**Võrguliikluse analüüs paketianalüsaatoriga**

Labor 6 juhend IT Kolledži õppeaines "I241 Sidevõrgud" kevadsemestril 2014.

Indrek Rokk, Marika Kulmar

**Töö eesmärk**

Töö eesmärgiks on uurida erinevate teenuste edastust pakettvõrgus. Edastuse uurimiseks ja analüüsiks kasutatakse vabavaralist paketianalüsaatorit [Wireshark](http://www.wireshark.org/).   
Esimeses osa tutvutakse paketianalüsaatoriga, kasutades seda IP protokollistiku ja selle rakenduste (ping ja traceroute) analüüsiks.   
Teises tutvutakse kuidas toimub veebilehe edastamine kasutajale.   
Kolmandas osas kuidas toimub aadresside transleerimine.

**Töö käik**

**Osa 1 - IP protokollistik ja selle rakendused.**

**A. kasutatava arvuti info**

Kirjutage üles oma arvuti IP aadress, võrgumask, vaikelüüs (*Default Gateway*) ja MAC aadress.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : example123.com

IPv6 Address. . . . . . . . . . . : 2001:db8:acad:b::b

Link-local IPv6 Address . . . . . : fe80::2887:52c0:d162:4877%11

IPv4 Address. . . . . . . . . . . : 172.30.85.175

Subnet Mask . . . . . . . . . . . : 255.255.255.224

Default Gateway . . . . . . . . . : 172.30.85.190

Küsimused:

1. Millisesse klassi see IP aadress kuuluks kui tegemist oleks klassisüsteemiga adresseerimsiega? Mitu bitti oleks antud klassis võrguosa pikkus?
2. Mis on antud laboris võrgumaski väärtus? Mitu bitti on selle maskiga eraldatud IP aadressist võrgu osale?
3. Mis on teie IP aadressi võrgu- ja levisaateaadressid (*broadcast*)?
4. Pange nii kümnend- kui kahendkujul kirja arvuti IP aadress, võrgu- ja levisaateaadress ning võrgumask.
5. Milline on kogu vajalik info arvuti seadistamiseks internetti kasutama?

**VASTUSED**:

1. B klass. 27 bitti.
2. 255.255.255.224. 27 bitti.
3. 192.30.85.191
4. Arvuti IP aadress (10101100000111100101010110101111, 2887669167), Võrk (10101100000111100101010110100000, 2887669152), Levisaateaadress (10101100000111100101010110111111, 2887669183). Võrgumask (11111111111111111111111111100000, 4294967264)
5. Arvuti peab teadma nimeserveri, vaikelüüsi ja enda aadressi ning lisaks võrgu maski, millest ta asub.

**B. wireshark**

Tegin ülesanded läbi.

**C. ping**

C.1 Käivitage pakettide püüdmine ja filtriks on   
Tegin ülesanded läbi.

C.2 Käivitage pakettide püüdmine. Käivitage terminali aknas käsk   
Tegin ülesanded läbi.

C.3 uurige, mida teevad allpool toodud käsud. Salvestage käskude väljundid (võite ise valida kas ekraanpildid või tekstifailid). Salvestage käskude uurimise ajal liidest läbinud paketid hilisemaks analüüsiks. Soovitatav on ühe käsu väljund salvestada ühte faili, sest see teeb hilisema analüüsi lihtsamaks.  
Käsud on:

* ping -a 193.40.252.130
* ping -n 6 rasi.lr.ttu.ee
* ping -l *1473* elab.itcollege.ee
* ping -l *1473* -f elab.itcollege.ee
* ping -i 1 elab.itcollege.ee
* ping -i 2 elab.itcollege.ee
* ping -l 40000 -w 200 elab.itcollege.ee
* ping -f -l 1472 -w 1 elab.itcollege.ee
* ping -f -l 1473 -w 1 elab.itcollege.ee

Küsimused:

1. Mis olid punktis C.3 toodud käskude tulemused?
2. Milliste protokollide pakette edastati?
3. Milliseid madalamate kihtide protokolle kasutati eelnevalt loetletud protokollide juures? Loetleda kõigi eelmises punktis toodud protokollide juures kõik need madalamate kihtide protokollid.
4. Millised kanali- ja võrgukihi protokolli päiste väljad näitavad ära paketis kõrgemal kihil asuva protokolli. Tuua ära need väärtused kuueteistkümnendkujul kõikide eelpool loetletud protokollide puhul.
5. Kui pikad olid edastatud protokollide päised?
6. Kui pikk oli pikim IP pakett? Miks just selline number?
7. Milline küsimus edastati ARP protokolli kaudu ning kellele ja milline oli vastus?
8. Mitmes bitt Etherneti aadressis näitab, kas tegemist on üksiksaate (*unicast*) või multisaate (*multicast*)/ levisaatega (*broadcast*) aadressiga? Mis on selle biti väärtus levisaate korral?
9. Kuidas saadakse teada nimest IP aadress?
10. Kuidas ICMP protokollis eristati erinevadi ping päringu pakette mida saadeti sihtpunkti? Kas oli erinevusi, kui ping päringu algatajateks oli mõni teine arvuti?
11. Millised on "näitamise filtrid" (*display filters*) näitamaks ainult ARP päringu pakette? Milline filter sobiks näitamaks kõiki pakette välja arvatud ARP päringu paketid? Pakette mille pikkus on suurem kui 1499 baiti?  
    Abiks filtrite koostamisel on Wiresharki Wiki artiklid ["DisplayFilters"](http://wiki.wireshark.org/DisplayFilters) ja ["Building display filter expressions"](http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html) ning packetlife.net "cheat sheet" ["Wireshark Display Filters"](http://packetlife.net/library/cheat-sheets/).

**D. traceroute (tracert)**

D.1. Käivitage paketi püüdmine, filtri parameetrid jätke samaks, mis ülesandes C.   
Käivitage uues terminaliaknas käsk   
**ipconfig /flushdns**   
Vajadusel avada see terminaliaken õigustes, mis võimaldavad teil seda käsku käivitada.   
  
Käivitage terminaliaknas käsk   
**tracert rasi.lr.ttu.ee**.   
Oodake kuni programm lõpetab töö ja lõpetage pakettide püüdmine.

Küsimused:

1. Milliseid protokolle kasutatakse?
2. Millisele masinale edastatakse UDP pakette?
3. Miks saadetakse meie masinale veateateid ja millistelt masinatelt need tulevad?
4. Võrrelge veateateid ja traceroute käsu tulemusena saadud infot.
5. Seletage saadud info põhjal traceroute toimimise põhimõtteid. Kirjeldage traceroute algoritmi nii nagu see töötas teil antud laboris.
6. Võrrelge veateateid saatnud masinate IP ja MAC aadresse ning seletage nähtut.
7. Millised on "näitamise filtrid" (*display filters*) näitamaks ainult pakette, mis on saadetud kindlast arvutist? Pakette, mille TTL on väiksem kui 5? Pakette, mille TTL on 3? ICMP "Time-to-live exceeded" pakette?

**Osa 2 - Veebilehe edastamine kasutajale.**

Wiresharki seadistused on samad, mis eelmises osas.   
**Kui ei ole märgitud teisiti tuleb kõik järgnevad sammud teha kõigis töös kasutatavates arvutites samaaegselt.**

ip.addr==193.40.252.130

host 172.30.85.175 not port 22

tudeng8 pakett8

**A. veebilehe vaatamine veebilehitsejaga**

1. Avada veebilehitseja ja tühjendada selle cashe.
   * Mozilla Firefox - "Tools" -> "Options" -> "Options" -> "Advanced" -> "Network" -> "Cached Web Content" -> nupp "Clear Now".
   * Internet Explorer 11 - "Safety" menüü -> "Delete Browsing History" -> jätta linnuke ainult "Temporary Internet files and website files" ette -> nupp "Delete".
2. Käivitada Wiresharkis pakettide püüdmine võrguliideselt
3. Avada lehitsejas URL <http://rasi.lr.ttu.ee/>
4. Oodata, kuni leht on laetud ja peale seda veel minimaalselt 2 minutit (120 sekundit), et püütaks kinni ka TCP ühendust lõpetavad paketid
5. Laadida see leht uuesti tehes lehele uuenduse (*Refresh*)
6. Oodata, kuni leht on laetud ja peale seda veel minimaalselt 2 minutit (120 sekundit)
7. Lõpetada pakettide püüdmine
8. Salvestada püütud paketid hilisemaks analüüsiks.

**B. veebilehe vaatamine käsitsi**

Antud punktis vaadatakse veebilehte käsurealt kasutades HTTP protokolli käsustikku.  
Serveriga saab ühendust kasutades telnet klienti ja pordiks on 80.

1. Avada labori juhend veebilehitsejas  
       Kuna kasutatava operatsioonisüsteemi telneti klient edastab iga sisestatud tähe koheselt serverile, siis on lehe edastuse hilisem analüüs raskendatud. Selle asemel kasutada antud punkti tegemisel programmi Putty.
2. Käivitada Wiresharkis pakettide püüdmine võrguliideselt
3. Käivitada programm Putty. "Connection Type" valida Raw, "Host Name" välja kirjutada rasi.lr.ttu.ee ja  "Port" välja kirjutada 80.
4. Avanenud aknasse kirjutada GET / HTTP/1.1 ja vajutada enterit. Järgmisele reale kirjutada Host: rasi.lr.ttu.ee ja vajutada enterit. Vajutada veelkord enterit.
5. Oodata kuni Putty aken on sulgunud ja lõpetada pakettide püüdmine
6. Salvestada püütud paketid hilisemaks analüüsiks.

Küsimused:

* Milliseid protokolle kasutatakse? HTTP, DNS
* Tuua ära kasutusel olnud IP aadressid ja transpordikihi pordinumbrid. Iga ühenduse kohta järjestusega:
  + kohalik võrgukihi aadress
  + kohalik transpordikihi pordinumber
  + teise osapoole võrgukihi aadress
  + teise osapoole transpordikihi pordinumber
* Millist infot antakse kliendi kohta ja millist infot serveri kohta nii A kui B vaatamise korral?
* Mis olid serveripoolsed vastused lehepäringule punktides A.3 ja A.5. Millise kliendipoolse info põhjal tehti see otsus?
* Kui palju andmeid (baitides) ja pakette edastati võrgu- ning kui palju transpordikihis? (vihjeks Statistics -> Conversations) Millisel korral oli andmemaht lehe edastamisel kõige väiksem ja miks?
* Kui pikad olid arvutite vahelised TCP ühendused? Aega hakatakse lugema esimesest paketist, millel oli seatud SYN lipp. Aeg esitada millisekundilise täpsusega
* Mis on reaalsed TCP ühenduste loomisel kasutatud *Sequence Number* mõlema osapoole juures. Näidata need numbrid nii kümnend- kui ka kuueteistkümnend kujul. Wireshark näitab originaalseadistuse korral sellel väljal *relative sequence number* ja esimesel paketil on see alati 0. Õige numbri leidmiseks vaadake tegelikke püütud andmeid (oktette, Wiresharki alumine aken).
* Millised on "näitamise filtrid" (*display filters*) näitamaks ainult pakette, mida kasutatakse ühe lehe edastamiseks? Näidatakse ainult TCP ühenduse loomise pakette (*three-way handsake*)? Näidatakse HTTP serveri vastuse pakette, milles *response code* on 200 OK?

**Osa 3 - NAT veebilehe vaatamisel.**

Wiresharki seadistused on peaaegu samad, mis eelmises osas. Capture filtrit tuleb täiendada selliselt et ei püütaks SSH ühenduse pakette. Selleks tuleb filtrisse lisada täiendavalt ***not port 22***  
  
**Kui ei ole märgitud teisiti tuleb kõik järgnevad sammud teha kõigis töös kasutatavates arvutites samaaegselt.**

1. Käivitada kasutatavas arvutites (klient arvutid) veebilehitseja
2. Avada veebilehitseja ja tühjendada selle cashe. Olenevalt lehitsejast on sammud:
   * Mozilla Firefox - "Tools" -> "Options" -> "Advanced" -> "Network" -> "Offline Storage" -> nupp "Clear Now".
   * Internet Explorer 8 - "Safety" menüü -> "Delete Browsing History" -> jätta linnuke ainult "Temporary Internet files" ette -> nupp "Delete".
3. Kasutades programmi Putty ja SSH protokolli, logida rasi.lr.ttu.ee serverisse.  
   Kasutajanime ja parooli annab juhendaja.
4. Serveris kasutada pakettide püüdmiseks programmi tshark ja püüda ainult pakette mille pordi numbriks on 80.  
   Käsk: tshark port 80 -i eth0 -w *teile sobiv faili nimi*.pcap
5. Käivitada kasutatavas arvutis Wiresharkis pakettide püüdmine võrguliideselt
6. Arvutis avada lehitsejas URL <http://rasi.lr.ttu.ee/>
7. Oodata, kuni leht on laetud ja peale seda veel minimaalselt 2 minutit (120 sekundit), et püütaks kinni ka TCP ühendust lõpetavad paketid
8. Laadida see leht uuesti tehes lehele uuenduse (*Refresh*)
9. Oodata, kuni leht on laetud ja peale seda veel minimaalselt 2 minutit (120 sekundit)
10. Lõpetada pakettide püüdmine nii kasutatvas arvutis kui ka serveris
11. Salvestada püütud paketid hilisemaks analüüsiks. Serverist salvestatud faili kättesaamiseks kasutada programmi WinSCP

Küsimused:

1. Tuua ära kasutusel olnud IP aadressid ja transpordikihi pordinumbrid nii klientarvuti kui ka serveri vaatest. Iga ühenduse kohta järjestusega:  
   Klient arvuti
   * kohalik võrgukihi aadress
   * kohalik transpordikihi pordinumber
   * teise osapoole võrgukihi aadress
   * teise osapoole transpordikihi pordinumber

Server

* + kohalik võrgukihi aadress
  + kohalik transpordikihi pordinumber
  + teise osapoole võrgukihi aadress
  + teise osapoole transpordikihi pordinumber

1. Teha vastavustabel kasutatavatest pordinumbritest. Kas mingitele portidele tehakse NAT? Kuna rasi.lr.ttu.ee serverisse võib teie mõõtmise ajal olla tehtud mitu ühendust, siis oma ühenduse pakettide leidmiseks kasutage TCP paketi päises oleva *Sequence Number* väärtust.

**Aruanne**

Aruandes tuleb vastata kõigis kolmes osas küsitud küsimustele. Vastused esitada vähemalt kolme laboris kasutatud arvuti kohta.