

Usługi i aplikacje Internetu rzeczy (PBL5)

Komunikacja z wykorzystaniem standardów 802.11 (Wifi)

Aleksander Pruszkowski

Instytut Telekomunikacji Politechniki Warszawskiej

Wprowadzenie

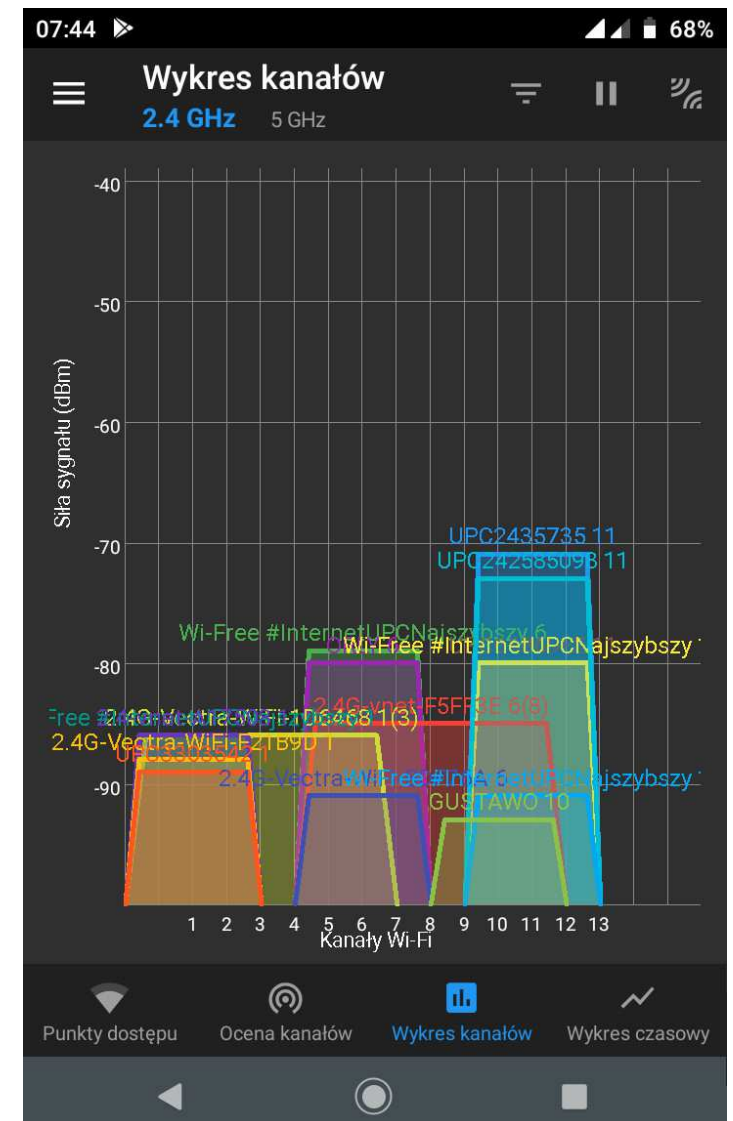
Wprowadzenie

■ Standard 802.11 – historia

■ 1997	802.11	2,4GHz	1...2Mbit/s
■ 1999	802.11a	5GHz	6...54Mbit/s
■ 1999	802.11b	2,4GHz	1...11Mbit/s
■ 2003	802.11g	2,4GHz	6...54Mbit/s
■ 2009	802.11n	2,4GHz 5GHz	100...600Mbit/s
■ 2013	802.11ac	5GHz	300...6770Mbit/s
■ 2021	802.11ax(wifi6)	2,4GHz 5GHz i 6GHz	<10Gbit/s

Wprowadzenie

- Podstawą działania sieci 802.11xx
 - Łączność radiowa niskiego zasięgu (<1Km, typowo 100m)
 - Łączność nie wymagająca licencji na nadawanie radiowe
 - Pierwotne wersje aż do obecnie stosowanych korzystają z tzw. pasma ISM
 - ISM to pasmo: przemysłowo-naukowo-medyczne (ang. Industrial - Scientific - Medical)
 - Łączność o limitowanej mocy nadajników
 - Europa: do 100mW
 - Japonia: do 10mW
 - USA: do 1W
 - Łączność nie daje gwarancji połączenia ani dostępu do medium
 - Łączność stosuje tzw. rozproszenie widma



Wprowadzenie

- Pasma stosowane w 802.11xx, cd.
 - Pasma dla 5GHz
 - Składa się z kanałów o szerokości min. 10MHz każdy od częstotliwości 5150MHz do 5720MHz (Polska)
 - Szerokość całego pasma to 500MHz
 - Pasma 2,4GHz ma szerokość 80MHz
 - Możliwość formowania kanałów użytecznych o szerokości od 20MHz do 160MHz
 - Użyteczne na całym niemal świecie kanały numerowane są od 36 do 140, z przerwami
 - informacje z wielu źródeł są w tej materii nie spójne
 - Kanały nie nachodzą na siebie(!)

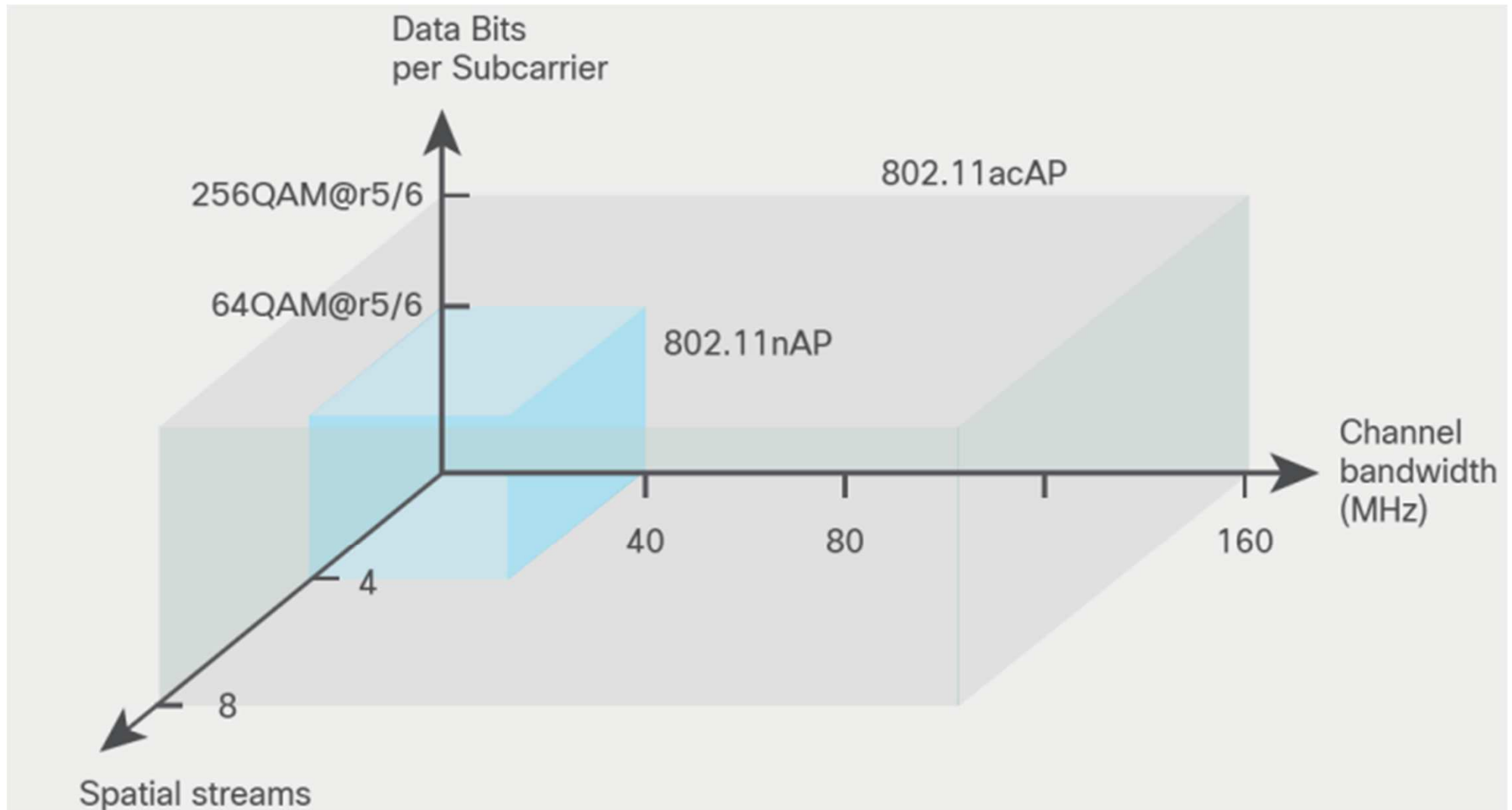
Wprowadzenie

■ Przepływności a pasmo i modulacja

- W standardzie 802.11n stosując modulacja 64-QAM i jeden strumień danych z pasmem 40MHz osiąga transfer na poziomie do 150Mbit/sek.
- W 802.11ac w tych samych warunkach ale z nową modulacja osiągniemy transfer 200Mbit/sek.
 - Poszerzając pasmo radiowe do
 - 80MHz osiągniemy transfer 433Mbit/sek.
 - 160MHz – 867Mbit/sek.
- Potrzeba większego transferu – osiągalna przez zwielokrotnienie strumieni wysyłanych danych
 - Opcja dostępna już w 802.11n – 4 strumienie
 - Strumień to przestrzenne rozłożenie dróg komunikacji (MIMO)
 - 802.11ac – oferuje do 8 strumieni
 - Co daje przy zastosowaniu modulacji 256-QAM i 8 strumieni transfer rzędu 6,93Gbit/sek.

Wprowadzenie

■ Przepływności a pasmo i modulacja, cd.



- Metody rozpraszania widma stosowane w 802.11
 - FHSS - Frequency-hopping spread spectrum
 - Tzw. „skakanie” po częstotliwościach
 - 802.11
 - DSSS - Direct-sequence spread spectrum
 - bezpośrednie modulowanie nośnej sekwencją kodową
 - 802.11, 802.11b
 - OFDM - Orthogonal frequency-division multiplexing
 - metoda zwielokrotnienia w dziedzinie częstotliwości polegająca na jednoczesnej transmisji danych na wielu ortogonalnych częstotliwościach nośnych
 - 802.11a, 802.11g
 - MIMO-OFDM - Multiple-input, multiple-output orthogonal frequency-division multiplexing
 - Metoda łączy techniki MIMO z OFDM
 - 802.11n, 802.11ac , 802.11ax

Wprowadzenie

- Dostęp do medium - CSMA/CA (ang. Carrier Sense Multiple Access with Collision Avoidance)
 - Przypadek w sieci Ad-Hoc
 - 1) urządzenie nasłuchuje czy ktoś nie zajął pasma
 - 2) przeczekuje zadany minimalny czas
 - 3) zaczyna nadawać
 - 4) po zakończeniu oczekuje ramki ACK od odbiorcy
 - 5) nadawca ponawia nadawanie jeżeli nie odbierze ramki ACK
 - Mechanizm nazywany też CCA (ang. Clear Channel Assessment)

Wprowadzenie

■ Dostęp do medium - CSMA/CA (ang. Carrier Sense Multiple Access with Collision Avoidance), cd.

■ Sieci BSS – mechanizm DCF (ang. Distributed Coordinated Function)

1) nadawca wysyła ramkę RTS (ang. Request to Send) z planowanym czasem transferu

- pozostałe stacje usłyszawszy tę ramkę wiedzą że ktoś chce coś nadać
- mają zaczekać ze swoimi próbami na czas DIFS

2) punkt dostępowy wysyła ramkę CTS (ang. Clear to Send)

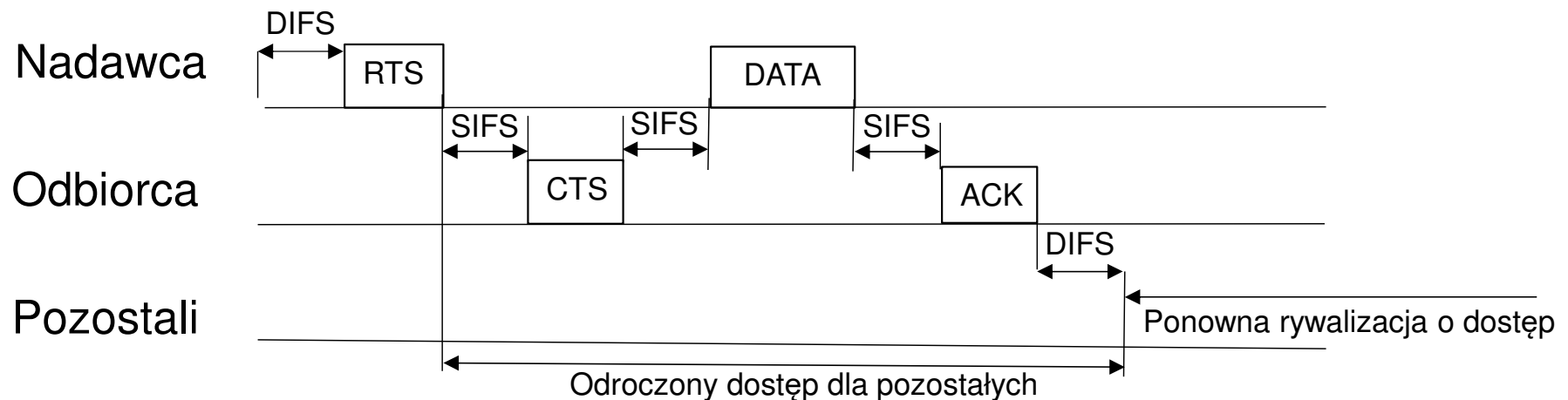
3) nadawca odbierając CTS wie że może nadawać właściwą treść

4) odbiorca potwierdza przez ramkę ACK odebranie właściwej treści

5) nadawca ponawia nadawanie jeżeli nie odbierze ramki ACK

- po czasie RTS-CTS-ACK następuje ponowna rywalizacja o dostęp do medium

■ W obu scenariuszach stacja nasłuchuje gdy nie nadaje



DIFS - Distributed Inter-Frame Space (28..128us)
SIFS - Short Inter-frame Spacing (6..28us)

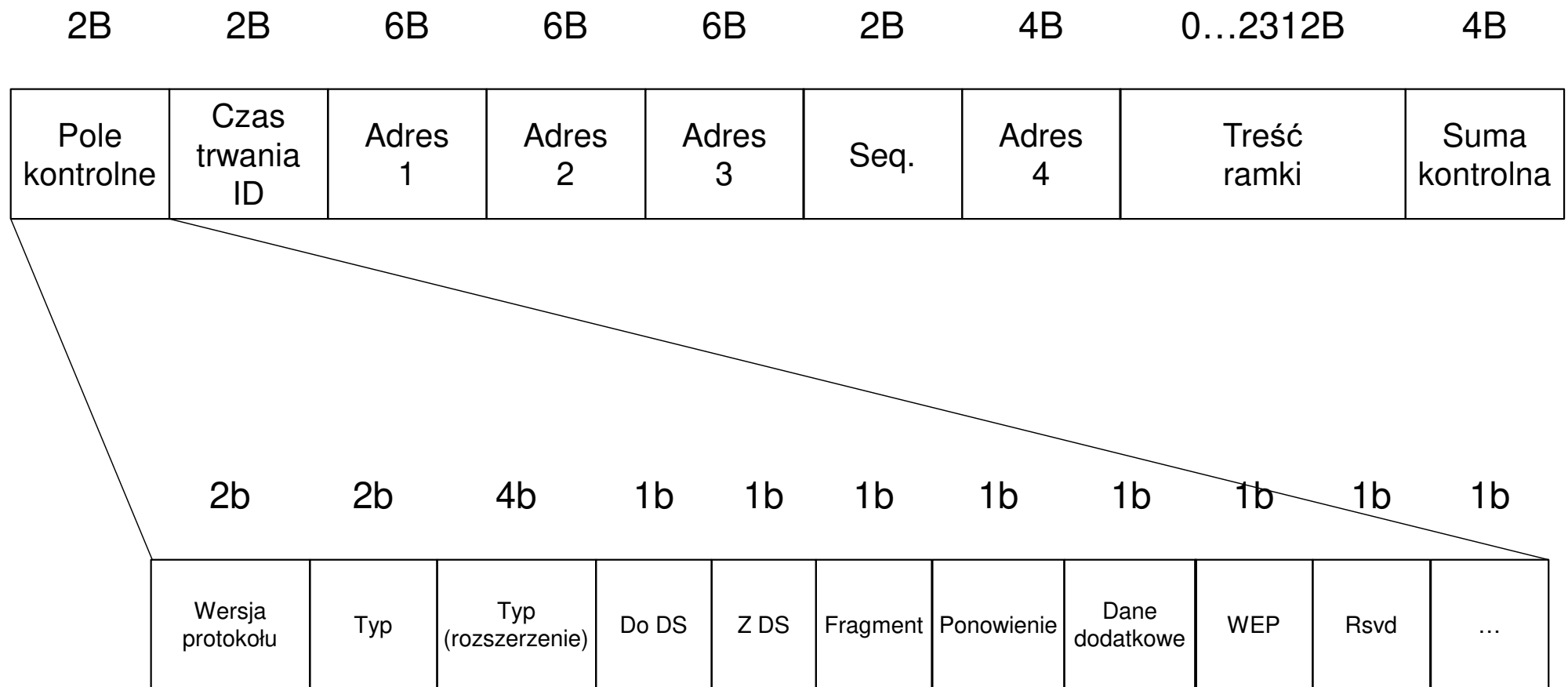
Wprowadzenie

- Dostęp do medium - CSMA/CA (ang. Carrier Sense Multiple Access with Collision Avoidance), cd.
 - Zalety
 - Równość
 - każda stacja ma te same szanse
 - Kolizje i zakłócenia mają prawo wystąpić
 - Wady
 - Trudno ustalić kiedy uda się otrzymać dostęp do medium
 - Im w sieci więcej użytkowników tym większa liczba kolizji
 - Malej także efektywność zużycia łącza
 - Wymagane dodatkowe informacje (RTS, CTS, ACK)
 - Problem ukrytego węzła (ang. Hidden Terminal)
 - Dwie stacje wysyłają ramkę RTS w niemal tym samym momencie – każda z nich „myślała” że kanał jest wolny

Wprowadzenie

■ Ramki 802.11

- Nagłówki: 32B
- Treść: 0...2312B



Do DS (ToDS) – do systemu rozproszonych elementów (Distributed System)
Z DS (FromDS) – z systemu rozproszonych elementów (Distributed System)

Wprowadzenie

■ Ramki 802.11

■ Ramka Beacon

- Ramka sygnalizacyjna wysyłana przez elementy nadrzędne (np.: punkty dostępowe) do elementów podrzędnych (np.: stacji klienckich)
- Jej zadaniem jest przekazanie potencjalnym klientom informacji o
 - Identyfikatorze SSID elementu nadrzędnego
 - Kanale radiowym na jakim pracuje ten element
 - Wspieranych prędkościach transmisji
 - Mocy sygnału radiowego
 - Użytym zabezpieczeniu

Wprowadzenie

■ Ramki 802.11, cd.

■ Ramka Sonda

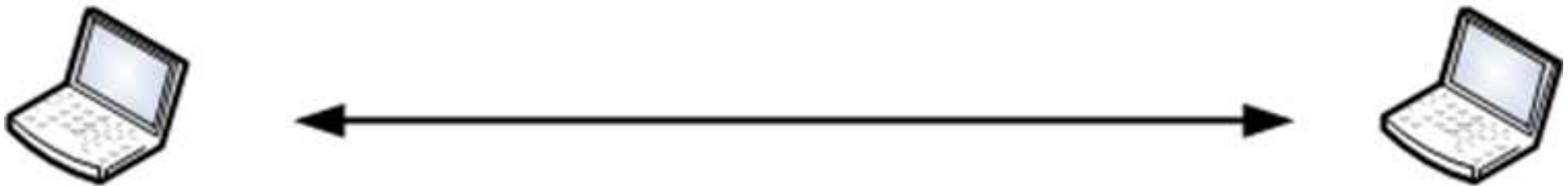
- Wysyłane przez klientów dla odszukania określonej sieci bezprzewodowej do jakiej chcą się dołączyć
- Zawiera identyfikator SSID szukanej sieci Wifi
 - Gdy nie znany jest SSID – tzw. pierwsze połączenie z punktem dostępowym, klient musi odkryć wszystkie te punkty, aby potem wybrać jeden z nich
 - Do tego służy ramka rozgłoszeniowa **Probe Request**
 - Nie zawiera ona identyfikatora SSID
 - Wszystkie punkty dostępowe w zasięgu odpowiadają ramką **Probe Response**

■ Topologie

- IBSS (ang. Independent Basic Service Set) inaczej Ad-Hoc
 - Brak wyróżnionej infrastruktury – każdy komunikuje się z każdym bez pośredników
- BSS (ang. Basic Service Set)
 - Klienci łączą się ze sobą za pomocą centralnego punktu (ang. Access Point)
- ESS (ang. Extended Basic Service Set)
 - Wiele sieci topologii BSS połączonych w jedną większą infrastrukturę za pomocą sieci LAN
- Podejście z Roaming'iem
 - Jak w ESS z wygodnym dla klientów przenoszeniem ich między poszczególnymi BSS
- Sieć z mostem
 - Wiele sieci topologii BSS połączone radio-łączem

Wprowadzenie

- Tryby pracy, cd.
 - **Tryb ad hoc** (Independent Basic Service Set)
 - Inna nazwa to tryb doraźny lub peer-to-peer
 - Tryb gdzie karty sieciowe komunikują się bezpośrednio ze sobą (brak infrastruktury)



■ Tryby pracy

■ **Tryb infrastruktury** (Basic Service Set)

- Inna nazwa to tryb zarządzany
- Typowy tryb działania kart WIFI klienckich
 - W systemie istnieje tzw. punkt dostępowy (ang. Access Point)
 - Klienci łączą się bezpośrednio tylko z punktem dostępowym
 - Punkt dostępowy spełnia funkcję bramy dostępowej za pomocą której łączą się klienci z siecią
 - Także poprzez ten punkt dostępowy łączą się klienci chcący wymieniać dane bezpośrednio między sobą



Wprowadzenie

- Tryby pracy, cd.

- **Tryb master**

- Specyficzny tryb gdzie jedna z kart sieciowych Wifi staje się punktem dostępowym (realizacja w sterowniku)
 - Tryb rzadko stosowany poza sytuacją gdzie tworzony jest punkt dostępowy

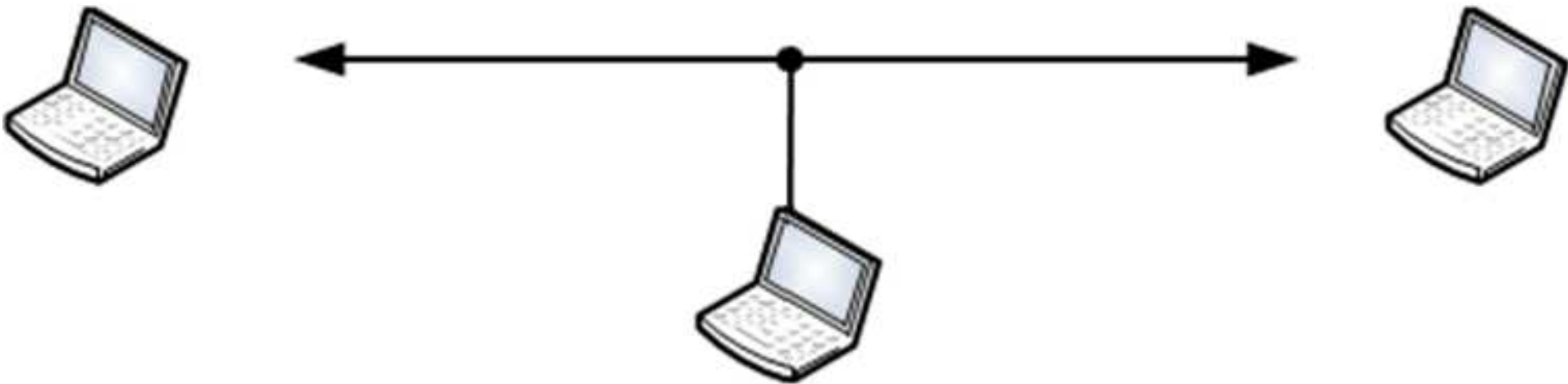


Wprowadzenie

■ Tryby pracy, cd.

■ Tryb monitoringu

- Inna nazwa to RFMON mode lub monitor mode
 - Tryb diagnostyczny – gdzie karta WIFI nasłuchuje ruch sieciowy
 - Tryb przypomina tzw. tryb promiscuous stosowany przez np.: Wireshark w kartach sieciowych ethernet
 - Tryb ten musi być wspierany przez układ radiowy (tzw. chipset) oraz sterowniki karty sieciowej
 - Typowo karty z tymi układami radiowymi są nieco droższe
 - Specjalne aplikacje wspierają ten tryb np.: Kismet, Airodump czy Wireshark

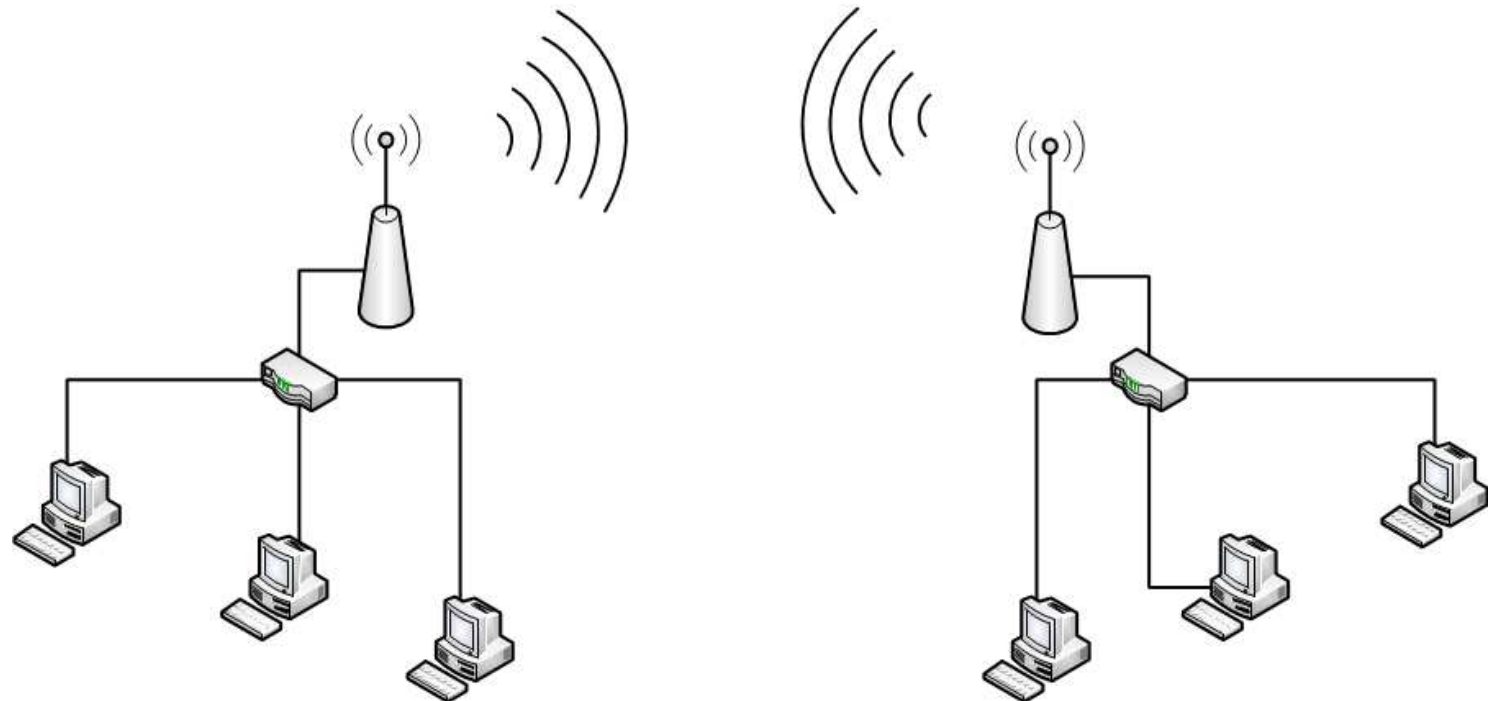


Wprowadzenie

■ Tryby pracy, cd.

■ Tryb mostu punkt-punkt

- Pozwala nam na połączenie ze sobą dwóch sieci zapewniając jednolitą adresację IP
- Dwa AP tworzą most pomiędzy sieciami
 - Cała komunikacja pomiędzy komputerami znajdującymi się w tych sieciach odbywa się dzięki połączeniu zestawionemu pomiędzy punktami dostępowymi
- Stacje klienckie – nie łączą się poprzez sieć Wifi
- Ten typ trybu pracy może być także mostem punkt-wielopunkt

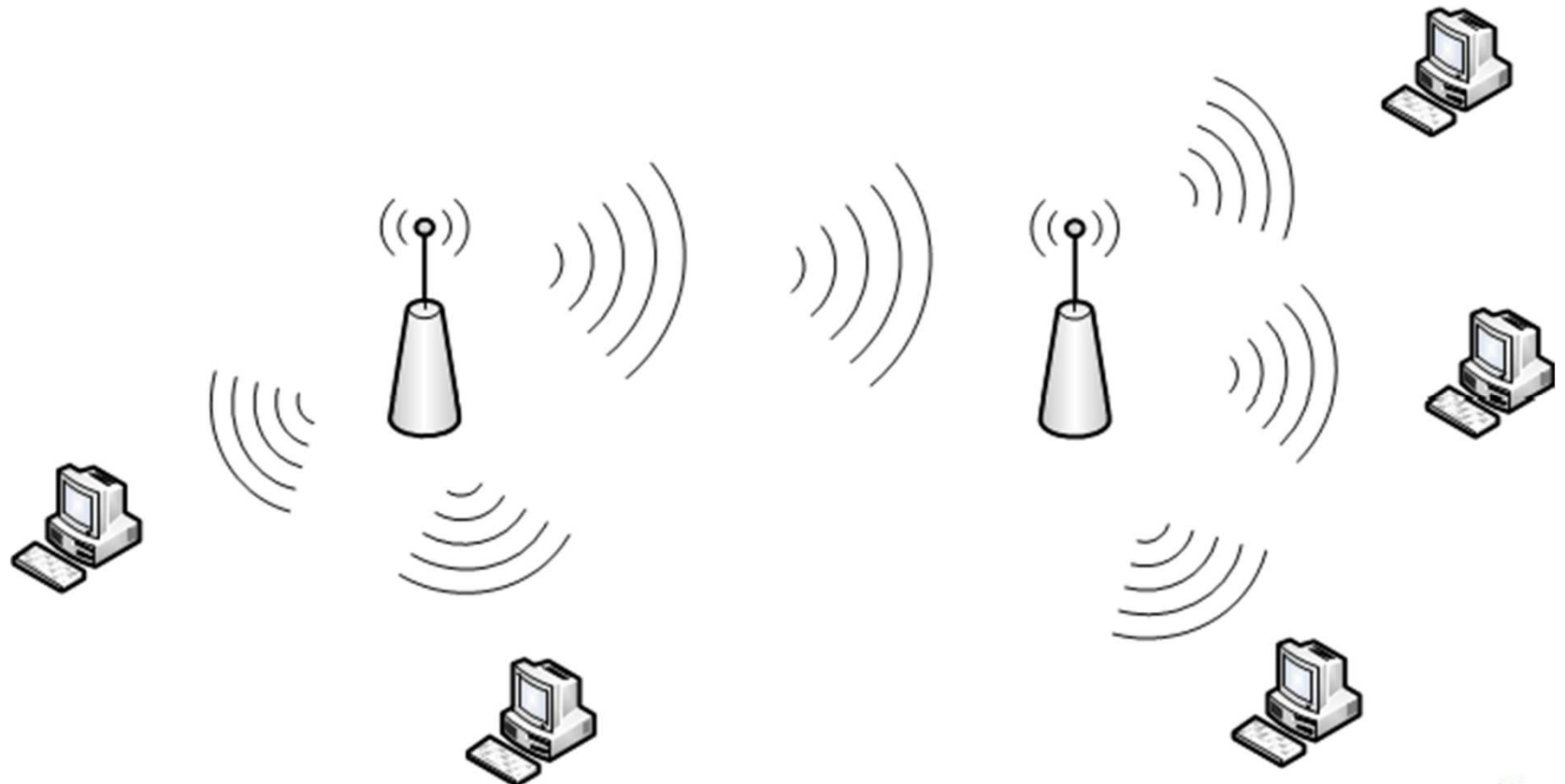


Wprowadzenie

■ Tryby pracy, cd.

■ Tryb repeatera

- Tryb w którym dla pokrycia większego obszaru siecią bezprzewodową instaluje się elementy wzmacniające sygnał
- Uwaga(!) to podejście zwiększa zagęszczenie ruchu sieciowego – całościowo spowalnia transfer
 - Stacja kliencka nadaje pakiet -> repeater odbiera pakiet -> repeater nadaje pakiet



■ Punkt dostępowy (ang. Access Point)

- Łączy „obszar radiowy” z inną siecią (najczęściej Ethernet)
 - W routerach SOHO jest częścią wewnętrznej sieci, która może mieć reguły routowania z innymi sieciami
 - Klasyczny punkt dostępowy nie routuje pakietów (!)
- Posiada jedną lub więcej anten (szyk antenowy)
 - Antena musi być zaprojektowana dla danej częstotliwości radiowej
 - Istnieją punkty dostępowe z anteną
 - wbudowaną (wdrukowaną jako antena PCB)
 - trwale połączoną z resztą elektronik
 - podłączoną poprzez odpowiednie gniazda radiowe - opcja bardzo atrakcyjna umożliwia zastosowanie anteny zwiększającej kierunkowo tzw. zysk antenowy, uwaga na standard złącza: SMA, uFL, ...
 - Anteny mają też określone parametry związane z kierunkowością
 - Dookólne
 - Panelowe, sektorowe, paraboliczne, ...

Wprowadzenie

- Proces dołączania się do sieci 802.11
 - Skanowanie
 - Poznanie otaczających sieci BSS – lista w której są
 - BSSID – identyfikator BSS
 - SSID – nazwa sieci ESS
 - Typ oferowanej łączności (Ad-Hoc czy BSS)
 - Przyłączenie
 - Uwierzytelnienie
 - Open-system
 - Shared-key
 - WEP...
 - Kojarzenie
 - Przydzielanie stacji numeru AID (ang. Association ID)

■ Uwierzytelnienie

- WEP – obecnie nie używany ze względu na to że jest to podejście skompromitowane – nie zaleca się stosowania tej metody
 - Mechanizm WEP - dla zapewnienia bezpieczeństwa i poufność - oparty jest na koncepcji współdzielonego klucza
 - Sieć korzystająca z tego typu zabezpieczenia podatna jest na ataki oraz możliwość podsłuchania transferowanych danych
 - Mimo ułomności dla zapewnienia zgodności wstecznej metoda ta jest nadal implementowana

Wprowadzenie

■ Uwierzytelnienie, cd.

■ WPA2/3

■ WPA - Personal

■ WPA - Enterprise

■ 802.1x (Extensible Authentication Protocol)

■ WPA2 istnieje od 2004

- Oddzielono proces uwierzytelnienia użytkowników od mechanizmów zapewniania integralności i poufności transferowanych danych

Wprowadzenie

■ Uwierzytelnienie, cd.

- Proces konfigurowania profilu zabezpieczeń
 - Ustalenie algorytmu zabezpieczeń: WEP, WPA, WPA2, RADIUS
 - Ustalenie klucza sieci
 - Dla uwierzytelnienia z zewnętrznym serwerem (RADIUS) - podanie tzw. realm i odpowiedniego hasła
 - Realm przykład: student@elektron

Wprowadzenie

■ Kojarzenie

- Ostatni etap
- Proces ustanowienia kanału komunikacyjnego między klientem Wifi a punktem dostępowym
- Składa się z kroków
 - Finalizacja opcji zabezpieczeń
 - Ustalanie szybkość transmisji
 - Zestawienie łącza transmisji
 - Przypisanie klientowi identyfikatora skojarzenia tzw. AID (Association Identifier)
 - Odpowiednik portu przełącznika sieciowego w sieciach przewodowych
 - Punkt dostępowy na bazie tego identyfikatora rozróżnia podłączonych klientów

Łączność 802.11 – aspekty praktyczne system Linux

Łączność 802.11 – aspekty praktyczne

■ Stacje klienckie

■ Narzędzia z GUI

- Mało ciekawe i brak w nim wielu ważnych aspektów czy opcji ale proste w używaniu

■ Narzędzia linii poleceń

- Pakiety wpasupplicant i wireless-tools – ten ostatni zawiera

- ip / ifconfig

- Generyczne narzędzie zmiany parametrów kart sieciowych

- iwconfig

- Główne narzędzie konfiguracji kart wifi

- iwlist

- Narzędzie szczegółowej inspekcji karty wifi

- iwgetid

- Inspekcja elementów infrastruktury sieci bezprzewodowej (NWID - Network Interface Description, ESSID, AP/Cell adres)

- iwevent

- Narzędzie raportujące zdarzenia generowane przez kartę wifi

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **ip** / **ifconfig**

- Podstawowe narzędzie ustawiania i inspekcji interfejsów sieciowych
 - Narzędzie *ifconfig* jest uznawane za przestarzałe, choć jest nadal używane – pokazuje liczbę pakietów odebranych, transmitowanych i błędnych

```
apruszko@raspberrypi0w19:~ $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether b8:27:eb: brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.58/24 brd 10.0.0.255 scope global dynamic noprefixroute wlan0
        valid_lft 3566sec preferred_lft 3116sec
    inet6 fe80::27fc:e639:4daa:6a29/64 scope link
        valid_lft forever preferred_lft forever
```

```
apruszko@raspberrypi0w19:~ $ ifconfig
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 117 bytes 8907 (8.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 117 bytes 8907 (8.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.58 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::27fc:e639:4daa:6a29 prefixlen 64 scopeid 0x20<link>
    ether b8:27:eb: txqueuelen 1000 (Ethernet)
    RX packets 117 bytes 19798 (19.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 121 bytes 21764 (21.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Bez *ifconfig* liczby pakietów dostępne są poprzez plik: **/proc/net/dev** – choć dane są mniej czytelne (obróbka „maszynowa”)

Obecnie *ifconfig* trzeba uruchamiać jako „root” albo z pełną ścieżką: **/sbin/ifconfig**

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **ip**

- W systemach zgodnych z Debian (Ubuntu, Mint, Kali, Raspbian OS, ...) jest to składnik pakietu *iproute2*

■ Składania

- **ip** *opcje* **obiekt** polecenie ...

- Obiekty (wybrane)
 - address lub addr lub a – adresy IP v4 i IP v6 warstwy IP i MAC przypisane kartom sieciowym
 - link – adresy warstwy MAC
 - neighbour – tablice odwzorowań protokołów ARP (Address Resolution Protocol) i NDISC (Neighbour Discovery table)
 - route – tablica routingu

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **ip**

- W systemach zgodnych z Debian (Ubuntu, Mint, Kali, Raspbian OS, ...) jest to składnik pakietu *iproute2*

■ Przykłady

`ip addr add 192.168.0.1 dev wlan0` – ustawienie adresu interfejsu wlan0

`ip link set wlan0 up` – uaktywnienie interfejsu

`ip link set wlan0 down` – dezaktywacja interfejsu

`ip route show` – inspekcja tablicy routingu

`ip route add 10.0.0.1/24 via 192.168.1.1 dev wlan0` – dodanie statycznej trasy przez 192.168.1.1 i urządzenie wlan0 dla osiągnięcia sieci 10.0.0.1/24

`ip route del 10.0.0.1/24` – usunięcie trasy do 10.0.0.1/24

■ Identyfikatory sieci bezprzewodowych (uporządkowanie pojęć)

■ SSID (Service set identifier) – nazwa sieci BSS

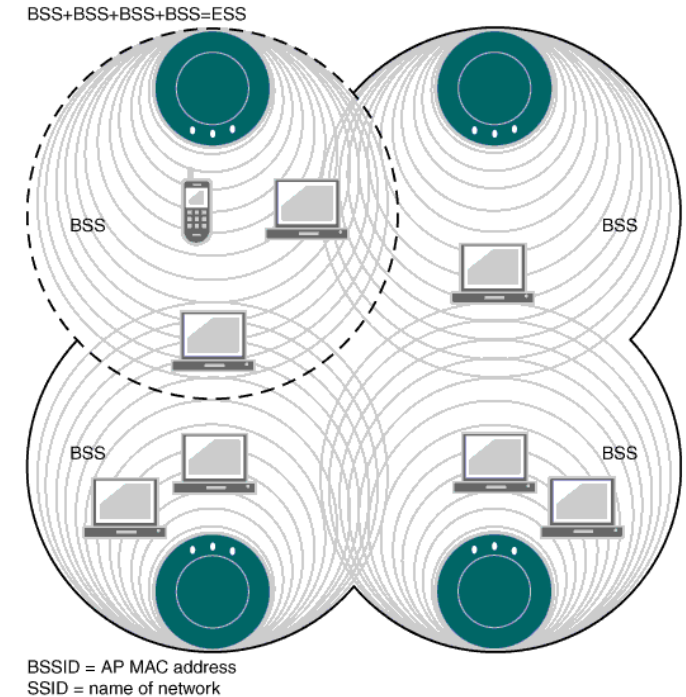
- Unikalna tekstowa nazwa określonej sieci Wifi
 - Może składać się z wielu punktów dostępowych
 - Na tym identyfikatorze koncentruje uwagę użytkownik
 - Nazwa może mieć długości do 32 znaków (UTF-8)

■ ESSID (Extended service set)

- Dla użytkownika jest to odpowiednik SSID tyle, że dla systemu z wieloma AP zarządzanymi wspólnie

■ BSSID (Basic Service Set Identifier)

- Niepowtarzalny identyfikator każdego urządzenia bezprzewodowego – typowo identyfikator określonego BSS
- Identyfikator BSSID to adres MAC urządzenia, fizycznie jest to 48 bitowy adres MAC punktu dostępowego
- Jest częścią każdego pakietu transmitowanego poprzez karty sieciowe Wifi



Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwconfig**

- Podstawowe narzędzie konfiguracji interfejsu sieci bezprzewodowej Wifi

```
apruszko@raspberrypi0w19:~ $ iwconfig
lo          no wireless extensions.

wlan0       IEEE 802.11  ESSID:"j23nadaje2i"
            Mode:Managed  Frequency:2.412 GHz  Access Point: 76:AC:B9:
            Bit Rate=65 Mb/s   Tx-Power=31 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Power Management:on
            Link Quality=70/70  Signal level=-31 dBm
            Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
            Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

■ Składnia

`iwconfig <nazwa_interfejsu> parametry argumenty...`

■ Parametry

- **ESSID** - ustalenie identyfikatora komórki tworzącej wirtualną sieć (mogąca składać się z wielu elementów takich jak punkt dostępowy lub repeater)

- Przykład

```
iwconfig wlan0 essid "My Network"
```

■ Narzędzia – **iwconfig**, cd.

■ Parametry

■ **mode** – ustalenie trybu działania karty, dozwolone tryby

- Ad-Hoc, Managed, Master, Repeater, Monitor
- Secondary (zapasowy punkt dostępowy)
- lub Auto (znaczenie nie jasne)
- Przykłady

```
iwconfig wlan0 mode Managed
```

```
iwconfig wlan0 mode Ad-Hoc
```

■ **freq** lub **channel** – ustalenie częstotliwości lub kanału na jakim ma działać karta

- Wartości poniżej 1000 określają kanał, powyżej częstotliwość
- Przykłady

```
iwconfig wlan0 freq 2422000000 równoważne iwconfig wlan0 freq 2.422G
```

```
iwconfig wlan0 channel 3
```

```
iwconfig wlan0 channel auto
```

- Dla trybów Ad-Hoc taka specyfikacja może być ignorowana gdy karta dołącza się do innych urządzeń – one wpływają na wybrane parametry połączenia

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwconfig**, cd.

■ Parametry, cd.

- **ap** – wymuszenie dołączenia się do określonego punktu dostępowego – wskazanego jako argument

- Przykład

```
iwconfig wlan0 ap 12:34:56:78:9a:bc
```

- **rate** lub **bit** – gdy karta wspiera wiele różnych przepływności wskazanie którą chcemy używać (nie zawsze najszybsze jest najlepsze)

- Przykład

```
iwconfig wlan0 rate 11M
```

- Wybranie 5.5M lub mniejszej przepływności

```
iwconfig wlan0 rate 5.5M auto
```

- **txpower** – gdy karta wspiera możliwość regulacji mocy nadajnika, ustalenie tej mocy

- Przydatne gdy chcemy nie przeszkadzać sobie nawzajem lub zmniejszyć szansę podsłuchania

- Przykłady

```
iwconfig wlan0 txpower 15 – ustalenie mocy w dBm
```

```
iwconfig wlan0 txpower 30mW – ustalenie mocy w mW
```

```
iwconfig wlan0 txpower off – wyłączenie radia
```

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwconfig**, cd.

■ Parametry, cd.

- **sens** – ustalenie poziomu czułości, jak karta ma postępować gdy warunki transmisji będą złe

- W nowych kartach poziom pozwala na uruchomienie roamingu – przejścia do innego punktu dostępowego
- W starszych kartach – próg kiedy to transmisja jest przerywana a kanał uznany jako zajęty
- Gry argument >0 oznacza surową albo procentową wartość odbieranego sygnału jako próg, gdy <0 jest to wartość w jednostkach dBm
- Przykłady

```
iwconfig wlan0 sens -80
```

```
iwconfig wlan0 sens 2
```

- **retry** – ustalenie liczby powtórzeń

- Przykłady

```
iwconfig wlan0 retry 16 – do 16 powtórzeń
```

```
iwconfig wlan0 retry lifetime 300m – powtarzaj przez 300m sek.
```

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwconfig**, cd.

■ Parametry, cd.

- **rts** – zwiększa długość najmniejszego pakietu RTS dla upewnienia się że kanał jest czysty, mechanizm w efekcie zmniejsza szybkość transferu ale system staje się odporniejszy na zjawisko ukrytego terminala (hidden terminal)

- Przykłady

```
iwconfig wlan0 rts 250
```

```
iwconfig wlan0 rts off – wyłączenie mechanizmu RTS/CTS
```

- **frag** – wprowadzenie fragmentaryzacji pakietów, pozwala w środowisku z dużymi zakłóceniami o charakterze impulsowym przesłać poprawnie więcej pakietów (minimalizacja „wstrzelenia” się zakłócenia niszczącego cały pakiet)

- Przykłady

```
iwconfig wlan0 frag 512
```

```
iwconfig wlan0 frag off – wyłączenie mechanizmu
```

- **modu** – wymuszenie określonej modulacji (listę wspieranych - udostępnia iwlist)

- Przykłady

```
iwconfig wlan0 modu 11g
```

- **commit** – niektóre karty wymagają wydania tego polecenia aby wymusić uaktywnienie zmian wcześniej wykonanych

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwlist**

- Sprawdzenie jakie punkty dostępowe i węzły Ad-Hoc są w okolicy i jakie są ich parametry

```
apruszko@raspberrypi0w19:~ $ iwlist wlan0 scanning
wlan0      Scan completed :
            Cell 01 - Address: 76:AC:B9:
                Channel:1
                Frequency:2.412 GHz (Channel 1)
                Quality=70/70  Signal level=-32 dBm
                Encryption key:on
                ESSID:"j23nadaje2i"
                Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                        9 Mb/s; 12 Mb/s; 18 Mb/s
                Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                Mode:Master
                Extra:tsf=0000000000000000
                Extra: Last beacon: 645680ms ago
                IE: IEEE 802.11i/WPA2 Version 1
                    Group Cipher : CCMP
                    Pairwise Ciphers (1) : CCMP
                    Authentication Suites (1) : PSK
```


Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwlist**, cd.

- Jakie częstotliwości wspiera określona karta
 - Informacje te mogą zależeć od lokalizacji w jakiej działa urządzenie (ustalanej przez użytkownika a utrzymywanej przez system operacyjny)

```
apruszko@raspberrypi0w19:~ $ iwlist wlan0 channel
wlan0      13 channels in total; available frequencies :
           Channel 01 : 2.412 GHz
           Channel 02 : 2.417 GHz
           Channel 03 : 2.422 GHz
           Channel 04 : 2.427 GHz
           Channel 05 : 2.432 GHz
           Channel 06 : 2.437 GHz
           Channel 07 : 2.442 GHz
           Channel 08 : 2.447 GHz
           Channel 09 : 2.452 GHz
           Channel 10 : 2.457 GHz
           Channel 11 : 2.462 GHz
           Channel 12 : 2.467 GHz
           Channel 13 : 2.472 GHz
           Current Frequency:2.412 GHz (Channel 1)
```

Łączność 802.11 – aspekty praktyczne

■ Narzędzia – **iwgetid**

- Pobranie adresu MAC punktu dostępowego z jakim współpracujemy

```
apruszko@raspberrypi0w19:~ $ iwgetid wlan0 --ap  
wlan0      Access Point/Cell: 76:AC:B9:
```

- Częstotliwość pracy

```
apruszko@raspberrypi0w19:~ $ iwgetid wlan0 --freq  
wlan0      Frequency:2.412 GHz
```

- Tryb pracy

```
apruszko@raspberrypi0w19:~ $ iwgetid wlan0 --mode  
wlan0      Mode:Managed
```

- Protokół

```
apruszko@raspberrypi0w19:~ $ iwgetid wlan0 --protocol  
wlan0      Protocol Name:"IEEE 802.11"
```

- Kanał

```
apruszko@raspberrypi0w19:~ $ iwgetid wlan0 --channel  
wlan0      Channel:1
```

Zadanie:

Używając narzędzi systemu Linux (maszyna wirtualna: unifi4test) pobierz aktualną listę dostępnych w okolicy punktów dostępowych podając ich ESSID oraz adres MAC

Łączność 802.11 – aspekty praktyczne system Windows

Łączność 802.11 – aspekty praktyczne (Windows)

■ Informacje o sterowniku - **netsh wlan show drivers**

Interface name: Wi-Fi

Driver : **Intel(R) Centrino(R) Wireless-N 130**
Vendor : Intel Corporation
Provider : Microsoft
INF file : netwsw00.inf
Type : Native Wi-Fi Driver
Radio types supported : **802.11b 802.11g 802.11n**
FIPS 140-2 mode supported : Yes
802.11w Management Frame Protection supported : No
Hosted network supported : Yes
Authentication and cipher supported in infrastructure mode:

Open	None
Open	WEP-40bit
Open	WEP-104bit
Open	WEP
WPA-Enterprise	TKIP
WPA-Enterprise	CCMP
WPA-Personal	TKIP
WPA-Personal	CCMP
WPA2-Enterprise	TKIP
WPA2-Enterprise	CCMP
WPA2-Personal	TKIP
WPA2-Personal	CCMP
Open	Vendor defined

Authentication and cipher supported in ad-hoc mode:

Open	None
Open	WEP-40bit
Open	WEP-104bit
Open	WEP
WPA2-Personal	CCMP

Wireless Display Supported: No (Graphics Driver: No, Wi-Fi Driver: No)

TKIP (Temporal Key Integrity Protocol), obecnie wycofywany na rzecz CCMP (Counter Mode CBC-MAC Protocol) stający się standardem

Łączność 802.11 – aspekty praktyczne (Windows)

■ Informacje sieciach w okolicy – **netsh wlan show interface**

Interface name : Wi-Fi

There are **8 networks** currently visible.

SSID 1 : j23nadaje2

Network type	:	Infrastructure
Authentication	:	WPA2-Personal
Encryption	:	CCMP
BSSID 1	:	74:ac:b9:xx:xx:xx
Signal	:	99%
Radio type	:	802.11n
Channel	:	1
Basic rates (Mbps)	:	6.5 16 19.5 24 39 117 156
Other rates (Mbps)	:	18 19.5 36 48 54

SSID 2 : UPC2435735

Network type	:	Infrastructure
Authentication	:	WPA2-Personal
Encryption	:	CCMP
BSSID 1	:	c4:27:95:xx:xx:xx
Signal	:	58%
Radio type	:	802.11n
Channel	:	11
Basic rates (Mbps)	:	1 2 5.5 11
Other rates (Mbps)	:	6 9 12 18 24 36 48 54

SSID 3 : ...

Łączność 802.11 – aspekty praktyczne (Windows)

- Informacje obecnej w komputerze karcie sieciowej –

netsh wlan show interface

There is 1 interface on the system:

```
Name : Wi-Fi
Description : Intel(R) Centrino(R) Wireless-N 130
GUID : 236bf5c1-78f1-4943-a906-5315033cff34
Physical address : b8:03:05:xx:xx:xx
State : connected
SSID : j23nadaje2
BSSID : 74:ac:b9:xx:xx:xx
Network type : Infrastructure
Radio type : 802.11n
Authentication : WPA2-Personal
Cipher : CCMP
Connection mode : Auto Connect
Channel : 1
Receive rate (Mbps) : 72
Transmit rate (Mbps) : 72
Signal : 99%
Profile : j23nadaje2

Hosted network status : Not started
```

Łączność 802.11 – aspekty praktyczne (Windows)

- Informacje zapisanych profilach sieci z jakimi się komputer łączył -
netsh wlan show profile

Profiles on interface Wi-Fi:

Group policy profiles (read only)

<None>

User profiles

All User Profile	: MiNIa
All User Profile	: j23nadaje2
All User Profile	: moto6g
All User Profile	: No1ok
All User Profile	: SztetkeTyS
All User Profile	: samAPItpw
All User Profile	: d605ap01
All User Profile	: apmr30202019
All User Profile	: BylemJuzRozpaczyBlisko
All User Profile	: meag2b

Łączność 802.11 – aspekty praktyczne (Windows)

■ Eksport profilu – **netsh wlan export profile name=No1ok**

- Powstaje plik Wi-Fi-No1ok.xml, o treści:

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>No1ok</name>
  <SSIDConfig>
    <SSID>
      <hex>4E6F316F6B</hex>
      <name>No1ok</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>true</protected>
        <keyMaterial>...</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
  <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
    <enableRandomization>false</enableRandomization>
  </MacRandomization>
</WLANProfile>
```

Zadanie:

Używając narzędzi systemu Windows (laptop) pobierz możliwie dużo informacji o ostatnio używanym punkcie dostępowym

Kontrolery sieci 802.11

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi

- Przykładem są produkty Unifi firmy Ubiquiti Inc. [ui.com]

- Punkty dostępowe, np.:

- U6 Enterprise, U6 Professional, U6 Lite, ..., UAP-AC-LITE, UAP

- Kontrolery sieci

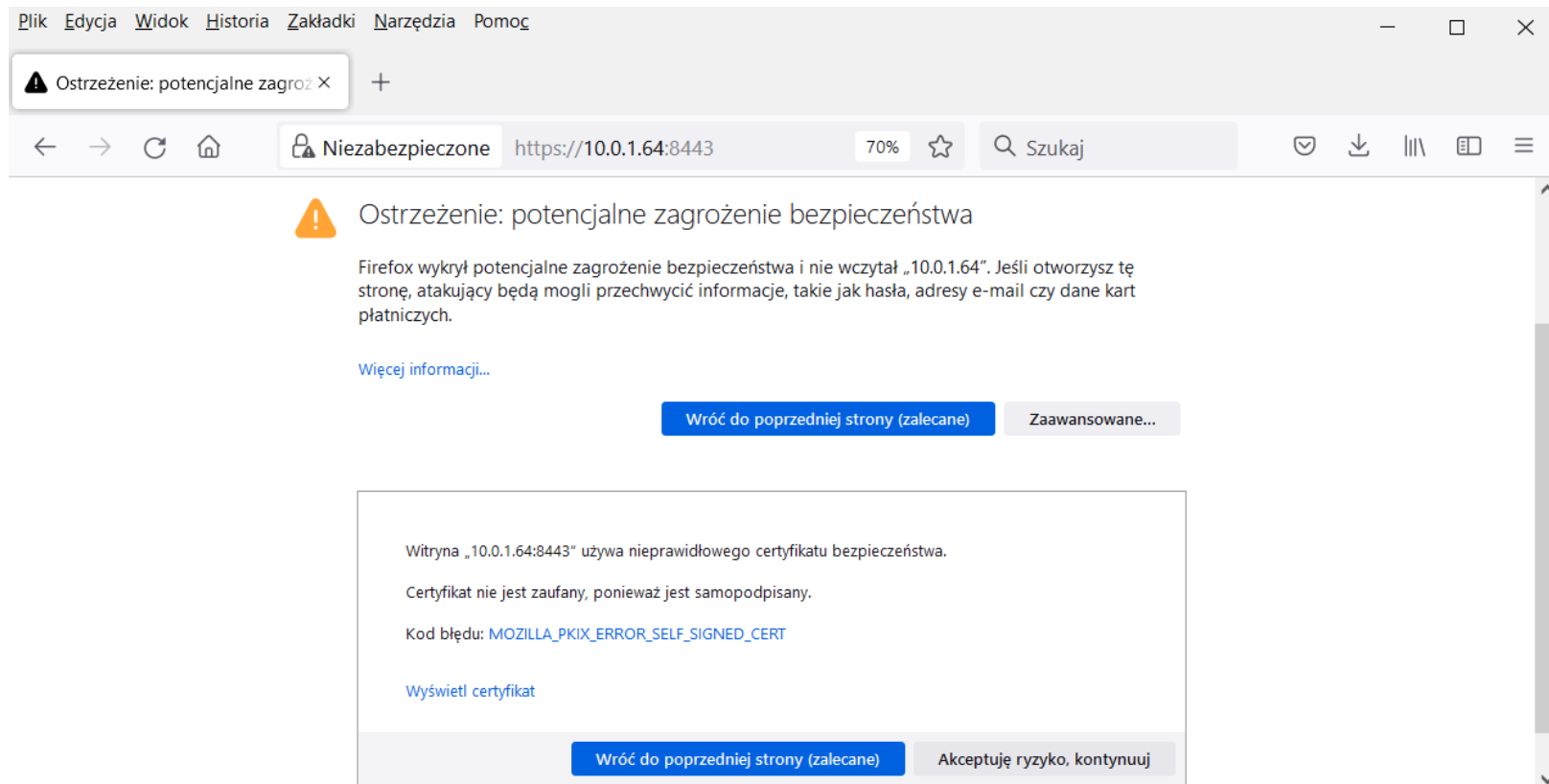
- Dream Machine Pro, Cloud Key Gen2 Plus, ... , Linux/Windows PC



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

- Konfiguracja kontrolera Unifi – zainstalowany na maszynie wirtualnej (Debian)
 - 0. Przeglądarka WWW jak punkt wejścia (URL: `https://__numer_IP__:8443`)

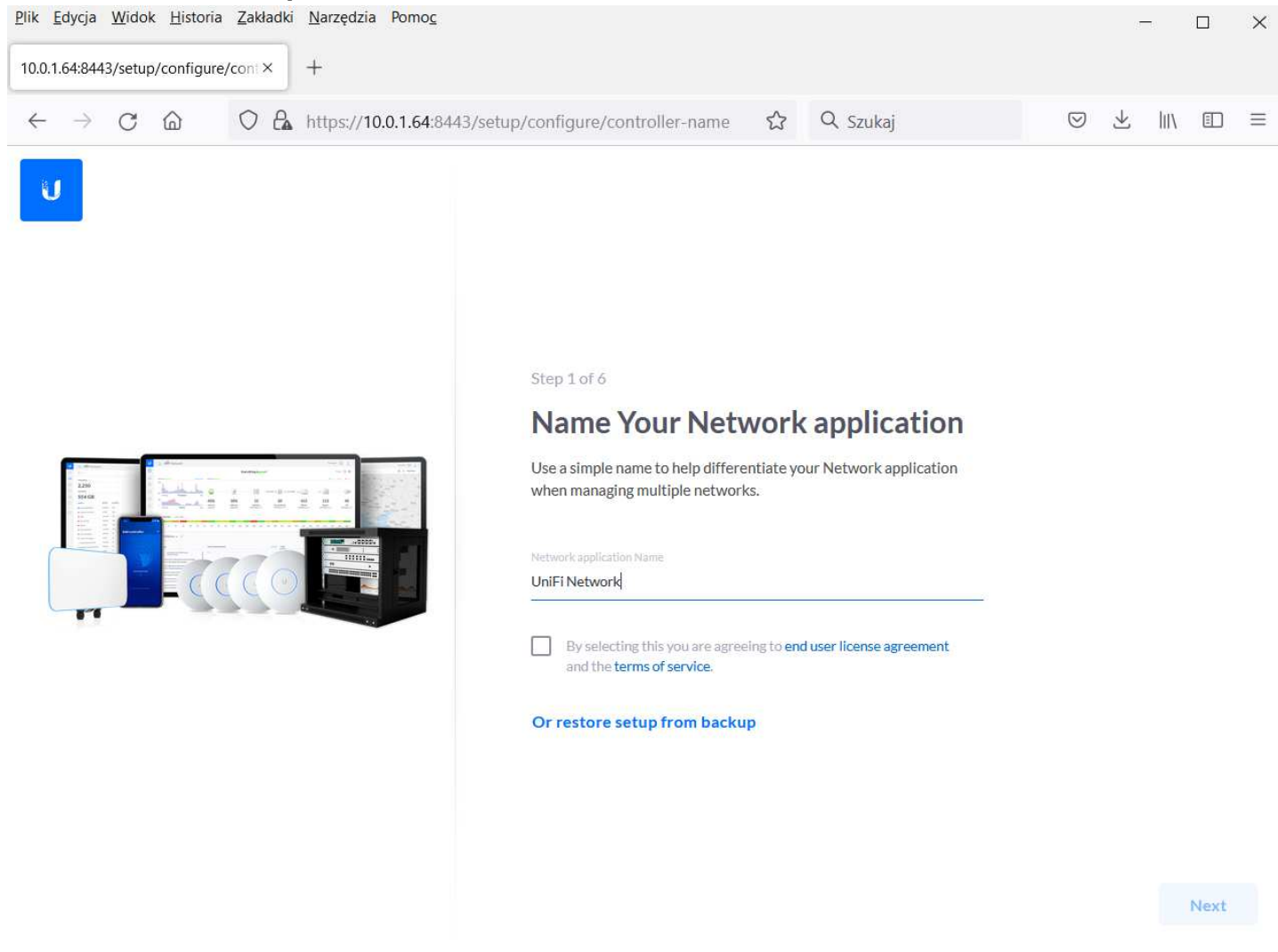


- Typowe zachowanie – produkty na ogół nie posiadają poprawnych i aktywnych kluczy dla protokołu SSL/TLS
 - Tu należy zaakceptować ryzyko – w wersji produkcyjnej można zainstalować właściwe certyfikaty

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

■ 1. Nadanie nazwy sieci/kontrolera



Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

10.0.1.64:8443/setup/configure/cont X

← → ↻ 🏠 🔒 https://10.0.1.64:8443/setup/configure/controller-name ☆ 🔍 Szukaj

U

Step 1 of 6

Name Your Network application

Use a simple name to help differentiate your Network application when managing multiple networks.

Network application Name

UniFi Network

☐ By selecting this you are agreeing to [end user license agreement](#) and the [terms of service](#).

[Or restore setup from backup](#)

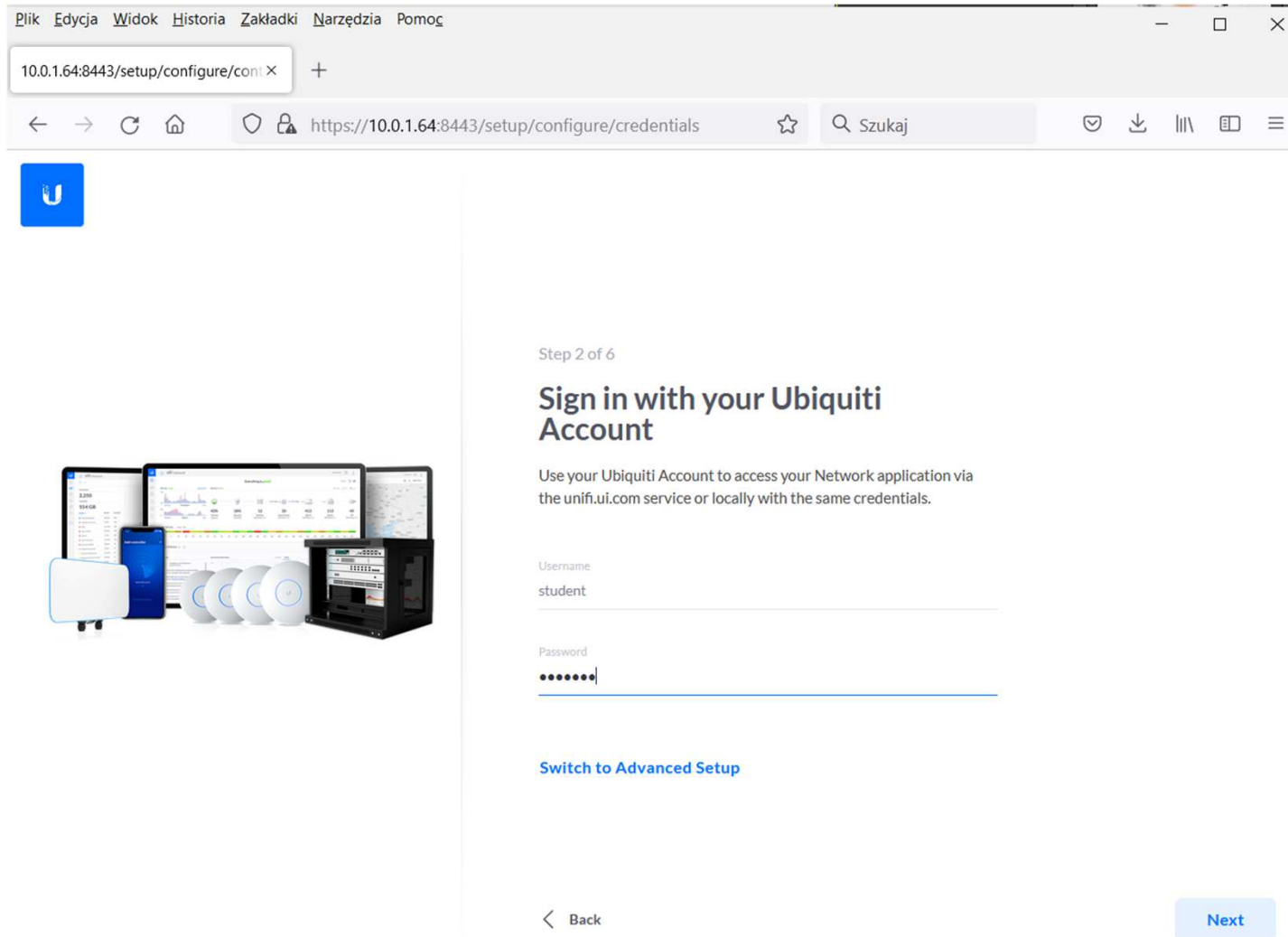
Next

- Gdy mamy wiele kontrolerów pomaga zarządzać nimi

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.


■ 2. Konfiguracja administratora kontrolera – model ze wsparciem Unifi



Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

10.0.1.64:8443/setup/configure/cont X +

← → ↻ 🏠 🔒 https://10.0.1.64:8443/setup/configure/credentials ☆ 🔍 Szukaj 📄 📌 📄 ☰



Step 2 of 6

Sign in with your Ubiquiti Account

Use your Ubiquiti Account to access your Network application via the unifi.ui.com service or locally with the same credentials.

Username
student

Password
••••••

[Switch to Advanced Setup](#)

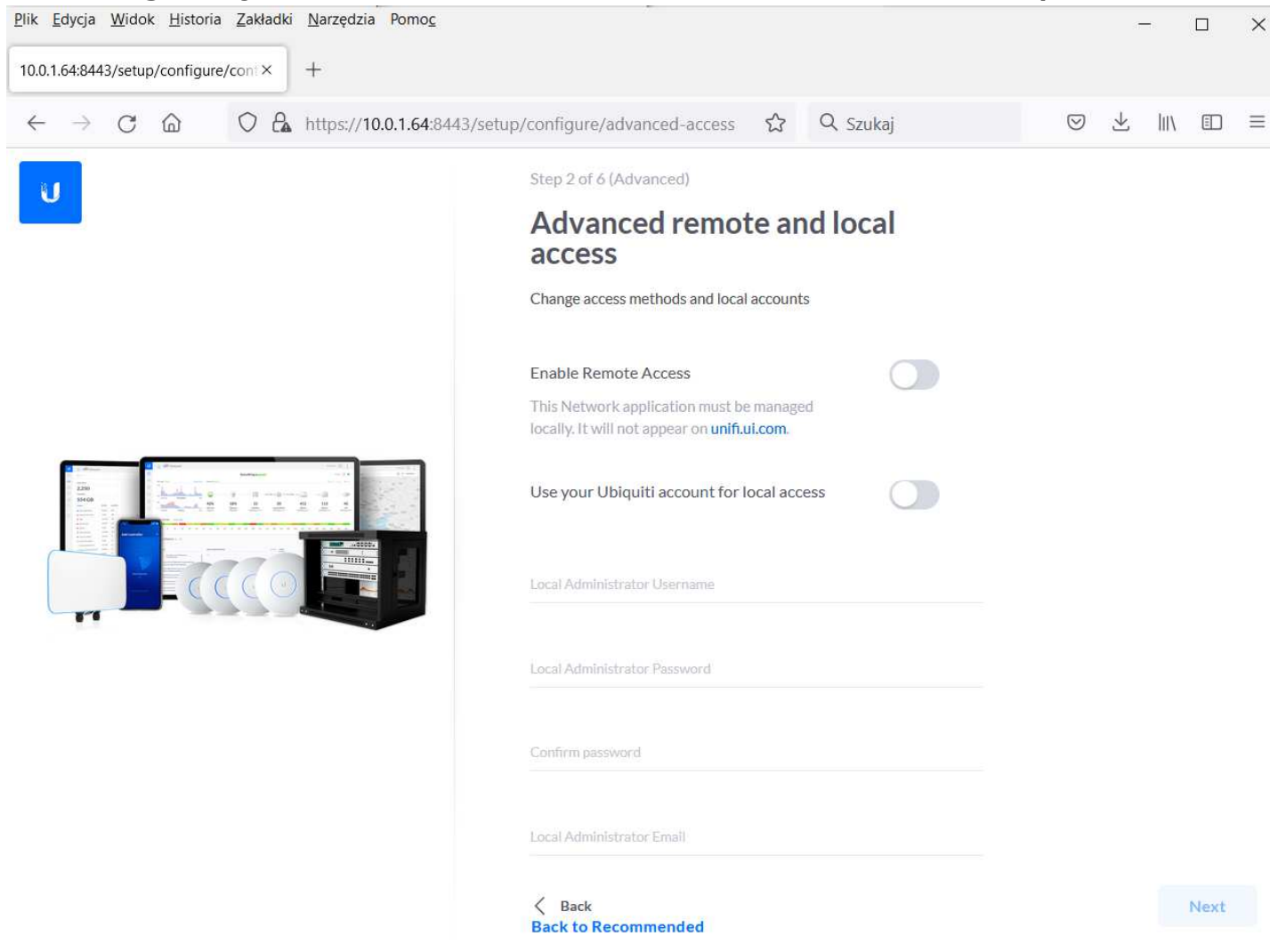
< Back [Next](#)

- Podając login i hasło warto je zapamiętać w bezpieczny sposób – nie znana jest metoda jego odzyskania bez skasowania obecnej konfiguracji
- W laboratorium wybieramy „Switch to Advanced Setup” dla konfiguracji lokalnej

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.


■ 2b. Konfiguracja administratora kontrolera – model lokalny



Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

10.0.1.64:8443/setup/configure/confi X

← → ↺ 🏠 🔒 https://10.0.1.64:8443/setup/configure/advanced-access ☆ 🔍 Szukaj 📧 ⬇️ 📄 📁 ☰



Step 2 of 6 (Advanced)

Advanced remote and local access

Change access methods and local accounts

Enable Remote Access ☐

This Network application must be managed locally. It will not appear on unifi.ui.com.

Use your Ubiquiti account for local access ☐

Local Administrator Username

Local Administrator Password

Confirm password

Local Administrator Email

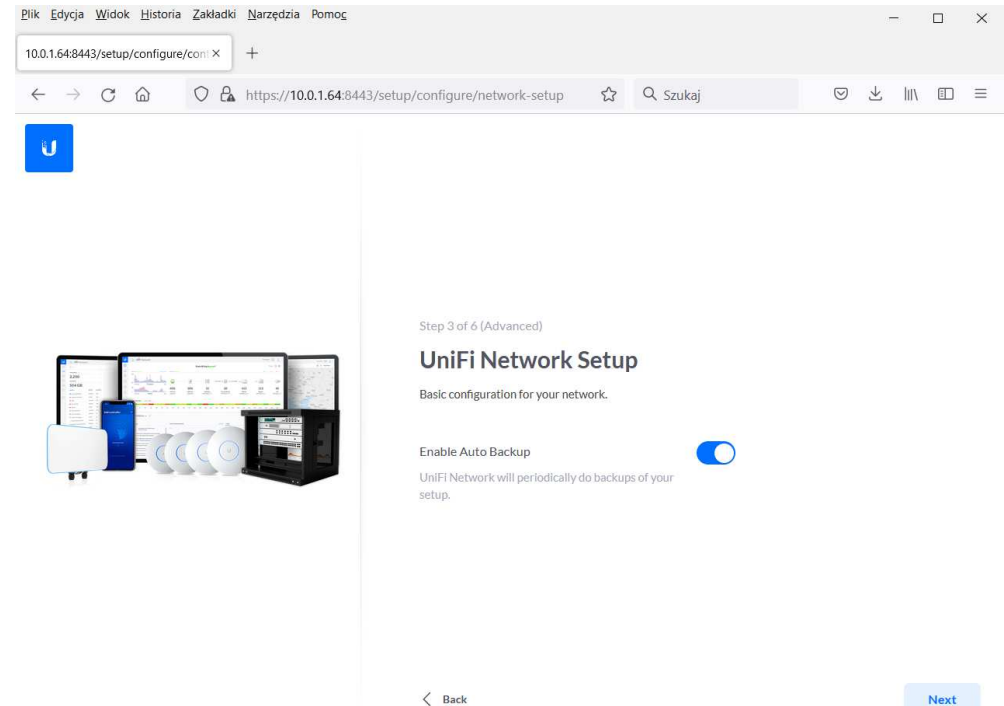
< Back [Back to Recommended](#) [Next](#)

- Dostęp do systemu będzie tylko lokalny, zdalny o ile nasza sieć będzie udostępniać TCP port 8443 dla przeglądarek z innych lokalizacji (typowo np.: port forwarding + ddns)

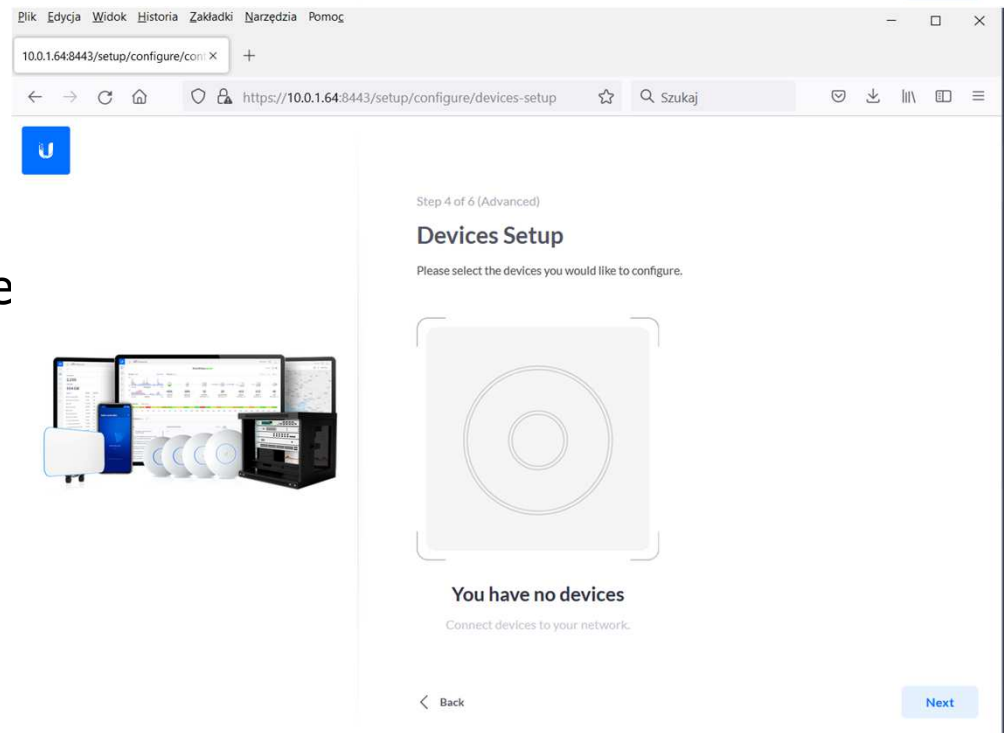
Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

- 3. Rutynowe pytania konfiguratora – automatyczna archiwizacja konfiguracji



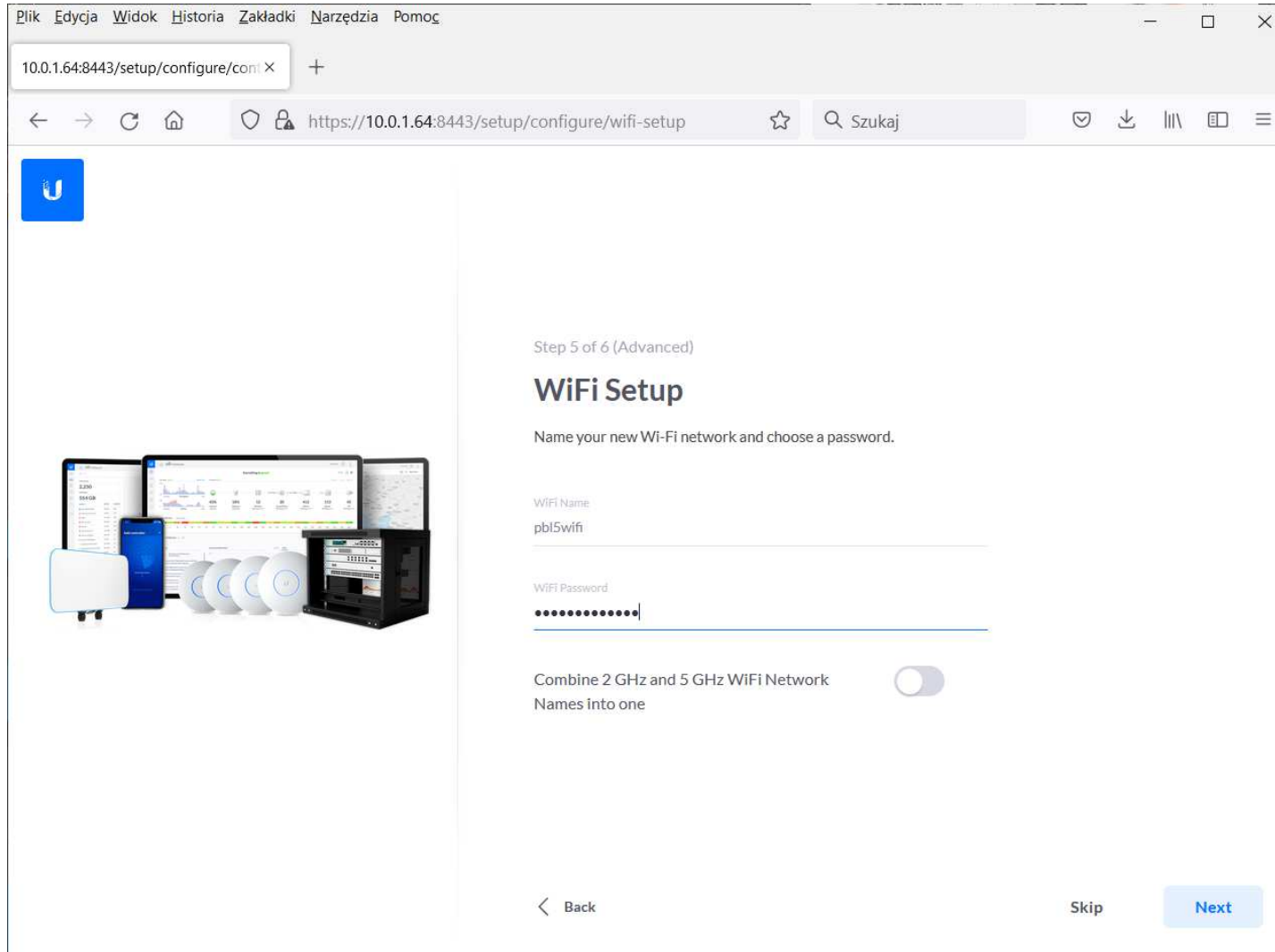
- 4. Konfiguracja urządzeń – w modelu z PC opcja trudna w realizacji, dodawanie urządzeń można realizować inaczej



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.


■ 5. Konfiguracja podstawowej sieci Wifi



Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

10.0.1.64:8443/setup/configure/confi X +

← → ↻ 🏠 🔒 https://10.0.1.64:8443/setup/configure/wifi-setup ☆ 🔍 Szukaj 📧 ⬇️ 📄 📁 ☰



Step 5 of 6 (Advanced)

WiFi Setup

Name your new Wi-Fi network and choose a password.

WiFi Name
pbl5wifi

WiFi Password
●●●●●●●●

Combine 2 GHz and 5 GHz WiFi Network Names into one ☐

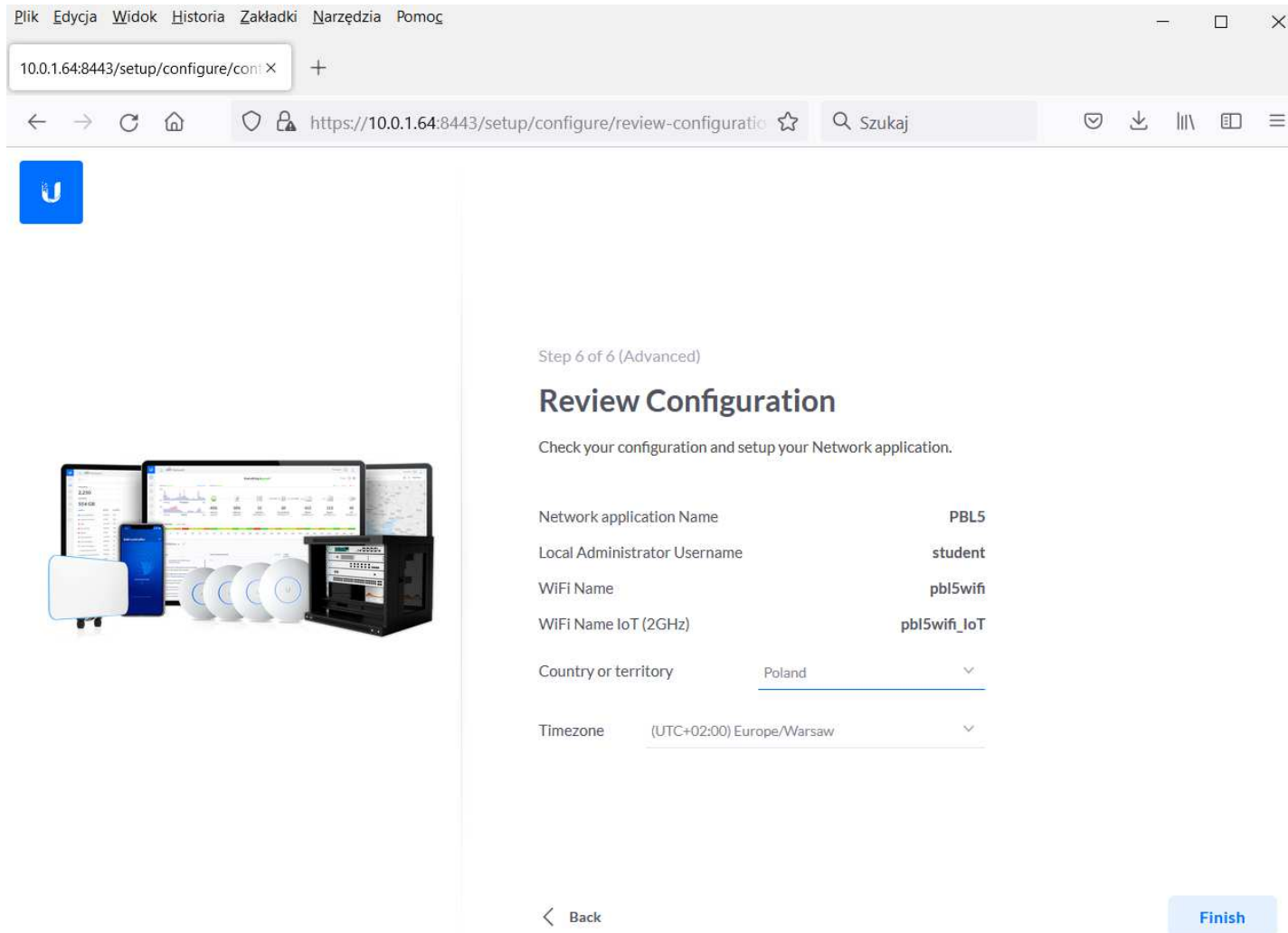
< Back Skip **Next**

- Tutaj ustalamy ESSID sieci i odpowiednie jej hasło

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.


■ 6. Podsumowanie wybranych ustawień



Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

10.0.1.64:8443/setup/configure/conf X +

← → ↻ 🏠 🔒 https://10.0.1.64:8443/setup/configure/review-configuration ☆ 🔍 Szukaj 📧 ⬇️ 📄 📖 ☰



Step 6 of 6 (Advanced)

Review Configuration

Check your configuration and setup your Network application.

Network application Name	PBL5
Local Administrator Username	student
WiFi Name	pbl5wifi
WiFi Name IoT (2GHz)	pbl5wifi_IoT
Country or territory	Poland ▼
Timezone	(UTC+02:00) Europe/Warsaw ▼

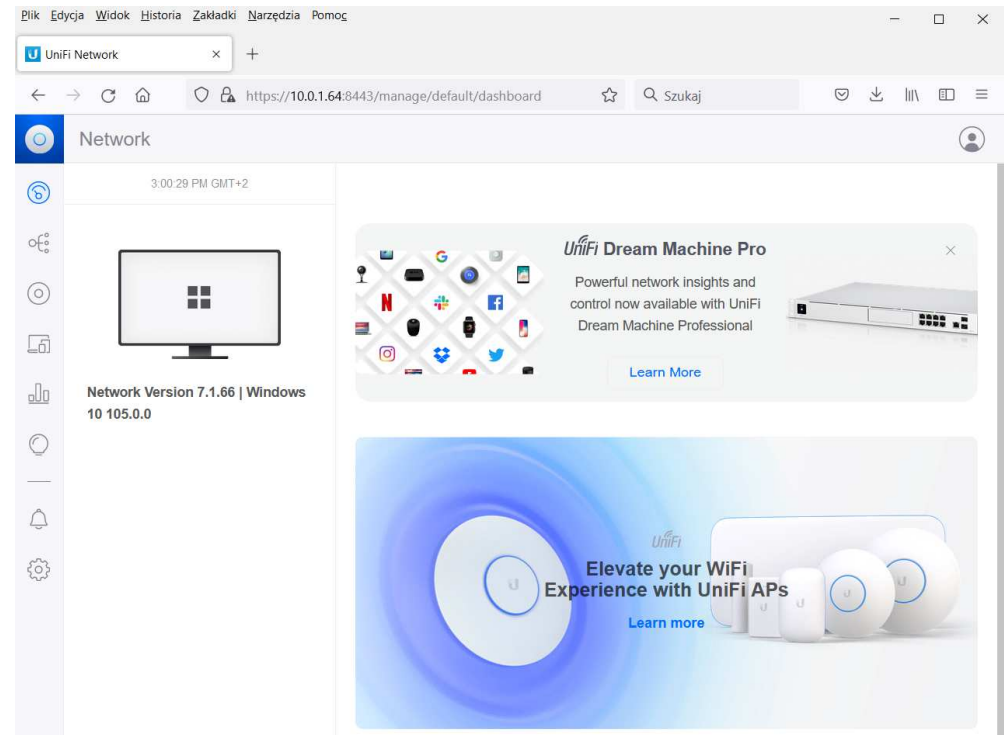
< Back Finish

- Proszę pamiętać że z poziomu kontrolera wiele z powyższych ustawień można zmienić

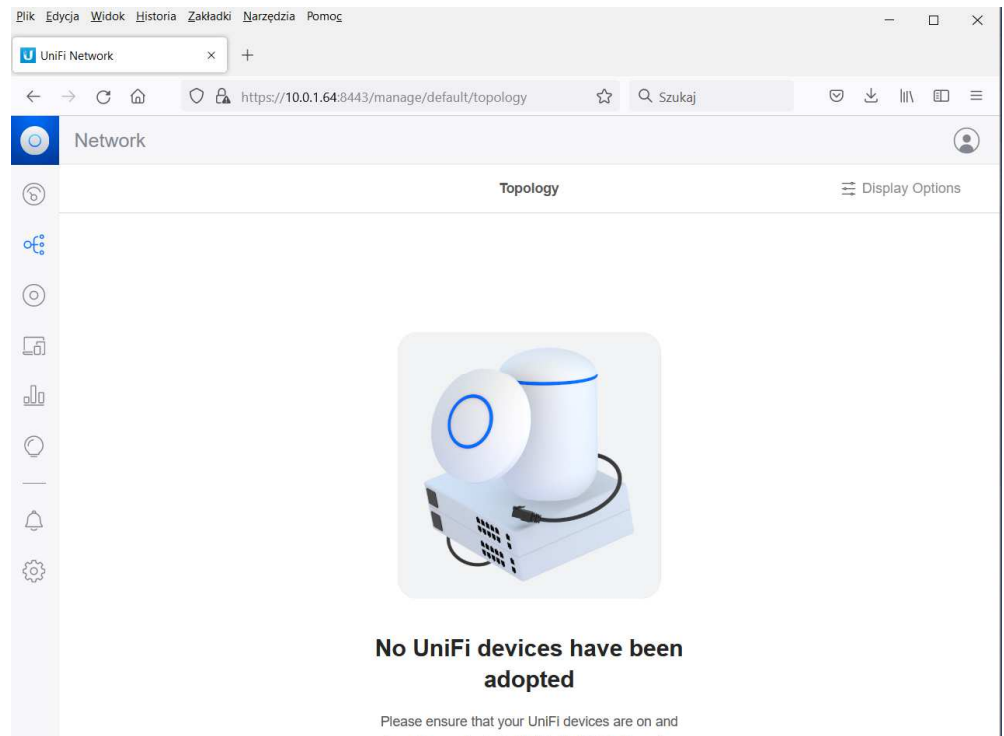
Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

■ Widok głównego panelu



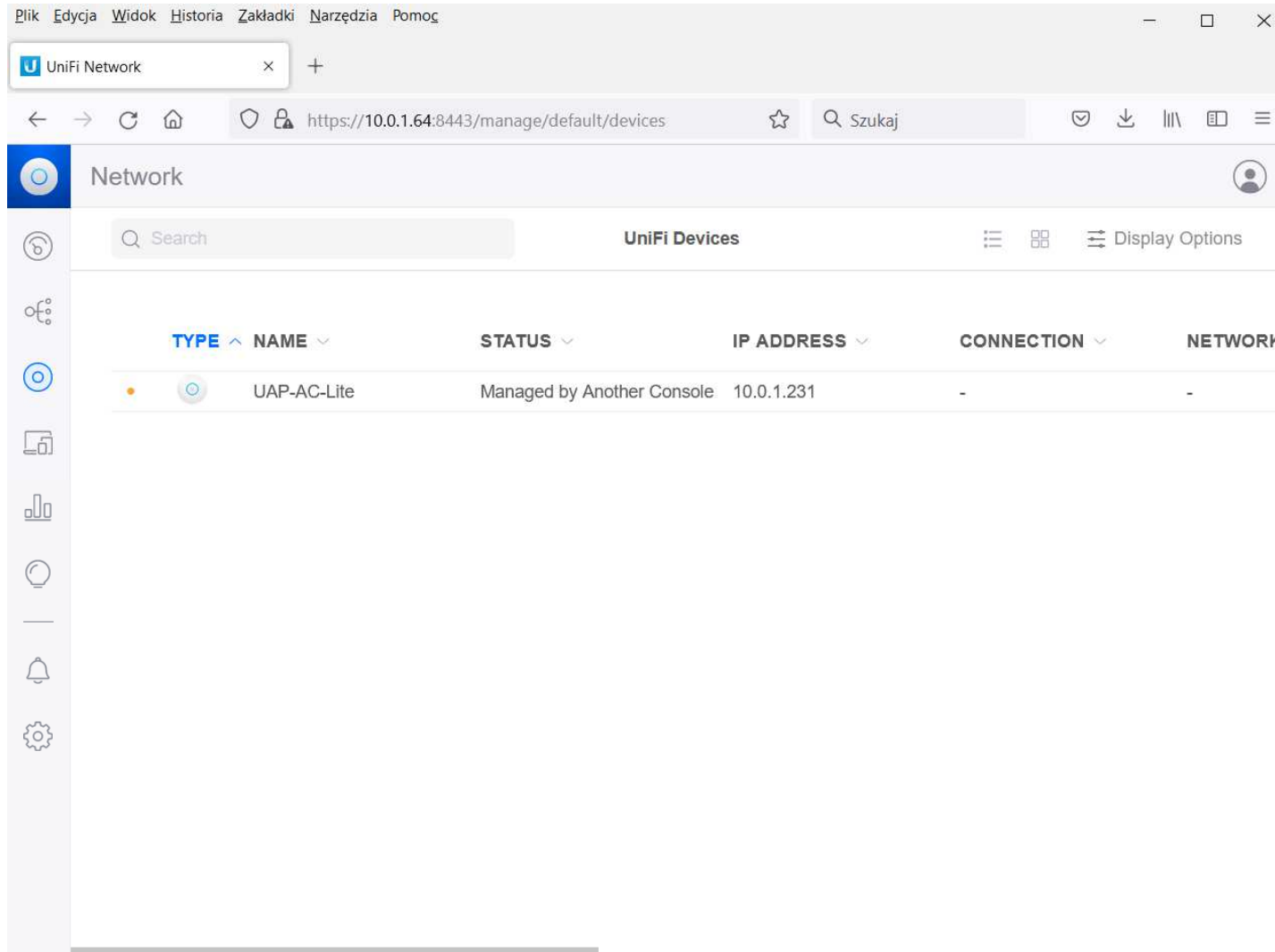
■ Topologia – jeszcze pusta



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

■ Dodajemy punkty dostępowe – metoda intuicyjna



■ Gdy brak punktów dostępowych do adopcji - możliwe jest ręczne ich dołączanie

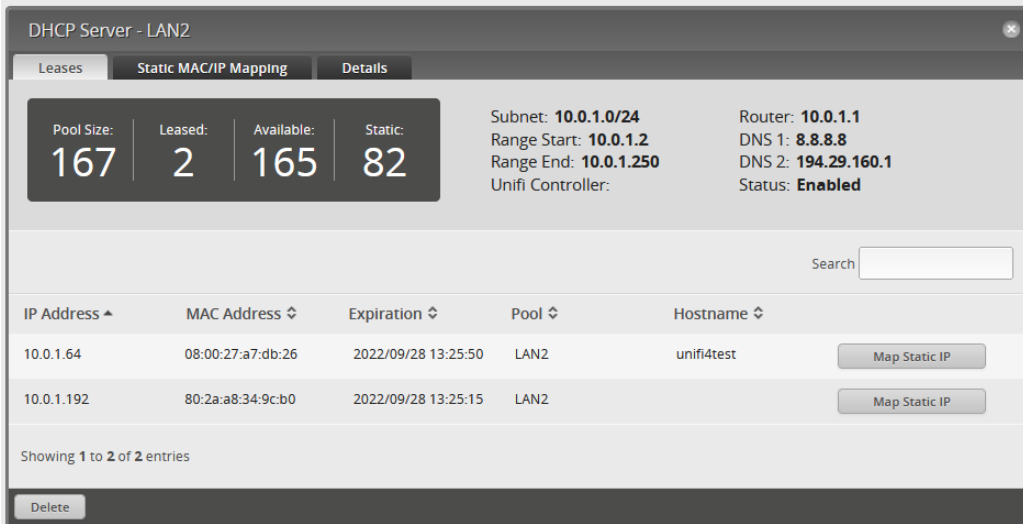
Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

■ Ręczne dołączanie punktów dostępowych

■ Szukamy punktu dostępowego w sieci (pomocny jest log serwera DHCP)

- Uwaga! Na obudowie urządzenia nie ma numeru MAC
- W laboratorium – prowadzący podaje te informacje



DHCP Server - LAN2

Leases Static MAC/IP Mapping Details

Pool Size:	Leased:	Available:	Static:
167	2	165	82

Subnet: 10.0.1.0/24
Range Start: 10.0.1.2
Range End: 10.0.1.250
Unifi Controller:

Router: 10.0.1.1
DNS 1: 8.8.8.8
DNS 2: 194.29.160.1
Status: Enabled

Search

IP Address	MAC Address	Expiration	Pool	Hostname	
10.0.1.64	08:00:27:a7:db:26	2022/09/28 13:25:50	LAN2	unifi4test	Map Static IP
10.0.1.192	80:2a:a8:34:9c:b0	2022/09/28 13:25:15	LAN2		Map Static IP

Showing 1 to 2 of 2 entries

Delete

- Znając IP punktu dostępowego – używając np.: program PuTTY logujemy się na urządzenie (login i hasło domyślne: ubnt:ubnt) a następnie wydajemy polecenie (zakładamy, że kontroler jest pod adresem 10.17.0.98):

```
set-inform http://10.17.0.98:8080/inform
```

- Proszę pamiętać iż oba urządzenia muszą być w stanie skomunikować się poprzez sieć IP
- Czasami przed tą operacją należy wykonać akuzację oprogramowania

Łączność 802.11 – aspekty praktyczne

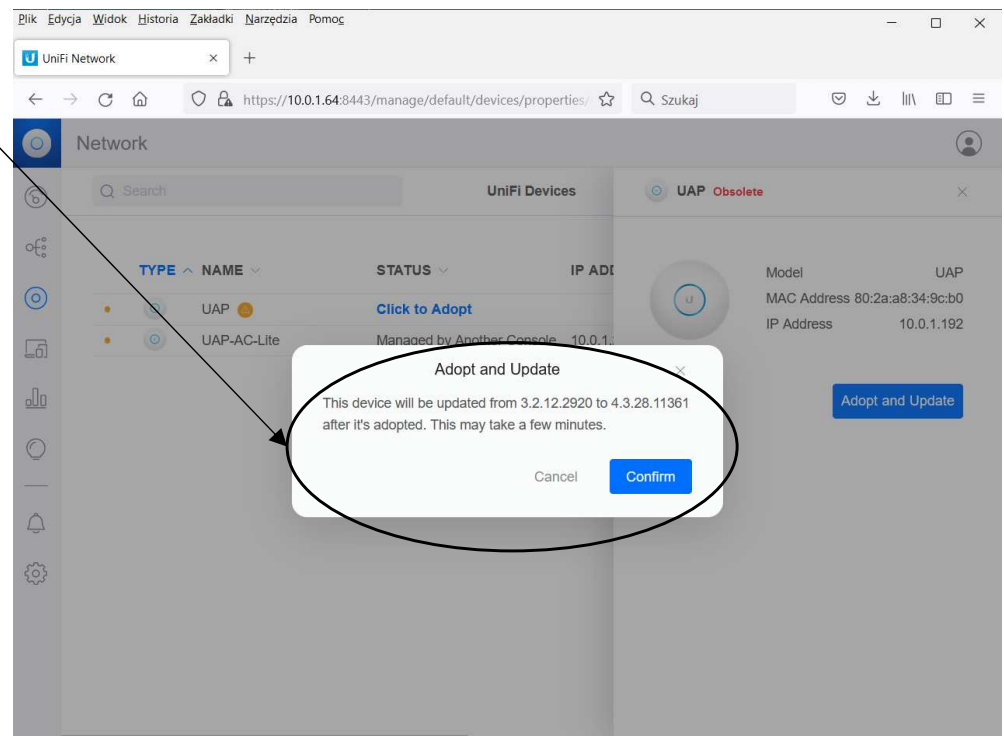
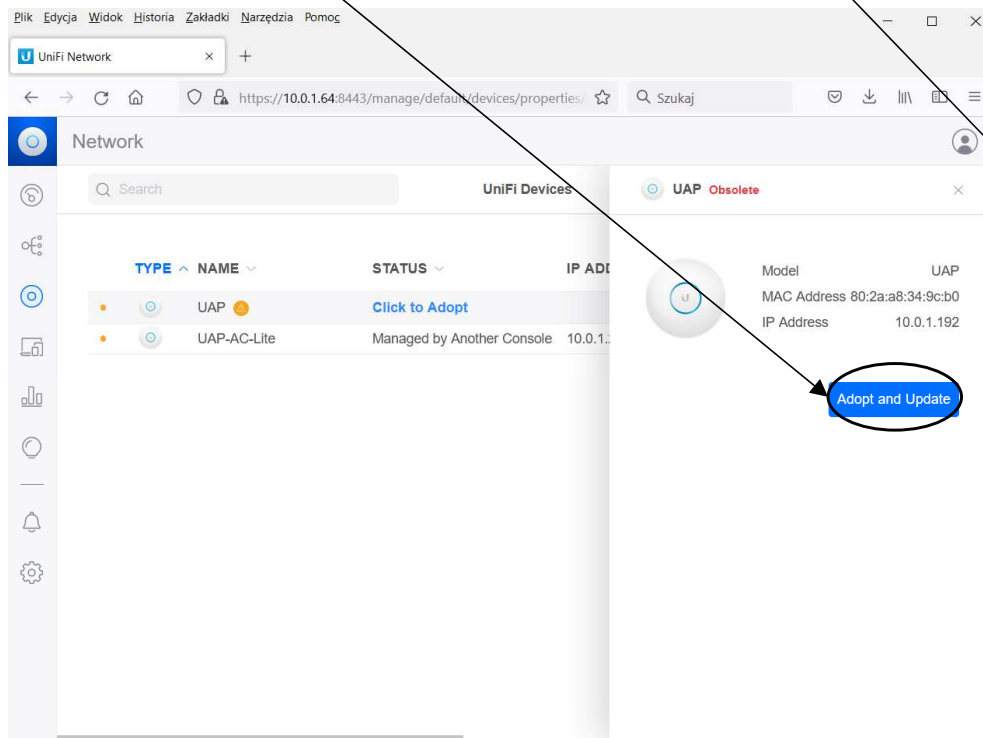
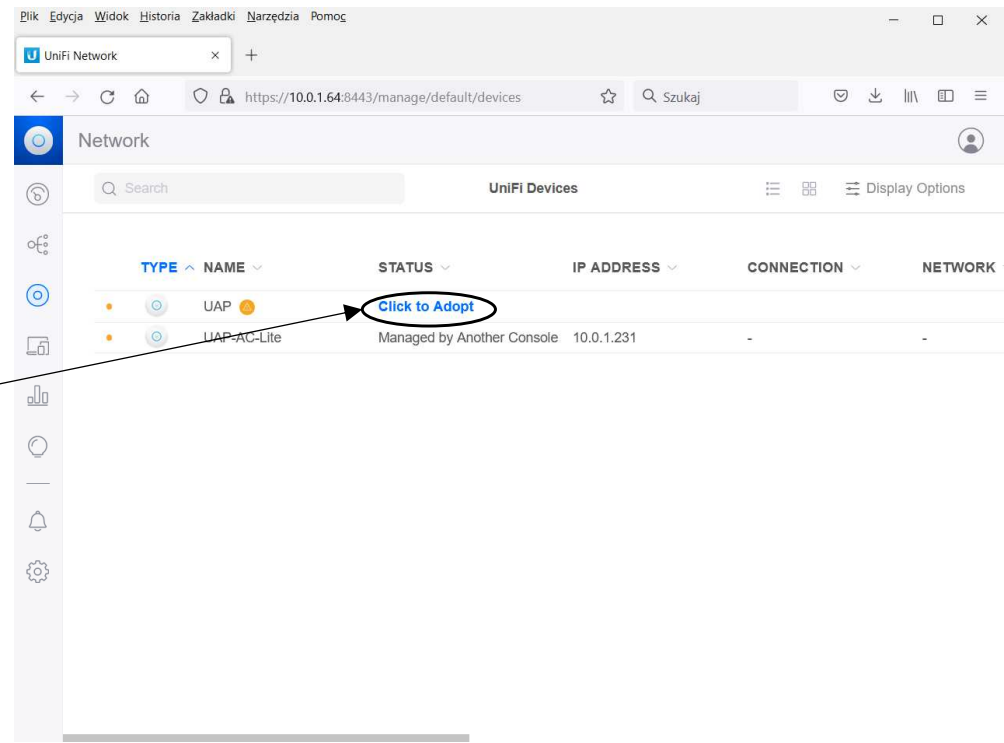
■ Kontrolery sieci Wifi, cd.

■ Dodawanie poprzez panel zarządzania

1. Wybieramy i klikamy dla dołączenia nowego punktu dostępowego do kontrolera

2. System każe nam upewnić się i zdecydować na aktualizację oprogramowania

3. System ponownie upewnia się czy aktualizacja oprogramowania jest zezwalana

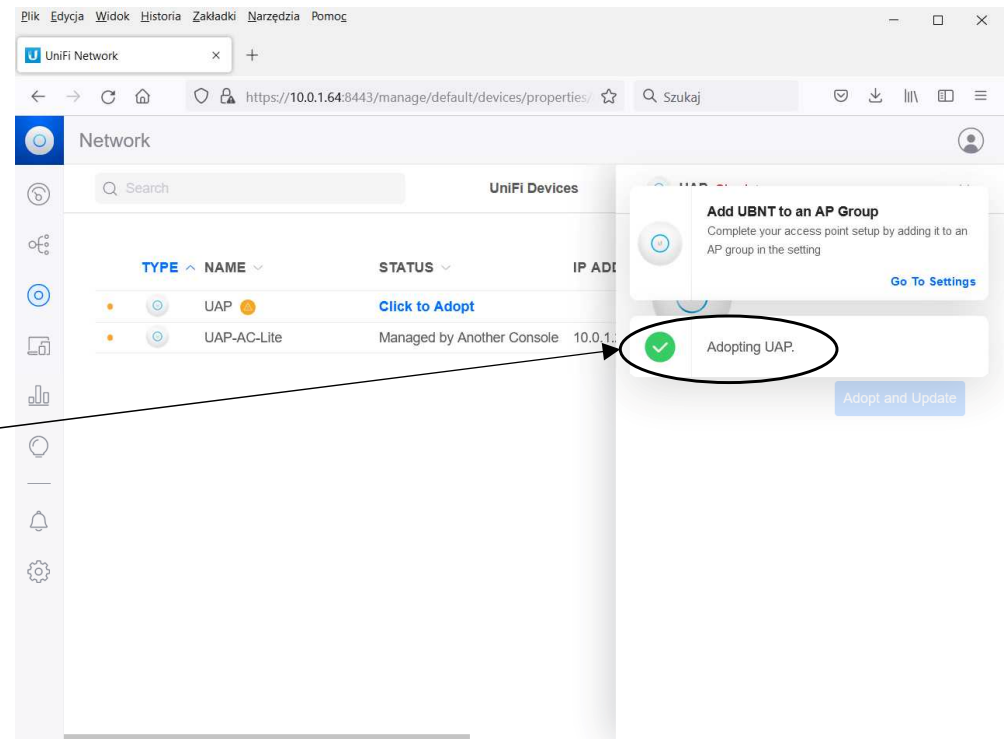


Łączność 802.11 – aspekty praktyczne

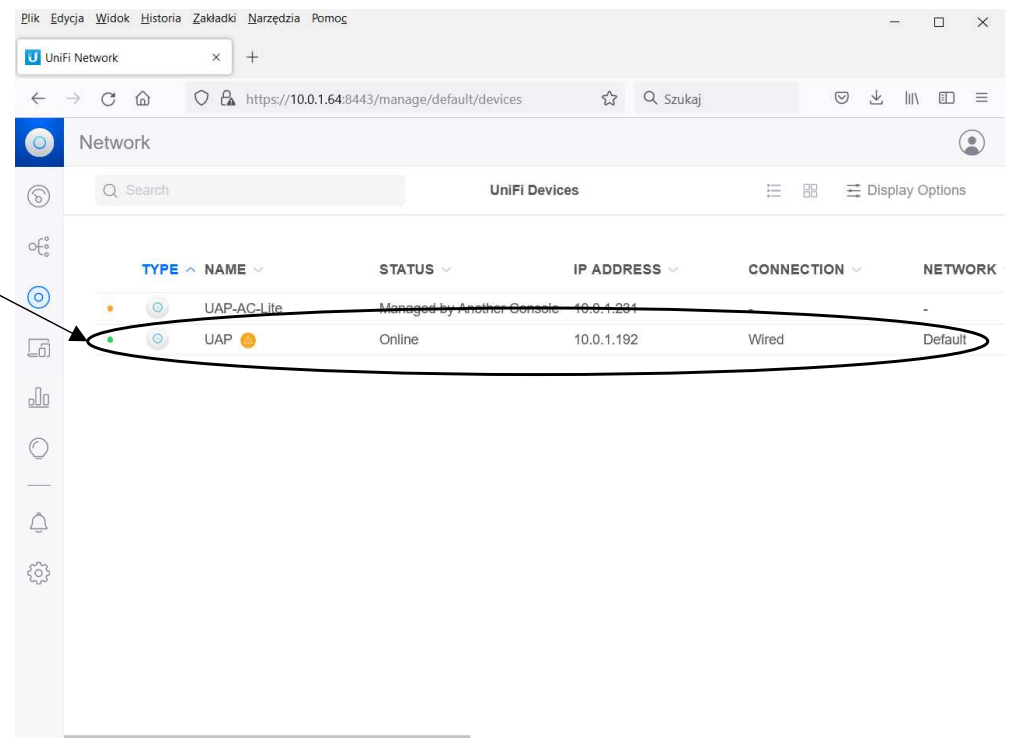
■ Kontrolery sieci Wifi, cd.

- Dodawanie poprzez panel zarządzania

Kontroler przyjął nowe urządzenie do adopcji



Kontroler zaadoptował nowe urządzenie



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

- Zarządzanie sieciami WIFI – widok po skonfigurowaniu sieci (tu podczas inicjacji)

The screenshot shows the UniFi Network management interface in a web browser. The browser's address bar displays the URL `https://10.0.1.64:8443/manage/default/settings/wifi`. The interface has a sidebar on the left with various network management options, including 'WiFi', 'Networks', 'Internet', 'VPN', 'Traffic Management', 'Firewall & Security', 'Profiles', and 'System'. The 'WiFi' option is currently selected and highlighted in blue. The main content area is titled 'WiFi' and contains a table with the following columns: 'NAME', 'NETWORK', 'AP GROUPS', 'CLIENTS (PEAK)', and 'AU'. The table lists one network named 'pbl5wifi' with a status icon, 'Default' network, 'All APs' group, and '0 (0)' clients. Below the table is a link to 'Create New WiFi Network'. Underneath the table, there are sections for 'Global AP Settings' and 'Channel Width'. The 'Channel Width' section shows two sliders: one for '2.4 GHz' (ranging from 20 MHz to 40 MHz) and one for '5 GHz' (ranging from 20 MHz to 40 MHz).

NAME	NETWORK	AP GROUPS	CLIENTS (PEAK)	AU
pbl5wifi	Default	All APs	0 (0)	Wf

[Create New WiFi Network](#)

Global AP Settings

Channel Width

2.4 GHz: 20 MHz to 40 MHz

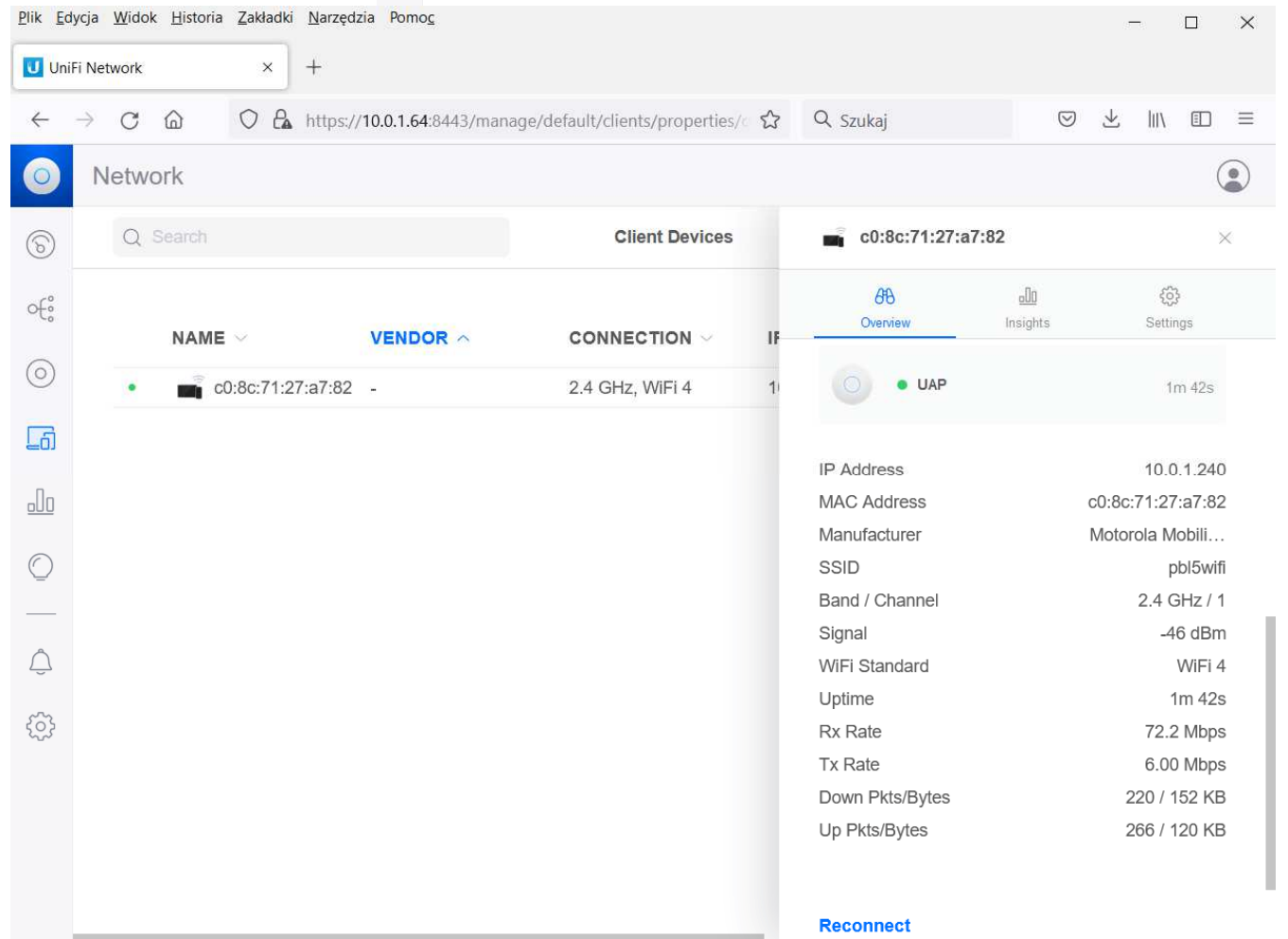
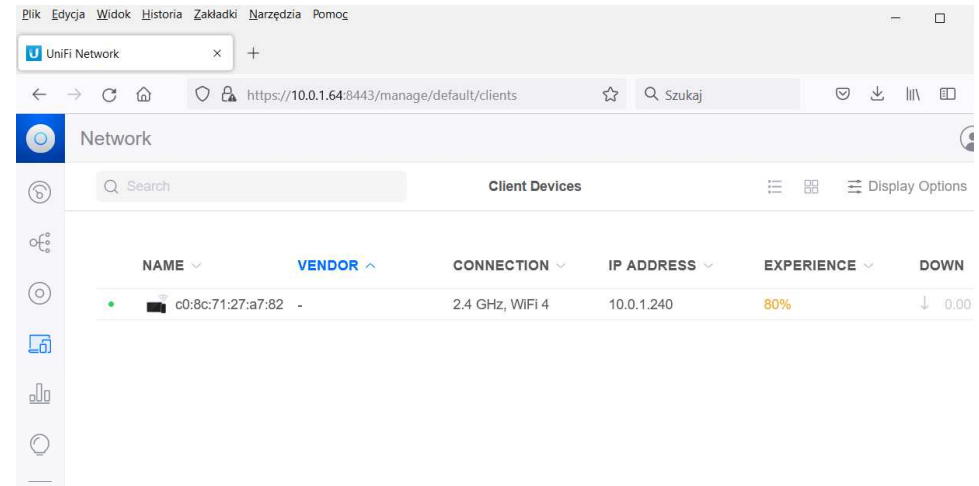
5 GHz: 20 MHz to 40 MHz

Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

- Zarządzanie sieciami WIFI – widok po dołączeniu się pierwszego klienta

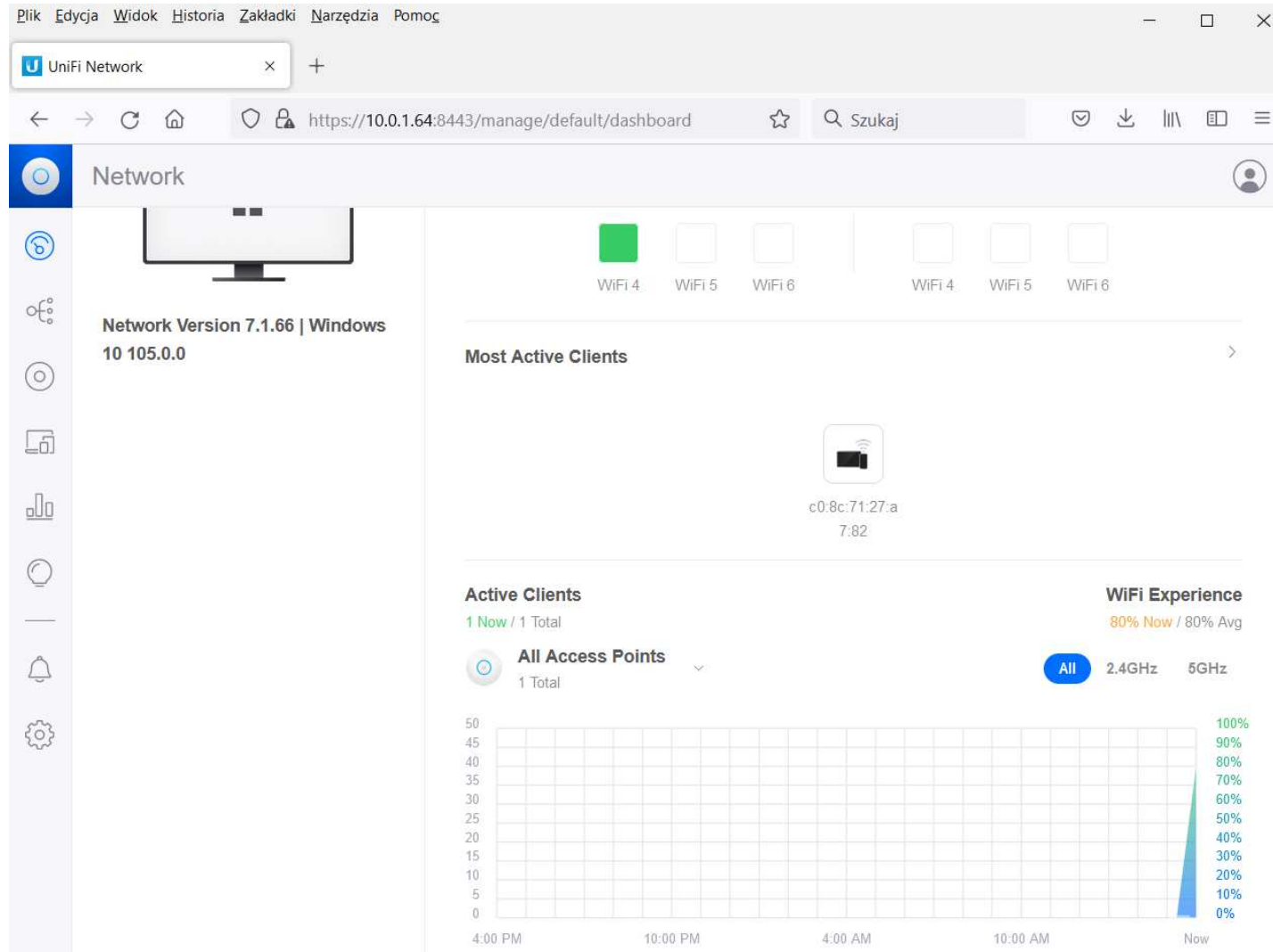
■ Detale nt. klienta



Łączność 802.11 – aspekty praktyczne

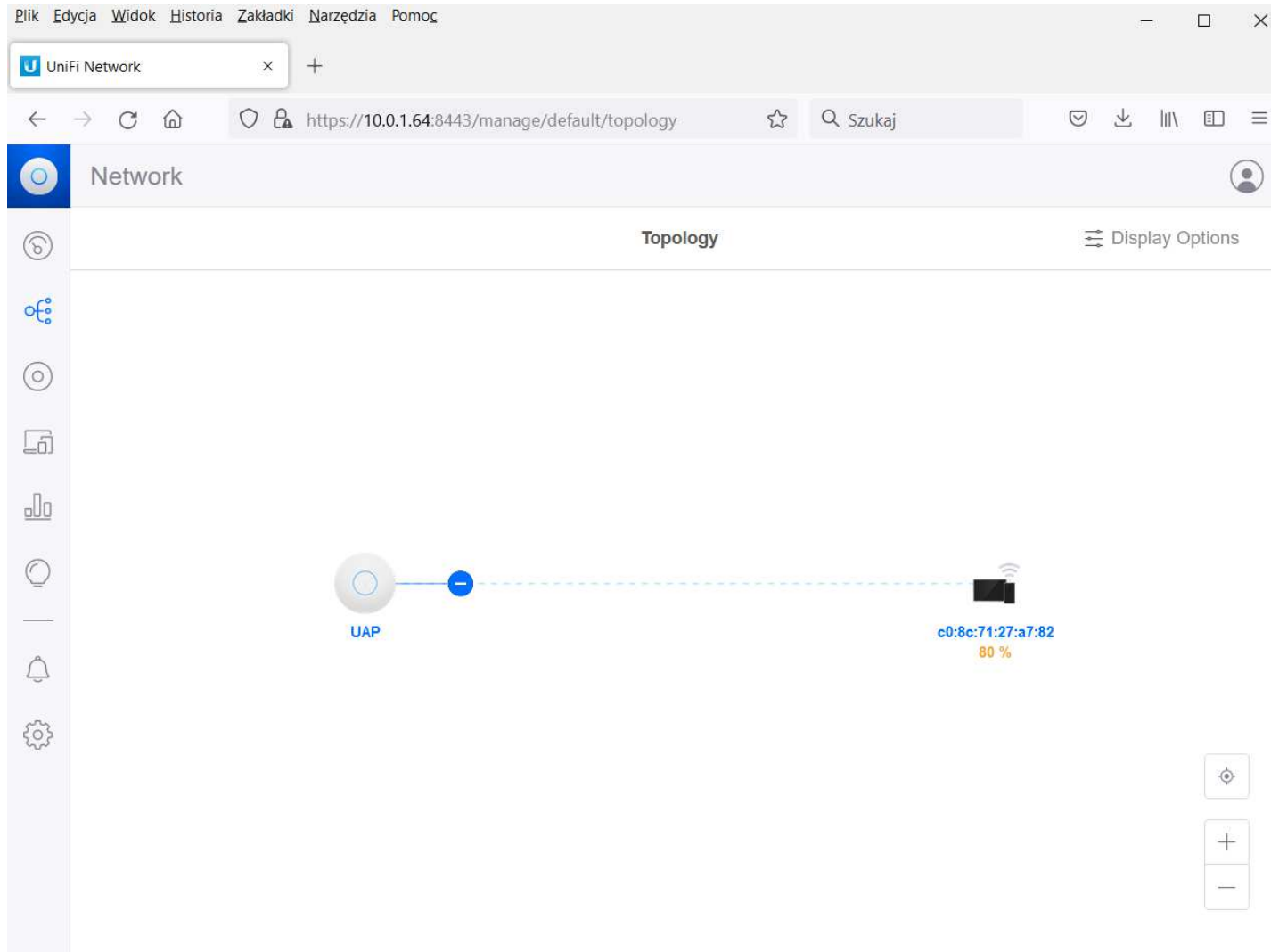
■ Kontrolery sieci Wifi, cd.

■ Zarządzanie sieciami WIFI – stan sieci, zdawkowy raport



Łączność 802.11 – aspekty praktyczne

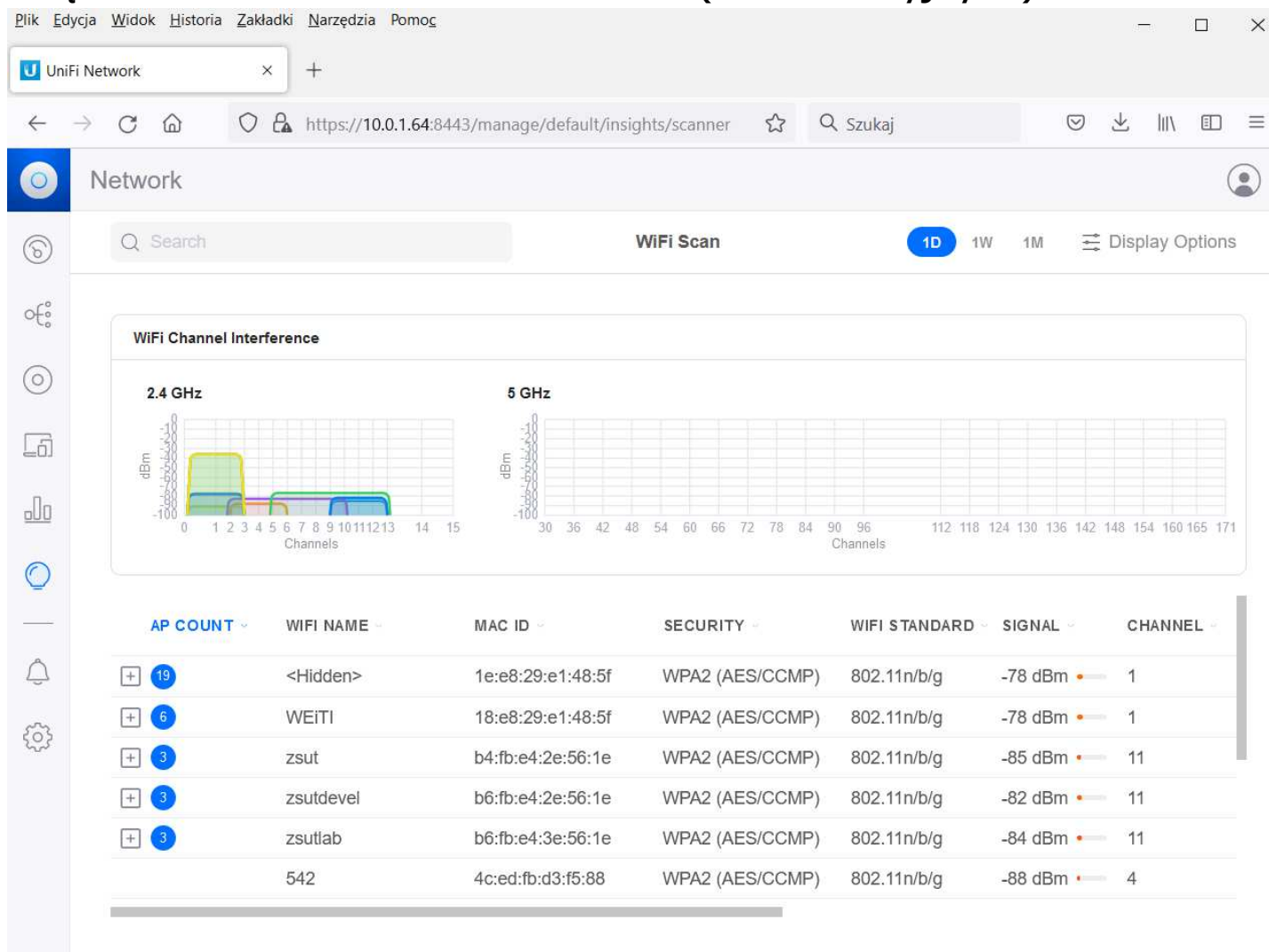
- Kontrolery sieci Wifi, cd.
 - Zarządzanie sieciami WIFI – stan topologii



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

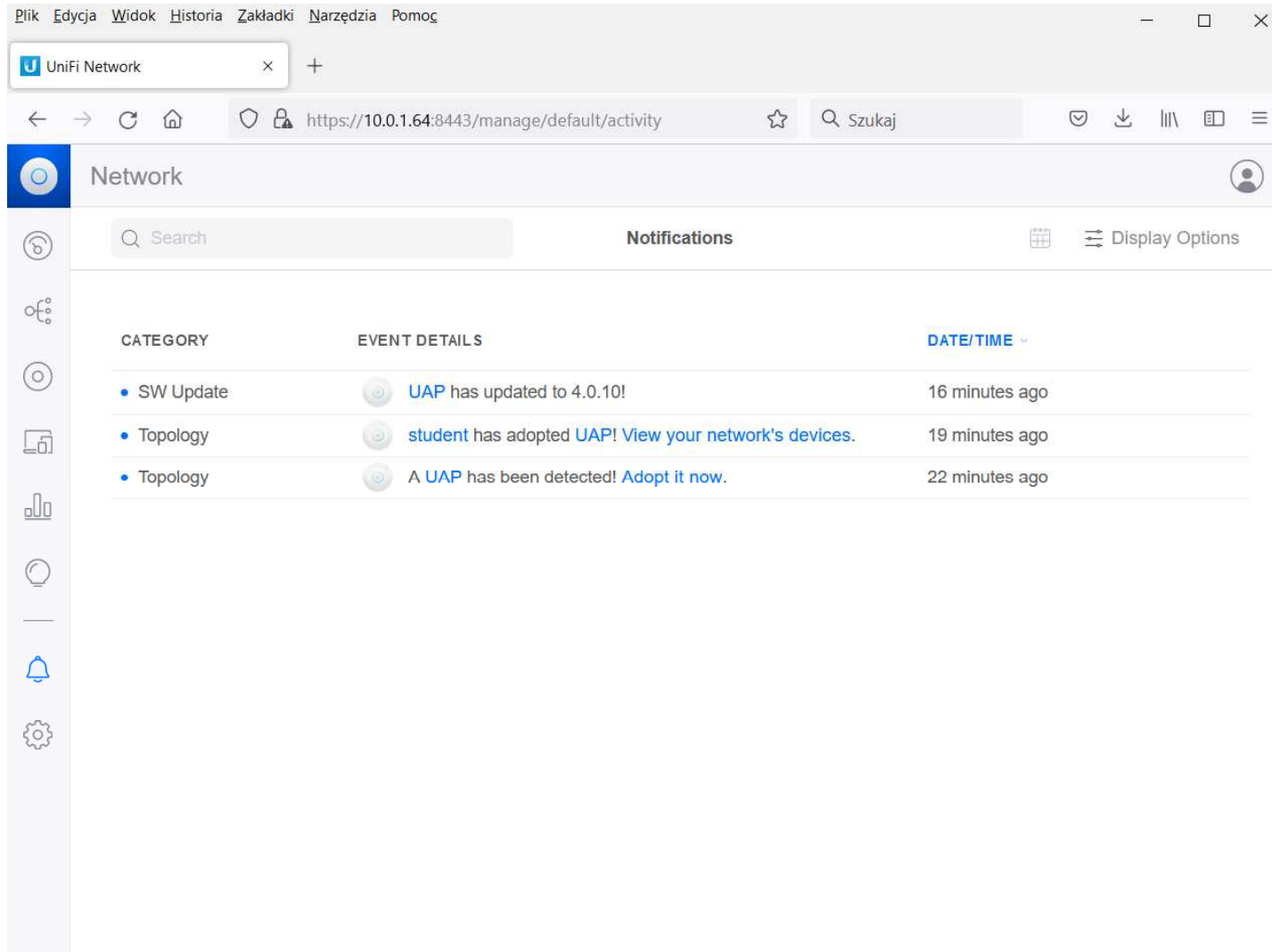
■ Zarządzanie sieciami WIFI – skan sieci (konkurencyjnych)



Łączność 802.11 – aspekty praktyczne

■ Kontrolery sieci Wifi, cd.

■ Zarządzanie sieciami WIFI – zdarzenia



The screenshot shows the UniFi Network management interface in a web browser. The browser's address bar displays the URL `https://10.0.1.64:8443/manage/default/activity`. The interface features a sidebar with navigation icons and a main content area titled "Network". The main area displays a list of events under the "Activity" tab. The events are organized into three columns: CATEGORY, EVENT DETAILS, and DATE/TIME.

CATEGORY	EVENT DETAILS	DATE/TIME
• SW Update	UAP has updated to 4.0.10!	16 minutes ago
• Topology	student has adopted UAP! View your network's devices.	19 minutes ago
• Topology	A UAP has been detected! Adopt it now.	22 minutes ago

Zadanie:

Utworzyć system z jednym punktem dostępowym a następnie podłączyć do niego laptop (zapamiętaj konfigurację i opisz kolejne kroki)

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego

- Stosowany jest system Linux/Debian
- Wspierane funkcje: obsługa sieci Wifi, przydzielanie numerów IP, routing pakietów
- Instalacja wymaganych pakietów (tutaj prawa root'a zapewnia sudo)

```
sudo apt-get update
```

```
sudo apt-get install hostapd dnsmasq wireless-tools
```

- W szczególnych przypadkach wymagane może być zainstalowanie tzw. firmware
 - Zamknięte obrazy ładowane do określonego urządzenia (tu karty sieciowej), utworzone przez producenta, wspierające działanie tego urządzenia (może zawierać kod obsługi realizowany przez kontroler wbudowany w to urządzenie)
 - Firmware jako takie uznawane są wyłom w otwartości systemu Linux – wynika z polityk firm produkujących te urządzenia, które nie chcą ujawniać szczegółów budowy ich produktów

```
sudo apt-get install firmware-realtek ...
```

- zgodnie z posiadanym sprzętem (wymagana analiza treści zwracanej przez polecenie dmesg)
- Proszę pamiętać(!) że w jądrze systemu muszą być uwaktywnione między innymi: wsparcie dla Wifi, wsparcie routowania pakietów, ...

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

- Utworzenie wpisu dla urządzenia sieciowego Wifi i Ethernet (tzw. forwarding)
- Dodajemy wpisy w **/etc/network/interfaces**

```
allow-hotplug eth0  
iface eth0 inet dhcp
```

← Ustawienia karty Ethernet – klient dhcp (dla rozważań o Wifi nie jest istotne, nowe systemy nie potrzebują tego wpisu)

```
allow-hotplug wlan0  
iface wlan0 inet static  
    address 10.0.100.1  
    netmask 255.255.255.0  
    broadcast 255.255.255.255  
    network 10.0.100.0
```

← Ustawienia karty Wifi – IP nadane statycznie (typowe dla punktów dostępowych)

UWAGA!!! W nowszych dystrybucjach (Debian/Ubuntu/Raspbian) zamiast DHCPD instalowany jest pakiet DHCLIENT lub NetworkManager – co zmienia sposób konfigurowania sieci

- Po tym zmianach można wykonać restart urządzenia
 - Podejście z restartem serwisów sieciowych – na ogół zawodzi

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

- Serwer DHCP – tutaj będzie nim **DNSMasq**[1]
 - Narzędzie to jest także serwerem DNS dla sieci lokalnych, stąd jego nazwa
 - Dopisujemy - sprawdzając czy nie ma z obecnymi wpisami sprzeczności – na końcu pliku **/etc/dnsmasq.conf**:

```
interface=wlan0
```

```
bind-interfaces
```

```
domain=test100.com
```

Jaki interfejs będzie związany z DNSMasq

Zlecenie DNSMasq by nie obsługiwał innych interfejsów – tutaj działanie na eth0 mogło by spowodować problemy w sieci Ethernet gdyby w niej pracował inny serwer DHCP

Jaką domenę chcemy obsługiwać w sieci Wifi

```
dhcp-option=3,10.0.100.1
```

```
dhcp-option=6,8.8.8.8
```

```
dhcp-option=15,test100.com
```

Opcje protokołu DHCP (domyślny Gateway – opcja 3, domyślny serwer DNS – opcja 6, domyślna domena, ustawiana klientom – opcja 15)

```
dhcp-range=wlan0,10.0.100.100,10.0.100.199,15m
```

Ustalenie zakresu przydzielanych numerów IP (100 numerów) oraz czasu dzierżawy (15m). Słowo *wlan0* w definicji **dhcp-range** jest nadmiarowe, ale przydatne gdy DNSMasq równocześnie obsługuje wiele interfejsów sieciowych (np.: *wlan0* i *wlan1*)

[1] <https://thekelleys.org.uk/dnsmasq/doc.html>

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

- Po zmianach w pliku **/etc/dnsmasq.conf** konieczne jest ponowne uruchomienie serwisu np.:

```
sudo systemctl restart dnsmasq
```

lub „po staremu”

```
sudo /etc/init.d/dnsmasq stop
```

```
sudo /etc/init.d/dnsmasq start
```

- Błędy i logi można obserwować w pliku: **/var/log/syslog**
 - Najlepiej użyć polecenia **tail -f /var/log/syslog** uruchomione w innej konsoli niż polecenia zacytowane powyżej
- Uwaga jeżeli interfejs wlan0 nie jest jeszcze „podniesiony” – uruchomienie DNSMasq zakończy się nie powodzeniem
 - Można „recznie” podnieść ten interfejs i uruchomić DNSMasq ponownie, albo ponownie zrestartować węzeł

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

■ Konfiguracja punktu dostępowego Wifi bazującego na **HostAPD** [1]

- Jest on odpowiedzialny m.in. za uwierzytelnienie klientów

■ Tworzymy plik **/etc/hostapd/hostapd.conf**

`interface=wlan0`

jaki interfejs Wifi hostapd ma obsługiwać

`ssid=wlan100`

SSID tej sieci

`driver=nl80211`

sterownik „działający nad” kartą sieciową (czyli nad wspólnym API kart sieciowych)

`country_code=PL`

ustalenie pasma radiowego zgodnie z lokalizacją

`hw_mode=g`

Standard: a-IEEE 802.11a, b-IEEE 802.11b, g-IEEE 802.11g, ...

`channel=7`

Numer kanału radiowego

`max_num_sta=5`

wielkość tablicy obsługiwanych klientów, definiuje ilu obsłużymy

`wpa=2`

bit nr. 2 tego pola wskazuje użycie: IEEE 802.11i/RSN (WPA2)

`auth_algs=1`

Alg. uwierzytelnienia (tu: Shared Key Authentication)

`rsn_pairwise=CCMP`

typ algorytmu szyfrowania

`wpa_key_mgmt=WPA-PSK`

lista wspieranych algorytmów zarządzania, tu:

WPA-PSK = WPA-Personal / WPA2-Personal

`wpa_passphrase=wlan100pb15`

ustanowienie hasła dla tworzonej sieci (Personal)

[1] <http://w1.fi/hostapd/>

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

■ Uruchomienie testowe HostAPD

```
sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf
```

- Obserwując komunikaty generowane przez HostAPD można próbować usuwać błędy konfiguracji

■ Jeżeli działa poprawnie (klienci mogą się połączyć) – należy uaktywnić domyślny serwis systemu Debian (lub podobnego):

- Wpisujemy do pliku **/etc/default/hostapd** linię

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

- Poprzez:

```
sudo systemctl start hostapd
```

Czasami przed tym trzeba wykonać polecenie:

```
sudo systemctl unmask hostpad
```

- Na tym etapie nie będziemy mieli pożytku z takiej sieci – brak routowania pakietów IP między sieciami
- W przypadku problemów z uruchomieniem HostAPD warto wykonać polecenie

```
sudo rfkill unblock wlan
```

- W przypadku Raspberry PI niezbędne jest ustawienia lokalizacji - czyli w jakim państwie używamy WIFI (raspi-config)

Łączność 802.11 – tworzenie sieci

■ Tworzenie punktu dostępowego, cd.

- Uaktywnienie routowania pakietów między sieciami tutaj: **eth0** i **wlan0**
 - reguły routowania zależą od preferencji administratora sieci(!)
- Przykład popularnej konfiguracji
 - Z sieci **wlan0** można łączyć się z Internetem przez **eth0**, ruch w drugą stronę dozwolony gdy jest to ruch tzw.: skojarzony (poniższe kroki wymagają praw root'a):

1) uaktywnienie przekazywania pakietów (podstawa)

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2) Pakiety skojarzone przepuszczamy z eth0 na wlan0

```
iptables -A FORWARD -i eth0 -o wlan0 -m state \  
--state ESTABLISHED,RELATED -j ACCEPT
```

← Uwaga to jedna linia

3) Wypuszczamy pakiety z sieci wlan0 poprzez interfejs eth0

```
iptables -A FORWARD -s 10.0.100.0/24 -o eth0 -j ACCEPT
```

4) stworzymy Maskarade - translacja adresów w pakietach tworząc tzw. NAT

```
iptables -t nat -A POSTROUTING -s 10.0.100.0/24 -o eth0 -j MASQUERADE
```

- Uwaga tak ustawiona konfiguracja wspiera routowanie pakietów aż do restartu systemu(!)

Łączność 802.11 – tworzenie sieci

■ Konfiguracja komputerów klienckich

■ Podejście z wykorzystaniem pakietu wpa_supplicant

■ Instalacja wymaganych pakietów (jako root)

```
sudo apt-get update
```

```
sudo apt-get install wpa_supplicant
```

...

Np.: firmware-realtek

■ Ustawienie konfiguracji w: /etc/wpa_supplicant/wpa_supplicant.conf

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
```

```
update_config=1
```

Pozwolenie by inne programy (wpa_cli) mogły swoje zmiany zapisywać w tym pliku

Definicja gdzie jest punkt (DIR) sterowania i prawa (GROUP) dostępu, gdy inne programy chcą sterować Wifi (np.: wpa_cli)

```
country=PL
```

Pasmo radiowe używane przez Wifi (w Raspberry PI ustala się to za pomocą raspi-config)

```
network={
    ssid="wlan100"
    psk="wlan100pb15"
}
```

Sekcja opisująca do jakich sieci chcielibyśmy się dołączać (tu jedna: wlan100).

Sekcja może zawierać wiele zdefiniowanych sieci – automatycznie wybrana będzie ta która będzie w zasięgu lub będzie miała większą moc. Słowo 'priority' pozwala zarządzać którą chcemy wybrać – większa wartość to większy priorytet.

- Uwaga! Plik ten powinien być tajny – jego wyciek to naruszenie zasad bezpieczeństwa, wymagająca zmiany hasła przez wszystkich klientów

Łączność 802.11 – tworzenie sieci

■ Konfiguracja komputerów klienckich

- Podejście z wykorzystaniem pakietu wpa_supplicant, cd.
 - Pole 'psk' powinno być tworzone programem wpa_passphrase które tworzy tzw. HASH z hasła
 - Nie jest to zabezpieczenie przez użyciem tych danych a jedynie utrudnienie odczytania jawnego hasła do sieci wifi

```
wpa_passphrase wlan100 wlan100pb15
```

- Wynik działania tego programu trzeba skopiować do pliku wpa_supplicant.conf
 - Pola otoczone znakami " są traktowane jak ciąg tekstowy
 - Pole 'psk' z treścią w wersji wygenerowanej przez wpa_passphrase wpisujemy bez otaczających znaków "
- Proces łącznia można testować ręcznie (bez przenoszenia procesu w „tło”) wskazując kartę i konfigurację (przydatne gdy coś nie chce działać):

```
sudo wpa_supplicant -Dwext,nl80211 -i wlan0 -c wpa_supplicant.conf
```

- Gdyby nie udało się karcie wlan0 pobrać numeru IP proszę spróbować wywołać następujące polecenia

```
sudo wpa_supplicant ... wpa_supplicant.conf &
```

```
sudo dhclient -v wlan0
```

To polecenie pozwala pobrać numer IP wraz z podglądem na ten proces

To przenosi wpa_supplicant'a w „tło” i zwracając dostęp do shell'a pozwala uruchomić następne polecenie

Zadanie:

Na platformie Raspberry PI utworzyć punkt dostępowy (przetestować go Laptopem)

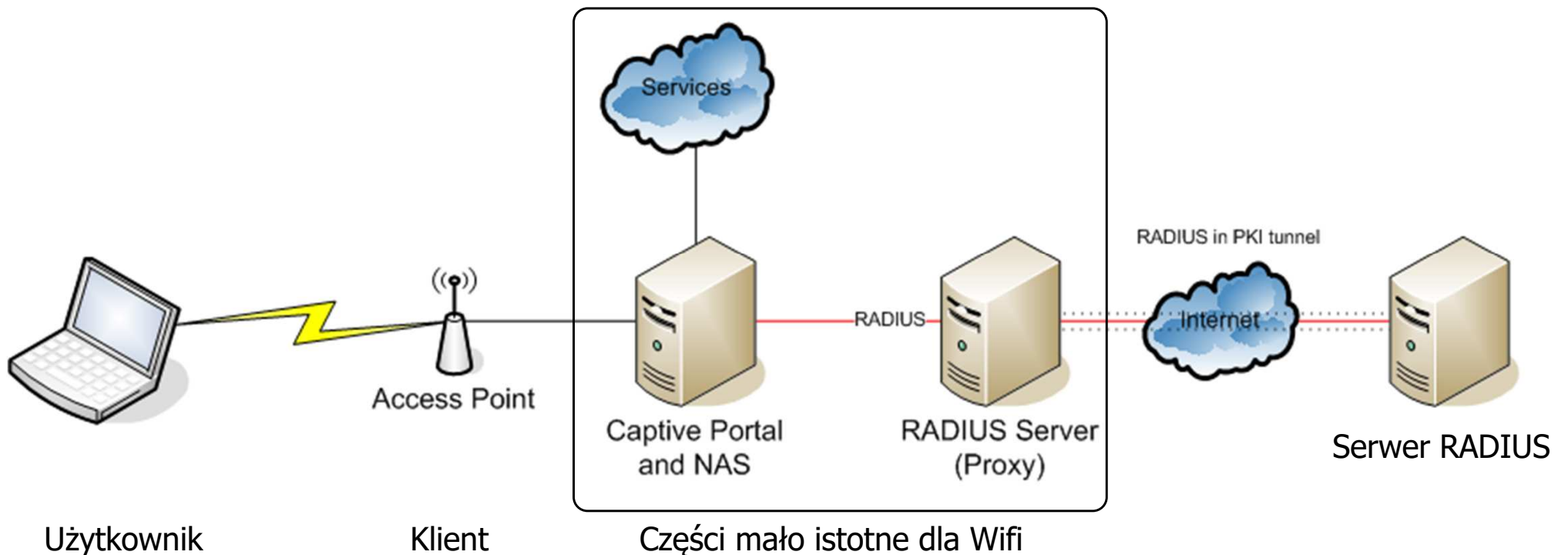
Dla chętnych (ekstra punkty): sprawić aby ustawienia były permanentne – konieczność uaktywnienia Systemd dla Dnsmasq, Hostapd i ustawienia trwałych zasad routingu (wymagana lektura dokumentacji systemu Debian i pochodnych)

Łączność 802.11 – Zaawansowane mechanizmy autentykacji

Łączność 802.11 – aspekty praktyczne

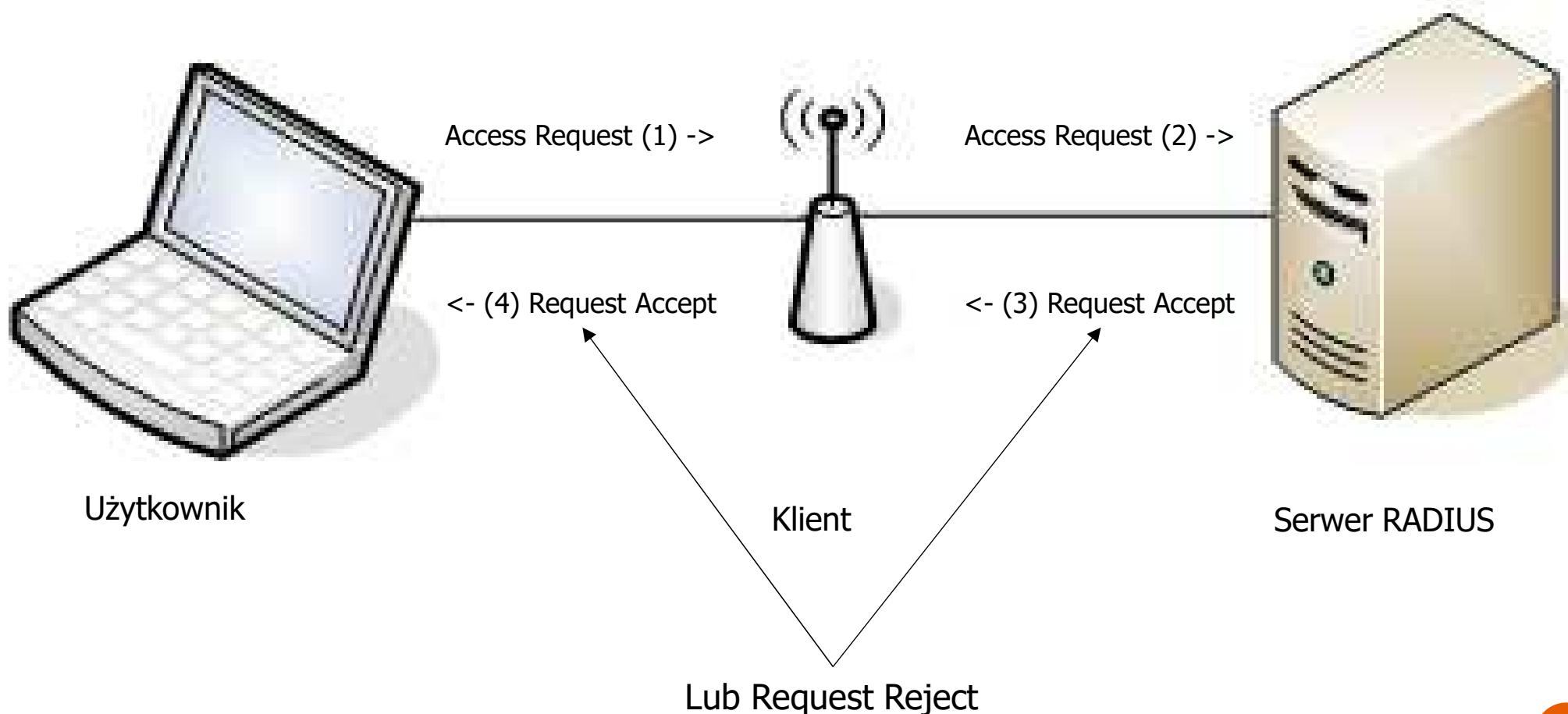
■ WPA2-Enterprise wprowadzenie

- Co to jest
 - Serwer
 - Klient - punkt dostępowy
 - Użytkownik - podmiot dołączający się do sieci
- Architektura



Łączność 802.11 – aspekty praktyczne

- WPA2-Enterprise wprowadzenie, cd.
 - Działanie – przepływ informacji



■ WPA2-Enterprise wprowadzenie, cd.

- Dostępne metody uwierzytelnienia EAP i ich warianty

EAP-TLS

EAP-PEAP/MSCHAPv2 (PEAPv0 i PEAPv1)

EAP-PEAP/TLS (PEAPv0 i PEAPv1)

EAP-PEAP/GTC (PEAPv0 i PEAPv1)

EAP-PEAP/OTP (PEAPv0 i PEAPv1)

EAP-PEAP/MD5-Challenge (PEAPv0 i PEAPv1)

EAP-TTLS/EAP-MD5-Challenge

EAP-TTLS/EAP-GTC

EAP-TTLS/EAP-OTP

EAP-TTLS/EAP-MSCHAPv2

EAP-TTLS/EAP-TLS

EAP-TTLS/MSCHAP

EAP-TTLS/PAP

EAP-TTLS/CHAP

EAP-SIM

EAP-AKA

EAP-PSK

EAP-PAX

LEAP

EAP-MD5-Challenge

EAP-MSCHAPv2

EAP-GTC

EAP-OTP

...

Łączność 802.11 – aspekty praktyczne

■ WPA2-Enterprise wprowadzenie, cd.

- Z pośród najbardziej znanych metod uwierzytelnienia stosowane są EAP-TLS, EAP-TTLS i PEAP
 - W warunkach praktycznych musimy wybrać tzw. „wspólny mianownik” spośród metod – tak aby był on wspieranych przez wszystkich użytkowników sieci Wifi
 - EAP-TTLS i PEAP – sprawdzanie certyfikatów klienckich nie jest obowiązkowe
 - PEAP – jest jedynym wspieranym przez system Windows
 - EAP-TLS – wymaga weryfikacji certyfikatów zarówno serwera jak i użytkownika (Mutual Authentication)
 - Co daje najsilniejsze zabezpieczenie
 - Metoda nie wspierana przez komputery z systemem Windows
- Zestawianie połączenia
 - EAP-TLS – jedna faza podczas której wymieniane są klucze publiczne i z ich użyciem tworzony jest tunel TLS
 - EAP-TTLS i PEAP – dwie fazy, w każdej stosowana może być inna tożsamość użytkownika
 - Faza zewnętrzna – widnieje w pakietach sieciowych (podobnie EAP-TLS przesyła tożsamość jawnie), stąd stosuje się tu tożsamość anonimową
 - Faza wewnętrzna – tu przesyłana jest tożsamość właściwa, a transfer może być przesyłany jawnym tekstem bo całość w tej fazie jest już szyfrowana

Łączność 802.11 – aspekty praktyczne

■ WPA2-Enterprise konfiguracja - punkt dostępowy

■ Konfiguracja uproszczona

- Punkt dostępowy i serwer radius na tym samym komputerze, dane uwierzytelniające dla użytkowników na tej samej maszynie
- Instalacja wymaganych pakietów (ponownie jako root)

```
sudo apt-get update
```

```
sudo apt-get install freeradius ...
```

■ Test czy radius działa po instalacji

```
sudo netstat -anulp | grep radius
```

udp	0	0	0.0.0.0:1812	0.0.0.0:*	8430/freeradius
udp	0	0	0.0.0.0:1813	0.0.0.0:*	8430/freeradius

Komunikacja procesów uwierzytelnienia

Komunikacja procesów naliczania

- Ustalenie loginu i hasła użytkownika – przechowywane dla uproszczenia w pliku **/etc/freeradius/3.0/users** o przykładowej treści

```
wlanwpa Cleartext-Password := „pbl5wpa2enterprise”
```

- Uwaga ten plik powinien być utajniony – rozwiązanie tu przytaczane to stan gdzie punkt dostępowy serwer radius pracują na jednej maszynie oraz dane uwierzytelniające są składowane na tej samej maszynie, taki przykład można uznać wyłącznie za przykład edukacyjny!

Łączność 802.11 – aspekty praktyczne

■ WPA2-Enterprise konfiguracja - punkt dostępowy, cd.

- Ustalenie jakiem klientom wolno łączyć się z serwerem Radius - ustala plik **/etc/freeradius/3.0/clients.conf** o przykładowej dopisanej treści:

```
client 10.0.100.0/24 {  
    ipaddr = 127.0.0.1  
    secret = testing1234  
    shorname = siec_10_0_100_0  
}
```

Identyfikacja wpisu (może być ich wiele, np.: po jednym dla każdego punktu dostępowego)

Z jakiego adresu zapytanie klienta zostanie przyjęte

Poufne hasło jakie zastosuje klient (nie użytkownik) by się uwierzytelnić

Krótki alias, o użycia zamiast adresu IP lub FQDN

- Po wszelkich zmianach - restartujemy serwer

```
sudo /etc/init.d/freeradius stop  
sudo /etc/init.d/freeradius start
```

Łączność 802.11 – aspekty praktyczne

■ WPA2-Enterprise konfiguracja - punkt dostępowy, cd.

- Testowanie - aby mieć pewność że serwer Radius działa poprawnie

- Zadajemy pytanie wywołując narzędzie `radtest`

```
radtest wlanwpa pbl5wpa2enterprise localhost 1812 testing1234
```

Dane uwierzytelniające użytkownika

Dane uwierzytelniające klienta (punktu dostępowego)

- Otrzymujemy wynik:

```
Sent Access-Request Id 245 from 0.0.0.0:36210 to 127.0.0.1:1812 length 78
```

```
User-Name = "wlanwpa"
```

```
User-Password = „pbl5wpa2enterprise"
```

```
NAS-IP-Address = 127.0.1.1
```

```
NAS-Port = 1812
```

Network Access Server (NAS) –
tutaj punkt dostępowy

```
Message-Authenticator = 0x00
```

```
Cleartext-Password = "testing1234"
```

```
Received Access-Accept Id 245 from 127.0.0.1:1812 to 127.0.0.1:36210 ...
```

- Więcej informacji diagnostycznych jest w pliku `/var/log/freeradius/radius.log`

Łączność 802.11 – tworzenie sieci

- WPA2-Enterprise konfiguracja - punkt dostępowy, cd.
 - Plik **/etc/hostapd/hostapd.conf** (najważniejsze różnice względem WPA2-personal)

```
interface=wlan0          #jaki interfejs Wifi hostapd ma obsługiwać
ssid=wlan100
driver=nl80211
country_code=PL
hw_mode=g
channel=7
max_num_sta=5
ieee8021x=1             #uwierzytelnienie zgodne z IEEE 802.1X
wpa=3                  #WPA i WPA2
wpa_key_mgmt=WPA-EAP   #usatlenie akceptowalnych algorytmów zarządzanie kluczem
rsn_pairwise=CCMP
auth_algs=1
#Dane dla połączenia punktu dostępowego z serwerem Radius
auth_server_addr=127.0.0.1   #adres
auth_server_port=1812       #port
auth_server_shared_secret=testing1234 #uwierzytelnienie klienta
```

Łączność 802.11 – tworzenie sieci

■ WPA2-Enterprise konfiguracja - komputerów klienckich

- Ustawienie konfiguracji w: /etc/wpa_supplicant/wpa_supplicant.conf

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
```

```
update_config=1
```

```
country=PL
```

```
network={
```

```
    ssid="wlan100"
```

```
    key_mgmt=WPA-EAP      #wybieramy metodę uwierzytelnienia
```

```
    eap=PEAP              #
```

```
    identity="wlanwpa"
```

```
    password="pb15wpa2enterprise"
```

```
    phase2="auth=MSCHAPV2"
```

```
}
```

- W systemie Windows – usatwień dokonuje się za pomocą menu wyboru sieci WIFI

Zadanie:

Utworzyć punkt dostępowy na platformie Raspberry PI z WPA2-Enterprise

Łączność 802.11 – ESP32

Łączność 802.11 – ESP32

■ Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32

- Zakłada się że stosowany będzie framework ESP-IDF oraz WPA-Enterprise
- Źródła przykładowego kodu są dostępne w drzewie esp-idf:

```
esp/esp-idf/examples/wifi/wifi_enterprise/main/wifi_enterprise_main.c
```

- Aby skompilować ten kod należy wydać polecenia konfiguracji zmiennych środowiskowych

```
cd /home/student/esp/esp-idf/
```

```
. ./export.sh
```

- Poczynam system zaraportuje następująco:

```
Setting IDF_PATH to '/home/student/esp/esp-idf'
```

```
Detecting the Python interpreter
```

```
...
```

```
Done! You can now compile ESP-IDF projects.
```

```
Go to the project directory and run:
```

```
idf.py build
```

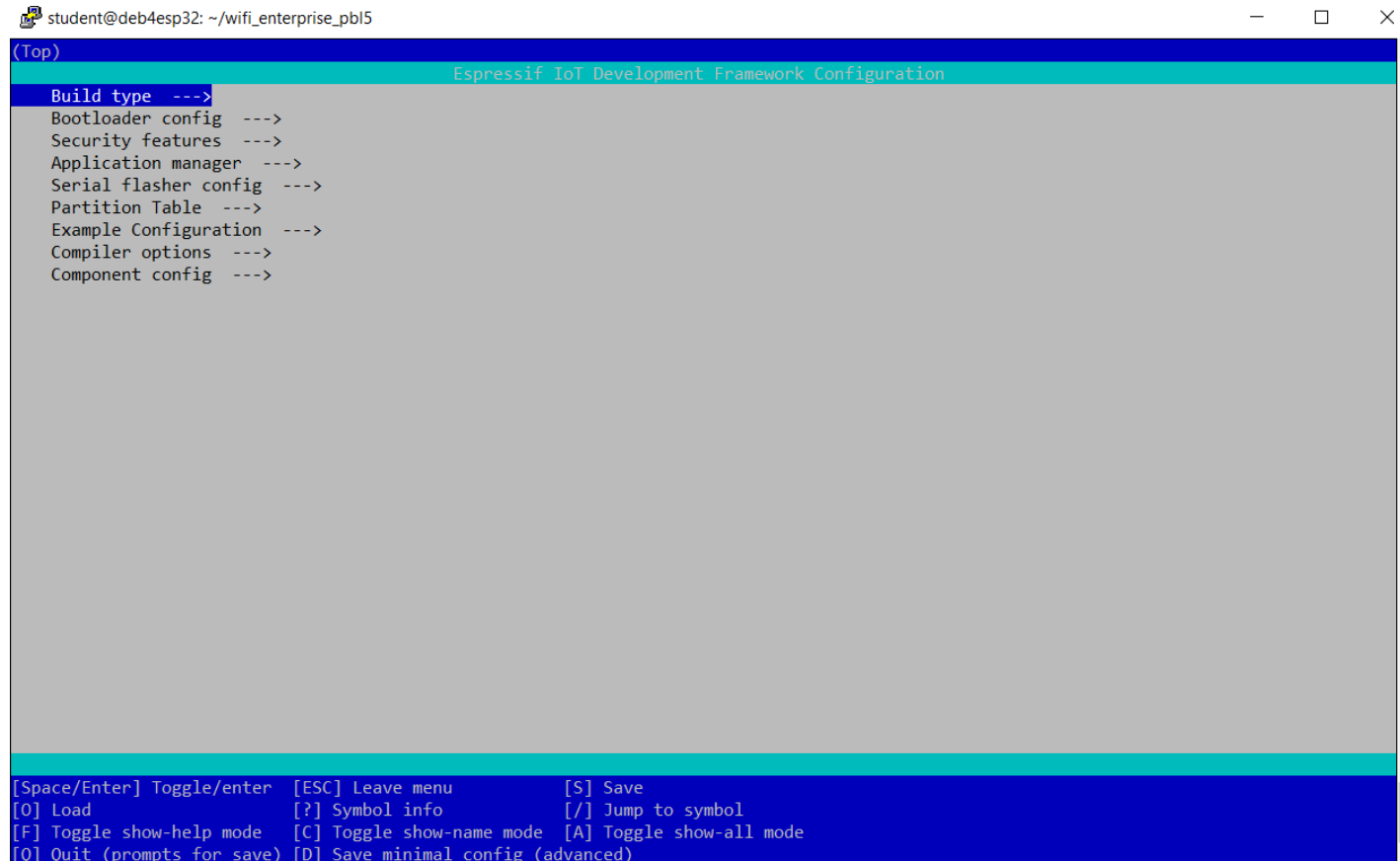
Źródła do pobrania w razie potrzeby z
<https://github.com/espressif/esp-idf.git>

Łączność 802.11 – ESP32

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Wchodzimy do katalogu: `esp-idf/examples/wifi/wifi_enterprise` i konfigurujemy otoczenie kompilacji kodu:

`idf.py menuconfig`

- Pojawi się następujące okienko



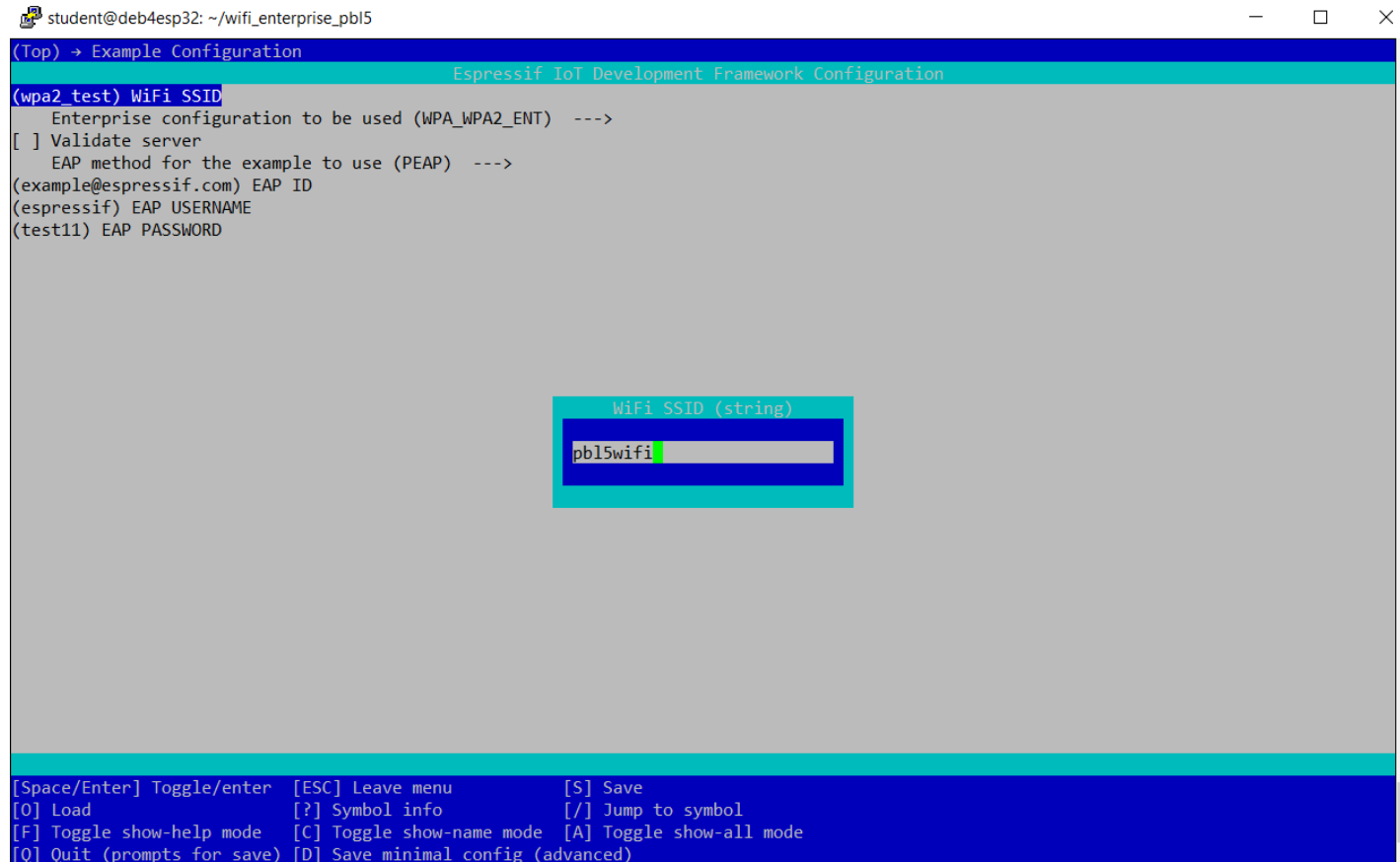
The screenshot shows a terminal window titled "student@deb4esp32: ~/wifi_enterprise_pbl5". Inside the terminal, the "Espressif IoT Development Framework Configuration" menu is displayed. The menu is a list of options with a teal header bar. The options are: Build type --->, Bootloader config --->, Security features --->, Application manager --->, Serial flasher config --->, Partition Table --->, Example Configuration --->, Compiler options --->, and Component config --->. The "Build type" option is currently selected and highlighted. At the bottom of the terminal, there is a blue bar containing keyboard shortcuts for navigating the menu: [Space/Enter] Toggle/enter, [ESC] Leave menu, [S] Save, [O] Load, [?] Symbol info, [/] Jump to symbol, [F] Toggle show-help mode, [C] Toggle show-name mode, [A] Toggle show-all mode, [Q] Quit (prompts for save), and [D] Save minimal config (advanced).

```
student@deb4esp32: ~/wifi_enterprise_pbl5
(Top)
Espressif IoT Development Framework Configuration
Build type --->
Bootloader config --->
Security features --->
Application manager --->
Serial flasher config --->
Partition Table --->
Example Configuration --->
Compiler options --->
Component config --->

[Space/Enter] Toggle/enter  [ESC] Leave menu          [S] Save
[O] Load                   [?] Symbol info           [/] Jump to symbol
[F] Toggle show-help mode  [C] Toggle show-name mode [A] Toggle show-all mode
[Q] Quit (prompts for save) [D] Save minimal config (advanced)
```


Łączność 802.11 – ESP32

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Po wybraniu „Example configuration” pojawią się opcje WIFI



```
student@deb4esp32: ~/wifi_enterprise_pbl5
(Top) → Example Configuration
Espressif IoT Development Framework Configuration
(wpa2 test) WiFi SSID
Enterprise configuration to be used (WPA_WPA2_ENT) --->
[ ] Validate server
EAP method for the example to use (PEAP) --->
(example@espressif.com) EAP ID
(espressif) EAP USERNAME
(test11) EAP PASSWORD

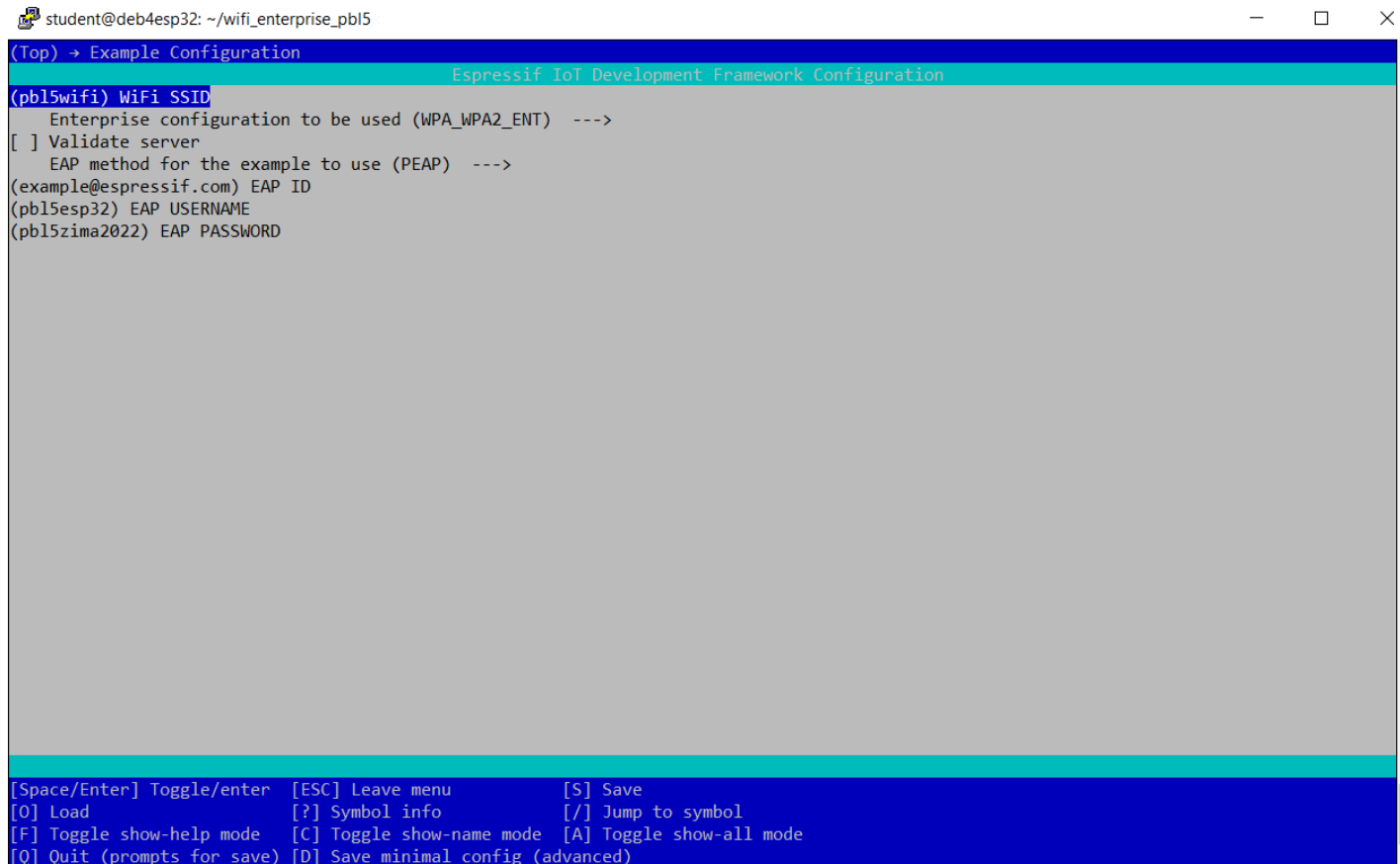
WiFi SSID (string)
pbl5wifi

[Space/Enter] Toggle/enter [ESC] Leave menu [S] Save
[O] Load [?] Symbol info [/] Jump to symbol
[F] Toggle show-help mode [C] Toggle show-name mode [A] Toggle show-all mode
[Q] Quit (prompts for save) [D] Save minimal config (advanced)
```

- Wybierając opcję „WiFi SSID” podajemy ID sieci z jaką ESP ma się łączyć (tu jest to pbl5wifi)
- Odznaczamy także pozycję „Validate server” – chyba że użyjemy kluczy X.509

Łączność 802.11 – ESP32

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Ustawiamy także „EAP USERNAME” (tu pbl5esp32) oraz „EAP PASSWORD” (tu pbl5zima2022)



```
student@deb4esp32: ~/wifi_enterprise_pbl5
(Top) → Example Configuration
Espressif IoT Development Framework Configuration
(pbl5wifi) WiFi SSID
  Enterprise configuration to be used (WPA_WPA2_ENT) --->
[ ] Validate server
  EAP method for the example to use (PEAP) --->
(example@espressif.com) EAP ID
(pbl5esp32) EAP USERNAME
(pbl5zima2022) EAP PASSWORD

[Space/Enter] Toggle/enter [ESC] Leave menu [S] Save
[O] Load [?] Symbol info [/] Jump to symbol
[F] Toggle show-help mode [C] Toggle show-name mode [A] Toggle show-all mode
[Q] Quit (prompts for save) [D] Save minimal config (advanced)
```

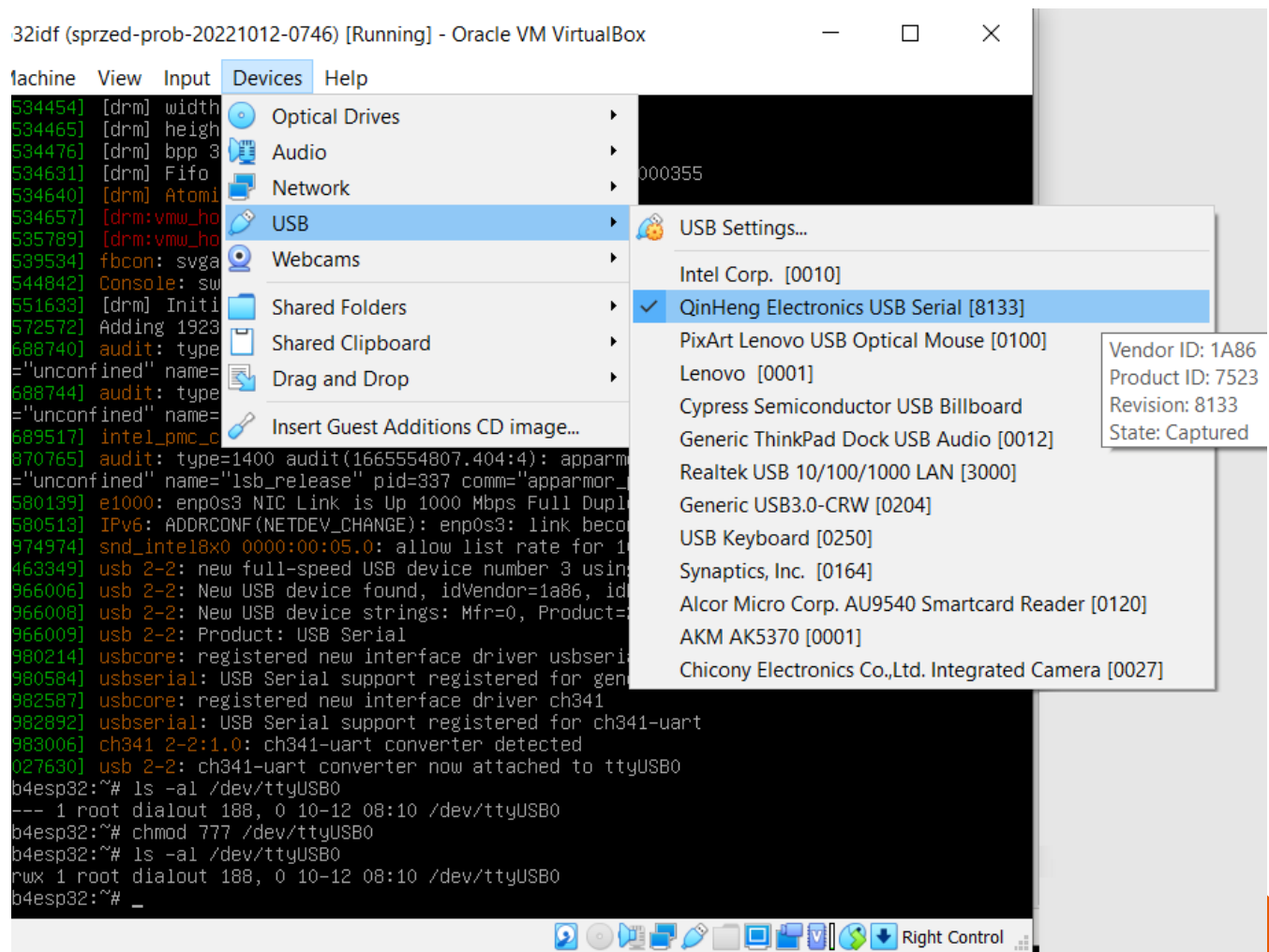
- Proszę pamiętać że powyższe ustawienia muszą być zgodne z ustawieniami punktu dostępowego w omawianym przykładzie: hostapd.conf i /etc/freeradius/3.0/users

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Po dokonaniu zmian przy pomocy klawisza ESC wychodzimy z menu możemy sprawdzić dokonane zmiany analizując plik sdkconfig, który zawierać będzie między innymi linie:

```
CONFIG_EXAMPLE_WIFI_SSID="pb15wifi"  
CONFIG_EXAMPLE_WPA_WPA2_ENTERPRISE=y  
CONFIG_EXAMPLE_EAP_METHOD_PEAP=y  
CONFIG_EXAMPLE_EAP_METHOD=1  
CONFIG_EXAMPLE_EAP_ID="example@espressif.com"  
CONFIG_EXAMPLE_EAP_USERNAME="pb15esp32"  
CONFIG_EXAMPLE_EAP_PASSWORD="pb15zima2022"
```

Łączność 802.11 – ESP32

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Pracując z ESP-IDF zainstalowanym na maszynie wirtualnej należy spiąć ją z modułem ESP32
 - ESP32 używają dla komunikacji z PC układ CH340 (VID: 1A86, PID:7523)



- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - Aby użytkownik student na maszynie wirtualnej mógł przeprowadzić procesy związane z dostępem do portu szeregowego łączącego z ESP32 należy zmienić odpowiednie prawa dostępu, np.:

```
su -c "/usr/bin/chmod 777 /dev/ttyUSB0"
```

- Istnieje szereg innych metod realizacji powyższego (zmiana w konfiguracji udev, dodanie użytkownika do grupy dialout) – metoda powyższa jest najprostsza, choć musi być przeprowadzona po każdorazowym fizycznym rozłączeniu platformy ESP32 od maszyny wirtualnej

Łączność 802.11 – ESP32

- Utworzenie stacji klienckiej z wykorzystaniem platformy ESP32, cd.
 - W następnym kroku należy aplikację skompilować, wgrać i przygotować do obserwacji logów:

```
idf.py -p /dev/ttyUSB0 build flash monitor
```

- Co na ekranie raportującym proces zakończyć powinno się następującą treścią

```
I (7101) wifi:connected with zsut, aid = 4, channel 6, BW20, bssid =  
b4:fb:e4:xx:xx:xx
```

```
I (7101) wifi:security: WPA2-ENT, phy: bgn, rssi: -81
```

```
...
```

```
I (9091) esp_netif_handlers: sta ip: 10.15.0.44, mask: 255.255.255.0,  
gw: 10.15.0.1
```

```
I (10801) example: ~~~~~~
```

```
I (10801) example: IP:10.15.0.44
```

```
I (10801) example: MASK:255.255.255.0
```

```
I (10801) example: GW:10.15.0.1
```

```
I (10801) example: ~~~~~~
```

Tutaj widać że finalnie zestawiono
połącznie z punktem dostępowym

Wyjście z ESP-IDF monitora następuje za
pomocą kombinacji klawisza CTRL i]

Zadanie:

Używając WPA2-Enterprise zapewnij ESP32 łączność wifi (etap I) oraz zintegruj kod z obsługą protokołu MQTT poprzez broker zainstalowany na maszynie wirtualnej z tzw. „wzorcową konfiguracją” (etap II)

Dodatek A

- Wzorcowy konfiguracja brokera mosquitto (plik mosquitto.conf):
 - Nie zalecana dla instalacji produkcyjnych

```
autosave_interval 1800  
  
persistence true  
  
persistence_file m2.db  
  
persistence_location /home/student/tmp/  
  
connection_messages true  
  
log_timestamp true  
  
log_dest file /home/student/log/mosquitto.log  
  
log_dest syslog  
  
log_dest stdout  
  
log_dest topic  
  
listener 1883  
  
allow_anonymous true
```


Dodatek B

■ Ręczne uruchomienie brokera mosquitto (wersja dla eksperymentów)

■ Przygotowanie plików

```
cd /home/student  
mkdir log  
mkdir tmp  
chmod 777 tmp  
chmod 777 log  
touch log/mosquitto.log  
chmod 777 log/mosquitto.log
```

■ Właściwe uruchomienie brokera (dla zakończenia: CTRL + C)

```
/usr/sbin/mosquitto -c /home/student/mosquitto.conf -v
```

■ Przed powyższym proszę sprawdzić czy broker mosquitto nie jest już uruchomiony (!)

Dziękuję za uwagę