

Računalniške komunikacije

2020/21

omrežna plast
IPv4, fragmentacija, naslavljanje,
podomrežja, hierarhija

Pridobljeno znanje s prejšnjih predavanj

- **povezavna plast**
 - PPP (point-to-point protocol)
 - struktura okvirja, vrivanje podatkov
 - naslavljanje z **naslovi MAC** ($48 = 24+24$ bitov)
 - **protokol ARP** za preslikovanje logičnih naslovov IP v fizične naslove MAC
 - aktivna oprema (ponavljalnik, razdelilnik, stikalo)
 - delovanje **stikal**
 - stikalna tabela; akcije: **poplavljjanje, posredovanje, filtriranje**
 - vloga stikal v topologiji omrežja (medsebojno povezovanje stikal)
- **omrežna plast**
 - funkcije usmerjevalnikov: **posredovanje in usmerjanje**
 - **storitve** omrežne plasti (zagotovljena dostava, čas, zaporedje, pasovna širina, varianca zakasnitve, varnost)

Storitve omrežne plasti

Omrežna plast *lahko omogoča* naslednje storitve:

1. **zagotovljena dostava** paketov
2. dostava paketov v **zagotovljenem času**
3. dostava paketov v **pravem zaporedju**
4. zagotovljena spodnja **meja pasovne širine**
5. največja dovoljena **varianca zakasnitve (jitter)**:

$$t_{\text{pošiljanja}}(P_2) - t_{\text{pošiljanja}}(P_1) \approx t_{\text{prejetja}}(P_2) - t_{\text{prejetja}}(P_1)$$

6. **varno komunikacijo** (zaupnost, integriteto podatkov, avtentikacijo)



Storitve Interneta

- Katere od naštetih storitev zagotavlja Internet?

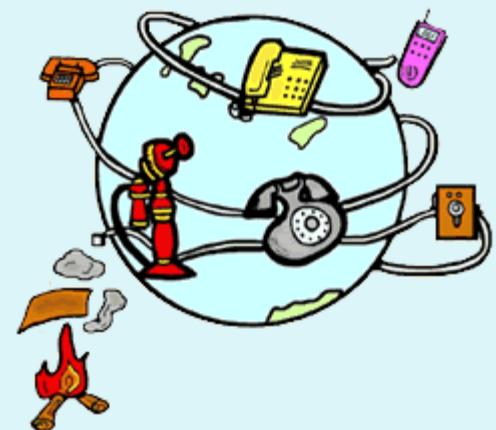
Prav nobene. ☺

(best-effort service)

"Best-effort service is a euphemism for no service at all"

Omrežje	Model	zagotovljene storitve					skupek storitev je model storitev
		pas. širina	brez izgube	Vr. red	Čas	obv. o zamašitvi	
Internet	best effort	ne	ne	ne	ne	ne (izguba)	na internetu te težave rešujemo na višjih plasteh (transportna ...)
ATM	CBR constant bit rate	konstantna	da	da	da	ni zamašitev	
ATM	ABR available bit rate	minimalna	ne	da	ne	da	

Povezavna in nepovezavna omrežja

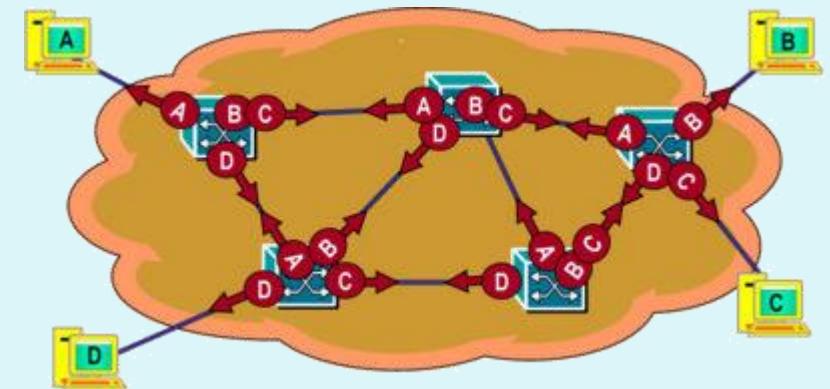
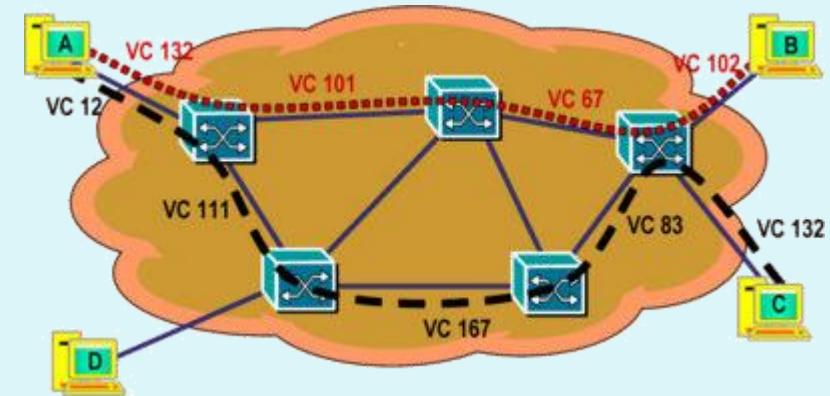


Povezavna in nepovezavna omrežja

circuit-switching

- **povezavna omrežja** (navidezni vodi) omogočajo vzpostavitev zveze v omrežni infrastrukturi med pošiljateljem in prejemnikom
- **nepovezavna omrežja** (datagramska, paketna) omogočajo posredovanje paketov skozi infrastrukturo brez vzpostavljenih povezav

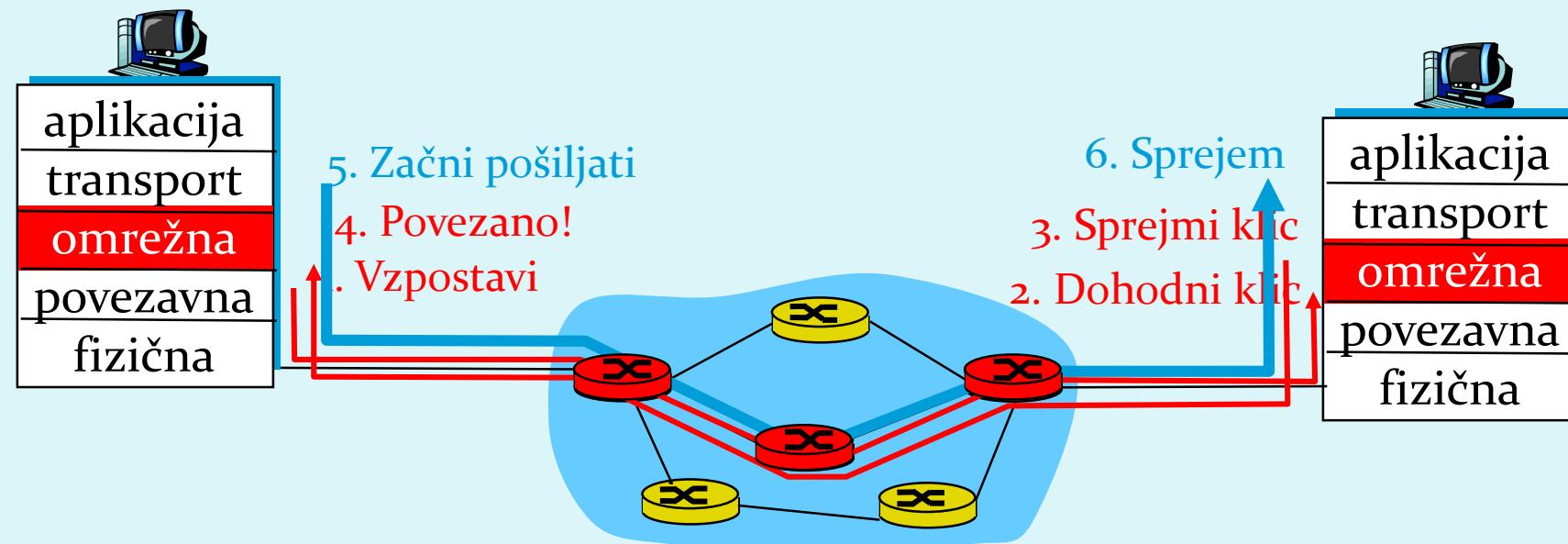
=> Kam spada Internet?



Navidezni vodi

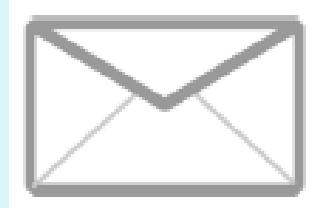


- podobno kot telefonske zveze
- faze pri izvedbi navideznega voda: vzpostavitev, tok podatkov, rušenje
- številke vodov na povezavah neodvisne, kar omogoča lažjo konfiguracijo
- usmerjevalniki usmerjajo pakete glede na **številke vodov**
- uporaba: ATM, X.25, MPLS, Frame Relay (ne Internet!)

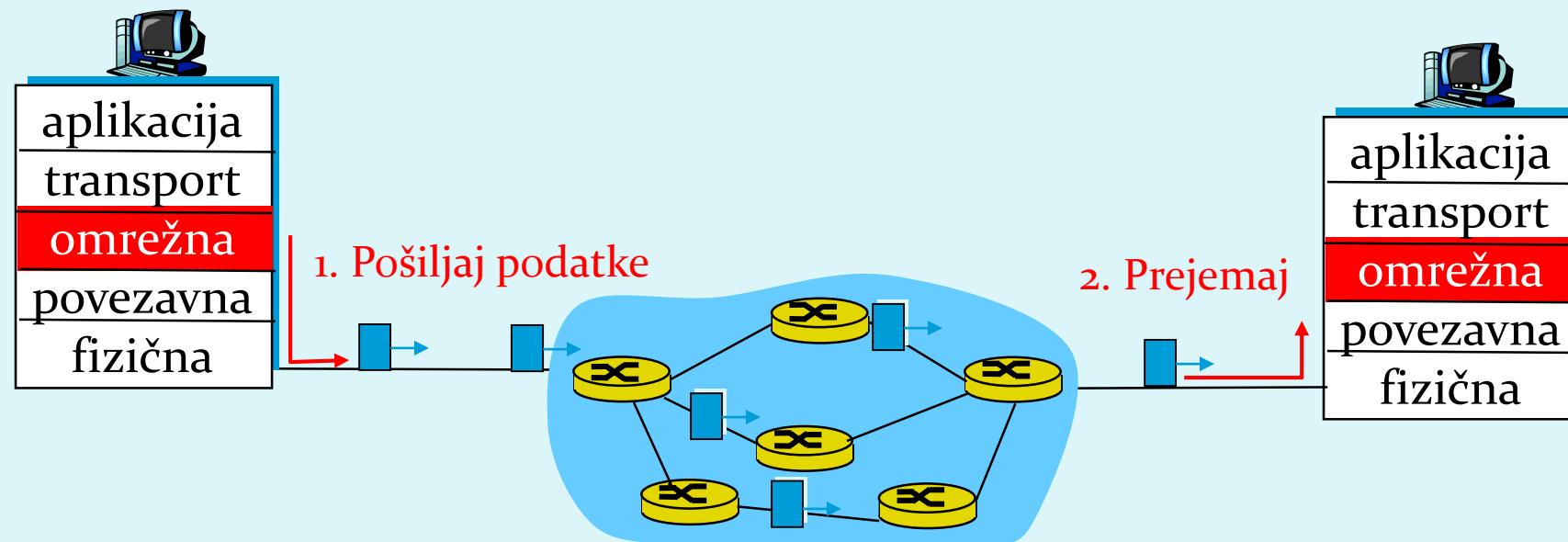


Datagramska omrežja

= INTERNET

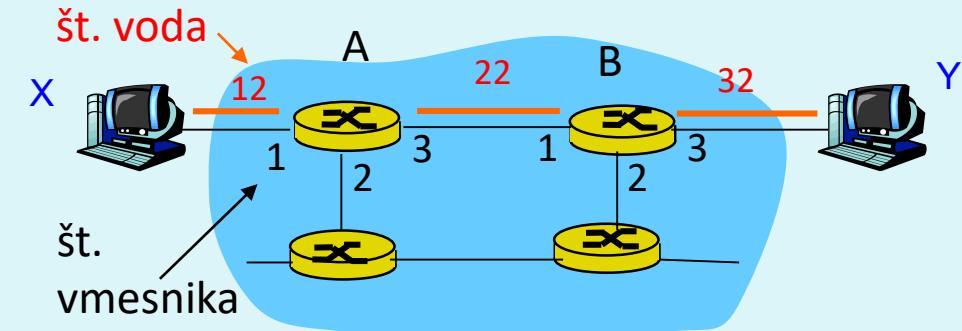


- ni faze vzpostavljanja povezave
- usmerjevalniki ne hranijo podatkov o končnih povezavah
- paketu se doda **naslov cilja** in se ga "vrže" v omrežje
- usmerjevalniki **posredujejo glede na ciljni naslov** v paketu
- paket lahko med istim izvorom in ciljem potuje po različnih poteh



Navidezni vodi: posredovalne tabele

- posredovalna tabela se nahaja v usmerjevalniku:** vsebuje podatke za posredovanje paketov
- paketi so označeni z **identifikatorjem voda**



Vhodni vmesnik	Vhodna št. voda	Izhodni vmesnik	Izhodna št. voda
1	12	3	22
2	63	1	18
3	7	2	17
...

kar pride na vhodni vmesnik 1 preko voda 12, gre ven na izhodni vmesnik 3 in izhodni vod 22

na B pride na vhodni vmesnik 1 preko voda 22, in gre ven na izhodni vmesnik 3 in izhodni vod 32

(od X proti Y)

Vhodni vmesnik	Vhodna št. voda	Izhodni vmesnik	Izhodna št. voda
1	22	3	32
1	34	2	23
2	4	1	55
...

Datagramsko omrežje: posredovalne tabele

- uporabljamo 32-bitne naslove pošiljateljev in prejemnikov
- naslovimo lahko $2^{32}=4$ milijarde naslosov, kar bi zahtevalo ogromne posredovalne tabele
- **(možna) REŠITEV 1:** združimo dele nasloov v range (razpone nasloov):

Ciljni naslov	Vmesnik povezave
Od 11001000 00010111 00010000 00000000	0
Do 11001000 00010111 00010111 11111111	
Od 11001000 00010111 00011000 00000000	1
Do 11001000 00010111 00011000 11111111	
Od 11001000 00010111 00011001 00000000	2
Do 11001000 00010111 00011111 11111111	
sicer	3

te deli so isti (predpone)

te deli se razlikujejo

- **REŠITEV 2:** posredujemo na podlagi **PREDPONE** (prefiksa) - začetnih bitov naslova ← to je zanimivo!

Ujemanje najdaljše predpone (longest prefix match)

- namesto pisanja rangov:

Ciljni naslov	Vmesnik povezave
Od 11001000 00010111 00010000 00000000 Do 11001000 00010111 00010111 11111111	0
Od 11001000 00010111 00011000 00000000 Do 11001000 00010111 00011000 11111111	1
Od 11001000 00010111 00011001 00000000 Do 11001000 00010111 00011111 11111111	2
sicer	3

definiramo usmerjanje na podlagi predpon, torej:

Ciljni naslov	Vmesnik povezave
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
sicer	3

Ujemanje najdaljše predpone (longest prefix match)

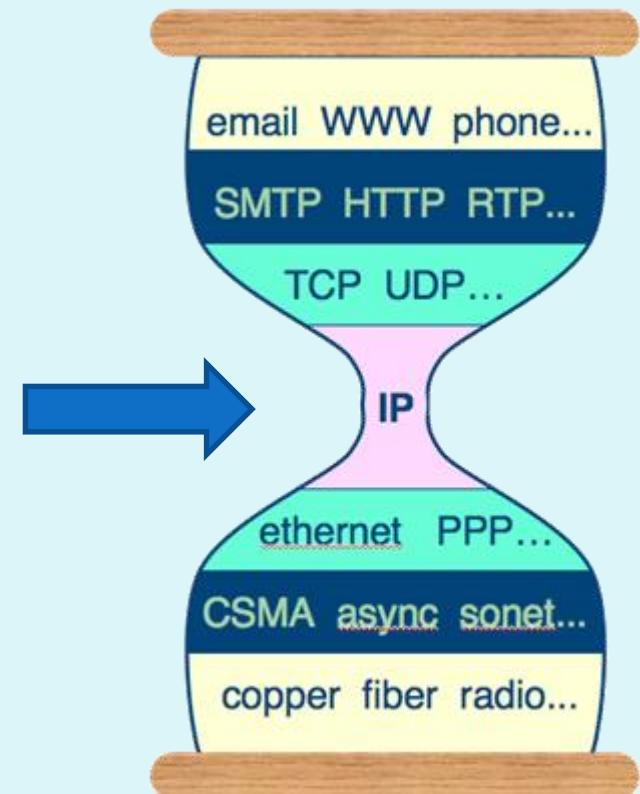
Ciljni naslov	Vmesnik povezave
11001000 00010111 00010	0
11001000 00010111 00011000	1
11001000 00010111 00011	2
sicer	3

- zapis s predponami je krajši in bolj učinkovit
- če ustreza več predpon, uporabimo ujemanje NAJDALJŠE. Primer:
naslov 11001000 00010111 00011000 10100001 se ujema z naslednjima zapisoma:
 - ❖ 11001000 00010111 00011000 10100001 (vmesnik 1)
 - ❖ 11001000 00010111 00011000 10100001 (vmesnik 2)
 - ❖ usmerimo ga na vmesnik 1 (najdaljše ujemanje)
- usmerjevalniki morajo hraniti posredovalne tabele in stanje o povezavah
 - za njihovo avtomatsko posodabljanje skrbijo **usmerjevalni algoritmi** (njihovo delo je počasno - v intervalu nekaj sekund - v primerjavi z vzpostavitvenim časom navideznih vodov - nekaj mikrosekund)

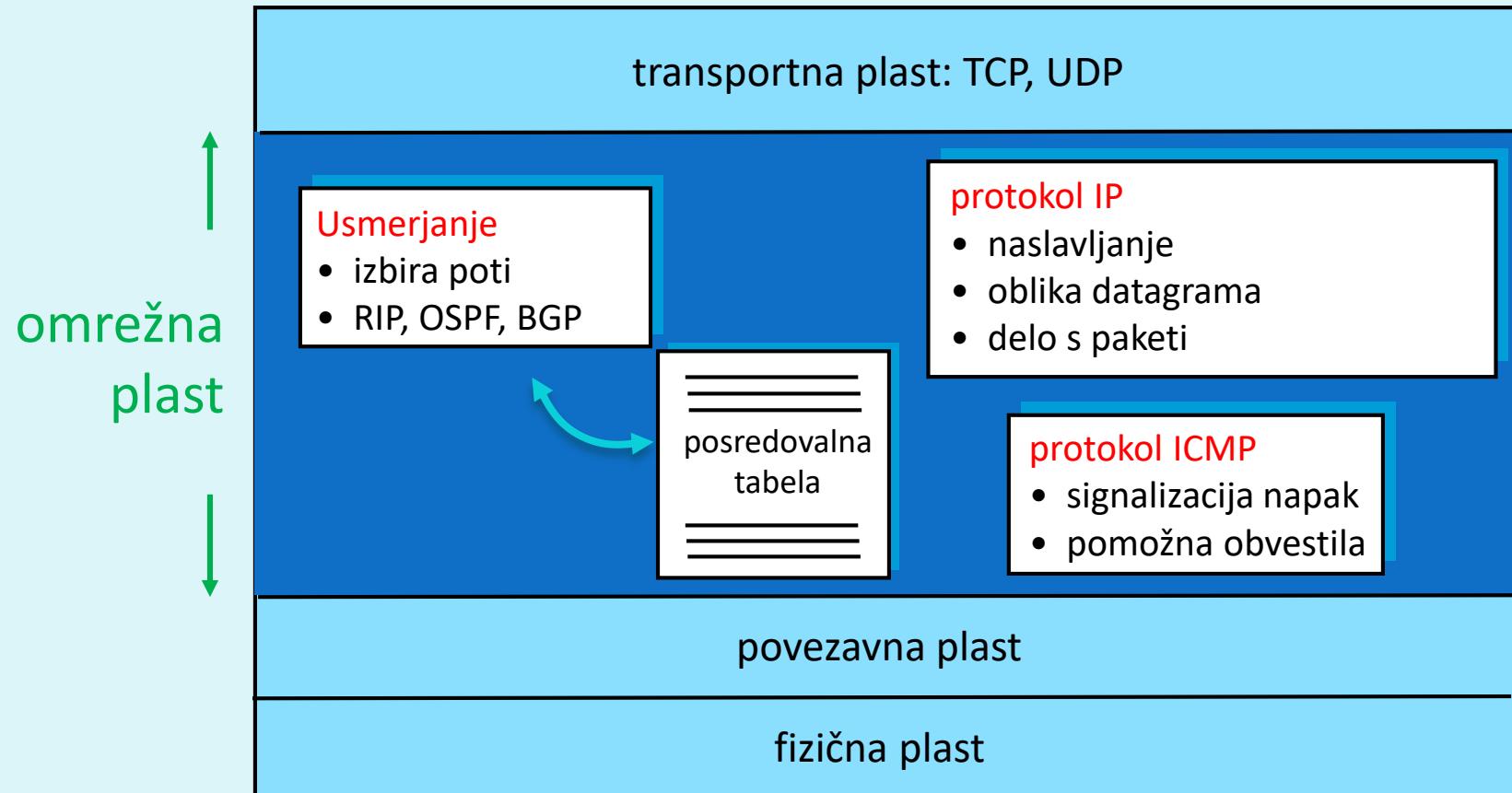
Primerjava obeh tipov omrežij

Internet (datagramsko)	ATM (VC omrežje)
usmerjanje glede na ciljni naslov	usmerjanje glede na ID voda
komunikacija med računalniki : zato so dovoljene elastične storitve, kjer čas ni tako pomemben	izvira iz telefonije : zakasnitev in zanesljivost sta pomembna
težka zagotovila kakovosti	preprosta zagotovila kakovosti
<ul style="list-style-type: none">• končni sistemi so "pametni", znajo sami popravljati napake in izvajati manjkajoče storitve• omrežje je preprosto	<ul style="list-style-type: none">• končni sistemi so "neumni"• omrežje je kompleksno, saj mora zagotavljati storitve kakovosti
preprosto dodajanje novih storitev (aplikacij) in povezovanje heterogenih omrežij	težje dodajanje novih storitev, pogojeno z infrastrukturo omrežja

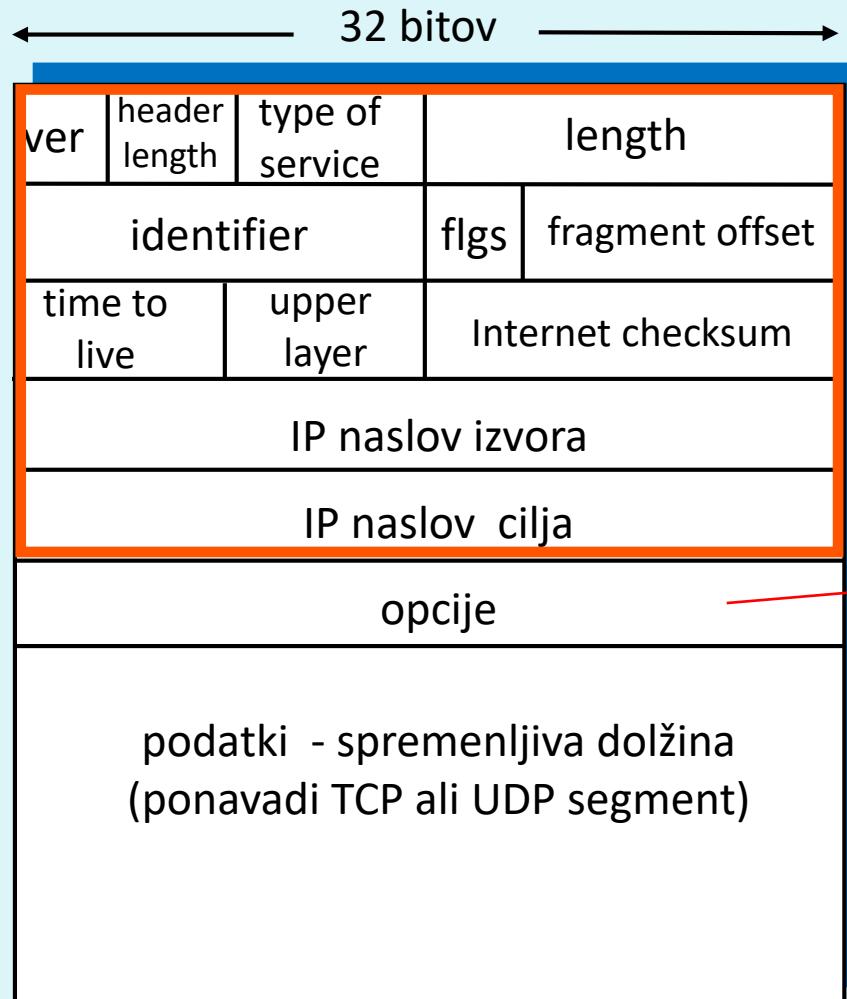
Internet Protocol (IP)



Funkcije omrežne plasti

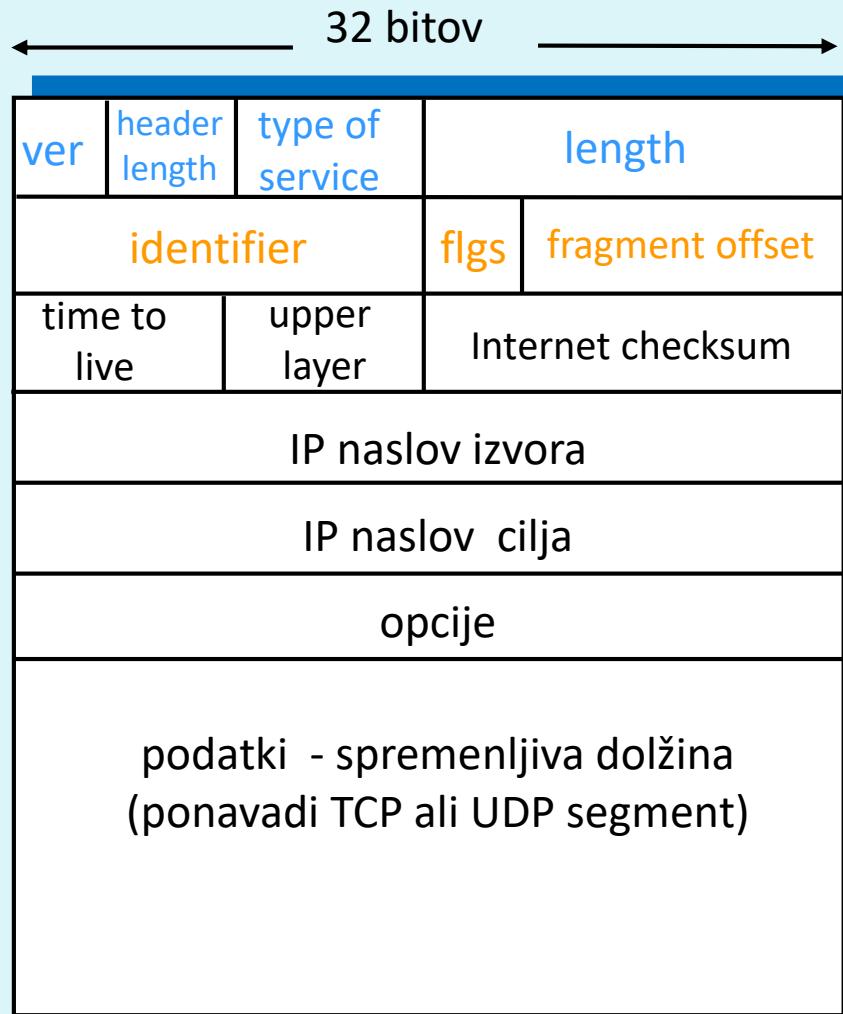


IP protokol: format paketa IPv4



- **VER (4b)**: verzija IP protokola
- **HEADER LENGTH (4b)**: dolžina glave (v 32-bitnih besedah), poda, kje se začnejo podatki (ponavadi 5×32 bitov)
- **TYPE OF SERVICE (8b)**: za razlikovanje datagramov, ki potrebujejo "posebno" obravnavo
- **LENGTH (16b)**: skupna dolžina celega datagrama v Byte-ih (običajno dolžina 1500B)
- **ID, FLAGS, OFFSET (32b)**: potrebno za IP fragmentacijo (razbitje podatkov na več delov)

IP protokol: format paketa IPv4

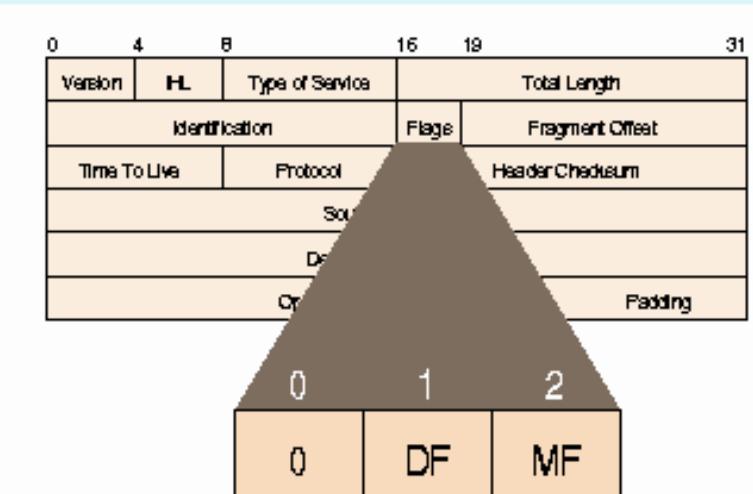
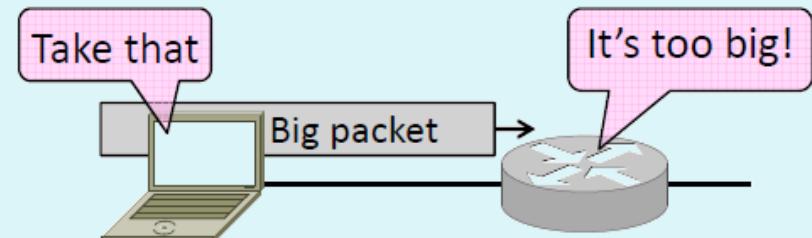


- **TTL (8b)**: za preprečitev ciklanja datagramov po omrežju, vsak usmerjevalnik zmanjša vrednost za 1
- **UPPER LAYER (PROTOCOL) (8b)**: številka enkapsuliranega protokola v podatkih (6-TCP, 17-UDP)
- **CHECKSUM (16b)**: kontrolna vsota (samo) glave datagrama, preračuna jo vsak usmerjevalnik
- **IP naslovi (32b)**: naslovi izvora in cilja (začetnega in končnega sistema)
- **OPCIJE (32b)**: za možne razširitve glave datagrama (slabosti: večji čas procesiranja, neznana lokacija začetka podatkov; običajno jih ni, glava dolga 20B)
- **PODATKI (spremenljiva dolžina)**

Fragmentacija

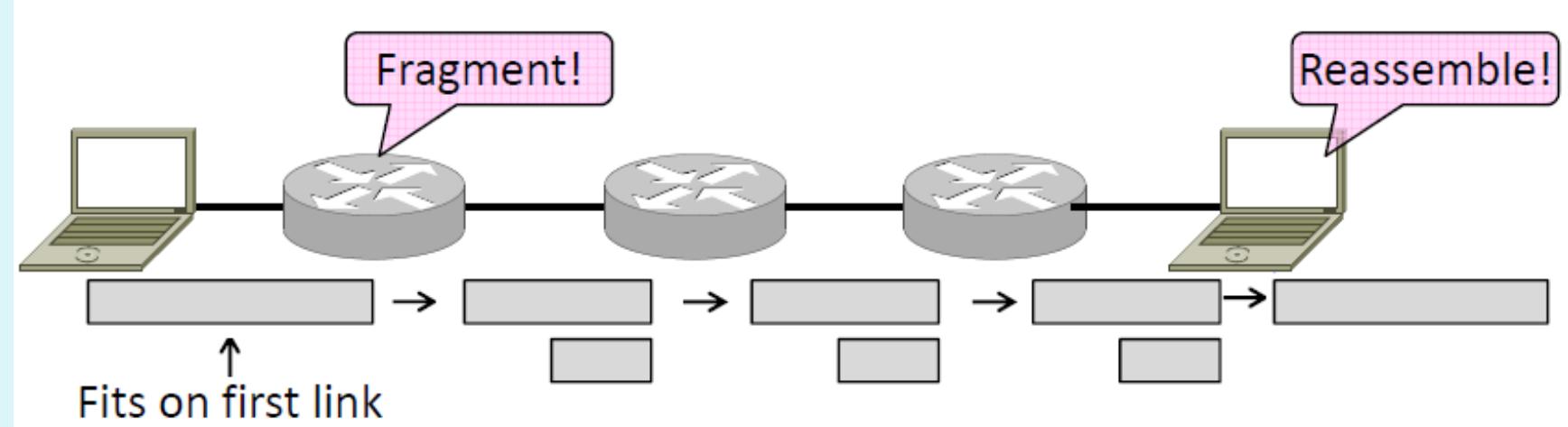
- **ZAKAJ?** IP datagrami se morajo enkapsulirati v okvirje povezavne plasti, ti pa imajo omejeno dolžino (MTU, maximum transmission unit, Ethernet: do 1500B, 802.11: 7981B)
- **FRAGMENTACIJA:** (pre)velik paket IP se razbije na več manjših
- **KAKO?** Polja ID, FLAGS, OFFSET se uporabljajo za fragmentacijo

- bita v zastavicah (FLAGS):
 - DF: don't fragment
 - MF: more fragments



Fragmentacija

- Opombe:
 - v omrežju je lahko več tehnologij, zato se lahko MTU med potjo spreminja. Fragmentacijo lahko izvede tudi usmerjevalnik sredi poti.
 - fragmente združi šele omrežna plast prejemnika pred predajo transportni plasti

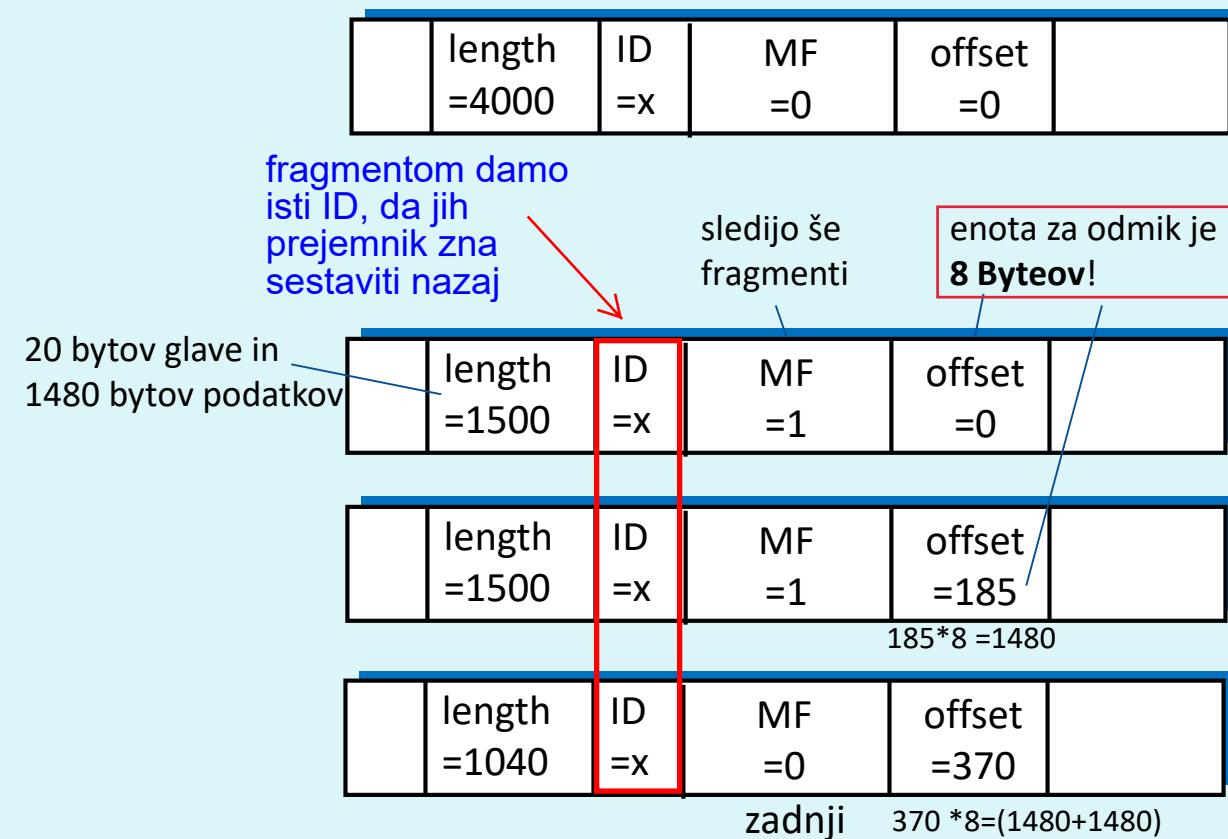
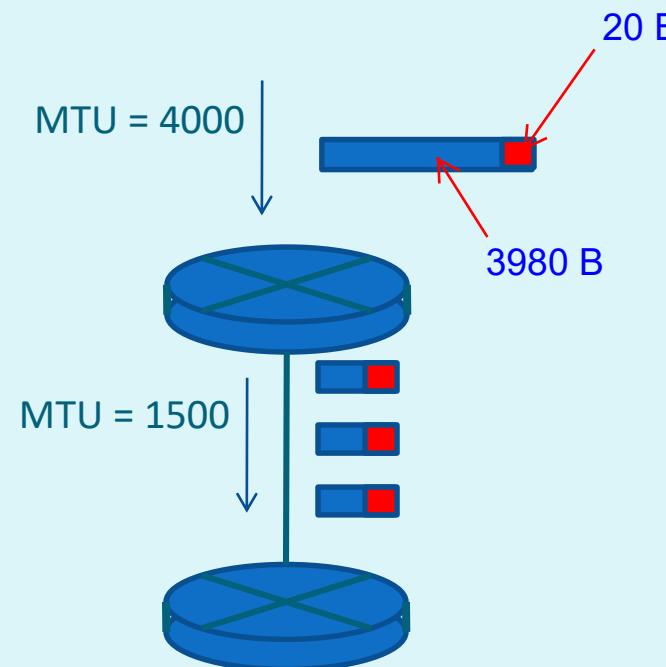


Fragmentacija: primer

- imamo paket dolžine 4000B (torej 20 glava + **3980 podatki**), MTU pa je 1500B
- pri MTU 1500B pomeni, da je 20B glave in **1480B podatkov**
- velikosti podatkov v fragmentih bodo: **1480B + 1480B + 1020B = 3980B**

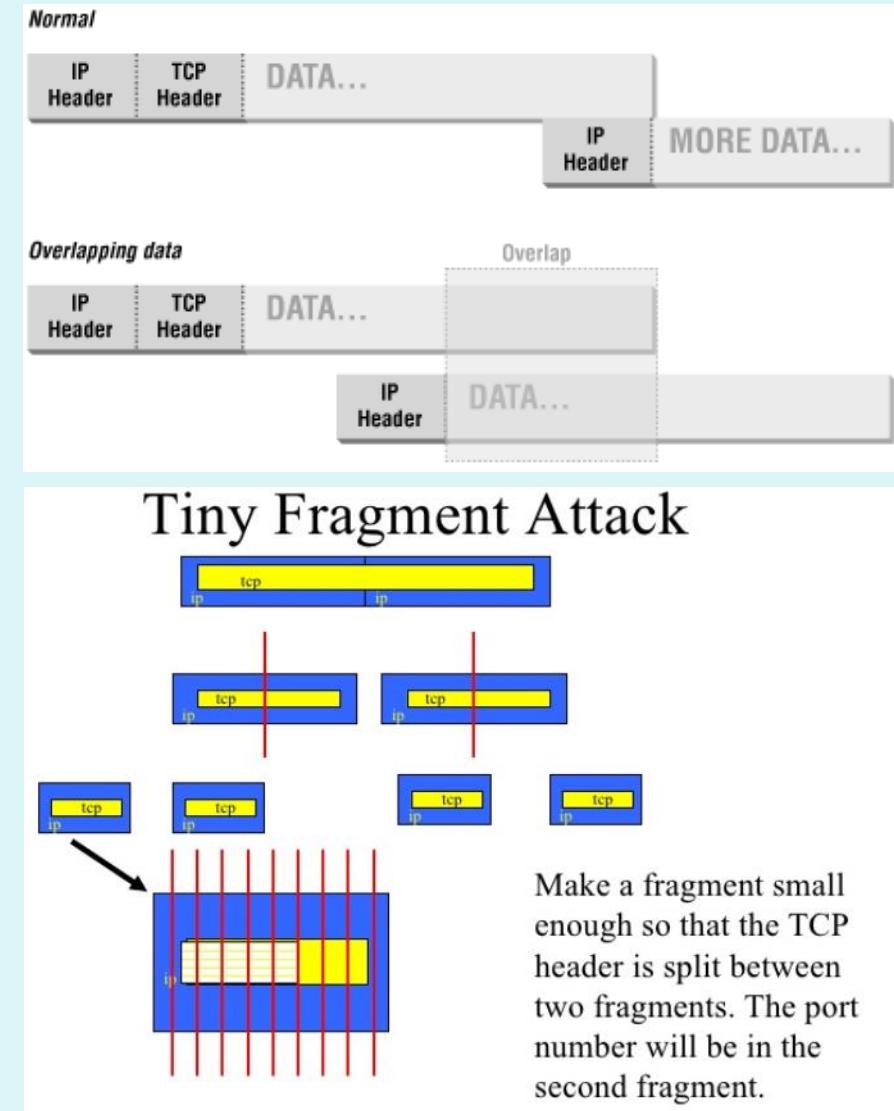
(opcij ne uporabljamo, zato je glava velika 20 B)

v primeru, ko ne dobimo celih št. (npr. $1490 / 8 = 185,125$), vedno zaokrožimo navzgor, da ne odsekamo informacij



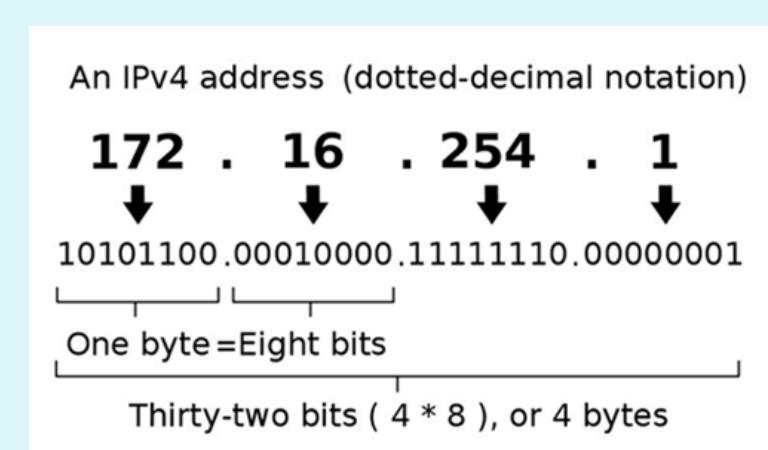
Napadi z uporabo fragmentacije

- obstajajo različni napadi, ki fragmentacijo izkoriščajo, da onemogočijo delovanje omrežnih sistemov (DoS)
 - *overlapping fragment attack*: napadalec fragmentira pakete z namerno napačnimi odmiki/dolžinami (prekrivanje). Pri sestavljanju se ciljni sistem lahko zmede in sesuje (napaka v kodi TCP/IP sklada)
 - *tiny fragment attack*: s fragmentacijo napadalec podatke razkosa tako, da fragmentira tudi podatke v glavi enkapsuliranega protokola. Na ta način ni možno izvesti varnostnega filtriranja po podatkih v glavi.



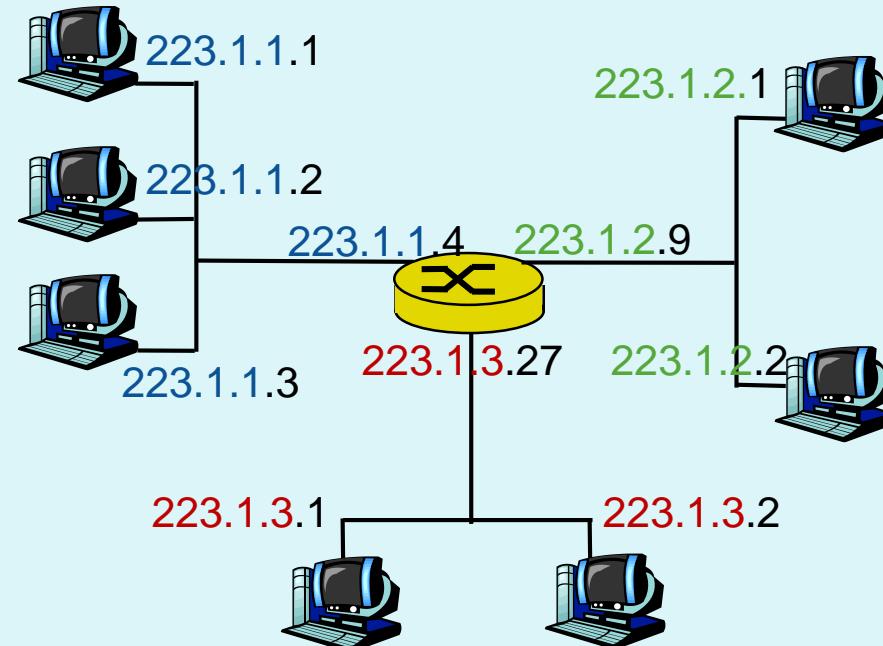
IPv4 nasavljanje

- vmesniki imajo IP (v4) naslove, ki so dolžina 32 bitov
- računalniki imajo običajno en vmesnik, usmerjevalniki več
- primer IPv4 naslova: 11011111 00000001 00000001 00000001
desetiški zapis: 223.1.1.1
- ker je naslov 32-biten, je obstaja cca. 4 milijarde IP naslovov
- naslovi naprav na Internetu morajo biti *globalno* unikatni



Podomrežje

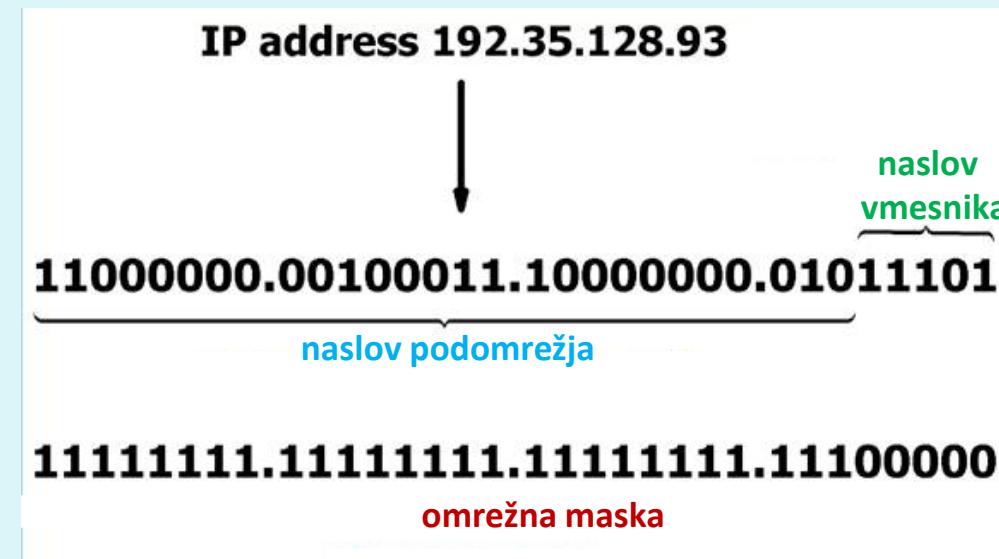
- IP naslove organiziramo v podomrežja (*subnet*), predpona predstavlja naslov podomrežja
- IP naslovi so smiselno hierarhično organizirani tako, da imajo "lokacijsko sorodne" naprave "podobne" IP naslove
 - analogija: naslovi hiš v isti ulici so podobni



Podomrežje

- **2 dela IP naslova:** naslov omrežja | naslov naprave
- **(Pod)omrežje** je množica vmesnikov, ki imajo enak naslov omrežja, ti vmesniki so medseboj dosegljivi brez posredovanja usmerjevalnika
- **Maska podomrežja** določa dolžino naslova podomrežja (je 32-bitni niz, ki ima enice na mestih, ki označujejo naslov omrežja, na ostalih pa ničle). Okrajšamo jo lahko s številom najbolj pomembnih bitov, npr.: "/25". Primer maske: **11111111 11111111 11111111 10000000** ali **255.255.255.128**

25 enic



Naslavljjanje IPv4

- v Internetu uporabljamo 32-bitne naslove pošiljateljev in prejemnikov (naslov IPv4)
- primer naslova IPv4, binarni in desetiški zapis:

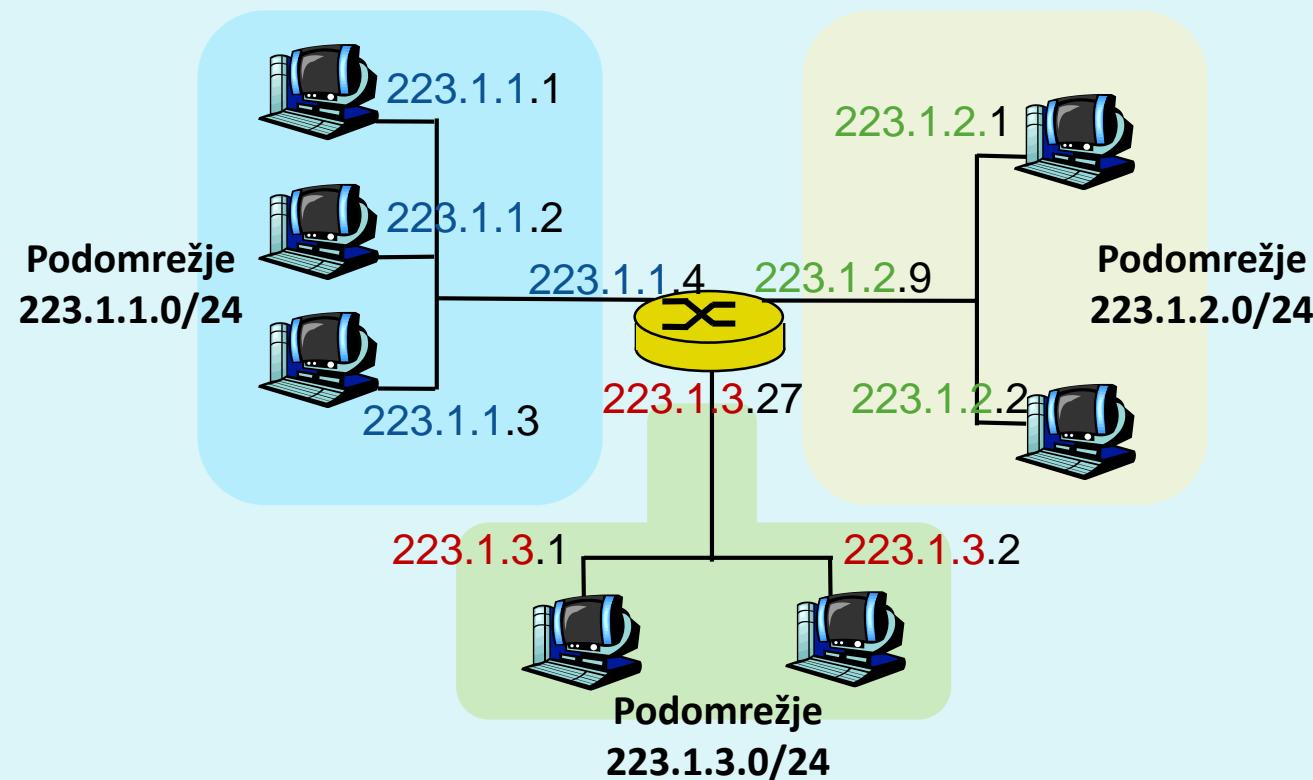
00010010	00011111	10010110	00111110			
18	.	31	.	150	.	62

- naslovi so razdeljeni v predpono (naslov omrežja) in naslov vmesnika
- primer: 20-bitna predpona

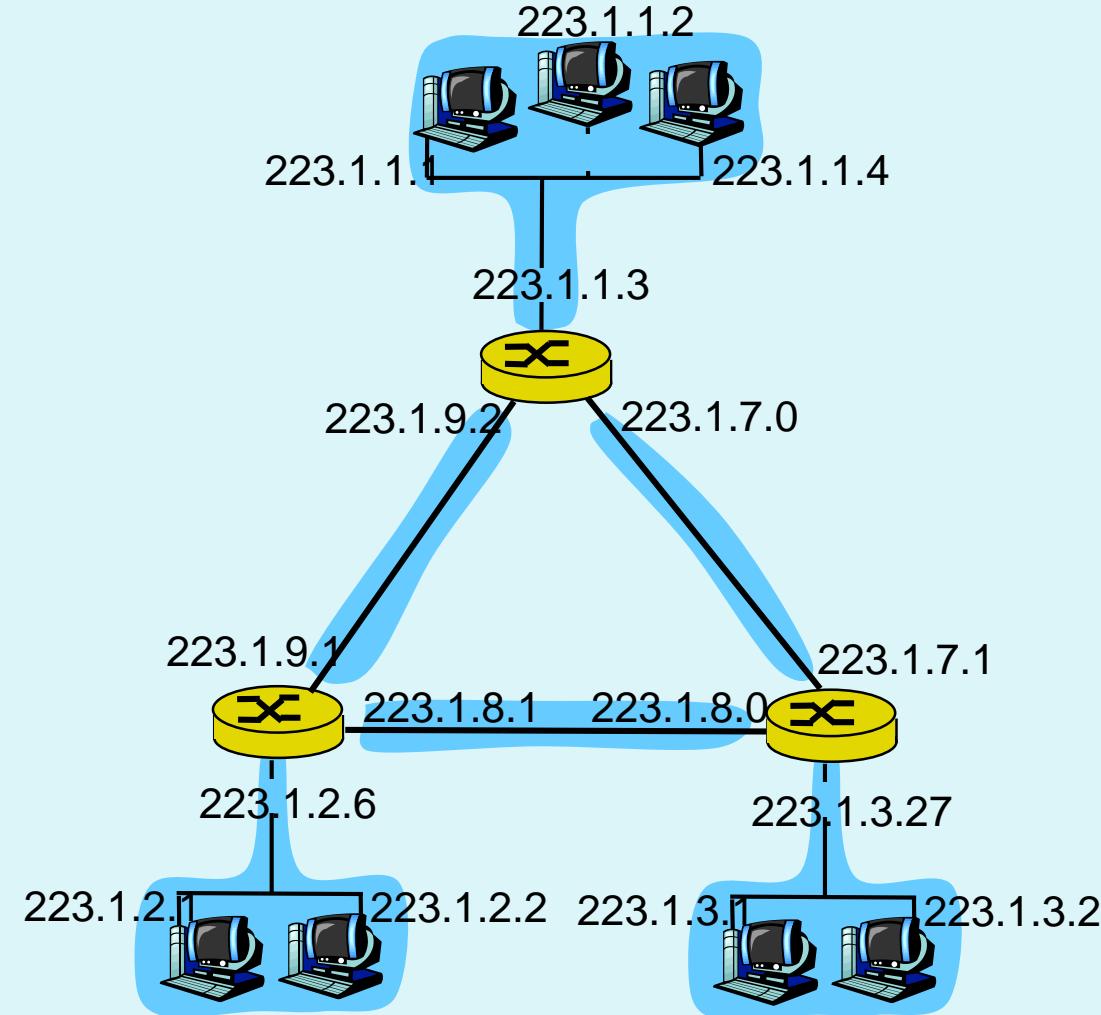
naslov:	00010010	00011111	10010110	00111110			
omrežna maska:	11111111	11111111	11110000	00000000			
	255	.	255	.	240	.	0
naslov omrežja:	00010010	00011111	10010000	00000000			
	18	.	31	.	144	.	0
zapis naslova:	18.31.150.62 / 20						
ali:	naslov 18.31.150.62, omrežna maska 255.255.240.0						

Podomrežje: primer naslavljanja

- usmerjevalnik ima na vsakem vmesniku **drugo podomrežje**
- znotraj (pod)omrežja ni usmerjevalnikov, so pa lahko stikala (switch) in zvezdišča/razdelilniki (hub)

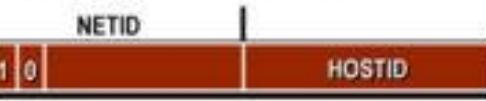


Primer: koliko podomrežij imamo?



Delitev na podomrežja

- sprva definirajo razrede (class) omrežij, ki uporabljajo maske iz 8, 16 ali 24 bitov:

Class	First Octet Range	Max Hosts	Format
A	1-126	16M	
B	128-191	64K	
C	192-223	254	

(fiksna delitev)

nesmotrna raba (premalo ali preveč)
naslovov, neuporabljeni iz razreda B
ostanejo globalno neizkoriščeni

A: 3 okteti x 8 bitov >> 2^24 naprav
B: 2 okteta x 8 bitov >> 2^{16} naprav
C: 1 oktet x 8 bitov >> 2^8 naprav

-
- kasneje se vpelje **prefiksna ali CIDR notacija** (Classless Inter-Domain Routing), ki omogoča dodelitev poljubnega števila bitov maski /sajdr/
 - "poseben" IP naslov je *broadcast* naslov, ki naslovi vse naprave na podomrežju (naslov naprave je sestavljen iz samih enic, npr. 233.1.1.255 ali 255.255.255.255)

Kako določimo IP naslove?

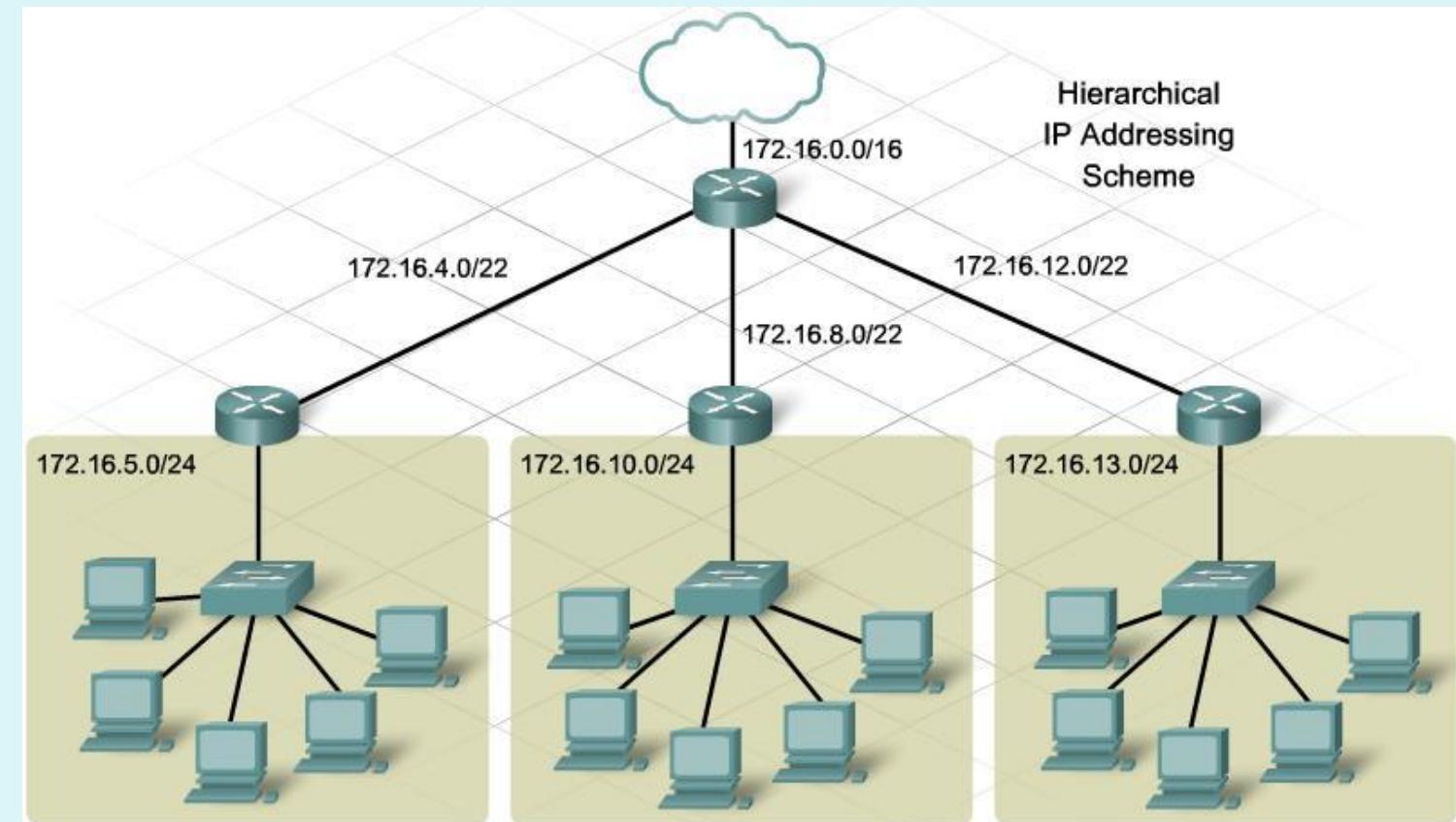
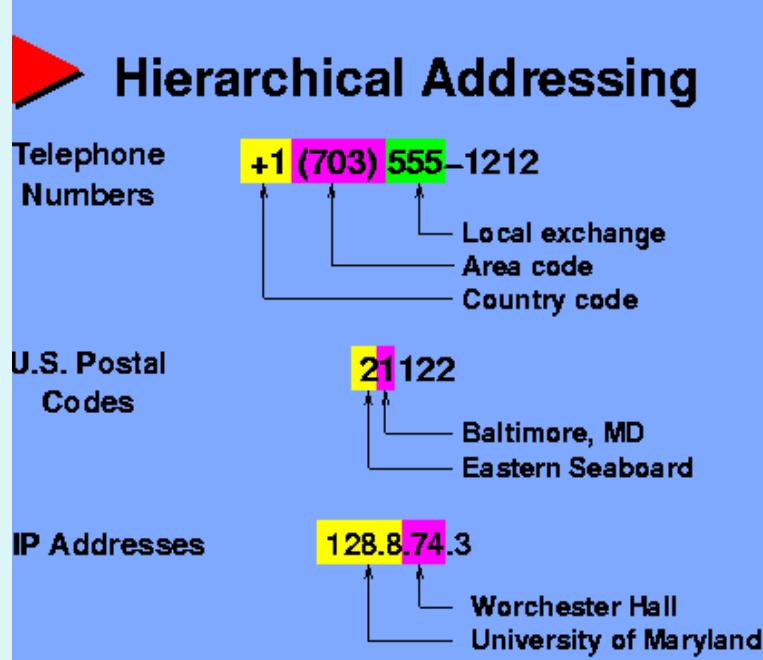
- **Naprava:**
 - administrator vpiše naslov (fiksen) ali
 - DHCP (*Dynamic Host Configuration Protocol*) strežnik dodeli naslov (dinamičen)
- **Omrežje podjetja:**
 - Ponudnik dostopa do interneta (ISP) dodeli del svojega naslovnega prostora.

ISP-jev blok:	11001000 00010111 00010000 00000000	200.23.16.0/20	
Podjetje1:	11001000 00010111 0001 000 0 00000000	200.23.16.0/23	maska se podaljša za 3 bite
Podjetje2:	11001000 00010111 0001 001 0 00000000	200.23.18.0/23	
...	

8 podjetjem želimo dodeliti naslovni prostor,
zato uporabimo 3 bite

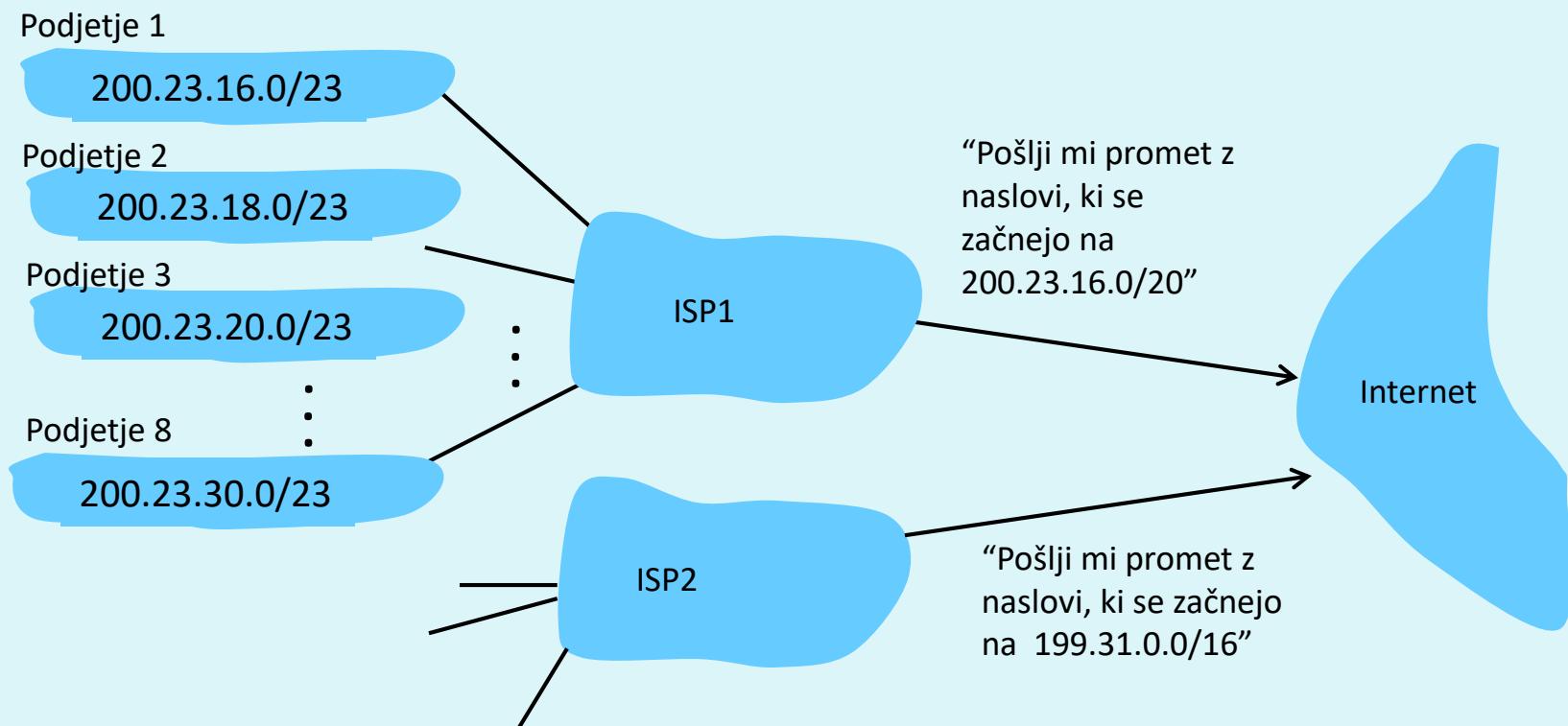
- **Ponudnik interneta (ISP):**
 - dodeli mu ga ICANN (Internet Corporation for Assigned Names and Numbers), neprofitna namenska organizacija, ki vzdržuje tudi korenske DNS strežnike

Hierarhična organizacija naslovov IP



Primer hierarhičnega naslavljanja

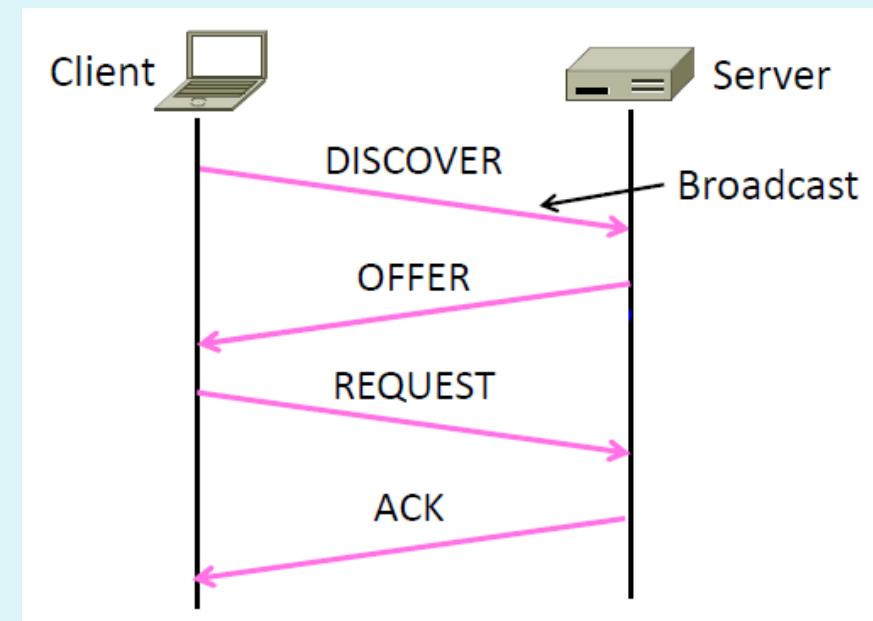
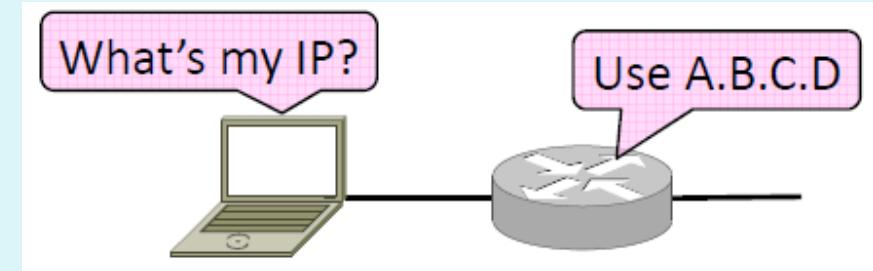
- pravilno dodeljevanje CIDR naslovov olajša usmerjanje: z eno omrežno predpono lahko usmerjamo v več omrežij naenkrat



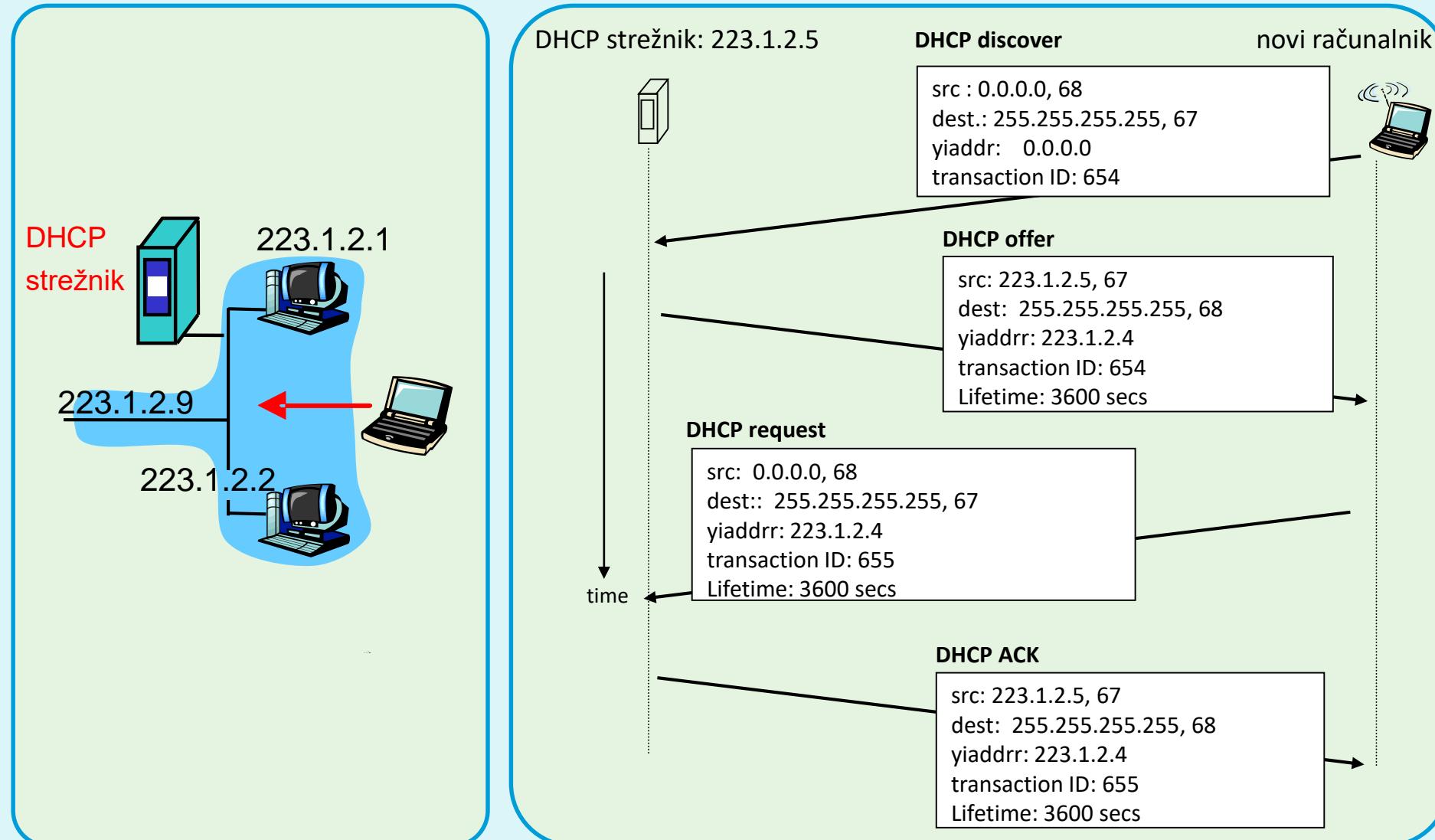
200.23.16.0 = 11001000 00010111 00010000 00000000

Dinamično dodeljevanje: DHCP

- ob priklopu naprava nima naslova IP, potrebna dodelitev osnovnih omrežnih nastavitev
- protokol DHCP (Dynamic Host Configuration Protocol)
- DHCP strežnik dodeli naslov v 4 fazah:
 - DISCOVER
 - OFFER
 - REQUEST
 - ACK



Dinamično dodeljevanje: DHCP strežnik



NAT (*Network Address Translation*)

- NAT: preslikovanje IP naslovov (pre-naslavljanje) se uvede zaradi pomanjkanja IPv4 naslovnega prostora
- namesto, da "trošimo" unikatne javne (**globalne**) naslove, uporabljajmo raje **lokalne naslove**, ki so lahko ponovljivi med različnimi podjetji (ne nastopajo v javnem internetu)
- zasebni naslovni prostor

Naslovi	Omrežje/maska	Št. naslovov
10.0.0.0 - 10.255.255.255	10.0.0.0/8	2^{24}
172.16.0.0 - 172.31.255.255	172.16.0.0/12	2^{20}
192.168.0.0 - 192.168.255.255	192.168.0.0/16	2^{16}

- usmerjevalnik uporabi NAT, da lokalni naslov preslika v globalni

NAT: primer delovanja

2: NAT usmerjevalnik spremeni naslov izvora 10.0.0.1, 3345 v 138.76.29.7, 5001, In to vstavi v tabelo

NAT preslikovalna tabela: IP, port	
Naslovi WAN strani	Zasebni naslovi
138.76.29.7, 5001	10.0.0.1, 3345
.....

1: rač. 10.0.0.1 pošlje datagram na 128.119.40, 80

2: NAT usmerjevalnik spremeni naslov izvora 10.0.0.1, 3345 v 138.76.29.7, 5001, In to vstavi v tabelo

3: Odgovor s ciljnim naslovom 138.76.29.7, 5001

S: 10.0.0.1, 3345
D: 128.119.40.186, 80

10.0.0.4

S: 128.119.40.186, 80
D: 10.0.0.1, 3345

4: NAT usmerjevalnik spremeni naslov cilja v 10.0.0.1, 3345

10.0.0.1

10.0.0.2

10.0.0.3

S: 128.119.40.186, 80
D: 138.76.29.7, 5001

138.76.29.7

3

1

4

Prednosti in slabosti pristopa NAT

PREDNOSTI

- zadošča samo 1 javni naslov za dostop celega omrežja do Interneta
- naslove notranjih naprav in ponudnika interneta (!) lahko **spreminjamamo neodvisno** od zunanjega naslova
- večja **varnost** notranjih naprav, ker niso javno dostopne
- 16-bitno polje za vrata (port) omogoča evidentiranje cca. 60.000 povezav do notranjih naprav

KRITIKA

- usmerjevalniki **naj bi delali na 3. plasti** (torej ne bi imeli opravka z vrati - ki so del 4. plasti!)
- vrata (porti) so namenjeni **naslavljjanju procesov**, ne računalnikov
- krši **princip končnih sistemov** (*end-to-end argument*), ki zahteva, da je za aplikacije omrežje transparentno; težavo imamo pri P2P aplikacijah, do katerih znotraj NATa ni možno dostopiti.
- za reševanje pomanjkanja naslovov je **bolje uporabiti IPv6!**

Naslednjič gremo naprej!

- omrežna plast:
 - ICMP
 - IPv6
 - (IPSec)
 - usmerjevalni protokoli

