# Usporedba IPV4 i IPV6 protokola

**Babić, Kristijan**

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

**KRISTIJAN BABIĆ**

# USPOREDBA IPV4 I IPV6 PROTOKOLA

Završni rad

Pula, rujan 2017.

Sveučilište Jurja Dobrile u Puli

Odjel za informacijsko-komunikacijske tehnologije

**KRISTIJAN BABIĆ**

# USPOREDBA IPV4 I IPV6 PROTOKOLA

Završni rad

**JMBAG: 0303046229; redoviti student**

**Studijski smjer: Informatika**

**Kolegij: Elektroničko poslovanje**

**Znanstveno područje: Društvene znanosti**

**Znanstveno polje: Informacijsko-komunikacijske znanosti**

**Znanstvena grana: Informacijski sustavi i informatologija**

**Mentor: prof. dr. sc. Vanja Bevanda**

Pula, rujan 2017.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Kristijan Babić, kandidat za prvostupnika Informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, rujan, 2017. godine

IZJAVA

o korištenju autorskog djela

Ja, Kristijan Babić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Usporedba Ipv4 i Ipv6 protokola koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

# Sadržaj

# 1. Uvod

Naslov završnog rada je Usporedba IPv4 i IPv6 protokola. Svrha mu je prikazati razlike između ova dva protokola te ih usporediti. Internet protokol (IP) je jedan od najvažnijih, najpoznatijih i najčešće je korišten protokol za komunikaciju. Internet protokol pruža mogućnost prepoznavanja svakog računala na mreži ili na Internetu pomoću adrese. Glavni problem IPv4 protokola je nedostatak adresnog prostora te upravo je zbog tog razloga došlo do potrebe za razvojem novog IPv6 protokola. Rad je koncipiran u šest cjelina.

U drugom poglavlju objašnjen je OSI referentni model, što je OSI referentni model i koja je njegova svrha. Također navedeni su i objašnjeni slojevi OSI referentnog modela i navedeni protokoli koji pripadaju pojedinom sloju.

U trećem poglavlju objašnjen je TCP/IP model, njegova povijest te u potpoglavlju arhitektura TCP/IP i objašnjenje arhitekture, odnosno slojeva od kojih je sastavljen.

U četvrtom poglavlju objašnjen je Internet protokol verzije 4, adresiranje, klasifikacija, odnosno podjela IP adresa na klase, tipovi adresa, zaglavlje IPv4 protokola, fragmentacija paketa i usmjeravanje paketa kako bi stigli s izvorišta na odredište.

Naslov petog poglavlja glasi Internet protokol verzije 6  i u njemu je navedeno adresiranje, tipovi adresa, zaglavlje IPv6 protokola, dodatna zaglavlja, fragmentacija i usmjeravanje.

## 2. OSI referentni model

"OSI (Open System Interconnection Basic Reference Model) referentni model je apstraktni, slojeviti model koji služi stručnjacima kao preporuka za razvijanje računalnih mreža i protokola."[1] OSI model daje smjernice u razvijanju mrežnih protokola. Mrežni komunikacijski protokoli predstavljaju određena pravila kao što su prikaz podataka, autorizacija, signalizacija i otkrivanje pogrešaka te su potrebni kako bi se preko komunikacijskih kanala ti podaci prenijeli. OSI referentni model podijeljen je na sedam slojeva u kojoj svaki sloj ima svoju zadaću, tj. svaki sloj ima skup funkcija koje služe za jedan dio računalne komunikacije. Slojevi zajedno predstavljaju tok podataka od izvorišta do odredišta.

Slojevi OSI referentnog modela su:

- Aplikacijski sloj (Application layer)
- Prezentacijski sloj (Presentation layer)
- Sloj sesije (Session layer)
- Transportni sloj (Transport layer)
- Mrežni sloj (Network layer)
- Podatkovni sloj (Data-Link layer)
- Fizički sloj (Physical layer)

Komunikacija među slojevima vrši se samo s prvim slojem iznad i ispod sebe što znači da prezentacijski sloj komunicira samo s aplikacijskim i sesijskim slojem. OSI model je razvijen kako bi olakšao razvoj protokola i komunikacije. Pridržavanjem smjernica ubrzava se razvoj samih protokola za svaki od slojeva. Prednost toga je neovisnost o brzini razvoja protokola na drugim slojevima.

Slojevi OSI referentnog modela:

- **Aplikacijski sloj:** Najviši je sloj te on komunicira direktno s korisnikom ili s programskim aplikacijama. Aplikacijski sloj omogućuje korisničke servise kao što su npr. elektronska pošta i transfer datoteka (FTP- engl. File Transfer Protocol). Kod protokola za slanje datoteka, aplikacijski sloj na jednom kraju

[1] Pralas, Toni. 2008. "Računalne mreže – OSI referentni model". Sys.portal Carnet. https://sysportal.carnet.hr/node/352

šalje datoteku direktno do drugog aplikacijskog sloja bez obzira na korištenu mrežu ili računalnu arhitekturu. Neki od protokola u ovom sloju su HTTP, FTP, Telnet, DNS, SMTP i dr.[2]

- **Prezentacijski sloj:** Odgovoran je za predstavljane podataka u takvom obliku da ih krajnji korisnik može razumjeti. Na primjer, dva računala mogu koristiti različite formate zapisa te prezentacijski sloj prevađa formate zapisa tako da bi se korisnici na suprotnim stranama mogli međusobno razumjeti, što znači da korisnici ne trebaju biti fokusirani na oblik formata već na sadržaj informacija koje šalju. [3]
- **Sloj sesije:** Ovaj sloj omogućuje aplikacijama na različitim stranama da ostvare međusobnu komunikaciju. Sesijski sloj pomaže pri koordinaciji procesa na način da obavještava svaku stranu kada može slati podatke ili kada mora pričekati. Taj način predstavlja jedan oblik sinkronizacije. Također ovaj sloj ima zadaću za ispravljanje grešaka. Na primjer, kada korisnik šalje veliku datoteku preko mreže na kojoj se dogodio kvar. Nakon otklona kvara korisnik ne mora ponoviti slanje datoteke jer sesijski sloj omogućava postavljanje kontrolnih točaka te one sprječavaju gubitak podataka, odnosno bit će izgubljeni samo oni podatci koji su poslani nakon zadnje kontrolne točke. Protokoli u ovom sloju su NetBIOS, PAP, CHAP, SSH i dr. [4]
- **Transportni sloj:** Ovaj sloj se bavi komunikacijom između dvije strane, utvrđuje koja se mreža može koristiti za komunikaciju te se brine da svi podaci stignu s jednog na drugi kraj mreže. Transportni sloj bavi se razbijanjem podataka na manje dijelove ukoliko je to potrebno te ih nakon toga predaje mrežnom sloju. Najpoznatiji protokoli transportnog sloja su Protokol prijenosa kontrole (TCP - engl. Transmission Control Protocol) i Korisnički podatkovni protokol (UDP - engl. User Datagram Protocol).
    - TCP: „Dominantan, spojevni, prijenosni protokol interneta koji garantira pouzdanu isporuku podataka od izvorišta do odredišta u kontroliranom redoslijedu.“ [5]

[2] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str 22
[3] Ibid.
[4] Ibid.
[5] Mujarić, Eldis. 2009. "Računalne mreže". Layer-x. http://mreze.layer-x.com/s040100-0.html

    - UDP: Funkcioniranje ovog protokola moguće je bez uspostavljanja veze te je puno jednostavniji od TCP protokola, ali ne omogućava siguran prijenos podataka.
- **Mrežni sloj:** Brine se o pravilnom prijenosu podataka između transportnog sloja i krajnje stanice te uspostavlja, održava i raskida mreže. Glavni zadatak mrežnog sloja je odabrati put kojim će se najbrže i najbolje poslati podaci. Mrežni sloj mora dozvoliti prijenos podataka bez obzira na međusobne razlike (npr. veličina paketa, protokola itd.). Mrežni sloj preuzima odgovornost za usmjeravanje paketa od izvora do odredišta unutar ili izvan podmreža različitim shemama adresiranja i protokolima. Najpoznatiji protokoli u mrežnom sloju su Internet protokoli (IP - engl. Internet Protocol), odnosno Internet protokol verzije 4 (IPv4) i Internet protokol verzije 6 (IPv6) koji zamjenjuje dosadašnji IPv4.
  Prema Kozieroku neki od specifičnih poslova koje izvodi mrežni sloj su:
    - Logičko adresiranje (Logical Addressing)
    - Usmjeravanje (Routing)
    - Enkapsulacija datagrama (Datagram Encapsulation)
    - Fragmentacija i ponovno sastavljanje (Fragmentation and Reassembly)
    - Rješavanje problema i dijagnostika (Error Handling and Diagnostics)
- **Podatkovni sloj:** Drugi najniži sloj OSI referentnog modela je podatkovni sloj koji ima zadaću osigurati siguran prijenos podataka putem linije. Podatkovni sloj koristi se tehnikama otkrivanja i ispravljanja grešaka te se na taj način osigurava prijenos bez grešaka. Ukoliko se dogodi greška može se zahtijevati novi prijenos ili ispravljanje iste. Podaci se u ovom sloju najčešće prenose u okvirima, a okvire čine grupe organiziranih bitova ovisno o formatu koje podatkovni sloj prepoznaje. Protokoli u ovom sloju su PPP, HDLC, Frame Relay i dr. [6]
- **Fizički sloj:** Najniži sloj OSI referentnog modela je Fizički sloj. Fizički sloj je jedini sloj u kojem se podaci fizički premještaju preko mrežnog sučelja dok svi ostali slojevi obavljaju funkcije slanjem poruka. Drugim riječima, fizički sloj bavi se fizičkim prijenosom podataka. Da bi se podaci uspješno poslali, poruke

[6] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 103

moraju biti prenesene kroz sve ostale slojeve sve do fizičkog sloja. Protokoli u ovom sloju su Token Ring, IEEE 802.11 i dr.[7]

# 3. TCP/IP model

Najvažnijim protokoli u TCP/IP modelu smatraju se Internet protokol (IP) i Protokol prijenosa kontrole (TCP). Internet protokol je primarni protokol mrežnog sloja OSI referentnog modela te on pruža adresiranje, usmjeravanje datagrama i ostalo. TCP/IP protokoli razvijeni su od Agencije za napredene istraživačke projekte Sjedinjenih Američkih Država (DARPA ili ARPA) kao dio istraživačke mreže. Prvi naziv ove mreže bio je ARPAnet te je osmišljena za korištenje brojnih protokola na već postojećim tehnologijama. Protokoli u ARPAnet mreži imali su nedostatke i ograničenja u konceptu ili u praktičkim stvarima, kao što je npr. kapacitet, ali daljnjim razvijanjem ARPAnet mreža postala je današnji Internet. Prethodnik TCP protokola u ARPAnet mreži bio je NCP (engl. Network Control Protocol) koji je dizajniran kako bi dopustio korisnicima pristup i korištenje računala i uređaja na udaljenim lokacijama i prijenos datoteka između računala. [8]

## 3.1 Arhitektura TCP/IP modela

TCP/IP model ima četiri sloja, a to su: Aplikacijski sloj, Transportni sloj, Internet sloj te Sloj mrežnog sučelja. Svaki od slojeva iz TCP/IP modela odgovara jednom ili više slojeva iz OSI referentnog modela.

Aplikacijski sloj omogućava aplikacijama pristup servisima ostalih slojeva i definira protokole koje aplikacije koriste za razmjenu podataka. Najpoznatiji protokol Aplikacijskog sloja su HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) i Telnet.

Transportni sloj predstavlja vezu između aplikacija i mreže. Zadatak ovog sloja je održavanje komunikacije između aplikacija s obje strane. Glavni protokoli u ovom sloju su TCP i UDP protokoli. Transportni sloj TCP/IP modela odgovara sloju istog naziva u

[7] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 102
[8] Ibid., str. 122

OSI referentnom modelu, ali uključuje i dijelove koji se nalaze u Sesijskom sloju OSI modela.

Internet sloj je odgovoran za funkcije adresiranja, usmjeravanja, slanje paketa. Glavni protokoli u Internetskom sloju su IP, ARP, ICMP i IGMP. IP protokol je odgovoran za IP adresiranje, usmjeravanje, fragmentaciju te sastavljanje paketa. ARP (engl. Address Resolution Protocol) je protokol kojeg koristi IP, najviše IPv4 na način da mapira IP mrežnu adresu na hardversku adresu koju koristi protokol za podatkovne veze (Data link layer). ICMP (engl. Internet Control Message Protocol) protokol je odgovoran za pružanje dijagnostičkih funkcija i izvješćivanje pogrešaka koje su se dogodile zbog neuspješne dostave IP paketa. IGMP (engl. Internet Group Management Protocol) protokol je odgovoran za upravljanje IP multicast grupama.

Glavni zadatak sloja mrežnog sučelja je sastavljanje TCP/IP paketa na mrežnom mediju te primanje TCP/IP paketa s mrežnog medija. U većini slučajeva mrežni medij je u obliku kabela. Ovaj sloj nema protokole već LAN tehnologije poput Ethernet-a, token ring-a i WAN tehnologije poput X.25 i Frame Relay. Sloj mrežnog sučelja obuhvaća podatkovni i fizički sloj OSI referentnog modela.


Slika 1: Prikaz slojeva OSI referentnog modela i TCP/IP modela te protokola u TCP/IP modelu

Izvor:http://umag.hr/sadrzaj/dokumenti/NATJECAJ_informaticki_referent_Uvod_u_racunalne_mreze_Visoko_uciliste_Algebra.pdf

Slika 1 prikazuje slojeve OSI referentnog modela i TCP/IP. Glavna razlika između OSI referentnog modela i TCP/IP modela je u broju slojeva. [9]

# 4. Internet protokol verzije 4

Internet protokol nalazi se na mrežnom sloju OSI referentnog modela i na internet sloju TCP/IP modela. IPv4 koristi 32-bitnu logičku adresu, odnosno 2^32 IP adresa, a to je ukupno 4.29 milijardi adresa koje su već dodijeljene raznim korisnicima diljem svijeta. Postoje dvije vrste IP adresa, a to su privatne i javne. Kako je razvojem Interneta počelo nedostajati slobodnih IP adresa, rješenje tog problema bile su privatne adrese jer se one mogu duplicirati, ali uz uvjet da se ne nalaze na istoj lokalnoj mreži. Kada korisnik izlazi iz lokalne mreže na Internet, privatna adresa se pretvara u javnu adresu putem NAT (engl. Network Address Translation) metode. Usmjerivač na kojem je podešen NAT mijenja privatnu adresu sa svojom javnom koja se dalje usmjerava internetom. Nakon što se dobije odgovor ponavlja se postupak mijenjajući javnu adresu sa odgovarajućom privatnom adresom računala koje je poslao zahtjev.[10]

Prema Mujariću, osnovne značajke IP protokola su:[11]

- Definiranje sheme adresiranja na internetu
- Definiranje IP paketa
- Prosljeđivanje podataka između razine pristupa mreži i prijenosne razine
- Fragmentacija i sastavljanje paketa

## 4.1 Adresiranje IPv4 adresa

Prema Mujariću, IP adresa se koristi za adresiranje na Internet sloju TCP/IP modela. IP adresa predstavlja jedinstvenu adresu svakog uređaja koji se spaja na neku mrežu. IP adresa se zapisuje u četiri okteta, odnosno jednostavnije rečeno u četiri broja u decimalnom obliku odvojenim točkom. Primjer zapisa IP adrese je B.B.B.B gdje je B je decimalni broj zapisa jednog okteta. IP adresa može biti zapisana u decimalnom i u binarnom obliku zapisa. Primjer IP adrese zapisane u decimalnom

[9] "TCP/IP Protocol Arhitecture". 2017. Microsoft. https://technet.microsoft.com/enus/library/cc958821.aspx
[10] "IP adresa". 2012. Vidipedija. http://www.vidipedija.com/index.php?title=IP_adresa
[11] Mujarić, Eldis. 2009. "Računalne mreže". Layer-x. http://mreze.layer-x.com/s030100-0.html

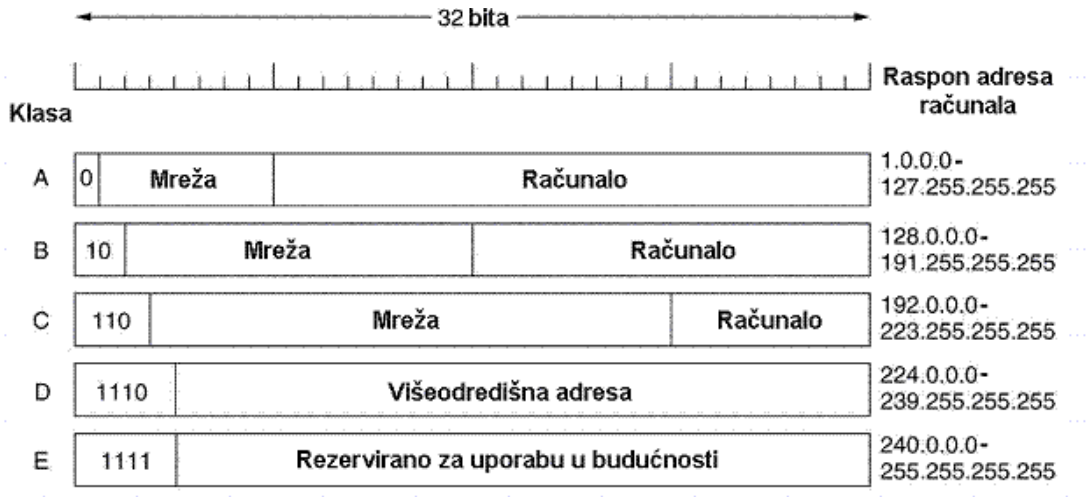
obliku je 192.168.1.30, dok u binarnom obliku zapisa je 11000000 10101000 00000001 00011110.[12]

Kod IPv4, IP adresa se sastoji od dva dijela:

- Adrese mreže (engl. network address) - identificira mrežu
- Adrese računala (engl. host address) – identificira host dio, tj. Domaćina

### 4.1.1 Klasifikacija IPv4 adresa

IP adrese podijeljene su u klase A,B,C,D i E. Klase IP adresa identificiraju se samo po prvih nekoliko bitova. Ukoliko je prvi bit 0, IP adresa pripada klasi A. Ukoliko je prvi bit 1, a drugi bit 0, radi se o klasi B IP adrese. Ukoliko su prva dva bita 1, a treći bit 0, radi se o klasi C IP adrese. IP adresa klase D je ako su prva tri bita 1,a četvrti 0. IP adresa klase E je ako su prva četiri bita 1. Tako da od 4.29 milijardi IP adresa, polovina adresa pripada klasi A, jedna četvrtina klasi B i jedna osmina klasi C. IP adresa klase D služi samo za više odredišne adrese, odnosno više odredišnu komunikaciju (engl. multicasting) . IP adrese klase E rezervirane su za buduće korištenje te eksperimentalno korištenje.




Slika 2. Klase IP adresa

Izvor: http://mreze.layer-x.com/s030101-0.html

[12] Mujarić, Eldis. 2009. "Računalne mreže". Layer-x. http://mreze.layer-x.com/s030101-0.html

Svaka klasa alocira određeni broj bitova za mrežni dio i određeni broj bitova za host dio, osim klasa D i E. Mrežni dio klase A ima alocirano 7 bitova (prvi bit je 0), a host dio ima alocirano 24 bitova. Zbog toga postoje samo 126 mreža klase A koje mogu imati do 2^24 -2 uređaja, tj. 16 777 214 uređaja. Mrežni dio klase B ima alocirano 14 bitova (prva dva bita su 10), a host dio ima alocirano 16 bitova. Zbog toga postoje 16 384 mreža klase B koje mogu imati od 2^16-2 uređaja, tj. 65 534 uređaja. Mrežni dio klase C ima alocirano 21 bit (prva tri bita su 110), a host dio ima alocirano 8 bitova. Zbog toga postoje 2^21 mreža odnosno 2 097 152 mreža klase C, a svaka mreža može imati 2^8-2 uređaja, tj. 254 uređaja. Klasa D rezervirana je za višeodredišne adrese, odnosno za istovremeno slanje na više različitih odredišta. Klasa E rezervirana je za uporabu u budućnosti. [13]

### 4.1.2 Tipovi IPv4 adresa

IP adrese podijeljene su na tri tipa a to su:

- Unicast adrese
- Multicast adrese
- Broadcast adrese

**Unicast adrese**

IPv4 unicast adrese identificiraju položaj, odnosno lokaciju sučelja na mreži. Funkcija IPv4 unicast adrese može se usporediti s funkcijom uličnog broja u adresi bez kojeg nije moguće točno locirati određeni stambeni ili poslovni objekt.

Na isti način IPv4 unicast adresa mora biti globalna i jedinstvena na mreži te mora imati jedinstveni format. IPv4 unicast adrese dostupne su samo za klasu A,B i C.

Svaka unicast IPv4 adresa sastoji se od dva dijela:

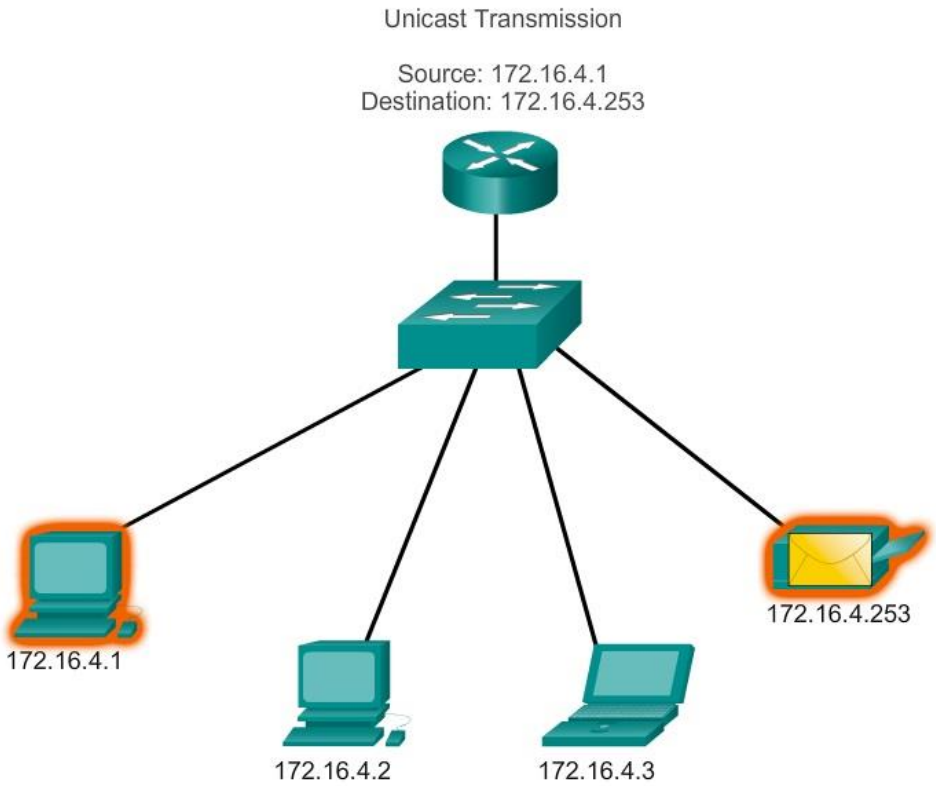
- Mrežnog ID-a (adresa mreže)
- Host ID-a (host adresa)

Mrežni dio unicast adrese je fiksni dio IPv4 adrese koji identificira skup sučelja te se oni nalaze na istom fizičkom i logičkom segmentu mreže koji su okruženi IPv4

[13] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 531, 532, 533

usmjerivačem. Na TCP/IP mrežama, mrežni segment je poznatiji kao podmreža. Sustavi koji se nalaze na istom fizičkom ili logičkom segmentu moraju koristiti isti mrežni ID i taj mrežni ID mora biti jedinstven za cijelu TCP/IP mrežu.

Host dio je varijabilni dio Ipv4 adrese te se koristi za identifikaciju sučelja mrežnog čvora. Host ID je jedinstven za mrežni ID. Jedinstvenost mrežnog ID-a za TCP/IP mrežu i host ID jedinstven za mrežni ID, onda je cjelokupna IPv4 unicast adresa jedinstvena za cijelu TCP/IP mrežu.




Slika 3: Komunikacija dva uređaja unicast adresom

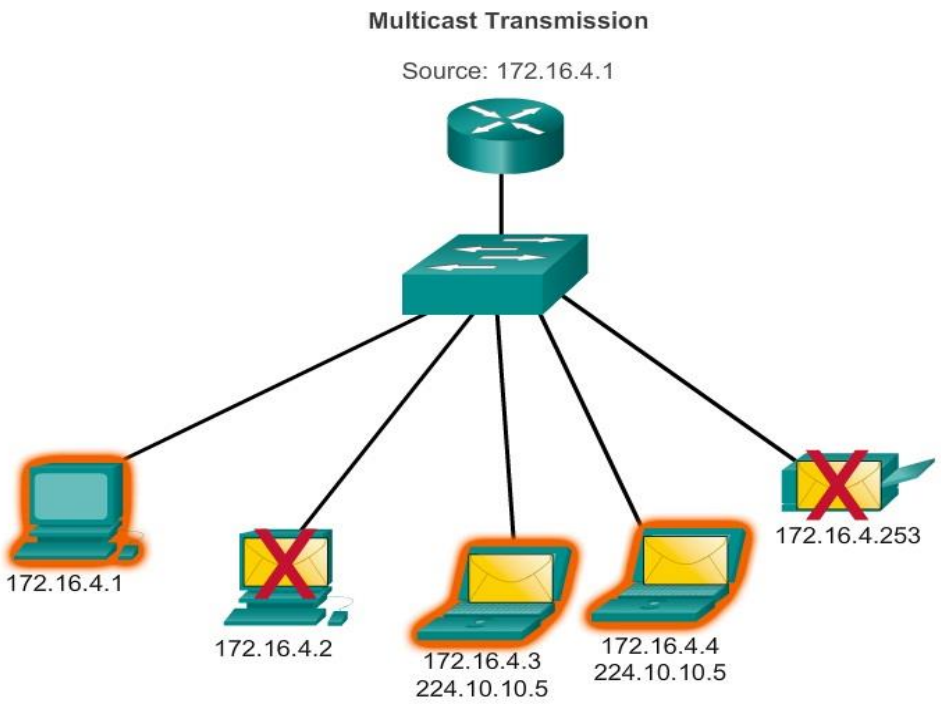
Izvor: http://www.hitechmv.com/wp-content/uploads/2014/05/unicastss1.jpg

Na slici 4 prikazana je komunikacija dva uređaja pomoću putem unicast adresom. Podaci se šalju podmrežom s jednog uređaja (računala s IP adresom 172.16.4.1) na drugi (pisača s IP adresom 172.16.4.253).

**Multicast adrese**

Ipv4 multicast adrese koriste se za slanje jednog paketa jednom ili većem broju primatelja i definirane su početnim bitovima 1110 koji pripadaju klasi D IP adresa. Skupina IPv4 multicast adresa ima raspon adresa od 224.0.0.0 do 239.255.255.255,

pri čemu su adrese u tom rasponu podijeljene na rezervirane adrese za lokalne linkove( reserved link local addresses) i globalno raspoložive adrese (globally scoped addresse). Rezervirane adrese za lokalne linkove imaju raspon od 244.0.0.0 do 244.0.0.255 te su rezervirane za protokole samo na lokalnom mrežnom segmentu. Globalno raspoložive adrese imaju raspon od 244.0.1.0 do 238.255.255.255 i slobodne su za korištenje na Internetu. Komunikacija multicast adresama koristi se za npr: video i audio emitiranje, distribuciju softvera, igranje na daljinu i dr. [14]




Slika 4: Komunikacija uređaja multicast adresama

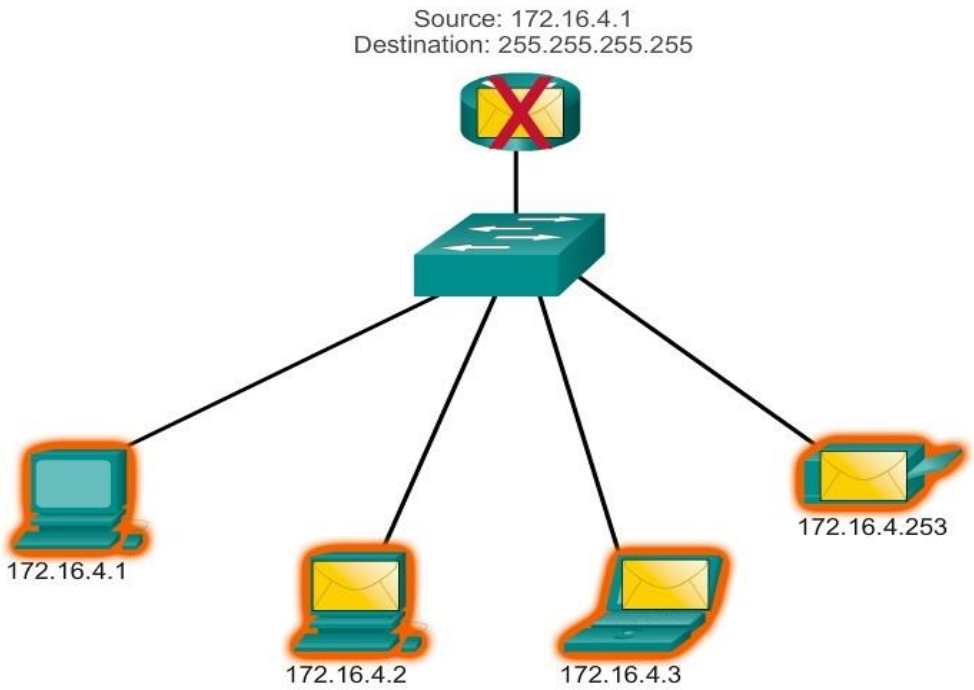
Izvor: http://cdn4.hitechmv.com/wp-content/uploads/2014/05/multicast-transmi1.jpg

Na slici 5 prikazana je komunikacija uređaja putem multicast adresa. Multicast prijenos podataka ostvaren je tako da se skup hostova (računala sa IP adresom 172.16.4.3 i 172.14.4.4) pretplate na multicast grupu pa im izvorni host (računalo s IP adresom 172.16.4.1) pošalje paket koji trebaju primiti. Izvorni host može poslati jedan paket stotinama odredišnim računalima.

[14] "IPv4 unicast, broadcast, and multicast". 2014. TechMV. http://www.hitechmv.com/ipv4-unicast-broadcast-and-multicast/

**Broadcast adrese**

IPv4 broadcast adrese koriste se za slanje paketa svim primateljima u mreži tako da se koristi broadcast adresa mreže. S broadcast-om paket kojeg se šalje sadrži odredišnu IP adresu sa svim hostovima. To znači da će svi hostovi na lokalnoj mreži broadcast domene moći primiti i pregledavati paket koji im je poslan.




Slika 5: Komunikacija uređaja broadcast adresama

Izvor: http://cdn2.hitechmv.com/wp-content/uploads/2014/05/limited-broad1.jpg

Postoje četiri vrste broadcast adresa, a to su:

- Mrežne broadcast adrese (Network Broadcast)
- Podmrežne broadcast adrese (Subnet Broadcast)
- Podmrežne adrese direktnog broadcasta (All Subnets Directed Broadcast)
- Ograničene broadcast adrese (Limited Broadcast)

Mrežne broadcast adrese su adrese koje su formirane postavljanjem svih bitova domaćina (hosta) na 1 za klasificirane adrese. Primjer broadcast adrese za

klasificiranu adresu podmreže 131.107.0.0/16 je 131.107.255.255. Usmjerivač ne prosljeđuje pakete broadcast mreži.

Podmrežne broadcast adrese su adrese koje su formirane tako da su svi bitovi domaćina (hosta) za neklasificiranu adresu postavljene na 1. Primjer podmrežne broadcast adrese za neklasificiranu adresu mreže 131.107.26.0/24 je 131.107.26.255. Podmrežne broadcast adrese se koriste za slanje paketa svim hostovima subnetted, supernetted ili bilo koje druge neklasificirane mreže. Također kao i kod mrežne adrese usmjerivač ne prosljeđuje podmrežne broadcast pakete.

Podmrežne adrese direktnog broadcasta su adrese koje su formirane tako da su bitovi domaćina (hosta) izvorne klasificirane adrese podmreže postavljeni na 1 za neklasificirani prefiks adrese. Primjer podmreže adrese direktnog broadcasta za adresu podmreže 131.107.26.0/24 je 131.107.255.255. Usmjerivači kod podmrežne adrese direktnog broadcasta može prosljeđivati broadcast pakete.

Ograničene broadcast adrese su adrese koje su formirane tako da je svih 32 bita postavljena na 1, odnosno adresa je 255.255.255.255. Ovaj tip adrese se koristi kada IP čvor mora obaviti isporuku paketa svima na lokalnoj mreži, a da je pritom mrežni ID nepoznat. Usmjerivači kod ovog tipa adrese ne prosljeđuje ograničene broadcast pakete.[15]

## 4.2 Zaglavlje IPv4 protokola

Internet protokol definira paket pod nazivom zaglavlje (tablica 1.). IP koristi zaglavlja kao uslugu prijenosa paketa između krajnjih sustava pomoću usmjerivača. Zaglavlje IPv4 protokola sastoji se od 14 polja, od kojih su 13 obvezna. U nastavku objašnjena su sva polja u zaglavlju IPv4 protokola.

[15] "IPv4 Addressing". 2009. Microsoft.https://technet.microsoft.com/en-us/library/dd379547%28v=ws.10%29.aspx

| | | | |
|---|---|---|---|
| Verzija | Duljina zaglavlja | Tip servisa | Duljina paketa |
| Identifikacija | | Kontrolne zastavice | Odmak fragmenta |
| Vrijeme života | Protokol | Checksum | |
| Izvorišna IP adresa | | | |
| Odredišna IP adresa | | | |
| Opcije | | | |
| Podaci | | | |

Tablica 1. Struktura IP zaglavlja

Izvor: William A. Shay., Savremene Komunikacione tehnologije i mreže

Verzija (engl. Version): Kod IPv4 verzija zauzima četiri bita i definira verziju IP-a koji je kreirao paket. Četiri bita imaju vrijednost 4, te to u binarnom obliku je 0100 koji ukazuje na IPv4 verziju. Polje verzija omogućava zajedničko funkcioniranje različitih verzija IP-a.

Duljina zaglavlja (engl. Header Lenght): Drugo polje u IPv4 zaglavlju je duljina zaglavlja koji definira broj 32-bitnih riječi u zaglavlju paketa. Kako je duljina zaglavlja promjenjiva, odnosno može sadržavati promjenjivi broj, ovo polje određuje veličinu zaglavlja. Najmanja moguća vrijednost ovog polja iznosi 5.

Tip servisa (engl. Type of service, TOS): Treće polje je tip servisa, duljina ovog polja iznosi 8 bita i njegova zadaća je da definira zahtjeve transportnog sloja u vezi načina rukovanja paketima. Opcije zahtjeva koje dopušta ovo polje su prioritet (engl. Precedence), malo kašnjenje (engl. Low delay), visoka propusnost (engl. High throughput) i visoka pouzdanost (engl. High reliability). Opcija zahtjeva, prioritet je tro bitno polje koje omogućava određivanje prioriteta paketa i posebno je koristan za ispunjavanje određene kvalitete servisa (QoS). Skala prioriteta iznosi od 0 za niski prioritet do 7 za visoki prioritet. Zahtjev za malim kašnjenjem koristan je kada korisnik

koji je prijavljen na udaljeno računalo želi brz odaziv. Zahtjev za visoku propusnost je koristan kod prijenosa velikih količina podataka. Zahtjev za visoku pouzdanost služi za traženje mreže koje nude pouzdane servise.

Ukupna duljina (engl. Packet lenght): Definira ukupnu duljinu IP paketa. Ovo polje zauzima 16 bita i osigurava maksimalnu duljinu od 65 535 bajta.

Identifikacija (engl. Identification): Zauzima 16 bita i važan je kod povezivanja fragmenata u paket. Primarna svrha ovog polja je identificiranje originalnih fragmenata IP zaglavlja.

Kontrolne zastavice (engl. Flags): Zauzimaju 3 bita i koriste se za kontrolu ili prepoznavanje fragmenata. Prvi bit u ovom polju je rezerviran te uvijek iznosi 0, drugi bit služi za fragmentiranje, ukoliko je vrijednost bita 0 paket se smije fragmentirati, a ukoliko je vrijednost bita 1 paket se ne smije fragmentirati. Treći bit predstavlja lokaciju paketa u nizu već fragmentiranih paketa, ukoliko je vrijednost bita 0, paket se nalazi na zadnjem fragmentnom mjestu u nizu ili nije fragmentiran, a ako je vrijednost bita 1, paket se ne nalazi na zadnjem mjestu fragmentiranih paketa i očekuje se dolazak još fragmentiranih paketa. Ovo polje sadrži „More Fragments bit“ (mfb) kojeg usmjerivač postavlja na 1 u svim fragmentima osim u posljednjem. Također postoji i „Do Not Fragment bit“, u slučaju da je on postavljen tada fragmentacija nije moguća. Ukoliko usmjerivač primi takav paket, on istog odbacuje te šalje poruku o greški do stanice s koje je poslan.

Odmak fragmenta (eng. Fragment offset): Zauzima 13 bita i njime je riješen problem sekvenciranja fragmenata označavanjem uređaja primatelja gdje se u cjelokupnoj poruci treba staviti svaki pojedini fragment. Odmak ima raspon od 0 do 8 191. Svaki fragment specificiran je jedinicama od 8 bajta, te zbog toga duljina fragmenta mora biti višekratnik broja 8. Kako je maksimalna dopuštena duljina IP zaglavlja 65 528, a duljina fragmenta mora biti višekratnik broja 8, 8 * 8 191 daje maksimalnu dopuštenu duljinu IP zaglavlja odnosno 65 528. Ukoliko ovo polje ima vrijednost 0, to znači da paketi nisu fragmentirani ili su prvi paketi u nizu fragmentiranih paketa.[16]

[16] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 347

Vrijeme života (engl. Time To Live. TTL): Ovo polje definira vrijeme koje paket može provesti na mreži i zauzima 8 bita. Nakon što paket stigne do drugog usmjerivača, taj usmjerivač smanjuje polje Vrijeme života za onoliko koliko je proveo na mreži, te se paket šalje slijedećem usmjerivaču. Kada vrijednost polja postane 0, usmjerivač odbacuje paket i šalje poruku o greški do stanice koja je poslala paket. Ovo polje sprječava da se problemi usmjeravanja ili problemi zagušenja neće odvijati beskonačno tj. da paketi neće kružiti u mreži.

Protokol (engl. Protocol): Ovo polje definira protokol višeg sloja te zauzima 8 bita. Omogućava prijenos podataka odredišnog IP-a do odgovarajućeg entiteta na toj strani. Na slici 6 prikazane su vrijednosti pojedinog protokola za ovo polje zaglavlja.

| Value (Hexadecimal) | Value (Decimal) | Protocol |
|---|---|---|
| 00 | 0 | Reserved |
| 01 | 1 | ICMP |
| 02 | 2 | IGMP |
| 03 | 3 | GGP |
| 04 | 4 | IP-in-IP Encapsulation |
| 06 | 6 | TCP |
| 08 | 8 | EGP |
| 11 | 17 | UDP |
| 32 | 50 | Encapsulating Security Payload (ESP) Extension Header |
| 33 | 51 | Authentication Header (AH) Extension Header |

Tablica 2: Vrijednosti pojedinih protokola za polje Protokol

Izvor: Charles M. Kozierok., The TCP/IP Guide

Checksum: Služi za detekciju grešaka u zaglavlju te da bi se podaci zaštitili od grešaka, odnosno da nije došlo do nekakve izmjene. Ovo polje se izračunava prilikom svakog prijenosa paketa kroz mrežu jer se prilikom prijenosa mijenja polje Vrijeme života. [17]

Izvorišna IP adresa (engl. Source Address): Sadrži adresu uređaja koji je poslao zaglavlje i zauzima 32 bita.

[17] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 538, 541

Odredišna IP adresa (engl. Destination Address): Sadrži adresu krajnje, tj. odredišne destinacije i zauzima 32 bita.

Opcije (engl. Options): Ovo polje nije obavezno u svakom paketu, ali može se koristiti za slanje zahtjeva za specijalno tretiranje paketa i varijabilne je duljine. Neke od opcija ovog polja su: „Record Route“, „Timestamp“, „Source Route“, „Loose Source Route“, i „Security“. Opcija „Record Route“ prati rutu kojom paket putuje. Svaki usmjerivač koji usmjerava paket, on zapiše svoju adresu na listu. Opcija „Timestamp“ slična je opciji „Record Route“. Osim zapisa adrese usmjerivača ova opcija zapisuje i vrijeme kada se je usmjerio paket. Opcija „Source Route“ omogućava pošiljatelju da naznači rutu kojom se treba proslijediti paket tako da se navedu sekvence IP adresa. Opcija „Loose Source Route“ ne osigurava točnu rutu, već daje listu usmjerivača preko kojih paket mora proći. Opcija „Security“ omogućava da se navedu određeni usmjerivači ili lokacije koje treba izbjeći tijekom usmjeravanja.

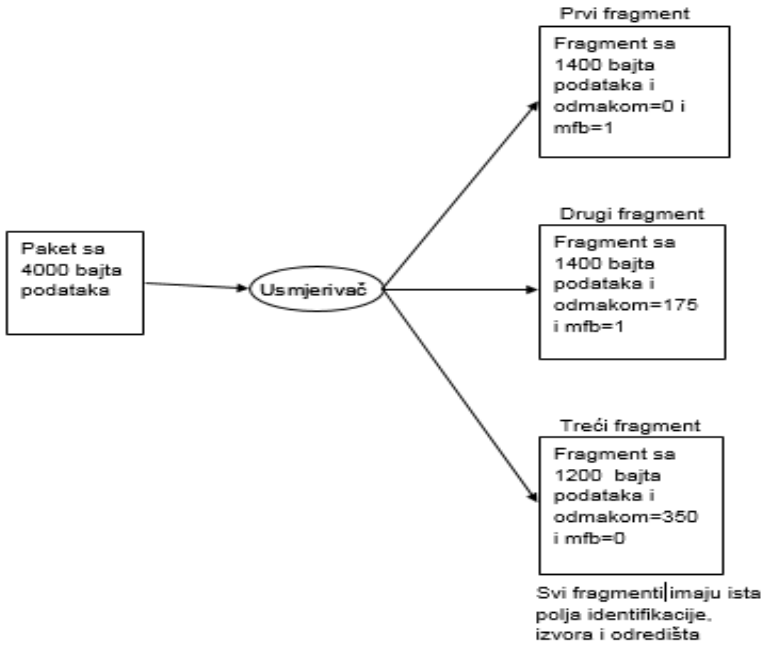
Podaci (engl. Data): Sadrže podatke koji su neophodni višem sloju i varijabilne je duljine. [18]

### 4.2.1 Fragmentacija IPv4 zaglavlja

Jedan od glavnih problema s kojim se suočava Internet protokol je da različite mrežne arhitekture dopuštaju različite veličine okvira koje se još nazivaju maksimalne jedinice prijenosa (engl. maximum transmission unit ili MTU). Ako je duljina IP paketa manja od MTU-a na kojeg se nailazi na putanji prijenosa, onda se prijenos odvija bez problema, ali ako je MTU manji, onda se paket dijeli na manje jedinice koje se nazivaju fragmenti. Ti isti fragmenti putuju do svojih konačnih odredišta preko različitih putanja te se na kraju ponovno sastavljaju. Da bi se fragmentacija uspješno izvršila, odredišni IP mora razlikovati fragmente od nefragmentiranih paketa, mora prepoznati fragmente koji odgovaraju istom paketu, kojim se redoslijedom moraju sastaviti i koliko se fragmenata nalazi u pojedinom paketu. Ove radnje omogućavaju polja Identifikacije, Kontrolne zastavice i Odmak fragmenta.

[18] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 537, 538, 539

U nastavku slijedi primjer fragmentacije paketa.




Slika 6. Fragmentacija paketa

Izvor: William A. Shay., Savremene Komunikacione tehnologije i mreže.

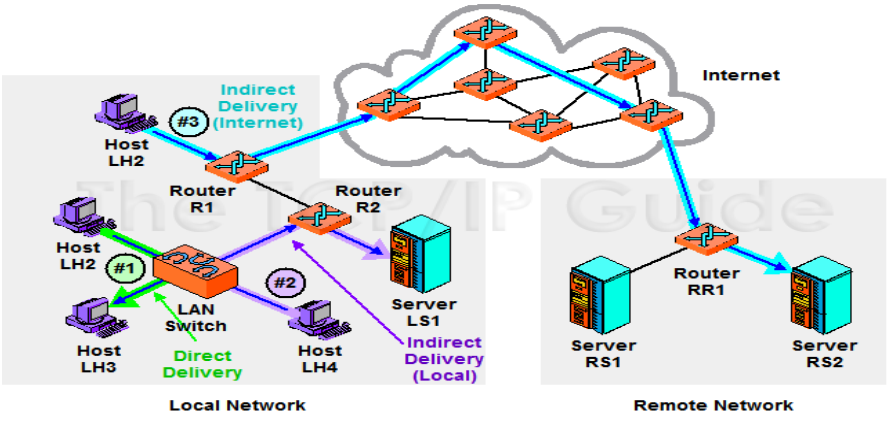
Na slici 6 prikazan je paket koji je podijeljen na tri fragmenta. Ako pretpostavimo da mreža ima MTU koji dopušta najviše 1400 bajta podataka. Dolaskom paketa veličine 4000 bajta usmjerivač dijeli paket na tri fragmenta. Prva dva fragmenta imaju po 1400 bajta podataka dok treći ima preostalih 1200 bajta. U prvom fragmentu polje odmak fragmenta ima vrijednost 0, te se time ukazuje da podaci počinju sa odmakom 0 u izvornom paketu. U drugom fragmentu odmak ima vrijednost 175 čime se ukazuje da njegovi podaci počinju od bajta 1400 (8*175) u paketu, dok treći fragment ima odmak 350 i njegovi podaci počinju od bajta 2800 (8*350) u paketu. Mfb „More fragments bit“ u prva dva fragmenta su 1 koji ukazuju da iza svakog postoji još fragmenata. U trećem fragmentu mfb je postavljen na 0 koji ukazuje da je to posljednji fragment. Kada odredišni IP primi dva različita fragmenta s istom identifikacijom, izvorišnom i odredišnom adresom on zna da fragmenti dolaze iz istog paketa. Nakon toga se sastavljaju paketi onim redom koji je određen vrijednošću polja odmaka.[19]

[19] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 540, 541

## 4.3 IPv4 usmjeravanje

„Usmjeravanje je proces prijenosa podataka sa izvorišta do odredišta putem određenog puta između dviju ili više mreža. Također omogućuje da dva ili više uređaja na različitim TCP/IP mrežama budu povezana jedno s drugim.“[20] Usmjeravanje uključuje TCP/IP host i IP usmjerivač. Oni moraju odlučiti na koji način će se paketi poslati. Svaki usmjerivač prihvaća zaglavlja iz raznih izvora. Nakon prihvaćanja zaglavlja usmjerivač ispituje IP adresu odredišta i odlučuje o next hop kojeg zaglavlje treba poduzeti kako bi paket stigao čim je moguće bliže odredištu. Usmjerivač ima skup informacija koje mu omogućavaju mapiranje između različitih mrežnih ID-ova i ostalih usmjerivača. Ove informacije se nalaze u strukturi podataka koje se nazivaju tablice usmjeravanja. Svaki podatak unutar tablice usmjeravanja predstavlja informacije o jednoj mreži, pod mreži ili hostu. Postoje dvije vrste usmjeravanja, a to su izravno i neizravno usmjeravanje. Izravno usmjeravanje se javlja kada se zaglavlje šalje između dva uređaja koji se nalaze na istoj mreži. Neizravno usmjeravanje se javlja kada uređaji nisu na istoj mreži, odnosno kada se zaglavlje šalje preko više usmjerivača do konačnog odredišta. [21]

Na slici 7 prikazano je izravno i neizravno dostavljanje IP zaglavlja.




Slika 7. Izravno i neizravno dostavljanje

Izvor:[http://www.tcpipguide.com/free/t_IPDatagramDirectDeliveryandIndirectDeliveryRouting.htm](http://www.tcpipguide.com/free/t_IPDatagramDirectDeliveryandIndirectDeliveryRouting.htm)

[20] "IP Routing". 2017. Techopedia. https://www.techopedia.com/definition/7816/ip-routing
[21] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. str. 357

Slika 7 prikazuje tri primjera isporuke IP zaglavlja. Prva isporuka označena zelenom bojom prikazuje izravnu isporuku dva uređaja unutar lokalne mreže. Druga isporuka označena ljubičastom bojom prikazuje neizravnu isporuku unutar lokalne mreže između klijenta i poslužitelja odvojena usmjerivačem. Treća isporuka označena je plavom bojom te prikazuje neizravnu isporuku između klijenta na lokalnoj mreži i poslužitelja na Internetu.[22]

# 5. Internet protokol verzije 6

Internet protokol verzije 6 je nova generacija protokola koja postupno zamjenjuje stariju verziju Internet protokola verzije 4. Kod IPv6 protokola adresa je veličine 128 bita što čini otprilike $3.4 \times 10^{38}$ adresa. Kada bi se adrese rasporedile po površini zemlje, postojale bi 1024 adrese po kvadratnom metru.[23]

Prema CARNet-u glavne značajke IPv6 protokola su:[24]

- Novi format zaglavlja
- Veličina adresnog prostora
- Ugrađeni sigurnosni mehanizmi
- Poboljšana podrška za kvalitetu usluge (QoS)
- Proširivost

## 5.1 Adresiranje IPv6 adresa

Velika potražnja za IP adresama dovela je do razvoja velikog adresnog prostora kojeg nudi IPv6. Prema procjenama u bežičnoj domeni postoji više od milijardu mobilnih uređaja, osobnih digitalnih pomoćnika (PDA) i drugih bežičnih uređaja koji zahtijevaju pristup Internetu, a svaki od njih zahtijeva svoju vlastitu jedinstvenu IP adresu. Duljina proširene adrese koju nudi Ipv6 uklanja potrebu za korištenjem tehnika poput NAT kako bi se izbjeglo istjecanje dostupnog adresnog prostora.[25] IPv6 adresa se razlikuje od IPv4 adrese. IPv6 adresa najčešće je zapisana u obliku

[22] "IP Datagram Direct Delivery and Indirect Delivery (Routing)". 2005. The TCP/IP Guide http://www.tcpipguide.com/free/t_IPDatagramDirectDeliveryandIndirectDeliveryRouting.htm
[23] "Ipv6 protokol". 2006. CARNet. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf
[24] Ibid.
[25] "IPv6 Addressing". 2006. IPv6.com https://www.ipv6.com/general/ipv6-addressing/

osam grupa heksadecimalnih kvarteta koji su međusobno odvojeni dvotočkama (:). Primjer 128 bitne IPv6 adrese je:

01110100011101110000000000000000000000000000000000000000000000000000

00000000000000000000101011111111000110111101111101111111111111111

IPv6 adresa u obliku osam grupa po 16 bitova:

0111010001110111 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000101011111111 0001101111011111 0111111111111111

Svaki blok adrese pretvara se u heksadecimalne znamenke te ih se razdvaja dvotočkom:

7477:0000:0000:0000:0000:0AFF:1BDF:7FFF

Ukoliko adresa sadrži mnogo nula, koristi se skraćeni zapis adrese. Skraćeni zapis adrese dobiva se izostavljanjem nula, ali umjesto njih zapisuju se dvije dvotočke (::). Stvarni broj izostavljenih nula izračunava se oduzimanjem broja heksadecimalnih znamenaka u notaciji od 32 broja heksadecimalnih znamenaka koje su potrebne za puni 128-bitni pregled adrese. Na primjer, prethodna adresa bi bila zapisana kao

7477::0AFF:1BDF:7FFF

Kako ova adresa sadrži 16 znamenaka, zna se da joj nedostaje 16 nula. U slučaju da adresa započinje nulom, adresa započinje dvotočkom. Na primjer adresa

0000:0000:0000:0000:0AFF:1BDF:000F:0077

može se zapisati kao

0AFF:1BDF:000F:0077

Kako bi se adrese pojednostavile, vodeće nule u četveroznamenkastim grupama ne moraju se navesti. Prethodna adresa bi izgledala u obliku:

::AFF:1BDF:F:77

Kako IPv4 dijeli svoje adrese u različite klase tako radi i IPv6. Trenutno postoje 22 različita tipa IPv6 adrese i svaki tip ima svoj jedinstveni bitski prefiks. Prefiksi mogu sadržavati od tri do deset bitova. Ukoliko adresa započinje s osam nula, ona odgovara

IPv4 adresi.[26] „Dio IPv6 adresa koje sadrže bitove čija je vrijednost fiksna ili određena prefiksom podmreže naziva se prefiks IPv6 adrese.“ IPv6 prefiksi označavaju se slično CIDR zapisu IPv4 protokola na način da koristi notaciju adresa/dužina prefiksa. Za primjer može poslužiti prefiks podmreže:

21DA:D3:0:2F3B::/64

Kod IPv4 koristila se je notacija prefiksa mreže koja je poznatija kao mrežna maska dok se kod IPv6 protokola koristi samo notacija s dužinom prefiksa[27].

### 5.1.1 Tipovi IPv6 adresa

Adrese kod Ipv6 protokola svrstavaju se u tri kategorije:

- Unicast (Jednoodredišne adrese)
- Anycast (Najbliže adrese)
- Multicast (Višeodredišne adrese)

Iz ove tri kategorije može se primjeriti da nema broadcasta adresa. U IPv6 protokolu izbačene su broadcast adrese zbog problema opterećenja uređaja na mreži i čestog nepotrebnog korištenja univerzalnih paketa koji nisu bili namijenjeni uređajima. Ulogu broadcast adresa u IPv6 preuzele su anycast adrese.

**Unicast adrese**

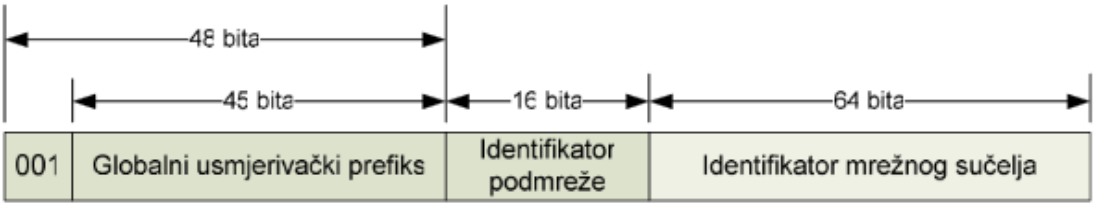
Unicast adresiranje je adresiranje jednog mrežnog sučelja. Unicast adresirani paketi isporučuju se samo jednom sučelju pa se prilikom adresiranja koristi komunikacija 1:1. IPv6 unicast adrese mogu se spojiti s prefiksima proizvodne duljine slično CIDR IPv4 adresama. Postoji nekoliko tipova IPv6 unicast adresa, a to su:

- Globalne jednoodredišne adrese
- Adrese lokalne poveznice (engl. link-local) Scoped Local Addresses
- Adrese administrativne domene (engl. site-local)

[26] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 566,567
[27] "Ipv6 protokol". 2006. CARNet. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

- Jedinstvene lokalne IPv6 jednoodredišne adrese
- Posebne adrese

Globalne jednoodredišne adrese slične su javnim IPv4 adresama i dostupne su na globalnoj razini. One imaju prefiks 2000::/3.



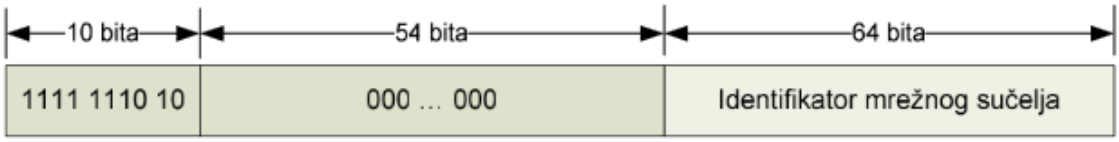

Slika 8: Struktura globalne jednoodredišne adrese

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

Struktura globalno jednoodredišne adrese podijeljena je na četiri dijela. Prvi dio predstavlja prefiks globalne adrese te on binarno iznosi 001. Drugi dio predstavlja globalni usmjerivački prefiks te on označava administrativnu domenu određene organizacije. Prefiks globalne adrese i globalni usmjerivački prefiks čine kombinaciju od 48 bita. Usmjerivači prosljeđuju sav promet koji se poklapa s prvih 48 bita adrese prema usmjerivačima neke određene organizacije. Treći dio strukture je identifikator podmreže. On se koristi unutar neke organizacije kako bi identificirao podmrežu kojoj je paket namijenjen. Ovo polje veličine je 16 bita i omogućava stvaranje 65.536 podmreža. Četvrti dio strukture je identifikator mrežnog sučelja. To je 64 bitni identifikator koji određuje mrežno sučelje određene podmreže unutar domene organizacije kojoj je paket namijenjen.

Jednoodredišne adrese za lokalno korištenje dijele se na adrese lokalne poveznice i adrese administrativne domene.

Adrese lokalne poveznice dizajniranje su kako bi se koristile za adresiranje na jednoj vezi za svrhu kao što je konfiguracija automatske adrese, otkrivanje susjeda ili kad nema usmjerivača. Usmjerivači ne smiju prosljeđivati pakete s Link-local izvorom ili odredišnim adresama prema drugim vezama. Ovaj tip adrese može se koristiti samo na lokalnim mrežama. Prefiks ove adrese je FE80::/64.

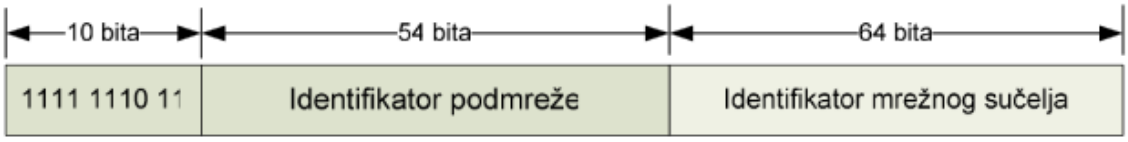



Slika 9: Struktura adrese lokalne poveznice

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

Struktura adrese lokalne poveznice podijeljena je na 3 dijela. Prvi dio predstavlja fiksnu binarnu vrijednost 1111 1110 10. Drugi dio je 54 bitni niz nula, dok treći dio predstavlja identifikator mrežnog sučelja.

Adrese administrativne domene izvorno su dizajnirane za uporabu pri adresiranju unutar web-lokacije bez potrebe za globalnim prefiksom. Ovaj tip adrese se koriste za komunikaciju među dva čvora unutar iste administrativne domene i nisu dostupne izvan nje. One odgovaraju adresnom prostoru privatnih IPv4 adresa kao što su 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Prefiks ove adrese je FEC0::/10.

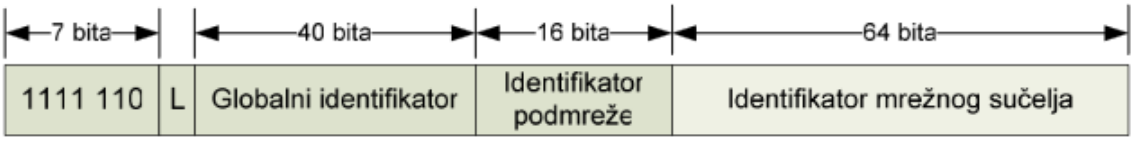



Slika 10: Struktura adrese administrativne domene.

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

Struktura adrese administrativne domene podijeljena je na 3 dijela. Prvi dio predstavlja fiksnu binarnu vrijednost 1111 1110 11. Drugi dio predstavlja Identifikator podmreže, dok treći dio predstavlja identifikator mrežnog sučelja.

Jedinstvene lokalne IPv6 jednoodredišne adrese slične su privatnim IPv4 adresama te omogućavaju privatno adresiranje. Prefiks ove adrese je FD00::/7.




Slika 11: Struktura jedinstvene lokalne IPv6 jednoodredišne adrese

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

Struktura jedinstvene lokalne IPv6 jednoodredišne adrese podijeljena je na pet dijelova. Prvi dio predstavlja fiksnu binarnu vrijednost 1111 110. Drugi dio predstavlja zastavicu L. Ukoliko je vrijednost zastavice 1, adresa će imati gore navedeni prefiks, a ukoliko je vrijednost zastavice 0, onda je ostavljena za buduću upotrebu. Treći dio predstavlja globalni identifikator. Četvrti dio je identifikator podmreže, a peti predstavlja identifikator mrežnog sučelja.[28]

U posebne adrese spadaju neodređene adrese (engl. Unspecified) i adrese povratne petlje (engl. Loopback).

Neodređena adresa identična je neodređenoj IPv4 adresi 0.0.0.0, te se upotrebljava kada sučelje nama svoju IPv6 adresu. Vrijednost neodređene adrese je 0:0:0:0:0:0:0:0.

Povratna adresa ima istu namjenu kao i IPv4 adresa 127.0.0.1. Vrijednost povratne adrese je 0:0:0:0:0:0:0:1. Sučelja koriste ovu adresu samo kako bi omogućili da pakete šalju samom sebi. [29]

**Anycast adrese**

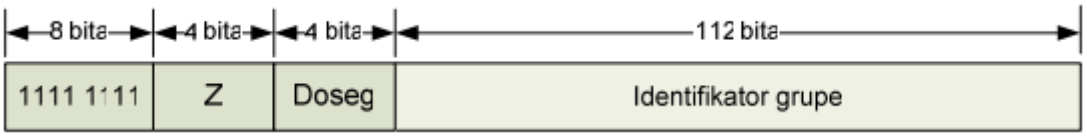
Anycast adrese su jedinstveni tip adresa koje su nove IP adrese u IPv6. Anycast adresa je adresa koja je dodijeljena na više sučelja koji većinom pripadaju različitim čvorovima, sa svojstvom da se paket koji se šalje na anycast adresu usmjerava na najbliže sučelje koje ima tu adresu. Anycast adrese se dodjeljuju iz unicast adresnog prostora tako da se koristi bilo koji definirani tip unicast adrese. Ovaj tip adrese sintaktički se ne razlikuje od unicast adresa. Kada se unicast adresa dodjeljuje na više

[28] "Ipv6 protokol". 2006. CARNet. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf
[29] "Types and Categories of IPv6 Addresses". 2008. IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SSB27U_5.4.0/com.ibm.zvm.v54.kijl0/hcsk7b3014.htm

od jednog sučelja, ona se pretvara u anycast adresu s time da čvorovi na koje je dodijeljena adresa moraju biti konfigurirani da bi znali da je to anycast adresa.[30]

**Multicast adrese**

Multicast adrese se koriste za slanje paketa grupi primatelja. IPv4 dopušta adresiranje pomoću klase D u adresnoj shemi. Kod IPv6 multicast adrese se dodjeljuju iz multicast bloka. U multicast adrese spada 1/126 odnosno 0.8% cjelokupnog adresnog prostora. Multicast adrese se prepoznaju po početnih osam bitova koji su 1111.1111. Stoga svaka multicast adresa ima prefiks FF00::/8. Princip adresiranja je isti kao i kod IPv4, ali kako je veći adresni prostor IPv6 pruža više jedinstvenih multicast adresa. Kod IPV6 multicast adresiranja čvorovi mogu u bilo kojem trenutku napustiti multicast grupu.




Slika 12: Struktura multicast adrese

Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf

Struktura multicast adrese podijeljena je na četiri dijela. Prvi dio predstavlja osam bitni prefiks multicast adrese koji iznosi 1111 1111. Drugi dio predstavlja četvero bitno polje zastavice Z. Ukoliko je vrijednost zastavice postavljena na 0, onda se radi o višeodredišnoj adresi koju je dodijelila organizacija IANA (engl. Internet Assigned Numbers Authority). Ako je vrijednost zastavice postavljena na 1 radi se o privremenoj višeodredišnoj adresi. Treći dio predstavlja polje doseg. Polje doseg veličine je 4 bita te namjena mu je prikazivanje dosega koji je namijenjen za višeodredišni paket. Najčešće vrijednosti polja su 1, 2 i 5. Vrijednost 1 ukazuje na doseg lokalnog mrežnog sučelja. Vrijednost 2 ukazuje na doseg lokalne poveznice, dok vrijednost 5 ukazuje na

[30] "IP Version 6 Addressing Arhitecture". 2006. Internet Engineering Task Force. https://www.ietf.org/rfc/rfc4291.txt

doseg lokalne administrativne domene. Posljednji dio predstavlja identifikator grupe i veličine je 112 bita.[31]

## 5.2 Zaglavlje Ipv6 protokola

Zaglavlje IPv6 protokola je pojednostavljen u odnosu na zaglavlje IPv4 protokola. U usporedbi s IPv4 zaglavljem odmah na pogled uočavaju se dvije razlike. Prva razlika je da IPv6 adresa ima više bitova, a zaglavlje ima manje polja odnosno opcija. Zaglavlje IPv6 protokola može imati nula ili više opcijskih zaglavlja koja su zapravo proširenja za osnovno, tj. fiksno zaglavlje koje je prikazano na tablici 3. Bitno je za napomenuti da su izbačena neka polja IPv4 zaglavlja zbog zastarjelosti i slabog korištenja. U nastavku su objašnjena sva polja u zaglavlju IPv6 protokola. [32] [33]

<table>
<tr><td>Verzija</td><td>Prioritet</td><td colspan="2">Oznaka toka</td></tr>
<tr><td colspan="2">Duljina korisnih informacija</td><td>Slijedeće zaglavlje</td><td>Broj skokova</td></tr>
<tr><td colspan="4">Izvorišna adresa</td></tr>
<tr><td colspan="4">Odredišna adresa</td></tr>
</table>

Tablica 3: Fiksno zaglavlje IPv6 protokola

Izvor: William A. Shay., Savremene Komunikacione tehnologije i mreže.

Verzija (engl. Version): Kod IPv6 polje verzija zauzima četiri bita i definira verziju IP-a koji je kreirao paket. Ovo polje ima istu svrhu kao i kod IPv4.

Prioritet (engl. Priority): Ovo polje zauzima osam bita, koristan je za kontrolu zagušenja i zamjenjuje polje Tip servisa iz IPv4 zaglavlja. Koncept ovog polja je jednostavan: veće vrijednosti ukazuju na važnije pakete. IPv6 prepoznaje da su kašnjenja u nekim aplikacijama kao npr. Email skoro pa neprimjetna, dok kašnjenja u

[31] "Ipv6 protokol". 2006. CARNet. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf
[32] "IPv6 - Headers". 2008. Tutorials point. https://www.tutorialspoint.com/ipv6/ipv6_headers.htm
[33] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 561

drugim aplikacijama poput multimedijalnih uzrokuju nemogućnost korištenja istih. Glavna zadaća ovog polja je da identificira one pakete koji pripadaju pojedinoj aplikaciji. Vrijednost prioriteta nalazi se na skali od 0 do 7. Na primjer, email ima prioritet 2, FTP i HTTP 4, Telnet 6, a SNMP 7.

Oznaka toka (engl. Flow label): Koristi se s poljem Prioriteta te zauzima 20 bitova. Služi za identificiranje paketa koji zahtijevaju "specijalan tretman" u usmjerivaču. IPv6 protokol definira red paketa koji se šalju od izvora do odredišta kao odaziv na neku aplikaciju. Ukoliko su paketi dizajnirani na takav način da se prikazuju u realnom vremenu na odredištu, "specijalni tretman" podrazumijeva njihovo usmjeravanje na način da svi paketi stignu u ispravnom redoslijedu. Da bi se uspostavio tok, izvor generira nasumično bilo koji broj (osim nule) i smješta ga u ovo polje zaglavlja kod svih paketa. Nakon toga usmjerivač primjenjuje hash funkciju na broj toka kako bi se izračunala lokacija na kojoj se nalaze informacije na koji način paket treba tretirati. Upute o "specijalnom tretmanu" paketa postavljene su prije slanja istog. Usmjerivač koristi hash funkciju zbog toga što ta funkcija predstavlja najbrži način pretrage, a nasumični brojevi se koriste zbog toga što oni dovode do manjeg broja kolizija kada se na njih primjene hash funkcije. [34]

Duljina korisnih informacija (engl. Payload lenght): Služi kako bi se reklo usmjerivačima koliko informacija pojedini paket sadrži, može sadržavati i dodatna zaglavlja o kojim će biti riječ u nastavku. Ovo polje ima 16 bitova i može naznačiti do 65535 bajta, ali s dodatnim zaglavljima, točnije sa zaglavljem za pojedinačne skokove (Hop-by-hop header) taj broj može biti i veći. Vrijednost ovog polja uvijek mora biti postavljena na nulu. Ovo polje zamjenjuje polje duljina zaglavlja iz IPv4 zaglavlja

Slijedeće zaglavlje (engl. Next header): Zamjenjuje polje Protokol iz Ipv4 zaglavlja, zauzima 8 bitova i ima dvije svrhe. Kada zaglavlje ima dodatna zaglavlja ovo polje određuje identitet prvog zaglavlja proširenja koji je slijedeći u nizu. Kada zaglavlje nema nikakva dodatna zaglavlja, ovo polje služi svrsi kao i stari IPv4 protokol i ima iste vrijednosti samo za IPv6 protokol. Ovo polje određuje gornji sloj, tj. protokol transportnog sloja.

[34] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 561, 562

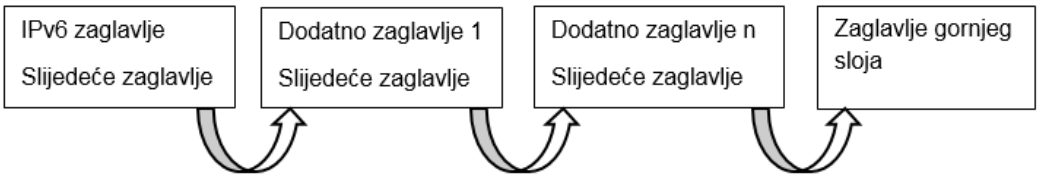
Broj skokova (engl. Hop limit): Ima istu funkciju kao i polje Vrijeme života kod IPv4 zaglavlja. Vrijednost ovog polja se smanjuje za 1 kad prođe kroz neki uređaj. Kada vrijednost polja dođe do 0, paket se odbacuje.

Izvorišna adresa (engl. Source address): Označava adresu pošiljatelja paketa i ima 128 bitova.

Odredišna adresa (engl. Destination address): Označava adresu primatelja kojem je namijenjen paket i ima 128 bitova. [35]

### 5.2.1 Dodatna zaglavlja IPv6 protokola

IPv6 protokol osim fiksnog zaglavlja sadrži i dodatna zaglavlja. Fiksno zaglavlje sadrži samo one informacije koje su neophodne i izbjegava one informacije koje nisu potrebne ili se rijetko koriste. Takve informacije stavljaju se između fiksnog zaglavlja i zaglavlja gornjeg sloja u dodatna zaglavlja. Svako dodatno zaglavlje određeno je različitom vrijednošću. Kada se koriste dodatna zaglavlja, polje slijedeće zaglavlje kao što je već navedeno ukazuje na prvo dodatno zaglavlje. Ukoliko ima više od jednog dodatnog zaglavlja polje slijedeće zaglavlje u nastavku zaglavlja ukazuje na drugo itd. Ovo polje na zadnjem dodatnom zaglavlju ukazuje na zaglavlje gornjeg sloja. [36]




Slika 13. Format zaglavlja proširenja

Izvor: https://www.tutorialspoint.com/ipv6/ipv6_headers.htm

Postoje šest tipova dodatnih zaglavlja a to su:

- Zaglavlje sa opcijama za odredište
- Zaglavlje fragmentacije
- Zaglavlje za pojedinačne skokove
- Zaglavlje za usmjeravanje

[35] "IPv6 - Headers". 2008. Tutorials point. https://www.tutorialspoint.com/ipv6/ipv6_headers.htm
[36] Ibid.

- Sigurnosno zaglavlje
- Zaglavlje autentifikacije

Zaglavlje s opcijama za odredište (engl. Destination options header): Ovo zaglavlje sadrži informacije o odredištu i ne koristi se za vrijeme usmjeravanja.[37]

Zaglavlje fragmentacije (engl. Fragmentation header): Osigurava informacije u slučaju neophodnog ponovnog sastavljanja fragmenata paketa, sadrži podatke o odmaku fragmenta, Last fragment bitu i identifikatoru koji je jedinstven za originalni paket. Ovo je slično fragmentaciji i ponovnom sastavljanju kod IPv4 protokola, ali postoji i razlika. Prijelazni IPv4 usmjerivači mogli su fragmentirati pakete ukoliko su oni bili preveliki dok IPv6 to ne dopušta. Prednost toga je što to pojednostavljuje logiku usmjerivača i doprinosi efektivnijem i bržem usmjeravanju. Ukoliko usmjerivač primi paket koji je prevelik, on šalje poruku preko ICMP-a natrag do izvora. Poruka sadrži informacije da je paket prevelik i označava se maksimalna dopuštena veličina. Nakon toga će izvor fragmentirati paket i poslati fragmente, koji sadrže zaglavlje fragmentacije. Fragmenti će se ponovno sastaviti na odredištu. [38]

Zaglavlje za pojedinačne skokove (engl. Hop-by-hop header): Ovo zaglavlje, ukoliko postoji, mora se proučiti u usmjerivaču jer se koristi za nošenje dodatnih informacija koje se moraju pregledati na svakom usmjerivaču duž puta za isporuku paketa. Ovo zaglavlje mora biti odmah nakon fiksnog zaglavlja i njegova prisutnost identificirana je vrijednošću nulom u polju slijedeće zaglavlje IPv6 zaglavlja. Ideja ovog zaglavlja je da se navedu informacije koje moraju imati svi usmjerivači. Kako je veličina polja duljina korisnih informacija 16 bitova , maksimalna veličina paketa je 64 KB. Ovo zaglavlje dopušta pakete veće od 64 KB, što je korisno kod prijenosa većih količina podataka kao npr. video zapisa.[39]

Zaglavlje za usmjeravanje (engl. Routing header): Osigurava dodatne informacije o usmjeravanju kao što je opcija Loose Source Route kod IPv4. Odnosno ono sadrži 124 bitne adrese usmjerivača preko kojih paket mora proći.

[37] William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 563
[38] Ibid.
[39] "IPv6 Headers". 2010. Portal IPv6 Cuba. http://www.cu.ipv6tf.org/literatura/chap3.pdf

Sigurnosno zaglavlje (engl. Security header): Omogućava da se šifrira sadržaj paketa te da ga samo primatelj može pročitati.

Zaglavlje autentifikacije (engl. Authentication header): Ovo zaglavlje služi za autentifikaciju paketa koja se koristi sa IPSec-om, odnosno sigurnosnim protokolom na nivou paketa.[40]

### 5.2.2 Fragmentacija IPv6

Postupak fragmentacije IPv6 je sličan fragmentaciji IPv4, samo što se treba paziti na rukovanje dodatnim zaglavljima. U svrhu fragmentacije, zaglavlja se dijele na dva dijela:

- Nefragmentirani dijelovi: Nefragmentirani dio uključuje glavno zaglavlje izvornog zaglavlja i dodatna zaglavlja koja moraju biti prisutna svakom fragmentu.
- Fragmentirani dijelovi. Fragmentirani dio uključuje podatkovni dio zaglavlja i ostala dodatna zaglavlja.

Nefragmentirani dio mora biti prisutan u svakom fragmentu dok fragmentirani dio je podijeljen među fragmentima. Kako bi se fragmentiralo zaglavlje, uređaj kreira skup fragmentiranih zaglavlja od kojih svaki sadržava:

- Nefragmentirani dio: Cijeli nefragmentirani dio od izvornog zaglavlja s duljinom korisnih informacija (Payload lenght) izmijenjen je na duljinu zaglavlja fragmenta.
- Zaglavlje fragmenta: Zaglavlje fragmenta s odmakom fragmenta (Fragment offset), identifikacijom i zastavicama postavljeni su na isti način kao što su postavljeni i u IPv4.
- Fragment: Sadrži fragment od fragmentiranog dijela izvornog zaglavlja.

U nastavku slijedi primjer fragmentacije IPv6. Pretpostavimo da je IPv6 datagram velik 370 bajta koji se sastoji od 40 bajta IP zaglavlja, četiri zaglavlja proširenja s 30 bajta i 210 bajta podataka. Dva zaglavlja proširenja su nefragmentirana

[40] S William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd: Kompjuter Biblioteka, 2004. str. 564

dok su dva fragmentirana. MTU iznosi 230 bajta. Po ovome se zaključuje da treba tri fragmenta, a ne dva zbog toga što se treba staviti 30 bajta nefragmentiranog zaglavlja proširenja u svaki fragment i da duljina svakog fragmenta bude višestruka od broja 8. Struktura fragmenata je takva da:[41]

1. Prvi fragment: Sastojao bi se od 100 bitnog nefragmentiranog dijela, nakon čega slijedi 8 bitno zaglavlje fragmenta i prvih 120 bajta fragmentiranog dijela izvornog datagrama. To bi sadržavalo dva fragmentirana zaglavlja proširenja i prvih 60 bajta podataka. To ostavlja 150 bajta podataka za slanje.
2. Drugi fragment: Sadržavao bi nefragmentirani dio od 100 bajta. Nakon toga slijedi zaglavlje fragmenta i 120 bajta podataka. Nakon ovog fragmenta ostati će 30 bajta podataka za slanje.
3. Treći fragment: Sadržavao bi nefragmentirani dio od 100 bajta, zaglavlje fragmenta i posljednjih 30 bajta podataka.

## 5.3 IPv6 usmjeravanje

Većina koncepta IPv6 usmjeravanja isti je kao i kod IPv4. Datagrami se isporučuju izravno kada su uključeni izvorni i odredišni čvorovi na istoj mreži. Ukoliko se čvorovi nalaze na različitim mrežama tada je isporuka neizravna i prvo se radi usmjeravanje na odredišnu mrežu, a tek zatim na krajnje odredište. Usmjerivači gledaju IP adrese i određuju koji je dio identifikator mreže (network ID) i koji je dio identifikator domaćina (host ID). IPv6 to određuje na isti način kao i u IPv4 bez klasa neovisno o IPv6 unicast adresama. Usmjeravanje se obavlja na bazi next-hop jer izvori ne znaju na koji način će datagrami doći od točke A do točke B. Usmjerivanje se izvodi pomoću usmjerivača koji održavaju tablice usmjerivanja koje im govore gdje treba proslijediti datagrame kako bi stigli na odredišta.

Većina promjena koje su se dogodile u usmjeravanju kod IPV6 povezana je s promjenama koje su se dogodile kod drugih protokola. Neka od glavnih pitanja vezana za usmjerivanje i usmjerivače kod IPv6 su[42] :

[41] Ibid., str. 420
[42] Charles M. Kozierok., The TCP/IP Guide, San Francisco: no strach press, 2005. Str. 421

- **Hijerarhijsko usmjerivanje i agregacija.** Jedan od glavnih ciljeva strukture za organiziranje unicast adresa bilo je poboljšanje usmjerivanja. Format unicast adresiranja osmišljen je tako da se omogući bolja podudarnost između adresa i Internetske topologije te olakša agregiranje rute.
- **Adrese sa lokalnim dosegom.** Lokalne adrese za upotrebu koje uključuju adrese lokalne poveznice i adrese administrativne domene definirane su u IPv6 i usmjerivači ih moraju prepoznati i također moraju ih usmjeriti ili ne usmjeriti kada je to potrebno.
- **Multicast i Anycast usmjerivanje.** Multicast adrese su standard u IPv6 protokolu dok su u IPv4 protokolu opcionalne te prilikom usmjerivanja usmjerivači moraju ih podržavati. Anycast adresiranje je nova vrsta adresiranja kod IPv6 te ih usmjerivači također moraju podržavati.
- **Podržavanje više funkcija.** Moraju se dodati sposobnosti usmjerivačima kako bi podržali nove značajke koje dovodi IPv6.
- **Novi protokoli usmjerivanja.** Dotadašnji protokoli usmjerivanja poput protokola RIP moraju biti ažurirani kako bi podržavali IPv6.
- **Prijelazni problemi.** Usmjerivači čine važnu ulogu u podržavanju prijelaza s IPv4 na IPv6. Oni imaju odgovornost za povezivanje i obavljanje prijelaza kako bi IPv4 i IPv6 mogli međusobno komunicirati tijekom duljeg razdoblja prijelaza s IPv4 na IPv6 odnosno sve dok se svi uređaji prebace na IPv6.

# 6. Zaključak

Kada je IPv4 dizajniran, nije bio predviđen eksponencijalni rast tolikog broja uređaja kojima je potrebna IP adresa te je zbog toga nastao problem nedostatka adresnog prostora kojeg je posjedovao IPv4. Iz tog razloga razvijen je novi IPv6 protokol koji će trajno riješiti taj problem. Cjelokupan broj IP adresa IPv4 protokola stane u manje od 1% cjelokupnoga adresnog prostora koje ima IPv6 protokol što predstavlja ogromno povećanje adresnog prostora.

Prelazak s IPv4 na IPv6 neće biti lagan zbog decentraliziranosti interneta te će se odvijati postupno jer ne postoji način da se organizira istovremeni prelazak s IPv4 na IPv6 protokol. IPv6 ima dodatne mogućnosti kao što su autentifikacija i šifriranje te je dodana bolja sigurnost pomoći IPSec koje IPv4 nije imao.

Velike promjene odnose se na zaglavlja protokola. Kod zaglavlja IPv6 protokola neka polja su izbačena, neka su zadržana, ali im je promijenjena pozicija i dodano je jedno polje. IPv4 ima samo jedno zaglavlje, dok IPv6 protokol ima jedno fiksno i jedno ili više dodatnih zaglavlja koja omogućuju jednostavnu implementaciju proširenja protokola kako na krajnjim točkama tako i na usmjerivačima na IPv6 mreži. Pozitivne i efikasne značajke IPv4 zadržane su kod IPv6, dok su nedostaci ispravljeni.

Također IPv6 ima pojednostavljeno zaglavlje tako da je usmjeravanje puno efikasnije u usporedbi s prethodnom verzijom protokola iako se odvija na sličan način kod oba protokola.

Fragmentacija i ponovno sastavljanje paketa kod IPv6 protokola se ne izvodi više u međučvorovima kao kod IPv4. Fragmentacija IP paketa imala je nedostatke te su sva polja vezana za fragmentaciju uklonjena s fiksnog IPv6 zaglavlja.

# Literatura

## Knjige


1. Charles M. Kozierok., The TCP/IP Guide, San Francisco, 2005.
2. James F. Kurose, Keith W. Ross, Computer networking a top-down approach, Boston, 2008.
3. Radovan Mario, Računalne mreže (1), Rijeka, 2010.
4. William A. Shay., Savremene Komunikacione tehnologije i mreže, Beograd, 2004.


## Internet izvori:


"IP adresa". 2012. Vidipedija. http://www.vidipedija.com/indeks. php?title=IP_adresa (pristupljeno: 16. lipnja 2017).

"IPv4 Addressing". 2009. Microsoft. https://technet.microsoft.com/en-us/library/dd379547%28v=ws.10%29.aspx (pristupljeno: 22. lipnja 2017).

"IP Routing". 2017. Techopedia. https://www.techopedia.com/definition /7816/ip-routing (pristupljeno: 16. lipnja 2017).

"IP Datagram Direct Delivery and Indirect Delivery (Routing)". 2005. The TCP/IP Guide http://www.tcpipguide.com/free/t_IPDatagramDirectDeliveryandIndirect DeliveryRouting.htm (pristupljeno: 20. lipnja 2017).

"IPv4 unicast, broadcast, and multicast". 2014. TechMV. http://www.hitechmv.com/ipv4-unicast-broadcast-and-multicast/ (pristupljeno: 25. lipnja 2017).

"Ipv6 protokol". 2006. CARNet. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-173.pdf (pristupljeno: 1. srpnja 2017).

"IPv6 Addressing". 2006. IPv6.com https://www.ipv6.com/general/ipv6-addressing/ (pristupljeno: 8.srpnja 2017).

"IP Version 6 Addressing Arhitecture". 2006. Internet Engineering Task Force. https://www.ietf.org/rfc/rfc4291.txt (pristupljeno: 17. srpnja 2017).

"IPv6 - Headers". 2008. Tutorials point. https://www.tutorialspoint.com/ipv6/ipv6_headers.htm (pristupljeno: 20. srpnja 2017).

"IPv6 Headers". 2010. Portal IPv6 Cuba. http://www.cu.ipv6tf.org/literatura/chap3.pdf (pristupljeno: 25. srpnja 2017).

Mujarić, Eldis. 2009. "Računalne mreže". Layer-x. http://mreze.layer-x.com (pristupljeno: 15. lipnja 2017).

Pralas, Toni. 2008. "Računalne mreže – OSI referentni model". Sys.portal Carnet. https://sysportal.carnet.hr/node/352 (pristupljeno: 10. lipnja 2017).

"TCP/IP Protocol Arhitecture". 2017. Microsoft. https://technet.microsoft.com /en-us/library/cc958821.aspx (pristupljeno: 20. lipnja 2017)

"Types and Categories of IPv6 Addresses". 2008. IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SSB27U_5.4.0/com.ibm.zvm.v54.kijl0/hcsk7b3014.htm (pristupljeno: 15. srpnja 2017).

"Uvod u računalne mreže". 2014. Algebra otvoreno učilište. http://umag.hr/sadrzaj/dokumenti/NATJECAJ_informaticki_referent_Uvod_u_racunalne_mreze_Visoko_uciliste_Algebra.pdf (pristupljeno: 6. rujna 2017).

# Popis slika



# Popis tablica

Sažetak

U ovom završnom radu se obrađuje usporedba Internet protokola verzije 4 i Internet protokola verzije 6. Internet protokoli služe za prijenos podataka s izvorišta na odredište. Na početku rada objašnjen je OSI referentni model i TCP/IP model. Nadalje u ovom radu bit će ukazane osnovne razlike između ova dva protokola poput duljine adresa i adresnog prostora, razlike između zaglavlja pojedinog protokola, usporedba adresiranja i usmjeravanja paketa između izvorišta i odredišta. Osnovna zadaća ovog rada je ukazati na razlike između dva protokola.

Ključne riječi: Internet protokol verzije 4, Internet protokol verzije 6, IPv4, IPv6, IP adresa, usmjeravanje, adresiranje

Summary

In this final paper, a comparison of Internet Protocol Version 4 and Internet Protocol Version 6 is handled. Internet protocols serve to transfer data from sources to the destination. At the beginning of the work, the OSI reference model and the TCP/IP model were explained. Further, in this paper, the basic differences between these two protocols, such as the length of address and address space, the differences between the headers of a particular protocol, comparison of addressing and routing of packets between source and destination will be shown. The basic task of this paper is to point to the differences between the two protocols.

Keywords: Internet protocol version 4, Internet protocol version 6, IPv4, Ipv6, IP address, routing, addressing.