Standardy sieci Wi-Fi

802.11

Pierwsza możliwość łączenia komputerów w sieć bezprzewodową pojawiła się w 1997 roku jako standard IEEE802.11. Użytkownik mógł liczyć na prędkość przesyłania danych na poziomie 1 lub 2 Mb/s. Jako medium wykorzystywano promieniowanie podczerwone oraz fale radiowe 2,4 GHz.

We wrześniu 1999 roku ogłoszono dwa nowe warianty IEEE802.11. Pierwszy oznaczony jako 802.11a wykorzystywał fale radiowe o częstotliwości 5 GHz i oferował przepustowość do 54 Mb/s. Drugi, 802.11b, działał w paśmie 2,4 GHz i pozwalał na przesyłanie danych z prędkością do 11 Mb/s. Obecnie standard 802.11b nie jest już od dawna używany, natomiast 802.11a sporadycznie.

802.11g

Na kolejną wersję oznaczoną jako 802.11g użytkownicy musieli poczekać do czerwca 2003 roku. Wtedy to właśnie oficjalnie zatwierdzono tę najbardziej popularną do tej pory wersję standardu Wi-Fi. Urządzenia obsługujące 802.11g działały w paśmie 2,4 GHz i były kompatybilne wstecz z 802.11b, przy czym umożliwiały osiągnięcie przepustowości maksymalnie 54 Mb/s.

802.11n

Kolejną wersją był 802.11n, jednak nim standard ten został oficjalnie zatwierdzony, na rynku pojawiło się wiele urządzeń opisywanych przez producentów jako Draft N. Jedne umożliwiały pracę z prędkością 150 Mb/s (N Lite), inne zaś miały wydajność 300 Mb/s. W październiku 2009 roku finalnie zatwierdzono 802.11n i określono jego maksymalną szybkość na poziomie 600 Mb/s przy wykorzystaniu dwóch pasm - 2,4 i 5 GHz.

802.11n

W 802.11n zaczęto stosować technologię MIMO wykorzystującą wiele anten do nadawania i odbioru. Dzięki niej sygnał Wi-Fi jest rozdzielany na kilka strumieni, które są niezależnie nadawane i równocześnie odbierane przez kilka odbiorników (2x2, 3x3). **MIMO polepsza zasięg sieci Wi-Fi oraz wydajność**. Dodatkowym zabiegiem na podniesienie transferów było rozszerzenie szerokości kanału z 20 do 40 MHz.

Porównanie

Nazwa standardu	Częstotliwość radiowa	Zasięg sygnału	Maksymalna szybkość transmisji
802.11b	2.4 GHz	30 metrów	11 Mb/s
802.11a	5 GHz	30 metrów	54 Mb/s
802.11g	2.4 GHz	30 metrów	54 Mb/s
802.11n	2.4 GHz / 5 GHz	50 metrów	600 Mb/s
802.15.1 Bluetooth	2.4 GHz	10 metrów	2 Mb/s

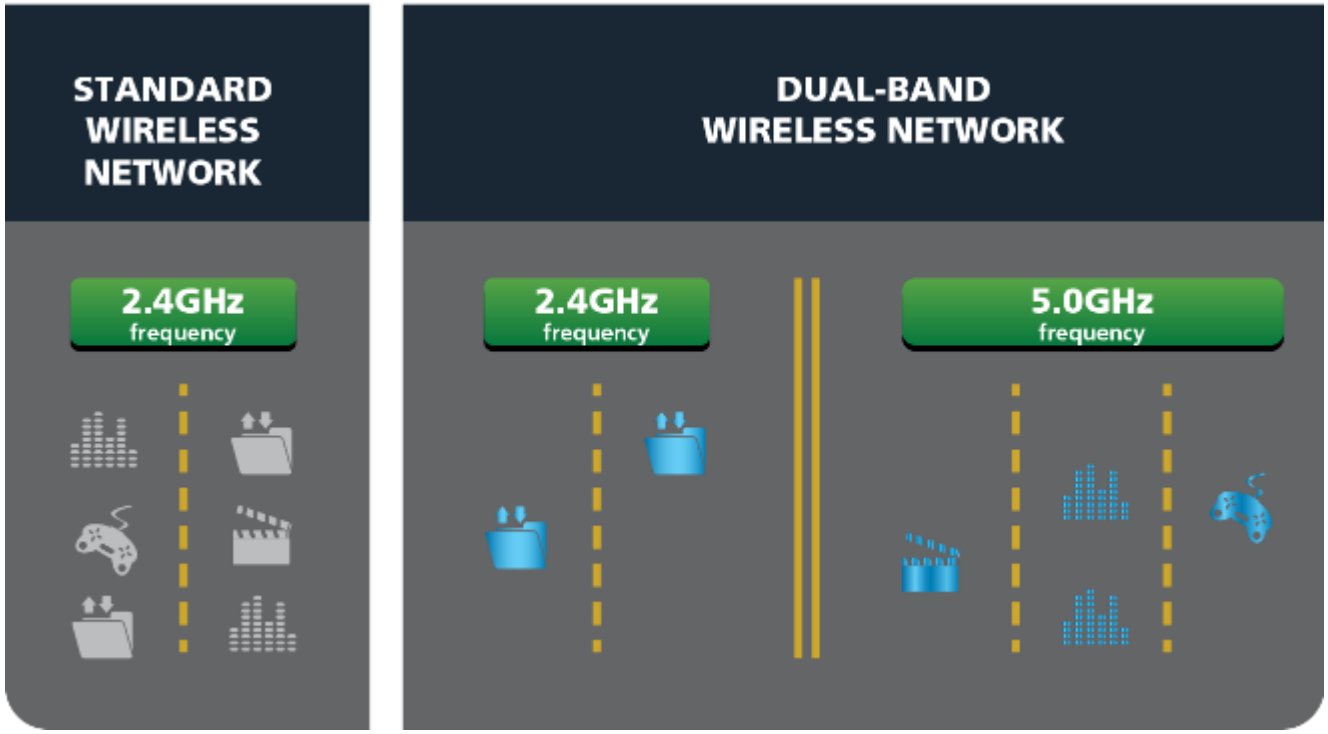
MIMO

Rozwiązanie zwiększające przepustowość i zasięg sieci bezprzewodowej poprzez wykorzystanie transmisji wieloantenowej w nadajniku i odbiorniku. W technologii N do czterech, a w AC nawet do ośmiu anten!

Beamforming

To technologia kształtująca wiązkę fal radiowych. **Rozwiązanie to jest w stanie zlokalizować urządzenie klienckie i kierunkowo transmitować sygnał**. Dzięki temu możliwe jest obniżenie mocy sygnału sieci Wi-Fi. Jest to nowoczesna technologia przetwarzania sygnału, która sprawia, że wykorzystanie fal radiowych jest bardziej optymalne.

Dual Band



To praca na dwóch różnych pasmach radiowych. W wypadku sieci Wi-Fi są to pasma 2,4 GHz i 5 GHz. Rutery Dual Band mogą pracować jednocześnie w obu pasmach (standardy 802.11n i 802.11ac) lub w jednym z nich (tylko rutery 802.11n).

Magiczne liczby wpisywane przez producentów w specyfikacjach są sumą danych wydajności z dwóch pasm. **Pamiętajmy o tym, wybierając ruter!** *Tak jak i o tym, że najczęściej niestety łączyć będziemy się tylko z jedną siecią naraz - 2,4 GHz lub 5 GHz. Uzyskanie więc obiecywanej wydajności nie zawsze będzie możliwe - będzie wymagało posiadania kompatybilnej karty sieciowe*

Typ	2,4 GHz	5 GHz
N300	300 Mb/s	-
N300	150 Mb/s	150 Mb/s
N450	300 Mb/s	150 Mb/s
N600	300 Mb/s	300 Mb/s
N750	300 Mb/s	450 Mb/s
N900	300 Mb/s	600 Mb/s
AC600	150 Mb/s	433 Mb/s
AC750	300 Mb/s	433 Mb/s
AC1200	300 Mb/s	867 Mb/s
AC1300	400 Mb/s	867 Mb/s
AC1450	450 Mb/s	975 Mb/s
AC1600	300 Mb/s	1300 Mb/s
AC1750	450 Mb/s	1300 Mb/s
AC1900	600 Mb/s	1300 Mb/s
AC2350	600 Mb/s	1733 Mb/s
AC3200	600 Mb/s	2600 Mb/s

Jaki router wybrać?

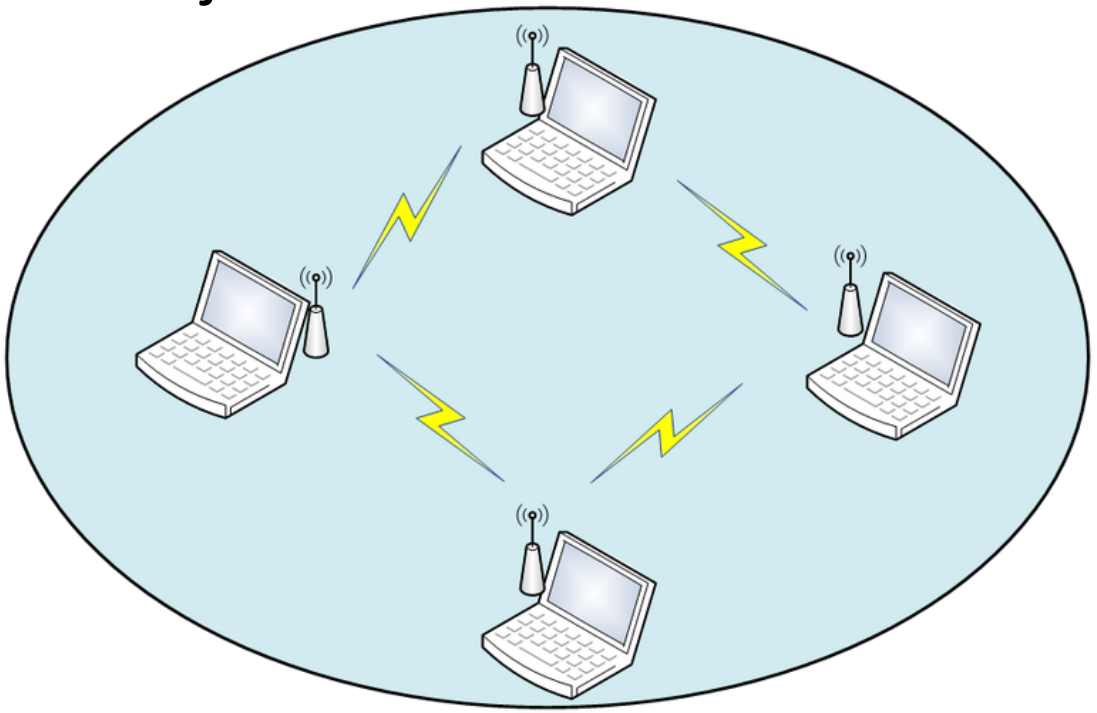
https://www.youtube.com/watch?v=DTolyaCX3-w

Kanały

Dokładna częstotliwość stosowana w określonej sieci bezprzewodowej zależy od wykorzystywanego kanału transmisyjnego. Na przykład w USA używa się 11 kanałów, w Polsce 13, w Japonii 14 a we Francji tylko 4.

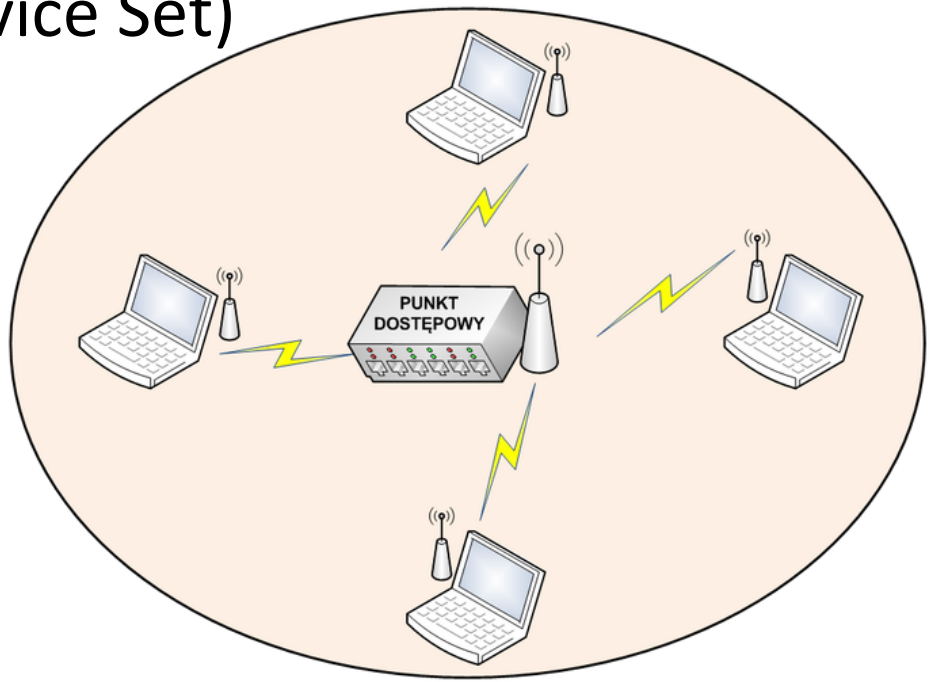
Technologia sieci „ad-hoc” - IBSS

Sieć w technologii **„ad-hoc”** określana mianem **IBSS** (ang. Independent Basic Service Set) pozwala na wymianę danych między kilkoma komputerami bez użycia punktu dostępowego, ale i bez dostępu do istniejącej struktury sieciowej.



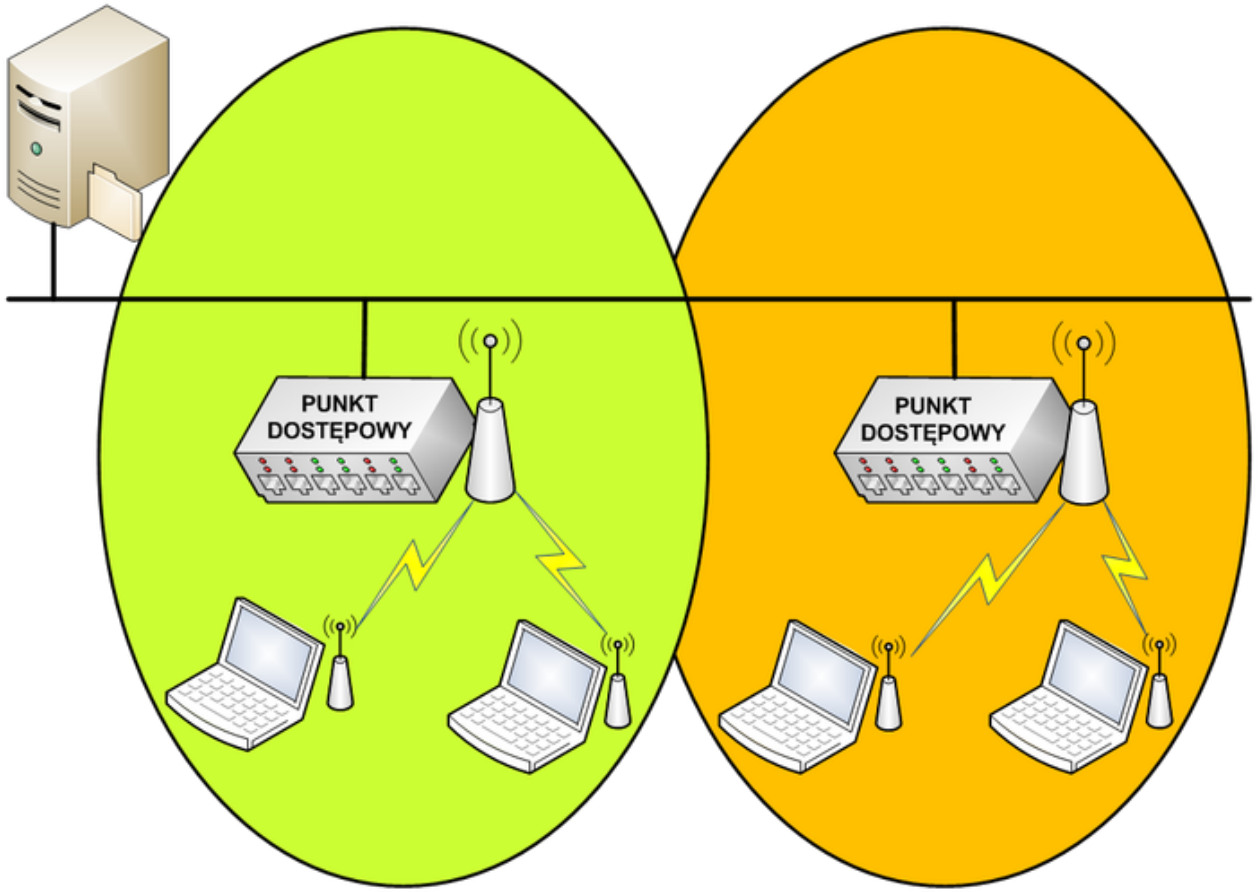
Technologia sieci infrastrukturalnej - BSS

Każda stacja bezprzewodowa wymienia komunikaty i dane z punktem dostępowym, który przekazuje je dalej do innych węzłów sieci LAN lub WLAN.
Sieć infrastrukturalna, zawierająca tylko jedną stację bazową (punkt dostępowy, router) jest określana mianem **BSS** (ang. Basic Service Set)



Technologia sieci infrastrukturalnej - ESS

Jeśli infrastrukturalna sieć bezprzewodowa korzysta z kilku punktów dostępowych, określa się ją mianem **ESS** (ang. Extended Service Set).



Bezpieczeństwo sieci Wi-Fi

1. **Identyfikator SSID** (ang. Service Set ID) – wszystkie punkty dostępu oraz wszyscy klienci znajdujący się w sieci muszą mieć ustawiony taki sam SSID. Identyfikator ten zapewnia pewną bardzo ograniczoną formę kontroli dostępu, ponieważ trzeba go podać w trakcie nawiązywania połączenia do sieci Wi-Fi i jest on wartością tekstową, którą można dowolnie określić. Większość punktów dostępu rozsyła zwykle sygnał kontrolny, który rozgłasza identyfikator SSID danej sieci. Gdy karta sieciowa przeprowadza skanowanie sygnałów radiowych, wykrywa je i wyświetla listę znalezionych identyfikatorów SSID w swoim programie kontrolnym (można również tę funkcję wyłączyć).
2. **Szyfrowanie WEP** (ang. Wired Equivalent Privacy) – jest dostępne w każdym systemie działającym w standardzie Wi-Fi. Szyfrowanie to bazuje na współdzielonym kluczu szyfrującym o długości 40 lub 104 bitów oraz 24-bitowym wektorze inicjującym.

Bezpieczeństwo sieci Wi-Fi

3. **Standard 802.1x** – scentralizowanie identyfikacji użytkowników, uwierzytelnianie, dynamiczne zarządzanie kluczami. Wszystkie te środki zapewniają dużo większe bezpieczeństwo w sieci niż kontrola dostępu wbudowana w protokół 802.11.
4. **Szyfrowanie WPA** (ang. Wi-Fi Protected Access) – znacznie bezpieczniejsze szyfrowanie niż WEP, ponieważ używa protokołu TKIP (ang. Temporal Key Integrity Protocol) w celu automatycznej zmiany klucza szyfrującego po upływie określonego czasu lub gdy nastąpi wymiana określonej liczby pakietów. Na szyfrowanie WPA składają się poniższe składniki:
    - WPA = 802.1x + EAP + TKIP + MIC
    - EAP (ang. Extensible Authentication Protocol)
    - TKIP (ang. Temporal Key Integrity Protocol)
    - MIC (ang. Message Integrity Check)