

An abstract graphic of a globe with a network overlay. The globe is composed of a grid of dots, and a complex network of white lines connects various points on its surface, creating a web-like structure. The colors are primarily blue and white.

Wydanie VI

Joe Casad

TCP/IP

w 24 godziny 

SAMS

Helion 

Tytuł oryginału: Sams Teach Yourself TCP/IP in 24 Hours, Sixth Edition

Tłumaczenie: Andrzej Watrak

ISBN: 978-83-283-3708-4

Authorized translation from the English language edition, entitled: SAMS TEACH YOURSELF TCP/IP IN 24 HOURS, Sixth Edition; ISBN 0672337894; by Joe Casad; published by Pearson Education, Inc, publishing as SAMS Publishing.
Copyright © 2017 by Pearson Education, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

Polish language edition published by HELION S.A. Copyright © 2017.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo HELION

ul. Kościuszki 1c, 44-100 GLIWICE

tel. 32 231 22 19, 32 230 98 63

e-mail: helion@helion.pl

WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/tcp246>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

	O autorze	15
CZĘŚĆ I	PODSTAWY TCP/IP	17
Godzina 1.	Czym jest system TCP/IP?	19
	Sieci i protokoły	19
	Rozwój systemu TCP/IP	21
	Cechy systemu TCP/IP	23
	Instytucje standaryzacyjne i specyfikacje RFC	28
	Podsumowanie	29
	Pytania i odpowiedzi	30
	Warsztaty	30
	Ważne pojęcia	31
Godzina 2.	Jak funkcjonuje system TCP/IP?	33
	System protokołów TCP/IP	33
	Modele TCP/IP i OSI	36
	Pakiety danych	38
	Uproszczona struktura sieciowa modelu TCP/IP	39
	Podsumowanie	41
	Pytania i odpowiedzi	41
	Warsztaty	42
	Ważne pojęcia	42
CZĘŚĆ II	SYSTEM PROTOKOŁÓW TCP/IP	45
Godzina 3.	Warstwa dostępową	47
	Protokoły i urządzenia sieciowe	47
	Warstwa dostępową i model OSI	48
	Technologia sieciowa	49
	Adresy fizyczne	51
	Ethernet	52

	Budowa ramki Ethernet	54
	Podsumowanie	55
	Pytania i odpowiedzi	55
	Warsztaty	56
	Ważne pojęcia	56
Godzina 4.	Warstwa sieciowa	59
	Adresy IP — krótkie wprowadzenie	59
	Adresacja komputerów i dostarczanie danych	60
	Protokół IP	62
	Protokół ARP	74
	Protokół RARP	75
	Protokół ICMP	75
	Podsumowanie	77
	Pytania i odpowiedzi	77
	Warsztaty	77
	Ważne pojęcia	78
Godzina 5.	Podsieci i adresacja CIDR	81
	Podsieci	81
	Podział sieci	82
	Stary sposób — maska podsieci	83
	Nowy sposób — adresacja CIDR	90
	Podsumowanie	92
	Pytania i odpowiedzi	92
	Warsztaty	93
	Ważne pojęcia	94
Godzina 6.	Warstwa transportowa	95
	Wprowadzenie do warstwy transportowej	95
	Pojęcia związane z warstwą transportową	96
	Protokoły TCP i UDP	101
	Zapory i porty	110
	Podsumowanie	111
	Pytania i odpowiedzi	112
	Warsztaty	113
	Ważne pojęcia	114

Godzina 7.	Warstwa aplikacyjna	117
	Czym jest warstwa aplikacyjna?	117
	Warstwa aplikacyjna modelu TCP/IP a model OSI	118
	Usługi sieciowe	119
	Interfejsy API i warstwa aplikacyjna	123
	Narzędzia protokołu TCP/IP	123
	Podsumowanie	124
	Pytania i odpowiedzi	124
	Warsztaty	125
	Ważne pojęcia	125
CZĘŚĆ III	SIECI TCP/IP	127
Godzina 8.	Trasowanie	129
	Trasowanie w protokole TCP/IP	129
	Trasowanie w dużych sieciach	140
	Routery wewnętrzne	141
	Routery zewnętrzne i protokół EGP	143
	Trasowanie bezklasowe	145
	Wyższe warstwy	145
	Podsumowanie	146
	Pytania i odpowiedzi	146
	Warsztaty	147
	Ważne pojęcia	147
Godzina 9.	Połączenie z siecią	149
	Telewizja kablowa	149
	Linia DSL	151
	Sieci WAN	152
	Sieci bezprzewodowe	153
	Połączenia wdzwaniane	162
	Urządzenia sieciowe	166
	Przełączanie a trasowanie	170
	Podsumowanie	172
	Pytania i odpowiedzi	172
	Warsztaty	173
	Ważne pojęcia	173

Godzina 10. Odwzorowywanie nazw	177
Co to jest odwzorowywanie nazw?	177
Odwzorowywanie nazw za pomocą plików hostów	179
System DNS	180
Rejestrowanie domen	185
Typy serwerów nazw	186
Domeny i strefy	187
Narzędzia systemu DNS	193
System DDNS	196
System NetBIOS	197
Podsumowanie	198
Pytania i odpowiedzi	198
Warsztaty	199
Ważne pojęcia	199
 Godzina 11. Bezpieczeństwo	 201
Czym jest zaporą sieciowa?	201
Techniki ataków	208
Czego chcą hakerzy?	209
Podsumowanie	221
Pytania i odpowiedzi	222
Warsztaty	222
Ważne pojęcia	223
 Godzina 12. Konfiguracja	 225
Dołączanie się do sieci	225
Przypisywanie adresów IP przez serwer	226
Czym jest protokół DHCP?	227
Jak działa protokół DHCP?	227
Konfiguracja serwera DHCP	230
Translacja NAT	231
Konfiguracja automatyczna	233
Konfigurowanie ustawień TCP/IP	236
Podsumowanie	244
Pytania i odpowiedzi	244
Warsztaty	245
Ważne pojęcia	246

Godzina 13. IPv6 — protokół nowej generacji	247
Po co nowy protokół IP?	247
Format nagłówka IPv6	249
Adresacja IPv6	252
Podsieci	254
Rozgłaszanie komunikatów	254
Adresy lokalne	255
Wykrywanie sąsiadów	255
Automatyczna konfiguracja	255
Protokół IPv6 i jakość usług	256
Protokoły IPv6 i IPv4	257
Tunele IPv6	257
Podsumowanie	260
Pytania i odpowiedzi	260
Warsztaty	261
Ważne pojęcia	261
 CZĘŚĆ IV NARZĘDZIA I USŁUGI	263
Godzina 14. Klasyczne narzędzia	265
Problemy sieciowe	266
Niewłaściwie funkcjonujące lub błędnie skonfigurowane protokoły ...	266
Problemy z łączem	272
Problemy z odwzorowywaniem nazw	272
Problemy z wydajnością sieci	273
Telnet	277
Narzędzia Berkeley	279
SSH	281
Zarządzanie siecią	282
Podsumowanie	288
Pytania i odpowiedzi	288
Warsztaty	289
Ważne pojęcia	290
 Godzina 15. Klasyczne usługi	293
Protokół HTTP	294
Poczta elektroniczna	294
Protokół FTP	295
Protokół TFTP	298

Usługi udostępniania plików i drukarek	299
Protokół LDAP	301
Zdalne sterowanie	304
Podsumowanie	305
Pytania i odpowiedzi	306
Warsztaty	306
Ważne pojęcia	307

CZĘŚĆ V INTERNET 309

Godzina 16. Internet — bliższe spojrzenie	311
Jak wygląda Internet?	311
Co się dzieje w Internecie?	314
Adresy URI i URL	315
Podsumowanie	318
Pytania i odpowiedzi	318
Warsztaty	318
Ważne pojęcia	319

Godzina 17. WWW, HTML i HTTP	321
Co to jest WWW?	321
Język HTML	324
Arkusze CSS	328
Protokół HTTP	329
Skrypty	332
Przeglądarki	335
Sieć semantyczna	338
Język XHTML	341
Język HTML5	341
Podsumowanie	346
Pytania i odpowiedzi	346
Warsztaty	347
Ważne pojęcia	348

Godzina 18. Usługi WWW	349
Systemy zarządzania treścią	349
Portale społecznościowe	351
Blogi i bazy wiedzy	351
Sieci peer-to-peer	354

Usługi WWW	355
Język XML	357
Protokół SOAP	358
Język WDSL	359
Systemy usług WWW	360
Protokół REST	360
Handel elektroniczny	363
Podsumowanie	365
Pytania i odpowiedzi	365
Warsztaty	366
Ważne pojęcia	366
Godzina 19. Szyfrowanie, śledzenie i prywatność transmisji danych	369
Szyfrowanie i poufność danych	369
Śledzenie aktywności użytkowników	384
Sieci anonimowe	392
Podsumowanie	394
Pytania i odpowiedzi	394
Warsztaty	394
Ważne pojęcia	395
CZĘŚĆ VI TCP/IP W PRAKTYCE	397
Godzina 20. Poczta elektroniczna	399
Czym jest poczta e-mail?	399
Format wiadomości e-mail	400
Jak działa poczta e-mail?	401
Protokół SMTP	404
Odczytywanie wiadomości	406
Programy pocztowe	408
Usługa webmail	410
Spam	411
Podszywanie się	413
Podsumowanie	414
Pytania i odpowiedzi	414
Warsztaty	414
Ważne pojęcia	415

Godzina 21. Strumieniowanie i rozgłaszanie danych	417
Problem strumieniowania danych	417
Krótkie wprowadzenie do plików multimedialnych	418
Protokół RTP — strumieniowanie za pomocą protokołu UDP	421
Protokół RTMP — strumieniowanie za pomocą protokołu TCP	424
SCTP i DCCP — zamienniki protokołów warstwy transportowej	425
Strumieniowanie za pomocą protokołu HTTP	425
Protokół HTML5 i multimedia	427
Podcasting	428
Usługa VoIP	428
Podsumowanie	430
Pytania i odpowiedzi	430
Warsztaty	431
Ważne pojęcia	431
Godzina 22. Szybowanie w chmurze	433
Czym jest chmura?	433
Chmury prywatne	443
Przyszłość chmury obliczeniowej	444
Podsumowanie	445
Pytania i odpowiedzi	445
Warsztaty	445
Ważne pojęcia	446
Godzina 23. Internet rzeczy	447
Czym jest Internet rzeczy?	447
Platformy IoT	449
Bliższe spojrzenie — protokół MQTT	452
Technologia RFID	454
Podsumowanie	455
Pytania i odpowiedzi	455
Warsztaty	456
Ważne pojęcia	456
Godzina 24. Implementacja sieci TCP/IP — 7 dni z życia administratora	457
Krótka historia firmy Fikcyjna sp. z o.o.	457
Siedem dni z życia Maurycego	458
Podsumowanie	466

Pytania i odpowiedzi	466
Warsztaty	466
Ważne pojęcia	467

DODATKI 469

Dodatek A	Odpowiedzi na pytania i rozwiązania ćwiczeń	471
	Rozdział 1. Czym jest system TCP/IP?	471
	Rozdział 2. Jak funkcjonuje system TCP/IP?	471
	Rozdział 3. Warstwa dostępową	472
	Rozdział 4. Warstwa sieciowa	473
	Rozdział 5. Podsieci i adresacja CIDR	474
	Rozdział 6. Warstwa transportowa	474
	Rozdział 7. Warstwa aplikacyjna	475
	Rozdział 8. Trasowanie	475
	Rozdział 9. Połączenie z siecią	475
	Rozdział 10. Odwzorowywanie nazw	476
	Rozdział 11. Bezpieczeństwo	476
	Rozdział 12. Konfiguracja	477
	Rozdział 13. IPv6 — protokół nowej generacji	477
	Rozdział 14. Klasyczne narzędzia	477
	Rozdział 15. Klasyczne usługi	478
	Rozdział 16. Internet — bliższe spojrzenie	478
	Rozdział 17. WWW, HTML i HTTP	478
	Rozdział 18. Usługi WWW	479
	Rozdział 19. Szyfrowanie, śledzenie i prywatność transmisji danych	480
	Rozdział 20. Poczta elektroniczna	480
	Rozdział 21. Strumieniowanie i rozgłaszanie danych	481
	Rozdział 22. Szybowanie w chmurze	481
	Rozdział 23. Internet rzeczy	482
	Rozdział 24. Implementacja sieci TCP/IP — 7 dni z życia administratora	482
Dodatek B	Źródła informacji	483
	Skorowidz	485

Godzina 12.

Konfiguracja

W ciągu tej godziny poznasz następujące zagadnienia:

- ▶ dynamiczne przypisywanie adresów IP;
- ▶ protokół DHCP;
- ▶ translacja NAT;
- ▶ konfiguracja Zeroconf.

W dawnych czasach każdy komputer posiadał statyczny adres IP określony w pliku konfiguracyjnym i aby zmienić adres komputera, administrator musiał ten plik edytować. Dzisiejsze sieci wymagają stosowania bardziej zaawansowanych i wygodniejszych metod, umożliwiających dynamiczne i automatyczne konfigurowanie wszystkich komputerów. W tym rozdziale opisanych jest kilka najczęściej stosowanych metod konfigurowania ustawień TCP/IP.

Po przeczytaniu tego rozdziału będziesz potrafił:

- ▶ opisać protokół DHCP i korzyści płynące z jego stosowania;
- ▶ opisać proces przypisywania adresu IP za pomocą protokołu DHCP;
- ▶ opisać zastosowanie translacji NAT;
- ▶ opisać protokoły do automatycznego konfigurowania komputerów.

Dołączanie się do sieci

Protokoły opisane w poprzednich rozdziałach i relacje między nimi mogą przytłaczać, ale współczesne systemy w automatyczny sposób bardzo dobrze radzą sobie z ich wszystkimi niuansami. Od użytkownika wymaga się jedynie podania kilku parametrów konfiguracyjnych TCP/IP podczas instalacji systemu. Choć w różnych systemach wygląda to inaczej, najczęściej trzeba wykonać jedną z poniższych podstawowych operacji:

- ▶ skonfigurowanie statycznego adresu IP;
- ▶ przystosowanie komputera do automatycznego uzyskiwania adresu IP za pomocą protokołu DHCP.

W większości przypadków należy podać również identyfikator, który będzie pełnił funkcję nazwy komputera w sieci (więcej informacji o nazwach hostów oraz o systemach DNS i NetBIOS zawiera rozdział 10., „Odwzorowywanie nazw”).

Jak dowiesz się z dalszej części rozdziału, niektóre systemy operacyjne oferują możliwość automatycznego konfigurowania ustawień TCP/IP, bez konieczności definiowania statycznego ani dynamicznego adresu IP. Funkcjonalność ta stała się w ostatnich latach bardzo popularna.

Po zakończonej instalacji systemu operacyjnego trzeba za pomocą jego interfejsu graficznego wykonać pewne operacje konfiguracyjne. W każdym systemie wygląda to inaczej, ale najbardziej podstawowe parametry są wszędzie takie same. W tym rozdziale poznasz ustawienia TCP/IP stosowane w najnowszych systemach Windows, macOS i Linux Ubuntu. Informacje na temat konfigurowania parametrów w innych systemach znajdziesz w odpowiedniej dokumentacji.

Pojęcie statycznej konfiguracji TCP/IP jest zrozumiałe. Wymaga ona jedynie określenia nazwy komputera, jego adresu IP, maski i adresu bramy domyślnej. Konfiguracja dynamicznego adresu jest jeszcze prostsza, jednak w takim przypadku komputer wykonuje w tle serię operacji za pomocą protokołu **DHCP**, któremu poświęcona jest pierwsza część tego rozdziału.

Przypisywanie adresów IP przez serwer

Jak już wiesz, każdy komputer, aby mógł działać w sieci, musi mieć przypisany adres IP. Pierwotnie adresowanie polegało wyłącznie na konfigurowaniu w każdym komputerze jego własnego adresu IP. Jest to tzw. adresacja statyczna. Każdy komputer po uruchomieniu ma przypisany adres IP i może od razu korzystać z sieci. Adresacja statyczna dobrze sprawdza się w małych, niezmiennych sieciach, ale w dużych sieciach, których konfiguracja nieustannie się zmienia (np. dołączane są i odłączane kolejne komputery), adresacja ta ujawnia pewne swoje ograniczenia.

Adresacja statyczna ma następujące najważniejsze wady:

- ▶ **Pracochłonna konfiguracja** — każdy komputer trzeba osobno skonfigurować. Zmiana zakresu adresów lub innego parametru sieciowego (np. adresu serwera DNS) wymaga modyfikowania konfiguracji każdego komputera.
- ▶ **Nieefektywne gospodarowanie adresami** — adres IP trzeba przypisać każdemu komputerowi niezależnie od tego, czy aktualnie działa w sieci, czy nie działa.
- ▶ **Mała elastyczność** — po przeniesieniu komputera do innej podsieci trzeba ręcznie zmienić jego konfigurację.

W celu rozwiązania powyższych problemów opracowano protokół DHCP umożliwiający konfigurowanie ustawień TCP/IP na żądanie. Jest on udoskonaloną wersją protokołu BOOTP używanego pierwotnie w komputerach bez dysków twardych (takie komputery podczas uruchamiania pobierają przez sieć kompletny system operacyjny). Wraz z wyczerpywaniem się adresów IP i rozwojem dużych, dynamicznych sieci protokół DHCP zyskał w ciągu ostatnich lat ogromną popularność.

Z dużym prawdopodobieństwem można założyć, że większość komputerów korzystających z Internetu uzyskuje konfigurację za pomocą protokołu DHCP. Mały router lub zaporę, z której korzystasz w domu do łączenia się z Internetem, prawdopodobnie również pełni funkcje serwera DHCP. Laptop, który łączy się z siecią bezprzewodową w kawiarni, w taki sam sposób uzyskuje adres IP.

Czym jest protokół DHCP?

DHCP jest to protokół umożliwiający automatyczne konfigurowanie ustawień TCP/IP w komputerach. Protokół ten został zdefiniowany w dokumencie RFC 1531 i zaktualizowany w RFC 1534, 1541, 2131 i 2132. Obecnie obowiązujący standard jest opisany w RFC 2131 i aktualizacjach RFC 3396, 4361, 5494 i 6842. Serwer DHCP przesyła do komputera ustawienia TCP/IP, m.in.: adres IP, maskę podsieci i adres serwera DNS.

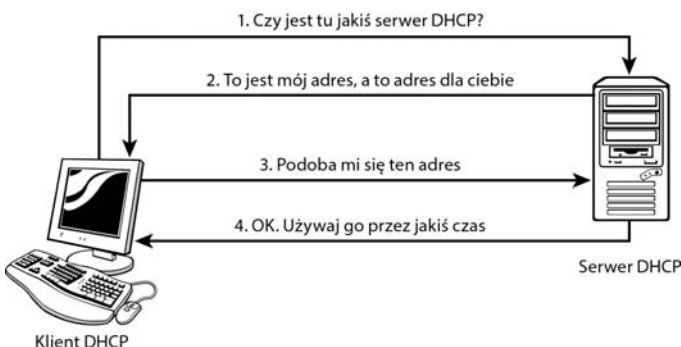
Ponieważ serwer DHCP przypisuje komputerom adresy IP, teoretycznie tylko on musi posiadać statyczny adres IP (inne urządzenia zainstalowane na stałe w sieci, np. drukarki, również często posiadają statyczne adresy). W komputerach stacjonarnych, laptopach i innych urządzeniach klienckich wystarczy skonfigurować parametr umożliwiający uzyskiwanie adresu IP z serwera DHCP. Całą pozostałą konfigurację TCP/IP komputer pobierze z tego serwera. Jeżeli administrator sieci zmieni jakiś jej parametr TCP/IP, wtedy musi jedynie uaktualnić serwer DHCP, a nie każdy komputer użytkownika osobno.

Co więcej, każdy komputer uzyskuje swój adres na określony czas. Jeżeli po upływie tego czasu komputer nie korzysta ze swojego adresu, jest on przypisywany innemu komputerowi. Dzięki temu mechanizmowi zazwyczaj nie jest potrzebnych w sieci tyle adresów IP, ile komputerów z niej korzysta.

Protokół DHCP odgrywa szczególnie ważną rolę w dużych korporacjach, w których wielu użytkowników podłącza swoje laptopy w różnych miejscach sieci. Gdyby taki komputer miał przypisany statyczny adres IP, należałoby go ręcznie zmieniać po każdorazowym podłączeniu komputera do innej podsieci. Jeżeli natomiast komputer korzysta z protokołu DHCP, wtedy automatycznie uzyskuje wszystkie ustawienia TCP/IP z serwera.

Jak działa protokół DHCP?

Gdy komputer korzystający z protokołu DHCP zostanie włączony, uruchamia oprogramowanie obsługujące protokół TCP/IP. Ponieważ komputer nie ma wtedy jeszcze przypisanego adresu IP, nie może się komunikować z innymi komputerami. Może jednak wysyłać i odbierać datagramy rozgłoszeniowe, które stanowią podstawę funkcjonowania protokołu DHCP. Proces uzyskiwania adresu IP z serwera DHCP polega na przesłaniu czterech datagramów (rysunek 12.1):



RYСУNEK 12.1. Proces przypisywania komputerowi użytkownika adresu IP przez serwer DHCP

1. **DHCPDISCOVER** — komputer użytkownika inicjuje proces poprzez wysłanie za pomocą protokołu UDP datagramu rozgłoszeniowego z portem docelowym 67 (jest to port wykorzystywany przez serwery DHCP i BOOTP). Pierwszy datagram jest komunikatem wykrywającym serwer DHCP. Jest to zapytanie o konfigurację skierowane do wszystkich serwerów DHCP. Datagram ten składa się z wielu różnych pól, a jedno z najważniejszych zawiera adres fizyczny komputera użytkownika.
2. **DHCP OFFER** — serwer DHCP przydzielający adresy komputerom w sieci, w której znajduje się komputer użytkownika, wysyła za pomocą protokołu UDP datagram rozgłoszeniowy zawierający odpowiedź na otrzymane zapytanie. Datagram ten ma port docelowy 68 i zawiera adres fizyczny oraz adres IP serwera DHCP, jak również adres IP i maskę podsieci przeznaczone dla komputera użytkownika.

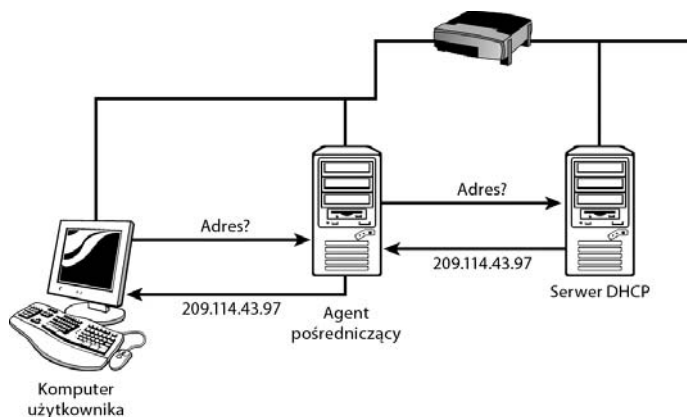
Jeżeli w sieci jest kilka serwerów DHCP, wtedy komputer użytkownika może otrzymać kilka odpowiedzi. Zazwyczaj komputer akceptuje pierwszą z nich.
3. **DHCP REQUEST** — komputer użytkownika odbiera odpowiedź i wysyła datagram rozgłoszeniowy z informacjami dla serwerów DHCP. Datagram ten zawiera adres IP serwera DHCP, od którego pochodzi odpowiedź, oraz adres fizyczny komputera użytkownika. Datagram realizuje dwie podstawowe funkcje. Po pierwsze, informuje wybrany serwer DHCP, że komputer użytkownika zaakceptował przypisany mu adres IP (i inne ustawienia). Po drugie, informuje wszystkie pozostałe serwery DHCP, że komputer użytkownika odrzucił ich odpowiedzi.
4. **DHCP ACK** — serwer DHCP, którego odpowiedź zaakceptował komputer użytkownika, wysyła ostatni **datagram z potwierdzeniem**. Zawiera on przypisany komputerowi adres IP i maskę podsieci. Często zawiera też adres bramy domyślnej, adresy serwerów DNS i jeden lub dwa adresy serwerów WINS. Oprócz tego datagram może zawierać dodatkowe informacje, takie jak typ węzła NetBIOS-a określający sposób odwzorowywania nazw.

W potwierdzeniu zawarte są również trzy ważne pola określające różne przedziały czasu. Pierwsze pole określa czas przypisania adresu, natomiast dwa pozostałe, oznaczone jako T1 i T2, są wykorzystywane przez komputer użytkownika do przedłużenia czasu przypisania adresu.

Agenty pośredniczące

Jeżeli komputer użytkownika i serwer DHCP znajdują się w tym samym segmencie sieci, proces przypisywania adresu przebiega dokładnie w opisany wyżej sposób. Jeżeli natomiast oba urządzenia znajdują się w różnych podsieciach połączonych za pomocą jednego lub kilku routerów, proces jest bardziej skomplikowany. Routery zazwyczaj nie przesyłają datagramów rozgłoszeniowych, dlatego aby można było używać protokołu DHCP, potrzebne są urządzenia pośredniczące. Takim urządzeniem może być komputer zainstalowany w tej samej podsieci co komputer użytkownika albo sam router. W obu przypadkach urządzenie to nosi nazwę **agenta pośredniczącego DHCP** lub **agenta pośredniczącego BOOTP**.

Agent posiada statyczny adres IP i zna adres IP serwera DHCP, dzięki temu może odbierać i wysyłać datagramy. Ponieważ znajduje się w tej samej podsieci co komputer użytkownika, może się z nim komunikować za pomocą datagramów rozgłoszeniowych (rysunek 12.2).



RYSUNEK 12.2. Agent DHCP umożliwia komputerowi użytkownika komunikowanie się z serwerem DHCP znajdującym się w innej podsięci

Agent odbiera datagramy rozgłoszeniowe wysyłane na port UDP 67. Jeżeli taki datagram zawiera zapytanie skierowane do serwera DHCP, przesyła je bezpośrednio do niego. Gdy agent odbierze odpowiedź z serwera DHCP, wtedy wysyła ją za pomocą datagramu rozgłoszeniowego do wszystkich komputerów w podsieci. W celu zwięzłości opisu zostało tu pominiętych kilka szczegółów, niemniej jednak oddana jest istota funkcji agenta.

Często stosowana praktyka łączenia serwera DHCP i routera w jednym urządzeniu zmniejsza w większości sieci potrzebę stosowania agentów. Więcej informacji o agentach zawiera dokument RFC 1542.

Pola czasu w odpowiedzi DHCP

Komputer użytkownika uzyskuje adres IP z serwera DHCP na określony czas. Ten czas jest skonfigurowany na serwerze DHCP. Pola T1 i T2 umieszczone w komunikacie DHCPACK są wykorzystywane do przedłużania okresu przypisania adresu. Pole T1 oznacza moment, w którym komputer użytkownika powinien rozpocząć proces przedłużania. Zazwyczaj przypada on w połowie okresu przypisania adresu. Załóżmy, że okres przypisania adresu wynosi osiem dni. W takim przypadku po czterech dniach komputer użytkownika wysyła do serwera DHCP datagram DHCPREQUEST z zapytaniem o możliwość przedłużenia okresu przypisania. Jeżeli serwer DHCP jest dostępny, wtedy zazwyczaj odsyła odpowiedź DHCPACK zawierającą przedłużenie okresu. Tym razem jednak oba komunikaty nie są przesyłane za pomocą datagramów rozgłoszeniowych, ale bezpośrednio pomiędzy obydwojema urządzeniami. Jest to możliwe, ponieważ w tym czasie posiadają one ważne adresy IP.

Jeżeli serwer DHCP nie jest dostępny w połowie okresu przypisania adresu (tj. po czterech dniach), wtedy komputer użytkownika ponawia próbę po trzech czwartych okresu, czyli po sześciu dniach. Jeżeli ta próba również się nie powiedzie, następna jest podejmowania po upływie siedmiu ósmych okresu. Za każdym razem komputer użytkownika wysyła datagramy bezpośrednio do serwera DHCP. Jeżeli wszystkie próby zakończą się niepowodzeniem, to w chwili T2 komputer wyśle komunikat rozgłoszeniowy do wszystkich serwerów

DHCP w sieci. Jeżeli i tym razem nie uda się przedłużyć okresu przypisania adresu ani uzyskać nowego, komputer musi zwolnić przypisany mu adres i zaprzestać wykonywania wszelkich operacji za pomocą protokołu TCP/IP.

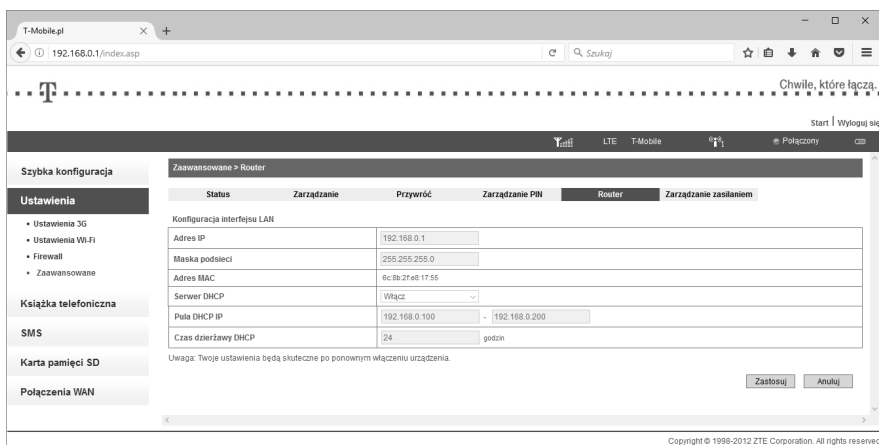
Konfiguracja serwera DHCP

Jeżeli nie jesteś administratorem średniej ani dużej sieci, prawdopodobnie nie miałeś okazji konfigurowania serwera DHCP. Jeżeli jednak konfigurowałeś serwer, to prawdopodobnie korzystałeś z dokumentacji zawierającej znacznie bardziej szczegółowe informacje niż zawarte w tej książce.

System Windows oferuje graficzny interfejs do konfigurowania serwera DHCP. W systemie Linux jest to usługa `dhcpd`. Konfiguracja tej usługi może być różna w zależności od odmiany systemu, ale zazwyczaj jest zapisana w pliku `/etc/dhcpd.conf`. Plik ten zawiera informacje niezbędne do przypisywania adresów IP komputerom użytkowników, jak również opcjonalne ustawienia, np.: adres rozgłoszeniowy, nazwę domeny, adres serwera DNS i bramy domyślnej. Poniżej przedstawiony jest przykładowy plik `/etc/dhcpd.conf`:

```
default-lease-time 600;
max-lease-time 7200;
option domain-name "helion.pl";
option subnet-mask 255.255.255.0;
option broadcast-address 185.142.13.255;
subnet 185.142.13.0 netmask 255.255.255.0 {
    range 185.142.13.10 185.142.13.50;
    range 185.142.13.100 185.142.13.200;
}
```

Jak wspominałem wcześniej w tym rozdziale, funkcję serwera DHCP często pełni router lub zaporę. W instrukcji do swojego routera znajdziesz informacje, jak skonfigurować serwer DHCP. W urządzeniach tego typu zazwyczaj wykorzystuje się do tego celu przeglądarkę (rysunek 12.3). Po zalogowaniu się do routera można zmienić konfigurację serwera DHCP. W większości przypadków nie jest to jednak konieczne.



RYСУNEK 12.3. Konfiguracja serwera DHCP w domowym routerze

Czasami zdarza się, że niektóre urządzenia w sieci muszą posiadać statyczny adres IP, nawet jeżeli wszystkie komputery uzyskują swoje adresy dynamicznie. Na przykład drukarka musi mieć statyczny adres, aby w komunikujących się z nią komputerach nie trzeba było nieustannie aktualizować jej adresu. Niektóre serwery oferują usługę zwaną rezerwacją adresu IP, umożliwiającą wiązanie adresów IP z adresami fizycznymi (MAC). Dzięki temu urządzenie w sieci zawsze uzyskuje z serwera ten sam adres IP.

Translacja NAT

Ekspertci zauważyli, że skoro serwer DHCP przypisuje komputerom adresy IP, nie ma ważnego powodu, aby były to oficjalne, „legalne” adresy internetowe. Wystarczy, aby tylko router miał taki adres i mógł pełnić funkcję pośrednika w komunikacji komputerów z Internetem, tj. zmieniać lokalne adresy w wysyłanych przez nich datagramach na adresy z publicznego zakresu stosowanego w Internecie. Wiele nowoczesnych routerów oferuje usługę zwaną **translacją adresów** (ang. *Network Address Translation* — NAT).

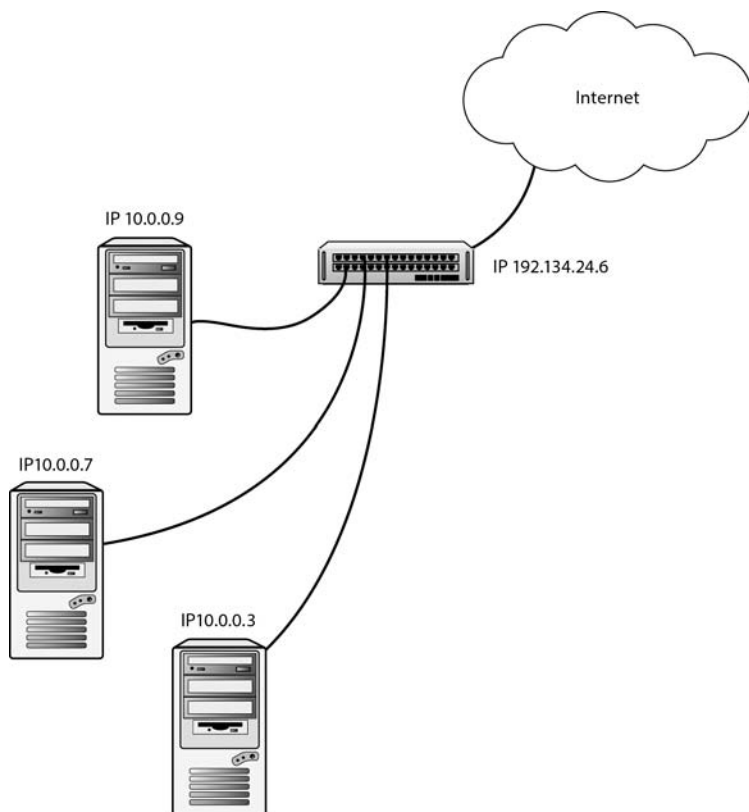
Translacja NAT pozwala ukryć przed zewnętrznymi urządzeniami szczegóły lokalnej sieci, a nawet ukryć jej istnienie. Rysunek 12.4 przedstawia urządzenie realizujące translację NAT. Umożliwia ono komputerom w lokalnej sieci komunikowanie się z Internetem. W lokalnej sieci mogą być stosowane adresy IP z dowolnego zakresu. Gdy komputer w sieci lokalnej potrzebuje skomunikować się z serwerem w Internecie, wtedy w połączeniu pośredniczy urządzenie NAT. Zmienia ono we wszystkich pakietach odbieranych z Internetu adresy docelowe na adresy stosowane w lokalnej sieci i przesyła je do komputera, który nawiązał połączenie.

Translacja NAT zwiększa bezpieczeństwo sieci, ponieważ uniemożliwia hakerowi z zewnątrz jej wykrycie (aczkolwiek sama translacja nie powinna być stosowana jako jedyny środek bezpieczeństwa). Z zewnątrz sieci urządzenie NAT wygląda jak pojedynczy host dołączony do Internetu. Nawet jeżeli haker będzie znał lokalny adres komputera w sieci, nie będzie mógł nawiązać z nim połączenia, ponieważ lokalne adresy nie są w żaden sposób powiązane z adresami stosowanymi w Internecie. Jak dowiedziałeś się z rozdziału 4., „Warstwa sieciowa”, dla lokalnych sieci zarezerwowane są poniższe „prywatne” zakresy adresów IP:

- ▶ od 10.0.0.0 do 10.255.255.255;
- ▶ od 172.16.0.0 do 172.31.255.255;
- ▶ od 192.168.0.0 do 192.168.255.255.

(W dalszej części rozdziału dowiesz się, że zakres od 169.254.0.0 do 169.254.255.255 jest przeznaczony do automatycznego konfigurowania adresów IP i nie jest uwzględniany w translacji NAT).

Translacja NAT obejmuje zazwyczaj adresy z powyższych prywatnych zakresów. Adresy te nie są stosowane w sieciach publicznych, więc komputer może komunikować się z Internetem *wyłącznie* za pośrednictwem urządzenia NAT. Dzięki translacji liczba publicznych adresów internetowych wykorzystywanych w instytucji może być mniejsza. Jedynie router realizujący translację musi mieć publiczny adres internetowy. Dzięki możliwości zmniejszenia liczby stosowanych adresów publicznych i poprawie bezpieczeństwa sieci translacja NAT stała się bardzo popularna zarówno w sieciach korporacyjnych, jak i domowych.

**RYSUNEK 12.4.** Translacja NAT

Oczywiście bezpieczeństwo sieci często nie jest takie, jakiego można sobie życzyć. Nawet pozornie odporne na włamania urządzenie NAT jest podatne na ataki. Niektóre urządzenia oferują specjalne funkcjonalności umożliwiające uzyskanie do nich dostępu administracyjnego z Internetu. Jeżeli funkcjonalności te nie zostaną wyłączone, mogą narazić sieć na niebezpieczeństwo.

Rosnąca popularność translacji NAT spowodowała pojawienie się nowych technik omijania naturalnych zabezpieczeń lokalnych sieci. Jedną z nich, umożliwiającą hakerowi dostanie się do lokalnej sieci, polega na uzyskaniu zaproszenia od użytkownika. Hakerzy często wysyłają wiadomości e-mail z odnośnikami do fałszywych stron WWW, aby sprowokować użytkowników do nawiązania połączenia z niebezpiecznym serwerem. Zagrożenie tego typu atakami jest jednym z powodów, dla których ostrzega się użytkowników przed klikaniem odnośników w nieoczekiwanych wiadomościach. Dzisiejsze przeglądarki udaremniają niekiedy ataki realizowane za pomocą skryptów międzydomenowych i innych metod.

Przy okazji

Protokół IPv6 i translacja NAT

Protokół nowej generacji, IPv6, oferuje funkcje lokalnej adresacji, które mogą sprawić, że urządzenia NAT stosowane w dzisiejszych sieciach staną się niepotrzebne. Więcej informacji na temat protokołu IPv6 znajdziesz w rozdziale 13., „IPv6 — protokół nowej generacji”.

Konfiguracja automatyczna

Zapewne zastanawiasz się, co się stanie, gdy komputery w sieci będą przystosowane do pobierania konfiguracji z serwera DHCP, ale serwer ten będzie niedostępny. Komputery nie mają przypisanych statycznych adresów IP ani nie będą mogły ich uzyskać za pomocą protokołu DHCP. W takiej sytuacji istnieje możliwość (choć jest to rzadki przypadek) utworzenia małej grupy komputerów bez łączności z Internetem ani żadnym serwerem DHCP czy routerem.

Twórcy systemów operacyjnych opracowali metody umożliwiające komputerom znajdującym się w lokalnej sieci nawiązywanie między sobą komunikacji bez konieczności statycznego przypisywania adresów IP ani korzystania z protokołu DHCP. Pierwsze protokoły stosowane w sieciach LAN, np. NetBEUI (w systemie Windows) i AppleTalk (w systemie Apple), oferowały funkcje komunikacji sieciowej bez konieczności jej konfigurowania, dlatego dostawcy systemów operacyjnych zaczęli szukać możliwości zaimplementowania ich w modelu TCP/IP.

Pierwszym krokiem w tym kierunku było opracowanie koncepcji **lokalnej adresacji łącza** (ang. *link-local addressing* — IPv4LL). Funkcjonalność tę posiadają systemy Apple, począwszy od wersji iOS9, oraz Microsoft od wersji Windows 98.

W systemach Windows funkcjonalność IPv4LL nosi nazwę **APIPA** (ang. *Automatic Private IP Addressing* — automatyczne przypisywanie prywatnych adresów IP). Jeżeli komputer nie ma przypisanego statycznego adresu IP i nie może go uzyskać w sposób dynamiczny, wtedy sam przypisuje sobie adres z nieużywanego w publicznych sieciach zakresu od 169.254.0.0 do 169.254.255.255. Jeżeli inne komputery w sieci znajdują się w podobnej sytuacji, również przypisują sobie wolne adresy z powyższego zakresu. Dzięki temu komputery mogą komunikować się ze sobą w obrębie lokalnej sieci. Oczywiście ponieważ ich adresy nie są stosowane w publicznych sieciach, nie mogą komunikować się z Internetem ani serwerami spoza lokalnej sieci.

Istota adresacji APIPA polega na tym, że nie wymaga konfiguracji, więc nic więcej na ten temat nie można powiedzieć. W większości systemów Windows funkcjonalność tę można *wyłączyć*, zmieniając klucz w rejestrze. Szczegółowe informacje na ten temat znajdują się w dokumentacji do systemu.

Adresacja APIPA może być przyczyną problemów. Jeżeli komputery uzyskują swoje konfiguracje w prawidłowy sposób, ale jeden z nich dziwnym trafem nie może się komunikować, wtedy trzeba sprawdzić, czy nie utracił łączności z serwerem DHCP i czy nie użył adresacji APIPA do samodzielnego przypisania sobie adresu spoza zakresu stosowanego w sieci.

Nowsza technologia o nazwie **Zeroconf** jest znacznie doskonalsza i całkowicie zautomatyzowana. Stanowi rozszerzenie adresacji IPv4LL i umożliwia w pełni automatyczną konfigurację małych lokalnych sieci. Adresacja Zeroconf zaimplementowana w systemach Apple nosi nazwę Bonjour. W systemach Windows dostępna jest podobna funkcjonalność wykorzystująca nieco inne protokoły. W systemach Linux adresacja ta nosi nazwę Avahi i jest podobna do tej z systemów Apple'a.

Nowa automatyczna adresacja posiada trzy ważne funkcjonalności:

- ▶ **Adresacja lokalnego łącza** (ang. *link-local addressing*) — komputery same przypisują sobie adresy IP z zakresu od 169.254.0.0 do 169.254.255.255 (zob. opis IPv4LL wyżej).
- ▶ **Rozgłoszeniowe odwzorowywanie nazw** (ang. *Multicast DNS*) — nazwy nie są odwzorowywane za pomocą serwera DNS ani pliku hostów, ale za pomocą zapytań wysyłanych na określony rozgłoszeniowy adres IP i port. Komputery w sieci odbierają te zapytania i odsyłają odpowiedzi zawierające żądane informacje.
- ▶ **Wykrywanie usług za pomocą DNS** (ang. *DNS Service Discovery*) — komputery same dowiadują się o dostępnych w sieci usługach.

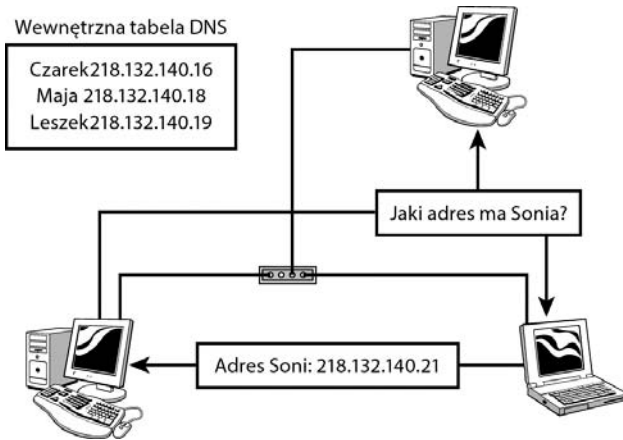
Powyższe funkcjonalności umożliwiają utworzenie środowiska, w którym komputer bez żadnej wstępnej konfiguracji TCP/IP może uzyskać prywatny adres IP, przekazać innym komputerom swoją nazwę i wykryć dostępne usługi (np. serwery plików lub wydruków). Usługi te są dostępne w przeglądarce plików pod nazwą *Otoczenie sieciowe* i można z nich łatwo korzystać, klikając wybraną pozycję.

Gdy pojawiła się potrzeba stworzenia odpowiednika usługi DNS, umożliwiającego korzystanie z usług i urządzeń w prostych sieciach bez konieczności konfigurowania komputerów, jak w przypadku adresacji AppleTalk, firma Apple opracowała technologie uzupełniające funkcjonalności rozgłoszeniowego odwzorowywania nazw i wykrywania usług. Technologie te pozwalają uzyskać wgląd w lokalną sieć, ale nie sprawdzają się w dużych sieciach. Są raczej przystosowane do pojedynczych segmentów LAN.

Komputer obsługujący rozgłoszeniowe odwzorowywanie nazw (mDNS) posiada własną bazę danych, którą wykorzystuje do odwzorowywania nazw. Jak pokazuje rysunek 12.5, gdy komputer musi użyć nazwy, której nie ma w bazie, wtedy rozsyła komunikat na rozgłoszeniowy adres 224.0.0.251. Inne komputery, obsługujące odwzorowywanie mDNS, odbierają zapytania wysyłane na powyższy adres. Komputer, który może odpowiedzieć na zapytanie, wysyła komunikat zawierający adres IP powiązany z daną nazwą.

Funkcjonalność wykrywania usług (DNS-SD) umożliwia komputerom rozgłaszanie informacji o oferowanych przez nich usługach. Popularne dzisiaj małe urządzenia przenośne szeroko korzystają z tej funkcjonalności, dzięki której mogą szybko połączyć się z siecią i wykryć przydane urządzenia, np. drukarki czy serwery muzyczne, bez konieczności uprzedniej konfiguracji.

Wykrywanie DNS-SD polega na przesyłaniu rekordów SRV zawierających informacje o usługach dostępnych w sieci. Na przykład w sieci z konwencjonalną usługą DNS rekord SRV może zawierać nazwę i adres IP serwera FTP lub kontrolera domeny. W wykrywaniu DNS-SD wykorzystywane są na małą skalę odmiany powyższego rekordu i kilku innych.



RYSUNEK 12.5. W usłudze mDNS każdy komputer posiada własną bazę nazw i adresów (w praktyce komputery przesyłają między sobą również inne informacje niezbędne do odwzorowywania nazw)

Na przykład rekord PTR (wykorzystywany do odwzorowywania adresów IP) zawiera informacje o instancjach dostępnych w sieci usług. Odpowiedź na zapytanie może zawierać następujące informacje:

- ▶ **Instancja usługi** (możliwy jest przypadek, w którym kilka serwerów w tej samej sieci oferuje tę samą usługę).
- ▶ **Nazwa usługi** (lista typów usług jest dostępna na stronie: <http://www.dns-sd.org>).
- ▶ **Nazwa domeny**, w której dostępna jest usługa.

Na podstawie odebranych odpowiedzi komputer tworzy listę dostępnych w sieci usług i ich instancji.

Gdy użytkownik lub aplikacja wybierze określoną usługę z listy, wtedy uzyska nazwę hosta i numer portu niezbędne do nawiązania połączenia z serwerem. Ponadto otrzyma rekord TXT zawierający dodatkowe informacje o usłudze.

Wykrywanie usługi opiera się na wysyłaniu rozgłoszeniowych zapytań DNS, dzięki czemu nie jest konieczna konfiguracja tej usługi, ale po wprowadzeniu pewnej minimalnej konfiguracji można z niej korzystać również w sieciach z zaimplementowaną konwencjonalną usługą DNS.

Firma Microsoft opracowała alternatywną do mDNS usługę o nazwie **LLMNR** (ang. *Link-Local Multicast Name Resolution* — lokalne rozgłoszeniowe odwzorowywanie nazw). Protokół **SSDP** (ang. *Simple Service Discovery Protocol* — prosty protokół wykrywania usług) umożliwia wykrywanie usług. Wykorzystuje on jednak protokół HTTP, a nie tradycyjną usługę DNS. Wpisuje się więc w trend tworzenia usług opartych na adresach URL, ale nie jest kompatybilny z konwencjonalną usługą DNS. Protokół UPnP (ang. *Universal Plug and Play* — uniwersalne urządzenie typu „podłącz i korzystaj”), umożliwiający wykrywanie usług podobnie jak w DNS-SD, jest oparty na protokole SSDP.

Microsoft, Apple i inni producenci oprogramowania uczestniczą w otwartej dyskusji na temat automatycznej konfiguracji ustawień TCP/IP, ale ich systemy różnią się od siebie.

Największe różnice są widoczne w protokołach wykrywania usług. Jeszcze inny protokół, SLP (ang. *Service Location Protocol* — protokół lokalizowania usług), jest stosowany w drukarkach HP i wielu innych urządzeniach.

Protokoły automatycznej konfiguracji zostały zdefiniowane w różnych dokumentach RFC, a analogiczny system jest równolegle rozwijany w ramach protokołu IPv6. W ciągu najbliższych lat funkcjonalności automatycznej konfiguracji niewątpliwie będą zyskiwały coraz większą popularność.

Przy okazji

Odmiany adresacji Zeroconf

Fakt, że najwięksi dostawcy systemów operacyjnych oferują własne wersje protokołów, nie oznacza, że w danym systemie można stosować tylko ten akurat protokół. Programiści tworzący aplikacje mogą dowolnie dostosowywać wykorzystywane przez siebie protokoły. Firma Apple opracowała nawet odmianę swojej adresacji Bonjour przeznaczoną dla systemów Windows.

Konfigurowanie ustawień TCP/IP

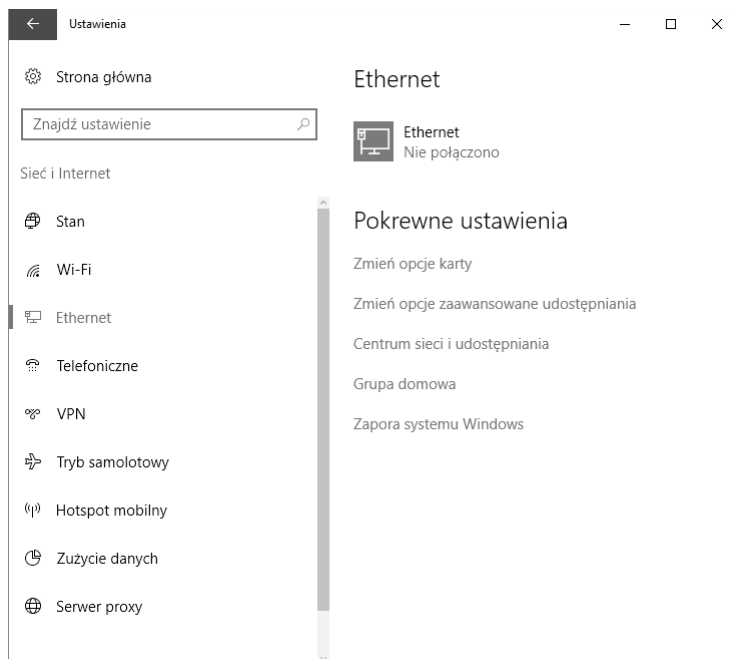
Jak już wspomniałem w tym rozdziale, większość dzisiejszych komputerów wymaga zdefiniowania bardzo prostych ustawień sieciowych, a najczęściej dokonuje się tego, korzystając ze specjalnego kreatora podczas instalacji systemu lub jego pierwszego uruchomienia. Trzeba wtedy określić nazwę komputera, zdecydować, czy ma on posiadać statyczny, czy dynamiczny adres IP, wybrać kilka podstawowych ustawień, a całą resztą zajmie się system. Później jednak może pojawić się potrzeba sprawdzenia ustawień sieciowych, a czasami również ich zmiany. W kolejnych częściach rozdziału opisane są typowe ustawienia TCP/IP w systemach: Windows, macOS i Linux Ubuntu.

Konfiguracji i diagnostyce ustawień sieciowych w powyższych trzech systemach można byłoby z łatwością poświęcić osobną książkę. Poniższe sekcje nie stanowią pełnego podręcznika konfiguracyjnego i diagnostycznego. Ich celem jest dostarczenie ogólnych informacji o konfigurowaniu środowiska sieciowego i pokazanie, jak za pomocą interfejsu graficznego można zmieniać ustawienia protokołów sieciowych. Szczegółowe informacje na temat konfiguracji poszczególnych systemów znajdziesz w dokumentacji i w Internecie.

Windows

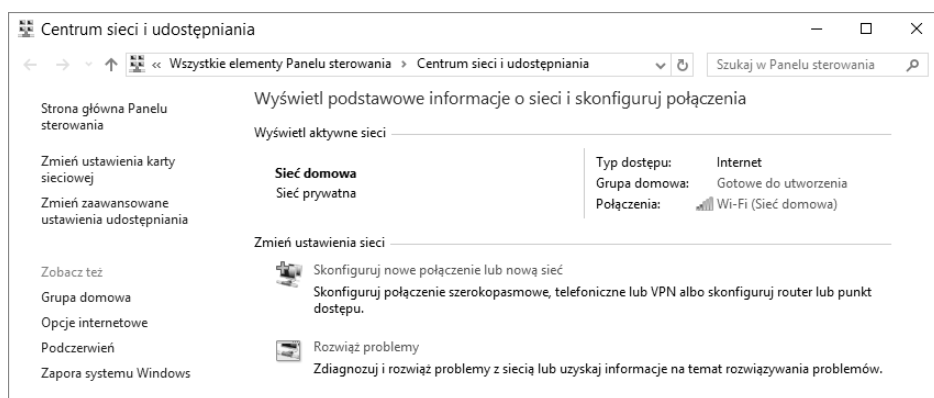
Ustawienia sieciowe w systemie Windows są zapisane w rejestrze. Manipulowanie rejestrem jest niebezpieczną operacją, chyba że wie się dokładnie, co się robi. Dlatego preferowaną metodą konfigurowania ustawień sieciowych jest korzystanie z graficznych narzędzi. Zgodnie z przyjętą w systemie Windows zasadą różnorodne okna dialogowe można otwierać na kilka sposobów. W najnowszych wersjach systemu ustawienia sieciowe są dostępne w narzędziu zwanym *Centrum sieci i udostępniania*. Aby otworzyć to narzędzie w systemie Windows 7, należy kliknąć przycisk *Start* i polecenie *Panel sterowania*. Następnie w głównym oknie panelu należy kliknąć ikonę *Sieć i Internet*, a potem odnośnik *Centrum*

sieci i udostępniania. W systemie Windows 10 po kliknięciu przycisku *Start* trzeba kliknąć ikonę *Ustawienia*. Po wybraniu opcji *Sieć i Internet* pojawiają się różne opcje konfiguracyjne (rysunek 12.6).



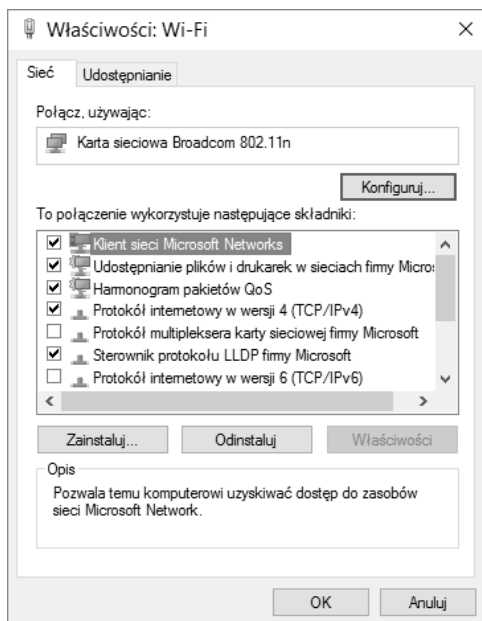
RYСУNEK 12.6. Okno ustawień sieciowych w systemie Windows 10

W górnej części okna *Centrum sieci i udostępniania* (rysunek 12.7) znajdują się bieżące ustawienia sieciowe, a po lewej stronie opcje konfiguracyjne. Aby utworzyć nowe połączenie sieciowe, należy kliknąć odnośnik *Skonfiguruj nowe połączenie lub nową sieć*.



RYСУNEK 12.7. Centrum sieci i udostępniania w systemie Windows 10

W systemie Windows każde połączenie sieciowe jest traktowane jako osobny obiekt. Aby sprawdzić aktualnie skonfigurowane połączenia sieciowe w systemie Windows 7 lub nowszym, należy kliknąć odnośnik *Zmień ustawienia karty sieciowej*. Pojawi się okno zawierające jedną lub kilka ikon reprezentujących połączenia lokalne, bezprzewodowe i inne. Po kliknięciu prawym przyciskiem myszy jednej z ikon i wybraniu polecenia *Właściwości* pojawi się okno z ustawieniami (rysunek 12.8).

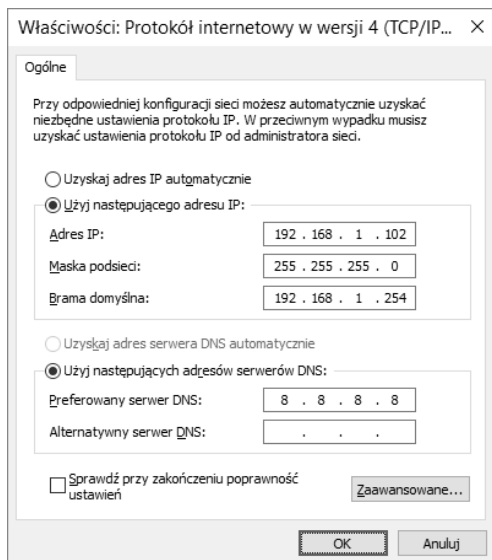


RYСУNEK 12.8. Okno z właściwościami połączenia sieciowego

Jak widać na rysunku 12.8, okno *Właściwości* zawiera listę tzw. *składników* połączenia sieciowego. Słowo „składnik” może wydawać się nieścisłe, ale szybko można się przekonać, że oznacza ono opcjonalny komponent modelu TCP/IP. Trzy pierwsze składniki na rysunku 12.8 należą do warstwy aplikacyjnej modelu TCP/IP.

Aby sprawdzić aktualne ustawienia TCP/IP (przy założeniu, że system wykorzystuje protokół IPv4, jak w ogromnej większości przypadków), kliknij składnik *Protokół internetowy w wersji 4 (TCP/IPv4)*, a następnie przycisk *Właściwości*.

W oknie z właściwościami (rysunek 12.9) można przede wszystkim określić, czy komputer ma uzyskiwać adres IP automatycznie za pomocą protokołu DHCP, czy też ma mieć przypisany adres statyczny. Jeżeli Twój komputer ma ustawione automatyczne uzyskiwanie adresu IP i funkcjonuje prawidłowo, lepiej pozostaw te ustawienia bez zmian. Jeżeli natomiast chcesz ręcznie zmienić ustawienia, kliknij opcję *Użyj następującego adresu IP*, a następnie wpisz adres komputera, maskę i adres bramy domyślnej (muszą to być parametry właściwe dla Twojej sieci; więcej informacji na temat adresów IP i masek znajdziesz w rozdziałach 4., „Warstwa sieciowa”, i 5., „Podsieci i adresacja CIDR”).



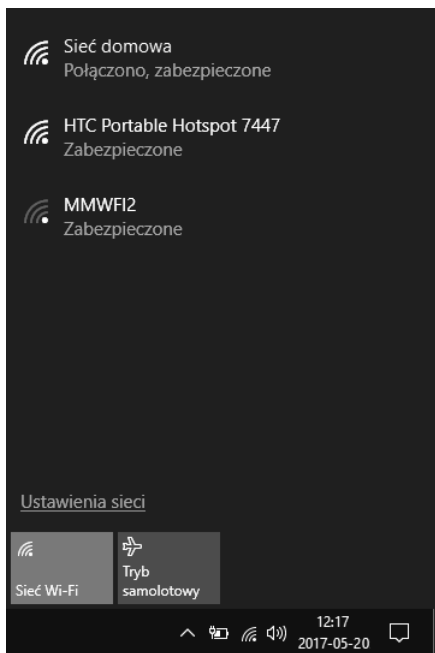
RYSUNEK 12.9. Właściwości protokołu IPv4 w systemie Windows

Przycisk *Zaawansowane* (widoczny na rysunku 12.9) otwiera okno umożliwiające określenie dodatkowych ustawień bramy domyślnej, jak również serwerów DNS i WINS (zob. rozdział 10.).

Zaletą osobnych, logicznych obiektów jest możliwość definiowania osobnych połączeń sieciowych wykorzystywanych w różnych sytuacjach. Jeżeli Twój komputer wykorzystuje protokół DHCP, prawdopodobnie nie ma potrzeby tworzenia dodatkowych połączeń. Wystarczy, że podłączysz komputer do sieci, a swoją konfigurację określi on sam. Jeżeli jednak używasz laptopa, którego podłączasz do różnie skonfigurowanych sieci (np. jednej z zastosowanym protokołem DHCP, a potem innej ze statycznymi adresami IP), wtedy musisz utworzyć osobne połączenia. W tym celu w oknie *Centrum sieci i udostępniania* kliknij polecenie *Skonfiguruj nowe połączenie lub nową sieć*. Otworzy się nowe okno, w którym będziesz mógł uruchomić kreator sieci LAN, sieci bezprzewodowej, szerokopasmowej lub VPN. W każdym przypadku kreator wyszuka niezdefiniowane połączenia i pozwoli Ci wybrać dostępną sieć lub urządzenie.

Jak już wiesz, połączenie bezprzewodowe pod względem funkcjonowania w warstwach wyższych niż sieciowa nie różni się od innego typu połączeń. Jednak ze względu na swój charakter konfigurowanie połączenia bezprzewodowego i korzystanie z niego wygląda nieco inaczej niż w innych połączeniach.

W komputerach z systemem Windows połączenie bezprzewodowe jest zazwyczaj konfigurowane automatycznie. Czasami, w zależności od ustawień, komputer po uruchomieniu może nie łączyć się automatycznie z siecią bezprzewodową. Aby otworzyć listę dostępnych sieci bezprzewodowych, kliknij ikonę połączenia bezprzewodowego znajdującą się w prawym dolnym rogu ekranu. Zaznacz na liście żadaną sieć i kliknij przycisk *Połącz* (rysunek 12.10). Będziesz musiał wpisać niezbędne dane, np. identyfikator SSID (*Service Set Identifier* — identyfikator usługi sieciowej).



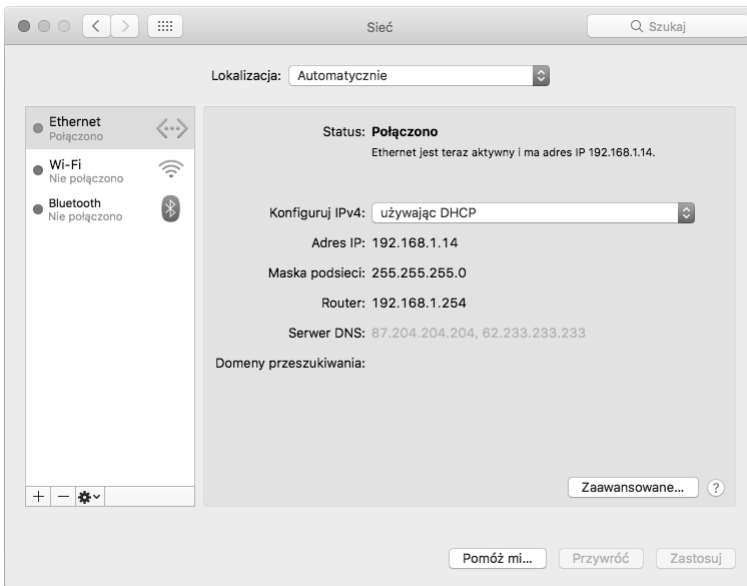
RYSUNEK 12.10. Lista sieci bezprzewodowych w systemie Windows 10

macOS

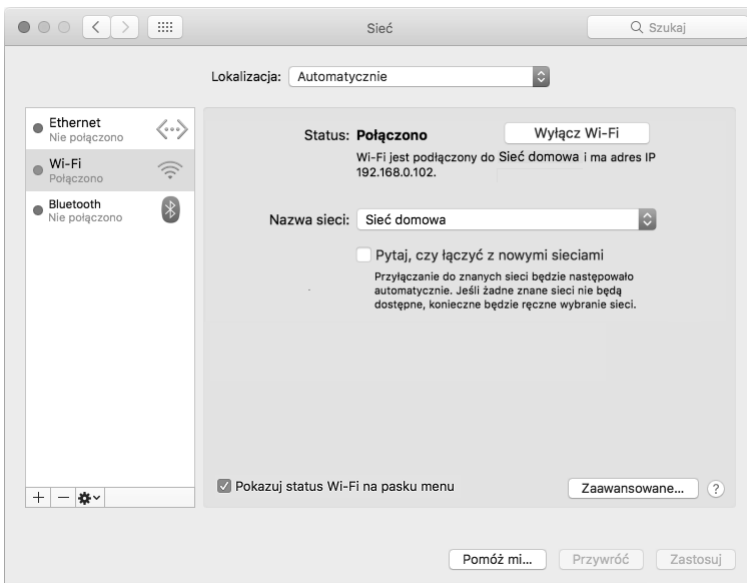
W systemie macOS, podobnie jak w Windowsie, można w prosty sposób wyszukiwać dostępne sieci przewodowe i bezprzewodowe i łączyć się z nimi, jeżeli jest w nich stosowany protokół DHCP. Aby otworzyć ustawienia sieciowe, kliknij na pasku narzędzi ikonę *Preferencje systemowe*, a następnie ikonę *Sieć*. Okno *Sieć* (rysunek 12.11) jest centralnym miejscem, w którym konfiguruje się ustawienia TCP/IP. Aby zobaczyć ustawienia zwykłego przewodowego połączenia LAN, kliknij na liście sieci po lewej stronie pozycję *Ethernet*.

Kliknij rozwijaną listę *Konfiguruj IPv4* umożliwiającą wybranie protokołu DHCP lub ręczne wpisanie konfiguracji. Jeżeli wybierzesz pozycję *ręcznie*, będziesz mógł wpisać adres IP komputera, maskę i adres bramy domyślnej. Aby wpisać dodatkowe informacje, np. ustawienia serwerów DNS lub WINS, kliknij przycisk *Zaawansowane*. Na koniec kliknij przycisk *Zastosuj*, aby zapisać wprowadzone zmiany.

Aby określić ustawienia sieci bezprzewodowej, kliknij po lewej stronie pozycję *Wi-Fi* (w starszych systemach jest stosowana nazwa *AirPort*). Aby włączyć lub wyłączyć połączenie bezprzewodowe, kliknij przycisk w prawej górnej części okna (rysunek 12.12). W liście *Nazwa sieci* wybierz sieć, z którą chcesz się połączyć. Jeżeli wybierzesz opcję *Przyłącz się do innej sieci*, będziesz musiał podać identyfikator SSID sieci, hasło i inne informacje. Opcja *Sieci komputer-komputer* umożliwia utworzenie połączenia *ad hoc* z innym komputerem wyposażonym w kartę bezprzewodową.



RYSUNEK 12.11. Ustawienia TCP/IP w systemie macOS



RYSUNEK 12.12. Konfiguracja połączenia bezprzewodowego w systemie macOS

Na pasku narzędzi w systemie macOS dostępna jest również ikona umożliwiająca wygodne wybieranie sieci bezprzewodowej i określanie ustawień konfiguracyjnych.

Przy okazji

Wyłączanie sieci Wi-Fi

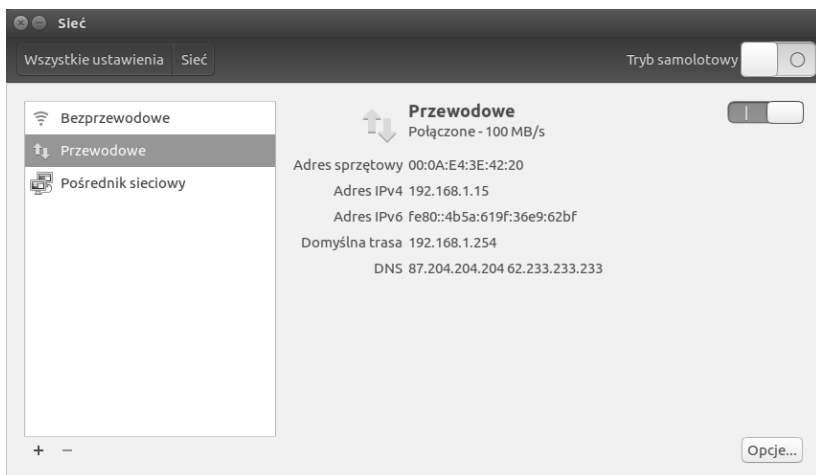
System macOS nie pozwala korzystać z dwóch różnych połączeń sieciowych jednocześnie. Jeżeli zamierzasz eksperymentować z ustawieniami sieci przewodowej i bezprzewodowej, przed wybraniem połączenia Ethernet musisz wyłączyć sieć Wi-Fi. W tym celu w oknie ustawień kliknij przycisk *Wyłącz Wi-Fi*. Sieć Wi-Fi możesz również wyłączyć, klikając ikonę w pasku narzędzi. Sieć będzie wyłączona tak długo, dopóki jej ręcznie nie włączysz. Aby reaktywować połączenie, kliknij je w oknie po lewej stronie. Jeżeli połączenie wykorzystuje protokół DHCP, kliknij przycisk *Zaawansowane*, a następnie przycisk *Odśwież dzierżawę DHCP*.

Linux

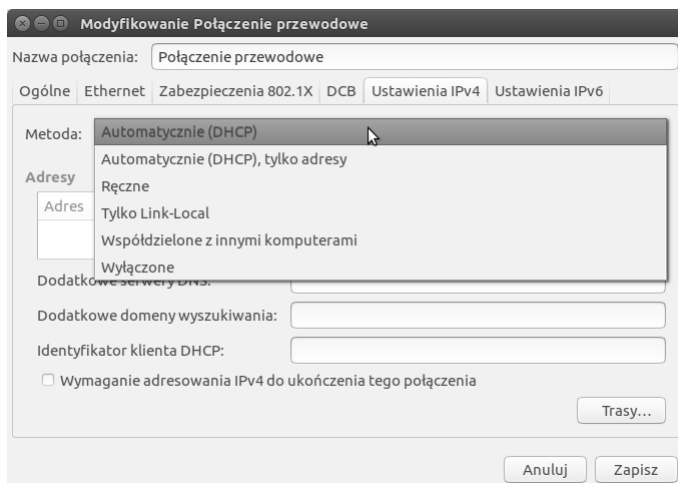
Ubuntu jest popularną odmianą systemu Linux opartą na dystrybucji Debian. W tym systemie wykorzystany jest panel Unity wyglądający nieco inaczej niż w innych dystrybucjach systemu, ale korzysta się z niego w podobny sposób.

Tak jak w systemach Windows i macOS, również w systemie Ubuntu dostępna jest ikona na pasku narzędzi umożliwiająca szybkie uzyskanie dostępu do ustawień sieciowych. Można również kliknąć ikonę *Ustawienia systemu* (przedstawiającą koło zębate i klucz), a następnie ikonę *Sieć* w części *Sprzęt*.

W głównym oknie *Sieć* (rysunek 12.13) można sprawdzić i zmienić ustawienia sieci przewodowej i bezprzewodowej, jak również ustawienia serwera proxy. Aby skonfigurować sieć przewodową, kliknij przycisk *Opcje*. W oknie *Modyfikowanie Połączenie przewodowe* kliknij zakładkę *Ustawienia IPv4*. Za pomocą listy *Metoda* (rysunek 12.14) wybierz dynamiczne przypisywanie adresu IP za pomocą protokołu DHCP lub ręczną konfigurację adresu statycznego. W tej zakładce możesz również wprowadzić dane serwerów DNS, bramy domyślnej i parametry trasowania.

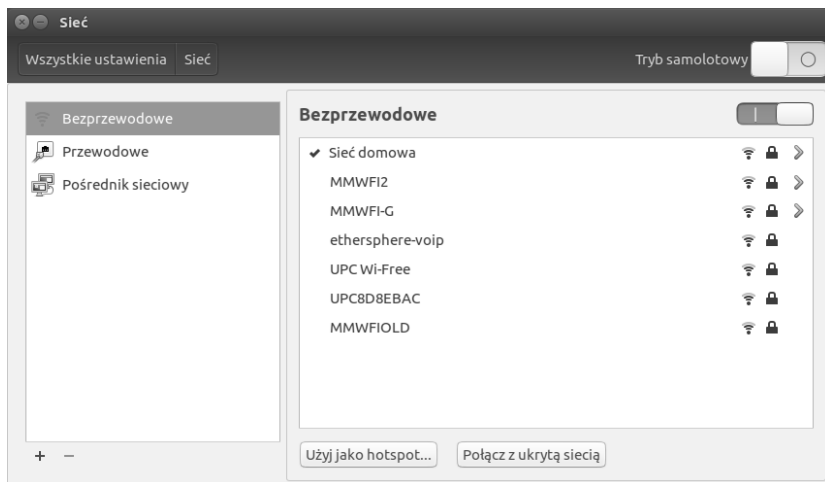


RYSUNEK 12.13. Okno z ustawieniami sieciowymi w systemie Linux Ubuntu



RYSUNEK 12.14. Okno do modyfikowania połączenia sieciowego umożliwiające wybranie automatycznego lub statycznego przypisywania adresu IP

W oknie *Sieć* kliknij w panelu po lewej stronie pozycję *Bezprzewodowe* i otwórz okno z ustawieniami sieci bezprzewodowej (rysunek 12.15). W tym oknie możesz połączyć się z jawną lub ukrytą siecią. Po kliknięciu symbolu strzałki po prawej stronie nazwy sieci otwiera się okno z ustawieniami wybranego połączenia.



RYSUNEK 12.15. Wybierz z listy dostępną sieć bezprzewodową; symbol strzałki po prawej stronie otwiera okno z ustawieniami połączenia

System Linux ma to do siebie, że w jego różnych odmianach (dotyczy to również starszych wersji odmiany Ubuntu) okna konfiguracyjne wyglądają nieco inaczej. Niemniej jednak wszystkie pełnią funkcję interfejsu graficznego służącego do modyfikowania plików konfiguracyjnych. Szczególnie ważny jest plik `/etc/network/interfaces` zawierający adresy IP i inne ważne ustawienia.

W powyższym pliku statyczna konfiguracja interfejsu *eth0* (pierwszej karty sieciowej) wygląda następująco:

```
iface eth0 inet static
address 203.121.14.13
netmask 255.255.255.0
gateway 203.121.14.1
```

Wpisy konfigurujące przypisywanie ustawień za pomocą protokołu DHCP wyglądają tak:

```
auto eth0
iface eth0 inet dhcp
```

Plik */etc/network/interfaces* może zawierać wiele innych ustawień. Szczegółowe informacje na ten temat znajdziesz w dokumentacji do systemu Linux.

W systemie Linux, inaczej niż w systemach Windows i macOS, wciąż z powodzeniem jest wykorzystywany wiersz poleceń. Wielu użytkowników woli konfigurować i diagnozować połączenia sieciowe za pomocą narzędzi wiersza poleceń, które poznasz w rozdziale 14.

Z powodu problemów z uzyskiwaniem bieżących informacji o sterownikach sprzętowych i ich funkcjonowaniu w otwartych systemach operacyjnych połączenia bezprzewodowe niekiedy wymagają dodatkowej konfiguracji. Jeżeli używasz systemu Ubuntu, zapoznaj się z przewodnikiem *Ubuntu Wireless Troubleshooting Guide* (podręcznik diagnostyczny do sieci bezprzewodowych w systemie Ubuntu: <https://help.ubuntu.com/community/WifiDocs/WirelessTroubleShootingGuide>). Serwis Linux Wireless Wiki (<http://wireless.wiki.kernel.org>) również jest dobrym źródłem ogólnych informacji o obsłudze sieci bezprzewodowych w systemach Linux.

Podsumowanie

Na początku tego rozdziału został opisany protokół DHCP umożliwiający przypisywanie komputerom adresów IP i innych ustawień sieciowych. Serwer DHCP przydziela komputerom adresy IP (jak również inne ustawienia konfiguracyjne). Protokół DHCP jest dzisiaj tak szeroko stosowany, że w większości sieci stanowi standard. Komputer skonfigurowany tak, aby uzyskiwał dynamicznie adres IP, jest klientem serwera DHCP.

W tym rozdziale została również opisana translacja NAT i protokoły automatycznej konfiguracji. Na koniec przedstawionych zostało kilka przykładów konfigurowania ustawień TCP/IP w systemach Windows, macOS i Linux.

Pytania i odpowiedzi

P.: W jaki sposób komputer użytkownika po uruchomieniu komunikuje się z serwerem DHCP?

O.: Poprzez rozsyłanie i odbieranie komunikatów rozgłoszeniowych.

P. W jaki sposób translacja NAT zwiększa bezpieczeństwo sieci?

O.: Ponieważ lokalne adresy IP nie są powiązane z adresami internetowymi i nie mogą być w tej sieci stosowane, haker z zewnątrz nie może nawiązać połączenia z komputerem w lokalnej sieci. Należy jednak pamiętać, że ta ważna cecha nie gwarantuje pełnego bezpieczeństwa. Haker może zastosować wiele innych technik umożliwiających uzyskanie dostępu do sieci z zastosowaną translacją NAT.

Warsztaty

Poniższe warsztaty składają się z serii pytań i praktycznych ćwiczeń. Pytania mają na celu sprawdzenie Twojej ogólnej wiedzy o tematach opisanych w bieżącym rozdziale. Ćwiczenia praktyczne dadzą Ci możliwość wykorzystania pojęć opisanych w ciągu tej godziny. Zanim przejdziesz do następnego rozdziału, poświęć nieco czasu na rozwiązanie quizu i wykonanie ćwiczeń. Odpowiedzi na pytania znajdziesz w dodatku A, „Odpowiedzi na pytania i rozwiązania ćwiczeń”.

Quiz

1. Co należy zrobić, aby komputer użytkownika mógł uzyskiwać adres IP z serwera DHCP znajdującego się w innej sieci?
2. Jakiego rodzaju rekordy są głównie wykorzystywane w usłudze DNS-SD?

Ćwiczenia

Jeżeli Twój komputer nie łączy się z siecią, musisz przede wszystkim odnowić przypisanie adresu IP za pomocą protokołu DHCP. W tym celu, jeżeli używasz systemu macOS, rozwiń główne menu i wybierz polecenie *Preferencje systemowe*. W oknie *Preferencje systemowe* kliknij ikonę *Sieć* (jak w jednej z poprzednich części rozdziału). Następnie wybierz opcję *Ethernet*, jeżeli korzystasz z sieci przewodowej, lub *Wi-Fi* (w starszych wersjach systemu *AirPort*) w przypadku sieci bezprzewodowej.

W oknie konfiguracyjnym będzie widoczny aktualny adres IP. Kliknij przycisk *Zaawansowane*, następnie zakładkę *TCP/IP* i przycisk *Odśwież dzierżawę DHCP*. W zależności od wersji systemu ta procedura może wyglądać inaczej, dlatego jeżeli nie odpowiada powyższemu opisowi, przyjrzyj się dokładnie zawartości okien i poszukaj odpowiedników wyżej wymienionych opcji. Twój komputer powinien usunąć aktualne ustawienia i uzyskać z serwera DHCP nowy adres. (W zależności od serwera DHCP i jego konfiguracji może się zdarzyć, że adres będzie taki sam).

Aby wykonać to samo ćwiczenie w systemie Windows, będziesz potrzebował uprawnień administratora. W celu ich uzyskania kliknij prawym przyciskiem ikonę wiersza poleceń i wybierz opcję *Uruchom jako administrator*. Wpisz hasło administratora, a jeżeli jesteś już zalogowany jako administrator, potwierdź chęć wykonania operacji. Aby sprawdzić bieżący adres IP, w oknie wpisz polecenie:

```
ipconfig
```

Następnie wpisz poniższe polecenie, aby zwolnić przypisany adres IP:

```
ipconfig /release
```

Ponownie wpisz:

```
ipconfig
```

Adres IP powinien zniknąć. Czasami zdarza się, że komputer sam przypisuje sobie lokalny adres z zakresu od 169.254.0.0 do 169.254.255.255.

Wpisz następujące polecenie:

```
ipconfig /renew
```

Jeżeli jeszcze raz wpiszesz polecenie `ipconfig`, zauważysz, że adres IP został przypisany. Więcej na temat tego polecenia i innych narzędzi diagnostycznych dowiesz się z rozdziału 14.

Ważne pojęcia

Poniżej znajduje się lista ważnych pojęć:

- ▶ **APIPA (ang. *Automatic Private IP Addressing*)** — technika przypisywania lokalnych adresów stosowana w niektórych wersjach systemu Windows.
- ▶ **BOOTP** — protokół pierwotnie stosowany do przypisywania adresów komputerom bez dysków twardych.
- ▶ **DHCP (ang. *Dynamic Host Configuration Protocol*)** — protokół dynamicznego przypisywania adresów IP.
- ▶ **Klient DHCP** — komputer uzyskujący dynamiczny adres IP za pomocą protokołu DHCP.
- ▶ **Serwer DHCP** — komputer przydzielający komputerom użytkowników ustawienia konfiguracyjne TCP/IP za pomocą protokołu DHCP.
- ▶ **DNS-SD (ang. *DNS Service Discovery*)** — metoda wykrywania usług stosowana w automatycznie konfigurowanych komputerach.
- ▶ **Lokalna adresacja łącza** — metoda automatycznego przypisywania adresów IP.
- ▶ **LLMNR (ang. *Link-Local Multicast Name Resolution*)** — alternatywna metoda automatycznego odwzorowywania nazw, opracowana przez Microsoft.
- ▶ **Multicast DNS** — technika odwzorowywania nazw bez serwera DNS i bez pliku hostów.
- ▶ **SSDP (ang. *Simple Service Discovery Protocol*)** — opracowana przez Microsoft metoda wykrywania usług oparta na protokole HTTP, a nie usłudze DNS. Protokół SSDP jest powiązany z protokołem UPnP.
- ▶ **Zeroconf** — zestaw protokołów umożliwiających automatyczną konfigurację ustawień TCP/IP.

Skorowidz

A

Adobe Flash, 424

adres

docelowy 54

w sieci

bezprzewodowej, 156

dynamiczny, 354

e-mail, 26

fizyczny, 23, 26, 35, 60,

167, 170, *Patrz też:*

adres MAC

programowalny, 52

ramki, 135

IP, 24, 26, 48, 51, 52, 59,

62, 66, 81, 315

127.0.0.1, 179

datagramu, 135

identyfikator hosta, 63

identyfikator sieci, 63

klasa A, 67, 82, 89, 91

klasa B, 67, 86

klasa C, 67, 68, 86, 87,

88, 90, 91

klasa D, 68

IPv4, 90

IPv6, 90

Konfiguracja błędna, 60

logiczny, 24, 35, 48, 129,

167, 170, *Patrz:*

adres IP

MAC, 23, 52

odwrócony, 189

pętli lokalnej, 73

rozgłoszeniowy, 73, 90

sieci, 73

statyczny, 85

system

bezklasowy, 81

klasowy, 82

URI, *Patrz:*

identyfikator URI

URL, 295, 303, 316, 322

hasło, 317

podmiot, 316

schemat, 316, 322

śledzący, 390

wiadomości, 402, 403

w sieci bezprzewodowej,

156, 157

WWW, 26

źródłowy, 54

adresacja, 33

CIDR, *Patrz:* CIDR

ADSL, 151

agent macierzysty, 160

algorytm

RC4, 159

szyfrowania

symetrycznego, 373

szyfrujący, 370, 371

trasowania

dynamicznego, *Patrz:*

trasowanie

dynamiczne algorytm

API, 35, 123

NetBIOS, 197

aplikacja, 20, 27

FTP, 106

Archie, 293

arkusz kaskadowych stylów,

Patrz: CSS

ARPAnet, 21, 35, 141, 178,

311, 399

AT&T, 312

atak

aplikacyjny, 209, 215,

216

cel, 203

DDoS, 219

DoS, 210, 219

na poświadczenia, 209,

210, 211

zapobieganie, 214

na sieć WWW, 413

podszycania się,

Patrz: phishing

przeciwdziałanie, 220

przez tylne wejście, 210

sieciowy, 209, 215

słownikowy, 213

za pomocą ciasteczek,

387

ATM, 152

audio, 345, 418

autentykator, *Patrz:* podpis

cyfrowy

Autonomous System, *Patrz:*

system autonomiczny

B

back door attack, *Patrz:*

atak przez tylne wejście

baza

danych, 350

MIB, 283, 284

wiedzy, 353

Berners-Lee Tim, 321, 322,

338

bezpieczeństwo, 370

DNS, *Patrz też:* system

DNSSEC

biblioteka RFC, 29

BIND, 187

bit kontrolny, 105, 107

blog, 350, 351, 352

Bluetooth, 162

błąd

danych odbieranych, 47
transmisji, 34, 96

fizyczny, 34
wykrywanie, 102
wykrywanie, 40, 47

brama, 61

domyślna, 134, 273
VoIP, 429
wewnętrzna, 141

bridge, *Patrz:* most

broadcast, *Patrz:*

rozgłaszanie

burza rozgłoszeniowa, 273

C

CA, 376

caching-only server,

Patrz: serwer buforujący

Cascading Style Sheet,

Patrz: CSS

centrum danych, 441, 442

Cerf Vinton, 22

certyfikat cyfrowy, 376, 377

CGI, 333

Chatty Things, 450

chmura, 312, 433

bezpieczeństwo

danych, 436

EC2, 443

hybrydowa, 438

prywatna, 443

ciasteczko, 342, 343, 385

sesyjne, 386

śledzące, 386

trwałe, 386, 387

ustawienia, 388

zarządzanie, 388

zewnętrzne, 387

CIDR, 63, 81, 83, 91, 92, 145

sufiks, *Patrz:* sufiks CIDR

CMS, 328, 350

cookie, *Patrz:* ciasteczko

CSS, 328

czytnik

RFID, 454

wiadomości, *Patrz:*

program pocztowy

D

dane

audio, *Patrz:* audio

autentyczność, 374

bezpieczeństwo, 102

centrum, *Patrz:* centrum

danych

demultipleksacja, 96, 101

kopia zapasowa, 436

multipleksacja, 96, 101

porządkowanie, 102, 108

poufność, 374

priorytet, 102

przetwarzanie

strumieniowe, 102

sterowanie przepływem,

102, 108

szyfrowanie, *Patrz:*

szyfrowanie

transmisja w czasie

rzeczywistym, 110

weryfikowanie

poprawności, 96

wideo, *Patrz:* wideo

datagram, 39, 54, 61, 134,

165

IP, 41

UDP, 108

DDNS, 185

default gateway,

Patrz: brama domyślna

default route, *Patrz:* trasa

domyślna

dekoder, 418

demilitarized zone,

Patrz: DMZ

demon, 295, *Patrz też:*

usługa

denial of service,

Patrz: atak DoS

deszyfrowanie, 370

DHCP, 150, 185

distance-vector, *Patrz:*

wektor odległości

Distinguished Name,

Patrz: DN

DMZ, 204

DN, 302, 303

DNS, 26, 28, 119, 121, 178,

179, 180, 181, 273, 313,

Patrz też: serwer DNS

bezpieczeństwo, 190,

191, 192

implementacja, 187

konfiguracja, 187

testowanie, 193, 194, 195

Unix/Linux, 187

Windows, 187

wykrywanie usług, 197

dokument

HTML, 324, 325

przesyłanie, 329, 330

statyczny, 328

metadane, 324

RFC, 29

treść, 328

WDSL, 360

domena, 179, 181, 187

handlowanie, 186

nazwa, 26, 182, 183

rejestrowanie, 185, 186

struktura, 182, 183

Dreamweaver, 350

DSL, 151

DSLAM, 151

E

e-mail, *Patrz:* usługa poczta

elektroniczna

EME, 427

enkapsulacja, 35

Ethernet, *Patrz:*

technologia Ethernet

F

Facebook, 351

FCS, 54

Fielding Roy, 361

firewall, *Patrz:* zaporą

ogniowa

Foreign Agent, *Patrz:* agent

obcy

format

audio, 418, 420

binarny, 68, 69, 70

dziesiętny, 68, 70
JSON, 356
MIME, 400, 401
video, 418, 420
XML, 356, 359
formularz, 333
FQDN, 179, 181
ftp, 28
FTP, 119, 121, 295
 bezpieczeństwo, 298
 transmisja, 297
 binarna, 296, 297
 tekstowa, 296, 297
Fully Qualified Domain
Name, *Patrz:* FQDN

G

gniazdo, 98, 99, 378
Google Analytics, 390
Gopher, 293
GPS, 345
grafika skalarna, 344
Graphical User Interface,
 Patrz: GUI
GUI, 304

H

haker profil psychologiczny,
 208
handel elektroniczny, 363,
 365
hasło, 210, 211
 przechwytywanie, 210,
 212, 213
 szyfrowanie, 213, 214, 372
 uzyskiwanie, 210, 211,
 212
HDLC, 152
HDSL, 151
hipertekst, 322
Home Agent, *Patrz:* agent
macierzysty
host, 62, 67, 81
 identyfikator, 83, 84, 85,
 87
 nazwa, 177, 178, 181
 plik, *Patrz:* plik hostów

hostname, *Patrz:* host nazwa
hub, 26, 167, 170
 inteligentny, 168
 problemy, 272

I

IaaS, 434, 437, 438
IAB, 28, 313
IANA, 28, 99, 144, 313
ICANN, 28, 99, 185, 313
identyfikator
 RFID, 454
 URI, 316, 317, 322, 339
 URN, 316
IDSL, 151
IETF, 28, 29, 313
implementacja, 21
 TCP/IP, *Patrz:* TCP/IP
 implementacja
Infrastructure as a Service,
 Patrz: IaaS
infrastruktura jako usługa,
 Patrz: IaaS
interfejs
 API, *Patrz:* API
 aplikacji sieciowych, 95
 CGI, *Patrz:* CGI
 lokalny, 143, 179
 Sockets, 123
 użytkownika
 graficzny, *Patrz:* GUI
 tekstowy, 400
Internet, 129, 140, 141,
 143, 311
 działanie, 314
 poziom, 311, 312
 prywatność, 392
 rzeczy, *Patrz:* IoT
 śledzenie
 użytkowników, 384,
 385, 387, 390
 Do Not Track, 391,
 392
Internet Architecture
Board, *Patrz:* IAB
Internet Assigned Numbers
Authority, *Patrz:* IANA

Internet Corporation for
Assigned Names and
Numbers, *Patrz:* ICANN
Internet Engineering Task
Force, *Patrz:* IETF
Internet Research Task
Force, *Patrz:* IRTF
Internet Service Provider,
 Patrz: ISP
inter sieć, 35
IoT, 447, 454
 platforma
 administracyjna, 448,
 449
IoTivity, 450
IRTF, 28
ISDN, 152
ISP, 141, 150, 294, 312
IXP, *Patrz:* punkt IXP

J

język
 AJAX, 334
 HTML, 321, 324, 328
 interfejs graficzny,
 350
 HTML5, 336, 341, 342
 funkcje
 geolokalizacyjne,
 345
 mikrodane,
 Patrz: mikrodane
 multimedia, 344
 tworzenie grafiki, 344
 znacznik, 345
JavaScript, 334
opisu usług WWW,
 Patrz: WSDL
PHP, 333, 334
skryptowy, 334
TeX, 322
VBScript, 334
WDSL, 359, 360
WSDL, 357, 360
XHTML, 328, 341
XML, 328, 341, 357, 358,
 360
 schemat, 358

język

znaczników, 321, 322, 324

rozszerzalny,

Patrz: język XML

Juggernaut, 215

K

Kahn Robert, 22

kanał RSS, 418, 428

karta

dostępowa, 454

Ethernet, 60

adres, 23

kredytowa, 363

radiowa, 155

sieciowa, 47

adres, 23, 24, 60, 62

oprogramowanie, 33

sterownik, 48

katalog

informacji, 302

Microsoft Active

Directory, 302, 304

schemat, 302

zasobów sieciowych, 302

klient, 106

klucz

DNSKEY, 191, 192

szyfrujący, 371, 372

prywatny, 374

publiczny, 374, 375,

376

zabezpieczanie, 382

zmienianie, 373

kod

ASCII, 322

formatujący, 328

HTML, *Patrz:* język

HTML

śledzący, 390

kodek, 344

kolizja ramek, *Patrz:* ramka

kolizja

komputer

dostęp zdalny, 304, 305

wieloadresowy, 130,

131, 132

komunikat, 38

Destination Unreachable, 76

Echo Reply, 75

Echo Request, 75

Fragmentation Needed, 76

ICMP, 75, 108

metadane, 361

SOAP, 359

Source Quench, 76

Time Exceeded, 76

Koncentrator CMTS, 150, 151

kontener, 440, 441

koń trojański, 210, 211, 212

Kubernetes, 441

L

LAMP, 360

LAN, 299, 314, 380

link-state, *Patrz:* stan łącza

login, 210, 211

loopback, *Patrz:* interfejs

lokalny

lpr, 28

Ł

łańcuch zaufania, 191

M

magazyn

danych lokalny, 342, 343

wady, 343

DOM, 342

WWW, 342

makro, 409

mapa sieci, 139, 143

maska

podsieci, 83, 85, 89

format binarny, 85

format dziesiętny, 86

supersieci, 91

VLSM, 91, *Patrz też:*

sufiks CIDR

maszyna wirtualna, 439,

440, 441, 442

matrioszka, 39

MediaWiki, 353

medium, 19

metadane, 361

metoda CSMA/CD, 52, 53

mikrodane, 346

mikroformat, 340, 341, 346

hCard, 340

model

ARPAnet, 35

DOM, 344

OSI, 36, 49, 118

pięciowarstwowy, 35

TCP/IP, *Patrz:* TCP/IP

model

modem, 150, 162

DSL, *Patrz:* DSL

telefoniczny, 149, 150,

162, *Patrz też:*

połączenie

wdzwaniane

telewizyjny, 150

moduł PAM, *Patrz:* PAM

most, 26, 150, 161, 167

MQTT, 450

MSE, 427

multihomed computer,

Patrz: komputer

wieloadresowy

multimedia, 417, 428

strumieniowanie, 293,

418, 419, 421, 424

protokół HTML5, 427

protokół HTTP, 425

udostępnianie, 418

multiplexer DSLAM,

Patrz: DSLAM

N

nagłówki, 35, 38, 64, 130

budowa, 64, 65, 66

DNT, 391, 392

TCP, 104, 105

UDP, 109

Napster, 354

narzędzie, *Patrz też:*

polecenie
 arp, 124, 267
 dig, 195
 finger, 124
 ftp, 124, 295
 hostname, 124, 273
 ifconfig, 124
 konfiguracyjne, 267, 269
 netstat, 124, 276
 nslookup, 273
 NSLookup, 194
 NX, 305
 pcAnywhere, 305
 ping, 124, 193, 219, 266, 267, 272
 opcje, 268
 r*, 279
 rcp, 280
 Resolve, 273
 rexec, 280
 Rlogin, 280
 route, 124, 275
 rr*, 280
 rsh, 280
 ruptime, 280
 rwho, 280
 scp, 281
 sftp, 281
 ssh, 281
 tftp, 124
 Timbuktu, 305
 traceroute, 124, 273, 274, 275
 VNC, 305
 Zdalny pulpit, 305
 NAT, 24, 28, 60, 64, 73, 171, 207
 National
 Telecommunications
 and Information
 Administration,
 Patrz: NTIA
 nazwa
 hosta, *Patrz:* host nazwa
 odwzorowywanie, *Patrz:*
 odwzorowywanie
 nazw

 w pełni kwalifikowana,
 Patrz: FQDN
 wyróżniająca, *Patrz:* DN
 względna wyróżniająca,
 Patrz: RDN
 Nessus, 215
 NetBIOS, 26, 197, 198
 nazwa komputera, 198
 NFS, 120, 121
 Nmap, 210, 215
 nslookup, 28
 NTIA, 28
 numer
 AS, 144
 ASN, 144
 VLAN, 54

O

odnośnik, 321, 322, 324, 325, 327
 odwzorowywanie nazw, 117, 121, 177, 178, 184, 185
 hierarchiczne, 178
 problemy, 272, 273
 w małej sieci, 179
 okno ruchome, 108
 oktet, 66
 Open Shortest Path First,
 Patrz: OSPF
 OpenSSH, 281
 OpenStack, 441
 oprogramowanie
 jako usługa, 434, 435
 wirtualizacyjne, 440
 OSPF, *Patrz:* protokół OSPF

P

PaaS, 434, 438
 pakiet, 39, 165
 LCP, 165
 NCP, 165
 SSH, 298, *Patrz też:*
 protokół SSH
 PAM, 304
 pętla
 lokalna, 73
 transmisyjna, 76

phishing, 218, 413
 piksel śledzący, 390
 ping, 28
 PIR, 185
 Platform as a Service,
 Patrz: PaaS
 platforma, 438
 opisywania zasobów, 339
 RDF, 339, 340
 trójka, 339, 340
 platforma jako usługa,
 Patrz: PaaS
 plik
 /etc/hosts.equiv, 280, 281
 audio, *Patrz:* audio
 CSS, 358
 hostów, 177, 178, 179, 180, 272
 hosts.txt, 178
 manifestu pamięci, 343
 multimedialny,
 Patrz: multimedia
 odwrotnego
 przeszukiwania strefy,
 189
 rhosts, 280, 281
 strefy, 187, 188
 wideo, *Patrz:* wideo
 XML, 350
 XSD, 358
 Pluggable Authentication
 Module, *Patrz:* PAM
 podcasting, 428
 podpis cyfrowy, 375
 podsieć, 24, 63, 64, 68, 81, 83, 170
 agregowanie, 91
 identyfikator, 83, 86
 maska, *Patrz:* maska
 podsieci
 podwarstwa
 LLC, 49
 MAC, 49, 52
 polecenie, *Patrz też:*
 narzędzie
 arp, 271
 ascii, 297
 binary, 297

- polecenie
 - bye, 297
 - cd, 297
 - close, 297
 - DELETE, 361
 - dir, 296
 - ftp, 296
 - get, 285, 297
 - GET, 330, 361
 - getnext, 285
 - HEAD, 361
 - help, 296
 - ifconfig, 269, 270
 - ls, 296
 - mget, 297
 - mkdir, 297
 - mput, 297
 - open, 297
 - ping, 28, 75
 - POST, 361
 - put, 297
 - PUT, 361
 - pwd, 297
 - quit, 297
 - Resolve-DnsName, 196
 - rmdir, 297
 - set, 285
 - status, 297
 - Test-NetConnection, 196
 - tftp, 298
 - type, 297
 - user, 296
- połączenie
 - głosowe, 428
 - peer-to-peer, 354
 - punkt – punkt, 162, 163, 381
 - TCP, 295
 - Telnet, *Patrz:* Telnet
 - VPN, 215, 381, 392, 412
 - wdzwaniane, 162, 163, 380
- POP, *Patrz:* punkt POP
- port, 27
 - 22, 110
 - 389, 302
 - 80, 317
- blokowanie dostępu,
 - 110, 111
- dobrze znany, *Patrz:*
 - port standardowy
- Ethernet, 150
- numer, 98, 315
- otwarcie, 106
- standardowy, 99, 101, 317
 - lista, 99, 100
- TCP, 27
- UDP, 27
- portal społecznościowy, 293, 351
- potrójny uścisk dłoni, 107
- powłoka
 - bezpieczna, *Patrz:* SSH
 - PowerShell, 196, 273
 - SSH, *Patrz:* SSH
- preambuła, 54
- procedura obsługi karty sieciowej, 47
- proces
 - ftpd, 295
 - routed, 142
- program pocztowy, 96, 294, 401, 408, 409
- protokół, 20
 - ARP, 52, 60, 74, 134, 180, 270
 - bezpoległościowy, 40, 96, 97, 101
 - BGP, 141, 144
 - BGP4, 145
 - BitTorrent, 119
 - Bluetooth Encapsulation, 161
 - BOOTP, 75, 298
 - Chatty Things, 450
 - CIFS, 119, 121, 299, 300, 301
 - dane statystyczne, 276
 - DCCP, 110, 425
 - DHCP, 119, 185
 - DNS, 119, 121
 - DSL, 151
 - DTLS, 379
 - dynamiczny, 132, 134
 - eBGP, 144
 - EIGRP, 143
 - Finger, 120
 - Flash, 424
 - FTP, 119, 121
 - H.323, 429
 - HTML5, 427
 - HTTP, 120, 122, 293, 294, 317, 321, 356, 425
 - polecenia, 361
 - wersja, 329, 331, 332
 - iBGP, 144
 - ICMP, 75, 269, 273
 - IGP, 141
 - IGRP, 143
 - IMAP, 120, 294, 401, 403, 407, 408
 - implementacja, 138
 - IoTivity, 450
 - IP, 60, 62, 180
 - mobilny, *Patrz:* sieć bezprzewodowa MIP
 - IPsec, 76, 379, 380, 381
 - IPv4, 62
 - IPv6, 28, 62, 64, 76, 145
 - Kerberos, 304, 382, 383, 384
 - nazwa, 384
 - komunikatów kontrolnych, 75
 - LCP, 164
 - LDAP, 120, 216, 301, 303
 - adres danych, 303, 304
 - format danych, 303
 - uwierzytelnianie, 304
 - MQTT, 450, 452
 - NCP, 165
 - NFS, 120, 121, 299, 300
 - NTP, 120
 - OpenLDAP, 302
 - OSPF, 137, 141, 142, 143, 145
 - połączeniowy, 40, 96, 97, 101
 - POP, 120, 294, 403, 407, 408
 - PPP, 152, 164, 165
 - PPPoE, 152
 - punkt – punkt, 152, 164
 - RARP, 52, 75, 298

RDP, 305
 RIP, 137, 141, 142, 145
 RIPng, 142
 RMON, 282, 286, 287
 RPC, 120
 RTCP, 422, 423
 RTMP, 424
 RTP, 110, 421, 422, 429
 SCTP, 110, 425
 SIP, 429
 SLIP, 164, 165
 SMB, 120, 121, 299, 300, 301
 sesja, 300
 SMTP, 294, 399, 402, 404, 406, 408
 SNMP, 120, 282, 283
 agent, 282, 283, 285
 baza MIB, *Patrz:* baza MIB
 monitor, 282, 283, 285
 wady, 286
 SOAP, 351, 358, 360, 362
 SSH, 110, 277, 279
 SSL, 378, 379
 statyczny, 132
 stos, 34
 system, *Patrz:* system protokołów
 szyfrujący, 335
 TCP, 40, 96, 98, 101, 102, 144, 295, 299, 302, *Patrz:* nagłówek TCP
 blokowanie portu, 110
 nawiązanie połączenia, 103
 połączenie, 106, 107, 108
 zamykanie połączenia, 102
 TCP/IP, *Patrz:* TCP/IP
 Telnet, *Patrz:* Telnet
 TFTP, 121, 298
 implementacja, 298

TLS, 378, 379
 transmisji danych
 w czasie rzeczywistym, 110
 trasowania, 137
 UDP, 38, 40, 41, 96, 98, 101, 102, 108, 109, 298, 299, *Patrz:* nagłówek UDP
 blokowanie portu, 110
 uwierzytelniający
 EAP, 159
 Kerberos, 159
 WinSock, 123
 zbiór, 21
 przeglądarka, 96, 335, 336
 blokowanie skryptów, 334, 337
 Chrome, 388
 Firefox, 336, 388
 blokowanie skryptów, 390
 Internet Explorer, 335, 337, 388
 Microsoft Edge, 337
 obsługa ciasteczek, 388
 Safari, 337
 wtyczka, 336
 wyświetlanie kodu strony, 352
 przełącznik, 26, 53, 168, 170
 cut-through, 169
 ograniczenia, 171
 store and forward, 169
 warstwy
 drugiej, 170
 trzeciej, 170
 pseudonagłówek, 105, 108, 110
 Public Internet Registry, *Patrz:* PIR
 punkt
 dostępowy, 155
 NAP, 161
 IXP, 312
 POP, 312

Q

QoS, 145, 418
 Quality of Service, *Patrz:* QoS
 Qwest, 312

R

ramka, 39, 41, 54, 130
 Ethernet, 54
 filtrowanie, 150
 kolizja, 53
 numer kontrolny, 54, *Patrz też:* FCS
 PPP, 165
 RDN, 302
 readresator, 122
 redirector, *Patrz:* readresator
 reguła filtrująca, 205
 rekord, 187
 Relative Distinguished Name, *Patrz:* RDN
 requester, *Patrz:* readresator
 REST, 360, 361, 362, 363
 router, 24, 25, 103, 129, 171, 201
 aktywny, 142
 bezprowodowy, 155
 identyfikator, 143
 pasywny, 142
 wewnętrzny, 141, 144
 wieloprotokołowość, 142
 zewnętrzny, 141, 144
 routing, 25, 26, *Patrz też:* trasowanie
 dynamiczny, *Patrz:* trasowanie
 dynamiczne
 rozgłaszanie, 68, 109

S

- SaaS, 434, 435
- SDSL, 151
- Secure Shell, *Patrz:* SSH
- segment, 38
- serwer, 106
 - buforujący, 186
 - CIFS, 300
 - DHCP, 60, 85, 86, 171
 - DNS, 181, 273,
 - Patrz też:* DNS
 - odpytywanie, 210
 - dodatkowy, 186
 - FTP, 106, 204
 - KDC, 382
 - nazw, 26, 273
 - pocztowy, 204
 - poczty, 294
 - proxy, 62, 68, 207
 - odwrotny, 208
 - zapamiętywanie treści, 207
 - rezerwowy, 186
 - wirtualny, 437
 - zaufany, 191
- serwis informacyjny, 350
- sesja
 - FTP, 295
 - przechwytywanie, 387
 - SSH, 110
- sieć, 19, 20, 81
 - 802.11, 154, 155, 156, 157, 158
 - adres, *Patrz:* adres sieci
 - anonimowa, 392
 - ARPAnet, *Patrz:* ARPAnet
 - bezczłowna, 154, 155
 - bezpieczeństwo, 158, 161
 - Bluetooth, 161
 - MIP, 159
 - przyłączanie, 158
 - diagnostyka, 35
 - Ethernet, 24, 41, 50,
 - Patrz też:* technologia Ethernet
 - Fast Ethernet, 53
 - IBSS, 155
 - identyfikator, 82, 83, 86, 87
 - Internet, *Patrz:* Internet
 - IoT, 448, 450
 - konfigurowanie, 86
 - LAN, 22, 23, 41, 60, 170
 - architektura, 49
 - technologia, *Patrz:* technologia
 - topologia, 49
 - warstwa, 49
 - mapa, *Patrz:* mapa sieci
 - NSFNET, 311
 - P2P, *Patrz:* sieć peer-to-peer
 - peer-to-peer, 354, 355
 - problemy z wydajnością, 273
 - prywatna wirtualna,
 - Patrz:* sieć VPN
 - rozległa, *Patrz:* sieć WAN
 - rozproszona, 354
 - semantyczna, 316, 338, 339, 345
 - strukturalna BSS, 155
 - telefoniczna, 162
 - telewizji kablowej, 150
 - TOR, 392
 - VPN, 381, 392
 - WAN, 152, 153, 299, 380
 - zarządzanie, 282, 283
- skaner sieciowy, 210, 215
- skok, 138, 139, 142
- skrypt, 332, 334
 - blokowanie, 390
 - kliencki, 332, 334, 342
 - zagrożenia, 334
 - międzydomenowy, 387
 - PHP, 333
 - serwerowy, 332, 333, 334
 - startowy, 138
 - śledzący, 390
- Slash, 352
- sliding window, *Patrz:* okno
- sliding window, 393
- Snowden Edward, 393
- Software as a Service,
 - Patrz:* SaaS
- spam, 411
 - lista, 411, 412
 - ograniczanie, 412
- Sprint, 312
- SSH, 122, 281
- stacja robocza, 298
- Stallings William, 384
- stan łącza, 137, 138, 139, 142, 143
- zalety, 139
- standard, 21
 - 802.11, 155, 156, 157, 158
 - 802.11i, 159
 - AES, 373
 - CIM, 282
 - DES, 373
 - DOCSIS, 151
 - DSL, *Patrz:* DSL
 - RFC 1661, 164, 165
 - szyfrowania danych,
 - Patrz:* standard DES
 - WBEM, 282
 - WEP, *Patrz:* szyfrowanie WEP
 - zaawansowanego
 - szyfrowania, *Patrz:* standard AES
- standard TCP/IP, *Patrz:* TCP/IP standard
- stateful firewall, *Patrz:* zaporowa stanowa
- sterownik
 - karty sieciowej, *Patrz:* karta sieciowa
 - sterownik
 - MAC, 49
- stos protokołów, *Patrz:* :
 - protokół stos
- strefa, 187
 - plik, *Patrz:* plik strefy
 - przeszukiwanie
 - odwrotne, 189
 - transfer, 186
 - zdemilitaryzowana,
 - Patrz:* DMZ

strona
 publikowanie, 350
 tworzenie, 350
 wyświetlanie kodu w przeglądarce, 352
 strumieniowanie, 293
 sufiks CIDR, 91
 sufiks CIDR, *Patrz też:*
 maska VLSM
 system
 autonomiczny, 141, 144
 BIND, 196
 DDNS, 196
 DNS, *Patrz:* DNS
 DNSSEC, 190, 191, 192
 gospodarza, 439
 gościa, 439
 H.323, 429
 Kerberos, *Patrz:*
 protokół Kerberos
 NetBIOS, *Patrz:* NetBIOS
 operacyjny, 441
 BSD, 123, 142, 279
 plików, 300
 protokołów, 33
 Unix, *Patrz:* Unix
 wirtualny, 439
 zarządzania treścią, 328, 332, *Patrz też:* CMS
 szyfrowanie, 370, 372
 asymetryczne, 374
 IPsec, 214
 konwencjonalne, 372
 odwrotne, 375
 SSL, 214
 symetryczne, 372, 373, 374, 383
 WEP, 158, 159
 WEP2, 159
 WPA2, 159

T

tabela
 ARP, 74, 270, 271
 mostu, 167
 trasowania, 84, 91, 133, 134, 137, *Patrz*
 komputera, 134

minimalizowanie, 138
 optymalizacja, 275
 routera, 134, 137, 142
 wpis statyczny, 138
 TCP/IP, 19, 21, 23, 60, 98, 300
 adresowanie lokalne, 23
 bezpieczeństwo, 378
 diagnozowanie, 265, 266
 historia, 21
 implementacja, 21
 model, 21, 34, 35, 38
 narzędzia, 27
 obsługa błędów, 26
 oprogramowanie, 60
 standard, 21, 48, 50
 standaryzacja, 29
 usługa, 21
 zabezpieczenia, 377
 technologia, 49
 ASP, 334
 ATM, *Patrz:* ATM
 bezprzewodowa, 52, 153, 154
 IEEE 802.3, 50
 IEEE 802.11, 153, 154, 155, 156, 157, 158, 159
 bezpieczeństwo, 158, 161
 Bluetooth, 161
 MIP, 159
 CGI, *Patrz:* CGI
 Ethernet, 50, 51, 52
 bezprzewodowy, 154
 oprogramowanie, 54
 ramka, *Patrz:* ramka
 Ethernet
 Frame Relay, 152
 Gigabit Ethernet, 53
 HDLC, *Patrz:* HDLC
 IEEE 802, 50
 ISDN, *Patrz:* ISDN
 peer-to-peer, 314
 Point-to-Point Protocol, 50
 PPP, 50
 RFID, 454
 RSS, 428

specyfikacja, 49
 WiMAX, 50
 WLAN), 50
 telefonia internetowa, 418, 428
 Telnet, 277, 279
 terminal, 22
 token śledzący, 390
 traceroute, 28
 transfer stref, 186
 translacja NAT, *Patrz:* NAT
 trasa
 domyślna, 134
 śledzenie, 273
 trasowanie, 130, 132, 135, *Patrz też:* routing
 Bellmana-Forda, 138
 bezklasowe, 145
 bezpośrednie, 136
 cebulowe, 392
 dynamiczne, 22, 132, 134, 137
 algorytm, 137
 pośrednie, 136
 stan łączy, *Patrz:* stan łączy
 statyczne, 132, 137
 tabela, *Patrz:* tabela
 trasowania
 w dużych sieciach, 140
 wektor odległości, *Patrz:* wektor odległości
 trojan, *Patrz:* koń trojański

U

Unix, 23, 142
 urząd certyfikacyjny, *Patrz:* CA
 urządzenie
 bezprzewodowe, 155, 156, 161
 kompatybilność, 158
 zmiana położenia, 154, 156, 158, 160
 GPS, *Patrz:* GPS
 inteligentne, 454
 końcowe, 22, 103

urządzenie
 m warstwy trzeciej, 129
 NAP, 161
 peryferyjne, 22
 sieciowe, 166
 warstwy trzeciej,
Patrz: router
 usługa, 295, *Patrz też:*
 demon
 AWS, 442, 443
 DDNS, *Patrz: DDNS*
 DHCP, *Patrz: DHCP*
 DNS, 121
 drukowania plików, 120
 FTP, *Patrz: FTP*
 infrastruktura, *Patrz:*
 IaaS
 jakość, *Patrz: QoS*
 katalogowa
 udostępnianie, 301,
 302
 LDAP, 293
 oprogramowanie,
Patrz: SaaS
 platforma, *Patrz: PaaS*
 poczta elektroniczna,
 293, 294, 399, 401,
Patrz też: program
 pocztowy, serwer
 poczty
 wiadomość,
Patrz: wiadomość
 załącznik, 400
 readresator,
Patrz: readresator
 RSS, 428
 sieciowa, 119
 SSH, 122
 subskrypcja, 433
 udostępniania plików,
 120, 121
 ukryta, 393
 VoIP, 429
 w chmurze, 434
 webmail, 401, 410
 WWW, 293, 295, 321,
 334, 356
 architektura, 355

architektura REST,
 360, 361, 362, 363
 komponent, 356
 zastosowanie, 356

V

VDSL, 151
 VeriSign, 185, 376
 Verizon, 312
 Veronica, 293

W

warstwa, 36, 145, 170
 aplikacyjna, 35, 36, 37,
 40, 109, 117, 118, 119,
 122, 299, 302
 zapora, 202
 danych, 35, 36, 37, 48
 podwarstwa, 49
 dostępową, 34, 35, 41,
 47, 48, 49, 50, 51, 55,
 130, 132, 133, 158,
 160
 fizyczna, 35, 36, 37, 48
 host – host, 35
 prezentacyjna, 36, 37,
 118
 procesowa/aplikacyjna,
 35, 118
 sesyjna, 36, 37, 118
 sieciowa, 34, 35, 37, 38,
 41, 60, 62, 101, 129,
 160
 transportowa, 26, 35, 37,
 38, 40, 95, 96, 101,
 103, 293, 378
 Web Services Description
 Language, *Patrz: WSDL*
 WECA, 158
 wektor odległości, 137, 138,
 142, 143
 działanie, 138
 wady, 139
 well-known port, *Patrz:*
 port standardowy

węzeł
 SOAP, 359
 TOR, 393
 wiadomość, 400
 adres, 402, 403
 bezpieczeństwo, 413
 nagłówek, 400
 odczytywanie, 401, 406
 prywatność, 413
 treść, 400
 wysyłanie, 401, 402,
 404
 załącznik, 400
 wideo, 344, 345, 418
 format, 419
 kontener, 419
 Wi-Fi Alliance, 158
 Wikipedia, 353
 Windows Defender, 337
 Windows Live Writer, 352
 WINS, 26
 Wireless Ethernet
 Compatibility Alliance,
Patrz: WECA
 wirtualizacja, 439, 440
 wirus, 203, 217, 409
 jądrowy, 217
 wojna przeglądarkowa, 335
 wstrzykiwanie treści, 216

X

X Window System, 117

Z

zakotwiczenie, 325
 zapora
 ogniowa, 92, 110, 111,
 201, 202, 203
 połączona z routerem,
 203
 osobista, 205
 stanowa, 202
 zapytanie, 315, 317
 REST, 361
 SQL, 216

znacznik, 324, 325, 357
!DOCTYPE, 325
a, 325
article, 345
aside, 345
b, 324, 326
body, 324, 325
canvas, 344
font, 325, 326
footer, 345
h1, 324, 326
h2, 324, 326
head, 324, 325

header, 345
hgroup, 345
html, 324, 325
i, 324, 326
img, 325, 390
mark, 345
nav, 345
p, 326
section, 345
style, 325
svg, 344
time, 345
title, 325

tworzenie, 357
u, 324
video, 344, 427
zone, *Patrz:* strefa

Ż

żądanie, 122
ARP, 74
GET, 330

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

Protokół TCP/IP jest podstawą współczesnych technologii sieciowych, a przede wszystkim internetu. Próba rozwiązywania problemów z siecią bez choćby podstawowej wiedzy o TCP/IP prawdopodobnie skończy się porażką. Mimo że ta technologia liczy sobie ponad 30 lat, wciąż jest uważana za kluczową. Założeniem twórców tego protokołu było zbudowanie sieci, która działałaby nieprzerwanie nawet po zniszczeniu części jej fizycznej infrastruktury — i rzeczywiście, internet taki właśnie jest. Niestety, protokół TCP/IP jest dość skomplikowany i wymaga znajomości wielu szczegółów technicznych.

Książka, którą trzymasz w dłoni, została pomyślana jako zwięzły podręcznik składający się z 24 godzinnych lekcji. Znajdziesz tu szczegóły działania protokołów i opis szerokiego spektrum usług dostępnych dziś w internecie. Dowiesz się, jak konfigurować sieci i nimi zarządzać oraz jak rozwiązywać problemy. W obecnym, szóstym już wydaniu znalazły się opisy najnowszych technik, takich jak śledzenie i ochrona prywatności transmisji danych, chmura obliczeniowa, sieci mobilne i internet rzeczy. Zrozumienie prezentowanych treści ułatwią Ci praktyczne przykłady, quizy i ćwiczenia, a także liczne porady i sztuczki niezwykle ułatwiające korzystanie z najlepszych cech TCP/IP.

Najważniejsze zagadnienia ujęte w książce:

- Standard TCP/IP i jego ewolucja, a także model ISO OSI i warstwy sieci
- Bezpieczna transmisja danych
- Protokoły IPv4 i IPv6
- Protokół TCP/IP w środowiskach chmurowych i IoT
- Wydajne strumieniowanie i rozgłaszanie danych
- Diagnostyka i rozwiązywanie problemów z siecią komputerową

Joe Casad — inżynier, który szczególnie interesuje się sieciami komputerowymi i zarządzaniem systemami. Jest również autorem i współautorem kilkunastu książek o tej tematyce. Obecnie ma funkcję redaktora naczelnego pism „Linux Pro Magazine” i „ADMIN Magazine”. Wcześniej był redaktorem naczelnym „C/C++ Users Journal” i redaktorem technicznym „SysAdmin Magazine”.



Już wkrótce poznasz
wszystkie sekrety TCP/IP!

Helion

SAMS

księgarnia internetowa



<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>

Sprawdź najnowsze promocje:
• <http://helion.pl/promocje>
Książki najchętniej czytane:
• <http://helion.pl/bestsellery>
Zamów informacje o nowościach:
• <http://helion.pl/nowosci>

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN 978-83-283-3708-4



9 788328 337084

Informatyka w najlepszym wydaniu

cena: 79,00 zł