

## **Laboratorinio darbo ataskaita**



VILNIAUS UNIVERSITETAS  
MATEMATIKOS IR INFORMATIKOS FAKULTETAS  
INFORMACINIŲ SISTEMŲ INŽINERIJA, 3 KURSAS

### **Laboratorinis darbas 1 – Kompiuterių tinklo aplinkos tyrimas su CMD KOMPIUTERIŲ TINKLAI**

Atliko: Martynas Jašinskas

VU el. p: [martynas.jasinskas@mif.stud.vu.lt](mailto:martynas.jasinskas@mif.stud.vu.lt)

Vilnius, 2022

1. Nustatykite ir pateikite savo darbo kompiuterio tinklo sąsajos (tinklo plokštės) informaciją: IP adresą; tinklo plokštės (virtualios ar fizinės) adresą; potinklio kaukę; DNS serverio(-ių) IP adresą(-us); standartinių vartų (angl. gateway) adresą; naudojamas IP adresas yra statinis ar dinaminis?

Žemiau pateikta informacija, gauta su komanda *ipconfig /all*.

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

Windows IP Configuration

Host Name . . . . . : DESKTOP-KC8T8NT
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Dlink

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : Dlink
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 70-85-C2-6B-2B-43
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fd01::2a2e:1ed0:ffd6:4399(Preferred)
Temporary IPv6 Address. . . . . : fd01::70b8:a74e:e229:a620(Preferred)
Link-local IPv6 Address . . . . : fe80::88e3:3725:433b:38d7%6(Preferred)
IPv4 Address. . . . . : 192.168.0.39(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 05 December 2022 20:16:16
Lease Expires . . . . . : 06 December 2022 20:16:15
Default Gateway . . . . . : fe80::f2b4:d2ff:fec8:1ffe%6
                          192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 108037570
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-5F-64-6F-70-85-C2-6B-2B-43
DNS Servers . . . . . : fe80::f2b4:d2ff:fec8:1ffe%6
                          5.20.0.10
                          5.20.0.11
                          fe80::f2b4:d2ff:fec8:1ffe%6
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
Dlink
Dlink
```

IP adresas: 192.168.0.39

Tinklo plokštės MAC: 70-85-C2-68-2B-43

Subnet'o kaukė: 255.255.255.0

DNS serverio IP adresas: 5.20.0.10 arba 5.20.0.11

Gateway adresas: 192.168.0.1

IP adresas yra dinaminis, nes DHCP yra įjungtas.

**2. Pateikite kompiuterio faile Hosts įrašytų DNS įrašų sąrašą. Pagal kurį parametą galime suprasti, kad DNS įrašas yra pateikiamas iš Hosts failo? Kokį vaidmenį atlieka Hosts faile esantys įrašai Windows OS?**

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1             localhost
#   ::1                   localhost
```

DNS įrašai iš „Hosts“ failo pasižymi tuo, kad čia yra saugomi tik domenų (arba subdomenų) pavadinimai. T.y. nėra protokolų ar kitų pavadinimų priesagų. Taip pat, jeigu įrašai turi groteles, tai galime spręsti jog jiė yra iš „Hosts“ failo, nes čia šitas simbolis indikuoja komentarus.

Kompiuterio OS, kai reikia konvertuoti domeną į IP adresą, pirmiausia pasižiūri į savo lokalų Hosts failą.

**3. Kokį protokolą naudoja ping komanda? Kuo šis protokolas skiriasi nuo kitų?**

Naudoja ICMP protokolą.

Šis protokolas nėra „data transfer“ protokolas, pirmu taikiniu, kaip TCP arba UDP. Jo esmė yra nešti paketus, laikančius informaciją apie tinklo būseną. Taip pat, vienas iš išskiriančių bruožų šio protokolo, tai kad jis siunčia tik vieną paketą.

**4. Kodėl ping komandoje nereikia nurodyti prievado (angl. port) numerio?**

ICMP protokolas yra 3 OSI lygmens protokolas, todėl jam nereikia porto, kad operuoti.

5. Paleiskite ping komandą nurodydami savo darbo kompiuterio vartų IP adresą. Koks vidutinis (angl. average) paketo RTT laikas?

```
C:\Users\Miautawn>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Vidutinis RTT – 0ms.

6. Paleiskite ping komandą nurodydami VU informacinės sistemos IP adresą 158.129.159.11. Koks vidutinis (angl. average) paketo RTT laikas?

```
C:\Users\Miautawn>ping 158.129.159.11

Pinging 158.129.159.11 with 32 bytes of data:
Reply from 158.129.159.11: bytes=32 time=1ms TTL=57
Reply from 158.129.159.11: bytes=32 time=1ms TTL=57
Reply from 158.129.159.11: bytes=32 time=1ms TTL=57
Reply from 158.129.159.11: bytes=32 time=1ms TTL=57

Ping statistics for 158.129.159.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Vidutinis RTT – 1ms.

7. Kodėl skiriasi RTT laikai lyginant 5-os ir 6-os užduoties gautus RTT laikus?

RTT gali skirtis, kadangi kviečiant VU adresą, mum reikia „peršokti“ daugiau router'ių, kas užima laiko, kol mano „default gateway“ yra čia pat kur ir kompiuteris. *Tracert* į *default gateway* ir *VU adresą* yra pateikti žemiau.

```
Tracing route to dlinkrouter.Dlink [192.168.0.1]  
over a maximum of 30 hops:
```

```
  1    <1 ms    <1 ms    <1 ms  dlinkrouter.Dlink [192.168.0.1]
```

```
Trace complete.
```

```
Tracing route to 158.129.159.11 over a maximum of 30 hops
```

```
  1    <1 ms    <1 ms    <1 ms  dlinkrouter.Dlink [192.168.0.1]  
  2     1 ms     1 ms    <1 ms  data-136-2.cgates.lt [5.20.136.2]  
  3     1 ms     1 ms     1 ms  dmz-7-2.cgates.lt [5.20.7.2]  
  4     1 ms    <1 ms    <1 ms  193.219.62.6  
  5     1 ms    <1 ms    <1 ms  rs.vu.lt [193.219.95.2]  
  6     1 ms     1 ms     1 ms  rs2.vu.lt [193.219.95.4]  
  7      *      *      *      Request timed out.  
  8     1 ms     1 ms     1 ms  158.129.159.11
```

```
Trace complete.
```

8. Pirmoje užduotyje radote savo darbo kompiuterio potinklio kaukę. Naudodami ping komanda nustatykite aktyvius tinklo įrenginius savo potinklyje. Imtis – 10-imt IPv4 adresų iš bet kurio potinklio režio.

```
C:\Users\Miautawn>for /l %i in (1,1,10) do @ping 192.168.0.%i -w 10 -n 1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pinging 192.168.0.2 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.2:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.3 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.3:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.4 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.5 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.5:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.6 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.6:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.7 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.7:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.8 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.9 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.9:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.10 with 32 bytes of data:
Request timed out.
```

Vienintelis aktyvus yra mano „default gateway“, kas yra mano routeris.

**9. Nustatykite naudodami savo darbo kompiuterį ar nurodyti kompiuteriai/serveriai yra aktyvūs globaliame tinkle (GAN).**

Google.lt

```
Pinging google.lt [142.250.203.195] with 32 bytes of data:
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=9ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120
Reply from 142.250.203.195: bytes=32 time=8ms TTL=120

Ping statistics for 142.250.203.195:
    Packets: Sent = 30, Received = 30, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 9ms, Average = 8ms
```

0% loss, vidutinis RTT – 8ms

**webmail.vu.lt**

```
C:\Users\Miautawn>ping -n 30 web4k.vu.lt
```

Pinging web4k.vu.lt [158.129.159.164] with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 158.129.159.164:  
Packets: Sent = 30, Received = 0, Lost = 30 (100% loss),

100% loss

**Oafx.eu**

```
C:\Users\Miautawn>ping -n 30 www.oafx.eu
Ping request could not find host www.oafx.eu. Please check the name and try again.
```

Nepasiekiamas



# Havenworks.com

```
C:\Users\Miautawn>ping -n 30 havenworks.com

Pinging havenworks.com [81.171.28.45] with 32 bytes of data:
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Reply from 81.171.28.45: bytes=32 time=28ms TTL=57
Ping statistics for 81.171.28.45:
    Packets: Sent = 30, Received = 30, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 28ms, Average = 28ms
```

0% loss, vidutinis RTT – 28ms

10. Nustatykite naudodamiesi tinklalapiu <https://ping.eu/ping/> ar nurodyti kompiuteriai/serveriai yra aktyvūs globaliame tinkle (GAN).

#### Google.lt

```
IP address or host name:  Enter code:

--- PING google.lt (142.250.74.99) 56(84) bytes of data. ---
64 bytes from 142.250.74.99: icmp_seq=1 ttl=115 time=33.5 ms
64 bytes from 142.250.74.99: icmp_seq=2 ttl=115 time=33.6 ms
64 bytes from 142.250.74.99: icmp_seq=3 ttl=115 time=33.6 ms
64 bytes from 142.250.74.99: icmp_seq=4 ttl=115 time=33.5 ms

--- google.lt ping statistics ---

packets transmitted 4
received           4
packet loss        0 %
time               3017 ms

--- Round Trip Time (rtt) ---

min   33.474 ms
avg   33.529 ms
max   33.578 ms
mdev  0.039 ms
```

0% loss, vidutinis RTT – 3017ms

#### webmail.vu.lt

```
IP address or host name: 

--- PING web4k.vu.lt (158.129.159.164) 56(84) bytes of data. ---

--- web4k.vu.lt ping statistics ---

packets transmitted 9
received           0
packet loss        100 %
time               8282 ms
```

100% loss

**Oafx.eu**

Nepasiekiamas

**Havenworks.com**

```
--- PING havenworks.com (74.63.241.25) 56(84) bytes of data. ---
64 bytes from 74.63.241.25: icmp_seq=2 ttl=49 time=130 ms
64 bytes from 74.63.241.25: icmp_seq=3 ttl=49 time=129 ms
64 bytes from 74.63.241.25: icmp_seq=4 ttl=49 time=129 ms
64 bytes from 74.63.241.25: icmp_seq=5 ttl=49 time=129 ms

--- havenworks.com ping statistics ---

packets transmitted 5
received 4
packet loss 20 %
time 4072 ms

--- Round Trip Time (rtt) ---

min 129.310 ms
avg 129.365 ms
max 129.506 ms
mdev 0.081 ms
```

20% loss, vidutinis RTT – 4072ms

**11. Palyginkite 9-oje ir 10-oje užduotyje gautų vidutinių RTT laikų rodiklius. Kodėl jie skiriasi? Iš kur atsiranda skirtumas?**

Galime pastebėti, Windows ir tinklapio *ping* komandos bando siųsti skirtingo dydžio paketus (Windows – 32B, tinklapio – 64B). Kita priežastis gali būti tiesiog didesnis routerių kelias jeigu siunčiame *ping* paketus iš tinklapio.

**12. tracert komandoje įveskite „tracert vu.lt“. Kiek šuolių (angl. hop) per maršrutizatorius atliekama, kol pasiekiamas vu.lt serverio IP adresas? Savais žodžiais aprašykite tracert kelyje esančių taškų (nurodytų DNS vardų) reikšmes.**

```

C:\Users\Miautawn>tracert vu.lt

Tracing route to vu.lt [158.129.163.49]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dlinkrouter.Dlink [192.168.0.1]
  2  <1 ms     1 ms     <1 ms    data-136-2.cgates.lt [5.20.136.2]
  3   1 ms     <1 ms     1 ms    dmz-7-2.cgates.lt [5.20.7.2]
  4  13 ms     <1 ms     <1 ms    193.219.62.6
  5   1 ms     <1 ms     <1 ms    rs.vu.lt [193.219.95.2]
  6   1 ms     1 ms     1 ms    rs2.vu.lt [193.219.95.4]
  7   *        *        *        Request timed out.
  8   1 ms     1 ms     1 ms    158.129.163.49

Trace complete.

```

Yra padaroma 8 šuoliai. Kai išeinama iš mano routerio, pirmiausia yra pasiekiami mano ISP routeriai „cgate“; Peršokama per nežinomą mazgą – 193.219.62.6; Galiausiai atsiduriame prie VU routerių, kas matoma iš jų hostnames.

### 13.Kodėl kai kuriose tracert eilutėse rodikliai pateikiami žvaigždute (\*)?

Žvaigždutės indikuoja, kad vienas iš routerių neatsakė į requestą. Tai gali būti dėl to, kad „time-outino“, arba buvo sukonfigūruotas neatsakyti į tokius requestus.

### 14.tracert komandoje įveskite „tracert aliexpress.com“. Kiek šuolių (angl. hop) per maršrutizatorius atliekama, kol pasiekiamas aliexpress.com serverio IP adresas? Kodėl skaičius didesnis nei vu.lt kelio? Išrašykite tracert kelyje esančių miestų pavadinimus.

```

Tracing route to aliexpress.com [47.254.177.101]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dlinkrouter.Dlink [192.168.0.1]
  2  <1 ms     <1 ms     <1 ms    data-136-2.cgates.lt [5.20.136.2]
  3   *        1 ms     <1 ms    dmz-2-251.cgates.lt [5.20.2.251]
  4   *        *        *        Request timed out.
  5   *        *        *        Request timed out.
  6   *        *        *        Request timed out.
  7   *        *        *        Request timed out.
  8  23 ms     23 ms     23 ms    47.254.177.101

Trace complete.

```

Skaičius yra didesnis, nes mes bandome pasiekti tolesnę geografinę vietą, kurioje „aliexpress“ serveris yra pahostintas. Šiuo atveju mūsų ieškomas serveris yra Vokietijoje.

Routerių miestai:

- D-link router – Vilnius, Lietuva
- Data-136-2 cgates – Vilnius, Lietuva
- Dmz-2-251 cgates Vilnius, Lietuva
- 72.254.2177.101 – Hesenas, Vokietija

## 15.Kas yra adresų domenas? Ar galime naršyti interneto tinklalapius be DNS įrašų? Kodėl?

Domenas – tai yra žmogui suprantamas vardas, kuris yra priskiriamas kažkokiam viešam IP adresui. Mes naudojame domenus tam, kad naršyti po internetą būtų daug patogiau žmonėms ir nereikėtų vesti tiesioginių IP adresų.

Kadangi domenas yra tik IP adresui asocijuotas pavadinimas, kuris vėliau verčiamas į IP adresą, mes galime pasiekti kitus network'us ir įrenginius tiesiai per IP adresus.

## 16.Pasinaudoję nslookup komanda raskite vu.lt pašto serverio vardą(-us).

```
C:\Users\Miautawn>nslookup -type=mx vu.lt
Server: UnKnown
Address: fe80::f2b4:d2ff:fec8:1ffe

Non-authoritative answer:
vu.lt MX preference = 0, mail exchanger = vu-lt.mail.protection.outlook.com

vu.lt nameserver = ns.bi.lt
vu.lt nameserver = ns.vu.lt
vu.lt nameserver = ns2.domreg.lt
ns2.domreg.lt internet address = 83.171.8.8
ns.bi.lt internet address = 213.226.131.130
ns.vu.lt internet address = 193.219.80.1
ns2.domreg.lt AAAA IPv6 address = 2001:778:0:8::8
```

Pašto serverio vardas - vu-lt.mail.protection.outlook.com.

**17. Pasinaudoję nslookup komanda raskite vu.lt vardų serverio (angl. name server) adresą(-us).**

```
C:\Users\Miautawn>nslookup -ty=ns vu.lt
Server: UnKnown
Address: fe80::f2b4:d2ff:fec8:1ffe

Non-authoritative answer:
vu.lt      nameserver = ns.bi.lt
vu.lt      nameserver = ns2.domreg.lt
vu.lt      nameserver = ns.vu.lt

ns.bi.lt   internet address = 213.226.131.130
ns.vu.lt   internet address = 193.219.80.1
ns2.domreg.lt internet address = 83.171.8.8
ns2.domreg.lt AAAA IPv6 address = 2001:778:0:8::8
```

Vu.lt vardų serveriai yra: *ns.bi.lt*, *ns2.domreg.lt*, *ns.vu.lt*.

**18. Pasinaudoję nslookup komanda raskite ibm.com vardų serverio (angl. name server) adresą(-us). Kaip manote, ką subdomeno pavadinimas(-ai) reiškia?**

```
C:\Users\Miautawn>nslookup -ty=ns ibm.com
Server: UnKnown
Address: fe80::f2b4:d2ff:fec8:1ffe

Non-authoritative answer:
ibm.com nameserver = usc2.akam.net
ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = eur5.akam.net
ibm.com nameserver = eur2.akam.net

eur5.akam.net internet address = 23.74.25.64
eur2.akam.net internet address = 95.100.173.64
usc3.akam.net internet address = 96.7.50.64
usc2.akam.net internet address = 184.26.160.64
asia3.akam.net internet address = 23.211.61.64
usw2.akam.net internet address = 184.26.161.64
ns1-206.akam.net internet address = 193.108.91.206
ns1-99.akam.net internet address = 193.108.91.99
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
```

Ibm.com vardų serveriai: *usc2.akam.net*, *ns1-206.akam.net*, *ns1-99.akam.net*, *usw2.akam.net*, *usc3.akam.net*, *eur5.akam.net*, *eur2.akam.net*.

Iš subdomenų galime įsivaizduoti kur tie vardų serveriai yra hostinami (pvz. eur5.akam.net galėtų būti hostinamas Europoje, kol asia3.akam.net gali būti Azijoje)

**19.nslookup komanda raskite domeno aciū.lt IPv4 adresą(-us). Kuriai tinklo klasei priklauso nurodytas IPv4 adresas?**

```
C:\Users\Miautawn>nslookup -A aciū.lt
*** Invalid option: A
Server: UnKnown
Address: fe80::f2b4:d2ff:fec8:1ffe

Non-authoritative answer:
Name: aciū.lt
Address: 91.224.135.41
```

Kadangi nematome subnet mask'o, tai iš IP adreso galime spėti jog čia yra A klasės IPv4 adresas.

**20.nslookup komanda raskite kuriais IPv4 adresais galima pasiekti domeno aciū.lt IPv4 adresą(-us) naudodami VeriSign šakninio serverio adresą 198.41.0.4. Pakomentuokite gautus rodiklius.**

```
C:\Users\Miautawn>nslookup aciū.lt 198.41.0.4
in-addr.arpa    nameserver = e.in-addr-servers.arpa
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
e.in-addr-servers.arpa internet address = 203.119.86.101
e.in-addr-servers.arpa AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa internet address = 193.0.9.1
f.in-addr-servers.arpa AAAA IPv6 address = 2001:67c:e0::1
d.in-addr-servers.arpa internet address = 200.10.60.53
d.in-addr-servers.arpa AAAA IPv6 address = 2001:13c7:7010::53
c.in-addr-servers.arpa internet address = 196.216.169.10
c.in-addr-servers.arpa AAAA IPv6 address = 2001:43f8:110::10
b.in-addr-servers.arpa internet address = 199.253.183.183
b.in-addr-servers.arpa AAAA IPv6 address = 2001:500:87::87
a.in-addr-servers.arpa internet address = 199.180.182.53
a.in-addr-servers.arpa AAAA IPv6 address = 2620:37:e000::53
Server:  UnKnown
Address:  198.41.0.4

Name:     aciū.lt
Served by:
- a.tld.lt
    195.8.218.131
    lt
- b.tld.lt
    194.0.20.1
    2001:678:19::1
    lt
- e.tld.lt
    194.0.18.1
    lt
- d.tld.lt
    194.0.3.1
    2001:678:6::1
    lt
- c.tld.lt
    194.0.1.4
    2001:678:4::4
    lt
- f.tld.lt
    194.0.19.1
    2001:678:8c::1
    lt
```

IPv4 adresai – 195.8.218.131, 194.0.20.1, 194.0.18.1, 194.0.3.1, 194.0.1.4, 194.0.19.1.

Tačiau, šie adresai niekur neveda, todėl gali būti kad šio šakninio serverio duomenys yra pasenę.



**21.netstat komanda pateikite savo darbo kompiuterio IPv4 statistiką.  
Aprašykite trumpai kiekvieną rodiklį, kurio reikšmė > 0.**

```
C:\Users\Miautawn>netstat -sp IP

IPv4 Statistics

Packets Received                = 3019011
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 55
Received Packets Discarded      = 4070
Received Packets Delivered      = 3048351
Output Requests                 = 3119909
Routing Discards                = 0
Discarded Output Packets        = 108
Output Packet No Route          = 0
Reassembly Required             = 0
Reassembly Successful           = 0
Reassembly Failures             = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created               = 0
```

*Packets Received* – kiek paketų viso gauta.

*Unknown Protocols Received* – kiek paketų buvo gauta ir atmesta dėl nežinomų arba nepalaikomų protokolų.

*Received Packets Discarded* – kiek gautų paketų buvo atmesta.

*Received Packets Delivered* – kiek iš viso gautų paketų buvo priimta.

*Output Requests* – kiek iš viso buvo sukurta atsako paketų užklausų.

*Discarded Output Packets* – kiek buvo sukurtų atsako paketų, kurie negalėjo būti išsiųsti.

**22. Kurią netstat komandą paleisite, kad gautumėte visų išsiųstų segmentų skaičių?**

```
C:\Users\Miautawn>netstat -sp TCP

TCP Statistics for IPv4

Active Opens                = 10098
Passive Opens               = 22
Failed Connection Attempts  = 6098
Reset Connections           = 968
Current Connections         = 33
Segments Received           = 830050
Segments Sent                = 740002
Segments Retransmitted      = 24236
```

*netstat -sp TCP*. Segmentų skaičius bus indikuotas „Segments Sent“ lauke.

**23. Kurią netstat komandą paleisite, kad CMD pateiktų jums visų esamų sesijų sąrašą?**

*netstat -na*.

```
C:\Users\Miautawn>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING
TCP   0.0.0.0:5040            0.0.0.0:0               LISTENING
TCP   0.0.0.0:7680            0.0.0.0:0               LISTENING
TCP   0.0.0.0:8733            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49664           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49665           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49666           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49667           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49668           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49689           0.0.0.0:0               LISTENING
```

**24. Naudojantis netstat komanda aprašykite savo darbo kompiuterio aktyvias sesijas – kurios darbo kompiuterio aplikacijos naudoja šias sesijas?**

```
C:\Windows\system32>netstat -b

Active Connections

  Proto Local Address          Foreign Address         State
  TCP    127.0.0.1:50572         DESKTOP-KC8T8NT:65001  ESTABLISHED
[nvcontainer.exe]
  TCP    127.0.0.1:50617         DESKTOP-KC8T8NT:50678  ESTABLISHED
[NVIDIA Web Helper.exe]
  TCP    127.0.0.1:50678         DESKTOP-KC8T8NT:50617  ESTABLISHED
[NVIDIA Share.exe]
  TCP    127.0.0.1:57405         DESKTOP-KC8T8NT:57406  ESTABLISHED
[firefox.exe]
  TCP    127.0.0.1:57406         DESKTOP-KC8T8NT:57405  ESTABLISHED
[firefox.exe]
  TCP    127.0.0.1:57410         DESKTOP-KC8T8NT:57411  ESTABLISHED
[firefox.exe]
  TCP    127.0.0.1:57411         DESKTOP-KC8T8NT:57410  ESTABLISHED
[firefox.exe]
  TCP    127.0.0.1:65001         DESKTOP-KC8T8NT:50572  ESTABLISHED
```

Šias sesijas naudojančios programos yra: Discord, Nvidia services, Firefox, Windows services ir t.t.

**25. Naudodami netstat komandą pateikite sąrašą IPv4 adresų, prie kurių yra jungiamasi 443 prievadu.**

```
C:\Windows\system32>netstat -an | findstr :443
  TCP    192.168.0.39:53669      162.159.137.232:443    ESTABLISHED
  TCP    192.168.0.39:53738      20.199.120.85:443      ESTABLISHED
  TCP    192.168.0.39:55011      13.32.99.21:443        CLOSE_WAIT
  TCP    192.168.0.39:55018      13.32.99.21:443        CLOSE_WAIT
  TCP    192.168.0.39:55472      13.32.99.21:443        CLOSE_WAIT
  TCP    192.168.0.39:57418      54.149.156.115:443     ESTABLISHED
  TCP    192.168.0.39:57453      23.64.12.72:443        CLOSE_WAIT
  TCP    192.168.0.39:58533      162.159.129.235:443    ESTABLISHED
  TCP    192.168.0.39:61608      162.159.134.234:443    ESTABLISHED
  TCP    192.168.0.39:61615      162.159.130.235:443    ESTABLISHED
  TCP    192.168.0.39:63092      162.159.137.234:443    ESTABLISHED
```

Galima surasti su komanda `netstat -an | findstr :443`

**26.netstat komanda nuskenaukite visus darbo kompiuterio atvirus/prieinamus prievadus. Kaip juos galima „uždaryti“? Kam, pagal saugumo rekomendacijas, rekomenduojama visuomet turėti „uždarytus“/nenaudojamus prievadus?**

```
C:\Users\Miautawn>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:5040             0.0.0.0:0               LISTENING
TCP   0.0.0.0:7680             0.0.0.0:0               LISTENING
TCP   0.0.0.0:8733             0.0.0.0:0               LISTENING
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49666            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49667            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49668            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49689            0.0.0.0:0               LISTENING
```

Tai galime padaryti su ta pačia *netstat -an* komanda, ir pažiūrėti kurie portai yra „LISTENING“

Atvirus portus palikti atdarus yra gan pavojinga, nes tuomet mūsų tinklas yra atviras nenorimiems prisijungimams. Uždaryti juos galime paprasčiausiai su Windows Firewall jeigu kalbame apie kompiuterio atvirus portus, tačiau verta įsitikinti kad ir router'io nenaudojami prievadai būtų išjungti.

**27.Naudodamiesi arp komanda pateikite savo darbo kompiuterio ARP lentelę. Ką nurodo fizinis kompiuterio adresas ff-ff-ff-ff-ff-ff? Kodėl vieni adresai yra dinaminiai, o kiti – statiniai?**

```
C:\Windows\system32>arp -a

Interface: 192.168.0.39 --- 0x6
    Internet Address      Physical Address         Type
192.168.0.1               f0-b4-d2-c8-1f-fe       dynamic
192.168.0.255             ff-ff-ff-ff-ff-ff       static
224.0.0.2                 01-00-5e-00-00-02       static
224.0.0.22                01-00-5e-00-00-16       static
224.0.0.251               01-00-5e-00-00-fb       static
224.0.0.252               01-00-5e-00-00-fc       static
239.192.152.143           01-00-5e-40-98-8f       static
239.255.255.250           01-00-5e-7f-ff-fa       static
255.255.255.255           ff-ff-ff-ff-ff-ff       static
```

ff-ff-ff-ff-ff-ff adresas indikuoja *broadcast'o adresas*. Šiam adresui skirti paketai bus pasiunčiami visiems kai jis eis per switch/router, tam kad būtų surastas norimas adresatas pagal kažkokį IP adresą.

Statiniai MAC adresai konfigūruoti rankomis ir dažnai yra tikimasi jog jie nesikeis, o dinaminiai MAC adresai, priešingai negu dinaminiai, turi savo gyvavimo laiką ir kartais gali būti išmokti automatiškai.

**28.Naudodamiesi arp komanda pridėkite savo darbo kompiuterio ARP lentelėje naują įrašą „192.168.12.12 01-00-5e-00-00-16“. Jei dėl administratoriaus teisių apribojimų neleidžia to padaryti OS, tuomet parašykite pilną komandos tekstą.**

```
C:\Windows\system32>arp -s 192.168.12.12 01-00-5e-00-00-16  
C:\Windows\system32>arp -a  
Interface: 192.168.0.39 --- 0x6  
Internet Address      Physical Address      Type  
192.168.0.1           f0-b4-d2-c8-1f-fe    dynamic  
192.168.0.255         ff-ff-ff-ff-ff-ff    static  
192.168.12.12         01-00-5e-00-00-16    static  
224.0.0.2             01-00-5e-00-00-02    static  
224.0.0.22            01-00-5e-00-00-16    static  
224.0.0.251           01-00-5e-00-00-fb    static  
224.0.0.252           01-00-5e-00-00-fc    static  
239.192.152.143       01-00-5e-40-98-8f    static  
239.255.255.250       01-00-5e-7f-ff-fa    static  
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```