



W przypadku wystąpienia niskiego transferu przy korzystaniu z routera należy mieć na uwadze liczne aspekty. Poniżej ich zestawienie. Bardziej szczegółowy opis wybranych zagadnień znajduje się w dalszej części rozdziału.

- Czy połączenie z routerem realizowane jest przewodowo czy bezprzewodowo → jest to istotne zwłaszcza dla szybkich pakietów internetowych. Sieć bezprzewodowa ma ograniczoną przepustowość zależnie od standardu.
- Czy port LAN ETH działa w standardzie gigabit ethernet (dla pakietów > 100 Mb/s)?
- Czy router i host pracują w standardzie 11n (dla pakietów > 60 Mb/s) przy pracy bezprzewodowej?
- Czy urządzenie jest odpowiednio zabezpieczone, sieć WiFi jest zabezpieczona przed dostępem osób trzecich? Czy standard zabezpieczeń minimalizuje ryzyko nieautoryzowanego dostępu?
- Czy do routera nie są podłączone inne urządzenia (na przykład monitoring, telewizor, konsola do gier), mogące wysyłać/pobierać dane w tle?
- W jaki sposób sieć bezprzewodowa jest zabezpieczona?
- Czy kanał WiFi nie jest zbyt okupowany w eterze (inne urządzenia bezprzewodowe, działające w otoczeniu nadają na tym samym kanale, zakłócając się wzajemnie)?
- Czy na połączeniu bezpośrednim transfer również jest za niski? Jaka jest metodologia wykonywania pomiaru? Czy problem nie powstaje na poziomie komputera?

### 1.1. Sieci nieszyfrowane.

Jeśli państwa sieć nie została zabezpieczona kluczem sieciowym, istnieje obawa że osoby trzecie mogą się z nią łączyć w dowolnym momencie i wysysać łącze poprzez pobieranie dużej ilości danych z udziałem np. programów p2p, co skutkuje zaniżonym transferem, a w przypadku zapchania łącza całkowitym brakiem usługi Internetowej. Dodatkowo istnieje obawa, że użytkownicy niezabezpieczonej sieci będą narażeni na ataki cyber przestępców, umożliwiające podsłuchiwanie aktywności sieciowej użytkowników lub przejmowanie ich ważnych danych (np. unikalnych loginów lub haseł, numerów kart kredytowych, itp.) → wynika to z faktu, że dane wysyłane i odbierane na takiej sieci przez urządzenie komputerowe nie są w żaden sposób szyfrowane. Należy zatem zadbać o należyte zabezpieczenie sieci utworzonej w routerze. Podobnie nie zaleca się zabezpieczania sieci archaicznym kluczem WEP → jest to zabezpieczenie słabe, którego obejście zajmuje kilka minut. Jedynym skutecznym zabezpieczeniem domowej sieci Wi-Fi jest zastosowanie szyfrowania WPA2 i wprowadzenie mocnego klucza sieciowego (zawierające znaki różnej wielkości, cyfry, itp.). Przykładem mocnego hasła jest np. *Multimedia\_1*.

- ▲ Należy mieć świadomość, że starsze urządzenia komputerowe lub systemy operacyjne (np. Windows XP SP 2, czy Windows ME) nie będą działać z szyfrowaniem WPA2 → trzeba wtedy wybrać WPA albo skorzystać z opcji łączonej WPA/WPA2 w ustawieniach routera.



## 1.2. Zakłócenia radiowe.

Na chwilę obecną technologia Wi-Fi obsługuje trzy standardy: 802.11b, 802.11g i 802.11n, które pracują na paśmie radiowym 2,4 GHz. Na takim samym paśmie operują inne urządzenia wykorzystywane w gospodarstwie domowym, takie jak kuchenki mikrofalowe, nadajniki bluetooth (np. bezprzewodowe myszy komputerowe), czy bezprzewodowe aparaty telefoniczne. Natężenie tego typu urządzeń w państwa lokalu będzie skutecznie zagłuszać sieć bezprzewodową, co przyczyni się do spadku transferu przesyłu danych lub zrywania połączeń internetowych. Wyłączenie tego typu urządzeń na czas korzystania z Internetu lub odseparowanie od routera pozwoli poprawić stabilność sieci. Najnowsze routery pracujące w standardzie 802.11n umożliwiają często wybranie częstotliwości 5,0 GHz, która jest odporna na zakłócenia innych urządzeń radiowych, jednak urządzenia starsze, nie obsługujące tego standardu, nie będą w stanie uzyskać połączenia z uwagi na brak kompatybilności wstecz → należy brać to pod uwagę przy wyborze tego właśnie ustawienia sieciowego.

### 1.2.1. Propagacja fali radiowej w mieszkaniu.

Wadą routerów jest relatywnie niski zasięg rozgłaszanej sieci. Większość producentów, deklaruje, że ich urządzenia są w stanie transmitować sieć o promieniu 90 metrów w zamkniętych pomieszczeniach, jednak są to dane uzyskiwane w warunkach laboratoryjnych, które nigdy nie będą osiągnięte w gospodarstwie domowym. Instalując router trzeba mieć na uwadze liczne przeszkody, takie jak elewacja budynku, grubość ścian budynku i wykorzystany budulec, czy urządzenia wyposażenia domowego. Typowy router jest najczęściej wyposażony w antenę o mocy ~ 5dBi i każda przeszkoda, jaką napotka sygnał rozgłaszany z routera, zakłóci tę wartość. Poniższa tabela ilustruje jak poszczególne elementy wykończenia budynku wpływają na tłumienie rozgłaszanego sygnału.<sup>1</sup>

Nazwa elementu	Materiał	Grubość [cm]	Tłumienie [dB]
Ściana wewnętrzna	Cegła	10	7
Ściana wewnętrzna	Cegła	30	9
Ściana działowa	Rigips i wełna szklana	7	2
Strop	Beton	30	11
Okno	Szkło	2x szyba + 1 cm przerwy	4,5
Drzwi	Drewno	4	2,5

<sup>1</sup> <http://blog.alvarus.org/wp-content/uploads/2014/04/Lukasz-Jasinski-Pomiar-tlumienia-scian-i-innych-elementow-charakterystycznych-dla-srodowiska-wewnatrzbudynkowego-w-pasmie-2-4GHz.pdf>



- ⚠ W przypadku, gdy sygnał sieci bezprzewodowej nie dociera do wszystkich pomieszczeń w użytkowanym lokalu należy dokupić mocniejszą antenę do routera (jeśli router posiada wymienną antenę) lub dokupić wzmacniacz sygnału Wi-Fi<sup>2</sup> i za jego pomocą wzmocnić rozgłaszaną sieć.

### 1.2.2. Obce sieci bezprzewodowe.

Coraz częściej (zwłaszcza w miastach) sygnał sieci bezprzewodowej jest niestabilny z uwagi na obecność innych routerów / nadajników radiowych, które wzajemnie się zakłócają (pracują na pokrywających się częstotliwościach). Oczywiście, efektem jest degradacja efektywności tych sieci (tzw. Błędy interferencji). W takiej sytuacji pomoc może zmienić kanał pasma 2,4 GHz, na którym operuje państwa router. Pomoc w wyborze najlepszego kanału może pomóc jedna z licznych aplikacji (np. popularny [inSSIDer](#)) skanujących otoczenie sieciowe i pozwalających wybrać optymalny kanał. Należy ocenić który z kanałów w naszym otoczeniu jest najmniej okupowany. Jeżeli znajdziemy najmniej okupowany kanał, przystępujemy do zmiany na routerze.

Jeśli nie możemy skorzystać z takiego skanera otoczenia sieciowego:

- Jeśli w ustawieniach kanałów radiowych routera jest pozycja *AUTO*, taką wartość warto wybrać na początku → router będzie sam sobie dobierał optymalną częstotliwość pracy i jeśli napotka błędy interferencji, to zmieni kanał radiowy na inny.
- ⚠ Należy mieć świadomość, że w chwili, gdy router będzie zmieniał kanał na inny, dojdzie najprawdopodobniej do zerwania połączenia internetowego. Jeśli w ustawieniach routera masz ustawiony kanał radiowy na *AUTO* zrywa połączenia sieci bezprzewodowej to warto w pierwszej kolejności zrezygnować z autoustawienia kanału.
- Jeśli w ustawienia routera nie można skorzystać z automatycznego przydzielania kanału, zaleca się wybrać któryś ze skrajnych kanałów (np. 1 lub 12), gdyż są one zwykle najmniej zakłócone → większość urządzeń pracuje na kanałach z zakresu 6-9.
- Jeśli kanał na którym pracuje router jest zakłócony, przyległe kanały również nie będą działać prawidłowo → jeśli np. zakłócony jest kanał 9, kanały 8 i 10 również będą zdegradowane.
- Niektóre starsze hosty mogą nie wspierać wybranego kanału (nie pracują na takiej częstotliwości). Jeśli po konfiguracji routera host nie widzi sieci Wi-Fi, należy zmienić kanał na inny.
- Jeśli podłączasz urządzenie komputerowe zakupione poza granicami kraju, może ono nie pracować na wszystkich dostępnych w twoim routerze kanałach → np. laptop zakupiony w Stanach Zjednoczonych będzie pracował wyłącznie na kanałach z zakresu 1-11 i nie połączy się z kanałem o numerze np. 12 (nie wy-

---

<sup>2</sup> Fachowo zwany Repetaerem - jest to zwykle kompaktowe urządzenie, które instaluje się w gnieździe elektrycznym i jego zadanie polega na skupianiu sygnału Wi-Fi i rozsiewaniu go dalej, jednocześnie wzmacniając go.



kryje tak rozgłaszanej sieci na liście dostępnych sieci bezprzewodowych). Stan ten wynika z odrębnych regulacji dotyczących użytkowania sprzętu radiowego w danym kraju.

### 1.3. Zmiana kanału radiowego.

Zmiany kanału radiowego dokonać należy w panelu konfiguracyjnym routera. Sposób logowania do panelu jest opisany [tu](#). W chwili zalogowania do MENU i wybrania opcji *Ustawienia Zaawansowane* należy wybrać zakładkę *Ustawienia sieci bezprzewodowej*. Następnie należy przejść do karty *Podstawowe ustawienia sieci bezprzewodowej*. Poniżej przykład, jak taka funkcja jest opisana w routerze marki PENTAGRAM.

Enable wireless function

Wireless Working Mode  Wireless Access Point(AP)  Network Bridge(WDS)

Network Mode 11b/g/n mixed mode

SSID twoja nazwa sieci

Broadcast(SSID)  Enable  Disable

Channel AutoSelect

Channel Bandwidth  20  20/40

Extension Channel Auto Select

WMM Capable  Enable  Disable

Na powyższym przykładzie widać, że obecnie w routerze jest ustawiona funkcja AUTO → router sam dopiera sobie optymalną częstotliwość pracy. W przypadku konieczności zmiany kanału należy kliknąć w polu *Auto*. Powinien pojawić się suwak, za pomocą którego może wybrać właściwy kanał.

Gdy klikniemy w polu *Channel* pojawi się suwak, za pomocą którego może wybrać właściwy kanał.

Enable wireless function

Wireless Working Mode  Wireless Access Point(AP)  Network Bridge(WDS)

Network Mode 11b/g/n mixed mode

SSID twoja nazwa sieci

Broadcast(SSID)  Enable  Disable

Channel AutoSelect

Channel Bandwidth

Extension Channel

WMM Capable

- AutoSelect
- 2412MHz (Channel 1)
- 2417MHz (Channel 2)
- 2422MHz (Channel 3)
- 2427MHz (Channel 4)
- 2432MHz (Channel 5)
- 2437MHz (Channel 6)
- 2442MHz (Channel 7)
- 2447MHz (Channel 8)
- 2452MHz (Channel 9)
- 2457MHz (Channel 10)
- 2462MHz (Channel 11)

Po wybraniu kanału, który nas interesuje zatwierdzamy operację klikając na przycisk

Należy jeszcze zrestartować router, by uruchomił się z nowymi ustawieniami → można to zrobić poprzez odłączenie urządzenia od zasilania



## Najczęściej zadawane pytania

**1.4. Posiadam modem do którego podłączony jest router. Chcę mieć dalej sieć Wi-Fi, ale korzystać z jednego urządzenia, nie dwóch.**

Można otrzymać od nas modem kablowy posiadający funkcje typowego routera Wi-Fi w ramach usługi [Mega BSM](#).

**1.5. Nie potrafię prawidłowo skonfigurować swojego routera. Czy wykwalifikowany pracownik MMP może to zrobić dla mnie?**

Nie. MMP świadczy usługi w zakresie szerokopasmowego dostępu do Internetu i odpowiada za samo działanie usługi. Konfiguracja urządzenia końcowego – komputera lub routera leży po stronie użytkownika końcowego. W takiej sytuacji należy skorzystać z usług serwisu komputerowego.

**1.6. Dlaczego, gdy dzwonię na infolinię wsparcia technicznego MMP oczekuje się ode mnie podłączenia komputera do modemu z pominięciem routera?**

Pełną weryfikację zgłaszanej usterki nasi konsultanci są w stanie przeprowadzić wyłącznie na połączeniu bezpośrednim.

**1.7. Nie mogę w pełni korzystać z Internetu, gdyż mam blokowane porty. Dlaczego?**

W ramach świadczonej usługi dostępu do Internetu porty nie są blokowane przez MMP. W tej sytuacji za blokowanie portów odpowiada Państwa router. Należy je odblokować korzystając z załączonej do urządzenia instrukcji obsługi. Nawet jeśli porty są domyślnie zablokowane w routerze, nie uniemożliwi to korzystania z większości usług, takich jak WWW czy komunikatory lub programy p2p. W przypadku jednak bardziej zaawansowanych usług, np. monitoringu czy podłączania dysków sieciowych, do których dostęp chcemy zapewnić z zewnątrz, będą wymagane dodatkowe działania w routerze.

**1.8. Router był dawno temu konfigurowany i nie pamiętam hasła do sieci Wi-Fi, a chcę podłączyć nowe urządzenie.**

Problem ten jest poruszony [tu](#).



Informacje zwarte w tym dokumencie mają charakter wyłącznie informacyjny. Pokazane grafiki oraz użyte opisy, dotyczące konfiguracji parametrów routerów, mogą się różnić. Multimedia Polska nie ponosi odpowiedzialności za szkody wynikające z błędnie zaprogramowanego routera. Odpowiedzialność za skonfigurowanie jak i użytkowanie routera leży po stronie użytkownika końcowego.