Napredno korištenje operacijskog sustava Linux

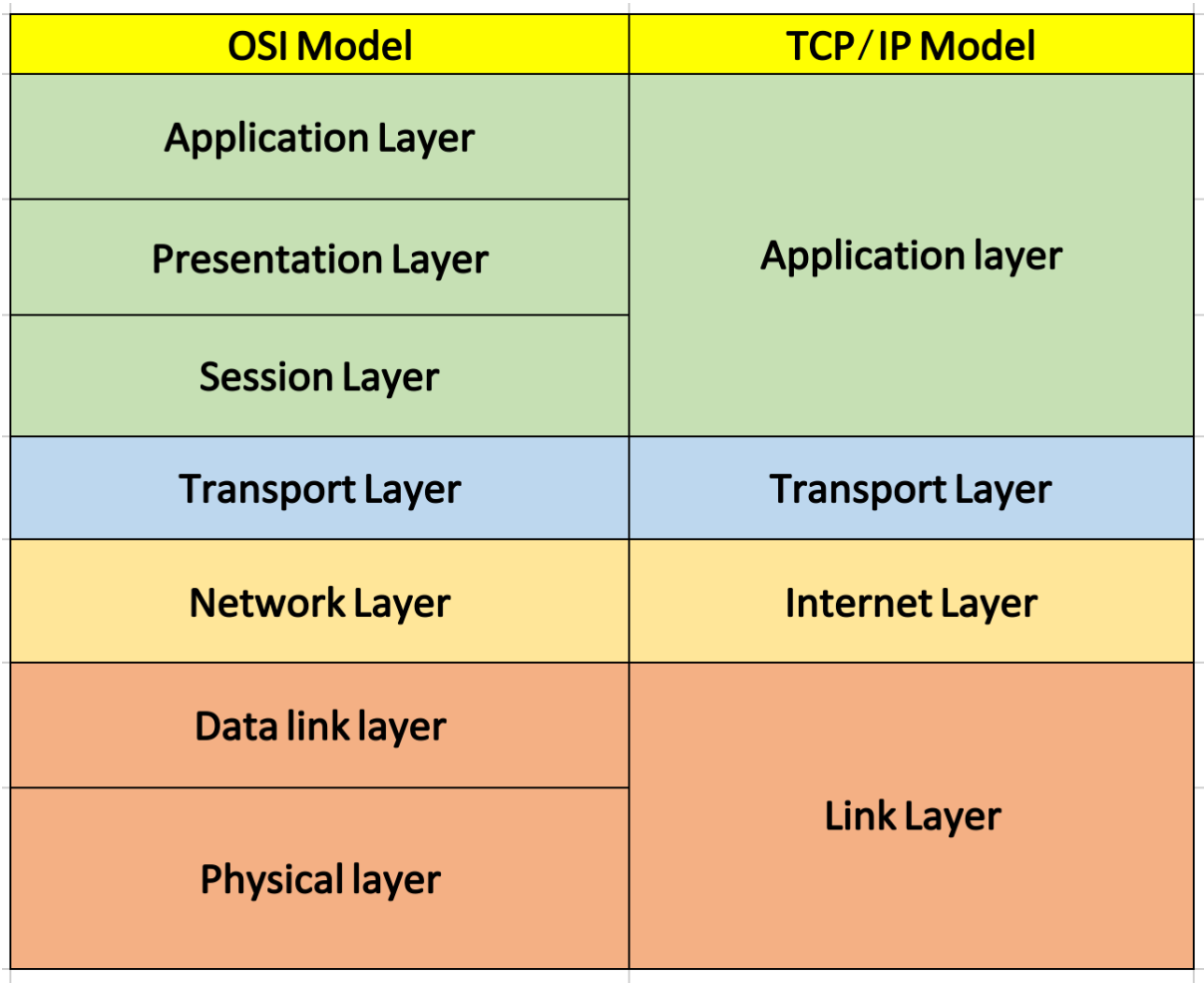
Skripta za predavanje mreže, protokoli i web poslužitelji

Tin Komerički
Nositelj: doc. dr. sc. Stjepan Groš
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

31. ožujka 2020.

UVOD

Komunikacijsku mrežu čine međusobno povezani komunikacijski sustavi na koje se spaja korisnička oprema (komunikacijska, računalna) i druga oprema potrebna za pružanje informacijskih i komunikacijskih usluga te potporu aplikacija korisnicima (poslužiteljska računala i drugi sustavi).[1]
Mrežu možemo podijeliti vertikalno po slojevima ovisno o funkciji koju svaki sloj izvodi. Spomenuti ćemo dva modela podjele: OSI i TCP/IP.



Slika 1 Slojevi prema OSI i TCP/IP modelima[2]

Kako se krećemo iz nižeg sloja u viši, tako razina apstrakcije raste. Za potrebe NKOSL-a nećemo se zamarati načinom rada slojeva, već ćemo opisati neke elemente pojedinih slojeva koji su važni za razumijevanje gradiva na predavanjima, ali i za daljnje samostalno istraživanje. O ulogama i načinu rada pojedinih slojeva govori se na kolegiju Komunikacijske mreže.

MAC adresa

MAC adresa (engl. Media Access Control address) je jedinstvena adresa svakog mrežnog uređaja. Sastoji se od 48 bitova koji se zapisuju u heksadekadskoj notaciji (npr. 08:00:20:4C:D3:E5). Prva 3 okteta predstavljaju jednoznačni identifikator proizvođača tog uređaja (OUI), dok druga 3 okteta predstavljaju identifikator mrežnog sučelja (NIC). MAC adresom možemo direktno adresirati uređaj koji želimo koristiti u komunikaciji.

IP adresa

IP adresa je logička adresa koju sudionici u komunikaciji koriste kako bi identificirali sebe i druge uređaje na mreži. Prilikom priključivanja uređaja na mrežu, tom uređaju se IP adresa može dodijeliti:

- Statički
- Dinamički

Ovisno o duljini postoje IPv4 i IPv6 adrese. IPv4 adresa koristi 32-bitni zapis, a IPv6 128-bitni. U zapisu IPv4 adrese bitovi se grupiraju u oktete koji se prikazuju dekadskim ekvivalentom te se odvajaju točkom. IPv6 se zapisuje heksadekadskim znamenkama koje se grupiraju u 8 grupa od po 4 heksadekadske znamenke i odvajaju dvotočkom.
Primjeri:

- 192.168.205.74 - IPv4 adresa
- 0000:0000:0000:0000:0000:ffff:c0a8:cd4a - IPv6 adresa

IPv6 adresa počela se koristiti zato što IPv4 adresa (koja može adresirati 2^{32} = 4.294.967.296 uređaja) ne može pratiti konstantan rast broja uređaja koji pristupaju Internetu te je jednostavno potreban veći adresni prostor, što IPv6 osigurava.

Svaka IP adresa sastoji se od identifikatora mreže (Net ID) i identifikatora krajnjeg uređaja (Host ID). Ovu podjelu je najlakše objasniti na primjeru. Ako je na vašoj kućnoj mreži povezano nekoliko uređaja, njihove IPv4 adrese mogle bi izgledati npr. ovako:

- 192.168.104.129
- 192.168.88.131
- 192.168.103.10

Drugim riječima, IP adresa u nekoj podmreži (engl. subnet) kao što su kućanstvo, tvrtka, kafić i sl., sastoji se od fiksnog identifikatora mreže i varijabilnog ostatka što je zapravo identifikator krajnjeg uređaja. Identifikator mreže u CIDR notaciji za ovaj primjer glasi: 192.168.64.0/18
Broj desno od '/' označava broj bitova počevši od najvećeg po veličini koji tvore identifikator mreže. Preostali bitovi se nužno postavljaju u 0 (zadnjih 14 bitova je 0). Taj broj nam također omogućava modeliranje subnet maske i to tako da (ovom slučaju) 18 najvećih bitova postavimo u 1, a preostalih 14 u 0.

	Identifikator mreže	Subnet maska
Dekadski zapis	192.168.64.0/18	255.255.192.0
Binarni zapis	11000000.10101000.01000000.00000000	11111111.11111111.11000000.00000000

Ovo možemo protumačiti i na sljedeći način: 2 su uređaja u ovoj podmreži ako im IPv4 adresa izgleda ovako: 11000000.10101000.01******.********, odnosno ako joj je prvih 18 bitova točno gore navedenih vrijednosti, dok je preostalih 14 bitova proizvoljne vrijednosti, iz čega slijedi da uređaj u ovoj mreži može imati IPv4 adresu u rasponu 192.168.64.0 – 192.168.127.255.

Postoje IP adrese koje su rezervirane za posebne namjene, kao što su adrese za lokalnu mrežu, broadcast adrese, adresa za vlastiti uređaj i sl. U tablici je popis IPv4 rezerviranih adresa[3]. U tablici su vidljiva 3 identifikatora mreže koji služe za lokalnu komunikaciju unutar privatne mreže, ovisno o tome koliko se uređaja nalazi u privatnoj mreži (192.168.0.0/16 za "male" mreže, 10.0.0.0/8 za server sobe i sl.).

Address block	Description
0.0.0.0/8	Current network (only valid as source address).
10.0.0.0/8	Used for local communications within a private network.
100.64.0.0/10	Shared address space for communications between a service provider and its subscribers when using a carrier-grade NAT.
127.0.0.0/8	Used for loopback addresses to the local host.
169.254.0.0/16	Used for link-local addresses between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server.
172.16.0.0/12	Used for local communications within a private network.
192.0.0.0/24	IETF Protocol Assignments.
192.0.2.0/24	Assigned as TEST-NET-1, documentation and examples.
192.88.99.0/24	Reserved. Formerly used for IPv6 to IPv4 relay (included IPv6 address block 2002::/16).
192.168.0.0/16	Used for local communications within a private network.
198.18.0.0/15	Used for benchmark testing of inter-network communications between two separate subnets.
198.51.100.0/24	Assigned as TEST-NET-2, documentation and examples.
203.0.113.0/24	Assigned as TEST-NET-3, documentation and examples.
224.0.0.0/4	In use for IP multicast. (Former Class D network).
240.0.0.0/4	Reserved for future use. (Former Class E network).
255.255.255.255/32	Reserved for the "limited broadcast" destination address.

ARP

IP i MAC adresama komuniciraju različiti slojevi. U OSI referentnom sustavu IP adrese koristi Network Layer (komunikacija preko više uređaja), dok MAC adrese koristi Data Link Layer (samo izravna komunikacija 2 povezana uređaja). Tako na primjer mrežna kartica prepoznaje samo MAC adrese, što znači da kako bi ostvarili komunikaciju internetom moramo ostvariti vezu između IP i MAC adrese. Upravo to radi ARP protokol. U sklopu protokola uređaji rukuju ARP spremnikom u kojem se nalaze parovi IP - MAC adresa susjednih uređaja. Ukoliko za neku IP adresu s kojom radimo nemamo uparenu MAC adresu možemo ju saznati kroz nekoliko koraka:

- Izvorišni uređaj šalje ARP zahtjev (broadcast svim uređajima s kojima je neposredno povezan) u kojem traži da mu uređaj sa IP adresom koju izvor zna javi svoju MAC adresu
- samo traženi uređaj mu vraća odgovor koja je njegova MAC adresa
- Oba uređaja ažuriraju svoje ARP tablice jer sad oba uređaja znaju jedan za drugoga

DNS

DNS (engl. Domain Name System) se može opisati kao „imenikom Interneta“. Njegova najčešća uporaba je pridruživanje IP adrese lako pamtljivom imenu računala, tako na primjer imenu www.fer.hr DNS pridružuje 161.53.72.119. To znači da korisnici ne moraju pamtiti IP adrese uređaja s kojima žele komunicirati, nego simboličko ime. DNS također omogućava stvaranje svojevrsne hijerarhije umreženih računala grupiranjem skupine uređaja u domene (domene su .hr, .us, .de, .ru, …). Ako poznajemo simboličko ime računala možemo saznati njegovu IP adresu putem DHCP-a (više o tome na predmetu Komunikacijske mreže).

Routing table

Zamislimo jednu veću tvrtku u kojoj svaki kat ima vlastiti router na koji su priključeni svi uređaji tog kata te koji je povezan s routerima na susjednim katovima (npr. router na 2. katu je povezan s routerom na 3. i na 1. katu) te koji je povezan na router koji tvrtku povezuje s ostatkom interneta. Kada radnik tvrtke na svom računalu šalje npr. mail, on se prosljeđuje routeru na tom katu koji mora na osnovu adrese primatelja odrediti kome će dalje proslijediti mail kako bi osigurao da on stigne na odredište. Ovdje nastupa tablica usmjeravanja (engl. routing table). U njoj se nalaze podaci potrebni da se jedinstveno odredi daljnje prosljeđivanje svakog paketa koji pristigne na taj uređaj. Na slici je prikaz jedne takve tablice koju dohvaćamo naredbom *route -n*.

```
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.0.0.0        192.168.1.2     255.0.0.0       UG    1      0        0 eth0
0.0.0.0         192.168.1.10    0.0.0.0         UG    0      0        0 eth0
```

Slika 2 Routing table

Destination predstavlja adresu mreže odredišta definiranu maskom *Genmask*, a *Gateway* definira na koji izlaz iz uređaja da se paket proslijedi.

PORT

Vrata (engl. port) krajnja su točka komunikacije jednog uređaja. IP adresa i port zajedno jednoznačno određuju servis na uređaju kojem se pristupa. Port je broj u rasponu 0-65535. Neki portovi su rezervirani za neke web usluge – ti portovi se zovu „dobro poznati“ portovi. Važno je napomenuti da se „dobro poznati“ portovi ne moraju nužno koristiti.

Port Number	Transport Protocol	Service Name	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

Slika 3 Tablica "dobro poznatih" portova[4]

NAT

Network Address Translation je izvorno uveden zbog nedostatka IP-adresa u IPv4 zapisu. NAT prevodi privatne IP adrese uređaja jedne (pod)mreže u jednu ili nekoliko javnih IP-adresa koje će se zapravo koristiti za komunikaciju s Internetom. Komunikacija će se odvijati koristeći javnu IP adresu, a uređaj koji je izveo prevođenje adrese će u svoju NAT tablicu pohraniti par privatna-javna IP adresa. Kada paket pristigne na javnu adresu uređaj koji je izveo prevođenje će iz tablice iščitati privatnu IP adresu i nastaviti prosljeđivanje paketa prema tom uređaju.

Dodatno, moguće je prevesti i port uređaja koji se koristi (tada govorimo o NAT-u s pretvaranjem portova). Tada se u NAT tablicu pohranjuju par privatna IP adresa i port - javna IP adresa i port s čime onda može postojati samo jedna javna IP adresa dok je razlika samo u dodijeljenom javnom portu.

Koristeći NAT štedi se adresni prostor i povećava sigurnost jer privatna adresa nije poznata izvan (pod)mreže u kojoj se uređaj nalazi i jer se sama (pod)mreža odvaja od Interneta.

Transportni protokoli

Govorit ćemo o 2 transportna protokola: TCP i UDP.
TCP (engl. Transmission Control Protocol) je spojno-orijentirani, pouzdani internetski protokol. TCP omogućuje dvosmjerni transport kontinuiranog niza podataka. Postoje brojni mehanizmi koji osiguravaju pouzdanost prijenosa kao što su detekcija pogrešaka i potvrđivanje primitka podataka. TCP vezu definiraju 4 podatka:

- IP adresa izvora
- Port izvora
- IP adresa odredišta
- Port odredišta

TCP koristimo:

- Kada nam je važan redoslijed kojim podaci pristižu
- Kada je najvažnija pouzdanost (ne želimo izgubiti niti jedan podatak)
- Kada izvodimo dulje komunikacije između dva uređaja
- Neki primjeri: transfer datoteka, elektronička pošta, transakcijske primjene, rad na udaljenom računalu i sl.

UDP (engl. User Datagram Protocol) je jednostavan transportni protokol koji prenosi podatke od izvora prema odredištu uz minimalne dodatne funkcionalnosti. Zbog toga, prijenos podataka nije pouzdan, nema očuvanja redoslijeda podataka, nema uspostave veze ni kontrole toka (ako pošiljatelj prebrzo šalje podatke, oni se gube). Iako iz ovoga slijedi da je TCP superioran u svakom pogledu, UDP i dalje ima prednost u brzini prijenosa, upravo zato što ne koristi mehanizme pouzdanosti i uspostavljanje veze.

Zbog toga, UDP se koristi:

- Kada je brzina prijenosa važnija od dostave svih podataka (npr. video ili audio poziv, višekorisničke igre i sl.)
- Kod kratkih komunikacija gdje uspostava veze daleko nadmašuje trajanje komunikacije (brzi request/response, DNS i DHCP upiti)

HTTP(S)

HTTP(S) (engl. Hypertext Transfer Protocol (Secure)) je aplikacijski protokol čija je glavna zadaća prijenos poruka na najvišoj razini apstrakcije. HTTP definira format poruke i način razmjene poruka. Poruke se dijele na zahtjev (request) i odgovor (response). Postoji 5 kategorija ishoda odgovora, ovisno o kodu koji je vraćen (popularni error 404 jedan je od tih ishoda):

- 1xx – informativna poruka
- 2xx – uspjeh
- 3xx – preusmjeravanje
- 4xx – greška na klijentu (pošiljatelju)
- 5xx – greška na poslužitelju

HTTPS je sigurnija varijanta komunikacije koja koristi enkripciju sadržaja pri komunikaciji.
Za komunikaciju ovim protokolom koristi se TCP transportni protokol, s time da je za HTTP dobro poznati port 80, a za HTTPS 443.

SSH

SSH (engl. Secure Shell) je mrežni protokol koji osigurava sigurnu komunikaciju između 2 procesa koja se često nalaze na 2 različita, udaljena poslužitelja. Sigurna komunikacija postiže se simetričnom enkripcijom podataka i pristupom udaljenom poslužitelju koristeći lozinku. SSH se koristi za:

- Sigurni pristup korisnicima i automatiziranim procesima udaljenom poslužitelju
- Prijenos datoteka
- Izvođenje naredbi na daljinu i dr.

SSH koristi TCP transportni protokol s dobro poznatim portom 22. Daljnje povećanje sigurnosti može se postići korištenjem nekog drugog porta umjesto standardnog te korištenjem autentifikacije asimetričnim parom ključeva umjesto lozinkom.

VPN

VPN (engl. Virtual Private Network) je mrežna tehnologija koja omogućuje povećanu sigurnost prilikom pristupanja i rada unutar privatne mreže. To se postiže kriptiranjem veze između korisnika i privatne mreže.
Korisnik koji je priključen na VPN ima direktan pristup podacima unutar te mreže, no moguće je omogućiti i pristup vanjskim resursima. U tom slučaju VPN dohvaća rezultat pretrage za nas te izvana izgleda kao da je sav mrežni promet napravila ta privatna mreža. To znači da privatni podaci nisu javno dostupni prilikom pretraživanja nikome osim VPN-u.
Postoje i neki nedostaci VPN-a kod korištenja za dohvat vanjskih resursa. Zbog posrednog pretraživanja Interneta, brzina prijenosa podataka opada. Ovisno o pružatelju VPN usluge, neke VPN bilježe online aktivnost korisnika, povijest pretrage i sl. što znači da korištenje VPN-a ne mora biti potpuno anonimno.

Izvori:

[1] Prezentacije s predmeta „Komunikacijske mreže“, 2018./2019.
[2] http://mhshohag.com/compare-and-contrast-osi-and-tcp-ip-models/
[3] https://en.wikipedia.org/wiki/Reserved_IP_addresses
[4] https://ipwithease.com/common-tcp-ip-well-known-port-numbers/

Korisni linkovi:

https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking
https://en.ryte.com/wiki/IP_Address
https://www.domain.com/blog/2018/12/20/what-is-an-ip-address/
https://www.lifewire.com/internet-protocol-tutorial-subnets-818378
https://whatismyipaddress.com/subnet
https://www.avalon.hr/blog/2011/12/20/kako-radi-dns-i-zasto-je-toliko-vazan/
https://www.grandmetric.com/2018/01/20/how-does-routing-table-work/
https://whatismyipaddress.com/nat
https://whatismyipaddress.com/mac-address
https://whatismyipaddress.com/port
https://www.ssh.com/ssh/protocol/
https://www.nginx.com/resources/wiki/
https://hr.vpnmentor.com/blog/sve-o-vpn-ovima-vpnmentorov-vodic-kroz-vpn-ove-za-pocetnike/