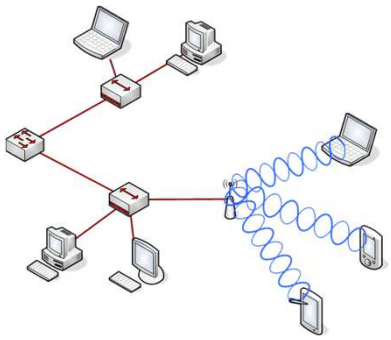
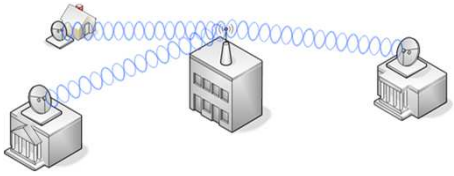
Standard 802.11 – Wi-Fi

Zastosowania LAN/MAN

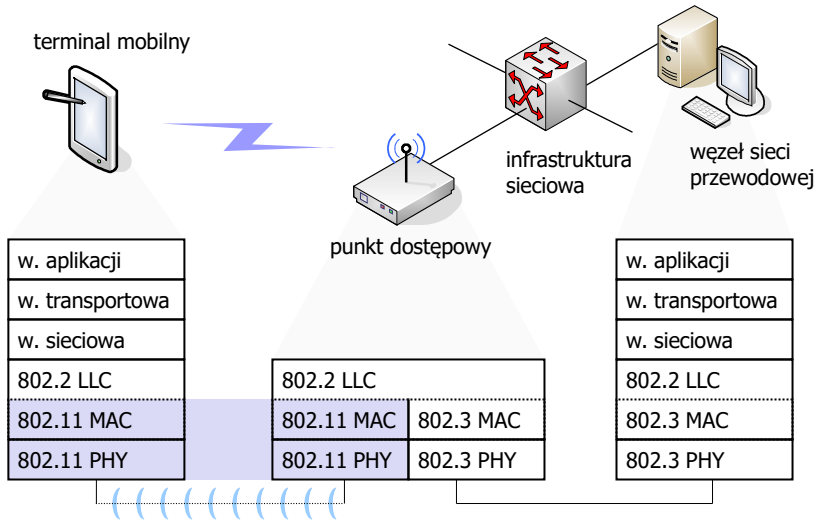
- Sieć Wi-Fi przypomina sieć komórkową.
- Najczęściej jest rozszerzeniem topologii sieci LAN.





- Wykorzystanie anten kierunkowych umożliwia zastosowanie w sieciach miejskich.

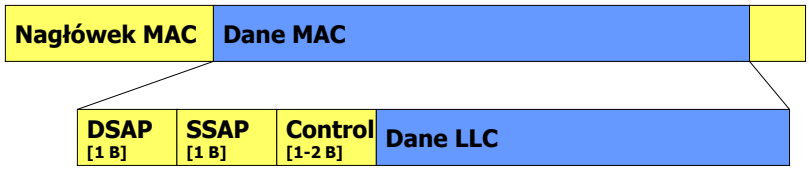
Zakres definicji w IEEE 802.11



Przypomnienie – IEEE 802.2

- Warstwa łącza danych dzieli się na dwie podwarstwy:
  - MAC (Medium Access Control) – warstwę dostępu do medium, np. 802.3 (Ethernet), 802.5 (TokenRing),
  - LLC (Logical Link Control) – niezależną od technologii.
- LLC określa własne PDU
- Dzięki LLC możliwe jest łączenie sieci o różnych standardach MAC urządzeniem pracującym w drugiej warstwie modelu OSI/ISO – *bridging*.

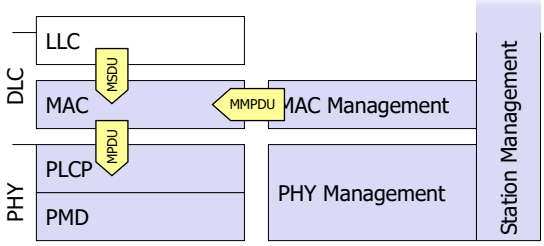
Przypomnienie – IEEE 802.2



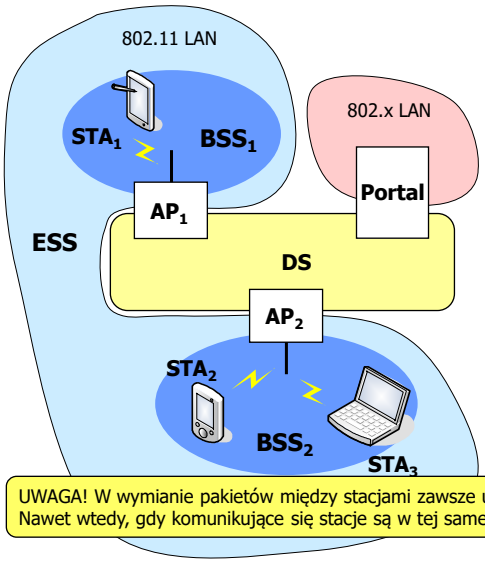
- DSAP (*Destination Service Access Point*) – kod protokołu warstwy wyższej, do którego mają trafić dane
- SSAP (*Source Service Access Point*) – kod protokołu warstwy wyższej, z którego pochodzą dane
- Control – np. sterowanie przepływem, numerowanie pakietów.
- Dane (lub wypełnienie), wielkość zapewniająca minimalną długość całego pola danych

802.11 – warstwy i funkcje

- MAC *Medium Access Control*
  - sposób dostępu do medium, fragmentacja, enkrypcja.
- MAC *Management*
  - synchronizacja, *roaming*, MIB, sterowanie mocą, tworzenie komórek BSS.
- *Station Management*
  - koordynacja wszystkich funkcji zarządzania.
- PLCP *Physical Layer Convergence Protocol*
  - mapowanie ramek MPDU na ramki warstwy fizycznej,
  - wykrywanie zajętości kanału.
- PMD *Physical Medium Dependent*
  - definiuje charakterystykę medium i metody transmisji i odbioru danych
- PHY *Management*
  - channel selection, MIB

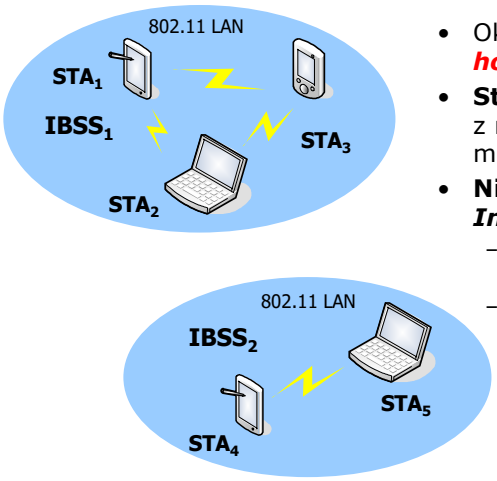


Architektura (1) - Extended Service Set



- Określana jako tryb ***infrastructure***,
- **Stacja** (**STA**) – urządzenie z możliwością dostępu do medium bezprzewodowego
- **Komórka *Basic Service Set*** (**BSS**) – zbiór skoordynowanych stacji (np. pracujących na wybranym kanale)
- **Komórka *Extended Service Set*** (**ESS**) – zbiór jednej lub więcej komórek BSS wraz z dołączonymi sieciami LAN
- **Punkt dostępowy** (**AP**) – stacja umożliwiająca dostęp do systemu dystrybucji
- **Portal** – mostek do innych niż 802.11 sieci LAN (np. przewodowych)
- **ystrybucji** (**DS**) – system ka komórek BSS oraz sieci LAN w celu utworzenia komórki ESS.

Architektura (2) - Independent Basic Service Set



- Określana jako tryb ***ad-hoc***.
- **Stacja** (**STA**) – urządzenie z możliwością dostępu do medium bezprzewodowego.
- **Niezależna komórka BSS *Independent BSS*** (**IBSS**)
  - komunikacja odbywa się w ograniczonym zasięgu,
  - każda stacja musi widzieć się z pozostałymi.

IEEE 802.11. Nie tylko a/b/g/n/ad

- 802.11 – Specyfikacja standardu WLAN – warstwa fizyczna: 2,4 GHz DSSS, FHSS oraz IR.
- 802.11a (**Wi-Fi 2**) – Warstwa fizyczna dla 5,2 GHz, OFDM.
- 802.11b (**Wi-Fi 1**) – Warstwa fizyczna dla 2,4 GHz, DSSS + CCK.
- 802.11c – Usprawnienia w warstwie MAC dla bridge'ów.
- 802.11d – Regulacja zakresów częstotliwości dla większej liczby krajów.
- 802.11e – Rozszerzenie warstwy MAC o sterowania parametrami QoS.
- 802.11F – Inter-Access Point Protocol – określa wymagania dla AP i pozwala na tworzenie sieci z punktów dostępowych różnych producentów.
- 802.11g (**Wi-Fi 3**) – Usprawnienia wersji **b** w warstwie fiz., przepływność > 20 Mb/s.
- 802.11h – Rozszerzenie wersji **a** o zarządzanie mocą i dynamiczny wybór kanału.
- 802.11i – Rozszerzenia warstwy MAC o mechanizmy bezpieczeństwa.
- 802.11n (**Wi-Fi 4**) – Przepływności do 200 Mb/s, technologia MIMO (09.2009)
- 802.11ac (**Wi-Fi 5**) – Warstwa fizyczna 5 GHz, przepływność > 500 Mb/s (01.2014)
- 802.11ad (WiGig) – Warstwa fizyczna 60 GHz, przepływność do 7 Gbit/s
- 802.11ax (**Wi-Fi 6**) – w trakcie specyfikacji, przepływność ok. 10 Gbit/s
- Ponadto 802.11{j|k|m|p|r|s|T|u|v}

Wi-Fi 0/1/2/3/4/5/6/7

Wi-Fi Generations

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)
Wi-Fi 7	802.11be	40000	TBA	2.4/5/6
Wi-Fi 6E	802.11ax	600 to 9608	2020	2.4/5/6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	433 to 6933	2014	5
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5
(Wi-Fi 3)	802.11g	6 to 54	2003	2.4
(Wi-Fi 2)	802.11a	6 to 54	1999	5
(Wi-Fi 1)	802.11b	1 to 11	1999	2.4
(Wi-Fi 0)	802.11	1 to 2	1997	2.4

Warstwa fizyczna – 802.11

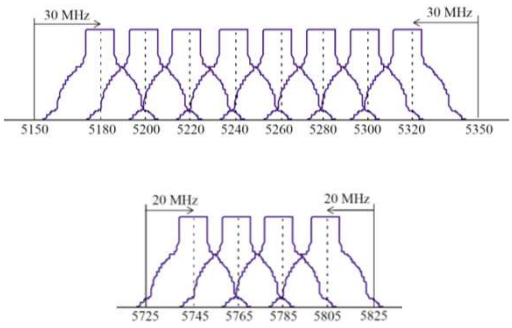
- 802.11
  - przepływności 1 lub 2 Mb/s,
  - pasmo 2,4-2,4835 GHz,
  - technika transmisji: DSSS, FHSS, IR-PPM.
- 802.11b
  - przepływności do 11 Mb/s
  - pasmo 2,4-2,4835 GHz,
  - technika transmisji: DSSS + CCK

- efektywne przepustowości uzyskiwane w warstwie aplikacji to co najwyżej 50% podanej przepustowości,
- zależą m.in. od zakłóceń, interferencji, odległości od stacji.

- 802.11a
  - przepływności do 54 Mb/s
  - pasmo 5,2-5,8 GHz
  - technika transmisji: OFDM.
- 802.11g
  - przepływności do 54 Mb/s
  - pasmo 2,4-2,4835 GHz,
  - technika transmisji: ERP-DSSS, ERP-OFDM
- 802.11n
  - przepływności do 200 Mb/s
  - pasmo 2,4-2,4835 GHz,
  - technika transmisji: MIMO-OFDM.
- 802.11ac
  - przepływności do 1300Mb/s
  - pasmo 5 GHz (ISM),
  - technika transmisji: MIMO, MU-MIMO, OFDM.

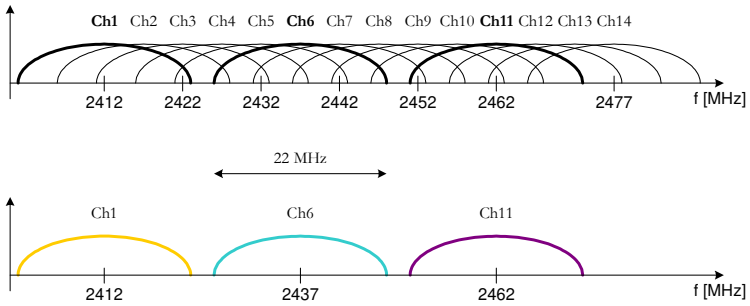
Warstwa fizyczna 802.11a - OFDM

- 12 niepokrywających się kanałów o szerokości 18 MHz odległych od siebie o 20 MHz
- różne sposoby modulacji dla różnych przepływności:
  - 6, 9 Mb/s BPSK
  - 12, 18 Mb/s QPSK
  - 24, 36 Mb/s 16-QAM
  - 48, 54 Mb/s 64-QAM



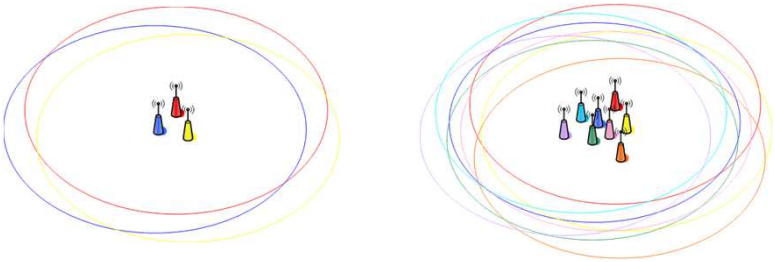
Warstwa fizyczna 802.11b - DSSS

- 14 kanałów o szerokości 22 MHz odległych od siebie o 5 MHz

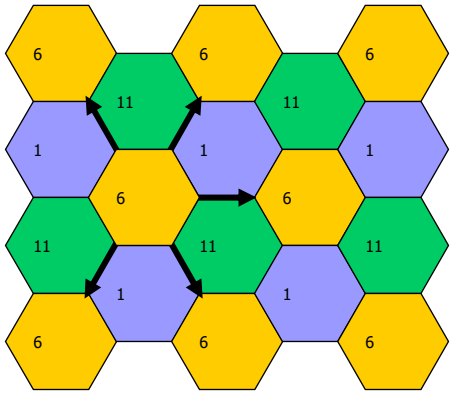


Skalowalność w ESS

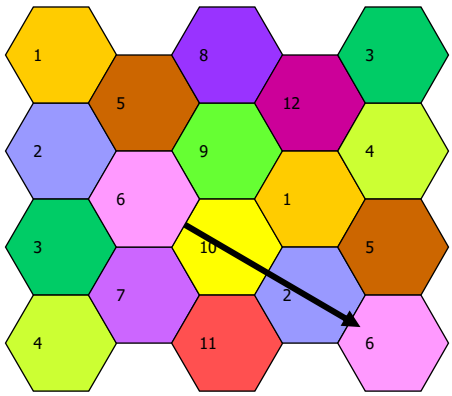
- Niepokrywające się kanały umożliwiają zwiększenie pojemności sieci
  - 3 * 11 = 33 Mb/s dla 802.11b
  - 3 * 54 = 162 Mb/s dla 802.11g
  - 12 * 54 = 648 Mb/s dla 802.11a



Pokrycie dla zakresu 2,4-2,48 GHz



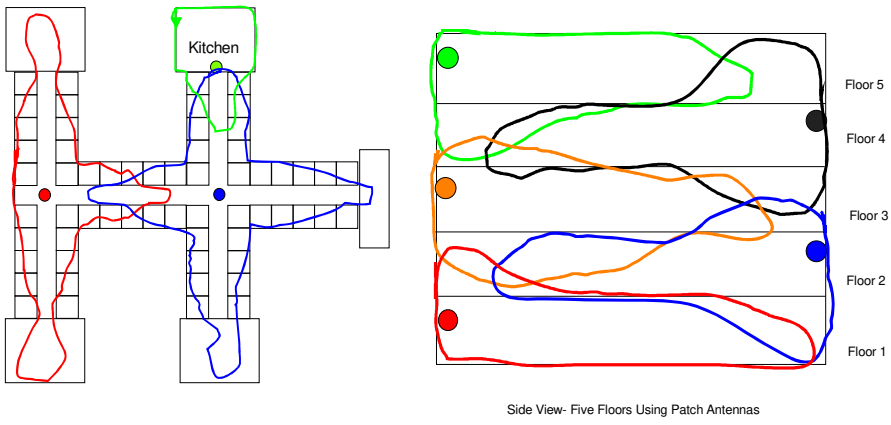
Pokrycie dla zakresu 5-5,8 GHz



Wdrożenie

- Zapewnienie odpowiedniego pokrycia przestrzeni
  - dopasowanie rozwiązania do istniejących warunków,
  - przeprowadzenie pomiarów zasięgu.
- Zapewnienie skalowalności rozwiązania
  - możliwości rozszerzenia zasięgu infrastruktury,
  - możliwości zwiększenia pojemności.
- Niezawodność
  - dostarczenie urządzeń zapasowych.
- Zabezpieczenie przed niepowołanym dostępem.

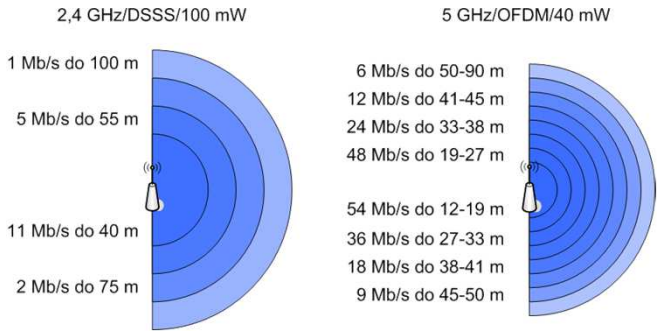
Przykład pokrycia – biurowiec



Side View- Five Floors Using Patch Antennas

Przepustowość w funkcji odległości

- Maksymalny zasięg:
  - 40 km @ 2 Mb/s,
  - 18 km @ 11 Mb/s,

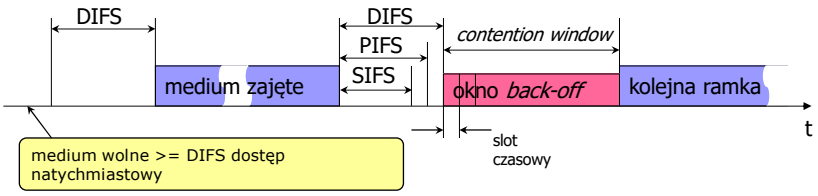


Metody dostępu do medium

- *Distributed Coordination Function* (DCF)
  - [wymagana] realizuje metodę dotępu CSMA/CA (*carrier sense multiple access with collision avoidance*),
  - wykorzystywana obu trybach *infrastructure* i *ad-hoc.*
  - do transmisji punkt-punkt może stosować mechanizm wykrywania zajętości medium: RTS/CTS (*request to send*/*clear to send*).
- *Point Coordination Function* (PCF)
  - [opcjonalna] realizuje metodę CF (*contention free*),
  - ma priorytet nad DCF i dostarcza ramki bez rywalizacji,
  - wymaga centralnego sterowania (-> koordynatory punktowe PC - *Point Coorinators*)
  - wykorzystywana tylko w trybie *infrastructure*,
  - rzadko wykorzystywana ze względu na zwiększenie obciążenia w BSS.

Warstwa MAC

- Priorytety dostępu do medium
  - określone przez długość przestrzeni międzyramkowej tzw. IFS,
  - nie gwarantują dostępu,
  - cztery długości:
    - SIFS (*short inferframe space*),
    - PIFS (PCF *interframe space*),
    - DIFS (DCF *interframe space*),
    - EIFS (*extended interframe space*).



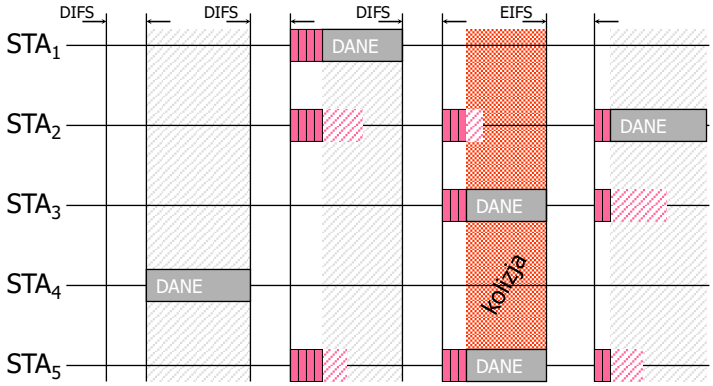
Dostęp DCF

- Podstawowy sposób dostępu do medium.
- Redukuje prawdopodobieństwo wystąpienia kolizji.
- Każda poprawnie odebrana ramka jest potwierdzana (pozytywne potwierdzenia).
- Dlaczego CSMA/**CA** a nie CSMA/**CD**?

Algorytm:

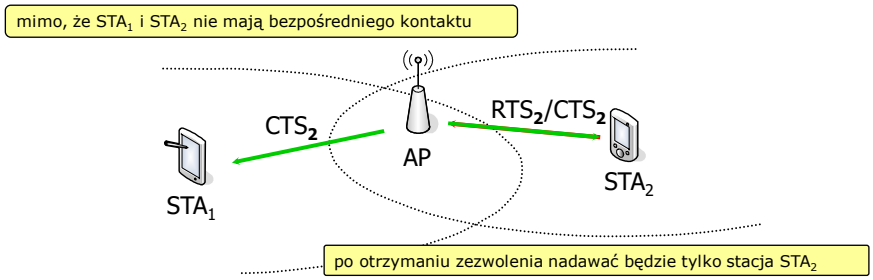
1. Stacja zaczyna wykrywać zajętość medium.
2. Jeśli medium jest zajęte to stacja oczekuje na jego zwolnienie.
3. Jeśli medium jest wolne to stacja oczekuje czas DIFS.
4. Jeśli w tym czasie medium zostanie zajęte to powrót do pkt. 2.
5. Jeśli w tym czasie medium pozostaje wolne to stacja generuje losowe opóźnienie tzw. *backoff interval*
6. Jeśli w czasie *backoff* medium zostanie zajęte stacja wstrzymuje *backoff* i czeka DIFS na zwolnienie medium
7. Jeśli w czasie *backoff* medium pozostaje wolne to stacja może transmitować.

Dostęp DCF



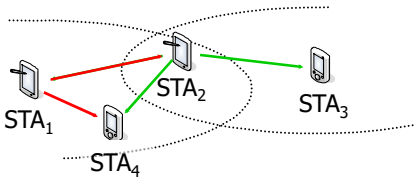
DCF + RTS/CTS

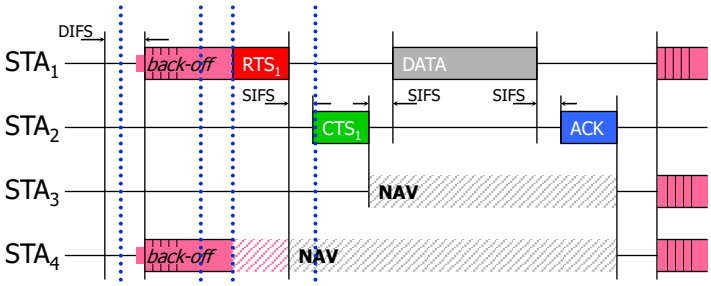
- *Request to Send/Clear to Send*
  - alokacja zajętości łącza na określony czas,
  - zmniejsza problemy z ekspozycją węzłów,
  - jest podstawą wirtualnego wykrywania zajętości medium.



Wykrywanie zajętości medium Carrier Sense

- Dwa rodzaje:
  - w warstwie fizycznej
  - w warstwie MAC – za pomocą mechanizmu RTS/CTS





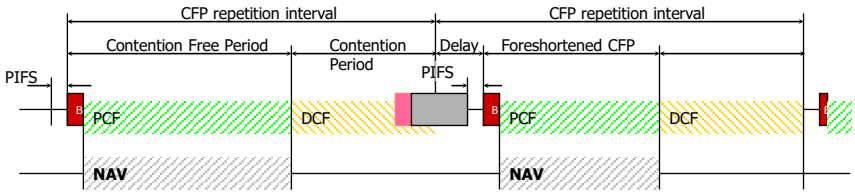
Dostęp PCF

- Gwarantuje bezsporny (ang. *contention-free*) dostęp do medium.
- Kluczowym elementem jest punkt koordynacji (ang. *Point Coordination*) implementowany przez AP

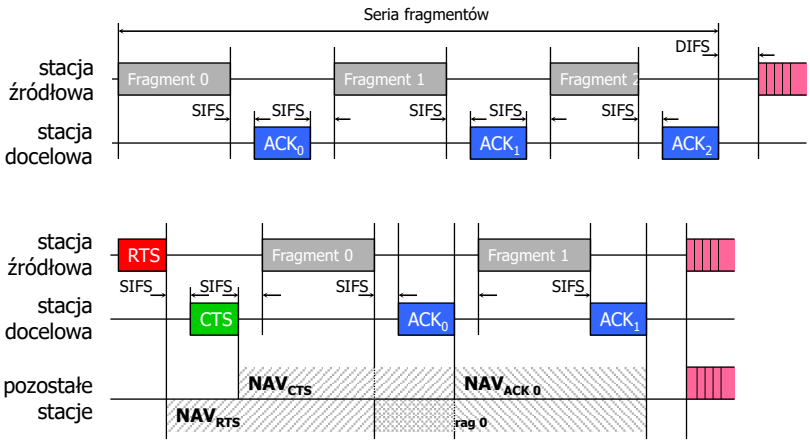
  ⇒ PCF przeznaczony jest tylko dla trybu *infrastructure*.
- Wykorzystuje priorytet (tj. krótszy IFS niż DCF : PIFS < DIFS) w dostępie do łącza.
- Współpracuje ze stacjami w trybie DCF.

Dostęp PCF

- Podział na dwa okresy (sposoby dostępu):
  - bez kolizyjny – *CFP*,
  - kolizyjny (CSMA/CA) – *CP*.



Fragmentacja



Tworzenie komórek BSS

- Komórka – zbiór skoordynowanych stacji z określonymi parametrami:
  - identyfikator SSID, BSSID,
  - wspólny zegar,
  - wybrany kanał (dla DSSS, OFDM)/sekwencja skakania (dla FHSS),
  - inne np. *aBeaconPeriod*.
- Każda stacja może utworzyć własną komórkę BSS lub IBSS.
- Funkcja realizowana przez operację podwarstwy zarządzania MAC *Management*.

Jak stacja dołącza do komórki BSS?

1. Wykrycie dostępnych komórek BSS
   - aktywne, pasywne,
   - *infrastructure* BSS, *independent* BSS.
2. Synchronizacja z komórką BSS.
3. Uwierzytelnianie:
   - w systemie otwartym (ang. *open system authentication*),
   - z kluczem dzielonym (ang. *shared key authentication*).
4. Asocjacja z punktem dostępowym
   - oczywiście może mieć miejsce tylko w przypadku komórki typu *infrastructure*.

Wykrywanie dostępnych komórek BSS

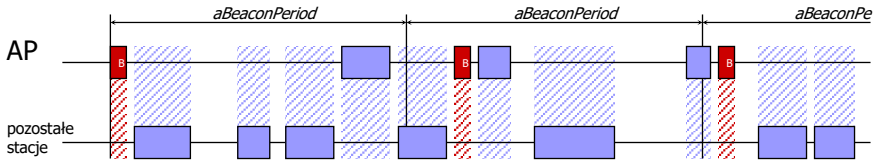
- Pasywne:
  - stacja nasłuchuje na ramki *beacon*,
  - z zestawu ramek wybierane są następnie te o zadanej wartości identyfikatora komórki SSID,
  - w ramkach *beacon* zawarta jest także m.in. informacja o typie komórki: *infrastructure*, *ad-hoc*,
- Aktywne:
  - dla każdego/określonego kanału stacja transmituje ramki *Probe* z żądanym SSID oczekując na odpowiedź *ProbeResponse*.
  - może też transmitować ramki *Probe* z SSID typu *broadcast* szukając dowolnej komórki.
- Po wykryciu dostępnych komórek stacja ma potrzebne informacje, żeby móc dołączyć do komórki.

Synchronizacja z komórką BSS

- Wszystkie stacje tworzące BSS muszą mieć zsynchronizowany zegar
  - szczególnie istotne dla FHSS – określenie czasu *aCurrentDwellTime*.
- Realizowane przez funkcję TSF (ang. *time synchronization function*)
  - w trybie *infrastructure* funkcja realizowana przez AP,
  - w trybie *ad-hoc* funkcja realizowana przez wszystkich uczestników w sposób rozproszony.
  - wartość znacznika przekazywana w ramkach *beacon* i *ProbeResponse*.
- Zegar TSF ma częstotliwość 1 MHz i implementowany jest na 64-bitowym znaczniku

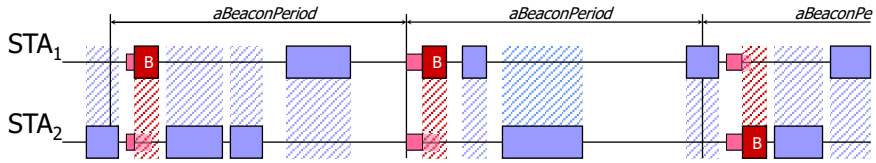
Synchronizacja w trybie *infrastructure*

- AP generuje okresowo – co *aBeaconPeriod* – ramki *beacon* zawierające kopię swojego TSF.
- Każda stacja w komórce BSS obsługiwanej przez dany AP ustawia swój zegar zgodnie z wartością TSF zawartą w ramce *beacon*.



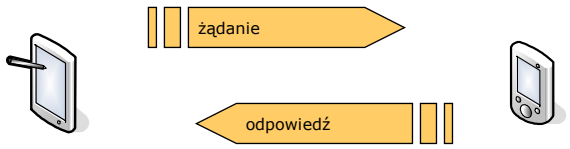
Synchronizacja w trybie *ad-hoc*

- Każda może wygenerować ramkę *beacon* z aktualnym znacznikiem TSF.
- Każda stacja odbierająca ramkę *beacon* ustawia swój zegar zgodnie ze znacznikiem TSF zawartym odebranej ramce *beacon*, jeśli jest on późniejszy niż jej aktualny zegar.



Uwierzytelnianie w systemie otwartym

- Najprostszy możliwy sposób uwierzytelniania.
- Stacja, która żąda uwierzytelnienia zostaje uwierzytelniona, jeśli tylko stacja uwierzytelniająca wyraża taką chęć.



- Efektem jest wzajemne uwierzytelnienie.
- W tym sposobie uwierzytelniania można wykorzystać WEP do szyfrowania danych (nie nagłówka).

Uwierzytelnianie z dzielonym kluczem

- Oparte o współdzielony klucz, którego dostarczenie powinno nastąpić drogą inną niż 802.11.
  - wykorzystuje 128-bitowe pole *challenge*, które jest następnie szyfrowane przy użyciu mechanizmu WEP

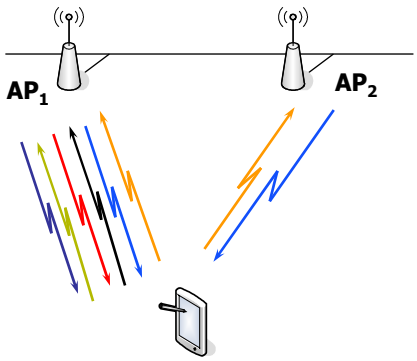
- Efektem jest jednostronne uwierzytelnienie
- Procedura podatna jest na atak *man-in-the-middle*.

(Re)asocjacja stacji

- Dialog stacji z punktem dostępowym, dzięki któremu możliwe są:
  - wymiana danych z punktem dostępowym,
  - *roaming* węzła pomiędzy poszczególnymi komórkami BSS w komórce ESS.
- (Re)asocjacja odbywa się na wyraźne żądanie warstw wyższych (w tym np. użytkownika).
- Może nastąpić dopiero po uwierzytelnieniu.
- (Re)asocjacja wiąże się z nadaniem przez punkt dostępowy identyfikatora *association ID* (AID).
- Odpowiedź na żądanie (re)asocjacji powinna zostać potwierdzona przez stację.
- Punkt dostępowy informuje system DS o (re)asocjacji stacji
  - na komunikat o (re)asocjacji poprzedni punkt dostępowy może zwolnić zasoby przydzielone dla danej stacji.

▪ 802.11F – IAPP *Inter-Access Point Protocol* – współpraca punktów dostępowych urządzeń różnych producentów.

Proces dołączania do komórki AP



Klient wysyła próbnik (ramka *Probe*)

AP odpowiada (ramka *ProbeResponse*)

Klient ocenia otrzymane odpowiedzi, wybiera najlepszą i dokonuje synchronizacji

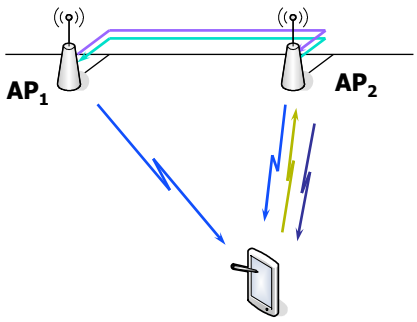
Klient wysyła żądanie uwierzytelnienia do wybranego AP.

AP potwierdza uwierzytelnienie.

Klient wysyła żądanie dołączenia do komórki AP.

AP potwierdza dołączenie i nadaje klientowi identyfikator AID.

Roaming pomiędzy komórkami



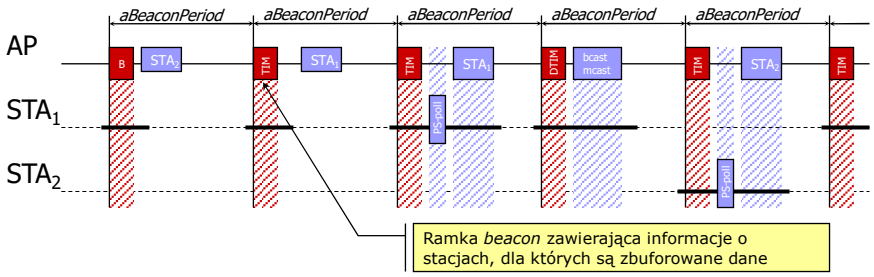
- Klient słucha ramek *beacon* i ocenia, kiedy dokonać *handoveru*. Klient ocenia otrzymane odpowiedzi, wybiera najlepszą i dokonuje synchronizacji.
- Klient wysyła żądanie dołączenia do komórki AP.
- AP potwierdza dołączenie i nadaje klientowi identyfikator AID.
- AP_2 informuje AP_1 o reasocjacji
- AP_1 wyrejestrowuje klienta i przekazuje AP_2 zbuforowane ramki.

Zarządzanie energią

- Stacja może znajdować się w jednym z dwóch stanów:
  - *awake*: stacja jest w pełni funkcjonalna, może odbierać i nadawać dane,
  - *doze*: stacja jest w trybie zmniejszonego poboru mocy i nie odbiera ani nie nadaje żadnych ramek.
- Stacja pracuje w jednym z dwóch trybów:
  - tryb *Active Mode* – AM: stacja jest w stanie *awake*,
  - tryb *Power Save* – PS: większość czasu stacja jest w stanie *doze*, ale przechodzi w stan *awake*:
    - na czas odbioru wybranych ramek *beacon*,
    - podczas CFP (por. PCF) jeśli jest *CF-Pollable*,
    - wymiany danych z AP na wyraźne żądanie – *PS-poll*.

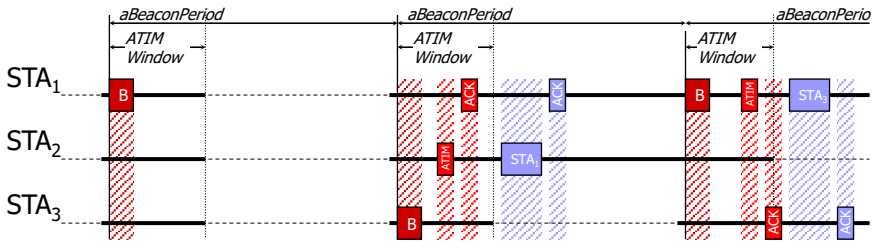
Zarządzanie energią tryb infrastructure

- Stacja przekazuje do AP informacje o zmianie trybu pracy z: PS ↔ AM.
- Jeśli stacja STA pracuje w trybie oszczędzania energii AP buforuje ramki skierowane do STA.
- Informacja o stacjach, dla których zbuforowano ramki przesyłana jest w ramkach *beacon* jako tzw. *traffic indication map* (TIM) lub DTIM.
- Po wykryciu danych stacja wysyła ramkę PS-Poll.



Zarządzanie energią tryb ad-hoc

- Stacje są zsynchronizowane i równocześnie przechodzą w stan *awake* w określonych odstępach czasu.
- Każda stacja buforuje ramki przeznaczone do stacji w trybie PS.
- Informacja o zbuforowanych danych przesyłana w specjalnej ramce ATIM adresowanej do odbiorcy danych
  - stacja docelowa musi potwierdzić otrzymanie ATIM.



Bezpieczeństwo

- W sieciach bezprzewodowych szczególnie istotne
  - nie wystarczą drzwi, kłódka, ani strażnik.
- Możliwości:
  - bezpieczeństwo oparte o SSID – niebezpieczeństwo,
  - bezpieczeństwo oparte o adresy MAC – filtrowanie,
  - bezpieczeństwo oparte o WEP (*Wired Equivalent Privacy*),
  - WPA (*WiFi Protected Access*)
  - standard 802.11i – WPA2,
  - sieci prywatne wirtualnie VPN.

Bezpieczeństwo – WEP

- Standard definiuje wykorzystanie kluczy 40 bitowych
  - większość producentów używa kluczy >= 128b,
  - szyfrowanie *Rivest Cipher 4* (RC4).
- Klucz musi być współdzielony pomiędzy obiema komunikującymi się stronami
  - w standardzie nie rozwiązany jest problem dystrybucji klucza,
  - wykorzystuje się dwa sposoby:
    - wszystkie stacje współdzielą do czterech różnych kluczy – łatwiejszy wyciek,
    - pomiędzy każdymi dwoma komunikującymi się stacjami współdzielone inne klucze – trudniejsza dystrybucja.

Bezpieczeństwo – WEP

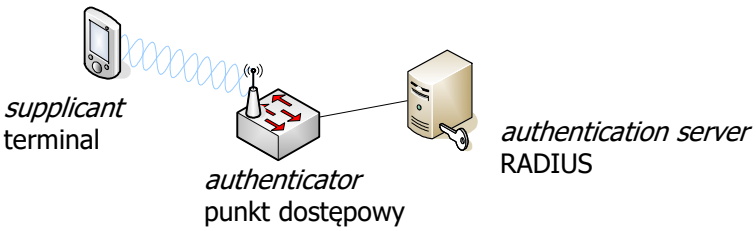
- Klucz nie identyfikuje użytkownika, tylko urządzenie
  - kłopoty w przypadku utraty (klucz staje się dostępny).
- Poziom bezpieczeństwa zapewniony przez WEP okazuje się niewystarczający
  - zbyt słaba ochrona poufności danych,
  - zbyt słaba ochrona integralności danych.

802.11i

- Inaczej nazywane WPA2 (*Wi-Fi Protected Access*)
- Wykorzystanie standardu 802.1X w sieciach bezprzewodowych
  - 802.11 dostarcza funkcji zabezpieczania danych,
  - 802.1X dostarcza mechanizmów uwierzytelniania
  - oba współpracują w zarządzaniu kluczami.
- Wykorzystanie TKIP *temporal key integrity program*.
  - zmiana klucza co 10 000 pakietów.
- Obecnie wykorzystuje się AES *Advanced Encryption Standard* jako zamiennika 3DES.

802.1x

- Uwierzytelnia użytkownika a nie urządzenie.
- Uwierzytelnienie jest wzajemne.
- Wykorzystuje RADIUSa.
- Umożliwia wykorzystanie różnych sposobów uwierzytelniania:
  - LEAP, EAP-TLS, PEAP, EAP-MD5 i inne.



KONIEC