

IEE1220 Side arvutivõrgu protokollid

labori aruanne

Töö tegija nimi: Glen Kink

Töö tegemise kuupäev: 16.11.2021

4.2 Arvuti IP aadress

```
C:\Users\glkink>ipconfig/all

Windows IP Configuration

Host Name . . . . . : U02-20906K
Primary Dns Suffix . . . . . : intra.ttu.ee
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : intra.ttu.ee

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : intra.ttu.ee
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : 40-A8-F0-43-E8-35
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::c541:73cf:dd2d:9d51%6(Preferred)
IPv4 Address. . . . . : 172.22.92.126(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : reede, 12. november 2021 20:36:30
Lease Expires . . . . . : laupäev, 20. november 2021 20:36:23
Default Gateway . . . . . : 172.22.92.254
DHCP Server . . . . . : 192.168.133.249
DHCPv6 IAID . . . . . : 88123632
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-E4-98-7C-40-A8-F0-43-E8-35
DNS Servers . . . . . : 192.168.133.251
                        192.168.133.253
                        192.168.133.252
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . : 
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-5C-7F-E9
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::8071:6424:ec4d:c732%31(Preferred)
IPv4 Address. . . . . : 172.30.0.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 520099165
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-E4-98-7C-40-A8-F0-43-E8-35
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\glkink>
```

A. Enda arvuti MAC aadress käsurealt vaadates: 40-A8-F0-43-E8-35

B. Enda arvuti IP aadress käsurealt vaadates: 172.22.92.126

Enda arvuti IPv6 aadress käsurealt vaadates: fe80::c541:73cf:dd2d:9d51%6

C. Oma võrgu marsruuteri IP aadress (Default Gateway): 172.22.92.254

D. Nimeserverite IP aadressid (DNS servers): 192.168.133.251

192.168.133.253

192.168.133.252

E. Veebilehel näidatud enda arvuti IP aadress: 172.30.0.1

F. Mis on võimalike erinevuste põhjuseks? ipconfig käsk näitab sisevõrgu IP aadressi, veebileht aga välisvõrgu aadressi.

4.3 Ping (protokollid ARP, ICMP, UDP, DNS)

Salvestada käsurea aken koos ping tulemustega.

```
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\glkink>ping 172.22.92.143

Pinging 172.22.92.143 with 32 bytes of data:
Reply from 172.22.92.143: bytes=32 time<1ms TTL=128
Reply from 172.22.92.143: bytes=32 time<1ms TTL=128
Reply from 172.22.92.143: bytes=32 time<1ms TTL=128
Reply from 172.22.92.143: bytes=32 time<1ms TTL=128

Ping statistics for 172.22.92.143:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

A. Mida programm ping teeb ja mida tulemus näitab? Ping mõõdab lähtehostilt sihtarvutisse saadetud sõnumite edasi-tagasi aega, mis kajatakse tagasi allikale.

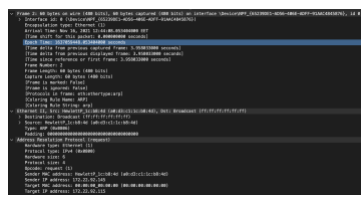
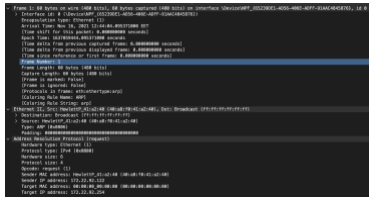
ARP

B. Milliste protokollide päiseid ARP paketid sisaldavad? Aadressiteisenduse protokoll (inglise Address Resolution Protocol, lühend ARP) on protokoll IP-aadressi vastendamiseks riistvara aadressi ehk MAC-aadressiga. Protocols in frame: eth:ethertype:arp

C. Millisele aadressile saadetakse ARP päring? Dst: Broadcast (ff:ff:ff:ff:ff:ff)

D. Milliselt aadressilt tuleb ARP vastus? Source: HewlettP 41:a2:40 (40:a8:0:41:22:40)

E. Milline on ARP pakettide sisu? ARP päringu pakett sisaldab lähte-MAC-aadressi ja lähte-IP-aadressi ning sihtkoha IP-aadressi. Iga kohaliku võrgu host saab selle paketi.



Lisada ekraanipilt Wiresharki keskmisest aknast, kus näha dekodeeritud kujul ARP päringu paketi EthernetII ja ARP osa ning teine ekraanipilt Wiresharki keskmisest aknast, kus näha ARP vastuse paketi dekodeeritud EthernetII ja ARP osa.

IP

F. Milline väärtus on väljal Flags ja millist informatsiooni see annab? Flags: 0x00

0... = Reserved bit: Not set Kui see on 1 pannakse üks bitt kõrvale kui tulevikus protokollil vaja on.

.0.. = Don't fragment: Not set Kui see on 1 ja IP peab paketi killustama ehk omakorda pakettideks jagama, siis IP viskab paketi minema killustamise asemel.

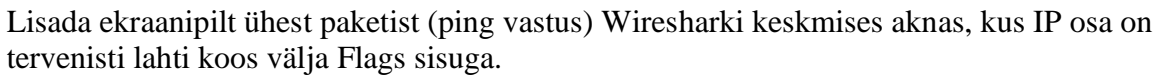
..0. = More fragments: Not set Kui see on 0, tähendab et rohkem andmekilde (pakette) ei tule.

G. Milline väärtus on väljal Header Length ja millist informatsiooni see annab? 0101 = Header Length: 20 bytes (5)

Näitab mitu 32 bitist sõna on päises. $32/8=4$ baiti $4*5=20$ baiti. Praegusel juhul ütleb, et päise pikkus on 20 baiti ehk 5 nelja baidist sõna. Päis on alati vähemalt 20 baiti.

H. Milline väärtus on väljal Total Length ja millist informatsiooni see annab? Total Length: 206
Näitab kogu andmemahu suurust ehk praegu 206 baiti.

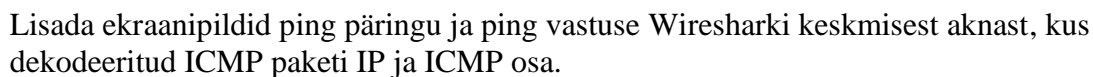
I. Milline väärtus on väljal Protocol ja millist informatsiooni see annab? Protocol: UDP (17)
Kasutajadatagrammi protokoll (ingl User Datagram Protocol, UDP) on transpordikihi andmesideprotokoll, mis on defineeritud IPga sõnumite saatmiseks ehk näitab IP-le kuhu paketid saata.



J. Milliste protokollide päseid ICMP paketid sisaldavad? **Protocols in frame:**
eth:ethertype:ip:icmp:data

MAC: (40:a8:f0:43:8:35) IP: 172.22.92.126

M. Mis on päringu ja vastuse Data osas (kirjeldada oma sõnadega andmete kogust ja sisu)?
andmekogus on 32 baiti ja sisu on numbrid ja tähed, kust täpitähed puuduvad.



IP: 93.184.216.34

IP: 93.184.216.34

```

> Frame 40: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{65239DE1-AD56-406E-ADFF-91AAC4845876}, id 0
> Ethernet II, Src: Fortinet_09:00:24 (00:09:0f:09:00:24), Dst: HewlettP_43:e8:35 (40:a8:f0:43:e8:35)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 172.22.92.126
> Internet Control Message Protocol

```

Lisada ekraanipilt ping päringu ja ping vastuse pakettidest Wiresharki keskmises aknas, (kus kõik plussid kinni).

UDP, DNS

P. Milliste protokollide päiseid DNS paketid sisaldavad? Protocols in frame:

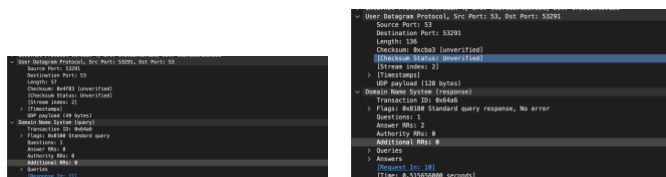
eth:ethertype:ip:udp:dns

R. Kui pikk on UDP päis? 8 baiti

S. Mis sisaldub UDP päises? User Datagram Protocol, päringu saatva IP aadressi port, päringu vastuvõtva IP aadressi port

T. Milline on UDP pordi number DNS jaoks (serveri port)? 53

U. Mis sisaldub DNS osas? Transaction ID, Flags, Queries



Lisada ekraanipildid DNS päringu ja vastuse pakettidest Wiresharki keskmises aknas, kus UDP ja DNS osad on lahti.

4.4 Traceroute

```
C:\Users\glkink>tracert www.example.com

Tracing route to www.example.com [93.184.216.34]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  172.22.92.254
  2  *      *      *      Request timed out.
  3  1 ms   1 ms   1 ms   ttu-gw.eenet.ee [193.40.244.1]
  4  2 ms   2 ms   2 ms   fi-csc2.nordu.net [109.105.98.113]
  5  17 ms  17 ms  17 ms   de-hmb.nordu.net [109.105.97.77]
  6  24 ms  24 ms  24 ms   nl-sar.nordu.net [109.105.97.51]
  7  24 ms  24 ms  29 ms   nl-ams.nordu.net [109.105.97.217]
  8  108 ms 108 ms 108 ms   us-man.nordu.net [109.105.97.64]
  9  100 ms 100 ms 100 ms   edgecast.com [198.32.160.14]
 10  101 ms 102 ms 101 ms   ae-66.core1.nyb.edgecastcdn.net [152.195.69.131]
 11  100 ms 100 ms 100 ms   93.184.216.34

Trace complete.
```

Lisada ekraanipilt käsurealt olevatest traceroute tulemustest.

A. Mis on traceroute tulemuseks üldiselt? Enamik rakendusi sisaldab vähemalt valikuid, et määrata ühe hüppe kohta saadetavate päringute arv, vastuse ootamise aeg, vaheldumislimiit ja kasutatava port. Määramata suvanditeta traceroute'i kutsumine kuvab saadaolevate valikute loendi, samas kui man traceroute pakub rohkem üksikasju, sealhulgas kuvatud vealipud. Näitab mis marsruuterist pakett läbi läks ja kaua tal läks aega.

B. Mitme marsruuteri kaugusel meie võrgust asub www.example.com? 9 äkki

C. Milliseid protokolle kasutatakse tracert käsu täitmiseks? ICMP, DNS

D. Milline paketi eluaja (Time To Live, TTL) väärtus on kõikidel ICMP päringu pakettidel ning vastuse pakettidel? Päringu pakettidel 91, vastuste pakettidel 134.

E. Mida TTL näitab? Näitab kaua pakette hoitakse enne kui need kustutatakse.

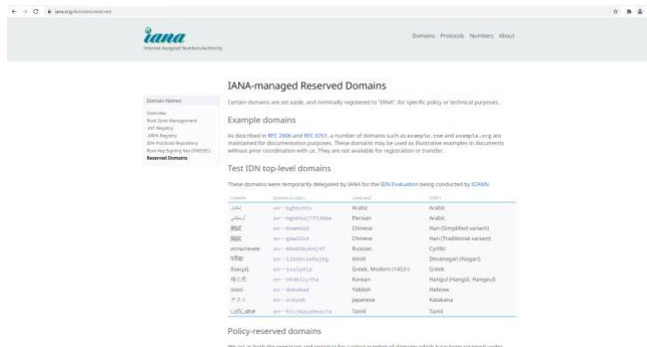
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.22.92.126	192.168.133.251	DNS	75	Standard query 0x16fc A www.example.com
2	0.000384	192.168.133.251	172.22.92.126	DNS	91	Standard query response 0x16fc A www.example.com
3	0.000197	172.22.92.126	93.184.216.34	ICMP	106	Echo (ping) request id=0x0001, seq=92/23206
4	0.000437	172.22.92.254	172.22.92.126	ICMP	134	Time-to-live exceeded (time to live exceeded)
5	0.000859	172.22.92.126	93.184.216.34	ICMP	106	Echo (ping) request id=0x0001, seq=92/23552
6	0.000248	172.22.92.254	172.22.92.126	ICMP	134	Time-to-live exceeded (time to live exceeded)
7	0.010434	172.22.92.126	93.184.216.34	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808
8	0.010655	172.22.92.254	172.22.92.126	ICMP	134	Time-to-live exceeded (time to live exceeded)
9	0.012697	172.22.92.126	152.195.69.131	DNS	86	Standard query 0x0658 PTR 254.92.22.172.in-addr.arpa
10	0.013233	192.168.133.251	172.22.92.126	DNS	171	Standard query response 0x0658 No such name
11	1.000311	172.22.92.126	192.168.133.251	DNS	92	Standard query 0xf6b1 A eu-v20.events.data.ripe.net
12	1.007029	192.168.133.251	172.22.92.126	DNS	213	Standard query response 0xf6b1 A eu-v20.events.data.ripe.net
13	5.528739	172.22.92.126	93.184.216.34	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064

Lisada Wiresharki ülemise akna ekraanipilt koos kõikidest traceroutega seotud pakettidest.

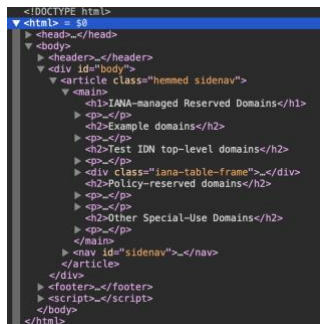
4.5 WWW (protokollid TCP, HTTP)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.22.92.126	93.184.216.34	TCP	66	60044 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
2	0.001430	172.22.92.126	93.184.216.34	TCP	66	60045 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
3	0.091018	93.184.216.34	172.22.92.126	TCP	66	80 → 60044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
4	0.091107	172.22.92.126	93.184.216.34	TCP	54	60044 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5	0.091433	172.22.92.126	93.184.216.34	HTTP	487	GET / HTTP/1.1
6	0.092542	93.184.216.34	172.22.92.126	TCP	66	80 → 60045 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
7	0.092652	172.22.92.126	93.184.216.34	TCP	54	60045 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8	0.182477	93.184.216.34	172.22.92.126	TCP	60	80 → 60044 [ACK] Seq=1 Ack=434 Win=67072 Len=0
9	0.182947	93.184.216.34	172.22.92.126	HTTP	1081	HTTP/1.1 200 OK (text/html)
10	0.224103	172.22.92.126	93.184.216.34	TCP	54	60044 → 80 [ACK] Seq=434 Ack=1028 Win=261632 Len=0

Lisada Wiresharki ülemisest aknast ekraanipilt.



Lisada ekraanipilt külastatud veebilehest.



Lisada salvestatud lehe lähtekood.

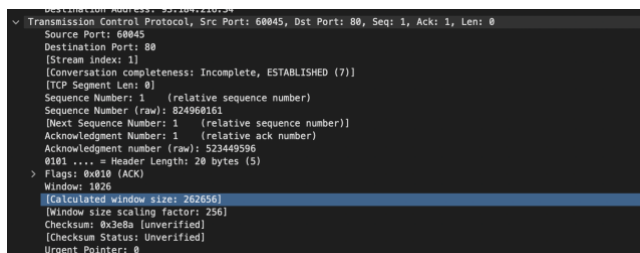
A. Milliste protokollide päseid saadud paketid sisaldavad? TCP, HTTP

B. Kui pikk on TCP päis? 32 baiti

C. Millised väärtused on väljadel Sequence Number ja Acknowledgement number ja millist informatsiooni see annab? 0 ja 0. See näitab, et valisin esimese paketi - pakett on teele saadetud aga pole veel vastu võetud. Järgmine pakett näitaks 0 ja 1, mis tähendab et pakett saadi kätte. Järjenumbr on saadetud TCP-paketi (nimetatakse ka TCP segmendiks) andmete esimese baidi baidinumber. Kinnitusnumber on järgmise baidi järjenumbr, mille vastuvõtja ootab. Kinnitusnumber kehtib ainult siis, kui ACK-lipp on üks.

D. Kuidas TCP ühendust alustatakse (3 esimest paketti - milline arvuti millisele saadab ja millised TCP lipud on aktiveeritud)? Lipud aktiveeritud : 1) [SYN], 2) [SYN] , [ACK] 3) [ACK] ehk esimene arvuti teisele, teine esimesele ja esimene uuesti teisele

E. Kuidas TCP ühendust lõpetatakse (4 viimast paketti - milline arvuti millisele saadab ja millised TCP lipud on aktiveeritud)? Lipud aktiveeritud : 1) [FIN], [ACK] 2) [ACK] 3) [FIN], [ACK] 4) [ACK] ehk teiselt arvutilt esimesele, esimeselt teisele, esimeselt uuesti teisele ja lõpuks teiselt esimesele arvutile.



Lisada Wiresharki ekraanipilt ühest paketist, kus keskmises aknas on TCP osa lahti.

HTTP

F. Milline HTTP päring saadetakse (järgmine pakett, mille Teie arvuti saatis pärast TCP ühenduse loomist)? GET / HTTP/1.1

G. Milline tuleb HTTP vastus sellele päringule? HTTP/1.1 200 OK (text/html)

H. Milline on TCP pordi number HTTP jaoks (serveri port)? Destination Port: 80


```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Content-Encoding: gzip\r\n
    Accept-Ranges: bytes\r\n
    Age: 468177\r\n
    Cache-Control: max-age=604800\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Date: Tue, 16 Nov 2021 18:58:05 GMT\r\n
    Etag: "324752594f-gzip\r\n
    Expires: Tue, 23 Nov 2021 18:58:05 GMT\r\n
    Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n
    Server: ECS (nyb/3D19)\r\n
    Vary: Accept-Encoding\r\n
    X-Cache: HIT\r\n
  > Content-Length: 648\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.091514000 seconds]
  [Request in frame: 3]
  [Request URI: http://www.example.com/]
  Content-encoded entity body (gzip): 648 bytes -> 1256 bytes
  File Data: 1256 bytes

```

Lisada ekraanipilt päringu paketist Wiresharki akna keskmine osa, kus HTTP osa on lahti ning vastuse paketist Wiresharki akna keskmine osa, kus HTTP osa on lahti.

4.6 Individaalülesanne

Lähteandmete kogumine

```

glenkink@01ens-MBP ~ % ping -s 1900 www.example.com -t 10
PING www.example.com (93.184.216.34): 1900 data bytes
1900 bytes from 93.184.216.34: icmp_seq=0 ttl=64 time=128.659 ms
1900 bytes from 93.184.216.34: icmp_seq=1 ttl=64 time=128.002 ms
1900 bytes from 93.184.216.34: icmp_seq=2 ttl=64 time=128.806 ms
1900 bytes from 93.184.216.34: icmp_seq=3 ttl=64 time=126.922 ms
1900 bytes from 93.184.216.34: icmp_seq=4 ttl=64 time=130.968 ms
1900 bytes from 93.184.216.34: icmp_seq=5 ttl=64 time=127.726 ms
1900 bytes from 93.184.216.34: icmp_seq=6 ttl=64 time=128.692 ms
1900 bytes from 93.184.216.34: icmp_seq=7 ttl=64 time=128.158 ms
1900 bytes from 93.184.216.34: icmp_seq=8 ttl=64 time=128.668 ms
1900 bytes from 93.184.216.34: icmp_seq=9 ttl=64 time=127.833 ms
--- www.example.com ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 126.922/128.385/130.968/1.916 ms

```

Lisada ekraanipilt ping käsureast ja tulemustest.

Üliõpilaskood: 213427IACB

Ping käsurida: ping -s 1900 www.example.com -t 10

Keskmine RTT:128ms

Wiresharkist leida:

mitmes fragmendis etteantud pikkusega üks ping päring saadeti:

ühe päringu andmete (data) osa pikkus (kõikides fragmentides kokku): 1514

EthernetII päise pikkus:2

IP päise pikkus:4

ICMP päise pikkus:1

•	1	0.000000	192.168.1.160	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0
•	2	0.000177	192.168.1.160	93.184.216.34	ICMP	462	Echo (ping) request id=0x6f53, seq=0/0, tt
•	3	0.128433	93.184.216.34	192.168.1.160	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0
•	4	0.128434	93.184.216.34	192.168.1.160	ICMP	462	Echo (ping) reply id=0x6f53, seq=0/0, tt

Lisada Wiresharki ekraanipilt, kus peal ülemises aknas üks päring koos fragmentidega ja üks vastus fragmentidega (iga pakett on üks rida).

LISADA ÜLESANDE LAHENDUSKÄIK JA TULEMUSED!!

Kasulikud andmed: 1900baiti = 15 200 bitti

Edastatud andmed: 1908 baiti

Kulunud aeg: 128 ms = 0,128 s

Edastuskiirus = $15200 / 0,064 = 237.5\text{ kbit/s}$

Efektiivsus = $1900/1908*100 = 99,6\%$

Kokkuvõte ja järeldused

KIRJUTA KOKKUVÕTE JA JÄRELDUSED SIIA!

Õppisin laboris kasutama Wiresharki ning arvutivõrgu protokollidest õppisin ka omajagu juurde. Labor oli põnev, aga aruannet oli väga raske kirjutada, kuid üldmulje oli hea. Õppejõud oli super nagu alati.