

1) IP adresa

Internet Protocol (IP) adresa jeste brojčana oznaka, kao na primer 192.0.2.1, koja je povezana na kompjutersku mrežu i koja koristi te protokole za komunikaciju. IP adresa ima 2 glavne funkcije: identifikacija u interfejsu mreže i adresiranje lokacije.

IPv4 (Internet Protocol version 4) definiše IP adresu kao 32-bitan broj. Zbog proširenja interneta i neizbežnog crpljenja IPv4 adresa, napravljen je novi standard u oznaci IPv6 koji koristi 128-bitne adrese.

Primer IPv4 (32-bitne) adrese:

172 . 16 . 254 . 1
↓ ↓ ↓ ↓
10101100 . 00010000 . 11111110 . 00000001

Ona se sastoji iz 4 bajta, maksimalni decimalni broj je 255 u svakom od bajtova ($2^8 = 256$), izmedju svakog bajta jeste tačka koja služi za razdvajanje. IP adrese se mogu prikazati, pored binarnog i decimalnog, u oktalnom i heksadecimalnom obliku.

2) Subnet maska

Svaki uređaj ima IP adresu sa 2 dela: klijent (ili host) adresa i server (ili mrežna) adresa. IP adrese se konfigurišu ili preko DHCP servera ili manuelno (statičke IP adrese). Subnet maska razdvaja IP adresu u host i mrežne ip adrese i tako definiše koji deo od ta dva pripada uređaju, a koji deo mreži.

Subnet maska je 32-bitan broj koji host bitove setuje na 0, a mrežne na 1.

255 se dodeljuje broadcast adresi, a 0 adresa je uvek dodeljena mrežnoj adresi. Ni 0, ni 255, se ne mogu dodeliti host-u jer je on definisan za specijalne uslove.

Subnet maske služe da smanje mrežni saobraćaj i da npr. omoguće organizacijama da prevaziđu limite LAN mreža (recimo maksimalni broj host-ova).

Internet mora da radi sa mrežama različitih veličina, napravljen je klasni sistem subnet maski postoe klase od A – E, sa tim da klasa D je rezervisana za multicasting, a klasa E se ne koristi na internetu pošto je ona rezervisana za IETF (Internet Engineering Task Force).

Klasa A je za mreže sa više od 65,536 hostova, klasa B za one koje imaju od 256 do 65,536, klasa C je za mreže sa manje od 254 hosta.

IP/Mask je skraćenica kada se misli na neku IP adresu i subnet masku koju ona koristi, pa tako imamo:

10.0.1.1 /24, ovo je isto kao:

IP ADRESA: 10.0.1.1, **SUBNET MASKA:** 255.255.255.0

3) MAC adresa mrežnog uređaja

Računari koji koriste neku mrežu ili internet moraju biti identifikovani. Zbog toga, mnoge konekcije kao što su fizičke (ethernet) ili Wi-Fi, koriste jedinstvene adrese za identifikovanje mrežne kartice, kojom uređaj pristupa internetu.

Ove adrese se nazivaju Media Access Control address ili MAC adresa.

Svakom uređaju se dodeljuje jedna MAC adresa od strane proizvodjača i to na takav način da postoji 2^{48} mogućih MAC adresa (48-bitne su) i one takodje identifikuju o kakvom uređaju je reč

4) Access liste

Access lista (ACL), lista pristupa, jeste skup pravila za kontrolisanje mrežnog saobraćaja i smanjenje napada na mreži. ACL se koriste da filteruju saobraćaj zavisno od tih pravila kojim se definiše ulazni i izlazni saobraćaj neke mreže.

Neka pravila ACL-a:

- Set pravila se gleda serijski, tj. podudaranje počinje od prve linije, pa druge itd.
- Paketi se proveravaju samo dok se podudaraju sa pravilom, jednom kad se podudare paket i pravilo onda će se to pravilo izvršiti (znači čim pravilo koje se prvo poklopi sa paketom će se i izvršiti)
- Ako se do kraja ne poklope paket i pravilo, onda će se taj paket odbaciti

Kada se neka ACL napravi onda ona može biti aplicirana ili na dolazeći ili na odlazeći interfejs.

Takodje postoje 2 tipa ACL zavisno od toga da li se koriste samo IP adrese prilikom pravljenja pravila, pa tako imamo:

Standard Access-list:

Ove liste koriste samo IP adrese i ove liste ne razlikuju IP saobraćaj kao što je npr TCP, UDP, HTTPS itd. Korišćenjem brojeva od 1-99 ili 1300-1999 ruter će razumeti da se radi o standardnoj access listi.

Extended Access-list:

Ove ACL koriste izvorni IP, IP destinacije, izvorni port i destinacioni port. Kada želimo da kažemo ruteru da se radi o EACL onda koristimo brojeve od 100-199 ili 2000-2699.

5) Klase adresa i njihov opseg

Internet mora da radi sa mrežama različitih veličina, napravljen je klasni sistem subnet maski postoji klase od A – E, sa tim da klasa D je rezervisana za multicasting, a klasa E se ne koristi na internetu pošto je ona rezervisana za IETF (Internet Engineering Task Force).

Klasa A: IP adresa koja počinje sa brojem izmedju 1 i 127 je klasa A.

Opseg je **1.0.0.0 – 126.255.255.255**

Klasa B: IP adresa koja počinje brojem izmedju 128 i 191 je klasa B.

Opseg je **128.0.0.0 – 191.255.255.255**

Klasa C: IP adresa koja počinje brojem izmedju 192 i 223 je klasa C.

Opseg je **192.0.0.0 – 223.255.255.255**

Klasa D i E: 224-239, 240-255

6) Klijent-server model

Klijent-server model je distribuirana aplikaciona struktura koja deli zadatke (workload) izmedju provajdera izvornih resursa usluga (**servera**) i onih koji te usluge traže (**klijenti**). Obično klijenti i serveri komuniciraju psihički odvojeni, ali može se takodje na ovaj način komunicirati na istom sistemu.

Server obično pokreće jedan ili više programa koji dele resurse sa klijentima. Klijenti obično ne dele svoje resurse – oni zatraže (request) sadržaj ili usluge sa servera. Klijenti, dakle, inicijaru komunikacijske sesije sa serverima, koji čekaju dolazeće zahteve. Primeri servisa koji koriste client-server model su e-mail, mrežni štampač, WWW.

7) Slojevita arhitektura mrežnog softvera TCP/IP

The internet protocol suite je set komunikacionih protokola koji se koriste na internetu ili sličnim kompjuterskim mrežama. Osnovni protokoli danas su Transmission Control Protocol (TCP) i Internet Protocol (IP), kao i User Datagram Protocol (UDP).

TCP/IP jeste kombinacija TCP i IP-a i radi na sledeći način: IP nalaže da podaci na internetu stignu na pravo mesto, onda TCP proverava da li su podaci poredjani na pravi način i da li neki nedostaje. TCP takođe pomaže da se saobraćaj na internetu ne preoptereti.

Ovi protokoli su dizajnirani tako da odredjeni programi (kao što su pretraživači ili e-mail klijent) mogu da ih koriste.

TCP je jako bitan jer omogućava kompjuterskim programima da komuniciraju jedni sa drugim, obično preko kompjuterske mreže.

Kada program želi da pošalje mnogo podataka, TCP služi da te podatke podeli, pošalje ih tako podeljene i onda ih sredi kako treba na drugom računaru. U tom procesu IP bira koji putevi su najpogodniji da se ti podaci pošalju. To radi pomoću paketa.

8) Koje su 2 osnovne funkcije ruter?

Ruter je računar čiji su softver i hardver dizajnirani da premeštaju podatke izmedju mreža. Ruter obezbeđuje da saobraćaj izmedju uredjaja ode tamo gde treba. Oni to postižu tako što biraju najkraći put izmedju uredjaja korišćenjem komplikovanog sistema pravila koji se nazivaju routing protocols. Ruteri obično sadrže OS, RAM, procesore, kao i više mrežnih interfejsa.

Ruteri takođe služe da se korisnik poveže na internet, prvi ruter na koji se računar poveže i umreži zove se default gateway. Tako iz gateawaya, ruter se šalje podatke ISP (Internet Service Provider) i odatle se povezuje sa ostalim ruterima i šalje neke podatke dokle trebaju da stignu.

Osnovne dve funkcije ruteru su, dakle: **povezivanje više IP mreža i određivanje najboljeg puta za slanje paketa.**

9) U rutingu tabeli postoje 3 tipa ruta. Nabrojati ih

Automatsko rutovanje, statičko (manuelno) rutovanje i dinamičko rutovanje

10) IEEE standard 802.11

IEEE 802.11 je serija protokola za bežično umrežavanje. Obično se nazivaju Wireless LAN, WLAN ili Wi-Fi. Takav protokol omogućava uredjajima, koji imaju potrebne komponente za bežično komuniciranje, medusobnu bežičnu komunikaciju.

Ima mnogo Wi-Fi standarda koji određuju specifikacije u pogledu brzine i na koju daljinu ih možete koristiti.

Prvi Wi-Fi standard je napravljen 1997. njegovo ime je 802.11 i omogućava komunikaciju 1-2 MBit/s. Danas taj standard je zastareo, pa se dodaju slova na njegovo ime, oni su označeni 802.11a do 802.11g, postoje planovi da se dodaju h, i, j, n, p i s. Svi su kompatibilni medusobno.

Noviji standardi imaju bitrate od 54 Mbit/s ali samo 40-50% je moguće iskoristiti u svakodnevnim situacijama.

Od 2007. najkorišćeniji standardi su g i b.

11) UDP protokol

UDP (User Datagram Protocol) je jedan od osnovnih protokola na internetu. Sa UDP kompjuterske aplikacije mogu da šalju poruke, koje se nazivaju datagrami, do drugih host-ova na IP mreži i prilikom tog slanja ne trebaju se uspostaviti specijalni kanali za prenos. UDP se takođe naziva Universal Datagram Protocol i napravljen je 1980.

UDP koristi datagram sokete da uspostavi host-to-host komunikaciju. Soketi služe kao završna tačka porta prenosa podataka. Port je softverska struktura koja se definiše pomoću njegovog 16-bitnog broja i tako postoje portovi od 0 do 65,535. Port 0 je rezervisan ali se može koristiti u slučaju kada se ne očekuje povratna poruka.

UDP protokol se danas koristi prilikom peer-to-peer komunikacije (npr Torrentovanje).

12) TCP protokol

TCP/IP jeste kombinacija TCP i IP-a i radi na sledeći način: IP nalaže da podaci na internetu stignu na pravo mesto, onda TCP proverava da li su podaci poredjani na pravi način i da li neki nedostaje. TCP takođe pomaže da se saobraćaj na internetu ne preoptereti.

Ovi protokoli su dizajnirani tako da odredjeni programi (kao što su pretraživači ili e-mail klijent) mogu da ih koriste.

TCP je jako bitan jer omogućava kompjuterskim programima da komuniciraju jedni sa drugim, obično preko kompjuterske mreže.

Kada program želi da pošalje mnogo podataka, TCP služi da te podatke podeli, pošalje ih tako podeljene i onda ih sredi kako treba na drugom računaru. U tom procesu IP bira koji putevi su najpogodniji da se ti podaci pošalju. To radi pomoću paketa.

13) NAT – Network Address Translation

U računarskom umrežavanju, NAT je tehnika modifikovanja informacija o adresi u zaglavljima IP paketa prilikom prenosa paketa kroz saobraćaj rutera. Takva tehnika korektuje prostor ip adrese u drugi adresni prostor. Ovo dozvoljava da više uređaja dele istu javnu IP adresu, što je postalo neophodno zbog nedovoljnog broja unikatnih IP adresa za svaki uređaj na svetu.

Danas, NAT se koristi za skrivanje mreže (network masquerading) ili za skrivanje IP (IP masquerading). To je mehanizam koji krije ceo adresni prostor, obično se sastoji od privatnih mreža adresa koje su iza jedne IP adrese koja je u javnom domenu adresnog prostora.

NAT mehanizam se implementuje u ruteru koji beleži stanje mrežnih konekcija. Ruter koristi tabele prevodjenja da mapira „sakrivenе“ adrese u jednu adresu i onda korektuje odlazeće IP pakete na izlazu tako da ispadne da su paketi poslati iz ruter-a. Prilikom primanja paketa ovaj proces se obrće korišćenjem istih tabela.

NAT se koristi samo u IPv4, jer IPv6 ima dovoljno ip adresa za svaki uređaj na svetu.

14) PAT – Port Address Translation

PAT je ekstenzija NAT-a i njegova osnovna funkcija je da podeli jednu javnu IP adresu izmedju više klijenata kojima treba internet.

Primer PAT-a jeste kućna mreža povezana na internet. Ruter ima svoju IP adresu, više korisnika može pristupiti internetu preko rutera i svakom korisniku se dodeljuje jedan port.

PAT se koristi da da unutrašnjim host-ovima pristup spoljašnjim host-ovima. Npr. prilikom pristupa preko LAN-a mnogi uređaji se povezuju na internet preko tog LAN rutera. Svaki klijent traži pristup internetu i svako je povezan na internet sa jednom IP adresom. Tako da PAT služi da svaki uređaj na LAN-u „sjedini“ u jednu javnu IP adresu.

Ruter onda šalje pakete preko te IP adrese, a prilikom primanja paketa on ih prosledjuje određenom portu (kome je taj paket i bio namenjen).

15) Statički i dinamički NAT

Statički NAT se podešava manuelno i mora se svaka privatna IP adresa mapirati ka javnoj IP adresi. Statički NAT je koristan kada mrežni uredjaj unutar privatne mreže treba biti dostupan preko interneta.

Dinamički NAT može se definisati kao mapiranje privatne adrese u jednu javnu IP adresu koja se bira iz NAT bazena javnih adresa. Dinamički NAT uspostavlja mapiranje između privatne i javne IP adrese. Ovde je IP adresa uzeta iz bazena adresa, to se konfiguriše na izlazu NAT rutera. Javno u privatno mapiranje zavisi od dostupnih adresa u NAT bazenu.

16) DNS – Domain Name System

Domain Name System (DNS) je sistem koji se koristi da pretvori računarski host name u IP adresu na internetu. Npr. ako uredjaj treba da komunicira sa web serverom *primer.com*, uredjaju treba IP adresu web servera *primer.com*. Posao DNS-a jeste da prevede ime host-a u IP adresu web servera. Ponekad se DNS naziva telefonski imenik interneta zato što prevodi ime veb sajta, koje ljudi znaju, u broj koji internet, u stvari, koristi.

Ime domena su napravljena od više delova, ili oznaka koje su spojene tačkom. Npr *www.primer.com*

- U ovom slučaju najveći nivo domena (Top Level Domain, TLD) je *.com*
- Subsekcija je *primer*
- Subdomen je *www*

Svaki deo može da ima 63 karaktera, i ime domena ne može da ima više od 253 karaktera.

Proces slanja:

1. PC pošalje DNS zahtev DNS serveru. Ovaj zahtev traži IP adresu servera
2. DNS server šalje DNS odgovor PC-u koji ima IP adresu servera
3. PC sada može da pošalje IP pakete IP adresi servera

17) Objasniti šta je administrativna distanca (kod rutiranja)

Administrativna distanca je vrednost koju ruteri koriste da bi izabrali najbolji put kada ima 2 ili više rute do iste odrednice. Administrativna distanca broji pouzdanost ruting protokola.

AD može da ima vrednost između 0 i 255, sa tim da je 0 najpouzdanija, dok je 255 najnepouzdanija.

18) Nabrojati dinamičke ruting protokole

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System to Intermediate System)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

20) Spanning tree algoritam

Spanning Tree Protocol (STP) je menadžment protokol koji daje putanje odbacivanja dok sprečava nepoželjne petlje u mreži. Kada se govori o Ethernet mrežama samo jedan aktivni put može postojati izmedju 2 stanice da bi mreža funkcionala kako treba. Petlje se mogu u mreži desiti iz mnogo razloga, najčešći razlog jeste kada u mreži postoji pokušaj višestrukog odbacivanja.

Spanning Tree omogućava samo jednostruku putanju ka odrednici kada imamo više povezivanja (kao u slučaju višestruko povezanih switcheva). Switchevi razmenjuju informacije između sebe korišćenjem Bridge Protocol Data Units (BPDU) i onda će „slušati“ sve svoje portove za poruku tog protokola. Kada se bridge upali, automatski stavlja da je ROOT BRIDGE u STP tree.

STP bira root bridge i računa sve putanje od sebe do sebe. U slučaju otkazivanja jednog root-a bira se novi.

21) SMTP

Simple Mail Transfer Protocol (SMTP) je komunikacioni protokol na internetu koji se koristi za slanje email poruka između email servera. On se ne koristi za uzimanje poruka sa servera. Za uzimanje poruka sa servera koristi se obično IMAP.

22) Šta je VPN?

Virtual Private Network (VPN) je set tehnologija koje služe za povezivanje računara koji kreiraju privatnu mrežu. Druga mreža se koristi za prenos podataka, koji su enkriptovani (šifrovani). Prenosna mreža će videti pakete podataka koje ona rutuje. Korisnicima VPN-a izgledaće kao da su uredjaji direktno povezani jedni sa drugim.

VPN garantuje:

- Da će mreža koja prenosi podatke te podatke preneti bez dekriptovanja
- Da će ljudi morati da identikuju sebe da bi koristili mrežu
- Kada se poruke šalju treba se obezbediti njihov integritet, tj da postoji način na koji će se proveriti da li se poruka promenila

VPN se obično koriste da povežu ljude iz drugih kancelarija, ili da omoguće nekom pristup nekoj mreži na daljinu.

VPN takođe nudi korisnicima anonimnost preko koje je teško pratiti nečiji rad na internetu, VPN se mogu koristiti da se gleda sadržaj koji je blokiran u nekoj zemlji, takođe mnogi ljudi ga koriste da bi se zaštitili dok koriste javni Wi-Fi.