

» Idź do

- Spis treści
- Przykładowy rozdział

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl
© Helion 1991-2008

Sieci bezprzewodowe. Przewodnik po sieciach Wi-Fi i szerokopasmowych sieciach bezprzewodowych. Wydanie II

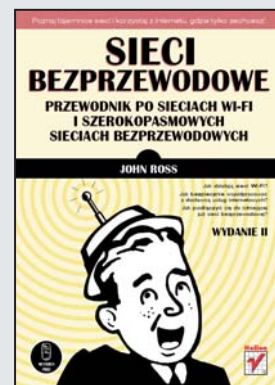
Autor: John Ross

ISBN: 978-83-246-1899-6

Tytuł oryginału: [The Book of Wireless:](#)

[A Painless Guide to Wi-Fi and
Broadband Wireless, 2nd edition](#)

Format: 170x230, stron: 376



Poznaj tajemnice sieci i korzystaj z Internetu, gdzie tylko zechcesz!

- Jak działają sieci Wi-Fi?
- Jak bezpiecznie współpracować z dostawcą usług internetowych?
- Jak podłączyć się do istniejącej już sieci bezprzewodowej?

Szerokopasmowe sieci bezprzewodowe zbliżają nas do wymarzonego stanu, jakim jest zapewnienie wszystkim dostępu do Internetu, bez względu na aktualne miejsce ich pobytu. Zawsze i wszędzie dostępne usługi internetowe mogą zmienić nasz tryb życia, metody pracy i sposób korzystania z rozrywek. Jednak bez właściwego przewodnika sieci bezprzewodowe mogą wydawać się skomplikowane i sprawiać wiele problemów. O tym, jak sobie z nimi skutecznie radzić i jednocześnie wykorzystywać ich możliwości, dowiesz się z tego podręcznika.

Książka „Sieci bezprzewodowe. Przewodnik po sieciach Wi-Fi i szerokopasmowych sieciach bezprzewodowych. Wydanie II” zawiera przejrzyste wyjaśnienia wszelkich zagadnień związanych z zakładaniem i używaniem sieci bezprzewodowych, a także ciekawe informacje na temat nowych i przyszłych standardów bezprzewodowej szerokopasmowej transmisji danych. Dzięki temu podręcznikowi dowiesz się, jak skonfigurować sprzęt i oprogramowanie dla Twojej sieci Wi-Fi, a także poznasz sposoby wyszukiwania sieci otwartych i ochrony prywatności podczas korzystania z Internetu w miejscach publicznych. Nauczysz się korzystać z usług VoIP za pośrednictwem połączenia bezprzewodowego i będziesz mógł wykonywać tanie połączenia telefoniczne.

- Wprowadzenie do sieci
- Działanie sieci bezprzewodowych
- Zarządzanie połączeniami Wi-Fi
- Korzystanie z programów do konfiguracji sieci bezprzewodowych
- Bezpieczeństwo sieciowe
- Łączy dalekosiężne typu punkt-punkt
- Alternatywne sposoby szerokopasmowej transmisji danych
- Smartfony i urządzenia typu PDA
- Wirtualne sieci prywatne
- Wykorzystanie łączy szerokopasmowych do rozmów telefonicznych

Spis treści

PODZIĘKOWANIA	15
----------------------------	-----------

WSTĘP	17
--------------------	-----------

I

WPROWADZENIE DO TEMATYKI SIECI	21
---	-----------

Przesyłanie danych	22
Bity i bajty	22
Kontrola błędów	23
Uzgadnianie	23
Odnajdowanie odbiorcy	24
Model ISO OSI	27
Warstwa fizyczna	28
Warstwa łączy danych	28
Warstwa sieciowa	28
Warstwa transportowa	28
Warstwa sesji	29
Warstwa prezentacji	29
Warstwa aplikacji	29
Podsumowanie	29

2

WPROWADZENIE DO TEMATYKI SIECI BEZPRZEWODOWYCH	31
---	-----------

Działanie sieci bezprzewodowych	32
Fale radiowe	33
Bezprzewodowe sieci transmisji danych	35
Korzyści łączności bezprzewodowej	41
Bezprzewodowe usługi przesyłania danych	41
Wi-Fi	42
Bezprzewodowe usługi telefonii komórkowej	45

WiMAX	46
A co z technologią Bluetooth?	48
Przydzielanie częstotliwości	48
Wybór usługi	50

3

JAK DZIAŁAJĄ SIECI WI-FI? 53

Kontrola sieci Wi-Fi	53
Warstwa fizyczna.....	53
Warstwa kontroli dostępu (MAC, Media Access Control).....	55
Pozostałe warstwy kontroli dostępu	56
Protokoły w sieciach Wi-Fi.....	56
Częstotliwości radiowe	57
Kanały bezprzewodowe.....	58
Zmniejszanie interferencji	59
Urządzenia sieciowe.....	60
Karty sieciowe	61
Punkty dostępu.....	62
Budowa sieci.....	63
Sieci publiczne i prywatne	65
Podsumowanie	66

4

SPRZĘT W SIECIACH WI-FI 67

Wszyscy mówią tym samym językiem (lepiej lub gorzej)	67
Karty sieciowe	69
Rodzaj obudowy	70
Antena — wewnętrzna czy zewnętrzna?	75
Współdziałanie	76
Sterowniki do kart sieciowych	77
Komfort pracy	79
Bezpieczeństwo	81
Dokumentacja i wsparcie techniczne	82
Reputacja	83
Karty sieciowe dla sieci ad hoc	83
Karty sieciowe podwójnego przeznaczenia	84
Punkty dostępu	85
Standardy operacyjne	86
Homogeniczne bezprzewodowe sieci lokalne	86
Bezprzewodowy dostęp do przewodowej sieci lokalnej	87
Połączenie punktu dostępu z koncentratorem kablowym	88
Bramy szerokopasmowe	89
Wiele punktów dostępu	90
Punkty dostępu o zwiększonej wydajności	91

Anteny zewnętrzne	92
Charakterystyki anten	93
Jak wybrać antenę	95
Konstruowanie własnych anten	96
Kiedy korzystać z anten kierunkowych?	96
Anteny tworzą całkiem inny świat	98
Pora na zakupy	99

5

ZARZĄDZANIE POŁĄCZENIAMI WI-FI 101

Instalowanie karty sieciowej PCMCIA	101
Instalowanie karty sieciowej USB	102
Instalowanie wewnętrznej karty sieciowej w komputerze przenośnym	103
Instalowanie wewnętrznej karty sieciowej w komputerze stacjonarnym	104
Instalowanie sterownika	104
Wybór programu kontrolnego	106
Program narzędziowy Połączenie sieci bezprzewodowej firmy Microsoft	106
Program PROSet/Wireless firmy Intel	114
Inne karty Wi-Fi i programy kontrolne	116
Informacje o stanie połączenia	117
Zmiana ustawień konfiguracyjnych karty sieciowej	119
Konfigurowanie połączenia sieciowego	120
Przemieszczanie się między sieciami	121
Nie tylko Windows	122
Poziom i jakość sygnału	123

6

SIECI WI-FI W SYSTEMACH WINDOWS 127

Ogólnie o konfiguracji sieci bezprzewodowych w systemie Windows	129
Adresy IP	129
Maska podsieci	131
Bramy	131
Serwery DNS	132
Udostępnianie plików i drukarek	132
Opcje konfiguracji karty sieciowej	133
Nazwa komputera	133
Konfigurowanie sieci w systemie Windows	135
Czy masz najnowsze oprogramowanie sprzętowe?	135
Korzystanie z programów do konfiguracji sieci bezprzewodowych	135
Parametry karty sieciowej	141
Nazwa komputera	142
Rozwiązywanie problemów z połączeniem	144

7

SIECI WI-FI W SYSTEMACH LINUX I UNIX 145

Sterowniki, zaplecze i inne szczegóły	146
Gdzie szukać sterowników?	148
Sterowniki dla systemu Linux	149
Sterowniki dla systemu Unix	152
Programy do obsługi Wi-Fi	152
Korzystanie z programów wbudowanych	153
Dodatkowe programy do obsługi Wi-Fi	155
Zaglądamy pod maskę	157
Narzędzia bezprzewodowe	158
Programy działające w oparciu o Wireless Tools	159
Programy monitorujące	160
Konfigurowanie punktu dostępu	161
Wi-Fi w systemach Unix	162
Narzędzia konfiguracyjne	162
wiconfig i wicontrol	162

8

WI-FI W KOMPUTERACH MACINTOSH 165

Sprzęt typu AirPort	166
Konfigurowanie sieci typu AirPort	167
Instalowanie sprzętu	168
Uruchamianie programu AirPort Setup Assistant	168
AirPort Utility	169
Ikona AirPort Status	169
Korzystanie z sieci bezprzewodowej typu AirPort	170
Podłączanie komputerów Macintosh do innych sieci	170
Korzystanie z kart sieciowych innych producentów niż Apple na komputerach Macintosh	171
Łączenie kart sieciowych typu AirPort z punktami dostępu innego typu	172
Łączenie innych klientów sieci Wi-Fi z siecią typu AirPort	173
Właściwości sieci	174
Konfigurowanie stacji bazowej AirPort Extreme w systemie Windows	174
Czy AirPort jest najlepszym rozwiązaniem?	175

9

INSTALOWANIE I KONFIGUROWANIE PUNKTÓW DOSTĘPU 177

Instalowanie punktów dostępu	178
Konfigurowanie punktu dostępu za pomocą przeglądarki internetowej	180
DHCP i inne atrakcje	182
Adresy serwerów DNS	183
Polecenia i parametry konfiguracyjne	183
Ile punktów dostępu?	188
Sieć z wieloma punktami dostępu	191

Testowanie pomieszczeń	191
Wykonanie planu pomieszczeń	192
Testowanie i jeszcze raz testowanie	196
Zakłócenia	200
Zalety sieci mieszanych	202
Punkty dostępu wyposażone w funkcje koncentratorów lub routerów działających jak bramy	203
Zwiększanie zasięgu sieci	204
Kwestie prawne	205
Zewnętrzne anteny i punkty dostępu	206
Sieci akademickie	212
Podłączanie punktów dostępu do sieci LAN i internetu	213
Podłączanie sąsiadów do sieci	215
Jak bezpiecznie współpracować z dostawcą usług internetowych?	215
Bezpieczeństwo sieciowe — każdy jest twoim sąsiadem	217

10

ŁĄCZA DALEKOSIĘŻNE TYPU PUNKT-PUNKT 219

Rozszerzanie sieci lokalnej	220
Broutery	222
Połączenia typu punkt-punkt i punkt-wielopunkt	223
Instalowanie łącza typu punkt-punkt	224
Wybór ścieżki sygnału	225
Łąca dalekosiężne	225
Pozycjonowanie anten	226
Przeszkody i przekazywanie sygnału	228
Alternatywy dla łączy Wi-Fi typu punkt-punkt	229
Anteny do kart sieciowych	230
A może by tak zbudować własną antenę?	230

11

PODŁĄCZANIE SIĘ DO ISTNIEJĄCEJ SIECI WI-FI 235

Publiczne sieci Wi-Fi nie są bezpieczne	236
Wyszukiwanie punktu dostępu Wi-Fi	237
Bezpieczeństwo danych	240
NetStumbler i inne programy nasłuchujące	241
Publiczne punkty dostępu	242
Miejskie sieci Wi-Fi	245
„Darmowy” dostęp do internetu	246
Niezabezpieczone prywatne punkty dostępu	248

I 2

BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH 253

Ochrona sieci i danych	256
Ochrona komputera	259
Narzędzia bezpieczeństwa Wi-Fi	260
Nazwa sieci (identyfikator SSID)	260
Szyfrowanie WEP	262
Szyfrowanie WPA	266
Kontrola dostępu (filtrowanie adresów MAC)	268
Wirtualne sieci prywatne	269
Uwierzytelnianie — standard 802.1x	270
Zapory sieciowe	270
Trzymanie intruzów na odległość	271
Odseparowanie sieci lokalnej od internetu	273
Punkty dostępu wyposażone w zapory sieciowe	274
Oprogramowanie dla zapór sieciowych	276
Wyłączanie DHCP	278
Odlączanie zasilania	278
Fizyczne bezpieczeństwo	279
Udostępnianie sieci na zewnątrz	281
Uwagi końcowe na temat bezpieczeństwa sieci Wi-Fi	283

I 3

ALTERNATYWNE SPOSOBY

SZEROKOPASMOWEJ TRANSMISJI DANYCH285

Co jest nie tak z Wi-Fi?	286
Szerokopasmowe usługi transmisji danych	286
Porównanie technologii	289
Wybór dostawcy usług	291
Zasięg	292
Szybkość transmisji danych	292
Koszt	292
Wybór karty sieciowej	293
Obsługa i pomoc techniczna	293
Szerokopasmowe usługi bezprzewodowe na całym świecie	294
Podłączanie się do szerokopasmowych sieci bezprzewodowych	294
Korzystanie z kilku komputerów	295
Bezpieczeństwo usług szerokopasmowych	296
Clearwire, Sprint i inne usługi typu pre-WiMAX	297
Szerokopasmowy, bezprzewodowy dostęp do internetu w samochodach i innych środkach transportu	298
TracNet	300
Anteny zewnętrzne	301
Kwestie bezpieczeństwa	301

14

SMARTFONY I URZĄDZENIA TYPU PDA 303

Dostęp do internetu za pomocą urządzeń typu PDA i innych urządzeń przenośnych	304
Wybór smartfonu	305
Systemy operacyjne instalowane w smartfonach	306
Co wybrać?	314

15

WIRTUALNE SIECI PRYWATNE 315

Metody VPN	318
Serwery sieci VPN	319
Konfigurowanie serwera Windows do obsługi bezprzewodowych sieci VPN	319
Serwery VPN w systemie Unix	321
Sprzęt sieciowy z wbudowaną obsługą sieci VPN	322
Oprogramowanie klienta sieci VPN	323
Konfigurowanie systemu Windows do obsługi sieci VPN	323
Klient L2TP/IPSec sieci VPN firmy Microsoft	327
Tworzenie połączeń w systemie Windows	327
Opcje systemu Windows XP	328
Klienci VPN dla systemu Unix	330
Korzystanie z bezprzewodowych wirtualnych sieci prywatnych	331
Nawiązywanie połączenia	333
Omijanie połączeń VPN	334
Korzystanie z sieci VPN za pośrednictwem sieci publicznych	334

16

WYKORZYSTANIE ŁĄCZY SZEROKOPASMOWYCH

DO ROZMÓW TELEFONICZNYCH 337

Korzystanie z VoIP za pośrednictwem szerokopasmowych	
łączy bezprzewodowych i WiMAX	340
Przesyłanie głosu za pośrednictwem łączy Wi-Fi	342

17

WSKAZÓWKI I PORADY 347

Komputer nie wykrywa mojej karty sieciowej	347
Program obsługi połączeń bezprzewodowych uruchamia się nawet wtedy,	
gdy nie korzystam z karty sieciowej	349
Mój komputer nie może się połączyć z siecią lokalną	350
Mój komputer łączy się z niewłaściwą siecią	350
Widzę sieć lokalną, ale nie mogę połączyć się z internetem	351
Mam dostęp do internetu, ale nie widzę innych komputerów w sieci LAN	351
Sygnał jest słaby lub niskiej jakości	352
Nie mogę znaleźć sieci publicznej	352
Nie wiem, czy jestem w zasięgu sieci	352
Sieć działa bardzo wolno	353

Mój komputer zrywa połączenie	353
Moja sieć Wi-Fi uległa awarii	354
Czy mogę poprawić wydajność za pomocą anteny zewnętrznej?	354
Co jeszcze mogę zrobić, aby poprawić wydajność sieci?	355
Kiedy przechodzę do innego punktu dostępu, karta sieciowa „gubi” połączenie	356
Gdzie mogę znaleźć dokumentację standardów Wi-Fi?	356
Jak mogę się dowiedzieć, kto jest producentem mojej karty sieciowej?	356
W jaki sposób sprawdzić, czy na karcie sieciowej lub w punkcie dostępu jest zainstalowana najnowsza wersja oprogramowania?	358
Nie mogę uzyskać połączenia z siecią szerokopasmową	359
Mam kłopot z nawiązaniem połączenia z siecią VPN	359
W jaki sposób mogę wydłużyć czas pracy baterii komputera?	360
Czy punkt dostępu może działać jako most sieciowy?	361
Podobno sygnały radiowe emitowane przez telefony komórkowe mogą być szkodliwe. A jak to jest z Wi-Fi?	361

SKOROWIDZ	363
------------------------	------------

3

Jak działają sieci Wi-Fi?



BEZPRZEWODOWE SIECI ETHERNET, ZNANE LEPIEJ JAKO WI-FI, ROZPROWADZAJĄ DANE KOMPUTEROWE W SIECIACH LOKALNYCH ZA POMOCĄ SYGNALIZACJI RADIOWEJ W TECHNOLOGII rozproszonego widma. Ten rozdział opisuje szczegóły techniczne związane z sieciami Wi-Fi, włącznie z różnicami, jakie występują między standardami Wi-Fi i strukturą sieci.

Zawiera również informacje o bezprzewodowych punktach dostępu (zwanym też **stacjami bazowymi**) i kartach sieciowych.

Kontrola sieci Wi-Fi

Specyfikacje standardu Wi-Fi kontrolują sposób przesyłania danych w warstwie fizycznej (łącze radiowe) i definiują warstwę kontroli dostępu (MAC, ang. *Media Access Control*), która pośredniczy w wymianie danych między warstwą fizyczną a pozostałą strukturą sieci.

Warstwa fizyczna

W sieci standardu 802.11 nadajnik radiowy dodaje do każdego pakietu 144-bitową preambułę, która składa się ze 128 bitów, wykorzystywanych przez odbiornik do synchronizacji z nadajnikiem, oraz z 16-bitowego pola sygnalizującego początek ramki (**ramka** to pakiet zawierający dodatkowe dane na początku lub na końcu

ciągu bitów). Po preambule znajduje się 48-bitowy nagłówek zawierający informacje o szybkości przesyłania danych, długości danych zawartych w pakiecie oraz sekwencję sumy kontrolnej. Nagłówek ten nazywany jest preambułą PHY (od ang. *physical* — fizyczny), ponieważ kontroluje on warstwę fizyczną (w modelu ISO) łączy komunikacyjnego.

Ponieważ nagłówek zawiera informację o szybkości przesyłania danych, razem z preambułą jest zawsze przesyłany z szybkością 1 Mbps. Dlatego też, nawet jeśli łączy sieciowe działa z pełną szybkością 11 Mbps, efektywna szybkość transferu danych może być znacznie niższa. W praktyce w najlepszym razie można oczekiwać osiągnięcia ok. 85 procent szybkości nominalnej. Należy też pamiętać, że inne rodzaje danych nadmiarowych, znajdujących się w pakietach, jeszcze bardziej zmniejszają rzeczywistą prędkość transferu.

Ta 144-bitowa preambuła została odziedziczona po starszym i wolniejszym systemie DSSS. Została ona włączona do standardu, aby zapewnić zgodność urządzeń pracujących w standardzie 802.11b z urządzeniami pracującymi w starszych standardach, w rzeczywistości jednak do niczego się nie przydaje. Dlatego też istnieje możliwość korzystania z 72-bitowej preambuły. W przypadku tej krótszej preambuły pole synchronizacji składa się z 56 bitów, po których występuje 16-bitowe pole sygnalizujące początek ramki, takie samo jak to, które występuje w dłuższej preambule. 72-bitowa preambuła nie jest kompatybilna ze starszym sprzętem pracującym w standardzie 802.11, w przypadku nowoczesnych sieci Wi-Fi nie ma to jednak znaczenia, ponieważ wszystkie węzły sieci rozpoznają jej krótszy format. Pod wszystkimi innymi względami krótsza preambuła działa równie dobrze jak dłuższa.

W sieci komputerowej przetwarzanie długiej preambuły trwa maksymalnie 192 milisekundy, a krótszej — 96 milisekund. Innymi słowy, krótsza preambuła powoduje dwukrotne zmniejszenie ilości informacji nadmiarowych w każdym pakiecie. Daje to dużą różnicę w rzeczywistej szybkości transmisji danych, zwłaszcza w przypadku przesyłania danych strumieniowych, takich jak dźwięk, wideo oraz usługi telefonii internetowej.

Część producentów stosuje domyślnie długą preambułę, a inni używają krótkiej. Zazwyczaj istnieje możliwość zmiany długości preambuły za pomocą oprogramowania służącego do konfigurowania kart sieciowych i punktów dostępu.

Z punktu widzenia większości użytkowników długość preambuły to tylko jeden z technicznych szczegółów, nad którym nie trzeba się zastanawiać, jeśli tylko wszystkie urządzenia używają preambuły tej samej długości. 15 lat temu, gdy najpopularniejszym sposobem wymiany danych między odległymi komputerami były modemy telefoniczne, wszyscy musieli wiedzieć, jak ustawić liczbę bitów danych i bit stopu, gdy próbowali nawiązać połączenie modemowe. Można było nie wiedzieć, czym dokładnie jest bit stopu (to czas wymagany do tego, by drukarka mogła przejść do stanu oczekiwania po wysłaniu lub odebraniu każdego z bajtów przez telex), wiadomo jednak było, że ustawienia te muszą być takie same na obu końcach połączenia. Długość preambuły jest równie tajemniczym ustawieniem. Musi być ona taka sama w każdym węźle sieci, większość osób nie musi jednak o tym wiedzieć ani się nad tym zastanawiać.

Warstwa kontroli dostępu (MAC, Media Access Control)

W ramach modelu ISO warstwa kontroli dostępu (którą zwykle określa się jako podwarstwę warstwy łącza danych) sprawuje kontrolę nad przesyłaniem danych w sieci radiowej. Korzystając z zestawu reguł, zwanych w skrócie CSMA/CA (ang. *carrier sense multiple access/collision avoidance* — protokół wielodostępu do łącza ze śledzeniem stanu nośnika i unikaniem kolizji), warstwa kontroli dostępu odpowiada za unikanie kolizji i konfliktów podczas przesyłania danych oraz obsługuje funkcje bezpieczeństwa, zdefiniowane w standardach 802.11. Jeśli sieć zawiera kilka punktów dostępu, ta warstwa przypisuje każdego klienta sieci do punktu dostępu zapewniającego mu najlepszą jakość sygnału.

Gdy kilka węzłów sieci próbuje równocześnie wysłać dane, protokół CSMA/CA nakazuje wszystkim węzłom, z wyjątkiem jednego, wybranego, zakończenie transmisji i podjęcie próby nadawania w późniejszym czasie. Wybrany węzeł ma wtedy możliwość wysłania swojego pakietu. Protokół CSMA/CA działa w następujący sposób: gdy węzeł sieci jest gotowy do wysłania pakietu, zaczyna najpierw nasłuchiwać, czy w ośrodku są obecne inne sygnały. Jeśli niczego nie wykryje, wówczas odczekuje losowo wybrany (lecz krótki) okres, a następnie nasłuchuje ponownie. Jeżeli wciąż nie wykrywa żadnego sygnału, wysyła pakiet. Odbiornik po otrzymaniu pakietu przetwarza go i jeśli dotarł nienaruszony, wysyła nadajnikowi potwierdzenie odbioru. Jeśli jednak węzeł nadawczy nie odbierze potwierdzenia, zakłada, że w sieci wystąpiła kolizja z innym pakietem, w związku z czym odczekuje wybrany losowo czas, a następnie ponawia próbę wysłania pakietu.

Protokół CSMA/CA ma także dodatkową funkcję, która umożliwia zdefiniowanie punktu dostępu (spełniającego funkcję mostu między bezprzewodową siecią lokalną i siecią szkieletową) jako punktu koordynacyjnego, który odpowiada za nadawanie priorytetu węzłowi wysyłającemu dane, dla których istotny jest czas przesyłu (takie jak przekaz głosowy lub media strumieniowe).

Do autoryzacji urządzenia w sieci warstwa kontroli dostępu dysponuje dwoma mechanizmami uwierzytelniania: otwartym i za pomocą klucza współdzielonego. Konfigurując sieć, należy pamiętać o tym, że wszystkie węzły muszą używać tego samego sposobu uwierzytelniania. Za wysyłanie danych przez wyższe warstwy sieciowe odpowiadają funkcje administracyjne warstwy kontroli dostępu, co odbywa się za pośrednictwem wymiany (lub prób wymiany) serii ramek sterujących. Ponadto warstwa sieciowa może ustawiać następujące opcje na kartach sieciowych:

- Tryb zasilania — karty sieciowe obsługują dwa tryby zasilania: **tryb stałego czuwania** (ang. *continuous aware mode*) i **tryb oszczędzania energii z odpytywaniem** (ang. *power save polling mode*). W trybie stałego czuwania odbiornik radiowy jest zawsze włączony i cały czas pobiera energię. W trybie oszczędzania energii z odpytywaniem odbiornik przez większość czasu jest nieaktywny, ale okresowo odpytuje punkt dostępu, aby sprawdzić, czy nie pojawiły się nowe wiadomości. Jak sama nazwa wskazuje, tryb oszczędzania energii z odpytywaniem zmniejsza zużycie baterii w urządzeniach przenośnych, takich jak laptopy czy palmtopy (PDA, ang. *Personal Digital Assistants*).

- **Kontrola dostępu** — karty sieciowe zawierają mechanizm kontroli dostępu, który uniemożliwia korzystanie z sieci nieautoryzowanym użytkownikom. Sieć Wi-Fi może stosować dwa rodzaje kontroli dostępu: **SSID** (nazwę sieci) i **adres MAC** (unikatowy ciąg znaków, identyfikujący każdy węzeł w sieci). Każdy węzeł musi mieć zapisany programowo identyfikator SSID, w przeciwnym razie punkt dostępu nie pozwoli na utworzenie połączenia z takim węzłem. Opcjonalna tabela adresów MAC może ograniczyć dostęp bezprzewodowy tylko do urządzeń o adresach znajdujących się na liście. Karty sieciowe zawierają również funkcję kontroli dostępu przez szyfrowanie WEP (ang. *Wired Equivalent Privacy*) lub WPA (ang. *Wi-Fi protected access*). W WEP do szyfrowania i odszyfrowywania danych przesyłanych przez łącza radiowe używa się klucza 64- lub 128-bitowego; w WPA jest stosowany 128-bitowy klucz i 48-bitowy wektor początkowy (patrz rozdział 12., zawierający informacje na temat szyfrowania w sieciach Wi-Fi).

Pozostałe warstwy kontroli dostępu

Wszystkie działania określone w standardach 802.11 mają miejsce w warstwie fizycznej oraz w warstwie kontroli dostępu. Wyższe warstwy odpowiadają za kontrolę takich elementów, jak adresowanie i wyznaczanie tras oraz spójność, składnia i format danych zawartych w każdym pakiecie. Dla wyższych warstw nie ma znaczenia, czy pakiety są przesyłane kablem, światłowodem, czy drogą radiową. Dlatego też sieć bezprzewodowa może współpracować z dowolną siecią LAN lub innymi protokołami sieciowymi. Te same urządzenia radiowe mogą obsługiwać protokoły TCP/IP, NetWare firmy Novell oraz wszelkie inne protokoły sieciowe, wbudowane w systemy Windows, Unix, Mac OS X i inne.

Protokoły w sieciach Wi-Fi

Pierwszym standardem Wi-Fi, jaki pojawił się na rynku, była wersja 802.11b (w 1999 roku), a rok później pojawił się 802.11a, choć oba te standardy zostały wydane w tym samym czasie. W 2003 roku organizacja standaryzująca IEEE opracowała nowszą specyfikację w postaci standardu 802.11g, który był połączeniem najlepszych cech obu poprzednich wersji: ta sama szybkość co 802.11a i większy zasięg sygnału niż 802.11b. Ponadto specyfikacja 802.11g jest zgodna wstecz ze standardem 802.11b, dzięki czemu karta sieciowa 802.11b będzie działać (choć wolniej, tak jak w sieci 802.11b) z punktem dostępu 802.11g.

UWAGA *Istnieją też specyfikacje określone jako 802.11c, d, e i f, ale dotyczą one takich rzeczy, jak działanie mostów pomiędzy sieciami i QoS (ang. Quality of Service — jakość usług). Jeśli nie jesteś producentem stacji bazowych, nie musisz się tym przejmować.*

Najnowsza specyfikacja Wi-Fi to 802.11n. Zapewnia ona większą szybkość i bezpieczeństwo w porównaniu z wcześniejszymi wersjami. Punkty dostępu 802.11n powinny działać także z kartami sieciowymi 802.11b i 802.11g.

Łącząc się z internetem drogą radiową, należy pamiętać, że szybkość transmisji danych przez łącze bezprzewodowe nie ma wielkiego znaczenia. Maksymalna przepustowość wychodzącego sygnału Wi-Fi nie może przekraczać szybkości pobierania danych przez punkt dostępu. Nawet jeśli stacja bazowa sieci Wi-Fi może obsłużyć stosunkowo dużą przepustowość, prawdopodobnie jest ona podłączona do internetu za pośrednictwem T-1, modemu kablowego lub linii DSL, których maksymalna szybkość przesyłania nie przekracza 5 Mbps, taka też będzie maksymalna szybkość przesyłania sygnału zwrotnego.

Częstotliwości radiowe

Zgodnie z regulacjami międzynarodowymi zakres częstotliwości radiowych wokół częstotliwości 2,4 GHz jest przeznaczony do zastosowań przemysłowych, naukowych i medycznych (są to tzw. pasma ISM, od ang. *Industrial, Scientific & Medical*), które nie wymagają koncesji, oraz dla sieci bezprzewodowych, działających w systemie rozproszonego widma. Z tych pasm korzystają wszystkie usługi 802.11b, 802.11g i 802.11n.

Zakres częstotliwości w okolicach 5,3 GHz określa się jako pasma U-NII (ang. *unlicensed national information infrastructure*). Federalna Komisja Łączności (FCC, ang. *Federal Communications Commission*) w Stanach Zjednoczonych i podobne urzędy regulacyjne w innych krajach dopuszczają korzystanie z sieci bezprzewodowych zarówno w pasmach ISM, jak i U-NII (w paśmie U-NII działają sieci standardu 802.11a).

Dokładna wartość przydzielonych częstotliwości jest nieco inna w różnych częściach świata. Tabela 3.1 zawiera dokładny wykaz częstotliwości z zakresu 2,4 GHz w wybranych rejonach geograficznych.

Tabela 3.1. Niewymagające koncesji częstotliwości z zakresu 2,4 GHz

Region	Pasmo częstotliwości ISM
Ameryka Północna	2,4000 do 2,4835 GHz
Europa	2,4000 do 2,4835 GHz
Francja	2,4465 do 2,4835 GHz
Hiszpania	2,445 do 2,475 GHz
Japonia	2,471 do 2,497 GHz

Prawie każde państwo na świecie wykorzystuje jedno z tych pasm. Niewielkie różnice w przydziale częstotliwości nie mają większego znaczenia (z wyjątkiem tak nietypowych sytuacji, jak przesyłanie danych przez granicę między Francją a Hiszpanią), ponieważ większość sieci bezprzewodowych działa wyłącznie w obrębie jednego kraju lub regionu, a standardowy zasięg sygnału to zazwyczaj tylko

killkadziesiąt metrów. Zakresy częstotliwości przyjęte w różnych krajach nakładają się w znacznym stopniu na siebie, co umożliwia wykorzystanie tego samego sprzętu właściwie w dowolnym miejscu na świecie. Producenci urządzeń sieciowych zazwyczaj ustawiają w nich zestaw kanałów przeznaczony dla kraju, w którym dany sprzęt jest sprzedawany.

Kanały bezprzewodowe

Dokładna częstotliwość stosowana w określonej sieci bezprzewodowej zależy od używanego kanału. W Ameryce Północnej urządzenia typu Wi-Fi w sieciach 802.11b/g korzystają z 11 kanałów. W wielu innych krajach (w tym w Polsce) wykorzystywanych jest 13 kanałów, w Japonii można korzystać z 14, a we Francji tylko z 4. Na szczęście, na całym świecie używa się tej samej numeracji kanałów, dzięki czemu kanał numer 9 w Nowym Jorku zajmuje dokładnie tę samą częstotliwość co kanał 9. w Tokio lub w Paryżu. W tabeli 3.2 znajduje się lista kanałów wykorzystywanych w różnych krajach i regionach.

Tabela 3.2. Kanały sieci bezprzewodowych typu Ethernet

Numer kanału	Częstotliwość	Używany w
1	2412	USA*, EMEA**, Chiny, Japonia
2	2417	USA, EMEA, Chiny, Japonia
3	2422	USA, EMEA, Izrael, Chiny, Japonia
4	2427	USA, EMEA, Izrael, Chiny, Japonia
5	2432	USA, EMEA, Izrael, Chiny, Japonia
6	2437	USA, EMEA, Izrael, Chiny, Japonia
7	2442	USA, EMEA, Izrael, Chiny, Japonia
8	2447	USA, EMEA, Izrael, Chiny, Japonia
9	2452	USA, EMEA, Izrael, Chiny, Japonia
10	2457	USA, EMEA, Francja, Chiny, Japonia
11	2462	USA, EMEA, Francja, Chiny, Japonia
12	2467	EMEA, Francja, Japonia
13	2472	EMEA, Francja, Japonia
14	2484	Japonia

* W Kanadzie i w niektórych innych krajach półkuli zachodniej przyporządkowanie numerów kanałów jest takie samo jak w Stanach Zjednoczonych.

** EMEA oznacza kraje leżące na obszarze Europy, Bliskiego Wschodu oraz Afryki (ang. Europe, Middle East and Africa). We Francji, choć należy ona do obszaru EMEA, można korzystać tylko z kanałów o numerach od 10. do 14.

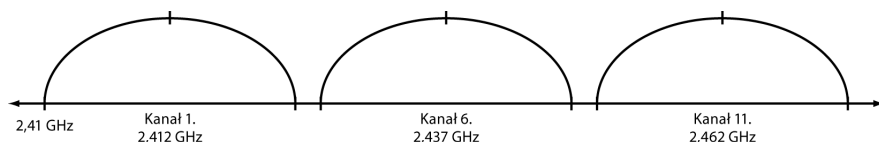
W przypadku wyjazdu za granicę może zająć konieczność przestawienia karty sieciowej na inny kanał (jeśli nie wykryje ona sygnału automatycznie), niemal zawsze istnieje jednak jakaś możliwość nawiązania połączenia, jeśli karta znajduje się w zasięgu sieci. Jeżeli nie masz pewności, z jakich kanałów można korzystać w danym kraju, można to sprawdzić w lokalnym urzędzie regulacyjnym.

Zawsze możesz też korzystać z kanałów o numerach 10 i 11, które są dostępne na całym świecie poza Izraelem.

Zmniejszanie interferencji

Należy zauważyć, że częstotliwości odpowiadające każdemu z tych kanałów w rzeczywistości są częstotliwościami środkowymi dla pasm o szerokości 22 MHz. Dlatego też każdy z tych kanałów nakłada się z kilkoma innymi, położonymi wyżej lub niżej. W całym paśmie 2,4 GHz występują tylko trzy całkowicie nienakładające się kanały, więc jeśli nasza sieć działa np. na czwartym kanale, a sąsiad korzysta z piątego lub szóstego, to sygnały płynące z drugiej sieci będą odbierane jako zakłócenia. Oczywiście, obydwie sieci będą działać, ich wydajność (czyli szybkość transferu danych) nie będzie jednak tak dobra jak wtedy, gdy kanały są od siebie oddzielone.

Aby zminimalizować taki rodzaj interferencji, warto skoordynować użycie kanałów z administratorami innych sieci bezprzewodowych, znajdujących się w najbliższym otoczeniu (przez administratora mam tu na myśli także sąsiada, który założył sobie domową sieć Wi-Fi). Jeśli to możliwe, każda z sieci powinna korzystać z kanałów, które są oddalone od siebie przynajmniej o 25 MHz lub o pięć numerów. Aby wyeliminować interferencje między dwiema sieciami bezprzewodowymi, najlepiej użyć jednego kanału o dużym numerze i jednego o małym. W przypadku trzech kanałów najlepiej będzie wybrać kanały 1., 6. i 11., co przedstawia rysunek 3.1. Jeśli jest więcej sieci, trzeba pogodzić się z występowaniem pewnej interferencji, ale można ją zminimalizować, przydzielając nowy kanał pomiędzy już istniejącymi.



Rysunek 3.1. Kanały 1., 6. i 11. nie zakłócają się

W rzeczywistości nie jest to istotne. W praktyce można zoptymalizować wydajność sieci, wybierając dla niej numer kanału maksymalnie oddalony od używanego przez pobliską sieć. Nawet jeśli sąsiadujące z sobą sieci korzystają z kanałów przylegających bezpośrednio do siebie, prawdopodobnie i tak będą one funkcjonować poprawnie, choć szybkość transferu może być nieznacznie mniejsza niż w przypadku oddalonych kanałów. Większym problemem mogą być zakłócenia pochodzące z innych urządzeń korzystających z pasma 2,4 GHz, takich jak telefony bezprzewodowe i kuchenki mikrofalowe.

Specyfikacja Wi-Fi 802.11a używa innego zakresu częstotliwości radiowych, wymienionych w tabeli 3.3. Kanały mają szerokość 20 MHz, mają tu więc zastosowanie te same reguły dotyczące ich rozdzielania.

Tabela 3.3. Częstotliwości radiowe w sieciach 802.11a

Numer kanału	Częstotliwość w GHz	Region, w którym jest używany
34	5,17	Japonia
36	5,18	Ameryka Północna, Europa, Singapur
38	5,19	Japonia
40	5,20	Ameryka Północna, Europa, Singapur
42	5,21	Japonia
44	5,22	Ameryka Północna, Europa, Singapur
46	5,23	Japonia
48	5,24	Ameryka Północna, Europa, Singapur
52	5,26	Ameryka Północna, Tajwan
56	5,28	Ameryka Północna, Tajwan
60	5,30	Ameryka Północna, Tajwan
64	5,32	Ameryka Północna, Tajwan

Wybór kanału operacyjnego leży w gestii operatora sieci. Gdy podłączasz się do istniejącej sieci, Twój komputer lub karta sieciowa automatycznie wykryje jeden lub więcej sygnałów Wi-Fi i umożliwi Ci wybór tego, którego chcesz użyć. Większość bezprzewodowych kart sieciowych potrafi rozpoznawać różne protokoły sieciowe i konfigurować połączenie odpowiednio do aktywnego sygnału. Jeśli więc Twój komputer wykryje dwa sygnały: 802.11a i 802.11g, będziesz mógł wybrać jeden z nich bez potrzeby ręcznej zmiany wewnętrznych ustawień.

Specyfikacje 802.11 oraz różne narodowe urzędy regulacyjne (takie jak Federalna Komisja Łączności w Stanach Zjednoczonych czy Urząd Komunikacji Elektronicznej w Polsce) nakładają ponadto ograniczenia na maksymalną dopuszczalną moc nadajników oraz zysk anten, których można używać w bezprzewodowych sieciach Wi-Fi. Ograniczenia te mają na celu zmniejszenie zasięgu działania sieci bezprzewodowej, aby na tym samym kanale mogła działać większa liczba sieci, nie zakłócając się. W rozdziale 10. zostały przedstawione metody radzenia sobie z ograniczeniami związanymi z mocą nadajników i zyskiem anten oraz rozszerzaniem zasięgu sieci bezprzewodowych bez łamania prawa.

Urządzenia sieciowe

Po określeniu formatu danych i łączy radiowych kolejnym krokiem będzie utworzenie struktury sieciowej. Należy odpowiedzieć sobie na pytanie: W jaki sposób komputery używają urządzeń radiowych i określonego formatu danych do wymiany informacji?

W sieciach bezprzewodowych wyróżniamy dwa rodzaje urządzeń radiowych: karty sieciowe i punkty dostępu. **Karta sieciowa** jest podłączona do komputera lub innego urządzenia (np. drukarki), które wymienia dane za pośrednictwem

sieci bezprzewodowej. **Punkt dostępu** to stacja bazowa sieci bezprzewodowej lub most łączący ją z tradycyjną, przewodową siecią komputerową.

Karty sieciowe

Karty sieciowe przeznaczone do stacji bezprzewodowych mogą występować w kilku różnych wersjach.

Karty sieciowe PCMCIA, podłączane do gniazd PCMCIA w większości laptopów

Aby obejść ograniczenie związane z wewnętrznym ekranowaniem, anteny oraz lampki sygnalizacyjne bezprzewodowych kart sieciowych wystają zwykle ok. półtora centymetra poza gniazdo złącza. Niektóre karty PCMCIA mają gniazda przeznaczone do podłączenia anteny zewnętrznej.

Wewnętrzne karty sieciowe PCI, umieszczane w złączu na płycie głównej komputera biurkowego

Część kart sieciowych PCI to w rzeczywistości karty bazujące na złączach PCMCIA, które umożliwiają użytkownikowi zainstalowanie karty na tylnej ścianie komputera, ale inne są wbudowane bezpośrednio na kartach rozszerzeń typu PCI. Alternatywa dla gniazd w tylnej ścianie komputera to produkowane przez firmę Actiontec oraz innych producentów oddzielne gniazda PCMCIA, które można zainstalować z przodu komputera, w miejscu przeznaczonym na dodatkowe urządzenia.

Zewnętrzne karty sieciowe USB

Karta sieciowa typu USB to często lepszy wybór niż karta PCMCIA, ponieważ łatwo ją zainstalować i niemal zawsze kartę sieciową zainstalowaną na kablu można przesunąć w miejsce, w którym występuje najsilniejszy sygnał pochodzący z najbliższego punktu dostępu.

Wewnętrzne, bezprzewodowe karty sieciowe, wbudowane do laptopów

Wewnętrzne karty sieciowe to moduły podłączane do płyty głównej komputera. Dla systemu operacyjnego wyglądają dokładnie tak samo jak zewnętrzne karty PCMCIA. Anteny wbudowanych kart sieciowych są zwykle ukryte wewnątrz obudowy monitora.

Podłączane karty sieciowe dla palmtopów i innych urządzeń kieszonkowych

Palmtopy i inne urządzenia kieszonkowe są często wyposażone w gniazda, do których można podłączyć jedną z kilku rodzajów kart rozszerzeń. System operacyjny traktuje je zazwyczaj dokładnie tak samo jak większe karty rozszerzeń w laptopach. Karty sieciowe w palmtopach i urządzeniach kieszonkowych zwykle nie mają gniazd na antenę.

Wewnętrzne interfejsy sieciowe, wbudowane do innych urządzeń, takich jak zestawy telefoniczne z dostępem do internetu oraz różne urządzenia biurowe i domowe

Drukarki, aparaty cyfrowe, radia internetowe, telefony VoIP (ang. *Voice over Internet Protocol*), domowe centra rozrywki i inne urządzenia korzystają obecnie z łączy Wi-Fi w celu wysyłania i pobierania zdjęć, dźwięków i innych danych.

W przyszłości różne skomplikowane urządzenia domowe będą używać łącz bezprzewodowych do powiadamiania np. o tym, że ubrania już wyschły albo że pieczeń jest gotowa.

Karta sieciowa powinna działać z dowolnym systemem operacyjnym, jeśli tylko jest dostępny odpowiedni sterownik. W praktyce oznacza to, że prawie dla każdego urządzenia można znaleźć sterowniki systemu Windows, nieco gorzej jest natomiast w przypadku komputerów z systemem operacyjnym Mac OS, Linux lub Unix. Informacje o stronach WWW, na których można znaleźć sterowniki dla systemów Linux i Unix, znajdują się w rozdziale 7., a informacje na temat korzystania z Wi-Fi w systemie Mac OS zawiera rozdział 8.

Karty sieciowe dla różnych rodzajów sieci

W pewnych sytuacjach musisz korzystać z różnych rodzajów połączeń sieciowych w zależności od miejsca, w którym przebywasz. Laptop w biurze podłączasz np. do sieci LAN przez łącze bezprzewodowe, aby móc korzystać w firmowego, szerokopasmowego konta internetowego oraz wymieniać pliki i wiadomości z innymi komputerami w sieci lokalnej. Jeśli jednak zabierasz ten sam komputer w podróż, chcesz się łączyć z internetem dzięki usłudze przesyłania danych, oferowanej przez operatora komórkowego. Dobrze by więc było, gdyby komputer mógł automatycznie wybrać najlepszy rodzaj połączenia dla danej lokalizacji.

Obecnie jedynym sposobem zmiany rodzaju sieci jest ręczne wybranie oprogramowania kontrolującego każdy rodzaj sieci; można również fizycznie usunąć jedną kartę sieciową i włożyć inną. Kilku producentów laptopów i kart sieciowych pracuje nad tym problemem i w nieodległej przyszłości będzie mogło zaoferować jedną kartę sieciową i oprogramowanie sterujące, wykrywające kilka rodzajów usług bezprzewodowych, których wybór będzie polegał na wskazaniu jednej z opcji na ekranie lub będzie odbywał się automatycznie.

Po zainstalowaniu jednej z takich wielozadaniowych kart sieciowych będziesz mógł ustalić własną listę priorytetów; możesz np. wprowadzić takie ustawienia, aby w pierwszym rzędzie była wyszukiwana domowa lub biurowa sieć LAN, a dopiero jeśli okaże się niedostępna, następowało połączenie z usługą przesyłania danych operatora komórkowego.

Punkty dostępu

Punkty dostępu często łączą w sobie również wiele innych funkcji sieciowych. Można spotkać autonomiczne punkty dostępu, podłączane do przewodowej sieci LAN za pomocą odpowiednich kabli, ale istnieje też wiele innych możliwości. Najpopularniejsze punkty dostępu są skonfigurowane jako:

- Proste stacje bazowe zawierające most do internetu, połączony z portem do komunikacji z siecią lokalną.
- Stacje bazowe zawierające przełącznik, koncentrator (hub) lub router, jeden lub kilka przewodowych portów ethernetowych oraz bezprzewodowy punkt dostępu.

- Szerokopasmowe routery stanowiące most pomiędzy modemem kablowym lub portem DSL a bezprzewodowym punktem dostępu.
- Programowe punkty dostępu, w których funkcję stacji bazowej pełni jedna z bezprzewodowych kart sieciowych w komputerze.
- Stacjonarne bramy obsługujące ograniczoną liczbę kanałów operacyjnych.

Wygląd zewnętrzny punktów dostępu może różnić się w zależności od producenta. Niektóre wyglądają jak urządzenia przemysłowe, przeznaczone do instalacji na podłodze lub w nierzucającym się w oczy miejscu na ścianie, inne natomiast (zwłaszcza te przeznaczone do zastosowań domowych) mają bardzo „aerodynamiczne” kształty i są zaprojektowane tak, aby można je było postawić w widocznym miejscu na stoliku lub obok komputera domowego. Niektóre z nich są wyposażone w anteny wewnętrzne, inne (jak ten widoczny na rysunku 3.2) posiadają podłączone na stałe krótkie, pionowe antenki, a jeszcze inne mają gniazdka do podłączania anten zewnętrznych (które można kupić razem z urządzeniem lub osobno). Niezależnie od rozmiaru i kształtu każdy punkt dostępu zawiera urządzenie radiowe, służące do wysyłania i odbierania komunikatów oraz danych pomiędzy bezprzewodowymi stacjami sieci a portem Ethernet, do którego podłącza się sieć przewodową.



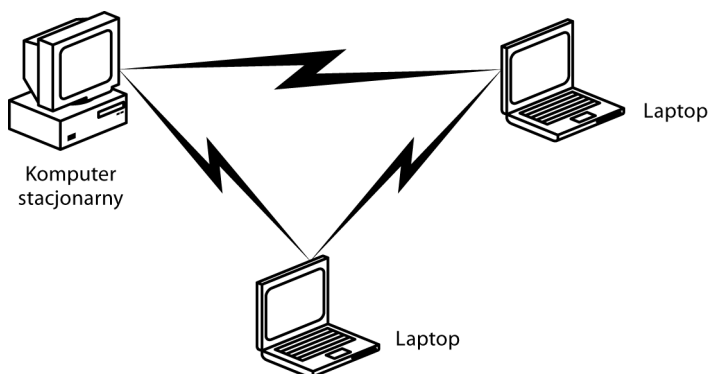
Zdjęcie zamieszczone za zgodą firmy Linksys (oddział Cisco Systems, Inc.)

Rysunek 3.2. Przykład typowego punkt dostępu Wi-Fi firmy Linksys

Budowa sieci

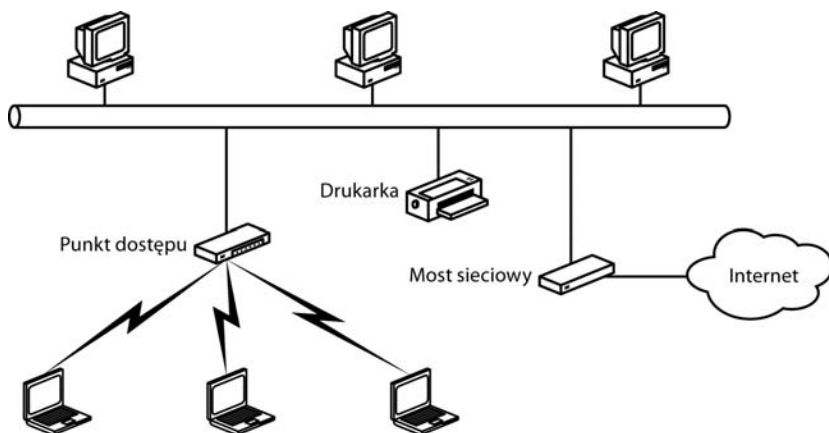
Sieci Wi-Fi mogą działać w dwóch trybach: *ad hoc* (równorzędnym) i *infrastrukturalnym*. Jak sama nazwa wskazuje, sieć **ad hoc** jest zwykle tymczasowa, stanowi grupę niezależnych stacji roboczych, które nie mają połączenia z większą siecią lokalną ani z internetem. Taka grupa zawiera stacje bezprzewodowe

bez punktu dostępu lub bez możliwości łączenia się z resztą świata. Sieci ad hoc określa się również mianem sieci równorzędnych (ang. *peer-to-peer*) lub sieci niezależnych usług podstawowych (IBSS, ang. *independent basic service set*). Rysunek 3.3 przedstawia przykład prostej sieci ad hoc.



Rysunek 3.3. Bezprzewodowa sieć typu ad hoc z trzema stacjami roboczymi

W skład **sieci infrastrukturalnej** wchodzi zwykle jeden lub więcej punktów dostępu, które prawie zawsze są połączone z siecią przewodową. Każda stacja bezprzewodowa wymienia komunikaty i dane z punktem dostępu, który następnie przesyła je do innych węzłów sieci bezprzewodowej lub przewodowej sieci LAN. Każda sieć, która wymaga połączenia przewodowego do drukarki, serwera plików lub bramy internetowej za pośrednictwem punktu dostępu, jest siecią infrastrukturalną. Rysunek 3.4 przedstawia przykład sieci infrastrukturalnej.



Rysunek 3.4. Prosta sieć infrastrukturalna

Sieć infrastrukturalna, zawierająca tylko jedną stację bazową, jest określana jako **BSS** (ang. *basic service set*, **zestaw usług podstawowych**). Jeśli infrastrukturalna sieć bezprzewodowa korzysta z kilku punktów dostępu, określa się ją jako

ESS (ang. *extended service set*, **zestaw usług rozszerzonych**). Jak już wcześniej wspomniałem, skrót określający identyfikator sieci to **SSID**. W przypadku sieci z jednym punktem dostępu używa się skrótu **BSSID**, w sieci z wieloma punktami dostępu skrótem identyfikatora sieci jest natomiast **ESSID**.

W sieciach zawierających więcej niż jeden punkt dostępu pojawia się kilka dodatkowych komplikacji. Po pierwsze, sieć musi być tak skonfigurowana, by tylko jedna stacja bazowa obsługiwała dane z wybranego węzła sieci, nawet jeśli znajduje się on w zasięgu kilku stacji bazowych. Po drugie, jeśli w czasie sesji sieciowej stacja użytkownika znajduje się w ruchu lub gdy w pobliżu pierwszego punktu dostępu występują jakieś lokalne zakłócenia, sieć musi mieć możliwość przekazania połączenia z jednego punktu dostępu do innego. Sieci Wi-Fi radzą sobie z tym problemem przez skojarzenie stacji z tylko jednym punktem dostępu jednocześnie i ignorowanie sygnałów pochodzących z pozostałych stacji. Gdy sygnał pochodzący z jednego punktu dostępu zanika, a silniejszy sygnał dociera z innego punktu dostępu lub gdy natężenie ruchu sieciowego zmusza sieć do równoważenia obciążenia stacji bazowych, może nastąpić przyporządkowanie stacji do nowego punktu dostępu, który jest w stanie zapewnić usługi na akceptowalnym poziomie. Jeśli uważasz, że przypomina to roaming stosowany w telefonii komórkowej, to masz całkowitą słuszność. Nawet terminologia jest tu taka sama — również określa się to mianem **roamingu**.

Sieci publiczne i prywatne

Wi-Fi jest usługą radiową, niewymagającą koncesji, co oznacza, że każdy może uruchomić stację bazową (koncesjonowane usługi radiowe wymagają zazwyczaj uzyskania kosztownego zezwolenia na świadczenie takiej usługi w określonej lokalizacji przez wyznaczony czas). Niektóre z tych stacji bazowych umożliwiają dostęp tylko wybranym użytkownikom, ale inne pozwalają na nawiązanie połączenia przez dowolny komputer znajdujący się w zasięgu sygnału radiowego.

Gdy rozpoczniesz wyszukiwanie sygnału Wi-Fi, prawdopodobnie znajdziesz kilka aktywnych sieci; niektóre z nich mogą być prywatne, a inne będą dostępne dla każdego. Publiczne punkty dostępu, zwane również **hotspotami**, umożliwiają nawiązanie połączenia z każdego komputera, jaki znajduje się w pobliżu; niektóre wymagają płatnych kont, ale istnieje sporo innych, zwłaszcza w takich miejscach, jak szkoły i biblioteki, które są darmowe (choć mogą wymagać podania nazwy użytkownika i hasła).

Większość sieci prywatnych powinna mieć włączoną co najmniej jedną opcję zabezpieczeń, np. szyfrowanie lub ograniczenie dopuszczalnych adresów MAC, które uniemożliwiłyby dostęp nieautoryzowanym użytkownikom, często jednak można spotkać domowe lub firmowe sieci z otwartym dostępem, ponieważ ich właścicielom nie chciało się włączyć opcji zabezpieczających. Informacje na temat wprowadzenia ograniczenia dopuszczalnych adresów MAC i innych opcji zabezpieczeń zostały przedstawione w rozdziale 12.

Podsumowanie

Łącza radiowe, struktura danych oraz architektura sieciowa to trzy główne elementy tworzące wewnętrzną strukturę sieci Wi-Fi. Elementy te powinny być całkowicie niewidoczne dla użytkowników — jeśli mogą oni wysyłać i odbierać wiadomości, czytać pliki lub wykonywać inne działania w sieci, nie powinni przejmować się technicznymi szczegółami funkcjonowania sieci.

Oczywiście, trzeba założyć, że sieć zawsze pracuje prawidłowo, a użytkownicy nie muszą dzwonić do pracowników pomocy technicznej i pytać, czemu nie mogą przeczytać swojej poczty. Po lekturze tego rozdziału prawdopodobnie wiesz już więcej na temat sposobu przesyłania komunikatów w bezprzewodowej sieci LAN, niż 95 procent użytkowników sieci Wi-Fi. Będziesz mógł teraz lepiej zrozumieć pracownika obsługi technicznej, gdy poprosi o sprawdzenie, czy na pewno korzystasz z kanału 11., czy nie trzeba zmienić długości preambuły albo czy Twoja karta sieciowa działa w trybie infrastrukturalnym.