Računalniške komunikacije

Omrežna plast

Jurij Mihelič, UniLj, PeF

Vsebina

Plast	Podatkovna enota	Opis
aplikacijska	sporočilo	Visoko nivojski API.
predstavitvena		Predstavitev podatkov, kompresija, enkripcija/dekripcija.
sejna		Upravljanje sej (dvosmerna izmenjava informacij).
transportna	segment	Povezave med vozlišči, zanesljivost.
omrežna	datagram	Prenos med več vozlišči v omrežju, logično naslavljanje.
povezavna	okvir	Prenos okvirjev med dvema omrežnima napravama, povezanima s fizično plastjo, fizično naslavljanje.
fizična	bit	Prenos toka bitov po prenosnem mediju.

Vsebina

- Omrežna plast
  - namen storitve
  - povezavna in nepovezavna omrežja
- Usmerjevalnik
  - posredovanje in usmerjanje
- Posredovanje
- Usmerjanje

Omrežna plast

- Namen
  - dostava paketov
    - od *pošiljatelja* preko *omrežja* do *prejemnika*
    - preko omrežja pomeni preko ostalih vozlišč
- Storitve
  - enkapsulacija segementov transportne plasti
  - dekapsulacija paketov v segmente

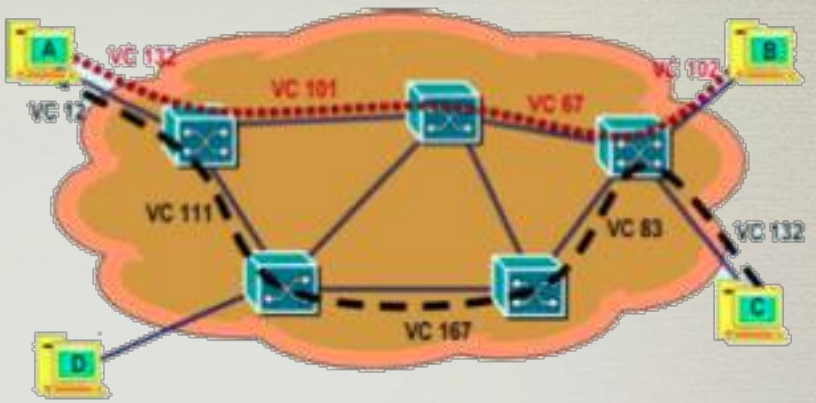
Omrežna plast

- Potencialne storitve
  - zagotovljena dostava paketov
  - dostava paketov v zagotovljenem času
  - dostava paketov v pravem zaporedju
  - zagotovljena spodnja meja pasovne širine
  - največja dovoljena varianca zakasnitve
  - varna komunikacija
    - zaupnost, integriteta, avtentikacija

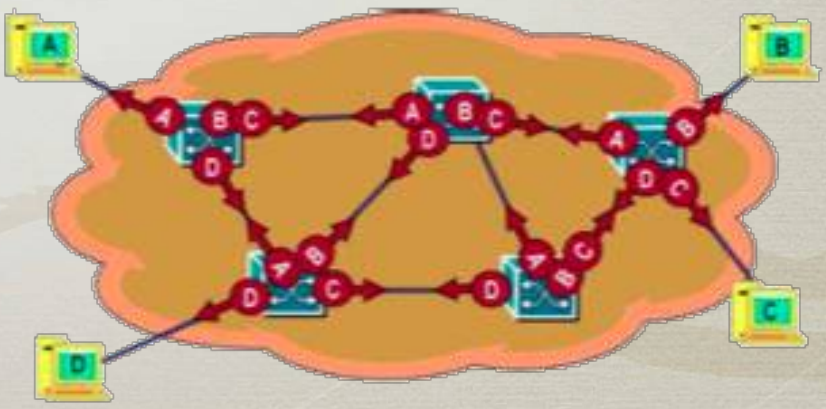
Kaj od naštetega zagotavlja Internet? (best-effort service)

Omrežna plast

- Povezavna omrežja (navidezni vodi)
  - najprej se vzpostavi fiksna zveza v omrežju
  - nato sledi prenos podatkov



- Nepovezavna omrežja (datagramska, paketna)
  - posredovanje podatkov v obliki paketov skozi omrežje
  - brez vnaprej vzpostavljene zveze



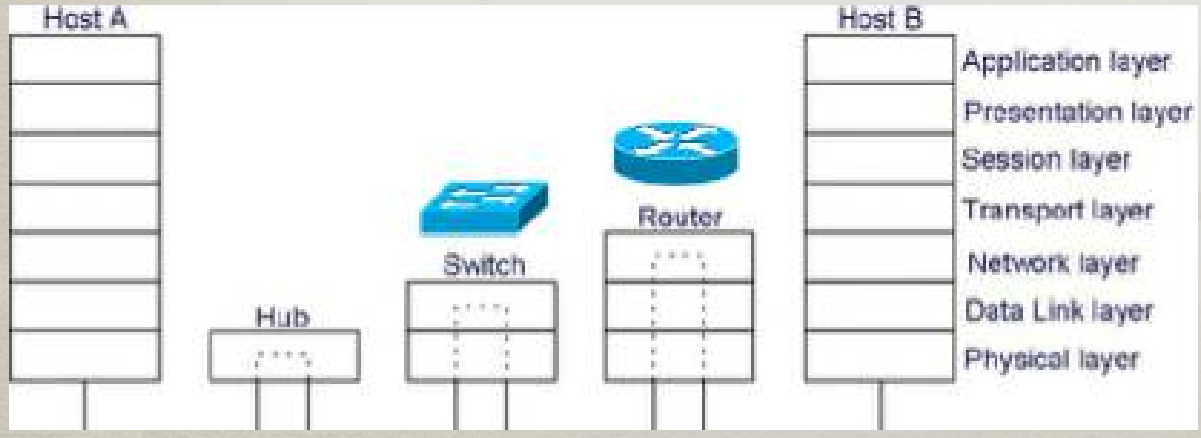
Omrežna plast

- Primerjava obeh vrst omrežij

	povezavno omrežje	**nepovezavno omrežje**
osnovni namen	klasična telefonija	računalniška komunikacija
pretok podatkov	vodi	paketi
posredovanje	glede na št. voda	glede na ciljni naslov paketa
zagotavljanje kakovosti	zakasnitev in zanesljivost sta pomembna	elastične storitve, čas ni tako pomemben
omrežje	zahtevno: zagotavlja kakovost	preprosto: le posredovanje paketov
končni sistemi	preprosti	zahtevni: sami zagotavljajo kakovost storitve
razširljivost	težko dodajanje novih storitev, pogojeno z infrastrukturo omrežja	preprosto dodajanje novih storitev in povezovanje heterogenih omrežij

Usmerjevalnik

- Naprava omrežne plasti
  - transport datagrama po jedru omrežja
  - funkciji usmerjevalnika
    - **posredovanje** paketov
    - **usmerjanje** paketov



Usmerjevalnik

- Posredovanje (forwarding)
  - poteka znotraj posameznega usmerjevalnika
  - prenos paketa iz vhodnega v izhodni vmesnik
  - posredovalna tabela (forwarding table)
    - določa izhodni vmesnik, kamor je potrebno poslati paket
  - analogija: določite točke vstopa in izstopa za posamezen kraj na poti

Usmerjevalnik

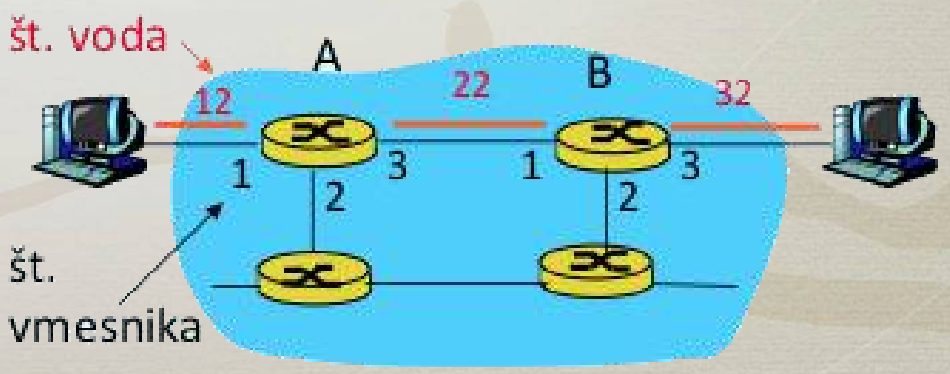
- Usmerjanje (routing)
  - kolektivno delo vseh usmerjevalnikov na poti
  - izvaja usmerjevalni algoritem (porazdeljeni)
  - analogija: planiranje pot iz Kopra do Lendave

Posredovanje

- Povezavna omrežja
  - navidezni vod / zveza / povezava
    - fiksna pot od izvora do cilja ustvarjena za čas komunikacije
    - **številka voda** – namenjena za posredovanje
  - faze izvedbe
    - vzpostavitev povezave, prenos podatkov, rušenje povezave
    - spreminjanje posredovalnih tabel v vseh usmerjevalnikih navideznega voda

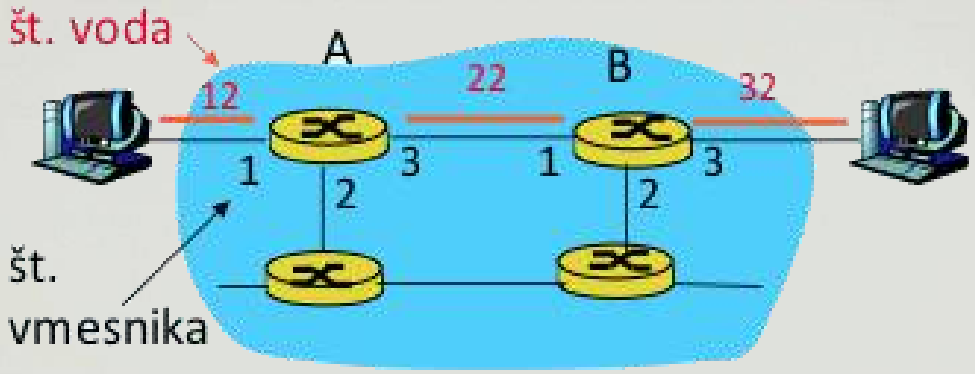
faze izvedbe

oddajnik	prejemnik
1. vzpostavi povezavo	2. dohodni klic
4. potrditev povezave	3. sprejmi klic
5. pošiljanje podatkov	6. sprejem podatkov
7. rušenje povezave	8. prekinitev povezave



Posredovanje

- Povezavna omrežja
  - številka voda je različna pri vhodnih in izhodnih vmesnikih usmerjevalnikov



stikalo A – posredovalna tabela

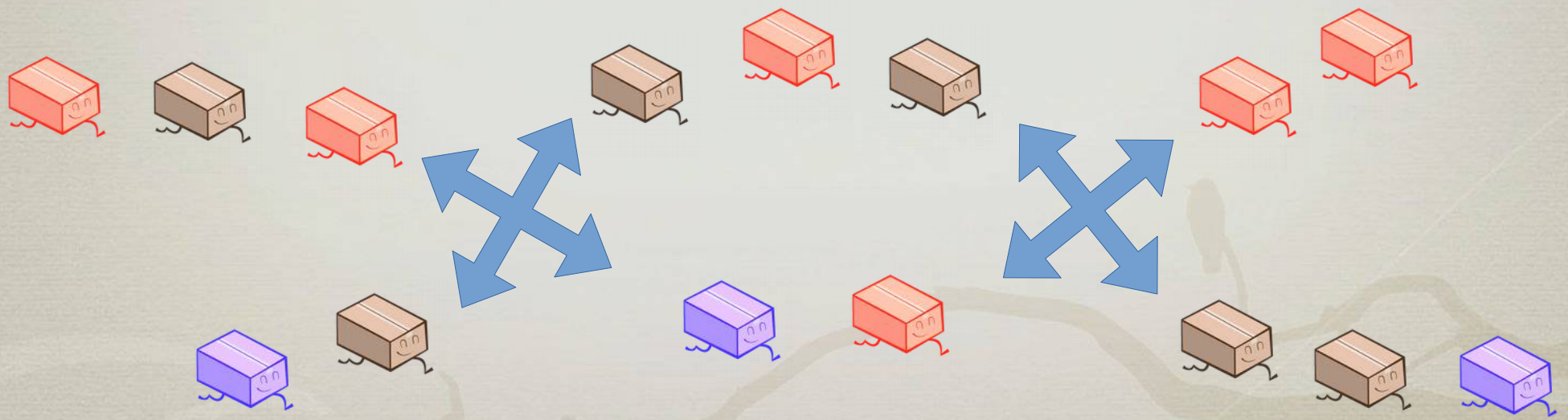
vhodni vmesnik	vhodna št. voda	izhodni vmesnik	izhodna št. voda
1	12	3	22
2	63	1	18
3	7	2	17
...	...	...	...

stikalo B – posredovalna tabela

vhodni vmesnik	vhodna št. voda	izhodni vmesnik	izhodna št. voda
1	22	3	32
1	34	2	23
2	4	1	55
...	...	...	...

Posredovanje

- Nepovezavna omrežja (datagramska, paketna)
  - paket vsebuje naslov cilja
  - usmerjevalniki posredujejo glede na naslov
  - paket lahko potuje po različnih poteh med istim izvorom in ciljem



Posredovanje

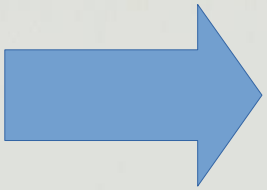
- Nepovezavna omrežja (datagramska, paketna)
  - težava: ogromne posredovalne tabele
    - hranjenje preslikav za vse možne naslove
  - rešitev: združevanje naslovov
    - naslove združimo v skupine glede na intervale
    - hranimo le intervale

ciljni naslov	izhodni vmesnik
od 0000 0000 do 0011 1111	0
od 1100 0000 do 1100 1111	1
od 1101 0000 do 1101 1111	2
od 1110 0000 do 1111 1111	3

Posredovanje

- Nepovezavna omrežja
  - ujemanje najdaljše predpone

ciljni naslov	izhodni vmesnik
od 0000 0000 do 0011 1111	0
od 1100 0000 do 1100 1111	1
od 1101 0000 do 1101 1111	2
od 1110 0000 do 1111 1111	3



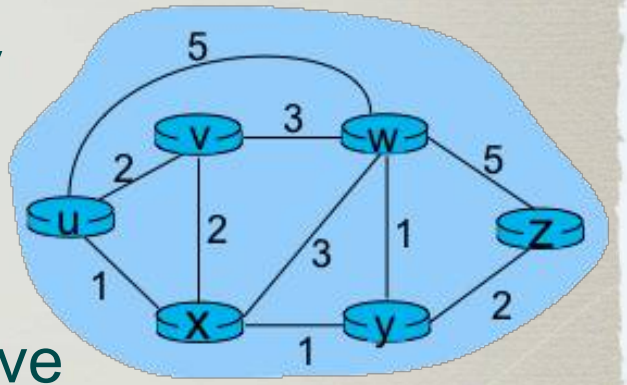
ciljni naslov	izhodni vmesnik
00	0
1100	1
1101	2
111	3

primeri

ciljni naslov	vmesnik
0001 0110	0
1110 0010	3
1100 0101	1
1101 0101	2

Usmerjanje

- Problem
  - po kateri poti naj paket potuje od izvora do cilja
    - končne naprave so priključene na usmerjevalnik
    - zanima nas pot od usmerjevalnika do usmerjevalnika
  - omrežja modeliramo s teorijo grafov
    - graf $G = (V,E)$
    - vozlišča V … usmerjevalniki
    - povezave E … komunikacijske povezave
    - cena povezave … cena prenosa paketa po povezavi
      - cena: razdalja, denar, hitrost, politika, …
    - navadno obstaja več poti med izvorom in ciljem

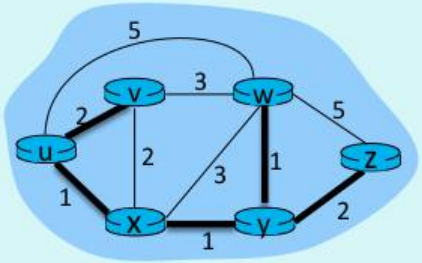


Usmerjanje

- Usmerjevalni protokol
  - konfigurira posredovalne table
  - usmerjevalni algoritem
    - iskanje čim cenejše poti od izvora do cilja
    - **centralizirani** (globalni, *link state* algoritmi)
      - ima podatke o celotnem omrežju
    - **porazdeljeni**
      - ima podatke samo o neposrednih povezavah (soseščina)
    - prilagodljivi in neprilagodljivi
      - prilagajajo cene povezav glede na njeno zasičenost

Usmerjanje

- Centralizirano usmerjanje
  - stanje povezav v celem omrežju
    - vsako vozlišče sporoča stanje povezav vsem ostalim
  - vsako vozlišče zase izračuna *najkrajše poti* do ostalih vozlišč
    - drevo najkrajših poti za dano vozlišče
      - Dijkstrov algoritem
    - osnova za izgradnjo posredovalne tabele

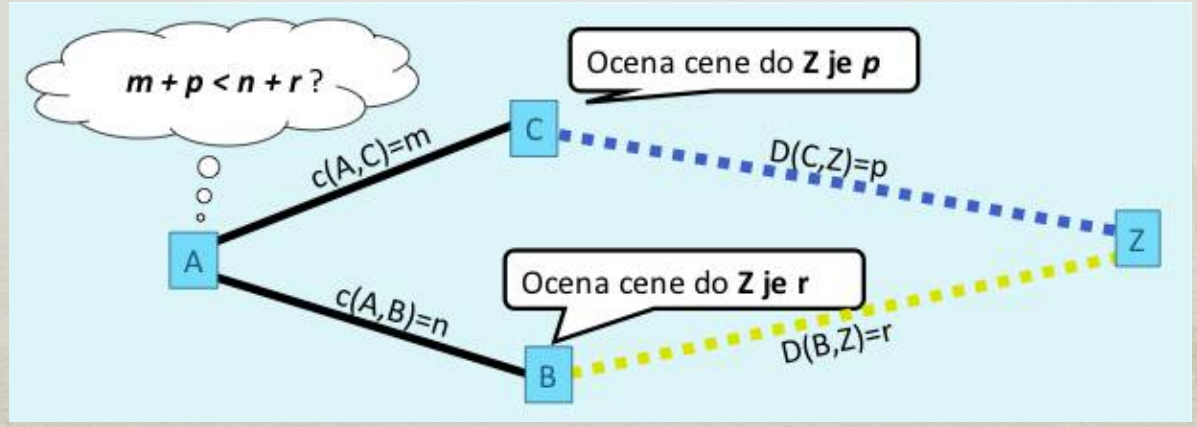


Izračunana posredovalna tabela **vozlišča u**

cilj	povezava/vrata	cena
v	(u,v)	2
x	(u,x)	1
y	(u,x)	2
w	(u,x)	3
z	(u,x)	4

Usmerjanje

- Porazdeljeno usmerjanje
  - uporaba le lokalnih podatkov, prejetih od sosedov
    - cena povezave do soseda
    - ocena cene najcenejše poti od soseda do cilja
  - algoritem poteka iterativno
    - posredovalne tabele sčasoma konvergirajo v najcenejše poti



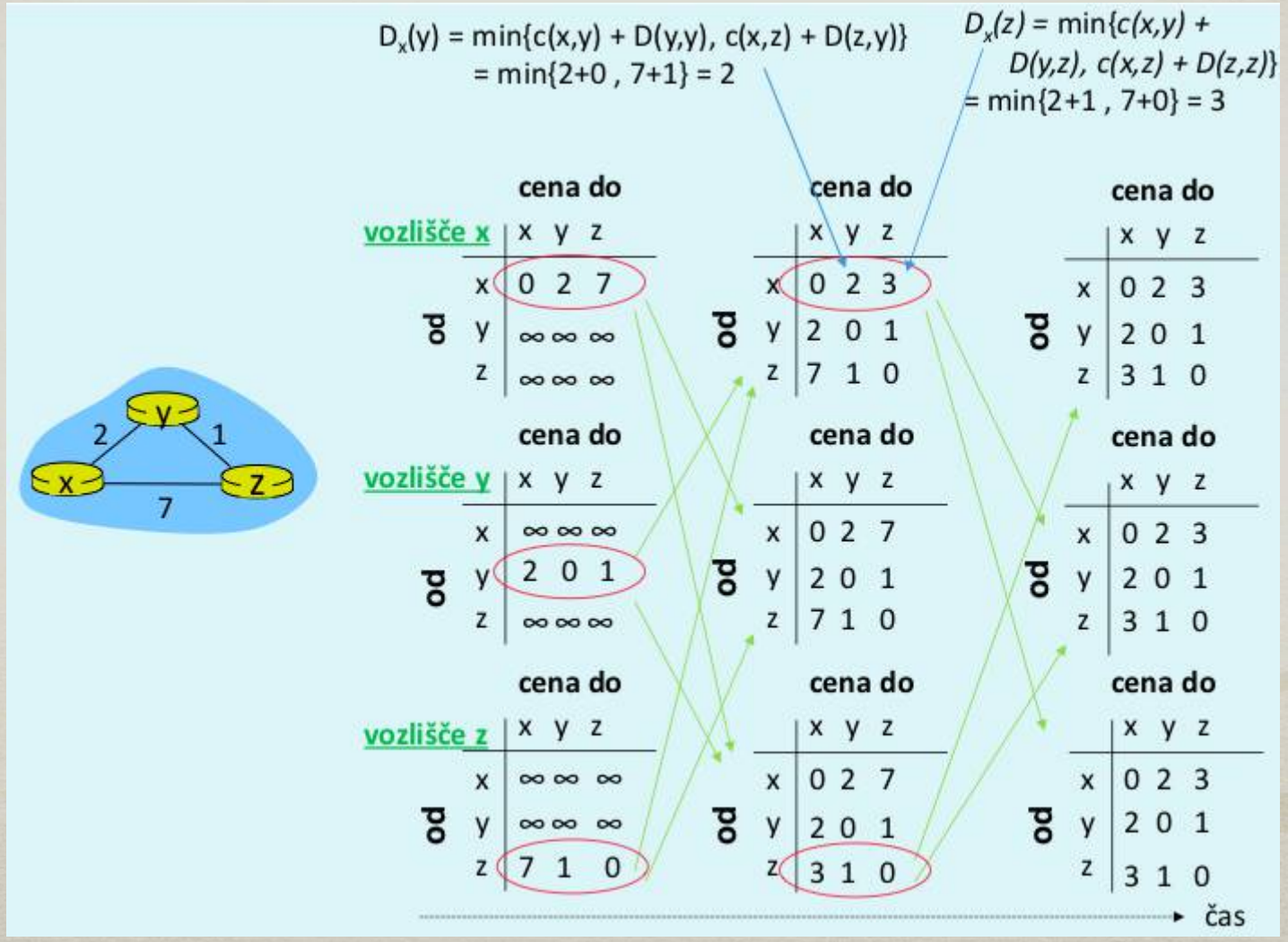
Usmerjanje

- Porazdeljeno usmerjanje – **vektor razdalj**
  - vektor razdalj = seznam razdalj do vseh vozlišč
  - vsako vozlišče hrani
    - svoj vektor razdalj
    - vektorje razdalj vseh svojih sosedov
    - posredovalno tabelo
  - ideja algoritma
    - ko vozlišče x prejme sosedov vektor razdalj $d(s,y)$, popravi svoj vektor razdalj $d(x,y)$

$$d(x,y) \leftarrow min_{s \in S} c(x,s) + d(s,y)$$

Usmerjanje

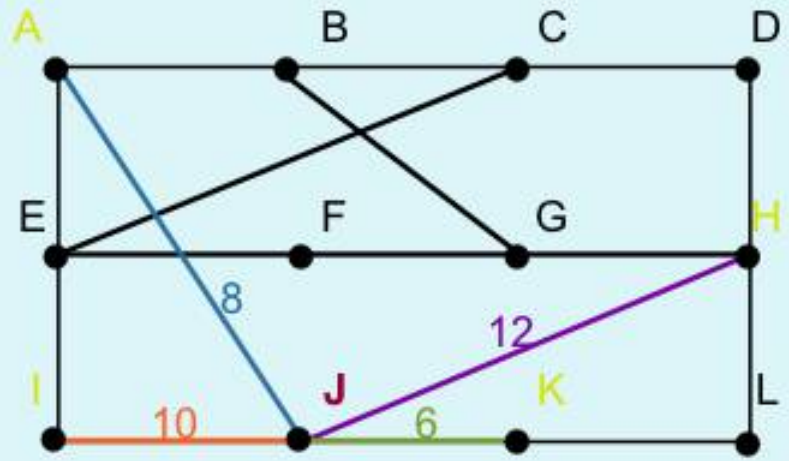
- Porazdeljeno usmerjanje – konvergenca posredovalne tabele



Usmerjanje

- Porazdeljeno usmerjanje – lokalno izvajanje usmerjevalnega algoritma

J dobi tabele od sosedov. Poišči njegovo novo posredovalno tabelo!



JA: 8 JH: 12

JI: 10 JK: 6

prejeti vektorji razdalj

Dobi od / Smer	A	I	H	K
A	-	24	20	21
B	12	36	31	28
C	25	18	19	26
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	-	19
I	21	-	14	22
J	9	11	7	10
K	24	22	22	-
L	29	33	9	9

nova posredovalna tabela

Smer	Ocena	Sosed
A	8	A
B	20	A
C	28	I
D	20	H
E	17	I
F	30	I
G	18	H
H	12	H
I	10	I
J	-	-
K	6	K
L	15	K

Usmerjanje

- Porazdeljeno usmerjanje – **hierarhično usmerjanje**
  - veliko usmerjevalnikov → velike usmerjevalne tabele
  - rešitev
    - usmerjevalniki organizirani v avtonomne sisteme (AS)
      - intra-AS usmerjevalni algoritem
        - vsak sistem uporablja isti usmerjevalni algoritem
        - različni sistemi lahko uporabljajo različne algoritme
      - inter-AS usmerjevalni algoritem
        - med sistemi se uporablja poseben usmerjevalni protokol
        - Interior Gateway Protocol

Usmerjanje

- Interior gateway protocols
  - RIP, routing information protocol
    - usmerjanje v vektorjem razdalj, optimizira št. skokov
    - vektor razdalje se pošilja na 30 s; če se ne pošlje v 180 s, se povezava smatra za prekinjeno
  - OSPF: open shortest path first
    - glede na staje povezav
    - poplavljanje, hierarhično usmerjanje
  - IGRP, interior gateway routing protocol
    - Ciscova izboljšava RIP
    - cena kot utežena vsota pasovne širine, zakasnitve, obrementive, MTU in zanesljivosti

Računalniške komunikacije

Omrežna plast Interneta

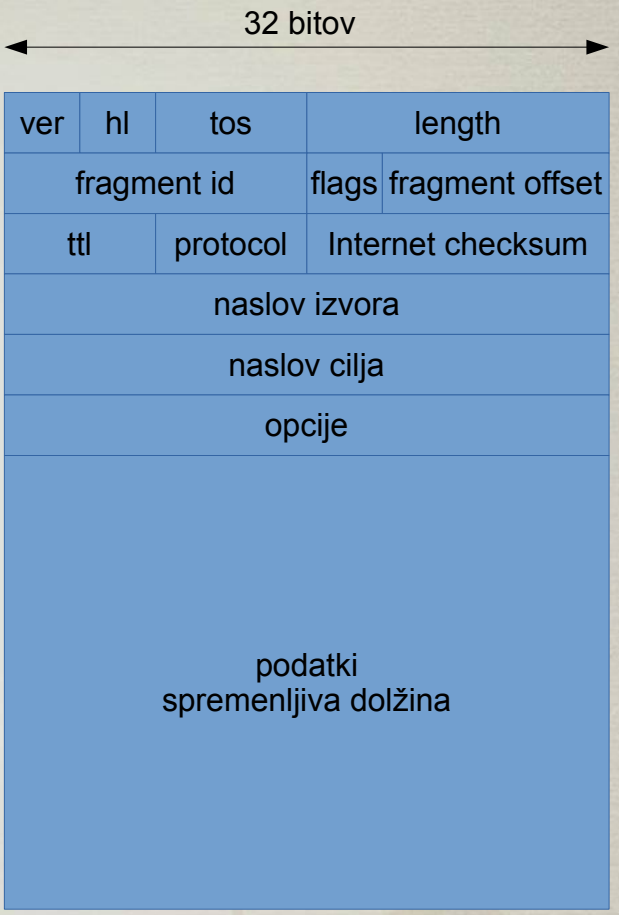
Jurij Mihelič, UniLj, PeF

Pregled vsebine

- IPv4
- IPv4 fragmentacija
- IPv4 naslavljanje
- DHCP
- NAT
- ICMP
- IPv6
- IPSec

IPv4

- Format paketa
  - **ver** (4b): verzija IP protokola, v4
  - **hl, header length** (4b): dolžina glave v 32-bitnih besedah, odmik podatkov
  - **tos, type of service** (8b): vrsta datagrama za posebno obravnavo
  - **length** (16b): dolžina celotnega paketa v bajtih
  - **fragment id, flags, offset** (32b): fragmentacija paketa
  - **ttl, time to live** (8b): preprečitev ciklanja v omrežju, vsak usmerjevalnik zmanjša vrednost za 1
  - **protocol** (8b): št. enkapsuliranega protokola, 6-tcp, 7-udp
  - **Internet checksum** (16b): kontrolna vsota glave datagrama
  - **naslov izvora in cilja** (32b): IP naslov
  - **opcije** (32b): morebitne razširitve, običajno jih ni, torej hl = 5 besed = 20 bajtov
  - **podatki**: npr. segment TCP oz. datagram IP protokola

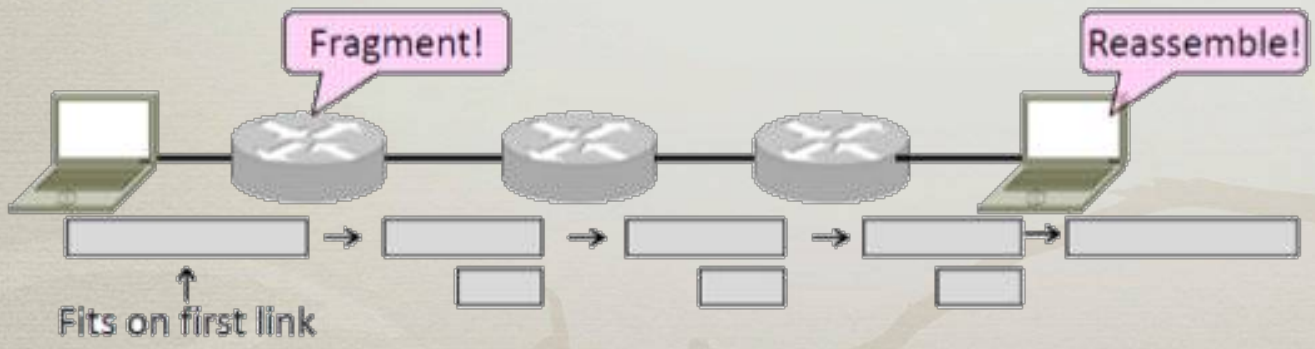


IPv4 fragmentacija

- Težava na poti – prevelik paket
  - paket se enkapsulira v okvir povezavne plasti
  - okvir ima pogosto omejeno dolžino
    - MTU – maximum transmission unit,
      Ethernet: do 1500 B, WiFi: 7981 B
    - MTU se tekom poti lahko spreminja
  - fragmentacija
    - razbitje prevelikega **paketa** na več manjših **fragmentov**

IPv4 fragmentacija

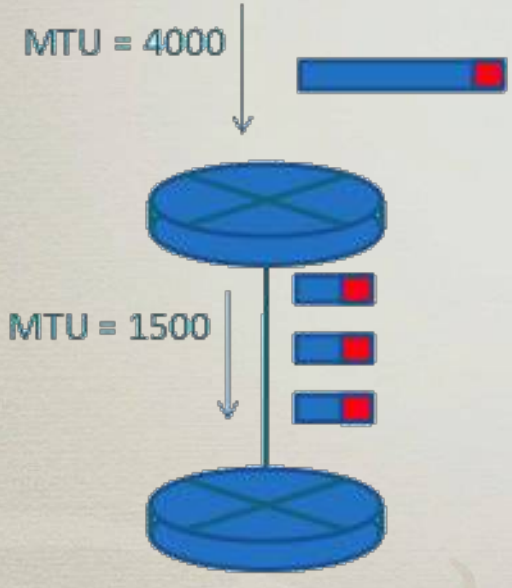
- Fragmentiranje
  - se zgodi v usmerjevalniku (lahko kjerkoli na poti)
  - uporaba „fragmentnih“ polj v paketu
- Defragmentiranje
  - združitev fragmentov šele na cilju v omrežni plasti

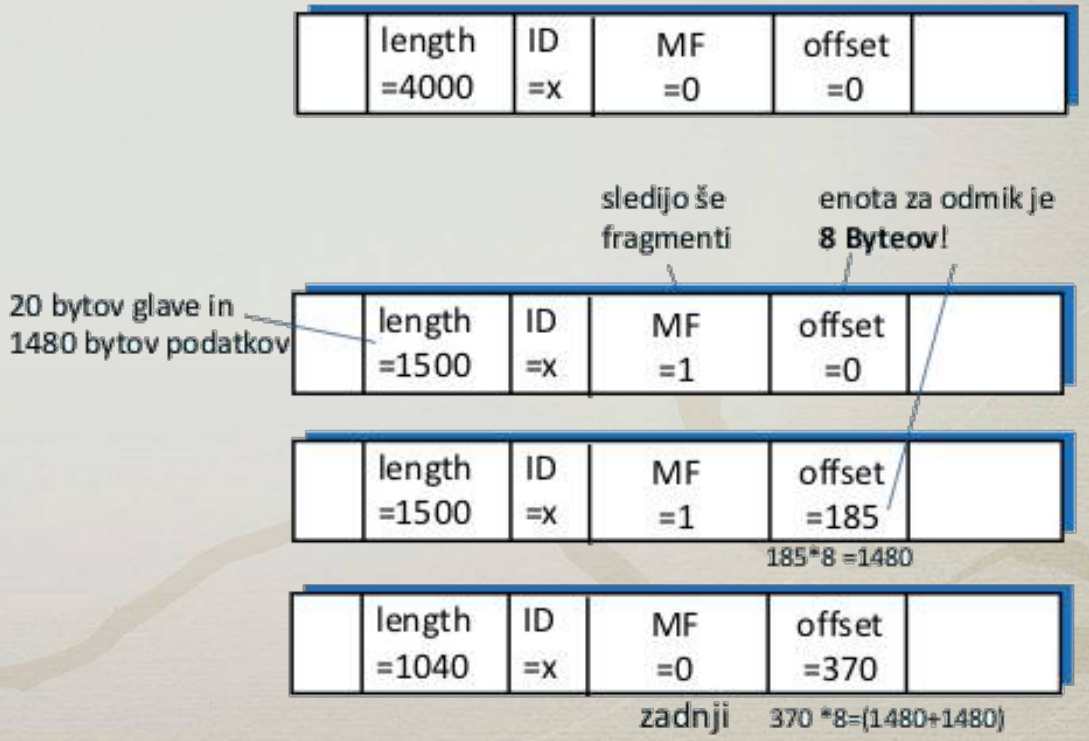


ver	hl	tos	length	
fragment id			flags	fragment offset
ttl		protocol	Internet checksum	
naslov izvora				
naslov cilja				
opcije				
podatki spremenljiva dolžina				

IPv4 fragmentacija

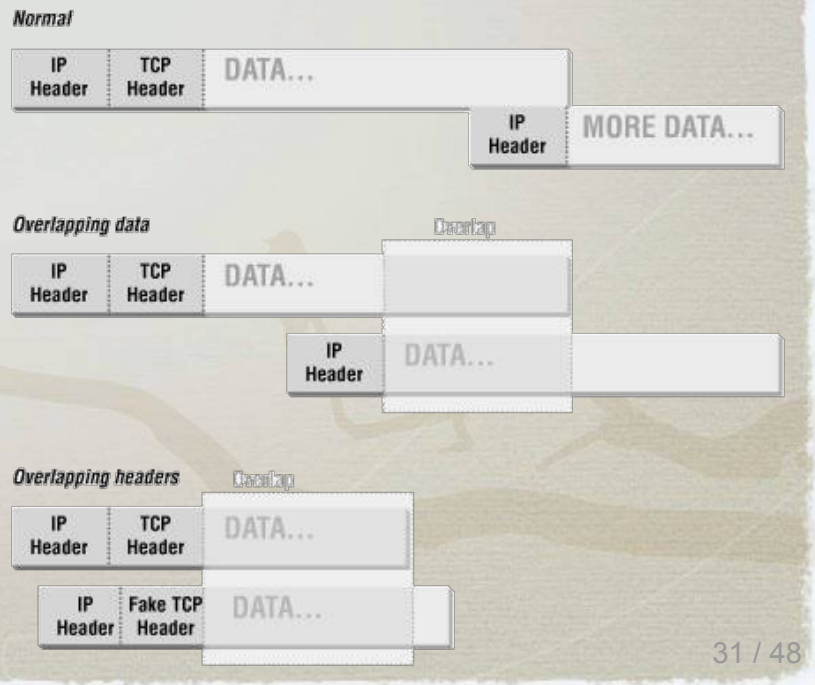
- Primer
  - paket dolžine 4000 B (glava=20, podatki=3980)
  - omejitev MTU=1500 B (glava=20, podatki=1480)
  - fragmenti: 1480 B + 1480 B + 1020 B = 3980 B





IPv4 fragmentacija

- Napadi
  - DoS napadi
  - *overlapping fragment attack*
    - napadalec generira fragmente z napačnimi odmiki, da se prekrivajo
    - pri sestavljanju se končni sistem lahko zmede in sesuje
  - *tiny fragment attack*
    - razkosa se tudi glava datagrama
    - tako ni možno izvesti varnostnega filtriranja

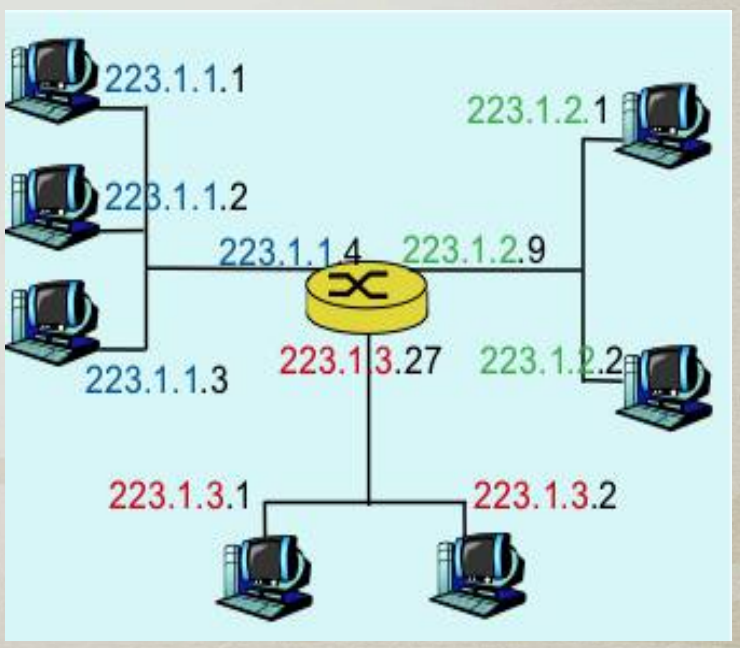


IPv4 naslovni prostor

01111011 00000001 00000010 00000011

123.1.2.3

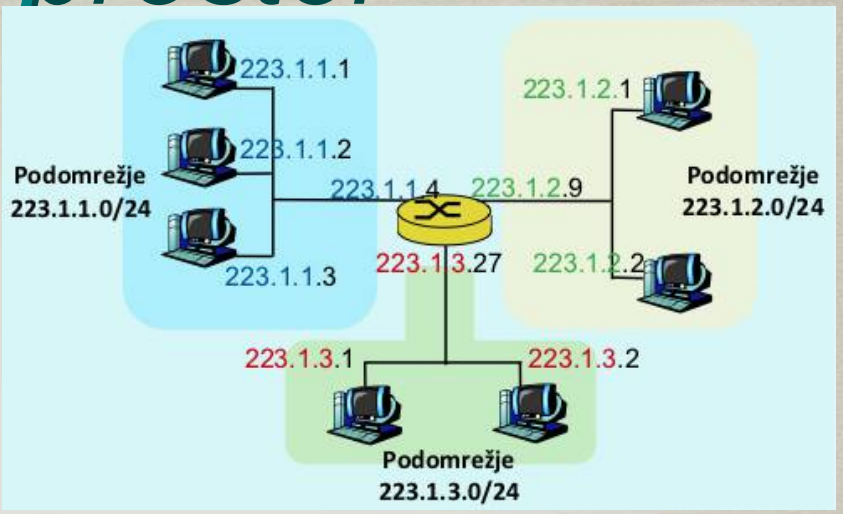
- 32-bitni naslovi
  - vsak vmesnik ima svoj naslov
    - naprava ima lahko več vmesnikov/naslovov
    - naslovi morajo biti globalno unikatni, NAT?
    - računalnik ima navadno en naslov
    - usmerjevalnik ima več naslovov
  - podomrežje (subnetwork)
    - prostor razdeljen na podomrežja
    - „lokacijsko sorodne“ naprave imajo podobne naslove
    - broadcast: naslov naprave = 11...1



naslov omrežja | naslov naprave

IPv4 naslovni prostor

- Podomrežje
  - možica vmesnikov z enakim naslovom omrežja
  - maska podomrežja
    - določa dolžino predpone (naslova omrežja)
    - 32-bitni niz z enicami na mestih predpone
    - okrajšava: zapis št. bitov



maska

11111111 11111111 11111111 11000000
255.255.255.192
/ 26

naslov: omrežje + vmesnik

01111011 00000001 00000010 00000011
123.1.2.0 | 3
123.1.2.0 / 26

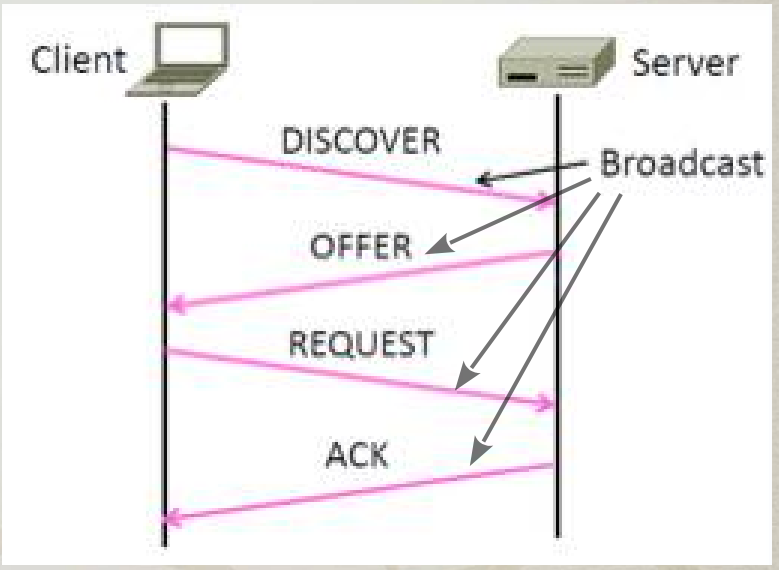
Sprva so bili definirani razredi omrežij, ki uporabljajo maske iz 8, 16, 24 bitov.

IPv4 naslovni prostor

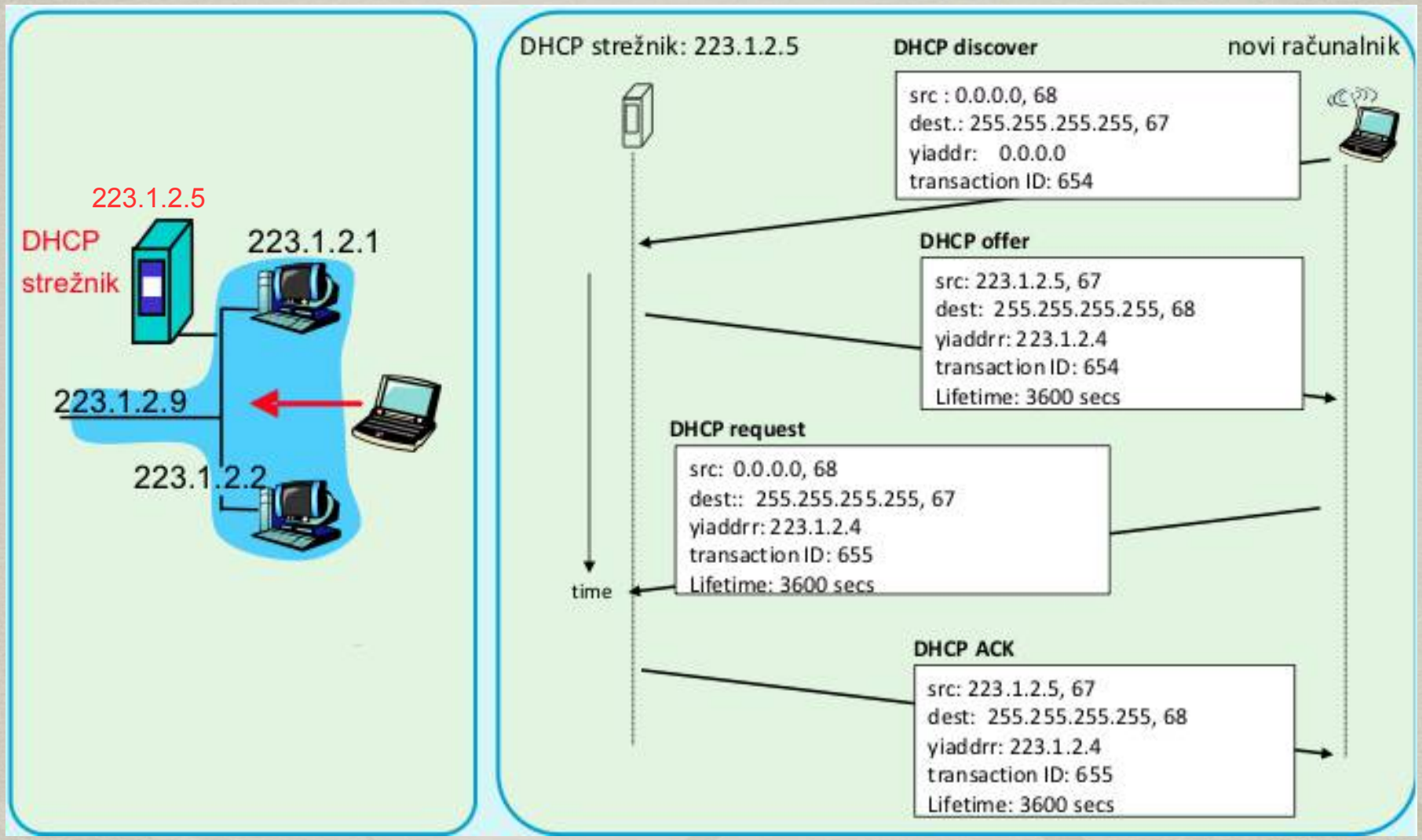
- Določanje naslovov
  - statično
    - uporabnik naprave vpiše naslov vmesnika, ki mu ga določi administrator omrežja (ponudnik)
    - ponudnik dostopa do omrežja (ISP, internet service provider)
    - ponudnik dobi naslovni prostor od ICANN
  - dinamično
    - DHCP

DHCP

- Dinamično dodeljevanje naslova
  - DHCP, dynamic host configuration protocol
  - ob priklopu v omrežje vmesnik nima naslova
  - v omrežju je DHCP strežnik
  - faze dodeljevanja naslova
    - DISCOVER, OFFER
    - REQUEST, ACK



DHCP

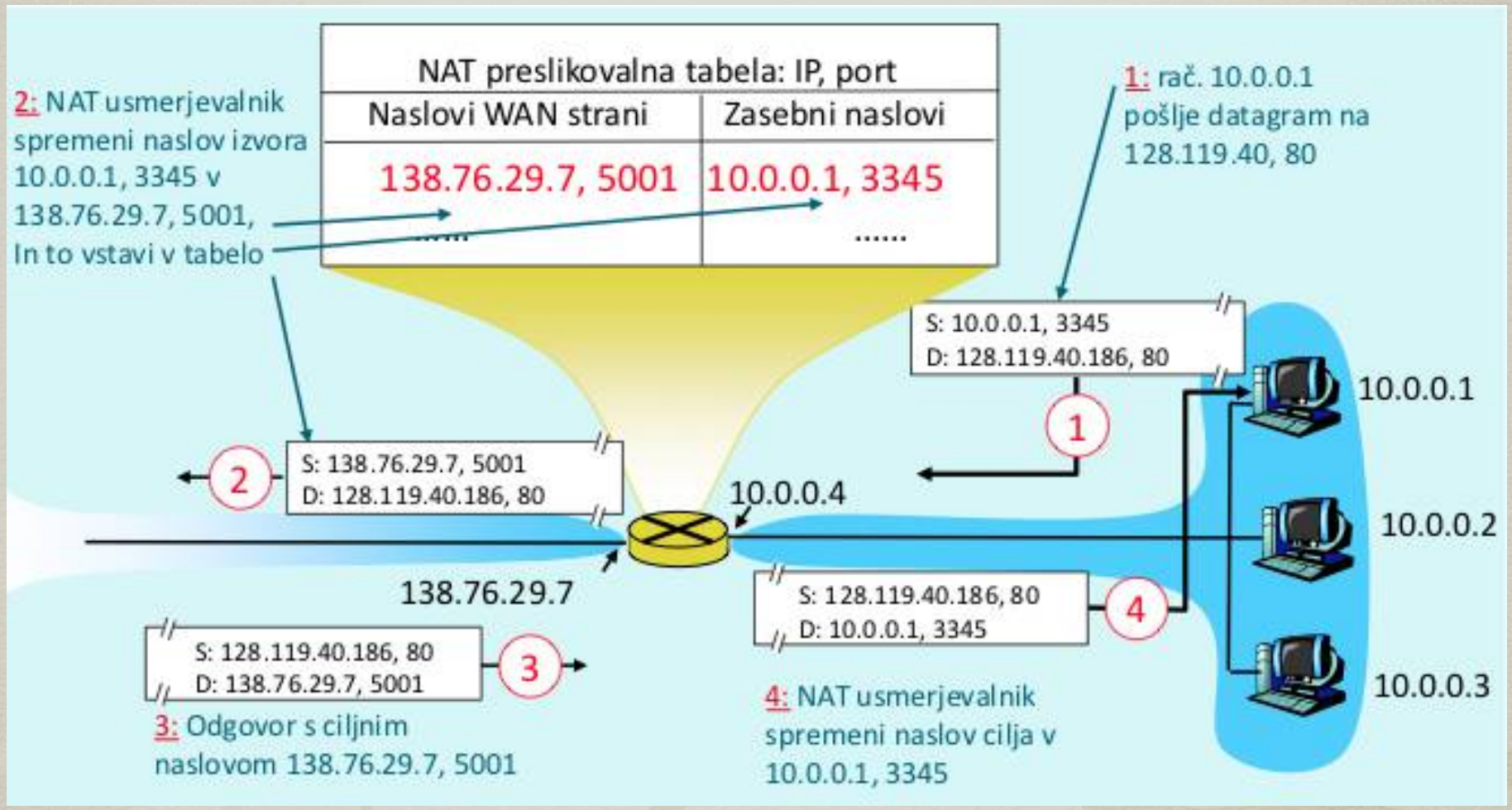

223.1.2.5
DHCP
strežnik
223.1.2.1
223.1.2.9
223.1.2.2
DHCP strežnik: 223.1.2.5
DHCP discover
novi računalnik
src : 0.0.0.0, 68
dest.: 255.255.255.255, 67
yiaddr: 0.0.0.0
transaction ID: 654
DHCP offer
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 654
Lifetime: 3600 secs
DHCP request
src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddrr: 223.1.2.4
transaction ID: 655
Lifetime: 3600 secs
time
DHCP ACK
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 655
Lifetime: 3600 secs

NAT

- Preslikovanje naslovov: globalno ↔ lokalno
  - NAT, network address translation
  - problem IPv4: pomanjkanje naslovnega prostora
  - namesto uporabe globalno unikatnih naslovov uporabljamo lokalne naslove, ki se lahko ponavljajo znotraj podomrežij
  - lokalni naslovni prostori

naslovni prostor	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 – 192.168.25.255	192.168.0.0/16	2^{16}

NAT


NAT preslikovalna tabela: IP, port
Naslovi WAN strani
Zasebni naslovi
138.76.29.7, 5001
10.0.0.1, 3345
.....
.....
2: NAT usmerjevalnik spremeni naslov izvora 10.0.0.1, 3345 v 138.76.29.7, 5001, In to vstavi v tabelo
1: rač. 10.0.0.1 pošlje datagram na 128.119.40, 80
S: 10.0.0.1, 3345
D: 128.119.40.186, 80
1
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
2
S: 138.76.29.7, 5001
D: 128.119.40.186, 80
138.76.29.7
S: 128.119.40.186, 80
D: 10.0.0.1, 3345
4
S: 128.119.40.186, 80
D: 138.76.29.7, 5001
3
3: Odgovor s ciljnim naslovom 138.76.29.7, 5001
4: NAT usmerjevalnik spremeni naslov cilja v 10.0.0.1, 3345

NAT

PREDNOSTI

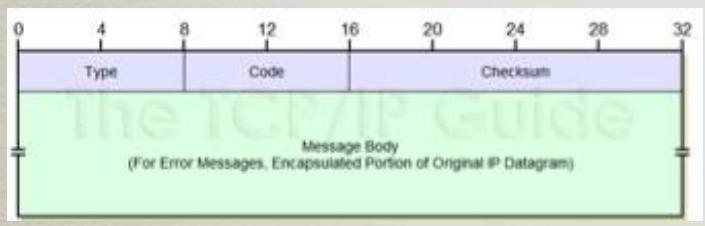
- zadošča samo 1 javni naslov za dostop celega omrežja do Interneta
- naslove notranjih naprav in ponudnika interneta (!) lahko **spreminjamo neodvisno** od zunanjega naslova
- večja **varnost** notranjih naprav, ker niso javno dostopne
- 16-bitno polje za vrata (port) omogoča evidentiranje cca. 60.000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

ICMP

- Nadzor omrežja
  - ICMP, internet control message protocol
  - uporaba za izmenjavo sporočil v zvezi z omrežjem
    - dostopnost, napake, nedosegljivost, …
  - sporočilo ICMP je enkapsulirano znotraj paketa
    - kot da bi šlo za protokol na transportni plasti



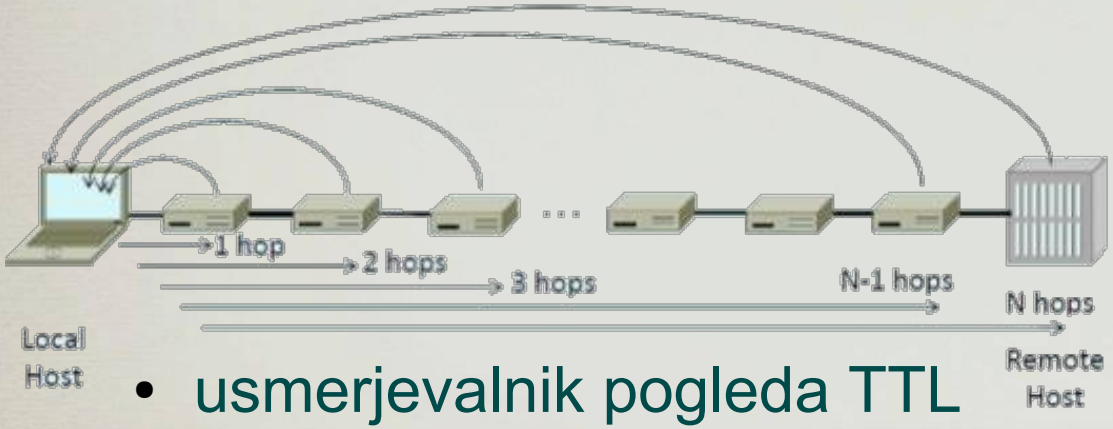
Tip	Koda	Pomen
0	0	echo reply (ping)
3	0	dest network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

ICMP

- Aplikacija **ping**
  - dosegljivost omrežja
  - preverjanje dosegljivosti preko sporočil
    - echo request
    - echo reply

ICMP

- Aplikacija **traceroute**
  - po kateri poti gre paket od izvora do danega cilja
    - izvor zaporedoma pošilja ICMP pakete cilju
      - paket vsebuje *echo request*, z naraščajočim TTL = 1, 2, ...



    - usmerjevalnik pogleda TTL
      - >0: dekrementira TTL in posreduje naprej
      - =0: odgovori z *TTL expired* (vključuje naslov usmerjevalnika)
    - končno vozlišče
      - odgovori z *echo reply* (postopek se konča)

IPv6

- Motivacija
  - večji naslovni prostor
    - premalo IPv4 32-bitnih naslovov
    - IPv6: 128-bitni naslovni prostor
  - potrebno hitrejše usmerjanje
    - fiksna glava 40 bajtov, brez opcij
    - fragmentacija paketov ni podprta
  - potrebno zagotavljanje kakovosti storitev za posebne tokove podatkov
    - oznaka vrste toka v paketih IPv6

IPv6

- Sintaksa IPv6 naslova
  - dvojiška oblika
    - 00100000111011010000000001101001100000000000000000010111100111011
      00000010101010100000000011111111111111000101000100111000101101O
  - razdelitev v osem 16-bitnih skupin
    - 0010000111011010 0000000011010011 0000000000000000 0000000000000000
      0000000000000000 0000000011111111 1111111000101000 1001110001011010
  - zapisan šestnajstiško, ločeno z dvopičji
    - 21DA:00D3:0000:0000:0000:00FF:FE28:9C5A
    - 21DA:D3:0:0:0:FF:FE28:9C5A (vodilne 0 izpustimo)
    - 21DA:D3::FF:FE28:9C5A (zaporedje ničelnih skupin nadomestimo z ::)
  - kompatibilnost z IPv4
    - spredaj dodamo ničle
    - 193.2.71.1 → ::193.2.72.1 (lahko pustimo pike)

IPv6

- Hitrejše usmerjanje
  - fragmentacija ni podprta
    - fiksna glava 40 bajtov, brez opcij
    - za ustrezno majhnost paketov skrbijo vozlišča sama
    - če je paket prevelik, ga usmerjevalnik zavrže in sporoči pošiljatelju ICMPv6 „Packet to big“
  - glava ne vsebuje kontrolne vsote
    - ni potrebno preračunavanje ob spremembi TTL
    - preverjanje paketov se izvaja že na drugih nivojih
  - polja opcije v glavi paketa ni več
    - opcije možno podpreti na drug način

IPv6

- Format paketa
  - **version**: IPv6
  - **traffic class**: podobno IPv4 TOS
  - **flow label**: oznaka toka, posebno zagotavljanje kakovosti (avdio/video)
  - **payload length**: velikost podatkov, ki sedijo glavi
  - **next header**: tip enkapsuliranega protokola, kot *protocol* pri IPv4
  - **hop limit**: TTL IPv4
  - **source address**, **destination address**: IPv6 naslov

IPv6

- Prehod iz IPv4 na IPv6
  - „flag day“ način
    - vseh naprav ni mogoče nadgraditi naenkrat
  - dvojni sklad (dual stack)
    - vozlišča hkrati podpirajo IPv4 in IPv6
    - če vozlišče ne podpira IPv6, se promet pretvori v IPv4
      - IPv6 specifična polja se pri tem izgubijo
  - tuneliranje (tunneling)
    - paket IPv6 zapakiramo v paket IPv4 kot podatke

Ostalo

- IPSec
  - varnost v omrežju