (engl. *connection tracking*)

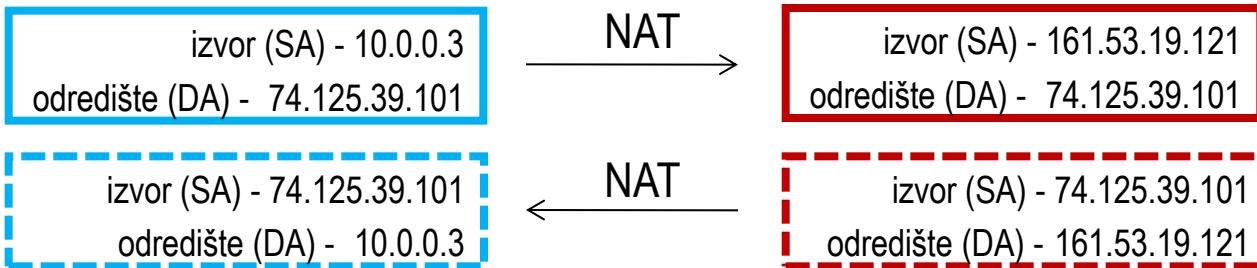
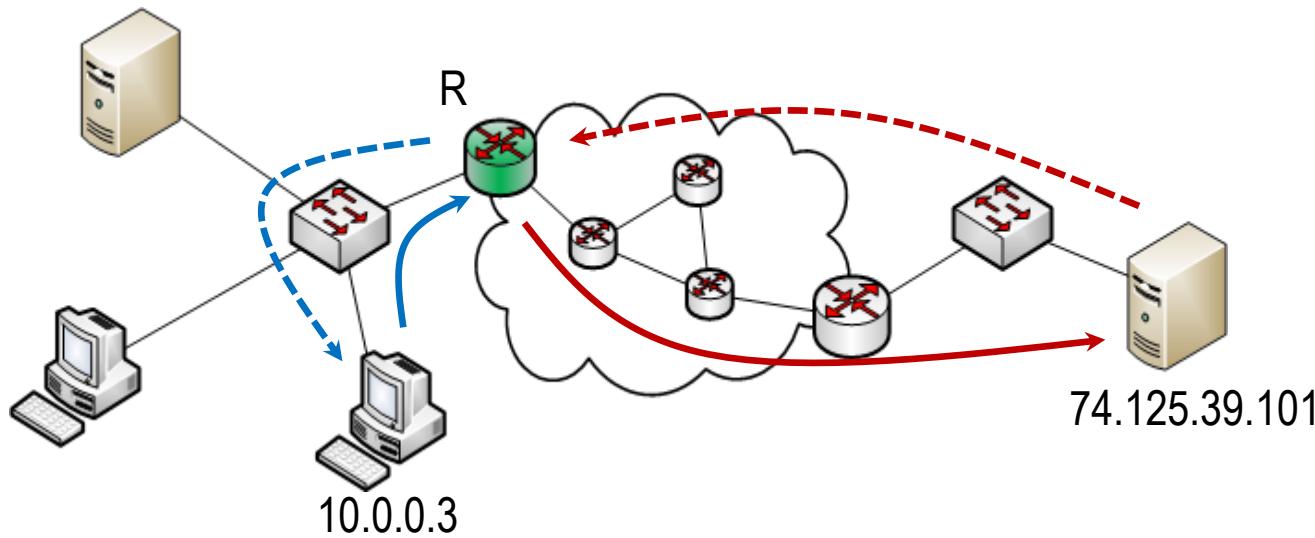
NAT – Network Address Translation (2)

- ◆ Prednosti:
 - Štednja adresnog prostora
 - Prilikom promjene ISP-a nije potrebno mijenjati adresni prostor privatne (lokalne) podmreže
 - Povećana razina sigurnosti - primjena:
 - Odvajanje privatne mreže od Interneta, kada *nije* na raspolaganju primjerena sigurnosna stijena (vatrozid)
 - Privatne (unutarnje) IP-adrese *nisu objavljene* u Internetu: zaštita poslužitelja od napada uskraćivanja usluga
- ◆ Nedostaci:
 - Povećano kašnjenje
 - Nemogućnost praćenja puta paketa s kraja na kraj
 - Ako aplikacijski protokol koristi IP-adrese, onda NAT mora znati kako promijeniti adresne podatke u aplikacijskom protokolu (npr., HTTP)

Usmjeravanje datagrama (privatne, statičke adrese)

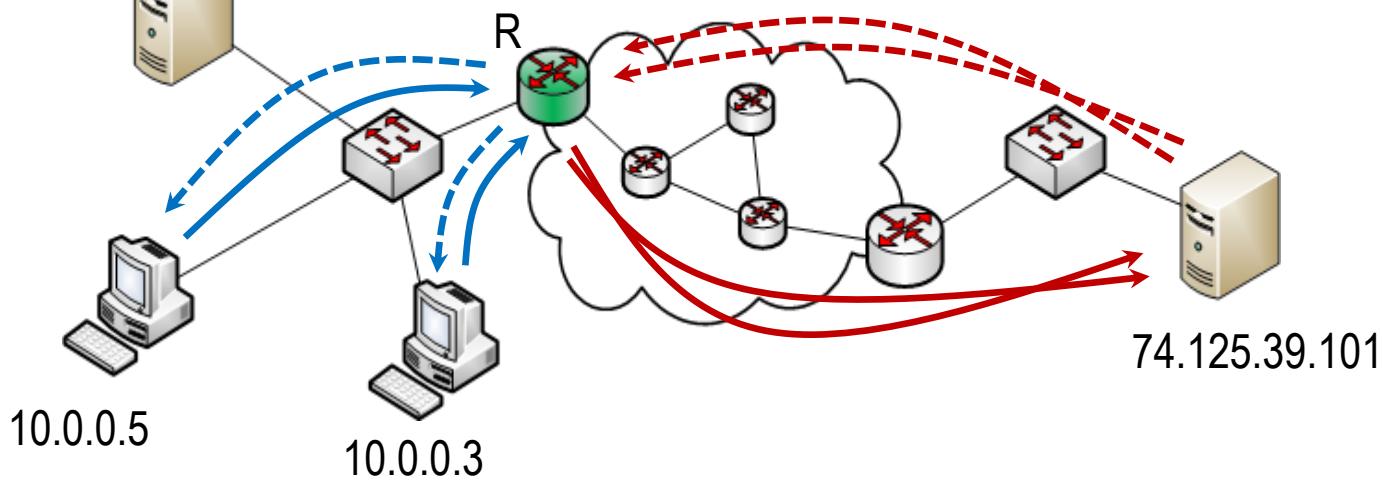
NAT-tablica

Privatna adresa	Javna adresa	Odredišna adresa
10.0.0.3	161.53.19.121	74.125.39.101



PAT – primjer (1)

NAT-tablica		
Privatna adresa:vrata	Javna adresa:vrata	Odredišna adresa:vrata
10.0.0.3:1222	161.53.19.121:1222	74.125.39.101:80
10.0.0.5:1333	161.53.19.121:1333	74.125.39.101:80



10.0.0.5

10.0.0.3

SA:vrata - 10.0.0.3:1222
DA:vrata - 74.125.39.101:80

NAT

SA:vrata - 161.53.19.121:1222
DA:vrata - 74.125.39.101:80

SA:vrata - 10.0.0.5:1333
DA:vrata - 74.125.39.101:80

NAT

SA:vrata - 161.53.19.121:1333
DA:vrata - 74.125.39.101:80

SA:vrata - 74.125.39.101:80
DA:vrata - 161.53.19.121:1222

NAT

SA:vrata - 74.125.39.101:80
DA:vrata - 10.0.0.3:1222:1222

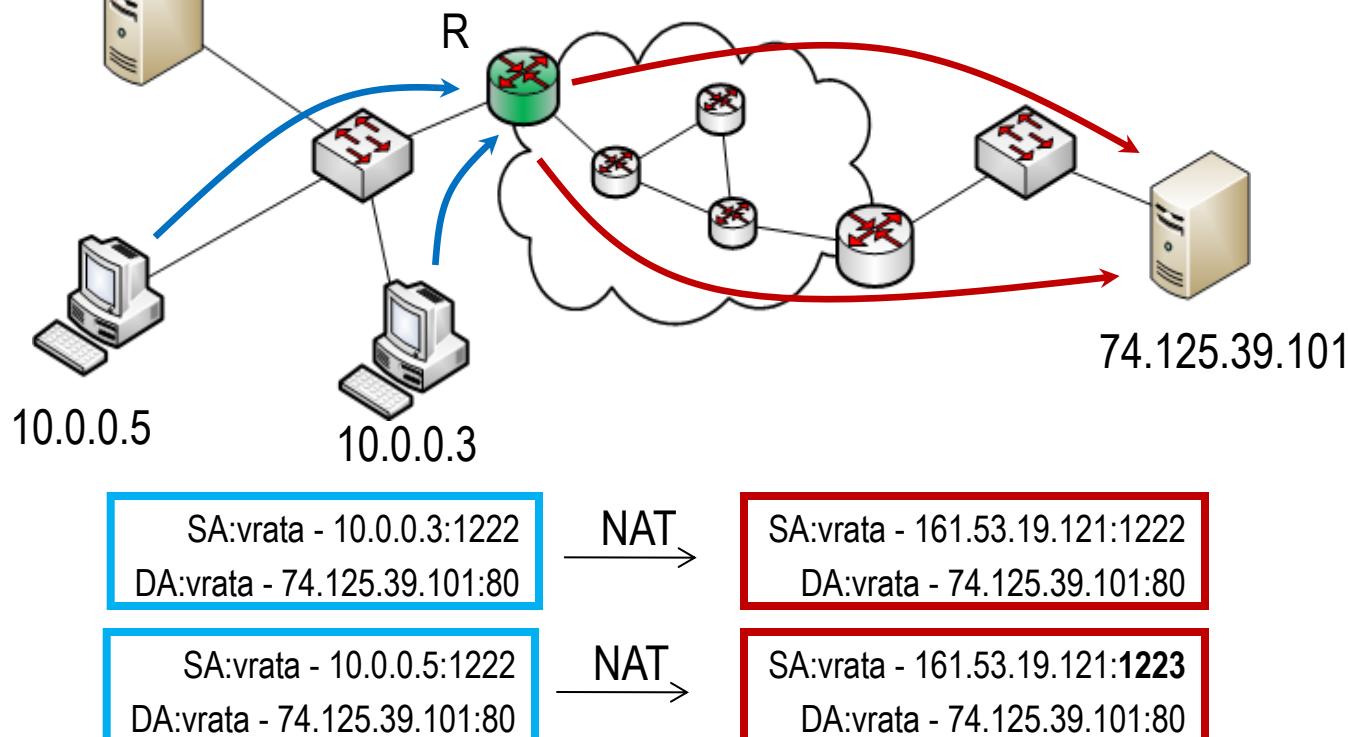
SA:vrata - 74.125.39.101:80
DA:vrata - 161.53.19.121:1333

NAT

SA:vrata - 74.125.39.101:80
DA:vrata - 10.0.0.5:1333

PAT – primjer (2)

NAT-tablica		
Privatna adresa:vrata	Javna adresa:vrata	Odredišna adresa:vrata
10.0.0.3:1222	161.53.19.121:1222	74.125.39.101:80
10.0.0.5:1222	161.53.19.121:1223	74.125.39.101:80

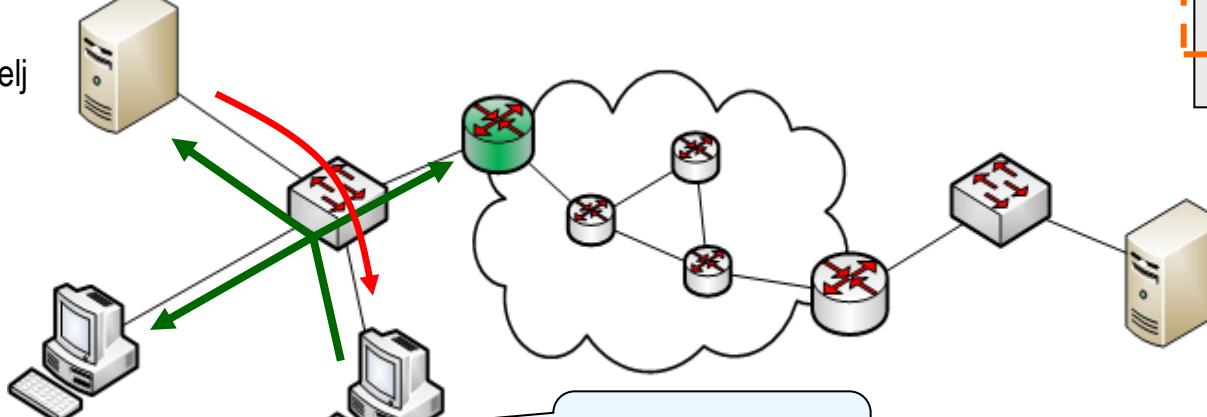


Usmjeravanje datagrama (privatne, dinamičke adrese)

2. DHCP
offer

4. DHCP
acknowledge

DHCP poslužitelj



Raspoloživo:

10.0.0.2
10.0.0.3
10.0.0.4

5. prebaci

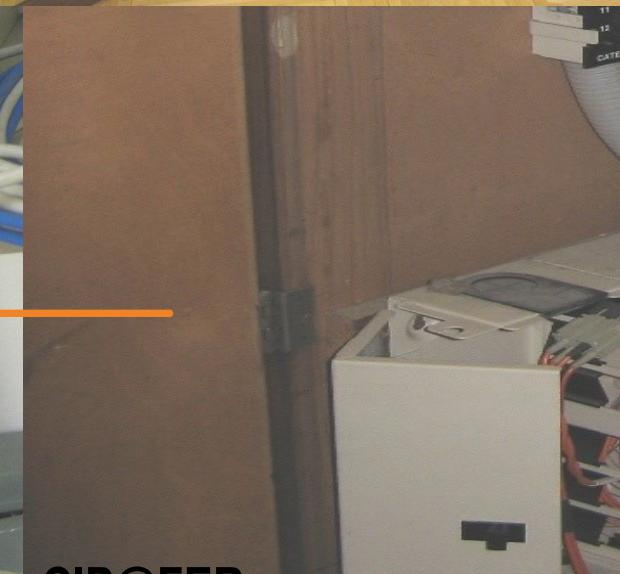
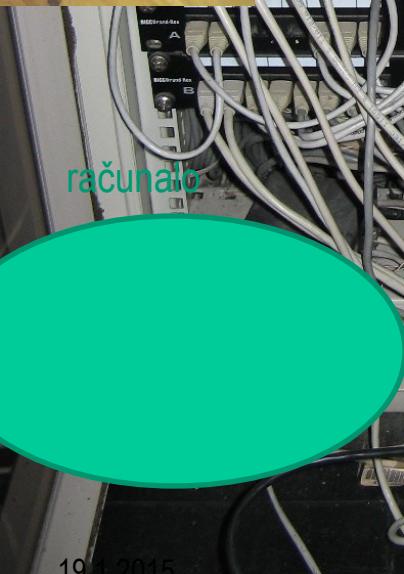
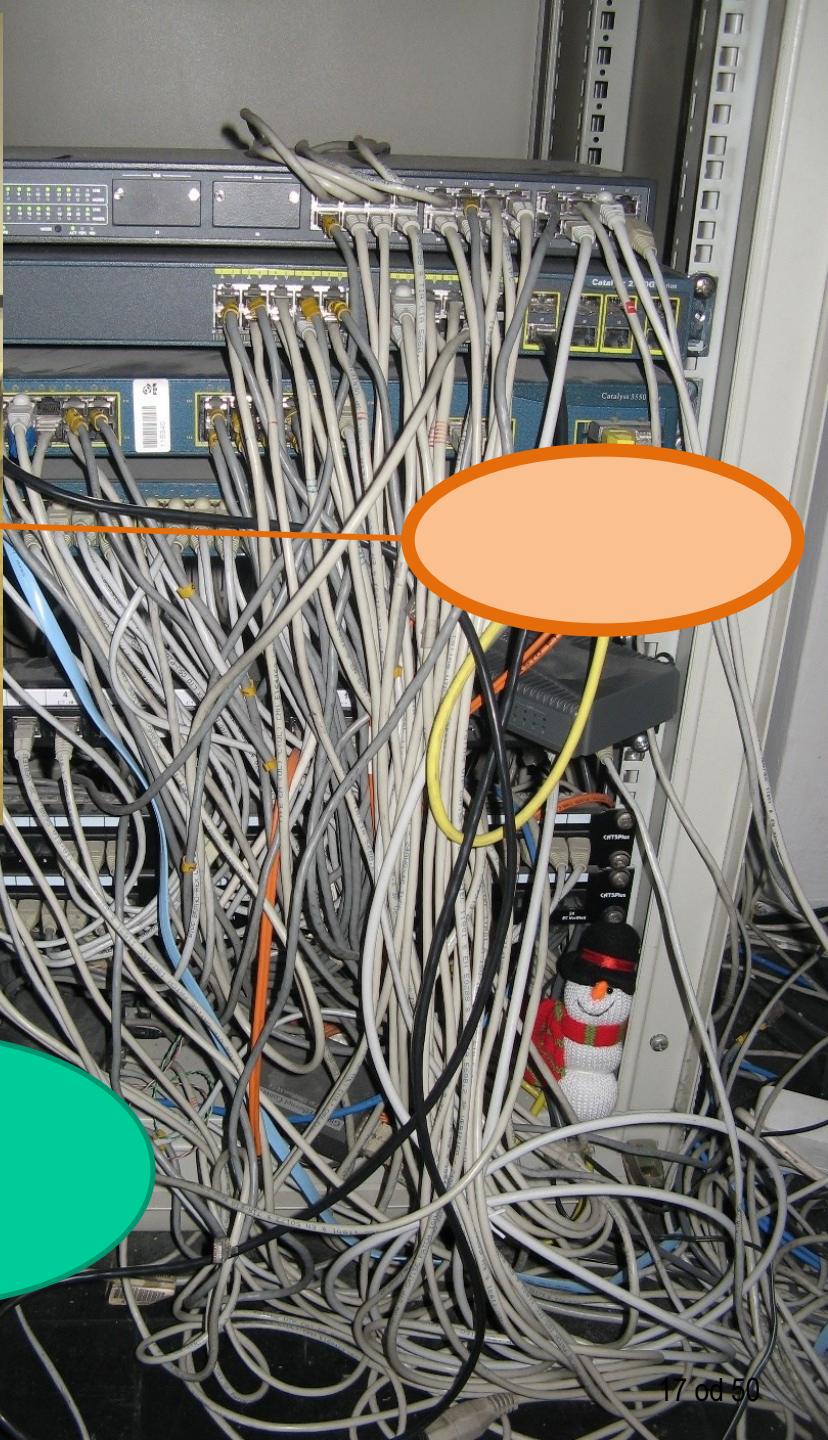
Izdano

10.0.0.1
10.0.0.5
10.0.0.3

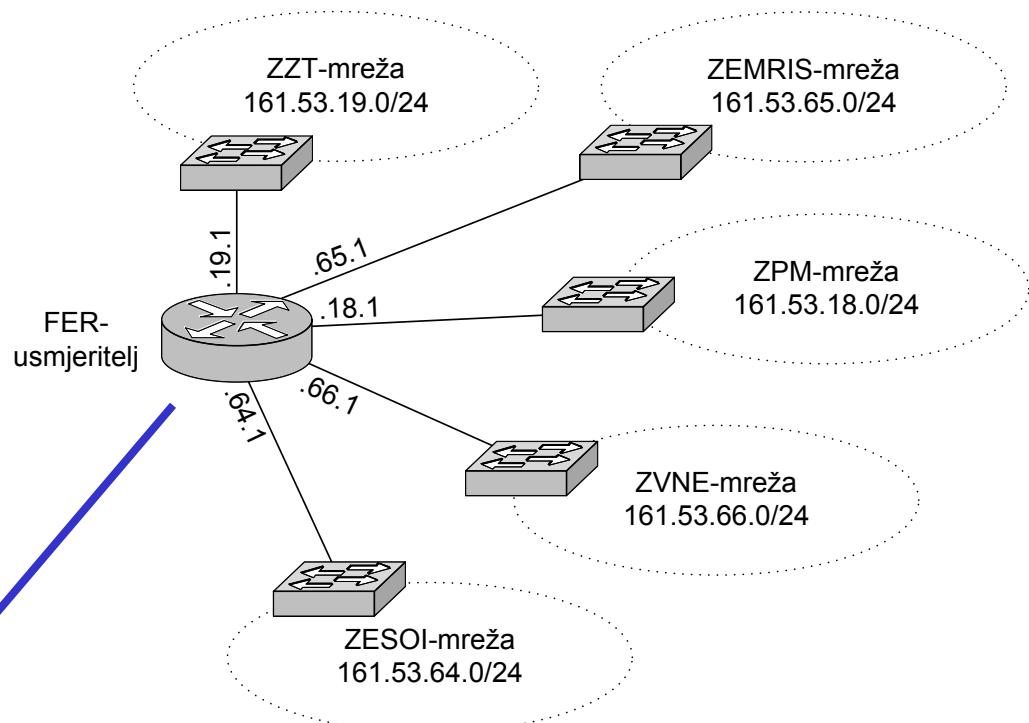
Primjer: akademska i istraživačka mreža CARNet

Organizacija ZZT-mreže

Optička vertikalna



Organizacija FER-ove mreže

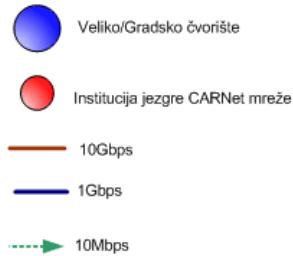


IP odredište	IP adresa sljedećeg skoka	izlazno sučelje
161.53.19.0/24	0.0.0.0	eth0
161.53.18.0/24	0.0.0.0	eth1
161.53.66.0/24	0.0.0.0	eth2
161.53.64.0/24	0.0.0.0	eth3

tablica usmjeravanja

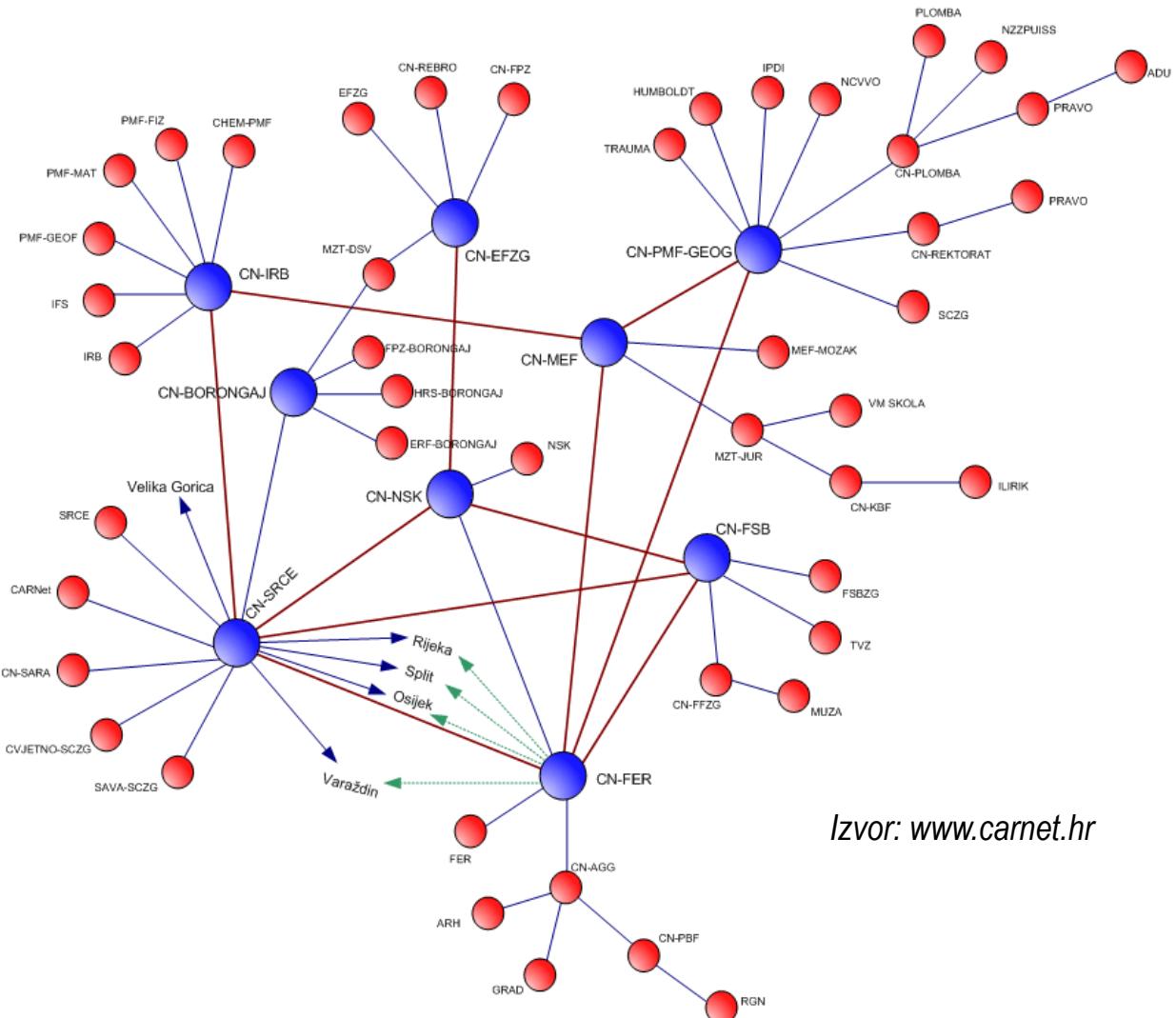


CARNet-ova mreža u Zagrebu



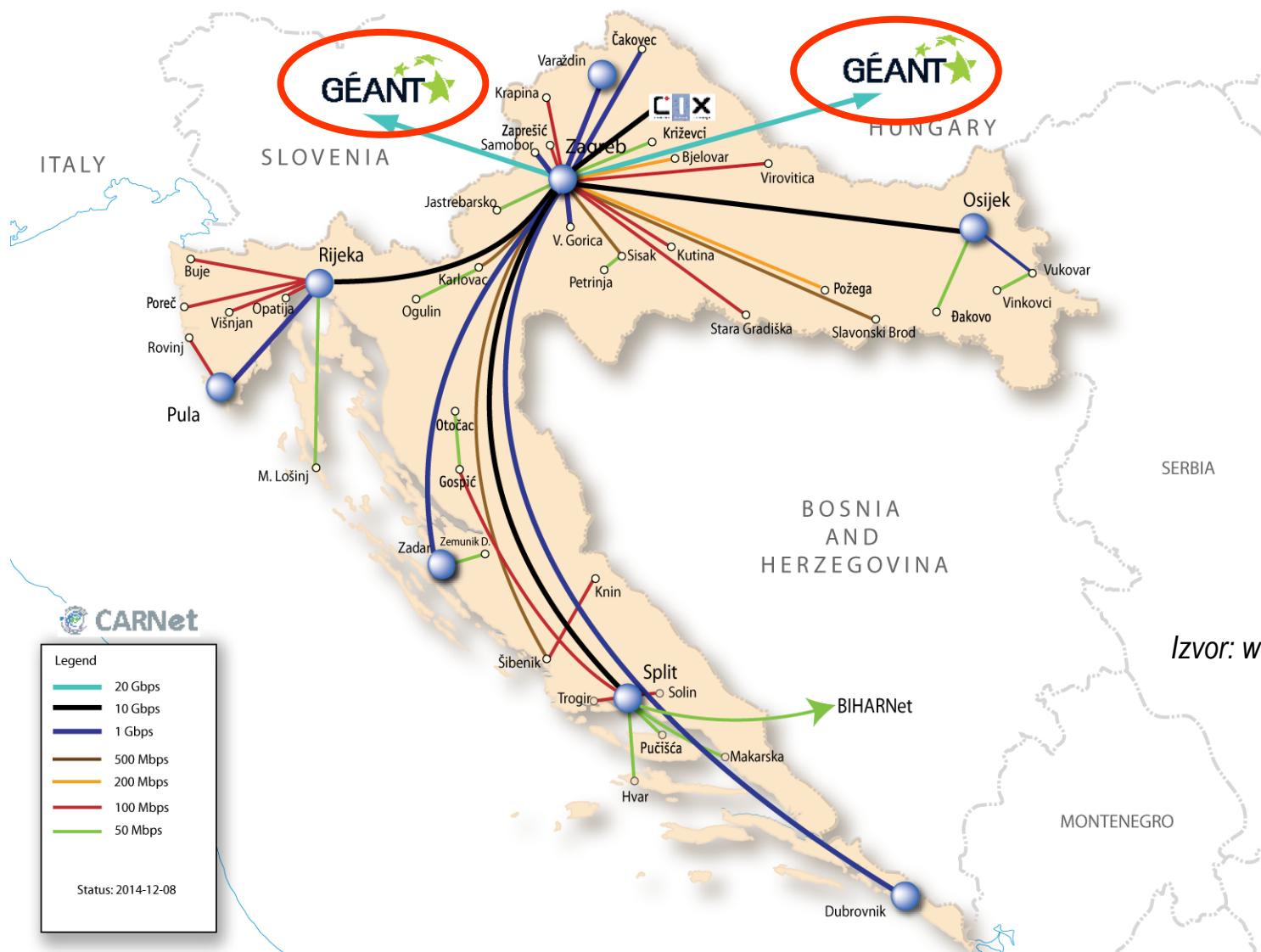
Stanje na 01.04.2009.

CN-SRCE	Sveučilišni računski centar
CN-FER	Fakultet elektrotehnike i računarstva
CN-FSB	Fakultet strojarstva i brodogradnje
CN-NSK	Nacionalna i sveučilišna knjižnica
CN-IRB	Institut Ruđer Bošković
CN-MEF	Medicinski fakultet
CN-PMF-GEOG	PMF-Geografski odsjek
CN-EFZG	Ekonomski fakultet Zagreb
CN-BORONGAJ	Sveučilišni računarski centar
CN-SARA	Studentski dom Ante Starčević
CVJETNO SCZG	Studentski dom Cvjetno naselje
SAVA SCZG	Studentski dom Stjepan Radić
CN-AGG	Arhitektonski fakultet
ARH	Arhitektonski fakultet
GRAD	Gradevinski fakultet
CN-PBF	Prehrambeno - biotehnički fakultet
RGN	Rudarsko-geološko-naftni fakultet
CN-FFZG	Filozofski fakultet
MUZA	Muzička akademija
TVZ	Tehničko veleučilište u Zagrebu
CHEM-PMF	Prirodoslovno-matematički fakultet
PMF-FIZ	PMF-Fizički odsjek
PMF-MAT	PMF-Matematički odsjek
PMF-GEOF	PMF-Geofizički odsjek
IFS	Institut za fiziku
MEF-MOZAK	Medicinski fakultet, Hrvatski institut za istraživanje mozga
MZT	Ministarstvo znanosti, obrazovanja i športa
VM SKOLA	Zdravstveno veleučilište
CN-KBF	Katolički bogoslovni fakultet
ILIRIK	Theološki fakultet Matija Vlačić Ilirik s pravom javnosti
TRAUMA	Klinika za traumatologiju
HUMBOLDT	Klub hrvatskih Humboldtovaca
IPDI	Institut društvenih znanosti Ivo Pilar
NCVVO	Nacionalni centar za vanjsko vrednovanje obrazovanja
CN-PLOMBA	Stomatološki fakultet
CN-REKTORAT	Sveučilište u Zagrebu-Rektorat
SCZG	Studentski centar u Zagrebu
NZZPUISS	Nacionalna zaklada za potporu učeničkom i studentskom standardu
PRAVO	Pravni fakultet
ADU	Akademija dramske umjetnosti
CN-REBRO	Klinički bolnički centar Rebro
CN-FPZ	Fakultet prometnih znanosti
HRS	Hrvatski studiji
ERF	Edukacijsko rehabilitacijski fakultet



Izvor: www.carnet.hr

Mreža CARNet



Croatian Internet eXchange (CIX)

◆ www.cix.hr

Nepotpuna tablica
“peering” ugovora

Oznake:

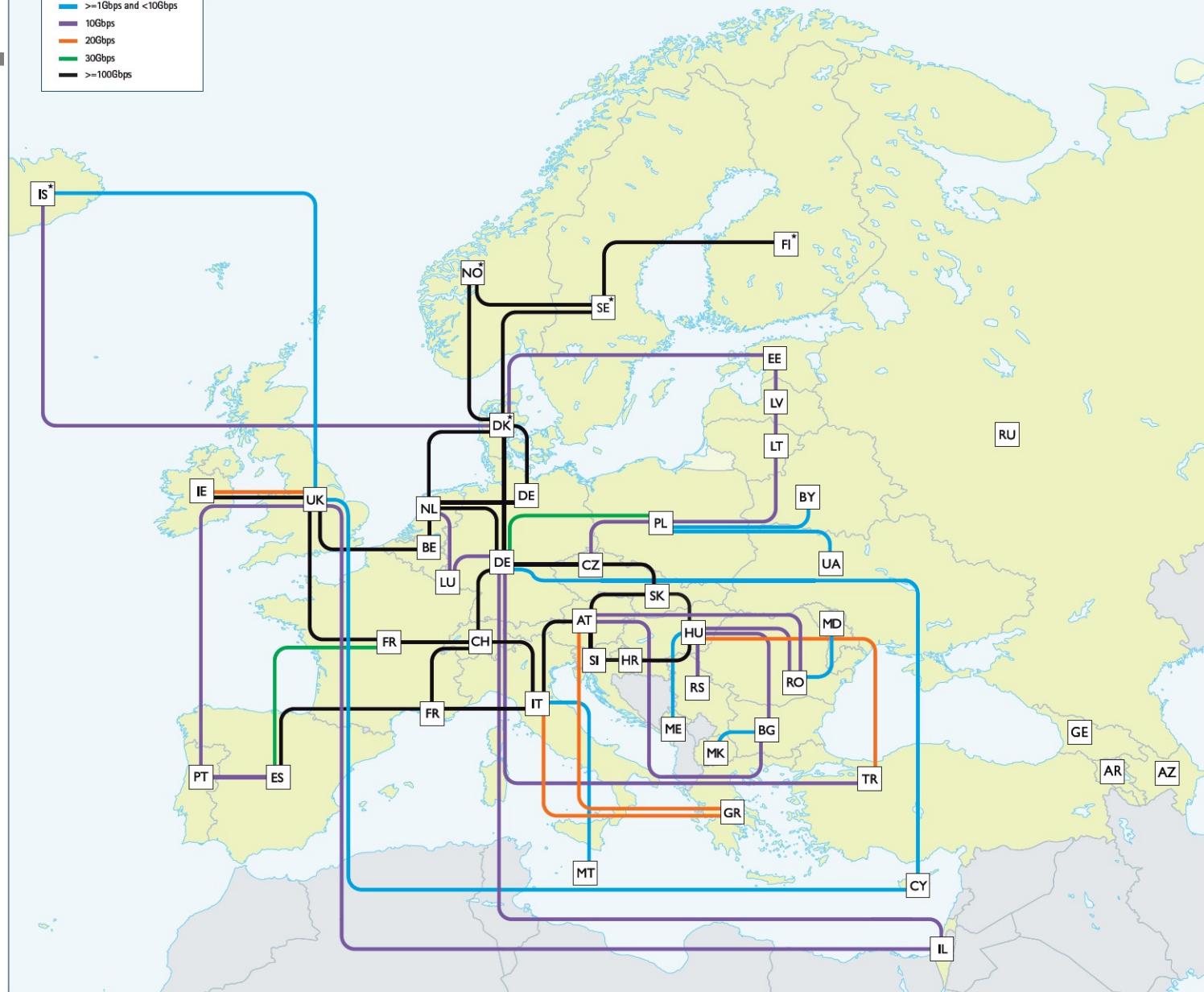
“+” postoji peering
“-” ne postoji peering
“?” nepoznato

	CARNet	Iskon	Metronet telekomun.	VIP-NET	Optima Telekom	HRT	HEP	Amis Telekom
CARNet		+	+	+	+	+	+	+
Iskon	+		+	+	+	+	?	?
Metronet	+	+		+	+	-	-	+
VIP-NET	+	+	+		+	-	-	+
Optima	+	+	+	+		+	+	+
HRT	+	+	-	-	+		+	+

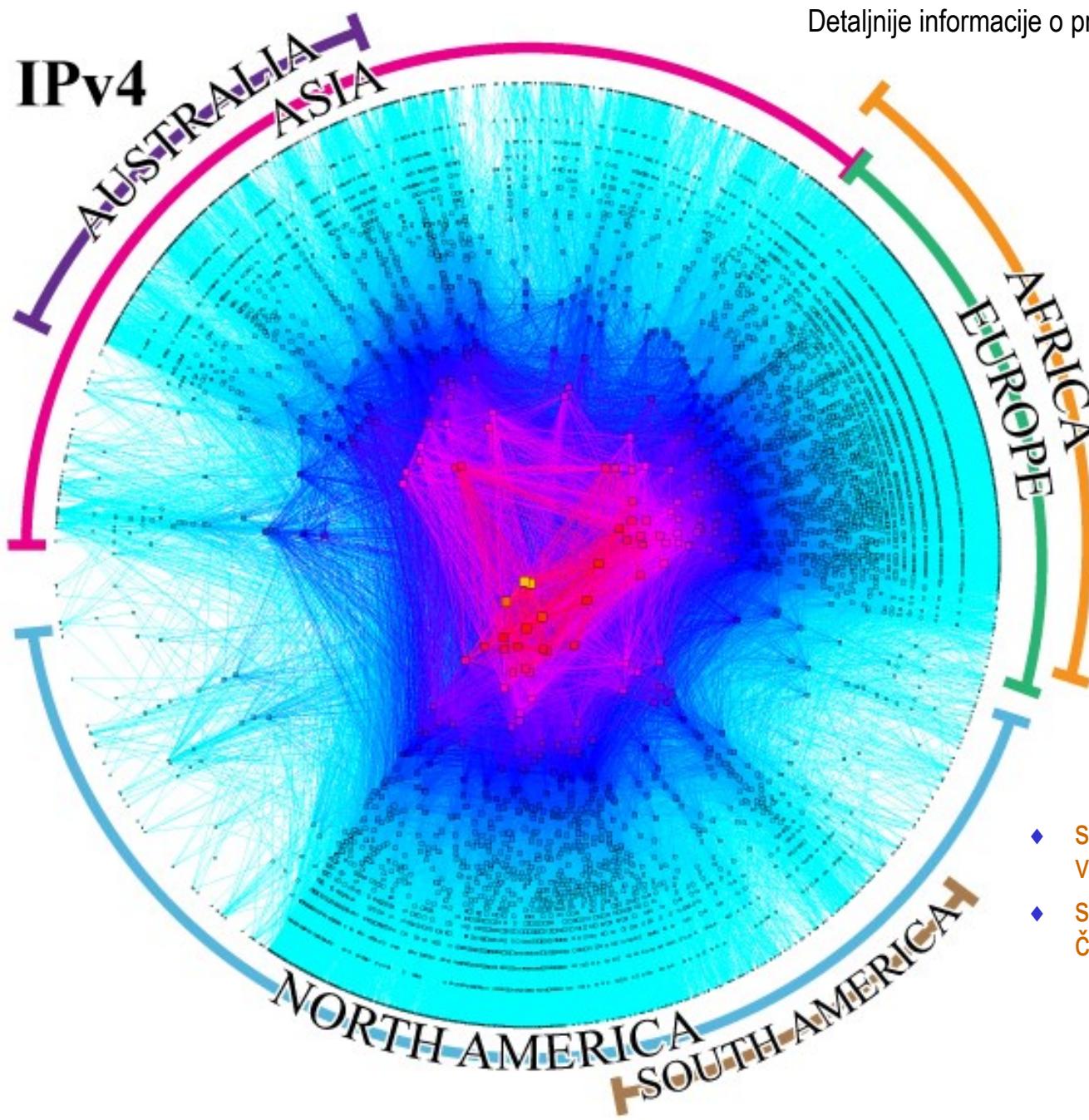
Europska istraživačko- ekademska mreža

Topologija
okosnice mreže
GEANT2

- >=1Gbps and <10Gbps
- 10Gbps
- 20Gbps
- 30Gbps
- >=100Gbps



GEANT connectivity as at January 2014. GEANT is operated by DANTE on behalf of Europe's NRENs.



- svaki "kvadratić" = 1 AS (ukupno više od 45000)
- slika smješta svaki AS na lokaciju čije su polarne koordinate:
 - kut je zemljopisna dužina na kojoj se nalazi uprava AS-a
 - radijus je 1- logaritam od relativnog stupnja povezanosti s drugim AS-ovima

Odabране теме из технологија Интернета (1)

Sigurnosni izazovi protokola sloja podatkovne poveznice;
sigurnosna stijena (engl. *firewall*)

- ◆ Lokalna mreža Ethernet je, bez posebnih zaštita, vrlo nesigurna mreža
- ◆ Napadi su mogući na
 - Mrežne uređaje - LAN-komutatore
 - Krajnje stanice
- ◆ Primjeri napada
 - Neautorizirano priključivanje na mrežu
 - Snimanje mrežnog prometa
 - Preusmjeravanje komunikacije
 - Manipulacija upravljačkih protokola LAN-komutatora

Neautorizirano priključivanje na mrežu

- ◆ Svaka otvorena utičnica omogućava neautorizirano spajanje
- ◆ Podešavanje DHCP-a kako ne bi davao adrese nepoznatim stanicama nije nikakva zaštita
 - MAC-adrese se mogu lažirati
 - Može se snimati mrežni promet te odrediti mrežne parametre koji se potom „ručno” postave računalu
- ◆ Zaštita:
 - Isključivanje mrežnih utičnica koje se ne koriste
 - Autentifikacija prije nego što se omogući spajanje - 802.1x

Snimanje mrežnog prometa

- ◆ Činjenica da je mreža Ethernet komutirana ne onemogućava snimanje svog prometa u mreži!
- ◆ LAN-komutator za „učenje“ ima ograničenu količinu memorije
 - Da bi se LAN-komutator degenerirao u parični obnavljač potrebno je preplaviti tu memoriju
 - Alati koji generiraju veliku količinu prometa s velikim brojem MAC-adresa
 - Kada više nema mjesta za novu MAC-adresu, LAN-komutator se započinje ponašati kao parični obnavljač - moguće snimanje svog prometa!
- ◆ Zaštita:
 - Napredniji LAN-komutator omogućavaju limitiranje broja MAC-adresa po pristupu! Alarmiranje administratora!

Preusmjeravanje komunikacije

- ◆ ARP je vrlo problematičan protokol
 - Nema nikakve zaštite
 - Za prvu stanicu koja odgovori izvorište će pretpostaviti da posjeduje traženu adresu!
- ◆ Kada neka stanica pita za usmjeritelj, napadač može odgovoriti sa svojom MAC-adresom
 - Preusmjerava komunikaciju tako da ide preko njega
 - Napadač može utjeloviti bilo koju stanicu, ne samo usmjeritelj
- ◆ Zaštita
 - Indirektna: kontrola tko se spaja na mrežu
 - Fiksiranje ARP/IP-zapisa, indirektno uz pomoć viših protokola (SSL, IPsec)

Sigurnosna stijena (1)

- ◆ Danas ključni element zaštite
 - Sam za sebe ipak nedovoljan!
- ◆ Nalazi se na granici dvije ili više mreža
 - Mreže kojoj se vjeruje (najčešće lokalna mreža)
 - Mreža koju štiti
 - Mreže kojoj se ne vjeruje (Internet)
 - Mreža od koje se štiti
 - Često se poslužitelji kojima se pristupa s Interneta smještaju u posebnu mrežu
 - Demilitarizirana Zona (DMZ)
 - Za svaku mrežu na koju je spojen ima zasebno sučelje
 - Bitno je da svi paketi koji prolaze između mreža idu preko sigurnosne stijene

Sigurnosna stijena (2)

- ◆ U osnovi jednostavan filter paketa
 - Svaki paket koji prolazi uspoređuje se s bazom pravila
 - Svako pravilo sadrži uvijete te akciju
 - Uvjeti su podaci iz protokola (IP-adrese, vrata transportnog sloja, ...)
 - Akcija je blokiranje/odbacivanje paketa, ili njegovo propuštanje
 - Prvo pravilo čiji uvjeti odgovaraju paketu se primjenjuje
 - Pravila definira i upisuje u sigurnosnu stijenu administrator na temelju onoga što je dozvoljeno (ili zabranjeno)
- ◆ Dobra sigurnosna praksa kaže da sve što nije eksplicitno dozvoljeno je zabranjeno
 - Ako niti jedno pravilo ne odgovara IP-paketu onda se podrazumijeva akcija blokiranja!

Sigurnosna stijena (3)

- ◆ Podjela sigurnosnih stijena
 - Bez stanja (engl. *stateless*)
 - Svaki paket tretira se nezavisno od svih ostalih
 - Teži za podešavanje, nesigurniji, brži
 - Sa stanjem (engl. *statefull*)
 - Sigurnosna stijena vodi evidenciju o paketima i zna koji paket pripada kojoj vezi
 - Relativno lakši za podešavanje, sigurniji, sporiji
- ◆ Često se sigurnosna stijena kombinira s usmjeriteljem i NAT-uređajem
 - To je posebno slučaj kod jeftinijih uređaja
 - ADSL-uređaj
 - **Sigurnosna stijena i NAT nisu isti uređaji!**

Odabране теме из технологија Интернета (2)

Protokol IPv6

Protokol IPv6

- ◆ Protokol IPv4 - podsjetnik
- ◆ Razlozi uvođenja protokola IPv6
- ◆ Glavne značajke IPv6
- ◆ Adresiranje
- ◆ Format IPv6-datagrama, osnovno i dodatna zaglavlja
- ◆ Uvođenje protokola IPv6 u mrežu: tranzicijski mehanizmi

Odlike protokola IP: podsjetnik

- ◆ *Internet Protocol (IP)*, verzija IPv4 (RFC 791, STD-5)
 - ◆ Glavne odlike:
 - Neovisan o nižim protokolima
 - Ethernet, IEEE 802.3, PPP, ...
 - Datagramski način rada
 - Nespojna usluga
 - Nepotvrđena usluga
 - Nema mehanizama kontrole toka
 - Nema garancije očuvanja redoslijeda datagrama
 - ◆ Uloga u protokolnom složaju TCP/IP: omatanje (engl. *encapsulation*)
 - Prihvata podatke od višeg sloja (npr. transportnog protokola TCP, UDP), smješta ih u podatkovno polje IP-datagrama i predaje datagram protokolu sloja podatkovne poveznice (npr. Ethernet)
- } usluga IP-a transportnom sloju:
nepouzdana dostava datagrama

Funkcionalnost protokola IP: podsjetnik

- ◆ Definira **shemu adresiranja** u Internetu
 - Jedinstveni adresni prostor
 - Svako krajnje računalo ima po jednu IP-adresu za svako mrežno sučelje
 - Svako krajnje računalo može koristiti i više posebnih adresa (npr., adresa *localhost*, *multicast*, *broadcast*, ...)
 - Ako su izvorišna i odredišna adresa u različitim mrežama, IP-datagrami se usmjeravaju preko jednog ili više IP-usmjeritelja

- ◆ Definira kako provesti **fragmentaciju**
 - Datagram mora “stati” u podatkovno polje okvira sloja podatkovne poveznice
 - Datagram veći od toga mora se fragmentirati
 - Na strani primatelja fragmenti se sastavljaju

Protokol IP – verzije

- ◆ Trenutno u primjeni IP verzije 4 (IPv4)
- ◆ Nova inačica IP-a je verzija 6 (*Internet Protocol Version 6, IPv6*)
 - Specifikacija u RFC 2460
 - Standardiziran 1998. godine

Razlozi uvođenja IPv6 (1)

◆ Ograničenja IPv4:

- ◆ Broj raspoloživih IP-adresa postao premalen (**32-bitne adrese**)
- ◆ Prevelike tablice usmjeravanja
- ◆ Problemi upravljanja mrežom
- ◆ Nedovoljni **sigurnosni mehanizmi** na mrežnom sloju
- ◆ Nedovoljni **mehanizmi pokretljivosti** na mrežnom sloju
- ◆ Slaba potpora za prijenos podataka u stvarnom vremenu: **kvaliteta usluge (QoS)**

Razlozi uvođenja IPv6 (2)

- ◆ Novosti u IPv6:
 - Duljina adrese 128 bita
 - Veći adresni prostor (2^{128} adresa) omogućuje globalnu umreženost i dostupnost svih čvorova, bez “skrivenih” mreža i računala
 - Učinkovitije usmjeravanje
 - Mogućnost označavanja tokova (označavanje paketa koji pripadaju istom medijskom toku, npr. govora ili videa)
 - Podrška za QoS (prijenos u stvarnom vremenu)
 - Provjera autentičnosti i zaštita privatnosti, integritet podataka, povjerljivost
 - Bolja podrška za pokretljivost

Zapis IPv6 adresa

- ◆ Notacija - 8 grupa po 4 heksadekadske znamenke:
npr. EFD1:0989:AB02:7654:C4ED:890B:DE65:1240
- ◆ Adrese v4 se mogu pretvarati u v6 dodavanjem odgovarajućeg prefiksa:
npr. 161.53.19.201 (hex: A135:13C9) postaje
0000:0000:0000:0000:0000:FFFF:A135:13C9
- ◆ Mogući načini zapisa: npr. ::FFFF:161.53.19.201 ili
::FFFF:A135:13C9
- ◆ IPv6-adrese imaju mrežni i računalni dio

Vrste IPv6-adresa

◆ *Unicast* - jednoodredišna adresa

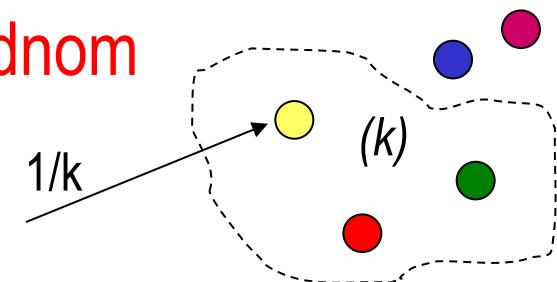
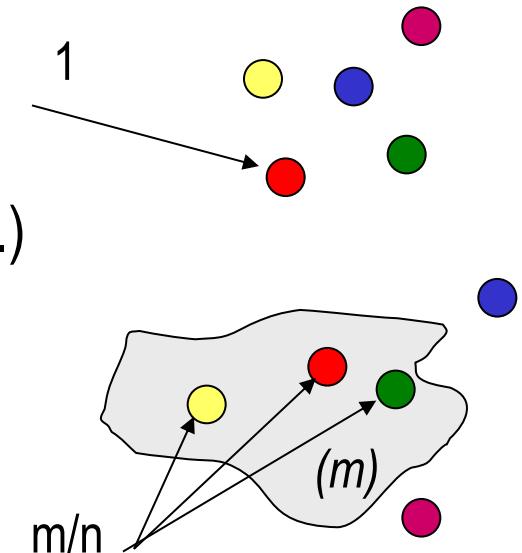
- identificira jedno sučelje računala/čvora
- globalne i lokalne adrese
- posebne adrese (*loopback*, nespecificirane, ...)

◆ *Multicast* - višeodredišna adresa

- određuje skup sučelja
(obično na različitim čvorovima)
- paket se dostavlja svima sučeljima određenim tom adresom

◆ *Anycast* - adresa više sučelja, dostava jednom sučelju

- paket se dostavlja samo jednom (“najbližem”) sučelju s definiranom adresom

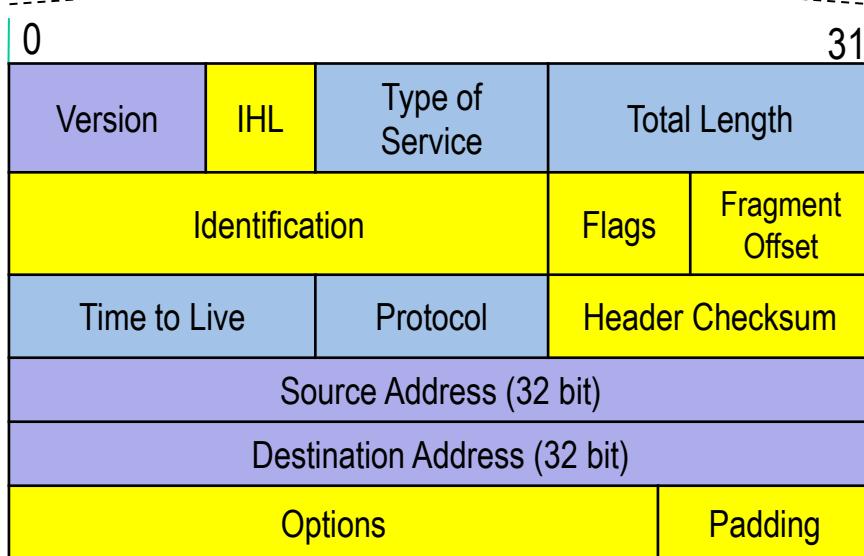


Dodjela jednoodredišne IPv6-adrese

- ◆ Statičko (“ručno”) postavljanje
- ◆ Autokonfiguracija bez poslužitelja (*stateless*) - jednoodredišna adresa se stvara iz MAC-adrese
- ◆ Autokonfiguracija s poslužiteljem (*statefull*) - koristi se DHCPv6 poslužitelj

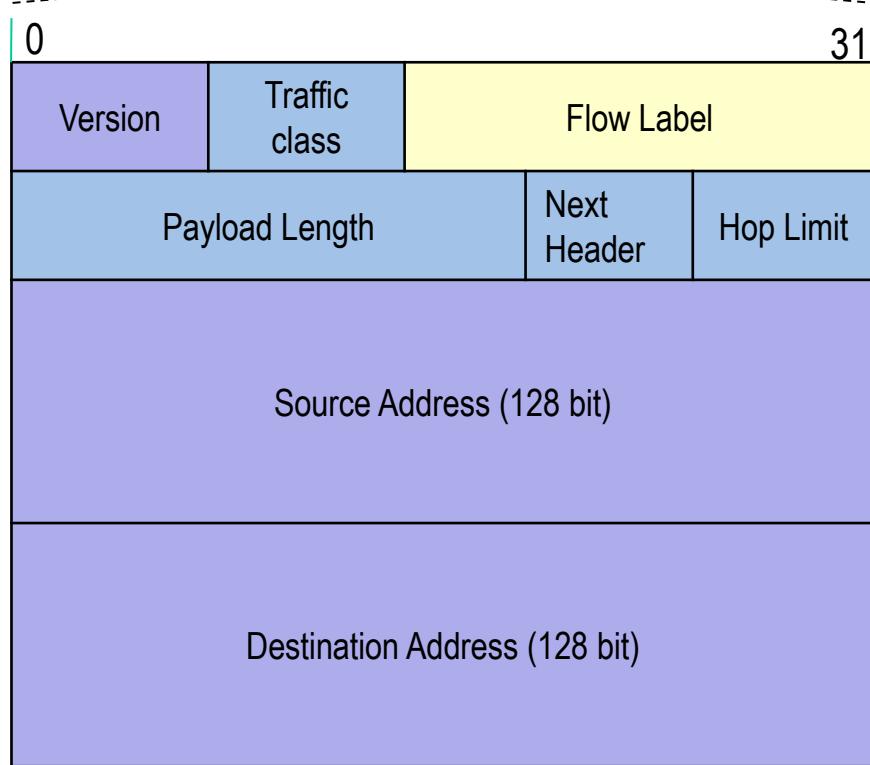
Usporedba zaglavlja IPv4 i IPv6

IPv4-zaglavje



Bez opcija 20 okteta; s opcijama max. 60 okteta

IPv6-zaglavje



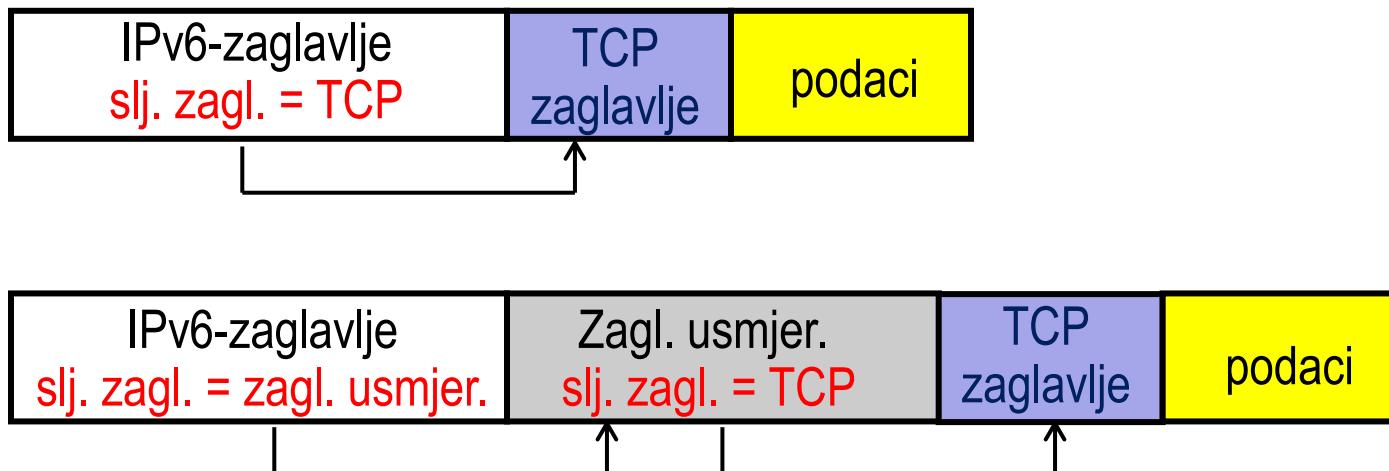
Fiksno 40 okteta

- naziv polja isti u IPv4 i IPv6
- polje izbačeno u IPv6
- promjena imena i pozicije polja u IPv6
- novo polje u IPv6

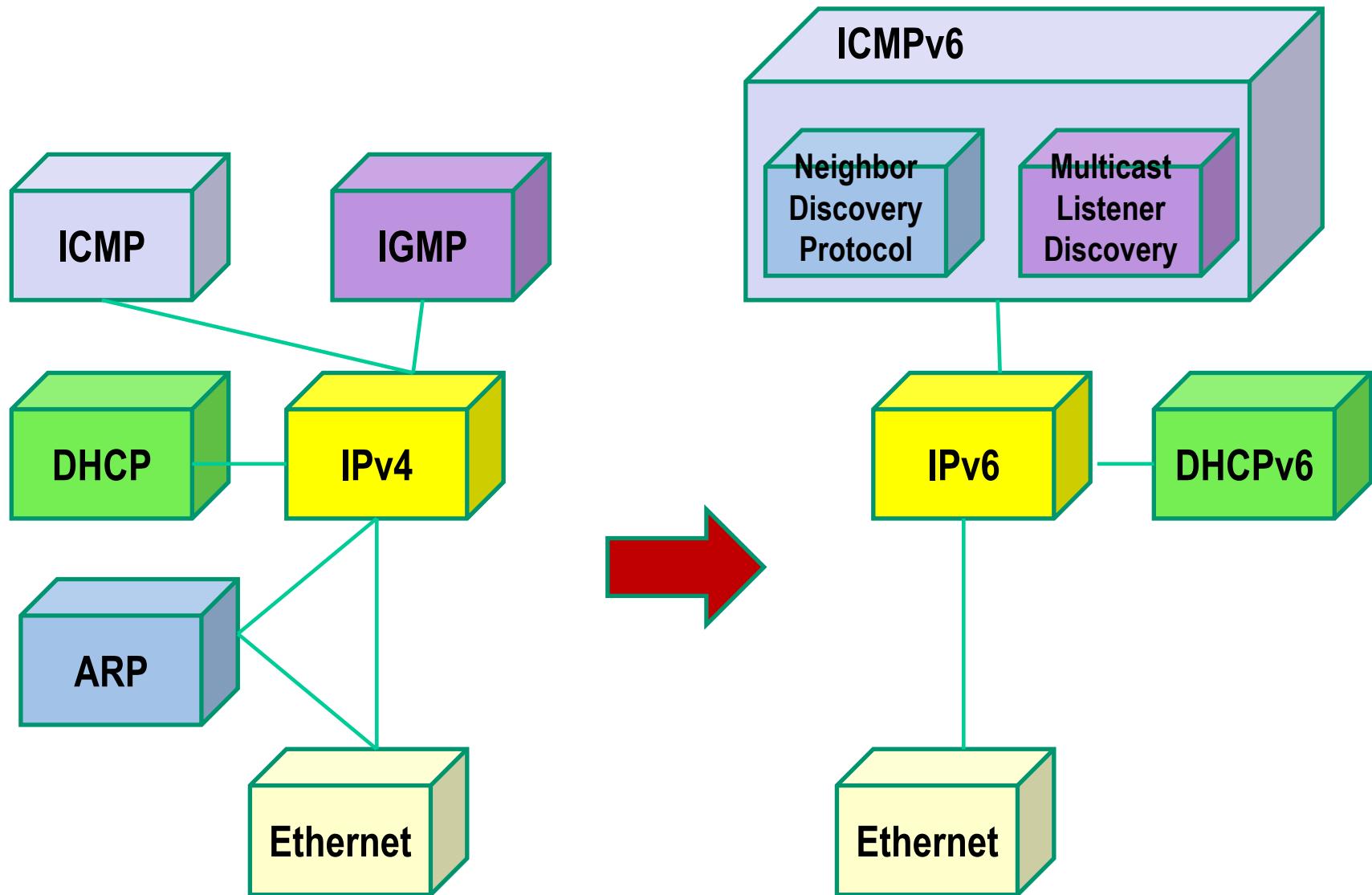
Dodatna zaglavlja

- ◆ Korištenje posebnih opcija u IPv4 usporava prosljeđivanje paketa u usmjeriteljima
- ◆ U IPv6 se iza osnovnog zaglavlja, po potrebi, dodaju dodatna zaglavlja

Primjeri:



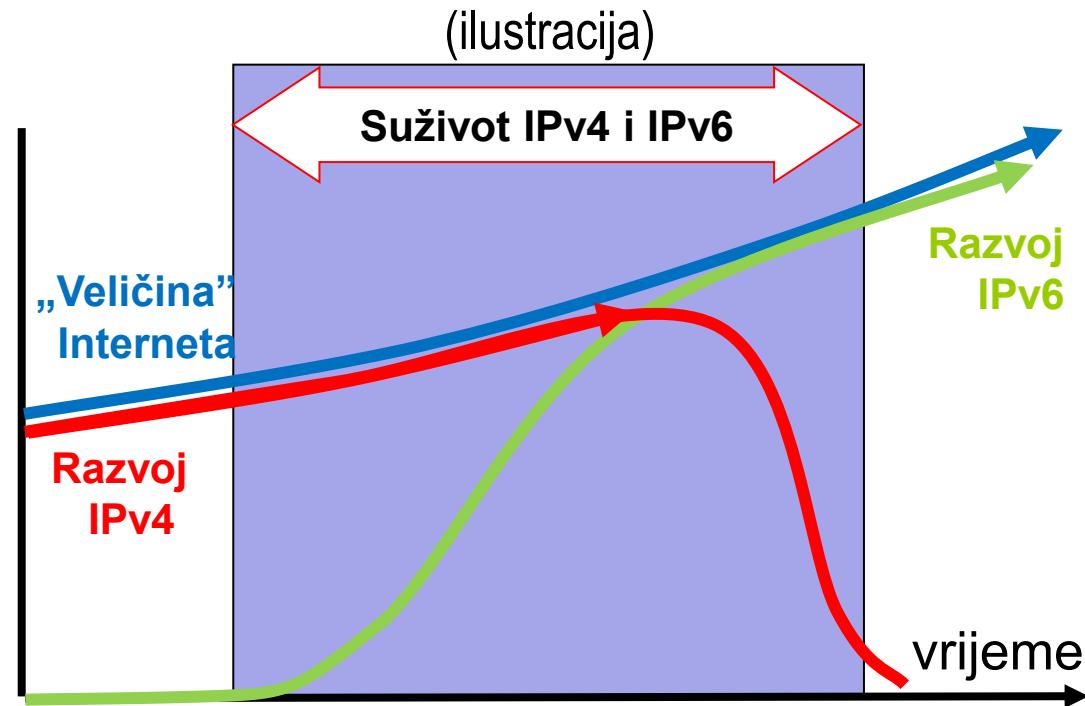
Kontrolni protokoli za IPv6



Prelazak na IPv6

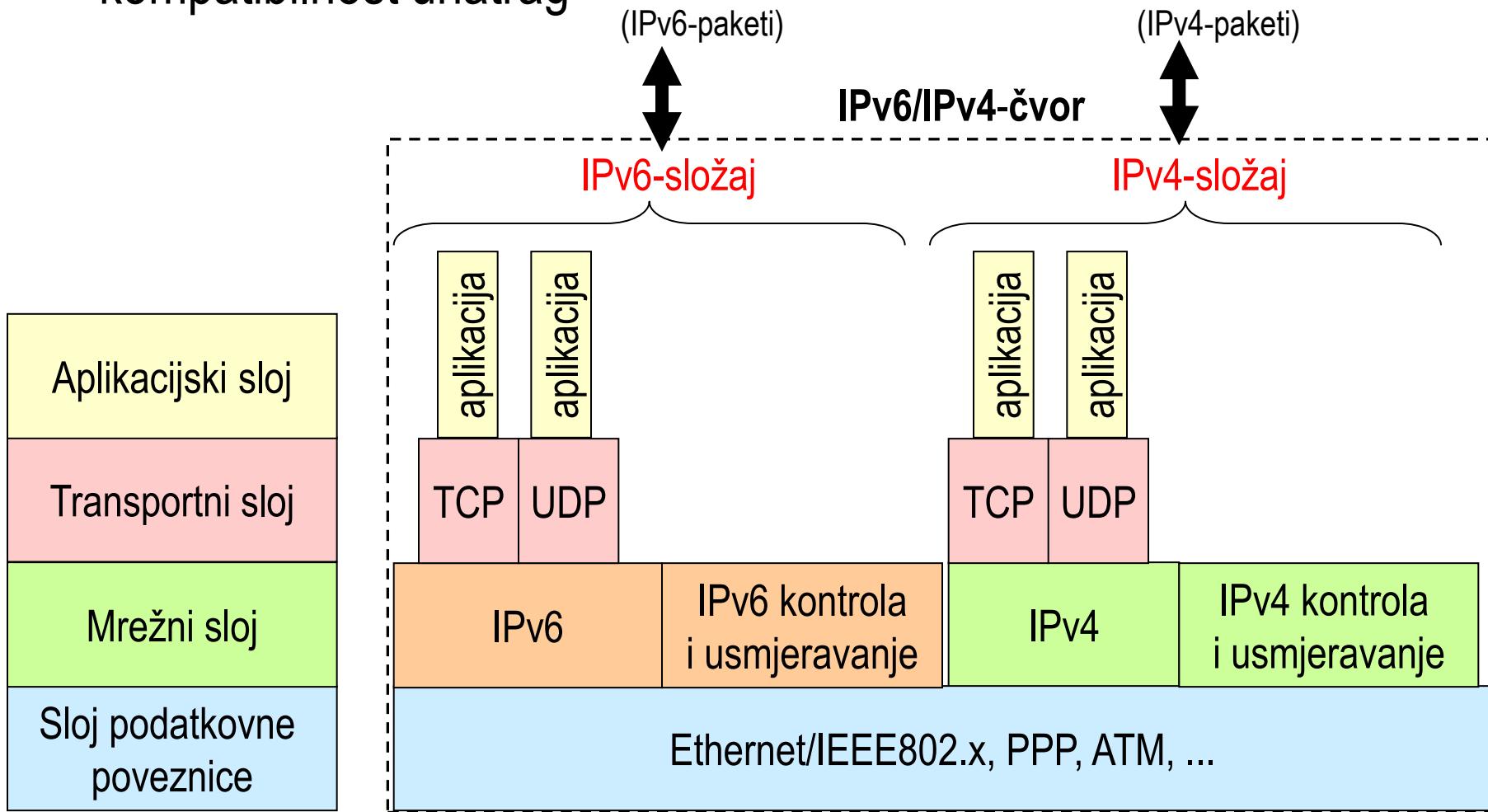
- ◆ Protokoli IPv4 i IPv6 nisu međusobno kompatibilni
- ◆ Očekuje se da će prelazak na IPv6 trajati godinama
- ◆ Za komunikaciju IPv6 čvorova preko IPv4 infrastrukture potrebni su posebni tranzicijski mehanizmi

- ◆ Tri osnovna tranzicijska mehanizma:
 - **dvostruki složaj (dual stack)**
 - **tuneliranje**
 - **prevodenje protokola**



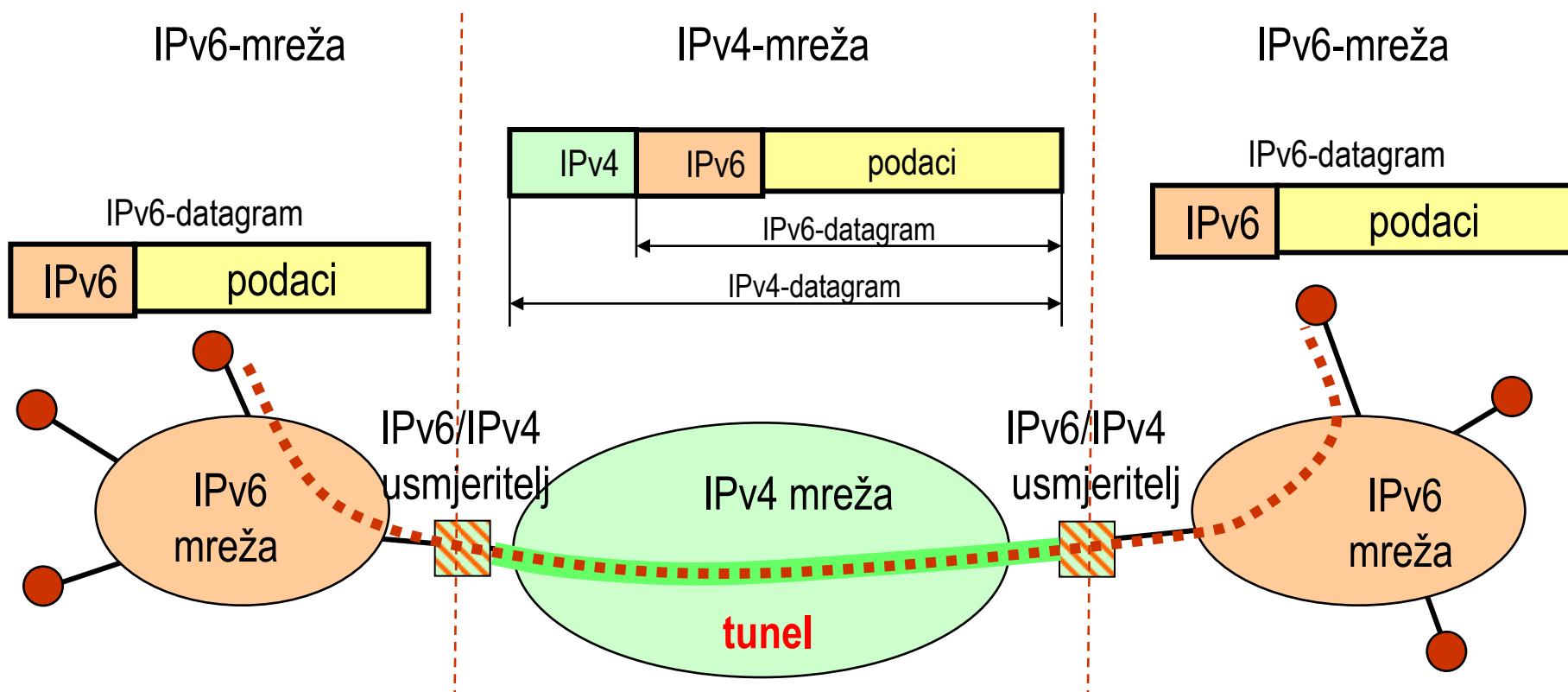
Dvostruki složaj – IPv6/IPv4-čvor

- ◆ IPv6/IPv4-čvor - IPv6-čvor koji sadrži i izvedbu protokola IPv4 za "kompatibilnost unatrag"



Primjer tuneliranja

- ◆ Datagrami IPv6 ovijaju se datagramima IPv4
- ◆ Konfiguracija tuneliranja: usmjeritelj - usmjeritelj



Postupno uvođenje IPv6

- ◆ 1. faza: suživot IPv4 i IPv6 - prevladavajući protokol IPv4
 - IPv6-mreže komuniciraju putem IPv4-mreže s usmjeriteljima koji ne podržavaju IPv6
 - IPv6-mreže komuniciraju putem IPv4-mreže s usmjeriteljima koji podržavaju IPv6
- ◆ 2. faza: suživot IPv4 i IPv6 - prevladavajući protokol IPv6
- ◆ 3. faza: konačno rješenje s IPv6

Umjesto kraja...

... dalje u studiju o komunikacijskim mrežama

◆ 6. semestar

- Višemedijske usluge
- Telekomunikacijski sustavi i mreže
- Lokalne mreže
- Javna pokretna mreža
- Mrežno programiranje
- Integracija računala i telefonije

◆ 7. semestar

- Informacijske mreže
- Komunikacijski protokoli
- Fotoničke telekomunikacijske mreže

◆ Itd.