

Administrowanie systemami sieciowymi

Sprawozdanie z laboratorium

Data	Tytuł zajęć	Uczestnicy
22.12.2020 11:15	Konfiguracja i monitorowanie sieci; zdalny dostęp	Bartosz Rodziewicz (226105)

Opis środowiska

Zajęcia laboratoryjne z części nt. systemu Linux zostały wykonane na maszynie wirtualnej postawionej z wykorzystaniem VirtualBox. Zainstalowana w maszynie dystrybucja to Manjaro 20.2 ze środowiskiem (DE) KDE Plasma. Do zajęć użyta została czysta instalacja systemu po doinstalowaniu najnowszych aktualizacji pakietów. W wielu miejscach używany jest alias `ll`, który jest aliasem na `ls -aIf`.

Przebieg laboratorium

Zainstalować i uruchomić serwer (demon) `ssh`.

Po instrukcji laboratoryjnej nr 1 w systemie jest zainstalowany pakiet `openssh`. Poniżej widać uruchomienie serwera.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo systemctl start sshd
[sudo] password for baatochan:
[baatochan@baatochan-virtualbox Desktop]$
```

Określić adres sprzętowy interfejsu sieciowego (karty sieciowej) i bazując na tej informacji ustalić jego producenta.

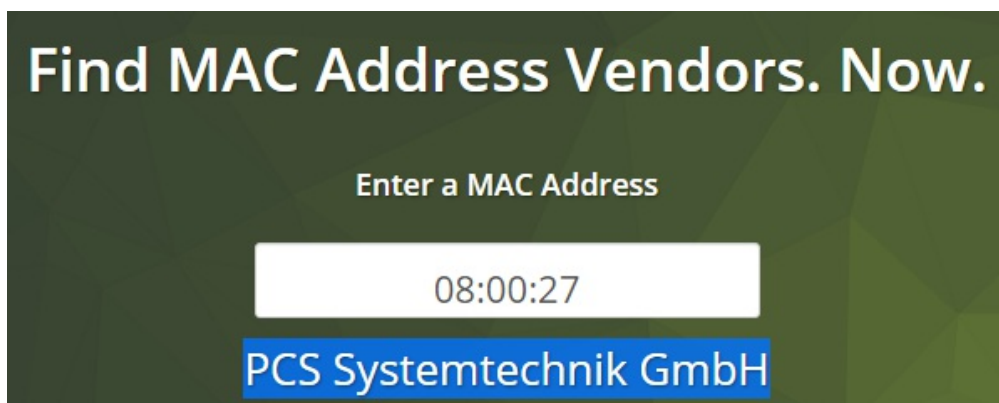
Adres sprzętowy (MAC) odpowiedniego interfejsu można sprawdzić za pomocą komendy `ifconfig`, co widać na poniższym zrzucie.

```
[baatochan@baatochan-virtualbox Desktop]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.58 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::9352:df68:3f31:71f0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:04:62:ae txqueuelen 1000 (Ethernet)
    RX packets 5167 bytes 7079554 (6.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 503 bytes 44578 (43.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 12468 (12.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 12468 (12.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[baatochan@baatochan-virtualbox Desktop]$
```

Producenta interfejsu sieciowego można sprawdzić korzystając z 6 pierwszych cyfr adresu MAC, w tym wypadku `08:00:27`. Sprawdzenie producenta jest możliwe na wielu stronach internetowych, np. macvendors.com.



"Producentem" karty o adresie `08:00:27` jest firma PCS Systemtechnik GmbH. Trzeba wziąć jednak pod uwagę, że jest to karta wirtualna, wygenerowana przez VirtualBox i jej adres MAC jest najprawdopodobniej losowy.

Zapoznać się z konfiguracją interfejsu sieciowego (karty sieciowej). Dodać i skonfigurować nowy pseudointerfejs (wraz z adresem, żeby odpowiadał na 'pingi').

Konfigurację interfejsu można poznać za pomocą komendy `ifconfig`, której zrzut jest widoczny w poprzednim zadaniu.

Aby dodać pseudointerfejs można użyć komendy `ifconfig`. Dodanie interfejsu bazującego na innym wymaga użycia komendy: `ifconfig <nazwa_int>:<nr> <adres ip>`. Wykonanie tej komendy widać na poniższym zrzucie.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo ifconfig enp0s3:0 192.168.1.169
[sudo] password for baatochan:
[baatochan@baatochan-virtualbox Desktop]$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.58 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::9352:df68:3f31:71f0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:04:62:ae txqueuelen 1000 (Ethernet)
    RX packets 9701 bytes 8152527 (7.7 MiB)
    RX errors 0 dropped 4 overruns 0 frame 0
    TX packets 1388 bytes 103700 (101.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.169 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:04:62:ae txqueuelen 1000 (Ethernet)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 12468 (12.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 12468 (12.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[baatochan@baatochan-virtualbox Desktop]$ ping 192.168.1.169
PING 192.168.1.169 (192.168.1.169) 56(84) bytes of data.
64 bytes from 192.168.1.169: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 192.168.1.169: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 192.168.1.169: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 192.168.1.169: icmp_seq=4 ttl=64 time=0.033 ms
64 bytes from 192.168.1.169: icmp_seq=5 ttl=64 time=0.032 ms
64 bytes from 192.168.1.169: icmp_seq=6 ttl=64 time=0.034 ms
64 bytes from 192.168.1.169: icmp_seq=7 ttl=64 time=0.042 ms
64 bytes from 192.168.1.169: icmp_seq=8 ttl=64 time=0.035 ms
^C
--- 192.168.1.169 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7103ms
rtt min/avg/max/mdev = 0.030/0.034/0.042/0.003 ms
[baatochan@baatochan-virtualbox Desktop]$ sudo ifconfig enp0s3:0 down
[baatochan@baatochan-virtualbox Desktop]$
```

Na powyższym zrzucie widać też, że interfejs odpowiada na pingi oraz komendę na wyłączenie takiego interfejsu. Taki pseudointerfejs odpowiadał również na pingi z innego hosta co widać poniżej (WSL na komputerze będącym hostem VM). Pingi zostały oczywiście wysłane przed wyłączeniem interfejsu.

```
[baatochan@BARTOSZ-PC:/mnt/c/git/UniversityStuff (ass-lab7)]$ ping 192.168.1.169
PING 192.168.1.169 (192.168.1.169) 56(84) bytes of data.
64 bytes from 192.168.1.169: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.1.169: icmp_seq=2 ttl=64 time=0.439 ms
64 bytes from 192.168.1.169: icmp_seq=3 ttl=64 time=0.524 ms
64 bytes from 192.168.1.169: icmp_seq=4 ttl=64 time=0.802 ms
^C
--- 192.168.1.169 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.439/0.697/1.025/0.233 ms
[baatochan@BARTOSZ-PC:/mnt/c/git/UniversityStuff (ass-lab7 %)]$
```

Dla trzech wybranych węzłów w sieci Internet (Polska, Europa, Świat):

- określić średni czas potrzebny na osiągnięcie węzła przez pakiet
- zbadać trasę jaką są przesyłane pakiety do podanego węzła
- określić maksymalny rozmiar pakietu, dla którego węzeł docelowy "odpowiada"

Węzeł Polska - Radio rmf.fm

Określić średni czas potrzebny na osiągnięcie węzła przez pakiet

Można to określić za pomocą komendy `ping` lub wspomnianego przeze mnie w kolejnym punkcie pakietu `mtr`.

```

64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=25 ttl=52 time=10.4 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=26 ttl=52 time=9.87 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=27 ttl=52 time=10.5 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=28 ttl=52 time=10.1 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=29 ttl=52 time=10.2 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=30 ttl=52 time=10.0 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=31 ttl=52 time=10.3 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=32 ttl=52 time=10.6 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=33 ttl=52 time=13.7 ms
64 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=34 ttl=52 time=10.3 ms
^C
--- rmfm.fm ping statistics ---
34 packets transmitted, 34 received, 0% packet loss, time 33053ms
rtt min/avg/max/mdev = 9.865/10.650/13.688/0.806 ms
[baatochan@baatochan-virtualbox Desktop]$

```

Po komendzie `ping` widać, że średni czas to 10.65s.

Zbadać trasę jaką są przesyłane pakiety do podanego węzła

Trasę do konkretnego węzła można sprawdzić za pomocą komendy `tracert` lub `mtr`. Zalecaną metodą jest komenda `mtr`, ponieważ dzięki temu, że łączy ona w sobie funkcjonalność `ping` to wyniki z niej często prezentują więcej informacji (pakiety rzadziej są blokowane przez firewall).

```

baatochan-virtualbox (192.168.1.58) -> rmfm.fm
My traceroute [v0.94]
2021-01-10T04:56:50+0100
Keys: Help Display mode Restart statistics Order of fields quit

Host      Loss%  Snt   Last   Avg    Best  Wrst  StDev
1. netiaspot.local
2. (waiting for reply)
3. (waiting for reply)
4. host-87-99-33-89.internetia.net.pl
5. 83.238.251.231
6. kato001rt02.inetia.pl
7. 87.204.225.23
8. 87.204.225.170
9. jawo001rt11.inetia.pl
10. krakh001rt11.inetia.pl
11. static-81-219-183-234.devs.futuro.pl
12. 217.74.64.200
13. mike.rmfm.pl

```

Powyżej widzimy trasę do serwera rmfm.fm. Cała trasa znajduje się w obrębie sieci Netii (futuro.pl to sieć Netii, przedostatni węzeł się nie zidentyfikował).

Określić maksymalny rozmiar pakietu, dla którego węzeł docelowy "odpowiada"

Do określenia rozmiaru maksymalnego pakietu na który dany serwer odpowiada, można użyć komendy `ping` z parametrem `-s`.

Serwer rmfm.fm odpowiada na pakiet o wielkości 65535, czyli największy rozmiar jaki może mieć pakiet IP.

```

[baatochan@baatochan-virtualbox Desktop]$ ping -s 65507 rmfm.fm
PING rmfm.fm (217.74.66.211) 65507(65535) bytes of data.
65515 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=1 ttl=52 time=27.5 ms
65515 bytes from mike.rmfm.pl (217.74.66.211): icmp_seq=2 ttl=52 time=18.5 ms
^C
--- rmfm.fm ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 18.473/22.969/27.465/4.496 ms
[baatochan@baatochan-virtualbox Desktop]$ ping -s 65508 rmfm.fm
PING rmfm.fm (217.74.66.211) 65508(65536) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
^C
--- rmfm.fm ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1022ms
[baatochan@baatochan-virtualbox Desktop]$

```

Węzeł Europa - Technische Universität Berlin tu.berlin

```

baatochan-virtualbox (192.168.1.58) -> tu.berlin
My traceroute [v0.94]
2021-01-10T05:23:00+0100
Keys: Help Display mode Restart statistics Order of fields quit

Host      Loss%  Snt   Last   Avg    Best  Wrst  StDev
1. netiaspot.local
2. (waiting for reply)
3. (waiting for reply)
4. host-87-99-33-89.internetia.net.pl
5. krakh001rt09.inetia.pl
6. lag-108.bear1.Prague1.Level3.net
7. ae-0-4.bar1.Hamburg1.Level3.net
8. 195.122.181.62
9. cr-tub2-be13.x-win.dfn.de
10. kr-tub87-4.x-win.dfn.de
11. e-ns-e-n.gate.tu-berlin.de
12. tu.berlin

```


Określić średni czas potrzebny na osiągnięcie węzła przez pakiet

Z powyższego zrzutu widać, że średni czas pakietu to 33.3s.

Zbadać trasę jaką są przesyłane pakiety do podanego węzła

Trasa do węzła tu.berlin prowadzi przez sieć operatora Netia (mój ISP), przez Pragę i Hamburg (sieć amerykańskiej korporacji telekomunikacyjnej Lumen Technologies), później przez sieć DFN (Niemiecka Sieć Uniwersytecka), aż do bramy uniwersytetu TU, który zdaje się samemu hostować swoją stronę.

Określić maksymalny rozmiar pakietu, dla którego węzeł docelowy "odpowiada"

```
[baatochan@baatochan-virtualbox Desktop]$ ping -s 65507 tu.berlin
PING tu.berlin (130.149.8.20) 65507(65535) bytes of data.
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=1 ttl=240 time=53.3 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=2 ttl=240 time=48.2 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=3 ttl=240 time=50.8 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=4 ttl=240 time=48.5 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=5 ttl=240 time=48.8 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=6 ttl=240 time=48.1 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=7 ttl=240 time=42.7 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=8 ttl=240 time=48.7 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=9 ttl=240 time=58.4 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=10 ttl=240 time=49.5 ms
65515 bytes from tu.berlin (130.149.8.20): icmp_seq=11 ttl=240 time=48.7 ms
^C
--- tu.berlin ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 42.747/49.614/58.353/3.641 ms
[baatochan@baatochan-virtualbox Desktop]$
```

Serwer tu.berlin odpowiada na pakiet o wielkości 65535, czyli największy rozmiar jaki może mieć pakiet IP.

Węzeł Świat - amtrack.com

Planowałem opisać ścieżkę do strony amerykańskich kolei Amtrak, jednak dopiero po skończeniu opisywania całego zadania zobaczyłem, że opisałem stronę amtrack.com, która przekierowuje na pustą stronę railroad-usa.com.

```
My traceroute [v0.94]
baatochan-virtualbox (192.168.1.58) -> amtrack.com
2021-01-10T05:38:15+0100
Keys: Help Display mode Restart statistics Order of fields quit

  Packets
Host Loss% Snt Last Avg Best Wrst StDev
1. netiaspot.local 0.0% 287 1.1 1.4 0.9 12.9 0.9
2. (waiting for reply)
3. (waiting for reply)
4. host-87-99-33-89.internetia.net.pl 0.0% 286 3.0 6.4 1.9 13.0 2.4
5. krakh001rt09.inetia.pl 0.0% 286 12.9 9.9 5.5 15.9 2.3
6. lag-108.bear1.Prague1.Level3.net 83.5% 286 25.6 26.0 25.1 30.2 0.8
7. ae-24-24.bear1.Phoenix1.Level3.net 97.2% 286 160.5 161.0 160.5 162.1 0.5
8. ae6.ibrma1205-02.phx3.bb.godaddy.com 0.0% 286 161.1 162.6 160.4 205.7 5.3
9. (waiting for reply)
10. 148.72.32.5 0.0% 286 173.3 163.2 160.9 197.8 4.4
11. ip-184-168-0-113.ip.secureserver.net 0.0% 286 171.0 171.5 170.6 180.4 0.8
12. ip-184-168-1-134.ip.secureserver.net 0.0% 286 171.6 171.9 170.8 185.6 1.3
13. ip-184-168-131-241.ip.secureserver.net 0.0% 286 186.4 172.1 170.9 196.4 2.5
```

Określić średni czas potrzebny na osiągnięcie węzła przez pakiet

Z powyższego zrzutu widać, że średni czas pakietu to 172.1s.

Zbadać trasę jaką są przesyłane pakiety do podanego węzła

Trasa do serwera amtrack.com odbywa się bez użycia CDN. Najpierw oczywiście jest sieć Netii, później pakiety idą przez Pragę oraz Phoenix (sieć Lumen Technologies), następnie przez sieć GoDaddy, kończąc w sieci Wild West Domains (które może być powiązane z GoDaddy), która hostuje stronę amtrack.

Określić maksymalny rozmiar pakietu, dla którego węzeł docelowy "odpowiada"

```
[baatochan@baatochan-virtualbox Desktop]$ ping -s 35321 amtrack.com
PING amtrack.com (184.168.131.241) 35321(35349) bytes of data.
^C
--- amtrack.com ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8106ms

[baatochan@baatochan-virtualbox Desktop]$ ping -s 35320 amtrack.com
PING amtrack.com (184.168.131.241) 35320(35348) bytes of data.
35328 bytes from ip-184-168-131-241.ip.secureserver.net (184.168.131.241): icmp_seq=4 ttl=43 time=185 ms
35328 bytes from ip-184-168-131-241.ip.secureserver.net (184.168.131.241): icmp_seq=5 ttl=43 time=186 ms
35328 bytes from ip-184-168-131-241.ip.secureserver.net (184.168.131.241): icmp_seq=7 ttl=43 time=188 ms
35328 bytes from ip-184-168-131-241.ip.secureserver.net (184.168.131.241): icmp_seq=8 ttl=43 time=184 ms
^C
--- amtrack.com ping statistics ---
8 packets transmitted, 4 received, 50% packet loss, time 7051ms
rtt min/avg/max/mdev = 183.760/185.783/188.384/1.664 ms
[baatochan@baatochan-virtualbox Desktop]$
```

Zarejestrować i zapisać do pliku (za pomocą `tcpdump`) wszystkie pakiety związane z:

testowaniem za pomocą polecenia ping nieistniejącego hosta (np. niematakiegohosta.pl)

Do tego testu wykorzystana została wspomniana wyżej domena `niematakiegohosta2.pl`.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -w ping-unknown-host1
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6 packets captured
8 packets received by filter
0 packets dropped by kernel
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -r ping-unknown-host1
reading from file ping-unknown-host1, link-type EN10MB (Ethernet)
04:30:48.365486 IP baatochan-virtualbox.57943 > netiaspot.local.domain: 34760+ A? niematakiegohosta2.pl. (39)
04:30:48.365824 IP baatochan-virtualbox.57943 > netiaspot.local.domain: 3014+ AAAA? niematakiegohosta2.pl. (39)
04:30:48.424611 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:30:48.458909 IP netiaspot.local.domain > baatochan-virtualbox.57943: 3014 NXDomain 0/1/0 (96)
04:30:48.460642 IP netiaspot.local.domain > baatochan-virtualbox.57943: 34760 NXDomain 0/1/0 (96)
04:30:49.414779 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
```

Powyżej widać pakiety wysyłane przy pingowaniu nieistniejącego hosta, a dokładniej pakiety DNS - zapytanie o adres hosta oraz odpowiedź `NXDomain` wysłaną przez router.

testowaniem za pomocą polecenia ping dowolnego istniejącego hosta

Do tego testu wykorzystana została domena `tu.berlin` użyta w poprzednim ćwiczeniu. Do ćwiczenia użyta została komenda `ping` z parametrem `-c 1` by wysłany został tylko jeden pakiet ICMP.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -w ping-known-host1
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15 packets captured
15 packets received by filter
0 packets dropped by kernel
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -r ping-known-host1
reading from file ping-known-host1, link-type EN10MB (Ethernet)
04:38:32.423745 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:38:32.964939 IP baatochan-virtualbox.55677 > netiaspot.local.domain: 45558+ A? tu.berlin. (27)
04:38:32.965130 IP baatochan-virtualbox.55677 > netiaspot.local.domain: 3322+ AAAA? tu.berlin. (27)
04:38:32.968573 IP netiaspot.local.domain > baatochan-virtualbox.55677: 45558 1/0/0 A 130.149.8.20 (43)
04:38:32.979043 IP netiaspot.local.domain > baatochan-virtualbox.55677: 3322 0/1/0 (82)
04:38:32.979873 IP baatochan-virtualbox > www.static.tu.berlin: ICMP echo request, id 38, seq 1, length 64
04:38:33.012291 IP www.static.tu.berlin > baatochan-virtualbox: ICMP echo reply, id 38, seq 1, length 64
04:38:33.014601 IP baatochan-virtualbox.43664 > netiaspot.local.domain: 64497+ PTR? 20.8.149.130.in-addr.arpa. (43)
04:38:33.020212 IP netiaspot.local.domain > baatochan-virtualbox.43664: 64497 5/0/0 PTR www.static.tu.berlin., PTR t
u.berlin., PTR www.tu.berlin., PTR apply4master.studsek.tu-berlin.de., PTR go.tu.berlin. (173)
04:38:33.255090 IP Anachronos.local.xmsg > baatochan-virtualbox.42926: Flags [ ], ack 1946525814, win 501, options [
nop,nop,TS val 1937901028 ecr 1935501791], length 0
04:38:33.255121 IP baatochan-virtualbox.42926 > Anachronos.local.xmsg: Flags [ ], ack 1, win 501, options [nop,nop,T
S val 1935511818 ecr 1937895938], length 0
04:38:33.283847 ARP, Request who-has Anachronos.local tell baatochan-virtualbox, length 28
04:38:33.285035 ARP, Reply Anachronos.local is-at 60:45:cb:9a:cf:7b (oui Unknown), length 46
04:38:33.440437 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:38:33.467334 IP6 fe80::3456:f581:403c:6b1e > ff02::1:ff90:e0f2: ICMP6, neighbor solicitation, who has fe80::86f:2
bab:4f90:e0f2, length 32
```

W tym wypadku widać pakiety DNS - zapytanie o adres oraz pakiet z adresem. Później widać pakiety ICMP (żądanie i odpowiedź) oraz odwrotne zapytanie DNS i odpowiedź na nie.

rejestrowaniem trasy do dowolnego istniejącego hosta (nie odwiedzanego wcześniej) za pomocą `traceroute`.

Do tego ćwiczenia wykorzystana została domena `tum.de`, będąca domeną uczelni Technische Universität München.

Zrzuć w kolejności najpierw pierwszy wiersz lewo, później prawo, następnie drugi wiersz lewo i prawo.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -w traceroute
[sudo] password for baatochan:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C205 packets captured
205 packets received by filter
0 packets dropped by kernel
[baatochan@baatochan-virtualbox Desktop]$ sudo tcpdump -r traceroute
reading from file traceroute, link-type EN10MB (Ethernet)
04:47:22.431023 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:22.649220 ARP, Request who-has 192.168.1.57 tell netiaspot.local, length 46
04:47:23.009858 IP baatochan-virtualbox.43263 > netiaspot.local.domain: 34549+ A? tum.de. (24)
04:47:23.009961 IP baatochan-virtualbox.43263 > netiaspot.local.domain: 61946+ AAAA? tum.de. (24)
04:47:23.022073 IP netiaspot.local.domain > baatochan-virtualbox.43263: 34549 1/0/0 A 129.187.255.151 (40)
04:47:23.024881 IP netiaspot.local.domain > baatochan-virtualbox.43263: 61946 1/0/0 AAAA 2001:aca0:0:103:81bb:ff97
:52 (52)
04:47:23.025514 IP baatochan-virtualbox.40709 > www.v1.tum.de.traceroute: UDP, length 32
04:47:23.025617 IP baatochan-virtualbox.33826 > www.v1.tum.de.traceroute: UDP, length 32
04:47:23.025759 IP baatochan-virtualbox.41907 > www.v1.tum.de.33436: UDP, length 32
04:47:23.025833 IP baatochan-virtualbox.54004 > www.v1.tum.de.33437: UDP, length 32
04:47:23.025941 IP baatochan-virtualbox.56432 > www.v1.tum.de.33438: UDP, length 32
04:47:23.026041 IP baatochan-virtualbox.30798 > www.v1.tum.de.33439: UDP, length 32
04:47:23.026175 IP baatochan-virtualbox.55681 > www.v1.tum.de.33440: UDP, length 32
04:47:23.026244 IP baatochan-virtualbox.53570 > www.v1.tum.de.33441: UDP, length 32
04:47:23.026426 IP baatochan-virtualbox.53641 > www.v1.tum.de.33442: UDP, length 32
04:47:23.026493 IP baatochan-virtualbox.50491 > www.v1.tum.de.33443: UDP, length 32
04:47:23.026844 IP baatochan-virtualbox.58817 > www.v1.tum.de.33444: UDP, length 32
04:47:23.027075 IP baatochan-virtualbox.41051 > www.v1.tum.de.33445: UDP, length 32
04:47:23.027146 IP baatochan-virtualbox.55969 > www.v1.tum.de.33446: UDP, length 32
04:47:23.027220 IP baatochan-virtualbox.33191 > www.v1.tum.de.33447: UDP, length 32
04:47:23.027263 IP baatochan-virtualbox.39340 > www.v1.tum.de.33448: UDP, length 32
04:47:23.027344 IP netiaspot.local > baatochan-virtualbox: ICMP time exceeded in-transit, length 68
04:47:23.027351 IP netiaspot.local > baatochan-virtualbox: ICMP time exceeded in-transit, length 68
04:47:23.027581 IP baatochan-virtualbox.60164 > www.v1.tum.de.33449: UDP, length 32
04:47:23.027593 IP baatochan-virtualbox.39516 > netiaspot.local.domain: 25148+ PTR? 1.1.168.192.in-addr.arpa. (42)
04:47:23.028605 IP netiaspot.local > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:23.035390 IP host-87-99-33-89.internetia.net.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length
76
04:47:23.039281 IP netiaspot.local.domain > baatochan-virtualbox.39516: 25148 NXDomain 0/0/0 (42)
04:47:23.039281 IP host-87-99-33-89.internetia.net.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length
76
04:47:23.040697 IP host-87-99-33-89.internetia.net.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length
76
04:47:23.041641 IP krakh001r09.inetia.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:23.041641 IP krakh001r09.inetia.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:23.041641 IP krakh001r09.inetia.pl > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:23.144259 IP6 baatochan-virtualbox.mdns > ff02::fb.mdns: 0 PTR (QM)? 1.1.168.192.in-addr.arpa. (42)
04:47:23.144889 IP baatochan-virtualbox.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 1.1.168.192.in-addr.arpa. (42)
04:47:23.151576 IP netiaspot.local.mdns > 224.0.0.251.mdns: 0+ [0q] 1/0/0 (Cache flush) PTR netiaspot.local. (65)
04:47:23.151577 IP baatochan-virtualbox.58558 > www.v1.tum.de.33450: UDP, length 32
04:47:23.152112 IP baatochan-virtualbox.54572 > www.v1.tum.de.33451: UDP, length 32
04:47:23.152333 IP baatochan-virtualbox.47681 > netiaspot.local.domain: 50235+ PTR? 89-33-99-87.in-addr.arpa. (42)
04:47:23.413577 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:23.651423 ARP, Request who-has MSI.local tell netiaspot.local, length 46
04:47:24.419800 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:24.680511 IP 192.168.1.47.xmsg > baatochan-virtualbox.42926: Flags [ ], ack 1946525814, win 501, options [nop,
nop,TS val 1938432441 ecr 1936033213], length 0
04:47:24.680535 IP baatochan-virtualbox.42926 > 192.168.1.47.xmsg: Flags [ ], ack 1, win 501, options [nop,nop,TS va
l 1936045243 ecr 1938427342], length 0
04:47:26.199229 IP baatochan-virtualbox.45387 > www.v1.tum.de.251.mdns: 4 [2q] PTR (QM)? _99SE7C8F47989526C9CD95024084F6F
B827C5ED..sub3.googlecast..tcp.local. PTR (QM)? googlecast..tcp.local. (94)
04:47:25.418003 IP BARTOSZ-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:26.198936 IP netiaspot.local.domain > baatochan-virtualbox.47681: 50235 1/0/0 PTR host-87-99-33-89.internetia
.net.pl. (80)
04:47:26.181432 IP baatochan-virtualbox.34105 > netiaspot.local.domain: 57280+ PTR? 43-249-238.83.in-addr.arpa. (44)
04:47:26.197303 IP netiaspot.local.domain > baatochan-virtualbox.34105: 57280 1/0/0 PTR krakh001r09.inetia.pl. (80)
04:47:26.198410 IP baatochan-virtualbox.38823 > www.v1.tum.de.33452: UDP, length 32
04:47:26.198548 IP baatochan-virtualbox.33805 > www.v1.tum.de.33453: UDP, length 32
04:47:26.198661 IP baatochan-virtualbox.49813 > www.v1.tum.de.33454: UDP, length 32
04:47:26.198814 IP baatochan-virtualbox.43050 > www.v1.tum.de.33455: UDP, length 32
04:47:26.198910 IP baatochan-virtualbox.59358 > www.v1.tum.de.33456: UDP, length 32
04:47:26.199003 IP baatochan-virtualbox.49350 > www.v1.tum.de.33457: UDP, length 32
04:47:26.199107 IP baatochan-virtualbox.46092 > www.v1.tum.de.33458: UDP, length 32
04:47:26.199708 IP baatochan-virtualbox.59757 > www.v1.tum.de.33459: UDP, length 32
04:47:26.199324 IP baatochan-virtualbox.39228 > www.v1.tum.de.33460: UDP, length 32
04:47:26.199420 IP baatochan-virtualbox.39644 > www.v1.tum.de.33461: UDP, length 32
04:47:26.199513 IP baatochan-virtualbox.46844 > www.v1.tum.de.33462: UDP, length 32
04:47:26.222320 IP baatochan-virtualbox.50165 > www.v1.tum.de.33463: UDP, length 32
04:47:26.199708 IP baatochan-virtualbox.59757 > www.v1.tum.de.33464: UDP, length 32
04:47:26.225645 IP ae-0-4.bar1.Hamburg1.Level3.net > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.225645 IP ae-0-4.bar1.Hamburg1.Level3.net > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.225645 IP ae-0-4.bar1.Hamburg1.Level3.net > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.228366 IP 195.122.181.62 > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.229220 IP 195.122.181.62 > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.230230 IP 195.122.181.62 > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.232102 IP cr-hanz-be3.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.231402 IP cr-hanz-be3.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.232107 IP cr-fraz2-be12.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.232107 IP cr-fraz2-be12.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.232107 IP cr-fraz2-be12.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.234479 IP cr-hanz-be3.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.243973 IP cr-garl-be3.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.339893 IP netiaspot.local.domain > baatochan-virtualbox.58457: 59293 1/0/0 PTR ae-0-4.bar1.Hamburg1.Level3.
net. (88)
```



```
04:47:26.340352 IP baatochan-virtualbox.58035 > www11.tum.de.33465: UDP, length 32
04:47:26.340438 IP baatochan-virtualbox.33510 > www11.tum.de.33465: UDP, length 32
04:47:26.340535 IP baatochan-virtualbox.33888 > www11.tum.de.33467: UDP, length 32
04:47:26.340672 IP baatochan-virtualbox.52849 > www11.tum.de.33468: UDP, length 32
04:47:26.340763 IP baatochan-virtualbox.48376 > www11.tum.de.33469: UDP, length 32
04:47:26.340852 IP baatochan-virtualbox.43266 > www11.tum.de.33470: UDP, length 32
04:47:26.341100 IP baatochan-virtualbox.51970 > netiaspot.local.domain: 43675+ PTR? 62.181.122.195.in-addr.arpa. (45
)
04:47:26.379435 IP cr-gar1-be6.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.379436 IP cr-gar1-be6.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 76
04:47:26.380314 IP kr-gar188-0.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.380315 IP kr-gar188-0.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.380977 IP kr-gar188-0.x-win.dfn.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.382393 IP vl-3001.cvr2-2wr.lrz.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:26.419620 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:26.421163 IP netiaspot.local.domain > baatochan-virtualbox.51970: 43675 NXDomain 0/1/0 (105)
04:47:26.524147 IP6 baatochan-virtualbox.mdns > ff02::fb.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:26.524628 IP baatochan-virtualbox.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:27.413704 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:27.528888 IP6 baatochan-virtualbox.mdns > ff02::fb.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:27.528890 IP baatochan-virtualbox.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:28.033461 ARP, Request who-has baatochan-virtualbox tell netiaspot.local, length 46
04:47:28.033479 ARP, Reply baatochan-virtualbox is-at 08:00:27:04:62:ae (oui Unknown), length 28
04:47:28.418478 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:29.177434 IP baatochan-virtualbox.52064 > 192.168.1.56.xmsg: Flags [..], ack 379210533, win 501, options [nop,
nop,TS val 4057712238 ecr 55741011], length 0
04:47:29.300503 IP 192.168.1.56.xmsg > baatochan-virtualbox.52064: Flags [..], ack 1, win 374, options [nop,nop,TS va
l 55744053 ecr 4054198112], length 0
04:47:29.416517 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:29.530176 IP6 baatochan-virtualbox.mdns > ff02::fb.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:29.530592 IP baatochan-virtualbox.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 62.181.122.195.in-addr.arpa. (45)
04:47:29.603759 IP baatochan-virtualbox.42926 > Anachronos.local.xmsg: Flags [..], ack 1, win 501, options [nop,nop,T
S val 1936048167 ecr 1938427342], length 0
04:47:29.604304 IP Anachronos.local.xmsg > baatochan-virtualbox.42926: Flags [..], ack 1, win 501, options [nop,nop,T
S val 1938437369 ecr 1936043243], length 0
04:47:30.413878 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:31.417602 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:31.427367 IP baatochan-virtualbox.55205 > netiaspot.local.domain: 8782+ PTR? 38.144.1.188.in-addr.arpa. (43)
04:47:31.470550 IP netiaspot.local.domain > baatochan-virtualbox.55205: 8782 1/0/0 PTR cr-han2-be3.x-win.dfn.de. (81
)
04:47:31.471638 IP baatochan-virtualbox.47047 > netiaspot.local.domain: 62627+ PTR? 133.144.1.188.in-addr.arpa. (44)
04:47:31.511982 IP netiaspot.local.domain > baatochan-virtualbox.47047: 62627 1/0/0 PTR cr-fra2-be12.x-win.dfn.de. (
83)
04:47:31.512468 IP baatochan-virtualbox.41875 > netiaspot.local.domain: 30411+ PTR? 230.145.1.188.in-addr.arpa. (44)
04:47:31.560987 IP netiaspot.local.domain > baatochan-virtualbox.41875: 30411 1/0/0 PTR cr-gar1-be6.x-win.dfn.de. (8
2)
04:47:31.561721 IP baatochan-virtualbox.43135 > www11.tum.de.33471: UDP, length 32
04:47:31.562056 IP baatochan-virtualbox.36530 > www11.tum.de.33472: UDP, length 32
04:47:31.562299 IP baatochan-virtualbox.43240 > www11.tum.de.33473: UDP, length 32
04:47:31.562524 IP baatochan-virtualbox.48381 > www11.tum.de.33474: UDP, length 32
04:47:31.562845 IP baatochan-virtualbox.57857 > www11.tum.de.33475: UDP, length 32
04:47:31.563097 IP baatochan-virtualbox.59537 > www11.tum.de.33476: UDP, length 32
04:47:31.563265 IP baatochan-virtualbox.57100 > www11.tum.de.33477: UDP, length 32
04:47:31.563948 IP baatochan-virtualbox.47226 > www11.tum.de.33478: UDP, length 32
04:47:31.564135 IP baatochan-virtualbox.55705 > www11.tum.de.33479: UDP, length 32
04:47:31.564260 IP baatochan-virtualbox.43810 > www11.tum.de.33480: UDP, length 32
04:47:31.564728 IP baatochan-virtualbox.52328 > netiaspot.local.domain: 6305+ PTR? 90.37.1.188.in-addr.arpa. (42)
04:47:31.600995 IP vl-3001.cvr2-2wr.lrz.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:31.600996 IP www11.tum.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:31.601836 IP www11.tum.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:31.601836 IP vl-3001.cvr2-2wr.lrz.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:31.605321 IP www11.tum.de > baatochan-virtualbox: ICMP time exceeded in-transit, length 36
04:47:31.612134 IP netiaspot.local.domain > baatochan-virtualbox.52328: 6305 1/0/0 PTR kr-gar188-0.x-win.dfn.de. (80
)
04:47:31.612802 IP baatochan-virtualbox.44950 > netiaspot.local.domain: 17919+ PTR? 168.0.187.129.in-addr.arpa. (44)
04:47:31.753596 IP netiaspot.local.domain > baatochan-virtualbox.44950: 17919 1/0/0 PTR vl-3001.cvr2-2wr.lrz.de. (81
)
04:47:31.753844 IP baatochan-virtualbox.52727 > www11.tum.de.33481: UDP, length 32
04:47:31.753971 IP baatochan-virtualbox.33333 > www11.tum.de.33482: UDP, length 32
04:47:31.754081 IP baatochan-virtualbox.36628 > www11.tum.de.33483: UDP, length 32
04:47:31.754157 IP baatochan-virtualbox.34969 > www11.tum.de.33484: UDP, length 32
04:47:31.754229 IP baatochan-virtualbox.59703 > www11.tum.de.33485: UDP, length 32
04:47:31.754309 IP baatochan-virtualbox.55699 > www11.tum.de.33486: UDP, length 32
04:47:31.754497 IP baatochan-virtualbox.58184 > netiaspot.local.domain: 12021+ PTR? 151.255.187.129.in-addr.arpa. (4
6)
04:47:31.796186 IP netiaspot.local.domain > baatochan-virtualbox.58184: 12021 1/0/0 PTR www11.tum.de. (73)
04:47:31.796824 IP baatochan-virtualbox.41200 > www11.tum.de.33487: UDP, length 32
04:47:31.799243 IP baatochan-virtualbox.49905 > www11.tum.de.33488: UDP, length 32
04:47:31.799636 IP baatochan-virtualbox.42738 > www11.tum.de.33489: UDP, length 32
04:47:31.799726 IP baatochan-virtualbox.60056 > www11.tum.de.33490: UDP, length 32
04:47:31.799887 IP baatochan-virtualbox.53540 > www11.tum.de.33491: UDP, length 32
04:47:32.414943 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:32.721379 IP BART05Z-PC-2.local.db-isp-disc > 192.168.1.255.db-isp-disc: UDP, length 210
04:47:33.416157 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:34.325339 ARP, Request who-has baatochan-virtualbox tell 192.168.1.56, length 46
04:47:34.325356 ARP, Reply baatochan-virtualbox is-at 08:00:27:04:62:ae (oui Unknown), length 28
04:47:34.413698 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:34.703812 IP 192.168.1.47.xmsg > baatochan-virtualbox.42926: Flags [..], ack 1, win 501, options [nop,nop,TS va
l 1938442468 ecr 1936043243], length 0
04:47:34.703834 IP baatochan-virtualbox.42926 > 192.168.1.47.xmsg: Flags [..], ack 1, win 501, options [nop,nop,TS va
l 1936053267 ecr 1938437369], length 0
04:47:36.414726 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:36.412397 IP BART05Z-PC-2.local.54915 > 192.168.1.255.54915: UDP, length 263
04:47:36.569605 IP baatochan-virtualbox.55995 > www11.tum.de.33492: UDP, length 32
```

Na powyższych zrzutach duża liczba pakietów się powtarza jednak w gruncie rzeczy widać tam następujące pakiety - zapytanie DNS o hosta docelowego wraz z odpowiedzią, pakiety UDP kierowane na adres hosta z coraz większym TTL, odpowiedzi o przekroczeniu TTL wysyłane przez kolejne hosty na trasie oraz odwrotne zapytania DNS o adres hosta. Poniżej widzimy też sam efekt wykonania **tracroute**.

```
[baatochan@baatochan-virtualbox Desktop]$ traceroute tum.de
traceroute to tum.de (129.187.255.151), 30 hops max, 60 byte packets
 1 netiaspot.local (192.168.1.1) 1.916 ms 1.819 ms 3.851 ms
 2 * * *
 3 * * *
 4 host-87-99-33-89.internetia.net.pl (87.99.33.89) 8.902 ms 12.441 ms 13.626 ms
 5 krakh001rt09.inetia.pl (83.238.249.43) 14.499 ms 14.425 ms 14.352 ms
 6 * * *
 7 ae-0-4.bar1.Hamburg1.Level3.net (4.69.142.205) 27.247 ms 27.102 ms 26.989 ms
 8 195.122.181.62 (195.122.181.62) 29.557 ms 30.316 ms 31.232 ms
 9 cr-han2-be3.x-win.dfn.de (188.1.144.38) 31.128 ms 35.255 ms 32.084 ms
10 cr-fra2-be12.x-win.dfn.de (188.1.144.133) 32.692 ms 32.599 ms 32.501 ms
11 cr-gar1-be6.x-win.dfn.de (188.1.145.230) 44.270 ms 39.113 ms 39.003 ms
12 kr-gar188-0.x-win.dfn.de (188.1.37.90) 39.784 ms 39.648 ms 40.218 ms
13 vl-3001.cvr2-2wr.lrz.de (129.187.0.168) 41.546 ms 40.141 ms 38.961 ms
14 www11.tum.de (129.187.255.151) 43.039 ms 38.489 ms 39.009 ms
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * f5slb4.lrz.de (129.187.255.244) 1220.875 ms !H *
```

Za pomocą `tcpdump` ustalić, czy korzystanie z e-Portalu jest bezpieczne, tzn.:

Do tego ćwiczenia wykorzystane zostały parametry `-A`, który wyświetla zawartość każdego pakietu oraz filtr, który wyświetla tylko pakiety na oraz z konkretnego adresu.

```
[baatochan@baatochan-virtualbox Desktop]$ tcpdump -A -r eportal host eportal.pwr.edu.pl or oauth.pwr.edu.pl
reading from file eportal, link-type EN10MB (Ethernet)
05:59:03.936490 IP baatochan-virtualbox.59562 > del-moodle-app-test.pwr.edu.pl.https: Flags [P.], seq 2753335691:2753335753, ack 2143473615, win 11065, options [nop,nop,TS val 2961918423 ecr 3396286975], length 62
E..r..@..@.....F.....+9.3.....
..I..o9.....9...7b.Nf<OY...EU...S2..6.I...<.....(....nY....9.U>mny
05:59:03.980680 IP del-moodle-app-test.pwr.edu.pl.https > baatochan-virtualbox.59562: Flags [.], ack 62, win 332, options [nop,nop,TS val 3396310477 ecr 2961918423], length 0
E..4...@.7.....F.....L.$.....
..o....I..
05:59:04.044389 IP del-moodle-app-test.pwr.edu.pl.https > baatochan-virtualbox.59562: Flags [P.], seq 1:8121, ack 62, win 332, options [nop,nop,TS val 3396310540 ecr 2961918423], length 8120
E.....@.7..6..F.....
..o....I.....N$.~..q.V...5.....08.....[.4.1J..L../......S.....M6].....{.g5.....c..fT.....
..i..W.b...*.G.%..(.....O.E.....Wf.v.'.....>..h...<'1.2 ..].....3..I.....tV....X...2i.Ho.'..fx.'.....T.W.].F.J.S.
...X.....u...*.NZ...*.C.....a.xv.B.Vm...<[.....N...[:/.QT...$...F..C..oL..-E.y...t]-H...r...P...^.....=1>..
...oiY.0..#W...5p.....l.Z'T.kBM...?~'...>...^+Q...[:>Q)"U...N.q;CX...N..D6..}....v.n...*.....[....'/\..
..P"
...p...=6.....b..S...=32.r9E...f...*O.S..3~...../K.[8]>....V9~[<.../h.h.u5".K.+?.../..8...z.L+.uCtF.....
..71.#.
)U.../h...2<:V'x...[.dk.l.....QM.e..d'.N.c.;{.....K.O.8d&...~9.....K...PF.....n.'.....xO...IX6.Z.?.S...r...<.a.
.O.VU...Gpf...~\43..U2X...i<.../.....y.q.k...1.....;V.
r..O.rL:a?.....T.....J..9W.a.I.E..ID...;1..+A...h...{...#qDck..M.7..P....y..fz...\#..~1...1...e...].lMHR...y.
u.....mM...B.pE.)7.....%.)w...[.6....2/.f.../\...j%...j]"P].8..e.....M.....>....a.6..a...F7..
wI..R...j..iS...Q.Q.f.[.....$X.MT:.....a.....
".d.@.T.*...h..B..M.P$..$.9.{.Km..4..RP..e3m.j..1.8...Wfr]..u.s.\.....P]..iZ!...%X(.C....7g+.....A<.K@.i
*)..9x..5...V...a..9.....0.....
Ye..r...)#Pk=...A..A..t...yH.9[5...G.....f.].W:..$b...D..n}...../?*...K..R=A
.O.#.k!!U...0...D...@.M'V.w:rk.T.A'k..v...*5.\{.o...k..&..A..n.....o.....9-..7&..A..2...$.S.\./..1...!
..@...n...@...~..n.0*.A.L$.~H..l'.....>~Y...&v..V..V.Go..%#.....*/.z.=.....L..t.....*)...../E=\.8.S)...\\
b...o..w..1...A..H.iSU+8.j...[.....0...[.JX...R...j...Pz.Ci...JY...+;t...~{.....
w...g"...xdo...Z}>..s.E...7.g.g'.Ks&..I6.am.r..s.(.F%..7...w9.&(.U...3".R/&1(.....jH..b.^[.l.ny...n..56K.4.
.G.@...o.N...X.QaU...x...]{*q.....%1.N.7mC).....~h..u...aE.....$'.V8hH.g..3<..BxU3.1....
..v..^.....&h...6.D.S.....@...?;K..l...yx2..&.F.5..CW...{.6...^..hx..H.3R.../..BJ...s.7;.S.....=...c
...[.da....x...\\
.cH...WBc...l.}....u.M.....1.bE.Wmh.e1.....I...vD+j..f...=..j..H..S<..7..lw..9g..$F...8.....w.....K...5.
...@I.9I..^...\\HoK.....K...{^d.....oy..f8.8...{*...>-)B...Id.d...=...[.....1Z./..01W...7J.u).....o....
...jEF...74...oM>-..VP..
J@.....SR..H.q'6...l;..i.i<.&..]9...f...b...Y
..X.I..gt...H.A.=...pD.....
..C..63l6hy...).z...\\9.....V.S.....q...v1..9B.....B0....da2eH".....m.....$jh...|.b...Nb*..V.....~(.....S6..
*1s.7...+...M..u..l...s.7.....}...u...
...W...$4z...<Dt.....)(%..^..2LX..^=)...#.1...Z.....J.....5.....H..Q.*...Ae4.....b..^..G..zV..B..+
...i'.G...w&b..b..^A.C9...[~.....?f#[.P.*..Q...6.k'.9Z.5*...Z<F.*..%.6.H..g7e...h-
..l..J...etl..N..dN].g.]`...*.h.v$..
^U...Vb...).R..o.$e...P.'i...l...R^.....N...k.N$P&...z4I.p:St.....I.v.i.X.....n.jY..K.....
p...j&k...*.q.d'[(.....^C..$9Ku...D.Z.1;...
```

Powyżej widać, że komunikacja pomiędzy ePortalem (eportal.pwr.edu.pl) oraz serwisem autoryzacyjnym (oauth.pwr.edu.pl) jest zabezpieczona SSL i nie można nic przeczytać (ani haseł, ani nazw kursów).

Wyświetlić bieżącą tablicę tras, usunąć ścieżkę domyślną dla pakietów (sprawdzić czy jest dostęp do Internetu), a następnie dodać ją ponownie.

Do wyświetlania oraz edycji tablicy tras można użyć polecenia `route`.

```
[baatochan@baatochan-virtualbox Desktop]$ route
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
default            netiaspot.local   0.0.0.0           UG    100    0      0 enp0s3
192.168.1.0        0.0.0.0           255.255.255.0    U     100    0      0 enp0s3
[baatochan@baatochan-virtualbox Desktop]$ ping tum.de
PING tum.de (129.187.255.151) 56(84) bytes of data:
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=1 ttl=240 time=36.4 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=2 ttl=240 time=36.7 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=3 ttl=240 time=36.2 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=4 ttl=240 time=36.3 ms
^C
--- tum.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 36.196/36.393/36.730/0.205 ms
[baatochan@baatochan-virtualbox Desktop]$ sudo route del default
[sudo] password for baatochan:
[baatochan@baatochan-virtualbox Desktop]$ route
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
192.168.1.0        0.0.0.0           255.255.255.0    U     100    0      0 enp0s3
[baatochan@baatochan-virtualbox Desktop]$ ping tum.de
ping: connect: Network is unreachable
```

Na powyższym zrzucie widać aktualną tablicę oraz sprawdzenie, że internet działa. Następnie widać usunięcie domyślnej trasy oraz sprawdzenie, czy internet działa. Oczywiście połączenie nie może zostać nawiązane.


```
[baatochan@baatochan-virtualbox Desktop]$ sudo route add default gw 192.168.1.1
[baatochan@baatochan-virtualbox Desktop]$ route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          netiaspot.local 0.0.0.0         UG    0      0      0 enp0s3
192.168.1.0      0.0.0.0        255.255.255.0   U     100    0      0 enp0s3
[baatochan@baatochan-virtualbox Desktop]$ ping tum.de
PING tum.de (129.187.255.151) 56(84) bytes of data:
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=1 ttl=240 time=36.2 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=2 ttl=240 time=35.5 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=3 ttl=240 time=35.6 ms
64 bytes from wwwv11.tum.de (129.187.255.151): icmp_seq=4 ttl=240 time=35.9 ms
^C
--- tum.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 35.477/35.807/36.203/0.278 ms
[baatochan@baatochan-virtualbox Desktop]$
```

Powyżej widać dodanie trasy oraz to, że połączenie internetowe z powrotem zaczęło działać.

Korzystając z polecenia `netstat` wyświetlić listę połączeń opartych na protokole TCP. Następnie nawiązać sesję z dowolnym serwerem WWW. Ponownie wyświetlić listę połączeń - dwa razy: raz z nazwami hostów i portów, a drugi raz numerami IP hostów i portów. Przeanalizować wyniki odpowiadające nawiązanym sesjom, wyjaśnić znaczenie pól.

Do wyświetlania aktywnych połączeń tcp można użyć komendy `netstat`, parametr `-t` powoduje ograniczenie wyników do samych połączeń TCP.

```
[baatochan@baatochan-virtualbox Desktop]$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
[baatochan@baatochan-virtualbox Desktop]$
```

Powyżej widać pusty wynik `netstat` przed nawiązaniem połączenia do serwera.

```
[baatochan@baatochan-virtualbox Desktop]$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 baatochan-virtual:51866 waw02s18-in-f10.1:https ESTABLISHED
tcp        0      0 baatochan-virtual:60190 del-moodle-app:www-http ESTABLISHED
tcp        0      0 baatochan-virtual:42942 del-moodle-app-te:https ESTABLISHED
tcp        0      0 baatochan-virtual:49874 151.101.194.109:https ESTABLISHED
tcp        0      0 baatochan-virtual:38918 172.64.206.35:https ESTABLISHED
[baatochan@baatochan-virtualbox Desktop]$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.58:51866      216.58.209.10:443      ESTABLISHED
tcp        0      0 192.168.1.58:60190      156.17.70.219:80       ESTABLISHED
tcp        0      0 192.168.1.58:42942      156.17.70.219:443      ESTABLISHED
tcp        0      0 192.168.1.58:49874      151.101.194.109:443    ESTABLISHED
tcp        0      0 192.168.1.58:38918      172.64.206.35:443      ESTABLISHED
[baatochan@baatochan-virtualbox Desktop]$
```

Powyżej widać połączenia nawiązane przez przeglądarkę po połączeniu z serwerem ePortalu.

Kolejne kolumny znaczą odpowiednio:

- protokół połączenia,
- ilość bajtów odebrana przez komputer, ale nie odebrana przez program, który otworzył to połączenie,
- ilość bajtów nie potwierdzona przez serwer,
- adres i port lokalny,
- adres i port zdalnego serwera,
- stan połączenia

5 pozycji na liście `netstat` znaczą kolejno:

- linijka 2 - połączenie na porcie 80 do serwera ePortalu, używane do rozpoczęcia szyfrowanej transmisji SSL i wymiany certyfikatów,
- linijka 3 - połączenie na porcie 443 do serwera ePortalu już po SSL
- pozostałe linijki - połączenia SSL do innych serwerów, by pobrać dodatkowe zasoby wymagane przez ePortal do działania.

Korzystając z polecenia `nmap`:

ustalić jakie komputery w sieci laboratorium (lub domowej) są dostępne (wykorzystać pakiety ICMP, wyniki zapisać do pliku XML).

Aby wykonać skanowanie sieci lokalnej użyte zostały następujące flagi:

- `-sP` - tryb skanowania, który pomija skanowanie otwartych portów (tylko pingiem sprawdza, które urządzenia są w sieci)
- `-oX <file>` - flaga włączająca eksport danych do pliku typu XML


```
[baatochan@baatochan-virtualbox Desktop]$ sudo nmap -sP -oX LAN.xml 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-12 00:08 CET
Nmap scan report for 192.168.1.1
Host is up (0.00075s latency).
MAC Address: 8C:59:C3:6C:64:E0 (ADB Italia)
Nmap scan report for OnePlus5T (192.168.1.13)
Host is up (0.053s latency).
MAC Address: 94:65:2D:D6:0E:E3 (OnePlus Technology (Shenzhen))
Nmap scan report for android-dc4ecf64c076d94b (192.168.1.25)
Host is up (0.043s latency).
MAC Address: 00:0A:F5:20:6B:08 (Airgo Networks)
Nmap scan report for EPSONF1773D (192.168.1.30)
Host is up (0.040s latency).
MAC Address: 38:9D:92:F1:77:3D (Seiko Epson)
Nmap scan report for 192.168.1.39
Host is up (0.00024s latency).
MAC Address: 2C:56:DC:3B:F9:3D (Asustek Computer)
Nmap scan report for RedmiNote5APrime-Jul (192.168.1.41)
Host is up (0.078s latency).
MAC Address: 80:35:C1:0A:50:55 (Xiaomi Communications)
Nmap scan report for 192.168.1.47
Host is up (0.00072s latency).
MAC Address: 60:45:CB:9A:CF:7B (Asustek Computer)
Nmap scan report for 192.168.1.54
Host is up (0.14s latency).
MAC Address: 52:C9:E6:C8:2E:C4 (Unknown)
Nmap scan report for 192.168.1.55
Host is up (0.10s latency).
MAC Address: 8E:7A:32:D5:1F:B8 (Unknown)
Nmap scan report for 192.168.1.57
Host is up (0.062s latency).
MAC Address: B8:08:CF:A0:04:97 (Intel Corporate)
Nmap scan report for baatochan-virtualbox (192.168.1.58)
Host is up.
Nmap done: 256 IP addresses (11 hosts up) scanned in 2.86 seconds
[baatochan@baatochan-virtualbox Desktop]$
```

przeskanować porty jednego z komputerów (można uruchomić wirtualną maszynę z Windows lub Linux). Przeanalizować wyniki dla jednego z otwartych portów.

Do skanowania użyta została tylko jedna flaga `-sV`, która włącza dodatkowo skanowanie jakie usługi i ich wersje są dostępne na otwartych portach.

```
[baatochan@baatochan-virtualbox Desktop]$ sudo nmap -sV 192.168.1.47
[sudo] password for baatochan:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-12 00:19 CET
Nmap scan report for 192.168.1.47
Host is up (0.00049s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4 (protocol 2.0)
MAC Address: 60:45:CB:9A:CF:7B (Asustek Computer)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
[baatochan@baatochan-virtualbox Desktop]$
```

Komputer użyty do skanowania to prywatna maszyna mojego współlokatora. Jedyny otwarty port to port 22 (czyli dokładnie tak jak powinno być).

Poszczególne kolumny o porcie przedstawiają następujące info:

- numer portu oraz protokół
- jego stan (domyślnie printowane są tylko otwarte)
- do jakiej usługi port należy
- dokładna wersja usługi działająca na tym porcie (dzięki flagie `-sV`)

Za pomocą `scp`:

- skopiować plik na zdalny komputer
- skopiować plik ze zdalnego komputera
- skopiować poddrzewo katalogów ze zdalnego komputera

Do wykonania tego zadania wymagane było stworzenie klucza do uwierzytelniania połączeń SSH (każdy komputer w mojej sieci lokalnej posiada zablokowane logowanie hasłem po SSH) oraz skonfigurowanie klienta `ssh` na maszynie wirtualnej.

Gdy połączenie SSH działało użycie `scp` wiązało się z bardzo prostą składnią: `scp <origin> <destination>`, uwzględniając, że lokalna część to po prostu ścieżka, a zdalna - `username@ip:path`, gdzie ścieżka może być absolutna lub relatywna do `~`. Do kopiowania folderu, konieczne było użycie flagi `-r`.

Do wykonania tego zadania również została użyta maszyna mojego współlokatora, z założonym kontem użytkownika na rzecz tego zadania.

```

[baatochan@baatochan-virtualbox .ssh]$ scp file5m baatochan@192.168.1.47:~
file5m 100% 4883KB 32.7MB/s 00:00
[baatochan@baatochan-virtualbox .ssh]$ scp baatochan@192.168.1.47:archive.test.tar .
archive.test.tar 100% 170KB 16.2MB/s 00:00
[baatochan@baatochan-virtualbox .ssh]$ scp -r baatochan@192.168.1.47:~/TerminalScripts .
Restart.lnk 100% 2527 1.5MB/s 00:00
Lock.lnk 100% 2496 2.0MB/s 00:00
Shut down.lnk 100% 2544 1.6MB/s 00:00
Sleep.lnk 100% 2503 1.6MB/s 00:00
lock.bat 100% 18 15.2KB/s 00:00
poweroff.ico 100% 4286 3.2MB/s 00:00
sleep.ico 100% 4286 3.5MB/s 00:00
restart.ico 100% 4154 3.4MB/s 00:00
lock.ico 100% 4286 2.8MB/s 00:00
sleep.bat 100% 18 19.2KB/s 00:00
restart.bat 100% 24 24.0KB/s 00:00
README.md 100% 693 820.6KB/s 00:00
poweroff.bat 100% 24 18.4KB/s 00:00
logitech_mouse_fix.bat 100% 93 102.4KB/s 00:00
Mouse Fix.lnk 100% 2105 1.4MB/s 00:00
README.md 100% 384 417.8KB/s 00:00
BeatsAudioOn.reg 100% 177 89.4KB/s 00:00
BeatsAudioOn.lnk 100% 1758 564.3KB/s 00:00
BeatsAudioOff.lnk 100% 1767 1.2MB/s 00:00
BeatsAudioOff.reg 100% 177 82.2KB/s 00:00
README.md 100% 337 153.1KB/s 00:00
tether-on.bat 100% 355 303.7KB/s 00:00
Turn off USB Tethering.lnk 100% 1729 1.0MB/s 00:00
Turn on USB Tethering.lnk 100% 1720 1.0MB/s 00:00
tether-off.bat 100% 356 100.6KB/s 00:00
README.md 100% 398 93.8KB/s 00:00
archive_all_dirs.sh 100% 205 61.8KB/s 00:00
README.md 100% 218 269.3KB/s 00:00
updateDates.sh 100% 1110 613.4KB/s 00:00
README.md 100% 469 360.7KB/s 00:00
findMissing.sh 100% 231 209.5KB/s 00:00
pull.bat 100% 664 688.9KB/s 00:00
export1SEFootage.sh 100% 220 213.7KB/s 00:00
crontab 100% 66 72.3KB/s 00:00
monthly.sh 100% 519 639.3KB/s 00:00
README.md 100% 607 299.9KB/s 00:00
daily.sh 100% 374 203.8KB/s 00:00
README.md 100% 227 155.7KB/s 00:00
LICENSE 100% 1075 509.1KB/s 00:00
HEAD 100% 23 15.4KB/s 00:00
description 100% 73 44.5KB/s 00:00
HEAD 100% 200 232.7KB/s 00:00

```

Powyżej widać transfery zakończone sukcesem. Wynik transferu został przycięty z uwagi na za dużą liczbę plików, by zmieścić na zrzucie.

Wyświetlić tablicę `arp`, przeanalizować wybrany wpis.

```

[baatochan@baatochan-virtualbox Desktop]$ arp -a
Anachronos.local (192.168.1.47) at 60:45:cb:9a:cf:7b [ether] on enp0s3
? (192.168.1.56) at c0:ee:fb:35:6c:80 [ether] on enp0s3
RedmiNote5APrime-Jul (192.168.1.41) at 80:35:c1:0a:50:55 [ether] on enp0s3
? (192.168.1.55) at 8e:7a:32:d5:1f:b8 [ether] on enp0s3
Chromecast (192.168.1.38) at 44:07:0b:9c:44:56 [ether] on enp0s3
android-dc4ecf64c076d94b (192.168.1.25) at 00:0a:f5:20:6b:08 [ether] on enp0s3
MSI.local (192.168.1.57) at b8:08:cf:a0:04:97 [ether] on enp0s3
netiaspot.local (192.168.1.1) at 8c:59:c3:6c:64:e0 [ether] on enp0s3
? (192.168.1.54) at 52:c9:e6:c8:2e:c4 [ether] on enp0s3
BARTOSZ-PC-2.local (192.168.1.39) at 2c:56:dc:3b:f9:3d [ether] on enp0s3
OnePlus5T (192.168.1.13) at 94:65:2d:d6:0e:e3 [ether] on enp0s3
EPSONF1773D (192.168.1.30) at 38:9d:92:f1:77:3d [ether] on enp0s3
[baatochan@baatochan-virtualbox Desktop]$

```

Do analizy wybrany został pierwszy wpis (ta sama maszyna co w poprzednich zadaniach). Po kolei widać następujące informacje:

- Nazwa hosta
- Adres IP
- Adres MAC
- Typ urządzenia (ARP wspiera nie tylko urządzenia Ethernet)
- Interfejs, którego dotyczy wpis