Operativni Sistemi i računarstvo u oblaku

II Semestar – 2023/24 – Vježbe

Sedmica 6

Handout za Vježbe

Agenda:

Linux Networking-Linux mrežna administracija

- Historijat mrežne administracije
- Mrežna administracija u Linux okruženju
    - MAC adrese
    - IP adresiranje
    - DHCP
    - DNS
- Osnovne naredbe za mrežnu administraciju

Historijat računarskog umrežavanja

Historijat moderne tehnologije računarskog umrežavanja seže u 1969. godinu, kada je ARPANET (Advanced Research Projects Agency Network) postao prva povezana računarska mreža implementirajući paket TCP/IP protokola, koji je kasnije postao Internet.

ARPANET je razvila Agencija za napredne istraživačke projekte (ARPA) kao podorganizavija Ministarstva odbrane SAD-a zbog vođenja hladnog rata. Umrežavanje je omogućeno s FDDI (eng. Fiber Distributed Data Interface) ili sučeljima distribuiranih podataka sa optičkim vlaknima za prijenos podataka u LAN-u nudeći brzine do 100 Mbit/s.

Nakon toga se dolazi do uspona Etherneta kojeg je 1973. godine razvio Bob Metcalfe u Xerox PARC-u, a patentiran je tek 1975. Otvoreni Ethernet standard je trajao još pet godina, a standardiziran je 1983. kao IEEE 802.3. Prvi Ethernet sistem koristio je koaksijalni kabl kao zajednički medij, a počeo je sa brzinama od **2,94 Mbit/s**.

Vremenom je Ethernet prešao na veze sa paricama ili optičkim vlaknima, kao i na prekidače, omogućavajući mu povećanje brzine, koja trenutno iznosi nevjerovatnih **40 Gb/s.**

Ethernet je ponudio jeftiniju alternativu mnogim prethodnim mrežnim standardima, posebno jer se prilagodio novim tipovima kablova kao što su kablovi sa optičkim vlaknima. Ostali standardi bili su ograničeni na vrste kablova koje su mogli koristiti. Budući da je Ethernet radio na protokolu otvorenog koda za razliku od vlasničkog protokola, bio je lakši za implementirati. Ethernet je sada relativno sveprisutan i smatra se jednom od glavnih komponenti Interneta kakvog poznajemo.

Budući da je Ethernet protokol, a ne vrsta kabla, postoji mnogo različitih vrsta Ethernet kablova. Možete odabrati verziju sa optičkim vlaknima za umrežavanje na velikim udaljenostima. Ako vam je potrebno napajanje preko Etherneta (PoE-Power over Ethernet), onda je potreban bakar. Zanimljivo je znati da 95% podataka cijelog interneta danas pristupa se podmorskim vezama (kablovi, bežični, satelitski).

Linux mrežna administracija

Vjerovatno najzanimljiviji rad s Linuxom je umrežavanje i mrežna administracija. Neke osnove koje se trebaju poznavati su sljedeće:

- Različite vrste mrežnih sučelja u Linuxu
- Kako konfigurisati IP adresiranje
- Alati koji su dostupni u Linuxu za rješavanje problema s umrežavanjem
- Kako spojiti više mrežnih sučelja/interfejsa zajedno.

Različite verzije Linuxa mogu različito imenovati mrežna sučelja. Općenito, skoro svi Linux operativni sistemi će imati najmanje dva mrežna sučelja, a to su:

- **Loopback**. Interfejs loopback (lo) s IP adresom 127.0.0.1, koji predstavlja samog hosta. Pretpostavimo da želite otvorite web stranicu koja radi na istom Linux serveru na kojem se nalazite. Možete otvoriti http://127.0.0.1 u svom web pretraživaču. Ta IP adresa neće biti dostupna preko mreže.
- **Eternet**. Ethernet 0 (eth0) sučelje je obično veza s lokalnom mrežom. Čak i ako koristite Linux na virtuelnoj mašini (VM), i dalje ćete imati eth0 interfejs koji se povezuje sa fizičkim mrežnim interfejsom hosta. Najčešće biste trebali osigurati da je eth0 u UP stanju i da ima IP adresu tako da možete komunicirati s lokalnom mrežom i vjerovatno preko Interneta.

Linux naredba za konfiguriranje mrežnih sučelja/uređaja/veza (koji god termin koristite) je **ip link** koja bez dodatnih opcija komande pokazuje dva različita sučelja, njihov status i njihove MAC adrese povezane sa svakim od njih:

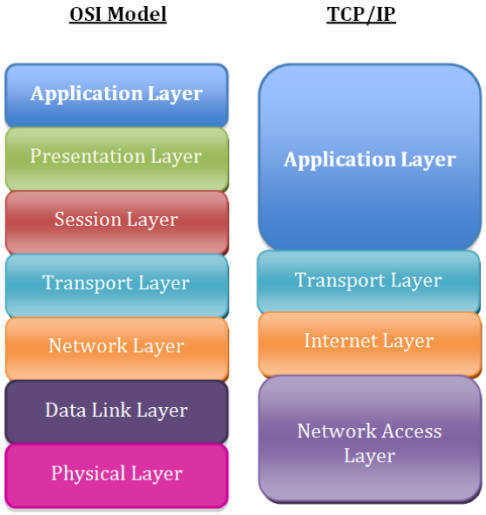
Komanda ip link se također koristi za konfigurisanje mrežnih interfejsa. Na primjer, možete promijeniti status interfejsa sa: **ip link [dev] { up | down }.** Također možete rekonfigurirati mrežna

sučelja pomoću naredbe kao što je **ip link set lo mtu 1500**. Za više informacija o komandi ip link koristite man ip link.

MAC adresa

MAC adresa (adresa za kontrolu pristupa medijima , eng. Media Access Control) je 12-cifreni heksadecimalni broj koji se dodjeljuje svakom uređaju spojenom na mrežu. Primarno specificirana kao jedinstveni identifikator tokom proizvodnje uređaja, MAC adresa se često nalazi na mrežnoj kartici uređaja (NIC). MAC adresa je potrebna kada pokušavate locirati uređaj ili kada obavljate dijagnostiku na mrežnom uređaju.

MAC adresa pripada sloju podatkovne veze modela otvorenog sistema međusobne veze, Open Systems Interconnection (OSI).



Svakom mrežnom sučelju u uređaju je dodijeljena jedinstvena MAC adresa, tako da je moguće da uređaj ima više od jedne MAC adrese. Na primjer, ako laptop ima i port za Ethernet kabal i ugrađen Wi-Fi, u konfiguraciji sistema će biti prikazane dvije MAC adrese.

IP adresiranje

IP (eng. Internet Protocol) adrese su jedinstvene na istoj mreži, svaki uređaj ima barem jedan, a adrese obično padaju negdje između 1.1.1.1 i 255.255.255.255. Da biste vidjeli IP adrese, koristite naredbu **ip address** ili samo **ip addr**.

IP adresa loopback interfejsa je 127.0.0.1. Eth0 “inet” adresa (IPV4 adresa) je također navedena tom naredbom kao dinamička adresa, primljena preko DHCP-a, o kojoj ćemo govoriti u nastavku.

Još jedan Linux mrežni alat je **ping** kao najosnovniji alat za testiranje dostupnosti mreže. Ping šalje paket protokolisan sa **Internet Control Message Protocol (ICMP)** preko mreže i obavještava vas da li postoji odgovor. Ako je host pokrenut i može komunicirati na mreži, ICMP odgovor će biti vraćen. Ako, međutim, host nije dostupan, dobit ćete obavijest da je host nedostupan ili da je isteklo vrijeme (što znači da ping test nije uspio). Primjer: $ ping -c5 192.168.192.196

(“-c5” je korišten za slanje samo pet ping paketa; u suprotnom, ping će nastaviti zauvijek).

Još jedan uobičajeni alat za rješavanje problema u Linux mreži je **traceroute**. Traceroute ispituje mrežu između lokalnog sistema i odredišta, prikupljajući informacije o svakom IP ruteru na putu. Naredba traceroute je korisna kada mislite da postoji problem sa mrežom npr. spor odgovor od jednog od posredničkih čvorova, i želite saznati koji čvor stvara problem. Na primjer: $ traceroute www.apple.com

DHCP

Ukoliko imate desetine, stotine ili hiljade računara na vašoj mreži onda je nevjerovatno dugotrajno ručno dodijeliti IP adrese i zapravo pratiti koje mašine imaju koju IP adresu. Tu na scenu stupa dinamički protokol konfiguracije hosta (DHCP – eng. Dynamic Host Configuration Protocol).

DHCP se koristi za dobijanje IP adrese kada se host ili uređaj prvi put pojavi na mreži. DHCP se obično koristi za klijentske sisteme ili uređaje koji ne doživljavaju nikakve nuspojave zbog periodične promjene IP adrese. Na serverskim sistemima, administratori ili ručno konfigurišu statičke IP adrese, ili kreiraju ono što je poznato kao statičke DHCP rezervacije koje su vezane za MAC adresu mrežnog adaptera. Ove statičke rezervacije osiguravaju da će mrežni adapter dobiti istu IP adresu svaki put kada se ponovo pokrene.

Evo kako funkcionira tipičan DHCP proces:

1. Kada se računar pokrene, on šalje DHCP zahtjev mreži.

2. Pod pretpostavkom da je DHCP server prisutan, DHCP server odgovara konfiguracijom IP adrese za taj uređaj.

3. Ta IP adresa je označena kao rezervirana kako ne bi slučajno bila dodijeljena nekom drugom uređaju.

Većina uređaja krajnjih korisnika je konfigurisana za korištenje DHCP-a. Većina operativnih sistema, uključujući Linux, je konfigurisana da koristi DHCP klijent za dobijanje njihove početne IP adrese. Možete reći da sučelje koristi DHCP ako je njegova IP adresa postavljena na DYNAMIC.

Lokalna konfiguraciona datoteka za DHCP klijenta (nazvana dhclient) je na /etc/dhcp/dhclient.conf. Ovo je konfiguraciona datoteka koja diktira Linuxu kako će primati informacije o IP konfiguraciji od DHCP servera. Da biste provjerili status na DHCP klijentu, možete **cat syslog** (sistemski dnevnik) i grep za dhcp: **$ sudo grep -Ei dhcp /var/log/syslog**

DNS

Računari koji se međusobno povezuju koristeći TCP/IP (najčešći oblik protokola povezivanja) razgovaraju jedni s drugima koristeći IP adrese; međutim, bilo bi zaista bolno da morate zapamtiti IP adresu svega na šta želite da se povežete. Zamislite da morate da se sjetite Googleove IP adrese svaki put kada želite da pretražujete internet.

Sistem imena domena (DNS) se koristi za mapiranje IP adresa u imena. DNS pretragom bezbolno vršimo pretrage na internetu bez potrebe da unosimo IP adrese naše pretražene destinacije. Da biste saznali da li vaš Linux host koristi DNS možete kosristit naredbe kao što su **dig** i **nslookup**.

Osnove DNS-a u Linuxu su sljedeće:

• Lokalni fajl pod nazivom **/etc/hosts** se koristi za prvu tačku traženja bilo kog imena hosta prije odlaska na DNS server na mreži. Ako se ime nađe tamo, više se ne traži. Kao superkorisnik, imate opciju da uredite hosts fajl i konfigurišete statičko ime za mapiranje IP adrese.

• Datoteka **/etc/resolv.conf** prikazuje lokalne domene koje treba pretraživati i koja imena servera koristiti za DNS rješavanje. Na primjer pogledajte datoteku resolv.conf: $ sudo cat /etc/resolv.conf

- **dig**: obavlja opširne DNS pretrage i odličan je za rješavanje problema s DNS-om.
- **getent**: sa opcijom **ahosts** nabraja fajlove za prebacivanje usluga imena, posebno za unose hosta.
- **nslookup**: obavlja niz različitih traženja DNS servera, pretraživanja mail servera i mnogo toga. Obično se koristi za traženje IP adrese hosta.

Osnovne naredbe za mrežnu administraciju

- **Ifconfig**: Linux ifconfig je skraćenica za konfigurator interfejsa. To je jedna od najosnovnijih naredbi koje se koriste u inspekciji mreže. ifconfig se koristi za inicijalizaciju interfejsa te konfigurisanje IP adresa. Također se koristi za prikaz rute i mrežnog interfejsa.

- **Ip**: Ovo je najnovija i ažurirana verzija naredbe ifconfig sa opcijama:
  - ip a
  - ip addr

  Ova komanda daje detalje o svim mrežama kao što je ifconfig te se može koristiti za dobijanje detalja o određenom interfejsu.

- **Traceroute**: Linux traceroute je jedna od najkorisnijih naredbi u umrežavanju. Koristi se za rješavanje problema na mreži. On detektuje kašnjenje i određuje put do vašeg cilja. U osnovi pomaže na sljedeće načine:

  - Daje imena i identifikuje svaki uređaj na putu.
  - Prati rutu do odredišta
  - Određuje odakle dolazi kašnjenje mreže i izvještava o tome.

- **Tracepath**: Linux tracepath je sličan komandi traceroute. Koristi se za otkrivanje kašnjenja u mreži. Međutim, ne zahtijeva root privilegije. Podrazumijevano je instaliran u Ubuntu. Prati rutu do navedenog odredišta i identificira svaki skok u njemu. Ako je vaša mreža slaba, prepoznaje tačku na kojoj je mreža slaba.

- **Ping**: Linux ping je jedna od najčešće korištenih naredbi za rješavanje problema s mrežom. U osnovi provjerava mrežnu povezanost između dva čvora. Ping je skraćenica za Packet INternet Groper. Komanda ping šalje ICMP eho zahtjev za provjeru mrežne povezanosti. Nastavlja se izvršavati sve dok se ne prekine. Koristite **Ctrl+C** taster da prekinete izvršenje.

- **Netstat**: Linux netstat komanda se odnosi na mrežnu statistiku. Pruža statističke podatke o različitim interfejsima koji uključuju otvorene utičnice ili sockets, tabele rutiranja i informacije o vezi.

- **ss**: Linux ss naredba je zamjena za netstat komandu. Smatra se mnogo bržom i informativnijom komandom od netstat-a. Brži odgovor ss-a je moguć jer dohvaća sve informacije iz korisničkog prostora kernela.

- **dig**: Linux naredba dig je skraćenica od Domain Information Groper. Ova komanda se koristi u DNS traženju za upit DNS servera imena. Također se koristi za rješavanje problema vezanih za DNS. Uglavnom se koristi za provjeru DNS mapiranja, MX zapisa, host adresa i svih ostalih

DNS zapisa radi boljeg razumijevanja DNS topografije. Ova naredba je improvizirana verzija naredbe nslookup.

- **nslookup**: Linux nslookup je također komanda koja se koristi za upite vezane za DNS. To je starija verzija dig.

- **route**: Linux naredba route prikazuje i manipulira tablicom usmjeravanja koja postoji za vaš sistem. Ruter se u osnovi koristi za pronalaženje najboljeg načina za slanje paketa do odredišta.

- **host**: Linux naredba host prikazuje ime domene za datu IP adresu i IP adresu za dato ime hosta. Također se koristi za dohvaćanje DNS pretraživanja za upite koji se odnose na DNS.

- **arp**: Linux arp komanda je skraćenica za Address Resolution Protocol. Koristi se za pregled i dodavanje sadržaja u ARP tablicu kernela.

- **iwconfig**: Linux iwconfig se koristi za konfigurisanje interfejsa bežične mreže. Koristi se za postavljanje i pregled osnovnih WI-FI detalja kao što su SSID i enkripcija. Da biste saznali više o ovoj komandi, pogledajte man stranicu.

- **hostname**: Linux hostname je jednostavna naredba koja se koristi za pregled i postavljanje imena hosta sistema.

- **curl** ili **wget**: Linux komande curl i wget se koriste za preuzimanje datoteka sa interneta preko CLI. Naredba curl se mora koristiti sa opcijom "O" za preuzimanje datoteke, dok se komanda wget koristi direktno s URL linkom.

- **mtr**: Linux komanda mtr je kombinacija pinga i naredbe traceroute. Kontinuirano prikazuje informacije o paketima poslanim s vremenom pinga svakog skoka. Također se koristi za pregled mrežnih problema.

- **whois**: Linux naredba whois se koristi za dohvaćanje svih informacija koje se odnose na web stranicu. Možete dobiti sve informacije o web stranici uključujući registraciju i podatke o vlasniku.

- **ifplugstatus**: Linux naredba ifplugstatus se koristi za provjeru da li je kabal priključen na mrežni interfejs. Ova komanda nije direktno dostupna na Ubuntu i treba se instalirati.

- **iftop**: Linux iftop komanda se koristi u praćenju saobraćaja i mora se instalirati na sistem.

- **tcpdum**: Linux naredba tcpdump je najčešće korištena naredba u analizi mreže među ostalim Linux mrežnim komandama. On hvata promet koji prolazi kroz mrežni interfejs i prikazuje ga. Ova vrsta pristupa paketu bit će ključna prilikom rješavanja problema na mreži.

Bonus: https://www.computernetworkingnotes.com/linux-tutorials/

Pitanja, primjedbe, sugestije:

narcisa.hadzajlic@dl.unze.ba

The history of Network Management: An Infographic

"In the beginning, there was Cabletron…"

1980s to early 1990s

In the early days of enterprise networking, the idea of a PC per employee was still science-fiction.

Business networks typically consisted of a few computer stations linked via a standard phone line, and later ethernet.

Business networks were relatively uncommon outside large enterprises, as commercial packages were unfeasible for smaller businesses.

- Most network systems were vendor-proprietary
- NMS was provided by the vendor and was customised for each deployment
- Networking came down to adapting to the Customer-Premises Equipment (CPE)
- Only Layer 1 and 2 technologies exist at this stage
- No network convergence whatsoever
- Few providers of NMS - most were absorbed by the 'big players' at this early stage.

Mid to late-1990s

Widespread internet adoption in the early 90s made TCP/IP the go-to protocol for the public internet.

BSD and Linux gain popularity in personal and professional networking.

Windows NT makes huge improvements to network convergence in enterprises.

And then, TCP/IP happened:

- Until this point, Network Management methods were particular to hardware vendors
- Interoperability among networking hardware and software was non-existent
- Networking standards at this time were disparate, and operated in very different ways

Carl Malamud - the "Saviour of the Internet"

In the early 1990s, all telecoms standards are secret to the public and kept in the ITU's 'Blue Book'.

In the early 1990s, Malmud realises the ITU has no legal basis to hold copyrights over the material in the Blue Book.

Malamud publishes all the documents from the ITU's Blue Book to an FTP server, making them freely accessible to the public.

The papers for what will become the FCAPS network management framework are developed by the OSI (International Organisation for Standardisation).

What does this mean for the end-user?

- Free availability of Standards documentation makes it possible for vendors and admins to start 'talking the same language'
- FCAPS opens the NMS market to newcomers
- Admins and vendors can focus on adapting practices and products to published standards

Late 1990s - 2000

IInteroperability among network vendors means network management within stacks is no longer necessary - Layer 1 and 2 technology monopolies begin to dissolve.

Spinoff NMS platforms become the norm, and many companies go completely bankrupt.

The infamous Cabletron restructures as a holding company, and splits into four different networking companies.

The transitional period:

The post-transition period and modern NMS

2004 - present

The state of NMS as we know it today.

Lots of newcomers enter the market, including Netsaint, OpenNMS and SolarWinds.

Exponential increase in the number of Network Management options, including proprietary, open source and 'open core' systems.