Wi-Fi

ID artykułu: 199 / 698

URL: http://www.publikuj.org/199

Wi-Fi (lub Wi-fi, WiFi, Wifi, wifi, ang. "Wireless Fidelity") - zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem WiFi jest budowanie sieci lokalnych opartych na komunikacji radiowej czyli WLAN.

Zasięg od kilku do kilkuset metrów i przepustowości sięgającej 108 Mb/s, transmisja na dwóch kanałach jednocześnie. Produkty zgodne z WiFi mają na sobie odpowiednie logo, które świadczy o zdolności do współpracy z innymi produktami tego typu. Logo Wi-Fi jest znakiem handlowym należącym do stowarzyszenia Wi-Fi Alliance. Standard WiFi opiera się na IEEE 802.11. WiFi bazuje na takich protokołach warstwy fizycznej, jak:
- DSSS (Direct Sequence Spread Spectrum),
- FHSS (Frequency Hopping Spread Spectrum),
- OFDM (Orthogonal Frequency Division Modulation),

Sieć WiFi działa w darmowym paśmie częstotliwości od 2400 do 2485 MHz i 5000 MHz. WiFi jest obecnie wykorzystywane do budowania rozległych sieci Internetowych. ISP umożliwiają użytkownikom wyposażonym w przenośne urządzenia zgodne z WiFi na bezprzewodowy dostęp do sieci. Jest to możliwe dzięki rozmieszczeniu w ruchliwych częściach miast obszarów nazywanych hotspotami. W wielu dużych miastach na świecie, jak Seul czy Nowy Jork znajdują się już setki miejsc, gdzie można uzyskać dostęp do Internetu w ten sposób.

Standardy w sieciach bezprzewodowych

Główne standardy w sieciach bezprzewodowych:
- 802.11a - 54 Mb/s częstotliwość 5 GHz
- 802.11b - 11 Mb/s częstotliwość 2,4 GHz posiada zasięg ok. 30 m w pomieszczeniu i 120 m w otwartej przestrzeni; w praktyce można osiągnąć transfery rzędu 5,5 Mb/s. Materiały takie jak woda, metal, czy beton obniżają znacznie jakość sygnału; standard 802.11b podzielony jest na 14 niezależnych kanałów o szerokości 22 MHz, Polska wykorzystuje tylko pasma od 2400 do 2483,5 MHz - kanał od 1 do 13
- 802.11n - 108 Mb/s częstotliwość 2,4 GHz, standard który niedawno został wprowadzony na rynek. Następca standardu 802.11g
- 802.11g - 54 Mb/s częstotliwość 2,4 GHz, obecnie najpopularniejszy standard WiFi, który powstał w czerwcu 2003 roku, wykorzystanie starszych urządzeń w tym standardzie powoduje zmniejszenie prędkości do 11 Mb/s;

oraz:
- 802.11c
- 802.11d
- 802.11e
- 802.11f
- 802.11h (w Europie odpowiednikiem jest 802.11a na częstotliwości 5 GHz)
- 802.11i (w tym systemie wprowadzono nowe zabezpieczenia za pomocą szyfrowania)
- 802.11j (powstał ze standardu 802.11a na potrzeby Japonii)
- 802.11n (najnowszy standard sieci bezprzewodowych, posiada o wiele większy zasięg i szybkość transmisji danych)
- 802.11r (dość szybki roaming)

Problemy występujące w czasie dostępu do sieci bezprzewodowych typu WiFi
- Efekt przechwytywania - występuje, gdy do jednego odbiornika docierają dwa sygnały o różnej mocy. W tym przypadku sygnał mocniejszy zostanie odebrany prawidłowo natomiast słabszy zostanie zagłuszony.
- Zjawisko odkrytej stacji - zjawisko występuje, wtedy gdy stacja znajduje się w zasięgu stacji nadawczej, ale poza zasięgiem stacji odbiorczej.

- Zjawisko ukrytej stacji - stacja jest ukryta jeżeli znajduje się w zasięgu stacji odbierającej dane, ale jest poza zasięgiem stacji nadawczej.
- Interferencje - zakłócenia transmisji, powstają gdy stacja jest poza zasięgiem zarówno odbiornika jak i nadajnika, jednak wystarczająco blisko aby móc zakłócić przesyłanie informacji między nimi.

Bezpieczeństwo WiFi

Stosowane metody zabezpieczeń zgodne ze standardem 802.11:
- uwierzytelniania - identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika, który łączy się z siecią
- protokół WEP (ang. Wired Equivalent Privacy) - działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24 bitowym wektorze inicjującym. WEP jest aktualnie bardzo złym zabezpieczeniem które nie chroni nas przed włamaniami z zewnątrz. W średnio obciążonej sieci klucze WEP można złamać po około 1h pasywnego nasłuchiwania pakietów.
- protokoły WPA/WPA2 - nowe, dużo bardziej bezpieczne mechanizmy szyfrowania przesyłanych danych.
- autoryzacja - zgoda lub brak zgody na żądaną usługę przez uwierzytelnionego użytkownika. Zabezpieczenie to jest wykonane przez punkt dostępu lub serwer dostępu.
- rejestracja raportów - rejestr akcji użytkownika związanych z dostępem do sieci. Kontrola raportów pozwala na szybką reakcję administratorów na niepokojące zdarzenia w sieci.

W sieciach bezprzewodowych (WiFi) zabezpieczenia można podzielić na dwa typy: autoryzacji i transmisji. Autoryzacja ma na celu potwierdzić tożsamość użytkownika, natomiast typ transmisji ma nas zabezpieczyć przed "podsłuchiwaniem". Obecnie są już nowe systemy zabezpieczeń, które posiadają same w sobie zabezpieczenie autoryzacji i transmisji. Możliwe zagrożenia sieci bezprzewodowych:
- próby włamań do tego typu sieci,
- uruchamianie przez użytkowników nieautoryzowanych punktów dostępowych, stających się tylną furtką do sieci.

Wi-Fi kontra telefonia GSM

WiFi zapewnia dziś transfery rzędu 10 Mbit/s w hotspocie. Oznacza to, że jest wielokrotnie szybsze od połączeń GPRS oferowanych przez operatorów telefonii GSM. WiFi nie posiada jeszcze pełnej funkcjonalności sieci komórkowych, ale ma miejsce znaczny postęp w tej dziedzinie. Firmy takie jak Zyxel, SocketIP, Symbol Technologies czy Unitech oferują usługi telefoniczne oparte na WiFi. W związku z narastaniem konkurencji WiFi i sieci komórkowych pojawił się termin 4G. Oznacza on, że WiFi może stać się czwartą generacją telefonii komórkowej. Jednak wykorzystanie WiFi wiąże się jeszcze z dużymi problemami. Standard WiFi nie zawiera mechanizmów uwierzytelniania podobnych do kart SIM. Trwają pracę nad stworzeniem odpowiednich standardów. Bardzo dużym problemem w WiFi jest zasięg hotspotów. Nie przekracza on zwykle 50 metrów, co oznacza, że WiFi może być tylko uzupełnieniem sieci GSM, jeżeli system telefonii ma obejmować cały obszar kraju takiego jak Polska. Na koniec lata 2004 roku firma Intel zapowiedziała prezentację nowego układu scalonego łączącego w sobie funkcje komunikacji WiFi oraz GSM. Miał on nosić nazwę WWAN (ang. Wireless Wide Area Network). Połączenie zasięgu sieci GSM oraz prędkości transferu z sieci WiFi jest szansą na szybsze stworzenie telefonii trzeciej generacji bez wykorzystania bardzo drogiego standardu UMTS.

Dostęp do WiFi

Obszary, gdzie można uzyskać dostęp do WiFi nazywa się hotspotami. Sieci WiFi stają się coraz popularniejsze zarówno w Polsce jak i na świecie. Istnieją miasta gdzie dostęp do tego typu sieci jest całkowicie bezpłatna, a co za tym idzie darmowy dostęp do internetu (Nowy Orlean). Bogate państwa planują pokryć szczelną siecią WiFi swój kraj by wszyscy mieli dostęp do darmowego internetu. W innych przypadkach konieczne jest wnoszenie opłat. Czasami rozliczenia opierają się na limitach transferowanych danych. W wielu krajach na świecie dostęp do sieci WiFi jest bezpłatny. Firmy i instytucje posiadające nadmiarowe łącza internetowe niskim kosztem stawiają nadajniki WiFi i udostępniają sieć za darmo dla wszystkich. W Polsce rozdawanie Internetu przez firmy jest naruszeniem prawa skarbowego. Usługi teleinformatyczne podlegają podatkowi VAT. Urzędnicy szacują koszt połączenia z Internetem (np. koszt Neostrady) i naliczają firmie udostępniającej sieć podatek oraz domiar. Z tego względu publiczne rozdawanie Internetu za darmo przez firmy w Polsce jest nielegalne. Firma, która chce świadczyć usługi dostępu do

internetu powinna zgłosić ten fakt do UKE (dawniej URTiP), czyli do Urzędu Komunikacji Elektronicznej. Procedura legalizacji opisana jest na stronach Urzędu Komunikacji Elektronicznej. Instytucje publiczne takie jak samorządy terytorialne dzięki posiadaniu dostępu do infrastruktury miejskiej mogą tanim kosztem budować sieci WiFi pokrywające swoim zasięgiem centra aglomeracji miejskich. W Polsce przoduje pod tym względem Rzeszów. Samorząd tego miasta zbudował sieć radiową o nazwie ResMan, aby zapewnić swoim mieszkańcom dostęp do Internetu oraz umożliwić obsługę systemów takich jak monitoring ulic czy telematyka systemu sygnalizacji ulicznej. Do połowy roku 2006 powstały 44 hotspoty pokrywające gęstą siecią centrum miasta. Program został sfinansowany częściowo z funduszy strukturalnych Unii Europejskiej. Przykład ten stanowi wyjątek od reguły. Większość polskich samorządowców nie zdaje sobie sprawy z roli nowoczesnych technologii w rozwoju społeczeństwa oraz nie potrafi zabiegać o fundusze na te cele. Większość operatorów posługuje się standardem 802.11b. Prędkość zapewniana przez sieci to 11 Mbps.

Popularna "radiówka"

Niedrogi dostęp do Internetu poprzez sieć bezprzewodową lokalnego providera został rozpowszechniony szczególnie na terenach pozamiejskich, gdzie nie ma możliwości korzystania z globalnej sieci w inny sposób. Opinie o takim sposobie dostępu - popularnej "radiówce" są jednak podzielone. Lokalni providerzy, licząc na szybki zysk, wykupują łącze z Internetem oraz instalują kilka stacji bazowych rozmieszczonych zazwyczaj w pobliskich wsiach. Zdecydowana większość tzw. "radiówek" oferuje dostęp do Internetu przez nieszyfrowane łącze 802.11b (11 Mb/s). W Internecie dostępne są za darmo narzędzia (Wireshark (dawniej Ethereal), ettercap) umożliwiające podsłuchanie każdej wiadomości przesyłanej w takiej sieci. Część ISP próbuje zwalczyć ten problem umożliwiając wykupienie szyfrowanego kanału VPN, ale zwykle wiąże się to ze znaczącym kosztem. Sygnał pomiędzy stacjami bazowymi dosyłany jest poprzez mosty bezprzewodowe (pracujące najczęściej na częstotliwości 5Ghz). Przyczynami niewłaściwego działania bezprzewodowego dostępu do Internetu świadczonego przez Wireless Internet Service Providera mogą być:

- nieudolne kształtowanie ruchu przez providera
- korzystanie z łącz o małych przepustowościach, nie nadających się do wykorzystania jako łącza operatorskie (popularny DSL)
- niewłaściwy dobór sprzętu radiowego (urządzeń aktywnych, okablowania, anten)
- niestabilne połączenia pomiędzy kolejnymi stacjami bazowymi
- brak włączonej izolacji pomiędzy klientami na punkcie dostępowym
- zbyt duża ilość klientów korzystających jednocześnie z danego punktu dostępowego (maksymalna zalecana ilość - 25 dla sprzętu klasy średniej)

Jakość bezprzewodowego dostępu do Internetu świadczonego poprzez lokalnych providerów jest więc bardzo zróżnicowana.

Zalety

- Możliwość budowy sieci z dostępem do Internetu w domu lub biurze, pozbawionej plątaniny kabli.
- Korzystanie z bezprzewodowego Internetu poprzez lokalnych providerów.
- Korzystanie z darmowego internetu poprzez HotSpot-y (dostępne w większych miastach).
- Swoboda i mobilność - bezprzewodowe podłączanie do sieci mobilnych urządzeń (notebooki, palmtopy)
- Łatwo dostępne i coraz tańsze urządzenia WiFi na rynku.
- Duża odporność na wyładowania atmosferyczne w porównaniu z siecią LAN
- Tanie, szybkie w instalacji
- Możliwość łączenia się z internetem z każdego miejsca nawet w ruchu
- Czasami bardzo potrzebne w budynkach zabytkowych gdzie nie można stosować okablowania
- Relatywne szybkie w porównaniu do standardowych wymagań
- Są częściej używane i poprawiają efektywność pracy
- Stają się standardem w wielu domach prywatnych

Wady

- Wykorzystywany w WiFi standard 802.11b i 802.11g wykorzystuje pasmo 2,4 GHz. W tym samym zakresie pracują takie urządzenia jak Bluetooth, kuchenki mikrofalowe, telefony bezprzewodowe, radary meteorologiczne, radiowa telewizja przemysłowa oraz wiele innych. Efektem może być zagłuszanie sygnałów WiFi i ograniczenie zasięgu hotspota.

- Sieci WiFi mają stosunkowo mały zasięg. Zwykle hotspot oparty na 802.11b lub 802.11g jest dostępny w odległości do 90 metrów w pomieszczeniach lub 150 metrów na zewnątrz.
- Jeżeli urządzenie wykorzystujące WiFi nie zostanie poprawnie skonfigurowane, może się stać łatwym celem ataku. Wykorzystywany w sieciach radiowych standard kryptografii WEP jest łatwy do złamania. Jednak operatorzy wprowadzają powoli inny protokół WPA, który ma zapewnić lepsze bezpieczeństwo.
- Połączenia na dalekie odległości mogą niekiedy okazać się niestabilne, gdy odbierany sygnał z punktu dostępowego jest zbyt słaby.
- Prędkość transmisji danych w przypadku wykorzystania standardu WiFi nie dorównuje rozwiązaniom kablowym, jednak jest wystarczająca do korzystania z Internetu.
- Mniej bezpieczne wymagają dodatkowych zabezpieczeń co dodatkowo zmniejsza prędkość przesyłu
- Czasami eter jest zajęty szczególnie w dużych miastach gdzie nie ma wolnych pasm częstotliwości
- Wymagają rezerwacji odpowiedniego pasma
- Szybkość transmisji zależy od odległości między urządzeniami komunikującymi się
- Bardzo podatne na zakłócenia

Wi-Fi oraz Linux

Wielu producentów urządzeń WiFi nie dostarcza sterowników dla innych systemów niż Windows. Jednak praca środowiska związanego z wolnym oprogramowaniem spowodowała, że jądro Linuksa w wersji 2.6 posiada wbudowaną obsługę wielu urządzeń tego typu. Istnieje też możliwość zainstalowania sterowników windowsowych dla systemu Linux za pomocą płatnego oprogramowania driverloader lub otwartego ndiswrapper.

Źródło: Wikipedia (na licencji GNU FDL)