# TCP/IP na operacijskem sistemu Linux

Laboratorijske vaje so namenjene spoznavanju svežnja protokolov znanih pod imenom TCP/IP na operacijskem sistemu Linux. TCP/IP je sestavljen iz štirih plasti: plasti računalniškega omrežja, omrežne, transportne in aplikacijske plasti. Na vsaki od omenjenih plasti delujejo določeni protokoli, s katerimi lahko uporabnik operacijskega sistema komunicira preko sistemskih aplikacij, ki jih poganjamo z ukazi.

Laboratorijske vaje so razdeljene v štiri sklope, ki pokrivajo:

- 1. aplikacijsko plast: spoznavanje standardnih TCP/IP aplikacij,
- 2. plast omrežnega vmesnika: spoznavanje ukazov, ki omogočajo nadzor in upravljanje s plastjo omrežnih vmesnikov,
- 3. omrežno plast: spoznavanje ukazov, ki omogočajo nadzor in upravljanje z omrežno plastjo,
- 4. diagnostiko TCP/IP: ker Linux ne določa posebnih ukazov za nadzor in upravljanje transportnega protokola TCP, lahko njegovo delovanje opazujemo samo posredno, t.j. preko diagnostičnih programov.

Vsi ukazi, ki jih uporabljamo pri vajah, so podrobneje opisani v priročniku *Omrežni ukazi OS Linux*. Tega lahko najdete na Internetni strani <u>ftp://ftp.vss.si</u>. V veliko pomoč pa so tudi **man** strani operacijskega sistema Linux.

## Navodila:

V svoji mapi na omrežnem disku ustvarite novo mapo z imenom 'RKO-2', v kateri z urejevalnikom besedil odprete novi dokument 'Naloge.LNX'. Vse odgovore na postavljena vprašanja pišete v ustvarjeni dokument, t.i. delovno datoteko, ki ga na koncu vaj pošljete na elektronski naslov <u>iztok.fister@mdi2.net</u> kot priponko. Ne pozabite, da se vaje ocenjujejo in so predpogoj za pristop k pismenemu delu izpita RKO-2.

## Naloge:

## I. Aplikacijska plast:

- 1. Uporabite ukaz *ping* z naslovom vašega soseda. Ugotovite povprečni čas, ki ga paket rabi, da pride do vašega soseda. Zapišite tudi število prenesenih paketov in odstotek izgubljenih paketov. S pomočjo *man* strani ugotovite, kakšne možnosti ponuja? Primerjajte povprečni čas do vašega soseda s časom, ki ga paket rabi, da pride do naslova <u>www.google.com</u>? Kaj lahko sklepate iz dobljenega rezultata?
- 2. Z ukazom *hostname* določite ime vašega gostitelja.
- 3. S pomočjo ukaza FTP se povežite na FTP-strežnik z naslovom z IP-naslovom 194.249.251.4. Uporabite uporabniško ime *anonymous* in geslo svoj *E-mail naslov*. Poženite ukaz ? in zapišite nekaj odgovorov. Uporabite ukaz *dir*. Z ukazom *cd vss/ms/iztok\_fister/RKO-2* se pozicionirajte na mapo RKO-2 in

poskusite najti datoteko *Izpitna vprasanja...RKO*. To datoteko z ukazom *get* v binarni obliki (ukaz *bin*) prenesite na lokalni računalnik in jo priložite k rezultatom vaj.

4. Dodajte zapis FTP-strežnika v /*etc/hosts* datoteko. Zapišite ime, ki ste ga uporabili. Ne pozabite najprej narediti varnostne kopije datoteke *hosts* (npr. *cp* /*etc/hosts* /*etc/hosts.old*).

Format zapisa v datoteki *hosts* je naslednji:

## naslov ime1\_gostitelja ime2\_gostitelja...

kjer naslov pomeni IP-naslov gostitelja tega računalnika, ki lahko ima enega ali več imen gostitelja pridruženih temu IP-naslovu.

Da preverite, ali je bilo ime zapisano pravilno, uporabite ukaz *ping* z imenom gostitelja. Primer:

## 194.249.251.4 ftp-velenje

Vzpostavite originalno stanje datoteke hosts (npr. cp /etc/hosts.old /etc/hosts).

Prek protokola FTP se poskusite povezati s strežnikom <u>ftp.scv.si</u>. Kaj ugotovite? Kakšen je vrstni red razreševanja naslovov na vašem sistemu?

- 5. Uporabite ukaz *traceroute* z naslovom <u>www.google.com</u>. Ugotovite, koliko skokov je potrebnih, da paket najde pot do ponornega gostitelja. Kje so največji zastoji? Zakaj je ukaz uporaben?
- 6. Preberite *man* stran ukaza *netstat*. Za informacije o lokalnem vmesniku uporabite opcijo -i. Koliko vhodnih in izhodnih paketov je sprejel lokalni vmesnik *eth*0 vašega računalnika? Poskusite z opcijo -p. Kakšne informacije prikazuje? Zakaj je uporaben?
- 7. Uporabite ukaz *nslookup*. Ugotovite IP-naslov privzetega DNS-strežnika in ime gostitelja. Ugotovite tudi, kakšno je ime gostitelja z IP-naslovom 213.250.51.67 in kateri IP-naslovi se skrivajo pod imenom <u>www.ibm.com</u>.

#### II Plast omrežnega vmesnika ethernet

- 8. Uporaba ukaza **arp/arping**:
  - a. Prikažite vsebino tabele **arp** na vmesniku **eth0**.
  - b. V tabelo **arp** dodajte naslov svojega soseda tako, da računalnik sam prebere MAC naslov omrežnega vmesnika soseda in ta naslov objavi.
  - c. Poženite **ping** –**c 2** do vašega soseda in preverite vsebino tabele **arp**. Koliko odgovorov dobite?
  - d. IP naslov soseda v vaši tabeli arp zbrišite.
  - e. Preverite, ali je vaš sosed dosegljiv preko ukaza **arping** in potem preverite tabelo **arp**. Ali je zapis vašega soseda prisoten v tabeli **arp**?
  - f. Preverite, ali je IP naslov vašega računalnika res unikaten v omrežju.

Vse korake dokumentirajte.

- 9. Uporaba ukaza **ip link:** 
  - a. Z ukazom **ip link** prikažite karakteristike omrežnega vmesnika **eth0** na vašem računalniku.
  - b. Z ukazom tcpdump ocenite hitrost zavzemanja paketov IP v omrežju. Spremenite način delovanja omrežnega vmesnika v promiskuitetnega. Kaj se zgodi z delovanjem ukaza tcpdump? Razložite! Omrežni vmesnik vrnite v originalno stanje. (Namig: delajte v dveh različnih ukaznih oknih.)
  - c. Preverite stanje omrežnega vmesnika **eth0** in vsebino usmerjevalne tabele vašega računalnika. Z ukazom **ip link** deaktivirajte omrežni vmesnik in ugotovite, kakšne spremembe je povzročilo delovanje tega ukaza na konfiguracijo vašega računalnika.
  - d. Z ukazom **ip link** znova aktivirajte omrežni vmesnik in ugotovite, kakšne spremembe je povzročilo delovanje tega ukaza na konfiguracijo vašega računalnika. Ali lahko deskate po Internetu? Preverite ukaz **ping 85.10.194.170**.
  - e. Dodajte privzeti prehod in preverite vsebino usmerjevalne tabele. Ali lahko deskate po Internetu? Ali lahko dosežete Internetnega gostitelja **85.10.194.170**?
  - f. Z ukazom **ip link** spremenite velikost MTU na vrednost 576. Preverite delovanje ukaza **ping 85.10.194.170.** Velikost MTU vrnite na originalno vrednost.

Vse korake dokumentirajte.

## 10. Uporaba ukaza **ip neighbor:**

- a. Z ukazom **ip neighbor** prikažite vsebino tabele **arp** na omrežnem vmesniku **eth0**.
- b. V tabelo arp omrežnega vmesnika eth0 dodajte stalni zapis (angl. permanent entry) sosedovega računalnika, katerega MAC naslov poznamo že iz naloge 1. Kaj pomeni parameter nud v ukazu ip neighbor? Katera stanja označuje? Tabelo arp preverite! (Namig: pomagajte si z ukazom man.)
- c. Zbrišite zapis svojega soseda iz tabele arp in preverite, da zapisa v resnici ni v tabeli.
- d. Zbrišite vsebino celotne tabele arp.

Vse korake dokumentirajte.

## 11. Uporaba ukaza **mii-tool:**

- a. Preverite histrost in način delovanja omrežnega vmesnika eth0.
- b. Postavite hitrost omrežnega vmesnika na **10 MBitov** in način delovanja **half duplex**.
- c. Omrežni vmesnik restartajte. Ali omrežni vmesnik **eth0** deluje z novimi nastavitvami?
- d. Vrnite hitrost in način delovanja na originalne vrednosti.

Vse korake dokumentirajte.

## III Omrežna plast IP

12. Uporaba ukaza **ifconfig**:

- a. Z ukazom **ifconfig** prikažite trenutno konfiguracijo omrežnega vmesnika **eth0** in originalno usmerjevalno tabelo.
- b. Deaktivirajte omrežni vmesnik **eth0** in ugotovite stranske učinke delovanja ukaza **ifconfig**.
- c. Z ukazom **ifconfig** aktivirajte omrežni vmesnik **eth0** in ugotovite stranske učinke delovanja le-tega. Ali lahko deskate po Internetu? Preverite ukaz **ping 85.10.194.170**.
- d. Dodajte privzeti prehod in preverite vsebino usmerjevalne tabele. Ali lahko deskate po Internetu? Ali lahko dosežete gostitelja 192.168.0.51? (Slika 1).
- e. Dodajte statični prehod na omrežje 192.168.0.0 prek usmerjevalnika 193.2.128.102 in preverite ukaz ping **192.168.0.51**.
- f. Z ukazom ifconfig spremenite velikost MTU na vrednost 576. Preverite delovanje ukaza ping 85.10.194.170 in ukaza ping 192.168.0.51. Svoje ugotovitve komentirajte! Velikost MTU vrnite na originalno vrednost.
- g. Naredite nalogo 2.b s pomočjo ukaza ifconfig. Rezultate komentirajte!
- h. Kaj lahko zaključite ob koncu reševanja te naloge?

Vse korake dokumentirajte.



Slika 1: Usmerjanje v testnem omrežju

## 13. Uporaba ukaza **ip address**:

- a. Z ukazom **ip address** prikažite IP naslov omrežnega vmesnika **eth0**.
- b. Omrežnemu vmesniku eth0 dodajte IP naslov iz omrežja 192.168.1.0 in iz omrežja 172.16.0.0, kjer je naslov gostitelja enak originalnemu IP naslovu gostitelja. Kaj ugotovite? Kaj lahko gradimo na tak način?
- c. Dodani IP naslov gostitelja odstranite.
- d. Odstranite IP naslove gostitelja iz omrežja 172.16.0.0.
- e. Odstranite vse IP naslove na omrežnem vmesniku eth0.
- f. Omrežni vmesnik postavite v originalno stanje.

Vse korake dokumentirajte.

## IV Diagnostika IP

14. Narišite sliko vašega omrežja!

#### Koraki:

- a. Določite IP naslov vašega računalnika.
- b. Iz Broadcast naslova določite razred naslavljanja in zalogo vrednosti sosednjih računalnikov, t.j. naslov omrežja, naslov podomrežja in naslove gostiteljev.
- c. Z ukazom Broadcast ping, t.j. ping –b Broadcast\_naslov\_IP, določite gostitelje v vašem omrežju in jih popišite. Popis naj zajema IP naslove, DNS imena in MAC naslove računalnikov.
- d. Določite privzeti prehod v omrežju in strežnik DNS. Ali je strežnik DNS v istem omrežju kot vaš računalnik?

Naredite tabelarični popis opreme.

15. Uporaba ukaza wireshark:

Poženite ukaz **wireshark**. V meniju pojdite na <Capture>, in izberite <Start>. Zajemite 100 paketov. Če je proces prepočasen, v sosednjem ukaznem oknu poženite ukaz **ls** –**R**, ki generira določen promet NFS in pohitri postopek zajemanja IP paketov.

Koraki:

- a. Izberite kolono **Source** in ugotovite, kateri izvorni IP naslov se največkrat pojavlja v paketih?
- b. Kateri protokoli so najpogostejši v omrežju? (Namig: izberite kolono **Protocol** in jo sortiraj.)
- c. Kateri protokol se najpogosteje pojavlja v zajetih paketih?
- d. Izberite paket, ki je označen kot TCP paket. Določite naslednje vrednosti tega paketa:
  - i. MAC naslov ponornega gostitelja,
  - ii. IP naslov izvornega gostitelja,
  - iii. IP TTL,
  - iv. TCP izvorna vrata.
- e. Določite, ali je v omenjenem TCP paketu IP datagram fragmentiran?