Øving 9

Jakob Lønnerød Madsen, Pascal Pickel, & Sebastian Ikin

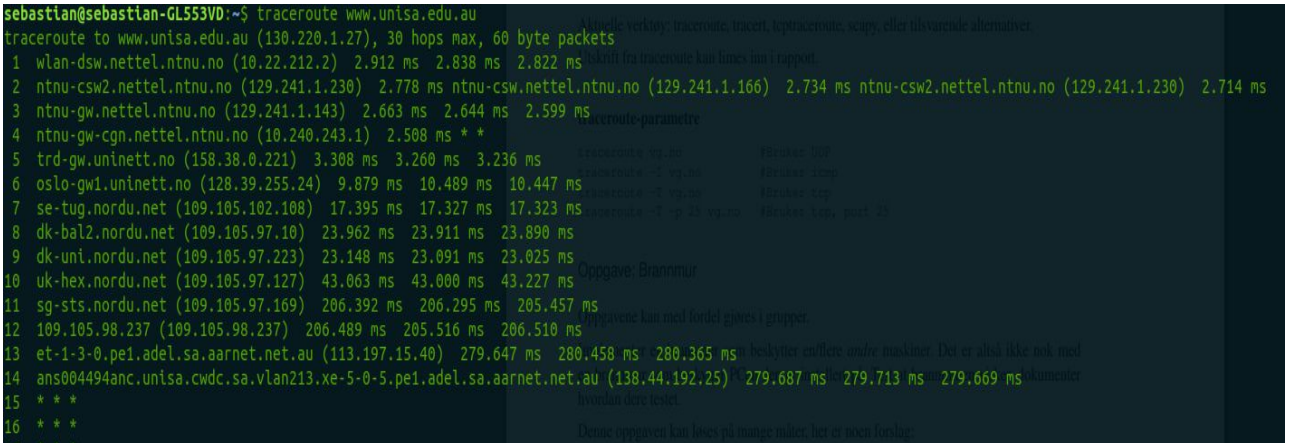
Oppgave Traceroute:
Her er traceroutes fra windows pc som sitter i eduroam nettverket. Windows traceroute bruker icmp protokoll.

```
C:\WINDOWS\system32>tracert ntnu.no

Tracing route to ntnu.no [2001:700:300:6::102]
over a maximum of 30 hops:

  1     4 ms     2 ms     2 ms  wlan-dsw.nettel.ntnu.no [2001:700:300:4003::2]
  2     2 ms     2 ms     2 ms  ntnu-csw.nettel.ntnu.no [2001:700:300::2e26]
  3     2 ms     2 ms     2 ms  dc-gsw2.nettel.ntnu.no [2001:700:300::2e03]
  4     2 ms     2 ms     2 ms  lvs160vip02.it.ntnu.no [2001:700:300:6::102]

Trace complete.
```

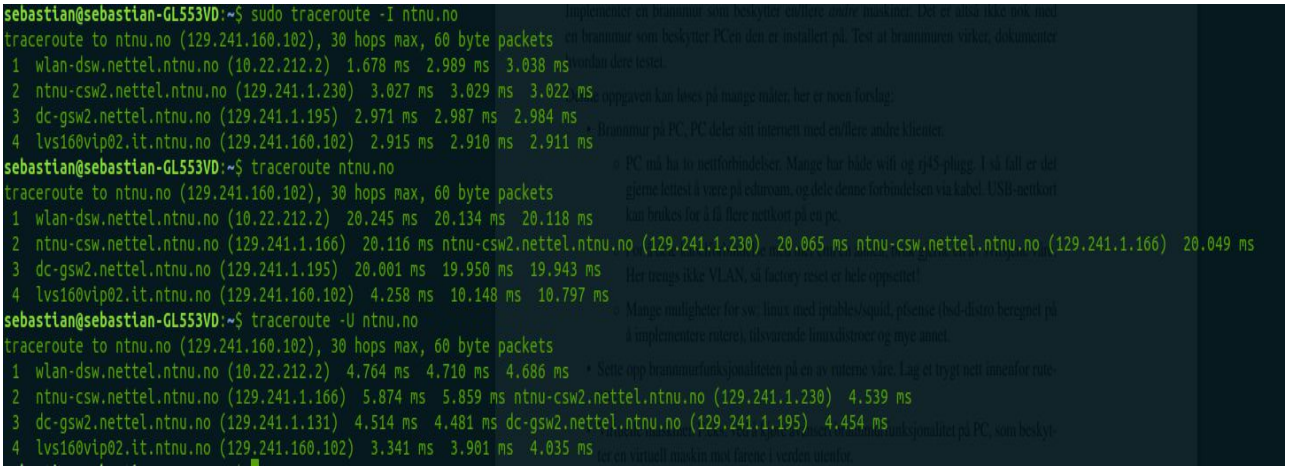
```
C:\WINDOWS\system32>tracert db.no

Tracing route to db.no [2a02:c0:ac:3:db::183]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  wlan-dsw.nettel.ntnu.no [2001:700:300:4003::2]
  2     8 ms    12 ms     2 ms  ntnu-csw.nettel.ntnu.no [2001:700:300::2e26]
  3     2 ms     2 ms     3 ms  2001:700:300::2e0b
  4     2 ms     2 ms     2 ms  trd-gw.uninett.no [2001:700:0:8001::1]
  5     *       10 ms    11 ms  oslo-gw1.uninett.no [2001:700:0:203f::1]
  6     9 ms     9 ms    10 ms  xe-2-1-0.cr1-osl3.n.bitbit.net [2001:7f8:12:1::3:9029]
  7    10 ms    10 ms    10 ms  swp3.c1-osl2.n.bitbit.net [2a02:c0:1:1::4]
  8    25 ms    37 ms    26 ms  lo.s2-a8-osl3.n.bitbit.net [2a02:c0:1::4:1]
  9    37 ms    32 ms    52 ms  2a02:c0:ac:3:db::183

Trace complete.
```

```
C:\WINDOWS\system32>tracert www.unisa.edu.au

Tracing route to www.unisa.edu.au [130.220.1.27]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  wlan-dsw.nettel.ntnu.no [10.22.12.2]
  2     2 ms     2 ms     2 ms  ntnu-csw2.nettel.ntnu.no [129.241.1.230]
  3     3 ms     2 ms     2 ms  ntnu-gw.nettel.ntnu.no [129.241.1.207]
  4     2 ms     *        2 ms  ntnu-gw-cgn.nettel.ntnu.no [10.240.243.1]
  5     3 ms    19 ms     4 ms  trd-gw.uninett.no [158.38.0.221]
  6     9 ms     9 ms     9 ms  oslo-gw1.uninett.no [128.39.255.24]
  7    17 ms    17 ms    17 ms  se-tug.nordu.net [109.105.102.108]
  8    24 ms    25 ms    23 ms  dk-bal2.nordu.net [109.105.97.10]
  9    23 ms    23 ms    25 ms  dk-uni.nordu.net [109.105.97.223]
 10    43 ms    42 ms    43 ms  uk-hex.nordu.net [109.105.97.127]
 11   210 ms   210 ms   206 ms  sg-sts.nordu.net [109.105.97.169]
 12   207 ms   206 ms   209 ms  109.105.98.237
 13   281 ms   279 ms   278 ms  et-1-3-0.pe1.adel.sa.aarnet.net.au [113.197.15.40]
 14   279 ms   279 ms   278 ms  ans004494anc.unisa.cwdc.sa.vlan213.xe-5-0-5.pe1.adel.sa.aarnet.
net.au [138.44.192.25]
 15     *        *        *     Request timed out.
 16   283 ms   282 ms   280 ms  universityofsouthaustralia.college [130.220.1.27]

Trace complete.
```

Her er traceroute med forskjellige protokoller fra ubuntu maskin. Vi ser at noen av disse ikke ikke virket med standardprotokoll. Under ser du en blokkert traceroute til unisa.edu.au

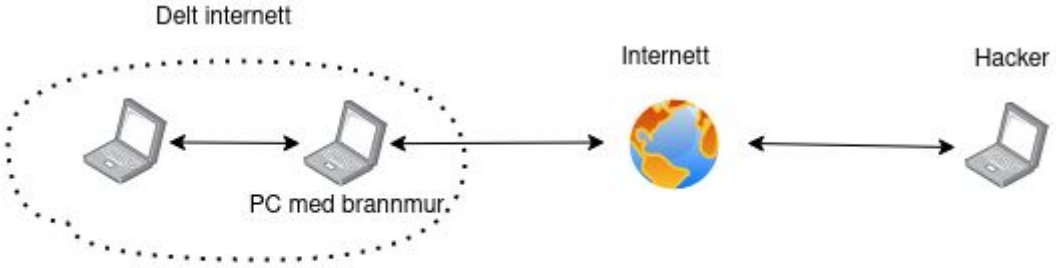


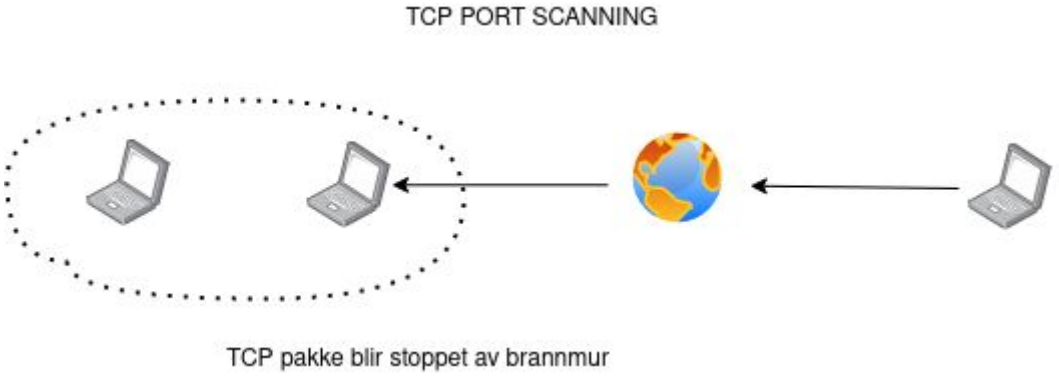
Traceroute med forskjellige flagg til ntnu.no.



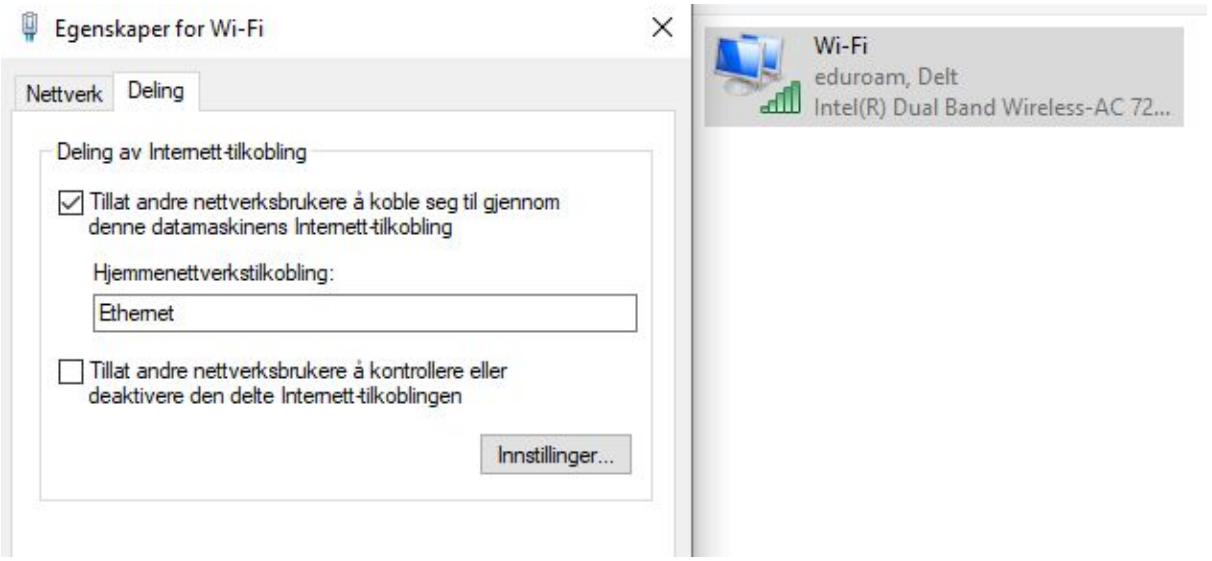
Oppgave Brannmur:

Vi delte eduroam nettverk gjennom en windows maskin. Vi hadde koblet til en ruter som grovt sagt bare ble brukt til en switch, men er teoretisk sett et ekstra lag med en brannmur og forskjellige nettverksregler.
Brannmuren på windows maskin var default windows brannmur konfigurert med eset smart security.





På windows var det veldig enkelt å dele wifi nett til ethernet.



Under ser du at nettverket fra Sebastians pc må igjennom Pascal for å koble til internett for å koble til vg. Her blir vi også blokkert.

```
sebastian@sebastian-GL553VD:~$ traceroute vg.no
traceroute to vg.no (195.88.55.16), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.536 ms  0.883 ms  0.817 ms
 2  Pascal-PC.mshome.net (192.168.137.1)  2.950 ms * *
 3  * * *
 4  wlan-dsw.nettel.ntnu.no (10.22.12.2)  5.279 ms  5.389 ms  5.362 ms
 5  ntnu-csw2.nettel.ntnu.no (129.241.1.230)  5.498 ms  5.471 ms ntnu-csw.nettel.ntnu.no (129.241.1.166)  5.603 ms
 6  ntnu-gw.nettel.ntnu.no (129.241.1.143)  5.693 ms  3.280 ms  3.665 ms
 7  * ntnu-gw-cgn.nettel.ntnu.no (10.240.243.1)  3.513 ms *
 8  trd-gw.uninett.no (158.38.0.221)  5.019 ms  5.080 ms  5.187 ms
 9  te5-0-0-150.trondh-prinsg39-pe2.as2116.net (193.156.93.3)  6.100 ms  6.160 ms  6.122 ms
10  te4-2-1.ar1.prinsg39.as2116.net (195.0.245.59)  13.746 ms  12.210 ms  12.265 ms
11  ae4.cr1.prinsg39.as2116.net (195.0.242.184)  17.936 ms  18.095 ms  17.662 ms
12  ae9.cr2.fn3.as2116.net (193.90.113.16)  13.351 ms  13.132 ms  12.282 ms
13  he3-0-2.ar2.ulv89.as2116.net (195.0.241.55)  12.522 ms  12.333 ms  11.680 ms
14  * * *
15  * * *
```

Ved nmap vil brannmuren blokkere alle TCP forespørseler.


```
madsen@MadsenPc:~/Documents/dataing/TDAT3020 Sikkerhet i programvare og nettverk/ovinger/oving8$ sudo nmap 10.22.12.218
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 11:12 CEST
Nmap scan report for dhcp-10-22-12-218.wlan.ntnu.no (10.22.12.218)
Host is up (0.0037s latency).
All 1000 scanned ports on dhcp-10-22-12-218.wlan.ntnu.no (10.22.12.218) are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

Her ser vi forskjell på en brannmur som blokkerer (øverst) og en brannmur som er åpen (nederst)

```
madsen@MadsenPc:~/Documents/dataing/TDAT3020 Sikkerhet i programvare og nettverk/ovinger/oving8$ ping 10.22.12.218
PING 10.22.12.218 (10.22.12.218) 56(84) bytes of data.
^C
--- 10.22.12.218 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7149ms

madsen@MadsenPc:~/Documents/dataing/TDAT3020 Sikkerhet i programvare og nettverk/ovinger/oving8$ ping 10.22.12.218
PING 10.22.12.218 (10.22.12.218) 56(84) bytes of data.
64 bytes from 10.22.12.218: icmp_seq=1 ttl=127 time=3.90 ms
64 bytes from 10.22.12.218: icmp_seq=2 ttl=127 time=4.31 ms
64 bytes from 10.22.12.218: icmp_seq=3 ttl=127 time=3.98 ms
64 bytes from 10.22.12.218: icmp_seq=4 ttl=127 time=4.51 ms
64 bytes from 10.22.12.218: icmp_seq=5 ttl=127 time=4.20 ms
64 bytes from 10.22.12.218: icmp_seq=6 ttl=127 time=3.85 ms
64 bytes from 10.22.12.218: icmp_seq=7 ttl=127 time=3.65 ms
64 bytes from 10.22.12.218: icmp_seq=8 ttl=127 time=4.37 ms
64 bytes from 10.22.12.218: icmp_seq=9 ttl=127 time=4.08 ms
64 bytes from 10.22.12.218: icmp_seq=10 ttl=127 time=4.05 ms
64 bytes from 10.22.12.218: icmp_seq=11 ttl=127 time=3.77 ms
64 bytes from 10.22.12.218: icmp_seq=12 ttl=127 time=4.03 ms
64 bytes from 10.22.12.218: icmp_seq=13 ttl=127 time=4.13 ms
64 bytes from 10.22.12.218: icmp_seq=14 ttl=127 time=4.22 ms
64 bytes from 10.22.12.218: icmp_seq=15 ttl=127 time=3.95 ms
c64 bytes from 10.22.12.218: icmp_seq=16 ttl=127 time=3.81 ms
64 bytes from 10.22.12.218: icmp_seq=17 ttl=127 time=3.88 ms
64 bytes from 10.22.12.218: icmp_seq=18 ttl=127 time=3.82 ms
^C
--- 10.22.12.218 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17026ms
rtt min/avg/max/mdev = 3.648/4.028/4.513/0.223 ms
```