1. Aktualnie Wykorzystywane Standardy Wi-Fi

Wi-Fi, znane również jako IEEE 802.11, to zestaw standardów definiujących komunikację bezprzewodową w sieciach lokalnych. Najważniejsze standardy Wi-Fi:

1.1. IEEE 802.11n (Wi-Fi 4)

- **Wprowadzenie**: 2009 rok.
- **Pasmo**: 2,4 GHz i 5 GHz.
- **Maksymalna przepustowość teoretyczna**: do 600 Mb/s.
- **Cechy**:
    - Wprowadzenie technologii MIMO (Multiple Input Multiple Output) zwiększającej przepustowość.
    - Kompatybilność wsteczna z wcześniejszymi standardami (802.11a/b/g).
- **Zastosowanie**: Sieci domowe i biurowe wymagające większej przepustowości, np. do strumieniowania wideo HD.

1.2. IEEE 802.11ac (Wi-Fi 5)

- **Wprowadzenie**: 2013 rok.
- **Pasmo**: 5 GHz.
- **Maksymalna przepustowość teoretyczna**: do 3,5 Gb/s.
- **Cechy**:
    - Szersze kanały (do 160 MHz).
    - Większa liczba strumieni MIMO (do 8).
    - Modulacja 256-QAM zwiększająca efektywność spektralną.
- **Zastosowanie**: Aplikacje wymagające wysokiej przepustowości, takie jak strumieniowanie wideo 4K, gry online.

1.3. IEEE 802.11ax (Wi-Fi 6)

- **Wprowadzenie**: 2019 rok.
- **Pasmo**: 2,4 GHz i 5 GHz.
- **Maksymalna przepustowość teoretyczna**: do 9,6 Gb/s.
- **Cechy**:
    - Technologia OFDMA (Orthogonal Frequency-Division Multiple Access) poprawiająca efektywność w zatłoczonych sieciach.
    - Lepsza obsługa wielu urządzeń dzięki ulepszonemu MU-MIMO.
    - Zmniejszone opóźnienia i większa wydajność energetyczna.
- **Zastosowanie**: Inteligentne domy, IoT, środowiska o dużym zagęszczeniu urządzeń.

1.4. IEEE 802.11ax z rozszerzeniem 6 GHz (Wi-Fi 6E)

- **Wprowadzenie**: 2020 rok.
- **Pasmo**: 2,4 GHz, 5 GHz i 6 GHz.
- **Maksymalna przepustowość teoretyczna**: do 9,6 Gb/s.
- **Cechy**:
    - Dodatkowe pasmo 6 GHz oferujące więcej kanałów i mniejsze zakłócenia.
    - Lepsza wydajność w zatłoczonych środowiskach.
- **Zastosowanie**: Aplikacje wymagające niskich opóźnień i wysokiej przepustowości, np. VR/AR.

1.5. IEEE 802.11be (Wi-Fi 7)

- **Wprowadzenie**: Oczekiwane w 2024 roku.
- **Pasmo**: 2,4 GHz, 5 GHz i 6 GHz.
- **Maksymalna przepustowość teoretyczna**: do 46 Gb/s.
- **Cechy**:
    - Szersze kanały (do 320 MHz).
    - Modulacja 4096-QAM zwiększająca efektywność transmisji.
    - Obsługa Multi-Link Operation (MLO) umożliwiająca jednoczesne korzystanie z wielu pasm.
- **Zastosowanie**: Aplikacje wymagające ultra-niskich opóźnień i bardzo wysokiej przepustowości, takie jak transmisje 8K, VR/AR, gry w chmurze.

Tabela porównawcza standardów Wi-Fi

Standard	Rok wprowadzenia	Pasmo	Maks. przepustowość
Wi-Fi 4	2009	2,4 GHz, 5 GHz	do 600 Mb/s
Wi-Fi 5	2013	5 GHz	do 3,5 Gb/s
Wi-Fi 6	2019	2,4 GHz, 5 GHz	do 9,6 Gb/s
Wi-Fi 6E	2020	2,4 GHz, 5 GHz, 6 GHz	do 9,6 Gb/s
Wi-Fi 7	2024	2,4 GHz, 5 GHz, 6 GHz	do 46

2. Starsze Standardy Wi-Fi

Można spotkać starsze standardy Wi-Fi, zwłaszcza w starszych urządzeniach, systemach przemysłowych i niektórych sieciach o ograniczonych wymaganiach. Oto starsze standardy Wi-Fi, które mogą być nadal wykorzystywane:

2.1. IEEE 802.11a (1999)

- **Pasmo**: 5 GHz, **Maksymalna przepustowość**: 54 Mb/s
    - Pierwszy standard działający w paśmie 5 GHz.
    - Mniejsze zakłócenia niż w 2,4 GHz, ale krótszy zasięg.
- **Czy jest jeszcze używany?**
    - **Rzadko**, ale niektóre starsze urządzenia mogą go nadal obsługiwać.

2.2. IEEE 802.11b (1999)

- **Pasmo**: 2,4 GHz, **Maksymalna przepustowość**: 11 Mb/s
    - Bardzo popularny na początku lat 2000.
    - Duża kompatybilność, ale wolne prędkości.
- **Czy jest jeszcze używany?**
    - **Tak, ale rzadko**, głównie w starszych urządzeniach IoT i systemach przemysłowych.

2.3. IEEE 802.11g (2003)

- **Pasmo**: 2,4 GHz, **Maksymalna przepustowość**: 54 Mb/s
    - Następca 802.11b, oferujący lepszą prędkość.
    - Kompatybilny wstecznie z 802.11b.
- **Czy jest jeszcze używany?**
    - **Tak**, choć coraz rzadziej – niektóre stare routery i urządzenia IoT nadal go obsługują.

Podsumowanie w tabeli:

Standard	Rok wprowadzenia	Pasmo	Maks. przepustowość	Czy nadal jest używany?
Wi-Fi 1 (802.11)	1997	2,4 GHz	2 Mb/s	❌ Nie
Wi-Fi 2 (802.11a)	1999	5 GHz	54 Mb/s	⚠️ Rzadko
Wi-Fi 2 (802.11b)	1999	2,4 GHz	11 Mb/s	⚠️ Sporadycznie (IoT, przemysł)
Wi-Fi 3 (802.11g)	2003	2,4 GHz	54 Mb/s	✅ Nadal w niektórych urządzeniach

3. Kompatybilność wsteczna i przyszłościowa

Kompatybilność wsteczna oznacza, że nowszy sprzęt może obsługiwać starsze standardy.

Standard	Kompatybilność wsteczna	Pasma
Wi-Fi 7 (802.11be)	✅ z Wi-Fi 6E, Wi-Fi 6, Wi-Fi 5, Wi-Fi 4	2,4 GHz, 5 GHz, 6 GHz
Wi-Fi 6E (802.11ax 6 GHz)	❌ Tylko z Wi-Fi 6E	6 GHz
Wi-Fi 6 (802.11ax)	✅ z Wi-Fi 5, Wi-Fi 4	2,4 GHz, 5 GHz
Wi-Fi 5 (802.11ac)	✅ z Wi-Fi 4	5 GHz
Wi-Fi 4 (802.11n)	✅ z Wi-Fi 3, Wi-Fi 2	2,4 GHz, 5 GHz
Wi-Fi 3 (802.11g)	✅ z Wi-Fi 2	2,4 GHz
Wi-Fi 2 (802.11b)	❌ Niekompatybilny z Wi-Fi 1	2,4 GHz
Wi-Fi 1 (802.11a)	❌ Niekompatybilny z innymi	5 GHz

3.1. Kluczowe zasady kompatybilności

- Wi-Fi 4 (802.11n) wprowadziło pełną kompatybilność między pasmami 2,4 GHz i 5 GHz, co oznacza, że routery Wi-Fi 4 mogą obsługiwać zarówno starsze 802.11a/b/g, jak i nowsze urządzenia.
- Wi-Fi 5 (802.11ac) obsługuje tylko pasmo 5 GHz, więc nie współpracuje z urządzeniami Wi-Fi 3 (802.11g) i Wi-Fi 2 (802.11b), które działają tylko na 2,4 GHz.
- Wi-Fi 6 (802.11ax) działa na 2,4 GHz i 5 GHz, co oznacza kompatybilność ze starszymi standardami.

Wi-Fi 6E działa tylko w paśmie 6 GHz, więc nie obsługuje starszych urządzeń działających na 2,4 GHz i 5 GHz.

4. Bezpieczeństwo sieci Wi-Fi – Standardy i Zalecenia

Bezpieczeństwo Wi-Fi jest kluczowe, ponieważ sieci bezprzewodowe są podatne na ataki, takie jak podsłuch, spoofing czy ataki typu „man-in-the-middle". Poniżej przedstawiam standardy zabezpieczeń Wi-Fi, ich poziom bezpieczeństwa oraz rekomendacje dotyczące ich stosowania.

4.1. Standardy szyfrowania Wi-Fi

Standard	Rok	Szyfrowanie	Poziom bezpieczeństwa	Czy używać?
WEP (Wired Equivalent Privacy)	1997	RC4 (64-/128-bit)	🚨 Bardzo słabe – podatne na ataki	❌ Nie używać
WPA (Wi-Fi Protected Access)	2003	TKIP (RC4)	⚠️ Przestarzałe – łatwe do złamania	❌ Nie używać
WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key)	2004	AES (CCMP)	✅ Bezpieczne (z silnym hasłem)	✅ Używać, jeśli nie ma WPA3
WPA2-Enterprise	2004	AES (CCMP)	✅ Bardzo bezpieczne (RADIUS, 802.1X)	✅ Używać w firmach
WPA3-PSK (Wi-Fi Protected Access 3)	2018	AES-GCMP	✅ Najbezpieczniejsze dla domów i firm	✅ Zalecane
WPA3-Enterprise	2018	AES-GCMP + 192-bit mode	🔒 Najwyższy poziom bezpieczeństwa	✅ Dla firm i instytucji

---

4.2. Jakie zabezpieczenia są rekomendowane?

✓ **Dla sieci domowej**:

- WPA3-PSK (Personal) – najlepsza opcja, jeśli router i urządzenia obsługują WPA3.
- WPA2-PSK (AES) – jeśli WPA3 nie jest dostępne.
- Silne hasło (min. 12 znaków, unikanie słownikowych fraz).

✓ **Dla firm i organizacji**:

- WPA3-Enterprise – najlepszy wybór, szczególnie w środowiskach o podwyższonym poziomie bezpieczeństwa.
- WPA2-Enterprise – alternatywa, jeśli starsze urządzenia nie obsługują WPA3.
- Autoryzacja RADIUS (802.1X) – zapobiega atakom typu „man-in-the-middle".

4.3. Zalecenia dodatkowe dla bezpieczeństwa sieci Wi-Fi

Zalecane praktyki:

- **Wyłącz WPS (Wi-Fi Protected Setup)** – WPS jest podatne na ataki brute-force.
  Zmień domyślną nazwę SSID – unikaj nazw sugerujących rodzaj sprzętu (np. "TP-Link_1234").
- **Ukrycie SSID?** – Nie zwiększa bezpieczeństwa, a może powodować problemy z niektórymi urządzeniami.
- **Aktualizuj oprogramowanie routera** – wiele luk w zabezpieczeniach wynika z nieaktualnego firmware'u.
- **Filtracja adresów MAC?** – Może być łatwo obejściem przez spoofing, nie jest kluczowym zabezpieczeniem.

Podsumowanie:

- WPA3 to obecnie najbezpieczniejszy standard i warto go stosować, jeśli jest dostępny.
- WPA2-AES nadal zapewnia dobrą ochronę, ale należy unikać TKIP i słabych haseł.
- WEP i WPA (TKIP) są całkowicie przestarzałe i nie powinny być używane.
- Dodatkowe zabezpieczenia, jak RADIUS, segmentacja VLAN i aktualizacje routera, zwiększają ochronę.