

# Laboratorium sieci komputerowych - c4

## Sieci bezprzewodowe

Krzysztof Dąbrowski gr. 3

27 maja 2019

### Spis treści

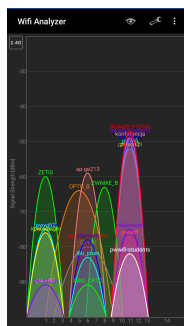
<b>1</b>	<b>Cel zajęć</b>	<b>1</b>
<b>2</b>	<b>Analiza przestrzeni radiowej</b>	<b>1</b>
<b>3</b>	<b>Schemat sieci</b>	<b>3</b>
<b>4</b>	<b>Podłączenie do sieci wifi w środowisku graficznym</b>	<b>4</b>
<b>5</b>	<b>Podłączenie w środowisku tekstowym na Ubuntu</b>	<b>5</b>
5.1	Połączenie do sieci . . . . .	6
5.2	Zmiana domyślnej trasy . . . . .	7
5.3	Sprawdzenie trasy pakietów . . . . .	8
<b>6</b>	<b>Podłączenie w środowisku tekstowym na FreeBSD</b>	<b>8</b>
6.1	Utworzenie interfejsu . . . . .	8
6.2	Podłączenie do sieci . . . . .	9
6.3	Zmiana tablicy tras . . . . .	10
6.4	Sprawdzenie połączenia . . . . .	11
6.5	Zakończenie pracy . . . . .	11

## 1 Cel zajęć

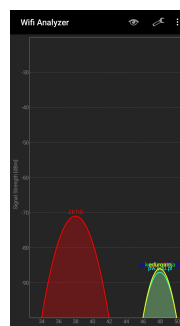
Celem laboratorium jest zbadanie lokalnych sieci radiowych oraz podłączenie i konfiguracja interfejsów radiowych na maszynach z systemami Ubuntu i FreeBSD.

## 2 Analiza przestrzeni radiowej

Przy pomocy aplikacji *Wifi Analyzer* przeskanowałem dostępne sieci radiowe oraz pokrycie poszczególnych kanałów. Wyniki analizy sieci pokazuje rysunek 1.



(a) Sieci na częstotliwości 2,4GHz



(b) Sieci na częstotliwości 5GHz

Rysunek 1: Analiza sieci radiowej

Dodatkowo przeskanowałem dostępne sieci przy pomocy polecenia `nmcli device wifi list`.

* SSID	MODE	CHAN	RATE	SIGNAL	SECURITY
konferencja	Infra	11	54 Mbit/s	74	WEP
pwwifi-students	Infra	11	54 Mbit/s	30	--
pwwifi2	Infra	11	54 Mbit/s	30	WPA2 802.1X
pwwifi-students	Infra	11	54 Mbit/s	35	--
vlab_net	Infra	11	54 Mbit/s	35	WPA2
konferencja	Infra	11	54 Mbit/s	30	WEP
pwwifi	Infra	11	54 Mbit/s	49	--
ZETIS	Infra	1	54 Mbit/s	99	WPA2 802.1X
pwwifi-students	Infra	6	54 Mbit/s	34	--
TROL	Infra	1	54 Mbit/s	29	--
pwwifi2	Infra	1	54 Mbit/s	52	WPA2 802.1X
pwwifi	Infra	11	54 Mbit/s	30	--
pwwifi2	Infra	11	54 Mbit/s	75	WPA2 802.1X
pwwifi2	Infra	6	54 Mbit/s	35	WPA2 802.1X
Sieć Wi-Fi (WE-Lech)	Infra	6	54 Mbit/s	30	WPA2
pwwifi-students	Infra	6	54 Mbit/s	37	--
Stery3	Infra	11	54 Mbit/s	30	WPA1 WPA2
asdf	Infra	9	54 Mbit/s	49	WPA1 WPA2
pwwifi2	Infra	6	54 Mbit/s	30	WPA2 802.1X
linksys	Infra	3	54 Mbit/s	24	WPA2
konferencja	Infra	1	54 Mbit/s	54	WEP
konferencja	Infra	6	54 Mbit/s	40	WEP
konferencja	Infra	1	54 Mbit/s	37	WEP
konferencja	Infra	6	54 Mbit/s	34	WEP
is_wifi	Infra	4	54 Mbit/s	30	WEP
konferencja	Infra	6	54 Mbit/s	30	WEP
pwwifi	Infra	1	54 Mbit/s	54	--
pwwifi-students	Infra	1	54 Mbit/s	49	--
pwwifi	Infra	6	54 Mbit/s	44	--
pwwifi	Infra	1	54 Mbit/s	37	--
pwwifi-students	Infra	11	54 Mbit/s	30	--
pwwifi2	Infra	1	54 Mbit/s	42	WPA2 802.1X
pwwifi2	Infra	6	54 Mbit/s	32	WPA2 802.1X
konferencja	Infra	1	54 Mbit/s	20	WEP
pwwifi	Infra	1	54 Mbit/s	37	--

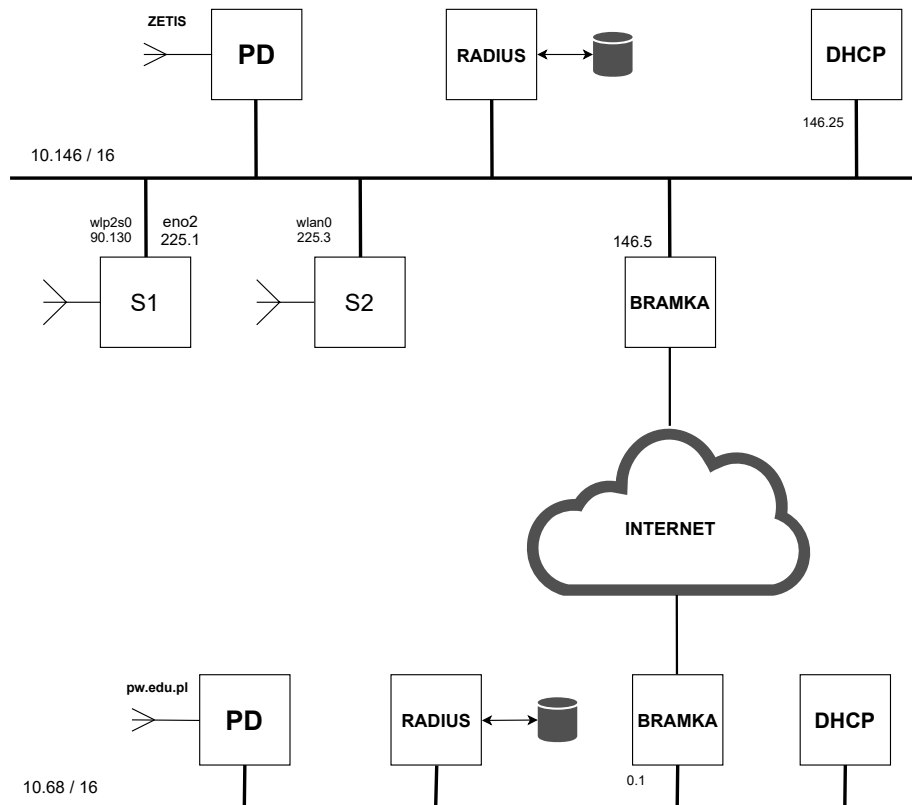
```

pwwifi-students      Infra 1      54 Mbit/s  24    --
pwwifi-students      Infra 1      54 Mbit/s  20    --

```

### 3 Schemat sieci

Strukturę urządzeń w sieci przedstawia rysunek 2.



Rysunek 2: Schemat sieci

## 4 Podłączenie do sieci wifi w środowisku graficznym

W celu przyłączenia do sieci skorzystam z nakładki graficznej na program *NetworkManager* wbudowanej w system Ubuntu.

Przed podłączeniem sprawdziłem stan interfejsu radiowego poleceniem `ip a`.

```
ip a
```

```
4: wlp2s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq
    state DOWN group default qlen 1000
link/ether 00:24:d7:92:0e:dc brd ff:ff:ff:ff:ff:ff
```

Oraz tablicę tras, poleceniem `ip r`.

```
ip r
```

```
default via 10.146.146.5 dev eno2
10.146.0.0/16 dev eno2 proto kernel scope link src 10.146.225.1
```

Z otrzymanych wyników widać, że interfejs radiowy jest **nieaktywny** a trasa domyślna wiedzie przez interfejs fizyczny.

Po podłączeniu do sieci **ZETIS** wyniki tych poleceń wyglądały następująco:

```
ip a
```

```
4: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq
    state UP group default qlen 1000
link/ether 00:24:d7:7d:ba:8c brd ff:ff:ff:ff:ff:ff
inet 10.68.17.233/16 brd 10.68.255.255 scope global dynamic wlp2s0
    valid_lft 3601sec preferred_lft 3601sec
inet6 fe80::224:d7ff:fe7d:ba8c/64 scope link
    valid_lft forever preferred_lft forever
```

```
ip r
```

```
default via 10.146.146.5 dev eno2
default via 10.68.0.1 dev wlp2s0 proto static metric 600
10.68.0.0/16 dev wlp2s0 proto kernel scope link src 10.68.17.233
    metric 600
10.146.0.0/16 dev eno2 proto kernel scope link src 10.146.225.3
169.254.0.0/16 dev wlp2s0 scope link metric 1000
192.0.2.4 via 10.68.0.1 dev wlp2s0 proto dhcp metric 600
```

Widać, że interfejs radiowy `wlp2s0` jest teraz włączony oraz skonfigurowany. Do tablicy tras została dodana nowa domyślna trasa prowadząca przez interfejs radiowy.

Dodatkowo pobrałem logi z serwera RADIUS połączeniem komend `ssh ldap grep -w $USER /var/log/radiusd | tail -2`.

```
ssh ldap grep -w \ $USER /var/log/radiusd | tail -2
```

```
Mon May 13 17:01:43 2019 : Auth: (2156) Login OK: [dabrowk1]
                        (from client ap225 port 0 via TLS tunnel)
Mon May 13 17:01:43 2019 : Auth: (2156) Login OK: [dabrowk1]
                        (from client ap225 port 0 cli 00-22-3F-01-F9-12)
```

Z zebranych logów wynika, że serwer RADIUS zaakceptował podane dane dostępowe.

Po podłączeniu do sieci **pw.edu.pl** stan interfejsów i tras wyglądał następująco:

```
ip a
```

```
5: wlx00223f01f912: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
mq
state UP group default qlen 1000
link/ether 00:22:3f:01:f9:12 brd ff:ff:ff:ff:ff:ff
inet 10.68.31.177/16 brd 10.68.255.255 scope global dynamic
wlx00223f01f912
valid_lft 3387sec preferred_lft 3387sec
inet6 fe80::222:3fff:fe01:f912/64 scope link
valid_lft forever preferred_lft forever
```

```
netstat -nr
```

Destination	Gateway	Genmask	Flags	MSS	Window	irrt
0.0.0.0	10.146.146.5	0.0.0.0	UG	0	0	0
0.0.0.0	10.68.0.1	0.0.0.0	UG	0	0	0
10.68.0.0	0.0.0.0	255.255.0.0	U	0	0	0
10.146.0.0	0.0.0.0	255.255.0.0	U	0	0	0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0
192.0.2.4	10.68.0.1	255.255.255.255	UGH	0	0	0

## 5 Podłączenie w środowisku tekstowym na Ubuntu

Domyślnie konfiguracją interfejsów radiowych zarządza program *NetworkManager*. Musiałem go wyłączyć by dokonać ręcznej konfiguracji.

Wyłączyłem ten program przy pomocy poleceń `sudo systemctl stop NetworkManager.service` oraz `sudo systemctl disable NetworkManager.service`.

Aby sprawdzić czy serwis został wyłączony wywołałem `sudo systemctl status NetworkManager.service`.

```
sudo systemctl status NetworkManager.service

* NetworkManager.service - Network Manager
Loaded: loaded (/lib/systemd/system/NetworkManager.service; disabled;
       vendor
Active: inactive (dead) since pon 2019-05-13 17:51:50 CEST
Main PID: 1458 (code=exited, status=0/SUCCESS)
```

## 5.1 Połączenie do sieci

Do połączenia się z siecią ZETIS skorzystam z programu `wpa_supplicant`.

Plik konfiguracyjny wygenerowałem poleceniem `wpa-config-zetis`. Ma on następującą treść:

```
ctrl_interface=/var/run/wpa_supplicant # dla wpa_cli

eapol_version=1
ap_scan=1

network={
    priority=30
    ssid="ZETIS"
    proto=WPA2
    key_mgmt=WPA-EAP
    identity="dabrowk1" # login
    password=hash:73a1da770586527f5d97f02a136a7795 # hasło
}
```

Wygenerowany plik zapisałem w katalogu `/etc/wpa_supplicant/wpa_supplicant.conf`.

Uruchomiłem demona `wpa_supplicant` poleceniem `sudo wpa_supplicant -B -i wlp2s0 -c /etc/wpa_supplicant/wpa_supplicant.conf`. Po wykonaniu tego polecenia system wyświetlił komunikat `Successfully initialized wpa_supplicant`.

**Stan interfejsu radiowego** po wykonaniu tych czynności uległ zmianie.

```
ip a

4: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
    UP group default qlen 1000
    link/ether 00:24:d7:92:0e:dc brd ff:ff:ff:ff:ff:ff
```

Widać, że jest teraz włączony.

**Pobranie adresu ip** na interfejsie radiowym wykonałem poleceniem `sudo dhclient wlp2s0`. Oraz sprawdziłem otrzymany adres poleceniem `ip`.

```
ip a

4: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
    UP group default qlen 1000
    link/ether 00:24:d7:92:0e:dc brd ff:ff:ff:ff:ff:ff
    inet 10.146.90.130/16 brd 10.146.255.255 scope global wlp2s0
        valid_lft forever preferred_lft forever
```

**Dziennik RADIUS** został zaktualizowany o wpis dotyczący tego połączenia. Przeczytałem jego zawartość poleceniem `ssh ldap grep -w $USER /var/log/radiusd | tail -2`

```
ssh ldap grep -w $USER /var/log/radiusd | tail -2

Mon May 20 21:57:20 2019 : Auth: (1401) Login OK: [dabrowk1]
    (from client ap225 port 0 via TLS tunnel)
Mon May 20 21:57:20 2019 : Auth: (1402) Login OK: [dabrowk1]
    (from client ap225 port 0 cli 00-24-D7-92-0E-DC)
```

**Dziennik DHCP** również posiada wpis opisujący przydzielenie adresu.

```
cat /var/log/syslog | grep -Ei 'dhcp' | tail -3

May 20 20:03:33 s1 dhclient[8615]: DHCPOFFER of 10.146.90.130 from
    10.146.146.25
May 20 20:03:33 s1 dhclient[8615]: DHCPACK of 10.146.90.130 from
    10.146.146.25
May 20 20:03:33 s1 dabrowk1: /etc/dhcp/dhclient-enter-hooks.d/avahi-
    autoipd returned non-zero exit status 1
```

Mogę przeczytać szczegóły przydzielonych dynamicznie wartości poleceniem `cat /var/lib/dhcp/dhclient.leases`.

## 5.2 Zmiana domyślnej trasy

W celu przekierowania ruchu przez interfejs radiowy zmieniłem trasę domyślną.

Usunąłem trasę domyślną przez interfejs `eno2` poleceniem `sudo ip route delete default` oraz ustawiłem nową poleceniem `sudo ip route add default via 10.146.146.5 dev wlp2s0`.

Stan tablicy tras po zmianie:

```
ip r

default via 10.146.146.5 dev wlp2s0
10.146.0.0/16 dev eno2 proto kernel scope link src 10.146.225.1
10.146.0.0/16 dev wlp2s0 proto kernel scope link src 10.146.90.130
```

### 5.3 Sprawdzenie trasy pakietów

By zweryfikować czy ustawiona trasa działa poprawnie skorzystałem z poleceń `tracert` i `ping`.

```
tracert volt
```

```
1 * * *
2 volt.iem.pw.edu.pl (194.29.146.3) 6.531 ms 6.535 ms 6.539 ms
```

Widać, że trasa wygląda inaczej niż gdy połączenie było przez interfejs `eno2`.

```
ping -c 1 google.com
```

```
PING google.com (172.217.16.14) 56(84) bytes of data.
64 bytes from mil02s06-in-f14.1e100.net (172.217.16.14): icmp_seq=1
ttl=54 time=114 ms
```

Po wyniku pingu widać większe opóźnienie (114 ms) co jest charakterystyczne dla sieci radiowych.

## 6 Podłączenie w środowisku tekstowym na FreeBSD

By przygotować stację do pracy zalogowałem się jako `root` zamontowałem katalog publiczny oraz uruchomiłem skrypt `labsk`. Zrobiłem to poleceniami `mount /pub` oraz `/pub/FreeBSD/zetis/config/labsk`.

Po ponownym zalogowaniu na stację była ona gotowa do pracy.

### 6.1 Utworzenie interfejsu

Interfejs radiowy wymaga konfiguracji przed rozpoczęciem pracy. Trzeba zainstalować odpowiednie sterowniki oraz ustawić konfigurację związaną z krajem.

Do wykonania tych akcji wykorzystam skrypt `sterowniki`.

```
sterowniki -w | sh -x
```

Poprawność utworzenia interfejsu mogę sprawdzić poleceniem `ifconfig`.

```
ifconfig wlan0
```

```
wlan0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0
mtu 1500
ether 00:24:d7:7d:ba:8c
inet6 fe80::224:d7ff:fe7d:ba8c%wlan0 prefixlen 64 scopeid 0x4
groups: wlan
ssid pwwifi-students channel 11 (2462 MHz 11g ht/20) bssid
00:24:14:31:8a:f2
regdomain ETSI country PL authmode OPEN privacy OFF txpower 30
bmiss 10 scanvalid 60 protmode CTS ampdulimit 64k ampdudensity 8
-amsdutr amsdurx shortgi -stbc -ldpc wme bintval 102
```



```
media: IEEE 802.11 Wireless Ethernet MCS mode 11ng
status: associated
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

## 6.2 Podłączenie do sieci

Do połączenia się z siecią ZETIS skorzystam z programu `wpa_supplicant`. Wykorzystałem taki sam plik konfiguracyjny jak w poprzedniej sekcji 5.1. Plik konfiguracyjny zapisałem w katalogu `/etc/wpa_supplicant/wpa_supplicant.conf`

Uruchomiłem demona `wpa_supplicant` poleceniem  
`sudo wpa_supplicant -B -i wlan0 -c /etc/wpa_supplicant/wpa_supplicant.conf`.  
 Po wykonaniu tego polecenia system wyświetlił komunikat `Successfully initialized wpa_supplicant`.

### Zmiana ustawień interfejsu

Poleceniem `ifconfig` zaobserwowałem zmianę w ustawieniach interfejsu.

```
ifconfig wlan0

wlan0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0
    mtu 1500
    ether 00:24:d7:7d:ba:8c
    inet6 fe80::224:d7ff:fe7d:ba8c%wlan0 prefixlen 64 scopeid 0x4
    groups: wlan
    ssid ZETIS channel 1 (2412 MHz 11g ht/20) bssid f0:9f:c2:7d:8c:40
    regdomain ETSI country PL authmode WPA2/802.11i privacy ON
    deftxkey UNDEF AES-CCM 2:128-bit AES-CCM 3:128-bit txpower 30
    bmiss 10
    scanvalid 60 protmode CTS ampdulimit 64k ampdudensity 8
    -amsdutr amsdurx shortgi -stbc -ldpc wme roaming MANUAL
    media: IEEE 802.11 Wireless Ethernet MCS mode 11ng
    status: associated
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

Przeanalizowałem też tablicę tras.

```
netstat -r
```

Destination	Gateway	Flags	Netif	Expire
0.0.0.0/8	link#2	U	em1	
default	nat2.iem.pw.edu.pl	UGS	em0	
10.146.0.0/16	link#1	U	em0	
s3.iem.pw.edu.pl	link#1	UHS	lo0	
localhost	link#3	UH	lo0	

### Pobranie adresu IP

Pobrałem adres IP poleceniem `dhclient wlan0`

Sprawdziłem rezultaty pobrania adresu:

```

ifconfig wlan0

...
inet 192.168.225.3 netmask 0xffff0000 broadcast 192.168.255.255
...

```

**Dziennik RADIUS** został zaktualizowany o wpis dotyczący tego połączenia. Przeczytałem jego zawartość poleceniem `ssh dabrowk1@ldap grep -w dabrowk1 /var/log/radiusd | tail -2`

```

Tue May 21 10:14:05 2019 : Auth: (1718) Login OK: [dabrowk1] (from
    client ap225 port 0 via TLS tunnel)
Tue May 21 10:14:05 2019 : Auth: (1719) Login OK: [dabrowk1] (from
    client ap225 port 0 cli 00-24-D7-7D-BA-8C)

```

**Dziennik DHCP** również posiada wpis opisujący przydzielenie adresu.

```
ssh dabrowk1@ldap grep -w 00:24:d7:7d:ba:8c /var/log/dhcpd | tail -3
```

```

May 21 10:22:53 ldap dhcpd[1311]: DHCPOFFER on 192.168.225.3 to
    00:24:d7:7d:ba:8c via vmx0
May 21 10:22:55 ldap dhcpd[1311]: DHCPREQUEST for 192.168.225.3
    (192.168.146.3) from 00:24:d7:7d:ba:8c via vmx0
May 21 10:22:55 ldap dhcpd[1311]: DHCPACK on 192.168.225.3 to 00:24:
    d7:7d:ba:8c via vmx0

```

Mogę przeczytać szczegóły przydzielonych dynamicznie wartości poleceniem `cat /var/db/dhclient.leases.wlan0`.

```

cat /var/db/dhclient.leases.wlan0

lease {
interface "wlan0";
fixed-address 192.168.225.3;
next-server 192.168.146.3;
filename "ipxe";
server-name "vol.wf";
option subnet-mask 255.255.0.0;
option routers 192.168.146.3;
option host-name "s3";
option domain-name "iem.pw.edu.pl";
option dhcp-server-identifier 192.168.146.3;
}

```

### 6.3 Zmiana tablicy tras

By ruch przechodził przez interfejs radiowy trzeba ustawić odpowiednią domyślną trasę. Aktualnie jedyna domyślna trasa przechodzi przez interfejs `em0`.

```
netstat -r4n
```

Destination	Gateway	Flags	Netif	Expire
0.0.0.0/8	link#2	U	em1	
default	10.146.146.5	UGS	em0	
10.146.0.0/16	link#1	U	em0	
10.146.225.3	link#1	UHS	lo0	
127.0.0.1	link#3	UH	lo0	
192.168.0.0/16	link#4	U	wlan0	
192.168.225.3	link#4	UHS	lo0	

Trasa do serwera volt wygląda następująco

```
traceroute volt
```

```
traceroute to volt.iem.pw.edu.pl (194.29.146.3), 64 hops max, 40 byte packets
```

```
1  nat2 (10.146.146.5) 0.552 ms 0.517 ms 0.335 ms
2  volt (194.29.146.3) 0.463 ms 0.521 ms 0.430 ms
```

Usunąłem domyślną trasę poleceniem `route delete default10.146.146.5` oraz ustawiłem nową poleceniem `route add default192.168.146.3`. Nowy adres bramy odczytałem z pliku `dhclient.leases.wlan0`.

Stan tablicy tras po zmianie

```
netstat -rn4
```

Destination	Gateway	Flags	Netif	Expire
0.0.0.0/8	link#2	U	em1	
default	192.168.146.3	UGS	wlan0	
...				

## 6.4 Sprawdzenie połączenia

Trasa do serwera volt wygląda teraz następująco

```
traceroute volt
```

```
traceroute to volt.iem.pw.edu.pl (194.29.146.3), 64 hops max, 40 byte packets
```

```
1  volt (194.29.146.3) 3.256 ms 5.527 ms 1.503 ms
```

Komunikacja z zewnętrznymi serwerami również jest możliwa.

```
ping -c 1 google.com
```

```
PING google.com (172.217.16.14): 56 data bytes
```

```
64 bytes from 172.217.16.14: icmp_seq=0 ttl=54 time=13.145 ms
```

## 6.5 Zakończenie pracy

By nie zostawić interfejsu radiowego włączonego usunąłem go poleceniem `ifconfig wlan0 destroy`