

SIECI BEZPRZEWODOWE

Sieć bezprzewodowa (ang. *Wireless LAN*)

sieć lokalna zrealizowana bez użycia przewodów

używa fal elektromagnetycznych (radiowych lub podczerwonych) do przesyłania informacji z jednego punktu do drugiego bez użycia medium fizycznego.

Są one projektowane z użyciem standardu **IEEE 802.11**. Do komunikacji za pomocą fal radiowych wykorzystuje się pasmo **2,4 GHz** lub rzadziej **5 GHz**.

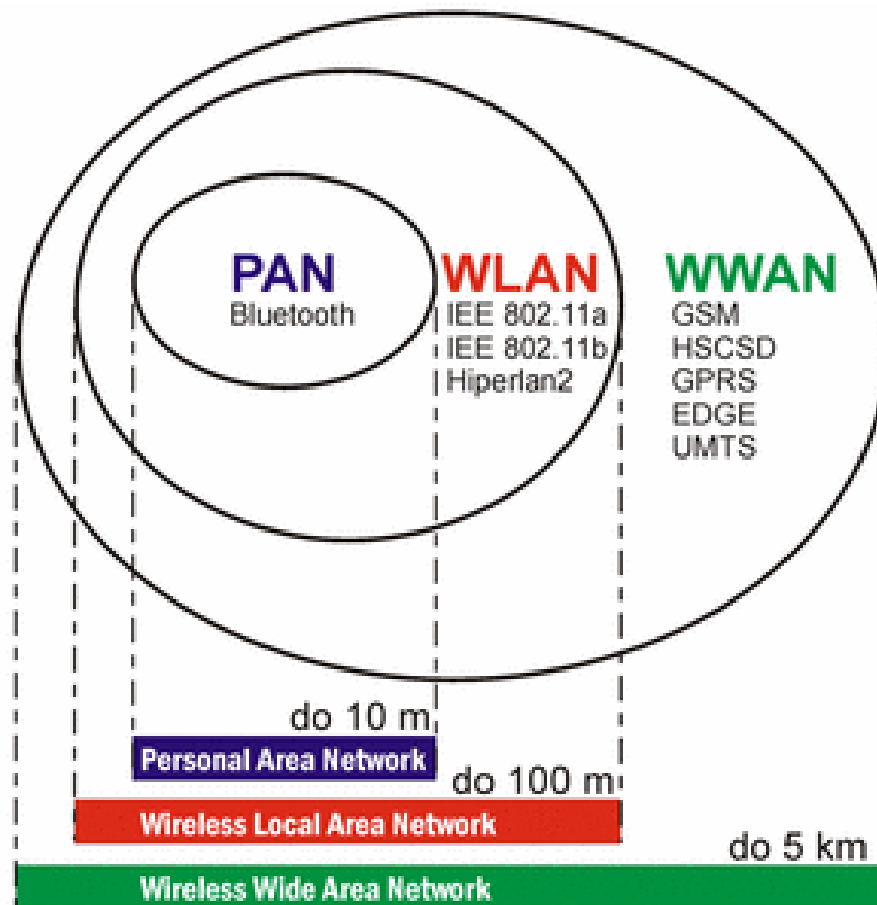
Pasmo 2,4GHz podzielone jest na **14 kanałów** w paśmie 2,4 – 2,5 GHz, które układają się co 5 MHz od 2412 do 2477 MHz. Każdy kanał ma swoją częstotliwość nośną, która jest modulowana przy przesyłaniu informacji.

Szybkość przesyłania danych zależna jest od użytego standardu i odległości pomiędzy użytymi urządzeniami i wynosi najczęściej 11, 22, 44, 54 lub 108 Mbps.

Technologie i standardy sieci bezprzewodowych

Instalatorzy sieci bezprzewodowych mają duży wybór rozmaitych technologii przy projektowaniu rozwiązań bezprzewodowych. Każda z nich ma swoje zalety, ale i ograniczenia.

Podział technologii pod kątem zasięgu:



WPAN (Wireless Personal Area Network) - Sieć o zasięgu kilku metrów służąca do wymiany informacji pomiędzy urządzeniami przenośnymi typu notebook, palmtop, telefon gsm itp. (obecnie do tych celów wykorzystuje się głównie technologię **Bluetooth**).



WLAN (Wireless Local Area Network) - sieć lokalna oparta o technologię bezprzewodową.

Sieć WLAN zlokalizowana jest w stosunkowo niewielkim obszarze obejmuje niewielką liczbę komputerów, zwykle kilka lub kilkanaście.



WWAN (Wireless Wide Area Network) - Rozległa sieć komputerowa oparta o technologię bezprzewodową, która obejmuje dużą liczbę komputerów na dużej przestrzeni i o dużym zasięgu.



Do komunikacji za pomocą fal radiowych wykorzystuje się pasmo **2,4 GHz** lub rzadziej 5 GHz.

W każdym paśmie (2,4-2,5 GHz) komunikacji bezprzewodowej zgodnej ze standardem Wi-Fi - 802.11b/g - wyodrębniono 14 niezależnych kanałów (co 5 MHz od 2412 do 2477 MHz).

Szybkość przesyłania danych zależna jest od użytego standardu i odległości pomiędzy użytymi urządzeniami i wynosi najczęściej: 11, 22, 44, 54 lub 108 Mbps.

Główne standardy w sieciach bezprzewodowych:

802.11a - **54** Mb/s częstotliwość 5 GHz

802.11b - **11** Mb/s częstotliwość 2,4 GHz

802.11g - **54** Mb/s częstotliwość 2,4 GHz

802.11n - **100-540** Mb/s

Stosowane metody zabezpieczeń zgodne ze standardem 802.11:

- **uwierzytelniania** - to identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika, który łączy się z siecią
- **protokół WEP** (Wired Equivalent Privacy) WEP działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24 bitowym wektorze inicjującym.
- **autoryzacja** - to zgoda lub brak zgody na żadaną usługę przez uwierzytelnionego użytkownika.
- **rejestracja raportów** - to rejestr akcji użytkownika związanych z dostępem do sieci.

(Kontrola raportów pozwala na szybką reakcję administratorów na niepokojące zdarzenia w sieci.)

Infrastruktura sieci bezprzewodowej

Na całość infrastruktury sieci bezprzewodowych składają się następujące elementy:

- **karty sieciowe** (najczęściej typu PCI, USB lub PCMCIA)

Każdy z nich ma swoje wady i zalety.

Najczęściej rodzaj złącza nie ma wpływu na przepustowość.

Karty PCI to są one zgodne ze standardem Plug&Play co jest ważne dla początkujących użytkowników sprzętu, choć nie zawsze oznacza to bezproblemową instalację.

Praktycznie wszystkie komputery stacjonarne posiadają złącza PCI, więc jest to na pewno najbardziej popularny typ kart.

Karty na złączach USB wymagają zwykle bardziej skomplikowanej instalacji oraz zużywają więcej zasobów komputera.

W komputerach przenośnych wykorzystywane są **karty PCMCIA**. Często odznaczają się one większą wydajnością od swych stacjonarnych odpowiedników.

Kolejną ważną sprawą jest kompatybilność adapterów. Zdarza się, że karty różnych producentów nie chcą współpracować ze sobą. Dochodzą tu także różne techniki komunikacji (warstwa fizyczna) choćby DSSS (rozpraszanie widma za pomocą sekwencji bezpośredniej) czy FHSS (rozpraszanie widma z przeskokiem częstotliwości). Dlatego aby nie mieć kłopotów instalacyjnych należy zdecydować się na jednego producenta (dot. także HUB-ów AP).

Przy wyborze kart sieciowych należy zwrócić uwagę również na prędkość adaptera. Do wyboru mamy: wersję **802.11B** - **11Mbit/s** lub wersję **802.11G** - **54Mbit/s**. Ostatnio popularny staje się standard **802.11N** o szybkości od 100 do **540 Mbit/s**. (Oczywiście są to wartości maksymalne, a rzeczywiste prędkości są raczej dwa razy mniejsze).

Przy zakupie należy upewnić się także czy do zestawu (w wypadku kart PCI) dostarczono odpowiednią antenkę, którą można umieścić na ścianie, biurku lub półce, co zapewnia najlepszy odbiór bez względu na lokalizację komputera.

Karty sieciowe



Punkty dostępowe (ang. *Access Point*)

Punkty dostępowe to najprościej mówiąc łączniki z już istniejącą siecią komputerową. Posiadają wbudowane tryby pracy stwarzając w ten sposób wiele pomysłów na rozwiązywanie czasem skomplikowanych topologii sieciowych. Z czasem wykrystalizowało się kilka trybów pracy dla AP, które w różnych modyfikacjach można spotkać u wielu producentów.

Access Point - tryb umożliwiający podłączanie abonentów do już istniejącej sieci LAN – głównie wykorzystywany w połączeniach z kartami sieciowymi klientów, którzy w ten sposób uzyskują dostęp do istniejącej wcześniej sieci – co w konsekwencji pozwala na pełne korzystanie z zasobów sieci do której podpięty jest AP. Tryb ten stosują np. dostawcy usług internetowych podłączający swoich klientów poprzez bezprzewodowe karty sieciowe, lub domowi użytkownicy Internetu dostarczanego drogą kablową – by w ten sposób rozdzielić dostęp do Internetu drogą radiową w obrębie własnego mieszkania czy domu na wszystkie komputery wyposażone w bezprzewodowe karty sieciowe. Jest to dobra alternatywa dla okablowywania mieszkania czy domu.

Ad Hoc – komputer podłączony do AP może zostać klientem takiej sieci – która w definicji łączy każde urządzenie radiowe z każdym innym będącym w polu widzenia.

AP Bridge Point To Point - W trybie tym Access Point pracuje jako bezprzewodowy most łączący dwie oddalone od siebie sieci LAN – np. sąsiednie budynki wcześniej okablowane – w jedną strukturę sieciową.

AP Bridge Point To Multipoint – podobny tryb do opisanego powyżej – z tym że można zwiększyć ilość połączonych sieci by stworzyć np. sieć o topologii gwiazdy.

AP Bridge WDS WDS - (Wireless Distribution System) charakteryzuje się możliwością jednoczesnej pracy AP w charakterze Access Point'a , oraz mostu bezprzewodowego między AP „bazowymi”, pozwala to na bezproblemowe tworzenie szkieletu sieci (o różnych strukturach), dając tym sygnał radiowy klientom końcowym oraz tym podpiętym z AP do switcha.

Access Point

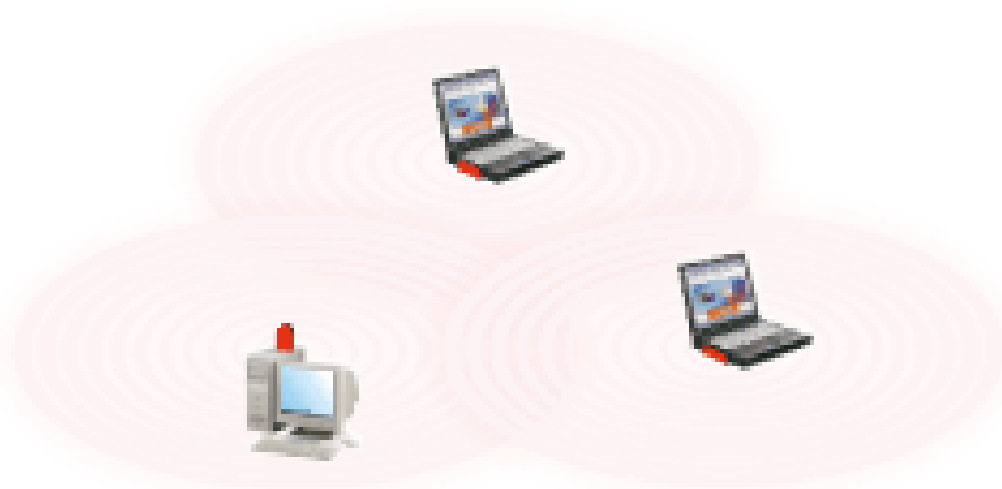


Konfiguracja sieci bezprzewodowych

Sieci bezprzewodowe mogą być proste lub złożone. W najprostszej wersji, dwa komputery wyposażone w karty radiowe tworzą niezależną sieć kiedy tylko znajdą się w swoim zasięgu.

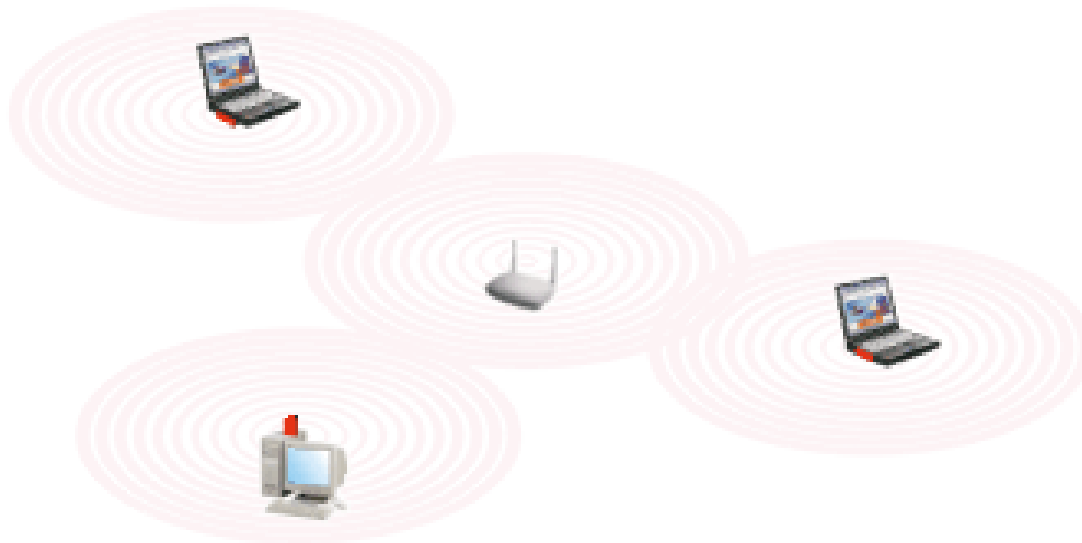
Nazywamy to siecią **peer-to-peer**.

Sieci takie nie wymagają administracji czy prekonfiguracji. W takim przypadku każdy użytkownik może mieć dostęp do zasobów drugiego użytkownika, lecz nie do centralnego serwera



Bezprzewodowa sieć peer-to-peer

Zainstalowanie punktu dostępowego może zwiększyć zasięg **sieci ad hoc**, efektywnie podwajając zasięg w jakim urządzenia mogą się komunikować.



Bezprzewodowa sieć z punktem dostępowym (AP)

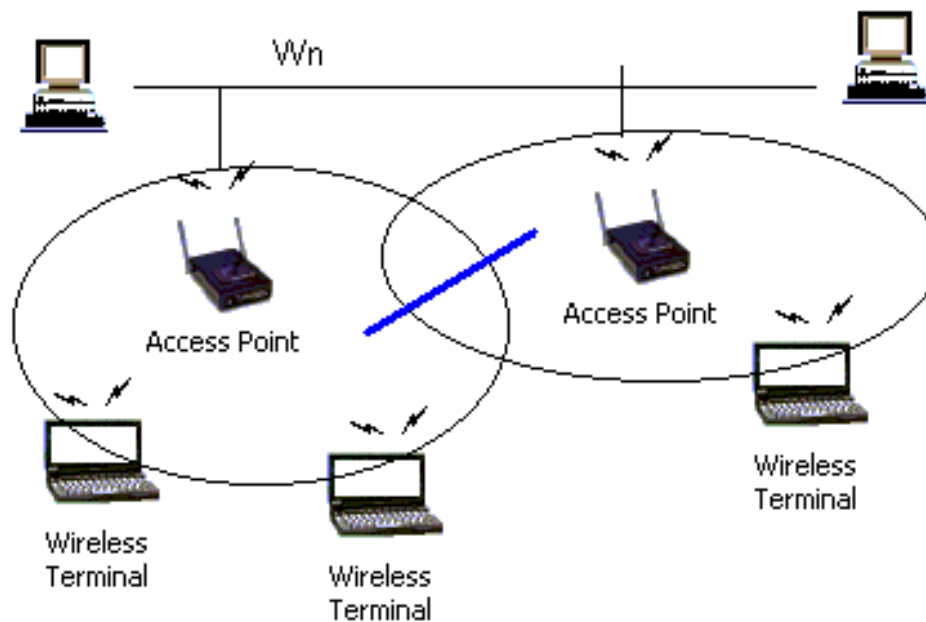
Ponieważ **punkt dostępowy** jest podłączony do sieci kablowej, każdy użytkownik ma dostęp zarówno do serwera jak i do innych użytkowników. Każdy punkt dostępowy może obsłużyć wielu użytkowników; dokładna liczba zależy od ilości i rodzaju transmitowanych danych. Wiele pracujących aplikacji działa w konfiguracjach, gdzie jeden punkt dostępowy obsługuje od 15 do 50 użytkowników.



**Bezprzewodowa sieć z punktem dostępowym
włączonym do szkieletu sieci**

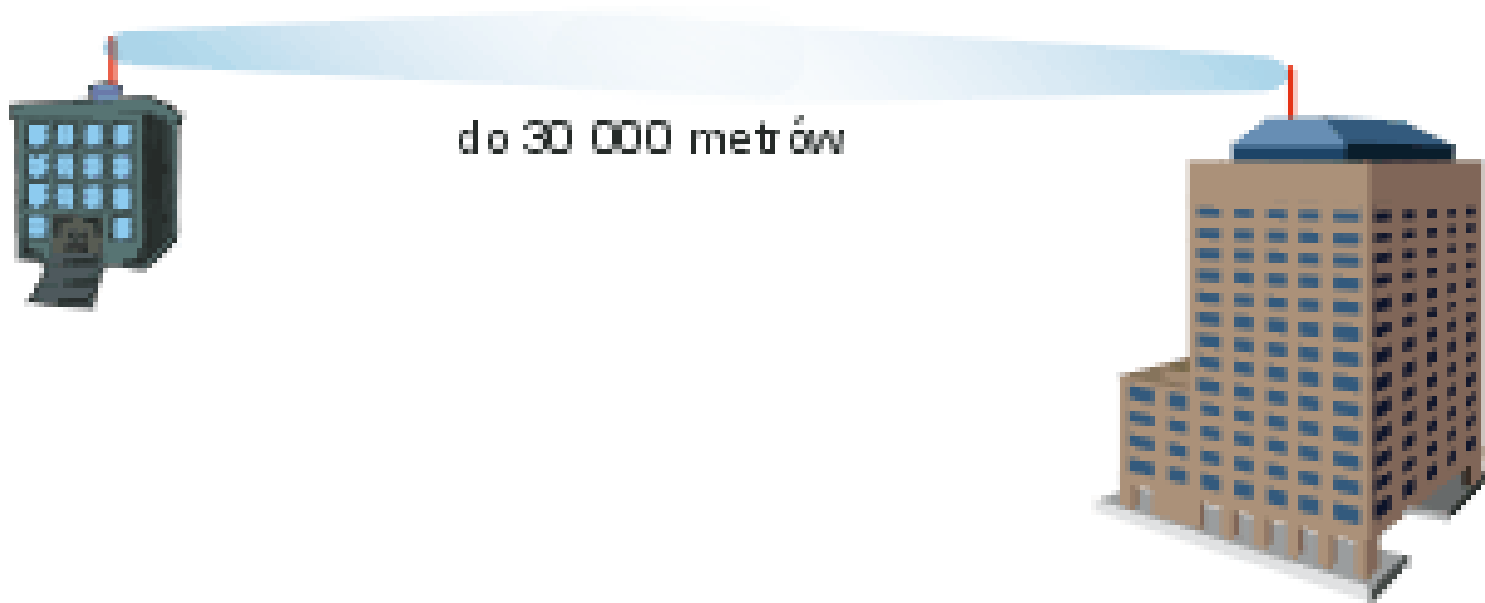
Punkty dostępowe mają ograniczony zasięg: 300 metrów w pomieszczeniach i 30000 metrów na otwartej przestrzeni. W rozległych infrastrukturach, takich jak magazyny, hurtownie, czy osiedla mieszkaniowe, prawdopodobnie będzie potrzeba zainstalowania więcej niż jednego punktu dostępowego. Lokalizację punktów dostępowych określa się robiąc właściwe pomiary. Celem jest pokrycie obszaru z zachowaniem nakładania się zasięgu poszczególnych komórek tak by użytkownik mógł poruszać się po danym obszarze bez utraty dostępu do sieci.

Taką możliwość poruszania się w zasięgu zespołu punktów dostępowych nazywamy [roamingiem](#). Punkty dostępowe, jeden po drugim, przekazują sobie użytkownika w sposób niezauważalny dla niego, zapewniając stałą łączność.



Kilka punktów dostępowych i roaming

Typowym zastosowaniem sieci bezprzewodowej jest połączenie dwóch punktów dostępowych łączem radiowym. Możemy w ten sposób połączyć np. centralę firmy z magazynem, czy salonem handlowym. Niezbędnym warunkiem dla zestawienia takiego połączenia jest widzialność optyczna kierunkowych anten nadawczo-odbiorczych.



Połączenie dwóch lokalizacji

Kolejny przykład przedstawia rozwiązanie dla dostawców np. Internetu. Możemy w ten sposób doprowadzić łącza Internetowe do użytkowników indywidualnych np. na osiedlu domków jednorodzinnych. Na punkcie dostępowym stosujemy antenę (lub anteny) dookólne a abonenci korzystają z anten kierunkowych.



Bezprzewodowe udostępnianie internetu

Niezbędnym warunkiem dla zestawienia takich połączenia jest widzialność optyczna kierunkowych anten nadawczo-odbiorczych abonentów i anteny na punkcie dostępowym.

Szyfrowanie:

Szyfrowanie to najczęściej stosowany sposób implementacji zabezpieczeń i ochrony informacji. W procesie szyfrowania wysyłane informacje zostają przetworzone przez zestaw instrukcji zwanych algorytmem szyfrowania. Instrukcje te łączą jawny tekst informacji z sekwencją liczb szesnastkowych zwanych kluczem szyfrującym.

Informacje, które mają być transmitowane drogą bezprzewodową, zostają wcześniej zaszyfrowane przez klienta bezprzewodowego lub punkt dostępowy. Podczas odbierania informacji punkt dostępowy lub klient bezprzewodowy używają tego samego klucza do odszyfrowania informacji. Informacje te mogą być odczytane tylko przez urządzenia sieci WLAN, które dysponują odpowiednim kluczem szyfrującym. Im dłuższy klucz, tym mocniejsze szyfrowanie.

Połączenia do sieci korporacyjnych za pomocą sieci bezprzewodowych mogą odbywać się także przy pomocy tuneli VPN.

W sieciach bezprzewodowych zgodnych ze standardem 802.11a/b/g wykorzystuje się w tym celu technologię **WEP (Wired Equivalent Privacy)**.

Standard specyfikuje **klucze 40- i 104-bitowe**, do których w procesie wysyłania ramki dołączany jest wektor inicjujący (IV) o długości **24 bitów**. Stąd popularnie mówi się o **64- i 128-bitowych** kluczach **WEP**, ale nie jest to stwierdzenie poprawne technicznie. W rozszerzeniach firmowych tego standardu znaleźć można również klucze o długości **232 bitów** (z IV daje to **256** bitów), które jednak z uwagi na znane słabości w doborze IV nie zwiększają w istotny sposób siły kryptograficznej całości rozwiązania.

IPsec (IP Security) to zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy kodowych pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia **Wirtualnej Sieci Prywatnej (VPN)**.

VPN oparta na **IPsec** składa się z dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanał wymiany kluczy za pośrednictwem którego przekazywane są dane związane z autentykacją oraz kodowaniem (klucze) oraz kanał (jednego lub więcej), który niesie pakiety transmitowane poprzez sieć prywatną. Kanał wymiany kluczy jest standardowym połączeniem UDP (port 500). Kanały przesyłu danych oparte są na protokole ESP (numer prot. 50) opisanym w dokumencie RFC 2406.

WPA (ang. *WiFi Protected Access*) to standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11.

Standard ten został zaproponowany przez organizację Wi-Fi Alliance jako następca mniej bezpiecznego WEP. Wykorzystuje protokoły TKIP i 802.1x oraz uwierzytelnianie EAP oparte na serwerze RADIUS.

WPA wykorzystuje klucze 128-bitowe.

Hotspot (ang. "hot spot" - gorący punkt) to otwarty i dostępny publicznie punkt dostępu umożliwiający dostęp do Internetu za pomocą sieci bezprzewodowej (WiFi).

Hotspoty są instalowane najczęściej w hotelach, restauracjach, lotniskach, dworcach, uczelniach, centrach miast i innych miejscach publicznych.

Umożliwiają one posiadaczom laptopów i palmtopów wyposażonych w bezprzewodową kartę sieciową standardu 802.11 podłączenie się i dostęp do Internetu. Usługa czasami jest bezpłatna lub też płatność następuje za pomocą karty kredytowej lub zakupu odpowiedniej zdrapki. Czasami też gdy dostęp jest bezpłatny ograniczony bywa zakres dostępnych usług na przykład tylko do strony WWW instytucji udostępniającej hotspot.

Do zabezpieczenia hotspotów służą:

- klucz WEP
- klucz WPA - WPA II
- Serwer Radius
- ukrywanie SSID
- VPN - Virtual Privacy Network - Wirtualne prywatne Sieci

Wyszukiwarka hotspotów w Polsce: <http://hot.spots.pl>

Zalety sieci bezprzewodowej

Do zalet sieci bezprzewodowych należy:

- mobilność - końcówki mogą się przemieszczać
- łatwość instalacji - nie trzeba kłaść przewodów
- elastyczność - łatwe dokładanie nowych końcówek
- zasięg - od kilku metrów (w budynkach) do kilkudziesięciu kilometrów
- szybka rozbudowa i modyfikacja struktury sieci.

Miejsca coraz powszechniejszych instalacji sieci WLAN:

- Transport – wymiana informacji przy transporcie towarów, przemieszczania ładunków uaktualnianie znaków drogowych itp.
- Handel – szybkie zmiany w organizacji wewnątrz
- Opieka zdrowotna – możliwość uzyskiwania przez lekarzy i personel szybkiego dostępu do danych pacjenta oraz korzystania z konsultacji, a także zdalnego używania komputerowo sterowanego sprzętu medycznego
- Usługi finansowe – łatwa organizacja usług bankowych i operacji handlowych
- Edukacja – dostępność uniwersyteckich komputerów z różnych punktów uczelni
- Produkcja – możliwość zdalnego sterowania pracą robotów

Wady sieci radiowych:

- stosunkowo duże rozpraszanie energii,
- wysoki poziom zakłóceń zewnętrznych,
- łatwość podsłuchu, nieautoryzowanego dostępu, celowego zakłócania