

informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

informatyka+

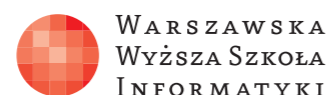
Wszechnica Popołudniowa: Sieci komputerowe

Podstawy działania
sieci bezprzewodowych

Dariusz Chaładyniak

Człowiek – najlepsza inwestycja

Człowiek – najlepsza inwestycja



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podstawy działania sieci bezprzewodowych



Rodzaj zajęć: Wszechnica Popołudniowa
Tytuł: Podstawy działania sieci bezprzewodowych
Autor: dr inż. Dariusz Chaładyniak

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** – ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).

www.informatykaplus.edu.pl

kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa

www.wysi.edu.pl

rektorat@wysi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2009

Copyright © Warszawska Wyższa Szkoła Informatyki 2009

Publikacja nie jest przeznaczona do sprzedaży.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podstawy działania sieci bezprzewodowych



Dariusz Chaładyniak

Warszawska Wyższa Szkoła Informatyki

dchalad@wwsi.edu.pl

Streszczenie

Wykład dostarcza podstawowych informacji, niezbędnych do zrozumienia działania sieci bezprzewodowych, będących bardzo ciekawą alternatywą dla klasycznych rozwiązań przewodowych. Choć te sieci raczej nie wyprą całkowicie tych drugich, to jednak mogą stanowić istotne ich uzupełnienie. Wykład przedstawia działanie i przeznaczenie typowych technologii bezprzewodowych (Wi-Fi, IrDA, Bluetooth, WiMAX). Bardzo istotnym zagadnieniem przy konfigurowaniu sieci bezprzewodowych jest ich właściwe bezpieczeństwo. Poświęca się temu zagadnieniu sporo miejsca. Omawia się także popularne zjawiska warchalking'u i wardriving'u. Wykład kończy opis konfiguracji punktu dostępu oraz sieciowej karty bezprzewodowej.

Spis treści

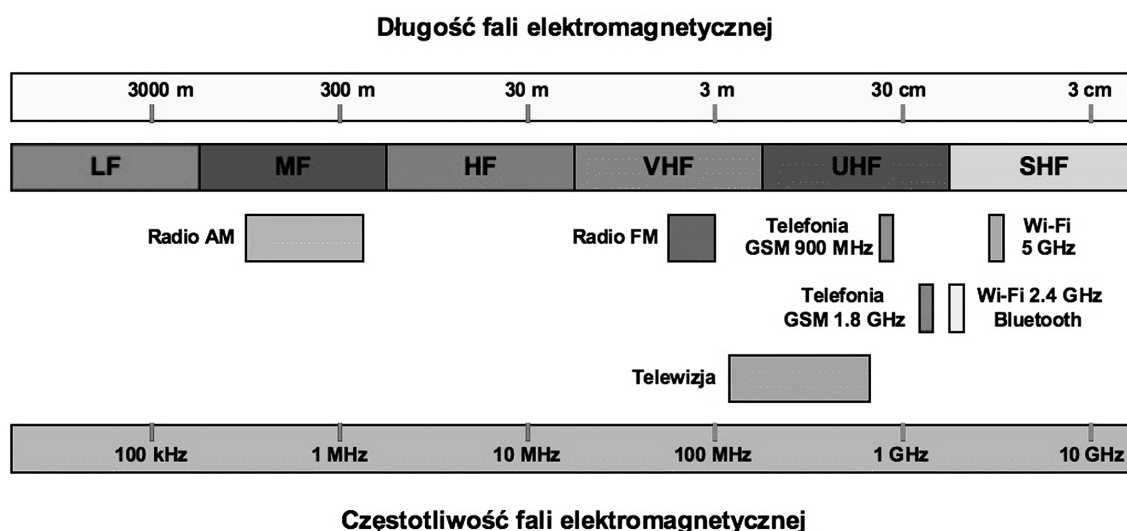
1. Wstęp do sieci bezprzewodowych.....	5
2. Technologia Wi-Fi.....	7
3. Technologia IrDA.....	12
4. Technologia Bluetooth	13
5. Technologia WiMAX	13
6. Warchalking, wardriving	14
7. Konfiguracja sieci bezprzewodowej	16
Literatura	29



1. WSTĘP DO SIECI BEZPRZEWODOWYCH

Sieci bezprzewodowe (ang. *wireless networks*) są bardzo ciekawą alternatywą dla klasycznych sieci przewodowych. Wszędzie tam, gdzie te drugie są mało ekonomicznym rozwiązaniem stosuje się sieci WLAN. Sieci bezprzewodowe jako medium transmisyjne wykorzystują fale radiowe (elektromagnetyczne) albo fale podczerwone.

Spektrum fal elektromagnetycznych



Rysunek 1.

Spektrum fal elektromagnetycznych

Spektrum fal elektromagnetycznych (rys. 1), często występujące również pod pojęciem **widma fal**, jest przedstawieniem fal w zależności od ich częstotliwość lub długość. Widmo fal elektromagnetycznych obejmuje takie fale, jak fale radiowe, mikrofałe, promieniowanie widzialne, promieniowanie podczerwone, ultrafioletowe, promieniowanie gamma, czy promieniowanie rentgenowskie.

W sieciach bezprzewodowych Wi-Fi i Bluetooth wykorzystuje się fale radiowe a w sieciach IrDA – fale w kanale podczerwieni. Na rys. 1 można zaobserwować, że dłuższym falom odpowiadają mniejsze częstotliwości i odwrotnie, krótszym falom odpowiadają wyższe częstotliwości. Częstotliwość fali wyrażana jest w hercach (Hz) i określa ilość cykli fali w ciągu sekundy.

Metody modulacji

Przesyłanie mowy, muzyki i innych dźwięków za pomocą fal radiowych polega na zmianie (czyli **modulacji**) sygnału prądu przemiennego tzw. nośnej sygnału. Każdy rodzaj bezprzewodowej sieci transmisji danych działa w określonym paśmie częstotliwości radiowych (2.4 GHz, 5 GHz).

W sieciach bezprzewodowych wykorzystuje się trzy rodzaje modulacji:

1. **DSSS** (ang. *Direct Sequence Spread Spectrum*) – technologia rozszerzonego widma z bezpośrednim szeregowaniem bitów. Strumienie danych są tu rozdzielane przy transmitowaniu z wykorzystaniem specjalnych bitów (zwanymi **bitami szumów**), a odbiornik musi dysponować układem deszyfrującym (który wykorzystuje tzw. *chipping code*, interpretując w odpowiedni sposób poszczególne strumienie danych). Cały proces polega na rozbiciu informacji na wiele „podbitów”, dzięki czemu pakiety są transmitowane przy użyciu dużo szerszego pasma przenoszenia danych niż w przypadku normalnej transmisji.
2. **FHSS** (ang. *Frequency Hopping Spread Spectrum*) – strumienie danych są przełączane z jednej częstotliwości na drugą (a każda częstotliwość to oddzielny kanał komunikacyjny), pozostając na każdej z nich nie dłużej niż 100 ms.



3. **OFDM** (ang. *Orthogonal Frequency Division Multiplexing*) – została tak zoptymalizowana, aby interfejs bezprzewodowy mógł transmitować dane w środowiskach pełnych zakłóceń, takich jak zatłoczone obszary miejskie.

Standardy sieci bezprzewodowych

Tabela 1.

Standardy sieci bezprzewodowych

Nazwa standardu	Częstotliwość radiowa	Zasięg sygnału	Maksymalna szybkość transmisji
802.11b	2.4 GHz	30 metrów	11 Mb/s
802.11a	5 GHz	30 metrów	54 Mb/s
802.11g	2.4 GHz	30 metrów	54 Mb/s
802.11n (proponowany)	2.4 GHz	50 metrów	540 Mb/s
802.15.1 Bluetooth	2.4 GHz	10 metrów	2 Mb/s

Sieci bezprzewodowe opierają się przede wszystkim na standardach z rodziny IEEE 802. IEEE. W tej rodzinie, sieci bezprzewodowych dotyczy grupa standardów IEEE 802.11. Rodzina 802.11 obejmuje trzy zupełnie niezależne protokoły skupiające się na kodowaniu (a, b, g). Pierwszym powszechnie zaakceptowanym standardem był 802.11b, potem weszły 802.11a oraz 802.11g. Standard 802.11n nie jest jeszcze oficjalnie zatwierdzony, ale coraz więcej sprzętu sieciowego jest kompatybilna z tą technologią.

Pierwszym standardem sieci radiowej był opublikowany w 1997 roku IEEE standard 802.11. Umożliwił on transmisję z przepustowością 1 oraz 2 Mb/s przy użyciu podczerwieni bądź też pasma radiowego 2.4 GHz. Urządzenia tego typu są już praktycznie nie stosowane.

Standard **802.11b** został zatwierdzony w 1999 roku. Pracuje w paśmie o częstotliwości 2.4 GHz. Umożliwia maksymalną teoretyczną szybkość transmisji danych do 11 Mb/s. Jego zasięg ograniczony jest do 30 metrów w pomieszczeniu i do 100 metrów w otwartej przestrzeni.

Standard **802.11a** został zatwierdzony w 1999 roku. Pracuje w paśmie częstotliwości 5 GHz. Jego maksymalna teoretyczna przepływność sięga 54 Mb/s.

Standard **802.11g** oficjalnie został zatwierdzony w 2003 roku. Pracuje podobnie jak standard 802.11g w paśmie o częstotliwości 2.4 GHz. Umożliwia osiągnięcie maksymalnej teoretycznej szybkości transmisji danych do 54 Mb/s. Zasięg jego działania w budynku ograniczony jest do 30 metrów natomiast w przestrzeni otwartej dochodzi do 100 metrów.

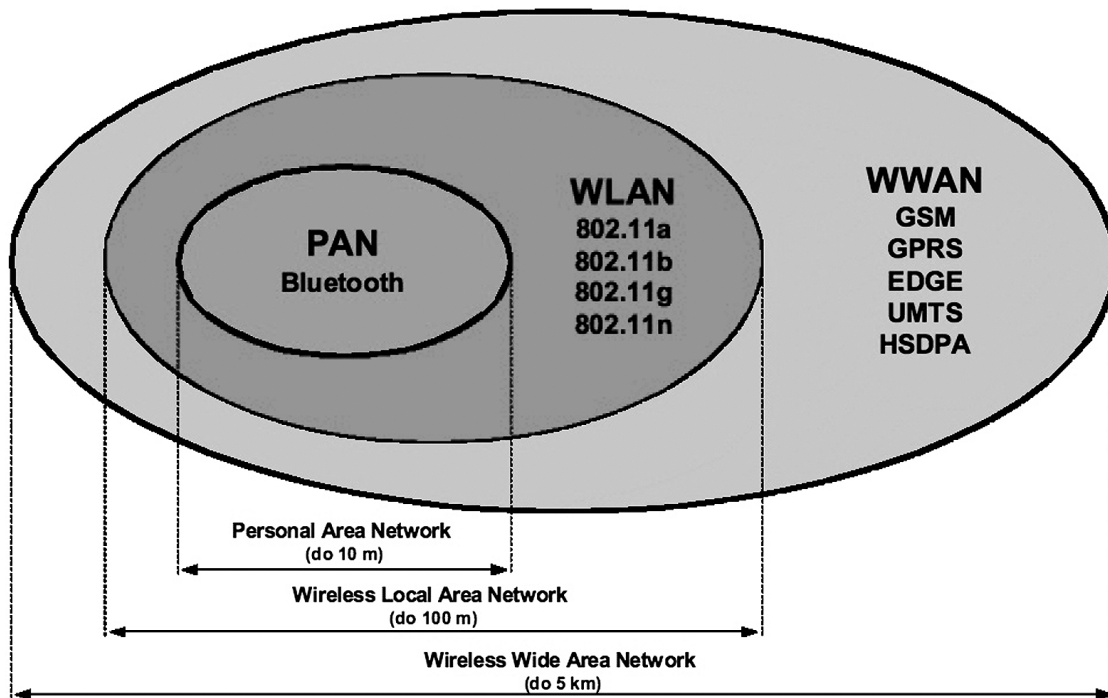
Najnowszy standard **802.11n** (oficjalnie jeszcze niezatwierdzony) będzie działać w paśmie radiowym o częstotliwości 2.4 GHz. Docelowo ma zapewnić przepływność przesyłu danych do 540 Mb/s. Zostanie również wydłużony jego zasięg działania do 50 metrów w pomieszczeniach. Standard ma ostatecznie zostać zatwierdzony w 2010 roku.

Podział zasięgu sieci bezprzewodowych

Pod względem zasięgu działania (patrz rys. 2) sieci bezprzewodowe możemy podzielić na trzy kategorie:

1. **Sieci PAN** (ang. *Personal Area Network*) – działają na odległości do 10 metrów. Jako przykład tej sieci można podać standard Bluetooth.
2. **Sieci WLAN** (ang. *Wireless Local Area Network*) – działają w zakresie do 100 metrów w otwartej przestrzeni. Przykłady tych sieci to standardy IEEE 802.11a/b/g/n.
3. **Sieci WWAN** (ang. *Wireless Wide Area Network*) – działają na odległości nawet do 5 kilometrów. To przede wszystkim systemy sieci telefonii komórkowej (GSM, GPRS, EDGE, UMTS, HSDPA).





Rysunek 2.
Podział zasięgu sieci bezprzewodowych

2. TECHNOLOGIA WI-FI

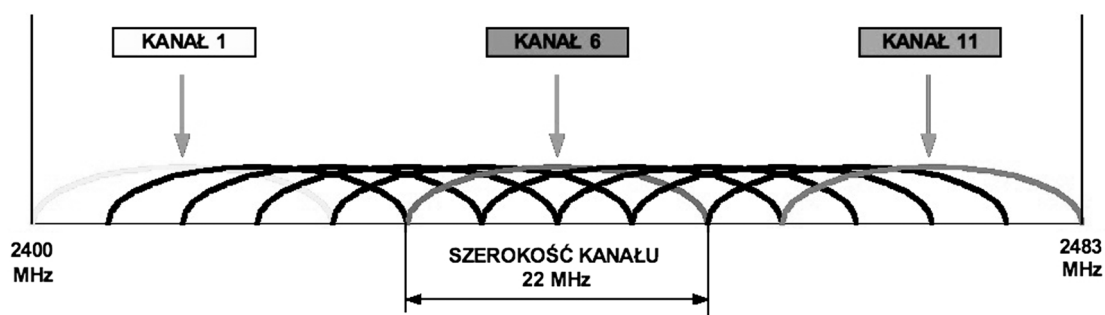


Rysunek 3.
Przykłady urządzeń wykorzystujących technologię Wi-Fi

Technologia Wi-Fi polega na bezprzewodowej łączności w dwóch zakresach częstotliwości: 2.4 GHz oraz 5 GHz.



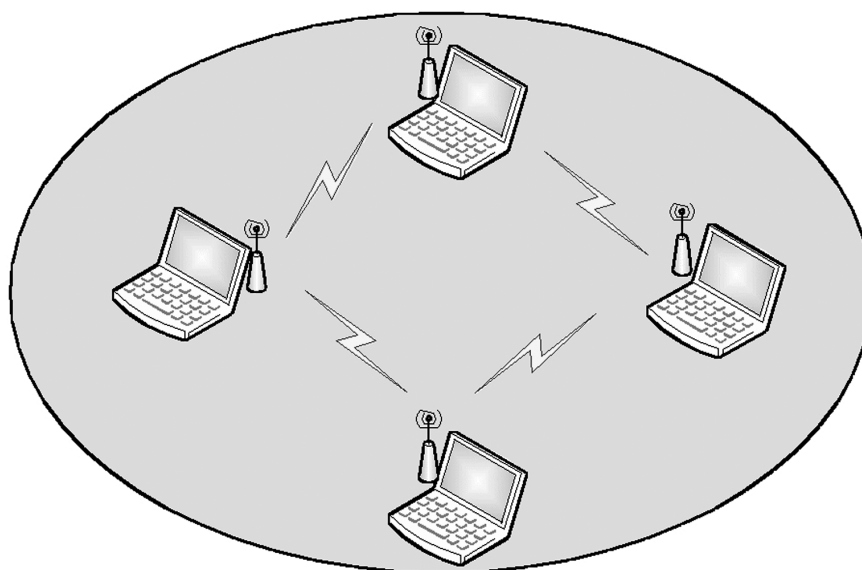
Kanały transmisyjne



Rysunek 4.
Kanały transmisyjne

Dokładna częstotliwość stosowana w określonej sieci bezprzewodowej zależy od wykorzystywanego kanału transmisyjnego. Na przykład w USA używa się 11 kanałów, w Polsce 13, w Japonii 14 a we Francji tylko 4. Aby zachować światowy standard, na całym świecie używa się tej samej numeracji kanałów czyli kanał nr 6 w Warszawie odpowiada tej samej częstotliwości co w Tokio czy Los Angeles. W przypadku wyjazdu za granicę może być konieczne przestawienie karty sieciowej na inny kanał, aczkolwiek robią one to automatycznie. Jeśli nie mamy pewności, z jakich kanałów można korzystać w danym kraju, wystarczy sprawdzić to w lokalnym urzędzie regulacyjnym. Niezależnie od tego można skorzystać z kanałów o numerach 10 i 11, które są dostępne na całym świecie (poza Izraelem).

Technologia sieci ad-hoc – IBSS

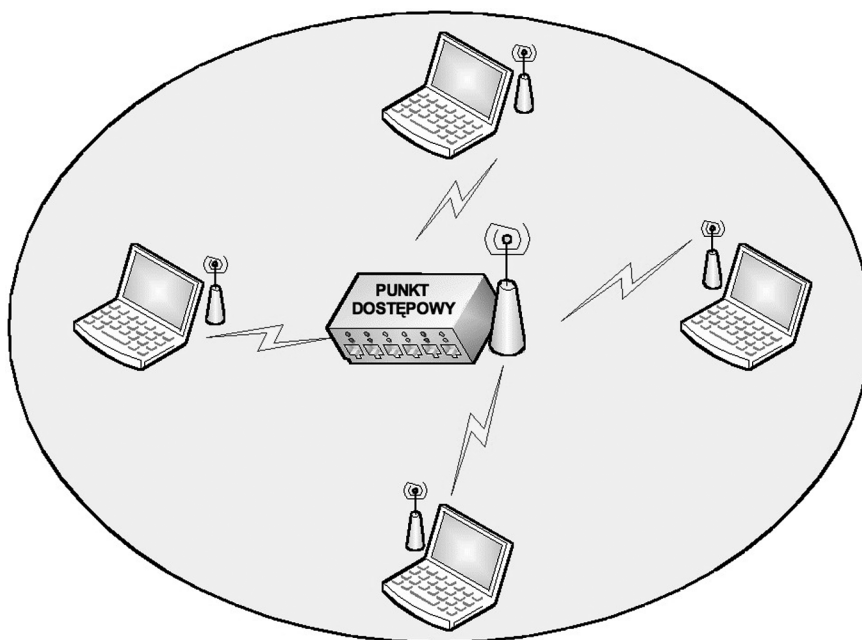


Rysunek 5.
Technologia sieci *ad-hoc*

Sieci Wi-Fi mogą działać w dwóch trybach pracy: *ad hoc* (równorzędnym) i infrastrukturalnym.

Sieć w **technologii *ad-hoc***, określana mianem **IBSS** (ang. *Independent Basic Service Set*) – rys. 5 – może być wykorzystana do wymiany danych między kilkoma komputerami bez użycia punktu dostępowego, ale i bez dostępu do istniejącej struktury sieciowej.

Technologia sieci infrastrukturalnej – BSS

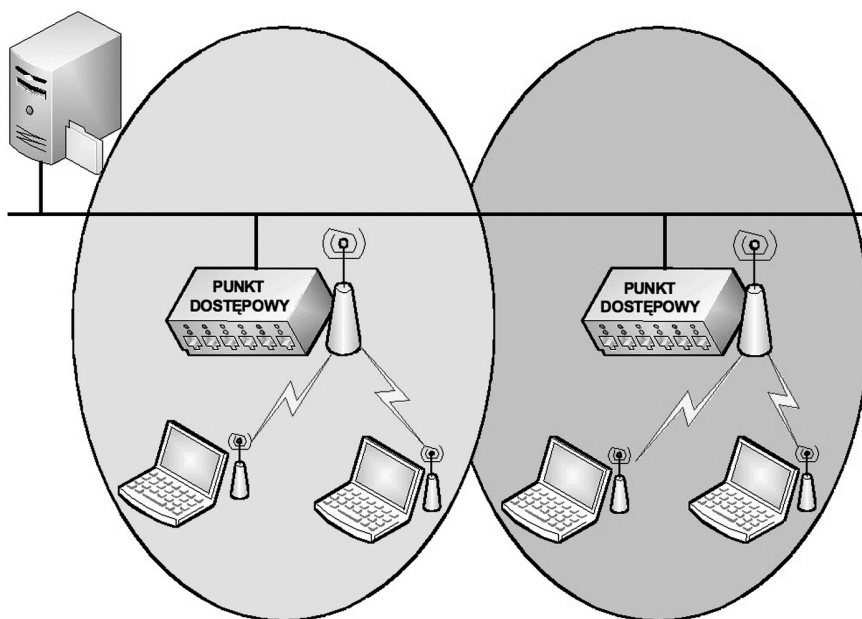


Rysunek 6.
Technologia sieci infrastrukturalnej BSS

W skład **sieci infrastrukturalnej** (rys. 6) wchodzi zwykle jeden lub więcej punktów dostępowych, które przyłączone są przeważnie do istniejącej przewodowej lokalnej sieci komputerowej. Każda stacja bezprzewodowa wymienia komunikaty i dane z punktem dostępowym, które są przekazywane dalej do innych węzłów sieci LAN lub WLAN.

Sieć infrastrukturalna, zawierająca tylko jedną stację bazową (punkt dostępowy, router), jest określana mianem **BSS** (ang. *Basic Service Set*).

Technologia sieci infrastrukturalnej – ESS

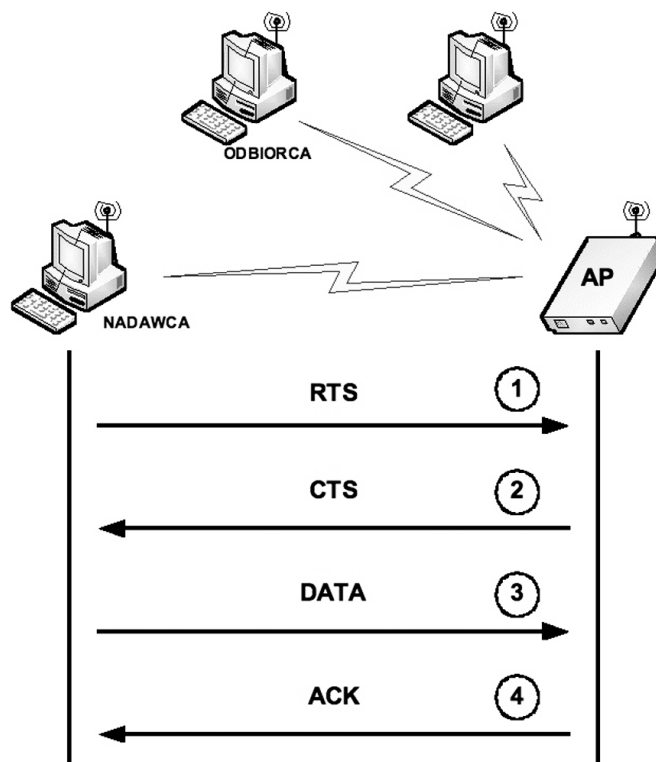


Rysunek 7.
Technologia sieci infrastrukturalnej ESS



Jeśli infrastrukturalna sieć bezprzewodowa korzysta z kilku punktów dostępowych, określa się ją mianem ESS (ang. *Extended Service Set*), rys. 7.

Metoda dostępu CSMA/CA



Rysunek 8. Schemat działania metody CSMA/CA

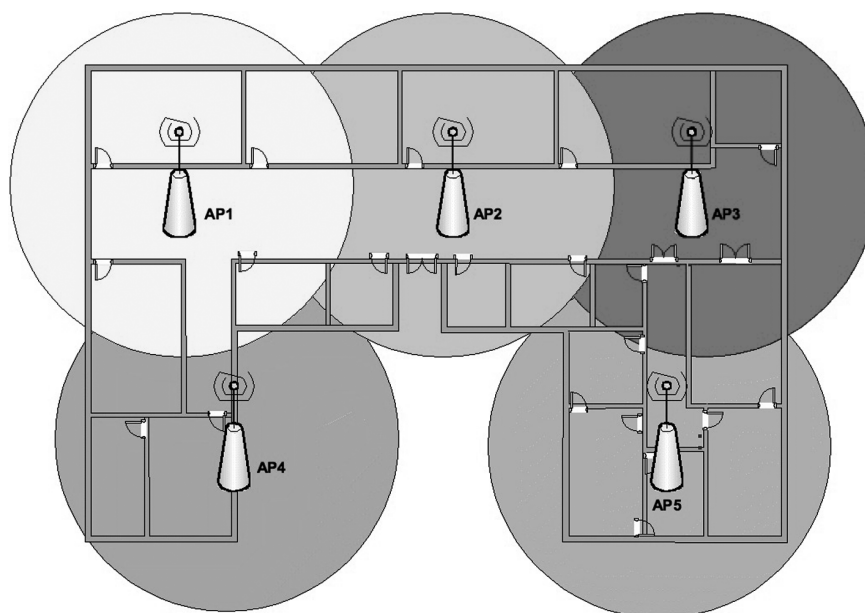
Metoda dostępu CSMA/CA (ang. *Carrier Sense with Multiple Access/Collision Avoidance*), stosowana w sieciach bezprzewodowych, polega na unikaniu kolizji.

W sieciach WLAN nie jest możliwe stosowanie używanego w sieciach LAN mechanizmu CSMA/CD (ang. *CSMA/Collision Detection*). Stacja próbująca nadawać nie może bowiem jednocześnie nasłuchiwać kanału, gdyż jej własny sygnał zagłuszałby wszystkie inne. Stacja chcąc nadawać prowadzi nasłuch pasma: jeśli przez określony czas nie wykryje transmisji, przełącza się w tryb gotowości do nadawania i czeka określony czas. Następnie, jeśli nadal nikt nie prowadzi nadawania, stacja rozpoczyna transmisję. Mechanizm ten jest określany skrótem CCA (ang. *Clear Channel Assessment*). Dodatkowo, dla każdej przesłanej ramki, do nadawcy musi dotrzeć potwierdzenie poprawności otrzymania danych, wysłane przez odbiorcę ACK (ang. *Acknowledge*).

Ponieważ stacje mogą być oddalone od siebie na odległość większą od swojego zasięgu nadawania, mechanizm CCA nie spełnia swoich zadań. W tym przypadku stacja nadawcza najpierw wysyła ramkę RTS (1) (ang. *Request To Send*), będącą informacją dla pozostałych stacji w jego zasięgu o zamiarze nadawania. Następnie Punkt dostępowy (AP) wysyła ramkę CTS (2) (ang. *Clear To Send*), informującą o gotowości do odbioru. Sygnał CTS dotrze do wszystkich stacji w zasięgu (wiadomość typu rozgłoszenie), czyli dotrze również do stacji odbiorczej, która dzięki temu zostanie powiadomiona o rozpoczynającej się transmisji. Po wymianie ramek RTS i CTS rozpoczyna się właściwa transmisja ramki (3) (DATA), której otrzymanie odbiorca potwierdza ramką ACK (4). Jeśli nadawca nie dostanie potwierdzenia ACK, musi ponowić transmisję danych.

Roźmieszczenie punktów dostępu

Jeden punkt dostępu (AP) może być całkowiec wystarczający do obsługi bezprzewodowej sieci lokalnej w domku jednorodzinny lub w małej firmie. Jeśli jednak sieć ma obejmować większy obszar (o średnicy po-



Rysunek 9.

Przykładowe rozmieszczenie punktów dostępu

nad 30 metrów), to są potrzebne dodatkowe punkty dostępu. Specyfikacja Wi-Fi zawiera funkcję *roamingu*, która automatycznie przestawia połączenie sieciowe z jednego punktu dostępu do innego, gdy jakość sygnału udostępnianego przez nowy punkt jest lepsza niż jakość sygnału obsługującego oryginalne połączenie.

Punkty dostępu powinny być tak rozmieszczone, aby ich obszary oddziaływania zachodziły na siebie ale jednocześnie działały na kanałach o innych numerach. Aby maksymalnie zmniejszyć zakłócenia pomiędzy nimi, każda para sąsiadujących ze sobą punktów dostępu powinna mieć przydzielone kanały odległe o co najmniej pięć numerów.

W większości przypadków, jeśli korzysta się z wielu punktów dostępu, powinny być one rozmieszczone w taki sposób, aby obszary oddziaływania sąsiednich punktów nakładały się na siebie w około 30 procentach, patrz rys. 9.

Bezpieczeństwo sieci Wi-Fi

Sieci bezprzewodowe są bardzo narażone na zagrożenia sieciowe. Narzędzia bezpieczeństwa w specyfikacji Wi-Fi nie są doskonałe, ale mogą w miarę skutecznie je zabezpieczyć. Poniżej przedstawiamy najważniejsze mechanizmy bezpieczeństwa w sieciach bezprzewodowych:

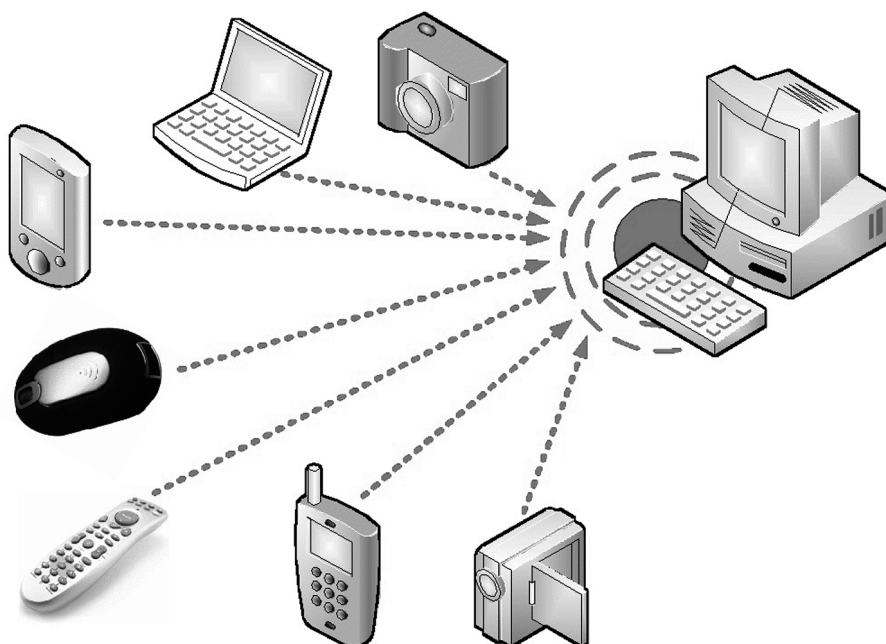
1. **Identyfikator SSID** (ang. *Service Set ID*) – wszystkie punkty dostępu oraz wszyscy klienci znajdujący się w sieci muszą mieć ustawiony taki sam SSID. Identyfikator ten zapewnia pewną bardzo ograniczoną formę kontroli dostępu, ponieważ trzeba go podać w trakcie nawiązywania połączenia do sieci Wi-Fi i jest on wartością tekstową, którą można dowolnie określić. Większość punktów dostępu rozsyła zwykle sygnał kontrolny, który rozgłasza identyfikator SSID danej sieci. Gdy karta sieciowa przeprowadza skanowanie sygnałów radiowych, wykrywa je i wyświetla listę znalezionych identyfikatorów SSID w swoim programie kontrolnym (można również tę funkcję wyłączyć).
2. **Szyfrowanie WEP** (ang. *Wired Equivalent Privacy*) – jest dostępne w każdym systemie działającym w standardzie Wi-Fi. Szyfrowanie to bazuje na współdzielonym kluczu szyfrującym o długości 40 lub 104 bitów oraz 24-bitowym wektorze inicjującym.
3. **Standard 802.1x** – scentralizowanie identyfikacji użytkowników, uwierzytelnianie, dynamiczne zarządzanie kluczami. Wszystkie te środki zapewniają dużo większe bezpieczeństwo w sieci niż kontrola dostępu wbudowana w protokół 802.11.

4. **Szyfrowanie WPA** (ang. *Wi-Fi Protected Access*) – znacznie bezpieczniejsze szyfrowanie niż WEP, ponieważ używa protokołu TKIP (ang. *Temporal Key Integrity Protocol*) w celu automatycznej zmiany klucza szyfrującego po upływie określonego czasu lub gdy nastąpi wymiana określonej liczby pakietów. Na szyfrowanie WPA składają się poniższe składniki:

- WPA = 802.1x + EAP + TKIP + MIC
- EAP (ang. *Extensible Authentication Protocol*)
- TKIP (ang. *Temporal Key Integrity Protocol*)
- MIC (ang. *Message Integrity Check*)

5. **Standard 802.11i** – zatwierdzony w lipcu 2004 roku, znany pod nazwą *Robust Security Networking*.

3 TECHNOLOGIA IRDA



Rysunek 10.
Przykłady urządzeń wykorzystujących technologię IrDA

W technologia IrDA (ang. *Infrared Data Association*) – rys. 10 – jest wykorzystywana silnie skupiona wiązka światła w paśmie podczerwieni (850-900 nm). Koniecznym warunkiem zastosowania tej technologii jest bezpośrednia widoczność nadajnika i odbiornika.

Właściwości technologii IrDA

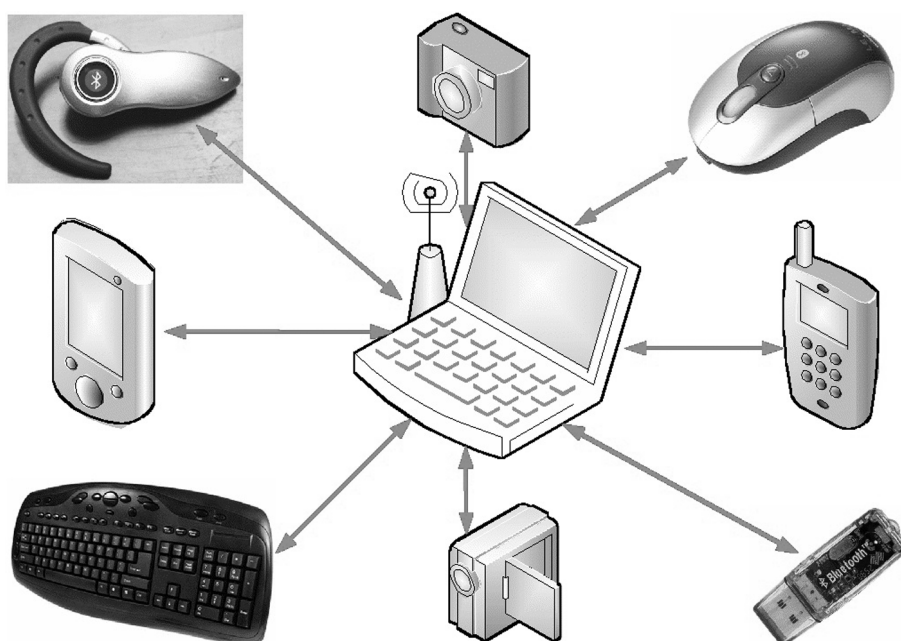
Tabela 2.
Wybrane parametry technologii IrDA

Tryb transmisji	Szybkość transmisji
Serial InfraRed SIR	2.4 - 115.2 kbps
Medium InfraRed MIR	0.576 - 1.15 Mbps
Fast InfraRed FIR	1.15 - 4 Mbps
Very Fast InfraRed VFIR	16 Mbps

Podstawowe właściwości technologii IrDA to:

1. Prosta i tania implementacja;
2. Mały pobór mocy;
3. Połączenie typu punkt-punkt;
4. Długość fali świetlnej: 850 – 900 nm;
5. Zasięg: do 10 metrów;
6. Kąt wiązki transmisji: 30°.

4 TECHNOLOGIA BLUETOOTH



Rysunek 11.

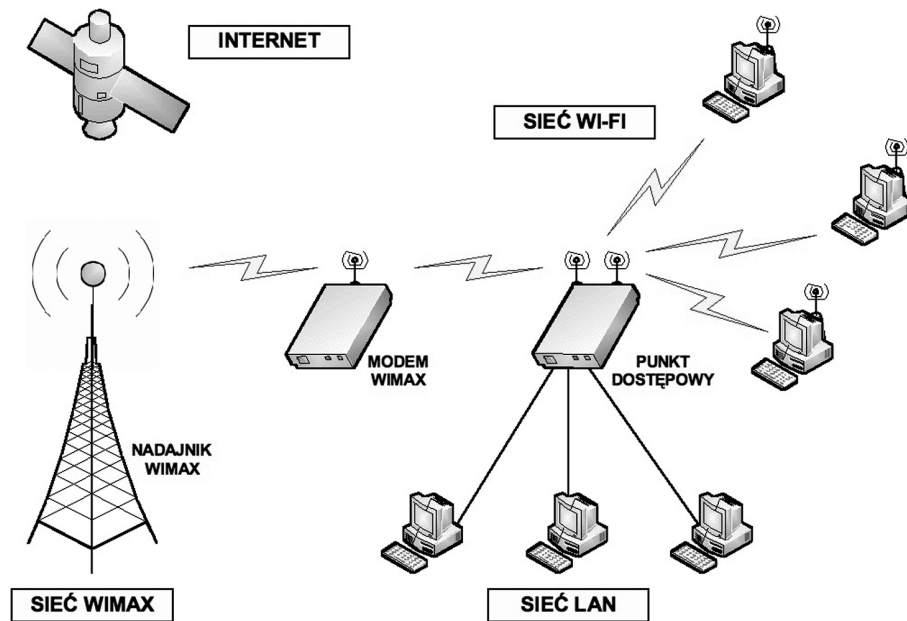
Przykłady urządzeń wykorzystujących technologię Bluetooth

Technologia Bluetooth (rys. 11) jest globalną inicjatywą bezprzewodowego dostępu radiowego grupy producentów: Ericsson, IBM, Intel, Nokia i Toshiba. Standard Bluetooth powstał w 1994 roku w Szwecji. Jego nazwa pochodzi od przydomka żyjącego w X wieku duńskiego króla Haralda I – *Blaatand* (czyli Sinozęby).

Technologia Bluetooth jest standardem połączeń radiowych o ograniczonym zasięgu, między telefonami komórkowymi, komputerami przenośnymi, urządzeniami peryferyjnymi (klawiatury, myszy, monitory, drukarkami), a także audiowizualnymi (piloty, odbiorniki TV i radiowe). W Bluetooth stosuje się bezkierunkowe łącze radiowe o niewielkim zasięgu (do 10 m), o częstotliwościach pracy w paśmie 2,402-2,480 GHz. Możliwa jest komunikacja między różnymi urządzeniami przenośnymi (maks. 256) z przepływnością do 1 Mb/s.

5 TECHNOLOGIA WiMAX

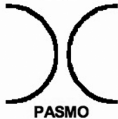
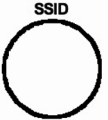

Technologia WiMAX (ang. *Worldwide Interoperability for Microwave Access*) – rys. 12 – to bezprzewodowa metoda szerokopasmowej transmisji danych na dużych obszarach geograficznych. Jest to bezprzewodowa sieć miejska, w której zazwyczaj stosuje się jedną lub więcej stacji bazowych, z których każda dystrybuje sygnał drogą radiową w promieniu do 50 km. Oficjalnie technologia WiMAX jest opisana w specyfikacji IEEE 802.16d. Każdy dostawca usługi WiMAX korzysta z koncesjonowanych częstotliwości z zakresu pomiędzy 2 GHz a 11 GHz. Łącze WiMAX może teoretycznie przesyłać dane z przepływnością do 70 Mb/s.



Rysunek 12.
Schemat działania technologii WiMAX

6 WARCHALKING, WARDRIVING

Znaki naznaczonego dostępu – oryginalne

KLUCZ	SYMBOL
WEZEL OTWARTY	SSID  PASMO
WEZEL ZAMKNIĘTY	SSID  PASMO
WEZEL WEP	PUNKT DOSTĘPOWY SSID  PASMO

Rysunek 13.
Oryginalne znaki naznaczonego dostępu

Anglik Matt Jones zaczął w czerwcu 2002 roku rysować w Londynie kredą na chodnikach i ścianach domów symbole identyfikujące miejsca, do których dochodzą sygnały sieci bezprzewodowych IEEE 802.11b i jest możliwe uzyskanie 'bezpłatnego' dostępu do Internetu. Na rys. 13 przedstawiono trzy oryginalne znaki naznaczonego dostępu.

Znaki naznaczonego dostępu – propozycja

KLUCZ	SYMBOL	KLUCZ	SYMBOL
NIEOGRANICZONY DOSTĘP		PUNKT DOSTĘPOWY Z FILTROWANIEM ADRESÓW MAC	
DOSTĘP OTWARTY Z OGRANICZENIAMI		PŁĄC ZA DOSTĘP DO PUNKTU DOSTĘPOWEGO	
PUNKT DOSTĘPOWY Z WEP		PUNKT DOSTĘPOWY Z WIELOMA RÓŻNYMI KONTROLAMI DOSTĘPU	
PUNKT DOSTĘPOWY Z ZAMKNIĘTYM ESSID		WABIK	

Rysunek 14.
Propozycja znaków naznaczonego dostępu

Na rys. 14 przedstawiono propozycję nowych znaków naznaczonego dostępu do sieci Internet. Znaki te są malowane za pomocą kredy, by osoba oznaczająca punkt dostępu nie została posądzona o wandalizm, jak to bywa w przypadku graffiti wykonanego sprayem (kredę łatwo da się zmyć).

Wardriving



Rysunek 15.
Przykład wardriving'u

Termin wardriving określa przede wszystkim techniki namierzania sieci bezprzewodowych, najczęściej wykorzystując do tego celu samochód. Jako narzędzi używa się laptopa wyposażonego w kartę Wi-Fi, antenę wzmacniającą oraz odpowiednie oprogramowanie. Metoda ta wiąże się nierozwalnie z techniką warchal-



kingu, czyli oznaczania ścian budynków lub chodników w miejscach, gdzie rozpoznany został otwarty punkt dostępowy. Istnieje także odmiana wardrivingu, zwana warstrolling, polegająca na pieszym przemieszczaniu się po mieście w celu odkrycia sieci Wi-Fi.

Najbardziej popularnym programem używanym przez amatorów rozpoczynających swą przygodę z wardriving jest Netstumbler wykorzystujący metody wykrywania za pomocą skanowania aktywnego. Polega ona na oczekiwaniu odpowiedzi w postaci ramek Probe Response, na uprzednio wysłane ramki Probe Request. Dzięki nim uzyskuje się takie informacje, jak identyfikator ESSID, numer kanału, oraz dotyczące mechanizmów WEP, natężenia ruchu i prędkości. Ta metoda jest możliwa jedynie do zastosowania w sieciach otwartych, sieci zamknięte bowiem nie odpowiadają na takie zapytania, a jej funkcjonalność może zostać znacznie ograniczona przez administratora sieci, który stosuje filtrowanie ramek niosących identyfikator ESSID. Oprócz tego użycie narzędzi tego typu jest ograniczone z powodu wymogu fizycznej obecności w obrębie zasięgu nadawania karty. Programy, takie jak Netstumblera, nie analizują również ruchu sieciowego, rejestrują jedynie ruch ramek odpowiedzi, przez co osobę go stosującą można bardzo szybko wykryć. Znacznie częściej są używane programy działające w trybie monitorowania sieci, takie jak Kismet, Airtraf, WifiScanner czy Wellenreiter.

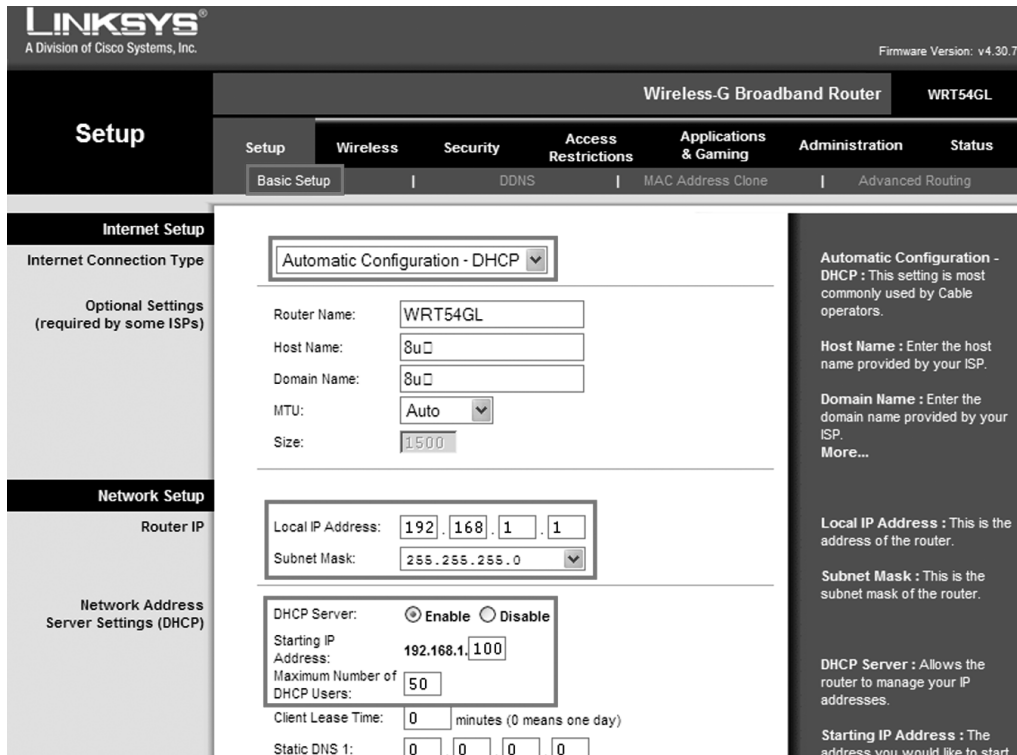
7 KONFIGURACJA SIECI BEZPRZEWODOWEJ

Konfiguracja punktu dostępu



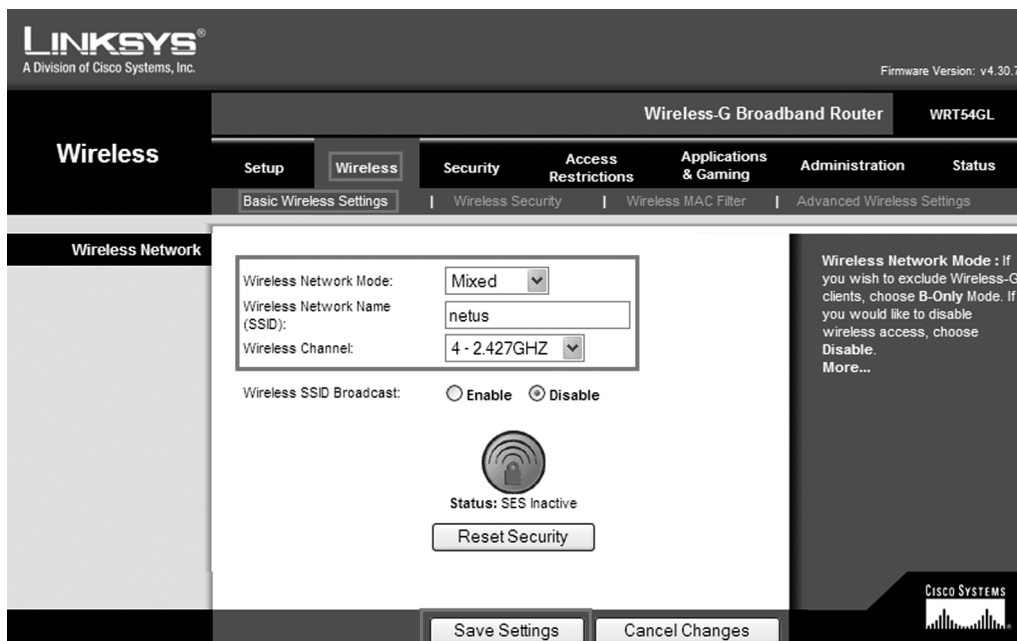
Rysunek 16.
Logowanie do konfiguracji punktu dostępu.

Aby móc korzystać z usług sieciowych w trybie bezprzewodowym należy właściwie skonfigurować zarówno punkt dostępu, jak i kartę sieciową Wi-Fi. Pokazujemy to na kolejnych ilustracjach. Większość współczesnych punktów dostępu (routerów) można skonfigurować poprzez przeglądarkę internetową. W jej górnym pasku (rys. 16) należy wpisać adres IP punktu dostępu (w naszym przypadku 192.168.1.1). Pojawi się wówczas zakładka logowania (oczywiście wcześniej należy utworzyć konto użytkownika i przypisać mu hasło). Po wpisaniu nazwy użytkownika i podaniu hasła klikamy na przycisku OK.



Rysunek 17.
Podstawowa konfiguracja punktu dostępu

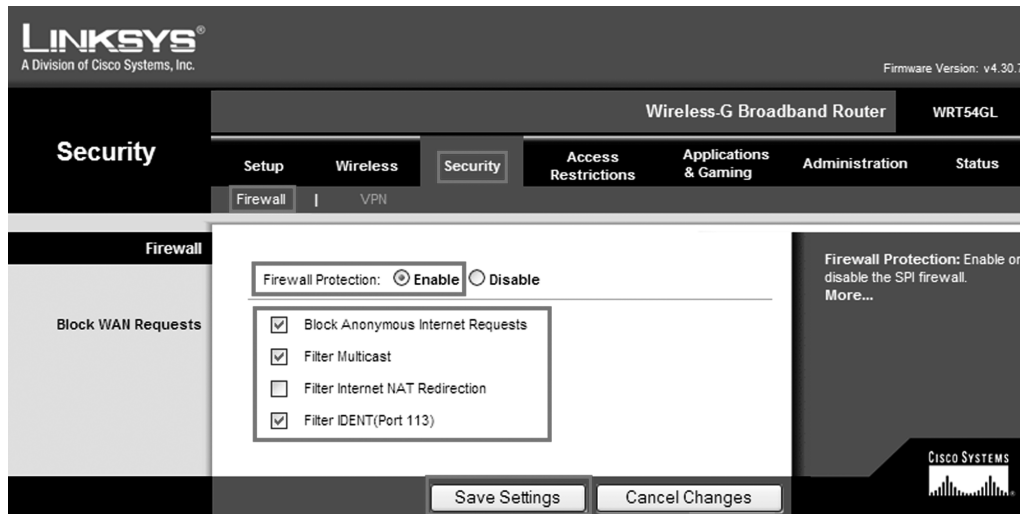
Po poprawnym zalogowaniu się zgłasza się panel konfiguracyjny punktu dostępu (rys. 17). W kategorii Setup wybieramy zakładkę Basic Setup, w której możemy określić między innymi: typ konfiguracji serwera DHCP, lokalny adres IP routera (punktu dostępu) i jego maskę podsieci a także zaznaczyć, czy serwer DHCP jest dostępny czy nie, a jeśli tak, to przeznaczyć dla niego odpowiednią pulę adresów IP poczynając od wybranej wartości.



Rysunek 18.
Konfiguracja trybu sieci bezprzewodowej, jej nazwy oraz kanału transmisyjnego

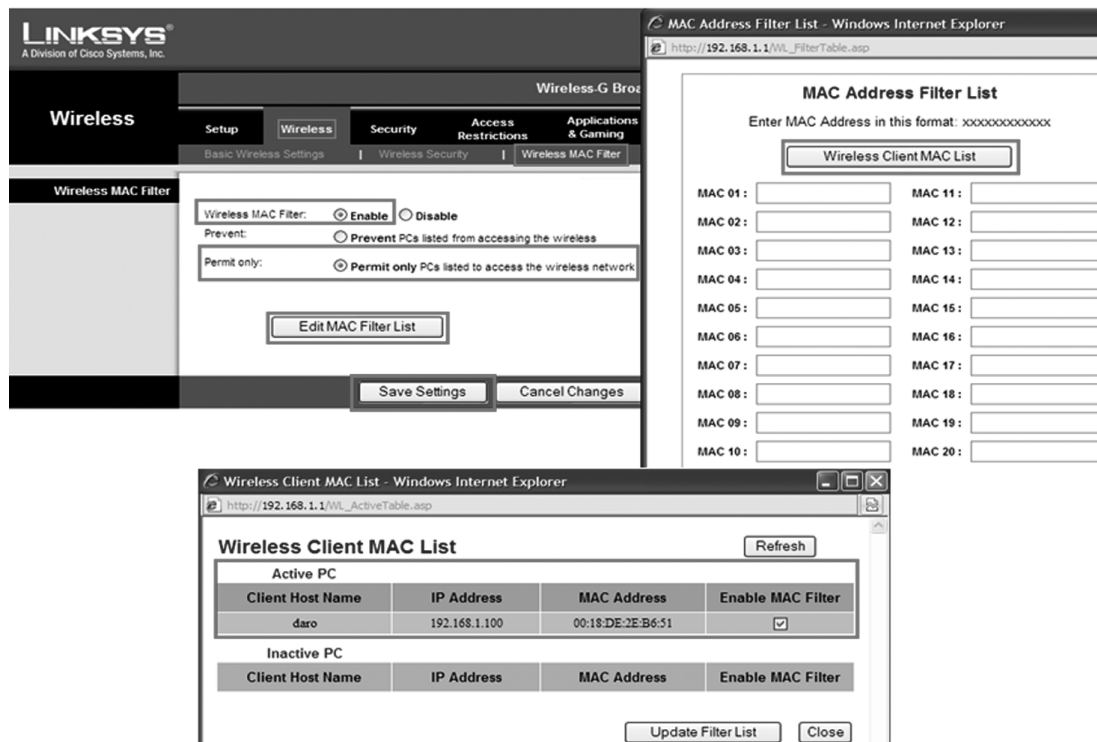


W kategorii Wireless (rys. 18) wybieramy zakładkę Basic Wireless Settings, w której określamy właściwy tryb sieci bezprzewodowej, jej nazwę (SSID) oraz numer kanału transmisyjnego i częstotliwość jego pracy. Po dokonaniu zmian, klikamy na przycisku Save Settings, aby zapisać ustawienia, albo na przycisku Cancel Changes, aby anulować zmiany.



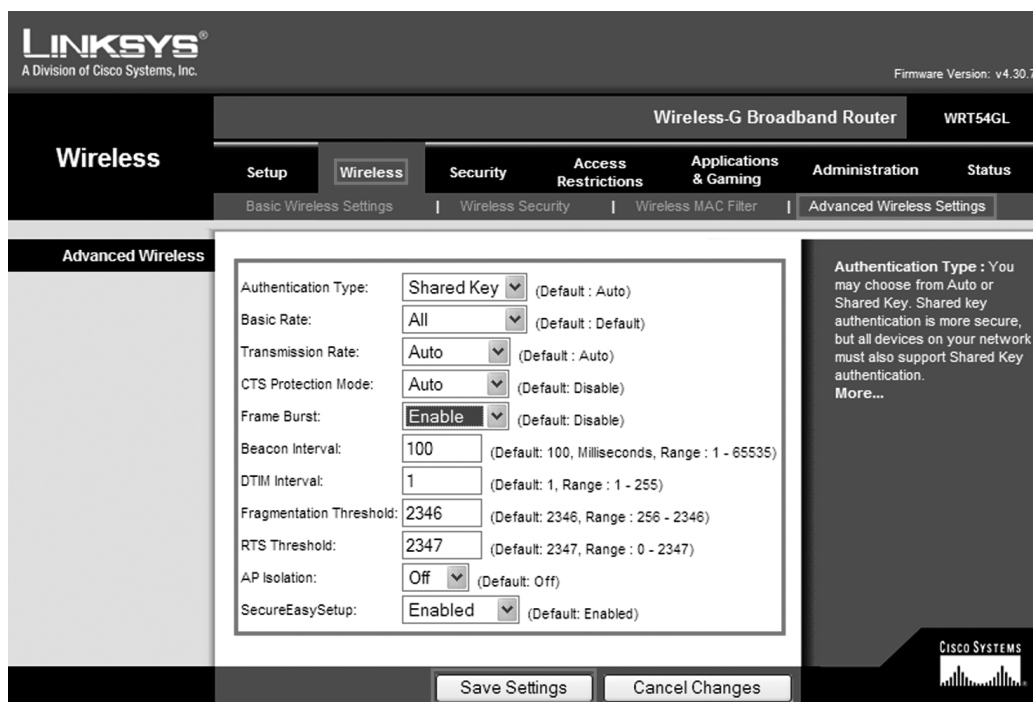
Rysunek 19. Konfiguracja zabezpieczeń sieci bezprzewodowej

Natomiast w zakładce Wireless Security (rys. 19) konfigurujemy zabezpieczenia sieci bezprzewodowej. W naszym przypadku jako tryb zabezpieczeń został wybrany bardzo silny protokół szyfrowania WPA2 wykorzystujący algorytm AES (ang. *Advanced Encryption Standard*). W polu WPA Shared Key można wpisać klucz współdzielony, a w polu Group Key Renewal – podać częstotliwość odnawiania tego klucza, czyli jak często router (punkt dostępu) powinien zmieniać klucze szyfrujące. Podobnie, albo zatwierdzamy zmiany (przycisk Save Settings), albo anulujemy (Cancel Changes).



Rysunek 20. Konfiguracja filtrowania adresów MAC

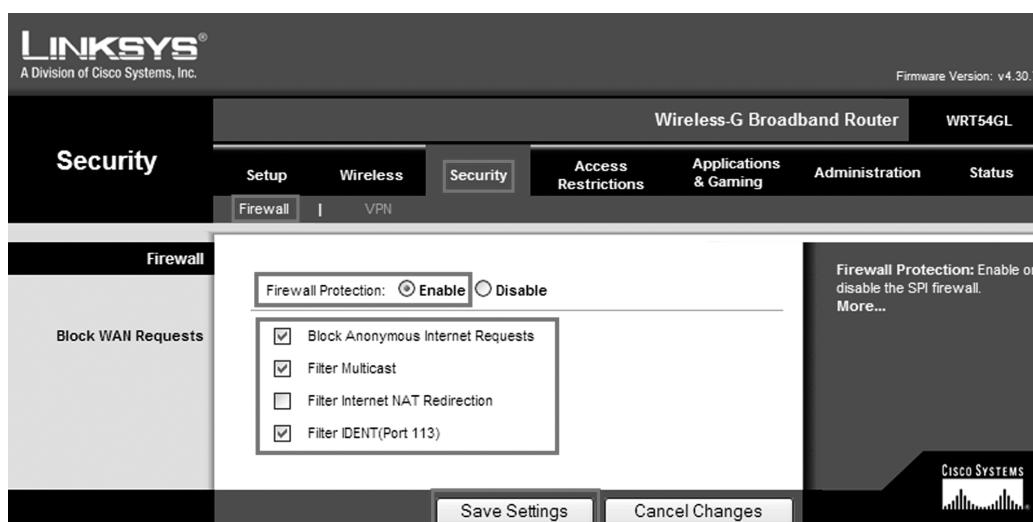
Z kolei w zakładce Wireless MAC Filter (rys. 20) możemy zaznaczyć opcję filtrowania adresów MAC i pozwolić korzystać z sieci bezprzewodowej tylko tym hostom, których adresy MAC na ich kartach sieciowych znajdują się na odpowiedniej liście.



Rysunek 21.

Konfiguracja zaawansowanych zabezpieczeń sieci bezprzewodowej

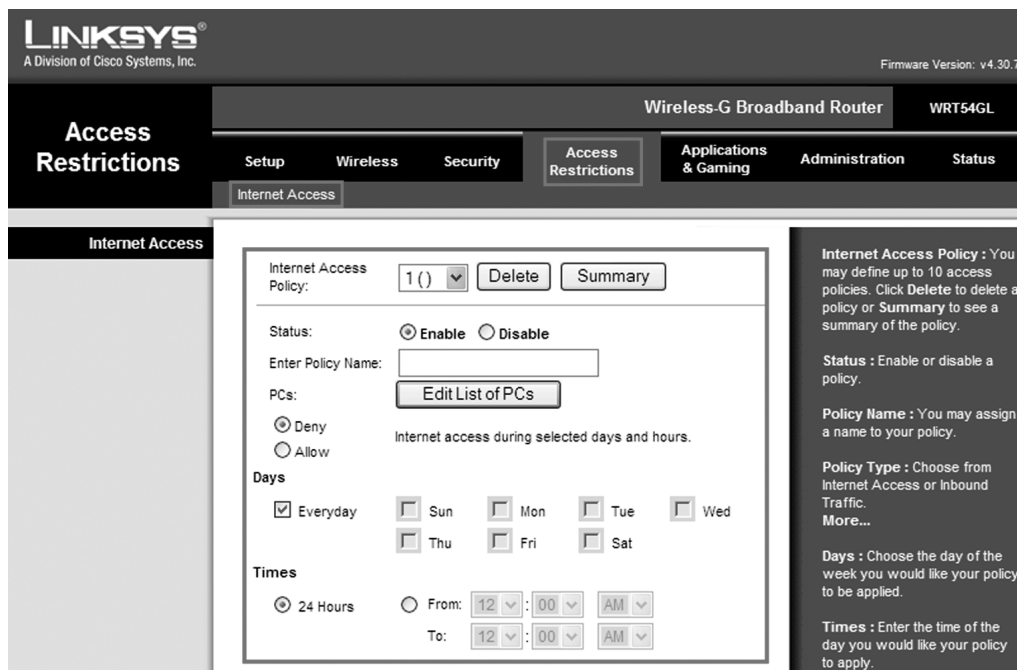
W kolejnej zakładce Advanced Wireless Settings w kategorii Wireless (rys. 21) możemy bardzo szczegółowo zdefiniować poszczególne elementy zabezpieczeń sieci bezprzewodowej.



Rysunek 22.

Konfiguracja ściany ogniowej

W kategorii Security wybieramy zakładkę Firewall (rys. 22), w której możemy uaktywnić ochronę sieci bezprzewodowej poprzez konfigurację ściany ogniowej.



Rysunek 23.
Konfiguracja dostępu do sieci Internet

W kategorii Access Restrictions (rys. 23) wybieramy zakładkę Internet Access, w której możemy określić politykę dostępu do sieci Internet. Dostępne opcje dają mnóstwo możliwości precyzyjnego określenia, które stacje robocze, kiedy i w jakim czasie mogą korzystać z internetu bądź też nie.



Rysunek 24.
Konfiguracja hasła dostępu do routera (punktu dostępu)

Z kolei w zakładce Management w kategorii Administration (rys. 24) określamy hasło dostępu do routera (punktu dostępu), czyli to hasło, które podaliśmy logując się do konfiguracji punktu dostępu.

Możemy również zaznaczyć, czy chcemy zarządzać punktem dostępu zdalnie czy tylko lokalnie.

The screenshot shows the Linksys router status page. The main navigation bar includes Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Router' sub-tab is selected. The 'Router Information' section displays the following details:

Firmware Version:	v4.30.7, Jun. 20, 2006
Current Time:	Tue, 28 Jul 2009 13:53:40
MAC Address:	00:1C:10:A4:1B:66
Router Name:	WRT54GL
Host Name:	8u
Domain Name:	8u
Login Type:	Automatic Configuration - DHCP
IP Address:	10.0.0.11
Subnet Mask:	255.0.0.0
Default Gateway:	10.0.0.1
DNS 1:	10.0.0.1
DNS 2:	
DNS 3:	
MTU:	1500

The 'Internet' section shows the 'Configuration Type' as Automatic Configuration - DHCP. A 'Refresh' button is located at the bottom right of the page.

Rysunek 25.

Podgląd podstawowych informacji o konfiguracji punktu dostępu

W zakładce Router w kategorii Status (rys. 25) możemy odczytać informacje o routerze (punkcie dostępu), takie jak: wersja oprogramowania sprzętowego, bieżący czas, adres sprzętowy (MAC) routera i jego nazwę. Ponadto możemy zapoznać się z konfiguracją adresów IP.

The screenshot shows the Linksys router status page with the 'Wireless' sub-tab selected. The 'Wireless' section displays the following details:

MAC Address:	00:1C:10:A4:1B:67
Mode:	Mixed
SSID:	netus
DHCP Server:	Enabled
Channel:	4
Encryption Function:	Disabled

The 'Refresh' button is visible at the bottom right of the page.

Rysunek 26.

Zbiorcze podsumowanie konfiguracji sieci bezprzewodowej

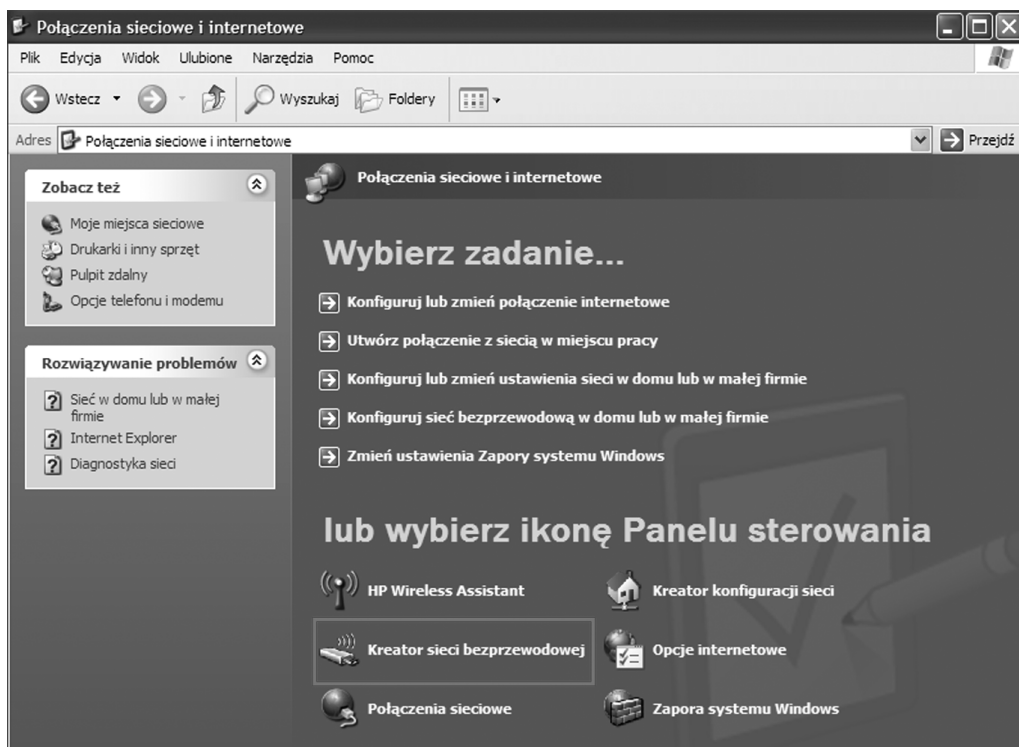
I wreszcie w zakładce Wireless w kategorii Status (rys. 26) otrzymujemy zbiorcze podsumowanie najważniejszych ustawień konfiguracyjnych naszej sieci bezprzewodowej – adres MAC punktu dostępu, tryb jego pracy, jego nazwę, dostępność serwera DHCP, numer kanału transmisyjnego oraz czy zostały uaktywnione funkcje szyfrujące przepływ danych.

Konfiguracja karty sieciowej Wi-Fi



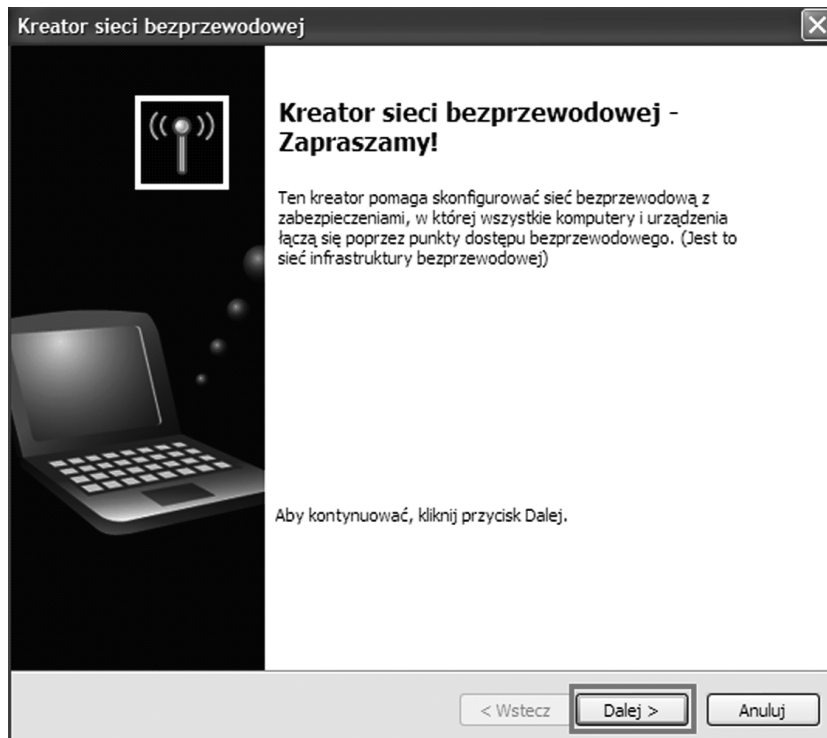
Rysunek 27.
Wybór kategorii – połączenia sieciowe i internetowe

Po skonfigurowaniu punktu dostępu należy skonfigurować kartę sieciową Wi-Fi. W Panelu sterowania dwukrotnie klikamy na opcji Połączenia sieciowe i internetowe (rys. 27), następnie dwukrotnie klikamy na ikonie Kreator sieci bezprzewodowej (rys. 28), co prowadzi nas do okna Kreatora sieci bezprzewodowej, w którym klikamy na przycisku dalej (rys. 29).

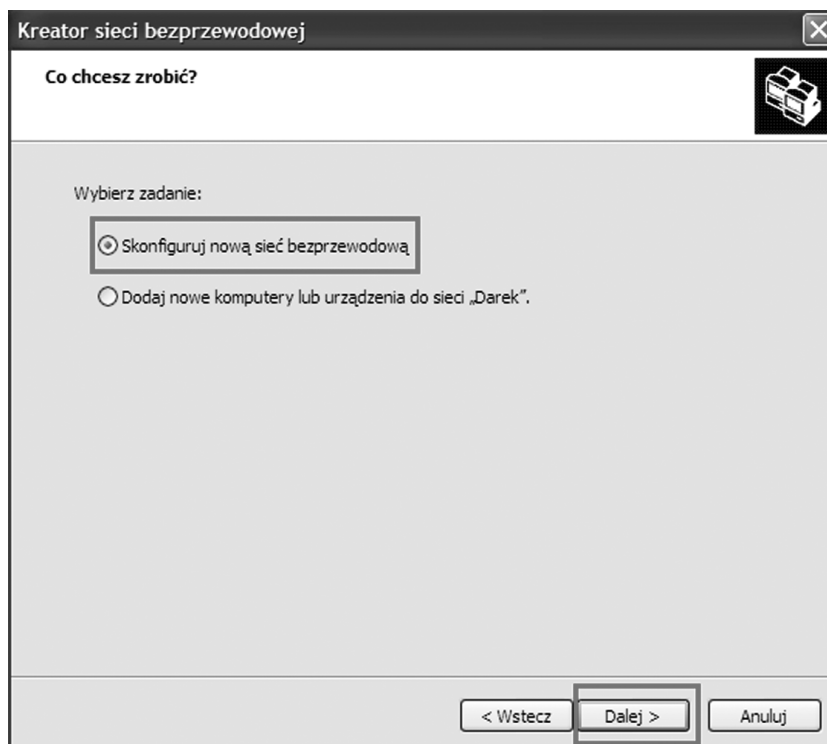


Rysunek 28.
Wybór kreatora sieci bezprzewodowej



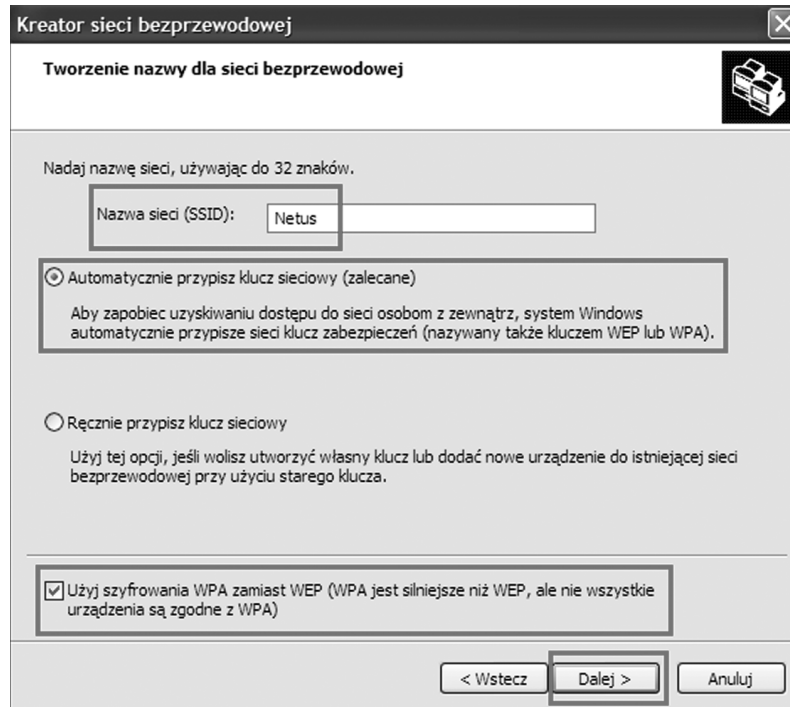


Rysunek 29.
Zgłoszenie się kreatora sieci bezprzewodowej



Rysunek 30.
Wybór konfiguracji nowej sieci bezprzewodowej

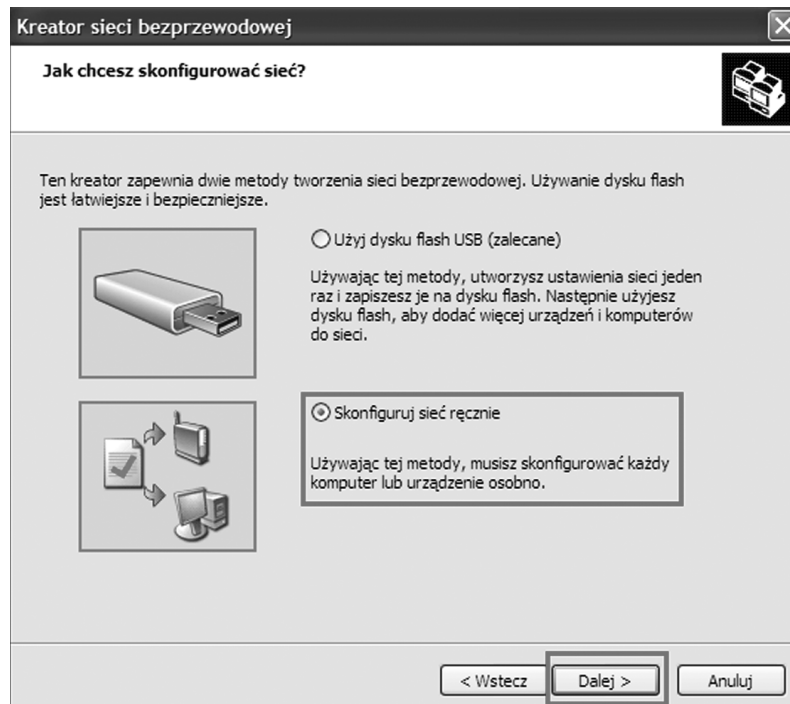
W następnym kroku (rys. 30) musimy wybrać jedno z dwóch dostępnych zadań – Skonfiguruj nową sieć bezprzewodową lub Dodaj nowe komputery lub urządzenia do sieci Darek (w naszym przypadku). Wybieramy opcję pierwszą a następnie klikamy na przycisku Dalej.



Rysunek 31.

Tworzenie nazwy dla sieci bezprzewodowej

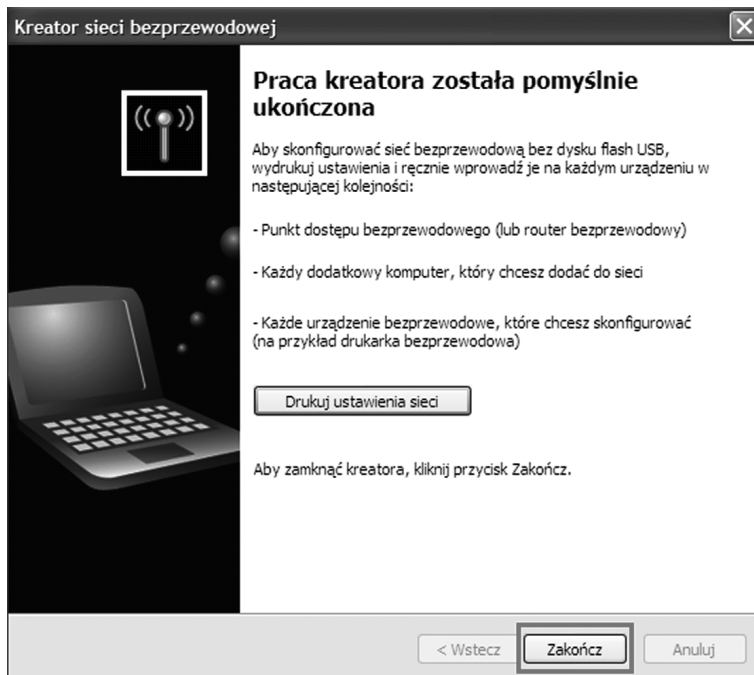
W procesie tworzenia nowej sieci bezprzewodowej (rys. 31) musimy najpierw podać dla niej nazwę (maksymalnie 32 znaki), a następnie zaznaczyć, jaką formę klucza sieciowego chcemy ustawić (automatycznie czy ręcznie). Wybieramy pierwszą opcję a ponadto zaznaczamy Użyj szyfrowania WPA zamiast WEP (WPA jest silniejsze niż WEP, ale nie wszystkie urządzenia są zgodne z WPA). Następnie klikamy na przycisku Dalej.



Rysunek 32.

Wybór metody konfiguracji sieci bezprzewodowej

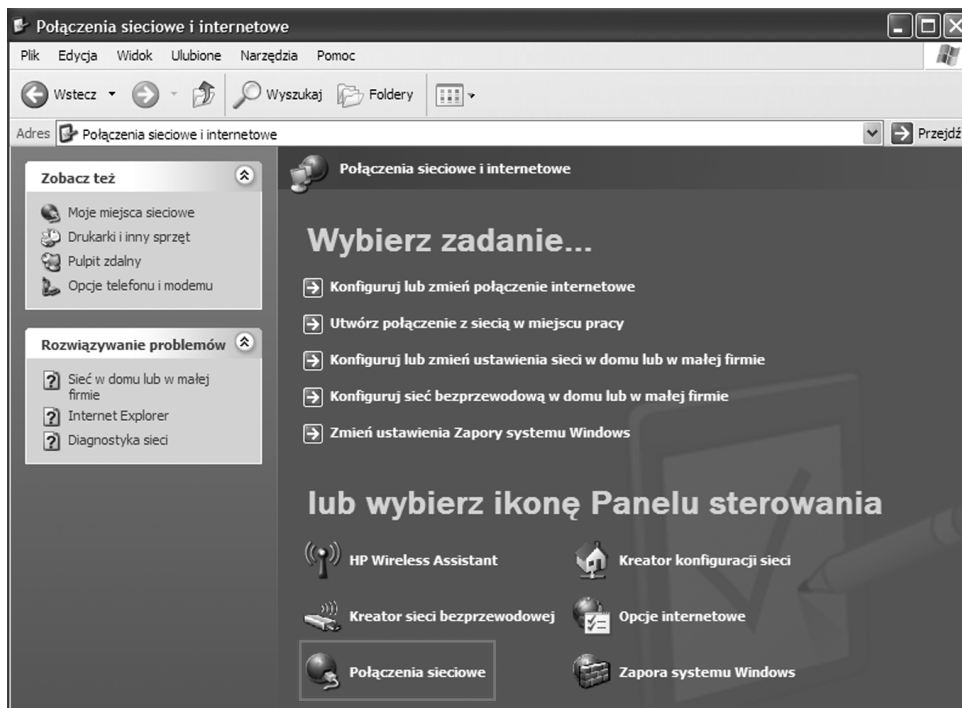
W kolejnym kroku (rys. 32) możemy określić sposób skonfigurowania sieci bezprzewodowej. Mamy do wyboru albo użycie dysku flash, albo skonfigurowanie ręczne. Z uwagi na to, że konfigurujemy małą sieć komputerową, wybieramy opcję drugą a następnie klikamy na przycisku Dalej.



Rysunek 33.

Koniec pracy kreatora sieci bezprzewodowej

Zwieńczenie dzieła jest pokazane na rys. 33 – oznajmienie, że praca kreatora została pomyślnie ukończona. Możemy skorzystać z dostępnej opcji i wydrukować ustawienia sieci. Aby zamknąć kreatora sieci bezprzewodowej, klikamy na przycisku Zakończ.

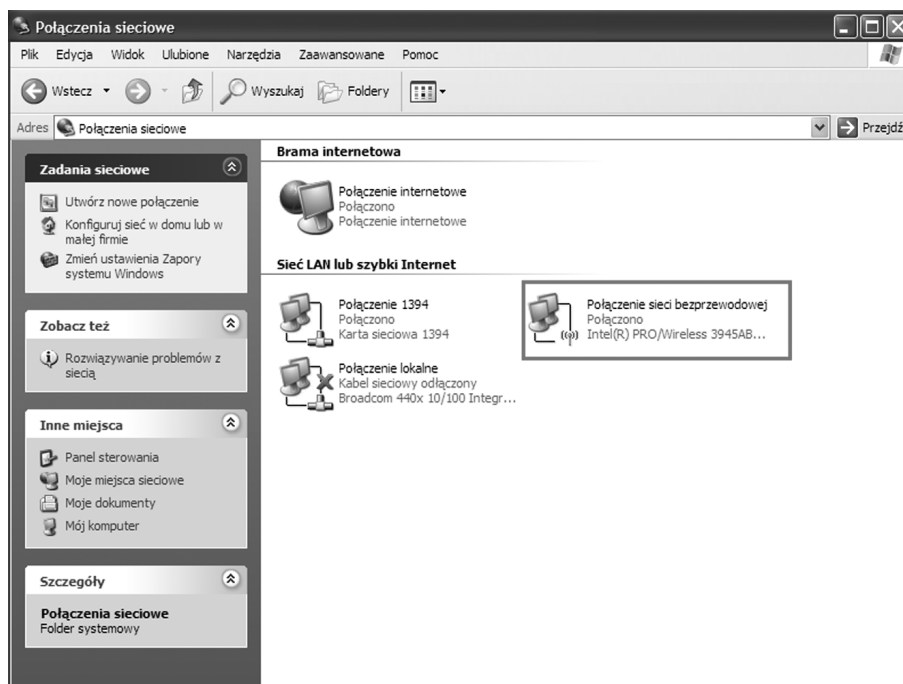


Rysunek 34.

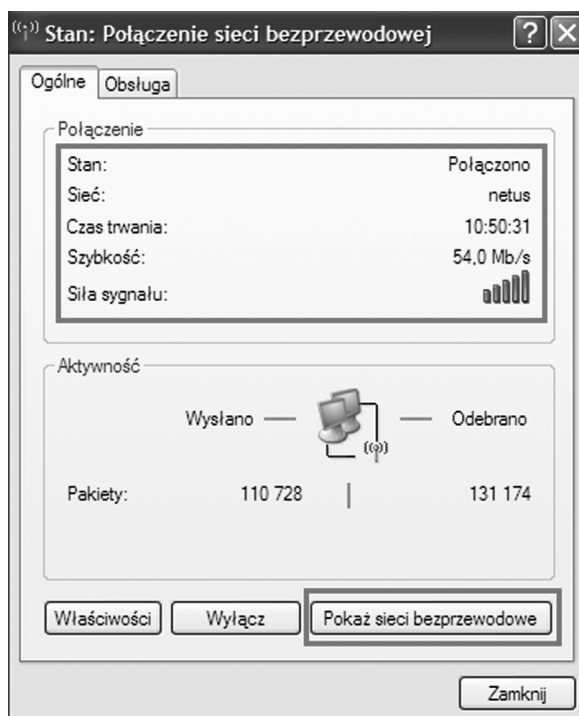
Pierwszy krok do konfiguracji karty sieciowej Wi-Fi



W kolejnym kroku konfigurowania karty sieciowej Wi-Fi, wybieramy Połączenia sieciowe z kategorii Połączenia sieciowe i internetowe (rys. 34) i klikamy dwukrotnie na ikonie Połączenia sieci bezprzewodowej, rys. 35.

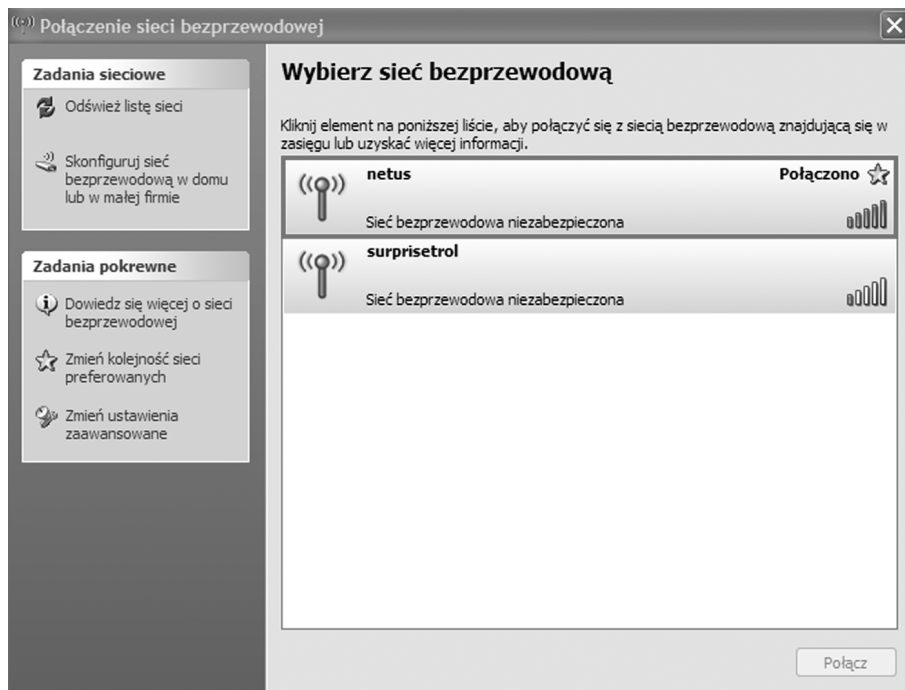


Rysunek 35.
Wybór zakładki – połączenie sieci bezprzewodowej



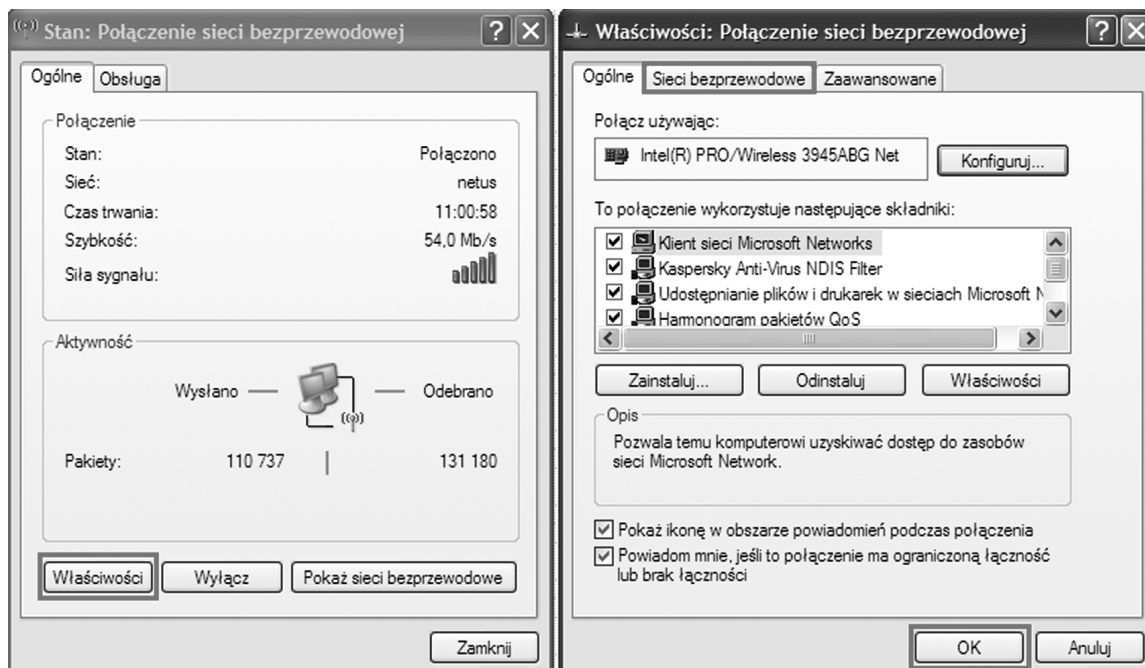
Rysunek 36.
Podgląd stanu połączenia sieci bezprzewodowej

Ukazuje się podgląd stanu połączenia sieci bezprzewodowej (rys. 36), widać jej nazwę, czas trwania połączenia, szybkość transmisji danych a także siłę sygnału radiowego. Możemy także odczytać, ile pakietów zostało wysłanych i ile zostało odebranych przez naszą sieć Wi-Fi.



Rysunek 37.
Lista wykrytych sieci bezprzewodowych

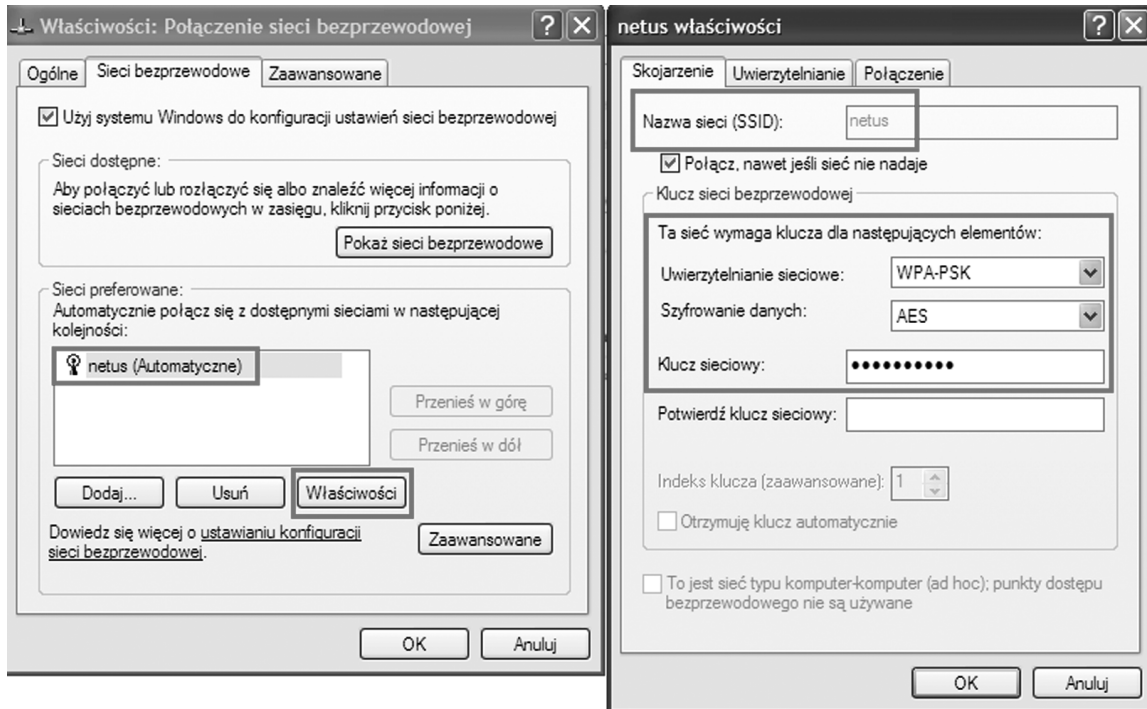
Możemy również podejrzeć (rys. 37) wykryte przez kartę sieciową sieci bezprzewodowe i wybrać tę, którą wcześniej skonfigurowaliśmy, patrz rys. 38 – efekt wyboru.



Rysunek 38.
Szczegółowe informacje o wykrytej i wybranej sieci bezprzewodowej

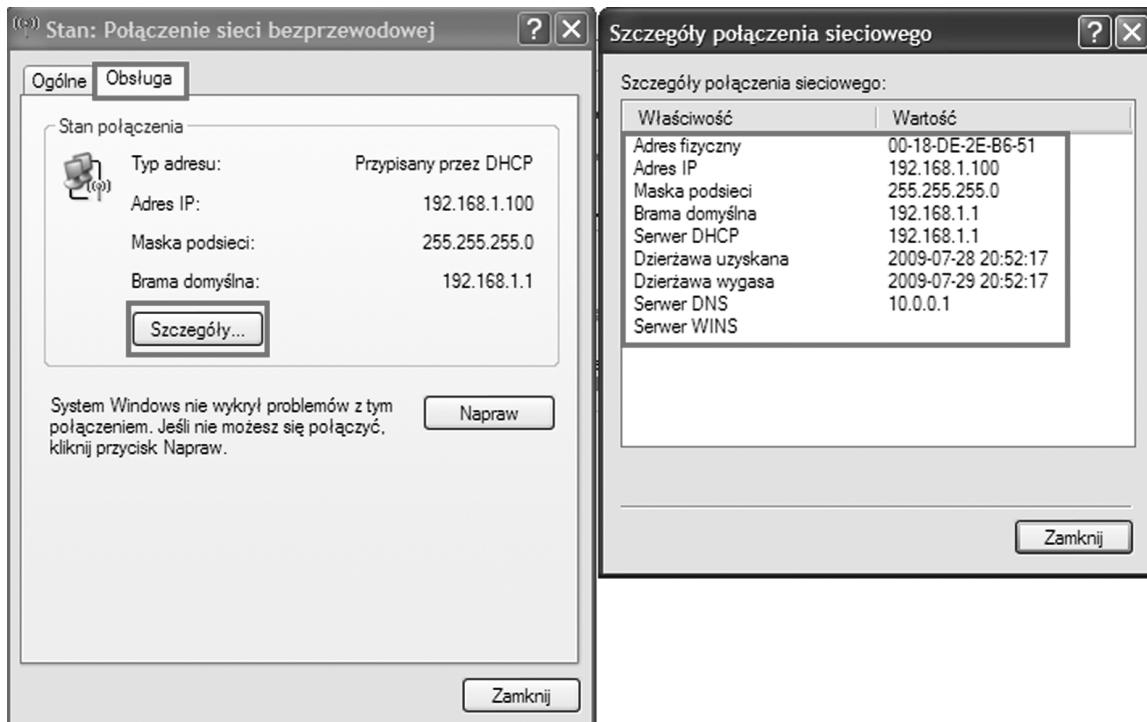
Po wybraniu przycisku Właściwości (rys. 38, lewa strona) możemy poznać szczegółowe informacje dotyczące wykrytych sieci bezprzewodowych, klikamy więc na przycisku OK, z prawej strony.





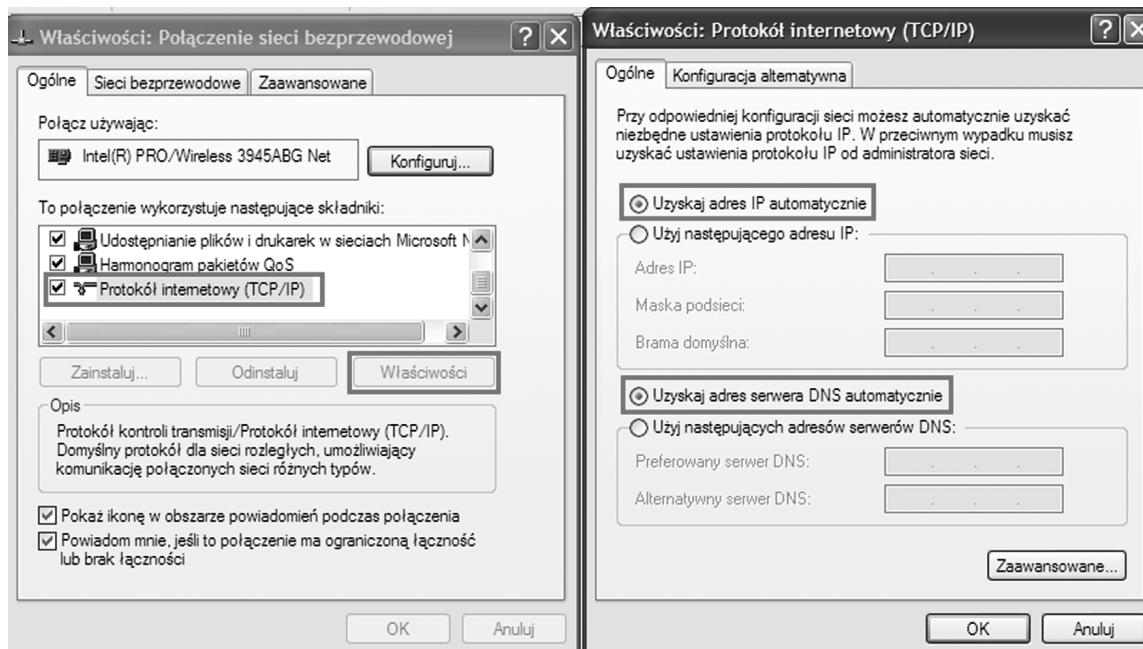
Rysunek 39.
Podgląd podstawowej konfiguracji sieci bezprzewodowej

Na rys. 39, z lewej strony widać sieci preferowane i metodę połączenia, automatyczną lub ręczną. Po zaznaczeniu wybranej sieci klikamy na przycisku Właściwości – ukazuje się podgląd ważnych informacji: nazwa sieci (SSID), protokoły służące uwierzytelnianiu sieciowemu, protokół szyfrowania danych a także klucz sieciowy.



Rysunek 40.
Podgląd szczegółowych informacji o konfiguracji sieci bezprzewodowej

Jeśli natomiast wybierzemy zakładkę Obsługa z kategorii Ogólne (rys. 40), to otrzymamy następujące informacje: typ adresu (przypisany ręcznie czy przez usługę DHCP), adres IP, maskę podsieci oraz adres IP bramy domyślnej. Gdy klikniemy na przycisku Szczegóły, to otrzymamy dodatkowe informacje (z prawej strony na rys. 40): adres fizyczny karty sieciowej (adres MAC), adres IP serwera DHCP, data uzyskania dzierżawy adresu IP i data jej wygaśnięcia, a także adres IP serwera DNS.



Rysunek 41.

Podgląd ustawień protokołu TCP/IP.

W zakładce Ogólne możemy również podejrzeć ustawienie protokołu TCP/IP. Wybieramy więc ten protokół a następnie klikamy na przycisku Właściwości. Na ekranie, widocznym z prawej strony na rys. 41, możemy zdecydować, czy adres IP hosta, maskę podsieci i bramę domyślną przypiszemy ręcznie czy zrobi to za nas usługa DHCP.

LITERATURA

1. Engst A., Fleishman G., *Sieci bezprzewodowe. Praktyczny podręcznik*, Helion, Gliwice 2005
2. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
3. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
4. Ross J., *Sieci bezprzewodowe. Przewodnik po sieciach Wi-Fi i szerokopasmowych sieciach bezprzewodowych*, Wydanie II, Helion, Gliwice 2009







W projekcie **Informatyka +**, poza wykładami i warsztatami,
przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
 - nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
 - konkursy dla uczniów, trzy w ciągu roku
 - udział uczniów w pracach kół naukowych
 - udział uczniów w konferencjach naukowych
 - obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu

www.informatykaplus.edu.pl