Internetne tehnologije

Internetni protokol

Žarko Čučej
e-naslov: zarko.cucej@uni-mb.si

Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko
Laboratorij za obdelavo signalov in daljinska vodenja

Maribor, 19. marec 2009

Predgovor

Internetni protokol (IP) je danes temeljni protokol za gradnjo in povezovanje skalabilnih, heterogenih omrežij v eno, logično celoto - medomrežje. Trendi trenutnega razvoja komunikacijskih omrežij gredo v smeri uporabe IP kot osnove za povezovanje omrežij, da je postala konvergenčna tehnologija prihodnosti. Zapis je razdeljen v štiri razdelke, v katerih opisujemo koncept in razvoj IP:

1. Povezovanje v omrežja in medomrežje — V tem razdelku na kratko povzemamo topologije, povezave podomrežij v omrežja in zahteve, ki morajo biti izpolnjene pri povezavi omrežij v medomrežje
2. Brezpovezavna omrežja — Glavna prednost in zato zahteva pri razvoju Interneta so brezpovezavne zveze oziroma storitve v tretji plasti ISO/OSI referenčnega modela medomrežja. V medomrežju se funkcije povezavnih in brezpovezavnih storitev s potrjevanjem vrši s protokoli TCP, UDP itd v četrti plasti.
3. IPv4 in ICMP — Protokol IP (verzija 4) izvaja funkcije tretje plasti ISO/OSI modela in je sestavni del zbirke protokolov TCP/IP. Skrbi za prenos podatkov med omrežji. Čeprav že star tri desetletja, je med najbolj razširjenimi protokoli, ki omogočajo medomrežja. Delovanje medomrežja in njegovih naprav krmilimo s protokolom ICMP.

Predgovor (2)

4. IPv6 in IPCMv6 Bliskovito širjenje Interneta že presega zmogljivosti, ki so bile predvidene pri razvoju protokola IPv4. Nov protokol, ki se izogne tem omejitvam, in upošteva bogate izkušnje, ki so se nabrale pri skoraj že eni milijardi uporabnikov Interneta, je IPv6. Njemu prilagojen krmilni protokol je ICMPv6.

Zapis predvideva, da so bralcu znane osnove komunikacijskih arhitektur (arhitekture 1) in gradniki žičnih omrežij (gradniki).

Prosojnice so izdelane s programom LaTeX in svežnjem paketov Beamer in TikZ. Za njihov ogled potrebujemo Adobe Reader™ verzije 5 ali novejše. Vse funkcije vgrajene v predstavitev smo preizkusili z Adobe Reader 8.1.2, Adobe Reader 9 in Adobe reader 9.1.

Žarko Čučej 19. marec 2009

Definicije

Omrežje (*Network*) je sistem komunikacijsko medsebojno povezanih naprav. Povezava med njimi je lahko fizična ali logična.

Medomrežje (*Internet*) je sistem medsebojno povezanih komunikacijskih omrežij. Povezave so izvedene z napravami, ki jih imenujemo vmesni sistemi.

Podomrežje (*Subnet*) je del omrežja z neko skupno značilnostjo, na primer skupno kolizijsko domeno ali delnim skupnim naslovom.

Končni sistem (*End System*: ES) je naprava, ki je priključena na omrežje. Uporablja se za izvajanje aplikacij končnega uporabnika. Zanjo se mnogokrat uporablja kratica DTE (*Data Terminal Equipment*) ali tudi termin gostitelj (*host*).

Vmesni sistem (*Intermediate system*: IS) je splošno ime naprav, ki omogočajo povezavo omrežij v medomrežje oziroma podomrežij v omrežje.

Definicije (2)

Mostič (*Bridge*) je naprava s funkcijami druge plasti ISO/OSI modela, ki omogoča delitev omrežij na (lokalna) podomrežja, ki uporabljajo iste protokole v logično-povezovalni podplasti. Mostič obdela informacije v fizičnih naslovih okvira (kdo pošilja, kdo sprejema. Zato deluje kot naslovno sito in omejuje na primer pri Ethernetu kolizijsko domeno oziroma omogoča paralelno delovanje podomrežij. Iz podomrežja prepušča samo pakete, ki imajo naslove izven njega. Mostič ne spreminja vsebine paketa.

Stikalo (*Switch*) je naprava z enakimi funkcijami kot mostič, razlikuje se v tem, da med priključenimi napravami (običajna uporaba) ali podomrežji (redkejša uporaba) izvede paketno komutacijo. S stikalom povezane naprave morajo imeti enako fizično in podatkovno-povezavno plast. V primeru uporabe v Ethernet omrežjih njegovo delovanje določa standard IEEE 802.1D

Definicije (3)

Usmerjevalnik (*Router*) je naprava s funkcijami tretje plasti ISO/OSI referenčnega modela, ki povezuje omrežja v medomrežje, ki lahko uporabljajo iste ali različne transportne protokole.

Stikalo L3 (*Switch L3*) je stikalo s funkcijami usmerjevalnika.

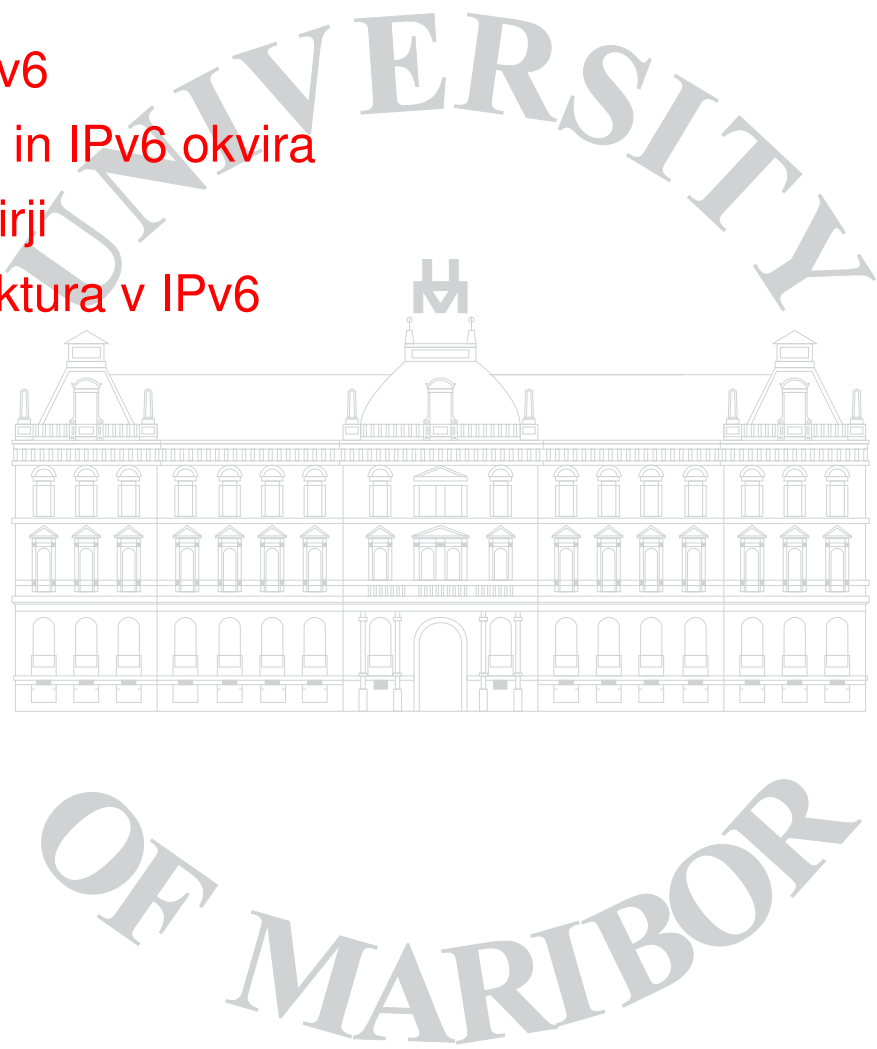
Stikalo L4 (*Switch L4*) je naprava, katere funkcije so odvisne od proizvajalca naprave. Pri večini to pomeni, da zmore prevajanje omrežnih naslovov in razporeditev prometa na osnovi TCP sej (torej funkcij 4 plasti, zato v imenu L4).

Stikalo L7 (*Switch*) je trgovsko ime napravam, ki zmorejo prepoznati nekatere funkcije aplikacijske plasti.

Proxy strežnik (*Proxy server*) je strežnik, ki na zahteve svojih odjemalcev posreduje ostalim strežnikom v omrežju ali medomrežju. Zagotavlja zmogljivosti za nekatere storitve, ki jih odjemalec sam ne zmore izvesti. Po potrebi lahko proxy strežnik spremeni zahtevo odjemalca ali izvrši zahtevano storitev ne da bi se povezal z ostalimi strežniki.

Vsebina

Vsebina (2)



Uvod

- Medomrežje – ali z uveljavljeno tujko internet – je povezava (računalniških) omrežij v – običajno globalno – omrežje, ki povezuje uporabnike v širšem krajevnem ali interesnem območju.
- Največje medomrežje na svetu je svetovni splet omrežij. Imenujemo ga Internet in zanj pogosto slikovito pravimo, da je *mati vseh omrežij*.
- Internet je nastal iz omrežja ARPAnet, ki je bilo zgrajeno na pobudo agencije za strateške raziskave (ARPA) pri ameriškem obrambnem ministrstvu in kasneje dano v javno uporabo.
- Rast Interneta je tako silovita, da bo kmalu zmanjkalo naslovnega prostora, ki pri protokolu IPv4 – ta je osnova delovanja Interneta – obsega $2^{31} = 2\ 147\ 483\ 648$ naslovov.
- Internet ni edino medomrežje svetovnih razsežnosti. Obstajajo še druga, manj znana, ki so namenjena ožjemu krogu uporabnikov.

Uvod (2)

- Medomrežja in internetni protokol, ki jih omogoča, postajajo danes dominanti komunikacijski sistemi in tehnika prenosa govora, slik, filmov, podatkov v raznih oblikah in prioritetah.

  S pojmom Internet danes že razumemo (navidezni) prostor, kjer je – z nekaj zanosa lahko rečemo – uskladiščeno človeško znanje, so na voljo vsakodnevne informacije in novice, ki povezuje ljudi ne glede na raso, spol, starost in vero ali prepričanje.

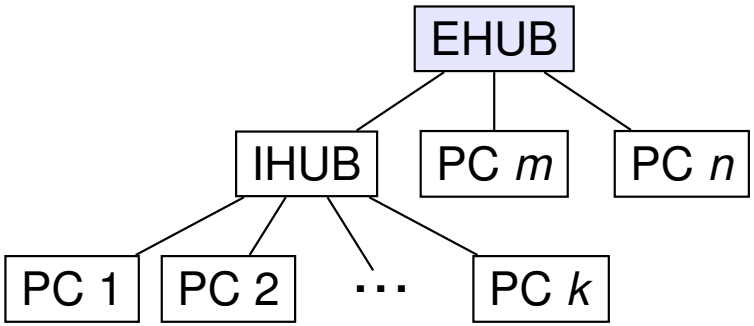
  Z drugimi besedami, Internet je danes ne samo tehniški sistem, ampak že sociološki pojem s vplivom, kot ga nima nobeden do sedaj znanih sistemov, na vse človeške dejavnosti, od izobraževanja, študija, zdravstvene skrbi, poslovanja, da naštejemo le nekatere.
- V nadaljevanju se seveda omejujemo le na tehnike in tehnologije, ki omogočajo povezave (računalniških) omrežij v medomrežja.

Drobitev omrežij

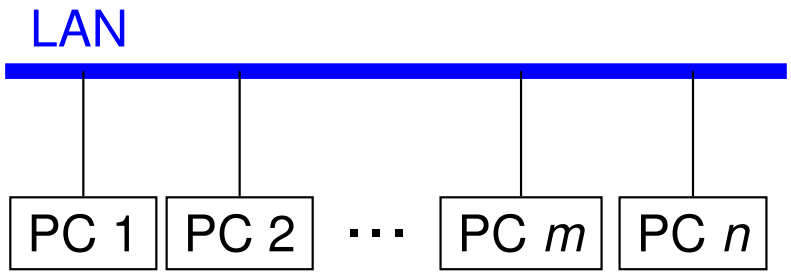
- Pojem omrežja utrdimo na primeru računalniškega omrežja, katerega delovanje določa standard ISO 8802.3 (IEEE 802.3) Ethernet.
- Značilnosti Etherneta so:
  - Vsi uporabniki si delijo skupni prenosni medij, zato lahko po njem posreduje podatke sočasno le en uporabnik omrežja.
  - Pravico do uporabe prenosnega medija dodeljuje mehanizem za nadzor dostopa do prenosa. Zanj je uveljavljena kratica MAC (Media Access Control). Nahaja se v podplasti MAC in pri Ethernetu zagotavlja enakopravni in pošteno dostop do prenosa.
  - Pri velikem številu uporabnikov omrežja opazimo dva pojava:
    - pri enovitem omrežju morajo vsi uporabniki omrežja čakati na kogarkoli v omrežju, da ga preneha uporabljati,
    - večina prometa na omrežju se odvija med uporabniki, ki pripadajo določeni organizacijski ali interesni skupnosti
  - Podrobnosti o omrežju Ethernet so na prosojnicah Ethernet

Drobitev omrežij (2)

- Danes so na Ethernet omrežje računalniki večinoma povezani preko (žičnih) gradnikov omrežij.
- Če gradniki zmorejo le funkcije fizične plasti (repetitorji in zvezdišča), z njimi lahko zgradimo omrežje z le eno kolizijsko domeno.



Slika 1.1: Zgradba omrežja.

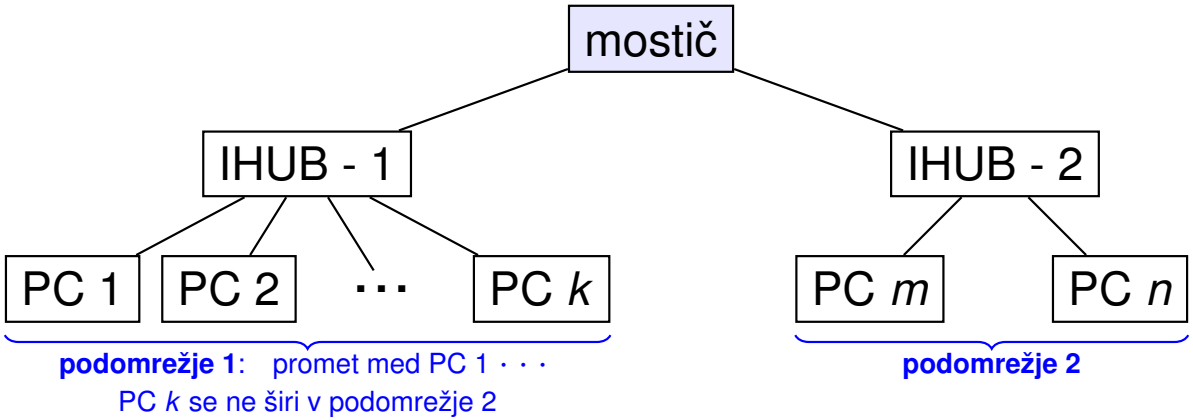


Slika 1.2: Ekvivalentna shema omrežja.

- Iz ekvivalentne sheme (Fig. 1.2) sledi, da na primer paket, ki ga na primer PC 1 pošlje PC2, lahko sprejmejo vsi računalniki na omrežju.

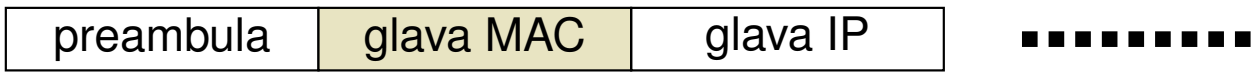
Drobitev omrežij (3)

- Širjenje paketov po omrežju lahko omejimo z razdelitvijo omrežja na podomrežja (Fig. 1.3).



Slika 1.3: Primer omrežja, ki ga sestavljata dve podomrežji in ju v omrežje povezuje mostič.

- Naprave, ki povezujejo podomrežja v omrežje, morajo biti sposobne analize fizičnih naslovov v glavi okvira (Fig. 1.4).

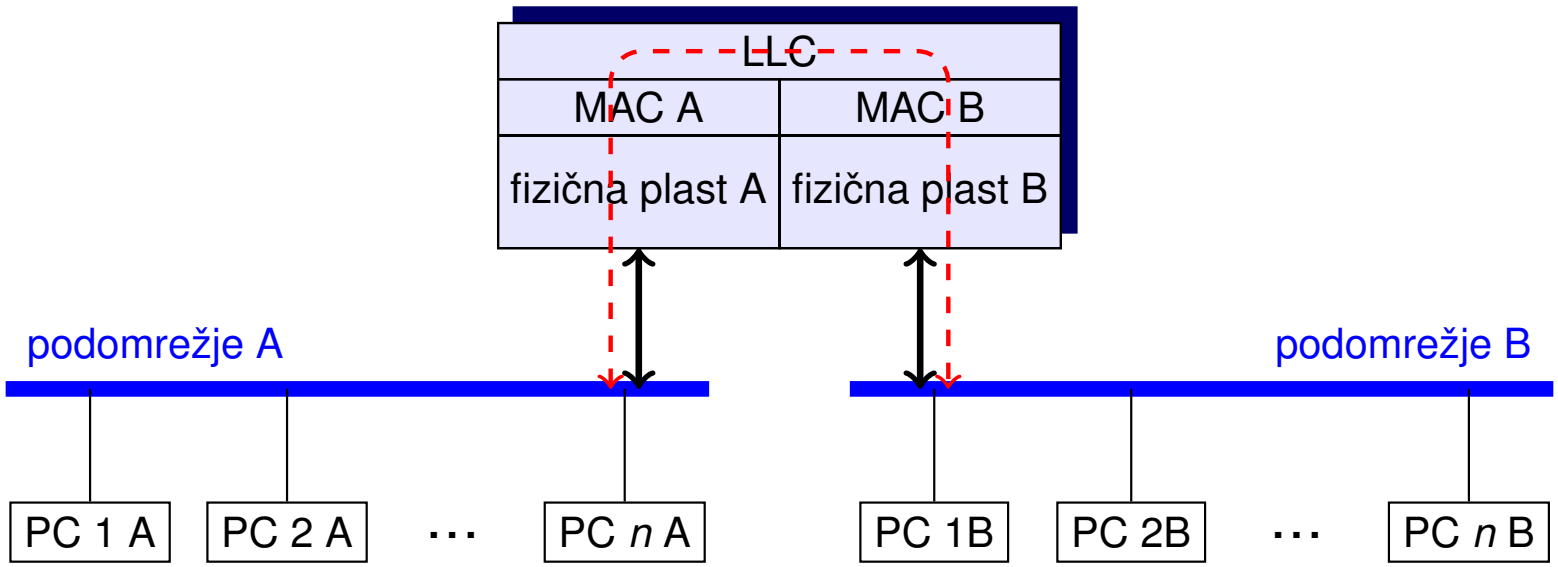


Slika 1.4: Mostič in stikalo L2 v vsakem paketu analizirata glavo MAC.

- Primer takih naprav so mostiči ali stikala L2.

Povezovanje v omrežja

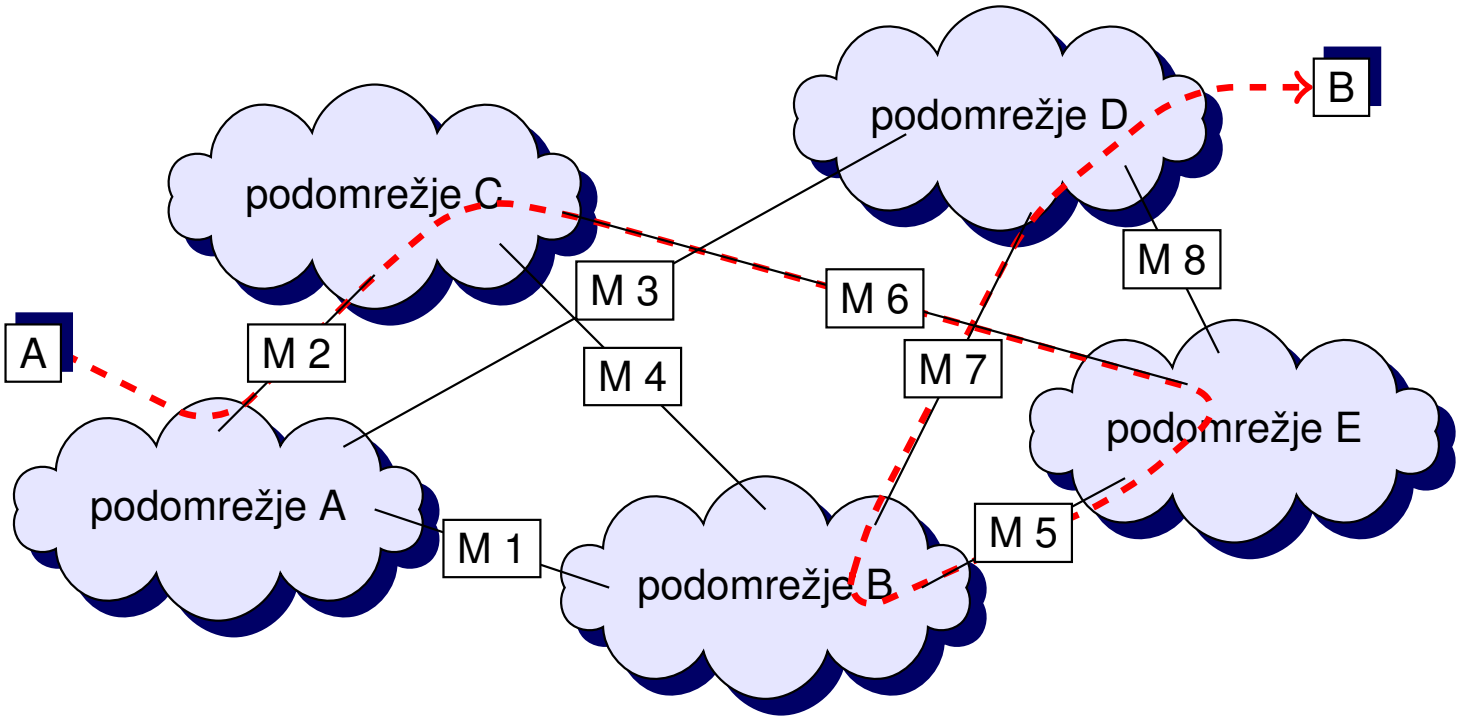
- Z mostiči in stikali L2 lahko v omrežja povezujemo podomrežja, ki imajo enako logično povezavo (LLC), smejo pa imeti različen dostop do omrežja in fizično povezavo naprav (Fig. 1.5).



Slika 1.5: Mostič in stikalo L2 v vsakem paketu analizirata glavo MAC.

Povezovanje v omrežja (2)

- Struktura povezav podomrežij v omrežje je lahko mrežna (Fig. 1.6) – tvorijo tako imenovana mrežna omrežja (mesh networks).



Slika 1.6: Mrežna omrežja (mesh networks). Pri njih lahko paketi do svojega cilja potujejo preko več podomrežij. V prikazanem primeru iz končnega sistema (računalnika) A potuje preko podomrežja A, mostiča M2, podomrežja C mostiča M6, podomrežja E, mostiča M5, podomrežja B, mostiča M7 in na koncu preko podomrežja D v končni sistem (računalnik) B.

Povezovanje v omrežja (3)

- Usmerjanje paketov skozi omrežje se izvede na osnovi poznavanja fizičnih naslovov končnih naprav.
- Prednosti mostičev:
  - Odstrani fizične omejitve pri številu uporabnikov, številu segmentov in razdaljah, ki jih lahko omrežje pokrije.
  - Vmesno hranjenje paketov pri posredovanju med podomrežji omogoča povezavo podomrežij z različnimi MAC.
  - Drobljenje omrežja v podomrežja poveča zanesljivost, razpoložljivost in uslužnost vsega omrežja.
- Slabosti mostičev:
  - Vmesno pomnjenje paketov vnaša dodatne zakasnitve.
  - MAC nima mehanizma za krmiljenje pretoka podatkov, zato mostič ne more varovati omrežja pred poplavo paketov.
  - Pri podomrežij z različnimi MAC, mostič pri prenosu paketa generira novo preveritveno vsoto. Pri tem sprejete podatke upošteva kot pravilne, zato prikriva nastale napake.

Usmerjanje z mostiči

Mostiči uporabljajo dve metodi usmerjanja paketov skozi omrežje:

- Transparentno povezovanje (*transparent bridging*), ki temelji na podatkovni bazi (Table 1), v kateri mostič zbere fizične naslove in druge podatke o računalnikih v posameznih podomrežij. Podatke mostič zbere z učenjem:

Tabela 1: Baza posredovanja paketov. Naslovi MAC so zapisani v “pika decimalni” obliki

vrata	**MAC naslov pošiljatelja**	**metrika**
1	111.22.33.44.51.60	podomrežje A
1	111.22.33.44.51.61	podomrežje A
1	111.22.33.44.51.62	podomrežje A
⋮	⋮	⋮
2	111.22.33.44.52.60	podomrežje B
2	111.22.33.44.52.61	podomrežje B

Usmerjanje z mostiči (2)

- Mostič v vsakem prispelem paketu prebere zapisana fizična (rečemo jima tudi MAC) naslova in preveri, ali sta zapisana bazi posredovanja paketov.
- Če naslova nima vpisana v bazi, prepiše naslov pošiljatelja v svojo bazo, ga označi s številko vrat, na katerih je naslov sprejel in okvir posreduje v vsa ostala podomrežja v omrežju.
- Nekateri (boljši) mostiči poled zapisa posredovanja, v tabeli še zapišejo še metriko paketa, da se izognejo njegovemu kroženju, če je možnih več poti širjenja paketov.
- Transparentno povezovanje se uporablja predvsem v Ethernet omrežjih, za njih ga določa standard ISO 8802.1D (IEEE 802.1D)

- Usmerjeno povezovanje (*Source route bridging*) kjer mostič uporabi posebne protokole za iskanje optimalnih poti paketov skozi omrežje. Med njimi je najbolj znan protokol odpiranja dreves.
- Pri usmerjevanem povezovanju mostič uporablja dve vrsti okvirov:

Usmerjanje z mostiči (3)

- okvir SR (Single Route frame), ki ga uporablja za prenos paketov po omrežju,
- okvir AR (All-Route frame), ki ga uporabljajo usmerjevalni protokoli za iskanje najboljše poti skozi omrežje.

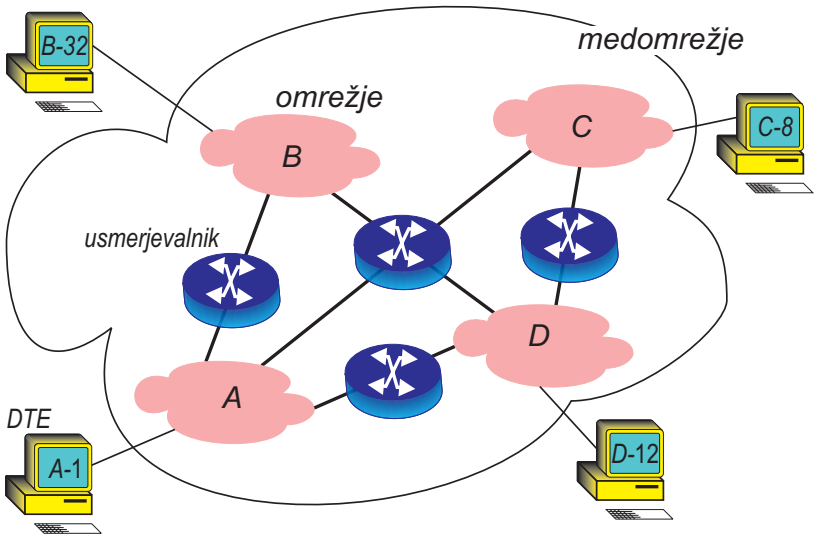
- Delovanje protokola odpiranja dreves (Spanning tree protocol):
  - Mostič pošlje okvir kot “sporočilo vsem”
  - Okvir na svoji poti zapiše vse mostiče, ki jih preide
  - Okvir ima življenjsko dobo določeno s številom etap, ki jih lahko prehodi (število etap je večje kot je diameter grafa, ki predstavlja omrežje).
  - Ob vsakem prehodu mostiča, se števec etap zmanjša za ena.
  - Ko je števec enak nič, se okvir zavrže in s tem prepreči njegovo kroženje po omrežju.
  - Prvi okvir AR, ki doseže cilj se upošteva, da je prešel najboljšo pot, zato se zapisana pot uporabi za usmerjanje okvirov SR, ki sledijo k istemu cilju.

Usmerjanje z mostiči (4)

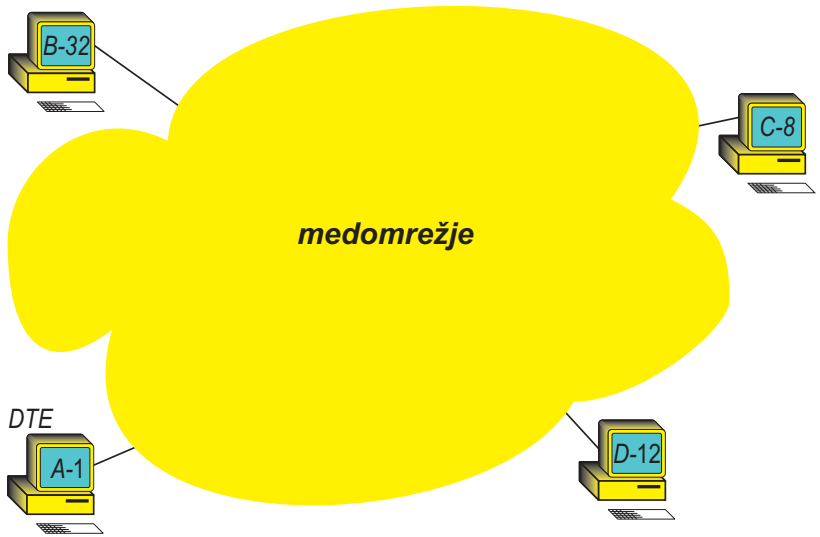
- Usmerjanje okvirov se lahko v primerih, ko je na voljo več poti do cilja, uporablja kot posredno uravnoteževanje obremenitve mostičev – bolj ko je določeni mostič obremenjen, manj je verjetno, da bo zapisan kot del optimalne poti do cilja – novi okvir AR bo našel drugo, hitrejšo pot, če seveda obstaja.
- Usmerjeno povezovanje se zelo razlikuje od transparentnega posredovanja, kjer se določenih (redundančnih) mostičev ne aktivira. Sposobnost poiskanja vseh poti oziroma usmerjanje paketov zahteva dodatni promet (paketi AR) in dodatni prostor v okvirih za zapis poti.

Povezovanja v omrežja

- Mnoga omrežja se medsebojno razlikujejo tudi v podplasti krmiljenja logične povezave (podplast LLC), zato niso povezljiva z mostiči.
- Te razlike lahko premostimo s povezovanjem na tretji plasti ISO/OSI modela – tu lahko povežemo poljubna omrežja (Fig. 1.7) tako, da končnim uporabnikom razlike med omrežji niso vidne (Fig. 1.8).



Slika 1.7: Zgradba medomrežja.



Slika 1.8: Medomrežje kot ga vidi uporabnik.

TCP/IP model model in protokoli

Aplikacijska plast
DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · XMPP · POP3 · RTP · SIP · SMTP · SNMP · SSH · TELNET · RPC · RTCP · RTSP · TLS (and SSL) · SDP · SOAP · GTP · STUN · NTP
Transportna plast
TCP, UDP, DCCP, SCTP, RSVP, ECN
Omrežna plast
IPv4, IPv6, IPsec, OSPF, IS-IS, BGP, ARP, RARP, RIP, ICMP, ICMPv6, IGMP
Podatkovno povezovalna plast
Ethernet, Token ring, FDDI, IEEE 802.11 (WLAN), Wi-Fi, IEEE 802.16 WiMAX, ATM, DTM, Frame Relay, GPRS, EVDO, HSPA, HDLC, PPP, PPTP, L2TP, ISDN, ARCnet, LLTD

Slika 1.9: Umestitev internetnih protokolov v model TCP/IP. Z rdečo barvo so označeni protokoli, ki jih opisujemo.

Internet in medomrežja

- Največje medomrežje na svetu je svetovni splet omrežij. Imenujemo ga Internet in zanj pogosto slikovito pravimo, da je mati vseh omrežij.
- Internet je nastal iz omrežja ARPAnet, ki je bilo zgrajeno na pobudo agencije za strateške raziskave (ARPA) pri ameriškem obrambnem ministrstvu in kasneje dano v javno uporabo.
- Rast Interneta je tako silovita, da bo kmalu zmanjkalo naslovnega prostora, ki pri protokolu IPv4 obsega $2^{31} = 2\ 147\ 483\ 648$ naslovov.
- Internet ni edino medomrežje svetovnih razsežnosti. Obstajajo še druga, manj znana, ki so namenjena ožjemu krogu uporabnikov.
- Vsa medomrežja imajo mnogo skupnega. Njihovo delovanje omogočajo protokoli iz omrežne plasti modela ISO/OSI oziroma modela TCP/IP.
- Vsako omrežje povezano v medomrežje, mora omogočiti ne le komunikacijo med “svojimi” priključki, ampak tudi med omrežji.

Osnovne lastnosti medomrežja

- Povezave omrežij v medomrežje morajo zagotoviti:
  1. najmanj fizično in logično povezavo (funkcionalnost prve in druge plasti ISO/OSI modela).
  2. usmerjanje prometa in dostavo podatkov med procesi v različnih omrežjih.
  3. obračunski servis – ta vsebuje tudi zapise uporabe usmerjevalnikov in omrežij z njihovimi statusi vred.
- Vse storitve medomrežja so (morajo biti) zagotovljene brez spreminjanja arhitekture kateregakoli omrežja, ki je povezano oziroma se povezuje v medomrežje.

Zahteve pri povezovanju omrežij

Medomrežje mora razrešiti mnogo zahtev neodvisno od posebnosti posameznih podomrežij:

- *Različni sistemi naslavljanja*.
  Podomrežja lahko uporabljajo različne oblike končnih imen, naslovov in map, kjer so zapisana imena. Zato mora biti dogovorjen skupen, globalni sistem naslavljanja kot tudi storitve njihovega zapisa.
- *Različne maksimalne dolžine paketov*.
  Paketi, ki potujejo skozi več omrežij (z različnimi prenosnimi karakteristikami), se lahko razdelijo (ob prehodih med omrežji ali pa pred pošiljanjem pri uporabniku) na manjše pakete. Ta postopek imenujemo *segmentacija* ali *fragmentacija*.
- *Različni postopki dostopa do prenosa*.
  Lokalna omrežja so lahko tipa Ethernet, Token bus, Token ring itd, zato končni uporabniki različno (uspešno) dostopajo do omrežja.

Zahteve pri povezovanju omrežij (2)

- *Različno dolga nadzorna časovna okna*.
  Pri mehanizmih potrjevanja pravilnega prispetja paketa se čaka na potrditev določen čas. Po njegovem izteku se avtomatsko pošlje nov paket. V splošnem se za prenos preko več različnih podomrežij potrebuje daljši čas.
- *Odpravljanje napak*.
  Medomrežja morajo zagotoviti različne nivoje storitev. Od prenosa brez odpravljanja napak do zanesljivih prenosov. Pri zanesljivih prenosih morajo biti mehanizmi odpravljanja napak neodvisni od mehanizmov v podomrežju. Nanje tudi ne smejo vplivati.
- *Poročanje o stanju naprav*.
  Omrežja se razlikujejo tudi po načinu javljanja in hranjenja poročil o dogajanju in stanju v podomrežju. Te informacije morajo biti na voljo pooblaščenim storitvam tudi v medomrežju.

Zahteve pri povezovanju omrežij (3)

- *Usmerjanje podatkovnega prometa*.
  V medomrežju je običajno možnih več poti med uporabniki,

  To je bila glavna zahteva pri načrtovanju omrežja ARPAnet!

  zato mora biti poskrbljeno za usmerjanje podatkovnega prometa. Usmerjanje je lahko odvisno od odkrivanja izpadov poti, zamašite ali zasičenja prometa. Medomrežje mora biti sposobno prilagajati promet razmeram v omrežju.

- *Nadzor nad uporabniki*
  Vsako omrežje ima svoj sistem nadzora in avtorizacije uporabljanja omrežja (kdo je uporabnik, kakšne pravice ima). Ta nadzor mora biti dostopen tudi medomrežju.

- *Povezavno-orientirane in brezpovezavne storitve*.
  Posamezna podomrežja lahko omogočajo povezavno orientirane storitve ali le brezpovezavne storitve. Zaželeno je, da so storitve medomrežja neodvisne od vrste storitev v podomrežju.

Komunikacijske zveze

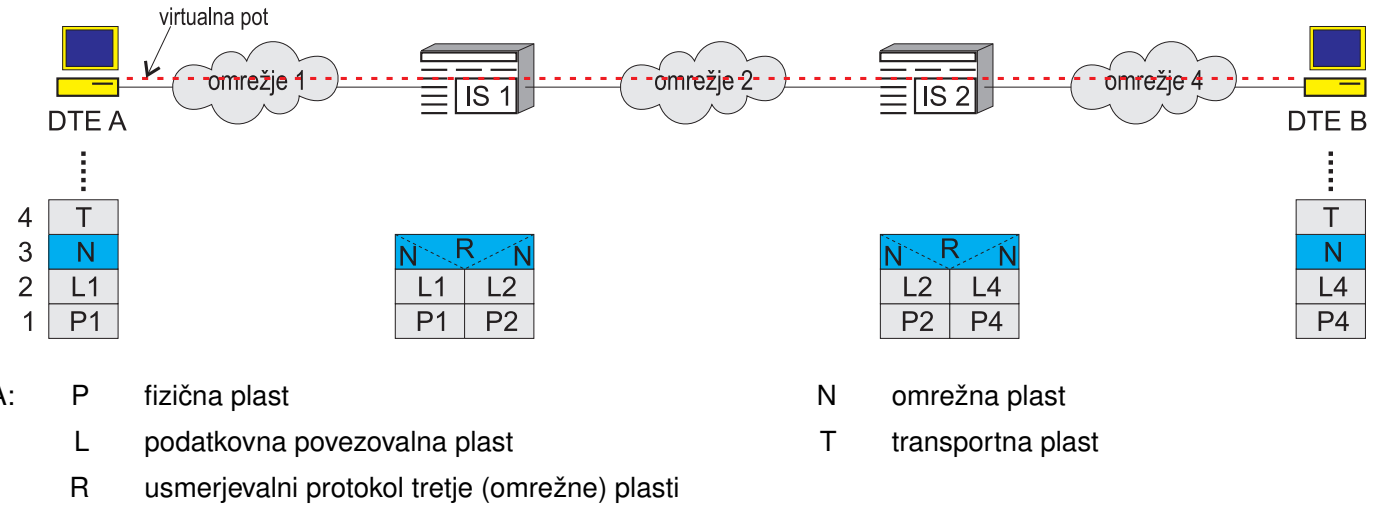
- Ponovimo, obravnavamo paketna omrežja, ki so medsebojno povezana v medomrežje s paketno komutacijo.
- Promet v medomrežju se lahko odvija na dva načina:
  - Povezavni način, kjer se posredovanje paketov izvrši v treh korakih:
    1. najprej se vzpostavi zveza – zaradi paketne komutacije je to virtualna pot ali kanal – med končnima sistemoma, ki želita izmenjati podatke
    2. izvrši se izmenjava podatkov, in
    3. po zaključku izmenjave podatkov se prekine zveza oziroma razgradi virtualna pot ali kanal.
  - Brezpovezavni način, kjer podatke preprosto pošljemo, medomrežje pa jih po svojih najboljših močeh skuša dostaviti naslovljenemu končnemu sistemu.
- Oba sistema zvez imata svoje prednosti in slabosti, nobeden izmed njiju ne prevladuje nad drugim.
- Vrsta zvez v medomrežju odločilno vpliva na arhitekturo protokola, na njegovo ranjlivost oziroma trdoživost ter prilagojenost posameznim področjem uporabe.

Povezavne zveze

- Podomrežja povezujejo vmesni sistemi: IS, ki jih omrežja “vidijo” kot enega od končnih sistemov (ES) Podomrežje jih vidi kot enega od končnih sistemov priključenih na omrežje
- Ko želi DTE A izmenjati podatke z DTE B, najprej med njima vzpostavi logično povezavo. Zaporedje logičnih povezav skozi podomrežja tvori *virtualno pot* med DTE (Fig. 2.10).
- Pogoj:Vsa podomrežja v medomrežju *morajo* nuditi povezavne storitve četudi jih sama ne uporabljajo.

  Na primer, lokalna omrežja ISO 8802 (IEEE 802) imajo storitev načina povezav določene v podplasti LLC. Dve sta brezpovezavni, ena pa povezavna storitev. Če se v lokalnem omrežju uporabljajo brezpovezavne storitve, potem moramo v omrežju izboljšati kakovost storitev, na primer z nadgradnjo podplasti LLC s protokolom X.25. S to nadgradnjo omrežje nudi medomrežju in svojim končnim uporabnikom, povezavne medomrežne storitve v lokalni promet pa izvaja z brezpovezavnimi storitvami.

Povezavne zveze (2)

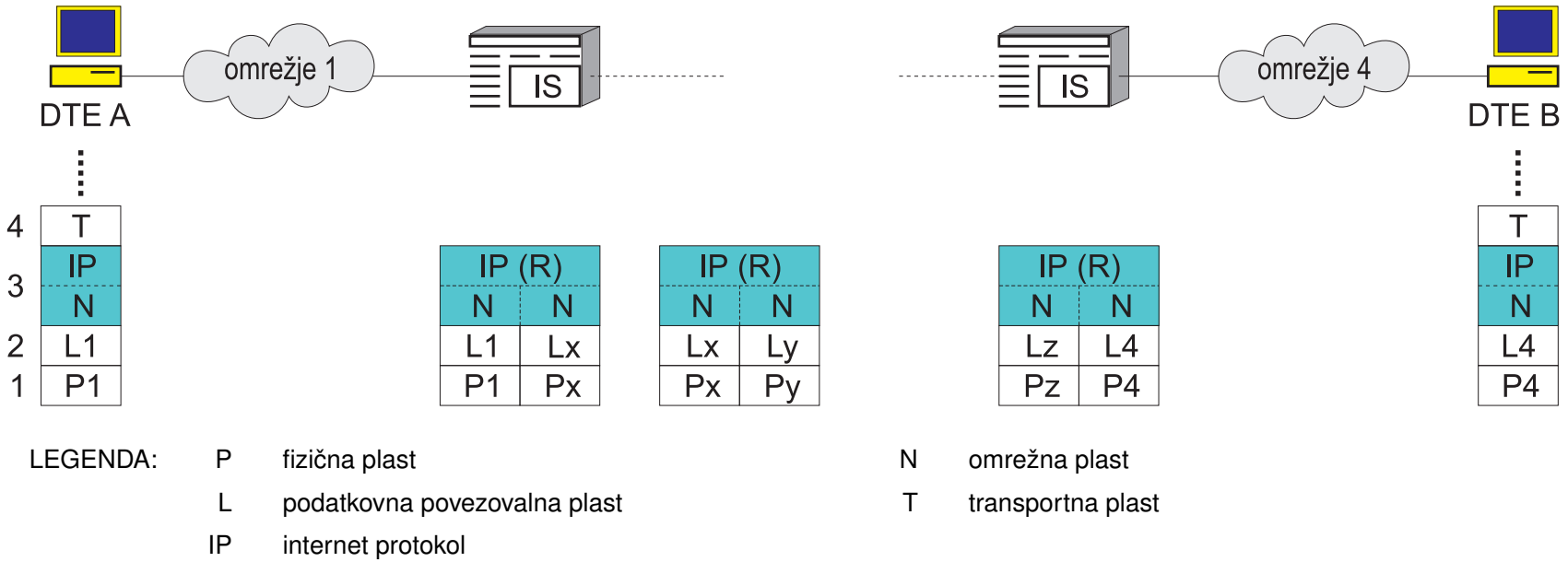


Slika 2.10: Medomrežna arhitektura: povezavno-orientirani način delovanja medomrežja.

- dostop do podomrežij omogočajo protokoli v omrežni plasti,
- IS so usmerjevalniki. Izvajajo naslednji ključni funkciji:
  - *Posredovanje* podatkovne enote iz enega podomrežja v drugo.
  - *Usmerjanje* virtualne poti ob vzpostavitvi zveze med končnima uporabnikoma.

Brezpovezavno delovanje

- Brezpovezavni način delovanja medomrežja lahko ponazorimo z delovanjem (klasične) pošte.



Slika 2.11: Medomrežna arhitektura: brezpovezavni način delovanja medomrežja.

Brezpovezavno delovanje (2)

- Brezpovezavni način delovanja medomrežja je podoben datagramskim (brezpovezavnim) storitvam v paketnih omrežjih.
- Vsaka podatkovna enota (PDU) se neodvisno obravnava na vsej svoji poti od svojega vira, na primer DTE A, do svojega cilja, na primer DTE B.
- Pri tem DTE A odloči, kateremu usmerjevalniku ga posreduje, ta neodvisno sprejme odločitev za naslednjo etapo potovanja in zadnji usmerjevalnik na poti preda PDU omrežju, na katero je priključen DTE B (Fig. 2.10).
- Prvi protokol IP je razvit za omrežje ARPAnet in je bil objavljen kot RFC 791.
- Danes obstajajo še drugi omrežni protokoli, na primer CLNP (Connection-Less Network Protocol) ISO 8473, ki ima podobno funkcionalnost kot IP.

Brezpovezavno delovanje (3)

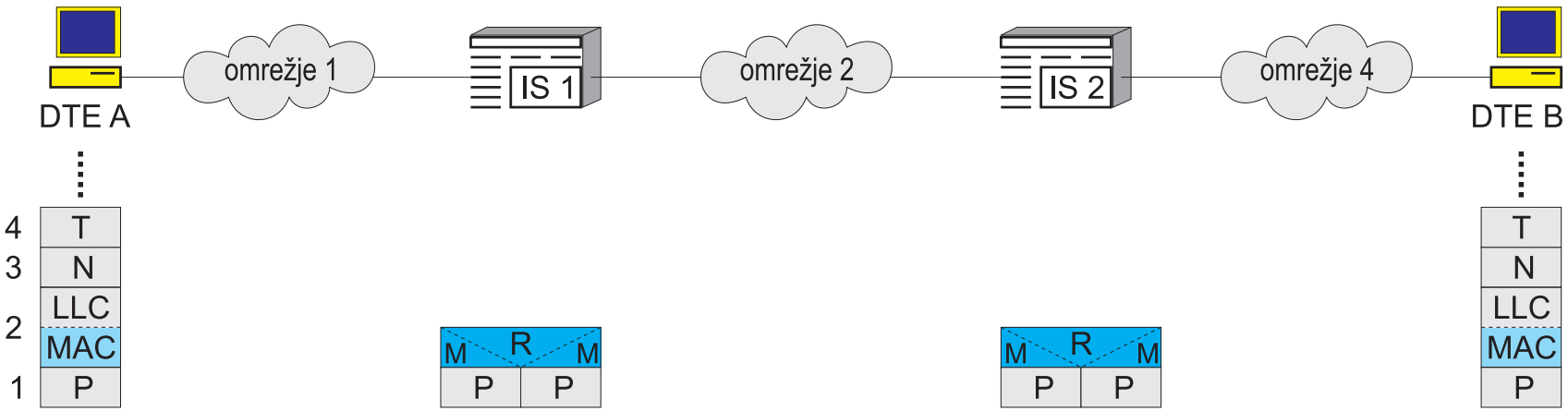
- Za delovanje IP in CLNP so potrebni še protokoli, ki omogočajo dostop do konkretnega podomrežja. Zato delimo omrežno plast na dve podplasti:

  DTE: v *zgornji* podplasti je protokol za funkcije medomrežja, v *spodnji* pa so funkcije za dostop do podomrežja.

  Usmerjevalniki: v *zgornji* podplasti so protokoli za usmerjanje, v *spodnji* pa so enaki kot v DTE.

Medomrežja z mostiči

- Preprosta medomrežja lahko zgradimo z mostiči.
- Povezana so na nivoju podplasti MAC.
- Uporabljajo brezpovezavni način delovanja.



Slika 2.12: Medomrežna arhitektura: brezpovezavni način delovanja medomrežja z mostiči.

Medomrežja z mostiči (2)

- V primeru uporabe mostičev kot IS si medomrežje deli skupni transportni in medomrežni protokol.
- Predpostavlja se, da vsa podomrežja uporabljajo iste protokole v podatkovni povezovalni plasti.

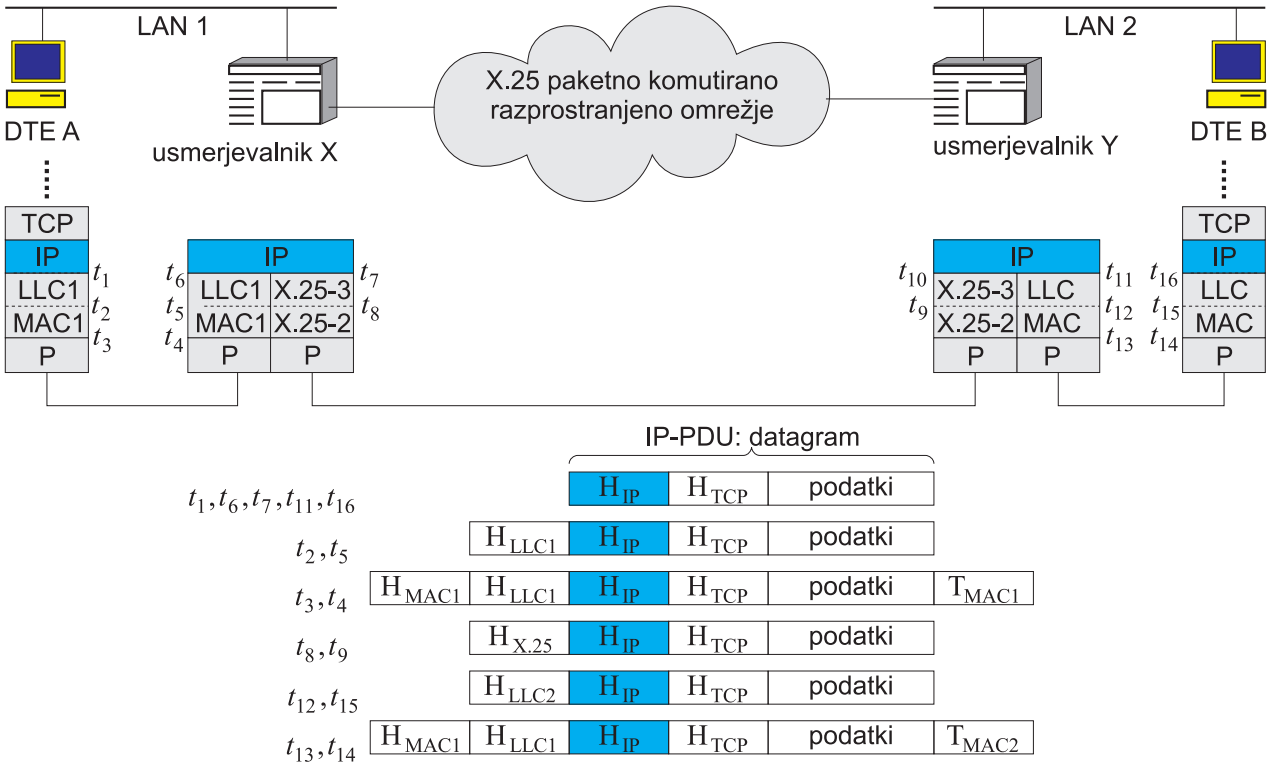
  Pri omrežjih ISO 8802 ali pri FDDI omrežjih to pomeni, da imajo vsa podomrežja isti protokol MAC in LLC. Na primer, da so vsa podomrežja tipa ISO 8802.3 (Ethernet), in da vsa uporabljajo nepotrjevane brezpovezavne storitve plasti LLC. V teh primerih bo mostič lahko posredoval okvire MAC iz enega podomrežja v drugega.

Brezpovezavna omrežja

- Protokol IP zagotavlja brezpovezavne, datagramske storitve med končnima sistemoma.
- Najpomembnejše med njimi so:
  - *Fleksibilnost*. To pomeni, da lahko medomrežje povezuje različna podomrežja, tudi taka, ki so brezpovezavna.
  - *Robustnost*. Brezpovezavne storitve so robustne zato, ker ne potrebujejo v naprej določene zveze med uporabnikoma. Ta se vzpostavlja sproti in ob izpadu, zamašitvi ali zasičenju uporabljenih povezav omogoča (samodejno) iskanje novih.
  - Brezpovezavne storitve so bolje prilagojene brezpovezavnim transportnim protokolom kot povezavne.
- IP ne jamči, da bodo podatki dostavljeni in da bodo poslani podatki prispeli v pravilnem zaporedju. Jamči le *najboljši poskus*, da bodo podatki prišli na cilj.

Delovanje brezpovezavnega medomrežja

- Primer pošiljanja podatkov (Fig. 2.13):



Slika 2.13: Delovanje omrežnega protokola: prenos podatkov med gostiteljema DTE A v podomrežju LAN 1 gostitelju DTE B v podomrežju LAN 2. Podomrežji povezuje paketno omrežje X.25.

Delovanje brezpovezavnega medomrežja (2)

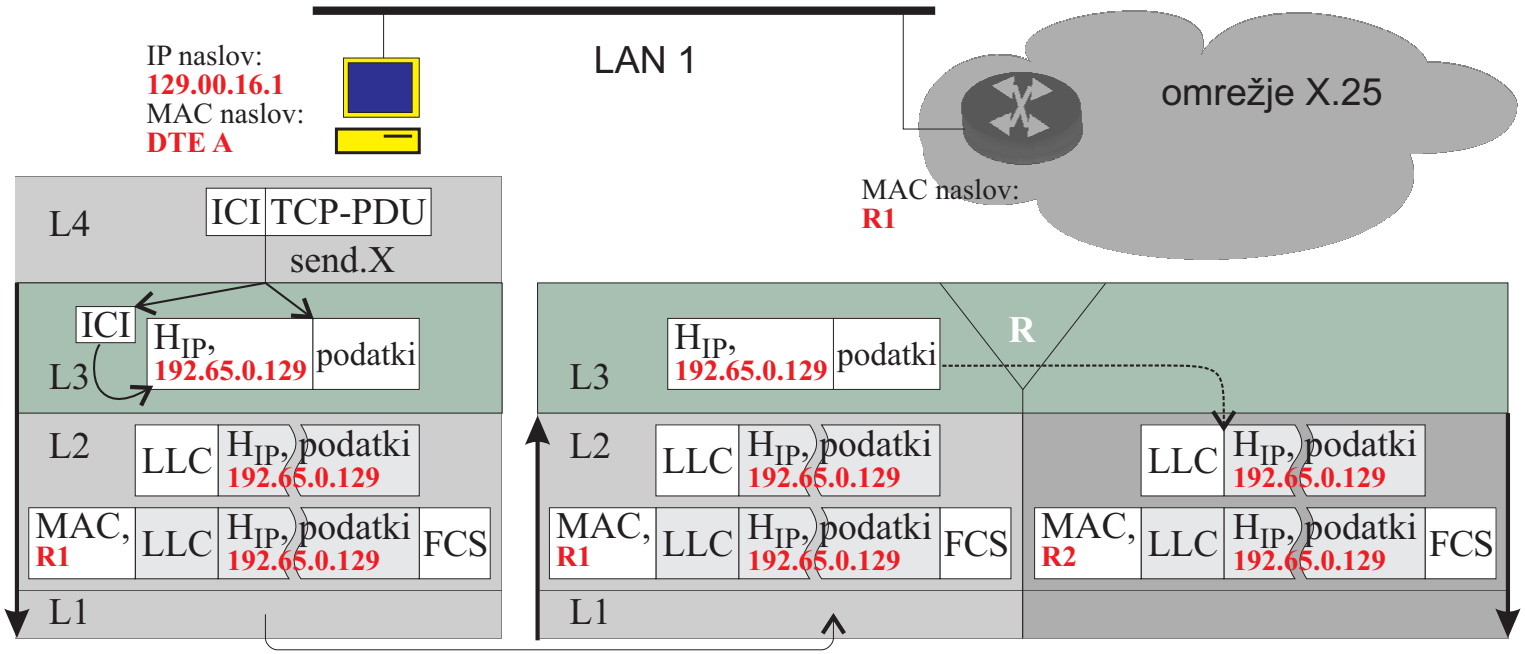
- Predpostavimo naslednje podatke:

	gostitelj A	usmerjevalnik 1	usmerjevalnik 2	gostitelj B
naslov IP:	192.0.65.1	–	–	192.65.0.129
naslov MAC:	DTE A	R1	R2	DTE B

- Opazujmo postopek od trenutka, ko protokol TCP s primitivom send.X preda TCP-PDU plasti IP
- Parametri primitiva so v ICI (Interface Control Information)
- Protokol IP odstrani ICI in v skladu z instrukcijami v ICI sestavi čelo datagrama ter datagram preda podplasti LLC
- Podplast LLC opremi datagram s svojim čelom – dobimo LLC-PDU, ki ga preda podplasti MAC

Delovanje brezpovezavnega medomrežja (3)

- Podplast MAC iz naslova IP uvidi, da je LLC-PDU namenjen gostitelju izven LAN 1, zato v naslov MAC vpiše fizični naslov usmerjevalnika R1, na katerega je povezan LAN 1 (Fig. 2.14).



Slika 2.14: Delovanje omrežnega protokola: prenos podatkov med gostiteljem DTE A in usmerjevalnikom R1.

Delovanje brezpovezavnega medomrežja (4)

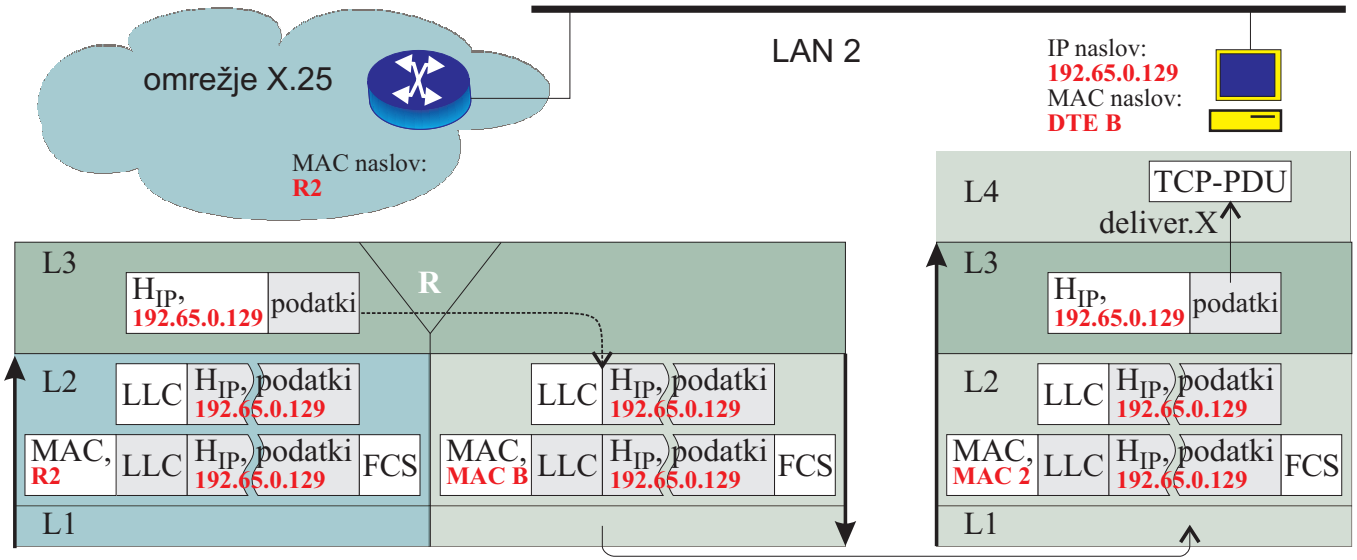
- Fizična plast okvir z enkapsuliranim datagramom pošlje usmerjevalniku R1.
- Usmerjevalnik R1 ob sprejemu okvira odreže čelo in popotnico MAC, potem pa še čelo LLC ter in prečita čelo datagrama.
- Z algoritmom usmerjanja določi najkrajšo pot skozi omrežje X.25. Ker naslednja etapa vodi do usmerjevalnika 2, preda datagram podplasti LLC s protokolom X.25-3.
- Podplast LLC opremi datagram s svojim čelom in preda LLC-PDU skupaj s potrebnimi instrukcijami podplasti MAC s protokolom X.25-2.
- Protokol X.25-2 v fizični naslov vpiše naslov usmerjevalnika R2, doda popotnico ter naroči fizični plasti, da okvir pošlje v omrežje X.25 (Fig. 2.14).

Delovanje brezpovezavnega medomrežja (5)

- Usmerjevalnik R2 ob sprejemu okvira v podplasteh X.25-2 in X.25-3 prečita in odreže čelo protokola X.25 ter datagram preda omrežni plasti.
- Usmerjevalni algoritem iz naslova IP ugotovi, da se ciljni gostitelj nahaja v podomrežju LAN 2, zato z ustreznimi instrukcijami preda datagram podplasti LLC2
- Protokol v LLC2 opremi datagram s svojim čelom in preda okvir podplasti MAC2.
- Protokol v MAC v skladu z instrukcijami določi fizični naslov, in pripada naslovu IP v datagramu
- Manipulacije z naslovi:
  - V čelu podatkovne enote, ki jo transportna plast posreduje omrežni, je *globalni* ali medomrežni naslov končnega uporabnika (DTE B).

Delovanje brezpovezavnega medomrežja (6)

- IP ob pregledu naslova ugotovi, da je prejemnik (DTE B) v drugem podomrežju. Zato da podplasti LLC instrukcijo, da pošlje datagram v usmerjevalnik X.



Slika 2.15: Delovanje omrežnega protokola: prenos podatkov med usmerjevalnikom R1 in gostiteljem DTE B.

- Podplast LLC posreduje te instrukcije podplasti MAC, ki LLC podatkovni enoti doda MAC naslov usmerjevalnika X.

Delovanje brezpovezavnega medomrežja (7)

- Podobno se dogaja v usmerjevalniku X:
  - V sprejeti podatkovni enoti odstrani čeli MAC in LLC.
  - V čelu IP datagrama prebere končni naslov datagrama. Glede na njega se odloči, kako bo usmeril nadaljno potovanje datagrama. Pri tem ima tri možnosti:
    1. Ciljni usmerjevalnik Y je povezan na isto podomrežje kot usmerjevalnik X. V tem primeru usmerjevalnik X pošlje podatke direktno usmerjevalniku Y.
    2. Med usmerjevalnikoma X in Y je več podomrežij. V tem primeru se mora usmerjevalnik X odločiti, kdo je naslednji usmerjevalnik, ki mu bo poslal podatke.
    3. Usmerjevalnik X ne pozna naslova usmerjevalnika Y. V tem primeru pošiljatelju okvira (DTE A) pošlje sporočilo *napaka, naslov neznan*.

Velikost paketov

- Maksimalna velikost paketov je lahko v podomrežjih različna.
- Zato mora vsak usmerjevalnik preveriti, ali lahko posreduje naprej paket v sprejeti velikosti.
- Če to ne more, usmerjevalnik podatke segmentira – razdeli na manjše dele - *fragmente*, ki postanejo neodvisni datagrami.
- Da usmerjevalnik lahko sestavi fragmente nazaj v originalni datagram, podatke o segmentaciji – zaporedno številko fragmenta – zapiše v čelo datagrama.
- Defragmentacijo – sestavljanje originalnega datagrama – izvede IP v končnem sistemu. Zanjo potrebuje vmesni pomnilnik, katerega velikost mora omogočiti sestavljanje datagrama, tudi v primeru, ko paketi ne prihajajo v istem vrstnem redu kot so bili poslani.

Načrtovanje IP

Pri načrtovanju IP moramo upoštevati naslednja opravila IP:

- usmerjanje paketov skozi medomrežje,
- skrb za življenjsko dobo datagrama,
- segmentacijo in sestavljanje datagramov iz segmentov,
- nadzor napak,
- nadzor podatkovnega prometa.

Usmerjanje

- Obstajata dve tehniki usmerjanja:
  1. Usmerjanje krmili usmerjevalnik na osnovi zapisanih podatkov o medomrežju, instrukcijah sistemskega administratorja ali algoritmov usmerjanja prometa.
  2. Pot paketa določi pošiljatelj. V tem primeru je sestavni del paketa specifikacija poti, ki vsebuje spisek zaporedja usmerjevalnikov.
- V prvem primeru se usmerjanje v splošnem vrši z vzdrževanjem *usmerjevalniških tabel* s podatki o vseh končnih sistemih in usmerjevalnikih v medomrežju.
- Iz tabeliranih podatkov lahko za vsako podomrežje določimo usmerjevalnik, kamor je potrebno poslati podatke.
- Usmerjevalniške tabele so lahko *statične* ali *dinamične*:

  Statične tabele — Podatke v statične tabele vpisuje administrator. Pripravi tudi alternativne poti, če te obstajajo. Aktivira jih administrator.

Usmerjanje (2)

Dinamične tabele

Dinamične tabele se same odzivajo na dogodke v medomrežju. Na primer, v Internetu usmerjevalnik pri ugašanju obvesti sosednje usmerjevalnike, da se izključuje. S tem jim omogoči, da lahko osvežijo svoje tabele z novim stanjem v medmrežju.

- Usmerjevalniške tabele se lahko uporabijo še za druge storitve, na primer, za varnost in prioritete.

  Na primer, posamezna podomrežja so lahko opredeljena za rokovanje s podatki določenega varnostnega razreda. Usmerjevalniki morajo v takih primerih zagotoviti, da podatki ne potujejo po podomrežjih, ki ne izpolnjujejo varnostnih zahtev.

Življenjska doba datagrama

- Paketi v medomrežju se lahko “izgubijo” – pričnо (do neskončnosti) krožiti po medomrežju.
- Posledice:
  - V brezkončnem kroženju datagrama imamo nekoristno zasedanje prenosnih zmogljivosti medomrežja,
  - Višji protokoli, na primer transportni, so odvisni od življenjske dobe datagrama.
- Rešitev:

  Vsakemu datagram ima vpisno življenjsko dobo. Ko je ta prekoračena, usmerjevalnik datagram zavrže.
- Merjenje življenjske dobe:
  - S štetjem prehojenih etap. Ko datagram preide usmerjevalnik, se zmanjša število dovoljenih etap na poti.
  - Z dejanskim časom. V teh primeru rabimo globalni urni mehanizem. Prednost merjenja časa se izkaže pri sestavljanju segmentov v datagram.

Segmentacija in sestavljanje datagrama

- Na začetku razvoja IP je prevladovalo mnenje, da z drobljenjem okvirov v fragmente, ko to postane v prenosu skozi medomrežje potrebno, optimiramo prenosne zmogljivosti
- Kasneje so izkušnje pokazale, da je segmentacija zahtevna in časovno potratna funkcija usmerjevalnikov.

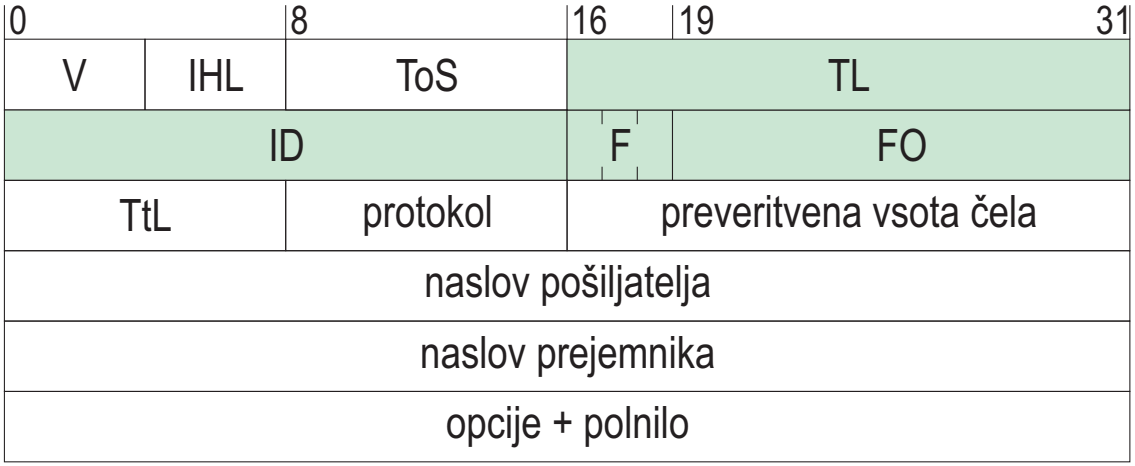
  Učinkoviteje je vnaprej informirati pošiljatelja, kako velik je lahko paket za določeno pot. Ta način delovanja medomrežja omogoča protokol IPv6.
- Pri segmentiraciji, posebej če se na poti dogodi večkrat, nastane vprašanje, kje datagram spet sestaviti.
- Najpreprosteje: samo v končnem prejemniku datagrama.

  Pri tej strategiji lahko po segmentaciji po medomrežju potujejo le paketi s fragmenti okvira, čeprav so prišli v podomrežja, ki zmorejo prenos na primer originalnega okvira!

Segmentacija in sestavljanje datagrama (2)

- Sestavljanje fragmentov v usmerjevalnikih optimira velikost paketov, ima pa naslednji slabosti:
  1. Usmerjevalniki potrebujejo večji vmesni pomnilnik. *Vedno pa obstaja nevarnost, da se bo ves vmesni pomnilnik uporabil za hranjenje fragmentov.*
  2. Vsi fragmenti morajo potovati skozi isti usmerjevalnik. S tem je onemogočeno dinamično usmerjanje. *Zato IP zahteva sestavljanje paketa iz fragmentov v končnem prejemniku paketa.*
- Za podporo segmentaciji je v čelu paketa IP predvidenih več polj (Fig. 2.16):
  - oznaka paketa,
  - dolžina podatkov,
  - zastavica *več fragmentov*
  - odmik fragmenta.

Segmentacija in sestavljanje datagrama (3)



LEGENDA:

V:	verzija protokola	ID:	identifikator paketa
IHL:	dolžina čela (Internet Header Length)	F:	zastavice (Flags)
ToS:	tip storitev (Type of Service)	FO:	odmik fragmenta (Fragment Offset)
TL:	skupna dolžina paketa (Total Length)	TtL:	življenjska doba (Time to Live)

Slika 2.16: Polja v čelu datagrama, ki so osenčena, se uporabljajo pri segmentaciji.

Segmentacija in sestavljanje datagrama (4)

- Zgradba čela datagrama:
  - Oznaka paketa enoumno določa paket. Pri IP jo določa *naslov prejemnika*, *ID* in *zaporedna številka*.
  - Dolžina podatkov je podana v oktetih. Enaka je TL - IHL.
  - Odmik (mnogokratnik 64 bitov) pove, koliko je začetek fragmenta odmaknjen od začetka podatkov v paketu.
- Pošiljatelj v čelo datagrama vpiše dolžino datagrama, v polje odmika in zastavice *več fragmentov* pa ničlo.
- Drobljenje paketov (Table 2):
  1. Usmerjevalnik podatke datagrama razdeli na dva približno enako velika dela. Dolžina prvega dela podatkov mora biti mnogokratnik 8 oktetov (= 64 bitov).
  2. K podatkom doda čelo originalnega paketa.
  3. Izračuna novo dolžino paketa (IHL + dolžina podatkov) in rezultat vpiše v polje TL.

Segmentacija in sestavljanje datagrama (5)

4. V prvem paketu postavi zastavico *več fragmentov* na resnično, polje odmik pa pusti nespremenjeno.
5. V drugem paketu v TL vpiše dolžino drugega paketa, v odmik pa dolžino podatkov v prvem paketu deljeno z 8. Zastavica *več fragmentov* ostane nespremenjena – "neresnično-- temu paketu ne sledijo paketi s fragmenti.

Tabela 2: Segmentacija datagrama v dva fragmenta.

originalni datagram	**prvi fragment**	**drugi fragment**
Dolžina podatkov = 768 Odmik fragmenta = 0 zastavica *več fragmentov* = 0	Dolžina podatkov = 512 Odmik fragmenta = 0 zastavica *več fragmentov* = 1	Dolžina podatkov = 256 Odmik fragmenta = 64 zastavica *več fragmentov* = 0

- Sestavljanje paketov:
  - Za sestavitev datagrama potrebujemo vmesni pomnilnik.
  - Ko prispejo fragmenti z isto oznako, se njihovi podatki vstavijo na pravo mesto v vmesnem pomnilniku.
  - Vstavljanje poteka dokler ne vstavimo podatkov iz fragmenta z zastavico *več fragmentov* postavljeno na "neresnično".

Segmentacija in sestavljanje datagrama (6)

- Pri sestavljanju nastanejo težave, če nekaj fragmentov ne prispe na mesto sestavljanja datagrama.

  To se lahko zgodi, saj IP ne jamči dostave. Zato moramo določiti pogoj, kdaj se nepopolna sestava datagrama zavrže in s tem sprosti vmesni pomnilnik za druge potrebe. Pogoj določimo na enega od naslednjih načinov:

  1. Ob prispetju prvega fragmenta se določi življenjska doba sestavljanja. Če se ta izteče preden je datagram sestavljen, se sprejeti fragmenti zavržejo.
  2. Uporabi se podatek o življenjski dobi fragmenta, ki je zapisana v čelu okvira. Podatek o dobi se zmanjšuje ob prispetju vsakega fragmenta. Če se življenjska doba prvega fragmenta izteče preden je datagram sestavljen, se sprejeti fragmenti zavržejo.

Nadzor nad napakami

- Medomrežje - kot vemo - ne jamči uspešne dostave datagrama.
- Ko usmerjevalnik zavrže datagram, je zaželeno, da to sporoči pošiljatelju.

  To informacijo lahko omrežna entiteta v pošiljatelju izkoristi za spremembo strategije pošiljanja paketov in za obvestilo nadrejeni plasti o zavrženju datagrama.
- Datagrami so lahko zavrženi iz več razlogov:
  - zaradi poteka življenjske dobe,
  - zaradi odpravljanje zamašitev z zavrženjem paketov
  - Zaradi odkrite napake v paketu (tu ni mogoče poslati obvestila, ker je lahko napaka v naslovu pošiljatelja).

Krmiljenje podatkovnega prometa

- Krmiljenje prometa omogoča usmerjevalnikom in/ali končnim napravam – sprejemnim postajam, da omejijo hitrost sprejemanja podatkov.
- Pri brezpovezavnih storitvah imamo omejene možnosti krmiljenja pretoka podatkov.
- Najboljši način krmiljenja pri brezpovezavnih storitvah je pošiljanje posebnih krmilnih paketov usmerjevalnikom in pošiljateljem, ki zahtevajo zmanjšanje dotoka podatkov.

Protokol IPv4

- Protokol IP v4 (verzija 4) je sestavni del zbirke protokolov referenčnega modela TCP/IP.
- Je med najbolj razširjenimi protokoli za medomrežne povezave.
- Njegova funkcionalnost je zelo podobna ISO/OSI protokolu CLNP.
- IP je razdeljen na dva dela:
  1. Vmesnik do višje plasti (transportne ali aplikacijske plasti, na primer do protokolov TCP ali UDP), kjer so določene storitve, ki jih IP nudi.
  2. Protokoli in mehanizmi delovanja protokola IP.
- Z imenom IP zajamemo množico protokolov, ki omogočajo medomrežno povezavo. Med njimi je širše znan Internet Control Message Protocol (ICMP) znan po ukazih *ping*.

Storitve IP

- Vmesnik IP, ki povezuje omrežno plast z nadrejenimi plastmi, ima določena dva primitiva za zagotavljanje storite (Table 3):
  - Send: zahteva po pošiljanju podatkovne enote
  - Deliver: obvestilo o prispetju podatkovne enote

Tabela 3: Primitiva storitev IP in njihovi parametri

Send(	Deliver(
naslov pošiljatelja	naslov pošiljatelja
naslov prejemnika	naslov prejemnika
protokol	protokol
oznaka tipa storitve	oznaka tipa storitve
oznaka paketa	
oznaka "ne fragmentiraj"	
življenjska doba	
dolžina podatkov	dolžina podatkov
opcijski podatki	opcijski podatki
podatki	podatki
)	)

Storitve IP (2)

- Parametri primitivov imajo naslednji pomen:

Naslov pošiljatelja	Medomrežni naslov entitete, ki pošilja datagram
Naslov prejemnika	Medomrežni naslov entitete, kateri je datagram namenjen.
Protokol	Protokol, ki ga mora imeti prejemnik sporočila.
Oznaka paketa	Skupaj z naslovom pošiljatelja in prejemnika in z oznako protokola (enoznačno) označi posamezen poslan okvir (ta podatek se potrebuje pri sestavi paketa iz fragmentov in pri javljanju napak).
Ne fragmentiraj	Oznaka pove, kdaj nadrejena identiteta dovoljuje IP razstaviti (fragmentirati) podatke v manjše dele – fragmente, ki so bolje prilagojeni prenosu.
Življenjska doba	Meri se v številu etap, ki jih lahko paket preide. Po izteku življenjske dobe se paket zavrže.
Dolžina podatkov	Dolžina podatkov v oktetih, ki bodo poslani.

Storitve IP (3)

Opcijski podatki Opcije, ki jih zahteva uporabnik IP (nadrejena entiteta, aplikacija).

Podatki Uporabnikovi podatki, ki jih želi poslati

- Pošiljatelj s *tipom storitev* določi eno ali več storitev:

  prednost *precedence* Mera relativne pomembnosti datagrama. Določenih je osem osem nivojev prednosti (prioritet). IP bo skušal zagotoviti izbrani način obravnave paketa za bolj pomembne datagrame.

  zanesljivost *reliability* IP ima dva nivoja zanesljivosti: normalno in visoko. Visoka zanesljivost zahteva, da mora biti minimizirana možnost izgube ali oškodovanja tega datagrama.

  zakasnitev *delay* Določena sta dva nivoja zakasnitve: normalna in mala. Pri mali zakasnitve se zahteva minimizacija zakasnitve pri dostavi datagrama.

Storitve IP (4)

prepustnost — Določena sta dva nivoja: normalna in visoka prepustnost.

throughput — Visoka prepustnost zahteva maksimiranje prepustnost za tako označen datagram.

- Ti parametri se lahko uporabljajo kot pomoč pri odločanju v usmerjevalnikih.

  Na primer, če ima usmerjevalnik na voljo več alternativ za naslednjo etapo datagrama, lahko izbere etapo s storitvijo *prepustnost* postavljeno na visoko.

- Parametri so lahko namenjeni tudi nižjim plastem.

  Na primer, če je izbran nivo *pomembnosti* ali *prioritete* in omrežje nudi različne prioritetne nivoje (na primer omrežja Token ring in Token bus), se nivo pomembnosti preslika v prioritetne nivoje podomrežja.

- Opcijski parametri so namenjeni za bodoče razširitve in za vključevanje parametrov, ki se običajno ne uporabljajo. Trenutno so definirane naslednje opcije

Storitve IP (5)

Varnost *Security*
Dovoljujejo, da je datagramu pripeta varnostna labela.

Usmerjanje iz vira *Source routing*
Vsebuje seznam naslovov usmerjevalnikov, skozi katere naj potuje datagram.

Usmerjanje ja lahko striktno (dovoljena je le navedena pot) ali ohlapno (dovoljujejo tudi druge poti).

Zapisovanje usmerjevalnikov *Route recording*
Datagramu je dodano je polje, v katero se zapisuje zaporedje naslovov usmerjevalnikov, skozi katere je potoval datagram.

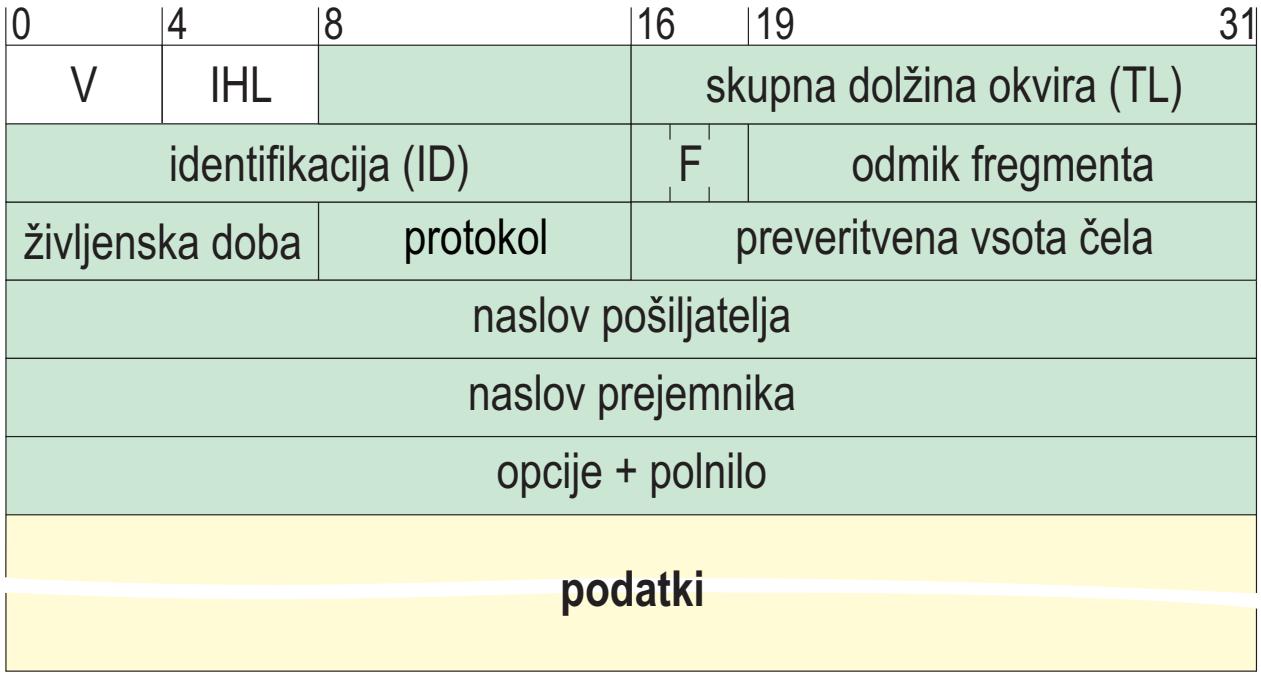
Oznaka toka podatkov *Stream identification*
Rezervira prenosne zmogljivosti. Ta storitev zagotovi posebno obravnavo za periodični promet (na primer prenos zvoka).

Storitve IP (6)

Časovno označevanje
Time stamping

Entiteta IP v viru, nekateri ali vsi usmerjevalniki, ki jih datagram preide, vpišejo čas (do mili sekunde natančno), kdaj so posredovali datagram naprej.

Omrežni protokol



Slika 3.17: Podatkovna enota pri protokolu IPv4.

Verzija (*V*) (4 bite) Označuje verzijo protokola. S tem je omogočen nadaljnji razvoj protokolov.

Omrežni protokol (2)

Dolžina čela IP (*IHL*) (4 bite) Dolžina čela, podaja se v 32-bitnih besedah. $\text{IHL}_{\text{min}} = 5 \Rightarrow$ dolžina čela: 20 oktetov.

Tip storitve (*ToS*) (8 bitov) Določa parametre storitve: *zanesljivost*, *pomembnost*, *zakasnitev* in *prepustnost*.

Skupna dolžina (*TL*) (16 bitov) Skupna dolžina datagrama, v oktetih.

Oznaka paketa (*ID*) (16 bitov) Zaporedna številka, ki skupaj z naslovoma pošiljatelja in prejemnika ter oznako protokola omogoči enolično razlikovanje datagramov v času, ko so v medomrežju.

Zastavice (*F*) (3 biti) Zaenkrat sta določeni dve zastavici:

- *ne fragmentiraj*: daje dovoljenje za razdelitev datagrama na fragmente,
- *več fragmentov*: paketu sledi še en ali več paketov s fragmenti datagrama.

Omrežni protokol (3)

Odmik fragmenta (*FO*) (13 bitov) Označuje odmik začetka podatkov v fragmentu od začetka podatkov v datagramu.

Odmik se meri v 64-bitnih besedah. Zato so lahko dolžine podatkov v vseh razen zadnjem fragmentnem paketu mnogokratnik 64 bitov.

Življenjska doba (*TtL*) (8 bitov) Določa, kako dolgo lahko paket potuje po internetu. Meri se v številu prepotovanih etap.

Protokol (8 bitov) Označuje naslednji višji protokol, ki sprejme podatke v podatkovnem polju.

Preveritvena vsota (16 bitov) Algoritem preveritve sešteje (v eniškem komplimentu) predhodne 16-bitne besede. Pri izračunu vsote polje vsebuje ničle.

Ker usmerjevalniki lahko spremenijo vsebino polj pred preveritveno vsoto, jo morajo pri spremembi čela ponovno izračunati.

Omrežni protokol (4)

Naslov pošiljatelja (32 bitov) Naslov sestavljata *naslov podomrežja*, kjer se vir nahaja in *naslov naprave* končnega uporabnika.

Naslov prejemnika (32 bitov) Enako kot pri naslovu pošiljatelja.

Opcije Dolžina polja je spremenljiva. V njega uporabnik, ki pošilja datagram, zapiše zahtevane opcije.

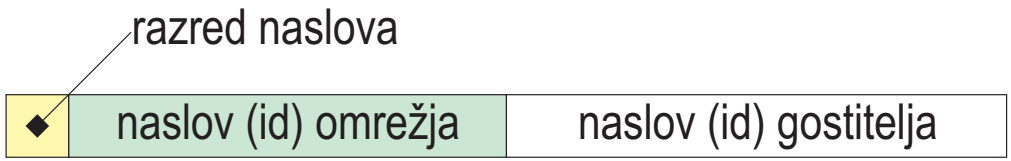
Polnilo To polje zapolnimo z zaporedjem 0 in 1 tako, da je dolžina čela mnogokratnik 32-bitne besede.

Podatki Podatkovno polje je spremenljive dolžine. Ta je določena z razliko med skupno dolžino datagrama in dolžino čela. Maksimalna dolžina je 64k oktetov.

Podatkovno polje vsebuje datagram hierarhično višjega protokola.

Formati naslovov

- Vsaki priključek na medomrežje ima svoj individualni naslov.
- Naslovi so strukturirani, določajo jih 32-bitne številke.



Slika 3.18: Splošna zgradba internetnega naslova.

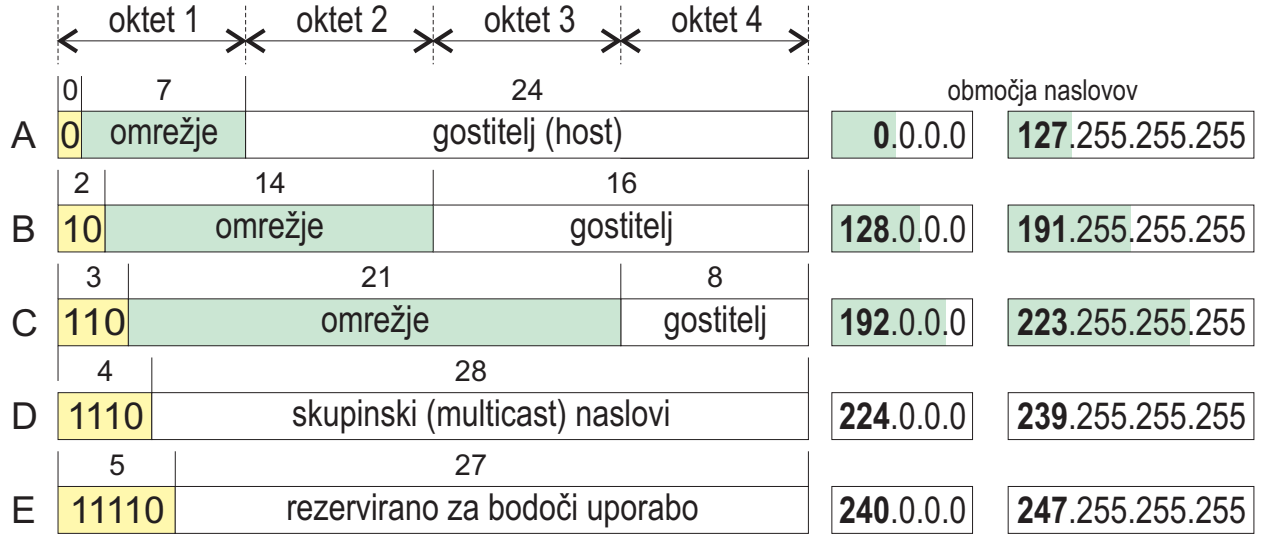
- Naslovi so razdeljeni v pet razredov (Fig. 3.18) in dve družini:
- posamezni ali unicast naslovi:
  - Razred A Sisteme z malo podomrežij in veliko napravami.
  - Razred B Sistemi s približno enako podomrežij in naprav.
  - Razred C Sisteme z veliko podomrežij in malo naprav.
- skupinski ali multicast naslovi:

Formati naslovov (2)

Razred D Skupinski naslovi.

- in

Razred E Naslovi rezervirani za bodočo uporabo.



Slika 3.19: Formati naslovov. Na desni strani slike so “pika decimalni” zapisi naslovov.

Formati naslovov (3)

- Administracija naslovov:
  - *Internet Network Information Center* (InterNIC) vodi evidenco le za naslove omrežij. Za naslove naprav je zadolžen sistemski administrator omrežja.
  - InterNIC je bil ustanovljen 1.aprila 1993. Pred tem je za Interenet naslove (in DNS imena) skrbela administracija NIC, ki sedaj skrbi le še za naslove v *Defense Data Netvork* (DDN) v medomrežju ameriškega obrambnega ministrstva.
  - Uporabniki Interenta se lahko registrajo pri InterNIC na naslovu

    `rs.interniv.net`

    , direktorij in bazo naslovov dobijo na

    `ds.internic.net`

    ter informacije na naslovu

    `is.internic.net`

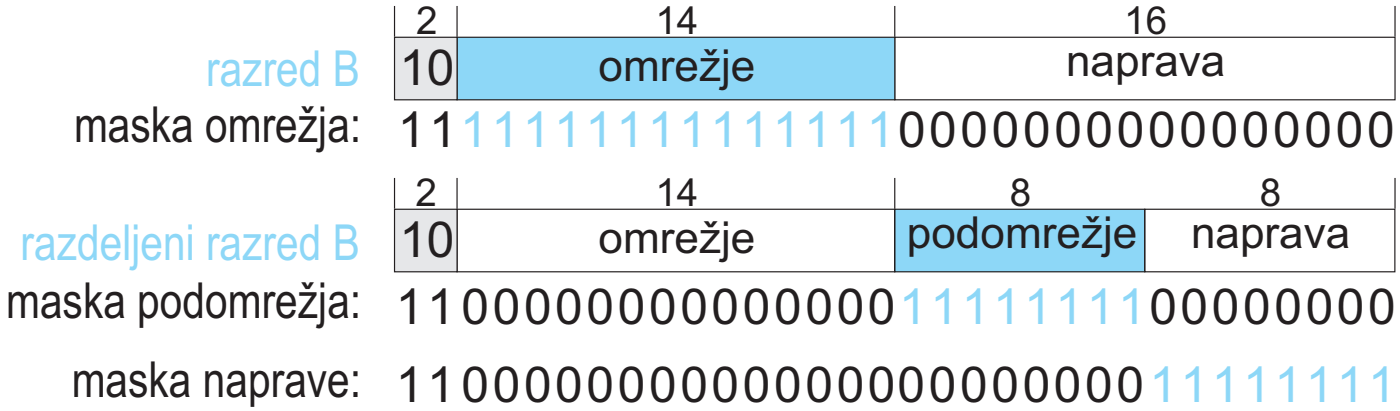
Naslavljanje podomrežij

- Danes so mnoga lokalna omrežja razdeljena na podomrežja, zato delitev naslovov IP le na razrede A, B in C ne zadošča.
- Podomrežja v lokalnih omrežjih omogočajo izolacijo prometnih tokov znotraj skupne uporabnikov. S tem se zmanjša nevarnost prometne poplave, v omrežjih.
- Ta delitev zahteva, da lokalni administrator vpelje dodatno polje v naslov, v katerem je zapisan naslov podomrežja.
- Dobro izhodišče tej strategiji je razred B (Fig. 3.20).

Slika 3.20: Delitev naslovov naprav v razredu B na naslove podomrežij in naslove naprav.

Maskiranje naslovov

- Ob vključevanju mora naprava (z)vedeti za strukturo naslova.
- Razlikovanje med naslovi omrežja, podomrežja in naprave omogoča naslovna maska.
- Naslovna maska je 32 bitni vzorec (Fig. 3.21).



Slika 3.21: Maska omrežja pri naslovih razreda B.

Maskiranje naslovov (2)

- “pika-decimalni” zapis mask:

```
255.255.0.0          maska omrežja
0.0.255.0            maska podomrežja
0.0.0.255            maska naprave
```

- šestnajstiški zapis mask (tu je ločilo dvopičje):

```
FF:FF:00:00          maska omrežja
00:00:FF:00          maska podomrežja
00:00:00:FF          maska naprave
```

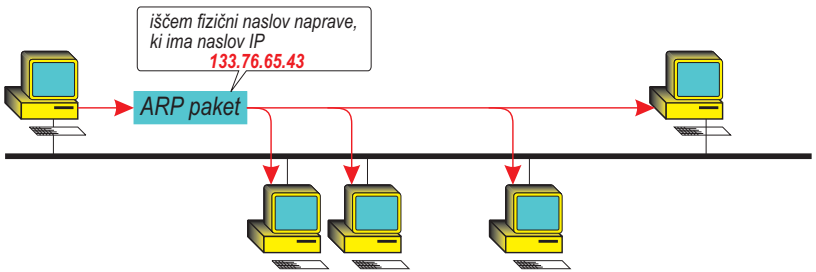
- S poznavanjem omrežne in podomrežne maske in naslova prejemnika lahko naprave enoumno določijo, ali sta prejemnik in pošiljatelj v istem podomrežju ali omrežju.

DNS, ARP in RARP

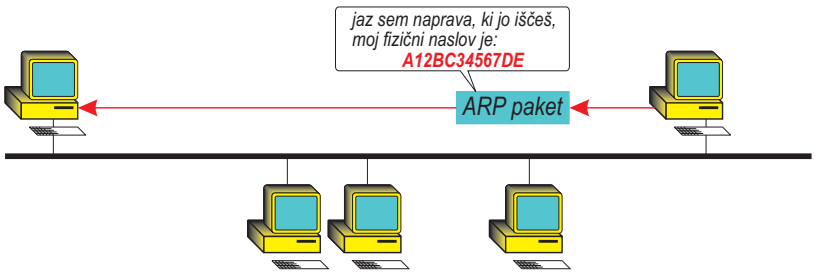
DNS (*Domain Name System*) je porazdeljena baza imen naprav, ki so priključene v neko (pod)omrežje. Ta baza preslika številčne naslove v imena naprav.

ARP (*Address Resolution Protocol*) poišče napravi z naslovom IP pripadajoči fizični naslov.

RARP (*Reverse Address Resolution Protocol*) omogoča gostitelju, da znanemu fizičnemu naslovu poišče pripadajoči naslov IP.



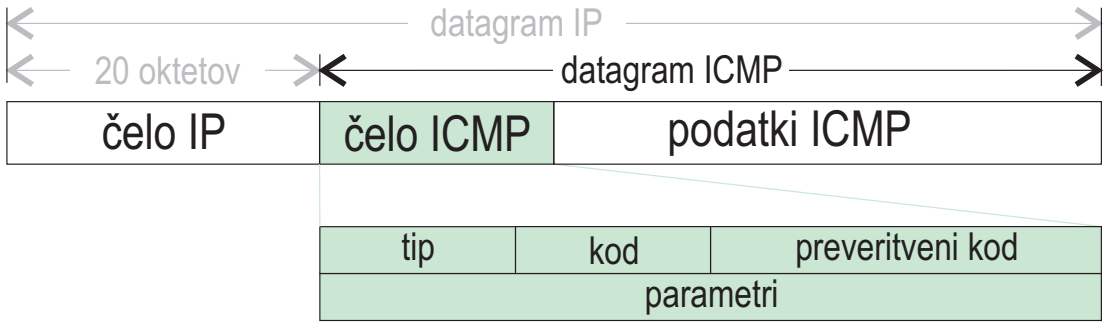
Slika 3.22: ARP: zahteva.



Slika 3.23: ARP: odziv.

ICMP

- ICMP je omrežni protokol, hierarhično nad IP (Fig. 1.9).
- Namenjen je sporočanju napak, ki se zgodijo pri prenosu paketov skozi omrežje ali medomrežje in za informiranje uporabnikov o stanju v medomrežju.
- S temi sporočili lahko upravljamo delovanje omrežij in medomrežij. Specifikacije ICMP so v RFC 792.
- Za prenos krmilnih sporočil ICMP uporablja IP (Fig. 3.24).



Slika 3.24: Datagram IP z ICMP.

ICMP (2)

- Vsa sporočila ICMP se prično s 64-bitnim čelom, v katerem so naslednja polja:

  Tip (en oktet) Določa vrsto sporočila ICMP.

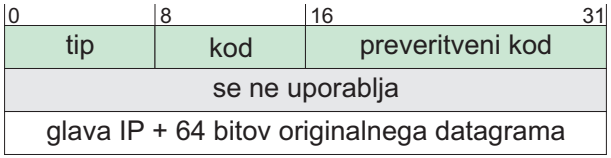
  Kod (en oktet) Določita parametre sporočila. Ti so lahko zapisani z enim ali več biti.

  Preveritveni kod (dva okteta) Vsebuje preveritveni kod celega sporočila. Uporablja enak algoritem kot IP.

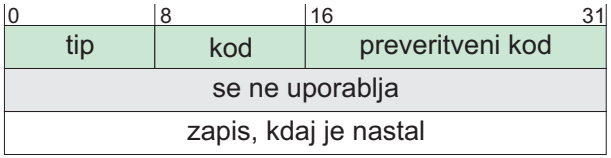
  Parametri (štirje okteti) Uporablja se za zapis daljših parametrov.

- Čelu sledi sporočilo spremenljive dolžine (Fig. 3.25).

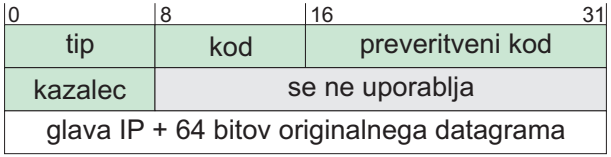
ICMP (3)



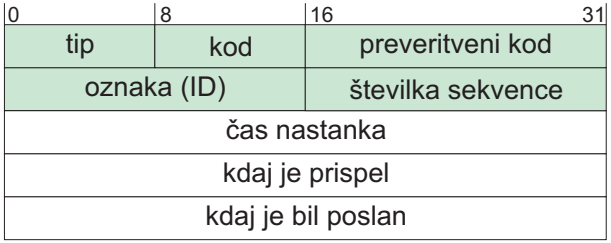
a: Destinacija ni dosegljiva, potekel je čas dostave



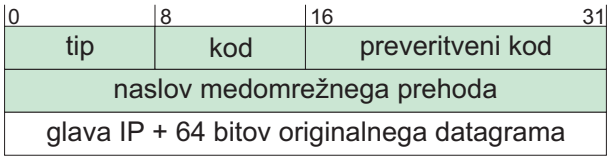
e: Označevanje (zapis) časa



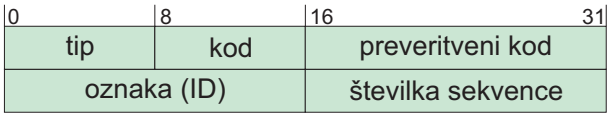
b: Problemi s parametri



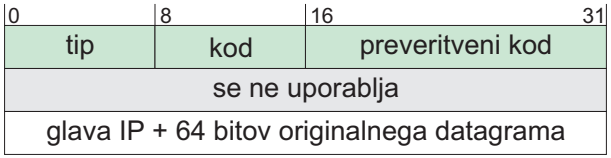
f: Odgovor s časovnim označevanjem



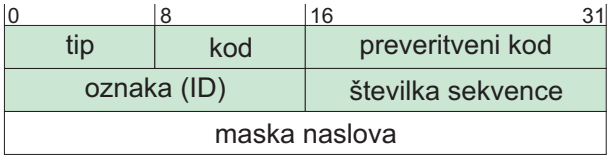
c: Preusmerjanje



g: Zahteva maskiranja



c: Odmev, odgovor na odmev



h: Odgovor na zahtevo maskiranja

Slika 3.25: Sporočila ICMP s formati njihovega zapisa.

ICMP sporočila

- *prejemnik nedosegljiv*
  - usmerjevalniki:
    - določena končna naprava ni dosegljiva.
    - čelo datagrama je nepravilno nastavljeno. (na primer, postavljena je zastavica *ne fragmentiraj*, usmerjevalnik pa bi moral izvesti segmentacijo datagrama.
    - datagram vsebuje instrukcije usmerjanja, pa specificirana pot od njega dalje ne obstaja.
  - končne naprave prejemnika:
    - nadrejeni protokol ni dosegljiv
    - dostopna točka storitve v višji plasti je nedosegljiva.
- *potek časa*
  - usmerjevalniki:
    - življenjska doba datagrama je potekla.
  - končne naprave prejemnika:
    - ni možno sestaviti originalni datagram.

ICMP sporočila (2)

- *Parametrski problemi*

  Vzrok sporočilu so sintaksne ali semantske napake v čelu IP. Na primer, v opcijah je zapisan nepravilni argument. Mesto, kjer je bila napaka odkrita, je v sporočilu označeno s kazalcem, ki je vpisan v polje parametrov.

- *Upočasnjevanje vira*
  - Usmerjevalnik ali končni uporabnik zahtevata zmanjšanje hitrosti pošiljanja datagramov. Ko vir sprejme to sporočilo, zmanjša hitrost oddajanja za določen delež.
  - Uporabi se lahko za obvestilo, da je bil zavržen datagram (ker je bil poln vmesni pomnilnik v usmerjevalniku).

- *Preusmerjanje*

  Pošlje usmerjevalnik, ki je direktno povezan z virom. Z njim svetuje viru boljšo pot do želenega prejemnika datagrama.

ICMP sporočila (3)

- *Odmev in odgovor na odmev*
  - Testira komunikacije med dvema možnima entitetama.
  - To sporočilo uporabimo pri znanem ukazu *ping*, s katerim preverjamo prisotnost določene naprave v omrežju.
  - Prejemnik sporočila *odmev* ogovori s sporočilom *odgovor na odmev*.
    - Oznaki in zaporedni številki sporočil *odmev* in *odgovor na odmev* se mora ujemati.
    - Oznako sporočila se lahko uporabi kot dostopno točko do storitve, zaporedno številko pa se običajno inkrementira po vsakem pošiljanju odgovora na odmev.
- *Zahteva maske in odgovor na zahtevo*

  Zahteva po naslovni maski in odgovor nanjo omogoči napravi, da se nauči naslovne maske lokalnega omrežja, na katero je priključena.
  - Naprava pošlje vsem v lokalnem omrežju zahtevo po maski.
  - Usmerjevalniki se odzovejo z *odgovor na zahtevo po maski*, v katerem zapišejo naslovno masko.

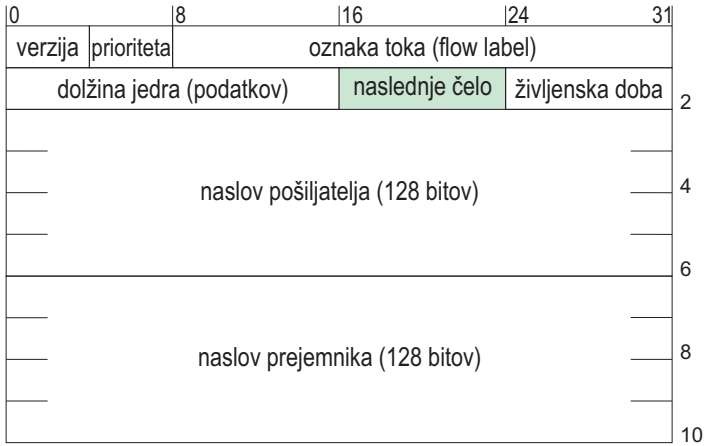
Internet protokol IPv6

- Največja pomanjkljivost protokola IPv4 je pomanjkanje naslovnega prostora in neorganizirano dodeljevanje naslovov.
- Ti pomanjkljivosti sta bili gonilna sila razvoja protokola “nove generacije” IPng = IPv6.
- Razvoj IPv6 vodi organizacija IETF (Internet Engineering Task Force).
- Glavne izboljšave IPv6 protokola:
  - razširjene naslovne in povezovalne zmogljivosti,
  - novi načini naslavljanja - anycast,
  - poenostavitve okvirja,
  - izboljšana podpora za dodatne opcije,
  - zagotavljanje kakovosti storitev,
  - zagotavljanje zaupnosti in preverjanje pristnosti.

Primerjava IPv4 in IPv6

- Čelo datagrama IPv6 je v primerjavi z datagramom IPv4:
  - preprostejše zgradbe
  - fiksne dolžine (40 zlogov)
  - manj polj v čelu – IPv4: 14, IPv6: 8.

Slika 4.26: Čelo datagrama pri IPv4.



Slika 4.27: Čelo datagrama pri IPv6.

- V IPv6 so opuščena ali preimenovana naslednja polja:
  - *dolžina čela (IHL)* – zaradi fiksne dolžine čela IPv6 ni več potrebno.

Primerjava IPv4 in IPv6 (2)

- *dolžina celotnega paketa* – je nadomeščena z *dolžina jedra*. Določa dolžina podatkov, ki jih je lahko 64 k zlogov.
- *življenjska doba* so preimenovali iz *time-to-live* v *hoop-limit*, vendar ima isto vlogo.
- *type of service* sta prevzela dve novi polji:
  - *prioriteta*
  - *oznaka toka*.

  Obe polje se uporabljata za zagotavljanje kvalitete servisa in rezervacijo sredstev v usmerjevalnikih na komunikacijski poti.
- *preveritev čela* je izpuščeno, ker imajo vsi višje in nižje ležeči protokoli lastno preverjanje pravilnosti podatkov. Zato je preveritveni kod v čelu IP nepotreben.
- *odmik, oznaka in zastavice* so v čelu IPv6 izpuščena. Njihove funkcije so prevzela posebna razširitvena čela.

Primerjava IPv4 in IPv6 (3)

Pri današnjih komunikacijskih povezavah je maksimalna velikost paketa fizične plasti statistično večja od aplikacijskih zahtev. Zato je odločitev za odstranitev teh polj iz IP okvirja in dodajanje posebnega opcijskega okvirja, smotrna.

- *opcije + polnilo*. V IPv6 so vse dodatne možnosti rešene z razširitvenimi okvirji.

  Opcije se v IPv4 le malo koristijo (za izvirno usmerjanje, varnost in podobno), zato so skupaj z mašilom glavna režija (overhead) pri prenosu podatkov.
  Določenim funkcijam, kot so varnost, avtentičnost in podobno, je bila pri razvoju IPv6 dana posebna pozornost. Za njih so uvedeni dodatna čela, ki te probleme rešujejo bolj učinkovito.

Razširitveni okvirji

- V IPv6 so za razne opcije predvideni razširitvena čela, ki v primeru uporabe sledijo čelu IP v zapisanem vrstnem redu:

  Hop-by-Hop options *čelo z etapnimi opcijami*
  Vsebuje informacije, ki jih mora, če je čelo prisotno, preveriti vsak usmerjevalnik na poti datagrama.

  Destination options *čelo z opcijami za vmesne cilje*
  Vsebuje opcije, ki se obdelajo v prvem cilju datagrama, ki je zapisan v naslovu prejemnika in nato zaporedoma v vseh destinacijah naštetih v čelu usmerjanja.

  Routing *čelo za usmerjanje*
  vsebuje navodila za usmerjanje datagrama skozi medomrežje.

  Fragmentation *fragmentarno čelo* vsebuje informacije, kako je pošiljatelj razdrobil originalni datagram v fragmente.

Razširitveni okvirji (2)

Authentication *čelo za avtentikacijo*

Vsebuje informacije o avtentičnosti pošiljatelja

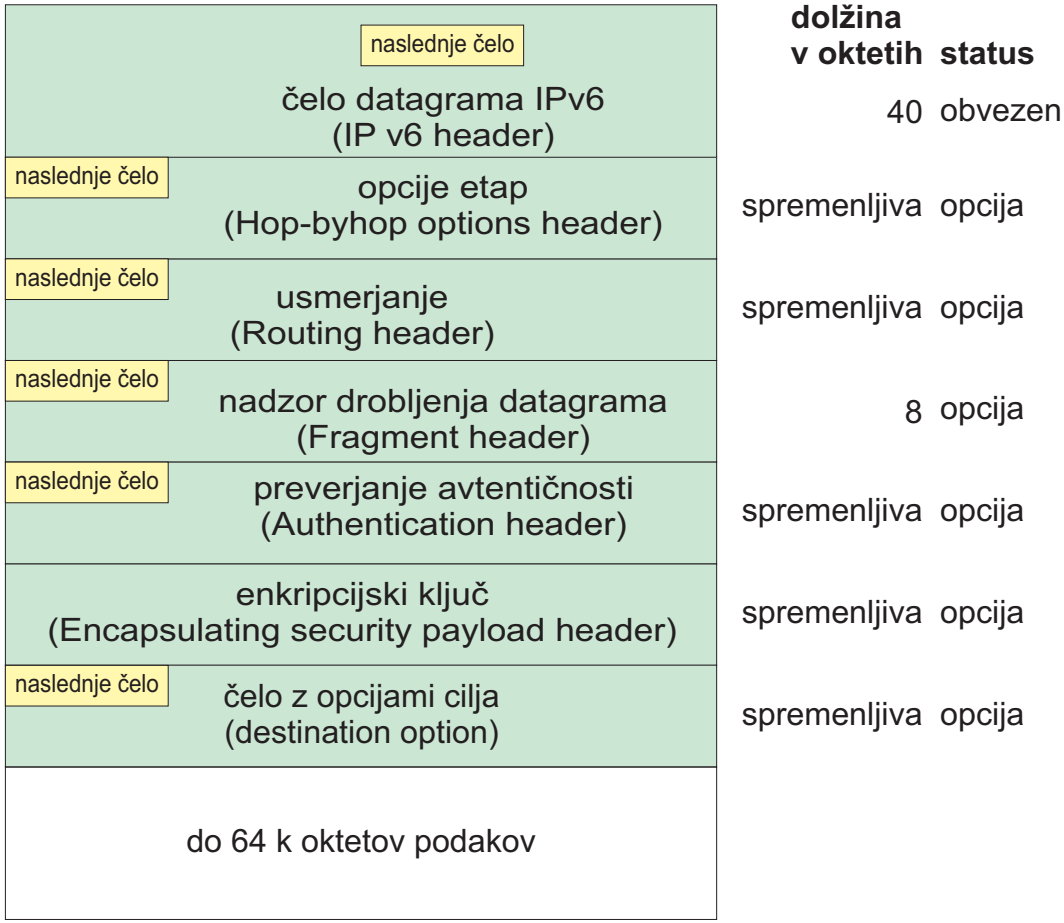
Encryption *čelo za kriptografsko zaščito*

vsebuje javni ključ zaščite podatkov

Destination options *čelo z opcijami za končni cilj*

Vsebuje opcije, ki se obdelajo samo v končnem cilju datagrama.

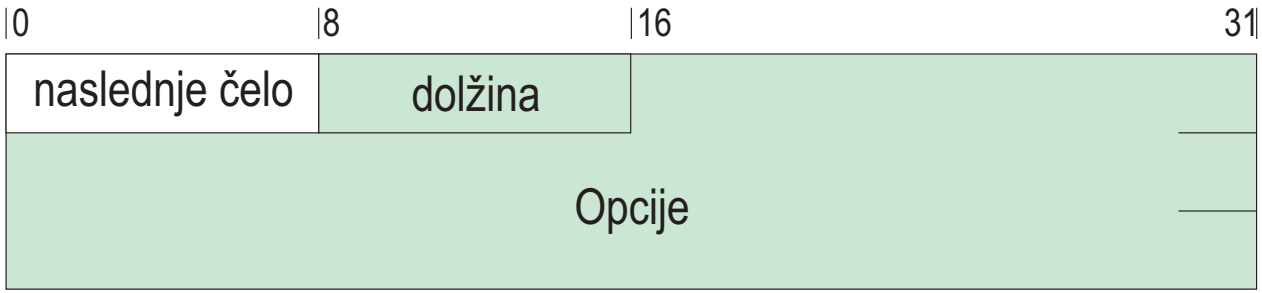
Razširitveni okvirji (3)



Slika 4.28: Zaporedje razširitvenih čel.

Etapno razširitveno čelo

- Informacije v etapnem čelu mora preveriti vsaka naprava na komunikacijski poti paketa. Sestavljajo ga tri polja (Fig. 4.29):



Slika 4.29: Zgradba etapnega čela (Hop-by-Hop Header).

naslednje čelo (8 bitov), pove tip naslednjega čela

dolžina čela (8 bitov), dolžina čela je podana 64 bitnih enotah

opcije polje nastavljive dolžine vsebuje eno ali več opcijskih določil. Vsako določilo ima tri podpolja:

1. tip opcije (8 bitov)
2. dolžina podatkov opcije (8 bitov)

Etapno razširitveno čelo (2)

3. podatki

- Tip opcije je razdeljen v tri dele:
  1. spodnjih 5 bitov določa opcijo,
  2. Zgornja 2 bita določata akcijo, če naprava ne prepozna opcije:

     00 preskoči to opcijo in nadaljuje z obdelavo ostalih opcij

     01 zavrži paket

     10 zavrži paket in z ICMP pošlji na naslov pošiljatelja sporočilo “problem s parametri” (koda 2) z označbo “neznan tip opcije”

     11 zavrži paket in z ICMP pošlji na naslov prejemnika, če ta ni skupinski, sporočilo “problem s parametri” (koda 2) z označbo “neznan tip opcije”

  3. tretji bit določa, ali se poti med pošiljateljem in prejemnikom datagrama lahko spremijo podatki opcij.
- Do leta 1997 je bila definirana le ena opcija: *jumbo payload* – orjaški paket, daljši od $2^{16} = 65\,536$ oktetov.

Etapno razširitveno čelo (3)

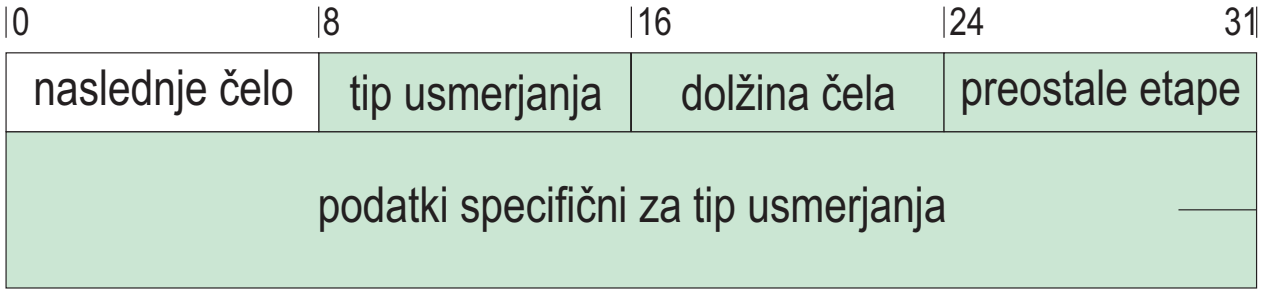
- V primeru te opcije:
  1. podatek v opciji določa dolžino podatkov v datagramu,
  2. najdaljši orjaški datagram je dolg okoli 4 milijarde, oktetov podatkov, kar zadošča za prenos zelo velike video datoteke,
  3. v dolžino podatkov v čelu IP so zapisane ničle in
  4. prepovedana je uporaba fragmentacijskega čela.

Čelo usmerjanja

- Čelo usmerjanja omogoča pošiljatelju datagrama določitev poti preko točno določenih naprav v medomrežju.

  Zato se za to čelo v angleški literaturi uporablja tudi ime Source Routing.

- Generična oblika čela ima določena naslednja polja (Fig. 4.30):



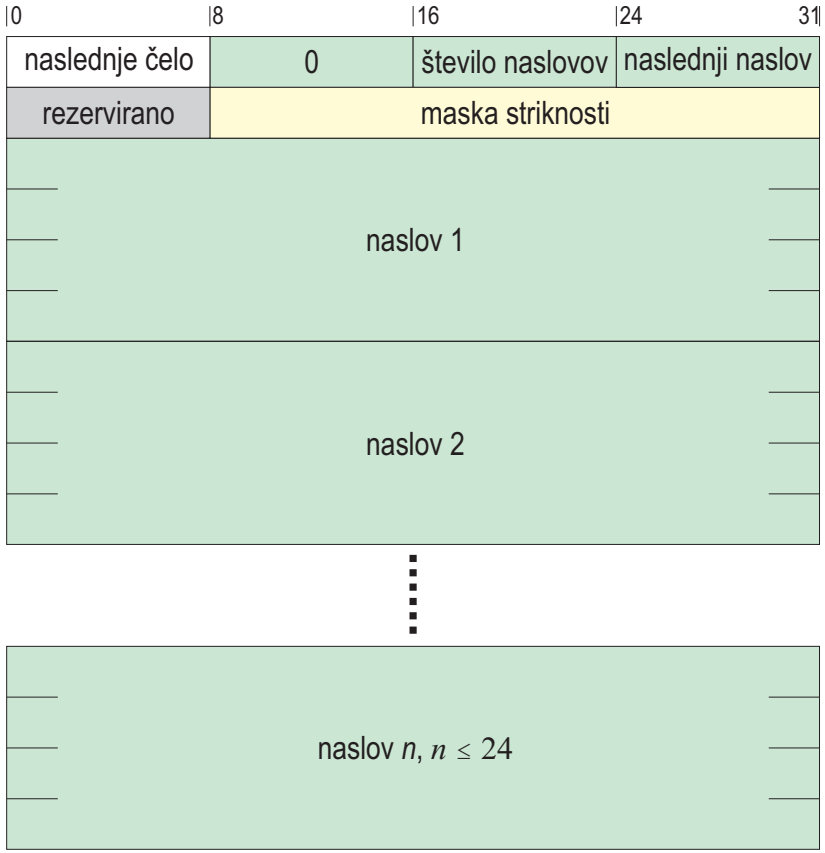
Slika 4.30: Splošna zgradba čela usmerjevanja.

Čelo usmerjanja (2)

naslednje čelo	(8 bitov), pove tip naslednjega čela
tip usmerjanja	(8 bitov), določa tip usmerjanja
dolžina čela	(8 bitov), določa število naslovov v čelu
preostale etape	(8 bitov), vsebuje število etap, ki jih mora datagram še “prehoditi” do končnega cilja
rezervacija	(32 bitov), za bodočo uporabo
podatki usmerjanja	(dolžina odvisna od tipa usmerjanja), specifični za tip usmerjanja

- Če usmerjevalnik ne prepozna tip usmerjanja, paket zavrže
- Do sedaj je bil definiran le tip usmerjanja “0”. Določa naslednja polja (Fig. 4.31):

Čelo usmerjanja (3)



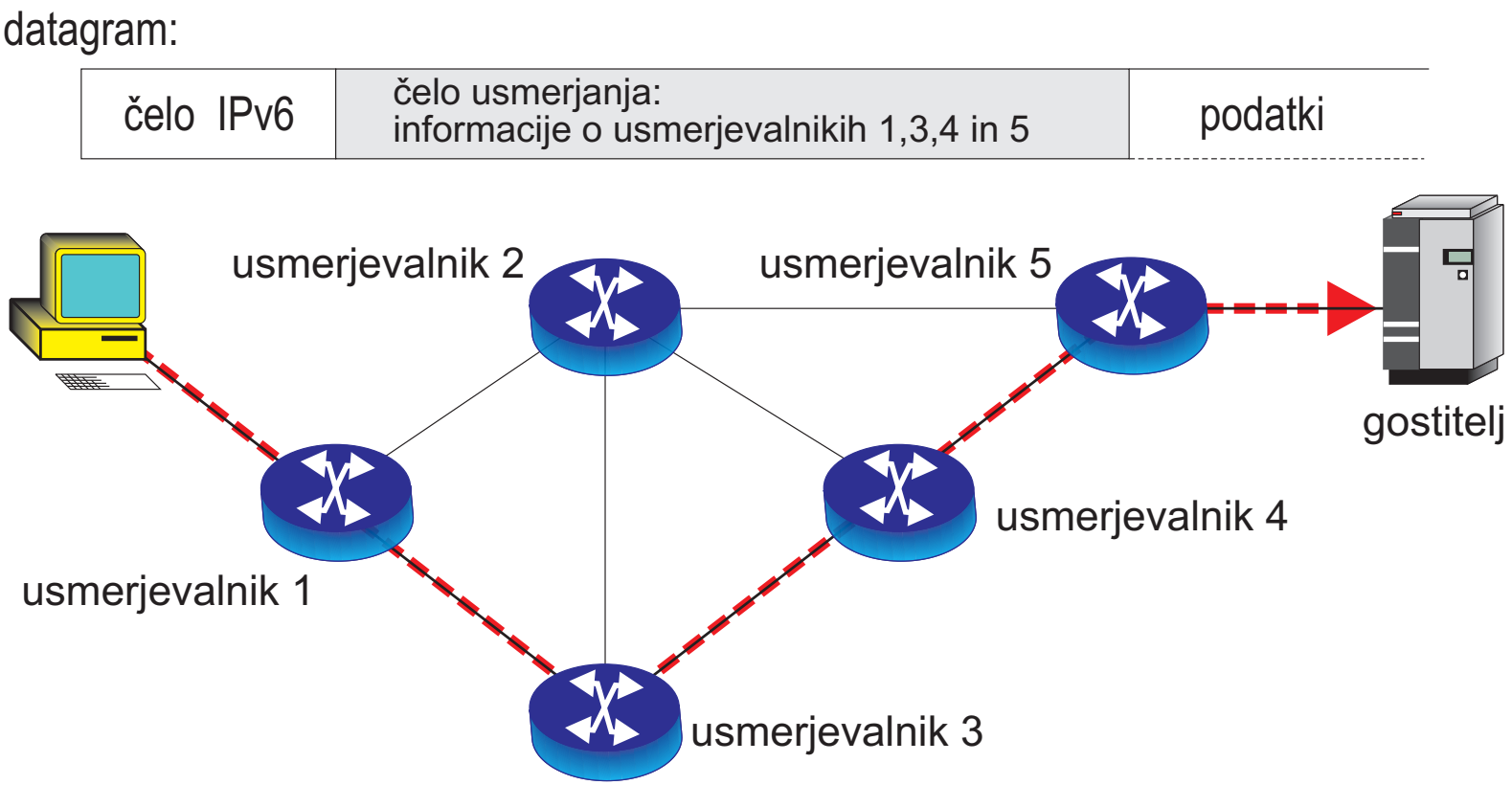
Slika 4.31: Splošna zgradba čela usmerjevanja pri usmerjanju skozi n usmerjevalnikov.

Število naslovov (8 bitov), dolžino čela izrazi s številom zapisanih naslovov. V enem čelu jih je lahko največ 23.

Čelo usmerjanja (4)

naslednji naslov	(8 bitov) vsebuje indeks naslednjega naslova, pošiljatelj ga postavi na nič.
rezervacija	(8 bitov), ni definirano
maska striktnosti	(24 bitov), bitu maske od leve proti desni označujejo zaporedne naslove usmerjevalnikov. Lega bitov od leve proti desni označuje zaporedne naslove usmerjevalnikov in predpisuje, ali je naslov naslednjega cilja datagrama sosed predhodnemu naslovu (1: mora biti, 0: ni nujno)
naslov	(128 bitov) vsebuje naslov usmerjevalnika, ki ga datagram mora preiti.

Čelo usmerjanja (5)



Slika 4.32: Primer uporabe čela usmerjanja.

- striktno usmerjanje

Čelo usmerjanja (6)

- v maski so z 1 označeni vsi naslovi usmerjevalnikov na poti datagrama
- če se na poti vrine nov usmerjevalnik, ki ni naveden v čelu usmerjanja, datagram ne pride na cilj
- primer striktnega usmerjanja kaže slika 4.32.

- ohlapno usmerjanje
  - v maski striktnosti je z 0 označenih (vsaj nekaj) naslovov usmerjevalnikov na planirani poti datagrama
  - datagram zato lahko preide vse navedene usmerjevalnike, lahko pa potuje tudi preko nenapovedanih

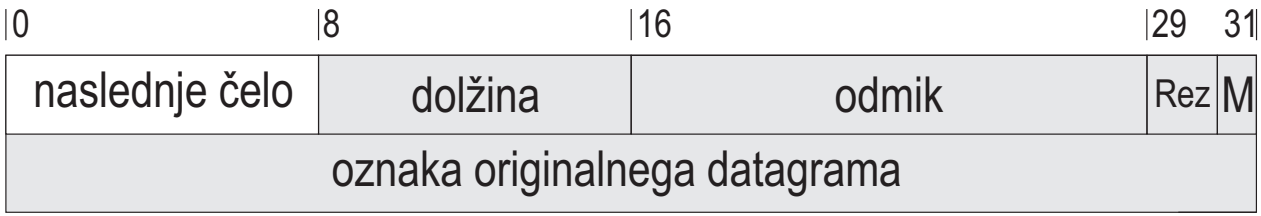
    Na primer, da sta striktno navedena na poti le usmerjevalnik 1, 4 in 5, usmerjevalnik 3 pa je ohlapno naveden (Fig. 4.32). V tem primeru bo v normalnih okoliščinah datagram potoval po označeni poti 1-3-4-5, v primeru izpada usmerjevalnika 3, pa bo ubral pot 1-2-4-5

Fragmentacijsko čelo

- Pri IPv6 vir datagrama, pri izvedenem drobljenju datagrama, s fragmentacijskim čelom prejemnika obvesti, da okviri, ki jih pošilja, vsebujejo fragmente datagrama.

  Ker fragmentacijo datagramov vrši pošiljatelj paketov, so usmerjevalniki razbremenjeni tega opravila. Zato se znatno poveča njihova prepustnost (hitrost usmerjevanja).

- Zgradba čela (Fig. 4.33):



Slika 4.33: Zgradba fragmentacijskega čela.

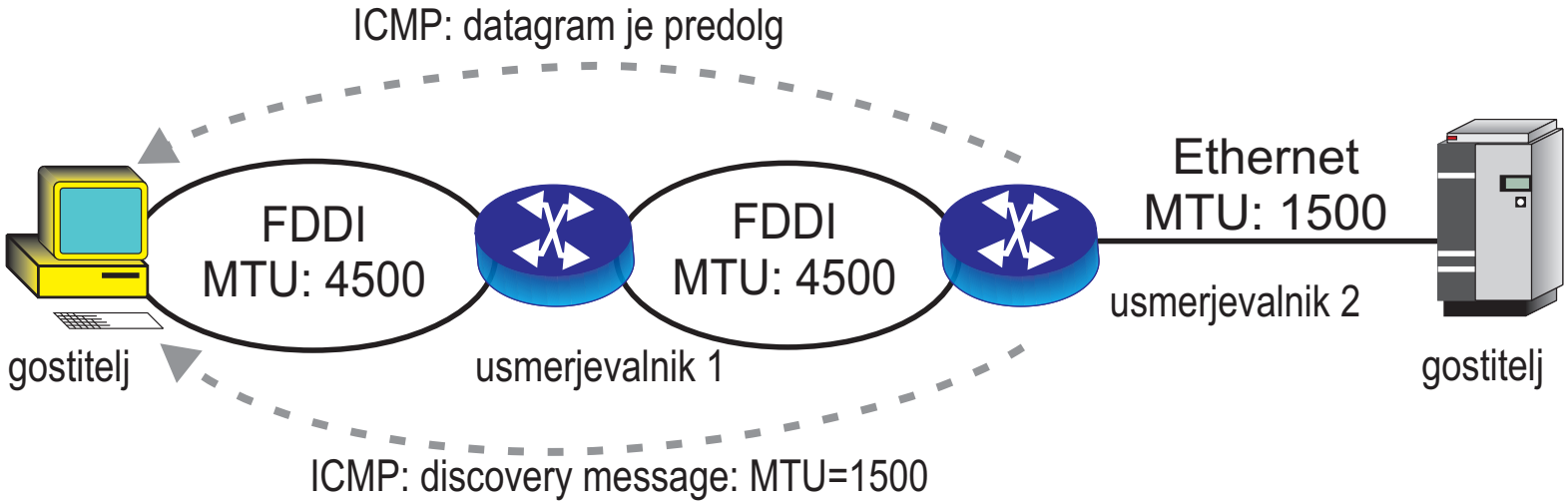
naslednje čelo (8 bitov), pove tip naslednjega čela

Fragmentacijsko čelo (2)

Rezervirano	(8 bitov), polje je rezervirano za bodočo uporabo
odmik fragmenta	označuje, kje se podatki v fragmentu začenjajo v originalnem datagramu. Odmik merimo v 64 bitnih enotah, zato so podatki – z izjemo zadnjega fragmenta – lahko dolžine enaki mnogokratniku 64 bitov.
Rez	(2 bita), rezervirana bita za bodočo uporabo
zastavica M	(1 bit): 1: sledi še en fragment, 0: zadnji fragment
oznaka	enoumno označi – identificira – originalni datagram. Oznaka mora biti v času, ko je/bo paket v (med)omrežju edinstvena za naslov pošiljatelja in prejemnika.

Fragmentacijsko čelo (3)

- *Primer drobljenja datagrama* (Fig. 4.34):



Slika 4.34: Drobljenje okvirov v IPv6.

- Drobljenje datagrama se izvrši glede na najmanjšo vrednost *Maximum Transmission Unit* (MTU) podomrežja, ki je na poti datagrama.
- Pošiljatelj pošlje prvi paket dolg 4500 oktetov (omejitev omrežja FDDI, na katerega je priključen).
- Ta paket usmerjevalnik 1 lahko posreduje preko podomrežja FDDI usmerjevalniku 2.

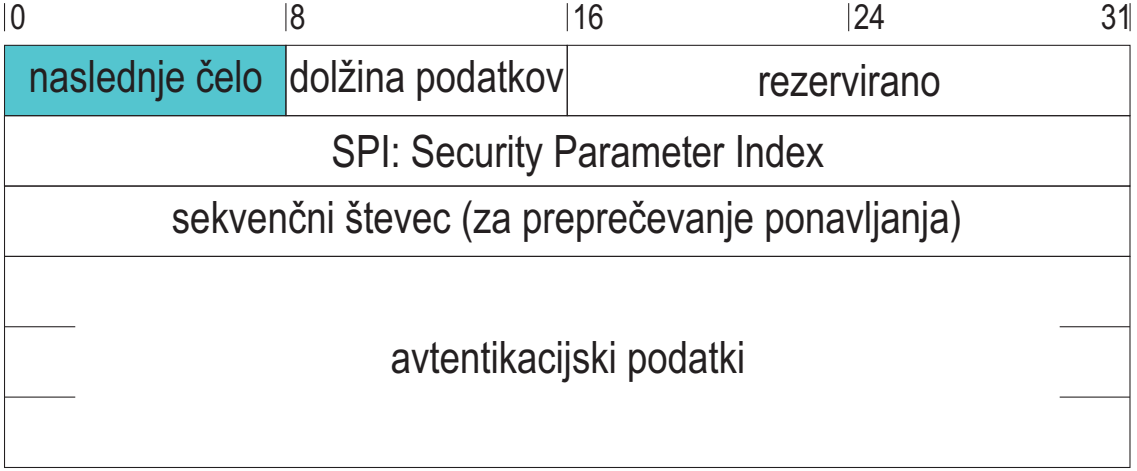
Fragmentacijsko čelo (4)

- Usmerjevalnik 2 ve, da ima omrežje Ethernet omejitev MTU = 1500 oktetov, zato:
  - zavrže datagram
  - pošiljatelju pošlje ukaz *ICMP: "Datagram too Big"*
  - in sporočilo *ICMP: "discovery message: MTU = 1500"*.
- Naslednji paket pošiljatelja ne bo daljši od 1500 oktetov, dodano pa mu bo fragmentacijsko čelo s podatki, kako je datagram drobljen.
- Če bi na poti paketa bilo omrežje s še manjšim MTU, bi se opisani postopek ponovil.

Ugotavljanje avtentičnosti

- Velika pomanjkljivost protokola IPv4 je, da ne omogoča ugotavljanje avtentičnosti sprejetega okvira in ne pozna kriptografskega prekodiranja.
- Zato je možno na komunikacijski poti – proti volji pošiljatelja – prestrezati, preusmerjati in spreminjati okvire.
  - Zlorabe, ki se lahko pri tem zgodijo, zelo omejujejo uporabo IPv4 v mnogih dejavnostih, kjer je avtentičnost in tajnost ključnega pomena, na primer v bančništvu.
  - Problem avtentičnosti in varnosti se pri omrežjih IPv4 v splošnem skuša reševati v višjih plasteh.
- Ta problem protokol IPv6 rešuje s posebnim čelom (Fig. 4.35), s katerim zagotavlja, da je bil sprejeti paket res poslan od avtentičnega izvora ter da med potovanjem ni bil spremenjen.

Ugotavljanje avtentičnosti (2)



Slika 4.35: Čelo za zagotavljanje avtentičnosti.

- Polja:

dolžina (8 bitov), dolžina podatkov o avtentičnosti v 32-bitnih besedah

SPI (32 bitov), indeks algoritma, ki izračuna podatke avtentičnosti

Števec (32 bitov) služi za štetje ponavljanja

Podatki avtentičnosti (spremenljiva dolžina), vsebina je odvisna od uporabljenega algoritma ugotavljanja istovetnosti

Ugotavljanje avtentičnosti (3)

- Podatki avtentičnosti se računajo z različnimi algoritmi. Najpogosteje se uporabljata DES in MD5
- Avtentičnost se ne glede na uporabljen algoritem računa za ves datagram z izjemo polj, ki se med prenosom spreminjajo (za ta polja se pri računanju avtentičnosti upoštevajo ničle)
- Računanje avtentičnosti se izvede pred fragmentacijo datagrama
- S števcem ponavljanja preprečimo, da se bi pri ponovnem pošiljanju paketa (zaradi ugotovljene napake med prenosom) ponovil varnostni algoritem za zagotavljanje avtentičnosti.

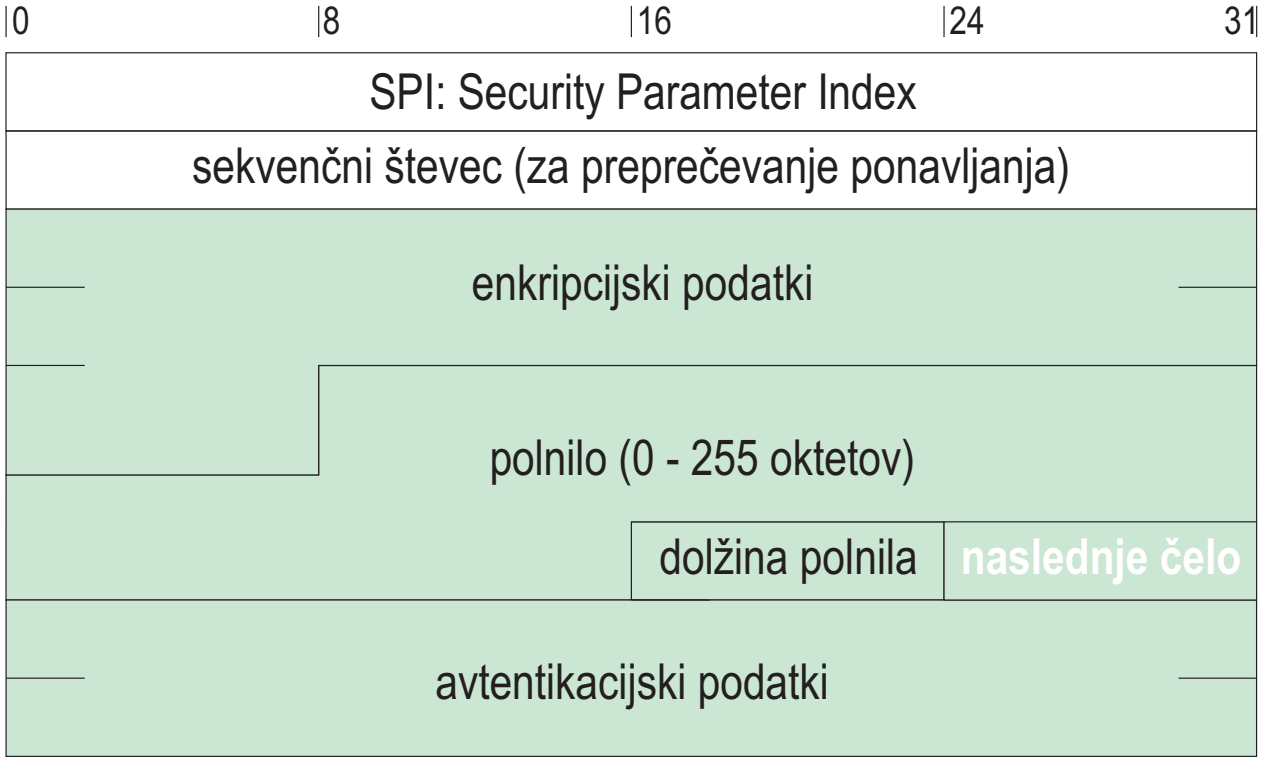
Enkripcijsko čelo

- Zagotovitev avtentičnosti sicer reši problem preverjanja pravega izvora podatkov, ne zaščiti pa poslanih (zaupnih) podatkov pred nepooblaščenim pregledom.
- Tajnost podatkov zagotovimo z enkripcijo podatkov.

  Za zagotovitev tajnosti poslanih podatkov so bili (šele) leta 1995 predlagani predlogi standardov za to področje:
  - RFC 1825: Pregled varnostne arhitekture
  - RFC 1826: Opis razširitve IP z avtentikacijo paketov
  - RFC 1828: Posebnosti avtentikacijskih mehanizmov
  - RFC 1827: Opis razširitve IP z enkripcijo
  - RFC 1829: Posebnosti kriptografskih mehanizmov

  IPv4 pogojno podpira tudi te mehanizme, pri IPv6 pa so sestavni del protokola.
- Z enkripcijskim čelom (Fig. 4.36) IPv6 datagram pretvori v kriptogram, ki zagotovi visok nivo tajnosti podatkov.
- Enkripcijsko čelo lahko vsebuje tudi podatke avtentičnosti vira.

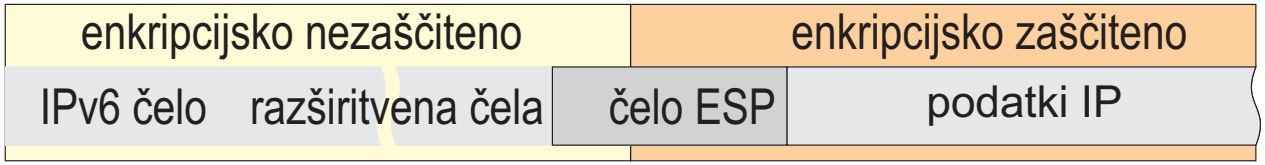
Enkripcijsko čelo (2)



Slika 4.36: Zgradba čela Encription.

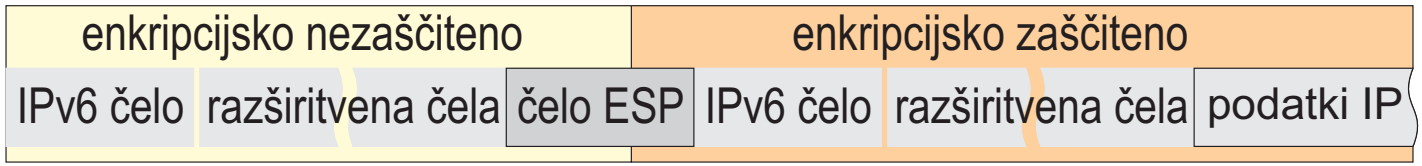
- Kriptogram lahko vsebuje enkapsuliran datagram od zaporedne številke paketa v enkripcijskem čelu nadalje ali pa ves datagram (Fig. 4.37).

Enkripcijsko čelo (3)



Slika 4.37: Možnost uporabe ESP okvirja.

- Kadar je enkapsuliran ves datagram, prenos zahteva tako imenovano *tuneliranje* (Fig. 4.38).

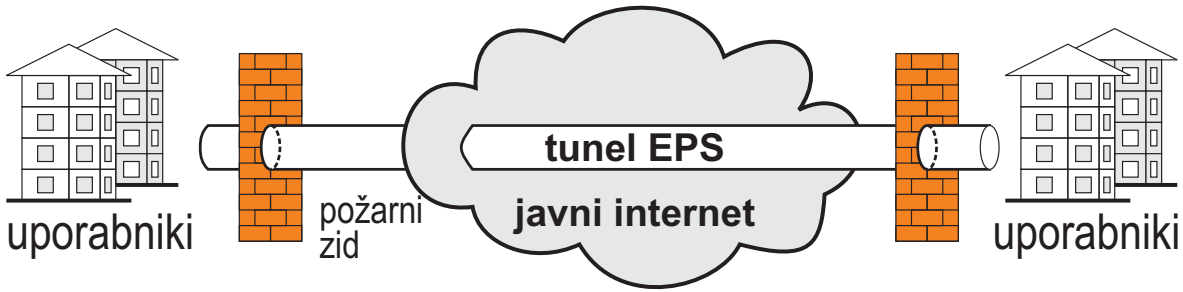


Slika 4.38: Tuneliranje.

- Šifriranje celotnega okvira onemogoči delovanje analizatorjev prometa, saj sta naslova izvora in ponora skrita.
  - V osnovi je bil ta način enkripcije razvit za zaščito s požarnimi zidovi. Ta izvede enkripcijo poslanega paketa, doda pa mu svoje čelo z naslovom sprejemnega požarnega zidu.
  - Sprejemni požarni zid odstrani enkripcijo in paket v originalni obliki pošlje naslovljeni napravi v originalni obliki.

Enkripcijsko čelo (4)

- Za pošiljatelja in prejemnika sta požarna zidova in/ali enkripcija transparenta.



Slika 4.39: Tunel skozi požarni zid .

Naslovna arhitektura v IPv6

- Glavne značilnosti:
  - dolžina 128 bitov
  - naslovi so dodeljeni vmesnikom in ne napravam
  - naprava (v terminologiji IPv6 *vozlišče*), ima lahko več individualnih (v terminologiji IPv6 *unicast*) naslovov
- Kombinacija dolgih naslovov in več naslovov po vozlišču zelo presega učinkovitost usmerjanja pri IPv4.
- Dolgi naslovi omogočajo kopičenje (*aggregation*) naslovov po hierarhijah omrežij, ponudnikih dostopa, geografski razdelitvi, korporacijah itd.
- Kopičenje (agregacija) omogoča, da so/bodo tabele usmerjanja manjše in hitrejše.
- Možnost več naslovov vozlišča omogoča uporabniku, da ima pri istem vmesniku dostop do različnih naslovnih agregacij.

Naslovna arhitektura v IPv6 (2)

- Zgradba naslovnega polja:
  - vsak naslov IPv6 se prične z oznako naslova,
  - oznaka je spremenljive dolžine (Table 4)
  - IPv6 pozna tri vrste naslovov:

    Unikast To je *individualni naslov* vmesnika vozlišča. Sporočilo s takim naslovom je dostavljeno samo enemu vmesniku.

    Anycast To je *skupinski naslov* množice vmesnikov, ki tipično pripadajo vsak svojemu vozlišču. Sporočilo s skupinskim naslovom bo dostavljeno enemu od vmesnikov s tem naslovom (najbližjemu glede na usmerjevalnikovo mero razdalje).

    Multicast To je *skupni naslov* za množico vmesnikov, ki tipično pripadajo vsak svojemu vozlišču. Paket s skupnim naslovom bo dostavljen vsem vmesnikom, ki imajo skupni naslov.

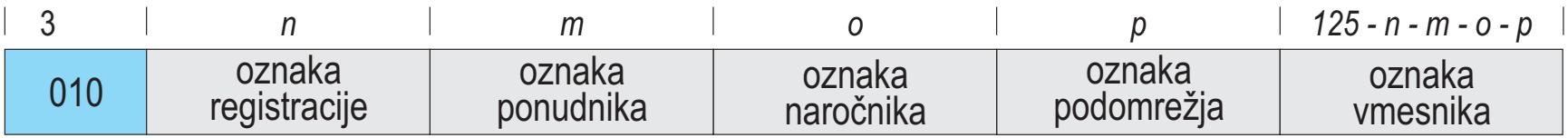
Naslovna arhitektura v IPv6 (3)

Tabela 4: Razdelitev naslovnega prostora pri IPv6

vrsta dodelitve	oznaka (binarna)	delež naslovnega prostora
rezerviran	0000 0000	1/256
nedodeljen	0000 0001	1/256
rezerviran za dodelitev NSAP	0000 001	1/128
rezerviran za dodelitev IPX	0000 010	1/128
nedodeljen	0000 011	1/128
nedodeljen	0000 1	1/32
nedodeljen	0001	1/16
nedodeljen	001	1/8
individualni naslovi za ponudnike	010	1/8
nedodeljen	011	1/8
rezervirano za geografsko razporejene individualne naslove	100	1/8
nedodeljen	101	1/8
nedodeljen	110	1/8
nedodeljen	1110	1/16
nedodeljen	1111 0	1/32
nedodeljen	1111 10	1/64
nedodeljen	1111 110	1/128
nedodeljen	1111 1110 0	1/512
lokalno naslavljanje glede na fizično povezavo (link-local),	1111 1110 11	1/1024
krajevno lokalno naslavljanje (site-local)	1111 1110 10	1/1024
skupni naslovi	1111 1111	1/1024

Individualni naslovi

- Individualnih naslovov je več vrst. Do sedaj so jih razdelili na:
  - ponudniške globalne naslove
  - lokalno naslavljanje glede na fizično povezavo (link-local),
  - krajevno lokalno naslavljanje (site-local)
  - vgrajene IPv4 naslove
  - povratno-zančne naslove
- *Ponudniški globalni naslovi* zagotovijo globalno naslavljanje v vsem "vesolju" povezanih končnih sistemov. Ti naslovi imajo poleg oznake naslova še pet polj (Fig. 4.40):



Slika 4.40: Globalni individualni naslovi, ki jih ponujajo ponudniki internetnih storitev.

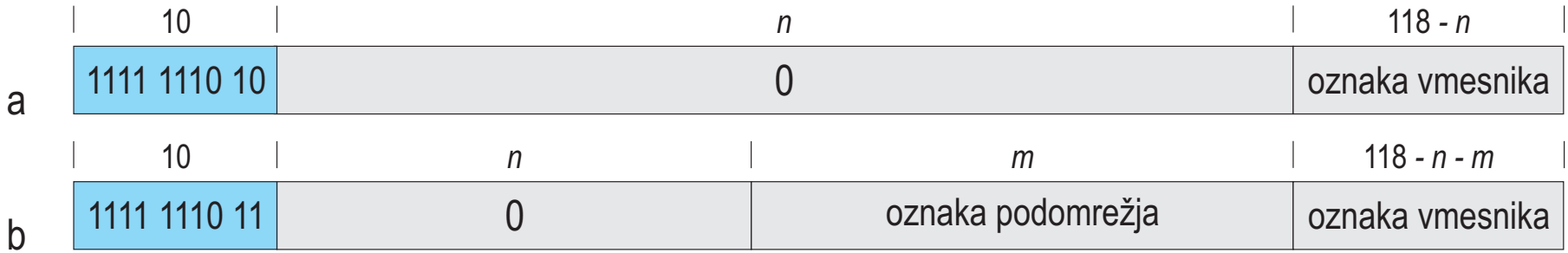
oznaka registracije Služi za identifikacijo urada, ki je ponudniku naslovov dodelil del naslovnega prostora.

Individualni naslovi (2)

oznaka ponudnika	Določa ponudnika internetnih storitev, ki je zakupil del naslovnega prostora
oznaka naročnika	Služi za razlikovanje med večkratnimi naročniki pri istem ponudniku
oznaka podomrežja	Označuje topološko povezano skupino vozlišč, ki se nahaja v omrežju naročnika
oznaka vmesnika	Določa vmesnik vozlišča v podomrežju

- Trenutno še ni določena dolžina nobenemu od naštetih polj, zato moramo biti pri načrtovanju posebej pozorni na zadnji dve polji.
- *Lokalni individualni nalovi* so namenjeni paketom, ki se lahko usmerjajo le znotraj enega ali nekaj lokalnih podomrežij.

Individualni naslovi (3)



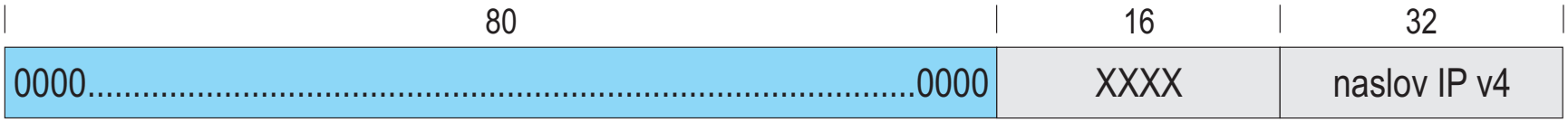
Slika 4.41: Struktura individualnih naslovov IPv6. a: lokalni naslovi glede na fizično povezavo (link-local), b: krajevno lokalno naslovi (site-local).

- Lokalni naslovi za fizične povezave so namenjeni za avtomatsko konfiguracijo naslovov, odkrivanje soseščine in podobne uporabe. Ne morejo biti integrirani v globalne naslove.
- krajevni lokalni naslovi so prav tako namenjeni lokalni uporabi kot lokalni individualni naslovi z razliko, da jih je kasneje mogoče integrirati v globalne naslovne sheme.

Individualni naslovi (4)

Zato njihova struktura že vsebuje polje za podomrežje. Ob prehodu na globalno naslavljanje se polje z *n* ničlami nadomesti s polji oznak *registracije*, *ponudnika* in *naročnika*.

- *Vgrajeni naslovi IPv4*
  - Ker je trenutni prehod iz IPv4 na IPv6 nemogoč, se predvideva daljše prehodno obdobje, v katerem bosta morala sobivati IPv4 in IPv6.
  - Za to obdobje sta predvidena dve naslovni shemi za vgradnjo naslovov IPv4:
    1. Naslovi IPv6 kompatibilni z IPv4. Ti imajo v predponi 96 ničel, katerim sledi 32-bitni naslov IPv4
    2. Naslovi IPv6 preslikani v IPv4. Ti imajo v predponi 80 ničel, katerim sledi 16 enic.



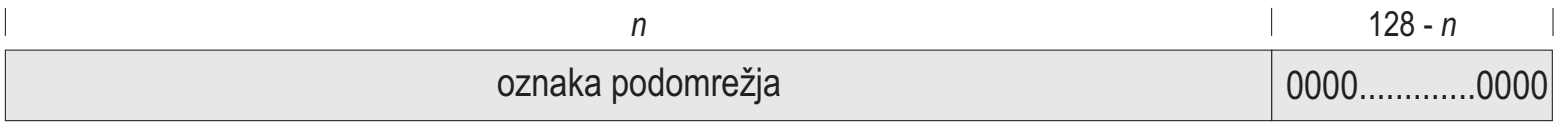
Slika 4.42: Vgrajeni naslov IPv4

Individualni naslovi (5)

- Vzdrževanje sočasnega delovanja obeh protokolov ni preprosto, zagotovi pa naslednje:
  1. Paketom, ki jih pošiljajo naprave z le IPv4, dualnih usmerjevalniki (IPv4 + IPv6) najprej pretvorijo naslove prejemnika v vgrajeni IPv4 naslov, nato pa sestavijo čelo IPv6.
  2. Pakete, ki jih pošiljajo dualne naprave (IPv4+IPv6), usmerjevalniki v omrežjih z IPv4 posredujejo s tehniko enkapsulacije datagrama IPv6 v datagram IPv4. Rečemo, da skozi omrežje z IPv4 naredimo tunel za promet IPv6.

Skupinski naslovi

- *Skupinski naslovi* so namenjeni avtomatskem dodeljevanju in konfiguraciji naslovov naprav v IPv6
- S temi naslovi določamo/ugotavljamo topologijo entitet – dodeljeni so skupinam vmesnikov.
- Primer skupine vmesnikov so usmerjevalniki v nekem podomrežju ali usmerjevalniki na hrbtenici omrežja in podobno
- Paket s skupinskim naslovom prejemnika bo dosegel najbližji (po merilu razdalje usmerjevalnikov) vmesnik v skupini.
- Od skupinskih naslovov se tudi pričakuje izboljšanje usmerjanja paketov skozi medomrežje.



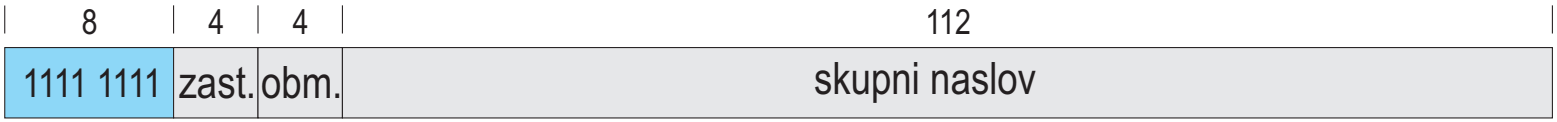
Slika 4.43: Skupinski naslovi

Skupni naslovi

- *Skupni naslovi* so namenjeni hkratnemu pošiljanju paketov vsem vmesnikom v omrežju.
- Glede na sprejem paketov ločimo:
  - *multicast naslov*, ko pakete sprejme le skupina vmesnikov
  - *broadcast naslov*, ko pakete sprejmejo vsi vmesniki.
- Paket s skupnim naslovom ima številne prednosti in uporabe:
  - ko je potrebno neko sporočilo poslati k več vmesnikom, da s skupnim naslovom ni potrebno pošiljati vsakemu posebej
  - Pri odkrivanju soseščine se na paket odzovejo le vmesniki, ki so registrirani za sprejem takega sporočila. S tem odpravimo nepotrebno delo vsem ostalim vmesnikom, za katere ta paket ni relevanten.
  - Ali bo določeni vmesnik bo sprejel paket ali ne, je izbira vmesnika.
- Vmesnik je lahko sočasno član več skupin, za včlanitev v skupino se ne rabi pogajati s komerkoli.

Skupni naslovi (2)

- *struktura skupnega naslova* (Fig. 4.41):



Slika 4.44: Skupni naslov.

- oznaka naslova (8 enic)
- zastavice (4 biti) trenutno so prve tri 0, četrta je T s pomenom:
  - T = 0 označuje, da je skupni naslov stalni, oziroma vsem dobro znani skupni naslov, ki ga je dodelil urad za za globalno dodeljevanje naslovov;
  - T = 1 označuje prehodni skupinski naslov
- območje (2 bita):

Tabela 5: Skupna naslovna območja

kod	območje	kod	območje	kod	območje	kod	območje
0	rezervirano	4	nedodeljeno	8	lokalna organizacija	12	nedodeljeno
1	lokalna vozlišča	5	lokalne območja	9	nedodeljeno	13	nedodeljeno
2	lokalne povezave	6	nedodeljeno	10	nedodeljeno	14	globalno
3	nedodeljeno	7	nedodeljeno	11	nedodeljeno	15	rezervirano

Skupni naslovi (3)

- skupni naslov (112 bitov)

- Prehodni skupni naslov ima pomen le znotraj danega območja, zato ga lahko sočasno uporabljamo v različnih območjih.
- *IGMP*: (Internet Group Management Protocol) je protokol, ki ga gostitelji uporabljajo za včlanjevanje skupne naslove.
- *Usmerjanje paketov s skupinskimi naslovi* ni preprosto.
- V ta namen so razvita zelo sofisticirana orodja, ki omogočajo reklamiranje naslova na internetu.
- *Usmerjanje pri znanem stanju medomrežja* omogoča preprosto dogradnjo skupnih naslovov.
- Ker je znana vsa topologija omrežja, lahko uporabljamo Dijkstrov algoritem za izračun najkrajše poti tudi za skupne naslove

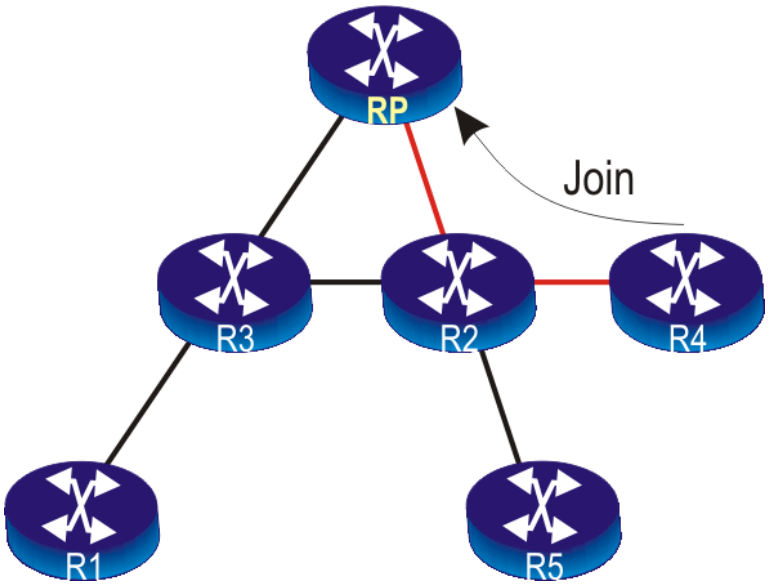
Skupni naslovi (4)

- Pri algoritmu na osnovi *vektorjev razdalj* ne poznamo vsega omrežja, zato je dodajanje skupnih naslovov težje.
- Postopek ima dva dela:
  1. oblikuje mehanizem razpošiljanja vsem podomrežjem v medomrežju,
  2. izboljša mehanizem tako, da izloči veje, ki ne vodijo do gostiteljev s skupnim naslovom
- *Protokolno neodvisno usmerjanje: PIM* (Protocol Independent Multicasting) so razvili z namenom, da zmanjšajo problem obsega prometa pri protokolih za dostavo paketov s skupnimi naslovi.
- PIM razdeli problem na dva dela:
  1. ko so naslovi na redko posejani
  2. ko so naslovi na gosto posejani
- V prvem primeru se usmerjevalniki s sporočili Join in Prune eksplicitno priključujejo ali izključujejo dostavi sporočil s skupnim naslovom.

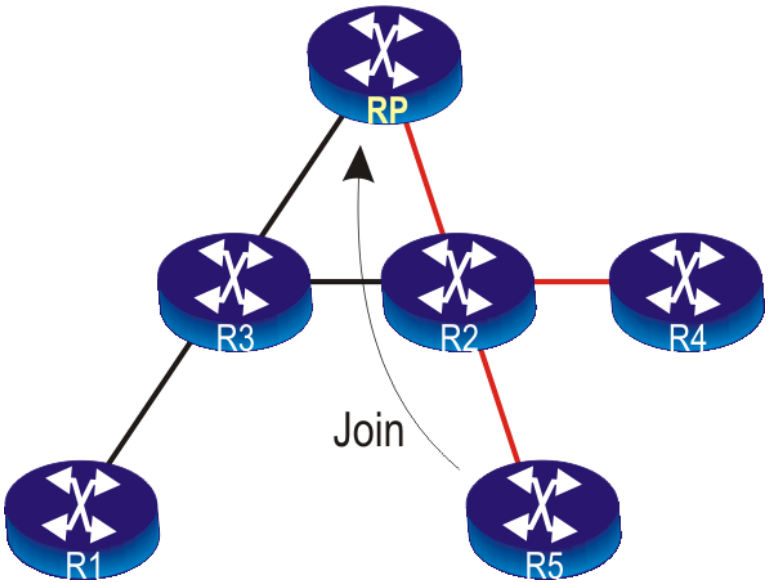
Skupni naslovi (5)

- Sporočila usmerjevalniki pošiljajo *točki sestajanja: rendezvous point (RP)*, ki so v usmerjevalnikih z dobro znanimi skupnimi naslovi.
- Usmerjevalniki na poti paketa *Join* si zabeležijo, da pripadajo drevesu skupnega naslova. Tako se zgradi drevo usmerjevalnikov s skupnim naslovom s staršem v RP.
- Četudi RP ni član skupnega naslova, v osnovi vsi paketi s skupnim naslovom potujejo preko njega.
- Tako delovanje seveda ni optimalno, zato so omogočena *specifična drevesa*, ki direktno povezujejo usmerjevalnike s skupnimi naslovi. Ločimo:
  - specifično drevo vira (Fig. 4.47)
  - specifično drevo prejemnika (Fig. 4.48)
- Ta postopek imenujemo protokolno neodvisni zato, ker ga lahko uporabimo pri vseh protokolih usmerjanja.

Skupni naslovi (6)

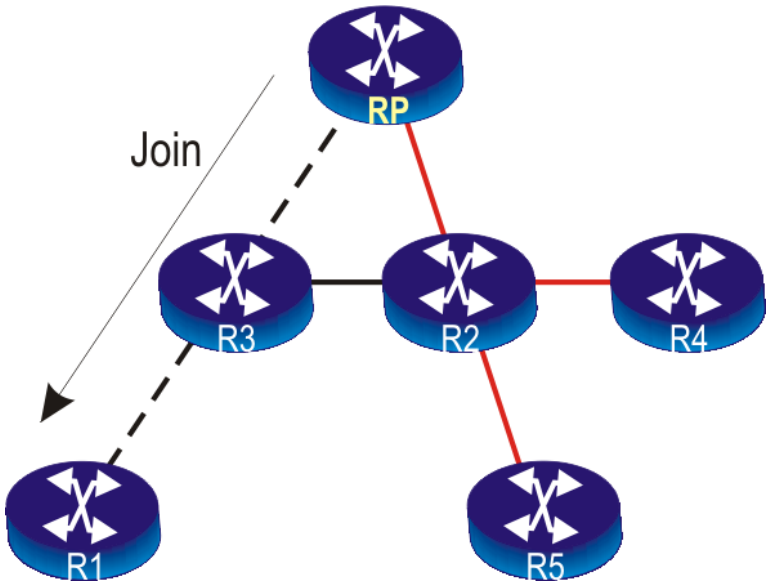


Slika 4.45: R4 pošlje *Join* RP in se s tem priključi drevesu skupnega naslova.

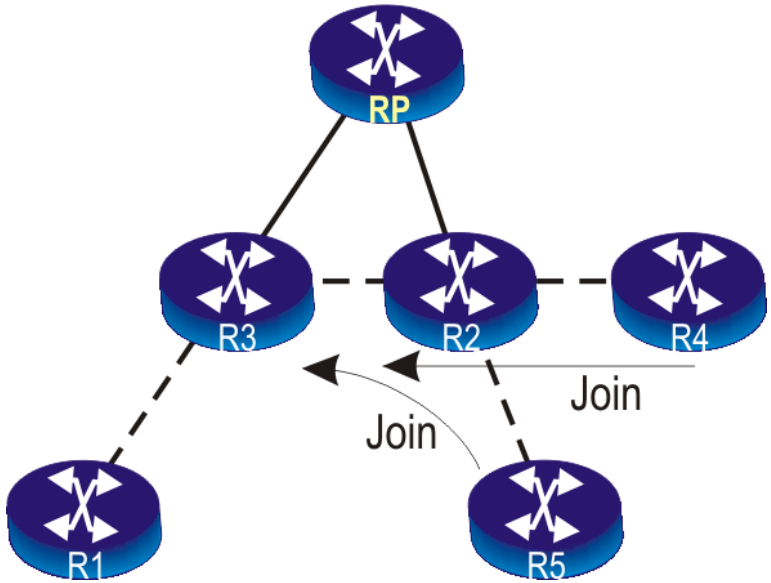


Slika 4.46: R5 se priključi drevesu skupnega naslova.

Skupni naslovi (7)



Slika 4.47: RP zgradi specifično drevo do R1.



Slika 4.48: R4 in R5 zgradita specifično drevo z R1.

Avtomatska konfiguracija IPv6 naslova

- Pomembna pridobitev IPv6 je avtomatska konfiguracija naslovov.
- Ima pomembno vlogo v rekonfiguraciji sistemov (prehod iz IPv4 na IPv6, prehod iz intraneta v internet, prehod iz enega oskrbovalca na drugega).
- Proces avtomatske konfiguracije naslova se prične z raziskovanjem soseščine (neighbour discovery - ND).
- ND protokol je kombinacija protokolov IPv4 ARP in ICMP
- obstajajo trije modeli avtomatskega dodeljevanja naslovov:
  1. *local scope* (lokalno delovanje), ki je namenjeno omrežjem brez usmerjevalnikov. V tem primeru lahko za naslov IP služi naslov MAC, ali pa jih dodeli preprosti dinamični sistem njihovega dodeljevanja.

Avtomatska konfiguracija IPv6 naslova (2)

2. *stateless server model* (statično dodeljevanje naslovov), kjer nova naprava pošlje zahtevo po naslovu dobro znanemu skupinskemu naslovu, ki lahko deluje kot naslovni strežnik. Sebe identificira z naslovom MAC ali drugim razpoznavnim ključem. Naslovni strežnik sestavi naslov IP na osnovi svojega poznavanja omrežja.
3. *statefull server model* (dinamično dodeljevanje naslovov), ki daje največjo podporo sistemski administraciji. Vzdržuje bazo dodeljevanja naslovov IP. Naslove, ki dodeljuje, imajo določeno življenjsko dobo. Po njenem izteku, mora naprava ponovno zaprositi za naslov IP.

- Pri dodeljevanju naslovov se uporablja protokol Neighbour Discocery (ND). Tipični scenarij pri drugi ali tretji strategiji je naslednji:
  - Naprava pošlje na znan naslov paket ND z svojim naslovom MAC
  - Če naslov ne obstaja, od prvega usmerjevalnika na poti paketa dobi sporočilo ICMP “naslov ne obstaja”, potem mora postopek ponavljati, dokler ne dobi odziv z dodeljenim naslovom
  - Ko ima dodeljen naslov, pošlje ICMP “router solicitation request” (ICMP RSR) s skupinskim naslovom usmerjevalnikov

Avtomatska konfiguracija IPv6 naslova (3)

Pri IPv4 se ta aktivnost izvede z ARP, ki pa zahtevo pošlje vsem napravam (broadcast sporočilo), zato zahteva sproži procesiranje v vseh napravah in s tem po nepotrebnem obremenjuje njihovo delovanje.

Na ICMP RSR se usmerjevalniki odzovejo z sporočilom ICMP “router advertisement” in dostavijo napravi naslovno predpono, ki jo rabi za konfiguracijo svojega naslova IP.

ICMPv6

- Specifikacija ICMPv6 temelji na RFC 1885.
- Od ICMPv4 se razlikuje v naslednjem:
  1. številki protokola (da ločimo ICMPv6 od ICMPv4),
  2. nekatera redko uporabljana sporočila ICMPv4 so opuščena,
  3. Maksimalna dolžina sporočila ICMPv6 je daljša (576 oktetov, v katerih so vključena tudi čela IPv6).
- Vsa sporočila ICMPv6 se pričnejo z enakimi kontrolnimi polji:

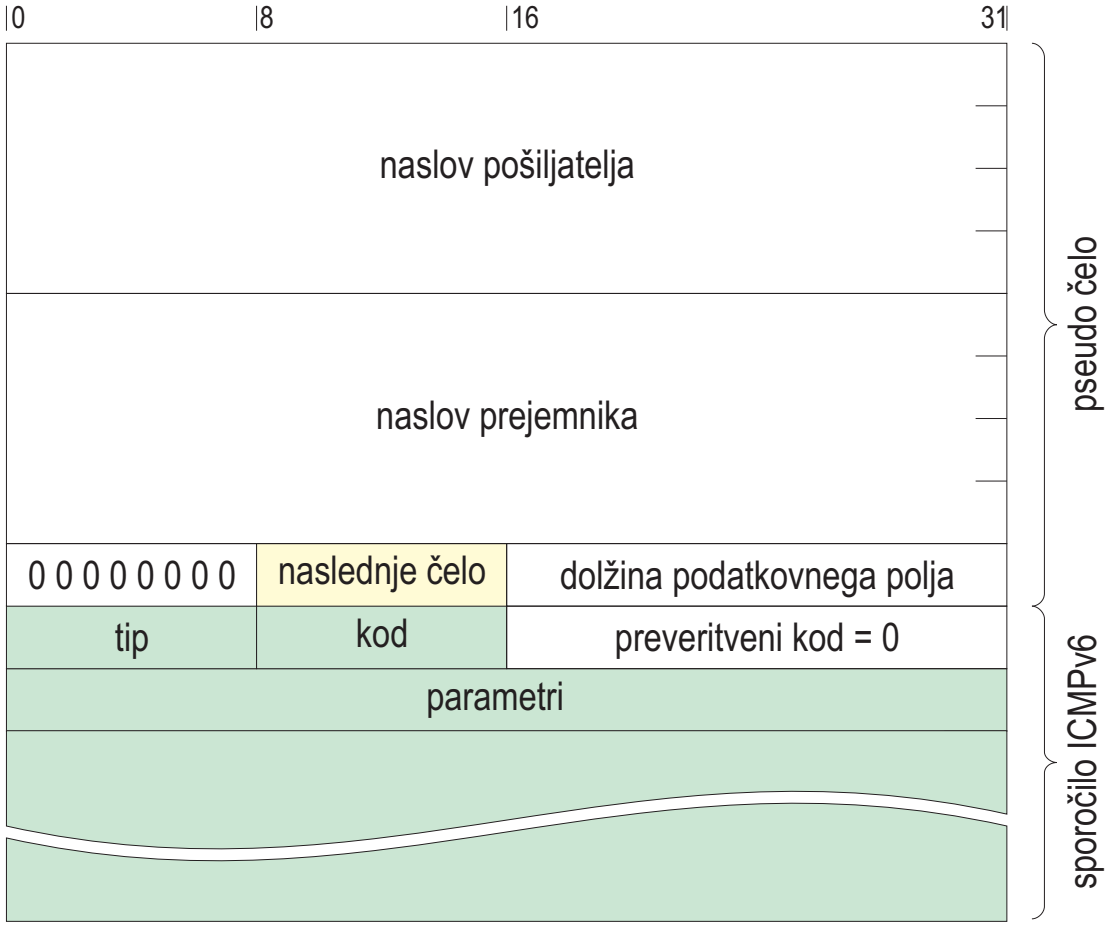
  tip (8 bitov), označuje sporočila ICMPv6:
  - štiri vrste sporočil o napakah
  - pet vrst informacijskih sporočil

  Kod (8 bitov), določa parametre sporočila.

  Preveritev (16 bitov), v računanju preveritvene vsote se poleg polj sporočila ICMPv6 upošteva še psevdo čelo (Fig. 4.49).

  Parametri (32 bitov), parametri so lahko daljši kot pri ICMPv4.

ICMPv6 (2)



Slika 4.49: Računanje preveritvene vsote.

ICMPv6 (3)

- Psevdo čelo vsebuje:
  - naslovni polji iz čela IPv6,
  - polje tip paketa (v njem so samo ničle),
  - številko naslednjega čela (enaka je 58)
  - dolžino podatkovnega polja.
- Psevdo čelo se uporablja le pri računanju preveritvene vsote, potem se odstrani (vrne v čelo IPv6).
- Z vključitvijo psevdo čela se ICMPv6 zaščiti pred napačno dostavo, ki bi jo povzročila napaka v naslovnem polju.

Sporočanje napak

- Protokol ICMPv6 ima definirana štiri obvestila o napakah:
  - Prejemnik ni dosegljiv
  - prevelik paket
  - čas je potekel
  - problemi s parametri
- Vsako od teh sporočil se nanaša na predhodni paket IPv6 in je poslano viru paketa.
- Obvestilo vsebuje tudi del paketa, na katerega se nanaša,

  Velikost prepisa paketa je omejena z razpoložljivi prostorom podatkovnega polja ICMP. Omejuje jo skupna dolžina paketa IPv6 z ICMP, ki znaša 576 oktetov.
- Sporočilo *Prejemnik nedosegljiv* javlja s parametrom v polju *Kod* tudi vzrok, zakaj je bilo poslano. Parametri so:

  bit 0 **ni poti do prejemnika**. Usmerjevalnik ne ve, kako priti do podomrežja prejemnika.

Sporočanje napak (2)

bit 2 **administrator je prepovedal komuniciranje s prejemnikom**. Dostava ni mogoča zaradi požarnega zidu ali katere druge administrativne omejitve pri prejemniku.

bit 3 **nedosegljiv naslov**. Usmerjevalnik ne zna preslikati naslova prejemnika v naslov povezave, ali pa so pri tem nastali problemi specifični za povezavo (link).

bit 4 **nedosegljiva vrata**. Prejemnikov transportni protokol (na primer UDP) ne vključuje vrata, kamor je bil paket poslan. Ta protokol nima na voljo drugih sredstev, da bi o tem obvestil pošiljatelja (da so naslovljena vrata neaktivna).

- Sporočilo *Prevelik paket* pošlje usmerjevalnik, kateremu sledi podomrežje z MTU manjšim od dolžine prispelega paketa.
- Sporočilo *čas je potekel* pošlje usmerjevalnik, ki sprejme paket, kateremu je potekla življenjska doba ali prejemnik, če ne more sestaviti paketa.

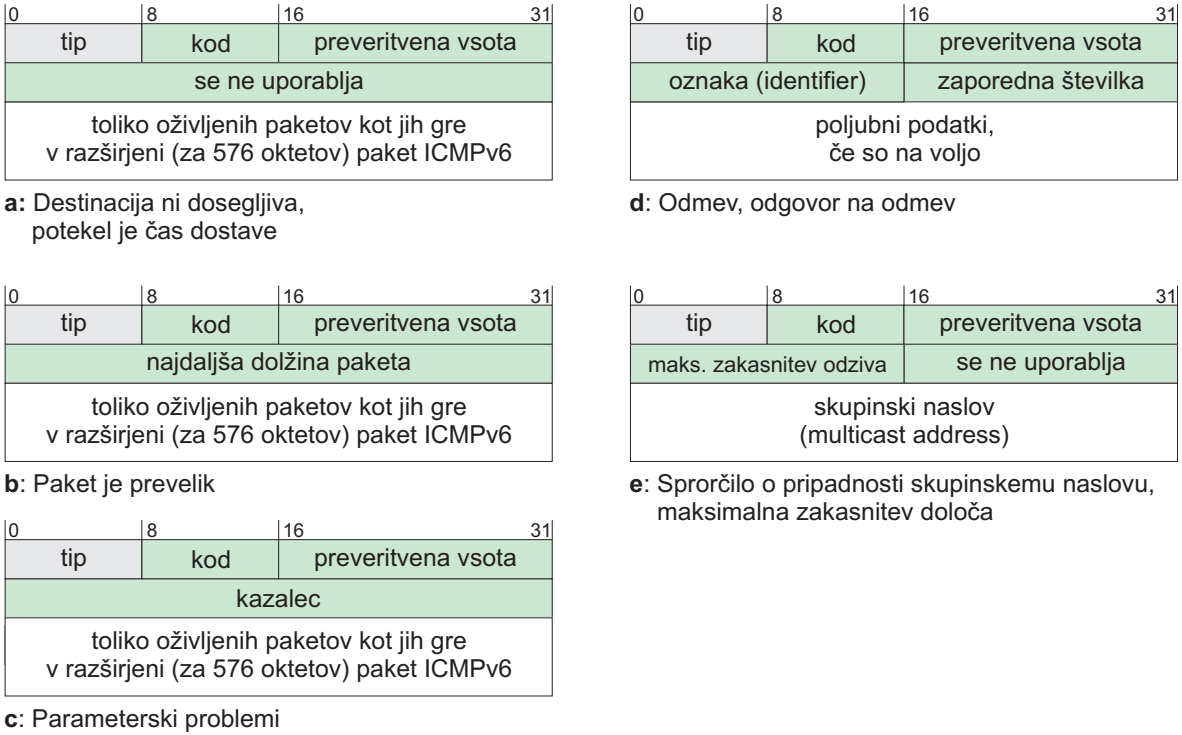
Sporočanje napak (3)

Pri poteku življenjske dobe paketa so v polju *življenjska doba* ničle. Če sporočilo pošlje usmerjevalnik, ima kod 0, če pa prejemnik pa kod 1. S tem lahko določimo vzrok poteka življenjske dobe.

- Sporočila *parametrski problemi* se pošljejo pri odkritju sintaksnih ali semantičnih napak v paketu. Sporočilo razlikuje tri vrste napak, ki jih označi v polju Kod:
  - napaka v polju čela (bit 0)
  - neobstoječi tip naslednjega čela (bit 1)
  - neobstoječe opcije (bit 2)

  Sporočilo vsebuje tudi kazalec, ki kaže na mesto odkrite napake.

Sporočanje napak (4)



a: Destinacija ni dosegljiva, potekel je čas dostave

b: Paket je prevelik

c: Parameterski problemi

d: Odmev, odgovor na odmev

e: Sprorčilo o pripadnosti skupinskemu naslovu, maksimalna zakasnitev določa

Slika 4.50: Sporočila ICMPv6.

Informacijska sporočila

- ICMPv6 vsebuje tri informacijska sporočila:
  - zahteva odmeva
  - odgovor na zahtevo odmeva
  - včlanitev v skupino
- Informacijo *zahteva odmeva* uporabljamo pri testiranju, ali je možna komunikacija med dvema entitetama,
  - torej enako kot pri ICMP z ukazom *ping* (opremljenim z ustreznimi parametri) preverimo, ali je določena naprava prisotna ali ne.
  - Prejemnik *zahteve odmeva* se odzove z *odgovorom na zahtevo odmeva* v katerem vrne telo zahteve, postavi oznako in zaporedno številko paketa na isto vrednost, kot jo je imela zahteva odmeva. Oznaka se lahko v posebnih primerih uporablja kot naslov dostopne točke do storitve, zaporedna številka pa se lahko inkrementira po vsakem pošiljanju zahteve po odmevu.
- Informacija *včlanitev v skupino* se uporablja v procedurah medomrežnega protokola za upravljanje skupin (IGMP).

Informacijska sporočila (2)

IGMP: Internet Group Management Protocol

IGMP je razširitev ICMP, določena z RFC 1112. Omogoča mehanizem odločanja o pošiljanju skupinskih (multicast) datagramov IPv4. V ICMPv6 so v ta namen določena tri sporočila, ki jih razlikujemo po tipu sporočila:

- iskanje članstva v skupini (tip = 130)
- poročanje o članstvu v skupini (tip = 131)
- zaključitev članstva v skupini (tip = 132)

- Neka naprava se lahko priključi skupini, katere člani imajo isti skupinski naslov in se dinamično oblikuje za sprejem določenega zaporedja skupinskih sporočil.
- Priključi se z oddajo sporočila *poročila o članstvu v skupini* podomrežju s skupinskim naslovom, v katerega zapiše telo sporočila. Paket IPv6, ki vsebuje to sporočilo, je naslovljen na isti skupinskih naslov.

Informacijska sporočila (3)

- Usmerjevalniki na podomrežjih, ki sprejmejo poročilo in shranijo informacijo, da je najmanj eno vozlišče v tem podomrežju član skupine.
- Naprava lahko zaključi članstvo v skupini z oddajo sporočila *konec članstva v skupini*.

Konec