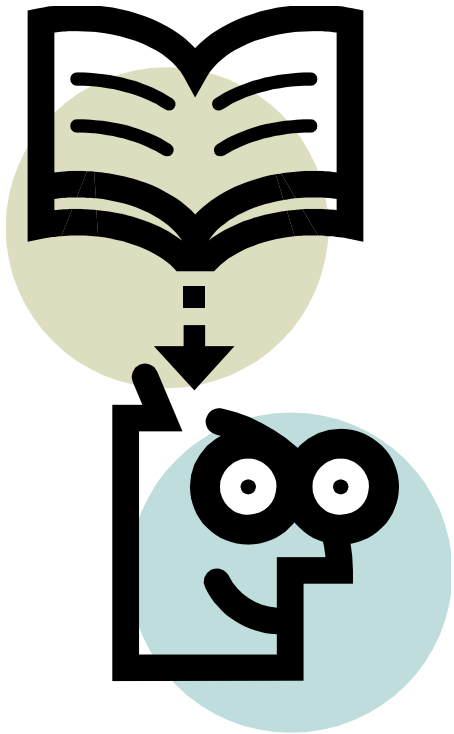
Projektowanie i Realizacja Sieci Komputerowych

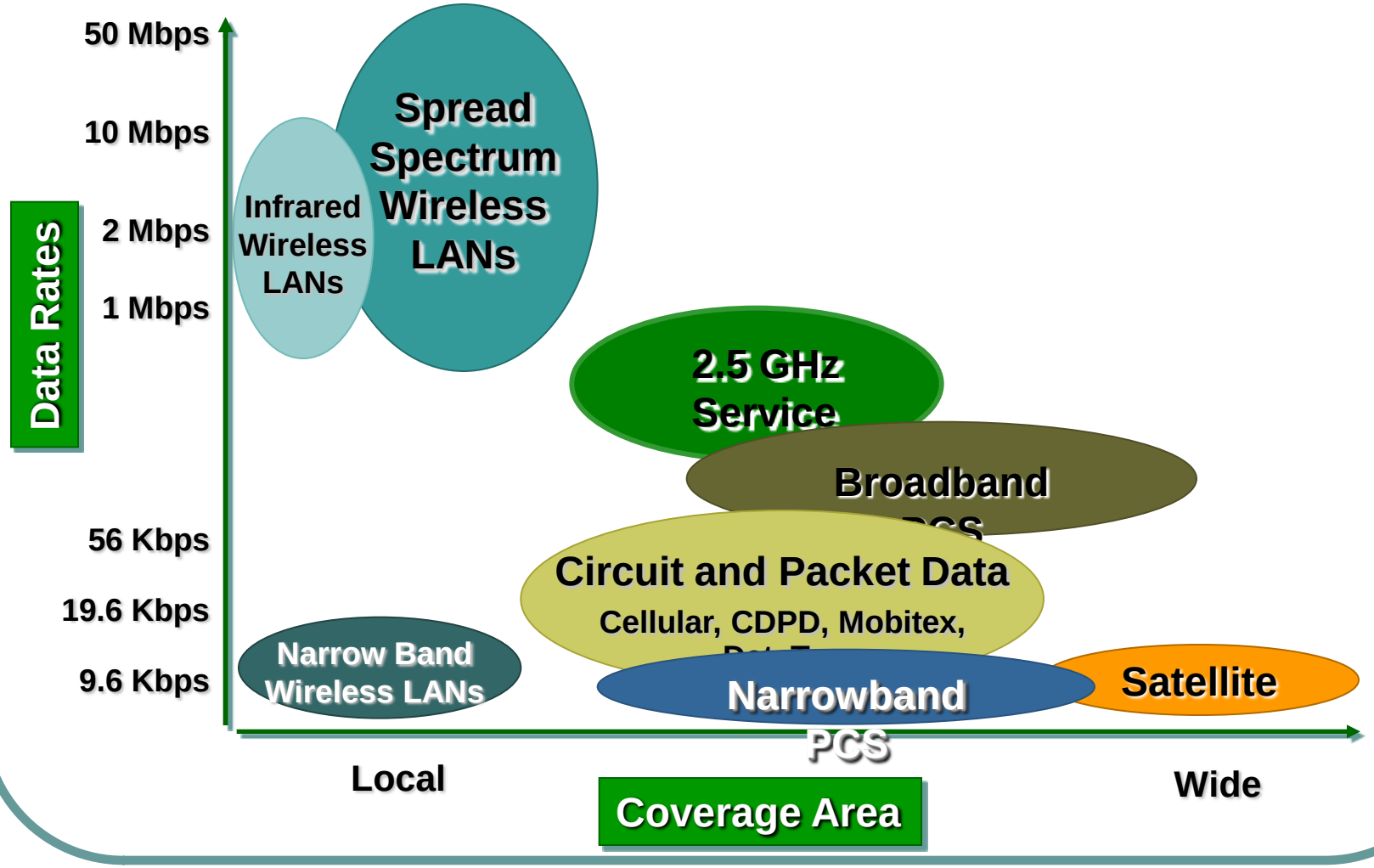
Wykład 7

1. Technologie sieci WLAN (*Wireless Local Area Network)*
2. Urządzenia sieci WLAN

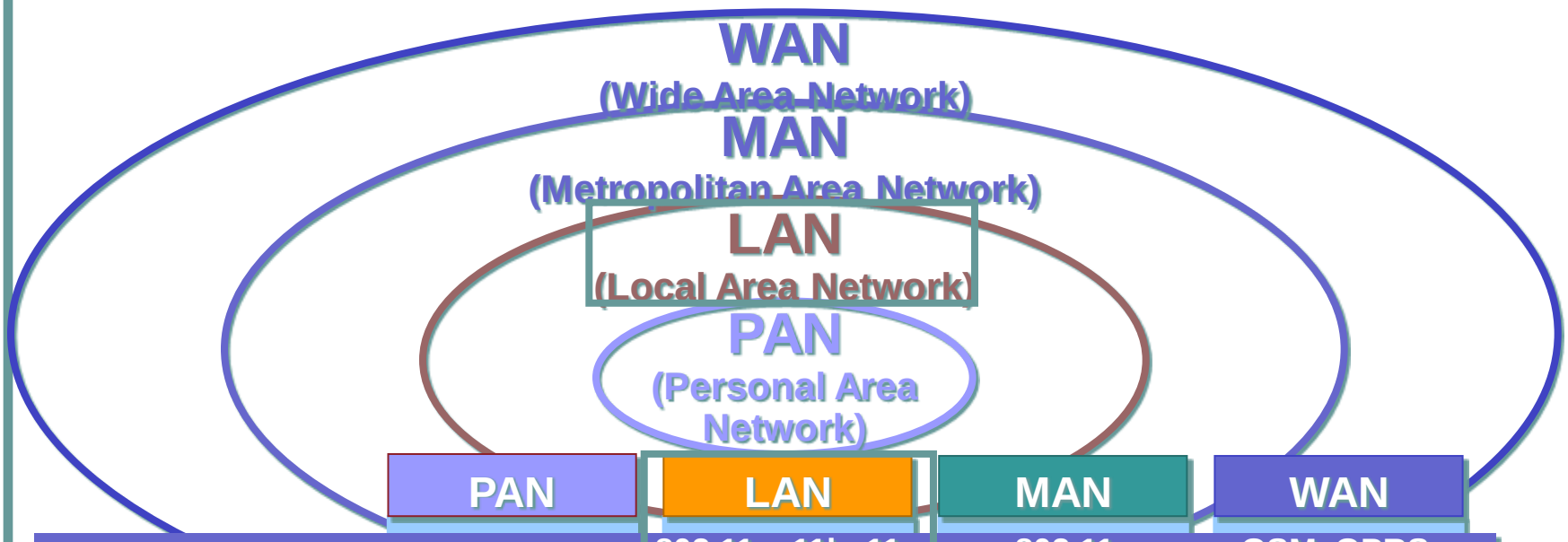


dr inż. Artur Sierszeń asiersz@kis.p.lodz.pl
dr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

Wireless Data Networks



Wireless Technologies



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5–3G
Speed	<1 Mbps	2–54+ Mbps	22+ Mbps	10–384 Kbps
Range	Short	Medium	Medium–Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Fixed, Last Mile Access	PDAs, Mobile Phones, Cellular Access

Transmisja bezprzewodowa

- Sieci bezprzewodowe – **WLAN** (*Wireless Local Area Network*)
- Organizacje i standardy dotyczące sieci bezprzewodowych:
  - Głównym twórcą standardów obowiązujących w sieciach bezprzewodowych jest organizacja IEEE

Transmisja bezprzewodowa

- Fale radiowe i mikrofale:
  - Nadajniki radiowe konwertują sygnały elektryczne na fale radiowe. Zmiana prądu elektrycznego w antenie nadajnika powoduje wygenerowanie fali radiowej.
  - Fale radiowe są tłumione w miarę oddalania się od anteny nadawczej.
    W sieci WLAN sygnał radiowy mierzony w odległości 10 metrów od anteny nadawczej będzie miał tylko 1/100 oryginalnej mocy.
  - Fale radiowe mogą być pochłaniane i odbijane przez niektóre ośrodki. Przy przechodzeniu z jednego ośrodka do innego (np. powietrze – ściana gipsowa) fale radiowe ulegają załamaniu.
    Fale radiowe są również rozpraszane i pochłaniane przez krople wody w powietrzu.

Propagacja sygnału radiowego

Źródło: David Wagner - Why Swiss-Cheese Security Isn't Enough

Sieci WLAN

- Zastosowanie:
  - Lokalizacje, w których nie można lub nie wolno instalować okablowania;
  - Miejsca użyteczności publicznej: lotniska, hotele, itp.;
  - Częste zmiany konfiguracji sieci, umiejscowienia urządzeń czy tymczasowe instalacje.

Standardy WLAN

- Podstawową technologią opisaną w standardzie **802.11** (1997r.) jest DSSS (*Direct Sequence Spread Spectrum*). Technologia DSSS dotyczy urządzeń bezprzewodowych pracujących w zakresie szybkości od 1 do 2 Mb/s.
- Standard **802.11b** jest nazywany również standardem **802.11 High Rate** lub **Wi-Fi™ ,** dotyczy systemów DSSS, które pracują z szybkością 1, 2, 5,5 i 11 Mb/s.
- Urządzenia 802.11b uzyskują wyższe szybkości przesyłania danych dzięki zastosowaniu innej techniki kodowania niż w przypadku 802.11, umożliwiając przesłanie większej ilości danych w tej samej ramce czasowej.

Standardy WLAN

- Standard **802.11a** dotyczy urządzeń sieci WLAN pracujących w paśmie transmisyjnym 5 GHz. Szybkość 54 Mb/s, przy zastosowaniu technologii zwanej „podwajanie szybkości” - 108 Mb/s.
- Standard **802.11g** zapewnia taką samą szybkość jak 802.11a, ale jest zgodny wstecz z urządzeniami 802.11b - technologia modulacji OFDM (*Orthogonal Frequency Division Multiplexing*).

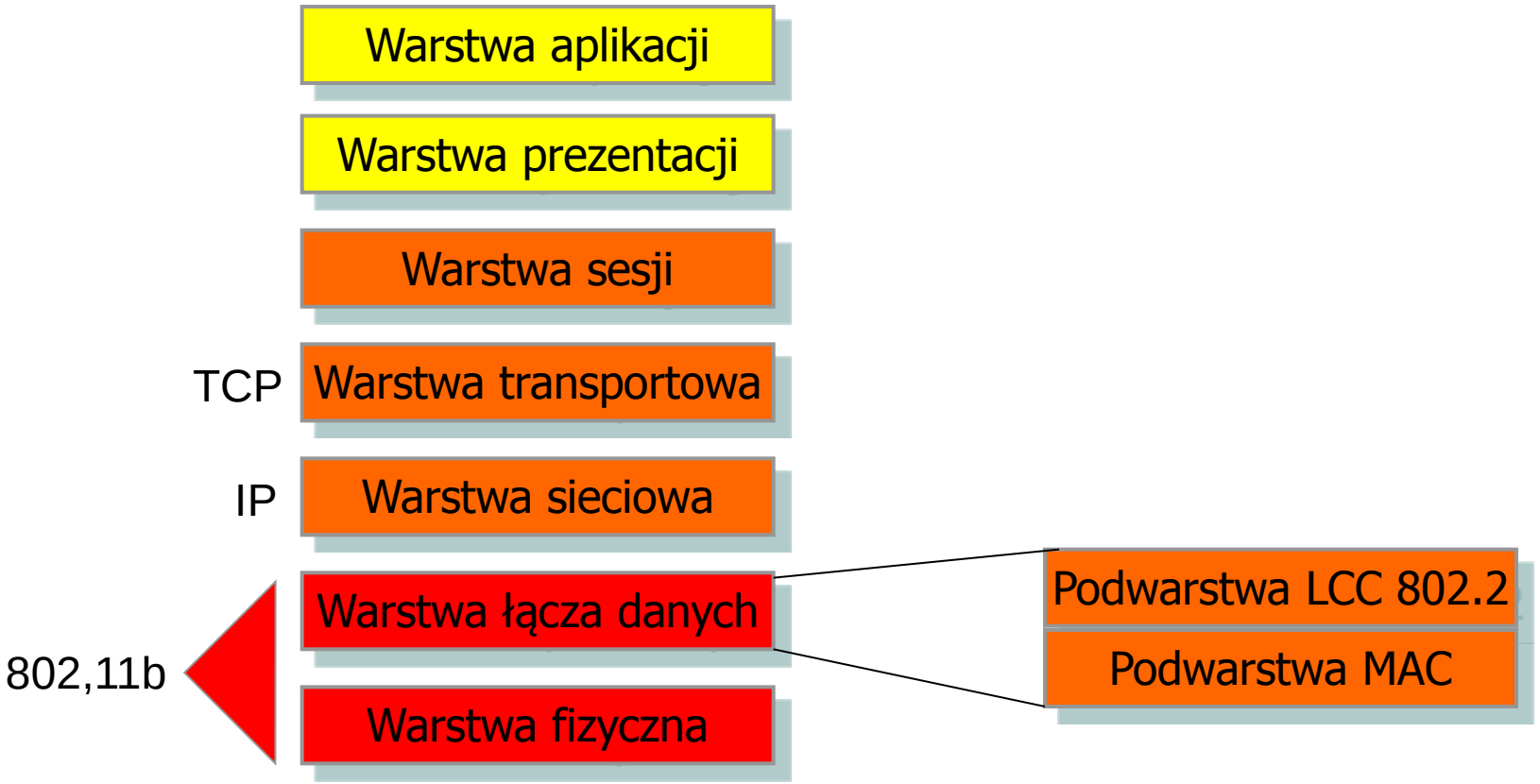
Standard 802.11b

- Standard **802.11b** jest nazywany również standardem **802.11 High Rate** lub **Wi-Fi™**:
  - Pasmo:
    - Europa i USA: 2,4 – 2,4835 GHz.
    - Japonia: 2,471 – 2,497 GHz.
  - Szybkość: 1, 2, 5,5 i 11 Mb/s.
  - Modulacja:
    - FHSS
    - DSSS.
  - Warstwa fizyczna:
    - Podwarstwa PLCP
    - Podwarstwa PMD
  - Warstwa łącza danych (LLC 802.2 oraz MAC 802.11b – metoda dostępu CSMA/CA):
    - Tryb pracy *ad hoc*
    - Tryb pracy infrastrukturalny

IEEE 802.11 Standardy

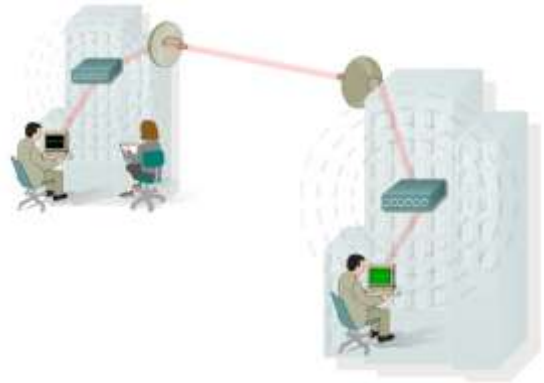
- 802.11a: 5GHz, 54Mbps
- 802.11b: 2.4GHz, 11Mbps
- 802.11d: Nadzorujący wspólne domeny
- 802.11e: Quality of Service (QoS)
- 802.11f: Inter-Access Point Protocol (IAPP)
- 802.11g: 2.4GHz, 54Mbps
- 802.11h: Dynamic Frequency Selection (DFS)
  Transmit Power Control (TPC)
- 802.11i: Security
- 802.11j: Japan 5GHz (4.9-5.1 GHz)
- 802.11k: Pomiary

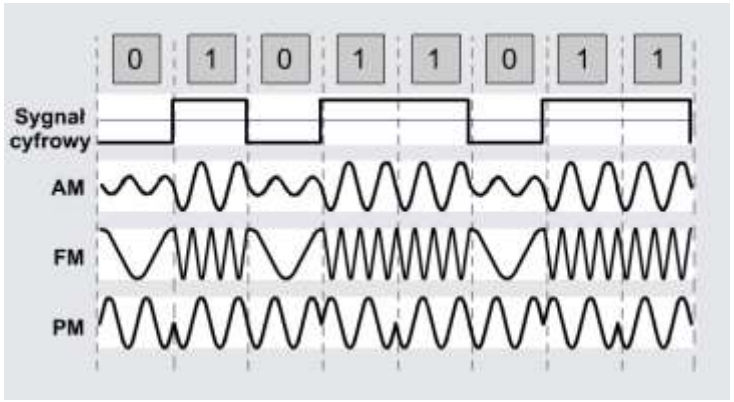
802.11b na tle modeli OSI



Transmisja bezprzewodowa

- Modulacja:
  - W nadajniku sygnały elektryczne (dane) pochodzące z komputera lub sieci nie są bezpośrednio wysyłane do anteny nadajnika. Sygnały te są używane do zmiany drugiego, silniejszego sygnału zwanego nośną.
  - Proces zmiany sygnału nośnej, która jest przesyłana do anteny, jest nazywany modulacją.





Warstwa fizyczna
Modulacja w 802.11b

- FHSS (*Frequency-Hopping Spread-Spectrum*):
  - Metoda modulacji, oparta na widmie rozproszonym, w której używany jest wąskopasmowy przebieg nośny o częstotliwości zmieniającej się zgodnie ze wzorcem znanym zarówno nadajnikowi, jak i odbiornikowi. Przy odpowiedniej synchronizacji urządzenia te tworzą pojedynczy kanał logiczny.
  - Odbiorniki, dla których transmisja nie jest przeznaczona, postrzegają sygnał FHSS jako szum złożony z krótkotrwałych impulsów.

Warstwa fizyczna
Modulacja w 802.11b

- DSSS (*Direct Sequence Spread Spectrum*):
  - DSSS jest metodą modulacji, opartą na widmie rozproszonym, w której do każdego transmitowanego bitu tworzony jest nadmiarowy, wzorcowy ciąg bitów. Wzorzec ten, nazywany żetonem lub kodem chipowym *(chipping code),* umożliwia odbiornikom odfiltrowanie sygnałów, które nie używają tego samego wzorca, w tym szumu oraz innych zakłóceń.
  - Kod ten identyfikuje dane, dzięki czemu odbiornik może rozpoznać je jako pochodzące z określonego nadajnika - nadajnik generuje kod chipowy, w związku z czym dane mogą być rozszyfrowane tylko przez odbiornik, który zna ten kod.

Warstwa fizyczna - podwarstwy

- Warstwa fizyczna jest podzielona na dwie podwarstwy:
  - PLCP (*PhysicalLayer Convergence Protocol)* - prezentuje interfejs dla sterowników warstw wyższych:
    - rozpoczyna się **144-bitową** preambułą. Zawiera ona 128 bitów synchronizacji i 16-bitowe pole ze wzorcem: 1111001110100000. Ta sekwencja jest stosowana do wskazania początku każdej ramki i jest nazywana SFD *(Start Frame Delimiter).*
    - Następne 48 bitów stanowi nagłówek PLCP zawierający 4 pola: Sygnał, Usługa, Długość i HEC *(Header Error Check).*

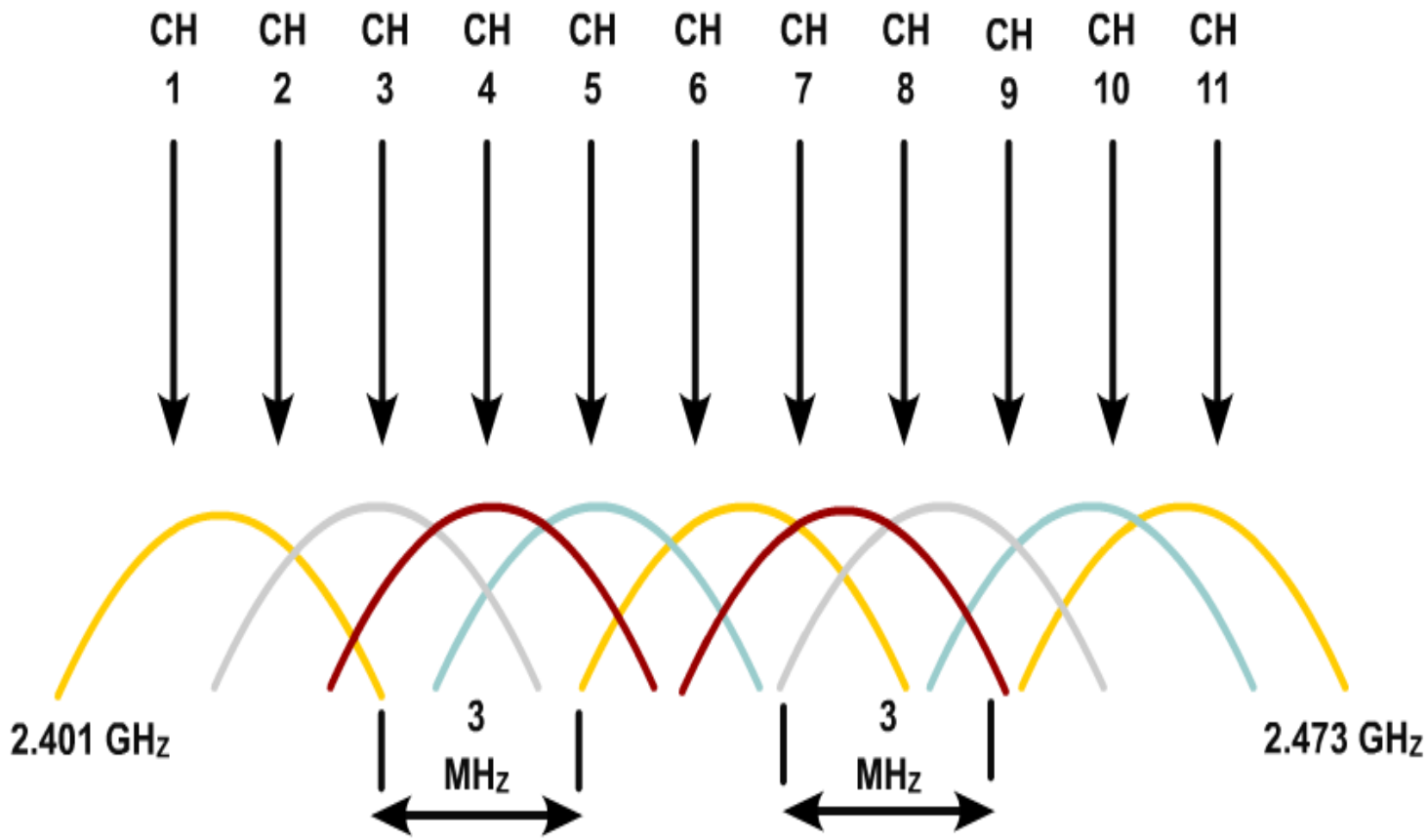
      Pole **Sygnał** wskazuje, z jaką przepływnością będzie przesyłany ładunek (1, 2, 5,5 i 11 Mb/s).
      Pole **Usługa** jest zarezerwowane.

      Pole **Długość** określa wielkość ładunku.
      Pole **HEC** jest 16-bitowym CRC.
  - PMD *(Physical Medium Dependent)* - nadzoruje bezprzewodowe kodowanie.

Warstwa łącza danych
Dostęp do medium

- CSMA/CA + Acknowledgement
- **Carrier Sense Multiple Access with Collision Avoidance**
- Działanie CSMA/CA:
  - Stacja nadawcza - nasłuch:
    - Wykrycie ciszy – nadawanie.
    - Kanał zajęty – czekanie:
      - Po wykryciu ciszy rozpoczyna się procedura jak po wykryciu kolizji.
- Uwaga: W przypadku dużego obciążenia kanału mogą wystąpić znaczne opóźnienia!

802.11b Channels



Sprzęt

- Punkt dostępowy (*Access Point*)
- Karty sieciowe do transmisji bezprzewodowej:
  - PCI
  - USB
  - PCMCIA

Bezpieczeństwo sieci WLAN

- Metody zabezpieczania punktów dostępowych:
  - SSID (*Service Set Identifier*)
  - Filtrowanie adresów MAC
  - Szyfrowanie transmisji

Bezpieczeństwo sieci WLAN

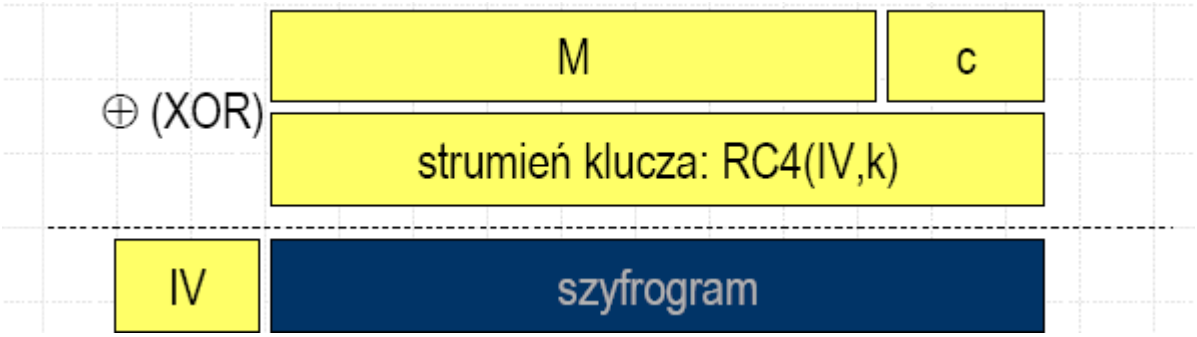
- 1997-2001: brak mechanizmów bezpieczeństwa
- 1997-2003: WEP (*Wired Equivalent Privacy*)
- 2003-2004: WPA (*Wi-Fi Protected Access WPA*)
- 2004-????: WPA2 / IEEE 802.11i

WEP – założenia projektowe

- **tajność klucza**
- **samosynchronizacja algorytmu** ze względu na charakter warstwy łącza danych
- **efektywność** w sprzęcie i oprogramowaniu
- **eksportowalność** algorytmu poza USA
- **opcjonalność** – implementacja i użycie WEP jako opcji

WEP – działanie

- bazuje na **RC4** z kluczem 64-bitowym (efektywnie 40-bitowym)
- użycie **RC4** z kluczem 128-bitowym (efektywnie 104-bitowym) jest rozwiązaniem niestandardowym
- nadawca i odbiorca dzielą tajny klucz – **k**
- wektor inicjujący – **IV**
- wiadomość – **M**
- przekształcenie **RC4(IV,k)** generujące strumień klucza
- suma kontrolna **c** realizowana za pomocą **CRC-32**
- **manualna dystrybucja klucza**



IEEE 802.11i

- W drafcie standardu 802.11i zdefiniowano dwa protokoły:
  - TKIP – kosmetyczna poprawka dla obecnych urządzeń;
  - CCMP – lepsze bezpieczeństwo w nowych urządzeniach.

TKIP

- TKIP (*Temporal Key Integrity Protocol*):
  - Może być zaimplementowany programowo
  - Wykorzystuje zaimplementowany sprzętowo WEP
  - Działa jako dodatkowy komponent
  - TKIP klucze:
    - 128-bitowy klucz szyfrujący (AP i klienci używają tego samego klucza)
    - 64-bitowy klucz do zapewnienia integralności (AP i klienci nie używają tego samego klucza)
  - Algorytm MICHAEL

CCMP

- CCMP (*Counter-Mode-CBC-MAC Protocol*):
  - Bazuje na AES (*Advanced Encryption Standard*) w trybie pracy CCM
  - AES wymaga wydajnego sprzętu zatem:
    - pojawią się nowe AP
    - pojawią się nowe urządzenia klienckie klasy hand-held
    - ale pozostaną PC
  - Niewielki związek z WEP

WPA (*Wi-Fi Protected Access*)

- WPA (2003r. – 2004r.):
  - Od 2003 obowiązkowy przy certyfikacji Wi-Fi
  - Podzbiór standardu 802.11i
    - 802.1X/EAP, TKIP
- WPA2 (2004r. – ????):
  - 2004 (testy współpracy 802.11i) – opcjonalny
  - 2005 (???) - obowiązkowy
  - W pełni zgodny z 802.11i
    - WPA + (Fast) Roaming + CCMP

WiMAX

- Rozwiązaniem problemu zbyt krótkiego zasięgu oraz problemy tzw. widoczności urządzeń nadawczo-odbiorczych ma byś wdrażany standard 802.16 nazywany WiMAX. Do jego podstawowych cech należy:
- duży zakres działania (tzn. w pasmach 11 – 66 GHz)
- duża efektywność w wykorzystaniu pasma
- zwiększona niezawodność transmisji
- zwiększona wydajność w niesprzyjających warunkach
- zwiększanie zasięgu kosztem pasma pozwala osiągnąć odległość ok. 45 km
- przepustowość maksymalna planowana ponad 70 Mb/s

Wykład 7

KONIEC