

1. OSI model

OSI (Open Systems Interconnection) model je konceptualni model koji opisuje kako se komunikacija odvija preko mreže. Podjeljen je na sedam slojeva: 7. Application layer, 6. Presentation layer, 5. Session layer, 4. Transport layer, 3. Network layer, 2. Data link layer i 1. Physical layer. Application, Presentation i Session slojevi se nazivaju gornji slojevi, a ostala četiri donji slojevi.

Aplikacijski sloj pruža mrežne usluge korisničkim aplikacijama, te usluge su protokoli koji obrađuju podatke koje korisnik koristi, primjer takvog protokola je HTTP.

Prezentacijski sloj priprema podatke kako bi se mogli koristiti na aplikacijskom sloju, odgovoran je za prevođenje, enkripciju i kompresiju podataka.

Sloj sesije je odgovoran za otvaranje i zatvaranje komunikacije između dva uređaja, vrijeme između otvaranja i zatvaranja komunikacije se naziva sesija, sloj sesije osigurava da sesija ostane dovoljno dugo otvorena kako bi se svi podaci mogli razmjeniti i zatvara sesiju kako bi se spriječilo trošenje resursa.

Podaci dolaze s gornjih slojeva na transportni sloj, transportni sloj segmentira podatke na manje cjeline pošto se podaci ne mogu prenjeti u komadu jer su preveliki, set podataka na transportnom sloju se naziva segment. Transportni sloj zatim dodaje opisne podatke, među koje spadaju izvorišni i odredišni port koji predstavlja aplikaciju koja će primiti promet. Uloga transportnog sloja: multipleksiranje – praćenje pojedinih konekcija na računalu, segmentacija podataka za slanje i sastavljanje primljenih segmenata, identifikacija aplikacija pomoću portova, uspostava, održavanje i raskidanje privremene komunikacijske veze između dvije aplikacije na računalima koja komuniciraju. Protokoli transportnog sloja: TCP - transmission control protocol, zadužen za održavanje pouzdane komunikacije između dva računala; UDP – user datagram protocol, nepouzdan, prednost je što ima znatno manje opisnih podataka, koristi se za aplikacije koje se događaju u realnom vremenu poput video streama ili telefonskog poziva

Segment se spušta dalje na mrežni sloj, temeljna funkcija mrežnog sloja je prijenos podataka od ishodišta do odredišta, segmenti ili datagrami podataka s transportnog sloja se na mrežnom sloju pakiraju u pakete koji se prosljeđuju kroz mrežu prema odredištu, odredište je definirano IP adresom set podataka na mrežnom sloju se naziva paket, on dodaje svoje opisne podatke, među koje spadaju izvorišna i odredišna IP adresa.

Dalje se podaci prosljeđuju sloju podatkovne veze koji dodaje svoje opisne podatke, među koje spada izvorišna i odredišna MAC adresa, i od paketa tvori frame. Za razliku od transportnog i mrežnog sloja koji podatke dodaju samo na početak, takozvani header, sloj podatkovne veze dodaje podatke i na kraj, trailer.

Podaci zatim dolaze na fizički sloj gdje se pretvaraju u bitstream, električne impulse, svjetlosne signale, radiovalove, signale na žici.

2. Tipovi komunikacije

Vrste komunikacije u mreži su unicast, multicast i broadcast. Unicast je komunikacija jedan na jedan, primjer je ARP reply ili ping. Broadcast je komunikacija jedan na sve, zaustavlja se na uređajima trećeg sloja (router), primjer je ARP request, DHCP discover. Multicast je komunikacija jedan na grupu, uobičajeno se zaustavlja na uređajima trećeg sloja, osim ako ti uređaji nisu konfigurirani da propuštaju multicast promet, kao što je slučaj s IP TV prometom. Primjer je IP TV.

3. CMD commands

Ipconfig – prikazuje nam tablicu sa mrežnim postavkama, poput IP adrese, subnet maske, gatewaya, Mac adrese

Ipconfig/all – kao i ipconfig samo što pokazuje još dodatnih informacija o postavkama, na primjer DNS

Ipconfig /release – otkazivanje leasea adrese

Ipconfig /renew – ponovno traži IP adresu od DHCP poslužitelja

Tracert 8.8.8.8 – prikazuje putanju paketa do te IP adrese

Ping 8.8.8.8 – pinganje te IP adrese četiri puta

Ping -n 7 8.8.8.8 – pinganje tamo tu p adresu 7 puta

Arp -a – otkriva nam sve ARP zapise, veze između IP adrese i MAC adrese koje računalo poznaje

Arp -d briše sve dinamičke IP adrese s kojima je računalo komuniciralo

Netstat -a

Nslookup – za komunikaciju s DNS, možemo saznati koja je IP adresa neke domene
telnet

4. Tipovi medija za komunikaciju

UTP – Unshielded twisted pair, STP – shielded twisted pair; parični kabeli, kabel od 4 upletene parice, oklopljeni se koriste radi bolje otpornosti na smetnje. Svjetlovodno vlakno pruža vrlo malen otpor kretanju signala, dva tipa prema širini samog vlakna: MMF – višemodno vlakno za kratke udaljenosti i SMF – jednomodno vlakno za velike udaljenosti

5. Uloga preklopnika i usmjernika

Preklopnik radi sljedeće: Learning – popunjava MAC tablicu na temelju source Mac adrese, Aging – nakon što timer za neki zapis u MAC tablici istekne ta MAC adresa se miče iz MAC tablice, Flooding – ako switch ne zna gdje poslati neki frame, jer nema mac adresu u tablici, tada ga šalje na sve portove osim na onaj na koji je frame došao, Selective Forwarding – proces pregleda destination MAC adrese i prosljeđivanje na određeni port, Filtering – ne šalje frame na port koji ga je dobio, ako je frame neispravan odbacuje ga.

Usmjernici na temelju odredišne adrese mreže usmjeravaju pakete prema odredištu procesom koji zovemo usmjeravanje

6. Mala mreža sa 4 računala koja mogu komunicirati jedno s drugima i i maju pristup internetu

Imamo 4 računala povezana na switch, switch je spojen na router koji radi kao gateway i provodi NAT.

Recimo da PC1 ima postavke: IP adresa: 192.168.0.10; Subnet maska: 255.255.255.0, Gateway 192.168.5.1, DNS 8.8.8.8, MAC adresa 00:00:00:00:00:AA; a server IP adresa 69.63.176.13 i MAC adresa 00:00:00:00:00:DD.

Gateway ima IP adresu 198.162.5.1 i MAC adresu 00:00:00:00:00:AB

Ako idemo sa računala prema serveru, da bi promet mogao izaći iz lokalne mreže to mora poslati svom gatewayu za što mu treba MAC adresa gatewaya koju će saznati preko ARP protokola. Na gatewayu će se provesti NAT i privatna IP adresa će se prevesti u javnu IP adresu. U svakoj lokalnoj mreži će se koristiti mac adresa koja se mijenja kroz svaku lokalnu mrežu (LAN)

PC1 (src MAC: AA / dst MAC: AB / src IP: 198.162.0.10 / dst IP: 69.63.176.13)

Gateway na vanjskom sučelju (src MAC: BB / dst MAC: BC / src IP: 89.164.254.86 / dst IP: 69.63.176.13)

ISP 1 iz LAN 3 (src MAC: CC / dst MAC: DD / src IP: 89.164.254.86 / dst IP: 69.63.176.13)

Server (src MAC: CC / dst MAC: DD / src IP: 89.164.254.86 / dst IP: 69.63.176.13)

7. 3 way handshake

Prije nego aplikacije međusobno komuniciraju otrebno je uspostaviti TCP vezu, a taj proces se naziva 3-way handshake. 1. korak – računalo koje inicira komunikaciju šalje zahtjev za uspostavom veze, 2. korak server potvrđuje da je primio zahtjev od računala i šalje računalu formalni zahtjev za uspostavu veze, 3. korak zatim računalo koje je iniciralo komunikaciju potvrđuje da je veza uspostavljena. Uloga 3-way handshakea: utvrđuje da je odredišni uređaj prisutan u mreži, provjerava da odredišni uređaj zaista ima aktivan servis i da prihvaća zahtjeve za komunikacijom na određenom broju porta, obavještava odredišni uređaj da se klijent želi povezati na određeni port, pregovaranje, npr. window scaling opcija

8. DHCP

Dynamic Host Configuration Protocol, služi za automatsko, dinamičko konfiguriranje mrežnih postavki uređaja u mreži, među koje spadaju IP adresa, subnet maska, gateway, DNS.

Dodjela ip adrese prolazi u 4 koraka: 1. DHCP discover – broadcast poruka da nađemo poslužitelja, 2. DHCP offer – poslužitelj ponudi adresu (unicast na MAC), 3. DHCP request – klijent broadcasta prihvaćanje, 4. DHCP ack – poslužitelj potvrđuje davanje adrese

Koristi UDP za komunikaciju, portovi 67 i 68 za komunikaciju, klijent sluša na 68, poslužitelj na 67

9. ARP

Address Resolution Protocol je protokol koji služi za povezivanje IP adrese sa trećeg sloja s MAC adresom drugog sloja. ARP se koristi kako bi računalo saznalo MAC adresu drugog računala s kojim želi komunicirati. Funkcionira tako da računalo šalje ARP request, koji je broadcast, svim uređajima koji su spojeni na mrežu, a ono računalo koje se prepozna će odgovoriti ARP replyom koji je unicast.

10. DNS

Za svaku domenu su definirani DNS poslužitelji koji imaju mapiranje IP <-> FQDN, svaki poslužitelj ne zna podatke o svakom računalu ali zna koga pitati

Domin Name System, mehanizam mapiranja IP adresa uređaja u mreži s imenima koja ljudi lakše pamte. Svako računalo mora imati konfiguriran DNS.

DNS sustav je hijerarhijski model koji je zapravo distribuirana baza podataka s delegiranim odgovornostima za pojedinu domenu.

DNS radi i: anti-phishing, anti spam, privatnost, dns otkriva vanjskim korisnicima samo ono što mi želimo da se javno vidi

11. NAT mehanizam

Ako računalo iz privatne mreže želi komunicirati s uređajem na javnoj mreži mora proći kroz uređaj koji obavlja funkcije NAT-a i PAT-a

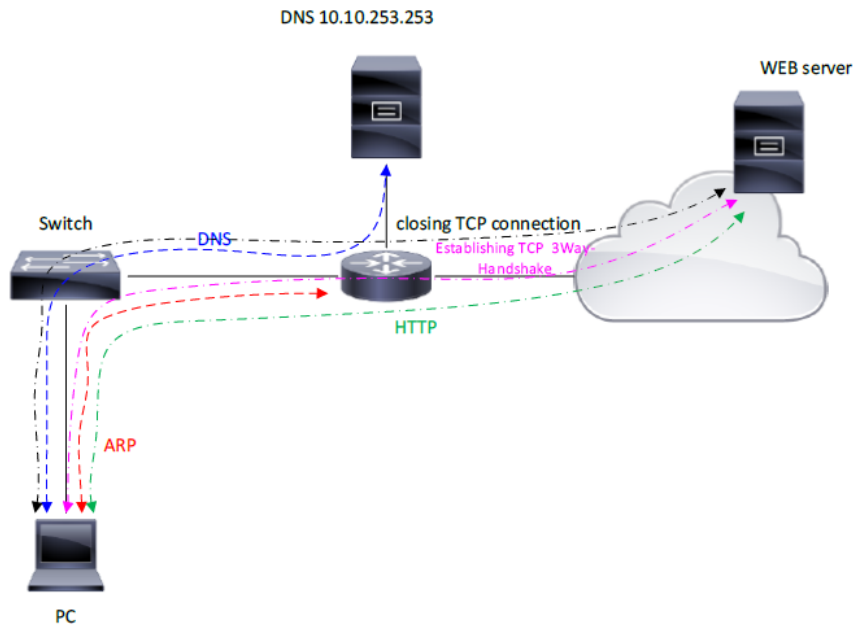
Network Address Translation je mehanizam koji prevodi jednu IP adresu u drugu IP adresu, najčešće se koristi za prevođenje privatnih IP adresa u javno dostupne IP adrese i obratno.

Dobre strane NAT-a: možemo samostalno upravljati vlastitim adresnim prostorom unutar naše organizacije, kojeg se izvana ne može vidjeti; lako razdvajamo lokalni od vanjskog prometa; NAT/PAT uređaj je najčešće uparen s vatrozidom te pruža dodatnu sigurnost našoj privatnoj mreži

Loše strane NAT-a: smanjuje performanse; neke aplikacije ne rade preko NAT-a i ne trpe promjenu IP adrese; otežava rješavanje problema u mreži

Što ne radi dobro kroz NAT: console gaming, video streaming, peer to peer, geo location

1. Dokumentirajte (opisi i wireshark capture s oznakama kao dokazi) sve faze u uspostavi, održavanju i raskidanju komunikacije između vašeg računala i web servera <https://www.freelancer.com> (svi protokoli na slici)



1.korak: ARP

Moje računalo kreiralo je DNS upit kako bi saznalo IP adresu web stranice s obzirom da DNS server nije u lokalnoj mreži moje računalo mora komunicirati s Gatewayom kako bi moglo izvršiti moje računalo je pokrenulo ARP request u kojemu traži MAC adresu gatewaya, kad smo zaprimili odgovor MAC adresu smo pohranili u ARP tablicu.

2. korak : DNS

Sada je moje računalo spremno poslati DNS upit prema DNS serveru. U upitu tražim IP adresu web stranice. Dobiveni odgovor moje računalo pohranjuje u DNS cache

3. korak: TCP

Tek sada je moje računalo spremno uspostaviti logičku vezu s web serverom, pomoću 3 way handshake mehanizma moje računalo uspostavlja pouzdanu vezu s web stranicom

4. korak: HTTP

Konačno u zadnjem koraku moje računalo pomoću http protokola dohvaća web stranicu i prikazuje ju mojem web pregledniku