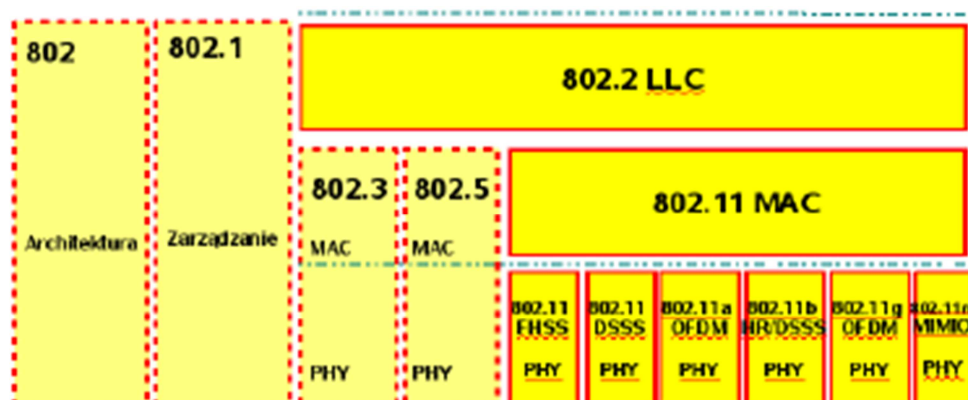


# Sieci Bezprzewodowe IEEE802.11

## 1. Informacje ogólne:

Rodzina standardów IEEE 802.11, określana popularnie jako WiFi (ang. Wireless Fidelity – „bezprowadowa wierność”) definiuje sposób działania sieci bezprzewodowej wykorzystującej (początkowo rozważano także podczerwień) pasmo mikrofalowe w w paśmie S (2-4GHz) konkretnie S PNM (2,4-2,5GHz) oraz paśmie C (4-8GHz) konkretnie C PNM (5,725-5,875GHz). Szczegółowe zakresy są regulowane przez ustawodawstwa poszczególnych państw. Pierwsze regulacje prawne w Polsce to Dz.U.02.138.1162 z dnia 6 sierpnia 2002 r. i dotyczy pasma S PNM i określa zakres częstotliwości oraz maksymalną moc nadajnika, która nie wymaga licencji URTiP na 100mW. Kolejne uregulowania weszły w życie wraz z uregulowaniami UE (głównie dotyczy to pasma C PNM). Prawo wymaga także aby sygnał radiowy używany przez nadajniki był rozproszony w pewnym zakresie częstotliwości przypominając tym samym szum. Standardy 802.11 (szczególnie warstwa LLC, sposób adresowania oraz sposób dostępu do medium CSMA/CD) zostały zaprojektowane dla możliwie dużej kompatybilności ze standardami 802.3 (Ethernet), który miał być w założeniu siecią szkieletową dla WiFi. Zakres częstotliwości dzielony jest na kanały (z których tylko kilka jest niezależnych) a kanały na pod kanały, których liczba zależna jest od warstwy PHY (typ rozpraszania, kodowanie i modulacja)



Rys 1 Warstwy I i II modelu OSI i odpowiadające im standardy 802.

## 2. Standardy 802.11:

Standard	rok	częstotliwości	prędkość transm.	inne
802.11	1997	2.4 -2.5 GHz	1/2Mb/s	
802.11a	1999	5.15-5.35 5.47-5.725 5.725-5.875 GHz	25/54Mb/s	~50m
802.11b	1999	2.4-2.5 GHz	6,5/11Mb/s	~100m
802.11g	2003	2.4-2.5 GHz	11/54Mb/s	~100m
802.11n	2008?	2,4/5GHz	200/540Mbs	~200m
802.11i				bezpieczeństwo

### 3. Działanie warstwy fizycznej PHY:

#### Architektura warstwy PHY 802.11

- PLCP (Physical Layer Convergence Procedure)
  - Dodaje swój nagłówek do przesyłanych do anteny ramek niezależnie od stosowanej metody modulacji w tym preambułę (SYNC 80b i SFD 16b) i elementy nagłówka (PLW – długość ramki MAC, PSF -określa prędkość dla FHSS; Signal, Service, Length dla DSSS, HEC/FHSS i CRC/DSSS – zabezpieczenie przed błędami nagłówka)
- PMD (Physical Layer Dependent)
  - Odpowiada za transmisję bitów za pomocą anteny
  - dla 802.11 zdefiniowano 2 technologie moc 10 do 100mW możliwość użycia kilku anten
- Funkcja CCA (Clear Channel Assessment )
  - Szacowanie wolnego kanału
  - Przekazuje informację do MAC
- FHSS (Frequency Hopping Spread Spectrum)
  - Rozpraszanie widma z przeskokami po częstotliwościach
  - Losowe przeskoki po częstotliwościach, krótkie sekwencje na różnych podkanałach o szerokości 1MHz
    - 2GFSK (Gaussian Frequency Shift Keying +/-160kHz) - 1Mbps
    - 4GFSK (+/-72 i +/-216kHz)- 2Mb/s
- DSSS (Direct Sequence Spread Spectrum)
  - Rozpraszanie widma za pomocą kluczowania bezpośredniego,
  - kolejność przeskoków – funkcja matematyczna
  - Szersze pasma częstotliwości 5MHz 14 kanałów ale tylko 3 niezależne (1-2412; 6-2437; 11-2461MHz)
    - DPSK
    - DBPSK
    - DQPSK (najszybsza 4 zmiany fazy, najmniej odporna na zakłócenia)
- HR/DSSS (High Rate DSSS)
  - Kluczowanie bezpośrednie o zwiększonej prędkości
  - Dla CCK (Complementary code keying)
    - transformacje matematyczne 5,5 i 11Mb/s
- OFDM (Orthogonal Frequency Division Multiplexing) lub DMT (Discrete Multitone Mod.)
- Ortogonalne zwielokrotnianie częstotliwości
- Podział szerokiego pasma na szereg wąskich – 48 podkanałów polaryzowanych naprzemiennie poziomo i pionowo dla zmniejszenia zakłóceń między podkanałami
  - prędkość 6 - 54/Mbs
- Dane przeplatane na wielu podkanałach równocześnie
- Lepsze wykorzystanie kanału w przypadku wielu urządzeń
- Modulacje
  - BPSK 6-9Mb/s
  - QPSK 12-18Mb/s
  - QAM - 24-54/Mbs
- MIMO (Multiple Input Multiple Output) Wiele wejść wiele wyjść
  - W projekcie prędkość przesyłania nawet do 380 (lub nawet 540) Mb/s i zasięgi pow 100 m
  - użycie wielu anten w odpowiednich odległościach dzięki temu każda odbiera sygnał z innymi zakłóceniami
  - wykorzystanie odbić wielodrożnych (które zakłócały starsze technologie) do odzyskiwania sygnału
- SIMO jw. ale za pomocą jednej anteny

#### 4. Dostęp do medium i adresowanie:

Sposób dostępu do medium przypomina CSMA/CD stosowany w standardzie IEEE802.3 tzn kolizje są typowym zachowaniem sieci. Zmiany jakie wprowadzono do tego schematu działania wynikają z „niepewności nośnika” i sprowadzają się do:

1. ponieważ nigdy nie jesteśmy pewni czy odbiorca ramki jest w zasięgu zastosowano technikę pozytywnego potwierdzenia: większość ramek musi być potwierdzone ramką ACK jej brak wymusza automatyczne ponowienie transmisji (mogą pojawić się ramki zdublikowane u odbiorcy)

2. Stacja, która z powodzeniem rozpoczęła transmisję informuje w każdym pakiecie jaki czas rezerwuje na transmisję: jest to tzw Wektor Alokacji Sieci (NAV – Network Allocation Vector) a pozostałe stacje przeliczają ten czas niezależnie (mogą być chwilowo poza zasięgiem)

3. W przypadku kiedy w sieci istnieją stacje które się „nie widzą” aby się wzajemnie nie zakłócały stosuje się sekwencję RTS (Request to Send – nadaje stacja rozpoczynająca transmisję u ucisza stacje w swoim zasięgu) – CTS (Clear to Send – stacja do której skierowana była ramka RTS odpowiada CTS uciszając stacje w swoim zasięgu) po czym rozpoczyna się transmisja

Najważniejszą ramką zarządzającą w sieciach 802.11 jest ramka Beacon rozsyłana jest w stałych odstępach czasu przez punkt dostępowy (AP) lub w sieci „Ad Hoc” przez stację która w pewnym przedziale czasowym wylosuje najkrótszy offset. Losowanie ponawiane jest za każdym razem kiedy przychodzi czas na wysłanie ramki Beacon.

##### Zawartość ramki beacon:

- Timestamp - stempel czasowy do synchronizacji
- Channel information – Informacja na temat kanału
- Data Rates – podstawowy i inne wspierane szybkości transmisji
- Service Set capabilities – dodatkowe parametry dla BSS lub IBSS
- SSID – nazwa sieci
- TIM (Traffic Indication Map) – informacja na temat buforowanych ramek dla stacji będących w trybie oszczędzania energii
- VPI (Vendor Proprietary Information) – Informacje zależne od producenta sprzętu

Typowo ramka Beacon jest rozsyłana 10 razy na sekundę.

##### Budowa ramki

Ramka w sieci 802.11 jest poprzedzona nagłówkiem zależnym od warstwy PHY

Treść – Ładunek użyteczny jest najczęściej zgodna z ramką LLC taką jak np w 802.3

FCS – służy kontroli poprawności przesłania ramki



##### Sposób adresowania i funkcje pól adresowych

Ramka 802.11 posiada 4 pola adresowe ich funkcja i zawartość jest zależna od trybu pracy sieci

Funkcja	DoDS	ZDS	Adres1	Adres2	Adres3	Adres4
IBSS	0	0	DA	SA	BSSID	NW
Do AP	1	0	BSSID	SA	DA	NW
Od AP	0	1	DA	BSSID	SA	NW
Most	1	1	RA	TA	DA	SA

DoDS - Do punktu dystrybucyjnego  
ZDS - Z punktu dystrybucyjnego  
DA – Adres przeznaczenia  
SA – Adres źródła  
NW – Nie wykorzystane

### Praca w sieci WiFi w przypadku zakłóceń

Sieć bezprzewodowa jest bardziej narażona na zakłócenia niż sieci oparte o okablowanie miedziane czy światłowodowe. Przy przechodzeniu przez powietrze a tym bardziej przez inne przeszkody (ściany budynków) sygnał ulega tłumieniu i rozpraszaniu. Gdy stacja jest w ruchu może wystąpić efekt Dopplera. Sygnał może dochodzić do odbiornika różnymi drogami co prowadzi do interferencji w wyniku której sygnał może nawet zostać wygaszony. Teoretycznie sieci radiowe radzą sobie z opóźnieniami rzędu 500ns ale w praktyce do efektywnego działania dla standardów a,b,g opóźnienia nie powinny przekraczać 65ns. W standardzie 802.11n/MIMO interferencja wielodrożna jest wykorzystywana dla poprawy warunków transmisji. Zakłócenia mogą pochodzić od innych sieci 802.11 – w sytuacji braku wolnych niezależnych kanałów wzajemne zakłócanie można zmniejszyć za pomocą sekwencji RTS-CTS ale odbywa się to kosztem zmniejszenia przepustowości. W przypadku zakłócania z 802.15(BT) nie ma prostego rozwiązania. Jeszcze gorzej sytuacja przedstawia się gdy mamy do czynienia z urządzeniami które emitują zakłócenia na paśmie mikrofalowym. W przypadku kuchenki mikrofalowej (emituje impulsy mikrofal co 2x częstotliwość sieci elektrycznej) można zmniejszyć ilość zakłóconych danych zmniejszając parametr MTU czyli wielkość ramki także kosztem większych narzutów na transmisję.

## 5. Budowa sieci 802.11 i tryby współpracy urządzeń

- IBSS (Independent Basic Service Set)– niezależne stacje łączące się w trybie „ad hoc” (w razie potrzeby/ z doskoku) na zasadzie peer-to-peer (każdy z każdym) tworząc pełną lub częściową siatkę (mesh). Ramka Beacon wysyłana jest przez stację, która wylosowała najmniejszy offset w oknie rywalizacji do wysłania tej ramki. Otrzymując ją inne stacje zaprzestają przygotowań do wysłania tej ramki aż do następnego cyklu.
- BSS (tryb zarządzany - 1 AP) – punkt dostępowy pełni rolę zarządzającą wysyłając ramki Beacon i decyduje czy dana stacja zostanie podłączona czy nie. Wspomaga zarządzanie energią stacji buforując pakiety. Cały ruch pomiędzy stacjami bezprzewodowymi i stacjami przewodowymi a siecią przewodową odbywa się za pośrednictwem AP
- ESS (Extended SS - infrastruktura - wiele AP) – jw ale wchodzące w skład ESS AP mogą pracować na jednym bądź kilku kanałach dla zwiększenia przepustowości. Funkcje autoryzacji są często scentralizowane i realizowane przez jeden AP lub wydzielone urządzenie (serwer dystrybucji kluczy np radius; DHCP). Punkty komunikują się ze sobą za pomocą protokołu IAP (Inter AccessPoint Protocol). Stacja może być skojarzona tylko z jednym punktem dostępowym.

Punkt dostępowy może spełniać różne funkcje:

- **bridge AP** funkcja mostu pomiędzy siecią przewodową (802.3) a 802.11 stacje za pośrednictwem WiFi łączą się z siecią szkieletową
- **bridge WDS (Wireless Distant Service)** funkcja mostu bezprzewodowego, w którym jeden AP nie ma dostępu do sieci strukturalnej (połowa pasma jest rezerwowana na funkcje mostu) umożliwia przedłużenie zasięgu sieci bez konieczności budowy przewodowej sieci szkieletowej
- **client** funkcja mostu w której AP nie może obsługiwać stacji bezprzewodowych tylko przewodowe

## 6. Podłączenie do sieci bezprzewodowej

### Skanowanie

- skanowanie pasywne – zmiany kanałów i nasłuchiwanie ramki Beacon
- skanowanie aktywne – zmiana kanału wysłanie ramki ProbeRequest (z identyfikatorem sieci SSID bądź bez) nasłuchiwanie ProbeResponse

### Przyłączenie do sieci

Wybór sieci

wybór punktu dostępowego

Dopasowanie parametrów PHY i synchronizacja czasu

### Uwierzytelnienie

**OpenSystem** (otwarty system) – krótka sekwencja, każda stacja jest akceptowana. Jest to jedyny typ uwierzytelnienia wymagany standardem

### SharedKey (klucz współdzielony)

Pierwsza implementacja zakładała użycie klucza WEP (Wireless ----- Privacy)

Stacja aby została zaakceptowana musi zaszyfrować przy pomocy algorytmu RC4 z użyciem otrzymanego inną drogą klucza ciągu znaków „ChallengeText” jeżeli punkt dostępowy odtworzy tekst źródłowy przy pomocy klucza przechowywanego u siebie stacja jest akceptowana. WEP zapewnia zarówno poufność jak i autoryzację

Obecnie Standard 802.11i oddziela autoryzację od zapewnienia poufności

Autoryzacja: np WPA - TKIP MIC; WPA2 – CCMP(AES), EAP/PEAP

Poufność np TLS

### Skojarzenie

W tym trybie stacja może przysyłać ramki poza AP (do innych stacji)

Tylko z jednym punktem dostępowym. Stacja wybiera nowy punkt jeżeli parametry transmisji spadną poniżej pewnego poziomu. Aby przyspieszyć skojarzenie jest możliwe skojarzenie wstępne

## 7. Programy używane na laboratoriach

### Android

#### a) WifiAnalyzer

WifiAnalyzer to darmowe narzędzie do analizy sieci bezprzewodowych. Pozwala sprawdzić jakie kanały są obecnie zajmowane przez konkretne sieci oraz sprawdzić moc sygnałów poszczególnych punktów dostępowych. Aplikacja może wygenerować wykresy natężenia sygnału każdej sieci bezprzewodowej w zadanym okresie czasu oraz określić częstotliwość i rodzaj zabezpieczeń poszczególnych sieci.

### Literatura:

[1] Gast, Matthew S.; „802.11 - sieci bezprzewodowe : przewodnik encyklopedyczny” t ł. Arkadiusz Romanek, Witold Ziolo; Wyd. Gliwice : Helion, cop. 2003. 46s

[2] Potter, Bruce. „ 802.11 – bezpieczeństwo”; tł. Marcin Jędrzyak; W yd.: Gliwice : Wydaw. Helion, 2004.

[3] Ross, John . ; „ Sieci standardu Wi-Fi” tł: Robert Filimonowicz W yd.: Poznań,, : Wydawnictwo "Nakom", cop. 2004

[4] Skop, Ireneusz.; „ Sieć bezprzewodowa Wi-Fi” ; Wyd: Gliwice : Helion, 2005 .

[5] Bezpieczeństwo bezprzewodowych sieci LAN / Krishna Sankar [et al.]; tł Marek Korbecki.; W yd. Warszawa : Mikom, 2005.

[6] Roshan, Pejman.; „ Bezprzewodowe sieci LAN 802.11 : podstawy”; tł: Maciej Baranowski. Wydanie Wyd. 1, Wyd . Warszawa : Wydawnictwo Naukowe PWN SA, 2006.

# Scenariusz nr 1

## 1. Sprzęt i oprogramowanie:

Sprzęt: Własny smartfon z systemem operacyjnym Android

Oprogramowanie: Aplikacja "Wifi Analyzer" - darmowa, dostępna z GooglePlay

## 2. Przygotowanie do wykonania ćwiczenia

- a. Zainstalować aplikację WiFi Analyzer
- b. Naszkicować mapę piętra w budynku na którym będą przeprowadzane testy.

## 3. Wariant scenariusza

- a. Piętra na których przeprowadzone będą testy .....
- b. Sieci do analizy (Faza A)
  - i. Rozległe (duży zasięg, mocny sygnał, zmieniające się adresy MAC AP)
    1. ...
    2. ....
  - ii. Unikalne parametry (znana / ciekawa lokalizacja AP, np. poza budynkiem, na dachu, punkt dostępowy z telefonu itp)
    1. ....
    2. ....
- c. Odnalezione punkty dostępowe (Faza B)
  - i. ....
  - ii. ....
  - iii. ....
  - iv. ....

## 4. Wykonanie ćwiczenia:

(Faza A) Na każdym piętrze, w 7 równo oddalonych od siebie punktach wykonać zrzuty ekranu ("migawka") w zakładce "lista punktów dostępu". W nazwie zrzutu ekranu uwzględnić numer piętra oraz numer punktu na piętrze.

(Faza B) W ramach obszaru na którym przeprowadzano testy w Fazie A zlokalizować ..... różne punkty dostępowe. Sposób realizacji: przemieszczając się po korytarzu na różnych piętrach, jednocześnie monitorując siłę sygnału, wyznaczyć dokładny punkt w którym siła sygnału dla danej sieci jest największa. Punkt zaznaczyć na naszkicowanej mapie i podać numer pokoju/laboratorium w którym prawdopodobnie znajduje się punkt dostępowy

## 5. Wyniki pomiarów:

Opracować informacje ogólne na temat badanego obszaru:

lista dostępnych sieci na poszczególnych piętrach

niezmienne charakterystyki wszystkich sieci (kanał, SSID, protokół, typ szyfrowania)

Dla sieci badanych w FazieA opracować mapę siły sygnału na poszczególnych piętrach

7 piętro	-86	-89	-91	-81	-90	-	-
6 piętro	-70	-75	-80	-88	-86	-89	-93
5 piętro	-63	-60	-63	-73	-78	-82	-83
	7	6	5	4	3	2	1

Dodatkowo dla sieci rozległych [FazaA podpunkt i)] opracować mapę AP dostępnych w poszczególnych punktach.

	Punkt 1	Punkt 2	Punkt 3	Punkt 4	Punkt 5	Punkt 6	Punkt 7
Piętro 5	1, 4	1	1, 2	1, 2	1, 2	1	1
Piętro 6	1	1	1	1	1	-	-
Piętro 7	1	1	1, 3	3	3	-	-

Dostępne adresy MAC sieci:

1. 00:23:33:2b:da:00
2. 00:23:33:2c:11:f0
3. 00:23:33:2c:19:e0
4. b4:e9:b0:58:39:a0

Dla sieci odnalezionych w FazieB oznaczyć ich lokalizację (na schemacie piętra) wraz z informacją o sile sygnału.

\*) Porównać z mapą sygnału wygenerowaną jak dla sieci z FazyA

Podsumować wyniki - opracować statystycznie typy sieci/protokołów oraz stosowane w nich sposoby zabezpieczeń (szyfrowania i autentyfikacji)

Opracować wnioski wynikające z danych uzyskanych podczas badań w trakcie laboratorium.