WiFi

(Wireless Fidelity)

WiFi czyli standard **802.11** obejmuje transmisję bezprzewodową z wykorzystaniem częstotliwości od **2400** do **2485** MHz (w Polsce tylko do **2483,5** MHz) oraz **5000** MHz.

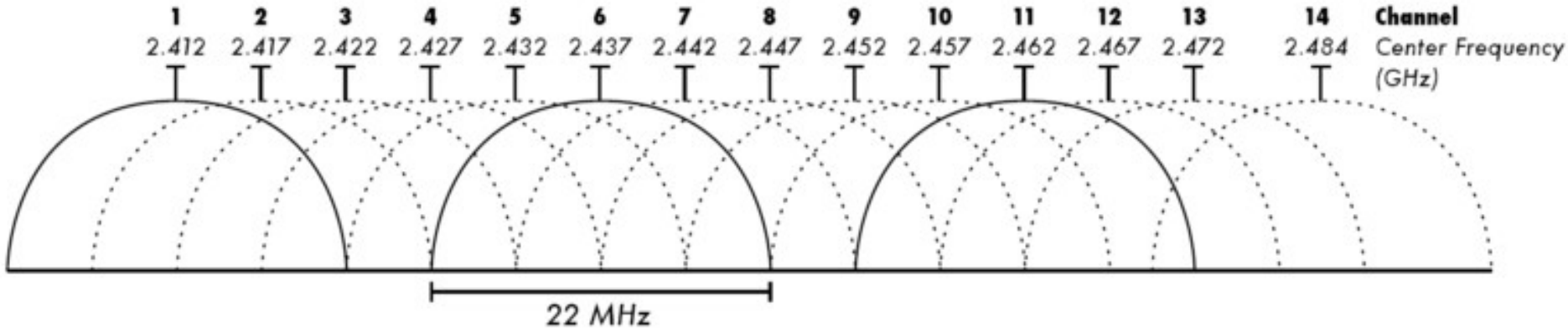
Aneksy:

Oryginalny	- częstotliwości: **2.4** GHz, szybkości: **1, 2** Mb/s
802.11b	- częstotliwości: **2.4** GHz, szybkości: **1, 2, 5.5, 11** Mb/s
802.11a	- częstotliwości: **5** GHz, szybkości: **6, 9, 12, 18, 24, 36, 48, 54** Mb/s
802.11h	- częstotliwości: **5** GHz, szybkości: **6, 9, 12, 18, 24, 36, 48, 54** Mb/s (TPC, Europa)
802.11g	- częstotliwości: **2.4** GHz, szybkości: **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54** Mb/s
802.11n	- częstotliwości: **2.4, 5** GHz, szybkości: **100, 300, 600** Mb/s

Uwaga!

W paśmie 2.4 GHz pracują również inne urządzenia bezprzewodowe – np. Bluetooth oraz...
...kuchenki mikrofalowe!

W standardach b oraz g mamy do dyspozycji 14 kanałów (z czego 13 w Europie). Częstotliwości poszczególnych kanałów zachodzą na siebie, więc odległości pomiędzy dwiema sieciami bezprzewodowymi powinny wynosić minimum trzy kanały – wtedy mamy do czynienia z jeszcze akceptowalnym poziomem zakłóceń. **Żeby częstotliwości się nie pokrywały możemy użyć tylko kanału 1, 6 oraz 11.**



W standardach 802.11a/h/n mamy do dyspozycji dużo więcej kanałów – dla Europy mamy aż 19 nie zachodzących na siebie kanałów.

Rekordowe zasięgi WiFi punkt-punkt:

382km – świat
168km – Polska (http://wifirekord.pl)

Metody na zwiększenie zasięgu sieci bezprzewodowej to stosowanie repeaterów lub WDS (Wireless Distribution System). W trybie WDS – czyli bezprzewodowego mostu urządzenia dostępowe (AP) przekazują sobie wzajemnie pakiety od stacji.

Metody zapobiegania kolizjom w sieciach bezprzewodowych:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – pomiędzy przesłanym pakietem stacja odczekuje czas **IFS** (Interframe Space) i słucha czy żadna inna stacja nie nadaje.

DCF (Distributed Coordination Function) jest to podstawowa funkcja dostępu do nośnika, która używa **DIFS** (Distributed Interframe Space). Czas DIFS jest wspólny dla wszystkich stacji.

Im krótszy czas IFS tym większy priorytet – w standardzie zdefiniowane są cztery (ale to w końcu tylko standard... ;))

W celu zapobiegania utracie danych jeżeli kolizja jednak nastąpi stacje potwierdzają otrzymanie ramki za pomocą ACK po czasie **SIFS** (Short Interframe SPACE), który jest krótszy niż DIFS, dzięki czemu ma wyższy priorytet.

„Problem ukrytej stacji” – zdarzają się sytuacje w których stacja do której nadajemy komunikuje się również ze stacją której sygnału nie można wykryć. W takiej sytuacji nie jest możliwe zapobieganie kolizjom poprzez nasłuch nośnika.

Z pomocą przychodzi mechanizm **RTS-CTS** (Request To Send – Clear To Send).

Stacja która chce wysłać pakiet wysyła najpierw RTS, jeśli odbiornik jest akurat wolny to odsyła CTS – zgodę na wysyłkę. CTS jest wysyłany z po czasie SIFS, dzięki czemu ma wyższy priorytet niż inny ruch w sieci.

RTS zawiera informację o czasie transmisji na tej podstawie inne stacje które go „złapią” mogą ustawić sobie licznik NAV (Network Allocation Vector) który dodatkowo zapobiega powstaniu kolizji.

Mechanizm ten ma jedną wadę – generuje bardzo duży ruch w sieci i dla małych pakietów jest on po prostu nieopłacalny. Wprowadzono więc parametr **RTS Treshold,** który określa wielkość pakietu po jakiej jest uruchamiany RTS-CTS.

Uwaga! Pakiety RTS/CTS można wysyłać nawet bez uwierzytelnienia!

Jeżeli stacja będzie wysyłała dużą ilość pakietów CTS (szczelina między pakietami będzie zawsze krótsza niż DIFS, gdyż CTS jest wysyłany z czasem SIFS) żadna inna stacja nie będzie mogła nadawać. (**CTS Flood**)

Metody zabezpieczeń sieci bezprzewodowych:

ukrywanie SSID (Service Set Identifier)– podstawowe zabezpieczenie, które powoduje, że AP nie rozgłasza nazwy sieci bezprzewodowej. Bardzo proste do obejścia, np.. poprzez pasywny nasłuch. W połączaniu z długimi odstępami wysyłania pakietów **BEACON** (informujących o takich parametrach jak np. prędkość, ssid) – Beacon Interval pozwala na ukrycie sieci na liście dostępnych.

Filtrowanie po adresach MAC – bardzo proste zabezpieczenie polegające na konfiguracji listy adresów fizycznych kart sieciowej stacji uprawnionych do podłączenia.

WEP (Wired Equivalent Privacy)- szyfrowanie oparte o algorytm **RC4** klucz od 64 do 128 bit z czego 24 przypada na **IV** (wektor inicjalizujący).

Łamanie WEP polega na wyłapaniu odpowiedniej ilości ramek i sprawdzaniu czy gdzieś nie wystąpiło powtórzenie klucza szyfrującego – co zdarza się tu bardzo często. Prawdopodobieństwo wystąpienia klucza ponownie wynosi 50% po przesłaniu ok. 4800 ramek.

Złamanie WEP 104 trwa poniżej minuty! (http://eprint.iacr.org/2007/120.pdf)

Inne proste ataki to wysyłanie dużej ilości ramek autentykacji lub/i deautentykacji.

WPA (WiFi Protected Access) – TKIP (Temporal Key Integrity Protocol) czyli protokół używany w WPA nadal korzysta z algorytmu RC4, wprowadzono tylko hashowanie wektora inicjalizującego (IV) oraz wymuszono zmianę klucza co określoną liczbę pakietów.

Metody łamania opisane przez Martina Beck i Erika Tews pozwalają złamać WPA podobną techniką co WEP (http://exp.syue.com/papers/250)

Dwie wersje – PSK (Pre Shared Key) oraz Enterprise – RADIUS.

WPA2 – standard 802.11i wprowadza algorytm **AES** zamiast RC4 (klucze są 128 bit-owe), posiada sprzętową akceleracje, automatycznie dystrybuuje klucze (802.1x).

Również w wersji PSK oraz Enterprise.

RADIUS

Usługa RADIUS to protokół klient-serwer używany do autoryzacji, uwierzytelniania i zarządzania kontami (AAA).

Model AAA zawiera trzy fazy:

- **uwierzytelniania**: weryfikacja nazwy użytkownika i hasła w oparciu o bazę danych. Po sprawdzeniu poświadczeń rozpoczyna się proces autoryzacji.

- **autoryzacji**: sprawdzenie, czy na podstawie żądania uzyskany zostanie dostęp do zasobu. Np. czy dana osoba ma prawo łączyć się z internetem po godzinie 22.

- **zarządzania:** zbieranie informacji dotyczących użytkowania zasobu, w celach analizy trendów, audytu, rozliczania czasu sesji lub naliczania kosztów połączenia (HOTSPOT!).