

Sprawozdanie
Sieci komputerowe laboratorium
Ćwiczenie 3 - konfiguracja interfejsów sieciowych
Wifi i Bluetooth

Rafał Chojnacki 262814
Eryk Banaś 266544

24.05.2017r.

Spis treści

1	Telefon komórkowy - program Wifi Analyzer	2
2	System FreeBSD - sieci WiFi	2
2.1	Załadowanie sterownika karty sieciowej, konfiguracja i stworzenie interfejsu . .	2
2.2	Połączenie z siecią ZETiIS	5
2.3	Połączenie z siecią pwwifi-students	6
3	Połączenie z siecią WiFi używając komputera z systemem Ubuntu	7
3.1	Dostępne sieci WiFi	7
3.2	Połączenie poprzez interfejs graficzny	8
3.3	Ręczne połączenie z siecią WiFi	8
3.4	Połączenie z siecią pwwifi-students	9
3.5	Połączenie z siecią ZETiIS	9

1 Telefon komórkowy - program Wifi Analyzer

Celem ćwiczenia było zainstalowanie na telefonie komórkowym z systemem Android programu Wifi Analyzer. Umożliwia on obserwację sieci radiowych znajdujących się w pobliżu. Dla każdej z sieci uzyskujemy parametry takie jak: informacje o kanale, adresie IP, sile sygnału, częstotliwości pracy oraz sposobie zabezpieczenia połączenia. Dzięki niemu możemy sprawdzić poziom zajętości poszczególnych kanałów i w razie potrzeb go zmienić na taki, na którym pracuje mniej urządzeń.

Przy połączeniu do sieci ZETiS autoryzacja odbywa się na podstawie danych logowania jak do serwisu ISOD. Połączenie z siecią pwwifi-students wymaga podania hasła w postaci numeru PESEL i pierwszej litery matki z dużej litery. Loginem jest numer albumu.

2 System FreeBSD - sieci WiFi

2.1 Załadowanie sterownika karty sieciowej, konfiguracja i stworzenie interfejsu

W zadaniu tym posłużyliśmy się szczegółową instrukcją dostępną w pliku z treścią ćwiczenia. Na początku należało załadować sterowniki karty sieciowej przy pomocy polecenia sterowniki -w.

```
k2% ssh chojnacr@t2
The authenticity of host 't2 (10.146.103.72)' can't be established.
ECDSA key fingerprint is SHA256:F/g7nrWkp3bWmAjfUb/1ZW9p8VPXJmTYAvXhTAd6Xqg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 't2,10.146.103.72' (ECDSA) to the list of known hosts.
Password:
Could not chdir to home directory /home/stud/chojnacr: No such file or directory
(1)
t2% sterowniki -h
uzycie: sterowniki -ebdfhksuwx [maszyna]
-e ethernet
-b bluetooth
-d dysk
-f fire-wire
-k konsola systemowa
-s port szeregowy (uart)
-u port USB
-w wifi
-x dodatkowe
t2% sterowniki -w
# Sterowniki dla maszyny t2 :
# Karta WIFI:
sudo kldload cbb cardbus
# Ładujemy sterowniki karty:
$ sudo kldload if_ath_pci
sudo kldload wlan_amrr
```

```

# Kreujemy interfejs wirtualny:
wlan=$(sudo ifconfig wlan create wlandev ath0)
# Jesli pojawi sie komunikat: 'ifconfig: SIOCIFCREATE2: Device not configured'
# oraz mruga na niej zielona lampka
# to nalezy karte wifi (PCMCIA) wysunac i ponownie wsunac.
# W efekcie powinniśmy uzyskac ciagle swiecenie zielonej lampki.
  sudo ifconfig $wlan country PL
  sudo ifconfig $wlan up
# Teraz można obejrzeć dostępne sieci:
  sleep 1                      # inicjalizacja karty jest wolna
  ifconfig $wlan
  ifconfig $wlan list scan
# Dalsze informacje o wifi można uzyskać przez polecenie: wifi-doc
# i w plikach w katalogu /usr/local/zetis/labsk.
# Uwaga! Nie wolno zostawiać interfejsów radiowych włączonych !
# Interfejs kasujemy poleceniem:
  sudo ifconfig $wlan destroy

t2% sudo kldload cbbcardbus
kldload: can't load cbbcardbus: No such file or directory
(1) t2% sudo kldload cbb cardbus kldload: can't load cbb: module already loaded or in
kernel kldload: can't load cardbus: module already loaded or in kernel
(1) t2% sudo kldload if_ath_pci
kldload: can't load if_ath_pci: module already loaded or in kernel
(1)
t2% sudo kldload wlan_amrr
kldload: can't load wlan_amrr: module already loaded or in kernel
(1) t2% wlan=$(sudo ifconfig wlan create wlandev ath0) t2% ifconfig
vr0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=82808<VLAN_MTU,WOL_UCAST,WOL_MAGIC,LINKSTATE>          ether 00:40:63:de:28:58
inet 10.5.225.4 netmask 0xffff0000 broadcast 10.5.255.255
  inet 0.0.0.0 netmask 0xff000000 broadcast 255.255.255.255
  nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
  media: Ethernet 100baseTX          status: active
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

options=209b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,WOL
L_MAGIC>          ether 00:1b:21:06:f3:1f          inet 10.146.103.72
netmask 0xffff0000
broadcast 10.146.255.255
  inet6 fe80::21b:21ff:fe06:f31f%em0 prefixlen 64 tentative scopeid 0x2
  nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
  media: Ethernet autoselect (1000baseT <full-duplex>)
  status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384

```

```

options=600003<RXCSUM, TXCSUM, RXCSUM_IPV6, TXCSUM_IPV6>
inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet 127.0.0.1 netmask 0xff000000
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
ath0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 2290
ether 00:0f:cb:fa:56:85
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    media: IEEE 802.11 Wireless Ethernet autoselect (autoselect)
    status: no carrier
wlan0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0f:cb:fa:56:85
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    media: IEEE 802.11 Wireless Ethernet autoselect (autoselect)
    status: no carrier
    ssid "" channel 1 (2412 MHz 11g)
    regdomain ETSI country PL ecm authmode OPEN privacy OFF txpower 30
    bmiss 7 scanvalid 60 protmode CTS wme burst bintval 0 t2% sudo ifconfig
    $wlan country PL
    t2% sudo ifconfig $wlan up

```

Sprawdzenie stanu stworzonego interfejsu

```

t2% ifconfig wlan0
wlan0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0f:cb:fa:56:85
    inet6 fe80::20f:cbff:fefa:5685%wlan0 prefixlen 64 scopeid 0x5
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    media: IEEE 802.11 Wireless Ethernet DS/1Mbps mode 11g
    status: associated
    ssid pwwifi channel 11 (2462 MHz 11g) bssid 00:24:14:31:2f:b0
    regdomain ETSI country PL ecm authmode OPEN privacy OFF txpower 30
    bmiss 7 scanvalid 60 protmode CTS wme burst bintval 102

```

Lista dostępnych sieci radiowych:

```
t2% ifconfig $wlan list scan
SSID/MESH ID      BSSID              CHAN RATE   S:N      INT CAPS
pwwifi            00:24:14:31:95:20  1   54M -93:-96 102 ES    HTCAP WME
pwwifi2           00:24:14:31:95:23  1   54M -92:-96 102 EPS    HTCAP RSN WME
pwwifi-stud...    00:21:a0:81:86:c2  1   54M -90:-96 102 ES    HTCAP WME
konferencja       00:21:a0:81:86:c1  1   54M -91:-96 102 EPS    WME
pwwifi2           00:21:a0:81:86:c3  1   54M -89:-96 102 EPS    HTCAP RSN WME
ZETiIS            00:1e:52:79:ca:59  6   54M -70:-96 100 EPS    RSN HTCAP WME
pwwifi            00:21:a0:81:15:d0  6   54M -92:-96 102 ES    HTCAP WME
konferencja       00:21:a0:81:15:d1  6   54M -92:-96 102 EPS    WME
pwwifi2           00:21:a0:81:15:d3  6   54M -91:-96 102 EPS    HTCAP RSN WME
pwwifi            00:24:14:31:2f:b0 11   54M -89:-96 102 ES    HTCAP WME
pwwifi-stud...    00:24:14:31:2f:b2 11   54M -92:-96 102 ES    HTCAP WME
konferencja       00:24:14:31:2f:b1 11   54M -89:-96 102 EPS    WME
is_wifi           00:1d:46:7d:72:60 13   54M -94:-96 100 EPS    WME
TP-LINK_81E9CF    18:d6:c7:81:e9:ce  8   54M -95:-96 100 EPS    RSN HTCAP WPA WME ATH WPS
t2% sudo ifconfig $wlan down
```

2.2 Połączenie z siecią ZETiIS

By połączyć się z siecią ZETiIS należy zmodyfikować zawartość pliku `/etc/wpa_supplicant.conf`. Należy wprowadzić login i hasło (w postaci jawnej lub funkcji hashującej – `wpa_passphrase`) oraz nadajemy sieci najwyższy priorytet spośród zdefiniowanych w tym pliku konfiguracyjnym, przy czym ważną rolę odgrywa typ protokołu zabezpieczającego – WPA2:

```
#ZETiIS (ap103, ap227, ap510 (channel 1) network={
    priority=19
    ssid="ZETiIS"
    proto=WPA2
    key_mgmt=WPA-EAP
    identity="chojncr"      # login-id
    password="*****"
}
# AP510 (channel 6) network={
    priority=6
    ssid="ZETiIS-227"
    key_mgmt=WPA-PSK
    # wpa_passphrase ZETiIS
    #psk="zetis-wifi"
    psk=990cace9809d0f3af810b08dc17cd0aaef2e4de0c0418aa5b6a4e985640eddc3
    # kldload wlan_tkip
}
```

Kolejnym krokiem jest uruchomienie program `wpa_supplicant` do wykreowania interfejsu `wlan0`:

```
t2% sudo wpa_supplicant -Dbsd -iwlan0 -c/etc/wpa_supplicant.conf Successfully initialized wpa_supplicant
wlan0: Trying to associate with 00:1e:52:79:ca:59 (SSID='ZETiIS' freq=2437 MHz)
wlan0: Associated with 00:1e:52:79:ca:59 wlan0: CTRL-Event-EAP-Started EAP authentication started
wlan0: CTRL-Event-EAP-Proposed-Method vendor=0 method=25 wlan0: CTRL-Event-EAP-Method EAP vendor
wlan0: CTRL-Event-EAP-Peer-Cert depth=1 subject='/C=PL/ST=Mazowieckie/L=Warszawa/O=Warsaw Univet
wlan0: CTRL-Event-EAP-Peer-Cert depth=1 subject='/C=PL/ST=Mazowieckie/L=Warszawa/O=Warsaw Univet
wlan0: CTRL-Event-EAP-Peer-Cert depth=0 subject='/C=PL/ST=Mazowieckie/O=Warsaw University of Teo
EAP-TLV: TLV Result - Failure wlan0: CTRL-Event-EAP-Failure EAP authentication failed
wlan0: Authentication with 00:1e:52:79:ca:59 timed out.
wlan0: CTRL-Event-Disconnected bssid=00:1e:52:79:ca:59 reason=3 locally_generated=1
wlan0: CTRL-Event-SSID-Temp-Disabled id=1 ssid="ZETiIS" auth_failures=1 duration=10 ioctl[SIOCS8
wlan0: Authentication with 00:21:a0:81:86:c2 timed out. wlan0: CTRL-Event-Disconnected bssid=00:
wlan0: CTRL-Event-SSID-Reenabled id=1 ssid="ZETiIS"
wlan0: Trying to associate with 00:24:14:31:2f:b2 (SSID='pwwifi-students' freq=2462 MHz) wlan0:
wlan0: CTRL-Event-Connected - Connection to 00:24:14:31:2f:b2 completed [id=0 id_str=] wlan0: CT
wlan0: Trying to associate with 00:21:a0:81:15:d2 (SSID='pwwifi-students' freq=2437 MHz) wlan0:
wlan0: CTRL-Event-Connected - Connection to 00:21:a0:81:15:d2 completed [id=0 id_str=]
```

Po połączeniu z siecią ZETIS (stan interfejsu)

```
t2% ifconfig wlan0
wlan0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0f:cb:fa:56:85
    inet6 fe80::20f:cbff:fefa:5685%wlan0 prefixlen 64 tentative scopeid 0x5
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
    media: IEEE 802.11 Wireless Ethernet autoselect (autoselect)
    status: no carrier
    ssid "" channel 6 (2437 MHz 11g)
    regdomain ETSI country PL ecm authmode WPA1+WPA2/802.11i privacy OFF
txpower 30 bmiss 7 scanvalid 60 protmode CTS wme burst bintval 102
```

2.3 Połączenie z siecią pwwifi-students

Sieć powinna mieć najwyższy priorytet spośród opisanych w pliku `/etc/wpa_supplicant.conf`. Należy sprawdzić stan interfejsu radiowego i poprawnie go skonfigurować, gdyż nie ma przypisanego adresu IP. W tym celu posłużyliśmy się programem `dhclient`.

```
t2% ifconfig wlan0
wlan0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0f:cb:fa:56:85
    inet6 fe80::20f:cbff:fefa:5685%wlan0 prefixlen 64 tentative scopeid 0x5
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

```
media: IEEE 802.11 Wireless Ethernet autoselect (autoselect)
status: no carrier
ssid "" channel 6 (2437 MHz 11g)
regdomain ETSI country PL ecm authmode WPA1+WPA2/802.11i privacy OFF
txpower 30 bmiss 7 scanvalid 60 protmode CTS wme burst bintval 102
```

```
t2% sudo dhclient wlan0
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 6 wlan0 link state up -> down
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 4 wlan0 link state down -> up
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 5
DHCPOFFER from 1.1.1.1
DHCPREQUEST on wlan0 to 255.255.255.255 port 67 DHCPACK from 1.1.1.1
bound to 10.66.29.161 -- renewal in 1800 seconds.
```

```
t2% ifconfig wlan0
wlan0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
ether 00:0f:cb:fa:56:85 inet6 fe80::20f:cbff:fefa:5685%wlan0 prefixlen 64 scopeid 0x5
inet 10.66.29.161 netmask 0xffff0000 broadcast 10.66.255.255
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL> media: IEEE 802.11 Wireless
Ethernet OFDM/54Mbps mode 11g status: associated
ssid pwwifi channel 11 (2462 MHz 11g) bssid 00:24:14:31:2f:b0
regdomain ETSI country PL ecm authmode WPA1+WPA2/802.11i privacy OFF
txpower 30 bmiss 7 scanvalid 60 protmode CTS wme burst bintval 102
```

W celu autoryzacji użytkownik musi połączyć się z adresem 1.1.1.1 I należy zadbać o to, aby trasa do niego prowadziła przez interfejs wlan0, w tym celu dodajemy go do tablicy tras:

```
t2% sudo route add 1.1.1.1 10.166.29.161
route: writing to routing socket: Network is unreachable
add host 1.1.1.1: gateway 10.166.29.161 fib 0: Network is unreachable
```

```
t2% telnet 1.1.1.1 Trying 1.1.1.1...
telnet: connect to address 1.1.1.1: Operation timed out telnet: Unable to connect to remote host
```

Przesył danych przez interfejs wlan0 możemy obserwować uruchamiając program tcpdump.

3 Połączenie z siecią WiFi używając komputera z systemem Ubuntu

3.1 Dostępne sieci WiFi

Dostępne sieci WiFi możemy wylistować używając polecenia:

```
k2% sudo iwlist wlp2s0 scan | grep ESSID ESSID:"lego"
ESSID:"ZETiIS"
```



```
ESSID:"pwwifi-students"  
ESSID:"pwwifi2"  
ESSID:"pwwifi"  
ESSID:"pwwifi2"  
ESSID:"konferencja"  
ESSID:"pwwifi-students"  
ESSID:"konferencja"  
ESSID:"konferencja"  
ESSID:"pwwifi2"  
ESSID:"AMX"  
ESSID:"pwwifi-students"  
ESSID:"pwwifi"  
ESSID:"pwwifi"  
ESSID:"pwwifi"  
ESSID:"konferencja"  
ESSID:"pwwifi-students"  
ESSID:"TP-LINK_81E9CF"  
ESSID:"pwwifi2"  
ESSID:"pwwifi"  
ESSID:"is_wifi"  
ESSID:"gg312"  
ESSID:"pwwifi-students"  
ESSID:"pwwifi-students"  
ESSID:"pwwifi-students"  
ESSID:"pwwifi"  
ESSID:"pwwifi"  
ESSID:"pwwifi"  
ESSID:"pwwifi-students"  
ESSID:""  
ESSID:"pwwifi-students"  
ESSID:"ZPNiSnet_4.2"  
ESSID:"konferencja"  
ESSID:"pwwifi ESSID:"MUEIV"
```

3.2 Połączenie poprzez interfejs graficzny

Program Network Manager w systemie Ubuntu umożliwia wybór interesującej nas sieci (która jest w zasięgu), podanie nazwy użytkownika a następnie zaznaczenie opcji 'No CA certificate is required'.

3.3 Ręczne połączenie z siecią WiFi

Poleceniem `ifconfig` sprawdzamy dostępne interfejsy odpowiadające za połączenia bezprzewodowe. Informacji na ich temat i możliwości konfiguracji np. zmiana częstotliwości lub hasła , dostarcza program `ifconfig`.

3.4 Połączenie z siecią pwwifi-students

Uwierzytelnienie w tym połączeniu odbywa się poprzez Web Authentication więc nie ma potrzeby umieszczania danych użytkownika w pliku konfiguracyjnym `wpa_supplicant`. Po podniesieniu odpowiedniego interfejsu i przypisaniu mu IP programem `dhclient` dokonujemy uwierzytelnienia otwierając przeglądarkę i logując się pod adresem 1.1.1.1. Dzięki poleceniu: `sudo tcpdump -i wlp2s0` sprawdzamy stan połączenia

3.5 Połączenie z siecią ZETiIS

Rozpoczynamy od wyłączenia programu Network Manager poleceniem: `sudo systemctl stop NetworkManager.service`

Połączenie z siecią umożliwia program `wpa_supplicant`, który plik konfiguracyjny `/etc/wpa_supplicant.conf` wczytuje w chwili uruchomienia. By nawiązać połączenie z wybraną siecią należy stworzyć taki plik:

```
ZETiIS (ap103, ap227, ap510 (channel 1)
network={
priority=21
ssid="ZETiIS"
proto=WPA2
key_mgmt=WPA-EAP
identity="chojnacr " # login-id
password=hash #hasło w postaci funkcji skrótu
}
```

Do połączenia z daną siecią konieczne jest ustawienie najwyższego priorytetu spośród wszystkich innych w pliku konfiguracyjnym. Uzyskiwanie funkcji skrótu z hasła odbywa się poprzez program `wpa_passphrase`:

```
k2% wpa_passphrase ZETiIS
# reading passphrase from stdin
```

Uruchamiamy program `wpa_supplicant`:

```
k2% sudo service wpa_supplicant start wlp2s0
```