Analiza značajki i primjene protokola mrežnog sloja TCP/IP skupine protokola

Milak, Tea

Undergraduate thesis / Završni rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:184495

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 14. ožujka 2017.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 3847

Pristupnik: **Tea Milak (0135231873)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza značajki i primjene protokola mrežnog sloja TCP/IP skupine protokola**

Opis zadatka:

U radu je potrebno opisati značajke mrežnih modela. Provesti analizu mrežnih modela. Analizirati model TCP/IP i njegove protokole po slojevima. Objasniti značajke protokola mrežnog sloja TCP/IP skupine protokola te napraviti usporednu analizu primjene protokola mrežnog sloja TCP/IP modela.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

doc. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Tea Milak

ANALIZA ZNAČAJKI I PRIMJENE PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA

ZAVRŠNI RAD

ZAGREB, 2017.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA ZNAČAJKI I PRIMJENE PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA

FEATURE ANALYSIS AND THE APPLICATION OF THE TCP/IP PROTOCOL NETWORK LAYER

Mentor: doc. dr. sc. Ivan Grgurević

Student: Tea Milak
JMBAG: 0135231873

Zagreb, rujan 2017.

ANALIZA ZNAČAJKI I PRIMJENE PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA

SAŽETAK

OSI (engl. *Open Systems Interconnection*) referentni model je apstraktni model koji se sastoji od sedam slojeva, a osigurava stručnjacima i ostalim dionicima (primjerice proizvođačima mrežne opreme) temelj na kojem proučavaju mrežu i sve njezine elemente i procese. Na TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) modelu zasniva se internetska arhitektura koja je opisana kroz svoja četiri sloja.U radu su detaljnije opisani protokoli mrežnog sloja TCP/IP modela. Internet protokoli služe za prijenos podataka. IPv4 protokol koristi se danas, no zbog previše IP adresa dolazi do prepunjavanja adresnog spremnika te se uvodi nova verzija Internet protokola poznata pod nazivom IPv6 protokol. IPv6 protokol donosi nova poboljšanja koja bi trebala doprinijeti bržem i sigurnijem prijenosu podataka. Zaglavlje IPv6 protokola je jednostavnije od IPv4 protokola. IPv6 protokol donosi nova poboljšanja koja bi trebala doprinijeti bržem i sigurnijem prijenosu podataka.

Ključne riječi: OSI referentni model; TCP/IP model; mrežni sloj; protokoli; IPv4; IPv6

SUMMARY

The Open Systems Interconnection (OSI) reference model is an abstract model that consists of seven layers and provides experts and other stakeholders (such as network equipment manufacturers) a foundation for studying the network and all its elements and processes. The TCP / IP (Transmission Control Protocol / Internet Protocol) model is based on an internet architecture that is described through its four layers. The work is described in more detail in the protocol protocol of the network layer of the TCP / IP model. Internet protocols serve to transfer data. The IPv4 protocol is used today, but too many IP addresses overflow the address server and introduce a new version of the Internet protocol known as the IPv6 protocol. The IPv6 protocol brings new improvements which should contribute to faster

and safer data transfer. IPv6 header the protocol is simpler than the IPv4 protocol. The IPv6 protocol brings new improvements that should contribute to faster and safer data transfer.

Key words: OSI model; TCP/IP model; Protocols; IPv4; IPv6

SADRŽAJ

1. UVOD 1
2. ZNAČAJKE I ANALIZA MREŽNIH MODELA 3
   2.1. OSI referentni model 3
      2.1.1. Aplikacijski sloj (engl. *Aplication layer*) 4
      2.1.2. Prezentacijski sloj (engl. *Presentation layer*) 5
      2.1.3. Sesijski sloj (engl. *Session layer*) 5
      2.1.4. Transportni sloj (engl. *Transport layer*) 5
      2.1.5. Mrežni sloj (engl. *Network layer*) 5
      2.1.6. Sloj veza (engl. *Data layer*) 6
      2.1.7. Fizički sloj (engl. *Physical layer*) 6
   2.2. TCP/IP model 6
3. ANALIZA MODELA TCP/IP 7
   3.1. Aplikacijski sloj 7
   3.2. Transporni sloj 8
   3.3. Internet sloj 8
   3.4. Sloj mrežnog pristupa 8
4. PROTOKOLI MODELA TCP/IP 10
   4.1. Aplikacijski sloj 10
   4.2. Transportni sloj 11
   4.3. Internet sloj 11
   4.4. Sloj mrežnog pristupa 12
5. ZNAČAJKE PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA 13
   5.1. Kontrolni protokoli 14
   5.2. Protokoli razlučivanja adrese 16
   5.3. Protokoli usmjeravanja 18
   5.4. Internet protokol (IP) 21
6. USPOREDNA ANALIZA PRIMJENE PROTOKOLA MREŽNOG SLOJA TCP/IP MODELA 25
   6.1. IPv4 25
   6.2. IPv6 26
   6.3. Komparacija IPv4 i IPv6 28
7. ZAKLJUČAK 33

LITERATURA 35
POPIS KRATICA I AKRONIMA 37
POPIS SLIKA 39
POPIS TABLICA 40

1. UVOD

U mrežnoj komunikaciji podaci putuju po slojevima modela za otvoreno povezivanje sustava (engl. *Open Systems Interconnection Model* - OSI) odnosno TCP/IP (engl. *Transmission Control Protocol / Internet Protocol*) modelu koji u biti radi ono što OSI objašnjava u teoriji.

Unutar tih modela mrežne komunikacije način obrade podataka određuju protokoli koji su smjernice tj. standardi. Oni se mogu definirati kao skupina pravila koja utvrđuje postupak prijenosa podataka u mreži. Referentni model po kojem se izrađuju ostali modeli je OSI referentni model te je iz njega nastao model TCP/IP koji se implementirao u telekomunikacije i postao najkorišteniji model za prijenos podataka.

Razvojem računalne mreže, Interneta, stručnjaci su razvili osnovne TCP/IP protokole nakon što je mreža postala operativna. Mrežni sloj, jedan od četiri sloja ovog modela ima zadaću pružanja usluge povezanosti i odabira najbolje rute za slanje podataka kroz mrežu.

Predmet završnog rada je analiza i usporedba značajki i primjene protokola mrežnog sloja TCP/IP skupine protokola.

Cilj završnog rada je prikazati značajke OSI referentnog i TCP/IP modela te njihovu usporedbu, navesti i objasniti protokole TCP/IP modela te napraviti usporednu analizu primjene protokola mrežnog sloja TCP/IP modela. Svrha završnog rada je proširiti znanje i istražiti mrežne modele i njihove pripadajuće protokole koji se danas koriste.

Završni rad sastoji se od sedam funkcionalno povezanih dijelova ili teza:

1. Uvod,
2. Značajke i analiza mrežnih modela,
3. Analiza modela TCP/IP,
4. Protokoli modela TCP/IP,
5. Značajke protokola mrežnog sloja TCP/IP skupine protokola,
6. Usporedna analiza primjene protokola mrežnog sloja TCP/IP modela te
7. Zaključak.

Prvo poglavlje završnog rada je *Uvod* u kojem se iznosi predmet rada, cilj, svrha te njegova struktura.

Drugo poglavlje rada odnosi se na općenita obilježja OSI referentnog modela, te opis svih slojeva OSI modela dok je u trećem poglavlju rada pojašnjen TCP/IP model te karakteristike svih slojeva. Računalna mreža definira se kao sustav od sedam slojeva (OSI referentni model) ili od četiri sloja (TCP/IP model).

U petom poglavlju prikazane su značajke protokola mrežnog sloja TCP/IP skupine protokola, a u šestom poglavlju rada prikazana je usporedba primjene protokola mrežnog sloja TCP/IP modela.

U šestom poglavlju rada prikazana je usporedba protokola verzija IPv4 i IPv6.

Sedmi dio rada je *Zaključak* koji je donesen na temelju istraživanja i vlastitih promišljanja.

Na kraju rada se uz popis literature nalazi i popis kratica i akronima te popis slika i tablica prikazanih u tekstu rada.

2. ZNAČAJKE I ANALIZA MREŽNIH MODELA

Da bi se olakšala analiza mreže i uređaja na njoj, uvedeni su slojeviti mrežni modeli. Tu se definiraju protokoli[1] koji pomažu u prijenosu podataka po slojevima do krajnjeg korisnika. Svakom sloju se dodjeljuju određene funkcije i definiraju se režimi rada tih funkcija.

Dva najčešće spominjana slojevita modela računalnih mreža su OSI referentni model[2] te tzv. TCP/IP ili IP grupa protokola. Dok je OSI model 7-slojni, TCP/IP je 4-slojni model, te je jednoznačno preklapanje nemoguće. Stoga se različiti protokoli i arhitekture računalnih mreža često referenciraju na jedan od ta dva modela, odnosno nalaze svoje mjesto na nekom od slojeva navedenih modela.

2.1. OSI referentni model

U ovom poglavlju objasnit će se OSI referentni model, njegove značajke, slojevi te protokoli.

Model za otvoreno povezivanje sustava je model mrežne komunikacije koju je sastavila Međunarodna Organizacija za Standardizaciju (engl. *Internacional Organization for Standardization* - ISO) 1977. godine. OSI model je podijeljen u sedam slojeva (engl. *layer*) i svaki od njih nosi određenu ulogu u prijenosu podataka. [1]

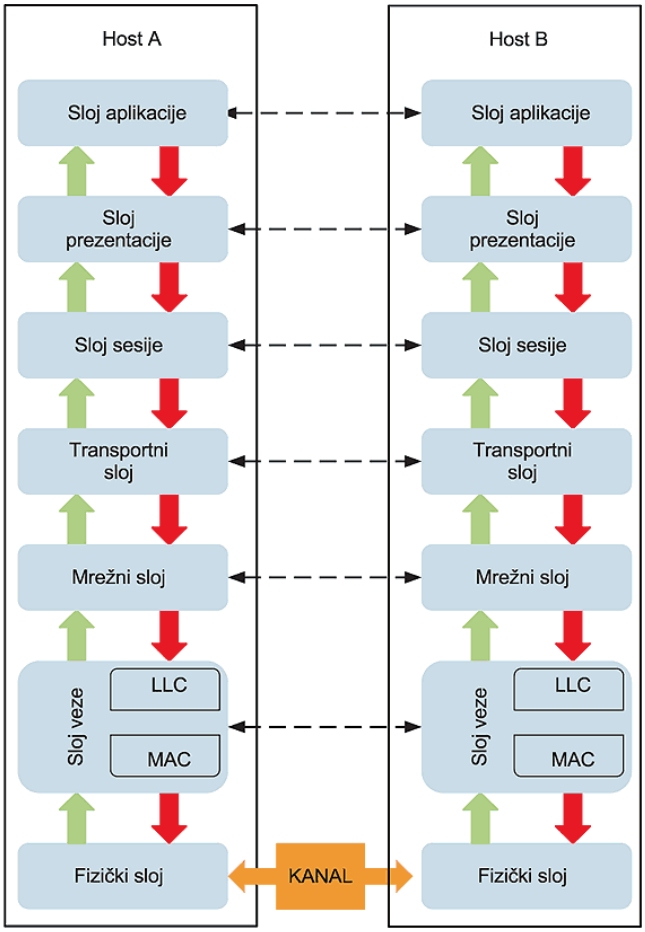
Prednosti korištenja slojevitog modela su sljedeće:

- dijeli komunikacijske procese u mreži na manje i jednostavne komponente,
- omogućava više proizvođački razvoj kroz standardizaciju mrežnih komponenti,
- omogućava različitim vrstama mrežnog hardvera i softvera zajednički rad te
- sprječava da izmjene na jednom sloju utječu na druge slojeve.

Slojevi unutar jednog modela komuniciraju samo s prvim slojem iznad i prvim slojem ispod sebe. Gornji protokol ovisi o funkcionalnosti koji pruža protokol ispod njega. Ukoliko komunikaciju prikažemo s dva OSI modela možemo vidjeti da se slojevi jednog modela povezuju samo sa slojevima istog nivoa drugog modela. Npr., transportni sloj jednog modela

[1] Protokol – dogovor između dvije jedinice o načinu komunikacije
[2] OSI referentni model-apstraktni, slojeviti model koji služi kao preporuka stručnjacima za razvoj računalnih mreža i protokola

šalje podatke transportnom sloju drugog modela. To se naziva komunikacija svaki sa svakim (engl. *peer to peer*). Svaki od modela u osnovi predstavlja jedan komunikacijski uređaj. [2]



Slika 1. Komunikacija između dva OSI modela [3]

Kod slanja dokumenta preko mreže on će proći put od aplikacijskog sloja preko prezentacijskog sve do fizičkog, a na računalu koje prima taj dokument, put će biti obrnut i ići će od fizičkog preko prezentacijskog sloja do aplikacijskog (kao što je prikazano na slici 1.).

2.1.1. Aplikacijski sloj (engl. *Aplication layer*)

Na ovom sloju dolazi do spoja između aplikacije i mrežnog softvera na računalu ili na nekom drugom uređaju. Upravo ovdje se nalaze programi koji nam omogućuju mrežnu komunikaciju. Na aplikacijskom sloju definirana su pravila kojima će krajnje aplikacije

prenositi podatke između sebe. Protokoli na ovom sloju procesuiraju zahtjeve od drugog računala s aplikacijskog sloja i tvore mrežu.

2.1.2. Prezentacijski sloj (engl. *Presentation layer*)

U ovom sloju se primljeni podaci pretvaraju u format koji je razumljiv drugom računalu tj. drugom aplikacijskom sloju. Njegova glavna uloga je da prevodi tekst koji je razumljiv njemu pa i na kraju čovjeku i računalu (ovisno o smjeru kretanja podataka). On se brine o enkripciji[3] i dekripciji tih podataka.

2.1.3. Sesijski sloj (engl. *Session layer*)

Već se iz naziva sloja može saznati za što je on zaslužan. On se brine o održavanju i uspostavi sesije između predajnika i prijemnika. Protokoli imaju funkciju razmijene podataka o uspostavljanju komunikacije, održavanja komunikacije aktivnom te ukoliko je potrebno da je ponovo uspostave i na kraju prekinu.

2.1.4. Transportni sloj (engl. *Transport layer*)

Uloga transportnog sloja je da omogući komunikaciju između sloja prije, sesijskog, i sloja poslije, mrežnog. Njegova primarna zadaća je da prihvati podatke izvorne aplikacije i dostavi ih odredišnoj aplikaciji, pri čemu se vodi briga o prijenosu, kontroli i ispravljanju grešaka pri prijenosu te isporuci podataka (tražiti će se potvrda svakog poslanog paketa).

2.1.5. Mrežni sloj (engl. *Network layer*)

Zadatak ovog sloja je pravilno usmjeravanje[4] podataka do odredišta kako se ne bi „zagubili“. U ovom sloju paket dobiva adresu, kako ishodišnu tako i odredišnu, točnije dobiva Internet Protokol (IP) adresu. Nudi se mogućnost usmjeravanja podataka preko mreže.

---

[3] Enkripcija – proces transformacije informacije tako da su nečitljive neovlaštenim osobama
[4] Usmjeravanje – postupak odabira puta za slanje podataka kroz mrežu.

2.1.6. Sloj veza (engl. *Data layer*)

Radi mogućnosti pojavljivanja pogrešaka prilikom prijenosa podataka neophodan je sloj koji kontrolira svaki uređaj u komunikaciji. Potrebno je osigurati kontrolu toka, formiranje okvira i ako dođe do pogreške njeno ispravljanje. Paketi koji se formiraju u okvire šalju se na fizički sloj tj. na medije za prijenos. Ovdje se u okvir stavlja gore dobivena ishodišna i odredišna fizička adresa uređaja (IP adresa dodjeljena fizičkoj (MAC) adresi).

2.1.7. Fizički sloj (engl. *Physical layer*)

Osnovna zadaća ovog sloja je da prevodi komunikacijske zahtjeve sloja veze u specifične operacije tj. da kodira bitove u signale. On ih tada šalje i prima putem fizičkog medija koji povezuje mrežna računala ili uređaje. Fizički mediji mogu biti raznovrsni: bakrena parica, optički kabel ili zrak (bežična veza).

2.2. TCP/IP model

Naziv TCP/IP potječe od dva najčešće korištena protokola, a to su TCP (engl. *Transmission Control Protocol*) i IP (engl. *Internet Protocol*). TCP/IP protokol prisutan je danas na skoro svim računalima, u prvom redu zbog jednostavnog definiranja adresa uređaja na mreži, te zbog mogućnosti povezivanja na Internet. Zbog svojih pogodnosti je jedan od najraširenijih mrežnih modela na internetu, zapravo to i je model na kojem radi Internet. [3]

Glavna karakteristika je da ne zahtijeva točno određen tip uređaja i operacijski sustav koje koriste krajnji korisnici; nego omogućava povezivanje različitih tipova mreže itd.

Analiza TCP/IP model[5]a obrađena je u sljedećem poglavlju.

[5] TCP/IP model- grupa protokola koju još nazivamo IP grupa protokola

3. ANALIZA MODELA TCP/IP

TCP/IP model je stvoren po uzoru na OSI referentni model s nekim preinakama kao što je broj slojeva, tako da TCP/IP model ima četiri sloja koji obuhvaćaju sve funkcionalnosti OSI modela koji ima sedam slojeva. [3]

Slika 2. Razlika OSI i TCP/IP modela po slojevima [1]

Model TCP/IP sastoji se od aplikacijskog sloja, transportnog sloja, Internet sloja i sloja mrežnog pristupa.

3.1. Aplikacijski sloj

Najviši sloj TCP/IP protokola je aplikacijski sloj. Aplikacijski sloj čine programi i procesi tj. korisnikove aplikacije, koji svoje zahtjeve ili podatke predaju izravno protokolima transportnog sloja. Dizajneri TCP/IP-a smatrali su da protokoli višeg nivoa[6] trebaju

[6] Viši sloj – protokoli višeg sloga čine aplikacijski sloj, prezentacijski sloj i sloj sesije.

objedinjavati detalje veze i prezentacije. Zbog toga su jednostavno kreirali aplikacijski sloj koji upravlja sa protokolima višeg nivoa, problematikom prikaza, enkodiranjem i kontrolom dijaloga. TCP/IP kombinira svu problematiku vezanu uz aplikativni dio u jednom sloju (aplikacijskom) i osigurava ispravno pakiranje podataka za sljedeći sloj. [6]

3.2. Transporni sloj

Transportni sloj osigurava uspostavu logičke veze[7] između dva računala u mreži, osigurava kontrolu toka s kraja na kraj, te pouzdanost prijenosa. Brine se o kvaliteti usluge[8], problematici pouzdanosti[9], protoku podataka i ispravljanju grešaka. [5]

Dva najznačajnija protokola transportnog sloja su TCP (engl. *Transmission Control Protocol*) i UDP (engl. *User Datagram Protocol*). Programeri mogu odabrati protokol koji najbolje odgovara njihovoj aplikaciji.

3.3. Internet sloj

Internet sloj je drugi sloj kod TCP/IP modela. Na ovom sloju omogućava se uspostava logičke veze između dva uređaja koja žele komunicirati. Uređaji se prepoznaju preko adresa koje su prema Internet protokolu predstavljena 32-bitnim brojem. Internet sloj prenosi podatke unutar TCP/IP modela tj. prihvaća ih od sloja mrežnog pristupa i predaje transportnom sloju, izdvajajući i analizirajući svoje zaglavlje. [4]

Osnovna jedinica podataka na ovom sloju je datagram. Datagram je blok podataka koji se šalje na mrežu kao jedna poruka.

Na Internet sloju osnovni su protokoli IP (engl. *Internet Protocol*) i ICMP (engl. *Internet Control Message Protocol*).

3.4. Sloj mrežnog pristupa

[7] Logička veza – predstavlja komunikaciju izmežu krajnjih uređaja bez obrzira na to postoji li fizička veza ili ne.
[8] Kvaliteta usluge – predstavlja mogućnost dodjeljivanja različitih prioriteta različitim aplikacijama.
[9] Pouzdanost – vjerojatnost da će sustav raditi na planiran način ostvarujući pri tome tražene aktivnosti.

TCP/IP je dizajniran tako da skriva funkcije nižih slojeva, a često spominjani protokoli IP, TCP, UDP i dr. spadaju u protokole viših slojeva. Funkcije koje se obavljaju na ovom sloju obuhvaćaju raspakiranje IP datagrama (osnovna jedinica za transmisiju na Internetu) u okvire koji se prenose mrežom i preslikavanju IP adrese u fizičku adresu koju koristi mreža. [4]
Jedna od snaga TCP/IP protokola je shema adresiranja kojom se jednoznačno identificira svako računalo na Internetu. Ta IP adresa se konvertira u adresu koja je pogodna za fizičku mrežu preko koje se vrši prijenos.

4. PROTOKOLI MODELA TCP/IP

TCP/IP je uobičajena oznaka grupe protokola koju još nazivamo IP grupa protokola (engl. *IP protocol suite*). Naziv je ova grupa protokola dobila prema dva najvažnija protokola iz te skupine, a to su TCP te prema samom IP protokolu.

U ovom poglavlju prikazani su protokoli TCP/IP modela po slojevima.

4.1. Aplikacijski sloj

Aplikacijski sloj TCP/IP modela ujedinjuje aplikacijski, prezentacijski i sloj sesije OSI referentnog modela, odnosno aplikacijski sloj osigurava mrežne mogućnosti aplikacijama koje to zahtijevaju. Aplikacijski sloj komunicira s aplikacijama koje zahtijevaju mrežne usluge, odnosno s aplikacijama koje se baziraju na komunikaciji s udaljenim korisnikom.

Jedni od važnijih protokola aplikacijskog sloja su FTP (engl. *File Transfer Protokol*), HTTP (engl. *Hypertext Transfer Protocol*) i SMTP (engl. *Simple Mail Trasfer Protocol*).

FTP protokol služi za dvosmjerni prijenos datoteka sa servera do klijenta i obrnuto. Funkcionira temeljem TCP protokola za prijenos podataka te koristi dvije TCP konekcije, a to su kontrolna konekcija i konekcija za podatke. Kontrolna konekcija služi za slanje kontrolnih informacija između dva računala, a konekcija za podatke služi za prijenos datoteka. [7]

Razlika između HTTP i SMTP protokola je u tome što SMTP prenosi datoteke od jednog do drugog servera za e-poštu, dok HTTP prenosi datoteke od web servera do web klijenta. HTTP je uglavnom prijemni protokol zbog toga što korisnik prima informacije na njegov zahtjev. SMTP je uglavnom predajni protokol zbog toga što korisnik većinom prima e-poštu na svoj server. SMTP zahtjeva da svaka poruka bude u ASCII (engl. *American Standard Code for Information Interchange*) formatu dok HTTP ne nameće takav zahtjev. [7]

Protokoli aplikacijskog sloja određuju:

- Tipove poruka koje se razmjenjuju,
- Sintaksu – tipove podataka,
- Semantiku poruke – značenje poruke,
- Odrađivanje pravila i vremena slanja i primanja poruka.

4.2. Transportni sloj

Transportni sloj je drugi sloj u TCP/IP modelu i njegove dvije osnovne zadaće su kontrola pogreški i kontrola toka. Kontrola pogreški obuhvaća praćenje i identifikaciju potencijalne pogreške. Do pogreške može doći zbog nepovoljnog stanja poveznice i zbog neodgovarajućeg usmjeravanja. [8]

Kontrola toka znači praćenje zagušenja u mreži odnosno prati se stanje poveznice. U slučaju prevelikog broja paketa na nekoj poveznici šalje se zahtjev za usporavanje slanja ili kompletna obustava slanja paketa. Dva su osnovna protokola transportnog sloja, a to su TCP i UDP protokol.

TCP protokol je konekcijski orijentiran protokol te se prije slanja podataka uspostavlja veza i određuje optimalna ruta kojom će svi paketi slati. TCP je pouzdaniji, kontrolira zagušenje[10] i kontrolira tok podataka od izvora do odredišta.

UDP protokol je nekonekcijski orijentiran protokol te se odmah počinju slati podaci. Podaci koji se šalju kroz mrežu mogu putovati različitim putevima, stoga postoji veća vjerojatnost da će podaci biti izgubljeni ili ne će doći onim redoslijedom kojim su poslani.

Multiplekisranje i demultipleksiranje su također zadaci transportnog sloja. Multipleksiranje je zadatak prikupljanja podataka s priključnica (engl. *socket*), enkapsulacija svakog dijela zaglavljem i prosljeđivanje mrežnom sloju. Demultipleksiranje je zadatak isporučivanja podataka na odgovarajuću priključnicu. [8]

4.3. Internet sloj

Internet sloj je treći sloj u TCP/IP modelu i on određuje optimalan put kojim će paketi putovati kroz mrežu te slanje paketa s mreže na međumrežje i njegov dolazak na odredište.

Usmjeravanje paketa se može izvesti na dva načina, a to su upotrebom virtualnog kanala i datagramski. Virtualni kanal znači da se prije prijenosa podataka uspostavlja konekcija izvorišta i odredišta, te se prilikom uspostave konekcije određuje put kojim će putovati svi

[10] Zagušenje – pojava kada čvor prima ili šalje toliko podataka da se javljaju gubici paketa ili stvaranje velikog reda čekanja.

paketi. Usmjeravanje izvedeno datagramski ne zahtjeva uspostavu konekcije nego se datagrami zasebno šalju kroz mrežu, pa je tako moguće da svaki datagram ide svojim putem. [9]

Važniji protokoli ovog sloja su IP protokol i ICMP protokol. IP protokol je zadužen za slanje paketa od izvora do odredišta. On se ne brine o tome je li paket stigao na odredište i je li taj isti paket stigao u cijelosti bez pogreške. IP protokol nema mogućnost identifikacije i korekcije pogrešaka, zbog toga je osmišljen ICMP protokol koji se koristi u tu svrhu.

Jedina zadaća ICMP protokola je identifikacija pogreške. On ima mogućnost detekcije ali nema mogućnost ispravljanja te pogreške. ICMP protokol javlja pošiljaocu da je došlo do pogreške te da se traži ponovno slanje paketa odnosno retransmisija. ICMP otkriva da paket nije stigao kada TTL (engl. *Time To Live*) odnosno vrijeme života paketa istekne i dođe do nule. Tada se paket smatra izgubljenim i traži se retransmisija paketa. [9]

4.4. Sloj mrežnog pristupa

Sloj mrežnog pristupa je najniži sloj u TCP/IP modelu. Ovaj sloj sadrži sve funkcije koje su spomenute u podatkovnom i fizičkom sloju OSI referentnog modela. Uspostavlja komunikaciju između dva terminalna uređaja[11] u mreži te prilagođava pakete za prijenos preko fizičkog medija. Ukoliko format paketa ne odgovara formatu koji podržava taj medij on ima zadaću konvertirati taj paket u oblik pogodan za prijenos. Njegova zadaća je enkapsulacija podataka u okvire (engl. *framing*) koji se tada dalje pretvaraju u oblik pogodan za prijenos kroz mrežu. Taj oblik najviše ovisi o tome kroz koju vrstu medija se šalje taj podatak od izvora do odredišta. [10] Također on postavlja adrese izvora i odredišta koje su najčešće izvedene kao MAC adrese.

[11] Terminalni uređaj – krajnji uređaj u telekomunikacijskoj mreži.

5. ZNAČAJKE PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA

Za različite načine komunikacije postoje i različite vrste protokola. Protokoli su grupirani u sedam različitih slojeva kod OSI referentnog modela, ili u četiri sloja kod TCP/IP modela. Kod TCP/IP modela protokoli su razvrstani na aplikacijski sloj, transportni sloj, internet sloj i sloj mrežnog pristupa. Način na koji su protokoli podijeljeni po slojevima ovisi o njihovoj zadaći i procesu koji obavljaju na sloju, budući da svaki sloj ima svoju strogo definiranu funkciju, tako i svaki protokol na pojedinom sloju ima svoju funkciju i proces koji mora odraditi u procesu komunikacije. [11] Funkcija svakog sloja je izabrana da zadovolji standardne protokole.

Protokoli se mogu definirati kao skup opće prihvaćenih pravila koja se primjenjuju kod elektroničkog načina prijenosa podataka u nekoj mreži. Protokola ima mnogo po svim slojevima, a da bi se koristili uslugama na Internetu, treba znati njihova značenja, zadaće, procese, prednosti i nedostatke.

Osnovne uloge protokola u računalnim mrežama su:

- definicija oblika poruka koje se prenose mrežom,
- definicija pravila ponašanja na mreži (tko, kada i na koji način smije komunicirati, zapravo bonton ponašanja na mreži),
- definicija veličine i semantike polja unutar paketa koji se prenose na mreži i
- definicija mehanizama koji su potrebni za uspješnu komunikaciju. [1]

Mrežni protokol je skup standardnih pravila za prikaz i signalizaciju podataka, te za provjeru od grešaka koju je potrebno izvršiti da bi se podatak uopće poslao.

Protokoli mrežnog sloja kod TCP/IP modela podijeljeni su u nekoliko skupina, i to na:

- kontrolne protokole,
- protokole razlučivanja adrese,
- protokole usmjeravanja i
- internet protokol.

5.1. Kontrolni protokoli

Kontrolni protokoli ICMP (engl. *Internet Control Message Protocol*) i IGMP (engl. *Internet Group Management Protocol*) smatraju se sastavnim dijelovima IP-a, iako koriste IP kao dostavni mehanizam. [12]

ICMP služi za dojavu pogrešaka prilikom usmjeravanja i dostave datagrama, upravljanje prometnim tokom i neke druge funkcije nadgledanja i upravljanja. Osnovna namjena ICMP protokola je osigurati kontrolu prijenosa podataka do odredišta. Ovaj protokol ne osigurava pouzdani prijenos podataka, već to treba osigurati protokol više razine. Poruke se šalju samo kao odgovor na poslane IP pakete, a na poslane ICMP pakete odgovor se ne šalje. U slučaju gubitka ICMP poruke, ne generira se nova ICMP poruka o nastaloj pogrešci. ICMP poruke se šalju koristeći osnovno IP zaglavlje, gdje prvi oktet polja podataka IP paketa definira tip ICMP poruke, čime je određen format ostatka paketa, kao što prikazuje slika 3.

Osim za dojavu grešaka, ICMP poruke mogu služiti i za slanje drugih informacija.

8	16	32bit
Type	Code	Checksum
Identifier		Sequence number
Address mask		

Slika 3. Format ICMP paketa [13]

ICMP generira osam različitih tipova poruka, a te poruke su: odredište nedostupno, istek vremena, problem s parametrima, blokiranja izvorišta, preusmjeravanje, echo zahtjev/echo odgovor, vrijeme/odgovor o vremenu, zahtjev za informacijom/odgovor na zahtjev za informacijom. Detaljnije objašnjenje ovih poruka nalazi se u nastavku, [13]:

- Odredište nedostupno (engl. *Destination Unreachable*) se šalje kada nije moguće uspostaviti vezu ili pronaći put do odredišnog računala, kao i u slučaju kad odredišno računalo ne može prepoznati koja se usluga od njega potražuje. Ako su mreža ili računalo nedostupni, poruku šalje usmjernik, a ako nije prepoznata priključna točka onda ju šalje odredišno računalo.

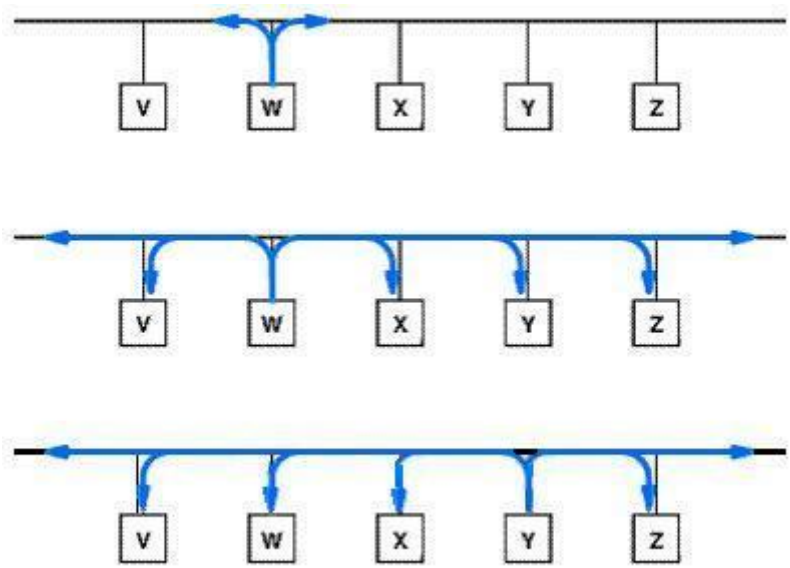
- Istek vremena (engl. *Time Exceeded*) se šalje kada je paket odbačen jer je polje "TTL" postalo jednako nuli. Ovaj tip poruke se koristi za određivanje puta kroz mrežu.
- Problem s parametrima (engl. *Parametar Problem*) u zaglavlju ne može završiti obradu podataka, te tada paket mora biti odbačen, a poruku generiraju usmjernik ili odredišno računalo.
- Blokiranje izvorišta (engl. *Source Quench*) se generira kada paketi stižu brže nego što ih odredište može obraditi pa usmjernik ili odredišno računalo šalju izvorištu ICMP poruku za privremeni prekid slanja paketa.
- Preusmjeravanje (engl. *Redirection*) je tip koji se provodi kada ICMP poruka koju šalje usmjernik u svojoj tablici usmjeravanja[12] nađe bolji put do odredišta, s tim da se drugi usmjernik mora nalaziti u istoj mreži.
- Echo zahtjev/echo odgovor (engl. *Echo Request/Echo Reply*) je tip koji se koristi kada par poruka kojima se saznaje je li odredište aktivno, u tom slučaju moraju adrese izvorišta i odredišta zahtjeva zamjeniti mjesta u odgovoru.
- Vrijeme/odgovor o vremenu (engl. *Timestamp/Timestamp Reply*) se šalje kada je potrebno saznati za koje vrijeme će se poruka preko odredišta vratiti do izvorišta.
- Zahtjev za informacijom/odgovor na zahtjev za informacijom (engl. *Information Request/Information Reply*) se koristi za doznavanje adrese vlastite mreže. Dok nam prvi kontrolni protokol ICMP služi za dojavu pogreške, drugi protokol ove skupine, IGMP nam služi za prijavu i odjavu sučelja krajnjeg uređaja u skupinu primatelja kod višeo dredišnog razašiljanja. Ovaj protokol je komunikacijski protokol koji koriste nositelji i granični usmjerivači na IP mreži. IGMP je protokol na mrežnom sloju TCP/IP složaja koji služi da računalo prijavi svoju prisutnost u multicast skupini na susjednim, udaljenim usmjernicima (engl. *routerima*).

[12] Tablica usmjeravanja – sadrži najbolje rute među pojedinim mrežnim odredištima.

5.2. Protokoli razlučivanja adrese

Protokoli razlučivanja adrese su ARP (engl. *Address Resolution Protocol*) i RARP (engl. *Reverse Address Resolution Protocol*). Dok je uloga ARP protokola da dobije fizičku adresu na lokalnoj mreži iz poznate IP adrese, uloga RARP protokola je obrnuta, te je taj protokol zadužen da iz poznate fizičke MAC adrese dobije IP adresu.

ARP protokol prevodi IP adresu u MAC adresu, a njegova najraširenija primjena danas je kod protokola Ethernet gdje se IP adrese povezuju s MAC adresama. ARP protokol radi na način da čvor u mreži koji želi dobiti neku MAC adresu razašilje (engl. *broadcast*) ARP zahtjev na mrežu, a čvor u mreži koji ima adresu iz zahtjeva, u odgovoru šalje svoju MAC adresu. Rad ARP protokola prikazan je na slici 4 dok je format ARP protokola prikazan na slici 5.



Slika 4. Rad ARP protokola [13]

Preslikavanje između virtualne IP adrese i fizičke adrese se zove pretvaranje adresa (engl. *address resolution*). Računalo ili usmjernik (engl. *router*) koriste prevođenje adresa samo kada šalju pakete unutar iste fizičke mreže, dok se adresa iz daleke fizičke mreže nikada ne prevodi.

Postoje tri osnovne tehnike prevođenja adresa, prva tehnika je pretvaranje adrese korištenjem tablice (engl. *table lookup*). Druga tehnika zove se pretvaranje adrese direktnim računanjem (engl. *closedform computation*), te posljednja tehnika naziva pretvaranje adrese izmjenom poruka (engl. *message exchange*). [13]

Kod TCP/IP modela mogu se koristiti sve tri navedene tehnike prevođenja virtualnih adresa. Tehnika pretvaranjem s tablicama se najčešće koristi za prevođenje adresa u WAN-u[13] (engl. *Wide Area Network*), dok se tehnika prevođenje izračunavanjem koristi za mreže koje podržavaju konfiguriranje fizičkih adresa. Zadnja tehnika prevođenje izmjenom poruka se koristi najčešće u LAN – ovima (engl. *Local Area Network*). ARP protokol se koristi za prevođenje 32-bitnih IP adresa u 48-bitne Ethernet adrese, a specificira se samo opći oblik ARP poruke. [14]

16		32 bit
Hardware Type		Protocol Type
HLen	Plen	Operation
Sender Hardware Address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

Slika 5. Format ARP poruke [13]

RARP (engl. *Reverse Address Resolution Protocol*) je mrežni protokol pomoću kojega se iz poznate fizičke MAC adrese može saznati IP adresa. 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 (engl. *server*) 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. [14]

[13] WAN-globalna mreža koja označava podatkovnu mrežu koja pokriva veće zemljopisno područje: gradove, države ili kontinente.

5.3. Protokoli usmjeravanja

Protokoli usmjeravanja se dijele na protokole unutrašnjeg usmjeravanja i protokole vanjskog usmjeravanja. Najčešći protokoli unutrašnjeg usmjeravanja koji su u uporabi su RIP (engl. *Routing Information Protocol*) i OSPF (engl. *Open Shortest Path First*), a protokol za vanjsko usmjeravanje je BGP (engl. *Border Gateway Protocol*). [15]

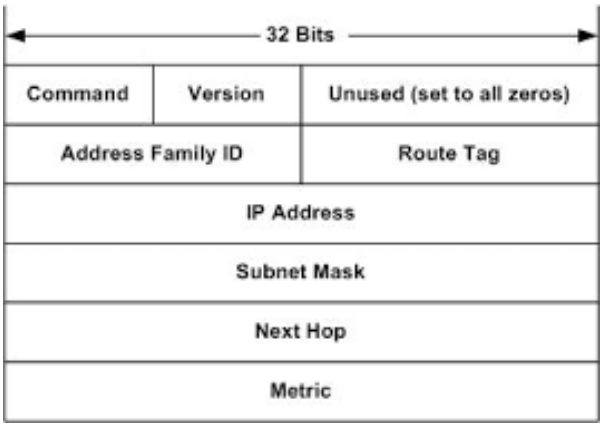
RIP (engl. *Routing Information Protocol*) je najstariji usmjerivački protokol koji se primjenjuje na Internetu, razvijen je za lokalne mreže, a zasniva se na razašiljanju (engl. *broadcast*). Ovaj protokol šalje nove usmjerivačke poruke u pravilnim intervalima ili kada se promjeni topologija mreže. Kada usmjernik dobije poruku usmjeravanja s promjenama, tablica usmjeravanja se mijenja i nadograđuje da bi prikazala novi put. Kod RIP protokola usmjernici čuvaju samo najbolji put prema odredištu, a ako nova informacija nudi bolji put onda taj novi put zamjenjuje stari. Nakon nadogradnje tablice usmjeravanja, usmjernik informira susjedne usmjernike o promjeni.

RIP protokol kao metriku koristi broj skokova te odabire smjer s najmanjim brojem skokova kao najbolji. Broj skokova je broj usmjernika koji paket treba proći na putu do odredišta. Svaki skok na putu od izvorišta do odredišta vrijedi 1, ako nije drugačije definirano, a ako je broj skokova veći od 15 tada se smatra da je odredište nedohvatljivo. RIP ima i mnogo stabilnosnih dodataka koji su zajednički za mnoge usmjerivačke protokole, a temogućnosti osiguravaju stabilnost zbog potencijalno brzih promjena u topologiji mreže. [15]

Najbitnije takve mogućnosti su:

1. Podjela obzorja (engl. *Split Horizons*) proizlazi iz činjenice da nije korisno slati informaciju o smjerovima u onom smjeru iz koje smo ju primili. Ovime se sprječava stvaranje usmjerivačkih petlji između dva usmjernika.
2. Zadržavanje promjene izbrisanih smjerova (engl. *Hold-Downs*) govori o ažuriranju smjerova koji su prekinuti i ne dolazi istovremeno na svaki usmjernik, pa se može dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je smjer još ispravan. Usmjernik koji je već obaviješten o prekidu smjera i koji primi takvu poruku, neće odmah takav smjer staviti u svoju tablicu usmjeravanja, već će određeno vrijeme zadržavati promjenu.

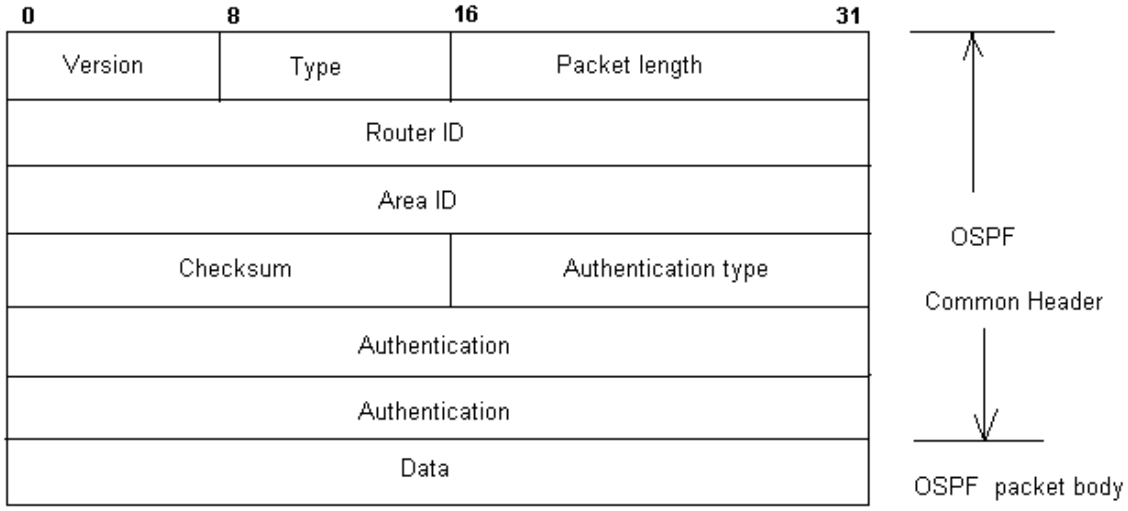
3. Ažuriranje prekinutih smjerova (engl. *Poison Reverse Updates*) je namijenjeno nalaženju i sprječavanju usmjerivačkih petlji između tri ili više usmjernika, a temelji se na tome da povećanje broja koraka za pojedini smjer obično ukazuje na pojavu usmjerivačke petlje.



Slika 6. Format paketa RIP [15]

Uz RIP protokol, sljedeći protokol unutrašnjeg usmjeravanja je OSPF (engl. *Open Shortest Path First*) protokol. Ovaj usmjerivački protokol je otvoren, njegove specifikacije su javne, protokol stanja veze koji zahtjeva slanje obavijesti o stanju veze ostalim usmjernicima unutar istog hijerarhijskog prostora. Iako je OSPF unutarnji usmjerivački protokol, sposoban je komunicirati s drugim autonomnim sustavima koji su podijeljeni u područja, a usmjernici mogu biti članovi više područja. Format paketa RIP prikazan je na slici 6.

Ako su usmjernici unutar istog područja onda imaju jednake topološke baze. Razdvajanje područja stvara dva različita tipa OSPF usmjeravanja, ovisno o tome jesu li izvorište i odredište u istim ili različitim područjima. Intraprostorno usmjeravanje se javlja kada su izvorište i odredište u istom području, a interprostorno usmjeravanje kada su u različitim područjima. Područje okosnice (engl. *Backbone Area*) OSPF-a je odgovorno za distribuiranje usmjerivačkih informacija između područja, sav promet koji povezuje neka druga područja prolazi preko njega. Sva područja moraju biti povezana na područje okosnice i svaki usmjernik unutar područja okosnice zna topologiju cijele mreže. [15]



Slika 7. Format paketa OSPF [16]

Ako postoji veći broj usmjernika u nekom području mora se pronaći način kako optimalno razmijeniti podatke između njih, a kada bi svaki usmjernik slao podatke svim ostalima to bi stvorilo velik broj međusobnih veza i prevelik te nepotreban promet. To se rješava proglašenjem glavnog usmjernika (engl. *Designated Router* - DR) i pomoćnog glavnog usmjernika (engl. *Backup Designated Router* - BDR) za svako OSPF područje mreže, te svaki usmjernik na tom području uspostavlja vezu samo prema DR-u i BDR-u, dok oni preplavljuju mrežu podacima i šalju informacije svim ostalim usmjernicima.

OSPF je dobar za srednje i velike mreže, dok minimalno opterećuje mrežu on omogućava praktički neograničen rast mreže. Ovaj protokol ima i nedostataka. On zahtijeva strukturiranu mrežnu topologiju[14] te je potrebno stručno osoblje koje će brinuti o izgradnji i održavanju mreže. Protokol održava bazu koja treba dosta prostora u memoriji usmjernika, te zahtijeva hijerarhijsku organizaciju mreže, dok ni procesorski zahtjevi nisu zanemarivi. Format paketa OSPF prikazan je na slici 7.

Protokol za vanjsko usmjeravanje je BGP (engl. *Border Gateway Protocol*) protokol. On je najpopularniji interautonomni sustavski *routing* protokol. Kada BGP usmjernik sazna prefiks dostupan kroz razne putove, odabire optimalni put, ubacuje ga u svoju tablicu usmjeravanja i objavljuje taj optimalni put ostalim usmjernicima s kojima je izravno spojen. Sam protokol ne pronalazi samostalno susjedne usmjernike, već njih ručno definira

[14] Mrežna topologija – opisuje raspored i veze između pojedinih čvorova.

administrator mreže. BGP je vrlo kompleksan protokol brojnih mogućnosti koji omogućava mrežnom administratoru detaljan utjecaj na tijekove informacija. [16]

Ovaj protokol predstavlja standard za razmjenu informacija između pružatelja internetskih usluga (engl. *Internet Service Provider* - ISP), te između ISP-ova i većih korisnika. Postoje dva tipa BGP protokola, a to su interni BGP (*Interior BGP* - iBGP) i eksterni BGP (*External BGP* - eBGP). Interni BGP (iBGP) koristi se za povezivanje usmjernika unutar istog autonomnog sustava, dok se eksterni BGP (eBGP) koristi za povezivanje različitih autonomnih sustava.

BGP protokol u svom radu koristi četiri tipa poruke: OPEN, UPDATE, KEEPALIVE i NOTIFICATION. Prva poruka, OPEN, se koristi za ostvarivanje sjednice između dva BGP usmjeritelja, a sjednica se temelji na TCP vezi. Tokom te sjednice usmjeritelji mogu izmjenjivati svoje tablice usmjeravanja preko druge vrste poruke, UPDATE poruke. Treći tip poruke, KEEPALIVE poruka, služi za održavanje sesije, dok se poruka NOTIFICATION šalje u slučaju greške. BGP protokol ima nekoliko nedostataka, a dva najveća su veličina tablica usmjeravanja i slaba sigurnost protokola. Još jedan od nedostataka je problem pojave koja se zove *route flapping*, često izbacivanje i ponovno dodavanje puta zbog krivo podešenog usmjeritelja ili zlonamjernog napada. U tom slučaju dolazi do razmjene velike količine nepotrebnih UPDATE poruka, a BGP usmjeritelj troši vrijeme na njihove obrade. Rješenje je uvođenje vremenske zadrške kod opetovane promjene dostupnosti nekog puta.

5.4. Internet protokol (IP)

Internet protokol (engl. *Internet protocol* - IP) je mrežni protokol za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže. Podatci u IP mreži se šalju u blokovima koji se nazivaju paketi ili datagrami, a prilikom slanja paketa između izvorišta i odredišta se ne određuje unaprijed točan put preko mreže kojim će podatci putovati, što znači da se IP mreža promatra kao paketska mreža. Ovaj protokol je temeljni protokol na mrežnom sloju TCP/IP modela, te ga koriste protokoli svih viših slojeva

IP je bespojni protokol, što znači da između izvorišta i odredišta nema dogovora o početku ili završetku prijenosa podataka, već kada se paket pošalje s izvorišta prema odredištu, nema

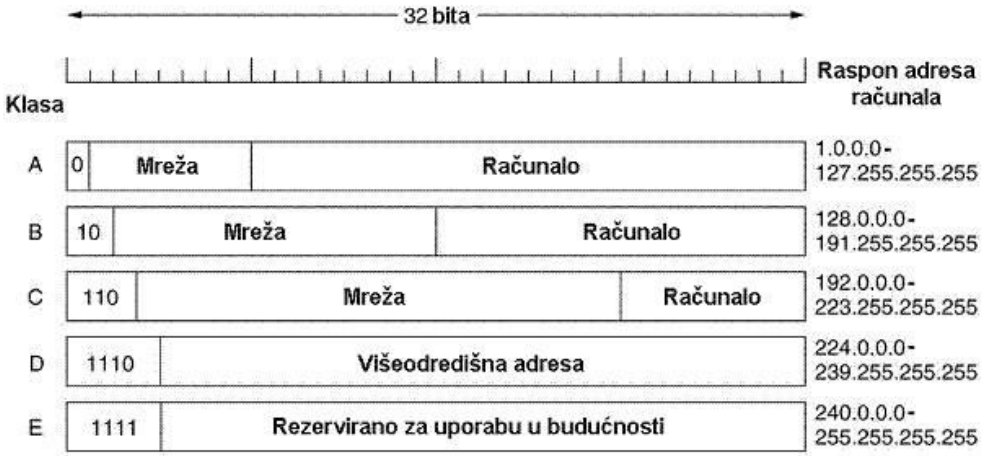
nikakve povratne informacije ili potvrde o prijemu paketa. Tek protokoli na višim slojevima provjeravaju konzistentnost podataka, te oni obavljaju detekciju i korekciju pogreški. Zbog takvog načina funkcioniranja ovog protokola, dobio je naziv „nepouzdani protokol“.

Osnovne funkcije IP protokola su:

- definiranje sheme adresiranja na Internetu,
- definiranje IP paketa,
- prosljeđivanje podataka između razine pristupa mreži i prijenosne razine, te
- fragmentacija i sastavljanje paketa. [17]

Glavna zadaća i temeljna funkcija mrežnog sloja je usmjeravanje paketa od izvorišta do odredišta na osnovu IP adrese prijemnika paketa.

IP adresa je jedinstvena adresa svakog računala, uređaja ili mrežnog sučelja spojenog na mrežu. Uređaji koji imaju više sučelja prema mreži imaju po jednu IP adresu za svako sučelje. IP adresa se sastoji od dva dijela: adrese mreže (engl. *network adress*) i adrese računala (engl. *host address*). Adresa mreže identificira podmrežu, dok adresa računala identificira računalo unutar podmreže. IP adresa je binarni broj, koji je kod verzije četiri IP protokola, binarni broj dug 32 bita. Radi lakšeg pamćenja IP adrese one se zapisuju u dekadskom načinu, gdje je 32-bitni broj podijeljen na četiri 8-bitna broja. Ti brojevi se prikazuju kao četiri decimalna broja odvojena točkom. Kod sljedeće verzije IP protokola, IPv6 verzije, predviđaju se 128-bitne adrese. IP adrese mogu biti privatne i javne. Javne IP adrese su jedinstvene, globalne i standardizirane, daljnjim razvojem Interneta počelo je nedostajati slobodnih IP adresa. Tako su se razvile privatne IP adrese, koje mogu biti duplicirane uz uvjet da se ne nalaze u istoj lokalnoj mreži. IP adrese su grupirane u pet mrežnih klasa A, B, C, D i E što je prikazano na slici 8. [17]



Slika 8. Klase IP adresa [13]

Osim funkcije adresiranja, IP omogućuje i specifikaciju vrste usluge, fragmentaciju i ponovno sastavljanje fragmenata, te specifikaciju posebnih mogućnosti, kao što je izvorno usmjeravanje i sigurnost. Ovaj protokol ne sadrži funkcije za upravljanje tokom, održavanje redoslijeda informacijskih jedinica i retransmisiju, koje bi povećale pouzdanost, već se te funkcije izvršavaju na višim slojevima. Internet protokol brine isključivo o „najboljoj mogućoj“ isporuci datagrama, a zaštitni kod koristi samo za otkrivanje i odbacivanje datagrama s pogreškom.

Tablica 1. Format IP paketa [24]

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Lenght</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Deatination Address</td></tr>
<tr><td colspan="5">Options (+ Padding)</td></tr>
<tr><td colspan="5">Data (Variable)</td></tr>
</table>

IP paket sadrži IP zaglavlje i podatkovno polje koji su opisani u nastavku, a prikazani su na tablici 1.

Verzija IP protokola *(engl. Version)* određuje format zaglavlja. IHL (engl. *Internet Header Length*) je duljina IP zaglavlja u 32-bitnim riječima, omogućava određivanje početka podataka.

Tip usluge (engl. *Type of Service*) omogućava usmjernicima različit tretman pojedinih paketa u cilju postizanja zadovoljavajuće kvalitete usluge.

Ukupna duljina (engl. *Total Length*) IP paketa u oktetima, koja uključuje IP zaglavlje i podatke.

Identifikator paketa (engl. *Identification*) je važan pri povezivanju svih fragmenata u paket.

Kontrolne zastavice (engl. *Flags*) definiraju je li fragmentacija dopuštena i ako jest, ima li još fragmenata istog paketa.

Mjesto fragmenta (engl. *Fragment Offset*) definira mjesto fragmenta u originalnom paketu.

TTL (engl. *Time to Live*) je maksimalno vrijeme života paketa u mreži, nakon čega se neisporučeni paket odbacuje, a mjeri se u sekundama.

Protokol (engl. *Protocol*) označava protokol više razine kojem se podaci prosljeđuju.

Kontrolni zbroj zaglavlja (engl. *Header Checksum*) se ponovno obračunava i provjerava pri svakoj promjeni podataka u zaglavlju.

Adresa izvorišta (engl. *Source Address*) je IP adresa predajnika paketa.

Adresa odredišta (engl. *Destination Address*) je IP adresa prijemnika paketa.

Opcije (engl. *Options*) sadrže kontrolne informacije o usmjeravanju i sigurnosne parametre.

Punjenje (engl. *Padding*) je varijabilna duljina, dopuna polja s nulama.42 Standard Interneta i najraširenija verzija internet protokola (IP) je verzija četiri (IPv4). IPv4 koristi 32-bitnu IP adresu, zbog prevelike iskoristivosti slijedeća je verzija šest (IPv6), koja koristi 128-bitnu adresu. Ove dvije verzije se razlikuju u načinu adresiranja, ali i brojnim drugim detaljima.

6. USPOREDNA ANALIZA PRIMJENE PROTOKOLA MREŽNOG SLOJA TCP/IP MODELA

Internet protokol je protokol mrežnog sloja TCP/IP složaja čija je uloga adresiranje i usmjeravanje odnosno prijenos datagrama kroz mrežu. Postoje dvije verzije, Internet protokol verzije 4 i Internet protokol verzije 6.

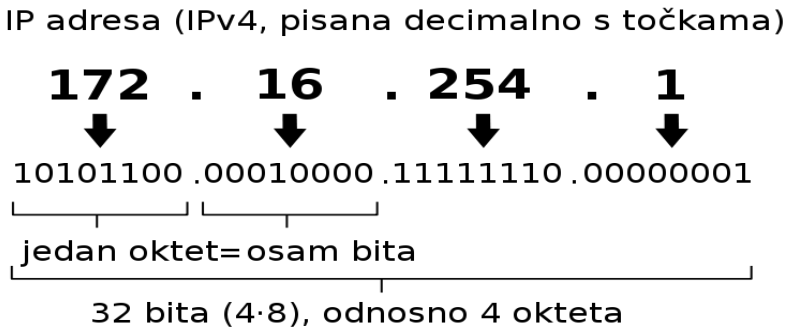
6.1. IPv4

IP protokol verzija 4, kraće IPv4, najraširenij 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: [21]

- Ne uspostavlja se veza između ishodišta i odredišta prije slanja paketa (engl. *Connectionless*)
- Najbrža moguća usluga (engl. *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 (engl. *Media indepedent*)

IP adresa je u binarnom obliku dugačka 32 bita, ali da bi se ljudi lakše snalazili u radu sa IP adresama prilagođen je zapis brojevima u intervalu od 0 do 255 koji su odvojeni s točkama prikazano na slici 9.



Slika 9. Format IP adrese [22]

Sve IP adrese se sastoje od dva dijela:

- identifikatora mreže (engl. *Network Identifier*) i
- identifikatora krajnjeg računala (engl. *Host Identifier*).

Identifikator mreže određuje broj bita koji identificiraju mrežu u kojoj se nalazi mrežno sučelje i dodjela adrese preko ICANN (engl. *Internet Corporation for Assigned Names and Numbers*). Identifikator krajnjeg računala predstavlja ostatak bita koji služe za identifikaciju mrežnog sučelja koja je zadana s *Net* ID, dodjeljuje ih mrežni administrator i može ih dodatno podijeliti za uvođenje podmreža [18].

Kako bi se omogućilo komuniciranje unutar adrese Internet standard definira 3 tipa IPv4 adresa, a to su:

- *Unicast* – dodjeljuje se jednom mrežnom sučelju koje se nalazi na određenoj podmreži i koristi se za komuniciranje jedan na jedan.
- *Multicast* – dodjeljuje se jednom ili više mrežnim sučeljima koji se nalaze na različitim podmrežama i koriste se kada jedan korisnik komunicira prema većem broju primatelja.
- *Broadcast* - dodjeljuje se svim mrežnim sučeljima, koja se nalaze na podmreži i koristi se za komunikaciju jednog korisnika prema svima koji se nalaze u toj podmreži. [18]

6.2. IPv6

Internet protokol verzija 6, ili kraće IPv6 je relativno nova verzija internet protokola koja će najvjerojatnije postati sljedeća standardna verzija komunikacijskog protokola na najvećoj računalnoj mreži danas - Internetu. Trenutačno najraširenija verzija je IP verzija 4, ili kraće IPv4. Pojedine verzije internet protokola se razlikuju po načinu adresiranja, izgledu zaglavlja paketa, ali i brojnim drugim detaljima. Najvažnija karakteristika IPv6 je da koristi 128-bitnu IP adresu, tj. propisana duljina svake IP adrese u ovoj verziji protokola je 128 bita.

Podijeljena je u dva dijela:

- mrežni prefiks (engl. *network prefix*) i
- računalni prefiks (engl. *host prefix*).

Mrežni prefiks se dodjeljuje od strane institucija, a računalni prefiks se dodjeljuje ili automatski iz MAC adrese ili od mrežnog administratora. IPv6 piše se u osam grupa po četiri heksadekadske znamenke i svaka grupa odijeljena je s ":".

Primjer IPv6 adrese je 2001:b68:0:0:c789:0:f123. Ukoliko se u adresi ponavljaju nule tada se one mogu zamijeniti sa znakom "::" koji se može upotrijebiti samo jednom. Osim navedenog, adresa se može zapisati u obliku 2001:b68:0:a123::f123/64 i uz ovakvu mrežu na raspolaganju je 64 bita.

Kod adresiranja može biti više adresa bilo kojeg tipa (jednoodredišna, višeodredišna, rezervirana) na jednom fizičkom sučelju. Sva sučelja imaju *Link-local* adrese i one su jedinstvene samo na razini linka. Svrha te adrese je autokonfiguracijaili trenutni pristup mreži ako nema usmjernika.

Usmjeravanje IPv6 paketa omogućava da usmjeravanje bude na razini usmjernika nakon što *Global unicast* adrese budu konfigurirane na razini lokalne mreže. Usmjeravanje može biti dinamičko – pomoću usmjerivačkih protokola ili tatičko - pomoću statičkih ruta.

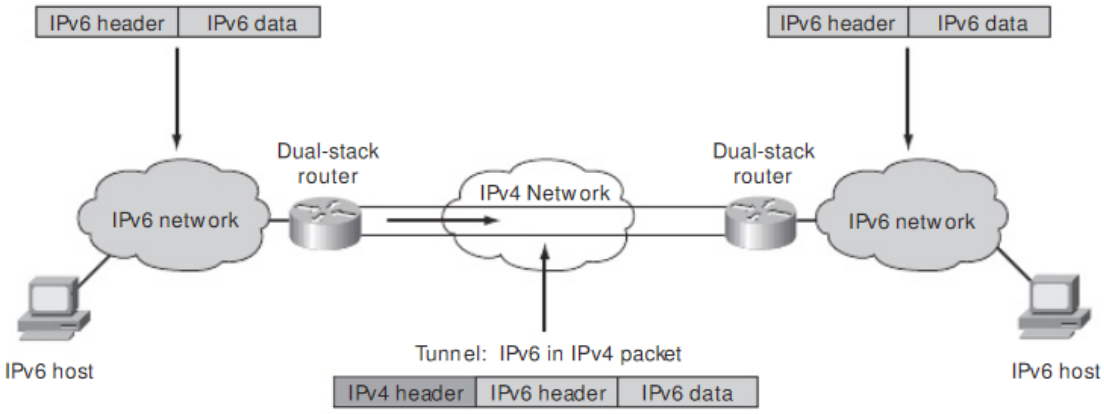
Uvođenjem IPv6 protokola prema [19] zaglavlje dobiva neke nove značajke:

- novi format zaglavlja,
- veličina adresnog prostora,
- ugrađeni sigurnosni mehanizmi,
- poboljšana podrška za kvalitetu usluge te
- proširivost.

Prelazak sa IPv4 na IPv6 nije jednostavan niti ga je moguće uvesti odjednom, već je za to potreban određen period. Da bi prelazak bio što jednostavniji razvijeno je nekoliko tehnika: [21]

- Dvostruk stog (engl. *Dual stack*) – obje verzije (IPv4 i IPv6) su istodobno aktivne, što znači da uređaji i usmjernici imaju i javnu IPv4 i javnu IPv6 adresu. Time se omogućava da se postupno prijeđe na novi protokol bez ikakvih gubitaka.
- Tuneliranje (engl. *Tunneling*) – ovom tehnikom se IPv6 protokoli enkapsuliraju unutar IPv4 paketa. Paket putuje kao IPv4 paket sve dok IPv6 mreža ne bude dostupna, tada se deenkapsulira IPv6 paket iz IPv4 paketa i proslijedi u IPv6 mrežu, prikazano na slici 10.

- Translacija (engl. *Translation*) – rješenje kojime se omogućava komunikacija IPv6 uređaja sa IPv4 uređajima pomoću NAT (engl. *Network address translation*) tehnike gdje se odrađuje mapiranje IPv6 adrese u IPv4 adresu i obrnuto.



Slika 10. Tuneliranje [23]

6.3. Komparacija IPv4 i IPv6

Internet Protokol verzije 6 (IPv6) zamjenjuje Internet Protokol verzije 4 (IPv4) kao Internet standard, te je sljedeća evolucija Internet protokola. Većina Internet komunikacije i dalje koristi IPv4 i taj protokol je pouzdan i fleksibilan već preko 20 godina, no on ima ograničenja koja mogu uzrokovati probleme prilikom proširenja mreže.

IPv6 je nova, ažurirana verzija IPv4 i postepeno je zamjenjuje kao Internet standard. To se odnosi na nedostatak IPv4 adresa koje su potrebne za sve nove uređaje koje se priključuju na Internet mrežu.

Osnovno i najbitnije u poboljšanju IPv6 je proširenje IP adresa od 32 bitova na 128 bitova, omogućujući skoro neograničene jedinstvene IP adrese. Kako sve više ljudi koristi prijenosna računala kao što su mobilni telefoni i ručna računala, povećani zahtjevi bežičnih korisnika doprinose iscrpljivanju IPv4 adresa. Ovakva proširena sposobnost IPv6 adresiranja daje rješenje problema iscrpljenih adresa, te daje dovoljno IP adresa za rastući broj bežičnih uređaja. [20]

IPv6 osigurava nove funkcije koje pojednostavljuju zadatke konfiguriranja i upravljanja adresama u mreži. Svojstvo autokonfiguracije IPv6 automatski konfigurira adrese sučelja i *default* smjerove, te uzima adresu kontrole pristupa mediju uređaja i prefiks mreže koje

osigurava lokalni usmjerivač i kombinira te dvije adrese za kreiranje nove, jedinstvene IPv6 adrese. Ako se koristi IPv6 ne treba ponovno numerirati adrese uređaja kada se promijeni dobavljač Internet usluga, jer se ono uglavnom izvodi automatski.

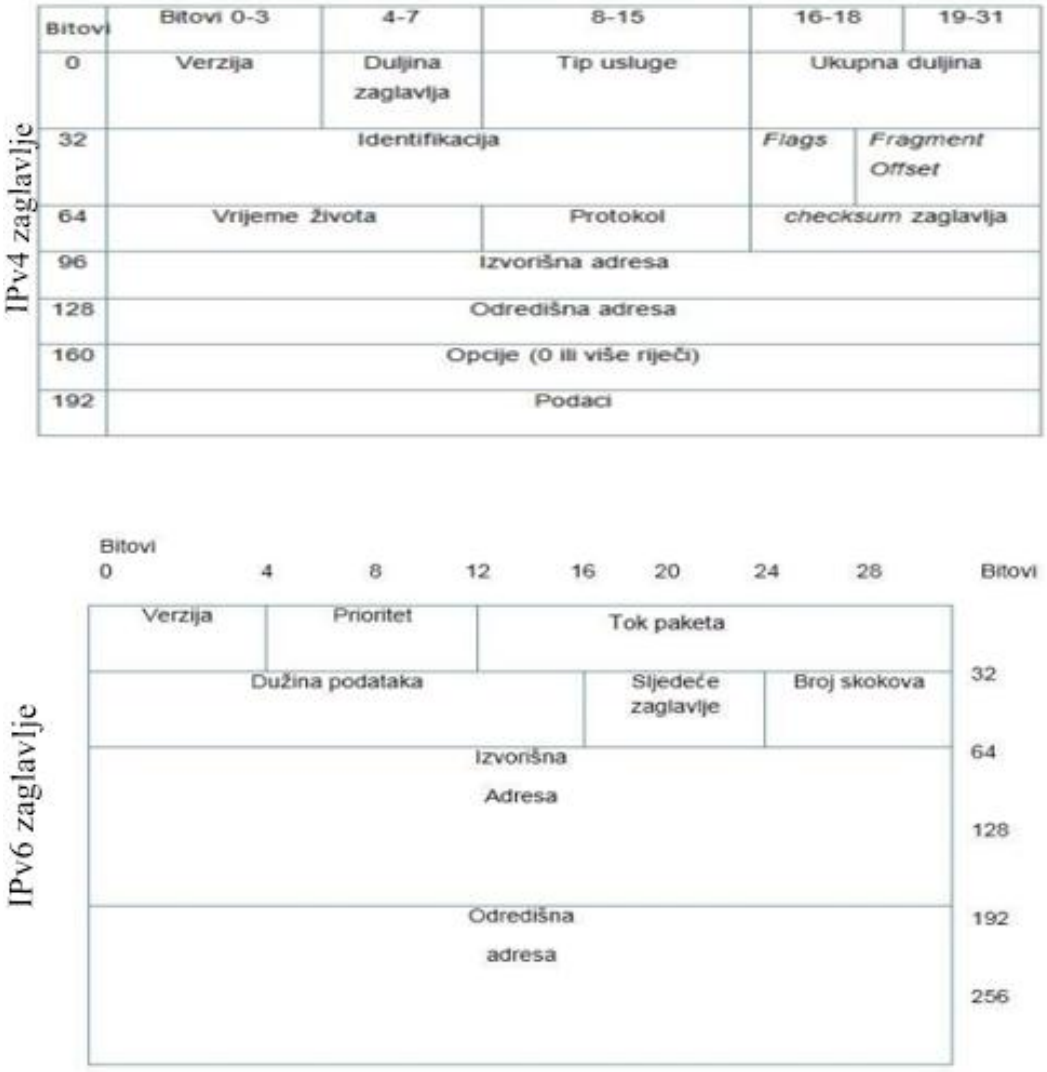
IPv6 rješava mnoge nedostatke IPv4, kao što je broj raspoloživih adresa, dodjela adrese, njezin životni vijek, opseg i tip adrese, brzina, jednostavnost konfiguracije, mobilnost, sustav imena domene, odlomci, sučelje, IP zaglavlje, prosljeđivanje i filtriranje paketa, privatne i javne adrese, pokretanje i zaustavljanje te još mnogo važnih faktora. [20]

Najbitnija razlika između ove dvije verzije je broj raspoloživih adresa, jer kod IPv4 adresa je duga 32 bita (4 bajta) i sastavljena je od mrežnog dijela i dijela hosta, koji ovise o klasi adrese. Ukupni broj IPv4 adresa je 4 294 967 296. Kod IPv6 adresa je duga 128 bitova (16 bajtova), a osnovnu arhitekturu čine 64 bita za broj mreže i 64 bita za broj hosta. Često je host dio IPv6 adrese izveden od MAC adrese ili drugog identifikatora sučelja. IPv6 ima kompliciraniju i složeniju arhitekturu od IPv4 i njezin broj adresa je 1028 puta veći od broja IPv4 adresa. Točan broj je 79 228 162 514 264 337 593 543 950 336. [20]

Životni vijek nije primjenjiv kod IPv4 adresa, osim za adrese koje su dodijeljene upotrebom DHCP-a, dok kod IPv6 adrese imaju dva životna vijeka, preferirani i važeći. Preferirani životni vijek je uvijek manji ili jednak važećem životnom vijeku i nakon njegovog isteka adresa se ne treba koristiti kao izvorna IP adresa za neke nove veze ako je dostupna dobra preferirana adresa.

Opseg adresa kod IPv6 je dio arhitekture i *unicast* adrese te imaju dva definirana opsega, uključujući lokalnu i globalnu vezu, dok *multicast* adrese imaju 14 opsega. Kod IPv4 za jednosmjerne adrese ovaj koncept se ne može primijeniti, jer postoji određeni raspon privatnih adresa i *loopback* te se pretpostavlja da su adrese globalne.

Tipovi adrese se kod IPv4 adresa kategoriziraju u tri osnovna tipa: jednosmjerna adresa, višesmjerna adresa ili univerzalna adresa. Kod IPv6, adrese se kategoriziraju također u tri osnovna tipa: jednosmjerna adresa, višesmjerna adresa i adresa najbližeg odredišta. Konfiguriranje kod IPv4 je potrebno raditi kod novo instaliranog sustava prije nego može komunicirati s drugim sistemima, što znači da IP adrese i smjerovi moraju biti dodijeljeni. Kod IPv6 konfiguracija nije obavezna, ovisno o traženim funkcijama, jer su IPv6 sučelja samokonfigurirajuća [21].



Slika 11. Format zaglavlja IPv4 i IPv6 [21]

IP zaglavlje kod IPv4 je varijabilne dužine od 20-60 bajtova, ovisno o prisutnim IP opcijama, dok je kod IPv6 ono fiksne dužine od 40 bajtova, te mnogo jednostavnije nego kod IPv4, kao što je prikazano na slici 11.

Tablica 2. Tablica usporedbe IPv4 i IPv6 [18]

	Internet protokol verzije 4	**Internet protokol verzije 6**
Adresa	32-bitna	128-bitna
Dodjela adrese	Adrese se dodjeljuju prema mrežnoj klasi, ali zbog prepunjavanja adresnog prostora, rade se manje dodjele uz pomoć *Classless Inter-Domain Routing* (CIDR).	Pomoću IETF (*Internet Engineering Task Force*) i IAB (*Internet Architecture Board*) se dodijeljuje prefiks podmreže
Životni vijek adrese	Primjenjuje se samo kod adresa koje su dodijeljene upotrebom DHCP-a (*Dynamic Host Configuration Protocol*).	IPv6 ima dva životna vijeka: preferirani i važeći gdje je preferirani uvijek manji ili jednak važećem. Nakon isteka preferiranog životnog vijeka, adresu ne treba koristiti kao izvornu IP adresu za nove veze, ako je dostupna preferirana adresa dobra.
Maska adrese	Koristi se za označavanje mreže u *host* dijelu.	Ne koristi se.
Prefiks adrese	Ponekad se koristi za označavanje mreže od *host* dijela.	Označava prefiks podmreže. Piše se kao /nnn (do 3 decimalne znamenke)
Protokol rezolucije adrese	Pomoću IPv4 pronalazi fizičke adrese, kao što su MAC ili *link* adrese koje su povezane s IPv4 adresom.	IPv6 ubacuje te funkcije unutar IP-a kao dio algoritma za samostalnu autokonfiguraciju i otkrivanje susjeda pomoću ICMPv6 (*Internet Control Message Protocol* verzije 6)
Opseg adrese	Za jednosmjerne IPv4 adrese, ne može se primijeniti. Za njihovu primjenu koriste se određeni rasponi privatnih adresa.	Raspon adresa je dio arhitekture. *Unicast* adrese imaju dva definirana opsega, a *multicast* 14 definiranih opsega.

Prilikom razvoja IPv6 protokola, nastojalo se zadržati dobre karakteristike IPv4 protokola i samim time pojednostaviti zaglavlje IPv6 paketa. U tablici 1 su prikazane bitne razlike među protokolima i što se uvođenjem IPv6 protokola promijenilo u odnosu na IPv4 protokol.

7. ZAKLJUČAK

Razvojem tehnologije protokoli postaju zastarjeli i imaju mnoge nedostatke te ih je potrebno zamijeniti sa novim, poboljšanim protokolima koji se mogu nositi sa sve većim i kompliciranijim zahtjevima aplikacija (korisika).

Upravo ti protokoli su neophodni za pravilnu međusobnu komunikaciju računala isto kako je i jezik potreban čovijeku za smislenu komunikaciju.

Da protokoli ne postoje došlo bi do kaosa u mreži tj. mreže ne bi ni bilo zato što su baš oni baza te iste mreže.

Referentni model po kojem se izrađuju ostali modeli je OSI referentni model te je iz njega nastao model TCP/IP koji se implementirao u telekomunikacije i postao najkorišteniji model za prijenos podataka.

OSI model je temelj na kojem se proučavaju mreže i svi elementi i procesi, a sastoji se od sedam slojeva. TCP/IP model je model na kojem se zasniva internetska arhitektura i sastoji se od četiri sloja.

Da bi se olakšala analiza mreže i uređaji na njoj uvedeni su slojeviti mrežni modeli. Tu se definiraju protokoli koji pomažu u prijenosu podataka po slojevima do krajnjeg korisnika. Svakom sloju se dodjeljuju određene funkcije i definiraju se režimi rada tih funkcija.

Protokoli mrežnog sloja podijeljeni su u četiri skupine. U prvu skupinu spadaju kontrolni protokoli (ICMP i IGMP) koji služe za dojavu pogrešaka prilikom usmjeravanja i dostave datagrama, upravljanje tokom i obavljaju funkciju nadgledanja i upravljanja. Druga skupina su protokoli razlučivanja adrese (ARP i RARP) koji imaju ulogu da iz poznate IP adrese dobe fizičku MAC adresu i obratno. Iduća skupina su protokoli usmjeravanja, koji se dijele na protokole unutrašnjeg usmjeravanja (RIP i OSPF) i protokole vanjskog usmjeravanja (BGP).

Najvažniji i najpoznatiji protokol mrežnog sloja je IP protokol. Protokol IP služi za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže, a razvijen je u dvije verzije: Protokol IPv6 polako dolazi u uporabu s ciljem zadovoljavanja potreba što većim brojem raspoloživih IP adresa za mrežne uređaje. Iako je IPv4 protokol odavno zastario, IPv6 i dalje nije pridobio veliki broj korisnika. Prema Google-ovoj statistici udio IPv6 adresa je tek oko 20.02 % i to u zemljama

poput Sjedinjenih Američkih Država, Kanade i zemalja Europske Unije, dok zemlje u razvoju nemaju mogućnost korištenja IPv6 protokola.

Kod IPv4 protokola, usmjeravanje se odrađuje na temelju odredišne IP adrese. Kod direktnog dostavljanja paketi se šalju rutom koja uključuje samo izvorište i odrediše te nema posrednika među njima, dok se kod indirektnog dostavljanja paketi šalju preko više usmjernika kako bi on stigao do odredišta. Kod IPv6 protokola, usmjeravanje je slično kao i kod IPv4, ali kod ovog protokola se prije korištenja tablice usmjeravanja provjerava baza za prosljeđivanje informacija kako bi se tražila potvrda o odredišnoj adresi.

I kod IPv4 i IPv6 bilo kakve promjene ili konfiguracije jednog protokola neće uzrokovati probleme na drugom protokolu. To ima svoje prednosti i mane. Prednost je da su protokoli neovisni jedan o drugom, ali mana je da na usmjerniku ne postoji jedan usmjerivački protokol nego dva.

LITERATURA

[1] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007

[2] Internetski izvor: http://sistemac.carnet.hr/node/352 (22.06.2017.)

[3] Internetski izvor: http://ahyco.uniri.hr/seminari2005/WLAN/sadrzaj_softver_protokoli.htm (27.06.2017.)

[4] Internetski izvor: http://papa.det.uvigo.es/~theiere/cursos/Curso_Internet/ISO.html (25.06.2017.)

[5] Internetski izvor: http://mreze.layer-x.com/s030201-0.html (02.07.2017.)

[6] Mrvelj, Š.: Autorizirani nastavni materijali - Tehnologija telekomunikacijskog prometa I, Fakultet prometnih znanosti, Zagreb, 2014.

[7] Internetski izvor: https://networklessons.com/cisco/tcpip-stack-tutorial/ (02.07.2017.)

[8] Internetski izvor: http://www.omnisecu.com/tcpip/tcpip-model.php (04.07.2017.)

[9] Internetski izvor: https://technet.microsoft.com/en-us/library/cc958821.aspx (04.07.2017.)

[10] Tetz, E.: Cisco Networking All-in-One For Dummies, 2011

[11] Internetski izvor: http://tfotovic.tripod.com/ni_protokoli.htm (06.07.2017.)

[12] Internetski izvor: https://hr.wikipedia.org/wiki/Ra%C4%8Dunalne_mre%C5%BEe (06.07.2017.)

[13] Internetski izvor: http://mreze.layer-x.com/s030300-0.html (05.07.2017.)

[14] Internetski izvor: http://web.studenti.math.pmf.unizg.hr/~manger/mr/MrezeRacunala-14.pdf (06.07.2017.)

[15] Internetski izvor: http://www.comptechdoc.org/independent/networking/guide/netarp.html (07.07.2017.)

[16] Internetski izvor: http://sistemac.carnet.hr/node/652 (07.07.2017.)

[17] Internetski izvor: http://www.cis.hr/dokumenti/bgp-protokol.html(07.07.2017.)

[18] Internetski izvor: http://ipv6now.com.au/whyipv6.php (07.07.2017.)

[19] Internetski izvor: https://www.carnet.hr/tematski/ipv6/rjecnik.html (07.07.2017.)

[20] Internetski izvor: http://www.phy.pmf.unizg.hr/~dandroic/nastava/mr/ipv6_adresiranja.pdf (07.07.2017.)

[21] Internetski izvor: http://umag.hr/sadrzaj/dokumenti/NATJECAJ_informaticki_referent_Uvod_u_racunalne_mreze_Visoko_uciliste_Algebra.pdf (31.08.2017.)

[22] Internetski izvor: https://hr.wikipedia.org/wiki/IP_broj#/media/File:Ipv4_address_hr.svg (31.08.2017.)

[23] Internetski izvor: https://josephmlod.files.wordpress.com/2011/06/ipv6-overipv4-tunnel.png (31.08.2017.)

[24] Internetski izvor: http://mreze.layer-x.com/s030100-0.html (31.08.2017.)

POPIS KRATICA I AKRONIMA

ARP (Address Resolution Protocol)

ASCII (American Standard Code for Information Interchang)

BGP (Border Gateway Protocol)

BDR (Backup Designated Router) pomoćni glavni usmjernik

CIDR (Classless Inter-Domain Routing)

DHCP (Dynamic Host Configuration Protocol)

DR (Designated Router) glavni usmjernik

FTP (File Transfer Protocol)

HTTP (HyperText Transfer Protocol)

IAB (Internet Arhitecture Board)

ICANN (Internet Corporation for Assigned Names and Numbers)

ICMP (Internet Control Message Protocol)

IETF (Internet Engineering Task Force)

IGMP (Internet Group Management Protocol)

IP (Internet Protocol)

IPv4 (Internet Protocol Version 4)

IPv6 (Internet Protocol Version 6)

ISO (International Organization for Standardization)

ISP (Internet Service Provider)

LAN (Local Area Network)

MAC (Media Access Control)

OSI RM (Open Systems Interconnection Reference Model)

OSPF (Open Shortest Path First)

RARP (Reverse Address Resolution Protocol)

RIP (Routing Information Protocol)

SMTP (Simple Mail Transfer Protocol)

TCP (Transmission Control Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol)

TTL (Time To Live)

UDP (User Datagram Protocol)

WAN (Wide Area Network)

POPIS SLIKA

Slika 1. Komunikacija između dva OSI modela [3] 4
Slika 2. Razlika OSI i TCP/IP modela po slojevima [1] 7
Slika 3. Format ICMP paketa [13] 14
Slika 4. Rad ARP protokola [13] 16
Slika 5. Format ARP poruke [13] 17
Slika 6. Format paketa RIP [15] 19
Slika 7. Format paketa OSPF [16] 20
Slika 8. Klase IP adresa [13] 23
Slika 9:Format IP adrese [22] 25
Slika 10:Tuneliranje [23] 28
Slika 11. Format zaglavlja IPv4 i IPv6 [21] 30

POPIS TABLICA

Tablica 1: Format IP paketa [24]..... 23
Tablica 2:Tablica usporedbe IPv4 i IPv6 [18] 31

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 **Analiza značajki i primjene protokola mrežnog sloja TCP/IP skupine protokola** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Studentica:

U Zagrebu, 5. 9. 2017. Tea Milak

(potpis) Tea Milak