Značajke IP adresa i usmjeravanja paketa u telekomunikacijskoj mreži

Knögel, Nikola

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Nikola Knögel

ZNAČAJKE IP ADRESA I USMJERAVANJE PAKETA U TELEKOMUNIKACIJSKOJ MREŽI

CHARACTERISTICS OF THE IP ADDRESSING AND PACKET ROUTING IN TELECOMMUNICATION NETWORK

Završni rad

Zagreb, rujan 2020.

SVEUŠILIŠTE U ZAGREBU
FAKULTET PROMETNIH
ZNANOSTI ODBOR ZA ZAVRŠNI
RAD

Zagreb, 27. ožujka 2018.

Zavod: **Zavod za informacijsko komunikacijski promet**

Predmet: **Tehnologija telekomunikacijskog prometa I**

ZAVRŠNI ZADATAK br. 4612

Pristupnik: **Nikola Knögel (0135236661)**

Studij: Promet

Smjer: Informacijsko-komunikacijski promet

Zadatak: **Značajke IP adresa i usmjeravanja paketa u telekomunikacijskoj mreži**

Opis zadatka:

Opisati TCP/IP protokolarni složaj i detaljno objasniti ulogu mrežnog sloja. Navesti karakteristike IP protokola, strukturu IP adrese, adresni prostor i različite vrste IP adresa. Objasniti uloge različitih uređaja za usmjeravanje te na primjeru prikazati usmjeravanje temeljeno na IP protokolu između dvije točke u mreži.

Mentor:

doc. dr. sc. Marko Matulin

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Završni rad

ZNAČAJKE IP ADRESA I USMJERAVANJE PAKETA U TELEKOMUNIKACIJSKOJ MREŽI

CHARACTERISTICS OF THE IP ADDRESSING AND PACKET ROUTING IN TELECOMMUNICATION NETWORK

Mentor: doc. dr. sc. Marko Matulin

Student: Nikola Knögel, 0135236661

Zagreb, rujan 2020.

Sažetak

U ovom radu objašnjen je TCP / IP (*Transmission Control Protocol / Internet Protocol*) protokolarni složaj i navedeni su njegovi slojevi. Prikazana je uloga protokola mrežnog sloja, i koje funkcije obavlja. Potom su objašnjeni IPv4 protokol i IPv6 protokol. Objašnjeni su korisnički prostor i prostor sustava te što je *paged pool* i *nonpaged pool*. Prikazano je usmjeravanje temeljeno na IP protokolu koristeći zadani pristupnik i tablicu usmjeravanja.

Ključne riječi: TCP/IP, mrežni sloj, IP protokoli, adresni prostor, usmjeravanje.

Summary

In this paper, the TCP / IP (Transmission Control Protocol / Internet Protocol) protocol stack is explained, and its layers are listed. The role of the network layer protocol is shown, and what functions it performs. The IPv4 protocol and the IPv6 protocol are then explained. User space and system space are explained and what is a paged pool and a nonpaged pool. Routing based on the IP protocol using the default gateway and routing table is shown.

Key words: TCP/IP, Internet layer, IP protocols, address space, routing.

Sadržaj

1. Uvod 1
2. TCP / IP protokolarni složaj 2
2.1 Aplikacijski sloj 2
2.2. Transportni sloj 3
2.2.1 User Datagram Protocol (UDP) 3
2.2.2 Transmission Control Protocol 4
2.3. Internet sloj 7
2.4. Sloj podatkovne veze 8
3. Uloga protokola mrežnog sloja 9
3.1. Protokol razlučivosti adrese (ARP) 9
3.2. Internet Control Message Protocol (ICMP) 11
3.2.1.Izvor gašenja poruka (engl. Source quench message) 11
3.2.2. Problem parametara 12
3.2.3.Vrijeme je prekoračeno poruka (engl. Time exceeded message) 12
3.2.4.Odredište je nedostupno (engl. Destination un-reachable) 13
3.2.5. Poruka o preusmjeravanju 14
3.3. Internet Group Management Protocol (IGMP) 14
3.3.1. IGMPv1 15
3.3.2. IGMPv2 16
3.3.3. IGMPv3 16
4. Osnovne značajke IP protokola 18
4.1. IPv4 18
4.2. IPv6 20
5. Adresni prostor 23
5.1. Korisnički prostor i prostor sustava 24
5.2. Paged pool i nonpaged pool 26
6. Usmjeravanje temeljeno na IP protokolu 27
6.1. Zadani pristupnik 27
6.2. Tablica usmjeravanja 28
6.2.1 Izravno povezane podmreže 29
6.2.2. Statičko usmjeravanje 29
6.2.3. Dinamičko usmjeravanje 31
7. Zaključak 33

Literatura.. 34
Popis slika.. 36

1. Uvod

Tema završnog rada je Značajke IP adresa i usmjeravanje paketa u telekomunikacijskoj mreži. IP (*Internet Protocol*) adresa je brojčana oznaka dodijeljena svakom uređaju spojenom na računalnu mrežu koji koristi Internet protokol za komunikaciju. Usmjeravanje je postupak odabira putanje za promet u mreži ili između više mreža.

Završni rad podijeljen je u sedam cjelina:

1. Uvod
2. TCP/IP protokolarni složaj
3. Uloga protokola mrežnog sloja
4. Osnovne značajke IP protokola
5. Adresni prostor
6. Usmjeravanje temeljeno na IP protokolu
7. Zaključak.

U drugom poglavlju opisane su značajke TCP / IP (*Transmission Control Protocol / Internet Protocol*) protokolarnog složaja te su opisani aplikacijski sloj, transportni sloj, internet sloj i sloj podatkovne veze .

U trećem poglavlju su opisane uloge protokola mrežnog sloja. Objašnjeni su protokoli razlučivosti adrese (ARP - *Address Resolution Protocol)* , *Internet Control Message Protocol* (ICMP) i *Internet Group Management protocol* (IGMP).

U četvrtom poglavlju objašnjene su osnovne značajke IP protokola IPv4 i IPv6 kao i njihove karakteristike. Prikazan i objašnjen je izgled njihovog zaglavlja.

U petom poglavlju objašnjeno je što je adresni prostor, koje su njegove prednosti i kako se on koristi.

U šestom poglavlju prikazano je usmjeravanje temeljeno na IP protokolu. Opisana je zadaća zadanog pristupnika i tablice usmjeravanja te su objašnjene sve tri metode za popunjavanje tablice usmjeravanja.

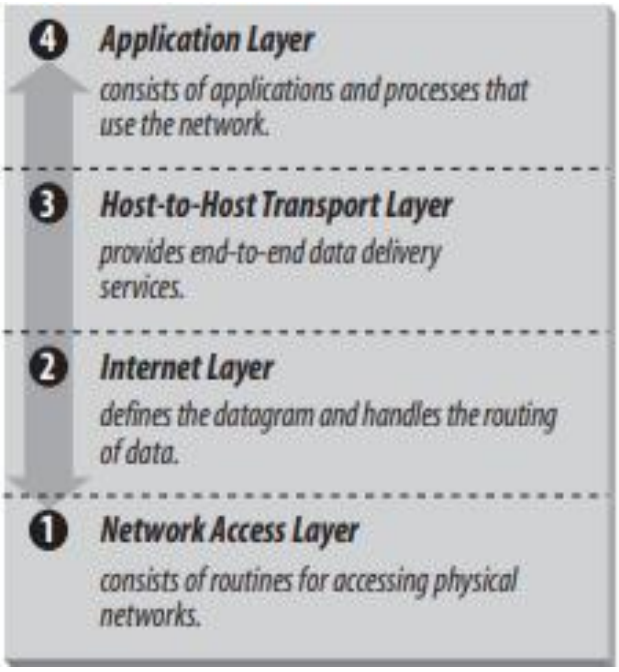
U sedmom poglavlju ili u zaključnom poglavlju su istaknuta saznanja iz navedenih poglavlja i završna razmatranja.

2. TCP / IP protokolarni složaj

TCP / IP složaj je skup komunikacijskih protokola koji se koriste za povezivanje mrežnih uređaja na Internetu. Značajke TCP / IP protokolarnog složaja su otvoreni standardni protokoli, besplatno dostupni i neovisno razvijeni od bilo kojeg računalnog hardvera ili operativnog sustava. Budući da je tako široko podržan, TCP / IP idealan je za objedinjavanje različitih hardverskih i softverskih komponenti, čak i ako se ne komunicira putem interneta.

Zbog toga TCP / IP je u mogućnosti integrirati u mnogo različitih vrsta mreža. TCP / IP može se pokrenuti preko Etherneta, DSL veze, *dial-up* linije, optičke mreže i gotovo bilo koje druge vrste fizičkog medija za prijenos.

Na slici 1 prikazan je TCP / IP složaj koji sastavljen od četiri sloja: aplikacijskog sloja, transportnog sloja, internet sloja i sloja podatkovne veze, [1].



Slika 1: TCP/IP arhitektura, [1]

2.1 Aplikacijski sloj

Na vrhu arhitekture TCP / IP složaja nalazi se aplikacijski sloj. Aplikacijski sloj uključuje sve procese koji za prijenos podataka koriste protokole transportnog sloja.

Najpoznatiji implementirani aplikacijski protokoli su:

1. Telnet – Protokol mrežnog terminala, koji omogućuje udaljenu prijavu putem mreže.

2. FTP (*File Transfer Protocol*) – koristi se za interaktivni prijenos datoteka.
3. SMTP (*Simple Mail Transfer Protocol*) – isporučuje elektroničku poštu.
4. HTTP (*Hypertext Transfer Protocol*) – način prijenosa podataka na globalnoj mreži.
5. DNS (*Domain Name System*) – preslikava IP adrese u imenima dodijeljenim mrežnim uređajima.
6. OSPF (*Open Shortest Path First*) – koristi se za pronalaženje najboljeg puta između izvora i odredišnog usmjerivača koristeći svoj prvi najkraći put.
7. NFS (*Network File System*) – Ovaj protokol omogućuje dijeljenje datoteka različitim domaćinima na mreži, [1].

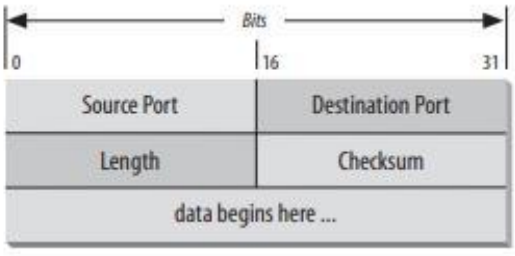
2.2. Transportni sloj

Dva najbitnija protokola na transportnom sloju su TCP (*Transmission Control Protocol*) i UDP (*User Datagram Protocol*). UDP se koristi kada je brzina poželjnija i kada ispravljanje pogrešaka nije potrebno (poput usluge telefonskih poziva, video konferencija i *stream*-a, te za prijenos podataka). Oba protokola isporučuju podatke između aplikacijskog sloja i Internet sloja.

2.2.1 User Datagram Protocol (UDP)

User Datagram Protocol omogućuje aplikacijskim programima izravan pristup usluzi dostave datagrama, poput usluge dostave koju pruža IP.

UDP je nepouzdan, bezkonekcijski protokol za prijenos datagrama. "Nepouzdan" samo znači da u protokolu nema tehnike za provjeru jesu li podaci ispravno stigli na odredište. Unutar računala UDP će ispravno dostaviti podatke. UDP koristi 16-bitne *Source Port* i *Destination Port* polja u zaglavlju da bi dostavili podatke ispravnim procesom prijave, [1]. Na slici 2 prikazan je format UDP zaglavlja.



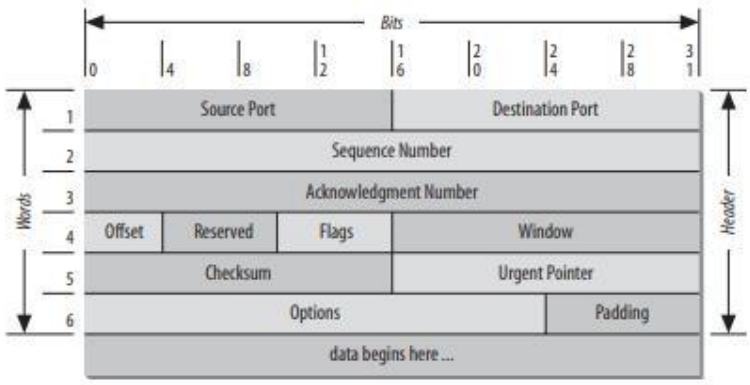
Slika 2: UDP format zaglavlja, [1]

2.2.2 Transmission Control Protocol

TCP protokol konekcijski je orijentiran protokol. Glavna zadaća navedenog protokola jest uspostava krajnje komunikacije između aplikacija. TCP može uspostaviti komunikaciju sa slojevima iznad i ispod sebe, a to su aplikacijski i internet sloj.

TCP pruža pouzdanost mehanizmom koji se zove *Positive Acknowledgment with Retransmission* (PAR). Sustav koji koristi PAR šalje podatke opet, osim ako ne primi podatak iz udaljenog sustava da su podaci stigli u redu. Jedinica razmijenjenih podataka između surađujućih TCP modula naziva se segment (vidi sliku 3). Svaki segment sadrži kontrolni zbroj koji primatelj koristi za provjeru da su podaci neoštećeni. Ako se segment podataka primi neoštećen, prijemnik šalje pozitivnu vrijednost potvrde natrag pošiljatelju. Ako je podatkovni segment oštećen, prijemnik ga odbacuje. Nakon odgovarajućeg vremenskog razdoblja, TCP modul koji šalje, šalje ponovno bilo koji segment za koji nije primljeno pozitivno priznanje.

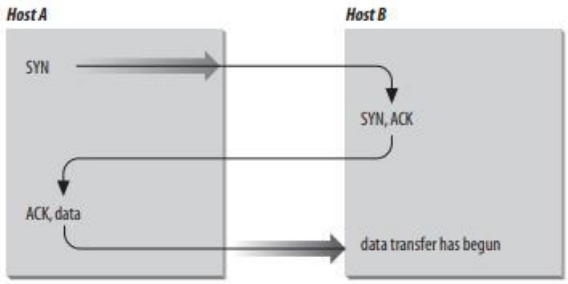
TCP je orijentiran na vezu. TCP uspostavlja logičnu *end-to-end* vezu između dvoje domaćina koji komuniciraju. Izmjenjuju se kontrolne informacije, koje se nazivaju rukovanje, između dvije krajnje točke za uspostavljanje dijaloga prije prijenosa podataka. TCP označava upravljačku funkciju segmenta postavljanjem odgovarajućeg bita u polju *Flag*.



Slika 3: TCP format segmenta, [1]

Vrsta rukovanja koju koristi TCP naziva se trosmjerno rukovanje, jer se segmenti dijele na tri dijela. Na slici 4 prikazan je najjednostavniji oblik trostranog stiska ruke. Domaćin A započinje vezu slanjem domaćinu B segment s postavljenim bitom "*Synchronize sequence numbers*" (SYN). Ovaj segment govori domaćinu B koje veze domaćin A želi, i to govori B koji će niz narednih brojeva A koristiti kao početni broj za njegove segmente (brojevi slijeda koriste se za održavanje podataka u pravilnom redoslijedu.) Domaćin B reagira na A s segmentom koji ima "*Acknowledgment*" (ACK) i postavljeni su SYN bitovi. B segment prepoznaje primitak A

segmenta i obavještava A s nizom brojeva s kojim će započeti B. Na kraju domaćin A šalje segment koji potvrđuje primanje segmenta B i prenosi prve stvarne podatke.



Slika 4: Trosmjerno rukovanje, [1]

Nakon te razmjene, TCP domaćin A ima potvrdu da je udaljeni TCP funkcionalan i spreman za primanje podataka. Čim se uspostavi veza, podaci se mogu poslati. Kad moduli za suradnju završe prijenos podataka, oni će razmijeniti trosmjerno rukovanje sa segmentima koji sadrže oznaku "*No more data from sender*“ bit (FIN bit) za zatvaranje veze.

TCP gleda na podatke koje šalje kao neprekidni tok bajtova, a ne kao neovisne pakete. Stoga TCP vodi računa da održi redoslijed u kojem su bajtovi poslani i primljeni. *Sequence Number* i *Acknowledgment Number* polja u zaglavlju TCP segmenta prate bajtove.

TCP standard ne zahtijeva da svaki sustav započne brojanje bajtova s bilo kojim određenim brojem; svaki sustav odabire broj koji će koristiti kao početnu točku. Da bi pratili ispravan protok podataka, svaki kraj veze mora znati početni broj drugog kraja. Dva kraja veze sinkroniziraju sustave brojanja bajtova razmjenom SYN segmenata tijekom rukovanja. *Sequence Number* polje u segmentu SYN sadrži *Initial Sequence Number* (ISN), koji je polazište za sustav numeriranja bajtova. Iz sigurnosnih razloga ISN treba biti slučajni broj.

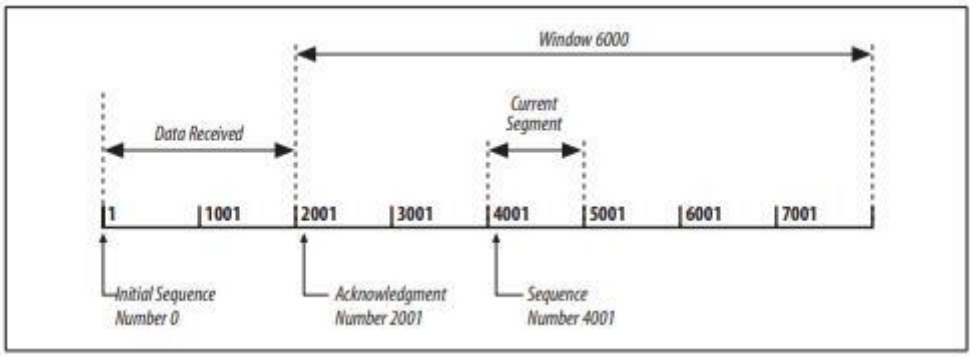
Svaki bajt podatka numerira se sekvencijalno iz ISN-a, tako da prvi pravi bajt podatka koji je poslan ima sekvencijalni broj ISN + 1. Sekvencijalni broj u zaglavlju podataka, segment identificira sekvencijalnu poziciju u protoku podataka prvog bajta podataka u segmentu. Na primjer, ako je prvi bajt u protoku podataka bio redni broj 1(ISN = 0) i 4000 bajta podataka je već preneseno, tada je prvi bajt podataka u trenutnom segmentu bajt 4001, a sekvencijalni broj bi bio 4001.

Acknowledgment segment (ACK) obavlja dvije funkcije: pozitivnu potvrdu i kontrolu protoka. Potvrda govori pošiljatelju koliko podataka je primljeno i koliko ih primatelj može još primiti. *Acknowledgment Number* je redni broj sljedećeg bajta koji prijemnik očekuje da će primiti. Standard ne zahtijeva pojedinačno potvrdu za svaki paket. *Acknowledgment Number* je

pozitivna potvrda svih bajtova do tog broja. Na primjer, ako je prvi poslani bajt bio numeriran sa 1 i 2000 bajtova je uspješno primljeno, tada bi *Acknowledgment Number* bio 2001.

Polje *Window* sadrži prozor ili broj bajtova koji je udaljeni kraj u stanju prihvatiti. Ako prijemnik može prihvatiti još 6000 bajtova, tada će prozor biti 6000 bajtova. Prozor upućuje pošiljatelja da može nastaviti slanje segmenata sve dok je ukupan broj bajtova koje pošalje manji od bajtova prozora koje prijemnik može prihvatiti. Prijemnik kontrolira tok bajtova od pošiljalaca promjenom veličine prozora. Nulti prozor upućuje pošiljatelja da prestane sa prijenosom sve dok ne dobije različitu vrijednost od nule.

Na slici 5 prikazan je TCP tok podataka koji započinje s *Initial Sequence Number*-om 0. Sustav prijema je primio i priznao 2000 bajtova, tako da je *Acknowledgment Number* 2001. U prijemniku se također nalazi dovoljno prostora za još 6000 bajtova. Pošiljalac trenutno šalje segmente od 1000 bajtova počevši s rednim brojem 4001. Pošiljalac nije primio potvrdu za bajtove od 2001, ali nastavlja s slanjem podataka sve dok se nalazi unutar prozora. Ako pošiljalac ispuni prozor i ne primi potvrdu prethodno poslanih podataka, nakon odgovarajućeg vremena, bude poslao podatke ponovno počevši od prvog nepriznatog bajta.



Slika 5: TCP protok podataka, [1]

Na slici 5 ponovni prijenos započeo bi od bajta 2001. ako se ne dobiju daljnje potvrde. Ovaj postupak osigurava pouzdano primanje podataka na kraju mreže.

TCP je također odgovoran za isporuku podataka primljenih s IP-a u ispravnu aplikaciju. Aplikacija za koju su vezani podaci identificirana je 16-bitnim brojem i naziva se *port number*. Ispravno slanje podataka u i iz aplikacijskog sloja je važan dio ono što radi transportni sloj, [1].

2.3. Internet sloj

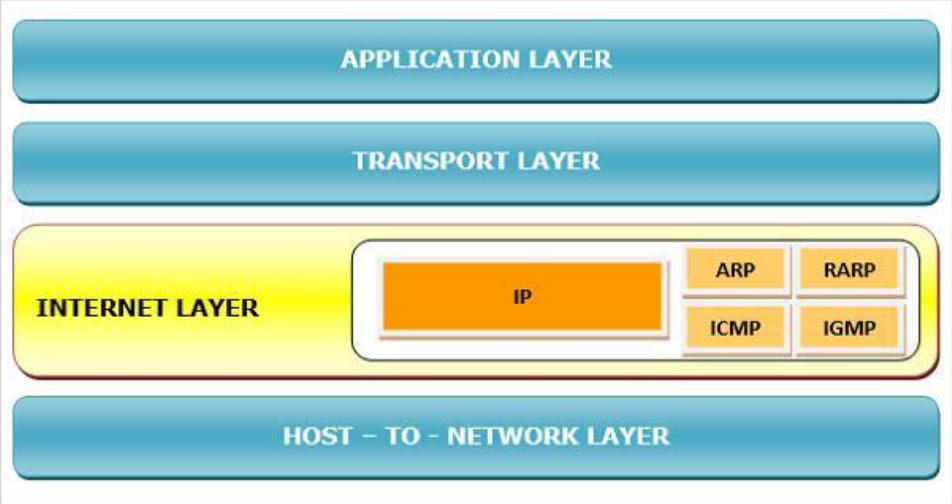
Internetski sloj odgovoran je za logičan prijenos paketa podataka putem interneta. Može se usporediti s mrežnim slojem OSI modela.

Glavne funkcije internetskog sloja su:

- prenosi paket podataka na sloj veze,
- svaki paket podataka usmjerava neovisno od izvora do odredišta, koristeći optimalnu rutu,
- ponovno sastavlja *out-of-order* pakete kada stignu na odredište,
- upravlja pogreškama u prijenosu paketa podataka i fragmentacijom paketa

podataka. Na slici 6 prikazani su protokoli koji se koriste u ovom sloju su:

- *Internet Protocol*, IP - to je bezkonekcijski i nepouzdan protokol koji pruža najbolju uslugu dostave. Prenosi pakete podataka zvane datagrami koji putuju različitim rutama kroz više čvorova.
- ARP (*Address Resolution Protocol*) - ovaj protokol mapira logičku adresu ili internetsku adresu domaćina na njegovu fizičku adresu.
- RARP (*Reverse Address Resolution Protocol*) - služi za pronalaženje internetske adrese domaćina kada je poznata njegova fizička adresa.
- ICMP (*Internet Control Message Protocol)* - nadzire slanje upita kao i poruke greške.
- IGMP (*Internet Group Message Protocol*) - omogućuje istovremeno slanje poruke grupi primatelja, [2].



Slika 6: Internet sloj u paketu TCP / IP složaja, [2]

2.4. Sloj podatkovne veze

Na ovom sloju nalaze se protokoli potrebni za povezivanje domaćina s fizičkom mrežom i isporuku podataka preko njega. Paketi s internetskog sloja šalju se niz sloj podatkovne veze radi isporuke unutar fizičke mreže. Odredište može biti drugi domaćin u mreži, on sam ili usmjerivač za daljnje prosljeđivanje. Dakle, internetski sloj ima pogled na cjelokupni *Internetwork* (praksa povezivanja više mreža, tako da bilo koji par domaćina u povezanim mrežama može razmjenjivati poruke bez obzira na njihovu hardversku razinu umrežavanja) dok je sloj podatkovne veze ograničen na granicu fizičkog sloja koju često određuje uređaj razine 3, poput usmjerivača, [3].

Protokoli sloja podatkovne veze su:

- Ethernet protokol kojim je definirano povezivanje lokalnih mreža zasnovanih na različitim tipovima fizičkog medija, pri različitim brzinama prijenosa, četiri formata Ethernet okvira koja su trenutno u primjeni (Ethernet II, Ethernet 802.3, Ethernet 802.4 i SNAP Ethernet).
- SLIP (*Serial Line Internet Protocol*), RFC 1 055 - standard za prijenos IP paketa preko modemskih veza koje podržavaju TCP / IP složaj
- PPP *(Point to Point Protocol*) RFC 1 548 – standard za prijenos podataka preko modemskih veza, [4].

3. Uloga protokola mrežnog sloja

Protokoli su formalna pravila ponašanja. U međunarodnim odnosima protokoli smanjuju probleme uzrokovane kulturološkim razlikama kada različite nacije rade zajedno. Pristajući na zajednički niz pravila koja su široko poznata i neovisna o bilo kojem nacionalnom običaju, protokoli umanjuju te nesporazume; svi znaju kako postupiti i kako tumačiti postupke drugih. Slično je i s računalima koja komuniciraju, potrebno je definirati skup pravila kojima će se upravljati njihovom komunikacijom.

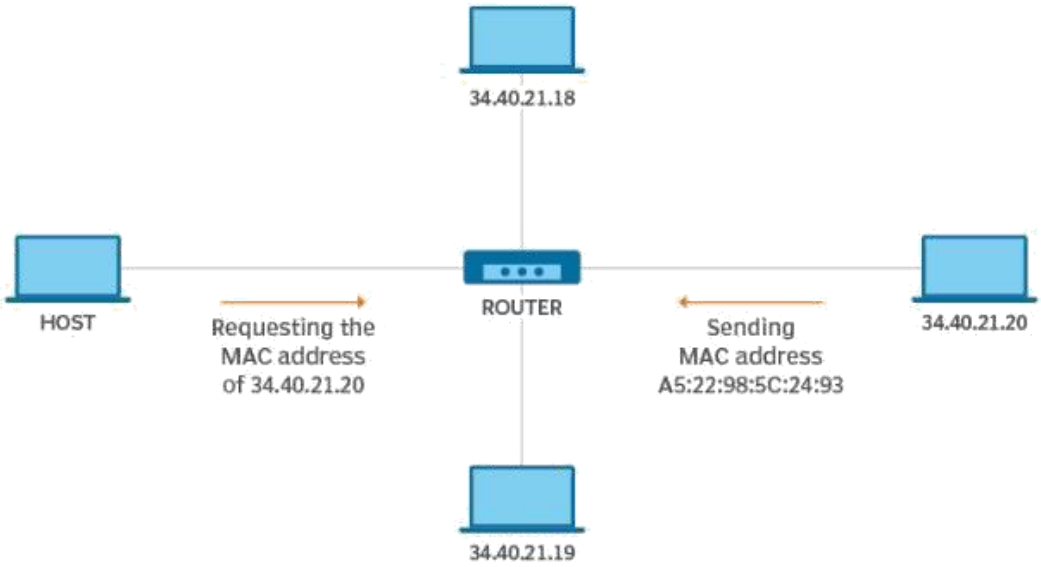
U podatkovnoj komunikaciji, ovi skupovi pravila nazivaju se protokoli. U homogenim mrežama, jedan dobavljač računala određuje skup komunikacijskih pravila dizajnirano za korištenje prednosti operacijskog sustava i hardverske arhitekture dobavljača. Ali homogene mreže su poput kulture jedne zemlje - samo domaći se osjećaju kao kod kuće. TCP / IP stvara heterogenu mrežu s otvorenim protokolima koji su neovisni o operacijskom sustavu i arhitektonskim razlikama. TCP / IP protokoli dostupni su svima i razvijaju se i mijenjaju konsenzusom, a ne zahtjevom jednog proizvođača. Svatko je slobodan razvijati proizvode koji zadovoljavaju ovim specifikacijama otvorenog protokola.

3.1. Protokol razlučivosti adrese (ARP)

Protokol razlučivosti adrese (*Address Resolution Protocol*) je postupak za mapiranje dinamičke adrese internetskog protokola (IP adrese) na stalnu adresu fizičkog uređaja u lokalnoj mreži (LAN). Fizička adresa uređaja naziva se još i *Media Access Control* ili MAC adresa.

Zadatak ARP-a je prevesti 32-bitne adrese u 48-bitne adrese i obrnuto. To je potrebno jer u IP verziji 4 (IPv4), najčešćoj verziji internetskog protokola (IP) koja se danas koristi, IP adresa je duga 32-bita, a MAC adrese su 48-bitne.

ARP funkcionira između mrežnih slojeva 2 i 3 kod *Open Systems Interconnection* modela (OSI model). MAC adresa postoji na 2. stupnju OSI modela, sloju podatkovne veze, dok IP adresa postoji na 3. stupnju, mrežnom sloju. ARP se također može koristiti za IP preko drugih LAN tehnologija, poput tokenskog prstena, sučelja distribuiranih vlakana (FDDI) i IP preko ATM-a. U IPv6, koji koristi 128-bitne adrese, ARP je zamijenjen sa *Neighbor Discovery* protokolom.



Slika 7: Prikaz rada ARP-a, [5]

Kad se novo računalo pridruži LAN-u, dodijeljena mu je jedinstvena IP adresa koja će se koristiti za identifikaciju i komunikaciju. Kada dolazni paket namijenjen *host* računalu na određenom LAN-u stigne na pristupnik (*gateway*), pristupnik traži da ARP program pronađe MAC adresu koja odgovara IP adresi. Tablica koja se zove ARP *cache* održava zapis svake IP adrese i odgovarajuće MAC adrese (slika 7).

Svi operativni sustavi u IPv4 Ethernet mreži održavaju ARP predmemoriju. Svaki put kada domaćin zatraži MAC adresu kako bi poslao paket drugom *hostu* u LAN-u, provjerava ARP *cache* da vidi postoji li prijevod sa IP adrese na MAC adresu. Ako se to dogodi, novi ARP zahtjev nije potreban. Ako prijevod već ne postoji, šalje se zahtjev za mrežne adrese i vrši se ARP.

ARP emitira paket zahtjeva na sve uređaje na LAN-u i pita je li bilo koji od uređaja poznat da upotrebljava tu određenu IP adresu. Kad uređaj prepozna IP adresu kao svoju, šalje odgovor kako ARP može ažurirati predmemoriju za buduću referencu i nastaviti s komunikacijom. Uređaji domaćini koji ne znaju vlastitu IP adresu mogu za otkrivanje koristiti protokol obrnutog ARP (*Reverse Address Resolution Protocol* - RARP).

ARP veličina predmemorije je ograničena i periodično se čisti od svih unosa kako bi se oslobodio prostor, adrese obično ostaju u predmemoriji samo nekoliko minuta. Česta ažuriranja omogućuju drugim uređajima u mreži da vide kada fizički domaćin promijeni traženu IP adresu.

U procesu čišćenja brišu se neiskorišteni unosi, kao i svi neuspjeli pokušaji komunikacije s računalima koja trenutno nisu uključena, [5].

RARP je mrežni protokol pomoću kojega se iz poznate fizičke MAC adrese može saznati IP adresa (slika 8). RARP protokol se primjenjuje kod sustava bez diska koji prilikom pokretanja ne znaju vlastitu IP adresu pa je dobivaju pomoću RARP upita. Format RARP poruka je sličan ARP formatu. Kada računalo šalje ARP zahtjev, on automatski stavlja svoju hardversku adresu u polje za slanje, te u polje za primanje u enkapsulirani ARP paket podataka. RARP poslužitelj će u svom odgovoru na poruku popuniti ispravno slanje i primanje IP adrese. Na taj način će računalo znati svoju IP adresu kada dobije poruku od RARP poslužitelja, [6].

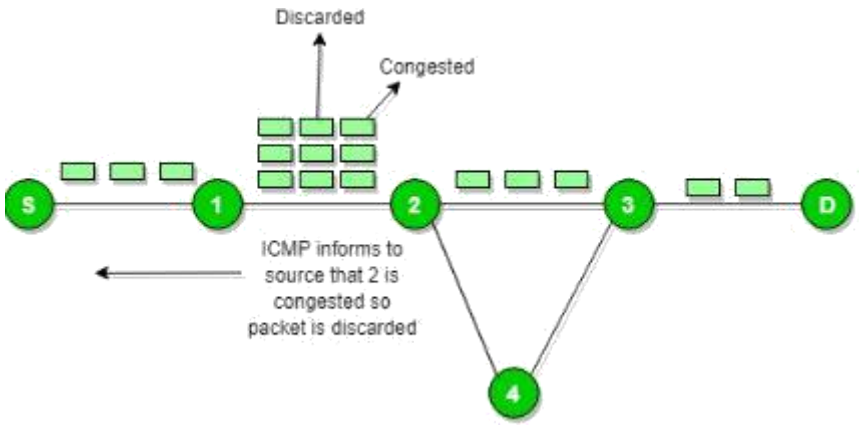
Slika 8: Prikaz rada RARP-a, [6]

3.2. *Internet Control Message Protocol* (ICMP)

Budući da IP nema ugrađeni mehanizam za slanje poruka o pogrešci i kontroli ovisi o ICMP-u koji će pružiti kontrolu pogrešaka. Koristi se za izvještavanje o pogreškama i upite upravljanja. To je potporni protokol i koriste ga mrežni uređaji poput usmjerivača za slanje poruka o pogrešci i operativnih podataka. Npr. zatražena usluga nije dostupna ili nije moguće doći do domaćina ili usmjerivača, [7].

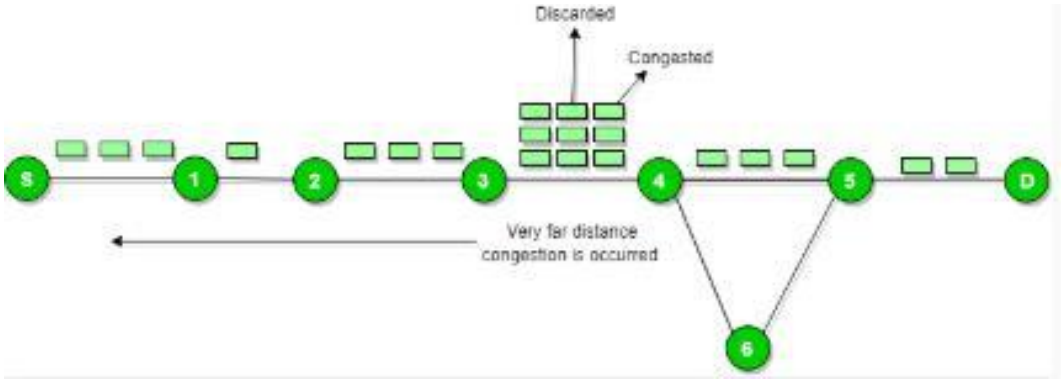
3.2.1. *Source quench message*

Source quench message je zahtjev za smanjenjem brzine slanja za poruke koje se šalju domaćinu (odredištu). Ili može se reći da ako prilikom primanja domaćin otkrije da je brzina slanja paketa prevelika, on šalje *source quench message* izvoru da bi usporio tempo kako ne bi izgubio niti jedan paket (slika 9).



Slika 9: Zahtjev za smanjenjem brzine, [7]

ICMP će preuzeti odbijeni IP izvor iz odbačenog paketa i obavijestit će ga putem slanja poruke usporavanje izvora. Tada će izvor smanjiti brzinu prijenosa tako da usmjerivač bude slobodan zbog zagušenja (slika 10).



Slika 10: Zahtjev za smanjenje brzine kada je zagušeni usmjerivač daleko od izvora, [7]

Kad je zagušeni usmjerivač daleko od izvora, ICMP će poslati skok po skok poruku o usporavanju izvora tako da svaki usmjerivač smanjuje brzinu prijenosa, [7].

3.2.2 Problem parametara

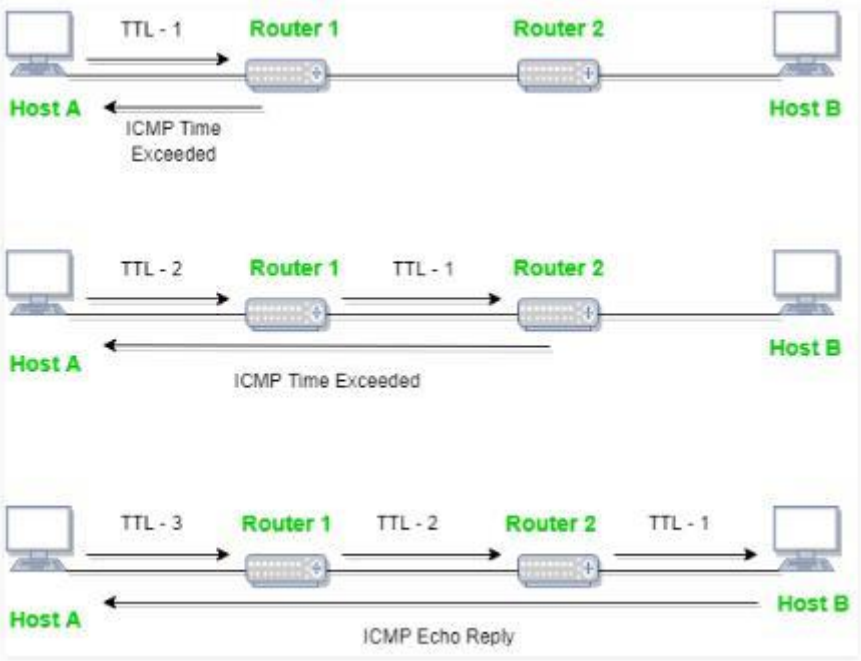
Kad god paketi dođu na usmjerivač, tada izračunata kontrolna suma zaglavlja treba biti jednaka primljenoj kontrolnoj sumi zaglavlja, tada usmjerivač prihvaća samo paket.

Ako postoji neusklađenost, usmjerivač će izbaciti paket. ICMP će preuzeti odlazni IP iz odbačenog paketa i obavijestit će ga putem slanja poruke problema s parametrima, [7].

3.2.3 *Time exceeded message*

Na slici 11 kad se neki fragmenti izgube u mreži, tada će fragmenti za zadržavanje od usmjerivača biti ispušteni, a ICMP će odbaciti IP izvor iz odbačenog paketa i obavijestiti ga o

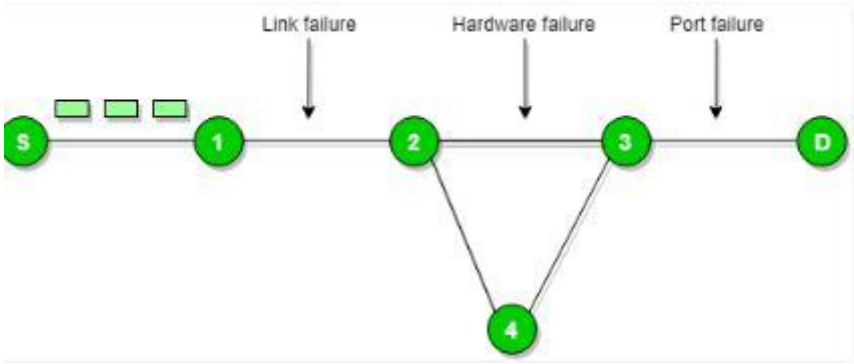
izvoru odbačenog datagrama zbog vremena koje je dosegnulo nulu, slanjem vrijeme je prekoračeno porukom, [7].



Slika 11: Slanje vrijeme je prekoračeno poruke, [7]

3.2.4 *Destination un-reachable*

Na slici 12 poruku *odredište je nedostupno* generira domaćin ili njegov ulazni pristupnik kako bi obavijestio klijenta da je odredište iz nekog razloga nedostupno.



Slika 12: Slanje odredište je nedostupno poruke, [7]

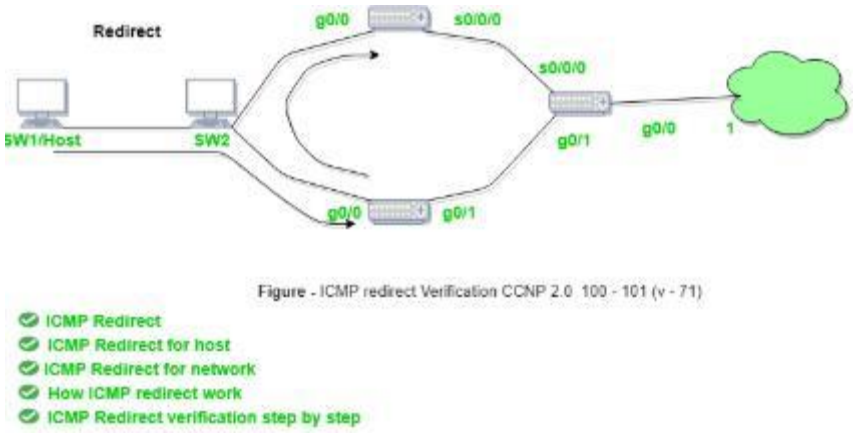
Ne postoji nužni uvjet da samo usmjerivač daje ICMP poruku o pogrešci, ponekad odredišni domaćin šalje ICMP poruku pogreške kada se u mreži dogodi bilo koji tip kvara (neuspjeh veze, hardverski neuspjeh, otkaz porta itd.), [7].

3.2.5 Poruka o preusmjeravanju

Preusmjeravanje zahtjeva je zahtjev da se paketi šalju na alternativni put. Poruka informira domaćina da ažurira svoje podatke o usmjeravanju (kako bi mogao slati pakete na alternativnoj ruti).

Na slici 13 ako domaćin pokušava poslati podatke putem prvog usmjerivača , a prvi usmjerivač šalje podatke na drugi usmjerivač i postoji izravni put od domaćina do drugog usmjerivača. Tada će prvi usmjerivač poslati preusmjeravajuću poruku da obavijesti domaćina da postoji bolji način do odredišta izravno putem preko drugog usmjerivača koji je dostupan. Tada domaćin šalje pakete podataka na odredište izravno preko drugog usmjerivača. Drugi usmjerivač će poslati originalni datagram na predviđeno odredište. Ali ako datagram sadrži informacije o usmjeravanju, ova se poruka neće slati čak i ako je dostupna bolja ruta, jer preusmjeravanja trebaju slati samo pristupnici, a ne trebaju ih slati i internetski domaćini.

Kad god se paket prosljeđuje u pogrešnom smjeru, kasnije se preusmjerava u trenutni smjer, tada ICMP će poslati poruku o preusmjeravanju, [7].



Slika 13: Primjer slanja poruke o preusmjeravanju, [7]

3.3 *Internet Group Management Protocol* (IGMP)

IGMP je komunikacijski protokol kojeg koriste domaćini i susjedni usmjerivači za *multicasting* komunikaciju s IP mrežama i učinkovito koriste resurse za prijenos poruka ili paketa podataka. Komunikacija putem *multicast*-a može imati jednog ili više pošiljatelja i primatelja, pa se IGMP može koristiti za *streaming* video zapisa, u igrama ili u alatima za *web* konferencije. Ovaj protokol se koristi u IPv4 mrežama, a za njegovo korištenje na IPv6 *multicast*-om upravlja *Multicast Listener Discovery* (MLD). Kao i drugi mrežni protokoli, IGMP se koristi na

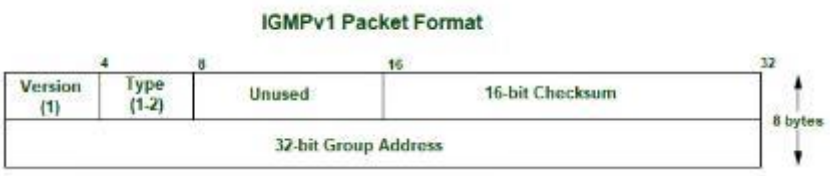
mrežnom sloju. MLDv1 je gotovo isti u funkcioniranju kao IGMPv2, a MLDv2 je gotovo sličan IGMPv3.

IGMP radi na uređajima koji su sposobni za rukovanje *multicast* skupina i dinamičnim *multicasting*-om. Ovi uređaji omogućavaju domaćinu da se pridruži ili napusti članstvo u grupi za višestruko slanje. Ovi uređaji također omogućuju dodavanje i uklanjanje klijenata iz grupe. Ovim se komunikacijskim protokolom upravlja između domaćina i lokalnog *multicast* usmjerivača. Kada se stvori grupa za višestruko slanje, adresa grupe za višestruko slanje nalazi se u rasponu IP adresa klase D (224-239) i prosljeđuje se kao odredišna IP adresa u paketu.

Uređaji L2 ili Level-2, kao što su prekidači, koriste se između domaćina i *multicast* usmjerivača za presnimavanje IGMP-a. Slušanje IGMP-a postupak je za kontrolirano slušanje mrežnog prometa IGMP-a na kontrolirani način. *Switch* prima poruku domaćina i prosljeđuje izvještaj o članstvu lokalnom *multicast* usmjerivaču. Promet *multicasta* dalje se preusmjerava na udaljene usmjerivače s lokalnih *multicast* usmjerivača pomoću PIM-a (*Protocol Independent Multicast*) kako bi klijenti mogli primiti pakete poruka ili podataka. Klijenti koji se žele pridružiti mreži šalju pridružujuću poruku u upitu i preklopnici primaju poruku i dodaju portove klijenata svojoj tablici usmjeravanja *multicast*. IGMP komunikacijski protokol učinkovito prenosi podatke *multicast*-a na prijemnike i na taj način se ne slažu neželjeni paketi na domaćina, što pokazuje optimizirane performanse, kad su sve zajedničke veze povezane širina pojasa se troši u potpunosti i domaćini mogu napustiti grupu za višestruko slanje i pridružiti se drugoj. Međutim, ne pruža dobru učinkovitost filtriranja i sigurnosti, a zbog nedostatka TCP-a može doći do zagušenja mreže. Osim toga, IGMP je ranjiv na neke napade kao što je DOS (*Denial-Of-Service*) napad, [8].

3.3.1. IGMPv1

Ova verzija IGMP komunikacijskog protokola omogućava svim domaćinima koji se podržavaju da se pridruže grupama za višestruko slanje putem zahtjeva za članstvo. No, domaćin ne može napustiti grupu samostalno i mora čekati određeni vremenski period da bi napustio grupu.

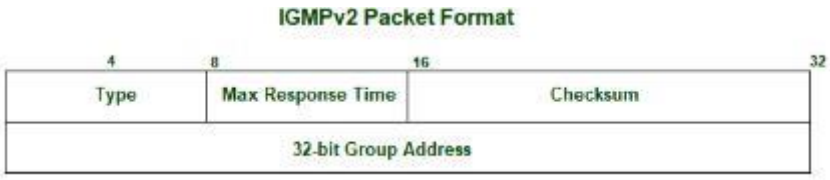


Slika 14: IGMPv1 format zaglavlja, [8]

Na slici 14 u gornjem lijevom kutu je polje *Version* postavljeno na 1, desno od toga se nalazi polje *Type* gdje je 1 za upit o članstvu domaćina a 2 je izvješće o članstvu domaćina. Potom slijedi polje *Unusued* gdje se nalaze 8-bitova nule koje se ne koriste. Na gornjoj desnoj strani je polje *Checksum* koji je jedna dopuna od jedne dopune od sume IGMP poruke. Polje adrese grupe je nula u trenutku kada je poslano, i ignorirano je kad je primljeno u poruci upita o članstvu. U poruci izvještaja o članstvu, polje adresa skupine preuzima IP adresu adrese domaćina o kojoj se izvješćuje, [8].

3.3.2. IGMPv2

IGMPv2 je preglednija verzija komunikacijskog protokola IGMPv1. Dodana je funkcionalnost napuštanja grupe za višestruko slanje korištenjem članstva u grupi.



Slika 15: IGMPv2 format zaglavlja, [8]

Na slici 15 primjećuje se da jedina razlika između formata IGMPv1 i IGMPv2 je ta da u IGMPv2 postoji *Max Response Time* i da IGMPv2 nema polje *Version* i polje *Type. Max response time* se zanemaruje za vrste poruka koje nisu upiti za članstvo. Za vrstu upita za članstvo maksimalno je dopušteno vrijeme prije slanja izvještaja o odgovoru. Vrijednost je u jedinicama od 0,1 sekunde, [8].

3.3.3. IGMPv3

U IGMPv3 verziji dodani su specifični izvori *multicasta* i skupljanje izvještaja o članstvu.

Na slici 16 prikazan je IGMPv3 paket format. Novo polje *Resv* postavljeno je na nulu kada je poslano i ignorirano je kada se primi. Polje *S flag* predstavlja zastavicu za suzbijanje procesora na strani usmjerivača. Kad je zastava postavljena, označava da se suzbijaju ažuriranja tajmera koji multimedijski usmjerivači izvršavaju nakon primanja upita. Polje QRV predstavlja Querier-ovu varijablu robusnosti. Usmjerivači nastavljaju dohvaćati QRV vrijednost iz posljednjeg primljenog upita kao vlastite vrijednosti dok najnoviji primljeni QRV nije jednak nuli. Polje QQIC predstavlja Querier-ov interval koda upita. Polje *Number of sources* predstavlja broj adresa izvora prisutnih u upitu. Za opći upit ili upit specifičan za grupu, ovo

polje je nula, a za upit specifičan za grupu i izvora, ovo polje nije nula. Polje *Source Address* predstavlja IP jednoznačnu adresu za N polja, [8].

IGMPv3 Packet Format

Bit Offset	0-3	4	5-7	8-15	16-31
0	Type = 0x11			Max Response Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address[1]				
128	Source Address[2]				
	Source Address[N]				

Slika 16: IGMPv3 format zaglavlja, [8]

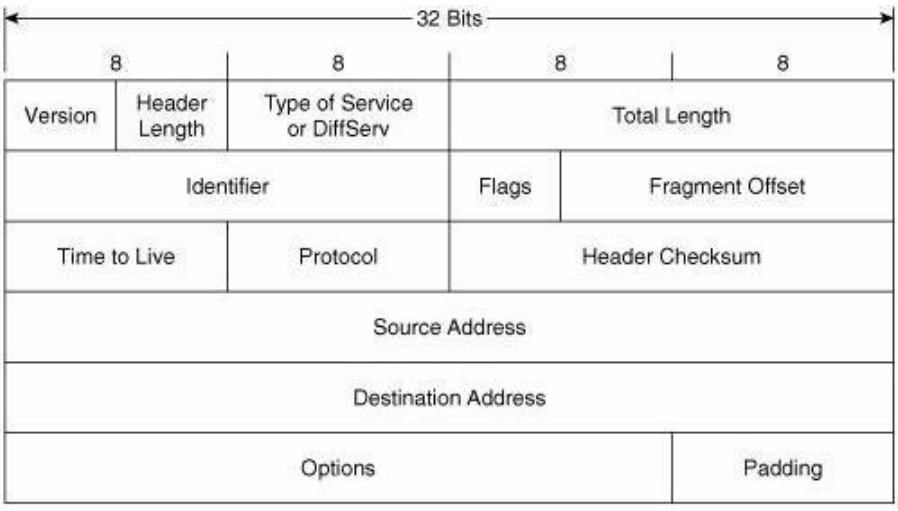
4. Osnovne značajke IP protokola

IP protokol je standardni internetski protokol, čije su osnovne funkcije adresiranje i usmjeravanje, tj. prijenos datagrama kroz mrežu. IP je jednostavni mrežni protokol koji se prilagođava različitim izvedbama prijenosne mreže. IP osigurava prijenos jedinica podataka, datagrama između računala i usmjeritelja, kao i između usmjeritelja. Izvor i odredište su označeni adresom fiksne duljine od 32 bita. Ako je veličina podataka koji dolaze iz transportnog sloja veća od maksimalne veličine, IP provodi fragmentiranje i ponovno sklapanje podataka. IP ne sadrži funkcije za kontrolu toka, održavanje slijeda informacijskih jedinica i ponovni prijenos, koje bi povećale pouzdanost prijenosa, već su one prepuštene višim slojevima. IP se isključivo brine o isporuci datagrama, to jest da svaki datagram stigne na odredište, [9].

4.1. IPv4

IP protokol verzija 4 najraširenija je IP protokol na najvećoj računalnoj mreži danas - Internetu. Pojedine verzije IP protokola razlikuju se po načinu adresiranja, izgledu zaglavlja paketa, ali i brojnim drugim detaljima. Osnovne karakteristike IPv4 protokola su:

- Ne uspostavlja se veza između ishodišta i odredišta prije slanja paketa (*Connectionless*).
- Najbrža moguća usluga (*Best effort*) – nema dodatnih kontrolnih paketa koji bi garantirali isporuku paketa. To mu omogućava najbrži mogući način prijenosa paketa od ishodišta do odredišta. Cijena brzine je nepouzdanost.
- Nezavisan od vrste medija za prijenos podataka (*Media independent*).



Slika 17: IPv4 zaglavlje, [10]

Na slici 17 na lijevom gornjem kutu IPv4 zaglavlja nalazi se polje *Version* koje označava verziju protokola i kod IPv4 zauzima četiri bita. Potom slijedi *Internet Header Length* (IHL) koji služi za specificiranje ukupne duljine zaglavlja i izražena je kao broj 32 bitnih riječi. Najmanja vrijednost koju ovo polje može imati je 5, što znači da je minimalna vrijednost IP zaglavlja 5 x 32 bita = 160 bitova = 20 bajta. Maksimalna vrijednost za 4 bitnu kombinaciju je 15 riječi, kada je 15 x 32 = 480 bitova što iznosi 60 bajta.

Type of Service (TOS) omogućuje određeno upravljanje prijenosom paketa. Služi za označavanje paketa u slučaju upotrebe QoS (*Quality of Service*) sustava. To je polje duljine 8 bita. Polje je osmišljeno za određivanje kvalitete usluge (QoS). Novije implementacije IPv4 protokola ovo polje mijenjaju sa 6 bitnim DSCP (*Differentiated Service Code Point*) i 2 bitnim ECN (*Explicit Congestion Notification*) poljem. DSCP polje određuje vrijednost QoS-a za svaki paket. ENC polje služi za dobivanje informacija o zagušenjima kroz mrežu.

Total Length služi za određivanje ukupne duljine IP paketa uključujući i podatke. Ova vrijednost uključuje veličinu podatkovnog dijela, veličinu TCP/UDP zaglavlja i veličinu IP zaglavlja. Ovo polje prezentira se oktetima i u zaglavlju zauzima 16 bita.

Identifier je jedinstvena identifikacija fragmenata jednog paketa. Upotrebljava se kako se fragmenti različitih paketa ne bi pomiješali (kad se paket pri prolazu kroz mrežu dijeli ili fragmentira na više dijelova). Zauzima 16 bita, a određeno je od strane pošiljatelja. Služi identifikaciji pojedinačnih paketa, koji su rastavljeni na fragmente od strane usmjerivača.

Flags služi za određivanje postupanja uređaja prema određenom IP paketu. Polje se sastoji od tri bita – zastavice. Prvi bit uvijek ima vrijednost 0, drugi bit služi za određivanje fragmentacije (0 –paket se smije fragmentirati, 1 –paket se ne smije fragmentirati), dok treći bit prezentira lokaciju paketa u nizu fragmentiranih paketa (0 –paket se nalazi kao zadnji fragment u nizu ili paket nije fragmentiran uopće, 1 –paket nije zadnji u nizu fragmentiranih paketa i treba se očekivati dolazak više fragmentiranih paketa). Prva je zastavica neiskorišteni bit u IP zaglavlju (*Reserved*), druga upravlja fragmentacijom (DF, *Don't Fragment*), a treća označava posljednji fragment u izvornom paketu (MF, *More Fragments*).

Fragment Offsett koristi 13 bita i upotrebljava se za određivanje pozicije fragmenta u paketu. Paketi koji nisu fragmentirani i prvi paketi u nizu fragmentiranih paketa uvijek imaju vrijednost ovog polja postavljenu u 0.

Time to Live je vrijednost u rasponu od 0 do 255 i označava starost paketa. Svaki put kada paket dođe na usmjerivač, ova se vrijednost umanjuje za jedan. Kada padne na nulu, paket se briše, odnosno uklanja s mreže. Upotrebljava se za sprečavanje nastanka petlji na mrežnom sloju.

Protocol ovo polje sadrži identifikator protokola (ICMP, TCP, UDP) kome treba isporučiti podatke dospjelog datagrama, što se naziva demultipleksiranje.

Header Checksum zauzima 16 bita. Služi kao metoda za provjeravanje i potvrđivanje da nije došlo do promjene niti jednog polja zaglavlja IP paketa. Upotrebljava se za provjeru ispravnosti paketa.

Source IP Address i *Destination IP Address* određeni su s 32 bita, označavaju IP adresu izvorišnog računala s kojeg je paket poslan i odredišnog uređaja, računala na koju je paket poslan.

Options ima varijabilnu vrijednost duljine i u njemu se određuju dodatne opcije za slanje. Većina IP paketa, koji se šalju u suvremenim mrežama, nemaju ovo polje, zato što se ovo polje najčešće ne koristi. To su polje dodatne IP opcije. Ispuna se upotrebljava kako bi zaglavlje bilo djeljivo s 32, [10].

4.2. IPv6

IPv6 je poboljšanje IP protokola. Izvorna motivacija za novi protokol bila je prijetnja potrošnje adrese. IPv6 ima 128-bitnu adresu, tako da potrošnja adresa nije problem. Velika adresa također omogućuje korištenje hijerarhijske strukture adresa za smanjenje opterećenja usmjerivača, a pritom još uvijek zadržavaju više nego dovoljno adresa za budućnost rasta mreže. Ali velike adrese samo su jedna od prednosti novog protokola. Ostale prednosti IPv6 su:

- Poboljšana sigurnost ugrađena u protokol.
- Poboljšane tehnike rukovanja opcijama zaglavlja.

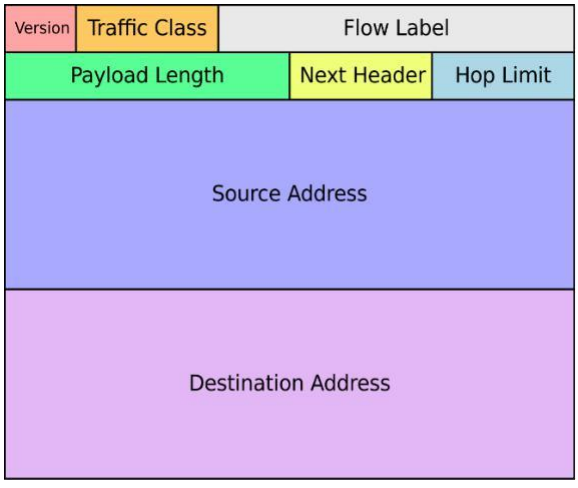
IPv6 ima nekoliko dobrih osobina, ali još uvijek se ne koristi često. Djelomično je to zbog toga što i dalje dolaze poboljšanja za IPv4, zbog poboljšanja performansi hardvera i promjene načina na koje su mreže konfigurirane smanjila je potražnju za novim značajkama IPv6.

Kritični nedostatak adresa nije se ostvario iz tri razloga:

- CIDR (*Classless Inter-Domain Routing*) dodjeljivanje adresa postaje fleksibilnije, što zauzvrat čini više adresa dostupno i dopušta združivanje radi smanjenja opterećenja usmjerivača
- Privatne adrese i NAT (*Network address translation*) znatno su smanjili potražnju službenih adresa. Mnoge organizacije radije koriste privatne adrese za sve sustave na njihovim internim mrežama jer privatne adrese smanjuju administrativni teret i poboljšavaju sigurnost.
- Stalno, fiksno dodjeljivanje adrese rjeđe je od dinamičke adrese. Većina sustava privremeno koristi dinamičke adrese dodijeljene konfiguracijskim protokolom DHCP (*Dynamic Host Configuration Protocol*).

Stvaranje IPsec standarda za IPv4 umanjilo je potrebu za sigurnosnim poboljšanjima IPv6. U stvari, mnogi sigurnosni alati i značajke dostupne za IPv4 sustav se ne koriste u potpunosti, što ukazuje da potražnja za alatima koji osiguravaju vezu može biti precijenjena.

IPv6 eliminira skok po skok segmentaciju, ima učinkovitiji dizajn zaglavlja i ima poboljšanu obradu opcija. Ove stvari čine ga učinkovitijim za obradu IPv6 paketa nego za rukovanje IPv4 paketima. Međutim, za veliku većinu sustava, ova povećana učinkovitost nije potrebna jer je obrada IP datagrama vrlo mali zadatak. Većina sustava nalazi se na rubu mreže i upravlja sa relativno malim brojem komunikacijskih paketa. Brzina procesora i memorija porasle su dok su cijene hardvera pale. Većina ljudi bi prije kupili više hardvera koristeći provjereni IPv4 protokol, nego riskirali implementiranje novog IPv6 protokola samo da bi produžili vijek uređaja. Samo oni sustavi koji se nalaze u blizini jezgre mreže bi zaista imali koristi od ove učinkovitosti, i iako su važni, ti su sustavi u relativnom malom broju, [1].



Slika 18: IPv6 zaglavlje, [18]

Na slici 18 vidljiva su polja IPv6 zaglavlja paketa s početkom na polju *Version* koje je polje dužine 4 bita, označava verziju. Polje je isto kao i kod verzije IPv4.

Traffic Class je polje slično polju " *Type of Service*" u IPv4. Omogućuje postavljanje željenog prioriteta pri uručivanju paketa. Dužina je 4 bita za postavljanje 16 različitih vrsta prometa. Neke od oznaka su već predefinirane, a neke ostavljene za buduće potrebe. Pravilo je da su brojevima od 0 do 7 označeni paketi kojima nije toliko bitno kašnjenje koliko pouzdana isporuka, dok su brojevima od 8 do 15 označeni paketi koji bi trebali stići u realnom vremenu. Ti paketi ne moraju putovati pretjerano pouzdano, ali ne smiju kasniti.

Flow Label je polje dužine 24 bita. S ishodišnom adresom čini jedinstveni broj koji označava pakete koji traže posebno rukovanje kod IPv6 usmjerivača. Uvedeno je radi određivanja slijeda paketa određene vrste usluge (VoIP).

Payload length je dužina korisnog sadržaja (u broju okteta). Polje slično polju „*total length*" u IPv4.

Next header polje označava koji tip zaglavlja slijedi odmah nakon osnovnog IPv6 zaglavlja (npr. TCP ili UDP zaglavlje na transportnom sloju ili zaglavlje proširenja (*extension header*). Zaglavlja proširenja može se dodati zbog autentifikacije, enkriptiranja podataka, ICMPv6 poruka i dr.

Hop limit je broj koji definira koliko usmjerivača paket može proći prije nego bude uništen. To je broj od 8 bitova koji se smanjuje za jedan kod svakog prolaska kroz usmjerivača. Paket se uništava ako vrijednost polja dođe na nulu. To je polje slično polju TTL u IPv4 verziji. U IPv6 izbačena je provjera ispravnosti podataka na mrežnom sloju kako bi se povećala učinkovitost prosljeđivanja paketa. Prema tome IPv6 nema polje sažetak zaglavlja (*checksum*). Ta je provjera izbačena jer se već ionako radi na podatkovnom i transportnom sloju.

Source address je adresa ishodišta paketa (128 bita). *Destination address* je adresa odredišta paketa (128 bita). *Extensions header* su opcionalna polja koja slijede osam obaveznih polja. Broj zaglavlja proširenja nije stalan pa ni ukupna dužina u oktetima nije definirana. To je jedna od znatnijih promjena. Kod protokola IPv4 polje opcije upotrebljava se za dodatne informacije o opcionalnim uslugama kao što je primjerice enkripcija sadržaja paketa. Zbog toga je dužina zaglavlja kod IPv4 promjenjiva i ovisi o broju korištenih opcija što usporava postupak obrade i prosljeđivanja paketa, [11].

5. Adresni prostor

Virtualni adresni prostor (*Virtual address space* - VAS) ili adresni prostor je skup raspona virtualnih adresa koje operativni sustav stavlja na raspolaganje procesu. Raspon virtualnih adresa obično započinje s niskom adresom i može se proširiti na najvišu adresu koju dopušta arhitektura računala i podržana je implementacijom veličine pokazivača operativnog sustava, a koja može biti 4 bajta za 32-bitnu ili 8 bajtova za 64- bitne verzije OS-a. To pruža nekoliko prednosti, od kojih je jedna sigurnost izoliranjem procesa pod pretpostavkom da se svakom procesu dobije zaseban adresni prostor.

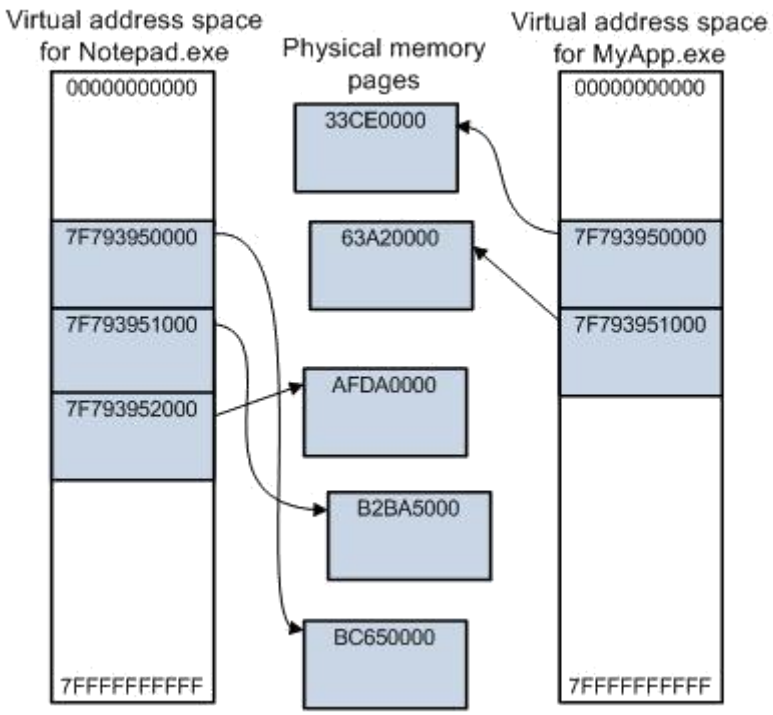
Kad procesor čita ili piše u memorijsku lokaciju, on koristi virtualnu adresu. Kao dio operacije čitanja ili pisanja, procesor virtualnu adresu prevodi u fizičku adresu. Pristup memoriji putem virtualne adrese ima ove prednosti:

Program može koristiti neprekidni niz virtualnih adresa za pristup velikom memorijskom međuspremniku koji nije u fizičkoj memoriji.

Program može koristiti niz virtualnih adresa za pristup memorijskom međuspremniku koji je veći od raspoložive fizičke memorije. Kako opskrba fizičke memorije postaje mala, upravitelj memorije sprema stranice fizičke memorije (obično veličine 4 kilobajta) u datoteku diska. Stranice podataka ili koda prema potrebi se premještaju između fizičke memorije i diska.

Virtualne adrese koje su korištene od različitih procesa su izolirane jedne od druge. Kod u jednom procesu ne može promijeniti fizičku memoriju koja koristi drugi proces ili operativni sustav.

Raspon virtualnih adresa dostupnih nekom procesu naziva se virtualni prostor adrese za postupak. Svaki postupak korisničkog načina ima svoj privatni virtualni prostor adrese. Za 32-bitni proces virtualni adresni prostor obično je raspon od 2 gigabajta od 0x00000000 do 0x7FFFFFFF. Za 64-bitni proces na 64-bitnom *Windows*-u virtualni je adresni prostor 128-terabajtski raspon 0x000'00000000 do 0x7FFF'FFFFFFFF. Paleta virtualnih adresa ponekad se naziva i raspon virtualne memorije.



Slika 19: Dijagram ključnih značajki virtualnih adresnih prostora, [12]

Slika 19 prikazuje virtualne adresne prostore za dva 64-bitna procesa: *Notepad.exe* i *MyApp.exe*. Svaki proces ima vlastiti virtualni adresni prostor koji ide od 0x000'0000000 do 0x7FF'FFFFFFFF. Svaki zasjenjeni blok predstavlja jednu stranicu (veličine 4 kilobajta) virtualne ili fizičke memorije. Proces *Notepad* koristi tri susjedne stranice virtualnih adresa, počevši od 0x7F7'93950000. Ali te tri susjedne stranice virtualne adrese preslikane su na nekonzistentne stranice u fizičkoj memoriji. Oba procesa koriste stranicu virtualne memorije koja započinje na 0x7F7'93950000, ali su te virtualne stranice mapirane na različite stranice fizičke memorije, [12].

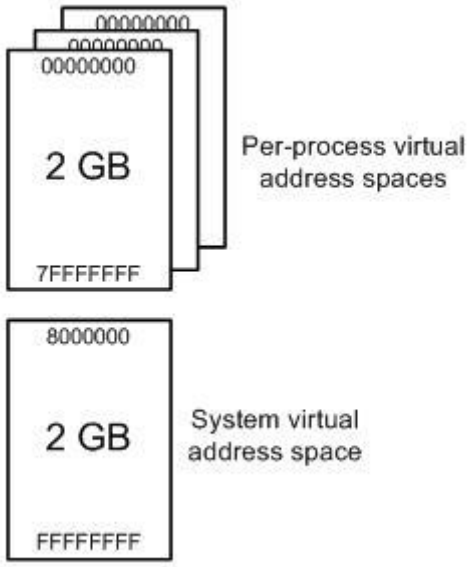
5.1. Korisnički prostor i prostor sustava

Procesi poput *Notepad.exe* i *MyApp.exe* pokreću se u korisničkom načinu. Glavne komponente operacijskog sustava i mnogi upravljački programi rade u povlaštenijem jezgrenom načinu.

Svaki postupak u korisničkom načinu rada ima svoj privatni virtualni adresni prostor, ali sav kod koji se izvodi u jezgrenom načinu dijeli jedan virtualni prostor adrese nazvan sistemski prostor. Virtualni prostor adrese za postupak korisničkog načina naziva se korisnički prostor.

U 32-bitnom sustavu ukupni raspoloživi prostor *Windows* virtualne adrese je 2^{32} bajta (4 24

gigabajta). Donja 2 gigabajta koriste se za korisnički prostor, a gornja 2 gigabajta za prostor sustava (slika 20).



Slika 20: Adresni prostor Windows-a, [12]

U 32-bitnom *Windows*-u postoji mogućnost navesti (prilikom podizanja sustava) da je više od 2 gigabajta dostupno za korisnički prostor. Posljedica toga je da je za sistemski prostor dostupno manje virtualnih adresa. Možete povećati veličinu korisničkog prostora na čak 3 gigabajta, u tom slučaju je za sustav dostupan samo 1 gigabajt. Za povećanje veličine korisničkog prostora koristi se BCDEdit / set *increaseuserva*.

U 64-bitnom *Windows* sustavu teorijska količina prostora za virtualnu adresu je 2^{64} bajta (16 exabajta), ali zapravo se koristi samo mali dio raspona od 16 exabajta. Kod koji radi u korisničkom načinu ima pristup korisničkom prostoru, ali nema pristup sistemskom prostoru. Ovo ograničenje sprječava da kod korisničkog načina očitava ili mijenja zaštićene strukture podataka operativnog sustava. Kod koji se izvodi u jezgrenom načinu ima pristup i korisničkom i sistemskom prostoru. Odnosno, kod koji radi u jezgrenom načinu rada ima pristup prostoru sustava i virtualnom adresnom prostoru trenutnog postupka korisničkog načina.

Driveri koji rade u jezgrenom načinu moraju biti vrlo pažljivi pri izravnom čitanju ili pisanju adresa u korisničkom prostoru. Ovaj scenarij ilustrira zašto.

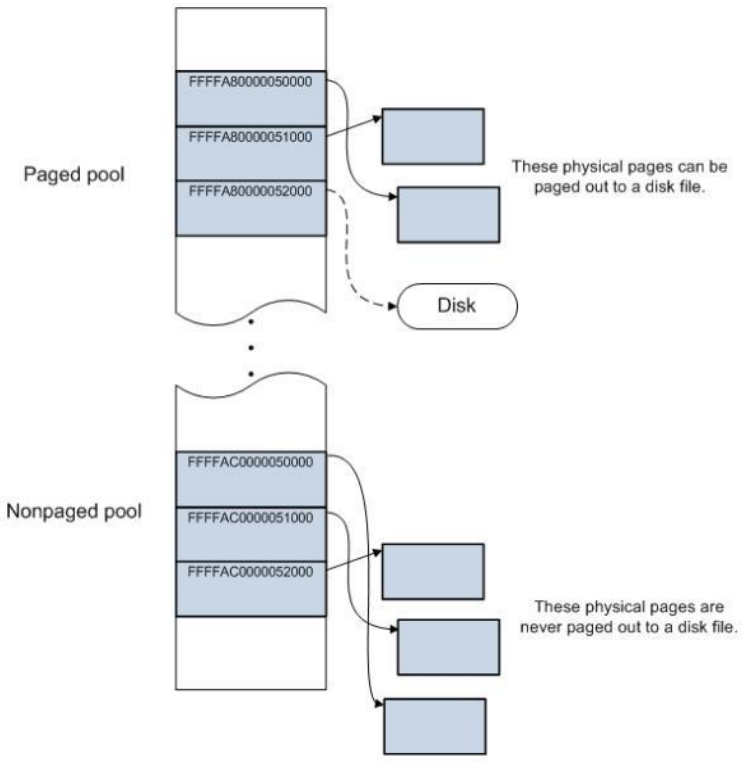
1. Program u korisničkom načinu pokreće zahtjev za čitanje nekih podataka s uređaja. Program isporučuje početnu adresu međuspremnika za primanje podataka.

2. *Routine driver* na uređaju, koji radi u jezgrenom načinu rada, pokreće postupak čitanja i vraća kontrolu pozivaču.
3. Kasnije uređaj prekida sve što trenutno radi kako bi rekao da je operacija čitanja gotova. Prekidom upravljaju *routine driver*-i upravljačkog programa.
4. U ovom trenutku *driver* ne smije upisivati podatke na početnu adresu koju je program u korisničkom načinu pružio u koraku 1. Ova se adresa nalazi u virtualnom adresnom prostoru procesa koji je pokrenuo zahtjev, a koji najvjerojatnije nije isto što i trenutni proces, [12].

5.2. *Paged pool* i *nonpaged pool*

U korisničkom prostoru sve stranice s fizičkom memorijom mogu se prikazivati na datoteku diska prema potrebi. U sistemskom prostoru neke se fizičke stranice mogu prepisati u stranicu, a druge se ne mogu. Na slici 21 vidljiv je prostor sustava koji ima dvije regije za dinamičko raspoređivanje memorije: *paged pool* i *nonpaged pool*.

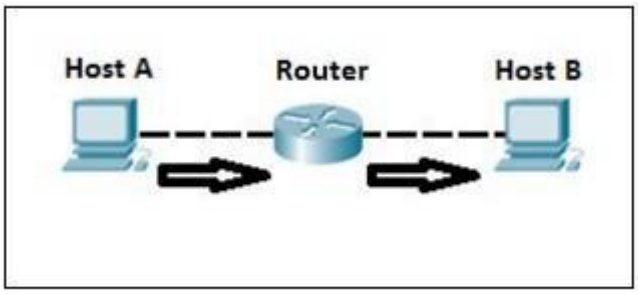
Memorija koja je dodijeljena u *paged pool*-u po potrebi se može prebaciti u datoteku diska. Memorija koja je dodijeljena u *nonpaged pool*-u nikada se ne može pozvati u datoteku diska, [12].



Slika 21: Paged pool i nonpaged pool, [12]

6. Usmjeravanje temeljeno na IP protokolu

IP usmjeravanje je postupak slanja paketa s glavnog računala na jednoj mreži do drugog računala koji je na drugoj udaljenoj mreži. Taj postupak obično rade usmjerivači. Usmjerivači pregledavaju odredišnu IP adresu paketa, određuju sljedeću adresu i prosljeđuju paket. Usmjerivači koriste tablice usmjeravanja kako bi odredili sljedeću hop adresu na koju se paket treba proslijediti.

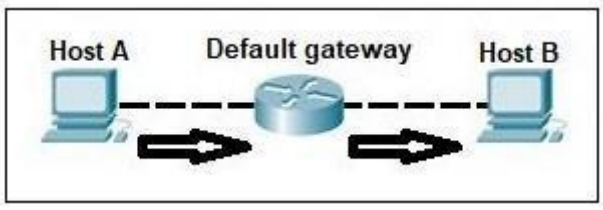


Slika 22: IP usmjeravanje, [13]

Na slici 22 domaćin A želi komunicirati s domaćinom B, ali domaćin B nalazi se na drugoj mreži. Domaćin A konfiguriran je za slanje svih paketa namijenjenim udaljenim mrežama prema usmjerivaču. Usmjerivač prima pakete, ispituje odredišnu IP adresu i prosljeđuje paket na odlazno sučelje povezano s odredišnom mrežom, [13].

6.1. Zadani pristupnik

Zadani pristupnik (*Default Gateway*) je usmjerivač koji domaćini koriste za komunikaciju s drugim domaćinima na udaljenim mrežama. Zadani pristupnik koristi se kada domaćin nema unos rute za određenu udaljenu mrežu i ne zna kako doći do te mreže. Domaćini se mogu konfigurirati za slanje svih paketa namijenjenih udaljenim mrežama na zadani pristupnik, koji ima put do te mreže.



Slika 23: Zadani pristupnik, [13]

Na slici 23 domaćin A ima IP adresu usmjerivača konfiguriranu kao adresu zadanog pristupnika. Domaćin A pokušava komunicirati s domaćinom B, domaćinom druge, udaljene mreže. Domaćin A pogleda u svoju tablicu usmjeravanja da provjeri postoji li unos za tu odredišnu mrežu. Ako unos nije pronađen, domaćin šalje sve podatke usmjerivaču. Usmjerivač prima pakete i prosljeđuje ih na domaćina B, [13].

6.2. Tablica usmjeravanja

Svaki usmjerivač održava tablicu usmjeravanja i pohranjuje ga u RAM-u. Tablicu usmjeravanja koriste usmjerivači za određivanje puta do odredišne mreže. Svaka tablica usmjeravanja sastoji se od sljedećih unosa:

- mrežna odredišna i podmrežna maska - određuje raspon IP adresa,
- daljinski usmjerivač - IP adresa usmjerivača koja se koristi da bi se došlo do te mreže,
- odlazno sučelje - odlaznim sučeljem paket bi trebao izaći van da bi stigao do odredišne mreže.

Postoje tri različite metode za popunjavanje tablice usmjeravanja:

1. izravno povezanim podmrežama,
2. pomoću statičkog usmjeravanja,
3. pomoću dinamičkog usmjeravanja.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/0
Router#
```

Slika 24: Prikaz tablice usmjeravanja usmjerivača, [13]

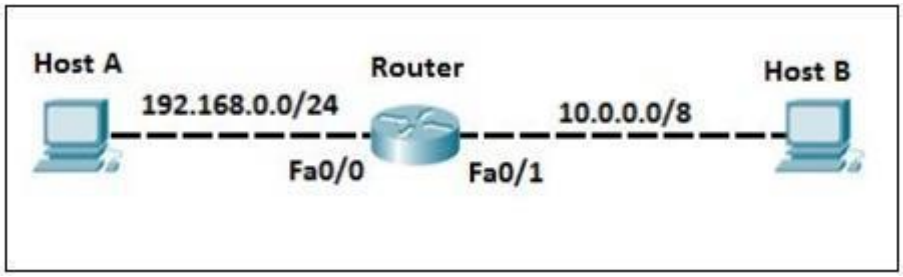
Pomoću naredbe *show ip route* iz omogućenog načina (*enabled mode*) može se dobiti prikaz tablice usmjeravanja usmjerivača. Kao što može vidjeti iz navedenog rezultata (slika 24), ovaj usmjerivač ima dvije izravno povezane rute do podmreža 10.0.0.0/8 i 192.168.0.0/24. Znak C

u tablici usmjeravanja označava da je ruta izravno povezana ruta. Dakle, kada domaćin A pošalje paket domaćinu B, usmjerivač će pogledati u svoju tablicu usmjeravanja i pronaći put do mreže 10.0.0.0/8 na kojoj domaćin B boravi. Usmjerivač će tada koristiti tu rutu za slanje paketa primljenih od domaćina A u domaćina B. [13]

6.2.1 Izravno povezane podmreže

Podmreže koje su izravno povezane s sučeljem usmjerivača dodaju se u tablicu usmjeravanja. Sučelje mora imati konfiguriranu IP adresu i oba koda statusa sučelja moraju biti u stanju *up and up*. Usmjerivač će moći usmjeriti sve pakete namijenjene svim domaćinima u podmrežama izravno povezanim sa njegovim aktivnim sučeljima.

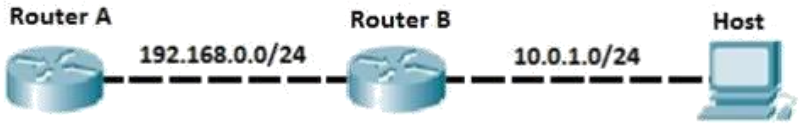
Na slici 25 usmjerivač ima dva aktivna sučelja, Fa0 / 0 i Fa0 / 1. Svako sučelje konfigurirano je s IP adresom i trenutno je u stanju gore, pa usmjerivač dodaje ove podmreže u svoju tablicu usmjeravanja. Kao što se vidi iz slike 25, usmjerivač ima dvije izravno povezane rute do podmreža 10.0.0.0/8 i 192.168.0.0/24. Znak C u tablici usmjeravanja označava da je ruta izravno povezana ruta, [14].



Slika 25: Izravno povezane podmreže, [14]

6.2.2. Statičko usmjeravanje

Dodavanjem statičkih ruta usmjerivač može naučiti rutu do udaljene mreže koja nije izravno povezana s jednim od njegovih sučelja. Statičke rute konfiguriraju se ručno upisivanjem naredbe za globalni način konfiguracije ip ruta DESTINATION_NETWORK SUBNET_MASK NEXT_HOP_IP_ADDRESS. Ova vrsta konfiguracije obično se koristi u manjim mrežama zbog razloga skalabilnosti (mora se konfigurirati svaka ruta na svakom usmjerivaču).



Slika 26: Statičko usmjeravanje, [14]

Na slici 26 usmjerivač A je izravno spojen na usmjerivač B. Usmjerivač B je izravno povezan s podmrežom 10.0.1.0/24. Budući da ta podmreža nije izravno povezana s usmjerivačem A, usmjerivač ne zna kako usmjeriti pakete namijenjene toj podmreži. Međutim. ta ruta može se konfigurirati na usmjerivaču A. Najprije je potrebno provjeriti tablicu usmjeravanja A prije nego što se doda statička ruta (slika 27).

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.0.0/24 is directly connected, FastEthernet0/0
```

Slika 27: Tablica usmjeravanja usmjerivača A, [14]

Sada je potrebno upotrijebiti naredbu statičke rute za konfiguriranje usmjerivača A da dođe do podmreže 10.0.0.0/24. Usmjerivač sada ima rutu da dođe do podmreže (slika 28).

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
S       10.0.0.0 [1/0] via 192.168.0.2
C    192.168.0.0/24 is directly connected, FastEthernet0/0
```

Slika 28: Prikaz naredbe statičke rute, [14]

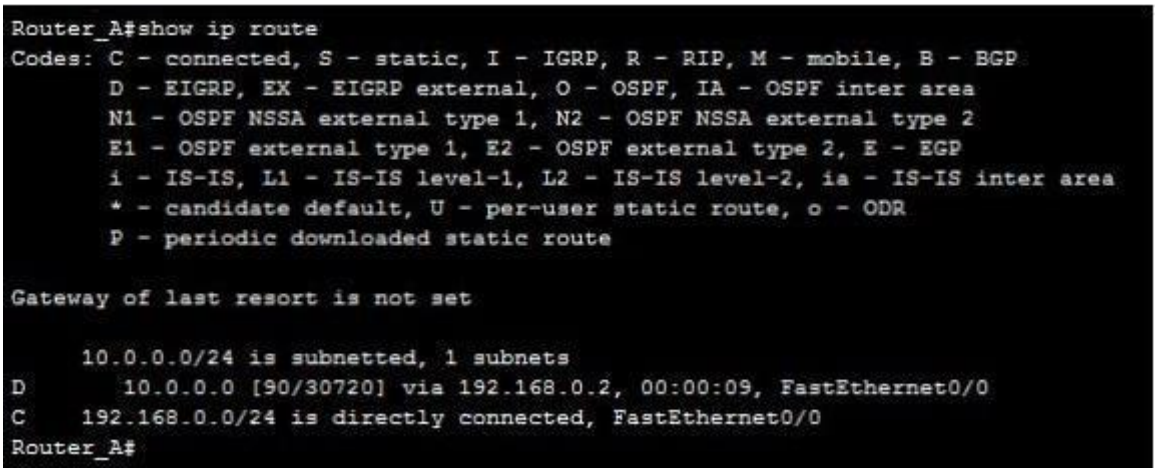
Znak S u tablici usmjeravanja (slika 28) označava da je ruta statički konfigurirana ruta. Postoji još jedna naredba ip route. Ne mora se navesti IP adresa sljedećeg skoka. Bolje je odrediti izlazno sučelje lokalnog usmjerivača. Na slici 28 može se upisati naredba *ip route* DEST_NETWORK NEXT_HOP_INTERFACE da usmjeri usmjerivač A da sav promet koji je namijenjen podmreži pošalje iz ispravnog sučelja. U tom slučaju naredba bi bila ip route 10.0.0.0 255.255.255.0 Fa0 / 0, [14].

6.2.3. Dinamičko usmjeravanje

Usmjerivač može naučiti dinamične rute ako je omogućen protokol usmjeravanja. Protokol usmjeravanja koriste usmjerivači za razmjenu podataka o usmjeravanju. Svaki usmjerivač u mreži tada može upotrijebiti informacije za izradu tablice usmjeravanja. Protokol usmjeravanja može dinamički odabrati drugi put ako veza padne, tako da je ova vrsta usmjeravanja otporna na pogreške. Također, za razliku od statičkog usmjeravanja, nema potrebe ručno konfigurirati svaku rutu na svakom usmjerivaču, što znatno smanjuje administrativne troškove. Treba samo definirati koje će se rute oglašavati na usmjerivaču koji se spajaju izravno na odgovarajuće podmreže - za ostalo se brinu protokoli usmjeravanja.

Nedostatak dinamičkog usmjeravanja je taj što povećava potrošnju memorije i CPU-a na usmjerivaču, jer svaki usmjerivač mora obraditi primljene informacije o usmjeravanju i izračunati tablicu usmjeravanja.

Primjer dinamičkog usmjeravanja nalazi se u nastavku. Oba usmjerivača imaju protokol usmjeravanja, EIGRP (*Enhanced Interior Gateway Routing Protocol*). Ne postoje statičke rute na usmjerivaču A, tako da R1 ne zna kako doći do podmreže 10.0.0.0/24 koja je izravno povezana s usmjerivačem B. Usmjerivač B zatim oglašava podmrežu na usmjerivač A pomoću EIGRP. Sada usmjerivač A ima rutu da dođe do podmreže. To se može provjeriti unosom naredbe show ip route što je prikazano na slici 29.



Slika 29: Prikaz naredbe dinamičke rute, [14]

Može se vidjeti da je usmjerivač A naučio podmrežu iz EIGRP-a. Slovo D ispred rute označava da je put naučen kroz EIGRP. Ako podmreža 10.0.0.0/24 ne uspije, usmjerivač B može odmah obavijestiti usmjerivač A da podmreža više nije dostupna, [14].

7. Zaključak

TCP / IP je otvoreni protokolarni složaj koji je zbog svoje široke podržanosti idealan za objedinjavanje različitih hardverskih i softverskih komponenti. TCP / IP je besplatno dostupan svim računalnim hardverima i operativnim sustavima te ga je moguće integrirati u više različitih vrsta mreža poput *Etherneta*, DSL veze, *dial-up* linije i optičke mreže. TCP / IP stvara heterogenu mrežu s otvorenim protokolima koji su neovisni o operacijskom sustavu i arhitektonskim razlikama. Navedeni protokoli dostupni su svima i razvijaju se i mijenjaju konsenzusom, a ne zahtjevom jednog proizvođača.

Virtualna adresa se koristi kada procesor čita ili unosi podatke u memorijsku lokaciju te ovakav pristup ima brojne prednosti. Među njima svakako je važno navesti mogućnost programa da koristi neprekidni niz virtualnih adresa kako bi mogao pristupiti velikom memorijskom međuspremniku koji nije u fizičkoj memoriji i koji je veći od raspoložive fizičke memorije. Isto tako, virtualne adrese kada se koriste od različitih procesa su međusobno izolirane.

Pri uspoređivanju IPv4 i IPv6 protokola postoje razlike u vidu poboljšanja IPv6 protokola u odnosu na IPv4. Povećao se broj raspoložih adresa, pojednostavljeno je zaglavlje, nepotrebna i zastarjela polja su izbačena, moguće je direktno usmjeravanje zbog većeg adresnog prostora i zbog toga je usmjeravanje učinkovitije ali i dalje je IPv4 rasprostranjeniji. Rasprostranjeniji je zbog toga što i dalje dolaze poboljšanja za IPv4, zbog poboljšanja performansi hardvera i zbog promjene načina na koje su mreže konfigurirane.

Literatura

1. Hunt, C.: TCP/IP Network Administration, O'Reilly Media, Inc. , 4. tra 2002.

2. The Internet Layer in the TCP/IP Model. Preuzeto sa: https://www.tutorialspoint.com/The-Internet-Layer-in-the-TCP-IP-Model [pristupljeno: 30.5.2020.].

3. Network Access Layer. Preuzeto sa: https://darkness19935.wordpress.com/category/network-access-layer/ [pristupljeno 30.05.2020.].

4. Mrežni protokoli. Preuzeto sa: http://tfotovic.tripod.com/ni_protokoli.htm [pristupljeno: 30.05.2020.].

5. Address Resolution Protocol (ARP). Preuzeto sa: https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP [pristupljeno: 1.6.2020.].

6. RARP. Preuzeto sa: https://www.geeksforgeeks.org/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/ [pristupljeno: 1.6.2020.].

7. Internet Control Message Protocol (ICMP). Preuzeto sa: https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/ [pristupljeno: 1.6.2020.].

8. What is IGMP(Internet Group Management Protocol)?. Preuzeto sa: https://www.geeksforgeeks.org/what-is-igmpinternet-group-management-protocol/?ref=rp, [pristupljeno: 2.6.2020.].

9. Promet u Internet mreži. Preuzeto sa: http://e-student.fpz.hr/Predmeti/T/Tehnologija_telekomunikacijskog_prometa/Materijali/10predavanje.pdf [pristupljeno:3.6.2020.].

10. Mrežni sloj, IPv4, . Preuzeto sa: http://kristinka-blazeka-blog.from.hr/?page_id=760, [pristupljeno:3.6.2020.].

11. Mrežni sloj, IPv6. Preuzeto sa: http://kristinka-blazeka-blog.from.hr/?page_id=936, [pristupljeno: 3.6.2020.].

12. Virtual address spaces. Preuzeto sa: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/virtual-address-spaces [pristupljeno: 4.6.2020.].

13. What is IP routing? . Preuzeto sa: https://study-ccna.com/what-is-ip-routing/, [pristupljeno:5.6.2020.].

14. Connected, static & dynamic routes. Preuzeto sa: https://study-ccna.com/connected-static-dynamic-routes/ [pristupljeno: 5.6.2019.].

15. TCPIP_Network_Administration. Preuzeto sa: https://www.gob.mx/cms/uploads/attachment/file/84434/02.-_TCPIP_Network_Administration.pdf [pristupljeno:30.5.2020.].

16. ARP protokol. Preuzeto sa: http://mreze.layer-x.com/s020303-0.html [pristupljeno: 1.6.2020.].

17. IPv6. Preuzeto sa: https://bs.wikipedia.org/wiki/IPv6 [pristupljeno: 3.6.2020.].

Popis slika

Slika 1: TCP / IP arhitektura 2
Slika 2: UDP format poruke 3
Slika 3: TCP format segmenta 4
Slika 4: Trosmjerno rukovanje 5
Slika 5: TCP protok podataka 6
Slika 6: Internet sloj u paketu TCP / IP složaja 7
Slika 7: Prikaz rada ARP-a. 10
Slika 8: Prikaz rada RARP-a 11
Slika 9: Zahtjev za smanjenje brzine 12
Slika 10: Zahtjev za smanjenje brzine kada je usmjerivač zagušenja daleko od izvora 12
Slika 11: Slanje vrijeme je prekoračeno poruke 13
Slika 12: Slanje odredište je nedostupno poruke 13
Slika 13: Primjer slanja poruke o preusmjeravanju 14
Slika 14: IGMPv1 Paket format 15
Slika 15: IGMPv2 Paket format 16
Slika 16: IGMPv3 Paket format 17
Slika 17: IPv4 zaglavlje 18
Slika 18: IPv6 zaglavlje 21
Slika 19: Dijagram ključnih značajki virtualnih adresnih prostora 24
Slika 20: Adresni prostor Windows-a 25
Slika 21: Paged pool i nonpaged pool 26
Slika 22: IP usmjeravanje 27
Slika 23: Zadani pristupnik 27
Slika 24: Prikaz tablice usmjeravanja usmjerivača 28
Slika 25: Izravno povezane podmreže 29
Slika 26: Statičko usmjeravanje 30
Slika 27: Tablica usmjeravanja usmjerivača A 30
Slika 28: Prikaz naredbe statičke rute 30
Slika 29: Prikaz naredbe dinamičke rute 32

Sveučilište u Zagrebu
Fakultet prometnih
znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz

necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

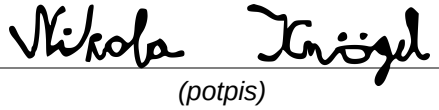
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Značajke IP adresa i usmjeravanje paketa u telekomunikacijskoj mreži**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 20.8.2020

Student/ica:



(potpis)