TCP / IP model

Povijesni razvoj

1969. Istraživački odjel ministarstva obrane SAD (DARPA - Defense Advanced Research Projects Agency) pokrenuo je projekt uspostave eksperimentalne mreže s prespajanjem paketa nazvane ARPANET, čija je namjena bila ispitati tehničke mogućnosti razmjene podataka pomoću računalne mreže.
1975. ARPANET je od eksperimentalne postala operativna mreža. TCP/IP skup protokola usvojen je kao vojni standard 1983. Korištenje tog standarda bio je preduvjet za spajanje na ARPANET. DARPA je potakla ugradnju TCP/IP u operacijski sustav UNIX i time je stvorena prva veza između operacijskog sustava UNIX (Sveučilište Berkley-BSD UNIX) i TCP/IP skupa protokola.
U vrijeme kad je TCP/IP postao standard počeo se pojavljivati termin Internet, a mreža ARPANET podijeljena je na dva dijela: MILNET (dio podatkovne mreže ministarstva obrane SAD) i manji ARPANET.
S vremenom Internet postaje dominantna svjetska računalna mreža koja povezuje skoro sve ostale mreže u svijetu.
TCP/IP skup protokola prihvaćen je kao standard zbog pogodnosti koje je jedini u danom trenutku nudio, neki od njih su:

- Neovisnost o tipu računalne opreme i operacijskih sustava, te o pojedinom proizvođaču
- Neovisnost o tipu mrežne opreme na fizičkoj razini i prijenosnog medija, što omogućava integraciju različitih tipova mreža (Ethernet, Token Ring, X.25...)
- Jedinstveni način adresiranja koji omogućava povezivanje i komunikaciju svih uređaja koji podržavaju TCP/IP
- Standardizirani protokoli viših razina komunikacijskog modela, što omogućava široku primjenu mrežnih usluga

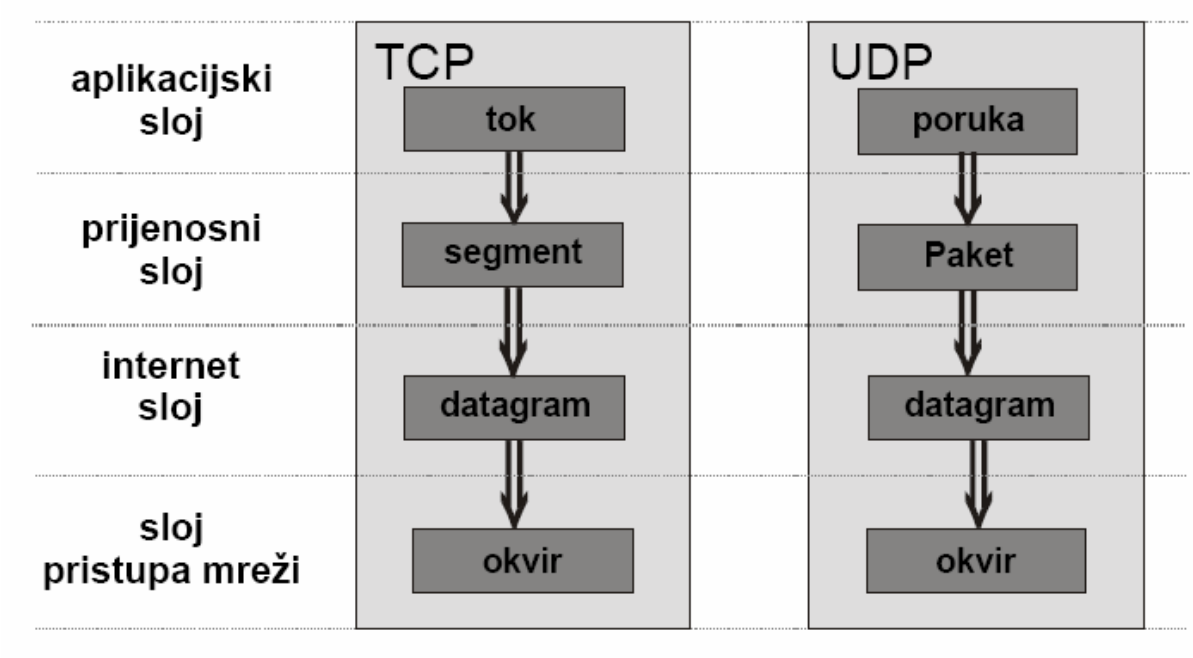
Arhitektura TCP/IP modela

Naziv TCP/IP potječe od dva najčešće korištena protokola: 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.

OSI referentni model	**TCP/IP referentni model**
Aplikacijski sloj	Aplikacijski sloj
Prezentacijski sloj	
Sjednički sloj	
Prijenosni sloj	Prijenosni sloj
Mrežni sloj	Internet sloj
Podatkovni sloj	Sloj mrežnog pristupa
Fizički sloj	

Tablica 1. Usporedba OSI i TCP/IP referentnih modela

Svaki sloj ima svoju strukturu podataka i terminologiju koja opisuje tu strukturu. Na aplikacijskom sloju TCP protokol za podatke koristi naziv tok (engl. *stream*), dok se kod UDP protokola koristi naziv poruka (engl. *message*). TCP na prijenosnom sloju naziva podatke segment, a UDP paket. Na internet sloju svi podaci su predstavljeni datagramom, a na sloju pristupa mreži okvirom.



Slika 1. Struktura podataka po slojevima TCP/IP modela

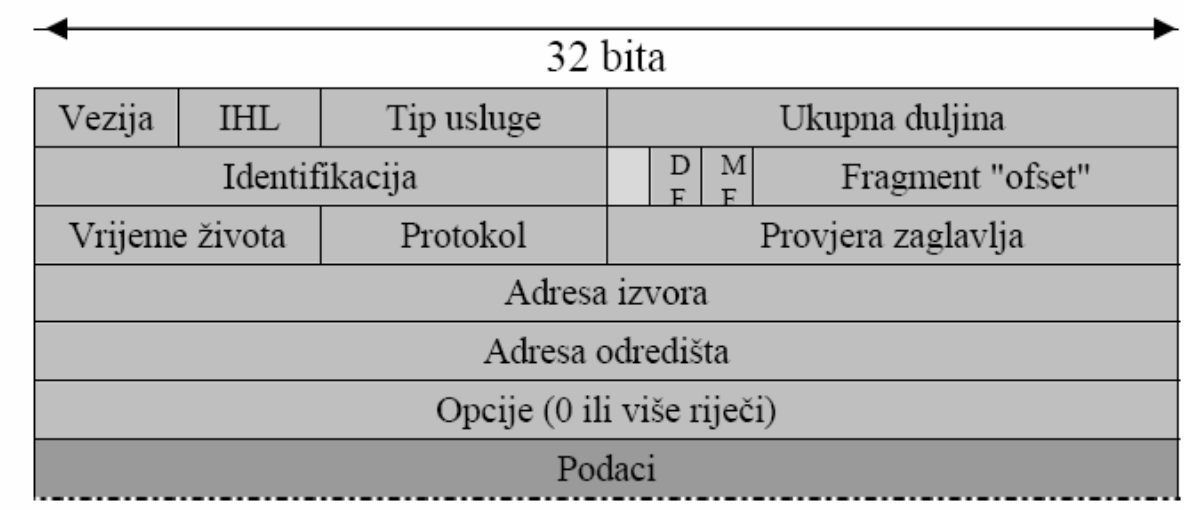
IP protokol

Internet protokol je najvažniji protokol unutar Internet sloja (TCP/IP model). IP je protokol za veze bez spajanja (engl. *connectionless protocol*), što znači da se dvije strane ne dogovaraju o početku ili završetku prijenosa podataka, nego predajna strana šalje podatke i ako nakon nekog vremena ne dobije potvrdu šalje podatke ponovo. IP znači ne razmjenjuje upravljačke podatke za uspostavu veze s kraja na kraj mreže, već se oslanja na protokole drugih slojeva koji trebaju uspostaviti vezu, ako žele da to bude veza sa spajanjem. IP se također oslanja na protokole viših i nižih slojeva za osiguravanje korekcije i detekcije pogreški, zbog čega se često naziva "nepouzdani protokol". IP će prenijeti podatke mrežom, ali neće provjeriti jesu li podaci točno preneseni, tu funkciju će obaviti protokoli ostalih slojeva u TCP/IP arhitekturi.
Funkcije Internet protokola:

- Definira datagram
- Definira shemu adresiranja na Internetu
- Prebacuje podatke između sloja za pristup mreži i prijenosnog (transportnog) sloja
- Vrši usmjeravanje datagrama do udaljenih računala

Datagram

Internet protokol definira paket pod nazivom datagram (slika 2.). Datagram je blok podataka koji se šalje na mrežu kao jedna poruka. Prvih pet ili šest 32-bitnih riječi u datagramu rezervirano je za upravljačke podatke (zaglavlje), a nakon zaglavlja slijede podaci. Zaglavlje sadrži sve elemente potrebne za predaju paketa (tip usluge, ukupnu duljinu, identifikaciju, zastavice, adresu izvora, adresu odredišta, ...). Polje verzija (engl. *version*) kaže koju verziju protokola koristi datagram. S obzirom da je duljina zaglavlja promjenljiva, u IHL (*Internet Header Length*) polju je naznačena duljina zaglavlja (pet ili šest riječi). U polju tip usluge (engl. *type of service*) host govori podmreži koju vrstu usluge želi (moguće su različite kombinacije pouzdanosti i brzine). Polje ukupna duljina (engl. *total length*) daje ukupnu duljinu datagrama (zaglavlje i podaci). Maksimalna duljina je 65535 bytova. Polje identifikacija (engl. *identification*) omogućava odredišnom hostu određivanje kojem datagramu pripada pristigli fragment[9]. Slijedi neiskorišteni bit, DF bit i MF bit. DF (Don't Fragment) bit naređuje usmjernicima da ne fragmentiraju datagram, jer ga odredište ne može složiti.
MF (More Fragments) bit imaju postavljen svi fragmenti osim zadnjeg kao znak da dolazi još fragmenata istog datagrama. Polje "ofset" fragmenta kaže gdje se u datagramu nalazi taj fragment. Polje vrijeme života paketa (engl. *time to live*) predstavlja brojač za ograničavanje životnog vijeka paketa. Smanjuje se pri svakom skoku i kad dosegne nulu paket se odbacuje. Ovo polje sprječava paket da kruži mrežom, što se može dogoditi ako se poremete tabele u routerima. Polje protokol govori mrežnom sloju koji će se protokol prijenosnog sloja koristiti. Polje za provjeru zaglavlja (engl. *header checksum*) provjerava samo zaglavlje. IP dostavlja datagram tako da čita adresu odredišta (peta riječ). Adresa odredišta je standardna 32-bitna IP adresa. Ako je adresa odredišta adresa u lokalnoj mreži paket se dostavlja direktno.
Ako adresa nije u lokalnoj mreži, paket se predaje usmjerniku za prijenos. Polje opcija (engl. *options*) služi za uključivanje informacija koje će biti potrebne u sljedećim verzijama protokola (trenutno je definirano pet opcija). Zatim slijedi polje sa podacima.



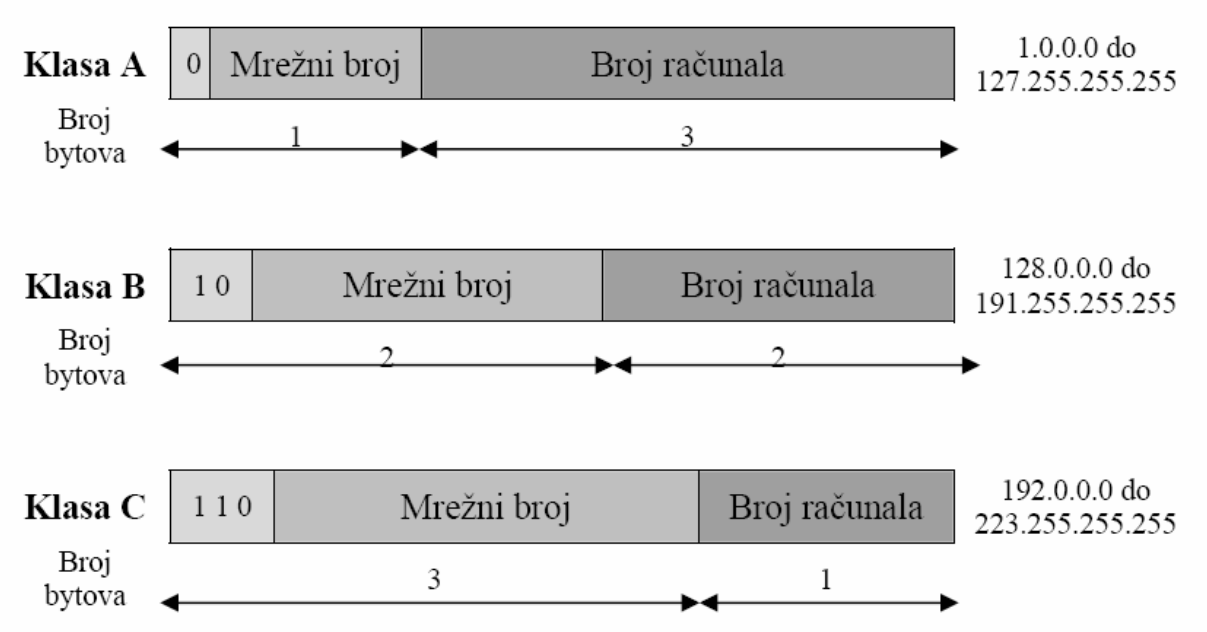
Slika 2. Struktura IP datagrama

IP adrese

Svako računalo i router na Internetu ima jedinstvenu IP adresu. IP adrese dodjeljuje NIC (Network Information Center).
IP adresa sastoji se od 32 bita tj. 4 byta (okteta), koji se kod zapisa odvajaju točkama (XXX.XXX.XXX.XXX). Svaki od 4 okteta zapisuje se decimalno (od 0 do 255), npr. heksadecimalna adresa C0290614 se piše kao 192.41.6.20. IP adresa ima dva dijela:

- mrežni broj (engl. *network number*) i
- broj hosta (engl. *host number*).

Na osnovu ukupnog broja računala u mreži, NIC dijeli mreže u klase:



Slika 3. Mrežne klase

Klasa A može imati otprilike 16 milijuna računala i njoj može pripadati do 126 mreža. Ova klasa je predviđena za mreže s velikim brojem računala.
Klasi B pripadaju mreže koje imaju do 65 536 računala, a takvih mreža može biti 16384.
Klasa C je najmanja i obuhvaća mreže koje imaju do 256 računala. U ovoj klasi može biti do 2 milijuna mreža.
Klasa D koja počinje sa 1110, a nakon toga slijedi adresa, koristi se za istovremeno pristupanje grupi računala (difuzija u grupi). Zauzima IP adrese od 224.0.0.0 do 239.255.255.255.
Klasa E koja započinje sa 11110 i zauzima adrese od 240.0.0.0 do 247.255.255.255 služi za buduće korištenje.

Neke adrese imaju posebnu namjenu, te se ne dodjeljuju određenom računalu na mreži. Adrese kod kojih mrežni broj ima posebno značenje:

- 0.0.0.0 se koristi kod podizanja računala tj. označava samog sebe
- IP adrese sa mrežnim brojem 0 označavaju računalo u istoj mreži
- IP adresa sa svim bitovima u 1 omogućava difuziju (engl. *broadcast*) tj. slanje svim računalima u lokalnoj mreži
- IP adresa sa određenim mrežnim brojem, a svim ostalim bitovima u 1, omogućava slanje paketa svim računalima u udaljenim lokalnim mrežama

- 127.xxx.yyy.zzz se uzima kao adresa povratne petlje (engl. *loopback*) i koristi se za provjeru rada računala u mreži, jer se podaci poslani na tu adresu vraćaju natrag istom računalu.

Adrese sa rezerviranim brojem računala:

- Adrese svih mrežnih klasa sa svim bitovima broja računala u 0 označavaju samu mrežu; npr. adresa 161.53.0.0 označava mrežu klase B 161.53 (CARNet)
- Adrese kod kojih su svi bitovi broja računala u 1, označavaju sva računala u mreži; npr. paket poslan na adresu 161.53.255.255 dostavlja se svim računalima u mreži 161.53
- Privatne adrese – 10.xxx.xxx.xxx, 172.16.xxx.xxx i 192.168.xxx.xxx; nazivaju se još i nerutabilnim adresama jer se ove adrese koriste na nivou pojedine ustanove koja ne raspolaže dovoljnim brojem IP adresa da svakom računalu dodijeli pojedinu tzv. javnu adresu. Uz privatne adrese obavezno se koristi i neki oblik „maskiranja", pri čemu jedno računalo (gateway, može biti i router) koristi dvije adrese – privatnu i javnu adresu, a sva računala (logički gledano) „ispod" njega imaju privatnu adresu. Na taj način sva računala su sa vanjskog dijela Interneta vidljiva isključivo kao jedno računalo sa jednom IP adresom (IP adresa gatewaya, routera ili sl.), stoga i naziv maskiranje.

IP protokol koristi mrežni dio IP adrese (mrežni broj), a puna se adresa gleda tek kad paket dođe na odredišnu mrežu. Kad IP datagram dođe do usmjernika gleda se adresa odredišta u tablici usmjeravanja. Ako je za udaljenu mrežu prosljeđuje se sljedećem usmjerniku, a ako je u lokalnoj mreži šalje se direktno na odredište. Ako se adresa ne nalazi u tablici usmjeravanja šalje se usmjerniku sa "većom" tablicom.
Podjela IP adrese na adresu mreže i adresu računala omogućila je efikasno administriranje adresa i usmjeravanje paketa. Međutim u praksi je velik broj adresa računala unutar dodjeljenog bloka ostao neiskorišten, jer je svaki korisnik uzimanjem jedne mrežne klase rezervirao veliki broj pojedinačnih IP adresa za svoje buduće potrebe. Problem se može riješiti na više načina:

- Dijeljenjem adresnog prostora neke klase na manje blokove primjenom mrežnih adresnih maski
- Ujedinjavanjem susjednih blokova neke klase u jednu veću klasu (C u B)
- Korištenjem skrivenih podmreža (intranet) s privatnim adresama
- Novom verzijom IP protokola, s adresom dovoljne duljine

Trenutno se još uvijek u većini mreža koristi IP verzije 4 (IPv4).

Mrežna maska

Primjenom mrežnih maski (engl. *subnet mask*) omogućeno je formiranje podklasa i podmreža unutar jedne dodjeljene mrežne klase. Na taj način se povećava broj mreža na račun broja računala.
Mrežna maska je 32-bitni broj koji kaže koje bitove originalne IP adrese treba promatrati kao bitove mrežnog broja. Ako je bit mrežne maske postavljen u 1 smatra se da taj bit pripada adresi mreže, svi ostali bitovi (koji su u 0) definiraju broj računala. Prema van se mreža još uvijek ponaša kao jedna iako je podijeljena.
Upotrebom maske usmjerivačke tablice se mijenjaju jer moraju sadržavati podatke o podmrežama. Router u podmreži mora znati kako doći do ostalih podmreža i računala u svojoj podmreži.
Svaki router mora napraviti logičku operaciju AND sa mrežnom maskom, kako bi dobio mrežni broj i potražio u tablici tu adresu.

IPv6

Problem IP načina adresiranja je u malom broju raspoloživih adresa, s obzirom na broj računala u Internetu i brzom širenju. Zbog nagle ekspanzije Interneta doći će do nedostatka IP adresa. 1990 g. IETF (Internet Engineering Task Force) započeo je rad na novoj verziji IP protokola u kojoj bi se riješili nedostaci iz IPv4.

Glavni ciljevi novog protokola su:

- Adrese za milijarde računala
- Smanjenje veličine usmjerivačkih tablica
- Pojednostavljenje protokola kako bi se routerima omogućio brži rad
- Bolja sigurnost
- Bolja podrška za servise pogotovo one koji rade u realnom vremenu
- Mogućnost da novi i stari protokoli rade zajedno

Od niza predloženih rješenja (RFC 1550) 1993. je prihvaćen SIPP (Simple Internet Protocol plus) i nazvan IPv6 (RFC 1883 – RFC 1887). Najvažnije prednosti IPv6 su:

- IPv6 ima adresu od 16 byta i na taj način osiguran je "neograničen" broj IP adresa.
- Pojednostavljeno zaglavlje, koje sadrži 7 polja (13 u IPv4). Kraće zaglavlje omogućava routerima da brže obrađuju pakete.
- Bolja podrška za opcije. Polja koja su u IPv4 bila obavezna sada više nisu, pa routeri mogu preskočiti opcije koje nisu njima namijenjene.
- Veliki napredak u sigurnosti. Autentikacija i privatnost su ključne osobine IPv6.
- Vodi se više računa o vrsti servisa. IPv4 ima 8-bitno polje za tip servisa, a IPv6 16 bitno polje.

Primjer IPv6 adrese: 3ffe:0501:0008:0000:0260:97ff:fe40:efab
Kako IPv6 adrese imaju 16 byteova, korištenjem IPv6 adresiranja imamo na raspolaganju 2^{128} adresa, ili približno $3x10^{38}$ adresa.

ICMP (Internet Control Message Protocol)

Usmjernici "prate" rad na Internetu. Kad dođe do neočekivane situacije ICMP prijavi događaj. Osnovna namjena ICMP protokola je osiguravanje nadzora i kontrole prijenosa podataka do odredišta, s obzirom da IP protokol to ne osigurava. ICMP šalje poruke koje osiguravaju kontolu toka, prijavu pogreške, pojavu alternativnog puta do odredišta i slično. Na ovaj način nije osiguran pouzdan prijenos podataka, već to treba osigurati protokol više razine. Svaka ICMP poruka je je "uokvirena" u IP datagram.

ARP (Address Resolution Protocol)

Iako svako računalo na Internetu ima IP adresu ona se ne može koristiti za slanje datagrama, jer uređaji na prijenosnom sloju ne razumiju IP adrese. Računala su priključena na LAN preko sučelja (mrežne kartice) koja razumiju samo LAN adrese (48-bitna adresa). Mrežne kartice primaju i šalju datagrame na osnovu 48 bitne LAN adrese i ne poznaju 32 bitnu IP adresu.
Svako računalo ima pokrenut ARP protokol, čiji je zadatak postavljanje pitanja i primanje odgovora. Kad računalo želi poslati podatke drugom računalu kreirat će datagram sa IP adresom računala u adresnom polju odredišta. Nakon toga potrebno saznati fizičku (LAN) adresu tog računala. Računalo koje želi slati podatke šalje ARP upit svim računalima (broadcast) u lokalnoj mreži, a stanica koja prepozna svoju IP adresu odaziva se ARP odgovorom, kojeg također primaju svi i koji sadrži fizičku adresu. Na taj način se povezuje IP adresa i fizička adresa, te omogućava slanje datagrama.