

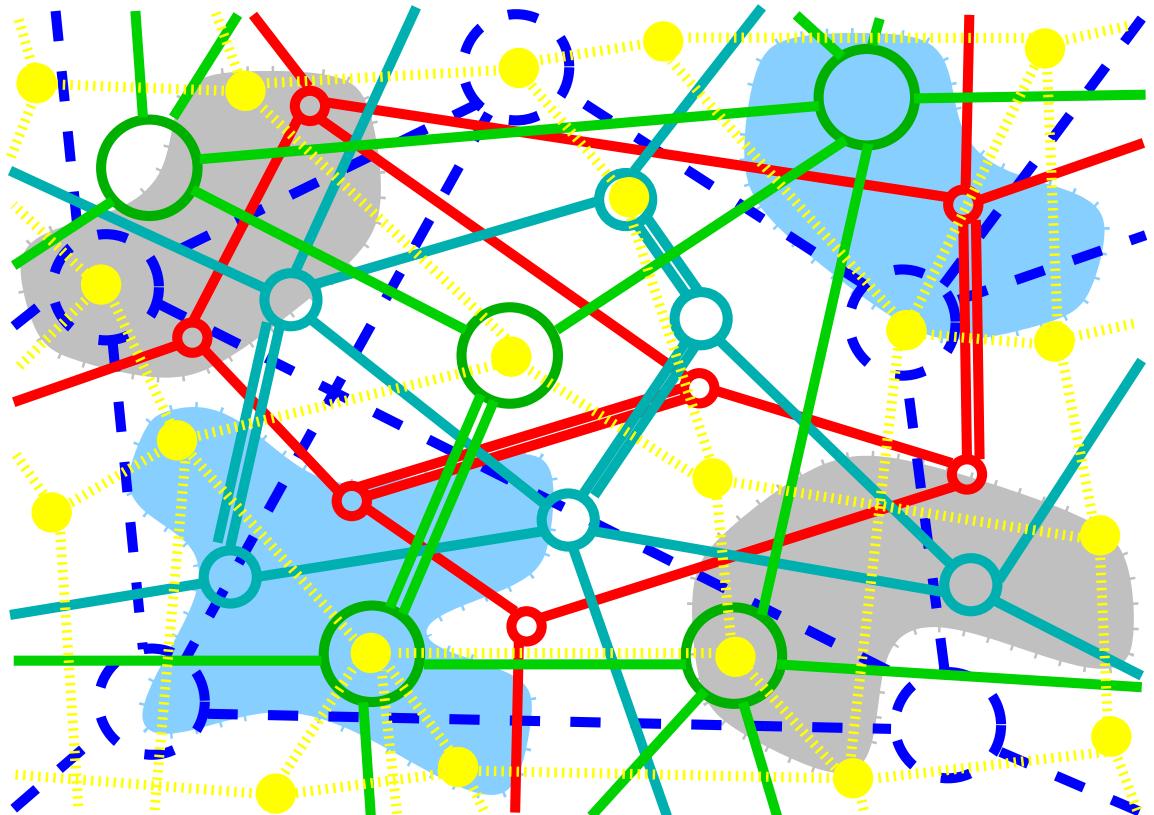
Instrukcja do laboratorium sieci komputerowych

Sieci bezprzewodowe WiFi

dr inż. Piotr Arabas

mgr inż. Jerzy Sobczyk

dr inż. Edward Śliwa



20 września 2024

10 Ćwiczenie 10 Konfigurowanie sieci bezprzewodowych WiFi

Wstęp

Ćwiczenie to jest wykonywane przez dwa dwuosobowe zespoły z których każdy konfiguruje jeden punkt dostępowy.

Do punktów dostępowych można się zalogować wykonując polecenie:

- telnet 172.17.**8**.100 z maszyny Net**2**
- lub telnet 172.17.**8**.200 z maszyny Net**4**.

UWAGA! Znak zapytania **?** w nazwach i adresach oznacza numer stanowiska = 1, 2 lub 3.

UWAGA! W tym ćwiczeniu tylko komputery Net14, Net24 i Net34 mają przez cały czas połączenie z Internetem. Pozostałe komputery uzyskają to połączenie dopiero po poprawnym wykonaniu ćwiczenia.

10.1 Cel ćwiczenia

Celem ćwiczenia jest praktyczne zapoznanie się z techniką sieci bezprzewodowych i efektami występującymi przy pracy w takich sieciach.

W ramach ćwiczenia tworzone są dwie sieci bezprzewodowe. Jedna z nich NetLab**2** pracująca w paśmie 2,4Ghz będzie siecią dostępową dla stacji roboczych Net**1** i Net**3**. Natomiast druga NetLab**5** pracująca w paśmie 5GHz będzie pełniła rolę mostu bezprzewodowego pomiędzy punktami dostępowymi. Obie sieci będą połączone w punkcie dostępowym apt**2** przy pomocy skonfigurowanego mostu (ang. bridge) tworząc razem jedną podsieć IP. Punkt dostępowy apt**4** będzie wykonywał routing do "reszty świata" przez maszynę Net**4**. Na Net**4** będzie też działał program freeradius wykorzystywany do autoryzacji w drugim etapie ćwiczenia.

10.2 Nazwy i adresy

Urządzenie/Sieć	Interfejs/Parametr	Stanowisko 1	Stanowisko 2	Stanowisko 3
Sieć 2,4 GHz	SSID	NetLab 1 _2	NetLab 2 _2	NetLab 3 _2
	Adresy	192.168.2 14 .0/24	192.168.2 24 .0/24	192.168.2 34 .0/24
Sieć 5 GHz	SSID	NetLab 1 _5	NetLab 2 _5	NetLab 3 _5
	Adresy	192.168.2 14 .0/24	192.168.2 24 .0/24	192.168.2 34 .0/24
Adresy przydzielane przez DHCP	od do	192.168.2 14 .10 192.168.2 14 .20	192.168.2 24 .10 192.168.2 24 .20	192.168.2 34 .10 192.168.2 34 .20
Net 1	wl1	DHCP	DHCP	DHCP
Net 3	wl1	DHCP	DHCP	DHCP
Parametry skonfigurowane automatycznie przed rozpoczęciem ćwiczenia - nie należy ich zmieniać				
Net 2	et2	172.17. 18 .102/25	172.17. 28 .102/25	172.17. 38 .102/25
Net 4	et2	172.17. 18 .204/25	172.17. 28 .204/25	172.17. 38 .204/25
apt 2	ether4	172.17. 18 .100/25	172.17. 28 .100/25	172.17. 38 .100/25
apt 4	ether4	172.17. 18 .200/25	172.17. 28 .200/25	172.17. 38 .200/25

10.3 Przebieg ćwiczenia

Ćwiczenie składa się z pieciu etapów:

1. Konfiguracja mostu bezprzewodowego z autoryzacją wspólnym kluczem.
2. Konfiguracja sieci dostępowej bez autoryzacji - otwartej.
3. Włączenie autoryzacji wspólnym kluczem w sieci dostępowej.
4. Zmiana autoryzacji na RADIUS dla sieci dostępowej.
5. Zmiana autoryzacji na RADIUS dla mostu bezprzewodowego.

10.3.1 Konfiguracja mostu bezprzewodowego z autoryzacją wspólnym kluczem.

Na wstępie każdy zespół uzgadnia klucze/hasła dla sieci 5GHz. Hasła te są następnie wpisywane do konfiguracji interfejsów punktach dostępowych.

Wszystkie interfejsy bezprzewodowe należy skonfigurować do pracy w Polsce.

apt ?2 Należy też utworzyć most (ang. bridge) łączący interfejsy **wlan1** i **wlan2** interfejsy. Most powinien otrzymać swój adres IP. Adres ten będzie potrzebny do testowania połączeń i konfigurowania autoryzacji RADIUS.

Interfejs **wlan2** należy konfigurować do pracy w trybie **station-bridge**.

apt ?4 Interfejs **wlan1** pozostawiamy nieskonfigurowany lub wyłączamy natomiast **wlan2** konfigurujemy do pracy w trybie **bridge**. Trzeba też skonfigurować routing kierując trasę domyślną do komputera **Net ?4** i pamiętając o routingu dla pakietów odpowiedzi.

Po zakończeniu tego etapu oba punkty dostępowe oraz komputery **Net ?2** i **Net ?4** powinny móc przesyłać pakiety (np. ECHO) między sobą jak również resztą świata.

10.3.2 Konfiguracja otwartej sieci dostępowej.

Częstotliwość pracy sieci 2,4 GHz należy dobrać z pośród dozwolonych w Polsce na podstawie analizy zajętości pasm.

apt ?2 Interfejs **wlan1** należy skonfigurować do pracy w trybie **ap-bridge**.

Należy też skonfigurować serwer DHCP, który będzie przydzielał adresy stacjom roboczym **Net ?1** i **Net ?3**.

Net ?1 i Net ?3 Należy polecienniem **iwctl** lub **iwgtk** przyłączyć interfejsy **wl0** od skonfigurowanej sieci 2,4GHz.

Po zakończeniu tego etapu komputery **Net ?1** i **Net ?3**. powinny uzyskać łączność ze światem i móc przesyłać pakiety (np. ECHO) między sobą jak również resztą świata.

10.3.3 Autoryzacja w sieci dostępowej wspólnym kluczem.

Net ?1 i Net ?3 Należy polecienniem **iwctl** lub **iwgtk** odłączyć interfejsy **wl0** od sieci WiFi.

apt ?2 Dla interfejsu **wlan1** należy skonfigurować autoryzację wspólnym kluczem innym niż klucz mostu bezprzewodowego.

Net ?1 i Net ?3 Należy ponownie przyłączyć interfejsy **wl0** od skonfigurowanej sieci 2,4GHz tym razem podając klucz wpisany na punkcie dostępowym.

Po zakończeniu tego etapu komputery **Net ?1** i **Net ?3**. powinny znów uzyskać łączność ze światem.

10.3.4 Autoryzacja RADIUS dla sieci dostępowej.

Na komputerze **Net ?4** działa serwer autoryzacyjny freeradius. W jego konfiguracji znajdują się wpisy w pliku **clients.conf**:

Plik clients.conf

```
client hAP {
    ipaddr      = 172.17.0.0/16
    secret      = APsekret123
}

client Net {
    ipaddr      = 192.168.0.0/16
    secret      = NETsekret123
}
```

oraz w pliku `mods-conf/files/authorize`:

Plik authorize

```
aptX2 Cleartext-Password := "APTx2sekret"
Reply-Message := "Hello, %{User-Name}"

netX1 Cleartext-Password := "sekretNETx1"
Reply-Message := "Hello, %{User-Name}"

netX3 Cleartext-Password := "sekretNETx3"
Reply-Message := "Hello, %{User-Name}"
```

Net ?1 i Net ?3 Należy poleciem `iwctl` lub `iwgtk` odłączyć interfejsy `wl0` od sieci WiFi.

apt ?2 Należy w konfiguracji punktu dostępowego podać dane serwera RADIUS, Utworzyć profil EAP_APT wykorzystujący autoryzację poprzez serwer RADIUS i przełączyć interfejs `wlan1` na ten profil.

Net ?1 i Net ?3 W katalogu `/var/lib/iwd` należy utworzyć plik `NetLab ?_2.8021x` zawierający dane autoryzacyjne odpowiedniego użytkownika wpisanego w konfiguracji serwera RADIUS (`netX1` lub `neX3`). Należy ponownie przyłączyć interfejsy `wl0` od sieci `NetLab ?_2`

I znów po zakończeniu etapu wszystkie komputery powinny mieć łączność ze światem.

10.3.5 Autoryzacja RADIUS dla mostu bezprzewodowego.

Net ?1 i Net ?2 Należy poleciem `iwctl` lub `iwgtk` odłączyć interfejsy `wl0` od sieci WiFi.

apt ?4 Należy w konfiguracji punktu dostępowego podać dane serwera RADIUS, Trzeba utworzyć nowy profil EAP_AP wykorzystujący autoryzację przez serwer RADIUS i przełączyć interfejs `wlan2` na używanie tego profilu.

apt ?2 Należy utworzyć nowy profil EAP_CL korzystający z autoryzacji poprzez drugi punkt dostępowy i przełączyć interfejs `wlan2` na ten profil.

Od tego momentu połączenie między punktami dostępowymi powinno ponownie zacząć działać.

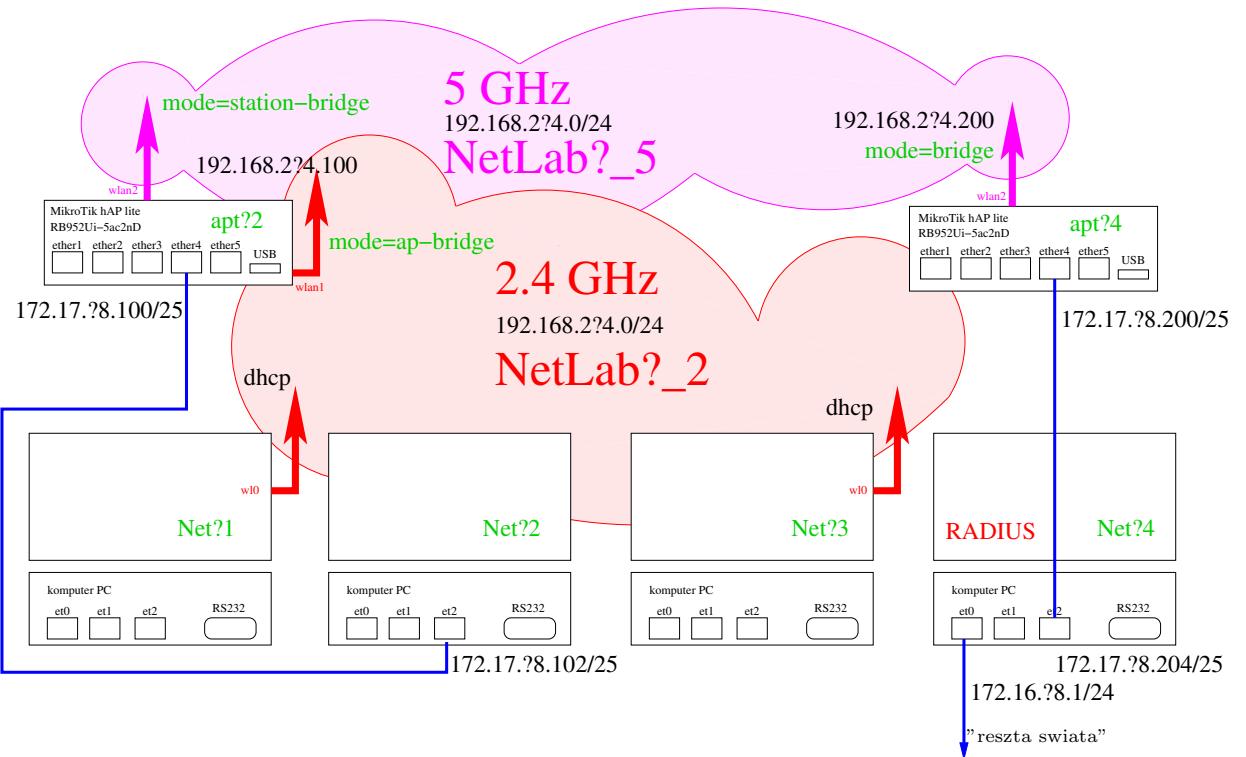
Net ?1 i Net ?2 Należy ponownie przyłączyć interfejsy `wl0` od skonfigurowanej sieci.

10.4 Sprawozdanie

Sprawozdanie powinno zawierać:

- Listę poleceń (wraz z wartościami parametrów) użytych do skonfigurowania każdego z punktów dostępowych na każdym etapie.
- Rezultaty poleceń wyświetlających spektrum, stan połączeń itp. a zwłaszcza pokazujące, że połączenie zostało nawiązane.
- Wyciągi z logów serwera RADIUS pokazujące udaną autoryzację.
- Wyjaśnienia problemów i odpowiedzi na pytania zawarte w opisach etapów.
- Uwagi na temat problemów napotkanych w trakcie wykonywania ćwiczenia.

10.5 Szczegóły techniczne



Rysunek 25: Schemat połączeń ćwiczenia 5

10.6 Zalecenia

1. Konfigurując kraj trzeba w tym samym poleceniu ustawić jednocześnie opcje `antenna-gain=4` i `frequency-mode=regulatory-domain`
2. Aby uniknąć długiego czasu włączania interfejsu 5 GHz związanego z testowaniem kanałów DFS należy zastosować opcję `skip-dfs-channels=all` albo ręcznie ustawić częstotliwość z zakresu: 5160..5240 GHz.
3. Należy bardzo uważać aby nie zmienić ustawień dla interfejsów `bridge`, `ether4` i `ether5` przez które zarządzamy punktem dostępowym gdyż możemy stracić z nim łączność.
4. Przed przystąpieniem do realizacji kolejnego etapu należy rozłączyć (ang. disconnect) interfejsy `wl0` w komputerach `Net?1` i `Net?3`.
5. Przy konfiguracji autoryzacji RADIUS można użyć metody PWD albo PEAP.
6. Przy konfiguracji autoryzacji RADIUS zalecane jest użycie opcji `AutoConnect=true` w sekcji `[Settings]`.
7. Przy konfiguracji serwera DHCP jako serwery DNS można wykorzystać dwa spośród adresów: 194.29.160.10, 194.29.160.20, 1.1.1.1, 8.8.8.8.
8. Do testowania łączności ze światem można wykorzystać adresy: 1.1.1.1 (cloudflare.com), 8.8.8.8 (google.com).

10.7 Przydatne polecenia

Polecenia routera MikroTik	
/interface wireless set <i>interface</i> <i>opcja1=wartość1 opcja2=wartość2 opcja3=wartość3 ...</i>	Ustawienie opcji interfejsu.
/interface wireless set <i>interface</i> ssid= <i>identyfikator</i>	Ustawienie identyfikatora SSID interfejsu.
/interface wireless set <i>interface</i> skip-dfs-channels=all	Rezygnacja w wykorzystania kanałów DFS w paśmie 5 GHz.
/interface wireless set <i>interfejs</i> security-profile= <i>profil</i>	Ustawienie profilu bezpieczeństwa dla interfejsu.
/interface wireless security-profiles add name= <i>profil</i> mode=dynamic-keys authentication-types=wpa2-psk wpa2-pre-shared-key= <i>wspólny_klucz</i>	Definicja profilu bezpieczeństwa korzystającej z WPA2 i wspólnego klucza.
/interface wireless security-profiles add name= <i>profil</i> mode=dynamic-keys authentication-types=wpa2-eap eap-methods=passthrough	Definicja profilu bezpieczeństwa korzystającej z WPA2 i EAP.
/interface wireless security-profiles add name= <i>profil</i> mode=dynamic-keys authentication-types=wpa2-eap eap-methods=peap supplicant-identity= <i>identyfikator</i> mschapv2-username= <i>login</i> mschapv2-password= <i>hasło</i> tls-mode=dont-verify-certificate	Definicja profilu bezpieczeństwa do autoryzacji RADIUS.
/radius add address= <i>adres_serwera</i> secret= <i>klucz</i> service=wireless	Konfiguracja autoryzacji RADIUS.
/interface wireless frequency-monitor <i>interfejs</i>	Uruchomienie monitora częstotliwości na wskazanym interfejsie.
/interface wireless spectral-scan <i>interfejs</i>	Uruchomienie analizy spektrum na wskazanym interfejsie.
/interface wireless scan <i>interfejs</i>	Wykrywanie działających urządzeń WiFi.
/interface wireless registration-table print	Wyswietlenie listy aktywnych połączeń WiFi.
/interface bridge vlan add bridge= <i>nazwa</i> tagged= <i>lista1</i> untagged= <i>lista2</i> vlan-ids= <i>vid</i>	Zdefiniowanie list portów, które przesyłają pakiety znakowane (<i>lista1</i>) i nieznakowane (<i>lista2</i>).
/interface bridge add name= <i>nazwa_mostu</i>	Utworzenie nowego mostu o podanej nazwie.
/interface bridge port add bridge= <i>most</i> interface= <i>interfejs</i>	Dodanie interfejsu do mostu.
/interface bridge port print	Wyswietlenie listy interfejsów przyłączonych do mostu.
/ip arp print	Wyswietlenie tablicy ARP.
/interface bridge host print	Wyswietlenie tablicy FDB mostu.
/ip dhcp-server setup	Uruchomienie konfiguratora serwera DHCP.
/ip dhcp-server print	Wyswietlenie konfiguracji serwera DHCP.
/ip pool print	Wyswietlenie zakresu adresów przydziałanych przez serwer DHCP.

<https://wiki.mikrotik.com/wiki/Manual:TOC>

Polecenia programu iwctl

iwctl device list	Wyswietlenie listy interfejsów.
iwctl device <i>if</i> show	Wyświetlenie atrybutów interfejsu.
iwctl device <i>if</i> set-property <i>atrybut wartość</i>	Ustawienie atrybutu na podaną wartość.
iwctl device <i>if</i> set-property Powered on	Włączenie interfejsu.
iwctl station <i>if</i> show	Wyświetlenie stanu interfejsu WiFi.
iwctl station <i>if</i> scan	Wyszukanie dostępnych sieci (bez wyświetlenia).
iwctl station <i>if</i> get-networks	Wyświetlenie listy dostępnych sieci (znalezionych polecienniem scan).
iwctl station <i>if</i> connect <i>SSID</i>	Przyłączenie się do sieci o wskazanym identyfikatorze <i>SSID</i> .
iwctl -passphrase= <i>hasło</i> station <i>if</i> connect <i>SSID</i>	Przyłączenie się do sieci o wskazanym identyfikatorze <i>SSID</i> .

<https://man.archlinux.org/man/extra/iwd/iwctl.1.en>

10.8 Plik konfiguracji sieci /var/lib/iwd/NetLab ?_2.8021x

Plik NetLab ?_2.8021x

```
[Security]
opcja=wartość
.....
[Settings]
opcja=wartość
.....
```

Opcje pliku z danymi sieci

EAP-Method= <i>metoda</i>	Ustawienie metody autoryzacji (zalecane PWD albo PEAP).
EAP-Identity= <i>id</i>	Identyfikator osoby/urządzenia łączącego się z serwerem RADIUS.
EAP-Password= <i>hasło</i>	Hasło osoby/urządzenia łączącego się z serwerem RADIUS.
EAP-PEAP-Phase2-Method= <i>metoda</i>	Ustawienie opcji fazy 2 autoryzacji PEAP (zalecane na "MSCHAPV2").
EAP-PEAP-Phase2-Identity= <i>id</i>	Identyfikator osoby/urządzenia łączącego się do sieci WiFi.
EAP-PEAP-Phase2-Password= <i>hasło</i>	Hasło osoby/urządzenia łączącego się do sieci WiFi.
AutoConnect= <i>true false</i>	Automatyczne dołączanie do sieci.

<https://wiki.archlinux.org/title/Iwd>

<https://iwd.wiki.kernel.org/networkconfigurationsettings>