S-Cabling

SIEMON™
CABLING SYSTEM

## Dlaczego Wi-Fi?

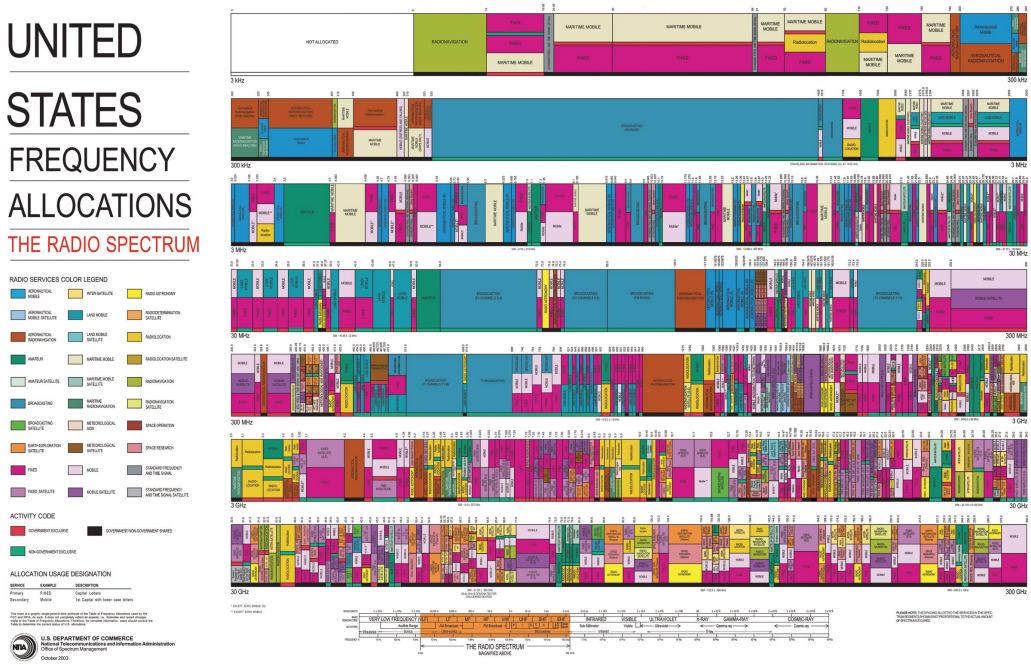
Sieci bezprzewodowe poczyniły ogromny postęp od czasu swych pierwszych wdrożeń do dzisiejszej szybkości przesyłania danych wynoszącej 54 Mbps w Wi-Fi (Wireless Fidelity). Pierwotna norma IEEE 802.11 umożliwiła transmisje sieci bezprzewodowej z szybkością przesyłu danych w wysokości 2 Mbps w paśmie ISM (Industrial-Scientific-Medical). Nowsze wersje tych norm różnią się trochę i nie wszystkie są kompatybilne. 802.11 a działa w paśmie 5GHz U-NII (Unlicenced National Information Infrastructure) i zapewnia szybkość od 1,2,5,11 do maksymalnie 54 Mbps. Z kolei 802.11 b działa w tym samym paśmie co oryginalna norma, czyli w paśmie ISM oraz umożliwia przesyłanie danych z szybkością 11 Mbps. Najnowsza z norm to 802.11 g. Ta norma, zatwierdzona w czerwcu 2004 r., pozwala na przyśpieszenie przesyłu danych do 54 Mbps i działa w obu pasmach. Zdolność działania w obu pasmach czyni tę normę kompatybilną zwrotnie z normą 802.11 b (nie 802.11 a). Kiedy się nad tym zastanowić, ważne, by zwrócić uwagę na fakt, że sprzęt 802.11 b był mniej kosztowny i jako pierwszy na rynku, dlatego też zyskał większy udział na rynku w stosunku do swego odpowiednika – 802.11 a.

Brzmi niejasno? Z pewnością nie jesteś w tym osamotniony. Temat ten był równie zagmatwany dla wielu pierwszych osób wdrażających Wi-Fi. To kwestia nowego nastawienia dla wielu profesjonalistów w zakresie sieci, przyzwyczajonych do „podłączenia" wyposażenia sieciowego bezproblemowo współpracującego z innymi urządzeniami. W takich przypadkach, główna uwaga skupiała się na prędkości i protokołach. Niemniej normy WiFi są odrobinę inne ze względu na kodowanie oraz fakt, że są one transmitowane w różnych częstotliwościach bez przewodów.

### Słowo na temat zakresów częstotliwości

Aby lepiej zrozumieć wdrożenie WiFi, warto posiadać podstawową wiedzę dotyczącą spektrum. Jest ono licencjonowane i zarządzane przez FCC (Federalną Komisję ds. Komunikacji). Produkty WiFi korzystają z częstotliwości pasm z nielicencjonowanego spektrum, udostępnionego przez FCC do komunikacji danych. Co oznacza słowo „nielicencjonowane"? W skrócie oznacza to zdolność do transmisji bez wymogu licencji. Aby posiadać część licencjonowanego spektrum, konieczne jest ubieganie się o licencję i zobowiązanie do transmisji wyłącznie w obrębie przydzielonego zakresu częstotliwości. Zaletą licencjonowanego bezprzewodowego spektrum jest to, że taka szerokość pasma może być kontrolowana i zagwarantowana. Jeśli firmy posiadają wieże transmisyjne jako część swojego BTA (Business Trade Area), muszą wówczas nadawać w swoich częstotliwościach, w swoim spektrum 24 x 7, podobnie jak stacje telewizyjne czy radiowe.

Różnica z nielicencjonowanym spektrum polega na tym, że funkcjonuje ono jako otwarta licencja dostępna dla każdego producenta, którego sprzęt podlega certyfikacji ze względu na spełnienie wymogów częstotliwości w obrębie spektrum. Ewentualne niewłaściwe wykorzystanie spektrum nie jest nadzorowane, dlatego też użytkownicy muszą zrozumieć, że mogą występować przerwy oraz zanieczyszczenie danych niepożądanymi sygnałami. W Stanach Zjednoczonych, spektrum 1-100 MHz to tzw. „publiczne fale powietrzne", przenoszące sygnały komunikacyjne marynarki wojennej, policji oraz straży pożarnej, radia HAM, radia CB klasy D, kanałów VHF 2-6 oraz rządowego sygnału lotniczego na częstotliwości 75 MHz, jak również wszystkie AM oraz część FM pasm częstotliwości radiowych.

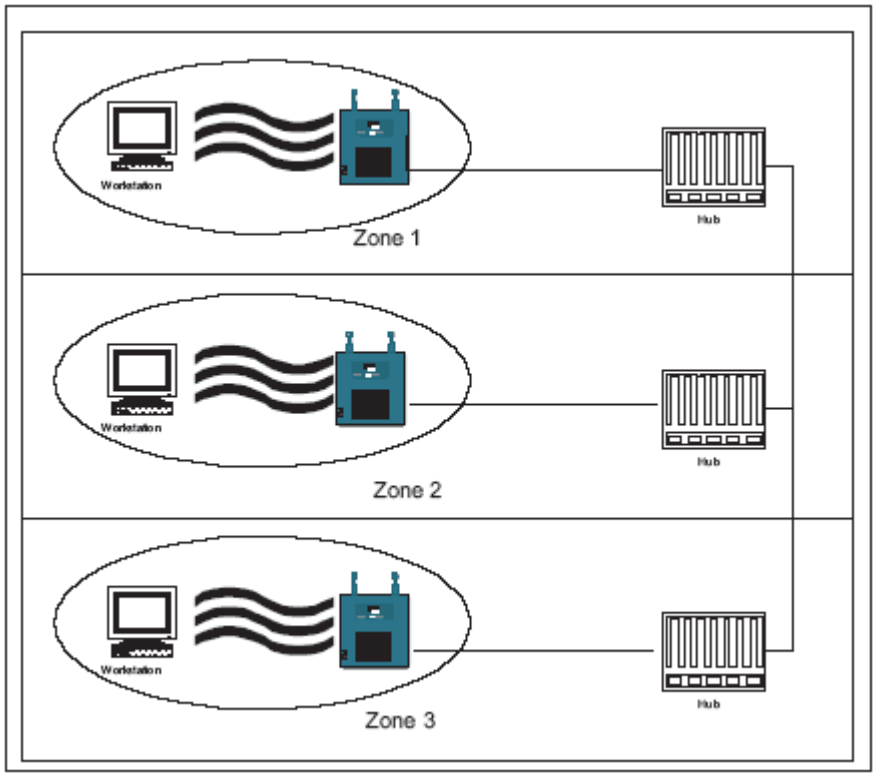



Rysunek 1 – Wykres spektrum FCC

Powyższy wykres przedstawia przydział częstotliwości w USA, zarządzany przez FCC oraz NTIA (wyłącznie dla częstotliwości rządowych). Jak widać, ilość częstotliwości oraz kanałów w ich obrębie jest dość rozległa. Mapy częstotliwości obejmują też sygnały telewizyjne, danych oraz radiowe.

**W jaki sposób działają sieci bezprzewodowe?**

Komputery oraz inne urządzenia sieci bezprzewodowej są wyposażone w kartę sieci bezprzewodowej. Karta taka zawiera radio. Wcześniejsze wersje kart mogły współpracować tylko z jedną technologią bezprzewodową (np. tylko z 802.11 b). Nowsze wersje kart oferowane przez część producentów mogą przeszukiwać wszystkie dostępne zakresy częstotliwości w celu znalezienia sieci poprzez transmitowanie za pomocą swojego radia w różnych zakresach częstotliwości. Usługi sieci są „ogłaszane" przez Wireless Access Point (WAP) – Bezprzewodowy Punkt Dostępu, który funkcjonuje jako stacja bazowa dla sygnałów radiowych. Zarówno nadajnik (komputer), jak i odbiornik (WAP) w każdej częstotliwości transmisji muszą się nawzajem rozumieć i działać w tym samym zakresie częstotliwości, aby komunikacja była możliwa. Gdy sieć jest już odnaleziona, przypisuje ona następnie informacje karcie bezprzewodowej, umożliwiając komunikację w sieci.




Rysunek 2 – strefy bezprzewodowe oraz komunikacja

WAP zajmuje się sygnalizacją pomiędzy bezprzewodowymi urządzeniami a siecią przewodową. Każdy punkt WAP działa w innym kanale w obrębie danej częstotliwości. Jak pokazano na rysunku 2, każdy WAP jest też połączony przewodowo z siecią. Umożliwia to transmisje poza sieć, na przykład, usług internetowych. Szerokość pasma jest dzielona między wszystkich użytkowników komunikujących się poprzez swoje punkty dostępu. Istnieje określony limit co do ilości urządzeń, które mogą się komunikować przez jeden punkt dostępu. Limit ten może być niższy dla niektórych punktów dostępu, w zależności od stopnia wykorzystania przez stanowiska pracy danej szerokości pasma.

Strefy są wydzielane na podstawie powierzchni budynku liczonej w metrach kwadratowych oraz pojemności punktu WAP. Przy projektowaniu sieci bezprzewodowej, należy przed wszystkim wziąć pod uwagę obszar zasięgu Punktu Dostępu, wynoszący z reguły około 30-90 m wewnątrz budynku. Ponieważ sygnały są sygnałami radiowymi, niektóre typy budynków mogą mieć wpływ na ich zasięg. Jeśli budynek jest wykonany lub uzbrojony za pomocą takich materiałów jak metal, kamień, cegła, płyty betonowe czy bardzo twarde drewno, sygnały radiowe mogą nie być wystarczająco silne, aby zapewnić połączenie przez te przeszkody. Ważne też, by pamiętać, że radio jest sygnałem promieniującym, czyli im dalej od punktu dostępu, tym wolniejsza prędkość połączenia; podobnie jak w przypadku jakiegokolwiek sygnału radiowego, sygnał sieci bezprzewodowej słabnie wraz z odległością. W zależności od siły sygnału, użytkownik

podłączony do 11 Mbps sieci może korzystać z prędkości zaledwie 1 Mbps z powodu odległości i/lub innych czynników osłabiających transmisję.

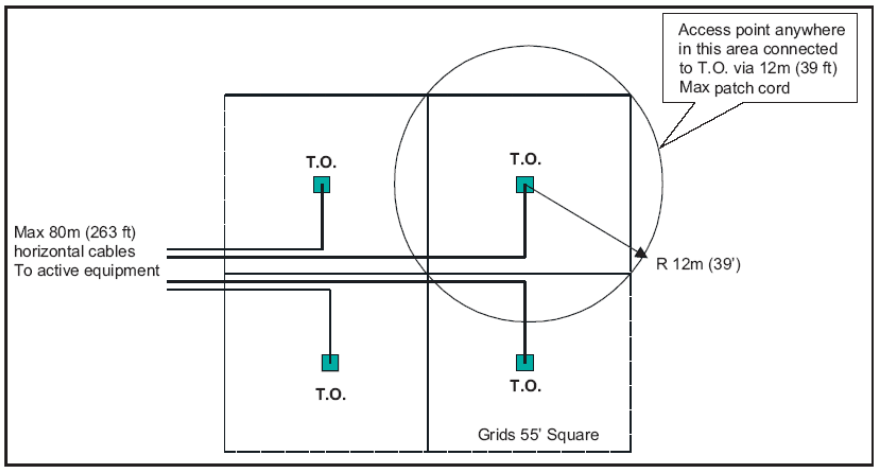
Pojedynczy punkt WAP może obsługiwać ograniczoną liczbę użytkowników. Liczba ta może się znacznie różnić w zależności od potrzeb każdego użytkownika w odniesieniu od usług sieciowych. Typowe punkty dostępu obsługują 10-20 osób, ze względu na „pęczniejący" charakter ruchu sieciowego. Niemniej dla bardzo aktywnych użytkowników lub tych, dla których połączenia mają fundamentalną wagę, dzielenie szerokości pasma z innymi może się okazać niedopuszczalne i wymagane mogą być dodatkowe punkty WAP, aby zapewnić wystarczającą bliskość wobec sygnału, gwarantującą najwyższy możliwy poziom szerokości pasma.

| | **Zakres maksymalny** | **Zakres przy 11 Mbps** |
|---|---|---|
| Na zewnątrz / otwarta przestrzeń ze standardową anteną | 750 -1000 ft | 150-350 ft |
| Biuro / otoczenie bez nadmiernego uprzemysłowienia | 250-350 ft | 100-150 ft |
| Osiedle mieszkaniowe | 125-200 ft | 60-80 ft |

Rysunek 3 – typowe ustawienia zakresów (dostarczone przez stowarzyszenie WiFi)

**Nowa norma TIA WLAN**

TIA opracowuje obecnie nową normę okablowania WLAN. Norma ta nie zawiera żadnych gwarancji zasięgu i ma mieć charakter ogólny. Oparta jest na systemie siatki w obrębie sufitu, dzięki której dostępne są najlepsze opcje konfiguracji i rozmieszczenia bezprzewodowych punktów dostępu. Siatka dzieli powierzchnię na 52' kwadraty, na środku każdego z nich umieszczone jest wyjście telekomunikacyjne. Dzięki sznurowi połączeniowemu o maksymalnej długości 12 m (30') punkt dostępu może się znajdować w dowolnym miejscu w obrębie sekcji siatki. Zapewnia to doskonały zasięg oraz możliwości konfiguracji rozmieszczenia punktów dostępu. Patrz rysunek 4 poniżej.




Rysunek 4 – obszary zasięgu

Wsparciem tej opracowanej właśnie normy są tendencje w stronę oddawania do użytku gotowych technicznie budynków, które obejmują już wyjścia telekomunikacyjne w obszarach roboczych, a także siatki ze wstępnie rozmieszczonymi przewodami zaznaczone na suficie przestrzeni biurowej.
Wyjścia telekomunikacyjne, które nie są wykorzystywane dla punktów dostępu, mogą służyć innym celom, np. kamerom IP. Jeśli wykorzystywany jest Power over Ethernet (PoE), nie są potrzebne obwody elektryczne w tych lokalizacjach. Nowe punkty dostępu mogą być łączone z siatką, w której połączenia są przełączane z jednego punktu do drugiego, ograniczając w ten sposób ilość położonych kabli do pomieszczenia telekomunikacyjnego. Takie konfiguracje grożą jednak powstawaniem pojedynczych miejsc awarii i nie są w związku z tym zalecane.

**Dlaczego warto stosować WiFi?**
WiFi z pewnością przynosi korzyści małym biurom oraz przejściowym miejscom pracy. Użytkownicy mają w ten sposób dostęp do sieci bez konieczności poszukiwania połączenia kablowego. WiFi to także dobre rozwiązanie dla pomieszczeń konferencyjnych, sal narad i wspólnych pokoi, gdzie użytkownicy mogą mieć potrzebę korzystania z tych samych usług i plików. W sytuacji, gdy połączenia sieciowe są niedostępne lub z jakichś powodów bardzo drogie do wykonania (ściany z płyt betonowych, przykładowo), WiFi może stanowić atrakcyjną alternatywę. Można by pomyśleć zatem, że WiFi oferuje spore oszczędności w okablowaniu sieciowym – ale tak nie jest.

Użytkownicy, którzy są regularnie w biurze i są przyzwyczajeni do sieci komutowanych 100 Mbps, w których szerokość pasma nie jest dzielona, mogą nie zaakceptować najwyższej wspólnie dzielonej prędkości 54 Mbps. Rzeczywista prędkość będzie wynosić 40-70% tej prędkości na jednego użytkownika, a nawet mniej w zależności od odległości od punktu WAP. Nowe urządzenia i użytkownicy będą wymagać dodawania kolejnych punktów WAP do sieci. Do sieci WAP wprowadzane są też komunikatory, telefony i inne urządzenia; każde pochłonie część szerokości pasma sieci. W momencie nasycenia, sieć musi być poszerzana.

Z każdym nowym punktem WAP związana jest dodatkowa instalacja kablowa. Każdy punkt dostępu musi być połączony przewodowo z przełącznikiem sieciowym, aby umożliwić dostęp do zasobów sieci przewodowej. Wraz ze zwiększaniem przez firmy ilości punktów dostępu, aby pokonać ograniczenia szerokości pasma i inne problemy, wymagane są kolejne porcje okablowania. Pozostałe przewodowe wyposażenie sieciowe, może raczej nie stwarzać możliwości modernizacji przez wprowadzenie bezprzewodowych kart. Reasumując, WiFi jest w zasadzie dalekie od wyeliminowania kabli.

**Kilka słów na temat bezpieczeństwa**
Kwestie bezpieczeństwa WiFi nakładają na organizacje konieczność starannego przemyślenia planów w zakresie bezprzewodowych sieci. Norma 802.11 b dostarcza mechanizm zwany WEP (Wireless Equivalent Privacy). Mechanizm ten zaopatruje w kodowany klucz, który musi być wymieniony pomiędzy kartą PC i punktem dostępu. Mimo iż nie jest to rozwiązanie idealne, dostarcza jednak pewnego poziomu zabezpieczenia. Klucz ten można zmieniać dowolną ilość razy. Mając na uwadze, że punkty dostępu ogłaszają usługi a karty PC wyszukują ich, wygląda to inaczej niż w przypadku sieci przewodowych. W sieci przewodowej, użytkownicy muszą mieć najpierw połączenie lub dostęp. W sieci bezprzewodowej, każdy mógłby w zasadzie

siedzieć w oknie i uzyskać dostęp do sieci za pomocą prostej karty, gdyby sieć nie była zabezpieczona. Wiele sieci dla małych i domowych biur korzysta dzisiaj z bezprzewodowego sieciowania. Do Twoich usług sieciowych mogą zalogować się sąsiedzi i wykorzystywać Twoją szerokość pasma, jeśli administrator nie zadba o takie sprawy.

Za pomocą zmiany nazwy swojej sieci i SSID oraz ręcznego zarządzania adresami MAC (Media Access Control), które mogą przylegać do Twojej sieci, można zablokować taką sieć przed niepożądanymi naruszeniami. Ale ponieważ jest to otoczenie emisyjne, poziom ochrony, jaki ono dostarcza, może nie odpowiadać użytkownikom korporacyjnym.

Kwestie kodowania w sieciach bezprzewodowych zostały już poruszone. Nowe normy wydane przez grupę roboczą IEEE 802.11 i zmierzają w stronę lepszych mechanizmów służących bezpieczeństwu sieci. Przez pewien czas zalecaną normą kodowania było TKIP. Metoda ta łagodziła większość znanych ataków, ale nie wszystkie. Z kolei nowa norma RSN wykracza poza łamane dotąd metody kodowania, zmieniając klucze i utrudniając ich złamanie, a jednocześnie nadal zapewniając zwrotną kompatybilność z TKIP. RSN stanowi lepszą metodę zabezpieczenia sieci, ale dopóki w sieci będzie choć jedno urządzenie nie spełniające normy RSN, cała sieć bezprzewodowa może być dalej zagrożona. Nie wiadomo też, na jak długo ta metoda kodowania zapewni poziom bezpieczeństwa wymagany dla poufnej komunikacji. Należy przypuszczać, że zdolność do łamania protokołów bezpieczeństwa będzie rozwijać się prawie tak szybko jak same protokoły.

Każda sieć bezprzewodowa musi być zaprojektowana i zaplanowana z uwzględnieniem dostępnych propozycji w zakresie bezpieczeństwa. Osoby zarządzające sieciami będą musiały monitorować znane defekty bezpieczeństwa, aby zapewnić, że ich sieci bezprzewodowe nie będą zagrożone. Przepisy dotyczące typów plików i komunikacji dozwolonej w sieciach bezprzewodowych pomogą w zapewnieniu, że poufne dokumenty nie dostaną się w niepowołane ręce. Jak w przypadku każdej sieci, połączenie różnych strategii w zakresie bezpieczeństwa jest najlepszą metodą zabezpieczenia komunikacji.

**Nowsze technologie bezprzewodowe**

802.11 n

Jednym z problemów sieci 802.11 poza bezpieczeństwem jest prędkość. IEEE zatwierdziło nową grupę roboczą – 802.11 N. Grupa ta pracuje nad wprowadzeniem prędkości wynoszących minimum 100 Mbps. Przewiduje się, że technologia ta zostanie wdrożona nie tylko w komputerach, ale także w drobnej elektronice, urządzeniach ręcznych oraz we wszystkich środowiskach – firmowych, publicznych, a nawet na obszarach mieszkalnych. Norma ta będzie zwrotnie kompatybilna z innymi normami 802.11. Grupa zadaniowa pracuje nad MIMO (multiple in multiple out) jako możliwym rozwiązaniem w zakresie zwiększenia prędkości, przy jednoczesnym pozostawieniu kompatybilności z sieciami 802.11 a/b/g. Chodzi zatem o wielokrotne kanały dla komunikacji przez wielokrotne anteny.

**Wi-Max**

Wi-Max (Worldwide Interoperability for Microwave Access) to najnowsza metoda komunikacji bezprzewodowej, która została unormowana przez grupę roboczą IEEE 802.16 (Broadband Wireless Access). Polega ona na dostarczaniu punktów do wielopunktowych architektur, które działają w zakresie spektrum między 2 GHz a 66 GHz. Transmisje mogą sięgać na odległość do 30 mil z dzielonymi prędkościami przesyłu

danych wynoszącymi 70 Mbps. Dla uzyskania wyższych częstotliwości, konieczna jest linia stacji. Wymaga to anten o dużo większej mocy niż typowa antena WiFi, ale w przypadku szerokopasmowego bezprzewodowego dostępu na obszarach wiejskich czy w miasteczkach studenckich przynosi to w efekcie znaczące korzyści wynikające z faktu, że komunikacja może przebiegać przez wielokrotne urządzenia, jak w przypadku emisji stacji radiowej. Dla osób, które nie mają możliwości korzystania z szerokopasmowego dostępu do Internetu, jednym z rozwiązań może z pewnością być WiFi. Nowe uzupełnienie normy pozwoli na stały i mobilny dostęp poprzez anteny Wi-Max.

**Podsumowanie**

Choć technologia WiFi ma niewątpliwe zalety, nie przewiduje się, by mogła zastąpić sieci w głównych środowiskach korporacyjnych. Technologia ta pozostanie najprawdopodobniej rozwiązaniem przejściowym lub odpowiednim dla rynku SOHO. Przy rosnącej szybkości obliczeniowej i ilości zastosowań oraz coraz większym zapotrzebowaniu na zasoby sieci, rozwiązania kablowe w większości głównych aplikacji będą dostarczać odpowiednią prędkość na potrzeby pełnej i bezpiecznej funkcjonalności. Dodatkowe środki bezpieczeństwa oraz czas poświęcany na administrowanie, jakiego wymaga WiFi przy wdrożeniu i utrzymaniu, w rzeczywistości przewyższają jakiekolwiek oszczędności w okablowaniu.

W związku z faktem, że szerokość pasma jest dzielona w sieci WiFi, rozwiązania połączeniowe wdrażane w części kablowej powinny dostarczać najwyższą możliwą szerokość pasma przy minimalnej ilości zakłóceń. Dzięki temu wszelkie spadki prędkości ograniczane są do minimum.

Co więcej, ponieważ spektrum wykorzystywane w technologii bezprzewodowej jest nielicencjonowane, może podlegać nasyceniu i jest podatne na zakłócenia, co powoduje dodatkowe problemy. Największą przeszkodę w rozwiązaniu tych problemów stanowi fakt, że różne skutki występują sporadycznie, przez co są trudniejsze do pokonania. Odbiór sygnałów może być zakłócany i prowadzić do nowego rodzaju ataków – odmowy usług. Jest zatem mało prawdopodobne, że WiFi zastąpi systemy kablowe, ale z pewnością dostarczy usług uzupełniających tam, gdzie jest to technicznie możliwe.